2009年度第4回ITリスク学研究会　　２０１０年1月１６日

クラウドとITリスク

東京電機大学未来科学部教授
情報セキュリティ研究室
佐々木良一
sasaki@im.dendai.ac.jp

目次案

目次案

クラウドコンピューティングとは

クラウドコンピューティング（Cloud Computing、単にクラウドともいう。クラウドは雲のこと）

米国グーグルのCEO エリック・シュミット（Eric Schmidt）が2006年に最初に利用

いろいろな定義がある中でのIBMの定義：

「ローカル・マシンやリモート・サーバ・ファームではなく、グローバルにアクセス可能な分散されたリソースの集合体を利用するコンピューティング」

NISTの定義 (v15)

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential **characteristics,** three **service models**, and four **deployment models**.

クラウドコンピューティングは、最小の経営努力あるいはサービスプロバイダー間のやり取りで、迅速に準備し提供されうる可変な計算資源 (たとえばネットワーク、サーバー、ストレージ、アプリケーション、サービスなど) の共有されたプールへの便利なオンディマンドネットワークアクセスを可能にするためのモデルである。

このクラウドモデルは可用性を推進するものであり、5つの重要な特徴、3つのサービスモデルそして4つの実現モデルによって構成される。

NIST: National Institute of Standards and Technology

http://csrc.nist.gov/groups/SNS/cloud-computing/index.html

5つの重要な特徴

重要な特徴(Essential Characteristics)	解　説
オンデマンド・セルフサービス On-demand self-service	ユーザーが、プロバイダーの提供するコンピューティング機能(サーバーの使用時間やネットワーク・ストレージなど)を人手を介することなく自動的に割り当てられ、提供されること。
広範なネットワークによる接続 Broad network access	ネットワーク上で利用される標準的なメカニズムを介して、異なるデバイス(携帯電話、ノートパソコン、PDA等)で利用できること。
システム資源のプール Resource pooling	プールされているプロバイダーの物理的なコンピューティング資源を仮想し、ユーザーの要求に応じて、ユーザーごとに独立したシステム単位(マルチテナント)として動的に割り当、再割り当てできること。コンピューティング資源がどこに存在しているかは、ユーザーからは、分らない。ここでいう資源とは、ストレージ、処理能力、メモリ容量、ネットワーク帯域幅、仮想マシンを言う。
迅速な順応性 Rapid elasticity	必要となる資源の増減が、システムによって迅速かつ弾力的に行われる機能を有していること。そして、この対応が自動的に行われること。
従量課金サービス Measured Service	各種サービス機能(例えば、ストレージ、計算処理、帯域幅など)をその使用量に応じて課金する仕組みを持つこと。

http://japan.zdnet.com/blog/netcommerce/2009/10/30/entry_27035197/?ref=rss

クラウドの3つのサービスモデル

ユーザ

（1） アプリケーションを提供
SaaS（Software as a Service）
Salesforce.comやGoogle Gmailなど

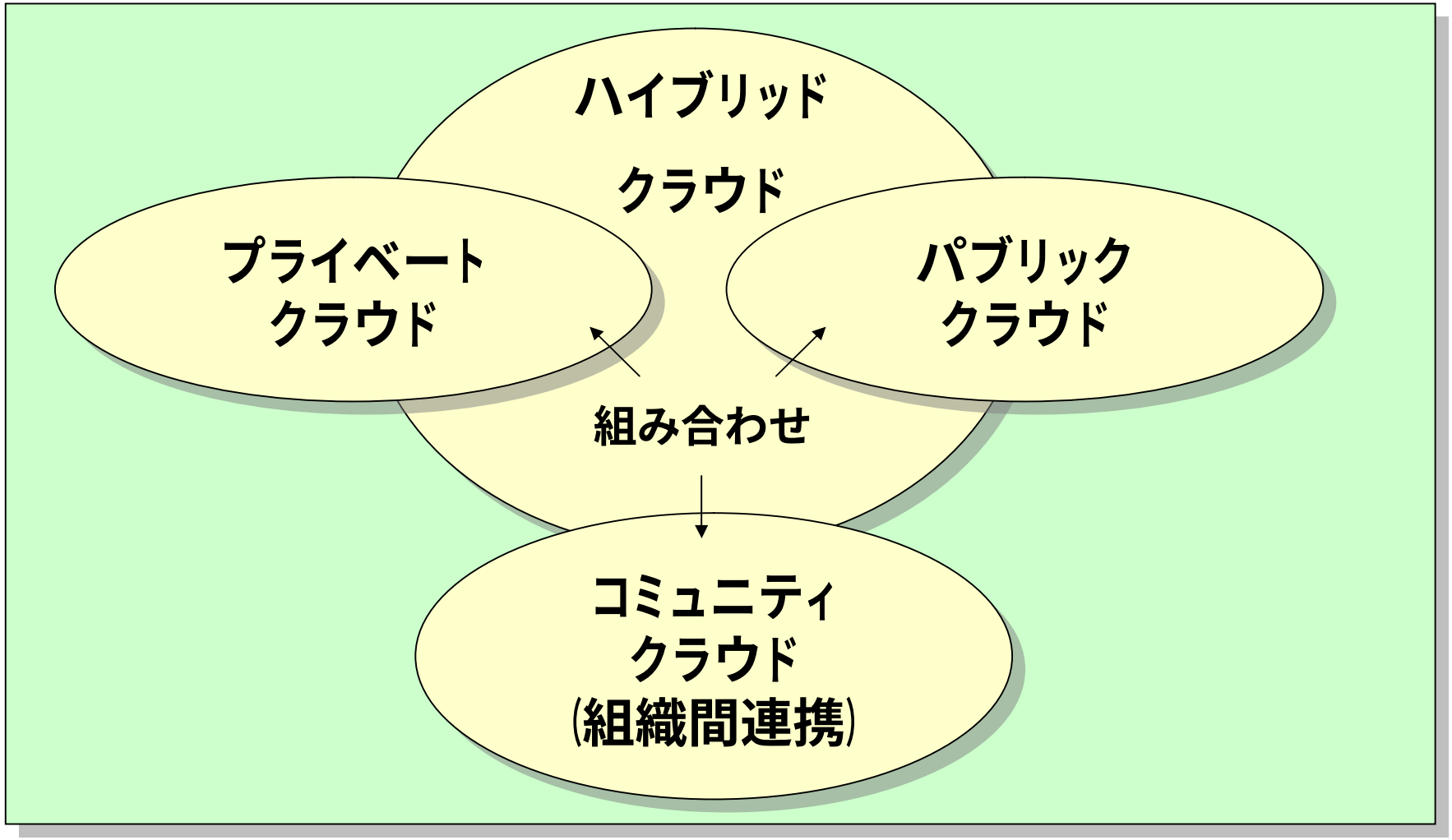
（2） アプリケーション稼働環境等のプラットフォームを提供：PaaS（Platform as a Service）:Google App Engineなど

（3） 仮想ハードウェア及びオペレーティングシステムを提供：IaaS（Infrastructure as a Service）：Amazon S3やEC2など

サービス提供業者

米国NISTの定義より

クラウドの4つの実現モデル



米国NISTの定義より

同床異夢としてのクラウド

(1)　国際的囲い込み戦略としてのクラウド (Googleなど)：
　日本のIT企業から見ると第4のダウンサイジング

(2)　「集中＝＞分散＝＞集中」論者の夢としてのクラウド (旧メインフレイマなど日本のIT業者)：
　自分たちに経験があり、かつ技術力が発揮できる
　　＝＞プライベートクラウド

(3)　いろいろなことが安価に実現できると期待するユーザの立場としてのクラウドなどなど

同床異夢としてのクラウド

(1)　国際的囲い込み戦略としてのクラウド (Googleなど) 日本のIT企業から見ると第4のダウンサイジング
　計算機＝＞ネットワーク＝＞ソフト＝＞SI

(2)　「集中＝＞分散＝＞集中」論者の夢としてのクラウド (旧メインフレイマなど日本のIT業者)：
　自分たちに経験があり、かつ技術力が発揮できる
　　＝＞プライベートクラウド

(3)　いろいろなことが安価に実現できると期待するユーザの立場としてのクラウドなどなど

変質を迫られるIT企業

1．システムインテグレータ：マーケットの喪失＝＞魅力あるプライベートクラウドの提案と安価な提供など

2．ソフトウエアベンダー：ライセンス体系の整備、クラウドを利用した新しいサービスの提供

3．サーバーメーカー：顧客の限定化対応（クラウドに最適化）、価格低下対応（省電力・高信頼化・高セキュリティ化？）など

4．ネットワーク機器ベンダー：クラウド向け製品の提供、価格低下対応（高信頼化・高セキュリティ化？）など

5．レンタルサーバ事業者・ホスティング事業者：マーケットの喪失、価格低下対策（高信用化？）など

城田真琴「クラウドの衝撃」東洋経済新報社、２００９　などを参照

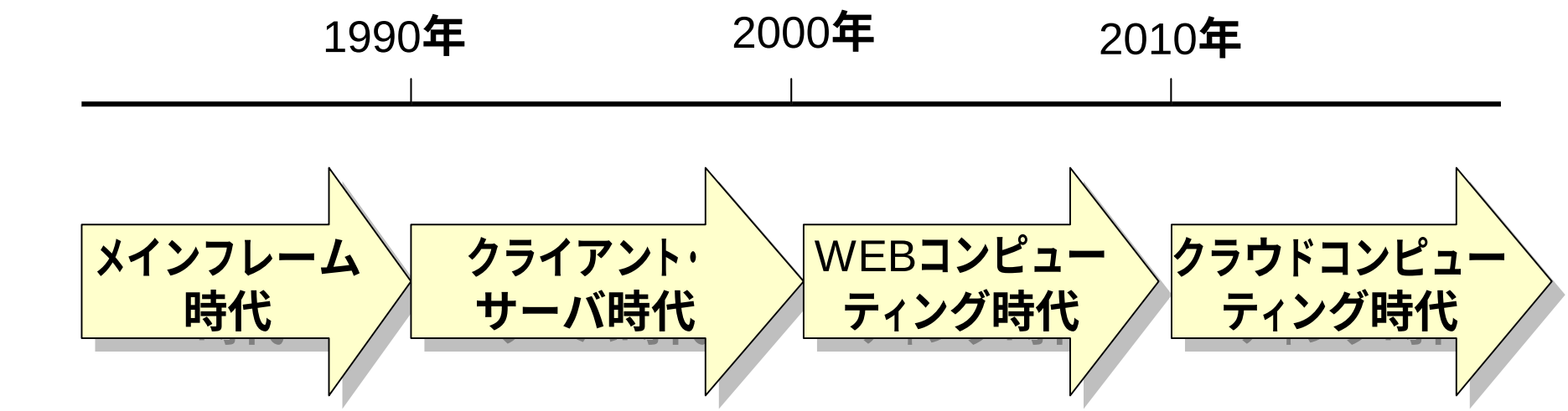
同床異夢としてのクラウド

(1)　国際的囲い込み戦略としてのクラウド (Googleなど)：
　日本のIT企業から見ると第4のダウンサイジング

(2)　「集中＝＞分散＝＞集中」論者の夢としてのクラウド (旧メインフレイマなど日本のIT業者)：
　自分たちに経験があり、かつ技術力が発揮できる
　　＝＞プライベートクラウド

