「クラウド時代のセキュリティと法律の関係」

弁護士 高橋郁夫

ISOG-J内部セミナー

アジェンダ

- クラウド・コンプライアンスリスクの一般面
- クラウド・コンプライアンスリスクの国際面
- コンプライアンスリスク対策
- 今後の動向について

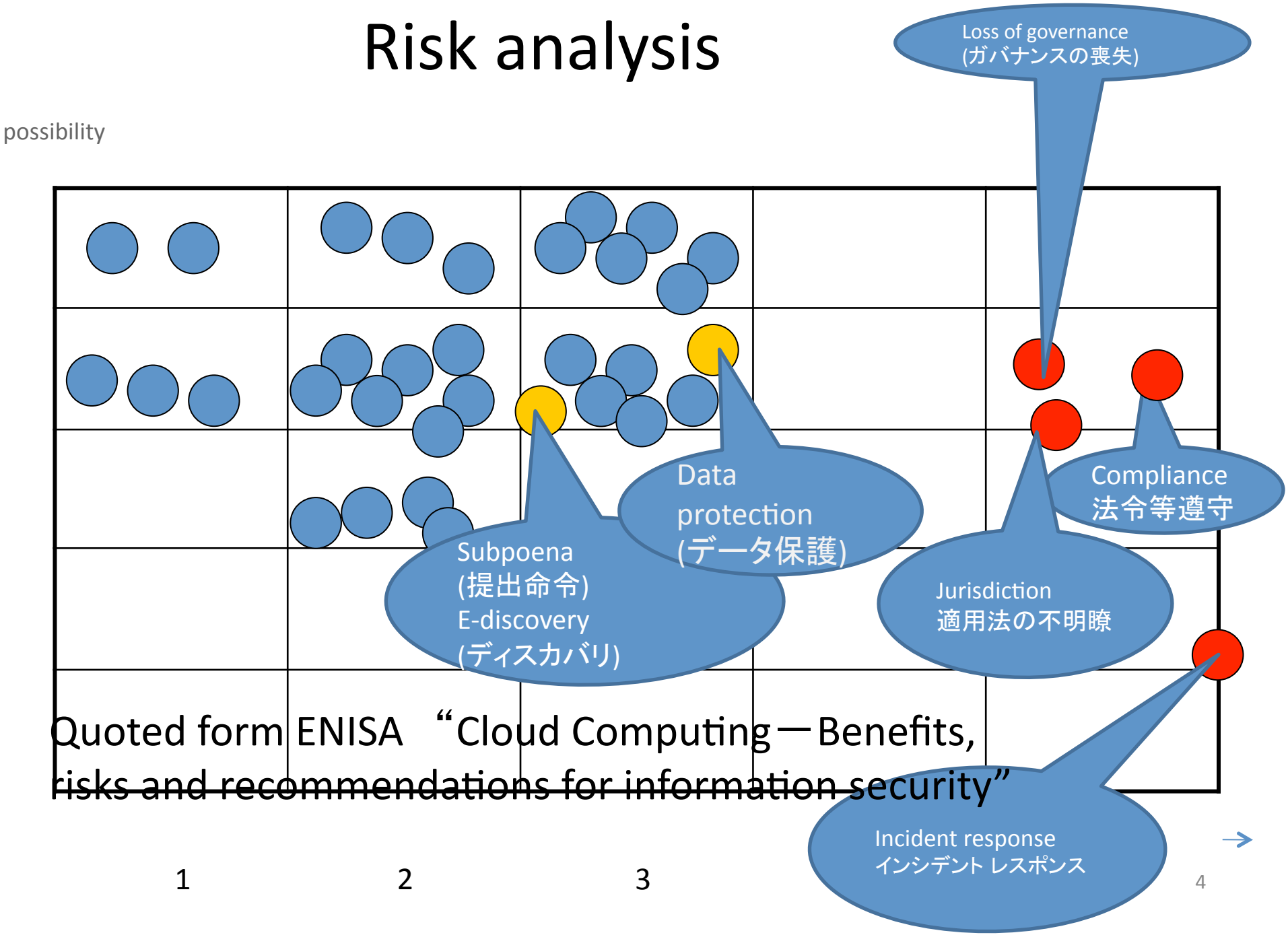
クラウドコンピューティングの定義

- 「クラウドセキュリティについては、仮想化技術もしくは分散コンピュータ技術を基盤としたITに関するオンデマンドのサービスモデル」
    - ENISA “Cloud Computing－Benefits, risks and recommendations for information security”より

- 基本的な視点
    - クラウドコンピューティングって何か新しいの？
    - ASPなどに比較して何か 特徴があるのだろうか
    - クラウドコンピューティングの特徴は、何かを付け加えているのだろうか

- 因子分析をしてみよう
    - 因子分析-「クラウドコンピューティングによるセキュリティの問題が、観測されるのであれば、それは、クラウドコンピューティングのどのような構成要素によって導かれるのであろうか」

