ISO/IEC 27000関連規格の最新動向

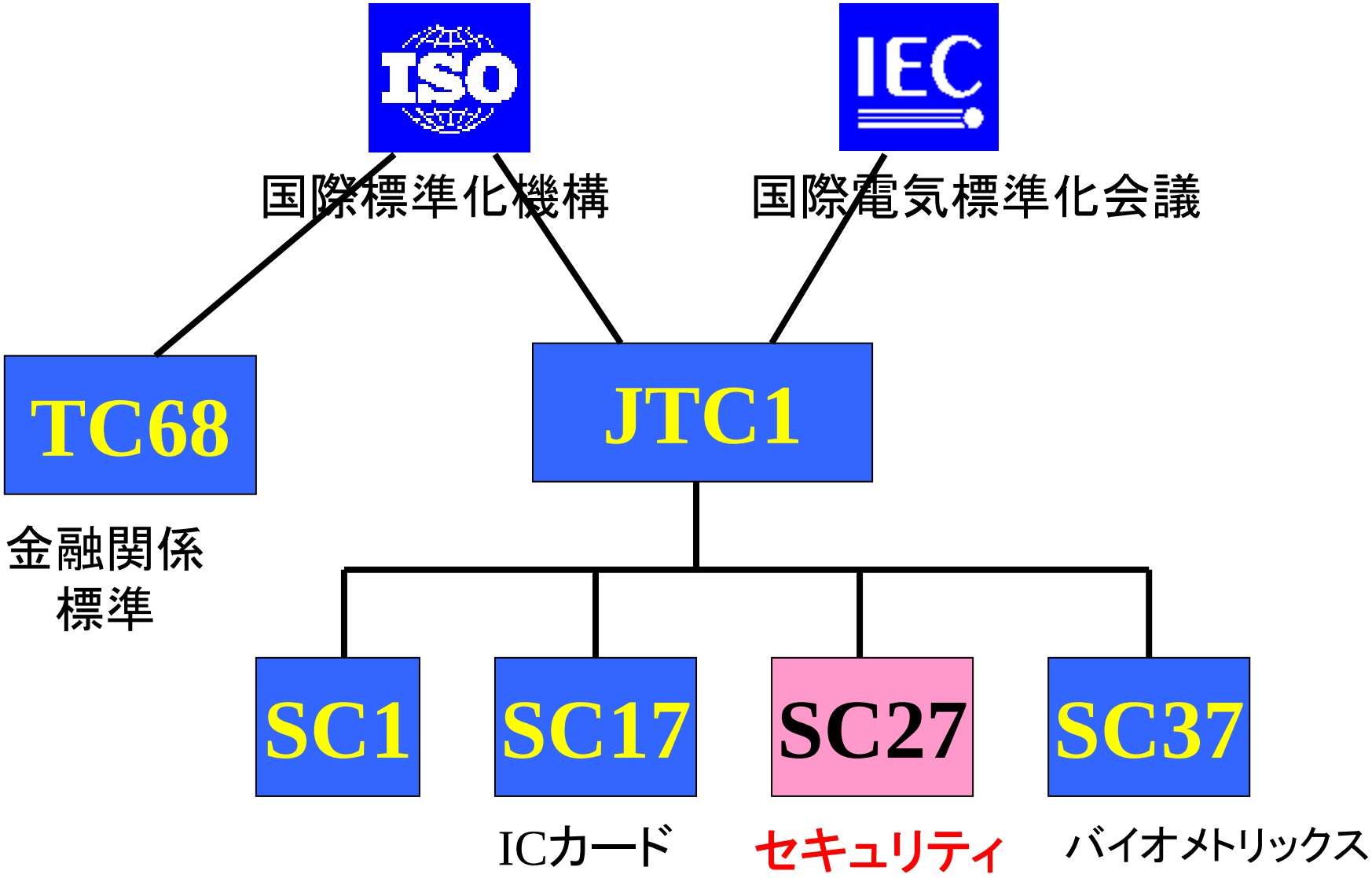
中尾　康二

KDDI 株式会社　情報セキュリティフェロー
NICT インシデント対策G　GL
JNSAメンバ、Telecomー ISACメンバ
National convener of WG4, ISO/IEC SC27
Vice-chair of ITU-T　SG17

- 2009年11月に米国（レッドモンド）で開催されたISO/IEC JTC1/SC27におけるWG1及びWG4において、ISO/IEC 27000関連規格に関する審議がなされました。本セッションでは、情報セキュリティマネジメント（ISMS）におけるコア規格となっているISO/IEC 27001/27002のみなおし状況、セキュリティ監査ガイドライン、及びセキュリティガバナンスなどの規格審議状況を報告するとともに、ISMSを支える具体的な技術として、例えば、ネットワークセキュリティ、アプリケーションセキュリティ、インシデントマネジメント、アウトソーシングセキュリティ、及びデジタルエビデンス（フォレンジック関連）などに関する最新審議動向を分かりやすく紹介します。

