資料7－2

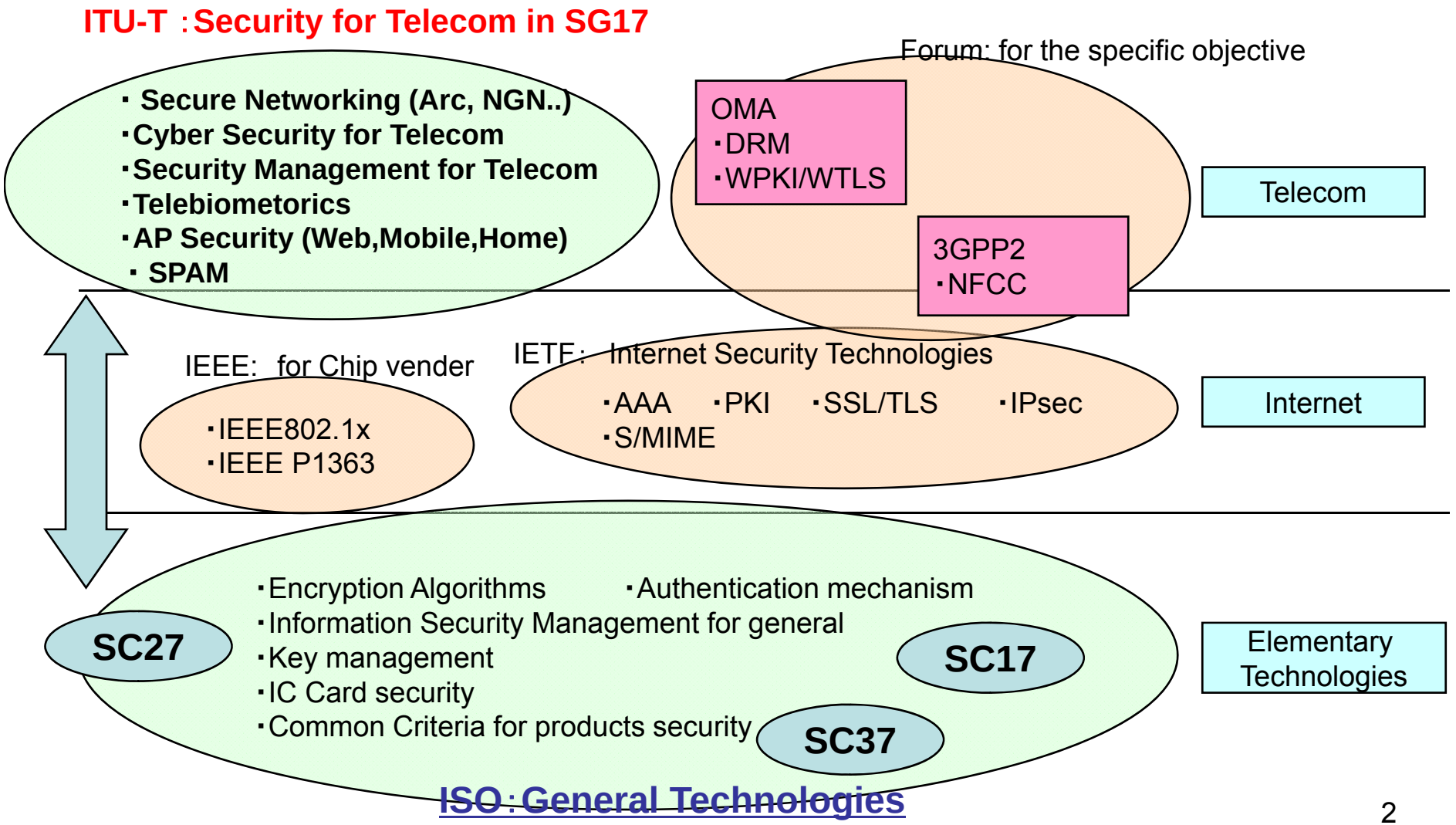
国際連携・協調について

(ISO/IEC SC27, ITU-T, ITU-D,
IETF, RAISS, etc)

