情報セキュリティの国際標準の先に見えるもの
－国際戦略･国際連携－

KDDI株式会社
中尾康二

本日の内容

1) 国際標準化の意義と標準化活動の全貌

2) ISO/IEC JTC1/SC27の活動

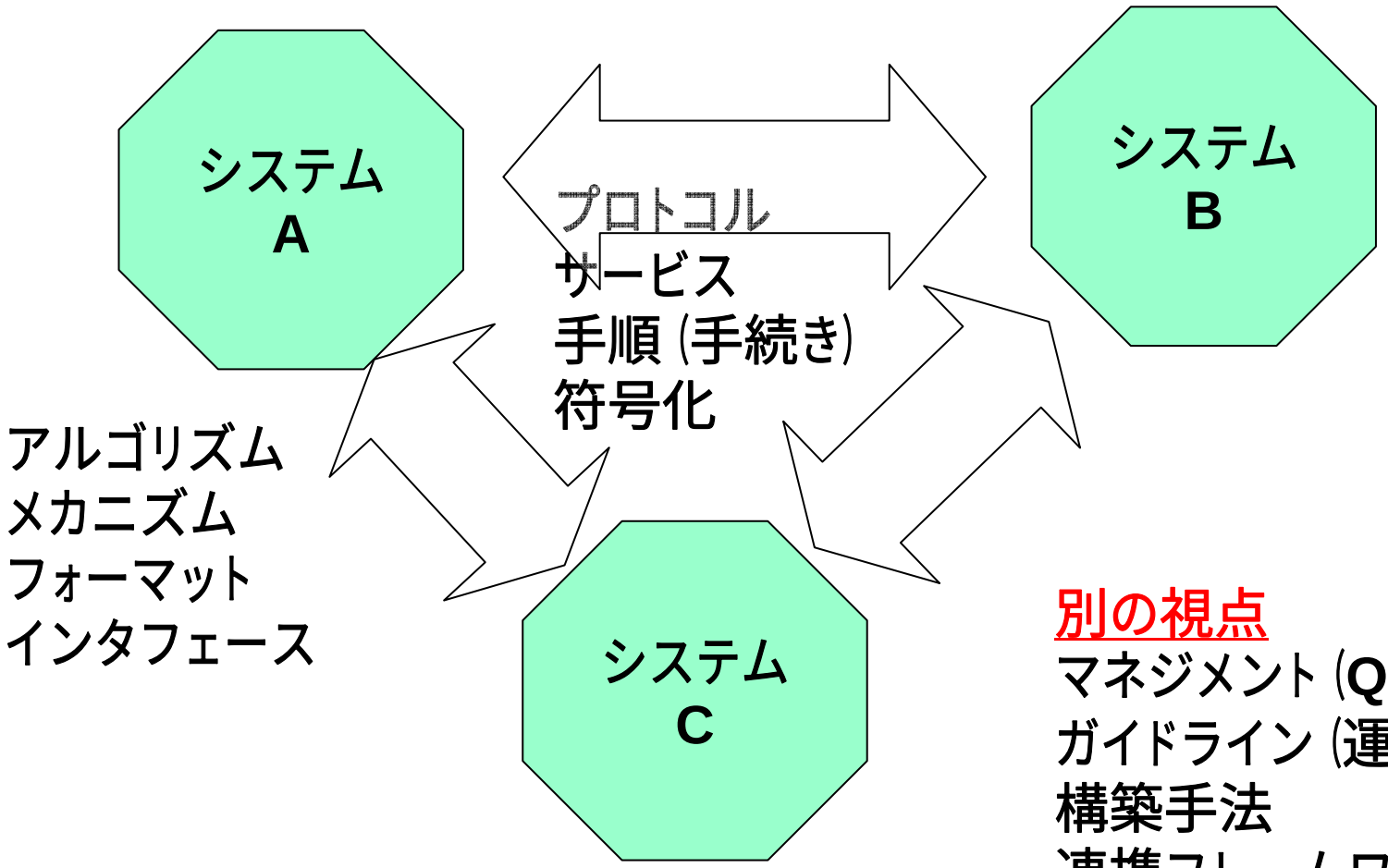
3) ITU-T　SG17の活動

4) その他の活動

5) 今後の国際規格化、国際連携への取り組み
- 現状の把握
- 今後

国際標準化の意義と標準化活動の全貌

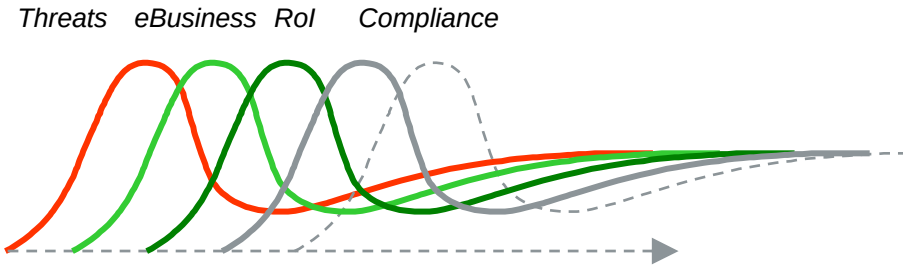
標準化の意義とトレンド



別の視点

マネジメント (QMS等)
ガイドライン (運用など)
構築手法
連携フレームワーク
解説

標準化 – *投資へのリターン*



–協力することの利点

- ⇨ **リスクの低減**
- ⇨ **ビジネス実施のコスト削減**
- ⇨ **より良いビジネス機会を通した投資へのリターン**
- ⇨ **コンプライアンス環境の構築･維持を支える役割**

–経済的な効果

- ⇨ The economic benefits of standardization are estimated to account for around 1% of gross domestic product (GDP)*. **ドイツの例**
- ⇨ The economic benefits of standardization are estimated to account for around 16 billion € per year for Germany**. **ドイツの場合**
- ⇨ **日本はどうでしょう**

*) result of a joint study carried out by the German, Austrian and Swiss associations for standardization.

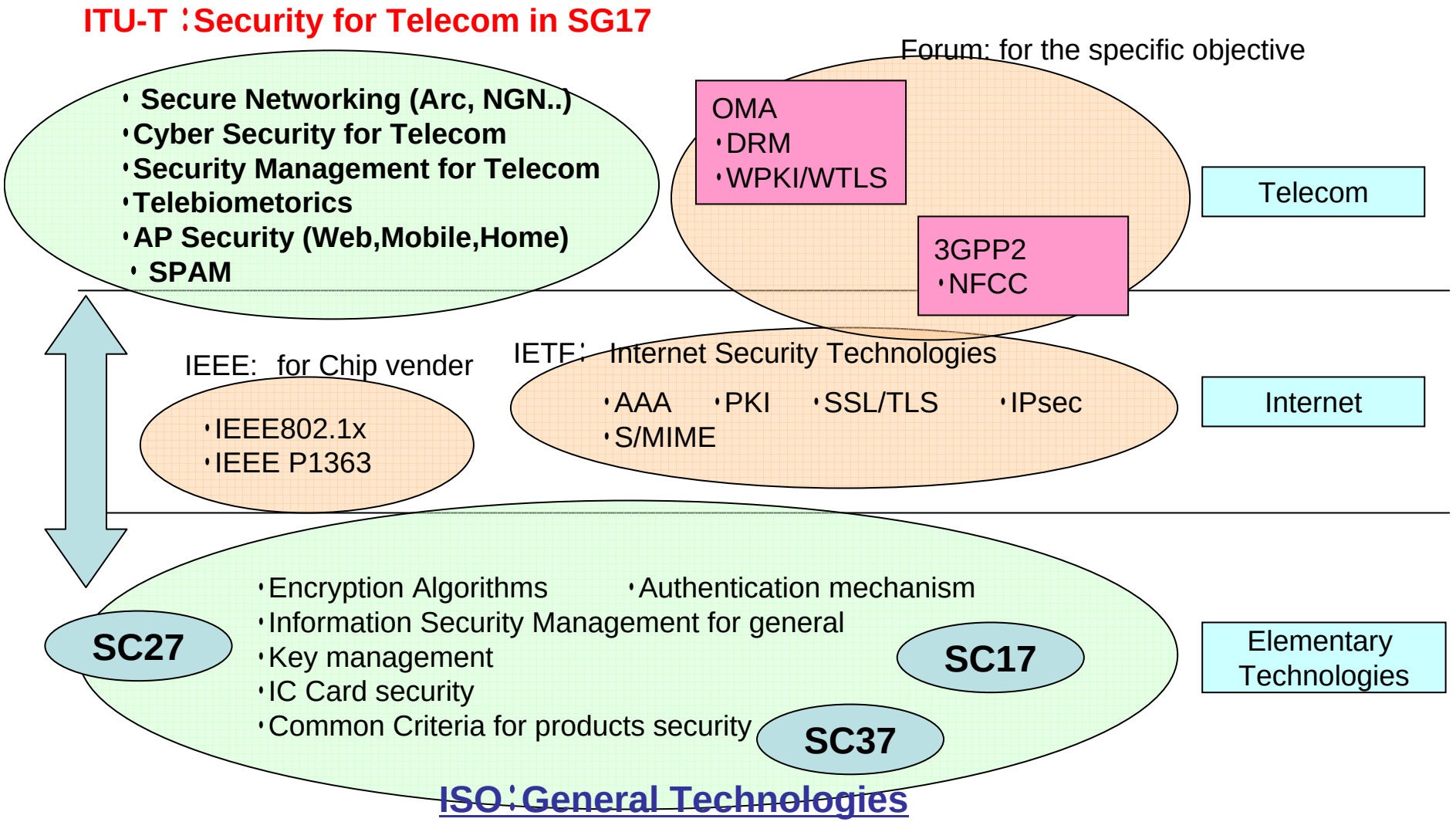
**) result of a study carried out by TU Dresden.

セキュリティ標準化における主役

- **International standards bodies** (e.g., **ISO, ITU-T**, ETSI) have formal processes
  - Procedures and processes take time
  - Progress in streamlining the time for standards approvals
- **IETF** processes are less formal
  - Number of participants, transparency of the processes have sometimes slowed the work
- **Industry groups and consortia** focus on specific technologies and applications
  - Focus has allowed work products to be produced rapidly, although limited in scope
  - Maintenance?

⇨ **結局、それぞれの団体･組織の役割があり、それに沿ったセキュリティの規格化を推進している。**

各標準化機関の相関

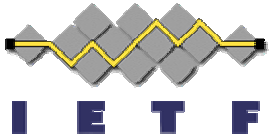

ITU-T：Security for Telecom in SG17
・Secure Networking (Arc, NGN..)
・Cyber Security for Telecom
・Security Management for Telecom
・Telebiometorics
・AP Security (Web,Mobile,Home)
・SPAM
Forum: for the specific objective
OMA
・DRM
・WPKI/WTLS
3GPP2
・NFCC
Telecom
IEEE: for Chip vender
・IEEE802.1x
・IEEE P1363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

暗号化技術の規格における主役

- **ISO/IEC JTC 1/SC 27**: Information technology - Security techniques
  - Standardization of generic IT security services and techniques
- **ETSI SAGE**: Security Experts Group
  - Creates reports (which may contain confidential specifications) in the area of cryptographic algorithms and protocols specific to public/private telecommunications networks
- **IEEE P1363**: Standard Specifications for Public-Key Cryptography
- **NIST**: National Institute of Standards and Technology
  - Issues standards and guidelines as Federal Information Processing Standards (FIPS) for use by the US government
- **ANSI X9F**: Data & Information Security
  - Standards for the financial services industry

セキュリティプロトコル・サービス規格化の主役

- **IETF**: Internet Engineering Task Force
  - IP Security Protocol, Transport Layer Security, Public-Key Infrastructure (X.509), S/MIME Mail Security,...

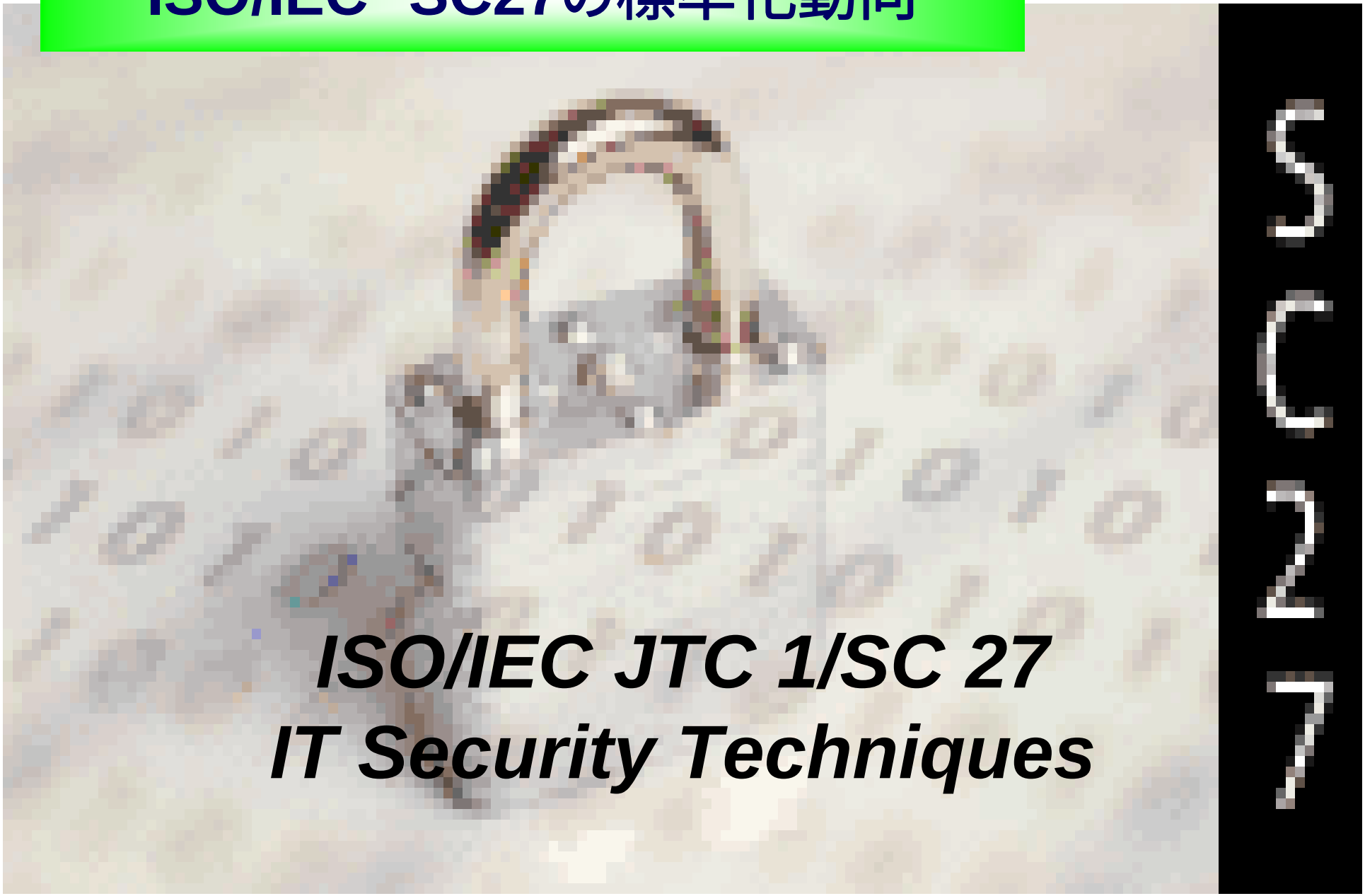


- **ITU-T**: International Telecommunication Union
  - X.509 (Public-key certificates), H.235 (Security and encryption for H-Series multimedia terminals), X.841, X.842, X.843, ...

- **ETSI**
  - GSM, 3GPP, TETRA, TIPHON, SPAN, TISPAN, ...

- **IEEE 802.11**: (Wireless) LANs
  - 802.11i, 802.1X, ...

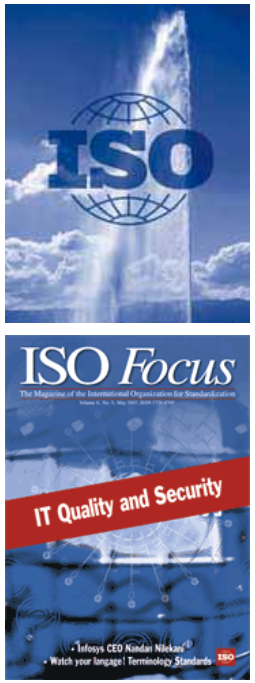
ISO/IEC　SC27の標準化動向



ISO/IEC JTC 1/SC 27
IT Security Techniques

JTC1 SC27

ISO – International Organization for Standardization



- Worldwide federation of national standards bodies from 157 countries, one from each country, e.g.,
  - JISC - Japanese Industrial Standards Committee (www.jisc.go.jp)
- ISO was established in 1947 (www.iso.org)

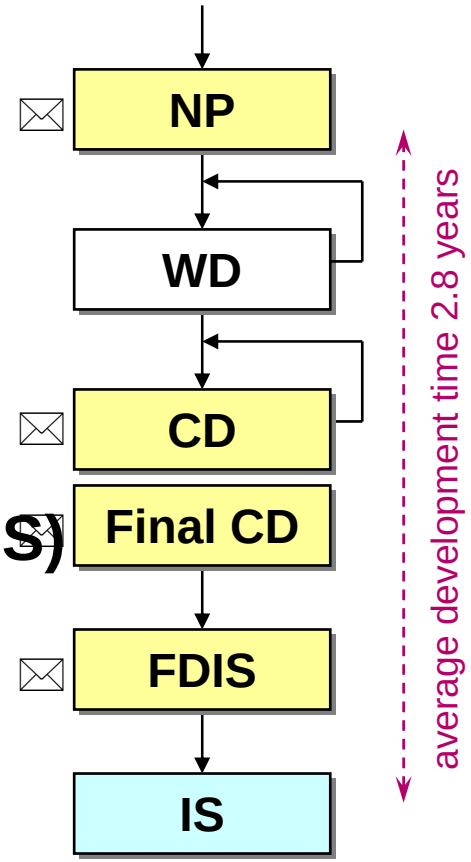
- 3.093 technical bodies
  - 201 technical committees (TCs)
  - 542 subcommittees (SCs)
  - 2.287 working groups (WGs)

- ISO**では、国際的な合意の下に、国際規格**(IS)**の作成、発行を行っている。**
  - 17.041 standards and standards-type documents
  - 1.105 (57.477 pages) published in 2007

ISO – ***標準化プロセス***

Maturity level / state of standardization

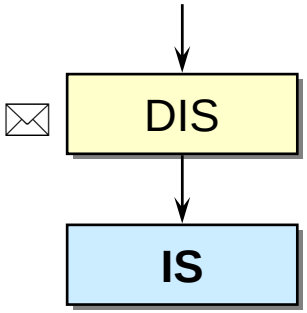
- Study Period / New Project (NP)
  - 2 month NP letter ballot*)
- **Working Draft (WD)**
- **Committee Draft (CD/FCD)**
  - 3 month CD ballot(s)
  - 4 month FCD ballot
- **Draft International Standard (DIS/FDIS)**
  - 2 month FDIS ballot
  - no more comments at this stage
- **International Standard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



