第９講　デジタルセキュリティとプライバシー

１．デジタルセキュリティ

デジタルセキュリティは，コンピュータシステムやネットワーク，データを保護し，機密性、完全性、可用性を確保するための取り組みと言われています。ほぼ同義の言葉として，**サイバーセキュリティ**，より広範な意味での**情報セキュリティ**があります。

サイバーセキュリティは，サイバーセキュリティ基本法第２条で次のように定義されています。

> 第二条　この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。

法律の厳密な定義や言い回しですので難しい表現ですが，言わんとしていることは，コンピュータシステムやデータ，ネットワークを保護するための技術や対策を指し，それらに対する攻撃やデータ漏洩からの防御の意味合いが強くなっています。

情報セキュリティは，より広い概念で，いわゆるサイバー空間（仮想空間）と私たちが生活し活動している３次元の現実空間（フィジカル空間）での対策や保護をします。情報セキュリティについても，JIS Q 27001 や ISO/IEC 27001 で明確な定義や考え方が示されており，**情報の機密性，完全性，可用性を維持すること**とされています。

２．情報セキィリティの３要素（機密性，完全性，可用性）

機密性（Confidentiality）とは，認可されていない者に情報を使用させないことです。許可されていない者とは人間のほか例えば，データやシステム，ローカルエリアネットワークに対してアクセスできるアプリケーションソフトやシステムを限定するといったことが含まれます。具体的にが，学校のネットワークやサーバーにアクセスできる人間を限定したり，外部からの接続を制限したりすることや，教師用端末には教員以外がログインできないようにするといったことです。

認可されていない者と許可されている者を識別し確認する仕組みを**認証**といいます。すなわち，システムやネットワークにアクセスするユーザーやデバイスの身元を確認するプロセスで，これにより許可された正当なユーザーだけがアクセスできるようにし，不正アクセスを防ぐことができます（**アクセス制御**）。機密性は，許可された者が許可された方法で

図　本人認証の種類

認証の種類	具体例	メリット	デメリット
物理認証	物理鍵，印鑑，ICカード。	簡便で安全。	貸し借りが可能。紛失・盗難のおそれ。管理が煩雑。複製が可能。
知識認証	パスワード，暗証番号。	導入が容易。無くさない。	推定やクラッキングで破られる可能性。本人が忘れる。
生体認証	指紋，声紋，虹彩，網膜，静脈，顔，歩容。	本人以外を認識する可能性が極めて低い。	導入コストが高い。体調の変化で誤認のおそれ。

のみ情報にアクセスできることを確実にすること，とも言えます。

認証のうち特に個人を認証する**本人認証**には次のような種類があります。

・物理認証：利用者は所持する物理的なもので認証する方法です。家の鍵は，それを持っていると家に入れ，待ってないと入れないという識別をしています。印鑑もそれを使用した人を本人とするお約束ですね。

・知識認証：パスワードのように，知っているかいないかで認証する方法で最も一般的ですが，パスワードや暗証番号の強度や管理が重要となります。短く単純なものだったり，名前や誕生日，電話番号など他人も知っている情報などから推測されやすいパスワード，フィッシングメールやサイトで入力して詐取されたりで，他者に知られると不正使用される可能性が高まります。その対策として，２要素認証（多要素認証）の利用があります。多要素認証は，パスワードに加えて，もう一つの要素（例：スマートフォンに送られるコード，本人しか所持しないコード表からアクセスの都度指示される数字列）を使用して認証する方法で，かなりセキュリティが強化されます。

・生体認証：指紋、顔認識、虹彩認識など，利用者の生体情報を使用して認証する方法です。紛失する心配や所持忘れがなく，本人以外を認証する可能性が極めて低いが，導入コストが高額であること，体調やケガなどで変化して誤認される（認証されない）ことがあります。

完全性（Integrity）とは，情報が正確であること又それを保護することです。情報が正確であるように維持したり正確であることを保障することで，そのために，意図せず書き換えられたり（改ざん）破損されたりしないようにすることです。

完全性を保つための技術の一つとして**デジタル署名**があります。デジタル署名は，電子文書やデータの真正性と整合性を保証するための技術です。具体的には，以下のような役割を果たします。

① 真正性の確認：デジタル署名は，文書やデータが特定の送信者から送られたものであることを確認します。これにより送信者の身元を証明できます。

② 整合性の保証：デジタル署名が付与された文書やデータは、送信後に改ざんされていないことを保証します。もし改ざんが行われた場合，署名が無効になります。

③ 否認防止：送信者が後から「自分はその文書を送っていない」と否認することを防ぎます。デジタル署名は、送信者がその文書を送ったことを証明するための証拠となります。

デジタル署名は，**公開鍵暗号方式**を使用して生成されます。送信者は自分の**秘密鍵**を使って文書に署名し，受信者は送信者の**公開鍵**を使ってその署名を検証します。これにより，文

