情報セキュリティ講習 資料

中小企業に求められる 情報セキュリティの基礎知識

～情報セキュリティの基礎知識と
中小企業に最低限求められる情報セキュリティ対策について～

2009-07-16
（15：00～16：40）

株式会社 横浜ITサポート (http://www.y-its.jp)

代表取締役　小杉 史郎 (skosugi@y-its.jp)

目次

1. 情報セキュリティの基礎
2. 情報資産と脅威、脆弱性の事例
3. 最低限必要な情報セキュリティ対策

   5分でできる！中小企業のための情報セキュリティ自社診断（IPA）より

4. 次へのステップ

1．情報セキュリティの基礎

1. 情報セキュリティとは
2. リスクと情報資産・脅威・脆弱性の関係

情報セキュリティとは？と聞かれたらどの様に答えますか。

まずは情報セキュリティに関する基本的な内容と、重要なポイントをみていきます。

1. 情報セキュリティとは

■ 情報資産を守ること
＝情報資産にかかわるリスクを低減すること

情報資産：組織にとって価値のある情報　例：顧客情報、機密情報

例：顧客情報を守る
＝顧客情報が漏えいするリスクや使えなくなるリスクを低減する(対策を施す)

参考

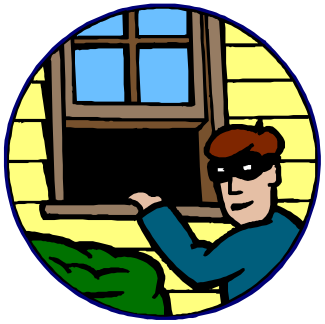
■ 情報セキュリティの定義（ISO/IEC27001等より）
情報の機密性，完全性及び可用性を維持すること

要素	概要	代表的な脅威	代表的な対策
機密性 Confidentiality	必要以外の人にはアクセスさせない	情報漏えい	個人認証 アクセス制御
完全性 Integrity	情報資産の完全さ正確さの保護	改ざん	データ認証
可用性 Availability	必要なとき確実に使えるようにする	障害	二重化 バックアップ

※これらの頭文字をとり、情報セキュリティのCIAとも呼ばれている

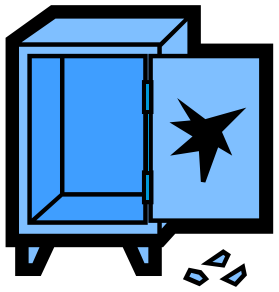
2. リスクと情報資産と脅威・脆弱性の関係

泥棒



壊れたドア

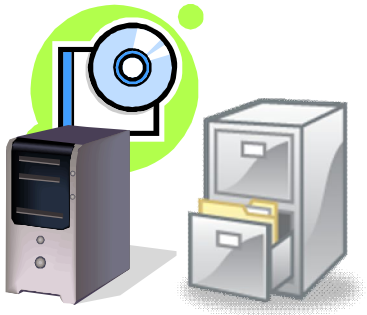
お金



脅威

脆弱性

資産



クラッカー
（コンピュータウイルス等）

災害・障害

・誰でも重要ファイルにアクセスできる
・ウイルス対策ソフトの未導入
・セキュリティホールの放置
・バックアップが無い　など

機密情報

個人情報　など

2. リスクと情報資産と脅威・脆弱性の関係

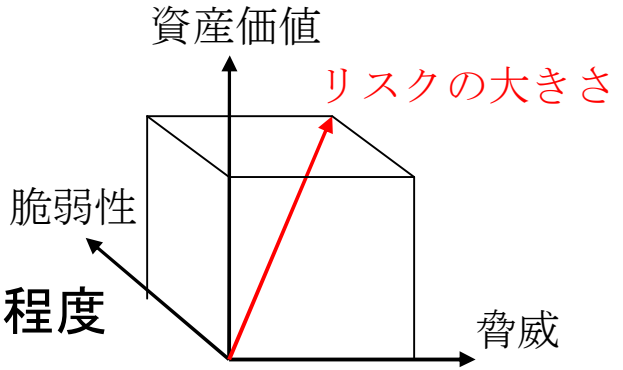
■ 情報資産，脅威，脆弱性の関係を言葉にすると

- 情報資産は、不正なアクセスやウイルス感染のような脅威にさらされている。
- 情報資産は一応は守られていても、どこか弱い点（脆弱性）を内在している。
- 脆弱性を突かれ、脅威が顕在化したとき、事件・事故（インシデント）が発生する。

■ リスクとは

- 脅威が顕在化する可能性
- リスクの大きさ＝

一般的に 資産の価値 × 脅威の程度 × 脆弱性の程度



参考 リスクの大きさ＝被害が発生した時の損失（金額）× 発生確率（頻度）
という表現もある

2. 情報資産と脅威、脆弱性の事例

1. 情報資産の例
2. 情報資産の考え方
3. 脅威の例
4. 脅威の最新事例（IPA 2009年 10大脅威より）
5. 脆弱性の例

注）IPA＝独立行政法人 情報処理推進機構

情報セキュリティとは情報資産を守ること、情報資産に係るリスクを低減することで、リスクは下記のように表現されました。

リスクの大きさ＝情報資産価値×脅威×脆弱性

ここでは、リスクを構成する、情報資産、脅威、脆弱性について一歩踏み込んで考えてみます。

1. 情報資産の例

- 情報資産とは：組織にとって価値のある情報
  （この「情報」を管理するシステム、機器なども含む）

参考

区分	例
情報	データベース及びデータファイル、システムに関する文書、ユーザマニュアル、訓練資料、操作または支援手順、継続計画、代替手順の手配、記録保管された情報
ソフトウエア	業務用ソフトウエア、システムソフトウエア、開発用ツール及びユーティリティ
ハードウエア	コンピュータ装置（プロセッサ、表示装置、ラップトップ、モデム）、通信装置（ルータ、PBX、ファクシミリ、留守番電話）、磁気媒体（テープ及びディスク）、その他の技術装置（電源、空調装置）、什器、旧称設備
サービス	計算処理及び通信サービス、一般ユーティリティ（例えば、暖房、証明、電源、空調）
人	関連する要員など

2. 情報資産の考え方

■ 一般的に言われる情報資産

組織にとって価値のある情報　　会社目線

・**顧客情報**：**顧客の個人的な情報**

顧客の趣味、趣向、クレジットカード番号、（住所、電話番号）

・**機密情報**（**組織の外部に知られると営業に差し障るようなマル秘情報**）

組織の経営計画、決算情報（発表前）

しかし今では、被害者からの目線が重視

■ 情報資産の価値を相手目線で考える：

情報セキュリティの３大要素（機密性・完全性・可用性）について検討

1. （**機密性**）もしも、私の（会社の）情報が漏えいしたら
2. （**完全性**）もしも、私の（会社の）情報が改ざんされたら
3. （**可用性**）もしも、私の（会社の）情報が利用できなくなったら

2. 情報資産の考え方

1. もしも、私の（会社の、顧客の）情報が漏えいしたら

   個人・顧客情報

   - 個人・顧客の情報は「預かっている情報」という考え方
   - 漏えいすると、個人情報保護法 安全管理義務違反となる
     ⇒情報漏えい時には届出義務がある
   - たとえ、情報自体にあまり価値が無くても、個人・組織名が漏えいすると、会社の信用問題に繋がる
     ⇒この会社は大丈夫？ 他の情報も漏えいしてるのでは・・・

   参照：Security Nextサイト

   機密情報

   - 顧客から入手した情報（図面情報等）
   - 製品の原価、仕切り額、取引実績
   - 社内の人事・給与・経理情報（社員の個人情報）

2. もしも、私の（会社の）情報が改ざんされたら

   - 誤って書き換えてしまったら
   - 他の情報と混ざってしまったら

   ・・・・・

   あまり改ざんされることは想定できなくても・・・

3. もしも、私の（会社の）情報が利用できなくなったら

   - PC、ファイルサーバが故障したら

     自分が作成していた報告書データファイル

     ・・・・・

3. 脅威の例

■ 脅威の分類と例 参考

大区分	区分	例	対策
人為的脅威	意図的脅威（外部･内部） 攻撃 内部犯行	コンピュータウイルス、不正侵入、改ざん、なりすまし 盗難、盗聴　など	(各種)技術的対策 (各種)物理的対策
	偶発的脅威	人為的（設定、運用、削除、廃棄、置き忘れ 等）ミス、誤動作 装置（PC、ネットワーク、ソフトウェア、電源 等）故障 など	教育、手順書作成 二重化、ﾊﾞｯｸｱｯﾌﾟ
環境的脅威	（自然） （環境）	地震、洪水、地すべり、落雷 停電、火災、静電気、汚染 など	(予防)物理的対策 (復旧)BCP ※

※BCP（Business Continuity Plan ）：事業継続計画

- 人為的 意図的脅威が社会問題になっている
- 脅威と脆弱性（情報資産に内在する弱点）は表裏一体の関係

4. 脅威の最新事例（IPA 2009年 10大脅威より）

毎年、IPAが有識者と話し合い、
その年の主となる脅威をピックアップ

■ 10大脅威 攻撃手法の『多様化』が進む

– 組織への脅威

第1位 DNSキャッシュポイズニングの脅威
第2位 巧妙化する標的型攻撃
第3位 恒常化する情報漏えい

– 利用者への脅威

第1位 多様化するウイルスやボットの感染経路
第2位 脆弱な無線LAN暗号方式における脅威
第3位 減らないスパムメール
第4位 ユーザIDとパスワードの使いまわしによる危険性

