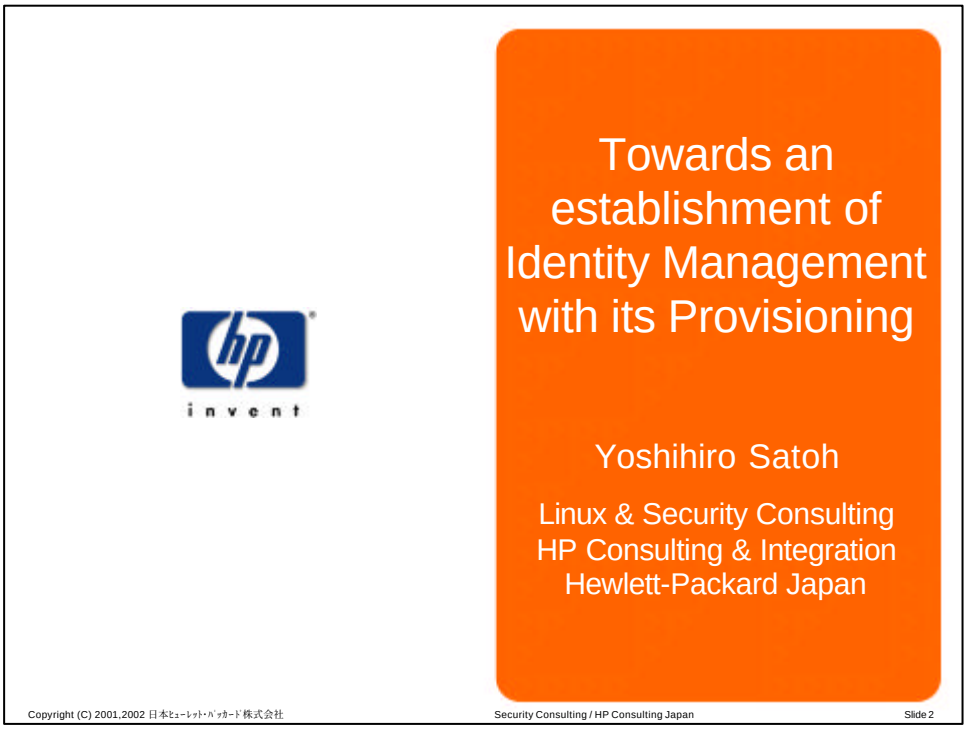


講師略歴

佐藤　慶浩 (さとう　よしひろ)
日本ヒューレット・パッカード株式会社
ＨＰコンサルティング統括本部
Linux & セキュリティ・コンサルティング部　部長

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・パッカード(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社の製品提供と相応して順次担当。この間 1993 年からの 2 年間はカリフォルニア州ク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・パッカード対応窓口を担当。また、ＦISC(金融情報システムセンタ)、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にて情報セキュリティポリシー策定方法論についての講演をしている。

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　非常勤研究員
金融情報サービスセンター(www.fisc.or.jp/)セキュリティポリシー研究会　委員
情報処理学会 情報規格調査会(www.itscj.ipsj.or.jp/) ISO/IEC JTC 1/SC 27/WG 1小委員会　委員
杉並区住基ネット調査会(www.city.suginami.tokyo.jp/)　技術専門委員
情報ネットワーク法学会(www.in-law.jp/) 理事

 Security Consulting / HP Consulting Japan Slide 3

講師略歴

佐藤　慶浩 (さとう　よしひろ)
日本ヒューレット・パッカード株式会社
ＨＰコンサルティング統括本部
Linux & セキュリティ・コンサルティング部　部長

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・パッカード(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社の製品提供と相応して順次担当。この間 1993 年からの 2 年間はカリフォルニア州ク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・パッカード対応窓口を担当。また、ＦISC(金融情報システムセンタ)、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にて情報セキュリティポリシー策定方法論についての講演をしている。

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　非常勤研究員
金融情報サービスセンター(www.fisc.or.jp/)セキュリティポリシー研究会　委員
情報処理学会 情報規格調査会(www.itscj.ipsj.or.jp/) ISO/IEC JTC 1/SC 27/WG 1小委員会　委員
杉並区住基ネット調査会(www.city.suginami.tokyo.jp/)　技術専門委員
情報ネットワーク法学会(www.in-law.jp/) 理事