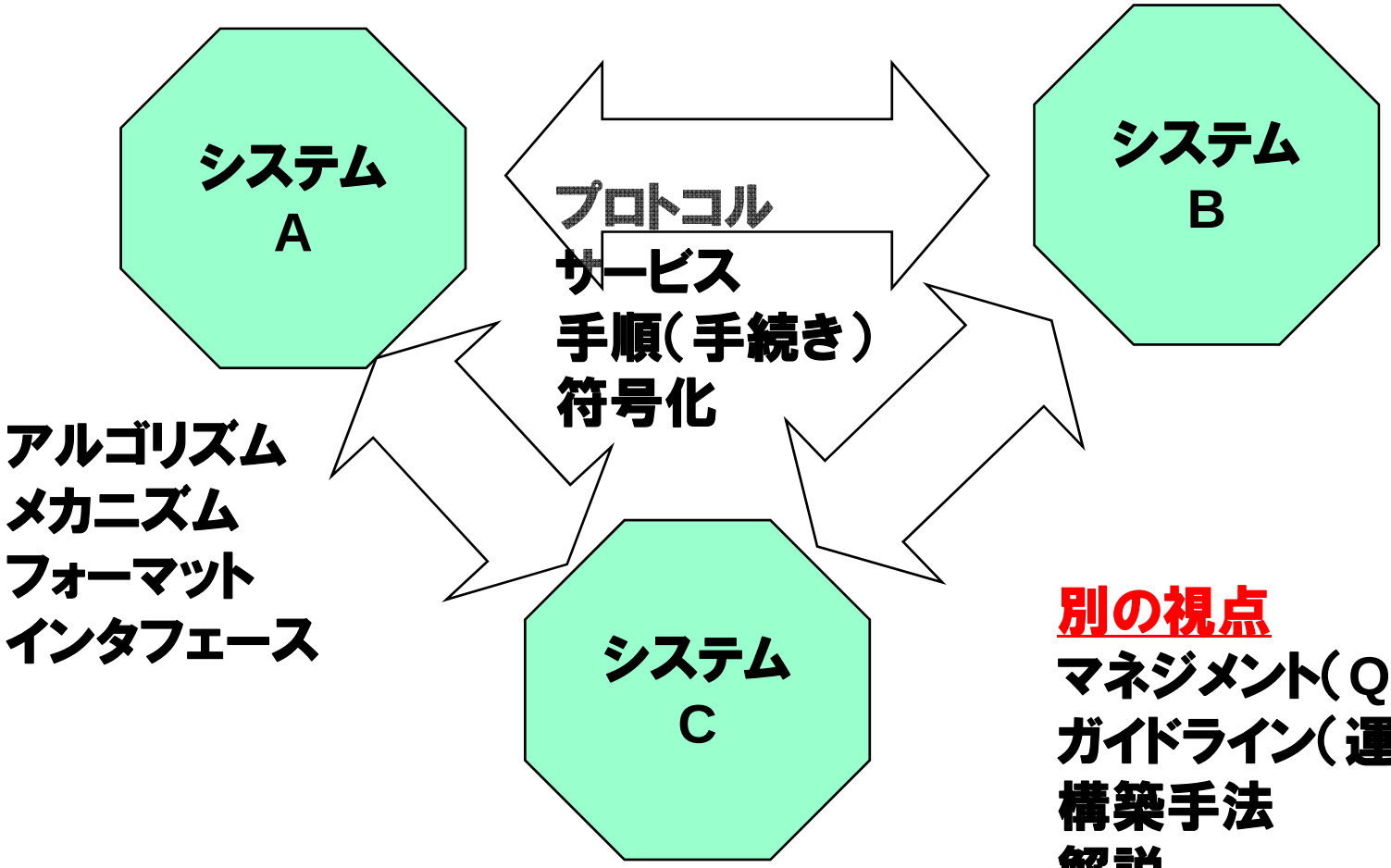
KDDI株式会社
中尾康二

国際標準化動向の全貌と意義

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

標準化の意義とトレンド

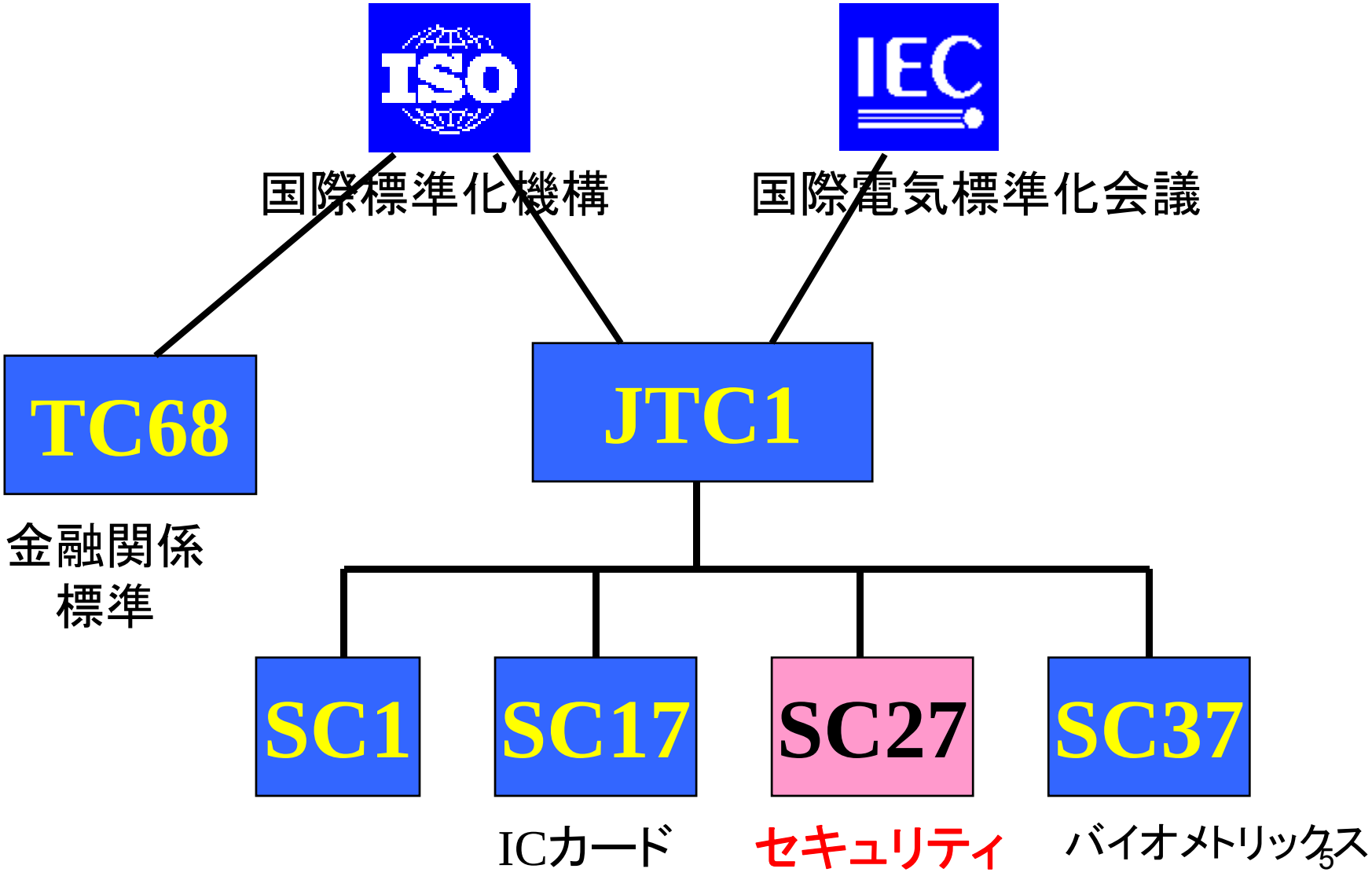


別の視点

マネジメント（QMS等）
ガイドライン（運用など）
構築手法
解説

ISO/IEC　SC27の標準化動向

ISO/IECの組織構造



SC 27 Membership =33 p members

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			South Africa	Kenya		
Korea		Ukraine	Malaysia	Austria	New Zealand	Uruguay
Australia	Poland	Czech Republic	India	Luxembourg	Singapore	Sri Lanka