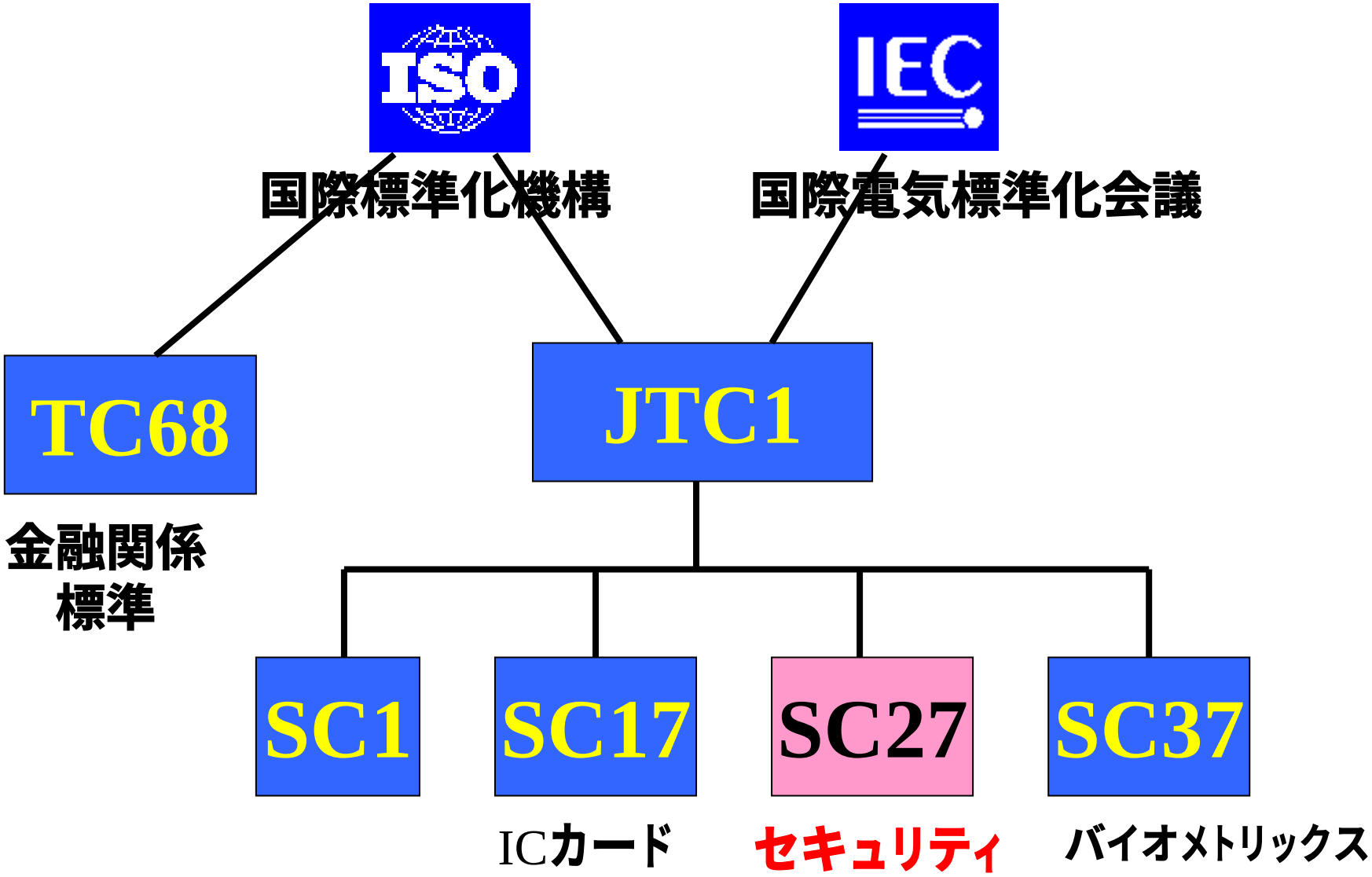
***) one vote per P-member**

ISO/IEC – *Fast Track Process*
(加速化プロセス)

- Motivation
  - **すでに存在する各種規格のリソース(国内標準でもOK)を有効活用して、国際規格化するために・・・**
- Process
  - Submission by a JTC 1 member organization or a recognized PAS submitter (PAS = Publicly Available Specification)
  - 6 month NB ballot (as DIS)
    - at least two thirds of the P-members voting need to approve **(2/3の以上の賛成が必要)**
    - not more than one-quarter of the votes may be negative **(1/4以上の反対があった場合は否決)**
  - Ballot Resolution
    - assignment of the project to a SC
    - appointment of Project Editor
    - establishment of a ballot resolution group
  - Publication



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*

- 情報とICTの保護に関わる規格開発を実施。ここでは、セキュリティ、プライバシーの両方に関わるジェネリックな手法、技法、ガイドラインを含む。例えば、
  - セキュリティ要求条件を抽出する手法、
  - 情報とICTのためのセキュリティマネジメント（ISMSとその応用）
  - 暗号化技術、およびその応用
  - 用語やガイドラインを含む支援文書（サポートドキュメント）の策定
  - IdM、バイオメトリクス、及びプライバシーに関わるセキュリティ事項
  - 情報セキュリティの分野におけるコンフォーマンス評価、認定、監査
  - セキュリティ評価基準（CC）

SC 27 - 組織

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*

SC 27のメンバ国

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

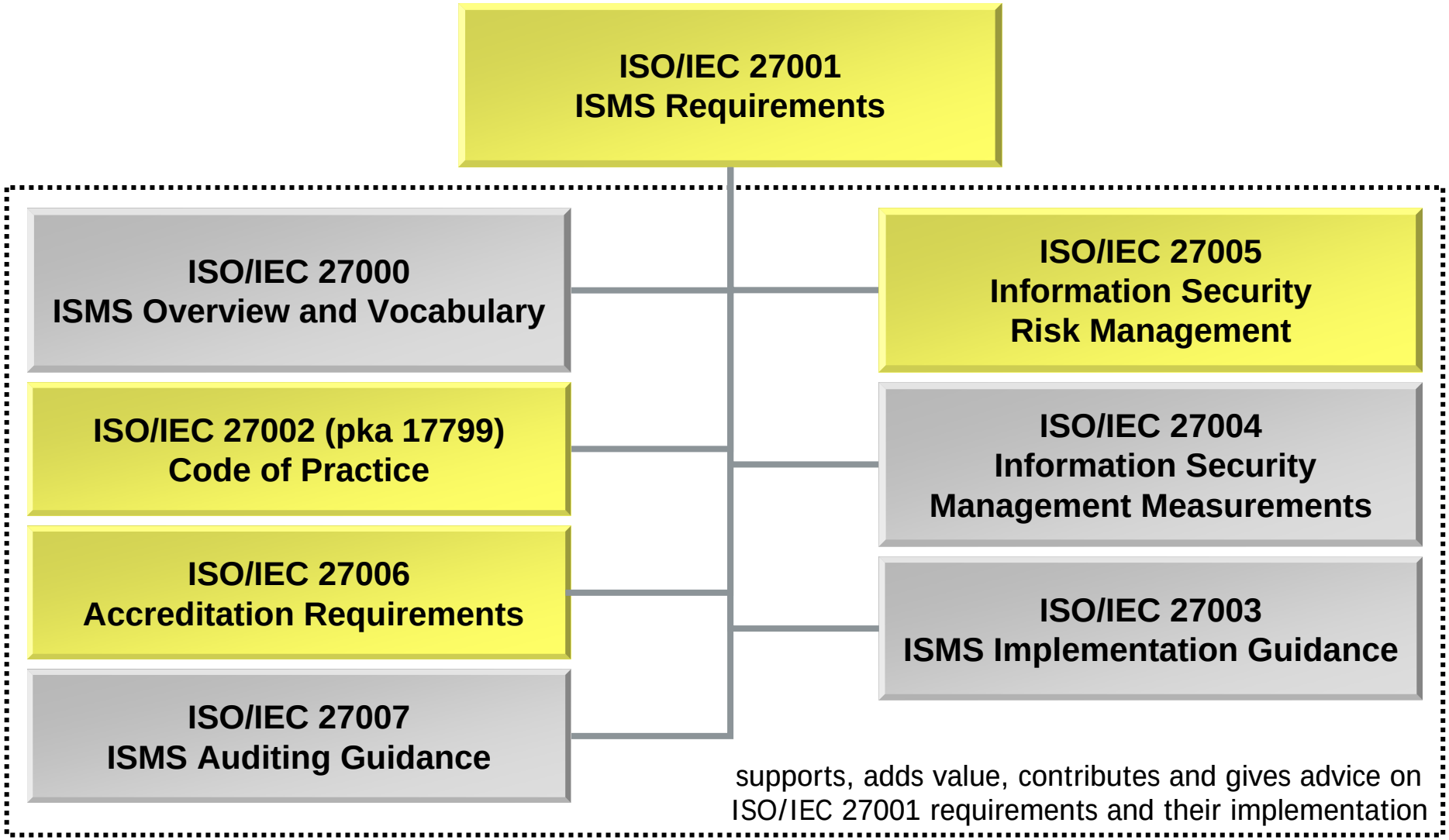
Russian Federation	Poland	South Africa	Kenya		Cyprus	Costa Rica
Korea	Ukraine	Malaysia	Austria	New Zealand	Uruguay	Venezuela
Australia	Czech Republic	India	Luxembourg	Singapore	Sri Lanka	Kazakhstan
1994	*1996-1999*	*2001*	*2002*	*2003*	*2005-2006*	*2007-2008*
additional P-Members (total: 37)						

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

WG 1
– Information Security Management Systems

- WG 1 **スコープ**
  - ISO/IEC 27000 family **の開発、保守**
    (ISMS**規格、関連ガイドライン**)
  - **将来の**ISMS**規格・ガイドに関係する要求事項の抽出**
  - **リエゾン、及び関連機関との連携**
    例えば、
    - ITU-T (Telecommunications)
    - ISO TC 215 (Healthcare)
    - ISO TC 68 (Financial Services)
    - ISO TC 204 (Transportation)
    - World Lottery Association (Gambling)

ISO/IEC 27000 – ISMS ファミリー規格



上記規格の詳細については、日本ISMSユーザグループセミナー
（２００８年、１２月１９日、早稲田）にて紹介予定

新課題　ISO/IEC 27010

- New WD　**on**
  sector to sector interworking and communications for industry and government
- Result of a Study Period on Critical Infrastructures
- Confusion at the last meeting – no new draft available, only a Dispo of Comments
- Scope: This International Standard provides guidance for information security interworking and communications between industries in the same sectors, in different industry sectors and with governments, either in times of crisis and to protect critical infrastructure or for mutual recognition under normal business circumstances to meet legal, regulatory and contractual obligations.

新課題 ISO/IEC 27012

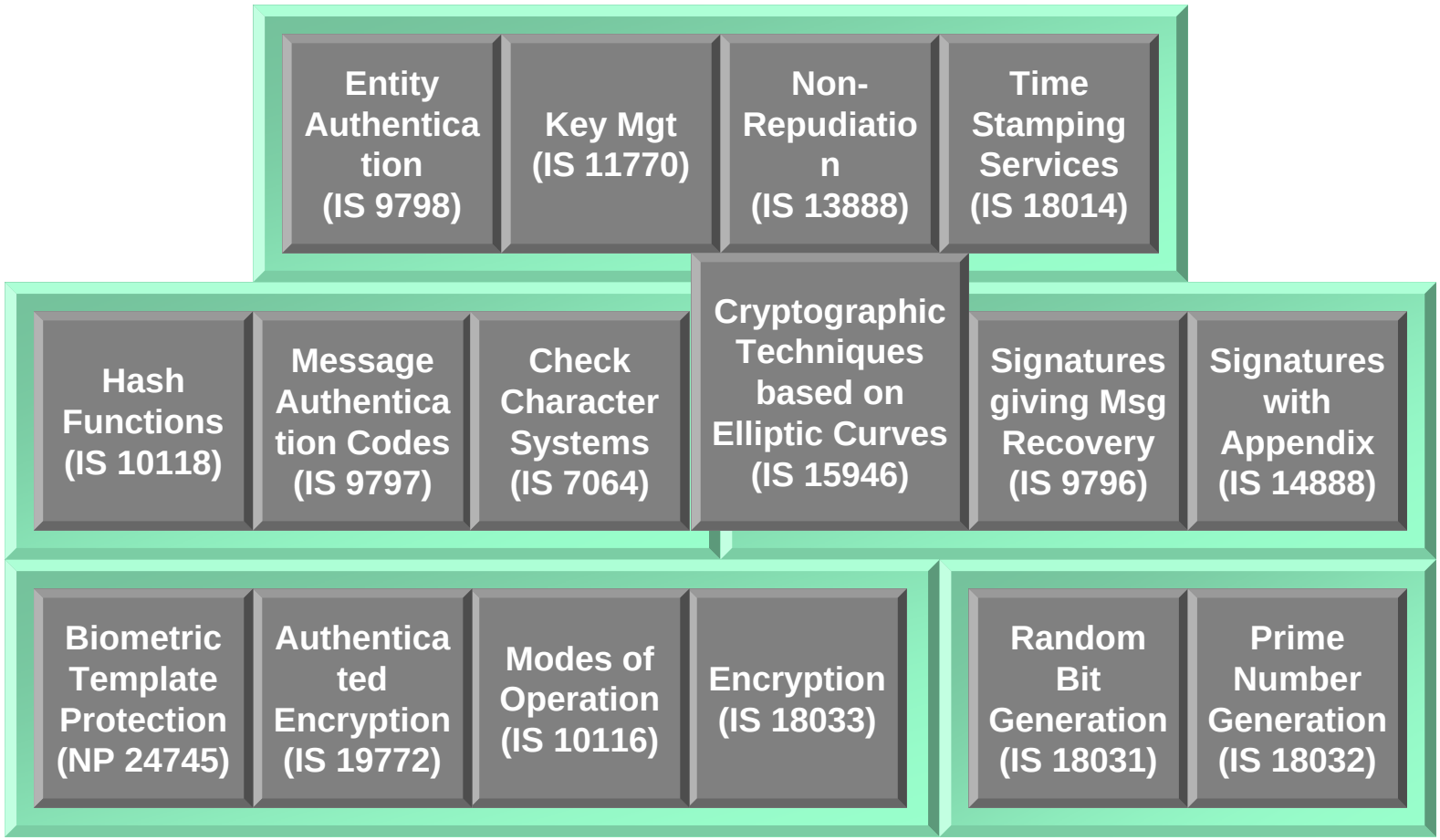
- A new standard containing

  ISMS guidelines for e-government – 1st WD
- The scope of this Standard is to define guidelines supporting the implementation of Information Security Management (ISM) in e-government services
- To provide guidance to the Public Administration on how to adapt 27002 controls and processes to specific e-government services and legally binding procedures

NP Information security governance framework

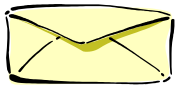
- A NWIP for IS governance
- Scope:
  - Help meet corporate governance requirements related to information security
  - Align information security objectives with business objectives
  - Ensure a risk-based approach is adopted for information security management
  - Implement effective management controls 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

SC 27 Standards – Cryptographic Techniques (WG2)



WG2の活動概要：アルゴリズム関連

- MAC：メッセージ認証子 (9797)
  - パート1：ブロック暗号利用、パート2：専用ハッシュ関数利用、パート3：ユニバーサルハッシュ
- ハッシュ関数(10118)
  - パート1：総論、パート2：ブロック暗号利用、パート3：専用ハッシュ関数
- 暗号アルゴリズム(18033)
  - パート1：総論、パート2：非対称暗号
  - パート3：ブロック暗号、パート4：ストリーム暗号
- ディジタル署名
  - メッセージ回復型署名 (9796シリーズ)
  - 添付型署名 (14888シリーズ)
- 楕円曲線生成 (15946-5)
- 乱数生成 (18031)、素数生成(18032)



ISO/IEC 18033 – Encryption Algorithms

- **Part 1: General**, 2005
- **Part 2: Asymmetric Ciphers**, 2006
  - RSA-ES (OAEP)
  - HIME(R)
  - RSA-KEM (Key Encapsulation Mechanism)
  - ECIES-KEM (Elliptic Curve Integrated Encryption Scheme)
  - PSEC-KEM (DH based)
  - ACE-KEM (DH based)

algorithm	block length	key sizes
3-DES	64	112 or 168
MISTY1	64	128
CAST-128	64	128
AES	128	128, 192 or 256
Camellia	128	128, 192 or 256
SEED	128	128

- **Part 3: Block Ciphers**, 2005
  - 3-DES (two- and three-key variant)
  - MISTY1 (Mitsubishi Electric, Japan)
  - CAST-128 (Entrust, Canada)
  - AES / Rijndael (NIST)
  - Camellia (NTT and Mitsubishi Electric, Japan)
  - SEED (KISA, Korea)
- **Part 4: Stream Ciphers**, 2005
  - MULTI-S01 (Hitachi, Japan)
  - plus several keystream generators

