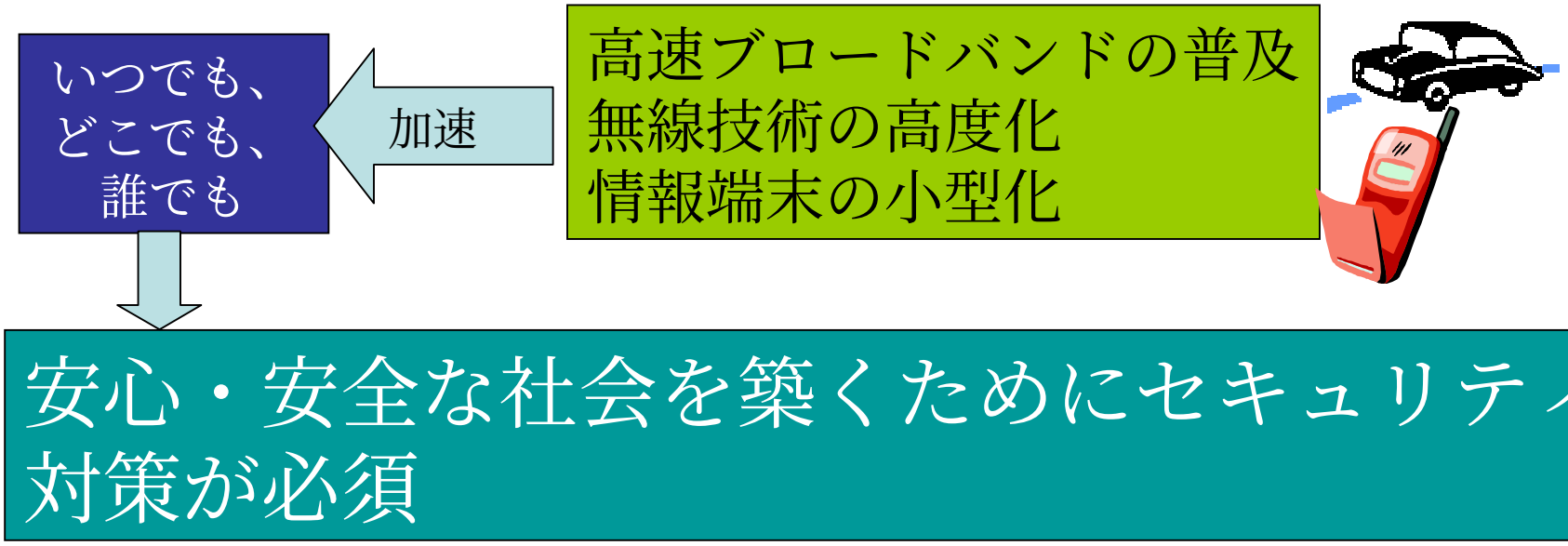
Empowered by Innovation NEC

セキュリティマネジメント と認証

NEC　ユビキタスソフトウェア事業部
小松　文子

U can change.

ユビキタス社会とセキュリティ

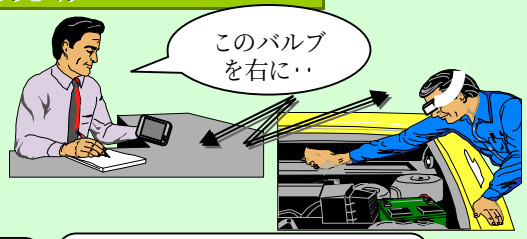


IT環境の変化により、脅威・脆弱性が変化しその対策が必要
①攻撃への対抗手段
②法遵守
③認証
　すべての構成要素を識別しシームレスなサービスを提供

ユビキタスオフィスの到来

ビジネスのあらゆるシーンで自由にコラボレーション

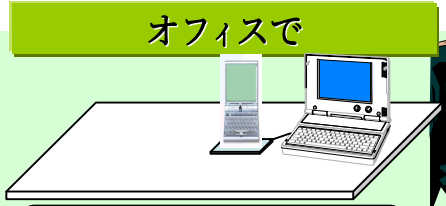
作業現場で



(サーバの) ビデオマニュアルを検索、再生、作業も効率アップ

ライブカメラで状況を見ながら、オペレート支援 (HMDで作業者ﾊﾝｽﾞﾌﾘｰ)

