

国立情報学研究所オープンハウス「スマホ持ち込みのセキュリティ対策」
2012年6月7日

IT戦略の中に情報セキュリティ対策を 位置付けることの重要性



弊社IT部門におけるモバイルIT環境構築を事例として

日本ヒューレット・パッカード株式会社
佐藤 慶浩

発表者紹介

佐藤 慶浩(さとう よしひろ)

日本ヒューレット・パカード 個人情報保護対策室 室長

社外の活動

元 内閣官房 情報セキュリティセンター 指導専門官

デジタル・フォレンジック研究会 理事

情報ネットワーク法学会 副理事長

など

詳細

よしひろ.com

<http://yoshihiro.com/profile/resume.html>



目次

IT環境構築事例の紹介

IT環境設計の考え方

まとめ



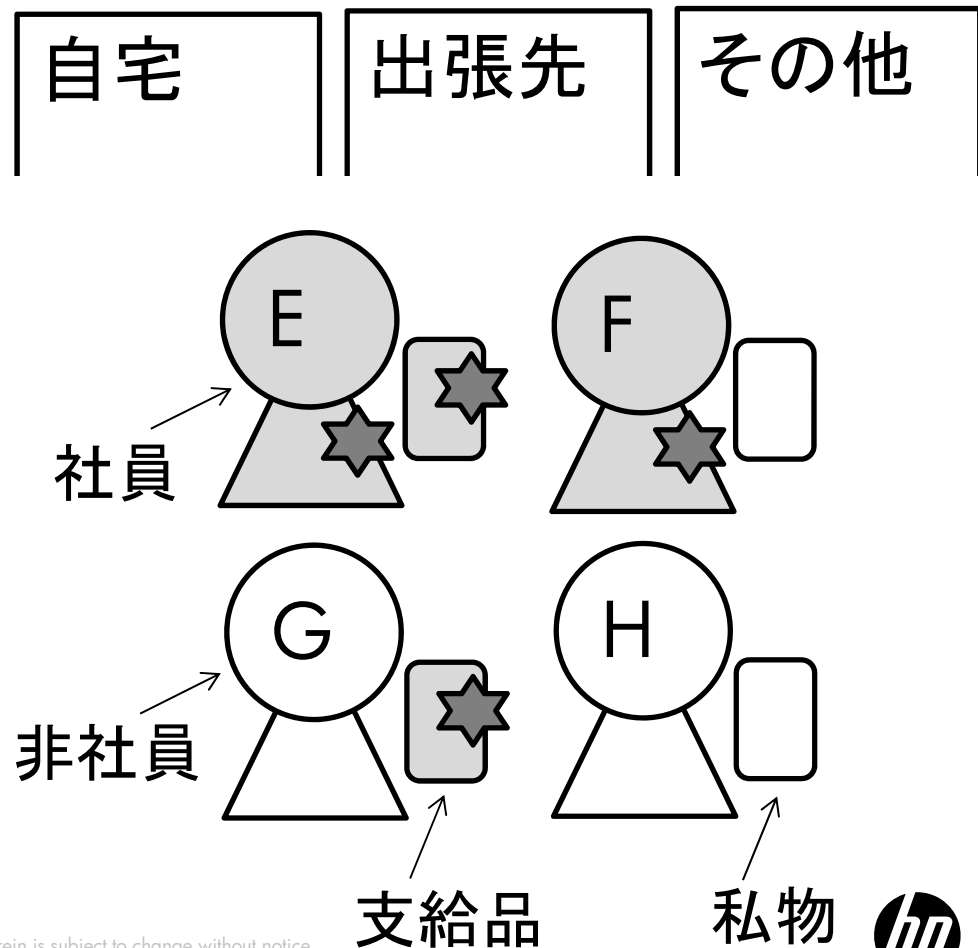
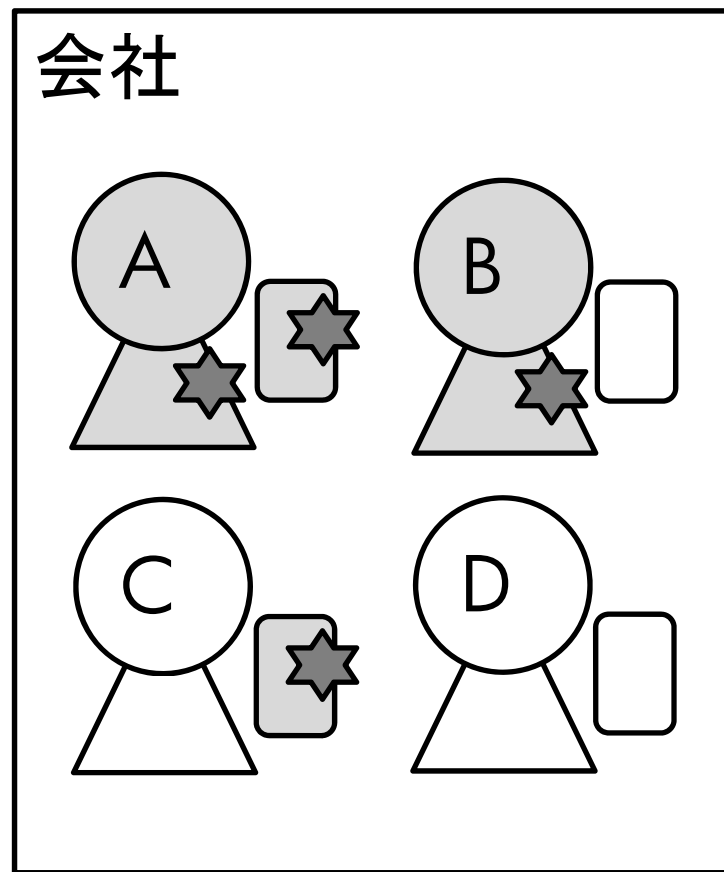
環境事例の紹介

HP社のIT部門が社員向けに提供しているサービスの紹介です



モバイルIT環境の事例紹介

MMS(Managed Mobile Service) Mobile-Net



MMS(Managed Mobile Service)概要

MMS(Managed Mobile Service) とは、弊社社員のモバイルIT機器を弊社内のITサービスにアクセスできるようにするサービスです。

モバイルIT機器として、弊社支給品と社員の私物(BYOD)の両方が対象であり、それらを技術条件として区別しません。

社員の私物(BYOD)の社内ネットワーク接続を認めるということではなく、弊社ITサービスにアクセスできるようにするという点が特徴です。

アクセス可能なITサービスは「電子メール、予定表、連絡先、タスクリスト」に原則として限定されます。(特別な承認を得ることでVPN接続も技術的には可能ですが、原則としては認められません。)



MMS(Managed Mobile Service)

