security 101

IT経営を強化する、セキュア・コンテンツ・マネジメント セミナー
～電子メールポリシーによるリスク管理と生産性向上の実現～

IT経営を強化する、セキュア・コンテンツ・マネジメント セミナー
～電子メールポリシーによるリスク管理と生産性向上の実現～

リスク管理としての 情報セキュリティ対策

2002年9月13日

日本ヒューレット・パッカード株式会社
HPコンサルティング事業統括本部
セキュリティ・コンサルティング部

ビジネスベース・セキュリティのすすめ

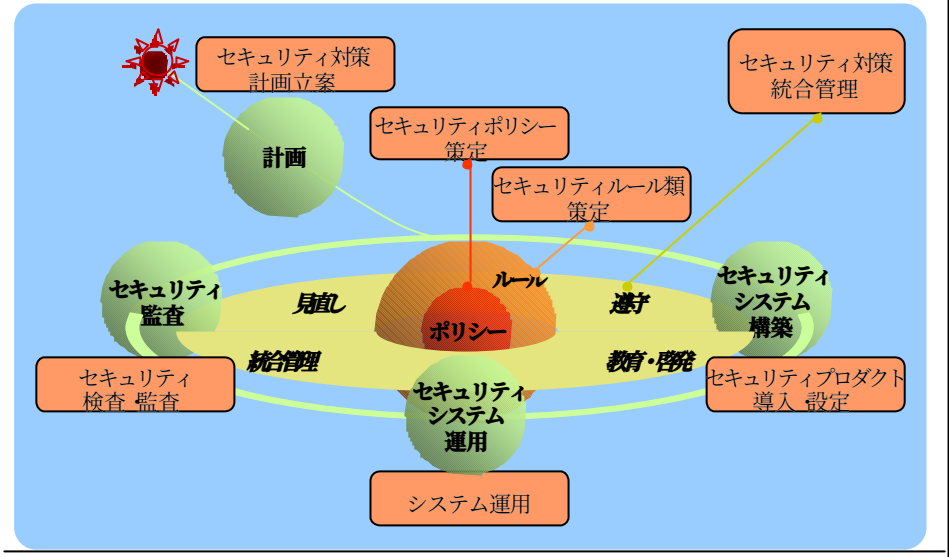
Did You Lock the Door?

Step -1) 全社情報セキュリティポリシーの必要性
Step 0) 策定委員会の編成
Step 1) 全社情報セキュリティポリシーの策定
Step 2) 情報セキュリティ体制の確立
Step 3) 情報セキュリティ対策の設計・開発・導入・運用
Step 4) 情報セキュリティ啓発と教育
Step 5) 情報セキュリティ維持の監査

security 101

IT経営を強化する、セキュア・コンテンツ・マネジメント セミナー
～電子メールポリシーによるリスク管理と生産性向上の実現～

hp トータル・セキュリティ・サービス



情報セキュリティポリシー策定支援コンサルティング説明資料

講師経歴

佐藤　慶浩（さとう　よしひろ）
日本ヒューレット・パッカード株式会社
HPコンサルティング事業統括本部
アジアパシフィック・セキュリティ・ソリューション・マネージャ

1986 年。日本アポロコンピュータ(株) 入社。International R&D に所属。マサチューセッツ州チェルムスフォード市にて日本語環境製品の開発に従事。
1990 年。日本ヒューレット・パッカード(株) 入社。新製品のテクニカル・マーケティングとして、ＯＳＦ／1、分散環境コンピューティング技術、マルチメディア技術、ハイアベイラビリティ技術、インターネット技術をＨＰ社の製品提供と相応して順次担当。この間1993年からの 2 年間はカリフォルニア州クパチノ市にてセキュリティ製品の仕様開発に従事。
1996 年、米国駐在中に計画した製品群の出荷が始まったため、現在は主としてセキュリティ・ソリューションのコンサルティングに従事している。
1997 年以後は、通常のコンサルティング活動の他に、ＪＰＣＥＲＴ／ＣＣのヒューレット・パッカード対応窓口を担当。また、ＦＩＳＣ(金融情報システムセンタ)、JISA (情報サービス産業協会)、JUAS（日本情報システム・ユーザ協会）、システム監査人協会や各種有料セミナにて情報セキュリティポリシー策定方法論についての講演をしている。

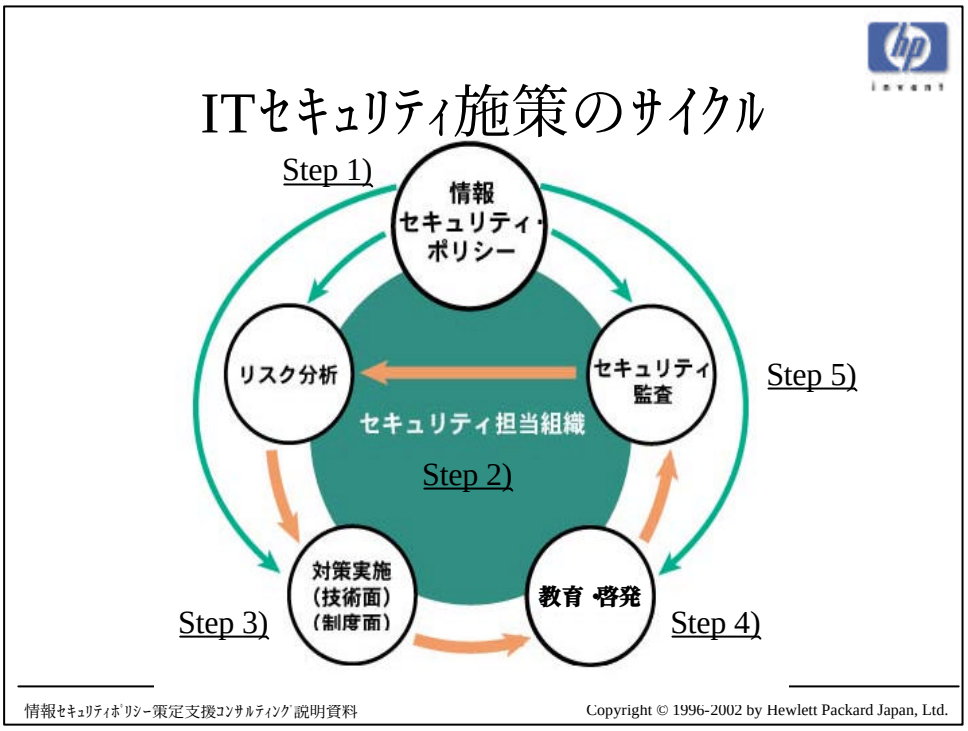
情報処理学会(www.ipsj.or.jp/)　正会員
日本ネットワークセキュリティ協会(www.jnsa.org/)　理事
情報処理振興事業協会(www.ipa.go.jp/)セキュリティセンター　非常勤研究員
金融情報サービスセンター (www.fisc.or.jp/)セキュリティポリシー研究会　委員
情報処理学会 情報規格調査会(www.itscj.ipsj.or.jp/) SC 27/WG 1小委員会　委員

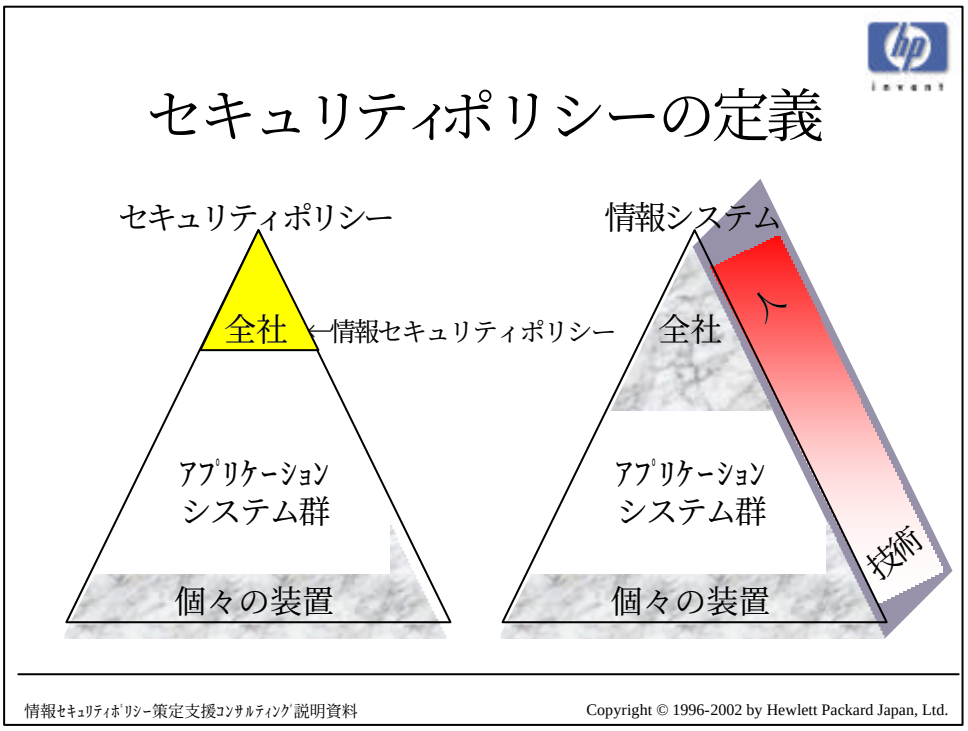
情報セキュリティポリシー策定支援コンサルティング説明資料

Copyright © 1996-2002 by Hewlett Packard Japan, Ltd.

