

# 情報セキュリティに対する脅威の実態 と包括的・体系的セキュリティ対策

- 恒久的データセキュリティの実現に向けて -

総務省 CIO補佐官

大塚 寿昭

2006年5月

# 情報セキュリティは新たな段階に

## 時代を画した2つの事件

- ・ 霞が関ホームページ改竄事件(2000年)
- ・ 一連の個人情報漏洩事件(2004年~)

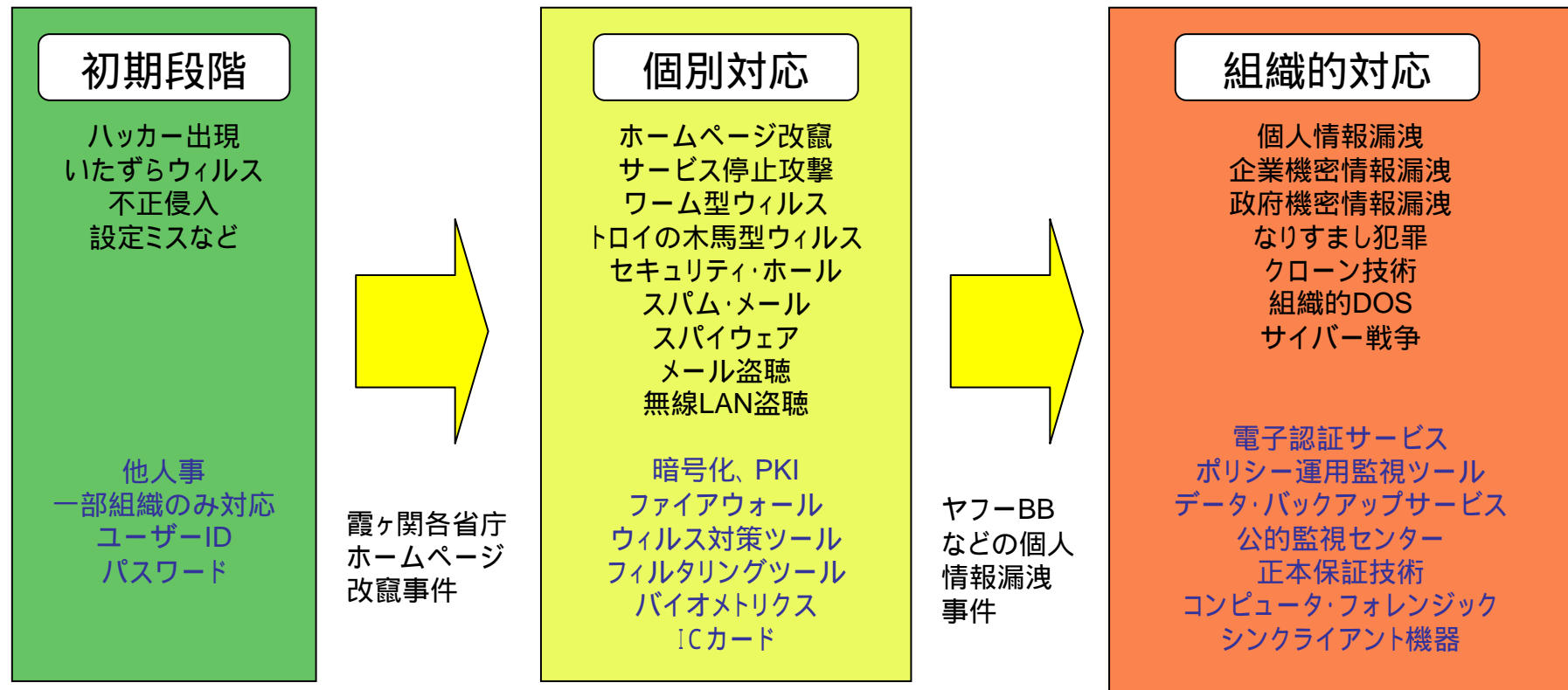
# 情報セキュリティ対策の進展

## - 情報セキュリティ対策は新段階へ -

これまでの概念を転換

PC・インターネットの機能増大や通信手段の多様化に伴って、セキュリティ・リスクも増大。

時代を画した2つの象徴的なセキュリティ事件



# 情報犯罪の現在

組織的犯罪者関与？ の事例

米国に於けるクレジットカード顧客情報流出 (各種報道記事による)