書の真正性と整合性が確認されます。

可用性（Availability）とは，許可された利用者が，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です。情報の機密性と完全性をがっちり守ろうとすれば例えば，情報が入ったファイルに強固なパスワードをかけ，可搬型メモリなどに入れ，頑丈な金庫に保管すれば大丈夫でしょう。確かに情報は守れますが，それでは必要な時に使えなかったり使い辛くなったりします。情報は本来，人が作成し人が利用するもので，使えなければ意味がないものです。可用性とは，情報を要求したときにアクセスできて使用できること，許可された者には情報がいつでも使える状態にすることです。

可用性を担保するには，システムの多重化・クラウド化やバックアップの定期的な作成といった方法があります。停電や故障でシステムやデータが使えなくなることも可用性が損なわれた状態です。システムの多重化やクラウド化はそのようなリスクに備える方策であり，バックアップの定期的な作成は，故障や災害などでデータが損傷することに備えたり，流行しているランサムウェア（Ransomware；感染したPCをロックしたり，ファイルを暗号化したりすることによって使用不能にし，元に戻すことと引き換えに「身代金」を要求する不正ソフト。身代金要求型不正プログラムとも呼ばれる。）感染に備えます。

３．情報セキィリティ対策の考え方

情報セキュリティは，ファイルやコンピュータに記録されているデータの保護，ウィルス対策や不正アクセス対策，コンピュータやネットワークシステムを対象としているわけではありません。それは狭い概念です。広義には，紙の文書なども含めた**情報資産**全体を守ることが目的で，リスクには，書類の紛失や盗難なども含まれます。個人情報も情報資産の主要な一部で，情報セキュリティ対策のうち，対象を個人情報に特化したものが**個人情報保護**となっています。

情報セキュリティでは，次のような脅威から情報資産を守るものと言われています。

- 自然災害　：
  地震，水害，火災などの脅威。自然災害以外でも，インフルエンザの流行や大規模停電など。発生頻度は小さい，発生したときの影響は非常に大きい。
- 機器の障害
  ハードウェアやネットワークの故障など。
- 人間の故意
  ウィルス，不正アクセス，不正持ち出し，詐取・窃盗など。
- 人間の過失
  プログラムミス，データの誤入力，誤配送，誤操作，文書やＵＳＢメモリの紛失など非常に多様。情報漏洩のトラブルでは，これが大多数と言われます。

情報セキュリティ対策では，リスクが顕在化して事故や事件（情報インシデント）となることを防ぐ対策や取り組みが重要ですが，リスクを完全になくすことは困難です。例えば自然災害が防げませんし，情報の利用や操作は人間が行うものですから，そこでの過失・うっかりも完全にゼロにはできません。ですので，情報セキュリティ対策では，起こったときにどう対応するかを事前に検討し対策を考えておくことも重要となります。

ここまでの説明をまとめますと，情報セキュリティとは，『**情報の機密性，保全性及び可用性を確保**することを目的として，自然災害，機器の障害，人間の故意，人間の過失等の**リスクを未然に防止**し，また，**発生したときの影響の最小化及び回復の迅速化**を図ること』となります。

すでにリスクという言葉を使っていますが，情報セキュリティでのリスクとは何でしょうか。リスクとは情報資産に与える脅威や脆弱性です。リスクは，情報資産，脅威，脆弱性の関係は次のように表せます。

リスク＝情報資産×脅威×脆弱性

・情報資産：組織にとって価値のある情報やシステム，機器など。
・脅威：情報資産に損失や損害をもたらす事象の潜在的原因。
・脆弱性：脅威の発生を誘引する原因。

リスクは情報資産，脅威，脆弱性の掛け算で表され，どれかが弱いと全体としても弱くなります。

以下に，情報資産，脅威，脆弱性それぞれの区分と例を示します。

情報資産の区分と例

区 分	例
情 報	データベースやデータファイル，契約書・同意書，システム関連文書，調査情報，利用者マニュアル，訓練資料，運用手順・サポート手順書，事業継続計画，代替手段の取り決め，監査証跡，保存情報
ソフトウェア	業務用ソフト，システムソフト，開発用ツール，ユーティリティソフト
物理的資産	コンピュータ装置，通信装置，取り外し可能な媒体，その他の装置
サ ー ビ ス	計算処理サービス，通信サービス，一般ユーティリティ（例えば，暖房，証明，電源，空調）
そ の 他	人，保有する資格・経験，無形資産（例えば，組織の評判・イメージ）

脅威の区分と例

大区分	区 分	例
人為的脅威	意図的脅威	コンピュータウィルス，不正侵入，改ざん，盗難 など
	偶発的脅威	人為的ミス，誤動作，故障 など
環境的脅威		地震，停電，火災，洪水，静電気 など

