スマートフォンセキュリティ
シンポジウム　2012

Web時代の脅威と課題

～安心･安全で豊かな生活のために～

平成24年11月21日
(社) 日本スマートフォンセキュリティ協会 会長
東京電機大学　未来科学部　学部長
CISSP　安田　浩

yasuda@mpeg.im.dendai.ac.jp
www.mpeg.im.dendai.ac.jp

講 演 概 要

新しい脅威とは何か

なぜ逃げられないのか　メディア社会への基盤整備と対処策

ＷＥＢ戦国時代　日本の危機

ＷＥＢ時代の完成　プラットフォームクラウド

脅威への対応

ＢＩＯＳ対策

新しい環境には新しいやり方を　ＢＹＯＤ

まとめ

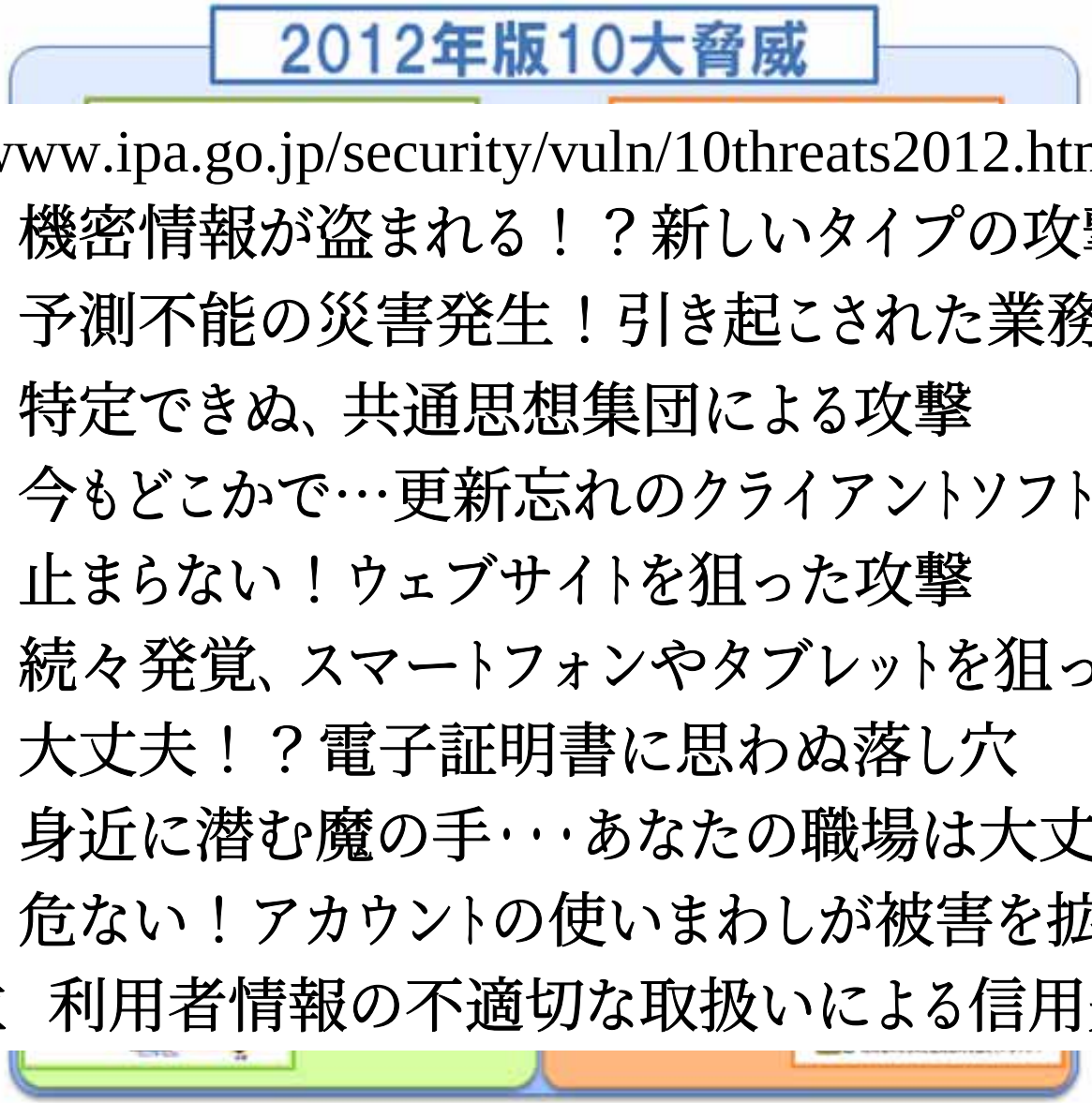
新しい脅威とは何か

古くて新しい脅威

BIOS

BYOD

2012版10大脅威 by IPA



http://www.ipa.go.jp/security/vuln/10threats2012.html

第1位 機密情報が盗まれる！？新しいタイプの攻撃

第2位 予測不能の災害発生！引き起こされた業務停止

第3位 特定できぬ、共通思想集団による攻撃

第4位 今もどこかで…更新忘れのクライアントソフトを狙った攻撃

第5位 止まらない！ウェブサイトを狙った攻撃

第6位 続々発覚、スマートフォンやタブレットを狙った攻撃

第7位 大丈夫！？電子証明書に思わぬ落し穴

第8位 身近に潜む魔の手・・・あなたの職場は大丈夫？

第9位 危ない！アカウントの使いまわしが被害を拡大！

第10位 利用者情報の不適切な取扱いによる信用失墜

【事例集】

No	発生時期	概要	目的	想定される攻撃手法
1	2003年8月	米鉄道会社のCSXは、同社のネットワークが2003年8月20日早朝(現地時間)、ウイルス感染によってダウン、一部列車の運行に障害が発生したと発表した。この影響で、旅客列車や貨物列車に運休や遅れが生じ、首都ワシントンD.C.でも通勤列車に影響があった。 同社の発表によれば、世界規模で感染を広げているワームに感染したため、としており、W32/BlasterワームW32/Nachiワーム、Sobig.Fに感染した疑いがある。同社では「ウイルス対策を行っていたものの防げなかった」としている。	サイバーテロ	マルウェア 各種脆弱性 セキュリティリスク
2	2008年1月	2008年1月11日、ポーランドで列車の制御システム（Lodz Train System）を14才の少年がテレビのリモコンを改造したものでハッキングした。その結果、列車4台が脱線し12名が負傷する大事故となった。この事故により、フィールドデバイスを含むシステムへの物理的なアクセスコントロールとプロトコルの安全性の強化が必要との認識が高まった。	サイバーテロ	各種脆弱性 セキュリティリスク
3	2011年3月	EMCは、3月17日付の書簡で、同社のセキュリティ部門であるRSAの情報システムがサイバー攻撃を受けて情報が盗まれ、RSA SecurIDの二要素認証製品に関する情報の一部が含まれていたことを公表。ただしその時点では、盗まれた情報によって広範なサイバーの一部としてセキュリティ効果が低下する可能性はあるが、RSA SecurIDの利用者への直接的な攻撃が成功することはないと説明していた。 しかし、米EMCは、社外に漏えいした「RSA SecurID」に関する情報を悪用したサイバー攻撃が5月に発生していたことを公表するとともに、顧客企業への新たな対応として、RSA SecurIDのワンタイムパスワード生成トークンの交換プログラムを実施することなどを発表。	産業スパイ	マルウェア 各種脆弱性 セキュリティリスク
4	2011年5月	ソニーグループのオンラインサービスから合計1億件以上の個人情報が流出した可能性がある事件。ソニートップの経営責任の追及や、ソニーのタブレット端末などネットワーク製品戦略に与える悪影響への懸念など、史上最悪規模の個人情報流出事件のインパクトは大きい。 ＜発生の原因とされる項目＞ ・攻撃されたアプリケーションサーバーの既知の脆弱性をパッチも当てず放置していた ・ハッカーによってサーバーが再起動させられるまで不正アクセスの事実に気付けなかった ・関連会社で漏洩した一部パスワードについては、暗号化（ハッシュ化）を行っていなかった ・セキュリティ担当者の知識不足、体制不備等	産業スパイ	各種脆弱性 セキュリティリスク
5	2011年9月	三菱重工業は19日、翌20日には、IHI(旧石川島播磨重工業)と川崎重工業も、同じくウイルス感染の危機にさらされたことが、報道により明らかになった。 三菱重工業の発表によると、ウイルス感染の可能性が判明したのは8月中旬で、その後、ウイルスの特性により、情報漏えいの危険性もあることがわかった。過去に、社内の一部のコンピューターのシステム情報(ネットワークアドレス等)が流出した可能性はあるが、製品や技術に関する情報の流出は確認されておらず、現時点ではウイルス感染による被害拡大は止まったとしている。	産業スパイ	マルウェア 各種脆弱性 セキュリティリスク
6	2011年11月	総務省は11月4日、調査を実施したところ、同省職員用のPCがトロイの木馬型ウイルスに感染していたと発表した。感染経路は、震災に関連する内容を騙ったメールだった。 ウイルスに感染した23台のPCが何らかの情報を外部に送信したことが確認されているが、情報の内容までは特定できていない。同省は「業務で関わった方の名刺情報などの個人情報、職員やその家族の個人情報、業務上の情報が含まれている可能性がある」としている。	産業スパイ	マルウェア 各種脆弱性 セキュリティリスク
7	2012年7月	財務省が7月20日付で、省内の複数の職員用端末がウィルスに感染し、外部サイトとの通信が行われていたことを発表。 感染台数：123台(財務省 行政情報化LANシステム内で発生)。流出した可能性のある情報（業務上作成した会議資料(二次被害の可能性を考え詳細は非公開。※国税関係の個人情報や防衛関連等の機密情報については本事案とは独立した専用システムであるため情報漏えいの可能性は無し。との事） 尚、これまでの中央省庁の感染報告は以下 2010/11：経済産業省 0台　2011/08：国土交通省四国地方整備局 1台　2011/10：衆議院 32台 2011/11：総務省 23台　2011/11：参議院 31台　2012/01：宇宙航空研究開発機構 1台　2012/02：農林水産省 0台　2012/03：特許庁 3台 2012/05：原子力安全基盤機構 19台　2012/07 財務省 123台	産業スパイ	マルウェア 各種脆弱性 セキュリティリスク

