2008年度　ITC横浜知識研修セミナー第4回　資料

中小企業における情報セキュリティ対策

～中小企業の規模・レベルに応じた情報セキュリティ対策の
取組方法についての御提案 ～

2009-01-31
（12：30～14：20）
（2009-02-03 一部修正版）

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. はじめに

2. ケース１：あまり対策が取られていない組織
   「最低限必要なセキュリティ対策」の実施

3. ケース２：最低限の対策は取られている組織
   IPA 情報セキュリティベンチマークの活用

4. ケース３：ある程度の対策が取られている組織
   情報セキュリティ管理基準の活用

5. まとめ

＊時間が余ったら － 社員向け教育用資料
＜情報セキュリティにおける最近の脅威について＞

資料別途

1．はじめに

中小企業の情報セキュリティ対策の状況の概説。

中小企業では、会社（規模、情報化、管理レベル）によってセキュリティ対策の実施状況が大幅に異なる。

中小企業の会社規模（情報化・管理レベル）により典型的な3つのケースを設定し、それぞれのケースごとの情報セキュリティの取組方法を考える。

1. 中小企業の情報セキュリティ対策の状況
2. 中小企業の情報セキュリティレベル ケース設定

1．中小企業の情報セキュリティ対策の状況

中小企業における情報セキュリティ対策の状況調査より

1. 情報セキュリティ対策の状況調査：調査対象 非上場300人未満の会社
（総務省：2002年9月発表資料による）
2. 個人情報保護法および情報セキュリティ対策に関するアンケート調査：調査対象 ？
（gooリサーチ、日刊工業新聞：2005年3月発表資料による）
3. SOHO事業者における情報セキュリティ対策研究調査：調査対象 従業員10人以下
（財団法人マルチメディア振興センター主催：2004年12月頃「SOHOにおける情報セキュリティ対策の研究会」による）

■ 中小企業は大企業と比べて、情報セキュリティ対策が遅れている

■ 中小企業がセキュリティ対策に取り組まない理由、取り組む上での問題点
- 知識・ノウハウが無い
- 費用・手間が掛かる
- どこまでやればよいか、分からない
- セキュリティに対する認識の無さ

＊中小企業の中でも会社規模（情報化レベル、管理・統制レベル）等により対策の状況は違うはず
←これらを調査した資料等は特になし

1．中小企業の情報セキュリティレベル ケース設定1

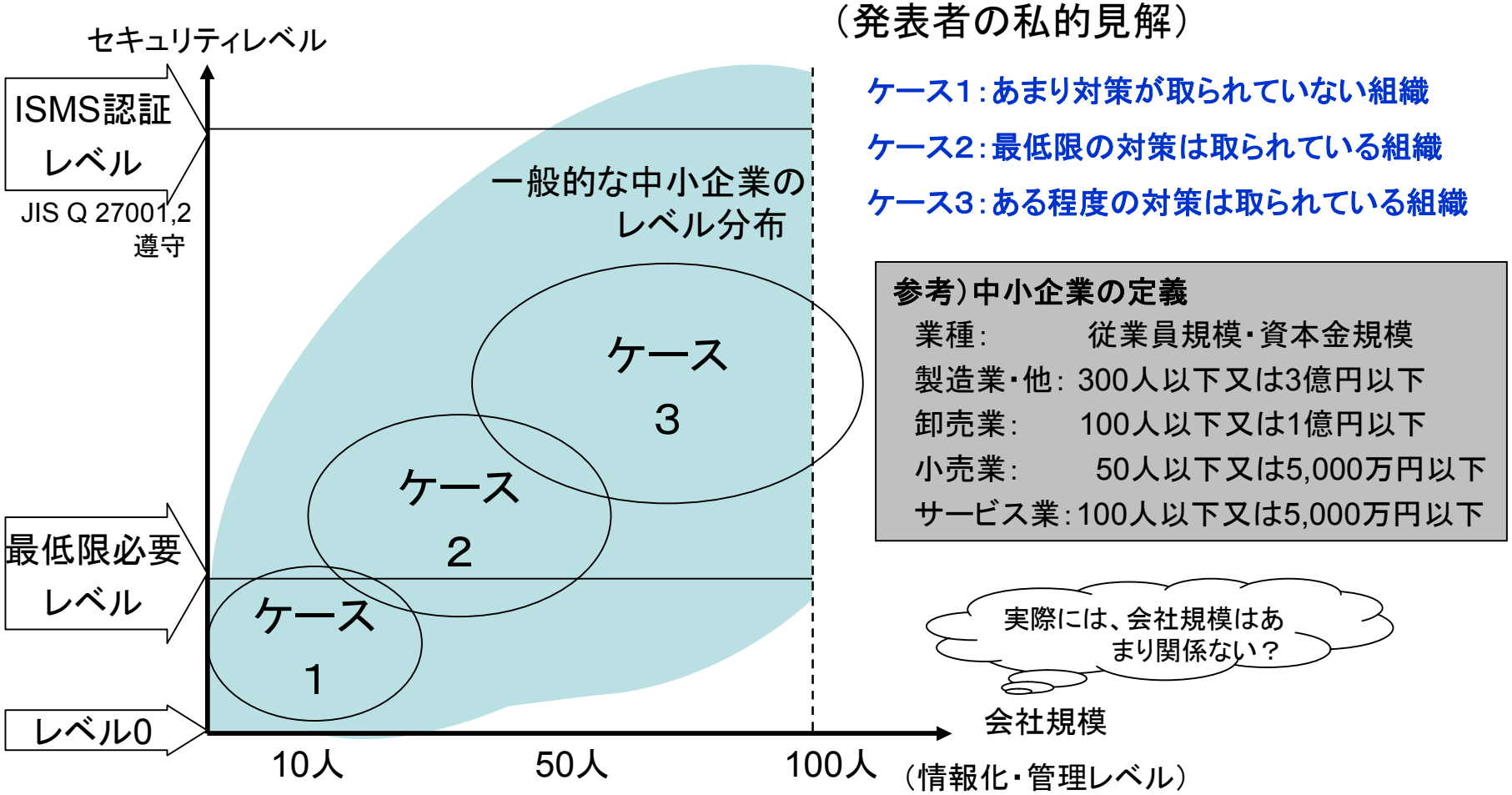
- 中小企業では現状のセキュリティレベルが様々
  （全く対策が出来ていない組織からISMS認証レベルの組織まで）
  ⇒ひとくくりに「中小企業のセキュリティ対策」うんぬんと言えない
- 中小企業にとって、現状のセキュリティレベルからのステップアップが重要
  ⇒典型的なケース設定をし、各ケースごとにどのように対策に取り組むかを検討