Risk analysis



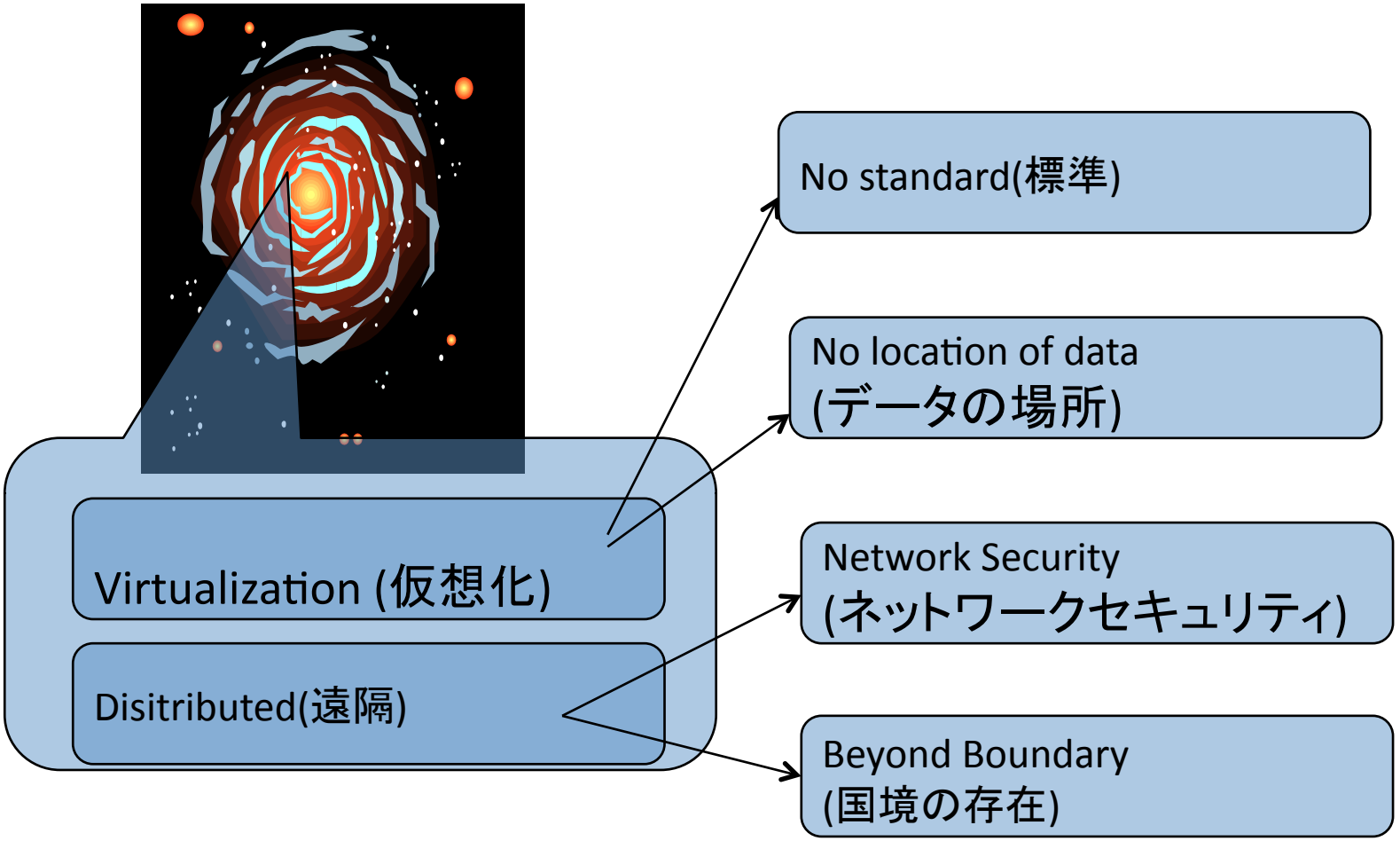
Quoted form ENISA “Cloud Computing－Benefits, risks and recommendations for information security”

リスク評価からわかること

- ポリシの実装および法律問題がクラウドセキュリティ問題にしめる割合が高い
  - これらの問題の重要性が十分に反映されているのか
    - 総務省「スマートクラウド研究会」報告書
    - 経済産業省「「クラウドコンピューティングと日本の競争力に関する研究会」報告書」
      - などの報告書においては、リスクについての論及が少なく、また、あまり体系的ではない

Factor Analysis of Cloud Computing

“仮想化技術もしくは分散コンピュータ技術”

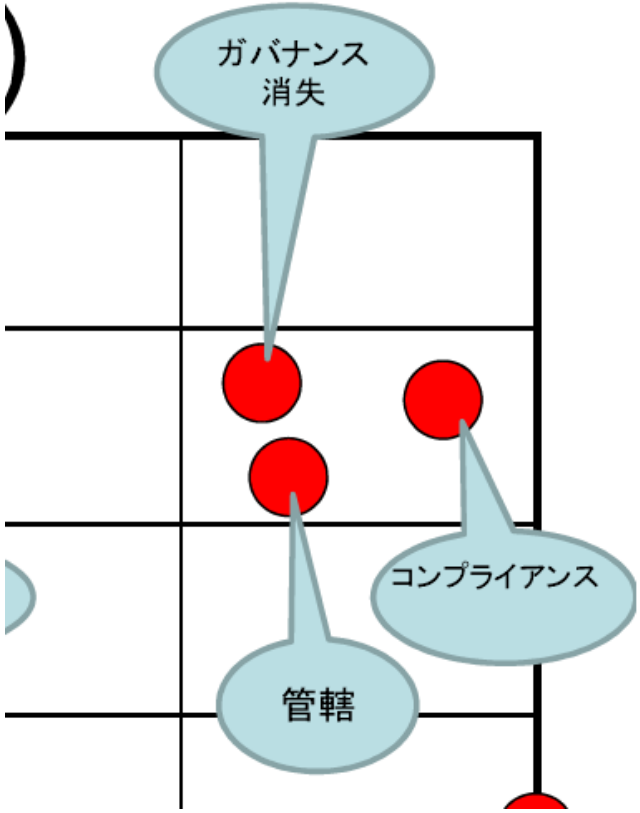


コンプライアンス問題を体系的に考えてみよう

- 国内要素のみの場合(Within Boundary)
  - ガバナンス関係
  - 個人情報保護法・情報セキュリティ法
  - 国際規格等
  - 一般的な情報セキュリティに関する論点
  - 種々のセキュリティリスク対応(管理策の確保)
- 国際的な要素が関連した場合(Transborder)
  - 基本的な考え方
    - 民事問題における複雑性
    - アクセス権限と属地性
    - 主権によるデータの域外移転禁止
    - 法執行の困難性

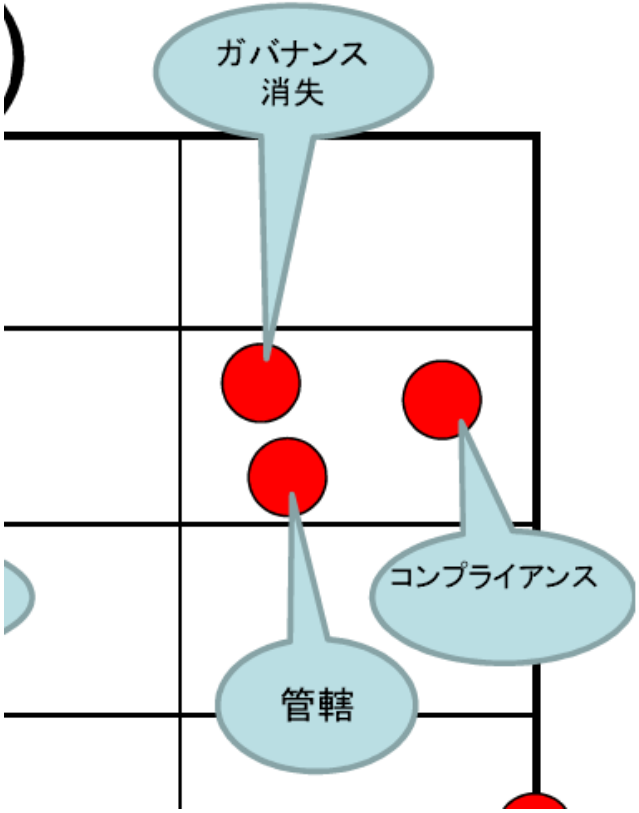
I-(1)ガバナンスの消失

- プロバイダのセキュリティに関する対応によって実際の企業の情報運用に対するガバナンスが左右される
- 自社の内部の運用
  - 自社の情報資産に応じてきめ細かな情報セキュリティポリシを構築して運用することが可能
- クラウドコピューティングにおいてはきめこまやかな運用は不可能