1994	*1996*	*1999*	*2001*	*2002*	*2003*	*2005/06*
additional P-Members						

O-members 16:

- Argentina, Hong Kong, Indonesia, Belarus, Cyprus, Estonia, Hungary, Ireland, Israel, Lithuania, Serbia and Montenegro, Romania, Slovakia, Turkey

SC 27 のWG構成

WG1
ISMS Standards
Chair Ted Humphreys
Vice-Chair Angelika Plate

WG4
Security Controls & Services
Chair Meng-Chow Kang

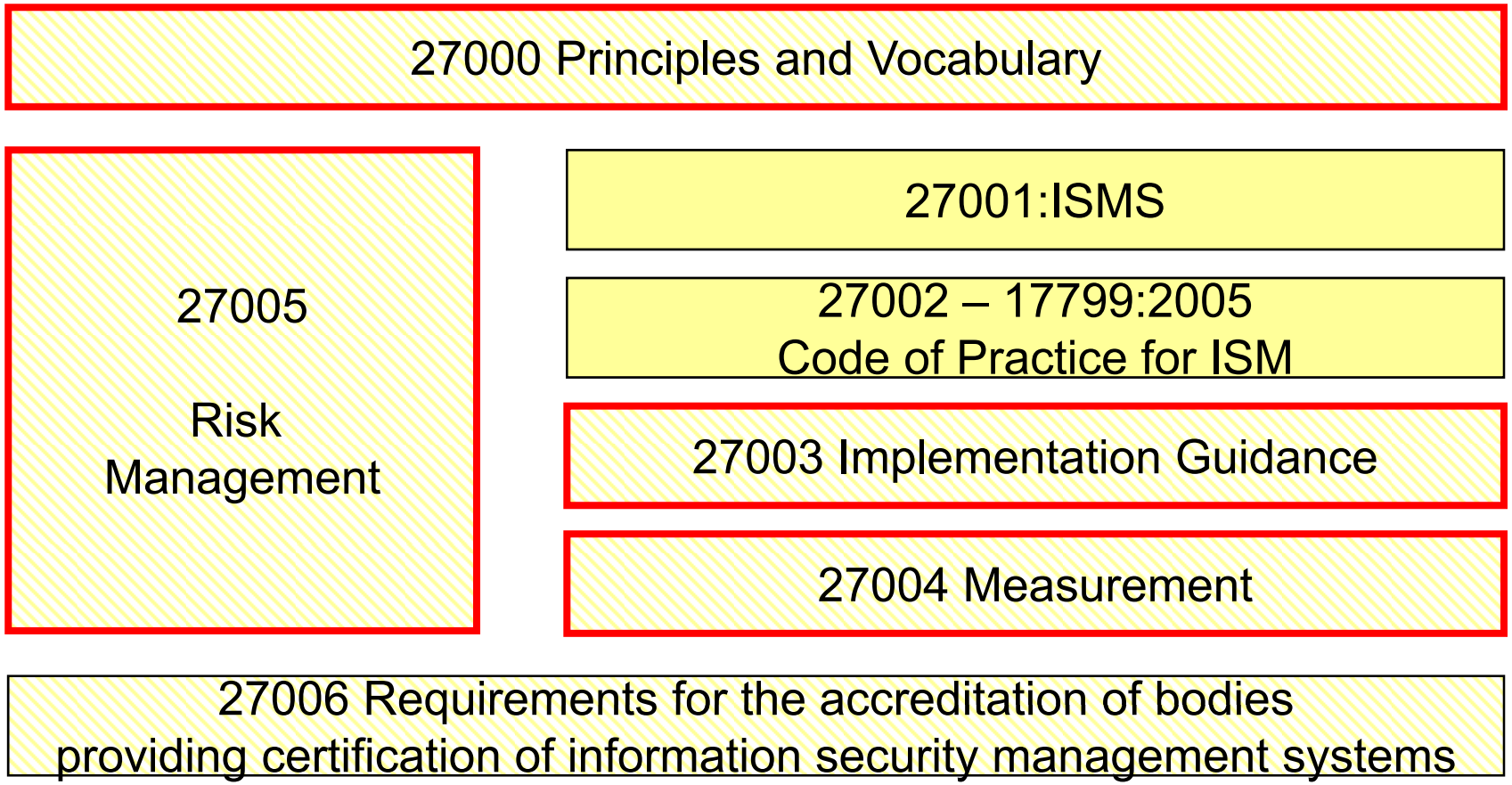
ISO/IEC JTC1 SC27
Chair Walter Fumy
Vice Chair Marijike de Soete

