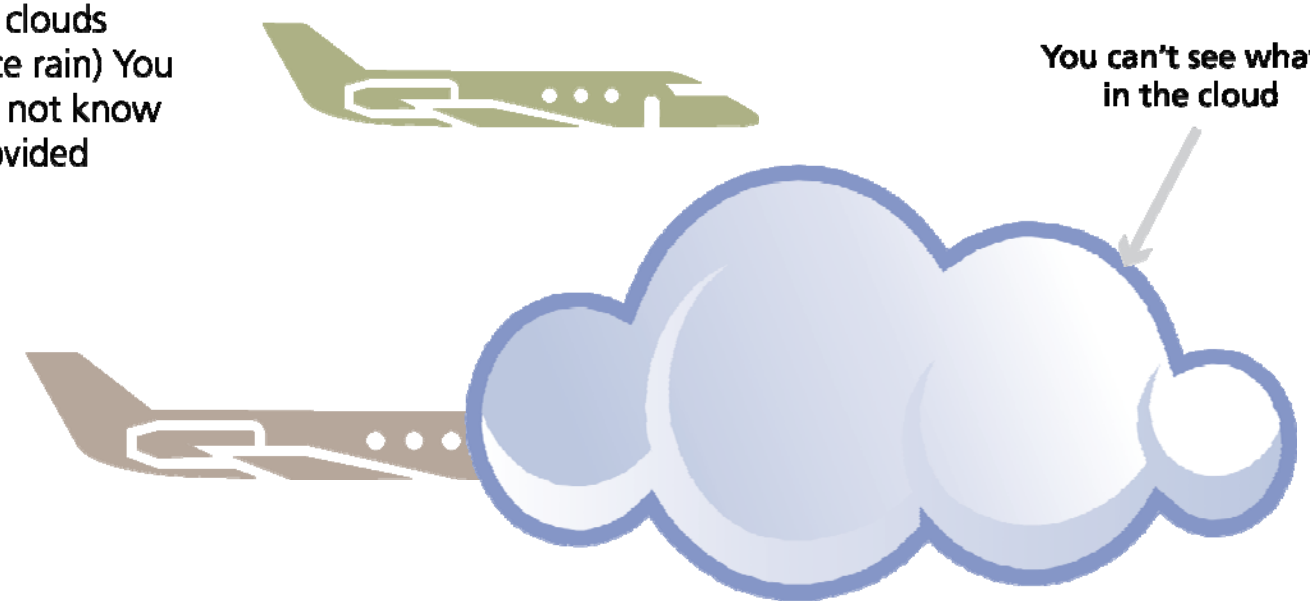
クラウドコンピューティング時代の高セキュリティ技術の動向とJNSAの関わり方

標準化部会長： 中尾 康二
（KDDI株式会社）

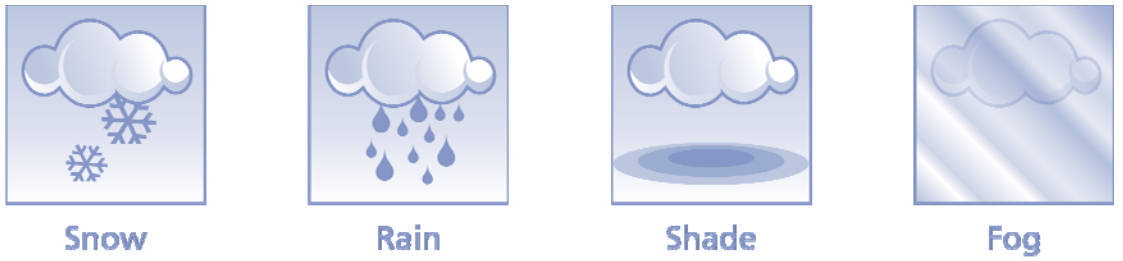
クラウドの特徴

Service providers operate in clouds (eg cloud seeding to produce rain) You receive the service, but may not know how (or from where) it's provided



Clouds are not for everyone – some people need more transparency (eg pilots)

The cloud provides services:



サービスの処理が見えない
1）データ保管場所は？
2）データの隔離は？
3）データの復旧は？

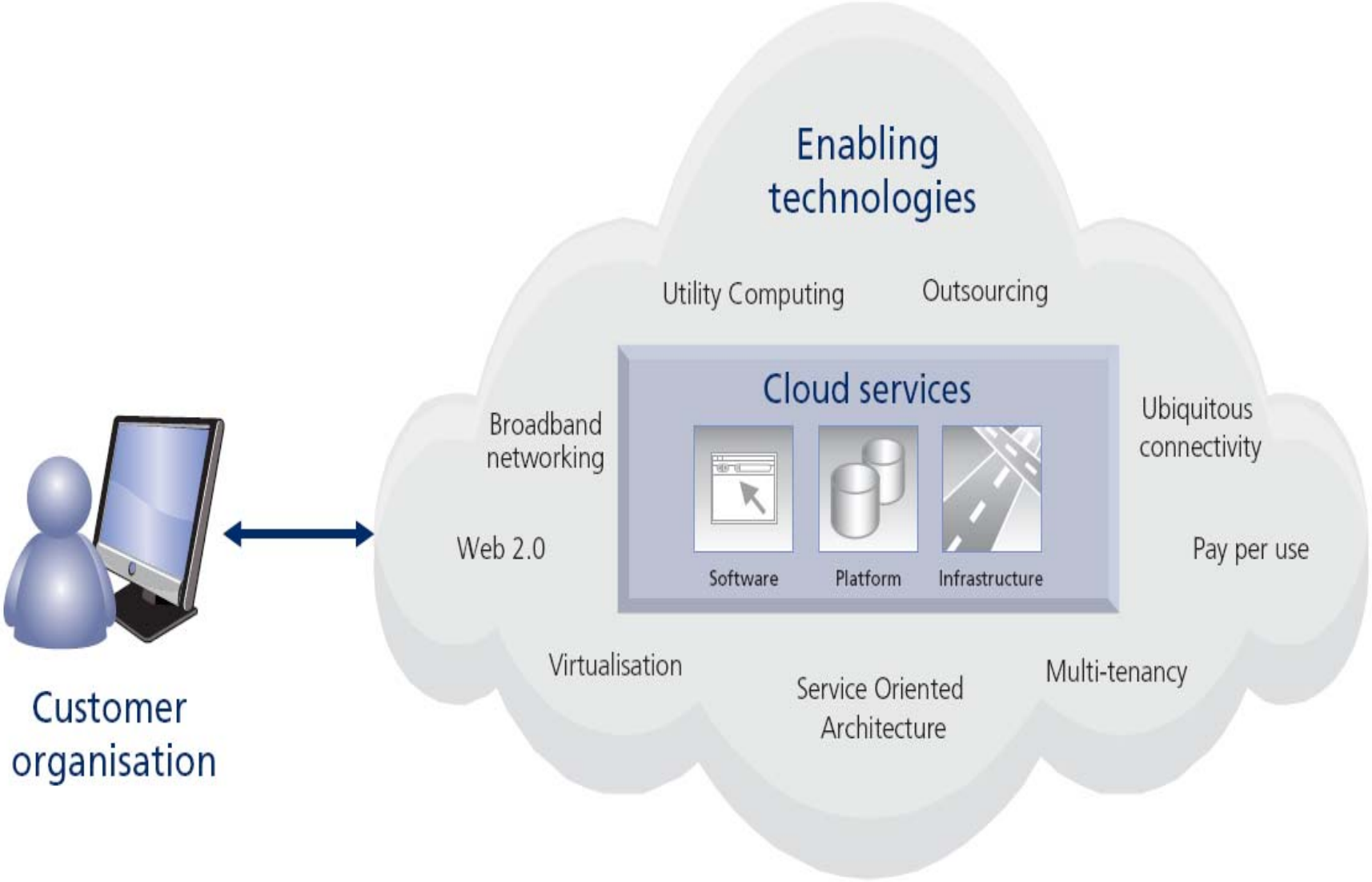
ISF－JNSAワークショップ（2010年1月）より

クラウドはどのように使える？

- **Infrastructure as a Service (IaaS)**
  - Services that deliver fundamental computing infrastructure: CPU cycles, storage (Storage as a Service) etc
- **Platform as a Service (PaaS)**
  - Services that deliver a suite of solutions to allow online development and hosting of applications
- **Software as a Service (SaaS)**
  - Applications that are provided and hosted in the cloud, often built on PaaS and IaaS infrastructures

ISF－JNSAワークショップ（2010年1月）より

クラウドコンピューティングのイメージ



ISF－JNSAワークショップ（2010年1月）より

Security guidelines for cloud computing

ISF/JNSAワークショップ

Today's workshop

- Security guidelines for cloud computing
  - Current work on cloud
  - Scope
  - Breakout
  - Next steps

OBJECTIVES

ISF suggested future work with JNSA

- **ISO Liaison**
  - Both the ISF and JNSA have representatives on the SC27 committee, which oversees the production of information security standards such as ISO 27001, 27004 and 27014. Collaboration between the ISF and JNSA should be explored and, where possible, either joint submissions or support for submissions should occur. It was agreed that the audit standard for the Cloud could be a suitable topic for future ISF / JNSA support.