ケース	会社規模（目安）	情報化・管理レベル	情報セキュリティ対策の状況
1	10人前後	社内LAN、インターネット、ファイル共有	あまり対策が取られていない 各個人での対応（対策を実施していない人もいる）、管理できていない
2	20～30人前後	（ケース1に加えて） PC1台/1人、情報共有 簡単な規定類作成	最低限の対策は取られている それ以外は多少手をつけている程度、簡単な規定作成。次へのステップが見えない。
3	50～100人前後	（ケース2に加えて） 基幹システム 規定類網羅、教育体制	ある程度の対策が取られている 簡単なセキュリティポリシー作成、管理体制構築。いかにしてISMS認証レベルへ。

1．中小企業の情報セキュリティレベル ケース設定2

■ 中小企業のセキュリティレベルの分布イメージと設定したケース

（発表者の私的見解）



ケース1：あまり対策が取られていない組織

ケース2：最低限の対策は取られている組織

ケース3：ある程度の対策は取られている組織

参考）中小企業の定義

業種：	従業員規模・資本金規模
製造業・他：	300人以下又は3億円以下
卸売業：	100人以下又は1億円以下
小売業：	50人以下又は5,000万円以下
サービス業：	100人以下又は5,000万円以下

2. ケース1：あまり対策が取られていない組織

セキュリティ対策があまり実施されていない、社員10人前後の組織に「最低限必要なセキュリティ対策」を実施する。

合わせて具体的な技術的対策の実践内容（ソリューション）を提示する。

最低限必要なセキュリティ対策

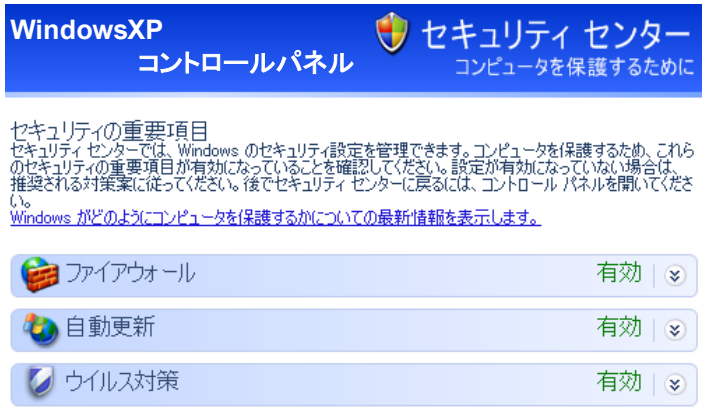
（ネットに繋げるだけで発生する脅威の対策、費用対効果のある対策 等）

1. コンピュータを守る
   （OSのアップデート、ウイルス対策ソフト、ファイアウォール）
2. データを守る（バックアップ、アクセス制御、暗号化）
3. 規定（ルール）と教育
4. 技術的対策 実践内容
   1. 企業向けウィルス対策ソフト
   2. ファイル共有：LAN接続型ハードディスク
   3. ファイルの持ち運び：暗号化USBメモリ
5. 良い点、悪い点（不足している点）