I-(2)コンプライアンスリスク

- 米国での遵守法令としてはFISMA、HIPAA、SOX、PCI、SAS　70などがあげられている。
- 我が国で検討すべきものとして
  - 個人情報保護法との関係
  - 情報セキュリティ法
  - 国際規格等
  - 種々のセキュリティリスク対応



I-(2)-A 個人情報保護法との関係

- SPIモデルにおいて、データを委託して処理することがある
  - 外部委託の問題になることがある
    - モデルによることになる。データ自体は、利用者が保存して、処理するというモデルも存在する。(ただ、外部でデータ処理されている場合、どのように解すべきかは、不明ということになる)
  - 「委託を受けた者に対する必要かつ適切な監督を行わなければならない」(個人情報保護法22条)
  - 「必要かつ適切な監督」
    - 各ガイドラインでは，個人データの安全管理が測られるよう，委託先選定基準を定めること，基準を定期的に見直すこと，安全管理措置を委託契約に盛り込むこと，定期的又は随時に委託契約に定める安全管理措置の遵守状況を確認し，安全管理措置を見直すこと，再委託の条件を設定することなどの方策
  - データのライフサイクル
    - 終了後の消去の確保も必要

I-(2)-B 情報セキュリティ法

- プライバシーを根拠とした損害賠償
  - 日本法 対 アメリカ法
    - 日本
      - ヤフーBB事件(大阪高判平成19年6月21日) 、TBC事件(東京地裁平成19年2月8日)
    - Twitter事件
      - 連邦取引委員会法（FTC Act）にもとづいて、セキュリティ管理態勢の整備を求めうるという形
      - 2009年1月および4月に漏えい
- 情報主体に対する通知の問題
  - The Security Breach Information Act (S.B. 1386)
  - 個人情報の保護に関する基本方針」（平成１６年４月２日閣議決定）および各種ガイドライン

I-(2)-C 国際的基準等

- CSAクラウド・コントロール・マトリックス（以下，「CSA CM」という）
- １１分野９８項目にわたるコントロールエリア
- 従来から存在する規格、法令
  - COBIT(Control Objectives for Information and related Technology)
  - HIPAA(Health Insurance Portability and Accountability Act)
  - ISO/IEC 27002-2005
  - NIST SP800-53
  - PCI DSS

I-(2)-D 一般的なセキュリティの問題

- ネットワークセキュリティの問題
  - D-DoS、標的型攻撃、その他
- クラウド事業者の健全性
  - Core IP Networksへの捜索・差押についての事例(後述)
- 仮想化技術特有の問題点
  - 仮想化自体が、サイドチャネル攻撃の危険を引き起こす可能性
  - 仮想マシンモニタを乗っ取られると被害が甚大
  - 仮想マシン自体の脆弱性をついた攻撃が可能
  - 物理的なエラーが攻撃のきっかけ
  - キャッシュ共有・メモリの覗き見等の攻撃が可能
- 不正競争防止法などの関係は？

おまけ Core IP Networks事件

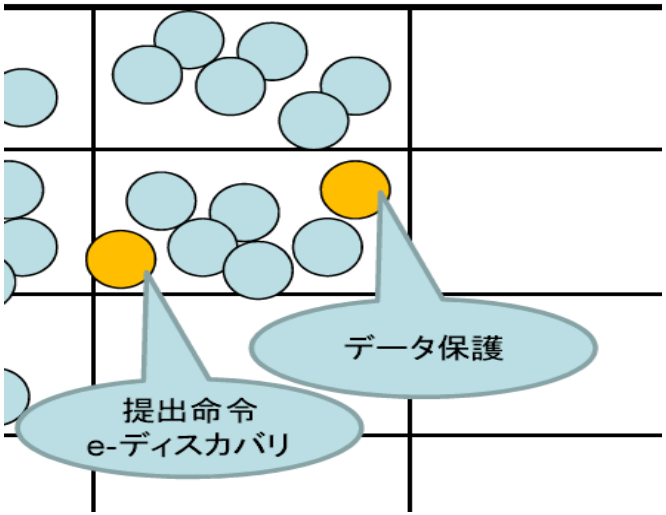
- ２００９年３月および４月
  - FBIがテキサスのデータセンター(Crydon Technology とCore IP Networks)に対して捜索・押収
    - サーバー・ルーターなどの機材を押収し、そのデータセンターを利用していた利用者にも損害が発生
  - 「愛国者法による損害」なのか「クラウド事業者の健全性の観点から捉えるほうが望ましい事例」なのか。
    - FBI Defends Disruptive Raids on Texas Data Centers” (http://www.wired.com/threatlevel/2009/04/data-centers-ra/)
    - FBI の捜査官は、データセンターのオーナーの関係者が書類を偽造して、大手の通信業者から、接続サービスを購入していたという証拠を把握しており、共謀があったことを信じるに付いての相当な理由
      - ノックなし令状
      - 「合法かつ営業中の事業を停止させ、非常に多くの人々の生活に支障をきたす可能性もある。」と記載されており、このような場合に対する慎重な配慮をなした捜索の計画を推奨(司法省　コンピューター捜索・差押マニュアル)
      SJG事件

I-(2)-E内部コントロールとの関係で

- リスクのマネジメントとしてのクラウドのコントロール
  - 外部委託に関する契約の管理
    - 企業が財務報告に関連して、ITに係る業務を外部委託している場合、監査人は、企業が適切に外部委託に関する契約の管理を行っているか検討する。
    - クラウド事業者自体の情報セキュリティの管理レベルをどのようにしてコントロールすべきかという問題がある。
    - モニターは、どうするか
    - そもそも、業者の選択は、どうするか
- 各種開示に関する規定とクラウドサービスの利用
  - 事業報告
  - 内部統制報告書
  - 有価証券報告書