(3)　いろいろなことが安価に実現できると期待するユーザの立場としてのクラウドなどなど

コンピューティングシステムの変遷



集中

分散

1964年IBM System/360

1981年 IBM PC

1991年Linux公開

1995年Win95

WEBサービス普及

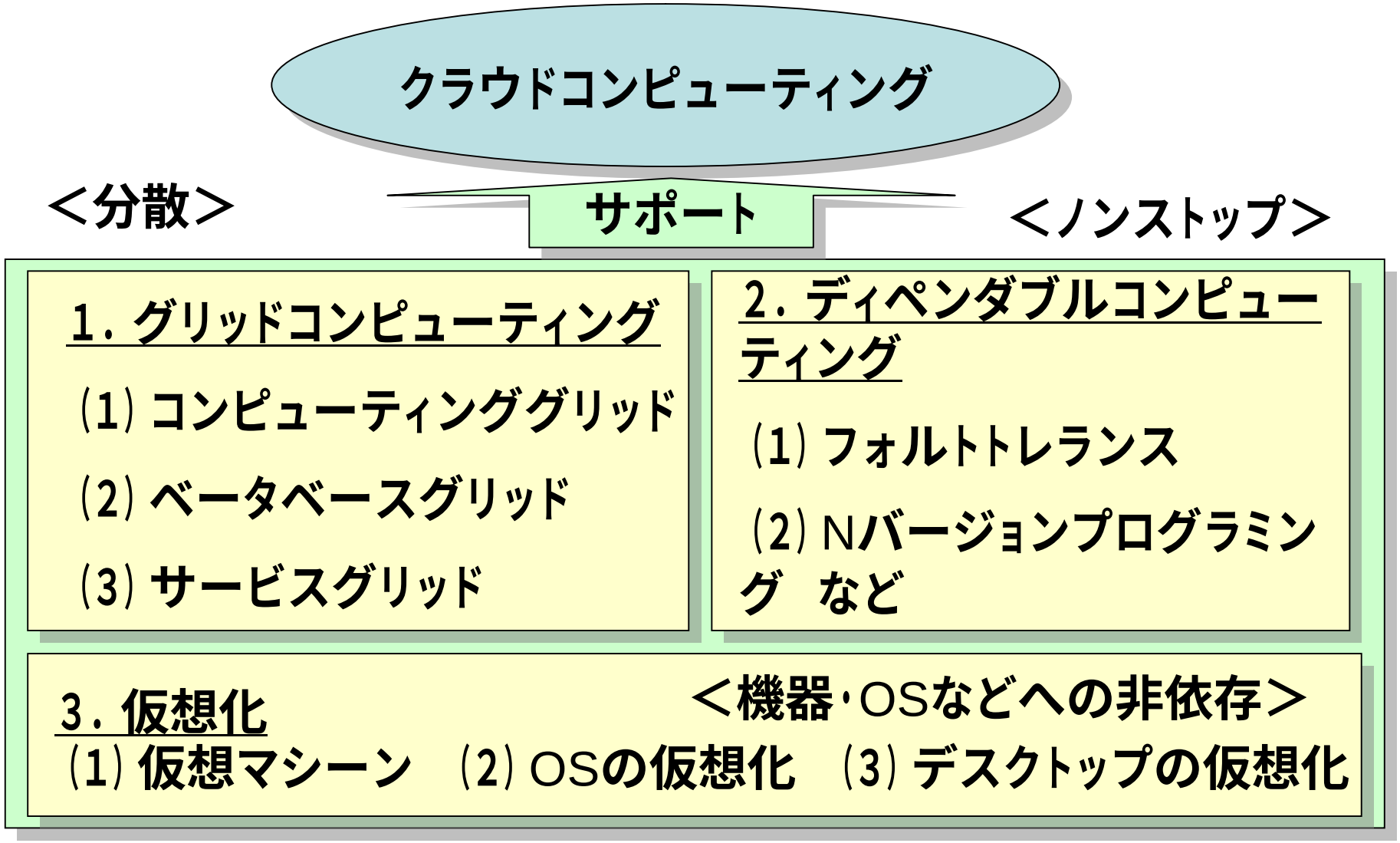
1998年 Google創業

1999年セールスフォースドットコム創業

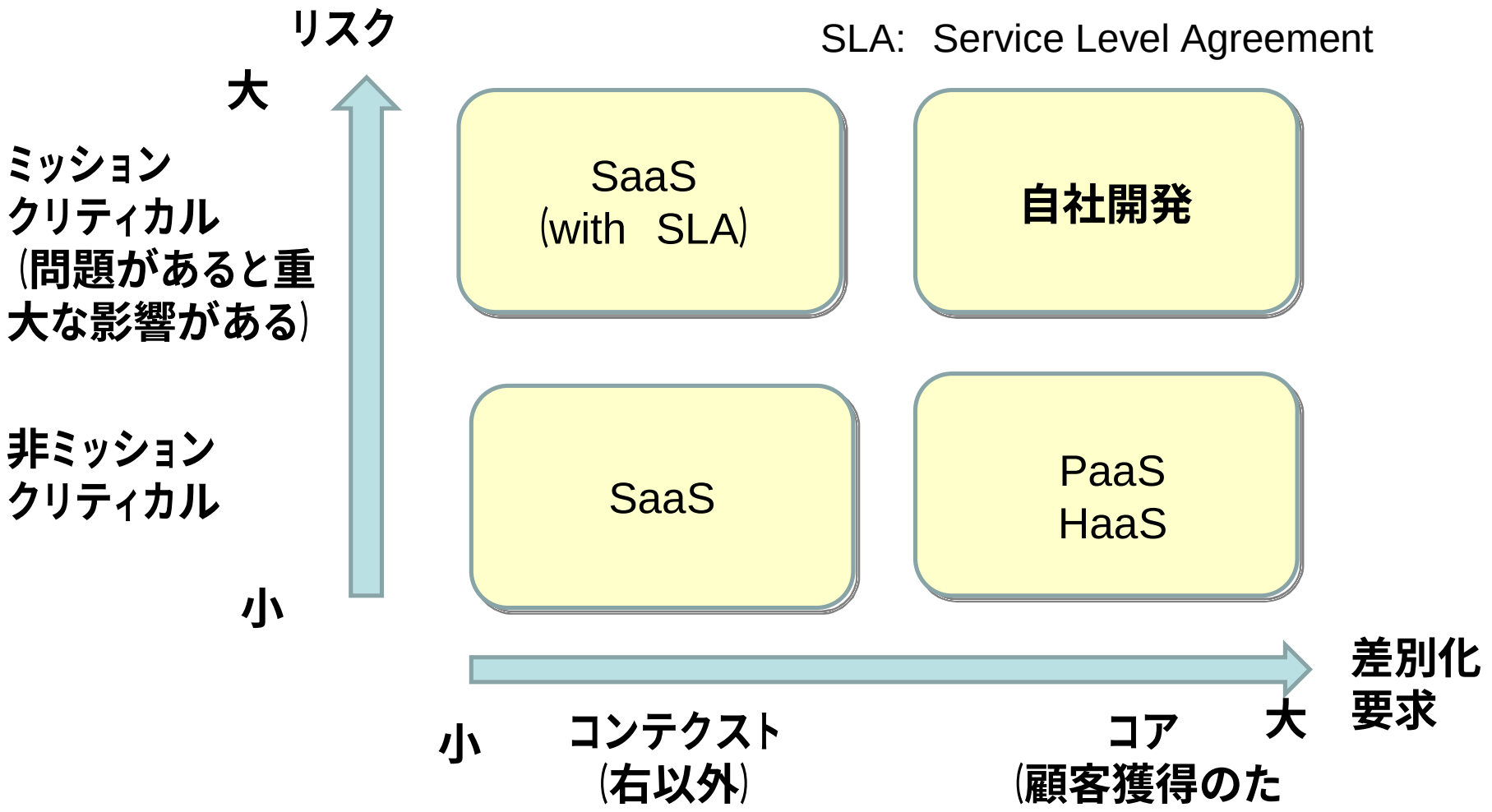
2008年 Googleアップエンジン開始

城田真琴「クラウドの衝撃」東洋経済新報社、2009　などを参照

クラウド実現のための基本技術

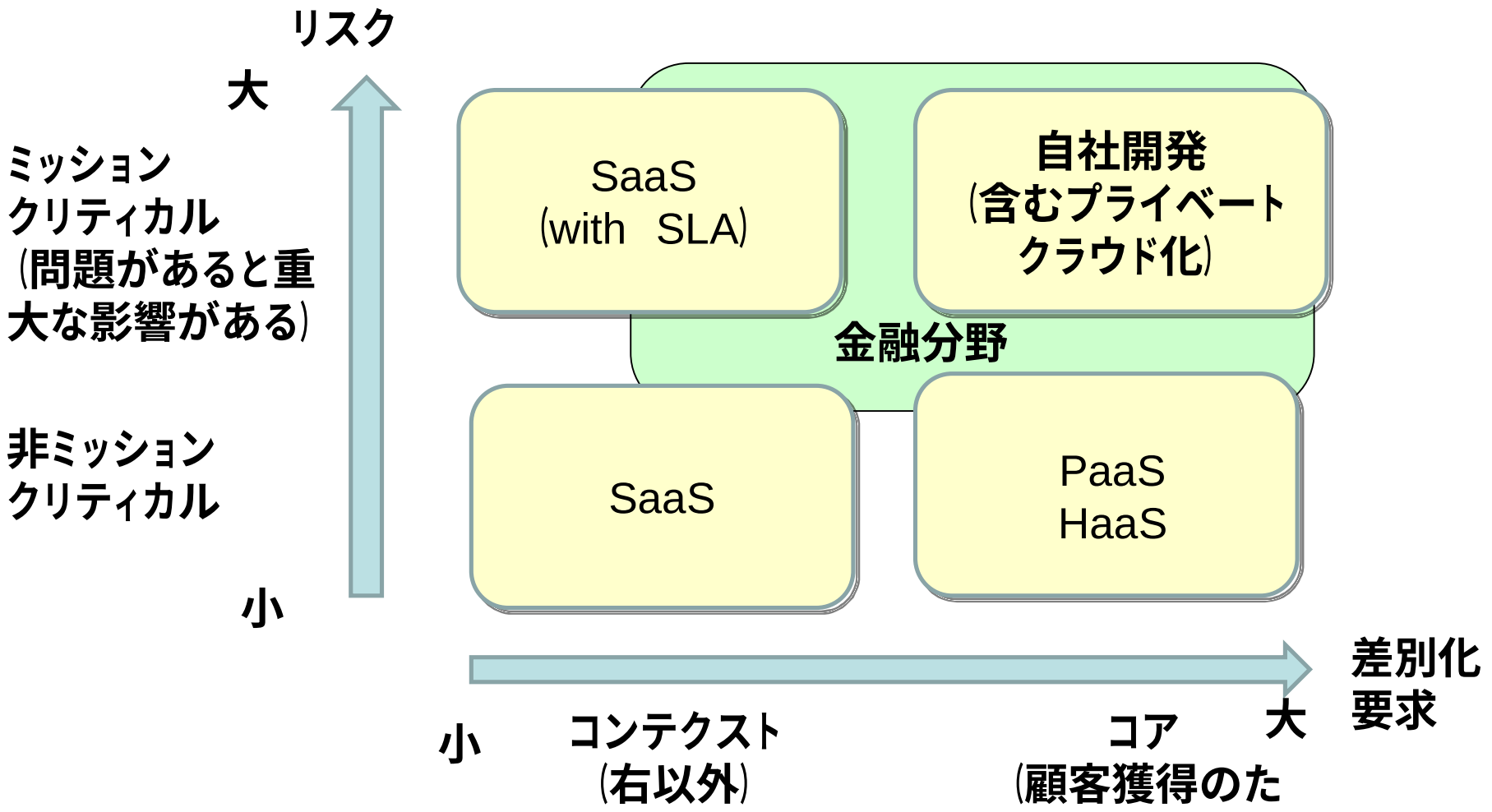


クラウドの適用領域



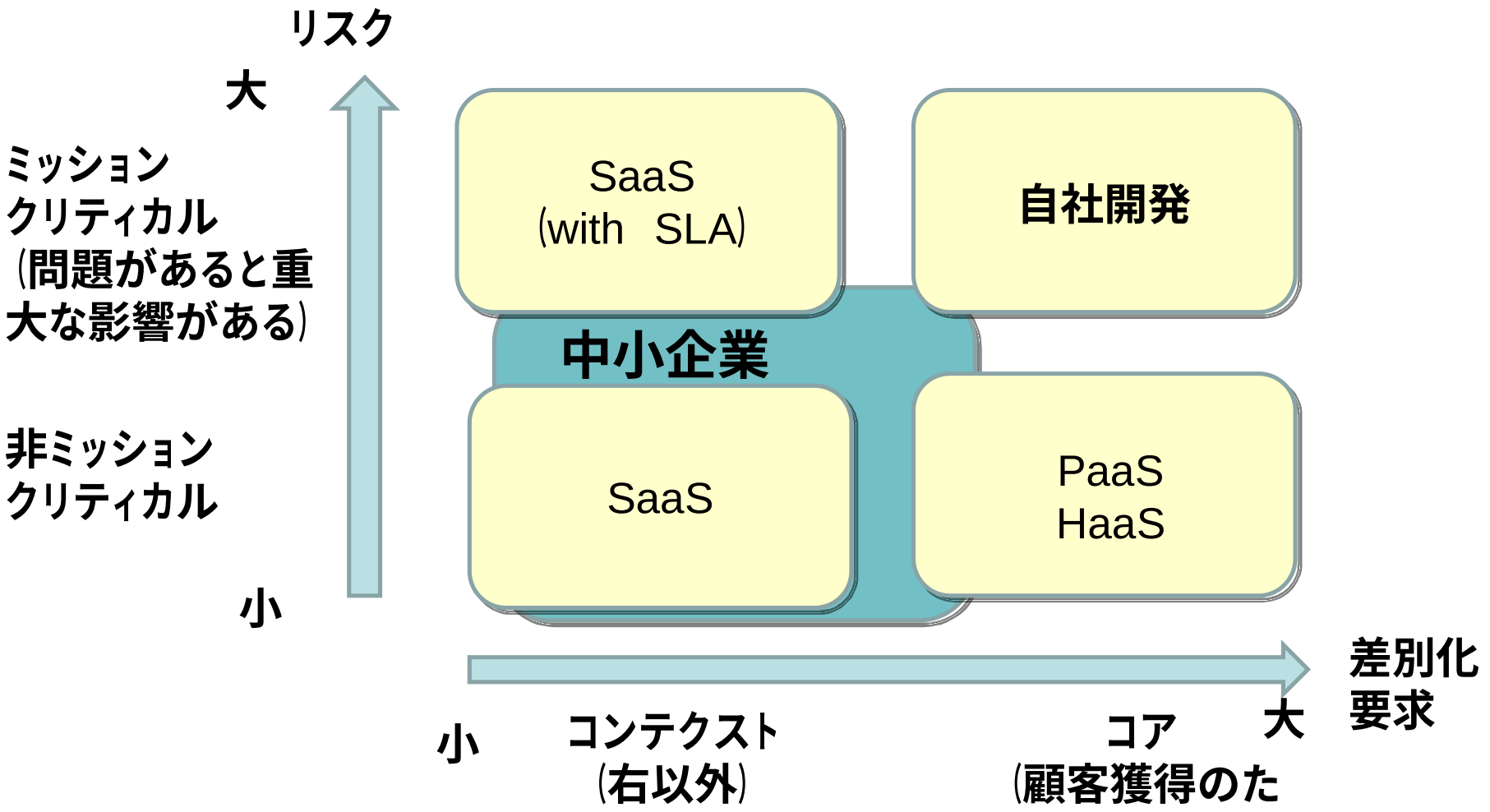
城田真琴「クラウドの衝撃」東洋経済新報社、2009
をベースに一部修正

金融におけるクラウドの適用領域



城田真琴「クラウドの衝撃」東洋経済新報社、2009