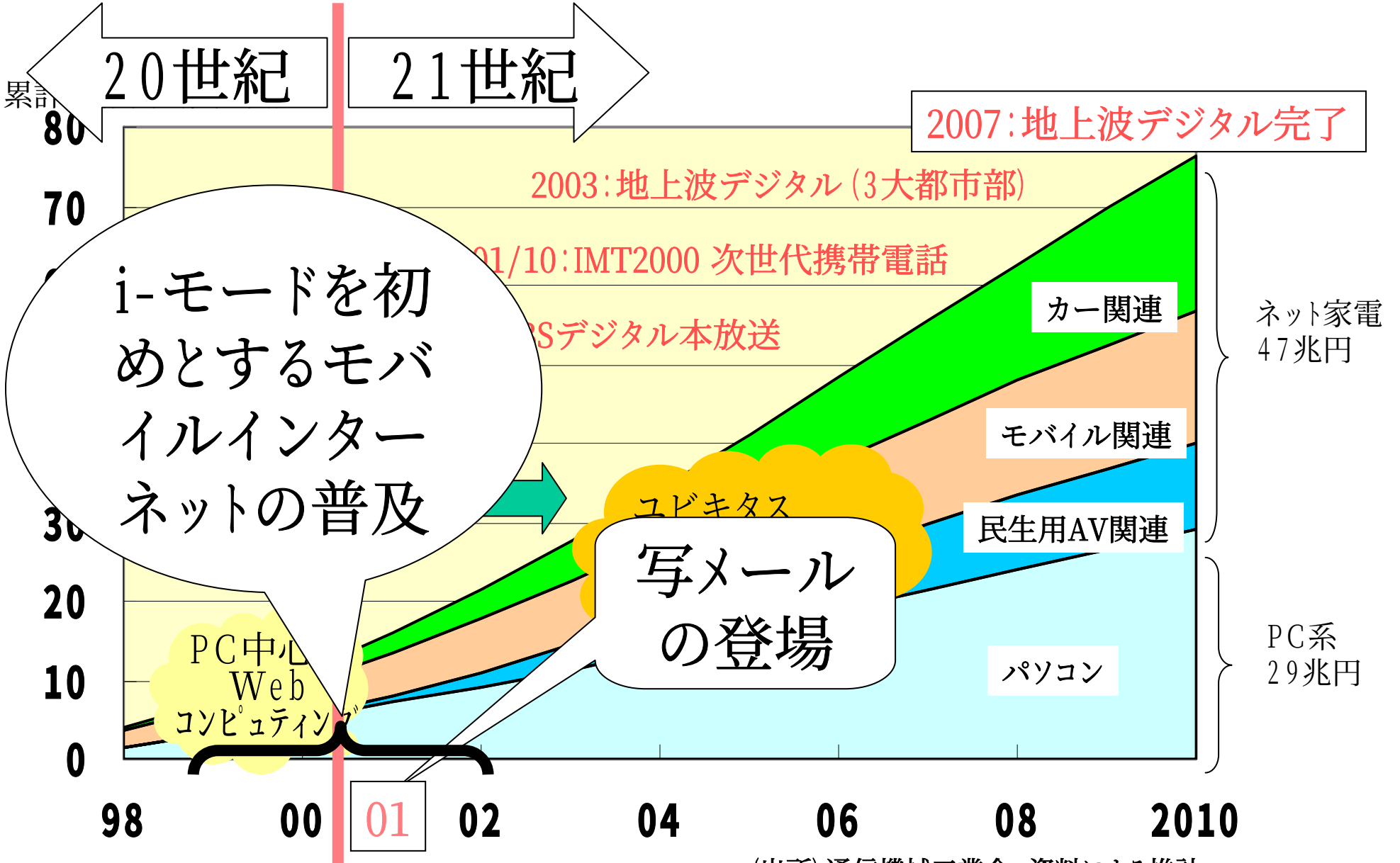
なぜ逃げられないのか

メディア社会の効用と基盤整備と対処策

メディアとは

分類	片方向	双方向
有線	(有線放送 スピーカの ことが多い)	有線電話
無線	無線放送	携帯電話

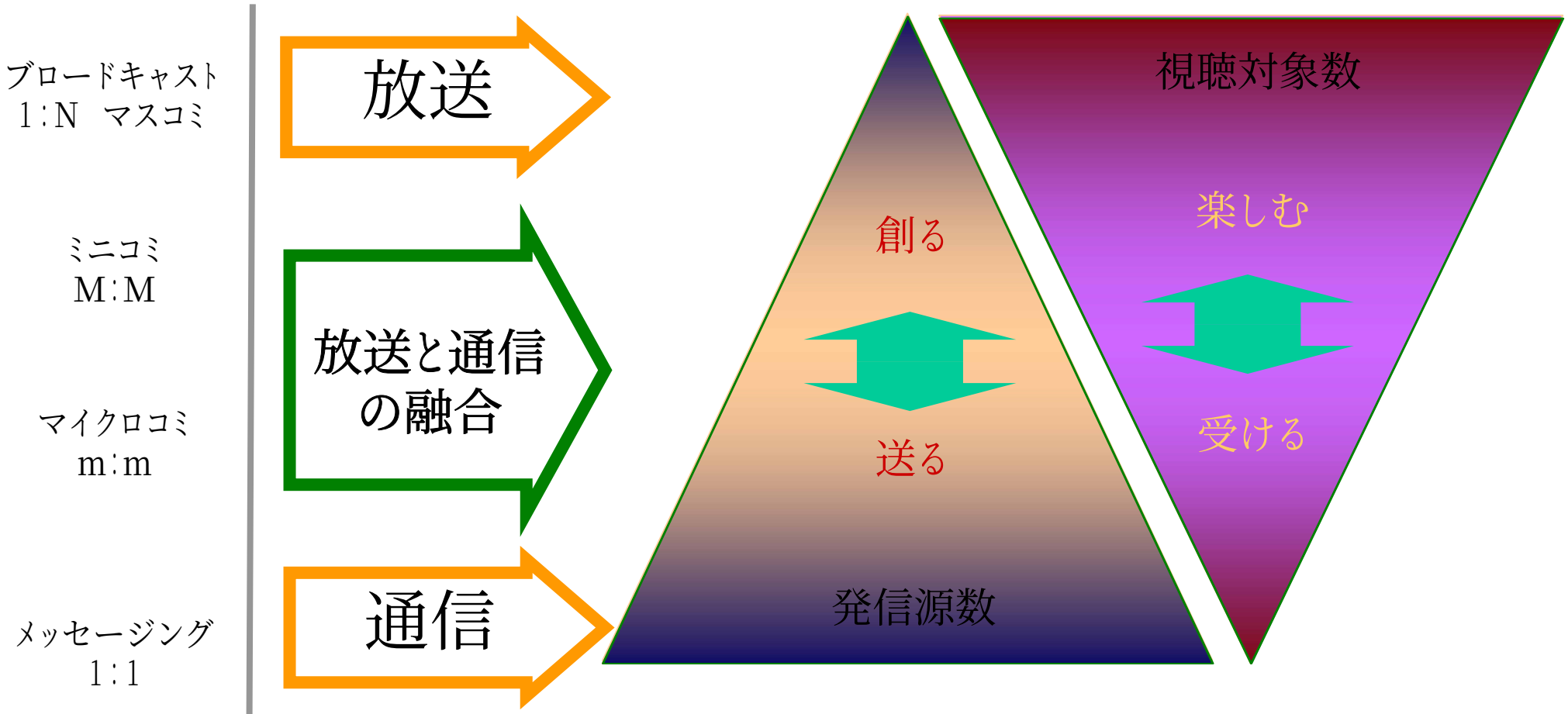
三位一体によるﾌﾞﾛｰﾄﾞﾊﾞﾝﾄﾞ・ユビキタスインフラの完成



(出所) 通信機械工業会、資料による推計

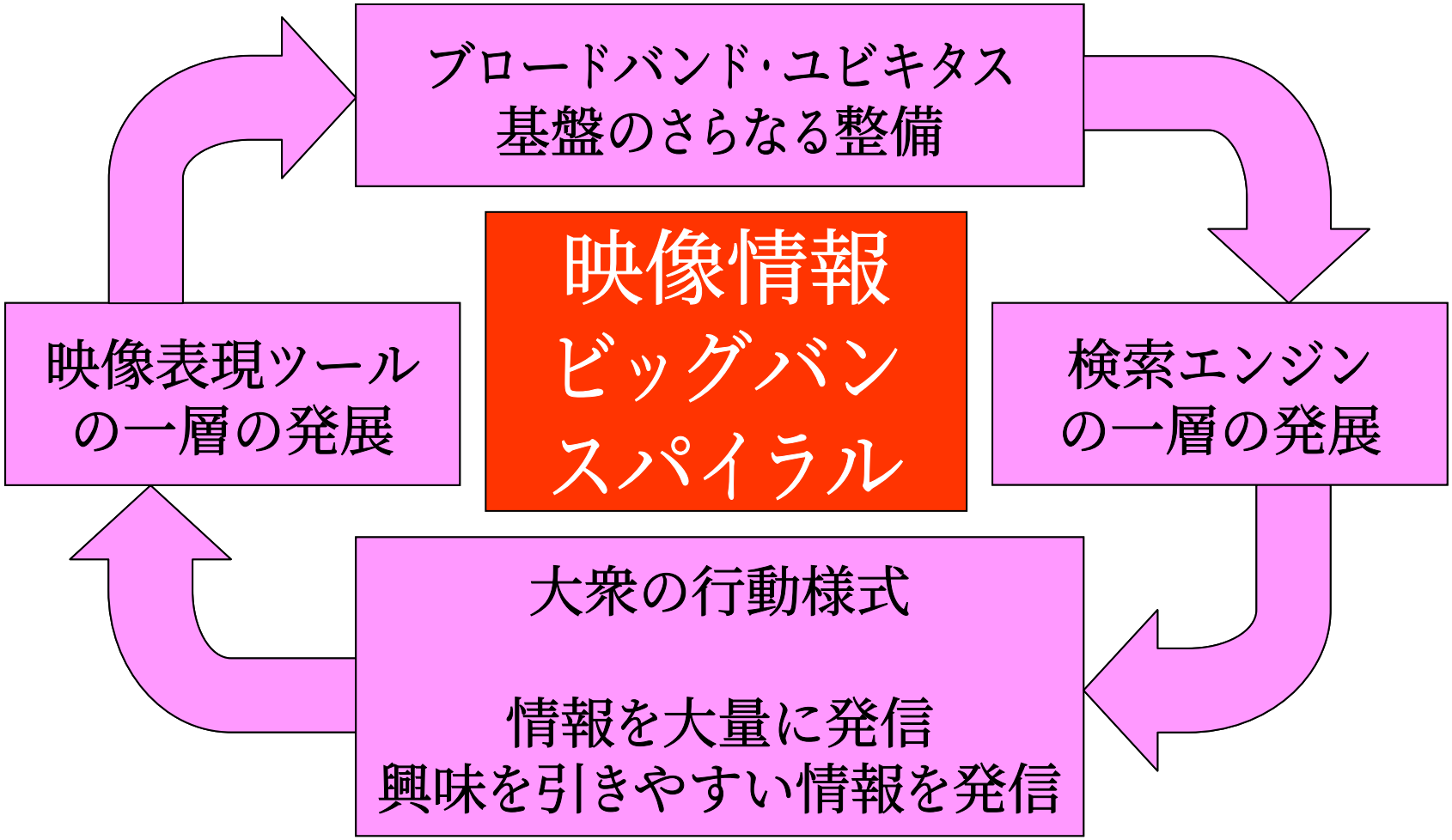
真のコミュニケーションへ

マイクロコミュニティの形成と自己顕示の高揚→ＳＮＳ



尖閣列島で中国漁船
海上保安庁巡視艇に
突っ込んで衝突
外交問題に発展か？

映像情報ビッグバンは必然！



WEB3.0&画像ビッグバンへの対処策

(1) 国内での情報の集積化と迅速なアクセスが必要

(2) グローバルに最新の情報への迅速なアクセスが必要

(3) 収集情報の再利用のための巨大アーカイブが必要

(4) 知識化･理解促進のためにすべてのデバイド解消が必要

(5) 情報の日本文化に整合した効率的理解促進が必要

