# 情報セキュリティ技術の国際標準化動向の最新報告

中尾 康二
KDDI株式会社 情報セキュリティフェロー
独立行政法人情報通信研究機構（NICT）主管研究員）

# 本日のトピック

０）標準化機関の相関図

１）プライバシー保護のマネジメント

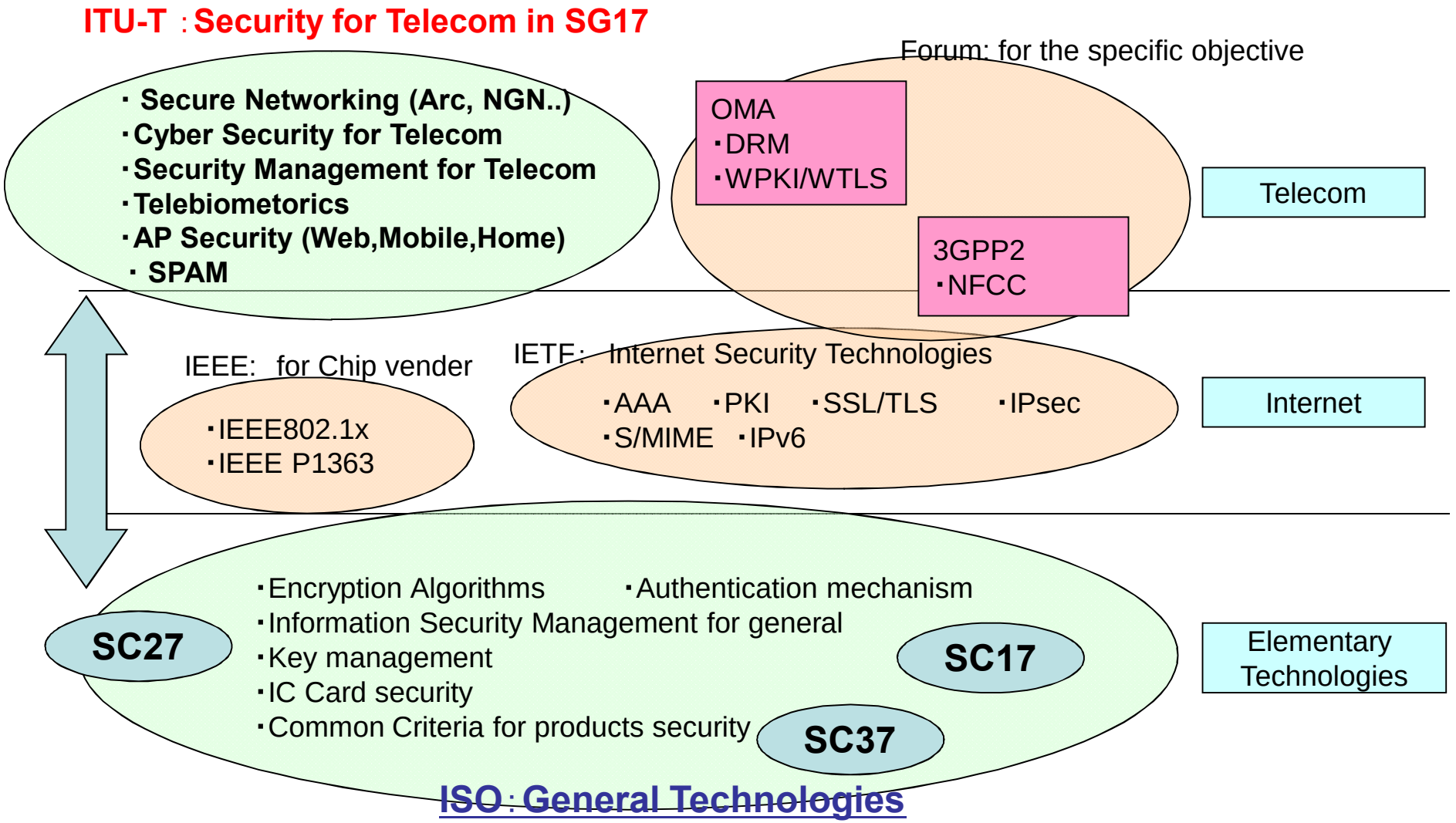
２）クラウドセキュリティ

３）サイバーセキュリティ（情報交換をベース）

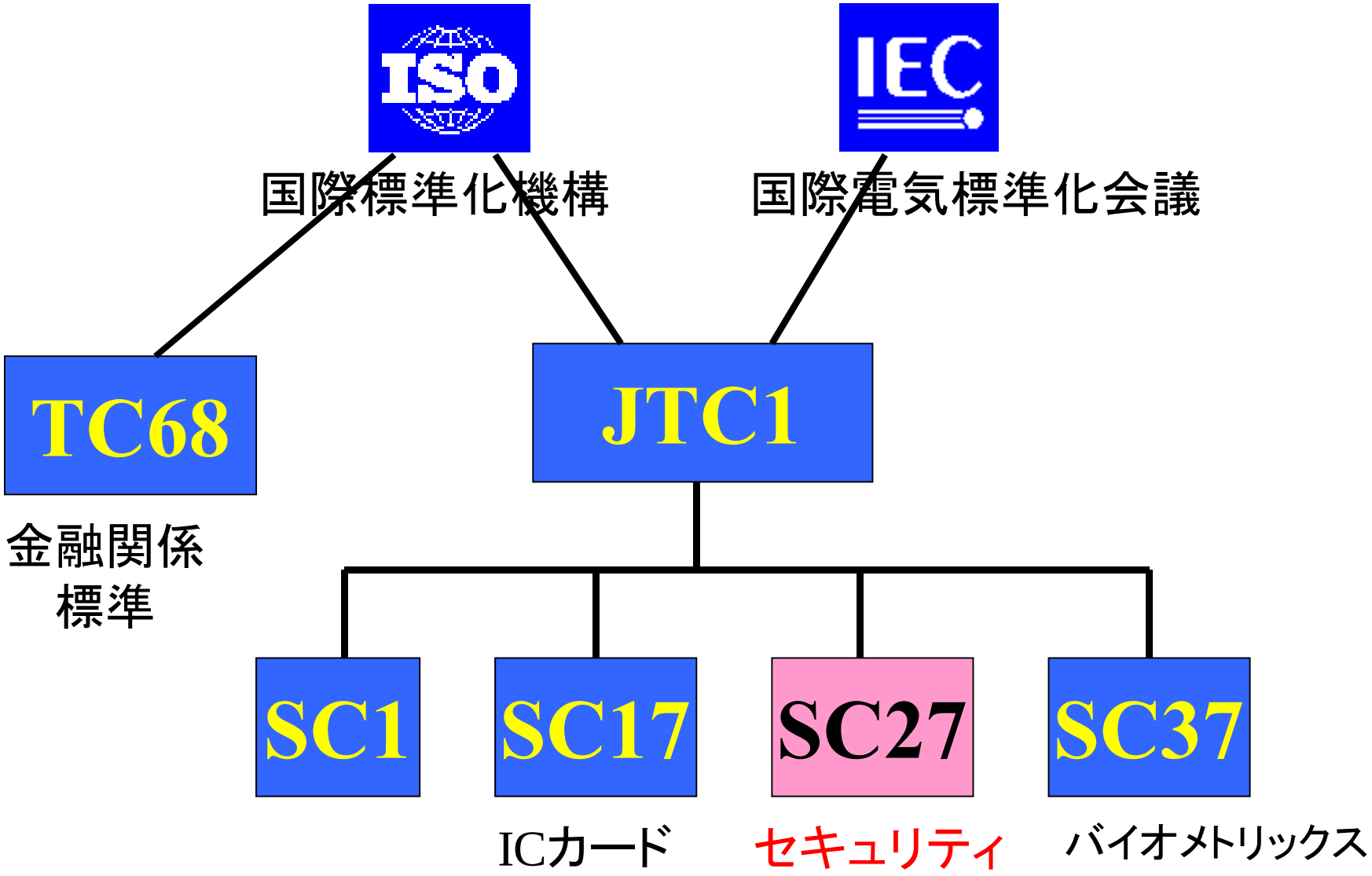
４）その他のトピック

- IPv6
- スマートグリッド/スマートフォン
- ISMS関係

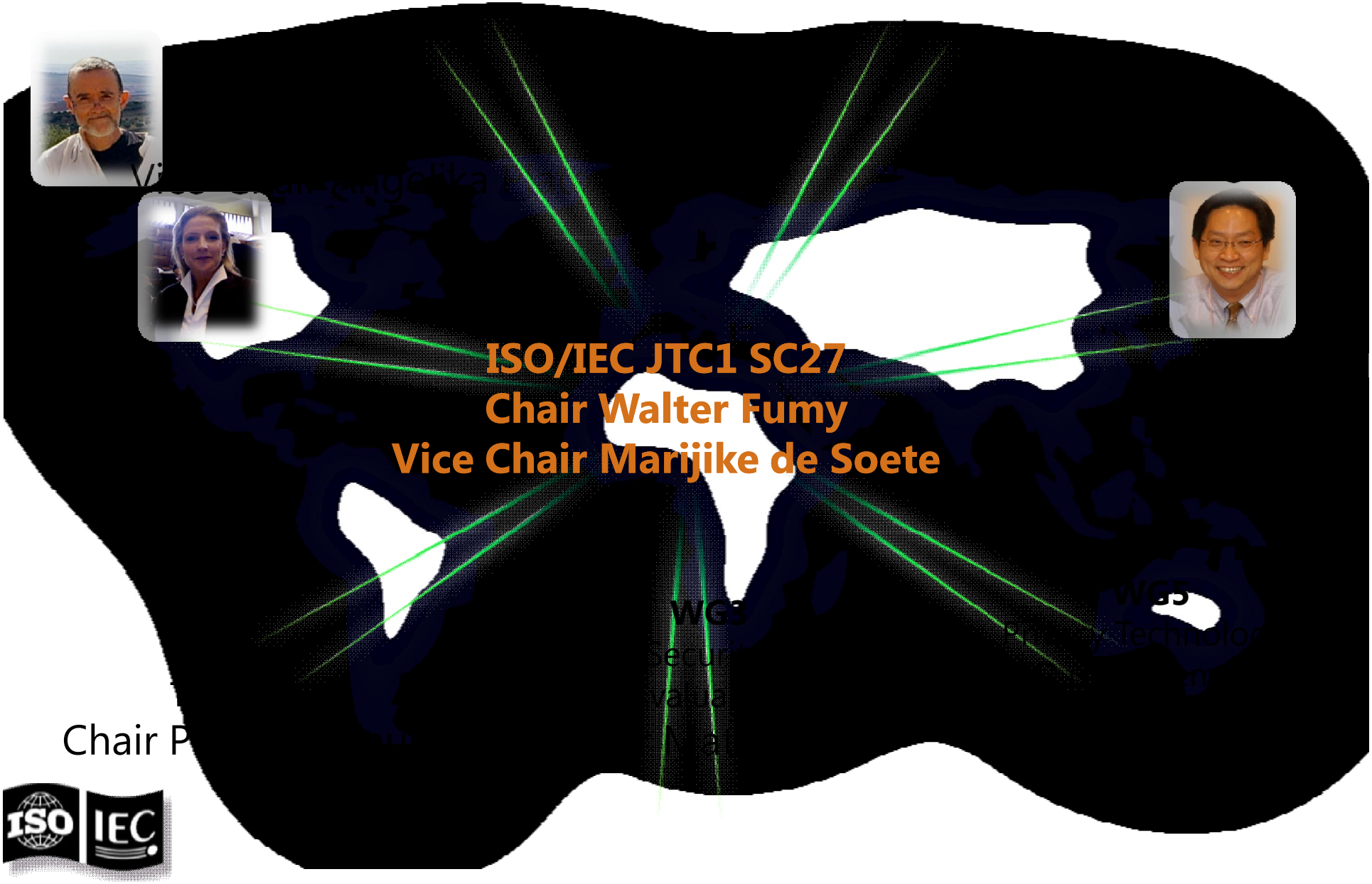
# 各標準化機関の相関


ITU-T：Security for Telecom in SG17
・Secure Networking (Arc, NGN..)
・Cyber Security for Telecom
・Security Management for Telecom
・Telebiometorics
・AP Security (Web,Mobile,Home)
・SPAM
Forum: for the specific objective
OMA
・DRM
・WPKI/WTLS
3GPP2
・NFCC
Telecom
IEEE: for Chip vender
・IEEE802.1x
・IEEE P1363
IETF: Internet Security Technologies
・AAA ・PKI ・SSL/TLS ・IPsec
・S/MIME ・IPv6
Internet
・Encryption Algorithms ・Authentication mechanism
・Information Security Management for general
・Key management
・IC Card security
・Common Criteria for products security
SC27
SC17
SC37
Elementary Technologies
ISO：General Technologies

