Household Equipment Engineering

家庭機器工学

岐阜女子大学

目　次

第１講　電気製品

【学修到達目標】

⎈身のまわりの電気製品について理解することができる。

⎈身のまわりの電気製品について説明することができる。

１．身のまわりの電気製品

身のまわりにはたくさんの「電気製品」「電化製品」「家電製品」がある。

電気製品は、電力を扱う製品すべての意味で、インターホン、キャッシュレジスター、精米機、スピーカー、トランシーバー、生ごみ処理機、マッサージチェアなど多岐に及ぶ。電気製品は、技術進歩などは関係なく、単に電力を用いる製品の総称である。

電化製品の「電化」とは、「熱・光・動力などを、電力を利用することでまかなうようにすること」や「生活に各種の電気器具を取り入れること」を意味する言葉である。電化製品は、「技術進歩により電気式に変わったもの、かつて手作業だったのが電化されたもの」を指す。電化製品の例は、冷蔵庫や洗濯機、電気絨毯、電気ポット、電気コンロ、アイロン、置時計などがある。

家電製品は、家庭用電化製品の略語である。主に家庭で使用するために作られた電化製品を指す。小型家電製品、大型家電製品などのように区別されることもある。家電製品の例として、冷蔵庫、食器洗い乾燥機、換気扇、オーブントースター、電子レンジ、扇風機、エアコン、電気カミソリ、ヘアドライヤー、携帯電話（スマートフォン）やパソコンなどがある。

電気製品に電化製品が含まれ、さらにその中に家電製品が含まれると説明することもできる。

家庭用電気機械器具は、家庭用の電気機械器具を指すための行政用語である。

昭和三十六年政令第三百四十一号・割賦販売法施行令・総務省行政管理局

昭和五十一年政令第二百九十五号・れ特定商取引に関する法律施行令・総務省行政管理局

白物家電とは、家庭内の家事の労力を減らしたり、あるいは生活に密着した家電製品の一般名称である。生活家電や家事家電ともいわれる。普及し始めた当初は娯楽家電（黒物家電）に対し筐体の色が白いものが多かったことからこの名前で呼ばれるようになった。

消費電力の大きさは W（ワット）で示され、1000W＝1kW である。1 時間使用した時の消費電力量は Wh（ワットアワー）とされ、電気代などの計算にはこちらが利用される。主な電気製品の消費電力は次のとおりである。

冷蔵庫（常時）	150-600W
トースター（加熱時）	1000W
電子レンジ	1300W
電磁調理器（卓上）	1200W
自動食器洗い機	1300W
炊飯器	300-700W
炊飯器（IH タイプ）	700-1300W
ホットプレート	1300W
洗濯機	500W
洗濯機（乾燥機能）	800-1000W
掃除機	1000W
扇風機（AC モーター）	50W
扇風機（DC モーター）	5W～20W
ドライヤー	800-1200W
アイロン	1200W
掃除機	1200W
コタツ	600W
電気カーペット	500-800W
ハロゲンヒーター	500-1000W
加湿器	300-500W
液晶テレビ（32 型）	150W
デスクトップ PC	150-300W
ノート PC	50-150W

アンペア数が高い家電は次のものがある。

常に電気を使っている家電のアンペア数（ベースの電力消費）

9.9A	電気ストーブ
6.6A	エアコン
5A	こたつ
2.5A	冷蔵庫（450L クラス）
2.1A	TV（42 型）
1A	照明
0.4A	LED 照明
0.3A	扇風機

一時的に使う家電のアンペア数（ピークの消費電力）

15A	電子レンジ
14A	オーブン/卓上 IH クッキングヒーター
13A	食器洗い洗浄機/炊飯器（5.5 合炊飯時）/ドラム式洗濯乾燥機（乾燥時）
12A	ドライヤー（強）
10A	電気ケトル/掃除機（強）
3A	洗濯機
2A	ドラム式洗濯乾燥機（洗濯時）

電子レンジやオーブン、食器洗い洗浄機などキッチン周りのものはアンペア数が高いものが多い。また、ドライヤーのアンペア数は意外と高いので、ほかの家電と時間帯をじょうずに分散して使う。

どのくらいの電気製品を知っているのか，確認してみよう。

ア) 1:全く知らない　2:少し知っている　3:よく知っている

イ) 1:使ったことがない　2:使ったことがある

	ア)	イ)	製品名
1			アイロン
2			インターホン
3			ウォーターオーブン
4			デジタルオーディオプレーヤー
5			テレビ
6			エア・コンディショナー （エアコン）
7			エアサーキュレーター
8			映像機器
9			AC アダプタ
10			オーブン
11			オーブントースター
12			オーブンレンジ
13			オイルヒーター（オイル密閉，非燃焼）
14			オーディオ → 音響機器，ミニコンポ，ラジカセ
15			温風器
16			カーオーディオ（車載機器の一種）
17			加湿器
18			換気扇
19			除湿機
20			給茶機
21			空気清浄機
22			給湯器
23			吸入器（家庭用の呼吸器用治療器）
24			蛍光灯
25			LED 照明
26			携帯電話　スマートフォン
27			ゲーム機
28			コードレス電話
29			コーヒーメーカー
30			氷かき機
31			コピー機

32			散髪器具
33			CD プレーヤー
34			除湿機
35			食器洗浄機
36			炊飯器
37			スピーカ
38			石油ファンヒーター
39			セラミックヒーター
40			洗濯機
41			扇風機
42			掃除機
43			体脂肪計
44			タイプライター
45			DVD プレーヤー
46			デジタルカメラ
47			デジタルオーディオプレーヤー
48			電気あんか
49			電気カーペット
50			電気ストーブ（赤熱式，遠赤外線）
51			電気ポット
52			電気毛布 電気掛敷毛 電気ひざかけ
53			電磁調理器
54			電子蚊取り 液体 マット
55			電子辞書
56			電子レンジ
57			電卓 - 電子卓上計算機
58			電動歯ブラシ
59			トースター
60			時計
61			ドライヤー
62			生ごみ処理機
63			白熱電球
64			パソコン
65			パネルヒーター
66			ハロゲンヒーター
67			パン焼き機
68			ビデオカメラ

69			複写機
70			布団乾燥機
71			プロジェクタ
72			ヘアドライヤー
73			ヘアーアイロン
74			ホームシアター
75			ホームベーカリー
76			ホットサンドメーカー
77			ホットプレート
78			ポンプ 風呂水ポンプ 水道ポンプ 揚水ポンプ
79			マッサージ椅子
80			ミキサー (調理器具)
81			ミニディスクプレイヤー/レコーダー (MD)
82			ミル（粉砕器）
83			餅つき器
84			ヨーグルトメーカー
85			ラジオ
86			ラジカセ - ラジオカセット
87			ランタン
88			冷水機
89			冷蔵庫
90			冷風機 スポットクーラー コンビニクーラー
91			冷風扇 水や氷を使用 打ち水

ア)

全く知らない　　少し知っている　　よく知っている

個　　個　　個

イ)

使ったことがない　　使ったことがある

個　　個

課　題

１．身のまわりの電気製品をひとつ選び、調べたことをレポートにまとめなさい。

家庭機器工学　レポートⅠ　　月　　日(　　曜日)

専攻　　番号　　氏名

1.題名

2.報告

(1)　はじめに

何について報告するのかを端的に書く

(2)

報告する内容の本文
タイトルは適切につける
内容が分かれていたら(2)-1,(2)-2…

(3)　まとめ

報告の内容を簡潔にまとめる

3.資料

参考にした資料，作成した資料があれば添付する

参考資料

著作物が自由に使える場合

著作権法では，一定の「例外的」な場合に著作権等を制限して，著作権者等に許諾を得ることなく利用できることを定めています（第 30 条～第 47 条の 8）。

これは，著作物等を利用するときは，いかなる場合であっても，著作物等を利用しようとするたびごとに，著作権者等の許諾を受け，必要であれば使用料を支払わなければならないとすると，文化的所産である著作物等の公正で円滑な利用が妨げられ，かえって文化の発展に寄与することを目的とする著作権制度の趣旨に反することにもなりかねないためです。

しかし，著作権者等の利益を不当に害さないように，また，著作物等の通常の利用が妨げられることのないよう，その条件は厳密に定められています。

また，著作権が制限される場合でも，著作者人格権は制限されないことに注意を要します（第 50 条）。

なお，これらの規定に基づき複製されたものを目的外に使うことは禁止されています（第 49 条）。また，利用に当たっては，原則として出所の明示をする必要があることに注意を要します（第 48 条）。

著作物が自由に使える場合

私的使用のための複製 （第 30 条）	家庭内で仕事以外の目的のために使用するために，著作物を複製することができる。同様の目的であれば，翻訳，編曲，変形，翻案もできる。 なお，デジタル方式の録音録画機器等を用いて著作物を複製する場合には，著作権者等に対し補償金の支払いが必要となる。 しかし，[1]公衆の使用に供することを目的として設置されている自動複製機器（注 1）を用いて複製するときや，[2]技術的保護手段（注 2）の回避により可能となった（又は，その結果に障害が生じないようになった）複製を，その事実を知りながら行うとき，[3]著作権等を侵害する自動公衆送信を受信して行うデジタル方式の録音又は録画を，その事実（＝著作権等を侵害する自動公衆送信であること）を知りながら行うときは，この例外規定は適用されない。 また，映画の盗撮の防止に関する法律により，映画館等で有料上映中の映画や無料試写会で上映中の映画の影像・音声を録画・録音することは，私的使用目的であっても，この例外規定は適用されない（注 3）。
図書館等における複製 （第 31 条）	[1]国立国会図書館と政令（施行令第 1 条の 3）で認められた図書館に限り，一定の条件（注 4）の下に，ア)利用者に提供するための複製，イ）保存のための複製，ウ）他の図書館のへの提供のための複製を行うことができる。 利用者に提供するために複製する場合には，翻訳して提供することもできる。 [2]国立国会図書館においては，所蔵資料の原本の滅失等を避けるため（＝納本後直ちに）電子化（複製）することができる。

引用 （第 32 条）	[1]公正な慣行に合致すること，引用の目的上，正当な範囲内で行われることを条件とし，自分の著作物に他人の著作物を引用して利用することができる。同様の目的であれば，翻訳もできる。（注 5）[2]国等が行政の PR のために発行した資料等は，説明の材料として新聞，雑誌等に転載することができる。ただし，転載を禁ずる旨の表示がされている場合はこの例外規定は適用されない。
教科用図書等への掲載 （第 33 条）	学校教育の目的上必要と認められる限度で教科書に掲載することができる。ただし，著作者への通知と著作権者への一定の補償金の支払いが必要となる。同様の目的であれば，翻訳，編曲，変形，翻案もできる。
教科用拡大図書等の作成のための複製等 （第 33 条の 2）	視覚障害等により既存の教科書が使用しにくい児童又は生徒の学習のために，教科書の文字や図形の拡大や，その他必要な方式により複製することができる。同様の目的であれば，変形，翻案もできる。 ただし，教科書の全部又は相当部分を複製して拡大教科書等を作成する場合には，教科書発行者への通知が，営利目的で頒布する場合には著作権者への一定の補償金の支払いが必要となる。
学校教育番組の放送等 （第 34 条）	学校教育の目的上必要と認められる限度で学校教育番組において著作物を放送等することができる。また，学校教育番組用の教材に著作物を掲載することができる。ただし，いずれの場合にも著作者への通知と著作権者への補償金の支払いが必要となる。同様の目的であれば，翻訳，編曲，変形，翻案もできる。
教育機関における複製等 （第 35 条）	教育を担任する者やその授業を受ける者（学習者）は，授業の過程で使用するために著作物を複製することができる。また，「主会場」での授業が「副会場」に同時中継されている場合に，主会場で用いられている教材を，副会場で授業を受ける者に対し公衆送信することができる。複製が認められる範囲であれば，翻訳，編曲，変形，翻案もできる。 ただし，ドリル，ワークブックの複製や，授業の目的を超えた放送番組のライブラリー化など，著作権者に不当に経済的不利益を与えるおそれがある場合にはこの例外規定は適用されない。
試験問題としての複製等 （第 36 条）	入学試験や採用試験などの問題として著作物を複製すること，インターネット等を利用して試験を行う際には公衆送信することができる。 ただし，著作権者に不当に経済的不利益を与えるおそれがある場合にはこの例外規定は適用されない。 営利目的の模擬試験などのための複製，公衆送信の場合には，著作権者への

	補償金の支払いが必要となる。 　同様の目的であれば，翻訳もできる。
視覚障害者等のための複製等 （第 37 条）	[1]点字によって複製, あるいは, 点字データとしてコンピュータへ蓄積しコンピュータ・ネットワークを通じて送信することができる。同様の目的であれば，翻訳もできる。 　[2]政令（施行令第 2 条）で定められた視覚障害者等の福祉に関する事業を行う者に限り，視覚障害者等が必要な方式での複製，その複製物の貸出，譲渡，自動公衆送信を行うことが出来る。同様の目的であれば，翻訳，変形，翻案もできる。 　ただし，著作権者又はその許諾を受けた者が，その障害者が必要とする方式で著作物を広く提供している場合にはこの例外規定は適用されない。
聴覚障害者のための自動公衆送信 （第 37 条の 2）	政令（施行令第 2 条の 2）で定められた聴覚障害者等の福祉に関する事業を行う者に限り，[1]著作物に係る音声を字幕等の聴覚障害者等が利用するために必要な方式によって複製, 自動公衆送信を行うこと, [2]聴覚障害者等への貸出の目的で，字幕等付きの映画の作成を行うことができる。 　同様の目的であれば，翻訳，翻案もできる。 　ただし，著作権者又はその許諾を受けた者が，その障害者が必要とする方式で著作物を広く提供している場合にはこの例外規定は適用されない。
営利を目的としない上演等 （第 38 条）	[1]営利を目的とせず, 観客から料金をとらない場合は, 公表された著作物を上演・演奏・上映・口述することができる。ただし，出演者などに報酬を支払う場合はこの例外規定は適用されない。 　[2]営利を目的とせず，貸与を受ける者から料金をとらない場合は，CD など公表された著作物の複製物を貸与することができる。ただし，ビデオなど映画の著作物の貸与については，その主体が政令（施行令第 2 条の 3）で定められた視聴覚ライブラリー等及び政令（施行令第 2 条の 2 第 1 項第 2 号）で定められた聴覚障害者等の福祉に関する事業を行う者（非営利目的のもの限る）に限られ，さらに，著作権者への補償金の支払いが必要となる。
時事問題に関する論説の転載等 （第 39 条）	新聞，雑誌に掲載された時事問題に関する論説は，利用を禁ずる旨の表示がない限り，他の新聞，雑誌に掲載したり，放送したりすることができる。同様の目的であれば，翻訳もできる。
政治上の演説等の利用 （第 40 条）	[1]公開の場で行われた政治上の演説や陳述, 裁判での公開の陳述は, ある一人の著作者のものを編集して利用する場合を除き，方法を問わず利用できる。

	[2]議会における演説等は，報道のために新聞等への掲載，放送等により利用することができる。同様の目的であれば，翻訳もできる。
時事の事件の報道のための利用（第 41 条）	著作物に関する時事の事件を報道するために，その著作物を利用する場合，又は事件の過程において著作物が見られ，若しくは聞かれる場合にはその著作物を利用できる。同様の目的であれば，翻訳もできる。
裁判手続等における複製（第 42 条）	[1]裁判手続のためや，立法，行政上の内部資料として必要な場合，[2]特許，意匠，商標，実用新案及び国際出願の審査等に必要な場合，[3]薬事に関する審査，調査等に必要な場合には，著作物を複製することができる。同様の目的であれば，翻訳もできる。 ただし，著作権者に経済的不利益を与えるおそれがある場合にはこの制限規程は適用されない。
情報公開法等における開示のための利用（第 42 条の 2）	情報公開法等の規定により著作物を公衆に提供又は提示する必要がある場合には，情報公開法等で定める方法により，著作物を必要な限度で利用することができる。
国立国会図書館法によるインターネット資料収集のための複製（第 42 条の 3）	国立国会図書館の館長は，国，地方公共団体，独立行政法人等により公衆に利用可能とされたインターネット資料を収集するために必要な限度において，当該インターネット資料に係る著作物を記録媒体に記録することができる。 また，国，地方公共団体，独立行政法人等は，国立国会図書館の求めに応じインターネット資料を提供するために必要な限度において，当該インターネット資料に係る著作物を複製することができる。
放送事業者等による一時的固定（第 44 条）	放送事業者又は有線放送事業者は，放送のための技術的手段として，著作物を一時的に録音・録画することができる。 なお，録音・録画したものは政令（施行令第 3 条）で定める公的な記録保存所で保存を行う場合を除き，6 ヵ月を超えて保存できない。
美術の著作物等の原作品の所有者による展示（第 45 条）	美術の著作物又は写真の著作物の原作品の所有者等は，その作品を公に展示することができる。 ただし，屋外に恒常的に設置する場合にはこの制限規定は適用されない。

公開の美術の著作物等の利用（第46条）	屋外に設置された美術の著作物又は建築の著作物は，方法を問わず利用できる（若干の例外あり（注6））。
美術の著作物等の展示に伴う複製（第47条）	美術の著作物の原作品又は写真の著作物の原作品を公に展示する者は，観覧者のための解説，紹介用の小冊子などに，展示する著作物を掲載することができる。
美術の著作物等の譲渡等の申出に伴う複製等（第47条の2）	美術又は写真の著作物は，それらの譲渡等の申出のために行う商品紹介用画像の掲載（複製及び自動公衆送信）を，政令（施行令第7条の2）で定める著作権者の利益を不当に害しないための措置（画像を一定以下の大きさ・画素にすることなど）を講じている場合に限って行うことができる。
プログラムの著作物の複製物の所有者による複製等（第47条の3）	プログラムの所有者は，自ら電子計算機で利用するために必要と認められる限度でプログラムを複製，翻案することができる。 ただし，プログラムの所有権を失った場合には作成した複製物は保存できない。
保守，修理等のための一時的複製（第47条の4）	記録媒体が内蔵されている複製機器を保守又は修理する場合，その製造上の欠陥などにより複製機器を交換する場合には内蔵メモリに複製されている著作物を一時的に別の媒体に複製し，修理後等に機器の内臓メモリに改めて複製し直すことができる。 修理等のあとには一時的に別の媒体に複製した著作物は廃棄すること。
送信の障害の防止等のための複製（第47条の5）	インターネットサービスプロバイダ等のサーバ管理を業とする者は，[1]アクセス集中による送信の遅滞等の防止（ミラーリング），[2]サーバへの障害発生時における復旧（バックアップ），[3]著作物の送信の中継の効率化（キャッシング）のために必要と認められる限度で，著作物を複製することができる。
送信可能化された情報の送信元識別符号の検索等のための複製等（第47条の6）	インターネット情報の検索サービスを業として行う者（一定の方法で情報検索サービス事業者による収集を禁止する措置がとられた情報の収集を行わないことなど，政令（施行令第7条の5）で定める基準を満たす者に限る。）は，違法に送信可能化されていた著作物であることを知ったときはそれを用いないこと等の条件の下で，サービスを提供するために必要と認められる限度で，著作物の複製・翻案・自動公衆送信を行うことができる。

情報解析のための複製等（第 47 条の 7）	コンピュータ等を用いて情報解析（※）を行うことを目的とする場合には，必要と認められる限度において記録媒体に著作物を複製・翻案することができる。 ただし，情報解析用に広く提供されているデータベースの著作物については，この制限規定は適用されない。 ※情報解析とは，大量の情報から言語，音，映像等を抽出し，比較，分類等の統計的な解析を行うことをいう。
電子計算機における著作物の利用に伴う複製（第 47 条の 8）	コンピュータ等において著作物を適法に利用する場合には，当該コンピュータ等による情報処理の過程で行われる著作物の複製を行うことができる。

（注 1）自動複製機器

文化庁
http://www.bunka.go.jp/seisaku/chosakuken/seidokaisetsu/gaiyo/chosakubutsu_jiyu.html

第２講　LED 照明

【学修到達目標】

- LED 照明のメリットを説明できる。
- 使用条件に合った種類の LED 照明を選択することができる。

１．LED 照明

LED と言う言葉は Light Emitting Diode の略で，発光ダイオードと呼ばれる。発光ダイオードは，電気を流すと発光する性質を持っている半導体のことで，この発光ダイオードを光源として利用して LED 照明が作られている。この発光ダイオードを利用した LED 照明には，LED 電球や LED シーリングライトなどを中心に，様々なタイプの照明器具が発売されている。

LED 電球

LED 蛍光灯

LED シーリングライト

LED ベースライト

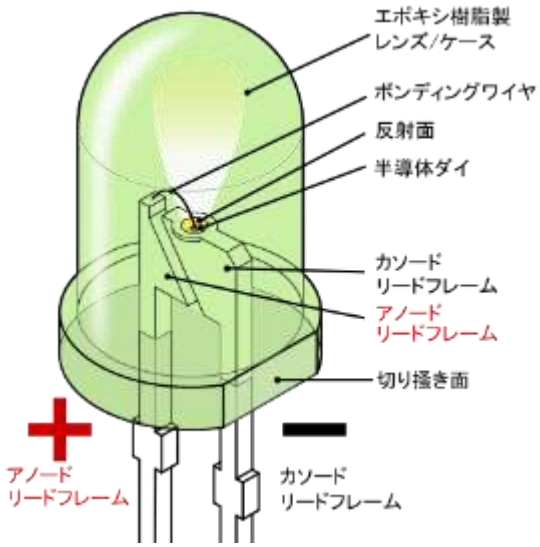
LED 照明の表示

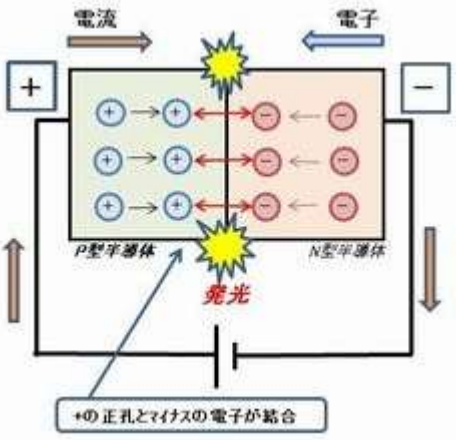
LED

a) Light Emitting Diode(発光ダイオード)といわれる電子部品(半導体素子)で，電気エネルギーを光エネルギーに変換して発光する。

b) 消費電力が少なく長寿命という性能の高さに加え，白熱電球や蛍光灯に比べると高価だった価格も低下している。近年は LED 電球・LED 蛍光灯を採用した照明器具が多くを占める。

c) ダイオードは，一組の PN 接合を持つ半導体素子で構成される。この素子に，p 型半導体のアノード電極にプラス（+），n 型半導体のカソード電極にマイナス（−）になるように外部から電圧をかけると，p 型半導体のホール（正孔）が左から右に向かって流れ，n 型半導体の電子が右から左に向かって流れる。p と n が接合する部分で−の電子が+の穴に再結合し，この時に余ったエネルギーが光として放出される(自然光放出発光)





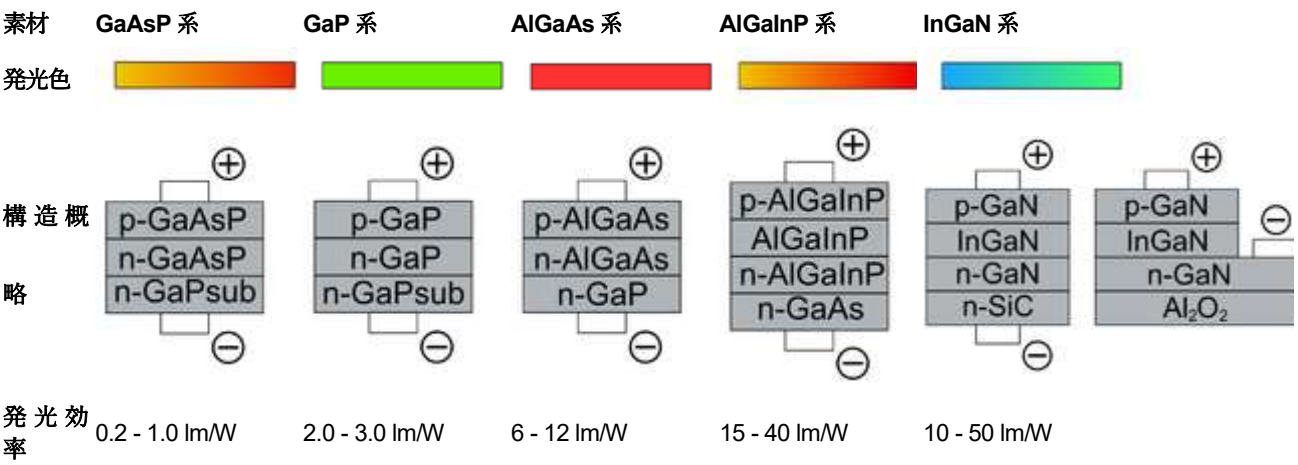
発色

LED チップに使われる材料(化合物)は RGB で異なる。使用される材料の化合物で放出する電磁波(光)が変わり，人の目に色として識別(可視光線…電磁波のうち，人の目に色として見える波長)される。

LED のカラーと波長，材料

色	波長(nm ナノメートル)	材料
赤	700～635	GaP GaAsP GaAlAs InGaAlP
橙	620～590	GaAsP InGaAlP
黄	590～570	GaP GaAsP InGaAlP
緑	570～495	GaP InGaAlP
青	495～450	GaN

色



光の波長と色

人の目に入って，直接に視感覚を起こすことのできる放射のことを可視放射（visible radiation)という。それより波長が短い放射は紫外放射(ultraviolet radiation)， 波長が長い放射を 赤外放射(infrared radiation)という。可視放射でも，どの波長域の光が強いかによって色が変わる。

種類	名称(色)	波長域
紫外放射	UV-C	100nm～280nm
	UV-B	280nm～315nm
	UV-A	315nm～400nm
可視放射	紫	400nm～435nm
	青	435nm～480nm
	緑青	480nm～490nm
	青緑	490nm～500nm
	緑	500nm～560nm
	黄緑	560nm～580nm
	黄 黄	580nm～595nm
	橙 橙	595nm～610nm
	赤	610nm～750nm
	赤紫	750nm～800nm
赤外放射	IR-A	800nm～1,400nm
	IR-B	1.4 μm～3 μm
	IR-C	3 μm～1mm

2. LED 照明の種類

LED 電球・LED 蛍光灯

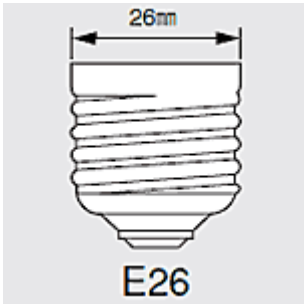
長寿命　⇒　従来型の照明器具と比較するとかなりの長寿命の 20000～40000 時間。一度設置すれば，頻繁に交換をする必要はない。

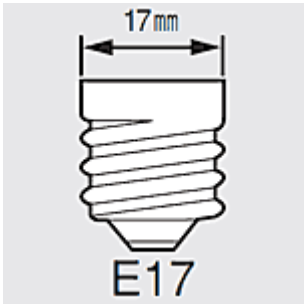
省エネ　⇒　電気の多くが発光に使われるので発光効率が高く，白熱電球と比べると同じ明るさを得るために必要な電気は少ない。熱となって失われる電気も少ないので発熱も少ない。

紫外線・赤外線が混ざらない　⇒　LED の発光成分には，目に見えない赤外線や紫外線がほとんど含まれない。赤外線がないので放射熱による悪影響がない。紫外線がないので紫外線を好む虫が寄り付きにくく，紫外線による展示物等の劣化を防ぐことができる。

タイプ　⇒　LED には電球タイプと蛍光灯タイプがある。LED 蛍光灯には長細い直管タイプとサークル状の丸形タイプがある。

口金　⇒　口金とは電球のソケットに差し込む金具の部分のことで，蛍光灯などの接続部分も口金という。数種類の大きさがありますが，LED 電球では，従来の一般電球やボール電球で採用されている E26 (26mm 口径)と，ミニクリプトン電球などで採用されている E17(17mm 口径)が一般的。直管蛍光灯では，従来の直管蛍光灯と同じ G13 が主流。



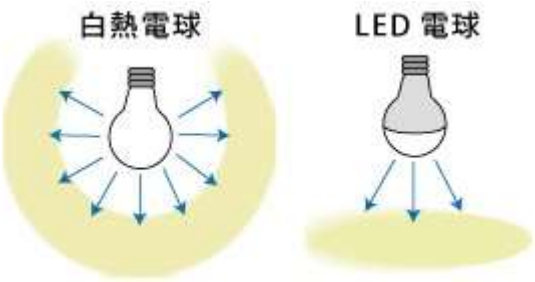


定格寿命　⇒　LED の電極部分の金属などの部品の劣化により当初の全光束(放出される全ての光の量)が減少する。LED を使った照明器具では，全光束または光度が初期の 70%となる時間を定格寿命と定めており，40000 時間のものが一般的。ただし，この数値は平均値なので，すべての商品で 40000 時間の使用を保証するものではない。

光色　⇒　LED 電球・LED 蛍光灯には数種類の色合いが用意されている。白熱電球の色合いに近い「電球色相当」，昼間のような白い色合いの「昼白色相当」，「昼光色相当」，「白色相当」がある。

全光束　⇒　全光束とは，光源から 360 度すべての方向に放出する光の量のことをいい，照明器具の明るさを表す。ルーメン(lm)という単位を使用し，数値が大きいほど明るい。

配光角　⇒　光がどの方向にどれだけ出ているかという光の広がり方を配光といい，広がり具合を角度で表わす。配光角が 300 度あれば，従来の電球のように全方向に光が広がり，120 度であれば光は下方向に集まる。



発光効率　⇒　一定のエネルギー(1W あたり)でどれだけ明るくできるかを示す指標(lm/W)。数値が大きいほど，効率よく電気を光に変換していることになる。

密閉型器具対応　⇒　密閉型器具とは，カバー(セード)などで覆われた外側から中が見えないタイプの照明器具のこと。LED 電球・LED 蛍光灯も，密閉型器具に対応した製品を選ぶ必要がある。バスルームの照明など，照明器具をカバーで覆っている密閉型器具を選ぶ。白熱電球に比べると LED 電球はあまり発熱しないが，発光する LED 素子は，電流を流すと光ると同時に発熱する。この熱を放置してしまうと，LED 素子が高熱になり，光が弱くなる，寿命が縮む，壊れるといったトラブルを招く。密閉型器具は，普通の照明よりも熱がこもりやすい。そこで各メーカーは放熱の方法に工夫を凝らして LED が過熱しないようにして，密閉型器具に対応させた製品を販売している。

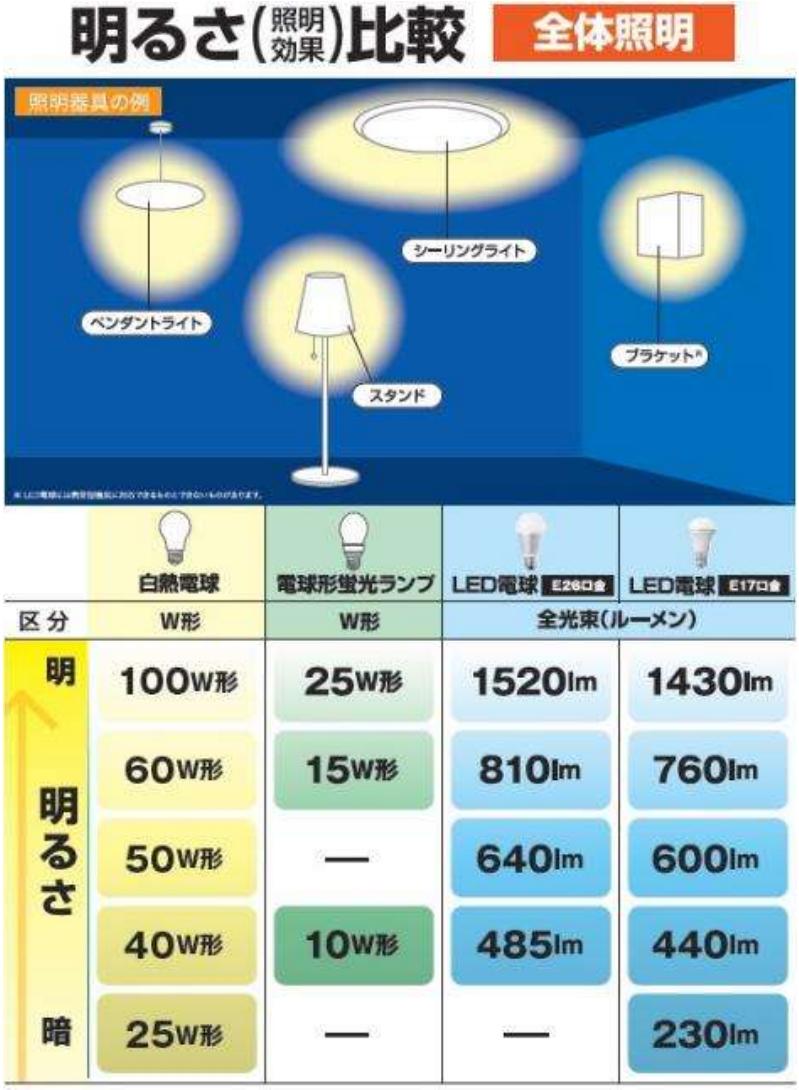
調光器対応　⇒　照明器具には，無段階や 100%・70%・50%というように段階的に明るさを変化させられる調光機能が付いたものがある。こうした器具に LED 電球・LED 蛍光灯を使用する場合は，“調光器対応”と書かれたものを選ぶ必要がある。

LED の明るさ

白熱電球では，照明器具を選ぶときの明るさの目安は W(ワット)。40W より 60W のほうが明るい。W は「消費電力」のこと。

LED は消費電力が少ないので，W 数で LED 照明器具を選ぼうとすると，数 W から十数 W という小さな数字で表記されてしまう。そこで，ルーメン（lm）で選ぶことになる。一般電球の 60W 形は 810 ルーメン（lm）と同じ明るさ。

消費電力　⇒　どれだけの電力を消費するかを示した数値。省エネ性能をチェックする場合は，消費電力だけでなく，発光効率や明るさも合わせてチェックする。



電球と明るさの関係

一般白熱電球（E26)との関係		**小形電球（E17）との関係**	
一般白熱電球 ワット(W)相当	ルーメン（lm）値	小形電球 ワット(W)相当	ルーメン（lm）値
20W 相当	170 ルーメン以上	25W 相当	230 ルーメン以上
40W 相当	485 ルーメン以上	40W 相当	440 ルーメン以上
60W 相当	810 ルーメン以上	50W 相当	600 ルーメン以上
80W 相当	1160 ルーメン以上	60W 相当	760 ルーメン以上
100W 相当	1520 ルーメン以上	75W 相当	1000 ルーメン以上

明るさと広さの関係

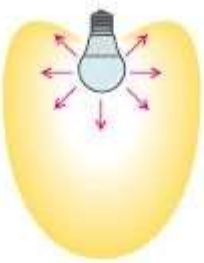
	2,000ルーメン	3,000ルーメン	4,000ルーメン	5,000ルーメン	6,000ルーメン
～4.5畳	2,200～3,200				
～6畳		2,700～3,700			
～8畳			3,300～4,300		
～10畳			3,900～4,900		
～12畳				4,500～5,500	
～14畳					5,100～6,100

LED 照明器具を選ぶ際には，まず取り付ける場所に必要な，あるいは欲しい光量のルーメン（lm）を確認して購入候補の器具を選んだうえで，各器具のルーメン パー ワット（lm/W）と消費電力を確認

光の広がり方

LED 照明器具やランプの中には，全方向が明るいタイプと下方向が明るいタイプがある。下方向が明るいタイプでは，照明の直下は明るく感じられても，部屋全体では以前より暗く感じる。

「光が広がるタイプ」あるいは「全方向」「広配光」「下方向」などと表記してある製品も多い。

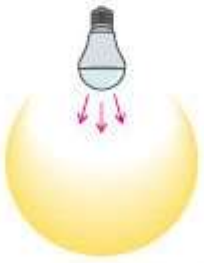


全方向が明るいタイプの光の広がり方

ダウンライト

ペンダント

フロア
スタンド



下方向が明るいタイプの光の広がり方

ダウンライト

スポットライト

LED 電球には一般的に「電球色」「昼白色」「昼光色」の大きく 3 種類の色が存在する。

電球色は,暖色系でオレンジっぽく温かみのある光の色で,比較的明るさを抑えた落ち着きのある色で,目も疲れにくくリラックスしたい場所に適している。

昼白色は，太陽の明るさに最も近い自然な光の色で，部屋はいきいきとした雰囲気になり，自然な明るさなのでどんな部屋にも適する。

昼光色は，白っぽく青みがった最も明るい色で，青みがかった光の色は脳を覚醒させる効果があるそうで，集中力を高めるのに最適と言われている。

組み合わせる器具も要確認する必要がある。安全に使用するためにまずは取り付け予定の器具や LED のパッケージや仕様書をよく確認する。下記 3 点の器具には，必ず「対応」と表記がある LED を選ぶ必要がある。

密閉形器具

お風呂などで使われていることが多い全体をカバーで覆っている密閉形器具には，必ず「密閉形器具対応」と表記のある LED を選ぶ。密閉形器具は電球の発熱により熱がこもってしまうことが原因で光が弱くなってしまったり寿命が縮まる，壊れるなどのトラブルに繋がる恐れがある。

調光機能付き照明器具

光を強くしたり弱くしたりと明るさを調節できる調光機能付き照明器具には，必ず「調光器対応」と表記のある LED を選ぶ。表記がない限り，LED 電球のほとんどは調光器対応ではないので注意が必要である。非対応の LED を取り付けると故障の原因になったり，最悪発煙の可能性がある。調光器対応の LED を調光機能がついていない器具に取り付ける場合も寿命が縮まったり故障することがある。

断熱材施工器具

天井にはめ込むような形で吊るされているダウンライトは，天井を覆っている断熱材により器具に熱がこもることがある。そのような断熱材施工器具には，必ず「断熱材施工器具対応」と表記のある

LED を選ぶ。断熱施工器具かどうかを見分けるために，器具に S マーク(SB，SGI，SG)という目印が表記されている。

課　題

１．使用条件に合った LED 照明の選び方について説明しなさい。

第３講　ディスプレイ

【学修到達目標】

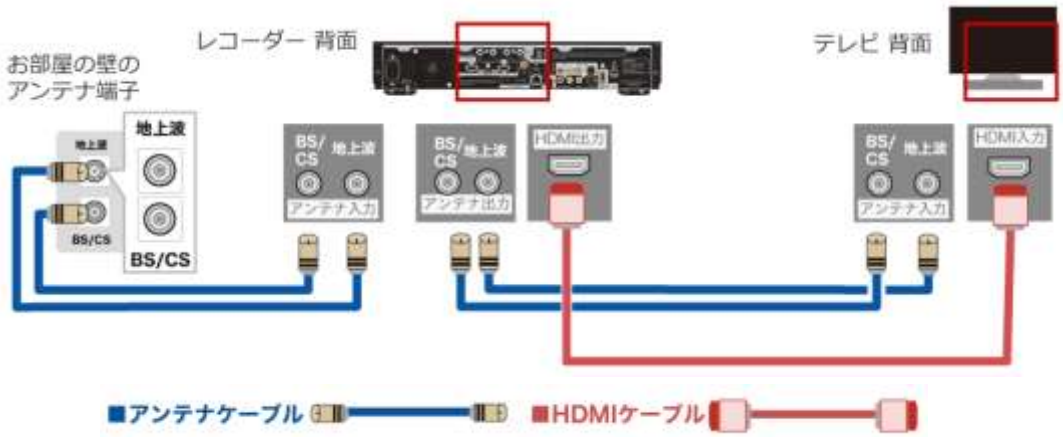
- ディスプレイの種類を説明できる。
- ディスプレイの仕組みを理解できる。

１．ディスプレイ

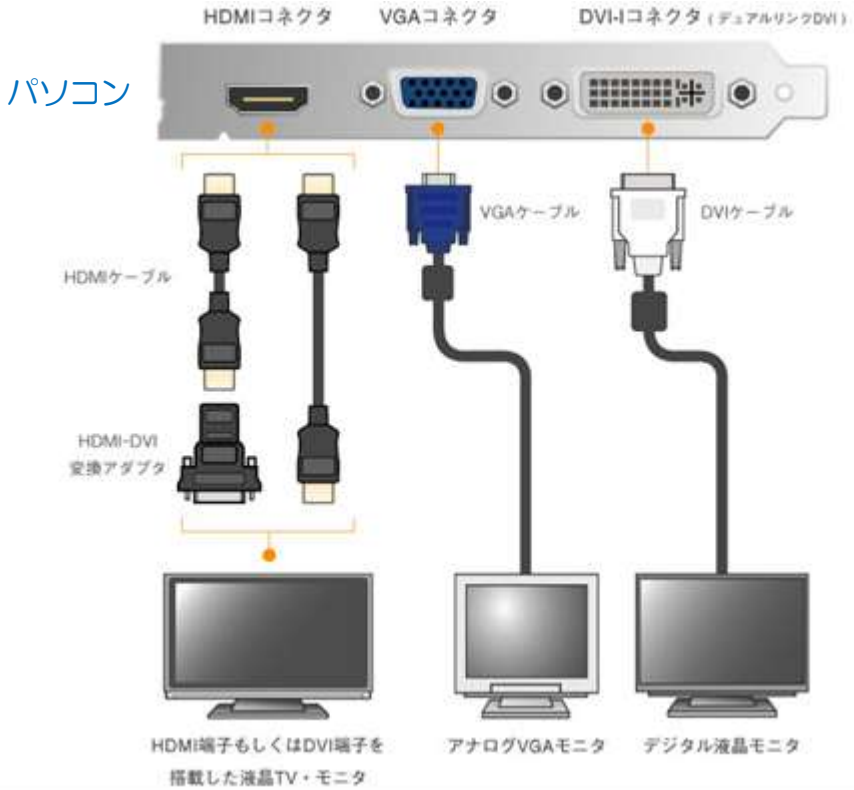
ディスプレイ（display）は，文字，図形，画像，映像（動画）などを表示する装置のことで，パソコンに接続してモニターとして利用したり,チューナーと組み合わされてテレビとして利用されたりしている。テレビの視聴に使われている液晶テレビと，パソコンで使われる液晶モニターは，一見すると同じように見える。同じ画面の大きさで比べると，液晶モニターの方が安いモデルが多いので，テレビも見られる液晶モニターを使えば，安く済む。しかし，液晶テレビはテレビを見るために特化した機能性能を持ち，一方の液晶モニターは，パソコンから出力される映像データを見るために特化した機能性能を持っている。テレビ視聴用の液晶テレビとパソコン用液晶モニターは，使い分けるのが望ましい。しかし，最近は１台２役をこなすモデルが続々登場しており，液晶テレビと液晶モニターの間の垣根は徐々になくなりつつある。

テレビを視聴するためには，TV チューナーが必要で，液晶テレビには必ず組み込まれている。一般的に液晶モニターには，TV チューナーがない。ただし，テレビも視聴できるように，TV チューナーが付いた液晶モニターもある。

液晶テレビは，HDD レコーダーなど接続して利用することが多く，液晶テレビと組み合わせて使う機器と接続するための端子が付いている。テレビとレコーダーを接続して使う場合，地上波と BS/110 度 CS を受信する場合に必要な部材は，アンテナケーブル４本と HDMI ケーブル１本が必要である。



パソコンに接続されたディスプレイはモニターとも呼ばれ。液晶モニターは，パソコンと接続するための端子が付いている。HDMI 端子で接続するモニターや最近は少なくなってきたが，VGA 端子で接続するもの，DVI モニターで接続するものもある。



最近，主にパソコンで使うために使うディスプレイ（モニター）において「USB Type-C（USB-C）端子」を備えるモデルが増加傾向にある。USB 端子のあるディスプレイ自体は以前から存在しているが，USB Type-C 端子付きのディスプレイには従来の「USB 端子付きディスプレイ」にはないメリットがある。USB Type-C ディスプレイは「DisplayPort Alternate Mode」に対応する USB Type-C 端子を備えている。DisplayPort Alternate Mode は，DisplayPort という規格の映像信号を USB Type-C 端子の Alternate Mode で伝送する仕組みである。映像信号の規格には，テレビでも使われている HDMI もあるが，DisplayPort には，高解像度や高リフレッシュレートのディスプレイに対応しやすい，ディスプレイのデイジーチェーン接続（数珠つなぎ）に対応している，別の映像信号規格に変換しやすいといったメリットがある。据え置きタイプの USB Type-C ディスプレイの多くは，接続したデバイスへの電源供給にも対応しており，ディスプレイが AC アダプター（充電器）代わりになる。

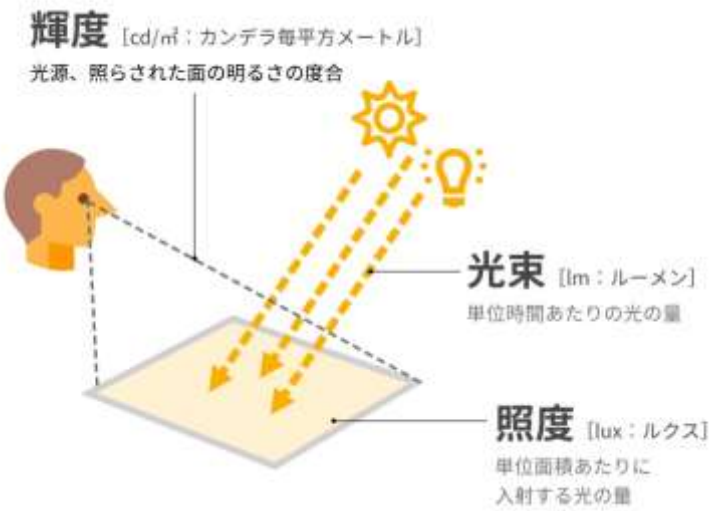
液晶テレビは，テレビを視聴するために作られているので，動く映像をきれいに表示できるように，輝度やコントラスト比，応答速度などのスペックに優れている。また，視野角も広く，液晶テレビを斜めから見ても，しっかりと映像を見られるようになっている。一方液晶モニターでは，一般的に動く映像を見る機会は少ないため，映像をきれいに表示するためのスペックはあまり優れていない。

2. 輝度，コントラスト比，応答時間，視野角，表示色

ディスプレイの基本スペックとして輝度，コントラスト比，応答時間，視野角，表示色がある。

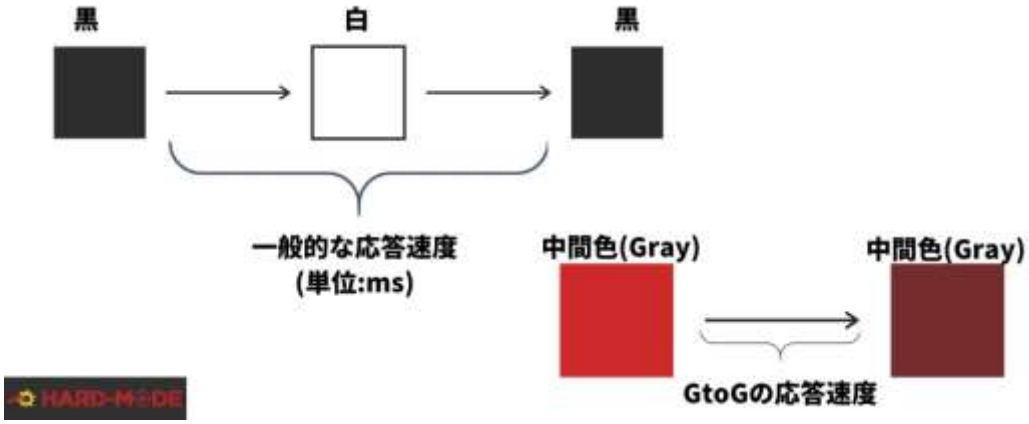
輝度とは，液晶テレビの場合は，バックライトの明るさである。液晶パネル自体は発光しない。パネル

の背面にはバックライトという光源があり，液晶パネルはこれに照らされて画面を表示する。バックライトの明るさが輝度で，スペックでは最大輝度が表記される。単位は cd（カンデラ）で，1 平方メートルあたりに照射される光量を基準とするので cd/m^2（カンデラ／平方メートル）と表記される。明るい場所で使うなら，それだけ輝度が高いほうが良い。一般的な目安としては，250～300cd/m^2 である。屋外使用では 300cd/m^2 の光が最低限必要とされる。テラスなどでパソコンを使うなら 400～500cd/m^2 がベストで，蛍光灯で明かりをとっている部屋なら 250～300cd/m^2 で充分である。



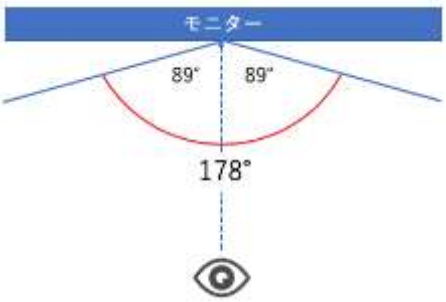
コントラスト比は，白と黒の比率である。「500：1」表記されていれば，「500 の白に対して，1 の黒」という意味である。比率が高いほどメリハリがあり，比率が低いと白い部分がグレイっぽくなる。500：1～1000：1 が目安である。通常のコントラスト比に対して，極端に高いコントラスト比の表示がされている場合がある。それはダイナミックコントラスト比という「擬似コントラスト比」である。ダイナミックコントラスト比は，液晶モニターそのものが持つコントラスト比ではなく，映し出されている映像の明るさに応じて輝度を変化させる機能で，擬似的にコントラスト比を上げている。

応答速度とは「映像信号がモニターに届いてから，モニター上で色が変化するために必要な時間」のことである。単位は ms（ミリセカンド）で表示され，1ms は 0.001 秒である。応答速度が遅いと，既に映像は進行しているのに切り替わる前の色がモニターににじんで「残像」が残る。応答速度が速ければモニター上のボヤッとした残像感が減ってより映像もしくはゲームに集中できるようになる。一般的に「黒から白」もしくは「白から黒」に変化する速度を「応答速度」と呼ぶ。応答速度には二種類ある。「G to G」または，「グレイ to グレイ」と表記されている場合がある。実際に応答速度で重要なのは中間色の切り替わりスピードなので，この表記の製品は高性能と考えることができる。



視野角は，画面を真正面から見たときを 0°として，そこから上下左右に動いても正常に見える範囲を角度で示す。たとえば，画面が真正面から右に 85°，左に 85°動いても正常に見えるとき，その視野角は「水平 170°」（85°+85°）と表記される。もしくは「左右 170°」と表記される場合もある。この角度が広ければ広いほど，さまざまな方向からモニターを見ることができる。

視野角の測定で「正常に見える」基準は，一般的にコントラスト比（白と黒を表示した場合の輝度の差）10：1 とされる。「適切の基準」というのは，コントラスト比が「10：1」までキープできる角度ということが多い。



最大表示色は，画面上で表示できる色の数である。「フルカラー」というのが 1677 万色で，1620 万色だと「疑似フルカラー」になる。液晶モニタの表示色は光の三原色（RGB=赤・緑・青）で構成されており，フルカラーは 8 ビット，疑似フルカラーは 6 ビットという階調の違いがある。エントリータイプは「疑似フルカラー」の場合がある。

RGB各色8ビットで約1677万色のフルカラーを再現可能

- 8ビット（2の8乗）＝256階調（色）
- 256階調（R）×256階調（G）×256階調（B）＝1677万7216色
- 1677万7216色≒約1677万色

専門的に写真や CG を扱うなら，色再現性をチェックする。「○%の NTSC 色域」とあれば，テレビ放送で用いられる色の範囲「NTSC」を基準に何パーセントの色域かを示している。「Adobe～」「sRGB」といった表記は，色空間を定義された規格にサポートしているということである。

3．ディスプレイの種類

フルハイビジョンを超える高解像度化がすすみ，4K 解像度のモニターが数多く登場している。目の疲れの原因になるとされるブルーライトや画面のちらつきを低減する機能を持つモニターも増えている。スマホの画像をモニターで表示するなどスマホとの連携も進んでいる。4K は，1,920×1,080 ドットのフルハイビジョンに対して，3,840×2,160 ドットと 4 倍の画素数となる。横の画素数が約 4,000 なので 4K（1K＝1,000）といわれており，5,120×2,880 の場合は 5K となる。目的に合った画面サイズを選ぶことが大切で，サイズが大きいと作業スペースが広く見やすくなるが，より広い設置場所を確保する必要がある。画面の形によってワイド型とスクエア型があり，同じ 19 インチ型でもワイドとスクエアでは縦と横の長さが違う。スクエア型は，画面の横と縦の比率が 5 対 4 のモニターで，縦方向への広さがあり，横幅を取らないので，デスクのスペースを有効に活用でき，Web ブラウザや文書作成ソフトが見やすいという特長がある。ワイド型は，画面の横と縦の比率が 16 対 9 もしくは 16 対 10 のワイドタイプが主流で，

作業領域を広く取れるので，複数の画面を同時に表示しても重なりにくいといった特長がある。ワイドモニターよりもさらに横幅が広いタイプです。横幅が縦幅の２倍以上になっているのがウルトラワイド型で，より広いワークスペースを確保でき，縦横の比率が 21 対 9 になっているモデルが主流である。

ディスプレイには様々な仕様があり，目的に合った仕様のディスプレイを選ぶ。

ディスプレイには，グレア（光沢）とノングレア（非光沢）がある。グレア（光沢）は，色が鮮やかでコントラストが高く，黒が引き締まって見えるので，静止画や映像がきれいに感じられる。一方で，表面がツヤツヤなため外部からの映り込みがあり，ノングレアと比べると目が疲れやすい。ノングレア（非光沢）は，外部からの映り込みを少なくするため，特殊な表面加工を施してある。発色が地味でコントラストが低く感じる場合もあるが，映り込みが少なく目への負担が軽い，表面がキズつきにくいという特長がある。

アスペクト比は，画面の縦と横の長さの比率で，「横：縦」で表記される。アスペクト比として次のものがある。

- 4：3
- 5：4
- 16：9
- 17：9
- 16：10
- 21：9
- 32：9

表示色は，画面上で表示できる色の数で，表示色が多くなるほど，階調表現がなめらかになる。表示色数には，次のものがある。

- ～1620 万色未満
- 1620～1677 万色未満
- 1677～10 億 6000 万色未満
- 10 億 6000 万色～

解像度は，画面に表示される点の数を表し，数字が大きいほど細部まで表現できるため，画像や映像を滑らかでキレイに表示でき，表示できる範囲が大きくなる。

応答速度は，画面の色を黒から白（白から黒）へ変える時間のことで，ms（1ms は 0.001 秒）で表し，数字が小さいほど残像が少なくなる。

コントラストは，画面内で最も明るい白と最も暗い黒の明るさの比で，画像のメリハリの強さを表す。

輝度は，画面から発することのできる明るさのことで，cd/m^2 で表す。数字が大きいほうが画面をより明るくすることができる。

ドットピッチは，画面を構成するドット（画素）の大きさで，数値が小さくなるほど密度が高くなり高精細な画像となる。

LED バックライトは，PC モニターを背面から照らすライトで，光源に LED を採用したものを LED バックライトという。ほかの光源と異なり，省電力で薄型・軽量，コントラスト比が高くなるといった特長がある。

3D 対応は，立体映像（3D 映像）に対応しているモニターで，ディスプレイやメガネなどの専用機材が必要なタイプと，昔ながらの赤青メガネを用いる手軽なタイプの 2 種類がある。

フリッカーフリーは，従来は LED バックライトを高速で点滅させることで，眼精疲労の原因になるといわれるフリッカー（ちらつき）が生じていたが，このフリッカーをなくした，目が疲れにくいモニターである。

パネルの種類は，4 つのタイプに分けられ，液晶パネルは，TN，VA，IPS の 3 タイプがあり，今では低価格化が進む高性能の IPS タイプや VA タイプが主流となっており，有機 EL（OLED）パネルを採用した製品も増えている。それぞれの特徴を次に示す。

TN パネル

TN（Twisted Nematic）パネルは，パソコンモニターなどに用いられることが多く，歴史も古いパネル

TN パネルのメリット：　・価格（コスト）が安い　　・応答速度が速い

TN パネルのデメリット：・視野角が狭い　　・発色，色の表現に弱い

TN パネルの一番のメリットは応答速度が速い　　0.1～1ms 程度

そのため画面の遅延が少なく，マウスカーソルの遅延ラグなどを抑えられる

ゲームなど，コンマ 1 秒の操作が求められるゲームに強み

ただし視野角が狭く，発色もあまりよくないため，映像の明るさや鮮やかさの面では弱い

VA パネル

VA (Vertical Alignment)パネルは，安価なことから液晶テレビ市場において近年主流となっているパネル

VA パネルのメリット：・価格が安い（ただし TN パネルよりは高い）

・黒の表現に強い，コントラストに優れる　・液晶寿命が長め

VA パネルのデメリット：・視野角が狭い（ただし TN パネルよりは広い）

・発色，色の表現に弱い（ただし TN パネルよりは良い）

・応答速度が遅い

VA パネルの最大のメリットは，「黒」の表現に強い

コントラスト（明るい部分と暗い部分の差）をはっきりと付けることができ，黒の引き締まった高級感ある画質を楽しめ，映画やドキュメンタリー番組などと相性がよい

発色や色の表現では，後述する IPS パネルや有機 EL パネルに劣り，全体的に暗め

視野角も狭め

応答速度も遅い

IPS パネル

IPS(In-Plane Switching)パネルは液晶テレビのパネルとして広く普及したが，近年は VA パネルにシェアを奪われつつある

明るさや視野角に優れる

IPS パネルのメリット：・発色がよい，色の表現が豊か　・明るい　・視野角が広い

IPS パネルのデメリット：・コントラストでは VA パネルに劣る　・全体的に白っぽくみえることがある

・価格が高め

IPS パネルの最大のメリットは，発色がよく，鮮やかで明るい

おなじ映像でも TN パネルや VA パネルよりはっきりとキレイに映し出せ，白のような明るい色もクリアに表現

視野角も広く，上下左右からのぞき込んでも違和感なく見れる

ただし，コントラストの表現はV Aパネルより劣るため，全体的に白っぽい

（蛍光灯の部屋のようなイメージ）映像になりやすく，安っぽくみえることがあります。

有機 EL パネル

有機 EL（Electro Luminescence）パネルは，高性能テレビやスマホなどに用いられることが多い

有機 EL は発光ダイオードで構成されており，厳密には「液晶パネル」ではない

有機 EL パネルのメリット：・高画質，綺麗でハッキリとした映像　・視野角が広い

・軽い，薄い　・画面遅延が少ない

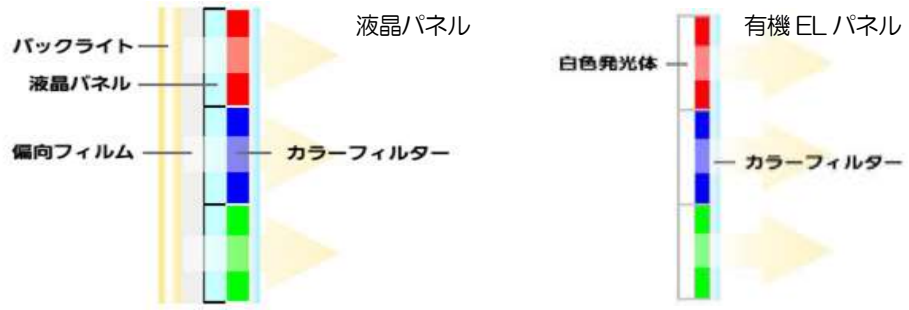
有機 EL パネルのデメリット：・コストが高い　　・消費電力が多い　　・寿命が短い

有機 EL パネルは，1 画素ごとに明るさを調整できるので，完全な黒を再現

液晶パネルに比べ，圧倒的な明るさ，鮮やか，コントラストを実現

ただしコストが高い

消費電力も液晶テレビの 2 倍以上



明るさの比較

明るい：有機ＥＬパネル> ＩＰＳパネル> ＶＡパネル> ＴＮパネル：暗い

コントラストの比較

コントラスト高：有機ＥＬパネル> ＶＡパネル> ＩＰＳパネル> ＴＮパネル：コントラスト低

視野角の比較

視野角広い：有機ＥＬパネル> IPS パネル> VA パネル> ＴＮパネル：視野角狭い

応答速度の比較

応答速度速い：有機ＥＬパネル※> TN パネル> IPS パネル> VA パネル：応答速度遅い

スピーカー

パソコン用スピーカーが用いられる事もあるせいか，液晶モニターに付いているスピーカーはあまり良いものではない。中にはスピーカー機能が無い液晶モニターもある。一方液晶テレビでは，スピーカーは付いており，ある程度音質も重視したスピーカーが内蔵されている事が多い。液晶テレビとしても液晶モニターとしても使えるモデルでは，最近は，液晶の性能が上がり，低価格化も進んだ事から，液晶テレビとしても液晶モニターとしても使えるモデルが珍しくなく，価格もそれほど高くない。安いものでもテレビ映像もパソコン画面もきれいに映るので，個人で使用するのであれば，一台で液晶テレビ＆液晶モニターとして使うのも問題ないといえる。ただし，リビングで家族と一緒にテレビを視聴するといった使用用途であれば，テレビを視聴する事を目的として作られたテレビ，またはテレビの視聴にも特化したモニターが望ましい。

