コンピュータ・インシデントへの対応計画と手順について

～ ポリシー文書策定から実践まで ～

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&ITストラテジー・コンサルティング・グループ

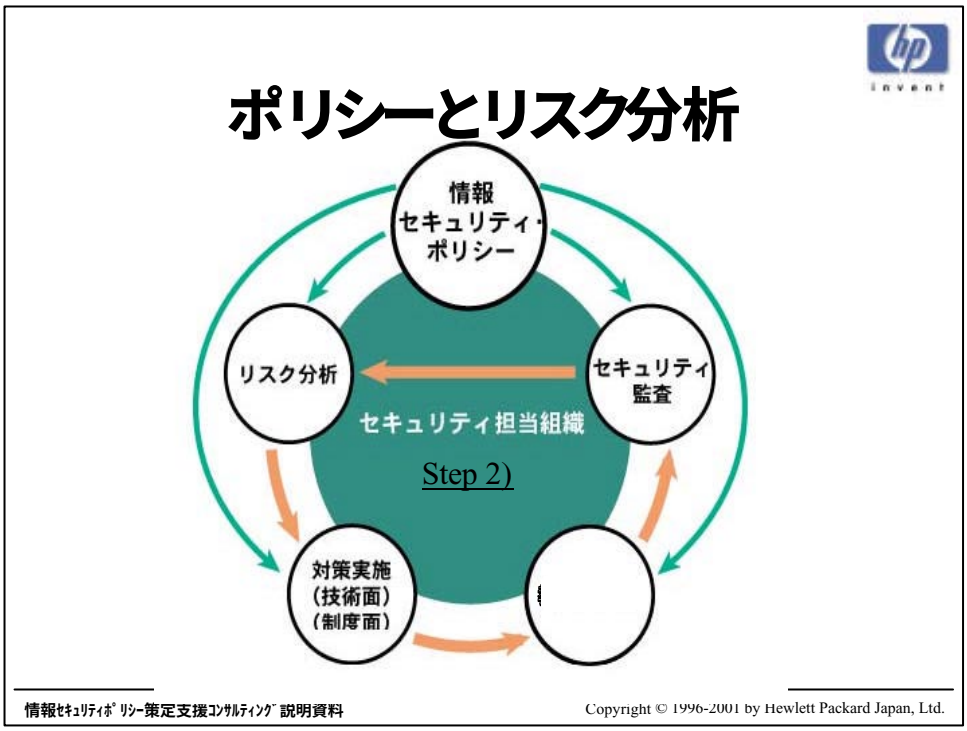
講師経歴

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ｺﾝｻﾙﾃｨﾝｸﾞ事業統括本部　ｾｷｭﾘﾃｨ　&ITｽﾄﾗﾃｼﾞｰ･ｺﾝｻﾙﾃｨﾝｸﾞ ｸﾞﾙｰﾌﾟ長
シニア・コンサルタント

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、ＦＢＣ(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。
1999 年 5 月より現職。

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　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


情報セキュリティ対策の設計
脆弱性検査
リスク分析
不正ｱｸｾｽ成功
検出漏れ
不正ｱｸｾｽ
防止
保護機構
検出機構
検出
対応機構
未対応
事前ケア
対応
セキュリティ構築
侵害検出
技術的観点
手順的観点
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
Copyright © 1996-2001 by Hewlett Packard Japan, Ltd.


ポリシーとリスク分析
情報セキュリティ・ポリシー
リスク分析
セキュリティ監査
セキュリティ担当組織
Step 2)
対策実施
(技術面)
(制度面)
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
Copyright © 1996-2001 by Hewlett Packard Japan, Ltd.

全社情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの策定

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？

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

全社情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの策定

Step 1.1 文書の位置づけと構成の決定

情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ」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

