１２．「情報セキュリティ」

本時のポイント

１．情報セキュリティについて理解します。

（１）ウイルス・不正アクセス・パスワード

①コンピュータウイルス

■情報セキュリティの被害；

http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h19/index.html

(a) ウイルスの定義

経済産業省告示「コンピュータウイルス対策基準」（平成７年７月制定，平成１２年１２月改訂）による定義

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であり，次の機能を一つ以上有するもの。

(b) 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

(c) 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

(d) 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

②ウイルスの種類

(a) 狭義のウイルス

ウイルスの入っているプログラムファイルを起動することにより感染します。

(b) マクロウイルス

ＷｏｒｄやＥｘｃｅｌなどのマクロ命令にウイルスを忍ばせたファイルを開いたときに感染します。

(c) スクリプトウイルス

ＨＴＭＬのスクリプト命令にウイルスを忍ばせておき，そのページを閲覧したしたときに感染します。

■インターネットの安心・安全な利用環境の実現；

http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h19/index.html

(d) ブートストラップ・ウイルス

パソコンに電源を入れたときにフロッピーが挿入されていると，ＢＩＯＳというＯＳ機能により，フロッピィのブートストラップ部分を読みます。そこにウイルスが潜んでいると電源を入れただけで感染してしまいます。

③ウイルスの感染経路

(a) 電子メールの添付ファイル

最も大きな感染経路は，電子メールの添付ファイルによるものです。ウイルスの多くは，単にパソコン内に潜入するだけでなく，パソコンにある宛先のリスト（アドレス帳）を調べて，その宛先へウイルス付きの添付ファイルを転送します。しかも，発信者の名前もリストの名前を騙ることもあるので，送信者を見て信頼することは危険です。

(b) ファイルのダウンロード

Ｗｅｂサイトからウイルスを含むファイルをダウンロードすることにより感染します。意識的にダウンロードをしなくても，閲覧したときにスクリプトにより自動的にダウンロードしてしまう危険もあります。

(c) ＨＴＭＬメール

ＨＴＭＬ形式による電子メールにウイルスが潜んでいる場合，そのメールを開くことにより感染します。メールソフトのプレビュー機能をオンにしておくと，受信しただけで感染する危険があります。

(d) 記憶媒体による感染

フロッピーやＣＤ-ＲＯＭなどに，ウイルスを含むファイルが存在する場合もあります。ブートストラップ・ウイルスがあると，それらを挿入しただけで感染する場合もあります。

④ウイルス対策

(a) ワクチン（アンチウイルス・ソフト）

ウイルスの検査，予防又は修復のいずれかの機能を含むソフトウェアをワクチンといいます。マイクロソフトでは Windows Update により提供していますし，ウイルスバスターやノートンアンチウイルスなど市販のソフトもあります。これらを最新の状況にアップデートしておく必要があります。

(b) 日常の注意

添付ファイルの開封，ダウンロード，フロッピー等の挿入などをするときには，ワクチンでチェックするなどの細心の注意が必要です。

※ウイルスを発見したときの措置

企業などでウイルスを発見したときは，次のような措置が必要です。

(c) 発見者（利用者）

決して独断で解決しようとしてはなりません。かえって対策を困難にする危険があります。

ともかく他のパソコンへの伝染を防ぐために，ネットワークから切り離します。

速やかにシステム管理者に電話して，その指示に従います。

(d) システム管理者

影響がそのパソコンだけに限定できるか，他に伝染しているかを調べます。

他への伝染が懸念される場合には，速やかに関係者全員に対処方法を指示します。

対象パソコンのウイルス除去をします。

ウイルス感染の必要情報をＩＰＡに届けます。

⑤不正アクセス

(a) 不正アクセスの定義

不正アクセス禁止法（不正アクセス行為の禁止等に関する法律，平成１１年８月成立，平成１２年２月施行）では，

ネットワークを通して

許可されていない者がなりすましをしてアクセスすること

許可されている者が許可されていないアクセスをすること

そのようなアクセスができるような状態にすること

を不正アクセスと定義しています(「なりすまし」とは，他人のユーザＩＤやパスワードを用いて，その人のように見せかけることをいいます）。

そして，不正アクセスをした者だけでなく，ユーザＩＤやパスワードなど第三者に漏らす「不正アクセスを助長する行為」も犯罪とされ，本法により罰せられます。また，システム管理者に適切な管理措置を講じる必要があることを努力義務としています。

