情報セキュリティリスクの低減

- ISO27001の活用 -

2006.10.05　　道廣　和男

はじめに

・昨今、個人情報の漏えい、フィッシング詐欺等企業の情報管理に
関連する事故をよく耳にします。
・「ああ、またか」と他人事のように捉えていませんか？
・情報は個人情報だけではありません。
　システム情報、顧客情報、事業ノウハウ・・・etc.
　事業を行う以上、『資産』を保持しているのです。
・大切な資産、貴社ではきちんと管理できていますか？
・「情報を管理する」ということは「情報に関連するあらゆるリスクを管理（セキュリティマネジメント）する」ことなのです。

今回は、情報セキュリティマネジメントシステムであるISO27001（以下、ISMS）とはどのようなものなのか、また企業にとってどのようなメリットがあるのかを中心に講演させていただきたいと思います。

ISMSの背景①

- IT化の進展に伴う、取扱い情報の重要性が向上
- 不正アクセスやコンピュータウイルスによる被害多発
- 内部不正者や外注業者による情報漏えい事件

・・・資産を脅かす要因が著しく増加

これらの脅威に対して適切にリスク管理を実施し、企業における総合的な情報セキュリティ確保を遂行するためには・・・

技術的なセキュリティ対策の他に、
人間系の運用・管理面の要素を取り入れたシステムが必要

＝ 情報セキュリティマネジメントシステム（ISMS）

ISMSの背景②－事故の紹介①－

◆ショッピングのモール出店企業3,169社の企業情報流出

原因：業務を委託している企業の社員の私有パソコンから漏えい（Winnyによるもの）

◆名前、住所、電話番号、契約種別等の契約者22,803件の個人情報盗難

原因：業務中、首からかけていた携帯端末のひったくりによる盗難

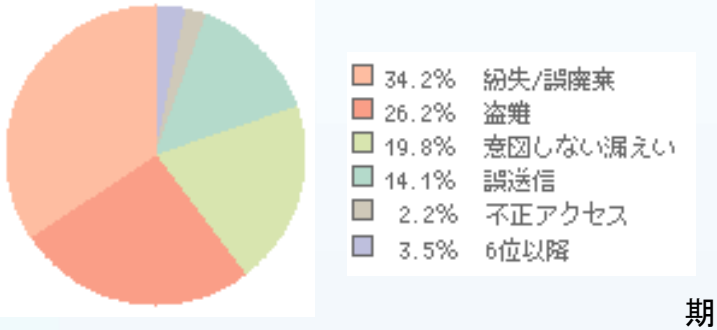
◆ユーザID、メールアドレス、パスワード、ログファイルの顧客情報295,775件が流出