脆弱性の区分と例

分 類	脆弱性の例	関連する脅威
環境，設備	自由に出入りできる事務所	盗難，不正アクセス
ソフトウェア	アクセス制限のないパソコン	不正アクセス，なりすまし，改ざん
ハードウェア	老朽化したファイルサーバ	故障（データ破壊）
人	不注意	盗難，置き忘れ，情報漏えい

情報セキュリティ対策の第一歩として，所属する学校や機関において，保有する情報資産は何か，具体的な脅威や脆弱性として存在することは何か，など具体的に何が該当するかを洗い出していくことが求められます。

情報セキュリティ対策（リスク対策）の区分と例です。

情報セキュリティ対策（リスク対策）の区分と例

大分類	小分類	情報セキュリティ対策の例
物理的 セキュリティ対策		・建物の耐震，耐火，建物の施錠 ・入退出管理，機器の盗難防止，無停電装置の設置
論理的 セキュリティ対策	技術的セキュリティ対策	・コンピュータウィルス対策 ・アクセス制御，暗号化対策
	管理的セキュリティ対策	・ISMSの運用，監査 ・インシデント対策
	人的セキュリティ対策	・教育，訓練 ・違反者に対する罰則

物理的セキュリティ対策では，災害に対する，例えばサーバー室内にある重要な情報機器が倒壊などしないような耐震対策，火災及び消化活動による情報機器やデータの損傷への対策などが考えられます。日常的な対策として，情報機器や個人情報が記載された書類等の盗難に備える建物や職員室等の施錠や入退出管理があります。

論理的セキュリティ対策のうち**技術的セキュリティ対策**とは，情報システムやネットワークを保護するための具体的な技術や手法を指します。以下に，一般的な技術的セキュリティ対策の例を示します。

・ファイアウォール：ネットワークの境界で不正なアクセスを防ぐための装置やソフトウェアです。外部からの攻撃をブロックし，内部ネットワークを保護します。

・アクセス制御：データやシステムへのアクセスを制限し，権限のない者が情報にアクセスできないようにします。人のアクセスに対しては，パスワードや生体認証などの認証手法が用いられます。

・暗号化：データを暗号化することで、第三者がデータを読み取れないようにします。これにより、データの機密性を保護します。

・ウィルス対策ソフトウェア：マルウェア（malware：malicious（マリシャス：悪意のある）に software の 2 つの単語が組み合わせた造語）やウィルスからシステムを保護するためのソフトウェアです。定期的なスキャンとリアルタイム保護，ウィルス定義ファイルの定期的な更新の設定が必須です。

・バックアップ：データの定期的なバックアップを行うことで，データの消失や破損に備えます。バックアップ媒体は，異なる場所に保存することが推奨されます。

・**ソフトウェア更新**：ソフトウェアやＯＳのバグや脆弱性を修正するためのパッチを適用することです。これによりセキュリティホールを塞ぎます。

管理的セキュリティ対策では，組織内でのセキュリティに関するルールやガイドラインを定め，従業員やユーザーに遵守させることでセキュリティを強化します。情報セキュリティ対策の基本方針や対策基準，実施手順などを定め，基本方針や対策基準は情報セキュリティポリシーとして制定し，基本方針は公開します。ＩＳＭＳ（Information Security Management System：情報セキュリティマネジメントシステム）は，情報セキュリティ対策を維持運用し，かつ絶えず改善を行うための仕組みです。また，情報インシデントが発生した際に速やかに対応するとともに復旧対応，原因究明，再発防止などを担う CSIRT（Computer Security Incident Response Team）を編成しておくこともします。

