クラウド導入に向けた情報セキュリティ技術の最先端

～JNSA/ISFにおける共同研究成果を含む～

中尾　康二
KDDI株式会社
情報セキュリティフェロー

Designing The Future
KDDI

Agenda

- クラウドの脅威の元となる、マルウェアについて
- ITU－T FG　クラウドコンピューティングの位置づけ
  ＊目的、方向性など
- ITU－T FG　クラウドコンピューティング報告
  ＊各関連活動の紹介
  ＊成果物の紹介
  ＊クラウドセキュリティの検討結果（現状）
- 今後の方向性　　JNSA内検討、ISFとの連携視点で

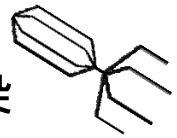
Designing The Future
KDDI

マルウェア関連用語

～ マルウェアの感染形態に着目した分類～

● ウイルス（狭義のウイルス）

- ✓ 単体動作せず，自分自身を他のファイルやプログラムに寄生
- ✓ ブートセクタ感染型：ハードディスクなどのシステム領域に感染
- ✓ ファイル感染型：実行可能ファイルを主な感染対象



ウイルス

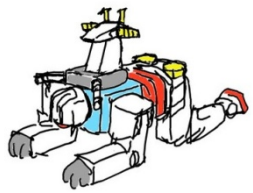
● ワーム

- ✓ 単体で動作し自己増殖を行う
- ✓ ウイルスに比べ高い感染力を有し，大規模感染を引き起こす
- ✓ 電子メールやリムーバブルメディア（USBメモリ等）を媒体とするもの
- ✓ Windowsのファイル共有やメッセージング機能を利用するもの
- ✓ OSやアプリケーションの脆弱性に対する攻撃コードを用い

ワーム

● トロイの木馬

- ✓ 有用なプログラムやファイルに偽装
- ✓ ユーザ自身によるシステムへのインストールや起動を誘う
- ✓ 感染機能を持たないものが多い



トロイの木馬

出典：GIZMODE Japan

マルウェア関連用語
～ マルウェアの目的に着目した分類～

- スパイウェア
  - ✓ 個人情報や行動履歴を収集し，特定のサーバなどに送信する
  - ✓ ユーザのキーボード操作を記録・収集するキーロガーもスパイウェアの一種

- アドウェア
  - ✓ ユーザに企業広告などを提示することを目的にしたプログラム
  - ✓ ユーザの同意なしに広告を頻繁にポップアップ／Webサイトに強制誘導

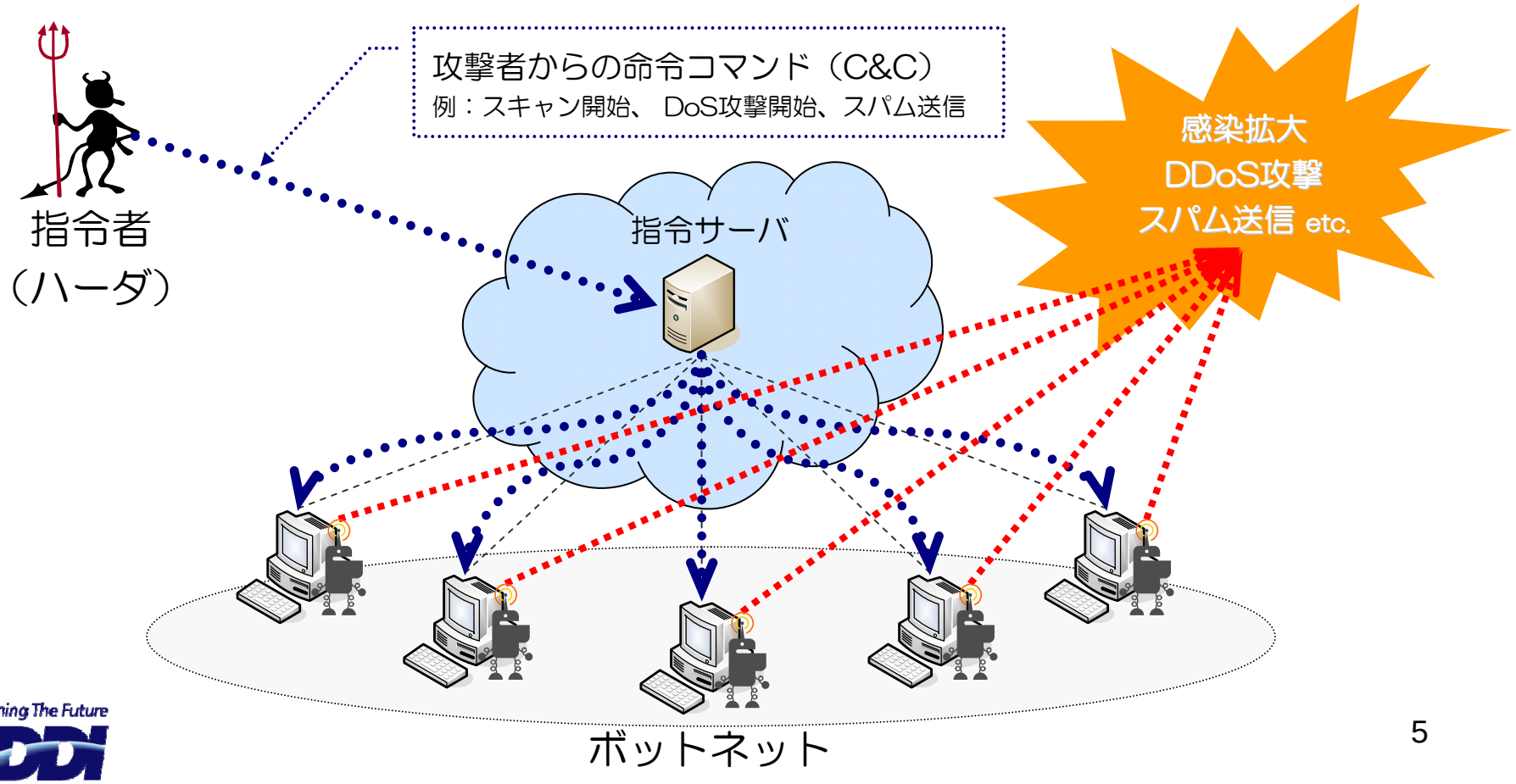
- ランサムウェア
  - ✓ ユーザのPC上のデータを強制的に暗号化／パスワード付きZIP圧縮
  - ✓ データの復号や解凍の見返りとしてユーザから身代金（ransom）を搾取

- スケアウェア
  - ✓ ユーザに虚偽の情報（マルウェア感染等）を提示
  - ✓ 不安（scare）を煽り無意味なソフトウェアを販売

4

マルウェア関連用語
～ その他の分類 ～

- ボット
  - ✓ 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）



マルウェア年表
（1970年～2010年）

年	Malware
1970	
1971	Creeper (1st worm)
1972	# The term “virus” first appeared in a SF novel “When H Was One”.
1973	
1974	
1975	# The term “worm” first appeared in a SF novel“The Sho Rider”.
1976	
1977	
1978	
1979	
1980	Xerox PARC Worm
1981	
1982	Elk Cloner(1st virus)
1983	
1984	# Cohen defined virus in his paper “Computer Viruses - T and Experiments”.
1985	
1986	Brain (1st IBMPC virus), PC-Write (1st Trojan horse), Vi
1987	Cascade, Jerusalem, Lehigh, Christmas Tree, MacMa
1988	Byte Bandit, Stoned, Scores, Morris Worm
1989	AIDS(1stransomware), Yankee Doodle, WANK

発見の時代

年	Malware
1990	1260 (1st polymorphic virus), Form, Whale
1991	Tequila, Michelangelo, Anti-Telefonica, Eliza
1992	Peach (1st anti-antivirus programs), Win.Vir_1_4 (1st Wi virus)
1993	PMBS
1994	Good Times (1st hoax)
1995	Concept (1st macro virus)
1996	Laroux, Staog (1st Linux m.w.)
1997	ShareFun, Homer, Esperanto
1998	Accessiv, StrangeBrew (1st Java m.w.), Chernobyl
1999	Happy99, Tristate, Melissa, ExploreZip, BubbleBoy, Babylo
2000	Loveletter, Resume, MTX,Hybris
2001	Anna Kournikova,BadTrans, CodeRed I, Sircam,CodeRe Nimda, Klez
2002	LFM-926 (1st Flash m.w.), Chick, Fbound,Shakira, Bugbe
2003	Sobig, SQLSlammer, Deloder, Sdbot, Mimail, Antinny, M Welchia, Agobot, Swen, Sober
2004	Bagle, MyDoom, Doomjuice, Netsky,WildJP, Witty,Sasse Bobax, Rbot, Cabir(1stSymbianm.w.), Amus, Upchan , Re Lunii, Minuka, Vundo
2005	Bropia, Locknut,BankAsh,Banbra, Anicmoo, Commwarr Pgpcoder, Zotob, Gargafx, Peerload, Cardblock,PSPBricl m.w), DSBrick (1st Nintendo DS m.w.), Dasher
2006	Kaiten, Leap (1st Mac OS X m.w.),Redbrowser, Cxover,E Mdropper,Flexispy, Spaceflash,Stration, Mocbot, Fujacks
2007	Storm Worm,Pirlames, Zlob, Srizbi (1st full-kernel m.w.), Pidief
2008	Mebroot,Infomeiti, Conficker
2009	Virux, Yxes,Gumbler, Induc, Ikee (1stiPhonem.w.)
2010	Zimuse, Trojan-SMS.AndroidOS.FakePlayer (1st Androidm. Stuxnet