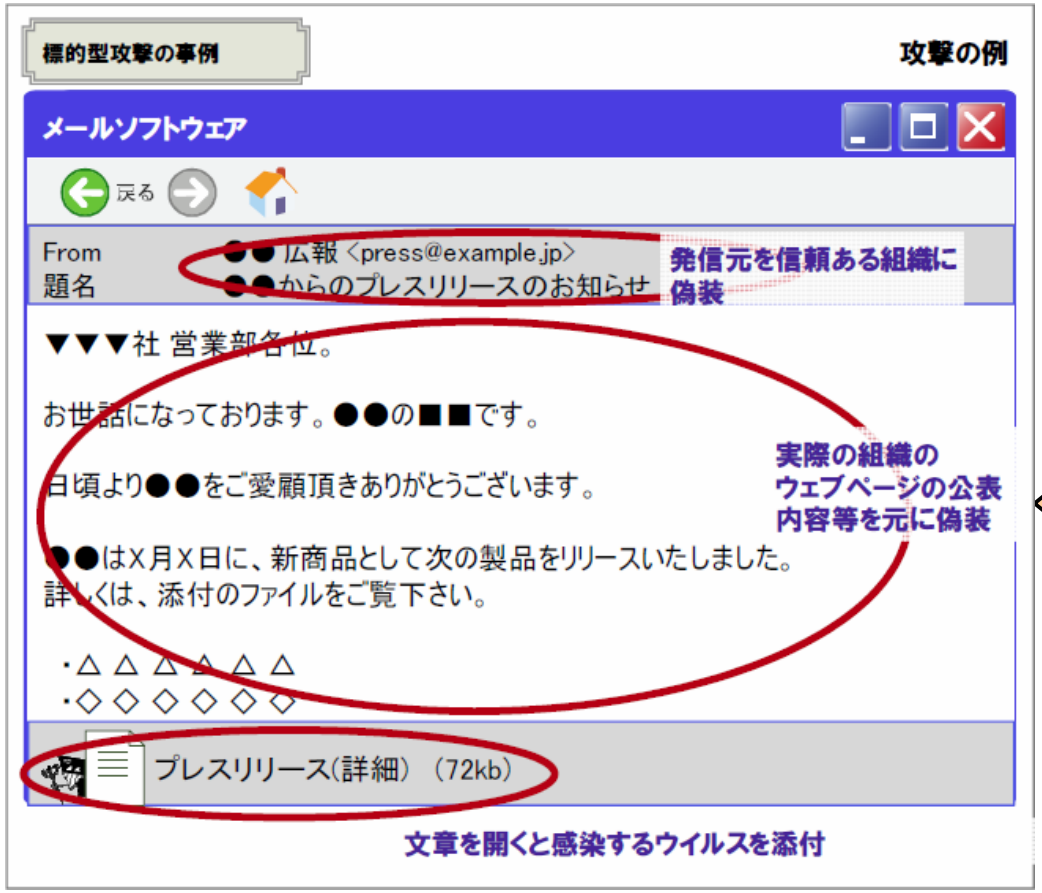
– システム管理者・開発者への脅威

第1位 正規のウェブサイトを経由した攻撃の猛威
第2位 誘導型攻撃の顕在化
第3位 組込み製品に潜む脆弱性

出典：http://www.ipa.go.jp/security/vuln/10threats2009.html

4. 脅威の最新事例（IPA 2009年 10大脅威より）

1. 巧妙化する標的型攻撃



今までの攻撃方法
不特定多数を狙う

最近増えてきた攻撃方法
特定の相手を狙う

特定の相手から情報搾取・脅迫 等
お金を稼ぐための攻撃も

・一部でしか使われないウィルスはウィルス対策ソフトで対応できない
・相手がついつい信じてしまい、被害に合う

出典：http://www.ipa.go.jp/security/vuln/documents/10threats2009.pdf

参考）標的型攻撃の例

- 事例）IPAを名乗ったウィルス添付メール

  2008年4月16日 何者かがIPAの名を語って（IPA実在のメールアドレス）ウィルス入りPDFファイル添付メールを送信
  宛先不明のエラーメールでIPAに返送されてきて発覚
  - メールの件名：セキュリティ調査報告
  - メール文面：IPAウェッブサイトのページ内容をコピー　　添付ファイル名：調査報告書.pdf

  – 対策
  - メール以外の通信手順を併用、送信者の詐称を防ぐ（電子署名、送信ドメイン検証）
  - 予防接種（イノキュレーション）の検討　　横浜市役所 事例

既存の攻撃の中にも

- **フィッシング（Phishing）**：相手をだまして情報を詐取する詐欺
  - 標的型例）銀行からのお知らせメールだと思い、リンク先をクリック。誘導されたサイトで、ID、パスワードを入力してしまう　⇒ID、パスワードを盗まれる

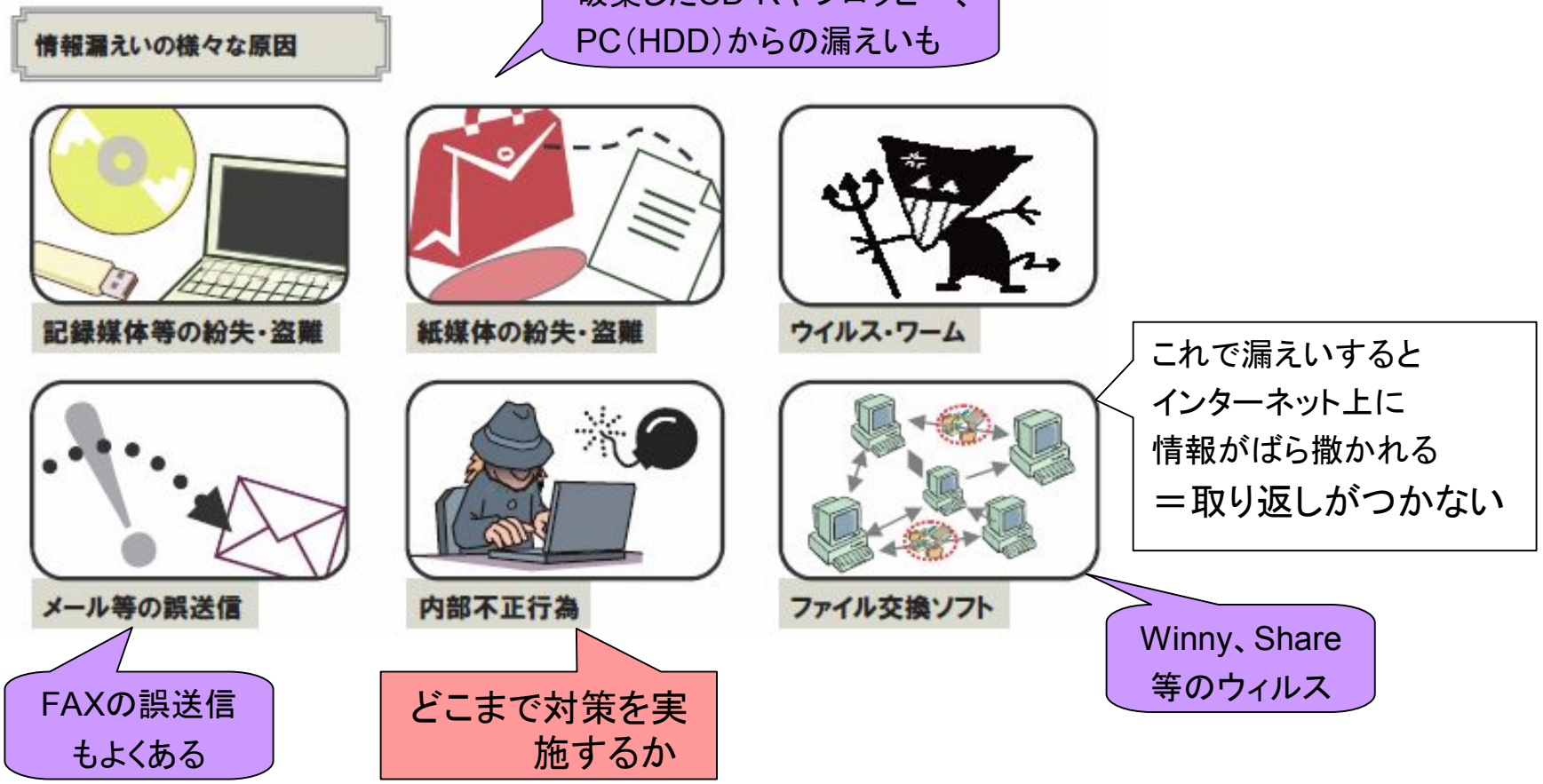
- **スパイウェア**：こっそりとPCに忍び込み、スパイ活動を行なう
  - 標的型例）銀行からCD-ROMが送られてきたので、インストールしたら、それ以降のキー操作がすべて記録されていた　⇒ID、パスワードを盗まれる

- **ソーシャル・エンジニアリング**：「社会的」な手段によって秘密情報を入手する
  - 標的型例）上司やシステム管理者などになりすまして、パスワードや個人情報を聞き出す

  ⇒**振り込め詐欺**も同様　ワンクリック詐欺なども

4. 脅威の最新事例(IPA 2009年 10大脅威より)