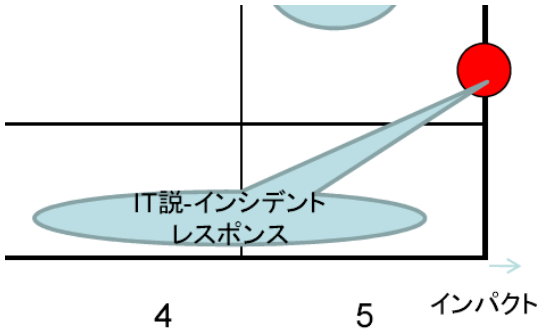
I-(3) クラウド・フォレンシック 提出命令・e-ディスカバリ

- フォレンジックの問題
  - 透明性の確保が必要になる(過去のデータの変遷を完全に把握する必要性がある)
  - 企業は、特定の事案に関連してそのクラウドに保有しているデータが、「すべてもれなく」検索・管理しうることを明らかにして、しかるべき機関に提供しないといけない
- 英国・米国では、訴訟当事者は、「トランプを表に」して、訴訟をするものと認識している
- 官公庁に対して説明責任をはたすときにクラウドのデータがすべて上のフォレンジック要求を満たしているときちんといえるのか
  - 「ガサ入れ対策」でクラウドを使おう？



なお、インシデントレスポンス

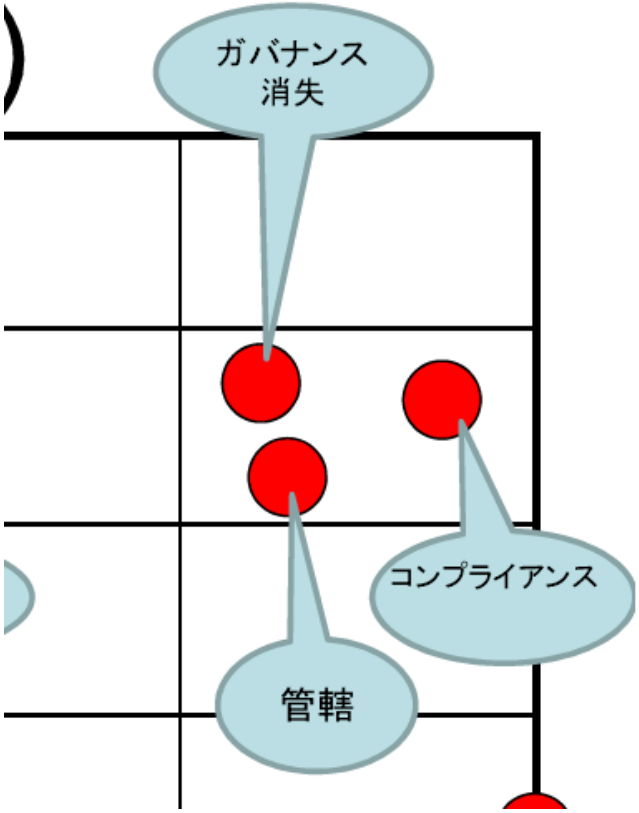
- 何か問題がおきたときに、クラウドからどのような情報が流出したのか、データの所在がわからないのにきちんと分析することができるのか



- これは、災難レベル(リスク分析の外)
  - LxLabs boss found hanged after vuln wipes websites -Shocking development in VAserv megahack affair (June9,2009)
  - http://www.theregister.co.uk/2009/06/09/lxlabs_funder_death/

T-管轄権は

- どこの法律の適用がなされるのか
  - 行政規定の適用関係がどうなのかが問題となることが多い
    - EUのデータ保護法は、域外への個人データの移転を禁止している
    - 行政目的からの検査の可能性などから、データの所在地が、特定の法域に存在することが要求される
    - プロバイダとの契約によって回避できるものではない



T-(1) 基本的な考え方

WikiLeaks事件を例にとる

- どこで
- どのような問題を

– ジュリアン・アサンジ(Julian Paul Assange)
  - WikiLeaksという秘密暴露サイトを管理
  - 住所不定(アイスランドに家)
  - サーバーは、スウェーデンの会社
  - 世界中にデータがある
– 機密資料約75000点以上が公表
  - 2010年7月25日
  - アフガニスタン紛争に関するアメリカ軍や情報機関の機密情報
  - 米国の連邦法違反

T-(2) 考えるべき要素

- どこの誰が
  - 国によって、法律の適用についての原則が異なっている
  - 執行権限を行使する場合においては、その行使は、領域の範囲内でしか行えない
- 法律問題の性質
  - 刑事法(属地主義、属人主義、保護主義など)
  - 民事法(国際私法)
  - 行政に関する法律(行政法のみならず公共的性質をもつ法)

T-(3) 4つの視点

- 民事上の問題についても、適用される法律を決定するのは、きわめて種々の問題が存在する。
- データが外国でアクセスしうる場合に、そのアクセスしうる国の法律の適用をうける場合がある。
- 主権国家は、その主権の行使として、パブリックローにもとづいてデータを域外に移転することを禁止することができる。
- データを管理する主体が国外に存在するとき、法的な要求を執行するのは、きわめて困難になる。

T-(3) -1

- 民事上の問題についても、適用される法律を決定するのは、きわめて種々の問題が存在する。
  - ひとつの例
    - 情報主体（日本在住）のデータを処理していた利用者（日本企業）から、委託をうけていたクラウド事業者
    - 脆弱性対応を怠り、流出させた
    - クラウド事業者が、外国に存在していたとする。情報主体が、クラウド事業者 に対して、プライバシー侵害を根拠に損害賠償を求めうるか
    - 日本法の考え方 対 米国での考え方

T-(3) -2

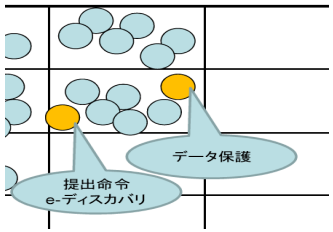
- データが外国でアクセスしうる場合に、そのアクセスしうる国の法律の適用をうける場合がある。
  - 法執行機関による適法なアクセス
    - 我が国では、令状が必要
    - 米国では、クラス付けとバランス、ノックなし令状がある
  - 民事手続によるe-ディスカバリ
    - 開示の義務と元の国とで、守秘命令がぶつかったらどうなるのか。
      - マーク・リッチ事件(アメリカの文書持参召還令状と守秘義務との相剋が問題となった)

T-(3) -3 主権による域外移転禁止

- 主権国家は、その主権の行使として、パブリックローにもとづいてデータを域外に移転することを禁止することができる。
  - (1)データ保護の話
  - (2)行政権による監督
  - (3)国家安全

T-(3) -3 主権による域外移転禁止 1-データ保護

- EUのデータ保護指令では、第三国が十分なデータ保護レベル水準（adequate level of protection）にない場合、EU域内から第三国へ個人データ移転してはならないことを定めている
  - 適切なレベルにあるとされている国
    - スイス、カナダ、アルゼンチン、ガンジー島、マン島、ジャージー島、オーストラリア、米国(セーフハーバー・旅客名称記録)
    - http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm
    - 2010年9月10日現在



