JSSEC総会基調講演

Web時代の7つの脅威

平成25年　5月24日
スマートフォン・セキュリティ・コンソーシアム会長
東京電機大学　未来科学部　学部長
(ISC)2理事　CISSP　安田　浩

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

新しい脅威とは何か

情報自己蓄積

映像発信

クラウド活用

悪意ソフト

BIOS攻撃

BYOD

ネット倫理脅威

WEB戦国時代
日本ピンチとチャンス

自己知識の集積とログ分析

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

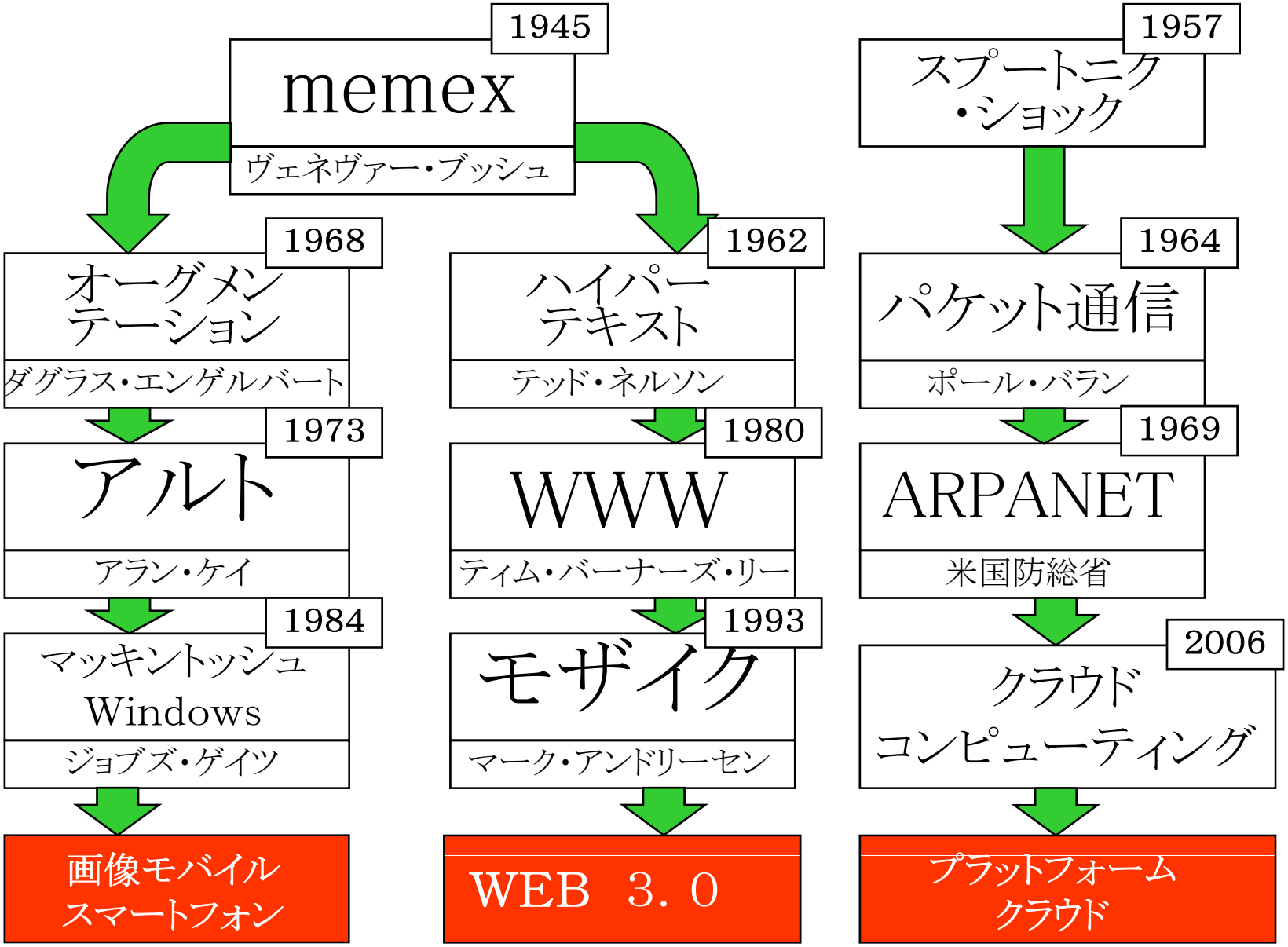
すべての情報は最新化され
情報取得は迅速に行え、相互参照が可能であり
情報の追加・削除・重み付けは自動的に成される