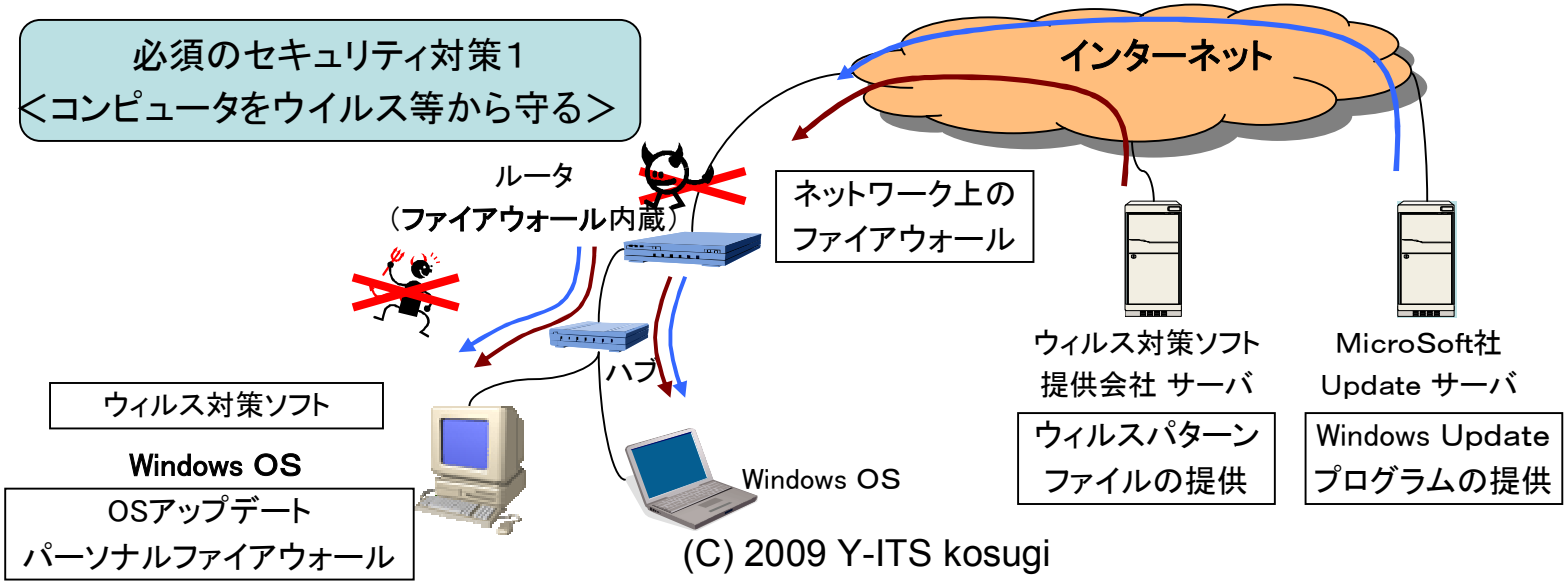
1．コンピュータを守る

コンピュータが守られれば
内部のデータも守られる

- ファイアウォール　＜ネットワーク上のファイアウォールとPCのパーソナルファイアウォール
  - 外部からの不正な攻撃（入口）を防ぐ
  - 不正アクセス・コマンドに有効
- 自動更新（アップデート）
  - ソフトの脆弱性（バグ、不具合）を修正する
  - ウイルスや不正アクセス・コマンドに有効
- ウイルス対策ソフト
  - ウイルスなどの不正なプログラムを防ぐ
  - ウイルス等の不正なプログラムに有効