(6) 個人型検索エンジン･プライベートアーカイブの開発

(7) グローバルな理解を得るための情報発信が必要

(8) 安心安全環境の構築（透明性と匿名性）が必要

(9) 上記を支えるためのNWインフラ･BCI技術が必要

WEB戦国時代
日本のピンチとチャンス

WEBとは

WEB1.0	WEB2.0	WEB3.0
centralized them	distributed us	decentralized me
集中した彼ら	分散する私たち	非集中の私
誰でも放送局	*誰でもコミュニティ*	*どこにも私*
情報提供者が一方的に発信する環境	ユーザ参加型の場（ブログ、SNS）	蓄積された情報と推測を活用すれば瞬間移動術が身につき、時間軸も移動可能か？

WEB3.0は時間移動も可能な *4次元の時代*

記憶拡張機概念誕生とヴァネヴァー・ブッシュ

1945年にブッシュ氏が発表した MEMory EXtender はWEB3.0の基礎概念であった

この概念では

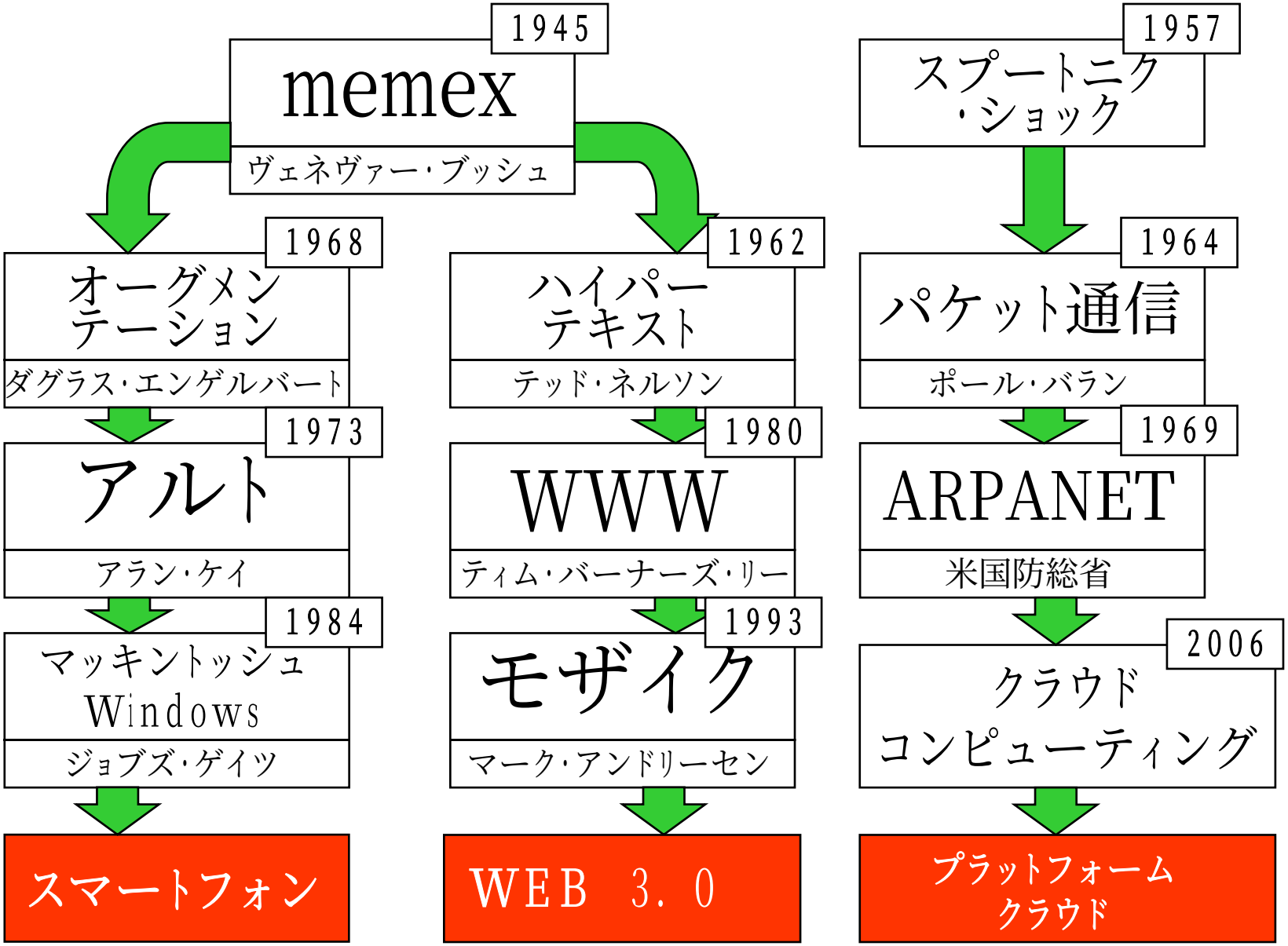
すべての情報は最新化され
情報取得は迅速に行え、相互参照が可能であり
情報の追加･削除･重み付けは自動的に成される