- Discussions on ISF / JNSA collaboration should occur at the ISO SC27 meetings.

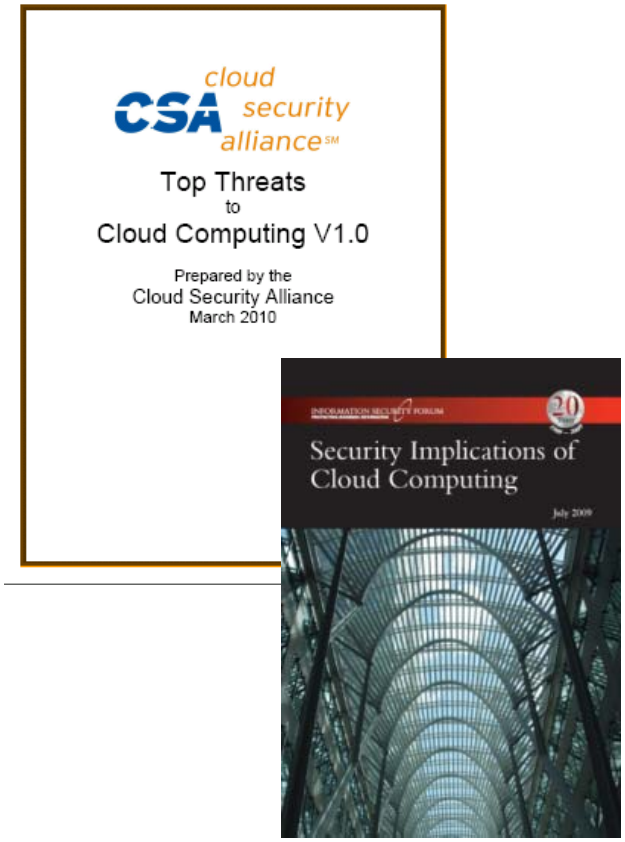
Objectives

- Consider the input for ISO/IEC SC27
  - Examine the content for guidelines
  - Threats
  - Controls
- Discuss the issues for ITU-T CC FG
  - How do we work with the ITU?
  - What do we submit?
- Develop strategy how to propose our idea for International standards bodies in near future (Berlin: ISO/SC27, ITU-T FG)

CURRENT WORK

Current work

- Cover the work of three organisations:
- CSA
- ISF
- JASA



ISF

(2010年1月ISF/JNSAワークショップより)

クラウドにおけるセキュリティのポイント（1）

利用者の視点

- 戦略的な方向性（利用の適用性判断、ビジネス要件との合致など）
- サービスの選択（コストとサービスレベルのバランスなど）
- クラウドへのアクセス（セキュア認証、アクセス制御など）
- ビジネス情報の制御
  （ビジネス情報へのアクセス権の欠如、ビジネス情報の場所が不明など）
- 利用者としての実践
  （データ保管のローカル化、個人デバイスの利用、クラウドからの情報コピーなど）

法的な視点

- 契約の定義
- 監査、及び法的順守
- 終了時の問題（資産の返却など。。。）

クラウドにおけるセキュリティのポイント（2）

悪意のある攻撃の視点

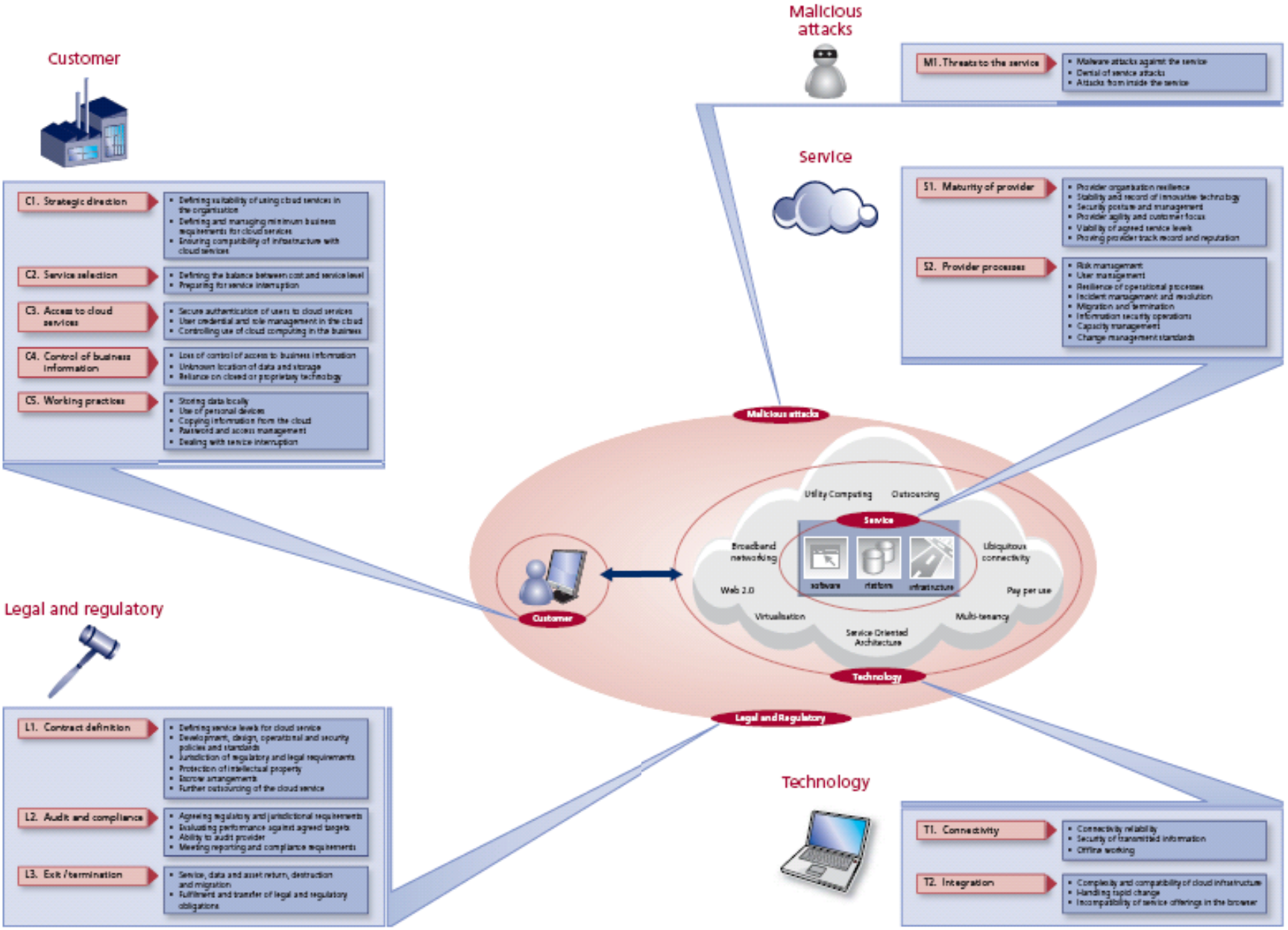
- サービスへの脅威
  - サービスに対するマルウェア攻撃
  - DOS
  - サービスの内部からの攻撃

サービス提供者の視点

- 提供者の習熟度（回復力のある提供組織、技術の安定性及び記録化、セキュリティに対する姿勢・管理、SLA、提供者の評価の検証など）
- 提供者における機能（リスク管理、利用者管理、回復力のある運用機能、インシデント管理と対応、リスクの低減化、情報セキュリティ運用（ISMS的な）など）

技術の視点

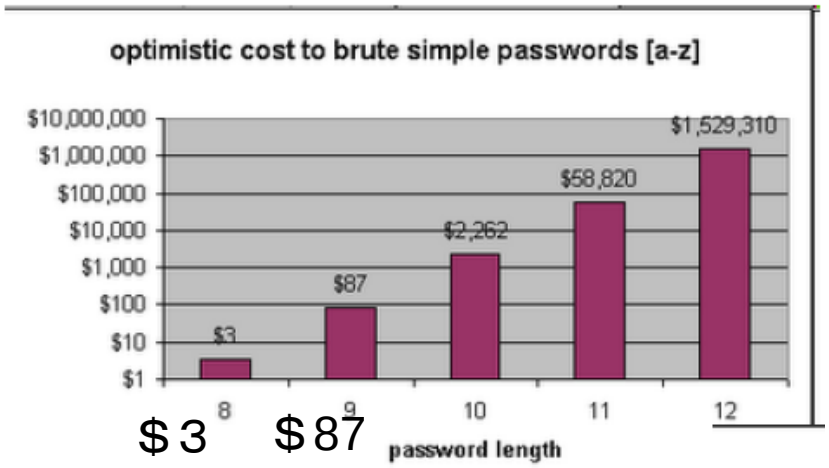
- 接続性（信頼性の確保、交換される情報のセキュリティなど）
- 統合化（クラウドインフラの複雑性・互換性、迅速な変更管理など）