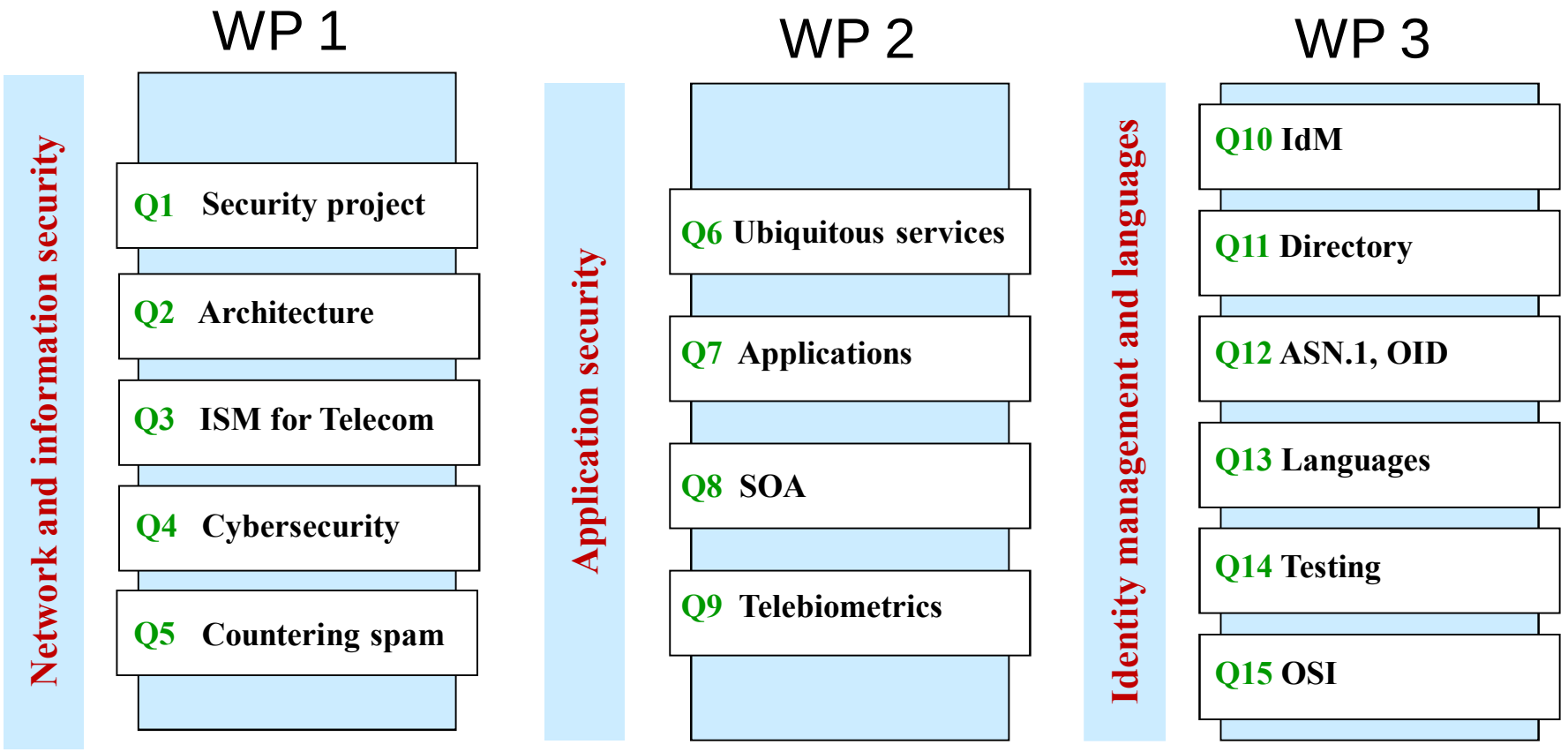
# ISO/IECの組織構造



# SC 27 のWG構成


ISO/IEC JTC1 SC27
Chair Walter Fumy
Vice Chair Marijike de Soete
WG3
WG5
Chair P

# ITU-T Study Group 17, Security



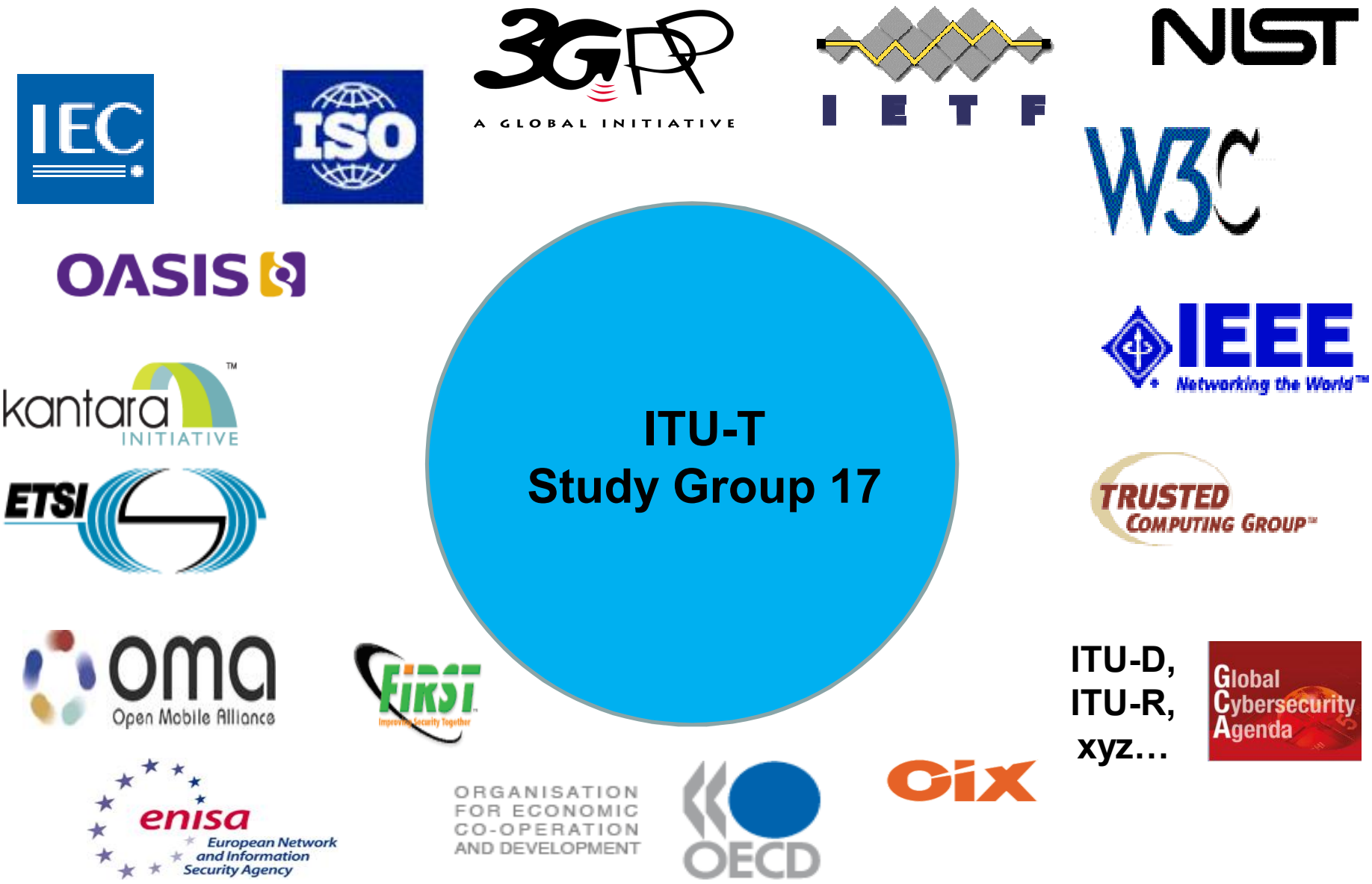

Lead Study Group on:

- Telecommunication security
- Identity management (IdM)
- Languages and description techniques

Parent for Joint Coordination Groups:

- Identity management
- Conformance & interoperability testing

# SG17との関連団体


IEC
ISO
3GPP
A GLOBAL INITIATIVE
IETF
NIST
W3C
OASIS
IEEE
Networking the World
kantara
INITIATIVE
ETSI
ITU-T
Study Group 17
TRUSTED
COMPUTING GROUP
oma
Open Mobile Alliance
FIRST
ITU-D,
ITU-R,
xyz…
Global
Cybersecurity
Agenda
enisa
European Network
and Information
Security Agency
ORGANISATION
FOR ECONOMIC
CO-OPERATION
AND DEVELOPMENT
OECD
oix

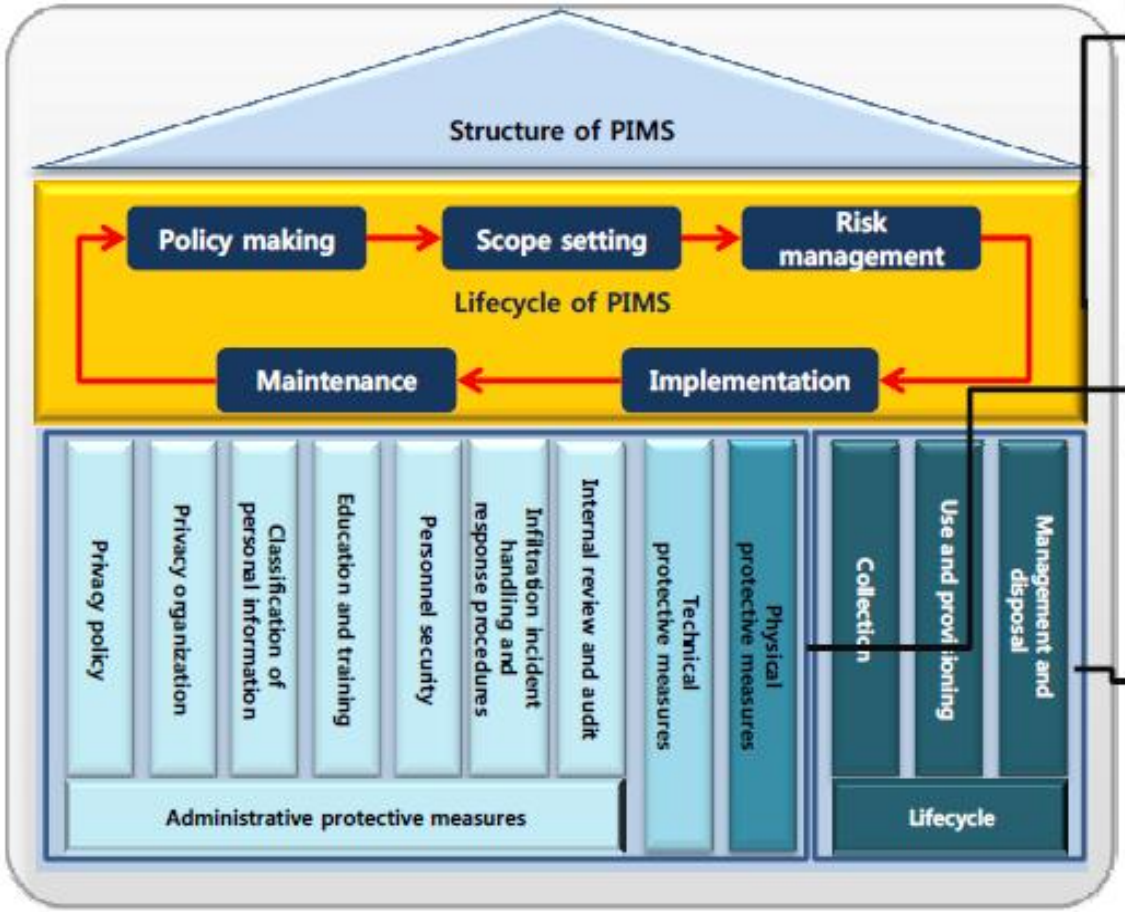
# プライバシーに関わる標準化
# PIMS: Personal Information Management System

# なぜPIMSの規格化か

- 多種多様な個人情報が国を跨って交換される。
- 各国で定める個人情報に関わる法規制は異なっており、国を跨った個人情報の扱いに問題がでてくる。
- システム的な、効率的な、かつ一貫性のある個人情報の管理の確立が望まれるところであり、組織における個人情報の処理が個人情報保護方針に合っているかのチェックも必要となる。
- しかし、個人情報管理に関するグローバルな仕組みや共通の理解は欠落しており、国を跨った個人情報の扱いにおいて、今後問題となる可能性がある。
- さらに、個人情報管理のための要求事項、プライバシー保護管理策などの策定は、国際的な共通認識の向上に貢献できる。

# What is the PIMS?

- The PIMS is a series of protective measures that is required for the enterprise to protect customer's personal information systematically and continuously.




**Management process (5 Requirements/11 Controls)**

To define periodical and systematical management process for personal information protection

**Managerial, Technical Safeguards (9R/79C)**

To define managerial, technical and physical protection measures for PI

**PI lifecycle protection (3R/28C)**

To define requirements by law for each life stage, from generation to disposal of PI

# Criteria of PIMS

| | |
|---|---|
| **Management Process** | Establishing personal information policy |
| | Establishing scope of management system |
| | Risk management |
| | Implementation |
| | Maintenance |
| **Managerial, Technical Safeguards (Controls)** | Personal information security policy |
| | Personal information security organization |
| | Classification of personal information |
| | Education and training |
| | Personnel security |
| | Procedure of incident process and respond |
| | Technological protection measures |
| | Physical protection measures |
| | Internal review and audit |
| **Personal Information Lifecycle Protection Controls** | Collection of personal information |
| | Use and transfer of personal information |
| | Retention and disposal of personal information |

# Procedure of PIMS certification

- The procedure of certification and assessment consists of four stages: ① Preparation, ② Assessment, ③ Certification and ④ Maintenance Stage.

| | |
|---|---|
| 1 Preparation | This stage features preparations for the assessment. When an application for certification is accepted, an agreement for certification assessment is executed |
| 2 Assessment | The assessment consists of a document review and the site inspection |
| 3 Certification | The Certification Board deliberates on the validity of the certificate based on the report of the results of the assessment, and the results of the certification assessment are reported and the certificate issued upon the consent of two-thirds or more of the members of the Board |
| 4 Maintenance | The maintenance stage consists of post-management assessment, renewal assessment and reassessment. |

# Criteria of PIMS certification

| Control Area | Control Content | No. of control objective | No. of control items | No. of check items |
|---|---|---|---|---|
| Management Process | 1.Establishing personal information policy | 1 | 3 | 5 |
| | 2. Establishing scope of management system | 1 | 2 | 5 |
| | 3. Risk Management | 1 | 3 | 7 |
| | 4. Implementation | 1 | 1 | 2 |
| | 5. Maintenance | 1 (5) | 2 (11) | 4 (23) |
| **Managerial, Technical Safeguards (Controls)** | 1. Personal information security policy | 3 | 6 | 11 |
| | 2. Personal information security organization | 2 | 5 | 9 |
| | 3. Classification of Personal Information | 2 | 4 | 7 |
| | 4. Education and Training | 2 | 4 | 7 |
| | 5. Personnel Security | 2 | 3 | 9 |
| | 6. Procedure of incident process and respond | 3 | 7 | 20 |
| | 7. Technological protection measures | 6 | 36 | 125 |
| | 8. Physical protection measures | 3 | 5 | 12 |
| | 9. Internal Reviews and Audits | 4 (27) | 9 (79) | 24 (224) |
| **PI Lifecycle Protection Controls** | 1. Collection of personal information | 3 | 7 | 17 |
| | 2. Use and transfer of personal information | 6 | 16 | 49 |
| | 3. Retention and disposal of PI | 1 (10) | 5 (28) | 12 (78) |
| **Total** | **17** | **42** | **118** | **325** |

# 韓国PIMSの規格化提案

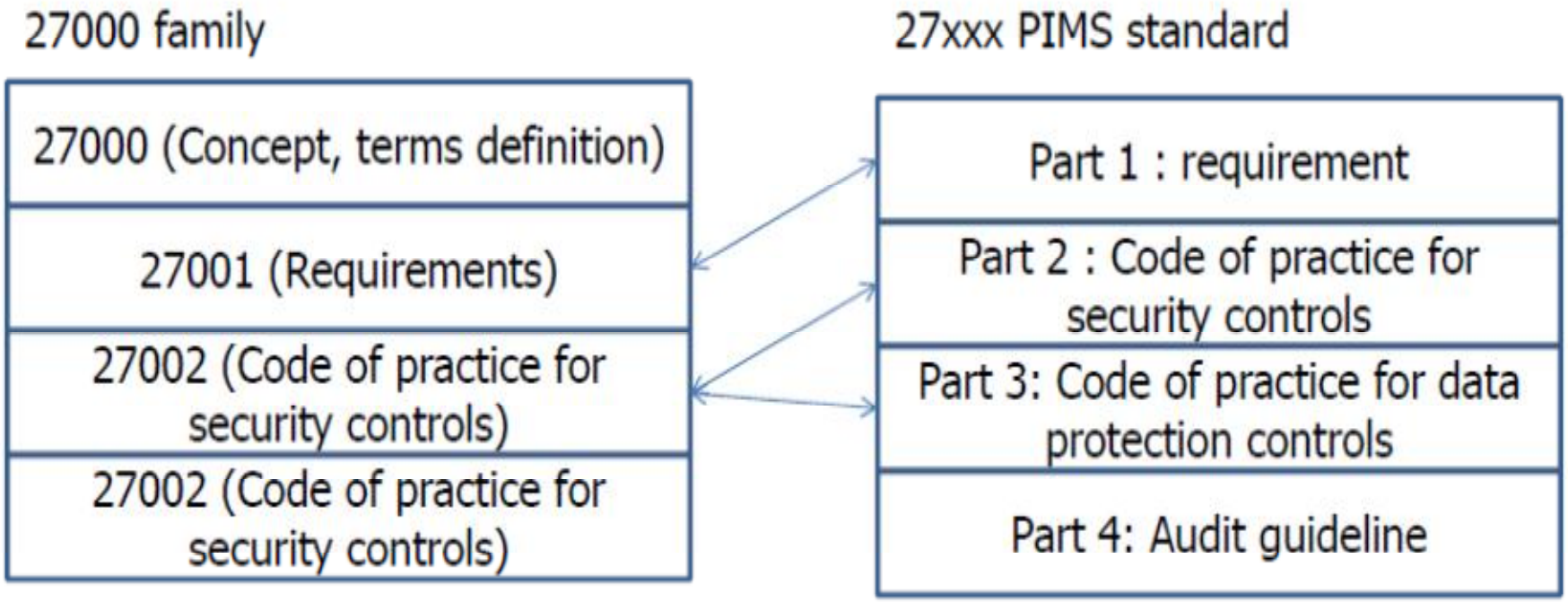
２０１１年９月

ITU-T（SG17）に新規課題として、「個人情報管理のためのガイドライン（通信事業者用）」を提案し、暫定的な合意となり、２０１２年２月に再審議の予定。

２０１１年１０月

ISO/IEC JTC1/SC27/WG1 & WG5に対して、新規課題「PIMS」を提案。通信事業者向けではなく、一般の企業利用を想定した、MS (Management System)として提案。結果、SP (Study Period)として、新課題（プロジェクト）設立に向けた基礎検討が開始された。