MMS利用承認

業務の必要性により承認

自己負担一直属上司承認

会社負担一直属上司及びVP承認 ☆利用条件は自己負担と同じ

※いずれも、Solution sourceによる電子申請と決裁

MMS利用制限

非機密、HP Restricted, HP Confidential情報まで取扱い可能

HP Private情報の取扱い禁止

MMS利用条件 ☆現時点の対応: Windows Phone 7, Android, iOS/iPhone, webOS/Palm

以下のすべての技術要件を満たすことが条件

端末のPINロック

40分以下のタイムアウト設定

遠隔データ消去機能(本人消去、IT Help Desk消去、IT部門消去)

遠隔管理機能及び暗号化 現時点ではWindows Mobile 6.xのみ

※上記すべて、端末認証時に自動設定



MMS(Managed Mobile Service)

Office Outlook Web Access
Microsoft Exchange に接続しました

オプション

上書き保存 ヘルプ

モバイル機器

ここでモバイル デバイスを管理します。

使用しなくなったデバイスを削除することができます。デバイスのパスワードを忘れた場合は、ここからアクセスできます。電話またはモバイル デバイスを紛失した場合、デバイスの消去をリモートで行うことで情報を保護することができます。

新しいデバイスを追加するには、デバイスから Microsoft Exchange とのパートナーシップを開始してください。それにより、以下の一覧にデバイスが表示されます。

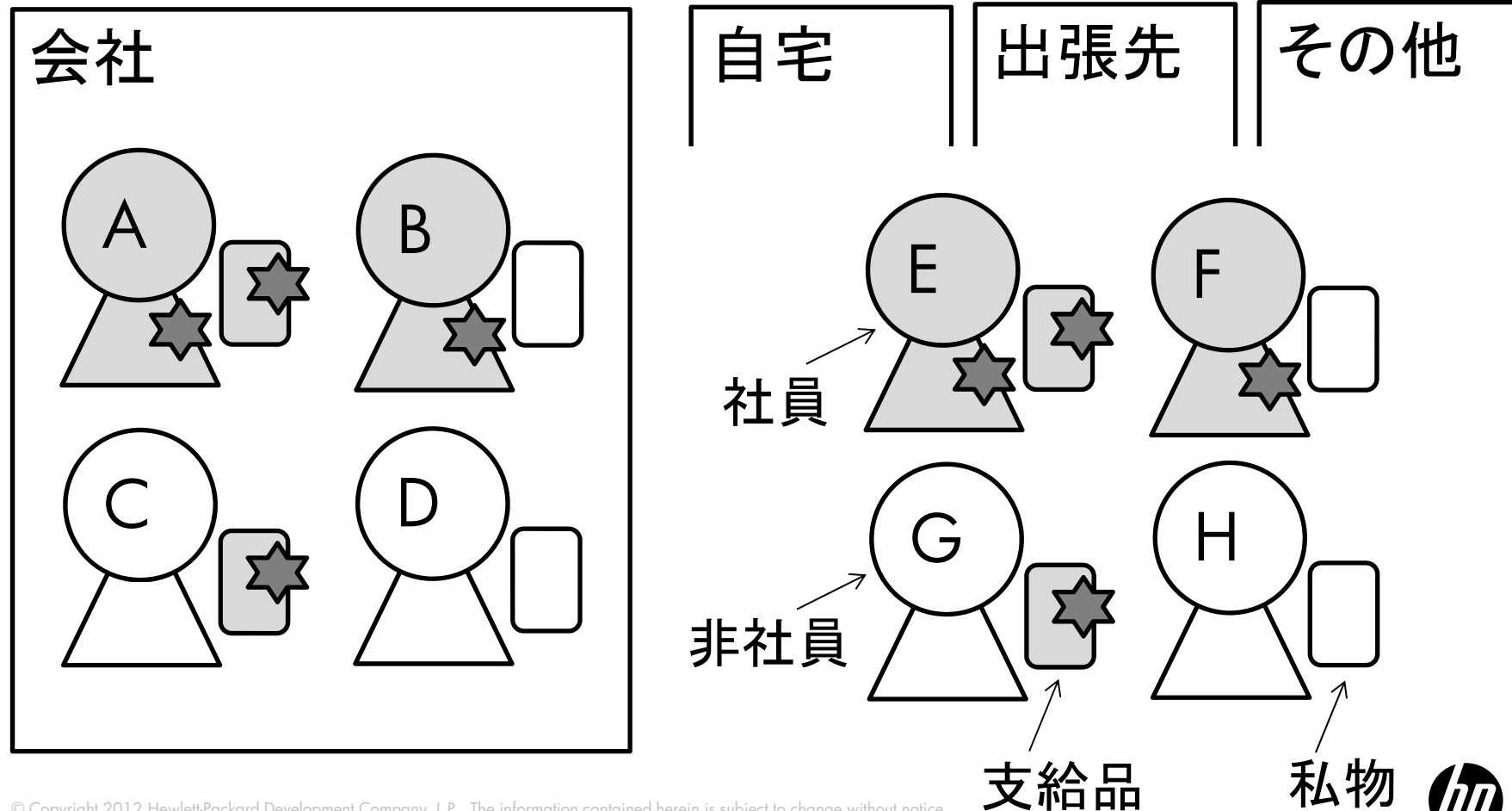
デバイスを一覧から削除... **デバイス上のすべてのデータの消去を実行...** 回復のパスワードを表示する

デバイス	最終同期時刻	状態
iPad	2012/02/02 (木) 16:02	OK 最初の同期日時: 2011/05/31 (火) 10:33 正常な最終同期日: 2012/02/02 (木) 16:02 デバイス ID: [REDACTED] ユーザー エージェント: [REDACTED]

不明なゾーン (混在) | 保護モード: 無効 100%

モバイルIT環境の事例紹介

MMS(Managed Mobile Service) Mobile-Net



Mobile-Net 概要

HP社内 Mobile-Net とは、弊社社員の私物IT機器 (BYOD:Bring your own device)と弊社施設に来訪される方々のIT機器をインターネット接続するための無線LAN環境です。

BYODについてWiFiスポットの作成を禁止 (WiFiテザリング)する代わりに、Mobile-Netを提供して、ルールの実効性を確実にしている。

社員によるセルフ管理サービスでお客様も利用可能。



Mobile-Net 概要

- ①ゲスト用アカウントの作成
- ②ゲスト用アカウントとパスワードの送信/印刷
- ③お客様によるゲスト用パスワードの受信
- ④端末でのゲスト用アカウントによる接続認証

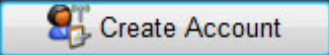
参考: ゲスト用アカウントの管理

参考: ゲストの接続状況の管理



Mobile-Net

①ゲスト用アカウントの作成

HP Employee LDAP Guest Account	
* Sponsor's Name:	@hp.com Name of the person sponsoring this visitor account.
* Visitor's Name:	John Guest Name of the visitor.
* Company Name:	Company Company name of the visitor.
* Email Address:	john.guest@company.com The visitor's email address. This will become their username to log into the network.
Account Activation:	Now Select an option for changing the activation time of this account.
Expires After:	1 day Amount of time before this visitor account will expire.
* Expire Action:	Delete and logout at specified time Select an option for controlling the expiration of this account. Note that a logout can only occur if the NAS is RFC-3576 compliant.
* Account Role:	Guest Role to assign to this visitor account.
Password:	03388565
* Terms of Use:	☒ I am the sponsor of this visitor account and accept the terms of use
 	

Mobile-Net

②ゲスト用アカウントとパスワードの送信/印刷

Finished Creating Guest Account

GUESTS

- Start Here
- Active Sessions
- Create Account
- List Accounts

The guest account was successfully created.