Malicious attacks
M1. Threats to the service
Malware attacks against the service
Denial of service attacks
Attacks from inside the service
Customer
C1. Strategic direction
Defining suitability of using cloud services in the organisation
Defining and managing minimum business requirements for cloud services
Ensuring compatibility of infrastructure with cloud services
C2. Service selection
Defining the balance between cost and service level
Preparing for service interruption
C3. Access to cloud services
Secure authentication of users to cloud services
User credential and role management in the cloud
Controlling use of cloud computing in the business
C4. Control of business information
Loss of control of access to business information
Unknown location of data and storage
Reliance on closed or proprietary technology
C5. Working practices
Storing data locally
Use of personal devices
Copying information from the cloud
Password and access management
Dealing with service interruption
Service
S1. Maturity of provider
Provider organisation resilience
Stability and record of innovative technology
Security posture and management
Provider agility and customer focus
Viability of agreed service levels
Proving provider track record and reputation
S2. Provider processes
Risk management
User management
Resilience of operational processes
Incident management and resolution
Migration and termination
Information security operations
Capacity management
Change management standards
Malicious attacks
Utility Computing
Outsourcing
Service
Broadband networking
Ubiquitous connectivity
software
platform
infrastructure
Web 2.0
Pay per use
Virtualisation
Multi-tenancy
Service Oriented Architecture
Technology
Customer
Legal and Regulatory
Legal and regulatory
L1. Contract definition
Defining service levels for cloud service
Development, design, operational and security policies and standards
Jurisdiction of regulatory and legal requirements
Protection of intellectual property
Escrow arrangements
Further outsourcing of the cloud service
L2. Audit and compliance
Agreeing regulatory and jurisdictional requirements
Evaluating performance against agreed targets
Ability to audit provider
Meeting reporting and compliance requirements
L3. Exit /termination
Service, data and asset return, destruction and migration
Fulfilment and transfer of legal and regulatory obligations
Technology
T1. Connectivity
Connectivity reliability
Security of transmitted information
Offline working
T2. Integration
Complexity and compatibility of cloud infrastructure
Handling rapid change
Incompatibility of service offerings in the browser

補足

- マルウェアの脅威の継続
  → スキャンのビデオ

- クラウドを用いたクラック例
  ーパスワードクラック
  （アマゾン利用の場合）
  ー暗号鍵探索　等



LAC新井氏　資料より

CSA

(2010年6月ISF/JNSAワークショップより)

Cloud Security Alliance

- 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

クラウドセキュリティの課題

アーキテクチャ領域

クラウドの統制・管理領域

- 統制とリスク管理（プロバイダーの管理体制など）
- 法務・契約事項（法環境の差など）
- コンプライアンスと監査（評価、監査など）
- 情報のライフサイクル管理
- 移植性と相互運用性

クラウドの運用（活用）領域

- データセンターセキュリティ、事業継続、災害復旧
- データセンター運用（データ/プロセスの分離など）
- インシデント対応、通知、回復
- アプリケーションセキュリティ
- 暗号化、及び鍵管理
- アイデンティティ・アクセス管理
- 仮想化（仮想化環境単位のセキュリティ装備など）

CSA：Security Guidance for Critical Area of Focus in Cloud Computing V2.1
より引用

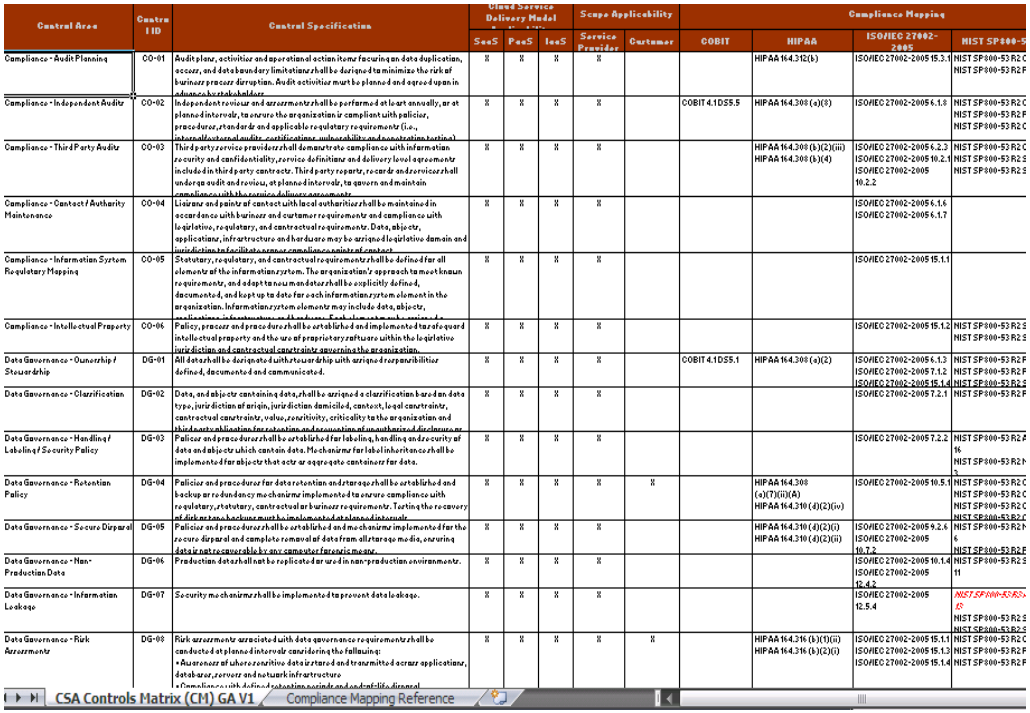
クラウドにおける脅威

脅威１：クラウドの誤用、悪用、及び不正利用
脅威２：インターフェース、APIの安全性欠如
脅威３：悪意のある内部犯行
脅威４：シェア技術に関する事項
脅威５：データの紛失、漏洩
脅威６：アカウント、またはサービスの乗っ取り
脅威７：不明なリスクプロファイル

CSA：Top Threats to Cloud Computing V1.0より引用

CSA: Controls matrix

- Divided into 13 domains
- Contains 97 controls
- Cross-referenced to CObIT, HIPAA, ISO, NIST…



Control Area	Control ID	Control Specification	Cloud Service Delivery Model			Scope Applicability		Compliance Mapping			
			SaaS	PaaS	IaaS	Service Provider	Customer	COBIT	HIPAA	ISO/IEC 27002-2005	NIST SP800-53
Compliance - Audit Planning	CO-01	Audit plans, activities and operational actions to ensure data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruptions. Audit activities must be planned and agreed upon in advance by stakeholders	X	X	X	X			HIPAA §164.312(b)	ISO/IEC 27002-2005 15.3.1	NIST SP800-53 R2 C NIST SP800-53 R2 P
Compliance - Independent Audits	CO-02	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing)	X	X	X	X		COBIT 4.1 DS5.5	HIPAA §164.308 (a)(8)	ISO/IEC 27002-2005 6.1.8	NIST SP800-53 R2 C NIST SP800-53 R2 P NIST SP800-53 R2 C
Compliance - Third Party Audits	CO-03	Third party service providers shall demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in third party contracts. Third party reports, records and services shall undergo audit and review, at planned intervals, to govern and maintain compliance with the service delivery agreements	X	X	X	X			HIPAA §164.308 (b)(2)(iii) HIPAA §164.308 (b)(4)	ISO/IEC 27002-2005 6.2.3 ISO/IEC 27002-2005 10.2.1 ISO/IEC 27002-2005 10.2.2	NIST SP800-53 R2 C NIST SP800-53 R2 S NIST SP800-53 R2 S
Compliance - Contact / Authority Maintenance	CO-04	Liaisons and points of contact with local authorities shall be maintained in accordance with business and customer requirements and compliance with legislative, regulatory, and contractual requirements. Data, objects, applications, infrastructure and hardware may be assigned legislative domain and jurisdiction to facilitate proper compliance point of contact	X	X	X	X				ISO/IEC 27002-2005 6.1.6 ISO/IEC 27002-2005 6.1.7	
Compliance - Information System Regulatory Mapping	CO-05	Statutory, regulatory, and contractual requirements shall be defined for all elements of the information system. The organization's approach to meet known requirements, and adopt new mandates shall be explicitly defined, documented, and kept up to date for each information system element in the organization. Information system elements may include data, objects, applications, infrastructure, and services. Each element may require de	X	X	X	X				ISO/IEC 27002-2005 15.1.1	
Compliance - Intellectual Property	CO-06	Policy, process and procedures shall be established and implemented to safeguard intellectual property and the use of proprietary software within the legislative jurisdiction and contractual constraints governing the organization.	X	X	X	X				ISO/IEC 27002-2005 15.1.2	NIST SP800-53 R2 S NIST SP800-53 R2 S
Data Governance - Ownership / Stewardship	DG-01	All data shall be designated with stewardship with assigned responsibilities defined, documented and communicated.	X	X	X	X		COBIT 4.1 DS5.1	HIPAA §164.308 (a)(2)	ISO/IEC 27002-2005 6.1.3 ISO/IEC 27002-2005 7.1.2 ISO/IEC 27002-2005 15.1.4	NIST SP800-53 R2 P NIST SP800-53 R2 P NIST SP800-53 R2 S
Data Governance - Classification	DG-02	Data, and objects containing data, shall be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organization and third party obligations for retention and prevention of unauthorized disclosure or	X	X	X	X				ISO/IEC 27002-2005 7.2.1	NIST SP800-53 R2 P
Data Governance - Handling / Labeling / Security Policy	DG-03	Policies and procedures shall be established for labeling, handling and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	X	X	X	X				ISO/IEC 27002-2005 7.2.2	NIST SP800-53 R2 P 16 NIST SP800-53 R2 P 3
Data Governance - Retention Policy	DG-04	Policies and procedures for data retention and storage shall be established and backup or redundancy mechanisms implemented to ensure compliance with regulatory, statutory, contractual or business requirements. Testing the recovery of disk arrays backup must be implemented at least on an annual	X	X	X	X	X		HIPAA §164.308 (a)(7)(ii)(A) HIPAA §164.310 (d)(2)(iv)	ISO/IEC 27002-2005 10.5.1	NIST SP800-53 R2 C NIST SP800-53 R2 C NIST SP800-53 R2 C NIST SP800-53 R2 C
Data Governance - Secure Disposal	DG-05	Policies and procedures shall be established and mechanisms implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	X	X	X	X			HIPAA §164.310 (d)(2)(i) HIPAA §164.310 (d)(2)(ii)	ISO/IEC 27002-2005 9.2.6 ISO/IEC 27002-2005 10.7.2	NIST SP800-53 R2 M 6 NIST SP800-53 R2 P
Data Governance - Non-Production Data	DG-06	Production data shall not be replicated or used in non-production environments.	X	X	X	X				ISO/IEC 27002-2005 10.1.4 ISO/IEC 27002-2005 12.4.2	NIST SP800-53 R2 S 11
Data Governance - Information Leakage	DG-07	Security mechanisms shall be implemented to prevent data leakage.	X	X	X	X				ISO/IEC 27002-2005 12.5.4	NIST SP800-53 R2 S AR NIST SP800-53 R2 S
Data Governance - Risk Assessments	DG-08	Risk assessments associated with data governance requirements shall be conducted at planned intervals considering the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers and network infrastructure • Compliance with defined retention periods and end-of-life disposal	X	X	X	X	X		HIPAA §164.316 (b)(1)(ii) HIPAA §164.316 (b)(2)(i)	ISO/IEC 27002-2005 15.1.1 ISO/IEC 27002-2005 15.1.3 ISO/IEC 27002-2005 15.1.4	NIST SP800-53 R2 C NIST SP800-53 R2 P NIST SP800-53 R2 P