をベースに一部修正

中小企業のクラウドの適用領域

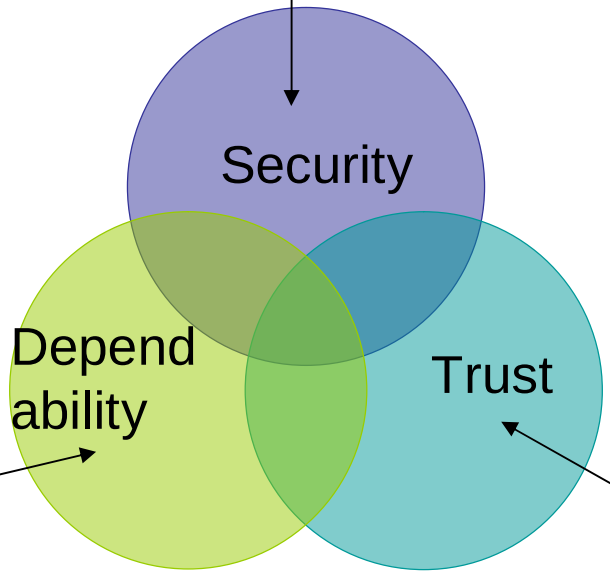


城田真琴「クラウドの衝撃」東洋経済新報社、2009
をベースに一部修正

目次案

クラウドの安全･安心のための課題
＜ITリスク克服のために＞

①外部や内部からの攻撃に対するセキュリティ対策
(a) クラウドへの攻撃　(b) 利用者の装置への攻撃

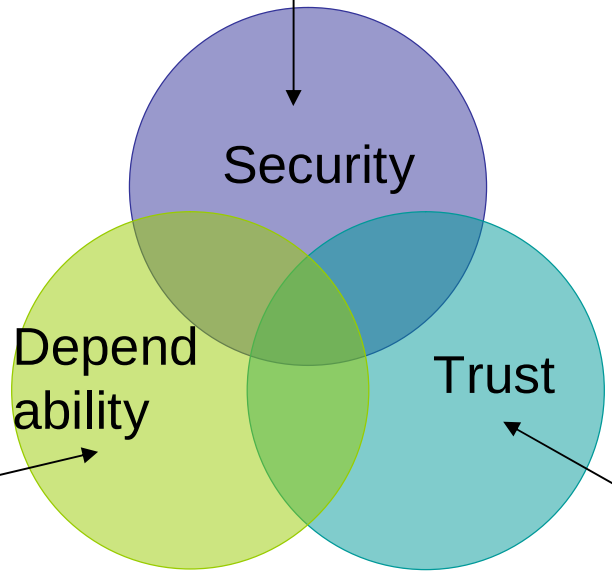


②バグや故障･災害などへの対策
(a) システムの停止
(b) データの喪失
(c) 誤処理

③サービス提供者へのトラストの確保対策
(a) 将来にわたりサービスしてもらえるか
(b) データの目的外使用や不正処理をしていないか
(c) 政府などによる検閲のある国で処理してないか
(d) 障害や不正があったとき調査などに協力してもらえるか

クラウドの安全･安心のための課題

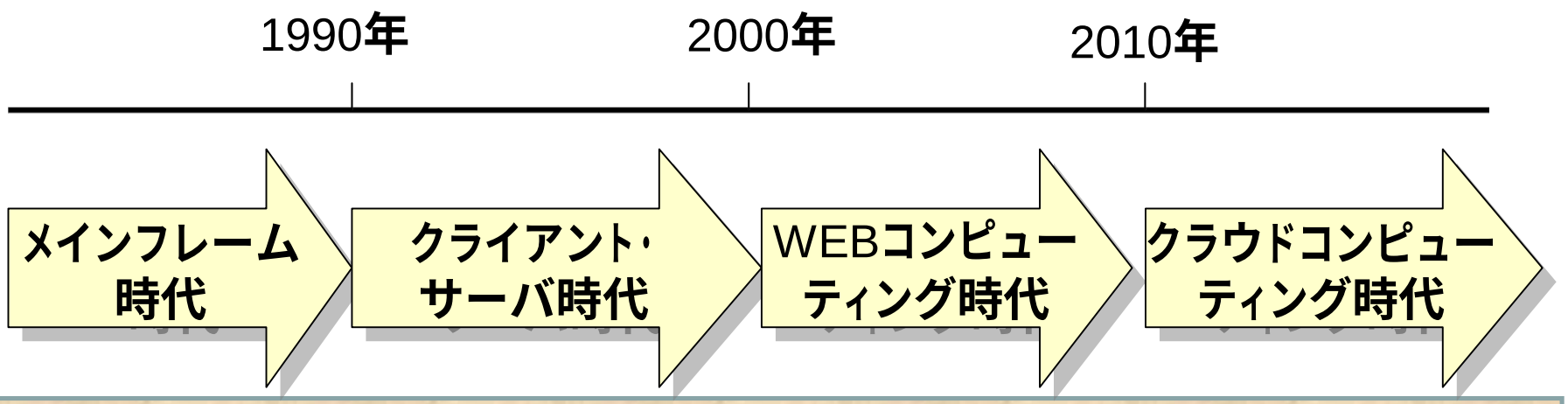
①外部や内部からの攻撃に対するセキュリティ対策
(a) クラウドへの攻撃　(b) 利用者の装置への攻撃