実験的試行の時代

悪用の時代

過去最悪のパンデミックConficker

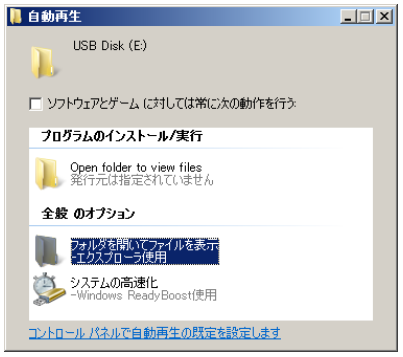
- 2008年10月23日 Microsoft緊急セキュリティ情報
  - MS08-067
  - 同日、セキュリティ更新プログラムをリリース
- MicrosoftServer Service の脆弱性
  - リモートからのバッファオーバーフローが可能
- Conficker（別名Downadup）出現
  - 2008年11月21日
- Microsoftが25万ドルの懸賞金
  - 2009年2月12日
- Blaster以来の大規模感染が続く･･･

Conficker の感染数

- **約900万ホスト（2009年1月時点）**
  - F-SECURE社調べ
  - 計測方法：Downadupが生成するドメインを実際に取得して、感染ホストからのコネクション（の中に含まれる感染数カウンタの値）を計測
- **約1200万ホスト（2009年2月時点）**
  - ARBOR Networks社調べ
  - 計測方法：同様

Conficker の感染経路

- **リモートエクスプロイト**
  - MS08-067の脆弱性をネットワーク経由で攻撃（445/tcp）
- **ネットワーク共有（NetBIOS）**
  - ID/パスワードを辞書攻撃
- **リムーバブルメディア**
  - USBメモリなどのAutorun機能により感染



日本のセキュリティチーム (Japan Security Team)
http://blogs.technet.com/jpsecurity/archive/2009/01/24/3191000.aspx

PCMAG.COM BLOGS, Security Watch
http://blogs.pcmag.com/securitywatch/2009/01/bug_in_autorun_on_windows.php

Conficker の特徴・機能 (1/2)

- **DLL形式で拡散**
  - 既存のプロセス内にリモートスレッドを生成してDLLを挿入
  - APIフック（DLLインジェクション）の典型的テクニック
- **UPnPを利用してファイアウォールにポートマッピング要求**
  - ハイポートでバックドアを生成
  - バックドア経由でアップデート
- **UTCをシードに3時間ごとにランデブーポイント（URL）を生成**
  - ランデブーポイントからターゲットのIPアドレスリストを取得
  - ダウンロードデータは公開鍵暗号方式で署名検証
- **IP geo-locationを基にターゲットの言語環境を推測**
  - Downadup.A: IP geo-locationをmaxmindから取得
  - Downadup B: IP geo-locationをRC4で暗号化して自身で保持

Conficker の特徴・機能 (2/2)

- **複数のWindowsサービスを停止**
  - Windows Update Service
  - Background Intelligent Transfer Service
  - Windows Defender
  - Windows Error Reporting Services

- **特定の文字列を持つオンラインサービスに接続不可**
  - Virus, spyware, malware, rootkit, defender, microsoft, symantec, norton, mcafee, trendmicro, sophos, panda, etrust, networkassociates, computerassociates, f-secure, kaspersky, jotti, f-prot, nod32, eset, grisoft, drweb, centralcommand, ahnlab, esafe, avast, avira, quickheal, comodo, clamav, ewido, fortinet, gdata, hacksoft, hauri, ikarus, k7computing, norman, pctools, prevx, rising, securecomputing, sunbelt, emsisoft, arcabit, cpsecure, spamhaus, castlecops, threatexpert, wilderssecurity, windowsupdate

- **システムの復元ポイントをリセット**

- **アンチVM、アンチデバッグ機能**

- **SYNフラッディング実行のためレジストリを変更**

HKLM¥SYSTEM¥CurrentControlSet¥Services¥Tcpip¥Parameters
"TcpNumConnections" = "0x00FFFFFE“

etc. etc...

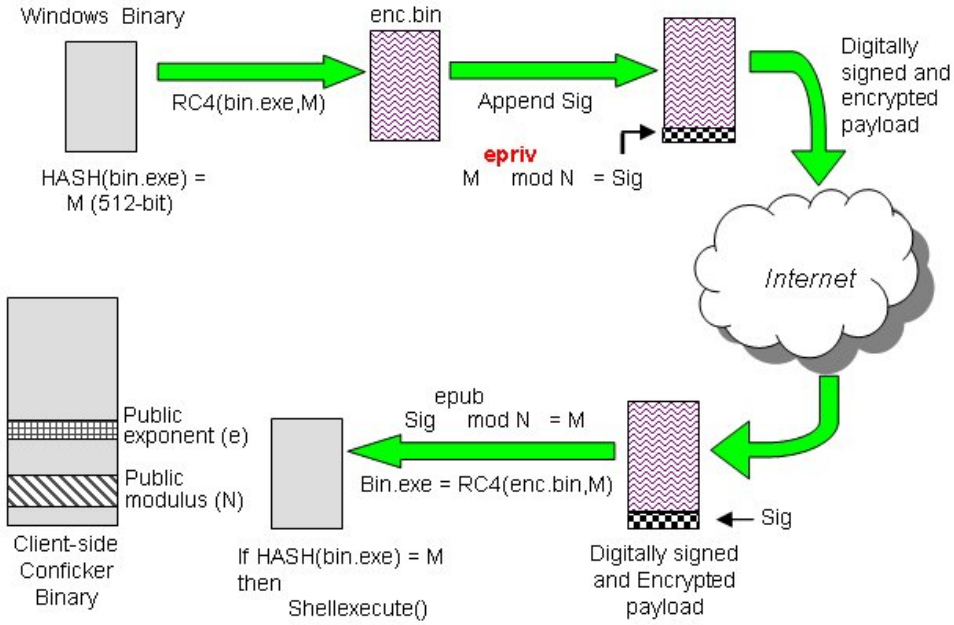
Confickerのペイロード暗号化・署名手法

送信者側

- ペイロードのハッシュ値M生成
- Mを共通鍵としてRC4によるペイロード暗号化
- Mをeprivで署名→Sig（RSA方式）

受信者側

- Sigをepubで署名検証
- 得られたMでペイロードを復号
- 復号後のペイロードのハッシュ値とMを比較して一致すれば実行



- Downadup.A: 法N 1024bit
- Downadup B: 法N 4098bit

SRI International, Technical Report
http://mtc.sri.com/Conficker/

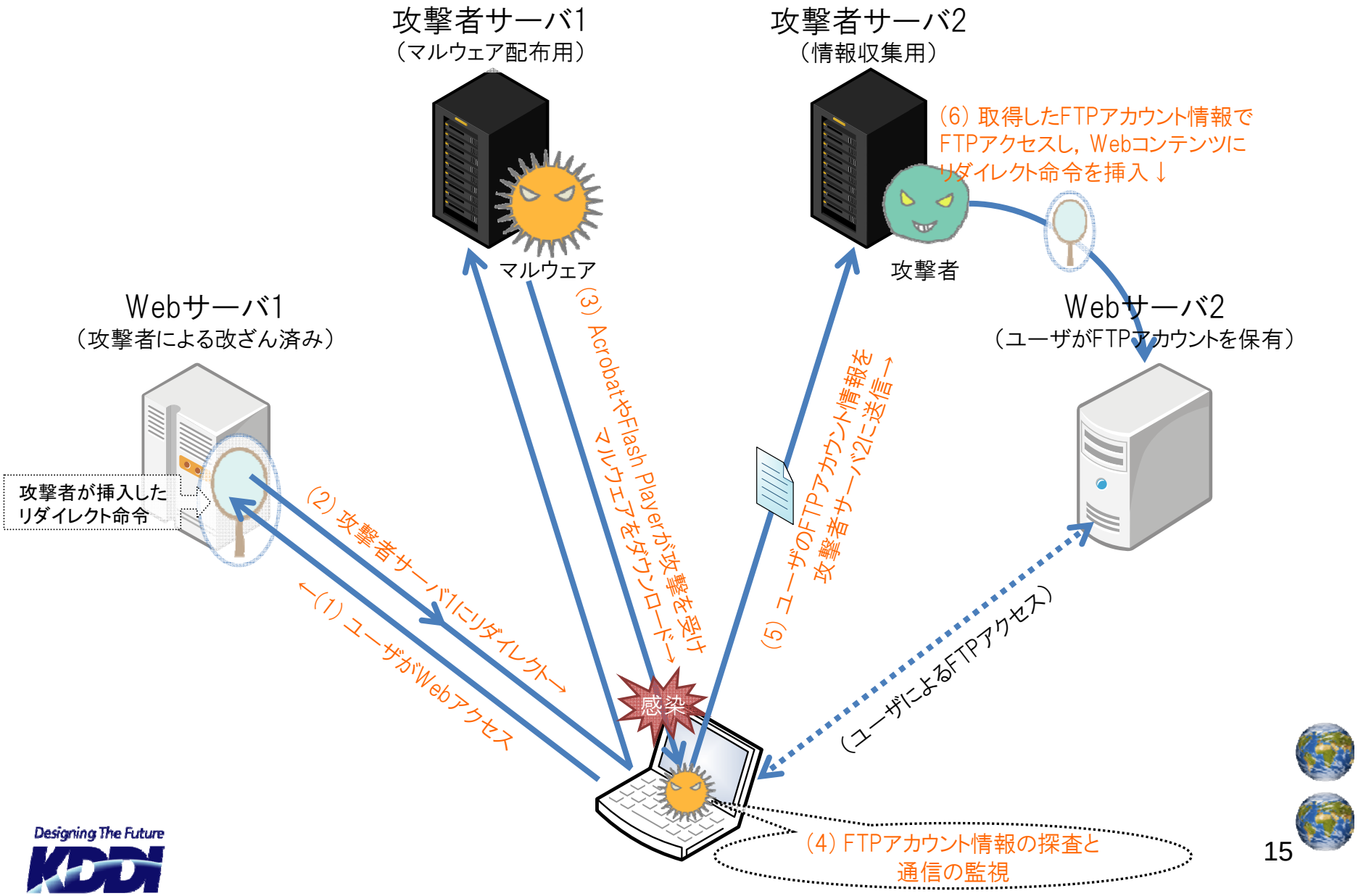
Conficker's P2P機能

- **SupernodeやPeer listに頼らないP2Pネットワークを構成**
  - Single Point of Failureを回避
  - P2P経由でペイロード（アップデータ、コマンド etc.）を共有
- **時刻同期**
  - 有名Webサイトに空のGET要求を送信
  - Webサイトからの返信に含まれるタイムスタンプで時刻を同期
- **P2Pプロトコル：Listenするポート番号**
  - IPアドレスからポート番号生成
  - IPアドレスとepoch week（2035～2348）からポート番号生成
  - 生成したポート番号をListen（TCP and UDP）
- **P2Pプロトコル：ランデブー**
  - ランダムに生成した（or 近傍の）IPアドレスに宛てTCP or UDPパケット送信
  - 宛先ポートは上記と同様に生成
  - P2P接続が成功するとペーロード（署名付き）をダウンロード