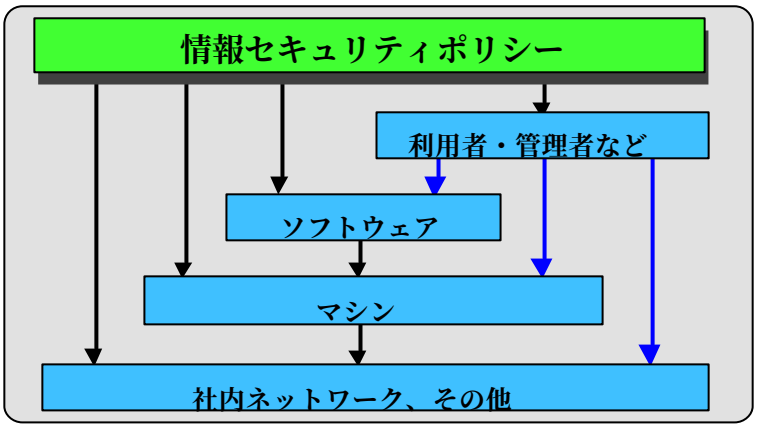
security 101

IT経営を強化する、セキュア・コンテンツ・マネジメント セミナー
～電子メールポリシーによるリスク管理と生産性向上の実現～





セキュリティポリシーの定義



全社情報セキュリティポリシーの策定

Step -1 情報セキュリティポリシーの必要性

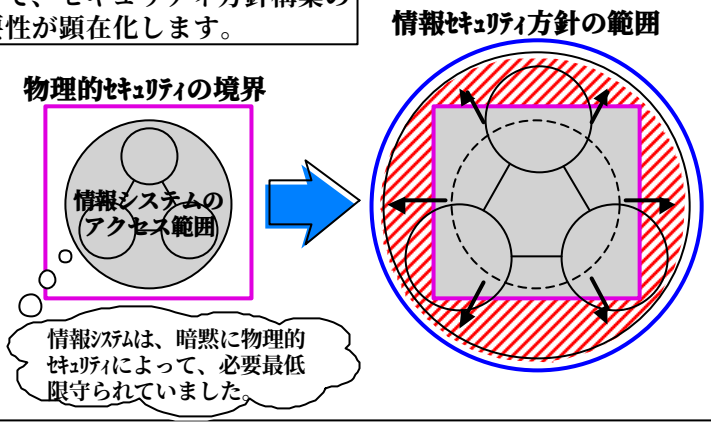
なぜ、作られるようになったか？

外部接続性の変化による要求
利用形態の自由度の変化による要求
ユーザの前提の変化による要求
↓
システム計画より以前の計画の必要性

全社情報セキュリティポリシーの策定

Step -1 情報セキュリティポリシーの必要性

インターネットなどの外部接続によって、セキュリティ方針構築の必要性が顕在化します。

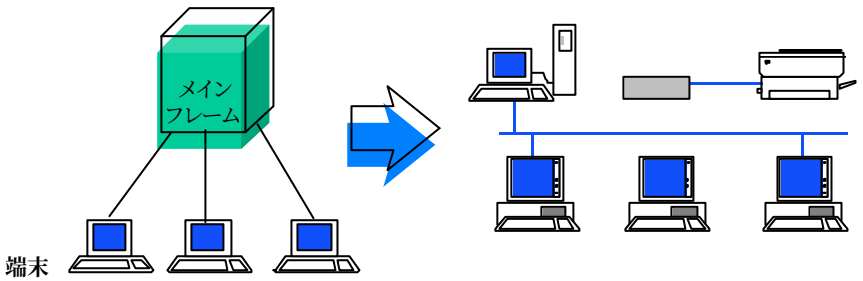


情報セキュリティポリシー策定支援コンサルティング説明資料

全社情報セキュリティポリシーの策定

Step -1 情報セキュリティポリシーの必要性

情報システムの利用形態の自由度と柔軟性が高まったことにより、セキュリティ方針構築の必要性が顕在化します。

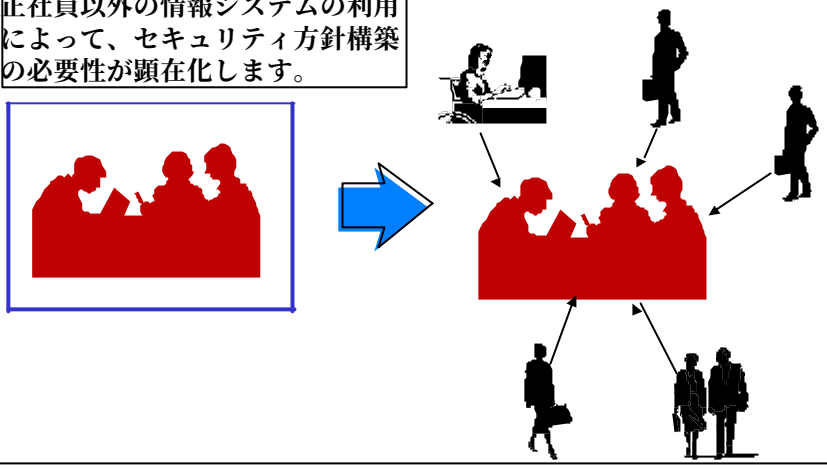


情報セキュリティポリシー策定支援コンサルティング説明資料

全社情報セキュリティポリシーの策定

Step -1 情報セキュリティポリシーの必要性

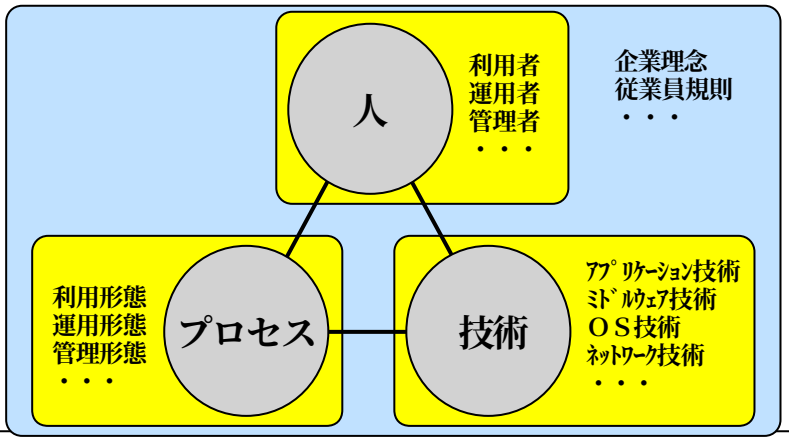
正社員以外の情報システムの利用によって、セキュリティ方針構築の必要性が顕在化します。



情報セキュリティポリシー策定支援コンサルティング説明資料

全社情報セキュリティポリシーの策定

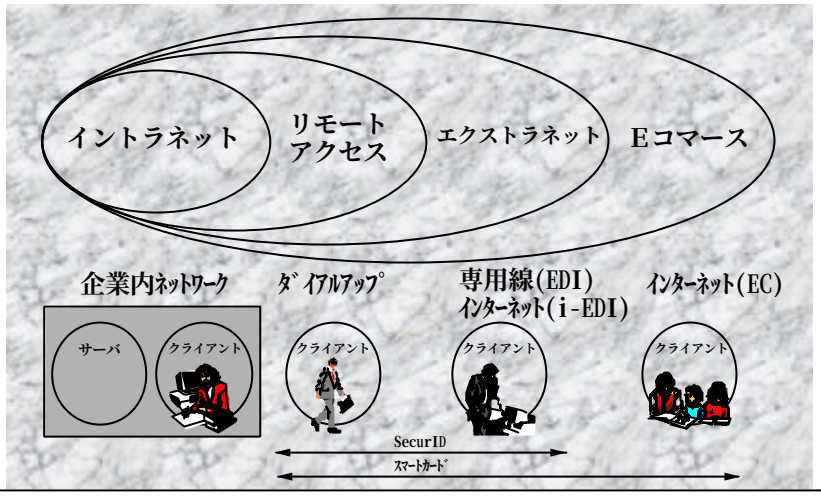
Step -1 情報セキュリティポリシーの必要性



情報セキュリティポリシー策定支援コンサルティング説明資料

全社情報セキュリティポリシーの策定

Step -1 情報セキュリティポリシーの必要性



情報セキュリティポリシー策定支援コンサルティング説明資料

全社情報セキュリティポリシーの策定

Step -1 情報セキュリティポリシーの必要性

	認証	認可	データ保護	否認不能性	可用性
イントラネット	企業内で Business within the enterprise				
リモートアクセス	出張先で Business within the enterprise				
エクストラネット	取引先と Business with Partners				
インターネット	お客様と Business with Customers				