■コンピュータ不正アクセス対策基準；

http://www.ipa.go.jp/security/ciadr/guide-crack.html

通商産業省告示「コンピュータ不正アクセス対策基準」（平成８年８月制定，平成１２年１２月改訂）では，不正アクセスとは「システムを利用する者が，その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うこと」であると定義して，コンピュータ不正アクセスによる被害の予防，発見及び復旧並びに拡大及び再発防止について，企業等の組織及び個人が実行すべき対策をとりまとめています。

(b) 不正アクセスによる被害

セキュリティ対策が不十分なために不正アクセスを受けると，自社が損失を蒙るだけでなく，第三者に多大な迷惑をかけることになります。

(c) データの漏洩，改ざん，破壊

自社の重要な情報が漏洩，改ざん，破壊されるのは，自社に大きな損害を与えます。

個人情報・取引先情報の漏洩

顧客名簿などの個人情報が漏洩すると顧客に多大な迷惑を与えます。個人情報保護法により，個人情報を保護することは事業者の責務とされています。個人情報ではなくても，取引情報が漏洩すれば取引先に損害を与えます。

(d) ウイルスの伝播

電子メールのサーバを介して，ウイルスを伝播させられる危険，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する危険があります。

(e) ＤｏＳ攻撃の踏み台

ＤｏＳ攻撃とは，いっせいに大量のデータを送信することにより，受信側の本来の機能を麻痺させる攻撃のことです。セキュリティ対

策が不十分だと，トロイの木馬とかボットというウイルスを仕掛けられ，一定の時刻あるいは不正アクセス者の指示により，第三者に大量のデータを発信させられるＤｏＳ攻撃の踏み台にされる危険があります。

(f) 不正アクセス対策

最も基本的な対策は，社員のパスワードを第三者に使われて，なりすましをされないようにすることです。パスワード管理については後述しますが，次のような対策があります。

⑤全体的な対策

(a) ファイアウォール

外部のインターネットと社内のネットワークとの接続個所に，許可されたアクセスは通過させ，そうではない利用は防止するといった関所の役目をするファイアウォールを設置することにより，不正アクセスを防止します。

(b) セキュリティ監視

ファイアウォールを潜り抜けてきたアクセスを監視するために，ネットワークを流れるデータを監視するシステムです。

⑥部分的な対策

(a) ワンタイムパスワード

アクセスをするたびに，毎回パスワードを変更する仕組みです。

(b) コールバック

会社のネットワークにダイアルアップで接続するとき，それでは接続しないで，サーバから登録された端末の電話番号にコールバックすることにより接続します。これにより，登録以外の場所からのなりすましを防止します。

■ファイアウォール；

ファイアウォール（防火壁）とは，ある特定のコンピュータネットワークとその外部との通信を制御し，内部のコンピュータネットワークの安全を維持することを目的としたソフトウェア，あるいはそのソフトウェアを搭載したハードウェアである。英語で防火壁と表現するのは，外部から内部のコンピュータネットワークへ侵入しようとするクラッキング行為を，火事に喩えたものである。

⑦パスワード

(a) 不適切な例

・氏名，生年月日，電話番号など，他者が知ることが容易な個人情報

・辞書にある単語－不正者はパスワード発見辞書を持っている

・短い文字列－総当りで発見できる。

(b) よいパスワード

・表面的には無意味な文字列

・適当な長さ（８文字以上）

・数字，英字，特殊記号を混在させる

⑧パスワードの管理

(a) パスワードの付与

最初にシステム管理者が利用者に仮パスワードを付与するときは，上記の「よいパスワード」になるようなランダムな文字列を与えて，利用者が最初にアクセスするときに，自分でパスワードを設定させます。

(b) パスワードの変更

利用者は，できるだけ頻繁にパスワードを変更するべきです。また，一定期間あるいは一定アクセス回数のたびに，強制的にパスワードを変更させる仕組み，８文字以上とか文字種混在の条件を満たさないと受け入れない仕組みなどが必要です。