Account Details	
Guest username:	john.guest@company.com
Guest password:	03388565
Account expiration:	Account will expire at Friday, 09 December 2011, 10:55 PM
Account role:	Guest
Sponsor name:	admin@hp.com

Open print window using template...

Send email receipt to john.guest@company.com

Send email receipt

Create another guest account

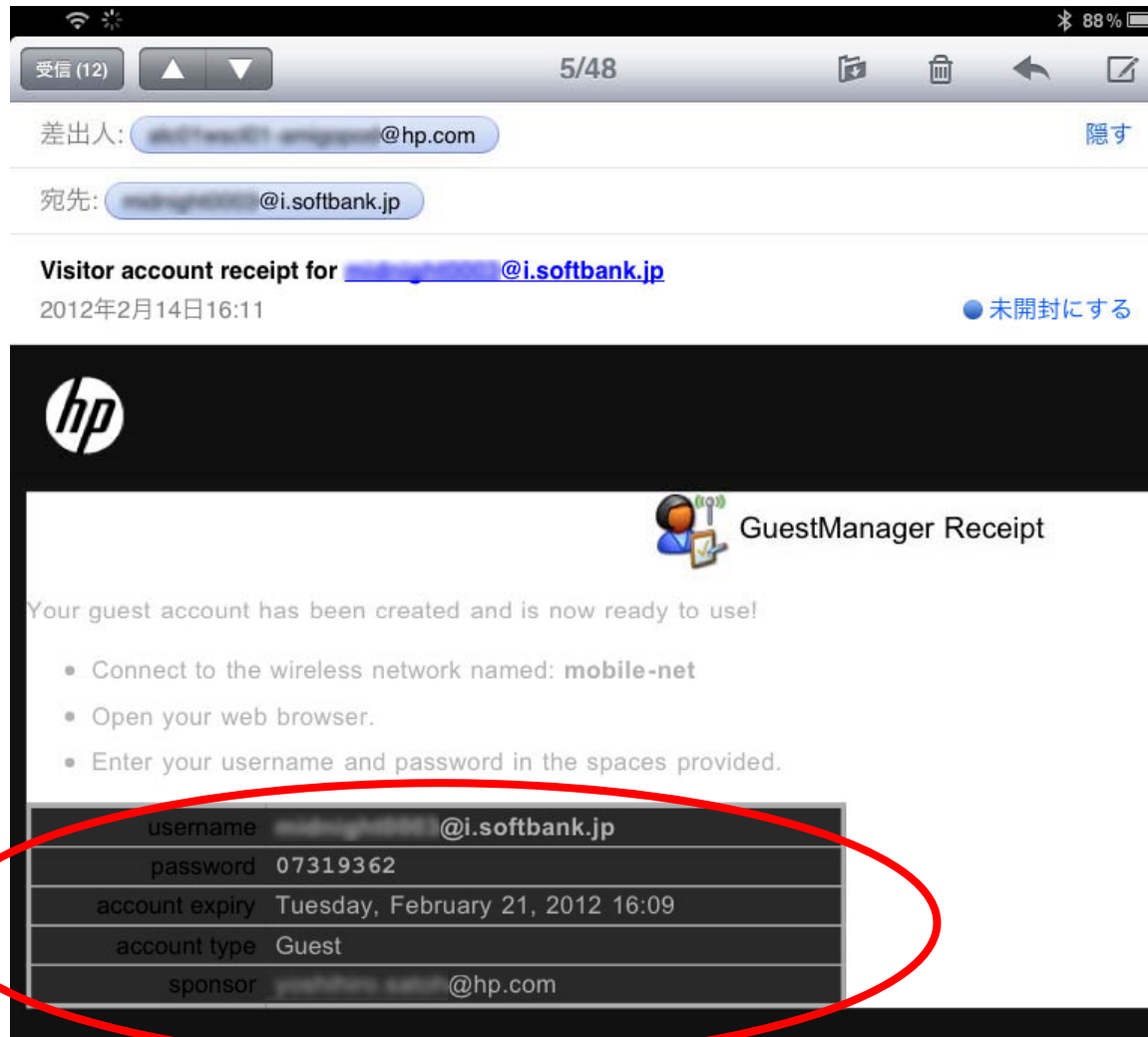
Back to guests

List guest accounts

Back to main

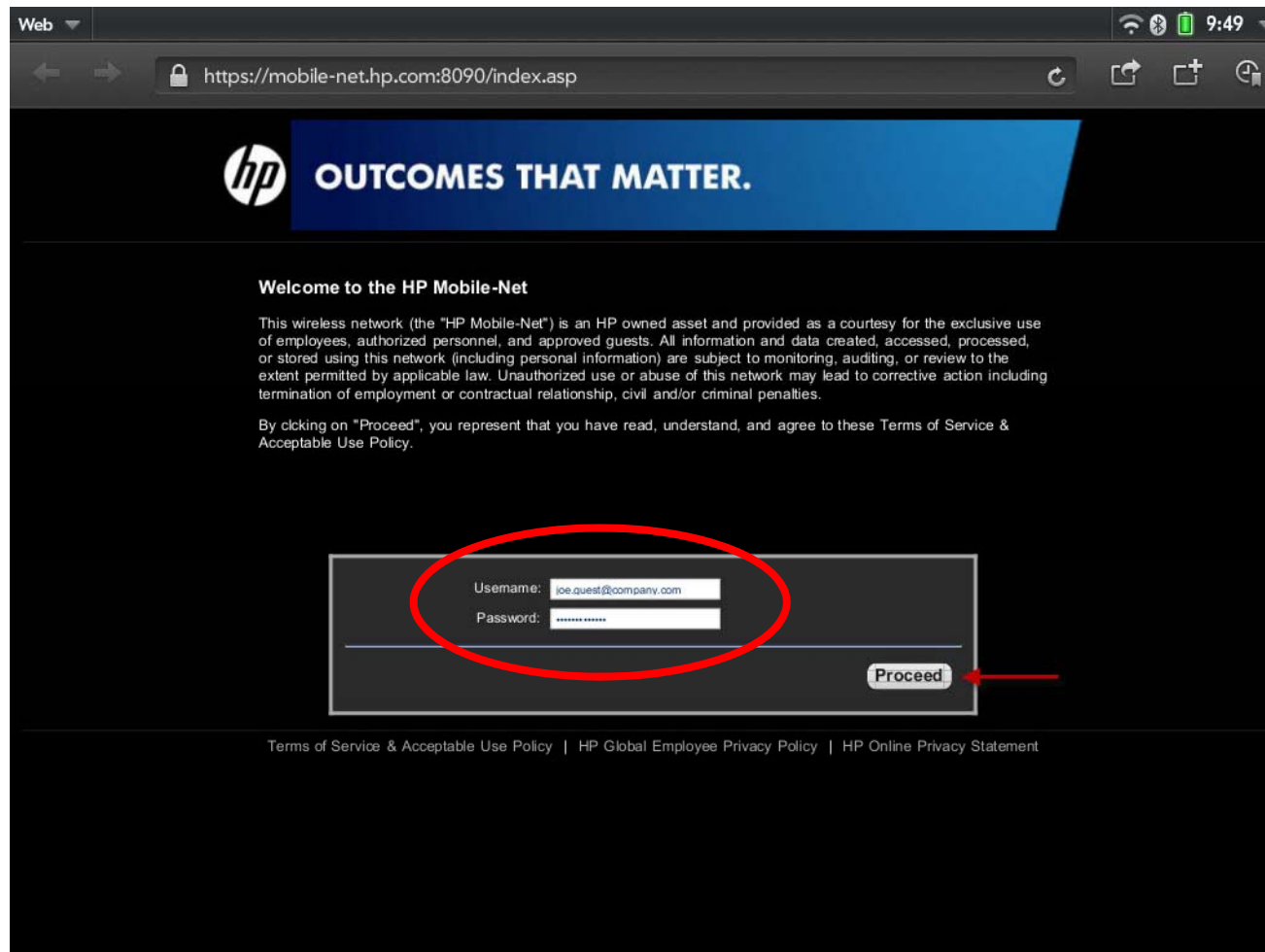
Mobile-Net

③お客様によるゲスト用パスワードの受信



Mobile-Net

④端末でのゲスト用アカウントによる接続認証



Web ▾

https://mobile-net.hp.com:8090/index.asp

hp OUTCOMES THAT MATTER.

Welcome to the HP Mobile-Net

This wireless network (the "HP Mobile-Net") is an HP owned asset and provided as a courtesy for the exclusive use of employees, authorized personnel, and approved guests. All information and data created, accessed, processed, or stored using this network (including personal information) are subject to monitoring, auditing, or review to the extent permitted by applicable law. Unauthorized use or abuse of this network may lead to corrective action including termination of employment or contractual relationship, civil and/or criminal penalties.

By clicking on "Proceed", you represent that you have read, understand, and agree to these Terms of Service & Acceptable Use Policy.

Username:

Password:

Terms of Service & Acceptable Use Policy | HP Global Employee Privacy Policy | HP Online Privacy Statement

参考：
社員所有の端末については、事前の設定や手続きなしに、社員自身のメールアドレスとパスワードにより、接続することができる。



Mobile-Net

参考: ゲスト用アカウントの管理

hp | Home | **Guests** | Logout

Guest Manager Accounts

GUESTS

Start Here
Active Sessions
Create Account
List Accounts

The following table shows the guest accounts that have been created. Click an account to modify it.

Username	Sponsor	Role	Status	Expiration
@i.softbank.jp	@hp.com	Guest	Enabled	2012-02-21 16:09
@gmail.com	@hp.com	Guest	Enabled	2012-02-21 16:15

Quick Help Create

Filter:

Reset password Remove Sessions Print

Refresh 1 Showing 1 - 2 of 2 20 rows per page

ゲスト用アカウントは、それを発行した社員が管理する。
パスワードのリセットも必要に応じて社員が行なう。