原因：共同運営会社の誤操作により、意図しないサーバ上にデータが格納

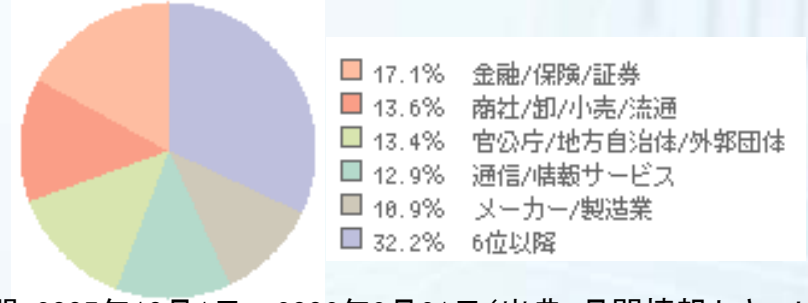
◆氏名、取引種類、通帳・証書等の区分等、約10,000件の顧客情報誤廃棄

原因：保存期間を過ぎた書類廃棄の際、誤って保存期間の過ぎていない書類が混在

■情報漏えいカテゴリ別



■情報漏えい業種別



期間：2005年10月1日～2006年9月21日（出典：月間情報セキュリティ）

参考：個人情報が流出すると・・・

・企業の損失が億単位になることもあります！

【コンビニのカード会員情報流出事件】

コンビニのカード会員情報（115万人分）が流出した事例では、
見舞金として1人あたり500円、総額5億7,500万円が支払われました。

500円×1,150,000人＝575,000,000円

【ADSLサービスの個人情報流出事件】

ADSLサービスで個人情報（約451万人分）が流出した事例では、
1人あたり500円、総額22億5,500万円の見舞金が支払われました。

500円×4,510,000人＝2,255,000,000円

1人あたりの金額は少なくても、
大量の個人情報が流出すると金額が膨れ上がります。

ISMSの背景②－事故の紹介②－

【事故の分類】

◆外部からの不正行為

→フィッシング、ファーミング、ハッカー行為

◆内部からの不正行為

→退職者の嫌がらせ、他社への情報提供

※情報漏えいの8割は内部犯行と言われています。

◆内部からの操作ミス、処理ミス

→送信先や添付ファイルの誤送、施錠忘れ

◆偶発的に起こる事故

→自然災害、火災等による事故

事故には、このように様々な種類があります。
外部だけではなく内部やその他の問題にも対応する必要があるのです。

ISMSの概要①

- ISMSは、個別の問題毎の技術対策の他、組織のマネジメントとして、**自らのリスクアセスメント※により、必要なセキュリティレベルを決め**、プランを持ち、資源配分して、システムを運用します。

※リスクアセスメント：リスク分析からリスク評価までのすべてのプロセス

【基本コンセプト】

組織が保護すべき資産について、
機密性、完全性、可用性をバランス良く維持し改善すること

機密性　認可されていない個人、エンティティ（団体等）又はプロセスに対して情報を使用不可又は非公開にする特性。

完全性　資産の正確さ及び完全さを保護する特性。

可用性　認可されたエンティティ（団体等）が要求したときに、アクセス及び使用が可能である特性。

（ISO/IEC 13335-1:2004より引用）

ISMSの概要②

・　以下はISMSの要求事項の構成ですが、ここに注目しましょう。

0. 序文
1. 適用範囲
2. 引用規格
3. 用語および定義
4. 情報セキュリティマネジメントシステム
4.1 一般要求事項
4.2 ISMSの確立および運営管理
4.3 文書化による要求事項
5. 経営陣の責任
5.1 経営陣のコミットメント
5.2 経営資源の運用管理
6. ISMS内部監査
7. ISMSのマネジメントレビュー
7.1 一般
7.2 レビューへのインプット
7.3 レビューからのアウトプット
8. ISMSの改善
8.1 継続的改善
8.2 是正処置
8.3 予防処置

8.3　予防処置
（略）
予防処置の優先順位は，
リスクアセスメントの結果に基づいて
決定しなければならない。

注記　不適合を予防するための処置は，多くの場合，是正処置よりも費用対効果が大きい。

（ISO/IEC 27001：2005より引用）

是正処置よりも予防処置の方が
効果あり、ということを言っています。

ISMSの概要③

・　リスクアセスメントに基づき、以下の管理策を選択して実施します。

A.5.　セキュリティ基本方針	1
A.6.　情報セキュリティのための組織	2
A.7.　資産の管理	2
A.8.　人的資源のセキュリティ	3
A.9.　物理的及び環境的セキュリティ	2
A.10. 通信及び運用管理	10
A.11. アクセス制御	7
A.12. 情報システムの取得、開発及び保守	6
A.13. 情報セキュリティインシデントの管理	2
A.14. 事業継続管理 ★	1
A.15. 法的要求事項の順守	3

39項目の詳細管理策
（小分類では133項目）

ここに注目！

参考：事業継続管理①

- 他の規格（ISO9001、14001等）の要求にはない事業継続管理の項目がISMSにはあります。
- 予防処置が重要だという背景と言えるでしょう。

事業継続管理とは、組織が事業を継続して行う為に、組織にとって致命的なリスクの顕在化の防止や顕在化した場合の復旧計画などを策定し被害を最小化する行為を指します。

- 特に不祥事が発生した時、消費者の安全と信頼回復のために、組織がどのような対応を取るのかによって、事業継続を脅かす事にもなりかねません。
- その場しのぎにならないために、先を見通し、相応の準備が必要になります。