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

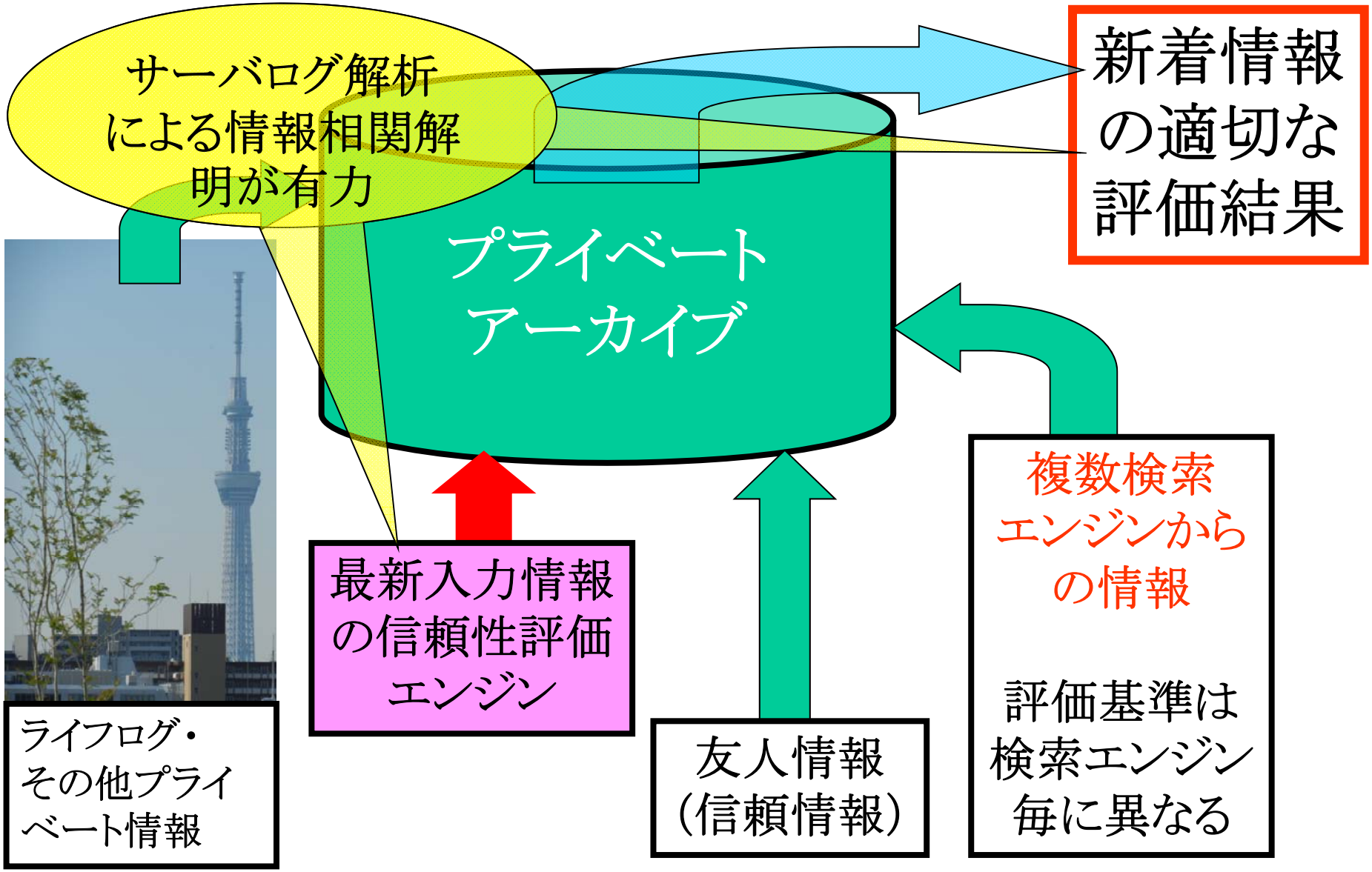
スマホ系操作機、検索エンジン、クラウド
が揃えば　WEB3.0は使えるか？

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

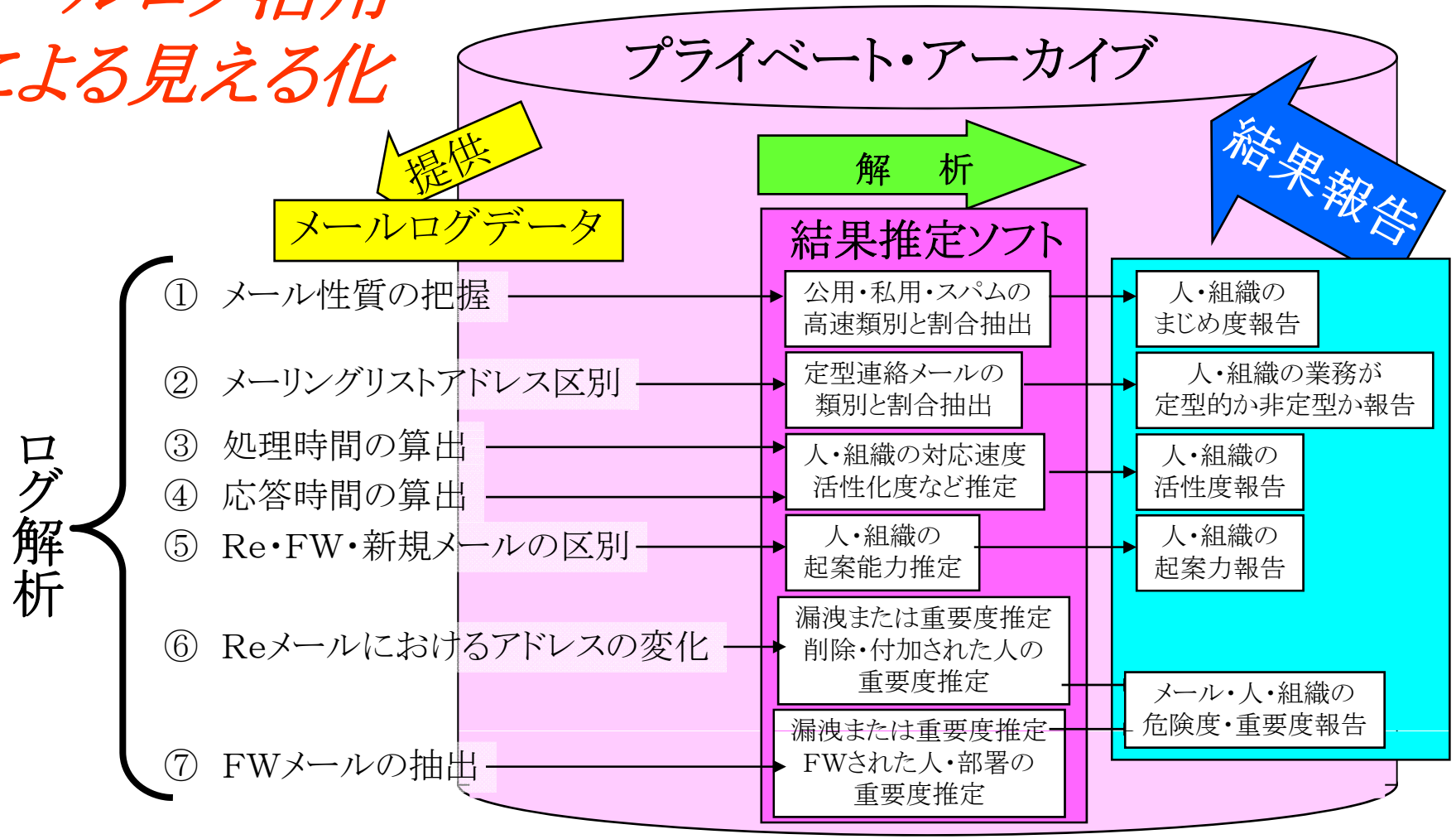
プライベート・アーカイブとは



サーバログ解析による情報相関解明

ログ分析の効用　→①安心・安全（情報漏洩分析等）
→②組織・人の生産性見える化

メールログ活用による見える化



WEB発信
映像を皆の手に

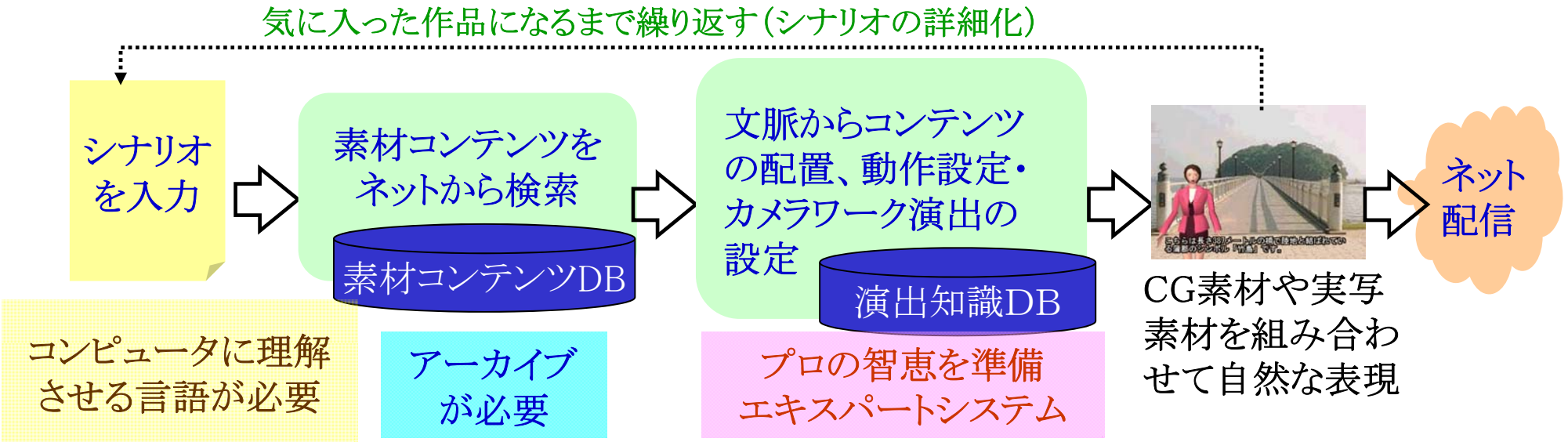