WG2
Security
Techniques
Chair Prof. K Namura

WG3
Security
Evaluation
Chair Mats Ohlin

WG5
Privacy Technology,
ID management
and Biometrics
Chair TBA

WG1：Structure of the Standards



これらは、ISMS　要求事項（27001）、およびその実施において、それらをサポートし、付加価値を与え、何らかの形で貢献するための規格群を27000シリーズ規格と呼ぶ。

SC27/WG2会議の主な審議規格

SC27 WG2 **国内委員会から提供**

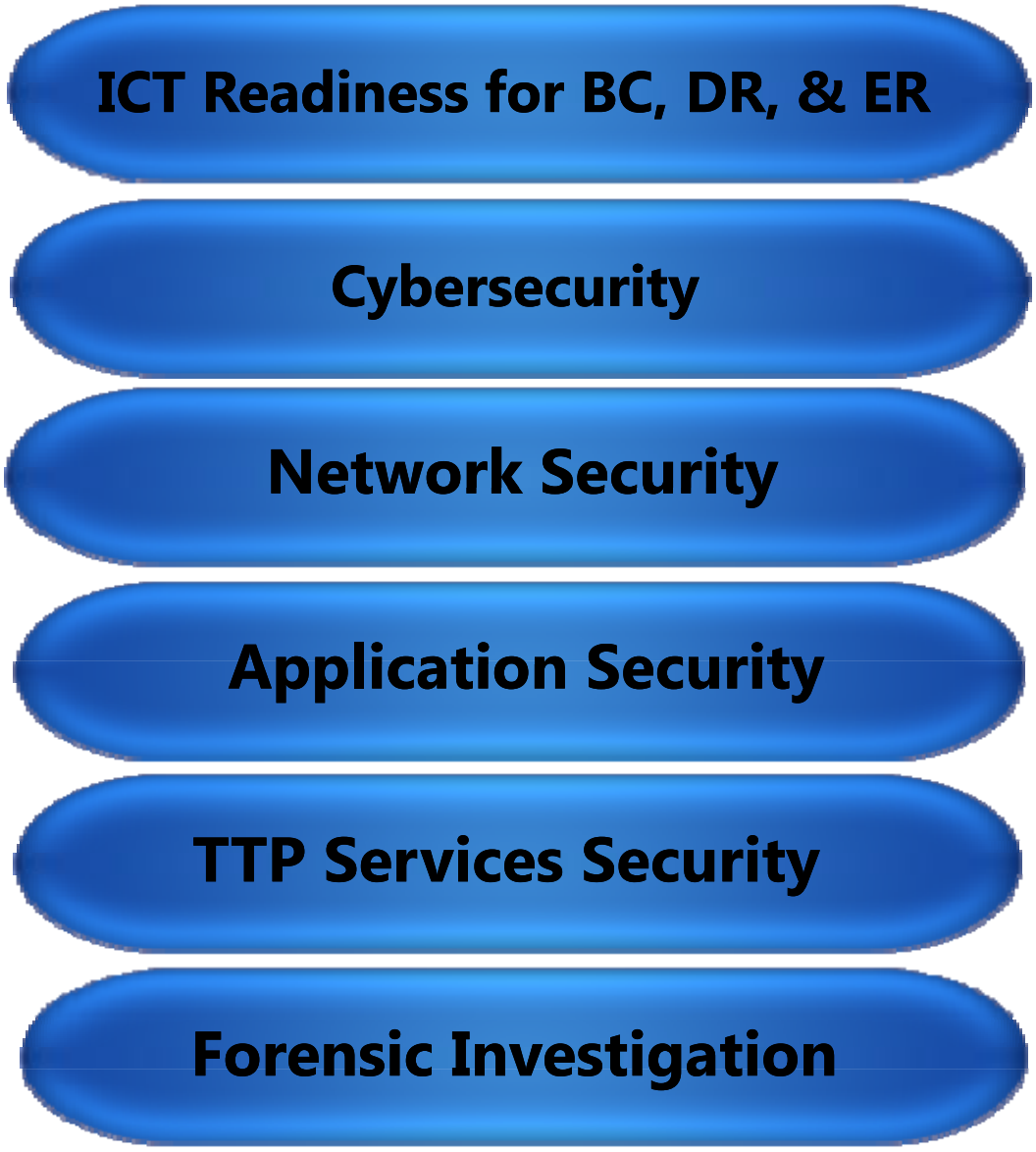
- 9796 メッセージ復元型ディジタル署名
- 14888 添付型ディジタル署名
- 9797 メッセージ認証
- 10118 ハッシュ関数
- 11770 かぎ管理
- 15946 楕円曲線に基づく暗号技術
- 18031 乱数生成
- 18033 暗号アルゴリズム
- 18014 タイムスタンスサービス
- 19772 データカプセル化機構
- バイオメトリクス

WG3

ISO/IEC JTC 1/SC27/WG3

- ISO/IEC 15408 Evaluation criteria for IT security
- ISO/IEC 15443 A framework for IT security assurance
  ISO/IEC 18045 Methodology for IT security evaluation
- ISO/IEC 19790 Security requirements for cryptographic modules
- ISO/IEC 19791 Security assessment of operational systems
- ISO/IEC 19792 A framework for security evaluation and testing of biometric technology