4. 有機 EL スマホ

有機 EL は，スマホにも採用され始めている。それは，次のようなメリットのためである。

バッテリーの持ちがいい

有機 EL の消費電力は，液晶より 30%ほど少ないと言われている。スマホの消費電力の内，ディスプレイが約 3 割を占めると言われており，有機 EL を搭載することで電池の持ちが大きく伸びる。液晶画面で 16 時間使えるスマホなら，有機 EL では更に 3 時間長く使えるという話もある。また，有機 EL は最小限のピクセルのみを起動することが可能である。

高画質

液晶よりも高画質である。特にコントラストがはっきりしている点と，黒色の発色の良さが注目されている。視野角が広いので複数人で一緒に画面を見るようなシーンにも適している。

曲面を生かしたデザインが可能

有機 EL ディスプレイは「折り曲げられる」という特性を持っている。その特性を生かして，スマホ全体が湾曲しているモデルも発売されている。より臨場感のある映像を楽しむことが出来ると注目を集めた。折りたたみ式で必要な時だけ画面を大きく出来るスマホも実用化される。

本体が薄い・軽い

有機 EL ディスプレイはバックライトが必要無いので，液晶よりも本体を薄く・軽くできる。

省電力

有機 EL ディスプレイは，ドット自体が発光するため，バックライトを必要としない。何がしかの画像や画面を表示するために必要なドット以外は発光しないよう制御することが可能なので，液晶ディスプレイよりも消費電力が少なくて済む。有機 EL ディスプレイ搭載スマホは，従来の液晶ディスプレイ搭載スマホよりも約 30%消費電力が少ないとされる。消費電力が少なければバッテリーの充電回数も減り，それによってバッテリーの寿命が延びる。携帯端末として出先でバッテリーの心配をしなくても良くなる。

高画質な動画の再生

有機 EL ディスプレイは，高画質な動画の再生に非常に強いディスプレイなので，4K 動画やその次に導入されると言われている 8K 動画の再生に最適と言える。有機 EL ディスプレイは高品質な表示が可能な上に応答性も高いため，スポーツなど動きの激しい動画の再生にも向いている。

有機 EL は，つぎのようなデメリットを持っている。

焼き付き

有機 EL ディスプレイの大きなデメリットのひとつに，画面の焼き付きがある。これは，技術的な進

化の当初から懸念されていた問題で，技術の根幹がブラウン管モニターと同じである有機 EL ディスプレイには，この焼き付きの問題が常につきまとっている。しかし，現在はかなり改善されており，12 時間以上同じ画面を表示し続けない限りは，焼き付きの問題はないとされる。

「画面の焼き付き」とは，画面を切り替えた時に，前に表示していた画面が残ってしまう現象のことである。同じ画面を長時間表示していると，ドットを構成している素子に，表示するための色が定着してしまうことがある。

ドット欠け

有機 EL ディスプレイも，液晶ディスプレイと同じくドットで構成されたディスプレイである。そのため，ドット欠けが発生する。新品のスマホを買ったときに，最初にドット欠けをチェックする。有機 EL ディスプレイの場合は，購入時にチェックするだけでは不十分と言える。使用を続けていくことでドット欠けを起こす可能性がある。ドットの１つ１つを制御する有機 EL ディスプレイでは，1 つのドットにかかる負担が大きくなってしまう傾向がある。液晶ディスプレイではまず起こりえない，使用していく中でのドット欠けが起きてしまう。

端末本体の価格が高い

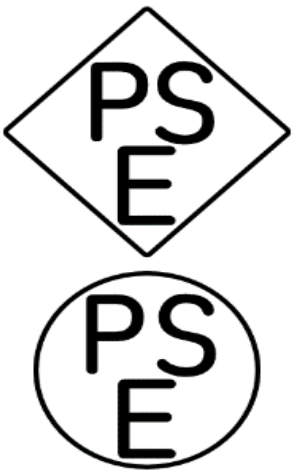
有機 EL ディスプレイは革新的な技術ゆえに，生産できるメーカーや生産量そのものがかなり限定される。そのため，スマホに搭載するためには，非常にコストがかかる。その分の価格はスマホ本体の値段に上乗せされて，本体価格が高くなる。

4. 電気製品に関連する法令

これらの電気製品には，安全に利用できるよう関連する法律が定められている。

電気用品安全法(PSE 法)

改正 PSE 法(2012 年 7 月)において，「エル・イー・ディー・ランプ」及び「エル・イー・ディー・電灯器具」の二品目が特定電気用品以外の電気用品に追加された。これらに該当する製品を 2012 年 7 月 1 日以降に製造もしくは輸入する場合は，製造者もしくは輸入者は，当該製品が PSE 法の技術基準に合致していることを確認した上で，特定電気用品以外の電気用品に表示する記号(○PSE 記号)を製品に表示する義務が



PSE 記号
（上）特定電気用品に表示する記号
（下）特定電気用品以外の電気用品に表示する記号

ある。加えて，製造者もしくは輸入者は PSE 法規定の手続きに沿って経産省に届出を行うと共に，同法が定めた製品検査を実施して検査記録を保管する義務がある。これら二品目に対して適用される PSE 法の技術基準には，ノイズに関する許容値と測定方法が含まれる。「エル・イー・ディー・ランプ」には，家庭で多く使われる E26 もしくは E17 口金の LED 電球が含まれる。 なお，LED を光源とする電気製品のうち以下の 6 品目は，既に PSE 法における特定電気用品以外の電気用品である。

1.電気スタンド

2.充電式携帯電灯

3.ハンドランプ

4.広告灯

5.庭園灯器具

6.装飾用電灯器具

電気事業法

経済産業省が管轄する電気事業法によって，電気の使用者の利益保護と電気事業の健全な発達を図り，電気工作物の工事，維持，運営を規制することで公共の安全の確保と環境の保全を図ることを目的としている。

電気設備技術基準

電気事業法に基づく経済産業省の省令であり，電気工作物の設計，工事，維持に関して守るべき性能基準を定めている。

電気工事士法

経済産業省が管轄する電気工事士法によって，電気工事作業に従事する者の資格と義務を定め，電気工事による災害発生の防止に寄与するための法律である。

日本工業規格

新 JIS マーク

日本工業規格の改正後，2005 年から登場した。

日本工業規格 (JIS) は鉱工業製品に関する日本での規格である。色に関する規格，電球・放電管・材料に関する規格，照明器具に関する規格，配線材料に関する規格など，多くの規格が含まれている。2005 年からは指定商品制度が廃止されて従来は規格対象外の為に JIS マークが付けられなかった製品にも，規格に合っていれば新 JIS マークが表示できるようになった。

建築基準法

国土交通省が管轄する建築基準法によって，建築物の敷地，構造，設備，用途に関する最低限の基準を定めている。この中には電気設備に関する基準も含まれ，非常用照明設備に関する設置基準やその明るさなどが定められている。なお，2013 年 6 月現在の建築基準法施行令においては，非常用照明設備で LED 照明を用いることは認められていない[出典 17]が，各メーカーより常時は LED 照明を用い，非常時には施工令で認められている白熱・ハロゲン電球や蛍光灯を用いる非常用照明器具が発売されている。

消防法

誘導灯や誘導標識などを決めているのは，基本となる消防法の元に細部が消防法施行令や消防法施行規則によって規定されており，地方自治体によって違いがある場合がある。

課　題

1．ディスプレイの仕組みと，種類についてまとめなさい。

第４講　電池

【学修到達目標】

- 電池の特徴を説明できる。
- 電池の仕組みを理解できる。

１．リチウムイオン電池(リチウムイオン二次電池)

1980 年代, 携帯電話やノートパソコンなどの携帯機器の開発により, 高容量で小型軽量な二次電池（充電可能な電池）のニーズが高く，新型二次電池が切望されていた。リチウムイオン二次電池（lithium-ion rechargeable battery）は，非水電解質二次電池の一種で，電解質中のリチウムイオンが電気伝導を担う二次電池である。正極にリチウム金属酸化物を用い，負極にグラファイトなどの炭素材を用いるものが主流である。リチウムイオン二次電池（LIB）は携帯電話，ノートパソコン，デジタルカメラ・ビデオ，携帯用音楽プレーヤーを始め幅広い電子・電気機器に搭載された。小型で軽量な LIB を搭載することで携帯用 IT 機器の利便性は大いに増大し，迅速で正確な情報伝達とそれにともなう安全性の向上・生産性の向上・生活の質的改善などに多大な貢献をしている。周期表では，リチウムは 3 番目に軽い元素である。

族 / 周期	1 A	2 A	3 A	4 A	5 A	6 A	7 A	8			1 B	2 B	3 B	4 B	5 B	6 B	7 B	0
	アルカリ金属元素	アルカリ土類金属元素	希土類元素	チタン族元素	バナジウム族元素	クロム族元素	マンガン族元素	鉄族元素 (26～28) 白金族元素 (44～46／76～78)			銅族元素	亜鉛族元素	ホウ素族元素	炭素族元素	窒素族元素	酸素族元素	ハロゲン族元素	希ガス族元素
1	1 ＊ H 水素 1.00794																	2 He ヘリウム 4.00260
2	3 Li リチウム 6.941	4 ＊ Be ベリリウム 9.01218											5 B ホウ素 10.81	6 C 炭素 12.011	7 N 窒素 14.0067	8 O 酸素 15.9994	9 F フッ素 18.998403	10 Ne ネオン 20.179
3	11 Na ナトリウム 22.98977	12 ＊ Mg マグネシウム 24.305											13 Al アルミニウム 26.98154	14 Si ケイ素 28.0855	15 P リン 30.97376	16 S 硫黄 32.06	17 Cl 塩素 35.453	18 Ar アルゴン 39.948
4	19 K カリウム 39.0983	20 Ca カルシウム 40.08	21 Sc スカンジウム 44.9559	22 Ti チタン 47.88	23 V バナジウム 50.9415	24 Cr クロム 51.996	25 Mn マンガン 54.9380	26 Fe 鉄 55.847	27 Co コバルト 58.9332	28 Ni ニッケル 58.69	29 Cu 銅 63.546	30 Zn 亜鉛 65.38	31 Ga ガリウム 69.72	32 Ge ゲルマニウム 72.59	33 As ヒ素 74.9216	34 Se セレン 78.96	35 Br 臭素 79.904	36 Kr クリプトン 83.80
5	37 Rb ルビジウム 85.4678	38 Sr ストロンチウム 87.62	39 Y イットリウム 88.9059	40 Zr ジルコニウム 91.22	41 Nb ニオブ 92.9064	42 Mo モリブデン 95.94	43 Tc テクネチウム [98]	44 Ru ルテニウム 101.07	45 Rh ロジウム 102.9055	46 Pd パラジウム 106.42	47 Ag 銀 107.8682	48 Cd カドミウム 112.41	49 In インジウム 114.82	50 Sn スズ 118.69	51 Sb アンチモン 121.75	52 Te テルル 127.60	53 I ヨウ素 126.9045	54 Xe キセノン 131.29
6	55 Cs セシウム 132.9054	56 Ba バリウム 137.33	57 - 71 ランタノイド	72 Hf ハフニウム 178.49	73 Ta タンタル 180.9479	74 W タングステン 183.85	75 Re レニウム 186.207	76 Os オスミウム 190.2	77 Ir イリジウム 192.22	78 Pt 白金 195.08	79 Au 金 196.9665	80 Hg 水銀 200.59	81 Tl タリウム 204.383	82 Pb 鉛 207.2	83 Bi ビスマス 208.9804	84 Po ポロニウム [209]	85 At アスタチン [210]	86 Rn ラドン [222]
7	87 Fr フランシウム [223]	88 Ra ラジウム 226.0254	89 - 108 アクチノイド															
	典型元素		遷移元素									典型元素						

＊は族分類に含まれない

リチウムイオン二次電池には次の特長がある。

・ エネルギー密度が高い

軽量でコンパクトなモジュール・パック構造

・ 急速充放電が可能

大電流での入出力が可能であり，風力発電，太陽光発電等の不安定な電力を効率的に安定化するシステムを構築

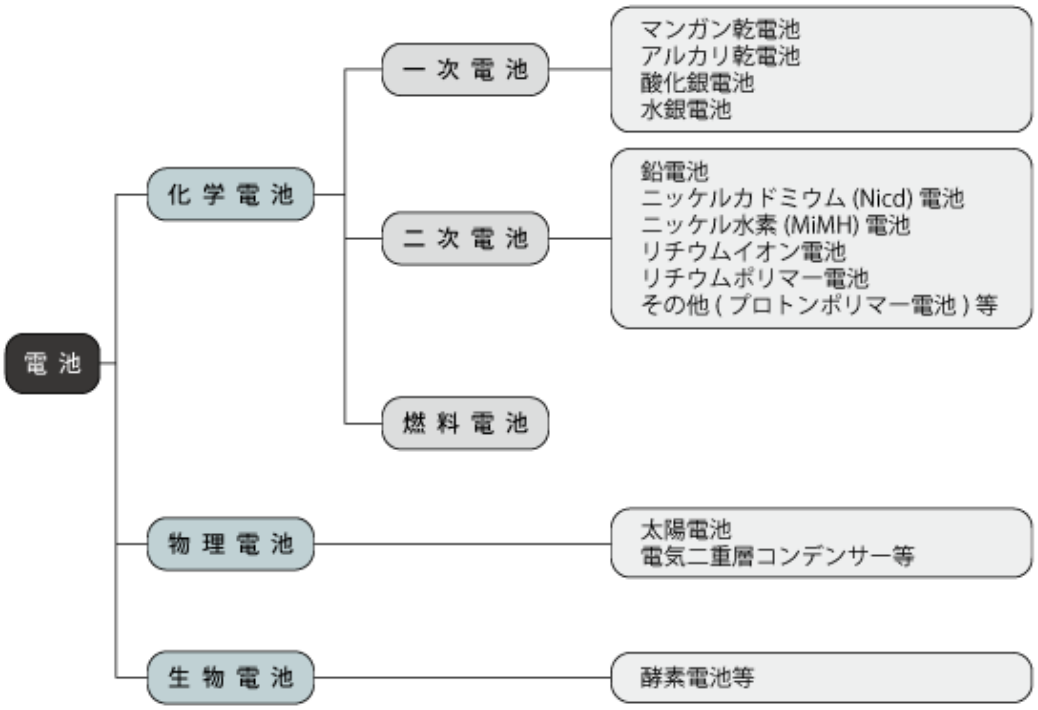
・ 長寿命

メモリー効果*がなく，長期間の使用が可能

*メモリー効果

蓄電池を使用しているうちに，使用できる容量が本来の容量よりも減少してしまう現象。蓄電池を使い切らないうちに充電すると，再充電した容量しか使えなくなってしまい，蓄電池が容量を記憶しているように見えることからこのように呼ばれる。蓄電池をきちんと使い切るようにすれば，解消できる。

二次電池とは，充電と放電を繰り返して使用することができる化学電池のことで，蓄電池や充電池，バッテリーなどとも呼ばれる。リチウムイオン電池，ニッケル・カドミウム電池などがあり，ノートパソコンや携帯電話などで広く使用されている。これらの電池は化学電池と呼ばれ，燃料電池も化学電池である。



電池には化学電池以外に物理電池や生物電池がある。

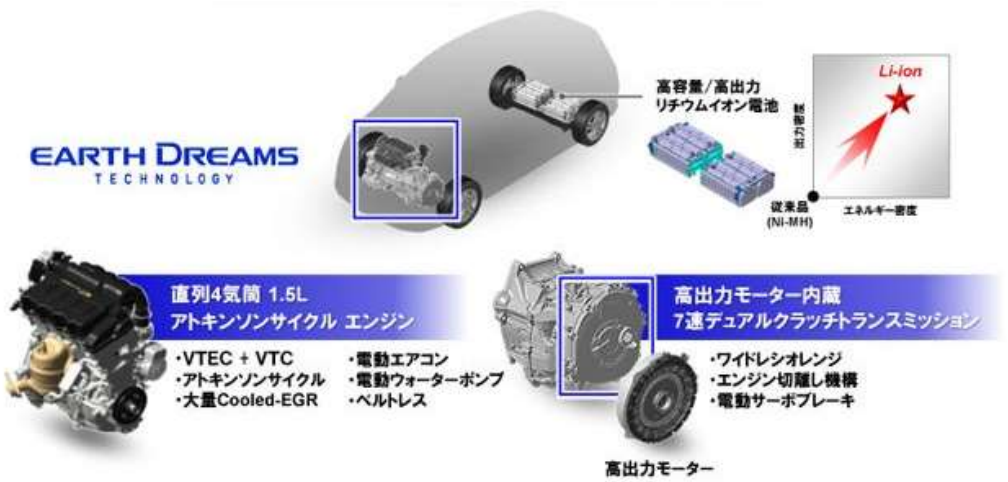
二次電池には，ニッケル水素電池や鉛蓄電池，リチウムイオン電池など多くの種類がある。二次電池は使用するたびに劣化し，サイクル充電を迎えると性能が低下する。二次電池の特徴は次のとおりである。

各種二次電池の比較（鉛電池を１００とした場合）

項目	鉛電池	ニッケル水素電池	ナトリウム硫黄電池	リチウムイオン二次電池
電圧（%）	100	60	100	185
容量密度（%）	100	153	250	313
出力密度（%）	100	200	140	300
寿命（%）	100	111	250	194
出力レート（%）	100	500	70～85	1,000
充放電エネルギー効率（%）	75～85	80～90	90	94～96
作動条件（℃）	常温	常温	250～300	常温

リチウムイオン二次電池は，家庭用だけでなく，大規模な利用も行われている。

エコカーと呼ばれる自動車（EV・HEV・P-HEV）などの交通機関の動力源として実用化が進んでおり，電力の平準化やスマートグリッド**のための蓄電装置としても利用されている



**スマートグリッドとは，IT 技術によって，供給側・需要側の双方から電力量をコントロールできる送電網のことで，「次世代送電網」とも呼ばれる。これまでの電力供給は，供給側である発電所から，企業や家庭などに向けて，一方向に電力が流れるものであった。一方，スマートグリッドでは双方向的に電力が流れるほか，電力供給の過不足といった情報もやり取りできる。スマートグリッドは，環境問題と経済問題を解決する手段として期待されている。スマートグリッドのメリットは，「効率的な電力供給」「再生可能エネルギーの効率的な導入」である。

効率的な電力供給 ： スマートグリッドでは，双方向でデータをやり取りでき，企業や家庭における消費電力情報や，電力会社からの電力抑制指示を送受信できる。電力会社は，企業や家庭の電気の消費量が減少したというデータを受け取った場合，それに合わせて電力供給を抑えることで，過剰な発電を防ぐことが可能となる。余剰電力を別の需要家に回すなどの調整ができる。スマートグリッドでは，需給バランスを調整できるため，停電防止にもつながる。

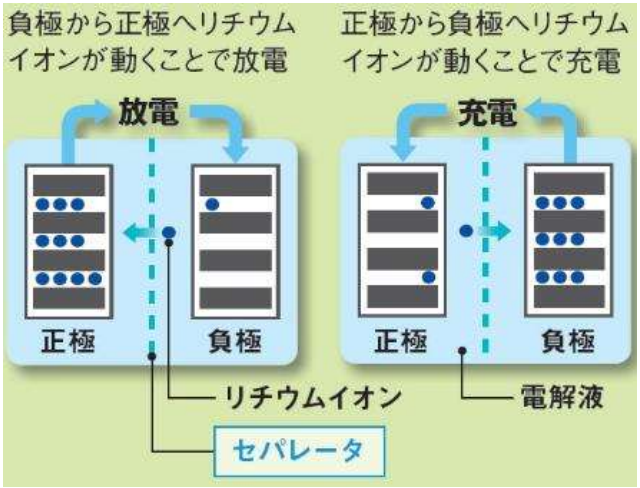
再生可能エネルギーの効率的な導入 ： スマートグリッドでは，従来の大規模発電所による電気と，家庭などで発電された電気を合わせてコントロールすることが可能である。地域で太陽光発電や風力発電システムをつなげ，優先的に電力を融通できれば，電気を地産地消することも可能である。再生可能エネルギーは発電量が天候に左右されるという不安定感があるが，その際は発電所から供給量を増やすことで，安定した電力供給が可能となる。

2. リチウムイオン電池のしくみ

リチウムイオン電池と呼ばれるのは，リチウムイオンが動作に重要な役割を果たしているからで，リチウムイオンはリチウム原子がイオンになったものである。リチウム（元素記号は Li）は原子番号 3 の元素で，1 つのリチウム原子から 1 つの電子が取り除かれたものがリチウムイオン（化学式は Li+）である。電子はマイナスの電荷をもっているので，リチウムイオンは電子 1 つ分プラスの電荷をもっていることになる。リチウムイオンは液体や固体の中を動きやすい性質を持っており，リチウムイオンは電池の内部でプラス極とマイナス極の間を行き来することができる。

リチウムイオン電池は，一般的にプラス極（正極）・マイナス極（負極）・ 電解液・セパレータから構成されます。電解液の中にプラス極とマイナス極が，セパレータを挟んだ配置で浸されている。プラス極（正極）：リチウムと金属を含む酸化物(セラミック)が使われる。例として，コバルト酸リチウム（LiCoO2）やニッケル酸リチウム（LiNiO2），マンガン酸リチウム（LiMn2O4）などがある。マイナス極 （負極）：主に黒鉛（鉛筆の芯の仲間）が使われる。電解液は，有機溶媒（油の仲間）にリチウム化合物（LiPF6，LiBF4，LiClO4 など）を溶かしたものが使われます。有機溶媒の例として，エチレンカーボネート，プロピレンカーボネート，ジメチルカーボネートなどがある。セパレータはポリオレフィンと呼ばれる高分子化合物からできた膜を使う。膜の表面には 1 マイクロメートル以下の小さな穴が開いている。ポリオレフィンの例として，ポリエチレンやポリプロピレンなどがある。容器は金属ケースやラミネート材（アルミニウムやステンレスのような薄い金属を，ポリエチレンテレフタレートやポリプロピレンなどの樹脂でサンドイッチしたもの）が使われます。

リチウムイオン電池が充放電（充電もしくは放電）するときには，リチウムイオンがプラス極とマイナス極の間をリチウムイオンが行き来する。リチウムイオン電池に使われる多くのプラス極とマイナス極の材料は層状の構造になっており，層と層の間にリチウムイオンをためることができる。リチウムイオンは



電子１つ分プラスの電荷を持っているので，リチウムイオンを含んだマイナス極の材料からリチウムイオンが出ていくと，マイナス極はマイナスの電荷をもつことになる。このマイナスの電荷を電子として電池から取り出すことで，電力を得ることができる。これが放電反応（電池を使う反応）である。

外部から電気を流し込んでマイナス極の中に電子を取り込ませると，マイナス極材料がマイナスの電荷をもつことになる。このマイナスを打ち消すために，プラス極側からやってきたリチウムイオンがマイナス極に取り込まれる。これが充電反応（電池を使える状態にする反応）である。

リチウムイオン電池は，正極に使用する金属の違いによって，いくつかの種類に分けられる。最初にリチウムイオン電池の正極に使用された金属は，コバルトであった。コバルトはリチウムと同じく産出量の少ないレアメタルなので，製造コストがかかる。そこで，安価で環境負荷が少ない材料として，マンガンやニッケル，鉄などが使用されるようになってきた。使われている材料ごとにリチウムイオン電池の種類が分かれる。

リチウムイオン電池の種類と特徴

リチウムイオン電池の種類	電圧	放電可能回数	長所・短所
コバルト系リチウムイオン電池	3.7V	500～1000 回	リチウムイオンの標準電池として広く普及 高価で車載用には使われていない
マンガン系リチウムイオン電池	3.7V	300～700 回	安全性が高い 急速充電，急速放電ができる
リン酸鉄系リチウムイオン電池	3.2V	1000～2000 回	安価でサイクル寿命（充放電による劣化），カレンダー寿命（放置による劣化）が長い 電圧が他のリチウムイオン電池より低い
3 元系リチウムイオン電池	3.6V	1000～2000 回	電圧がそこそこ高く，サイクル寿命も長い 材料の合成が難しい

コバルト系リチウムイオン電池

正極にコバルト酸リチウムを使用する。コバルト酸リチウムは比較的容易に合成でき，取り扱いが簡単であることから，リチウムイオン電池で最初に量産された。しかし，レアメタルで高価な金属であることから，自動車部品にはほとんど採用されていない。

マンガン系リチウムイオン電池

正極にマンガン酸リチウムを使用する。コバルト系リチウムイオン電池と同じくらいの電圧を出すことができ。安価で作れるというメリットがある。欠点として，充放電中に電解質にマンガンが溶出

することがあるので電池の寿命が短くなる。

リン酸鉄系リチウムイオン電池

正極にリン酸鉄リチウムを使用する。リン酸鉄系リチウムイオン電池は内部で発熱があっても構造が崩壊しにくく,安全性が高いうえに,鉄を原料とするためマンガン系よりもさらに安く製造できる。ただし，他のリチウムイオン電池よりも電圧は低い。

3 元系リチウムイオン電池

コバルトの使用量を下げるため，コバルト，ニッケル，マンガンの 3 種類の材料を使って作る電池である。現在では，ニッケルの割合が高いものが多くなっている。また，コバルト系やマンガン系よりも電圧はわずかに低下するが，製造コストは下げられる。それぞれの材料の合成が難しいことや安定性に劣るなどの課題がある。

単位容積あたり高い密度でエネルギーが蓄えられるリチウムイオン電池は，他の種類の電池に比べて安全性に十分な配慮が必要である。可燃性の有機溶媒を使っている点からも，水溶液を使っている他の電池と比べて取り扱いに注意が必要とされる。最も避けなければならないのは，内部短絡である。内部短絡とは，外部からカが加わって電池が変形し，正極と負極が直接繋がってしまう状態のことである。そこに電流が集中すると温度が上昇し，電池自体が発火するといった大きな事故となる。ごく小さな不純物でも，電池内部に混入することで内部短絡が起きてしまう可能性があるため，電池内に過剰な電流が流れないように保護回路を設けるといった事故防止機能を持たせることが必要である。さらに，電池の使用環境を60℃以下に保つために冷却装置を使用するなど，電池自体の温度をコントロールすることが重要になってくる。一定以上温度が上がった場合に，正極と負極を隔てる膜となっているセパレータが正極と負極の間を完全にシャットアウトするなど，さまざまな方法で安全性を高める工夫が考えられている。

パソコンやスマホにリチウムイオン電池が利用されるのは次の特性があるからである。

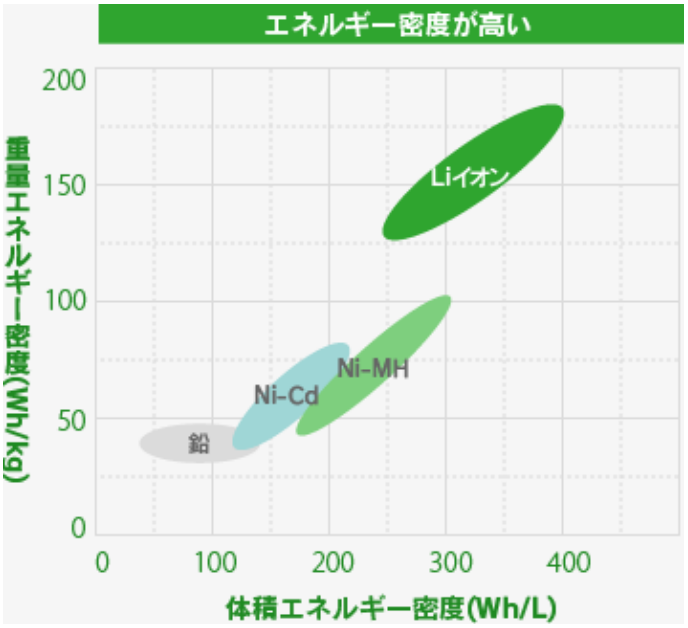
- リチウムイオン電池のように充電して繰り返し使える二次電池には，鉛蓄電池以外にもニッケル水素電池やニッケルカドミウム電池などがあるが，これらと比べて軽くてパワフルである。同じサイズで比べると，鉛蓄電池は 2.1V，ニッケル水素電池は 1.2V，ニッケルカドミウム電池は 1.25V までの電圧しか出せないのに対して,リチウムイオン電池は 3.2～3.7V の高い電圧まで出すことができる。
- リチウムイオン電池は電気を作る時に他の二次電池のような化学反応を利用しないので，他の二次電池に比べて電極の劣化が少なく，充電や放電の繰り返しにも非常に強い。
- リチウムイオン電池には急速充電ができる。ニッケル水素電池やニッケルカドミウム電池は急速充電はできるが，充電の終了判定が難しかったため実用化されなかった。リチウムイオン電池は，充電器側で終了判定が可能になり実用化された。

・充電ケーブルを使わずに充電するワイヤレス充電も，急速充電と同じくリチウムイオン電池以外の二次電池でも可能である。ワイヤレス充電の技術が確立されたのは 2007 年と比較的新しい技術であるため，すでに普及が見込まれていたリチウムイオン電池で採用されることになった。

・電池は使わなくても自然に放電してしまう「自己放電」という現象があり，自己放電は，放置しているだけでも少しずつ化学反応が進行することでおこる。他の二次電池で起きる電池反応とは少し違った反応を用いるリチウムイオン電池では，ほとんど自己放電は起きない。

電池の種類	電圧	
自動車で使われる鉛蓄電池	2V	正極：二酸化鉛，負極：鉛の組み合わせ （自動車にはこれを 6 直列にした 12V のものが使われる）
ニカド(Ni-Cd)電池	1.2V	正極：水酸化ニッケル，負極：水酸化カドミウムの組み合わせ
ニッケル水素(Ni-MH)電池	1.2V	正極：水酸化ニッケル，負極：水素吸蔵合金の組み合わせ
リチウムイオン電池	3.2～3.8V	

ニッケル水素電池に比べて，体積エネルギー密度で約 1.5 倍，重量エネルギー密度で約 2 倍と，同じ容量であれば，リチウムイオン二次電池はニッケル水素電池の 2/3 の体積で，かつ，半分の重さに小型軽量化することができる。しかし，リチウムイオン電池に力を加えて破損したり，充電しすぎると発火するといった課題もある。



3. 電池の種類

家庭で使われる電池は，マンガン乾電池＜一次電池＞，アルカリ乾電池＜一次電池＞，ニカド電池＜二次電池＞，ニッケル水素電池＜二次電池＞，リチウムイオン電池＜二次電池＞がある。それぞれの特性に合わせた電気機器に使用する。

マンガン乾電池＜一次電池＞

プラス極に二酸化マンガン，電解液に塩化亜鉛（または塩化アンモニウム），マイナス極に亜鉛を用いている。 歴史が古く，世界で一番使われている乾電池である。小さな電力で動く機器に適している。小さな電力で長い時間使う置き時計や掛け時計，また，リモコン，ガスや石油機器の自動点火など大きな電力で短い時間で時々使うものにおすすめで，安価で経済的である。

アルカリ乾電池＜一次電池＞

マンガン乾電池よりも大きな電流が取り出せるのが，アルカリ乾電池である。 これは電流の流れやすいアルカリ性水溶液の水酸化カリウムを電解液にしているためである。大きな電力が必要な機器に適している。マンガン乾電池の約２倍以上長く使える。デジタルカメラ，CD ラジカセ，ヘッドホンステレオ，モーターを使うおもちゃなど比較的長い時間使う用途に適している。

※単２形

ニカド電池(ニッケル・カドミウム蓄電池)＜二次電池＞

電圧は 1.2V で，ニッケル水素電池と同様，アルカリ乾電池と互換性(同じ形のもの)があり，電池を頻繁に交換して使用する機器におすすめで，経済的である。

ニッケル水素電池＜二次電池＞

ニカド電池と同じ 1.2V で，アルカリ乾電池と互換性がある。同じ大きさで，ニカド電池に比べて約 2 倍の電力を持っている。

リチウムイオン電池＜二次電池＞

電圧が 3.7V と，ニッケル水素電池などの約 3 倍の電圧で，軽くて大きな電力を持っていることが特長である。携帯電話，ノートパソコン，ビデオカメラ，デジタルカメラなどに使われる。

電池の種類による使い分けは，次のとおりである。

・高電圧を必要とする機器

デジタルカメラ・デジタルビデオに代表され，常時 1.0 ～ 1.05 V の電圧を必要とするレンジ。デジタル機器はアナログ機器と違い，終止電圧を下回ると機能が完全に停止する。

このレンジでは，マンガン電池は出力が低過ぎて不向き

・中電圧を必要とする機器

デジタルオーディオや CD・MD プレーヤーに代表され，およそ 0.9 V 以上の電圧を必要とするレンジ。このレンジでも，やはりマンガン電池では出力が低く不向きで，それ以外の電池では，やはりリ

チウム電池とニッケル水素充電池が長持ちかるが，差異が顕著ではなくなり，1 時間単位のコストで考えると,アルカリ電池が最もコストパフォーマンスが良い。これは高電圧を必要とする機器に比べ，消費電力が少なく，終止電圧も低い為である。

・低電圧しか必要としない機器

時計やリモコンに代表される低電圧を対象としたレンジである。このレンジでは，自己放電してしまう性質からニッケル水素充電池は不向きである。長期使用を考えれば，リチウム電池とアルカリ電池が有利といえるが， コストパフォーマンスや電池の特性を考えると，アルカリ電池かマンガン電池が有利である。特に電流を止めると一時的に起電力が回復する特性を持つマンガン電池は最適である。

		高電圧	中電圧	定電圧
一次電池	マンガン電池		○	◎
(乾電池)	アルカリ電池	○	◎	◎
二次電池	ニカド電池	◎	○	
(充電池)	ニッケル水素電池	◎	○	△

電池を長持ちさせるには，次のことに気を付ける。充電すれば繰り返し使える二次電池は，種類によって長持ちのコツがある。ニッケル水素電池の上手な充電方法は，使い切る前に継ぎ足し充電をすることである。携帯電話などに使われているリチウムイオン電池も同じように継ぎ足し充電を心がける。ニカド電池は，充電をきちんと使い切ってから充電する。

全固体電池とは，電流を発生させるために必要でこれまで液体だった「電解質」を固体にした仕組みの電池のことである。電池は主に「電極」「活物質」「電解質」で構成されており，活物質や活物質に含まれるイオンが電解質の中を泳ぐことで電極間（負極から正極の間）に電子を通し電気を発生させている。つまり，電池を構成する電解質は「イオンが素早く動き回れるような特性」を持っていなければならない。全固体電池ではこの電解質に特殊な物質を利用することで，固体であるにも関わらず電気が流れるようになる。全固体電池は長年実用化できないと考えられていた。ところが，固体であるにも関わらず，内部で電子を運搬する小さな物質（イオン）が動き回って十分な電気を流すことができる物質が発見されたことで全固体電池の開発が活発化した。

全個体電池が注目されているのは，次の特性があるからである。

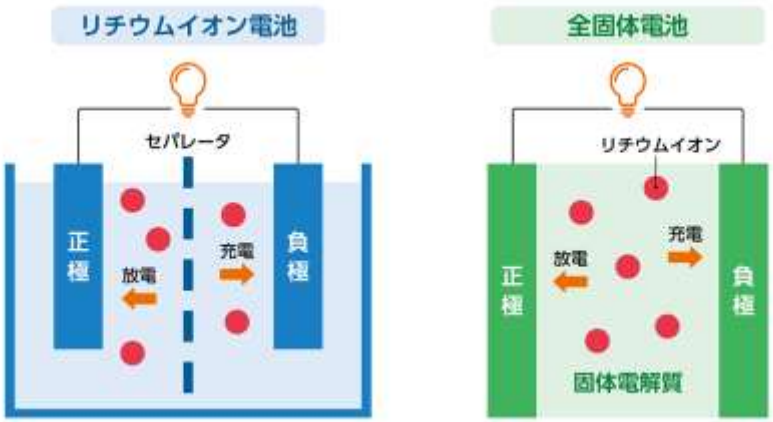
・低温から高温まで耐えられる。リチウムイオン電池の電解質は可燃性の有機溶媒（水に溶けない物質を溶かす液体）を使っているので，高温環境下での使用には懸念がある。全固体電池の電解質は可燃

性の材料が使われていないため，より高い温度での使用も可能になる。液体の場合は低温になるとイオンの動きが鈍くなって電池の性能が下がり，電圧が下がってくることがある。固体の場合は，低温になっても液体のように凍ることがないため，それほど内部の抵抗が上がらず，電池の性能はそれほど下がらない。

・急速充電が可能である。高熱に強いというメリットは，急速充電をする場合にも有利になる。電池は急速に充電するほど熱を持つので，高温に強い全固体電池は現在のリチウムイオン電池よりもさらに急速で充電させられる。

・寿命が長い。電池の寿命は電解質の性質によって変わる。リチウムイオン電池は，他の二次電池のような電池反応を利用しないことから，電極の劣化が少なく寿命が長いが，長く使用していると電解質の劣化が見られるようになる。全固体電池の電解質は液体よりも劣化が少ないので，さらに寿命を延ばすことが可能になる。

・形状の自由度が高い。液体の電解質は，液漏れを防ぐために構造上の制約があるが，全固体電池の場合はその縛りがないので小型化・薄型化しやすく，重ね合わせたり折り曲げたりして使用することも可能なのでさまざまな形状で利用することができる。



全固体電池の用途として期待されているものの一つは電気自動車である。現在，電気自動車にはリチウムイオン電池が使われているが，全固体電池であれば，可燃性の有機溶媒を含まないので，事故による発火などのリスクがより小さくなることが期待されている。また，現在の電気自動車はガソリンによる給油に比べると時間がかかるが，全固体電池であればより急速に充電することが可能になる。また，全固体電池の実用化が積極的に進められている背景の一つには，リチウムイオン電池が抱える高温に弱いという弱点が補えることが挙げられる。熱に強い特徴を生かせば電子基板に直接ハンダ付けできるので，電子機器

のバックアップ電源やIoTセンサなどでの活用も想定されている。さらに,リチウムイオン電池に比べて,より大容量，大出力が実現できることから，飛行機や船などでの活用も期待でき，高温から低温まで温度変化に強いことから，宇宙空間で使用されるデバイスなどにも用途が広がることが期待できる。

課　題

１．電池のしくみと特性についてまとめなさい。

第５講　家庭の電気設備

【学修到達目標】

⎈電気が家庭に届くまでの仕組みを理解できる。

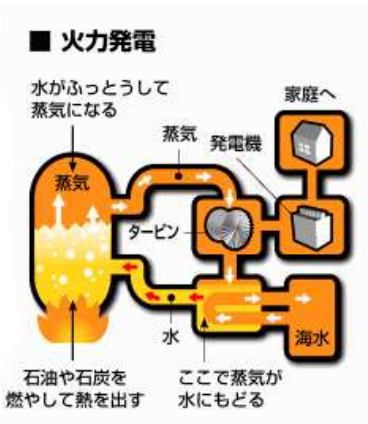
⎈家庭の電気設備の仕組みを理解できる。

１．配電

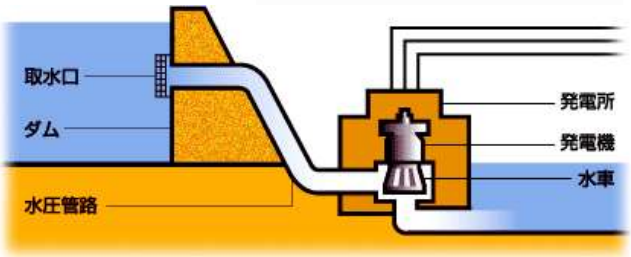
電気が家庭に届くまでには，発電→送電→変電所→配電の道筋を通る。　(出展:中部電力)

発電方法には火力発電，水力発電，原子力発電などがあり，それぞれに特性がある。一定量の発電に向いている発電方法や変動する電気の使用量に合わせてすばやく調整できる発電方法を組み合わせている。

火力発電は，石油・石炭や液化天然ガス（LNG）を燃やして水を熱し，そのときに発生する高温高圧の蒸気でタービン（羽根車）を回し，発電機を回して電気をつる（汽力発電）。このほかに，蒸気（水）の代わりに高温高圧に圧縮加熱したガスを使うガスタービン発電や，汽力発電とガスタービン発電を組み合わせたコンバインド・サイクル発電という方式もある。また，石油や石炭を燃やすと煙が出るが，煙の中のススなどの汚れは電気集塵機などで取り除いて，空気を汚さないようにしている。

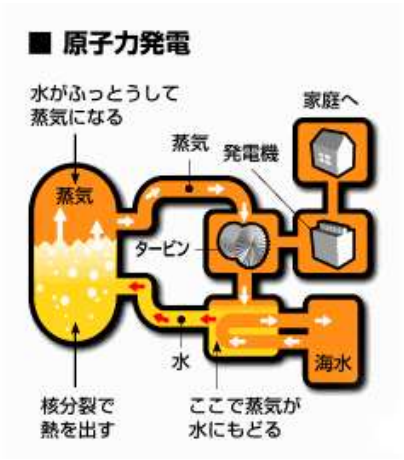


水力発電は，水が高いところから低いところへ落ちる力を使って水車を回し，発電機を回して電気をつくる。水車を回すには，たくさんの水を必要とするので，川にダムをつくって水をせき止めて利用する。水力発電の中には，夜間，火力発電所や原子力発電所でつくられた電気で

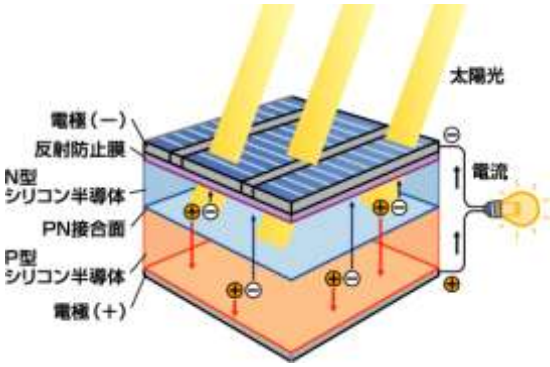


水を汲み上げ，昼間の電気がたくさん使われるときに，この水を落として発電に使う揚水発電所もある。

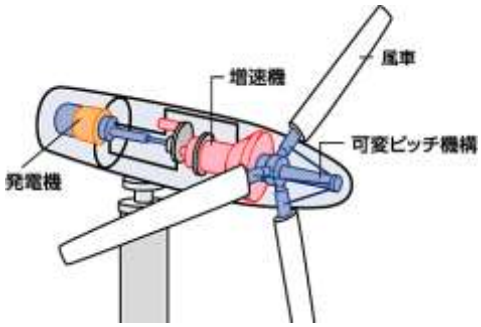
原子力発電は，ウラン燃料からでる熱で水を沸騰させて，蒸気をつくり，この蒸気の力でタービン（羽根車）を回し，発電機を回して電気をつくる。火力発電所がボイラーで石油，石炭，LNG などを燃やして蒸気をつくるのに対し，原子力発電は水の入った原子炉の中でウランの核分裂を起こし，その熱で蒸気をつくる。また，ウラン燃料は繰り返し使うことができる。原子力発電所をつくる場所は，特に固い岩盤が選ばれ，地震などに備えた何重もの安全対策をしている。



太陽光発電は，光エネルギーから直接電気を作る太陽電池を利用した発電方式である。太陽電池は，プラスを帯びやすい P 型シリコン半導体とマイナスを帯びやすいＮ型シリコン半導体を張り合わせてある。この 2 つの半導体の境目に光エネルギーが加わると，P 型シリコン半導体はプラスになり，N 型シリコン半導体はマイナスになる。電線をつなげば電気が流れ，光エネルギーがあたり続ければ電気は発生し続ける。太陽光発電の長所は，「自然のエネルギーを利用するために，なくなる心配がない。」「発電時に二酸化炭素などを出さないため，環境にやさしい。」「しくみが単純なため，管理しやすい。」である。短所は，「大量の電気を作るためには，広大な土地が必要になる。」「エネルギー密度が低い。」「雨や曇りの日，夜間は発電できないなど，自然条件に左右される。」「費用が高い。」である。



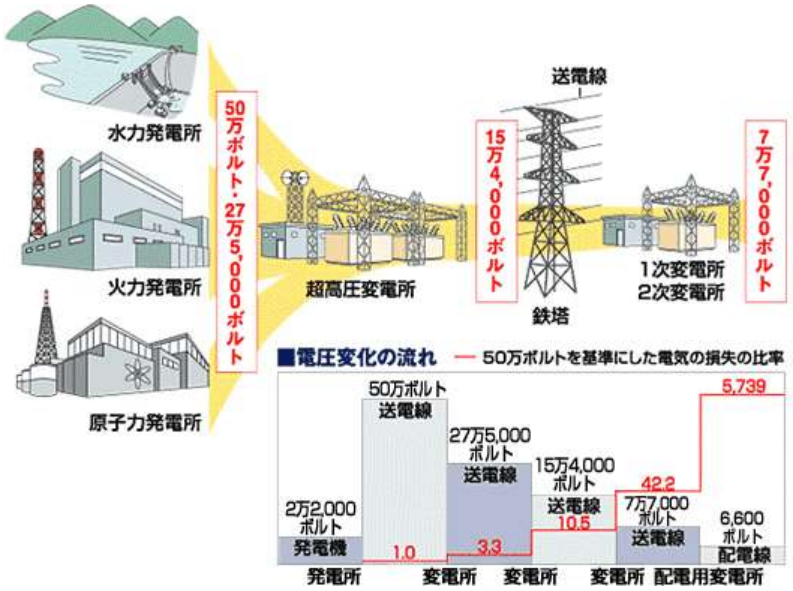
風力発電は，風の力を利用して風車を回し，風車の回転運動を発電機に伝えて電気を起こす。風力発電機は，風の強さや向きをはかり，羽根の角度や風車の向きを自動的に調整して，効率的に発電する。風速が大きくなって風車の回転速度が上がりすぎる時は，安全のため回転を停止させる。風車の回転軸により水平型，垂直型があり，風車の種類もプロペラ型のほかに，タリウス型などさまざまな構造がある。風力発電は，風が強い場所にたくさんの風車を設置することから，風車が集まっている場所をウインドファーム（風の牧場）または，ウインドパークと呼ぶ。風力発電の長所は，「自然のエネルギーを利用するため，なくなる心配がない。」「発電時に二酸化炭素などをださないため，環境にやさしい。」



である。短所は，「風の強い地域でないと発電効率が悪く，設置場所が限られる。」「風の強さに左右されるので，発電が不安定になる。」「騒音が出る。」である。

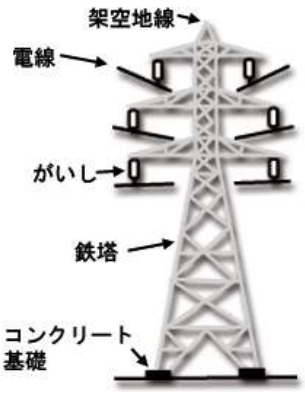
バイオマス発電は，木屑や燃えるゴミなどを燃焼する際の熱を利用して電気を起こす発電方式である。発電した後の排熱は，周辺地域の暖房や温水として有効活用できる。バイオマス発電の長所は，「大気中の二酸化炭素を増やさない。」「自然エネルギーを利用した発電方法の中では，連続的に資源を得られるため安定している。」である。短所は，「発電効率が低い。」「資源の収集や運搬・管理に費用がかかる。」である。

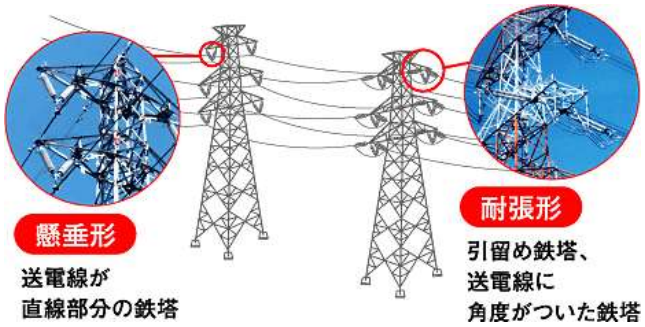
送電は，発電所や変電所を結び確実に電気を送ることである。都市部から遠く離れた発電所で作られた電気は，送る途中に熱となって逃げる電気の量を少なくするため，電圧を高くして送る。電気の使われる各家庭や工場に届ける前に，変電所で使いやすい電気の大きさに変える。



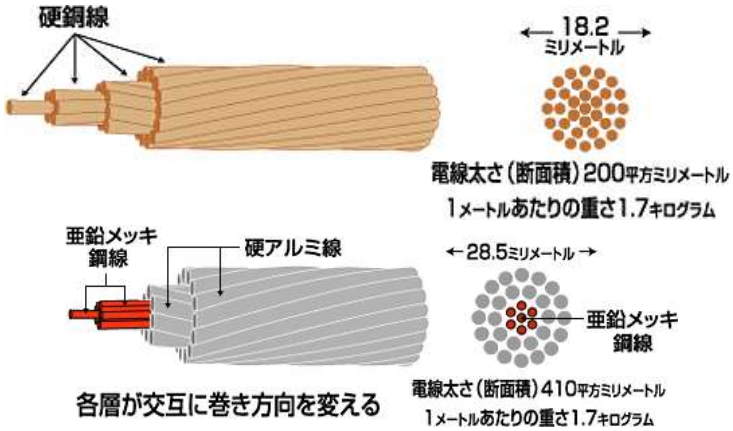
架空送電は，電圧を高くして電気を送る仕組みで，鉄塔などを使って，地上から高いところに電線を張って送る方法である。送る電気の電圧が高くなるにつれて，まわりにある建物や樹木などとの距離を大きくとらなければならないため，鉄塔の高さも高くなる。雷，台風，氷雪，豪雨などのときでも確実に電気を送ることができるように工夫されている。発電所でつくられる電気は，電線３本を１組として電力を送る三相交流と呼ばれる電気である。

鉄塔は，架空地線，電線，がいし，鉄塔，コンクリート，基礎などで構成されている。電線をささえるものには鉄塔，鉄柱，鉄筋コンクリート柱，木柱などがあるが，強度と信頼性が高いため，主として送電線には鉄塔が使われる。鉄塔は，設置場所や送る電気の電圧によって，いろいろな形状や大きさのものがある。例えば，送電線が直線部分の鉄塔は「懸垂型」，送電線に角度がついた鉄塔には「耐張型引留め鉄塔」が使われる。また，地上高 60m 以上のものは，赤白に塗り分けられたり，航空障害灯としてフラッシュライトがつけられている。



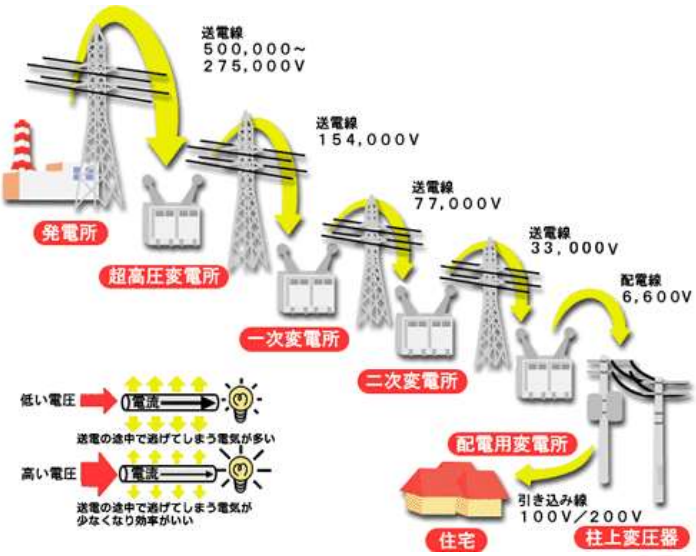


架空送電線は，がいしで絶縁されているため，絶縁電線ではなく，裸線を使用している。一般に鋼心アルミより線や裸硬銅より線が使われる。



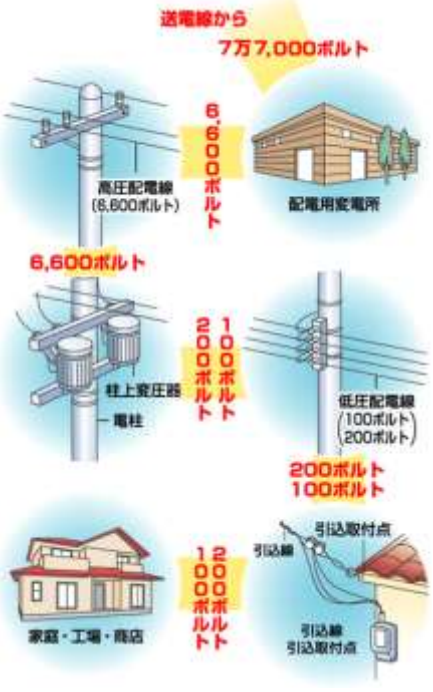
がいしは，送電線，配電線などの電気の流れる電線と鉄塔・電柱とを絶縁するためのもので，高い絶縁能力と大きな強度が必要である。がいしは，太陽光や温度変化による自然劣化が少ない磁器製が使われている。がいしには電線の重量や電線を張る力，そして風圧などの大きな力がかかる。一列のがいしで強さが足らない時は，二連，三連と並列に増やす。また，電圧を高くする時は直列に連結する。

変電所とは，電気の電圧を変える場所である。発電機で作り出される電気は 2 万 3 千ボルトや 1 万 2 千ボルトであり，電気抵抗によるロスが生じるため，50 万ボルトや 27 万 5 千ボルトという高い電圧にして送り出す。超高圧変電所，一次変電所，二次変電所，配電用変電所と各変電所で徐々に電圧を下げて，家庭や工場に届ける。変電所には変圧器のほかに，故障などのときに自動的に電気を切る「遮断器」，送電装置を点検するときに電気を切る「断路器」，落雷のときに雷の電気を地面ににがすための「避雷器」などの安全装置を備えている。



家庭や工場などに電気を送るには，電柱を使って電気を配る「架空配電」と地中に埋設したケーブルを使って，電気を配る「地中配電」がある。送電線から 7 万 7,000 ボルト，配電用変電所から 6,600 ボルト，高圧配電線（6,600 ボルト），柱上変圧器から 100 ボルト，200 ボルト，低圧配電線（100 ボルト，200 ボルト），引込線から引込取付点から 100 ボルト，200 ボルトで，家庭・工場・商店に届く。

家庭に送り届けられる電気には，3 本の電線を使って引き込む「単相 3 線式」と 2 本の電線を使って引き込む「単相 2 線式」がある。100 ボルトの電気しか使えない単相 2 線式に比べ，単相 3 線式では 100 ボルト・200 ボルトの両方の電気が使える。



２．家庭の電気設備

電柱から家庭の建物などに取り付けられた引込線までは，中部電力と契約している場合，送配電を行う中部電力パワーグリッドの設備である。引込線と建物側の接続部分である「引込線取付点」が，家庭と中部電力パワーグリッドとの財産および責任の境界となる。引込線は，電気をご家庭に送るための電線である。

電気メーターは，電気の使用量を計るための装置で，適正な計量をおこなうため，法の規定により定期的（一般のご家庭は概ね 10 年に 1 回）に取り替えている。定期的な取り替え工事は無料である。取り替え工事では，10 分程度停電する。

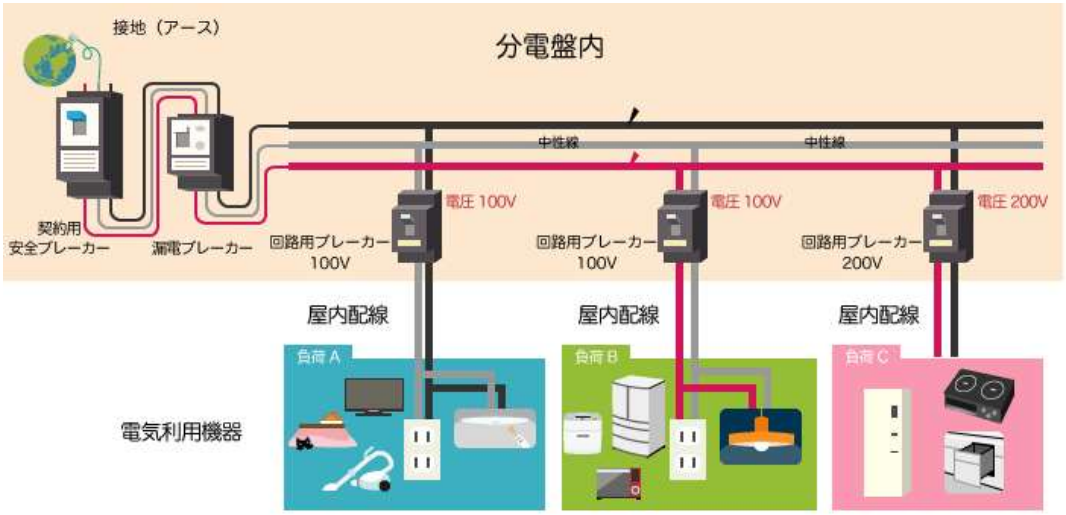
分電盤は，サービスブレーカーや漏電ブレーカーの他，各部屋に分けて送るための分岐スイッチが収められている。

アースは，万が一，漏電した時に，電気を大地に逃す役目をする。

漏電遮断は，回路の屋内配線や電気器具等のわずかな漏電を検出して，回路から切り離し感電事故や火災事故を未然に防止する役割を持つ。電気器具からケースの金属部に漏電した場合でも完全な絶縁物の上にある場合は，大地への漏電は起こらない。湿った床やコンクリート上に置かれている場合は，大地への漏電が起きる。人が触れた場合には，人体を通じても大地に漏電電流が流れ，漏電しゃ断器は動作しやすくなる器具等のケースアースを取り付けている場合は，より大きな漏電電流が流れ，しゃ断器の確実な動作が期待できる。

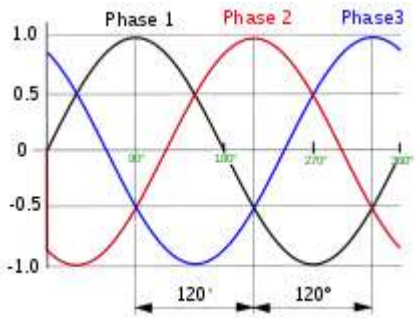
大きな電力を使うＩＨクッキングヒーターやエアコン，衣類乾燥機，食器洗浄器，電子レンジ，電気温水器，電気床暖房等が使用されるようになり，その電源として単相 200V が使われている。ほとんどの家庭では，電柱から一般家庭に引き込まれている電線の多くは３本（単相３線式　単相 3 線式 100/200Ｖ配線）で，200Ｖの電源が来ているので，200Ｖ機器専用コンセント取付等の簡単な工事をするだけで 200Ｖの機器を使うことができる。エコキュートを使用する場合，従来の電力量計から，時間帯別電力量計に取り替える必要があり，これにより時間帯ごとの電力使用量を計量できるようになる。100Ｖと 200Ｖの違いは，仕事をするカが 2 倍違うということで，IH クッキングヒーターやエアコン等大きな電気容量の機器を効率よく働かせることが可能である。アコンの場合，広い部屋の冷房に適しており，立ち上がりが早いので，消費電力の大きい 14 畳用以上のエアコンは 200Ｖ仕様，それ以下は 100Ｖ仕様が一般的である。

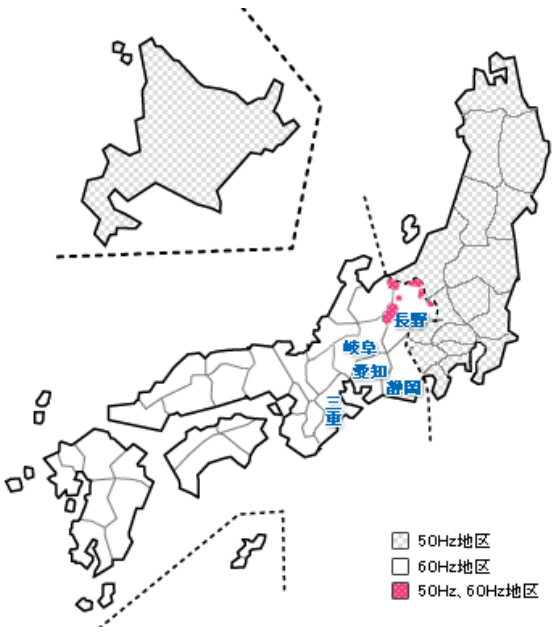
分電盤の回路用ブレーカーから屋内配線により各部屋へ電気を供給する。単相３線式の場合は，３本の線のつなぎ方により１００Ｖと２００Ｖの電気を使うことができる。白線と赤線または黒線を使用すると１００Ｖ，黒線と赤線を利用すると２００Ｖの電圧が利用できる（２００Ｖタイプのクッキングヒーター，食器洗洗浄機，電気温水器など)。



電気はコードの絶縁がはがれてはだかの銅線と銅線が接触するなどの，決められた回路を通らずに近道をすることがあり，これをショートまたは短絡と言う。ショートが起きると，大きな電流が流れ，電線の過熱や発火が発生して，火災を起こすなど非常に危険である。ブレーカーはこのようなショートが発生した場合，ただちに電気を切って，火災などの発生を防止する役目をもっている。

電力会社から家庭に送られる電気は，交流電流である。交流とは，波形のように，電流の大きさが周期的で，時間によって大きさの違う電流である。交流の周波数は，日本では地域によってことなり，50Hz か 60Hz である。