情報セキュリティポリシー策定支援コンサルティング説明資料

全社情報セキュリティポリシーの策定

Step -1 情報セキュリティポリシーの必要性

なぜ、作られるようになったか？

外部接続性の変化による要求
利用形態の自由度の変化による要求
ユーザの前提の変化による要求
↓
システム計画より以前の計画の必要性

ポリシーがないと。。。

全社情報セキュリティポリシーの策定

Step 0 策定委員会の編成

委員は、どのような部署から？どのような資質の人？で編成するか。
「策定」作業の細分：
作文
↓
審議（裏方：検証、承認層への説明）
↓
承認
↓
発布）

◎経営層はどこまで直接関わるのか？
◎どの部署（IT／企画）が主導的な役割を担うか？
◎全社の協力を得るためには？

全社情報セキュリティポリシーの策定

Step 1 全社情報セキュリティポリシーとは？

全社情報セキュリティポリシーとは、全社における情報に対するセキュリティ上のリスクの許容範囲を検討し、セキュリティ維持の目標を定めたもので、その目標達成を経営上の課題として意志表明したもの。
企業は情報の全使用者に対して、この目標達成・維持を求めるとともに、達成・維持に必要な支援を約束することを明文化する。

セキュリティ＝何から何を守るのか

全社情報セキュリティポリシーの策定

Step 1 全社情報セキュリティポリシーとは？

リスク対策としてのセキュリティ対策

セキュリティ対策は、リスク対策であるという考え方をしています。
リスク対策→セキュリティ対策の表現で書くと
回避→防御策を完全にする
軽減→防御策を可能な限り実施し、侵害発生時の被害の最小化にも努める
分散→侵害を想定し、被害発生後の復旧のための分散をはかる
復旧→侵害発生後に、予め分散しておいたもので被害からの回復をする
転嫁→侵害を前提として、保険加入などの直接的な対策以外の手段を講じる
受け入れ→直接的な対策をできないものと割り切る
から適宜、選択することになります。（セキュリティの場合、複数選択可）

情報セキュリティポリシー策定支援コンサルティング説明資料
Copyright © 1996-2002 by Hewlett Packard Japan, Ltd.

全社情報セキュリティポリシーの策定

Step 1.1 文書の位置づけと構成の決定

ポリシー文書の全体構成（目次）

1. 経営責任者からの意思表明
2. 目的
3. 原則群 *
4. ポリシー群
5. 改訂の手続き

20 ～ 40 のポリシー項目

個々のポリシー文の文章構造

4.i ポリシーの表題
4.i.1 ポリシー本文
4.i.2 趣旨（根拠、目標、定義）
4.i.3 範囲（主体、客体）
4.i.4 遵守事項
4.i.5 逸脱手続き
4.i.6 結果責任

* 原則群＝OECDの9原則等

全社情報セキュリティポリシーの策定

Step 1.1 文書の位置づけと構成の決定

「情報セキュリティポリシー」をいくつの文書で構成するのか？
それぞれの文書名
　　規則とそれ以外
文書の定義
　　読者の範囲は？
　　範囲の中は一様か？（階層があるか？）
　　読者（の階層ごと）にどれだけ読んでもらうか

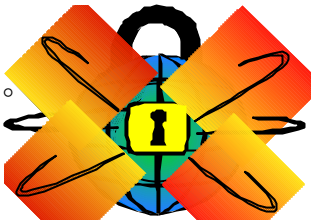
◎罰則条項
◎従業員以外（派遣、委託）への適用

全社情報セキュリティポリシーの策定

Step 1.1 文書の位置づけと構成の決定

目的の検討 例）

ビジネスを支える情報を、いつでも、
どこでも、安心して使えるようにする。



情報システムは、情報の隠蔽を目的としない。
積極的な情報の開示／共有をするための基盤です。
情報セキュリティは、積極的情報利用を現実のものとする
ために、情報を適切に保護します。

全社情報セキュリティポリシーの策定

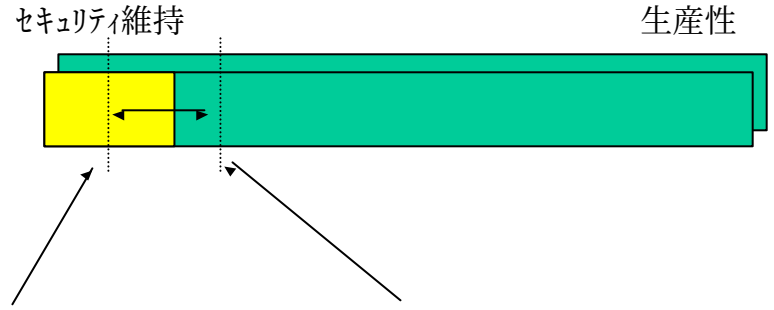
Step 1.2 策定のルールを定める

セキュリティの9原則 （OECD（経済協力開発機構）セキュリティガイドラインより）

1. 責務原則 (accountability principle)
   責任と説明義務を明確にする
2. 周知原則 (awareness principle)
   情報システムセキュリティのための手段・慣行・手続きの存在と、適切な知識を知ることができるようにすべきであり、また、知らされるべきである
3. 倫理原則 (ethics principle)
   他者の権利と正当な利益を尊重する
4. 多元的観点原則 (multidisciplinary principle)
   情報システムセキュリティのための手段・慣行・手続きは、技術・管理・組織・運営・営業・教育・法律を含む問題に関連するあらゆる考え・視点を考慮に入れ、注意を向けるべきである。
5. 均衡原則 (proportionality principle)
   セキュリティの要求は、情報の価値と要求される信頼度、セキュリティが破れた場合の被害の深刻度、発生可能性、波及度合に均衡すべきである
6. 統合原則 (integration principle)
   情報システムセキュリティのための手段・慣行・手続きは、その他のそれらと相互に、かつ、統合されるべきである
7. 適時性原則 (timeliness principle)
   防止や対応などは適時に協調的に行動すべきである
8. 再評価原則 (reassessment principle)
   定期的に再評価されるべきである
9. 民主制原則 (democracy principle)
   情報の合法的な利用および流れに適合すべきである

全社情報セキュリティポリシーの策定

Step 1.3 背景の調査と認識



Step 1.3.1 法令等の遵守　　Step 1.3.2 企業内規との整合

全社情報セキュリティポリシーの策定

監督官庁ガイドラインの例

通商産業省
- 情報システム安全対策
- コンピュータウィルス対策
- 不正アクセス対策基準

JIPDEC
- プライバシ・マーク

警察庁
- 情報システム安全対策指針
- コンピュータウィルス等不正プログラム対策指針

FISC
- 安全対策基準
- セキュリティポリシー策定手引書
- 個人データ保護取扱指針（改訂版）

総務省総合通信基盤局
- 情報通信ネットワーク安全・信頼性基準（H13.3.22改正案）

（一部出典：高橋　郁夫先生）

企業内規の例

社訓、就業規則、文書管理規程　など

＊被害を受けないことばかりではなく、加害者にならない配慮も重要

法令等の例

関係法令の例
刑法典上の犯罪
- 電子計算機詐欺罪（246条の2）
- 電磁的記録等毀棄罪（258条、259条）
- 電子計算機損壊等業務妨害罪（234条の2）
- 電磁的記録不正作出罪（161条の2）

特別法上の規制
- 不正競争防止法
- 著作権法
- 不正アクセス禁止法

（出典 **石井　徹哉先生**）

関係法令の例（追加）
- 個人情報保護基本法→個人情報保護法
- IT基本法
- 特定電子商取引円滑化法
- プロバイダー責任法

全社情報セキュリティポリシーの策定

監督官庁ガイドラインの例（その他）

経済産業省

平成13年10月23日
http://www.meti.go.jp/kohosys/press/0002003/
経済産業省は23日、「インターネット通販における『意に反して契約の申込みをさせようとする行為』に係るガイドライン」を公表した。これは、特定商取引法第14条において義務づけられている「インターネット通販における分かりやすい申込み画面設定」の解釈基準を整理する目的で公表されたもの。

平成13年10月30日
http://www.meti.go.jp/policy/netsecurity/crosssite1.htm
Webサイトにおけるクロスサイトスクリプティング問題への対応について

平成14年1月16日
http://www.meti.go.jp/feedback/downloadfiles/i20115bj.pdf
広告メール！表記義務

全社情報セキュリティポリシーの策定

監督官庁ガイドラインの例（その他）

経済産業省

平成14年3月6日
http://www.meti.go.jp/kohosys/press/0002435/
◆経産省が電子商取引の法適用ガイドライン案を公表
経済産業省は5日、電子商取引について、民法などの現行法が、どのように適用されるかを示すガイドライン「電子商取引等に関する準則(案)」をまとめた。新しい技術の登場によって、法律が作られた時には想定していなかったような事案が出てきたことに応えるもので、円滑な運用と解釈のための指針を目指している。同省サイトで公表し、パブリックコメントを募集した後、３月末までに、とりまとめて公表する予定。
関連記事＝ http://japan.cnet.com/News/Infostand/Item/2002-0305-J-7.html