ブッシュ氏は、この概念を「人」を構成要素として実現した

すなわち、各分野の第一人者を自分の部下として

常に最新の情報を持つこと
必要とするときに直ちに提供し、他の分野との関連を示すこと
が何故必要としたかに基づき情報を重み付けしておくこと

マルチメディアの進化の系譜



坪田知巳「2030年メディアのかたち」講談社、2009. 09. 25、p132

WEB3.0を活用するには

スマホ系操作機、検索エンジン、クラウド
が揃えば　WEB3.0は使えるか？

残念ながら、まだ足りません

情報の個人にとっての重み付けを
行う機構が必要です

そのためのプライベートアーカイブが必要です

プライベート・アーカイブとは

ライフログ・
その他プライベート情報

プライベート
アーカイブ

新着情報
の適切な
評価結果

最新入力情報
の信頼性評価
エンジン

友人情報
(信頼情報)

複数検索
エンジンから
の情報

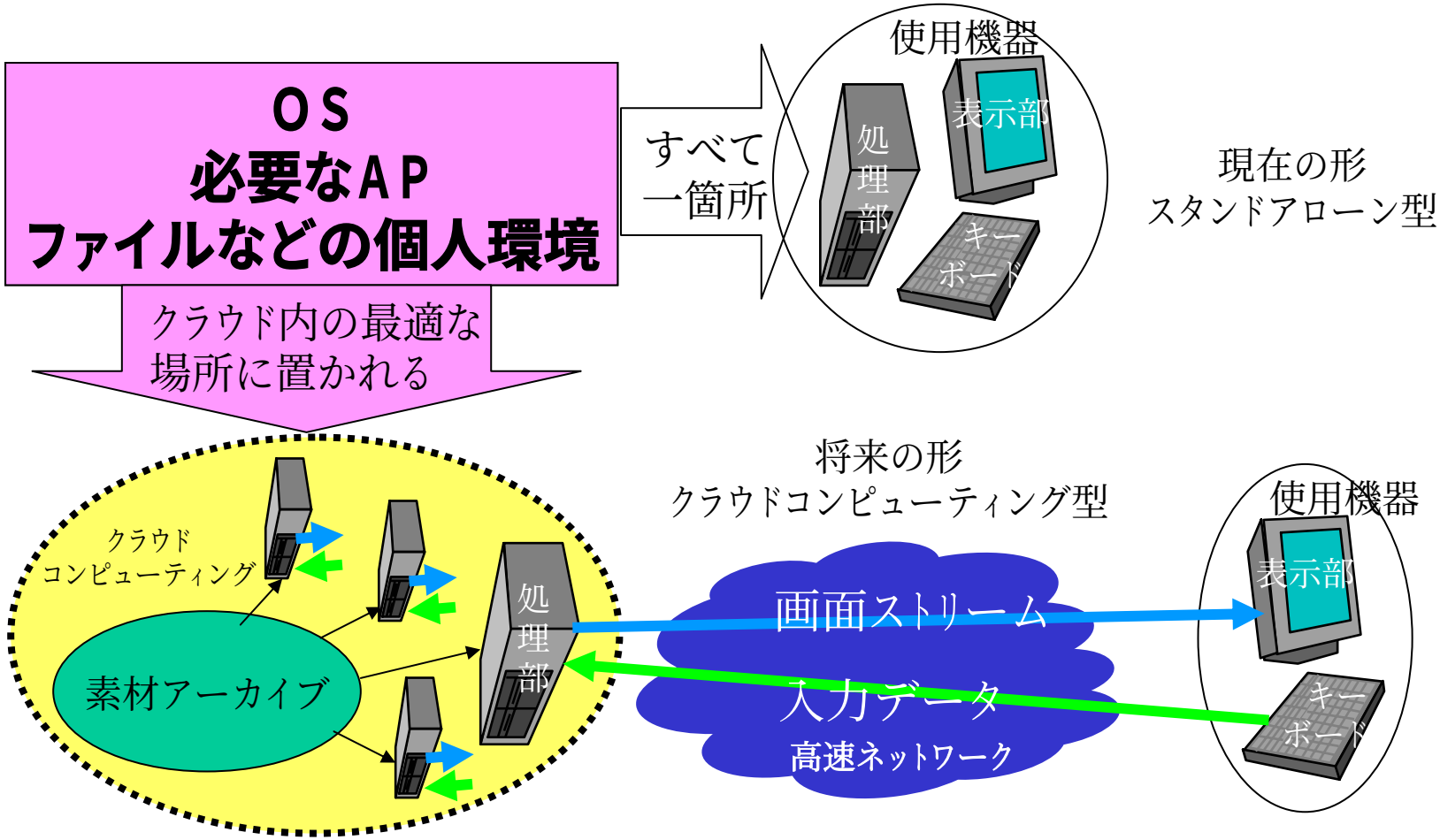
評価基準は
検索エンジン
毎に異なる

WEB時代の完成：

プラットフォームクラウド時代

ＰＦＣ：Platform Cloud

高速動作の大規模ＡＰには クラウドコンピューティング化



PFC:プラットフォームクラウドの構築

PFC＝サービス(SaaS)クラウド＋仮想個人環境(VPE)クラウド