オフィスで



無線内線電話として利用可能で、デスク上スッキリ

オフィス内のどこでも、メールや予定確認。

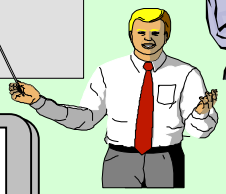
オフィスPCから無線LANやディスプレイ機能を利用

オフィス内位置確認による、構内案内。在席管理

ユビキタス
オフィス
基盤

会議/打合せ等で

Cタイプ
・小型
・軽量
・高性能



通訳サーバで、外国人と会話 (基本会話のみ＋各業種対応は個別対応)
*VoIPによる通訳電話方式

机上のパソコンからWeb会議。会議資料を共有し、音声、動画で意見交換。

会議等の音声を録音。文字に変換し、後から目的の場所を検索??

お客様先で

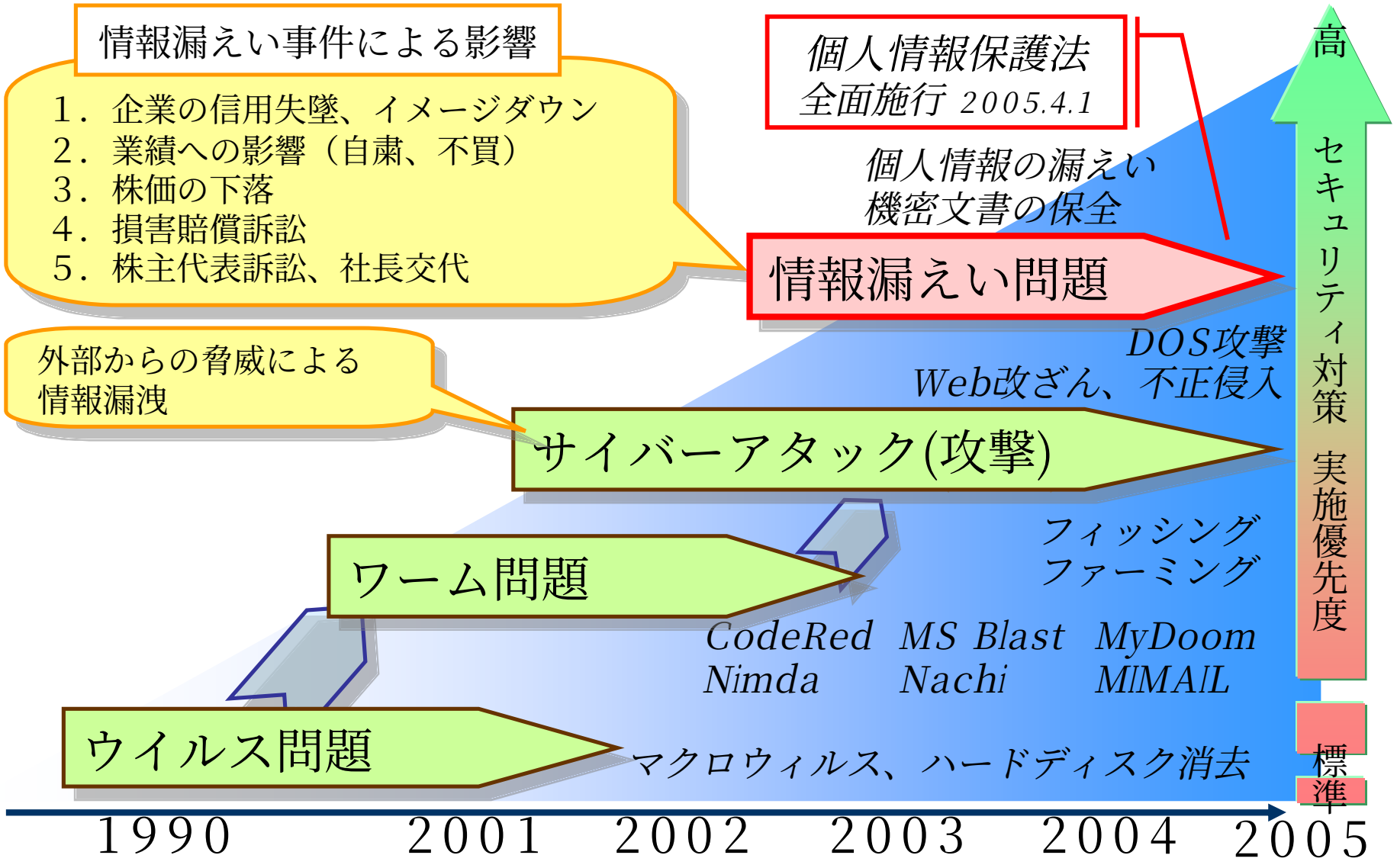
目の前のお客様情報を取得、最適な情報提供

ショートメッセージ (簡単な用件等) を音声で作成、メール送信

One to One Marketing

目次

拡大する情報セキュリティの脅威

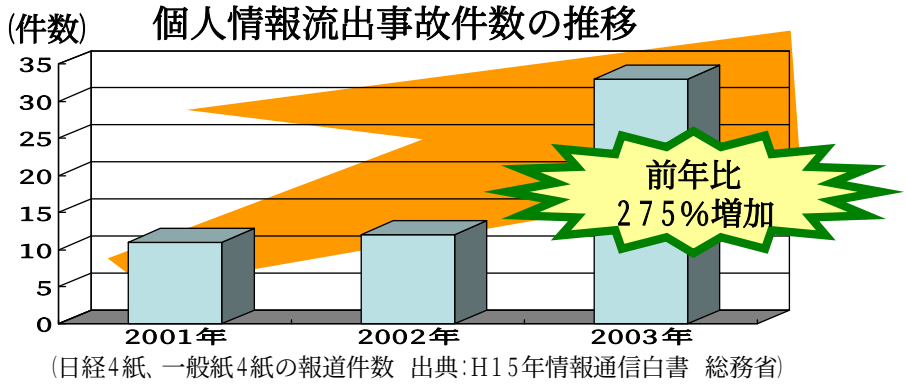


多発するセキュリティインシデント

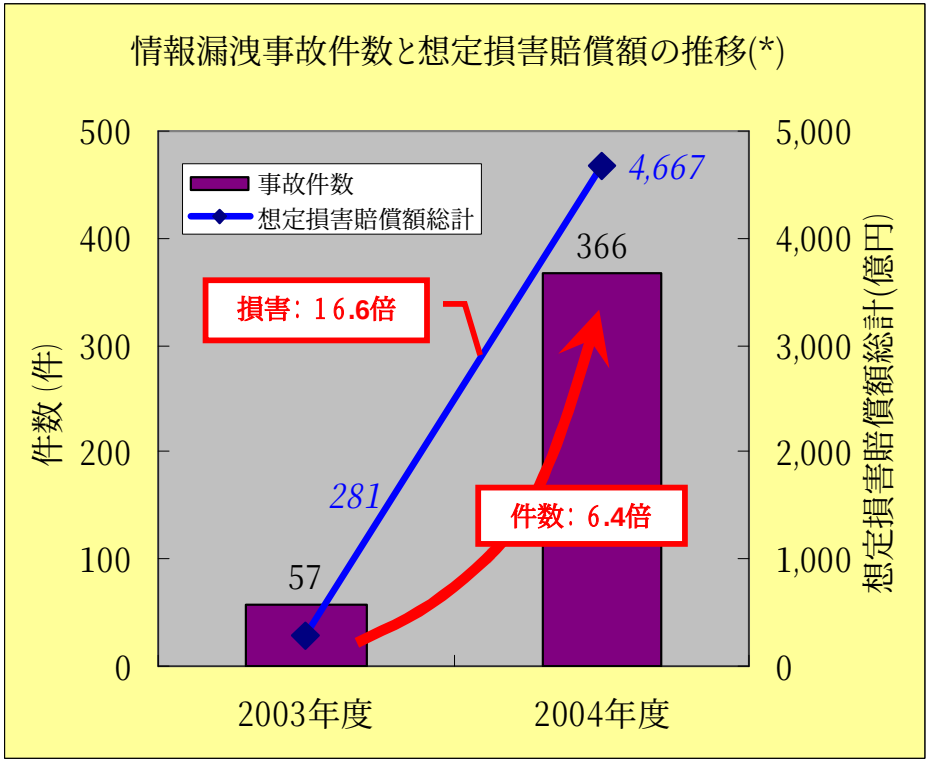
- **個人情報漏えい事件は経営リスク**
  - 個人情報漏えい事件が２００４年度には６倍増
  - 損害賠償額(平均１３.９億円*)のインパクトだけでなく、イメージダウンも深刻

