

security 101
技術編

セキュアWebサーバ構築の実践技法

HP-UX CMW (Compartmented Mode Workstation)
HP Praesidium VirtualVault

佐藤 慶浩

日本ヒューレット・パッカート株式会社

(2001年4月16日)
6月14日一部改訂



Slide 1

セキュアWeb
サーバ構築
実践技法

講師略歴

佐藤 慶浩 (さとう よしひろ)
日本ヒューレット・パッカート株式会社
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・パッカート(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社の製品提供と対応して順次担当。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・パッカート対応窓口を担当。また、FISC(金融情報システムセンター)、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ーにて情報セキュリティガ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



Slide 2

セキュアWeb
サーバ構築
実践技法

講演要旨

米国の TCSEC(通称、オレンジブック)で定められたセキュリティの要件について紹介します。TCSEC は、CC(CommonCriteria) になり、その後、ISO15408 へと発展していきます。国内でも ISO15408 の紹介が何度か行われていますが、ほとんどの場合、その枠組みや保証要件などの説明が多く、肝心の機能要件の技術説明がされていません。

今回のセミナーでは、TCSEC が ISO15408 へと発展していった背景などについても交えながら、この要件によってどのようなコンピュータが出来上がるのかを具体的な技術説明を中心に紹介します。

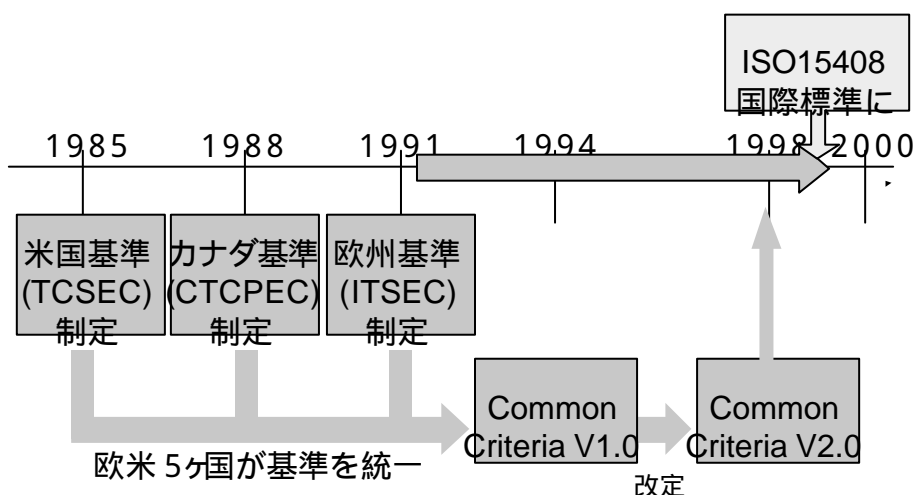
ご紹介する内容は B レベル・システムのセキュリティ機能ですが、これを使用する予定がない方々にとっても、B レベルを知っていただくことによって、逆にそれよりも低いレベルの OS である、Unix や Windows NT に、どのような潜在的な危険性があるのかを再確認していただくのに役立つ情報になります。

本セミナーでは、解説に加えて、日本ではあまり見る機会のない、実際に米国海軍で使用している実機の動作の様子をご覧いただくとともに、それらの技術を Web サーバでのデータ保護に応用した場合の説明も加えさせていただきます。