3．コンセント

コンセントは，電圧，接地の有無に多くの種類がある。代表的なコンセントの形状と電圧は下記の通りである。一般家庭で用いられる 100V コンセントのほか，エアコンや IH クッキングヒーター，業務用冷蔵庫のように，大きな電力を必要とする電気機器は 100V コンセントではなく 200V コンセントを使用する。冷蔵庫のように，大きな電力を必要とする電気機器は 100V コンセントではなく 200V コンセントを使用する。コンセントという名称は和製英語であり，海外では「アウトレット」という名称で呼ばれている。電話のモジュラージャックの接続口はコンセントではなく，アウトレットという名称が既に使われているため，コンセントは「電源を取れる差込口」を呼ぶのが一般的である。

単相 100V	一般		
	接地極付		
単相 200V	一般		
	接地極付		
三相 200V	一般		
	接地極付		

コンセントを計画する場合,使い勝手の良い場所に設置するのはもちろん,コンセントの用途を把握し,ブレーカーや配線に適正な電流が流れるよう計画しなければならない。分電盤に設置されているブレーカーは 20 アンペア以上の過負荷電流を遮断する性能を持っている。ドライヤーや電子レンジは 10～12A の電流が流れるので，2 台同時に使うような計画をしてはならない。

住宅用のコンセント高さは，接続する電気機器に応じた高さに設定する。汎用のコンセントは高さ 200mm とするのが原則である。下記は，住宅内に設けるコンセントの標準的な高さ設定である。

- 冷蔵庫：1,900mm
- 電子レンジ：1,200mm

•洗濯機：1,000mm

•エアコン：天井から 200mm

USB 充電用コンセントは，USB 機器の充電が可能なコンセントである。USB の接続端子が設けられており，100V 電源を 5V に変換して，USB からスマートフォンや携帯電話，バッテリーの直接充電が可能である。個人住宅やマンションなど家庭で使うことはほとんどなく，ホテルの宿泊施設，カフェ，空港のラウンジなどで多用されるコンセントである。日本国内とは電圧の違う海外諸国の充電器を持ち込まなくても，持参したスマートフォンが直接充電できるため，大変便利である。一般用の埋め込みコンセントと同じ，連用枠を用いた取付が可能なので，すっきりと仕上げられる。ホテルでは，テレビ台に内蔵させる事例も多くなり，海外からの観光客への配慮が進んでいる。

コンセントの極性と接地

100V用のコンセントは,2つの孔があいている差込口にプラグを差し込んで給電する配線器具である。コンセントに対面して左側の孔が大きく，右側の孔が小さく作られており，国内のコンセントはこの形状が基本である。100V コンセントには「極性」と呼ばれる性質があり，片方は「電気が送られてくる側」，もう片方は「負荷で使われた電気が戻っていく側」としている。直流ではプラスとマイナスを間違えると給電できないが，交流ではどちら方向であっても問題なく使用できてしまうので，あまり意識されることはない。しかし，電気設備分野では，コンセントの極性を基準どおりに計画し施工しなければならない。実情の使い勝手に何ら問題ないとしても，通信機器や音響機器では極性が逆になっていると不具合を起こす可能性がある。機器の不具合だけでなく，コンセントの交換や点検において，極性違い感電事故の原因ともなる。基本的な考え方として，孔が大きい側は「負荷から電源に戻る（白線）」とし，孔が小さい側は「充電されている（黒線）」としなければならない。つなぎ込む電線の識別色も，この原則に基いたカラーとすべきである。

通信機器や音響機器では，コンセントの極性違いによって通信品質が変化したり，音質が変化するといわれる。極性を重視する機器は，プラグ側にも「白線側に接続すること」を示す表示がされており，記載通りの接続をしているのに極性が逆になっているとあれば，大きな問題である。単相 2 線式（白線と黒線で 100V 供給）と呼ばれる回路では，白線側と接地線が接続されて大地とつながっている。大地はノイズの放流先であり，電源回路や通信機器，音響機器に含まれるノイズを効果的に外部へ逃がすには，白線側に正しく接続するのが効果的である。コンセントプラグの差込方向を変えることで，安定動作，品質向上，音質向上といった効果が表れるので，適切な接続になっていることを確認すると良い。白線に接続されている接地線を活用する方法ではなく，専用の接地線を接続できる製品であれば，白線の極性合わせによる効果を求めるよりも，ノイズに汚染されていないアース（接地線）につなぎ込むのが良い。白線は「中性

線」であり，接地線とつながっていても帯電している可能性があり，ノイズ放流先としては不十分である。完全に独立して大地に接続されている「接地線」とは違うため，混同しないよう注意を要する。

コンセントを用いた LAN（PLC）技術

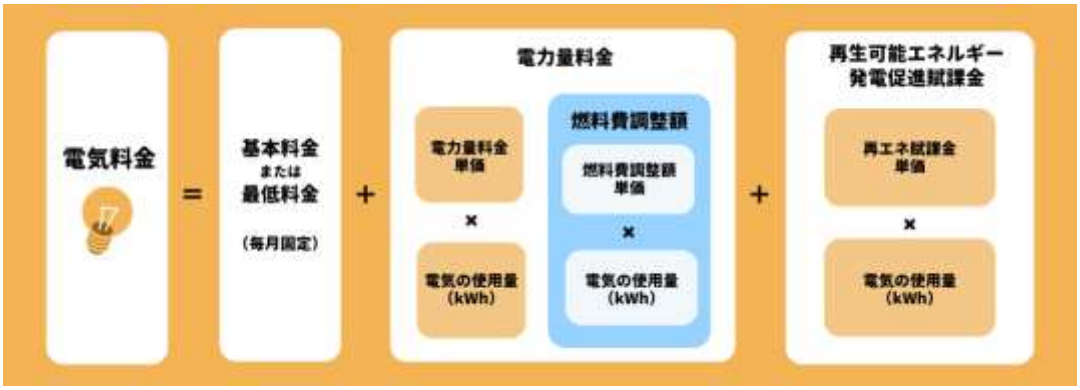
分電盤から張り巡らされているコンセントのケーブルに通信情報を乗せて，構内 LAN を構築する技術を「PLC（Power Line Ccommunication）」または「電力線通信」と呼ぶ。外部と接続されているルーターに対して PLC 親機を接続してコンセントに差し込めば，子機を他の部屋にあるコンセントに差し込むだけで，インターネットに接続が可能である。商用の電源周波数は 50Hz または 60Hz であるが，この電源に 2～28MHz の高周波を重畳させて通信を行う。電源を得るためのコンセントでデータ通信ができるため，通信用の LAN ケーブルを別に使用することなく，配線の省力化を図れる。PLC による通信では，理論上 210Mbps の高速伝送が可能とされており，実用ベースでも 30Mbps 程度の通信速度を得られるので，動画の大容量データ転送も可能である。LAN ケーブルを用いたイーサネット環境では，ギガビットイーサネットが普及しているため，PLC の導入によってさらなる高速化を望むものではないが，室内や廊下に LAN ケーブルを敷設するより，配線まわりをすっきりさせられる利点がある。現在では，無線 LAN の安定化と高速化が進んでおり，無線 LAN であってもギガビット以上の通信環境を構築できる。数本のアンテナを組み合わせて，安定性と通信速度を高める技術も開発されており「無線 LAN は接続が切れやすい」というイメージは過去のものとなる。PLC 構築によるメリットが，あまり感じられない時代ともいえるが，階をまたぐ長距離伝送であれば，無線 LAN よりも PLC の方が高い安定性を見込めることもある。パナソニックが販売している PLC 機器では，配線長 200m 程度までを実用範囲としており，一般家庭用であれば，ケーブル長がネックになることはありえない。

テーブルタップのたこ足配線の危険性

テーブルタップは，コンセントの個数を手軽に増やせる配線器具のひとつで，電源タップや OA タップと呼ばれることもある。パソコンへの電源供給では，パソコン，モニター，スピーカー，プリンターなど，電気容量が小さくても，数多くのコンセント接続口を必要とする。テーブルタップや，パソコンへの電源供給に特化した OA タップが使われる。テーブルタップは手軽にコンセントを増やせるが，供給できる電気容量が増えるわけではない。過剰に電気機器を接続すれば，本来供給できる電気容量を超過してしまい，異常発熱により火災につながる。テーブルタップに対してさらに増設のタップを追加し，沢山の電気機器を接続する行為が，火災の大きな原因として指摘されている。テーブルタップからたこの足のようにコードが出ている様をたこ足配線と呼ぶが，コンセントの危険な使用方法のひとつである。

４．電力料金

1kWh あたりの電気料金は電力会社によって異なる。一般的な電気料金プランは以下のように構成されている。



基本料金は，電気の使用量の大きさにかかわらず，毎月固定でかかる料金である。ただし，全く電気を使わなかった場合に，基本料金をいくらか割り引く電力会社もある。基本料金の決められ方は大きく分けてふたつあります。契約するアンペア容量の大きさによって料金が決められている場合（アンペア制）と，アンペア容量に関係なく一律の料金が決められている場合（最低料金制）である。基本的には，地域によってアンペア制か最低料金制かが分かれている。

アンペア制	北海道エリア，東北エリア，関東エリア，中部エリア，北陸エリア，九州エリア
最低料金制	関西エリア，中国エリア，四国エリア，沖縄エリア

アンペア制の場合，以下の東京電力の例のように，契約アンペアの大きさに比例して基本料金は高くなる。(2024/02 現在)

東京電力・従量電灯Ｂ：基本料金	
契約アンペア数	基本料金（円・税込）
10A	311.75 円
15A	467.63 円
20A	623.50 円
30A	935.25 円
40A	1247.00 円
50A	1558.75 円
60A	1870.50 円

電力量料金は，電力消費量（kWh）に応じてかかる料金/である。電力消費量（kWh）の合計に電力量料金単価（円/kWh，つまり 1kWh あたりの電気料金）をかけて計算されている。大手電力会社よりも新電力の方がこの電力量料金単価を安く設定している傾向がある。多くの電力会社において電力量料金単価が三段階で設定されている。

例：東京電力・従量電灯 B の電力量料金単価（1kWh あたりの電気料金）

電力消費量（kWh）	1kWh あたりの値段（円・税込）
120kWh まで	29.80 円
120kWh を超えて 300kWh まで	36.40 円
300kWh 以上	40.49 円

燃料費調整額は，電気の調達にかかるコストの増減を電気代に反映させるための料金で，電力量料金に含まれている。燃料費調整額も 1kWh あたりの単価が決まっていて，ひと月の電力消費量（kWh）によって総額が決まる。燃料費調整額の単価は，電気の調達コストの増減に応じて毎月変化する。たとえば，火力発電に必要な燃料（LNG 等）の輸入価格が上がれば，電気の調達コストも高くなるので単価が高くなり，逆に下がれば単価も低くなる。コストが安いときは単価がマイナスになることもある。

燃料費調整額の単価は，各電力会社が自由に決められる。これまでほとんどの新電力は同じエリア内にある大手電力会社の規制料金プランと同じ算定基準を採用して，同じ燃料費調整額を請求していた。これは，電気料金プランの比較を簡単にするため（＝基本料金と電力量料金だけ比べればどちらが安いかすぐわかるようにするため）という意図からである。しかし，ウクライナ危機に伴う燃料価格の高騰以来，燃料費調整額の単価は同じエリアの中でも多様化している。そのため，電気料金プランの比較をする際には，燃料費調整額も忘れずに確認することが重要となっている。

再生可能エネルギー発電促進賦課金は，日本における再生可能エネルギーの割合を増やすために国民が負担している税金である。再エネ賦課金も，電力使用量 1kWh あたりで単価が決まっている。この単価は国によって決定され，1 年間同じ金額が適用される（5 月～翌年 4 月）。再エネ賦課金の単価は全国どの電力会社でも同じである。ここ数年，再エネ賦課金の単価は上昇が続いている。

再エネ賦課金・過去５年の推移

2023 年度	2022 年度	2021 年度	2020 年度	2019 年度	2018 年度
1.40 円	3.45 円	3.36 円	2.98 円	2.95 円	2.90 円

５．電流と電圧

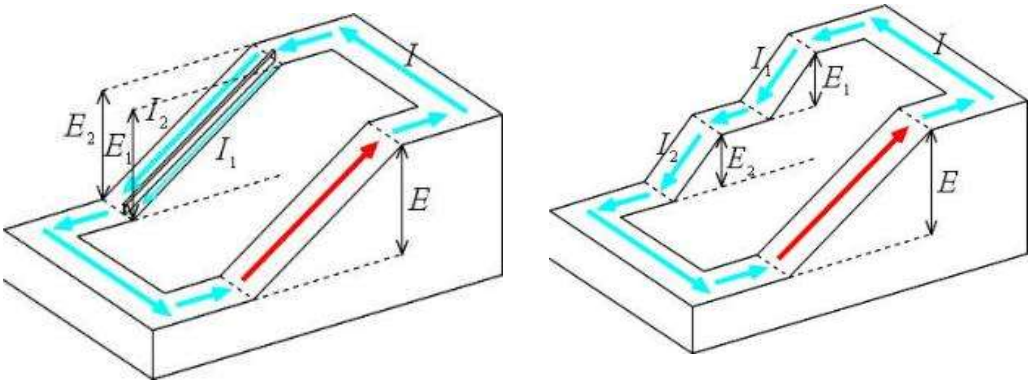
電流は，電子の流れのこと。電子の電荷がマイナスなので，電流の向きは，電子の動きの向きとは，反対の向きになる。電流の単位は，アンペアといい，単位の記号は A であらわす。物理学者のアンペールの名にもとづいている。電圧は，電流を流そうとするエネルギーのようなもの。電圧の単位はボルトといい，記号は V であらわす。

電流 I[アンペア]×電圧 V[ボルト]＝電力 VI［ワット］

電子の電荷の大きさ q[クーロン] ×電圧 V[ボルト]＝qV［ジュール］

電子の静電気力による位置エネルギー

電圧は単位電荷の１クーロンあたりの静電気力による位置エネルギーとも考えられる



電気製品には，安全のため，流しても良い限度の電流の強さや，加えても良い限度の電圧の大きさが規定されている。定格電流・定格電圧は，最大限の強さの電流や最大限大きさの電圧である。

定格電流：流しても良い限度の電流のうちの，最大限の大きさ

定格電圧：加えても良い限度の電圧のうちの，最大限の大きさ

事故による危険度が高いとされる品目の電気用品は，特定電気用品とされ，安全性の確認された電気用品には，電気用品安全法に基づき PSE マークが付けられる。

PSE マークには２種類あり，特定電気用品と，特定電気用品以外の電気用品がある。

（PS は Product Safety，E は Electrical Appliance & Materials の略）

電気用品に該当する製品の製造又は輸入を行う事業者は，経済産業大臣に事業の開始の届け出を行うほか，技術基準適合義務等のいくつかの義務を負い，これら義務を果たした事業者が自ら法に基づく手続きを行った証として，次の表示ができる。法に基づく表示がなされていない電気用品は販売できないなどの制限がある。

特定電気用品	特定電気用品以外の電気用品
 ・電気温水器 ・電熱式・電動式おもちゃ ・電気ポンプ ・電気マッサージ器 ・自動販売機 ・直流電流装置 など全１１６品目	 ・電気こたつ ・電気がま ・電気冷蔵庫 ・電気歯ブラシ ・電気かみそり ・白熱電灯器具 ・電気スタンド ・テレビジョン受信機 ・音響機器 ・リチウムイオン蓄電池など全３４１品目

電気用品安全法(2001 年)

電気用品安全法を補完し，電気製品の安全のための第三者認証制度で，Ｓマーク付電気製品は第三者認証機関によって製品試験及び工場の品質管理の調査が行われる。認証製品には，マークと，製品を認証した機関のロゴマークと組み合わせて表示される。

 S-JET マーク （認証機関:一般財団法人 電気安全環境研究所）	 S-JQA マーク （認証機関：一般財団法人 日本品質保証機構）
 S-UL Japan マーク （認証機関：株式会社 UL Japan）	 S-TÜV Rheinland マーク （認証機関：テュフ・ラインランド・ジャパン株式会社）

例題１　家庭用テーブルタップの主流の仕様は,電圧 125V まで,電流 15A まで,最大定格容量は 1500W までとなっている。定格値が，電圧 125V，電流 15A のテーブルタップに，消費電力が 1500W のホットカーペットと 1300W のアイロンをつなぐとなぜ危ないのか?

例題２　デスクトップ PC とプリンタをセットにして購入した。このデスクトップ PC とプリンタには次の表記があった。

定格：安定してその出力を保てるワット数

最大：その電源ユニットの限界のワット数

(最大は，最大定格出力やピーク値など書かれている事もある)

定格値が，電圧 125V，電流 15A のテーブルタップに，このデスクトップ PC とプリンタのセットを何セットまでつなぐことができるか?

デスクトップPC本体 130W

プリンタ本体 0.6A＝60W

(答 1)　1500W+1300W=2800W　なので　2800W÷100V=28A　の電流が流れ，テーブルタップが加熱して危険

(答 2)　デスクトップ PC とプリンタの 1 セットは　130W+60W=190W

テーブルタップの 最大定格容量は 1500W なので　1500W÷190W =7.8947・・

7 セット　　190W×7＝1330W　までつなぐことができる

課　題

1．家庭の電気設備の仕組みを説明しなさい。

第６講　電気工具と部品

【学修到達目標】

⋕電気工具の種類と使い方を理解できる。

⋕電気部品，電子部品の仕組みについて理解できる。

１．工具

電気系の資格は，電気を取り扱う設備を対象に，設備を工事したり管理したりするために必要である。電気系の資格，電気系と相性の良い資格は以下のものである。

・電気工事士

・電気主任技術者（電験）

・工事担任者

・電気工事施工管理技士

・電気通信工事施工管理技士

・消防設備士

電気工事法で定められた，無資格でもできる工事範囲は以下のものである。

・電圧 600V 以下で使用する差込み接続器などにケーブルを接続する工事

・電圧 600V 以下で使用する電力量計や電流制限器などを取り付ける工事

・電圧 600V 以下で使用する電気機器をねじ止めする工事

・インターホンや豆電球などに使用する小型変圧器の配線工事

・電柱や腕木の設置・変更にかかわる工事

家庭内の電気製品では，照明器具のソケット式の電球交換，コンセントに照明器具の線を繋げる，テレビのアンテナの配線，LAN ケーブルの接続などは，無資格でもできる。しかし，コンセントや配線の設置など，壁の中にまでかかわる工事は資格がないとできない。無資格でもできる工事には，専用の工具を利用すると便利である。

リード線の被覆を切り外して芯線を出すには，ワイヤーストリッパや穴あきニッパなどを用いて被覆を切り外す。ワイヤーストリッパ（wire stripper）とは，リード線の被覆を切って芯線を出すための工具である。 使い方は，ワイヤーストリッパにはリード線の径ごとの穴が何種類かあるので，径にあった穴で被覆を切る。このとき，芯線まで切らないように注意して用いる。

ニッパは，通信工事の細線や銅線の切断に利用する。

電気工事や針金の切断，金属板の折り曲げなどに使うのがラジオペンチとペンチである。

ドライバーは，ねじを締め付けたり緩めたりする際に使う工具である。装置や基盤についている，時計，カメラ，眼鏡などに使用される精密小ネジを締付ける工具が精密ドライバーである。

電動ドライバーは，ねじを締め付けたり緩めたりする際に使う工具である。モーターの力で先端を回転させるタイプのものを電動ドライバーと呼ぶ。ドリルドライバー，インパクトドライバー，振動ドリル，ハンマードリルなどがあり，ドリルとつくものは先端にドリルを取り付けることで穴あけ作業をすることが可能な工具である。

レンチは，ナットや六角ボルトを締め付けたり取り外す際に用いる工具である。スパナとは異なり，レンチはリング状で締め付ける際の接地面が多い。スパナは 2 箇所の接地面で締め付けを行う。レンチはボルトやナットをホールド（包み込む）する形状をしているが，スパナは接地面が 2 箇所なためハサミのような形状である。締め付けや取り外し作業をする際にはレンチを使用し，スパナは狭い箇所で使うことが多い。

メガネレンチ: 両サイドにある，ナットを包み込むような丸型リングの形状をしている。直線のストレートタイプや角度の付いたオフセットタイプもある。

モンキーレンチ: 一見するとスパナのような形をしている。口開きの幅を調整できるため，合わない形状でも自由にサイズ調整ができる。

はんだごては，はんだ付けで，はんだおよび接合部分を加熱するために用いる工具である。

やすりは，おもに金属の研削を行う手動工具である。金属や木材の表面を平らに削ったり，角を落としたりする際に使用される。

カッターは，ケーブルの被膜をはがすときなどに利用する。

２．電気部品と電子部品

電気部品と電子部品は，電気機器と電子機器を構成する要素である。電気部品は， 電気で動く機器の部品を指している。電子部品は，電子の流れを制御して信号制御を行う機器の部品である。

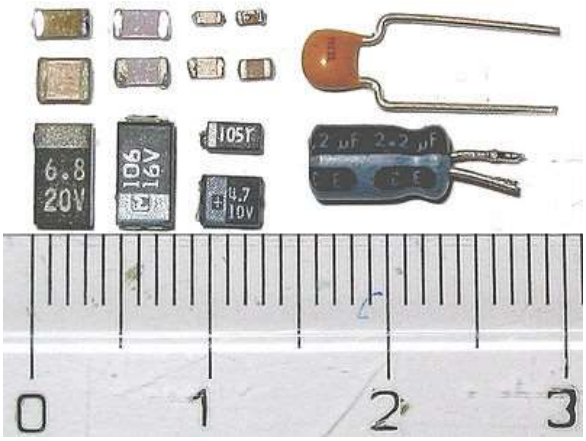
電子部品には，次のものがある。

抵抗は，電気エネルギーを単純に消費する素子である。

回路図記号は

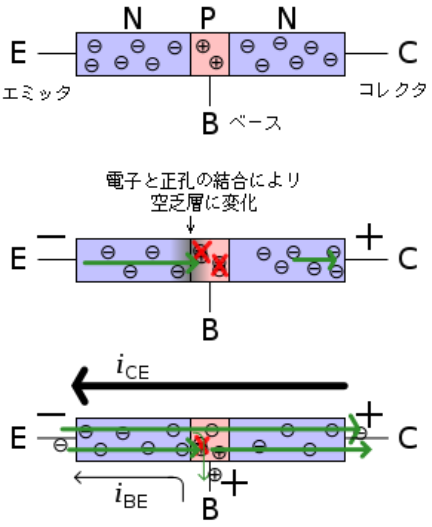
国際規格の IEC 60617 を元に作成された JIS C 0617（1997-1999 年制定）の図記号

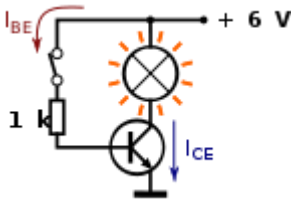
コンデンサは，電気・電子回路で多く使用される受動素子の一つで，枚の金属板を絶縁体で挟み込んで構成されている。電荷を蓄える特性を持ち，直流は通さないが，交流は通す特性がある。交流の周波数が高いほど通しやすい。基本的な使われ方として，放電回路では，蓄えた電荷を必要な時に放電するために使用される（カメラのストロボなど）。平滑回路では，交流電源から直流電源に変換した際の脈流を滑らかにするために使用さる。カップリング・デカップリング回路では，直流成分のカットやノイズの除去に使用される。同調回路では，特定の電波の周波数を算出するために使用される。



NPN 型トランジスタは，半導体に，いくつかの物質をまぜると，一方向にしか電子が流れないという現象が発見された。トランジスタは，電極の端子が 3 つあり，それぞれエミッタ（emitter），ベース（base），コレクタ（collector）である。ベースに電圧が加わらないと，トランジスタのエミッタ-コレクタ間には電流が流れない

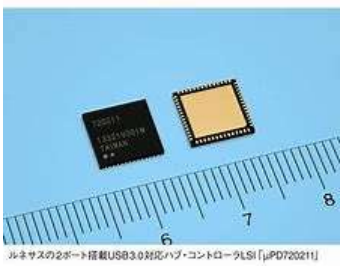
スイッチング作用の例として，トランジスタでは，ベース電圧により，エミッタ-コレクタ間の電流のオン・オフを切り替えられ，この仕組みをトランジスタの スイッチング作用（switching）と言う。





IC は，集積回路とも言われ，数 mm のチップに，電子素子をつめこんだ部品である。コンピュータ部品に IC が使われる。パソコンだけでなく，デジタル家電などの製品のほとんどに IC は入っている

IC（集積回路）と LSI（大規模集積回路）は，電子機器において重要な役割を果たす半導体デバイスである。IC（集積回路）は「Integrated Circuit」の略で，半導体素子を 1 つの基板に集積した超小型回路を指す。トランジスタやダイオードなどの素子を含むものがある。電子回路素子を多数組み込んだもので，密度が高く，小型化されている。メモリやマイクロプロセッサ（CPU），ロジック IC などが代表的なものである。LSI（大規模集積回路）は「Large Scale Integrated」の略で，IC をさらに大規模化したものを指す。1 つの基板に 1000 以上の素子を実装している。IC よりもさらに回路素子の集積度が高く，大規模な機能を持つ集積回路である。両者は技術の進歩により複雑化し，現在では特に区別せずに集積回路全般を IC または LSI と呼称することが一般的である。

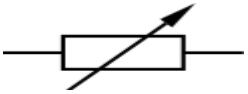


ルネサスの2ポート搭載USB3.0対応ハブ・コントローラLSI「μPD720211」

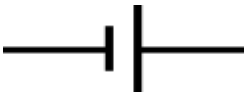
図記号

固定抵抗器

可変抵抗器

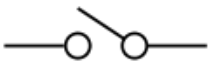


電池，直流電源
（長い方が正極）

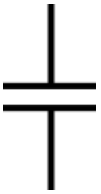


交流電源

スイッチ

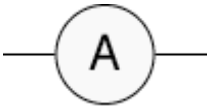


コンデンサ

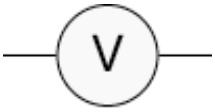


コイル

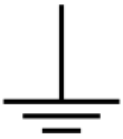
電流計



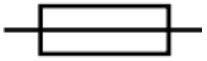
電圧計



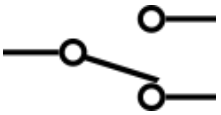
接地



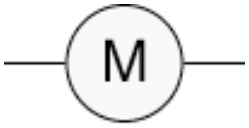
ヒューズ（fuse）



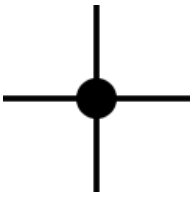
３極スイッチ



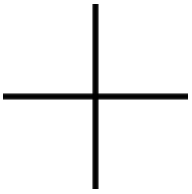
モータ



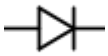
接続している交点



配線が接続せず，十字状に重なっているだけの場合

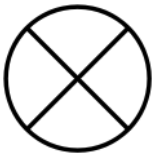


ダイオード



発光ダイオード

電球

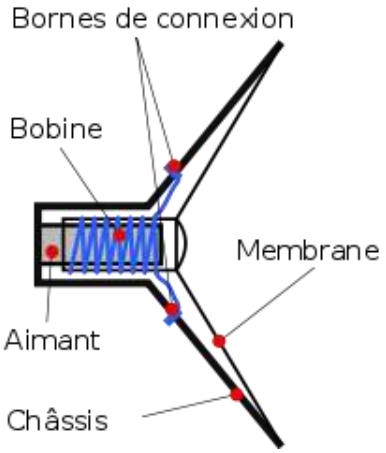


電気部品は， 電気で動く機器の部品であり，次のものがある。

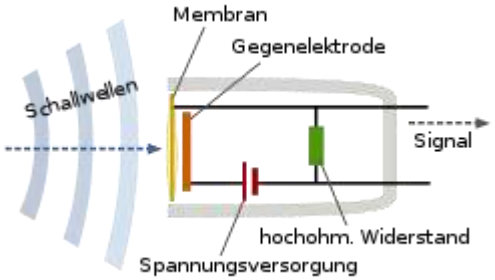
スピーカーはスピーカー内のコーン紙を振動させることで，空気を振動させている。

電磁石の可動コイルを利用して，電流の大きさを磁力の大きさに変え，その力の変化によって可動コイルが動くが，可動コイルとコーン紙とが一体で連動する構造なので，そのコーン紙が振動して，音を出している。

スピーカーは，電気を音に変換している。

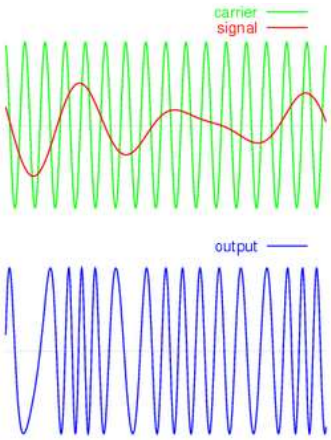


マイクロホンの仕組みは，振動板の動きを電気回路に連動させ，それによってコイルやコンデンサの抵抗が変わるので，電流の流れ方も変わり，結果として回路の共振周波数が変わることを利用している。マイクロホンは，このようにして，音を電気に変換している。



テレビや FM ラジオは，FM 電波を利用している。

電圧の大きさを周波数に変換する FM 変調の原理は，コイルとコンデンサの LC 共振回路に，コンデンサと並列にダイオードを合わせることで，ダイオードは電圧が順方向の時にしか電流が流れないから，結果としてダイオードが順方向電圧で導通している時と逆電圧で非導通との時とで，合成抵抗が変わることになる。この結果，電圧の大きさによって回路の合成抵抗が変わることになるので，その結果，共振周波数が変わることを利用している。



FM 変調の各波形

上 carrier：変調前の搬送波

上 signal：変調に用いる信号波

下：送信波

電子部品には様々な分類法があり，ひとつの分類法は素子と呼ばれる単機能の部品群と「その他の機構部品」などに大分類し， 素子を，さらに非線形や増幅などの動作をする素子である能動素子，および，そうした動作をしない受動素子に下位分類する方法である。

素子

能動素子（ダイオードやトランジスタなど）

受動素子（「LCR」などと呼ばれる，インダクタンスや静電容量や電気抵抗を発生させる素子）

その他の機構部品

次のような用語で分類する方法もある。

能動部品

能動素子単体および能動素子を組み合わせた部品（トランジスタ，IC，ダイオード，オペアンプなど）

受動部品

抵抗，コイル，コンデンサなど。

補助部品

素子（間）を接続/切断したり，固定するための部品（リレー，スイッチ，コネクタ，基板，端子，線材など）。

課　題

１．電気部品，電子部品の仕組みについて説明しなさい。

第７講　電気製品と安全

【学修到達目標】

⋕家庭内の電気製品の特長を理解できる。

⋕家庭内の電気製品を安全に使用することができる。

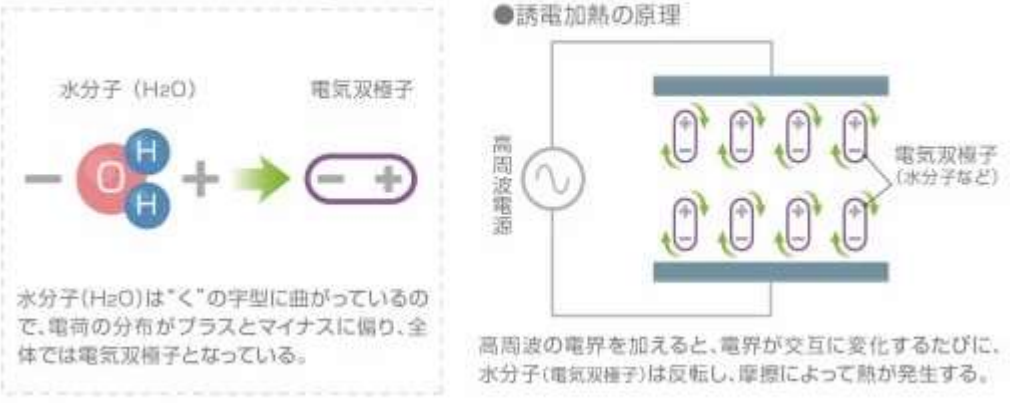
１．加熱器具(電子レンジ)

家庭の電気製品は，私たちの日常生活に欠かせないもので，さまざまな目的で使用されている。家庭で使う電気製品は，正しく使用することで安全に利用できる。安全に利用するための注意点は，「電源コードと電源プラグは正しく使う」「テレビ，冷蔵庫，電子レンジなどは地震等に備えて転倒防止対策をする」「家電製品を分解したり修理したりしない」「濡れた手で電気器具を触らない」「ヒーター応用製品は火災や火傷の原因になるので気を付けて使う」などがある。

電子レンジは,日本の家庭ではほぼ100%の普及率を誇る調理器具で,食品を加熱する際に利用される。高周波電界を利用して食品を加熱するため，金属を含む食品を加熱すると事故につながることがあり，安全に使うためには適切な知識と注意が必要である。

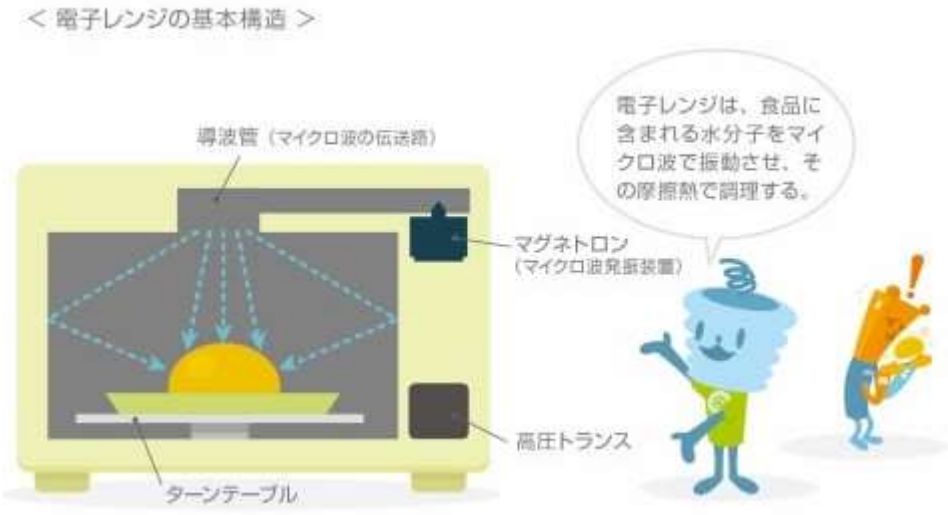
電子レンジは高周波電界を利用して誘電加熱と呼ばれる方式で食品を加熱する。物体の温度は構成する粒子（分子や原子など）の振動の度合によって決まる。加熱によって温度が高まるのは，粒子の振動がより激しくなるからである。電子レンジ(microwave oven)は,食品に含まれる水分子をマイクロ波(2.4GHz)

＜電子レンジの加熱原理（誘電加熱）＞



で振動させることで加熱する。H_2O は，酸素原子 O を中心に，“く”の字型に折れ曲がった構造をしている。このため分子全体の電荷分布は，わずかながらプラスとマイナスに偏った電気双極子となっている。この水分子に高周波の電界を加えると，電界の反転に応じて電気双極子である水分子も回転・振動し，互いに摩擦しあって熱を発生する。これが電子レンジの誘電加熱である。

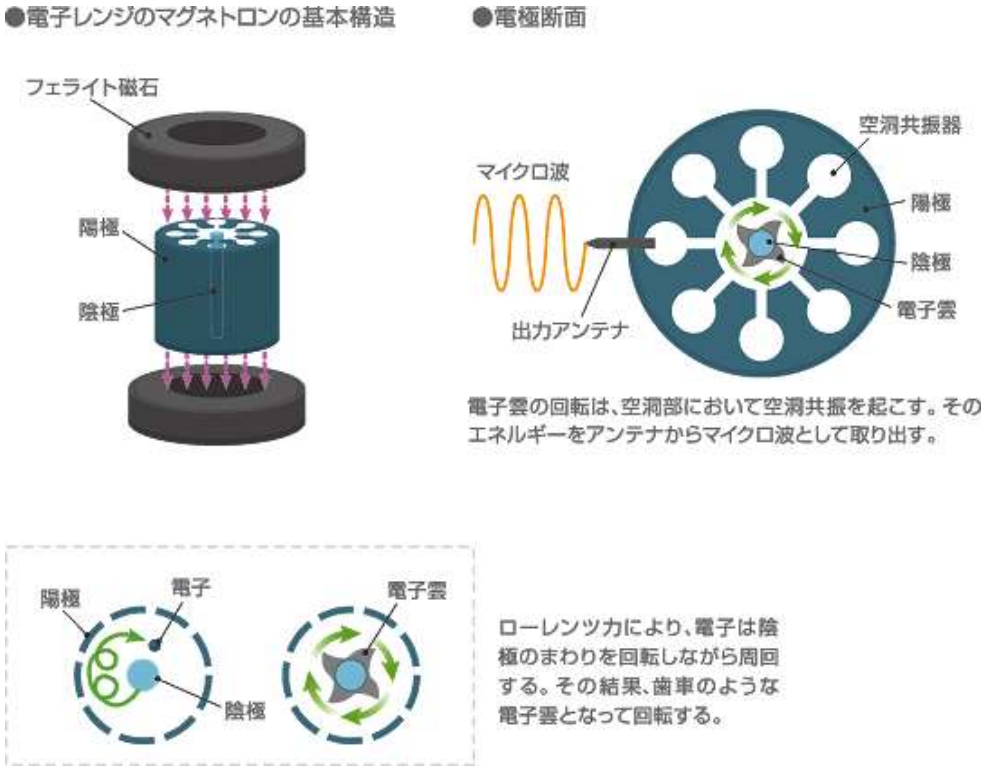
電子レンジの内部がステンレスなどの金属で覆われているのは，電波をよく反射させるためと，電波漏れを防止するシールドが目的である。電波漏れを起こすと無線 LAN（IEEE802.11b/g 製品）の電波と干渉する場合もある。電子レンジを使うたびに無線 LAN が切断したり，通信速度が遅くなるといった症状が出たら，電子レンジの不具合が原因の場合がある。



電子レンジは食品に含まれる水分子をマイクロ波で振動させて加熱するため，水分をほとんど含まないような根菜類や乾物を加熱する時には，発火する可能性があるので十分注意が必要である。殻がある卵や栗，膜があるたらこやウインナーも注意が必要である。マイクロ波により内部の水分が膨張して殻や膜に圧力がかかり，破裂する恐れがある。卵は割りほぐし，たらこやウインナーは膜に切り目を入れて，水蒸気の逃げ道を確保した状態で加熱する。また，飲み物やカレー，スープなどの液体を加熱する時にも注意が必要である。これらを加熱しすぎると，突沸現象が生じることがある。通常液体は沸点に達すると沸騰しますが，液体の成分や加熱条件によっては沸点に達しても沸騰しない場合がある(過加熱状態)。突沸とは，過加熱状態の液体に振動などの刺激が加わると，突然爆発するように激しく沸騰する現象である。適切な温め時間と出力に設定して，突沸現象が生じないように十分注意する。

食品中の水分子を振動させて加熱する電子レンジは，レーダ技術から偶然生まれた発明品である。レーダは 1930 年代のイギリスで開発され，第 2 次世界大戦時のアメリカで進歩を遂げた。電子レンジが発明されたのは大戦直後の 1946 年。レーダメーカーの技術者がレーダ電波を浴びたとき，ポケットに入れて

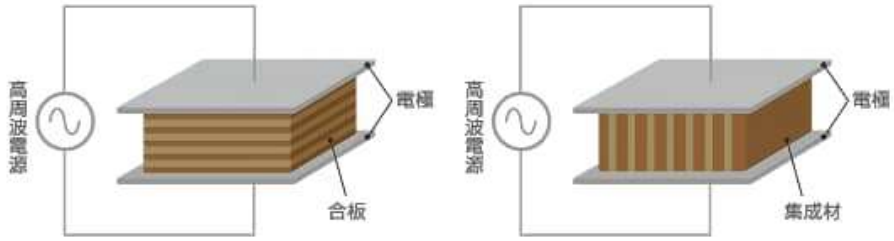
いた菓子が溶けたことからヒントを得たといわれる。レーダ技術のそもそもの始まりは，無線通信に影響を与える電離層の研究である。空に向けて電波を放って反射波の観測を続けているうちに，やがて航空機も電波を反射することがわかり，第 2 次世界大戦中には飛来する敵機の探知用に対空レーダが研究されるようになった。航空機の探知には，より波長の短い電波が必要とされ，マイクロ波（およそ波長 1～10cm）を発振するマグネトロンが開発された。マグネトロンは磁石による磁界を加えた特殊な二極真空管である。磁界中を運動する電子にはローレンツカが作用して，電子の軌道は曲げられる。そこで，二極真空管の電極構造を工夫して外部から磁界を加えると，陰極から放出された電子は陽極に届かず，陰極のまわりを回転運動をしながら周回するようになる。この振動を陽極側に設けた空洞で共振させ，アンテナからそのエネルギーを電波として取り出すのがマグネトロンである。初のマグネトロンはアメリカのハルによって考案され（1916 年），分割型陽極というアイデアでマイクロ波発振の道を開いたのは岡部金治郎である（1927 年）。



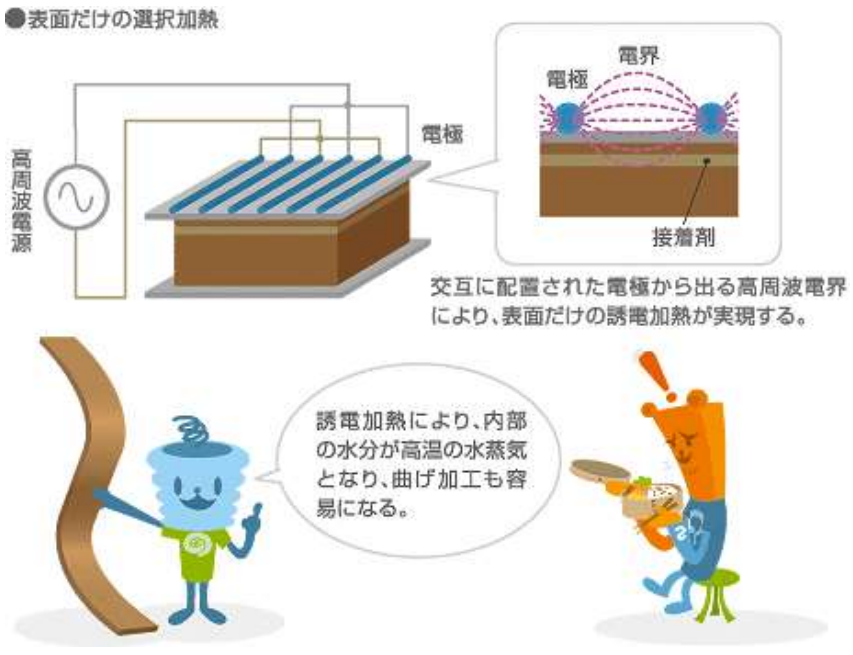
世界初の電子レンジは 1947 年にアメリカで販売された。当初は高価なうえ大型の装置であったため，一部のレストランなどで使われるだけであった。電子レンジの普及に貢献したのは，マグネトロンの小型化と低価格化である。これは主に日本メーカーの技術によるもので，アルニコ磁石にかわるフェライト磁石の採用も低価格化に大きく寄与し，1970 年代に急速に普及するようになった。誘電加熱の利用は電子

レンジだけではない。電子レンジの普及以前から，高周波を利用した誘電加熱は木材の乾燥や接着など，工業分野で活用されてきた。太い角材の乾燥も，減圧下の誘電加熱により，きわめて短時間ですむ。また，厚い特殊合板などは接着剤を塗布して貼りあわせてから，平行電極の間に置き，電極からの高周波電界により加熱・接着される。木製の食卓テーブルなどには，細長い角材･板材をつなぎ合わせた集成材が使われているが，この集成材の接着にも誘電加熱が用いられている。電極の配置により，ある部分だけを選択加熱することも可能で，すだれ状の金属棒の交互を高周波の電極とすると，表面だけを加熱することができる。

木材加工への誘電加熱の応用

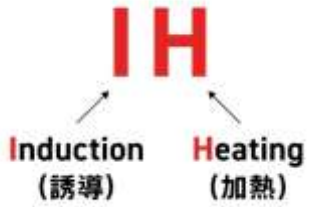


平行電極の間に合板や集成材を置き、高周波電界により接着剤を誘電加熱する。接着時間は著しく短縮する。



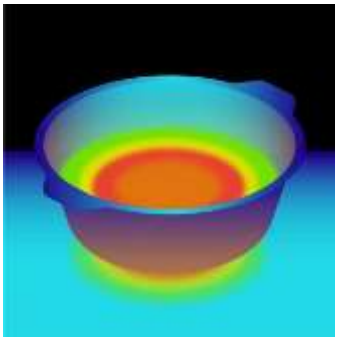
2. 加熱器具(IH)

IH とは「インダクションヒーティング（Induction Heating)」の略称で，電磁誘導加熱と訳される。これは，電気によって磁力線（磁場）を発生させ，IH のガラス製トッププレート上に置かれた鍋やフライパンなどの調理器具を発熱させる，という IH の仕組みを意味する名称である。トッププレートと呼ばれるツルツルとした結晶化ガラスの下に，コイルが仕込まれている。このコイルに電気を流すことで，調理器具が発熱する仕組みとなっている。



トッププレートの下のコイルに電気を流すと，コイルから磁力線（磁場）が発生する。この磁力線はトッププレートを介して，上に置かれた鍋やフライパンなどの調理器具の底面に当たる。このときに調理器具の底面で生まれるのが渦電流である。渦電流が発生すると鍋の底に電気が流れ，鍋の素材「鉄」の抵抗で発熱する。

IH 自体は発熱しておらず，トッププレートに置かれた鍋やフライパンの底面部を中心に発熱していることがわかる。調理器具の底面の電気抵抗によって発熱するため，IH の電源が入っていても，トッププレートに鍋やフライパンなどが置かれていなければ発熱しない。また，調理器具の底面部が発熱するため，鍋やフライパンの取手や持ち手も熱くなりにくいという特徴も，IH の仕組みならではと言える。



IH で使える調理器具は次のものである。

鉄・ホーロー

◎平らでトッププレートに密着するもの
◎左右IHは底径12～26cm、
後ろIHは底径12～18cm（目安）

【材質】鉄・ホーロー

鉄やホーローなど，磁石がくっつく材質でできた鍋やフライパン，やかんなどの調理器具は，基本的にどの IH でも使うことができる。一方で，ステンレス（磁石がくっつかないもの）や銅・アルミの調理器具は一般的な IH では使用できない。しかし，オールメタル対応の IH では使用可能である。

【底の形】平らでトッププレートに密着するもの

IH は，トッププレートを通して鍋やフライパンの底面自体が発熱する。そのため，底面が平らで，トッププレートに密着する調理器具である必要がある。

【大きさ】左右 IH は底径 12～26cm，後ろ IH は底径 12～18cm（目安）

調理器具の大きさは，トッププレートに密着する底面の直径から判断する。それぞれの IH の規格にもよるが，加熱スペースが 3 つある IH の場合，左右の IH は底径 12～26cm，後ろの IH は底径 12～18cm がひとつの目安となる。

調理器具の大きさを気にしたほうがいいのは，自動調理機能を使うときである。最近の IH では，揚げ物を作るときに「180℃に設定する」など，火加減を自動でコントロールしてくれる便利な機能が搭載されている。このような機能を使用する際には，調理器具の温度を調べるセンサーも併用しているため，調理器具が大きすぎたり小さすぎたりすると，正しく温度を感知できない可能性がある。自動調理機能を使う場合には，説明書に明記されている大きさの調理器具を使う。

IH で使えない調理器具の特徴

IH で使えない調理器具の特徴は次のとおりである。

土鍋・耐熱ガラス・陶磁器（セラミックス）

◎底面がトッププレートに密着しないもの
◎左右IH・後ろIHともに底径11cm以下
（熱効率が下がる可能性あり）

【材質】土鍋・耐熱ガラス・陶磁器（セラミックス）

土鍋や耐熱ガラス，陶磁器（セラミックス）は，磁力と金属による電気抵抗が起こらない材質のため，IH で使用することはできない（ただし，IH に対応した土鍋などは除きま

す)。

【底の形】底面がトッププレートに密着しないもの

底面に反りがある鍋や脚が付いているタイプ，底が丸いものなど，底面がトッププレートに密着しないものや，トッププレートと接触する面積が小さいものは，IH の仕組み上，うまく発熱できないため，使用することができない。また，もし発熱できても，トッププレートと調理器具の底面が密着しない場合，温度を検知するセンサーが正常に働かず，自動調理機能が使えなかったり，安全機能が正常に作動しなかったりする場合がある。

【大きさ】左右 IH・後ろ IH ともに底径 11cm 以下（熱効率が下がる可能性あり）

左右 IH，後ろ IH いずれも，底径 11cm 以下の小さい鍋やフライパンは，底面から上手く熱が伝わりにくく，熱効率が下がる可能性がある。

一般的に販売されている調理器具の場合，「IH 対応」か「オールメタル対応」かが，表記されていることがほとんどである。そのため，調理器具選びで悩んだときは，お使いの IH の種類や調理器具の性能を確認し，どのような調理器具が使えるのか，あるいは IH に対応しているかを確認する。

従来の IH では，アルミ製の調理器具は電気抵抗が小さいため使用できなかった。しかし，「オールメタル対応」という，アルミにも対応できる IH も登場している。

IH 対応の土鍋も登場しており，たとえば，通常の土鍋は IH で使用できないが，底面に鉄製プレートが付いていたり，鉄をはめ込んであったりする IH 対応の土鍋は使用できる。

ガスコンロに比べて IH は，次のメリットがある。

①正確に火力調整できる

IH の火力や温度は，コイルに流す電力量によって調整できる。電子制御となるため，IH の操作パネル上では「1～10（1 はとろ火，2～3 は弱火，4～6 は中火，7～10 は強火)」など，数字を目安にきめ細やかに火力調整できるようになっているのが一般的である。温度センサーを内蔵しているので，一定以上の温度にならないような調整なども可能である。さらに自動調理機能で，はじめは強火，10 分したら中火で 30 分，1 時間とろ火にするなど，火力と加熱時間を自動でコントロールできる場合もある。一方，ガスコンロは，ガスの量や火加減を目で確認しながら，手動で調整するタイプが多い。揚げ物などを作るとき，ガスコンロはこまめな火力の調整が必要であるが，IH なら正確かつ手軽にコントロールできる。

②効率よく加熱調理できる

周辺の空気を熱して加熱するガスコンロと比べて，熱効率に優れている。IH は鍋底自体が発熱する仕組みのため,無駄なエネルギー消費をすることなく食材に熱が伝わる。IH の熱効率は約 90%と非常に高く，電気エネルギーのほとんどを熱エネルギーにして調理に生かすことができる。

③便利な自動調理機能・アシスト機能が付いている

IH には多彩な自動調理機能や火加減のアシスト機能が備わっていることが多い。揚げ物のときに揚げ油の温度を自動で一定に保ってくれるように火加減を自動でコントロールしてくれたり，ホットケーキを何枚焼いても同じ焦げ色に仕上げてくれたり，ハンバーグや餃子などに最適な火加減に調整してくれたりする。また，グリルも進化して IH タイプも登場しています。従来のグリルは電熱線ですが，最新型ではより細かな火力の調整が可能である。

④火災などのリスクが低い

ガスコンロと異なり，火やガスを使わない IH は，衣服への着火や周辺への火の燃え移りなどの火災リスクが低く，一酸化炭素中毒の心配もないなど，比較的安全性が高いと言える。

⑤光熱費を抑えられる

IH は熱効率に優れるため，ランニングコストも抑えられる。効率よく調理することで省エネにつながり，光熱費の節約が期待できる。

⑥夏場の調理も快適

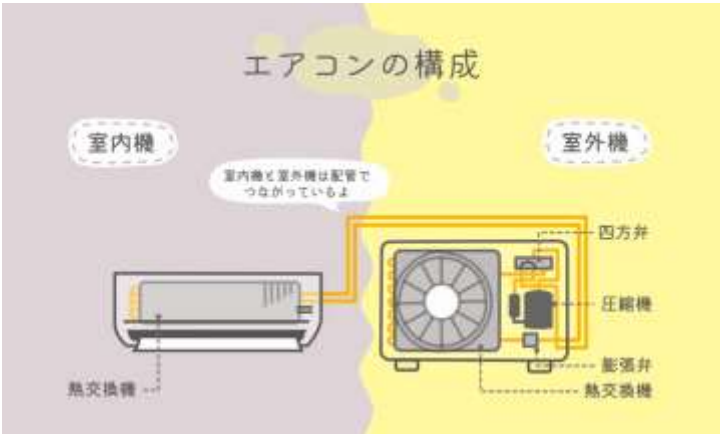
火を使うガスコンロの場合，夏場は熱気で調理に苦労するということも珍しくない。その点，IH は火を使わないため発生する熱も少なく，夏場も快適にキッチンに立つことができる。冷房の設定温度も下げずに済めば，省エネ効果も期待できる。また，火を使わないため扇風機を使用しても安心である。

⑦手入れがしやすい

IH は，凹凸が多いガスコンロとは異なり，天板もグリルもフラットな構造です。お手入れは布巾などでさっと拭くだけのため，毎日の掃除も非常に簡単である。また，火を使わない IH は燃焼に伴う水蒸気が発生しないという特徴もあめる。ガスコンロを使用するキッチンよりも結露やカビが生じにくく，衛生的に使用できる。燃焼ガスによる上昇気流がなく，油も飛び散りにくいため，換気扇や壁も汚れにくい。

3. 冷暖房

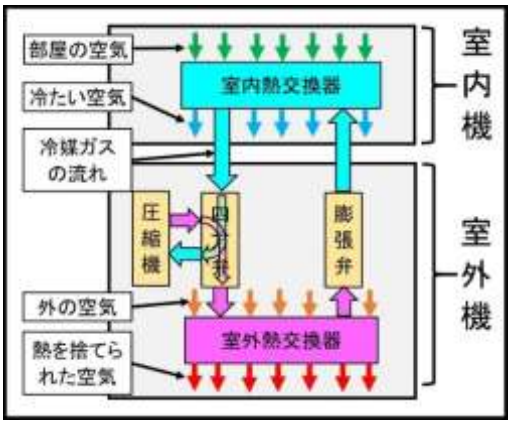
エアコンは，室内機と，室外機で構成されている。圧縮機は，エアコンの心臓部。冷媒を循環させたり，冷媒を圧縮して高温の気体にしたりする。四方弁は，冷房と暖房のときに冷媒の流れる向きを切り替える役割をもっている。室内機の熱交換器は，冷房のときは部屋の空気を冷やし，暖房のときは部屋の空気を暖める。膨張弁は，冷媒を狭い隙間に通すことで冷媒を減圧・膨張させて温度を下げる。室外機の熱交換器は，冷房のときは屋外の空気から熱を奪い，暖房のときは屋外の空気に熱を放散する。室内機と室外機は銅管でつながれていて，銅管の中には冷媒と呼ばれるガスが入っていて室内機と室外機を循環している。気体は，圧縮すると温度が上がり，圧力を下げると温度が下がる。この原理を利用して，エアコンは冷媒の状態をコントロールすることで冷房と暖房を実現させている。



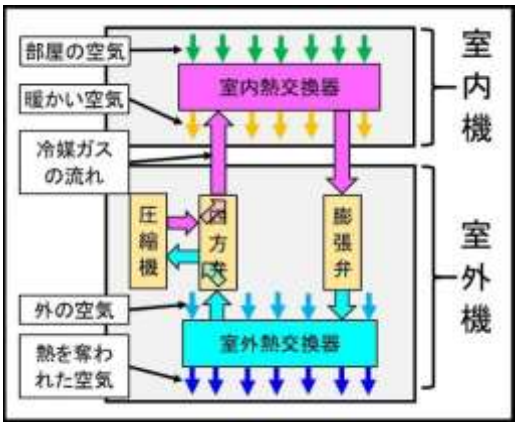
現在，ほとんどのルームエアコンでは，オゾン層破壊係数がゼロで地球温暖化係数が低い R32(ジフルオロメタン:CH_2F_2)という冷媒が使われている。

冷房の際は，部屋の空気の熱をヒートポンプで汲み上げて外の空気に捨てることにより，部屋の空気を冷やす。暖房の際は，外の空気の熱をヒートポンプで汲み上げて，部屋の空気を暖める。エアコンが冷暖房を行うためのヒートポンプ技術に必要な部品は，圧縮機・四方弁・膨張弁・室内熱交換器・室外熱交換器の５つである。５つの部品が一つの回路になっていて，その回路の中を熱を運ぶ役割をしている冷媒ガスが流れて熱を運んでいる。この５つの部品の中の室内熱交換器に入ってきた冷媒ガスと部屋の空気を熱交換させて，エアコンは空調を行っている。

冷房運転のとき,室内機の熱交換器には冷媒が５℃くらいの温度が低くて圧力が低い液体で入ってくる。温度が低くて圧力が低い液体の冷媒はとても蒸発しやすい状態になっている。熱交換器は，0.1 ミリほどの薄いアルミのフィンに冷媒が通る銅管が差し込まれているような構成になっている。銅管内の温度が低い冷媒によって，アルミフィンが冷やされる。アルミフィンの間をお部屋の暖かい空気が通ると，フィンが熱を奪って空気が冷やされる。熱を奪った冷媒は，蒸発して気体になる。室内機の熱交換器を銅管が何



冷房



暖房

度も往復しているなかで少しずつ冷媒の状態が変化する。室内機の熱交換器を出ることには 10℃くらいの気体になっている。冷房での室内機の熱交換器は，冷媒を蒸発させるため蒸発器（エバポレーター）とも言われる。このとき，部屋の暖かい空気に含まれていた水蒸気は冷やされて水滴となる。次に，室内機の熱交換器によって圧力が低くて温度が低い気体になった冷媒は室外機に流れていく。室外機では，冷媒はまず四方弁に入る。四方弁は冷房と暖房で冷媒の流れる方向を切り替える役割をもっている。冷房の時は，室外機に入ってきた冷媒を圧縮機に流す。四方弁から圧縮機に入る前に，気液分離器で液体と気体を分離させる。室内機からきた冷媒は完全に気体になっていれば良いが，液体の状態が混ざっていると圧縮機で液体を圧縮することになり故障の原因になる。気液分離器で分離された圧力が低くて温度が低い気体となった冷媒は，圧縮機で圧縮されて 50℃くらいの温度が高くて圧力が高い気体になる。

室外機の熱交換器も室内機と同じように，0.1 ミリほどの薄いアルミのフィンに銅管が差し込まれている。銅管内の温度が高い冷媒によって，アルミフィンが温められる。アルミフィンの間を屋外の暖かい空気が通ると，フィンが熱を放散して空気がさらに暖められる。放熱した冷媒は，凝縮して液体になる。実際は室外機の熱交換器を銅管が何度も往復しているなかで少しずつ冷媒の状態が変化する。室外機の熱交換器を出るころには 30℃くらいの液体になっている。冷房での室外機の熱交換器は，冷媒を凝縮させるため凝縮器（コンデンサー）とも言われる。室外機の熱交換器を出た圧力が高くて常温の液体は，膨張弁を通る。膨張弁は閉じていると冷媒は流れないが弁が開くとその狭い部分を冷媒が通過するときに流れが速くなって膨張し温度が下がる。一般的に使われている膨張弁は電動で開く度合い（開度）を決めることができる。そのため冷媒の状態によって最適な開度で制御することができる。この圧力が低くて温度が低い液体は，室内機の熱交換器へと流れていく。このように，水の場合のポンプと同様にヒートポンプを使って熱を汲み上げて，本来移動するはずのない低い温度の空気から高い温度の空気の方へと熱を移動させている。

エアコンの進歩しており，今では使った電気の約４～６倍のエネルギー量の空調を行うことができる。使った電力より多くのエネルギー量の空調ができるのは，外の空気との熱のやり取りを行うことで冷暖房をするヒートポンプのおかげである。エアコンは，実は使った電気の何倍も空調することができる，省エネ性能の高い電化製品である。

エアコンの APF は，エアコンの省エネ性能を表すための数値で，その数値が高いほど省エネ性能が高い。APF の数値はカタログなどに記載されている。

エアコンの APF の計算式

APF= 1 年間の空調エネルギー／年間消費電力

例えば APF が 5 だったとすると，消費電力の 5 倍のエネルギー分の空調を行うことができるという意味になる。現在のエアコンは，最も安く買えるスタンダードモデルで５～６，高級機種では６～７という数値になっている。

COP(エネルギー消費効率)は，冷房や暖房のある特定の運転条件中での省エネ性能を表した数値である。

COP=冷房（または暖房）能力／消費電力

昔は，エアコンの性能は APF ではなくこの COP で表されていた。この COP を計測するときの条件は実使用状態とはかけ離れていることが多く，実使用状態でどのくらい省エネになるのかは良く分からないという問題があった。そこで，APF が使わるようになった。APF は１年を通して色々な条件でエアコンを使った時に，どのくらい省エネになるのかで計算されているので，より実使用状態に近い数値である。

エアコンを選ぶ際に「対応畳数」を目安にするだけでなく，建物の構造（部屋の密閉率），暖房機能を使用するかを考慮する。冷房対応畳数 6～9 畳のエアコンがあった場合，木造なら 6 畳，鉄筋造なら 9 畳まで対応するという意味である。鉄筋造は気密性が高く冷房も効きやすいため，同じエアコンでも木造より対応畳数が多くなる。エアコンは冷房よりも暖房の方が消費電力が大きく，パワーが必要となる。そのため，対応畳数が「冷房」と「暖房」に分けて記載されている場合，暖房対応畳数の方が少なく記載されていることがほとんどである。エアコンを取り付ける部屋で暖房機能も使用するのであれば，冷房対応畳数ではなく暖房対応畳数を目安にしてエアコンを選ぶ。

