NICT情報通信セキュリティシンポジウム　2012

クラウドセキュリティ標準化の最新動向

（独）情報通信研究機構 ネットワークセキュリティ研究所
主管研究員　中尾　康二

目次

2000年～

マルウェアの変遷

危険度

メールから感染

ネットワークから感染

ウェブサイトなどから感染

営利犯
金儲けの道具

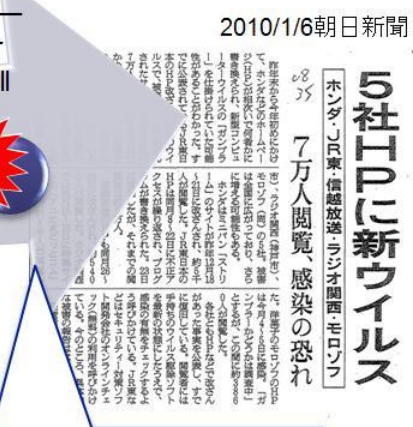
愉快犯
自己顕示欲

トロイの木馬
TROJ_AGENT.EH

ワーム
MS-Blaster
Slammer

ボット（BOT）
ロボットの略から命名
Agobot
ForBot

ガンブラー
Gumblar
Nine-Ball



W32/CIH(チェルノブイリ)、
Happy99

★目立つ→駆除しやすい

大量通信でネットワーク混乱（03年1月韓国ではネットが数時間利用不可）

感染したPCは遠隔操作される（迷惑メール、攻撃の踏み台など）

ウェブからPCにマルウェアを送り込まれる（：情報の抜き取り等）

★目立たない→駆除されにくい

感染ユーザは「少し調子がおかしいかな？」程度で、特段の不具合を感じない

2000年　2005年　2010年

高機能

【関係機関の取り組み】

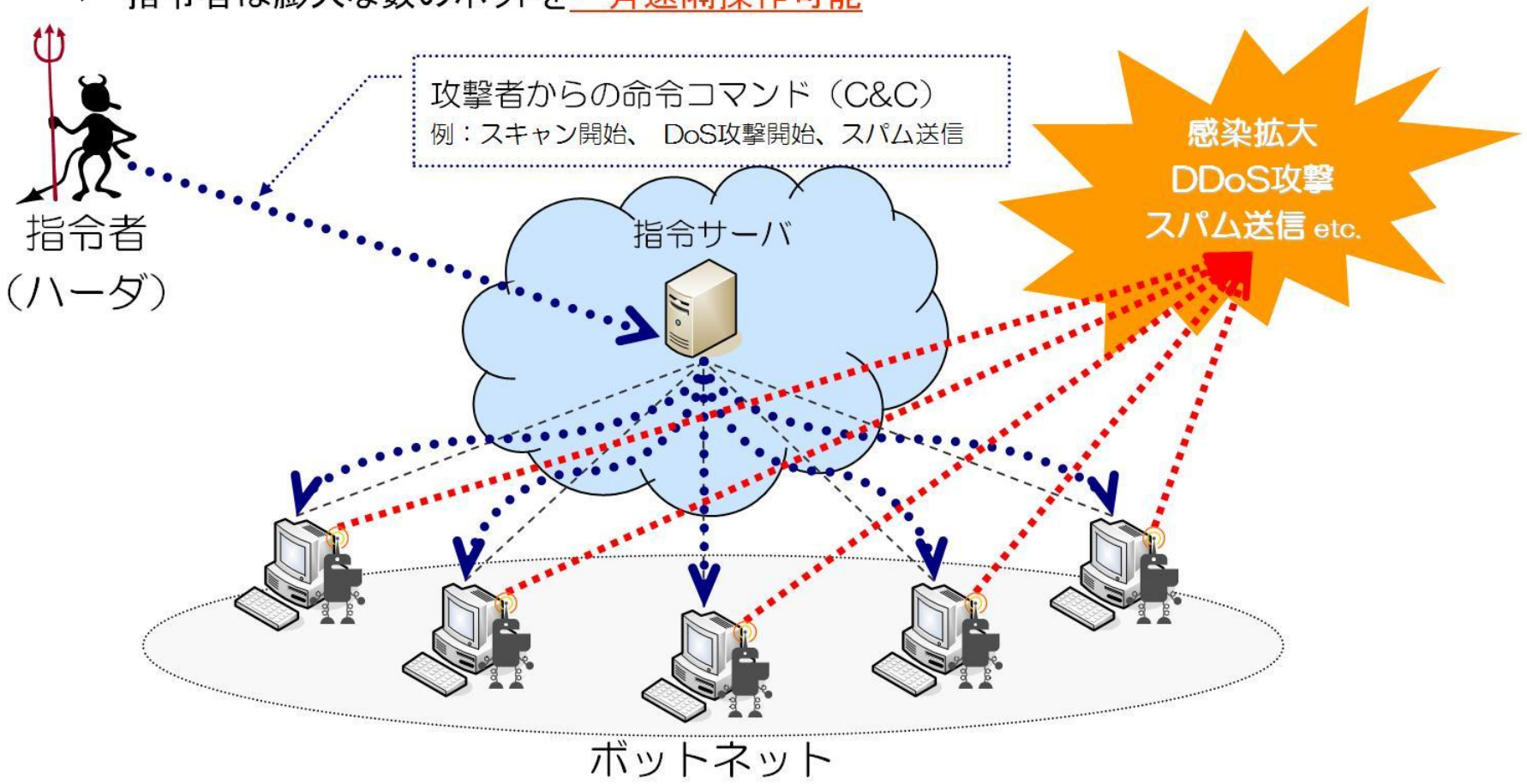
総務省関連 → インターネット接続事業者（ISP）によるセキュリティ情報の共有・分析体制（T-ISAC）の整備（2003年～）