Mobile-Net

参考: ゲストの接続状況の管理

The screenshot shows the HP Mobile-Net management interface. At the top, there's a navigation bar with the HP logo, 'Home', 'Guests' (highlighted in green), and 'Logout'. Below this is the 'Active Sessions' section. On the left, a sidebar lists 'GUESTS', 'Start Here', 'Active Sessions', 'Create Account', and 'List Accounts'. The main content area has a header 'Use this list view to view and manage the active sessions on the server.' and a sub-header 'Manage Multiple Sessions' which is circled in red. This dialog box contains three radio button options: 'Disconnect Active Sessions' (selected), 'Reauthorize Active Sessions', and 'Close Open Sessions'. It also has fields for 'Start Time' and 'End Time' with dropdown menus, and buttons for 'Make Changes' and 'Cancel'. Below the dialog, there's a search filter section and a table of active sessions. The table has columns for Username, IP Address, MAC Address, Role, NAS, Session Start, Session Time, and Session Traffic. One session is listed with Username '@i.softbank.jp', IP Address '10.44.1.197', MAC Address 'a4:67:06:00:00:04', Role 'Guest', NAS 'ssid1mc01', Session Start '2012-02-14 16:42', Session Time '0sec', and Session Traffic '0.0 MB'. At the bottom, there's a 'Refresh' button, a page number '1', and a 'Showing 1 - 1 of 1' indicator with a '20 rows per page' dropdown.

hp | Home | **Guests** | Logout

Active Sessions

GUESTS

Start Here
Active Sessions
Create Account
List Accounts

Use this list view to view and manage the active sessions on the server.

Manage Multiple Sessions

* Action:

- ☒ Disconnect Active Sessions
- ☐ Reauthorize Active Sessions
- ☐ Close Open Sessions

Start Time: ...
The selected action will apply to sessions that started after this point. Leave blank to use the earliest available session start time.

End Time: ...
The selected action will apply to sessions that started before this point. Leave blank to use the current time.

* required field

Filter:
Search all fields that have been configured for 'quick search'.

Showing: Active sessions only.