hp Slide 3

セキュアWeb
サーバ構築
実践技法

国際標準としての制定までの流れ



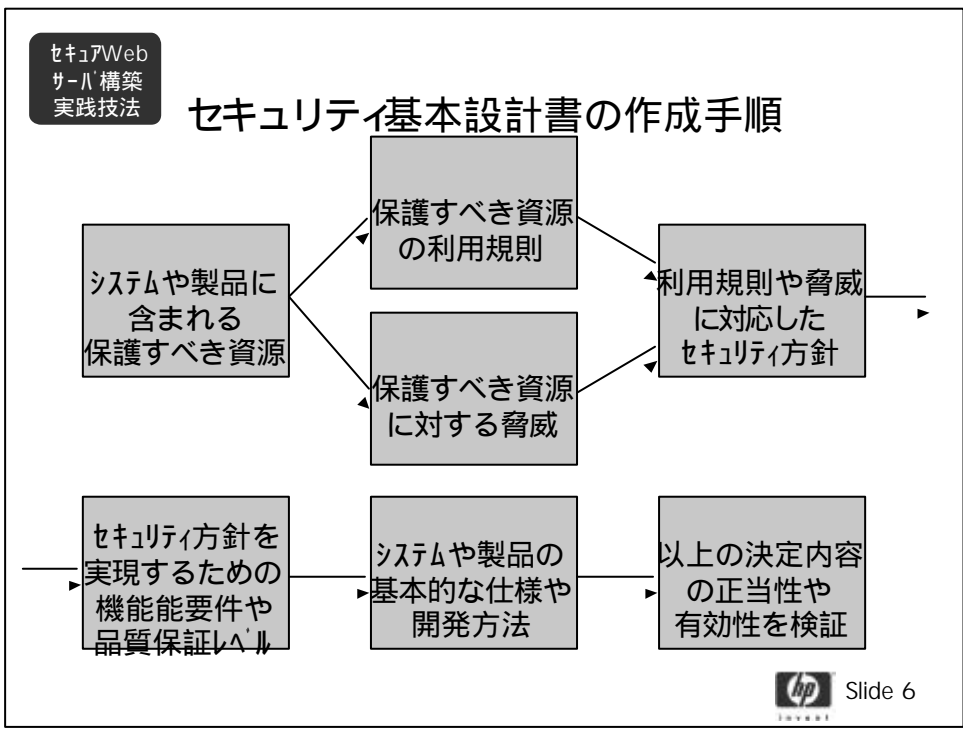
hp Slide 4

セキュアWeb
サーバ構築
実践技法

評価基準で規定している機能要件

- ユーザ・データの保護
- 利用者の識別と認証
- セキュリティ・プログラムの保護
- データやプログラムの利用
- 製品やシステムの利用
- 通信路
- セキュリティ通信
- 利用者のプライバシー
- 暗号鍵の管理
- セキュリティ監査
- セキュリティ管理