人的セキュリティ対策では，職員などに対する教育・訓練を行います。故意や重大な過失など違反者に対する罰則規定を設け抑止力とするケースもあります。

４．情報セキィリティポリシー

情報セキュリティポリシーは次のような構造で，各組織・機関において制定されます。

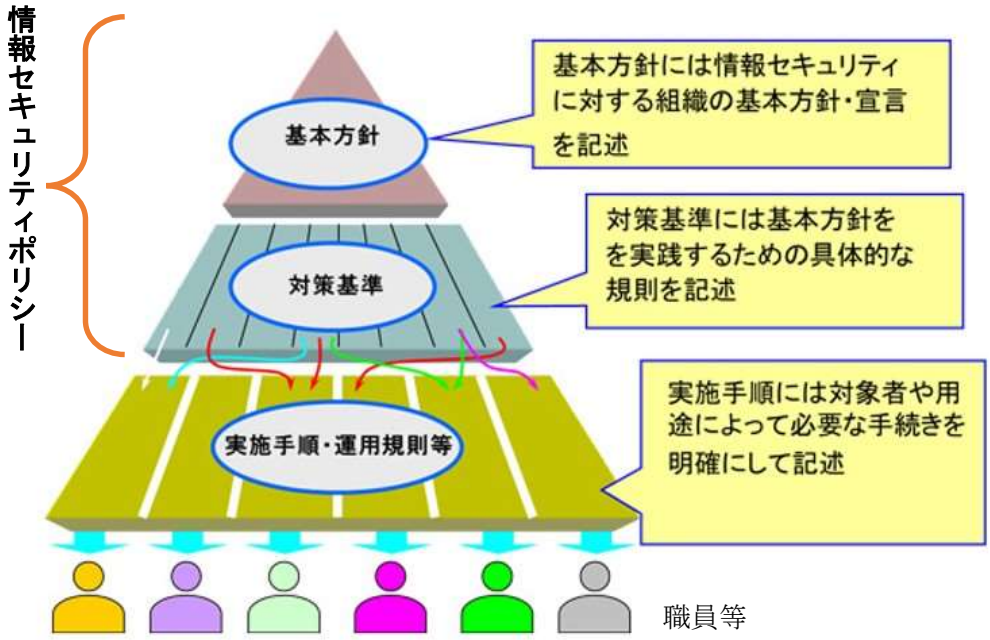


図　情報セキュリティポリシー

文部科学省は，平成 29 年に，**教育情報セキュリティポリシーに関するガイドライン**を制定して，学校の設置者に対し教育情報セキュリティポリシーを策定するよう求めました。その後，「GIGA スクール構想の下での校務の情報化の在り方に関する専門家会議」の提言（**GIGA スクール構想の下での校務 DX について～教職員の働きやすさと教育活動の一層の高度化を目指して～**）等を踏まえて，令和 6 年 1 月に改訂を行いました。

GIGA スクール構想の下での校務 DX について～教職員の働きやすさと教育活動の一層の高度化を目指して～

「教育情報セキュリティポリシーに関するガイドライン」公表について

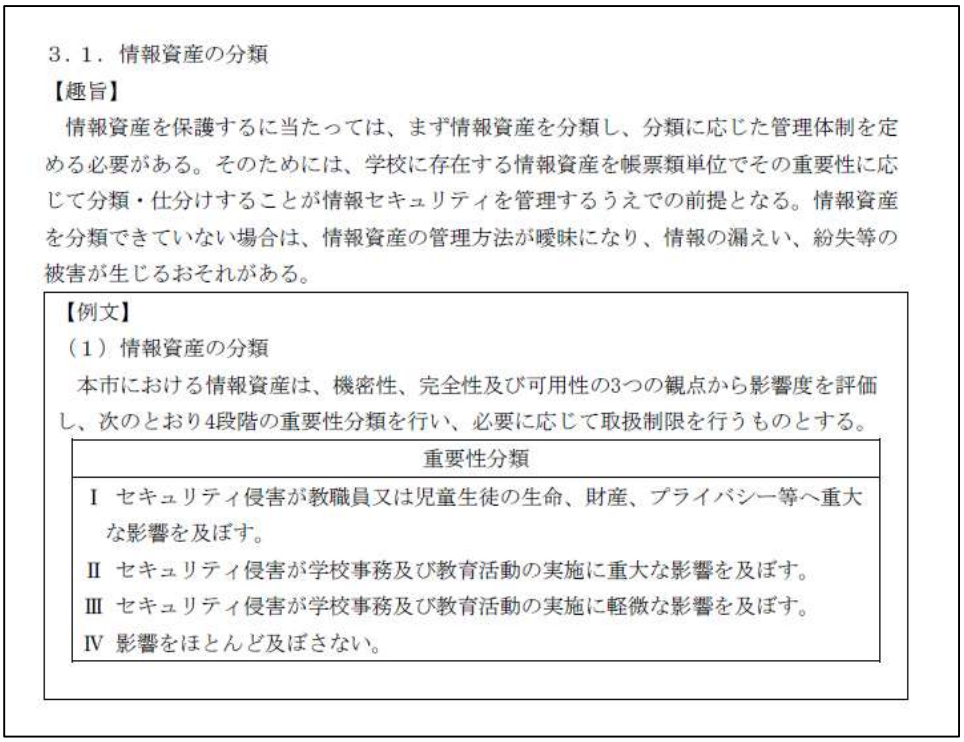
５．情報資産の格付け

先に述べたように，情報セキュリティ対策の第一歩として，所属する学校や機関において，保有する情報資産は何かを洗い出し，それぞれについてどの様な取り扱いをすべきかを決定していくことが不可欠です。守るべきものが分かってなければ守ることができず，漏えいや改ざんなどがあっても気づけないことになります。学校という組織では，保有する情報資産の多くが生徒・生徒に関わるものであり，それが適切に保護されないのは，個人情報漏えいということに止まらず，児童・生徒のプライバシーの侵害や様々な犯罪被害につながるおそれがあります。

（１）情報資産の分類（洗い出しと重要度の決定）

文科省・教育情報セキュリティポリシーに関するガイドライン（令和 6 年 1 月改訂）では，教育情報セキュリティポリシーに記述すべき情報資産の分類と重要度について以下のような例示をしています。

