クラウドやスマホとの付き合い方

山口英
奈良先端科学技術大学院大学
情報科学研究科

概要

- クラウドに代表される、大きく変わる情報処理環境に対応した情報セキュリティ管理の概要と方向性、さらに中小企業に求められる導入と運用のポイントについて述べる。

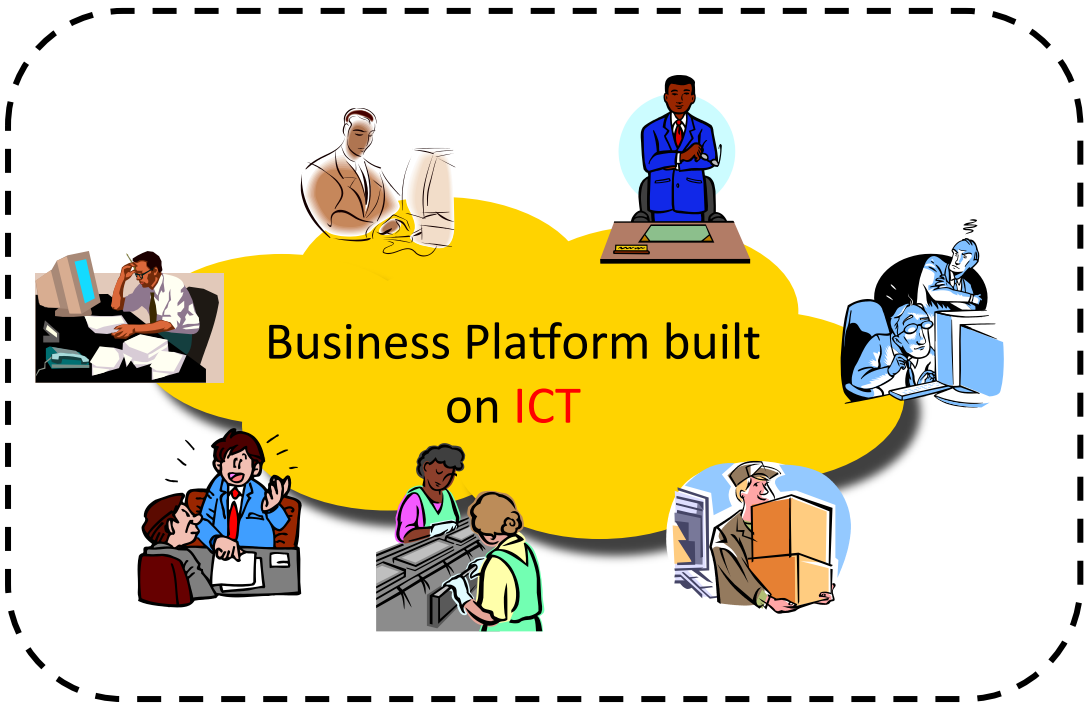
新しい情報処理スタイル

- クラウドコンピューティング (Cloud Computing)
  - ユーティリティ化された情報処理の活用
  - TCO削減がメリット

- BYOD / Bring Your Own Device
  - 個人が持つ情報処理デバイスを業務で使用
  - 境界防衛モデル (perimeter defense model) から、新たな管理モデルへの移行

仮想化技術と CLOUD COMPUTING

Business processes and ICT



Implementation of businesses on ICT platforms = visualization of business “know-how”

