INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

守るべき情報資産・情報リスクの考え方

1. そこにある情報資産
   –自社の情報資産と現状の対策の検証
2. 情報セキュリティの概念、脅威とリスク

1. そこにある情報資産

–自社の情報資産と現状の対策の検証

情報資産とは何か

- 「資産」としての「価値」がある情報
  - 例えば顧客情報、製品開発情報、経営計画の情報など
- あまり「価値」が高くない情報もある
  - Webページや四季報に載せるような情報
  - 所在地、電話番号など

情報の「価値」とは何か

- 「顧客情報」と「会社の所在地、電話番号」の違いは？
- 秘密にしておきたいかどうか＝漏洩したら困るかどうか
- 無くなったら困るかどうか

- 要するに、どれだけビジネスにインパクトがあるか、ということ

あなたの会社の情報資産は何がありますか？

- 情報資産を挙げてください

情報資産はどこにあるのか？

- 紙の書類はどこにあるのか？
  - 紙の書類はどこにあるのか挙げてみてください

- コンピュータ上の書類（電子データ）はどこにあるのか？

会社、組織には
どんなコンピュータがあるのか

- **普通のコンピュータ**
- **ノートパソコン**
- **携帯電話**
- PDA
- **サーバー**

電子データはどこにあるのか？

- コンピュータの中 (一般利用者、サーバー)
- 携帯電話の中
- USBメモリの中
- CD、DVDの中
- フロッピーディスクの中
- コピー機、ファックス機、プリンターの中
- (一瞬ですが) ネットワークの中

電子データ、紙の書類はどこで使われているのか？

- 外出先
- 出向先
- 派遣先
- （アクセスポイント付き）喫茶、食べ物屋、居酒屋
- 電波が通る電車の中
- 自宅

- もちろん仕事場

情報資産は誰が使っているのか？

- プロパーの社員
- 関係会社、協力会社の社員
- 派遣会社の社員
- 個人事業主
- パートタイマー
- もちろん、取引先も

脅威とは何か

- 情報資産にダメージを与えるもの、現象
  - 漏洩しました
  - 暴露されました
  - 改ざんされました
  - 破壊されました
- 脅威の元になるものは何か？

脅威の元になるもの

- コンピュータへの不正アクセス
- ネットワークの盗聴
- 無線LANの盗用
- スパイウエア、アドウエアというもの
- しかし、最も多いのは内部関係者による過失、紛失、意識的な漏洩

現状での情報資産管理 (紙)

- 紙の書類はどう管理していますか？
- 文書管理規定はありますか？
- 重要書類、社外秘などのランク分けはされていますか？
- 廃棄方法については規定していますか？
- 複製については規定していますか？
- 持ち出しについては規定していますか？

現状での情報資産管理 (電子データ)

- 電子データはどう管理していますか？
- 電子データ管理規定はありますか？
- 重要書類、社外秘などのランク分けはされていますか？
- 廃棄方法については規定していますか？
- 複製については規定していますか？
- 持ち出しについては規定していますか？

紙と電子データの違い

	紙	電子データ
持ち出し	・手で運ぶ （紙を持ち出さなければならない）	・メール ・P2P（ファイル交換） ・Webブラウザ ・メッセンジャー ・USBメモリ ・CD,DVD ・携帯電話 ・PDA （非常に多い）
複製	・コピー機 ・ファックス機 （手間がかかる）	・ファイルコピー ・コピー＆ペースト （非常に簡単）

紙と電子データの違い2

	紙	電子データ
廃棄	・ごみとして出す ・シュレッダー処理 ・焼く	・ハードディスクから削除、消去 ・ハードディスクの破砕 ・コンピュータの破壊 ・CD,DVDの破砕 ・プリンター、コピー機のメモリからの消去 ・USBメモリからの消去、廃棄 ・フロッピーディスクの破砕 （各保存形態ごとに複雑かつ手間がかかる）

非常に手間がかかる電子データの管理

- これまでに挙げたようなことを考慮して、管理していますか？
- 内部の人の紛失や過失を防ぐことができますか？
- 内部の人の意図的な漏洩を防ぐことができますか？

漏洩が起きてしまったら

- 誰が漏洩させたのか、犯人を突き止めることができますか？
- 犯人を突き止めるのは警察ですか？
  - 警察は「民事不介入」
  - 警察といえども「証拠」が無ければわからない
- 犯人を突き止められなければどうなりますか？
  - 社会的責任？
  - 顧客への責任？
  - 犯人がそのままだったら、脅威もそのまま

犯人を突き止めるには？

- 証拠が必要。では証拠とは何か？
  - コンピュータ、電子データの操作記録
  - 複数のコンピュータの記録
  - 電子データが入っているコンピュータそのもの
- 適切に証拠となるようなものを記録しておき、かつ何か起きた場合には証拠を保全しなければならない
  - 紛失等も同じ

新しい業務形態のもたらすリスク

- 今や仕事場所はどこにでもある
- 出先のホットスポットからの利用
  - ホットスポットは危険だらけ (盗聴、不許可アクセス、ウイルス･ワーム感染、バックドア汚染)
- 自宅からの利用
  - ファイアウォールも無い環境が多い
  - 他の家人のリスクも背負い込む
- 出向先からの利用
  - 出向先のポリシーと対策レベルに依存する
  - VPNなどの安全な利用？

ネットワーク接続のリスク

- ネットワークに繋ぐということは、周囲の人に見られるリスクを背負い込むこと
- PCは勝手に待ち受けている
- 通信は盗聴される
- 日々大量の通信がやり取りされるため、どのような情報がどうやり取りされているのか見極めることは非常に困難（内部犯行を防げない？）

ネットワークのリスク

- ネットワーク盗聴
  - 暗号通信も例外ではない
  - 必ずしも内容を理解する必要は無い
- 無線LAN
  - 通信が暗号化すらされていない？
  - 電波はどこまで届くかわからない

最大の問題は？

- コンピュータのリスク（機能）を理解できないユーザーも、コンピュータ使用が仕事上必須になってしまったこと
  - 管理する側にとっては非常に辛い

- 理解している側がサポートを強めるか、サポートするためのより強力な技術的補助策が必要となってきている

2. 情報セキュリティの概念

1) 情報セキュリティの概念 (機密性、完全性、可用性)

2) 脅威、リスク、インシデント

3) 守るべき情報資産と脅威

4) インシデントの種類・原因・予防

情報セキュリティの概念

正当な権利をもつ個人や組織が、情報やシステムを意図通りに制御できること

情報の機密性、完全性及び可用性の維持

（情報セキュリティマネジメントシステムの国際標準であるISO/IEC17799の定義）

- ◆**機密性**：アクセスを認可された者だけが、情報にアクセスできることを確実にすること
- ◆**完全性**：情報および処理方法が正確であること及び完全であることを保護すること
- ◆**可用性**：認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること

脅威・リスク・インシデント

脅威　：情報の機密性・完全性・可用性を阻害する要因
リスク：脅威によって情報資産が損なわれる可能性
インシデント：実際に情報資産が損なわれてしまった状態

脅威（要因）

◆外部からの要因
- 侵入、サービス妨害
- ウイルス感染
- 盗難、輸送中の紛失
- 停電

◆内在する要因
- ソフトの脆弱性
- ソフト及びハードの信頼性
- 運用ルール違反、設定ミス

リスク

脅威の顕在化

インシデント（現象）

◆運用停止
（業務停止）

◆情報消失・破壊

◆不正アクセス
（改ざん、盗聴、なりすまし、踏み台）

◆情報漏洩

守るべき情報資産と脅威
ー基本的考え方 ～ 何から何を守るか？

情報資産
・システム　・ネットワーク
・ハードウエア　・ソフトウエア
・データ　・ノウハウ等

外部からの要因
・ウィルス等
・侵入
・サービス妨害

弱点（脅威）

内在する要因
・ソフトウエアの脆弱性
・セキュリティ機能の欠如
・セキュリティモラルの欠如等

組織

守るべきもの

◆ 情報
（紙、電子媒体、ネットワーク上）
財務情報、人事情報、顧客情報、
戦略情報、技術情報 等

◆ 情報システム
コンピュータ（パソコン、サーバー、
汎用機）、ネットワーク、通信設備

◆ 社会的信用

なぜインシデントはおこるのか？

ー外部からの要因と引き起こされる被害

インシデントの原因 (外部からの要因)	引き起こされる被害
ウイルス感染	情報漏洩、改ざん、破壊、なりすまし、コンピュータ不正利用、不正プログラムの埋め込み、踏み台
外部からの侵入 (不正アクセス)	
サービス妨害 1. Dos攻撃 2. DDoS攻撃	サーバーのパフォーマンスを極端に低下させたり、システムダウンに追い込む。
3. メール攻撃	メールサーバーのパフォーマンスが極端に低下したり、サーバーがダウンする。
盗難、輸送中の紛失	情報漏洩、情報消失
停電・火災などの	情報消失、破壊
台風・地震などの自然災害	情報消失、破壊