CSA Controls Matrix (CM) GA V1 | Compliance Mapping Reference

CSA活動の要約

- クラウドコンピューティングはリアルなもので、変化するものである。
- 人、プロセス、技術、組織、国家のためのチャレンジ。
- 広い統制的なアプローチが必要。
- 戦術的に方向性を固めることが必要。
- 既存のベストプラクティスとまったく新たなベストプラクティスの組み合わせである。
- 将来のクラウドにおいて、CSAは大きくて重要な影響を与える。

DEFINING THE GUIDELINES FOR CLOUD SECURITY

Breakout: defining the guidelines

- For cloud services:

1. What are the threats?
2. What are the solutions?
3. What is the structure of the guidelines?

- Please:

✓ Appoint someone to write your flipchart

✓ Select one person to present your work

✓ Write everything on a flip chart

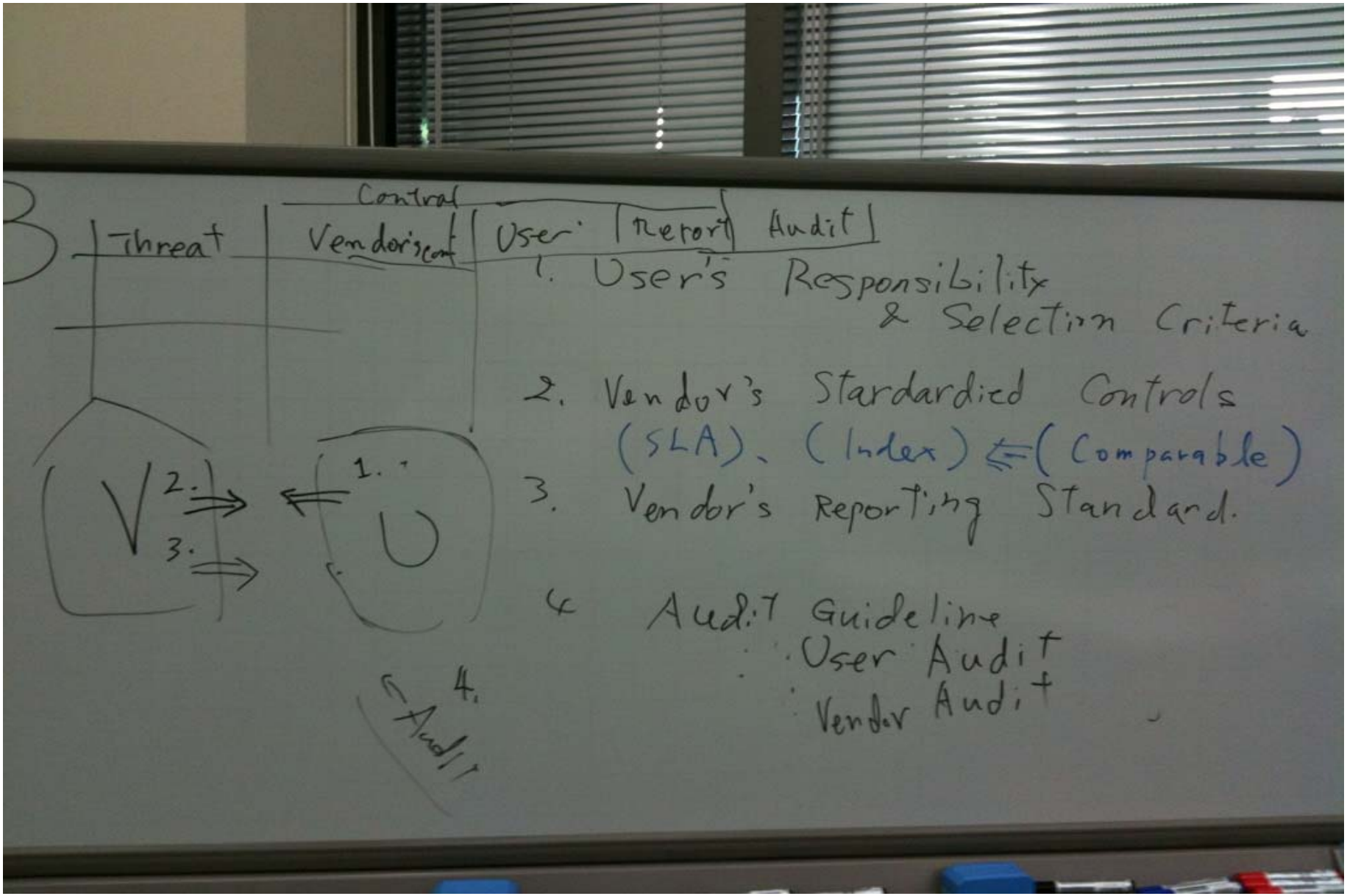
✓ Link threats to solutions

DEFINING THE GUIDELINES

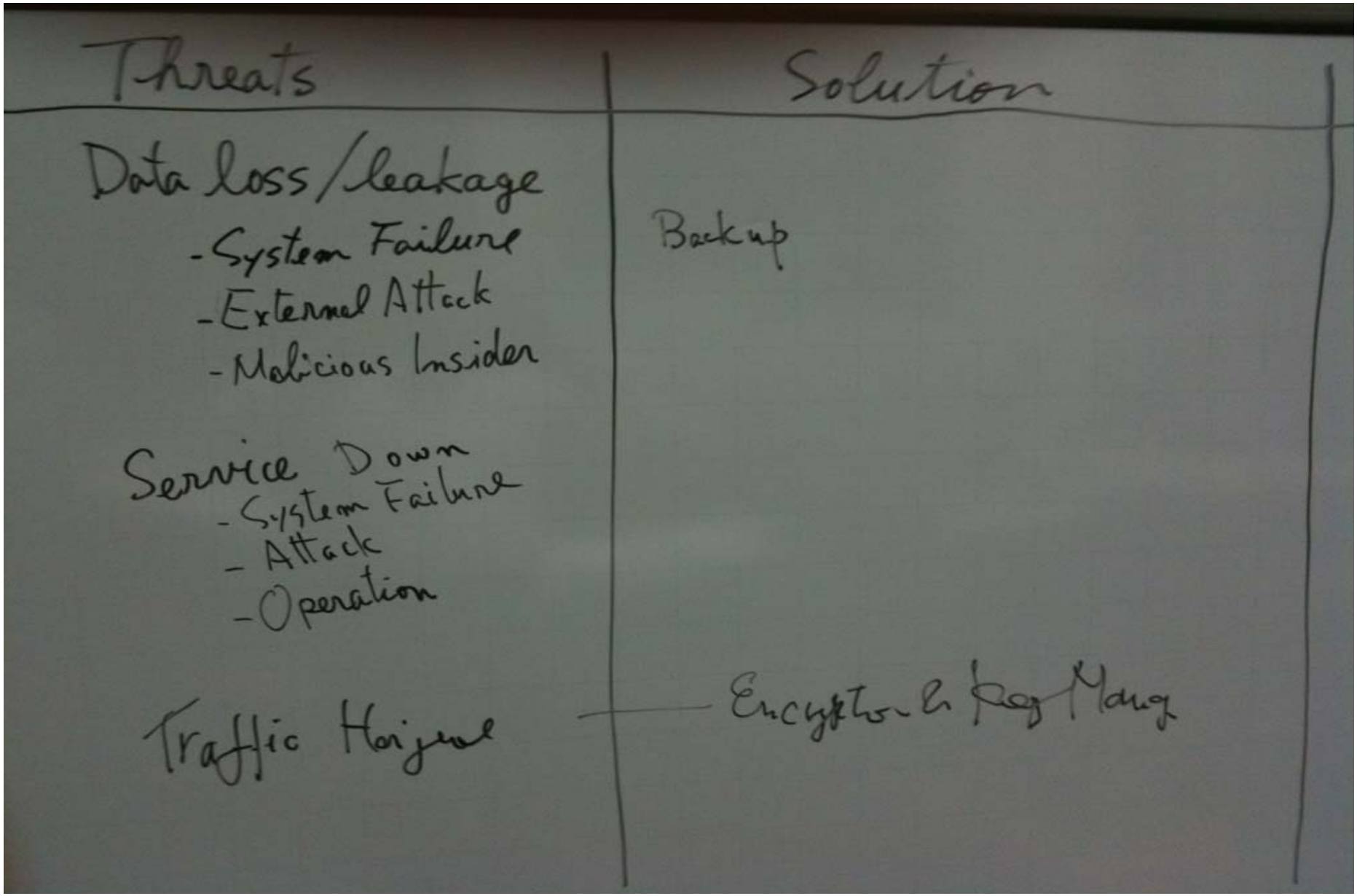
グループ2


Threat
Solution
Guidelines
① Information Leaking
Masquarade
Alter
· User Access Control
· 〃 Certification Authorization. IdM.
(OTP. PKI. Privilege)
· Encription (Network. Strage)
· definitions
· Requirements
· Proofness
theoritical backgrounds
· Test/ability
② Machine Image Falsification
· Signature Check Between Development
and Running.
· Virus Check
· Monitoring.
· Controls
· Compatibility
Interops---
③ Compliance Breach.
· Audit / Log management.
· Monitoring.
Compliance
Report
(PCI-DSS
HIPPA
P-Mark)

グループ3


Control
Threat
Vendor's cont
User
Report
Audit
1. User's Responsibility & Selection Criteria
2. Vendor's Stardardied Controls (SLA). (Index) ⇐ (Comparable)
3. Vendor's Reporting Standard.
4 Audit Guideline
User Audit
Vendor Audit
V
U
2.
3.
1.
4.
Audit

グループ1


Threats
Solution
Data loss/leakage
- System Failure
- External Attack
- Malicious Insider
Backup
Service Down
- System Failure
- Attack
- Operation
Traffic Hoijack
Encryption & Key Mang

WORKING WITH ITU-T / ISO

ITU-T Cloud Computing FG
（第1回　会合に向けて）

FGのScope