# Relationship between ISO 27001 series and PIMS series



# 本提案に関連する外部規格

- JIS　Q15001(ご存知）
- UK-BS 10012
- NIST SP800-53 Appendix J(1)

# UK-BS 10012

- BSIによって発行され、2009年3月に執行。
- Personal Information Management Systemの要求事項を規程している。（データ保護規約に準拠）
- PDCAサイクルを採用。
- 2011年7月までに、2件の組織が認証される。

## Criteria of BS 10012

| | |
|---|---|
| **3. Planning for PIMS** | 3.1 Establishing and managing the PIMS |
| | 3.2 Scope and objectives of the PIMS |
| | .<br>. |
| | 3.7 Embedding the PIMS in the organization's culture |
| **4. Implementing and operating the PIMS** | 4.1 Key appointments |
| | 4.2 Identifying and recording uses of personal information |
| | 4.3 Training and awareness |
| | 4.4 Risk assessment |
| | 4.5 Keeping PIMS up-to-date |
| | 4.7 Notification |
| | .<br>. |
| | 4.17 Maintenance |
| **5. Monitoring and reviewing the PIMS** | 5.1 Internal audit |
| | 5.2 Management review |
| **6. Improving the PIMS** | 6.1 Preventive and corrective actions |
| | 6.2 Continual improvement |

# NIST SP 800-53 Appendix J(1)

- プライバシー管理策の構造化セットを提供
- プライバシー対策とセキュリティの対策の関係を明示。8つの対策ファミリーと全部で23の対策を提供

| CNTL NO. | PRIVACY CONTROLS |
|---|---|
| **TR** | **Transparency** |
| TR-1 | Privacy Notice |
| TR-2 | Dissemination of Privacy Program Information |
| **IP** | **Individual Participation and Redress** |
| IP-1 | Consent |
| IP-2 | Access |
| IP-3 | Redress |
| IP-4 | Complaint Management |
| **AP** | **Authority and Purpose** |
| AP-1 | Authority to Collect |
| AP-2 | Purpose Specification |
| **DM** | **Data Minimization and Retention** |
| DM-1 | Minimization of Personally Identifiable Information |
| DM-2 | Data Retention and Disposal |
| **UL** | **Use Limitation** |
| UL-1 | Internal Use |
| UL-2 | Information Sharing |
| UL-3 | System Design and Development |
| **DI** | **Data Quality and Integrity** |
| DI-1 | Data Quality |
| DI-2 | Data Integrity |
| **SE** | **Security** |
| SE-1 | Inventory of Personally Identifiable Information |
| SE-2 | Privacy Incident Response |
| **AR** | **Accountability, Audit, and Risk Management** |
| AR-1 | Governance and Privacy Program |
| AR-2 | Privacy Impact and Risk Assessment |
| AR-3 | Privacy Requirements for Contractors and Service Providers |
| AR-4 | Privacy Monitoring and Auditing |
| AR-5 | Privacy Awareness and Training |
| AR-6 | Privacy Reporting |

# Cloud Securityに関する規格化

- ITU-T FG Cloud Computing
- ISO/IEC JTC1/SC27

# ITU-T FG-Cloud#8**会合（最終）報告**

2011**年**12**月**

# ITU-T FG-Cloud#8会合（最終会合）結果概要

1. 会合期間 2011年12月12日（月）～16日（金）
2. 目的 ITU-TにおけるCloud Computingの規格化推進のため、技術検討課題を洗い出し、結果を上部機関のTSAGに報告すること。
3. 参加者 48名

内訳 Microsoft5名、ZTE4名、France Telecom3名、Cisco2名、China Telecom2名、China Unicom2名、Oracle1名、EMC1名、中国2名、ドイツ1名、IBM1名他 リエゾン機関DMTF、CSA、GICTF

日本からの参加者 NTT（森田、坂井）、KDDI（中尾FG副議長、松尾）、日立（三宅）、NEC（釼吉）、富士通（加納） 事務局山田

4. 会合概要

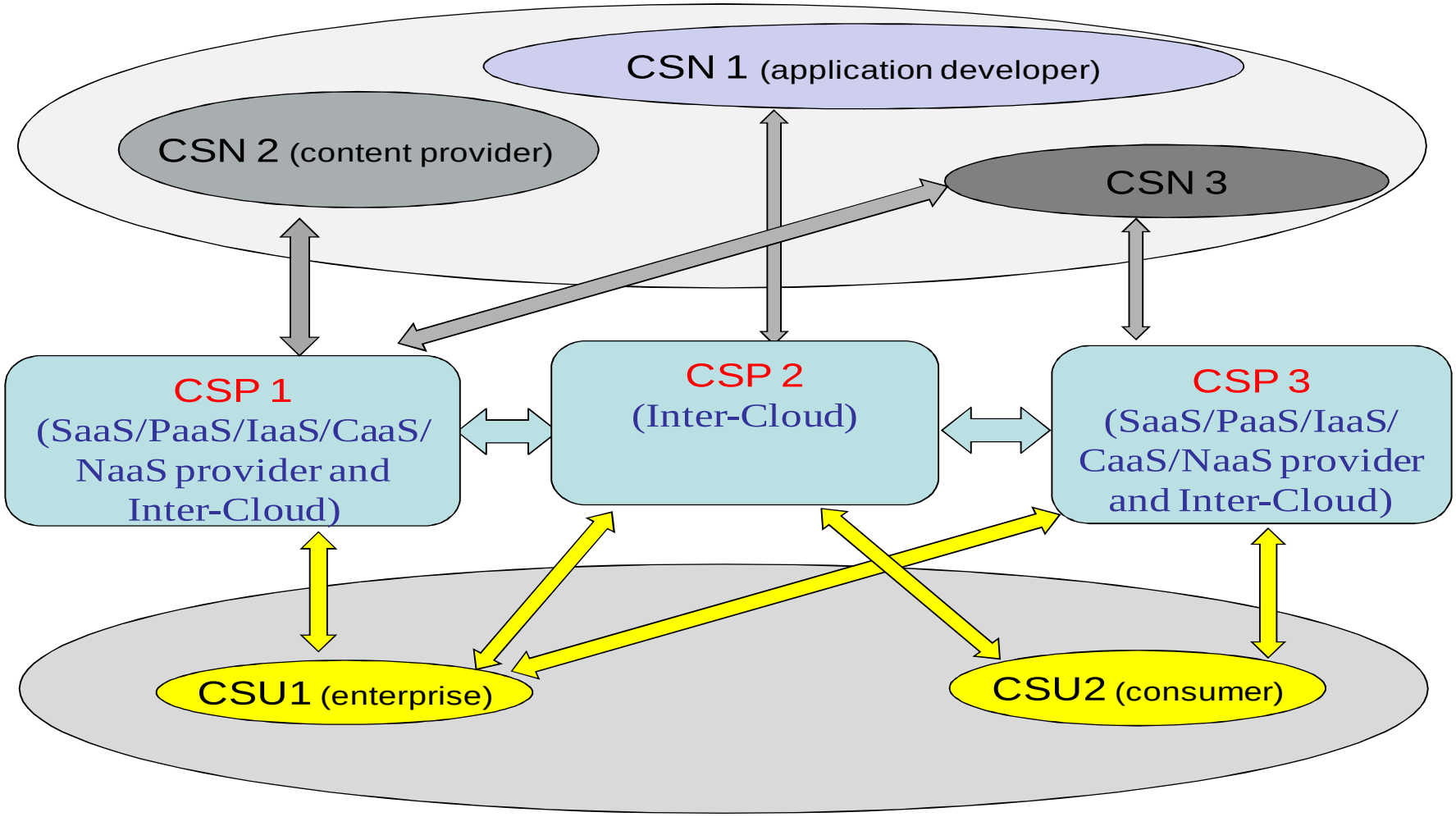
■ 今回は最終会合となるため、作成中であった7件の文書（Deliverables）の完成に向けての最終調整を行った他、親SGであるTSAG1月会合に向けて、ITU-Tが取り組むべき研究課題案（含むISO/IEC JTC1との共同研究提案）、FGが作成したDeliverablesの移管先候補案などを提言としてとりまとめた。

■ 日本からは、Eco文書のInter-Cloudに関する記述詳細化提案、FG成果文書移管先候補提案、Overview of SDOs文書のGap Analysi記述案を寄書により提案し、最終報告書に含まれるTSAGへの提言内容およびセキュリティ文書（エディタ中尾）を含む各文書の最終化に向けて大きな貢献を行った。

# 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



# 参考 : Functional Requirements and Reference Architecture

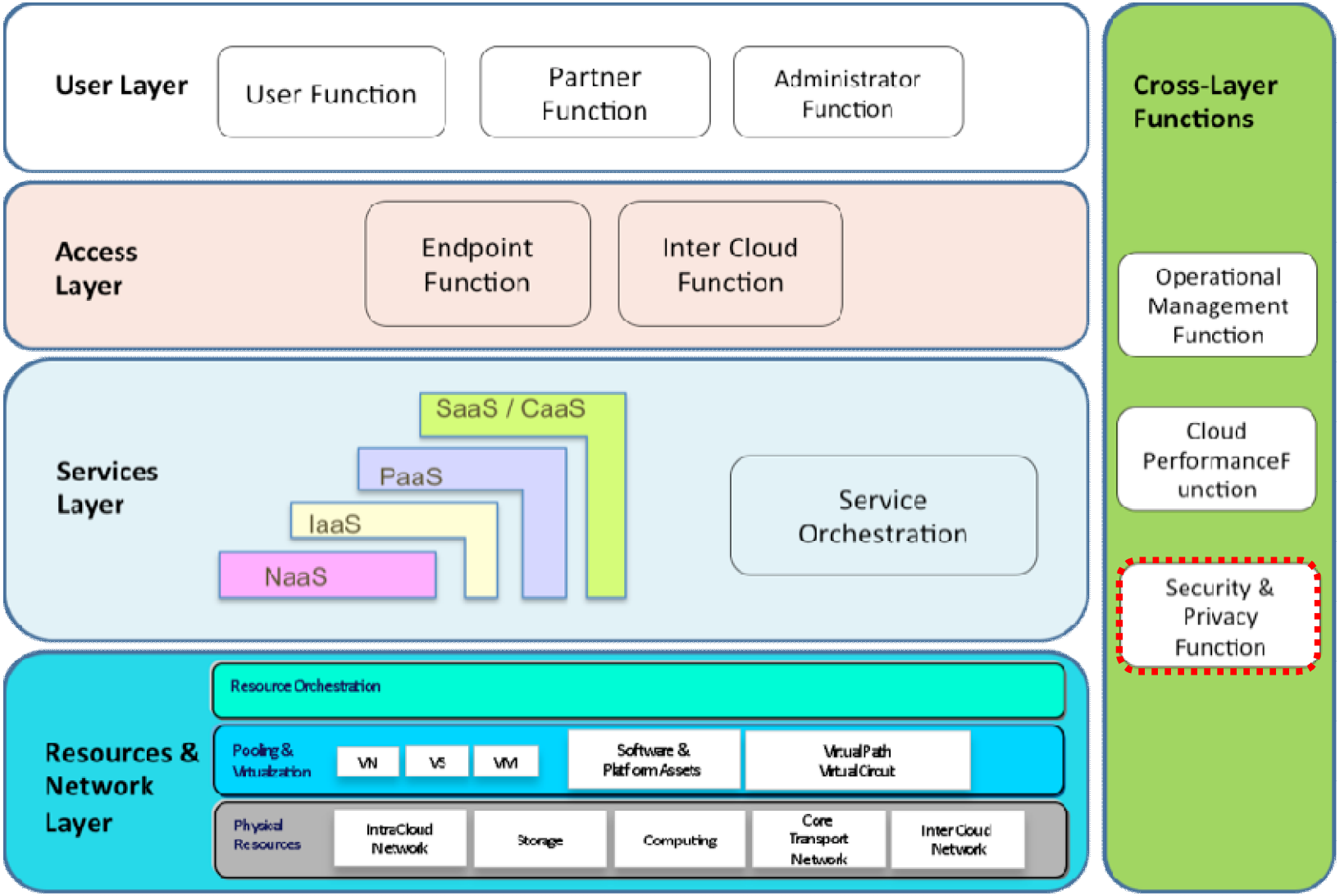
## 検討対象

- 機能要件および参照アーキテクチャを定義する。機能構造、機能レイヤの構成、機能ブロックの定義を含めたブロックダイアグラムの形式で表現している。
- 機能要件として、複数の標準インタフェースをサポートすることや、XaaSのような複数のサービスを提供できることなど、計13項目の要件を定義している。
- 機能レイヤの構成は、リソース・ネットワーク層、サービス層、アクセス層、ユーザ層の四層構造と、運用管理、性能管理、セキュリティ等層間にわたる機能を定義している。

## ハイライト

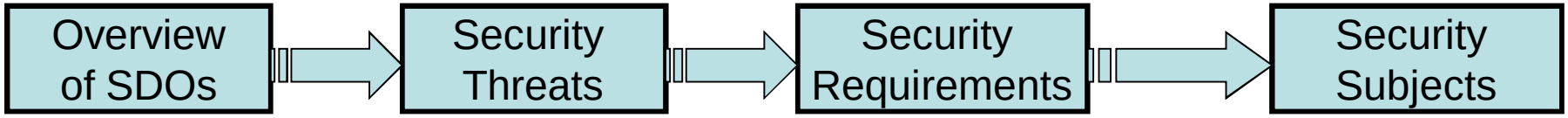
- 前回までは機能ダイアグラムの議論で何度も紛糾したが、今会合ではEcosystem文書との整合性を中心に用語の微調整で合意した。
  - 抽象的な表現を避けるため“Business Process”に記述はAnnexに移動。
  - “End-User”等の表記を”CSU: Cloud Service User”に統一。
  - “Administration Function”を“Administrator Function”に変更。
  - “Inter-Cloud”に関する記述をEcosystem文書と合わせて調整。
- SGへの移管後、実際に参照アーキテクチャの基本文書として勧告化できるかは不明。（ベンダやサービスプロバイダがこの参照アーキテクチャの定義に従うとは思えない。）

# Cloud Computing Functional Reference Architecture



# セキュリティ成果物の進め方

1) Review the existing activities (from CSA, DTMF, GICTF.....) including liaison from SG17
2) Considerations on Security Threats based on Eco-system or RA
3) Security requirements in views of cloud-providers, cloud-users
4) Subjects for security study for ITU-T



# 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

# セキュリティ成果物の結果（概要）

1. 当初の目的通り、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技術検討課題（Study　Subjects）の洗い出しを完了した。
2. クラウドコンピューティング環境における脅威分析、それに関連するセキュリティ要求事項（Requirements）、及び関連するセキュリティ技術検討課題の抽出をまとめた。
3. 最終的にTSAGに対して提出するセキュリティ技術検討課題は以下の通りである。
   - 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
4. これらの課題については、基本的にSG１７の課題として引き継ぐ方向であるが、フランステレコムオレンジは、SG１３において一部の課題を実施する意図がある模様。