(c) パスワードの失念

パスワードは本人以外が知るべきではありません。システム管理者も同様です。本人がパスワードを失念したときは，まず，そのユ

ーザＩＤでの利用を禁止し，改めてユーザＩＤ（同じでもよい）とパスワードを再発行するようにします。

(d) パスワード記録の禁止

パスワードを書いた付箋をパソコンに貼るのは論外。手帳に書くのも落としたとき困ります。特に重要なのが，パソコンの紛失・盗難・廃棄への考慮です。パソコンにパスワードを残さないために，「パスワードを記憶する」にせず，毎回入力させるようにします。

(e) バイオメトリクス認証

パスワードのような自分が覚えるものではなく，指紋，手形，網膜など身体の一部を用いることをバイオメトリクス認証といいます。これにより，さらに厳重な本人認証ができます。

（２）暗号化・電子署名・認証

①暗号方式の種類

(a) 秘密鍵暗号方式

秘密鍵暗号方式は共通鍵暗号方式ともいいます。暗号化鍵と複合鍵が同じです。代表的なものに，ＤＥＳがあります。

秘密鍵暗号方式には，次の欠点があります。

・鍵を第三者に秘密にする必要がある

・鍵を相手に電子メールで送る際に盗聴される危険がある

・相手が異なるたびに新しい鍵が必要になる

・相手が多くなると管理しきれない（オンライン取引）

(b) 公開鍵暗号方式

公開鍵暗号方式では，暗号化する鍵と復号する鍵が異なるのです。ドアを開ける鍵は秘密にする必要がありますが，ドアを閉める鍵は他人に使われてもよいように，復号鍵は秘密にしますが暗号化鍵は公開してもかまいません。それで，秘密鍵暗号方式の欠点がカバーされます。現在，一般的には公開鍵暗号方式が使われています。代表的なものに，ＲＳＡがあります。

送信者Ａが受信者Ｂに暗号化した文書を送るときは，次のようになります。

暗号化：ＡはＢの公開鍵で暗号化する。

Ｂの公開鍵は，ＢのＷｅｂページでのＦＯＲＭに内蔵されている。

Ａは，それを意識せずに暗号化して送信できる（のマーク）。

それで，誰でもＢに暗号化した文書を送ることができる。

復号：　Ｂはで復号する。

Ｂ以外の人はこの文書を読むことができない。

公開鍵暗号方式は優れた方式ですが，秘密鍵暗号方式にくらべて暗号化や復号に時間がかかる欠点があり，長い本文は秘密鍵暗号方式にすることが考えられます。それで，通信ごとに秘密鍵暗号方式の共通鍵を，公開かぎを使って暗号化して通信相手に送付する方式があります。これをセション鍵暗号方式といいます。実際の暗号化方式では，これが広く採用されています。

②電子署名と認証

電子メールでは，発信者が本人であるかどうか（なりすましをしているのではないか）を確認することができませんし，後になって，

そのような電子メールを発信した覚えはないと否認されても，対抗する手段がありません。

実社会では，印鑑証明を得た実印を文書に押印して，その実印の印鑑証明書を添付することにより，本人からの文書であることを証明します。その実印の押印が電子署名で，印鑑証明が認証です。

(a) 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は，次のように行います。当然，これらの操作はクリックするだけで行えるようになっています。

送信者Ａは，認証局（ＣＡ）から自分の認証番号を得ておく。

送信者Ａは，その認証番号をＡの秘密鍵で暗号化する。

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。

受信者Ｂは，その認証番号を認証局に問い合わせる。

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；
http://www.meti.go.jp/policy/netsecurity/digitalsign.htm

(b) 電子署名法

電子署名法（電子署名及び認証業務に関する法律，平成１２年５月成立，平成１３年４月施行）により，電子署名が実印と同じ法的効力をもつことが定められました。

③暗号化の標準

(a) 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。

(b) ＳＳＬ

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ます。

(c) 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です。ＳＳＬでは受取側（店舗）でクレジット番号を知ることになりますが，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ます。

（３）セキュリティマネジメント

①セキュリティ対策の基礎

(a) 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。このインテグリティは，完全性，保全性，一貫性など多