経済産業省関連 → ソフトウェアの脆弱性情報の収集・共有体制（IPA, JP-CERT）の整備（2004年～）

ISP、ソフトウェア業界や総務省・経産省が連携して、ボット対策プロジェクトを開始（2006年～）

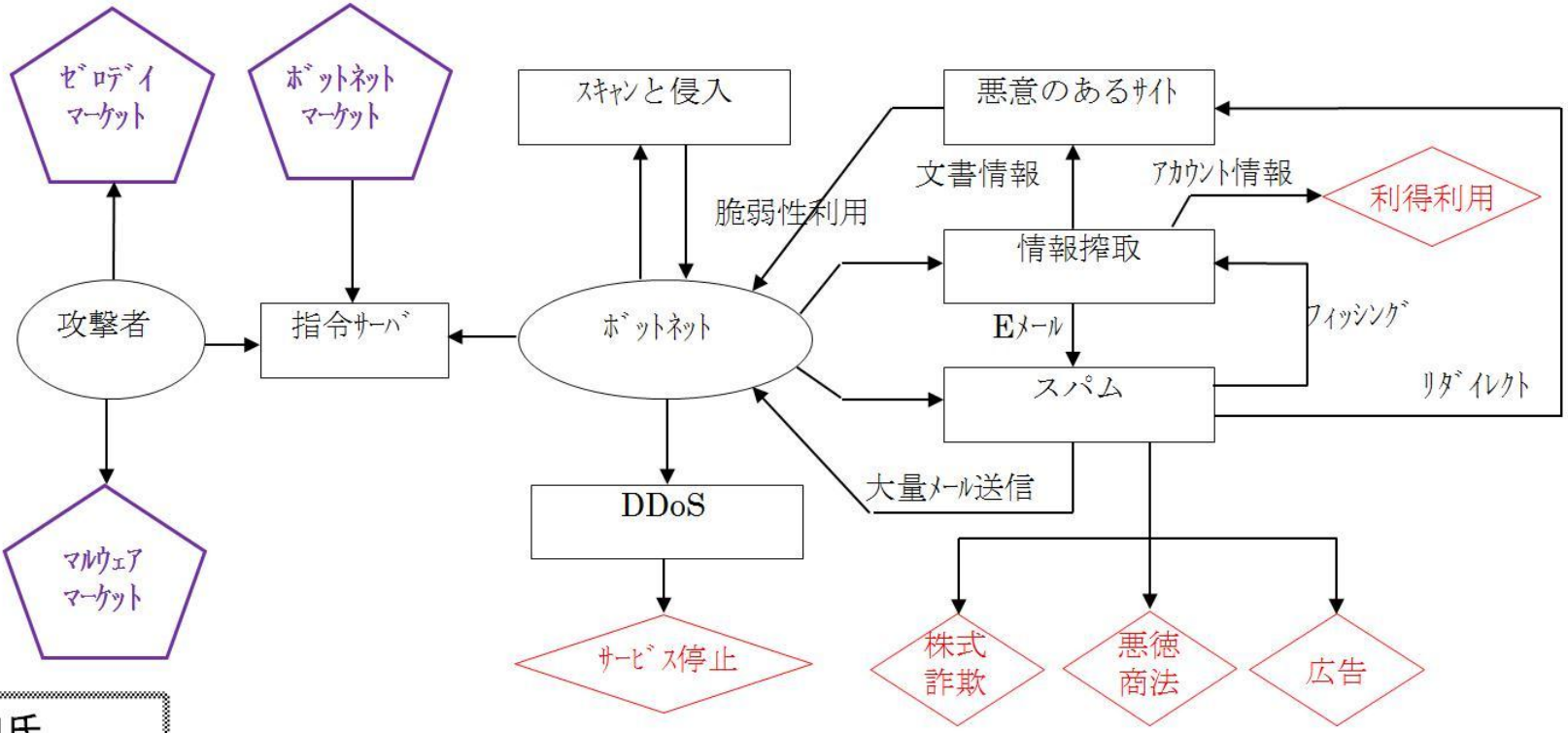
単独攻撃から連携攻撃(ボット)へ

- ボットの出現
  - ✓ 指令者からの遠隔操作により多岐に渡る活動を行うマルウェア
  - ✓ ボットネットと呼ばれるオーバレイネットワークを形成（数百～一千万台規模）
  - ✓ 初期のボット(Sdbot, Agobot, Rbotなど)は感染形態としてはワーム
  - ✓ 指令者は膨大な数のボットを一斉遠隔操作可能



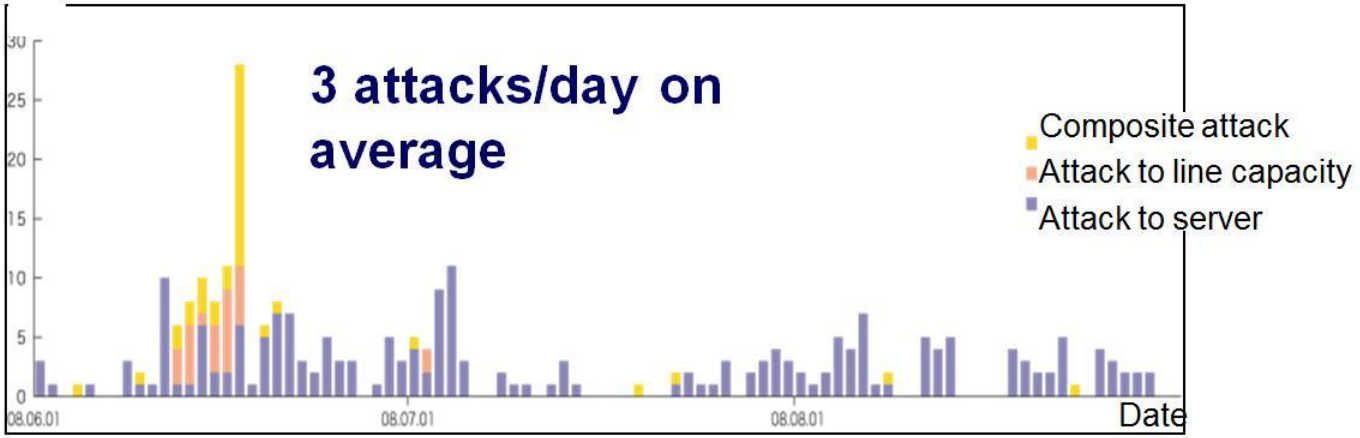
経済的利得に偏重した攻撃者

- 攻撃者が、競合他社等の「こちらにとって都合の良くない主体」に対するDDoS攻撃をすることによるサービス停止による営業妨害、不特定多数の人に対してスパムメールを送信することによる株式詐欺／悪徳商法／広告、そして、フィッシング詐欺サイトへの誘導によるアカウント情報の不正入手等をしていることを観測。



名和氏
Interop発表
資料より

Recent status of DDoS attack occurrence in Japan



ITU－Tにおけるクラウドコンピューティングのためのセキュリティ（FGの活動）

FGの目的

通信/ICTの視点からクラウドコンピューティングのサービス/アプリケーションを支援するために、標準化開発に向けた情報や概念を収集・文書化することを本FGの目的とする。

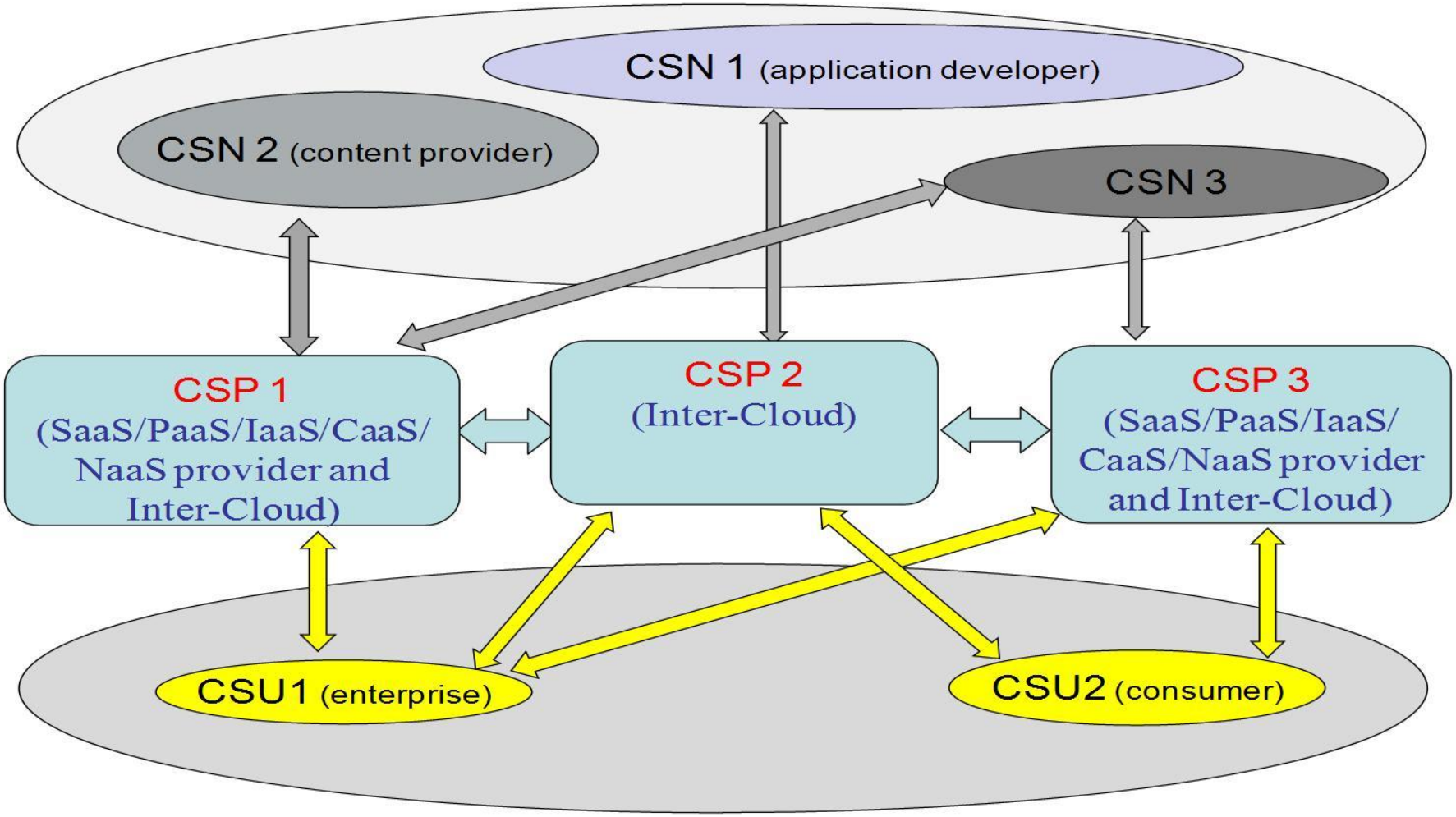
本目的を達成するためには、以下を行う必要がある。

- クラウドコンピューティングに関する現状の標準化団体、フォーラムなどのリストをアップデートする。
- クラウドコンピューティングを支援するための新たな関連アイディアを集め、潜在的な研究分野を発掘する。
- 通信/ICTの視点から、クラウドコンピューティングのためのビジョン、価値のある提案などを集める。
- クラウドコンピューティングのための用語を提供し、既存の用語類を可能な限り、利活用する。
- 通信/ICTのネットワーク要件について、クラウドコンピューティングの標準化の適切な時期を見極める（Assess）。
- クラウドコンピューティングのサービス/アプリケーションを支援するために、通信/ICTのネットワーク要件、機能、能力を分析する。
- 将来のITU-Tの研究項目、及び関連アクションを提言する。