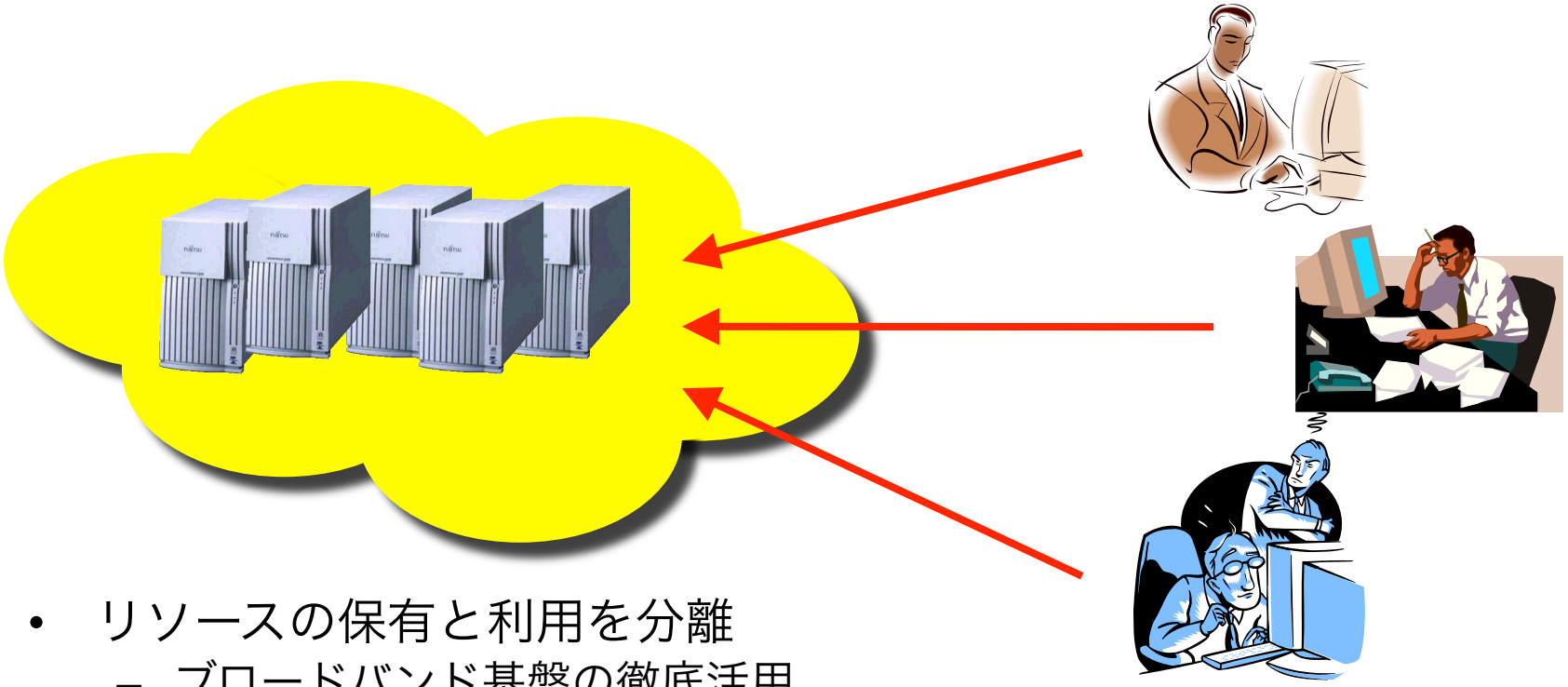
情報処理基盤の整備

- リソースを自己保有
  - 管理ポリシ適用の徹底
  - リソースの追加拡張、ソフトウェアの導入更新の実施が大変
- 運用コスト (TCO) の圧縮と品質の高い運用が常に課題
  - 専門家による運用が期待される
  - IT基盤はどんな業務にも必要になる

TCOの増大

- 管理対象の増大
- BCPと機能＆データのバックアップ
- Sustainable infrastructure
- Robust & Resilient infrastructure
- ソフトウェアのライセンス管理
- 各業務に対応したアプリケーション開発
- ログ記録と管理、さらには解析機能
- 監査基盤の構築と実施
- 情報システムの専門家確保
- 情報セキュリティ管理
- サービス構築専門家の育成と確保