	Username	IP Address	MAC Address	Role	NAS	Session Start	Session Time	Session Traffic
	@i.softbank.jp	10.44.1.197	a4:67:06:00:00:04	Guest	ssid1mc01	2012-02-14 16:42	0sec	0.0 MB

Showing 1 - 1 of 1

1 20 rows per page

設計の考え方

HP社のIT部門のIT環境設計時の考え方の紹介です



設計の考え方

組織としてどのようなIT環境を構築するのか、どのようなITサービスを提供するのかについての方針＝IT戦略に基づいて、ITシステムの構築を目的として実施する。
その中で、必要な情報セキュリティ対策を要件として実施する。



プチSoAと プチEAの薦め

SoA: Service oriented Architecture
EA: Enterprise Architecture

プチSoAの薦め

モバイル環境での業務に必要なITサービスを提供する。というIT戦略に基づく、モバイルITアクセス・サービスとして構築されている。

結果的に、弊社においてスマートフォン対策を独立したものとして特段に講じていない。

サービスの視点で、最初に考える＝SoA (Service oriented architecture)ということが重要。

×どのような端末を接続するのか？という議論

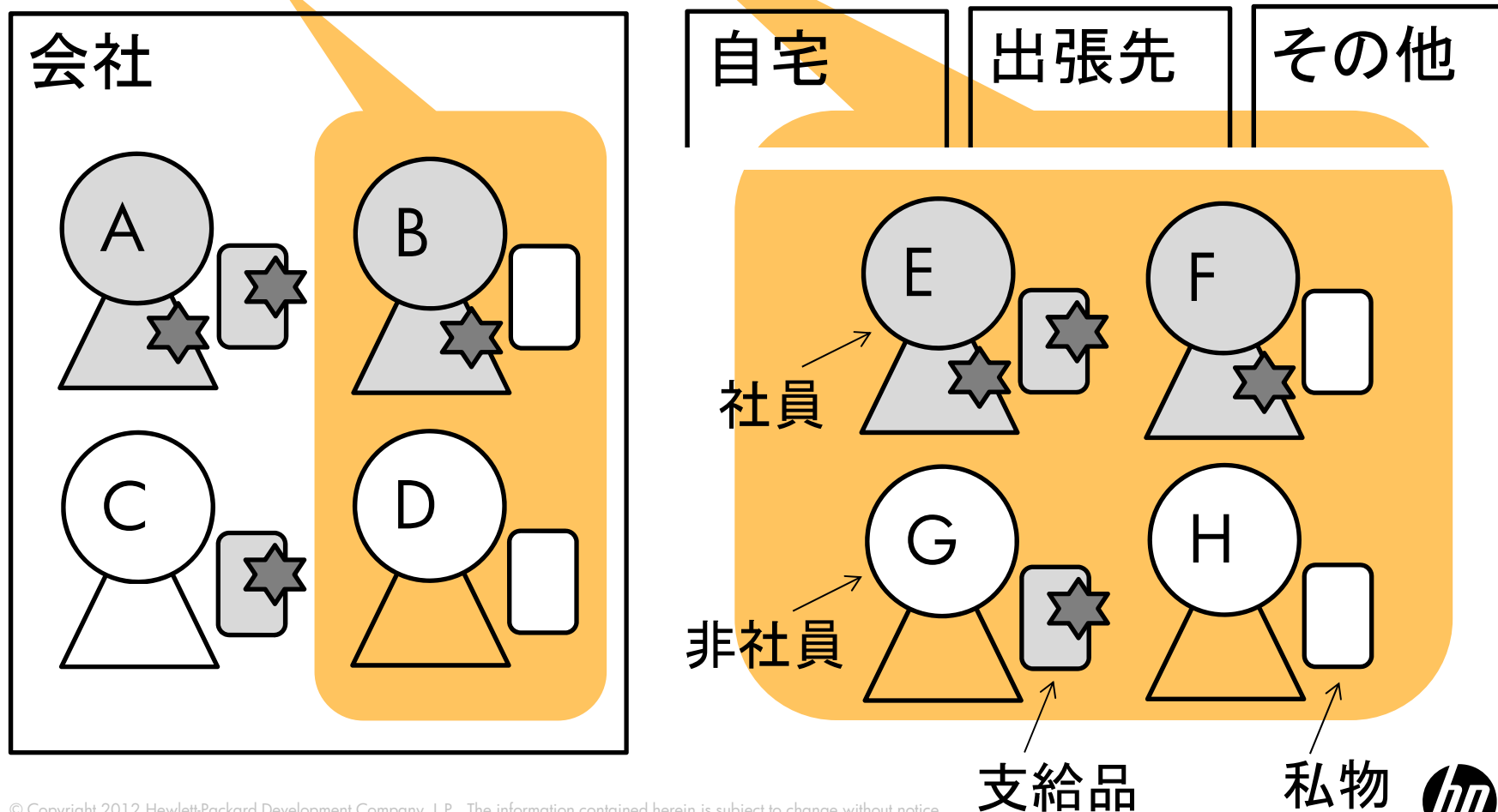
○どのようなサービスを端末に提供するのか？という議論

スマートフォンのセキュリティ対策は利用者個人としての課題として重要なこと。しかし、企業課題ではない。



プチSoAの薦め: モバイルIT環境の事例紹介

MMS(Managed Mobile Service)
Mobile-Net



プチSoAの薦め(つづき)

IT戦略なき、情報セキュリティ対策は、非効率かつ実効性の低下につながる。

簡単なチェックポイントは「どんなサービスの提供か？」という視点。(=SoA)