必須のセキュリティ対策1
＜コンピュータをウイルス等から守る＞

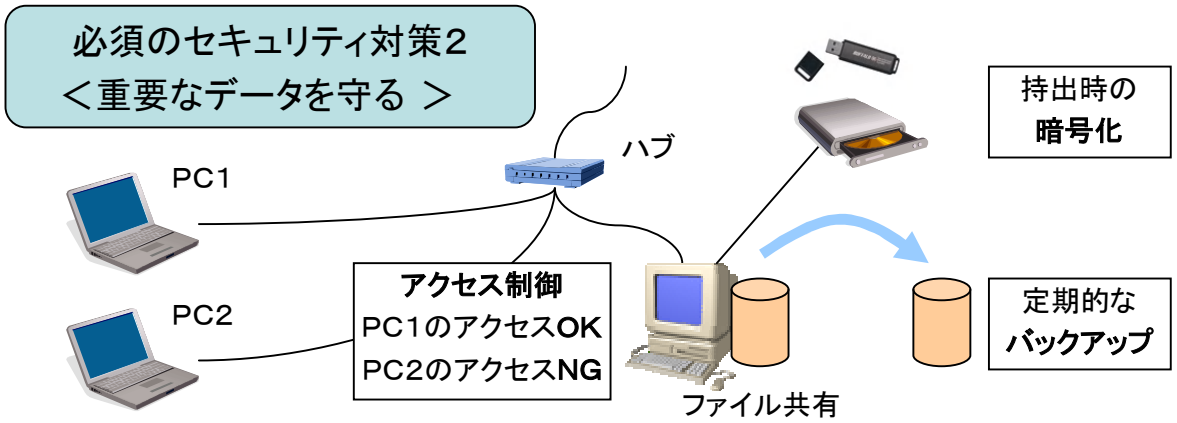


2. データを守る

- バックアップ
  - 重要な情報ファイルは定期的に(自動的に)バックアップしておく
  - ファイルが壊れたり、PCが故障したときに有効
  - バックアップの復元テスト、バックアップ媒体の遠隔地保管も重要
- アクセス制御
  - 重要なデータは必要な人だけが読み書きできるように設定（制御）しておく
  - 不正アクセスなどに有効
  - アクセスのためのID,パスワードの管理も重要

不正アクセス防止法でも必須

- 暗号化
  - 重要な情報ファイルを持ち出すときや送るときに暗号化する
  - 不正アクセスなどに有効、情報漏えい時の最後の砦



3．規程（ルール）と教育

■ 人的・管理的なセキュリティ対策

技術的な対策と併用

手順書・内部統制も大事

会社

社員及び外部委託会社とは**秘密保持契約を**

説明

教育

啓蒙

社員

○○会社 社員向け情報セキュリティのルール（サンプル）

1．業務用PCは下記注意を守り適切に管理すること
- ①業務に関係しないHPの閲覧をしない
- ②業務に関係しないメールを送らない、開かない
- ③ソフトをインストールするときは管理者に許可を取る
- ④ログオンするためのID、パスワードは厳重に管理する
- ⑤個人管理の重要な情報は定期的にバックアップを取っておく
- ⑥許可を得ずに他人のPCやデータファイルを操作しない
- ⑦ウィルス対策ソフト・OS等のアップデートの自動化を実施しておく