T-(3) -3 主権による域外移転禁止 2-行政庁の監督が望ましい分野

- 一定の行政庁の監督が望ましい分野については、データ自体の域外移転禁止を求めるということも合理的
  - 「医療情報システムの安全管理に関するガイドライン第4.1版（平成２２年２月）」
  - 以下のガイドラインが前提
    - 【ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドラインより抜粋】
      - 表3－8 災害等の非常時の対応におけるＡＳＰ・ＳａａＳ事業者への要求事項
      - 所管官庁に対して法令に基づく資料を円滑に提出できるよう、ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等は国内法の適用が及ぶ場所に設置すること。

T-(3) -3 主権による移転禁止
3 国家安全保障

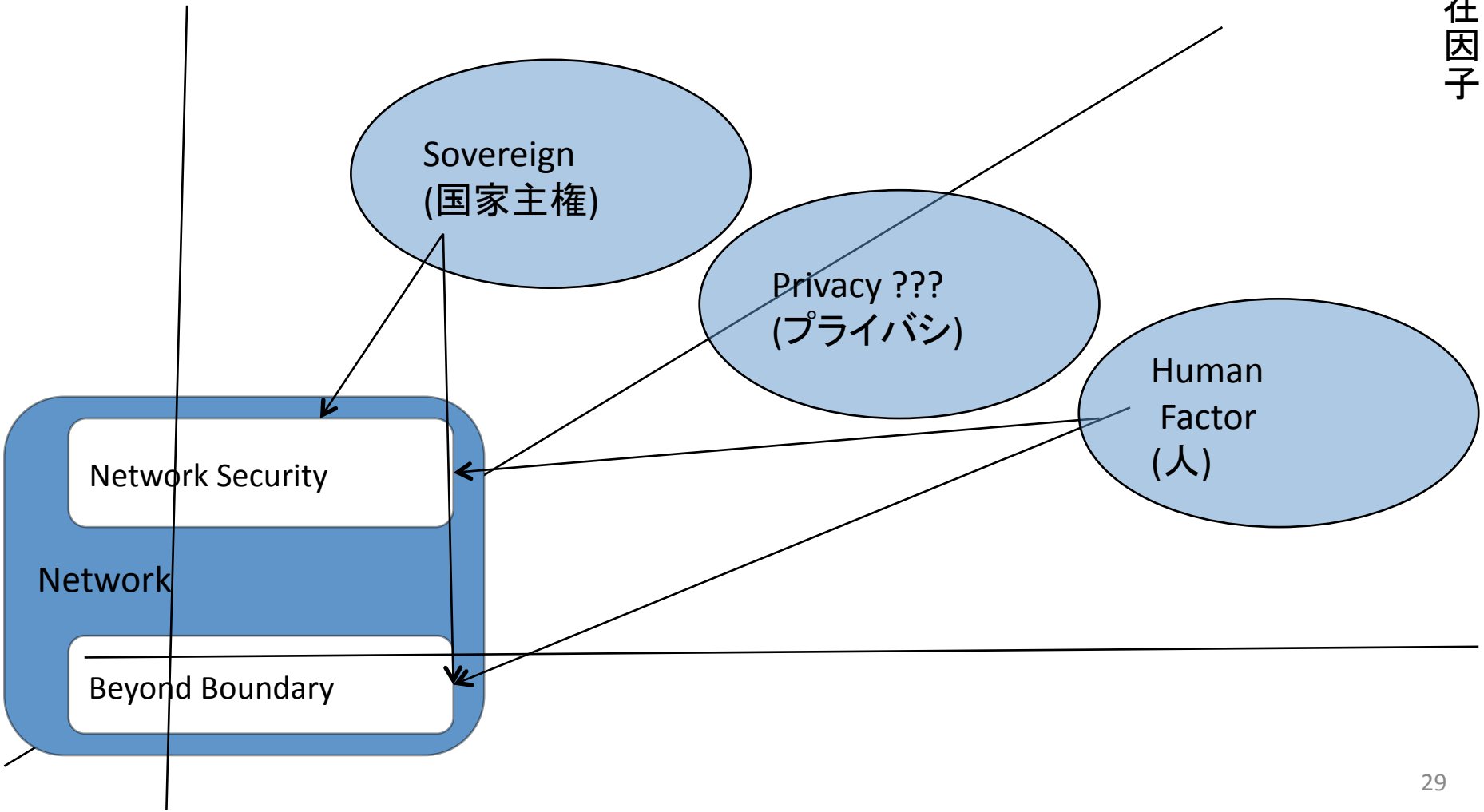
- 役務取引についての規制
  - 外国為替及び外国貿易法（外為法25条）
    - 「国際的な平和及び安全の維持を妨げることとなると認められる」貨物や技術 については、大臣の許可を受けなければならない（同法２５条１項）
    - 「第一項の規定の確実な実施を図るため必要があると認めるとき」について、「特定国において受信されることを目的として行う電気通信（略）による特定技術を内容とする情報の送信」についても大臣の許可を受ける義務を課される場合があるとさだめている（同３項）。
- サイバーエスピオナージ(ネットワーク上でなされる経済スパイ活動)
  - 大きな問題
  - 政府機関の情報についてデータの所在を国内に限定するということの意味
    - 定額給付金のデータってどこで処理されたの？

T-4 法執行の困難性

- データを管理する主体が国外に存在するとき、法的な要求を執行するのは、きわめて困難になる。
  - Wiki Leaks事件で説明した
    - 刑事であれば、捜査共助の枠組みになる
    - 捜査共助法においては「双方可罰性」が求められる