エアコンは，設置する部屋の環境や使用頻度によっても選び方が異なる。リビングやリビングとダイニングキッチンがまとまっている部屋は，エアコンの使用頻度も高くなる傾向がある。そのため，電気代を節約したいのであれば省エネ性能に優れたエアコンを選ぶと効果的である。キッチンは火などを使うため非常に冷房の効きが悪いという特徴がある。「料理中も涼しく快適に過ごしたい」という場合には，対応畳数が部屋の大きさよ

りも 3 畳ほど多いものを選ぶ。

使用頻度が高いリビングなどのエアコンは，省エネ性能に優れたエアコンを選ぶことで電気代を抑えることができる。電気代でエアコンを選ぶ場合は「年間の電気代」を計算するか，「省エネ性能評価」を確認する。

年間の電気代を計算するためには，エアコンの期間消費電力量（kWh）を確認する。期間消費電力量は 1 年を通じてエアコンを使用した場合の目安となる消費電力量である。年間の電気代は「期間消費電力量 × 料金単価（円／kWh）」で計算できる。エアコンには，省エネ性能がひと目でわかるように「統一省エネラベル」がラベリングされている。星 5 段階評価で省エネ性能が評価されているため，どの程度省エネ性に優れたエアコンかを判断することができる。

出典：経済産業省資源エネルギー庁｜小売事業者表示制度（統一省エネラベル等）

4. 暖房

暖房器具には，さまざまな種類があり，それぞれ暖房の仕組みが異なり，メリット・デメリット，電気代，安全性なども違っている。

広い部屋やリビングを暖めるのに向いているのはエアコンである。メリットとして，運転ボタンを押すとすぐに暖かい空気が発生し，室内を均一に暖めることが可能で，加湿機能やスマホ連携機能など様々な機能を搭載した製品もある。石油やガスなどの燃料を使わないので，一酸化炭素中毒のリスクがない。転倒の恐れもなく，ほかの暖房器具と比較して安全性が高い傾向なので，安心して利用できる。デメリットとして，エアコンを設置する際は工事が必要で，配管パイプを通す穴がない場合は穴あけ工事が必要になるなど，自宅の設置環境によっては高額な工事費用がかかるケースもある。本体価格は，安くても 60,000 円程度と暖房器具の中では高額である。電気代は対応畳数によって幅はあるものの，6 畳用のエアコンであれば 1 時間あたり 11 円程度である。フィルターの掃除を怠るとカビや悪臭が発生することがある。

ハロゲンヒーターは，電源を入れるとすぐに加熱して暖まる。体の一部を暖めるなど，狭い範囲を短時間で暖める性能に優れている。本体価格は安いものでは 3,000 円ほどで，手の届きやすい価格帯の製品が多い。電気代は弱・中・強など出力で変わり，一時間あたり 300W で 8.1 円，600W で 16.2 円，1,000W だと 27 円ほどである。コンパクトな製品が多いのも特徴で，電源のある場所であれば気軽に持ち運んで利用することができる。デメリットとして，室内全体を暖めるほどの出力はなく，あくまで狭い範囲を暖めるのに適している。加熱部位は非常に高温で，誤って触れてしまうと火傷の原因になる。燃えやすいものを近くに置かない，離れるときは電源を消すなどの注意が必要である。消費電力が高く，強運転では 1,000W ほどになる。

カーボンヒーターは，電源を入れるとすぐに暖かくなる。ハロゲンヒーターと比較して熱効率が高く，優れた速暖性を誇る。本体価格も安いものだと 5,000 円ほどの価格帯の製品が多い。消費電力は 300W～900W ほどで，一時間あたり弱運転で 8.1 円～強運転で 24.3 円ほどである。デメリットとして，エアコンのように部屋全体の温度を上げるのには向いていない。加熱部位が高温になるので，誤って倒してしまうと思わぬ引火事故につながることもある。転倒による引火事故が心配なときは「転倒時 OFF 機能」を搭載した製品を選ぶ。接触による火傷の可能性もあるので注意が必要である。

シーズヒーターは，電気ストーブの中で最も暖かいストーブである。コンパクトな製品が多く，持ち運ぶのも楽である。燃料を燃焼するものではないので，空気を汚さない。，シーズヒーターの発熱体の寿命はとても長く，一度購入すれば長期間の使用が期待できる。デメリットとして，電源を入れてから暖まるまでに 5 分程度時間がかかる。安いモデルでも 10,000 円ほどで，本体価格がやや高い傾向にある。消費電力は弱運転で 200W 程度，強運転で 1,200W で，1 時間あたり 5.4 円～32.4 円ほどである。電源を切っても温度が下がるまで時間がかかるので火傷に注意が必要である。

ガスストーブは，熱効率が高いため，部屋全体を暖めるのに適している。ガスの燃焼時には水蒸気が発生して，室内の乾燥を防ぐ。風を発生させる機構もないため，ホコリやハウスダストが舞いにくい。石油を使わないことから給油の手間もかからない。デメリットとして，ガスストーブは，1 時間に 1～2 回ほどの換気が必要である。換気を怠ると不完全燃焼により一酸化炭素中毒になる原因になる。本体購入価格は 10,000 円～75,000 円ほどでやや高めである。1 時間あたりのガス代は，一例として，木造 11 畳・コンクリート造 15 畳の製品を強運転で使用した場合で，都市ガスだと約

60 円，プロパンガスだと約 80 円である。

ガスファンヒーターは，燃料タンクがないことから本体はコンパクトで軽い。持ち運びが簡単であり，掃除のときにも移動させやすい。暖房能力が高いうえに，立ち上がりも素早く，室内全体を短時間で暖められる。給油する手間がないので，利用するときのストレスが少ない。デメリットとして，ガスホースをつなぐので使用する場所が限定される。ガスストーブと同じく，1 時間に 1～2 回ほどの換気が必要である。購入価格は 10,000 円～70,000 円ほどとやや高めである。1 時間あたりの電気代とガス代の合計は，一例として木造 11 畳・コンクリート造 15 畳の製品で都市ガスを利用した場合であれば約 43 円ほど，プロパンガスだと約 46 円ほどである。

オイルヒーターは，石油やガスを使わないので，室内の空気を汚さない。ファンが回ったり，風を送り出したりすることもないので，ホコリやハウスダストが舞いにくい。静音性に優れ，運転音が静かある。本体の表面温度も約 60～80 度程度なので誤って触れてしまっても火傷する可能性は低い。デメリットとして，暖房効率が悪く，運転を開始してから室内が暖まるまでに時間がかかる。暖まるのに時間がかかるため，その分，電気代が高くなる。本体の購入費用は安いもので 10,000 円ほどとやや高めである。電気代については 600W～1500W の機種の場合で一時間あたり約 16.2 円から 40.5 円ほどである。

セラミックファンヒーターは，石油やガスなどの燃料を使用しないので，工事や燃料の補給が必要ない。石油やガスを使用しないので，換気の必要がない。購入費用は 2,000 円～37,000 円ほどで，幅広い価格帯の製品がある。1 時間あたりの電気代は，550W（弱）であれば約 15 円，1,200W（強）であれば約 30 円である。デメリットとして，セラミックファンヒーターは，出力が弱い傾向があり，広い範囲をあたためるには不向きである。運転中の転倒や衣類の接触が火災の原因となる場合もあるので注意が必要である。長時間にわたる温風によって低温やけどや脱水症状が起きたりするリスクがある。温風を発生させるので，空気が乾燥したり，ホコリが舞ってしまったりする。

パネルヒーターは，輻射熱（ふくしゃねつ）で周囲を暖めるので，熱源がむき出しのストーブなどと比較して安全性が高い。石油やガスを燃焼させないので，空気が汚れない。換気も不要であり，窓のない部屋でも使える。購入費用は 4,000 円～55,000 円ほどで，幅広い性能の製品から選ぶことができる。1 時間の電気代は，300W であれば約 8 円，1,200W であれば約 30 円である。デメリットとして，パネルヒーターは，部屋を暖めるのに時間がかかる。

製品によっては温度を高く設定すると，消費電力とともに電気代が高くなってしまうことがある。タオルや服などをパネルヒーターにかけて乾かそうとするなど，誤った使い方をすると火災の原因になる。

電気カーペットは，体を直接温める効果があるので，暖房効果を実感しやすく，消費電力も抑えやすくなっている。エアコンと電気カーペットを組み合わせれば，エアコンの温度設定を低くして消費電力を下げることも可能である。購入費用は 1,700 円～45,000 円ほどで幅広い製品から選ぶことができる。1 時間の電気代は目安として，1 畳タイプ（200W）が 5 円ほど，2 畳タイプ（500W）が 14 円ほど，3 畳タイプ（740W）が 20 円ほどである。デメリットとして，座っている状態では下半身，立っている状態では足しか暖かさを感じられない。部分的にしか暖房効果がないので，部屋全体を暖める効果は期待できない。エアコンやガスファンヒーターのように風が発生しないので，電源が入っていることをうっかり忘れてしまいがちである。皮膚の弱い人が長時間寝そべっていると，低温やけどを生じる恐れがある。

電気毛布は，他の暖房器具と比べて電気代が安い。持ち運びやすく車中泊や冬キャンプなど様々なシーンで活躍する。購入費用は 3,000 円～25,000 円ほどで幅広い製品から選ぶことができる。消費電力は 3W～80W ほどで，一時間あたり 0.81 円～2.16 円ほどである。デメリットとして，体を直接温める効果はあるが，部屋全体を暖めるような効果はない。付けっぱなしにして寝てしまうと脱水症状や低温やけどなどの危険がある。入眠がスムーズになる一方で，睡眠の質の低下を招くとも言われている。

課　題

1．家庭内の電気製品を安全に使用するための方法について具体的に説明しなさい。

第８講　コンピュータ

【学修到達目標】

- コンピュータの仕組みを理解できる。
- 目的に合ったパソコンを選んで利用できる。

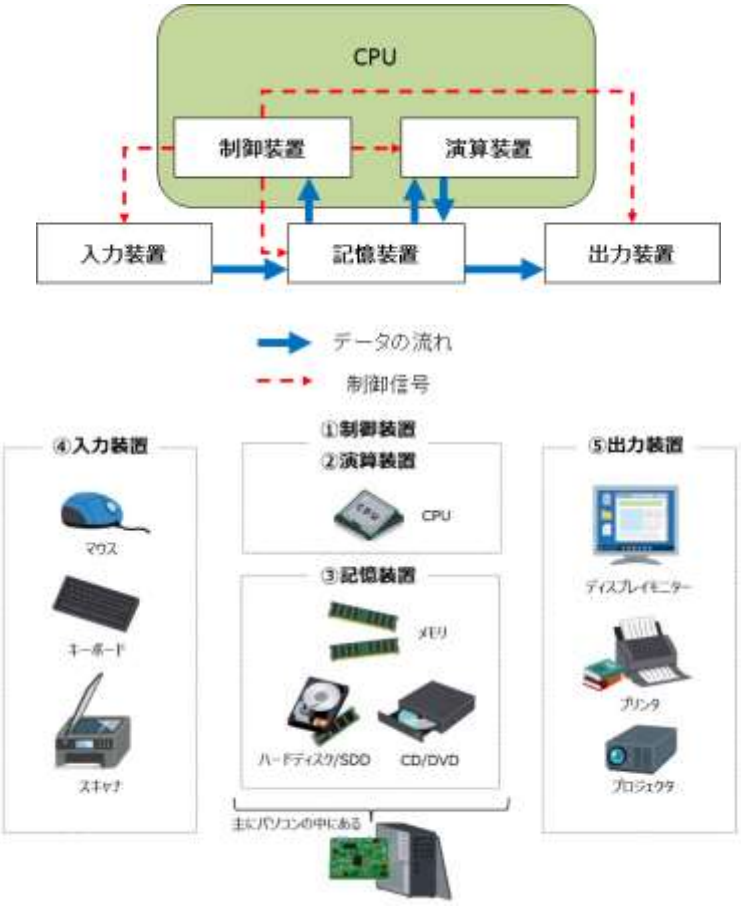
１．コンピュータの仕組み

「コンピュータ」は「データの処理をする装置」を指す言葉で，スーパーコンピュータのような超大型で大規模な装置や，ビジネス用のサーバ，家庭用のコンピュータなどを含む。スマートフォンや iPad，電子レンジの内部システム,スーパーのレジシステムなども広い意味ではコンピュータである。パソコン は，パーソナルコンピュータの略である。コンピュータの種類には，次のものがある。

種類	用途	説明
マイコンピュータ	炊飯器 オーディオ機器 エアコン 等	エアコンの制御, ラジコン, 自動車エンジンの燃料噴射装置, 家電製品の制御用として利用される。マイコンと呼ばれる。
スーパーコンピュータ	宇宙ステーション 気候変動調査	パソコンより超高性能で，大規模な科学技術計算などに用いられるコンピュータ。衛星の軌道計算など，膨大な情報量を短時間で処理する用途に利用される。
ワークステーション	在庫管理 顧客データ管理 銀行や役所などのシステム 設計支援（CAD） グラフィックデザイン 等	パソコンより高性能で, 大量のデータや, 事務処理等に特化した業務用のコンピュータ全般のこと。メインフレームとも呼ばれる。
パーソナルコンピュータ	ワープロ 表計算 データベース	パーソナルコンピュータ（Personal Computer）の略で，個人用途メインで作られたコンピュータのこと。パソコンや PC と呼ばれる。

コンピュータのハードウェアは大きく分けて，制御装置，演算装置，記憶装置，補助記憶装置，入力装置，出力装置で構成されている。主記憶装置と補助記憶装置は，コンピュータ内でデータやプログラムを記憶する装置で，半導体メモリを利用した主記憶装置（メインメモリ）と，ハードディスク，フロッピーディスク，CD-ROM やフラッシュメモリなどの外部記憶装置（補助記憶装置）に分けられる。

装置名称	代表的な機器
制御装置	中央処理装置（CPU:Central Processing Unit）
演算装置	CPU はコンピュータの中枢部分で，制御と演算を行う装置である。制御装置の指示に従って演算を行う。
記憶装置	主記憶装置
補助記憶装置	プログラムやデータを長期にわたり記憶する装置。長期保存が前提であるため，コンピュータの電源を切っても内容が破棄されることはない。代表的なものとしてはハードディスクがある。単にディスクやストレージ等と呼ばれる。
入力装置	外部からのデータをコンピュータに入力する為の装置で，代表的な例として，キーボード，マウス，スキャナなどがある。
出力装置	処理されたコンピュータのデータを出力する為の装置で代表的な例として，ディスプレイ，プリンタなどがある。



外部記憶装置は磁気的に記録を行うものが多いため，動作は遅いが記憶容量が大きく，電源を供給しなくても記録が消えないという特徴がある。主記憶装置は半導体素子を利用して電気的に記録するため，動作が高速で CPU から直接読み書きすることが出来るが，単位容量当たりの価格が高いため大量には使用できず，コンピュータの電源を切ると内容が失われる。通常コンピュータには両方が装備されており，利用者がプログラムを起動してデータの加工を行う際には必要なものだけ主記憶装置に呼び出して使い，長期的な保存には外部記憶装置が利用される。

メインメモリは単にメモリとも呼ばれ，メモリは大きく分けて RAM（ラム）と ROM（ロム）が存在する。

種類	特徴
RAM （Random Access Memory）	データを自由に読み書きできるが, 電源を切ると記憶データは消去される。
ROM （Read Only Memory）	電源を切っても記憶データは保持される。

RAM とはランダムに読み書きできるメモリのことで, DRAM（Dynamic RAM）と SRAM（Static RAM）に分類することができる。

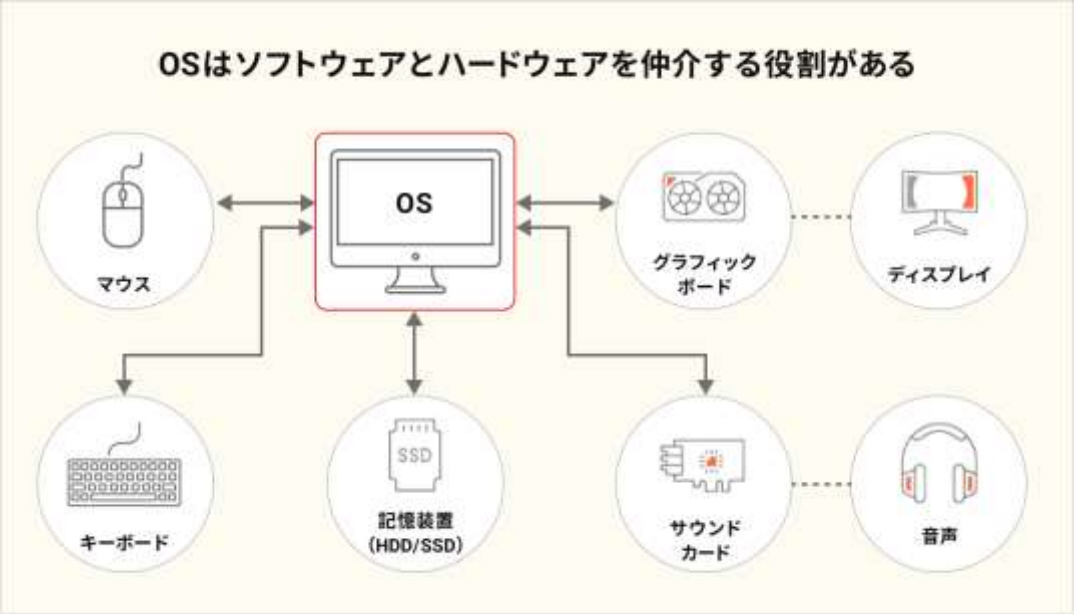
RAM の種類	使用する回路	リフレッシュ	速度	価格	主な用途
DRAM	コンデンサ	必要	低速	安価	主記憶装置
SRAM	フリップフロップ回路	不要	高速	高価	キャッシュメモリ

ROM は，リードオンリー（読み出しだけ）なメモリのことで，ROM といえば，マスク ROM のことを指すが，専用の機器を使うと記憶装置の消去と書き込みができる PROM という種類もある。

補助記憶装置は，主にハードディスクのことをさし，ハードディスクには金属製の円盤が入っており，これに磁気の力で書き込んだり読み込んだりする。ハードディスクの内部には容量に応じてプラッタという金属製のディスクが 1 枚以上入っていて，その表面に磁性体が塗布もしくは蒸着されている。この磁性体を磁気ヘッドで磁化させることでデータの読み書きを行う。ハードディスクを最初に使うときは，初期化が必要でこれを行うとプラッタの上にデータを記憶するための領域が作成される。作成された領域の，扇状に分かれた最小範囲をセクタ，そのセクタを複数集めたぐるりと 1 週分の領域をトラックといいう。同心円状のトラックを複数まとめると，シリンダという単位になる。

2. OS (Operating System：基本ソフトウェア)

OS は，システムソフトウェア，または，基本ソフトウェアとも呼ばれ，ユーザーの使い勝手を高めるコンピュータの制御システムで，ソフトウェアとハードウェアを仲介する役割があり，入出力の制御やソフトウェアの起動管理などの機能がある。

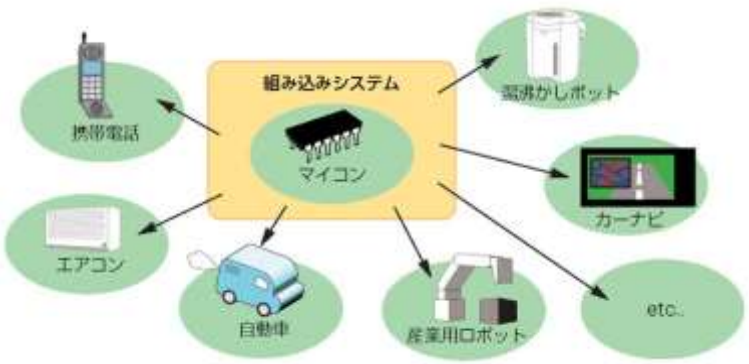


OS が主に果たす機能として，入出力の制御，ソフトウェアの起動・終了・切り替え，ファイルの管理，他コンピュータとのネットワーク通信がある。入出力の制御とは，キーボードやマウスといった機器からの入力を受け取ったり，コンピュータでの処理結果を画面上に出力したりする機能のことである。ソフトウェアの起動や終了，切り替えは，OS が管理しており，OS はソフトウェアの起動・終了・切り替えが起きたことを「メッセージ」で通知し，ソフトウェアはそれらの通知に応じてさまざまな処理を行う。ファイル管理とは，ファイルへの命名・ファイルの読み取り・ファイルへの書き込みといった操作のことで，OS が制御している。他のコンピュータとのネットワーク通信にも，OS の機能が使われており，通信プロトコルの管理やデータの送受信などを行う。

パソコンの OS の種類は，Windows，Mac OS，Chome OS，Linux がある。Windows は，Microsoft 社が 1985 年に開発した OS で，Windows OS（ウィンドウズ・オーエス）とも呼ばれる。販売されるパソコンの大部分が Windows OS を搭載している。Windows OS は GUI（グラフィックユーザインタフェース）といって，マウスなどのポインティングデバイスを使って画面を操作することでコンピュータに命令を伝える。Chrome OS は，Google が提供している Linux をベースにした OS で，GUI で直感的に操作できる。また，Windows OS のように Word や Excel などのソフトウェアをダウンロードして使う「応

用ソフトウェア」を使わない。ブラウザである「Google Chrome」を利用してブラウザ上で作業を行う仕組みになっている。Chrome OS は，「起動が早くて動作が軽い」「導入コストが低い」「データをクラウド上で管理」「堅牢なセキュリティ」「自動アップデート」「Android スマートフォンと同じアプリケーションを使用可能」という 6 つの特徴を持っている。iOS は，アメリカのアップル社が開発した iPhone・iPad 向けの OS で，2010 年 6 月に公開されたバージョン 4.0(iOS 4)より iPhone OS から iOS に呼び名が変更された。iOS は，「タッチパネルによる操作」「音声認識」「本体の動きや傾きを感知する加速度センサーなどのユーザーインターフェース」「マルチタスク機能」といった特徴を持っている。iOS はアップル製品にしか対応していない。Android（アンドロイド）は，スマートフォンなどの携帯情報端末のために，Google 社が開発した OS（オペレーションシステム）のことである。Android が搭載されている情報端末であれば，Android 対応のアプリが使える。「メールの送受信」「インターネット」「ゲーム」ができるという特徴がある。アプリケーションをダウンロードすることで自分の使いやすいようにカスタマイズすることができる。また Android 搭載のスマホなら，どのキャリアであろうと関係なく，Android 用のゲームやアプリを，ダウンロードして遊ぶことができる。

OS は，パソコン以外には電化製品に使われていて，知らず知らずのうちにふだんの生活で利用している。電化製品などはマイクロコンピューター（マイコン）と呼ばれる小型のコンピュータを搭載していて，それを制御するために OS が使われている。電化製品の特定の機能に特化しており，特定の目的に使われる OS のことを，組み込み OS（エンベッド OS）という。組み込み OS に対して，パソコンで使われている Windows や macOS などの OS のことを汎用 OS という。汎用 OS は OS そのものの機能だけでなく，アプリケーションをインストールすることが前提で，さまざまな機能を追加できる。汎用 OS は使用するユーザーによって，自由な使い方ができる高い汎用性を持っている。組み込み OS では電化製品を制御するため機能を最低限に絞り，また機械を制御するために決められた期間内に命令された処理を完了する仕組みになっている。この仕組みを持つ OS をリアルタイム OS という。汎用 OS は処理の完了の期限が決められていないが，機械の制御を行う組み込み OS では期限内に処理を完了させる必要があるために，リアルタイム OS が使用されている。



汎用 OS では，発見されたセキュリティの問題を解決したり，新しく登場したハードウェアに対応したりするために，定期的なアップデートが必要である。パソコンが常時インターネットに接続している状態では，セキュリティの問題を放置していると悪意あるユーザーから攻撃を受けるおそれがある。また新しく登場したハードウェアは，どういった影響を OS に与えるのかがわからないため，OS をアップデートする必要がある。

パソコンやスマートフォンに搭載されている OS やアプリケーションなどは，開発段階からセキュリティに対して十分に配慮されて開発されている。しかし最初から完璧なソフトウェアを開発することは，非常に難しい。ソフトウェアの脆弱性を悪用するサイバー攻撃の手口は日々進化している。ソフトウェアの開発時には対策できていた脅威でも，攻撃手法の変化や，未知の脆弱性の露呈などによって，対策が取れていないサイバー攻撃の被害にあってしまう。そこで，OS やソフトウェアは，脅威やセキュリティ上の脆弱性が発見されたら随時修正を行って，利用者が修正版にアップデートする必要がある。

アップデートのリスクも存在する。使用しているハードウェアによっては，最新の OS やソフトウェアが対応していない場合がある。古い機種に対してソフトウェアのアップデートをすると，正常にアップデートできないことや，アップデートによってデバイスの動作が不安定になることがある。大規模な OS のアップデートを行ったことで，デバイスにインストールされているアプリケーションが動かなくなることがある。アプリケーションが最新の OS に対応していないことで発生する不具合である。

IPA や JPCERT/CC といった機関が情報セキュリティに関する情報を発信している。これらの機関の報告を基に，すぐに対応すべき点を確認することが大切である。

3. パソコンの性能

パソコンの性能（スペック）で重要なのは，メモリ，CPU，HDD（SSD）である。メモリは大きいほどよく，作業机に例えると広くて大きいほど作業しやすい。CPU は，処理速度が早い方がよく，人間で言う頭の回転速度に例えられる。HDD（SSD）も大きいほどよく，書斎・本棚のようにあらゆるものを保存する場所に例えられる。

メモリは Memory「記憶」を語源とするように，コンピュータでプログラムやデータを記憶・保持するための装置を指し，ROM や RAM といった記憶装置である。読み出しができるが ROM で，データやプログラムの読み書き両方ができる記憶装置を RAM という。一般的に「メモリ」と呼んだ時は RAM であるメインメモリを指すことがほとんどである。メモリは，一時的に記憶する部品

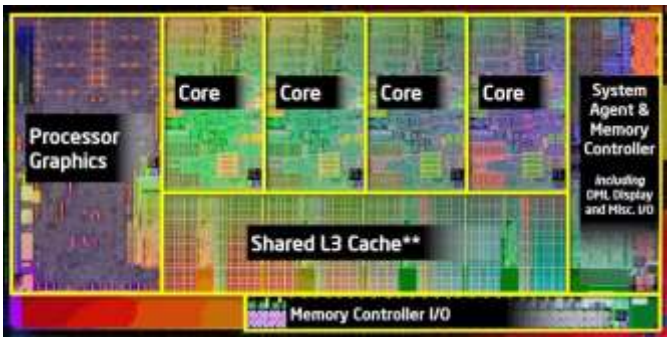
で，コンピュータでは 主記憶を担当し，卒論研究のための動画編集などをすることを考えると 16GB 以上が望ましい。主な目的と用途によるメモリ推薦容量を次に示す。

目的と用途	メモリ推奨容量
・OFFICE（ワード・エクセル・パワーポイント） ・インターネット検索，動画閲覧（Youtube,Hulu）など ・ビジネス用途 ・簡単な画像や動画の編集	4GB
・Adobe 系ソフトの使用（WEB デザイナー・コーダーに） ・本格的な画像編集，動画編集，製図（CAD 等） ・軽めのオンラインゲーム	8GB
・オンラインゲーム ・プロフェッショナルな動画編集 ・タスクを開きまくって作業したい人	16GB

メモリは，規格で標準化されており，パソコンには DDR SDRAM と呼ばれる規格のものを選ぶ。DDR SDRAM は，省略して DDR 呼ばれることが多い。DDR の世代が進むごとにスペックアップし，容量は大きく,また同じ容量であっても速度性能が向上している。世代によってピンの数や切りかけ部分も異なる。主流は DDR4，次いで前世代にあたる DDR3 の二つである。DDR4 の仕様は次のとおりである。

チップ規格	モジュール規格	メモリクロック	バスクロック	転送速度
DDR4-1600	PC4-12800	100	800	12.8GB/秒
DDR4-1866	PC4-14900	116	933	14.9GB/秒
DDR4-2133	PC4-17000	133	1066	17.0GB/秒
DDR4-2400	PC4-19200	150	1200	19.2GB/秒
DDR4-2666	PC4-21333	166	1333	21.3GB/秒
DDR4-2800	PC4-22400	175	1400	22.4GB/秒
DDR4-2933	PC4-23466	183	1466	23.4GB/秒
DDR4-3000	PC4-24000	188	1500	24.0GB/秒
DDR4-3200	PC4-25600	200	1600	25.6GB/秒
DDR4-3400	PC4-27200	213	1700	27.2GB/秒
DDR4-3600	PC4-28800	226	1800	28.8GB/秒
DDR4-4000	PC4-32000	250	2000	32.0GB/秒
DDR4-4266	PC4-34100	266	2133	34.1GB/秒

CPU は「Central Processing Unit」の略で制御や演算をする中央処理装置である。CPU はパソコンの演算処理を行う非常に重要な部分で，処理速度の速さに繋がる。CPU のメーカーは，Intel と AMD がある。Intel 製の CPU は Core，AMD 製の CPU は Ryzen と呼ばれる。CPU の性能を図る方法の一つがベンチマーク（性能測定）である。ベンチマークの測定方法には，マルチコアとシングルコアがある。CPU のチップには，①司令塔②問題の処理③データ保存 という３つの役割があり，コアはこの３つの中で②の問題の処理をする役割を行っており， CPU のスペックに大きく関係している。CPU のコア数は CPU の中に搭載されているコアの数を示している。



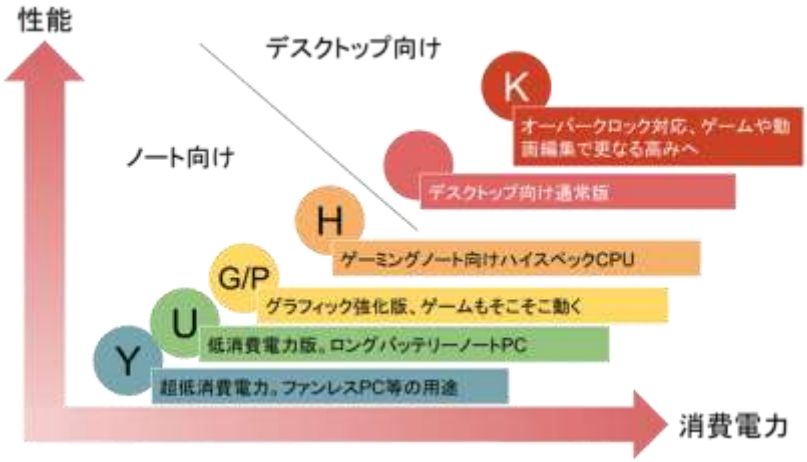
マルチコアのスコア（マルチスレッド性能）は，たくさんの作業を同時に行っているときの機敏さや，パソコンの起動速度，処理の分散にしている一部のソフトウェアの速度，画像加工や映像編集（エンコード）速度などに影響する。シングルコアのスコア（シングルスレッド性能）は，ほとんどのゲームやソフトウェアの動作速度，単一作業の速度などに影響する，基礎となる性能である。マルチコア性能はたくさんの処理を同時にやらせたときの評価なので，コアが多い CPU ほど高い数値になる。一般の用途だと大量の処理を同時に行うことは稀なので，たくさんのコアがあっても意味がないことも多い。パソコンは裏で様々な処理を行っているが，それでも同時処理数（スレッド数）は 8 ほどあれば一般的な用途では問題なく，それ以上がどのぐらい有効になるかは用途や環境による。多くのゲームは「重い単一処理」なので，スレッド数は影響しない。実況配信や録画など，別の作業も同時に行っている場合，コアが多い方が安定する。

シングルコア性能は，ひとつひとつの処理をどれぐらい速くこなせるかの目安となる。普段の使用時に影響が大きいのはシングルコア性能てせある。ただし，エクセル・ワードなどを含む事務ソフト Office や，フォトショップ・イラストレーターなどの Adobe 社のソフトは，処理の分散（マルチコア最適化）に対応しているため，マルチコアとシングルコアの双方が影響する。

Intel の方が安定していると言われ，ベンチマーク中でも Core の方が温度が安定していることが多く，Ryzen は割と 100℃近くの高温になりがちである。Core の方が比較的安全な，余力のある設定になっている。ゲームはシングルコア性能が重要で，シングルコアに強いのは一部の製品を除き，Intel の Core で

ある。Ryzen は表計算で Core より高い性能を発揮する。ただし Core Ultra，は表計算を得意とする。Core は型番で世代や種類を判別しやすく，製品のラインナップが整っている。Ryzen は型番で世代や種類を判別しにくい。Ryzen は価格が安めの割に性能が高めで，コストパフォーマンスがよい。ノート用の Core には Iris Xe というグラフィック機能が備わっていて，CPU 内蔵機能としては高い性能を持つ。Ryzen は上位 CPU 以外，内蔵グラフィック機能が弱く，Youtube などの動画サイトの表示時に処理がもたつくことがある。ただし Core Ultra は Intel Arc という新型グラフィック機能になったため，ソフト側の対応が進んでおらず，実力を発揮できないケースが多い。(2024 年 4 月現在)

Intel Core シリーズでは，シリーズと世代を理解する必要がある。シリーズは価格帯別のラインナップを表し，Core i3，Core i5，Core i7，Core i9 と数値が大きいほどハイエンドな CPU となる。世代は，ほぼ毎年刷新されるアーキテクチャが最初から数えて何番目かを示す。Core i7-14700K ならば，シリーズ名の i7 に続く 14 が世代を表す。ただし 2023 年末の Core シリーズのリブランディングの結果，Core Ultra 9 185H など i が消え，再び第 1 世代から始まることとなった。数値が大きいほどハイエンドというルール自体に変更はない。新しいほど改良が加えられて性能が向上し，世代が変わると年にもよるが 20%程度性能が上がることが多い。シリーズと世代の他で重要な要素が末尾文字で，Core i7-10510U ならば U が末尾文字であり，末尾文字は主に用途を表す。



Ryzen は 2017 年に発売を開始した AMD の CPU である。コスパや性能が高く，第 3 世代以降に弱点だったゲーム性能もインテルと比べて遜色のないものとなり自作デスクトップパソコンに Ryzen を利用することも多い。Ryzen の型番を理解すると大まかな CPU 性能が推測でき，比較が容易になる。Ryzen 9 7950X の場合，最初の 9 に関して，Ryzen は Ryzen 9, Ryzen 7, Ryzen 5, Ryzen 3 とシリーズが分かれており，数値が大きいほど性能が高い。次に 7950X の最初の 7 は世代を表す。世代は CPU のアーキ

テクチャが現在何番目であるかを示す値である。通例 1 年ごとに更新され，世代が上のものほど設計が洗練されパフォーマンスが高い。950 の部分はマイナーバージョンを表す数値である。アーキテクチャ自体に差異はないが，この数値が大きいほど性能が高い。最後に X は Extreme を表す文字である。末尾の文字が意味するところは様々であり，U は低消費電力，G は Graphic 機能ありといった意味がある。

CPU の末尾文字	性能
アルファベット無し	通常版
X	AMD の最高峰 CPU を冠した文字
G	GPU 内臓(AMD の CPU は G 以外だとグラフィックボードが必須)
U	ノート用低消費電力版
E	ノート用低消費電力版
H/HS	ノート用ハイパフォーマンス版

Ryzen PRO モデルは企業向けにセキュリティ機能を強化したバージョンである。

SSD・HDD 共にストレージという容量をつかさどる部分で，パソコンのあらゆるデータを保管する役割がある。容量が大きいほど多くのデータを保存できる。容量に対して写真・動画がどのくらい保存できるかは次のとおりである。

容量	写真保存枚数	動画保存時間
128GB	1800 万画素の写真データ 約 19,000 枚	約 20 時間
256GB	1800 万画素の写真データ 約 38,000 枚	約 40 時間
512GB	1800 万画素の写真データ 約 76,000 枚	約 80 時間
1TB	1800 万画素の写真データ 約 150,000 枚	約 160 時間

SSD は Solid State Drive（ソリッド・ステート・ドライブ）の略で，HDD と同じように使える記憶装置である。HDD は回転する円盤に磁気でデータを読み書きしているが，SSD は USB メモリーと同じように内蔵しているメモリーチップにデータの読み書きをしている。メリットとデメリットは次のとおりである。

HDD と比較した SSD のメリット

- 衝撃による故障リスクが低い
- 読み書きの速度が非常に速い
- 動作音が静か
- サイズが小さく軽い
- スティック型などデザインの自由度が高い

HDD と比較した SSD のデメリット

- 最大容量が少ない
- 大容量になると容量単価が高い

SSD と HDD にそれぞれ特徴があるので，目的に合わせて利用する。

	SSD	HDD
速度	◎	△
容量	△	○
静音性	◎	△
耐衝撃	◎	△
軽量	◎	△
価格	△	○

課　題

１．目的に合ったパソコンの選び方について説明しなさい。

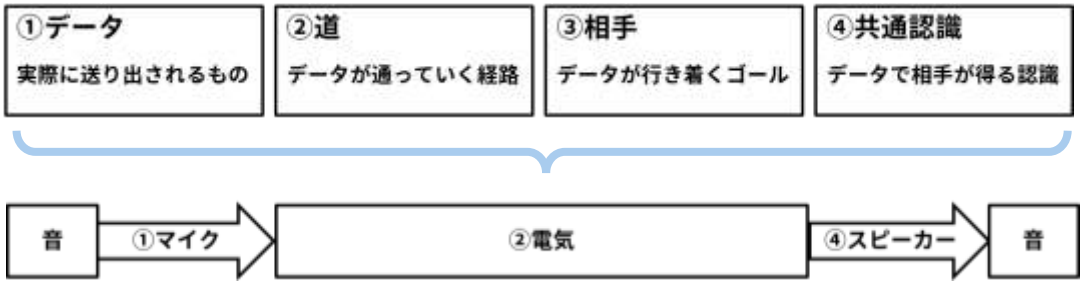
第９講　通信

【学修到達目標】

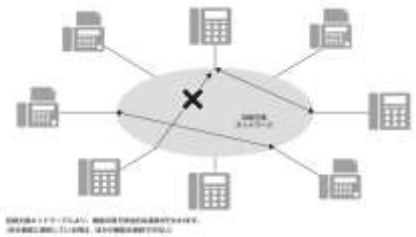
- 通信の仕組みを理解できる。
- 日本の通信の歴史を理解できる。

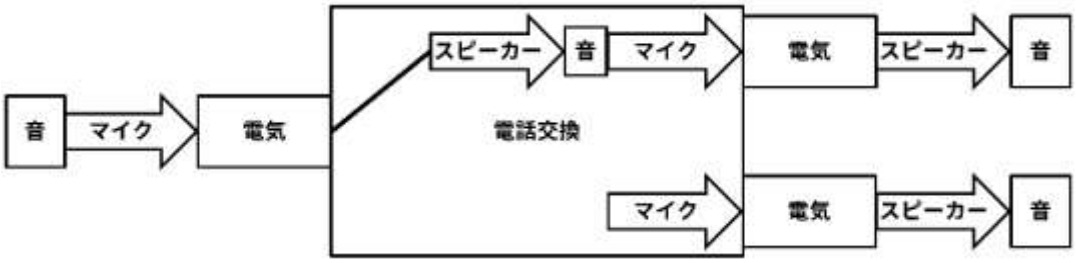
１．通信

通信（telecommunication）とは，生身で直接やり取りできない離れた場所にいる人間同士が，何らかの手段を用いて情報を伝達することである。現代では電気通信の意味で用いられることが多い。通信には，４つのポイントがある。①情報を伝える人は，情報を言葉などのデータに変換して送る。②データは，何らかの道（伝送路）を通って送られる。③データは，はじめから決めていた相手の宛先に届く。④相手がデータを読み取って，自分と認識を共有でき，共通認識ができる。昔の通信は，光や煙，音などを使って合図を伝えたり，飛脚や鳥などに手紙を届けてもらったりが通信であったが，①～④の流れに沿っていた。電話は，電気を使っているが，①～④の流れに沿っている。



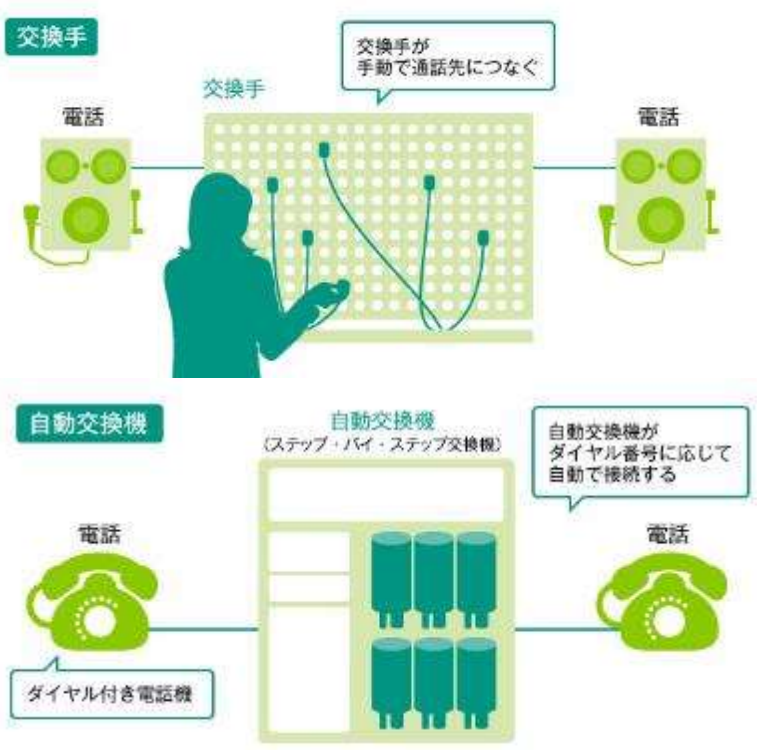
電話は，たくさんの人につながることで，便利で，低コストになる。電話の相手先を増やすため，スイッチング（電話交換）という，相手先切替のしくみが生まれた。初期の電話交換は人手でスピーカーとマイクをつなぎ換えていた。その後，電話番号（アドレス）が整備されて，スイッチングも人手を使わず，自動交換機（切替スイッチ）で相手先につながるようになった。自動交換では，あらかじめ網目状につながった伝送路が稼働しているため，その伝送路のつながりをネットワーク（通信網）と呼ぶようになった。





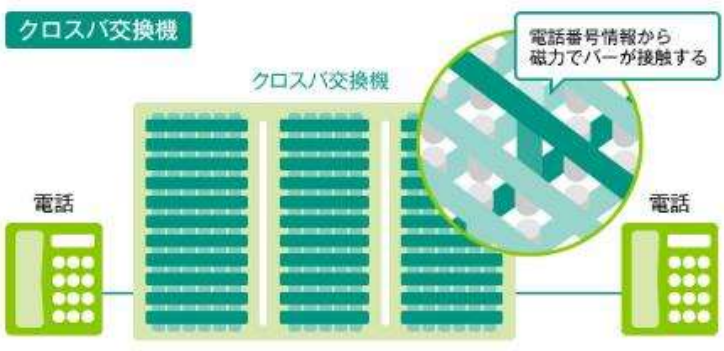
2. 日本の通信の歴史

1890 年，郵便や通信を管轄していたのが逓信省（ていしんしょう）だった。この年，東京市内と横浜市内を結ぶ電話サービスが開始され，電話したい相手に交換手に手動でつないでもらうという仕組みによって，日本の電話が始まった。電話機の受話器を上げると交換手につながり，「A さんにつないでください」と通話先を告げると，交換手が A さんにつなぐ，という仕組みだった。受話器を上げるだけで交換手につながる仕組みだったため，初期の電話機にはダイヤルがなかった。電話サービスが始まった当初は，加入者数も現在ほど多くなかったため「交換手」という人の手による取り次ぎが可能だったが，加入者数や利用回数が多くなるにつれ，取り次ぎが追いつかなくなった。そこで，1926 年から徐々に「交換手」に代わる「自動交換機」が導入されるようになった。



「自動交換機」とは，「交換手」の手を介さず，電話番号に基づいて自動で電話をかけたい相手につなげる通信機器のことである。この「自動交換機」の登場で，交換手が行っていた取り次ぎ業務が機械に置き換えられていくことになった。国内で初めて導入された自動交換機に採用されたのが「ステップ・バイ・ステップ」という方式である。電話したい相手につなぐには電話番号が必要とな

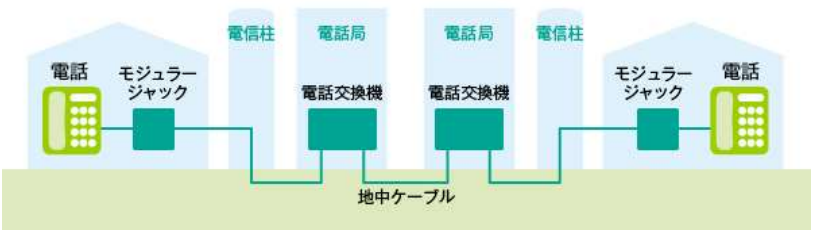
り，初めてダイヤルが付いた電話機が登場した。「ステップ・バイ・ステップ」とは，ダイヤル式電話機から送られてきたダイヤルの番号に応じて，その数字の回線に次々に接続していき，最終的に相手の電話機に回線がつながるという仕組みである。次々に接続していく一連の動作が「ステップ」と呼ばれ，「ステップ・バイ・ステップ交換機」という名称となった。



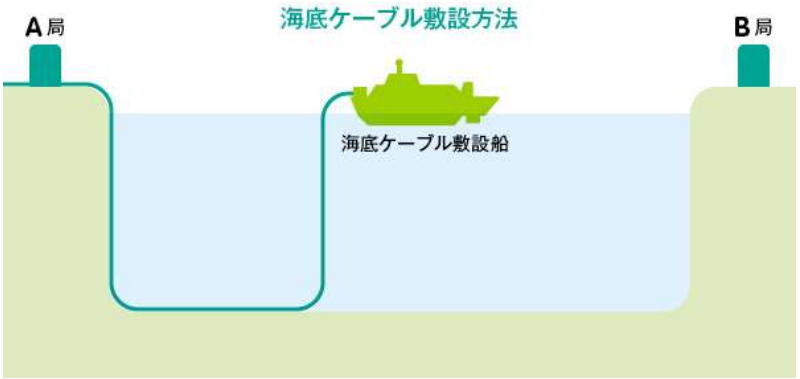
1952 年の日本電信電話公社発足当時，市内通話はステップ・バイ・ステップ交換機で自動的につながるようになったが，市外通話では依然として交換手が接続業務を行っていた。市外通話は，市内通話に比べて距離が離れていることもあり，各地に点在する自動交換機をいくつも経由して接続する必要があるため，接続に時間がかかる一方，ステップ・バイ・ステップ交換機には，保守が難しく，機器自体の寿命が短く設置・維持にコストがかかるというデメリットがあったためである。こうした問題を解消するため，1955 年には「クロスバ交換機」が導入された。「クロスバ交換機」では，縦と横に張り巡らされた複数のバーがクロス（交差）して設置され，電話をかけると，ダイヤルされた電話番号の情報から各バーに付いている電磁石の磁力により縦と横のバーが接触し，相手に電話をつなぐという仕組みになっている。ステップ・バイ・ステップ交換機よりもコストをかけずに，各地の自動交換機をいくつも経由する回線の自動接続が可能になり，市外通話の全自動化が実現された。クロスバ交換機では市外通話料金の自動記録が可能になった。こうして，交換手を介さず待ち時間もない市外通話は，クロスバ交換機の普及や回線の増設により 1967 年には県庁所在地級の都市で利用されるようになり，1978 年には全国に広まった。

電話サービスの普及率が上昇する中，1982 年には音声や制御信号がすべてデジタル化された「デジタル交換機」が導入された。これまでのアナログ通信と較べ，音声もクリアで聞き取りやすくなり，利用者はますます増えた。このように発展してきた電話サービス。2004 年には，NTT 東日本が「IP 電話」サービスである「ひかり電話」を開始した。「IP 電話」の仕組みには，電話番号を管理する「SIP サーバ」や，音声データを適切な回線に振り分ける「ルータ」など，インターネットで用いられる機器が採用された。これらの機器は従来の自動交換機より安価に導入でき，音声とデータをひとまとめで送信できることから，通信効率も高まった。こうしたメリットにより，通話料も安くなった。また，「音声」を伝える以外に「動画」を伝えることも可能となり，これによって「テレビ電話」が普及することになった。一対多人数の接

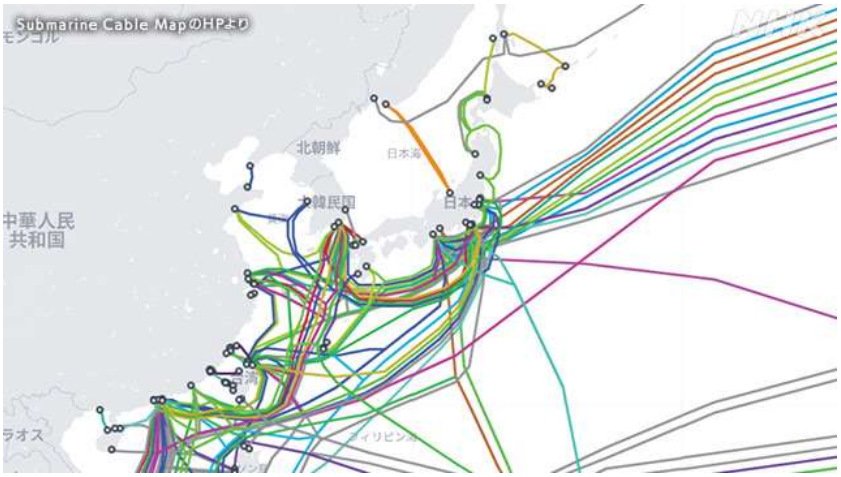
続も簡単にできるため，現在では，企業などで「テレビ（電話）会議」を採用するところも増えてきた。家庭から家庭へ電話するときは，モジュラージャックや電話交換機を通して，電気信号が送られる。



国際電話のケーブルは，海底にあり，海底ケーブルは，「海底ケーブル敷設船」という専用船を利用して敷設される。陸から伸びているケーブルを沖合でつないだあと，ケーブルを少しずつ海底にたらしていく。過酷な環境にある海底ケーブルには，メンテナンスが欠かせない。最深で約 1 万メートルある日本海溝でも，ケーブル自身の重さで切れてしまわないよう，海底にピッタリ沿うように敷設するので，最深部では 1 トン近い水圧がケーブルにかかっている。一方，浅いところでは船のいかりや網に引っかかったり，サメにかみつかれたり，海底ケーブルを取り巻く環境は非常に厳しい。 日本に最初の海底ケーブルが敷設されたのは，1871 年で，デンマークによって長崎～上海間と上海～ウラジオストック間に敷設された。



この地図にある無数の線はすべて日本列島につながれた海底ケーブルである。



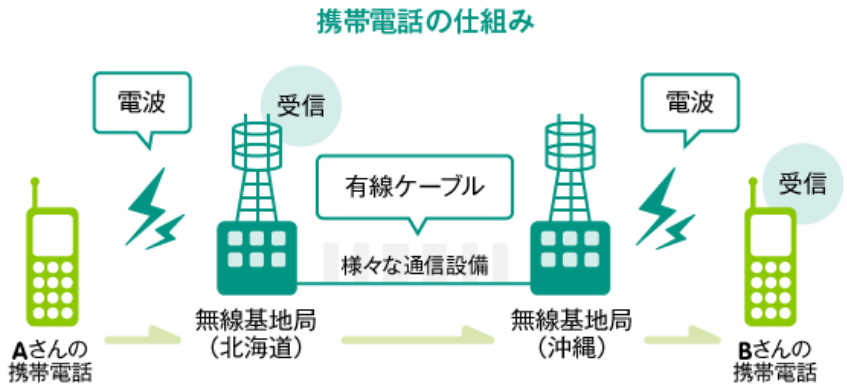
日本とつながるものだけでおよそ 30 本，世界では 400 本以上にのぼり，総延長は 130 万キロにおよぶ。スマホやパソコンと携帯の電波や Wi-Fi でつながる

ネットは，無線であるが，建物や携帯の基地局から先は有線のケーブルでつながれている。海を渡り国境を越えてつなげるために使われるのが海底ケーブルである。かつては通信衛星も使われていましたが，現在は膨大なデータ量とスピードを確保するために，国際通信の 99%を海底ケーブルが占めている。海底ケーブルがなければ，速度の遅延なく動画投稿サイトを見たり，クラウドに写真を保存したりといった当たり前の生活ができなくなる。

データ量の増加と通信スピードの加速に応じるために，技術は大きく進化を続けている。光ファイバーは髪の毛ほどの細さで，最新の技術ではそれを 48 本束ねて，金属などで頑丈に保護している。1 本で 1 秒あたり DVD にして 1 万 3300 枚分のデータを送信。その容量はこの 20 年で 100 倍にまで増えた。その技術は世界の中でも日本企業のレベルの高さが目立っている。アメリカ，フランスの企業とともに，日本の NEC がトップ 3 を形成し，3 社のシェア合計は 9 割を占めている。

3. 携帯電話

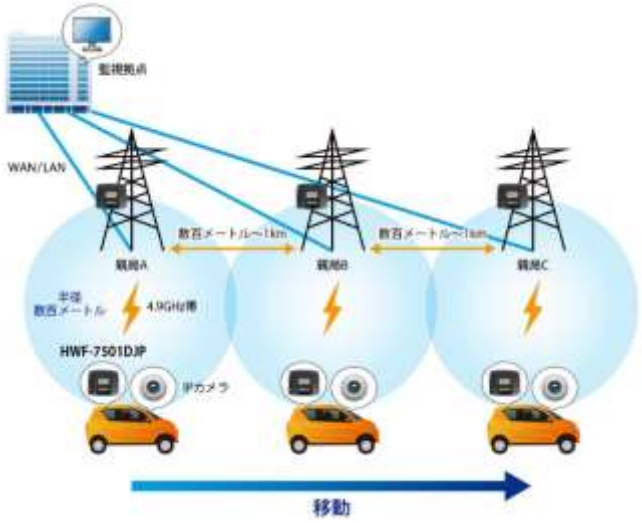
携帯電話の最大の利点は，「いつでも，どこでも通話できる」ことである。たとえば，北海道に住んでいる A さんと沖縄に住んでいる B さんが，携帯電話で通話しているとする。この場合，A さんの携帯電話から発せられた電波は，すぐ近くにある「無線基地局」という大型のアンテナつきの無線通信装置に届くと，光ファイバーなどの有線ケーブルを伝って，さまざまな通信設備を経由する。そして，通話相手である B



さんの近くにある無線基地局までたどり着くと，再び電波となって B さんの携帯電話に届いて，通話が成り立っている。つまり，A さんの携帯電話も B さんの携帯電話も，近くにある無線基地局までの間だけに無線が使われており，それ以外の部分は有線のケーブルでつながっている。A さんと B さんがお互いに近い場所にいたとしても，互いの携帯電話が発する電波で直接つながっているわけではなく，やはり一番近い無線基地局を経由して通話している。そのため，災害などで有線の部分に障害が発生すると，携帯電話の通話にも支障が出る。 もしも，北海道から沖縄まで直接電波で通信できる携帯電話にしようとしたら，それだけの大きな電波出力を行える装置が必要になるので，ものすごく重く大きな端末となってしまう。少なくともポケットに入れて持ち歩くことはできない，つまり「携帯できない携帯電話」になってしまう。

日本での携帯電話の原点は，1985 年に日本電信電話公社から民営化した NTT がサービス開始した「ショルダーフォン」である。携帯電話といっても，現在のものとは比べものにならないほど大きく，重さが約 3kg もあった。通常は自動車に搭載しておき，必要に応じて肩からショルダーバッグのようにベルトを掛けて持ち歩くというもので，現在の携帯電話とはかなり違っていた。「携帯電話」という名称が使われるようになったのは，1987 年に NTT から発売された携帯電話専用機に始まり，重さは約 900g に軽量化されてからである。以降，さらに小型化・軽量化されて，普及の一途をたどっていく。

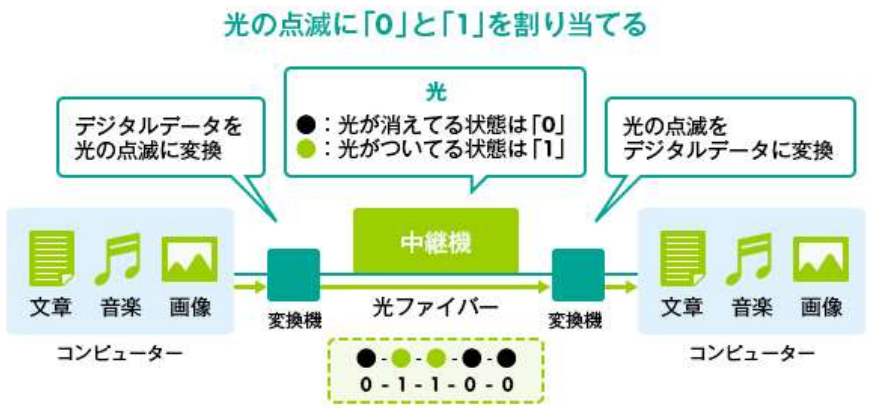
携帯電話ならではの利点は，移動しながら通話できることである。無線基地局がカバーするエリアは，広くても半径数十キロメートル，狭いところでは半径数メートルである。自動車で移動しながら通話していると，すぐに接続していた無線基地局の範囲外に出てしまう。ということは，たとえば A さんが自動車で B さんの住む沖縄に向かいながら通話していると，途中でたくさんの無線基地局を乗り換えながら通話を続けることになる。それでも通信が途切れたりしないのは，携帯電話は常に近隣の無線基地局の電波強度を測定し続けていて，電波がある一定の強度以下になると，それまでの回線を切断して，より強度の強い別の回線に切り替えるようになっているためである。常に次の接続の準備を行っているので，利用者に意識させることなく，スムーズに切り替えることができる。この仕組みは「ハンドオーバー」と呼ばれる。



FAX，コンピュータからレジ，ATM に至るまで，データ通信は私たちの生活のあらゆる場面で利用されている。データ通信は，電話と機能を補完し合うもので，電話とともに私たちの生活に必要不可欠なものとなっている。

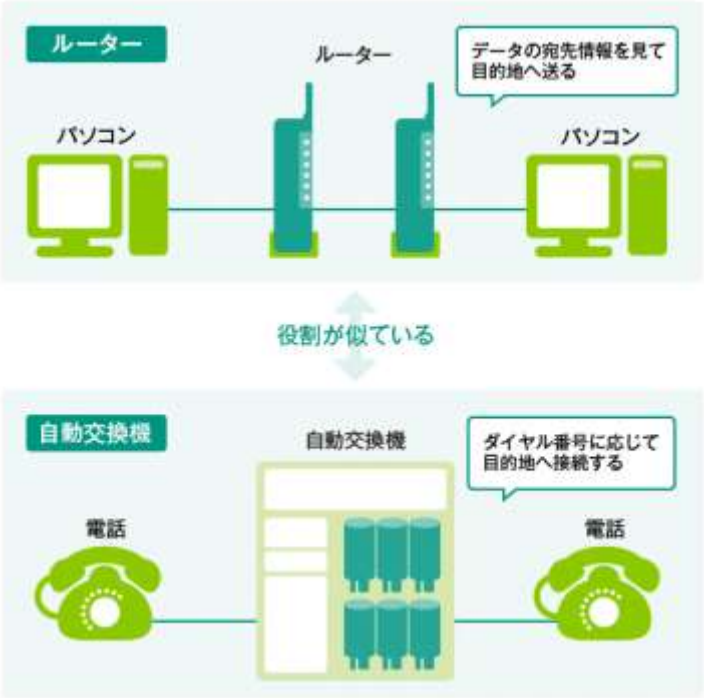
コンピュータなどの電子機器で処理されるデータは，文章も音楽も画像も全て「0」「1」という 2 つの数字だけで表現されるデジタルデータである。電話回線を使って音声化したデータを相手に話し，聞いた側で約束どおりにデジタルデータに戻せば，データをやり取りできる。電話回線は，人間が話した音声も，デジタルデータを変換した変な音声も区別せずに，同じように相手に届ける。コンピュータによるデータ通信ではモデムを使って，デジタルデータを音声にして電話回線に送信したり，受け取った音声をデジタルデータに変えたりする。データ通信は，モデム同士が電話で通話しているようなものである。

以前は，こうした仕組みを利用して電話回線でデータ通信を行っていた。しかし，電話回線を使ったデータ通信は通信速度に限界があったため，データ量の大きな画像や動画をやり取りすることが難しくなってき。こうした点を解消すべく登場したのが，光ファイバーを使った光通信である。光ファイバーは，デジタルデータを音の高低に割り当てるのではなく，光の点滅に割り当てる。「0」は光が消えている状態，「1」は光がついている状態に割り当てることで，デジタルデータのまま通信することができる。こうした技術によって，現在は画像や動画といった大容量のデータ通信が可能となった。