SC27/WG4 における審議項目



NP; Possibly include ISO/IEC 24762, Vulnerability Mgmt, IDS, & Incident Response related standards

Anti-Spyware, Anti-SPAM, Anti-Phishing,

ISO 18028 revision

NP (New Proposal)

Includes outsourcing and off-shoring security

Future NP

Identity Management and Privacy Technologies (WG 5)

- Scope: Development and Maintenance of Standards and Guidelines addressing Security Aspects of **Identity Management (IdM)** and **the Protection of Personal Information (PPI).**
- Current projects
  - Biometric Template Protection (ISO/IEC 24745)
  - Framework for Identity Management (ISO/IEC 24760)
  - Authentication Context for Biometrics (ISO/IEC 24761)
  - A Privacy Framework (ISO/IEC 29100)
  - A Privacy Reference Architecture (ISO IEC 29101)
  - Authentication Assurance (NP)
  - Official Privacy Documents (Standing Document – SD)
  - Joint ITU-T & ISO SC 27 Workshop on Digital Identity

ITU-Tのセキュリティ標準化動向

ITU-T Study Groups

- **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 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

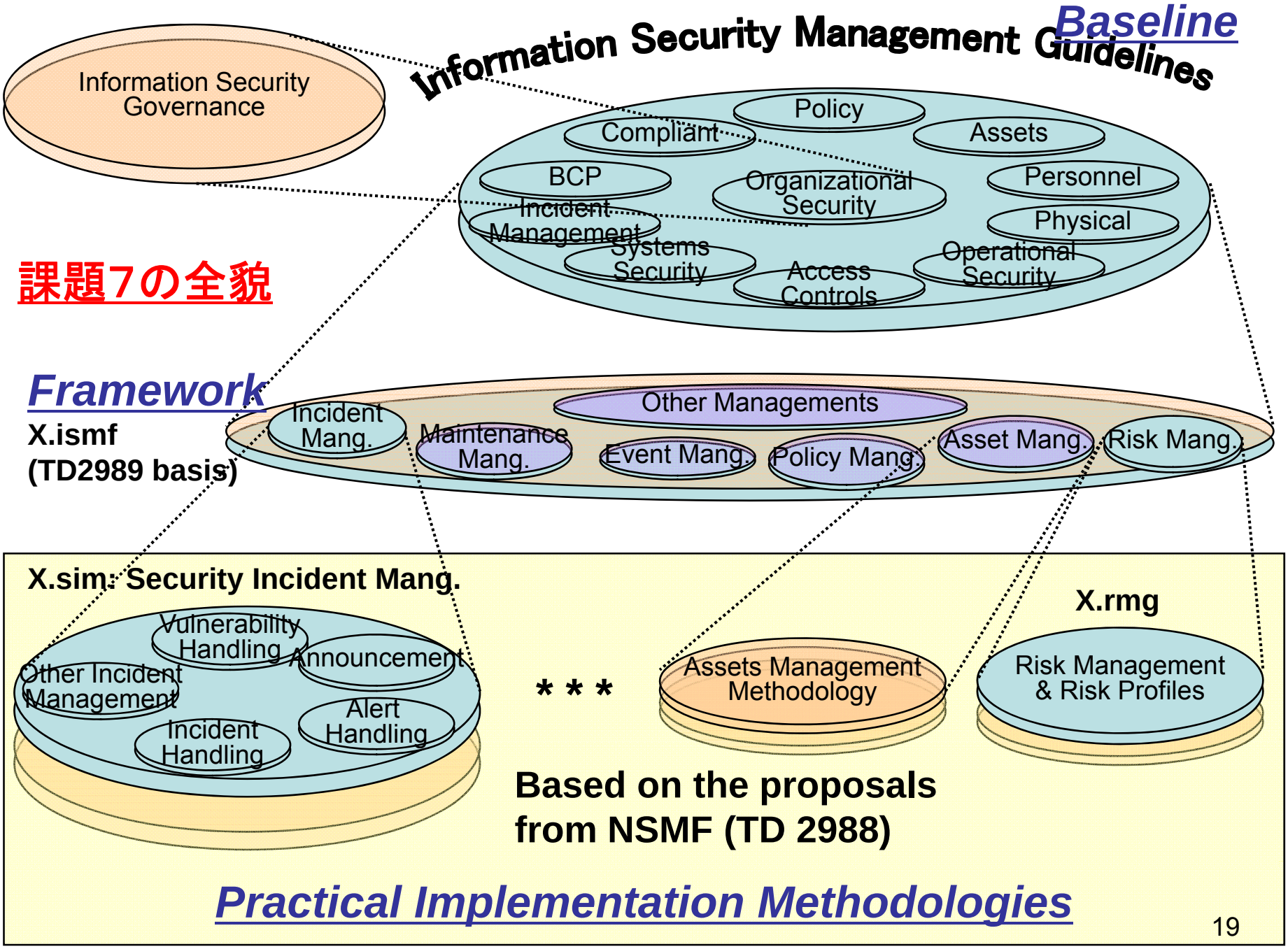
- **X.1100-1109: General for Q9-1**
- **X.1110-1119: Home NW**
- **X.1120-1139: Mobile NW (1121, 1122)**
- **X.1140-1149: Web Security (1141,1142)**
- **X.1150-1179: Secure AP service for Q9-5**