使用目的: 偽造クレジットカードの製作  
ネット取引の詐欺

ネット銀行のフィッシング詐欺 (各種報道記事による)

プロフェッショナル要素の高い犯罪手口

# 最近の情報犯罪の特徴

- ・ 組織犯罪者の関与と思われる特徴が顕著。
  - 偽造クレジットカード大量保有
  - 搾取した商品の換金ルートと接点がある
  - 現金入手のための他人口座保有
- ・ ITの技術や知識レベルの高い人物が犯罪組織に居る。
  - 巧妙なスパイウェアの開発
  - ネットを熟知した詐欺的手段を利用
- ・ 不特定多数を対象とせず、狙いを絞って攻撃する。
  - 効果的に現金を得るために標的を絞る
  - その標的の特性に合わせた犯罪手段の開発

## 最近のウィニー事件報道 (Yahoo News より)

- ・ <岡山県警情報流出> ウィニー使用禁止 違反なら懲戒免職も
- ・ <和歌山> Winnyで県立高校生徒の個人情報流出
- ・ 私物パソコン使用禁止...各省庁、情報流出対策急ぐ
- ・ ウィニー対策で全職員に誓約書提出求める...愛媛県警
- ・ 政府機関の情報管理基準、今月中に策定...各省庁に指示
- ・ 捜査情報流出:「ウィニー」使うな 徳島北署が講習会 / 徳島
- ・ 県警:全職員に公用PC配備 ウィニー対策、情報流出を遮断 / 島根
- ・ <アルプス技研> 社員の個人情報1007件、ウィニーで流出
- ・ 名古屋・情報流出:続発受け、松原市長が改善指示 / 愛知
- ・ <手術情報流出> 患者2800人の氏名など 富山の病院
- ・ 郵便局でウィニー流出 = 顧客情報など194人分 - 福岡
- ・ 約8000人分の個人情報流出 = ウィニーで - 住友生命
- ・ <ウィニー> 顧客情報と73社の企業情報流出 NTT東西
- ・ 陸自11師団内部文書流出 米軍との訓練報告ネットに
- ・ 1万3600件の情報流出 富士宮信金、口座番号など
- ・ 「秘」扱いデータ流出 海自、パソコンから

## 最近のセキュリティ事件の傾向

- ・ウィルスではトロイの木馬型で第三者からの侵入を許すタイプ(ボットなど)が増加
- ・狙う相手を特定した「スパイ型」ウィルスやフィッシングも増加、個人に限らず企業や政府機関も狙う
- ・30分に1つのファイルを消去するなどのメッセージを出すような、脅迫型のウィルスも出現

いずれもシステムだけでは対処が困難

## 最近のセキュリティ対策の傾向

- ・ファイル・プロテクション、ディザスター・リカバリーなど、データを保護したり破壊や消去などの被害に遭った場合、速やかに回復する仕組みを用意しておくことの重要性が認識されてきている。
- ・また、関係者のセキュリティに対する教育や通報体制も重要性が増している。

## 情報セキュリティ対策のキーポイント

事象対処でなく、総合的に予防策を

ICTを広く深く知る

情報をデジタルで扱うことの特徴を理解

敵をよく知る(最も弱いところを突いてくる)  
情報犯罪などの事例情報に常に注目しておく

自身のアプリケーション  
(業務・事業)の特性

かけるコストとの  
バランス

# 90年代からのIT環境の変化

クライアント・サーバー型システムの進展・普及

インターネットの普及・社会基盤化

パソコンの高性能化、機能多様化

通信技術の多様化、高速大容量化

携帯電話・PDA・デジカメなど情報端末の多様化

外部記憶機器の多様化、大容量化、小型化

# この10年余り・・・

ITはプロとノンインテリジェント端末の時代から、パソコンもインターネットもデジタル情報処理の危険な部分を知らない素人の間に広がった。

マルチメディア・ブームから発達したパソコンは多機能化・高性能化した。

インターネットも同様に多種多様の機能とサービスが発達し、ブロードバンドも急速に普及した。

これらの機能やサービスの発達と普及の間に、セキュリティに対する関心は一部を除いて低かった。

## 情報がデジタル化されることによるリスク

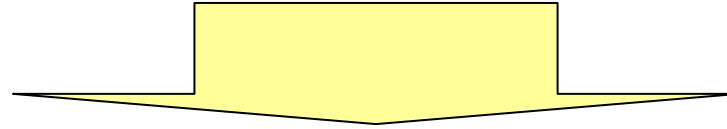
- ・複製が容易
- ・改竄が容易で痕跡が残らない
- ・ネットワークから侵入して、盗聴、改竄、破壊される
- ・目に見えないことによる様々な不注意が起きる
- ・重要情報がデジタル媒体のみに存在することがある