インターネットの基礎になっているのは，データ通信である。デジタルデータを音声，電気，光などの信号に変換して別のコンピュータに送信している。しかし，インターネットのように世界中にあるコンピュータにデータを届けるには，追加しないといけない機能がいろいろある。まず，データを送信する相手を見つけて，そのデータを送ってくれる仕組みが必要になる。「ルータ」という機器がその役割を果たしている。家庭や会社など，ひとまとまりのネットワークの出入口にはこのルータがあり，外部に出るデータをすべて受け取っている。そして，受け取ったデータに書かれている宛先情報を見て，目的地に近い別のルータに送り出すということを繰り返して，目的地までデータをリレーのようにして送っている。ルー

タの役割は電話の「自動交換機」とよく似ている。もちろん，機械としてはルータと交換機はまったく別のものであるが，宛先情報から目的地まで，機械が次々に連携して，情報を送信相手まで送り届ける，という役割は非常に似ている。



課　題

1．通信の仕組みについて説明しなさい。

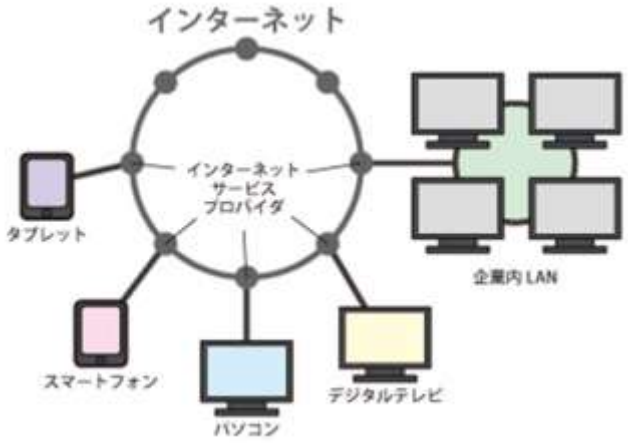
第 10 講　インターネットと Web ブラウザ

【学修到達目標】

- インターネットの仕組みを理解できる。
- Web ブラウザを利用してできることについて説明できる。

1．インターネット

複数のコンピュータを，ケーブルや無線などを使ってつなぎ，お互いに情報をやりとりできるようにした仕組みをネットワークと呼ぶ。インターネットは，家や会社，学校などの単位ごとに作られた１つ１つのネットワークが，さらに外のネットワークともつながるようにした仕組みである。外のネットワークと接続するために，ルータと呼ばれる機器や，インターネットサービスプロバイダと呼ばれる通信事業者のサービスを利用する。世界規模でコンピュータ同士を接続した，最も大きいネットワークである。



ネットワーク上で，情報やサービスを他のコンピュータに提供するコンピュータをサーバ，サーバから提供された情報やサービスを利用するコンピュータをクライアントと呼ぶ。私たちが普段使うパソコンや携帯電話，スマートフォンなどは，クライアントにあたる。インターネット上には，メールサーバや Web サーバといった，役割の異なる多数のサーバが設置されている。それらのサーバが，クライアントからの要求に従って，情報を別のサーバに送ったり，持っている情報をクライアントに渡したりすることで，電子メールを送信したり，Web ブラウザでホームページを見たりすることができるようになっている。

インターネットでは，コンピュータ同士が通信を行うために，TCP/IP（ティーシーピー・アイピー）という標準化されたプロトコルが使われている。プロトコルとは，コンピュータが情報をやりとりする際の

共通の言語のようなもので，この仕組みを利用してインターネット上で，機種の違いを超えて，さまざまなコンピュータが通信を行うことができるようになっている。インターネットで，情報の行き先を管理するために利用されているのが，それぞれのコンピュータに割り振られている IP アドレスと呼ばれる情報である。この IP アドレスは，世界中で通用する住所のようなもので，次の例のように表記されるのが一般的である。

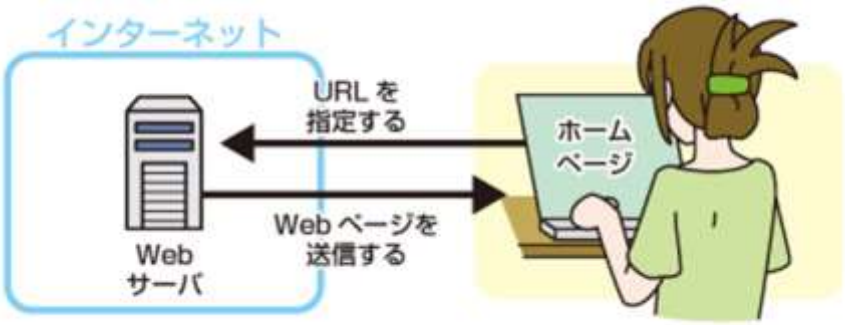
IP アドレスの例： 198.51.123.1

この IP アドレスは，コンピュータで処理するのには向いているが，そのままでは人間にとって扱いにくいので，ホームページや電子メールを利用するときには，相手先のコンピュータを特定するために，一般的にドメイン名が使われる。ドメイン名を使用した記述方法では，例えばホームページのアドレスでは“www.soumu.go.jp”のように指定する。ネットワーク上には，これらのドメイン名と IP アドレスを変換する機能を持つサーバ（DNS サーバ）があり，ドメイン名を IP アドレスに自動的に変換することで，電子メールの送り先やホームページの接続先を見つける仕組みになっている。近年，インターネットに接続する情報機器が爆発的に増えてきたことで，IP アドレスが足りなくなってきていることが問題になっている。使える IP アドレスの数を増やすために，IP アドレスの桁数を増やした IPv6 という規格が導入されている。IPv6 方式の IP アドレスは，次のように表そされる。

IP アドレスの例： 2001:db8:bb5c:8008:2013:a219:2210:8103

2. Web ブラウザ

インターネット上で情報を公開する仕組みを，ホームページと言う。ホームページのコンテンツ（内容）は，インターネット上に点在する，Web サーバというホームページ公開専用のコンピュータのなかに保存されている。端末から，そのパソコンに命令を出し，情報を送ってもらうことで，ホームページを見ることができる。ここでいうホームページとは，Web サイトと呼ばれるインターネット上のひとまとまりの Web ページのことである。元々は，Web サイトの入り口のページをホームページと呼んでいたが，日本では Web サイトと同じ意味で使われるようになった。 ホームページを閲覧する場合には，Web ブラウザという専用のソフトウェアで URL を指定する。URL を指定すると，Web ブラウザがインターネット上の Web サーバを探して，目的のホームページをコンピュータの画面上に表示する。URL は，「http://www.soumu.go.jp/joho_tsusin/joho_tsusin.html」のように指定する。「http」は，ホームページの閲覧に使用される HTTP というプロトコルを表している。「www.soumu.go.jp」は Web サーバを指定している。その後の「/joho_tsusin/joho_tsusin.html」が Web サーバの中のホームページの情報が保存されている場所を表している。このような URL を Web ブラウザで指定することで，自分が見たい Web サイトへ接続できる。URL の最後には「.htm」や「.html」という表記がよく見られるが，これはそのホー



ムページが，主に HTML 形式のファイルで作られていることを表している。この HTML ファイルの中には，画像や動画，音声などのマルチメディア情報を指定することができ，これにより，ホームページ上で多彩で動きのあるコンテンツを利用することができる。また，Web ページを見るのに，１つ１つちがう URL を Web ブラウザに入力するのは大変である。そこで，Web ページの中のテキストやイラスト，図などに URL の情報を埋め込んで，ここをクリックしてもらうことで，利用者を別の Web ページに誘導することができる。この仕組みはハイパーリンク（リンク）と呼ばれる。これにより，現在見ている Web ページから，関連する他の Web ページや Web サイトに移動することができる。

ブラウザとは，一般にウェブページを見るためのソフトの総称である。英語の「browse（閲覧する・拾い読みする）」が語源で，動詞の browse を名詞にして「ブラウザ（browser）」となった。正式名称は，「インターネットブラウザ」「Web ブラウザ」と呼ぶ。代表的なものとしては，Google Chrome，Microsoft Edge，Safari などがあり，PC やスマホでホームページを見る際には欠かすことができない。もともとブラウザは単にホームページを閲覧するだけのツールであった。しかし，現在では様々な用途で利用されており，Youtube などの動画を見たり，ブラウザ上でゲームを楽しんだりすることもできる。ビジネスにおいては，勤怠管理システムや経費申請，労務管理システムなどもブラウザを介して操作されることが増えてきた。ホームページの制作もブラウザ上で行えるようになってきた。ブラウザは，次のような機能・役割を持っている。

１）HTML などの言語で記述されたテキストを Web ページに変換する

HTML とは「Hyper Text Markup Language」（ハイパーテキスト・マークアップ・ランゲージ）の略語で，ホームページを作成するための専門言語である。HTML で記述されたテキストは，その知識が無い一般の人が見ても理解することはできない。ブラウザは，コンピュータでしか解読できないテキストを Web ページに変換して表示する役割がある。

２）サーバにリクエストを送信し，必要な情報を受信する

サーバとは情報やサービスを提供するコンピュータを指す。サーバに必要とする情報を要求して，ファイルを受信するのもブラウザの役割のひとつである。

3）ハイパーリンクを機能させる

ハイパーリンクとは，文書データなどの情報の中に埋め込まれた，他の文章や画像を参照できる文字列のことである。ブラウザは，インターネット上にある膨大な情報の中からハイパーリンクの参照情報を読み取って表示させる機能がある。

4）プラグインと拡張機能のサポートをする

ブラウザは通常，プラグインや拡張機能をサポートしている。これらによってユーザーがブラウザをカスタマイズし，新しい機能を追加することができる。例えば，広告ブロッカー，パスワードマネージャー，ウェブ開発ツールなどが挙げられる。ブラウザの拡張機能は，ユーザーにとって非常に便利なものとなっている。

5）セキュリティとプライバシーを保護する

ブラウザはセキュリティとプライバシー保護の重要な役割を果たしている。ブラウザは不正なウェブサイトをブロックし，セキュリティ証明書を確認してユーザーを保護する。また，プライバシーモードやトラッキング防止機能を提供して，ユーザーのプライバシーを守る手助けを行っている。

ブラウザにはいろいろな種類があり，普段使用する機会の多いブラウザは次のものである。

1）Google Chrome は，国内・海外ともにもっとも利用者の多いブラウザで，Android のスマートフォンやタブレットの多くで Chrome が標準ブラウザとされており，動作も軽快なためパソコンでも多くの利用者を獲得している。そのため，殆どの Web サービスは Chrome に対応している。標準の検索エンジンが Google なので使いやすく，Gmail や Google カレンダーなどの各種 Google サービスとも連携している。

2）Microsoft Edge

Windows の標準ブラウザが，Microsoft Edge である。Internet Explorer の後継である。機能性や表示速度が向上しており，ユーザーも徐々に増えてきている。Microsoft Edge は標準の検索エンジンが Bing で，検索結果は Google や Yahoo!とは異なる。そのため，いつも Google で検索している人は，Microsoft Edge だとうまく表示されない，ということが稀にある。

3）Safari

Safari は iPhone や iPad，Mac のパソコンなどの Apple 社製品の標準ブラウザである。日本では iPhone のシェアは Android と同じくらいなので，「スマホだと Safari をメインで利用している」という人も多い。iPhone などの iOS 端末との連携がしやすいのが最大の特徴で，Android のスマートフォン・タブレットでは利用することができない。

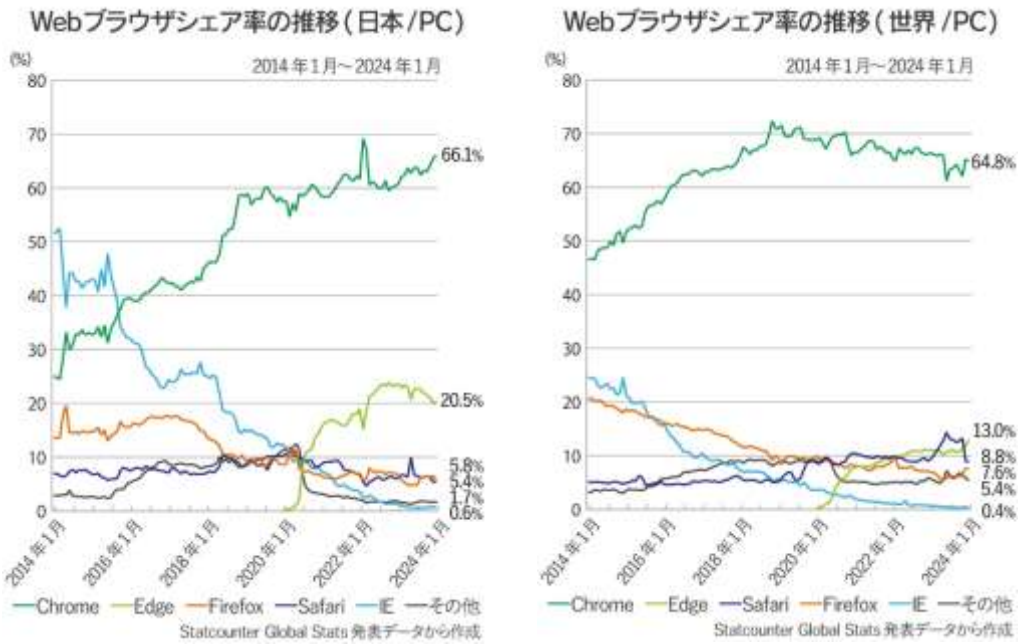
4）Firefox

Firefox は Mozilla Foundation が開発・提供している。豊富な拡張機能を自由に追加できるため，長年人気を得てきた。現在では，他のブラウザも拡張機能が充実してきたので，かつてほどの優位性は失われてきた。

5）Internet Explorer

1995 年から長期に渡って使用され続けた Internet Explorer は，全盛期には 95%のブラウザシェアを誇る，圧倒的な存在であった。しかし，セキュリティの問題がクローズアップされたこともあり，徐々にシェアを減らし，2022 年 6 月 16 日にサポート終了した。

2024 年 1 月の PC における Web ブラウザ使用率ランキングは，Google Chrome の 1 位は変わらないものの，Microsoft Edge が世界の 2 位に浮上した。これは，Microsoft Edge に最新の生成 AI「Copilot」を搭載したことが影響しているといわれる。



参考：Statcounter Global Stats　Browser Market Share

3. AI の実装

Microsoft Edge は最新の生成 AI「Copilot」を搭載したことで，便利な使いやすいブラウザに変わった。Microsoft Copilot は，かつて Bing AI と呼ばれていたものがアップデートを重ねて，ブラウザとシームレスに連携できるように進化した文章も画像も生成できる AI である。ChatGPT と違うところは，ネット

の検索結果から回答できて，より高性能な AI を無料で使うことができる点である。Copilot の中身は OpenAI 社の生成 AI「GPT-4 Turbo」である。これは無料版の ChatGPT に搭載されている「GPT-3.5」よりも，回答速度と性能が大幅に向上したバージョンである。ChatGPT で GPT-4 Turbo とネット検索を使うには，有料プラン（ChatGPT Plus）に入る必要があります。Copilot ならどちらも無料で利用できる。

Edge で使える Copilot の機能は以下の 7 つである。

1） Copilot とのチャット

Copilot の基本となる画面で，Microsoft アカウントにログインしていれば，右上の青いマークからだれでも無料で使うことができる。Copilot の最大の特徴が，回答を出すときにネットで必要な情報を集めてくれることである。また Web ページを開いた状態で Copilot を開くと，そのページの内容を要約したり，YouTube を開いていたら動画の内容の要約をしたりできる。文章を貼り付けて，背景にある文脈を推測してもらうこともできる。

2） 日本語チャットで画像生成

テキストから画像生成する機能である。1 日の生成回数には制限がある。英語だけでなく日本語にも対応している。Copilot のチャット画面から「〇〇の画像を生成して」と入力するだけで簡単につくることができる。中身は OpenAI（ChatGPT の開発元）の最新画像生成 AI「DALL-E 3」なので，クオリティは高い。Copilot AI エクスペリエンスの使用条件 によると，生成した画像に対する所有権について Microsoft は主張しないとされているため，商用利用も一応可能である。ただし既にある画像と似た画像が生成される可能性もあるため，使用は自己責任になる。AI を利用した画像生成や動画生成は，法的な整備が進んでおり，最新の情報に注意すべきである。よく寄せられる質問: AI，Microsoft Copilot，Microsoft Designer - Microsoft サポート の「Microsoft Designer で作成された作業を使用するにはどうしたらいいですか？」の項目でも，『Microsoft の許容される使用ポリシーを除き，Microsoft の条件は，これらのサービスで作成された画像の商用化を制限しませんが，お客様は，使用シナリオと関連管轄区域の法律を考慮して，出力コンテンツに含まれる IP 権利とその商用の使いやすさに関して独自の決定を行う必要があります。』との記載がある。

3）選択文字の検索

ブラウジングしている最中に出てきた気になる単語をその場で Copilot に聞ける機能である。単語をマウスで選択後に右クリックすると，「Copilot に質問する」が出てくる。これを選択するとサイドバーで Copilot がその単語の概要をまとめてくれる。しかし，下に出てくる「Web で〇〇を検索」をクリックする方が速く正確な情報が得られる場合がほとんどである。ただググっても理解できないような難しい単語のような場合は，意外と Copilot の方がわかりやすくまとめてくれることもある。

4）文章の作成

Copilot を開くと「チャット」の横にある「作成」から利用できる。情報の正確性が担保できないので，ここで出力した文章をそのまま商用利用するのは気をつける必要がある。

5）文章の書き換え

ブラウザ上のメモアプリやフォームなどに入力した文章を選択すると，「Copilot で書き換える」というポップアップが出てきます。（ショートカットは Alt + I）。文章を書いている中でしっくりくる言い回しが思いつかないときに便利である。「Copilot で書き換える」が出てこない場合は，設定> 言語> 文書作成支援 から「Web 上で Compose (AI による書き込み) を使用する」という項目にチェックを入れると有効になる。

6） PDF の読み込み

PDF を開いたときに出てくる「Copilot に質問する」をクリックすると，PDF の内容を Copilot に読み込ませることができる。要約が主な使い方である。Web 上の PDF を読み込む際は，オープンな場所にある PDF を開いているか注意する。大学や会社内のサーバに置かれた PDF の場合，認証が必要なので Copilot が参照できない場合がある。またローカルの PDF を読み込むことも可能である。エクスプローラーで「プログラムを開く」から Microsoft Edge を選択する。

7）ブラウザの操作

ブラウザの操作もできる。例えば「ダークモードにする」や，たくさんタブを開いている状態で「ニュースに関連するタブをグループ化する」などが対応している。

SGE（Search Generative Experience）は，Google が公開した新しい検索機能である。SGE はユーザーの検索に対して生成 AI を取り入れ，AI が検索者の欲している情報の意図を読み取り，自動的に最適な回答をしてくれるのが特徴である。生成された回答に対して，チャット形式で追加の質問をしてさらに精度の高い情報を取得できる。SGE には次の機能がある。

1）検索ページトップに表示

SGE を使用しているユーザーは，検索したトピックについての情報をより早く効率的に理解したり，さらに知りたい情報に簡単にアクセスできるようになる。トップに出てくるので，まずは AI の回答を確認して，足りない情報等があれば，自分で検索するといった使い方ができる。

2）会話形式の追加質問

SGE では，検索したワードに対し，重要な情報の概要を作成する。そしてその下に，追加で質問できる候補を提示してくれる機能を搭載している。また，この候補の中に自分が聞きたい質問がない場合は，「追加で聞く」をクリックすることで，チャット形式で質問をすることができる。この際，質問から質問へと文脈が引き継がれるため，自然な検索を続けることができる。

3）責任あるアプローチ

Google は，SGE を導入するにあたって慎重なアプローチをとっている。ChatGPT や Bard のような AI によって生成された回答が常に正しいものではない。これらハルシネーションと呼ばれる間違った情報を生成する現象を，Google は広くアナウンスしている。継続的にアップデートを進めるとともに，すべての検索に生成 AI による回答を表示させるのではなく，質問の種類に応じて，生成 AI による回答を表示させないようにしている。さらに，AI が生成した回答のソースを一緒に表示することで，ユーザー自身がその回答が本当に正しいのか確認できるようにもしている。生成 AI による回答がトップページに表示されてしまうと，ユーザーは広告からではなく，AI の回答結果から Web ページにアクセスするようになってしまうのではないかという懸念が，SGE の発表当初から取りざたされていた。Google の回答としては，広告はウェブが機能するための重要な要素だと考えており，SGE が導入されても，広告は引き続き広告専用枠に表示されるとしている。

４）Google SGE に画像生成機能が追加された。画像生成には，Google が開発して一般には公開されていない Imagen が用いられている。生成された画像には，AI によって生成されたことを示すラベルが表示される。生成された画像は，Google ドライブなどにエクスポートできる。今後，画像を評価する機能も追加される。

課　題

１．Web ブラウザを利用してできることについて説明しなさい。

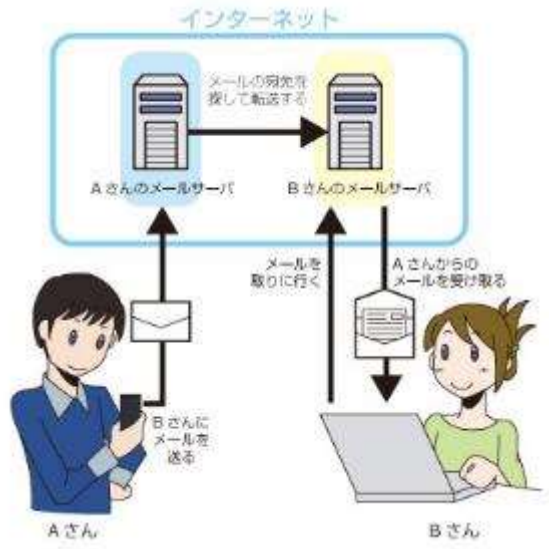
第 11 講　電子メールと SNS

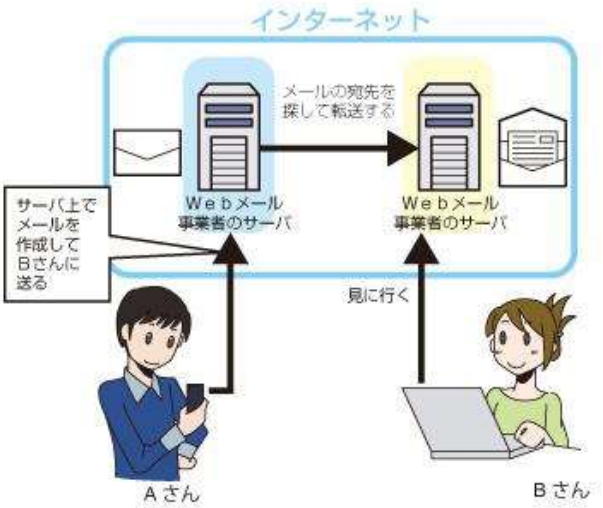
【学修到達目標】

- 電子メールの仕組みと利用の仕方を理解できる。
- SNS の特徴と注意点について説明できる。

1．電子メールの仕組み

電子メール(e-mail)とは，パソコンや携帯電話，スマートフォンなどの情報機器同士が，専用のメールソフトを使って，インターネットなどのネットワークを利用して情報をやりとりする機能である。やりとりできる情報は文章（テキスト）だけでなく，文書ファイルや画像などを添付ファイルとして扱うことができる。電子メールを送る際には，送り先のコンピュータを指定するためにアドレスを使う。電子メールのアドレスは，一般的に” xxx@example.co.jp”のように表記される。@の後には，所属する組織や利用しているインターネットサービスプロバイダなどの事業者のドメイン名が一般に使われる。また，一般的なメールソフトを使うのではなく，Web 上で Web ブラウザを使って送受信を行う Web メールという方式もあり，フリーメールサービスとして広く普及している。電子メールの送受信は，インターネット上の多くのメールサーバが連携することによって実現している。電子メールを送信すると，契約しているインターネットサービスプロバイダ，学校や会社にあるメールサーバにデータが送られる。電子メールを受け取ったメールサーバ





は，宛先として指定されているインターネットサービスプロバイダなどのサーバに，そのデータを転送する。電子メールを受け取ったサーバは，受取人が電子メールを取りにくるまで，サーバ内にデータを保管する。電子メールの受取人は，契約しているインターネットサービスプロバイダのメールサーバにある自分のメールボックスに自分宛の電子メールを取りに行く。

Web メールでは，送受信された電子メールがサーバに蓄積される。利用者は，Web サーバに Web ブラウザで接続することで，受信したメールの閲覧や，新規メッセージの作成・送信などができる。

電子メールは，さまざまな目的で広く利用されており，ビジネスにおいてはコミュニケーション，コラボレーション，情報共有の主要な手段である。電子メールは，社内外の顧客や同僚と情報を迅速かつ効率的に交換するために使用できる。パーソナルユースでは，友人や家族との連絡，ニュースや情報の受信，オンラインショッピングの確認などに利用される。電子メールは，連絡帳やリマインダーとしても機能し，予定やタスクを追跡するのに役立つ。また，マーケティングでは，宣伝や製品アップデートの送信，リードの育成，顧客関係の構築に使用されている。電子メールマーケティングは，パーソナライズされたメッセージングを大規模に配信する効果的な方法である。

電子メールは，人々が迅速かつ安価にコミュニケーションをとるのに役立つ便利なツールである。インスタントメッセージや電話とは異なり，電子メールは受信者が都合の良い時間にメッセージを確認できる。また，ドキュメントや画像などの添付ファイルを簡単に送信できるため，ビジネスや個人的な目的で使用できる。しかし，電子メールには欠点もある。スパムメールは，電子メールユーザーにとって迷惑である。さらに，電子メールはリアルタイムのコミュニケーションではないため，緊急の事柄には適していない。メッセージが盗聴や改ざんされる可能性がある。そのため，機密情報を含む電子メールを送信する際には注意が必要である。

電子メールのセキュリティを高めることは，オンラインでの安全を維持するために不可欠である。電子メールは悪意のあるアクタが攻撃するために利用される可能性がある。電子メールのセキュリティ対策として，以下のような対策がある。

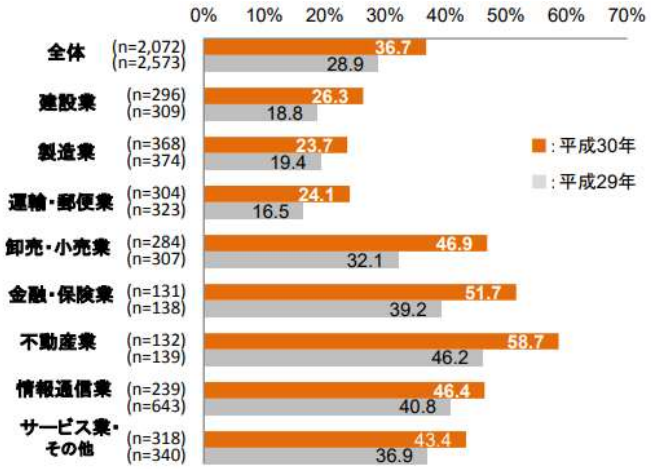
* 強いパスワードの使用推測不可能で複雑なパスワードを設定する
* 二要素認証の有効化パスワードに加えて，スマートフォンなどに送信されるコードも要求する
* 怪しい添付ファイルを開かない。見知らぬ送信者からの添付ファイルは，マルウェアを運んでいる可能性がある。
* フィッシング詐欺に注意銀行や政府機関を装ったメールで個人情報を要求する詐欺行為である
* 定期的なウィルス対策ソフトウェアの更新マルウェアやウィルスに対する保護を維持する
* スパムフィルターの使用迷惑メールや悪意のあるメールをブロックする

2. SNS

SNS は，ソーシャルネットワーキングサービス（Social Networking Service）の略で，登録された利用者同士が交流できる Web サイトの会員制サービスのことである。友人同士や，同じ趣味を持つ人同士が集まったり，近隣地域の住民が集まったりと，ある程度閉ざされた世界にすることで，密接な利用者間のコミュニケーションを可能にしている。最近では，会社や組織の広報としての利用も増えてきた。多くの SNS では，自分のホームページを持つことができ，そこに個人のプロフィールや写真を掲載する。ホームページには，公開する範囲を制限できる日記機能などが用意されていたり，アプリケーションをインストールすることにより，機能を拡張したりすることもできる。その他，Web メールと同じようなメッセージ機能やチャット機能，特定の仲間の間だけで情報やファイルなどをやりとりできるグループ機能など，多くの機能を持っている。さらに，これらの機能はパソコンだけではなく，携帯電話やスマートフォンなど，インターネットに接続できるさまざまな機器で，いつでもいろいろな場所で使うことができる。

アドレスを知らないと送れない Web メールとは異なり，SNS アカウントは基本的にオープンで，アカウントを見つければ気軽にフォローできる。LINE は，個人間でクローズドなやりとりができるため SNS に見えないかもしれないが，「オープンチャット」や「LINE VOOM」を活用すれば不特定多数のユーザーとコミュニケーションをとることができる。YouTube は「動画投稿サービス」のイメージがあるので，SNS のイメージは薄いかもしれないが，コメント欄などで自由に交流できる点で「SNS」に分類される。

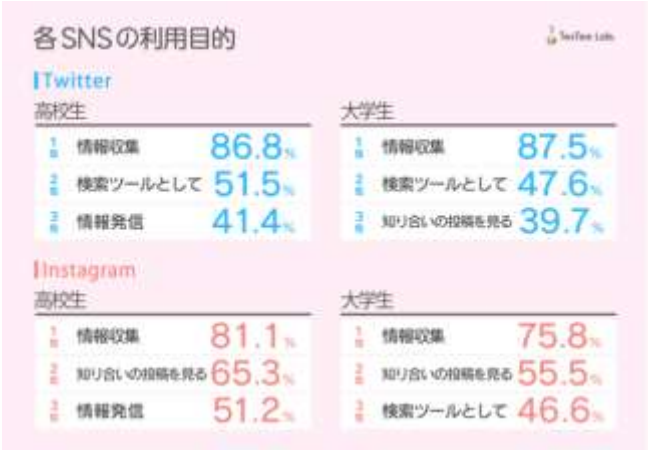
個人だけでなく，企業の SNS 利用も増えている。企業の SNS アカウントが増加すると，発信する内容を差別化しないと埋もれてしまう可能性が高まる。ビジネス目的で SNS を利用する際は「SNS 分析」を利用することが多い。



（引用元：総務省　平成 30 年通信利用動向調査）

SNS では「情報の発信・検索」と「ユーザー同士での交流」ができる。SNS では，自由に情報発信ができ，自分の考えていることや見せたい写真・動画などをインターネット上で公開できる。SNS は，情報発

信だけではなく情報収集にも役立つ。株式会社テスティーの調査によると，若い世代を中心に SNS を情報収集ツールとして活用している。



（参考：【2021 年】最新！高校生・大学生の SNS 利用目的とは？｜株式会社テスティー）

SNS アカウントを持っているユーザー同士で交流することができ，主な機能は下記 5 つである。

・「いいね」機能で共感を示す

・「拡散」機能で他の人に情報を共有する

・「返信（リプライ）」で反応する

・「フォロー」して交流を深める

・「ダイレクトメッセージ」で直接連絡する

SNS によって使える機能や内容が若干異なる。どの SNS でも適度な距離感・マナーを守って交流する必要がある。

主要な SNS サービスとして，Facebook（フェイスブック）がある。Facebook の特徴は，実名でのアカウント登録が基本であることで，他の SNS よりも「本人」と確認しやすいので，実生活で知っている人へ向けて投稿したい場合や近況を知りたい場合に向いている。また，短文を気軽に投稿するというよりは長文の投稿が多い。日本国内で Facebook を利用するユーザー数は 2,600 万人(2019 年 7 月公式発表)。利用者層は，他の SNS と比べて 40-50 代の中高年層が多い。実名制であることから，ビジネス目的で利用するユーザーが多い。企業で Facebook を活用する場合は「Facebook ページ」を作る。企業のホームページのように使える。Facebook アカウントはあくまで「個人」単位で，Facebook ページを持つと，イベントの集客や広告配信も可能になる。

Instagram は，写真や動画の共有がメインの SNS であり，視覚的にオシャレなコンテンツが豊富で，近年はストーリーズやリールなど縦型動画フォーマットが増えている。女性だけでなく 30-40 代の男性の利用も多い。Instagram の特徴は，ハッシュタグであり，ユーザーはタグ検索が可能である。

Twitter は 140 文字以内のテキストで簡単につぶやける。そのため,タイムラインに投稿が流れるスピードは早い。ニュース情報もすぐに入ってくるので「リアルタイム」な情報をスピーディーに知ることができる。ツイッターは 10 代・20 代の若者のアカウント所有率が高い。Twitter の特徴は，リツイート機能であり，ボタン一つでユーザーの投稿を気軽に拡散できる。

LINE（ライン）は家族や友人などとの連絡に使われることが多い。そのため，他の SNS サービスに比べてアクティブユーザー率が高い。LINE は日本国内で月間 9,200 万人以上（2022 年 3 月末時点・公式発表）が利用するコミュニケーションアプリで，これは日本の総人口の約 7 割にあたる。多くの人が日常的に利用する「コミュニケーションインフラ」といえる。企業が LINE を活用する場合は「LINE 公式アカウント」を利用する。個人の LINE アカウントとは異なり，メッセージの一斉配信やリッチメッセージ，クーポン配信などビジネスで役立つ機能が使える。YouTube（ユーチューブ）は，世界最大級の動画投稿プラットフォーム。他の SNS に比べて長尺の動画が投稿される傾向にある。近年は，多くのファンを獲得する「YouTuber（ユーチューバー）」の存在感も増してきている。日本における YouTube の月間利用者数は 6,500 万人以上（2020 年 9 月時点,Think with Google より）。年齢・性別問わず多くのユーザーに利用されている動画プラットフォームである。コネクテッド TV が普及し，テレビ画面で YouTube を視聴するユーザーも多い。2020 年 3 月時点で，1,500 万人以上がテレビ画面で視聴しているとされる。最近では，テレビ CM を YouTube に出稿することで普段テレビを見ないユーザーにアプローチする事例も増えている。

TikTok（ティックトック）は，ByteDance 社が提供するショートムービーに特化した SNS で，15 秒～10 分の短尺動画を作成・投稿できるプラットフォームである。ユーザーは動画を撮影する際，0.3 倍速～3 倍速と速さを調節したり，フィルターやメイク機能を用いたりできる。また，豊富なラインナップから好きな BGM を付けられる。10-20 代の若年層が利用している。TikTok 上で影響力のあるインフルエンサーを「TikToker（ティックトッカー）」と呼びます。特に若年層からの人気が高いため，タイアップする企業も増えている。

SNS を始める手順は次とおりである。始めたい SNS アプリをダウンロードする。アプリをインストールしたら，SNS アカウントを作成する。そして，メールアドレス，パスワード，アカウント ID 等を入力する。パスワードは漏洩するとアカウントがのっとられるリスクがある。特に，他の人と SNS アカウントを共有する場合は推測しやすいパスワードは避けたり，二段階認証を設定したりする。SNS アカウントを作成したら，プロフィールを作成する。プロフィールは，他のユーザーへの自己紹介ページである。「プロフィール画像」や「プロフィール文」を入力する。ビジネス利用の場合はホームページや電話番号なども登録する。プロフィールの設定ができたら，実際に投稿する。

不特定多数の人に見られるのが怖い場合，「鍵アカウント」にする。フォローリクエストが来て承認する形になるので，知らない人からフォローされていた，という事態を防げる。Facebook は鍵アカウントに

できないが，プロフィールや投稿の「公開範囲」を指定できる。ただし，企業アカウントは鍵アカウントに出来ないこともある。

企業で SNS をやりたい場合，個人の場合と異なる点がいくつかある。個人アカウントとは異なり，企業用のアカウント・ページがあることも多い。

・Facebook：Facebook ページ
・Instagram：プロアカウント（ビジネスアカウント）
・Twitter：Twitter プロ
・LINE：LINE 公式アカウント
・TikTok：ビジネスアカウント
・YouTube：ブランドアカウント

企業用アカウント・ページは，ショッピング機能を使えたり分析機能が充実している。個人アカウントに比べ，ビジネスで役立つ機能が揃っている。

企業アカウントは，炎上するとブランドイメージダウンにつながる。投稿の内容は，センシティブな話題（例：差別・宗教・スキャンダル・政治など）を避ける。

最近では，利用者同士が交流しながら遊べるソーシャルゲームも普及している。SNS は，とても身近で便利なコミュニケーション手段であると言えるが，アカウントの不正利用や，知り合い同士の空間であるという安心感を利用した詐欺やウィルス配布の被害に遭うなどの事例が発生している。また，友人間のコミュニケーションを目的として SNS を利用している場合であっても,プライバシー設定が不十分であったり, 友人から引用されることなどにより, 書きこんだ情報が思わぬ形で拡散する危険性もある。インターネット上に情報が公開されていることに変わりはないということを念頭に置いて，書き込む内容には十分注意をしながら利用することが大切である。

SNS を利用する時に特に気をつけるべきことは「①ネットの情報をうのみにしない」「②犯罪被害にあわない」「③誹謗中傷に気をつける」「④個人情報を公開しない」である。

①ネットの情報をうのみにしない

SNS を含むインターネットでは誰でも匿名で情報を公開することができる。そのため，デマやフェイクニュースといった嘘の情報や，有名人になりすました偽アカウントも多数存在する。特に，災害や事件が起こった時にこうした偽情報が多くでまわる傾向があるため「情報の出どころ」や「周りの反応」「公的機関のアナウンス」などをよく調べ安易に拡散しないことが重要である。

②犯罪被害や詐欺に気をつける

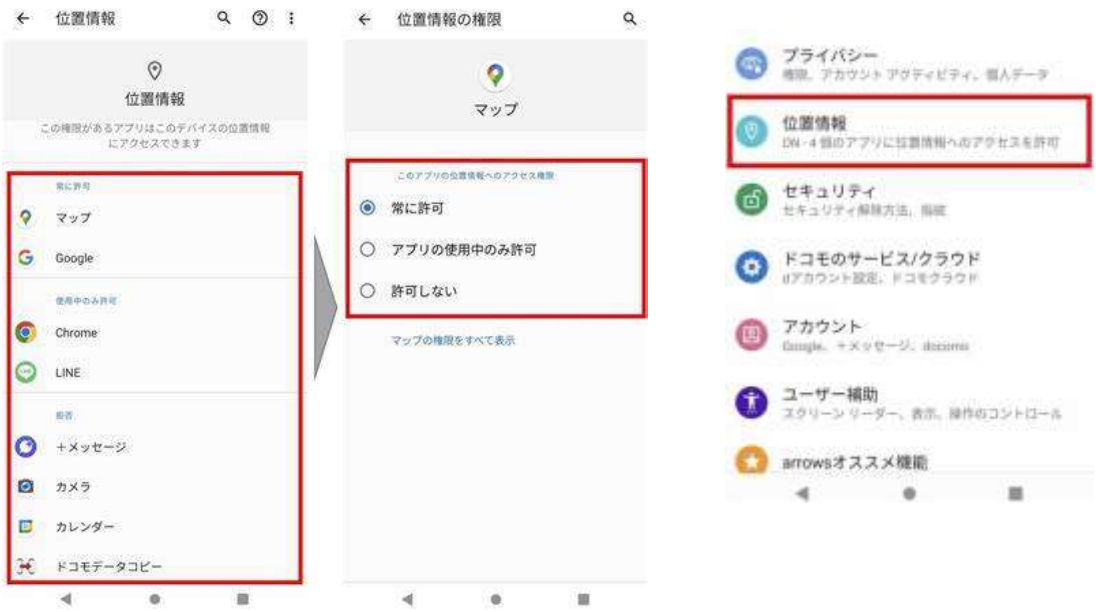
SNS を利用している人の中には悪意をもった人物も少なくない。特に，個人的なやり取りができる DM（ダイレクトメッセージ）を使った誘い文句や勧誘には十分気をつける必要がある。

③ネットに書き込む前に注意すること

SNS やネット上に文章を書き込む際には「一度投稿した内容は簡単にコピー・転載され，一生残り続けるかもしれない」という点に注意することが重要である。特に，ネット上では「有名人の不倫や失言」といったネガティブな話題が拡散され炎上に至る傾向がある。そのような時に，悪い行いをしたからといって直接その人物の SNS アカウントに攻撃的なコメントをつけてしまうと誹謗中傷と判断されてしまう恐れがある。

④写真を公開する時に注意すること

SNS に写真を投稿する時に注意することは「①位置情報」「②画像検索」「③顔認識技術」である。スマホで撮影した画像には GPS や Wi-Fi から取得した位置情報が追加される。そのため，たとえ写真の中に場所が特定できそうな目印が写り込んでいなかったとしても，特定のツールを使うことで撮影場所が特定されてしまう危険性がある。心配な場合は，スマホやアプリの設定から「位置情報をオフ」にする。また，Google などの検索エンジンには同じ画像を使ったページを割り出す「画像検索」という機能がある。ツイッターとインスタグラムに同じ画像を掲載していると，画像検索をかけた際にもう一方のアカウントがバレてしまうリスクが存在する。近年では SNS や画像加工アプリなどを中心に顔認識技術が利用されるようになっている。この顔認識によって同一人物であることが簡単に判明してしまうため，顔写真を公開する際にはその点にも注意を払う必要がある。



課　題

1．電子メールの仕組みと利用の仕方について説明しなさい。

2．SNS の特徴と注意点について説明しなさい。

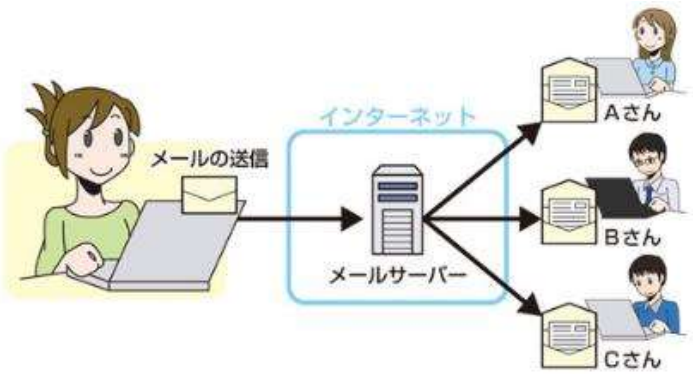
第 12 講　メーリングリストとネットを利用したサービス

【学修到達目標】

- メーリングリストの仕組みと利用の仕方を理解できる。
- ネットを利用したサービスの仕組みを知り，安全に利用できる。

1．メーリングリスト

メーリングリストは，電子メールを利用したコミュニケーションツールである。通常の電子メールで複数の相手に電子メールを送る場合には，全員分のメールアドレスを指定して送信するが，メーリングリストでは専用のメールアドレスに送信することで，そのメーリングリストに登録されているすべてのメールアドレスに同時に送信することができる。メーリングリストでは，投稿した電子メールは全員に送信されるため，特定の相手に対して返信したつもりでも，すべての参加者にその電子メールが送信されることになる。また，最近はメーリングリストにウィルス付きの電子メールが投稿されて，参加者全員にウィルスが配信されてしまうというトラブルが発生している。メーリングリストに参加する場合には，他の利用者に対する責任があるということを認識しておく必要がある。



メーリングリストを活用するメリットとして，手間なく複数人に対して一斉メールの配信が可能で，メール発信にかかる時間を短縮できますし，導入コストもかからない。宛先ミスによってメールアドレス情報が公開されるリスクも軽減できる。メーリングリストは配信の手間は減る一方で，リストへの追加や削除といった管理が面倒である。受信相手の環境によって迷惑メールフォルダに入ってしまうことがあり，メールが確認されない可能性がある。効果分析が必要なメルマガやメールマーケティングには不向きなこともデメリットになる。

メーリングリストに似た機能を持つものに，グループメールがある。グループメールもまた，複数名に対してメールを送ることが可能である。しかし，次の点で異なっている。グループメールは，誰でもグループメンバー宛にメールを送信できるが，メーリングリストは登録者のみである。届いたメールに返信した場合，返信メールの発信元はグループメールアドレスになるが，メーリングは各返信者のメールアドレスになる。

メーリングリストの作り方は，使用するメールソフトによって異なる。Gmail では「Google グループ」を作成し，グループメールアドレスを用いることでメーリングリスト機能が使用できる。なお，Gmail に限らずどのようなアドレスでもグループに登録が可能である。

Outloook はメーリングリストではなく，Microsoft 365 グループを設定することで同様の機能が使用できる。この機能は社内での活用に適しており，このほかにメールアドレスをグルーピングする連絡先グループ機能もある。

手順

1) Outlook on the web を開く
2) 「グループ」→「新しいグループ」をクリック。受信トレイ等に並んで「グループ」一覧が表示される。
3) グループ情報を入力。分かりやすいグループ名，および説明を入力。
4) 「作成」をクリック。メンバーに追加したい人の名前もしくはメールアドレスを入力し，「追加」をクリック。なお，メンバーの追加はグループ作成後でも可能。
5) 「メールを送信」を押してメールを作成。グループが作成されたら，「メールを送信」からグループメンバーにメールを送れる。

Outlook には，パソコン用ソフトで作成できる「連絡先グループ」がある。「Microsoft 365 グループ」とは機能が異なり，連絡先グループは複数ユーザーにメールを送信できるが，あくまで複数の連絡先を 1 つにまとめて管理・送信しているものである。メーリングリストのように，特定のメールアドレスに送信すれば全員に届くわけではない。また，連絡先グループは個人毎の管理となるので，メンバー全員でメールを共有する場合，各自がメンバーを含めた連絡柵グループを作成する必要がある。

メーリングリストやグループメールは，複数人に対してメールを一斉配信でる。そのため，メールによる情報の伝達・共有が効率化できる。ただし宛先間違いによる誤送信などにより，情報漏洩リスクが伴う。また，リスト数が増えたり，メンバーが増えてくると，管理の手間になる。そのため，オペレーションが複雑になるようであれば，専用のメール共有システムを活用した方が良い。専用システムであれば一斉配信だけでなく，メールの共有・管理等をより便利に行える機能が豊富に揃っている。

2．ビジネスメール

メールやメーリングリストをビジネスで利用するときには，ルールがある。

ビジネスメールは「宛先」「件名」「添付ファイル」「宛名」「挨拶と名乗り」「要旨と詳細」「結びの挨拶」「署名」「返信・転送」で構成されている。

①宛先（To，Cc，Bcc）を正しく使い分ける

To は宛先で，複数のメールアドレスを入力することができる。宛先は，そのメールに対応して欲しい人にする。Cc は，Carbon Copy（複写）の略で，複写なので，To の人のように対応を求めないものの，状況を把握しておいて欲しい人や情報を共有したい人のメールアドレスを入力する。Bcc は，Blind Carbon Copy（見えない複写）の略で，To や Cc の宛先を入れた人に送ったことを知られたくない場合に使う。To や Cc に入れた人からは，Bcc の人のメールアドレスは見えない。Cc と Bcc の違いは，ほかの人から見えるか見えないかである。To と Cc は，受け取った人全員にそれぞれのメールアドレスが見える。しかし Bcc の場合，To や Cc の人は Bcc の人がメールを受け取ったことを知らない。Bcc で受け取った人が To や Cc の人に返信してしまうというミスが起こりえる。また，Bcc で送るつもりが Cc に入れてしまって情報漏洩するということもあるので Bcc は基本的には使わない。

②具体的な件名を付ける

件名は，具体的に書く。読んでもらえる件名にするには，「いつの」「何の」用件で，「どうしたいのか」「どうしてほしいのか」がわかるように書く。

悪い例

・お願い（何のお願いなのかわからない）

・ご相談（何の相談なのかわからない）

・ご案内（何の案内なのかわからない）

良い例

・お見積もり内容ご確認のお願い（〇〇社様用）

・お打ち合わせ日程調整のお願い（8/10 本社営業部向け）

・新製品発売キャンペーンのご案内（9/1～9/30）

③添付ファイルの取り扱いに注意

添付ファイルの取り扱いで注意したいのは，ファイルサイズとファイル形式の 2 点である。相手の環境によって受け取れるファイルサイズの設定は異なる。ファイルサイズの合計が 2MB を超える場合は，相手にあらかじめ送受信できるファイルサイズを聞いておく。相手がファイルに対応したアプリケーションを持っていない場合には，受信しても添付ファイルを開くことができない。図面や動画などのファイルに

ついては，前もって相手に確認可能か聞いておく。添付ファイルは「添付し忘れ」や「誤添付」などのミスが起こりがちなので，送信前の再確認が，ミスや情報漏洩を防ぐ。

④宛名は「会社名＋部署名＋氏名＋様」とするのが基本

相手の顔が見えないメールだからこそ，より丁寧な対応が求められる。宛名はその代表格で，相手の氏名を絶対に間違えないのが基本である。

・社外宛メールの場合

社外宛メールの宛名は「会社名＋部署名＋氏名＋様」とするのが基本で，会社名は（株）（有）などと略さず，「株式会社」「有限会社」と書く。フルネームのほうが丁寧な印象を与える。「〇〇社御中 ××様」は間違いで，会社名の後に個人名が続く場合，御中は必要ない。

・社内宛メールの場合

社内宛メールの場合は「部署名＋氏名＋様」と書く。親しい場合は，「様」を「さん」に変えてもいい。

・Cc を使う場合

Cc を使用していることを強調する場合，括弧（）を使って宛名の下に書き添える。そもそもの目的が情報共有で，大人数を Cc に含めている場合には書き出す必要はない。

社外宛メールの宛名の例

株式会社〇〇

営業部

課長

××××様

社内宛メールの宛名の例

経理部

〇〇様

---

⑤挨拶と名乗りを入れる

挨拶は相手との関係や状況に応じて変える。どんなときも気持ちよい挨拶を心がける。社外メールでの名乗りは宛名と同様「会社名＋部署名＋氏名」とするのが基本で，社内メールの場合は「部署名＋名字」とする。

社外宛メールの挨拶・名乗りの例

・基本

いつもお世話になっております。〇〇商事〇〇課の〇〇です。

・状況に合わせて

お忙しいところ失礼いたします。〇〇商事〇〇課の〇〇です。

・初めての連絡

初めてご連絡いたします。〇〇商事〇〇課の〇〇です。

・返信

ご連絡いただき，誠にありがとうございます。

社内宛のメールの挨拶・名乗りの例

・基本

お疲れ様です。〇〇課の〇〇です。

---

⑥要旨を先に伝え，その後に詳細を書く

ビジネスメールでは，まず要旨を先に伝え，その後に詳細を続ける。最初に要旨を伝えることでメールの目的が明確になり，相手が内容を理解しやすくなる。また，見やすいレイアウトも重要で，20～30 文字で改行を入れ，段落と段落の間を空白で区切る。情報量が多い場合は，箇条書きで情報を整理すると見やすくなる。

⑦結びの挨拶で締める

メールの結びは挨拶で締める。挨拶に始まり挨拶に終わるのが，ビジネスメールのマナーである。結びの挨拶で念押しや心遣いをすることもできる。気持ちよい挨拶をする人だと思ってもらえるよう，挨拶を欠かさないようにする。

結びの挨拶の例

・基本

何卒よろしくお願い申し上げます。

引き続きどうぞよろしくお願いいたします。

・お願い

お手数かとは思いますが，ご確認よろしくお願いいたします。

お力添えのほど，よろしくお願いいたします。

・心遣い

ご不明な点などございましたらお気軽にご連絡ください。

ご多忙と存じますが，くれぐれもご自愛ください。

---

⑧メールには必ず署名を付ける

メールの署名とは，自分の氏名や所属，電話番号などの連絡先情報を記したものである。本文の最後に付けるのがマナーで，具体的には「会社名」「部署名」「氏名（読み仮名）」「電話番号」「FAX 番号」「郵便番号・住所」「メールアドレス」「会社 Web サイトへの URL」が挙げられる。名刺と同程度の情報を載せておけば，面識のない相手にも連絡先を知らせることができる。最近では，担当や役職，部署異動などが頻繁に起こることもあるので，以前に交換した名刺より署名の方が新しくて確実だといえる。

⑨返信・転送のマナーを守る

メールを受信した場合，その後の対応には「返信」「全員に返信」「転送」の 3 つがある。返信は，受信したメールの送り主だけに送信することで，全員に返信は，送り主を To として，Cc に入っていた人がそのまま Cc に入る。転送は，そのメールを受信していない人にメールを送ることである。返信の場合には，

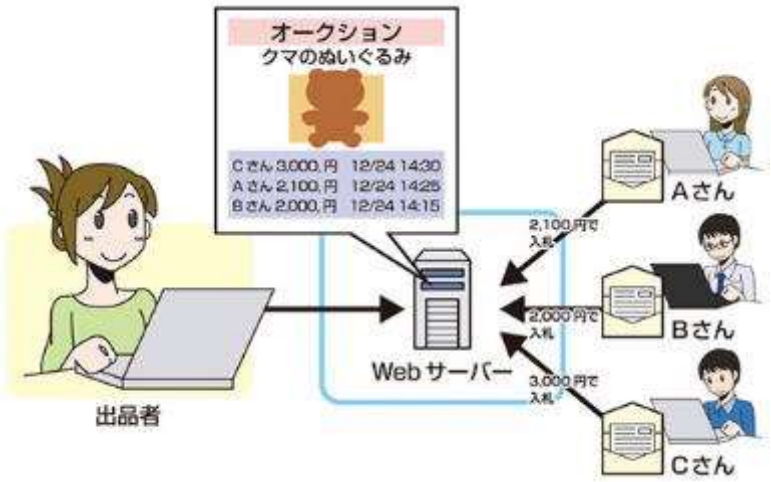
件名に「Re:」などが付き，転送の場合には「Fw:」「Fwd:」などが付くので，返信や転送だとわかる。転送の場合には，メールを転送する理由を明記した上で元のメールを編集せずにそのまま送る。それぞれの機能を理解して正しく使う。

3. ネットオークション

ネットオークションとは，インターネット上で行われるオークションのことで，出品されている商品の中から，気に入った品物を自分の指定した金額で入札することができる。一般的なオークションサイトでは，現在の最高価格が表示されており，その価格よりも高い金額であれば入札できるといった仕組みを設けている。あらかじめ決められた期間，入札を受け付けて，最終的にもっとも高い金額をつけた利用者がその商品を購入できる。また，オークションサイトによっては，参加者が自分の商品を出品することもできるようになっており,新しい形のフリーマーケットとして多くの人に利用されるようになってきた。オークション形式には,「オークション方式」と「一口価格方式」の 2 種類があり，出品者によって選択することができる。オークション方式では，入札期間中に参加者が商品の価格を競い合って最高値をつけた人が落札者となり，一口価格方式では出品者が指定した価格を支払った人が落札者となる。

インターネットオークションは，オンライン上で売り手と買い手が直接取引を行う，便利なショッピング形式である。ネットオークションでは，実店舗では入手困難なレアアイテムやヴィンテージ品を見つけたり，安く大量の商品を購入できたりする。また，自宅にいながら気軽にショッピングを楽しめ，時間的な制約がない。さらに，出品する側も中古品の処分や副収入を得られるというメリットがある。これらの利点から，ネットオークションは近年ますます人気が高まっている。

ネットオークションは，手軽に商品を売買できる便利なサービスだが，利用する際にはいくつかの注意点がある。出品者側には，偽物の商品を販売したり，落札後に連絡が取れなくなったりするといったトラ

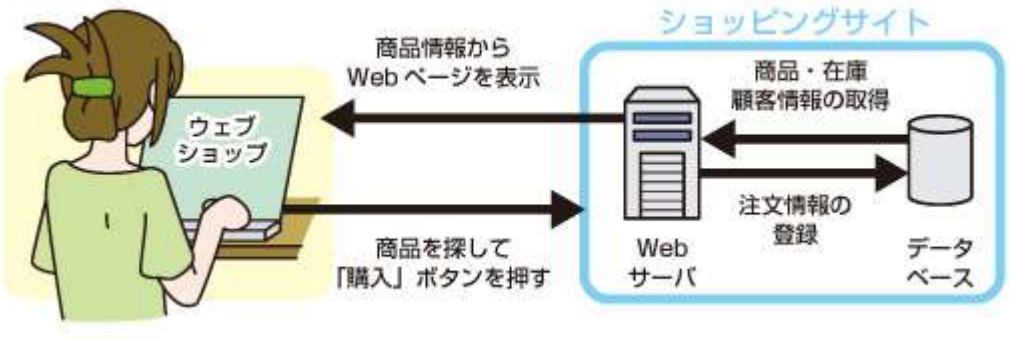


ブルの可能性がある。購入者側には，落札後に思っていたものと違った，というトラブルがある。また，ネットオークションでは個人間での取引が多いため，トラブルが発生した際の補償制度が十分に整っていない場合がある。そのため，利用する際には，出品者や商品の評価を慎重に確認し，不明な点があれば出品者に問い合わせるなど，十分な確認を行う。

ネットオークションでのトラブルを防ぐには，以下の注意事項を守ることが重要で，評価の高い出品者から購入し，怪しい取引を持ちかけられた際は慎重に判断する。さらに，出品物の状態をしっかりと確認し，疑問点は出品者に質問する。代金は入金前に商品を確認できる「代引き」や「着払い」を利用する。契約内容をしっかりと確認し，不明な点は必ず出品者に相談する。

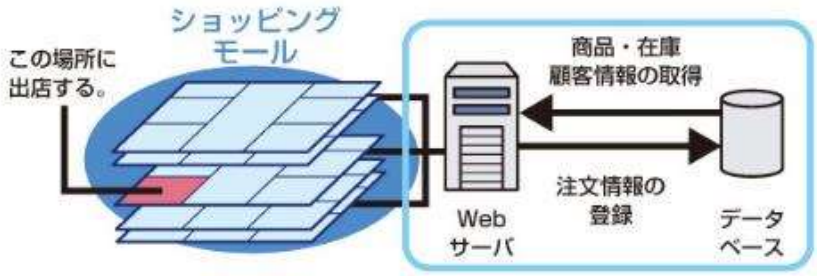
4. ショッピングサイト

ショッピングサイトは，インターネット上で買い物ができるホームページで，ほとんどのショッピングサイトでは，Web サーバとデータベースサーバが連携して動作している。データベースサーバには，顧客情報，商品情報，在庫情報，販売情報などが保管され，Web サイトの訪問者が入力した情報が，リアルタイムにデータベースに書き込まれ，更新される。訪問者が商品を購入すると，購入情報（購入者の顧客情報や購入商品とその在庫情報）がデータベースに登録される。すると，ショッピングサイト側は，利用者に購入受付が完了したことをホームページの画面上または電子メールなどで通知し，受注情報をショップの管理者側に通知する。ショップの管理者は，この情報から受注・決済などの処理（在庫確認，受付通知，入金確認など）をする。さらに，受注処理をもとにデータベースの情報処理経過や在庫数更新など）を更新し，これらの処理の経過状況を購入者に電子メール等で通知する。商品の発送処理（発送準備，発送など）や請求処理を行い，購入者に商品が届けられる。ショップの管理者は，データベースに保存された情報をもとに注文を受けてから発送完了までをショッピングサイトのプログラムを通して情報を更新しながら，並行して実際の処理をしていく流れになる。



ショッピングモールと呼ばれるショッピングサイト群があり，ここではその管理会社が Web サーバやデータベースサーバを用意して，ショッピングサイトの仕組みを提供している。そのため，ショッピングサイトは，このような仕組みを利用するだけではなく，自身で開設することもできる。個人や中小の商店でも,所定のホームページを作成するだけで,簡単にショッピングサイトを開設できるようになっている。

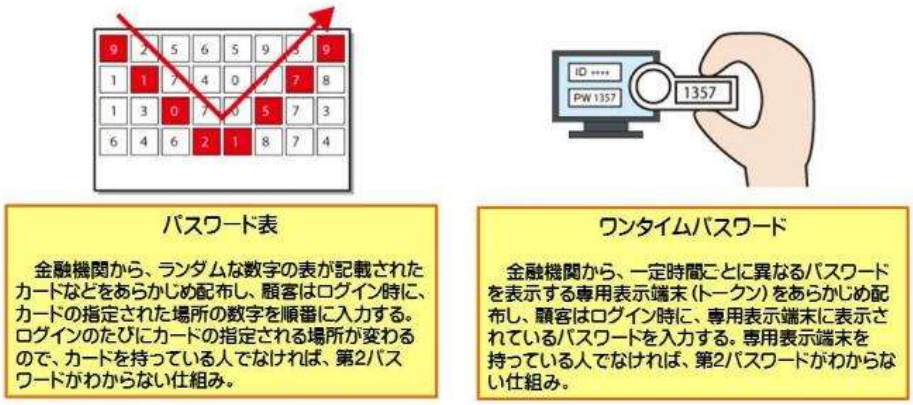
一般にショッピングサイトでは会員登録が必要となる。これにより，購入者は都度自分の発送先や決済情報の登録をせず利用ができ,ショップの管理者側は顧客管理などが効率的に行うことができる。しかし，これはお互いにとって重要な情報を預けたり預かったりすることでもある。預ける側は提供する情報の内容について，預かる側は保存し利用する情報の厳重な管理について注意が必要になる。