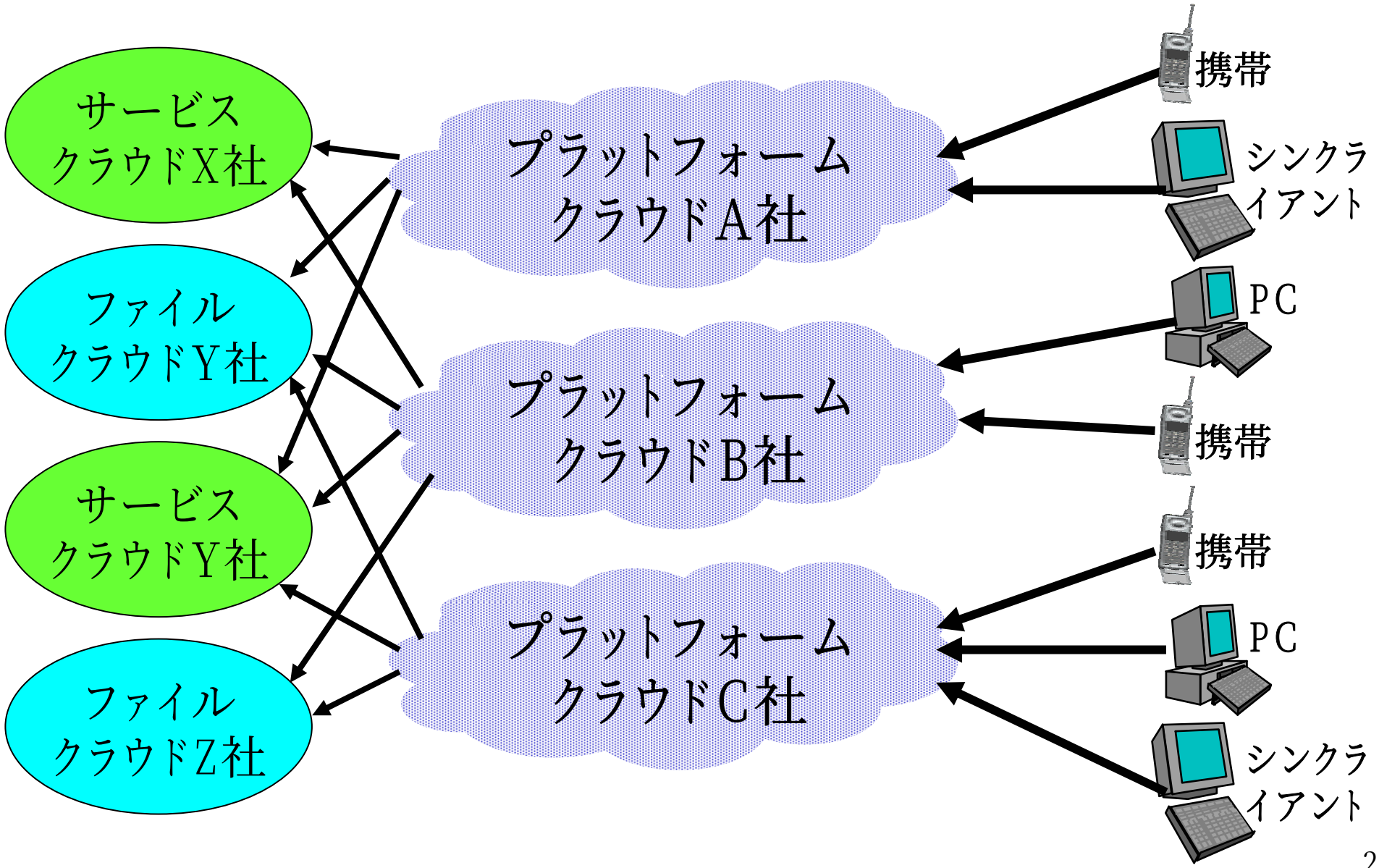
SaaS:**Software As A Service**　　VPE:**Virtual Personal Environment**

① Web基盤の利点→永遠のビギナの使用を促進する
　永遠のビギナ対策を行って全員ICTを使いこなすことが必須
　永遠のビギナは、個人環境の設定･再設定、セキュリティ対策等は苦手
　コスト／パフォーマンスを常に最適に保つためには、ICT時間貸しが必須

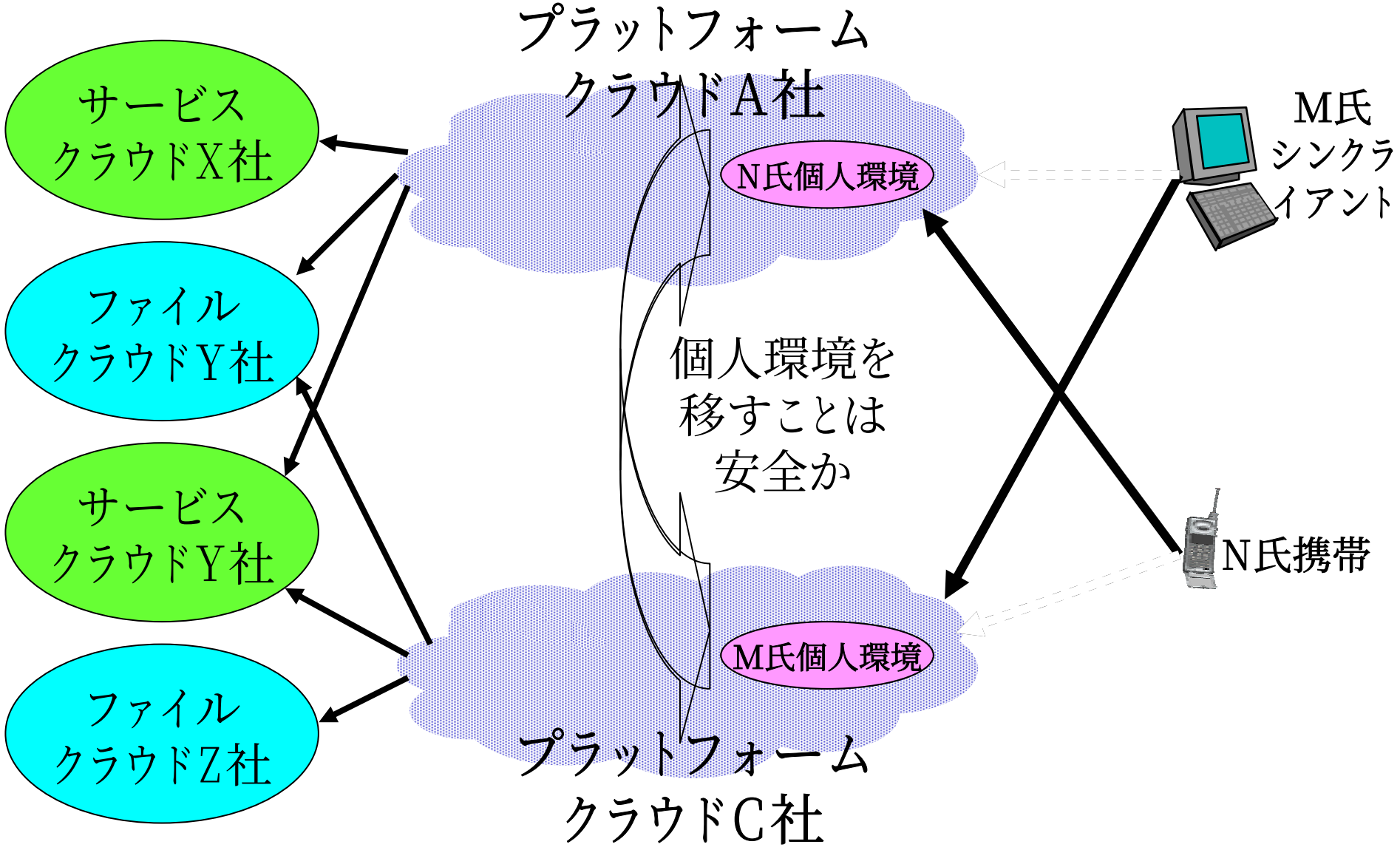
② 何故PFCが必要か→ICT時間貸しとセキュリティ向上のため
　サービス･応用ソフトの時間貸しを実現
　　→サービスソフトクラウドの構築←SaaSとして一部導入始まる
　利用者は「永遠のビギナ」と考え、個人作業環境はすべてサーバ側に設置
　　→仮想個人環境(VPE)クラウドの構築
　　←不完全な形態としてはシンンクライアント端末が存在

③ クラウド化のコストパフォーマンスを上げる
　認証機構や巨大サーバ･データベースの構築
　　→個人情報の蓄積場所が主権管理の及ばない場所になることは阻止
　VPEクラウドでは、VPEを移行可能とすることを義務付け、競争を担保する
　　→優位性を確保するためにサービスソフトクラウドとの一体化を認知