2. 恒常化する情報漏えい

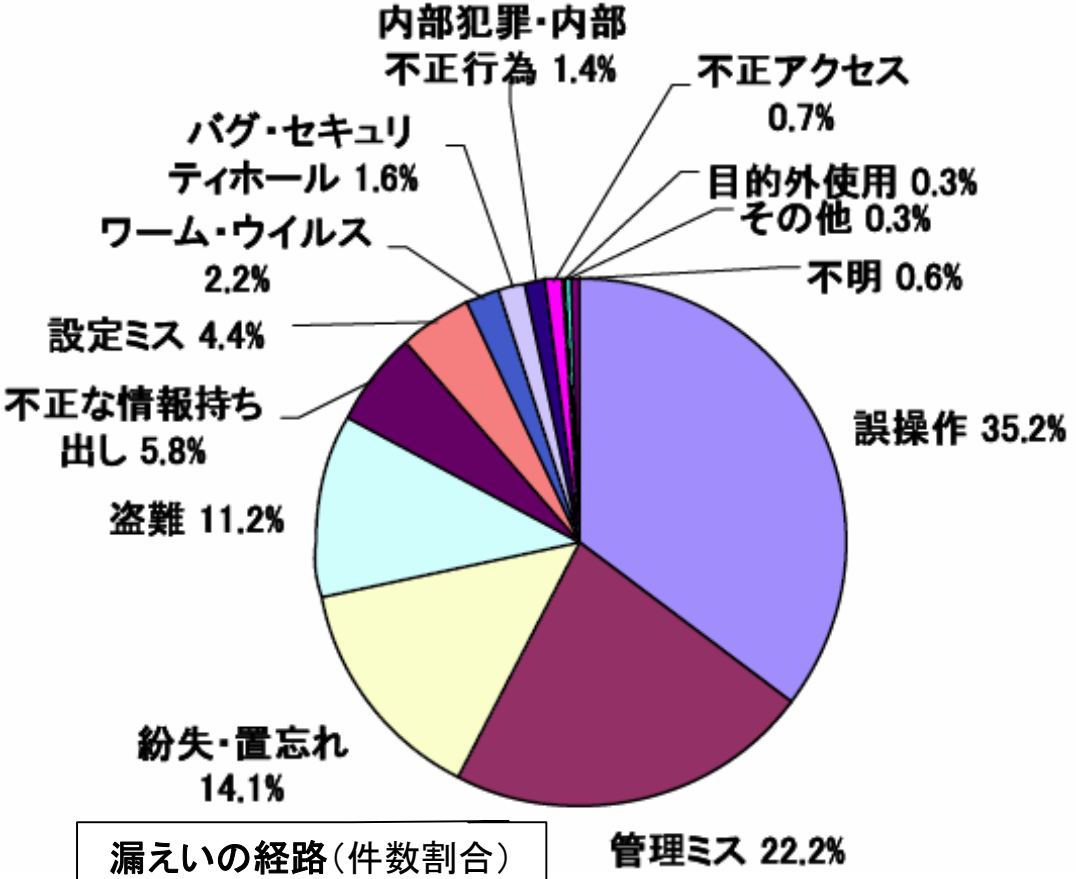


出典:http://www.ipa.go.jp/security/vuln/10threats2009.html

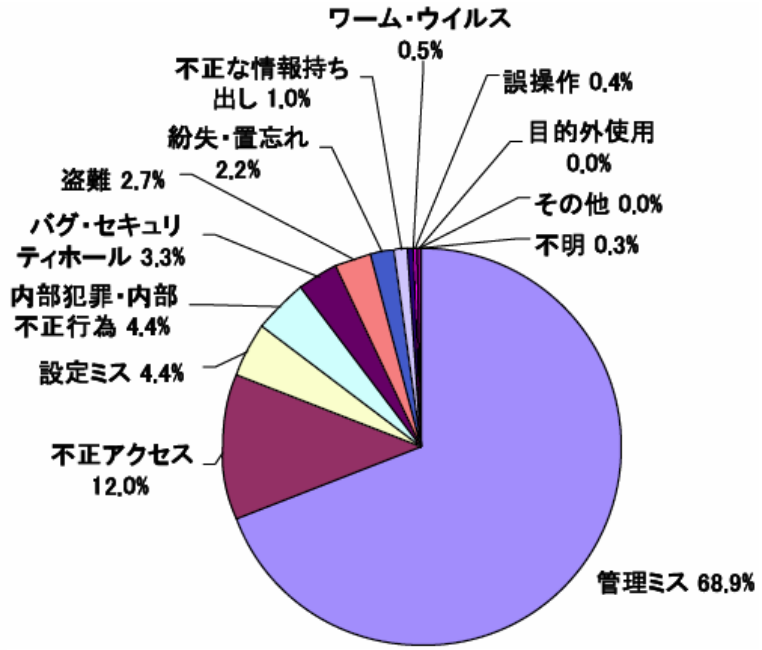
参考）情報漏えいの原因

漏えいの経路（人数割合）
紙媒体：59.5%
Web/Net：24.9%
USB等可搬記録媒体：10.5%

■漏えいの原因（件数割合）



漏えいの経路（件数割合）
紙媒体：56.0%
Web/Net：11.7%
PC本体：7.3%



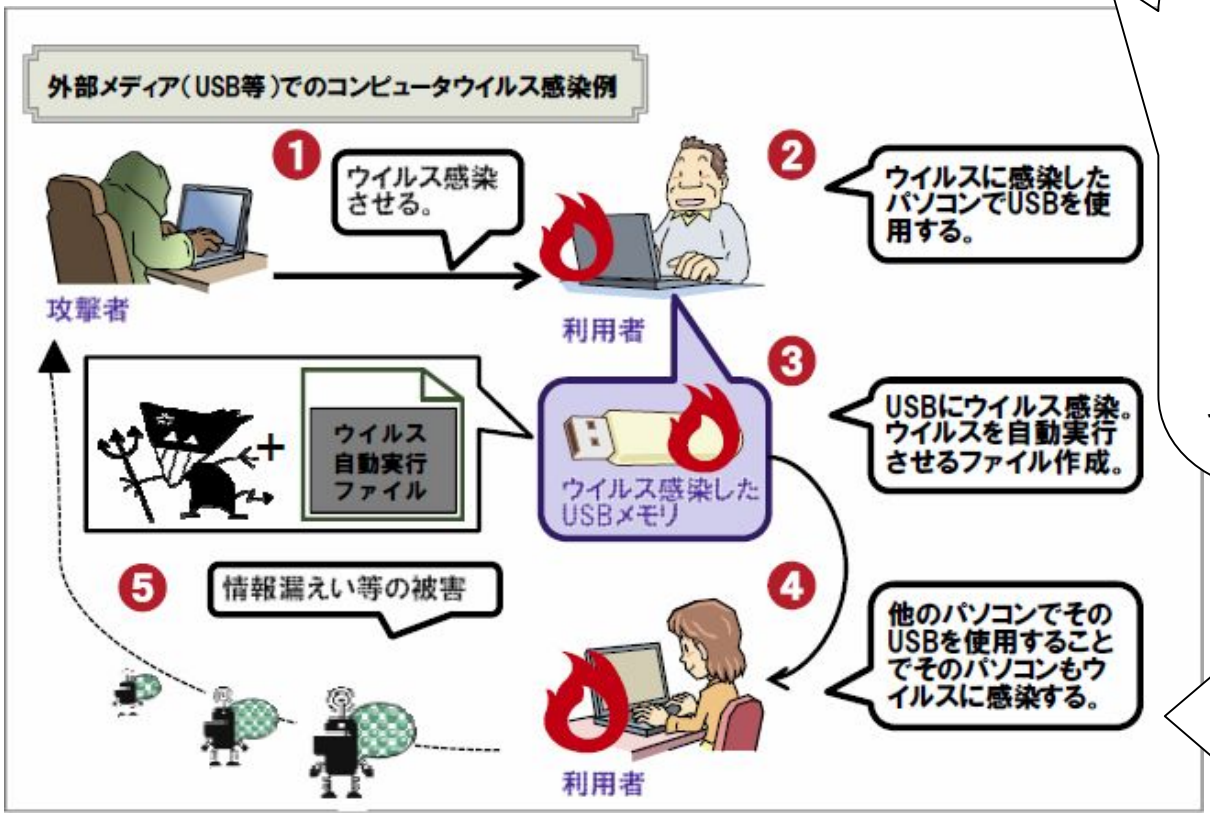
参考）漏えいの原因
（漏えい人数での割合）

INSA「2008年 情報セキュリティインシデン
-に関する調査報告書」2009
ttp://www.jnsa.org/result/2008/surv/inci
dent/2008incidentsurvey_v1.0.pdf