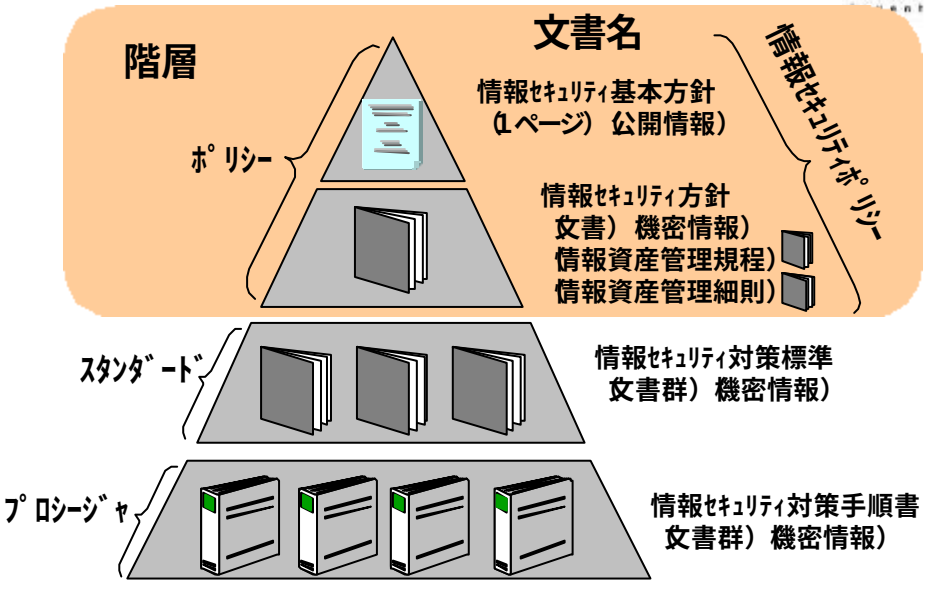
◎罰則条項
◎従業員以外 派遣、委託）への適用

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

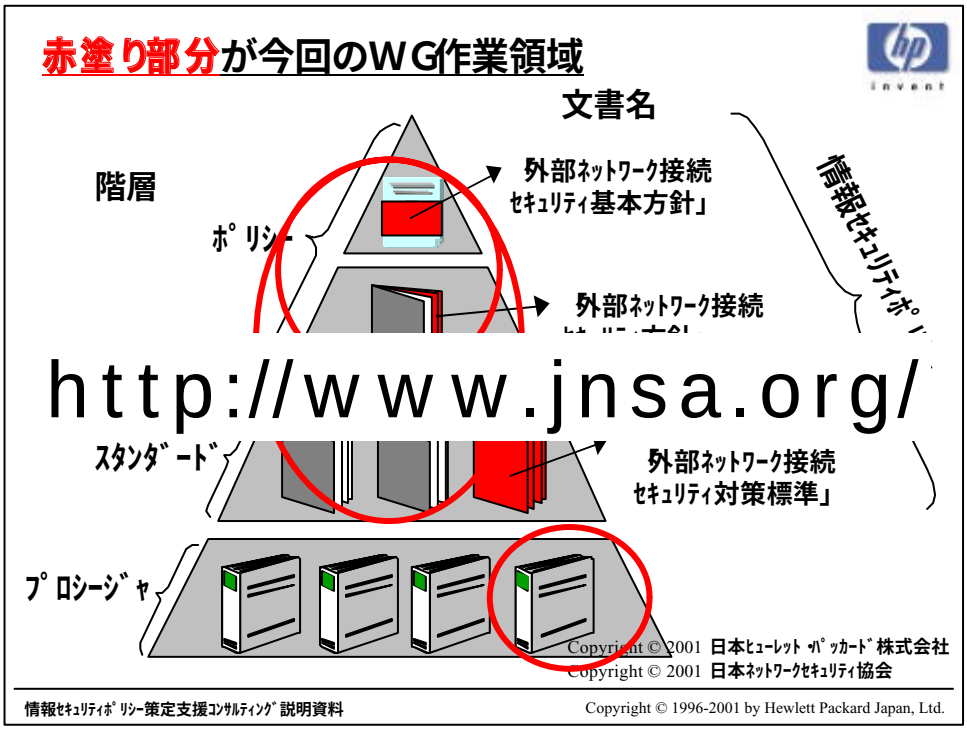
ポリシーと標準、手順書

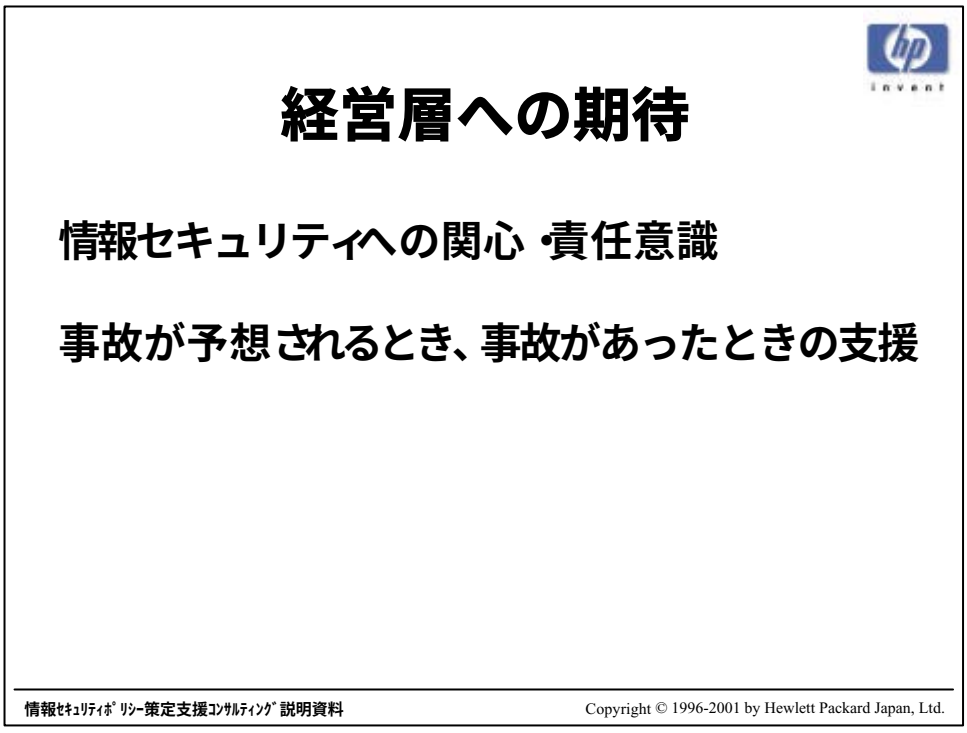
情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ策定支援ｺﾝｻﾙﾃｨﾝｸﾞ説明資料