ITU-T　A7勧告に従いFGが結成され、通信（Telecommunication)に関連する事象に貢献することを目指す。すなわち、通信ネットワークを介したトランスポート系、通信に関わるセキュリティ、サービス要求条件など、通信ネットワークの活用という視点から、クラウドコンピューティングにおけるサービスやアプリケーションを支援することを目指す。

特に、

- クラウドコンピューティングのために、通信/ICTのサポートを促進し、高度化することが求められる標準開発や標準化の特質について、何が潜在的なインパクトを与えるのかを見極める。
- ITU-Tのスコープの中で、固定・移動ネットワークのための将来研究項目を見つけ出す。
- 相互接続性や標準化の視点から、どの要素が最も有効であるかを分析する。
- クラウドコンピューティングのための通信/ICTに関わる支援について、チャレンジのある活動を進める標準化団体と精通する
- クラウドコンピューティングの支援において、通信/ICTの標準化の適切な時期を見極める（Assess）するために、クラウドコンピューティング属性、機能、特徴における変化（率）を分析する。

FSは、他の世界中のクラウドコンピューティングに関する団体（研究、財団、フォーラム、学会など）と連携していく。

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。

目的（その2）

- ITU-Tのスコープの中で、標準化開発における潜在的なインパクトを識別する。例えば、

– NGN including mobile and overlaying platforms
– Transport layer technologies
– Terminals and application aspects over integrated broadband cable and television networks
– ICT and climate change
– Management and control including signalling
– Interface of networks and Interoperability
– QoS and **security**
– Distributed media-rich processing and intelligent media coding
– Identity management

FGのマネジメントチーム構成

- Chairman: Vladimir Belenkovich（ロシア）
- Vice-Chairman: Jamil Chawki（フランス）
- Vice-Chairman: Kangchan Lee（韓国）
- Vice-Chairman: Mingdong Li（中国）
- Vice-Chairman: Monique Morrow （米国）
- Vice-Chairman: Koji Nakao（日本）

FG会議の構成（案）

WG1: Cloud computing benefits & requirements

1-1 Cloud Definition, Ecosystem & Taxonomy

1-2 Uses cases Requirements & Architecture

1-3 Cloud security

1-4 Infrastructure & Network enabled Cloud

1-5 Cloud Services & Resource Management, Platforms and Middleware

1-6 Cloud computing benefits & first Requirements from ICT perspectives

WG2: Gap Analysis and Roadmap on Cloud Computing Standards development in ITU-T

2-1 Overview of cloud computing SDOs activities

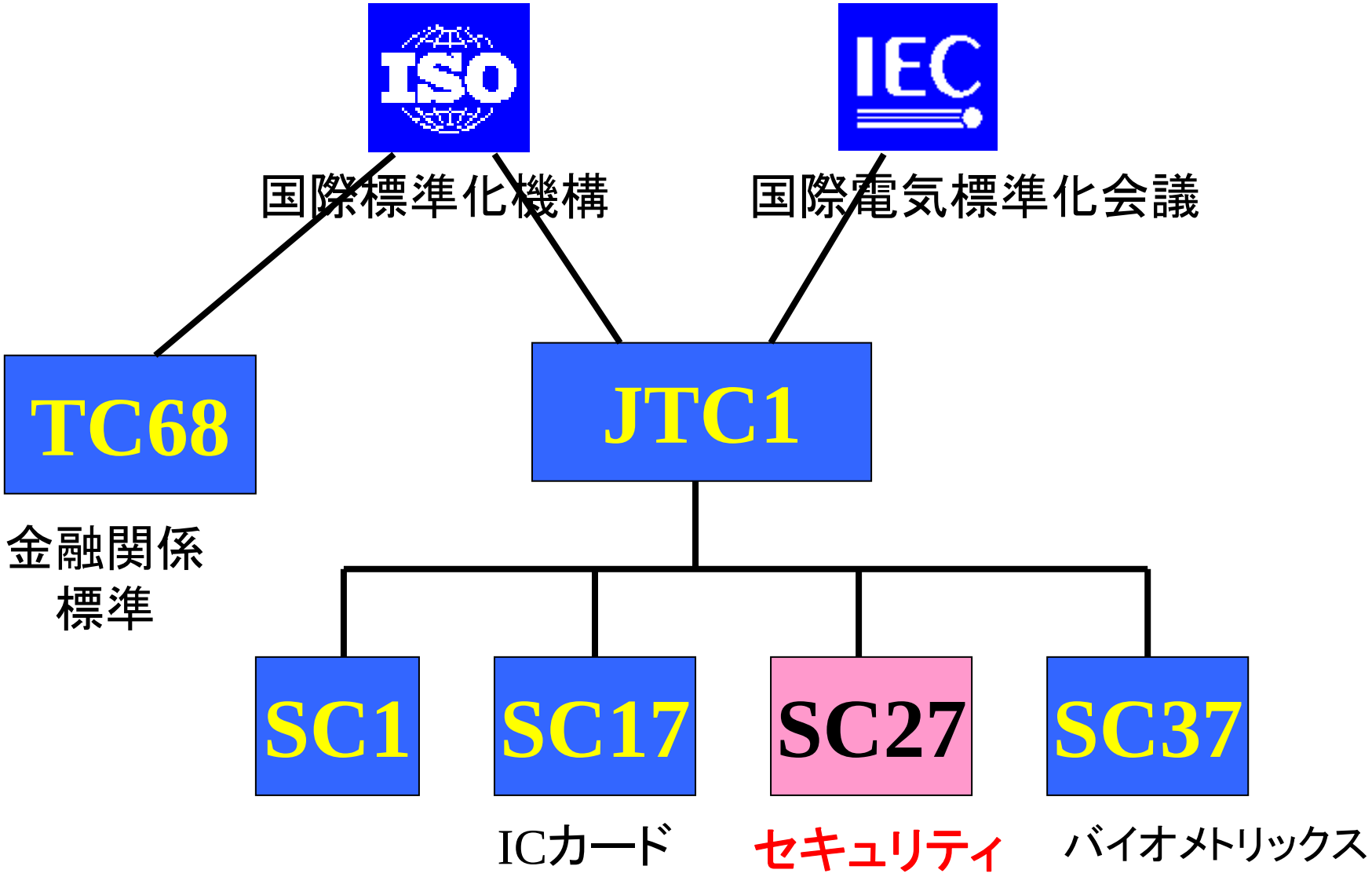
2-2 Gap analysis & Action plan for development of relevant ITU-T Cloud Standard