参照：Security Nextサイト

4．脅威の最新事例（IPA 2009年 10大脅威より）

3．多様化するウイルスやボットの感染経路



ボット：ウィルスの一種で、悪意を持った第三者が外部からコンピュータを操ることを目的として作成されたプログラム

ボットに感染すると情報漏えい、迷惑メールやDos攻撃の発信元となる

⇒被害者にも加害者にもなってしまう

見た目や体感速度では気が付かない

攻撃者がこっそり利用している

<u>少し前のウィルス感染</u>

PCが起動しない、遅くなる 等

ネットワークを介さない

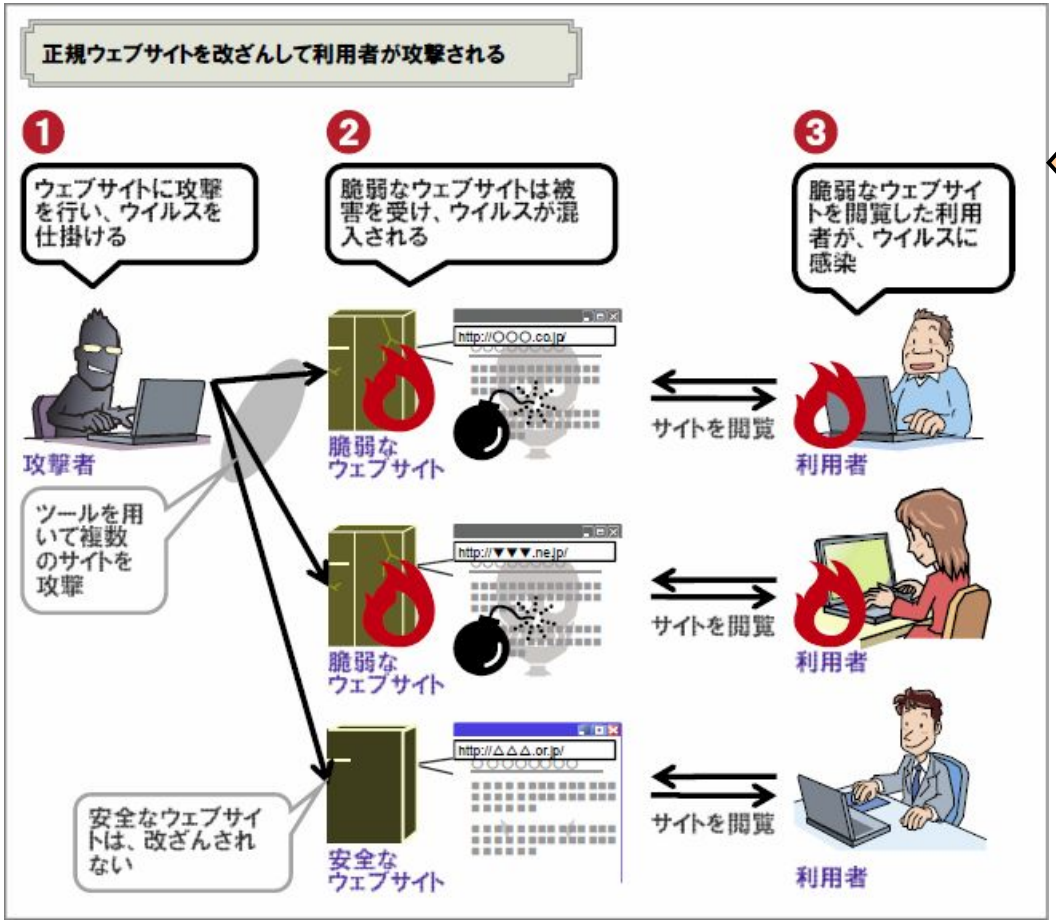
USBメモリを繋ぐだけで感染

Conficker ワーム等

出典：http://www.ipa.go.jp/security/vuln/10threats2009.html

4. 脅威の最新事例(IPA 2009年 10大脅威より)

4. 正規のウェブサイトを経由した攻撃の猛威



Web作成時の脆弱性の問題で
サイト利用者が攻撃を受ける

全攻撃に対するウェブサイト攻撃の割合(Lac社調査)
2006年 53% → 2008年 95%

よく見るサイトや検索エンジンで検索したサイトを見るだけでも感染する恐れがある

出典:http://www.ipa.go.jp/security/vuln/10threats2009.html

参考)価格コム 不正侵入(2005. 05)

- 不正アクセスにより、価格コムサイトにウィルスが仕掛けられる
  （トレンドマイクロ製ウィルス対策ソフトが正常に稼働していなかった？）
  - サーバ内のメールアドレス数万件抜き取られる
  - 同時にサイトにウィルスが埋め込まれる
- 価格コムを閲覧した人がウィルスに感染
  （ただし、下記の人は感染しない）
  - ウイルス対策ソフト「NOD32」を導入していた場合
  - 2004年に公開されたセキュリティ更新プログラム「MS04-013」を適用している場合
- 感染すると、
  - キーロガー(キー操作を記録するソフト)を仕掛けられる
  - ゲームサイトのアカウント情報を盗み出す

最近の事例：
2008/09/30 ゴルフダイジェスト･オンライン
2009/04/17 薬事日報ウェブサイト
2009/05/04 財団法人長岡京市体育協会 HP

5. 脆弱性の例

参考

分類	脆弱性の例	関連する脅威
環境、設備	自由に出入りのできる事務所 セキュリティに関心の無い組織	盗難、不正アクセス 様々なセキュリティ事故
ソフトウエア	作成ミスのあるソフトウエア アクセス制御のないPC	ウィルス感染 不正アクセス、なりすまし、改ざん
ハードウエア	持ち出せるノートPC 老朽化したファイルサーバ	盗難、置き忘れ、情報漏洩 故障(データ破壊)
人	うっかりミス 出来心、好奇心	情報漏えい、データ破壊 情報漏えい(内部犯行)、不正アクセス

- 脆弱性は、脅威の発生を誘引する原因のひとつ
- 脅威と脆弱性(情報資産に内在する弱点)は表裏一体の関係

5. 脆弱性の例（人の脆弱性について）

- セキュリティ対策における性善説と性悪説
  - 「内部犯行」を考えると、性悪説？

内部犯行に完全に対応しようとすると、
あらゆるセキュリティ対策が必要になる

- 見方を変えて→性弱説？
  - 人は間違えやすい生き物：うっかりミス
    - USBメモリをなくした
    - メールを間違えて他の顧客に送った
    - 間違えてファイルを消した

教育・規定
手順書（ミスの起こりにくい仕組み）

  - 人は弱い生き物：出来心、好奇心
    - 顧客情報が誰でも見えるフォルダーに置いてあった。私には関係ないが、面白そうなので一応コピーしておこう。
    - 来月末には退社することが決まりそうだ。何かの役に立つかも知れないから、共有フォルダのファイルをコピーして持ち帰ろう。

教育・規定（罰則含む）
出来心を起こさせない運用：内部統制

- 人の脆弱性をフォローする技術的なセキュリティ対策の必要性
  - ルールだけのセキュリティ対策では、人の脆弱性の対策が取れない
  - しかし、技術的なセキュリティ対策はコストが掛かる←バランスが必要

３．最低限必要な情報セキュリティ対策

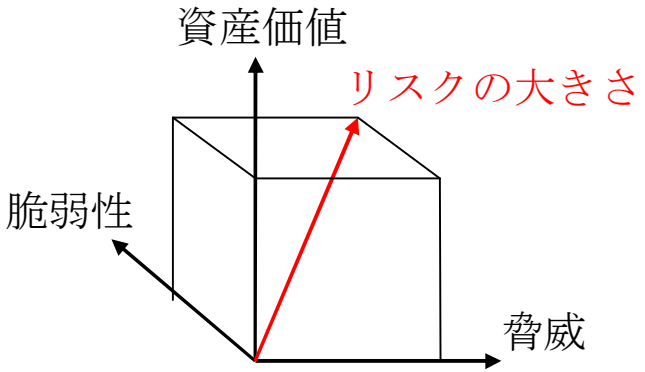
1. 情報セキュリティ対策とは
2. 最低限必要な情報セキュリティ対策
   5分でできる！中小企業のための情報セキュリティ自社診断（IPA）より
3. 情報セキュリティ対策のポイント
4. 具体的な技術的対策事例

セキュリティ対策にはその対象、レベルによりさまざまなものがあります。

ここでは、IPAが提示している「５分でできる！中小企業のための情報セキュリティ自社診断」より、最低限実施すべきセキュリティ対策をみてみます。

1. 情報セキュリティ対策とは

■ 情報セキュリティとは
　情報資産を守る⇒リスクを低減する
　リスクの大きさ＝
減らせない 資産価値×脅威×脆弱性
　⇒脆弱性を減らすとリスクが減る



■ リスクを減らす⇒脆弱性を減らす⇒情報セキュリティ対策

分類例
- 技術的な対策：ウイルス対策、アクセス制御 等
- 物理的な対策：機器の二重化、入退出管理 等
- 人・管理的な対策：規程を作成、教育、罰則 等

■ 参考）セキュリティ対策（脆弱性低減）以外でリスクを減らす対応
- リスク回避：情報資産を破棄 等
- リスク保有：問題が起きたらそのとき対処（その時のために資金を用意）
- リスク移転：保険に入る、アウトソーシング？ 等

業務は委託出来ても
責任は委託出来ない

2. 最低限必要な情報セキュリティ対策

IPA　5分でできる！

IPAは今後内容を追加していく予定

中小企業のための情報セキュリティ自社診断

- 対象：

  情報システム責任者を置けないまたは兼任となる組織

  経営資源が限られるため、対策費用はあまり掛けられない組織

参考 • 対策の前提

  代表者（経営者）が対策方針を直接指示・確認することができる

  社員全員が顔見知りである

  社内に複雑な設定を必要とするサーバやネットワーク機器が無い

– 自社診断シートの質問25題に回答をチェック

⇒得点による診断

自社診断シート：http://www.ipa.go.jp/security/manager/know/sme-guide/pdf/sheet_5min.pdf

– パンフレットに各質問のやさしい解説

パンフレット（解説）：http://www.ipa.go.jp/security/manager/know/sme-guide/pdf/pamphlet_5min.pdf