Copyright (C) 2001,2002 日本ﾋｭｰﾚｯﾄ･ﾊﾟｯｶｰﾄﾞ株式会社 Security Consulting / HP Consulting Japan Slide 4

情報セキュリティ対策の新たな課題

Identity Management

情報へのアクセスについて、「人」を特定する精度を高めなければならない。
管理の対象は、IDではなく、「人」の特定を目標にすべきである。

Provisioning

システム管理者でさえも、未承認のなりすましや、アクセス権変更ができないような運用をしなければならない。
最重要な情報保護は、技術だけではなく、運用を通じて暗黙の例外なく、担保することを目標にすべきである。

 Security Consulting / HP Consulting Japan Slide 5

New challenges for Information security measures

Identity Management

Higher accurate of specifying for “individual person” is needed in access to information.
The goal to be set is that the object of management should be specifying “individual person” instead of “ID code”.

Provisioning

It must be operated which even system administrator cannot spoof user or modify the access rights without approval.
The goal to be set is that the protection of the most important information should be secured without any implicit exception through not only technology but also operation.

 Security Consulting / HP Consulting Japan Slide 6

企業にとって、情報は活用すべきもの。
そのために、ITを導入している。
情報セキュリティは要件であって、目的ではない。

情報セキュリティ対策の基本構成：

性善説を前提に、性悪説を想定する。

これら2つの対策は、種の異なるものである。

 Security Consulting / HP Consulting Japan Slide 7

For enterprise, information is to make the best of use. IT is deployed to do so.
The information security is a requirement, but not objective.

Basic construction of information security measures:

Assumption: human nature is as fundamentally good

Constrain: ill-natured activity is possible

Those two measures are completely different kinds.

 Security Consulting / HP Consulting Japan Slide 8

性善説対策の確立

WHAT：覚えられないことは、守れない

WHY：理由がわからなければ、例外処理ができない

WHO：逸脱の必要性を想定し、誰なら逸脱を承認できるかを予め決めておく

適正水準の堅持

規則は守らなければならないこと→逸脱手続きがあるのだから守れないはずはない

規則は守れること→組織の支援は、組織の義務

最低水準より、適正水準

守りから攻めへ→足りぬは禁。やり過ぎも禁。ITの目的の認識。

人には教育が必要

教育は開催することではなく、受講することに意味がある

教育体制のトースタモデル化→セキュリティだけのための体制は荷が重いはず

部下の受講は上司の責務

部下の未受講に対する、管理職に対する、厳罰も検討→部下の問題ではないはず

 Security Consulting / HP Consulting Japan Slide 9

Establish of measures for nature as fundamentally good

WHAT: People cannot follow if they cannot remember.

WHY: People cannot do exceptional process if they do not know about the reason.

WHO: Assuming for deviation, it must be designed in advance who is the right person to approve the deviation.

holding the level of “just-enough”

規則は守らなければならないこと→逸脱手続きがあるのだから守れないはずはない

規則は守れること→組織の支援は、組織の義務

“just-enough” rather than “base-lining”

from defense to offence --- No less and No much. Remember the objective of IT.