情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ関連文書群の全体構成



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





全社情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの策定

Step -1 情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの必要性

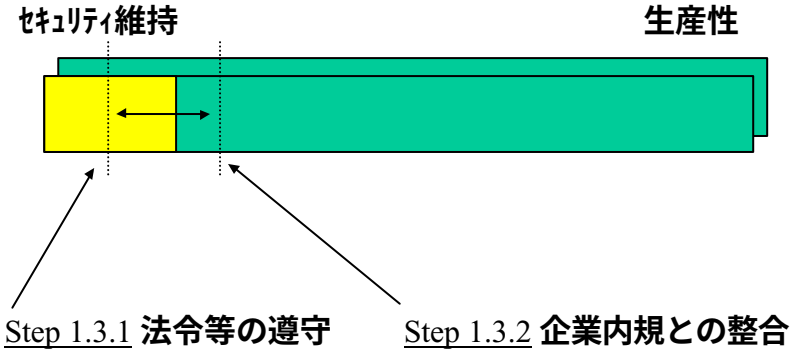
なぜ、作られるようになったか？

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

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

全社情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの策定

Step 1.3 背景の調査と認識

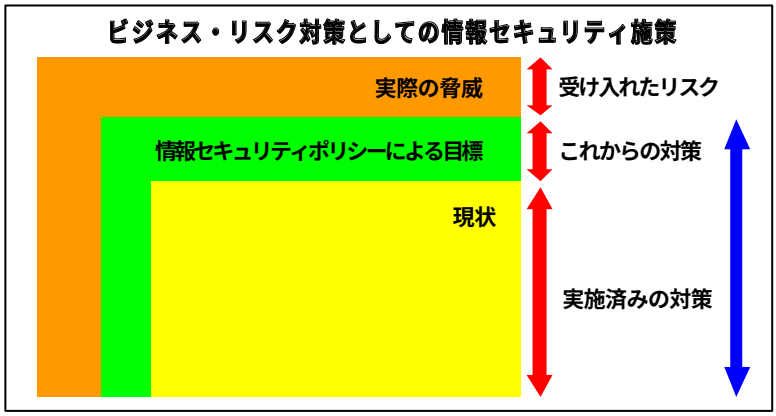


Step 1.3.1 法令等の遵守　　Step 1.3.2 企業内規との整合

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

全社情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの策定

Step 1.5.1 目標設定とその根拠→本文（WHAT）と目的（WHY）

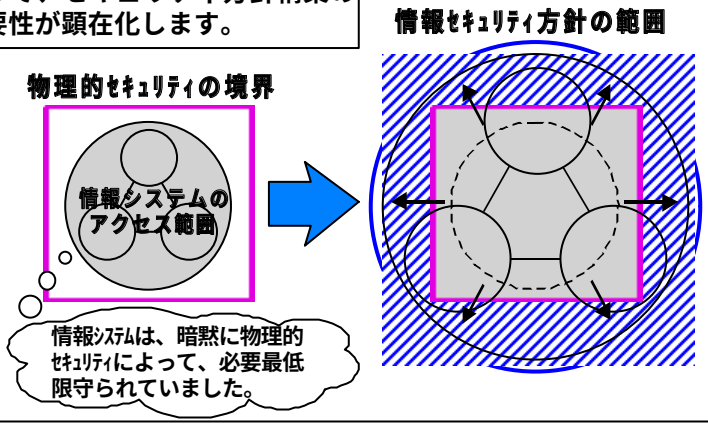


＊経営者とのコミュニケーション・ツールとしてのポリシー

全社情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの策定

Step -1 情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの必要性

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。



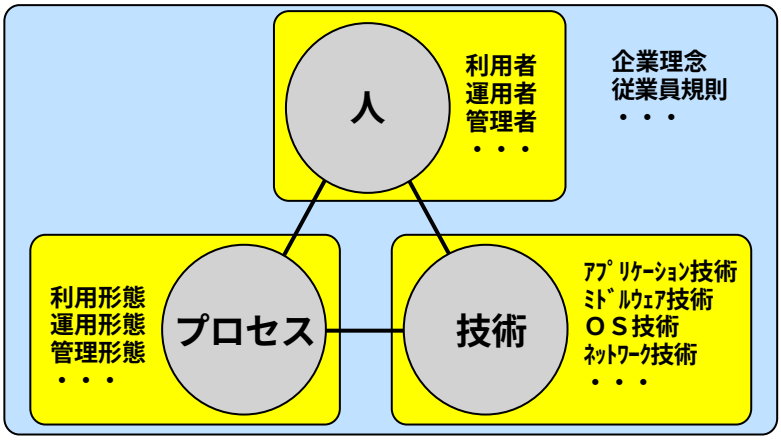
全社情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの策定