クラウドコンピューティング

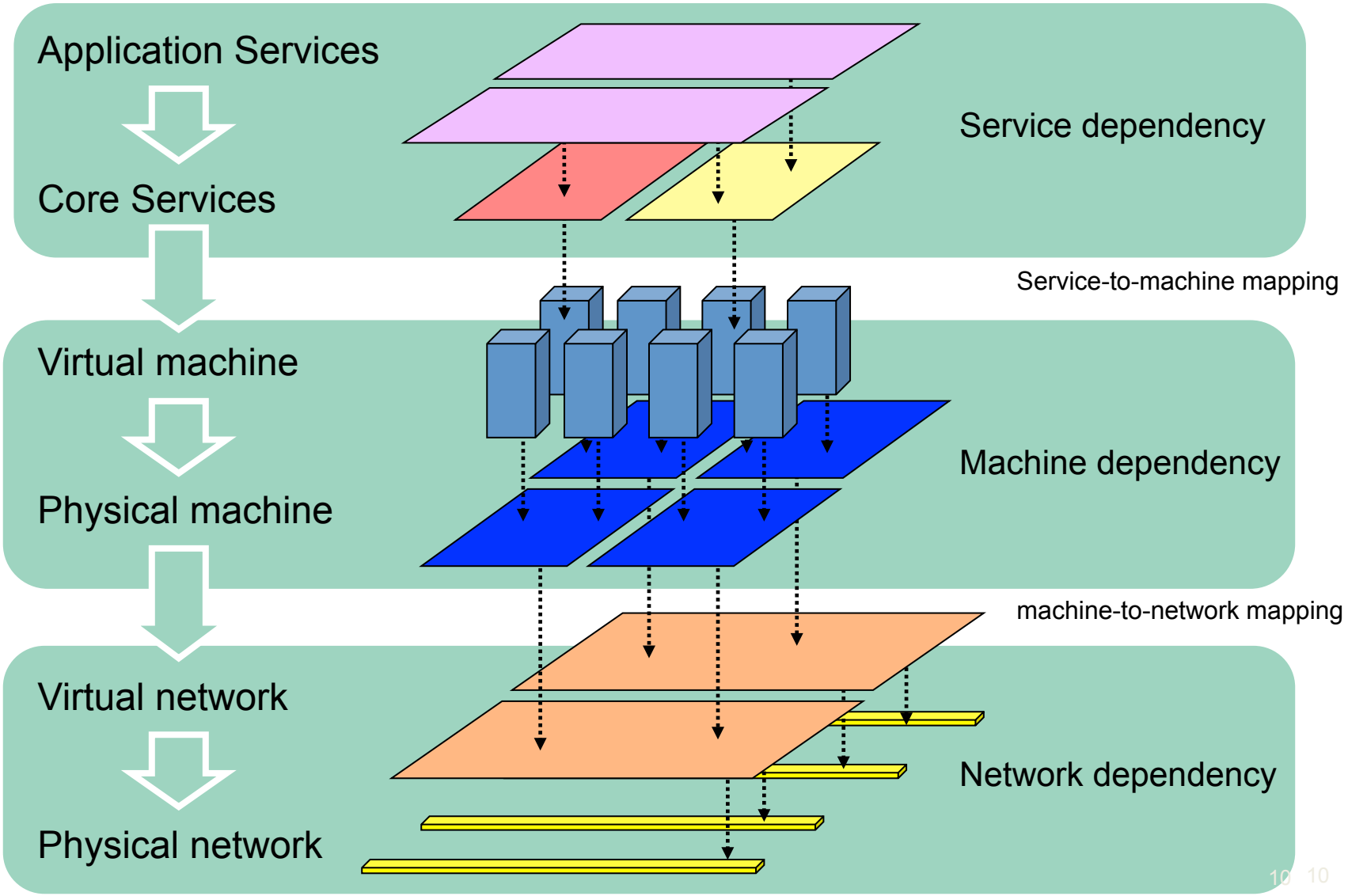


- リソースの保有と利用を分離
  - ブロードバンド基盤の徹底活用
  - 保有と管理のアウトソース
  - 複数のカスタマによる共有で、コスト圧縮をはかる
- ところがこれ以上のメリットを発見

Key Elements

- Virtualization（仮想化技術）
  - Optimization of resource usage
  - From exclusive assignment to shared assignment
- Off-site processing / storage（情報処理の集中化）
  - Professional management
  - On time basis of resource assignment
  - Robust & Resilient system operation are in the hand of operators.
- Open Innovation（オープン性）
  - Mainly by industries.
  - Less risk of “discontinue” incident.

Components in Information System



Cloud Computing の種類

- ネットワークを介してサービスを利用する
- サービスは大きく分けて三種類
  - Software (SaaS)
    - ASP
  - Platform (PaaS)
    - 開発環境
  - Infrastructure (IaaS)
    - 仮想マシンそのもの

Cloud Computing - 新しいインフラ

- 知見の積極的な注入/専門性の向上
  - 専門家の知見の展開が簡単に実施できる
  - 知恵と知見の集約によるインテリジェント化を達成
  - より洗練された機能提供
- 統合管理 (integrated management)
- 計測性を確保し「みえる化」を推進 (measurable infra.)
- 相互接続 (interconnected)
- 他者による利用を想定
  - Openな基盤構成
  - セキュリティ機能を強化した状態でのユーティリティ化
- 資源制限への調整機能と最適化
  - 代表的なものはグリーン機能
  - 仮想化 (virtualization) の活用が積極的
- 耐故障性能の高さ
  - クラスタ構成によるバックアップ構成

数多くのメリット

- データ処理の移動性を確保できる
  - 処理(process)とデータのシステム間転送が可能
    - Process migration
  - 物理的・地理的な分散が可能になる
  - 新たな分散処理基盤の構築と実装が可能
- On-demand resource assignment
  - 処理に必要な資源を動的に割り当てることができる
  - 処理の最適化
  - 夢の「適時適切な資源割り当て」

セキュリティ管理は頭痛の種

- クラウドコンピューティングは、相互接続とユーティリティ化の進化形
- 相互接続とユーティリティ化は、既存の境界防衛モデル (perimeter defense model) を崩壊させる
  - 内と外の区別が付けられない
- Cloud Computing サービス事業者とリスクを共有
  - CCSP もリスクの一つ

- ユーティリティ化の中で “trust” の概念再構築が必要
  - Trust chain は現実的な規模拡張性を持つのか?
- 基盤化の中で robust & resilient system が求められる
  - 従来、情報セキュリティでは余り考えられてこなかった。
  - “all hands” solution を考える必要が有る

拡張性が課題

- Cloud Computing に特有の課題
- どれだけの構成要素を管理するのか?
- データとプロセスの移転をどのように実装するのか?
- サービス停止時間をどのように最小化するか?
- システムログとセンサデータをどのように活用するのか?
- どれだけの資源をこの事業に割り当てることができるのか?