X.1200-1299：Cyber Security

- **To be detailed**

来会期課題 (2009-2012)

Question	Question Title	Continuation or New
I	Telecommunications Systems Security Project（調整のプロジェクト）	Continuation of Q.4/17
J	Security Architecture and Framework	Continuation of Q.5/17
K	Cybersecurity	Continuation of Q.6/17
L	Identity Management, Architecture and Mechanisms （IdM関連課題）	New
M	Telecommunications Information Security Management （ISMS関連）	Continuation of Q.7/17
N	Telebiometrics	Continuation of Q.8/17
O	Security Aspects of Ubiquitous Telecommunication Services	Continuation of part of Q.9/17
P	Secure Application services	Continuation of part of Q.9/17
Q	Countering Spam by Technical Means	Continuation of Q.17/17
T	Service Oriented Architecture Security	New


Information Security Management Guidelines
Baseline
Information Security Governance
Policy
Compliant
Assets
BCP
Organizational Security
Personnel
Incident Management
Physical
Systems Security
Operational Security
Access Controls
課題7の全貌
Framework
X.ismf
(TD2989 basis)
Other Managements
Incident Mang.
Maintenance Mang.
Event Mang.
Policy Mang.
Asset Mang.
Risk Mang.
X.sim: Security Incident Mang.
Vulnerability Handling
Announcement
Other Incident Management
Alert Handling
Incident Handling
* * *
X.rmg
Assets Management Methodology
Risk Management & Risk Profiles
Based on the proposals from NSMF (TD 2988)
Practical Implementation Methodologies

ITU-Dのサイバーセキュリティ

ITU Botnet Mitigation Toolkit プロジェクト

Botnet関連のプロジェクト

- ITUでは急増するBotnet問題を解決するために、Botnet Mitigation Toolkitの開発を進めている。既存のリソースを利用して、Australian Internet Security Initiative (AISI)の協力を得て開発をしている。
- このツールキットは、Botnetによる脅威が増大するITUメンバにおいて高い認識を得てもらうためのもので、他の技術的、社会的な各種Botnets対策と連携することが可能である。
- ツールキットは2007年12月に第1版が完成し、2008年にITUメンバにパイロットとして使ってもらう予定

AISIとは

- Australian Internet Security Initiative（AISI）は、ゾンビBotnetsの被害を軽減する目的で立ち上げられた。
- そのInitiativeは、感染したPC（Botnetsを構築するために使われている）上の情報を収集し、豪州のISPで収集管理されているBotnetsに感染しているIPアドレスリストとそのPCのアドレスを比較し、必要であれば、そのIPアドレスと関連するISPに対して、そのISPが利用者に連絡し、感染しているPCの問題を取り除くよう、助言する。
- 豪州通信メディア局は、AISIで使われる本ツールを国際パートナーとして共有する意思のあることをITUに対して通告している。

ITU-Dの試み（法規制との関係）

- ITU-D　SG1課題22（国としてのCybersecurityに対する組織的アプローチの枠組み）の5つの要素のひとつとして表明されているように、Cybercrime（サイバー犯罪）を抑制することは、国家のCybersecurity 及びCIIP政策の重要な要件となっている。

- 特に、本件は、犯罪のためのICTの不正利用を防止するために適切な法令、または国の重要インフラの完全性確保に関係する試みや活動を含む。

- このような脅威は、世界中のどこにでも発生するものであるため、本チャレンジは基本的に国際の視点でなされるもので、地域的、及び国際的な協調を進め、可能な限り法令などの規範のハーモナイズを行うことが望ましい。

- Cybercrimeの法規制のための本ITUツールキットは、Cybercrimeを阻止するための立法上のフレームワークを確立することを支援する目的で存在する。本ツールキットの開発は、複数の国際的な専門家グループによりなされたものであり、2008年の第1Qに第1版が完成し、ITUメンバの利用が可能となる予定である。