2．会社の情報資産を持ち出すときは、管理者に許可を取ること
（電子データの持ち出し時は暗号化等の対策をとる）

3．私物PCや情報機器の持ち込み・社内LANへの接続の禁止

4．セキュリティに関する事故が発生したら、管理者に連絡すること

5．重要文書、媒体（FD等）を破棄するときは、シュレッダー等にかけること

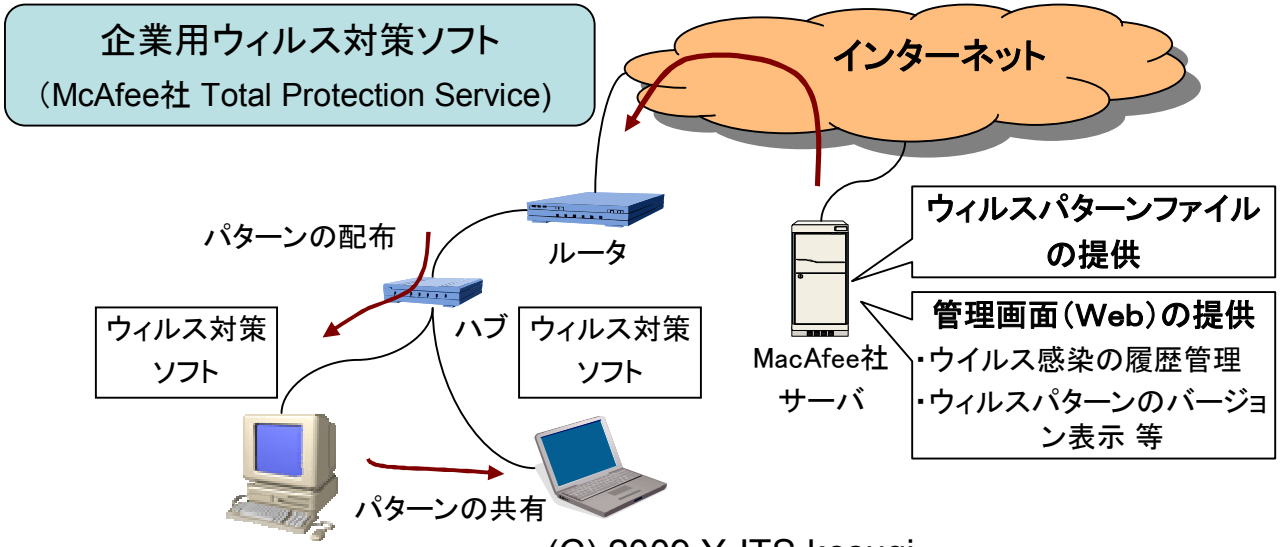
セキュリティ管理者：XXXXXX

参考）総務省 テレワークセキュリティガイドライン
http://www.soumu.go.jp/joho_tsusin/telework/pdf/060428_g2.pdf

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）



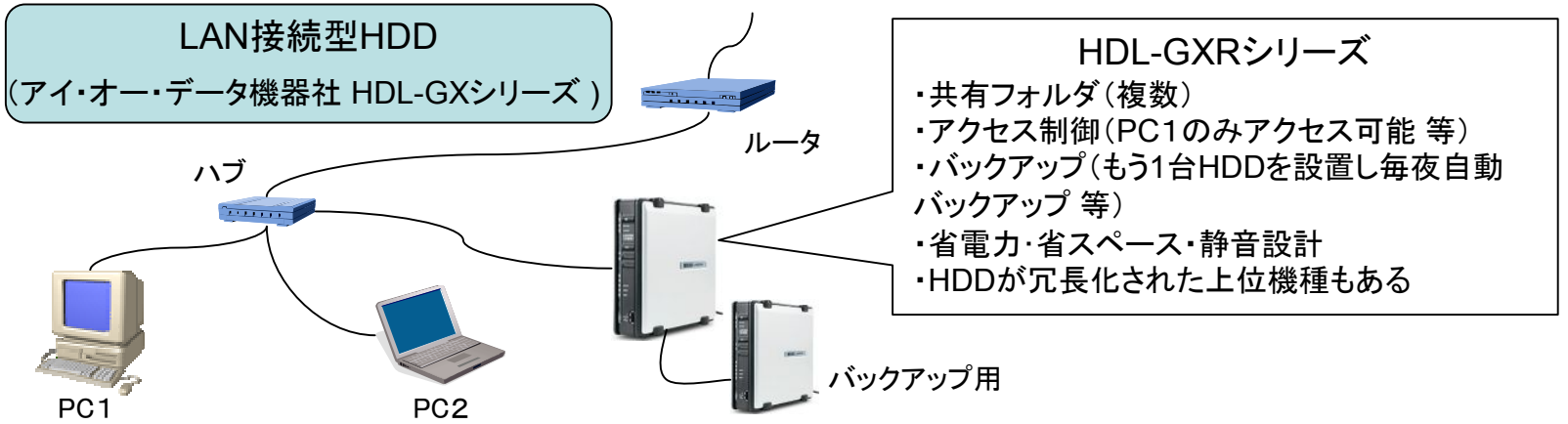
2．ファイル共有：LAN接続型ハードディスク

■ 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、
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）



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：1万円（2GB）程度～
  ＜バッファロー RUF2-HSC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（RUF2-FHS）もあり

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

5．良い点、悪い点（不足している点）

良い点

- どんな組織でもほぼ共通した必須事項である
- とりあえず実施すれば効果はある
- それほど費用は掛からない

悪い点（不足している点）

- 定期的なチェックと継続的実施の必要性（担当者が必要）
- いかにしてルールを守ってもらうか（しくみ、内部統制）
- 付加したい重要な対策（実践）
  - 物理的対策（セキュリティ区画等）
  - 技術的対策（OSアップデート管理、ログの取得 等）
  - リスク分析の考え方
    （厳密な分析は必要ないが、対策の重み付け・優先順位のために）