検討対象が、目的なのか手段なのかを明確にしてから検討することが重要。→目的がセキュリティ対策というのは、本末が転倒している警告。

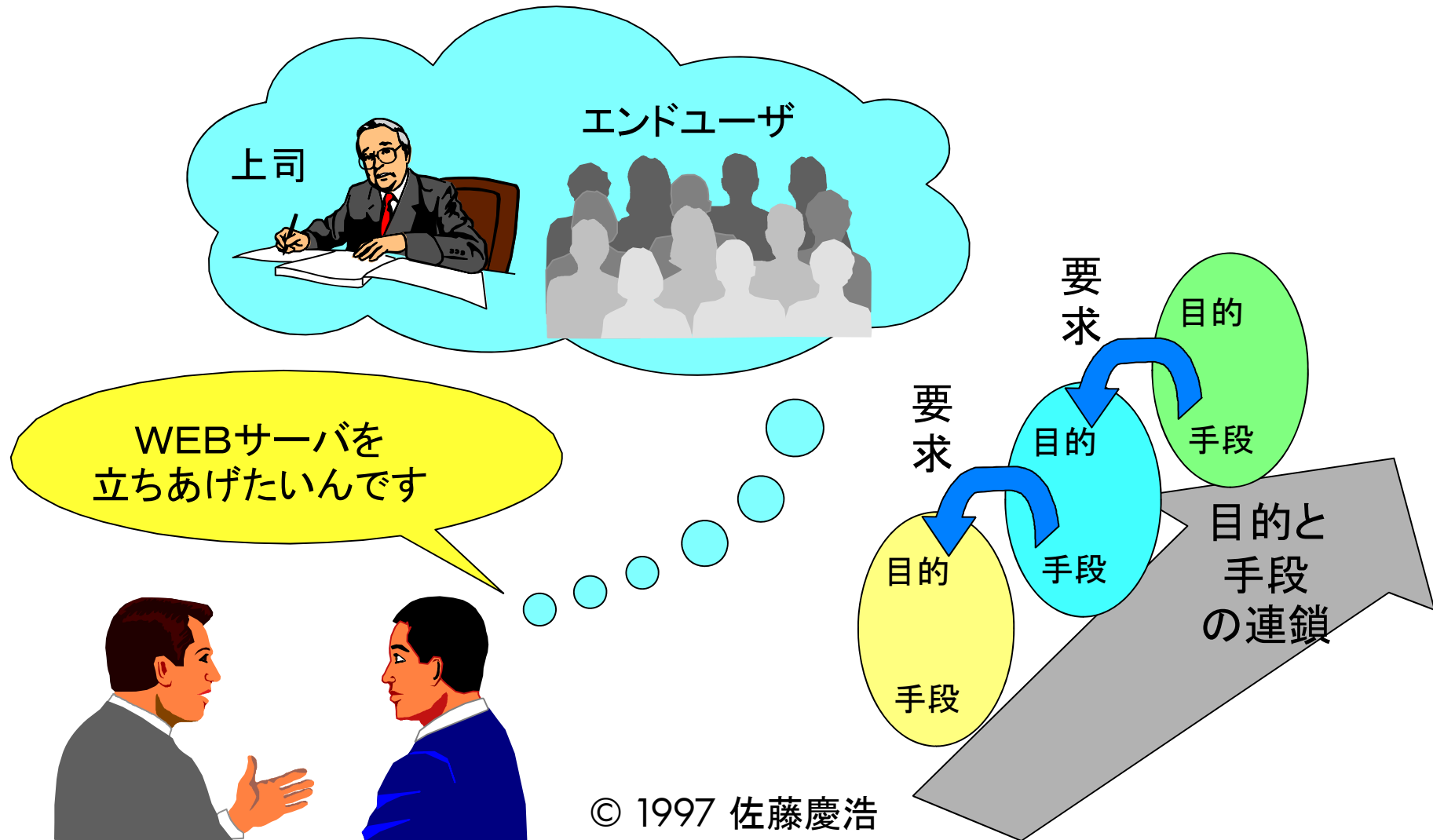
目的: 何らかのサービス提供

手段: 技術の利用

BYODやスマートフォンは手段。それらのセキュリティ対策という言葉は要注意。



プチSoAの薦め(つづき)

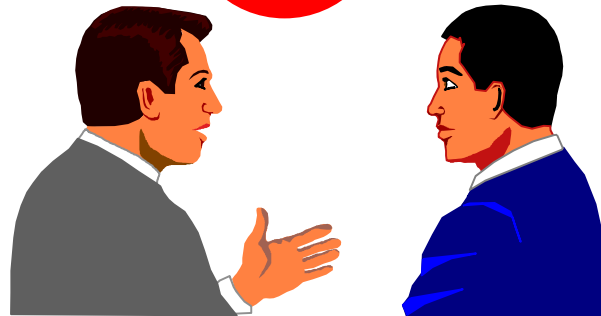


© 1997 佐藤慶浩

プチSoAの薦め(つづき)

スマートフォンを
使いたいです。

スマートフォンの
セキュリティ対策は・・・



プチSoAの薦め(つづき)



設計の考え方

組織としてどのようなIT環境を構築するのか、どのようなITサービスを提供するのかについての方針＝IT戦略に基づいて、ITシステムの構築を目的として実施する。
その中で、必要な情報セキュリティ対策を要件として実施する。



プチSoA と **プチEA** の薦め

SoA: Service oriented Architecture
EA: Enterprise Architecture

プチEAの薦め:チェックポイント例

情報は活用するためにある

情報セキュリティ偏重の過度の情報保護は禁物
情報活用が、企業における情報保持の目的
情報保護は、目的達成のための条件であり義務であるが、目的ではない
情報活用と情報保護のバランスをはかる情報セキュリティ施策とすべき

ビジネスに貢献しない施策は要注意

コンプライアンス施策をROIで考えてはいけない
IT施策におけるTCO削減は避けれない
ビジネスに貢献するような、IT施策でなければ実効性は高まらない
セキュリティ対策のひとつは単純化。単純化はコスト低減になるはず
逆にコスト低減になっていないということは、複雑化をもたらしている危険信号
ITの最適化計画の中でコンプライアンス施策を設計し、業務に組み込むべき



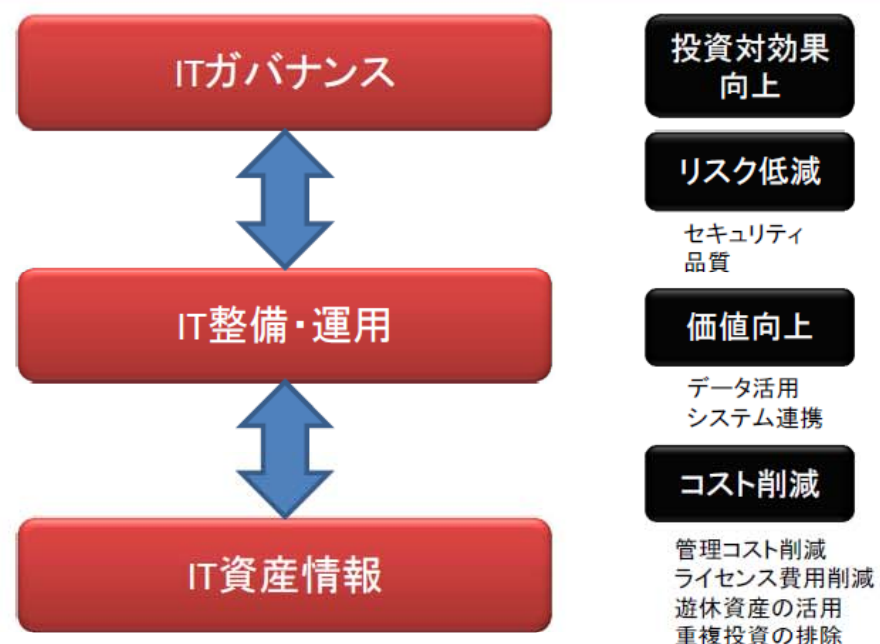
(参考) 政府情報システム棚卸しの基本コンセプト

資料2
(参考資料)