2.1. 情報のライフサイクルにおける対策

1. 保管について

重要情報を机の上に放置せず鍵付き書庫に保管し施錠するなどのように、重要情報がみだりに扱われないようにしていますか？

2．持ち出しについて

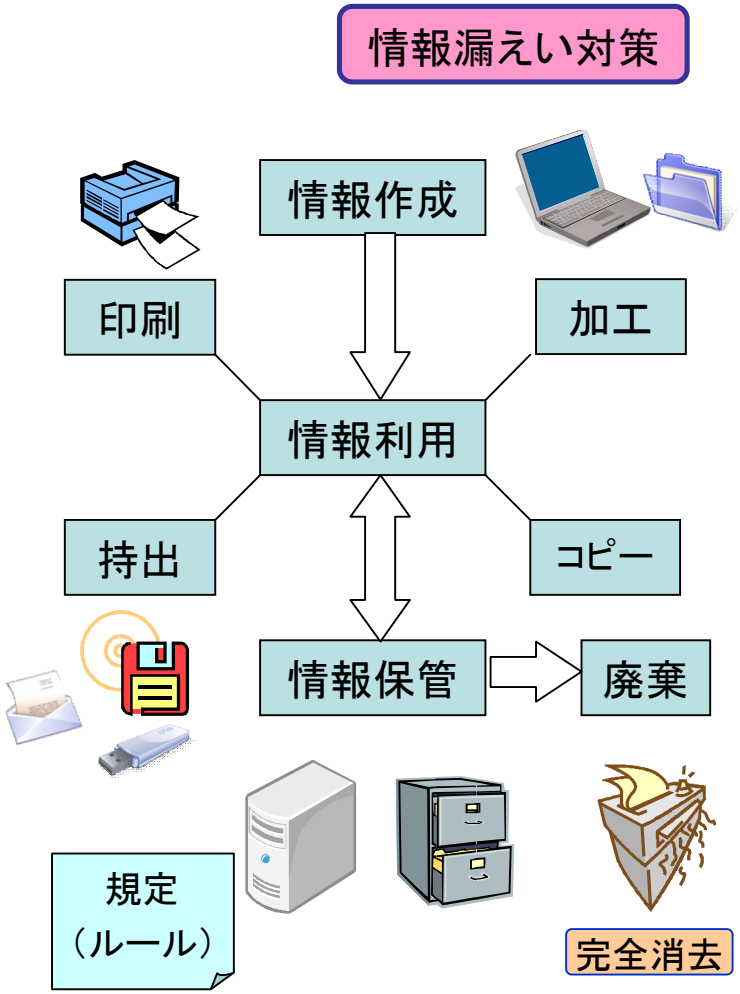
重要情報を社外へ持ち出す時はパスワードロックをかけるなどのように、盗難・紛失対策をしていますか？

3．廃棄について1

重要な書類やCDなどを廃棄する場合は、シュレッダーで裁断するなどのように、重要情報が読めなくなるような処分をしていますか？

4．廃棄について2

重要情報の入ったパソコン・記憶媒体を廃棄する場合は、消去ソフトを利用したり、業者に消去を依頼するなどのように、電子データが読めなくなるような処理をしていますか？



出典）http://www.ipa.go.jp/security/manager/know/sme-guide/pdf/sheet_5min.pdf

2.2. 物理的な対策

5．事務所について1

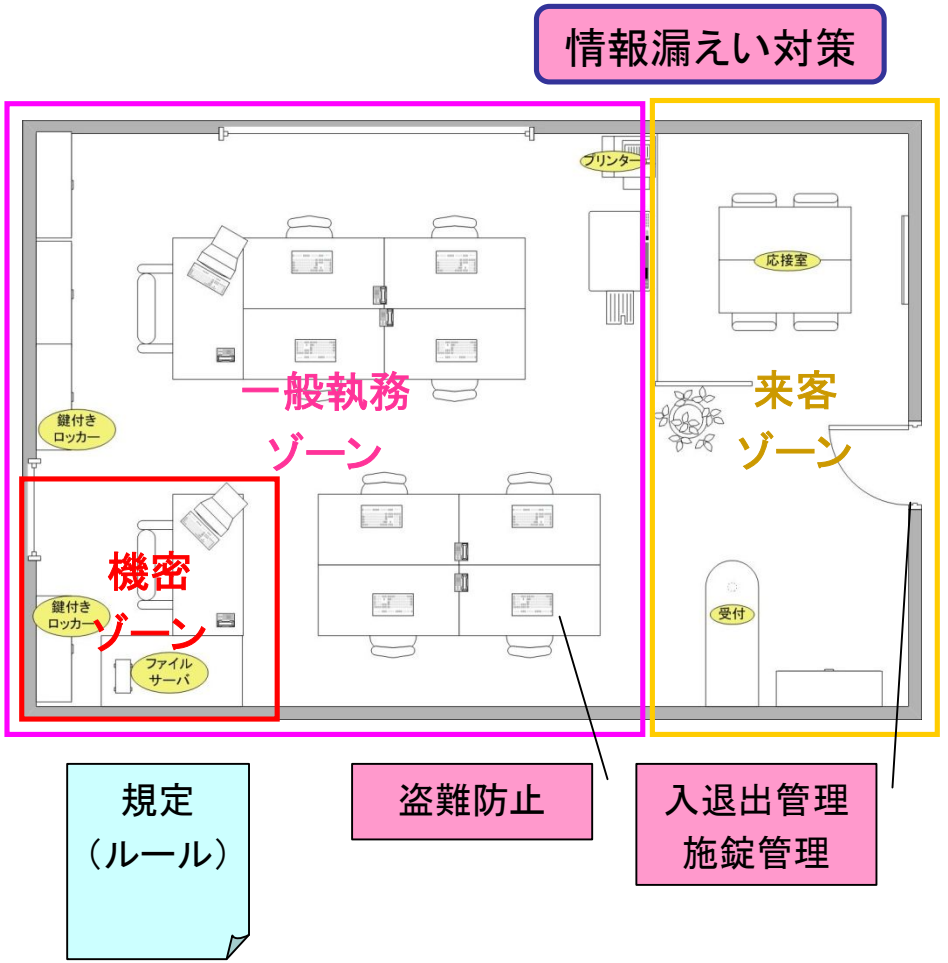
事務所で見知らぬ人を見かけたら声をかけるなどのように、無許可の人の立ち入りがないようにしていますか？

6．事務所について2

ノートパソコン利用者は、退社時に、机の上のノートパソコンを引き出しに片付けるなどのように、盗難防止対策をしていますか？

7．事務所について3

最終退出者は事務所を施錠し退出の記録（日時、退出者）を残すなどのように、事務所の施錠を管理していますか？



出典）http://www.ipa.go.jp/security/manager/know/sme-guide/pdf/sheet_5min.pdf

2.3. パソコンの対策

8．パソコンについて1　ウィルス対策

Windows Updateを行うなどのように、常にソフトウェアを安全な状態にしていますか？

9．パソコンについて2　漏えい対策

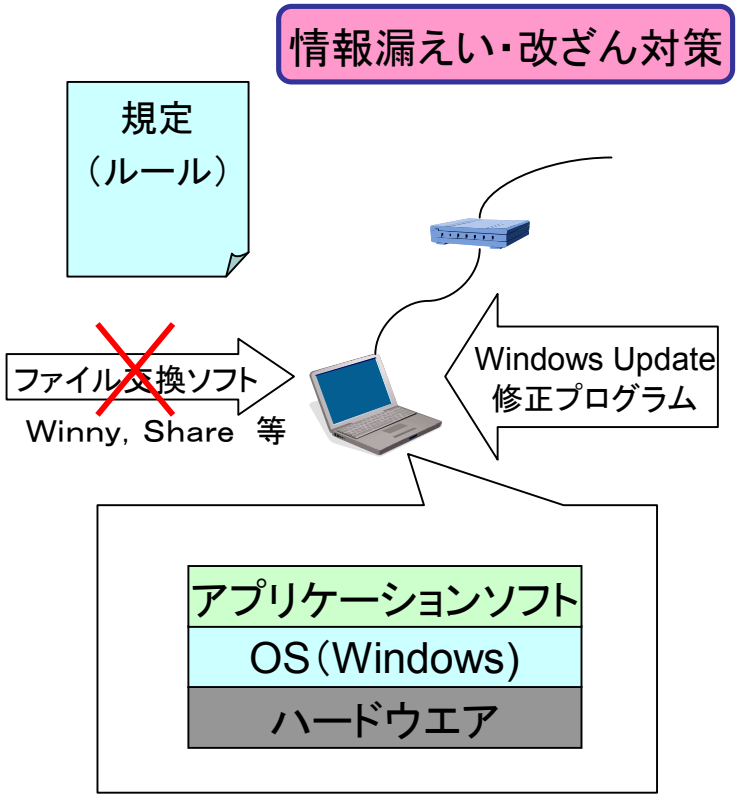
ファイル交換ソフトを入れないようにするなどのように、ファイルが流出する危険性が高いソフトウェアの使用を禁止していますか？