FGへの期待

- ITU-T　TSAGへの報告が2011年2月。
- セキュリティだけでなく、クラウドコンピューティング全般に関わる課題の抽出。
- ITU-T　の各SGでの課題割当、課題設定の実施。セキュリティはSG17で実施予定。
- 他の標準化団体、フォーラムなどとのうまい連携が鍵。(CSA，ISO，NIST，ENISA等)

ISO/IEC JTC 1/SC 27
IT Security Techniques

ISO/IECの組織構造



ISO/IEC JTC 1 “Information Technology” – *Security Related Sub-committees*

SC 6	Telecommunications and information exchange between systems
SC 7	Software and systems engineering
SC 17	Cards and personal identification
SC 25	Interconnection of information technology equipment
SC 27	IT Security techniques
SC 29	Coding of audio, picture, multimedia and hypermedia information
SC 31	Automatic identification and data capture techniques
SC 32	Data management and interchange
SC 36	Information technology for learning, education and training
SC 37	Biometrics

SC 27 - *Scope*

The development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as

- Security requirements capture methodology
- Management of information and ICT security; in particular information security management systems (ISMS), security processes, security controls and services
- Cryptographic and other security mechanisms
- Security management support documentation including terminology, and guidelines
- Security aspects of identity management, biometrics and privacy
- Conformance assessment, accreditation and auditing requirements in the area of information security
- Security evaluation criteria and methodology

Membership of SC 27

Brazil	Belgium	France	Netherlands	Sweden	~~USSR~~
Canada	Denmark	Germany	Norway	Switzerland	China
USA	Finland	Italy	Spain	UK	Japan
founding P-Members (in 1990)					

Russian Federation	Poland	South Africa	Kenya		Cyprus	Costa Rica
Korea	Ukraine	Malaysia	Austria	New Zealand	Uruguay	Venezuela
Australia	Czech Republic	India	Luxembourg	Singapore	Sri Lanka	Kazakhstan
1994	*1996-1999*	*2001*	*2002*	*2003*	*2005-2006*	*2007-2008*
additional P-Members (total: 37)						

- **O-members** (total: 14):
  Argentina, Belarus, Estonia, Hong Kong, Hungary, Indonesia, Ireland, Israel, Lithuania, Romania, Serbia, Slovakia, Thailand, Turkey

SC 27 - Organization

ISO/IEC JTC 1/SC 27

IT Security techniques

Chair: Mr. W. Fumy
Vice-Chair: Ms. M. De Soete

SC 27 Secretariat

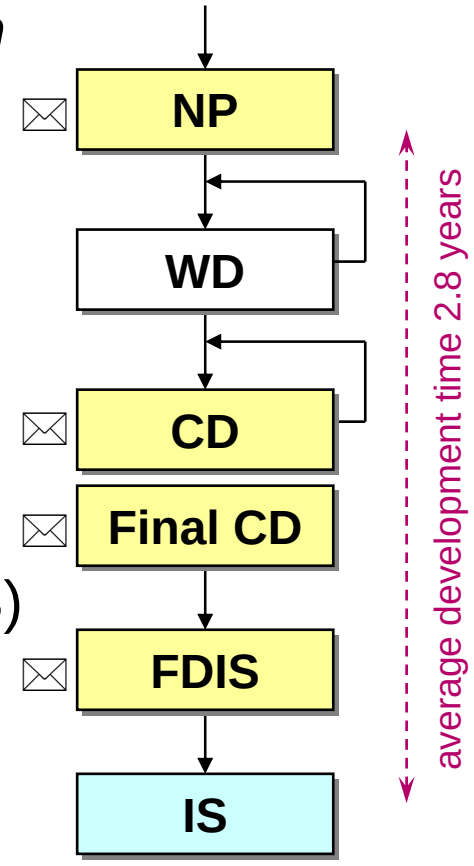
DIN

Ms. K. Passia

Working Group 1	Working Group 2	Working Group 3	Working Group 4	Working Group 5
Information security management systems	***Cryptography and security mechanisms***	***Security evaluation criteria***	***Security controls and services***	**Identity management and privacy technologies**
Convener	*Convener*	*Convener*	*Convener*	*Convener*
Mr. T. Humphreys	*Mr. K. Naemura*	*Mr. M. Ohlin*	*Mr. M.-C. Kang*	*Mr. K. Rannenberg*

ISO – *標準化のプロセス*

- *Maturity level / state of standardization*
  - Study Period / New Project (NP)
    - 2 month NP letter ballot*)
  - Working Draft (WD)
  - Committee Draft (CD/FCD)
    - 3 month CD ballot(s)
    - 4 month FCD ballot
  - Draft International Standard (DIS/FDIS)
    - 2 month FDIS ballot
    - no more comments at this stage
  - International Standard (IS)
    - review every 5 years
    - or after 'defect report'



***) one vote per P-member**

ISO/IEC JTC1/SC27/WG1の活動（その1）

Standard	Title	Status
27000	Overview and vocabulary	Published
27001	ISMS requirements	Published – now revised
27002	Information security management Code of Practice	Published – now revised
27003	ISMS Implementation guide	Awaiting publication
27004	ISM Measurements	Awaiting publication
27005	ISMS Risk management	Published
27006	Accreditation requirements for certification bodies	Published
27007	ISMS Audit guidelines	2nd CD
27008	Guidance on auditing ISMS controls	3rd WD

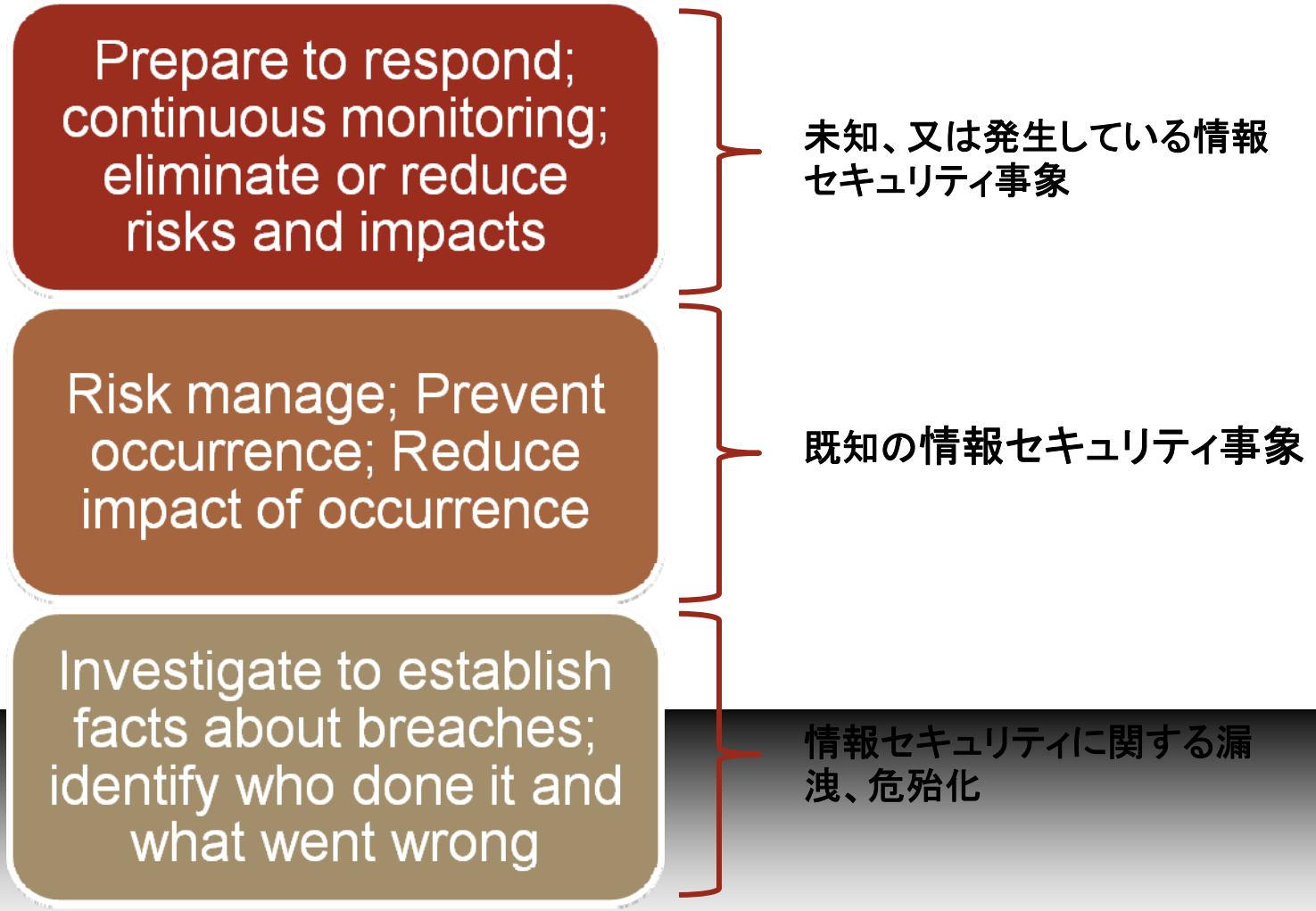
ISO/IEC JTC1/SC27/WG1の活動（その2）

Standard	Title	Status
27010	Sector to sector interworking and communications for industry and government	WD
27011	Information security management guidelines for telecommunications based on ISO/IEC 27002	Published
27012	ISMS guidelines for e-government	cancelled
27013	ISMS for service management	WD
27014	Information security governance framework	WD
27015	ISMS for the financial and insurance service sector	WD
Study Period	Information Security Management Economics	--