繊細で脆弱なデジタル情報は、プロフェッショナルの日夜弛まぬ努力と献身によって支えられてきた。今日にあっても、この繊細さと脆弱さという特性は変わっていない。

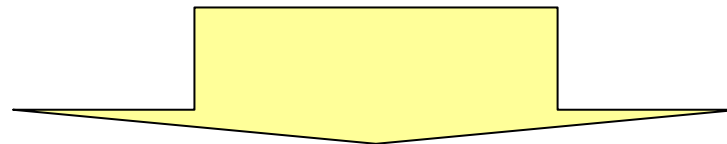
ユビキタスなどで謳われるように、いつでも・どこでも・誰でも使えるようにするならば、ベンダーはよほどの注意をもって製品やサービスの信頼性を確保しなければならない。

特にソフトウェアにバグ(セキュリティ・ホールはその一部)は必ずつきものである。これにどう対処して行くかについてのベンダーの責任は大きい。

# セキュリティ対策に偏りがある？ ( 関心領域に偏りがあった？ )



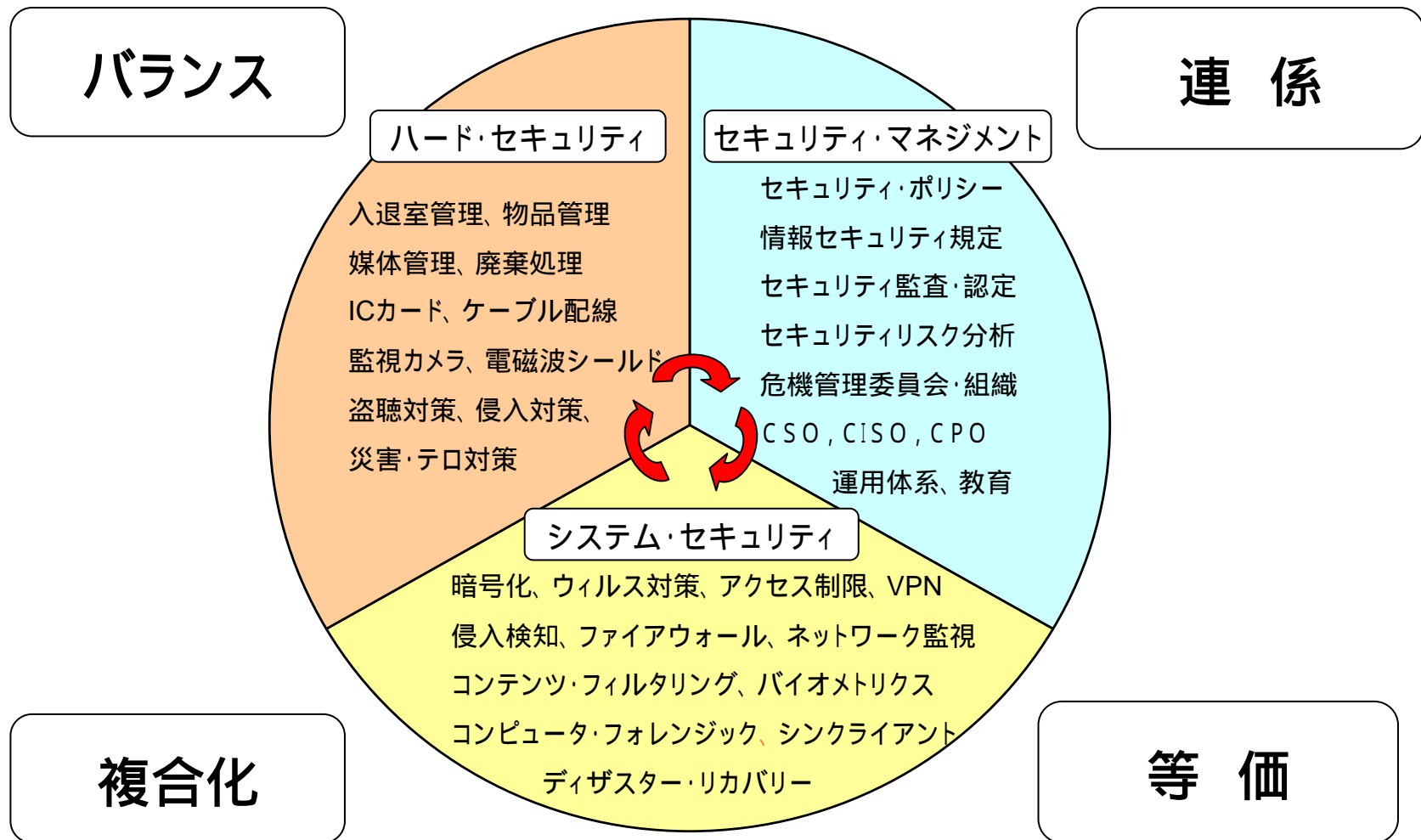
情報セキュリティの3原則  
Confidentiality  
Availability  
Integrity