Education is mandatory for human

教育は開催することではなく、受講することに意味がある

教育体制のトースタモデル化→セキュリティだけのための体制は荷が重いはず

部下の受講は上司の責務

部下の未受講に対する、管理職に対する、厳罰も検討→部下の問題ではないはず

 Security Consulting / HP Consulting Japan Slide 10

性悪説対策の確立

不正アクセス＝
許可されたアクセスの濫用＋無許可のアクセス

許可されたアクセスの濫用

やればできるが、やらない

証跡保全対策とその周知による抑止

無許可のアクセス

守れない限界の認識→ｲﾝｼﾃﾞﾝﾄ・ﾏﾈｰｼﾞﾒﾝﾄ

 Security Consulting / HP Consulting Japan Slide 11

Establish of measures for ill-natured activity

illegal access =
abuse of authorized access + unauthorized access

abuse of authorized access

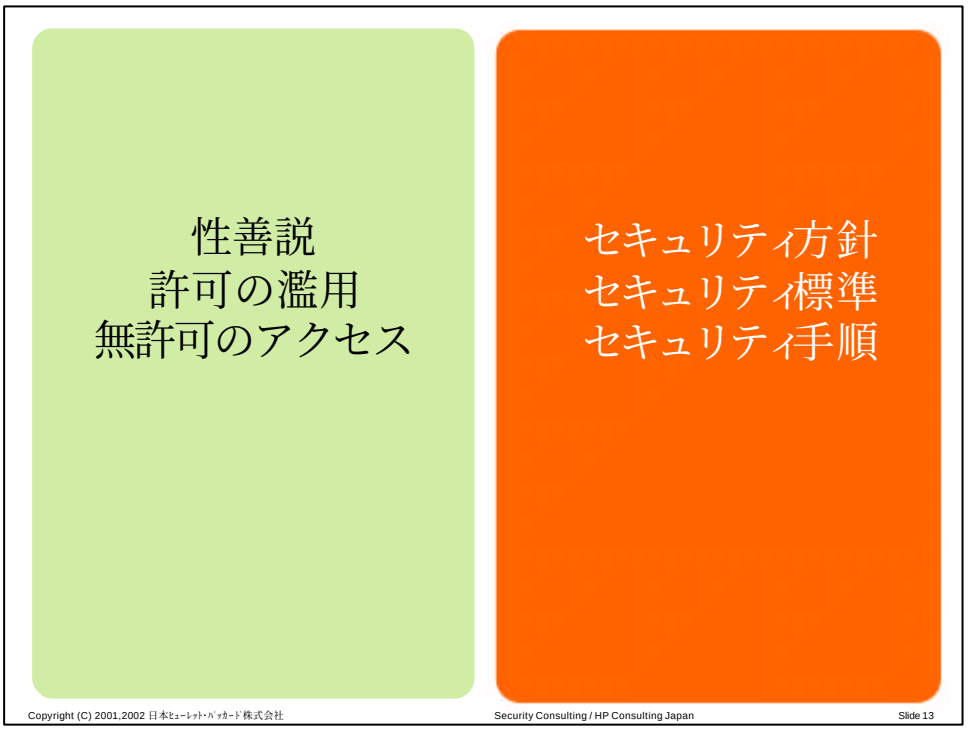
Never do although one can do

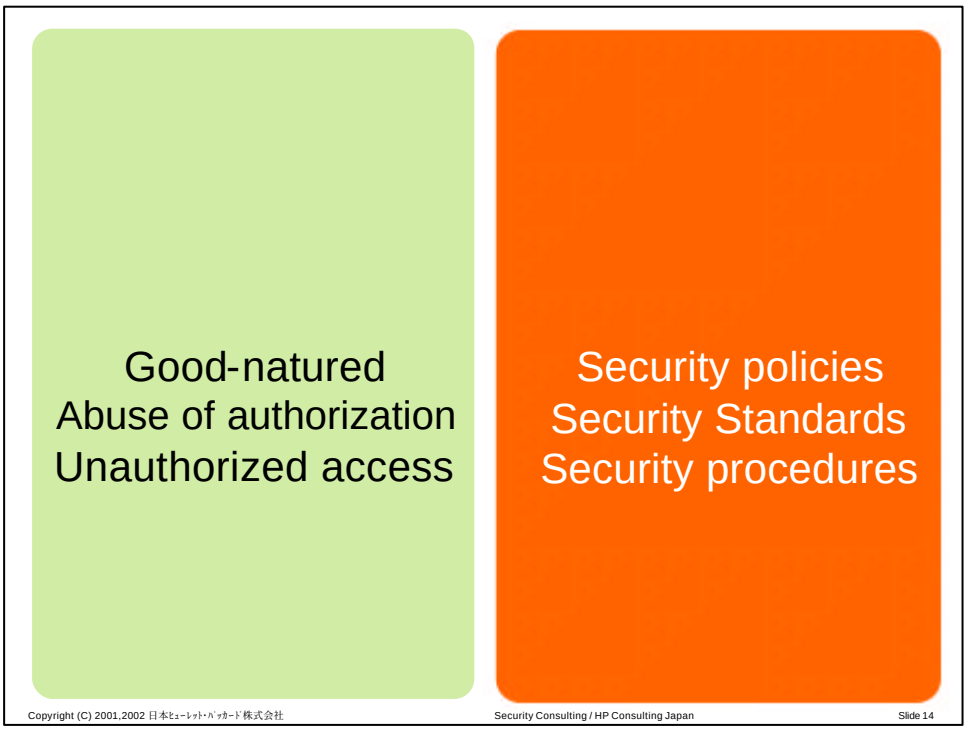
Integrity of audit trail and its awareness act as a deterrent