See Security Deliverable
最終成果物

# 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。

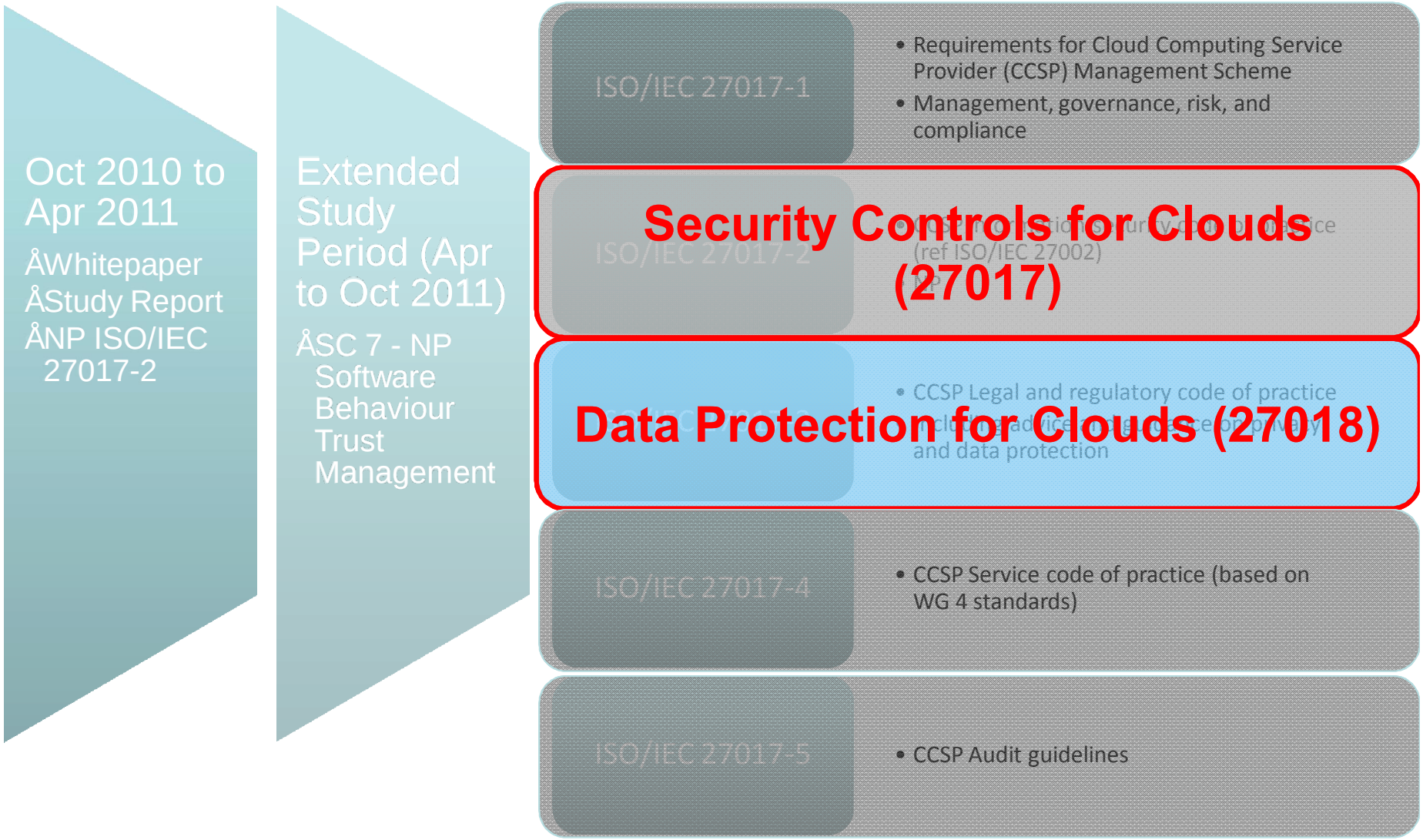
2．他の**SDO**との積極的なコラボレーション（とりわけ**JTC1(ISO & IEC)**との共同作業）を継続する。

3．本**TSAG**会合において**JCA (Joint Coordination Activity)**の設立する。
親**SG**は**SG13**。

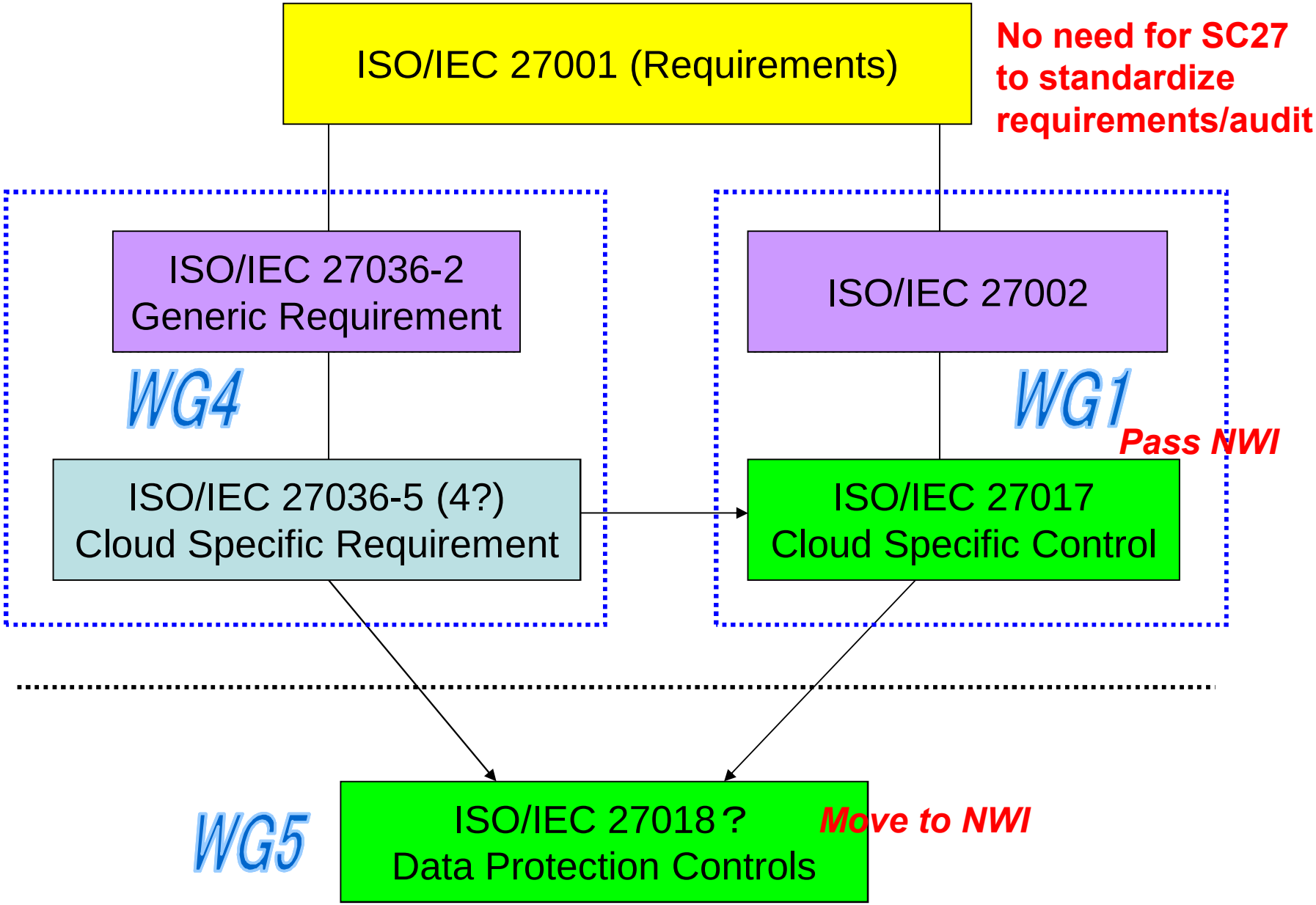
4．**FG** デリバラブルをパブリッシュ**(Publicly available)**する。

5．**Regulatory**関連の勧告化には**TAP**を適用する。

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



# 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



# SC27におけるクラウド規格化概要

1) Cloud Security Control based on 27002 (SC27/WG1) Ÿ ISO/IEC 27017
2) Cloud Data Protection Control (SC27/WG5) Ÿ ISO/IEC 27018？
3) Cloud Technical Controls Implementation (SC27/WG4) Ÿ 継続SP（WG1，WG5と）
   - Cloud (Technical) Requirements (27036-5)
   - BCP/Disaster Recovery (Guideline for ICT DR Services (24762))
   - Storage Security (27040)
   - Network monitoring and incident response (27035)
   - Network Security (27033)
   - Virtualization Security (New)
   - Cloud Digital Evidence (Forensic) (27037, 27041-43)
4) Integration of several cloud related projects into a single TR(?) to navigate their activities including relationship among them.

# サイバーセキュリティに関する規格化

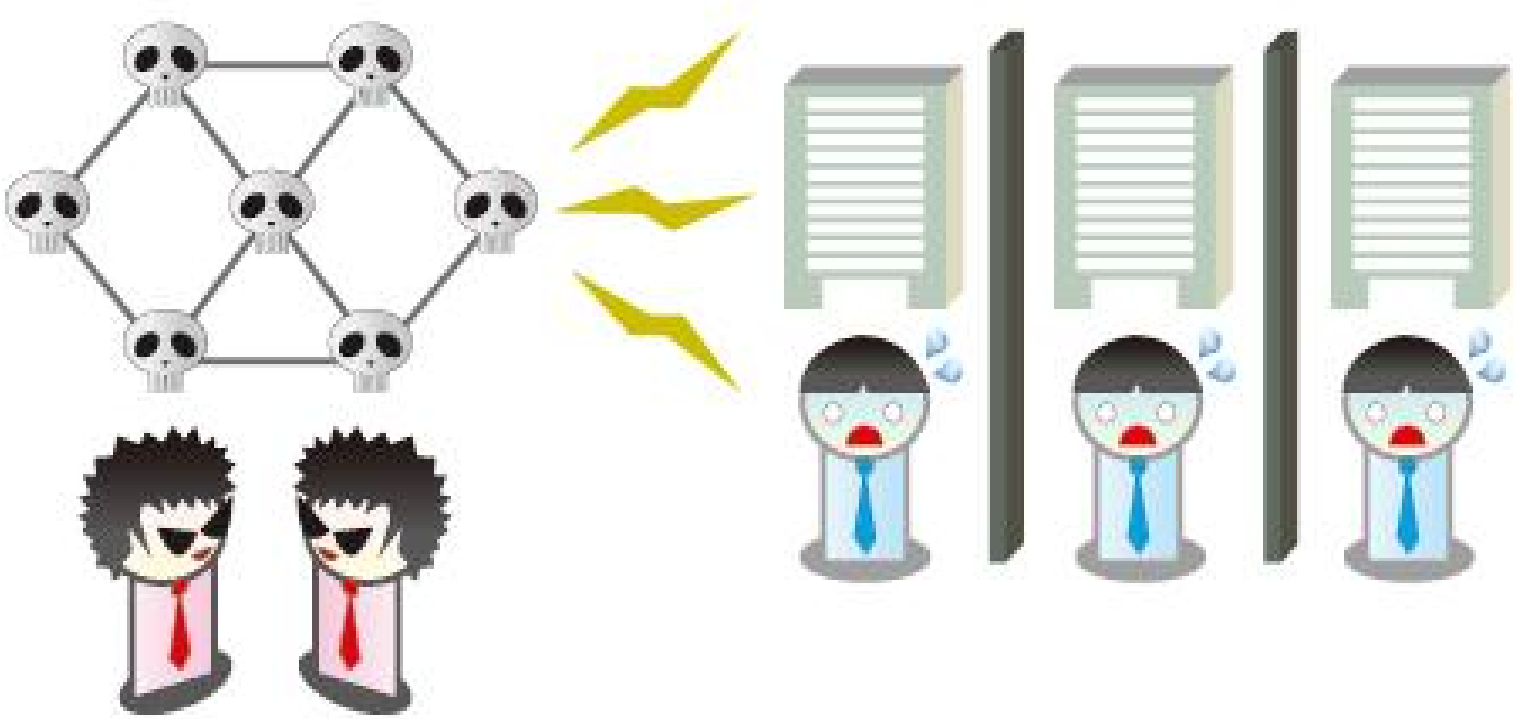
- ITU-T SG17 ñCYBEXòRec. X. 1500
- ISO/IEC 27032

# Cybersecurity information exchange framework (CYBEX)

CJK-SWISS 2011 高橋氏（NICT）資料からの抜粋

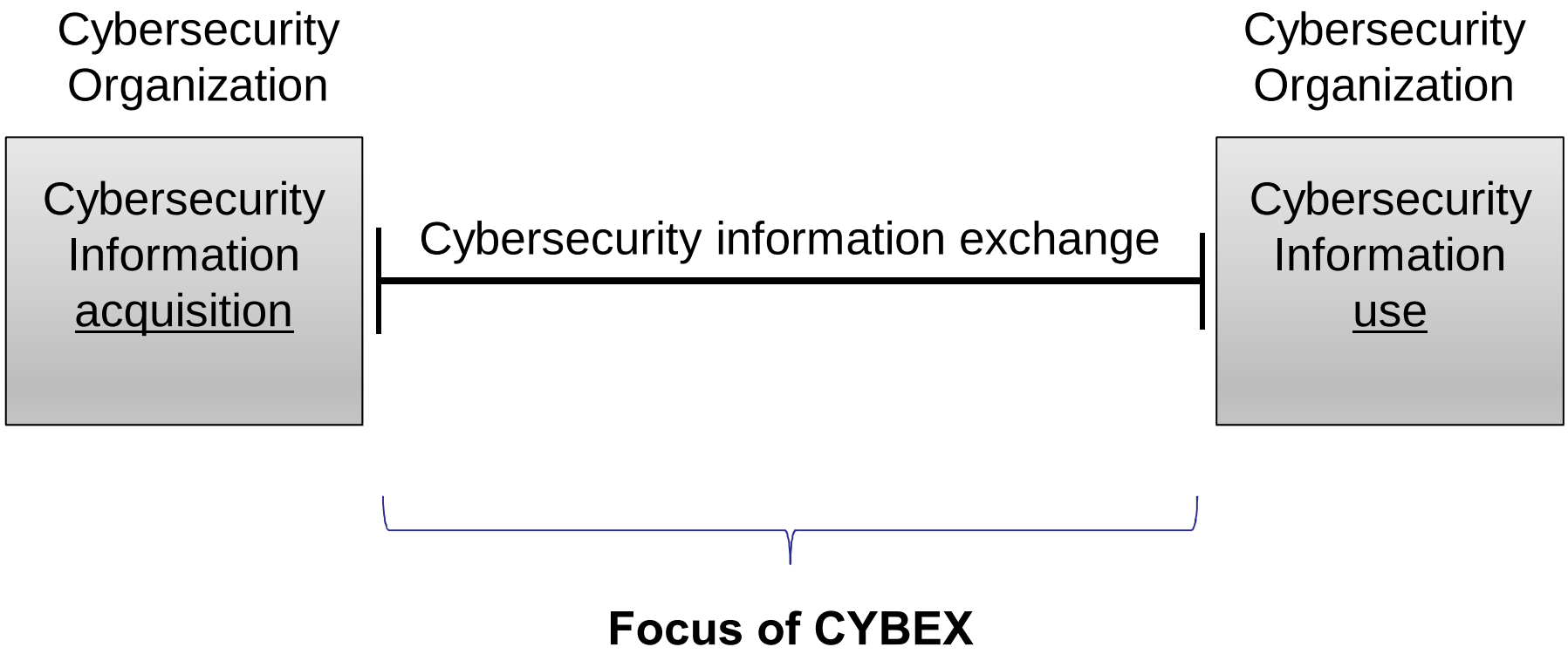
「CYBEX」とは、サイバーセキュリティ情報の交換のための技術的なフレームワークを提供することを目的とする。

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 |

Q.4/17 contributors (alphabetical order)

# X.1500 is developed in Q.4/17

**S. Adegbite (First)**

**I. Furey (DHS)**


**M. Hird (BIS)**


**Y. Kadobayashi (NICT)**

**R. Martin (MITRE)**

**T. Millar (US-CERT)**

**K. Moriarty (EMC)**

**K. Nakao (KDDI)**

**D. Rajnovic (FIRST)**

**G. Reid (Cisco)**


**A. Rutkowski (Yaana)**

**G. Schudel (Cisco)**

**T. Takahashi (NICT)**

**M. Terada (Hitachi)**

**H.Tian (CATR)**


**H. Y. Youm (Soon Chun Hyang uni.)**

# 参考文献


ÅñCYBEX ï the Cybersecurity Information Exchange Framework (X.1500),òACM CCR, http://ccr.sigcomm.org/drupal/?q=node/691, October 2010