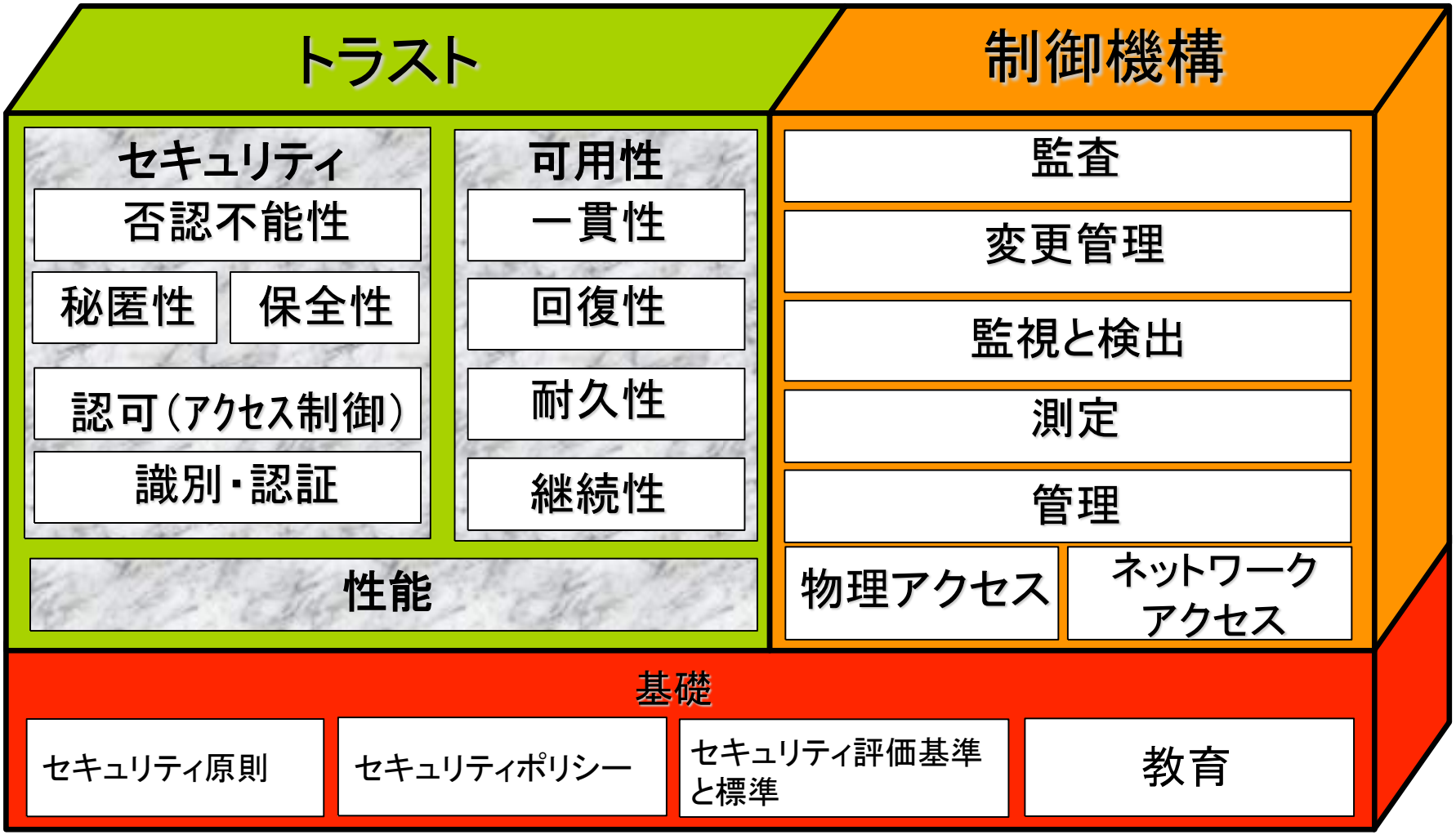
Behind Scenes

問題の潜在因子



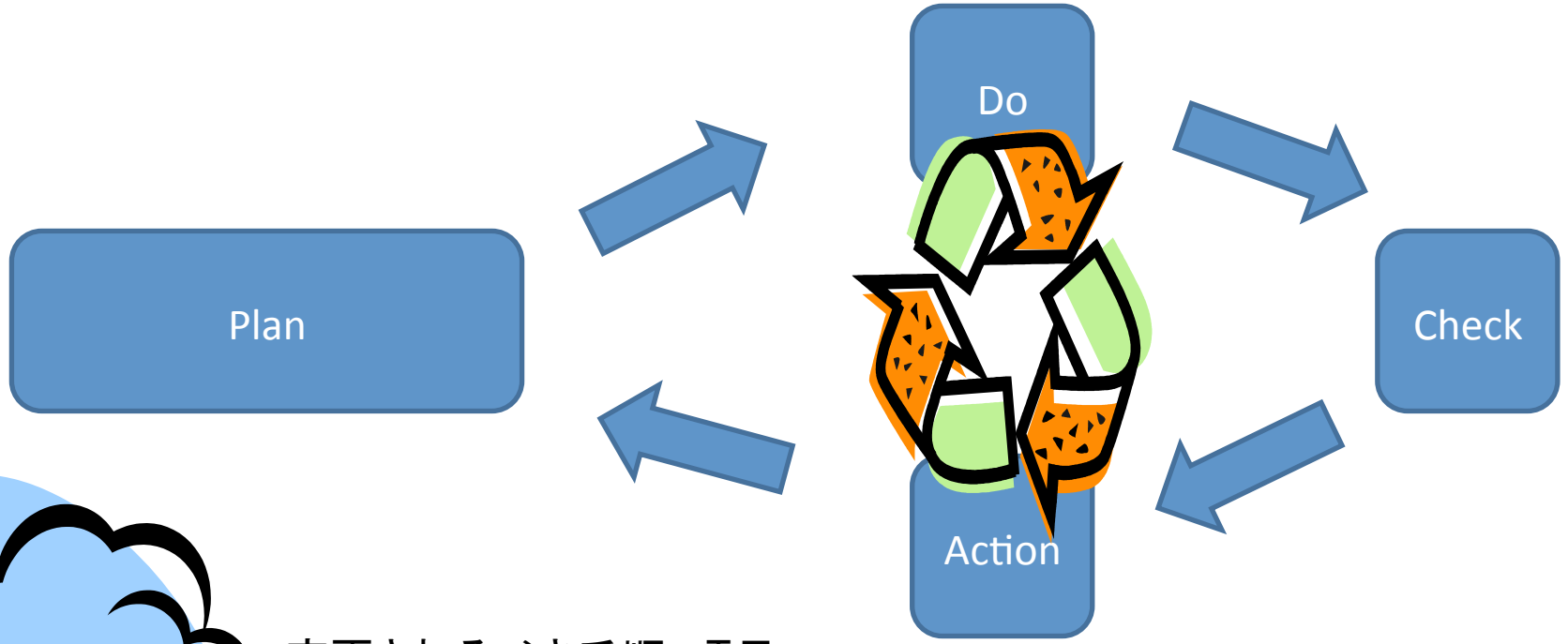
ITセキュリティポリシと
コンプライアンスリスク
ITセキュリティフレームワークとリスク

ITセキュリティ・フレームワーク



分散コンピューティングセキュリティ―ロックは大丈夫? (Hewlett-Packard professional books) [単行本]
グレン ブルース (著), ロブ デンプシー (著), Glen Bruce (原著), Rob Dempsey (原著),
さとう よしひろ (翻訳), 行本 年延 (翻訳), 掛川 潔 (翻訳) より