unauthorized access

Assuming the limitation of protection
--- incident management is mandatory

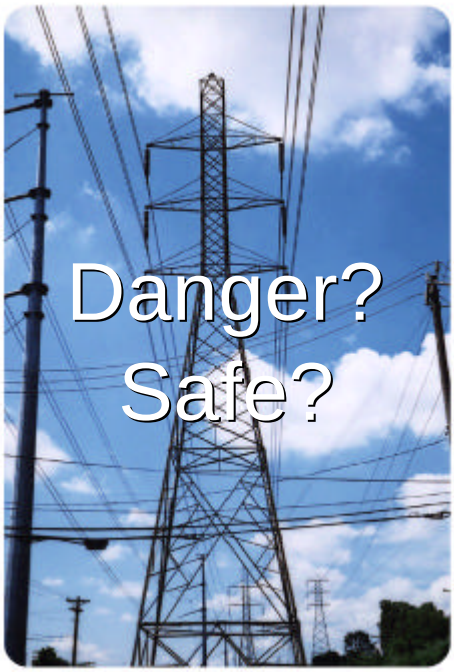
 Security Consulting / HP Consulting Japan Slide 12





ナイフで人を
傷つけられますか？

ナイフなしで
生活できますか？



Can a Knife be
used for killing?

Can you live without
any Knife?

われわれは、人を傷つけることが可能な、ナイフを使って生活している

やればできるが、やらない

We are living with the Knives which can be used to kill.

Never do although you can do

TCSEC の基礎技術要素の相互依存

CLASSIFICATION
AUTHENTICATION
ACCESS CONTROL
INFORMATION FLOW CONTROL
LEAST PRIVILEGE
AUTHORIZATION (DUAL LOCK)
AUDITING ◆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

covert channel

 Security Consulting / HP Consulting Japan Slide 19

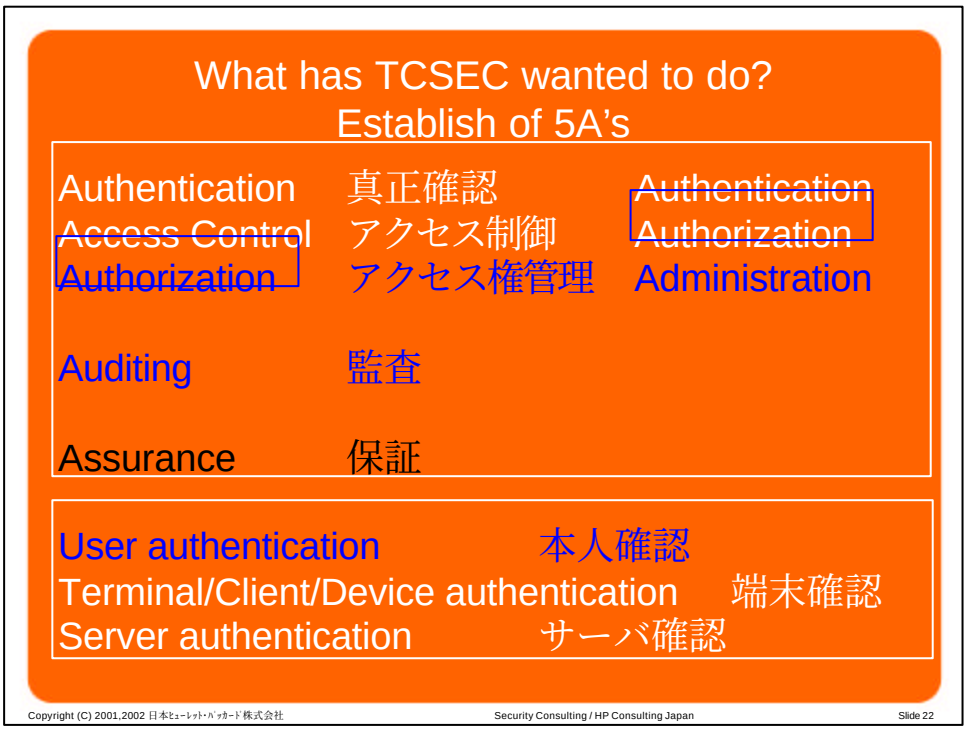
Inter-dependencies of fundamental technology components of TCSEC