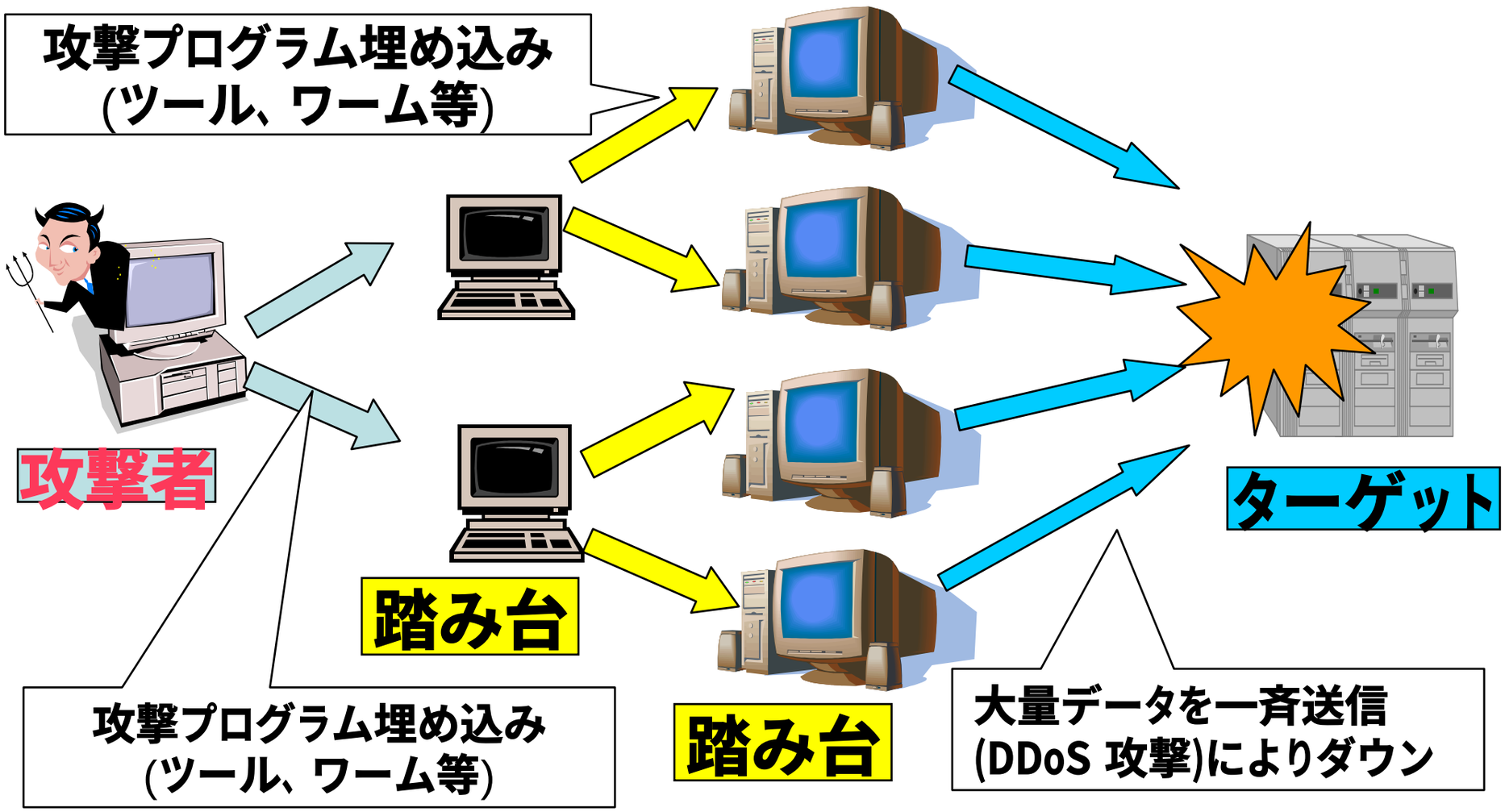
用語説明: 引き起こされる被害

不正行為	内　容
盗聴	ネットワーク上のデータや保存データを不正に入手。情報窃盗。 (例)・パスワードの盗用　・企業データの漏洩 ・個人データ(メール、日記など)の盗み見
改ざん	データを書き換え。(例)・Webページの改ざん、設定書換え
なりすまし	別の個人を装い、さまざまな行為を行う。 (例)・管理者になりすましてユーザのパスワードを取得 ・他人のクレジットカードでショッピング
破壊	データやプログラムの削除、ハードディスクの初期化など。
コンピュータ不正使用	コンピュータを不正に使用する。 (例)・コンピュータを遠隔地から操作　・夜中に自動的に起動
不正プログラムの埋め込み	不正プログラムには、ユーザの知らない間に情報を入手して外部へ送信したり、ファイルを破壊するなど様々な悪さを働くものがある。これらのプログラムを埋め込む。
踏み台	不正アクセスを行う際の中継地点として使用する。 (例)・アカウントを不正使用し他のサイト攻撃の拠点とする ・スパムメール(spam mail)の中継

用語説明: DDoS攻撃 (分散型サービス妨害攻撃)

DoS攻撃：サーバなどに大量の要求を出し過大な負荷をかけサービス不能に追い込む攻撃。DoS攻撃を多くのコンピュータから一斉に行うとDDoS攻撃

攻撃プログラムを埋め込まれて気づかずにDoS攻撃に加担することがある



なぜインシデントはおこるのか？

ー内部からの要因と引き起こされる被害

◆内在する要因

情報システムのセキュリティホール

1　**脆弱性とセキュリティホール**
2　**OSの脆弱性**
3　**Webブラウザやメールソフトの脆弱性**
4　**CGI, ASPの脆弱性**
5　**脆弱性を悪用する攻撃**

ソフト及びハードの信頼性

過失、運用ルール違反、設定ミス

内部犯行

脆弱性とセキュリティホール

脆弱性：情報システムのセキュリティ上の欠陥
セキュリティホールとも言う
ソフトウエアの設計もしくは実装上のエラーが原因

OS、Webブラウザ、メールソフトなどのソフトウェアにセキュリティ面での問題点（欠陥）があると、それが弱点となって、外部からの攻撃を受けてしまう。これをソフトウェアの脆弱性と呼ぶ。
ソフトウェアの脆弱性以外に、IDやパスワードのずさんな管理や、侵入されやすいシステムも、脆弱性があるといわれる。
一般的には、ソフトウェアの設計もしくは実装上のエラーが原因となるセキュリティ上の弱点を脆弱性といい、弱いパスワードや設定ミス、管理上の不備なども含んだ広い意味でのセキュリティ上の欠陥をセキュリティホールと言うことが多い。

情報セキュリティ対策をする上で
脆弱性は大きな問題になっている

参考図書：情報セキュリティ読本

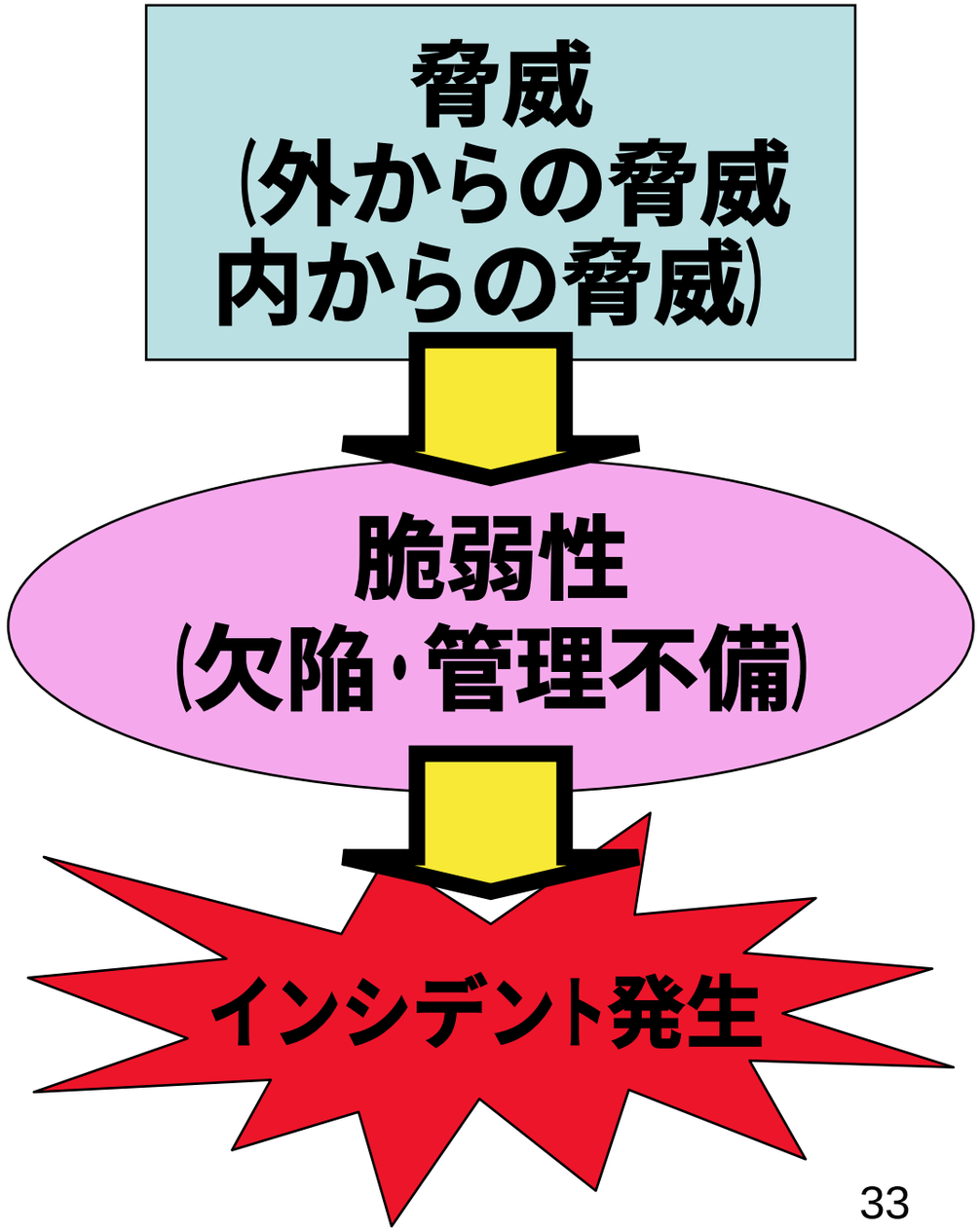
脅威と脆弱性

脅威と脆弱性のある状態=リスクを抱えている状態

・ウイルス　・不正アクセス
・ソフトの脆弱性
・ソフト及びハードの信頼性
・過失、ルール違反、内部犯行

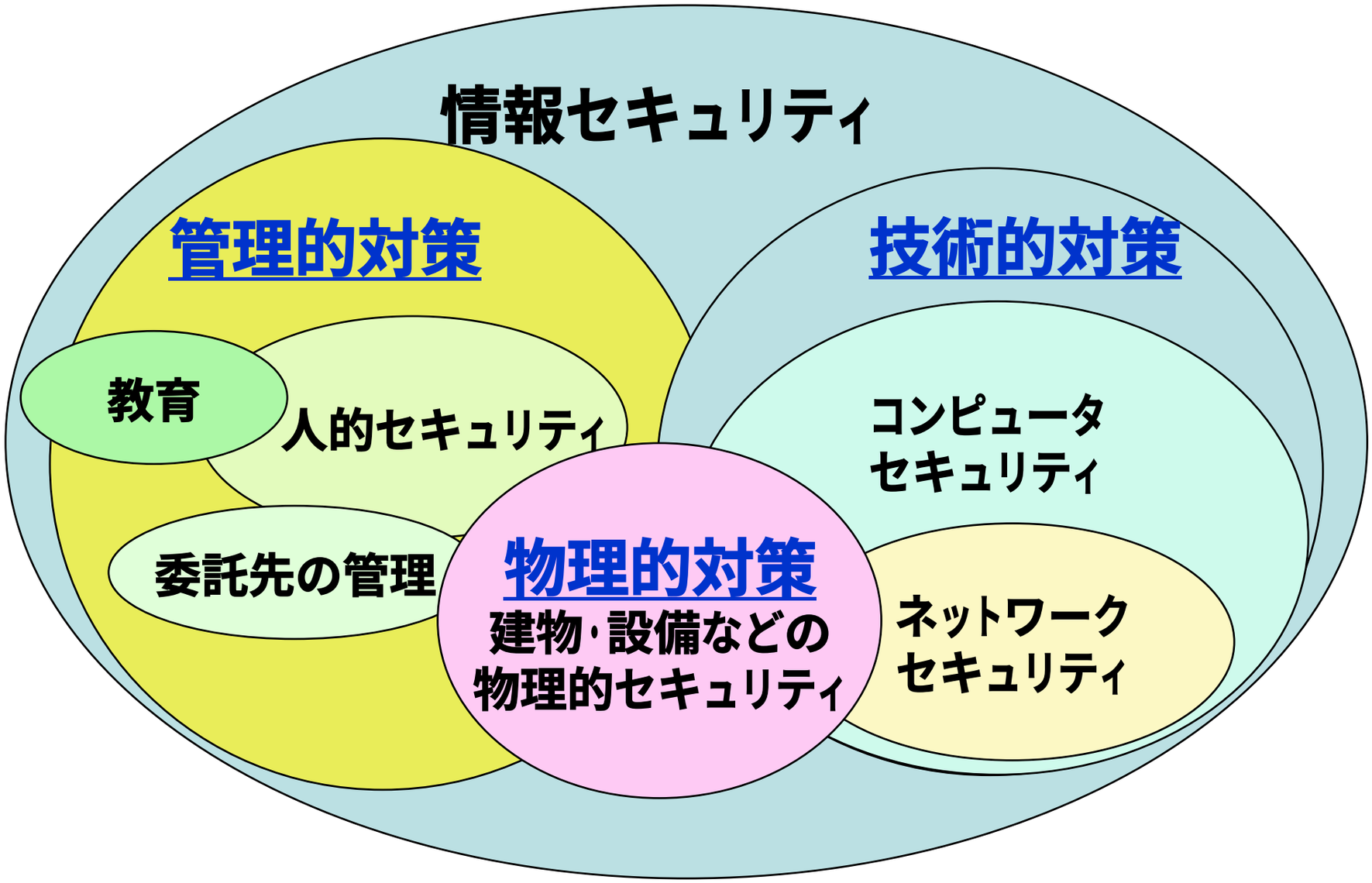
・ウイルスや不正アクセス対策不備
・脆弱性パッチ未適用、設定不備
・信頼性向上対策の不備
・管理対策の不備