WG2の活動概要：プロトコル関連

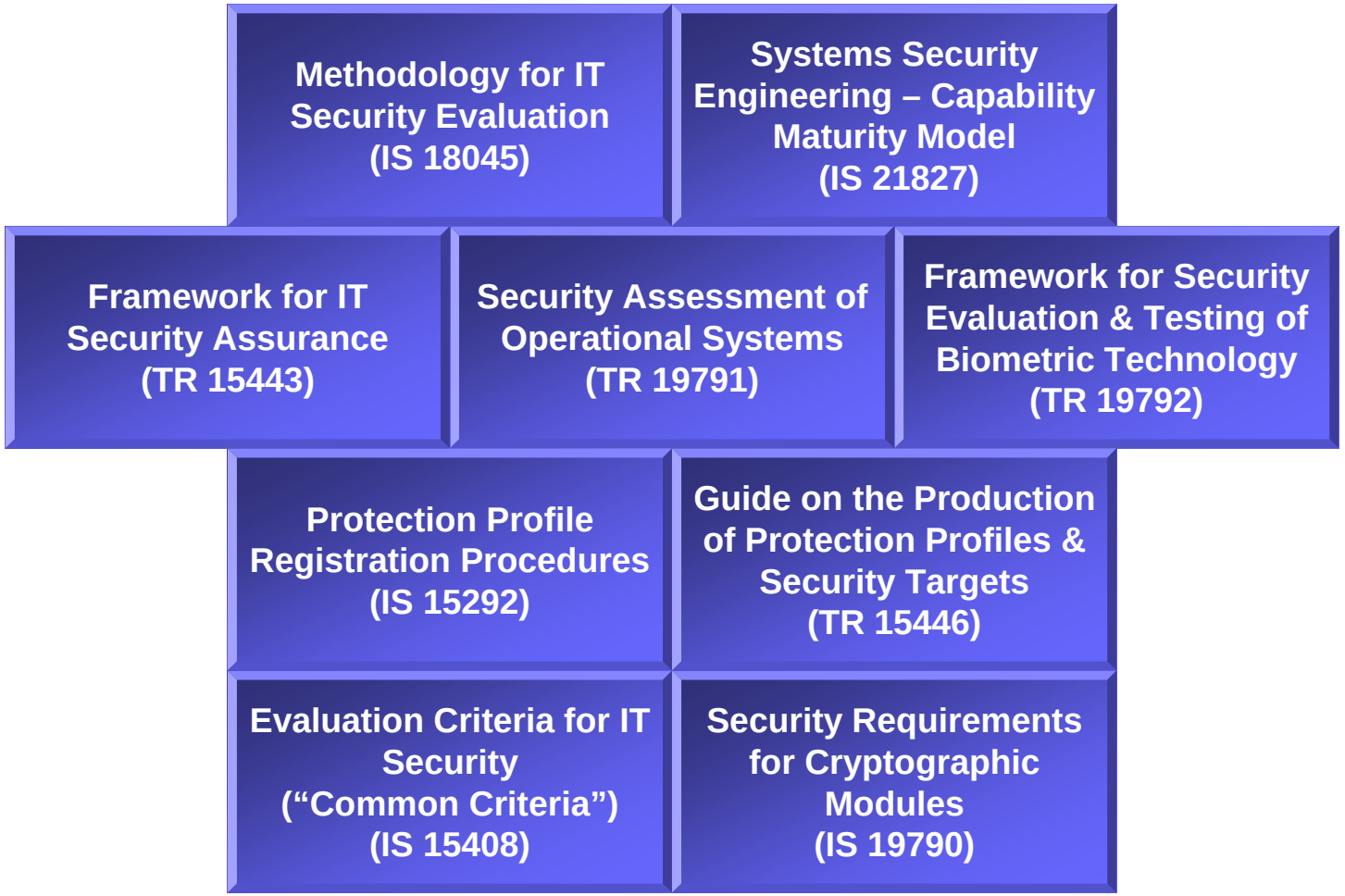
- エンティティ認証(9798)
  - パート1：総論、パート2：対象鍵暗号利用、パート3：非対称鍵暗号利用、パート4：暗号検査関数利用、パート5：ゼロ知識利用、パート6：手動データ転送
- 否認防止 (13888)
  - パート1：総論、パート2：対称鍵暗号利用、パート3：非対称鍵暗号利用
- 鍵管理 (11770)
  - パート1：総論、パート2：対称鍵暗号利用、パート3：非対称鍵暗号利用、パート4：弱い秘密に基づく
- タイムスタンプ(18014)
  - パート1：総論、パート2：独立トークン、パート3：リンク付きトークン

WG2の活動概要：その他、新課題

- 認証付き暗号(19772)
- Signcryption(29150)
- 軽量暗号（NWI：新課題）
- 鍵管理　パート5　グループ鍵管理（11770-5）

  等

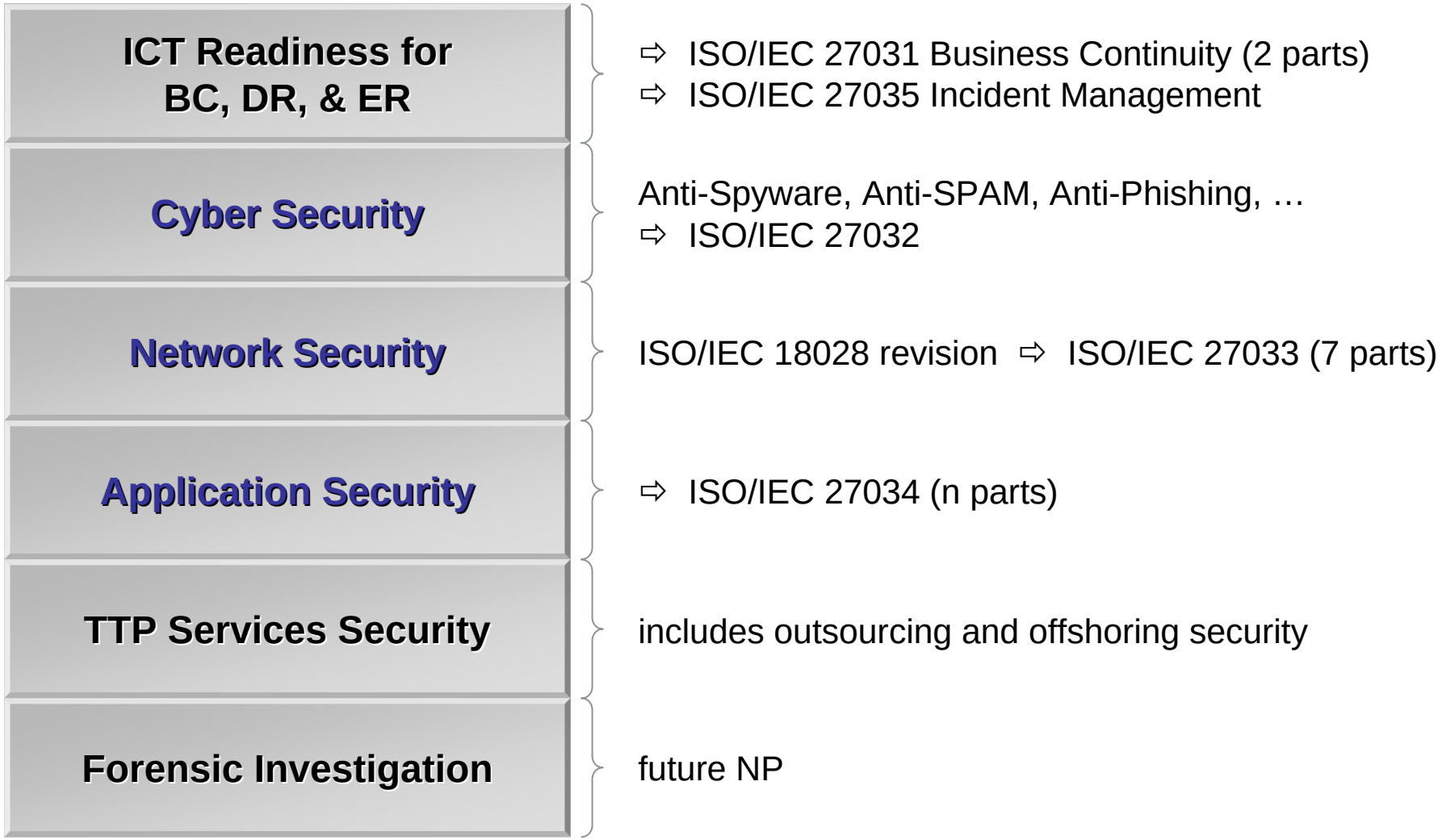
WG 3 – *Security Evaluation*



Recent SC 27 Publications – *WG 3*

- ISO/IEC 15408: Evaluation criteria for IT security –
  - Part 1: Introduction and general model, 3rd edition 2009e.
  - Part 2: Security functional components, 3rd edition 2008e.
  - Part 3: Security assurance components, 3rd edition 2008e.
- ISO/IEC TR 15443: A framework for IT security assurance –
  - Part 3: Analysis of assurance methods, 2007.
- ISO/IEC 18045: Methodology for IT security evaluation, 2nd ed. 2008e.
- ISO/IEC 19790: Security requirements for cryptographic modules, 2006.
- ISO/IEC 24759: Test requirements for cryptographic modules, 2008e.

WG 4 – Security Controls and Services



CyberSecurity**の規格？**

- Cyberspace, while not existing in any physical form, is a complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it.
- The complex environment encompasses the interconnecting networks and systems as well as any ICT devices belonging to different organizations and service providers that allow for the flow of information.
- However, there are security issues that are not covered by current information security, Internet security, network security and ICT security best practices because there are gaps between these domains.
- Cyberspace security, or Cybersecurity, is about the security of the Cyberspace, providing guidance to address issues arising from the gaps between the different security domains in the Cyberspace environment while at the same time providing an infrastructure for collaboration. **（情報共有フレームワークなど・・・）**
- **エディタは、シンガポールと日本**

Network Security規格について

- **規格番号**：ISO/IEC 27033(**複数パート構成**)
- **位置付けおよびスコープ**
  - ISMS**規格である**ISO/IEC 27001/27002**の管理策のうち、**Network Security**に関するものを詳細化**
  - Network Security**に関する概念、リスク、実装時の設計手法や管理策などのガイダンスを規定**
- **従来の規格**（18028**シリーズ**）**との関係**
  - ISMS**の**Network Security**規格は、**2005/4～2006/7**に**ISO/IEC 18028**シリーズ**(Part1～Part5)**として発行済**
  - **今回、新しい技術動向取り込み等のため、**ISO/IEC 27033**シリーズとして改訂中**
- **対象読者**
  - Network**の所有者、運営者、使用者**
  - Network Security**の計画、設計、実装、運用者**

Network Security規格のパート構成

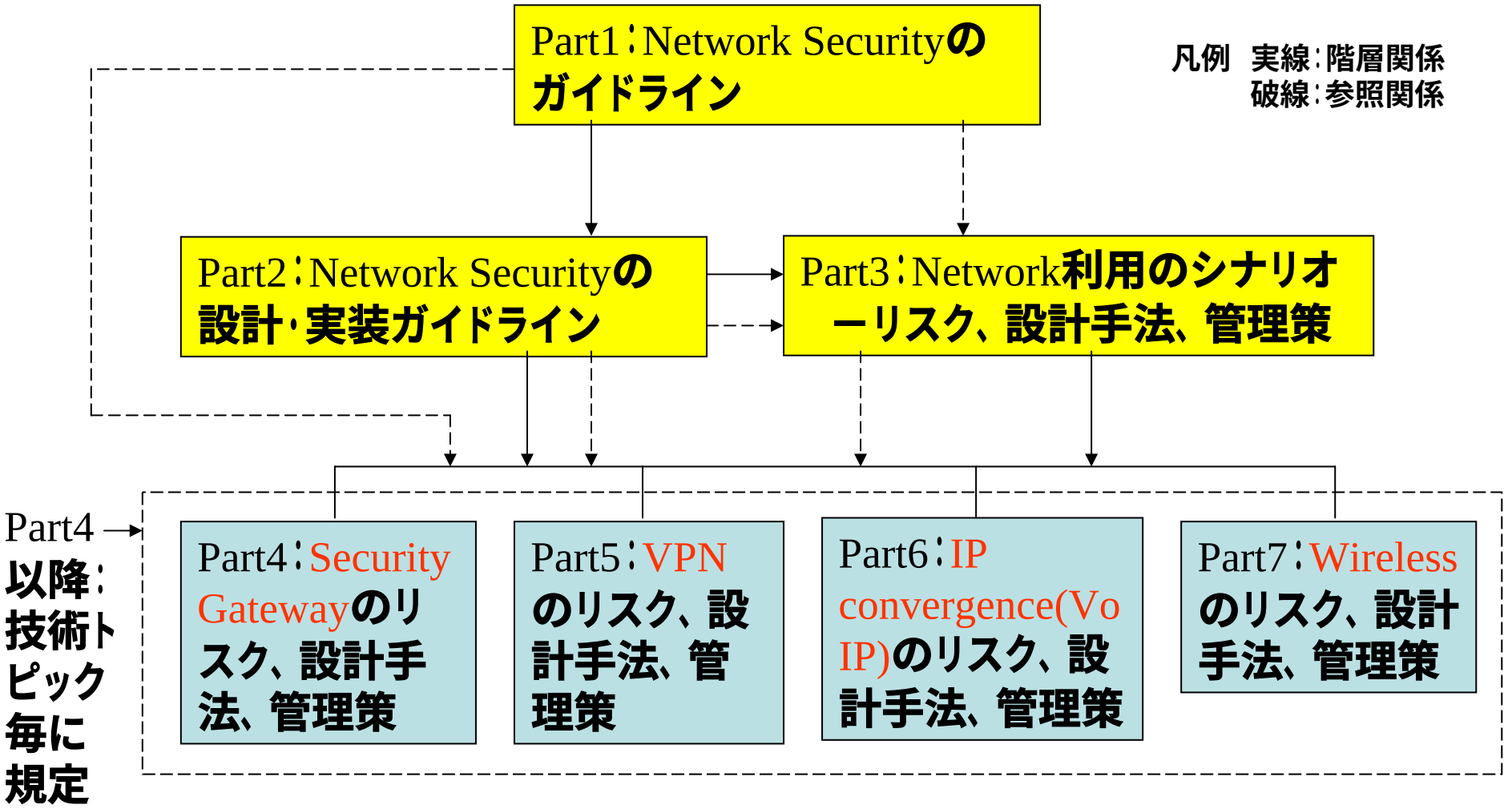
- Part1：Network Securityのガイドライン
- Part2：Network Securityの設計・実装ガイドライン
- Part3：Network利用のシナリオーリスク、設計手法、管理策
- Part4：Security Gatewayのリスク、設計手法、管理策
- Part5：VPNのリスク、設計手法、管理策
- Part6：IP convergence(VoIP)のリスク、設計手法、管理策
- Part7：Wirelessのリスク、設計手法、管理策

（Part4以降は、技術トピック毎に規定）

パートの概要（パート1～パート3の現在のドラフト）

- Part1：Network Securityのガイドライン
  - Network Securityの概念、用語定義
  - Network Securityのリスクの分析方法、分析に基づくセキュリティ要件
  - Network Securityのアーキテクチャや管理策の概要
  - Network利用のシナリオの概要
  - Network Securityの管理策の実装、運用の概要
  - 27033シリーズの概要とロードマップ
- Part2：Network Securityの設計・実装ガイドライン
  - モデル/フレームワークを用いたNetwork Security の計画、設計、実装の方法
- Part3：Network利用のシナリオーリスク、設計手法、管理策
  - 典型的なシナリオ（従業員によるインターネットアクセス、B to Bサービス、B to Cサービスなど）におけるNetwork Securityのリスク、設計手法、管理策

Network Security規格のロードマップ



既存のセキュリティ標準と27034

従来…

セキュリティの課題

・セキュリティ機能の必然性が不明
・セキュリティ実装における程度が不明
・セキュリティ対策の効果が不明
・運用時に必要なセキュリティ対策が不明

統一基準で明確化

①論理的正当化による解決（15408など）
- 脅威→セキュリティ機能（Protection Profile）
- 実装された機能の保証（EAL）
- 納品するまで。（運用面での規定ではない）