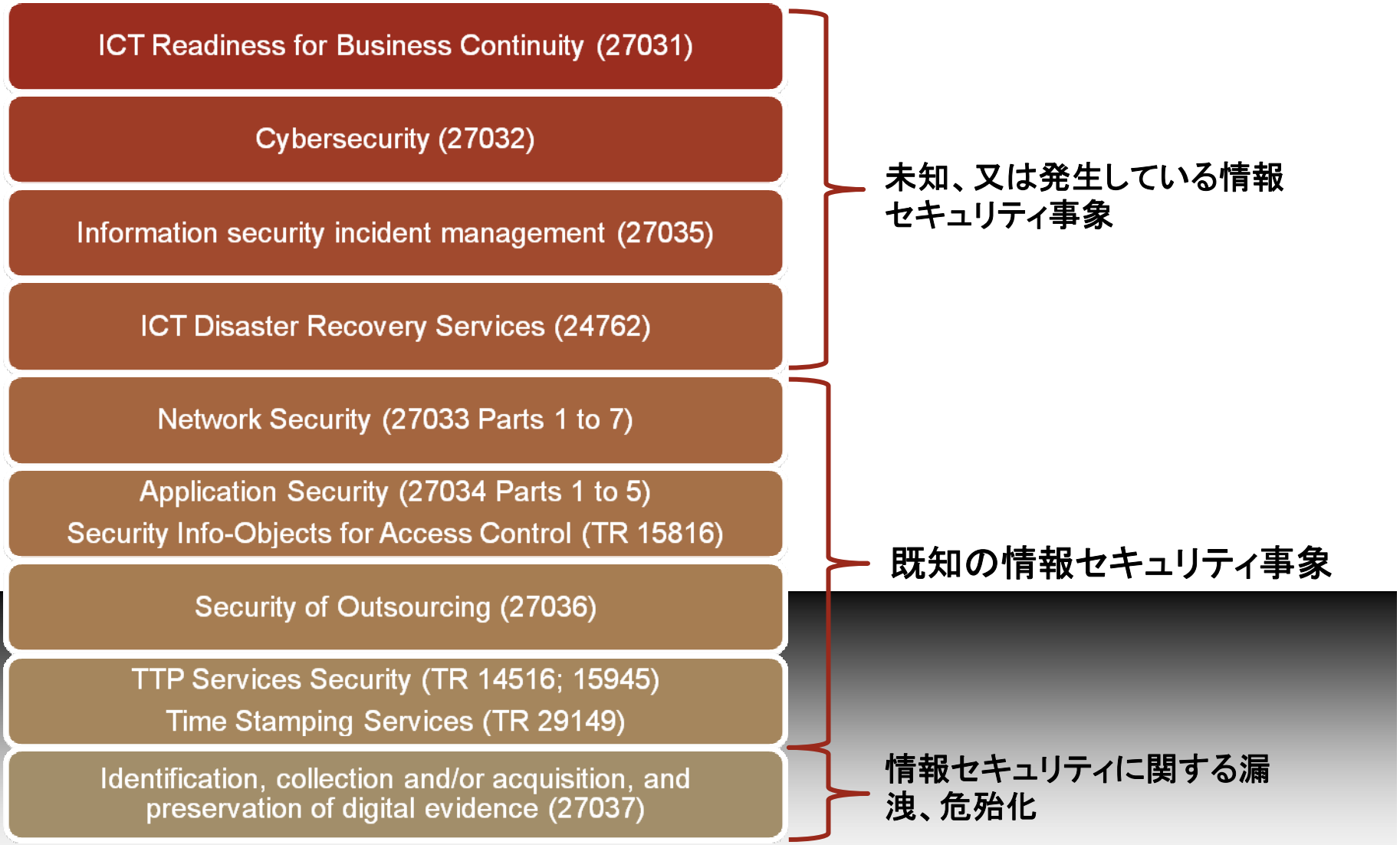
ISO/IEC 27014 Information security governance framework

- IS governance
- Scope:
  - Help meet corporate governance requirements related to information security
  - Align information security objectives with business objectives
  - Ensure a risk-based approach is adopted for information security management
  - Implement effective management controls for information security management
  - Evaluate, direct, and monitor an information security management system
  - Safeguard information of all types, including electronic, paper, and spoken
  - Ensure good conduct of people when using information

WG 4 Roadmap Framework



WG 4 Projects & Study Periods



Proposed Study Periods

1）Storage Security

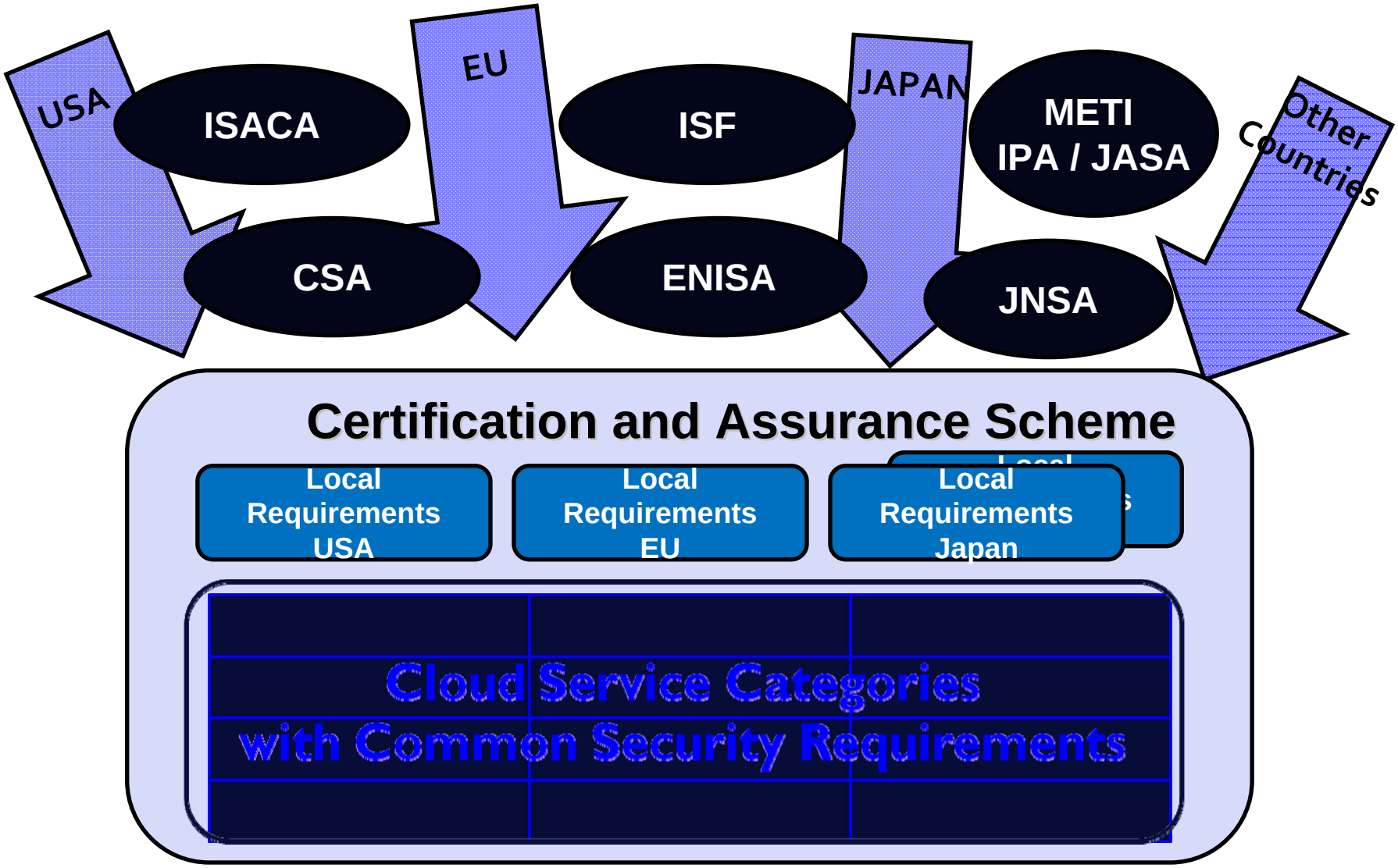
- 米国からストレージセキュリティ(N7924)のトピックのSPの提案があり、ラポーターとして、Eric Hibbard氏 (US)が指名された。次会合にて審議がなされる予定。

2）Supply Chain Security

- 米国からサプライチェーンセキュリティ(N7925)のトピックのSPの提案があり、ラポーターとして、Nadya Bartol女史 (US)が指名された。次会合にて審議がなされる予定。

NEXT STEPS

We need Global joint efforts



Possible direction of Cloud Service Certification and Assurance

Possible ISF project – now under voting

- Cloud Computing revisited:
- A follow-up report to the original ISF Cloud computing report will identify best practices for supplier selection, security risk assessments and examine ways of negotiating data security in the cloud after your senior management has already taken the plunge.