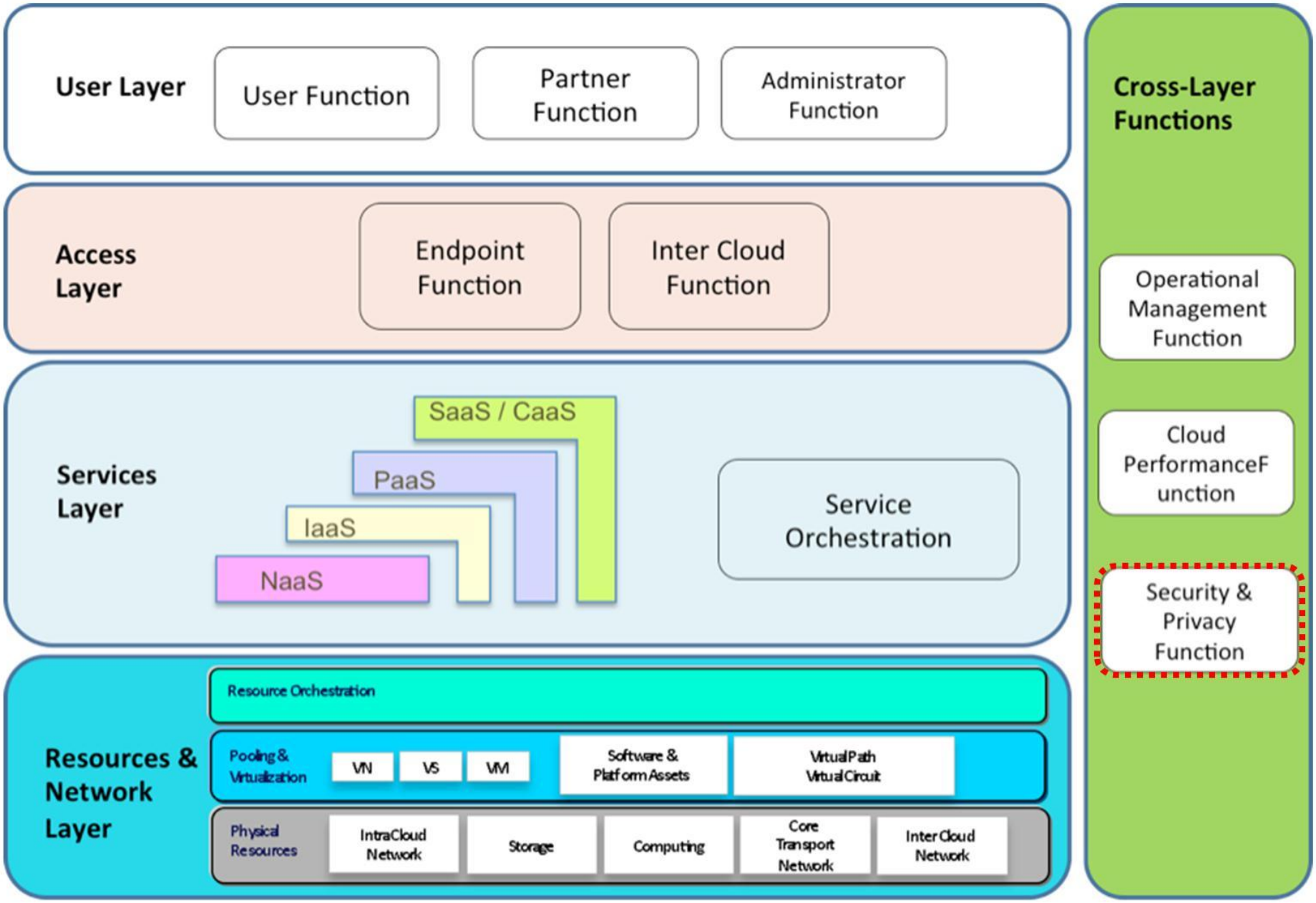
FGの成果物一覧

1) Introduction to the cloud ecosystem: definitions, taxonomies, use cases, high level requirements and capabilities
2) Functional requirements and reference architecture
3) Infrastructure and network enabled cloud
4) Cloud security, threat & requirements
5) Benefits of cloud computing from telecom/ICT perspectives
6) Overview of SDOs involved in cloud computing
7) Cloud resources management gap analysis

クラウド環境におけるプレイヤーとその役割

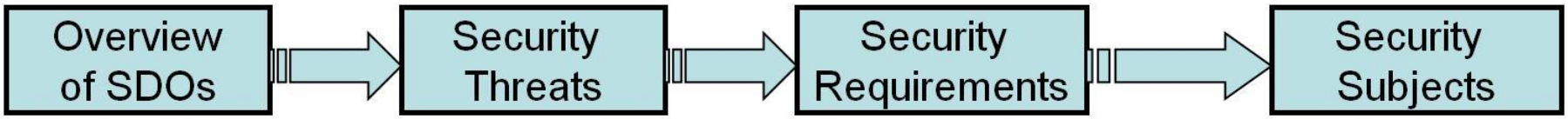


クラウド参照アーキテクチャ



セキュリティ成果物の進め方

1) 既存のクラウドセキュリティに関する活動調査
（CSA, DTMF, GICTFなど）
2) セキュリティに関する脅威の洗い出し
クラウド利用者、及びクラウドサービス提供者の視点
3) セキュリティ要求事項の洗い出し
クラウド利用者、及びクラウドサービス提供者の視点
4) ITU-Tにおけるクラウドセキュリティの研究項目の抽出