②運用管理の正当化による解決（27Kシリーズ）
- 組織・人・運営 面での解決
- 15408との連携はない

#①と②は補完関係

タイプ： ターゲットを明確に定めて毎回構築・評価する方法
提供物はほとんど開発する場合
評価・監査は、第3者

27034

既存標準の問題解決への提案

・評価にかかる時間とコストが大きい
・組合せ（マッシュアップなど）の評価が不明

違った観点で新たに標準化

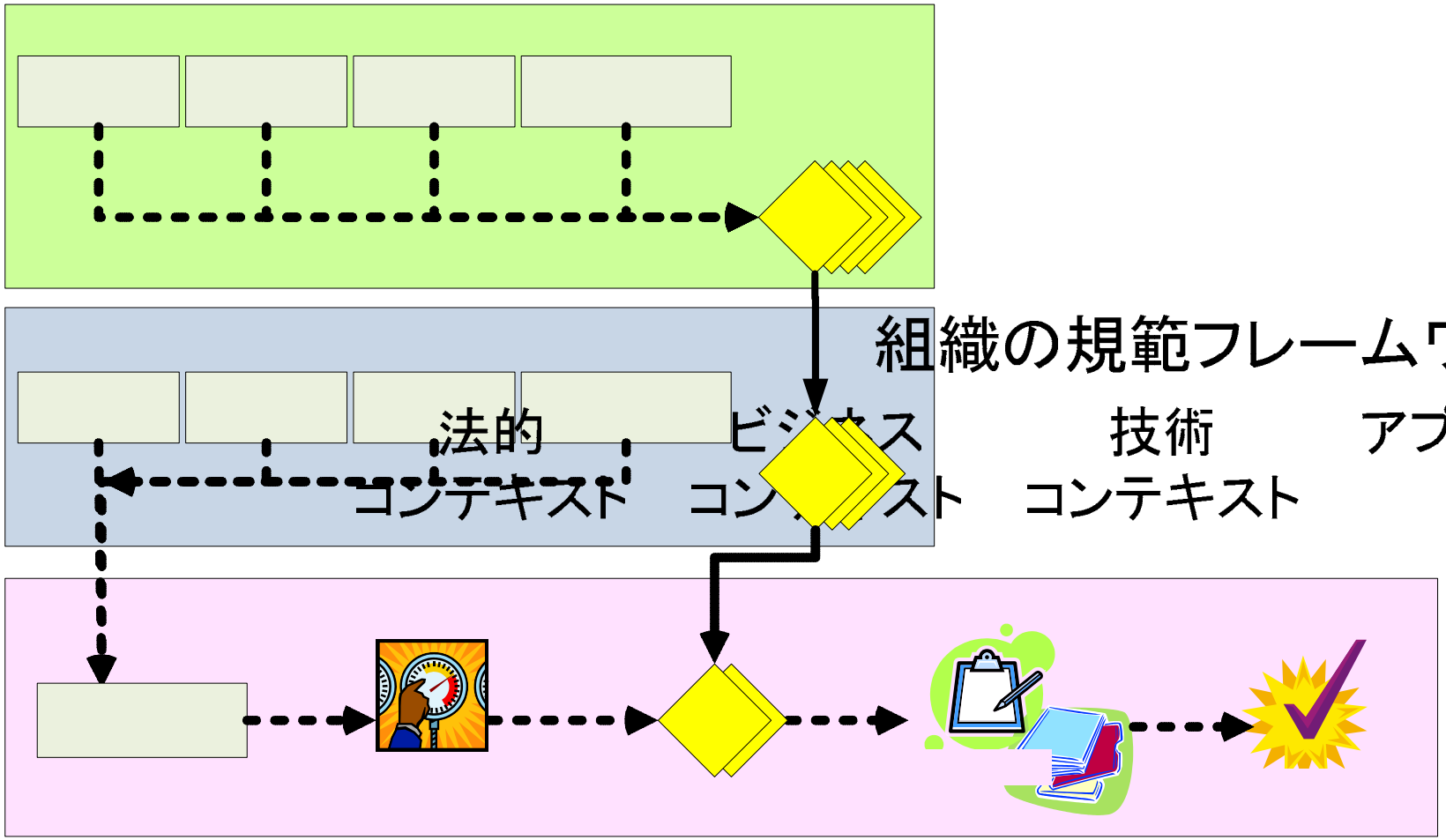
①生産性向上（軽量化）
- 再利用性の向上

②効率向上（明確化）
- 役割・コントロールの明確化
- 供給・調達の一貫性を狙う

タイプ： 部品を積上げてターゲットに適応する方法
組織が選んだ対策を組織毎に定め、
アプリケーション毎に実施。

ISO/IEC 27034の俯瞰

ASM：Application Security Measures

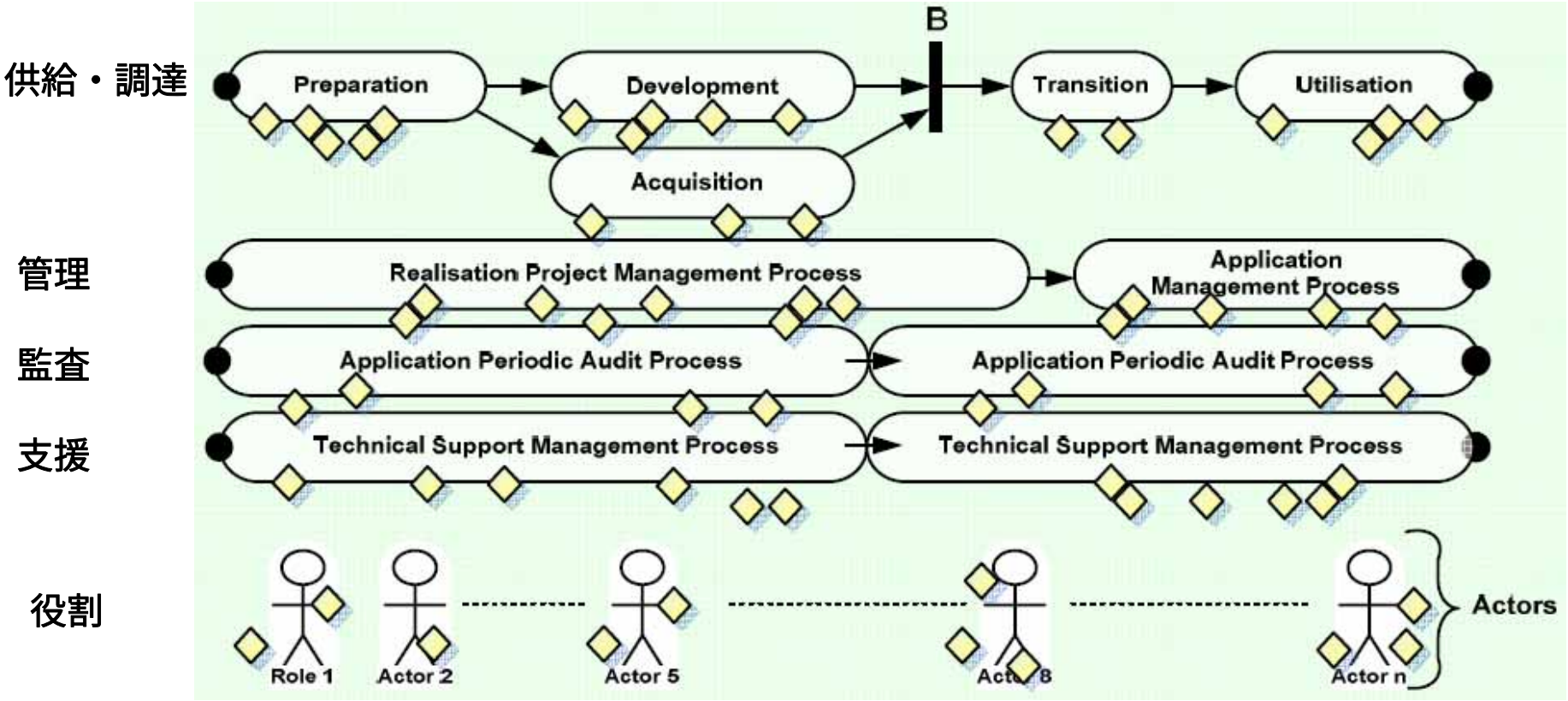


ASMが組織毎に用意される。アプリケーションで必要なものを抽出する。アプリケーションリスクを分析し、セキュリティ目標レベルを決め、アプリケーション毎に集めたライブラリから抽出して使う。設計・開発に使う。また運用時に使うことも考えている。例は、供給者サイドへの適用。

（個別の）アプリケーション規範フレーム

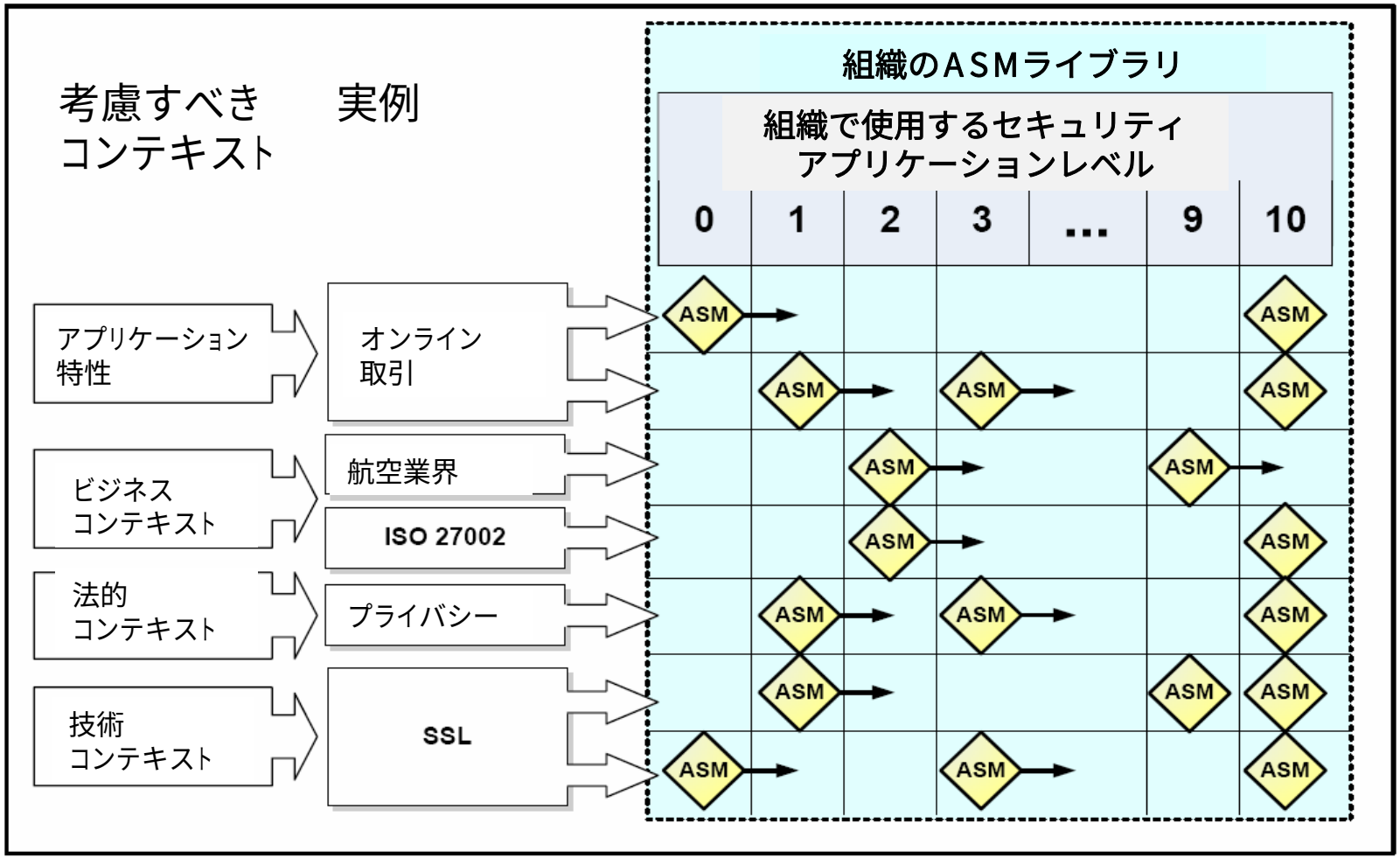
法的　ビジネス　技術　アプリケーショ

ASMのプロセス･役割への適用



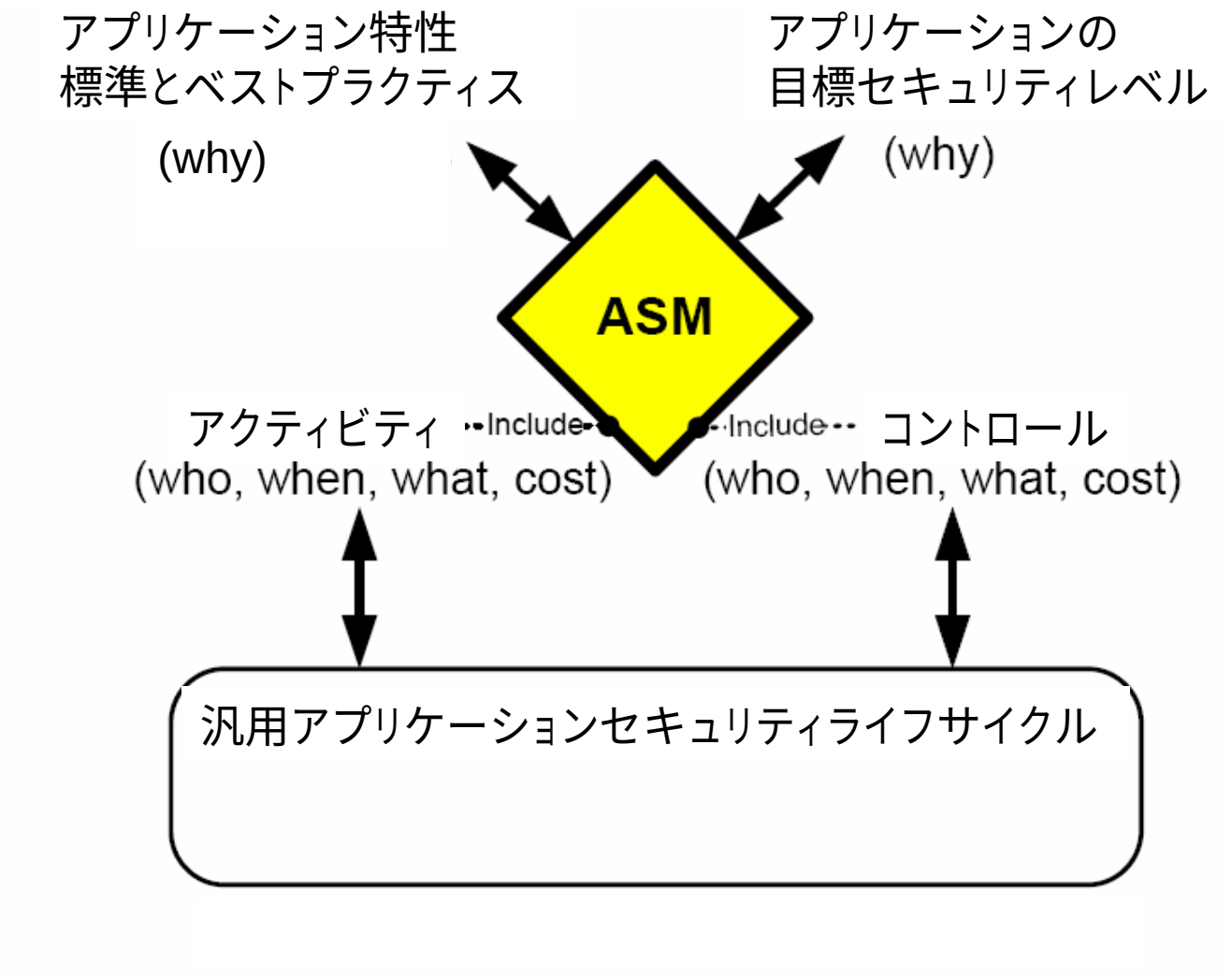
ASM (アプリケーションセキュリティ対策) は、各プロセス (供給･調達、管理、監査、支援) および役割に提供され、エビデンスの生成に利用される。

コンテキストに対応するアプリケーション、セキュリティレベル、に応じて選択されるASMの例



図は、市場要求のセキュリティレベル０－１０に対し、プライバシーの例ではレベル1、2で、あるASMが、レベル3-9で別のASMが、レベル10でさらに別のASMを使うことを示している。

27034で肝となるアプリケーションセキュリティ対策(ASM)



WG 5 – Identity Management & Privacy Technologies

- WG 5 covers the development and maintenance of standards and guidelines addressing security aspects of identity management, biometrics and the protection of personal data. This includes:
  - Current projects
    - A framework for Identity Management (ISO/IEC WD 24760)
    - Biometric template protection (ISO/IEC WD 24745)
    - Authentication context for biometrics (ISO/IEC CD 24761)
    - A privacy framework (ISO/IEC WD 29100)
    - A privacy reference architecture (NP 29101)
    - Authentication assurance (ISO/IEC WD 29115)
  - Identification of requirements for and development of future standards and guidelines in these areas.

IdMについては、ITU-Tの後で紹介

SC 27 – ***要約***

- SC 27 is responsible for
  - ~ 90 projects, including ~ 45 active projects
- Between 1990 and today, SC 27 has published
  - 70+ International Standards (IS) and Technical Reports (TR)

- Next Meetings
  - April 2009 China WGs & Plenary

- More Information & Contact
  - http://www.jtc1sc27.din.de/en SD7: Catalogue of SC 27 Projects & Standards
  - SC 27 Secretariat: Krystyna.Passia@din.de
  - SC 27 Chairman: Walter.Fumy@siemens.com
  - SC 27 Vice Chair: Marijke.DeSoete@pandora.be

ITU-Tのセキュリティ標準化動向

ITU Plenipotentiary Conference 2006
Resolution PLEN/2
- 情報と通信に関するセキュリティにおけるITUの役割強化

- Plenipotentiary Resolution 130 (2006),

  Strengthening the role of ITU in building confidence and security in the use of information and communication technologies – Instructs Director of TSB to intensify work in study groups, address threats & vulnerabilities, collaborate, and share information

- Plenipotentiary Resolution 149 (2006),

  Study of definitions and terminology relating to building confidence and security in the use of information and communication technologies - Instructs Council to study terminology

要は、情報通信技術への活用に向けて、セキュリティに関わる標準化活動をしっかりやれ！

ITU-T World Telecommunications Standardization Assembly (WTSA)での決議

- **決議　50, Cyberscecurity**
  - Evaluate existing and evolving new Recommendations with respect to their robustness of design and potential for exploitation by malicious parties
  （**既存/新規勧告に対する信頼性評価を実施すること**）
  - Raise awareness of the need to defend against the threat of cyber attack
  （**サイバー攻撃の脅威に対する防御の必要性認識**）

- **決議　52, Countering and combating spam**
  - Study Groups, in cooperation with other relevant groups, to develop as a matter of urgency technical Recommendations on countering spam
  （**スパム対策のための技術勧告の早期策定、他団体との連携**）
  - Report on international initiatives for countering spam
  （**スパムに対向するための国際的先導の報告**）
  - Member States to take steps within their national legal frameworks to ensure measures are taken to combat spam
  （**スパム対策を確実にする法的枠組みにおけるメンバ活動**）

規格化の主導権

- **ITU Global Cybersecurity Agenda (GCA)**
  - A Framework for international cooperation on cybersecurity
  - ITU response to its role as sole Facilitator for WSIS Action Line C5
  - Five key work areas: **Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, International Cooperation**
  - World renowned Group of High-Level Experts (HLEG)
    - **Report of the chairman of the HLEG to ITU Secretary-General contains recommendations in each of the five work areas**
- **ITU-D Work on Cybersecurity**
  - ITU-D Study Group 1 Question 22/1: *Securing information and communication networks: Best practices for developing a culture of cybersecurity*
  - ITU-D Programme 3 *ITU Cybersecurity Work Programme to Assist Developing Countries*

セキュリティ規格化における協力関係

- **ISO/IEC/ITU-T Strategic Advisory Group Security**
  - Oversees standardization activities in ISO, IEC and ITU-T relevant to security; provides advice and guidance relative to coordination of security work; and, in particular, identifies areas where new standardization initiatives may be warranted.
    - Portal established
    - Workshops conducted
- **Global Standards Collaboration**
  - ITU and participating standards organizations exchange information on the progress of standards development in the different regions and collaborate in planning future standards development to gain synergy and to reduce duplication. GSC-13 resolutions concerning security include:
    - **GSC-13/11 – Cybersecurity**
    - **GSC-13/04 – Identity Management**
    - **GSC-13/03 – Network aspects of identification systems**
    - **GSC-13/25 – Personally Identifiable Information Protection**

ITU-T におけるセキュリティ規格化活動

- Study Group 17 は「セキュリティ」に関する先導的なSG。
  - ITU-T全体の調整作業
  - 基幹となる勧告作成作業

- SG17は、以下のSGと連携しながら作業を進めている。
  - SG 4 for TMN security → SG 2にマージ
  - SG 9 for IPCablecom security
  - SG 13 for NGN security
  - SG 16 for Multimedia security

ITU-T Study Groups （SG)構成
(旧会期：２００５－２００８)

- **SG 2** Operational aspects of service provision, networks and performance
- **SG 3** Tariff and accounting principles including related telecommunications economic and policy issues
- **SG 4** Telecommunication management
- **SG 5** Protection against electromagnetic environment effects
- **SG 6** Outside plant and related indoor installations
- **SG 9** Integrated broadband cable networks and television and sound transmission
- **SG 11** Signalling requirements and protocols
- **SG 12** Performance and quality of service
- **SG 13** Next generation networks
- **SG 15** Optical and other transport network infrastructures
- **SG 16** Multimedia terminals, systems and applications
- **SG 17** **Security, languages and telecommunication software**
- **SG 19** Mobile telecommunication networks
- **TSAG** Telecommunication Standardization Advisory Group

www.itu.int/ITU-T

ITU-T Study Groups （SG)構成
(新会期：2009－2012)

- SG 2 (Operational aspects of service provision and telecommunications management)
- SG 3(Tariff and accounting principles including related telecommunication economic and policy Issues) **津川　副議長**
- SG 5 (Protection against electromagnetic environment effects)
- SG 9 (Television and sound transmission and integrated broadband cable networks) **宮地　副議長**
- SG 11 (Signalling requirements, protocols and test specifications) **釼吉　副議長**
- SG 12 (Performance, QoS and QoE) **高橋　副議長**
- SG 13(Future networks including mobile and NGN) **森田　副議長**
- SG 15 (Optical transport networks and access network infrastructures) **前田　議長**
- SG 16 (Multimedia coding, systems and applications) **内藤　議長**
- **SG 17 (Security) 中尾　副議長**

ITU-T security building blocks

Security Architecture Framework

X.800 – Security architecture
X.802 – Lower layers security model
X.803 – Upper layers security model
X.810 – Security frameworks for open systems: Overview
X.811 – Security frameworks for open systems: Authentication framework
X.812 – Security frameworks for open systems: Access control framework
X.813 – Security frameworks for open systems: Non-repudiation framework
X.814 – Security frameworks for open systems: Confidentiality framework
X.815 – Security frameworks for open systems: Integrity framework
X.816 – Security frameworks for open systems: Security audit and alarms framework

Telecommunication Security

X.805 – Security architecture for systems providing end-to-end communications
X.1051 – Information security management system – Requirements for telecommunications (ISMS-T)
X.1081 – A framework for specification of security and safety aspects of telebiometrics
X.1121 – Framework of security technologies for mobile end-to-end communications
X.1122 – Guideline for implementing secure mobile systems based on PKI