5. インターネットバンキング

インターネットバンキングは，インターネットを利用した銀行などの金融取引のサービスである。オンラインバンキングとも呼ばれることもある。パソコンだけでなく，携帯電話やスマートフォンなどからも利用できるサービスが多くなっている。インターネットバンキングでは，銀行の窓口や ATM に行かなくても,自宅や外出先などで,銀行の営業時間を気にすることなく振込や残高照会などをすることができる。このような便利さから，インターネットバンキングの利用は急速に拡大している。インターネットバンキングでは，利用者を識別するために，ATM でよく使われているキャッシュカードや暗証番号の代わりに，ID（契約者番号など）とパスワードでサービスを利用する。第 2 パスワードなど複数のパスワードや，秘密の質問（ペットの名前，出身小学校，母親の旧姓など）といった複数の情報を利用する場合もあり，なりすましなどの不正がないように管理されている。 しかし，利用の拡大に伴い，危険性も増大している。特に，フィッシング詐欺では，このインターネットバンキングという利用形態が最も狙われているサービスの 1 つとなっている。代表的な手口としては，電子メールで金融機関を名乗り，利用者の ID やパスワードなどアカウント情報の確認や更新を要求し，情報を盗み取ろうとするものがある。このような手口による被害にあわないよう，金融機関を名乗ってパスワード等の入力を求める電子メールに対しては，決して

第2パスワードの例



情報を入力してはいけない。その金融機関の Web サイトや問合せ窓口で確認するなどの注意をするようにする。また，最近ではインターネットバンキングを狙ったウィルスへの感染による被害も拡大している。

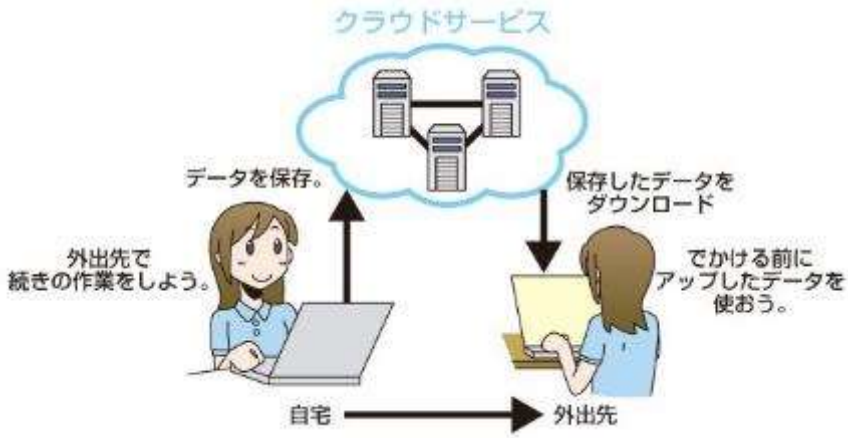
インターネットバンキングを利用することによって情報が盗まれる事例が発生している。これは，金融機関の名前を装った電子メールを送りつけて，利用者が本文中に書かれたリンクをクリックすると開くページで，口座番号などを入力させて情報を盗むといったもので，預金が不正に引き出されるという事例がある。

「Banking Trojan」や「MITB(Man In The Browser)」など，不正送金を行うウィルスがある。これらは正規のサイトを表示している際にポップアップとして口座番号や名前の入力を求めるポップアップを表示させて情報を入力させるというもので，入力された情報をもとに不正送金を行う。正規のサイトを利用中に表示されるので気づくのが難しいという問題がある。もし，インターネットバンキングを使っていて，不正送金など被害にあってしまった場合，速やかに金融機関のカスタマーセンターや，近くの警察に連絡をする。また，「被害保証金制度」というものがあり，全額保証されることになっている。安全に利用するために次のことに気を付ける。

- ウィルス対策ソフトの導入と定義ファイルの定期的な更新
- OS やソフトウェアに対するアップデートプログラムの適用
- 不審なメールのリンクや添付ファイルは開かない
- 不審なポップアップなどが出た場合は入力しない

6. クラウドサービス

クラウドサービスは，従来は利用者が手元のコンピュータで利用していたデータやソフトウェアを，ネットワーク経由で，サービスとして利用者に提供するものである。利用者側が最低限の環境（パーソナルコ



ンピュータや携帯情報端末などのクライアント，その上で動く Web ブラウザ，インターネット接続環境など）を用意することで，どの端末からでも，さまざまなサービスを利用することができる。これまで，利用者はコンピュータのハードウェア，ソフトウェア，データなどを，自身で保有・管理し利用していた。しかしクラウドサービスを利用することで，これまで機材の購入やシステムの構築，管理などにかかるとされていたさまざまな手間や時間の削減をはじめとして，業務の効率化やコストダウンを図れるというメリットがある。

クラウドサービス（特に，以下の分類でいう IaaS）では，主に仮想化技術が使われている。仮想化技術とは，実際に存在する 1 台のコンピュータ上に，ソフトウェアの働きにより，何台もの仮想のコンピュータがあるかのような働きをさせることができる技術である。逆に複数台のコンピュータをあたかも 1 台であるかのように利用することもできる。この技術により，利用者は，クラウドサービス事業者が保有するコンピュータの処理能力を，柔軟に必要な分だけ利用することができる。利用者から見て，インターネットの先にある自分が利用しているコンピュータの形態が実際にどうなっているのか見えづらいことを，図で雲のかたまりのように表現したことから，「cloud＝雲」という名称がついたと言われている。

クラウドサービスは，主に以下の 3 つに分類されている。

SaaS（サース，サーズ : Software as a Service）

インターネット経由での，電子メール，グループウェア，顧客管理，財務会計などのソフトウェア機能の提供を行うサービス。以前は，ASP（Application Service Provider）などと呼ばれていました。

PaaS（パース : Platform as a Service）

インターネット経由での，仮想化されたアプリケーションサーバやデータベースなどアプリケーション実行用のプラットフォーム機能の提供を行うサービス。

IaaS（アイアース，イアース : Infrastructure as a Service）

インターネット経由で，デスクトップ仮想化や共有ディスクなど，ハードウェアやインフラ機能の提供を行うサービス。HaaS（Hardware as a Service）と呼ばれることもあります。

クラウドサービスは，企業が情報資産を管理する手段として急速に普及している。また，個人が利用するインターネット上のさまざまなサービスが，意識するかどうかにかかわらず，クラウドサービス上で稼働するようになっている。クラウドサービスを利用する場合には，データがクラウドサービス事業者側のサーバに保管されているということ,インターネットを介してデータなどがやりとりされることなどから，十分な情報セキュリティ対策が施されたクラウドサービスの選択が重要であるということを理解した上で利用することが大切である。

課　題

1．ネットを利用したサービスの仕組みと安全な利用方法について説明しなさい。

第 13 講　セキュリティ

【学修到達目標】

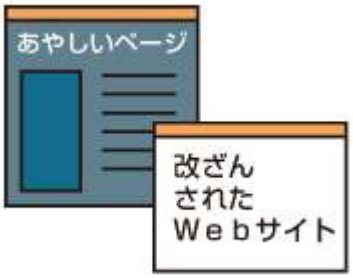
- セキュリティについて理解できる。
- ウィルスの活動とセキュリティ対策について説明できる。

1．セキュリティ

インターネットの脅威にはそれを引き起こす者がいる。悪意を持って攻撃をする者は,お金を稼いだり,請求を逃れたりといった金銭目的や恨みや不満を晴らす目的を持っている。そのために，インターネットを通じて,ウィルスを送りつけたり,政府機関や企業のサーバやシステムに不正アクセスを行ったりする。その他，政治目的やいたずらなどで同じような行為をする者もいる。これにより，サーバやシステムが停止したり，ホームページが改ざんされたり，重要情報が盗みとられたりする。その他にも，コンピュータやソフトウェアの不具合などによる障害，社員や職員の過失などによる事故，火災や台風など自然災害など，インターネットにおける危険性は多くある。

ウィルスは，電子メールやホームページ閲覧などによってコンピュータに侵入する特殊なプログラムである。最近では，マルウェア（“Malicious Software”「悪意のあるソフトウェア」の略称）という呼び方もされている。数年前までは記憶媒体を介して感染するタイプのウィルスがほとんどだったが，最近はインターネットの普及に伴い，電子メールをプレビューしただけで感染するものや，ホームページを閲覧しただけで感染するものが増えている。また，利用者の増加や常時接続回線が普及したことで，ウィルスの増殖する速度が速くなっている。ウィルスの中には，何らかのメッセージや画像を表示するだけのものもあるが,危険度が高いものの中には,ハードディスクに保管されているファイルを消去したり,コンピュータが起動できないようにしたり，パスワードなどのデータを外部に自動的に送信したりするタイプのウィルスもある。そして，何よりも大きな特徴としては,「ウィルス」という名前からも分かるように，多くのウィルスは増殖するための仕組みを持っている。たとえば，コンピュータ内のファイルに自動的に感染したり，ネットワークに接続している他のコンピュータのファイルに自動的に感染したりするなどの方法で自己増殖する。最近はコンピュータに登録されている電子メールのアドレス帳や過去の電子メールの送受信の履歴を利用して，自動的にウィルス付きの電子メールを送信するものや，ホームページを見ただけで感染するものも多く，世界中にウィルスが蔓延する大きな原因となっている。ウィルスに感染しないようにするためには，ウィルス対策ソフトを導入する必要がある。また，常に最新のウィルスに対応できるように，インターネットなどでウィルス検知用データを更新しておかなければならない。ウィルスは，USB

メモリなどの記憶媒体や電子メール，ホームページの閲覧など，そのウィルスのタイプによってさまざまな方法で感染する。また，ウィルスに感染すると，コンピュータシステムを破壊したり，他のコンピュータに感染したり，そのままコンピュータに残ってバックドアと呼ばれる不正な侵入口を用意したりするなど，さまざまな活動を行う。



Web ブラウザは，ホームページ上でさまざまな処理を実現できるように，各種のプログラムを実行できるようになっている。これらのプログラムの脆弱性を悪用するウィルスが埋め込まれたホームページを閲覧すると，それだけでコンピュータがウィルスに感染してしまう危険がある。最近では，Web ブラウザへ機能を追加するプラグインソフトの脆弱性(ぜいじゃくせい)を利用した感染方法が増加している。かつては怪しい Web サイトを訪問しなければ大丈夫と思われていたが，最近では正規の Web サイトが不正侵入を受けて書き換えられ，ウィルスが仕込まれてしまうケースも急増している。この場合は，正規の Web サイトを閲覧しても，ウィルスに感染してしまうことになる。

あたかも無料のウィルス対策ソフトのように見せかけて，悪意のあるプログラムをインストールさせようとする「偽セキュリティソフト」の被害が増えている。その代表的な手口は，ホームページなどで「あなたのコンピュータはウィルスに感染しています」のようなメッセージを表示し，利用者を偽のウィルス対策ソフトを配布する Web サイトに誘導する方法である。

電子メールの添付ファイルもウィルスの感染経路として一般的である。電子メールに添付されてきたファイルをよく確認せずに開くと，それが悪意のあるプログラムであった場合はウィルスに感染してしまう。かつては，電子メールで実行形式のファイル(ファイルの拡張子が.exe　のファイル)が送られてきたときには特に注意するように言われていたが，最近はファイル名を巧妙に偽装し，文書形式のファイルに見せかけて悪意のあるプログラムを実行させ，ウィルスに感染させる事例もある。また，文書形式のファイルであっても，文書を閲覧するソフトウェアの脆弱性を狙った攻撃も増加していることから，メールに添付されてきたファイルを安易に開くのは危険な行為である。

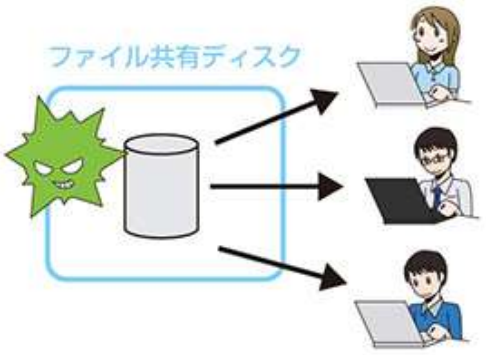
多くのコンピュータでは，USB メモリをコンピュータに差し込んだだけで自動的にプログラムが実行される仕組みが用意されている。この仕組みを悪用して，コンピュータに感染するウィルスがある。このようなウィルスの中には，感染したコンピュータに後から差し込まれた別の USB メモリに感染するなどの方法で，被害を拡大させるものもある。

ファイル共有ソフトとは，インターネットを利用して他人とファイルをやり取りするソフトウェアのことである。自分が持っているファイルの情報と，相手が持っているファイルの情報を交換し，お互いに欲しいファイルを送り合ったりすることから，ファイル交換ソフトとも呼ばれている。ファイル共有ソフト

では，不特定多数の利用者が自由にファイルを公開することができるため，別のファイルに偽装するなどの方法で，いつの間にかウィルスを実行させられてしまうことがある。

添付ファイルが付いていなくても，HTML 形式で書かれているメールの場合，ウィルスに感染することがある。HTML メールはホームページと同様に，メッセージの中にスクリプトと呼ばれるプログラムを挿入することが可能なため，スクリプトの形でウィルスを侵入させておくことができる。電子メールソフトによっては，HTML メールのスクリプトを自動的に実行する設定になっているものがあり，その場合には電子メールをプレビューしただけでウィルスに感染してしまう。

ウィルスによっては，感染したコンピュータに接続されているファイル共有ディスクを見つけ出し，特定のファイル形式など，ある条件で探し出したファイルに感染していくタイプのものがある。このようなウィルスは組織内のネットワークを通じて，他のコンピュータやサーバにも侵入して感染を拡げる可能性がある。とても危険度が高く，完全に駆除することが難しいのが特徴である。



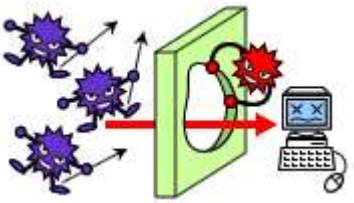
マイクロソフト社の Office アプリケーション（Word，Excel，PowerPoint，Access など）には，特定の操作手順をプログラムとして登録できるマクロという機能がある。このマクロ機能を利用して感染するタイプのウィルスが知られており，マクロウイルスと呼ばれている。Office アプリケーションでは，マクロを作成する際に，高度なプログラム開発言語である VBA（Visual Basic for Applications）を使用できるため，ファイルの書き換えや削除など，コンピュータを自在に操ることが可能である。そのため，マクロウイルスに感染した文書ファイルを開いただけで，VBA で記述されたウィルスが実行されて，自己増殖などの活動が開始されることになる。

2．ウィルスの活動

ウィルスの中には，インターネットや LAN を使用して，他の多くのコンピュータに感染することを目的としているものがある。特にワーム型と呼ばれるウィルスは，自分自身の複製を電子メールの添付ファイルとして送信したり，ネットワークドライブに保存されているファイルに感染したりするなど，利用者の操作を介さずに自動的に増殖する。

ウィルスによる情報漏洩は，大きく分類すると，コンピュータに保存されている情報が外部の特定のサイトに送信されて起こる場合と，インターネット上に情報が広く公開されて起こる場合がある。ウィルス

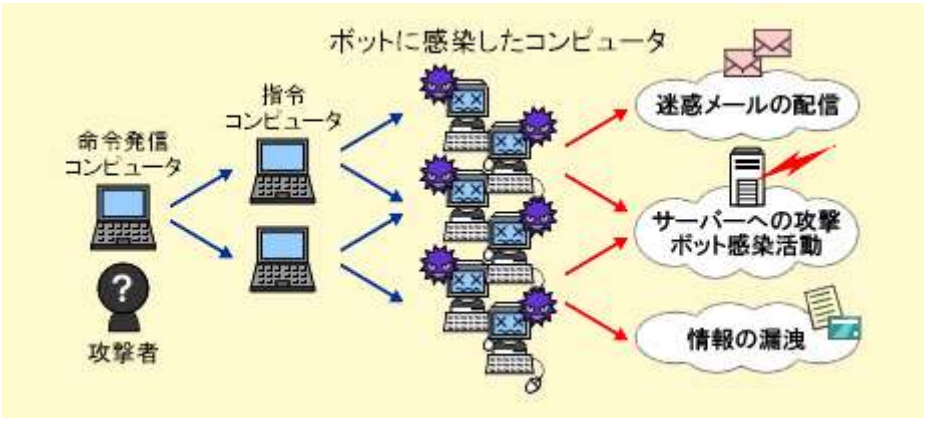
によって漏洩する情報は，ユーザーIDやパスワード，コンピュータ内のファイル，メール，デスクトップの画像など，さまざまである。情報漏洩を引き起こすタイプのウィルスには，利用者がキーボードで入力した情報を記録するキーロガーや，コンピュータ内に記録されている情報を外部に送信するスパイウェアと呼ばれるものなどがある。コンピュータがこのようなウィルスに感染していたとしても，コンピュータの画面上には何の変化も起こらないことが多いため，利用者はウィルスに感染していることに全く気が付かない。漏洩した情報がインターネットに掲載され，公開されてしまった場合は，その情報をネットワーク上から完全に消去することは非常に困難である。



感染したコンピュータの内部に潜伏するタイプのウィルスをトロイの木馬と呼ぶ。この中でも，コンピュータに外部から侵入しやすいように「バックドア」と呼ばれる裏口を作成するタイプのウィルスは極めて悪質である。この種のウィルスに感染すると，コンピュータを外部から自由に操作されてしまうこともある。外部からコンピュータを操作するタイプのウィルスは，RAT (Remote Administration Tool)とも呼ばれ，利用者に気が付かれることもなくコンピュータを遠隔操作する。多くの場合，コンピュータの画面上に何も表示されることなく，プログラムやデータファイルの実行・停止・削除，ファイルやプログラムのアップロード・ダウンロードなど，不正な活動を行う。

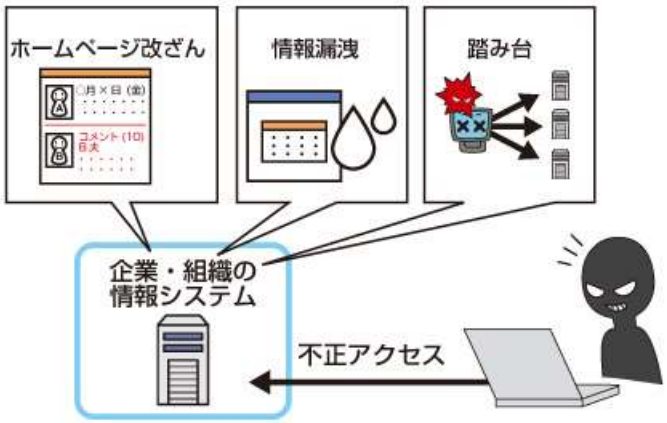
ウィルスによっては，コンピュータシステムを破壊してしまうものがある。その動作はウィルスによって異なるが，特定の拡張子を持つファイルを探し出して自動的に削除するものから，コンピュータの動作を停止してしまうものまでさまざまである。

ボット（BOT）とは，コンピュータを外部から踏み台にして遠隔操作するためのウィルスである。ボットに感染したコンピュータは，同様にボットに感染した他の多数のコンピュータとともにボットネットを形成し，その一員として動作するようになる。そして，インターネットを通じて，悪意のある攻撃者が，ボットに感染したコンピュータを遠隔操作する。外部から自由に操るという動作から，このような遠隔操



作ソフトウェアのことを，ロボット（Robot）をもじってボット（BOT）と呼んでいる。攻撃者は，ボットに感染したコンピュータを遠隔操作することで，インターネットに対して，「迷惑メールの配信」，「インターネット上のサーバへの攻撃」，「さらにボットを増やすための感染活動」など，迷惑行為や犯罪行為を行う。また，感染したコンピュータに含まれる情報や，コンピュータの利用者が入力した情報を盗み出す「スパイ活動」も行うことがある。ボットは旧来のウィルスのように愉快犯的な行為で作られたものではなく，迷惑メールの送信者や個人情報を不正に利用しようとする犯罪者と取引するために作られているという点で，手口が巧妙化している。このような目的から，旧来のウィルスと比べると，感染しているということに利用者が気付きにくいように作られているというのも特徴のひとつである。

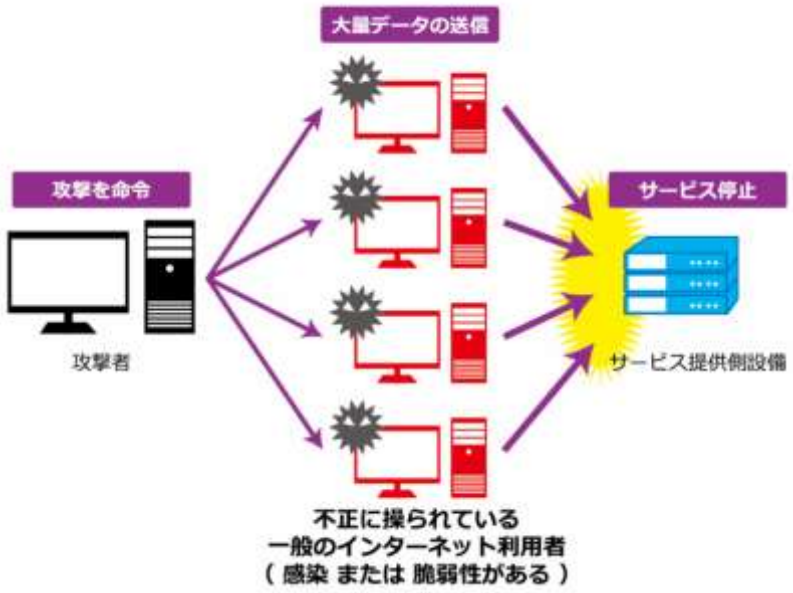
不正アクセスとは，本来アクセス権限を持たない者が，サーバや情報システムの内部へ侵入を行う行為である。サーバや情報システムが停止してしまったり，重要情報が漏洩してしまったりと，企業や組織の業務やブランド・イメージなどに大きな影響を及ぼす。インターネットは世界中とつながっているため，不正アクセスは世界中のどこからでも行われる可能性がある。



攻撃者は，インターネットを通じて企業や組織のサーバや情報システムに侵入を試みる。手口としては，ツールを用いてアカウント情報を窃取するための総当たり攻撃を行ったり，OS やソフトウェアの脆弱性（ぜいじゃくせい），設定の不備などを調べて攻撃することが知られている。攻撃者は侵入に成功すると，その中にあるホームページの内容を書き換えたり，保存されている顧客情報や機密情報を窃取したり，重要なファイルを消去したりすることもある。ホームページの書き換えは，攻撃者が全く関係のない画像を貼り付けるようなものもありますが，最近はホームページにあるリンクやファイルの参照先を不正に書き換え，接続してきた利用者をウィルスに感染させたり，パソコンから情報を盗み取ったりするものが増えている。ホームページが書き換えの被害を受けるということは，その企業や組織のセキュリティ対策が不十分であることを示すことになり，社会に対するイメージ低下は避けられない。また，顧客情報などが漏洩（ろうえい）してしまった場合は，その企業や組織の信用が大きく傷つけられてしまうのは言うまでも

ないが，過去には損害賠償にまで発展した事例もある。このように，不正アクセスは甚大な被害をもたらすこともある。

不正アクセスによって侵入されたシステムは，攻撃者がその後いつでもアクセスできるように，バックドアと呼ばれる裏口を作られてしまうことが知られている。攻撃者は，そのシステムを踏み台として，さらに組織の内部に侵入しようとしたり，そのシステムからインターネットを通じて外部の他の組織を攻撃したりすることもある。この場合に多く見られる例は，攻撃者によってボット ウィルスを送り込まれ，自分がボットネットの一員となってしまうというものである。ボットネットとは，攻撃者によって制御を奪われたコンピュータの集まりで，数千～数十万というネットワークから構成されていることもある。攻撃者はボットに一斉に指令を送り，外部の他の組織に対して大規模な DDoS 攻撃を行ったり，スパムメールを送信したりすることもある。このように，不正アクセスの被害に遭うと，知らない間に攻撃者の一員として利用されてしまうこともある。



インターネットでは，詐欺や犯罪行為などが増加しています。それらの詐欺や犯罪の中には

- □ 偽物のホームページに誘導し個人情報などを窃取するフィッシング詐欺
- □ 電子メールなどで誘導してクリックしたことで架空請求などをするワンクリック詐欺
- □ 商品購入などで架空出品をしてお金をだましとるオークション詐欺
- □ 違法薬物など，法令で禁止されている物を販売する犯罪
- □ 公序良俗に反する出会い系サイトなどに関わる犯罪

など多様な手口がある。

インターネットでの犯罪は，主に金銭目的で行われることも増えてきた。そのために，デマなどのウソの情報を流す，他人になりすます，ユーザーID やパスワード，プロフィールなどの個人情報を盗んで悪用するなど，さまざまな手法で行われる。金銭目的以外では，相手への恨みや不満，興味本位などの動機から，攻撃や嫌がらせなどを目的として行われることもある。インターネットが広く普及したことにより，これまで現実世界でも存在した詐欺やの犯罪行為などでもこの便利な技術が使われるようになってきた。インターネットが便利なのは，犯罪者にとっても同じです。これからも，ますます犯罪行為にインターネットが使われ，多様な手口が出現してくる。利用者はよりいっそうの注意が必要になる。

インターネットの脅威は，外部の攻撃者などにより意図的に行われるものばかりではない。人による意図的ではない行為や，組織などの内部犯行，システムの障害などの事故も大きな情報セキュリティ上の脅威である。人は意図的ではなく，脅威を引き起こすこともある。操作ミスや設定ミス，紛失など，いわゆる「つい，うっかり」の過失（ヒューマンエラー）である。電子メールの送り先を間違えたり，書類や記憶媒体の廃棄の方法を誤ったり，携帯電話やスマートフォンを紛失したり，といった過失が多く発生している。実は，企業や組織における情報漏洩の原因のほとんどが，このような人の「つい，うっかり」や IT の使いこなし能力（リテラシー）の不足によるものとされている。組織などの内部犯行も想定される脅威の一つとして，セキュリティ対策を講じておく必要がある。例えば，アカウント管理やデータのアクセス権限を適切に設定したり，アクセス記録を取ることで，人による脅威を未然に防ぐことになり得る。

その他の脅威としては，機器やシステムの障害や自然災害などがある。機器やシステムの障害は，コンピュータやネットワークを使っている限りは常に起こり得る問題である。システムの障害によって，データが失われてしまったり，業務が継続できなくなったりするなどの大きな影響が発生することもある。自然災害は，頻繁に起こる問題ではありませんが，ひとたび発生すれば企業や組織に甚大な被害や影響を与える。以上の脅威を起こり得ることとして想定し，あらかじめ事故や障害・災害が発生した場合の情報セキュリティ対策を講じておく必要がある。

パソコンやサーバ上で取り扱われているデジタル式のデータは主に，ファイル形式(file fomart : ファイルフォーマット)という記録形式で作成されて，フォルダという電子上の格納庫に保存される。エクセルやワード，PDF などで作られたテキストファイルや，画像，音声，映像等のバイナリーファイルといった様々な形で，アプリケーションソフトウェアの機能で独自の拡張子により作成される。しかし，ソフトウェアツールでファイルを製作したり上書き，コピー保存を行う際，稀にプログラム上の書き込みエラーが起こり，拡張子ファイルのプログラムが壊れる事がある。文字化けや画像の乱れといったエラーはこれが原因で起こる場合が多い。アプリケーションソフトウェアは正しく指定された手順に沿って使えば普通は問題なく作業できるが，パソコンや OS 上の動作環境が満たされていなかったり，対応していない種類のファイルを無理に開こうとすると，動作速度が鈍ったり書き込みに失敗する事もある。他で共有して使ってい

るソフトウェアやハードウェアとの互換性の相性が悪い，などイレギュラーな理由でもファイルやプログラムの破損を引き起こしてしまうケースも存在する。また，ヒューマンエラー（人為的な操作ミス）で壊れてしまう場合も多いですので，予備のバックアップはなるべくこまめに取る事がたいせつである。

3. セキュリティ対策

サイバーセキュリティ対策は，情報機器やインターネットを安全に利用するために欠かせないものである。インターネットに関する脅威が多様化する中で，さまざまなサイバーセキュリティ対策が必要となっているが，まずは『サイバーセキュリティ三原則』として，「ソフトウェアを最新に保とう」，「強固なパスワードの設定と多要素認証を活用しよう」，「不用意に開かない・インストールしない」の 3 点を心がけるようにする。

その 1 ソフトウェアを最新に保つ

アプリケーション・OS の更新（アップデート）は，セキュリティの観点から極めて重要である。最新のバージョンには，アプリケーション・OS の欠陥（脆弱性（ぜいじゃくせい））が改善され，セキュリティ機能の強化が含まれている。OS やアプリケーションのアップデートを定期的に確認し，すぐにインストールすることで，潜在的なリスクを軽減できる。

その 2 強固なパスワードの設定と多要素認証を活用する

推測されにくく，かつ文字数の多いパスワードを設定することは，不正アクセス防止に役立つ。また，設定と同様に重要なのがパスワードの管理で，同じパスワードを複数のサービスで使いまわさない等，意識することが重要である。さらに，可能であれば多要素認証を活用して，ログイン時のセキュリティを強化しする。多要素認証は，パスワード以外の認証方法（例えば，ショートメッセージで送られた数字を入力する，など）を追加することで，不正アクセスを防ぐ効果がある。

その 3 不用意に開かない・インストールしない

フィッシング詐欺やマルウェア（コンピュータウイルス）の感染につながる可能性があるため，メールや SMS のリンクや添付ファイルを不用意に開かないようにする。巧妙な詐欺メールが増えているため注意が必要である。公式サイトや公式ストア以外からダウンロードした，提供元がはっきりしないアプリによるマルウェア被害も報告されている。検索で見つけたユーティリティソフトやゲームなどをインストールする際には十分な注意が必要である。

推測できる簡単なパスワードを利用しない

パソコンにログインする等，インターネットのネットオークションやショッピングサイトを利用する際において，なりすましを防ぐための認証には，一般的にパスワードが利用されている。そのため，コンピュー

タやインターネットを利用する上では，どのようなパスワードを使用するかということが，とても重要である。パスワードの適切な管理（安全なパスワードの作成，保管，更新）はパソコンやサーバを安全に利用するためには欠かせない。パスワードの適切な管理には，次の要素がある。最低でも 10 文字以上の文字数で構成されるある程度長いランダムな英数字の並びとし，パスワード内に数字や記号，アルファベット（大文字，小文字）が混ざっていることが好ましい。スマートフォンや Web ブラウザの標準機能として，パスワード生成機能があるものもありますので，そういったものをうまく活用してもよい。せっかく安全なパスワードを設定しても，パスワードが他人に漏れてしまえば意味がない。パスワードは，同僚等の第三者に教えずに，秘密にすること。パスワードを電子メールでやりとりしないこと。パスワードのメモをディスプレイなど他人の目に触れる場所に貼ったりしないこと。各サービスで異なる充分に安全なパスワードを覚えておくのは大変なので，パスワードを覚える必要のない，パスワード管理ツールを使うことも推奨される。スマートフォンや Web ブラウザ標準機能，あるいは専用のアプリケーションのパスワード保存機能を活用する。これらのツールやサービスは，マスターパスワード（覚えられる充分に安全なもの）や，利用デバイス（スマートフォンなど）のロック（生体認証など）で守る必要がある。

パスワードはできる限り，複数のサービスで使い回さないようにする。サービスから流出したアカウント情報を使って，他のサービスへの不正ログインを試す攻撃の手口が知られている。もし重要情報を利用しているサービスで，他のサービスからの使い回しのパスワードを利用していた場合，他のサービスから何らかの原因でパスワードが漏洩してしまえば，第三者に重要情報にアクセスされてしまう可能性がある。

利用するサービスによっては，パスワードを定期的に変更することを求められることもあるが，実際にパスワードを破られアカウントが乗っ取られる等のサービス側から流出した事実がない場合は，パスワードを変更する必要はない。むしろ定期的な変更をすることで，パスワードの作り方がパターン化し簡単なものになることや，使い回しをするようになることの方が問題となる。定期的に変更するよりも，機器やサービスの間で使い回しのない，固有のパスワードを設定することが求められる。

3. 脆弱性(ぜいじゃくせい)

脆弱性とは，コンピュータの OS やソフトウェアにおいて，プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のことを言う。脆弱性は，セキュリティホールとも呼ばれる。脆弱性が残された状態でコンピュータを利用していると，不正アクセスに利用されたり，ウィルスに感染したりする危険性がある。このような脆弱性が発見されると，多くの場合，ソフトウェアを開発したメーカーが更新プログラムを作成して提供する。しかし，脆弱性は完全に対策を施すことが困難であり，次々と新たな脆弱性が発見されているのが現状である。脆弱性には，いくつかの種類がある。脆弱性が放置されていると，外部から攻撃を受けたり，ウイルス（ワーム）の感染に利用されたりする危険性があるため，

インターネットに接続しているコンピュータにおける情報セキュリティ上の大きな問題のひとつになっている。脆弱性はクライアントとサーバ，どちらのコンピュータにおいても重要な問題であるが，特にインターネットに公開しているサーバの場合には，脆弱性を利用した不正アクセスによって，ホームページが改ざんされたり，他のコンピュータを攻撃するための踏み台に利用されたり，ウィルスの発信源になってしまったりするなど，攻撃者に悪用されてしまう可能性があるため，脆弱性は必ず塞いでおかなければならない。脆弱性を塞ぐには，OS やソフトウェアのアップデートが必要となる。たとえば，Windows の場合には，サービスパックや Windows Update によって，それまでに発見された脆弱性を塞ぐことができる。ただし，一度脆弱性を塞いでも，また新たな脆弱性が発見される可能性があるため，常に OS やソフトウェアの更新情報を収集して，できる限り迅速にアップデートを行わなければならない。

ゼロデイ攻撃と呼ばれる脅威が増加している。ゼロデイ攻撃とは，OS やソフトウェアに対する脆弱性が発見されたときに，メーカーが修正プログラムを配布するまでの間に，その脆弱性を利用して行われる攻撃である。脆弱性が公開されてから，メーカーが対応策を検討して修正プログラムを開発することも多いため，完全な対策は困難と言わざるを得ない。そのため，指摘された脆弱性の内容を確認し，危険となる行為を行わないなど，修正プログラムを適用するまでの間は十分な注意が必要である。

課　題

１．ウィルスの活動とセキュリティ対策について説明しなさい。

第 14 講　データ記憶装置

【学修到達目標】

- データ破損とデータ破損対策について説明できる。
- データ記憶装置の特性を知り，適切に利用することができる。

1. データ破損

パソコンやサーバ上で取り扱われているデジタル式のデータは主に，ファイル形式(file fomart : ファイルフォーマット)という記録形式で作成されて，フォルダという電子上の格納庫に保存される。エクセルやワード, PDF などで作られたテキストファイルや, 画像, 音声, 映像等のバイナリーファイルといった様々な形で，アプリケーションソフトウェアの機能で独自の拡張子により作成される。しかし，ソフトウェアツールでファイルを製作したり上書き，コピー保存を行う際，稀にプログラム上の書き込みエラーが起こり，拡張子ファイルのプログラムが壊れる事がある。文字化けや画像の乱れといったエラーはこれが原因で起こる場合が多い。アプリケーションソフトウェアは正しく指定された手順に沿って使えば問題なく作業できるが，パソコンや OS 上の動作環境が満たされていなかったり，対応していない種類のファイルを無理に開こうとすると，動作速度が鈍ったり書き込みに失敗する事もある。

他で共有して使っているソフトウェアやハードウェアとの互換性の相性が悪い，などイレギュラーな理由でもファイルやプログラムの破損を引き起こしてしまうケースも存在する。また, ヒューマンエラー（人為的な操作ミス）で壊れてしまう場合も多いので，予備のバックアップはなるべくこまめに取る事を推奨する。

ハードディスクや SSD，USB メモリといったデータ記憶装置のファイルを記録している回路（プラッタなど）が物理的に故障して読み込めなくなるトラブルもある。ただ，HDD やフラッシュメモリが故障する事は良くあるのなのだが，その多くはモーターやヘッド部分，差込口といった別の箇所が破損しただけで，ファイルが記録されたメモリの回路自体が壊れるケースはまだ少ない。

基本的に，Windows の「ファイル履歴」や，Mac OS X の「TimeMachine」を有効に設定して自動バックアップを取ったり，また定期的に外付けハードディスクや RAID，NAS，クラウドなどにデータをバックアップしておくと，後からいつでも対象のファイルを復旧できる。また，使用しているユーティリティーによっては，「bak ファイル」という予備のデータが自動的に作成されるので，フォルダーを開いて，拡張子の部分を「.bak」から，壊れた対象のファイルと同じ拡張子名に変更をすると，同じデータの復旧がで

きる。ファイルが壊れたり，物理的にどこかが破損して読み込みできなくなったハードディスクや USB メモリ等の記憶装置は，なるべく早いうちに専門のデータ復旧サポートセンターに預けてチェックしてもらい，回復が可能なファイルを修復してもらうことで解決できる見込みがある。

USB メモリのデータ破損も時々起こる。USB メモリが破損してしまう原因で，多いのは USB メモリを安全に取り外すための手順を省くことである。コンピュータには，「書き込みキャッシュ」と呼ばれるものがあるため，このたったひと手間を怠ったせいで USB メモリが破損してしまうことがある。書き込みキャッシュとは，書き込みの速度を上げるための機能である。OS は，リクエストを受け取った時にその都度フラッシュメモリに書き込みを行うのではなく，いったんキャッシュメモリにリクエストを保存して，あとでまとめて書き込む。「安全に取り外す」または「アンマウント」を実行すると，もうすぐ USB メモリが取り外されることをコンピュータが理解し，キャッシュメモリにあるリクエストを書き込み，バックグラウンドで実行しているすべてのプログラムに対して， USB メモリへのアクセスを停止するよう命令する。この動作が完了するまで待たないと， USB フラッシュドライブに書き込まれるはずだったデータが正しく書き込まれず，ファイルシステムの破損につながる。

USB メモリは補助的なもので，重要なファイルを USB メモリだけに保存するようなことはしないことが大切である。大切なデータはバックアップを取り，少なくとも 2 つのドライブに保存しておくようにする。また，火災や水害などのリスクを考慮して，物理的に離れた 2 カ所以上の場所で保存しておく。どんな記憶装置であってもいつかは壊れてしまので，1 つのソリューションだけで安心しないようにする。

USB メモリは読み書きの回数が決まっている。USB メモリの寿命を伸ばすテクノロジーとしては，「ウェアレベリング」と「オーバープロビジョニング」が知られている。ドライブがウェアレベリングをサポートしている場合，大容量のドライブであれば，消耗した部分があっても，ほかの部分を利用することができる。

USB メモリは永久的に使用できるものではない。現在のフラッシュメモリはすべて，書き込み／読み込みできる回数に限りがあり，時間がたてばデータ損失が避けらない。データ損失のリスクを軽減するには，定期的にバックアップを取ったり，チェックサムを使ってデータを検証し，いつファイルが破損したかを把握しておいたりする。バックアップする記憶メディア(HDD や BD，DVD など)の比較と信頼性についての表を次に示す。

フラッシュメモリ(USB メモリ/SD カード/Flash SSD)の容量は数 10MB～数 GB，信頼性は低く，寿命は 5 年，書き換え回数に限度があり，一時的に保存するもので長期保存には適さないことが分かる。ハードディスクドライブ(HDD) の容量は数 10GB～数 TB，信頼性は高く，寿命は 3-5 年，磁気や振動，衝撃に弱いく，耐用年数が低い。ソリッドステートドライブ(SSD) の容量は数 10GB～数 TB，信頼性は低く，

寿命は５年，書き換え回数に制限があり，価格が高く，データが消失する可能性があり長期保存には適さないことが分かる。

メディアの名称	容量	信頼性	寿命	欠点	備考
フロッピーディスク(FD)	1.44MB 前後	低い	10 年	磁気，埃，汚れに弱い	容量が少なすぎてバックアップに向いていない
大容量磁気ディスク(ZIP/Jaz)	100MB～数 GB	-	-	磁気，埃，汚れに弱い	書き込み速度は速いが廃れたメディアである
磁気テープ	数 10GB～数 TB	高い	10 年	定期メンテナンスが必須	主に業務用の記憶メディアである
光ディスク(CD/DVD/BD)	640MB～128GB	高い	10-30 年	書き込み速度が遅い	海外製品は寿命が 0 年のものがあるので注意
フラッシュメモリ(USB メモリ/SD カード/Flash SSD)	数 10MB～数 GB	低い	５年	書き換え回数に限度がある	一時的に保存するもので長期保存には適さない
光磁気ディスク(MO)	100MB～2.3GB	高い	50 年	専用ドライブが入手困難	信頼性は高いが廃れたメディアである
ハードディスクドライブ(HDD)	数 10GB～数 TB	高い	3-5 年	磁気や振動，衝撃に弱い	耐用年数が低い
ソリッドステートドライブ(SSD)	数 10GB～数 TB	低い	５年	書き換え回数に制限，価格が高い	データが消失する可能性があり長期保存には適さない

上記の表から小規模のバックアップにおいてはハードディスク(HDD)及び光ディスク(CD/DVD/BD)が適していると思われる。近年，業務に使用する大規模のデータに関しても D2T(Disk to Tape)から D2D(Disk to Disk)に移行している模様である。

光メディアと DVD(ディーブイディー)，Blu-ray Disc(ブルーレイディスク)の比較を次に示す。

名称	容量	寿命	書き込み	備考
CD-R	700MB	10 年	一度しか書き込めない	容量が少ない
CD-RW	700MB	10 年	書き換え可能回数は 1,000 回	容量が少ない，DVD-R より価格が高い

名称	容量	寿命	書き込み	備考	推進団体など
DVD-R	4.7GB	9年～	一度しか書き込めない	互換性が高い	-
DVD+R	4.7GB	-	一度しか書き込めない	互換性が高い(主に海外)	-
DVD-RW	4.7GB	27年～	書き換え可能回数は1,000回	互換性の為にファイナライズする必要がある	パイオニア+(ソニー・シャープ・三菱電機)
DVD+RW	4.7GB	-	書き換え可能回数は1,000回	ファイナライズ不要，対応機器少ない	ソニー・フィリップス・HP
DVD-RAM	4.7GB	134年～	書き換え可能回数が100,000回	USB メモリのように使用できる。対応機器少ない	パナソニック・東芝・日立製作所・日本ビクター

名称	容量	寿命	書き込み	備考
BD-R	25GB	10年～	一度しか書き込めない	-
BD-R DL(片面2層)	50GB	10年～	一度しか書き込めない	対応機器が必要
BD-R XL(片面3/4層)	100/128GB	10年～	一度しか書き込めない	対応機器が必要
BD-R LTH	25GB	10年～	一度しか書き込めない	対応機器が必要。有機素材により低価格。
BD-RE	25GB	10年～	書き換え可能回数は10,000回	-
BD-RE DL(片面2層)	50GB	10年～	書き換え可能回数は10,000回	対応機器が必要
BD-RE XL(片面3層)	100GB	10年～	書き換え可能回数は10,000回	対応機器が必要

バックアップは元のデータの他に2種類以上のメディアに保存する事が大事である。

・一つ目はハードディスクまたはポータブルハードディスクに保存

・二つ目は光ディスク(DVD または BD)に保存

USB メモリ，SD カードは持ち運びが簡単だが，HDD に比べて容量が少なく，容量に対しての値段が高いが省電力だったり衝撃に強かったりする。欠点として，冬に静電気対策せずに SD カードさわると一瞬で使えなくなる。また，フラッシュメモリは書き込みや削除回数の上限が磁気ディスクより少なく，書き

込まなくても年数がたつと劣化して使えなくなる。これに対し，外付け HDD は上限回数が多いが，ほこりや熱，磁気に弱い.

外部記憶媒体の使い方として，次のように使うように心がける。

1) ファイルを直接編集しない

USB メモリの中にあるレポートや仕事のファイルを，そのまま開いて編集していたりしない．記録メディアには書き込み上限回数などが存在するためにレポートを開いて上書き保存を繰り返すたびに劣化する．また，Word などのソフトを使用していると編集時自動バックアップ機能が作動する．この自動バックアップ機能，たとえば急にプログラムがフリーズしたときにも編集中のデータを復元できるのでとても便利なのだが，上書き保存を自分がしていなくても勝手に編集中ファイルが自動保存されてしまう．記録メディアには書き込み上限が決まっているため自動保存のたびに寿命に近づいていく．記録メディアの中から使う時には劣化を早めるのでまずコンピュータのどこかの場所にコピーして，作業が終わったら記録メディアに保存するという使い方をする.

2) データ受け渡しに使用する

自宅と学校のパソコンを普段使用しているとすると．学校にいるときは学校のパソコンまたはノートパソコンを使うし自宅だとデスクトップパソコンも使う．どのパソコンでも簡単に同じファイルを編集できるから USB メモリなどに保存しておくとデータの受け渡しが便利である。必ずパソコンにコピーしてからパソコンの方のファイルを編集する．その最新版のファイルは消さずに記録メディアに移動ではなくコピーする．これで，どこかのパソコンには必ず最新版が保存されている.

3) 外付け HDD はファイルのバックアップに使う

外付け HDD は USB メモリや SD カードなどに比べて書き込み回数の上限と容量がはるかに多い一方，熱や埃などに弱い. そのため直射日光や埃のたまりやすい場所は避けて設置する。磁気を使用しているディスクなので近くに磁気を発するものがないところに設置する．そして，バックアップのための機器として使用する。バックアップソフトがネットで探せば無料でたくさん出ている．機能として

- 変更があればそのファイルだけを自動でバックアップ
- 毎回ではなく一か月，一週間，一日に一回など定期的にバックアップを自動で行う

など便利な機能がたくさんある.

2. USB の規格

USB の便利な点として次のものがある。

1) ホットプラグ機能

ホットプラグ機能とは電源を入れたままの状態の PC などの機器に直接接続することができる機能のことである。接続すれば自動的に PC が USB を認識し，デバイスシステムに組み込み必要な設定などを自動的に行う。

2) USB ハブで複数台接続できる

USB の差込口を増やせる USB ハブを使うと，複数の機器を接続できる。

3) 互換性がある

PC が USB 規格に対応している場合は，どの規格についても互換性がある。

USB の種類を次に示す。

発表月	バージョン	転送速度
1998/1	USB1.1	12Mbps
2000/4	USB2.0	480Mbps
2008/11	USB3.0 （USB3.1 Gen1）	5Gbps
2013/7	USB3.1 （USB3.1 Gen 2×1）	10Gbps
2017/9	USB3.2 （USB3.2 Gen 2×2）	20Gbps
2019/8	USB4 Gen 2 x2	20Gbps
2019/8	USB4 Gen 3 x2	40Gbps

USB のコネクターの形状を次に示す。

USB Type-A

PC に接続して使える USB メモリの標準的なコネクターである。

USB Type-B

プリンター，スキャナ，オーディオなどの PC の周辺機器に採用

USB Type-C

Android スマホ，Mac Book など

Mini USB Type-B

デジタルカメラやモバイルバッテリーなど

Micro USB2.0 Type-B

Android スマホやタブレットなど

Micro USB3.0 Type-B

PS4 や外付け HDD など

Lightning

iPhone，iPad，iPod，Apple Watch など

課　題

1．データ記憶装置の特性に合った利用法について説明しなさい。

第 15 講　暗号化

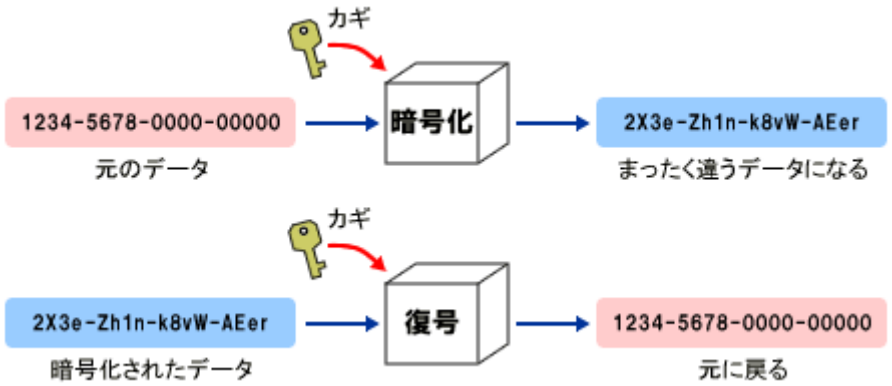
【学修到達目標】

- 暗号化の仕組みを理解できる。
- 情報セキュリティポリシーについて説明できる。

1．暗号化

暗号化とは，データの内容を他人には分からなくするための方法である。コンピュータを利用する際に入力するパスワードが，そのままの文字列でコンピュータ内に保存されていたとしたら，そのコンピュータから簡単にパスワードを抜き取られてしまう危険性がある。そのため，通常パスワードのデータは，暗号化された状態でコンピュータに保存するようになっている。

暗号化は，元のデータを暗号のシステムを使い暗号化する。この時に暗号鍵と呼ばれるデータを使用する。このような仕組みで暗号化をすると，元のデータは，まったく違うデータになる。暗号化されたデータは，同じように暗号のシステムを使い元のデータに戻す。これを復号と呼び，この際に暗号化の時と同じように暗号鍵を使う。つまり，暗号化をするときに使う暗号鍵が非常に重要な役割を果たす。これが他人に渡ってしまうと，暗号化したデータが読まれてしまうことになる。そのため，この暗号鍵は暗号化通信に関係のない人に渡ったりすることがないよう厳重に管理しなければならない。



Web ページの送受信データ，電子メール，無線 LAN による通信データにおいても，データを利用者以外にはわからなくするために，さまざまな暗号化技術が使われる。暗号技術を応用した仕組みとして，電子署名や電子証明書がある。電子署名を利用することにより，情報の送信元のなりすましやメッセージの改ざんが行われていないことを確認することができる。電子証明書は，電子署名技術を用いて，Web サイ

トや電子メールが正しいものであるかを証明するものである。Web ブラウザやメールソフトに表示される鍵のマークをクリックして,「証明書の表示」を選択することにより，その Web サイトや電子メールが正しいものであるかどうかを確認できる。

SSL（Secure Socket Layer）とは，インターネット上でデータを暗号化して送受信する仕組みのひとつである。クレジットカード番号や，一般に秘匿すべきとされる個人に関する情報を取り扱う Web サイトで，これらの情報が盗み取られるのを防止するため，広く利用されている。また，SSL は暗号化に加え，電子証明書により通信相手の本人性を証明し，なりすましを防止するなど，今日のインターネットの安心・安全を支えている。SSL は，Web サーバと Web ブラウザとの通信においてやりとりされるデータの暗号化を実現する技術である。インターネットバンキングで利用者登録する場合などは，この SSL を使ったホームページが使われる。入力された情報は暗号化され，金融機関の Web サーバに送られる。これにより，通信の途中で情報が盗み見られることを防いでいる。Web ブラウザにより，SSL を使ったサイトに接続するには，http://･･･で始まるアドレスではなく，https://･･･で始まるアドレスのサイトに接続する。SSL を利用したサイトに接続すると，アドレスバーの色が緑色に変わったり錠のマークが表示されたりする。これらにより，SSL 通信を使っているサイトかどうかを確認することができる。電子証明書などの詳細な情報を確認できる。Web ブラウザの種類やバージョンによっては，他の場所に保護を示すマークが表示されるので，普段，使用している Web ブラウザではどこにどのようなマークが出るかということを，あらかじめ確認しておく。

暗号化は技術の進歩とともに高度になり，安全にインターネット等を利用できるようになってきたが完璧ではない。パソコンを家族で共用して使用している場合，家族の誰かが勝手にファイル共有ソフトをインストールしたために，情報が漏洩したなどの事故も起こっている。こうした事故を防ぐために，家族共用のパソコンを使う場合は以下の点に注意する。

パソコンを購入したら，家族の一人ずつに一般ユーザ権限のアカウントを作成し，アカウントの共有はしないようにする。これは，万が一，家族の誰かがウィルスに感染したり，ファイル共有ソフトを導入したとしても，別の家族のデータに影響が及ぶ可能性を低くすることができるためである。

管理者権限は，ソフトウェアのインストールなど，必要な時だけ使用し，通常時には一般ユーザ権限で使うようにする。これにより，危険性の高いソフトウェアを家族が不用意に導入する可能性を低くすることができる。

スマートフォンはパソコンに近い性質を持った情報端末である。大切な仕事上のデータや，位置情報などのプライバシー情報がスマートフォンに保存されるようになったことで，情報漏洩が発生した場合のリスクがいっそう大きくなっている。またスマートフォンは，アプリケーションをインストールすることで，

さまざまな機能を追加することができる。この便利な性質が，一方でパソコン同様，スマートフォンがウィルスに感染するリスクを生んでいる。

タブレット端末はスマートフォンよりも大きな画面の携帯用端末だが，性質はスマートフォンとよく似ており，アプリケーションのインストールにより機能の追加が可能である一方，ウィルスに感染する危険性がある。

携帯電話・スマートフォンは持ち歩いての利用も多く，紛失したり盗難にあったりする可能性が高くなる。そのような対策として，本人しか使用できないようにパスワードロックをかける機能や，遠隔ロックする機能を利用することが有効である。また企業や組織などで利用している端末を紛失した際には，管理者にすぐ連絡して，指示を仰ぐなどの対応をする。

携帯電話・スマートフォンに保存された個人情報を目的として，廃棄された端末を売買するといった事例も発生している。携帯電話・スマートフォンを廃棄する際には，必ず登録されているアドレス帳や電子メールなどの個人情報を，確実に消去してから廃棄する。端末販売店で回収をしていることも多いので，そうした信頼できる事業者に廃棄を依頼するか，安全に廃棄できるリサイクル業者を選んで廃棄を依頼する。

スマートフォン・タブレット端末の OS やアプリケーションにはパソコンと同様に脆弱性が報告されることがある。OS やアプリケーションの更新の通知が来たら，忘れずインストールするようにする。

スマートフォン・タブレット端末を狙ったウィルスが発見されている。ウィルスは通常，アプリケーションの中に紛れ込ませる形で配布されており，これまでに，勝手に SMS(ショートメッセージサービス)の送信を行うものや，ワンクリック詐欺の機能を持つものなどが見つかっている。スマートフォンには機種に応じてウィルス対策ソフトが提供されているので，ウィルス対策ソフトを入れることを検討する。

通常，アプリケーションは契約している携帯電話会社や OS・機器メーカー等の公式サイトからダウンロードして利用するが，スマートフォンの機種によっては，それ以外のサイトから自由にアプリケーションをダウンロード可能なものもある。最近のアプリケーションには，ウィルスだけでなく，端末情報や電話帳内の情報などを十分な説明なく収集するものもあり，これらのアプリケーションによって電話帳内の情報が流出してしまった場合，自分だけでなく友人などにも被害を及ぼすことになってしまう。特に，運営者の身元が明らかでないサイトからアプリケーションをダウンロードすることは，こうしたアプリケーションが含まれている可能性があるため，非常に危険である。また最近では，公式サイトに似せた偽のアプリケーション提供サイトの出現も報告されているので，ダウンロードの際には注意する。

アプリケーションの中には，個人情報収集のために，スマートフォン内の電話帳情報などを取得するものがある。インストールする前には，アプリケーションの説明をよく読んで，そのアプリケーションがスマートフォン内のどのような情報や機能にアクセスするのかの表示をよく確認することが必要である。また，インストール時には，本来そのアプリケーションでは使う必要がないと思われる情報（連絡先情報，所有者情報，位置情報など）を収集しようとする確認画面が出てくる場合がある。インストール時に自分の情報の取り扱われ方に不安がある場合は，アプリケーションの利用をあきらめることも検討する。

携帯電話やスマートフォン・タブレット端末には無線 LAN の接続機能が付いている。これらのアクセスポイントは無料のものや有料のものもあるが，なかにはわざと無料のアクセスポイントに見せかけて情報を盗み取るような不正なアクセスポイントがある可能性がある。無線 LAN アクセスポイントに自動的に接続しない設定にするなど，日常的に普段使用している無線 LAN アクセスポイント以外にはできるだけ接続しないようにする。

無線 LAN は，ケーブルの代わりに無線を利用するという性質上，通信内容が傍受（盗聴）される危険性がある。そのため，無線 LAN を使ってユーザ ID やパスワードなどのログイン情報，クレジットカード番号のほか，プライバシー性の高い情報をやり取りする場合には，自分と相手先との間で SSL により通信が暗号化されていることを確認する。家庭内や職場のネットワークで複数のパソコンを利用する際には，家族や職場のパソコンとファイルのやり取りを円滑に行うために，ファイル共有機能を有効にしている人もいるかもしれない。しかし，公共の場で無線 LAN を利用するときに，このファイル共有機能が有効になっていると，他人からパソコンやスマートフォン内のファイルが読み取られたり，ウィルスなどの不正なファイルを送りこまれたりすることがある。公共の場で無線 LAN を利用する際には，必ずファイル共有機能を解除する。

自宅内などに自分で無線 LAN のアクセスポイントを設置して利用する場合には，アクセスポイントで暗号化の設定を行う。Wi-Fi 暗号化方式の種類と特徴は次のとおりである。

WPA とは『Wi-Fi Protected Access』の略で，技術も解読され，簡単に情報を盗める状態にあるため，現在では安全とは言えない暗号化方式である。

WPA 2 は 2004 年に発表された WPA の強化版である。WPA 2 には WPA2（TKIP）と WPA 2 （AES）２種類存在する。WPA 2 （AES）のほうが複雑な暗号なので，解読が難しい。iPhone の場合 iOS14 以降

『WPA・WPA２（TKIP)』の暗号化方式 Wi-Fi と接続した場合，『安全ではないセキュリティー』と表示されるようになった。HTTPS 化されているサイトしか閲覧しないように注意が必要である。フリーWi-Fi など，他者と共有する通信回線の場合には直接攻撃を受ける可能性があるため，利用しない。

WPA３は 2018 年 6 月に発表された最新の暗号化方式である。WPA3 には２種類あり，個人向けの『WPA3-Personal』と企業用の『WPA3-Enterprise』にわかれている。

接続している Wi-Fi 暗号化方式の確認手順を次に示す。

スマホ（iPhone)で暗号化方式を確認する場合には，現状下記の手順で『安全性の低いセキュリティー』が表示されるかどうかで判断する。

アクセスポイントに設定する管理パスワードや，認証・暗号化のための共有鍵は，単純なものや，無線 LAN のネットワーク識別子である SSID から類推できるものにしないよう，注意が必要である。一般的に SSID は公開されて使用されるため，SSID と似たパスワードを設定していると，第三者に類推されてしまう可能性がある。加えて，第三者からの不正なアクセスを防ぐために次の機能も追加的に利用するようにする。設定方法や機能の名称などは，機種によって異なるため，無線 LAN のアクセスポイントに付属しているマニュアルを参照する。

MAC アドレスによるフィルタリングを設定し，接続するクライアントを制限する。

SSID には，利用者や組織などの名称を使わず，SSID 自体を隠すステルス機能を利用する。

さらに，現在はセキュリティ機能を強化した無線 LAN 機器が普及しているので，そのような機器を積極的に利用することが大切である。

MAC アドレスとは，ネットワークに接続されるすべての機器に割り当てられた固有の番号のことである。ネットワーク上の住所のようなものである。MAC アドレスがあることによって，通信の際に相手の機器がどこにいるのかわかるようになっている。

MAC アドレスは，「OSI 参照モデル」の７階層のうちデータリンク層に位置しており，隣接した機器同士で通信する仕組みに関連している。

OSI 参照モデル

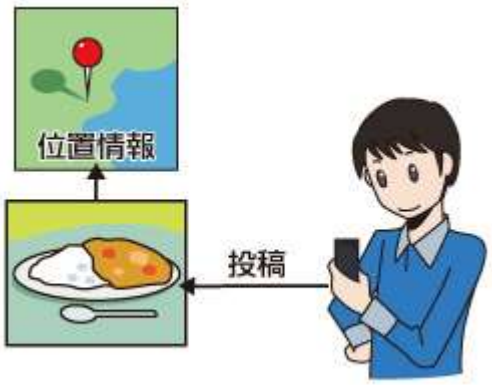
階層	モデル名称	プロトコル
7	アプリケーション層	アプリケーションプロトコル（HTTP など）
6	プレゼンテーション層	
5	セッション層	
4	トランスポート層	TCP，UDP など
3	ネットワーク層	IP，ICMP，ARP など
2	データリンク層	イーサネット，MAC アドレスなど
1	物理層	

SSID（Service Set Identifier）は，アクセスポイントを識別するための名前である。Wi-Fi を使って通信を行うときに，どのアクセスポイントを利用するかを指定するために利用する。自分が使っている PC やスマートフォンが複数のアクセスポイントと無線で通信可能な状況だった時，この複数のアクセスポイントのうち，どれと通信するのかを特定するために利用するのが SSID である。SSID はアクセスポイントの設定画面で変更することが可能であり,ユーザーが自由に指定できる。最近のアクセスポイントでは，出荷時にあらかじめ SSID とパスワードが設定されていて，その内容を記したカードが本体にセットされていたり，シールが本体に貼り付けられているケースがある。Wi-Fi を利用するときに，そのカードやシールに記載された SSID を PC やスマートフォン側で指定し,パスワードを入力すれば Wi-Fi でインターネットに接続できるようになる。この SSID は，5GHz 帯と 2.4GHz 帯で異なるものを設定することが一般的である。最適な周波数帯を自動で選択するバンドステアリング機能に対応した製品であれば，1 つの SSID で 5GHz 帯と 2.4GHz 帯のどちらかに自動で接続する。

スマートフォン・タブレット端末は OS やソフトウェアを変更することで，通常ではインストールできないソフトウェアをインストールできる場合もある。こうしたソフトウェア上の改造を行った端末は，本来のセキュリティレベルを下げ，ウィルス感染の危険性が高まるだけではなく，メーカーのサポート対象外となる可能性がある。また，本来は禁止されているサイトから，不正なアプリケーションをインストールしてしまう危険性も高まる。