重要性分類に基づく情報資産の例示は，ガイドラインの 36 頁を参照ください。（ここに複製し掲載しても細かく文字がつぶれて読めないので，上記 URL から参照してください。）



3．1．情報資産の分類

【趣旨】

情報資産を保護するに当たっては、まず情報資産を分類し、分類に応じた管理体制を定める必要がある。そのためには、学校に存在する情報資産を帳票類単位でその重要性に応じて分類・仕分けすることが情報セキュリティを管理するうえでの前提となる。情報資産を分類できていない場合は、情報資産の管理方法が曖昧になり、情報の漏えい、紛失等の被害が生じるおそれがある。

【例文】

（1）情報資産の分類

本市における情報資産は、機密性、完全性及び可用性の3つの観点から影響度を評価し、次のとおり4段階の重要性分類を行い、必要に応じて取扱制限を行うものとする。

重要性分類
Ⅰ セキュリティ侵害が教職員又は児童生徒の生命、財産、プライバシー等へ重大な影響を及ぼす。
Ⅱ セキュリティ侵害が学校事務及び教育活動の実施に重大な影響を及ぼす。
Ⅲ セキュリティ侵害が学校事務及び教育活動の実施に軽微な影響を及ぼす。
Ⅳ 影響をほとんど及ぼさない。

情報資産の分類と重要度についての記載例（ガイドライン 35 頁）

ガイドラインでの情報の格付け，すなわち重要度分類の考え方は以下に示すとおりです。

（１）情報資産の分類

情報資産について、機密性、完全性及び可用性を踏まえ、被害を受けた場合に想定される影響の大きさをもとに分類を行い、必要に応じて取扱制限を定める必要がある。

本来情報資産の分類の考え方とは、外部漏えいの影響（機密性）、情報の改ざんの影響（完全性）、情報が使えなくなる影響（可用性）の３次元での影響を考慮して、その影響度合いに応じて分類・仕分けを行うべきである。

一方で、学校教育においては、膨大な量の校務系情報が存在し、ひとつひとつの帳票類について３次元の影響を加味した分類・仕分けを行うことは現実的ではない。そのため、３次元を１次元に単純化した重要性分類によって、分類・仕分けをすることを推奨したい。

重要性分類とは、当該情報資産のセキュリティ侵害による影響（被害）の大きさによって分類する考え方である。重要な情報とは、万が一セキュリティ侵害が発生した場合により大きな影響（被害）を受けることを意味し、４段階で定義している。分類・仕分けにおいては、各分類の定義に留意しつつ実施されたい。

以下に各分類の位置づけと枠組みについて解説する

・重要性分類Ⅰ：

個人アカウント情報、人事情報など、個人の生命・財産に関わるような機密情報を指す。

業務に係る特定の教職員のみがアクセスできる情報である。

・重要性分類Ⅱ：

児童生徒のプライバシー性の高い機微情報（成績、健康関連、家族構成、生徒指導履歴等や学校運営に係る校務系情報のなかで機密性の高い情報が相当する。業務に係る教職員のみがアクセスできる情報である。

・重要性分類Ⅲ：

児童生徒が学習活動で生成する学習系情報や、職員会議資料のような教職員全員が共有できる校務系情報を指す。児童生徒の家庭学習や教職員が共有可能な校務系情報であるため、学校内外からのアクセスを許容する。

・重要性分類Ⅳ：

上記以外の情報であり、万が一セキュリティ侵害が発生しても、ほとんど影響を無視できる情報である。

（注１）公開系情報は機密性を有しないが、改ざんされて困る情報については、その影響度により重要性分類Ⅲ相当と位置付けることが望ましい。

一般の組織・企業では，情報の格付けと取扱制限は以下のようにですが，学校においては教育情報セキュリティガイドラインの，3.2 情報資産の管理で取り扱いの例示がされています（上記 URL から参照してください）。

情報の格付けと取扱制限

情報の格付け及び取扱制限の定義の例

格付け	分類基準
機密性3情報	機密文書に相当する機密性を要する情報
機密性2情報	機密文書に相当する機密性を要しないが，漏えいにより，利用者の権利が侵害され又は本学活動の遂行に支障を及ぼすおそれがある情報
機密性1情報	機密性2情報又は機密性3情報以外の情報

➢ 機密性2情報及び機密性3情報を「**要機密情報**」といいます。

格付け	分類基準
完全性2情報	改ざん，誤びゅう又は破損により，利用者の権利が侵害され又は本学活動の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
完全性1情報	完全性2情報以外の情報

➢ 完全性2情報を「**要保全情報**」といいます。

格付け	分類基準
可用性2情報	滅失，紛失又は当該情報が利用不可能であることにより，利用者の権利が侵害され又は本学活動の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
可用性1情報	可用性2情報以外の情報