Protocols

X.273 – Network layer security protocol
X.274 – Transport layer security protocol

Security in Frame Relay

X.272 – Data compression and privacy over frame relay networks

Security Techniques

X.841 – Security information objects for access control
X.842 – Guidelines for the use and management of trusted third party services
X.843 – Specification of TTP services to support the application of digital signatures

Directory Services and Authentication

X.500 – Overview of concepts, models and services
X.501 – Models
X.509 – Public-key and attribute certificate frameworks
X.519 – Protocol specifications

Network Management Security

M.3010 – Principles for a telecommunications management network
M.3016 – TMN Security Overview
M.3210.1 – TMN management services for IMT-2000 security management
M.3320 – Management requirements framework for the TMN X-Interface
M.3400 – TMN management functions

Systems Management

X.733 – Alarm reporting function
X.735 – Log control function
X.736 – Security alarm reporting function
X.740 – Security audit trail function
X.741 – Objects and attributes for access control

Televisions and Cable Systems

J.91 – Technical methods for ensuring privacy in long-distance international television transmission
J.93 – Requirements for conditional access in the secondary distribution of digital television on cable television systems
J.170 – IPCablecom security specification

Multimedia Communications

H.233 – Confidentiality system for audiovisual services
H.234 – Encryption key management and authentication system for audiovisual services
H.235 – Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals
H.323 Annex J – Packet-based multimedia communications systems – Security for H.323 Annex F (Security for simple endpoint types)
H.350.2 – Directory services architecture for H.235
H.530 – Symmetric security procedures for H.323 mobility in H.510

Facsimile

T.30 Annex G – Procedures for secure Group 3 document facsimile transmission using the HKM and HFX system
T.30 Annex H – Security in facsimile Group 3 based on the RSA algorithm
T.36 – Security capabilities for use with Group 3 facsimile terminals
T.503 – Document application profile for the interchange of Group 4 facsimile documents
T.563 – Terminal characteristics for Group 4 facsimile apparatus

Message Handling Systems (MHS)

X.400/F.400 – Message handling system and service overview
X.402 – Overall architecture
X.411 – Message transfer system: Abstract service definition and procedures
X.413 – Message store: Abstract service definition
X.419 – Protocol specifications
X.420 – Interpersonal messaging system
X.435 – Electronic data interchange messaging system
X.440 – Voice messaging system

ITU-T Recommendations are available from the ITU website http://www.itu.int/publications/bookshop/how-to-buy.html (this site includes information on limited free access to ITU-T Recommendations)

Current important security work in ITU-T includes

Telebiometrics, Security management, Mobility security, Emergency telecommunications

For further information on ITU-T and its Study Groups: http://www.itu.int/ITU-T

2005－2008研究期　セキュリティ課題

Telecom Systems Users

Q7

Security Management

*T-ISMS

*インシデントマネジメント

*リスク評価手法

*17799等

Telebiometorics Technology

*核 Telebiometorics

*Telebiometorics システムメカニズ

Q8

Security Architecture & Framework

*X.800 series

*新体系

*将来のモデル、フレームワーク

Q5

Applications & Services Security for telecom

*モバイルセキュア通信

*セキュア通信サービス

*セキュアWebサービス

Q9

Q6

Networks and Systems on Cyber Security for Telecom

*脆弱性情報共有

*インシデント対応運用

SPAM

Q17

Telecom Systems

Q4

Communication System Security　*プロジェクト、ロードマップ、辞典

課題と勧告体系

- X.805-809: Architecture & Framework for Q5
  <X.800-X.849: Security>

X.1000-X.1999 : Telecommunication security

X.1000-1099：Basic Security Control and Management

- X.1000-1009: for All Questions → General security aspects
- X.1010-1029 : for Q4
- X.1030-1049: Network Security (1031)
- X.1050-1069: Security Management (1051)
- X.1080-1099: Telebiometrics (1081)

X.1100-1199：Secure Applications and services

- X.1100-1109: General for Q9-1
- X.1110-1119: Home NW
- X.1120-1139: Mobile NW (1121, 1122)
- X.1140-1149: Web Security (1141,1142)
- X.1150-1179: Secure AP service for Q9-5

X.1200-1299：Cyber Security

- To be detailed

セキュリティに関連する来会期課題 (2009-2012)

課題	課題のタイトル	新規･継続
I	Telecommunications Systems Security Project（調整のプロジェクト）	Q.4/17の継続
J	Security Architecture and Framework	Q.5/17の継続
K	Cybersecurity	Q.6/17の継続
L	Identity Management, Architecture and Mechanisms （IdM関連課題）	新規
M	Telecommunications Information Security Management （ISMS関連）	Q.7/17の継続
N	Telebiometrics	Q.8/17の継続
O	Security Aspects of Ubiquitous Telecommunication Services	Q.9/17の一部継続
P	Secure Application services	Q.9/17の一部継続
Q	Countering Spam by Technical Means	Q.17/17の継続
T	Service Oriented Architecture Security	新規

SG17：新しい会期の議長陣とWP構成

Chairman: Mr Arkadiy Kremer (Russian Federation)

Vice Chairmen: Mr Jianyong Chen (China)、Mr M. Khair Almobark Elhaj (Sudan)、Mr Antonio Guimarães (Brazil)、Mr Koji Nakao (Japan)、Mr Patrick Mwesigwa (Uganda)、Mr Heung-Youl Youm (Republic of Korea)

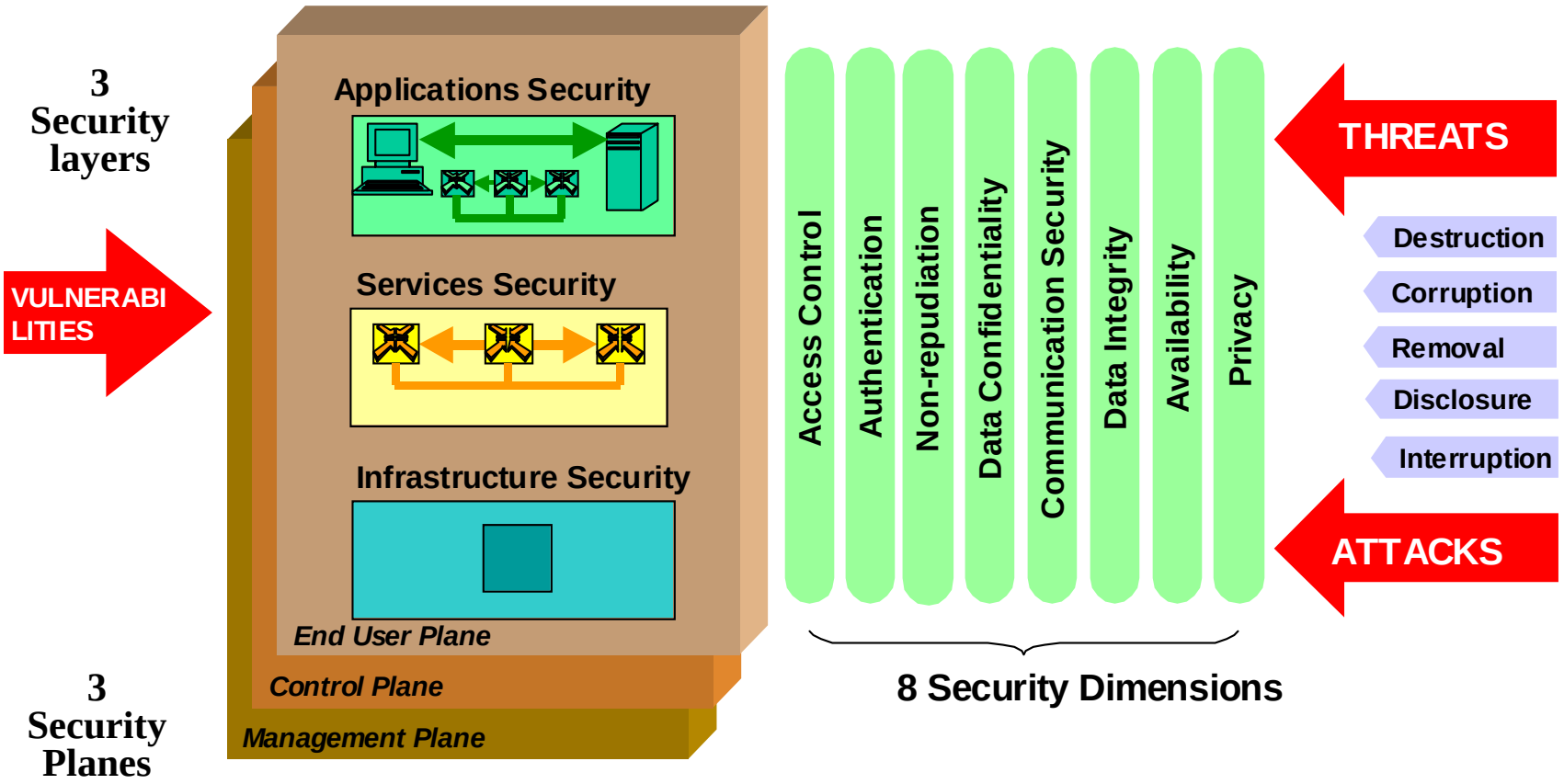
WP1/17 “Network and Information Security“ →WP**議長** Koji Nakao (Japan)
- Q.I/17, Telecommunications Systems Security Project
- Q.J/17, Security Architecture and Framework
- Q.M/17, Telecommunications Information Security Management
- Q.K/17, Cybersecurity
- Q.Q/17, Countering Spam by Technical Means

WP2/17 “Application Security” →WP**議長** Mr Heung-Youl Youm (**韓国**)
- Q.O/17, Security Aspects of Ubiquitous Telecommunication Services
- Q.P/17, Secure Application services
- Q.T/17, Service Oriented Architecture Security
- Q.N/17, Telebiometrics
- Q.E/17, Open Systems Interconnection (OSI).

WP3/17 “IdM and Languages” →WP**議長** Mr Jianyong Chen (**中国**)
- Q.L/17, Identity Management Architecture and Mechanisms
- Q.D/17, Directory Services, Directory Systems, and Public-key/Attribute Certificates
- Q.A/17, Abstract Syntax Notation One (ASN.1), Object Identifiers (OIDs) and associated registration
- Q.B/17, Formal Languages and Telecommunication Software
- Q.C/17, Testing Languages, Methodologies and Framework

Study Group 17 において注目される
セキュリティ勧告の紹介

X.805: Security Architecture for End-to-End Communications



- ぜい弱性は、各層、プレイン（面）、次元に存在する
- 72 のセキュリティ観点 (3 Layers ✖ 3 Planes ✖ 8 Dimensions)

ITU-T X.805 Approach

	Infrastructure Layer	Services Layer	Applications Layer
Management Plane	Module One	Module Four	Module Seven
Control/Signaling Plane	Module Two	Module Five	Module Eight
User Plane	Module Three	Module Six	Module Nine

Execute

- Top Row for Analysis of Management Network
- Middle Column for Analysis of Network Services
- Intersection of Each Layer and Plane for analysis of Security Perspective

Access Control	Communication Security
Authentication	Data Integrity
Non-repudiation	Availability
Data Confidentiality	Privacy

The 8 Security Dimensions Are Applied to Each Security Perspective

ITU-T X.805

全体的な視野に立ったアプローチ:

- **ネットワークの視点からの** End-to-End**セキュリティ**
- **いろいろなタイプのネットワーク技術への適用性**
  - **無線、有線、光ネットワーク**
  - **音声、データ、ビデオなどをカバーするネットワーク**
- **多様なネットワーク機能への適用性**
  - **サービス提供者ネットワーク**
  - **企業ネットワーク**
  - **政府系ネットワーク**
  - **マネジメント/運用管理ネットワーク**
  - **データセンターネットワーク**Data Center Networks
- **既存の規格/標準への対応が可能**
- **今後何が必要かというセキュリティパズルの不足点を補完**

電気通信事業者のための情報セキュリティマネジメント：勧告X.1051

- X.1051：Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
  - 通信事業者にとって、あらゆるビジネスリスクを軽減するために、情報セキュリティマネジメントの構築、運用、監査、保守を実行するためのガイドライン

- ISO/IEC JTC1/SC27/WG1との完全共同文書化を実現
  ISO/IEC 27011とCommon Text.

- 今後は、ITU-Tにおいて、ISO/IEC 27001に基づく通信事業者のための要求事項をまとめていく予定。
  （2009－2012研究会期の新課題となっている）

Introduction of Information security management guidelines for Telecommunications (X.1051) **新しい改版作業**

Revised X.1051

- Security policy
- Organising information security
- Asset management
- Human resources security
- Physical & environmental security
- Communications & operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

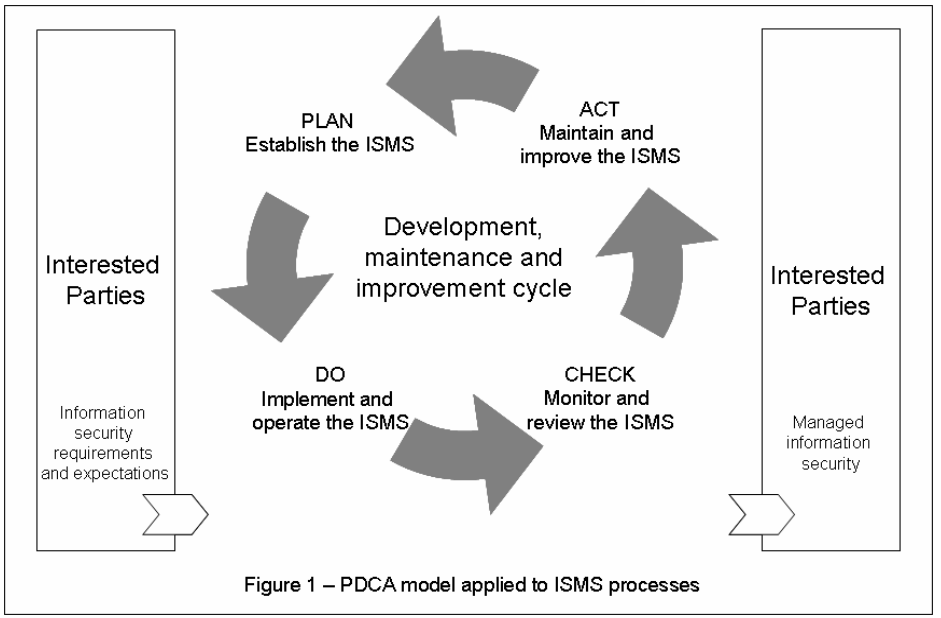
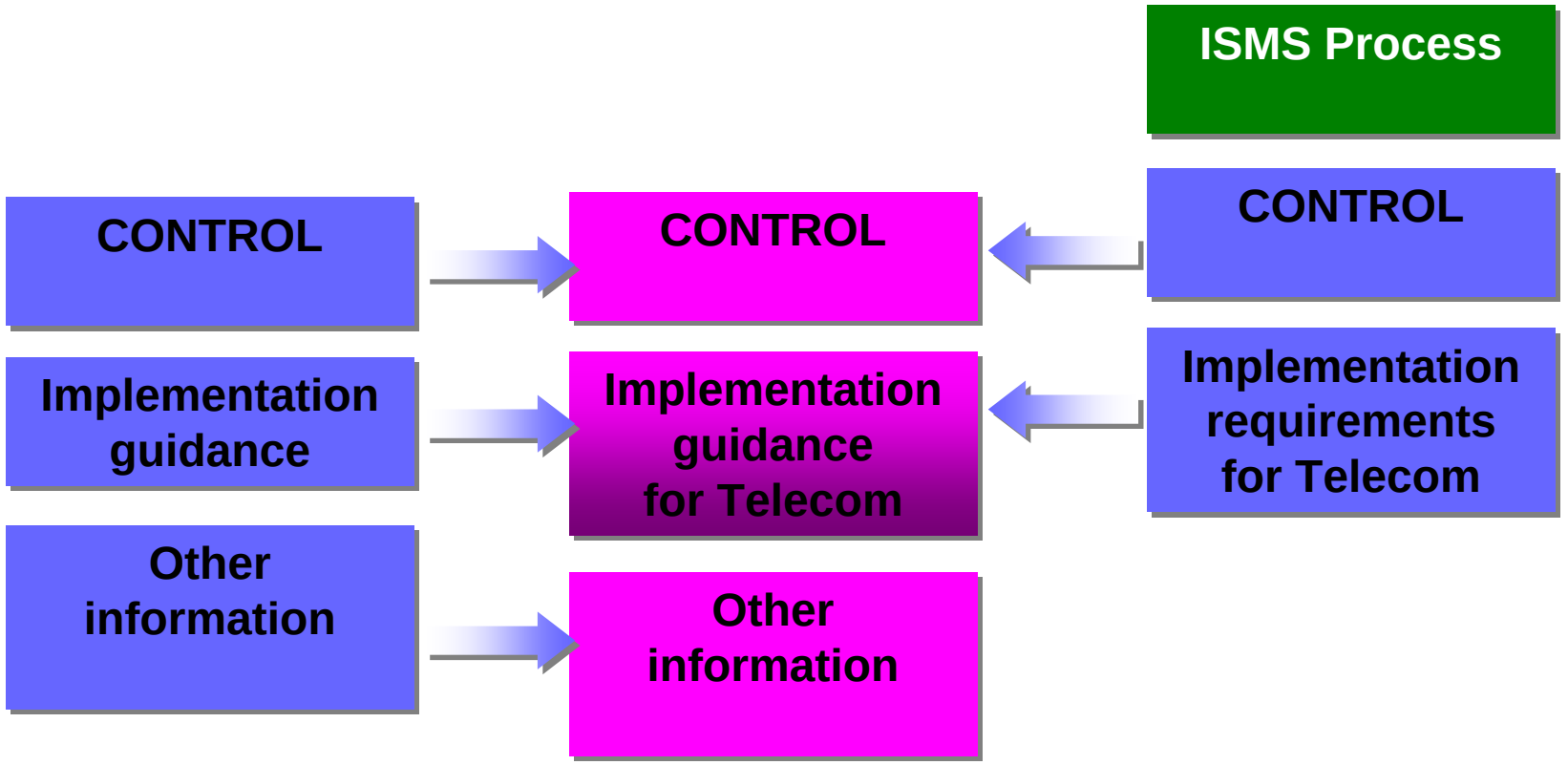