ISO/IEC JTC 1/SC 27
IT Security Techniques

ISO/IECの組織構造



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

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

ISO JTC1 IEC
Information Technology Standards

SC 27 - *Scope*

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

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

Membership of SC 27

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

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

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

SC 27 - 組織

ISO/IEC JTC 1/SC 27

IT Security techniques

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

SC 27 Secretariat

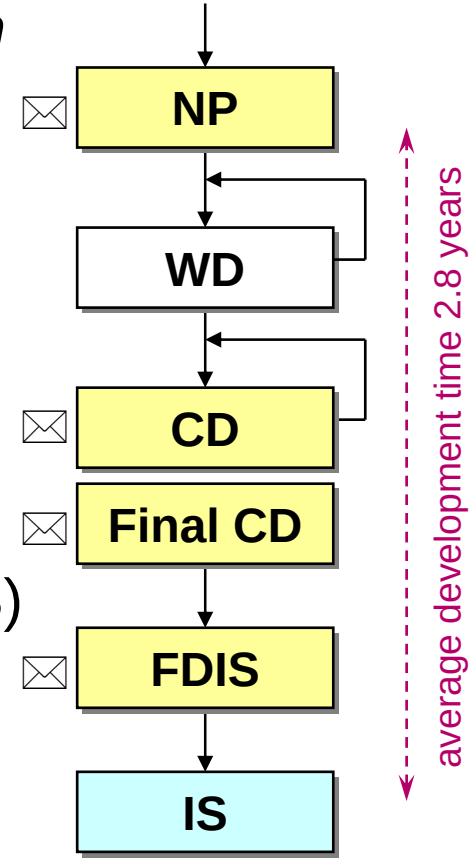
DIN

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*

ISO – *標準化のプロセス*

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



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

SC27／WG1における標準化文書リスト（1）

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

SC27／WG1における標準化文書リスト（2）

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

WG1：規格の見直しスケジュール

- ISO/IEC 27001 及び ISO/IEC 27002は、現在見直しのプロセスにあり、第2版のWDである。
- ISO/IEC 27002　は少なくとも、後1回のWDが必要であり、2012年完成を目指している。
- ISO/IEC 27001 は、CDに移行できるレベルにあると考えられ、2011年完成となる予定。
- ISO/IEC 27001 及び ISO/IEC 27002 の見直しを同時に実施するべきか、別々で問題ないのかについては、現在議論のあるところである。

見直し: 27001 - Framework

- 重要な規格であるため、本当に必要と考えられる修正点の修正を実施するという方針で臨んでいる。
- 以下の2つについては、明確な区別を行っている。
  - 27001における要求事項
  - その他の27000ファミリー規格におけるガイダンス
- その他の27000ファミリー規格については、ISO/IEC 27001に準拠する（他規格のために、27001の修正を行わない）必要がある。
- すべての用語定義については、ISO/IEC 27000に従うこととする。
- ISO 31000 (Risk management - Principles and guidelines:リスクマネジメントー原則及び指針）に準拠

JTCG の構造 (1)

- JTCG (a part of ISO TMB) では、すべてのマネジメントシステム規格に対して、共通の構造を与えることを審議している。
- 現状、そこで提案されている構造は以下である。
  - Standard clauses (scope, definitions, etc.)
  - Context of the organization
  - Leadership
  - Planning
  - Support
  - Operation
  - Performance evaluation
  - Support
- 審議の終了予定: Spring 2012

JTCG の構造 (2)

- Decisions
  - 2nd WG ISO/IEC 27001 の作成（2010年1月に発行）に当たっては、現状のJTCGの構造は参考にする程度としている。
  - JTCGの会合にできるだけ参加していく必要がある。（SC27としての組織的な参加が要）
  - 新たなJTCGの構造に我々SC27が準拠していくかどうかについては、後で決定することとしたい。

ISMS policy （27001）と information security policy (27002）の議論

- ISMS policy（27001）と information security policy (27002）が意味的にかなり重なっていることを懸念
- Decisions:
  - これらの用語はそのままとする。
  - ISMS policy（27001）については、微細な追加修正を行うこととする。（information security managementについて言及）
  - ISMS policy（27001）の方への参照のみとする。
  - information security policy (27002）は、ハイレベルのドキュメントであり、それはトップマネジメントが発行するものである。
  - information security policy (27002）については、双方のポリシーの表現に重なりを少なくするような修正を行うことで合意されている。

Top Management

- 「management」と「top management」の区別について議論がなされた。
- Agreement:「Top management」は、ISMSのスコープにおける最も高いレベルのマネジメントであり、すなわち、そのレベルは、組織の所有者であり、究極の権限を持ち、そこでのISMSに対して責任をもつものである。

管理策の選択と付属書A（Selection of Controls & Annex A）

- 付属書Aの発行の必要性、及び他の管理策のセットについて、Redmond会合で審議がなされた。
- Decisions:
  - 付属書A（Annex A）は、選択される管理策のための基本推奨セットとする。
  - その他の管理策のセットについては、当然活用が可能とする。管理策選択のプロセスにおいては、より自由度が与えられているとする。
  - 追加的な管理策についても当然選択可能とする。
  - 適合宣言書（Statement of Applicability）はそのまま。

リスク対応オプションについて（Risk Treatment Options）

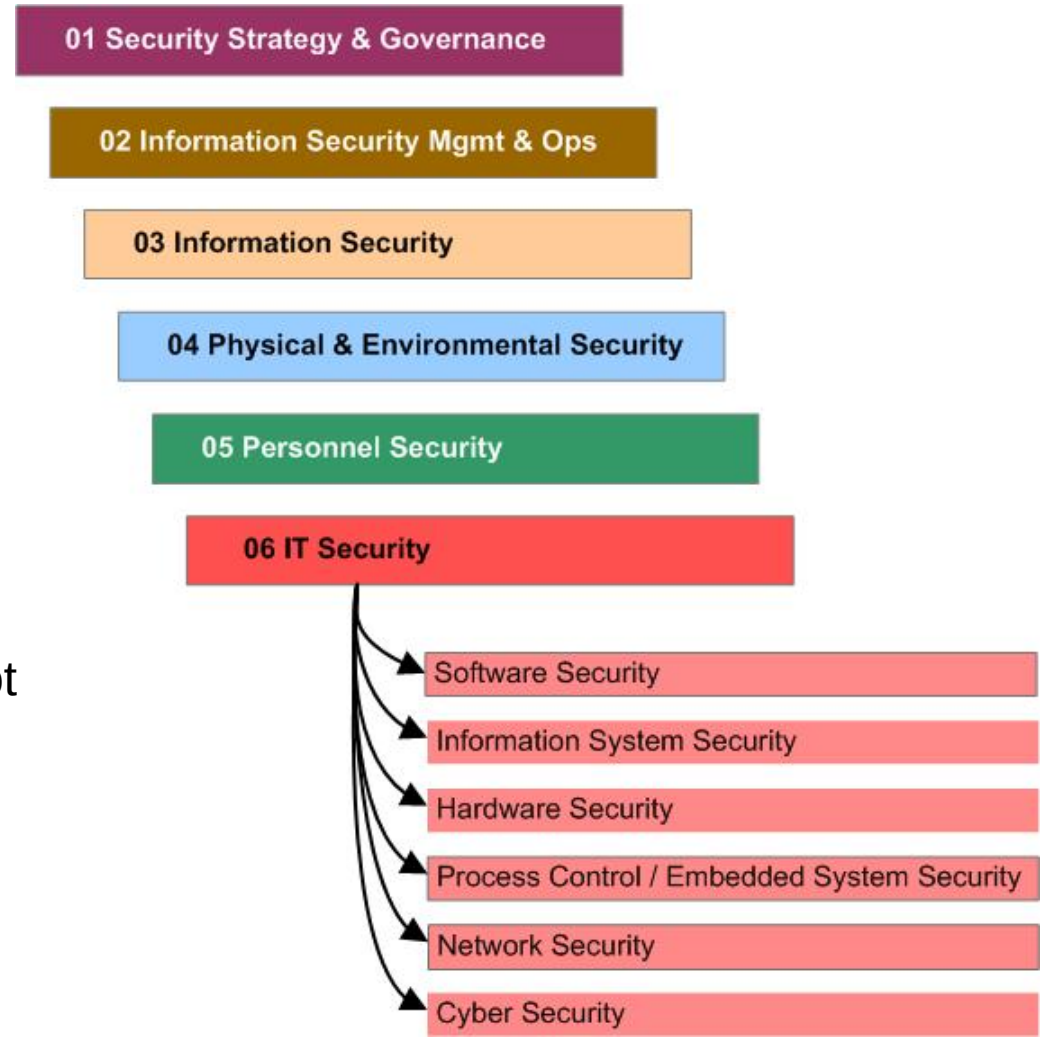
- 現状は、“risk reduction by controls”のオプションに焦点が当てられている。
- ISO/IEC 27001においては、すべてのリスク対応オプション（リスク削減、リスク保持、リスク回避, リスク移転, ）は、同等に記載されることが合意された。
- 上記は、４．２．３節に記載される。