全社情報セキュリティポリシーの策定

監督官庁ガイドラインの例（その他）

総務省

平成14年2月24日
6月よりIP電話の音質表示制度を導入
固定電話同等＝A、携帯電話同等＝B、それ以下＝C

全社情報セキュリティポリシーの策定

監督官庁ガイドラインの例（その他）

その他

平成14年2月25日
“プロバイダー責任法”の施行に向け運用ガイドライン作成へ
http://news.lycos.co.jp/comp/story.html?q=23impressi02&cat=14
昨年11月に公布された「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（プロバイダー責任法）の5月の施行に向けて、実際に運用するにあたっての指針を示すガイドラインの作成がスタートした。通信事業者団体や著作権団体などが参加して「プロバイダ責任法ガイドライン等検討協議会」が発足され、14日に第1回会合が開かれた。

全社情報セキュリティポリシーの策定

法整備動向

2002年1月
サイバー犯罪条約（2001/11策定）に批准。　通信傍受法の実効整備などに着手。
翻訳に課題あり。例）プロバイダー、エンティティ等。　（詳細=通信傍受法html 参照）

2002年1月30日
法務省が人権擁護法案大綱を公表。２月中に上程へ。
人権委員会（仮称）の主観により、「プライバシー侵害」 過剰取材・報道」を判断する。
取材・報道の中止勧告の権限を与える予定。
人権委員会は、法務省の外局組織。
青少年有害社会環境対策基本法案（自民党が上程準備中）も主観による判断。

2002年2月8日
ドメイン名の差し止め裁判判決確定。（上告棄却）
ドメイン名を商標権法の対象に。（メールアドレス、WebのURLとも）

2002年2月
オンライン・オークションを古物法の対象に。
製造販売禁止処分にしてあった、殺傷性能のあるエアガンがオークションで広く取り引きされていることから、警察庁が検討を開始。

全社情報セキュリティポリシーの策定

法整備動向

2002年2月12日
経済産業省が不正競争防止法改正案を２００３年通常国会提出方針。
企業秘密（営業秘密）漏洩に刑罰適用。
被害企業の立証責任の軽減も盛り込む予定。
アメリカ=経済スパイ法、フランス=不正競争防止法、ドイツ=刑法で刑事罰。

2002年2月21日
迷惑メール規制は2法案　対象を分け今国会提出へ
http://www.mainichi.co.jp/digital/netfile/archive/200202/21-3.html
携帯電話やパソコンに一方的に送りつけられる「迷惑メール」を規制する法案が、経済産業省と参院の与党3党から、それぞれ今国会に提出されることが21日に、決まった。同様目的の2法案が同時並行して準備され調整が難航したが、規制対象を分けることで、2法案を両立させることになった。
経済産業省案（政府法案）＝販売・提供業者を規制対象。主務大臣＝経済産業相
与党案（総務省案）（議員立法案）＝送信者を対象。主務大臣＝総務相
＊同時提出は異例

全社情報セキュリティポリシーの策定

法整備動向

2002年3月7日
行政機関個人情報保護法案、全文明らかに
http://www.mainichi.co.jp/digital/network/archive/200203/07/3.html
国の行政機関が保有する個人情報の保護を定めた「行政機関個人情報保護法案」の全文が7日、分かった。法案は、電算処理したデジタル情報に限らず手書きなどのマニュアル処理情報も保護対象に拡大した。開示請求の除外対象だった教育、医療分野も対象に加えた。政府は、独立行政法人などを対象にした関連4法案を来週中に閣議決定し、国会提出する方針だ。

2002年3月15日
個人情報保護法案　今国会での審議入りが濃厚に
http://www.mainichi.co.jp/digital/network/archive/200203/15/1.html
公的分野の個人情報保護関連4法案が15日閣議決定されたことで、政府が昨年3月に提出し、継続審議となっていた個人情報保護法案の審議入りが濃厚となってきた。同法案をめぐっては、与党内では公明党が公的分野の未整備を理由に、これまで慎重姿勢を示してきていた。

2002年3月15日
ネット・オークション規制法案を閣議決定
http://www.mainichi.co.jp/digital/network/archive/200203/15/2.html
インターネット・オークション業者を法規制する「古物営業法」の改正案が15日、閣議決定された。今年2月、警察庁が発表した同改正案の骨子では、業者側に盗品売買黙認など悪質な行為があれば、都道府県公安委員会が営業停止処分を命じることができるとしていたが、業者が盗品の判断をするのは困難なことから、同処分については見送った。

全社情報セキュリティポリシーの策定

電子政府動向

2002年3月8日
6割の都道府県が03年度までに電子申請システム導入へ
http://biztech.nikkeibp.co.jp/wcs/show/leaf?CID=onair/biztech/prom/173507
SIベンダ68社が組織する「地方公共団体行政サービスオンライン化促進協議会」は電子自治体の進捗状況に関する調査結果を発表した。それによると、都道府県の66.6％が2003年度までに「電子申請・届出システム」を導入する予定。

全社情報セキュリティポリシーの策定

関連判決

２００２年3月1日
最高裁判決
２４時間勤務の従業員の仮眠時間は労働時間に当たる
泊まり勤務手当の支給だけは不適当
（大星ビル管理／東京都文京区）　原告：元従業員と従業員の計１０人

全社情報セキュリティポリシーの策定

国際動向

２００２年2月２５日
WIPO、インターネットにおける著作権保護条約を5月に施行
http://www.watch.impress.co.jp/internet/www/article/2002/0222/wipo.htm
世界知的所有権機関(WIPO)は21日、インターネットなどのデジタル技術における海賊行為から音楽家やレコード会社を保護するための条約「WIPO Phonograms and Performances Treaty」(WPPT; WIPO演奏上演条約)に対し、ホンジュラスが30ヵ国目として批准し、5月20日に施行すると発表した。

全社情報セキュリティポリシーの策定

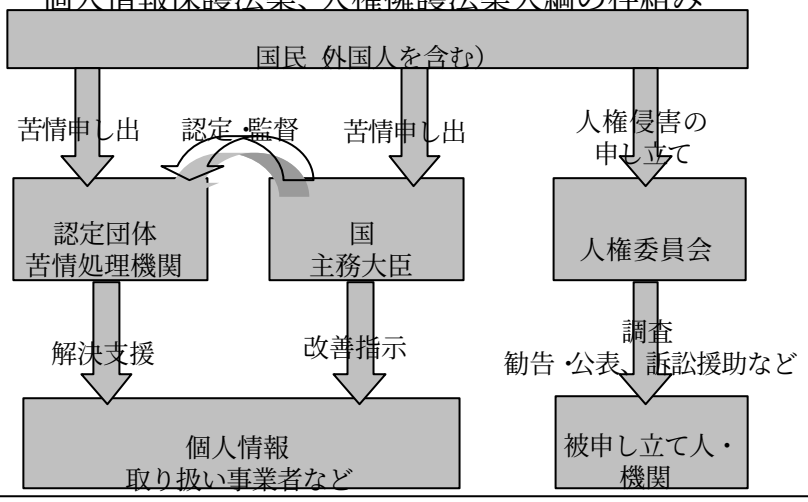
メディア規制　主な動き（H14.2.6 読売新聞朝刊）

1989年　行政機関のコンピューター処理による個人情報についての保護法施行
1999年6月　住民基本台帳法が改正。自治体が保有する個人情報を国の行政機関も共有できることに。政府は、個人情報保護法制度の充実を約束
7月　政府の個人情報保護検討部会が発足。11月、個人情報保護基本法の下に個別法と自主規制による保護という保護体系案を公表
8月　自民党「報道と人権等のあり方に関する検討会」が報道機関規制立法も選択肢とする報告書公表。
10月　人権擁護推進審議会事務局の法務省が日本新聞協会に「行政命令による記事の事前差し止めも検討したい」と表明。抗議を受け、11月に撤回。
2000年5月　自民党が青少年有害環境対策基本法案（素案）を取りまとめ
10月　検討部会の下の個人情報保護法制化専門委員会が個人情報保護基本法制大綱を取りまとめ。報道分野も「基本原則」の適用対象に
2001年3月　政府が「基本法」の文言を削除した罰則付き個人情報保護法案を国会に上程。継続審議。
5月　人権擁護推進審が人権救済制度について最終答申を取りまとめ。報道分野も人権委員会の勧告等の対象に。
2002年1月　法務省が人権擁護法案大綱を公表。3月国会上程を表明。

報道機関等がする人権侵害（人権擁護法案要旨、2月23日）
　救済対象者＝犯罪行為による被害者、犯罪行為を行なった少年、犯罪行為による被害者または犯罪行為を行なった者の配偶者、直系もしくは同居の親族または兄弟姉妹

全社情報セキュリティポリシーの策定

個人情報保護法案、人権擁護法案大綱の枠組み



全社情報セキュリティポリシーの策定

国際動向

RIAAが100万ドル徴収　社内ネットで音楽ファイル交換

全米レコード工業会(RIAA)は9日(米国時間)、社内に置いたサーバーで従業員に違法コピーしたMP3ファイルを交換させていた技術・ビジネスコンサルティング会社から100万ドルの示談金を受け取ることで同社と和解したと発表した。この会社は、不正コピーした数千のMP3音楽ファイルをサーバーに置いていたという。

