


 <small>HP Consulting</small>	<p>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</p> <p>企業における 個人情報保護の 保護体制</p> <p>日本ヒューレット・パッカー株式会社 佐藤 慶浩</p>
---	---

<p>個人情報保護対策 と 情報セキュリティ対策</p>	
---	--

情報セキュリティ対策 vs 個人情報保護対策

情報セキュリティ対策

- ポリシー 基本方針 方針
- スタンダード 標準
- プロシージャ 手順

個人情報保護対策

- ポリシー 基本方針 方針
- スタンダード 標準
- プロシージャ 手順

基本方針から順次実装していくことが可能
ビジネスの要件とのバランスで判断する

手順までをすべて整備する必要がある
ビジネス要件よりも優先して遵守する

Copyright©2003 Hewlett-Packard Japan, Ltd. page 3

情報セキュリティ対策 vs 個人情報保護対策

似て非なるもの。
密接に関係しつつ、それぞれに異なる対策の枠組みを持たせることを視野に入れる方がよい

お客様のもの
預かっているもの

基本方針から順次実装していくことが可能
ビジネスの要件とのバランスで判断する

手順までをすべて整備する必要がある
ビジネス要件よりも優先して遵守する

Copyright©2003 Hewlett-Packard Japan, Ltd. page 4

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

Copyright©2003 Hewlett-Packard Japan, Ltd. page 5

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

具体的 ↑↓ 抽象的	預り情報保護 管理基準	詳細 ↑↓ 概略	預り情報保護 管理手順	強制的 ↑↓ 自発的
	一般的 情報セキュリティ		一般的 情報セキュリティ	
全般 ↔ 特定 対象情報		全般 ↔ 特定 対象業務		

Copyright©2003 Hewlett-Packard Japan, Ltd. page 6

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)

Copyright©2003 Hewlett-Packard Japan, Ltd.

page 7

まとめ



成功のための枠組み:

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

Copyright©2003 Hewlett-Packard Japan, Ltd.

page 8

お問い合わせ先

<http://www.hp.com/jp/security>



本日の資料

<http://yoshihiro.com/business/>

yoshihiro.com

HP Consulting



予備資料

Copyright©2003 Hewlett-Packard Japan, Ltd.