hp Slide 5



セキュアWeb
サーバ構築
実践技法

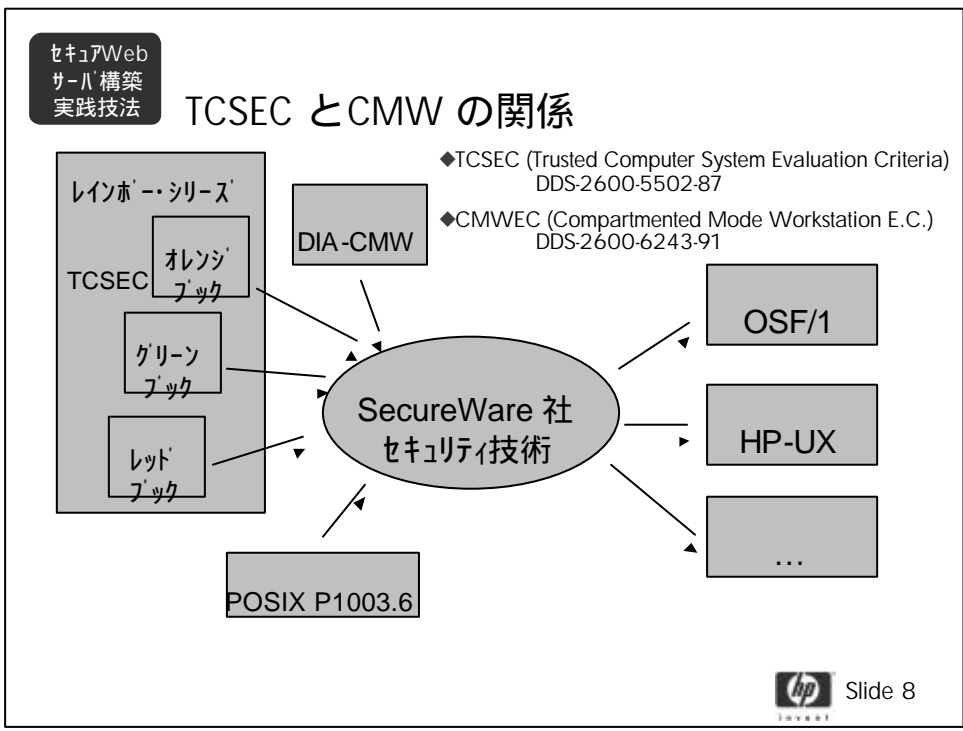
CCV2 に関する参考資料

論文：「セキュリティシステム構築のための計画手順の提案」
 織茂昌之氏(日立製作所) 他
 情報処理学会 コンピュータセキュリティ シンポジウム'98 pp75-80

雑誌記事：「セキュリティ評価基準」の詳細と対策
 田淵治樹氏(富士通)
 日経コンピュータ 1998.12.21(前編) & 1999.1.4(後編)

書籍：「国際セキュリティ標準 ISO15408 のすべて」
 田淵治樹氏(富士通)
 日経BP社 ISBN4-8222-2254-3

Slide 7



セキュアWeb
サーバ構築
実践技法

セキュリティ = C + I + A

高信頼性システム (Trusted System) とは、高いコンピュータ・セキュリティを保持することを目的に作られたコンピュータ・システムのことです。

コンピュータ・セキュリティとは、次の3つの属性を持ちます。

- 機密性 (Confidentiality)
- 保全性 (Integrity)
- 可用性 (Availability)



セキュアWeb
サーバ構築
実践技法

オレンジブック (TCSEC)

オレンジブックは、信頼性システムの評価基準を定めた文書で、"Department of Defense Trusted Computer System Evaluation Criteria"という。

内容は、各レベル (低い方から D, C1, C2, B1, B2, B3, A1) に対応する機能要件をセキュリティ方針、追跡性、保証、および文書の4つのカテゴリの中での達成基準として記述してある。

- C1 = 任意保護: 一般の UNIX システムが相当
- C2 = アクセス制御による保護
- B1 = ラベル式保護: Trusted HP-UX CMW
- B2 = 構造化保護

B Level Security = BLS



セキュアWeb
サーバ構築
実践技法

TCSEC の Division/Class の要件 (抜粋)

D: No Access Control
 C1 : Identification and Authentication
 C1 : Discretionary Access Control
 C2 : Strict Password
 C2 : Auditing
 B1 : Labeling
 B1 : Mandatory Access Control
 B1 : Trusted Path
 B2 : Least Privilege
 B2 : Subject Sensitivity Labels (Labeling to all models)
 B2 : Device Labeling (Labeling to all models)
 B3 : Trusted Facility Management (Security Administrator, 2KeyLock)
 B3 : Trusted Recovery
 B3 : Access Control List
 CMW: Compartment Mode
 CMW: Information Labels
 A1 : Trusted Distribution



Slide 11

セキュアWeb
サーバ構築
実践技法

TCSEC のセキュリティ要件

各セキュリティ機能には、次のような意味がある。

Identification and Authentication

パスワードによるユーザの識別とクリアランスによるユーザの権限の認証

Discretionary Access Control

各ユーザがユーザ ID などに基づいて所有のファイルなどに対するアクセスを制御

Least Privilege

ある操作を実行するときその操作を完了するのに必要な特権だけを与え、不要な特権は(使えるセキュリティ・レベルでも) 与えない

Auditing

ユーザの行動 (イベント) の監視

Labeling

セキュリティ・レベルに見合ったラベルを付ける

Mandatory Access Control

システムがユーザのクリアランスとファイルのセキュリティ・レベルに基づいてアクセスを制御

Subject Sensitivity Label

ファイル/デバイスだけではなく、ユーザやプログラムにもセキュリティ・ラベルを付ける



Slide 12

セキュアWeb
サーバ構築
実践技法

TCSEC のセキュリティ要件

Device Labeling

その装置にアクセスできる最高/最低のセキュリティ・レベルにみあったラベルを装置に付ける

Trusted Path

セキュリティに深く関わる操作を信頼度が高いプログラム/コマンドのみで行える方法が確立している

Trusted Facility Management

管理者の機能を分割して、役割を細分化し、権限の一極集中を防ぐ

Trusted Recovery

システムで障害が発生した場合、一旦一般ユーザを排除し、信頼性の回復を図ってから業務を再開する

Information Label

プログラムやファイルがどのレベルの情報を持っているか示すためのラベル

MaxSix

ネットワークを介して、ラベル付けされたデータをやりとりするための仕組み



Slide 13

セキュアWeb
サーバ構築
実践技法

グリーンブック (Password Management Criteria)