３．ケース２：最低限の対策は取られている組織

「最低限必要なセキュリティ対策」程度は実施済（しかし、ISMS認証レベルまでは考えていない）の組織が、次にどんな対策を検討したらよいか。

IPA 情報セキュリティベンチマークを利用した、脆弱性の解消と、更なるレベルアップを検討する。

情報セキュリティベンチマークの活用

1. IPA　情報セキュリティベンチマークとは
2. IPA　情報セキュリティベンチマークの活用法
3. IPA　情報セキュリティベンチマークの２５の質問
4. 良い点、悪い点（不足している点）

1．IPA 情報セキュリティベンチマークとは

- 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）

- 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）

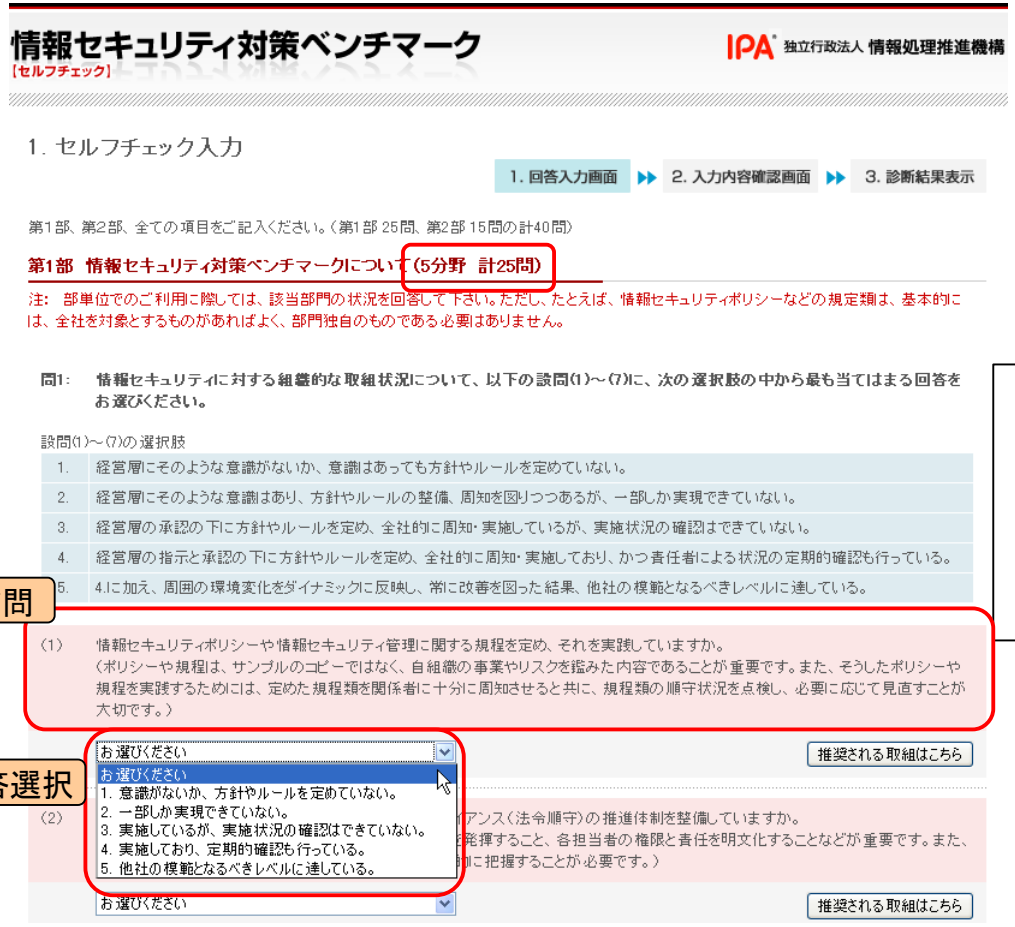
- 回答は、1から 5 の 5 段階で回答（1 は取り組みができていない状態、5 は他社の模範となるまで取組みが進んでいるレベル ）

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

3．ステップ2：情報セキュリティベンチマークの活用

1．IPA 情報セキュリティベンチマークとは

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）



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

2．IPA 情報セキュリティベンチマーク活用例

- 情報セキュリティ対策の実施状況の把握
  - 組織のセキュリティ上脆弱な部分を知る⇒対策により穴埋め
- 質問に対応した「対策のポイント・解説」資料により具体的な対策を検討
- 定期的利用で、情報セキュリティ対策の改善と向上
  - 実施状況の見直しに繋がる（マネジメントサイクル）
  - 更なるレベルアップが検討できる

他にも

- 他社と比べた自社の位置の確認
  - 自社のレベルを経営陣に伝えることが可能⇒予算取りのためのツール
- 委託元や取引先の要求を満たすために診断結果を提示
  - 逆に使われる可能性もあり
- ISMS適合性評価制度の準備段階で利用
  - 認証を取得していなくても、そのレベルにあることを認識可能