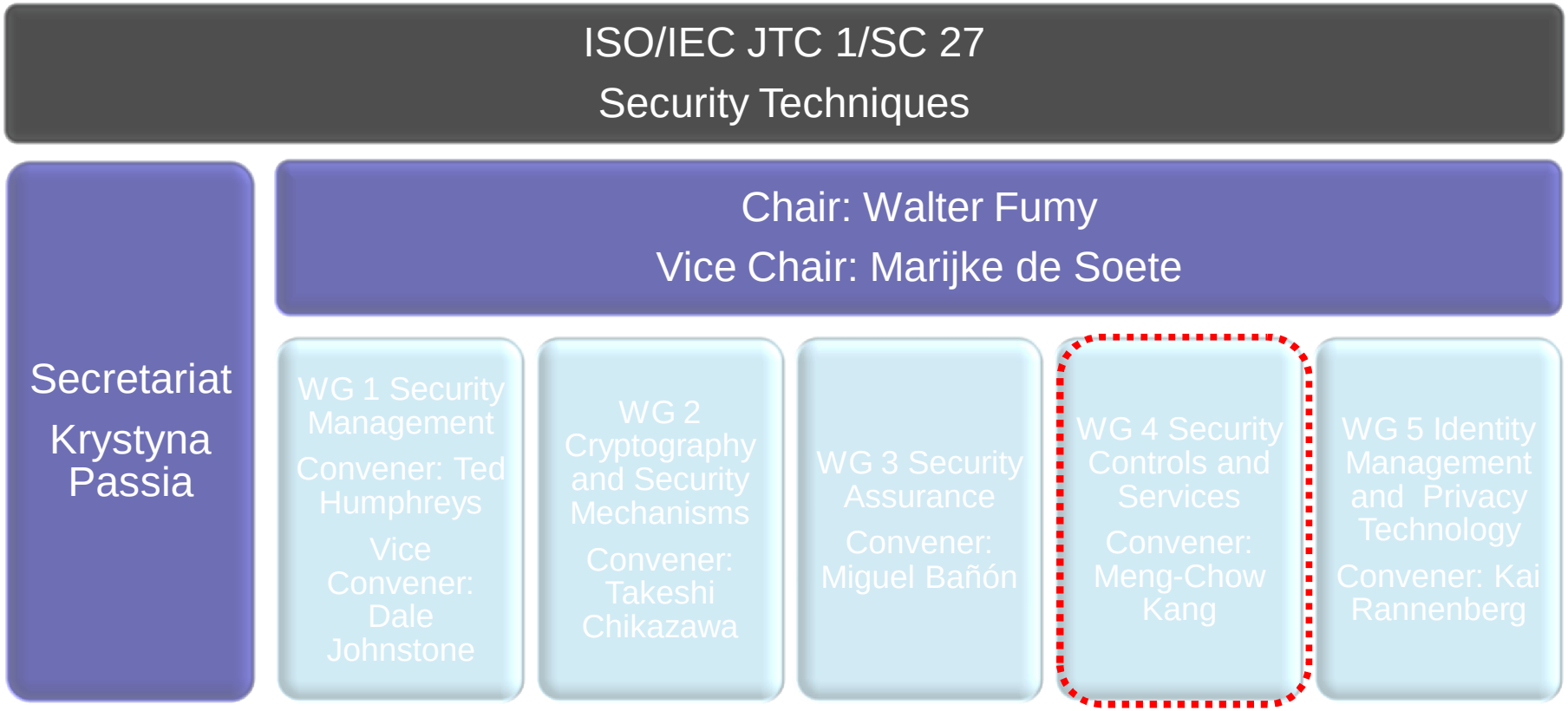
ÅñOntological Approach toward Cybersecurity in Cloud Computing,ò ACM SIN (awarded best paper), September 2010

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

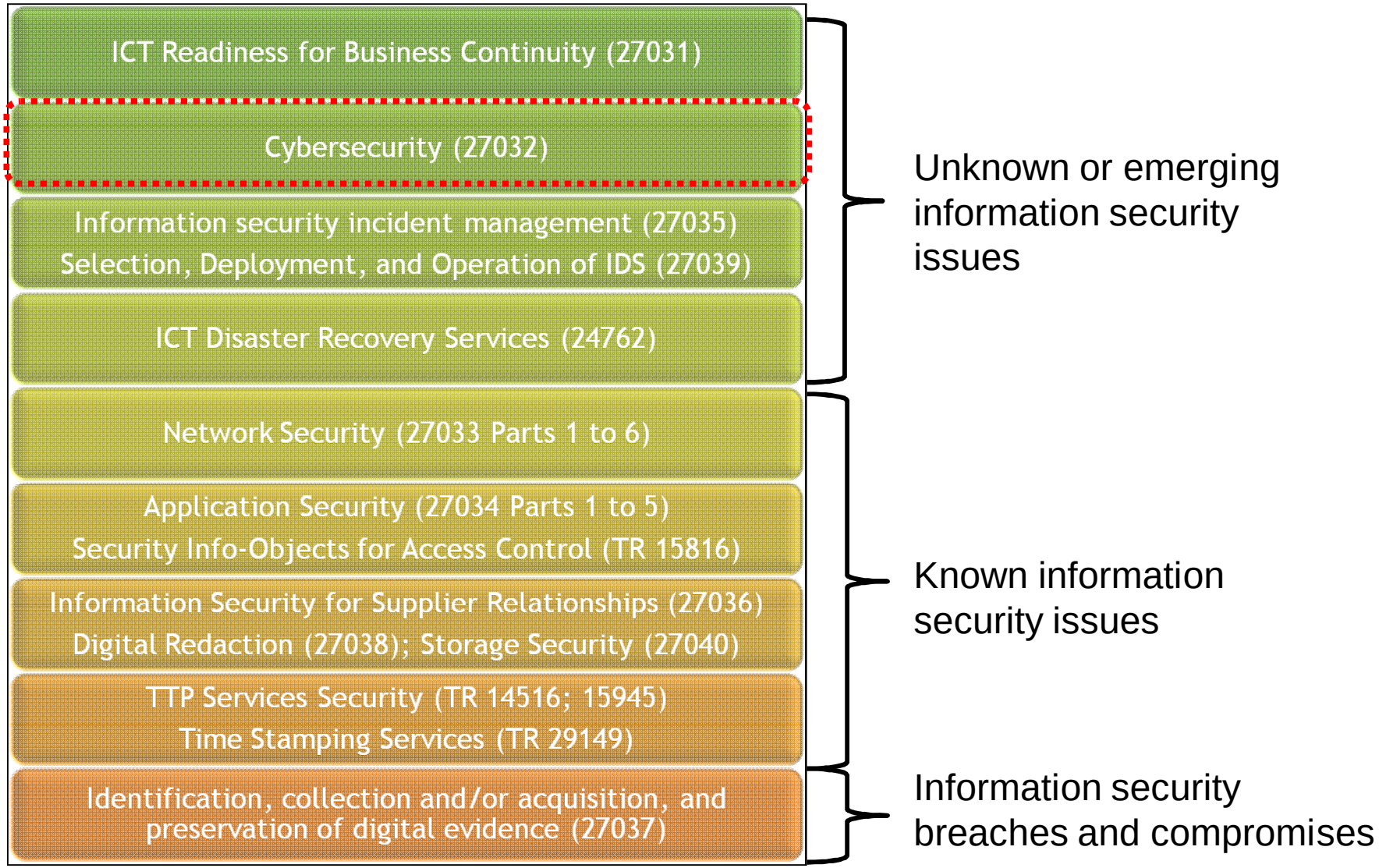
ÅñGlobal Developments in Cybersecurity Information Exchange Frameworkò, invited talk@AINTEC, ACM, November 2010(coming soon)

é etc.

# ISO/IEC JTC 1/SC 27 組織体制



# WG 4 プロジェクト


ICT Readiness for Business Continuity (27031)
Cybersecurity (27032)
Information security incident management (27035)
Selection, Deployment, and Operation of IDS (27039)
ICT Disaster Recovery Services (24762)
Network Security (27033 Parts 1 to 6)
Application Security (27034 Parts 1 to 5)
Security Info-Objects for Access Control (TR 15816)
Information Security for Supplier Relationships (27036)
Digital Redaction (27038); Storage Security (27040)
TTP Services Security (TR 14516; 15945)
Time Stamping Services (TR 29149)
Identification, collection and/or acquisition, and preservation of digital evidence (27037)
Unknown or emerging information security issues
Known information security issues
Information security breaches and compromises

# ISO/IEC 27032 ï Guidelines for Cybersecurity

FDIS

Å サイバー環境（空間）のセキュリティ確保を目的としたベストプラクティスとしたガイドライン。内容としては：

- ï Cybersecurityの概要
- ï Cybersecurity と他セキュリティタイプとの関係整理
- ï Cybersecurityを担うプレイヤーとそれらの役割分担整理
- ï 共通的なCybersecurity における課題
- ï 具体的には、情報共有のフレームワーク。関係するプレイヤー間の連携に注目