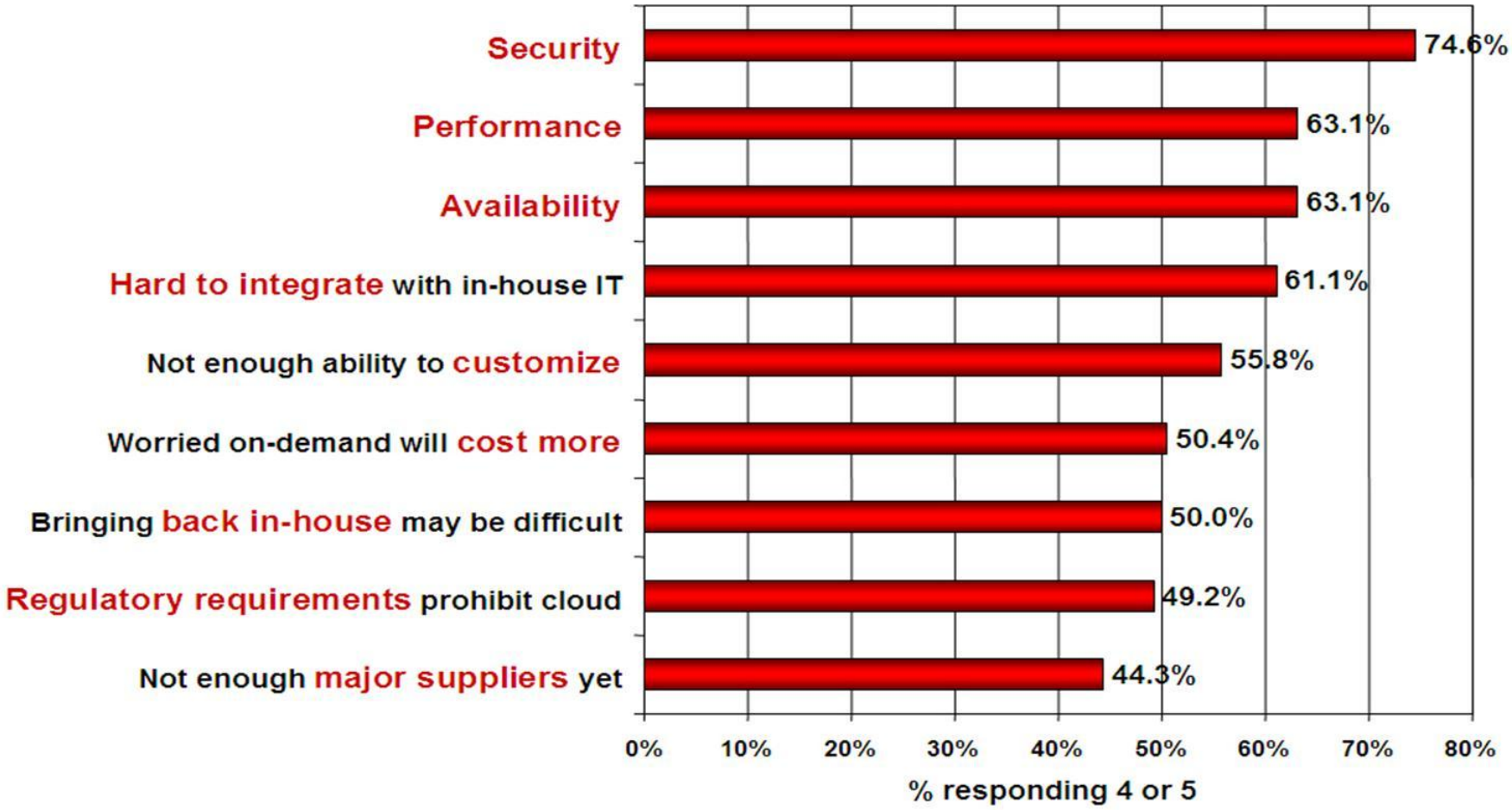
他SDO団体の活動調査

4.1 ENISA
4.2 CSA
4.3 DMTF
4.4 NIST
4.5 ISO/IEC JTC1/SC27
4.6 ISO/IEC JTC1/SC38
4.7 GICTF
4.8 ITU-T SG17
4.9 OASIS

（NIST） Security is the Major Issue

Q: Rate the challenges/issues ascribed to the 'cloud'/on-demand model

(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

（NIST） Cloud Securityの分析

- Some key issues:
  - trust, multi-tenancy, encryption, compliance
- Clouds are massively **complex systems** can be reduced to **simple primitives** that are replicated thousands of times and **common functional units**
- Cloud security is a “tractable” problem
  - There are both advantages and challenges

Former Intel CEO, Andy Grove: “only the paranoid survive”

GICTF

Introduction to Global Inter-Cloud Technology Forum (GICTF) and its Roadmaps

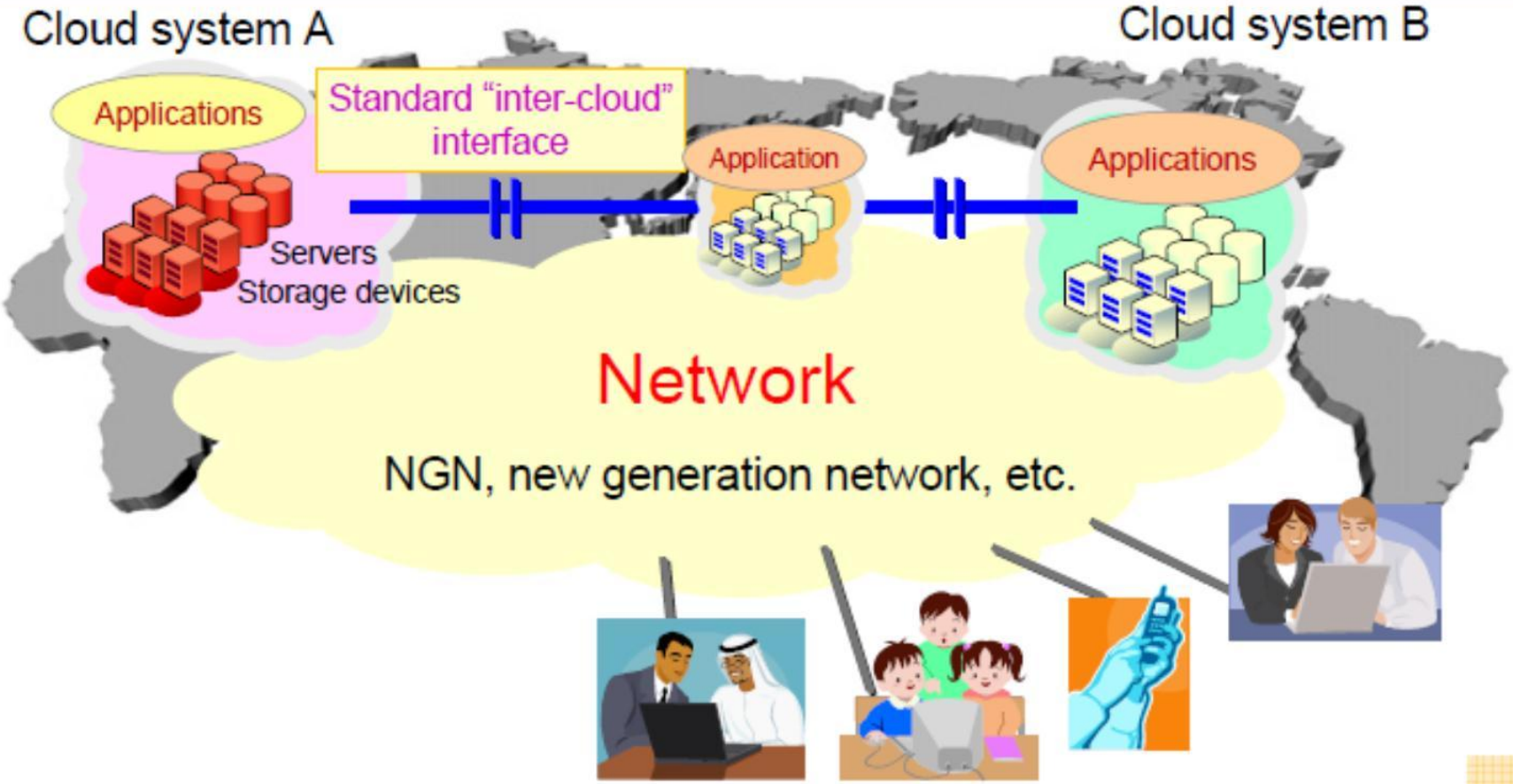
2010.6

グローバルクラウド基盤連携技術フォーラム（GICTF）からの入力

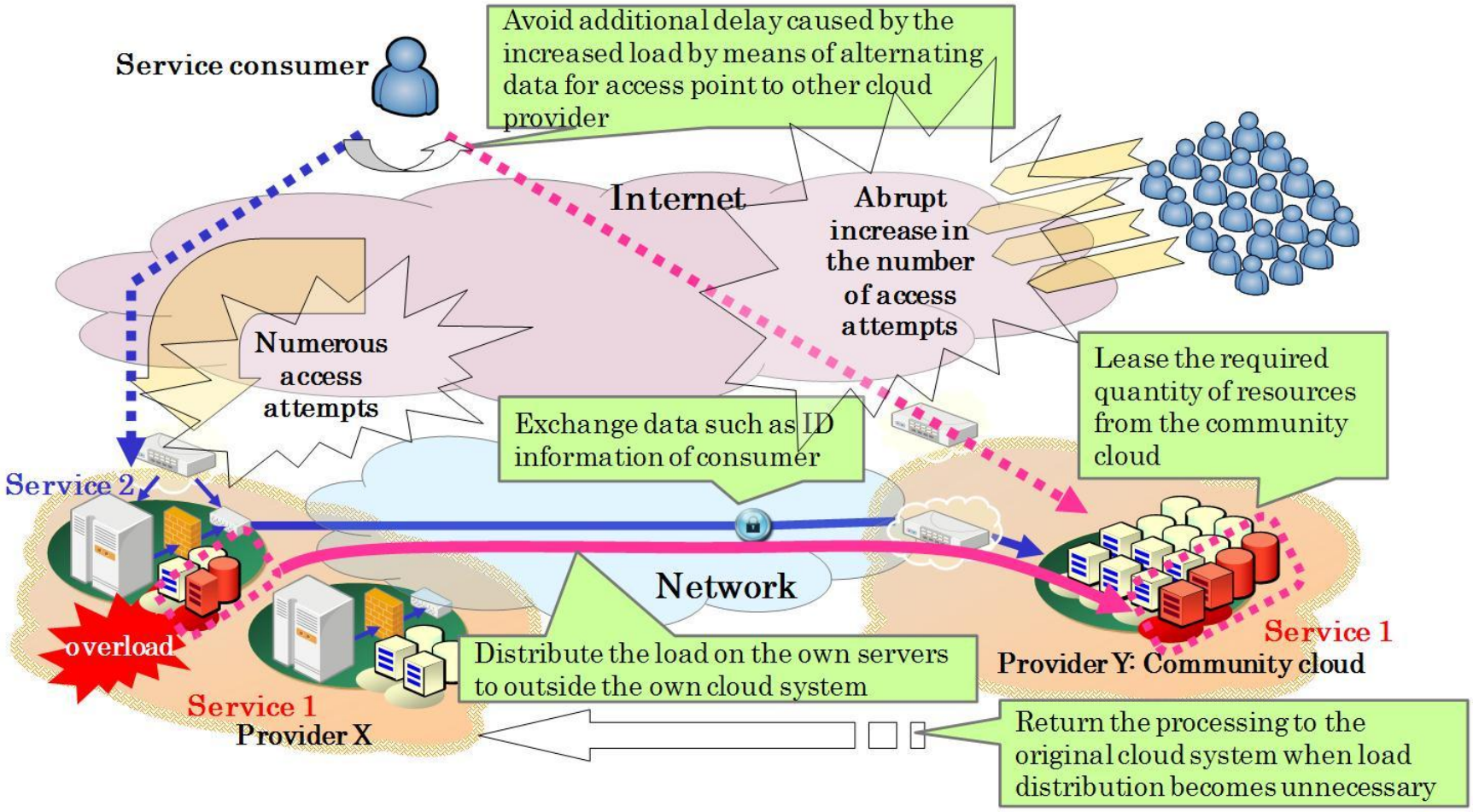
GICTF: A technology forum for the "Inter-cloud" era