様な訳語がありますが，どうも適切なものがなく，専門家は訳さずにインテグリティといっています。

・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。

リスクとインシデント

・脅威（Threat）

情報システムのセキュリティを脅かす原因となるものです。自然災害，機器の故障・誤動作，人間の過失，人間の故意などがあります。

・リスク（Risk）

学問的には，「何らかの事態が起こることに関する不確実性」のことをリスクといいますが，ここでは脅威と同義語としてもかまいません。

・インシデント（Incident）

実際に脅威が発生して実際に事件が生じている状態のことをインシデントといいます。

・リスクの大きさ

リスクの大きさ＝発生確率（リスクがインシデントになる確率）

×被害の額（インシデントになったときの損失）

・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（ぜいじゃくせい）といいます。情報セキュリティ対策とは，情報システムでのインシデントを減少させることです。ところが，脅威の存在自体をなくしたり，脅威の発生を減らしたりすることは

困難です。脅威が発生してもインシデントにならないようにするには，リスクを減らすことが必要です。そして，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です。

すなわち，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により，情報システムの脆弱性を減らすことだといえます。

■情報システム安全対策基準；

http://www.jipdec.jp/security/guideline/security-std.html

経済産業省告示「情報システム安全対策基準」（平成７年８月制定）は，「情報システムの機密性，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，故意・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ため，情報システムの利用者が実施する対策項目を列挙したもの」ですが，これが情報セキュリティ対策の定義であるといえます。

②個人情報保護法

■個人情報保護法；

http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/

リスクの大きな分野に，個人情報の漏洩があります。**個人情報保護法（個人情報の保護に関する法律，平成 15 年 5 月成立，平成１７年４月全面施行）**の目的は次の通りです。

「この法律は，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を目的とする。」

そして，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を個人情報データベース等といい，個人情報データベース等を事業の用に供しており，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て，個人情報の保護義務を定めています。

なお，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にプライバシーマーク制度があります。

③セキュリティマネジメント

(a) リスク対策の手順

・情報資産の調査（何を守るのか）

単に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が必要です。

また，すべての情報資産を完全に守るのは非現実的です。優先順位をつける必要があります。情報システム安全対策基準では，次のように重要度を定めています。

A 人命，他人の財産，プライバシー等社会に影響を与える情報システム

B 企業への影響の大きい情報システム

C 企業への影響の小さい情報システム

・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です。

・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します。

・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します。

⑹ 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です。

・成熟度の向上

一挙に理想的な状況にすることはできません。自社の現状を考慮して，逐次的に向上させることが必要です。成熟度として，次の５（６）段階がポピュラです。

（レベル０　Non-Existent（存在しない））

レベル１　Initial（初歩的）

レベル２　Repeatable（繰り返し可能）

レベル３　Defined（定義されている）

レベル４　Managed（管理されている）

レベル５　Optimized（最適化）

・ＰＤＣＡサイクル

ＰＤＣＡとは，Plan（計画）→Do（実行）→Check（確認）→Action（是正）のことです。これを適切にまわすことにより，成熟度が向上します。

・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です。

・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です。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です。

通常は，ウイルス対策ガイドラインとかパソコン利用規程など，ガイドラインや規程の形式になります。内容は，「利用者はパスワード秘守をしなければならない」といったレベルの記述になります。

・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です。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ます。通常は手引書とかマニュアルのような形式になる。　内容は「パスワードは８文字以上で，かならず特殊文字を２文字以上いれること」とか「月１回あるいはアクセス回数が１００回以上になったときはパスワードを変更すること」などの記述になります。

・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ります。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ります。

本時の重要事項

１．不正アクセス禁止法（不正アクセス行為の禁止等に関する法律，平成１１年８月成立，平成１２年２月施行）では，ネットワークを通して

許可されていない者がなりすましをしてアクセスすること

許可されている者が許可されていないアクセスをすること

そのようなアクセスができるような状態にすること

を不正アクセスと定義しています。

２．リスクの大きな分野に，個人情報の漏洩があります。個人情報保護法（個人情報の保護に関する法律，平成 15 年 5 月成立，平成１７年４月全面施行）の目的は次の通りです。

「この法律は，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を目的とする。」