Step -1 情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの必要性

利用形態の自由度の変化

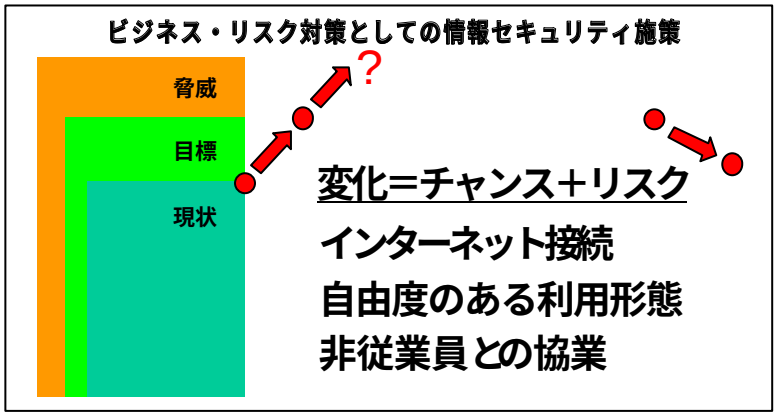
全社情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの策定

Step -1 情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの必要性



全社情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの策定

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ﾎﾟﾘｼｰの策定

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）
- 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）

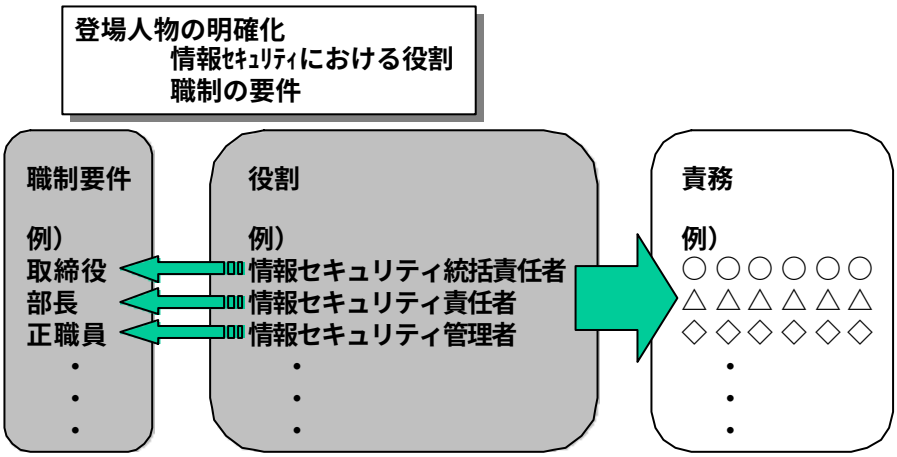
行為の限定ではなく理解の促進

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ﾎﾟﾘｼｰの策定

Step 1.4 ポリシー群の洗い出し



情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ策定支援ｺﾝｻﾙﾃｨﾝｸﾞ説明資料 Copyright © 1996-2001 by Hewlett Packard Japan, Ltd.

全社情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの策定

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

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 Copyright © 1996-2001 by Hewlett Packard Japan, Ltd.

全社情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの策定

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。

不正アクセス」という言葉

無権限（不許可）のアクセス
権限者の誤用

技術的に不可避な事柄

全社情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの策定

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）

(Sensitibity Level, Compartment & Marking)

全社情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰの策定

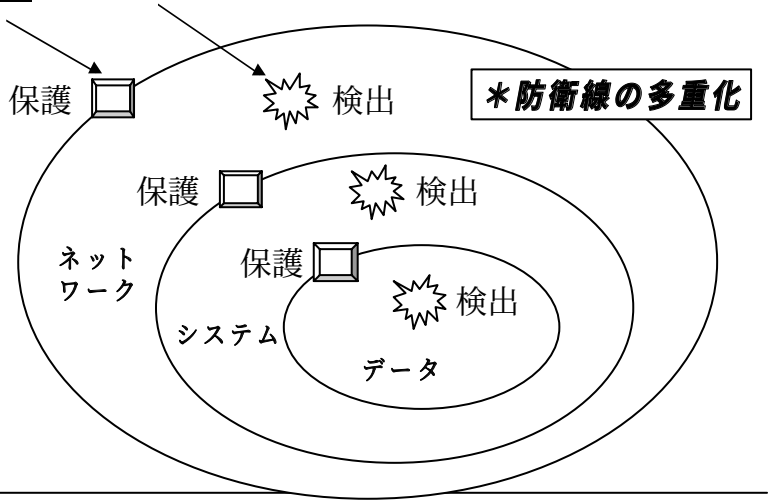
Step 1.4 ポリシー群の洗い出し

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
外部委託とサービス提供業者の利用
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）

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。



情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ策定支援ｺﾝｻﾙﾃｨﾝｸﾞ説明資料

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				

情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ策定支援ｺﾝｻﾙﾃｨﾝｸﾞ説明資料

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

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

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

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

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 遭難者救出で最大限の協力要請。
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分以内に官邸に戻る当番制」