Webからの脅威：Gumbler（GENO/JSRedir-R）

- 2009年4月4日にWeb通販ショップ「GENO」が改竄を受けたことで存在が明るみに
- Web媒介型マルウェア
  （Drive-by-Download型）
- Acrobat Reader等の脆弱性を利用
- 感染ホストのFTPアカウントを盗用
- 多数のWebサイトが改竄の被害に
  - ✓ JR東日本、ホンダ、ローソン
    京王グループ、ハウス食品・・・等々

Gumblar攻撃の流れ



重要インフラ震撼 Stuxnet

- 2010年7月アンチウイルスベンダVirusBlokAdaにより発見
  - ✓ Windowsに対する4つの脆弱性を悪用
    - MS08-067（MicrosoftServer Service脆弱性）
    - MS10-061（プリンタスプーラ脆弱性）
    - MS10-046（LNK脆弱性）
    - MS10-073（カーネルモードドライバ脆弱性）

- StuxnetがインストールするルートキットはRealtekSemiconductor社、JMicronTechnology社の証明書によって署名

- SCADA（Supervisory Control And Data Acquisition）を攻撃
  - ✓ 独Siemens社製 SIMATIC WinCC or SIMATIC PCS 7の脆弱性
  - ✓ PLC（プログラマブルロジックコントローラ）に悪質なコードの書き込み

16

マルウェアとクラウド

- マルウェア40年の歴史

  発見の時代 → 実験的試行の時代 → 悪用の時代

  愉快犯、自己顕示目的 → 金銭目的

  小規模 → 大規模分散協調（クラウドに繋がる）

- マルウェアの歴史＝マルウェア対策の歴史

  対策側も大規模分散協調（技術/体制）が不可欠！

- マルウェア作成者、攻撃者、現在待機中

  クラウド環境における多くの脅威により、これまで以上に
  攻撃も容易か？（既存の多くの脅威は、そのままの形でクラウド環境においても脅威となりうる・・・

ITU-T Cloud Computing FG

Designing The Future
KDDI

会合概要

第1回会合

- 開催日：2010年6月14日～16日
- 開催場所：ITU-T　ジュネーブ

第2回会合

- 開催日：2010年9月2日～6日
- 開催場所：ITU-T　ジュネーブ

第3回会合

- 開催日：2010年11月30日～12月3日
- 開催場所：France Telecom Orange　Lannion

第4回会合

- 開催日：2011年1月8日～1月11日
- 開催場所：ZTE　Nanjing

Designing The Future
KDDI

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。

成果物（Deliverables）

Deliverable 1:

Introduction to the Cloud Ecosystem

Deliverable 2:

Functional Requirements and Reference Architecture

Deliverable 3:

Infrastructure & Network enabled Cloud

Deliverable 4:

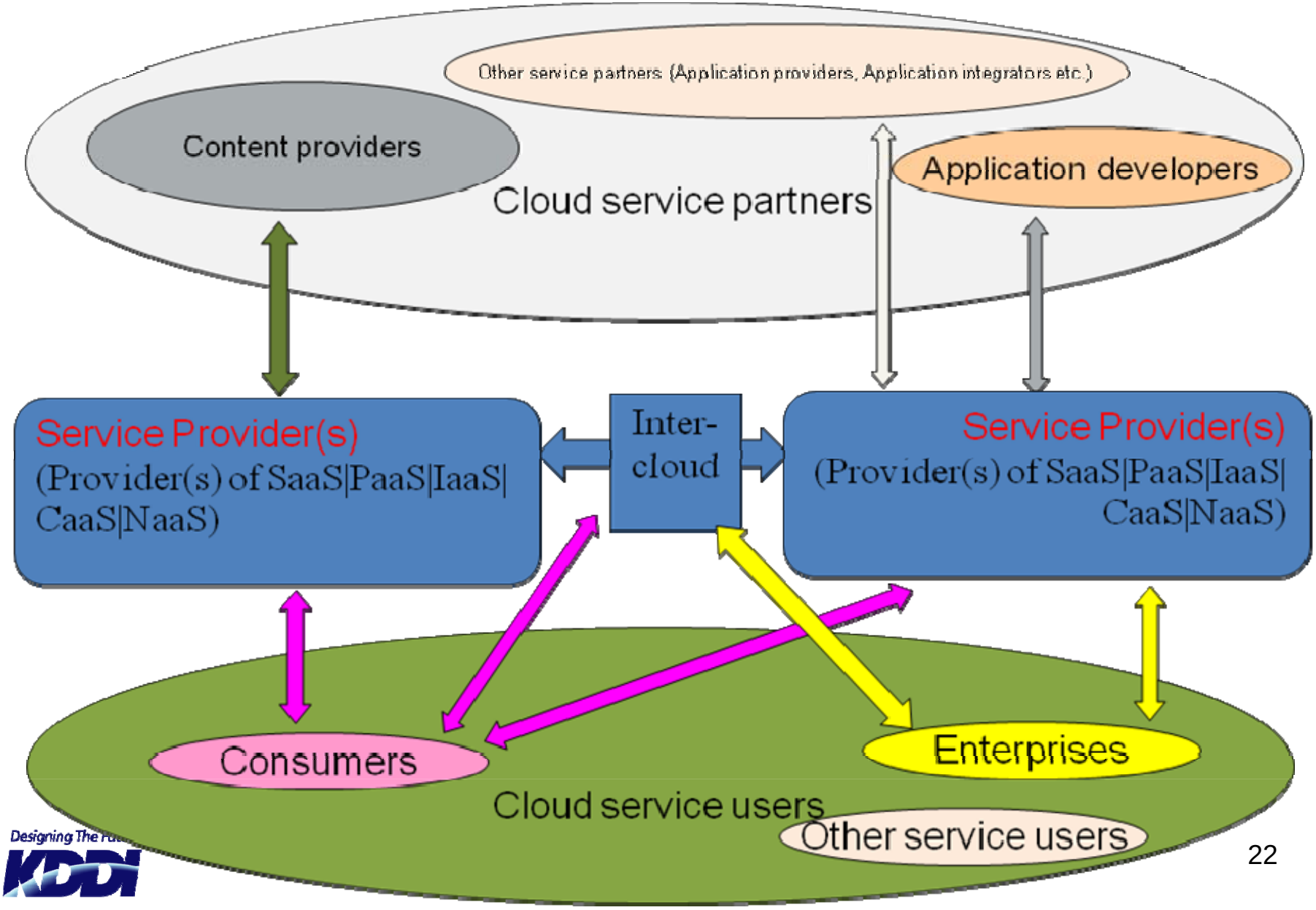
Overview of SDOs involved in Cloud Computing

Deliverable 5:

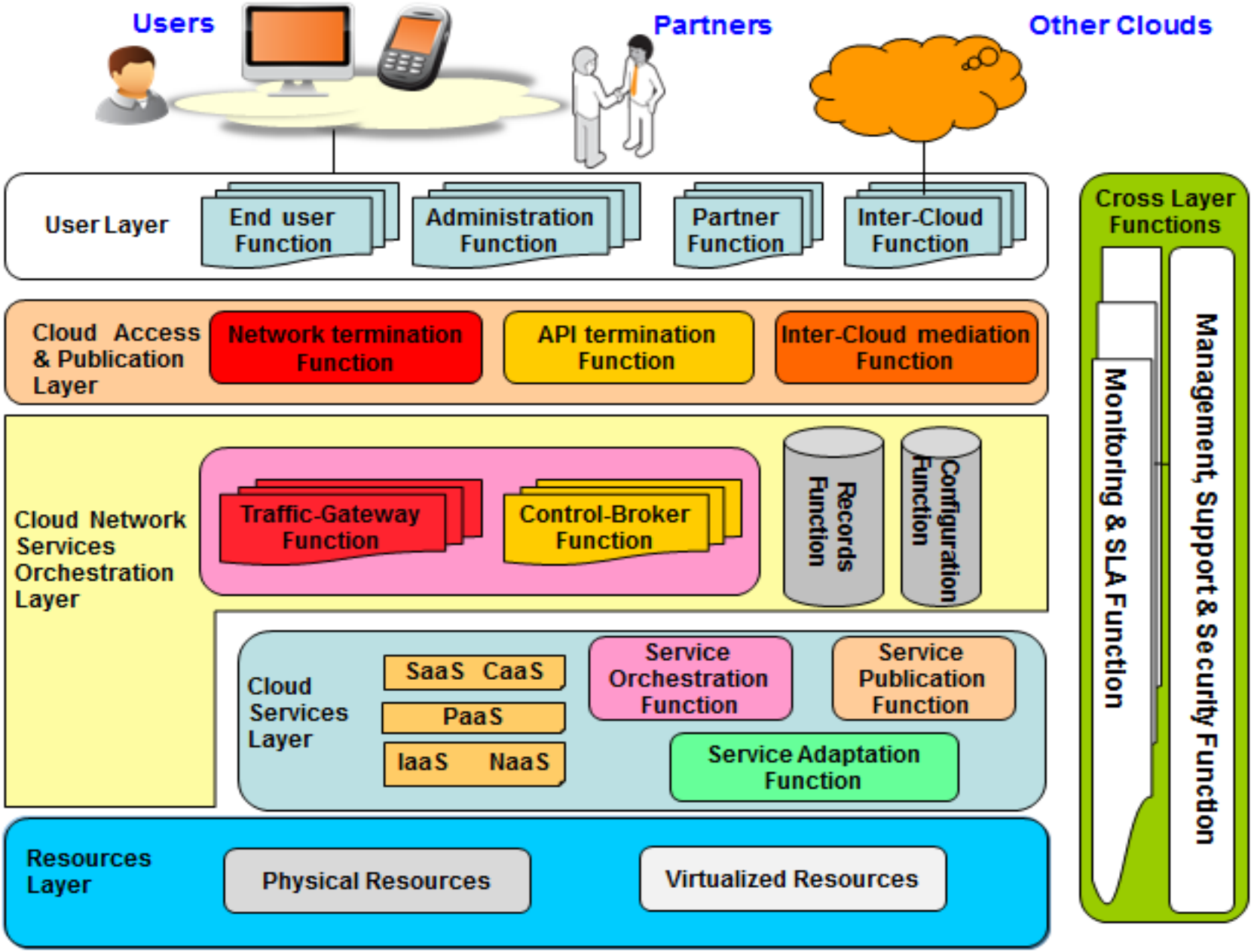
Cloud Computing Security

Designing The Future KDDI

クラウドエコシステムにおける役割（関係）



クラウド参照アーキテクチャ（多くの検討のベースに）（案）



第5の成果物:
Cloud　Security, threats & requirements

成果物の構成

1) 既存セキュリティ検討の活動のレビュー
（CSA, DTMF, GICTF，SG17リエゾンなど）

2) **Security Threats** の検討
（ユースケースの活用も視野）

3) **Security requirements** をクラウドサービス提供者、クラウド利用者、クラウド管理者の視点より検討，

4) **Subjects for security study** for ITU-T

既存のSecurity worksのレビュー

- **CSA**
- CSA/TCI (Cloud Security Alliance / Trusted Cloud Initiative)
- DMTF
- **GICTF**
- **NIST**
- Open Cloud Manifesto & Cloud Computing Use Cases Group
- CloudAudit
- OASIS
- OMG
- **ISO/IEC JTC1/SC27（検討課題の中で）**
- ITU-T SG17

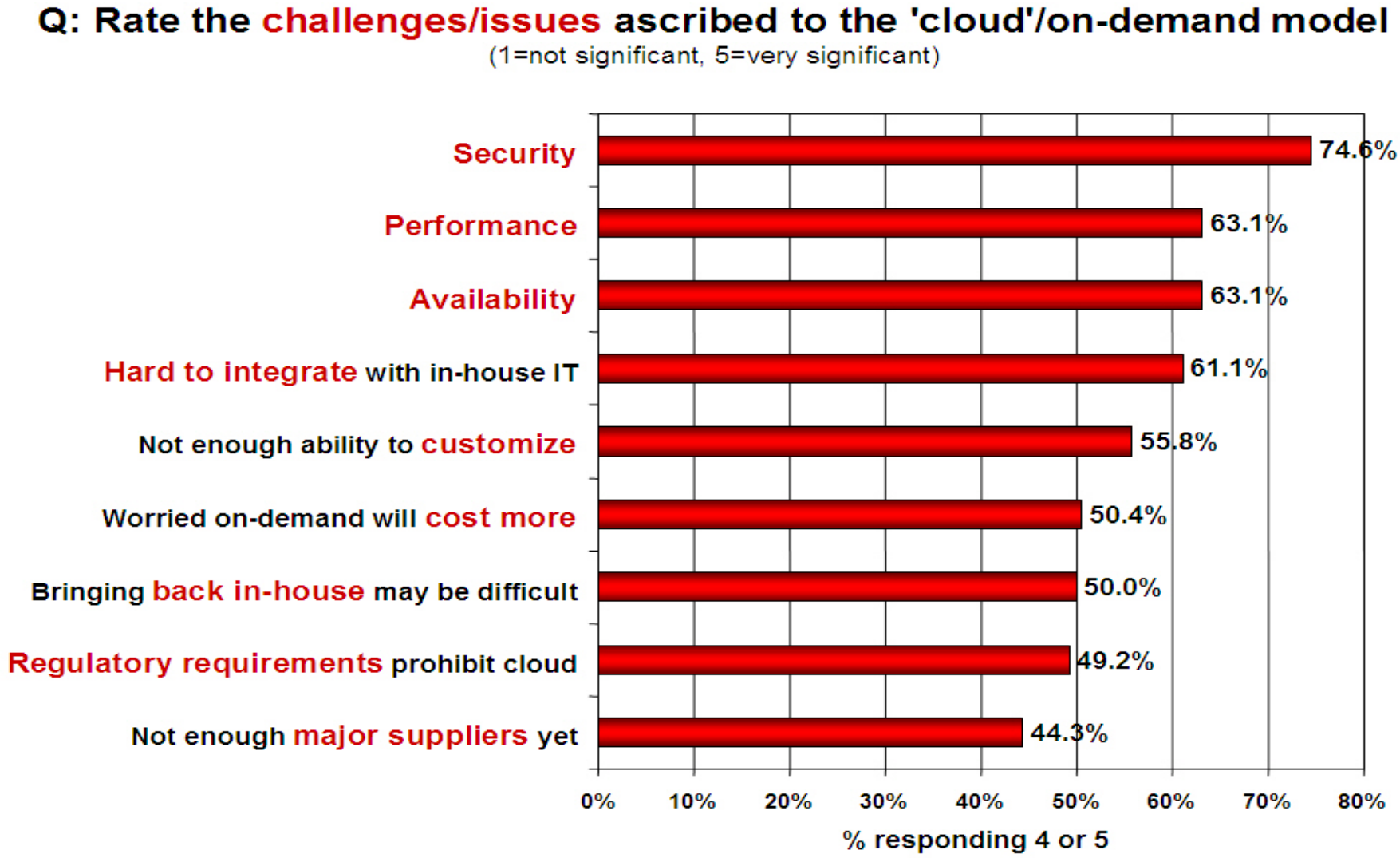
Designing The Future
KDDI

Cloud Security Alliance（CSA)

- Initiatives in Progress/Released
  - CSA Guidance V2.1 – Released Dec 2009
  - CSA Top Threats Research – Released March 2010
  - CSA Cloud Controls Matrix – Released April 2010
  - Trusted Cloud Initiative – Release Q4 2010
  - CSA Cloud Metrics Working Group
  - Consensus Assessment Initiative
- Initiatives Planned
  - CloudCERT
  - User Certification
  - Use Cases

Designing The Future
KDDI

（NIST） Security is the Major Issue



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”

Designing The Future KDDI

GICTF

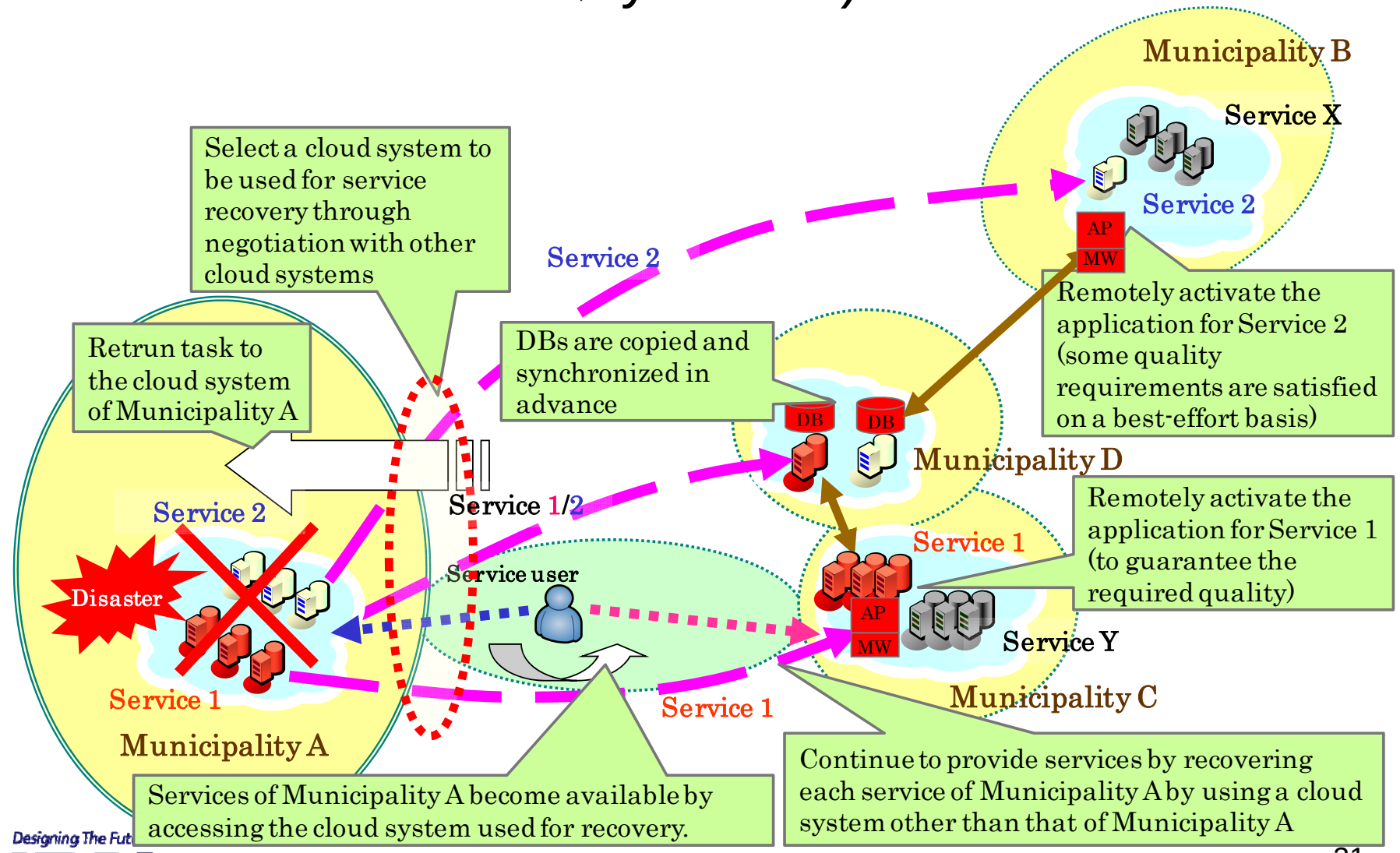
Introduction to Global Inter-Cloud Technology Forum (GICTF) and its Roadmaps