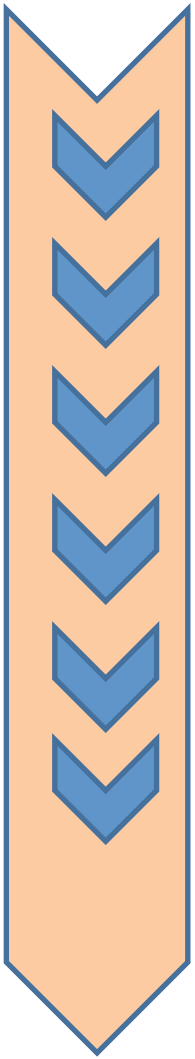
クラウドコンピューティングとPDCA



変更されるべき手順・項目
クラウドコンピューティングセキュリティ、ビジネス継続性、ディザスタリカバリーを、利用者自身のポリシーと手順に統合する
（CSA　ガイダンス 翻訳版85頁）

プランニングの手順

ITフレームワークのなかのクラウドコンピューティングの利用



ビジネスのリスク分析

クラウドの一般的リスク・機会分析

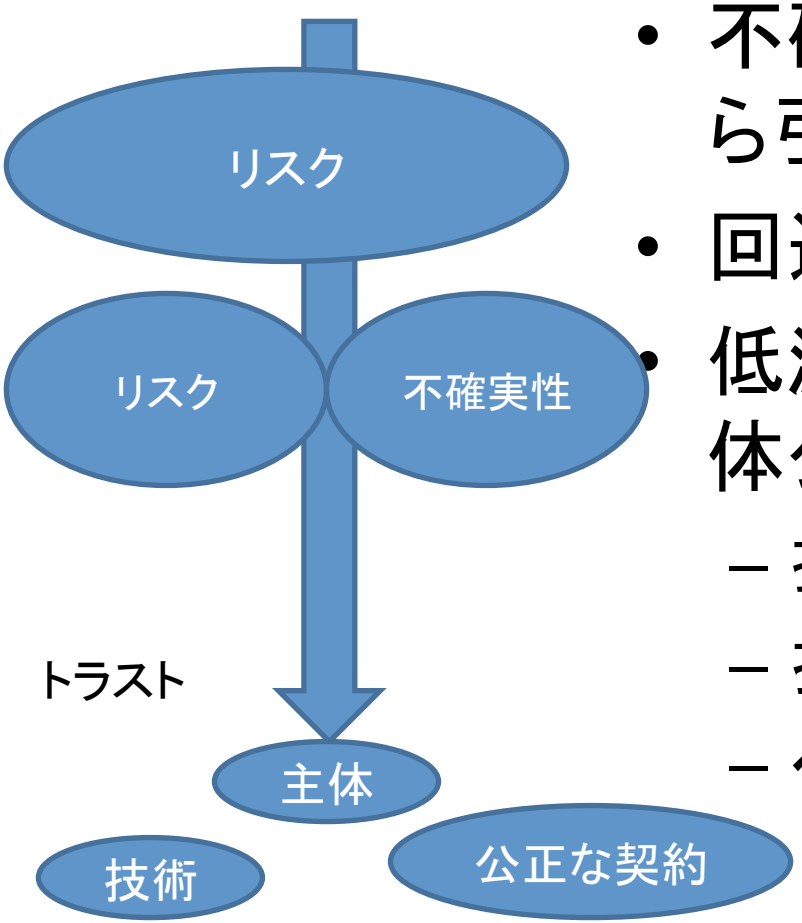
クラウドによって処理されるデータの分類

対応手法の検討

対策の選択および実施(リスク管理態勢の整備)

コントロール

リスク対応策



- 不確実性(リスクと不確実性)から引き起こされる
- 回避、低減、共有、受容
- 低減･共有策について(技術、主体公正な契約)
  - 提供者の評価およびベンダ選択
  - 技術の評価および利用
  - ベンダとの契約によるリスク共有

技術的対応

- 伝統的な論点
  - 暗号化
  - 鍵管理
  - アイデンティティ管理

	IaaS	PaaS	SaaS
プライベート	利用者の責任 大		
ハイブリッド			
パブリック			データ独立性・漏えいなどのリスク

クラウド事業者の評価

- 誰が(主体)、どのようなサービスを(種類)、どの程度の「質・価格」でもって提供しうるのか。
- 「客観的に評価」すること

- 参考
  - ”CSA Cloud Controls Matrix V1”
    - 「コンプライアンス」「データガバナンス」「物理的セキュリティ」「人的資源管理」「情報セキュリティ」「法的」「運営マネジメント」「リスクマネジメント」「レジリエンシー（弾力性）」「セキュリティアーキテクチュア」などの統制エリア
    - SPIモデルごとに、問題となるコントロールを論じる

主体

- 一般的な外部委託の場合の委託業者の選定基準が参考
  - サービス主体(サービス事業者)
    - 財政的健全性の問題
    - マーケットでの評価
    - 管理状況
    - 主要役員構成
    - 過去の受託等の業績の評価
    - サードパーティーベンダのリスト・役割、責任事項・インターフェース情報
  - リスク管理について
    - 事業者自体のリスクレベルの評価
    - ポリシの評価
    - 手続およびプロセスに対するレビュー
    - 事業継続性計画の有無等
    - コンプライアンスに関する態度、データのライフサイクル管理の可能性、損失に対する保険加入状況など

客観的な評価

- 契約は唯一のガバナンスのためのツールではなく、クラウド事業者に必須となる幅広い適正評価を含めていくべきである(CSA ガイダンス15頁)
- デューデリジェンス
  - 対象
    - サービス種類
    - サービス主体
    - サービス条件
    - SLAの実効性

人-クラウド事業者の行動コントロール

- 法的に対策をとる
  - SLAの有効性(契約で定めることによって、事業者をコントロールする)
    - データの独立性
    - データのアクセスに関する規定
    - 技術的手法の採用に関する規定
    - データの所有権限についての定め
    - モニタリングについての権限についての定め
    - 法的遵守事項についての定め
    - 円滑な契約終了のための定め
  - 円滑な終了の定め
    - 終了後のデータのアクセス
    - 移植性の問題

コントロール

- クラウドサービスに伴うリスクを評価し、対応策を選択したのであれば、その対応策が、正しく実施されるべきであり、また、正しく実施されていることを検証することが必要になる。
  - *クラウドコンピューティング環境におけるセキュリティは、組織の内部ポリシー、手順、標準、ガイドライン、プロセスをお互いに締め出してしまうものではないということを忘れてはならない(G70頁)。*
    - データがどのように保存され、処理され、アクセスされ、制御されるかという点についての定義と文書化
    - クラウド事業者が、それらの点についてこのレベルのとおりに行うのかというのを確認する
      - 監査基準書(SAS70)の報告書や監査委員会報告18号