映像創生ツールDMDの
CGM化

DMD：Digital Movie Director
CGM：Cosumer Generated Media

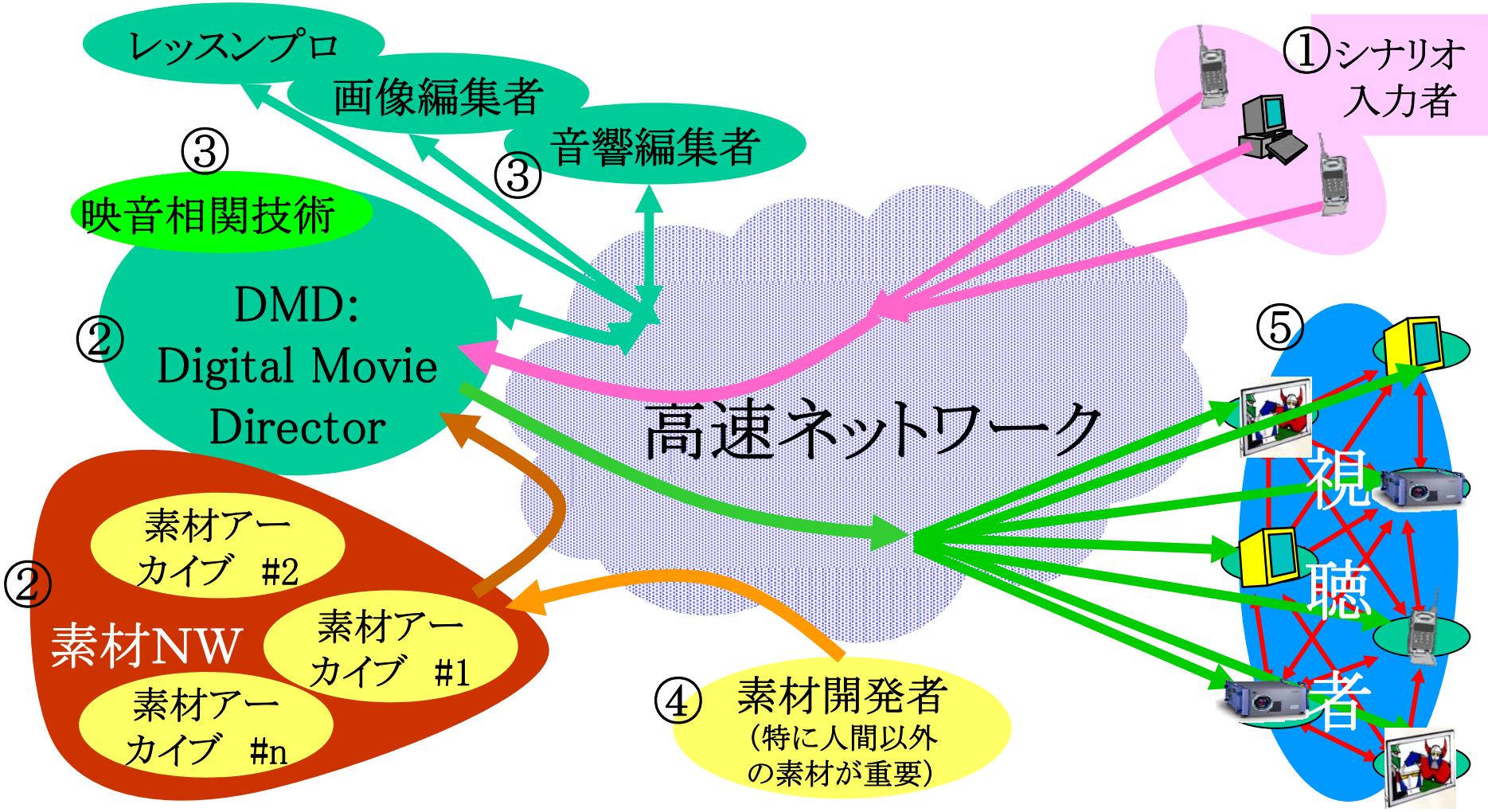
誰もが映像を簡単に創れるように

DMD: Digital Movie Director

映像（映像日記、映像BLOG、映像旅行記、映像プレゼン、映像コマーシャル等）を誰でも簡単に作成できる“シナリオ入力映像自動創生ソフトウェア”



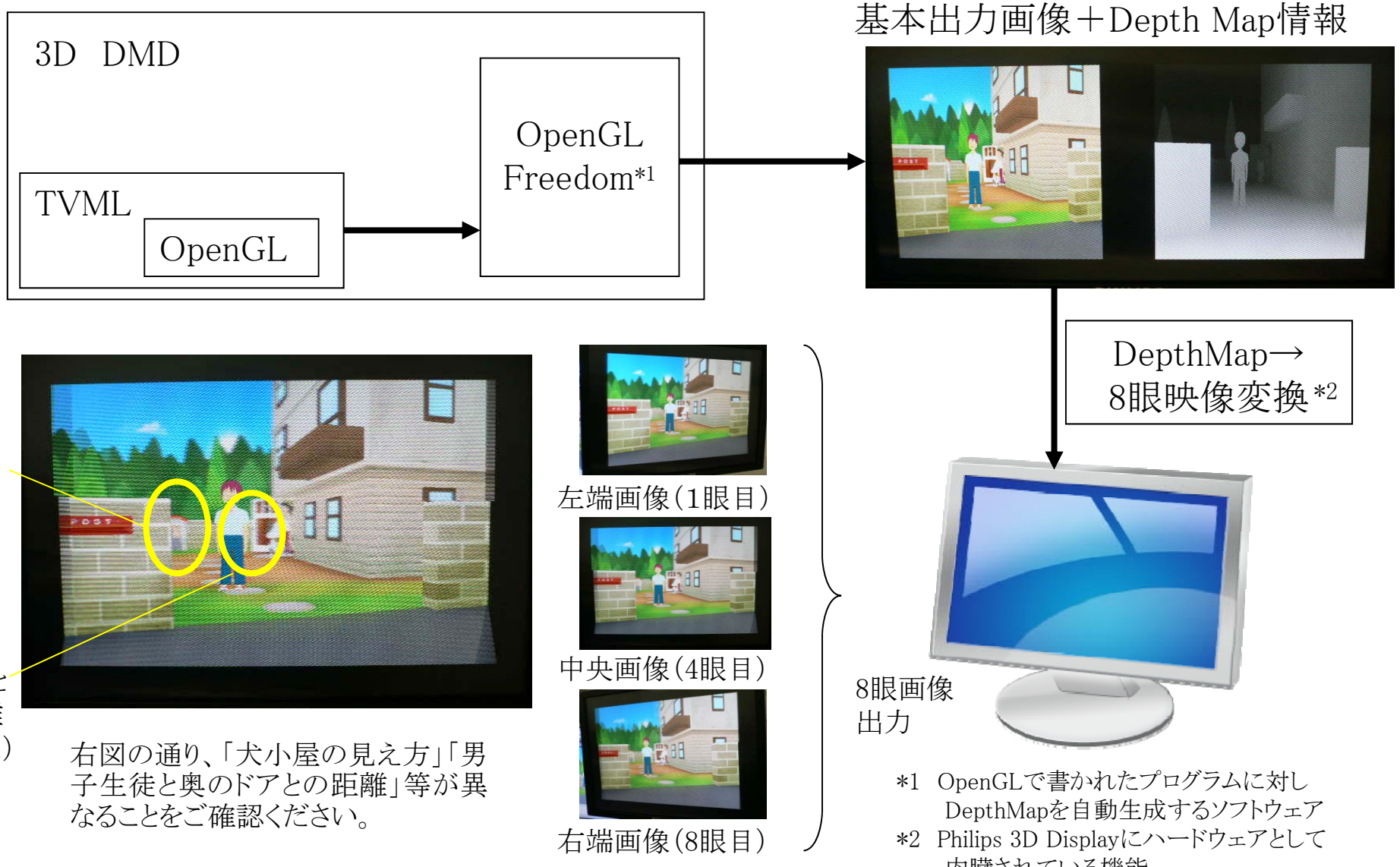
DMDは映像創りための簡単ツール



① シナリオをDMDに入力
② DMDが素材を用いて自動的に映像創生
③ 映音相関技術やエキスパートシステムが映像をリファイン
④ 素材映像を製作して入力
⑤ 創生された映像を視聴・評価