2010.6

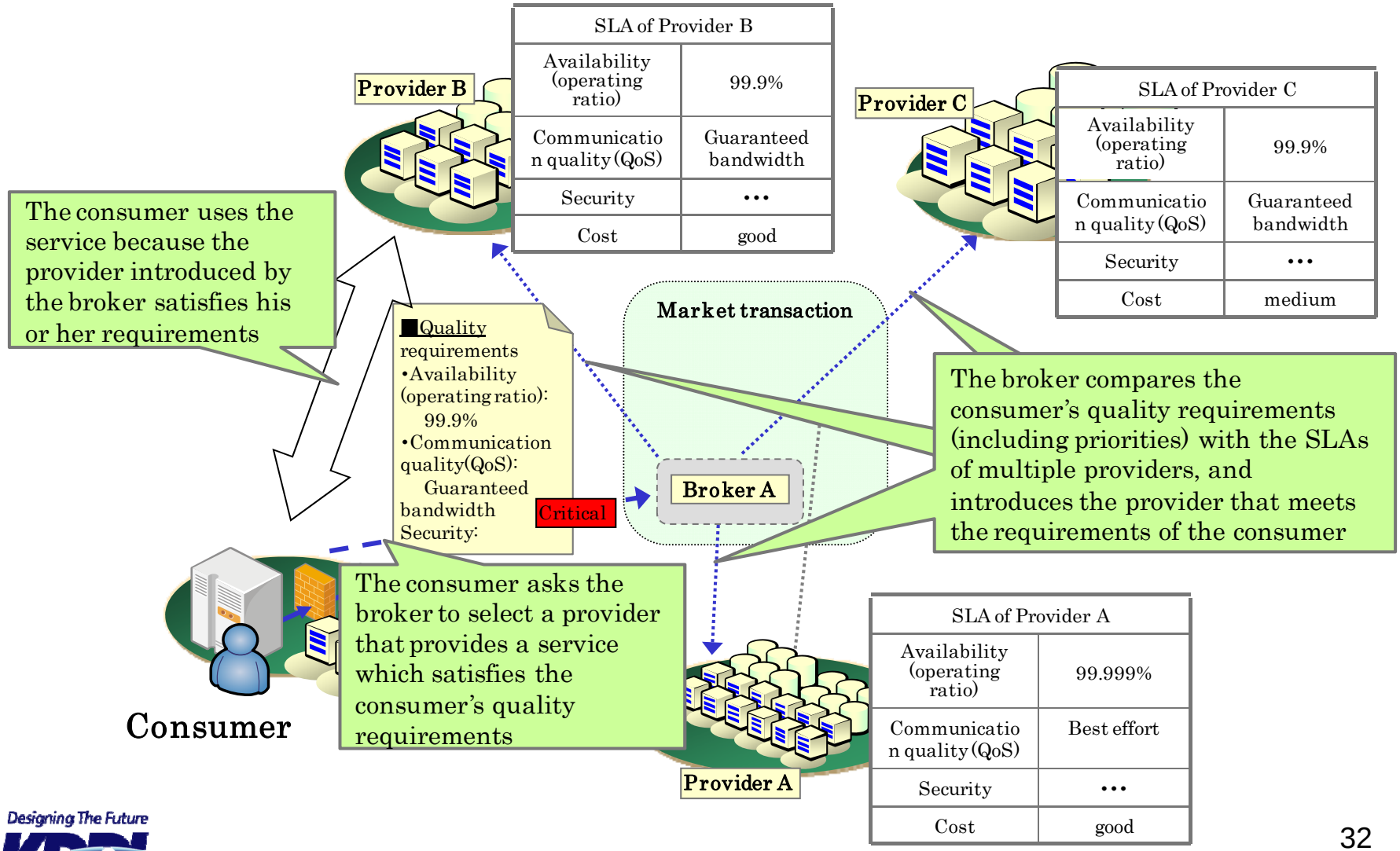
グローバルクラウド基盤連携技術フォーラム（GICTF）からの入力

Designing The Future
KDDI

災害や大規模障害における可用性保証のユースケース（by GICTF)



ブローカーを介するマーケットトランザクション（by GICTF）



Designing The Future KDDI

ITU-Tにおけるクラウドセキュリティの課題（現状案）

1)セキュリティ管理、監査に関わる技術
- 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

2) BCP（事業継続性）/災害復旧、ストレージセキュリティに関わる技術

3) セキュリティ/プライバシー確保

4) アカウント/ID管理

5) ネットワーク監視、インシデント対応に関する技術

6)* ネットワークセキュリティ

7)* インターオペラビリティ　セキュリティ

8)* 仮想化（バーチャライゼーション）セキュリティ

Designing The Future
KDDI

1)セキュリティ管理、監査に関わる技術

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

Designing The Future
KDDI

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

総務省情報

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

総務省情報

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）

Designing The Future KDDI

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る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。

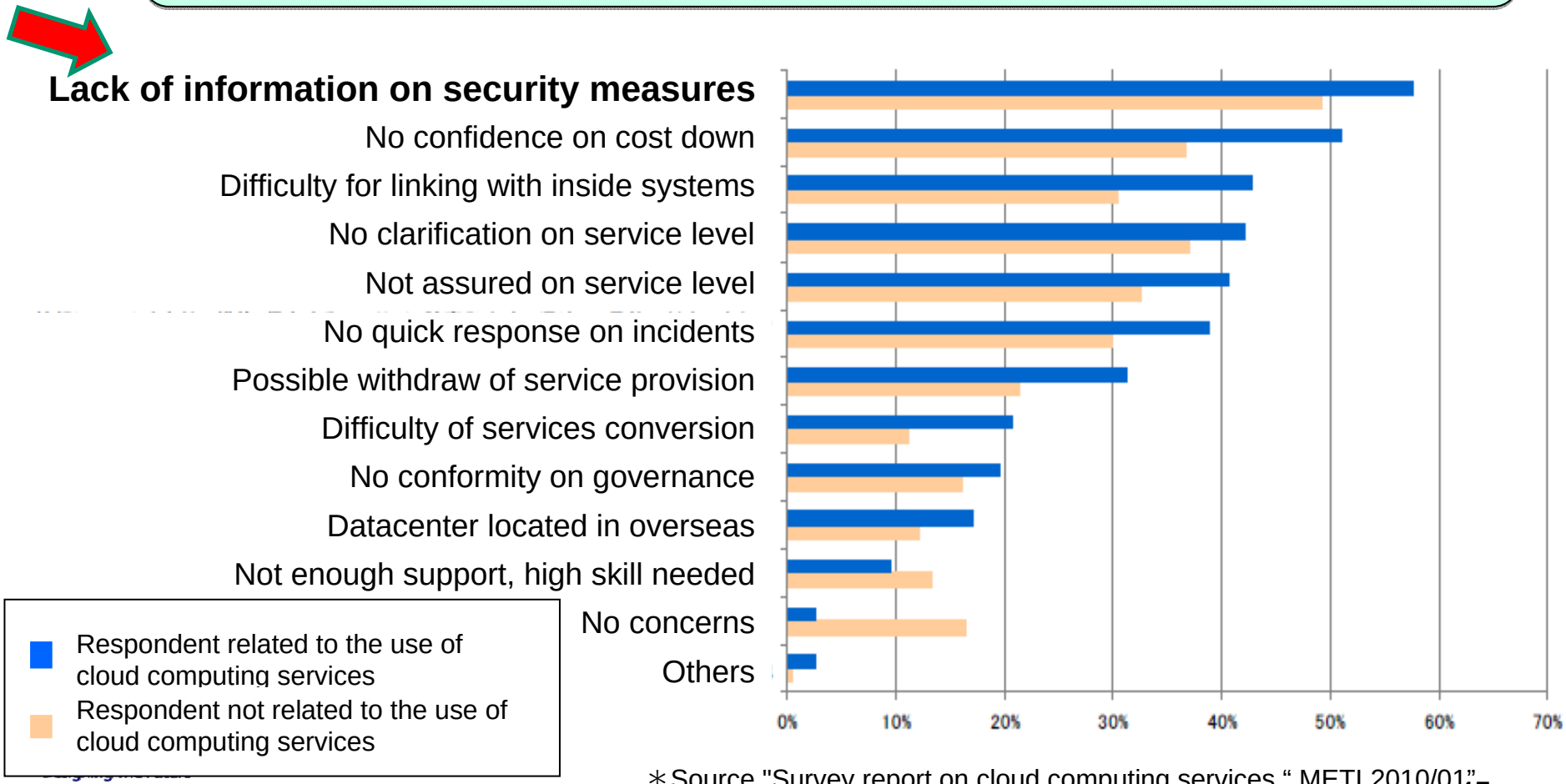
ISO/IEC JTC1/SC27における
クラウドセキュリティの検討
（経済産業省のアプローチ）

ーベルリン会合（10/4-8）以降ー

Designing The Future
KDDI

情報に対するセキュリティ対策の欠落（METI)

■The biggest concern on cloud services is “lack of information on security measures of service providers”.