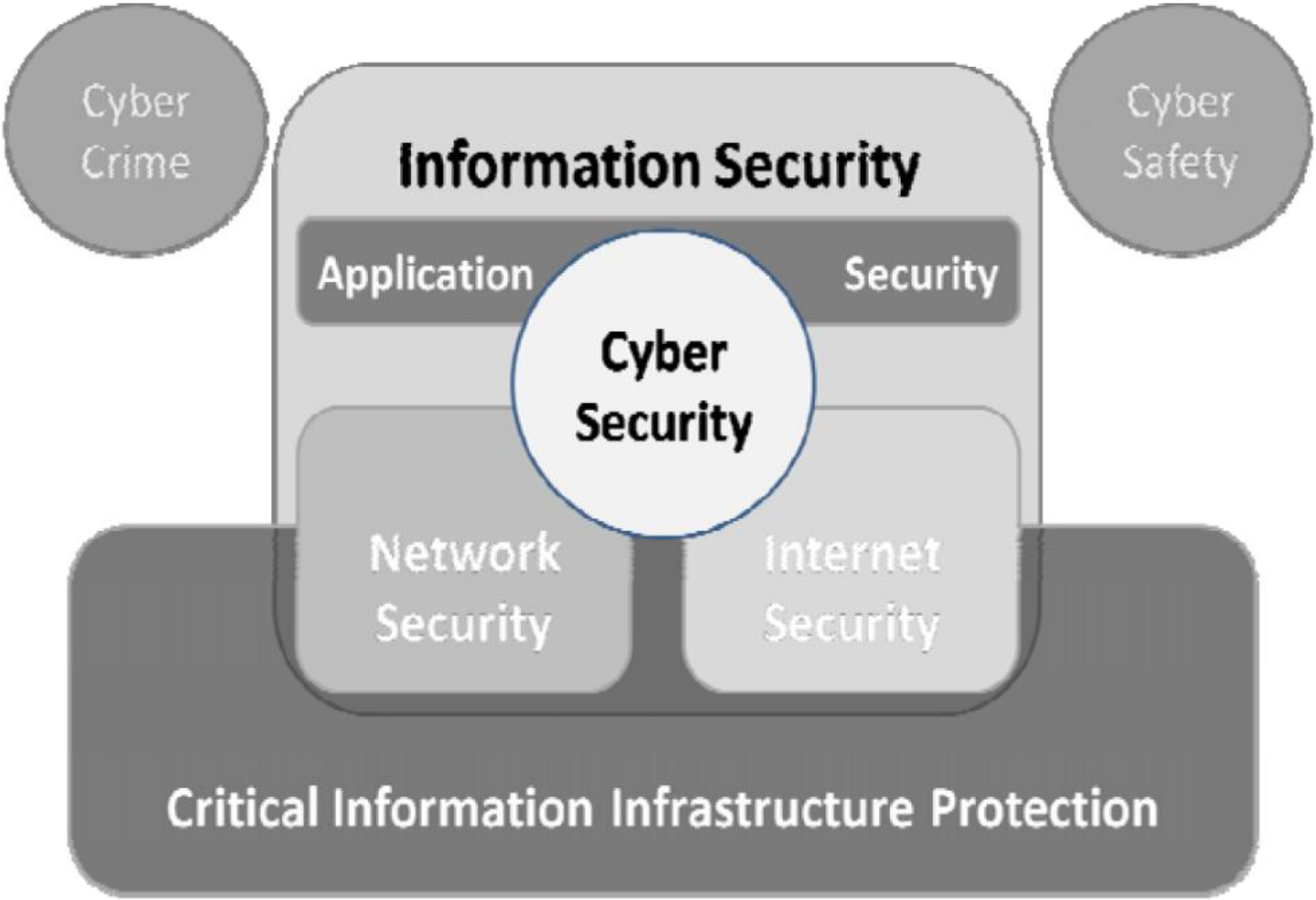



**Figure 1 — Relationship between Cybersecurity and other security domains**

# IPv6セキュリティに関する規格化

- ITU-T SG17 課題2

# 経緯

## 2011年2月に以下を提案

＊IPv6の実装に関わる技術ガイドライン

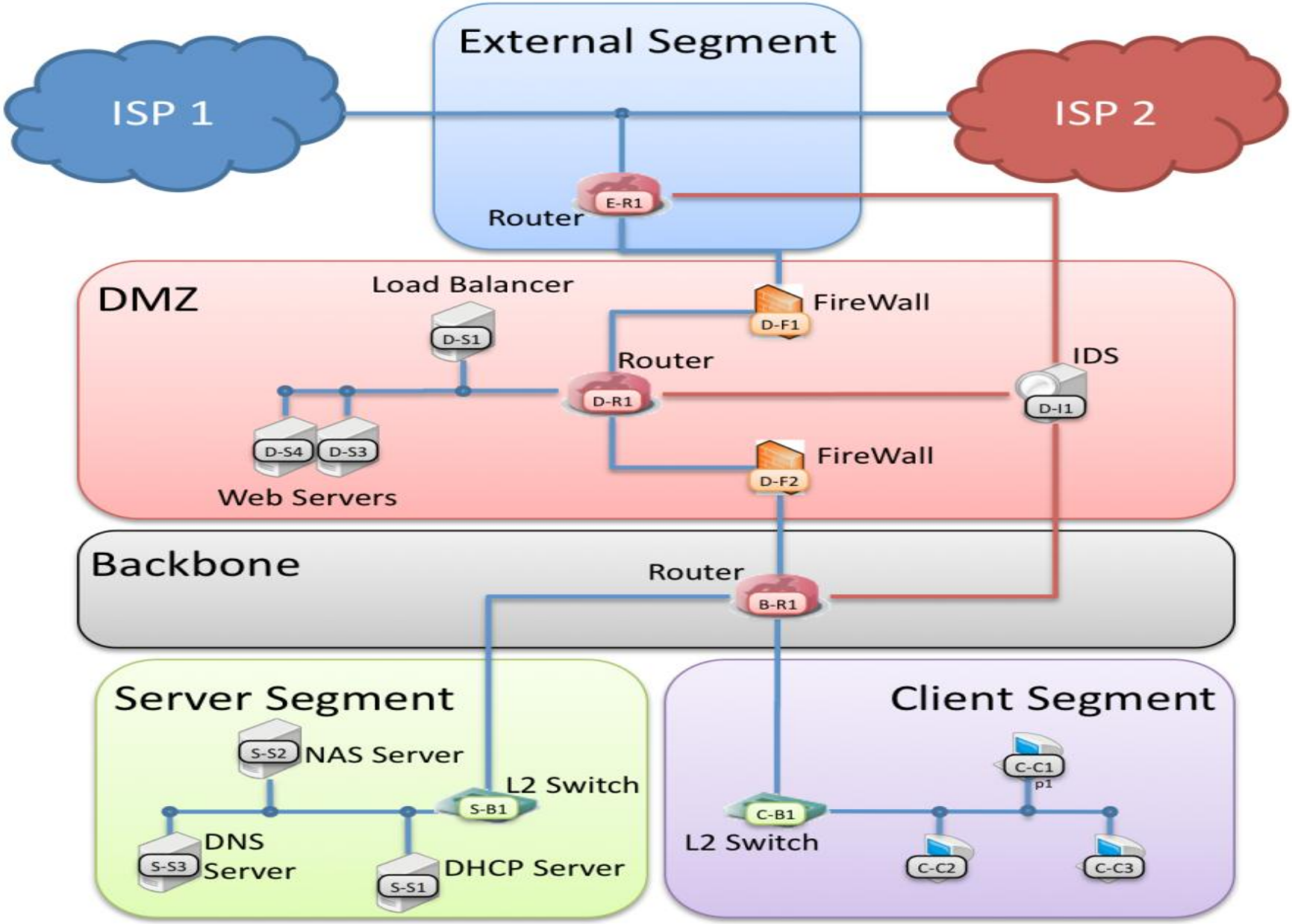
＊ IPv6の実装に関わるマネジメント技術に関わるガイドライン

## 2011年9月

＊ IPv6の実装に関わる技術ガイドライン勧告草案化を推進 （課題2）

＊マネジメント技術に関わるガイドラインについては、上記進捗をみて策定を進める （課題3）

# Figure 6-1 – Topology of IPv6 network



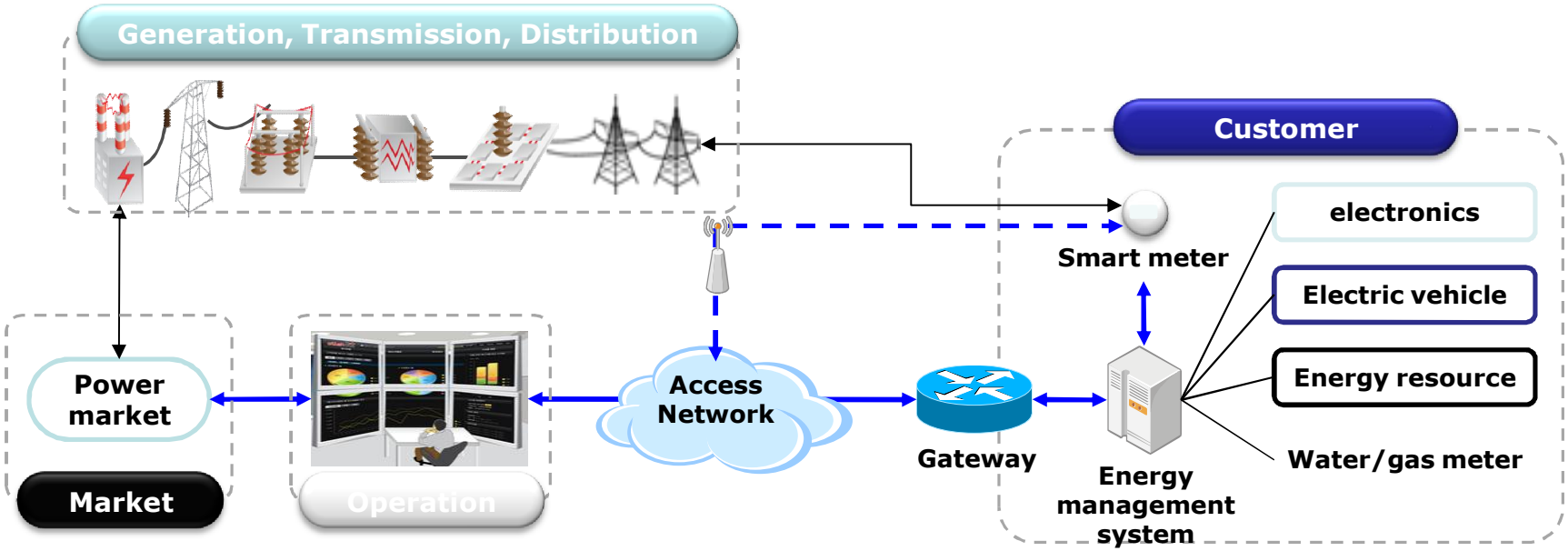
# 現勧告草案目次

# Smart Grid securityに関する規格化

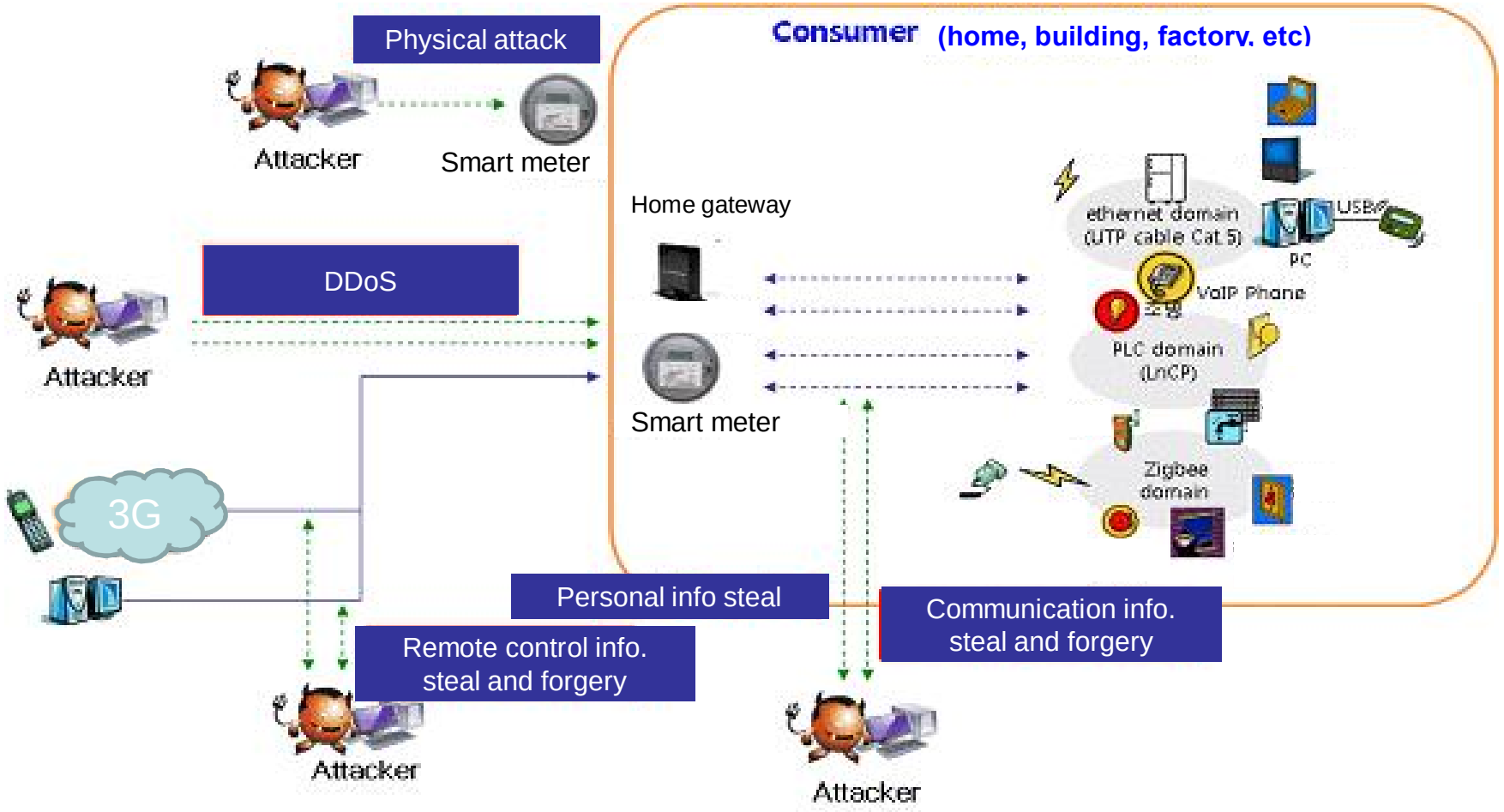
CJK-SWISS 2011 KIM女史　資料から抜粋

# What is Smart Grid?

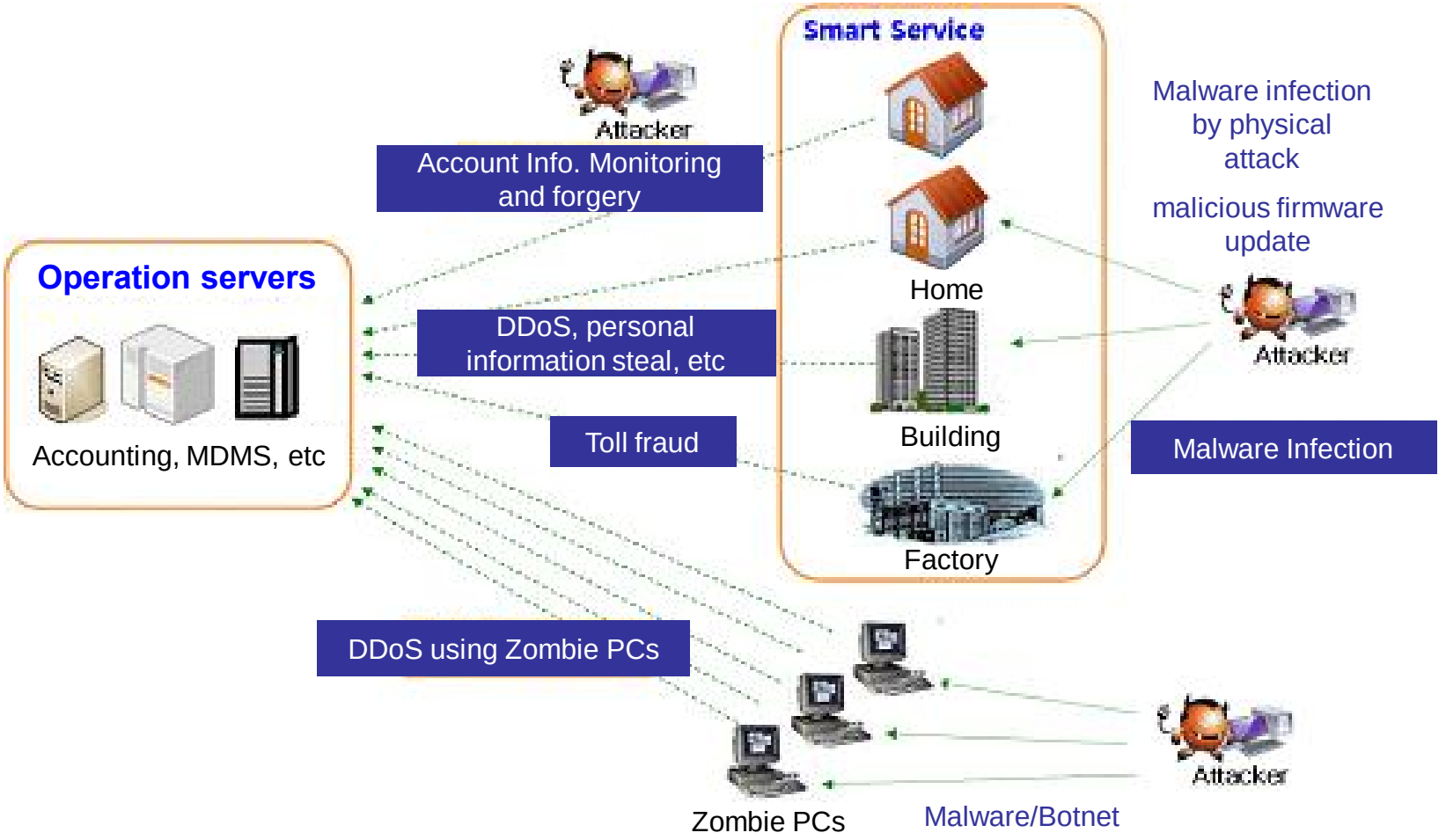
- Smart Grid
  - is an electricity network utilizing ICT technology
  - delivers electricity from suppliers to consumers using two-way digital communications to control appliances at customer's home
  - saves energy, reduces costs and increase service reliability and transparency



# Security threats in Smart Grid environment



# Security threats in Smart Grid environment



# Global Standardization trends on Smart Grid security

- NIST activities
- IEC activities
- ISO/IEC activities
- ITU-T activities
- Other SDOs activities

# NIST activities

- **NIST**
  - SGIP(Smart Grid Interoperability Panel)
  - Cyber Security Working Group
  - August 2010 NIST publishes: Guidelines for Smart Grid Cyber Security
    - Reflects Comments on Sept 2009 and Feb 2010 Draft Smart Grid Cyber Security Strategy and Requirements
  - Guideline includes:
    - Risk assessment guidance for implementers
    - Recommended security requirements
    - Privacy recommendations

# IEC activities

- **IEC TC57** (POWER SYSTEMS management and associated information exchange)
  - IEC 62351 Power systems management and associated information exchange - Data and communications security
- **IEC SG3** (Strategic Group on Smart Grid)
  - Smart Grid Standardization Roadmap is published on June 2010

| Standard | Detail |
|---|---|
| IEC 62351-1 | Introduction to the standard |
| IEC 62351-2 | Glossary of terms |
| IEC 62351-3 | Security for any profiles including TCP/IP |
| IEC 62351-4 | Security for any profiles including Manufacturing Message Specification |
| IEC 62351-5 | Security for any profiles including IEC 60870-5 and derivatives including DNP3 |
| IEC 62351-6 | Security for IEC 61850 profiles |
| IEC 62351-7 | Security through network and system management |

# ISO/IEC activities

- **ISO/IEC JTC1 SWG (Special Working Group) Smart Grid**
  - http://www.jtc1smartgrid.org/
  - ToR(Terms of Reference)
- Identify market requirements & standardization gaps for Smart Grid with particular attention to standards supporting the interoperability of Smart Grid technology and needed I.S.
- Encourage JTC1 SCs to address the need for ISO/IEC SG I.S.
- Promote JTC1 developed I.S.s for SG
- Coordinate JTC1 SG activities with IEC, ISO, ITU-T & other SDOs
- Provide a written report of activities & recommendations

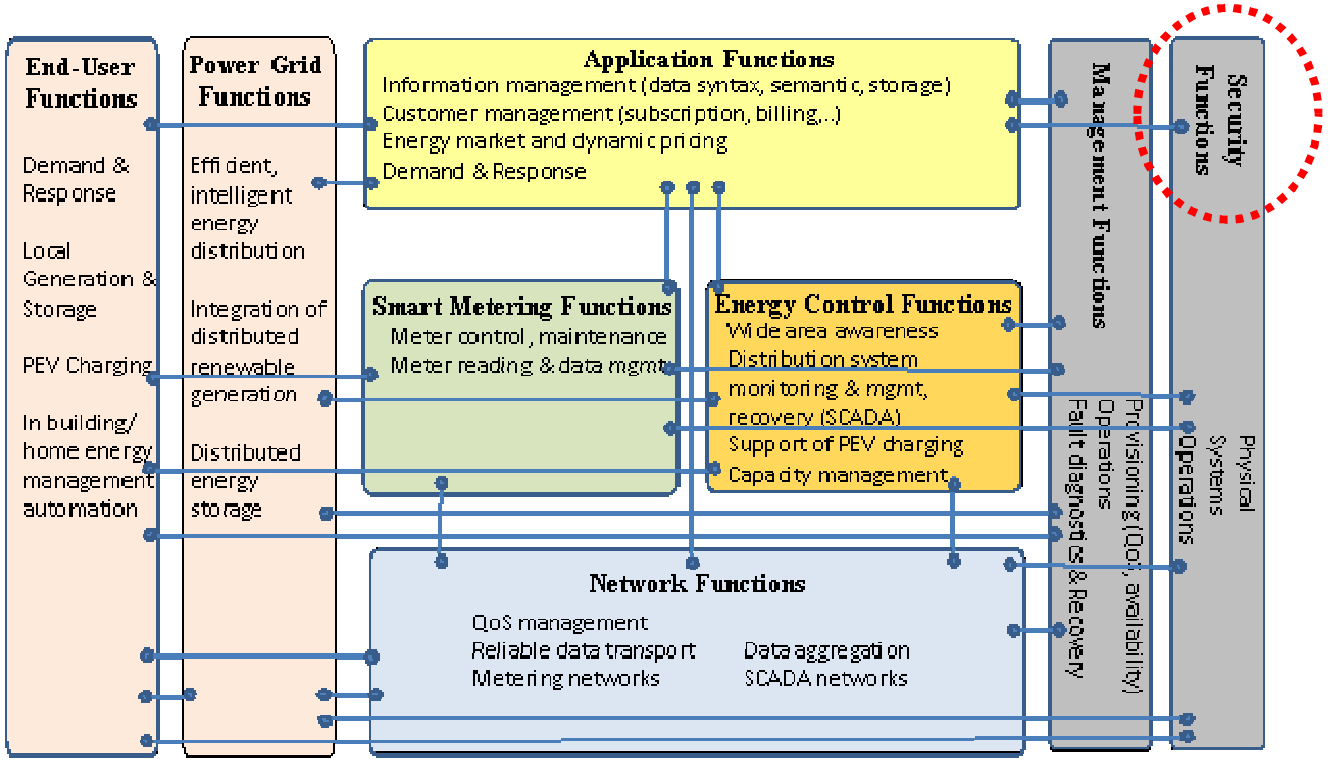
# ITU-T activities

- **ITU-T FG Smart**
  - ITU-T Focus Group on Smart Grid (FG Smart) was established further to ITU-T TSAG agreement at its meeting in Geneva, Jan. 2012
  - Five documents are progressing in FG Smart:
    - Terminology Deliverable
    - Use Case for Smart Grid
    - Smart Grid overview
    - Smart Grid Architecture
    - Deliverable Requirements