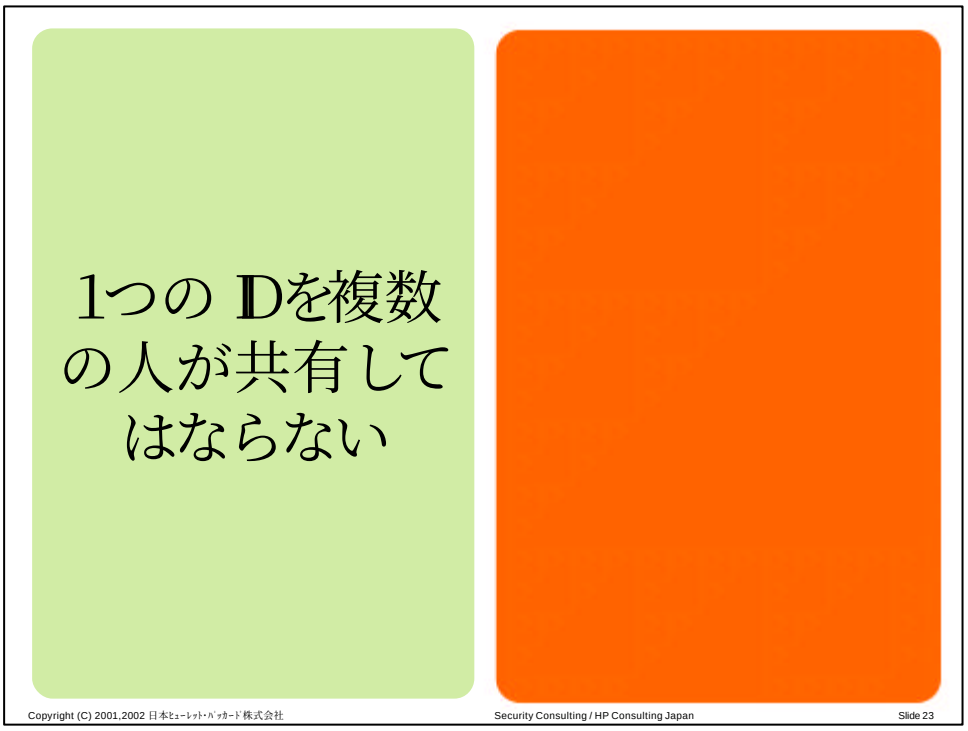
CLASSIFICATION
AUTHENTICATION
ACCESS CONTROL
INFORMATION FLOW CONTROL
LEAST PRIVILEGE
AUTHORIZATION (DUAL LOCK)
AUDITING ◆The strength of system security is determined by the integrity of its audit trail.