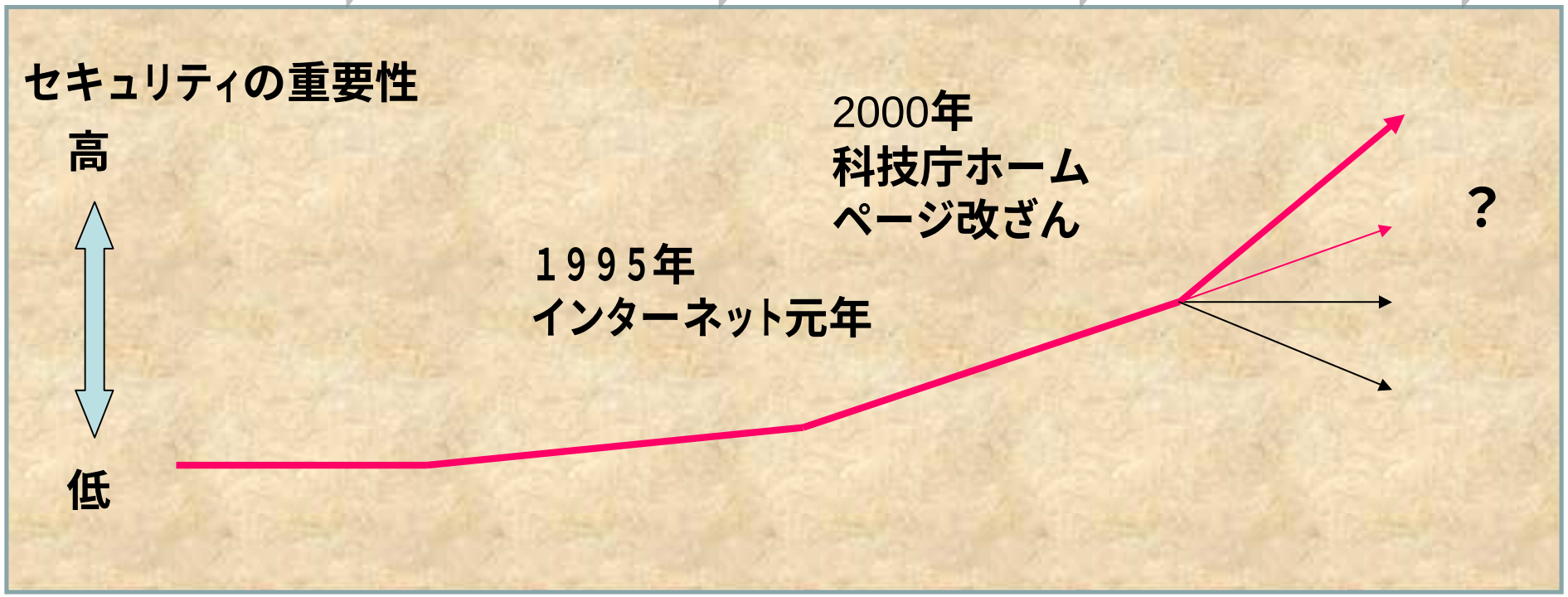


②バグや故障･災害などへの対策
(a) システムの停止
(b) データの喪失
(c) 誤処理

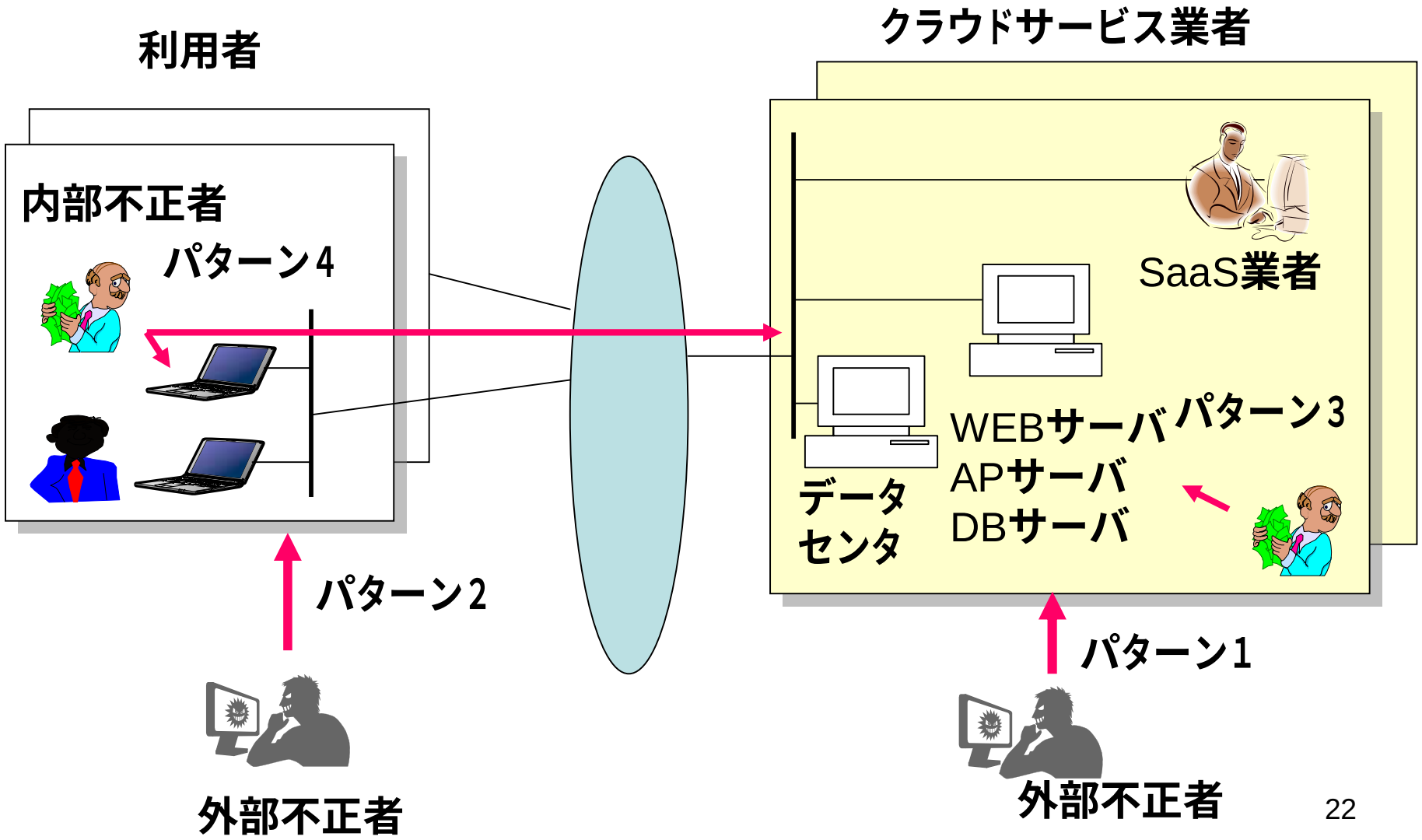
③サービス提供者へのトラストの確保対策
(a) 将来にわたりサービスしてもらえるか
(b) データの目的外使用や不正処理をしていないか
(c) 政府などによる検閲のある国で処理してないか
(d) 障害や不正があったとき調査などに協力してもらえるか

セキュリティの重要性


1990年
2000年
2010年
メインフレーム時代
クライアント・サーバ時代
WEBコンピューティング時代
クラウドコンピューティング時代


セキュリティの重要性
高
低
2000年
科技庁ホームページ改ざん
1995年
インターネット元年
？

セキュリティに対する攻撃パターン

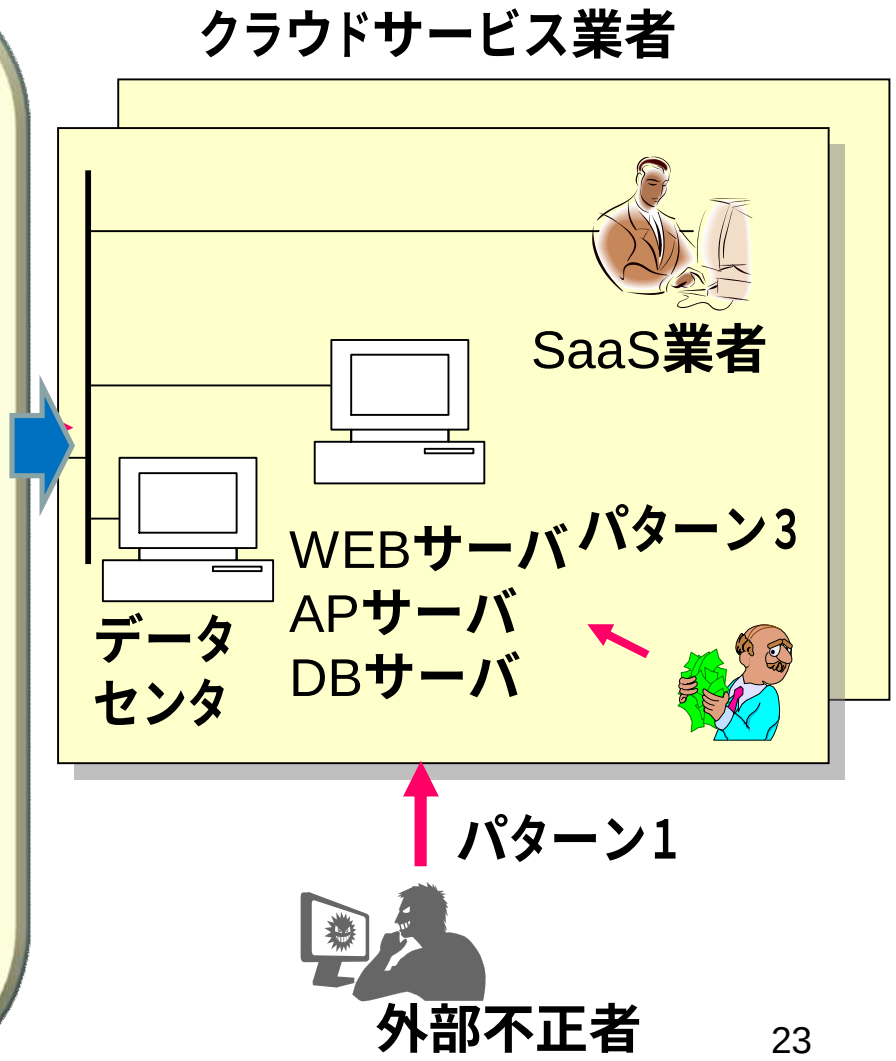


セキュリティ対策の特徴(1)