体系的アプローチが必要

情報セキュリティ・アーキテクチャ

# 情報セキュリティ・アーキテクチャ全体像



# セキュリティ・マネジメント

ポリシーや規則の制定、管理・運用組織の体制などのマネジメント分野

セキュリティ・ポリシーの制定  
情報セキュリティ規定・運用マニュアルなどの制定  
セキュリティリスク分析  
セキュリティ監査の実施(内部監査、外部監査)  
ISMSなどの公的認証を受ける  
危機管理委員会・セキュリティ管理室などの専任組織を設置する  
CSO, CISO, CPOなどのポジションを設置し、責任体制を明確にする  
セキュリティ対策のPDCAを組織的に回す  
取引先のセキュリティ監査  
セキュリティ予算の定常化  
セキュリティ技術の継続的調査・研究  
教育、啓蒙活動の実施(セキュリティ文化、マインドの養成)  
など

# システム・セキュリティ

コンピュータ・システムやネットワークのデジタル技術による  
セキュリティ対策

ウィルス対策、スパム対策、スパイウェア対策  
通信・データ暗号化、セキュアメール  
アクセス制限、データベース・セキュリティ  
侵入検知、ファイアウォール、VPN  
ネットワーク監視、サーバー(DB)バックアップ体制  
ポリシー・マネジメント・システム  
コンテンツ・フィルタリング  
バイオメトリクス、認証サービス  
コンピュータ・フォレンジック  
シンクライアント など

# ハード・セキュリティ

人の出入りや物品管理などの物的管理や建物・施設の  
セキュリティ対策

セキュリティゲートなどによる入退室管理  
物品管理(持ち込み禁止、持ち出し禁止)  
媒体管理(私有媒体の使用禁止、媒体廃棄対策)  
機器などの廃棄処理(残留磁気対策など)  
文書廃棄(シュレッダー、熔解)  
ICカードの社員証  
監視カメラの設置  
金属探知器  
電磁波シールド施設  
物理的盗聴対策  
物理的侵入対策(赤外線、パッシブセンサー)  
災害対策、テロ対策 など