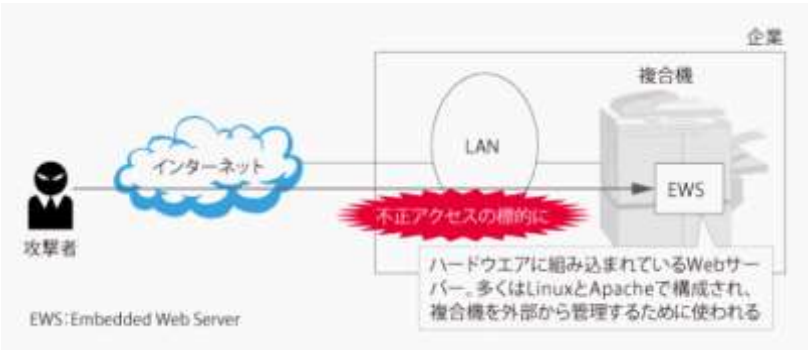
携帯電話，スマートフォン・タブレット端末は，電車や，バスの移動中など人目に触れやすいところで操作する場合，後ろからのぞき見されるなどの危険性もある。人混みの中ではアカウント情報の入力などの機微な操作を行わない，画面操作時に周りの視線に注意する，のぞき見防止シールなどを貼る，などの対策を意識する。

スマートフォン・タブレット端末のような GPS 機能を搭載した端末で撮影した写真には，設定によっては，目に見えない形で，撮影日時，撮影した場所の位置情報（GPS 情報），カメラの機種名など，さまざまな情報が含まれている場合がある。SNS などに，こうした位置情報などが付いた写真をよく確認せずに掲載してしまうと，自分の自宅や居場所が他人に特定されてしまう危険性があり，迷惑行為やストーカー被害などの犯罪の被害に遭う可能性もある。事前に使用している端末の設定を確認しておく。



歩きながらなど，移動しながらスマートフォンを操作していると，周囲の状況に対して不注意になり，トラブルにつながる場合もある。周囲に迷惑をかけないよう，移動しながらの利用は控える。

複合機におけるセキュリティの危険性は，専門家の間でしばしば指摘されてきた。例えば，セキュリティ業界団体「Cloud Security Alliance」の創設者の一人であるミカエル・サットン氏は，EWS（Embedded Web Server）の危険性を挙げる。EWS というのはネットワーク機器に組み込む形で搭載される「Web サーバ」である。



複合機やテレビ会議システム，Web 監視カメラ，IP 電話機など多くの機器が，内部に Web サーバを搭載している。

EWS の主な目的は，機器の自動的な構成管理や遠隔地からの保守点検，課金情報の収集などだ。複合機メーカーなどのシステムと通信して，必要な情報をやり取りする。そのため，

（1）外部からアクセスが可能

（2）Web サーバとして簡素な構成を持つ

という特徴がある。

これが，セキュリティ対策が不十分な Web サーバをインターネット上に公開している状態を生み出している可能性がある。サットン氏は，「メーカーは複合機を出荷した後，全く EWS にセキュリティーパッチ（修正プログラム）を当てていないことが多い」と指摘する。例えば EWS の多くは，Web サーバーソフトに「Apache HTTP Server（Apache：アパッチ）」を搭載している。アパッチは多数のバグが存在するソフトで，バグが発覚する度にパッチを配布している。当然，アパッチには常に最新のパッチを当てておかなければ，簡単にハッキングされる。

狙われるのはアパッチの脆弱性だけではない。複合機が搭載する Linux（リナックス）の脆弱性も放置されている可能性が高く，それも狙い目になる。さらに，宛先情報を窃取される可能性がある点にも注意が必要だ。最近の複合機はメールやインターネット FAX などに使う宛先情報の登録の手間を減らすため，「LDAP サーバ」から情報を取得できるようになっている。ここから，アドレス帳情報が外部に漏えいするといった事案が既に発生している。複合機を使ってスキャンやコピー，プリントアウトした文書

が，外部から見えてしまうという問題もある。“ハッカー御用達”の検索エンジン「SHODAN」を使うと，簡単に複合機の管理画面にアクセスできてしまう。

SHODAN はオンラインデバイスを機種別，国別に一覧表示するサービスで，トップ画面に「Expose Online Devices」（オンラインデバイスを暴く）との表示があるように，インターネットに接続されている Web カメラや複合機などのデバイスを検索できる。

メーカー，機種ごとに固有の文字列を SHODAN に入力して検索すれば，指定したメーカー，機種のデバイスが国別に何台オンライン状態にあるかが分かる。さらに，その一覧から個別の複合機にアクセスできる。SHODAN で検索するだけで，EWS 上で動作する Web サイト（複合機の管理画面）のトップページまでたどりつけるのだ。その管理画面ではさまざまな情報を取得できる。ある複合機では，複合機自身の IP アドレスや MAC アドレスのほか，プロキシーサーバーやデフォルトゲートウエイの IP アドレスなどが見えてしまう状態だった（図 4）。これらは企業ネットワークの構造を把握できる，攻撃者にとっては“おいしい情報”である。

対策は「もっともなもの」ばかりだ。一連の情報漏えいに関する報道を受け，IPA は 2013 年 11 月 8 日，「複合機のオフィス機器をインターネットに接続する際の注意点」と題した文書を公表した。IPA が公開している技術的な対策は，以下の 4 つである。ネットワークでの対策として，

（1）必要性がない場合には，オフィス機器を外部ネットワーク（インターネット）に接続しない

（2）外部ネットワークとオフィス機器を接続する場合には，原則ファイアウォールを経由させ，許可する通信だけに限定する

また，オフィス機器（複合機側）での対策として，

（3）オフィス機器の管理者パスワードを出荷時のものから変更する

（4）オフィス機器のアクセス制御機能を有効にし，データアクセス時に ID，パスワードなどの認証を求める運用にする

いずれももっともな対策である。ただしこの対策を読んで自社の複合機の設定やファイアウォールの設定を確認できる企業にとっては，複合機のセキュリティ問題は無縁だろう。今回の問題に関する報道が意味を持つとすれば，改めて複合機も IT 機器の一つであることを企業や団体の経営者やシステム関係者に認識させた点にある。ほとんどの場合，コピー機は総務部門や庶務部門の所管とされ，IT 機器であるとの認識がない組織が多いことが，この問題の根本的な原因の一つである。■なぜ学術機関の複合機が丸見えになるのか

IPA が示す対策（1）は，当然と思われるだろう。IPA は，11 月 8 日の発表の冒頭で「学術関係機関において複合機の情報がインターネットから閲覧できる状態になっていることが問題となっていることを受け，組織のシステム管理者に対し，広く対策の徹底を呼びかけるため，注意喚起を発することにしました」と述べている。もちろん，外から丸見えになっている複合機を保有するのは学術関係機関に限らず，民間企業も例外ではない。学術関係機関が特に目立つのは，複合機に対して，インターネットに接続された機器に一意に割り当てられる「グローバル IP アドレス」が振られている例が，民間企業に比べて圧倒的に多いからだ。その背景には，大学をはじめとする学術関係機関は，その規模の割に民間企業と比して潤沢な数の IP アドレスが割り当てられていることがある。だとすると今後，IP アドレスの IPv6 への移行が進み，すべての機器にグローバル IP アドレスを割り振れるようになれば，こうした事態が多くの組織で起こりかねない。

対策（2）は，システム部門の担当者からすれば当然の対策だが，果たして明確なシステム部門を持たない中小企業の場合には可能な対策だろうか。こうした企業の多くは，IT 機器の設定はすべて業者任せである。ましてや IT 機器であるとの認識がない複合機などは，IT 機器の後に追加で設置されることが多いと推測される。システム委託先の技術者の関心が低ければファイアウォールの設定が見直されることはなく，複合機が設置されることも珍しくないのだろう。

対策（3）ももっともな対策だが，今まで複合機のユーザは，複合機の設置にあたって管理者パスワードの設定変更が重要だと説明されることは少なかったようだ。そのような機能があることさえ知らないで利用しているユーザは，今も少なくないと推測される。さらに付け加えるなら，複合機のデフォルトパスワード（工場出荷時）は，その機種のマニュアルをインターネットで検索すれば容易に見つけられてしま

う。デフォルトパスワードは機器 1 台ごとに変えて，例えば固体番号にするなどの工夫がメーカーには求められる。

対策（4）については，そもそも古い機種では ID とパスワードによる認証機能がないものがある。こうなると複合機の制御システムの変更が必要になるが，制御システムはコピー機内の ASIC（特定用途向け IC）に焼き付けられているため，容易に変更できないのだ。この事実は，既知のセキュリティホールが放置される問題の根本原因になる。新製品の開発に当たって，メーカーが取り組むべき大きな課題だろう。

複合機の新たな脅威として，内部から外部に向かっての「アウトバウンドの DOS （Denial of Service）攻撃」が浮上している。毎年，米国ラスベガスで開催され，全世界から 2 万人近い自称“ハッカー”が集う大規模な祭典「DEFCON」で筆者が注目したのは，プリンタを踏み台として使用した DOS 攻撃だった。DOS 攻撃は外部から内部への「インバウンドの攻撃」が常識的だが，ここで実演されたのは内部から外部への DOS 攻撃だった。発表者は，舞台に設置したネットワーク内にあるプリンタからそのネットワーク上のルータへ DOS 攻撃を仕掛けた。結果はプリンタの勝利で，あえなくルータはダウンしてしまった。

こうした攻撃がサイバーテロに応用される可能性が高い。サイバー攻撃は永遠に続くものではなく，原因が特定されればそれらは排除され，いずれシステムは復旧する。しかし攻撃者はサイバー攻撃のダメージを最大化させるため，ウィルス検知を妨害したり，攻撃元の IP アドレスを短時間に変えて攻撃を持続させたりするのが最近の特徴だ。ここでネットワーク内にあるプリンタを乗っ取って，ここから DOS 攻撃を仕掛けるという，通常では想定しえない攻撃を受けたらどうなるだろう。ルータがダウンすれば多くのシステム管理者は，まず電源の再投入を試みるが，それでも攻撃は続くため，ルータはすぐさま再びダウンする。プリンタから DOS の攻撃パケットが発信されていることに気付くまでに，相当な時間を要する可能性がある。これはサイバー攻撃のダメージをできるだけ大きくしたいと考えるテロリストにとっては，非常に魅力的な攻撃手法だ。DEFCON でこの攻撃手法を公開したグループは，攻撃ツールとしてプリンタ以外に Web カメラや IP 電話機などでも応用できる点を指摘していた。

もちろん，どの攻撃でも対策は打てる。重要なのは，こうした攻撃を想定し得るかどうかという企業マネジメントの問題であることだ。システム管理者は TCP／IP プロトコルで通信される機器のすべてを管理下に置き，セキュリティ対策に抜かりがないかを点検する必要がある。

一方，メーカーに求めたいのは，IT に詳しくない企業ユーザでも，意識することなく安全に使用できる機器の開発である。「ファイアウォールの設定が適切に行われていれば心配無用」との説明は，専門の担当者がいない中小企業には通用しないだろう。

2. 情報セキュリティポリシー

① 情報セキュリティポリシー

企業や組織において実施する情報セキュリティ対策の方針や行動指針

② 記載内容

情報セキュリティポリシーには，社内規定といった組織全体のルールから，どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方，情報セキュリティを確保するための体制，運用規定，基本方針，対策基準などを具体的に

情報セキュリティ対策は画一的なものではなく，企業や組織の持つ情報や組織の規模，体制によって，大きく異なる

業務形態，ネットワークやシステムの構成，保有する情報資産などを踏まえた上で，その内容に見合った情報セキュリティポリシーを作成

③ 目的

企業の情報資産を情報セキュリティの脅威から守ること

導入や運用を通して社員や職員の情報セキュリティに対する意識の向上や，取引先や顧客からの信頼性の向上といった二次的なメリットを得ること

④ 大切なこと

情報セキュリティ担当者だけがネットワークやパソコンなどに対する情報セキュリティ対策を心がければよいというものではない

情報資産を共有するすべての社員や職員が適切な情報セキュリティ意識を持たなければ，ウィルス，情報漏洩などから組織を防御することは困難

⑤ 構成

「基本方針」,「対策基準」,「実施手順」の３つの階層

⑥ 体制

情報セキュリティポリシーを策定し運用するには，まず責任者を明確にして，情報セキュリティポリシー策定に携わる人材を組織化することが必要

組織の活動内容が情報セキュリティポリシー策定・運用の成果に大きく影響するため，企業や組織の実情や現在の社会状況に見合った情報セキュリティポリシーを策定・運用するためには，適切な人材を確保する

情報セキュリティポリシーの品質を高めるためには，外部のコンサルタントや法律の専門家に参加を依頼

⑦ 情報セキュリティ教育

策定した情報セキュリティポリシーに関して，組織幹部も含め全社員や職員に情報セキュリティ教育を実施して，遵守することを徹底

情報セキュリティに関する同意書にサインしてもらう，違反時の規定を設けるなどの方法で，情報セキュリティポリシーを意識させる仕組みが必要

情報セキュリティ診断システムなどを利用して，導入した情報セキュリティ対策の効果や情報セキュリティポリシーの浸透具合をチェック

すべての社員や職員が遵守するからこそ，情報セキュリティポリシーに意味があり，情報セキュリティ対策が効果的になる

情報セキュリティに対する意識を社員や職員一人一人に啓発することが，企業や組織における大切な情報セキュリティ対策のひとつ

⑧　情報収集

情報セキュリティ上のリスクは，常に変化している

情報セキュリティ対策もその変化に対応できなければならない

常に最新の情報セキュリティ関連の情報を収集する体制が必要

収集した情報を参考にして，現在の情報セキュリティポリシーの内容に不足している項目がないかどうかを評価

⑨　評価，監査，リスク分析

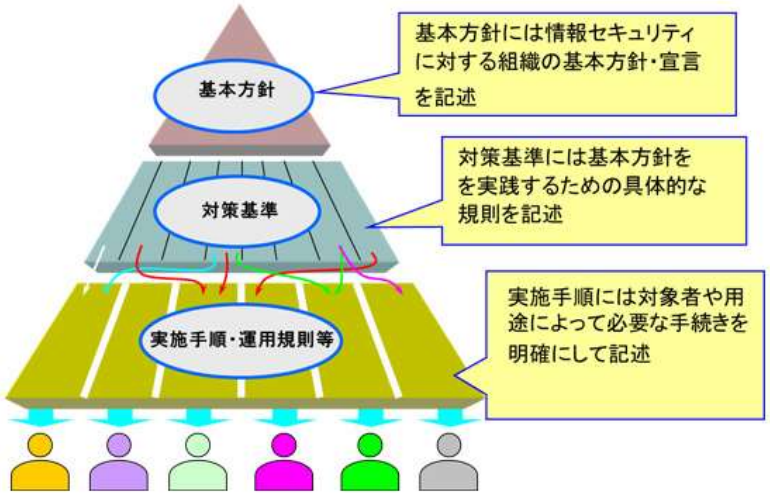
評価のためには，日常的に社員や職員へのモニタリングを行い，情報セキュリティポリシーが適切に守られているか，有効に機能しているかなどについての調査，定期的な監査，変動するリスクの分析などを行う

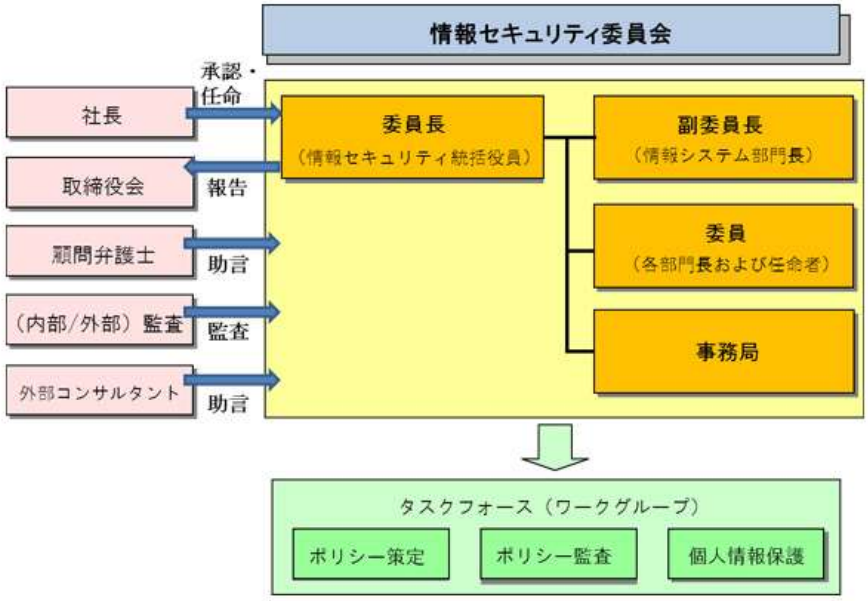
評価をする際には，情報セキュリティポリシーが現場の状況に適合しているか，最新の法律や企業や組織の現状を踏まえ，情報セキュリティポリシーに不備や不足はないか，なども考慮する必要がある

⑩　見直しと改訂

評価，監査，調査の結果，社員や職員からの要求に基づいて，情報セキュリティポリシーの見直しと改訂を行う

改訂した情報セキュリティポリシーは，再び計画のプロセスを経て，運用に移す





課　題

1．セキュリティ対策について説明しなさい。

資　料　肖像権

【学修到達目標】

⋕肖像権について理解し，対処の仕方を説明できる。

１．肖像権

肖像権とは，一般的に，人がみだりに他人から写真を撮られたり，撮られた写真をみだりに世間に公表，利用されない権利といわれている。法律上明示的に認められた権利ではなく，人格権に基づくものとして裁判例上認められてきた権利である。インターネットや SNS の流行等を踏まえ，肖像権侵害が問題となることも多くなってきている。人物の肖像の人格的利益に着目した肖像権を，狭義の肖像権といい，一般的に「肖像権」というときは，狭義の肖像権を指すことが多い。判例でも，人には，その容ぼう等を勝手に撮影等されない権利（狭義の肖像権）が保障されているといえる。人物の肖像の財産的価値に着目した肖像権を，パブリシティ権という。人の氏名，肖像等（以下，併せて「肖像等」という。）は，個人の人格の象徴であるから，当該個人は，人格権に由来するものとして，これをみだりに利用されない権利を有すると指摘している。さらに，「肖像等は，商品の販売等を促進する顧客吸引力を有する場合があり，このような顧客吸引力を排他的に利用する権利」を「パブリシティ権」と定義し，パブリシティ権についても，「肖像等それ自体の商業的価値に基づくものであるから，上記の人格権に由来する権利の一内容を構成するものということができる」と判示しており，肖像等がもつ顧客吸引力という財産的利益はパブリシティ権として保護されているといえる。パブリシティ権は，肖像等が持つ財産的利益を保護する権利ではあるが，肖像等に発生する権利であるため，人格権に由来する権利の一つと考えられている。また，肖像権は，人であれば誰にでも発生する権利といえるが，パブリシティ権は，肖像等が有する顧客吸引力を利用する権利なので，肖像等に顧客吸引力を有するような，著名人・有名人に発生する権利といえる。

1)「オジサン」の写真投稿で若い女性のツイッターが炎上

遊び心では許されない…若い女性の中高年盗撮，ＳＮＳ投稿で訴訟も

スマホの普及で，今や誰もがどこでも簡単に写真が撮れる時代。撮った写真をツイッターやフェースブックなどＳＮＳに投稿する人も多いだろう。しかし，無断で撮影した人物の写真の投稿は，訴訟に発展する可能性もある。ちょっとした遊び心では許されないこともあるので，注意が必要だ。（平沢裕子）

女性が盗撮の加害者に

「目の前のおっさん，きもい（笑）」－こんなコメントといっしょにツイッターに投稿された薄毛の男性の写真。電車でだらしなく熟睡しているサラリーマンや熱心にスマホを操作している太った男性の写真もある。いずれも若い女性とみられる人の投稿で，ツイッターが炎上したと週刊誌などで報じられたケースだ。以前は盗撮される対象といえば若い女性の方だったが，最近は「女性による中高年男性の盗撮→ツイッターなどＳＮＳへの投稿」も多いようだ。

ただ，女性のスカートの中を盗撮するのは明らかな犯罪行為だが，電車内のおじさんの姿を撮影することも犯罪やルール違反に当たるのだろうか。ＩＴ関連トラブルの法的問題に詳しい森居秀彰弁護士は「本人の同意を得ずに勝手に撮影すれば，肖像権の侵害に該当する可能性がある。直ちに犯罪行為となるとは限らないが，民事責任として損害賠償請求を問われる恐れはある」と指摘する。

ビール腹だけならＯＫ？

肖像権とは，みだりに自己の容貌や姿態を撮影されたり，撮影された肖像写真を公表されたりしない権利（人格的利益）をいう。つまり，電車内で見かけた人を承諾を得ずに勝手に撮影すること自体が，肖像権の侵害とみなされる可能性があるという。

スマホでエロ画像を見ている男性を撮り「おっさん…電車の中ではやめとけや笑」

スマホでエロ画像を見ているサラリーマンを撮り「おっさん…電車の中ではやめとけや笑。たまりすぎやろ爆笑」。ある女子高生が電車内にいた頭髪の薄い男性を写真付きであざ笑うような投稿をすることも。

「女性はきもいと感じた男性を話題にする傾向がある。テレクラがはやっていたときもそう」ＩＴジャーナリストの井上トシユキ氏は「女性はきもいと感じた男性を話題にする傾向がある。テレクラがはやっていたときもそう。女子中学生がテレクラでオッサンと駅前で待ち合わせをして，遠くから友達と，オッサンが来ているのを確認して『きもいヤツが来た』なんて笑い合う。それが今，ツイッターになった」と指摘する。

2)　新聞記者が乗客の足下の写真を投稿して炎上した例も

「品川で乗ってきた窓側の女が，ずっと，無言で泣いています」と隣席の女性の足下の写真を投稿

また６月には，新幹線で隣の席で泣いていた女性の足下の写真を投稿し朝日新聞記者のツイッターが炎上したこともある。記者は乗車中に「３人がけの通路側なう。品川で乗ってきた窓側の女が，ずっと，無言で泣いています」「女の涙って，ものすごくストレス」などと投稿していた。

記者は翌日，謝罪文を投稿する結果に…

【おわび】 昨日投稿いたしました，新幹線車内での女性の涙に関連した計 8 本のツイートに対し，不快である，といったご指摘を多数いただきました。当該ツイートは適切な内容ではありませんでした。一連のツイートを削除の上，ご不快にさせました皆様におわびいたします。申し訳ありませんでした。

実は勝手に撮影しただけで肖像権の「侵害」になる

電車内のおじさんの姿を撮影することも「肖像権の侵害に該当する可能性」

ＩＴ関連トラブルの法的問題に詳しい森居秀彰弁護士は，前出の若い女性たちの行為について，「本人の同意を得ずに勝手に撮影すれば，肖像権の侵害に該当する可能性がある。直ちに犯罪行為となるとは限らないが，民事責任として損害賠償請求を問われる恐れはある」と指摘する。

写真で「○○さんだ」と個人が特定されない場合は，「侵害」に当たらない可能性が高いが…

肖像権の侵害に当たるのは，撮影した写真で個人が特定できる場合。手や足などのパーツや後ろ姿，ビール腹のおなか周りなど，写真を見て「○○さんだ」と個人が特定されない場合は，通常，被写体になった人に心理的な負担を与えることはなく，肖像権の侵害に当たらない可能性が高い。

3) 女性の足だけを撮影した場合も，自治体によっては条例違反の恐れ

顔を写さずにミニスカートの女性の足だけを撮るのは，自治体によっては条例違反に当たる可能性もある。

ズボンの上からの撮影で「卑猥な言動」に該当すると定める条例も

２０１４年１０月には，静岡県御殿場市で県職員の男性（５３）がスマホで，ズボンを履いていた女性（２４）の下半身を盗撮し，県迷惑防止条例が定める「卑猥な行動」に該当するとして逮捕された。同条例第３条では，「正当な理由がなく，人を著しく羞恥させ，又は人に不安を覚えさせるような方法で，次に掲げる行為をしてはならない」としている。

許可を得て撮影しても無断掲載で訴訟に発展する可能性

街でファッションスナップを撮られた女性が訴訟を起こす。掲載した側に慰謝料の支払い命令判決

過去には，街でファッションスナップを撮られた女性が訴訟を起こした例がある。写真をウェブサイトに掲載した側に対し，慰謝料として３０万円の支払いを命じる判決が確定している。

「女性に強い心理的負担を覚えさせ，肖像権を侵害した」とする判決理由

女性の写真は，最先端のストリートファッション情報の発信という目的で撮影・掲載されたものだったが，写真がサイトに掲載されたことで「女性に強い心理的負担を覚えさせ，肖像権を侵害した」などとして，精神的苦痛を与えたことに対する慰謝料が認められた。

4)　知らない人が写り込んだ自撮り写真の投稿も注意

「社会生活上，我慢できる限度を超えるほどの肖像権の侵害かどうかで判断」と弁護士

前出の森居弁護士は，大勢いる中で自撮りした写真に知らない人が写っていた場合，その写真をそのままＳＮＳに投稿することについて，損害賠償請求されるか否かは「基本的には，被写体となってしまった人に社会生活上，我慢できる限度を超えるほどの肖像権（人格的利益）の侵害かどうかで判断される」と話す。

「一般的に観光地の記念写真などで問題が生じる余地は少ない」とも

森居弁護士は同時に「一般的に観光地の記念写真などで問題が生じる余地は少ないとみられる」と指摘する。

5) もちろん，芸能人の写真を投稿するのもＮＧ

肖像権に含まれる「パブリシティー権」の侵害に当たる恐れ

芸能人を発見して一緒に写真を撮ってもらえたとしても，それを SNS に投稿することは肖像権に含まれる「パブリシティー権」の侵害に当たる。パブリシティー権とは，個人の氏名・肖像が持つ商業的価値を保護する権利。侵害すれば芸能事務所に訴えられる恐れもある。

加害者にならないために…

ＳＮＳで写真を投稿する際は以下の対処を

一緒に写っている人物にＳＮＳ投稿の許可を得る

写り込んでしまった関係のない一般人は，モザイク機能やトリミングなどの加工でごまかす

ドローンでの撮影時には，住居内が写り込まないよう住宅地にカメラを向けない

総務省の研究会が５月にまとめた，小型無人機「ドローン」のカメラで撮影した映像をインターネット上で公開する際の指針には，住宅地では生中継で映像を配信しないことや車のナンバープレートなどにはぼかしを入れることなどを要求している。高所から撮影できるドローンは「のぞき」などに悪用される恐れがあるため。

用　語

アイコン
コンピュータ上で，操作する対象を表現した小さな図やイラストのこと。
アイコン（ICON）とは肖像・図像の意味を持つ言葉です。パソコンの表示画面から，マウスでアイコンを指示することで，直感的な操作を可能にしています。たとえば，マウスでクリックすると印刷が開始されるプリンタのイラストのように，操作を表すアイコンと，ハードディスクの中に表示される文書やシートのマークのように，ものを表すアイコンがあります。

アカウント
コンピュータやソフトウェア，ネットワークなどを使用するための権利や資格のこと。
また，それらのシステムにログインするために必要な ID とパスワードの組み合わせをアカウントと呼ぶこともあります。アクセス権限（アクセス・けんげん）コンピュータシステム上で，プログラムの実行や，データの参照，追加，変更，削除などをできる資格のこと。
企業や組織などでは，データの内容に応じて，利用者やグループごとに異なるアクセス権限を設定したりします。たとえば，機密情報を含むファイルについては，アクセス権限を必要な利用者のみに適切に設定すれば，安全性を高めることができます。

アクセスポイント
通常は，無線 LAN アクセスポイントを指します。アクセスポイントは，ノートパソコンやスマートフォンなどの無線 LAN 接続機能を備えた端末を，相互に接続したり，有線 LAN など他のネットワークに接続するための機器です。「親機」，「基地局」，「ステーション」などとも呼ばれます。

アクセスログ
利用者がソフトウェアやネットワーク機器などに接続した履歴（記録）のこと。
例えば，Web サーバのアクセスログであれば，接続元の IP アドレスや接続日時，閲覧されたファイル名などを確認することができます。

アップデート

OS やソフトウェアの一部または全部のプログラムを更新すること。
プログラムの不具合の修正や, 脆弱性対策, 小規模の機能追加などのために行います。アップロード自分のコンピュータから，ネットワーク上の Web サーバや FTP サーバなどにファイルを保存すること。

アドミニストレータ
コンピュータやネットワーク，データベースの管理者，または管理する権限のこと。
管理者とは，あらゆる権限を与えられる利用者を表します。そのため，アドミニストレータ権限を第三者に使用されてしまうと，コンピュータシステムを破壊されたり，格納されているデータを盗まれたり改ざんされたりする可能性があります。

アドホック・モード
無線 LAN のクライアント同士が, アクセスポイントを介さず, 直接通信を行う通信方式のこと。
ピア・ツー・ピアモードまたはインディペンデントモードなどとも呼ばれています。これに対して, 無線 LAN クライアントがアクセスポイントを経由して通信する方式は, インフラストラクチャ・モードといいます。

アドレス帳
パソコンやスマートフォンで，連絡先を管理するための機能のこと。
電子メールを送信するときには，宛先のメールアドレスを，アドレス帳にあらかじめ登録した相手の氏名やニックネームから選択することで，宛先のメールアドレスを簡単に指定することができます。ソフトウェアによっては，メールアドレスの他に，氏名や住所，電話番号なども登録しておくことができます。

アプリケーション
コンピュータの OS 上で動作するソフトウェアのこと。
ファイル管理やネットワーク管理，ハードウェア管理，ユーザ管理といった基本的な機能を持つ OS（基本ソフト）に対して，ワープロソフトや表計算ソフトといったソフトウェアのことをアプリケーション（応用ソフト）と呼びます。また, スマートフォンの場合は, ゲームをはじめ, 辞書機能や動画再生, 文書作成など, さまざまな目的に応じたアプリケーションがあります。「アプリ」と略されて使われる場合もあります。

アプリケーションサーバ
利用者からの要求を受け付けて，例えばプログラムの実行環境やデータベースへの接続などの仲介を行う機能を持ったサーバのこと。
Web ブラウザを用いて HTTP で通信する「Web アプリケーションサーバ」が主流で，単にアプリケーションサーバと言った場合，Web アプリケーションサーバのことを意味することが多いです。

暗号化
大事な情報を他人には知られないようにするため，データを見てもその内容がわからないように，定められた処理手順でデータを変えてしまうこと。
暗号化されたデータは，復号という処理によって元のデータに戻すことができます。

暗号鍵（あんごうかぎ）
データを暗号化するときに使われる鍵のこと。

アンチウイルスソフト
ウィルス対策ソフトのこと。

位置情報
人や機器などが今存在している場所に関する情報のこと。
例えば，携帯電話やスマートフォンなどの機能として，GPS を用いた位置情報サービスがあります。測定された位置情報は，携帯電話やスマートフォンで撮影した写真や，SNS（ソーシャル・ネットワーキング・サービス）への投稿時のデータなどにも利用されています。

インターネットサービスプロバイダ
インターネットに接続できるサービスを提供する事業者のこと。
通常，電子メールを送ったり，ホームページを閲覧したりするには，インターネットサービスプロバイダと契約する必要があります。

インフラ

インフラストラクチャ（Infrastructure）の略。基盤のこと。
インターネットの世界では，通信環境の設備やそれらを提供するサービスを表す言葉として使用されています。

インフラストラクチャ・モード
無線 LAN のクライアントが，無線 LAN のアクセスポイントを介して他の無線 LAN ノードや有線ネットワークと通信を行う通信方式のこと。

ウィルス
他のコンピュータに勝手に入り込んで，意図的に何らかの被害を及ぼすように作られたプログラムのこと。ディスクに保存されているファイルを破壊したり，個人情報などを盗むこともあります。また感染経路として，ウィルスは，インターネットからダウンロードしたファイルや，他人から借りた CD メディアや，USB メモリ，電子メールの添付ファイル，ホームページの閲覧など媒介して感染します。ウィルスにはウィルス対策ソフトでは検出・駆除できないものもあり，ウィルスに感染したことに気づかずにコンピュータを使用し続けるとウィルス自身が自分を複製する仕組みを持っていた場合には，他のコンピュータにウィルスを感染させてしまう危険性もあります。

ウィルス検知用データ
ウィルス対策ソフトがウィルスを発見するために使用するデータのこと。
ウィルスは日々新しいものが出現しているため，最新のウィルスに対応するためには，ウィルス検知用データを常に最新のものに更新しておく必要があります。
ウィルス検知用データは，ウィルス対策ソフトによっては「ウィルス定義ファイル」や「パターンファイル」，「シグネチャ」などと呼び名が異なります。

ウイルススキャン
コンピュータがウィルスに感染していないかどうかを検査すること。
　一般のウィルス対策ソフトは，通常の動作では，電子メールやファイルのコピーなどで送受信されるデータについて，ウィルス感染を調査するようになっています。そのため，既にコンピュータに感染してしまったウィルスを検出するには，ウイルススキャンを実行する必要があります。

ウィルス対策サービス
ウィルスからコンピュータを防御するためのサービスのこと。
多くの場合，インターネットサービスプロバイダなどが提供しています。このサービスを利用することで，ウィルス対策ソフトと同様に，ウィルスのチェックや駆除を行うことができます。

ウィルス対策ソフト
コンピュータをウィルスから防御するためのソフトウェアのこと。「アンチウイルスソフト」とも呼ばれています。
コンピュータに侵入したウィルスを駆除したり，電子メールなどで送信するファイルにウィルスが含まれていないかどうかをチェックしたりすることができます。他のコンピュータとの通信状況を監視してウィルスの侵入を予防するファイアウォールの機能を備えているものもあります。

ウェブアプリケーションファイアウォール
Web アプリケーションに対して行われる外部との通信を監視し，脆弱性への攻撃や情報の窃取などを防御するファイアウォールのこと。
Web Application Firewall（ウエブ・アプリケーション・ファイアウォール）を略して，WAF（ワフ）とも呼ばれています。 一般的なファイアウォールはネットワークレベルで監視していることに対して，WAF はアプリケーションレベルでの監視を行います。Web アプリケーションの脆弱性によって引き起こされる SQL インジェクションなどを防ぐことができます。

エスケープ処理
Web サーバに送信された入力データの特殊な文字列をあらかじめ別の文字列に置き換えておくこと。
このようにすることで，サーバで不正な処理が実行されることを防ぎます。

炎上
不注意な書き込み等によって，多くの人からの非難を浴びる状況。

エンベロープ情報

電子メールの送信に使われる情報のこと。
メール送信のプロトコルである SMTP を使って通信する際に使用されます。あて先アドレスとなる To（エンベロープ To）と，送信者アドレスとなる From（エンベロープ From）とがあります。

オークションサイト
インターネット上で行われるオークションを開催している Web サイト（ホームページ）のこと。

オートコンプリート
キーボードの入力を補助する機能のひとつ。
過去の入力履歴を参照して次の入力内容を予想し，あらかじめ表示すること。Web ブラウザのアドレス入力などに搭載されています。
また，この機能はパスワードの入力などにも使えますが，情報セキュリティの観点からは第三者でも冒頭の数文字が合うだけでパスワードを入力できてしまいかねません。そのため，オートコンプリートのもととなる入力履歴を消したり，オートコンプリート機能自身を使わないように設定できます。

オプトイン方式
事前に電子メールの送信に同意した相手に対してのみ，広告，宣伝，勧誘等を目的とした電子メールの送信を許可する方式のこと。

オフロード
携帯電話回線のネットワークを流れるデータ通信量の増加を防ぐために，携帯電話やスマートフォンの利用者が，無線 LAN などの別のネットワークを使うよう誘導する仕組み，またはその対策のことを言います。

オンラインストレージ
インターネット上にデータを格納するサービスのこと。
Web ブラウザや FTP クライアントソフトを利用してデータをやり取りする方式のほかに，専用のソフトウェアを利用するサービスもあります。

オンライントレード
インターネット上で行うことができる証券取引サービスのこと。
自分のパソコンなどから証券会社の Web サイトにアクセスすることで，株の売買を行う仕組みです。

拡張子
ファイル名のピリオド以降に指定されている文字列。 ファイルの種類を表す 2～4 字の文字列で，ファイルの種類を表します。たとえば，拡張子が「.exe」のファイルは実行可能なファイルであることを，「.htm」のファイルは HTML ファイルであることを示しています。 Windows では，この拡張子によって，表示されるアイコンが変化します。

仮想化
仮想化とは，コンピュータやハードディスク，OS やアプリケーションなどを物理的構成に拠らず柔軟に分割したり統合したりする技術です。1 台のものをあたかも複数台であるかのように利用できたり，逆に複数台のものをあたかも 1 台であるかのように利用することができたりします。仮想サーバ（かそう・サーバ）1 台のコンピュータを中央演算装置（CPU）やメモリ，ディスクをまとめて仮想的に複数の領域として分割し，それぞれがあたかも 1 台のコンピュータのように複数台の仮想的なコンピュータとして，それぞれに異なる別の OS（オペレーティングシステム）やアプリケーションソフトを同時に実行させる技術を使用したサーバのことを言います。

仮想デスクトップ
サーバやパソコンなどで複数の OS を動かし，ネットワーク経由で個々のデスクトップ端末へ割り当てて通常のデスクトップパソコン同様の機能を実現する技術のこと。
端末側には，記憶装置を持たない「シンクライアント」を使うことが多く使われます。ネットワークにさえ繋がっていれば，利用する環境の違いに関係なく同じ作業環境を提供できます。

可用性
認可された利用者が，必要なときに情報にアクセスできることを確実にすること。
国際標準化機構（ISO）が定める標準に定義されるもので，Availability（アベイラビリティ）の訳語です。

完全性
情報および処理方法の正確さおよび完全である状態を安全防護すること。
国際標準化機構（ISO）が定める標準に定義されるもので，Integrity（インテグリティ）の訳語です。

キーロガー
キーボードからの入力を記録するソフトウェア。
最近は，ウィルスなどを使ってコンピュータに常駐させることで，ユーザ ID やパスワード，クレジットカード番号などを不正に入手するために利用されることが増えています。

記憶媒体
コンピュータで作成したデータを保存しておくもの。
記憶メディアや記録メディア，または単にメディアと呼ばれることもあります。現在のコンピュータで利用されている記憶媒体には，ハードディスク，CD-R，USB メモリなどがあります。

基幹サーバ
情報システムにおいて，業務に密接に関連したサービスを提供しているサーバのこと。
基幹サーバが停止してしまうと，組織の運営そのものに影響してしまうため，通常は信頼性が高く，性能の良いサーバが使用されます。たとえば，企業の場合は，会計管理や販売管理，在庫管理を行うサーバが基幹サーバにあたります。

基幹システム
企業や組織内において，業務の中心的な役割を果たすための情報システムのこと。
業種によって異なりますが，多くの場合は，販売管理システムや在庫管理システムが基幹システムとなります。 基幹システムは，停止した際に業務自体に影響を与えてしまうことと，機密情報が格納されることが多いため，万全の情報セキュリティ対策による安定性と安全性とが要求されます。

機密性
情報にアクセスすることが認可されたものだけがアクセスできることを確実にすること。

国際標準化機構（ISO）が定める標準に定義されるもので，Confidentiality（コンフィデンシャリティ）の訳語です。

キャッシュ
データを一時的にメモリやディスク上の領域に格納して，次回の Web サイトへのアクセスの際にサーバにアクセスすることなく表示できる複製されたデータのこと。
サーバへのアクセスを軽減するとともに，表示の高速化が可能となります。

共通鍵
共通鍵暗号方式で使われる暗号鍵のこと。
暗号化と復号とで同じ共通の鍵を使用するため，こう呼ばれています。

共通鍵暗号方式
暗号化と復号で同じ鍵を使用する暗号方式のこと。
同じ鍵を持つ人の間で，途中で覗き見されることなくデータを送受信できます。
処理速度が速い半面，相手先ごとに固有の鍵を作成し，管理しなければならないという特性があります。大きなサイズのデータの暗号化や，限られた特定の相手とのやり取りに使われます。

共有フォルダ
複数の利用者がアクセスできるように設定したコンピュータ上のディスク領域のこと。
現在の Windows では，サーバだけでなく，クライアントでも共有フォルダを作成することができます。
共有フォルダは，利用者にとっては便利なものですが，適切な設定を行わずに利用した場合には，ネットワーク上からファイルを参照できてしまうため，情報セキュリティ上のリスクとなることがあります。共有フォルダを安全に利用するには，指定した利用者だけがアクセスできるようにアクセス制限をかけておく必要があります。

クライアント
ネットワーク上で情報やサービスを利用するコンピュータのこと。 通常は，一般利用者が使用するコンピュータがクライアントになります。 なお，クライアントが要求した情報やサービスを提供するコンピュータは，サーバと呼ばれています。

クラウドコンピューティング
インターネット上のネットワーク，サーバ，ストレージ，アプリケーション，サービスなどを共有化して，サービス提供事業者が，利用者に容易に利用可能とするモデルのことです。クラウドコンピューティングには主に仮想化技術が利用されています。

クラウドサービス
クラウドサービスは，クラウドコンピューティングの形態で提供されるサービスです。従来は，利用者側がコンピュータのハードウェア，ソフトウェア，データなどを，自身で保有・管理し利用していました。クラウドサービスでは，利用者側が最低限の環境（パーソナルコンピュータや携帯情報端末などのクライアント，その上で動く Web ブラウザ，インターネット接続環境など）を用意することで，さまざまなサービスを利用できるようになります。
クラウドサービスは,主に SaaS（Software as a Service）,PaaS（Platform as a Service）,IaaS（Infrastructure as a Service）の 3 つの形態で提供されています。

クラッカー
悪意を持って，システムに不正侵入したり，データの改ざんや破壊などを行ったりする人のこと。クラッキング重要ワード悪意を持って，システムに不正侵入したり，データの改ざんや破壊などを行う行為。

グループウェア
組織や企業で LAN を活用して情報共有やコミュニケーションの効率化を図り，グループで作業することを支援するソフトウェアの総称のこと。 主な機能としては, グループ内のメンバー間や外部とのコミュニケーションを行う電子メール機能，メンバー間の打ち合わせや議論などを行うための電子会議室機能，メンバー間の打ち合わせに利用されるテレビ会議機能，グループ全体に情報を伝達する電子掲示板機能，スケジュールを共有するスケジューラ機能,そのほか文書共有機能,決済や稟議などの通常の業務処理を電子化するワークフロー機能などがあります。実際の製品はこうした各機能のうちいくつかを組み合わせたものが多く，Web ブラウザからすべての機能を利用できるようにした製品が主流になりつつあります。

グローバル IP アドレス
インターネットにおいて，全世界で固有の番号を持つ IP アドレスのこと。 企業や組織内のネットワークでは，利用者が自由に使うことが許可されているプライベート IP アドレスという番号を使用して，コンピュータを管理します。しかし，プライベート IP アドレスでは,インターネット上で数多くのコンピュータが重複することになるため,インターネットに接続する場合には，すべてのコンピュータがグローバル IP アドレスを使用しなければなりません。 現在のアドレス体系では，全世界のコンピュータにグローバル IP アドレスを割り当てるには, アドレスの数が不足しているため, ルータがプライベート IP アドレスとグローバル IP アドレスの変換作業を行います。個人利用者の場合には, プロバイダから一時的にグローバル IP アドレスを割り当ててもらいます。

公開鍵
公開鍵暗号方式による暗号化を利用する場合に，相手に渡す鍵のこと。パブリック鍵とも呼ばれます。多くの場合，不特定多数に公開します。

公開鍵暗号方式
公開鍵暗号方式は，暗号化と復号とで異なる鍵を使用する暗号方式です。一方の鍵を公開鍵，もう一方を秘密鍵とすることで，途中で覗き見されることなくデータを送信したり，改ざんを検知できたりします。多くの人と暗号化して情報のやり取りをするときに有効で，電子証明書やデジタル署名等で使用されます。

公衆無線 LAN
駅や街中など，公共の場所で利用できるように設定された無線 LAN の施設やサービスのこと。

個人情報保護法
個人の権利と履歴を保護するために，2005 年 4 月から施行された法律。 個人情報保護法では，個人情報を所有する事業者に対する義務や対応を定めています。

個体識別番号
ワンクリック詐欺で利用される言葉。 個体識別番号とは, 携帯電話から個人を識別できたように見せかけるために Web サイトに表示される番号です。しかし，これらの番号から

は個人情報（氏名や住所，電話番号）を入手することはできません。 固体識別番号と表記されている場合もあります。

固有識別番号
ワンクリック詐欺で利用される言葉。 個人を特定できたように見せかけるために使用される言葉ですが，その多くはインターネットサービスプロバイダの情報などであり，実際に個人を特定できる情報がインターネットに流れているわけではありません。

コンテンツ
「内容」や「中身」を表す言葉。 インターネットでは，ホームページ上の情報をコンテンツと呼んでいます。また，小説や映画，テレビ番組，音楽などを電子化したデータについてもコンテンツと呼びます。

コンピュータシステム
ハードウェアやソフトウェア，環境設定などを含むコンピュータで動作する一まとまりの仕組みや機能全体のこと。 コンピュータを利用して動作する情報システムの仕組みのことを，コンピュータシステムと呼ぶこともあります。

サーバ
ネットワーク上で情報やサービスを提供するコンピュータのこと。
逆に，サーバに対して，情報やサービスを要求するコンピュータをクライアントと言います。
例えば，インターネットでは，Web サーバやメールサーバ，DNS サーバなどが使用されています。

サーバ証明書
SSL(TLS)を用いて，利用者がアクセスしているサーバが「本物」であることを保証する電子的な証明書のこと。
例えば，インターネットバンキングや，ショッピングサイトなど，利用者がアクセスする Web サーバなどの真正性が重要となる場面で使用され，そのサーバと暗号化通信を行うためにも使用されます。サーバ証明書は，認証局と呼ばれる第三者機関によって発行されます。

サービスパック
マイクロソフト社が Windows や Office アプリケーション用に提供するひとまとまりの更新プログラムのこと。 Windows や Office アプリケーションに対する不具合修正やセキュリティ対策などの更新プログラムは，通常インターネットで随時公開されますが，一定期間経過したところで，それまでに修正したすべてのプログラムがまとめて提供されることがあります。マイクロソフト社では，このようなプログラムをサービスパックと呼び，製品別に提供しています。 また，サービスパックの提供に合わせて，初めからサービスパックが追加された形で，Windows や Office アプリケーションのパッケージが提供されることもあります。

サンドボックス
サンドボックスとは「砂場」を意味し，アプリケーションを保護された領域で動作させることによって，システムが不正に操作されるのを防ぐセキュリティモデルのこと。

識別子
“もの”を特定するための番号や名前のこと。 コンピュータの世界では，コンピュータ名やネットワーク上の IP アドレスが識別子として使用されています。

システム
コンピュータで動作するひとまとまりの仕組みや機能のこと。 なお，コンピュータシステムという言葉は，ハードウェアやソフトウェア，環境設定などを含んだコンピュータそのものを表すこともあります。

自動実行機能
Windows などの機能のひとつで，外部記憶装置（USB メモリなど）をコンピュータに認識させると，内部に記録されたプログラムのうち指定されたものを自動的に実行する機能。Auto Run（オートラン）機能とも呼ばれます。 CD や DVD などをパソコンのドライブに挿入したり，USB メモリを使用する際にその中に記録された指定されたプログラムなどが自動的に起動される機能のことを言います。

指紋認証

現在，もっとも多く使用されている生体認証の技術。 指紋を登録しておくことで，本人以外の人間がコンピュータやシステムを利用したり，施錠された空間に入ったりすることができないようにするために利用されます。

社内システム
社内の業務を行うために開発された応用ソフト，もしくはその応用ソフトが動作するコンピュータのこと。 たとえば，顧客管理システムやスケジュール管理システム，経理システムなどがあります。

修正プログラム
ソフトウェアの欠陥や，脆弱性などを修正するために使用されるプログラムのこと。「修正パッチ」や「更新プログラム」と呼ばれることもあります。修正プログラムは，一般的にはメーカーの製品サポートページで配布されたり，CD メディアなどで配布されることもあります。

障害検知ツール
ネットワークやコンピュータなどの障害が発生したときに，それを検知しメールやあらかじめ指定した方法で知らせることが可能なソフトウェアのことを言います。

常時接続回線
常にインターネットに接続した状態になっているネットワーク回線のこと。 ネットワークの接続時間に関わらず料金が定額であるネットワーク回線のことを指すこともあります。代表的なものに光回線や ADSL があります。 常時接続回線を利用すると，常にインターネットに接続している状態になるため，ダイヤルアップ接続よりもハッキングなどによる侵入や攻撃をされる危険度が高くなります。そのため，より一層注意して情報セキュリティ対策を施す必要があります。

肖像権
人格権の一部で，自分の写真や絵の使用に関する権利のこと。たとえば，自分の写真や絵を承諾なしに公開されることを拒否することができます。

情報資産

企業や組織などで保有している情報全般のこと。顧客情報や販売情報などの情報自体に加えて，ファイルやデータベースといったデータ，CD-ROM や USB メモリなどのメディア，そして紙の資料も情報資産に含まれます。

情報セキュリティポリシー
重要ワード情報の機密性や完全性，可用性を維持していくために規定する組織の方針や行動指針をまとめたもの。

情報セキュリティマネジメント
企業・組織（企業，部，課など）における情報セキュリティを運用・管理するための仕組みのことを言います。情報セキュリティマネジメントは ISMS（Information Security Management System：インフォメーション・セキュリティ・マネジメント・システム）と呼ばれ，国際的な規格として ISO/IEC27001 として標準化されています。ショッピングサイトインターネットで商品を購入できる Web サイトのこと。 ショッピングサイトを利用すると，家やオフィスにいながら買い物をすることができます。

初動処理
事故などが発生した場合に，初めに行う行動のこと。

ショルダハッキング
キーボードで入力しているところを後ろから盗み見て，パスワードなどの重要な情報を不正に入手する方法。 ショルダハッキングは，ソーシャルエンジニアリングの手法のひとつで，肩越し（ショルダは“肩”の意味）に覗くことから，このように命名されています。

シンクライアント
企業・組織の情報システムで，社員などが利用するコンピュータ（クライアント）に最低限の機能だけを持たせて，サーバ側でアプリケーションソフトやファイルなどの管理を可能にするシステムの総称のこと。また，そのようなシステムを実現するための，機能を絞った低価格のクライアント用コンピュータのことを言います。

侵入検知システム
インターネットから送られてくるパケットを識別することで，不正侵入やアタック，事前

調査を検知するシステム。本来の英語表記である Intrusion Detection System（イントルージョン・ディテクション・システム）から IDS（アイディーエス）とも呼ばれ，不正なアクセスが発見された場合には，電子メールやアラームなど，事前に設定した方法で，管理者に連絡する機能を持ちます。

侵入テスト

コンピュータやネットワークの脆弱性を調査するために行うテストのひとつ。 外部からさまざまな攻撃方法を試しながら，特定のコンピュータやネットワークに侵入できるかどうかを実際に検証するテストのことです。 ペネトレーションテストとも言います。

侵入防止システム

インターネットに接続されたネットワークやサーバを不正侵入から防御するためのシステム。英語の Intrusion Prevention System（イントリュージョン・プリベンション・システム）として IPS（アイピーエス）とも呼ばれ，侵入検知システムの機能に加えて，不正なパケットを自動的に遮断する機能を持ちます。

信頼済みサイト

Web ブラウザのセキュリティゾーンのひとつで，あらかじめ信頼できることがわかっている Web サイト用のゾーンのこと。 一般的に信頼済みサイトでは，通常のインターネットサイトに比べて，セキュリティレベルを下げることでプログラムなどの実行を可能にします。

スクリーンセーバー

コンピュータを一定時間操作しなかった場合に表示するアニメーションのこと。 本来はディスプレイでの焼きつき（長時間同じ文字を表示し続けると，画面上に文字の痕跡が残されてしまうこと）を防止するための機能でした。現在の OS に搭載されているスクリーンセーバーでは，元に戻す際に，パスワードの入力を促す機能が搭載されているため，離席中に他人に自分のコンピュータを不正に使用されることを防ぐために利用することができます。

スクリプト

1 行ずつ実行される簡易なプログラム言語。 たとえば，JavaScript や VBScript といった

スクリプト言語を使用することで，ホームページにさまざまな動きを付け加えたり，利用者の操作に合わせた処理を実行できるようになります。

スケジューリング機能
OS やツールに搭載されているタスクの管理機能。 指定時刻に，あらかじめ設定したプログラムや機能を実行するように指定するためのものです。

ステルス機能
無線 LAN のアクセスポイントで，SSID を外部に見えなくする機能のこと。 アクセスポイントの存在を隠すことができるため，無線 LAN を利用する場合の情報セキュリティ対策のひとつとして利用できます。 なお，メーカーによっては，SSID 隠蔽（いんぺい）機能などの呼び名になっていることもあります。

スパイウェア
利用者の使用するコンピュータから，インターネットに対して個人情報やコンピュータの情報などを送信するソフトウェアのこと。 一般的には，そのようなソフトウェアがインストールされていることや動作していることに利用者が気づいていない状態で，自動的に情報を送信するソフトウェアをスパイウェアと呼びます。

スパムメール
重要ワード迷惑メールのこと。スマートフォンアプリケーションを追加することで，いろいろな機能を使うことができる携帯電話。音声通話のほか，Web ブラウザによる Web サイトの閲覧や，電子メールの送受信，文書ファイルの作成・閲覧，写真や音楽，動画の再生，内蔵カメラのある機種では写真や動画の撮影などができます。

脆弱性
重要ワードコンピュータやネットワークにおいて，情報セキュリティ上の問題となる可能性がある弱点のこと。 多くの場合は，OS やソフトウェアのセキュリティホールが脆弱性となります。また，設定ミスや管理体制の不備なども脆弱性のひとつとなることがあります。これらの脆弱性が具体的な脅威と結び付くと，情報セキュリティのインシデント（事件・事故）が発生してしまうことになります。

生体情報
バイオメトリクスのこと。生体認証（せいたいにんしょう）ひとりひとりが異なる人間の身体的特徴を利用する認証技術全般のこと。指紋や声紋，虹彩（眼球の模様）を登録しておくことで，本人以外の人間がコンピュータやシステムを利用したり，施錠された空間に入ったりすることができないようにするために利用されます。セキュリティサービスネットワークやコンピュータに対して，情報セキュリティ対策を実施するためのサービスのこと。
たとえば，インターネットサービスプロバイダでは，契約者に対して，電子メールや Web ページのウイルスチェックサービスや不正アクセスを防御するサービスなどを提供していることがあります。

セキュリティホール
OS やソフトウェアにおいて，情報セキュリティ上の欠陥となる不具合のこと。脆弱性とも呼ばれます。セッションハイジャックホームページの閲覧などパソコンと Web サーバとの間で通信を行っている際に，その通信を利用者以外の者が乗っ取る攻撃のこと。セッションハイジャックにより通信が乗っ取られると，本来の利用者になり代わって通信が行われてしまうことになります。

送信ドメイン認証
（SPF）送信ドメイン認証「Sender Policy Framework」（センダー・ポリシー・フレームワーク）とは，送信者のメールアドレスが正規なものであることを証明する技術。受信者側で，送信されたメールアドレスのドメインを見て，それが正規なメールサーバから発信されているか否かを検証する技術です。従来の未承諾広告メールやフィッシングメールなどの迷惑メールは，メールアドレスを詐称していることが多く，受信側のメールサーバの管理者が送信ドメイン認証を用いれば，正規のメールに混じって届く詐称メールを見つけやすくなります。

ソーシャルエンジニアリング
人間の心理的な隙などを突いて，コンピュータに侵入するための情報を盗み出すこと。ソーシャルには“社会的な”という意味があります。ソーシャルエンジニアリングの方法には，さまざまなものがあるため，万全な対策が取りにくいという点に注意しなければなりません。

ソーシャルゲーム
メンバーが交流しながら対戦したり，協力しあったりしながら，遊べるゲームのこと。ソーシャルネットワーキングサービスの 1 つとして提供されることもあります。

ダウンロード
ネットワーク上の FTP サーバや Web サーバからファイルを取り出して，自分のコンピュータに保存すること。

タスクバー
Windows でデスクトップの下に配置されている特殊なバーのこと。タクスバーには，[スタート] ボタンや現在実行されているプログラム，開かれているドキュメントなどが表示され，ボタンをクリックすることで，表示するウィンドウを切り替えることができます。また，タスクバーは，簡単にアプリケーションを起動するためのボタンが配置されていたり，現在の時刻を表示したり，実行中のアプリケーションのステータスを表示したりするのにも利用されています。

タッチパネル
指先や専用のペンで画面に触れることで入力を行う装置のこと。表示装置と入力装置が一体化したもので，指が触れた位置を検知して対応する動作を行います。
タブレット端末
薄い板状のパソコンやモバイル端末の総称で，液晶ディスプレイの表示画面で画面にタッチすることで操作可能なインターフェースを搭載した持ち運び可能なコンピュータのことを言います。

短縮 URL
Web サイトの URL を短く変換し，数文字程度に圧縮したもの。Web サービスとして，さまざまな企業が通常の URL から短縮 URL への変換サービスを提供しています。利用者は，まず短縮された URL にアクセスすると，短縮 URL サービス提供業者のデータベースにアクセスし，そこで元の URL を受け取り，目的のサイトへとたどり着くという仕組みになっています。URL が長い場合には，人間が入力したり覚えたりすることが困難であったり，SNS などのような文字数制限があるメディアへの書き込みにも不向きだった

ため，通常の URL が抱えるこれらの欠点を補うために開発されました。

チェーンメール
同じ内容のメールの転送を促す文章が書かれた電子メールのこと。連鎖メールとも呼ばれています。チェーンメールを送信してしまうと，インターネットで送信される電子メールの数がねずみ算的に増加してしまうため，ネットワークの負担を大きくしてしまう可能性があります。

チャット
インターネットで，複数の人と同時に文字やイラストを用いて会話できる仕組みのこと。チャット（chat）とは“おしゃべり”の意味で，インターネット上のチャットサーバに接続して利用します。

中間者攻撃
通信を行っている当事者間に悪意を持った第三者が割り込み，不正を行う攻撃のことを言います。英語で Man-in-the-Middle（マン・イン・ザ・ミドル）攻撃とも表記されます。

著作権
知的財産権のひとつで，著作物に対する著作者の権利のこと。 たとえば，自分の作った画像や撮った写真などを勝手に公開されることを拒否できます。

ディレクトリ
ハードディスクや CD-ROM などで，ファイルを保管する場所のこと。 数多くのファイルを分かりやすく管理できるようにするため，現在の OS では階層化されたディレクトリ構造を採用しています。なお，Windows や Mac OS では，ディレクトリをフォルダと呼んでいます。

データ消去サービス
ハードディスクの中身を復元できないように完全に消去してくれる業務サービスのこと。エクスプローラなどでハードディスク内のファイルを削除しても，データ復元ソフトを使うことによりファイルを復元することができることがあるため，機器の廃棄のときには，このようなサービスの利用が必要になります。

データセンター
インターネットに接続するための回線を装備して，顧客のサーバを預かる施設のこと。場所とインフラを提供するだけでなく，サーバの保守や運用を請け負うこともあります。

データ復元ソフト
誤って削除してしまったファイルやフォルダを復元するためのソフトウェア。 ただし，データ抹消ソフトで削除されたデータを復元することは困難です。

データベース
コンピュータにデータを蓄積するソフトウェアまたはそのデータの集まりのこと。データベースを利用することで，大量のデータを高速に検索し，集計することができます。データベースは，社内システムやショッピングサイトなどで利用されています。

デスクトップ
コンピュータの操作画面のこと。 デスクトップ上にプログラムを起動するためのアイコンを配置したり，ウィンドウを表示したりすることができます。つまり，コンピュータを利用するための“机”の役割を果たします。

電子掲示板
ネットワークを利用して，複数の人がコンピュータで同じ Web ページに読み書きを行うことができる仕組みのこと。業務連絡や友達同士での情報のやり取りに利用されます。省略して，掲示板と呼ばれたり，BBS と呼ばれたりすることもあります。

電子商取引
インターネットを使用して，商品の売買やサービスの提供など，商業活動を行う仕組みのこと。EC（Electronic Commerce－エレクトロニック・コマース），e コマースとも呼ばれます。 主に，企業と企業で行う BtoB（Business-to-Business）の仕組みと，企業と消費者で行う BtoC（Business-to-Consumer）の仕組みがあります。たとえば，ショッピングサイトやオンライントレードも，電子商取引のひとつです。 電子商取引においては，顧客の情報や購入履歴をデータとして保有することになるため，不正アクセスやデータ漏洩の問題など，もっとも情報セキュリティの強化が要求されているシステムと言えます。

電子署名
電子署名は，一般に暗号技術の一つである公開鍵暗号方式を利用して作成されます。電子署名は，メッセージの作成者が自分の鍵ペアのうちの秘密鍵（プライベート鍵とも呼ばれる）を使って作成します。メッセージを受信した人は，作成者の鍵ペアのうちの公開鍵（パブリック鍵）を使用して，受信したメッセージを検証します。つまり，作成者本人しか持ち得ない秘密鍵を使ってメッセージが作成されたことを検証することで，作成元の確認ができることになります。電子署名を利用することにより，なりすましやメッセージの改ざんが行われていないことの検証と，否認防止が可能になります。