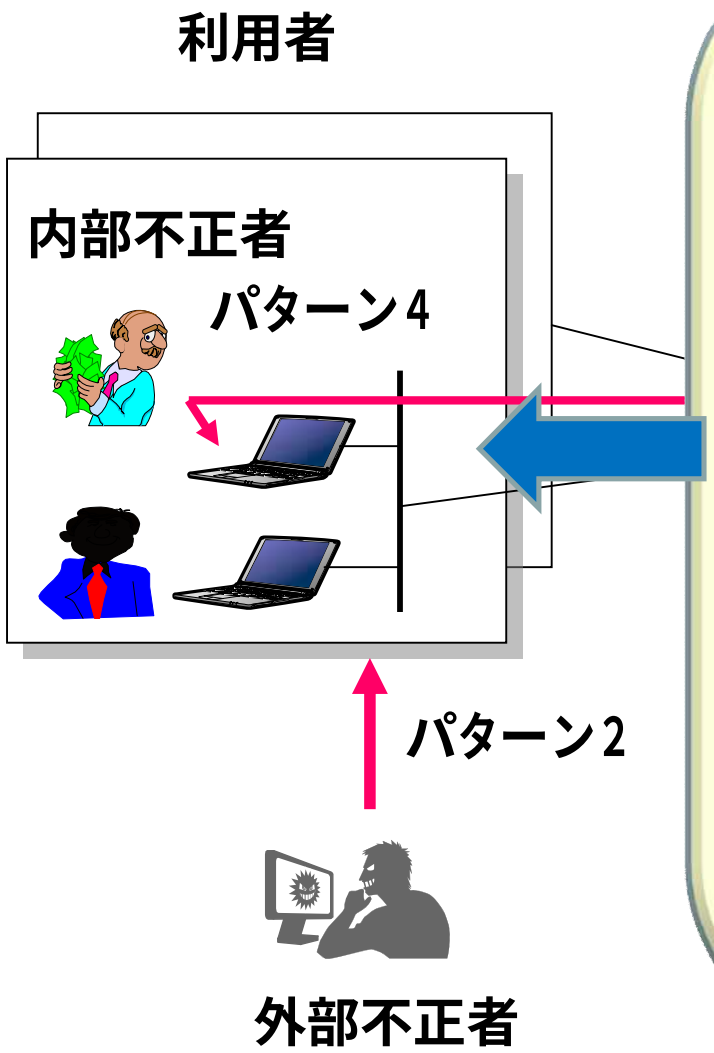
必要な主要対策
　　(a) 入退出管理、監視カメラなどの物理的対策
　　(b) アクセス制御、暗号化、セキュリティ監視などの情報処理的対策
　　(c) セキュリティ管理、監査などの管理的対策　他

① 一般企業と必要な対策は基本的に同じ

② 説明責任を果たすためログの収集などの対策は一般により強く要求される



セキュリティ対策の特徴(2)



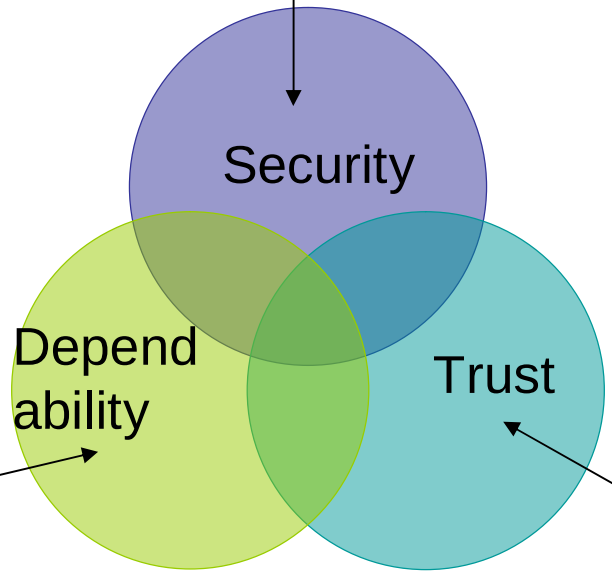
必要な主要対策
(a) セキュリティ監視
(b) セキュリティ教育　他

① これらの企業にもクライアントＰＣなどは残るが、それに対するセキュリティ対応能力はどんどん落ちると考えられ、ここへの攻撃が問題になりうる。

② セキュリティトータルサービスのクラウド化：検疫ネットやセキュリティ監視、セキュリティ応急対応と組み合わせたEnd-Endセキュリティサービスのクラウド化は大きなビジネスチャンスになりうる

クラウドの安全・安心のための課題

①外部や内部からの攻撃に対するセキュリティ対策
(a) クラウドへの攻撃　(b) 利用者の装置への攻撃



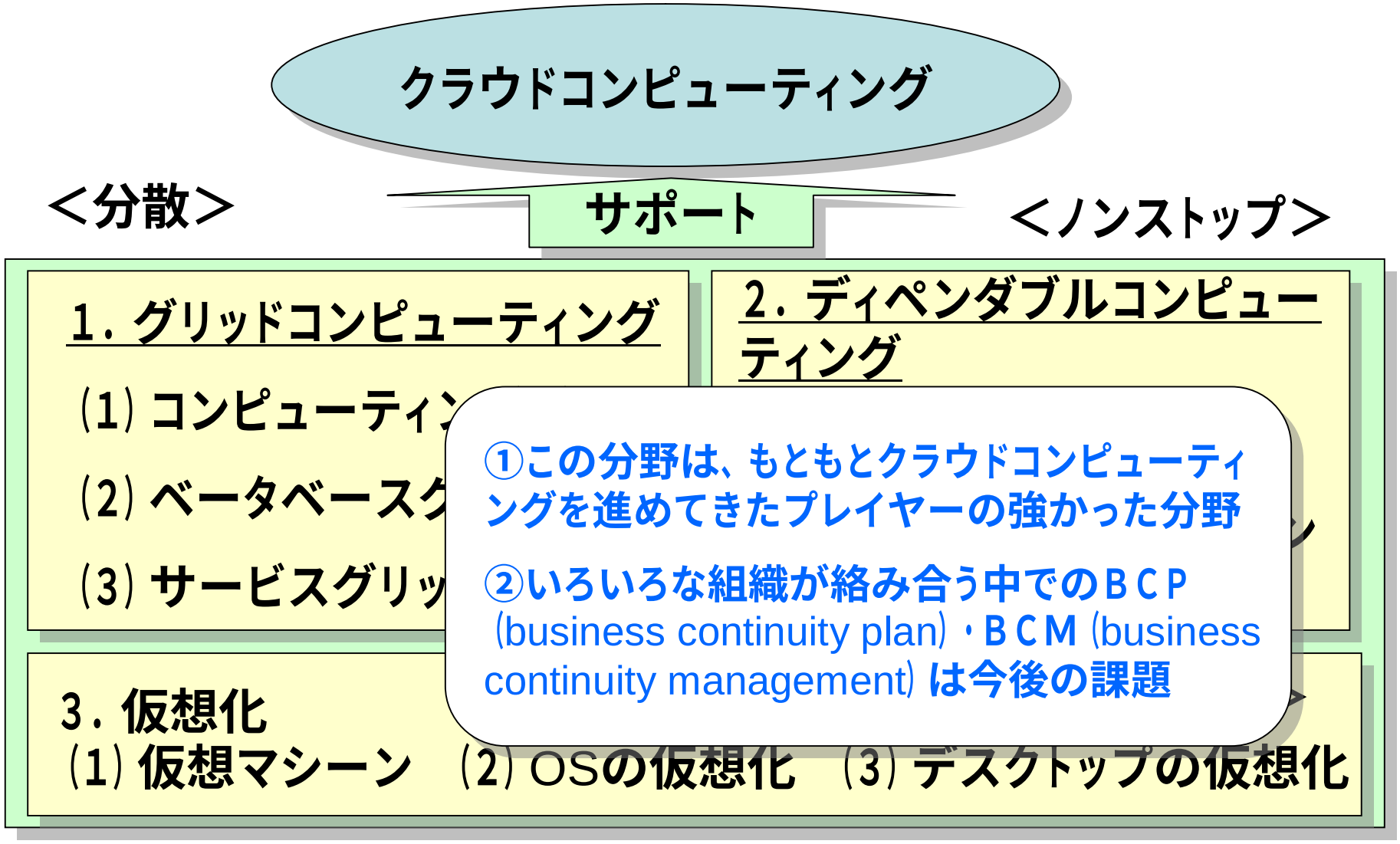
②バグや故障・災害などへの対策
(a) システムの停止
(b) データの喪失
(c) 誤処理

③サービス提供者へのトラストの確保対策
(a) 将来にわたりサービスしてもらえるか
(b) データの目的外使用や不正処理をしていないか
(c) 政府などによる検閲のある国で処理してないか
(d) 障害や不正があったとき調査などに協力してもらえるか

バグや障害・災害などへの対策

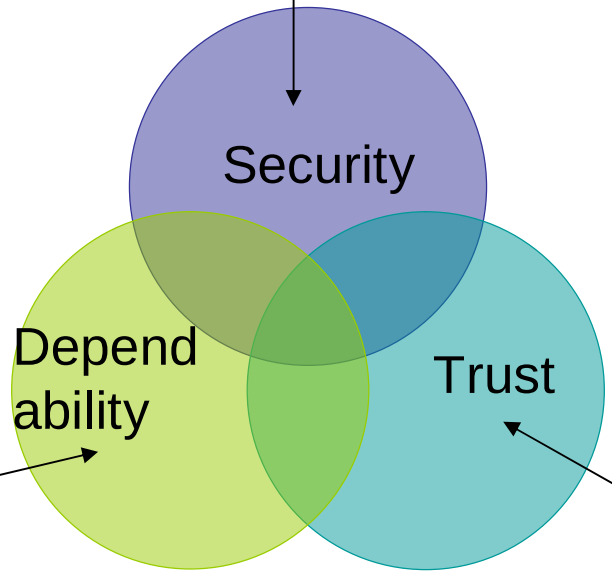
1．通常時対策
　(1) 機能更新時の変更管理
　(2) 分散環境におけるデータの同一性保持
　(3) 負荷変動への対応機能 (分散処理技術、サーバ仮想化技術)
2．障害回避対策 (フォルトアボイダンス)
　(4) バグの少ないソフトの導入など
3．障害時対策 (フォルトトレランス)
　(6) 計算機やネットワーク機能の多重化 (フォルトトレランス)
　(7) データのバックアップ (消去対応、アーカイビング)
　(8) 地震などに備えたバックアップセンターの設置 (ディザスタリカバリー)
　(9) ＢＣＰ・ＢＣＭの推進