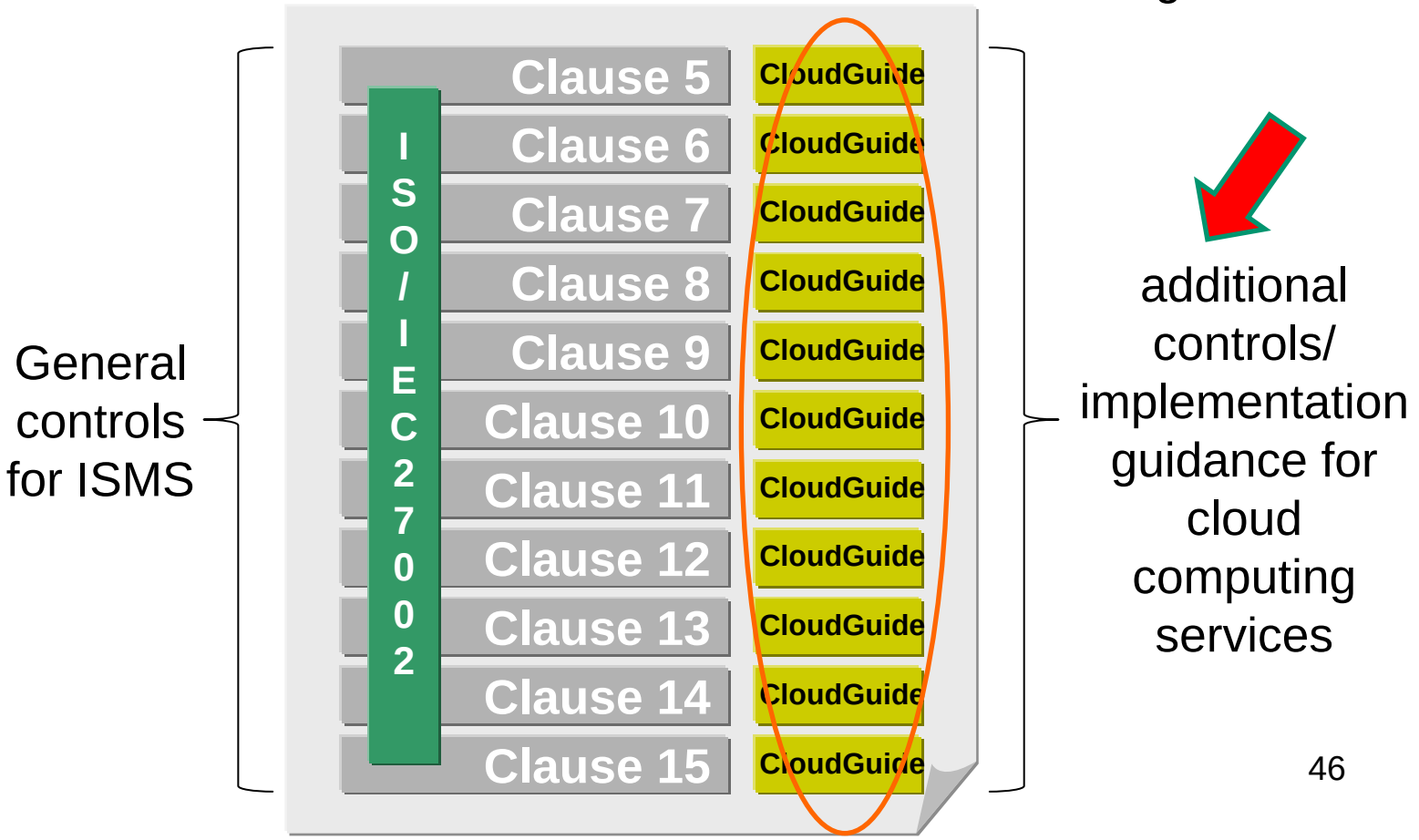


＊Source "Survey report on cloud computing services “ METI 2010/01”
Respondent number=500

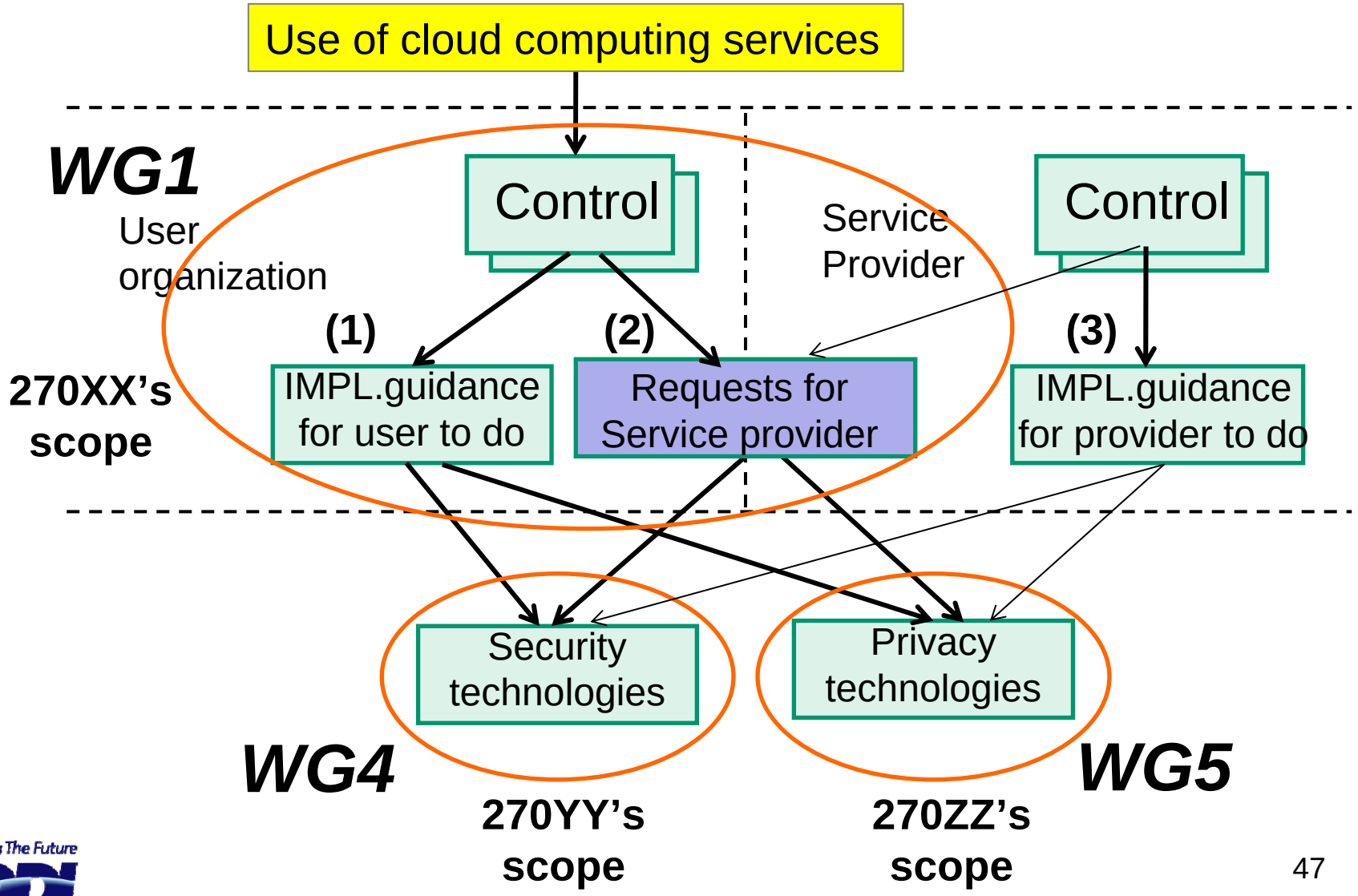
具体的なアプローチとしては

To make additional controls/implementation guidance in order to apply ISMS for common understanding for cloud computing services

ISMS is the mechanism for common understanding



ISO/SC27での基本構想
cloud computing security and privacy



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

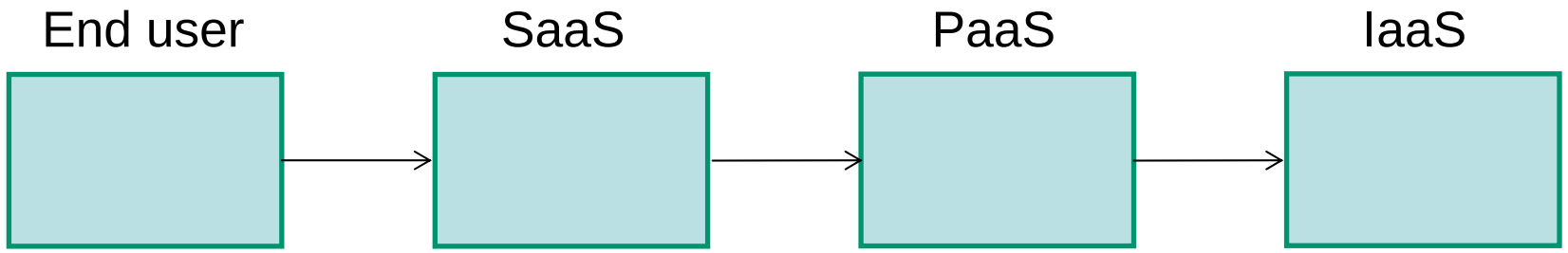
- クラウド利用者がクラウドサービスの利用においてクラウド事業者が行う事項について確認すべき事項を記述する。
- クラウド利用者がクラウドサービスの利用においてクラウド事業者に対して実施を求める事項を記述する。

Note.