ベンダー・ロックイン

- 一度 cloud computing サービスを使い始めた後
  - データを引き上げることができない
  - 同種の他サービスへ移行することができない
  - 特定のデータフォーマットになってしまい、特定のサービスでしか使えない
- 特定ベンダのサービスに閉じ込められてしまう
- “Vendor Lock-in”

CSPのモラルハザード

- CSPは本当に適正に投資をするのか?
  - 構築したサービスプラットフォームから日銭が上がる
  - できれば投資を圧縮して利益率を上げたい
  - 仮想化技術によって圧縮した投資ができる
  - しかも契約では責任を回避するための条項が満載

- CSPは本当に適正な管理をするのか?
  - 仮想化していることによって、実は管理の不可視性が上がっている。
  - 適正な管理をしていなくても利用者には分からない

ここまでのまとめ

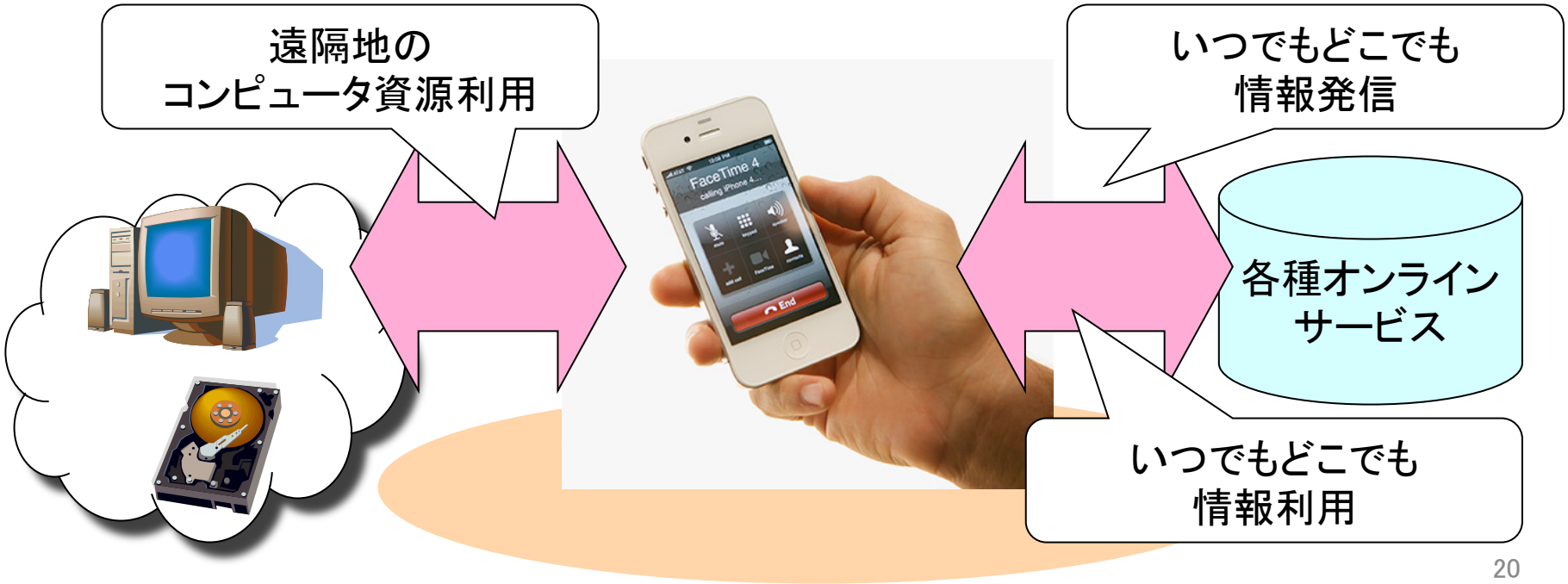
- Cloud computing は、情報処理機能の「保有」から「利用」への転換を図る機構
  - 他者の知見を活用する
  - 具体的な情報処理に対する知見だけではなく、システム運用の知見を活用する事も可能

- 運用のプロフェッショナルの知見を活用
  - 巨大システム
  - セキュリティ管理
  - BCP & Disaster Recovery Management (DRM)