(*: 日本ネットワークセキュリティ協会(JNSA)調査報告２００４年度より)

時期	組織名	漏洩規模	備考
2004.8	信販カードA社	約48万人	全会員に500円相当の金券配布
2004.3	通販B社	約30万人	最大66万人分
2004.2	プロバイダC社	約450万人	全会員に500円相当の金券配布
2003.10	コンビニD社	約18万人	対象者に1000円のカード配布
2003.6	コンビニE社	約56万人	全会員に500円の商品券配布



(日経4紙、一般紙4紙の報道件数　出典:H１５年情報通信白書　総務省)



個人情報保護法

個人情報保護法完全施行に対して企業での対策が必須

- ５０００件以上の個人情報を利用する企業に適切な取り扱いを義務付け
- 個人情報に対する意識改革：“企業のもの”から“お客さまからの預かりもの”へ
- 個人情報の取得・利用・管理に責任を負わなければならない

個人情報(2条1項)

・生存する個人に関する情報であって、
・当該情報に含まれる氏名、生年月日その他の記述等により
・特定の個人を識別することができるもの

個人情報の保護に関する法律、
公布　２００３年5月３０日、施行　２００５年 4月 １日

個人情報保護法

①利用目的の特定、制限（15条、16条）
②適正な取得と利用目的の通知（17条、18条）
③内容の正確性確保（19条）
④安全管理措置（20条～22条）
⑤第三者提供の制限（23条）
⑥公表、開示、訂正、利用停止等（24条～27条）
⑦苦情の処理（31条）

個人情報取扱事業者
（社団、個人も該当）

保有個人データ

市販人名簿等

・紙・電子を問わず整理・分類された５０００件以上の個人データを事業に用いる

・官報等の公開情報
・個別に収集した情報
・市販の情報
（映像情報、メールアドレス、名刺も対象）

・立法府・司法府
（別途取扱いを制定）
・行政機関
・独立行政法人

（憲法で保証）
・報道活動
・著述活動
・学術研究
・宗教活動
・政治活動

（他人作成、非変更
氏名・住所・電話番号のみ）
・電話帳、カーナビ等

２．情報セキュリティ対策

情報セキュリティ　リスクマップ

漏洩

■PC/媒体の紛失
■書類の紛失
■盗難
■社員による不正持ち出し
■ミスによる流出
■PC・書類の廃棄に伴う流出
■不正アクセス
■ワーム・ウィルス
■ソーシャルエンジニアリング
■輸送時の紛失(宅配便)
■無線LAN
■白版消し忘れ

破壊

■社員によるデータ消失
■自然災害、人災、停電、機器故障、落下、コーヒー
■不正アクセス、ワーム、サイバーテロ
■搬送中(事故、持ち逃げ)
■オペミス(通常/保守)
■プログラムバグ
■媒体劣化
■テロ

