日弁連コンピュータ委員会シンポジウム

ネットワーク時代における個人情報保護の最前線

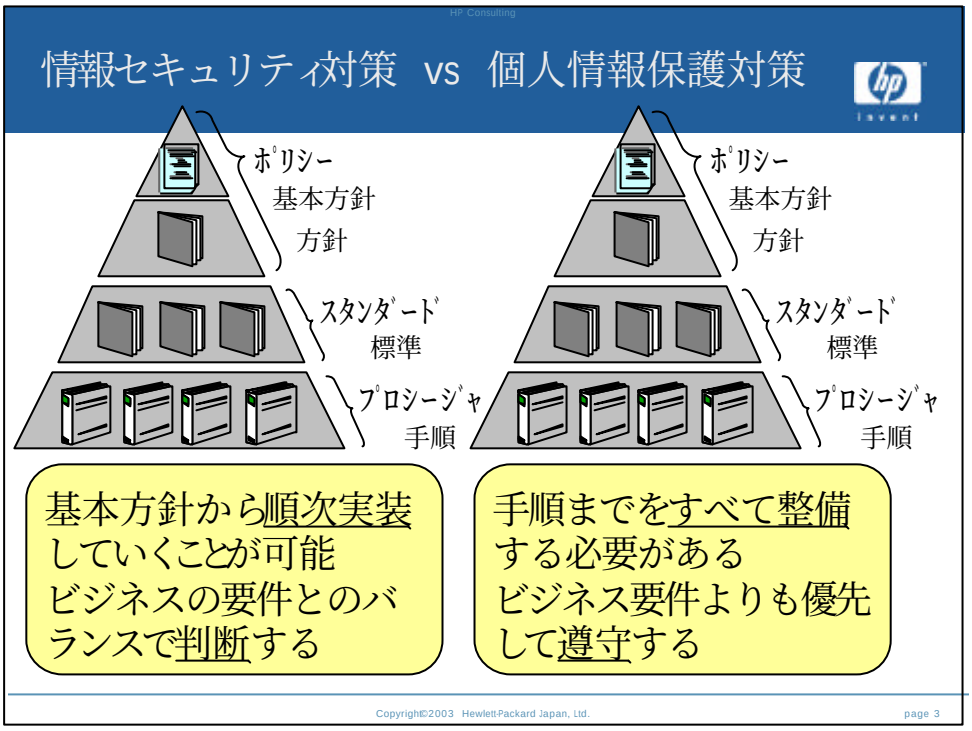
2003年12月3日

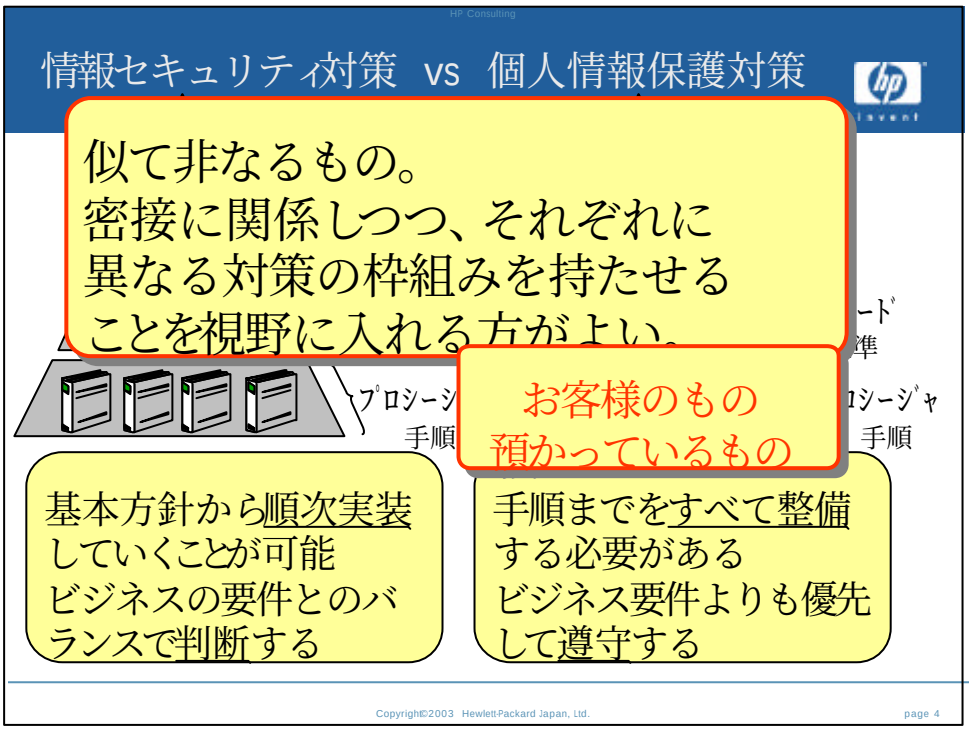
企業における個人情報保護の保護体制

日本ヒューレット・パッカード株式会社
佐藤　慶浩

HP Consulting

個人情報保護対策と情報セキュリティ対策





情報セキュリティ対策 vs 個人情報保護対策

個人情報保護

個人情報保護は、預り情報保護として取り組む

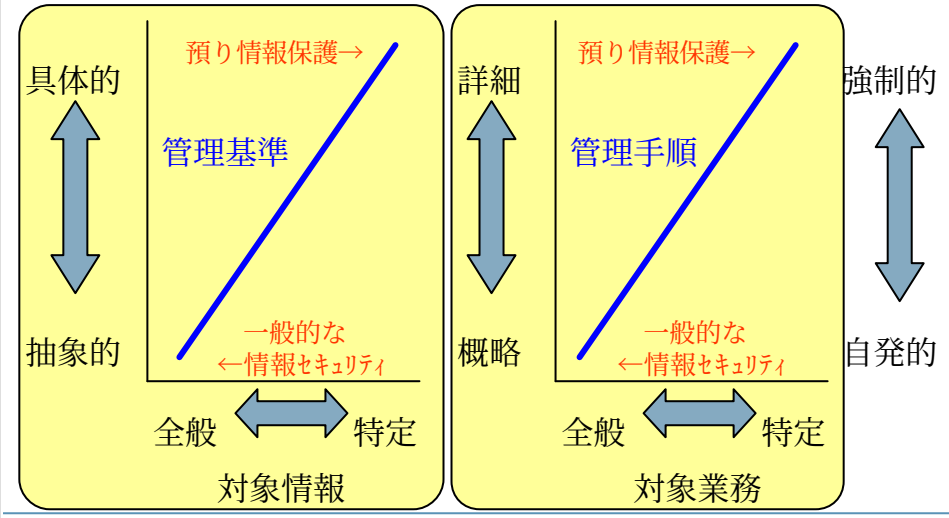
C:機密性（漏えいのない状態＝無許可の参照ができないような状態）
I:完全性（改ざんのない状態＝無許可の変更ができないような状態）
A:可用性（停止のない状態＝許可されたことができるような状態）

C:機密性（参照を許可した場合のみ参照できるようにすること）
I:完全性（変更を許可した場合のみ変更できるようにすること）

情報セキュリティ

情報セキュリティ統制特性

抽象的なことは制御できない



個人情報のライフサイクル

個人情報の取得
　利用目的・情報移転の了解を事前に得る
　必要最低限の取得→使用予定のないものは取得しない
個人情報の保管
　情報漏えい・書き換えの防御
　情報格付け、ｼｽﾃﾑ格付け：所在の管理、視認性の確保
個人情報の加工
　情報格付けの継承、ｼｽﾃﾑ要件の継承
個人情報の利用
　利用者の制限（無許可者からのアクセス防御）
　最小情報、最小数量の利用制限（許可者の最小権限）
　取扱い手順の明確化（許可者の注意義務）
個人情報の廃棄
　廃棄手順の明確化（電子化前後の廃棄手順を含む）

まとめ

<u>成功のための枠組み：</u>

個人情報保護対象の明確化
原則の明文化と経営者の約束
　↓　それによって　↓
情報セキュリティを基盤とするが、個人情報保護は、ビジネスよりも優先するということを周知・徹底する
　↓　そのためには　↓
実施可能な具体的な手順までを検討し、実践する必要がある