参考：事業継続管理②

【不祥事とその対応の事例】

無認可添加物使用の製品販売事件	事実を公認していましたが、公表しませんでした。結果、その方針を決めた取締役を含む被告11名全員に5億5,800万円の損害賠償の判決が下されました。
食肉偽装表示事件	購入客へ返金する旨の店頭告示をしましたが、記者会見直後、返金を求める客の殺到により事件の舞台となった店舗が一時閉鎖になる異常事態となりました。
石油暖房機事故	CMやHPによる積極的な広報活動を実施しました。死亡者を出す深刻な事態にもかかわらず、現時点での業績及びブランドへの影響を軽減に止めています。

参考：事業継続管理③

- 事故や事件をゼロにするのは難しい問題です。だからこそ、起こってしまった後のリカバリーが重要なのです。
- 問われるべきは「これまでの対応とこれからの対策」です。
- 「組織として万全を尽くした上での避けられない事故だった」こと、更に対策強化が評価されてこそ、消費者の信頼回復に繋がるのです。
- ISMSは、事業継続計画策定の枠組みが設けられています。

◆情報セキュリティを組み込んだ事業継続計画の策定及び実施（A.14.1.3）

重要な業務プロセスの中断又は不具合発生の後，運用を維持又は復旧するために，また，要求されたレベル及び時間内での情報の可用性を確実にするために，計画を策定し，実施しなければならない。

ISMSのポイント①

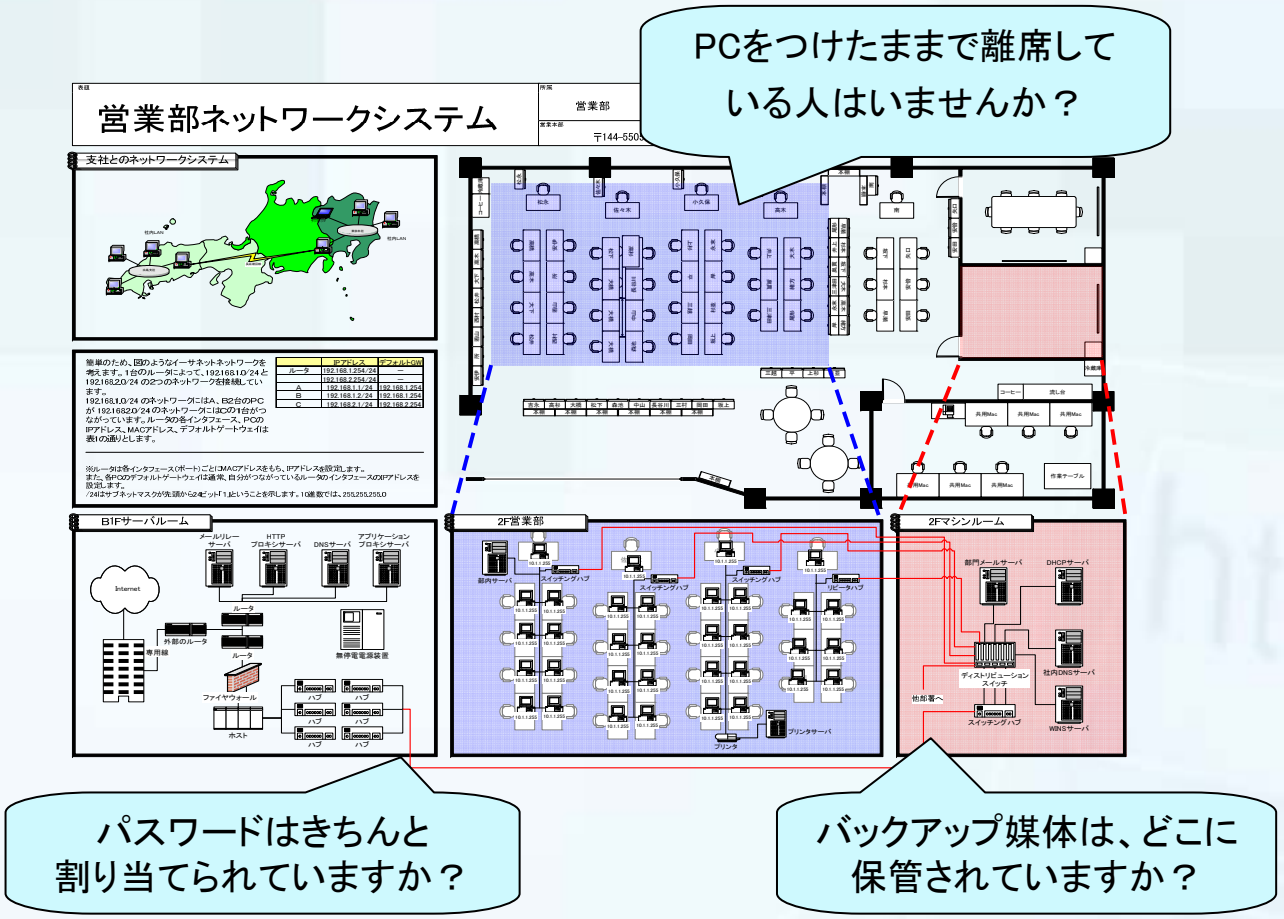
- 情報セキュリティ向上の最も重要なポイントは、
  人的セキュリティの向上（教育）です。