BYOD: BRING YOUR OWN DEVICE

スマートフォンの利用モデル

- 携帯性、通信機能を活用したさまざまな利用
  - ネットワーク上のサービスとの連携
  - ネットワーク上の資源利用

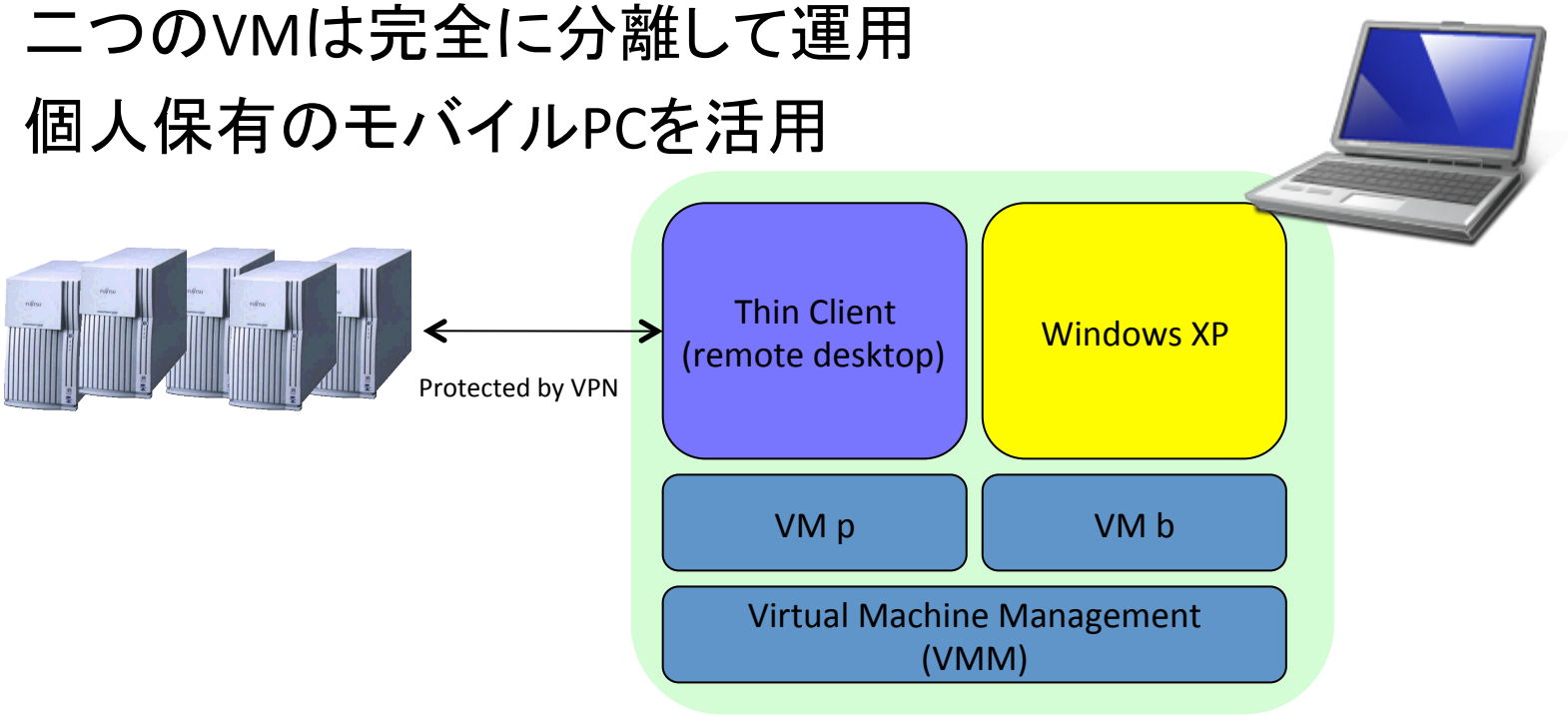


各OSの比較

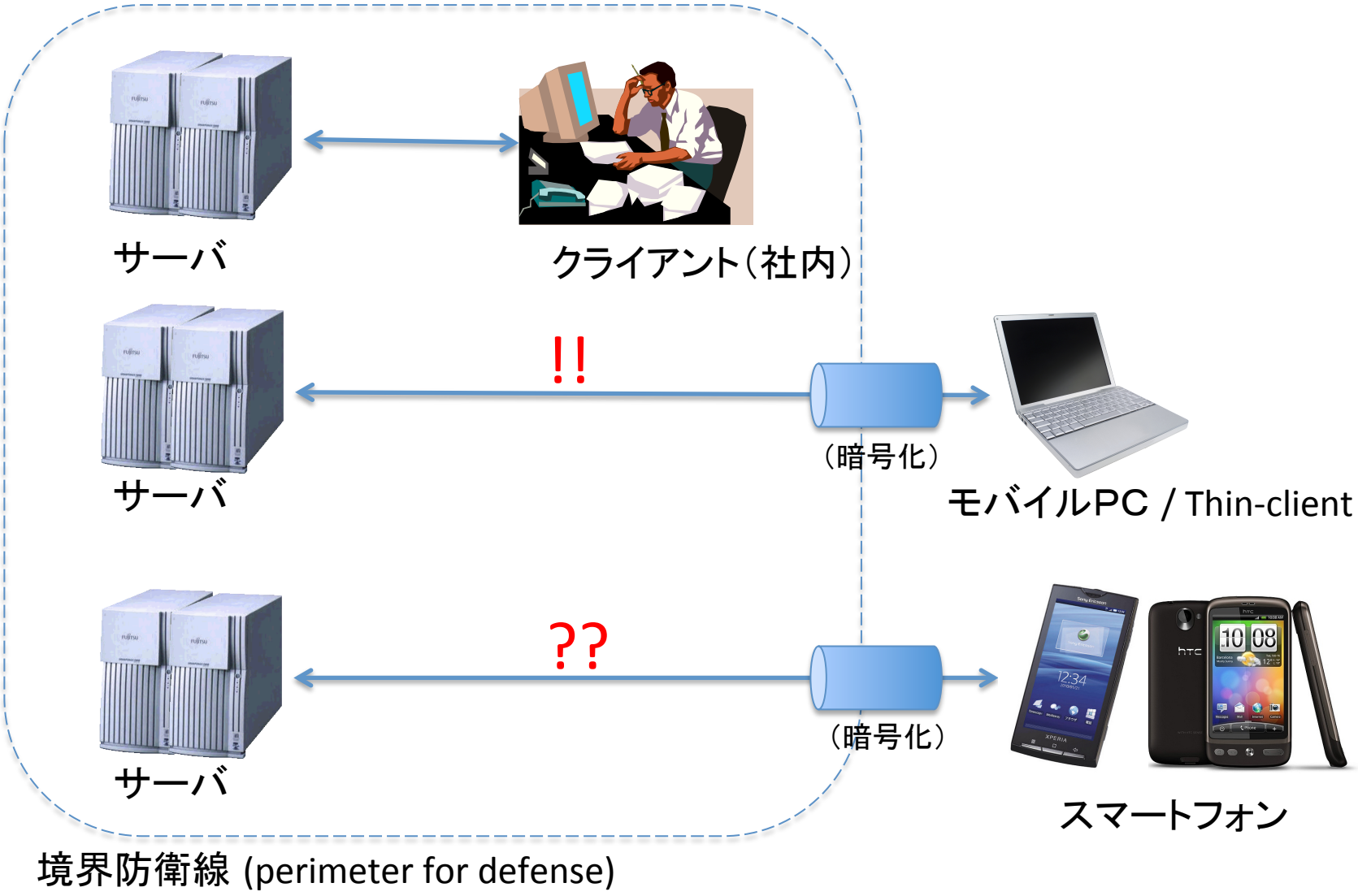
	Windows7	iOS	Android
対応CPU	x86	ARM	ARM
OSカーネル	MinWin (NT)	Darwin (Mach3.0 + FreeBSD)	Linux-2.6ベース
ユーザモデル	マルチユーザ	シングルユーザ	シングルユーザ
プロセス管理	マルチタスク	シングルタスク （バックグラウンドプロセス）	マルチタスク
認証	パスワード その他拡張に対応 (トークン, 生体認証など)	パスワード, 暗証番号	パスワード, 暗証番号
セキュリティ	暗号化, ファイアウォール …	鍵管理, 暗号化 遠隔データ管理	鍵管理, 暗号化 遠隔データ管理
ネットワーク	TCP/IPv4,IPv6	TCP/IPv5,IPv6 IPSec, L2TP, PPTP	TCP/IPv4,IPv6
通信IF	各種通信機器に対応 (3G, WiFi, Bluetoothなど)	3G/GSM, 802.11b/g/n, Bluetooth	3G/GSM, 802.11b/g/n, Bluetooth

モバイルPCでの安全対策

- “BYO” (bring your own) 方式によるコスト削減
  - VMM は二つの仮想システムを提供する
    - 一つがビジネス用の thin client (あるいは remote desktop)、もう一つが各ユーザの私的利用空間
  - 二つのVMは完全に分離して運用
  - 個人保有のモバイルPCを活用