お問い合わせ先
http://www.hp.com/jp/security

本日の資料
http://yosihiro.com/business/

yosihiro.com

予備資料

ちょっと復習 :なぜ、C/ I Aにこだわるのか

機密性 Confidentiality
正確性 Integrity
可用性 Availability

主体 Subject

アクセス Access

客体 Object

Subjects Access to Objects: **SAtO**モデル

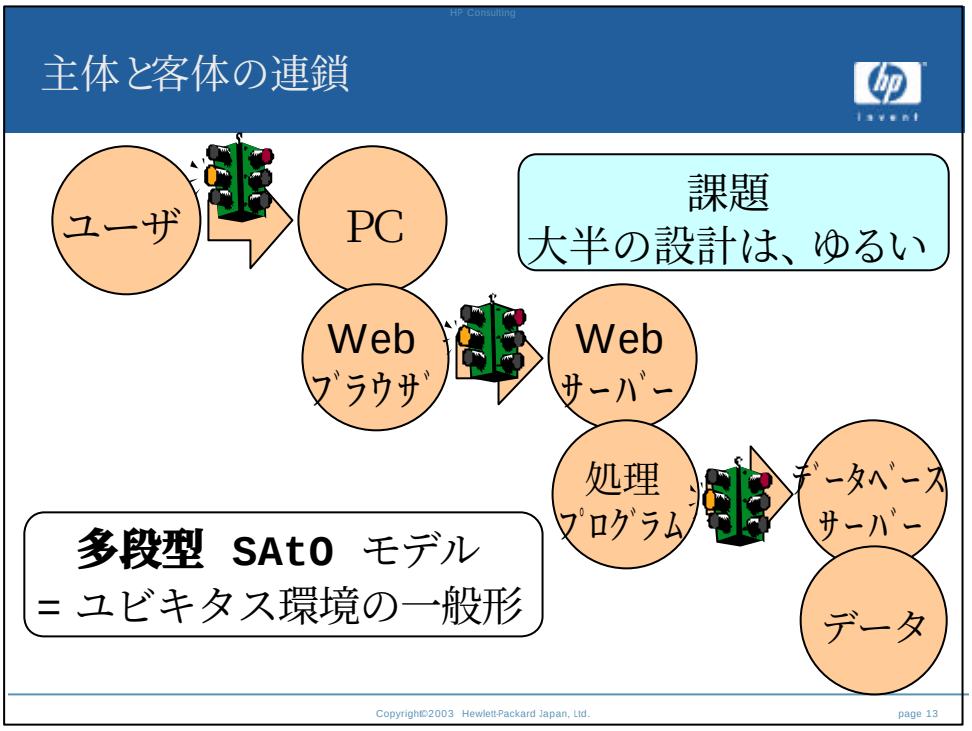
C/I/A に整理できると・・・

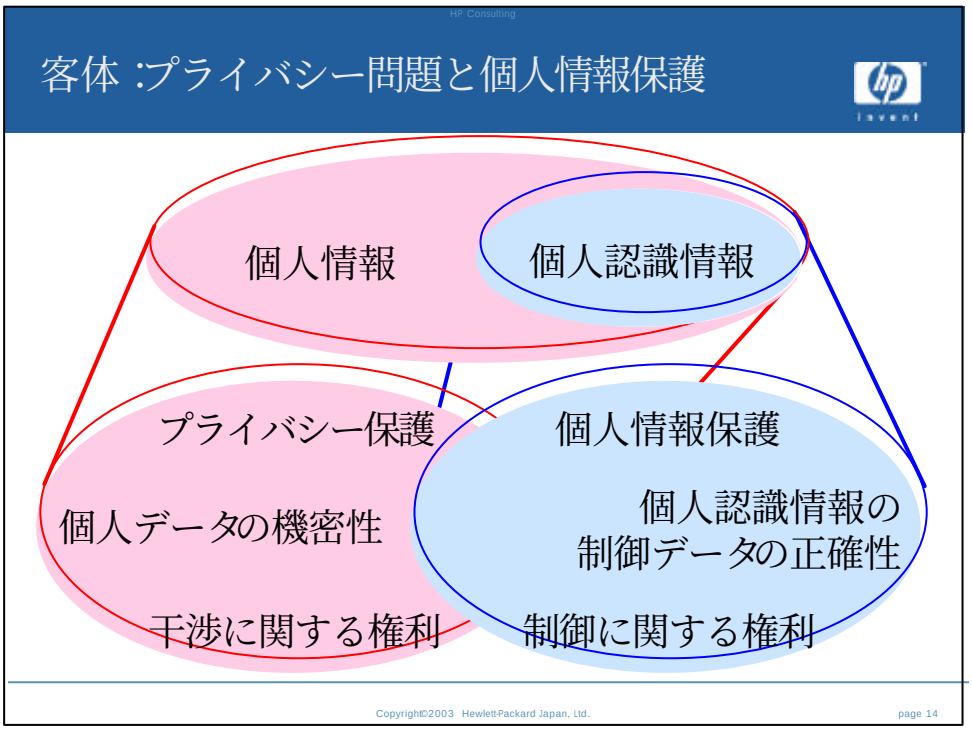
脅威の例

機密性	故意	事故
情報	漏洩 盗聴 詐取	誤配信

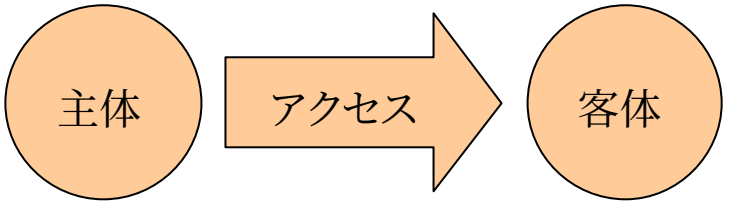
完全性	故意	事故
情報	改ざん 消去	(滅失) 消失
ファイル	破壊	消失

可用性	故意	事故
情報 システム	消去 DoS DDoS	消失 障害