(資源)消費

■SPAM
■ワームによるNWバンド消費
■自然災害
■オペミス
■故障
■空調トラブル
■テロ
■インターネット私用

信用低下

■風評被害
■信用失墜

改ざん

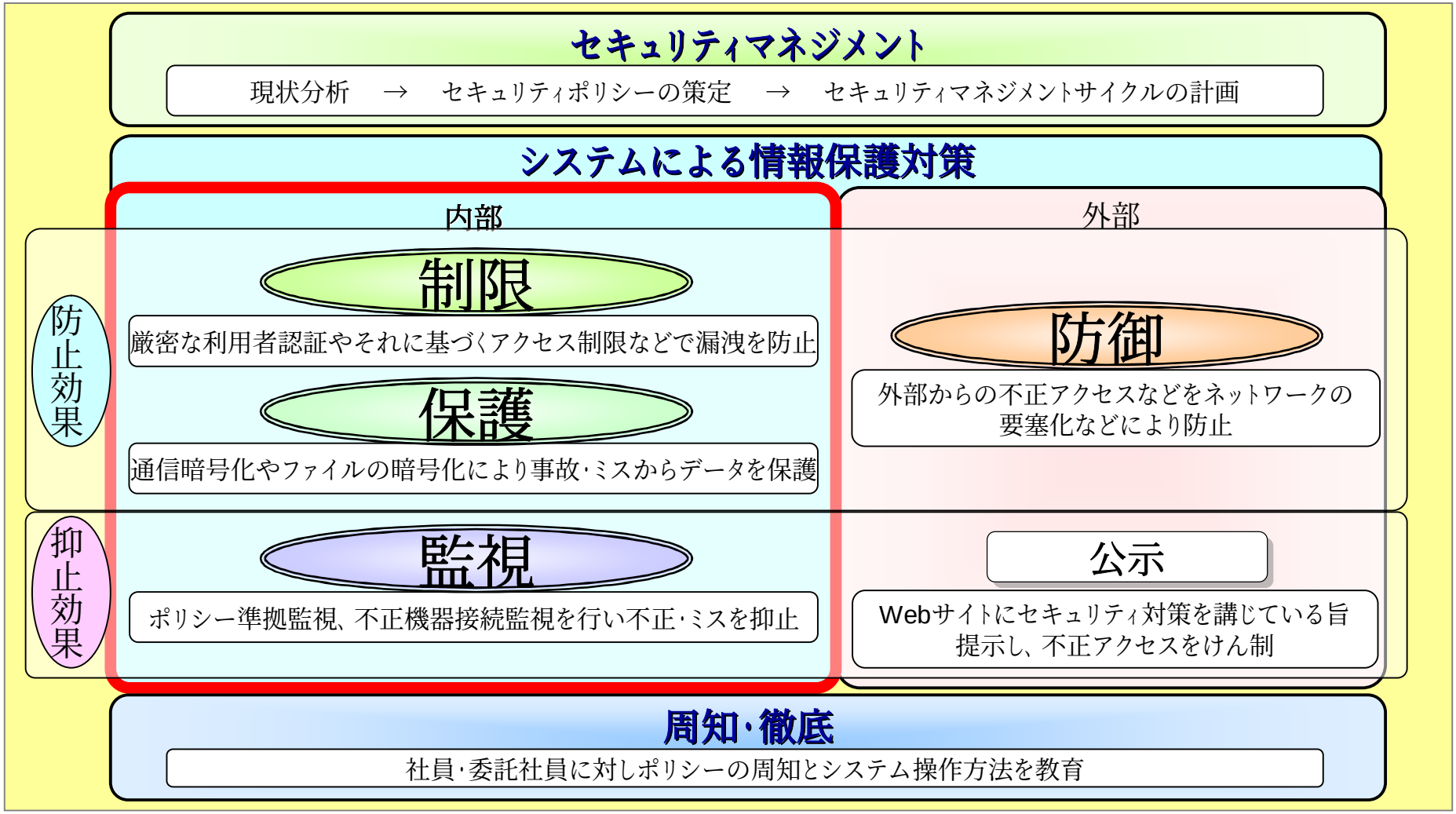
■内部者の改ざん(不正発覚阻止)
■不正アクセス
■HPの改ざん

サービス妨害

■DoS攻撃
■DDoS攻撃
■サイバー・シットイン
■回線妨害

情報セキュリティ対策の観点

制限・保護・監視･防御の４つの観点で対策を検討
セキュリティマネジメント・周知・徹底が重要！

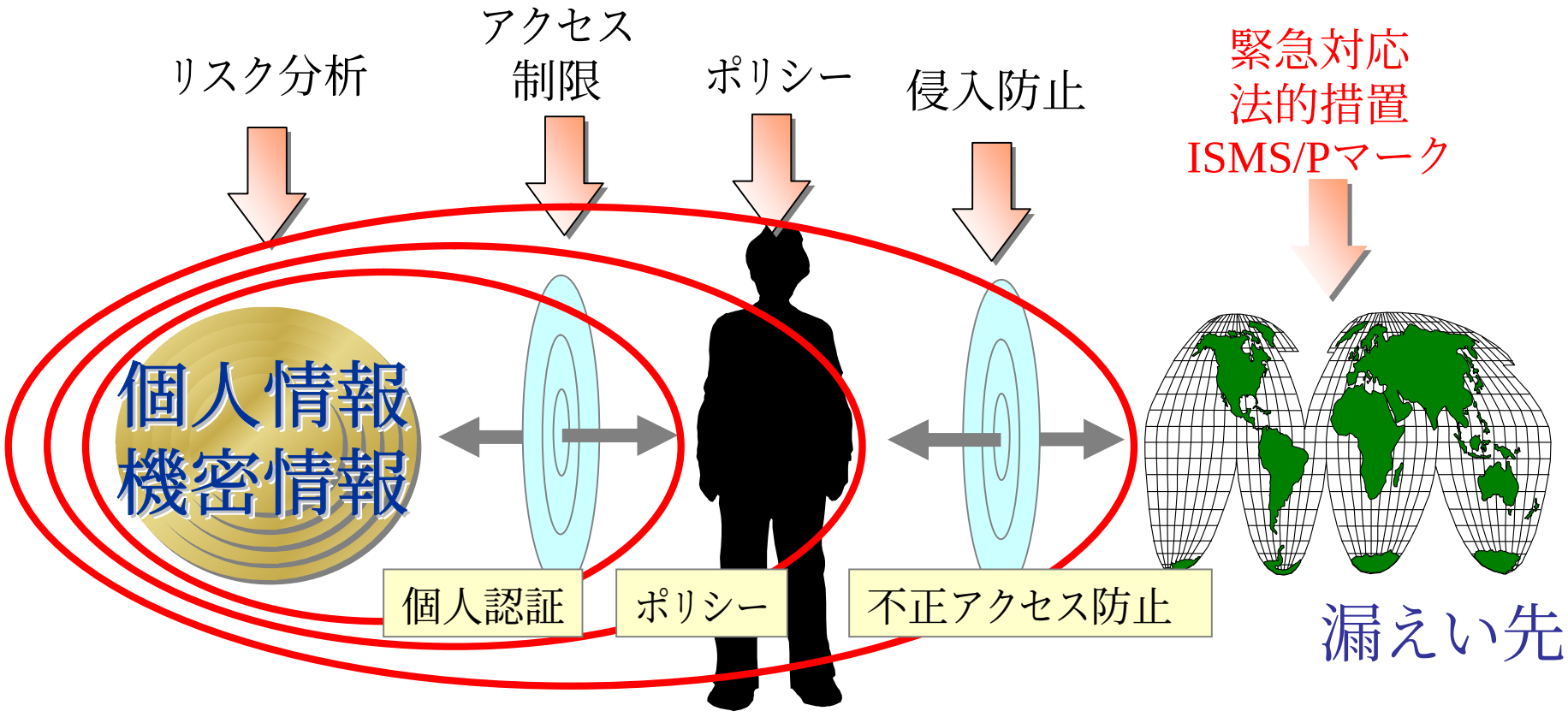


セキュリティ管理策とシステム分野(ISMSより)

セキュリティ管理策	内容
①基本方針②組織のセキュリティ③資産の分野と管理④人的セキュリティ	情報セキュリティ基盤・第三者によるセキュリティ・外部委託、資産に対する責任・情報の分類、職務定義および雇用・利用者の訓練・インシデント対応策
⑤物理的および環境的	物理的入退出管理、装置のセキュリティ、その他
⑥通信および運用管理(情報システムの管理)	運用手順および責任・システムの計画および受け入れ・悪意のあるソフトウェアからの保護・システムの維持管理・ネットワークの管理・媒体の取り扱い・情報およびソフトウェアの交換