スマートグリッドセキュリティに関する検討はほとんど無し

# ITU-T activities

- **ITU-T FG Smart (cont'd)**
  - Smart Grid Architecture (Smart-O-33Rev.5-3)




(source : ITU-T FG Smart Smart-O-33Rev.5-3)

< Simplified Smart Grid Domain Model in ICT Perspective>

# スマートグリッドセキュリティは

- **ITU-T FG Smart Grid**では、TSAGでの審議の結果、SG15（**Transport and Access)**がリードSGとして決定し、必要な連携を行うこととなった。

- SG17（セキュリティ）では、まだ検討提案が提出されたばかりであり、具体的な規格化の作業が進んでいない状況。

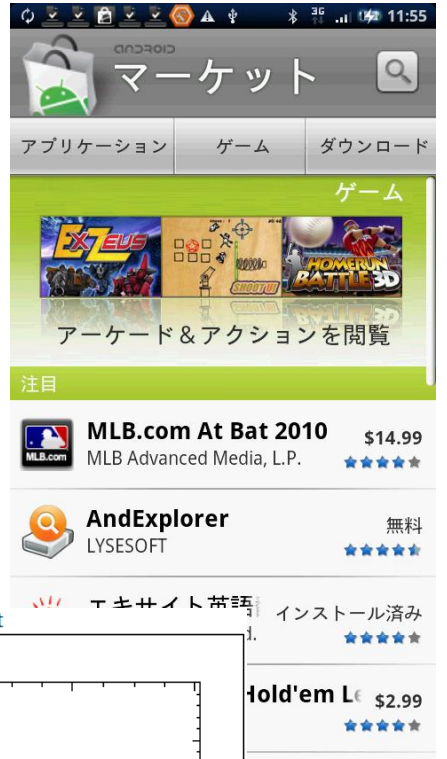
- 前出のように、NIST、IECなどでは、すでに**Smart Grid**に関連するセキュリティを重要事項と認識し、具体的な仕様化、ガイドライン化などを進めている状況。

- 現在、SG17では、本セキュリティに関連し、IEC　SG3との連携が期待されており、日本としても関係者が集結し、今後の方針を決定していく予定。

# スマートフォンの未来を支える
# セキュリティ技術と規格化

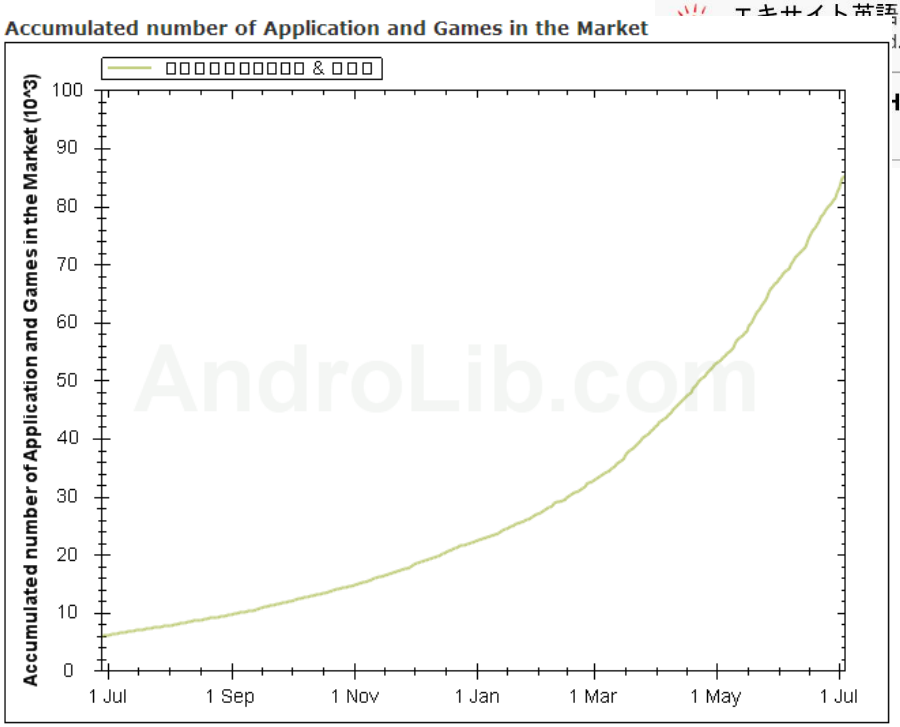
# Android向けアプリケーション

■ Androidの利点
- ◆ 世界中の開発者がアプリケーションを開発・公開している
- ◆ 2011年1月現在 25万以上のアプリケーションがAndroid Marketに公開されている。
- ◆ 端末ユーザは、様々なアプリケーションをダウンロードすることで、高機能化を図る。




■ 問題
- ◆ Android Marketでは、無審査でアプリケーションが公開される。

悪意のアプリケーション（マルウェア）を誤ってインストールしてしまう。




http://jp.androlib.com/appstats.aspx

# 記事

■ 記事のポイント

http://www.itmedia.co.jp/enterprise/articles/1006/24/news019.html

◆ Androidアプリの多くにスパイウェアとしての潜在的な脅威がある。

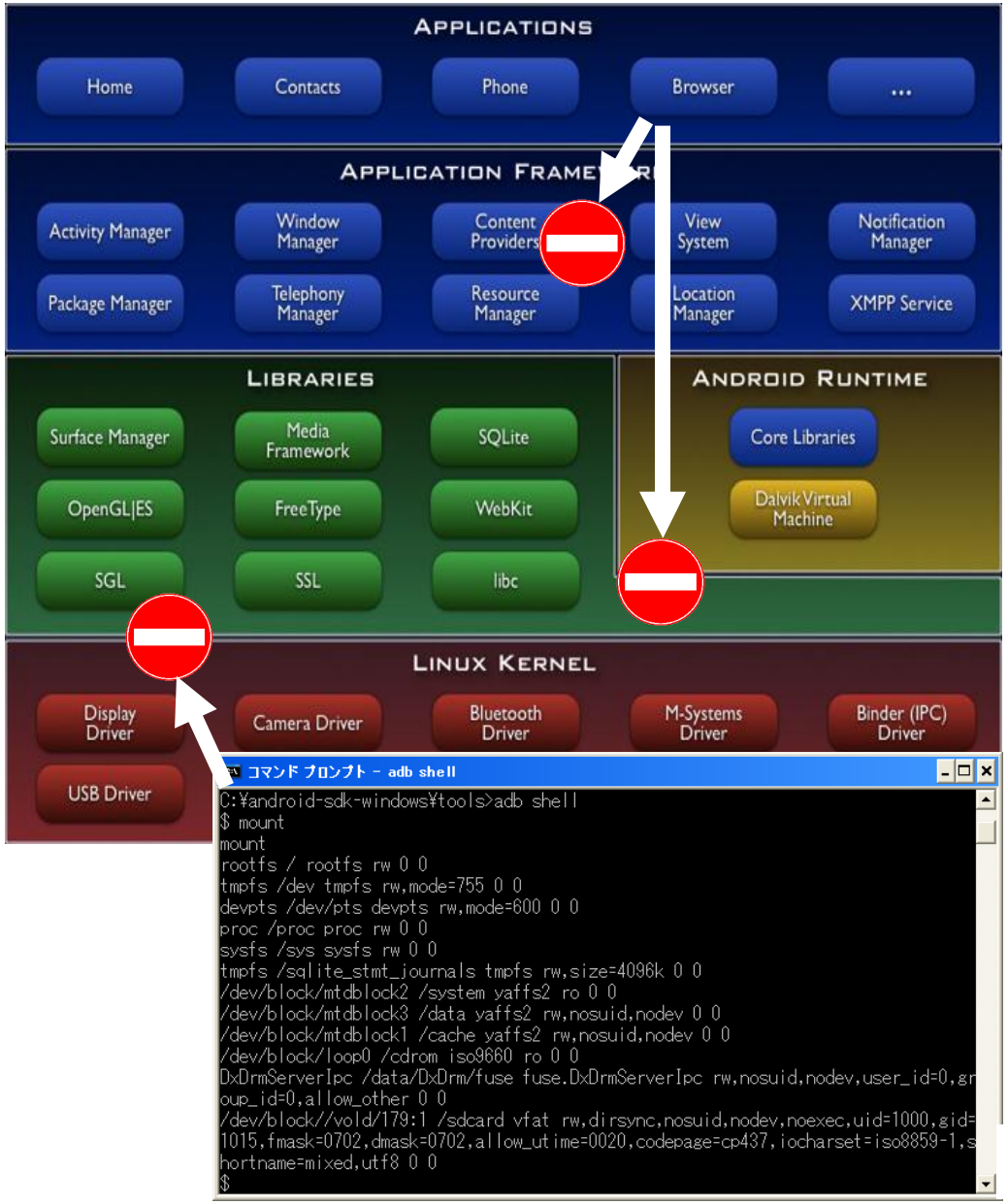
# 記事

■ 記事のポイント

http://jp.wsj.com/IT/node_67792

- ◆ スマートフォン向けアプリの増加に対してセキュリティチェックが追いつかない。
- ◆ 利用者による自浄作用で良いのか？
- ◆ AppStoreは身元検証を行っている。

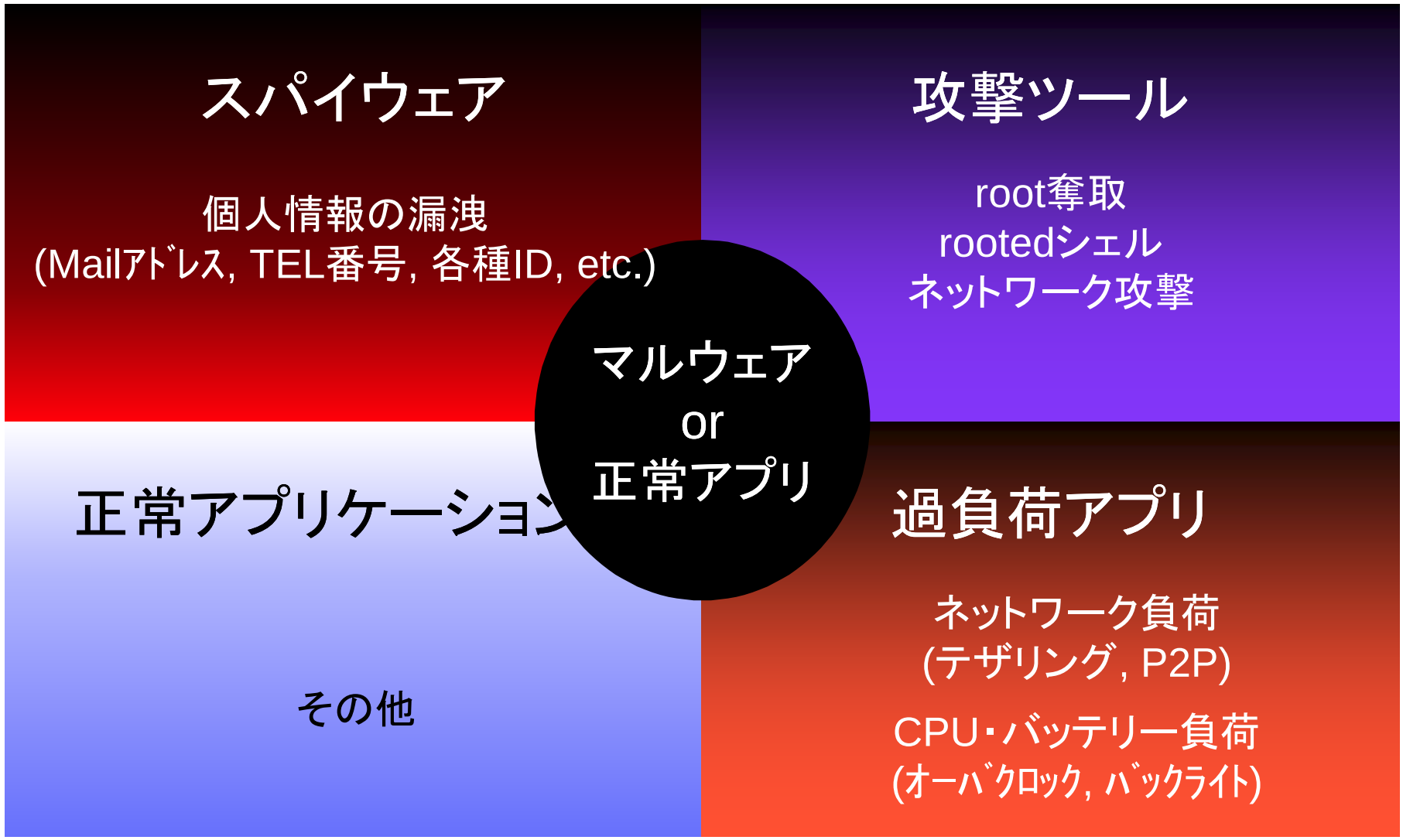
# Androidのセキュリティ・フレームワーク




- アプリケーション間データ連携
  - アプリケーション間の認証をContent Providerで行い、相互にデータ共有される。
- 仮想マシン
  - Dalvik仮想マシンのサンドボックスで、アプリケーションからライブラリ等へのアクセスが制限される。
- カーネル設定（端末／OS）
  - カーネル・ライブラリへのアクセスは、Linuxパーミッション“r/w/xò で保護される。

adb shell via USB

# アプリケーションの分類



# アプリケーション例 ～潜在的スパイウェア～

■ ID取得アプリ
- ◆ Android MarketにはIDを取得するアプリ、IDを外部送信するアプリが販売されている。

■ パーミッション
- ◆ READ_PHONE_STATE、WRITE_EXTERNAL_STORAGE

■ IDの取得方法
- ◆ IDの取得方法

```
TelephonyManager mTelephonyMgr =
                (TelephonyManager)getSystemService(TELEPHONY_SERVICE);
String imei = mTelephonyMgr.getDeviceId(); // Requires READ_PHONE_STATE
String phoneNumber=mTelephonyMgr.getLine1Number(); // Requires READ_PHONE_STATE
String softwareVer = mTelephonyMgr.getDeviceSoftwareVersion(); // Requires READ_PHONE_STATE
String simSerial = mTelephonyMgr.getSimSerialNumber(); // Requires READ_PHONE_STATE
String subscriberId = mTelephonyMgr.getSubscriberId(); // Requires READ_PHONE_STATE
String androidId = android.provider.Settings.System.getString(ctx.getContentResolver(),System.ANDROID_ID); // Requ
```

- ◆ 結果

DeviceId(IMEI) = 359496030831504
DeviceSoftwareVersion = null
Line1Number = 15555218135
SimSerialNumber(ICCID:ICｶｰﾄﾞ識別番号) = 89014103211118510720
SubscriberId(IMSI) = 310995000000000
Android_ID = 200146f5b1374390