ビジネスシステムの変遷

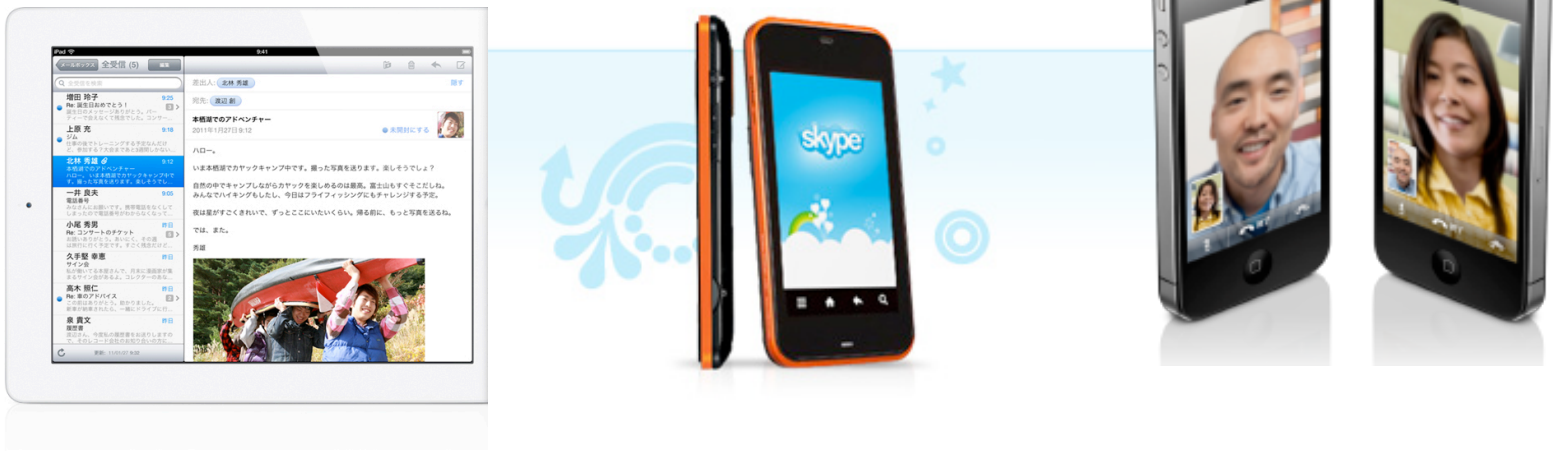


3つの利用形態

- Communication
  - 電子メール
  - メッセージサービス, 音声通話, テレビ会議システム等へのアクセス
- Data access
  - ビジネスシステム内のデータへのアクセス
  - 例えば、在宅勤務時のリモートデスクトップ機能や、ファイル共有機能など
- Data process
  - ビジネスシステムと連動して、何らかのデータ処理を行う情報処理装置
  - 例えば、POSシステムの一部として、モバイルPCを活用する

“Rich” Communication

- 実現は最も簡単
- 電子メール, チャットなどのコミュニケーション・ツールは当然利用できる
  - 情報漏洩リスクを、どのようにして低減しているのかが鍵
- より高度なコミュニケーション・ツールの展開
  - “FaceTime” for iPhone / iPad
  - Skype on Android terminals.

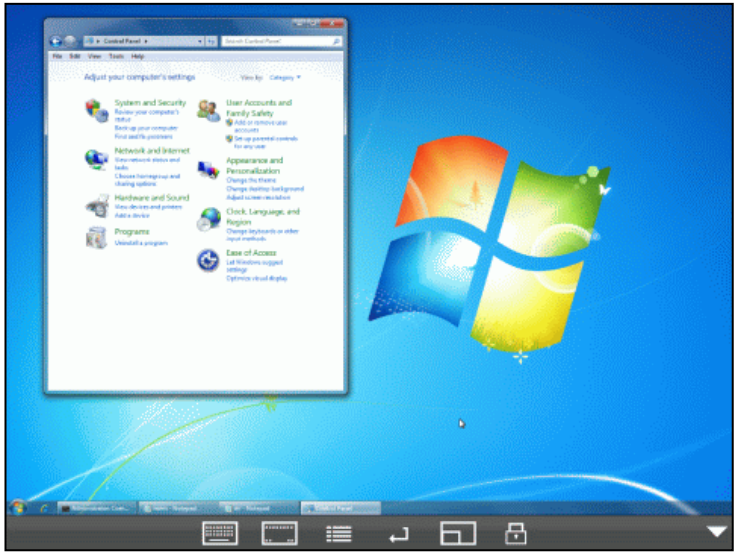


Data Access

- 実現はやや難しい
  - 境界防衛線を越えてのデータアクセスは、常に情報漏洩リスクを内包する
    - 特に、端末の紛失・盗難リスクをどのように取り扱うのか
- 二つの形態
  - Thin-client 方式
    - 直接的なデータアクセスは、境界防衛線内で行われる
    - セキュリティ対策としては高度で有効な対応
  - モバイルPC方式
    - 直接的なデータアクセスは、モバイルノードで行われる
    - モバイルPCにおけるセキュリティ対策が鍵

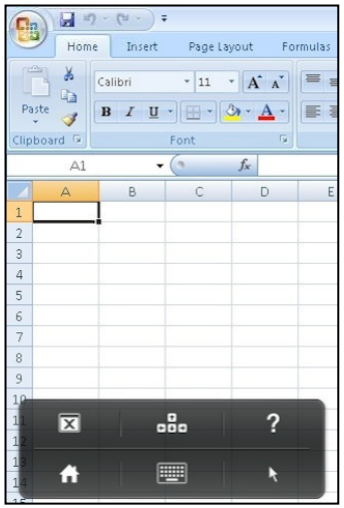
リモートデスクトップ

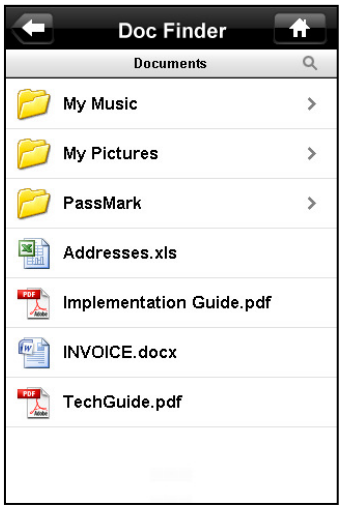
- 遠隔からのPC操作
  - VNC/Windows RDP/PCoverIP対応クライアント
  - 仮想マシンや実マシンなどを遠隔操作
  - 多数のアプリが存在