Figure 1 – PDCA model applied to ISMS processes

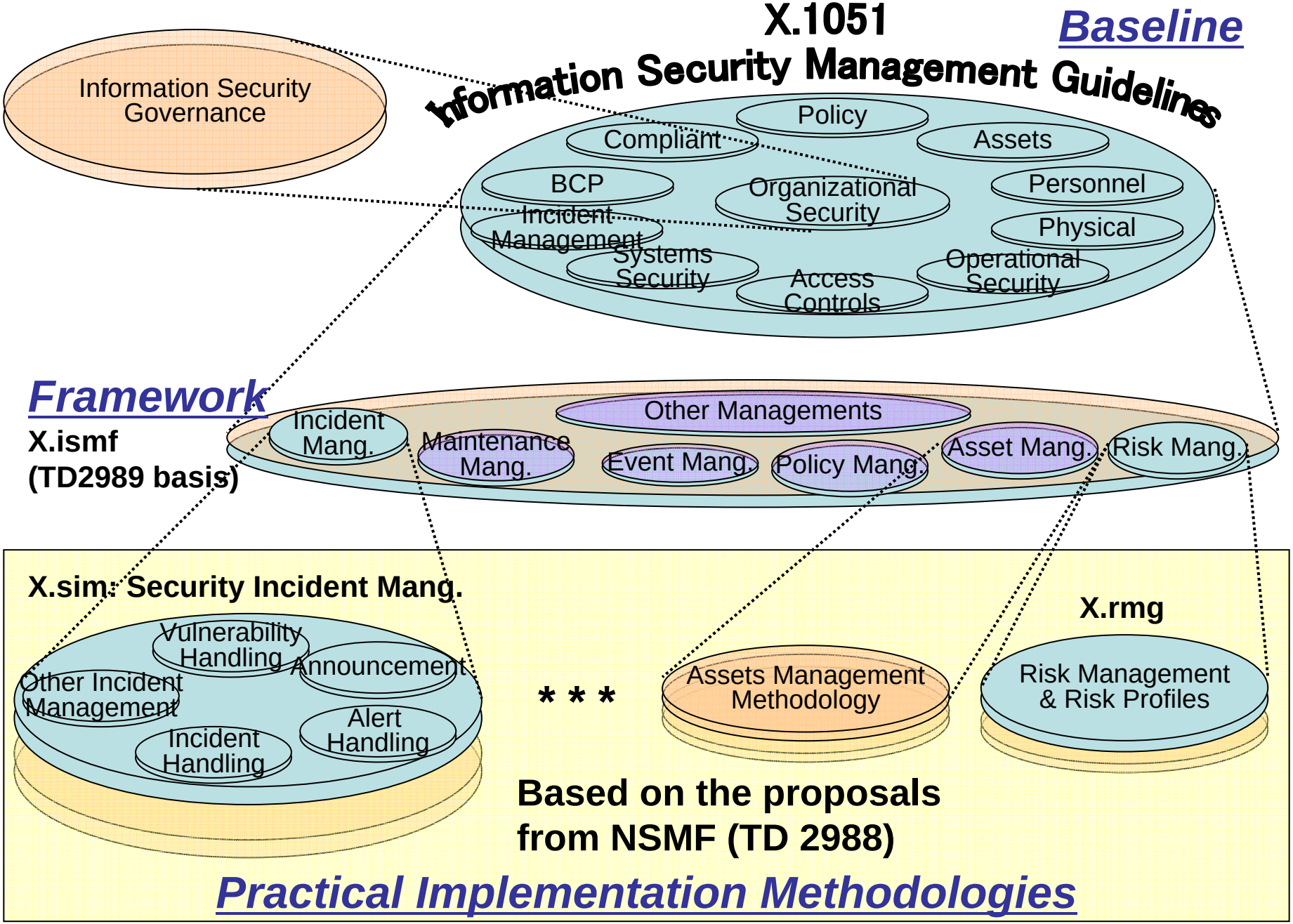
改版勧告X.1051の策定アプローチ



ISO/IEC 17799 (2005)

Revised X.1051

Existing X.1051



課題7（セキュリティマネジメントの課題）の全貌

その他の勧告例

テレバイオメトリクス関連

SG 17: X.1081 - The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics

SG 17: X.1082 - Telebiometrics related to human physiology

SG 17: X.1083 - Information technology – Biometrics – BioAPI interworking protocol

SG 17: X.1084 - Telebiometrics system mechanism – Part 1: General biometric authentication protocol and system model profiles for telecommunications systems

SG 17: X.1088 - Telebiometrics digital key framework (TDK) – A framework for biometric digital key generation and protection

SG 17: X.1089 - Telebiometrics authentication infrastructure (TAI)

ホームネットワーク関連

SG 17: X.1111 - Framework of security technologies for home network

SG 17: X.1112 - Device certificate profile for the home network

SG 17: X.1113 - Guideline on user authentication mechanisms for home network services

モバイルセキュリティ関連

SG 17: X.1121 - Framework of security technologies for mobile end-to-end data communications

SG 17: X.1122 - Guideline for implementing secure mobile systems based on PKI

SG 17: X.1123 - Differentiated security service for secure mobile end-to-end data communication

SG 17: X.1124 - Authentication architecture for mobile end-to-end data communication

SG 17: X.1125 - Correlative Reacting System in mobile data communication

セキュリティ言語関連

SG 17: X.1141 - Security Assertion Markup Language (SAML 2.0)

SG 17: X.1142 - eXtensible Access Control Markup Language (XACML 2.0)

サイバーセキュリティ

SG 17: X.1205 - Overview of cybersecurity

SG 17: X.1206 - A vendor-neutral framework for automatic notification of security related information and dissemination of updates

SG 17: X.1207 - Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software

SPAM**関連**

SG 17: X.1231 - Technical strategies for countering spam

SG 17: X.1240 - Technologies involved in countering e-mail spam

SG 17: X.1241 - Technical framework for countering e-mail spam

役に立つ web resources

- ITU Global Cybersecurity Agenda (GCA)
  http://www.itu.int/osg/csd/cybersecurity/gca/
- ITU-T Home page http://www.itu.int/ITU-T/
- Study Group 17 http://www.itu.int/ITU-T/studygroups/com17/index.asp
  e-mail: tsbsg17@itu.int
- LSG on Security http://www.itu.int/ITU-T/studygroups/com17/tel-security.html
- Security Roadmap http://www.itu.int/ITU-T/studygroups/com17/ict/index.html
- Security Manual http://www.itu.int/publ/T-HDB-SEC.03-2006/en
- Cybersecurity Portal http://www.itu.int/cybersecurity/
- Cybersecurity Gateway http://www.itu.int/cybersecurity/gateway/index.html
- ITU-T Recommendations http://www.itu.int/ITU-T/publications/recs.html
- ITU-T Lighthouse http://www.itu.int/ITU-T/lighthouse/index.phtml
- ITU-T Workshops http://www.itu.int/ITU-T/worksem/index.html

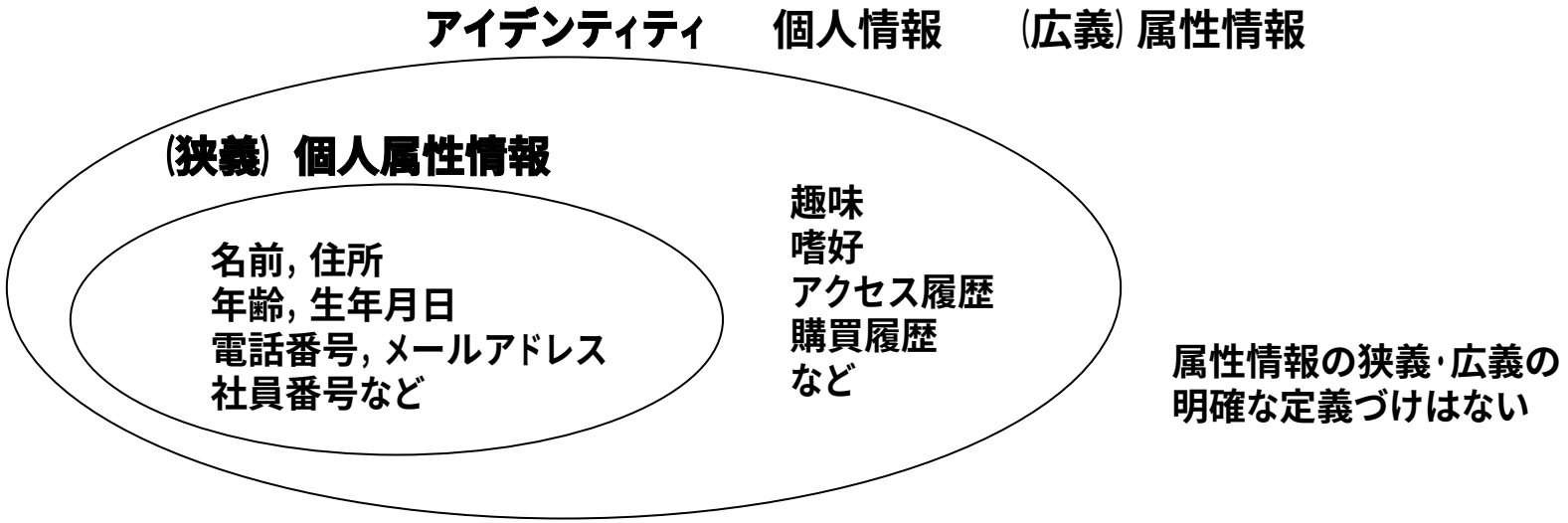
ITU-Tにおける ID管理の状況
～ ITU-T SG13とFG-IdMを中心に ～

日本電気株式会社　江川　尚志　様のご協力により

ID**管理**(IdM)**とは何か**

アイデンティティ（人）とは

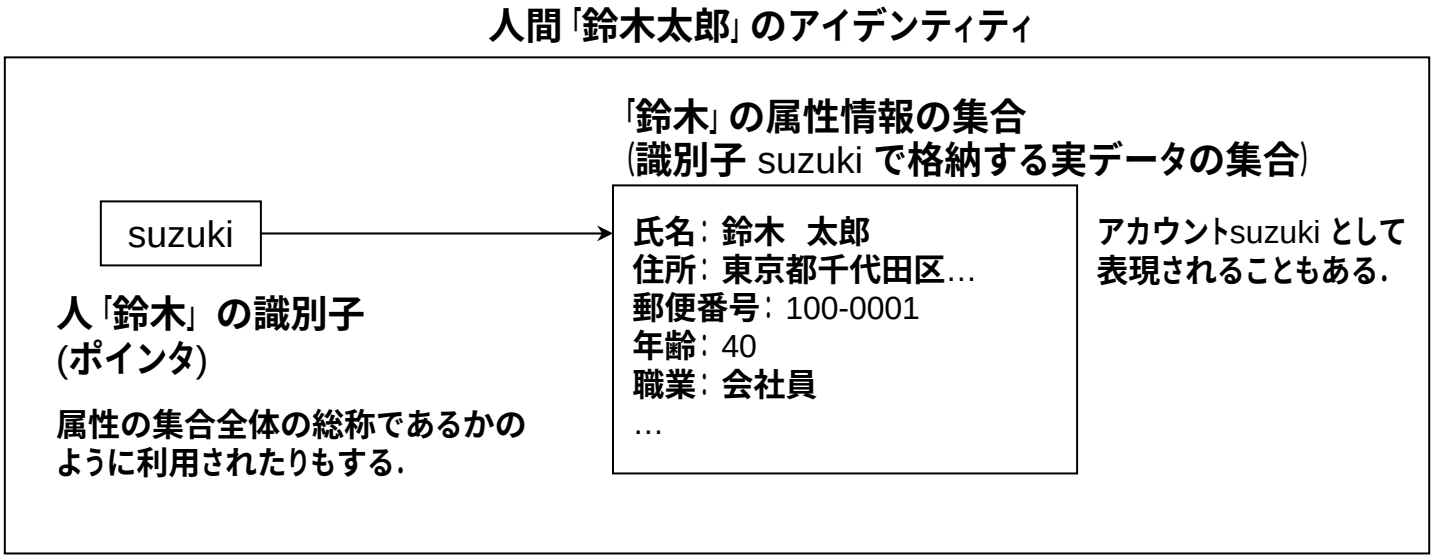
- 個人を特徴付ける属性情報の集合
  - （狭義）属性情報：
    - 名前，住所，電話番号，メールアドレス，その他
  - （広義）属性情報
    - 趣味，嗜好，アクセス履歴，その他



＊アイデンティティ管理では，主に「人」のアイデンティティが対象．
（ただし，人と関連付けられる「物」もアイデンティティの1つ．
従って「物」の情報化が主であるNIDとは直接には競合しない（注意は必要））

IDの2つの定義

- 一般に，人の IDは以下の両方の省略形として利用されることが多い．
  - Identity (アイデンティティ) → 「アイデンティティ管理」と呼ばれる領域
    - 上記，Identifierを包括した，人の属性情報の集合 (既出)
  - Identifier (アイデンティファイア：識別子)
    - アイデンティティへの参照情報 (ポインタ)．
      - いわゆる”ID/Password” のIDはこれに相当．
    - 本「識別子」という意味で用いながらも，その管理対象である「アイデンティティ」を指すこともあり．



＊「ID管理」という時，”Identity” なのか “Identifier” なのか注意が必要．

アイデンティティ管理の対象領域

アイデンティティ管理（広義）

アイデンティティ管理(狭義)

- **プロビジョニング**
  アカウントの配布
- **アカウント管理**
  アカウントの登録，削除，停止，再開など
- **クレデンシャル管理**
  パスワード，証明書の登録，発行など

アクセス管理

- **認証管理**
  所定の認証方式で認証
- **権限管理**
  権限情報の登録，削除，変更など
- **アクセス制御**
  権限を基にアクセスの認可判断を決定

アカウンティング管理

- **ログ管理**
  アクセスなどの証跡の収集と保管

ネットワークの発展に伴う
対象領域の拡大．
アイデンティティ情報をオン
ラインで動的に交換，連携
する機能へ．

近年の標準化の対象

- **アイデンティティ連携**
  パートナ間でアイデンティティ情報を関連付け
- **認証連携**
  組織をまたがるシングルサインオン
- **(一括) プロビジョニング**
  アカウントの配布機能の拡張
- **属性情報交換**
  信頼するパートナ間で属性情報の共有

技術の範疇外だが必要な領域

- **トラスト管理**
  情報を交換する相手同士の信頼関係の確立
- **コンプライアンス**
  法制，規制への準拠

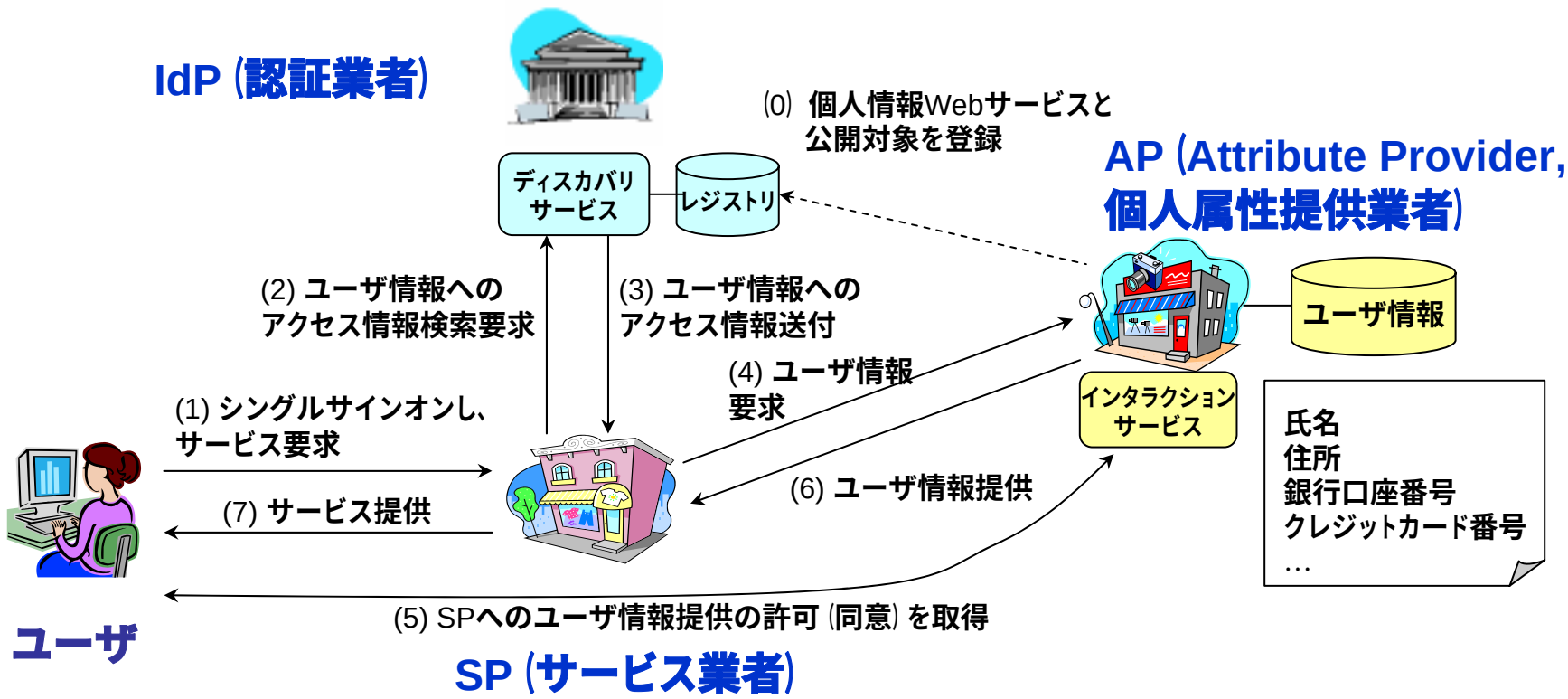
いわゆる古典的な
AAA (Authentication, Authorization, Accounting)

* 識別子管理は，全ての要素に関連

ID管理の例：Liberty ID-WSF

個人情報の安全な交換と活用

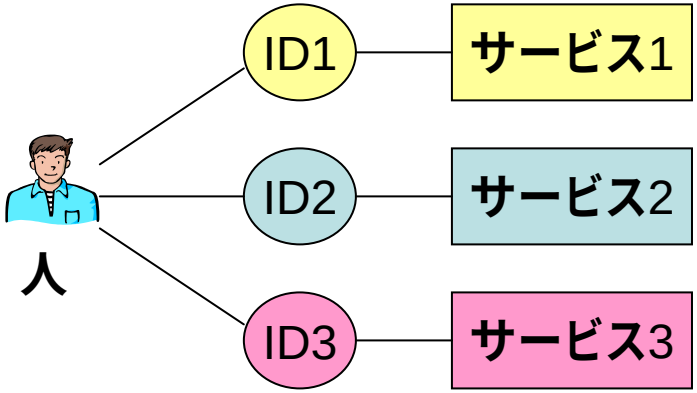
- サーバに登録されている個人情報をサービス業者間で直接交換し、ユーザのサービス登録や利用時の手間を省いたり、サービスのパーソナライズを図る。