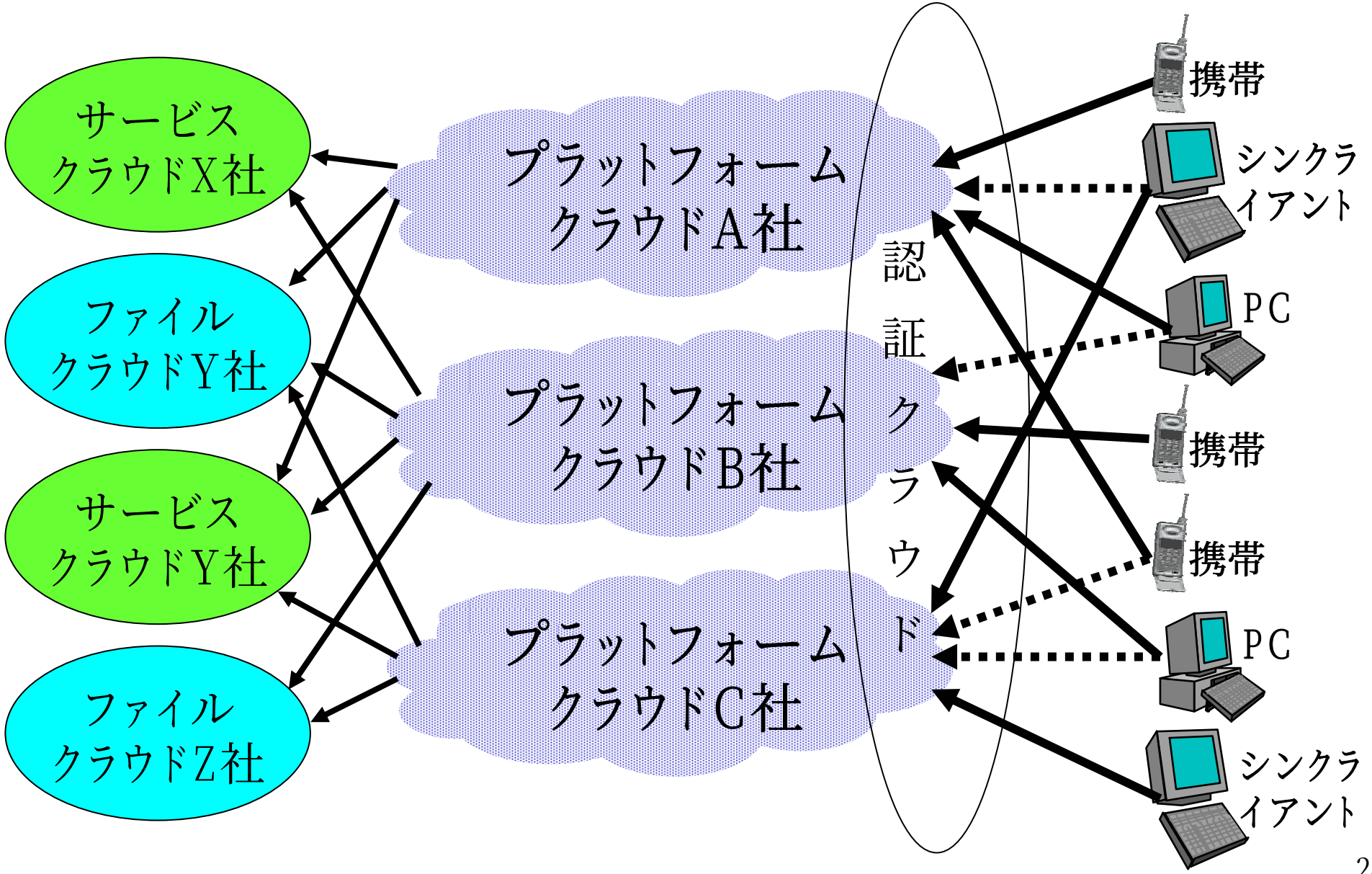
究極のクラウド：プラットフォームクラウド



プラットフォームクラウド間の移動



プラットフォームクラウドの最大の課題：認証



脅威への対応

相手の意識

A-type：愉快犯

愉快犯・自己顕示欲などは以前から存在し、恐らく今後も存在。

B-type：市場支配（プラットフォーマ）

市場支配者或いは支配を狙っている人。選択肢のない強制。

C-type：主義主張

国家や企業などの秘密や「犯罪」の告発。信条に基づいた「制限や統制」に対しての攻撃。

D-type：金銭

金銭を得る目的での、情報窃取や業務妨害と恐喝まがいの商売など。

E-type：権益拡大

平和維持、権益拡大のための諜報活動。他国の権益拡大行為や軍事活動の妨害。

F-type：ストーカ

個人相手だけではなく、企業も対象となる可能性。

国家が関与か？

高度な不正プログラム（ウイルス）

サイバー兵器と言って良いかもしれない。

２１世紀は、こういう不正なプログラム同士の戦いなのか？

主張する人たち！

1. 今回の表向きの攻撃
   1）アプリケーションサーバの脆弱性で改ざん
      → アプリケーションサーバ問題は根が深い。使用理由。運用管理をやりたくない！
   2）DDoS（ツール・やり方の提示）

2. 初めての「日本」への攻撃。
   → やり方に戸惑い。情報収集？リクルート？

3. 機密を盗み暴露したいはず。
   → ソニーの米子会社でやったような個人情報
   → メールのやり取り
4. デジタルコンテンツ権利関連政策や事業には敏感。
5. 原発再稼動を阻止する旨の宣言も。

主張する人たち！ 霞ヶ関？霞ヶ浦？

1. 多くの攻撃は、検索エンジンから。
2. 改ざん画面でのアンバランスなメッセージ。
   → 日本に詳しい？ 少し前に準備？
3. シャレが利いている。
   → 違法ダウンロードの誘発となめた選曲
4. 2チャンネラーが絡んでいる？
   → 今後の展開？
5. そうだとしたら、関係者のプライバシーが暴かれ、晒される。

どういうことが行われているのか？

基本的に3つのステップ

1. 潜り込む為の行動
   1) メールが多い。→ 今後は、ソーシャルメディアなども注意。
   2) USBメモリーやCDなどのメディア持ち込みや送付。
   3) 改ざんされたホームページの閲覧。

2. 情報筒抜け基盤の構築と維持
   1) 基盤を拡張する。
   → A部署からB部署へ。本社から工場へ。海外拠点から本社へなど。
   2) 基盤の維持や改善を行う。

3. 組織内部情報の調査や情報のクリッピング
   1) ドキュメントファイルは基本的に収集する。
   2) キーワード検索を行うことも。　・・・ 既存の管理システムの悪用。
   3) 破壊や誤作動の誘因による混乱の誘発なども可能。