➢ 可用性2情報を「**要安定情報**」といいます。

➢ 要機密情報，要保全情報及び要安定情報を「**要保護情報**」という

【機密性についての取扱制限】

取り扱い制限の種類	指定方法
複製について	複製禁止，複製要許可
配布について	配布禁止，配布要許可
暗号化について	暗号化必須，保存時暗号化必須，通信時暗号化必須
印刷について	印刷禁止，印刷要許可
転送について	転送禁止，転送要許可
転記について	転記禁止，転記要許可
再利用について	再利用禁止，再利用要許可
送信について	送信禁止，送信要許可
参照者の制限について	○○限り

【完全性についての取扱制限】

取り扱い制限の種類	指定方法
保存期間について	○○まで保存
保存場所について	○○において保存
書き換えについて	書換禁止，書換要許可
削除について	削除禁止，削除要許可
保存期間満了後の措置について	保存期間満了後要廃棄

【可用性についての取扱制限】

取り扱い制限の種類	指定方法
復旧までに許容できる時間について	○○以内復旧
保存場所について	○○において保存

学認コンテンツ(情報セキュリティ)より

６．プライバシー

プライバシーとは，個人の情報や生活に関する権利を保護する概念で，個人が自分自身に関する情報をコントロールし，その開示や利用を制限する権利や自由のことを指します。個人の自由や尊厳，自主性を守るために非常に重要なものです。

プライバシー権は，この「自己の情報をコントロールする権利」とともに，（自分に関する情報がみだりに公開されたり使用されたりすると私生活に干渉される可能性が生じますから）「他人から干渉・侵害を受けない権利」とされています。

プライバシーの概念は時代や文化，技術の発展に伴い進化してきました。具体的には，以下のような要素が含まれます。

(1) 個人情報の保護

名前，住所，生年月日，性別（基本４項目），電話番号，メールアドレスなど、個人を特定できる情報を保護すること。

(2) データの管理（情報プライバシー）

個人のデータが適切に管理され，不正に利用されないようにすること。今日のデジタル社会では，サイバー空間での個人の情報活動は進展し，ネット上での活動記録（ログ）や行動履歴が自動的に収集されるようになり，それらの適切な保護と利活用が求められています。

(3) 通信の秘密（コミュニケーションプライバシー）

個人の通信内容が第三者に知られないようにすることで，郵便やメールや電話などが含まれます。

(4) プライベートな空間の保護（身体的プライバシー）

自宅や個人の所有物など，プライベートな空間が侵害されないようにすること。

(5) 思想・心情の保護（心理的・感情的プライバシー）

思考，感情，信念などを他者に知られることなく保ったり強制されたりしないこと。

ICT 技術の進歩で，情報収集が容易になったこともあり，私たちの行動履歴の収集の容易になっています。

(6) 行動履歴の保護（行動的・位置情報プライバシー）

人の移動や行動パターン，位置情報の追跡など勝手に利用されないようにすること。

プライバシーとその保護について，日本国憲法や法律ではプライバシー保護に関する規定は明確には記載されていませんが，個人の尊重と幸福追求権を保障した憲法第１３条がプライバシー権の根拠とされています。これまでの多くの判例や学説により，憲法第１３条に定める人格権の一部として認められています。

> **憲法第１３条　すべて国民は、個人として尊重される。生命、自由及び幸福追求に対する国民の権利については、公共の福祉に反しない限り、立法その他の国政の上で、最大の尊重を必要とする。**