# アプリケーション例 ～潜在的スパイウェア～

■ 機能
- ◆ 方位磁石

■ パーミッション
- ◆ ACCESS_FINE_LOCATION、
  ACCESS_COARSE_LOCATION、
  INTERNET、READ_PHONE_STATE

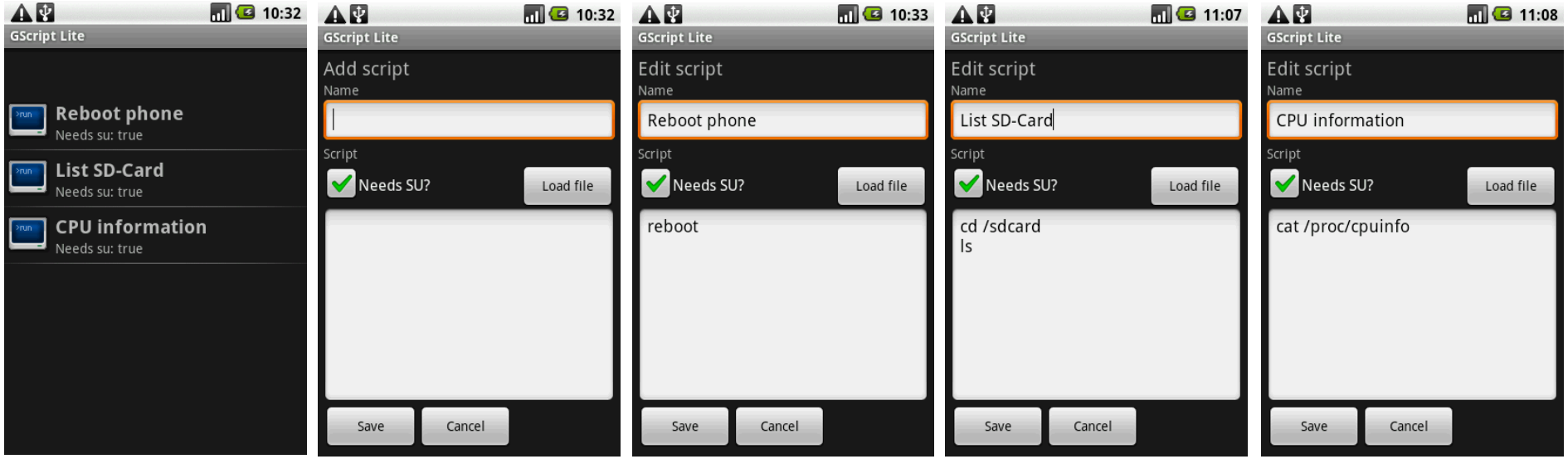
■ 処理中に、
- ◆ http://ad.qwapi.com/adserver/render（広告サイト）へ
  アクセスして、Android ID、位置情報（緯度・経度）を送信した。

⇒ 広告表示の為とはいえ、スパイウェアの要素を持つ。

# アプリケーション例 ～潜在的攻撃ツール～

■ 機能

◆ root権限付きシェル




■ パーミッション

◆ INTERNET、READ_PHONE_STATE、ACCESS_COARSE_LOCATION

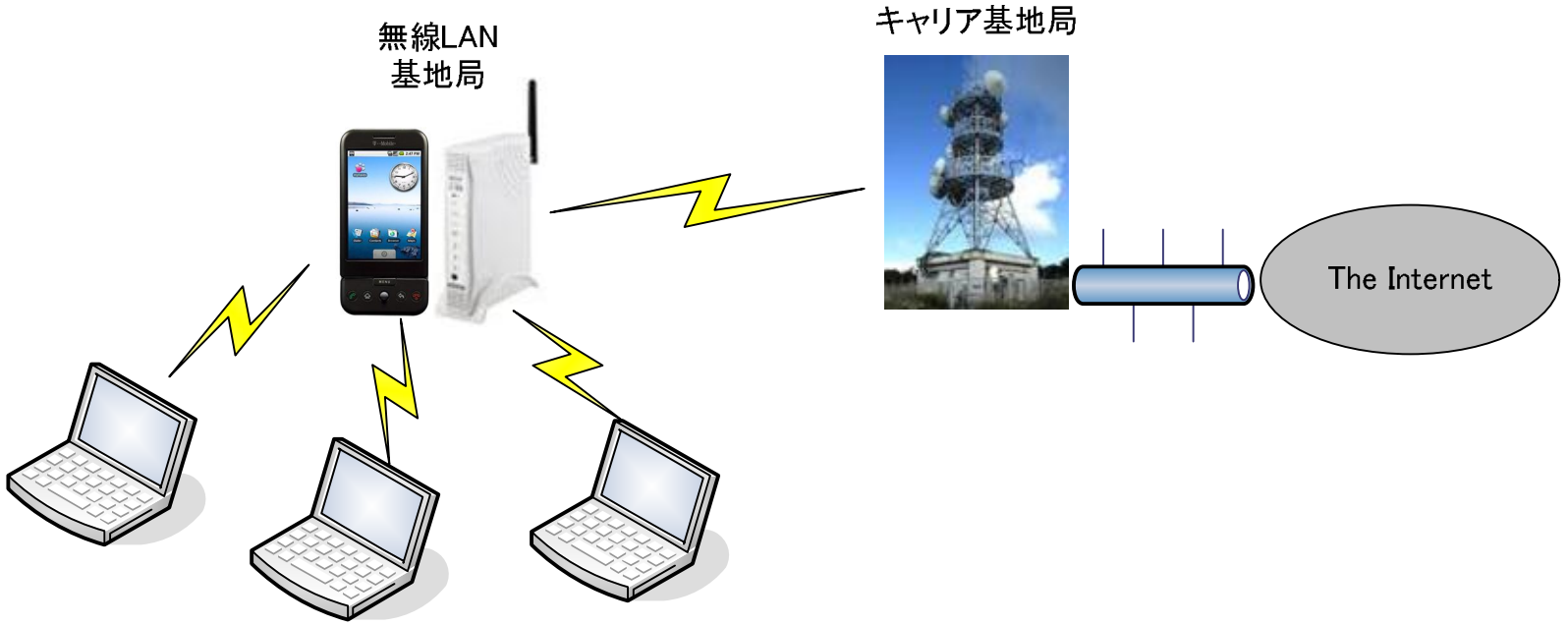
■ 処理中に、

◆ Android IDを作成者サイトへ送信した。

⇒ root権限利用とスパイウェアの要素を持つ。

# アプリケーション例 ～過負荷アプリ～

■ WiFIテザリングアプリ
- ◆ PCをインターネット接続する際に、通信キャリアのモデムとなるもの。
- ◆ スマートフォンが無線LANルータとになり、さらに通信キャリアの基地局に繋がる。




■ 過負荷
- ◆ WiFiと3Gの電波を使うため、電池消費が早い。
- ◆ 多量のパケットが通信キャリアの無線回線に流れ込む。

# まとめ

■ スマートフォン（Android）の特徴
- ◆ 高機能な端末H/W、PCベースのOSで構成される携帯電話である。
- ◆ 便利なアプリケーションを、誰もが自由に作成・公開できる。
- ◆ ユーザは、アプリケーションの潜在脅威を参考に、インストールを判断する。

■ 問題の把握
- ◆ 端末H/WとOSの脆弱性は、PCモデルと同じ。⇒既存のセキュリティ技術
- ◆ 個人に結びつきの強い携帯端末上のアプリケーションへの脅威が問題である。

■ 未来を支えるセキュリティ技術
- ◆ 多種多様なアプリケーションの安全性を高める技術が必要とされる。

# 今後の対策と規格化への方向

- 潜在脅威の表示
  - アプリケーションのインストール前に、パーミッションの概要を表示して、ユーザ承認（ユーザ責任）を求める。

- 問題点
  - 概要しか説明していない。
  - 既存の携帯電話ユーザには理解不能é 。

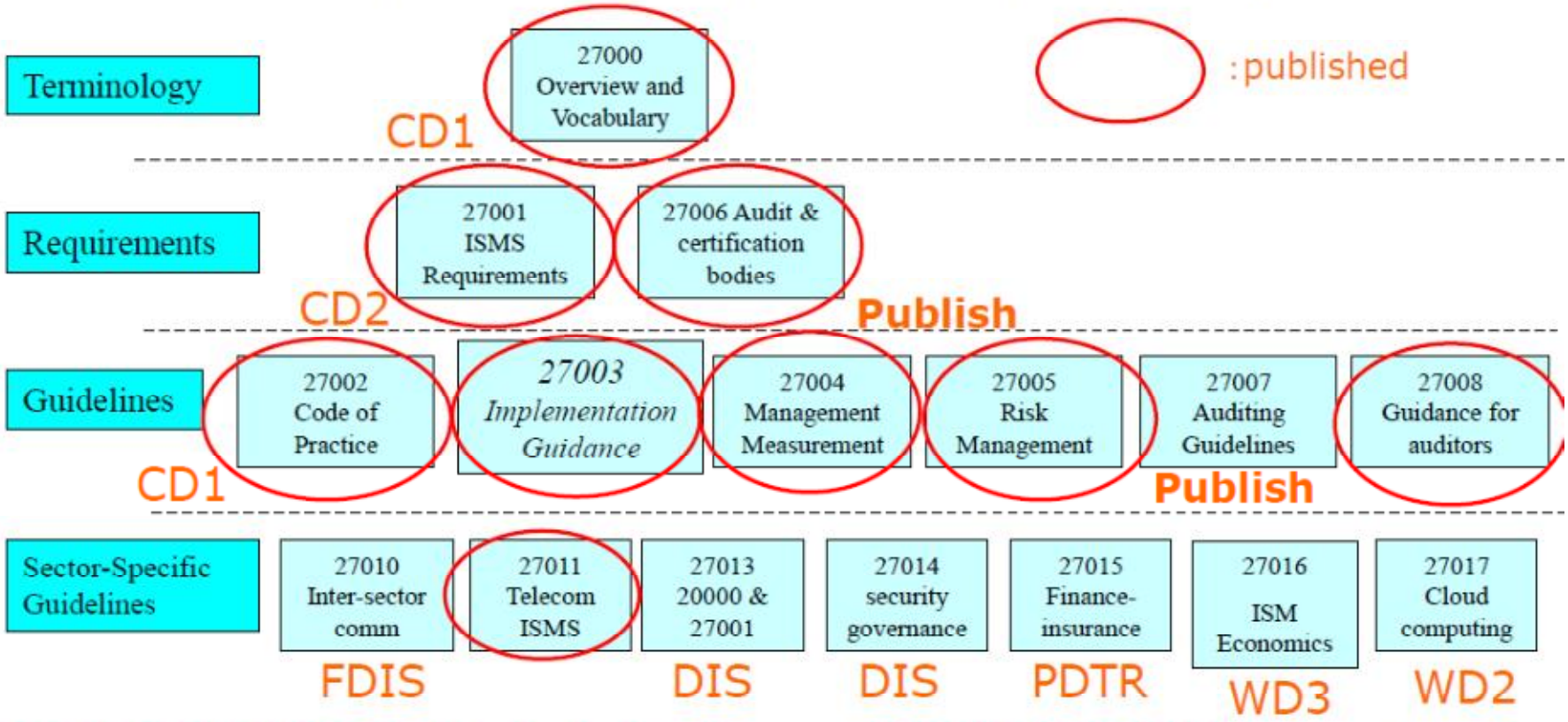
- スマートフォンの未来を支えるために
  - アプリケーションの脅威に関するユーザ教育
  - アプリケーション開発者向けの作成ガイドライン

- スマートフォンの規格化について
  - アプリケーション開発者向けガイドラインのITU－T勧告化の推進（2012年2月会合に提案）
  - ユーザ教育の一環として、ユーザガイドの規格化も考慮すべき。

# ISMS関連の規格化状況（概要）

# ISO/IEC27000 ISMS family of standards
## (WG1の規格：defined in ISO/IEC27000) at Nairobi

### *ISMS family of standards Relationships*




**ISO/IEC27000 ISMS family of standards support ISO/IEC27001, ISMS Requirements.**

# SC27/WG1における標準化文書リスト(1)

at Nairobi

| Standard | Title | Status |
|---|---|---|
| 27000 | Overview and vocabulary | Published – now revised, CD1 |
| 27001 | ISMS requirements | Published – now revised, CD2 |
| 27002 | Code of practice for information security controls | Published – now revised, CD1 |
| 27003 | ISMS Implementation guidance | Published 2010/02/01 |
| 27004 | ISM - Measurement | Published 2009/12/15 |
| 27005 | Information security risk management | Published 2011/06/01 |
| 27006 | Requirements for bodies providing audit and certification of ISMS | Published Revised, Publish |
| 27007 | Guidelines for ISMS auditing | Revised, Publish |
| 27008 | Guidance for auditors on Information security controls | Published 2011/10/15 |

# 27001　新構造(1)

ISO 31000に準拠

1 Scope
2 Normative references
3 Terms and definitions
4 Context of the organization
- 4.1 Understanding the organization and its context
- 4.2 Understanding the needs and expectations of interested parties
- 4.3 Determining the scope of the management system
- 4.4 Information security management system

5 Leadership
- 5.1 General
- 5.2 Management commitment
- 5.3 Policy
- 5.4 Organizational roles, responsibilities and authorities

# 27001　新構造(2)

6　Planning

- 6.1　Actions to address risks and opportunities
- 6.2　Information Security objectives and plans to achieve them

7　Support

7.1　Resources

7.2　Competence

7.3　Awareness

7.4　Communication

7.5　Documented information

- 7.5.1　General
- 7.5.2　Create and update
- 7.5.3　Control of documented information

# 27001 新構造 (3)

**8 Operation**

- **8.1 Operational planning and control**
- **8.2 Information security risk assessment**
- **8.3 Information security risk treatment**

9 Performance Evaluation

- 9.1 Monitoring, measurement, analysis and evaluation
- 9.2 Internal Audit
- 9.3 Management review

10 Improvement

- 10.1 Nonconformity and corrective action
- 10.2 Continual improvement

# SC27/WG1における標準化文書リスト(2)

at Nairobi

| Standard | Title | Status |
|---|---|---|
| 27010 | Sector to sector interworking and communications for industry and government<br>変更案： Information security management for inter-sector and inter-organisational communications | FDIS |
| 27011 | Information security management guidelines for telecommunications based on ISO/IEC 27002 | Published 2008/12/15 |
| 27012 | ISMS guidelines for e-government | cancelled |
| 27013 | Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 | DIS |
| 27014 | Governance of Information security | DIS |
| 27015 | Information security management guidelines for financial services | PDTR |
| 27016 | Information Security Management - Organisational economics | WD3 |

# SC27/WG1における標準化文書リスト(3)

at Nairobi

| Standard | Title | Status |
|---|---|---|
| 27017 | Guidelines on Information security controls for the use of cloud computing services based on ISO/IEC 27002 | WD2 |
| PIMS | Personal Information Management System | Study period |
| Roadmap | WG1 SD1 Road Map | SD |

# 最後に

1）多くの情報セキュリティ、サイバーセキュリティに関連するトピックが増加している。例えば、クラウド、スマートグリッド、プライバシー管理、情報交換、国際連携などが話題に上る。

2）国際標準化の視点からすると、ガイドライン化、MS (Management System)化などの規格化を実施することにより、よりセキュリティ確保に有効であり、効果的なものがある。 また、標準的な交換フレームワークや体系を整備することにより、国際連携に貢献できるものもある。
国際標準化がひとつの手段となって、よりセキュリティ向上に貢献できる。

3）上記のような環境にあるため、多くの標準化団体（SDO）が似たような標準を競い合って検討している。しかしながら、標準化のリソースには限度があり、その有効活用、及び不必要な標準化作業の重複作業は逆にマイナスとなる。SDO間の連携を十分に考慮した、効率的な標準化作業が望まれる。

4）日本目線で言うと、以下の項目については、国際標準化を有効に活用するよう、規格策定の段階からメンバとして活動することが重要と考える。

- クラウドセキュリティ
- サイバーセキュリティ技術（CYBEX主体として）
- セキュリティ監査技術（クラウドやサプライチェーンにおいても）
- スマートフォン/スマートグリッドセキュリティ
- IPv6セキュリティ
- MtoMセキュリティ（ETSIで活発に検討されている）

などなど

# Thank you for listening Q&A