グリーンブックには、オレンジブックで示されたパスワード保護について具体的なガイドラインが記述されている。それらを大まかにいえば次の3項目になる。

- ユーザは自分のパスワードを変更することができる
- パスワードをユーザではなくマシンが作成できる
- システムはある種の監査レポートをユーザに提示すべき



Slide 14

セキュアWeb
サーバ構築
実践技法

ユーザ識別とアカウント

ユーザ名とアカウント

- Sensitivity Level Clearance
- Authorization
- パスワードとパスワード制御
- ログイン・パラメータ
- ホーム・ディレクトリとコマンド・シェル
- ユーザ・グループ
- 1ユーザ・1アカウントの原則
- アカウント・ロック機能

アカウント名を監査証跡(audit trail)に記録



セキュアWeb
サーバ構築
実践技法

3重のアクセス制御

- DAC (C1) UNIX permission bits
- DAC (B3) ACL's (Access Control Lists)
- MAC (B1) Sensitivity Labels Sensitivity Level Clearance
Classifications
- (CMW) Compartments

- (CMW) Information Labels

*DAC: Discretionary Access Control (任意アクセス制御)

*MAC: Mandatory Access Control (強制アクセス制御) "automatic"



セキュアWeb
サーバ構築
実践技法

Unix のファイル保護

suzuki.tech
に write の
権限を与える
には？

```
$ chown sato:sales fileA
$ chmod 764 fileA
$ chmod u=rwx,g=rw,o=r fileA
```

Slide 17

セキュアWeb
サーバ構築
実践技法

ACL's (Access Control Lists)

ACL 表現 :

```
(sato.%,rwx)
(%.sales,rw)
(%.%,r)
```

↓

追加 (suzuki.tech,rw)
排除 (%.guest,-)

Slide 18

セキュアWeb
サーバ構築
実践技法

ACL's (Access Control Lists)


集合形式

リスト形式

- (sato.%, rwx)
- (%.sales, rw)
- (%.%, r)
- (suzuki.tech, rw)
- (%.guest, -)
-
-
-