Promotes the global standardization of inter-cloud system interfaces through collaboration between academia, government and industry

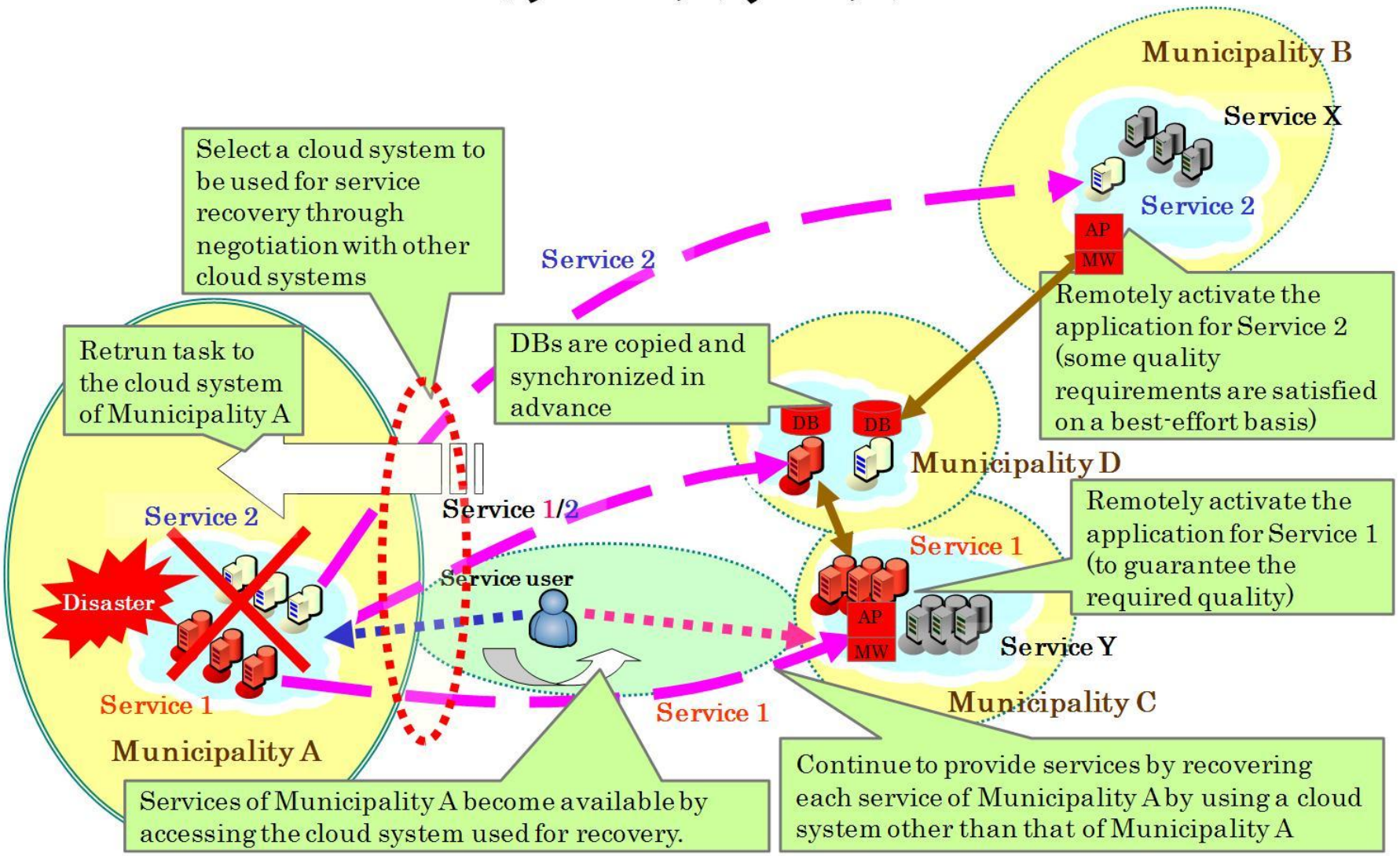
Established on July 17th 2009



急激な負荷増加に備えるための性能保証のユースケース（例）



災害や大規模障害における可用性保証のユースケース



クラウドコンピューティングにおける脅威

クラウドサービス利用者

- Responsibility Ambiguity
- Loss of Governance
- Loss of Trust
- Service Provider Lock-in
- Cloud Service User Remote Access
- Lack of Information/Asset Management
- Data loss and leakage
- Loss of Account/Service management

クラウドサービス提供者

- Responsibility Ambiguity
- Protection Inconsistency
- Evolutional Risks
- Business Discontinuity
- Supplier Lock-in
- License Risks
- Bylaw Conflict
- Bad Integration
- Unsecure Administration API
- Shared Environment
- Hypervisor Isolation Failure
- Service Unavailability
- Data Unreliability
- Abuse Right

クラウドコンピューティングにおける要求事項

利用者

- Method to trust cloud providers' security level
- Information/asset management.
- Confidentiality/integrity of data
- Proper account/identity management
- Service interoperability, portability & reversibility
- Interoperable Service interface & virtualization mechanisms
- Secure Virtual Machine

サービス提供者

- Hypervisor Protection
- Storage & Network Isolation
- Protection for Network Elasticity
- Interoperability
- Identity Management
- Disaster Recovery
- Data Traceability
- Secure VM Migration
- Trusted Compute Pools
- Different Security Models
- Multi-tenancy
- IP, License management & Jurisdictional Compliance
- Segregation of Role, Resource & responsibility
- Information & Data Quality Assurance

ITU-Tにおけるクラウドセキュリティの課題

- セキュリティ体系/モデル、及びフレームワーク
- セキュリティマネジメント、及び監査技術
- 事業継続性と事故からの復旧
- ストレージセキュリティ
- データ、及びプライバシー保護
- アカウント/ID管理
- ネットワークモニター、及びインシデント対応
- ネットワークセキュリティ管理
- インターオペラビリティ、及びポータビリティに関するセキュリティ
- 仮想化技術セキュリティ
- 法的規制に関する要件

セキュリティマネジメント、及び監査技術

a) クラウド利用者のためのセキュリティ要求条件に関わるガイドライン
b) クラウドサービス提供者の評価/監査するためのセキュリティ評価基準（クライテリア）
c) SLA（サービスレベル合意）の雛形に関わる規格

参考となるこれまでの検討：

1）ENISA（European Network and Information Security Agency)の検討
2）米国連邦政府のアプローチ（監査系）
3）経済産業省（日本）のアプローチ

ENISA検討

- クラウドにおける情報資産の整理
- クラウドにおけるリスクの検討
  ＊リスクの分類
    組織的リスク
    技術的リスク
    法的リスク
    共通なリスク
- クラウドにおける脆弱性評価項目

など

クラウドにおける情報資産の整理

情報資産	U	SP	重要度
企業の評判(ブランドなど)	○		最高
従業員の忠誠度、経験	○		最高
Sensitiveな個人情報（病歴など）	○	○	最高
実時間サービスの提供状況（品質など）	○	○	最高
アクセス制御、認証、権限付与の情報	○	○	高
アクセス時の認証情報、証明書	○		最高
取得したISO,PCIDSS等の認証	○	○	高

注:重要度は、最低、低、中、高、最高で分類。上記は一部の抜粋で、そのほかに16の情報資産(従業員情報、管理用インタフェース、セキュリティログ、バックアップ情報など)が抽出、整理されている。