ISO/IEC 27002の見直し

- Redmond会合の前の北京会合で、カナダがISO/IEC 27002 に対する大幅な構造の見直しの提案を行った。
- カナダの提案は、単純な見直し、エディティングといった範囲を完全に逸脱しており、そこには、大量の新しい管理策が提案されていた。

ISMS Taxonomy （カナダ提案）

- Comprehensive but not exhaustive
- Hierarchical and tiered
  - 6 sectors wide
  - 4 levels deep
- All topics organized by similarity
  - Precise matches not always possible
- A work in progress
  - Refinement and tuning required

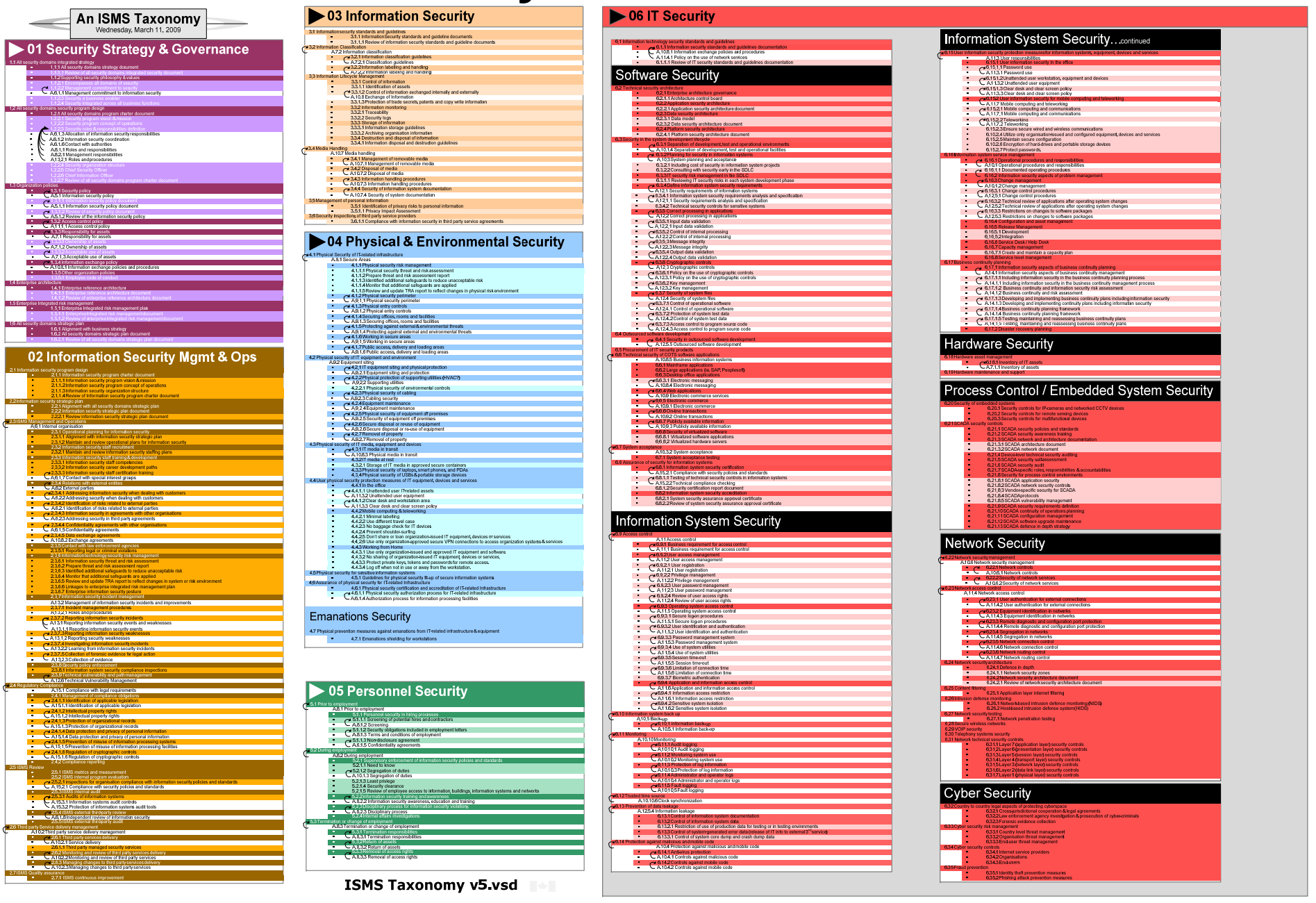


ドメイン 1

01 Security Strategy & Governance

- 1.1 All security domains integrated strategy
  - 1.1.1 All security domains strategy document
    - 1.1.1.1 Review of all security domains integrated security document
  - 1.1.2 Supporting security philosophy & values
    - 1.1.2.1 Encompasses all domains of security
    - 1.1.2.2 Management commitment to security
      - A.6.1.1 Management commitment to information security
    - 1.1.2.3 Security a business enabler
    - 1.1.2.4 Security integrated across all business functions
- 1.2 All security domains security program design
  - 1.2.1 All security domains program charter document
    - 1.2.2.1 Security program vision & mission
    - 1.2.2.2 Security program concept of operations
    - 1.2.2.3 Security roles & responsibilities definition
      - A.6.1.3 Allocation of information security responsibilities
      - A.6.1.2 Information security coordination
      - A.6.1.6 Contact with authorities
      - A.8.1.1 Roles and responsibilities
      - A.8.2.1 Management responsibilities
      - A.13.2.1 Roles and procedures
    - 1.2.2.4 Security organization structure
    - 1.2.2.5 Chief Security Officer
    - 1.2.2.6 Chief Information Officer
    - 1.2.2.7 Review of all security domains program charter document
- 1.3 Organization policies
  - 1.3.1 Security policy
    - A.5.1 Information security policy
    - 1.3.1.1 Information security policy document
      - A.5.1.1 Information security policy document
    - 1.3.1.2 Review of security policy document
      - A.5.1.2 Review of the information security policy
  - 1.3.2 Access control policy
    - A.11.1.1 Access control policy
  - 1.3.3 Responsibility for assets
    - A.7.1 Responsibility for assets
    - 1.3.3.1 Ownership of assets
      - A.7.1.2 Ownership of assets
    - 1.3.3.2 Acceptable use of assets
      - A.7.1.3 Acceptable use of assets
  - 1.3.4 Information exchange policy
    - A.10.8.1 Information exchange policies and procedures
  - 1.3.5 Other organization policies
    - 1.3.5.1 Employee code of conduct
- 1.4 Enterprise architecture
  - 1.4.1 Enterprise reference architecture
    - 1.4.1.1 Enterprise reference architecture document
    - 1.4.1.2 Review of enterprise reference architecture document
- 1.5 Enterprise Integrated risk management
  - 1.5.1 Enterprise Integrated risk management plan
    - 1.5.1.1 Enterprise Integrated risk management document
    - 1.5.1.2 Review of enterprise Integrated risk management document
- 1.6 All security domains strategic plan
  - 1.6.1 Alignment with business strategy
  - 1.6.2 All security domains strategic plan document
    - 1.6.2.1 Review of all security domains strategic plan document