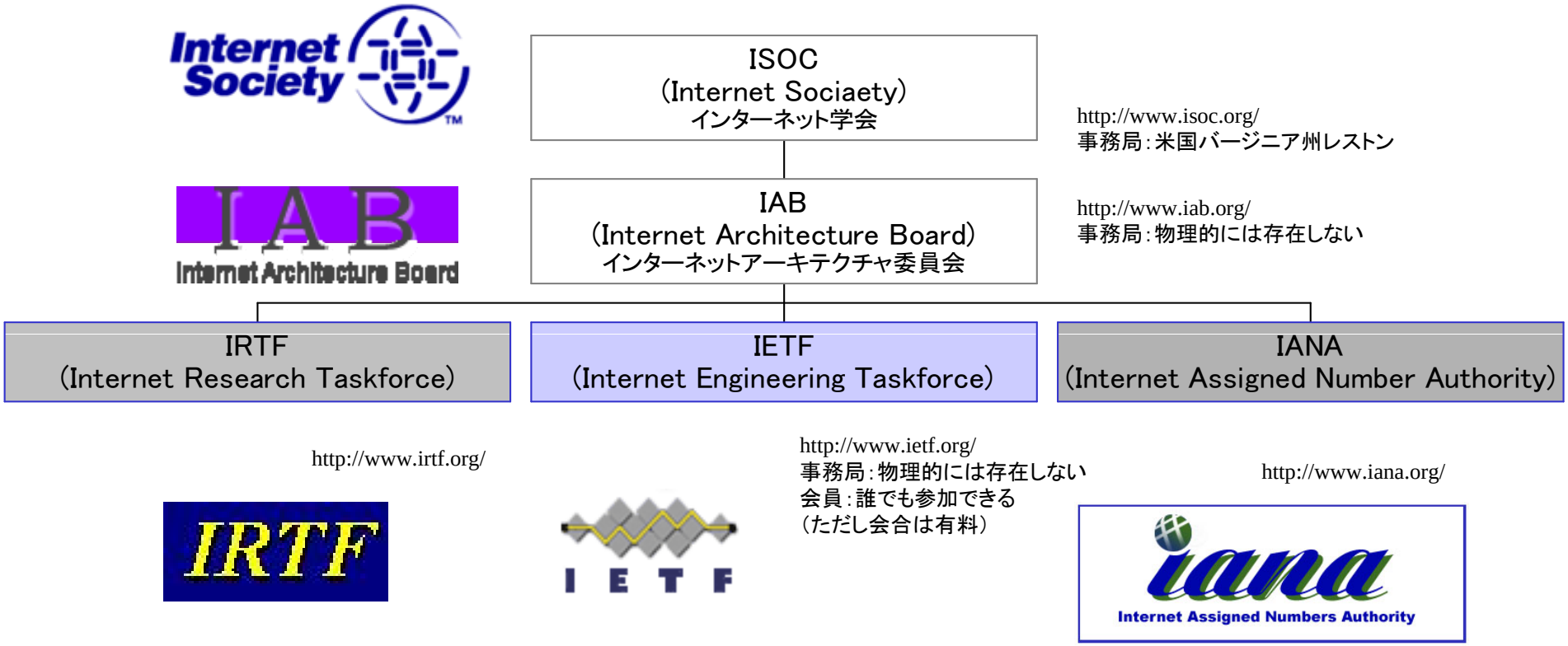
Cybersecurity文化

- Cybersecurity文化の意識向上のため、本ツールキットの目的は、発展途上国の中小企業、消費者、エンド利用者のためにCybersecurityの案件の意識向上をどのように進めるかのガイドラインを提供することである。
- Cybercrime法規制の重要性につき、ITUメンバの認識を向上させるために、Cybercrime法規制に関する地域的な活動（ワークショップなど）をさらに計画している。Council of Europe, UNODC, Interpolなどが本関連の活動の実施に協力している状況である。

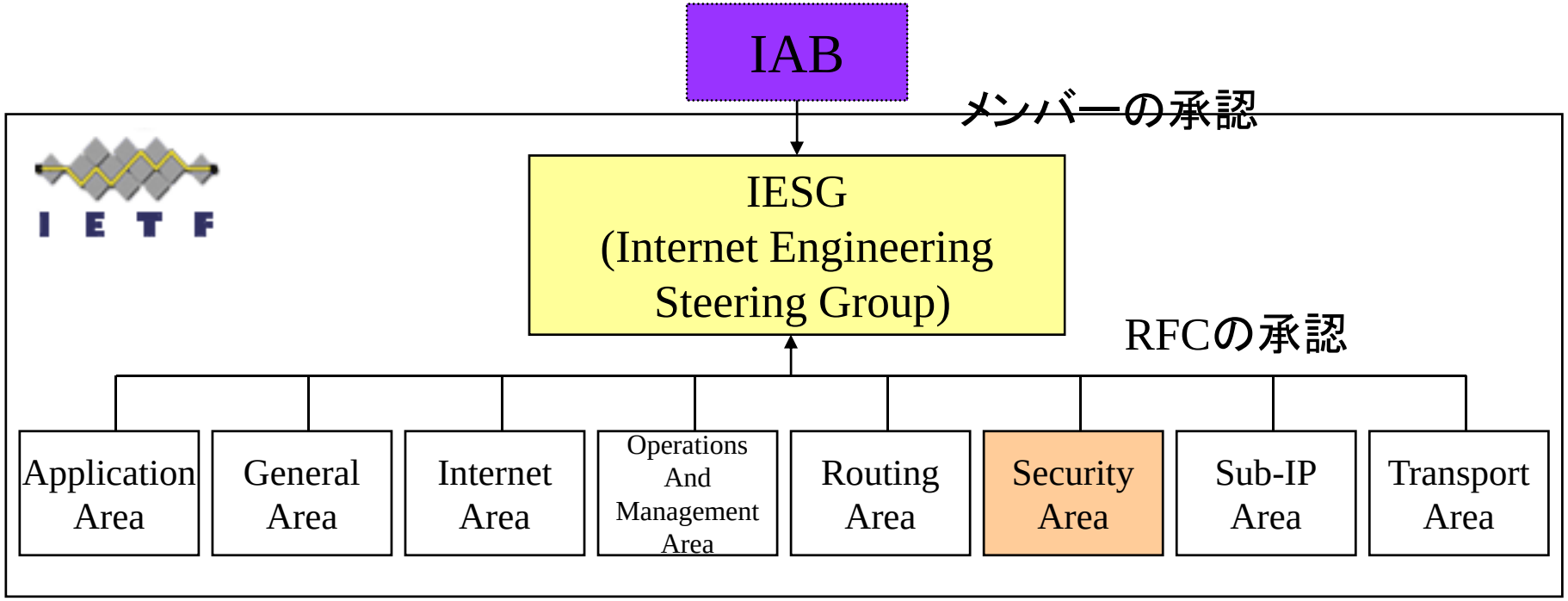
IETF 検討体制

IETFの位置付け（1992年以降）

インターネット標準化



IETF の構成


IAB
メンバーの承認
IETF
IESG
(Internet Engineering
Steering Group)
RFCの承認
Application Area
General Area
Internet Area
Operations And Management Area
Routing Area
Security Area
Sub-IP Area
Transport Area