# 情報セキュリティ・アーキテクチャの要点

バランス

連 係

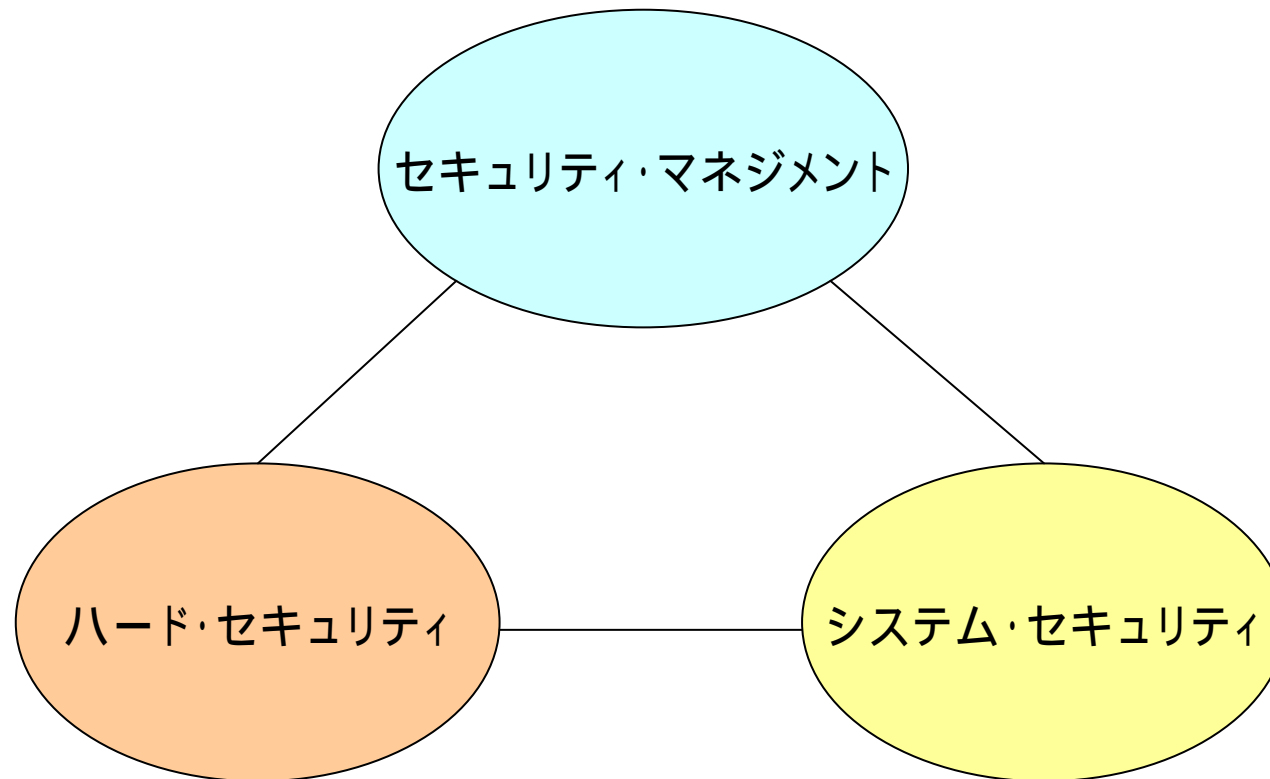
複合化

等 価

# バランス

情報セキュリティに関する3分野のバランスが重要

- 敵は弱いところを突いてくる -



## 連 係

### ログインと入退室管理の連係

ICカード社員証をログイン中はクライアント機に常時接続(挿入)しておく。会議室やトイレはセキュリティゲートの外側に設置して、離席時のセキュリティを自動的に防御。

さらに、高度なセキュリティ・エリア(サーバー室内)などでのクライアント機操作は、入室確認ができている人のみに許可されるようにするなど。

### ポリシーや規則とシステムの連係

ポリシーや規則で決められた手順や運用のルールが実行されてるかについて、系統的に管理する。例えば、パスワード変更期日管理、アクセスルール休眠アカウントと人事情報など。

### モバイル通信時の暗号鍵

ICカード社員証に暗号鍵を記録しておく。モバイル通信時の本人確認を、このICカードの存在によって行うと同時に暗号鍵、ID、パスワードの確認ができる。

## 複合化

セキュリティ技術は1対1の対抗策だけでは、イタチごっこになり、攻撃側が先手を取ってくるもの。

例えば廃棄するHDDの残留磁気対策については、重要情報が暗号化されていればそれほど神経質にならなくて良い。

また重要度のクラスによって、**複数のセキュリティ技術を組み合わせる**。例えば本人確認の方法を複合化して、ユーザーID,パスワードにプラスして、バイOMETRICSを採用する。あるいは入室状況と連動する。ワンタイム・パスワードと併用する。など

Integrity、Availability の観点から、データベースのバックアップ体制(正本性確保)を2重化、複数地点などに**分散化**する。同様に外部委託する。

## 等 価

### 「情報」はその形状を問わず、等価である

書類上であれ、デジタル化されたものであれ、情報の内容は等しい価値である。デジタル情報を厳重に守るならば、文書情報もその機密性のクラスごとに同等な扱いをしなければならない。