整理をしてみましょう。

1. 標的となっているのは
   1）入り込む手段
      → 外界と接触のある人。免疫のない人。

   2）内部を乗っ取る手段
      → システム管理者。権限のある人。

2. 対策の骨子
   1）出口対策。真中・入口見直し。大掃除。

   2）ID管理、特権管理、特権行使の見直し。

   3）予防接種、訓練、専門家、人脈。

どうすればいいのか？

間違ったセキュリティ対策 に気付く

例えば 1）OSなどを最新にしよう。

→ 正論であることに気づく。

→ 多くの場合、実はEXEを開いている。

例えば 2）ウイルス対策

① 感染したらネットワークから切り離し

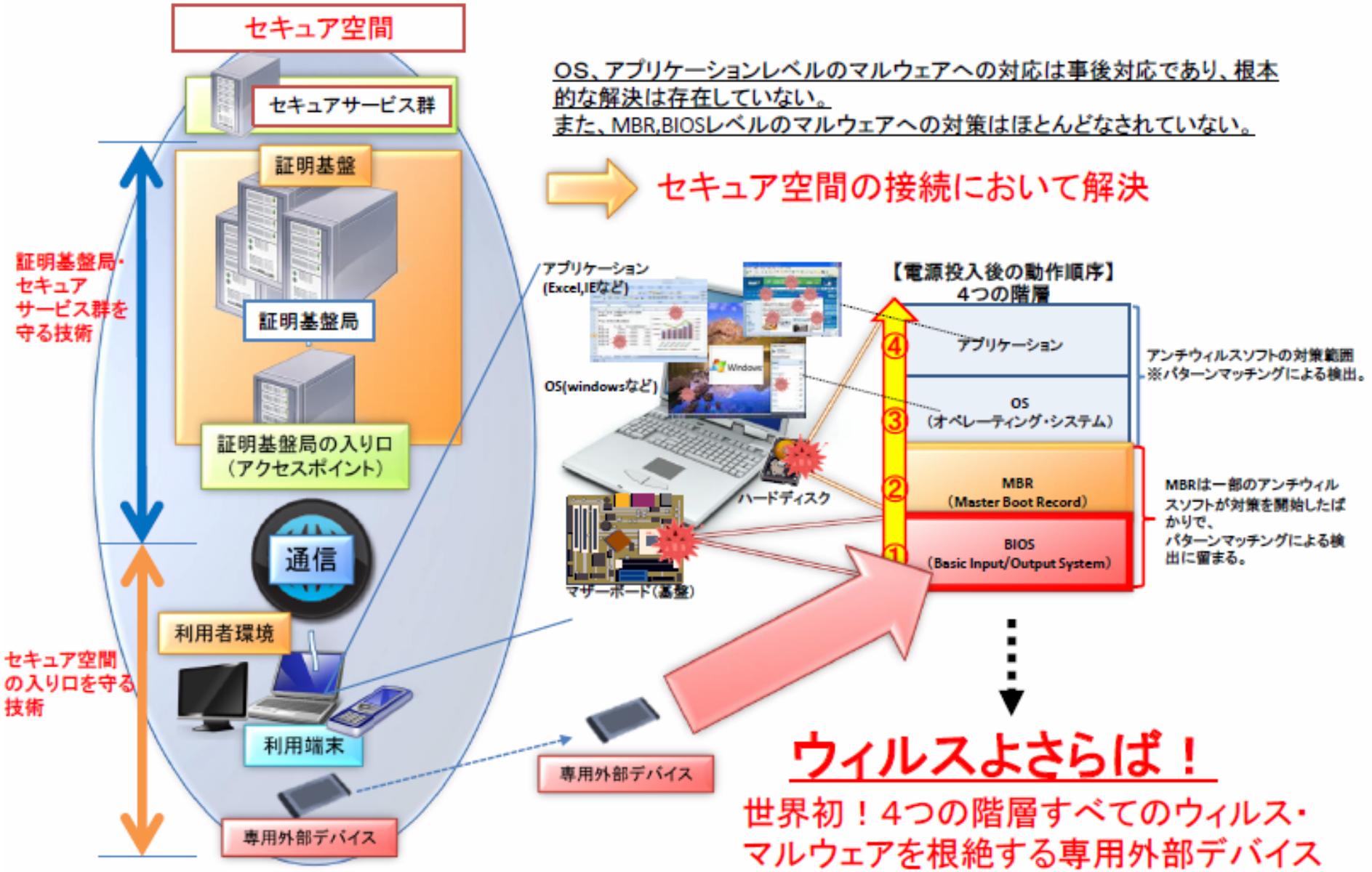
② 定義ファイルを最新にしてスキャン

③ 駆除できれば完了

誤解は、対策の完了が駆除であること。

BIOS対策

4つの階層からのマルウェアの排除



9

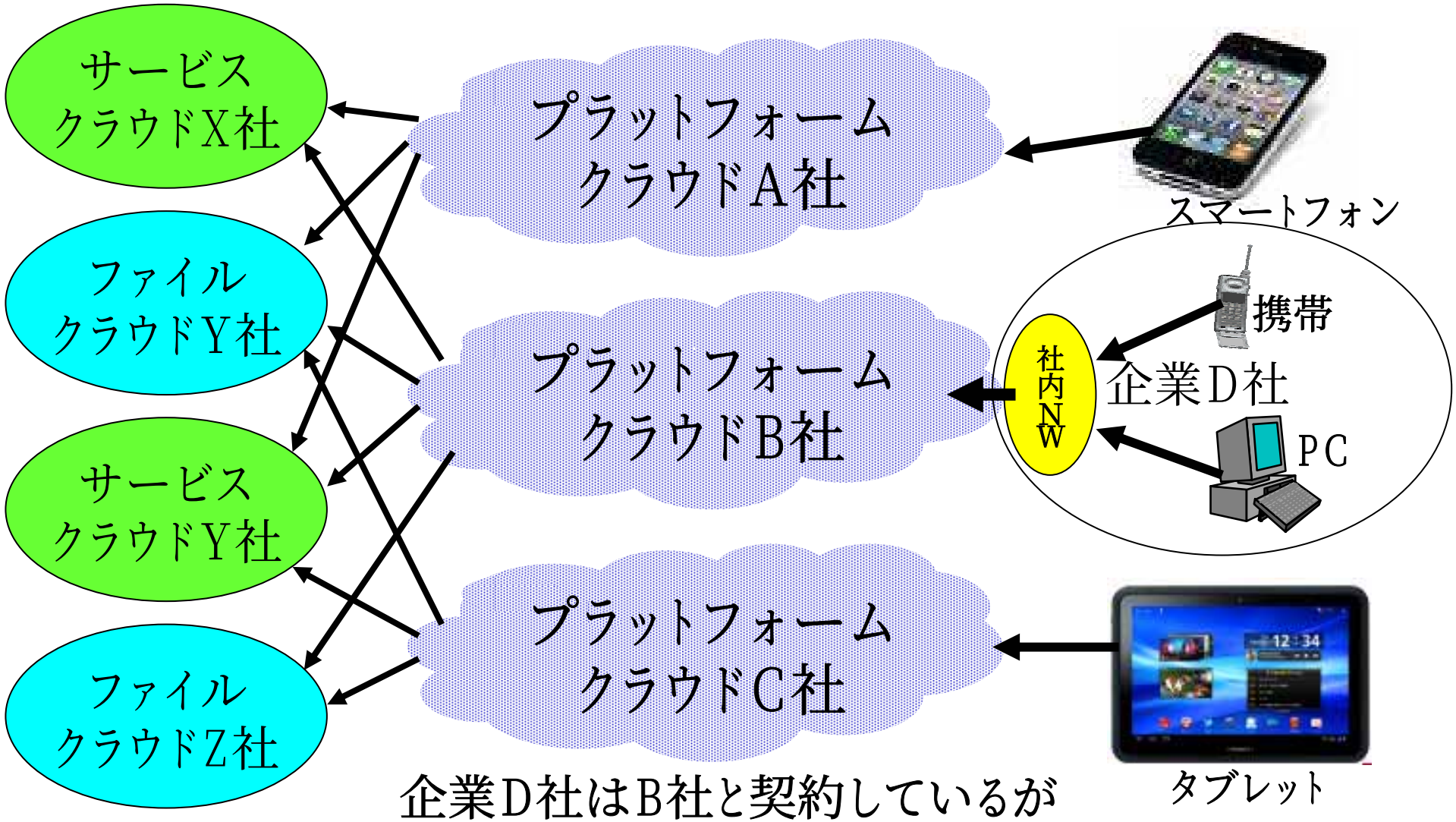
新しい環境には新しいやり方を

BYOD：Bring Your Own Device

スマートフォン市場規模予測（MM総研調べ）

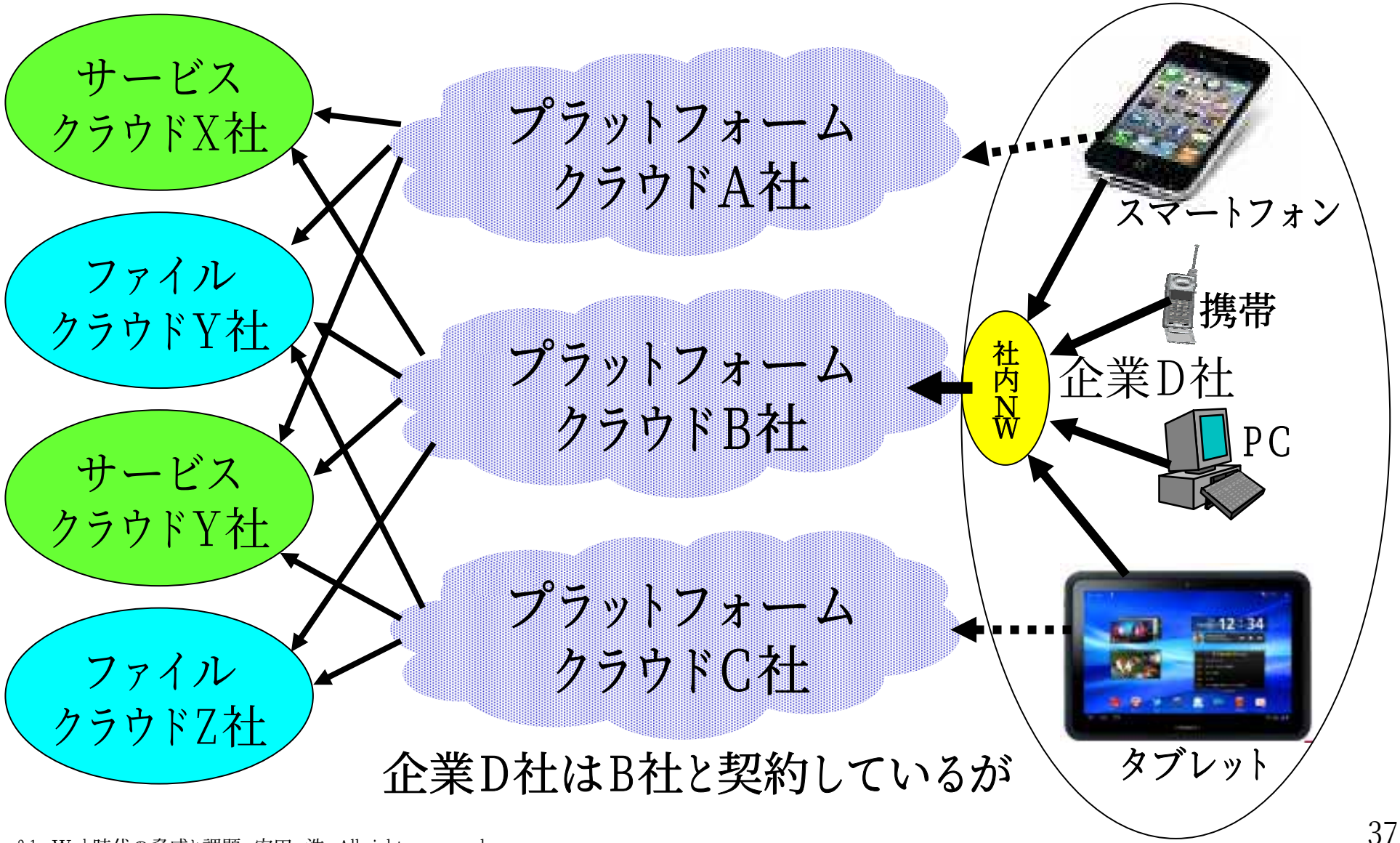
- 2011年度は前年比2．7倍の2340万台
- 2016年度は総出荷の83．4%の3555万台
- 2016年度の契約数は67．3%の8119万件