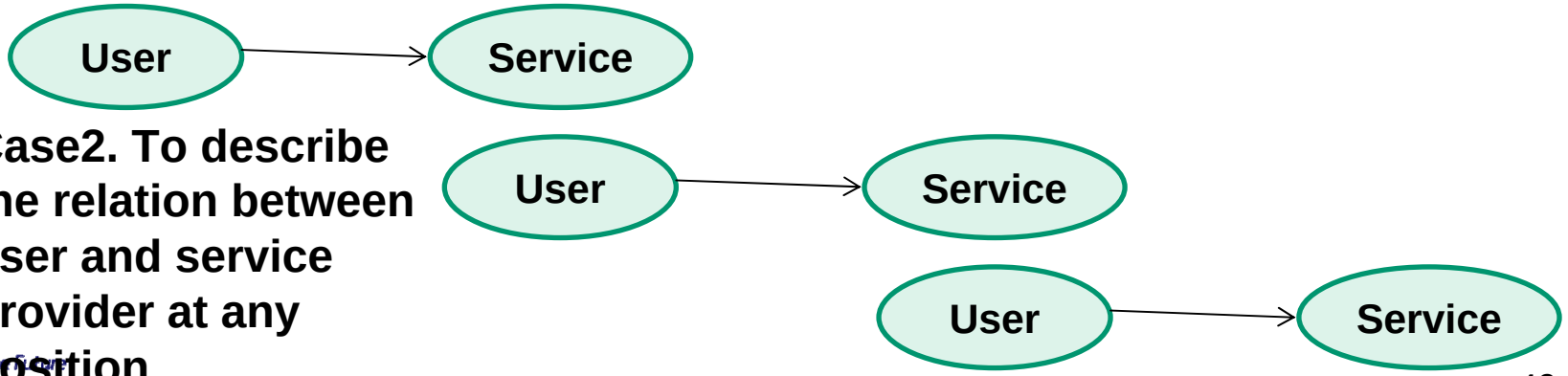
- クラウド事業者が自らの情報セキュリティ対策として行う事項であって、クラウド利用者の情報セキュリティ対策とすることを主たる目的としないものは、記述しない。
- クラウド利用者が要求してもクラウド事業者が対応しないと一般的に想定される事項は、記述しない。（例えば、物理的な管理策）
- ISO/IEC 27002の実施の手引に既にある記述に対してクラウドサービス利用における補足説明を加える場合には、当該補足説明は「クラウド利用者のための関連情報」に記述する。

クラウド利用者とSPとの関係
cloud computing security and privacy

■ Relation between user and service provider



Case1. To describe the measures including sub-services



Case2. To describe the relation between user and service provider at any position

4) アカウント/ID管理

- クラウド利用に関わるアカウントやサービスのハイジャックに対して、対策を検討する必要がある。本検討は、IdM技術などに基づく技術的な検討であり、以下の内容が包含される。

1＞Development of strong cloud-based authentication and authorization architecture and mechanisms (including strong two-factor authentication techniques)

2＞Detection method to proactively monitor unauthorized activities

3＞Study on strong network authentication

4＞Guideline how to securely use account credentials between users and providers

より具体的には

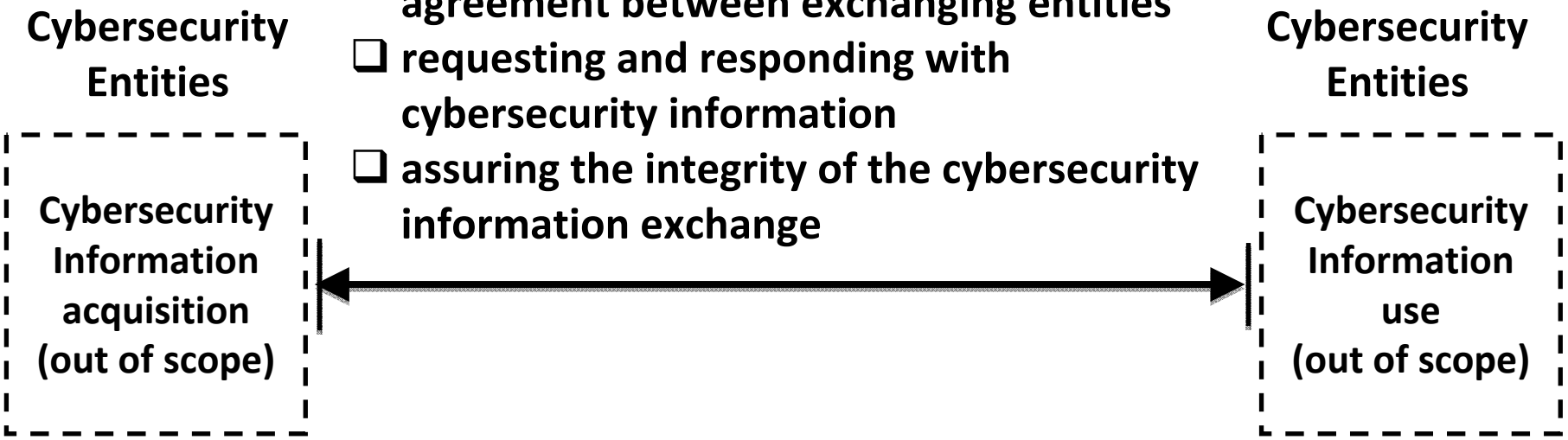
- 特に、IdMに関わる技術については、これまで多く議論がされている既存技術での対応が多く可能と考えられる。
- ただし、コンプライアンスの確保、リクマネジメント、利用者操作のログ管理、複数サービスに跨る場合の利用者Identityのライフサイクル管理など、多くの検討が必要となる。
- また、Inter-Cloud環境を想定した認証連携の確保についても重要な課題となる。

5) ネットワーク監視、インシデント対応に関する技術

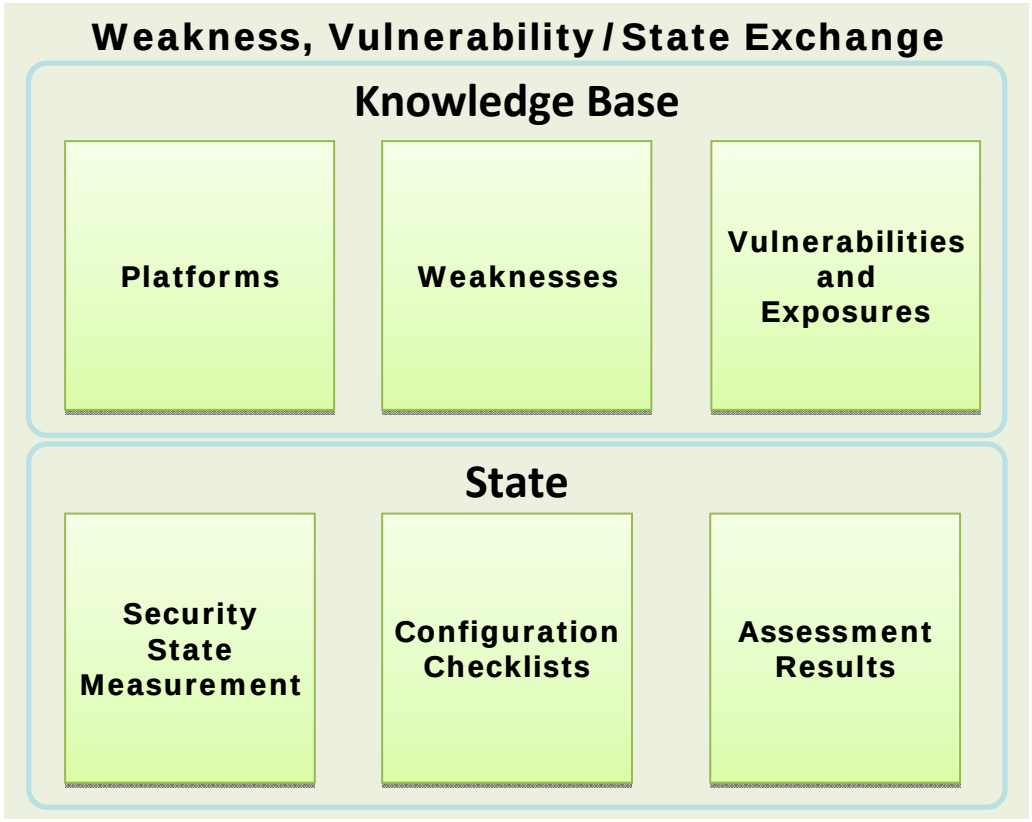
- 既存規格の活用
  ITU-T X.1056
  ISO/IEC 27036（現在FDISへ）
- ITU-T X.1500（CYBEX）の活用
- CSA:
  Telecommunication WGにてクラウドCERTなどの検討を開始