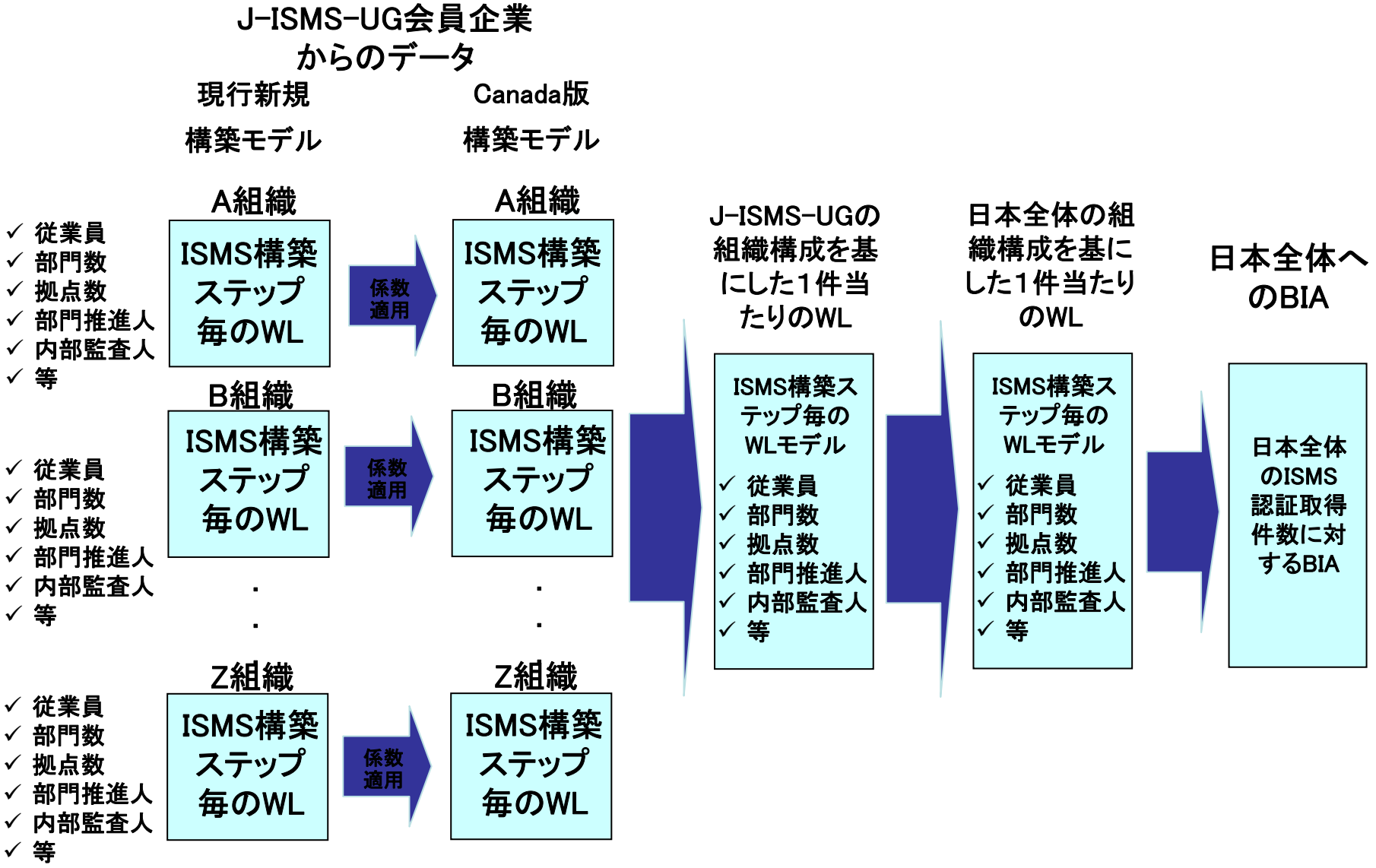
ISMS Taxonomy（カナダ提案の全貌）



日本ISMSユーザGによる、カナダ提案のビジネスインパクト分析の要約

1）日本ISMSユーザGの27組織での調査。JIPDECのアンケート調査の1158社に拡大展開、3298組織での見積もりを実施。
2）費用的なインパクト：今回のカナダ案に準拠すると、各組織はISMSを始めからやり直すことと等価なコストが発生する。一組織に対して、604K$ 。日本の認証組織に対しては、1,993M$ のコストが発生と見積もる。
3）利用のしやすさへのインパクト：目的、管理策などの基本構造を破壊するような提案となっているため、利用者の視点からは「非常に使いにくい」といわざるを得ない。
4）ISMS認証組織へのインパクト：現状のISMSからカナダ案に従ったものへ移行することに対する負荷は絶大と評価。このままで行くと、以後、ISMSの認証継続を断念する企業も発生する可能性大。
5）ISMS関連文書へのインパクト：現在の管理策の数と比較すると、カナダの提案は倍以上の管理策となり、ドキュメント上の管理も膨大となる。

Steps for Business Impact Analysis
（日本ISMSユーザGの作業）



ISO/IEC 27002の審議結果

- カナダの提案を採用しないことが合意された。しかし、その提案内容を完全に否定したわけではない。。。
- たくさんのISO/IEC 27002に対するコメントが提出されたが、すべてのコメントの処理ができていない状況にある。
- 審議未了のコメントについては、すべてのエディタ（27002の）に対応を依頼することとし、修正提案が受け入れられなかったところについては、明確な印をつけることとした。
- すでに審議されたその他の修正点については、エディタのドラフト案を慎重に見直しをする必要がある。

ISO/IEC 27007

- ISMS Auditor Guidelines, 現状 2nd CD
- ISMS特定のガイダンスの視点からISO 19011（Guidelines for quality and/or environmental management systems auditing）を捕捉するもの。
- ISO 19011の見直しに沿って、作業を進めている。（案外とその修正が大きい）
- ISO 19011の見直しのスケジュールなどに依存するため、それに合わせるのが難しい現状にある。
- Decision: ISO 19011の進捗を待ち、作業を進める。（19011がどのくらいかかっても）

ISO/IEC 27008

- ISMSの管理策の監査に焦点。
- 現状、TRで進んでいるが、将来ISに変更する可能性がある。次回のマレーシアで決着予定。
- ISO/IEC 27007 及び ISO/IEC 27008 との間の審議が必要とされる（エディタ：27007の意見）
- ISO/IEC 27007 及び ISO/IEC 27008 の間での合同会合を次回開催し、互いのスコープを区別化する。

ISO/IEC 27008

- Content:
  - 基本的な考え方は、ISMS管理策を見直すためのもの。
  - ISMS 管理策の見直し（監査）プロセスに焦点。
- ISMS管理策への視点で規格化を進めており、内容的に、より深い内容となっている。
- ISO/IEC 27007 もISMSの部分として管理策を含んでいるため、スコープの明確化が必要。

ISO/IEC 27010

- Sector to sector interworking and communications for industry and government
- Result of a Study Period on Critical Infrastructures
- Scope: このISは、同じセクター間の産業、別のセクター/政府における産業の間で、セキュリティに関する相互作業、情報交換を行うためのガイドラインである。これらは、危機的状況、重要インフラ防護、または、通常のビジネスにおける相互承認の環境で、法的、及び契約上の義務を追求するためのものである。

ISO/IEC 27013
Integrated 20000 and 27001

- Integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001
- Scope: ISMSとITサービスMSとを統合させるためのガイダンスを提供する。
- 本規格は、その統合MSの実施のための助言を提供するものであり、例えば:
  - ISO/IEC 20000-1 をすでに保有している状況で、ISO/IEC 27001の取得をする場合、またはその逆。
  - ISO/IEC 27001 及び ISO/IEC 20000-1 を同時に構築する場合。
  - 助言の内容は、すでに規格化されている、ISO/IEC 27001 及び ISO/IEC 20000-1のMSの実施に準拠していく。