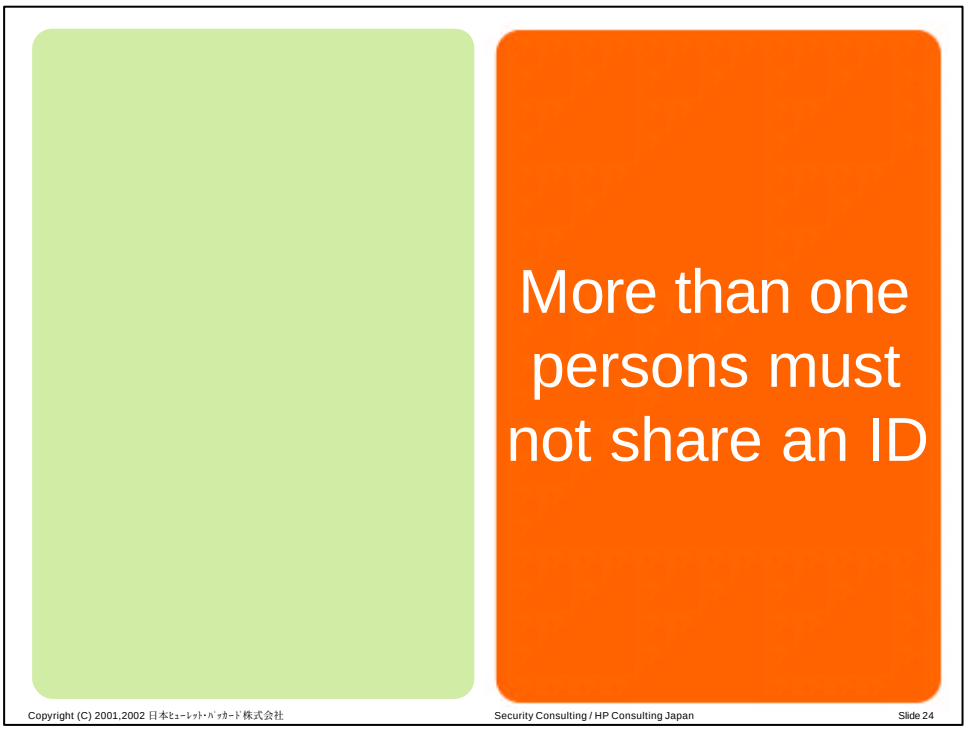
covert channel

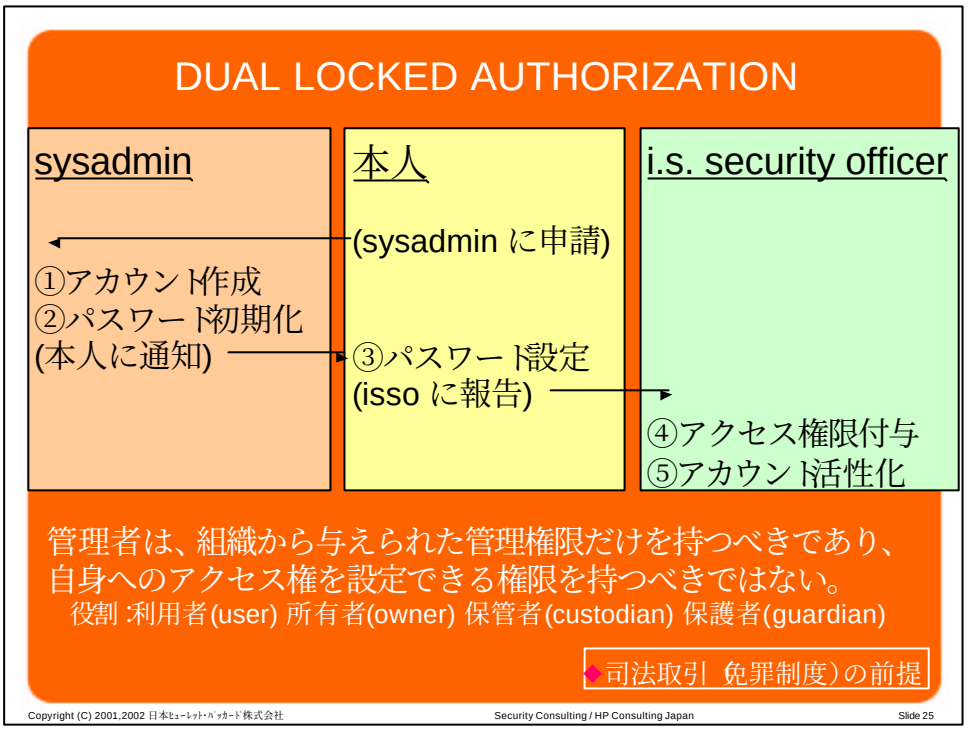
 Security Consulting / HP Consulting Japan Slide 20