クラウド実現のための基本技術



クラウドの安全・安心のための課題

①外部や内部からの攻撃に対するセキュリティ対策
(a) クラウドへの攻撃　(b) 利用者の装置への攻撃



②バグや故障・災害などへの対策
(a) システムの停止
(b) データの喪失
(c) 誤処理

③サービス提供者へのトラストの確保対策
(a) 将来にわたりサービスしてもらえるか
(b) データの目的外使用や不正処理をしていないか
(c) 政府などによる検閲のある国で処理してないか
(d) 障害や不正があったとき調査などに協力してもらえるか

サービス提供者へのトラストの確保

＜トラスト＞

(a) 将来にわたってサービスをしてもらえるか

(b) データの目的外使用や不正処理をしていないか

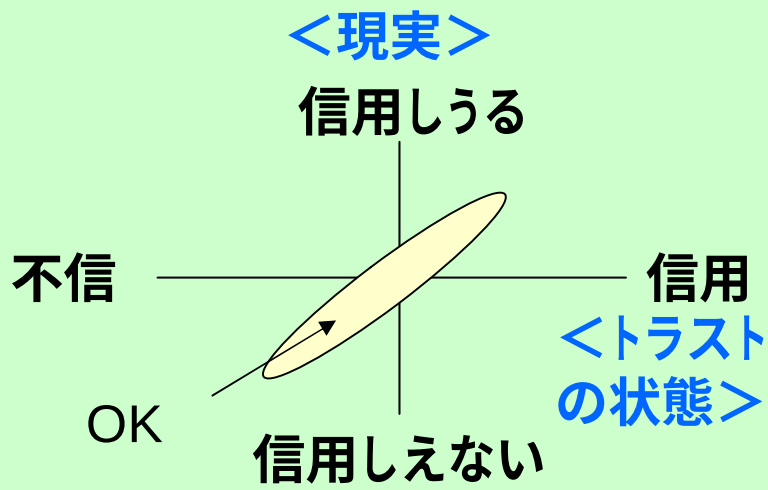
(c) 希望する安全レベルが確保されているか

(d) 政府などによる検閲のある国で処理してないか

(e) 障害や不正があったとき調査などに十分協力してもらえるか

＜トラストの実現形態＞

①トラストの状態と現実が一致



②実際により信用できる状態を実現

＜実現手段＞

契約

運用

仕組み

技術

サービス提供者へのトラストの確保

＜トラスト＞

(a) 将来にわたってサービスをしてもらえるか

(b) データの目的外使用や不正処理をしていないか

(c) 希望する安全レベルが確保されているか

(d) 政府などによる検閲のある国で処理してないか

(e) 障害や不正があったとき調査などに十分協力してもらえるか

＜実現手段＞

(a) 契約によるもの (①サービスレベルアグリーメント、②ガイドラインなど)

(b) 運用によるもの (①BCP,BCM　②コンプライアンス、③証拠性保全、④監視体制など)

(c) 仕組みによるもの (監査、監視など)

(d) 技術によるもの (①暗号プロトコル、②耐タンパー装置、③デジタルフォレンジック技術、④E-Discovery技術など)

サービス提供者へのトラストの確保

＜トラスト＞

(a) 将来にわたってサービスをしてもらえるか

(b) データの目的外使用や不正処理をしていないか

(c) 希望する安全レベルが確保されているか

(d) 政府などによる検閲のある国で処理してないか

(e) 障害や不正があったとき調査などに十分協力してもらえるか

＜実現手段＞

(a) 契約によるもの (①サービスレベルアグリーメント、②ガイドラインなど)

(b) 運用によるもの (①BCP,BCM　②コンプライアンス、③証拠性保全、④監視体制など)

(c) 仕組みによるもの (監査、監視など)

(d) 技術によるもの (①暗号プロトコル、②耐タンパー装置、③デジタルフォレンジック技術、④E-Discovery技術など)

SLA の構成要素とSaaS 用サービスレベル項目

SLA 構成要素	構成要素の概要
前提条件	サービスレベルに影響を及ぼす業務上／システム上の前提条件
委託範囲	合意された委託内容がカバーする範囲
役割と責任	利用者と SaaS 提供者の役割と責任を明確化した分担表
サービスレベル項目	管理対象となるサービス別に設定される評価項目および要求水準
結果対応	サービスレベルが達成されなかった場合の対応方法（補償）
運営ルール	利用者と SaaS 提供者間のコミュニケーション（報告・連絡）のルール／体制

分類	項目の概要
アプリケーション運用	システムの使い勝手に関わる項目（可用性／信頼性／性能／拡張性）
サポート	障害対応や一般的問合せ対応に関わる項目
データ管理	データバックアップを含む利用者データの保証に関わる項目
セキュリティ	公的認証や第三者評価（監査）を含むセキュリティに関わる項目

経済産業省「SaaS 向けSLA ガイドライン」より

サービス提供者へのトラストの確保

＜トラスト＞

(a) 将来にわたってサービスをしてもらえるか

(b) データの目的外使用や不正処理をしていないか

(c) 希望する安全レベルが確保されているか

(d) 政府などによる検閲のある国で処理してないか

(e) 障害や不正があったとき調査などに十分協力してもらえるか

＜実現手段＞

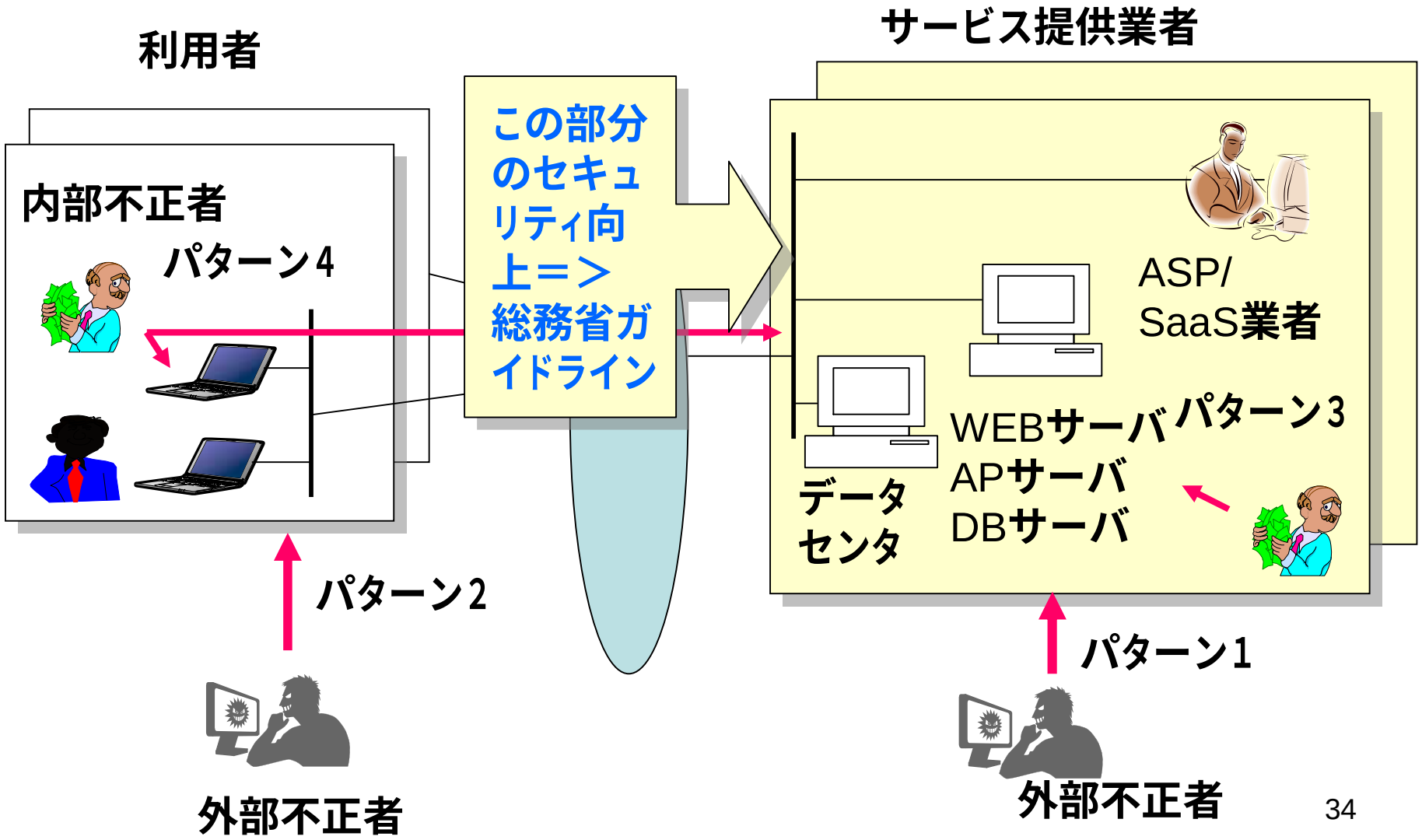
(a) 契約によるもの (①サービスレベルアグリーメント、②ガイドラインなど)

(b) 運用によるもの (①BCP,BCM　②コンプライアンス、③証拠性保全、④監視体制など)

(c) 仕組みによるもの (監査、監視など)

(d) 技術によるもの (①暗号プロトコル、②耐タンパー装置、③デジタルフォレンジック技術、④E-Discovery技術など)

総務省によるガイドライン



総務省における委員会

ＡＳＰ・ＳａａＳの情報セキュリティ対策に関する研究会（平成19年度）

目的：適切な情報セキュリティ対策が施されたＡＳＰ・ＳａａＳサービスの提供が促進され、企業等の生産性向上の健全な基盤となるよう、ＡＳＰ・ＳａａＳ事業者が講じるべき情報セキュリティ対策を検討

主要な実施事項：「ＡＳＰ・ＳａａＳにおける情報セキュリティ対策ガイドライン」の策定

座長　佐々木良一

座長代理　中尾康二　座長代理　藤本 正代

ガイドラインに関する基本的考え方

● 『ASP・SaaS事業者が、提供するサービスの特徴に基づいた適切な情報セキュリティ対策の実施を検討する際の具体的な指針』と位置づけ、ASP・SaaS事業者の実態や提供サービスの特性を反映した、新たな情報セキュリティ対策ガイドラインを策定。