クラウドにおける組織的リスク

リスク	頻度	影響度	リスク
ロックイン（SPに囲い込まれる）	高	中	高
ガバナンスの喪失（企業からの制御が利かない）	最高	最高	高
コンプライアンスの対応	最高	最高	高
共有サービスの利用による企業評価の低下	低	高	中
SP停止、中断（障害などによる）	ー	最高	中
SPの買収（セキュリティ要件が変更される）	ー	中	中
サプライチェーンのトラブル（サービス中断）	低	中	低

注:リスクは、低、中、高で分類。リスク値については、影響度と頻度により分析している。

クラウドにおける技術的リスク

リスク	頻度	影響度	リスク
リソース過不足の問題	中/低	中/低	中
同SP上の他ユーザ企業の影響を受ける	中/低	最高	高
内部犯罪（特権を利用した情報漏洩など）	中	最高	高
通信経路での盗聴、中間者攻撃など	中	高	中
データ漏洩	中	高	中
SPによるデータ消去漏れ	中	最高	中
DDoSによるリスク	中/低	高/最高	中

注:リスクとして、上記は抜粋。その他、13(暗号鍵の喪失、ハイパーバイザーの脆弱性、SPとユーザのセキュリティレベルの差異など)が抽出、整理されている。

その他のリスク

- 法的リスク
  - 証拠保全のリスク（高）
  - 司法権の違いによるリスク（高）
  - データ保護に関わるリスク（高）
  - ライセンスに関わるリスク（中）
- 共通リスク
  - NWダウンによるサービス中断（中）
  - NWの運用トラブル（高）
  - 権限奪取のリスク（中）
  - バックアップ失敗、盗難のリスク（中）
  - 機器盗難のリスク（低）
  - 災害のリスク（低）　等など

ENISAでは、これらのリスク分析の結果、主にSPの脆弱性を評価する項目を洗い出しており、全体で53項目に及ぶ。

米連邦政府におけるクラウドサービス調達の要件策定

- 連邦政府のクラウドサービス調達に際して当該サービスが一定のセキュリティ要件を満たしていることを承認・認可するプログラム「FedRAMP（Federal Risk and Authorization Management Program）」の枠組みの案「Proposed Security Assessment & Authorization for U.S. Government Cloud Computing（Draft 0.96）」が、2010年11月2日に、CIO評議会により公表された。
- 同枠組みには、連邦政府が利用するクラウドサービスのセキュリティ要件、FedRAMPのガバナンス、FedRAMPによる承認・認可（A&A: Assessment & Authorization）の手順が示されている。

- CIO評議会とは、28の連邦省庁のCIO及び副CIOから構成される評議会。議長はOMB副局長が努める。ITマネジメントポリシー等を策定する役割を担っている。

セキュリティ要件のベースライン

低及び中程度の影響を及ぼすクラウドサービスにおいてベースラインとすべきセキュリティ要件のリストを提示。このリストはNIST SP800-53Rev3[1]を基に作成されており、以下の分類で総計187項目から構成されている。連邦政府が調達するクラウドサービスはこれらの要件を満たすことが求められる。

[1] SP800-53 Recommended Security Controls for Federal Information Systems and Organizations http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

1）アクセス制御
2）意識向上およびトレーニング
3）監査および説明追跡性
4）承認と運用認可
5）構成管理
6）緊急時対応計画
7）識別および認証
8）インシデント対応
9）保守
10）記録媒体の保護
11）物理的および環境的な保護
12）計画作成
13）人的セキュリティ
14）リスクアセスメント
15）システム及びサービスの調達
16）システム及び通信の保護
17）システム及び情報の完全性

継続的なモニタリング

FedRAMP及びクラウドサービス提供者によるクラウドコンピューティングシステムのモニタリングについて、その内容と報告頻度を提示。報告基準についてはFISMA（連邦情報セキュリティ管理法）の基準との整合性が図られている。以下の13項目の報告で構成される。連邦政府が調達したクラウドサービスはこれらの項目について継続的なモニタリングを実施し、定期的に報告書を作成することが求められる。

1）全システムの調査（毎月）
2）FDCC遵守の証明（四半期毎）
3）緊急対応計画（毎年）
4）POAMの改善（四半期毎）
5）チェンジコントロールプロセス（毎年）
6）侵入テスト（毎年）
7）第三者検証（半年毎）
8）境界に変更がないことの確認（四半期毎）
9）システム構成管理ソフトウェア（四半期毎）
10）FISMA報告のデータ（四半期毎）
11）文書の更新（毎年）
12）緊急時対応計画（毎年）
13）デューティマトリックスの分離（毎年）
14）認知向上とトレーニング（毎年）

POAM: Plan of Action and Milestones, FDCC: Federal Desktop Core Configuration
FISMA: Federal Information Security Management Act

評価・承認の手続き

- NISTが策定したリスク管理に関する文書SP800-37Rev1を基に、FedRAMPの評価・承認の手続と、この手続きにおけるFedRAMP事務局、クラウド担当省庁(Sponsoring Agency)、クラウド提供事業者等の役割を提示。
- この手続きを実行するために、FedRAMPの最終意思決定機関としてJAB (Joint Authorization Board)を設置する。JABの構成員は、DHS、DOD、GSAの3省庁を常任メンバーとし、この他にクラウドサービス毎の担当省庁が非常任メンバーとして加わる。技術的な専門事項については、JABメンバーが任命した技術担当者取り扱う。
- 評価・承認の手続きの基本的な流れは、クラウドサービスを導入しようとする省庁が当該クラウドサービスの担当省庁となってFedRAMPにクラウド利用申請を行い、FedRAMPが当該クラウドサービスが諸基準を満たしていることの評価を行い、基準が満たされていことが確認されればFedRAMPが当該クラウドサービスの利用を承認するというもの。また、担当省庁がクラウドサービスを導入した後にはFedRAMPがクラウドサービスの継続的なモニタリングを監督する。この手続きは具体的には次の7段階で構成される。

ISO/IEC JTC1/SC27における
クラウドセキュリティの検討
（経済産業省のアプローチ）

ISO/IEC JTC1/SC27における審議
Joint WG Study Period on Cloud Computing Security and Privacy (Oct 2011)

Oct 2010 to Apr 2011

- Whitepaper
- Study Report
- NP ISO/IEC 27017-2

Extended Study Period (Apr to Oct 2011)

- SC 7 - NP Software Behaviour Trust Management

ISO/IEC 27017-1

- Requirements for Cloud Computing Service Provider (CCSP) Management Scheme
- Management, governance, risk, and compliance

ISO/IEC 27017-2

- CCSP information security code of practice (ref ISO/IEC 27002)
- NP

Security Controls for Clouds (27017)

ISO/IEC 27017-3

- CCSP Legal and regulatory code of practice
- Including advice and guidance on privacy and data protection

Data Protection for Clouds (27018)