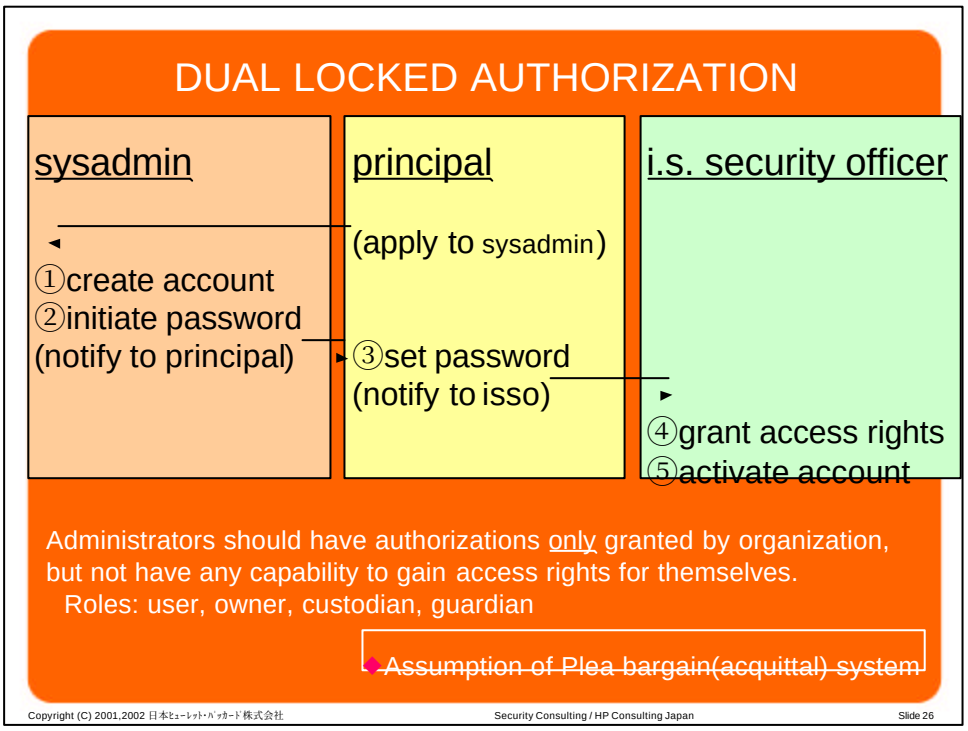

TCSEC は何がしたかったのか？
→ 5A の確立
Authentication 真正確認
Access Control アクセス制御
Authorization アクセス権管理
Auditing 監査
Assurance 保証
Authentication
Authorization
Administration
User authentication 本人確認
Terminal/Client/Device authentication 端末確認
Server authentication サーバ確認
Copyright (C) 2001,2002 日本ヒューレット・パッカード株式会社
Security Consulting / HP Consulting Japan
Slide 21


What has TCSEC wanted to do?
Establish of 5A's
Authentication 真正確認
Access Control アクセス制御
Authorization アクセス権管理
Auditing 監査
Assurance 保証
Authentication
Authorization
Administration
User authentication 本人確認
Terminal/Client/Device authentication 端末確認
Server authentication サーバ確認
Copyright (C) 2001,2002 日本ヒューレット・パッカード株式会社
Security Consulting / HP Consulting Japan
Slide 22