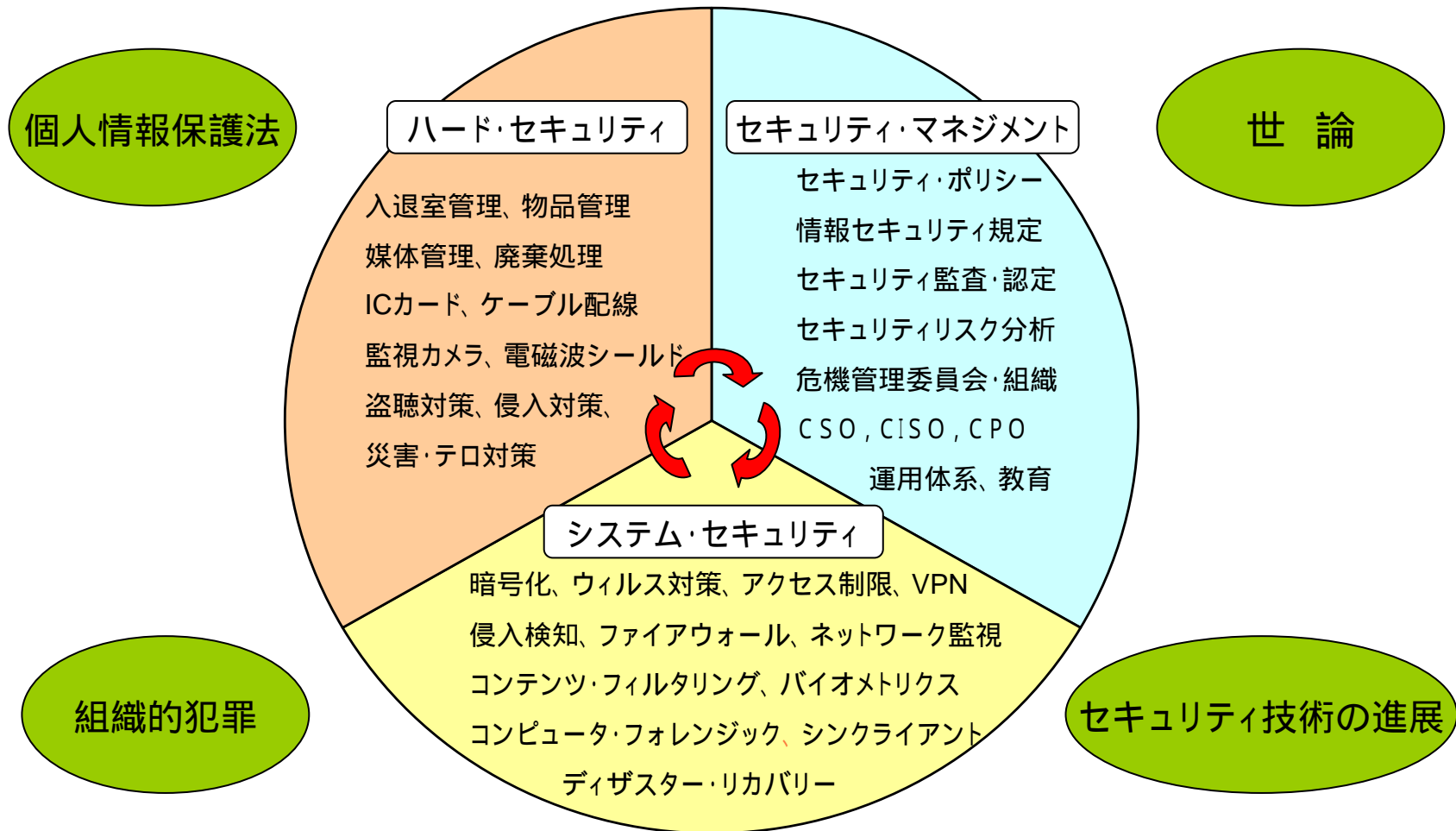
**正本性の確保(保証)**という観点においても同様に考えるべきである。デジタル情報の正本性(改竄対策)、システムから印字する文書の正本性(あるいはコピー対策)を確保する仕組みが必要。

ネットワーク・プリンター出力時の紛失、盗難対策にICカード社員証を利用する。システム・プリンター印刷時に透かし印刷するなど。

### キャビネット保管、バインダー持ち出し

にもシステム対応は可能である。例えば、開扉にICカード社員証を使用する(そのログはシステム記録)。バインダーにICタグを付け、開扉者と連動記録し、返却管理するなど。(キャビネット内にもセンサー設置)バーコードも有効。

# 情報セキュリティ・アーキテクチャ全体像



**安全な情報化社会の実現のために  
皆様のご活躍を期待します。**