・ 最先端のIT技術を駆使し、事業を行うのは全て「人」です。
・ 先に紹介した事故事例は、人によるものです。
・ 信頼関係のある組織ほど、内部の情報セキュリティ事故は少ないと言えるでしょう。
・ 経営者は、組織の情報セキュリティ方針を明文化させ、仕事に従事する人に徹底的に教育する必要があります。

【情報セキュリティ向上の重要課題】
①教育による人的セキュリティ向上
②情報システムや回線等の技術的セキュリティ向上
③鍵管理、出退勤管理等の物理的セキュリティ向上

ISMSのポイント②

・ 情報セキュリティの脆弱性を探って問題点を解決する仕組みです。

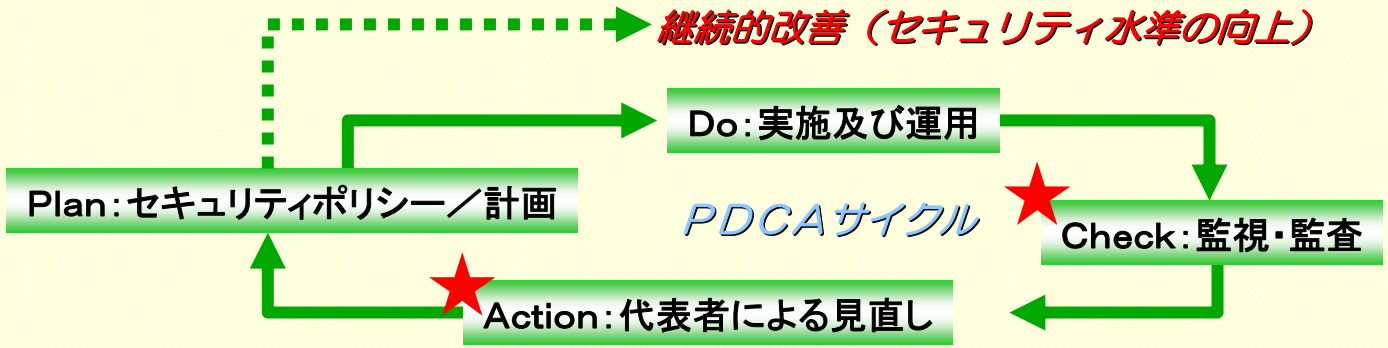


ISMS運用のポイント①

- ISMSは、組織が決めた方針の下に計画、運用、監視、見直し、維持、改善を繰り返します。
- **PDCAサイクルの特にC（監視・監督）とA（見直し）が重要です。**
- 分析を十分に行い、原因対策をしっかりした上で処置をすることに意味があります。