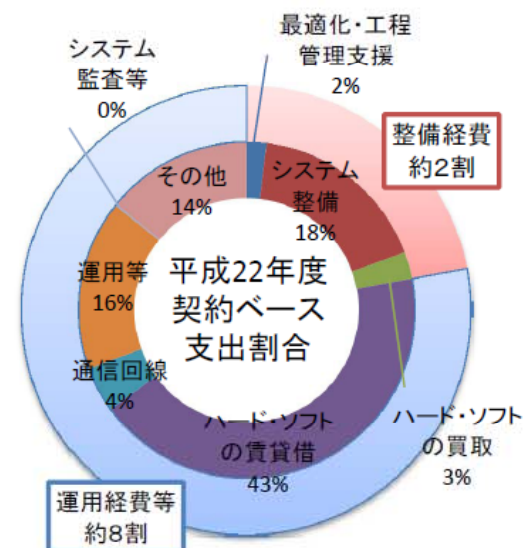
政府情報システムの棚卸し

情報システムのライフサイクルからコスト発生源を追究し、無駄かつ非効率な情報システム・IT投資を徹底的に排除するとともに、電子政府を戦略的に整備・運用していくための情報基盤として活用することが重要。

統一的かつ戦略的な資産管理スキーム



コスト構造

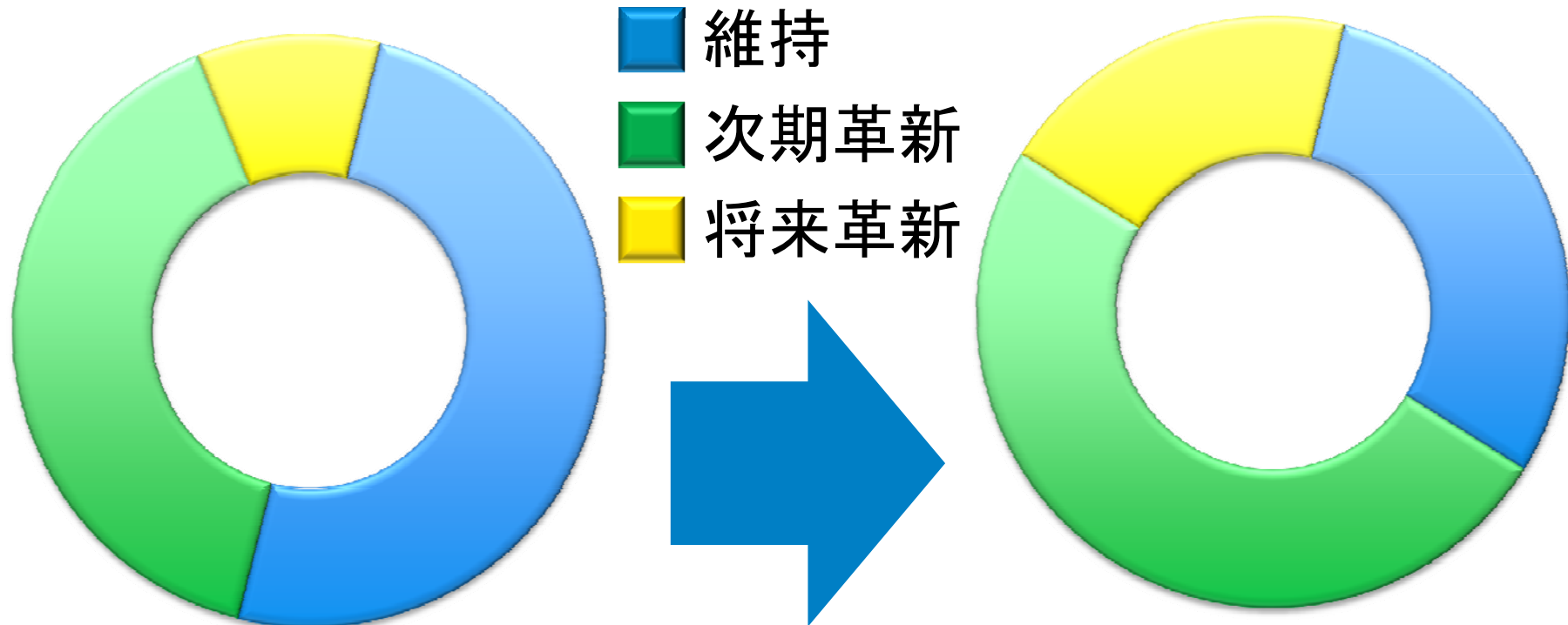


出典: 第46回 各府省情報化統括責任者(CIO)連絡会議

<http://www.kantei.go.jp/jp/singi/it2/cio/dai46/46gijisidai.html>

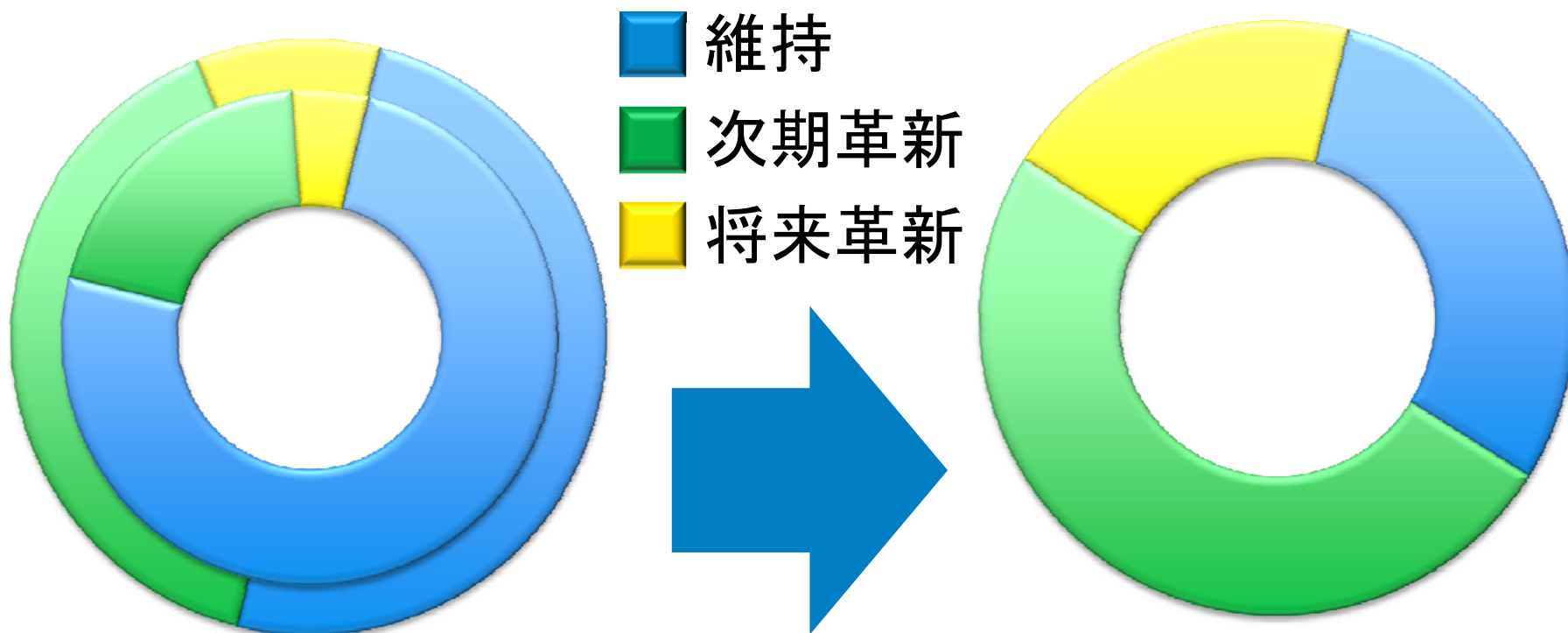
プチEAの薦め：投資プランニング（例）

革新のための投資を確保する必要がある。



プチEAの薦め：投資プランニング（例）

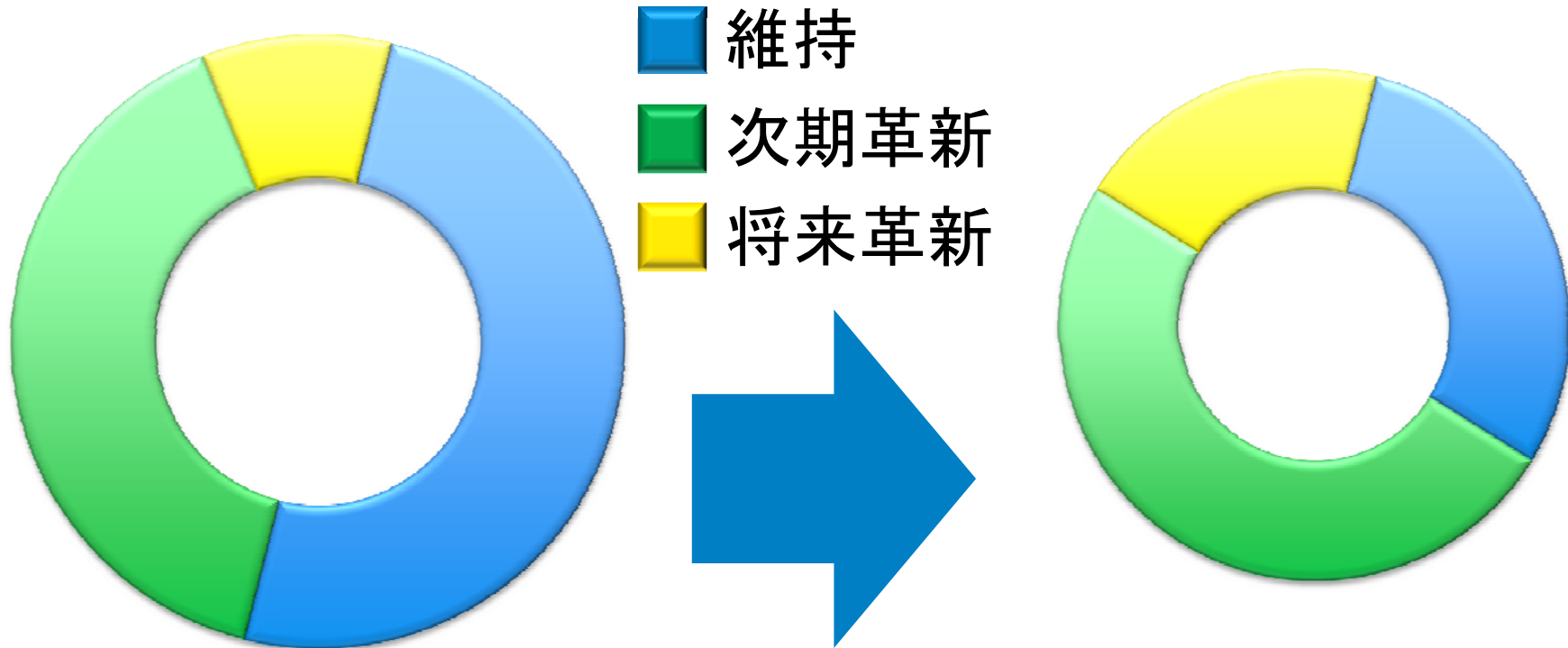
全体予算が削減される中で、
革新のための投資を確保する必要がある。



プチEAの薦め：投資プランニング（例）

（例）将来革新予算は、緊急措置の費用と兼用する

全体予算が削減される中で、
革新のための投資を確保する必要がある。



プチEAの薦め:チェックポイント例(つづき)

守れるルールだけが、守られる。

必ず遵守できるルールだけを設けて、「ルールはすべて守るものである」という意識を定着させることが、結果的に企業の内部統制レベルを向上することができる。
できることの他に、できれば望ましいようなルールを混在させて、「ルールは必ずしも守らなくても良い」という意識を持たれることは好ましくない。
具体的な遵守方法が十分検討されていないようなルールを設けることは論外。
ビジネスの要求に即したバランスを保つ、事前合意されたルールを設けることが重要。

性善説を前提。性悪説も想定。

性善説を前提とする。その上で、性悪説についても想定する。ことが重要。