ACL コマンド:

```
$ chacl  
$ lsacl
```




Slide 19

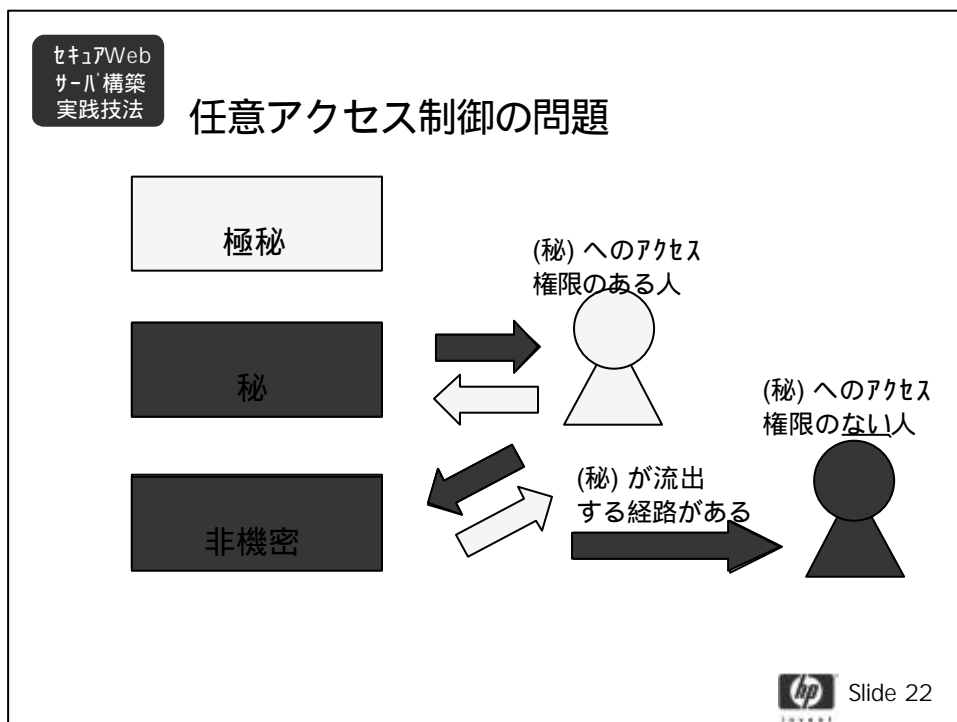
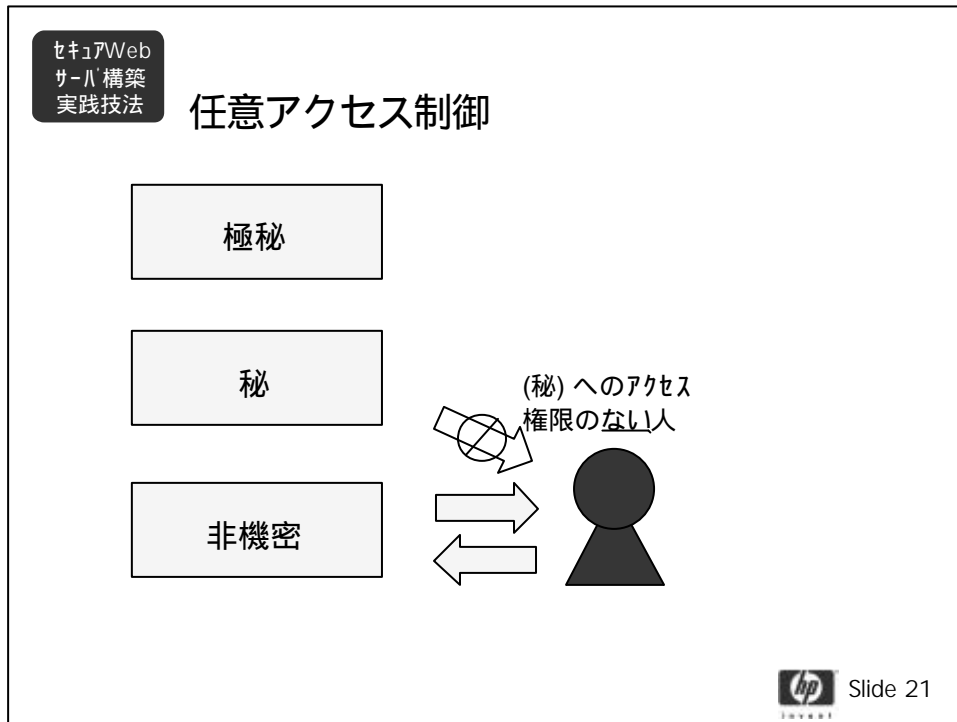
セキュアWeb
サーバ構築
実践技法