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

情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ策定支援ｺﾝｻﾙﾃｨﾝｸﾞ説明資料

対応計画成功のキーワード

ワン・ストップ、ノン・ストップ

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

対応計画成功のキーワード

4つの役割
管理と判断
暫定対応
恒久対応
渉外

対応計画成功のキーワード

被害であることの認識

情報セキュリティ対策の運用

危機管理計画のキーワード

対応ヨ復旧の認識

緊急時対応計画
　　事象の及ぼす影響の範囲と大きさ
災害復旧計画

リスク対策	事前←→事後	
受け入れ	○	
軽減	○	△
回避	○	△
分散	◎	
復旧		◎
転嫁	◎	

すぐに着手すべき対応
原因究明が必要な対応　併行
　原因調査
　　原因＝想定していた
　　　事前手順に基づき対応
　　原因＝予期していなかった
　　　状況分析しながら対応

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

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
- 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
- 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

情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ策定支援ｺﾝｻﾙﾃｨﾝｸﾞ説明資料

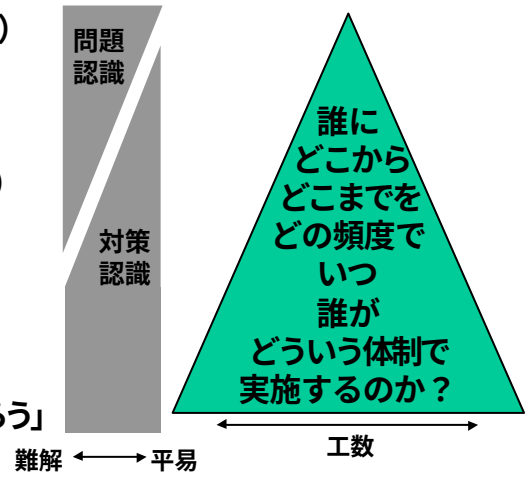
情報セキュリティ啓発と教育

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」

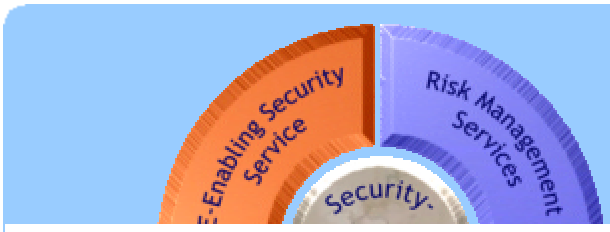


ベンダー選定のポイント

納品物の品質が定量的に評価できる事柄：
- 提案要件指定
- 価格競争

納品物の品質が定量的に評価できない事柄：
- 価格帯指定
- 提案内容競争

ヒューレット・パッカードの
情報セキュリティ・コンサルティング サービス



リスク・アセスメント
脆弱性検査
eSecurity Probe
侵害監視
セキュリティ・ダッシュボード

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

Vaulting (SAFE)
TripWire Express
VirtualVault Express