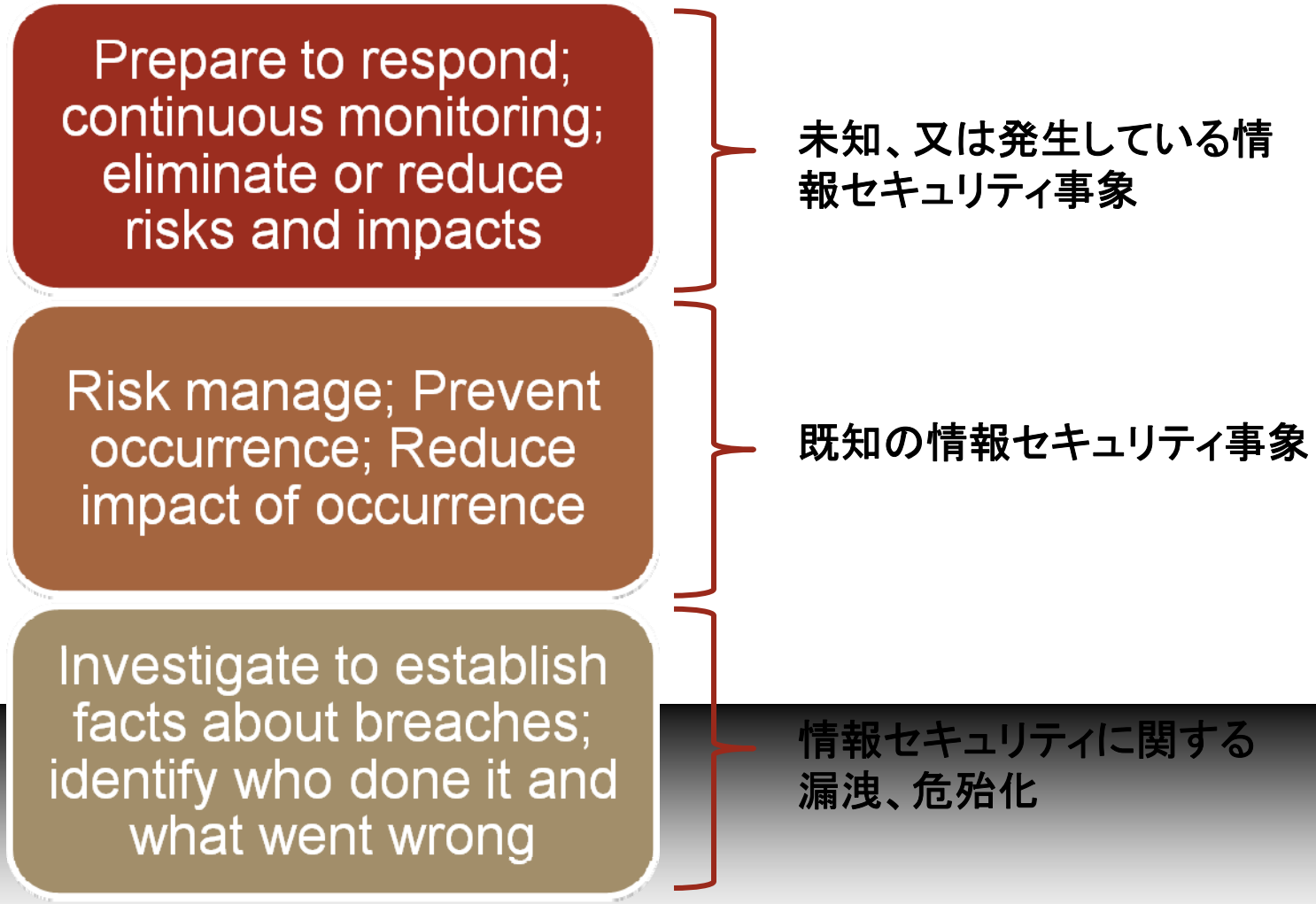
ISO/IEC 27014 Information security governance framework

- IS governance
- Scope:（英文のまま、掲載）
  - 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