・ウイルス感染
・不正侵入被害
・情報漏洩、盗難
・システム停止、業務継続困難



インシデントを防ぐために
ー 情報セキュリティ対策が必要

様々な要素を包含する情報セキュリティ



IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

実際のセキュリティ対策(1)

1. 対策を実施する上での指針
2. 対策の評価（費用対効果の考え方）

1. 対策を実施する上での指針

情報セキュリティ対策の目的・機能・多面性

セキュリティ対策の目的：機密性、完全性及び可用性の維持

セキュリティ対策の機能

- **抑止**：不正を働く気持ちを抑制する
- **防止**：脅威が現実の事故になるのを防止する
- **検知**：セキュリティ事故を発見する
- **回復**：セキュリティ事故からの復旧・回復

セキュリティ対策の多面性

- **技術的対策**：製品の導入や設定
- **管理的対策**：ポリシー、運用規定、教育など
- **物理的対策**：建物、施設、装置などへの保護

様々な情報セキュリティ対策

確保すべきもの	脅威	技術的対策	管理的対策
機密性	不正アクセス 情報漏洩 盗聴 プライバシー侵害 コンピュータウイルス	暗号化(暗号技術) 認証技術 アクセス管理技術 アクセス制御技術 ウイルス検出/除去技術	セキュリティポリシー (周知徹底・教育) 利用者管理 入退室管理 秘密保持契約 情報収集 (脆弱性情報 新技術情報 攻略方法 標準・法規) 情報のバックアップ 運用体制 (修正プログラム適用 パターンファイル更新 バックアップ計画) 教育 脆弱性検査 セキュリティ監査 緊急時対応計画 コンプライアンス 見直し
完全性	不正アクセス 改ざん、変更 破壊、削除 操作ミス コンピュータウイルス	電子署名 改ざん検出技術 改ざん防止技術 ウイルス検出/除去技術	
可用性	不正アクセス DoS攻撃 地震　火災 ハードウエア障害 誤作動、 コンピュータウイルス	認証 二重化、負荷分散 アクセス制御技術 ウイルス検出/除去技術 QoS技術	

情報セキュリティ対策を選択する

- 数多い情報セキュリティ対策
  - 何を選んだらいいのかわからない
  - 予算がどのくらい必要なのかわからない
- 対策を考える上で最初に行うことは何か？
- 対策を考える上で指針となるものは何か
  - リスク分析を行って、自社に最もインパクトがあるリスクは何なのか認識する
  - 対策費用が被害額を超えないようにリスクの容認も考慮する

リスク分析の前提

- リスク分析は以下のような手順で行われる
  - 情報資産の洗い出し
  - 情報資産の価値付け
  - 各資産ごとのリスクの洗い出し
  - 洗い出せたリスクのマージ
- 特に「価値付け」が最も難しい部分

価値付けがなぜ難しいのか？

- 金銭的価値、経済的価値を考えるから難しい
  - オカネには置き換えられない？
  - 重要なのはプライオリティをつけること
- プライオリティをつける方法は？
  - 実感できるリスクの程度を「印象」や「経験値」で判断する
  - チェックリストや対策実践情報を利用する
  - 点数化する

被害金額を想定する

損害賠償額 ＝ 漏洩個人情報価値
×社会的責任度
×事後対応評価

＝（基礎情報価値×機微情報度×本人特定容易度）
×情報漏洩元組織の社会的責任度
×事後対応評価

＝ 基礎情報価値　[500]
×機微情報度　[Max($10^{x-1}+5^{y-1}$)]
×本人特定容易度　[6, 3, 1]
×社会的責任度　[2, 1]
×事後対応評価　[2, 1]

数式 5-5：個人情報漏洩事件による損害賠償想定額の算出式［算出式('03)］

- **個人情報漏洩時の損害賠償額を想定する方法**
  - JNSA**方式**（2003**年方式、**2002**年方式**）
  - U**市の判例**
  - **コンビニエンスストア、**ISP**の手当て例**

2003**年度**JNSA**方式の損害賠償想定額算出式（出典：**2003**年度情報セキュリティインシデントに関する調査報告書；**JNSA、2004**年3月**）

2003年度JNSA方式の各パラメタ

基礎情報価値	500（固定）
機微情報度	MAX（$10^{x-1} + 5^{y-1}$） Simple-EP図を参照し算出
本人特定容易度	個人を簡単に特定可能＝6 コストをかければ特定可能＝3 特定困難＝1
情報漏洩元組織の社会的責任度（業種、公的性格などによる）	一般より高い＝2.0 一般＝1.0
事件後の対応姿勢	不適切な対応＝2.0 適切な対応、もしくは不明＝1.0

情報機微度のSimple-EP図

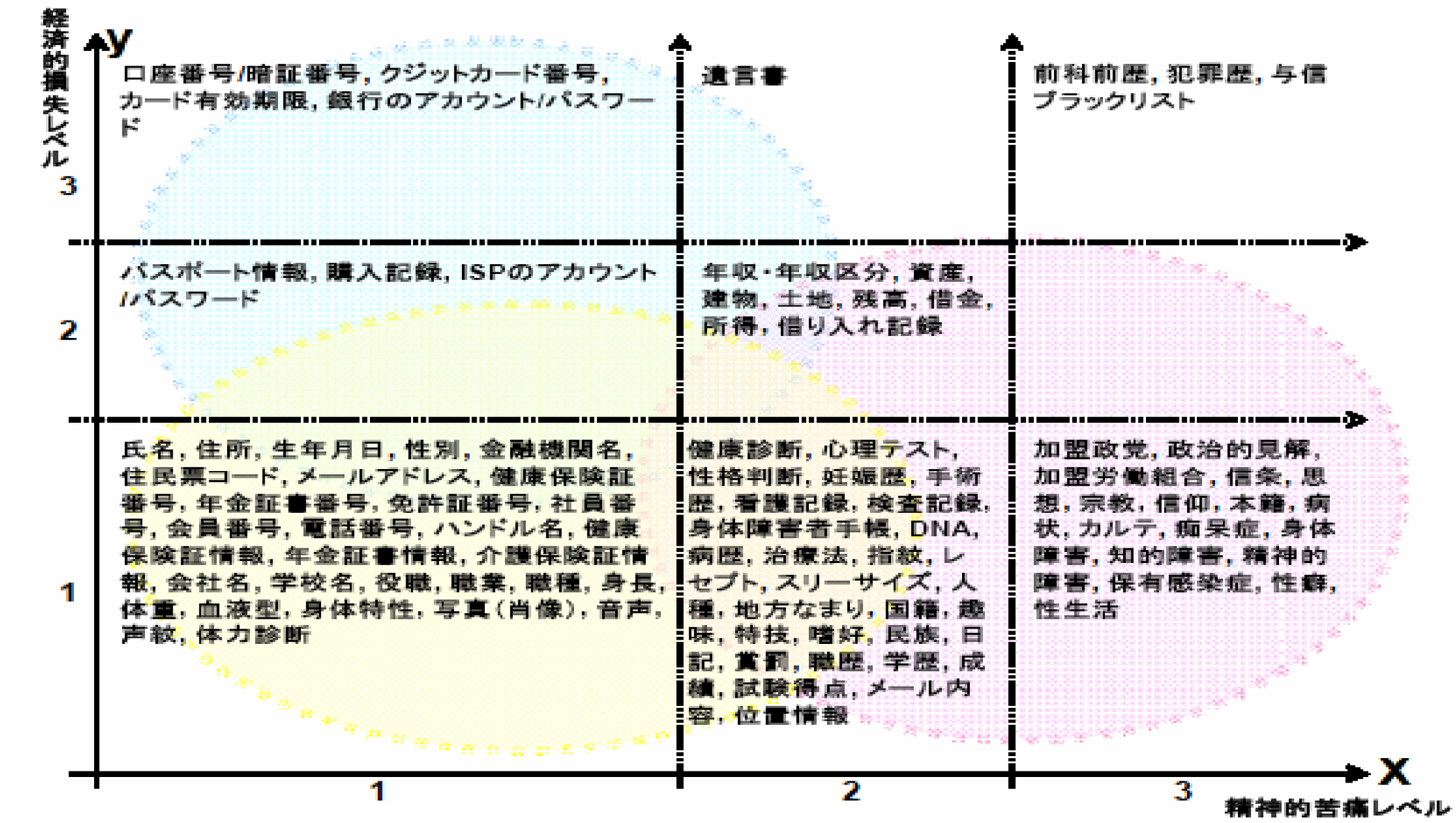


図 5-4 : Simple-EP 図

2003年JNSA方式の算出式

計算式は各5項目をすべて掛け合わせて1件当りの賠償額(想定)を出すもの。基礎価値は(500)、機微情報度は(＝2.0)、本人特定容易度は氏名住所アリで容易(＝6.0)、一般よりも社会的責任度が高い組織で(＝2.0)、事件後の対応姿勢が適切(＝1.0)の場合、500×2.0×6.0×2.0×1.0で1件12000円となる。

- **想定漏洩件数を入力させ、JNSA方式による1件当りの金額を掛け合わせて最大総額の計算を行う**
- **過去事例に基づく訴訟発生率(漏洩件数に対し、何人の被害者が損害賠償訴訟を起こしたか)と最大総額を掛け合わせ、訴訟に発展する可能性が高い金額の算出を行う**
  - **過去事例：U市では漏洩総数22万件に対し、訴訟となったのは3件のみ。某エステサロンでも3万件に対し10数件のみ(ただし1件100万円の請求)**

その他損害として想定すべき金額

- 株価変動、業務停止期間中の遺失利益など
- ブランド価値の下落
- 見舞金、お見舞い諸経費など
- 対策費用
  - 訴訟対策
  - セキュリティ対策
  - 広報費
  - 苦情対策費
- 漏洩による損害想定＝資産価値

情報漏洩事故の原因分析

No.	要素	原因	%	対応する要因
1	技術的	人為ミス	46	設定ミス、誤操作、管理ミス
2	技術的	対策不足	11	バグ･セキュリティホール、不正アクセス
3	非技術的	人為ミス	2	置き忘れ
4	非技術的	犯罪	25	内部犯罪、情報持ち出し、盗難
5	その他	その他･不明	16	その他･不明