DMDのインターフェース

DMDの3D映像化

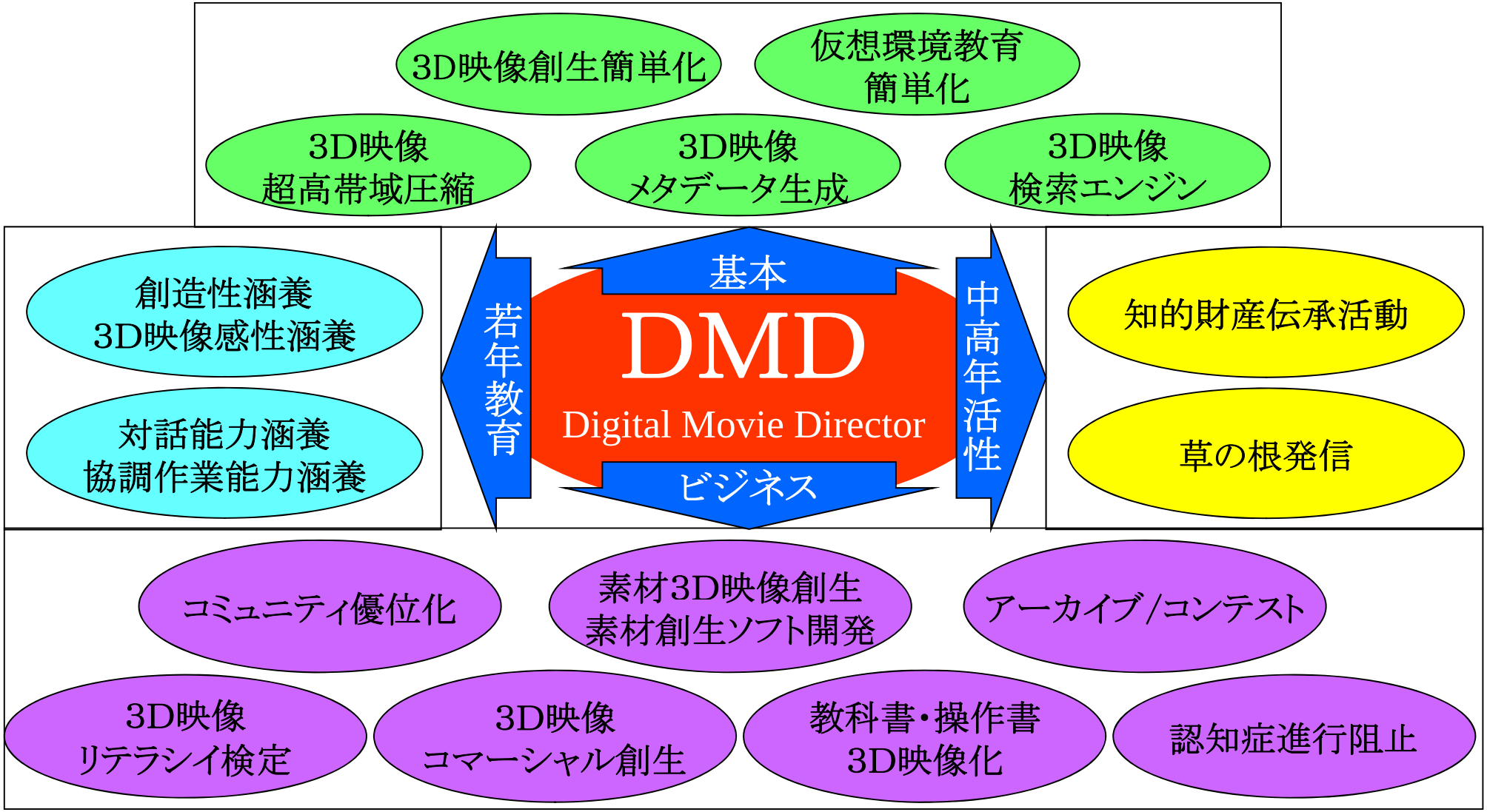


右図の通り、「犬小屋の見え方」「男子生徒と奥のドアとの距離」等が異なることをご確認ください。

*1 OpenGLで書かれたプログラムに対しDepthMapを自動生成するソフトウェア

*2 Philips 3D Displayにハードウェアとして内臓されている機能。

DMDはどのように使われるか

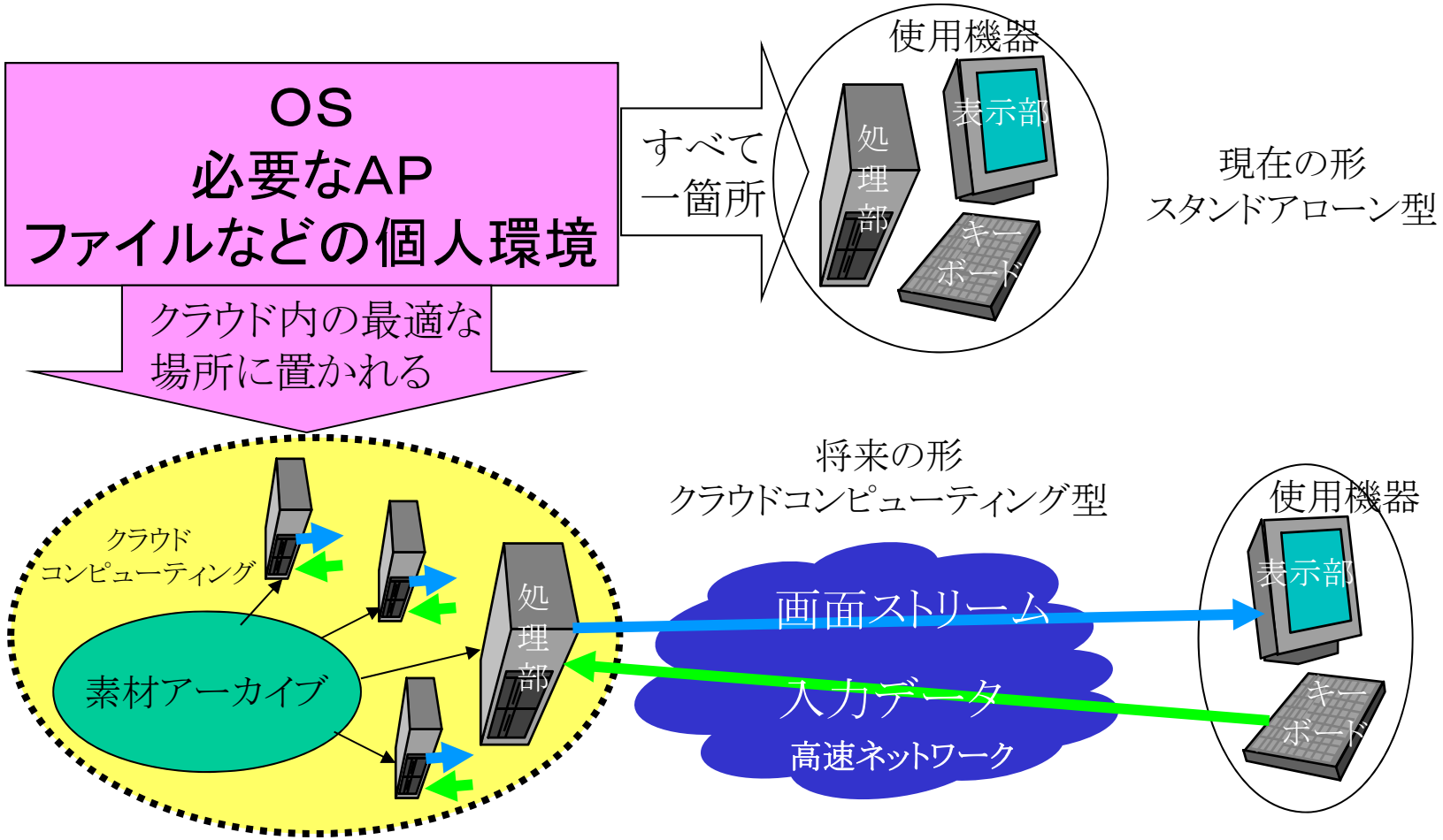


WEB時代の完成：

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が必要



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

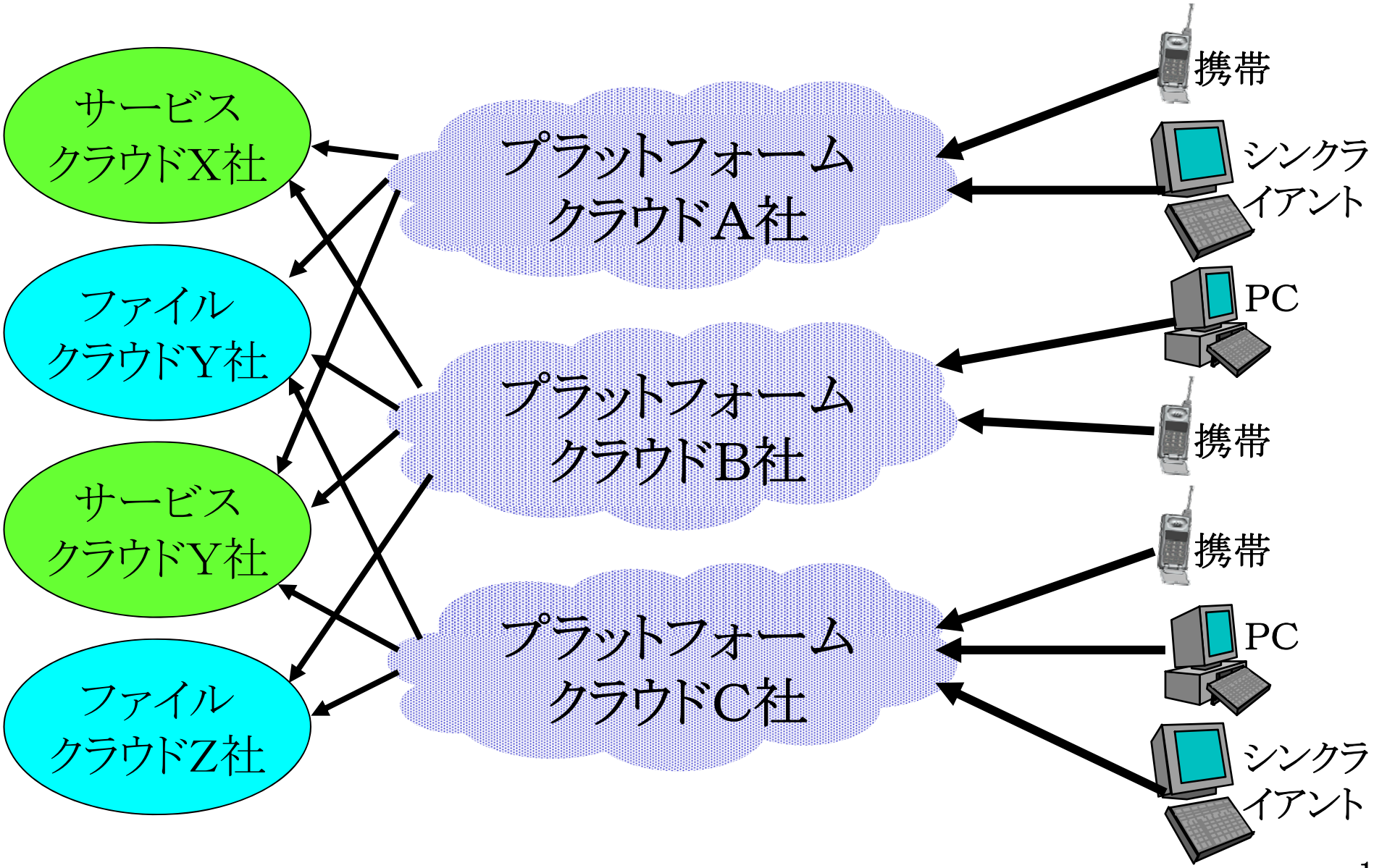
SaaS：Software As A Service　　VPE：Virtual Personal Environment