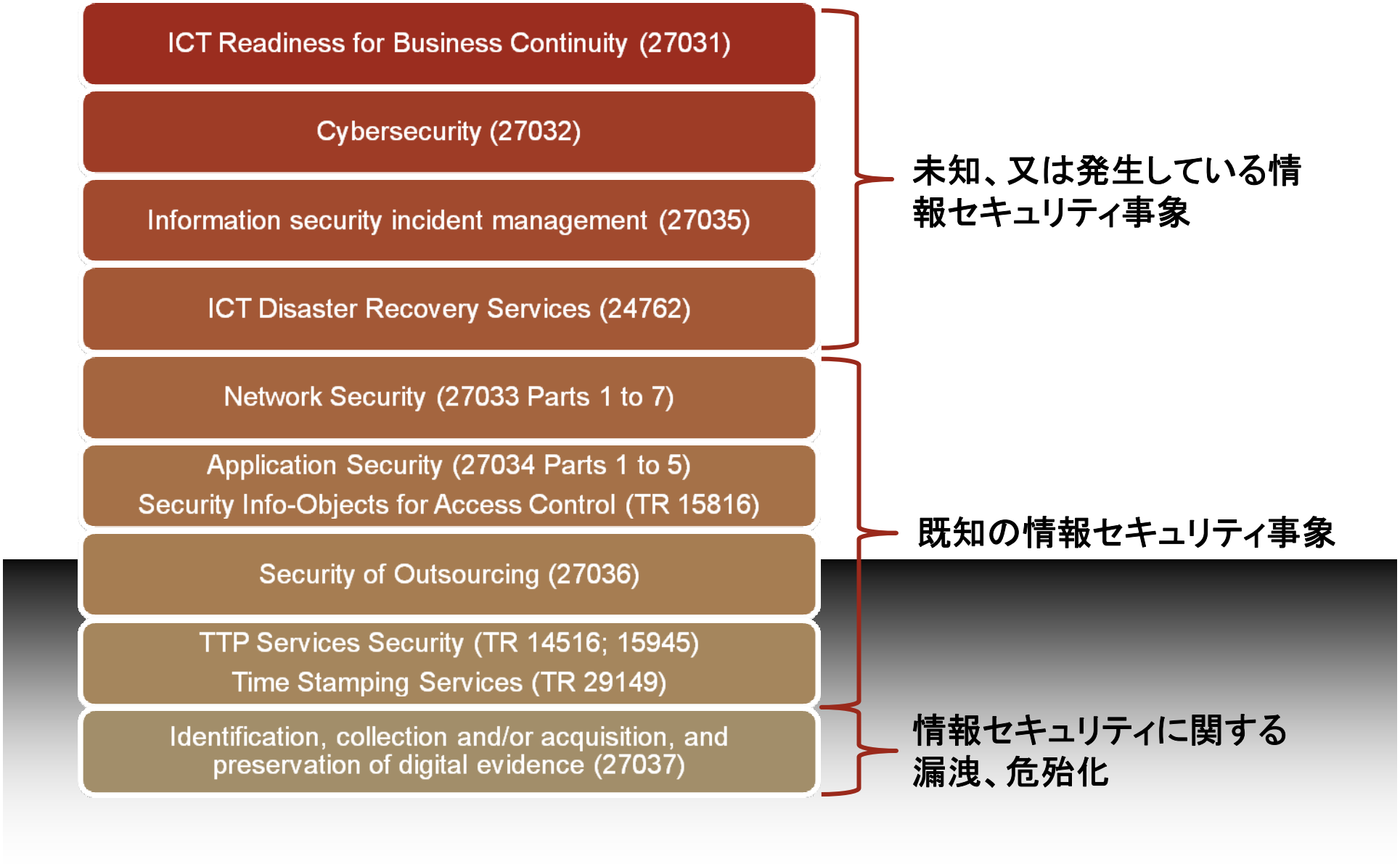
ISO/IEC 27015 Financial services

- 1st WD for financial and insurance services
- Scope: 本規格は、「financial and insurance services sectors」における情報セキュリティマネジメントの実施を支援するためのガイダンスを提供するものである。
- 本規格は、2700xのISMSの枠組みにどのように適合させるかといったガイドラインの提供を意図している。その目的は、法的な要求事項などに関連したセクター特有の情報セキュリティを満足することを目的としている。

WG 4 Roadmap Framework



WG 4 Projects & Study Periods



PROJECT: ISO/IEC 27031
（ICT READINESS FOR BUSINESS CONTINUITY）

PROJECT EDITORS' REPORT

- 第1版CDに対し、ブラジル、日本、ルクセンブルグ、マレーシア、シンガポール、スウェーデン、スイス、及びUK、さらに、TC223から、多数のコメントを受けた。プロジェクトエディタは、4回の会合をもち、コメント対応、解決法などの検討を実施した。

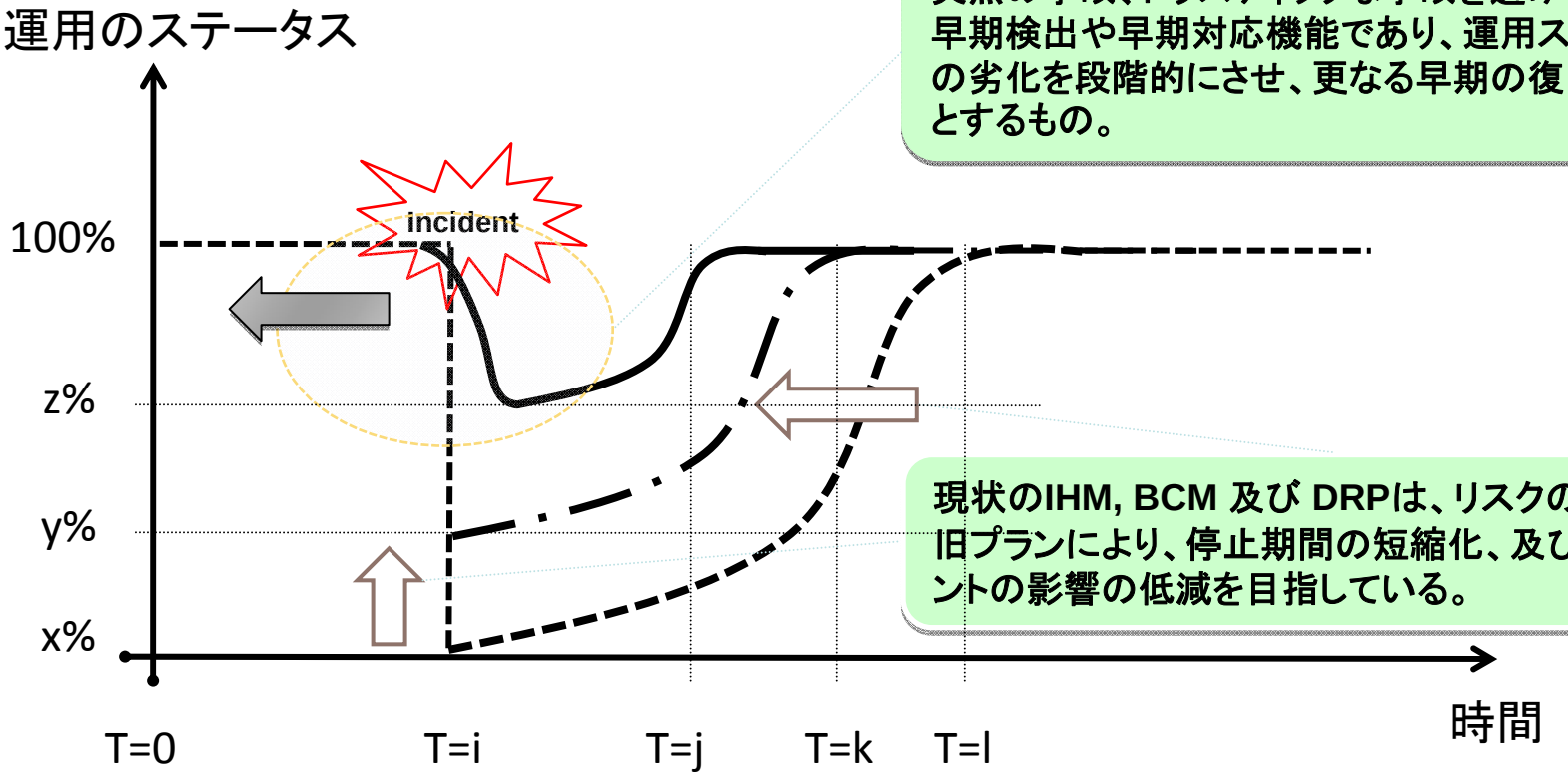
COMMENTS AND CONTRIBUTIONS

- 1st CD（N7556）に対する各NBからのコメントが審議され、会議の中で本規格案CDは、次のステージであるFCDに入るか否かの審議を行った。日本は、FCDのステージにはまだ早いという見解を示して、態度を留保した。結果、**FCDのステージに上がること**がPLで承認された。

日本からのコメントの対処結果

- 大枠合意された。

ISO/IEC 27031



突然の事故、ドラスティックな事故を避けるための早期検出や早期対応機能であり、運用ステータスの劣化を段階的にさせ、更なる早期の復旧を可能とするもの。

現状のIHM, BCM 及び DRPは、リスクの低減、復旧プランにより、停止期間の短縮化、及びインシデントの影響の低減を目指している。

--------- IHM, BCM, DRPを実装する前

– · — · — IHM, BCM, DRPを実装した後

———— ICT Readiness for BCを実装した後

用語

IHM: Incident Handling Management
BCM: Business Continuity Management
DRP: Disaster Recovery Plan

27032 : Cybersecurity

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 provide an infrastructure for collaboration.