⑦認証・アクセス制御	アクセス制御方針・アクセス制御の規則、利用者のアクセス管理・利用者登録、特権管理・利用者のクレデンシャルの管理・アクセス権の見直し、パスワードの使用、利用者領域にある無人運転の装置、ネットワークのアクセス制御、指定された接続経路、外部から接続する利用者の認証・ノードの認証、遠隔診断用ポートの保護、ネットワークの領域分割、ネットワークの接続制御、ネットワーク経路を指定した制御、ネットワークサービスのセキュリティ、OSのアクセス制御、端末のログオン、利用者の識別・認証、パスワード管理システム、システムユーティリティの使用、利用者を保護するための脅迫に対する警報、タイムアウト、接続時間の制限、業務用ソフトウェアのアクセス制限、情報へのアクセス制限、システムの隔離、事象の記録、使用状況の監視、コンピュータ内時刻同期、
⑧システムの開発・保守(情報システムに確実にセキュリティを組み込む施策・データの消失・誤用を防ぐ)	業務用システムのセキュリティ、暗号による管理策(暗号化、ディジタル署名、否認防止サービス、かぎ管理策、システムファイルのセキュリティ、開発・支援過程におけるセキュリティ(変更管理手順、OS変更の技術的レビュー、PPの変更に対する制限、隠れチャネルおよびトロイの木馬、外部委託によるソフトウェア開発
⑨事業継続管理	災害やセキュリティ侵害によって事業継続ができない場合の管理策
⑩適合性	法制度への適合性対策