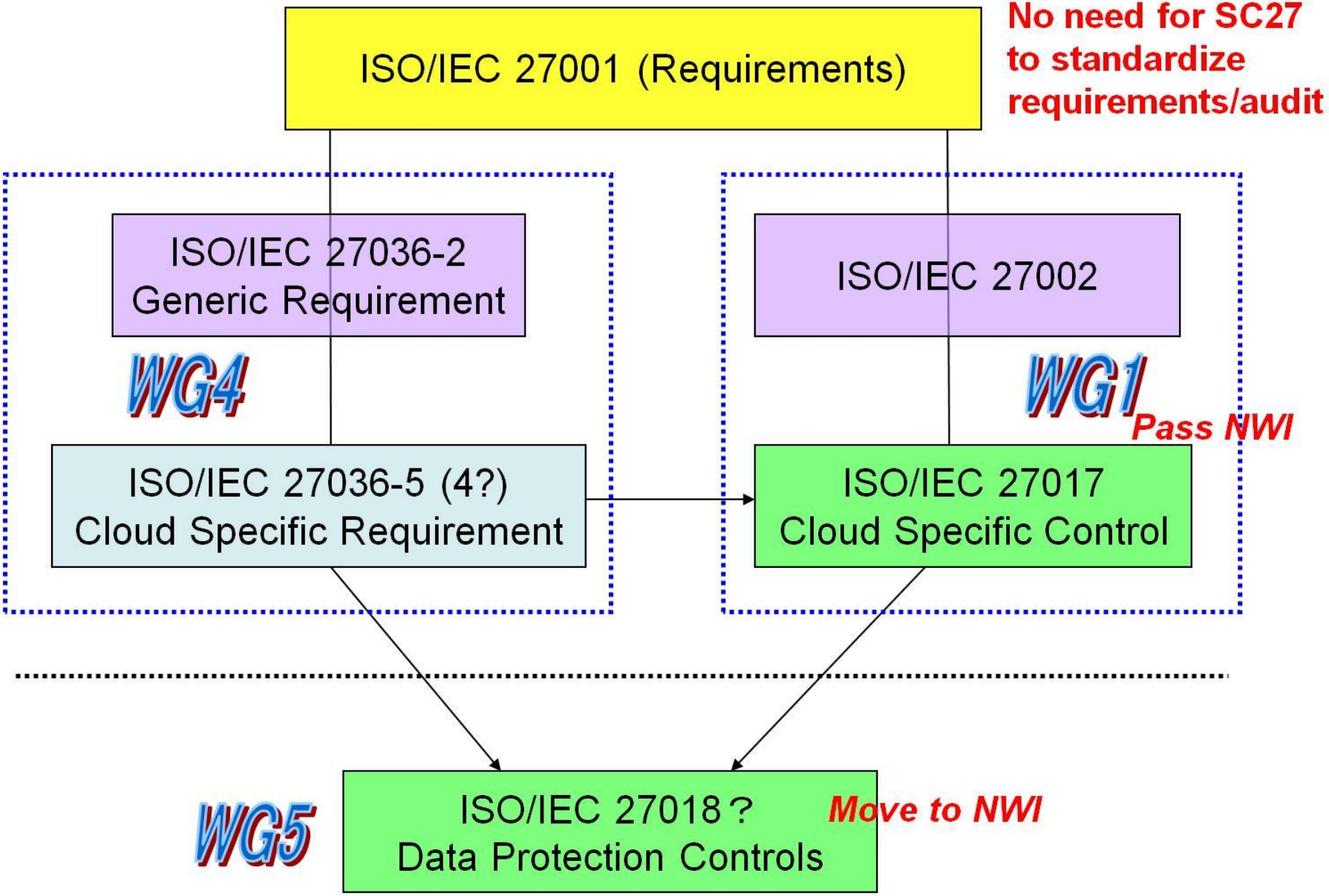
ISO/IEC 27017-4

- CCSP Service code of practice (based on WG 4 standards)

ISO/IEC 27017-5

- CCSP Audit guidelines

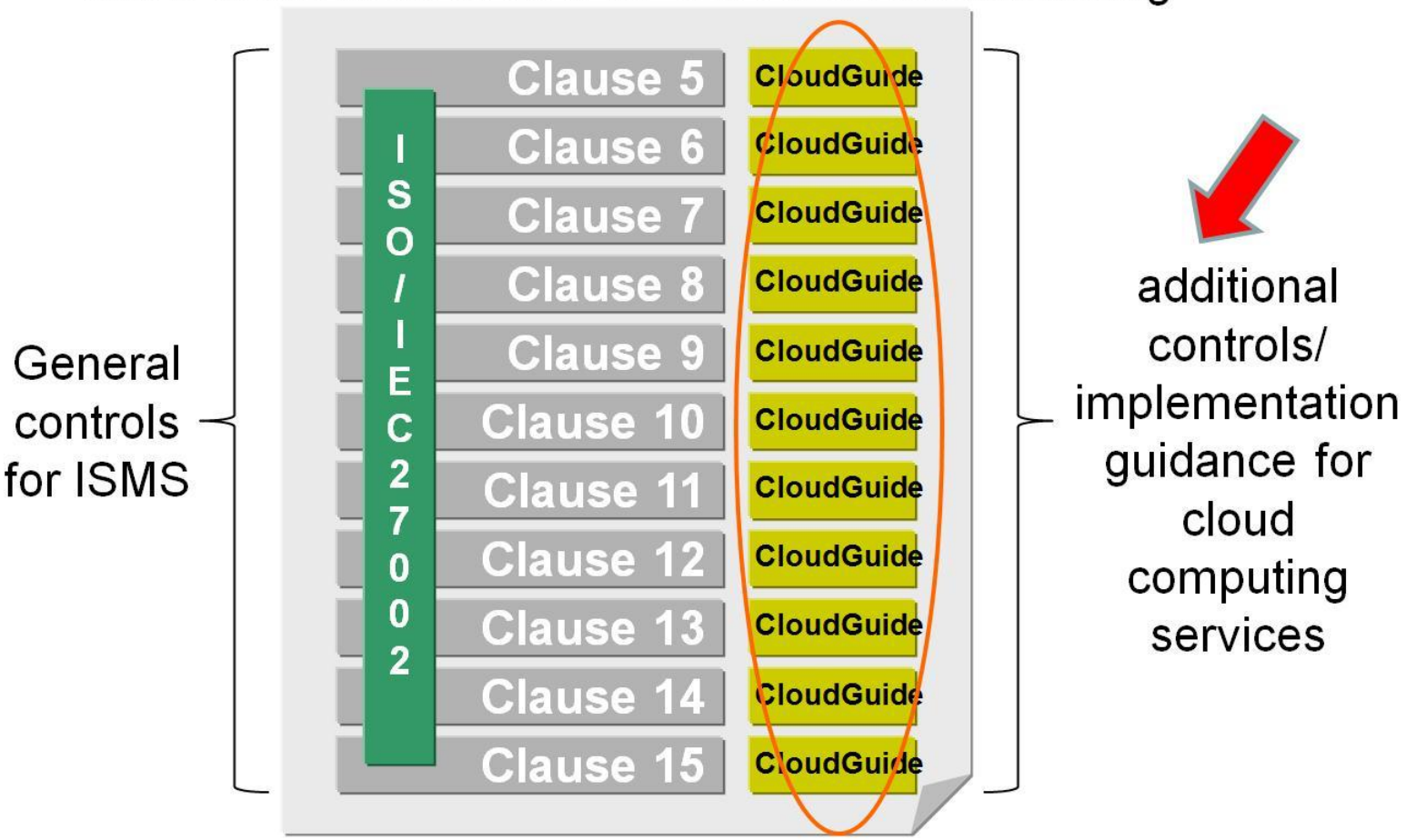
クラウドセキュリティに関するSC27 WG1, WG4 & WG5 （ケニヤ会合）の結果



具体的なアプローチとしては

クラウドサービスにおける共通な理解を得るために、ISMSの考え方を適用し、クラウド用に補足的な管理策(Controls)、実施のガイダンス(Implementation Guidance)を抽出する。

ISMS is the mechanism for common understanding



ガイドライン記載のルール

Rules

(1) Implementation guidance for cloud user to do

- クラウド利用者がクラウドサービスの利用において自ら実施する事項の手引を記述する。

(2) Requests for service provider

- クラウド利用者がクラウドサービスの利用においてクラウド事業者が行う事項について確認すべき事項を記述する。
- クラウド利用者がクラウドサービスの利用においてクラウド事業者に対して実施を求める事項を記述する。

Note.

- クラウド事業者が自らの情報セキュリティ対策として行う事項であって、クラウド利用者の情報セキュリティ対策とすることを主たる目的としないものは、記述しない。
- クラウド利用者が要求してもクラウド事業者が対応しないと一般的に想定される事項は、記述しない。（例えば、物理的な管理策）
- ISO/IEC 27002の実施の手引に既にある記述に対してクラウドサービス利用における補足説明を加える場合には、当該補足説明は「クラウド利用者のための関連情報」に記述する。

ネットワーク監視、インシデント対応に関する技術

- クラウドサービス利用者にとって、セキュリティに関わる事故（インシデント）の対応、及び必要な監視（特にネットワーク）が重要となる。
- これまでのインシデント対応技術の活用が可能であるが、具体的なクラウドサービス提供者内部での監視、インシデント発生における迅速な対応を実現するためには、よりクラウドに特化した検討が必要となる。
- ＣＳＡでは、 Telecommunication WGにてクラウドCERTなどの検討を開始している。
- 本技術検討の実施にあたり、ITU-Tですでに勧告化がなされているX.1500 (CYBEX)の活用が有効である。

ITU－T勧告X．1500
Cybersecurity information exchange framework (CYBEX)