任意アクセス制御

(秘) へのアクセス
権限のある人



Slide 20



セキュアWeb
サーバ構築
実践技法


強制アクセス制御による保護

極秘

秘

非機密

下位レベルに書き込めないため無権限者に(秘)が流出しない



Slide 23

セキュアWeb
サーバ構築
実践技法


強制アクセス制御による保護

極秘

秘

非機密

監査証跡は追記専用のため改竄が不可能



Slide 24

セキュアWeb
サーバ構築
実践技法

任意アクセス制御 と 強制アクセス制御

hp Slide 25

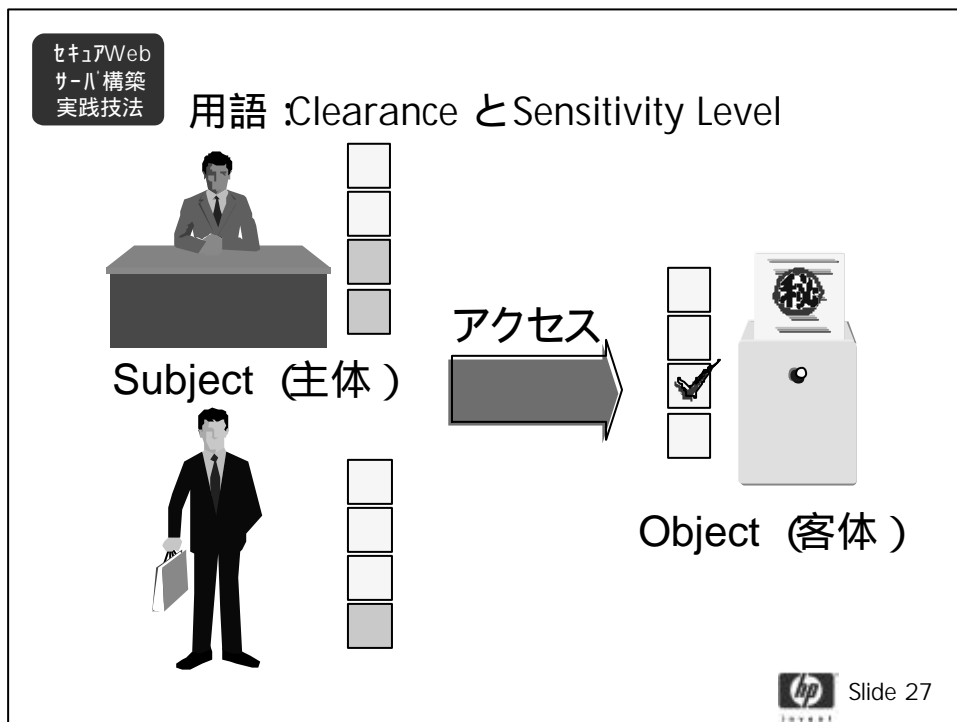
セキュアWeb
サーバ構築
実践技法

BLS の Sensitivity Level の設計 (定義)

最高機密	<input type="checkbox"/>
極秘	<input type="checkbox"/>
マル秘	<input type="checkbox"/>
社外秘	<input type="checkbox"/>