*ID-WSF: Identity Web Service Framework

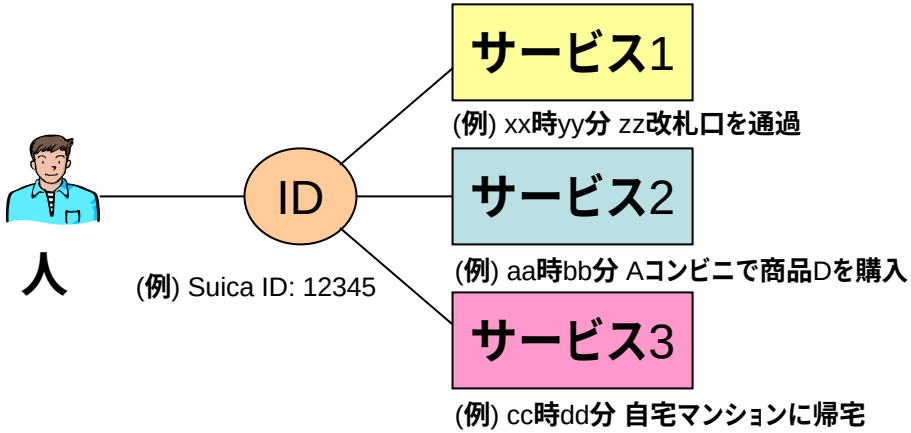
ID管理の課題例: トラッキングによるプライバシ漏洩

- ローカルID (識別子)
  - 有効範囲が限定的で、独立性が高い



・各IDは、人の各サービスにおける行動しか追跡できないので、
プライバシ漏洩リスクは低い

- グローバルID (識別子)
  - 有効範囲が広く、独立性が弱い



・共通化されたIDは、人の全てのサービスにおける行動を追跡可能とし、プライバシ漏洩リスクは高い
・ID自体がランダムな番号であっても漏洩リスクは同じ
・いずれかの情報から本人確度が高くなると全ての情報が本人と関連付けられてしまう

cf) http://java-house.jp/%7Etakagi/paper/iccard-world-2004-takagi.pdf

ID管理の基本目標: 第1回FG-IdM会合より (1)

通信事業の価値の源泉は、人々を結びつけることにある。
「私の娘は、Skypeで友達の家と常時接続し、空間を共有している。
これはもはや電話の置き換えではないのだ。
新しいSocial Networkのツールであり、ここに通信の価値がある」
(Lee Dryburgh, Bittech社　社長)
では、誰と誰を、いつ、どのような手段で結びつけるべきか？

- 解くべき課題
  - 属性を広告 (advertise) する方法
  - 広告されている属性を見つける方法 (discovery)
  - 強固な認証との結合(MSISDN, E.164, 名前、住所等)

「隣の寿司屋」で通信が出来るようにする方法は？
「この技術課題の解決法を知っている人間」を見つける方法は？

ID管理の基本目標: 第1回FG-IdM会合より (2)

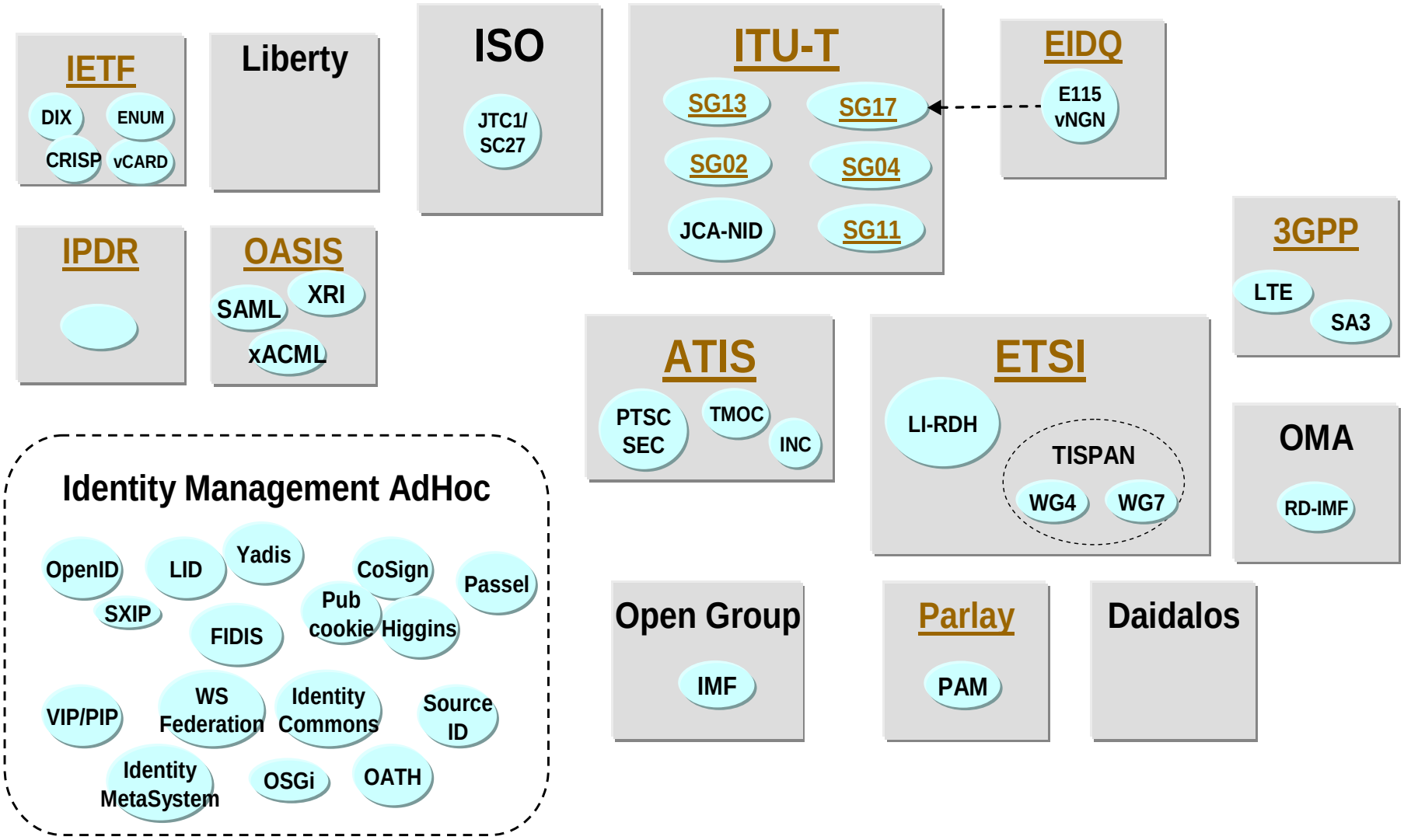
- 通信オペレータが持つ能力
  - 地理的位置情報の特定
  - コンタクトのためのIDや属性の特定
  - IDをSIM等で「アンカー」すること
  - ユーザ情報の提供 (ホーム/オフィス、利用端末、移動速度など)
  - ユーザのネットワーク (バディリストなど)の保管と広告

これらを、プライバシを守りつつ管理し、コンテキストに合わせて利用可能とすることがID管理の目標

GoogleのFON (無線LANホットスポット) への出資 (2006/02)

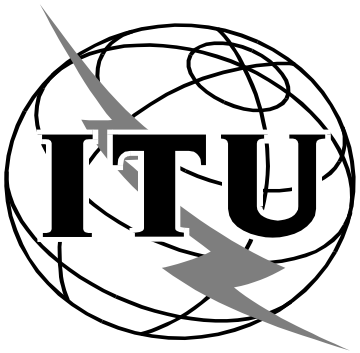
無線LANへの接続を用いてユーザの位置情報を把握し、それに基づくターゲット広告を行うシステムを確立するためとの憶測あり

アイデンティティ管理関連団体



* ITU-T Y.IdMsec仕様 から抜粋

ITU-Tにおける ID管理検討の現状
ーSG13及びSG17ー



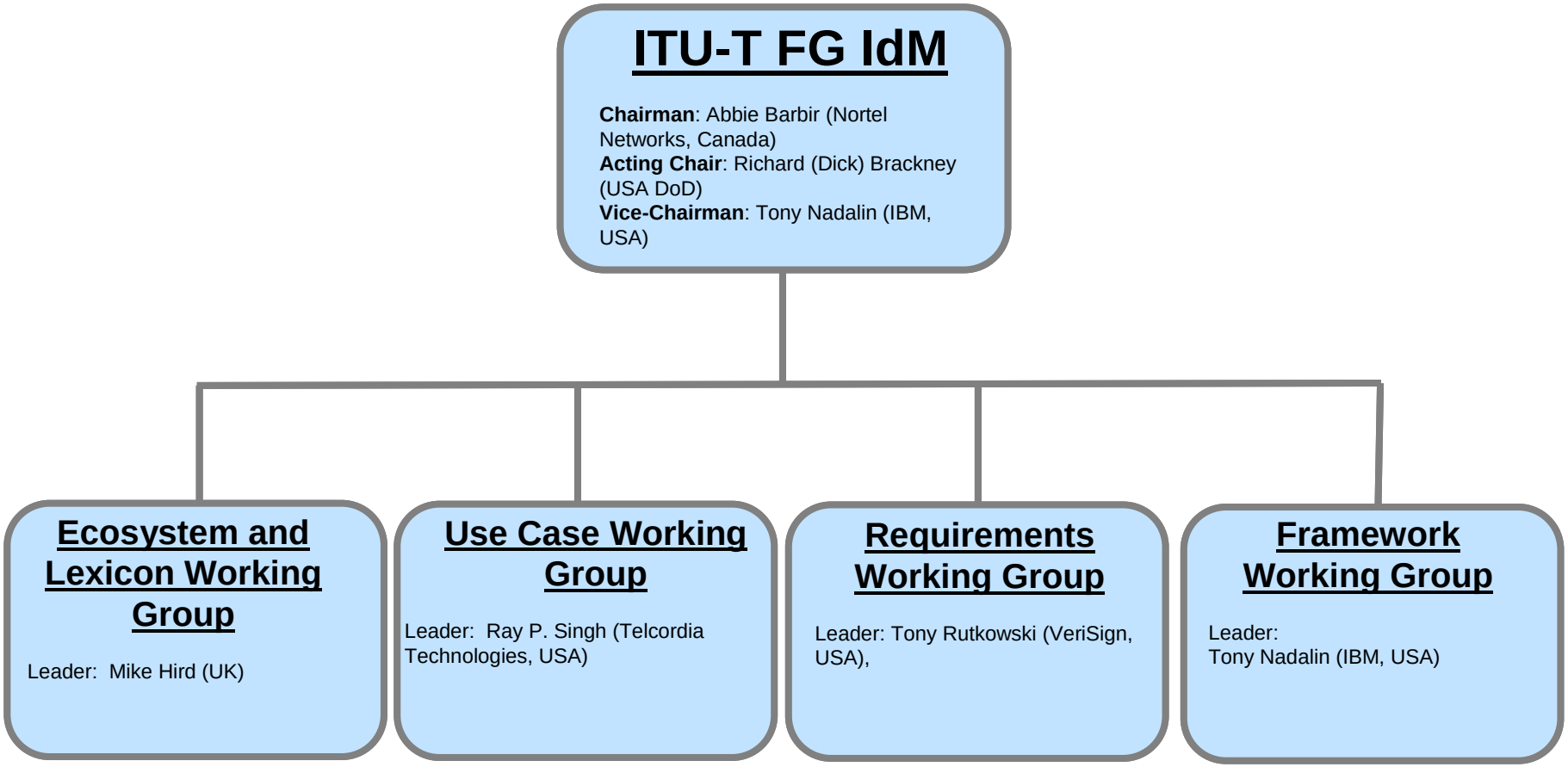
ITU-Tでの ID管理検討

- SG13 Q15 (NGN security)
  NGNでのIdM (Identity Management) を規定するY.IdMsec (NGN Identity Management Security) を2006年10月より検討
- FG-IdM (Focus Group on Identity Management)
  SG17配下で2007年2月よりIdM全般を検討

  これら2つの活動の中心人物はいずれも米国国防総省(DoD)のRichard (Dick) Brackney氏 (ISO/IEC JTC1 SC27 WG5の中心人物でもある)

- (JCA-NID)
  RFID等のタグとそれを支える網機能を検討
  (モノの情報化)

FG IdM – FG IdM 組織構造



FG-IdM: WG構成とリーダー

- 議長: Abbie Barbir (Nortel, カナダ); SG17 Q6ラポータ
- 副議長 Dick Brackney (DoD, 米); Y.IdMsecエディタ
- 副議長 Tony Nadalin (IBM、米); Higginsプロジェクト関係者

- Use Cases Working Group (ユースケース)
  - Sergio Fiszman (Nortel, 加)
  - Ray Singh (Telcordia, 米); Q15/13関係者
  - Mike Jones (Microsoft、米); Card Space関係者
  - David Recordon. (Verisign、米); Open IDの中心人物
- Requirements Working Group (要求条件)
  - Tony Rutkowski (Verisign、米); 弁護士、FCCやITUの役職を歴任
  - Jiwei Wei (Huawei Technologies、中); Q9/17副ラポータ
- Framework Working Group (フレームワーク)
  - Tony Nadalin (IBM、米); Higginsプロジェクト関係者
  - Amardeo Sarma (NEC、独); Daidalosプロジェクト関係者、元SG10議長
- Living List and Lexicon Working Group (他の活動調査および用語集)
  - Mike Hird (英); 商務省のコンサルタント; 用語集担当
  - Kaliya Hamlin (Identity Woman、米); Open Space担当のコンサルタント、他団体の調査担当
  - Karen Mulberry (Neustar, 米); SG2関係者

FG-IdM: ユースケースWG

- ユースケースを集めて分析し、以下の分野についてその問題の概要、基本的な情報の流れを示したダイアグラム、必要とされる要求条件と能力、既存の解決手法、本FGが取り組むべき既存の手法の抜け(gap) を記述
  - ID資源のディスカバリ
  - ID資源のフェデレーション間・Circle of Trust間相互運用性
  - 情報交換に用いる機構の相互運用性
  - IDの確からしさの尺度の相互運用性
  - 透明性と通知
  - 物の管理との統合
  - ID管理のセキュリティとアイデンティティ・パターン
  - トークンの変換
  - 静的なトラストモデルと動的な選択
  - 権限委譲
  - メタデータモデル
- 実際には、最初の7項目のみ作業が進み、報告書が完成している

FG-IdM: **要求条件**WG

- **ユースケースの分析と、法的な枠組みに基づき下記を作成**
  - **各種**IdM**に共通な要求条件**
    前提とするアーキテクチャモデル、プロビジョニング、ディスカバリ、ID**プロバイダ間やプロバイダのフェデレーション間での相互運用性、監査、脅威とリスクの軽減、パフォーマンス、信頼性、可用性**
  - **要求条件を実現する上で現在欠けているソリューション**
    共通的なIdM**アーキテクチャモデルと**IdM**レイヤ、グローバルなディスカバリ、グローバルな**ID**サービスの相互運用性、グローバルな**ID**保証** (identity assurance) **の相互運用性、透明性と通知、オブジェクト管理との統合、異なる法制度間での要求条件の違いの調停**
- **現在の完成度は低く、今後の更なる検討が必要。**

フレームワークWG

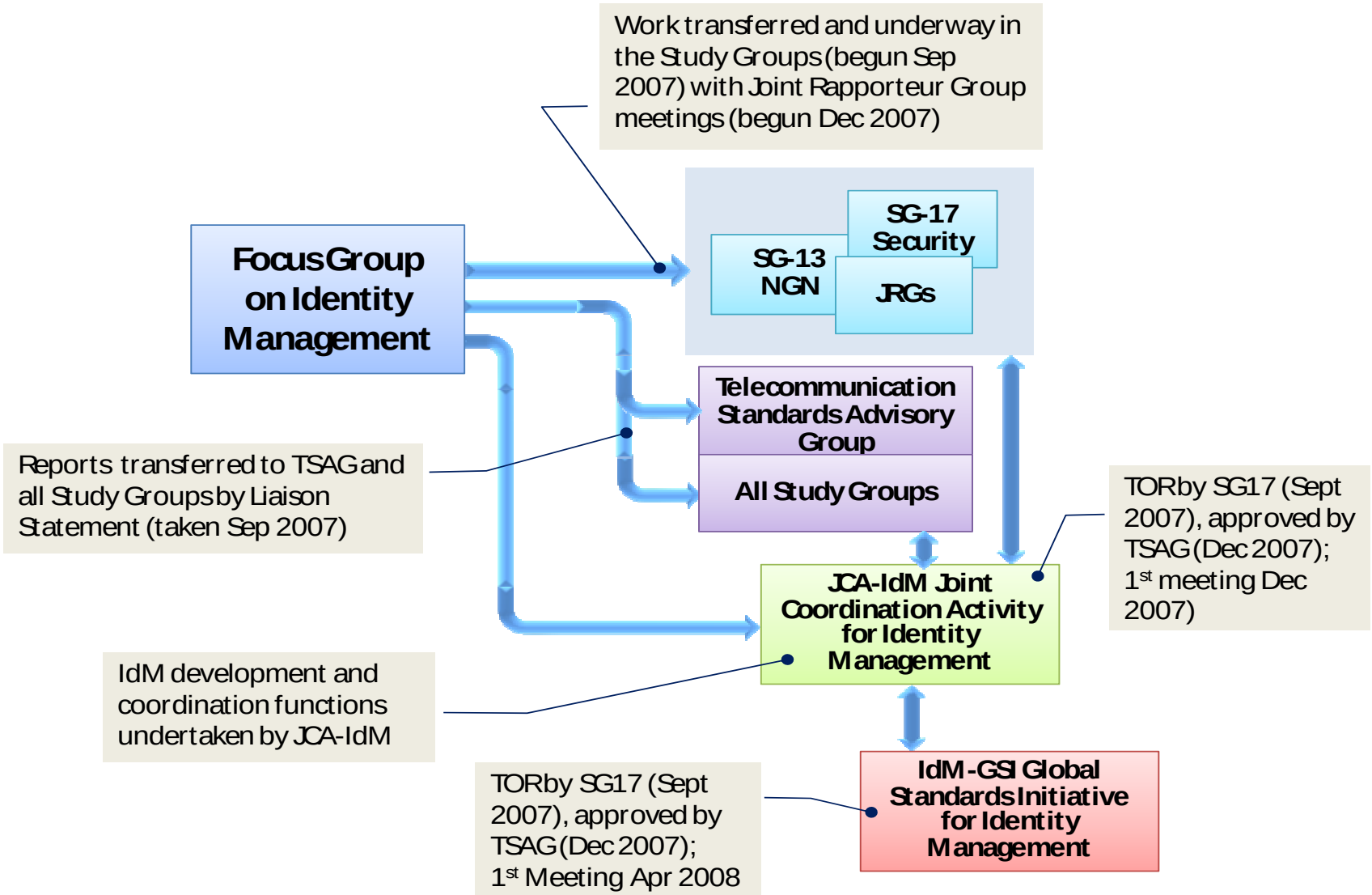
- ユースケース分析に基づき、IdMのアーキテクチャや必要な能力を分析、記述
- まだユースケース分析が完了していないためペンディング中
  - 第1回会合のフリーディスカッションをまとめたメモのみ
- アーキテクチャ
  - 各種IdMフレームワーク間でのディスカバリ、ID情報交換等の相互運用性に配慮つつ機能ブロック図を作成
- 各種IdMフレームワークの不足 (gap) を分析し、必要な機能を記述。必要な機能としては下記を想定。
  - 典拠のあるディスカバリやID情報の交換 (保証の尺度を含む)
  - エンティティの証明書、識別し、属性やバインディングなど
  - IDプロバイダやプロバイダのフェデレーション間での特権管理の相互運用性
  - ID管理に伴う脅威とリスク、およびその軽減策