アリゾナ州のインテグレーテッド・インフォメーション・システム(IIS)という会社で、RIAAによると、昨年半ば、RIAAが違法コピーを従業員に交換させていることに気づき、同社に対してただちに著作権侵害行為を中止するよう通知。損害賠償訴訟を起こすと警告していたという。

両者は、その後話し合いに入り、このほどIISが100万ドルの示談金を支払うことで合意した。違法コピーされていた音楽ファイルには、ポリスやエアロスミスなどのアーティストの曲が含まれていたという。

RIAAのマット・オッペンハイム・ビジネス・法務担当上席副会長は「これは企業が社内リソースを著作権侵害に利用することを許した場合、報いを受けるということを示す明白なメッセージだ。われわれは、責任を取って法廷で争うことなく和解を受け入れたIISを賞賛する」とコメントしている。

なおIISは、デジタルファイルの違法コピー配信を防止するソフトウェアを製品として販売している。

[RIAAの発表]
http://www.riaa.org/PR_Story.cfm?id=505

全社情報セキュリティポリシーの策定

Step 1.3 背景の調査と認識

情報セキュリティポリシーを取り巻く文書との関係
- 安全対策基準
- コンティンジェンシープラン
  （事業継続計画 - Business Continuity Plan）
- 顧客情報管理規定
- 個人情報管理規定

情報セキュリティ担当組織と別の体制の関係
- 緊急時対応計画

全社情報セキュリティポリシーの策定

Step 1.4 ポリシー群の洗い出し

ポリシーツリー（方針木）の設計

大きな方針を実現するためのより小さな方針を検討してゆく
できあがった小さな方針群を達成することで大方針を達成する

基本をなす方針項目の例

- 情報資産の定義
- 重要度の明確化
  - 情報種別
  - システム種別
- 登場人物の明確化
  - 情報セキュリティにおける役割
  - 職制の要件

企業色

*** ポリシーのテンプレート利用の危険性**

全社情報セキュリティポリシーの策定

Step 1.4 ポリシー群の洗い出し

重要度の明確化
- 情報種別
- システム種別

格付け（Classification）＝重要度の格と表現方法の定義

表記義務の明文化

機密性（例：極秘、関係者外秘、秘、非機密）
完全性（例：要保全、一般）
可用性（例：要安定、一般）
× 情報 / 情報システム

度合い（例：上記） ｜ 種別（例：人事秘、顧客情報）
マーキング（例：禁帯出、禁複製）

(Sensitivity Level, Compartment & Marking)

全社情報セキュリティポリシーの策定

Step 1.4 ポリシー群の洗い出し

脅威の例

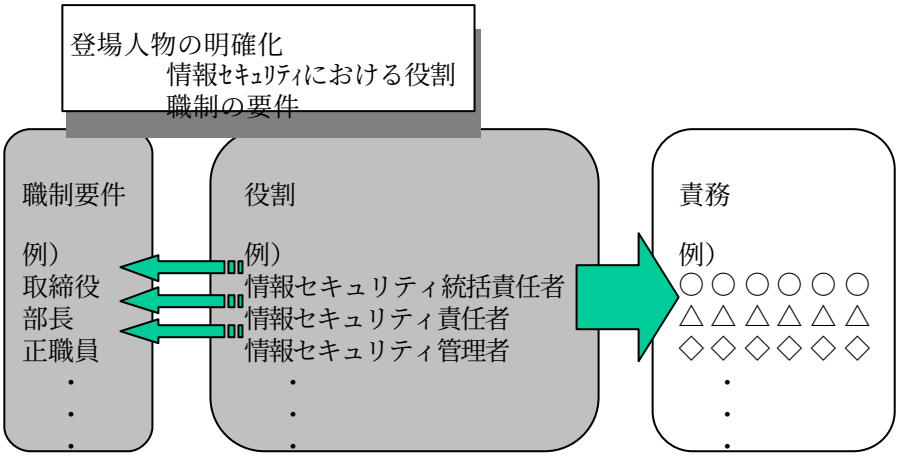
機密性	故意	事故
情報	漏洩 盗聴 詐取	誤配信

完全性	故意	事故
情報	改ざん	(滅失)
	消去	消失
ファイル	破壊	消失

可用性	故意	事故
情報	消去	消失
システム	DoS DDoS	障害

全社情報セキュリティポリシーの策定

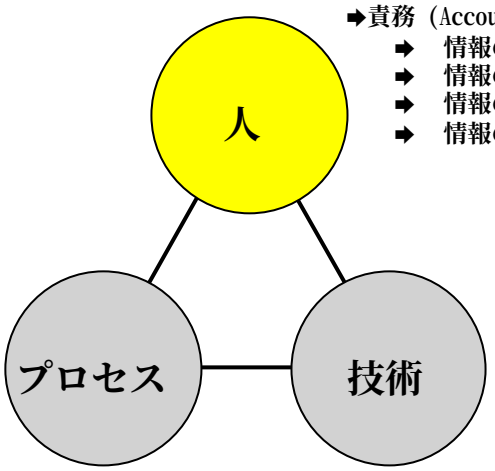
Step 1.4 ポリシー群の洗い出し



情報セキュリティポリシー策定支援コンサルティング説明資料
Copyright © 1996-2002 by Hewlett Packard Japan, Ltd.

全社情報セキュリティポリシーの策定

Step 1.4 ポリシー群の洗い出し



- 責務 (Accountability)
  - 情報の所有者 (Owner)
  - 情報の後見人 (Guardian)
  - 情報の利用者 (User)
  - 情報の保管者 (Custodian)

- 認証 (Authentication)
- 認可 (Authorization)
- 機密性 (Confidentiality)
  - 情報の機密分類 (Classification)
  - 情報の暗号化 (Encription)
- 保全性 (Integrity)
- 否認不能性 (Non-repudiation)
- 可用性 (Availability)

全社情報セキュリティポリシーの策定

Step 1.4 ポリシー群の洗い出し

最近のキーワードの例：

ウィルス対策
知的所有権・著作権などの保護と権利侵害の防止
顧客・個人情報の保護
私的利用（従業員プライバシの無保証）
ダイアルアップ接続　・・・ Script Kids
私物の転用（物・個人メール）

全社情報セキュリティポリシーの策定

Step 1.4 ポリシー群の洗い出し

最近のキーワードの例：

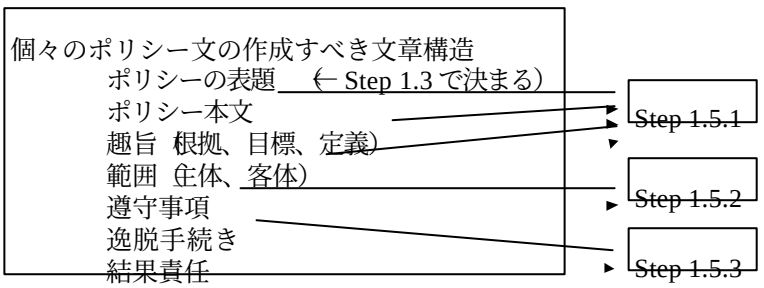
外部委託（アウトソーシング）

責任と義務の分離
機密保持＝守秘義務？

Responsibility とAccountability

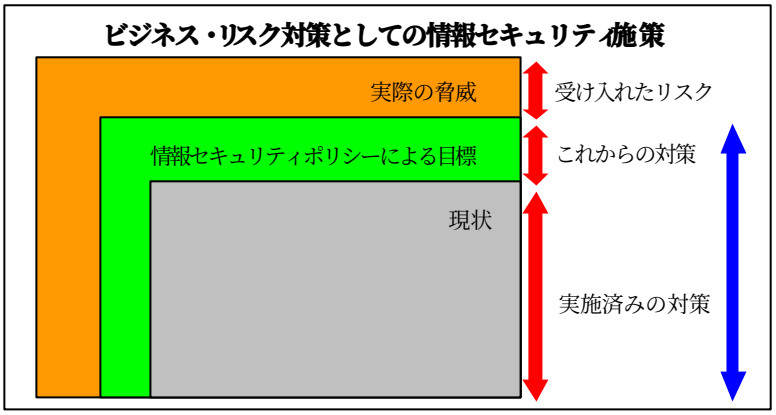
全社情報セキュリティポリシーの策定

Step 1.5 個々のポリシー文の記載内容の要件
何が目標か（WHAT）
なぜ、それが目標か（WHY）
誰が責任者か（WHO）



全社情報セキュリティポリシーの策定

Step 1.5.1 目標設定とその根拠→本文（WHAT）と目的（WHY）



＊経営者とのコミュニケーション・ツールとしてのポリシー

全社情報セキュリティポリシーの策定

Step 1.5.1 目標設定とその根拠→本文（WHAT）と目的（WHY）

回避 :事故発生の可能性をなくすべく、防御策を完全にする
軽減 :防御策を可能な限り施し、事故発生時の被害の最小化に努める
分散 :事故発生を想定し、事故発生後の復旧のために、被害対象の分散をはかる
復旧 :事故発生時に、予め分散しておいたもので被害からの復旧をはかる
転嫁 :事故発生を想定し、直接的対策ではない保険や契約締結のような手段を講じる
受け入れ :直接的対策をできず、被害発生は不可避と割り切る