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

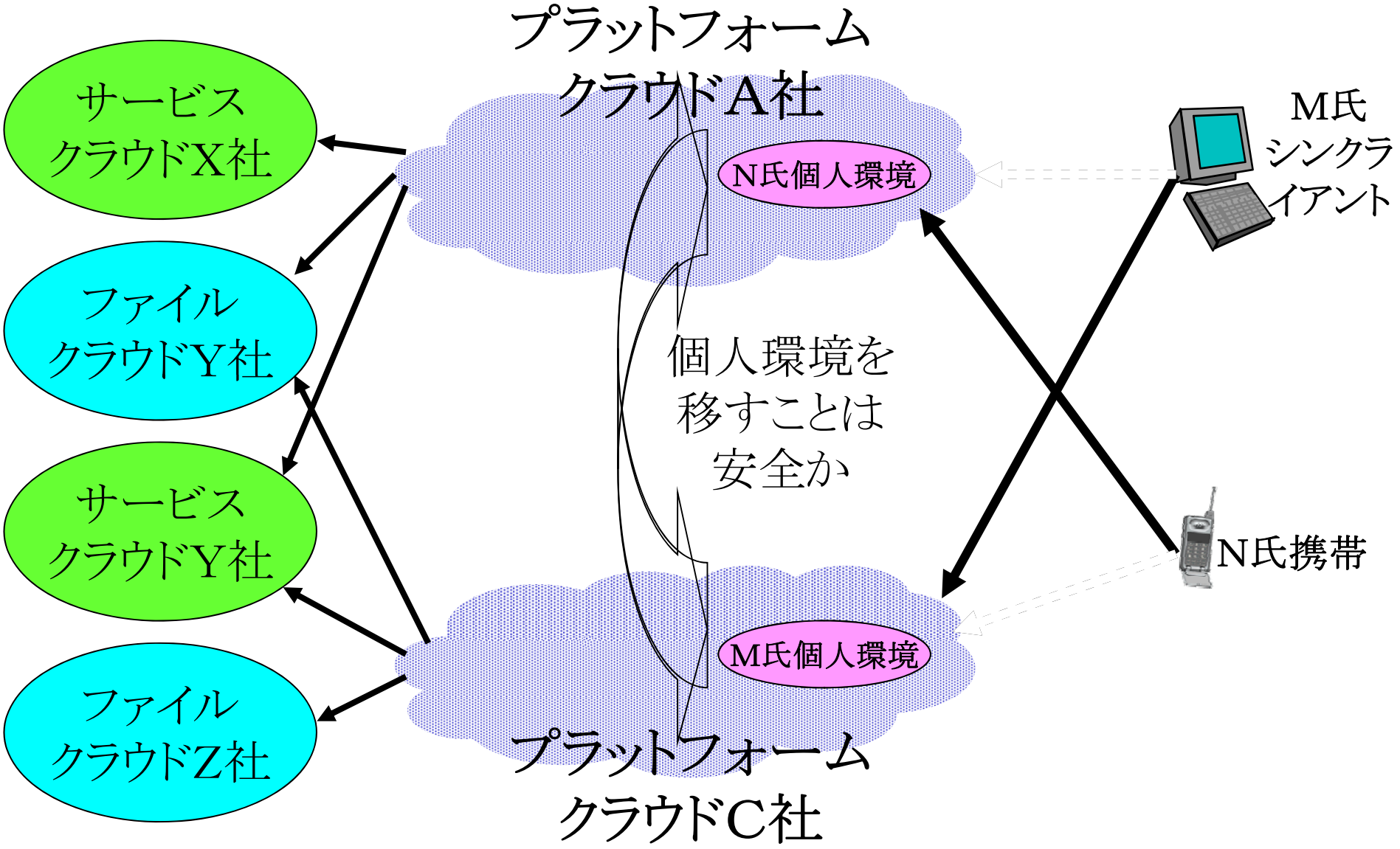
② 何故PFCが必要か→ICT時間貸しとセキュリティ向上のため
　サービス・応用ソフトの時間貸しを実現
　　→サービスソフトクラウドの構築←SaaSとして一部導入始まる
　利用者は「永遠のビギナ」と考え、個人作業環境はすべてサーバ側に設置
　　→仮想個人環境（VPE）クラウドの構築
　　←不完全な形態としてはシンンクライアント端末が存在

③ クラウド化の安全性と利便性を上げる
　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

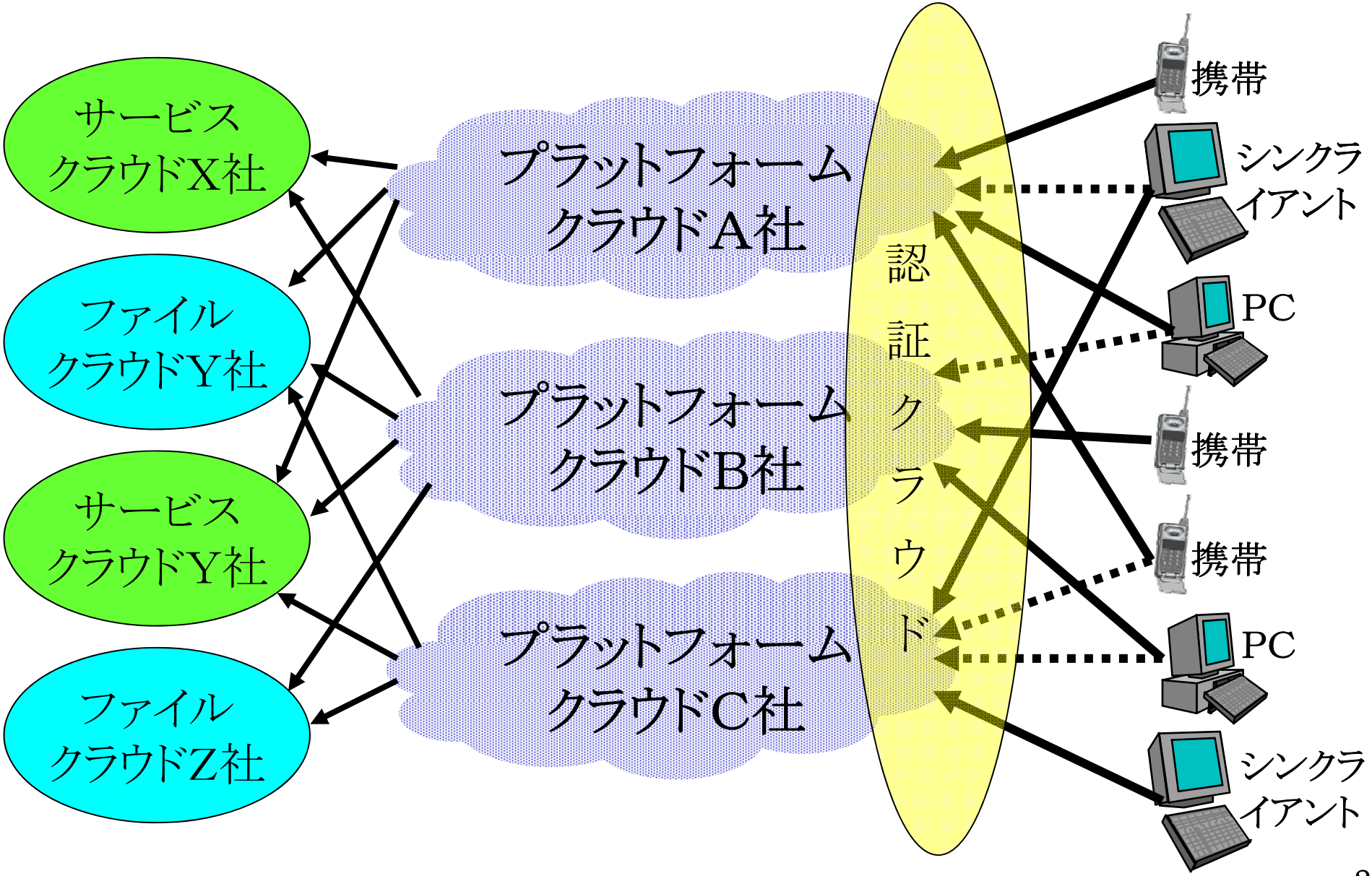
究極のクラウド：プラットフォームクラウド



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



古くて新しい脅威への対応

標的型攻撃・サイバーアタック対策

大手の製造業や政府系機関を対象とした昨今の標的型攻撃は、従来のソリューションで対策を施していても、それをすり抜けて企業の内部に侵入してきます。なぜならば、各種セキュリティ製品を研究しつくした攻撃者が、極めて限定的なターゲットに向けて、感染していることに気づかない巧妙な攻撃を仕掛けてくるからです。このような標的型攻撃には、従来のソリューションでは立ち向かうことができません。