参考）パンフレット
http://www.ipa.go.jp/security/benchmark/documents/BM_katuyo_2.pdf

3. IPA 情報セキュリティベンチマークの25の質問1

1. 情報セキュリティに対する組織的な取組状況

①情報セキュリティポリシーや情報セキュリティ管理に関する規程を定め、それを実践していますか。

②経営層を含めた情報セキュリティの推進体制やコンプライアンス（法令順守）の推進体制を整備していますか。

③重要な情報資産（情報及び情報システム）を、その重要性のレベルごとに分類し、さらにレベルに応じた表示や取扱いをするための方法を定めていますか。

④重要な情報（たとえば個人データや機密情報など）については、入手、作成、利用、保管、交換、提供、消去、破棄などの一連の業務プロセスごとにきめ細かくセキュリティ上の適切な措置を講じていますか。

⑤外部の組織に業務や情報システムの運用管理を委託する際の契約書には、セキュリティ上の理由から相手方に求めるべき事項を記載していますか。

⑥従業者（派遣を含む）に対し、採用、退職の際に守秘義務に関する書面を取り交わすなどして、セキュリティに関する就業上の義務を明確にしていますか。

⑦経営層や派遣を含む全ての従業者に対し、情報セキュリティに関する自組織の取組や関連規程類について、計画的な教育や指導を実施していますか。

できていない

回答選択肢

1.	経営層にそのような意識がないか、意識はあっても方針やルールを定めていない
2.	経営層にそのような意識はあり、方針やルールの整備、周知を図りつつあるが、一部しか実現できていない
3.	経営層の承認のもとに方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない
4.	経営層の指示と承認のもとに方針やルールを定め、全社的に周知・実施しており、かつ責任者による状況の定期的確認も行っている。
5.	4. に加え、周囲の環境変化をダイナミックに反映し、常に改善を図った結果、他社の模範となるべきレベルに達している

できている

3. IPA 情報セキュリティベンチマークの25の質問2

2. 物理的（環境的）セキュリティ上の施策

①特にセキュリティを強化したい建物や区画に対して、必要に応じたセキュリティ対策を実施していますか。

②顧客、ベンダーや、運送業者、清掃業者など、建物に出入りする様々な人々についてセキュリティ上のルールを定め、それを実践していますか。

③重要な情報機器や配線などは、自然災害や人的災害などに対する安全性に配慮して配置または設置し、適切に保守していますか。

④重要な書類、モバイルPC、記憶媒体などについて適切な管理を行っていますか。

3. 情報システム及び通信ネットワークの運用管理

①情報システムの運用に際して、運用環境や運用データに対する適切な保護対策が実施されるよう、十分に配慮していますか。

②情報システムの運用に際して、必要なセキュリティ対策を実施していますか。

③不正プログラム（ウイルス、ワーム、トロイの木馬、ボット、スパイウエアなど）への対策を実施していますか。

④導入している情報システムに対して、適切なぜい弱性対策を実施していますか。

⑤通信ネットワークを流れるデータや、公開サーバ上のデータに対して、暗号化などの適切な保護策を実施していますか。

⑥モバイルPC やUSB メモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などを想定した適切なセキュリティ対策を実施していますか。

3．IPA 情報セキュリティベンチマークの25の質問3

4．情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況

①情報（データ）や情報システムへのアクセスを制限するために、利用者ID の管理、利用者の識別と認証を適切に実施していますか。

②情報（データ）や情報システム、業務アプリケーションなどに対するアクセス権の付与と、アクセス制御を適切に実施していますか。

③ネットワークのアクセス制御を適切に実施していますか。

④業務システムの開発において、必要なセキュリティ要件を定義し、設計や実装に反映させていますか。

⑤ソフトウェアの選定や購入、情報システムの開発や保守に際して、セキュリティ上の観点からの点検をプロセスごとに実施するなど、適切なプロセス管理を実施していますか。

5．情報セキュリティ上の事故対応状況

①万が一システムに障害が発生しても、必要最低限のサービスを維持できるようにするため、情報システムに障害が発生する場合をあらかじめ想定した適切な対策を実施していますか。

②情報セキュリティに関連する事件や事故が発生した際に必要な行動を、適切かつ迅速に実施できるように備えていますか。

③何らかの理由で情報システムが停止した場合でも、必要最小限の業務を継続できるようになっていますか。

4．良い点、悪い点（不足している点）

良い点

- JIS Q 27002をベースにしているため網羅性があり、脆弱な部分（対策が取られていない部分）が見えてくる
- 他の組織との比較が行なわれるため、やる気を出させられる
- IPAにより定期的に見直し（メンテナンス）がされている
- IPAがこれを元に「中小企業の情報セキュリティ対策パッケージ」資料を作成中

現在「情報セキュリティ対策の入門診断シート」「組織的な情報セキュリティ対策ガイドライン」等を作成中（2009/3/M～4/F頃公開予定：2009/2/2セミナー講演：IPAセキュリティセンター長による話）