情報漏洩の原因分析

出典：2003**年度情報セキュリティインシデントに関する調査報告書**（JNSA　2004**年3月**）

原因別詳細分類

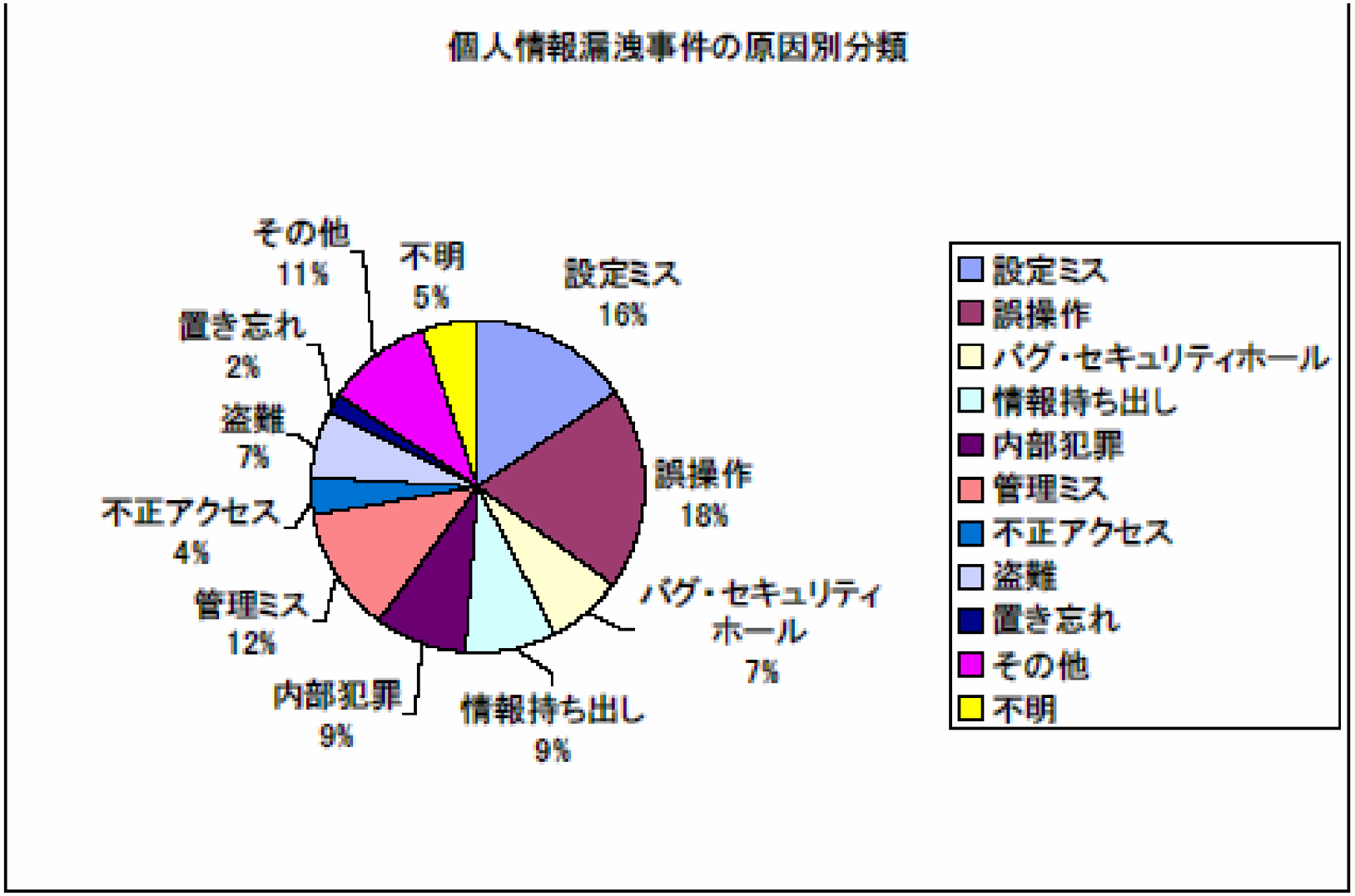


図 4-3：情報漏洩原因

情報漏洩の原因分析

出典：2003**年度情報セキュリティインシデントに関する調査報告書**（JNSA　2004**年3月**）

原因分析からわかること

- 内部スタッフが原因に関与する割合が非常に多い
  - 不明、その他、盗難、不正アクセスを除くと73%
  - 閲覧権限を持っているので、リスクを背負っている
- 73%内の傾向
  - ミスが多い（対策不足も含めると59%）
  - 内部「犯罪」は9%のみ
- その他、不明の中にも潜在的に内部スタッフの関与が想定されるものが多いと予想される

ここまでのまとめ

- 情報資産を洗い出した
- 現状の情報資産の管理･運用を把握した
- 想定被害金額などをもとに情報資産に価値をつけた（対策の優先度を決める）
- 情報漏洩事例をもとに、事故発生の原因について傾向を見た

リスクと情報セキュリティ対策との関係

- 例えば、情報漏洩の原因分類を列挙してみる
  - 設定ミス、誤操作、バグ・セキュリティホール、情報持ち出し、管理ミス、内部犯罪、不正アクセス、盗難、置き忘れなど
- 一般的な管理策（情報セキュリティ対策）が、列挙した漏洩原因に対してどのくらい効果を発揮しそうか、印象をもとに5段階評価、3段階評価を行ってみる
- 最も点数が多い対策が、最も効果が高い管理策
  - コストパフォーマンスを考える場合には、管理策ごとに1点あたりいくらかかるのかを調べてみる

情報セキュリティ対策集を参照する

- ISO/IEC17799、**あるいは**ISO/IEC TR13335 (GMITS) **に記載の管理策 (情報セキュリティ対策) を参照して対策を考える**
- IPA**の**Web**サイトの読者層別情報セキュリティ対策実践情報を参照して対策を考える**
  (http://www.ipa.go.jp/security/awareness/awareness.html)
- **総合的なソリューションベンダーの対策メニューを見てみる**

IPAの対策実践情報

ITユーザ向け	情報システム部門責任者の方	組織の経営管理者に認識していただきたい諸論点をご紹介します。
	システム管理者の方	サイトにおけるシステム管理者／ネットワーク管理者およびシステムインテグレータのエンジニアを対象に、対策や資料をまとめています。
	SOHO（小規模サイト）の管理者の方	特に自身の小規模なサイトにおいてインターネットサーバーを運用管理している方を対象とした情報です。
	エンドユーザ・ホームユーザの方	ご家庭でコンピュータを利用するホームユーザ、組織において情報システムを利用するエンドユーザに向けた情報です。
	ネットワークサービス事業者の方	ネットワークサービス事業者のネットワーク管理者を対象とした情報です。
ITベンダ向け	ソフトウエア開発者の方	セキュリティエンジニアリングに関する情報です。ソフトウェアやファームウェア（組込みソフトウェア）の開発に携わるプロジェクト管理者、設計者およびプログラマ向けです。

2. 対策の評価 (費用対効果の考え方)

情報資産と管理策の照らし合わせ

- プライオリティが高い情報資産と、その資産が必要とする管理策の照らし合わせを行う
  - コストパフォーマンス
- 最後に問題になるのは管理策のコストと予算枠

リスクと管理策の関係から対策のコストパフォーマンスを測定

	コスト	内部犯行	外部からの侵入者対策	スタッフのミス	評価	1点の値段
物理的な出入り	400万円	△	◎	ー	6点	66万
手順書作成	600万円	○	ー	◎	8点	75万
委託先とのセキュリティ契約	150万円	◎	△	○	9点	16万

◎＝5点、○＝3点、△＝1点、ーは0点。

横軸の対策に対し、縦軸に設定されたリスクのどこにどれだけ効果があるかを任意に記入していく。それを積算して1点あたりのコストとして導き出すと、コストパフォーマンスの指標とすることができる

そして上位10個の対策を実施するなどの方針のもと、予算に応じて検討していけば、プライオリティと予算、パフォーマンスという検討が可能

関係表のバリエーション

- 縦軸（脅威）をもう少し細かくしてみる
  - 一般利用者のPCから漏洩するリスク
  - サーバーから漏洩するリスク
  - ネットワーク盗聴などが原因で漏洩するリスク
- 脅威のスケール感に関わらず、すべて列挙すると、個別の対策それぞれのリスクへの実感的な影響度が見えてくる

関係表バリエーション

	コスト	一般PCのリスク	サーバ漏洩	ネットワーク	評価	1点の値段
管理手順書作成	200**万円**	△	◎	△	7**点**	29**万**
IDS	150**万円**	○	**ー**	◎	8**点**	19**万**
クライアントPC操作記録	300**万円**	◎	○	△	9**点**	33**万**

◎＝5点、○＝3点、△＝1点、ーは0点。

予算の枠内で、どこに優先的に投資するか、カテゴリー別に比較するとわかりやすい。
全体のバランスを見る場合には、縦軸はスケール感にとらわれず列挙する

実際にあるコストパフォーマンスを測定する方法

- ROSI：Return On Security Investment
  (http://www.macnica.net/lanch/lanch56/se01.html)
  - **年間予想損失＝資産価値×リスク係数×年間発生率**
  - **対策の価値＝年間予想損失×対策を施したことによるリスクの軽減率**

- **対策の費用対効果＝リスクの脅威への値付け**

情報セキュリティ対策予算

- **総務省の調査結果**
  ⑴http://www.soumu.go.jp/s-news/2004/040705_2.html⑵
  - **上場企業におけるセキュリティへ対策関連の投資額は、**100**万～**500**万円未満が**34.2**%と一番多い。**
  - **次に**1000**万円～**5000**万円未満が**18.7**%と多くの投資を行っており、企業の意識の高さが見られる。**
  - **セキュリティへと投資を行っていない企業が、全体の**7.1%**を占める。**
  - **自治体、大学では、**100**万～**500**万円未満が一番多く、それぞれ約**46**%、約**35**%を占める。**
  - **病院では、セキュリティ対策の投資を行っていない企業が、約**49**%を占める。**
  - **研究機関では、セキュリティ投資額が**100**万円未満の企業が一番多く、全体の約**40**%を占める。**

IT予算全体

- **経済産業省の情報処理実態調査**
  (http://www.meti.go.jp/policy/consumer/press/0005547/index.html)
- **回答**4,491**社、企業規模の平均は、資本金規模**6,834.7**百万円、年間事業収入規模**66,969.5**百万円、従業員規模**875.7**人である**
- **1企業当たりのIT投資額は4年ぶりに増加 平成**14**年度におけるIT投資の事業収入に占める割合は**1.4%**(前年度比**0.1**ポイント増)となり、対事業収入比は平成**10**年度以降5年連続の上昇となった。 また、1企業当たりのIT投資額は、平成**11**年度以来4年ぶりの増加となり、1企業当たり**9**億**2,854**万円(前年度比**15.6%増)**

予算枠と対策選定

- 対策は各側面から見てプライオリティが高い順に選定していく
  - 企業規模、予算規模に合わせて選定
  - 最低限選択すべき情報セキュリティ対策については、以降のセッションや前掲の参考資料を参照してください