Lexicon and Ecosystem WG

- **用語の定義** (lexicon)
  - **定義が合意できた用語**(terminology) **と合意できていない用語** (lexicon) **についての文書を作成**

- **他の**ID**管理の団体との関係を整理** (ecosystem)
  - **現在調査済の団体**: ITU-T, 3GPP, IETF, ISO, Liberty Alliance, OASIS, OMA, W3C, ETSI TISPAN, FDIS, Guide, Higgins, **その他各種業界団体など**26**団体**

ITU-T における今後の活動



IdMの今後の展望

技術的な重要課題として、アクセス管理（制御）を含めた、Identityの管理に関わ技術が注目されており、ITU-T、及びISO/IECで精力的に取り組まれつつある。

＜標準化の方向＞　→　今後の認証基盤の確立に影響

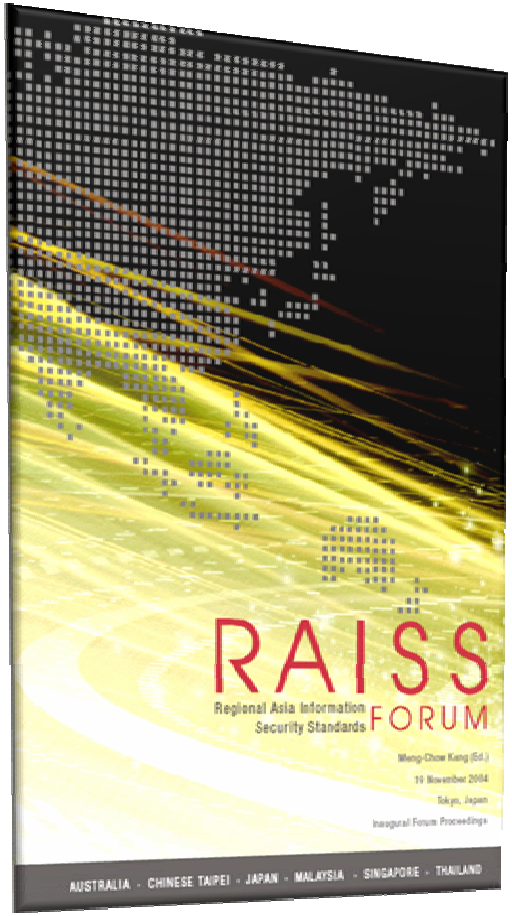
- アイデンティティ連携
  パートナ間でアイデンティティ情報を関連付け
- 認証連携
  組織をまたがるシングルサインオン
- （一括）プロビジョニング
  アカウントの配布機能の拡張
- 属性情報交換
  信頼するパートナ間で属性情報の共有

IdM技術は、今後のいろいろな技術と何らかの関係を保有していくことは間違えないと考える。　→　今後の日本のしての対応の精査、戦略が要

その他の活動
RAISS及びSWIS

RAISE Forum
Regional Asia Information Security Exchange

- Inaugural meeting held Nov 19, 2004 in Tokyo
- 2nd meeting held in June 27/28, 2005 in Singapore
  - Day 1 – Workshop on ISO/IEC 17799:2005(E), by Ted Humphrey & Angelika Plates
  - Day 2 – Forum meeting with regional presentations and projects discussion
- 3rd meeting held on Nov 12, 2005 in Kuala Lumpur, in conjunction with ISO/IEC/JTC1/SC27 Meeting
  - Parallel tracks on four projects
    - Security Standards Toolkit
    - Mutual Recognition
    - Application Security Standards
    - Security Assessment Guides
- 4th meeting on April 21, 2005, Jeju, Korea
- 5th meeting on October 4-5, 2006, Tokyo
- 6th meeting on August 22-23, 2007, Singapore
- 7th meeting on July 17-18, 2008, Kuala Lumpur
- http://www.itsc.org.sg/raiss.html



Security Standardization

- Security standards organization
  - Australia, China, India, Japan, Malaysia, South Korea, Singapore, Thailand, Chinese Taipei
- Localized and local security standards
  - Australia, Japan, Malaysia, South Korea, Singapore, Thailand, Chinese Taipei
  - Most common standards – ISO/IEC 17799 and BS 7799-2

Projectsと最近の関心

- Security Standards Toolkit：IPAベンチマークも考慮
- Application Security and Certification Framework
- Mutual Recognition of Local Security Certification
- Security assessment guides for Network and Systems Security Administrators
- Business Continuity and Disaster Recovery Services Standards Deployment（ISO規格と関係）
- **最近の関心としては、「情報共有フレームワーク」、「既存規格と現状のギャップを埋めるガイドライン」等**

SWIS会議（CJK-セキュリティ標準化会議）

- 日中韓の連携により、国際標準の推進を行うことが目的
  （議長：Chen（中国）、Youm（韓国）、中尾（日本））
- 現在、2回開催されている
  第1回：2007年11月（韓国、ソウル）
  第2回：2008年12月（日本、東京）
  第3回：2009年11月（中国、北京）　→　予定
- 参加者は、日中韓のセキュリティ標準化専門家、及び
  大学関係者
- 第2回のトピック
  ＊トレースバック技術
  ＊ボットネット対策
  ＊IdM技術
  ＊IPTV技術
  ＊第3世代携帯技術（情報提供のみ）
- 今後は、CJK正式会合でのセキュリティWGの成立に向けて
  検討を進める予定。

今後の国際規格化、国際連携への取り組み

国際標準化活動への力点

- ISO/IEC JTC1/SC27：**セキュリティ基盤技術**
- ITU-T　SG17：
  通信事業者のためのセキュリティ技術
- ITU-D：**発展途上国　(活動が活性化しつつある)**
- IETF：**インターネット系技術**
- RAISE：ISO/ITU-T**とアジア諸国の橋渡し**
- SWIS：CJK**からみた**ISO/ITU-T**への橋渡し**

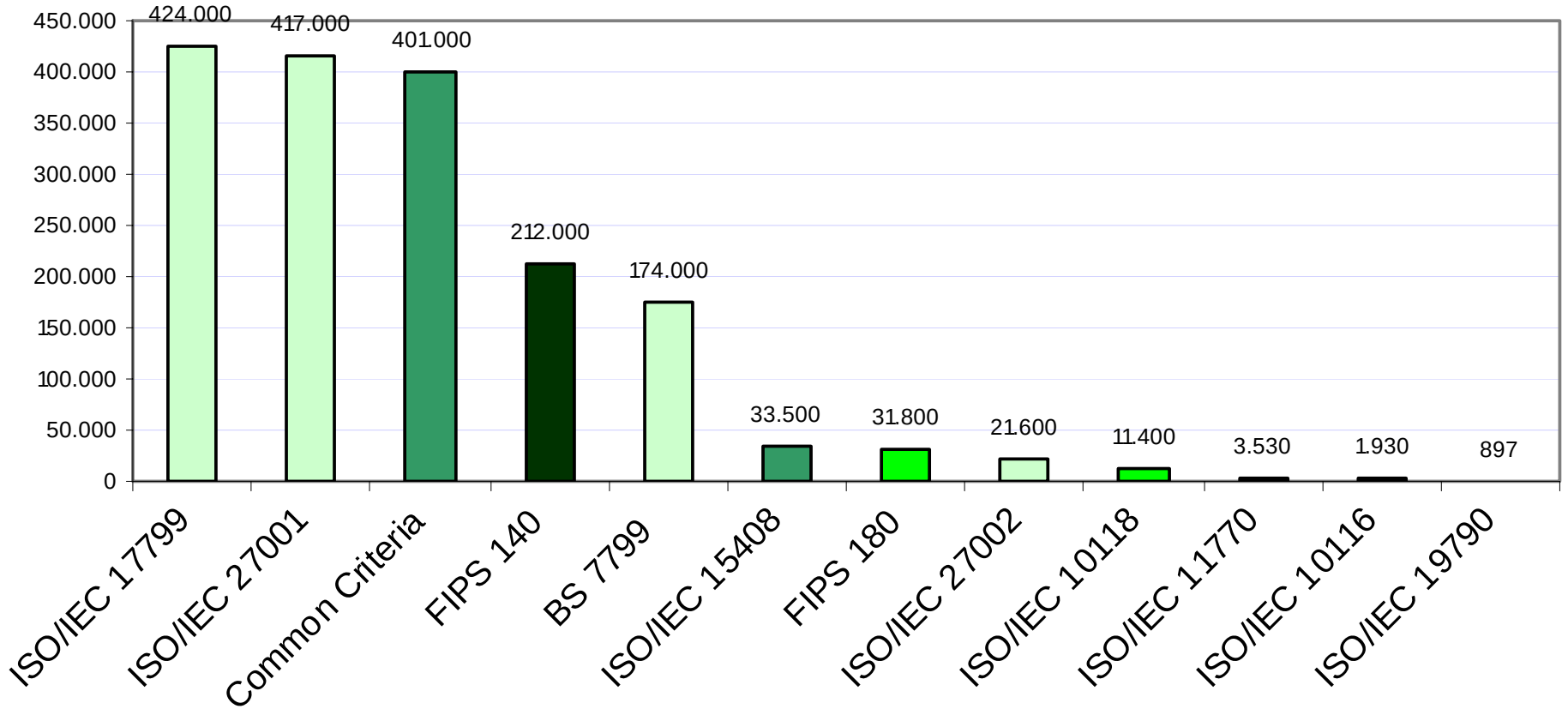
標準は使われなくては意味がない、使う人との初めからの連携が必要！

最近の流れ･方向性（1）

- 基軸となる「技術」の標準化は必要
- ISO、及びITU-Tの活動はボランティア的、規格が本当に使われるのか、規格のユーザ（利用者）の意思が重要
- 流れとして
  「どのように脅威に対向するか」の命題
- **連携の仕方、意識向上のための施策**などの検討が新たな国際規格化のミッションに追加され始める
- ITU-Dの施策は米国などが牽引しているが、これまでと異なる方向性

Popularity of Selected Security Standards

(Google Hits 2008-04-07)



最近の流れ･方向性 (2)

- ISO:サイバーセキュリティに関するガイダンスを構築中 (連携などを焦点に)
- ITU-T：同様な連携の骨組みのガイドラインを作成中
- RAISS、SWISなどでその連携を実践すべき
- たとえば、
  トレースバック問題、セキュリティ情報共有問題、重要インフラのセキュリティなど、多くの話題が抽出されている

最近の流れ･方向性 (3)

- 国際標準化は、完全に
  ＊1　「積極的に参加、検討をする国」
  ＊2　「文句ばっかり言う国」
  ＊3　「自分では貢献しないが、結果のみに
  　　興味がある国」
  に分類される。
- 日本は、一応＊1であり、＊1であるべき。すなわち、技術規格化の推進には積極的。ただし、「連携の旗振り」については超下手。

- どのように連携し、効率的、効果的な標準を作ることができるかは、不透明。
- 会議の数が多すぎる、Face-to-Faceでないと進まない･･･など、問題山積
- ITU-Tでは、セキュリティコラボレーションチームを結成する計画を進めたが失敗。原因は、ボランティアベースなので、余計なコラボはする時間がない (専門家たちとして)

最近の流れ･方向性 (4)

- **規格に関わるトピックへの偏りが見られる**
- IdM、CyberSecurity**といったキーワードが見られると敏感になる。(米国、欧州は特に)**
  →　国際戦略と関係、ビジネスの匂いがする
- **事例1**
  ISMS**について、英国が戦略的に27001の世界的普及に成功。英国の認証ビジネスと連結**
- **事例2**
  進行中であるが、IdM**に関わるリソースの多くは米国が創出。政府、ベリサインなど･･･　具体的なビジネス展開、及び米国の戦略が見える (詳細は不明)**

今後の方向性 (1)

- 規格の性格分類を実施し、その中で戦略を練る必要あり
- 分類1：皆が共有すると嬉しい、個々の企業単位ではなく、
  団体、国のレベルの要求事項に依存
  例えば、「セキュリティ情報の共有体制（フレームワーク）」、
  「脅威への共同対策実施に関わる規格」など
- 分類2：国家的な施策となる規格、国の要求事項に基づく
  例えば、「ISMSなどのマネジメント規格（ガバナンスなどを
  含む）」、「プライバシー関連規格」、
- 分類3：企業など私的なビジネスに関係しやすい規格
  例えば、「IdM」、「バイオメトリクス」、「暗号系」
- 分類4：ガイドライン的で、皆が喜ぶ規格
  例えば、「セキュリティ教育系」、「セキュリティツール系」
- 分類5：どうでも良い規格　（ダメージ制御が必要！）

今後の方向性 (2)

- 日本としては、技術力の向上に加え、新しい国際標準化、及び国際連携の枠組みに向かって努力すべき。
- 国レベルの戦略の明確化が必要 (マネジメント系、ガバナンス、E-政府、重要インフラの整備・連携など)
- 団体 (例えば、Telecom-ISAC, JP-CERT/CC、IPAなど) は、関連する海外の団体との連携を図り、戦略的な規格策定の乗り出すべき。(情報共有、ボット対策連携、トレースバック対応連携など)
- 企業については、なかなか人的リソースを標準化に向けられない現状もあるが、企業の先見的なビジネス戦略に関わる規格を積極的に見出し、規格化をうまく活用すべき。
- 国際規格化団体 (ISOやITU-Tなど) だけではなく、ローカルな協議会、標準化会議への参画により、地域的な規格化から推進すべき。(RAISEやSWISはその手始め)
- 本当に意味のある、役に立つ規格つくりとその投資リターンがないと、今後の標準化人材は枯渇することは見えている。人材の確保は大きな問題。

事例：次世代の情報セキュリティ政策に関する研究会

研究会の開催

総務省において、昨年10月より「次世代の情報セキュリティ対策に関する研究会」を開催（座長 安田 浩 東京電機大学教授）3年から5年後の近い将来にむけて、変遷過程で生じる課題を抽出し、次世代の情報セキュリティ政策を検討

背景

課題

脅威の対象となる範囲の拡大（物、人）
- ネットワークにつながる機器、人、機会の増加

×

脅威の対象となる情報の増加・多様化
- 個人・企業情報がネットワークを流れる機会が増大
- 価値ある情報の流通が増加

＝

対策の困難性の拡大
- 将来脅威の予測が困難
- 対象の複雑な関連
- 脅威の高度化、潜行化

課題への対応

利用者を取り巻く環境における情報セキュリティ対策の徹底
- 利用者への普及啓発
- 電気通信事業者による対策

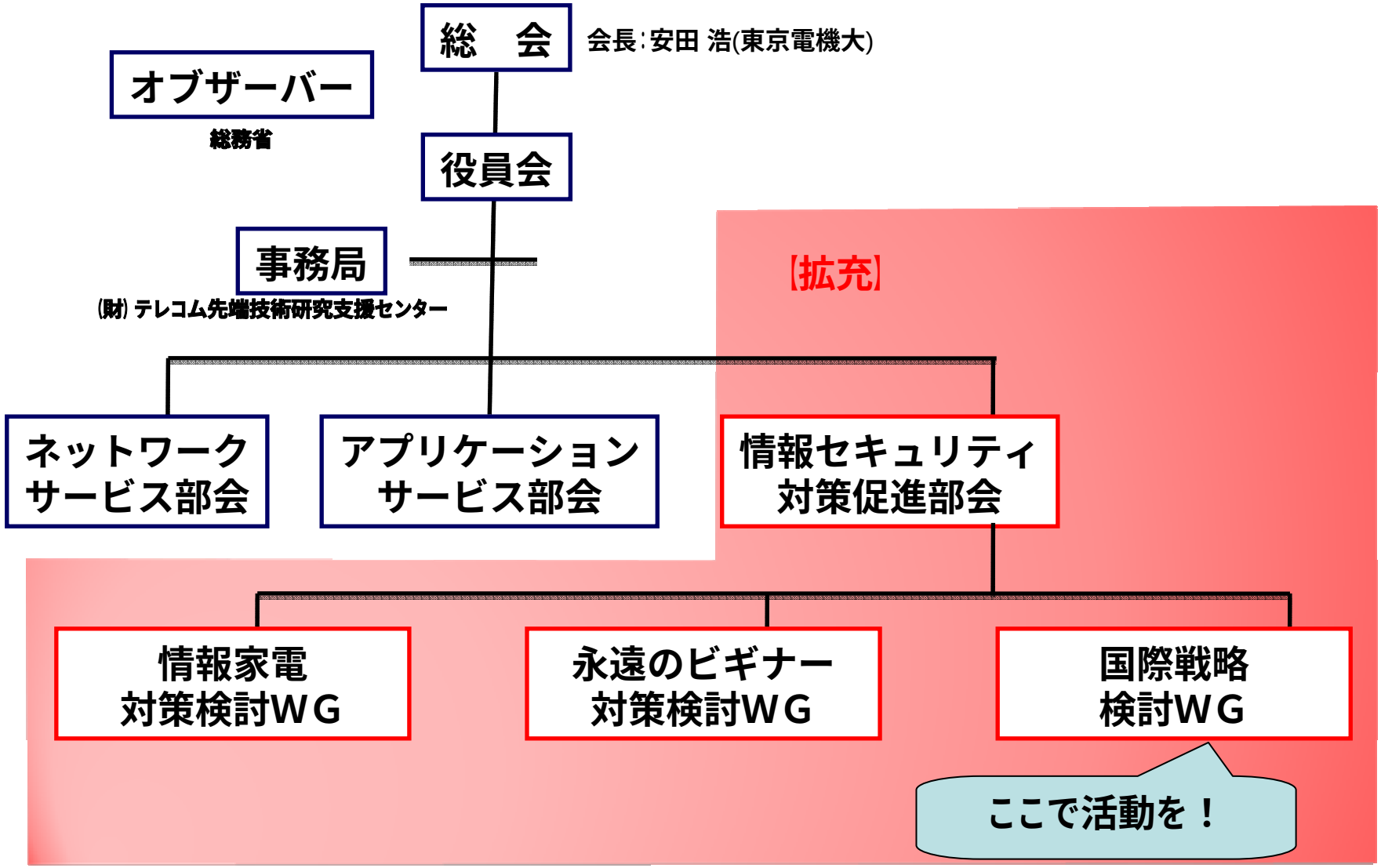
産学官連携による先進的な研究開発の実施
- マルウェア感染手法の巧妙化等への対策
- 新技術移行時の技術的課題への対策

情報セキュリティ対策に係る人材育成の推進
- 産学官が連携した人材育成の取り組み

関係機関における連携強化
- 業界横断的な検討体制の整備等
- 実行性のある情報共有体制の充実

安心・安全なグローバルICT環境の実現に向けた国際連携の推進
- 先進的技術開発による国際競争力の強化
- 国際動向の把握・プレゼンスの向上

例：安心・安全インターネット推進協議会



Thank you for listening Q&A