ASP・SaaSの情報セキュリティ対策の現状と課題

○ ASP・SaaS事業者及びサービスの特性を反映し、「どこに」「何を」「どの程度」実施すべきかを示した情報セキュリティ対策の指針がない

- 情報セキュリティ対策の優先付けがされていない
- 提供するASP・SaaSサービスの特徴に基づいた、適切な情報セキュリティ対策の実施がされていない

情報セキュリティ対策ガイドラインへの期待

- 利用者がASP・SaaSサービスを適切に選別できるような判断基準としての役割
- 様々な規模のASP・SaaS事業者への対応
- 新規に参入するASP・SaaS事業者にとっての指南書としての役割

ガイドライン策定にあたっての重点ポイント

○ ASP・SaaS事業者及びサービスの特性を反映し、優先的に取り組むべき情報セキュリティ対策を絞り込む

○ ガイドラインをそのまま利用することで、比較的簡単に自ら提供するサービスに即した情報セキュリティ対策を実施可能にする

○ ASP・SaaS事業者が理解および実施しやすい具体的な情報セキュリティ対策を示す

○ 利用者にとっての理解しやすさも考慮する

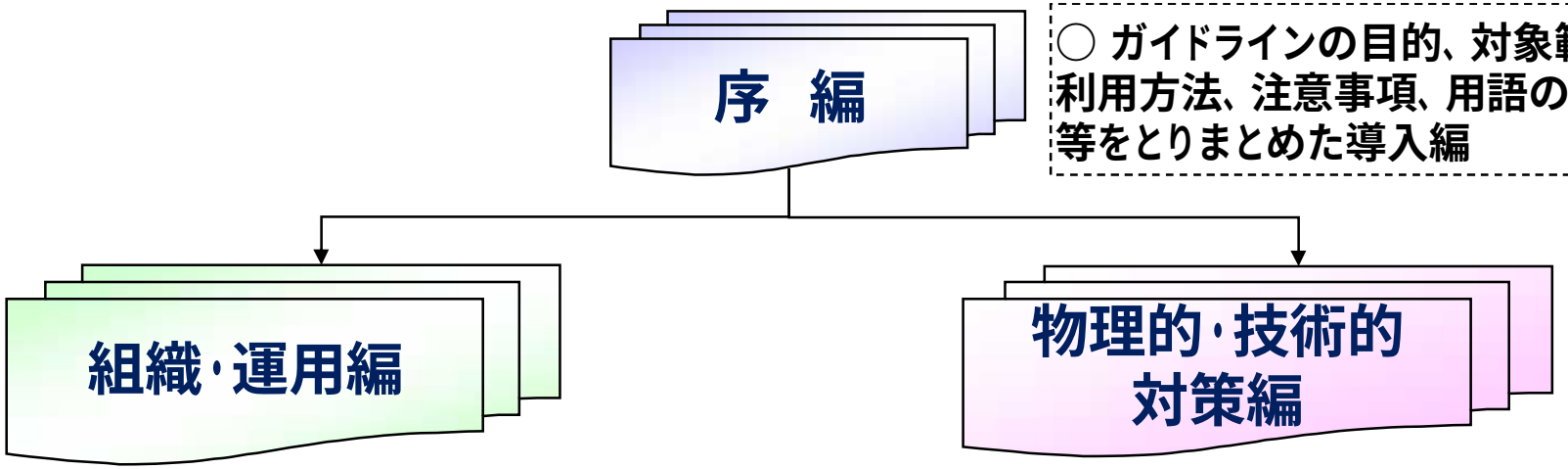
本ガイドラインを足がかりとして、ASP・SaaS事業者における情報セキュリティマネジメントシステムの確立、導入、運用、監視、見直しが実施され、継続的に情報セキュリティ対策が改善されていくことを期待

ASP・SaaSの情報セキュリティ対策に関する研究会報告書より

ＡＳＰ・SaaSにおける
情報セキュリティ対策ガイドラインの策定

● ASP・SaaS事業者がASP・SaaSサービスを提供する際、実施すべき情報セキュリティ対策全般を対象※。
● 積極的かつ幅広い利用を促すため、可能な限り分かりやすく、かつ使いやすいものになるように留意して作成しており、「序編」、「組織・運用編」及び「物理的・技術的対策編」の3編から構成。

「ASP・SaaSにおける情報セキュリティ対策ガイドライン」の構成



○ ガイドラインの目的、対象範囲、利用方法、注意事項、用語の定義等をとりまとめた導入編

○ 運用管理体制・外部組織との契約における留意事項、利用者に対する責任等、組織・運用に係る情報セキュリティ対策をとりまとめた対策集

○ 主として、経営者等の組織管理者によって参照されることを想定

○ ASP・SaaSの典型的なシステム構成を基に、アプリケーション、ネットワーク、建物・電源等の構成要素における情報資産に対する情報セキュリティ対策をとりまとめた対策集
○ 主として、ASP・SaaSサービスを運用する現場の技術者等によって参照されることを想定

※ ASP・SaaSの情報セキュリティ対策に関する研究会報告書より

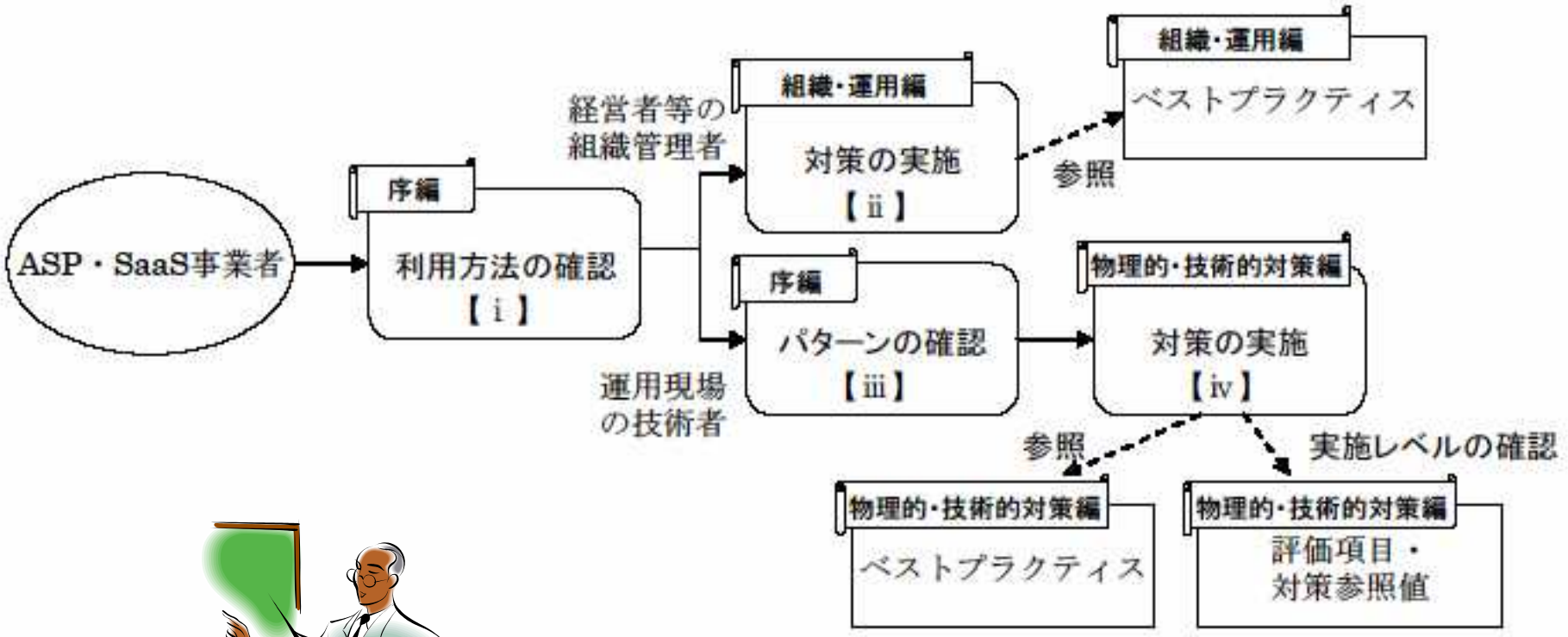
パターン化

パターン	セキュリティへの要求			サービス種別の例
	C	I	A	
1	高	高	高	受発注、ネットショッピング支援、電子入札、他
2	高	高	中	販売管理、公共窓口業務、在庫管理、他
3	高	高	低	販売支援、契約、採用管理、メール配信、他
4	低	高	高	ネットワーク監視
5	低	高	中	ECサポート（産地直送など）
6	低	高	低	広告、IT資産管理、ニュースリリース業務、他

C：機密性　I：完全性　A：可用性

ASP・SaaSの情報セキュリティ対策に関する研究会報告書より

利用パターン



ASP・SaaSの情報セキュリティ対策に関する研究会報告書より

セキュリティガイドの一例

重要な物理的セキュリティ境界に対して監視カメラを設置し、その稼働時間と監視範囲を定めて監視を行うこと。また、監視カメラの映像を予め定められた期間保存すること。

【ベストプラクティス】

i. 監視性を高めるため、死角を作らないことが望ましい。

ii. 監視カメラは、カラー撮影であり、デジタル記録が可能であることが望ましい。

iii. 監視カメラは用途に応じて十分な解像度を持つことが望ましい。

iv. 監視カメラは、撮影日時が画像内に時分秒まで記録可能であることが望ましい。

v. 非常時に防犯機関等への通報ができる非常通報装置を併設することが望ましい。

vi. 重要な物理的セキュリティ境界においては、個人認証システムと併設することが望ましい。

監視映像保存期間

パターン	対策参照値
1	6ヶ月
2	1ヶ月
3	1週間
4	-
5	-
6	-

ASP・SaaSの情報セキュリティ対策に関する研究会報告書より

サービス提供者へのトラストの確保

＜トラスト＞

(a) 将来にわたってサービスをしてもらえるか

(b) データの目的外使用や不正処理をしていないか

(c) 希望する安全レベルが確保されているか

(d) 政府などによる検閲のある国で処理してないか

(e) 障害や不正があったとき調査などに十分協力してもらえるか

＜実現手段＞

(a) 契約によるもの (①サービスレベルアグリーメント、②ガイドラインなど)

(b) 運用によるもの (①BCP,BCM　②コンプライアンス、③証拠性保全、④監視体制など)

(c) 仕組みによるもの (監査、監視など)

(d) 技術によるもの (①暗号プロトコル、②耐タンパー装置、③デジタルフォレンジック技術、④E-Discovery技術など)

将来必要になりうる技術

(1) 狭義のセキュリティに関連して
クラウドユーザのための検疫ネットやセキュリティ監視、セキュリティ応急対応と組み合わせたEnd-Endセキュリティサービス技術