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

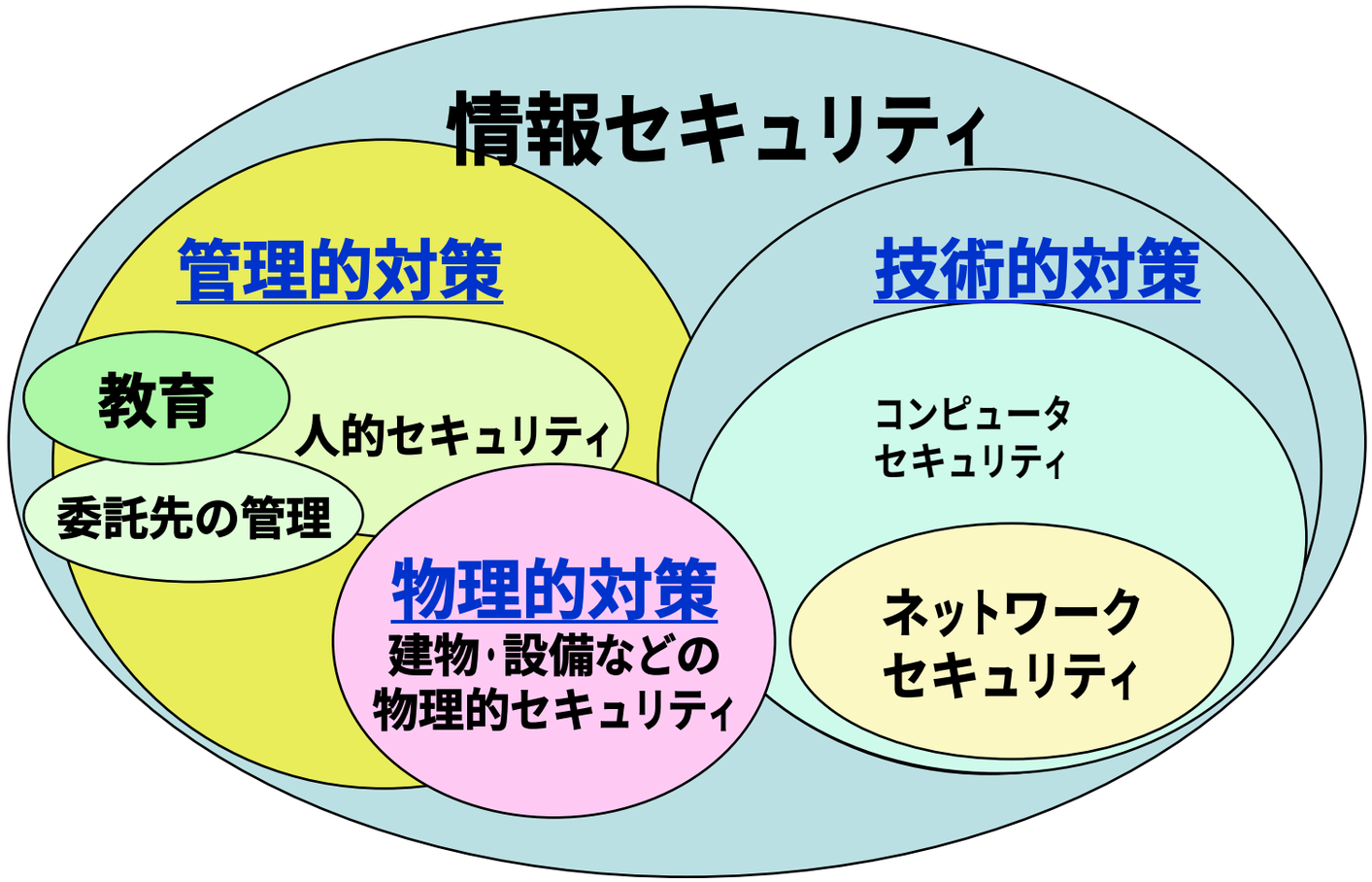
実際のセキュリティ対策(2)

1. 社内コンピュータユーザの行うべきセキュリティ対策
2. 組織ネットワークをセキュリティの脅威から守るための対策
   1) 技術的対策
   2) 管理的対策
   3) まとめ

情報セキュリティ担当者･責任者の行う対策

組織ネットワークをセキュリティの脅威から守る
社内ユーザのセキュリティ対策を支援・教育する

1) **技術的対策**
2) **管理的対策**
3) **物理的対策**



社内ユーザのセキュリティ対策の支援と教育

社内ユーザの行うセキュリティ対策

1) **ウイルス対策**
2) **セキュリティホールの解消**
3) **Webブラウザのセキュリティレベルの設定**
4) **ネットサーフィンの危険についての認識と対策**
5) **メールの利用に伴う危険と**
   メールソフトのセキュリティレベルの設定
6) **メールの暗号化とディジタル署名の利用**

情報セキュリティ対策には個々のコンピュータユーザが行う対策と、企業レベルで行う対策があります。情報セキュリティ担当者は、社内コンピュータユーザが行うべきセキュリティ対策を社内のユーザに周知徹底し、確実に行えるようにサポートする必要があります。

社内コンピュータユーザの行うセキュリティ対策
ー 1) ウイルス対策　2) セキュリティホールの解消

セキュリティ担当者は、ユーザへ対策の意義と方法を周知徹底

1) **ウイルス対策**　　2) **セキュリティホールの解消**

1. **ウイルス感染の症状や感染により受ける被害について周知する**
2. **なぜウイルスに感染してしまうのかを周知する**
3. **なぜセキュリティホールの解消が重要なのか理解させる**
3. **実際の対策を徹底し、実行できるようにサポートする**
4. **ウイルスに感染した場合の対処方法を周知する（駆除と復旧）**

ウイルス対策の基本

予防：ウイルスに感染しないように対策する
発見（検知）：（感染前に）ウイルスを検知する
駆除：ウイルスを検知したら駆除する
復旧：ウイルス感染から復旧する

社内コンピュータユーザの行うセキュリティ対策
ー3)Webブラウザ 4) ネットサーフィン 5) メールの利用

3) Webブラウザのセキュリティレベルの設定
4) ネットサーフィンの危険についての認識と対策
5) メールの利用に伴う危険と
メールソフトのセキュリティレベルの設定

1. ネットサーフィンの際に遭遇する可能性のある危険や安易なダウンロードがもたらす被害について周知する
2. Webブラウザのセキュリティレベルの設定について教育する
3. メールの利用に伴う危険について周知し、危険を回避するための方策について教育する
4. 特にメールの添付ファイルへの注意を促す

具体的な対策方法は「インターネットに潜む危険」を参照

社内コンピュータユーザの行うセキュリティ対策
ー 6) メールの暗号化とディジタル署名の利用

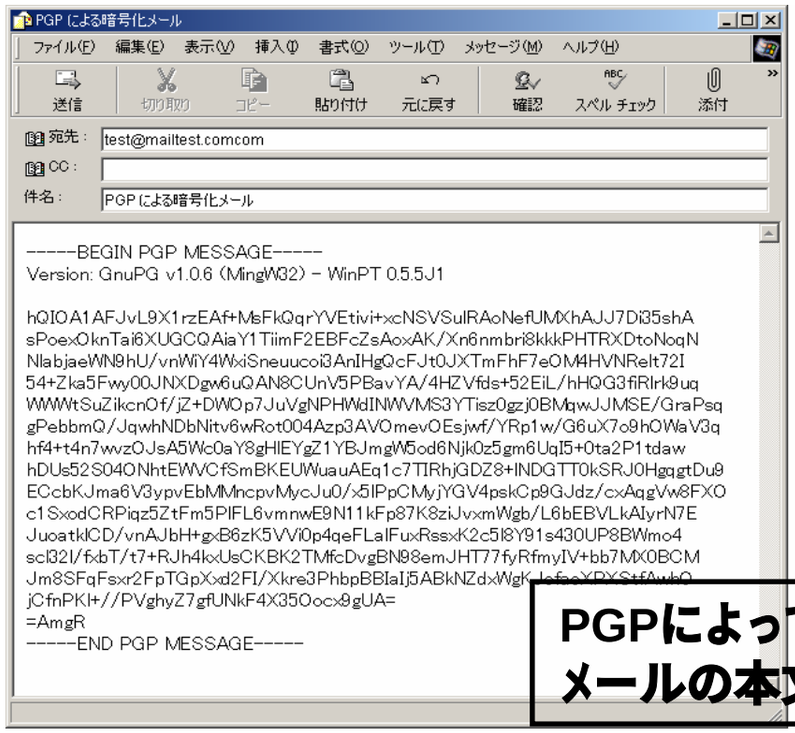
メールの暗号化とディジタル署名を使用すると、なりすまし、改ざん、盗聴などの不正行為を封じることができます。現在暗号化に利用できるものには、
PGPとS/MIMEなどがあります。

- メール本文を暗号化し、内容を第三者に読まれないようにする (盗聴の防止)
- メッセージダイジェストにより、受信メールの改ざんの有無を確認する (改ざんの検証)
- ディジタル署名により差出人が本人であると証明できる (なりすましの防止)

暗号化メールは機密情報を扱う時など必要に応じて導入

PGP ：フリーのソフトウエア
公開鍵の正当性は本人同士が確認

S/MIME：電子メールを暗号化する際のプロトコル。
この約束事で定められた仕様に沿ってS/MIMEを実装したメーラーを使う。
公開鍵の正当性を認証局が証明 (有料)



PGPによって暗号化したメールの本文

社内ユーザへの教育と周知の方法

- 教育の2つの側面
  - 社内の情報セキュリティポリシーを周知徹底する
  - コンピュータ使用に際し遭遇する危険やその対策方法について教育する

→ 情報セキュリティ読本の活用

- 教育の方法
  - 定期的な教育（新入時、中途採用時など期日を決める）
  - 派遣社員の教育や外注先の教育状況にも留意
  - 集合教育、各種ポスター掲示、メールによる通知等

組織のネットワークを守るための対策

技術的対策・管理的対策・物理的対策

1) 技術的対策について知る

適切な対策を選択するために、技術的対策の概要を知り、
対策の重要度や必要性を理解する必要がある。

2) 管理的対策の全容を知り、取捨選択する

セキュリティ事故は管理的対策の不備や間隙を突いて発生
することが多くなっています。漏れの無い対策を行うために、
管理的対策をリストアップし、取捨選択する必要がる。