性善説であれば、「ルールは守られる」というところから検討し始めることができる。
性悪説への対策は、ルールを守っている性善説の人達によって実施する。しかない。

プチEAの薦め:チェックポイント例(つづき)

守れるルールだけが、守られる。

- BYODを許可します。
- IT部門以外による無線LAN環境の構築を禁止します。
→WiFiルータ、WiFiテザリングは禁止です。



- MMS(Managed Mobile Service)の利用を許可します。
- 館内では、Mobile-Netに接続して利用してください。

プチEAの薦め:

ご紹介したモバイル環境の運用を支える
弊社EAの共通基盤コンポーネント

- Enterprise Directory
- Authorization Server
- Self Service Manager
- Solution Center
- Adaptive Network Architecture

これらが既存であることにより、MMS(Managed Mobile Service)とMobile-Netの構築費用は、極僅かでしかない。



まとめ



まとめ

組織としてどのようなIT環境を構築するのか、どのようなITサービスを提供するのかについての方針＝IT戦略に基づいて、ITシステムの構築を目的として実施する。
その中で、必要な情報セキュリティ対策を要件として実施する。



プチSoAとプチEAの薦め

SoA: Service oriented Architecture
EA: Enterprise Architecture

発表資料のダウンロードと 録音の掲載

[http://yoshihiro.com/
speech/#2012-06-07](http://yoshihiro.com/speech/#2012-06-07)

お問い合わせ

twitter

<http://twitter.com/4416sato>

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