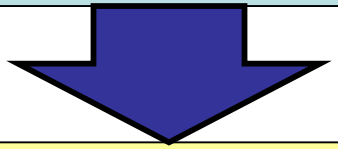
情報セキュリティ対策の多層防御

「認証」「セキュリティマネジメント」「不正アクセス対策」
を中心とした多層防御が鍵



認証

- 識別(Identification)
  - システムに対してユーザであるかどうか確認する
    例：システムを使う際にユーザIDだけを入力
- 認証 (authentication)
  - ユーザが正当なユーザであるかどうか(本人性)を確認すること
    例：システムを使う際にユーザIDとパスワードを入力
- 認可 (authorization)
  - 認証された利用者に対して、利用者毎のアクセス権に応じたサービスを提供すること（アクセス制御）
    例：認証の後に、ユーザの属性情報を取得し、利用可能な情報を制御する

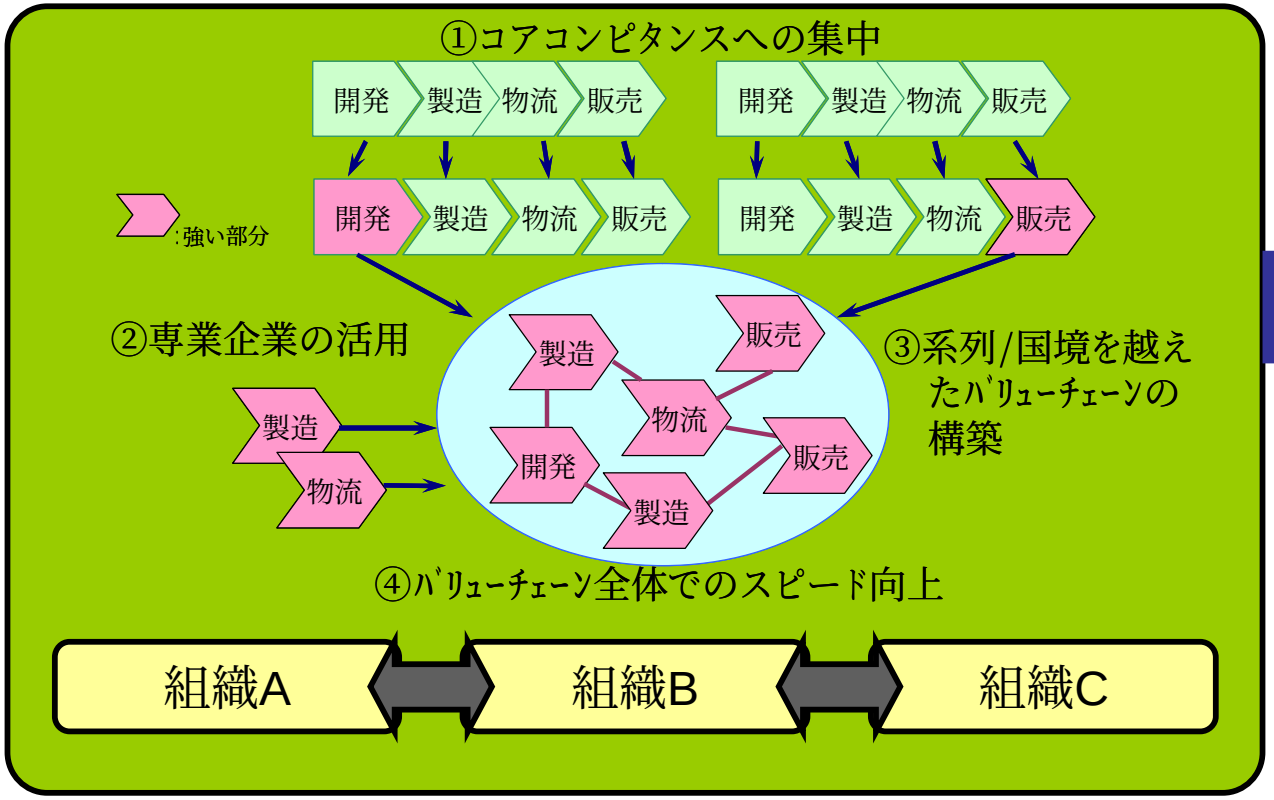


•「本当にあなたですか」（認証）が不十分な場合には、「だれ」（識別）も不確かになり「これにアクセスして良い」（認可）を与えられない

•権限のある利用者が**適切に資源を活用し生かす**しくみ

　　•責任の所在を明らかにするしくみ　→　**トレーサビリティ確保**

認証プラットフォームの実現



課題

- 複数組織の連携による価値向上
- トレーサビリティの実現
- プライバシー保護を主眼とした属性情報連携

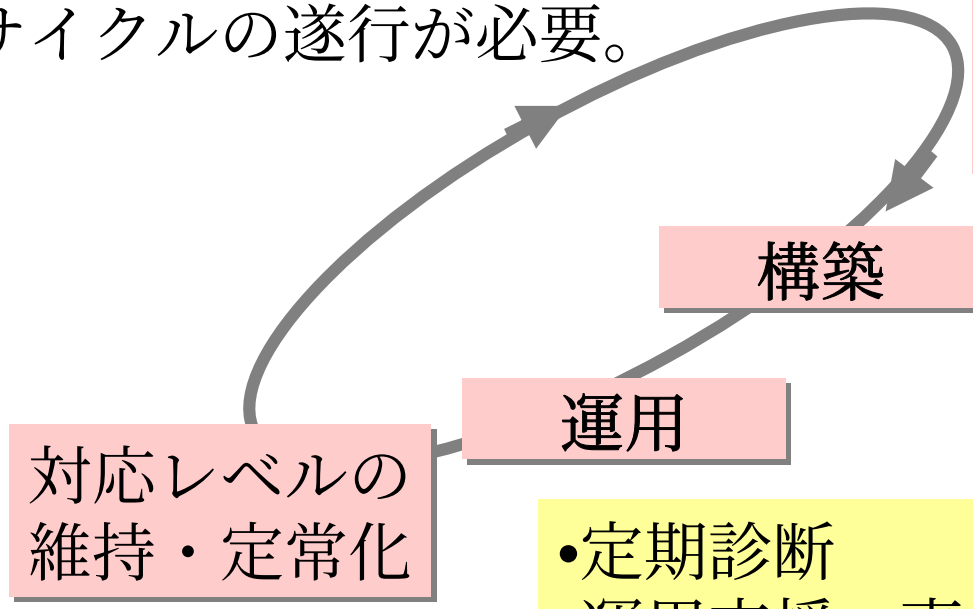
アクセス制御機構の相互運用性

WS-Security、LibertyAlliance、SAML技術検証