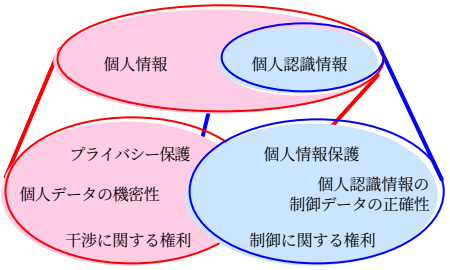


情報」にまつわる 「人」としての主体



所有者 Owner
利用者 User

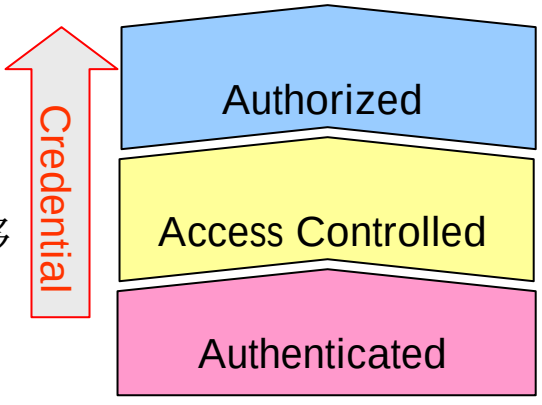
保管者 Custodian
保護者 Guardian



ちょっと予習 :アクセス制御の役割

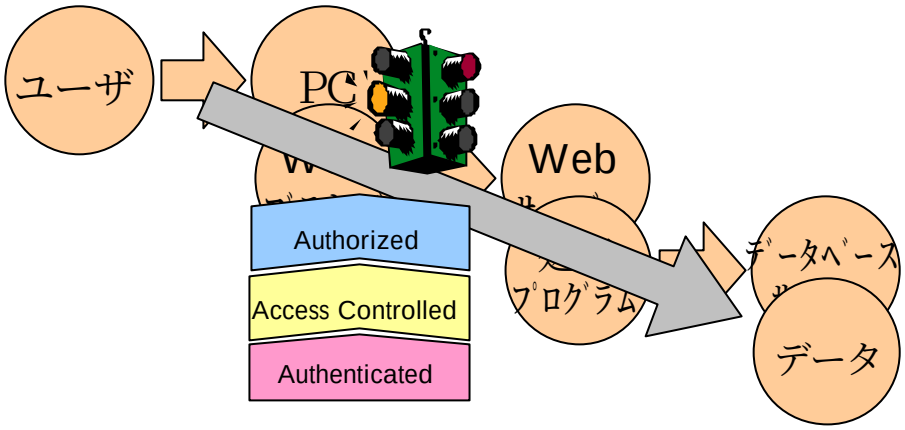
Authenticate して Access Control により
Authorize する

主体の状態の遷移



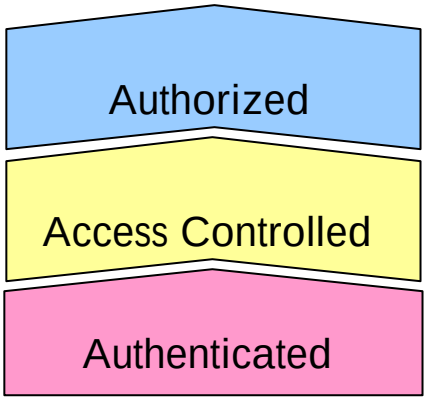
ユビキタス環境でのプライバシー問題

単一型 **SAtO** を想定したアーキテクチャの問題



ユビキタス環境でのプライバシー問題

状態遷移の精度の問題



Authenticate =
Identify + Proof

Anonymity =
Un-identified
&
Un-authenticated

ユビキタス環境でのプライバシー問題

ユビキタス環境では、多段型 **SAtO** を前提にする