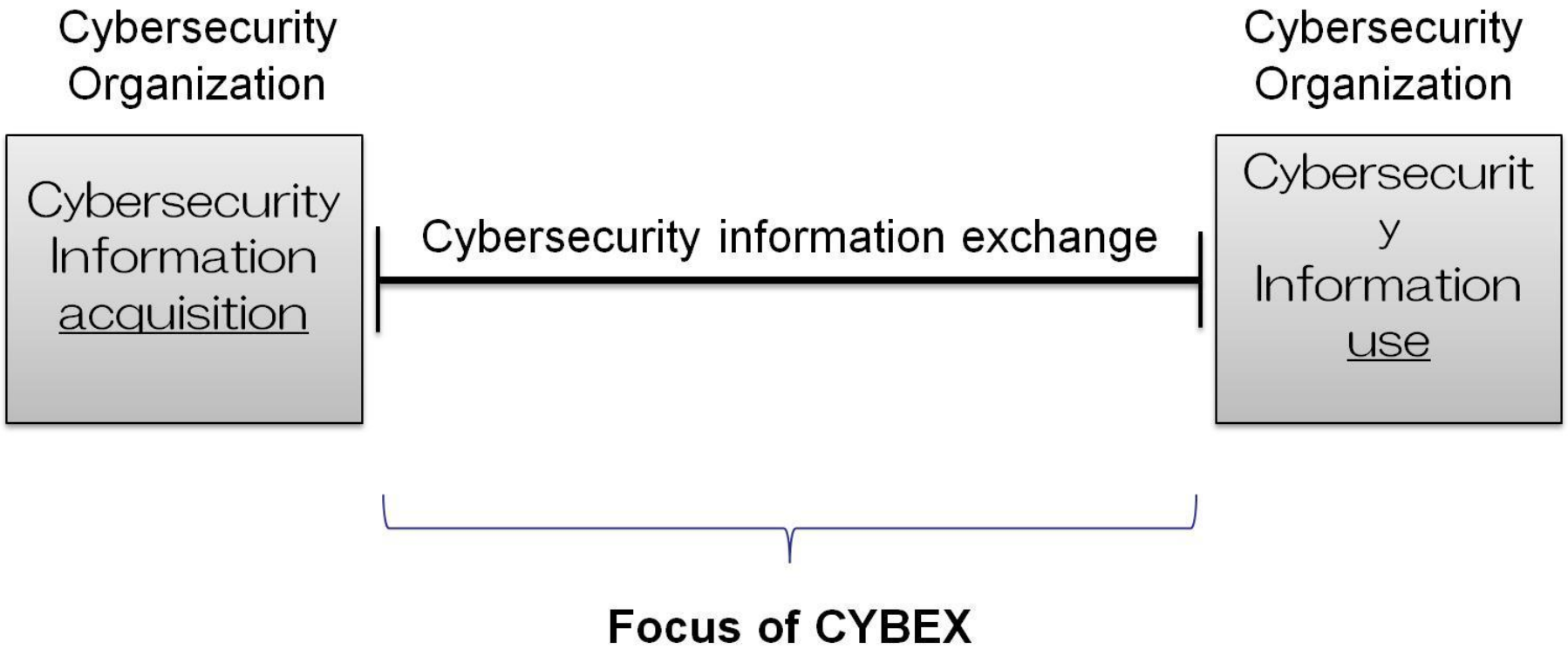
CJK-SWISS 2011 高橋氏（NICT）資料からの抜粋

「CYBEX」とは、サイバーセキュリティ情報の交換のための技術的なフレームワークを提供することを目的とする。

多様化、高度化するサイバー空間の脅威に対抗するため、脆弱性、攻撃手法などの情報交換が有益

Source: http://www.atmarkit.co.jp/fsecurity/rensai/cybex01/cybex01.html

CYBEX（勧告X．1500）の交換フレームワーク



概要:

CYBEX は、ネットワークを介して、サイバーセキュリティ情報を交換するために、以下の4つの機能ブロックを規定している。

Information Description block	This block structures cybersecurity information	→ Appendices of X.1500
Information Discovery block	This block identifies and discovers the above structured information	→ X.1570 (next section)
Information Validation block	This block ensures the validity of the information	
Information Transport block	This block exchanges cybersecurity information over networks	

勧告X．1500のAppendix Aには、以下に示す多くの機能仕様が規程されている。これらは、サイバーセキュリティ情報として用いられる。

CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CWSS	Common Weakness Scoring System
OVAL	Open Vulnerability and Assessment Language
XCCDF	eXtensible Configuration Checklist Description Format
CPE	Common Platform Enumeration
CCE	Common Configuration Enumeration
ARF	Assessment Result Format
CEE	Common Event Expression
IODEF:	Incident Object Description Exchange Format
CAPEC	Common Attack Pattern Enumeration and Classification
MAEC	Malware Attribution Enumeration and Characterization Format
PFAM	Phishing, fraud and misuse format

参考文献

- “CYBEX – the Cybersecurity Information Exchange Framework (X.1500),” ACM CCR, http://ccr.sigcomm.org/drupal/?q=node/691, October 2010

- “Ontological Approach toward Cybersecurity in Cloud Computing,” ACM SIN (awarded best paper), September 2010

- Cybex Information Exchange Tool (cybiet) -- A Cybex Discovery and Cybex BEEP profile implementation, http://cybiet.sourceforge.net/

- “Global Developments in Cybersecurity Information Exchange Framework”, invited talk@AINTEC, ACM, November 2010(coming soon)

…etc.

仮想化(バーチャライゼーション)セキュリティ(１)

-VM内(VMInternal)の攻撃/脆弱性

- 仮想マシン上のOS管理
- I/O Fuzzing攻撃
  （仮想マシンのデバイスを過剰に叩き、管理OS乗っ取りや悪意あるコードの挿入を行う）
- メモリエラーが引き金になる脆弱性
  （悪意のあるコードにジャンプする仕組みをメモリ内に敷き詰め、メモリエラーを待つ）
- ランダムにならない乱数
  （仮想マシンモニタは仮想マシンの実行途中を保存するスナップショット機能を提供。スナップショットイメージを複数回使うと前の疑似乱数生成を繰り返すことになる）

JITA講演資料「IaaS型クラウドにおける仮想マシンのセキュリティ課題」須崎氏(AIST)より

仮想化(バーチャライゼーション)セキュリティ(2)

-VM間(Cross VM)の攻撃/脆弱性

- 物理キャッシュによるサイドチャネル攻撃
  (セットアソシアティブキャッシュを共有している「悪意のあるVM」が連続してキャッシュを叩く。キャッシュの反応が遅れると他のVMでアクセスしていることが判り、限定した環境だが鍵漏洩の恐れあり)
- 仮想マシンメモリの覗き見
  (既存の物理メモリへの覗き見攻撃。管理OSを乗っ取られればVM Introspection機能から可能)
- 仮想ネットワークによるセキュリティ障害
  (仮想マシンモニタでは、同一物理マシン上の仮想マシン間を高速な仮想ネットワークで繋ぐため、全通信が仮想マシンモニタ内に閉じ込められ、フィルタリング、ネットワーク型IDSなど既存のツールを利用できない。)
- LiveMigration時のRootKit混入
  (VM移動中にRootkitを仕込まれてしまう)

JITA講演資料「IaaS型クラウドにおける仮想マシンのセキュリティ課題」須崎氏(AIST)より

FGからTSAGへの報告と結果

ＦＧからＴＳＡＧへの報告：

- 成果物
- 内容のサマリー

ＴＳＡＧでの審議結果：

1．関連する他のSGとのコーディネーションを行うため、SG13 (Future Networks) をクラウドに関するリードSGに指名する。ただし、
   - 他の関連するSG、例えば、気候変動：SG5, プロトコル SG11, QOS:SG12, セキュリティ：SG17 との密接なコラボレーションが必要である。
   - 上記の各SGの必要な “Coordination” の責任を保持する
2．他のSDOとの積極的なコラボレーション（とりわけJTC1 (ISO & IEC) との共同作業）を継続する。
3．本TSAG会合においてJCA (Joint Coordination Activity) の設立が決定した。親SGはSG13。
4．FG デリバラブルをパブリッシュ (Publicly available) する。
5．Regulatory関連の勧告化にはTAPを適用する。

まとめ

● クラウドセキュリティ

- ✓ 既存のセキュリティ脅威の多くがそのままクラウドの脅威となる。
- ✓ 多くの団体において、クラウドセキュリティの研究がなされている。（CSA, ENISA, NIST　など）
- ✓ ITU-Tでは、FGでの検討が一段落し、具体的な標準化に向けた検討が開始される段階に来た。

● 情報セキュリティ対策の強化、及び今後の動向

- ✓ 多くの団体で同じ検討を並行して実施していくより、お互いが連携し、より完成度の高いものを共通ドキュメントとして作成する必要がある。
- ✓ クラウドセキュリティの体系化、クラウドセキュリティマネジメント、クラウド第3者監査、クラウドインシデント対応などの検討が優先的に実施されるべきである。
- ✓ さらに、クラウドサービスの提供が国の境界を跨った形で実施されることを考慮し、法規制に関わるガイドラインなどの整備も重要となる。（国際規格化になるか否かは不明）

Thank you for listening Q&A