東京新聞社説

PC遠隔操作　冤罪生まぬ捜査心せよ

2012年10月10日

誰もが知らない間に犯罪者に仕立て上げられてしまう時代になった。大阪と三重で発覚したパソコン（PC）の遠隔操作事件はその恐ろしさを物語る。冤罪（えんざい）を生まないよう捜査は慎重を期すべきだ。一貫して「身に覚えがない」と否認しているのに、男性二人が八月と九月に相次いで捜査当局に身柄を拘束される事件があった。いずれもPCを使った威力業務妨害容疑だった。

大阪府のアニメ演出家は、七月に大阪市のホームページに無差別殺人を予告する書き込みをしたと疑われ、業務妨害罪で起訴された。八月に日本航空に届いた飛行機の爆破予告メールの発信源ともみられた。

三重県の無職男性は、九月にインターネット掲示板の2ちゃんねるに伊勢神宮の爆破予告を書き込んだ疑いが持たれた。ところが、三重のPCには新種の“乗っ取りウイルス”が感染していて、他人が遠隔操作できる状態だったことが判明した。大阪のPCも調べ直してみると、類似のウイルスに感染していた痕跡が確かめられたという。二人とも事件には関わっていなかった可能性が高まり、釈放された。アニメ演出家の勾留は一カ月近くに及んだ。危うく無実の罪を着せられるところだったのだ。

サイバー犯罪の捜査では、情報端末のネット上の住所に当たるIPアドレスを手掛かりに持ち主を割り出すことが多い。だが、この手法に頼り切ると冤罪を生み出し、真犯人を逃しかねない。この事件はそう警鐘を鳴らしている。ネット社会では誰の情報端末であれ、第三者に乗っ取られ、勝手に操作される危険がつきまとうことを自覚したい。役所や企業、個人の情報を盗んだり、流出させたりする中継点として気づかないうちに悪用されることもある。PCやスマートフォンなどの情報端末では基本ソフト（OS）やウイルス対策ソフトを最新に保つ。不審なメールの添付ファイルを開けたり、怪しいウェブサイトに接続したりしない。利用者も自衛手段を忘れてはならない。

情報技術（IT）は“秒進分歩”で進化している。サイバー犯罪者はいつも最先端の知識や技術を駆使して個人や組織のコンピューターに侵入し、新手の攻撃を仕掛けてくる。いたちごっこの面は否めないが、捜査当局も捜査手法を磨き続ける必要がある。そうでないと犯罪者に裏をかかれるばかりだ。

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

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

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。

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。

究極はBIOS対策

JCSA（日本通信安全促進協会）の試み

BIOSセキュリティ(1)

米政府、サーバBIOSへの攻撃に備える新セキュリティ標準案を公開

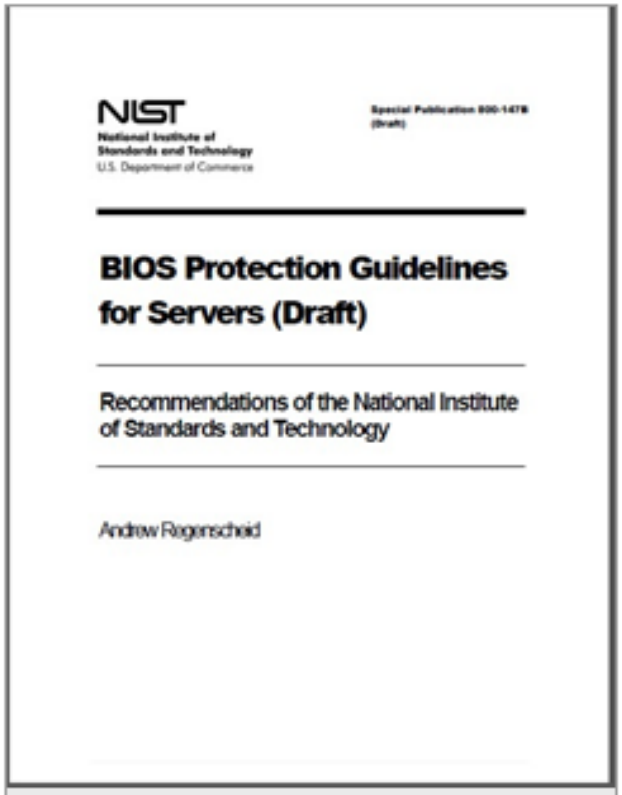
BIOS更新時の認証など、政府調達ガイドラインとしてセキュリティ要件を定める

http://www.ciojp.com/news/12699

2012/08/27

米国標準技術局(NIST: National Institute of Standards and Technology)は8月21日、サーバ・コンピュータのBIOS(Basic Input/Output System)に関する新たなセキュリティ・ガイドラインのドラフトを公開した。BIOSへの攻撃リスクが高まる中で、サーバ・メーカーが実現すべきセキュリティ水準を引き上げるものとなる。

BIOSはコンピュータの起動時、最初に読み込まれ、OSの読み込みなどを実行するソフトウェア(ファームウェア)だ。従来、サイバー犯罪者たちはWindowsアプリケーションやOSを狙ったマルウェアの開発に時間を費やしてきたが、BIOSを攻撃することで深刻な被害が引き起こせるため、そうした攻撃への懸念が高まっている。



NISTの公開した「BIOS Protection Guidelines for Servers(サーバ向けBIOS保護ガイドライン)」ドラフト版

BIOSセキュリティ(2)

政府調達におけるBIOSセキュリティ標準を策定

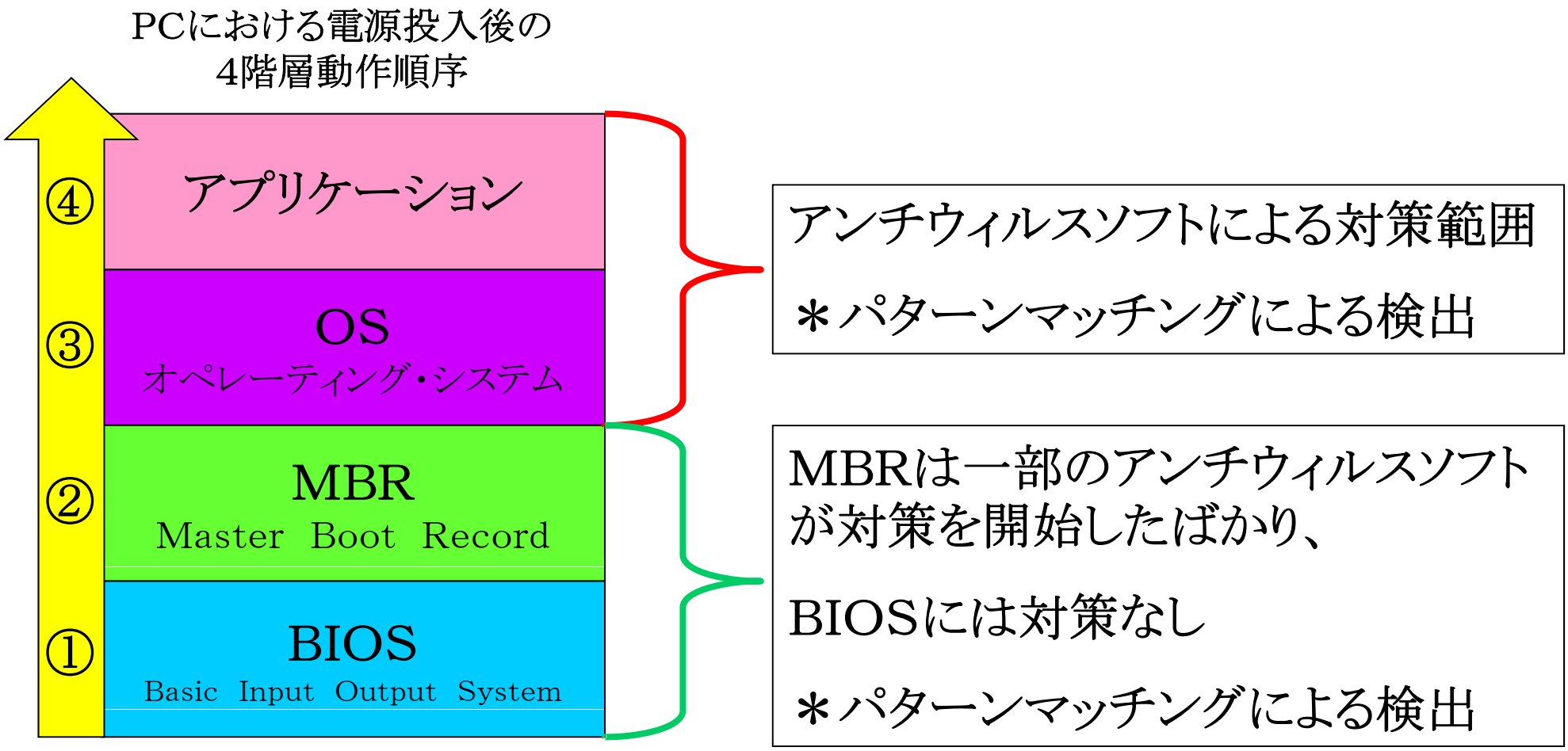
NISTが今週公開した「BIOS Protection Guidelines for Servers(サーバ向けBIOS保護ガイドライン)」はドラフト版であり、9月中旬までパブリック・コメントを受け付ける。同ガイドラインの目的は、「マルウェアがBIOSファームウェアを不正に書き換える」攻撃を防ぐことである。