検討内容の一例

Security Area

+ inch WG:

この inch WG の目的はセキュリティインシデント情報を交換するためのデータフォーマット(IODEF)の定義をおこなうこと

Operations and Management Area

+ opsec WG:

目的は実際のネットワーク運用から得られたノウハウをまとめ、ベンダやオペレータに役立ててもらうこと。(対象としては ISPネットワークやエンタープライズネットワーク、無線/セキュリティデイバイスそのもの(FW、IDSなど)/個々のホストなどは対象外。)

+ ipfix WG:

目的は standard IP flow の概念を定義し、実際に計測出来るようにする こと。(つまりこの定義が単なるコンセプトにとどまることなく、その定義に基づいて実ネットワークの流量を測定できるようにすること)

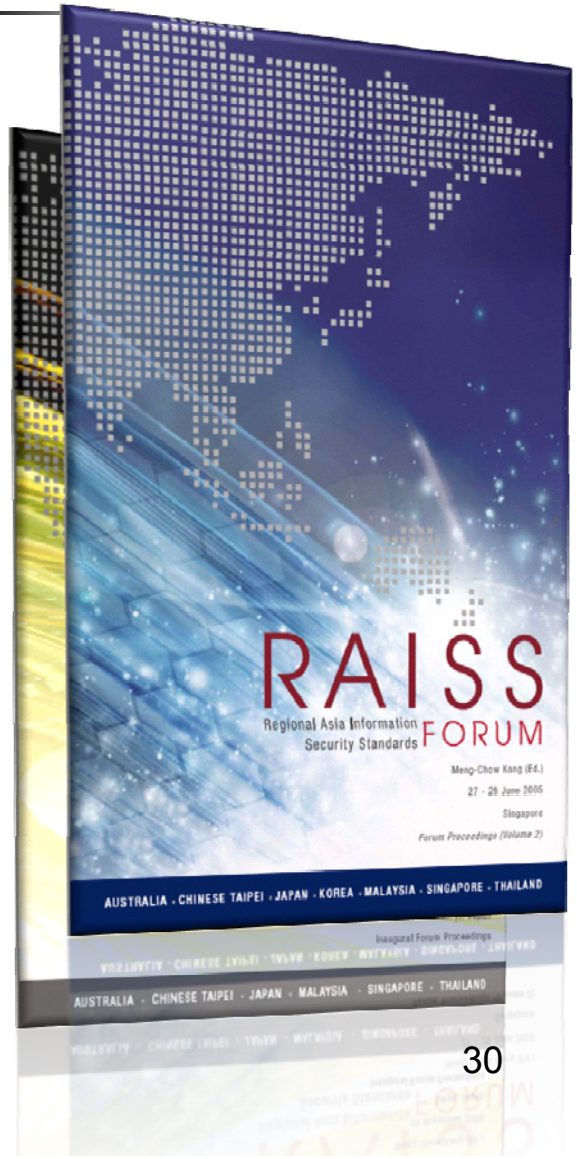
+ psamp WG:

目的は
i)パケット採取(サンプリング)のオペレーションを定義する。
ii)採取したパケットから得られる情報にはどういうものがあるのかを定義する。
iii)採取したパケットの情報を送信するためのプロトコルを定義する。
iv)パケット採取や情報送信の設定を変更するためのプロトコルを定義する。

RAISSの活動（概要）

RAISS Forum
Regional Asia Information Security Standards

- 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, Sungapore
- 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

- Security Standards Toolkit
- 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

Current Focus

- Improving information sharing and communications
- Extending help and outreach to emerging economies
- Closing the gaps in existing international standards arena
  - New standards
  - Guidance on use/implementation
- Preparing the region for emerging/new development (upcoming standards)

その他の標準化活動

1）SWIS
　情報セキュリティに関する国際標準のためのワークショップ（CJKが中心に）
・2007年　10月ソウル、2008年　11月東京（予定）
各国の標準化施策を共有し、ISO/ITU-Tへの反映をもくろむ

2）27000GoesGlobal会議
・英国が主導的な会議で、ISMSを国際的に利用拡大を狙ったビジネス主体の会議
・近年、いろいろな技術分野を含む会議に拡大化
→　2008年　12月　ロンドン　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技術
- ITU-D：発展途上国　（これから）
- IETF：インターネット系技術
- RAISS：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/ITU-T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の施策はそのひとつ

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。

最近の流れ・方向性（4）

- 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）

今後の方向性(1)

- 情報社会の進展に伴い，安全な社会システムの構築が産官学において必須
- セキュリティは皆が関わっているとの認識が必要
- セキュリティは備えを考えた設計が必要 （Built-in）
- 技術の規格化に加え、Awareness に関する規格化も重要
- さらに、Awarenessを発展させ、情報共有化、連携手法の検討が重要で、その国際規格化、ガイドライン化の方法を現在、いろいろな組織で模索中

今後の方向性(2)

- 日本としては、技術に加え、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。
- 手始めに、最も最寄の国から連携を進めては。
- CJK会合(SWIS会合)にターゲットを絞り、具体的な枠組みの提案、連携方法について具体化をする。
  - ＊セキュリティ情報共有フレームワーク(見直し)
  - ＊CCC関連
  - ＊トレースバック関連
- その後、RAISSなどを通し、アジア全体、および欧州、米国を巻き込んでいく。
- 完全なボランティアでは難しく、資金的、人材的な確保が本施策の要