10．パソコンについて3

社内外での個人パソコンの業務使用を許可制にするなどのように、業務で個人パソコンを使用することの是非を明確にしていますか？

11．パソコンについて4

退社時にパソコンの電源を落とすなどのように、他人に使われないようにしていますか？



出典）http://www.ipa.go.jp/security/manager/know/sme-guide/pdf/sheet_5min.pdf

2.4. パスワードの管理

12．パスワードについて1

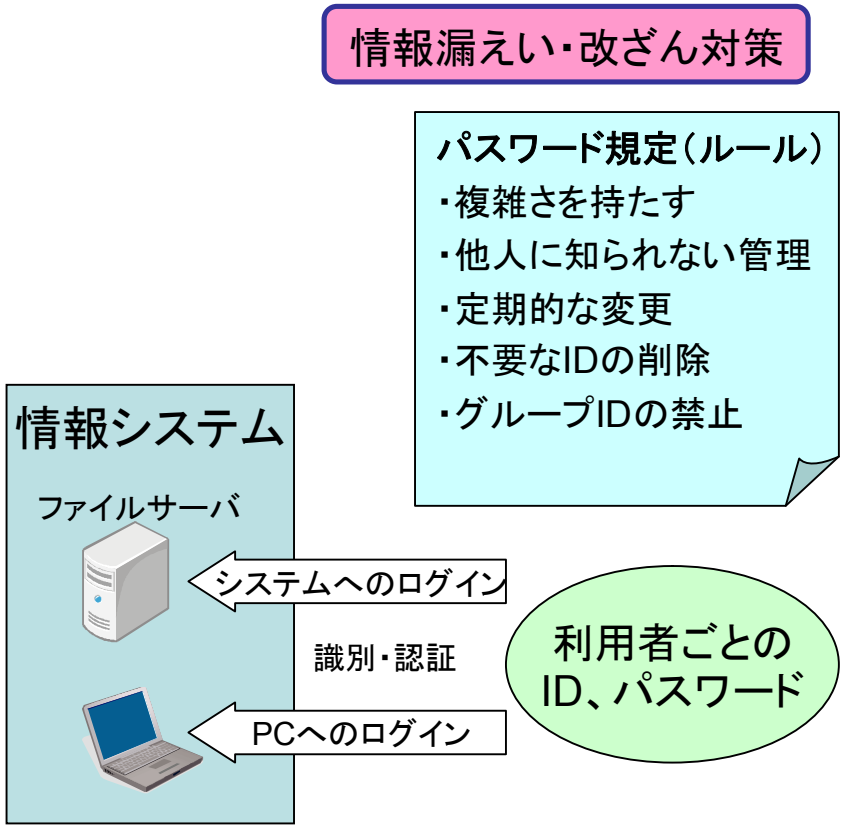
パスワードは自分の名前を避けるなどのように、他人に推測されにくいものに設定していますか？

13．パスワードについて2

パスワードを他人が見えるような場所に貼らないなどのように、他人にわからないように管理していますか？

14．パスワードについて3

ログイン用のパスワードを定期的に変更するなどのように、他人に見破られにくくしていますか？



参考）強力なパスワードの作り方（＋パスワードチェッカー）
http://www.microsoft.com/japan/athome/security/privacy/password.mspx

出典）http://www.ipa.go.jp/security/manager/know/sme-guide/pdf/sheet_5min.pdf

2.5. ウィルス対策とバックアップ

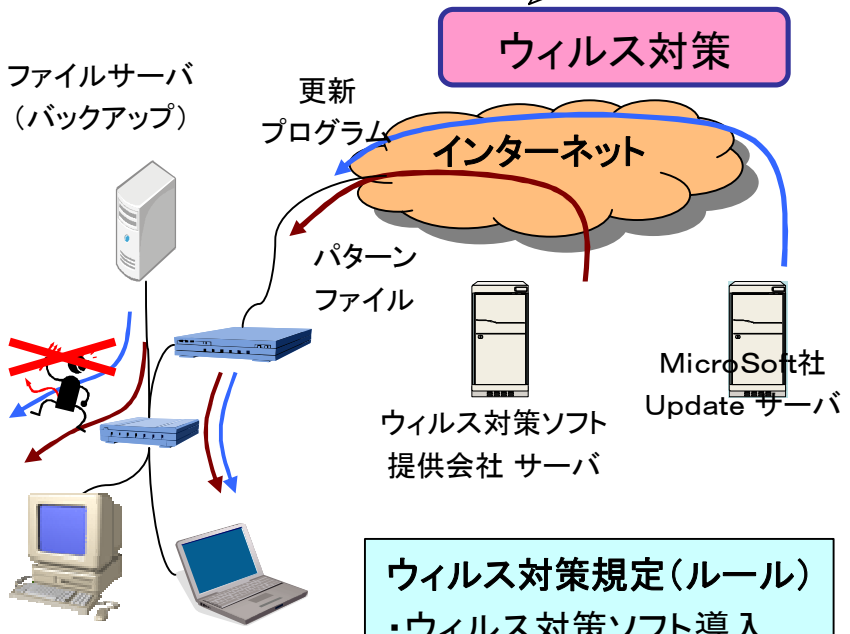
情報漏えい対策
障害対策

15．ウイルス対策について1

パソコンにはウイルス対策ソフトを入れるなどのように、怪しいWebサイトや不審なメールを介したウイルスから、パソコンを守るための対策をおこなっていますか？

16．ウイルス対策について2

ウイルス対策ソフトのウイルス定義ファイル（パターンファイル）を自動更新するなどのように、常に最新のウイルス定義ファイルになるようにしていますか？



ウィルス対策規定（ルール）
・ウィルス対策ソフト導入
・パターンファイルの更新
・定期的なウィルス検査

バックアップ規定（ルール）
・重要情報のバックアップ
（自動バックアップ）

20．バックアップについて

障害対策

重要情報のバックアップを定期的に行うなどのように、故障や誤操作などに備えて重要情報が消失しないような対策をしていますか？

情報が使えなくならないように

出典）http://www.ipa.go.jp/security/manager/know/sme-guide/pdf/sheet_5min.pdf

2.6. メールに関する対策

情報漏えい対策

17．メールについて1

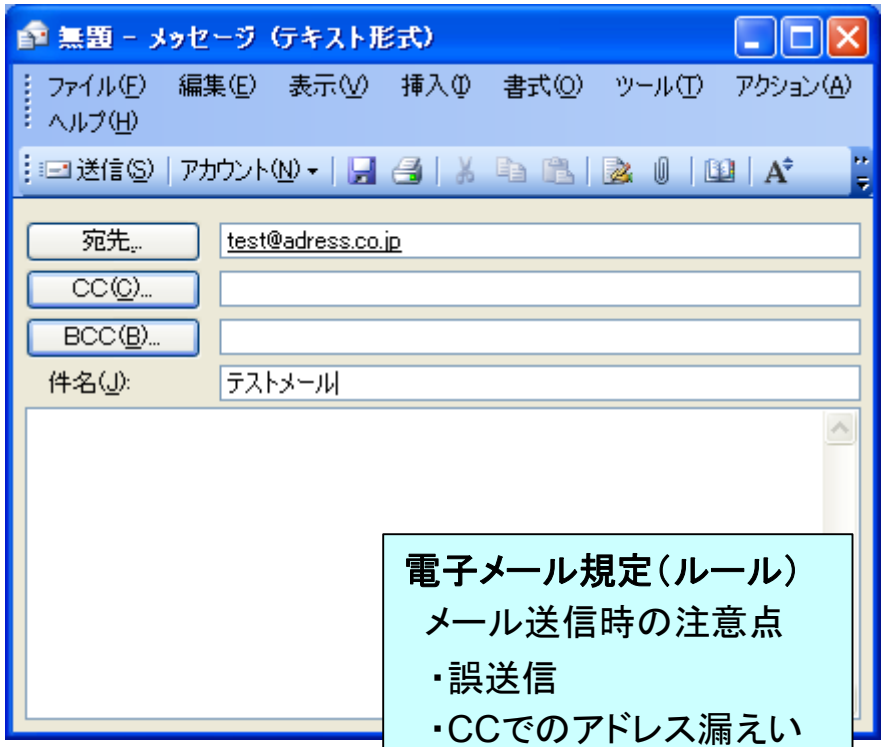
電子メールを送る前に、目視にて送信先アドレスの確認をするなどのように、宛先の送信ミスを防ぐ仕組みを徹底していますか？

18．メールについて2

お互いのメールアドレスを知らない複数人にメールを送る場合は、Bcc機能を活用するなどのように、メールアドレスを誤って他人に伝えてしまわないようにしていますか？

19．メールについて3

重要情報をメールで送る場合は、暗号メールを使うか、重要情報を添付ファイルに書いてパスワード保護するなどのように、重要情報の保護をしていますか？



電子メール規定（ルール）

メール送信時の注意点

- 誤送信
- CCでのアドレス漏えい
- 重要情報の暗号化

出典）http://www.ipa.go.jp/security/manager/know/sme-guide/pdf/sheet_5min.pdf

2.7. 組織的な対策

21．従業者について1

採用の際に守秘義務があることを知らせるなどのように、従業者に機密を守らせていますか？

22．従業者について2

情報管理の大切さなどを定期的に説明するなどのように、従業者に意識付けを行っていますか？

23．取引先について

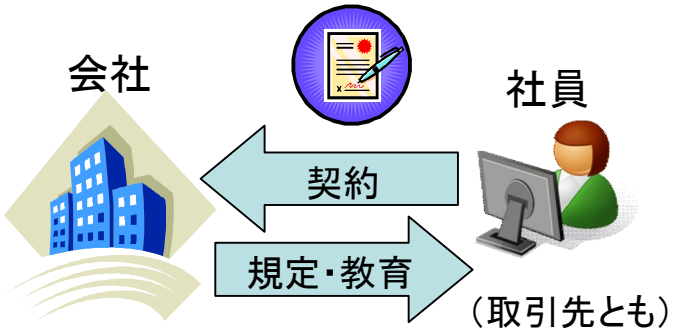
契約書に秘密保持（守秘義務）の項目を盛り込むなどのように、取引先に機密を守ることを求めていますか？