同ガイドラインでは、政府が将来のサーバ調達(一般的なサーバからブレード・サーバ、マネージド・サーバまでを含む)において、「BIOSアップデート時の認証」や「(BIOSの)ローカル・アップデートの安全性」が考慮されているか、また「ファームウェアの完全性保護」や「バイパス(回避)不可能な機能」が実装されているかを確認することが指示されている。

上述のようなBIOSのセキュリティ機能を実現するためには、デジタル署名や公開鍵認証などの技術を採用する必要がありそうだが、リゲンシード氏は「NISTでは特定の技術を要求しているわけではない」と説明する。

http://www.ciojp.com/news/12699

究極のセキュリティシステムへ向けて(1)



究極のセキュリティシステムへ向けて(2)

現在までのセキュリティの根本的問題

1. 全てが後追い対策
2. しかもウィルス動作をとめるだけで駆逐するわけではない
   → いつかはまた動き出す
3. 徐々に深層に食い込み、ついにBIOSが侵されつつある
4. BIOSへの侵入
   →自分では正しいソフトを読み込んだつもりで、全く異なるソフトが読み込まれる

究極のセキュリティシステムへ向けて(3)

究極のセキュリティ対策への指針

1. 全ての悪意ソフトはOSを介して侵入する
   → OSの掌握する範囲外に対しては無力
2. BIOSが侵されていると悪意OSが読み込まれ
   コンピュータは悪意ソフトに支配される
   → 常にBIOSは真正化する
3. データの受け渡しで結局悪意ソフトが侵入する
   → データの受け渡しを全数チェックする
4. 究極のセキュリティソフトが常に真正であることを
   維持する必要がある
   → 内部犯行があっても真正性が保たれる対策が必要