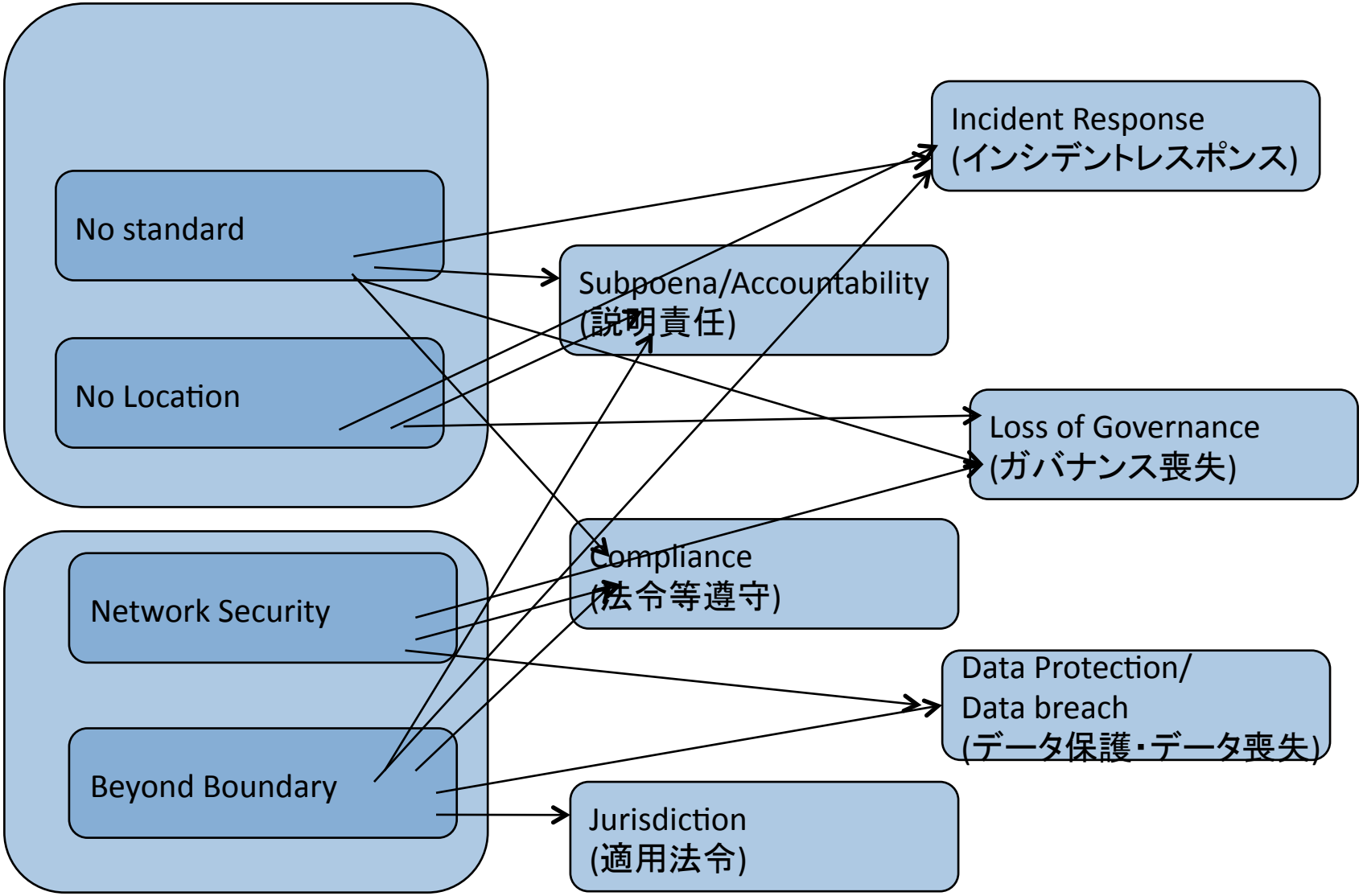
クラウド利用と開示

- 事業報告書
  - 「損失の危険の管理に関する規定その他の体制」を、事業報告に記載(会社法施行規則100条１項２号)
  - クラウドサービスの利用に際して、導入および利用に伴う社内体制を整備した旨が記載されれば、足りる。
- 内部統制報告書
  - 適正な財務報告を実現すための内部統制に関する事項
  - この文言の解釈の問題がある
- 有価証券報告書等
  - 一般的に記載対象となるとはいえない
    - 具体的なIT技術の導入それ自体が、リスクになるという観点からの指摘はない点

今後の動向を考える

技術の社会的成熟と国際的協調

Compliance/Governance Issues



コンプライアンス問題の位置づけ

技術の社会的熟成と国際協調

- 技術的な成熟が必要であることは認めるべきであろう
- フォレンジックの産業標準の確立
  - レスポンスのためのライブについては、かなりの意義
  - 「すべてのデータ」についての保障をどう確立するか
- 各法域において行政検査のための円滑な情報流通システム
  - 検査による取得システムの業界標準化
  - 取得データのフォーマット統一と交換プロトコルの統一
    - これができれば、医療情報のクラウド処理も可能かも
    - 例えば、証券取引監視委員会は、情報交換システムを確立しているよね

Framework and industrial standard

- クラウド・コンピューティング条約の必要性
  - Cloud Computing Convention Initiative (?)
    - 保存データのセキュリティ標準
      - Cloud Stored Security Standard all over the world
    - プライバシの適用法についての国際合意
      - Applicable law of privacy
    - 行政調査についての標準データ
      - Industrial Standard for administrative investigation
    - 説明責任・レスポンスにおける標準手法
      - Industrial Standard for Forensic research of cloud stored data
    - 民事裁判における開示手続の適用と除外
      - Define the domicile at Civil litigation
    - ....

参考資料

参考資料

NIST ”Effectively and Securely Using the Cloud Computing Paradigm”
ENISA“Cloud Computing－Benefits, risks and recommendations for information security”
CSA “Security Guidance for Critical Areas of Focus in Cloud Computing”

なお、日本クラウドセキュリティアライアンス提供セッションで配布される「解説CSAクラウド・セキュリティ・ガイダンス 」(ITポリシ構築編・法律編) およびそこでの参考文献

特にリスク管理態勢と法律を説く資料として、濱野敏彦・浦野雄介「クラウド・コンピューティングが変える法律実務」(NBL 918号ないし930号)