情報の格付け
Classifying Information

hp Slide 26



セキュアWeb
サーバ構築
実践技法

Clearance と Sensitivity Level

最高機密						Subject (主体)
極秘						
マル秘						
社外秘						
	営業	企画	開発	人事	経理	

最高機密						Object (客体)
極秘						
マル秘		✓				
社外秘						
	営業	企画	開発	人事	経理	

hp Slide 29

セキュアWeb
サーバ構築
実践技法

アクセスを許可

適合する

		✓		

営業管理職の
アクセス権

アクセスを許可

ドキュメントの機密ラベル
マル秘 / 企画部門

		✓		

hp Slide 30

セキュアWeb
サーバ構築
実践技法

アクセスを拒否

営業管理職の
アクセス権

適合しない

アクセスを拒否

ドキュメントの機密ラベル
社外秘 / 製品開発部門

hp Slide 31

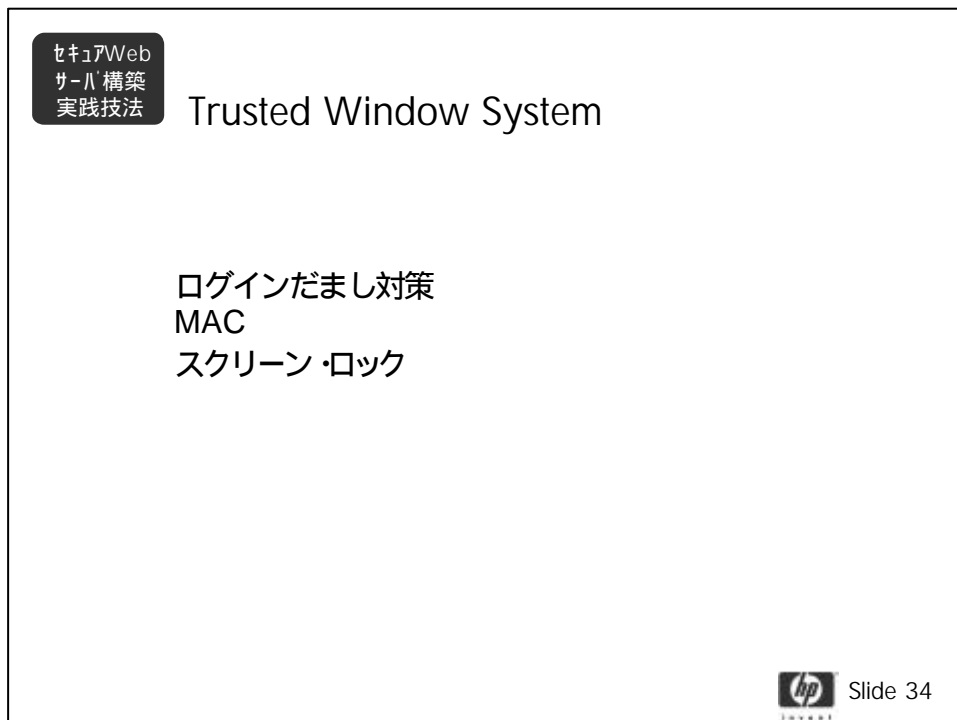
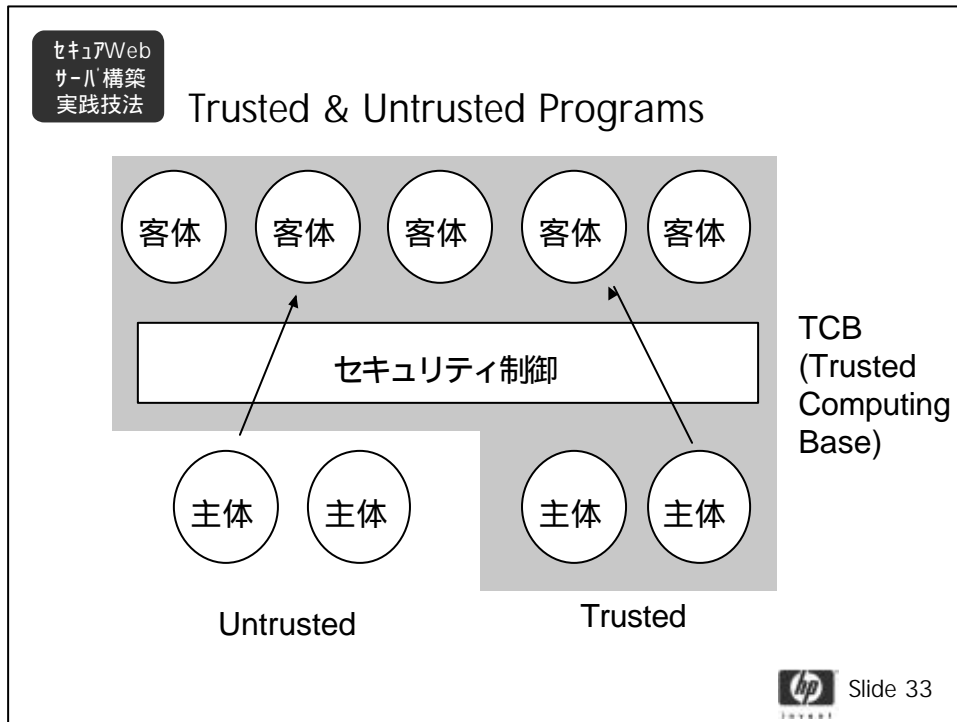
セキュアWeb
サーバ構築
実践技法

Classification と Compartment

Classification (縦軸)	Compartment (横軸)
TOP SECRET (TS)	NATO
SECRET (S)	ALPHA
CONFIDENTIAL (C)	SIOP
UNCLASSIFIED (U)	ULTRA (UL)
	SAC
	TRIDENT (TR)

* CMW TAC4 調達の場合

hp Slide 32



セキュアWeb
サーバ構築
実践技法

Trusted Path

Trusted Chain



Slide 35

セキュアWeb
サーバ構築
実践技法

Sensitivity Labels

- The Basics
- Making them mandatory
- Directory Trees
- Working with SL's
- Multilevel Directories
- Life Under SL's