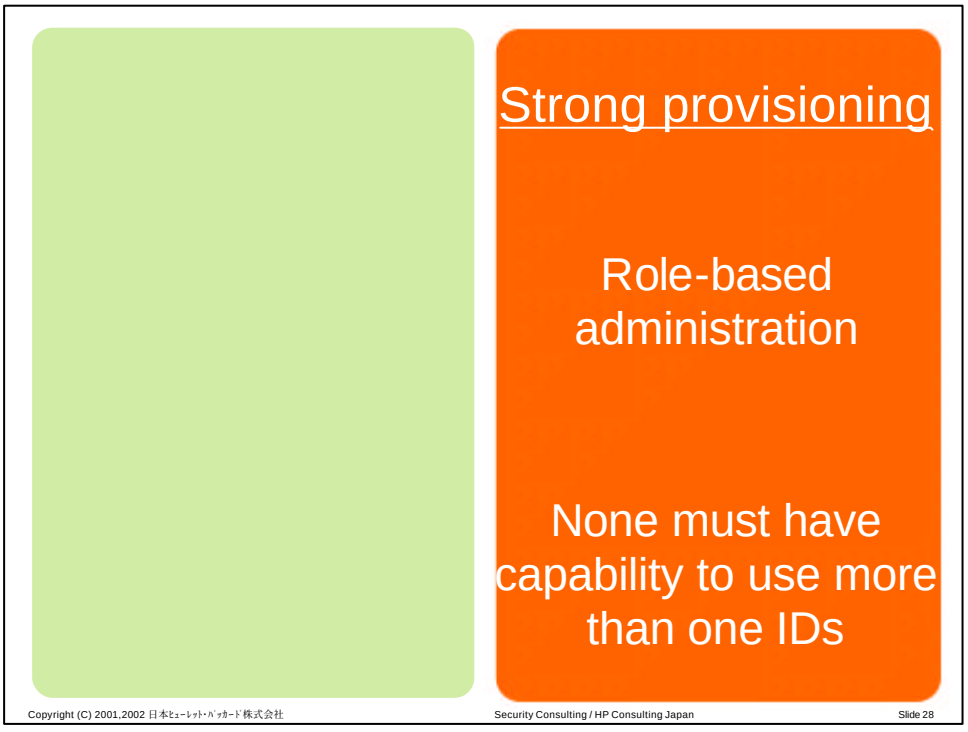

1つの IDを複数の人が共有してはならない
Copyright (C) 2001,2002 日本ヒューレット・パッカード株式会社
Security Consulting / HP Consulting Japan
Slide 23


More than one persons must not share an ID
Copyright (C) 2001,2002 日本ヒューレット・パッカード株式会社
Security Consulting / HP Consulting Japan
Slide 24






強固な provisioning
役割ベースのシステム管理
一人が複数の IDを使用できてはならない
Copyright (C) 2001,2002 日本ヒューレット・パッカード株式会社
Security Consulting / HP Consulting Japan
Slide 27


Strong provisioning
Role-based administration
None must have capability to use more than one IDs
Copyright (C) 2001,2002 日本ヒューレット・パッカード株式会社
Security Consulting / HP Consulting Japan
Slide 28

情報セキュリティ対策の新たな課題

Identity Management

情報へのアクセスについて、「人」を特定する精度を高めなければならない。
管理の対象は、IDではなく、「人」の特定を目標にすべきである。

Provisioning

システム管理者でさえも、未承認のなりすましや、アクセス権変更ができないような運用をしなければならない。
最重要な情報保護は、技術だけではなく、運用を通じて暗黙の例外なく、担保することを目標にすべきである。

 Security Consulting / HP Consulting Japan Slide 29

New challenges for Information security measures

Identity Management

Higher accurate of specifying for “individual person” is needed in access to information.
The goal to be set is that the object of management should be specifying “individual person” instead of “ID code”.

Provisioning

It must be operated which even system administrator cannot spoof user or modify the access rights without approval.
The goal to be set is that the protection of the most important information should be secured without any implicit exception through not only technology but also operation.

 Security Consulting / HP Consulting Japan Slide 30

www.hp.com/jp/security

http:// yosihiro.com /

Copyright (C) 2001,2002 日本ヒューレット・パッカード株式会社 Security Consulting / HP Consulting Japan Slide 31

www.hp.com/jp/security

http:// yosihiro.com /

Copyright (C) 2001,2002 日本ヒューレット・パッカード株式会社 Security Consulting / HP Consulting Japan Slide 32