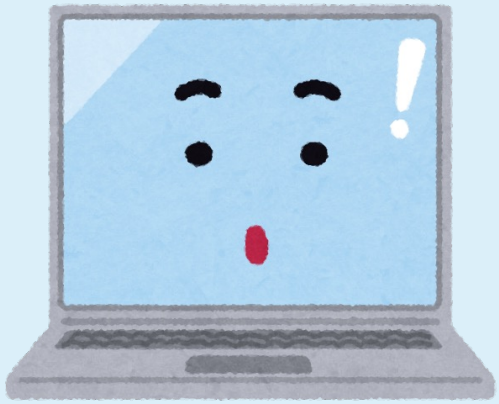
情報セキュリティの基礎

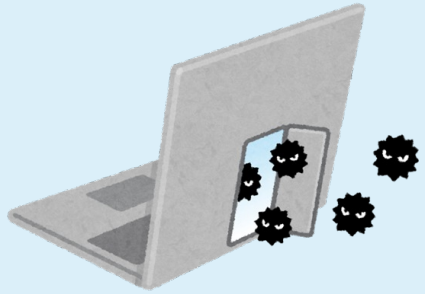
〈目次〉

①ウィルス・不正アクセス・パスワード
②暗号化・電子署名・認証
③セキュリティマネジメント



①ウィルス・不正アクセス・パスワード

コンピュータウィルスとは？



「第三者のプログラムやデータベースに対して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」

（経済産業省のコンピューターウイルス対策基準の定義より）

■　ウィルスが持つ特性

・自己伝染機能：自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、 他のシステムに伝染する機能

・潜伏機能：発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

・発病機能：プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

ウィルスの種類と感染経路

ウィルスの種類

- 狭義のウィルス
- マクロウィルス
- スクリプトウィルス
- ブーストラップ・ウィルス　など

ウィルスの感染経路

- 電子メールの添付ファイルから
- ファイルのダウンロード
- HTMLメールから
- 記憶媒体による感染

○ウィルス対策

・ウィルス対策としてウイルスの検査や予防、修復のいずれかの機能を含むソフトウェア（通称：ワクチン）を入手し最新の状況にアップデートしておく

・添付ファイルの開封や、ダウンロード、フロッピー等の挿入などをする際は細心の注意を払う

・ウィルスを発見した場合、パソコンをネットワークから切り離してシステム管理者が状況を調べるようにする

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」

（総務省　国民のための情報セキュリティサイトより）

⚠アクセスするだけでなく、第三者に情報を漏らす「不正アクセスを助長する行為」も犯罪になってしまう！

不正アクセスによる被害

・データの漏洩や改ざん、破壊が起こってしまう

・電子メールのサーバを介してウイルスを伝播させられたり、 ホームページを改ざんされてウイルスの伝播に使われたり反社会的な表示をさせられたりしてしまう

・セキュリティ対策が不十分だと、第三者によってDoS攻撃の踏み台にされる危険もある

不正アクセス対策＆パスワード

- 全体的な対策

⇒ファイアウォールやセキュリティ監視を設置して、アクセスを監視＆防止

- 部分的な対策

⇒ワンタイムパスワードやコールバックなどの仕組みを利用した対策

- パスワード

⇒他人が知ることが容易な情報（氏名、生年月日、電話番号）で作成せず、数字や文字、特殊記号を混在させた適当な長さのパスワードを作成する

・パスワードは定期的に更新するようにすると良い。一定期間後、強制的にパスワードを変更する仕組みなどを使っていくこともパスワードの安全性に繋がる

・パスワードは記録せず毎回入力する、また、顔などの身体の一部を用いたバイオメトリクス認証を使うことも安全性の徹底に繋がる

②暗号化・電子署名・認証

暗号方式の種類

■　秘密鍵暗号方式

⇒共通鍵暗号方式ともいい、暗号化鍵と複合鍵が同じ。代表的なものにDESがある。しかし、盗聴の危険や相手が違うたびに鍵が新しく必要になることからあまり使用されていない。

■　公開鍵暗号方式

⇒この方式は暗号化する鍵と復号する鍵が異なるもの。 ドアを開ける鍵は秘密にする必要があるが、ドアを閉める鍵は 他人に使われてもよいよう復号鍵は秘密にするが暗号化鍵は公開してもいいようになっている。現在、一般的に公開鍵暗号方式が使われており、代表的なものにRSAがある。欠点は暗号化や復号に時間を要する。

そのため、セクション鍵暗号方式が暗号化に広く採用されている！！

電子署名と認証の仕組み

■　送信者Ａが受信者Ｂに、送信者がＡであることを電子署名するとき次のように行う

①送信者Ａは、認証局（ＣＡ）から自分の認証番号を得ておく。

②送信者Ａは、その認証番号をＡの秘密鍵で暗号化する。

③受信者Ｂは、Ａの公開鍵で復号する。 誰でもＡの公開鍵は得られる。文書に添付することもできる。Ａ以外には、Ａの秘密鍵を使える人はいない。それにより、ＢはＡの実印が押印されていると判断する。