認証ポリシーガイドライン（基準）

セキュリティマネジメント

常に変化していく組織や
セキュリティ脅威への
セキュリティ対策は
継続したマネジメント
サイクルの遂行が必要。



- ポリシー策定
- リスクアセスメント
- セキュリティ診断
- 戦略策定
- ルール策定・体制構築

- 製品選定
- 導入・システム構築
- 運用設計

- 定期診断
- 運用支援・事故対応
- 教育・アウトソーシング

３．情報セキュリティ対策取り組み例

まとめ

- セキュリティインシデントは毎日発生
- セキュリティ対策のポイントは「複数対策」
  - ポリシーを遵守するための「セキュリティマネジメントサイクル」を維持
  - ワームやウィルスなどへの「不正アクセス対策」
  - 「認証」による資源活用
    - 個人、組織のトレーサビリティを確保するための手段

プロフィール

- 小松　文子（Komatsu　Ayako）
  - NEC入社以来、ネットワーク管理の国際技術標準化活動等を経て、セキュリティ製品およびサービスの研究・コンサルテーションおよび開発に従事
  - １９９８より、政府認証基盤、地方自治体認証基盤、公的個人認証サービスなどのシステム構築を推進
  - 日本PKIフォーラム相互技術部会長、次世代認証基盤プロジェクトリーダ
  - 主な著書　「改訂PKIハンドブック」２００４.１１　ソフトリサーチセンター
  - 現在、NECユビキタスソフトウェア事業部　シニアエキスパート、上席システムズアーキテクト
  - ２００６.４ よりNECインターネットシステム研究所　技術主幹