Classification Compartments

Clearance

cannot know even about existence of the space you cannot access

A dominates B
if & only if
the class of A is higher than or equal to the class of B,
** and **

A contains all the compartments of B (and maybe more)



Slide 36

セキュアWeb
サーバ構築
実践技法

MAC

データフロー制御 (Data Flow Control)

昇格 (Upgrade)

降格 (Downgrade)

Write-Up



Slide 37

セキュアWeb
サーバ構築
実践技法

Directory Trees

Walking a Tree

Single-Level Trees

Multilevel Directories / Not-multilevel Directories



Slide 38

セキュアWeb
サーバ構築
実践技法

Life Under Sensitivity Labels

適切でない Multilevel 環境 - 混在
適切な Multilevel 環境 - 整理

spax



Slide 39

セキュアWeb
サーバ構築
実践技法

Information Labels

Floating Rule
Files
Programs



Slide 40


セキュアWeb
サーバ構築
実践技法

Markings

Ex.

- Shred
- KeepOnSite
- HandCarry
- DoNotCopy
- KeepOnSystem *
- ExpiresMid92 *
- EncryptForTransport *
- NoCommLine *

* Programs could also enforce!



Slide 41

セキュアWeb
サーバ構築
実践技法


Authorizations

Privileges - プログラムの属性
Authorizations - ユーザの属性 (credentials) : 免許証 (車なし)

ISSO がユーザに付与 実行ファイルに付与 プロセスが実行中に保持

Command Authorization Kernel Authorizations Base Privileges	Potential Privilege Granted Privilege	Effective Privilege Potential Privilege
---	--	--

最少特権 (Least Privilege)



Slide 42

セキュアWeb
サーバ構築
実践技法

Trusted Chain

```
$ auths  
chown upgrade writeup  
$ auths -v  
chown upgrade writeup  
(Command auths available)  
$ vi  
  :!sh  
$ auths  
$ auths -v  
chown upgrade writeup  
(Command auths unavailable)
```

 Slide 43

セキュアWeb
サーバ構築
実践技法

パスワード

 Slide 44

セキュアWeb
サーバ構築
実践技法

Import & Export

リムーバブル・メディア
プリント・アウト

Slide 45

セキュアWeb
サーバ構築
実践技法

"Two Key" System

Standard "Roles"

- Security Officer (ISSO)
- System Admin
- Operator
- Network Security Officer

No "root" account
retire? or not?

Slide 46

セキュアWeb
サーバ構築
実践技法

Auditing & Reports



Slide 47

セキュアWeb
サーバ構築
実践技法

Networking --- MaxSix

MaxSix 3.0

DNSIX 2.1 (DoDIIS Network Security for Information Exchange)

CIPSO (Commercial IP Security Option) by TSIG/IETF

RIPSO (Revised IP Security Option) by US DoD



Slide 48

セキュアWeb
サーバ構築
実践技法

CMW 実演

Classification (縦軸)	Compartment (横軸)
TOP SECRET (TS)	NATO
SECRET (S)	ALPHA
CONFIDENTIAL (C)	SIOP
UNCLASSIFIED (U)	ULTRA (UL)
	SAC
	TRIDENT (TR)

* CMW TAC4 調達の場合

 Slide 49

セキュアWeb
サーバ構築
実践技法

質疑応答

 Slide 50

セキュアWeb
サーバ構築
実践技法

Leakage (Covert Channels)

TCSEC のむすび

コンピュータ・システム技術
だけでは、Covert Channels に
よる Leakage (漏洩) を完全
に防ぐことはできない。



Slide 51

セキュアWeb
サーバ構築
実践技法

WEBサーバでの応用例

- ファイアウォール問題の再確認
- サーバの要塞化



Slide 52

セキュアWeb
サーバ構築
実践技法

評価基準の運用

ユーザ教育の徹底

Sensitivity Level の Labeling から始まる

注意義務

報告義務

システムのセキュリティ強度は、そのシステムの
監査証跡 (Audit Trail) の保全性強度に依る

法制度の前提

Dual Lock と司法取引 (免罪制度)

PP(Protection Profile), ST(Security Target), EALの正しい理解

入札方式 (落札基準)との整合が不可欠

 Slide 53