７．個人情報保護法

我が国でのプライバシー情報のうち個人情報の保護については，**個人情報保護法**（個人情報の保護に関する法律が担っています。

個人情報保護法は，2005(平成 17)年 4 月に全面施行され，2015(平成 27)年に番号法制定に伴う改正，その後何度か改正されています。

個人情報保護法（以下，法と略します）の主旨は，次のとおりです。

・個人情報の有用性に配慮しつつ，個人情報の取得・利用に関わるルールを制度化し，個人のプライバシー、権利利益を保護する。

・個人に関わる情報の適正な取り扱い方法を整備し、またそのためのルール遵守を個人情報取扱事業者に義務づける。

法が制定された背景は，

・高度情報通信社会においては情報が価値を持つ。

・コンピュータ処理によって複数の情報を組み合わせたり、複数の機関で共有したりすることが容易になった。

・個人情報を悪用した犯罪も起きてきている。

・ネットワークを活用した国際的な企業活動が旺盛になった。

などがあげられ，今日のサイバー空間での情報利用のなかでは，個人に関する情報の扱いとその価値が飛躍的に増大しており，適正な利用と保護がますます重要となっています。

法の要点は、以下に挙げるとおりです。

・個人情報を収集する際には利用目的を明確にしなければいけない。

・個人情報を，情報取得の際に示した目的以外の目的で利用する場合には，本人の同意を得なければいけない。

・個人情報を収集した場合，利用目的を本人に通知・公表しなければならない。

・個人情報を集めた場合，その情報が漏洩しないよう対策を講じなければならない。

・本人の同意を得ずに第三者に情報提供してはならない。

・本人からの求めに応じて情報を開示しなければならない。

・公開された情報が事実と異なる場合，訂正や削除に応じなければならない。

８．法に規定される個人情報とプライバシー情報

法第２条で，個人情報が以下のように規定されています。簡単に言えば，個人情報とは，

・生存する個人に関する情報

・当該情報に含まれる氏名，生年月日その他の記述等で，**特定の個人を識別することができる**もの

・他の情報と容易に照合することができ，それにより特定の個人を識別することができることとなるものを含む。

・個人識別符号が含まれるもの。

です。

> **第２条**　この法律において**「個人情報」**とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。
>
> **一**　当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第２号において同じ。）で作られる記録をいう。第18条第２項において同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）
>
> **二**　個人識別符号が含まれるもの

法に定める個人情報は，生存している特定の個人を識別できる情報としており，私たちが日常使っている「個人情報」という意味には，すなわち他人に知られたくない情報，すなわちプライバシー情報に近いと思われます。プライバシー情報には「個人情報」以外の「個人の秘密にしたい情報」や「公開されると私生活に干渉される可能性がある情報」など幅広い情報を含んでいます。

番号法（行政手続における特定の個人を識別するための番号の利用等に関する法律）により，　2016(平成28)年１月よりマイナンバー制度が導入されました。マイナンバー制度は，行政を効率化し，国民の利便性を高め，公平・公正な社会を実現する社会基盤ですが，行政が保有する様々な個人に関する情報が紐づけされる可能性から，より厳しい保護が求められました。「マイナンバー（個人番号）をその内容に含む個人情報」を特定個人情報と定義し，一般的な個人情報よりも厳重な管理と利用目的も明確に定められました。

2015(平成 27)年の法改正で，個人情報に「個人識別符号が含まれるもの」を追加（改正法２条１項，２項）し，

①個人の身体的特徴を変換した符号等

ゲノムデータ，顔，指掌紋,手の平・手の甲・指の静脈,歩容,声紋等の認識データ

②役務・サービスの利用者・購入者別に割り当てられる符号等

マイナンバー，運転免許番号，旅券番号，保険証番号，基礎年金番号，国家資格の登録番号，住民票コード等

など，情報技術の進歩などで，従来はそれのみで個人情報とは考えられてこなかった情報，人間の目や耳で知覚できない電子データによる個人に関する情報が該当します。

さらに，改正法（2条3項）で，**「要配慮個人情報」**という**「人種，信条，社会的身分，病歴，犯罪の経歴，犯罪により害を被った事実その他本人に対する不当な差別，偏見その他の不利益が生じないようにその取り扱いに特に配慮を要するものとして政令で定める記述等**

が含まれる個人情報」が規定されました。これは「個人の秘密にしたい情報」や「公開されると私生活に干渉される可能性がある情報」の情報の一部と言ってよいものですから，その扱いはより厳しいものとなっており，要配慮個人情報の取得には本人同意が必須であること，本人同意がない**第三者提供特例（オプトアウト）**は禁止されています。

なお，一般の個人情報も，情報の収集と利用に当たっては次のことに留意が必要です。

・個人情報を取り扱うに当たっては，どのような目的で個人情報を利用するのか具体的に特定する必要があります。
・個人情報の利用目的は，あらかじめホームページ等により公表するか，本人に知らせなければなりません。
・取得した個人情報は，利用目的の範囲でしか利用できません。
・取得している個人情報を，特定した利用目的の範囲外のことに利用する場合，あらかじめ本人の同意が必要です。

このように，本人に情報の収集や利用に関する十分な情報を提供し，その同意を得ることで，プライバシーすなわち自己の情報をコントロールする権利を保護するための手法を**インフォームドコンセント**と言います。

先に述べたように，プライバシー権の内容として自己の情報をコントロールする権利がありますが，個人情報保護法は，自分の個人情報について開示・訂正・利用停止等の情報コントロールをする権利を認める法律であり，法が求める個人情報の適正な取り扱いを徹底することで，プライバシー権を含む個人の権利や利益の保護が図られます。

９．ビッグデータ・ＡＩ時代における個人情報の活用

近年の情報通信技術の発展により，これまで蓄積された多種多様かつ膨大な，いわゆるビッグデータの収集・分析が可能となり、データの利活用が経済の活性化を促進すると言われています。こうした中，個人情報保護法に対し，個人情報として取り扱うべき範囲の曖昧さのため事業者が利活用を躊躇し，ビッグデータのうち特に利用価値が高いとされている個人の行動・状態等に関するパーソナルデータの利活用が十分に行われていないとの指摘があり，また一方では，多くの個人情報データの流出を始め，消費者の個人情報及びプライバシーの保護が十分でないとの指摘がなされています（谷澤 2015)。