page 10

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**

Copyright©2003 Hewlett-Packard Japan, Ltd. page 11

C/I/A に整理できると・・・

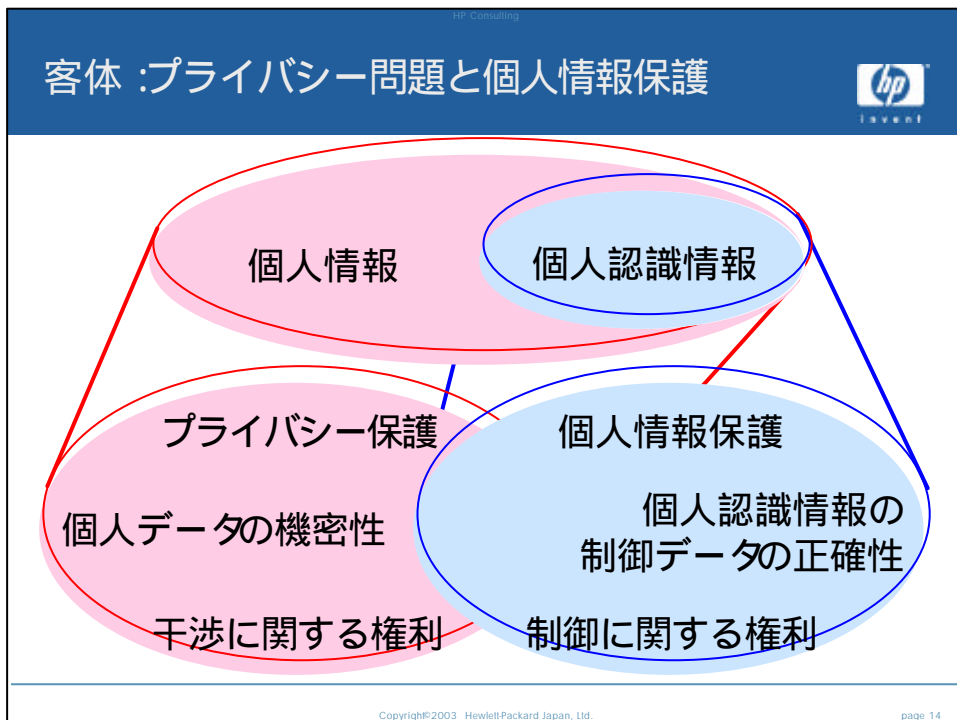
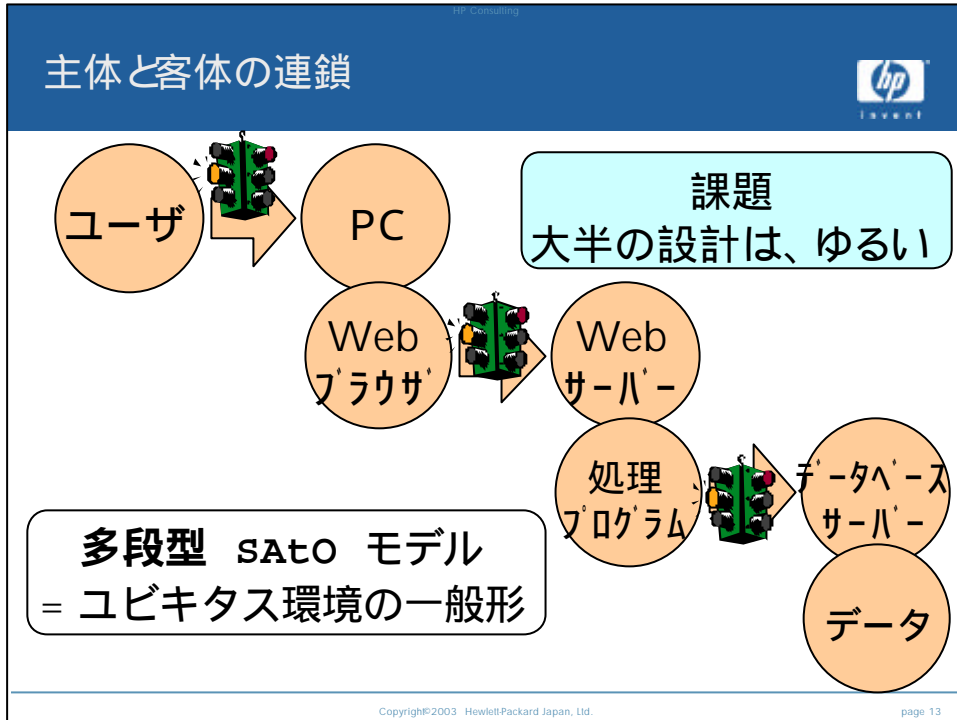
脅威の例