Trusted PKI
セキュリティポリシー策定
セキュリティ社内教育・啓発

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

CSIRT体制と効果的な
インシデント対応について

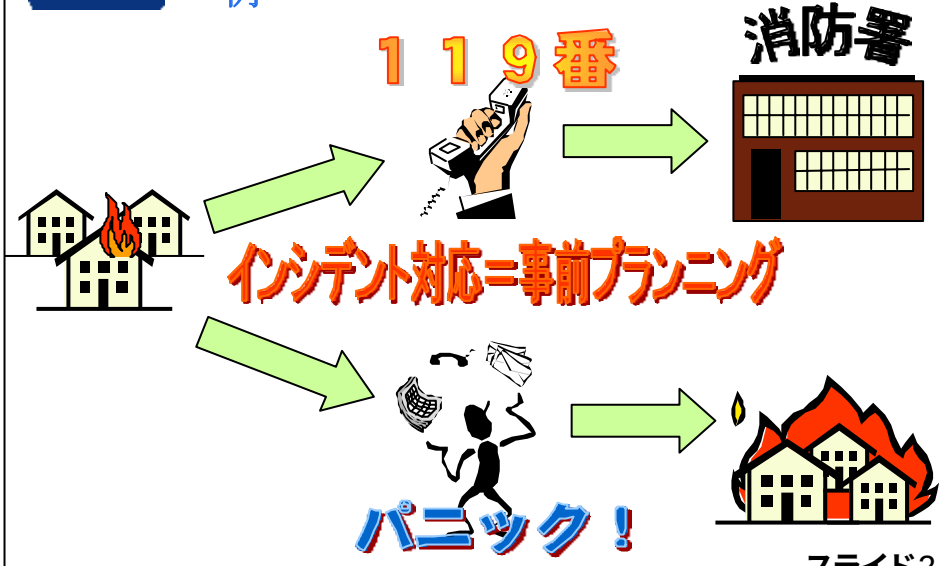
情報処理振興事業協会

セキュリティセンター

この資料は http://www.ipa.go.jp/ で公開されている資料の抜粋です。全文については、上記 URL から入手してください。

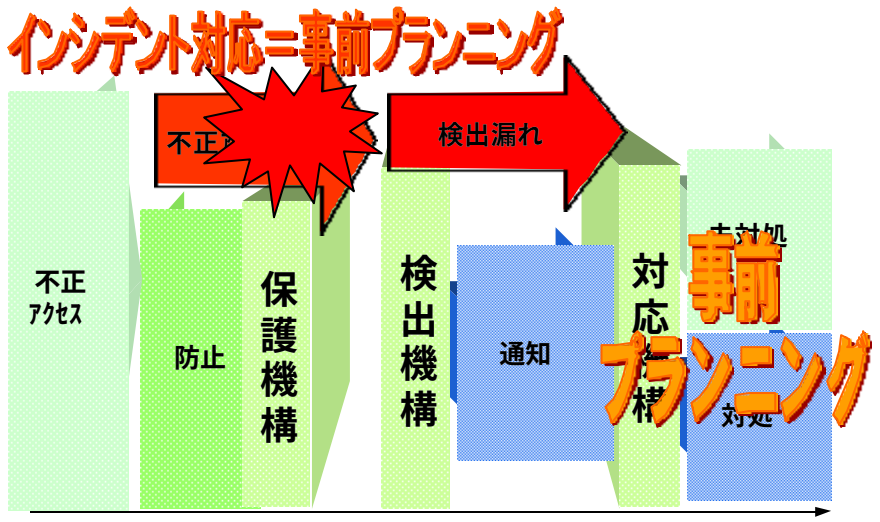
スライド1

インシデント対応の必要性 ―例



スライド2

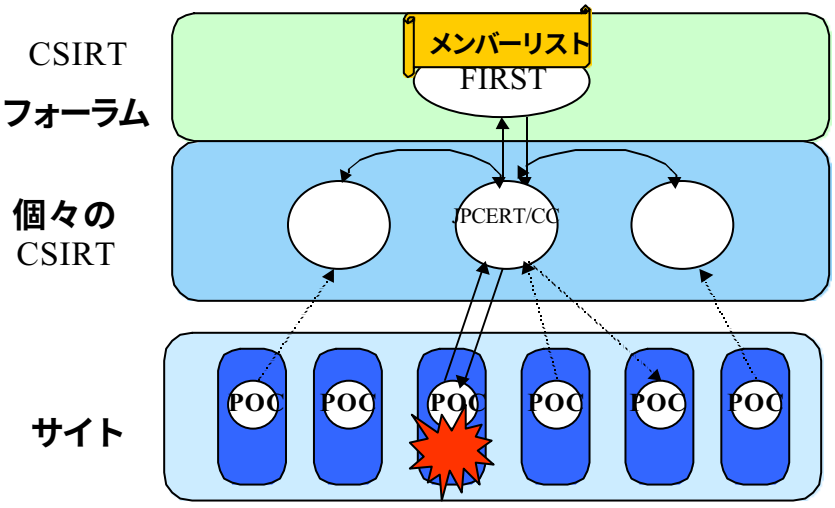
事前プランニングの必要性
ーコンピュータインシデントの場合



出典：GAO(米国会計検査院) / AIMD-96-84 Defense Information Security

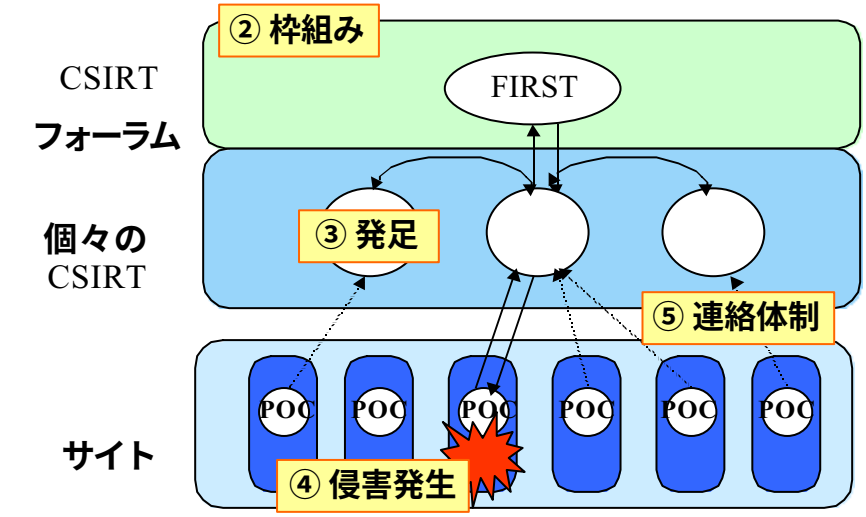
スライド3

インシデント対応のフレームワーク
ー全体の仕組み



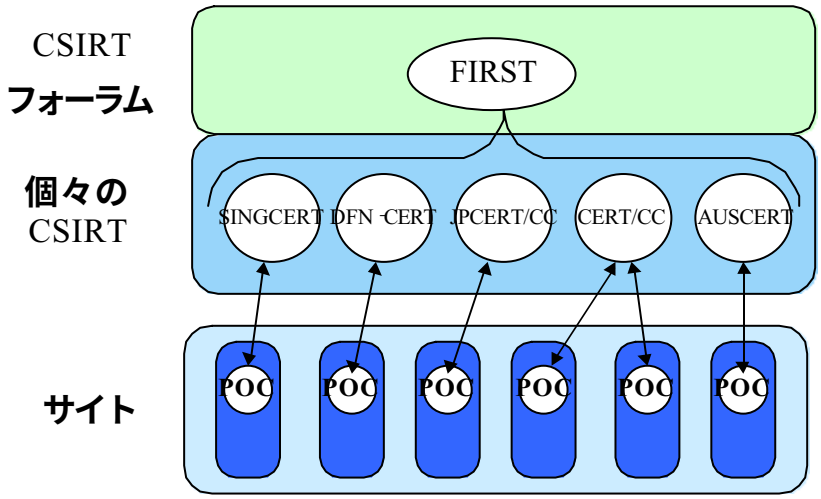
スライド4

インシデント対応のフレームワーク
－全体の枠組み