＊経営者とのコミュニケーション・ツールとしてのポリシー

情報セキュリティポリシー策定支援コンサルティング説明資料

全社情報セキュリティポリシーの策定

Step 1.5.1 目標設定とその根拠→本文（WHAT）と目的（WHY）

WHYをリスクの観点で検討すべきであることを述べた。
では、なぜ、WHYを検討すべきなのか：

ポリシーでは、
　しなければならないこと
　してはならないこと　等を記述する。
しかし、だからといって、
　記述されていないことを、しなくてもよい
　記述されていないことを、してもよい
という訳ではない。
それを判断してもらうために、WHYを記述する。

WHATや HOW TO 列記の限界

性善説と性悪説

全社情報セキュリティポリシーの策定

Step 1.5.1 目標設定とその根拠→本文（WHAT）と目的（WHY）

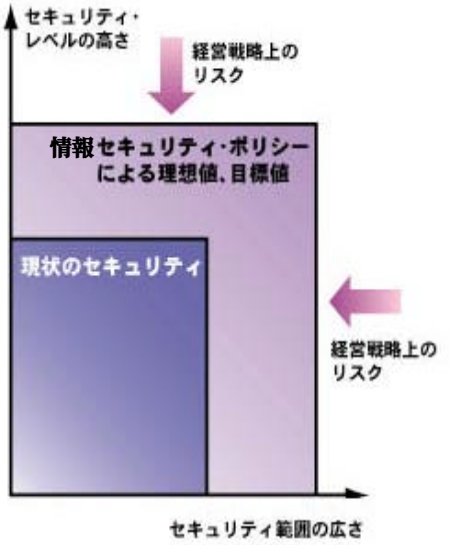
「受け入れられないリスク」だが、「対策を取れない」ような課題はどうするか？
①ポリシー群ではなく、表明や目的、原則群で言及し、姿勢を示す。
②罰則条項による牽制。

情報セキュリティポリシー策定支援コンサルティング説明資料
Copyright © 1996-2002 by Hewlett Packard Japan, Ltd.

全社情報セキュリティポリシーの策定

受け入れるリスクの
２つの観点

(1) 対象範囲
(2) 許容する脆弱性



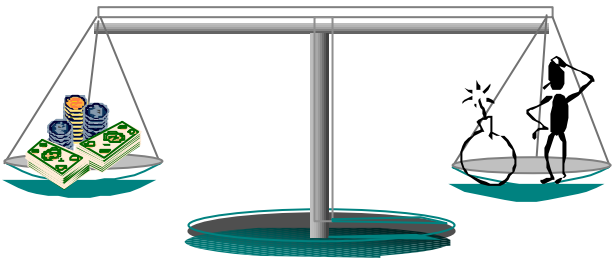
＊必ずしも全社のリスク対策を画一的に定める必要はない。

情報セキュリティポリシー策定支援コンサルティング説明資料

全社情報セキュリティポリシーの策定

情報セキュリティに対する基本姿勢

「情報資産に対するアクセスへのビジネスニーズ」と「これらの資産の機密性、保全性、可用性および適正な使用を守る」との効果的なバランスを取る。

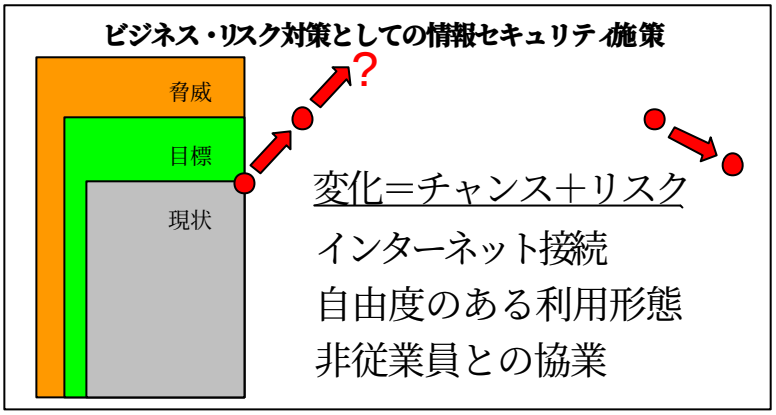


情報セキュリティポリシー策定支援コンサルティング説明資料

Copyright © 1996-2002 by Hewlett Packard Japan, Ltd.

全社情報セキュリティポリシーの策定

Step 1.5.1 目標設定とその根拠→本文（WHAT）と目的（WHY）



＊環境の変化には、もれなくリスクの認識が必要

全社情報セキュリティポリシーの策定

Step 1.5.2 理解の促進→用語定義と遵守事項

用語などの定義

通常の業務で使用していない用語には定義が必要
社外の標準に合わせることを偏重しない（用語対応表で対処）

日本語での留意事項

カタカナの使用の最小化
→カタカナ用語は用語解説（付録）で定義

主語の明文化
→英訳文の試作で検証

全社情報セキュリティポリシーの策定

Step 1.5.2 理解の促進→何を統一的に定めるか

文の種類の事前定義

定義事項の文

遵守事項の文

- 必須行為（People Must Do ：～しなければならない）
- 推奨行為（People Should Do:～することが望ましい）
- 禁止行為（People Must Not Do ：～してはならない）
- 許諾行為（People May Do ：～することができる）

行為の限定ではなく理解の促進

- 支援義務（Company Must Do ：～する）
- 権限留保（Company May Do ：～する場合がある）
- 権限放棄（Company Never Do ：～することはない）

決意表明と事前通知

何を定める？　最低水準（Baseline）と／か適正水準（Just enough）

全社情報セキュリティポリシーの策定

Step 1.5.3 責任者の決定→逸脱手続き（WHO）

＊ビジネスの例外を前提にする

ビジネスの例外→情報システム使用の例外→情報セキュリティの例外

初期値は、代表取締役社長＝経営的・法的な最高責任者

~~「例外を認めない」~~ → 「社長決裁をしなければならない」

責務の委任　　経営資産＝人、物、金、情報

方針内のそれぞれに異なる条件を記載可。　　一般的規則とポリシーの違い

全社情報セキュリティポリシーの策定

Step 1.5 個々のポリシー文の記載内容の要件

何が目標か（WHAT） →あるべき姿の考察
なぜ、それが目標か（WHY） →受け入れられないリスクの考察
誰が責任者か（WHO） →受け入れるリスクの考察

情報セキュリティ体制の確立

Step 2 情報セキュリティ維持のための体制の確立

性善説を前提とする。

情報セキュリティ体制の確立

Step 2 情報ｾｷｭﾘﾃｨ維持のための体制の確立

情報ｾｷｭﾘﾃｨにおける役割の組織化
　　業務としての認識
　　権限、責任、報告　説明）義務

一人二役、二人一役も一定の条件下で認める。
条件としての留意点
　　一人二役では **職務の分離**」
　　例）報告の作成と受理、申請の依頼と承認
　　二人一役では **個人の特定**」
　　例）ログイン **D**の共用

情報セキュリティ対策の設計

Step 3 情報ｾｷｭﾘﾃｨ対策の設計 :全体像と網羅性

Step 3.1 対策の時空間の設計

対策を時間の経過で考える。詳細の程度は任意。
　　予防→保護→検出→対応
対策を空間的に考える。詳細の程度は任意。
　　ネットワーク→サーバ→情報

Step 3.2 テンプレートによる網羅性検証と事前計画

技術的対策
対策の体制

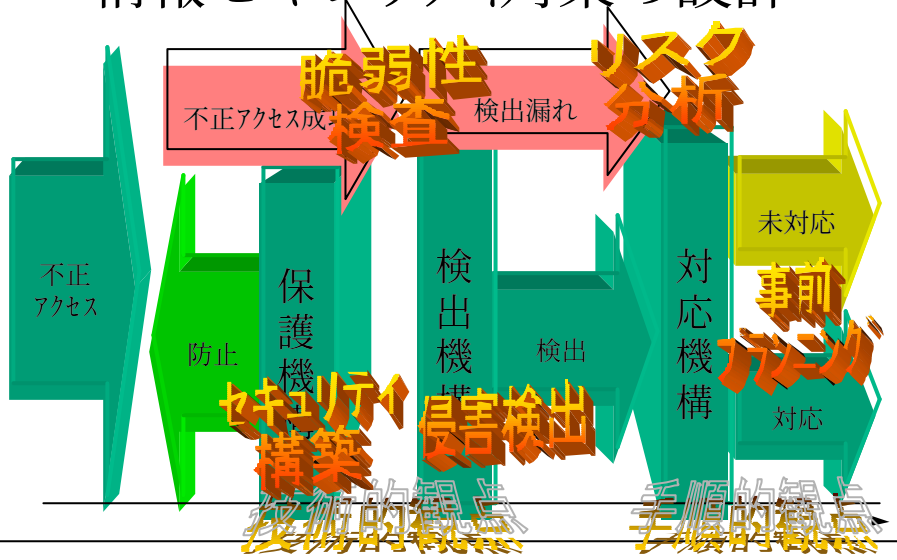
情報セキュリティ対策の設計

Step 3.1.1 対策を時間の経過で考える。詳細の程度は任意。

予防（回避） Avoidance
　無権限の行為を未然にさせないようにすること
保護（防止） Protection
　無権限の行為を不可能（困難）にさせること
検査（保証） Assurance, Assessment, Audit
　定めた保護が機能しているか確認すること
　- 設定内容の検査（静的）
　- 脆弱性の検査（動的）
検出 Detection
　無権限の行為を見つけ出すこと
　- 記録・通知・対処
分析・調査 Investigation
　検出した内容の調査をすること
対応（回復） Reaction/Fix
　行為の被害を最小限にするべく対処すること