Next steps: Guidelines

- JNSA / JASA / ISF
  - JNSA and JASA draft guidelines
  - ISF (if resources permit) will review
  - ISF to support submission to ISO

- ISO
  - Submit the guidelines to ISO October 2010
  - Recommend the guidelines be confirmed as part of the 2700X series
  - Manage the approval process through SC27

Is SC27 the right committee?
What other activities can we perform?

Next steps: ITU

- ITU-T Cloud Computing FGの動向把握
→　JNSA/ISFへのフィードバック
- 現状のFGは、標準化推進項目の洗い出し
- JNSA/ISFの成果物を想定した、標準化検討項目の提案の実施（FGへ）
- 実際の作業は、2011年度からSG17（セキュリティ）にて推進される予定。

クラウドを見据えたセキュリティ研究の方向は？（1）

1）クラウドそのもののセキュリティ確保

・クラウド内の技術要件、実装要件の不透明さ

・事故（インシデント）の発生時のトレーシングの重要性を認識（クラウドの挙動監視）

→ クラウド内のデータ転送情報の可視化

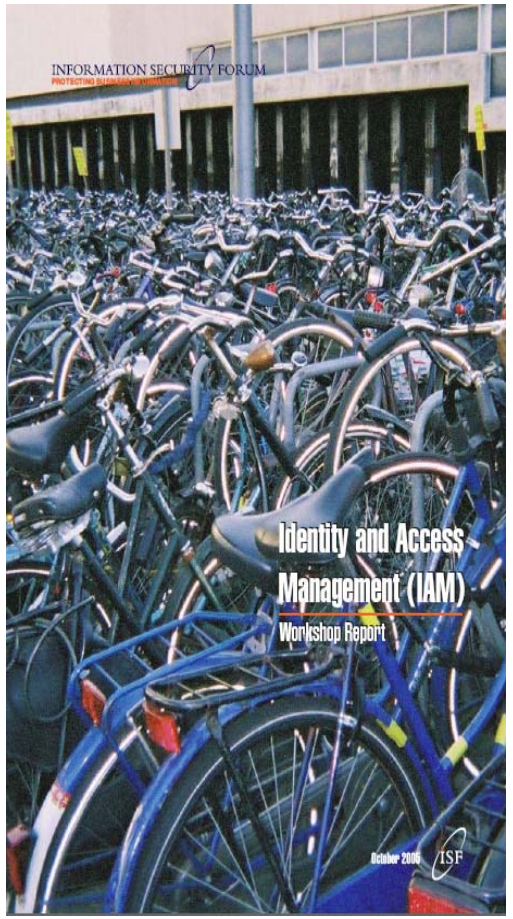
（例：Atlas－X）

→ リスクの抽出、評価の実施

→ 共有ファイアウォールのあり方　等

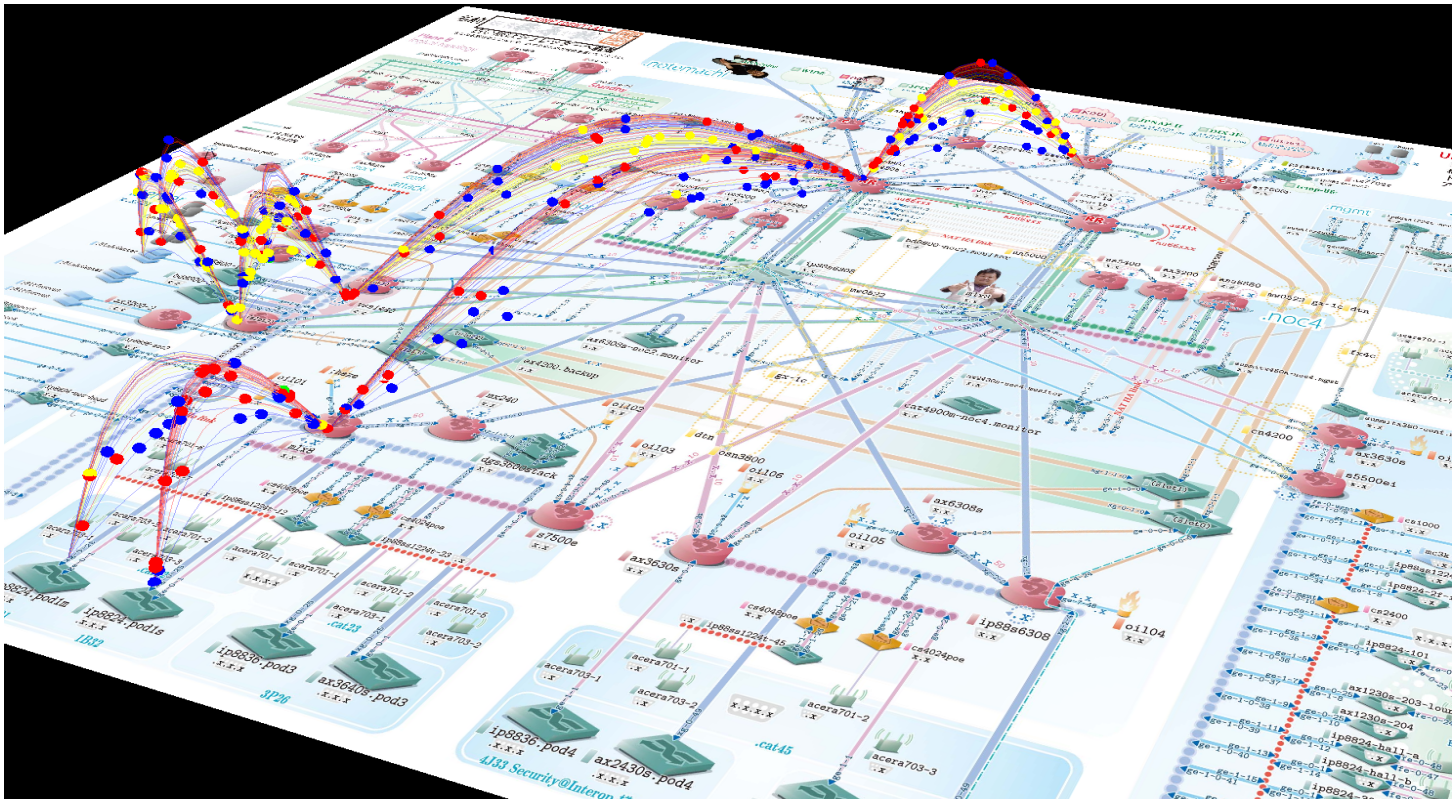
・クラウド脅威評価（リスク評価と連携して）

外部からの脆弱性評価試験などを通して、クライドのネットワークセキュリティとしての安全性の検証を実施



例:リアルトラフィック観測・可視化ツール (Atlas X) 開発

本システムは Interop 2009 の基幹ネットワークである ShowNet において実運用に供され，障害把握・ボトルネック調査等に貢献した.



クラウドを見据えたセキュリティ研究の方向は？（2）

2）クラウドを利用したセキュリティ技術

－ハニーポット（Web，DNS，FTPのセット等）など、セキュリティを目的とする情報収集システムをクラウド上に仕掛ける。

－クラウドを用いたセキュリティ情報共有システムの構築

JNSAの関わり方（1）

クラウドの統制・管理領域　→　JASA領域

- 統制とリスク管理（プロバイダーの管理体制など）
- 法務・契約事項（法環境の差など）
- コンプライアンスと監査（評価、監査など）
- 情報のライフサイクル管理
- 移植性と相互運用性

クラウドの運用（活用）領域　→　JNSA領域

- データセンターセキュリティ、事業継続、災害復旧
- データセンター運用（データ/プロセスの分離など）
- インシデント対応、通知、回復
- アプリケーションセキュリティ
- 暗号化、及び鍵管理
- アイデンティティ・アクセス管理
- 仮想化（仮想化環境単位のセキュリティ装備など）

JNSAの関わり方（2）

検討の母体、及び方針（案）：

当面、JNSA標準化部会の下に、**「クラウド検討WG」**を設置し、

- 検討すべき技術課題の洗い出し
- 数件の検討項目の選択
- 技術検討の詳細実施
- ISFとの間での相互レビュー
- 国際標準化などへの展開

Thank you for listening Q&A