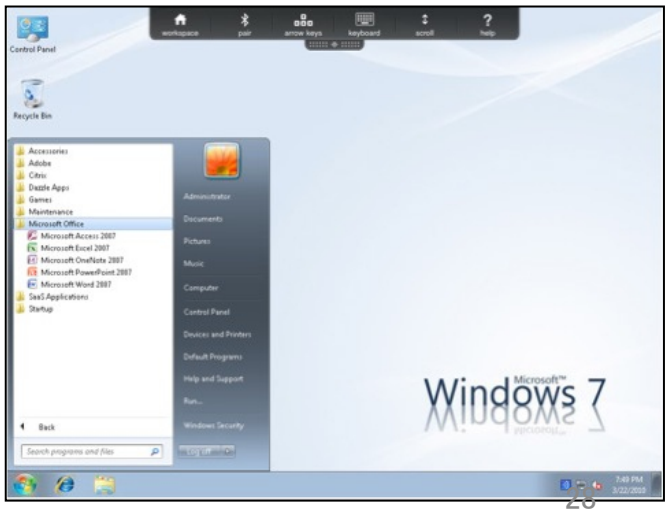


Citrix Receiver

- 仮想マシン上のアプリケーション操作アプリ
  - Citrix社のXenApp環境に対応
  - アプリケーション操作とファイル送受信







Dropbox

- クラウド上のファイルストレージ利用アプリ
  - オンラインストレージの利用
  - オンラインストレージを介したファイル同期

在宅勤務での利用提案

- 在宅勤務の手段としてのスマートフォン利用
  - 仮想マシンとリモートデスクトップの組み合わせ
  - 「PC環境」を提供するサービス
  - 節電、BCPを目的として各SIより提案
  - スマートフォンをインターフェイスとして利用

例: ソフトバンクテレコム
「ホワイトクラウドデスクトップサービス」

Data Process

- 実現が最も難しい
- ビジネスシステムに直結した情報処理を、モバイルPC・スマートフォンで行う
  - 強力なセキュリティ対策が必須
  - ビジネスプロセスの構築、改良が必須
  - 場合によっては、特別なデバイスの取り付けが必要になることもある
- スマートフォン特有の『アプリケーション』の役割を活かせるかどうかは、より積極的なBPRが必須

iPad利用POSレジ

- ユビレジ社が提供するPOSレジサービス
  - 月額5000円のSaaS型POSレジ
  - iPadにて利用するソフトウェアレジ
  - 安価かつカスタマイズ性の高さ、強力な集計

導入時に必要になること (1)

- ビジネスプロセスの明確化と改良は必須
  - 改めて「仕事はどのように行うのか」を考える
    - オフィスに居ない状況での職務執行を冷静に考える
    - オフィスでなければ出来ない業務も沢山ある
    - 勤怠管理、執務管理、ワークロード管理も必要
  - セキュリティ管理の観点から、再点検と改良が求められる
    - 情報漏洩リスクへの対応、特に個人情報保護
    - 暗号化の積極的な利用
- モバイルPC・スマートフォン利用による効果測定をどのようにするのか
  - システムを導入したけど、実際に効果が上がってなければ単なるおもちゃにしかならない
  - 何を見ると効果と言えるかを、組織で合意することが必須

導入時に必要となること (2)

- 特定の業務のためのアプリケーション開発が求められる時もある
  - アプリケーション = 外部の第三者によるビジネスシステム利用を、安全かつ管理された状態での利用を実現する仕掛け
    - 具体的な処理プロセスの詳細を利用者から隠すことができる
    - ブラウザ等の他のコンポーネントへの依存度を減らす
  - 開発コストは十分考える必要が有る

- とりあえず「在宅勤務」環境の構築を考えてみる
  - 技術、運用、制度

ここまでのまとめ

- モバイルPC・スマートフォンをビジネス環境でも導入することは可能であり、実際に効果を上げ始めている
  - セキュリティ対策を合理的かつ十分に行うことが必要
  - 「何をするのか」の明確化が一番の課題
  - 在宅勤務を想定して検討するのが簡単なアプローチ

- より多くの知見共有が必要
  - 個人情報保護法施行以来、わが国ではモバイルPCの利用が激減してしまった
    - どのようにリスクを低減しているのか
  - 広く日本国全体でみると、企業環境でのモバイルPC利用についての知見が十分蓄積・活用はされていない

Summary - 付き合い方のヒント

- クラウドコンピューティング
  - TCO削減以上のメリットが現実にある
  - ベンダロックインには注意を払う
  - 適正なトラブル対応がされるかが鍵

- BYOD
  - どのような業務で使うのか、ビジネスプロセスを明らかにすることが大切
  - “step by step” アプローチが大切