プラットフォームクラウドとスマホ



企業D社はB社と契約しているが

プラットフォームクラウドとスマホ

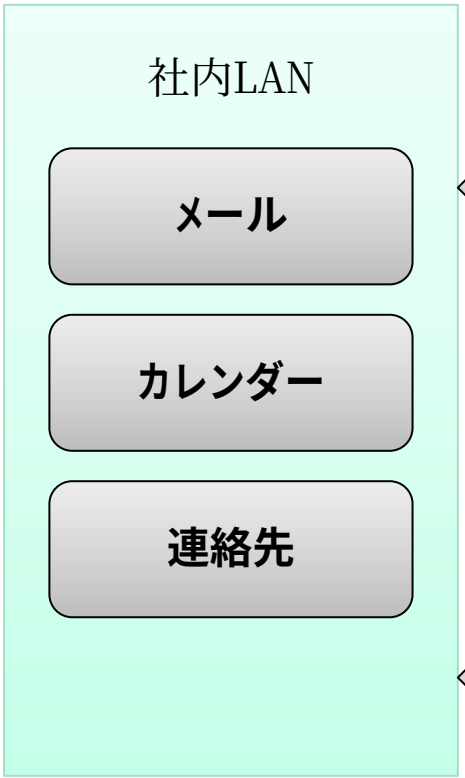


企業D社はB社と契約しているが

スマホ系導入の背景

・会議の多い上位マネジメントや、出張の多い営業職員が多かったが、安全性の面から
メールやカレンダーは自席PCからしか確認できず、社外からの利用を許していなかった。

→ 持ち運び・利便性等からスマホ系デバイスを持つ人が増える見込み



会議

- **会議の連続で自席に戻ることが少ない。**
- **会議中は確認する事ができない。**
- **スケジュールのダブルブッキングなどが発生していた。**

出張

- **本来許可していない私用メールへの転送などが行われている節があった。**
- **お客様からの連絡にスピーディーに答えられない。**
- **出張から帰るとメールの処理に追われて仕事にならない。**

リアルコム社　福田雅和氏　2011.08.12講演より

私物デバイスの社内接続は必要か

マルチデバイスアクセスが可能な体制であれば接続を許可することにより、ＩＣＴ活用が活発化する ← ビジネス時とプライベート時の連続性のため

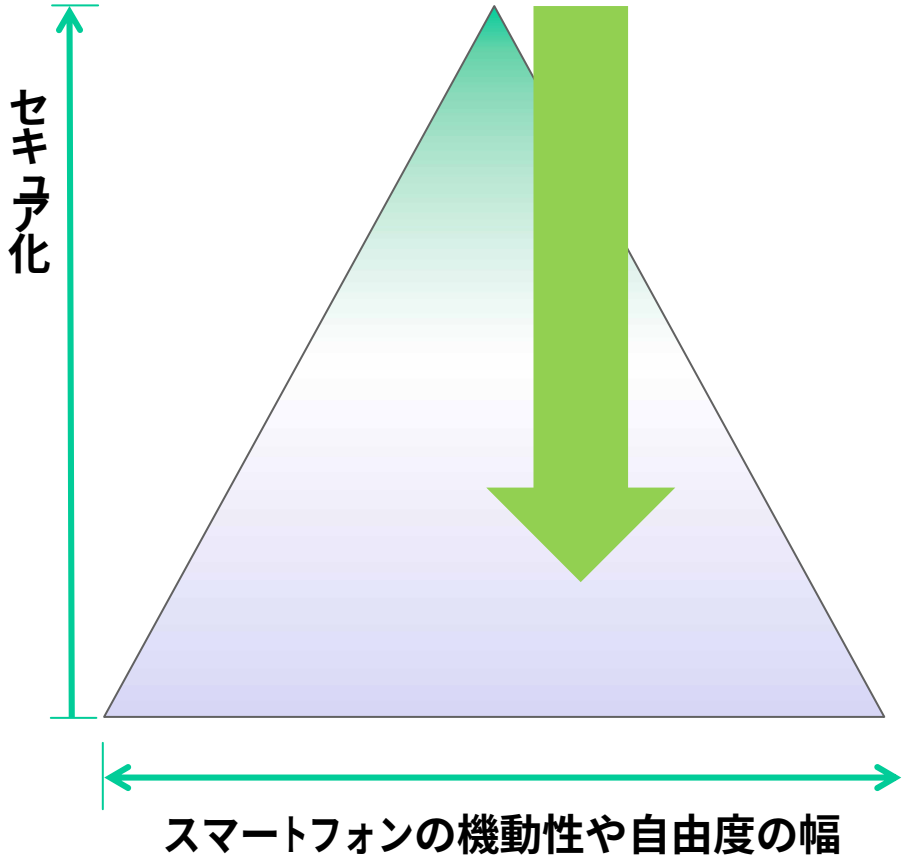
役員	管理職	一般社員
• 会議続きの中で、カレンダーをリアルタイムで確認して、参加･不参加を決定できる。 • 出張中にメールが参照でき、適切な指示を出せる。	• 社外にいる事が多く、メールをリアルタイムに参照し返事ができる。 • 電話と併用する事で出張時の取引もスムーズに行えるようになった。	• 自身の私用端末を利用できる制度なので、業務端末に比べ、精神的ハードルが低減でき、活用が進んでいる。

上位層を巻き込んでの早期パイロット利用を行い、安全確保をしながら企業サービスの利用規制を緩和する事でスムーズな展開を行う事が可能 → ＢＹＯＤ：Bring Your Own Device の実現

リアルコム社　福田雅和氏　2011.08.12講演より

BYODセキュリティ対策の勘所

•セキュリティ対策を充実させていくと、スマートデバイスのメリットである、機動性や自由度を殺す事になっていくため、極力活用の幅を狭めない対策がポイントとなる。



目指すべきセキュリティ対策

- 3G環境での利用も含めてユーザーの利活用を阻害しない。
- PCや携帯電話とは違う目的で導入されている事を理解して対策を考える。
- 事前防止の観点と併せて、事後対応の観点も考慮に入れてバランスの取れた対策を行う。

よくある堅いセキュリティ対策

- 全てサーバー側にデータを置いて一切スマートデバイスにダウンロードさせない。
- 必ず自社のネットワークにVPN接続した上で利用する。
- 機能を絞って必要な機能のみが使える様な形に制限して配布する。

リアルコム社　福田雅和氏　2011.08.12講演より

私用端末の業務利用（BYOD）で気をつけるべきポイント

入手できる端末自体は、原則法人向けもコンスーマー向けも変わりが無い事を理解した上で、端末のコントロールにどこまで手を出すかがポイントとなる。

所有者/契約者の違い

- 企業が所有しない、またはキャリアと契約していない端末の場合、たとえば強制的なリモートワイプや、回線停波の処理がしにくい。（法的に訴えられた場合の事例が無い）
- 企業端末であれば禁止事項にできるバックアップや自宅PCとの接続も禁止しにくい。

資産管理

- スマートデバイスは大抵1つのIDでアクティベーションされ、アプリの購入履歴や、付加サービスを実現しているが、個人のIDでアクティベーションされた物に、たとえば企業として利用すべきと判断した有償アプリを入れる場合、既に入っていた場合などの管理が煩雑になる。

サポートコスト

- iOSデバイス（今回の事例）であれば問題無いが、Androidの場合、バージョンや、メーカーごとの差異が非常に大きいため、問い合わせへの対応や、相性の検証にコストがかかる。

リアルコム社　福田雅和氏　2011.08.12講演より

まとめ

脅威への対策は全員の自覚から

古くて新しい脅威

ＤＢＳＣ：データベースセキュリティコンソーシアム
http://www.db-security.org/

ＢＩＯＳ

ＪＣＳＡ：日本通信安全促進協会
http://www.j-csa.com/

ＢＹＯＤ

ＪＳＳＥＣ：日本スマートフォンセキュリティ協会
http://www.jssec.org/