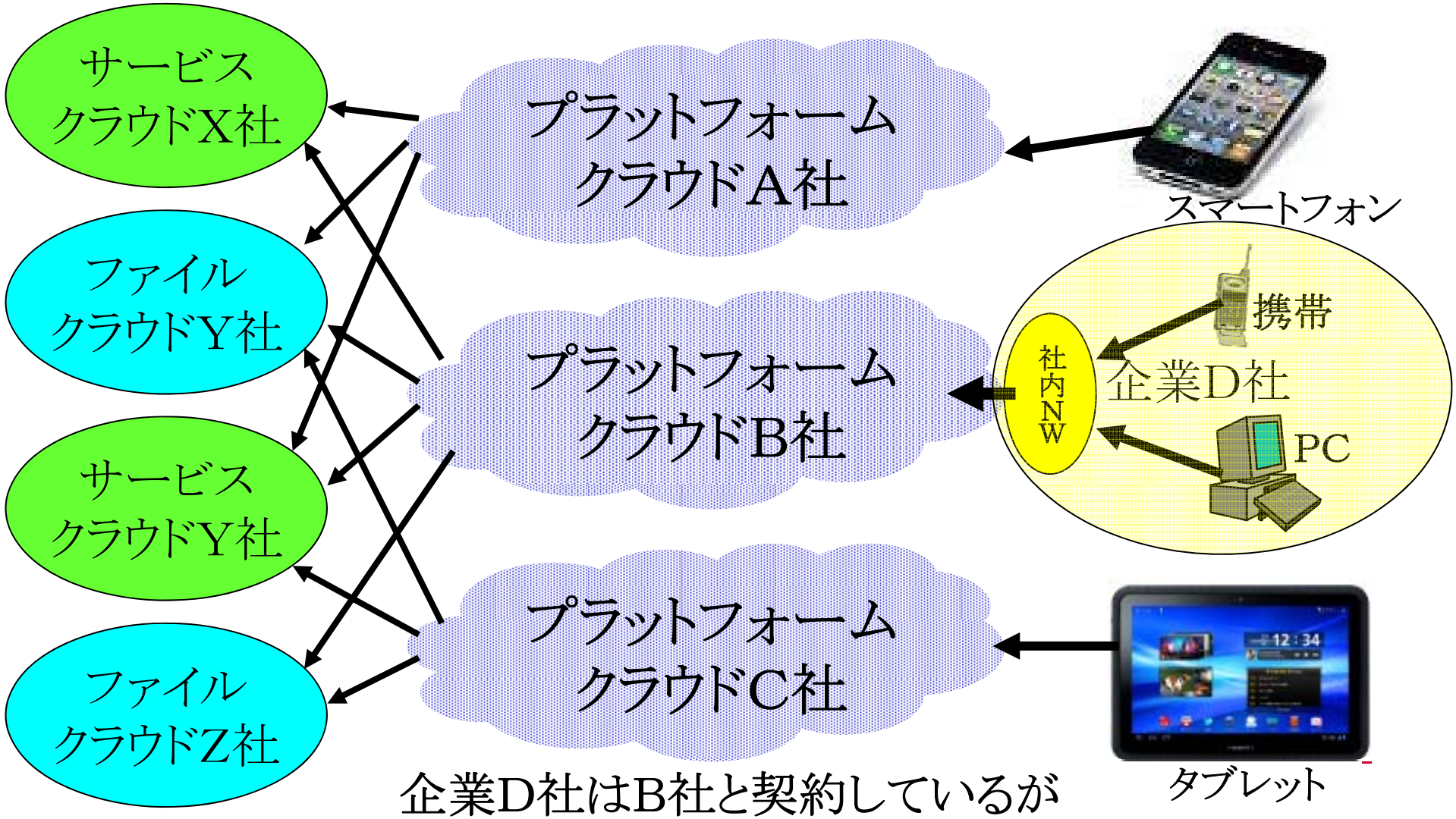
新しい環境には新しいやり方を

BYOD：Bring Your Own Device

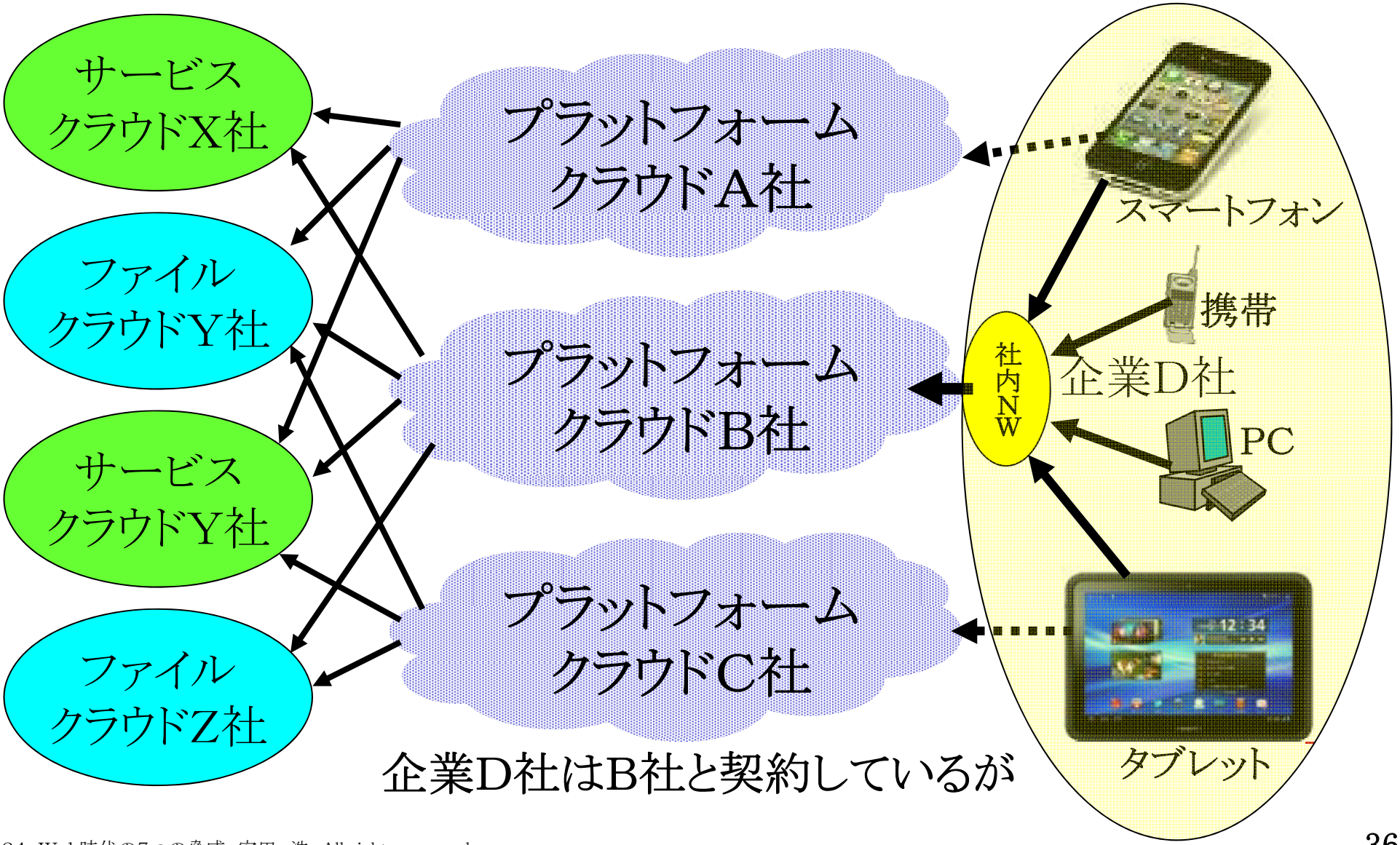
スマートフォン市場規模予測（MM総研調べ）

- 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



プラットフォームクラウドとスマホ

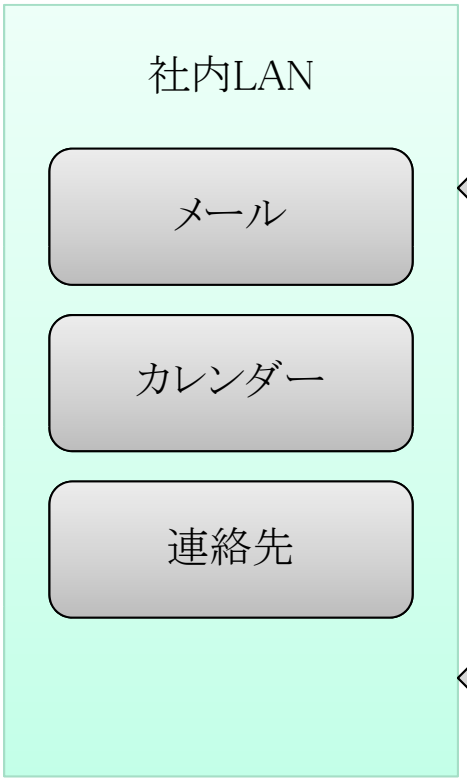


企業D社はB社と契約しているが

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

ネット倫理脅威

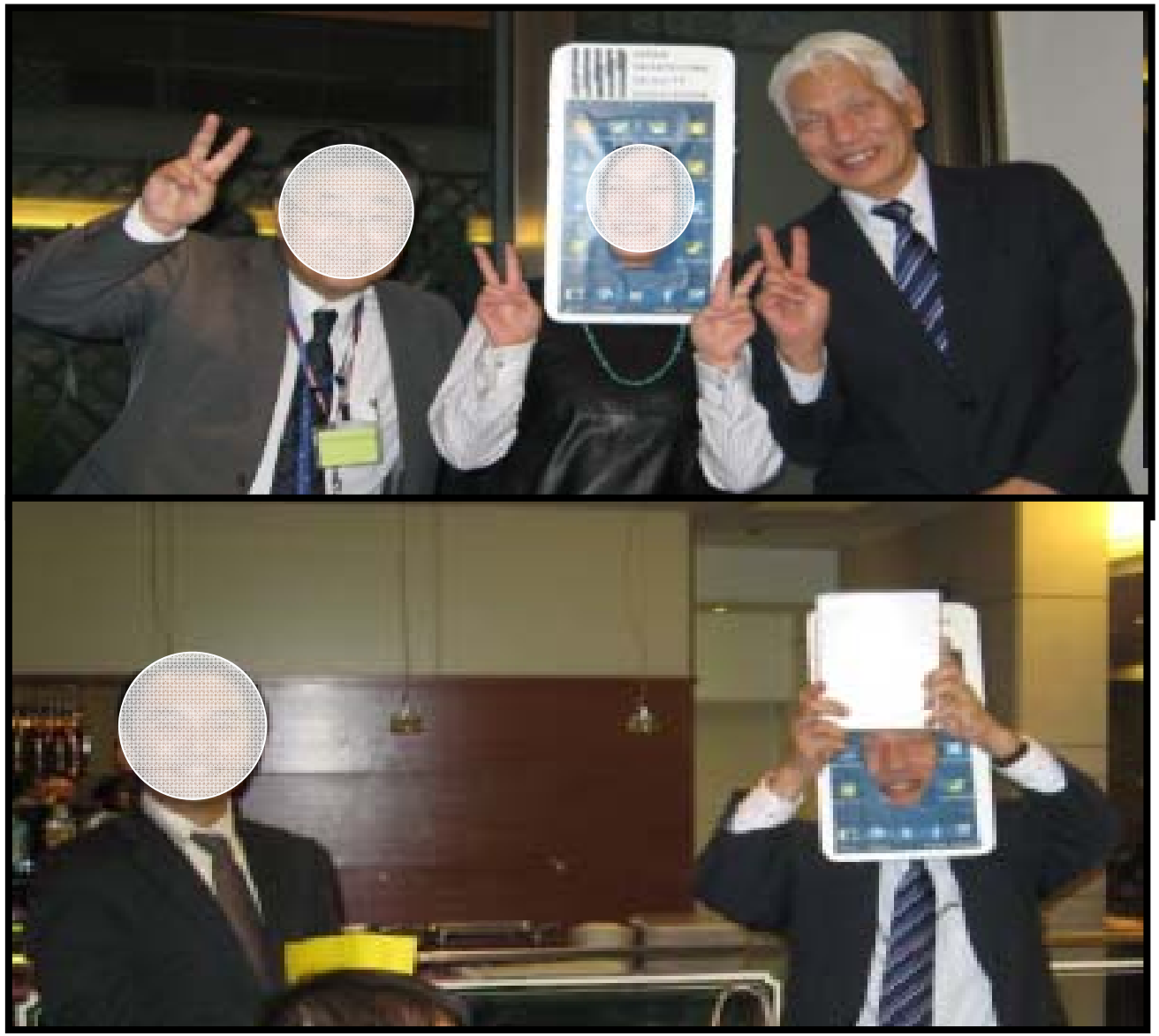
ある日の私　その1

白石イベントWGリーダーの司会進行で飯村PR部会長がカンパイのご発声（練習）！

ご歓談＋ご馳走

安田会長による開式のご挨拶と乾杯！

ある日の私　その2



ある日の私　その3

情報漏洩とネット倫理

他人の情報を意識無く使う

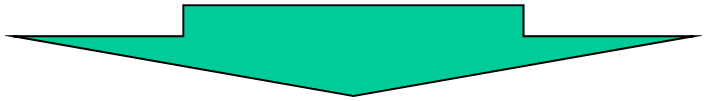
コピペ文化

情報量制限を意識しない

アドレスの乱用

肖像権の侵害等

1984年のテレスクリーンを招きたいのか



教育と免許制

まとめ

新しい脅威と対策

情報自己蓄積→プライベート・アーカイブ
サーバログ解析

映像発信→DMDのCGM化

クラウド活用→認証とプラットフォーム化

悪意ソフト→対応の最新化

BIOS攻撃→BIOSを守る

BYOD→スマホの導入と活用

ネット倫理脅威→教育と免許制