3) 物理的対策

情報の入れ物としての装置や事務所、建物の安全策も必要。

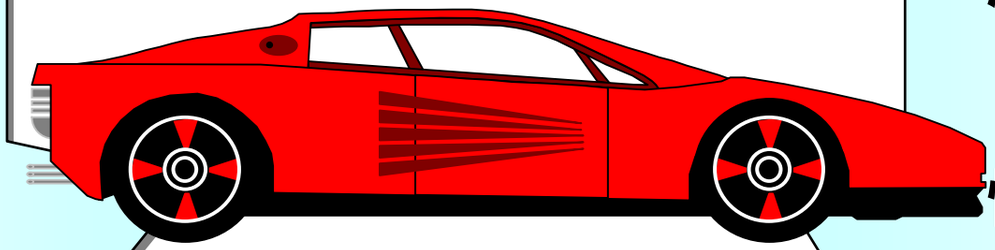
技術的対策と管理的対策

技術的な対策

- ワクチンソフト
- ファイアウォール
- ネットワーク監視(IDS)
- 利用者認証
- 情報の暗号化
- セキュアOS

セキュアな設計

情報セキュリティの確保には
①技術的な対策
②マネジメント的な対策
の両輪が必要



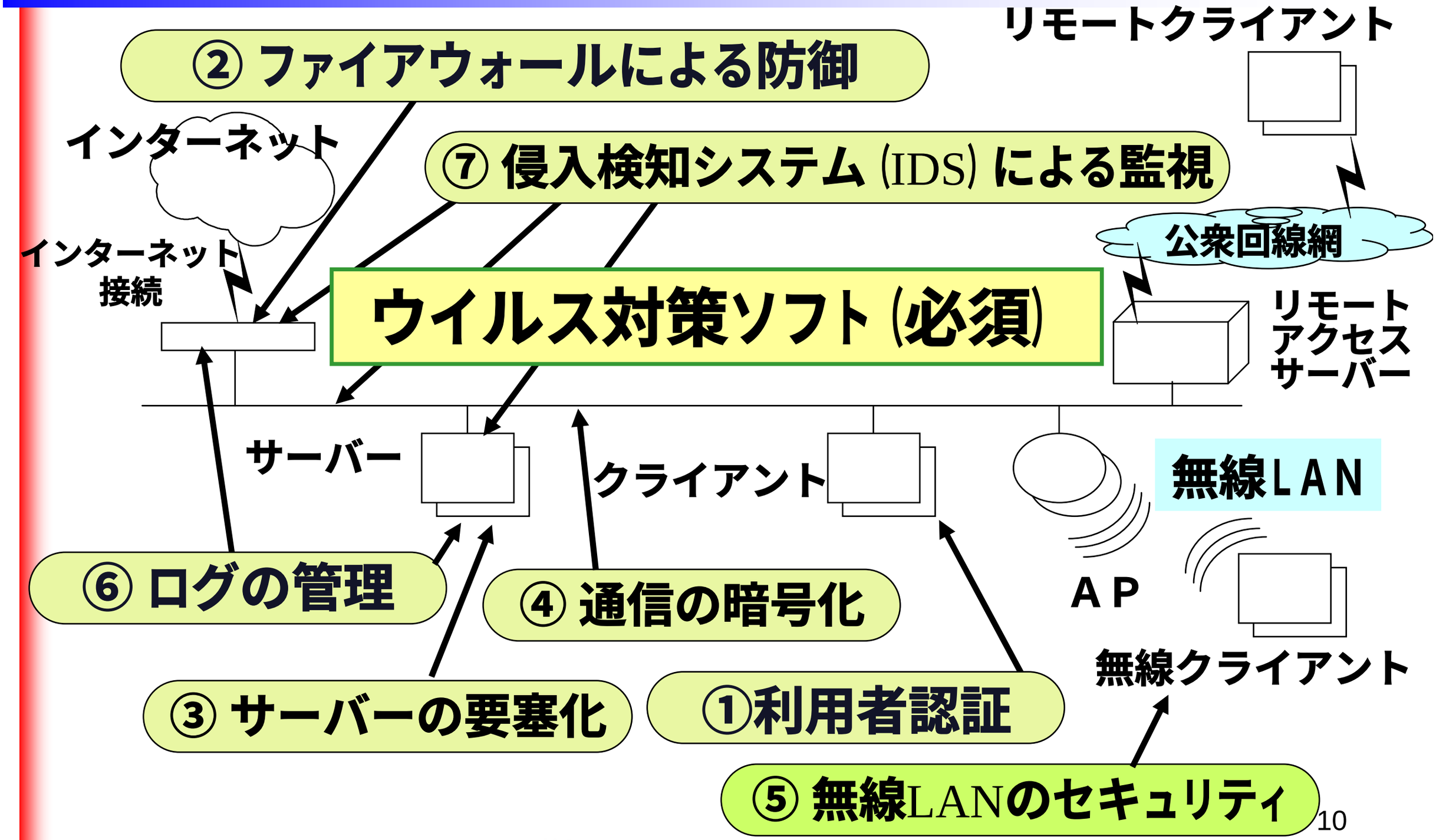
管理的対策

- 利用者管理
- 入退室管理
- 脆弱性情報の収集と修正プログラム適用
- 情報のバックアップ
- 教育　・委託先の管理
- 脆弱性検査　・監査

セキュアな運用

リスク評価→リスクマネジメント→業務継続管理

技術的な対策の概要



セキュリティ対策の基本
― 多重防御と最小権限

多重防御 ー1ヶ所が破られてもセキュリティを確保

・ファイアウォールを通り抜けた攻撃パケットがサーバーに到達しても
サーバーの要塞化により重要データへアクセスできなかった
・内部犯行者がネットワーク上を流れる情報を盗み見ようとしても、
データが暗号化されていたため、情報が漏洩しない

最小権限 ー権限の付与は必要最小限に留める

IDやパスワードによる認証と権限付与はセキュリティ対策の基本

認証（本人確認）：情報にアクセスを許可された人を認証する
権限付与：情報に対する権限の設定　→　読む(r)、書く(w)、実行(x)
　　読む(r)：情報を見ることができる
　　書く(w)：情報を書き込むことができる
　　実行(x)：情報の修正、変更、削除などあらゆることが可能

技術的な対策① ー 利用者認証

IDやパスワードによる本人認証は、セキュリティ対策の基本
アクセスを認可された者だけが情報にアクセスできることを確実にする
IDやパスワードを適切に管理されてこそ効力を発揮

ネットワークやシステムは、誰にでも利用（アクセス）を認めているわけではない。
利用できるユーザを限定し、ユーザによって利用できる範囲（権限）を決めている。
利用権限のことを「アカウント」と呼び、ユーザに利用権限を与える口座がアカウント。
IDは個人を識別するための番号。システムはIDを使用して、どのユーザが接続しているかを知る。パスワードは、正しいユーザ（本人）であることを示す証明となる。

本人確認のために使うもの

本人が記憶しているもの:	パスワード
本人が所持しているもの:	IDカード
本人に特有の特徴:	指紋

適切なパスワード設定は「インターネットに潜む危険」を参照

利用者認証のための手法

- **ワンタイムパスワード**

  使い捨てのパスワード。ユーザがシステムにアクセスするたびに、新しいパスワードを作成して使うための装置。新しいパスワードは一回限り有効なので、ワンタイムパスワードと呼ばれる。

- **バイオメトリックス**

  生体的、行動的特徴による利用者の正当性の確認
  (指紋、虹彩、静脈、筆跡、キーストローク等)

- **メモリデバイス**

  本人しか携帯できないデバイスによる利用者の正当性の確認
  (スマートカード、USBトークン)

- **PKI (公開鍵基盤)**

  ICカードに電子証明書を格納

本人認証技術の現状に関する調査 (2003年7月更新)
http://www.ipa.go.jp/security/fy14/reports/authentication/index.html

技術的な対策② ー ファイアウォール

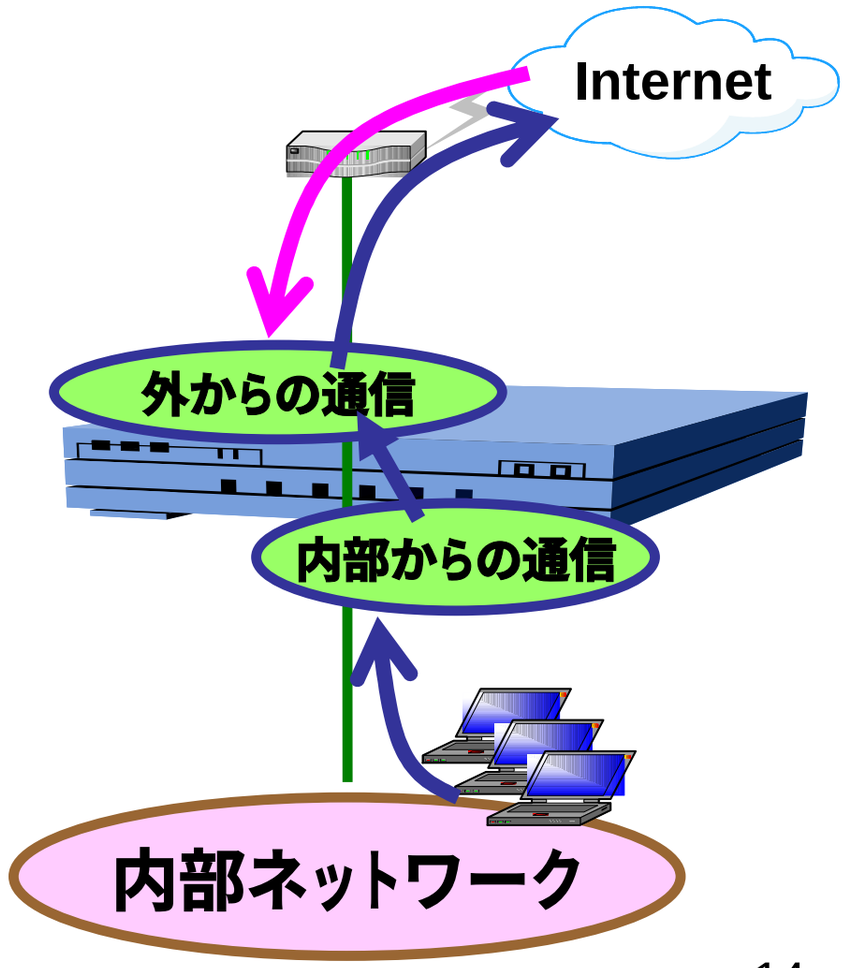
IPフィルタリングやアプリケーションプロキシ等のアクセス制御方式により不正アクセスから内部ネットワークを静的に防御する装置

設定ポリシーに規定されたアクセス制限を実装

通信ネットワークの内と外のネットワークの境界線（ルータの後ろ）に置き、外部から内部ネットワークに侵入されるのを防ぐシステム

IPアドレスやポート番号によるアクセス制御を実施

ファイアウォールについては「情報セキュリティ読本」参照



技術的な対策③ ー サーバーの要塞化

IPA

ファイルの改ざん･削除防止のためサーバー自体に施すセキュリティ対策
正当なﾄﾗﾌｨｯｸに見せかけてﾌｧｲｱｳｫｰﾙを素通りした攻撃にも有効

サーバーの要塞化とは

サービスを提供しているサーバーが、
それぞれの環境において自身を守るために適切なセキュリティ対策を行うこと

例：不要なサービスの停止

不要なサービスがあればリスク増大
デフォルト設定は最大限利用可能な状態
→ 提供すべきサービスを把握
→ デフォルト設定の見直し
→ 不要なサービスを停止する
＝ サービスを提供しているポートを閉じる