電子メール
インターネットを用いて，コンピュータや携帯電話でやり取りする電子版の手紙のこと。文章を送信するだけでなく，ファイルを添付することができます。なお，HTML 形式の電子メールを利用すると，文字の色やサイズを指定したり，文中に画像を挿入することなどが可能になります。
電子メールソフト
電子メールを送受信するためのソフトウェアのこと。 主な電子メールソフトには，Microsoft Outlook や Mozilla Thunderbird などがあります。

添付ファイル
電子メールで本文とともに送信されるファイルのこと。電子メールでは，本文に書き切れない情報や，ワープロ文書などを添付ファイルとして送信できます。

統合セキュリティ対策ソフト
ウィルス対策，パーソナルファイアウォール，スパイウェア対策，迷惑メール対策といった機能を備えた，統合型の情報セキュリティ対策ソフト。

ドキュメント
本来は文書を意味する言葉。コンピュータの世界では，ワープロソフトや表計算ソフトで作成されたデータのことをドキュメントと呼びます。

ドメイン

インターネット上で接続しているネットワークに設定される名前のこと。 本来ドメインは, IP アドレスという数字の範囲によって管理されていますが, IP アドレスは人間にとって判別が困難であるため, “soumu.go.jp.”のようにドメイン名で記述できるようになっています。

ドメインツリー構造
DNS で管理されるドメイン名は階層構造で名前を表現するので, その構造のことを言います。

ドメイン名
ネットワーク上にあるコンピュータの配置を，ドメインというひとかたまりの管理単位に分ける際に設定される名前のこと。 たとえば，“soumu.go.jp.”のように記述します。また, ドメイン名の中で, “www.soumu.go.jp”というドメイン単位に配置されるコンピュータの名前（www）まで含めたドメイン名を，完全修飾ドメイン名と呼びます。

トラッシング
ソーシャルエンジニアリングのひとつである“ごみ箱あさり”のこと。ハッカーがターゲットとしたネットワークに侵入する際に，初期の準備作業として行われることが多いと言われています。対象とした企業や組織のネットワーク情報や社員情報，ユーザ情報などを探し出すことを目的とする行為です。

トラフィック
ネットワークを流れるデータの流れのこと。 本来は「往来」や「交通」という意味を持ちます。 通常, ネットワークの混雑具合を説明する際に,「トラフィックが増加する」,「トラフィックが大きい」などの言い方をします。ネットワークのトラフィックが増加すると，ホームページがなかなか表示されなかったり，電子メールの受信に時間がかかったりするようになります。なお，通信の分野では，通常トラヒックと言います。

トロイの木馬
コンピュータの内部に潜伏して, システムを破壊したり, 外部からの不正侵入を助けたり, そのコンピュータの情報を外部に発信したりするプログラム。トロイの木馬は感染能力を持つプログラムではないため，本来はウィルスに含まれるものではありませんが，現在で

は利用者には分からないように悪意のある行為を働くことがあるため,広義の意味で,ウィルスのひとつとして扱われることがあります。

なりすまし
他の利用者のふりをすること。または，中間者（Man-in-the-Middle）攻撃など他の利用者のふりをして行う不正行為のこと。たとえば，その当人であるふりをして電子メールを送信するなど,別人のふりをして電子掲示板に書き込みを行うような行為が挙げられます。

認証局
電子証明書の登録，発行および失効などを行う第三者認証機関のこと。

認証サーバ
利用者が本人であることを確認するためのサーバのこと。 OS やデータベースなどにも認証の機能が付属していますが，認証サーバは認証の機能のみを独立して提供するサーバです。 認証サーバと，OS やデータベースなどを連携させることによって，シングルサインオンの横断的な認証基盤を導入することができます。

ネットオークション
インターネット上で行われるオークションのこと。 実世界のオークションと同様に，もっとも高値をつけた人がその商品を購入する権利を得ることができます。また，個人が自分の持ち物をオークションに出品できる仕組みを用意しているネットオークションのホームページもあります。

ネットワーク
複数のコンピュータを接続して，データを共有化したり，他のコンピュータの機能を利用したり，共有のプリンタを使用したりできるようにする通信網のこと。もっとも小さな単位のネットワークは,家庭や会社において,何台かのコンピュータを接続したものですが，それらのネットワークが世界的に接続されて，インターネットが構成されています。

ネットワークドライブ
ネットワークに接続されたコンピュータが持っているディスクを，自分のコンピュータに

あるディスクと同じように使用できるシステムのこと。または,そのディスク自体のこと。この機能を利用すると，ネットワーク上のコンピュータ間で簡単にデータを共有することができます。

パーソナルファイアウォール

個人で利用するためのファイアウォール製品。ソフトウェアとして提供されることが多く，インターネットに接続するコンピュータにインストールして利用します。

バイオメトリクス

人間の身体的な特徴のこと。生体情報とも言います。これを利用した認証方法をバイオメトリクス認証と言い，指紋や網膜，声紋，静脈（静脈の血管形状パターン）など，さまざまな認証方法が研究されています。なりすましがしにくい認証方法であり，ユーザ名とパスワードによる認証や，IC カードなどの持ち物による認証に比べて，一般的に情報セキュリティが強化されます。 キーボードによる入力が不要になるため，キーボードを持たない環境（ドアなど）や，携帯電話のように，キーボードよりも速やかな認証を行いたい場面でも利用されるようになっています。

ハウジングサービス

インターネットに接続されたサーバの設置場所を貸し出すサービスのこと。 耐震設備や入退室管理などの情報セキュリティ対策を施した環境を持ち,サーバの設置場所とともに，通信回線，電源設備などを提供するサービスです。

パケット

ネットワークを通して送信されるデータを分割する際に使われる単位のこと。たとえば，ファイルを他のコンピュータに送信する際には，ファイルのデータをいくつかのパケットに分割して，各パケットにヘッダ情報を付加します。ヘッダには，IP アドレスなどの相手のコンピュータを識別する情報，受信した相手がパケットに分割されたデータを組み立て直すためのそれぞれのパケットの順番情報と，データのエラー補正のための情報などが含まれています。送信データをパケットに分割することにより，データの送信途中にエラーが発生してデータの再送信が必要になっても,データ全体を再送信するのではなく,パケット単位で再送信を行うだけで済むため，データの転送効率を向上させることができます。現在の携帯電話では，インターネットの接続料金をこのパケットの単位で課金されることが多いようです。

パスワード
本人であることを確認するために，ユーザ名とともに入力する文字列。銀行のキャッシュカードの暗証番号も，一種のパスワードです。
ハッカー
コンピュータ技術に長けた人のこと。または，コンピュータ技術を利用して，ハッキングを行う人のこと。本来は，悪い意味の言葉ではありませんでしたが，現在では，悪意を持って，コンピュータの不正利用や攻撃を行うクラッカーと同じ意味でも使われることが増えています。

ハッキング
高度なコンピュータ技術を利用して，システムを解析したり，プログラムを修正したりする行為のこと。本来は悪い意味を持つ言葉ではありませんでしたが，現在は不正にコンピュータを利用する行為全般のことをハッキングと呼ぶことが増えています。そのような悪意のある行為は，本来はクラッキングと呼ばれます。

バックアップ
データを磁気テープなどの別の記憶媒体に保存して，大事なデータの複製を作っておくこと。 バックアップを取っておくことで，データが壊れてしまったときに，バックアップ時の状態に復元することができます。

バックアップソフト
コンピュータシステムの環境やディスクに保管されているファイルを保管するためのソフトウェア。市販のバックアップソフトでは，OS に付属しているバックアップツールに比べて，多くの機能が装備されています。別の言い方で，バックアップユーティリティと呼ばれることもあります。ユーティリティ（utility）には“便利なもの”という意味があります。

バックドア
外部からコンピュータに侵入しやすいように，“裏口”を開ける行為，または裏口を開けるプログラムのこと。このプログラムが実行されてしまうと，インターネットからコンピュータを操作されてしまう可能性があります。なお，一部のウィルスでは，感染時にバックドアを埋め込むことがあります。

パッケージソフト
CD-ROM や DVD などのメディアに記録され，マニュアルなどとともに包装されて店頭で販売されているソフトウェア製品,または市販ソフトウェア製品のこと。最近ではインターネットからダウンロード販売されるものもあります。

パッチ
完成したプログラムに対して，脆弱性などをなくすために後から配布される修正プログラムのこと。メーカーのホームページなどで提供されます。

光回線
光ファイバーを利用した通信回線のこと。 ブロードバンド回線のひとつで，光ビームによってデータを送信する通信回線です。電気信号を用いる ADSL よりも高速で減衰が少なく，電気的干渉を受けにくいことから，高速なデータ通信や長距離のデータ通信に適しています。

否認防止
送信元（あるいは受信者）が，あとになってその送信事実（受信事実）またはその内容を否定する主張をすること。

秘密鍵
公開鍵暗号方式による暗号化や電子署名を利用する場合に，他人に見せることなく所有する鍵のこと。プライベート鍵やシークレット鍵とも呼ばれます。

標的型攻撃
特定の組織を狙って，機密情報や知的財産，アカウント情報（ID，パスワード）などを窃取しようとする攻撃です。この攻撃では，標的の組織がよくやり取りをする形式のメールを送りつけ，そこについている添付ファイルやリンクをクリックさせ実行させ，そこからマルウェア配布サイトに誘導するなどの手口がよく使われています。

ファームウェア
ハードウェアの基本的な制御のために，コンピュータなど機器に組み込まれたソフトウェ

アのこと。コンピュータなどの機器に固定的に搭載され，あまり変更が加えられないことから，ハードウェアとソフトウェアの中間的な存在としてファームウェアと呼ばれています。コンピュータや周辺機器，家電製品等に搭載されており，内蔵された記憶装置やメモリなどに記憶されます。パソコンの BIOS もファームウェアの一種です。機能の追加や不具合修正のため，後から変更できるようになっているものが多くなっています。

ファイアウォール

外部のネットワークと内部のネットワークを結ぶ箇所に導入することで，外部からの不正な侵入を防ぐことができるシステムのこと。またはシステムが導入された機器。 ファイアウォールには“防火壁”の意味があります。火災のときに被害を最小限に食い止めるための防火壁から，このように命名されています。 また，ウィルス対策ソフトに機能が統合された，個人向けのパーソナルファイアウォールソフトもあります。

ファイル共有

ネットワークを介して，ひとつのファイルを複数のコンピュータで利用できるようにすること。 ファイルの共有機能を使うと，記憶媒体を使用せずに，複数のコンピュータ間でデータをやり取りすることができるようになります。またファイルを共有するためにあらかじめ設定されたフォルダのことを，ファイル共有フォルダと言います。

ファイル共有ソフト

複数の利用者によるネットワークでのファイルのやり取りを可能にしたソフトウェア。ファイルの交換は，P2P（ピア・トゥー・ピア）で実行されます。 同じような機能を持つソフトウェアには，ファイル交換ソフトがあります。 厳密な分類としては，WinMX や Napster のようにクライアントを特定するシステムをファイル交換ソフトと呼び，Winny のようにクライアントを特定しないシステムをファイル共有ソフトと呼びます。インターネットで利用できるファイル共有ソフトを使用すると，ファイル自体を保管するサーバを用意することなく，必要なファイルを個々のコンピュータ間でやり取りすることができるようになります。利用者にとっては便利なソフトウェアですが，このようなファイル共有ソフトを利用して，インターネットで音楽，映画，ゲームソフトなど，違法なデータがやり取りされ著作権など法令に抵触することもあり，大きな社会問題のひとつになっています。

ファイルサーバ
ファイルを保存して，ファイル共有の機能を提供するコンピュータのこと。企業や組織では，共有する文書ファイルを保管するために利用しています。

フィッシング詐欺
実在の金融機関（銀行やクレジットカード会社），ショッピングサイトなどを装った電子メールを送付し，これらのホームページとそっくりの偽のサイトに誘導して，住所，氏名，銀行口座番号，クレジットカード番号などの重要な情報を入力させて詐取する行為のことを言います。

フィルタリング
一般的な意味では「ろ過」することですが，コンピュータや Web などインターネットの世界では「情報ろ過」を指します。情報ろ過としては，未成年者に対する成人サイトや有害情報サイトなどからの保護などが代表的な例です。その他に，コンピュータウイルスや不正アクセスからの保護を主な目的とするファイアウォールも，フィルタリングの一種と言えます。こうしたそれぞれの目的によって，Web サイトの内容に応じて閲覧の制御を行うコンテンツフィルタリングや，ネットワークを行き交うパケットをポリシーに応じて制御するパケットフィルタリングなどの手法があります。

フォーマット
ワープロソフトや表計算ソフトにおける文字などの書式設定のこと。また，記憶媒体を初期化して，使用できる状態にするという意味もあります。

復号
暗号化されたデータを元に戻して，人やコンピュータが識別できる情報にすること。

不正アクセス
利用する権限を与えられていないコンピュータに対して，不正に接続しようとすること。実際にそのコンピュータに侵入したり，利用したりすることを不正アクセスに含むこともあります。 日本国内においても，インターネットに接続されたコンピュータに対する不正アクセスによる被害が急増したため，これらの行為を処罰する不正アクセス禁止法が施行されました。

不正侵入
利用する権限を与えられていないネットワークやコンピュータに侵入して，不正にネットワークやコンピュータを操作する行為のこと。

踏み台
不正侵入の中継地点として利用されるコンピュータのこと。 他人のコンピュータに侵入するときに，直接自分のコンピュータから接続すると，接続元の IP アドレスによって，犯人が特定されてしまう可能性があります。そこで，いくつかのコンピュータを経由してから，目的のコンピュータに接続することで，犯人が自分のコンピュータを探しにくくします。このように，現実的な被害はないけれども，不正侵入の中継地点としてのみ利用されるコンピュータのことを踏み台と言います。

プライバシー
“私人の秘密”，“他人の干渉を許さない，各個人の私生活上の自由”のこと（広辞苑より引用）。プライバシーの侵害（プライバシーのしんがい）他人のプライバシーに関する権利を損なうこと。

プライバシーポリシー
ホームページなどで個人情報の扱い方や考え方を明記したもの。たとえば，ショッピングサイトで買い物するときには，住所や氏名などの個人情報の入力が必要です。そのため，ショッピングサイトでは多くの個人情報が収集されます。これらの個人情報については，ホームページの管理者がプライバシーポリシーを定めて，正しい方法で管理する責任があります。

ブラウザクラッシャ
ホームページの訪問者に対して,連続的に新しいウィンドウを開いたり,電子メールのメッセージウィンドウを開いたりすることで，訪問者のコンピュータに異常な動作をさせる Web ページのこと。 省略して，ブラクラとも呼ばれています。

プラグインソフト
Web ブラウザなどのソフトウェアに対して，機能を追加するための拡張プログラムのこ

と。

プラットフォーム
ソフトウェアが動作する土台となる基本システムや OS のこと。

フリーウェア
無償で使用できるソフトウェアのこと。フリーソフト，フリーソフトウェアと呼ばれることもあります。主に，インターネットで公開されており，ダウンロードして利用できるようになっています。ただし，利用制限等のあるフリーウェアも存在するので，商用利用の場合などには確認が必要です。

フリーメール
インターネットを通じて無料で提供される電子メールサービスのこと。登録すれば誰でも無料でメールアドレスが割り当てられ，電子メールの送受信が行えるようになります。Web ブラウザを使って受信メールの閲覧やメッセージの作成・送信を行う「Web メール」型のシステムが一般的です。

プレビュー
電子メールを読む前に，小さなウィンドウで中身を確認すること。または，プリンタで印刷する前に，コンピュータの画面上で印刷のイメージを確認すること。

ブロードバンド
ネットワークにおける広帯域幅を表す言葉。大容量のデータを高速に流すことができる ADSL や光回線などのネットワークやそこで提供されるサービスを指すこともあります。
ブロードバンドルーター
ADSL や光回線などのブロードバンドネットワークで，インターネットに接続する際に利用するルータのこと。ブロードバンドルーターの多くには，ファイアウォール機能など，安全にインターネットを利用できるようにするための機能も装備されています。

プロキシサーバ
企業・組織などの内部のネットワークとインターネットの間にあって，直接インターネットに接続できない内部ネットワークのコンピュータに代わって，「代理」としてインター

ネットとの接続を行うコンピュータ，またはそのための機能を有するソフトウェアのことを言います。

ブログ
インターネット上で公開されている日記形式のホームページのこと。 もともとは，「Web log」（ホームページの履歴の意味）から派生した言葉であると言われています。

プロトコル
ネットワークを介してコンピュータ同士がデータをやり取りするために定められた，データ形式や送受信の手順などの国際標準規則のこと。通信プロトコルとも呼ばれます。 文化や言語が異なる国と国との外交様式の決めごとというのが元々の意味です。コンピュータや通信機器も，メーカーや機種ごとに通信形式が異なると相互に通信が行えないため，ITU-T などの国際機関で標準が決められています。標準に準拠した形で開発されるため，コンピュータや通信機器は,メーカーが異なっても相互に通信を行うことができるのです。

ペアレンタルコントロール
インターネットや携帯電話・タブレット端末，ゲーム機などで，青少年に悪影響を及ぼすような暴力的表現や性的表現などを含んでいるサービスやコンテンツを閲覧できないように，親などが利用制限をかけることを言います。 情報機器やゲーム機でのペアレンタルロック（視聴制限機能）のことを指す場合もあります。

ヘッダ
データの先頭にあるデータ自体の内容を表す情報。または，印刷した用紙の上部に固定で印字するタイトルなどの文字。たとえば，電子メールには，本文の前にヘッダの情報があります。電子メールのヘッダには，送信者，送信先，送信日時などの情報が書き込まれています。なりすましやスパムメールの被害にあった場合に，電子メールの送信者を突き止めるための情報として利用できます。

傍受
交信者以外の人間が無線の通信内容を入手する行為。 故意または偶然のどちらであっても傍受となります。

ポート
インターネットで情報のやり取りを行うために，使用される番号のこと。ポート番号またはサービス番号とも呼ばれています。IP アドレスとともに指定される補助用のアドレスで，通常，プロトコルに応じてポートが割り当てられています。たとえば，FTP は TCP の 21 番ポート（制御用）と 20 番ポート（データ用），HTTP は TCP の 80 番ポート，HTTPS は TCP の 443 番ポートを使用します。

ホスト名
ネットワーク上の 1 台 1 台のコンピュータを識別するための名前のこと。

ボット
コンピュータを外部から遠隔操作するためのコンピュータウイルスの一種。ボットに感染してしまうと，インターネットを通じて，悪意のあるハッカーにコンピュータを遠隔操作されてしまうことがあります。外部から遠隔操作するという動作から，このようなウィルスのことをロボット（Robot）をもじってボット（BOT）と呼んでいます。

ポッドキャスト
インターネット上で配信されているラジオ番組，ニュース，英会話などパソコンやスマートフォンなどを使って気軽に聴くことができる仕組みのことを言います。アップル社のポータブルオーディオプレイヤーの iPod と broadcast（放送）を組み合わせた造語で，iPod が初期の頃からこの仕組みに対応していたためにこう呼ばれています。

ボットネット
多数のコンピュータウイルスの一種であるボットに感染したコンピュータによって構成される特殊なネットワークのこと。 ボットネットに接続されたコンピュータは，インターネット上から攻撃者が指示を出すことで,迷惑メールの配信や他のコンピュータへの攻撃，情報の窃取などを行うようになります。

ユーザアカウント
コンピュータやネットワークで，利用者を識別するための情報。 ユーザアカウントには，ユーザ名，パスワード，環境設定，使用権限などが含まれます。

ユーザ権限
コンピュータやネットワーク上のサービスにおいて，個々の利用者がどのような機能を利用できるかといった使用権限の設定内容のこと。 ユーザ権限を詳細に設定すると，組織やネットワーク内の情報資産を限られたユーザにアクセスを許すように制限できるため，情報セキュリティを強化することができます。

ユーザ認証
利用者が本人であるかどうかを確認する仕組み。 一般的には，ユーザ名とパスワードでユーザ認証を行いますが，なりすましを困難にするために，最近では IC カードや指紋，声紋，網膜などを利用する技術も登場しています。

ユーザ名
コンピュータやネットワークに接続する利用者を区別するために，それぞれの利用者に割り当てられた名前。ユーザ ID とも呼ばれています。

有線
物理的なケーブルで接続されている状態のこと。 コンピュータのネットワークにおいては，無線で接続する無線 LAN に対して，LAN ケーブルで接続されたネットワークを有線 LAN と言います。

リスクマネジメント
危機管理。発生する可能性のある事故に対して，その発生をできるだけ少なくし，事故が発生した場合の損害を最小に抑えるようにするために行う一連の行動や規範のことです。

リンク
ハイパーリンクの略。Web ページの文章内に埋め込まれた，他の関連文章の URL を示すもの。 一般的な Web ブラウザでは，リンクが設定されている文字列には下線と色が付いて表示されます。Web ブラウザでリンクをクリックすることにより，設定された URL の Web ページが表示されます。

ルータ
セグメントと呼ばれるネットワークの単位にネットワークを分割する装置のこと。もしく

は，別のセグメントのネットワークへ通信する際の経路情報の管理を行う装置のこと。ルータは，ネットワークをセグメントに分割することで，セグメント外に不要な通信を流さない役割を担います。また，個々のコンピュータ自身で通信する相手の経路情報を管理させないため，ルータを使うことで，効率的な通信が実現されます。

ルート証明書
認証局が自分自身の正当性を証明するために，自らに対して発行する証明書のこと。

ログ
コンピュータが保有するユーザの接続時刻や処理内容などを記録したファイル。 通常は，ログを参照することで，コンピュータが正常に動作しているかどうかを管理することができます。 たとえば，Web サーバの場合には，管理している Web サイトに訪問してきたユーザの情報が格納されます。

ログアウト（ログオフ）
コンピュータやネットワークの利用を終了すること。

ログイン（ログオン）
コンピュータやネットワークの利用を開始するために,利用者が認証を行って,コンピュータを使用可能な状態にすること。 一般的には，ユーザ名とパスワードを用いて，ユーザ認証を行います。

ワーム
他のファイルに寄生して増殖するのではなく，自分自身がファイルやメモリを使って自己増殖を行うタイプのウィルスのこと。

ワンクリック詐欺
電子メールと Web サイトを利用した詐欺行為のこと。携帯電話やパソコンに送りつけた電子メールによって Web サイトに誘い込み，Web サイトを訪問した人に対して，脅迫めいた手口で料金の振り込みを迫るという詐欺行為です。

Access（アクセス）

マイクロソフト社から発売されているデータベース管理ソフト。正式名称は，Microsoft Access。

ADSL

Asymmetric Digital Subscriber Line（アシンメトリック・デジタル・サブスクライバ・ライン：非対称デジタル加入者線）の略。 ブロードバンドの回線のひとつ。 現在，光回線とともに，高速な通信回線として普及しています。 通常の音声では使用しない周波数帯を利用することで，通常のアナログの電話回線で高速なデータ転送を可能にしています。

AES

米国標準技術局が選定した強固な暗号化アルゴリズム。Advanced Encryption Standard（アドバンスト・エンクリプション・スタンダード）の略。米国標準技術局により，「今後 30 年以上，暗号として利用可能な強度が見込める暗号化技術」として全世界に対して公募が行われ，集まった提案の中から審査を経て 2000 年 10 月に選定されました。

ASP

Application Service Provider（アプリケーション・サービス・プロバイダ）の略。 インターネット上でアプリケーションを提供するサービスの提供者（事業者）のことを言い，提供されるソフトウェアやサービスのことを ASP サービスと言います。

BCC

Blind Carbon Copy（ブラインド・カーボン・コピー）の略。電子メールの送信先指定方法のひとつ。 ブラインドには“隠れた”，カーボンコピーには“複写したもの”という意味があります。通常の宛先である TO に指定したユーザ以外に，同じ内容の電子メールを送信する場合に使用します。 CC（カーボン・コピー）と違い，電子メールのほかの受信者には，同じ内容の電子メールが BCC に指定したユーザにも送信されているということは通知されません。 そのため，他の受信者には，そのユーザに電子メールを送っているということを隠しておきたい場合に利用できます。

BIOS（バイオス）

Basic Input Output System の略。 コンピュータの電源を入れたときに最初に起動するプログラムであり，キーボードやマウス，ハードディスクなどの外部とのインターフェー

スを制御するプログラムが含まれています。Windows や Mac OS などの OS は，基本的に BIOS を介してこれらの機器とやり取りをしています。

Bluetooth（ブルートゥース）

パソコンや，スマートフォン，携帯電話などで，数メートル程度の離れた機器の接続に使われる短距離無線通信技術のひとつ。IEEE 802.15.1 として標準化されています。ケーブルを使わずに接続し，音声やデータをやり取りすることができます。

CC

Carbon Copy（カーボン・コピー）の略。電子メールの送信先指定方法のひとつ。 カーボンコピーには，“複写したもの”という意味があります。通常の宛先である TO に指定したユーザ以外にも同じ内容の電子メールを送信する場合に使用します。 電子メールの受信者は，同じ内容の電子メールが CC に指定されたメールアドレスに送信されていることがわかります。

CD-R

データを一度だけ書き込むことができる CD メディアのこと。媒体によって，650M バイトや 700M バイトといったデータを保存できます。

CD-RW

書き換えを可能にした CD メディア。媒体によって，650MB や 700MB といったデータを書き込むことができます。 CD-R は一度書き込んだデータを消去することはできませんが，CD-RW では何度でもデータを消去して，新たに別のデータを書き込むことができます。また，最近の CD-ROM ドライブや DVD-ROM ドライブは，ほとんどの場合，CD-RW に書き込まれたデータを読み取ることができます。そのため，日常的に取り扱うデータなどのバックアップに適したメディアであると言えます。

Chrome（クローム）

Google社が開発したオープンソース（ソースコードを無償で公開しているソフトウェア）の Web ブラウザです。ホームページの閲覧に使用します。

Cookie（クッキー）

ホームページを閲覧した際に，Web サーバが利用者のコンピュータに保存する管理用の

ファイルのこと。 利用者の登録情報や今までのショッピングカートの内容などを利用者のコンピュータに保存しておくことで，次回その利用者が同じ Web サイトを訪問した場合に，それらのデータを利用できるようにする仕組みです。 たとえば，Cookie を利用すると，ログイン情報を保管することもできるため，次回利用するときにログイン処理を省略できるようになるといった利点があります。

DDoS 攻撃（ディー・ドス・こうげき）
Distributed Denial of Service attack（ディストリビューテッド・デナイアル・オブ・サービス・アタック）。分散サービス拒否攻撃のこと。
Web サーバやメールサーバなどに対して，複数のコンピュータから大量のサービス要求のパケットを送りつけることで，相手のサーバやネットワークに過大な負荷をかけ，使用不能にします。 同様の攻撃方法である DoS 攻撃は 1 台のコンピュータから実行するものですが，DDoS 攻撃の場合は，例えば第三者のコンピュータをボットに感染させておくなどして，攻撃者の指示によって複数のコンピュータ(ボット)が一斉に攻撃します。

DHCP
Dynamic Host Configuration Protocol（ダイナミック・ホスト・コンフィグレーション・プロトコル）の略。
LAN に接続するコンピュータやデバイスなどに対して，IP アドレスを始めとして，ホスト名や経路情報，DNS サーバの情報など，通信に必要な設定情報を自動的に割り当てるプロトコルのこと。

DKIM（ディー・キム）
Domain Keys Identified Mail（ドメインキー・アイデンティファイド・メール）の略。 電子署名を利用した，電子メールの送信ドメイン認証技術のひとつ。スパムメール，フィッシングメールなどの迷惑メールへの対策のひとつとして利用できます。

DNS
Domain Name System（ドメイン・ネーム・システム）の略。“soumu.go.jp.”などのドメイン名を IP アドレスに変換する仕組みのこと。
インターネットに接続されたコンピュータは，数字で構成される IP アドレスで通信を行いますが，ドメイン名は IP アドレスとは異なり，“soumu.go.jp.”のような文字列で記述

できるため，人間にとって扱いやすいことから，ドメイン名と IP アドレスとの対応付けを行う DNS という仕組みが作られました。

DNSSEC（ディー・エヌ・エス・セック）
セキュリティを向上させるために，DNS の仕様を拡張したもの。DNS Security Extensions（セキュリティ・エクステンションズ）の略。
公開鍵暗号方式により DNS の応答データに電子署名を行い，データを受け取った側でデータ作成元を認証したり，受け取ったデータが正しいかどうかを確認できるようになっています。DNSSEC の利用により，フィッシングサイトへの誘導や情報の窃取を図る「DNS キャッシュポイズニング」を検知し，攻撃を防ぐことができます。

DNS キャッシュポイズニング
インターネットでコンピュータの IP アドレスを参照するために使用される DNS（ドメイン・ネーム・システム）に対する攻撃の一種。コンピュータの IP アドレスとドメイン名を対応させるために保存している情報に対して偽の情報を発信し，インターネット上の DNS サーバに伝播させることにより，一般の利用者がそのドメイン名のサーバに到達できないようにしたり，ドメイン所有者の意図しない別のサーバにアクセスを誘導する攻撃方法のことです。

DoS 攻撃（ドス・こうげき）
重要ワード Denial of Service（デナイアル・オブ・サービス）攻撃の略。サービス拒否攻撃のこと。攻撃者は，Web サーバやメールサーバなどに対して大量のサービス要求のパケットを送りつけ，過大な負荷をかけて相手のサーバやネットワークを使用不能にします。

DVD+R（ディー・ブイ・ディー・プラス・アール）
一度だけ書き込みできる DVD の規格。 記憶容量は片面 4.7GB です。追記型のメディアであるため，一度使用したディスクに対しても，さらにデータを書き込むことができます。

DVD+RW（ディー・ブイ・ディー・プラス・アール・ダブリュー）
書き換え可能な DVD の規格のうちのひとつ。 DVD+RW アライアンスという団体が策定した規格で，記憶容量は片面 4.7GB です。 DVD-RW よりも DVD-ROM との互換性が高いため，ほとんどの DVD-ROM ドライブで読み込むことができます。なお，DVD+RW は，

DVD-RW とは互換性がありません。

DVD-R（ディー・ブイ・ディー・アール）
一度だけ書き込みできる DVD の規格。 記憶容量は片面 4.7GB です。追記型のメディアであるため,一度使用したディスクに対しても,さらにデータを書き込むことができます。

DVD-RAM（ディー・ブイ・ディー・ラム）
書き換え可能な DVD の規格のうちのひとつ。 DVD フォーラムによって策定された統一規格です。記憶容量は片面 2.6GB，両面 5.2GB のものと，片面 4.7GB，両面 9.4GB のものがあります。DVD-RW や DVD+RW に比べて，DVD-ROM との互換性が低いという欠点がありますが，最近の DVD-ROM ドライブでは DVD-RAM のメディアを読み出すことができるものが増えてきました。

DVD-RW（ディー・ブイ・ディー・アール・ダブリュー）
書き換え可能な DVD の規格のうちのひとつ。 DVD フォーラムによって策定された統一規格です。記憶容量は，片面 4.7GB です。 DVD-RAM よりも，DVD-ROM との互換性が高いのが特徴です。

Excel（エクセル）
マイクロソフト社から発売されている表計算ソフト。正式名称は，Microsoft Excel。

EXE（エグゼ）
Windows で実行可能なファイルに付けられる拡張子。“実行”を意味する Execute（エクゼキュート）の先頭 3 文字からつけられています。

Firefox（ファイアフォックス）
Mozilla 社が開発したオープンソース（ソースコードを無償で公開しているソフトウェア）の Web ブラウザです。ホームページの閲覧に使用します。

FTP（エフ・ティー・ピー）
File Transfer Protocol（ファイル・トランスファー・プロトコル）の略。他のコンピュータとファイルを送受信するためのプロトコルのこと。 トランスファーには“転送する”，プ

ロトコルには“規約”という意味があります。 FTP は，インターネットで主に大きなサイズのファイルの送受信を行うときに，標準的に利用されています。

GPS（ジー・ピー・エス）
Global Positioning System（グローバル・ポジショニング・システム）の略。人工衛星を利用して自分が地球上にいる位置を正確に測定できるシステムです。日本語では「全地球測位システム」と呼ばれています。

HTML
Hyper Text Markup Language（ハイパー・テキスト・マークアップ・ランゲージ）の略。ホームページを作成するための言語。 HTML には，文字だけでなく画像や音声を埋め込むことができます。HTML 形式のファイルは，Web ブラウザで閲覧することができます。また，HTML 形式のファイルに埋め込まれたリンクをクリックすることで，参照先などの Web ページに移動できます。

HTML ファイル（エイチ・ティー・エム・エル・ファイル）
HTML で記述されたファイル。HTML メール（エイチ・ティー・エム・エル・メール）HTML で記述された電子メール。 通常の電子メールとは異なり，文字だけでなく，文字の大きさや色，レイアウトを工夫した電子メールを作成することができます。また，通常のホームページと同様に，さまざまな動作を実行するスクリプトを埋め込むこともできます。

HTTP（エイチ・ティー・ティー・ピー）
Hyper Text Transfer Protocol（ハイパー・テキスト・トランスファー・プロトコル）の略。Web ブラウザが，Web サーバに対して HTML 形式のファイルを受け取るためのプロトコル。 トランスファーには“転送する”という意味があります。

IaaS（イアース，アイアース）
Infrastructure as a Service（インフラストラクチャー・アズ・ア・サービス）の略。インターネット経由での，サーバ仮想化やデスクトップ仮想化，共有ディスクなど，ハードウェアやインフラ機能の提供を行うサービスのこと。HaaS（Hardware as a Service:ハードウェア・アズ・ア・サービス）と呼ばれることもあります。

IC カード
キャッシュカードやクレジットカードのようなプラスチック製のカードに, IC チップを埋め込んだもの。IC チップには, さまざまな情報が書き込まれており, 専用の IC カードリーダーを使用することで, その内容を読み出すことができます。IC カードに書き込まれた値によって,ユーザ認証に利用したり,電子マネーの残高を管理したりすることができます。

ICT
Information and Communication Technology の略。情報通信技術のこと。従来から使われていた IT（Information Technology）に替わって，通信ネットワークによって情報が流通することの重要性を意識して使用される言葉です。

ID
identification（アイデンティフィケーション）の略。個人を識別・把握する情報の総称のこと。ユーザ名，ユーザ ID とも呼ばれます。

IDS
Intrusion Detection System（イントリュージョン・ディテクション・システム）の略。侵入検知システムのこと。

IEC
International Electrotechnical Commission（インターナショナル・エレクトロテクニカル・コミッション）の略。国際電気標準会議のこと。 電気および電子技術分野における国際標準の策定を行う国際標準化機関です。

IEEE802.11a（アイトリプルイー・ハチマルニー・テン・イチイチ・エー）
無線 LAN の規格のひとつ。周波数帯 5GHz 帯の電波を使い，最大 54Mbps（理論値）の転送速度で通信することができます。

IEEE802.11ac（アイトリプルイー・ハチマルニー・テン・イチイチ・エーシー）
無線 LAN の規格のひとつ。 周波数帯 5GHz 帯の電波を使い，最大 6.9Gbps（理論値）の転送速度で通信することができます。

IEEE802.11b（アイトリプルイー・ハチマルニー・テン・イチイチ・ビー）
無線 LAN の規格のひとつ。 周波数帯 2.4GHz 帯の電波を使い最大 11Mbps（理論値）の転送速度で通信することができます。

IEEE802.11g（アイトリプルイー・ハチマルニー・テン・イチイチ・ジー）
無線 LAN の規格のひとつ。IEEE802.11b と同じ周波数帯 2.4GHz 帯の電波を使い，最大 54Mbps（理論値）で通信することができます。

IEEE802.11n（アイトリプルイー・ハチマルニー・テン・イチイチ・エヌ）
無線 LAN の規格のひとつ。 周波数帯 2.4GHz 帯，5GHz 帯のいずれか，もしくは両方の電波を使い，最大 600Mbps（理論値）の転送速度で通信することができます。他によく利用される無線 LAN の規格として，IEEE802.11a，IEEE802.11b，IEEE802.11g などがあります。また，無線 LAN や有線 LAN で使用される認証方式として IEEE802.1X があります。

IEEE802.1X（アイトリプルイー・ハチマルニー・テン・イチ・エックス）
LAN におけるユーザ認証方式の規格。 IEEE802.1X は，無線 LAN だけでなく，有線も含んだユーザ認証の方式です。クライアントが接続を要求した場合には，認証サーバである RADIUS（ラディウス）サーバが認証処理を行います。クライアントが認証された場合には，セッションごとに暗号鍵が与えられます。なお，IEEE802.1X では通常，暗号化を行わないため，無線 LAN を利用する場合には WPA，WPA2 による暗号化を利用します。

iframe タグ（アイ・フレーム・タグ）
インラインフレームを実現するための HTML タグのこと。インラインフレームとは，ホームページを作成する場合に，通常の分割画面などによる方法ではなく，表示したいページ内の任意の場所に指定したサイズの他のホームページの内容を表示する技術のことです。iframe タグを使用すると，Web ページ内に別の Web サイトの Web ページを埋め込むことができます。

Internet Explorer（インターネット・エクスプローラ）
マイクロソフト社が開発した Web ブラウザ。IE とも呼ばれています。 ホームページの閲覧に使用します。

IPS
Intrusion Prevention System（イントリュージョン・プリベンション・システム）の略。侵入防止システムのこと。

IP アドレス
コンピュータをネットワークで接続するために，それぞれのコンピュータに割り振られた一意の数字の組み合わせのこと。 IP アドレスは，127.0.0.1 のように 0～255 までの数字を 4 つ組み合わせたもので，単にアドレスと略されることがあります。 現在主に使用されているこれらの 4 つの数字の組み合わせによるアドレス体系は，IPv4（アイ・ピー・ブイフォー）と呼ばれています。また，今後情報家電等で大量に IP アドレスが消費される時代に備えて，次期規格として，IPv6（アイ・ピー・ブイシックス）と呼ばれるアドレス体系への移行が検討されています。なお，IPv6 では，アドレス空間の増加だけでなく，情報セキュリティ機能の追加などの改良も加えられています。

ISO
International Organization for Standardization（インターナショナル・オーガニゼーション・フォー・スタンダーディゼーション）のこと。 電気および電子技術分野を除く全産業分野（鉱工業，農業，医薬品等）における国際標準の策定を行う国際標準化機関です。略称が英文名称の頭文字語「IOS」ではなく「ISO」になっているのは，ギリシャ語で「平等」を意味する「isos」という言葉が起源のためです。

ISO/IEC15408（アイ・エス・オー/アイ・イー・シー15408）
IT 関連製品やシステムの開発，製造，運用に関わるセキュリティ品質を客観的に評価するための国際評価基準。 対象の製品やシステムが，評価基準に準拠しているかどうかを検証して，基準に達している場合に認証書を発行します。 日本においては， 2000 年 7 月に「ISO/IEC15408」に対応する国内標準として「JIS X 5070」が制定されました。

ISO/IEC27001（アイ・エス・オー/アイ・イー・シー27001）
企業や組織における情報セキュリティマネジメントに関する基準のこと。ISO/IEC27001 は，ISO/IEC15408 が製品やシステムのセキュリティ品質を評価するのに対して，組織における情報資産を正しく運用管理することを主な目的としています。 日

本においては， 2006 年 5 月に「ISO/IEC27001」に対応する国内標準として「JIS Q 27001」が制定されました。

ISP（アイ・エス・ピー）
インターネットサービスプロバイダのこと。

IT（アイ・ティー）
Information Technology（インフォメーション・テクノロジー：情報技術）の略。コンピュータやネットワークに関わるすべての技術を総称する言葉として使用されています。

Java（ジャバ）
サン・マイクロシステムズ社が 1995 年に発表したプログラミング言語。 Java は，どのコンピュータ上でも動作することを目的に開発された言語です。Java で開発されたプログラムは，Java 仮想マシン（Java Virtual Machine）と呼ばれる仮想環境上で動作するため，OS に関係なく同じプログラムを実行することができます。 現在は，パソコンだけでなく，携帯電話のアプリケーションなどでも利用されています。

JavaScript（ジャバ・スクリプト）
ネットスケープ社とサン・マイクロシステムズ社が共同で開発したホームページに埋め込むことができるスクリプト言語。 JavaScript は，静的な文字と画像しか表示できなかった Web ページに，動きを付け加えたり，利用者の操作に合わせた処理を実行できるようにしたりすることを目的として開発された言語です。 Java が言語のベースになっているため，Java という名前が付いていますが，実際にはまったく別の言語です。現在は，事実上の Web ページ用の標準的なスクリプト言語となっています。

LAN（ラン）
Local Area Network（ローカル・エリア・ネットワーク）の略。同じ建物内などの比較的近い距離でコンピュータを接続するネットワークのこと。LAN を導入すると，同じ LAN に接続しているコンピュータとのファイル共有や，プリンタの共有などを行うことができます。

LAN カード（ラン・カード）

LAN やインターネットに接続するために，コンピュータやプリンタなどの機器を接続するための拡張カードのこと。現在発売されているコンピュータには,あらかじめ LAN カードの機能が用意されているものが多く，イーサネットカードやネットワークカードとも呼ばれています。

LAN ケーブル（ラン・ケーブル）
ネットワーク（LAN）を構成するコンピュータ，ルータ，サーバなどの機器をつなぐために使用される通信ケーブルのこと。イーサネットケーブルとも呼ばれています。

Mac OS（マック・オーエス）
アップル社のパーソナルコンピュータ Macintosh に搭載されている OS。

MAC アドレス（マック・アドレス）
Media Access Control（メディア・アクセス・コントロール）アドレスの略。LAN カードの中で, イーサネットを使って通信を行うカードに割り振られた一意の番号のこと。 インターネットでは，IP アドレス以外にも，この MAC アドレスを使用して通信を行っています。LAN カードは，製造会社が出荷製品に対して厳密に MAC アドレスを管理しているため, まったく同一の MAC アドレスを持つ LAN カードが 2 つ以上存在することはありません。

MDM（エム・ディー・エム）
Mobile Device Management（モバイル・デバイス・マネジメント）の略。 主に企業や組織などで，スマートフォンやタブレット端末などの携帯端末を安全に管理する仕組みのこと。スマートフォンやタブレット端末は，企業や組織の外に持ち出され，さまざまな環境や場所で利用されることから，紛失・盗難時の対策など，端末内の情報を安全に管理するためのさまざまな機能があります。

MTA（エム・ティー・エー）
Mail Transfer Agent（メール・トランスファー・エージェント）の略。 インターネットで電子メールを配送するソフトウェアの総称で，メール転送エージェントのこと。利用者が送信したメールを受け取って，他の MTA と連携してバケツリレー式に目的地まで配送する機能を持ちます。

NTP（エヌ・ティー・ピー）
Network Time Protocol（ネットワーク・タイム・プロトコル）の略。
コンピュータやルータなど，ネットワークに接続された機器が持つ時計を，正しい時刻に同期させるためのしくみのこと。
Office アプリケーション（オフィス・アプリケーション）
マイクロソフト社から発売されている統合ビジネス用ソフトウェア。 ワープロソフトの Word や表計算ソフトの Excel などが含まれています。

OS（オー・エス）
Operating System（オペレーティング・システム）の略。コンピュータを動作させるための基本的な機能を提供するシステム全般のこと。 たとえば，メモリやディスクなどのハードウェアの制御，キーボードやマウスといったユーザインタフェースの処理，画面への表示とウィンドウの制御など，コンピュータが動作するための数多くの基本処理を行っています。さらに，コンピュータシステムを管理するための数多くのツールが用意されています。代表的な OS には Windows，Mac OS などがあります。

Outlook（アウトルック）
マイクロソフト社から発売されているスケジュール管理や電子メールのやり取りを行うためのソフトウェア。 正式名称は，Microsoft Outlook。

P2P（ピー・ツー・ピー）
Peer To Peer（ピア・ツー・ピア）の略。コンピュータの世界では，to が two と同じ発音であることから，“to”を“2”に置き換えた命名を行うことがあります。 P2P とは，不特定多数のコンピュータを直接接続して情報をやり取りするタイプのシステム提供方式のことです。インターネットの世界では，これまでサーバとコンピュータが連携した情報提供方法 が採用されていましたが，最近では，P2P を利用したシステムも増えてきました。たとえば，音楽配信サービスの Napster，データ配信サービスの Winny などが P2P のシステムです。 サーバとコンピュータが連携した情報提供を行うシステムでは，サーバという情報を管理するコンピュータが決められていましたが，P2P の仕組みではすべてのコンピュータがそれぞれ情報を配信するサーバの役割を果たします。

PaaS（パース）
Platform as a Service（プラットフォーム・アズ・ア・サービス）の略。インターネット経由で，仮想化されたアプリケーションサーバやデータベースなどアプリケーション実行用のプラットフォーム機能の提供を行うサービスのことを言います。

POP3（ポップ・スリー）
Post Office Protocol - Version 3（ポスト・オフィス・プロトコル・バージョン・スリー）の略。メールサーバに保存されている電子メールを電子メールソフトが取りに行く際に利用されるプロトコルです。

PowerPoint（パワーポイント）
マイクロソフト社から発売されているプレゼンテーションソフト。正式名称は，Microsoft PowerPoint。

PSK（ピー・エス・ケー）
Pre-Shared Key（プリ・シェアード・キー）の略。 TKIP または AES という暗号化方式を使用して生成される鍵のこと。 暗号化を行う鍵ではなく，暗号鍵を生成するための鍵であるため，事前共有鍵と呼ばれています。

RAT (ラット)
Remote Administration Tool（リモート・アドミニストレーション・ツール）の略。 利用者に認識されることなくひそかにインストールされ，実行される遠隔操作のためのプログラムです。多くの場合，コンピュータの画面上に表示されることなく，プログラムやデータファイルの実行・停止・削除，ファイルやプログラムのアップロード・ダウンロードなどの活動を，許可なく不正に行います。

SaaS（サース，サーズ）
Software as a Service（ソフトウェア・アズ・ア・サービス）の略。インターネット経由で，電子メール，グループウェア，顧客管理などのソフトウェア機能の提供を行うサービス。以前は，ASP（Application Service Provider）などと呼ばれていました。

SFTP（エス・エフ・ティー・ピー）

SSH File Transfer Protocol（エスエスエイチ・ファイル・トランスファー・プロトコル）の略。SSH（エス・エス・エイチ）で暗号化された通信路を使って，安全にファイルを送受信するファイル転送プロトコルのこと。また，それを利用して暗号化ファイルの送受信を行うコマンドのことを言います。

SMTP（エス・エム・ティー・ピー）
Simple Mail Transfer Protocol（シンプル・メール・トランスファー・プロトコル）の略。電子メールの送信と転送を行うためのプロトコル。 Windows が搭載されているコンピュータと Mac OS が搭載されているコンピュータや，携帯電話とパソコンといった異なった機種の間でも電子メールのやり取りができるのは，このプロトコルに準拠しているためです。

SNS（エス・エヌ・エス）
Social Networking Service（ソーシャル・ネットワーキング・サービス）の略。登録した利用者だけが参加できるインターネットの Web サイトのこと。
SQL インジェクション（エス・キュー・エル・インジェクション）
SQL とは，データベースを操作するためのプログラミング言語のこと。インターネットの Web サイトなどの入力画面に対して，直接 SQL 命令文の文字列を入力することで，データベースに不正アクセスを行い，情報の入手や，データベースの破壊，Web ページの改ざんなどを行うこと。これは Web アプリケーションにおけるエスケープ処理が適切に行われていない脆弱性を狙った攻撃で， 最近では，SQL インジェクションによる情報漏洩事件や，Web ページの改ざんにより正規の Web サイトにウィルスを埋め込まれる事件が増加しています。

SSH（エス・エス・エイチ）
Secure Shell（セキュア・シェル）の略。ネットワークを介して別のコンピュータにログインしたり，遠隔地のコンピュータから命令を実行したり，他のコンピュータへファイルを移動したりするためのプログラムのこと。 SSH を利用するとネットワーク上を流れるデータは暗号化されるため，インターネット経由でも安全に操作を行うことができます。

SSID（エス・エス・アイ・ディ）
Service Set Identifier（サービス・セット・アイデンティファイア）の略。無線 LAN で特

定のコンピュータや通信機器で構成されるネットワークを指定して，接続するためのユニークな識別コードのこと。ESS ID（イー・エス・エス・アイ・ディ）とも呼ばれています。 無線 LAN で送信するパケットのヘッダに含まれ，受信側は，SSID が一致しない場合は，そのパケットを無視するため通信ができません。

SSL（エス・エス・エル）
Secure Socket Layer（セキュア・ソケット・レイヤ）の略。 インターネットにおいてデータを暗号化したり，なりすましを防いだりするためのプロトコルのこと。ショッピングサイトやインターネットバンキングなど，個人情報や機密情報をやり取りする際に広く使われています。 利用者は，認証機関により発行されたサーバ証明書によって，サーバの真正性を確認します。現在は，SSL3.0 をもとに改良が加えられた TLS1.2 が標準的なプロトコルとして利用されています。

TCP（ティー・シー・ピー）
Transmission Control Protocol（トランスミッション・コントロール・プロトコル）の略。インターネットで使用されているプロトコルのひとつ。 TCP は，相手と接続を確立してから通信を行うため，UDP に比べて信頼性が高いプロトコルです。TCP は，HTTP や FTP，SMTP，POP3 といった，インターネットにおける主要なサービスで使用されるプロトコルの基盤となっています。TCP/IP（ティー・シー・ピー・アイ・ピー）インターネットで標準的に利用されているプロトコルのこと。 TCP/IP は TCP と IP という 2 つのプロトコルを省略した呼び名であり，TELNET，FTP，HTTP など，TCP や IP を基盤にした多くのプロトコルの総称です。

TELNET（テルネット）
Telecommunication network（テレコミュニケーション・ネットワーク）の略。ネットワークに接続された環境で，手元のコンピュータから，別の場所に置かれているコンピュータを遠隔操作するためのプロトコル。または，その機能を実現するソフトウェアのこと。

TKIP（ティー・ケー・アイ・ピー　または　ティー・キップ）Temporal Key Integrity Protocol（テンポラル・キー・インテグリティ・プロトコル）の略。WPA-PSK や WPA-EAP の暗号化方式で使用されているプロトコルのこと。

TLS（ティー・エル・エス）
Transport Layer Security（トランスポート・レイヤ・セキュリティ）の略。インターネットにおいてデータを暗号化したり，なりすましを防いだりするためのプロトコルのこと。TLS は，SSL を元にして標準化されました。SSL と同様に，ショッピングサイトなどで，個人情報や機密情報をやり取りする際に使われています。

TO（トゥー）
電子メールの送信先指定方法のひとつ。 TO には，電子メールの通常の送信先のメールアドレスを記述します。電子メールの宛先は，TO 以外に，CC や BCC に指定することができます。

UDP（ユー・ディー・ピー）
User Datagram Protocol（ユーザ・データグラム・プロトコル）の略。インターネットで使用されているプロトコルのひとつ。 インターネットを利用するアプリケーションなどの通信では，TCP と UDP のいずれかのプロトコルが使用されています。UDP は，TCP に比べてシンプルなプロトコルであるため,高速ですが信頼性が低いという特徴があります。そのため，確実なデータ転送が要求される Web や電子メールでは，TCP が使用されています。

UPS（ユー・ピー・エス）
Uninterruptible Power Supply（アンインタラプティブル・パワー・サプライ）の略。無停電電源装置のこと。

URI（ユー・アール・アイ）
Uniform Resource Identifier（ユニフォーム・リソース・アイデンティファイヤ）の略。インターネット上で情報が格納されている場所を示すための住所のような役割を果たす文字列のこと。 HTML4 の仕様より URL を拡張した URI が定義されたことから，徐々に URI という表現を見かけるようになっています。

URL（ユー・アール・エル）
Uniform Resource Locator（ユニフォーム・リソース・ロケータ）の略。インターネット上で情報が格納されている場所を示すための住所のような役割を果たす文字列のこと。

URL は，Web ブラウザなどでホームページを閲覧するときの指定に利用されます。プロトコル名，ホスト名，パス名で構成されます。 たとえば，“http://www.soumu.go.jp/index.html” のように記述します。

USB（ユー・エス・ビー）
Universal Serial Bus（ユニバーサル・シリアル・バス）の略。コンピュータにさまざまな周辺機器を接続することができる外部ポートの規格。 USB には，コンピュータの電源を切らずに，機器を抜き差しできるという特徴があります。 USB のポートには，CD-ROM ドライブ，ハードディスク，光磁気ディスクなどのドライブ類から，マウス，キーボードなどのインターフェースまで，数多くの周辺機器を接続することができます。 当初使用されていた USB1.1 という規格では，転送速度が最大 12Mbps と比較的低速なものであったため，ハードディスクなどの高速なドライブの接続にはあまり適しませんでしたが，現在は転送速度を最大 5Gbps まで可能にした USB3.0 という規格が登場したため，さらに数多くの対応機器が登場してきています。

USB 媒介ウィルス
USB メモリなどをコンピュータに差し込んだだけで感染するウィルスのこと。USB 媒介ウィルスは，感染したコンピュータに差し込まれた他の USB メモリに感染する形で広がっていきます。なお，USB メモリだけでなく，記憶領域を持つ外付けハードディスクやデジタルオーディオプレーヤーなどでも感染します。

USB メモリ（ユー・エス・ビー・メモリ）
重要ワードコンピュータの USB 端子に接続して利用できる小さなメモリデバイスのこと。USB 端子に接続するだけで，外部ドライブとして簡単に読み書きができる。消しゴム程度のサイズであるため，手軽に利用できるという利点はありますが，その分だけ盗難や紛失の危険性が高く，情報セキュリティ上のリスクが高いという欠点があります。また，最近は USB メモリをターゲットにした USB 媒介ウィルスが発生しています。USB 媒介ウィルスは，コンピュータに USB メモリを差し込んだだけでウィルスに感染してしまうものです。

VBA（ブイ・ビー・エー）
Visual Basic for Applications（ビジュアル・ベーシック・フォー・アプリケーションズ）

の略。マイクロソフト社が開発した Office アプリケーション用のプログラミング言語。Visual Basic を元にして，Office アプリケーションで利用できるように開発されたものです。たとえば，Excel で VBA を使用すると，罫線，フォントの大きさや色といった書式を設定して，表を作り上げることを自動的に処理することが可能になります。

Web アプリケーション（ウェブ・アプリケーション）
Web ブラウザを利用して，Web サーバに接続することで，動作するアプリケーションソフトのこと。
Web サーバは，Web ブラウザからの要求やデータ送信に応じて，動的にコンテンツを配信したり，データを格納したりします。

Web サーバ（ウェブ・サーバ）
HTML ファイルや画像ファイルなどを格納して，利用者の要求によって，Web ページを送信するソフトウェア。または，そのソフトウェアが動作しているコンピュータのこと。 本来の Web サーバは，コンテンツを送信する機能だけしか持っていませんでしたが，最近の Web サーバではプログラムを利用することで，利用者の要求に合わせた情報を送信することができるようになっています。

Web サイト（ウェブ・サイト）
ホームページのサービスを提供しているシステムやサーバのこと。
Web ブラウザ（ウェブ・ブラウザ）
ホームページを閲覧するためのソフトウェア。代表的なソフトとして，Internet Explorer や Google Chrome，Firefox，Safari などがあります。

Web ページ（ウェブ・ページ）
HTML で記述されたファイルのこと。 ホームページでは，多くの Web ページが公開されています。利用者は Web ブラウザを使用して，これらの Web ページを閲覧することができます。

Web メール（ウェブ・メール）
ホームページを閲覧する Web ブラウザで利用可能な電子メールシステムのこと。 メールの閲覧や，新規メッセージの作成・送信などを Web ブラウザで行いますが，通常の電

子メールと違ってメールの内容をサービス提供事業者側のサーバで管理するため，利用者はインターネットを使って，どこからでもメールをチェックしたり過去のメールを参照したりできる利点があります。

WEP（ウェップ）
Wired Equivalent Privacy（ワイアード・エクイヴァレント・プライバシー）の略。無線 LAN の規格である IEEE802.11 で採用されている暗号化方式。 無線 LAN は無線区間内での傍受が簡単であるため，暗号化によって送信されるデータの解読を困難にする必要があります。 しかし，WEP は現在では容易に解読可能とされていますので，なるべく使用しない方が良いでしょう。

Wi-Fi（ワイ・ファイ）
無線通信の国際標準通信規格で，IEEE 802.11 シリーズ（IEEE802.11a / IEEE802.11b / IEEE802.11g / IEEE802.11n / IEEE802.11ac など)を利用した無線通信のこと。業界団体の Wi-Fi Alliance が発行しており，相互接続性などに関する試験をパスした装置には，このロゴの表示が許可されています。
IEEE 802.11a/b/g/n/ac については，それぞれについて個別に認定が行われ，互換性に適合した商品パッケージ等には「Wi-Fi CERTIFIED」ロゴを表示できるようになります。このロゴには対応している規格が「a」「a/b」「b/g」「a/b/g/n」「a/b/g/n/ac」などとして表示され，IEEE 802.11 のどの規格に対応しているかが分かるようになっています。

Wi-Fi Alliance（ワイ・ファイ・アライアンス）
Wi-Fi Alliance は，高速無線 LAN の規格の普及促進を図ることを目的とした業界団体のこと。主に無線 LAN の相互接続性試験方法の策定，製品の認証，および Wi-Fi ブランドの普及に向けたプロモーション活動を行っている団体であり，通信機器メーカーなどを中心に無線 LAN 関連業界の企業が参加しています。

WiMAX（ワイマックス）
無線を使ったブロードバンドモバイル通信規格の 1 つで，ADSL 並みの速度と料金でデータ通信ができる技術として注目されています。WiMAX は，従来は 10～66GHz の周波数帯を使用していましたが，IEEE802.16a という規格では 2～11GHz を利用するよう改め

られています。また，見通しのきかない範囲にある端末とも通信できるよう改良されています。通信速度や最大距離は変わらず，1 台のアンテナで半径約 50km（30 マイル）をカバーし，最大で 70Mbps の通信が可能になっています。

Windows（ウィンドウズ）
マイクロソフト社が開発した OS（オペレーティング・システム）。
Windows Update（ウィンドウズ・アップデート）
Windows に搭載されている OS やソフトウェアの更新補助機能。インターネットに接続している環境であれば，Windows Update を実行することで，現在のコンピュータの環境やインストールされているソフトウェアに応じて，更新が必要なプログラムをダウンロードし，インストールしてくれます。

Winny（ウィニー）
日本で開発されたファイル共有ソフト。 インターネット上で，クライアント同士がお互いの保有するファイルをやり取りすることができる P2P 方式のソフトウェアです。ただし，映画や音楽，ゲームソフトなど，違法なデータがやり取りされることも多く，違法なデータを提供していた利用者が逮捕されたこともあります。

Word（ワード）
マイクロソフト社から発売されているワープロソフト。正式名称は，Microsoft Word。

WPA（ダブリュー・ピー・エー）
無線 LAN の暗号化方式「Wi-Fi Protected Access」（ワイファイ・プロテクテッド・アクセス）のひとつで，従来の WEP 方式による SSID と WEP キーに加えて，ユーザ認証機能を備え，暗号鍵を一定時間ごとに自動的に更新する「TKIP」（Temporal Key Integrity Protocol）と呼ばれる暗号化プロトコルを使用しています。 WPA には，家庭など小規模なネットワークを想定した WPA-PSK と，企業などの大規模なネットワークで利用される WPA-EAP があります。

WPA2（ダブリュー・ピー・エー・ツー）
無線 LAN の暗号化方式「Wi-Fi Protected Access」（WPA）の新バージョン。暗号化には，WPA より強度の高い「AES」を採用しており，128～256 ビットの可変長鍵を利用し

た強力な暗号化が可能です。 WPA2 には，家庭など小規模なネットワークを想定した WPA2-PSK と，企業などの大規模なネットワークで利用される WPA2-EAP があります。

WPA2-EAP（ダブリュー・ピー・エー・ツー・イー・エー・ピー）
業界団体である Wi-Fi Alliance（ワイファイ・アライアンス）が制定したセキュリティ規格のひとつで，WPA-EAP の後継方式に位置付けられるもので，暗号化方式として，より強固な AES を採用しています。 企業向けの暗号化方式で，外部の認証サーバを利用して暗号化を行います。

WPA2-PSK（ダブリュー・ピー・エー・ツー・ピー・エス・ケー）
業界団体である Wi-Fi Alliance（ワイファイ・アライアンス）が制定したセキュリティ規格のひとつで，WPA-PSK の後継方式に位置付けられるもので，暗号化方式として，より強固な AES を採用しています。 外部の認証サーバを用いずに，PSK を利用して暗号化を行う方式です。

WPA-EAP（ダブリュー・ピー・エー・イー・エー・ピー）
業界団体である Wi-Fi Alliance（ワイファイ・アライアンス）が制定したセキュリティ規格のひとつ。WPA は Wi-Fi Protected Access（ワイファイ・プロテクテッド・アクセス）の略で，EAP は Extensible Authentication Protocol（エクステンシブル・オーセンティケーション・プロトコル）の略。 企業向けの暗号化方式で，外部の認証サーバを利用して暗号化を行います。

WPA-PSK（ダブリュー・ピー・エー・ピー・エス・ケー）
業界団体である Wi-Fi Alliance（ワイファイ・アライアンス）が制定したセキュリティ規格のひとつ。WPA は Wi-Fi Protected Access（ワイファイ・プロテクテッド・アクセス）の略で，PSK は Pre-Shared Key（プリ・シェアード・キー）の略。 外部の認証サーバを用いずに，PSK を利用して暗号化を行う方式です。