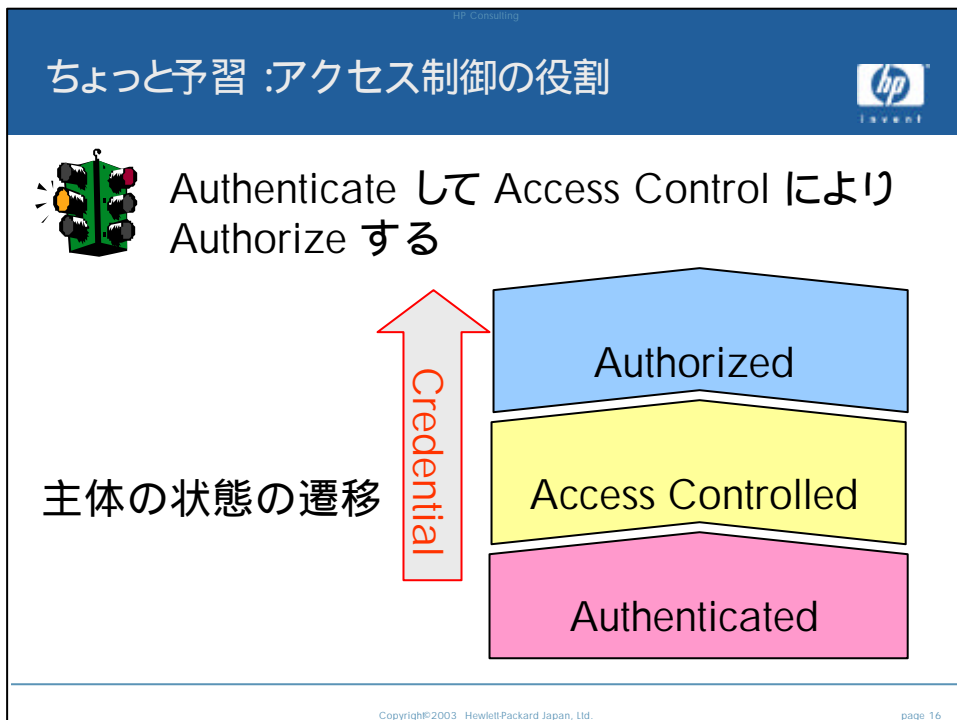
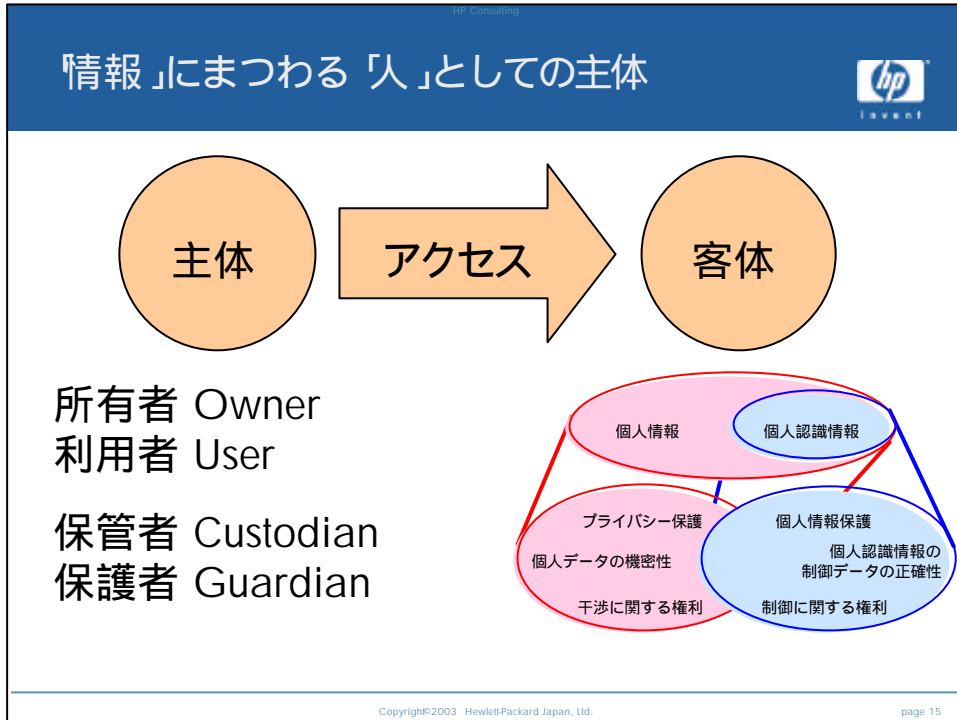
機密性 情報	故意	事故
	漏洩 盗聴 詐取	誤配信

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

可用性 情報 システム	故意	事故
	消去	消失
	DoS DDoS	障害

Copyright©2003 Hewlett-Packard Japan, Ltd. page 12





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

ユーザー → PC → Web → データベース
データ

Authorized
Access Controlled
Authenticated

Copyright © 2003 Hewlett-Packard Japan, Ltd. page 17

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

Authorized
Access Controlled
Authenticated

Authenticate =
Identify + Proof

Anonymity =
Un-identified
&
Un-authenticated

Copyright © 2003 Hewlett-Packard Japan, Ltd. page 18

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、多段階 SAto を前提にする

それぞれの段階での
need to know