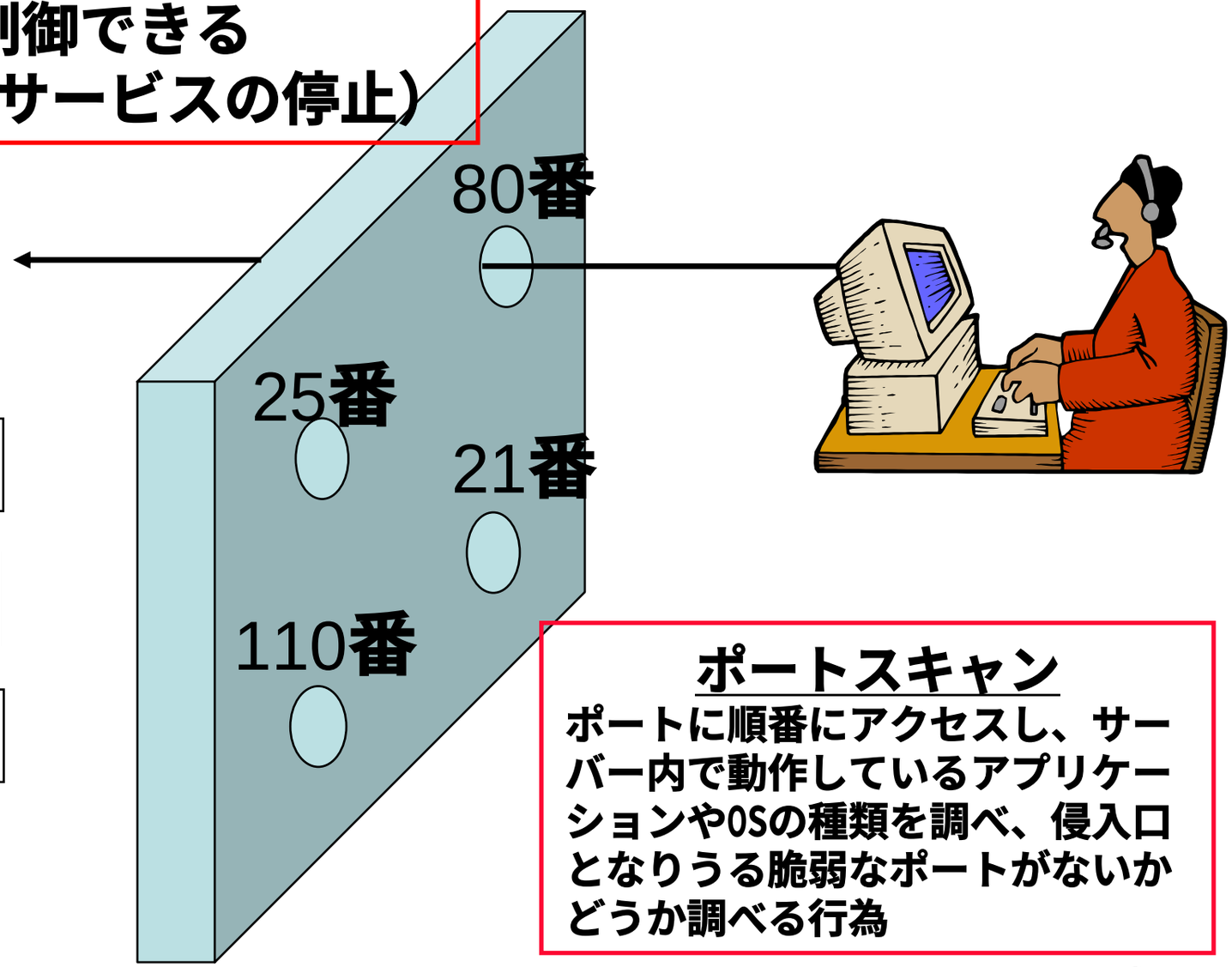
用語解説：サービスとポート番号

ポート：通信プロトコル（= サービス）を区別するための番号

開いているポートが分かれば、提供しているサービスが分かる

ポートは閉じたり開いたり制御できる
→ 不要なポートは閉じる（サービスの停止）

- **WWWプロトコル**（HTTP）
- **メール送信プロトコル**（SMTP）
- **ファイル転送プロトコル**（FTP）
- **メール受信プロトコル**（POP3）



ポートスキャン

ポートに順番にアクセスし、サーバー内で動作しているアプリケーションやOSの種類を調べ、侵入口となりうる脆弱なポートがないかどうか調べる行為

技術的な対策④ ー 通信の暗号化

データの暗号化により通信の機密性を確保　盗聴(情報漏洩) 防止
VPN (Virtual Private Network)よる仮想私設網構築のための基礎技術

暗号技術を使ったセキュリティ対策

1) メールの暗号化
PGP, S/MIME

2) インターネットVPN (IPSec)
主に拠点間接続で利用、モバイルでのクライアント接続も可能。
ほぼすべてのサービスが利用可能。

3) SSL-VPN
モバイルアクセスでのクライアント接続に限定。
Webブラウザを使用して専用クライアントなしで接続可能。
ただし、利用可能なサービスは限定される。

4) IP-VPN
通信事業者が提供するVPNサービス。

技術的な対策⑤ー無線LANのセキュリティ

無線LANには「通信の盗聴」「 無線LANの不正利用」等の危険性がある。
セキュリティ対策を徹底する必要がある - 事例参照

設定項目	設定内容	備考
SSID設定	工場出荷状態のSSIDから変更する	SSIDは機種、使用者/部署/企業名等を推測しにくい値に変更する (空白、ANYはNG)
WEPキー設定	104bit(128bit)以上のWEP暗号を有効にする	WEPキーは推測しにくい値に定期的に変更する。SSIDから推測できる値は避ける
MACアドレス認証	MACアドレス認証により端末を制限する	
拡張ユーザー認証 (オプション)	拡張ユーザー認証を導入・強化する	802.1xなど

*拡張ユーザー認証の方式：EAP (Extensible Authentication Protocol) 、EAP-MD5、LEAP (Light EAP) 等

技術的な対策⑥ ー ログの管理

**ログを収集･監視･分析することは、自組織のネットワークに
異常がないかどうかを検出し、セキュリティ対策をする上で重要である。**

- 必要な情報を収集するようにログを設定する
- ログサーバーで集中管理
- ログを安全に保管する (改ざん、削除を防止)
- ツールを利用して分析する
- 詳細な監査ログ
- 時計の同期 (照合のため)
- 普段からチェックし正常時を把握しておく

ログに記録する内容 (例)

一般

・利用者ID、ログオンとログオフの日時、 (可能なら端末のIDや場所の識別)
・アクセスの成功と失敗の記録 (システムへのアクセス、データや資源へのアクセス)

許可されているアクセス

・利用者ID、事象の日時、事象の内容
・アクセス対象ファイル、使用したプログラムとユーティリティ

特権操作

・スーパユーザアカウントの使用　・システムの起動及び停止
・入出力装置の取付け、取外し

無許可のアクセス

・失敗した試みと回数　　・侵入検知システムからの警告
・ネットワークゲートウェイやファイアウォールのアクセスポリシ違反と通知

システム警告や障害

・コンソール警告やメッセージ、システムログ例外事項、ネットワーク管理アラーム

技術的な対策⑦ ー 侵入検知システム

侵入検知システム（IDS）は、動的な攻撃パターンをデータベースに持つことにより、DDoS攻撃、メール爆弾、トロイの木馬、バッファオーバフローなどの動的な攻撃に対しネットワーク資源を保護する装置。

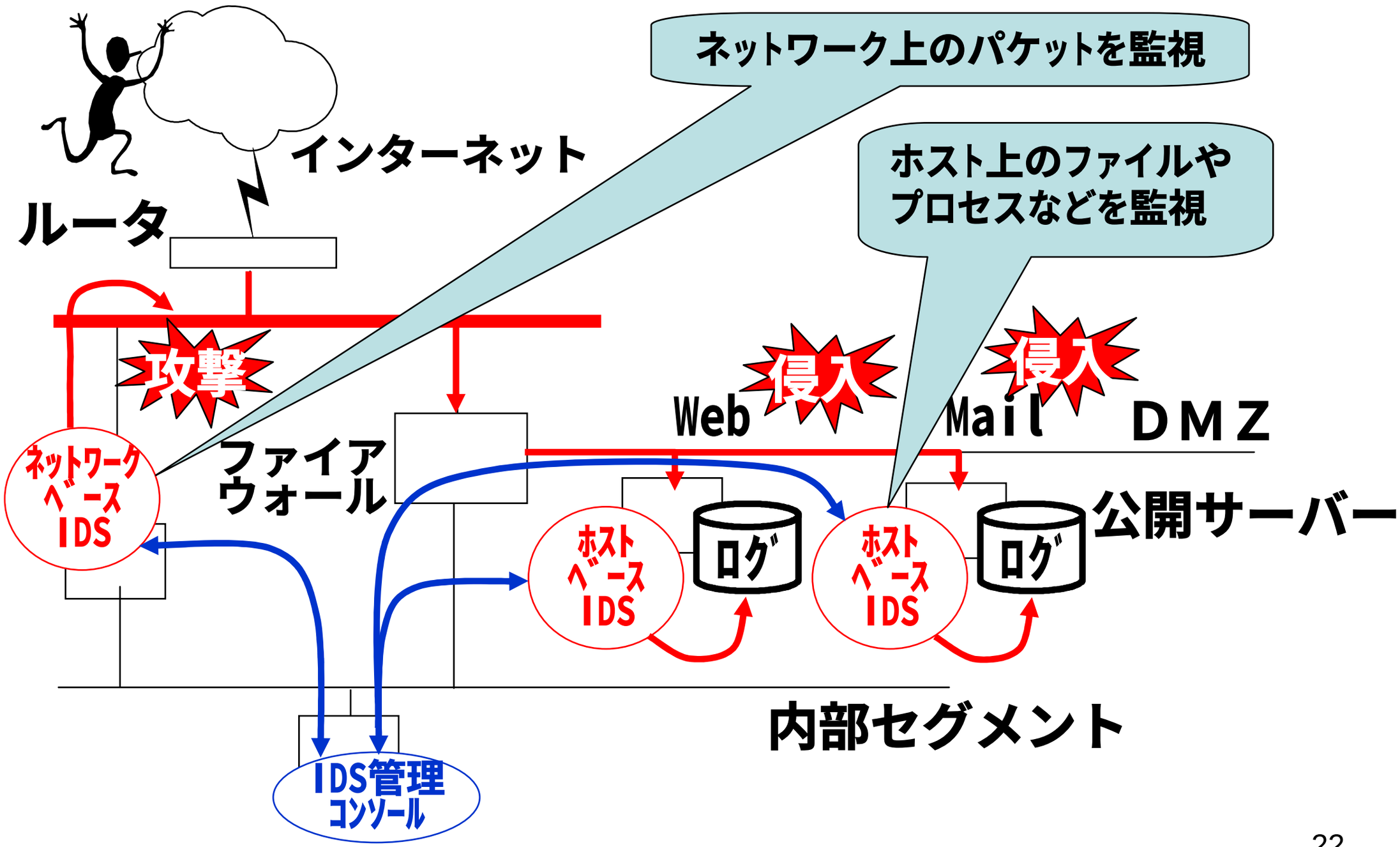
- **ネットワークベース**IDS

  ネットワーク上のパケットを監視

- **ホストベース**IDS

  ホスト上のファイルやプロセスなどを監視

ネットワークベースIDSとホストベースIDS



運用管理上の対策 (1)

- 最新版/パッチの適用
- 脆弱性情報などのセキュリティ情報の収集

- 完全性保護対策 – Tripwireなど
- バックアップ

- セキュリティ監査
- インシデント対応

運用管理上の対策 (2) ツールの利用

パッチ管理

- Microsoft Baseline Security Analyzer (HfNetChk)

  http://www.microsoft.com/japan/technet/security/tools/tools/mbsahome.asp

- Microsoft Software Update Services(SUS)

  http://www.microsoft.com/japan/windows2000/windowsupdate/sus/default.asp

- Solaris パッチの管理用ツール

  http://docs.sun.com/db/doc/817-2462/6mi4fl28n?l=ja&a=view

脆弱性監査ツール

- Nessus

  http://www.nessus.org/

- SARA (Security Auditor's Research Assistant)

  http://www-arc.com/sara/

パッチ配布/適用を自動化するツール

- システム管理者は、組織内の個々コンピュータに、パッチを適用し、かつウイルス対策ソフトを更新するという際限のない作業を続けています。
- これらの問題を解決するために『パッチ配布/適用を自動化するツール』があります。
- また、組織内の個々コンピュータに、『パッチの適用が行われているか検査するツール』もあります。
- このようなツールを利用することで、システム管理者の負担を軽減でき、かつセキュリティが高いレベルで維持できる可能性があります。

『パッチ自動』『パッチ適用』

脆弱性検査ツール・サービス

- 組織内の個々コンピュータ (クライアントおよびサーバー) の脆弱性 (セキュリティホール)を診断するツールやサービスがあります。
- Webアプリケーションの脆弱性を診断するツールやサービスがあります。
- このようなツールを利用することで、システム管理者の負担を軽減できる、かつセキュリティが高いレベルで維持できる可能性があります。

『脆弱性検査』『セキュリティホール自動検出』

改ざんを監視するツール･サービス

- Webサーバーへの攻撃やWebコンテンツの改ざんを監視するツールやサービスがあります。
- Webコンテンツの復旧まで実施してくれるツールもあります。
- Webサーバーへの攻撃から、Webアプリケーションを守るためのツールもあります。
- このようなツールを利用することで、システム管理者の負担を軽減できる、かつセキュリティが高いレベルで維持できる可能性があります。