悪い点（不足している点）

- 抽象的な言い回しが多い（回答するにも困る）
- 細かい（具体的な）対策が明示されていない
- 項目を絞った分、検討漏れが気になる
- どこに重点を置くべきかは、別途検討が必要

４．ケース３：ある程度対策が取られている組織

（認証の取得はともかく）ISMSの認証レベルを目標に、情報セキュリティ管理のスタンダードであるJIS Q 27002の適用を検討する。
（JIS Q 27001は「認証のための基準」のため、概要のみ把握）

ここでは、JIS Q 27002 と内容が同じである、情報セキュリティ監査制度の「情報セキュリティ管理基準」を利用する。

情報セキュリティ管理基準の活用

1. JIS Q 27001,27002とは
2. 情報セキュリティ管理基準とは
3. 情報セキュリティ管理基準の利用方法
4. 良い点、悪い点（不足している点）

1．JIS Q 27001,27002とは

- JIS Q 27001、27002＝ISO/IEC 27001,27002
  - 情報セキュリティマネジメントのスタンダード
  - 国内外の様々な基準等に採用（参照）されている

- JIS Q 27001：2006
  セキュリティ技術－情報セキュリティマネジメントシステム－要求事項
  - ISMS認証取得の要求事項
  - JIPDEC ISMSパンフレットで概要理解（組織体制、リスク分析、PDCAサイクル 等）
    http://www.isms.jipdec.jp/doc/ismspanf.pdf

- JIS Q 27002：2006
  情報セキュリティマネジメントの実践のための規範
  - 情報セキュリティ対策(管理策)のベストプラクティス
  - 11のマネジメント領域、39のカテゴリ、133の管理策
  - 133の管理策ごとに詳細に述べられている
  - しかし、著作権的に非公開（実際には解説本で内容理解）
    - ISO/IEC17799（JIS Q 27002）詳解 情報セキュリティマネジメントの実践のための規範（日本規格協会 発行）

2．情報セキュリティ管理基準とは

- 経産省により設立された「情報セキュリティ監査制度」（2003年４月より）における
  監査のための管理基準（監査項目）
  - 別途、「情報セキュリティ監査基準」あり
  - 参考）情報セキュリティ監査制度http://www.meti.go.jp/policy/netsecurity/audit.htm
- 2008年11月に改訂され、JIS Q 27001と27002に準拠したものが公開された
- 前半部分（マネジメント基準）は、JIS Q 27001の内容に準拠している。
  後半部分（管理策基準）は、JIS Q 27002の内容とほぼ同一で、かつ項目が細分化されている
- チェックリストとして利用できるように、Excelファイルでも公開されている
  （133の管理策を1153項目に細分化したもの）

項番	項目	目的	管理策基準		詳細管理策	
1.1	情報セキュリティ基本方針	情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項、関連する法令及び規制に従って規定するため	1.1.1	情報セキュリティ基本方針文書は、経営陣が承認し、また、全従業員及び関連する外部関係者に公表し、通知する	1.1.1.1	情報セキュリティ基本方針文書に、経営陣の責任を明記し、情報セキュリティの管理に対する組織の取組み方を示す
					1.1.1.2	情報セキュリティ基本方針文書に、情報セキュリティの定義、その目的及び適用範囲、並びに情報共有を可能にする基盤としてのセキュリティの重要性に関する記述を含める

39カテゴリ　133管理策　1153詳細管理策

3．情報セキュリティ管理基準の利用方法

1. 管理策1153項目の理解
   - 不明な用語などを確認し理解する
2. 組織の現状のセキュリティレベルから、まず取り組むべき管理策をピックアップ
   - レベル的に合わない（高すぎる）管理策は次回以降
   - 自組織に関係ない管理策は除外
3. 計画の実施
   - ピックアップした管理策（と今まで実施していた管理策）がPlan
4. 計画のチェックと見直し
   - CheckとAct
5. 再度、2から取り組む
   - PDCAサイクルを回す

4．良い点、悪い点（不足している点）

良い点

- JIS Q 27002であり網羅性、内容についても問題なし

悪い点（不足している点）

- 量が多すぎ、内容も理解するのが難しい
  ⇒1153管理策に解説
  ＋管理策の重要度付け（1～3程度)があれば・・・

参考）政府機関統一基準

- 情報のライフサイクル（作成～利用～廃棄）に応じた管理策の提示
  ⇒一般職員（社員）はこの管理策を中心に守っていけばよい
- 実施マニュアルや手順書のサンプルも公開されている

参照URL）http://www.nisc.go.jp/active/general/kijun01.html

5. まとめ

■ 中小企業の情報セキュリティ対策