24．事故対応について

重要情報の流出や紛失、盗難があった場合の対応手順書を作成するなどのように、事故が発生した場合に備えた準備をしていますか？

25．ルールについて

情報セキュリティ対策（上記1～24など）を会社のルールにするなどのように、情報セキュリティ対策の内容を明確にしていますか？



各種規定（ルール）

事故対応手順
・情報漏えいが発生したら
・ウィルスに感染したら
・・・・・

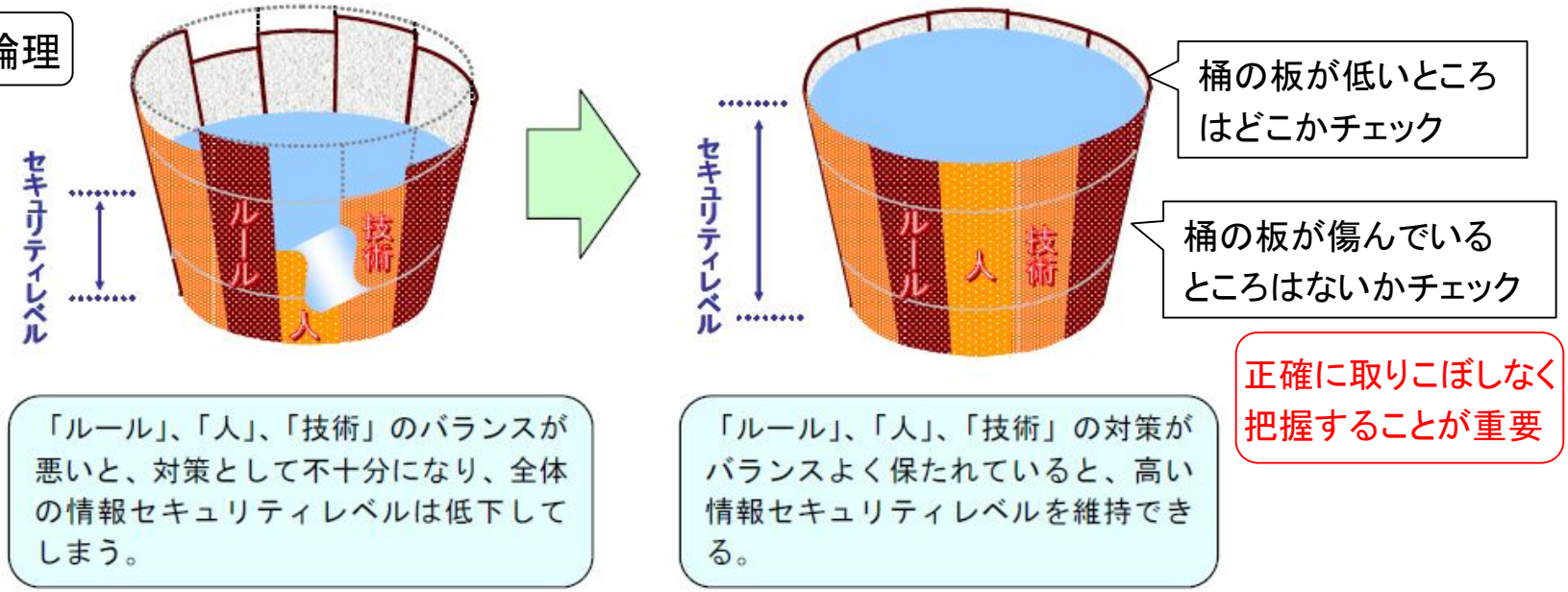
出典）http://www.ipa.go.jp/security/manager/know/sme-guide/pdf/sheet_5min.pdf

3. 情報セキュリティ対策のポイント

■ セキュリティレベルの低い（脆弱性の高い）ところから対応が必要

・バランスが悪い情報セキュリティ対策　　・バランスがとれた情報セキュリティ対策

桶の論理



出展）http://www.soumu.go.jp/joho_tsusin/telework/pdf/060428_g2.pdf

■ 多層防御（Defense In Depth）の必要性

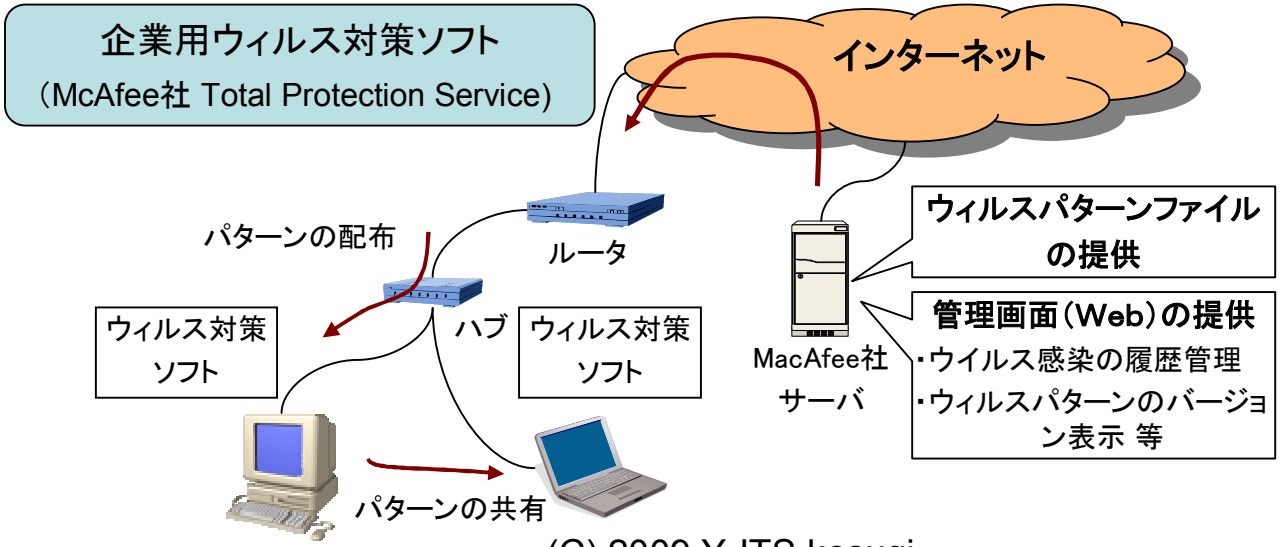
城の構造

何枚もの防衛壁を設置するように、複数のセキュリティ保護対策を組み合わせて実施することが大事（1つで完璧なセキュリティ対策は有りえない）

4．1．企業向け ウィルス対策ソフト

■一元管理が可能なウィルス対策ソフト

- ウイルス対策ソフトの導入状況（パターンファイルのバージョン、検知状況 等）が一元管理可能
- ライセンス購入が可能なため、毎年の更新が楽
- 価格：6千円程度／1台1年　～
  マカフィー社：Total Protection Service
  大塚商会：セキュリティワンコインサービス
  （トレンドマイクロ社：ビジネスセキュリティのASP版）



4．2．ファイル共有：LAN接続型ハードディスク

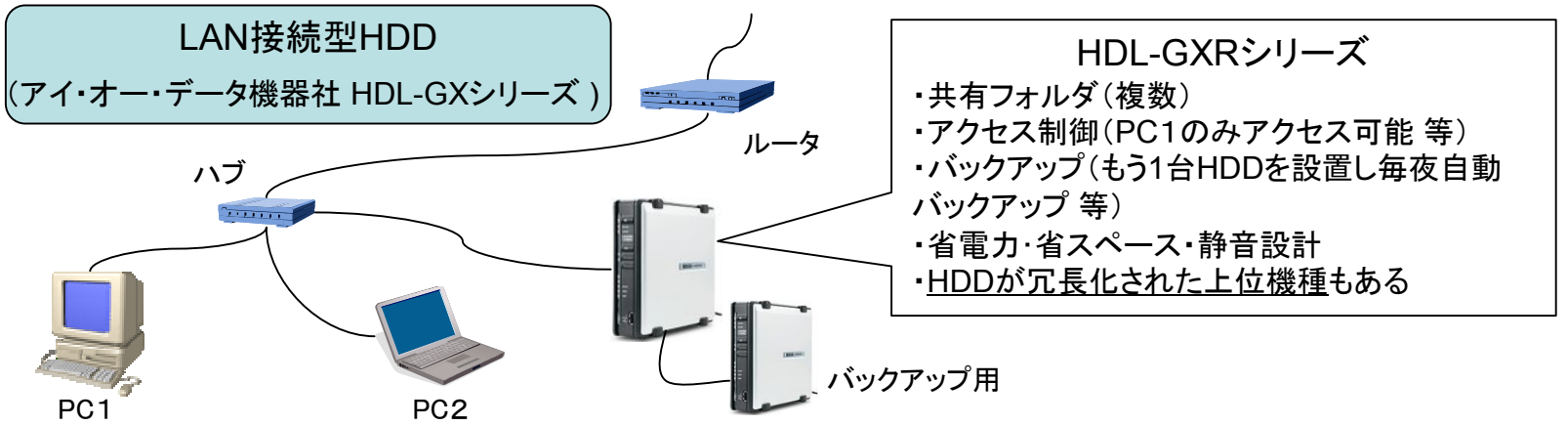
■ LAN接続型HDD

LANに直結できるハードディスク（ファイルサーバ）
ファイル共有機器（LinuxOS搭載のコンピュータ）

参考：きめ細かなアクセス制御、ログ収集
定期的なパスワード変更
等まで求めるならば
Windowsサーバのファイルサーバ（ActiveDirectory）等
台数が増えたら管理サーバ要

- アクセス制御（ログインIDでフォルダアクセス許可）
- バックアップ（USB接続HDDを繋ぎ自動バックアップ）
- 省電力・省スペース
- USB接続プリンタを繋ぎ、プリンタ共有も可能
- 価格：2万円程度～＜IO・データ HDL-GXRシリーズ等＞
- HDDを複数台搭載した冗長型もあり（HDDに障害が発生したら止めずに交換可能）

バッファロー社にも多機種あり



4．3．ファイルの持ち運び：暗号化USBメモリ

■USBメモリ（ハードウエア暗号化）

USBメモリに暗号化ソフトが組み込まれている
USBにアクセスするときにパスワードの入力が強要される

- ソフトインストール不要、そのまますぐに使える
- 強力な暗号化（AES256ビット）
- 価格：5千円（1GB）程度～
  ＜バッファロー RUF2-HSCLシリーズ等＞
- パスワードの管理は必須（集中管理ソフトもあり）
- パスワードの代わりに指紋認証するものもあり