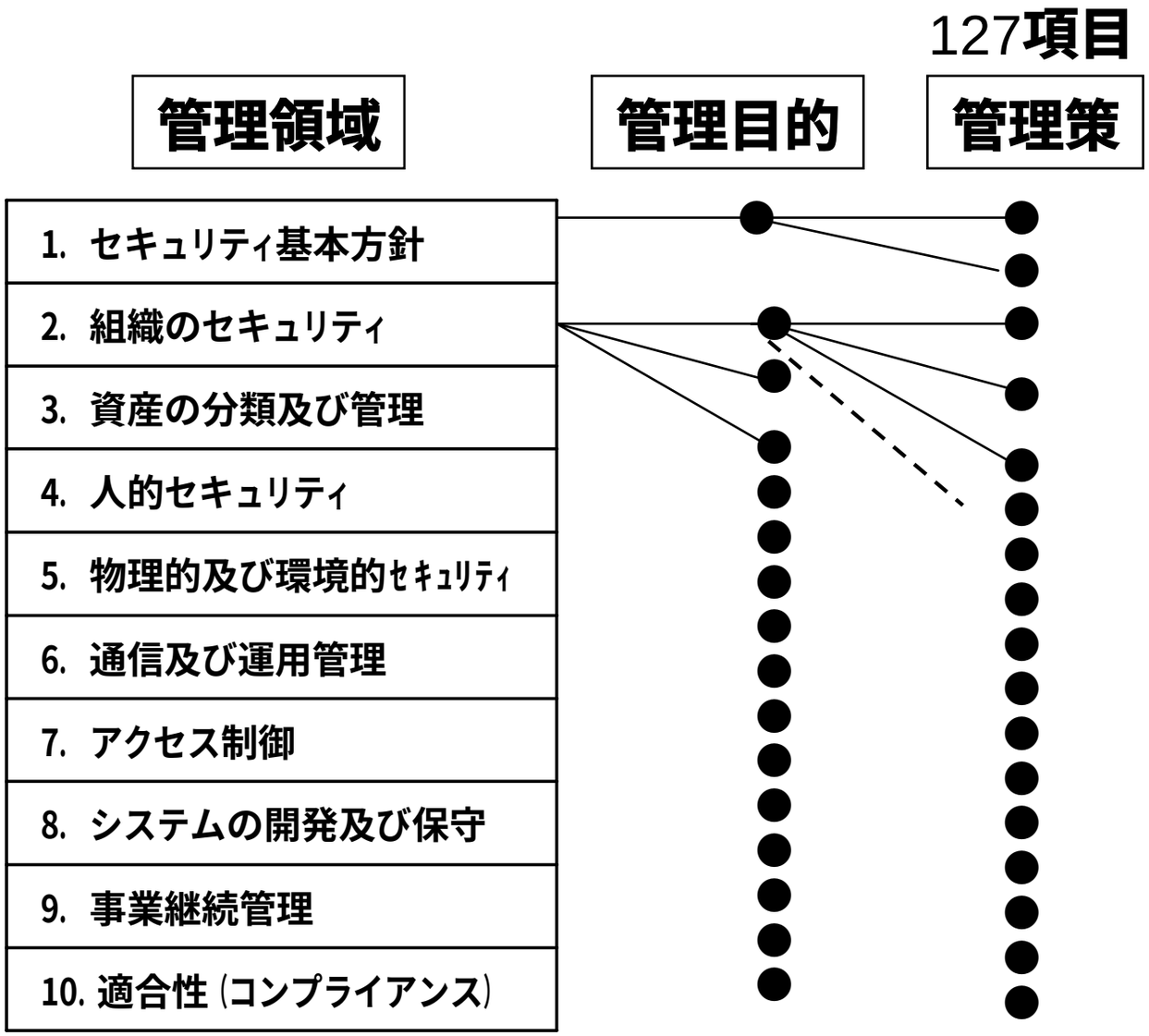
『Web改ざん 監視』『Web改ざん 対策』

技術的対策まとめ

- 計画的に不正アクセス対策を確実に実施
- ポリシーに基づいてセキュリティ機能を実装
- 継続的な改善によりセキュリティを維持
- 最小限のアクセスのみ許可する
- 多段階での防御をする
- 防御、検知、リアクション

管理的対策概要 – 広範囲で多くの対策ポイント

ISO/IEC17799などの既存の標準や対策基準の利用



- 情報セキュリティポリシー
- 教育と周知徹底
- 利用者管理
- 入退室管理
- 人的管理（秘密保持契約）
- 委託先管理
- 情報収集
- 情報のバックアップ
- 運用体制の整備
  （修正プログラム適用
  パターンファイル更新
  バックアップ計画）
- 脆弱性検査
- 緊急時対応計画
- コンプライアンス
- セキュリティ監査
- 見直し

セキュリティ担当者が行う対策

ーインシデント対応(被害拡大防止と早期復旧)

インシデント対応計画の策定

対応と復旧の手順を事前に策定しておく

★セキュリティ事故に応じた手順を事前に定める

ウイルス感染、Web改ざん、情報漏洩それぞれ対応が違う

対応によって、直接的な一次的被害、社会的信用失墜などの二次的被害の大きさが違ってくる

例1：情報漏洩の際には、対策窓口を設置、被害者への対応を迅速に行う
　　広報を窓口として、報道機関に適切な告知をする

例2：ウイルスに感染したら、ネットワークを停止する等、一斉に漏れなく行う
　→ 修復が確認できるまで、ネットワークにつながせない
　→ 最小限の被害にとどめる → 最小限の労力で復旧

業務継続管理→バックアップの二重化など

ウイルス・不正アクセス被害を受けたら、最終確認を兼ねIPAへ届け出を！

セキュリティ担当者・責任者が行う対策 - まとめ

組織ネットワークをセキュリティの脅威から守る
エンドユーザのセキュリティ対策を支援・教育する

- セキュリティポリシーの策定、対策の選定と導入、見直し
- セキュリティ製品の導入と運用
  - 適切な設定と不要なサービスの停止
  - 脆弱性パッチの適用
    - 定期的にベンダーサイトをチェックし、最新情報を収集
    - 脆弱性ツールなどの活用により、異常を早期発見
- 適切なID・パスワード管理 – 最小権限の付与
- ログの取得と定期的な分析
- ネットワークの監視とユーザへの助言
- バックアップ管理 – バックアップスケジュールなど
- 定期的な教育の実施 (社内ユーザの行う対策を周知徹底)
- 必要に応じセキュリティ監査を実施、セキュリティ情報の収集
- コンプライアンス、リスクマネジメント

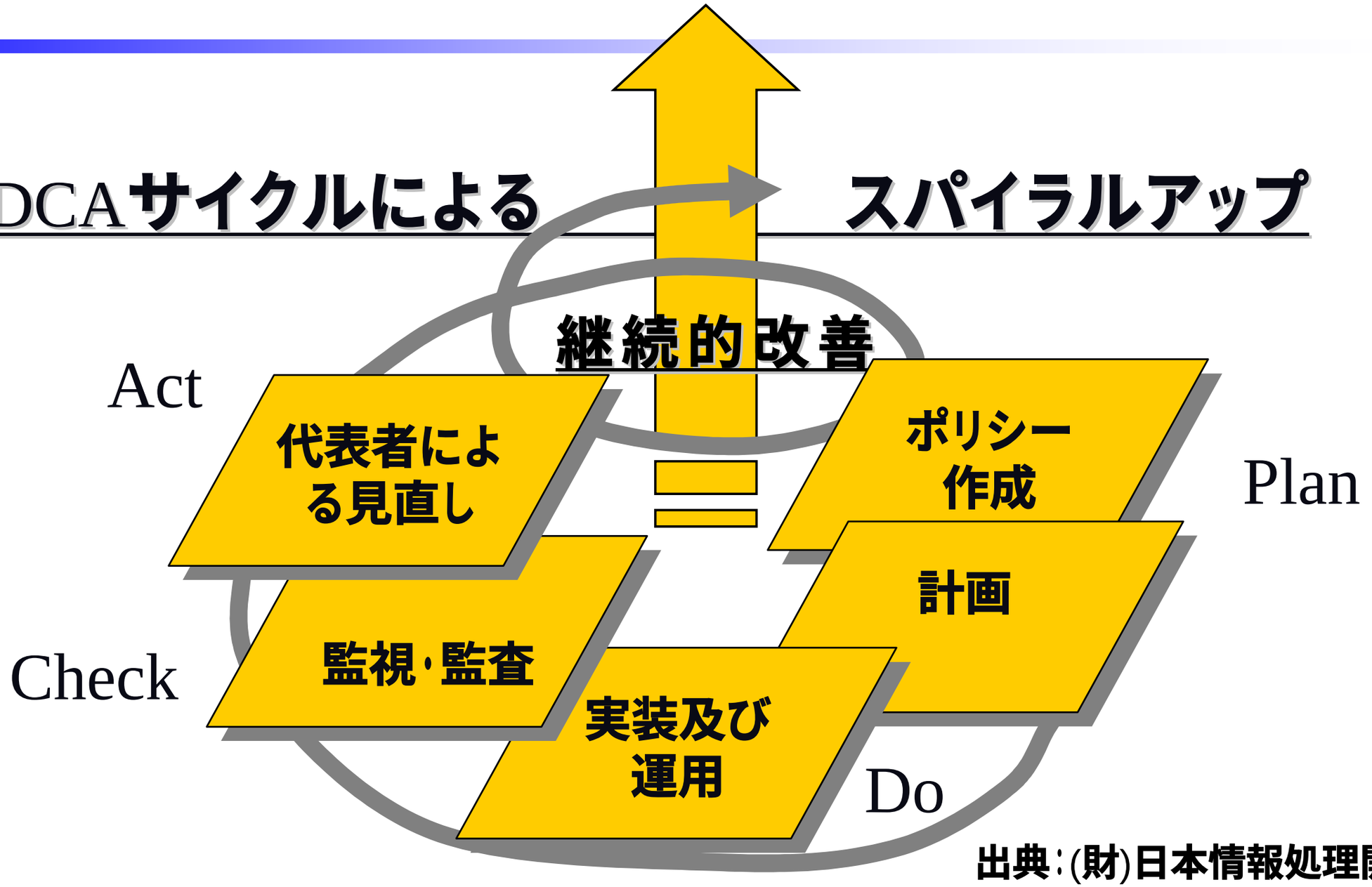
参考

組織体の長（経営陣）が行うべき対策

情報セキュリティの最高責任者は経営者である
セキュリティポリシーの承認と宣言
情報セキュリティの脅威と対策の理解を深める
セキュリティ担当者のセキュリティ施策を支援する

情報セキュリティ読本の活用
http://www.ipa.go.jp/security/publications/dokuhon/index.html

ISMS：情報セキュリティマネジメントシステム



出典：(財)日本情報処理開発協会

リスク評価→リスクマネジメント→業務継続管理

セキュリティ対策情報源

- IPA/ISEC (http://www.ipa.go.jp/security/)
- JPCERT/CC (http://www.jpcert.or.jp/)
- CERT/CC (http://www.cert.org/)
- SANS Institute (http://www.sans.org/)
- SecurityFocus (http://www.securityfocus.com/)
- **製品提供元のサポートサービス**
  - Web、**定期的なメールを利用した公開情報**
- **脆弱性・攻撃に係わる情報源**
  - **セキュリティ対策関連のメールサービス**