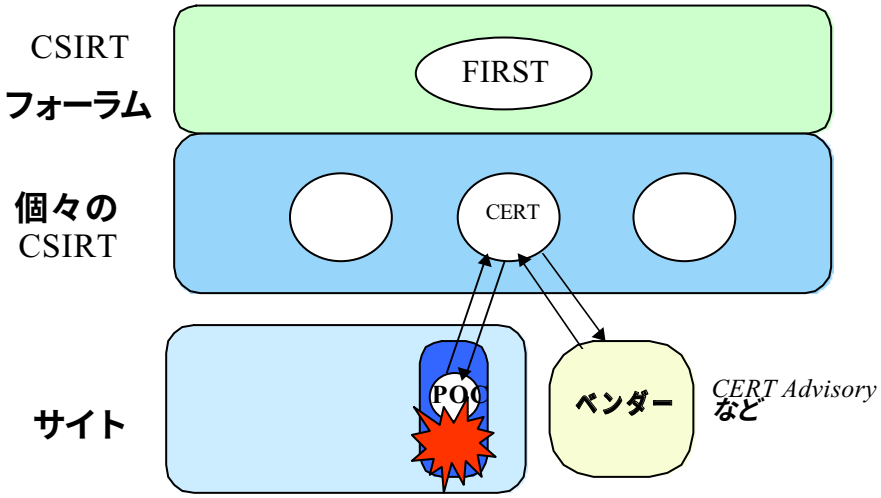
スライド5

インシデント対応のフレームワーク
－世界規模のCSIRT体制



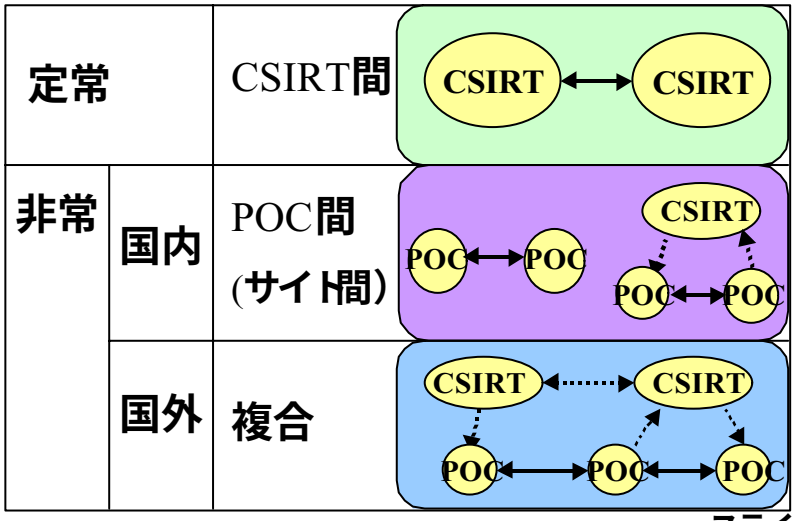
スライド6

インシデント対応のフレームワーク
ーベンダーとの連携



スライド7

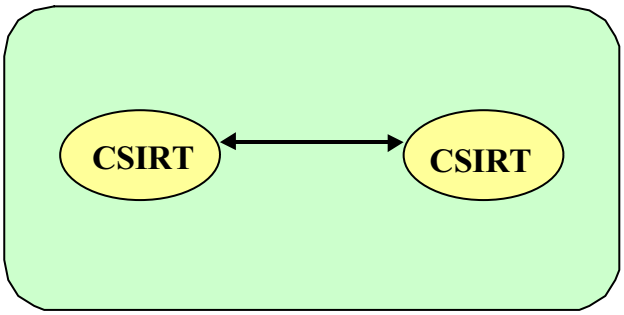
関係者間の連絡体制
ーインシデントが発生した際の連絡体制



スライド8

関係者間の連絡体制
ーインシデントが発生した際の連絡体制

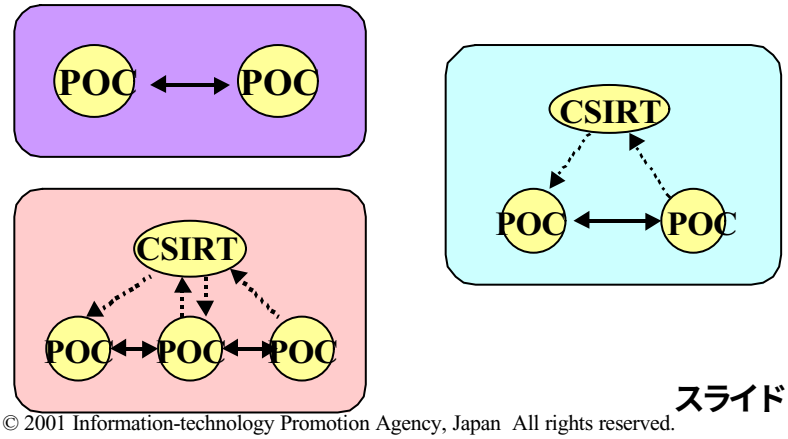
• CSIRT間



スライド9

関係者間の連絡体制
ーインシデントが発生した際の連絡体制

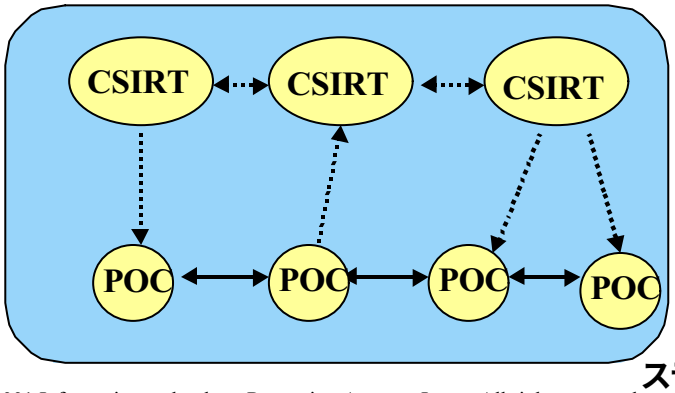
• POC間



スライド10

関係者間の連絡体制
ーインシデントが発生した際の連絡体制

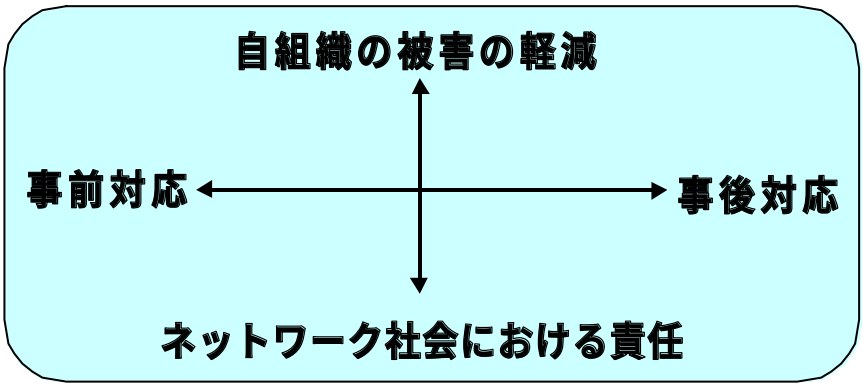
• 複合（CSIRTとPOC間）



スライド11

まとめ

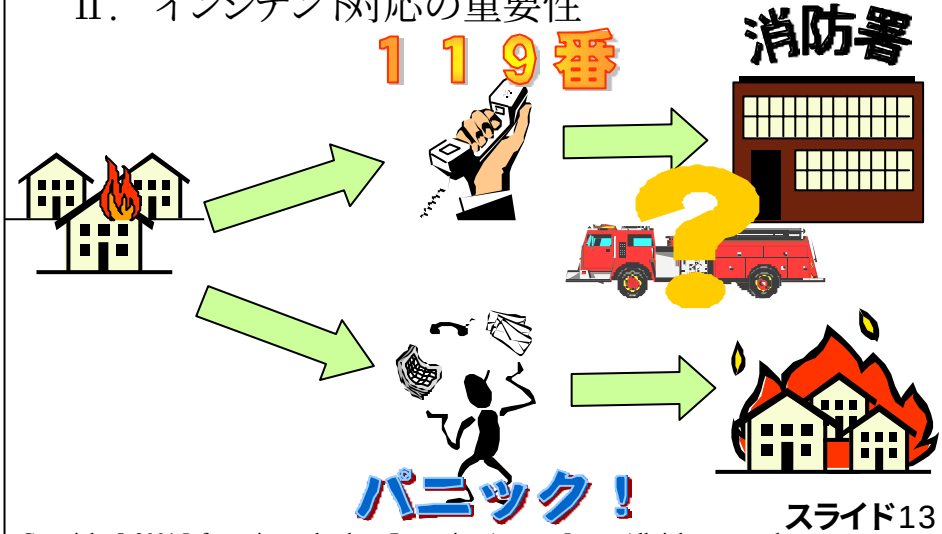
II． インシデント対応の重要性



スライド12

まとめ

Ⅱ． インシデント対応の重要性



スライド13