トレンドマイクロ社ウィルス対策ソフト付き

誤送信時の対策、メールはハガキのようなもの

参考）メールでファイル送信するときなどは、ファイルの暗号化ソフトが有用

- » ファイル暗号化フリーソフト：**アタッシェケース**
- » ファイル圧縮フリーソフト（パスワード設定可）：Lhaplus

ノートPCの持出では、HDDの暗号化ソフトが有用
HDDの完全削除ソフト：AOS社ソフト等、フリーソフトもあり

4. 次へのステップ

1. 情報セキュリティ管理
2. IPA　情報セキュリティベンチマーク
3. ISMS認証レベルを目標に

最低限実施すべき対策を実施出来たら、自組織のセキュリティ対策は万全でしょうか。

ここでは、次へのステップとして必要な考え方やツールなどをご紹介します。

1. 情報セキュリティ管理

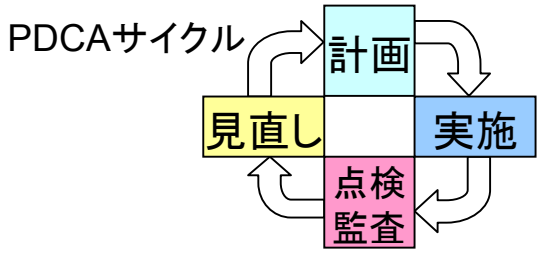
- 最低限必要なセキュリティ対策の計画
  - 一度に出来なければ、出来るところから
  - どこが出来ていないか把握する
- 最低限必要なセキュリティ対策の実施
  - とりあえず実施してみる

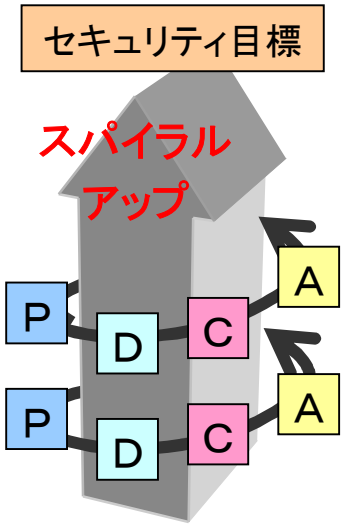
これでOK？ ← 確認と見直しが必要

- 本当に継続して対策を実施しているか
- 対策は実情に合っているか

- 情報セキュリティ管理（マネジメントシステム）

計画（Plan）
実施（Do）
確認（Check）
見直し（Act）





2．IPA 情報セキュリティベンチマーク

- 組織の情報セキュリティマネジメントシステムの実施状況を、自らが評価する自己診断ツール（2005 年 8 月より IPA の Web 上で提供）

- Web ページ上の25の質問に答えることで、組織の情報セキュリティへの取組状況を 簡便に自己評価することが可能
  （さらに、企業プロフィールに関する15項目の回答から、回答企業がどの程度情報セキュリティの対策が求められる（3つの）層かを判断）
  「5分でできる自社診断」より高度で抽象的な質問

- 何千件もの実データに基づき、望まれる水準や他社の対策状況と自社の対策状況を比較することができる
  （散布図やレーダーチャートでグラフィカルに表示）

- この 25 問は、ISMS 認証基準である JIS Q 27001 付属書 A の管理策（ 133 項目、=JIS Q 27002）をベースに作成されている
  （評価項目の量を 25 項目に抑え、わかりやすい言葉を使っている）

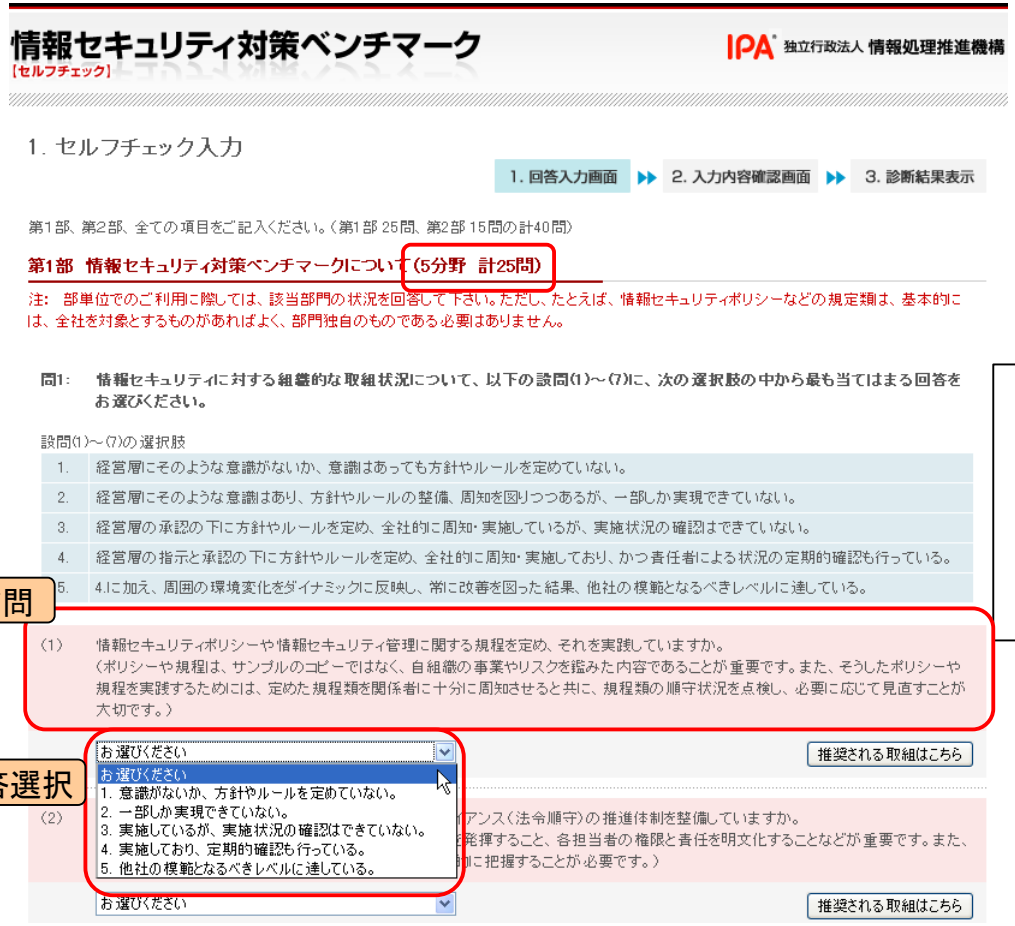
- 回答は、1から 5 の 5 段階で回答（1 は取り組みができていない状態、5 は他社の模範となるまで取組みが進んでいるレベル ）
  ○×ではなく、管理できているかを問う

- 様々な資料（活用事例集、設問ごとの解説・対策のポイント 等）などが揃っている

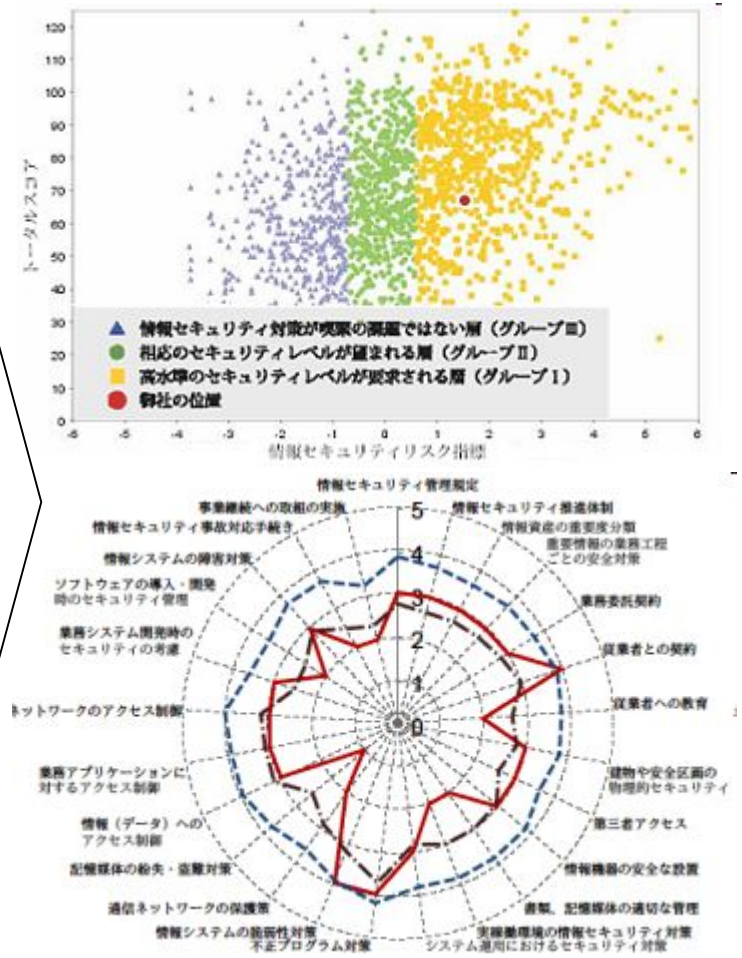
出典）http://www.ipa.go.jp/security/benchmark/benchmark-gaiyou.html

2. IPA 情報セキュリティベンチマーク

25の質問(＋15の企業プロフィール質問)に回答(5つの選択肢)



アウトプット



URL) https://isec.ipa.go.jp/benchmark-main/benchmark/

3. ISMS認証レベルを目標に

業務委託元から
相応のセキュリティ
レベルを求められる