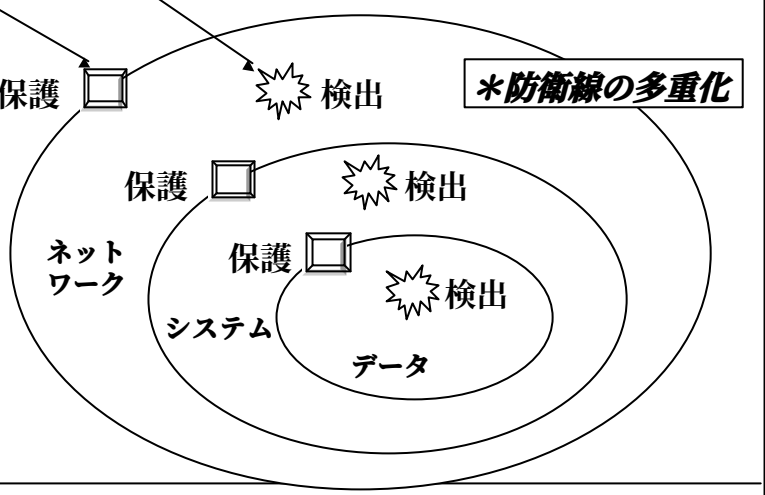
抑止：Prevent
監視：Monitor
対応：Respond

情報セキュリティ対策の設計



情報セキュリティ対策の設計

Step 3.1.2 対策を空間的に考える。詳細の程度は任意。



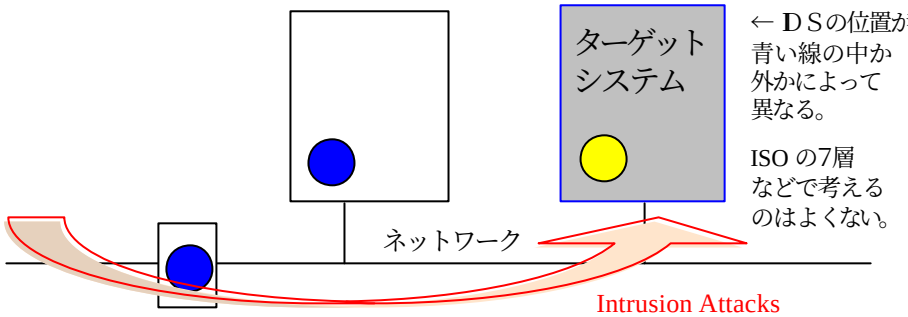
情報セキュリティ対策の設計

Step 3.2.1 テンプレート作成（技術）

対策テンプレート1	予防	防止	検査 (能動)	検出 (受動)
ネットワーク侵入				
システム侵入				
データ・セキュリティ				

情報セキュリティ対策の設計

ネットワーク型ＩＤＳとホスト型ＩＤＳ



ホスト型ＩＤＳ ： ＩＤＳがターゲットホスト内にある場合

ネットワーク型ＩＤＳ ： ＩＤＳがターゲットホスト外にある場合

情報セキュリティ対策の設計

Step 3.2.2 テンプレート作成（体制）

＊事前の計画・準備が必須

対策テンプレート2

	担当者	報告受理 / 承認者
警報監視		
警報内容調査		
警報調査結果報告		→
対応内容考察		
対応内容承認		→
対応作業実施		
対応作業報告		→
効果確認		
効果報告		→

→原因究明と再発防止対策の検討

security 101

IT経営を強化する、セキュア・コンテンツ・マネジメント セミナー
～電子メールポリシーによるリスク管理と生産性向上の実現～

情報セキュリティ対策の設計

Step 3.2.2 テンプレート作成（体制）

事前の計画がされていないと。。。

侵害は、それによる被害の波及が進み、
侵蝕に進化しやすくなる。

避難訓練の喩え

事前計画の考察

（時刻は日本時間。2月10日）

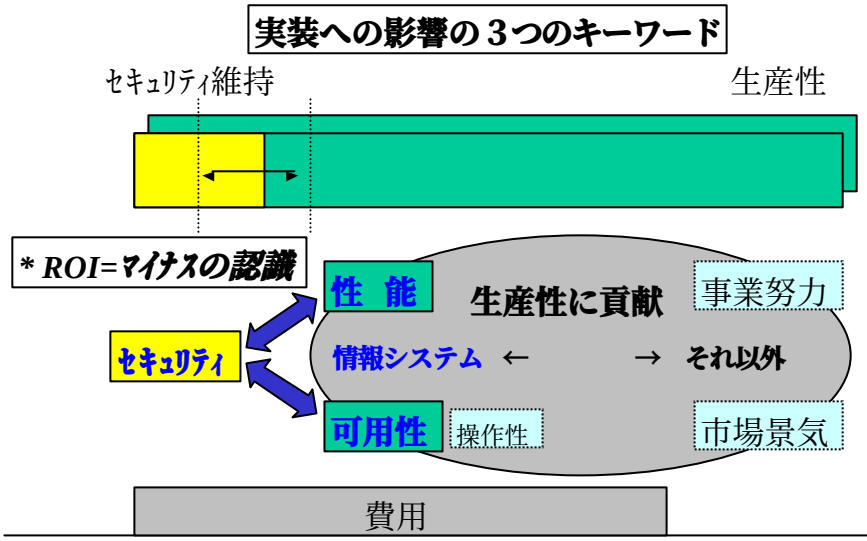
08：47　えひめ丸の遭難信号を海上保安庁がキャッチ。
48　えひめ丸沈没。
09：50　休暇中の米大統領に一報。国家安全保障会議（ＮＳＣ）を中心として事故調査と救命活動をするように命令。日本側へのお詫びと遺憾の意を伝える指示。
55　米太平洋軍外交顧問トワイニング大使から、ホノルル総領事へ連絡。
10：00　ハワイ領事館に対策室設置。
15　海上保安庁から首相官邸の危機管理センターへ連絡。
30　ファーゴ太平洋艦隊司令官からホノルル総領事へ「救命活動に最大限努力」の連絡。
米国務次官補代理が柳井駐米大使に電話で謝罪。
同　センターから首相、官房長官の秘書官らに連絡開始。
40　官房長官に事故の一報。
43　海上保安庁からセンターに「２５人救助」の連絡。
50　首相秘書官から首相に一報。
11：00　首相から秘書官を通じて、米国に人命救助と情報収集の最大限の協力要請を指示。
海上保安庁に遭難事故対策室。米国防次官補から柳井大使に電話。
12：00　首相官邸に連絡室、外務省に対策本部。福田官房長官、前橋市を出発。
30　文部科学省に対策本部設置。
43　安藤危機管理監、同センターに到着。
54　首相、横浜市内のゴルフ場を出発。
13：00　河野外相がフォーリー米駐日大使、米太平洋艦隊司令官に遭難者[illegible]
13　安部**官房副長官**、河野外相が同センターに到着。
43　福田**官房長官**、同センターに到着。
14：16　首相、同センターに。対策会議を開催。
45　福田長官が首相官邸で記者会見。
16：47　伊吹**危機管理担当相**、同センターに到着。
夜　米国務長官が河野外相に電話で陳謝。