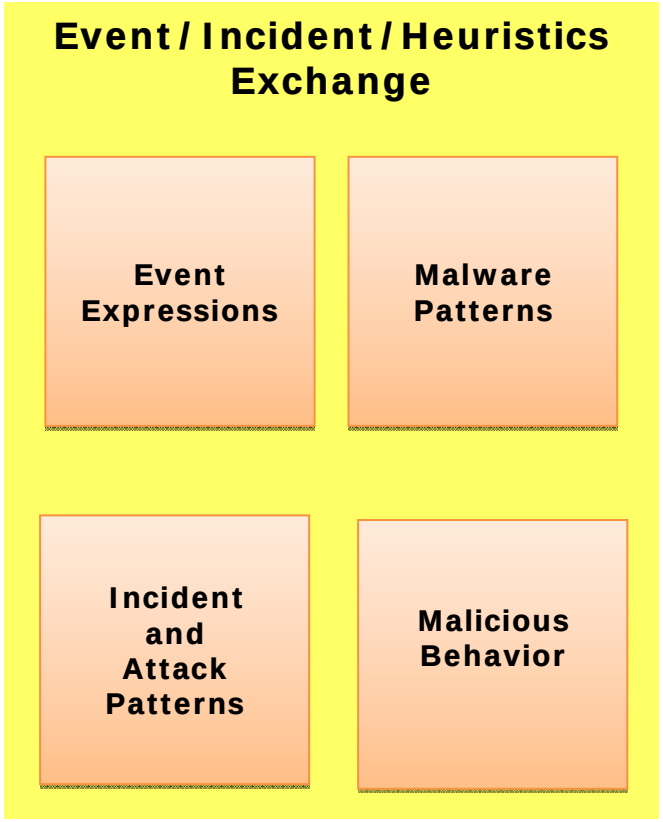
The CYBEX Model

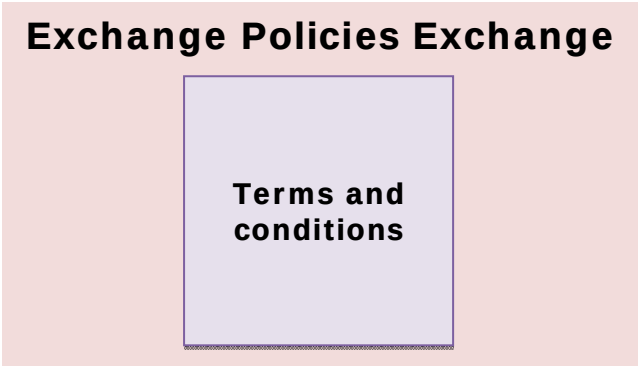
- structuring cybersecurity information for exchange purposes
- identifying and discovering cybersecurity information and entities
- establishment of trust and policy agreement between exchanging entities
- requesting and responding with cybersecurity information
- assuring the integrity of the cybersecurity information exchange



CYBEX Technique Clusters: Structured Information

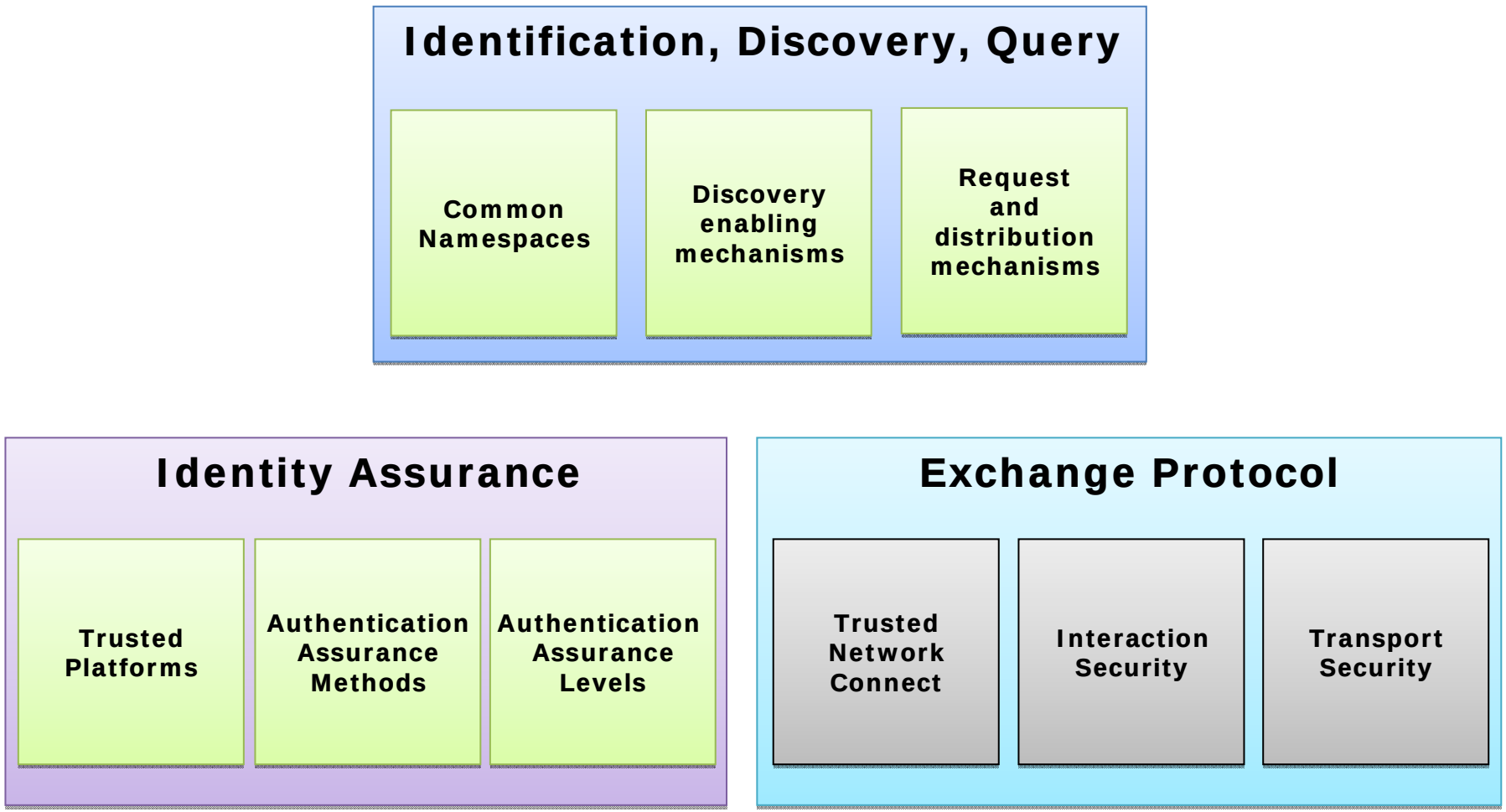






Designing The Future
KDDI

CYBEX Technique Clusters: Utilities



Designing The Future KDDI

8)* 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

8)* 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）

Designing The Future KDDI

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

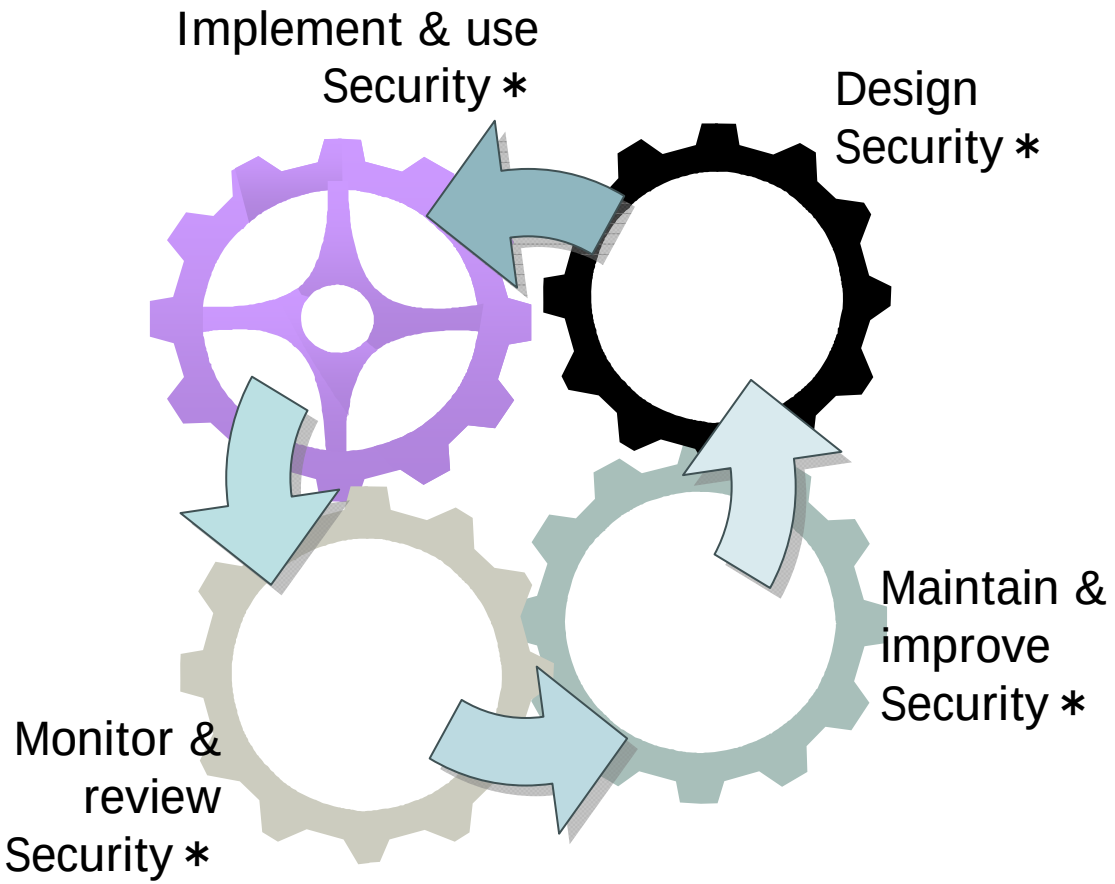
JNSAの視点からのクラウドセキュリティ

- 多くの外部活動（ITU-T FG, CSA, ENISA等） の活動のレビュー継続（可能な連携）。
- クラウドユーザより、クラウドSP視点の技術的セキュリティ機能のガイドライン化
  - BCP（事業継続性）/災害復旧、ストレージセキュリティに関わる技術
  - プライバシー確保
  - アカウント/ID管理
  - ネットワーク監視、インシデント対応に関する技術
  - ネットワークセキュリティ
  - 仮想化（バーチャライゼーション）セキュリティ
  - クラウド評価環境の構築

  等
- クラウドセキュリティガイドラインのユーザ
  - ＊クラウドSP（JNSAメンバ含む）
  - ＊プライベートクラウド構築者
  - ＊パブリッククラウド利用者
- 可能な部分をISO/SC27、ITU-T/SG17に標準化提案（ISFと連携して）

Designing The Future
KDDI

Thank you for listening Q&A



Designing The Future
KDDI