④ 受信者Ｂは、その認証番号を認証局に問い合わせる。

⑤ 認証局は、Ｂに認証証明書（印鑑証明書）を送る。 それにより、Ｂはその実印が正しいことを確認できる。

電子署名法によって、電子署名が実印と同じ法的効力をもつことが定められるようになった。

暗号化の標準

- S/ＭＩＭＥ

⇒公開鍵暗号方式を利用したインターネット電子メールの暗号化と電子署名に関する国際規格。

- ＳＳＬ（ＴＬＳ）

⇒ インターネット上で情報を暗号化して送受信するプロトコル。公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティ技術を組み合わせたもので、WWWやＦＴＰなどのデータ を暗号化して送受信することができる。

- ＳＥＴ

⇒インターネットでクレジットカード決済をするときのセキュリティのプロトコル。ＳＳＬでは受取側（店舗）でクレジット番号 を知ることになるが、ＳＥＴでは受取側にもクレジット番号を伝えることなく、取引できる仕組みになっている。

最新のものでは「ＱＵＩＣ」という最新型も出始めている！！

③セキュリティマネジメント

セキュリティ対策の基礎

情報セキュリティの３要件＝ＣＩＡ

- 機密性（Confidentiality）

⇒許可された者が許可された方法でのみ情報にアクセスできるこ とを確実にすること。

- 完全性（Integrity）

⇒情報及び処理方法の正確さ及び完全である状態を安全防護すること。

- 可用性（Availability）

⇒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。

情報システムの脆弱性と情報セキュリティ対策

情報システムが機密性・完全性・可用性が欠けている状態を脆弱性という

情報セキュリティ対策＝ 情報システムでの*インシデントを減少させること

（*インシデント⇒脅威が発生して実際に事件が生じている状態のこと）

リスクを無くすことはできないため、減らすことが大切

↓

リスクを減らすということは情報システムの脆弱性を減らすこと

情報セキュリティ対策とは機密性、完全性、可用性を 高めることで情報システムの脆弱性を減らすこと

個人情報保護法

- リスクの大きな分野に、個人情報の漏洩がある
- 個人情報保護の目的（個人情報の保護に関する法律より）

「高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることにかんがみ、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の有用性に配慮しつつ、個人の権利利益を保護すること」

- 個人情報データベース

⇒個人情報を含む情報の集合物で、検索することができるように体系的に構成したもの

・個人データの量が 過去６ヶ月以内で５０００人を超える者を個人情報取扱事業者とし、個人情報の保護義務を定めている。

※個人情報保護体制を適切に行っている事業者であることを第三者が認定する制度「プライバシーマーク制度」を導入

セキュリティマネジメント

■　リスク対策の手順

・情報資産の調査（何を守るのか）

コンピュータシステムだけでなく、紙での情報も含む全体的な調査や、情報資産に優先順位をつける必要がある。

・脅威の調査（何から守るのか）

自然災害、機器の障害、故意・過失等のリスクを洗い上げることが必要。

・リスクの大きさの分析（＝どの程度守るのか）

リスクの大きさ（発生確率×発生時の損失）を推定して、何の資産を何の脅威からどの程度のレベルで守るのかを明確にする。

・対策の策定（どのようにして守るのか）

具体的に守る手段を列挙して、効果的な方法を選択する。

■　セキュリティマネジメントの考えかた

・経営者のリーダーシップ

全社的な継続的な運動として推進するために、経営者が中心とな ってリーダーシップをとることが重要。

・成熟度の向上

一挙に理想的な状況にすることはできないため、自社の現状を考慮して、逐次的に向上させることが必要。

セキュリティポリシー

基本方針（狭義のセキュリティポリシー）

情報セキュリティマネジメントの最高責任者である経営者が、情報セキュリティに関する基本的な方針を示すものとして、情報 セキュリティに対する目標とその目標を達成するために企業がとるべき行動を社内外に宣言するもの。

- 対策基準

セキュリティポリシーに基づいて適切なセキュリティ対策が行われるために、関係者が遵守すべきセキュリティ活動の基準を具体的に明文化したもの。個々の情報資産のリスクへの対策と情報資産の重要性を比較し、適切なセキュリティ対策を規定するもの。

- 実施基準

適切なセキュリティを維持するために、関係者が遵守すべきセキ ュリティ対策の実施手順を具体的に示したもの。対策基準で定めた内容に対応する実施手順を、各担当部門や職務に関して定める。

- セキュリティ監査

情報セキュリティの分野では、どのようにセキュリティ対策を進めればよいかについては、情報セキュリティ監査制度があり、それを第三者認定するＩＳＭＳ適合性評価制度がある。また個人情報保護の分野での第三者認定にはプライバシーマーク制度がある。

参考サイト

- コンピュータウイルス対策基準 (meti.go.jp)
- 国民のための情報セキュリティサイト (soumu.go.jp)
- コンピュータウイルスの種類や基礎知識、セキュリティ対策について (hammock.jp)
- 個人情報の保護に関する法律 | e-Gov法令検索