個人情報の収集と利用については，先に説明したように，利用目的を本人に知らせること，目的使用や第三者提供する場合は本人の同意を得ることが求められますが，個人の行動・状態等のように自動的かつ膨大に収集される情報についてはその都度本人同意を得ることは困難です。それらが利用できないと新しい情報サービスやビジネスなどが実現できず，経済活性化できないという側面と，本人にとっても利益となる新しいサービスが利用できないという側面も考えられます。

改正法では，個人の特定性を低減したデータである**匿名加工情報**については個人情報か

ら除外することとしました。匿名加工情報は「特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものをいう」（第２条第９項）と規定されています。匿名化により個人の識別を困難にして個人のプライバシーを保護しつつ，データの利用が可能となります。

改正法におけるプライバシー保護は，国際的に特にＥＵの状況からみて不十分と言われます。ＥＵの**一般データ保護規則**（General Data Protection Regulation ： **GDPR**）は，対象とする「個人データ」を広範に定義し，ヨーロッパ市民に関する個人情報を扱うすべての企業（ほかの大陸の企業を含む）に適用されます。GDPR における個人データ（Personal Data）とは，名前，写真，メールアドレス，銀行の詳細，SNS の投稿やウェブサイトの更新情報，場所の詳細，医療情報，IP アドレス，生体遺伝子情報，思想信条，入れ墨に至るまで，個人に関する広範囲な情報です。

> **GDPR 第４条**　個人データとは，識別された又は識別され得る自然人（以下「データ主体」という。）に関するあらゆる情報を意味する。識別され得る自然人は，特に，氏名，識別番号，位置データ，オンライン識別子のような識別子，または当該自然人に関する物理的，生理的，遺伝子的，精神的，経済的，文化的もしくは社会的アイデンティティに特有な一つ，もしくは複数の要素を参照することによって，直接的にまたは間接的に、識別され得るものをいう。

世界がインターネットでつながっている現在，GDPR の影響は全世界に及んでいます。当然 EU 加盟 27 ヵ国から遠く離れた日本でも，EU 域内の個人データを扱っている企業は数多くあります。GDPR の基準を満たすのはハードルが高く，中小企業や個人営業の業者は対応に苦慮しています。（例えば，田舎の小さな日本旅館がＥＵ域内から予約を受けた場合，予約者の氏名・連絡先等の個人データの扱いも GDPR に従わなくてはならず，その基準をクリアできなければ，EU からの客を受け入れられないことになります。）

１０．　デジタルセキュリティとプライバシー

デジタルセキュリティ対策とプライバシー保護は密接に関連しています。セキュリティが確保されていないシステムやデータ管理では，不正アクセスや攻撃のリスクが高まり，個人情報やプライバシーが侵害される可能性があります。セキュリティ対策が十分に実施されることで，プライバシーの保護が強化されます。

デジタルセキュリティとプライバシーの重要性は，今日ますます高まっています。すべての情報機器・情報端末はもちろん，これまで情報機器と考えられなかった様々な機器がオンラインで全世界につながり（Internet of Things：**IOT**），情報の生成，収集，蓄積が瞬時に行われる時代です。個人の情報は，私たちが明示的に作成したり発信したりするもののほか，行動履歴や位置情報など意識しないで収集される情報も増大しています。明示的な情報でも，クレジットカードや銀行口座の金融情報などの秘匿性が高い情報，診療や投薬情報など機微情報がオンラインで扱われることが多くなっています。今日の私たちの

生活や仕事で，自分に関する情報でデジタル化されていない情報を挙げるほうが難しい時代となっており，情報の価値も増大しているわけです。

これらの情報を狙うサイバー攻撃も増加しています。サイバー攻撃やデータ侵害のリスクが増加しているため，組織や個人においてもセキュリティ対策やプライバシー保護がより重要となっています。

■

参考文献

・文部科学省（2023）GIGA スクール構想の下での校務 DX について～教職員の働きやすさと教育活動の一層の高度化を目指して～，
https://www.mext.go.jp/b_menu/shingi/chousa/shotou/175/mext_01385.html
（2024/11/16 参照）

・文部科学省（2024）教育情報セキュリティポリシーに関するガイドライン，
https://www.mext.go.jp/content/20240202-mxt_jogai01-100003157_1.pdf
（2024/11/16 参照）

・宇賀克也(2013)個人情報保護法の逐条解説 第４版，有斐閣

・宇賀克也(2014)番号法の逐条解説，有斐閣

・瓜生和久(2015)一問一答平成 27 年改正個人情報保護法，商事法務

・谷澤光（2015）個人情報の保護と有用性の確保に関する制度改正―個人情報保護法及び番号利用法の一部を改正する法律案―，立法と調査，No.363，参議院事務局企画調整室