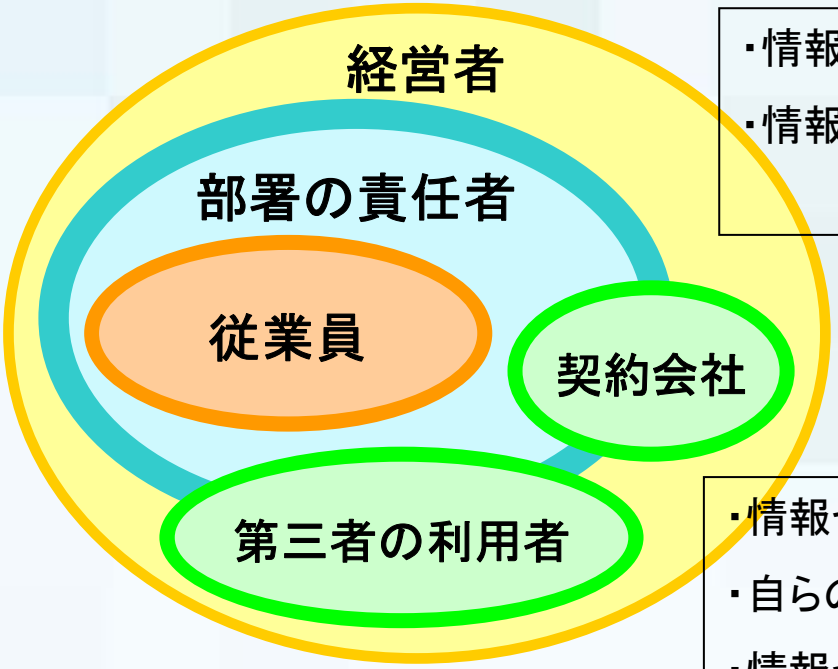
※IT産業は製造業と異なり、事故が顕在化しにくい傾向があります。可能な限り、顕在化することが重要です。

【ISO27001:2005のＰＤＣＡサイクル】



ISMS運用のポイント②

- それぞれ役割と責任があり、必要な教育があります。



・情報セキュリティ基本方針の制定
・情報処理設備に対する許可プロセスの制定・実施
（経営者）

・関連する部署の情報セキュリティ調整
（部署の責任者）

・情報セキュリティ基本方針の教育
・自らの責任の理解
・情報セキュリティに関する雇用契約
・情報セキュリティの脅威及び諸問題、並びに責任及び義務に対する認識
（従業員、契約会社、第三者の利用者）

ISMS構築・運用のメリット

- 技術面及び人間系の運用・管理面の総合的なセキュリティ対策の実現
  - ◆社員のスキル向上
  - ◆責任の明確化
  - ◆緊急事態の対処能力の向上等

- 総合的マネジメントの視点から、効率的なセキュリティ対策の実現
  - ◆費用対効果を考えた資産管理
  - ◆リスクマネジメントの定着等

＊上記の活動を継続することにより、セキュリティ意識の向上等の効果が期待されます。（JIPDEC HPより引用）

まとめ

- ISMSは、リスクマネジメントのツールです。
- すなわち、事業を継続する上で欠かせない予防処置と言えます。事後処理では、取り返しのつかないことになる危険性が高いのです。
- 組織によって、対応できるリスク対策は異なります。自組織にとって、リスクとは何かを明確化させ、リスク発生の要因を洗い出し、対策と効果を認識しましょう。それに基づき、ISMSを確立させます。身の丈に合ったシステムを構築することがポイントです。
- 情報セキュリティ向上の最も重要なポイントは、人的セキュリティの向上です。教育が全ての基本となります。

参考：ISMS構築から取得までの日数

事務局工数（事務局として業務の1/2を準備にあてる計算）				
ステップ	事務局（人・日）	月稼働日	月数	日
調査	0.5	22	1	11
構築	0.5	22	3	33
運用	0.5	22	4	44
審査対応	0.5	22	2	22
合計			10	110
部門メンバー工数（4部門で各1名が業務の1/4を準備にあてる計算）				
ステップ	事務局（人・日）	月稼働日	月数	日
調査	0.25*4	22	1	22
構築	0.25*4	22	3	66
運用	0.25*4	22	4	88
審査対応	0.25*4	22	2	44
合計			10	220
総合計				330

＊　従業員は、50人～100人程度を想定している。

－質疑応答等－

【Memo】