(2) ディペンダビリティに関連して
いろいろな組織が絡み合う中でのＢＣＰ (business continuity plan)・ＢＣＭ (business continuity management) 技術

(3) トラストに関連して
クラウドサービス提供業者のようなサーバなどの管理者であっても不正を行えばすぐにわかる技術。サーバの管理者であれば記録の消去などいろいろな処理を行い得るのでその実現は簡単ではないが重要な技術である。

クラウド環境下ではデジタルフォレンジックが大切に

有罪！

不正は
していない
のに．．．

証拠保全システム

手術

複数
装置
からの
入力

種々の装置を利用した適切な作業記録　＋

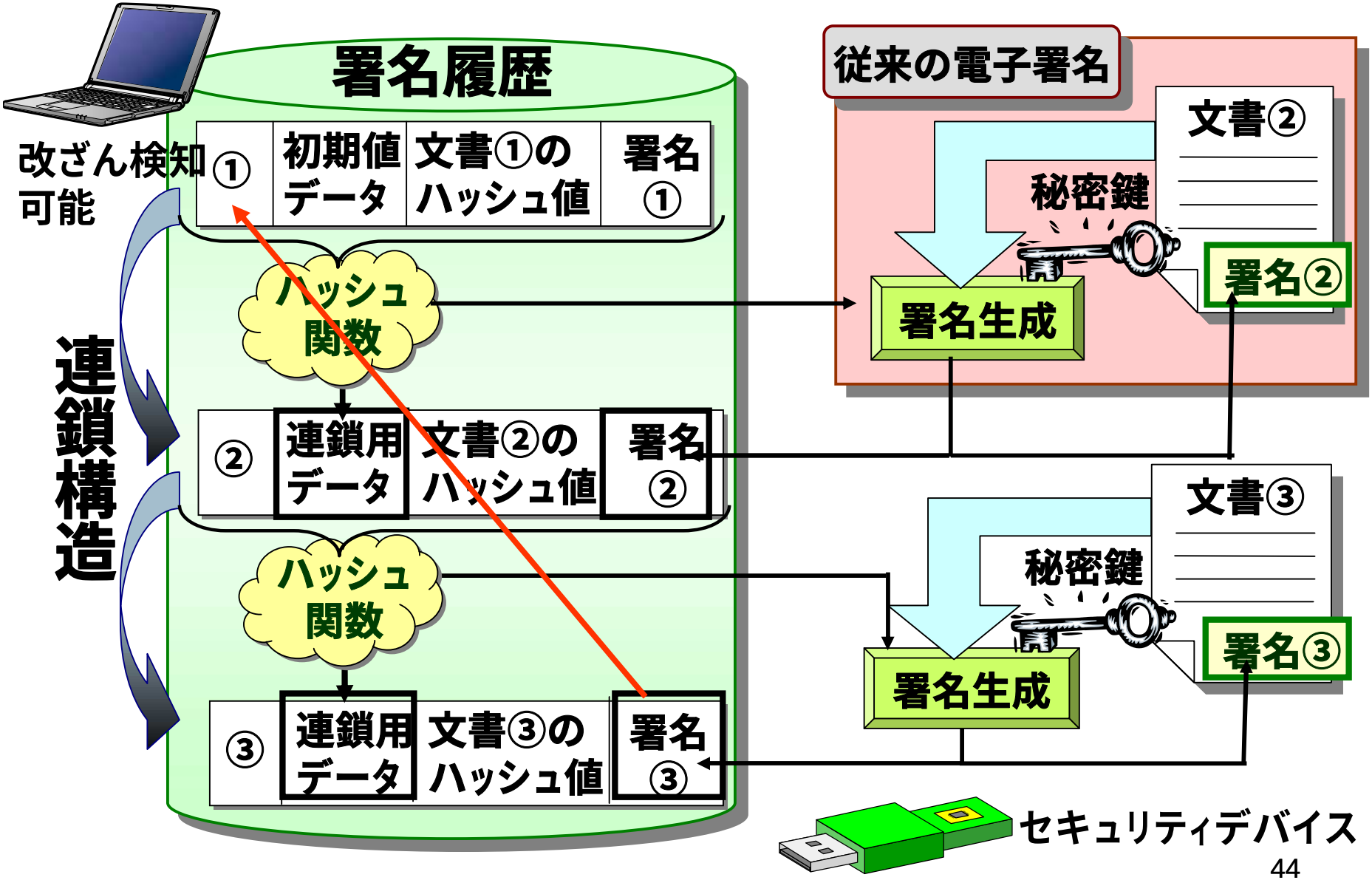
ヒステリシス署名による内容や前後関係の改ざんの検知

証拠を確保

不正･ミスや証拠の改ざんはしていない！

･確実な証拠で裁判などで有利に

ヒステリシス署名


改ざん検知
可能
連鎖構造
署名履歴
①
初期値
データ
文書①の
ハッシュ値
署名
①
ハッシュ
関数
②
連鎖用
データ
文書②の
ハッシュ値
署名
②
ハッシュ
関数
③
連鎖用
データ
文書③の
ハッシュ値
署名
③
従来の電子署名
文書②
秘密鍵
署名②
署名生成
文書③
秘密鍵
署名③
署名生成
セキュリティデバイス

PC内での不正を防止するために

これで不正は行えないはず。

しかし、PCの持ち主がPC内でログデータの改ざんを行った後、署名をしたら不正は容易

ICカード（スマートカード）のような耐タンパー装置の中なら装置の持ち主であっても不正はできない

PC全体を耐タンパー化できないか

耐タンパー高速処理装置

耐タンパ性を持ち高速処理を行える

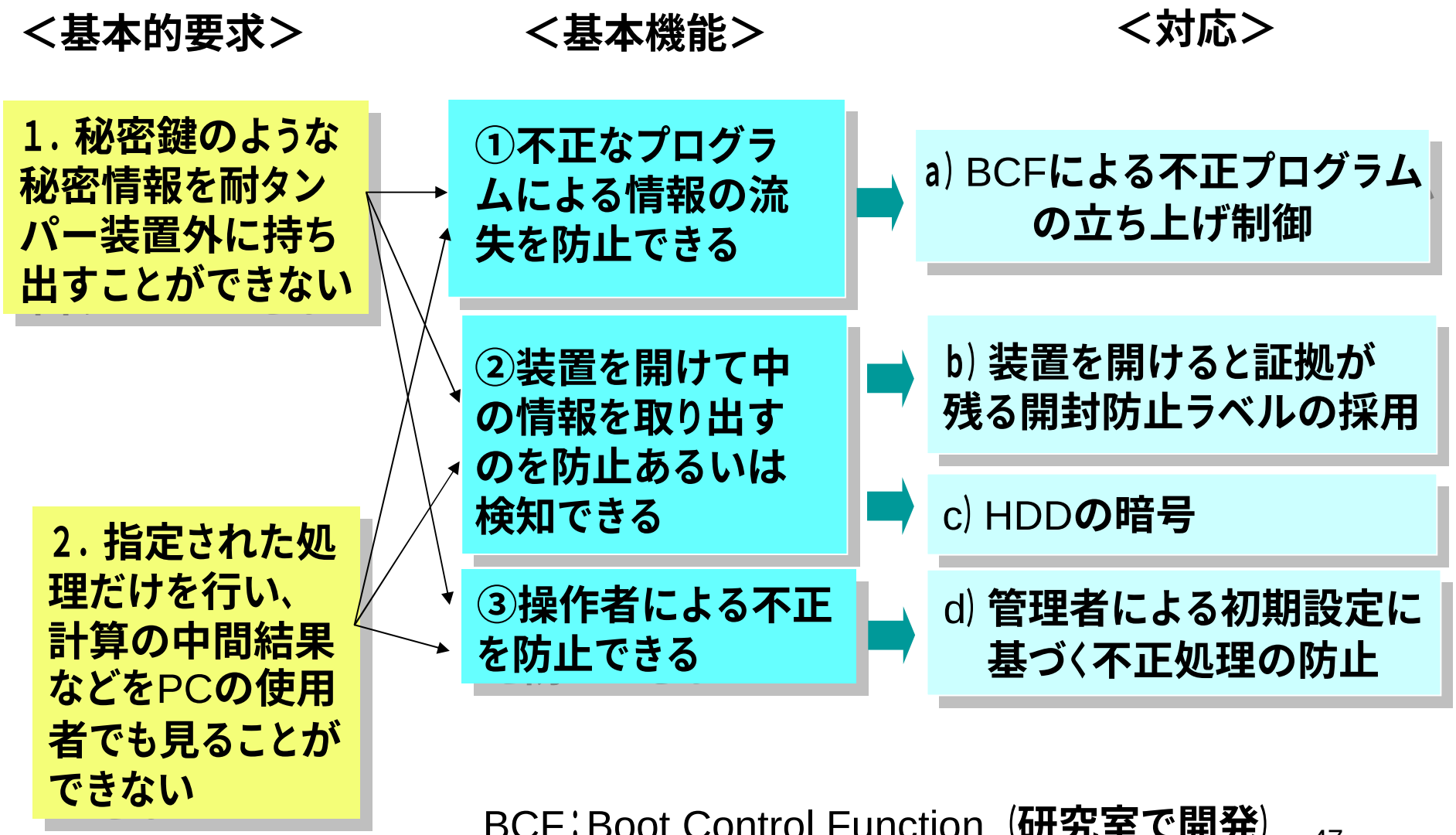
ＰＣベースのハード･ソフト

High Grade Anti-Tamper Equipment

HiGATE

を試作する

HiGATEの機能要件と対策



BCF：Boot Control Function（研究室で開発）

HiGATEの構成

HiGATEの構造

アプリケーションプログラム ⇔ ホワイトリスト

HiGATE基本プログラム

- 起動制御機能 (BCF/Vista)
- HDD暗号
- ファイル抹消機能 (オプション)

TPM 鍵管理

Windows Vista Ultimate

ハードウェア (PCをベースに内部にさわろうとすると対応できる機能)[開封防止ラベル] [電源を自動的に落とす(オプション)[入力機器の制限(オプション)]

HDD

HiGATEの適用可能対象

1．コンピュータの持ち主の、証拠性保全に関する不正の検知

2．疫学における複数の個人情報のマッチングを演算用ＰＣの持ち主でも中間結果などを見ればすぐにわかる演算

3．墨塗り問題において墨塗り部分に含まれてはならないキーワードが含まれていないことの検証

4．その他

目次案

今後の展開

1．クラウドコンピューティング化動向の監視

2．マーケットに受け入れられるITリスク低減化対策の検討

3．マーケットに受け入れられるITリスク低減化技術（含むHiGATE）の開発

4．実用化展開


END