内閣情報集約センター（危機管理センター）

首相官邸警戒態勢（2000年1月～）
官房長官、官房副長官、危機管理担当相
「３０分以内に官邸に駆ける当番制」

1998年海上自衛隊なだしお衝突
竹下首相、小渕官房長官の
首相官邸入りは8時間後

情報セキュリティ対策の設計



情報セキュリティ対策の設計

Step 3 情報セキュリティ対策の設計 :全体像と網羅性

Step 3.1 対策の時空間の設計

対策を時間の経過で考える。詳細の程度は任意。

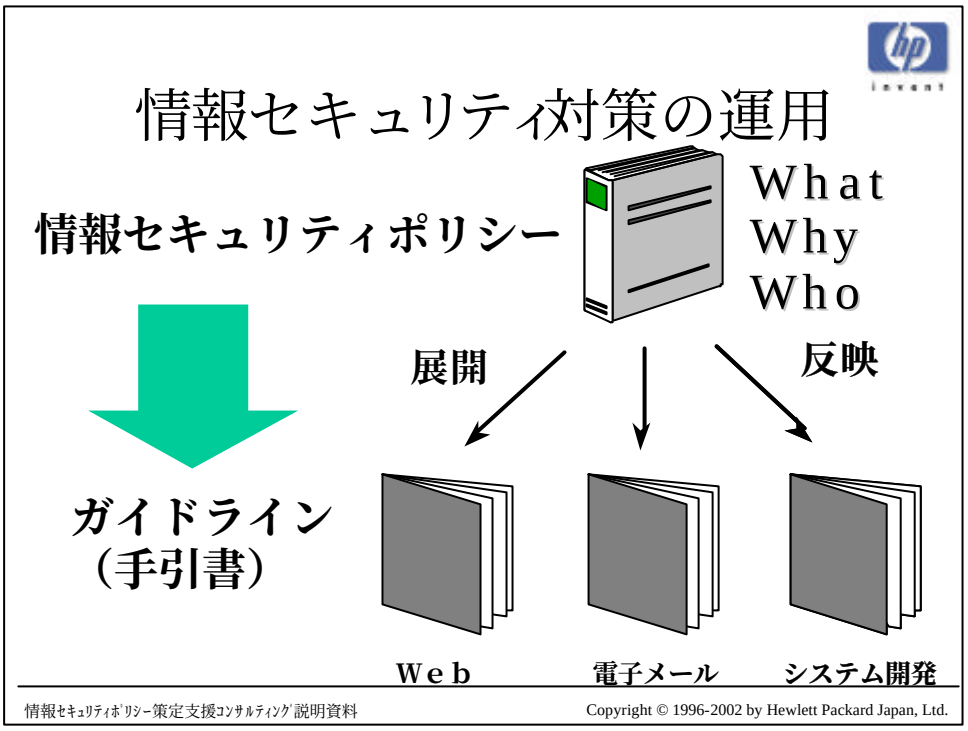
予防→保護→検出→対応

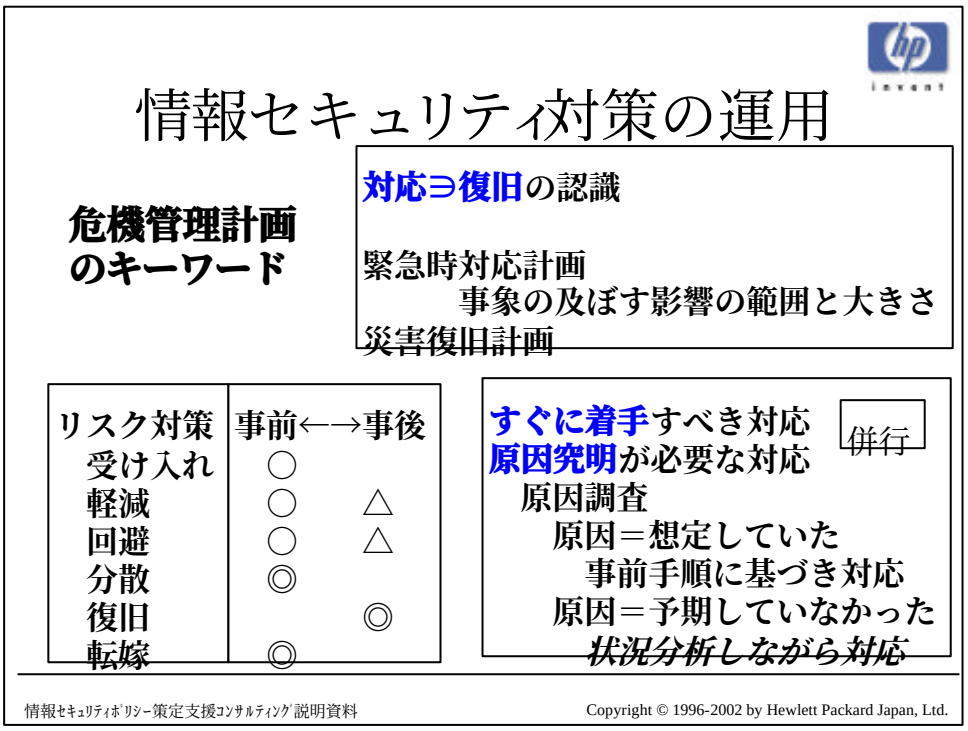
対策を空間的に考える。詳細の程度は任意。

ネットワーク→サーバ→情報

Step 3.2 テンプレートによる網羅性検証と事前計画

技術的対策
対策の体制





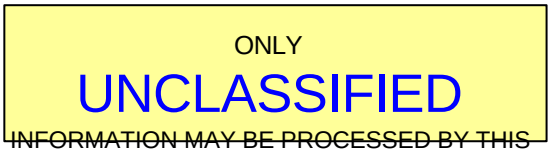
情報セキュリティ対策の運用

国の取り組み

総務省：
「情報セキュリティ・ビジネスの発展と官民連携のあり方に関する調査研究会」
2001年10月24日 第１回会合
2002年5月までに報告をまとめる
警視庁：
「サイバー 電脳）テロ対策協議会」
2001年10月23日発足
警視庁と電力や通信を含むインフラ企業

情報セキュリティ対策の運用

事例



情報セキュリティポリシー策定支援コンサルティング説明資料
Copyright © 1996-2002 by Hewlett Packard Japan, Ltd.

情報セキュリティ啓発と教育

Step 4 情報セキュリティ啓発と教育

品質保証との類似性

類似点　ISO 9001 プロセス型

一次的生産性をあげるものではない
完全を目指せば、きりがない
発生した場合の問題はビジネスに影響する
加害者になる場合がある

相違点→追加点　ISO 14001 PDCA型

取り組むべき部署の範囲の程度
対象業務との独立性の程度
時間経過に伴う効果の劣化性の程度

→ 広範な体制が必要

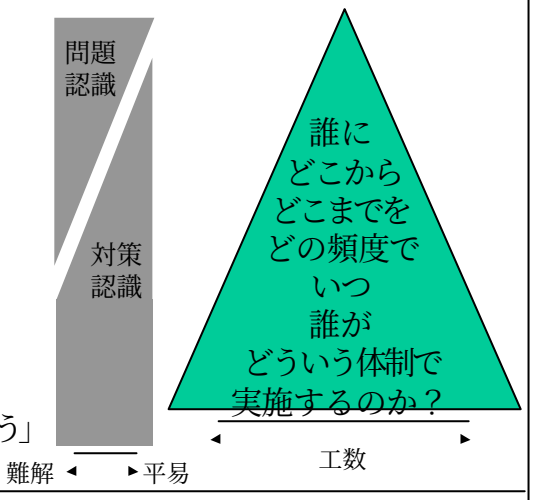
情報セキュリティ啓発と教育

周知・徹底の３つのレベル

Step 4.1 啓発（awareness）
知識
「知ってもらう」

Step 4.2 教育（education）
理解
「正しくわかってもらう」

Step 4.3 訓練（training）
実践
「できるようになってもらう」



情報セキュリティ啓発と教育

＊全使用者に年最低 1回の教育が必要

＊実施状況の定量評価が必要

→集合教育以外の検討＝WBT (Web Based Training) など

http://www.jpn.hp.com/go/education

**コンピュータは信頼できないが、
人間はもっと信頼できない。**

書籍「マーフィの法則」より
アーサー・ブロック著、倉骨彰訳、アスキー出版局発行

コンピュータは犯罪を起こさない

アラン・E・ブリル氏
元ニューヨーク捜査局情報安全部長

情報セキュリティ維持の監査

Step 5 情報ｾｷｭﾘﾃｨ維持の監査

Step 5.1 自己検査
- 意識向上（誰かが」ではなく自分達が」）
- 全員参加による情報ｾｷｭﾘﾃｨの維持

Step 5.2 内部監査
- 牽制効果
- 現場との 敵対」ではなく支援」の立場
- 違反への対応＝始末書ではなく理由書
- 現場に則した HOW を知る機会損失の防止

Step 5.3 外部監査
- 客観性、専門性、独立性
  （内的主観の回避、外的評価の認識、利害関係依存の排除）

手段としての自動化

基本プロセス

- Security Classification　セキュリティーの区分
- User Account Management　使用者のアカウント管理
- Identification / Authentication　識別 / 真正確認
- Authorization　認可
- Risk Acceptance　危険性の承認
- Security Monitoring　セキュリティーの監視
- Security Incident Response　セキュリティー上のインシデントへの応答
- Self Audit　自己監査
- Audit Review　内部監査による調査
- Security Process Maintenance　セキュリティープロセスの維持

ﾋﾞｼﾞﾈｽﾍﾞｰｽ・ｾｷｭﾘﾃｨのすすめ

Did You Lock the Door?

Step 1) 全社情報セキュリティポリシーの策定
Step 2) 情報セキュリティ体制の確立
Step 3) 情報セキュリティ対策の設計 ・開発 ・導入 ・運用
Step 4) 情報セキュリティ啓発と教育
Step 5) 情報セキュリティ維持の監査

まとめ

Did you Lock the Door?

情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ策定支援ｺﾝｻﾙﾃｨﾝｸﾞ説明資料