Guidelines for Cybersecurity

- "Best practice" guidance in achieving and maintaining security in the cyber environment
  - –an overview of Cybersecurity;
  - –an explanation of the relationship between Cybersecurity and other types of information security;
  - –a definition of stakeholders and a description of their roles in Cybersecurity;
  - –guidance for addressing common Cybersecurity issues; and
  - –a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.

PROJECT WD 27032：
（Redmondの審議）

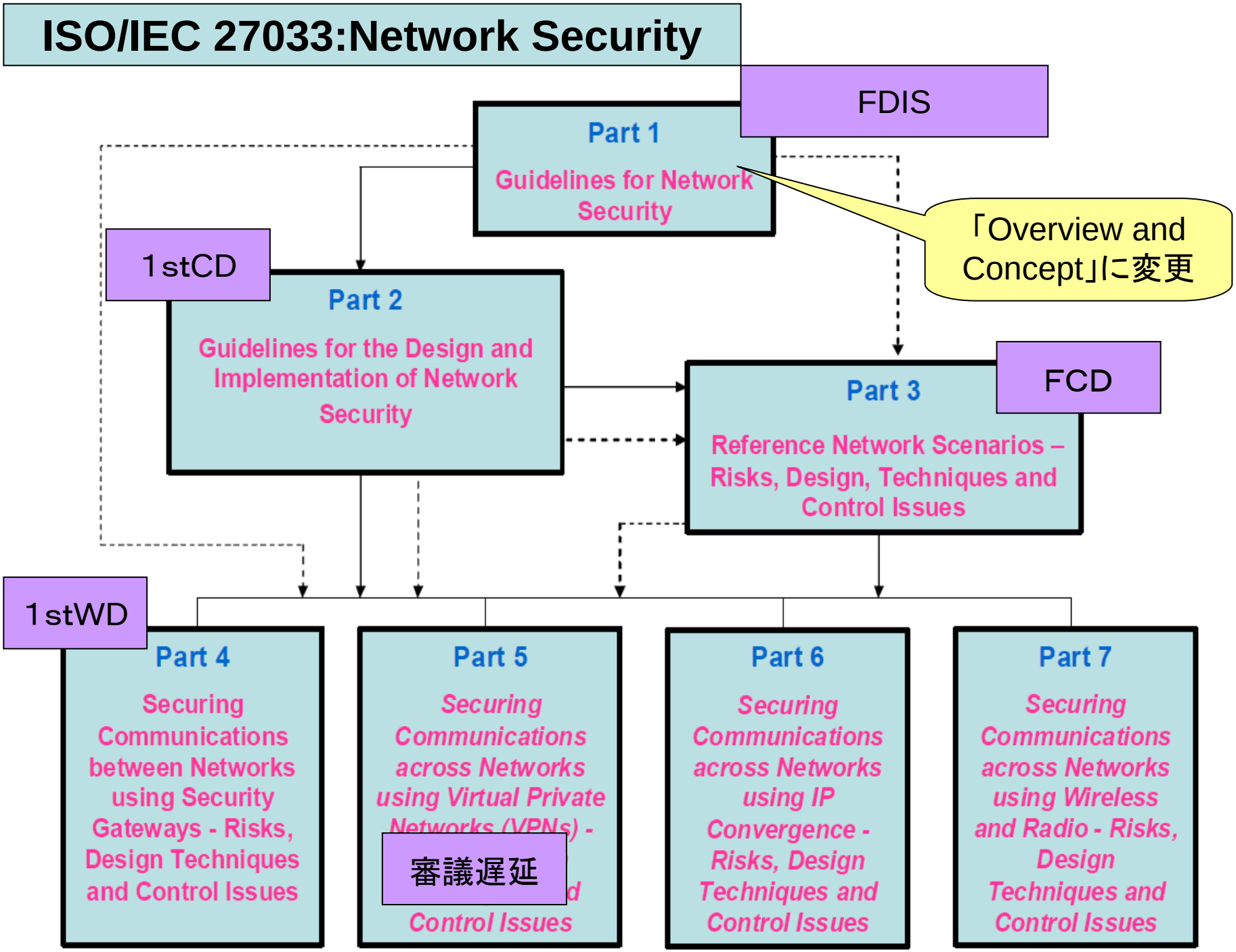
PROJECT EDITORS' REPORT

- 豪州、ベルギー、日本、南アフリカ、及び米国から248のコメントを受けた。プロジェクトエディタは3回の会合を開催し、コメント対処の審議を実施した。

COMMENTS AND CONTRIBUTIONS

- 3rd WDへのコメントは、7カ国から248件（AU 9、CA 4、IT 3、JP 17、ZA 154、US 25、BE 36）が提出され、全てのコメントが処理された。
- コメント処理の主な内容は、構造上の修正、用語の利用の一元化、さらに、サイバーセキュリティの目的をより明確にすることが課題としてエディタに課せられた。
- その結果、WG4のClosing PlenaryでのResolutionで、**1st CD**に進むことが確定した。1st CD（N7917）の締め切りは2010年1月4日である。
- 補足的な議論として、27032の番号をやめ、27000シリーズから番号を外すべきとの議論があった。しかしながら、当面のところ、27001/27002への関係も考慮できるため、番号は据え置きとなった。

ISO/IEC 27033:Network Security



Guidelines for Application Security (27034)

構造

- Part 1 – Overview and concepts　1stCD→2ndCD
- Part 2 – Organization normative framework
- Part 3 – Application security management process
- Part 4 – Application security validation
- Part 5 – Protocols and application security controls data structure
- Part 6 – Security guidance for specific applications

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

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

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

違った観点で新たに標準化

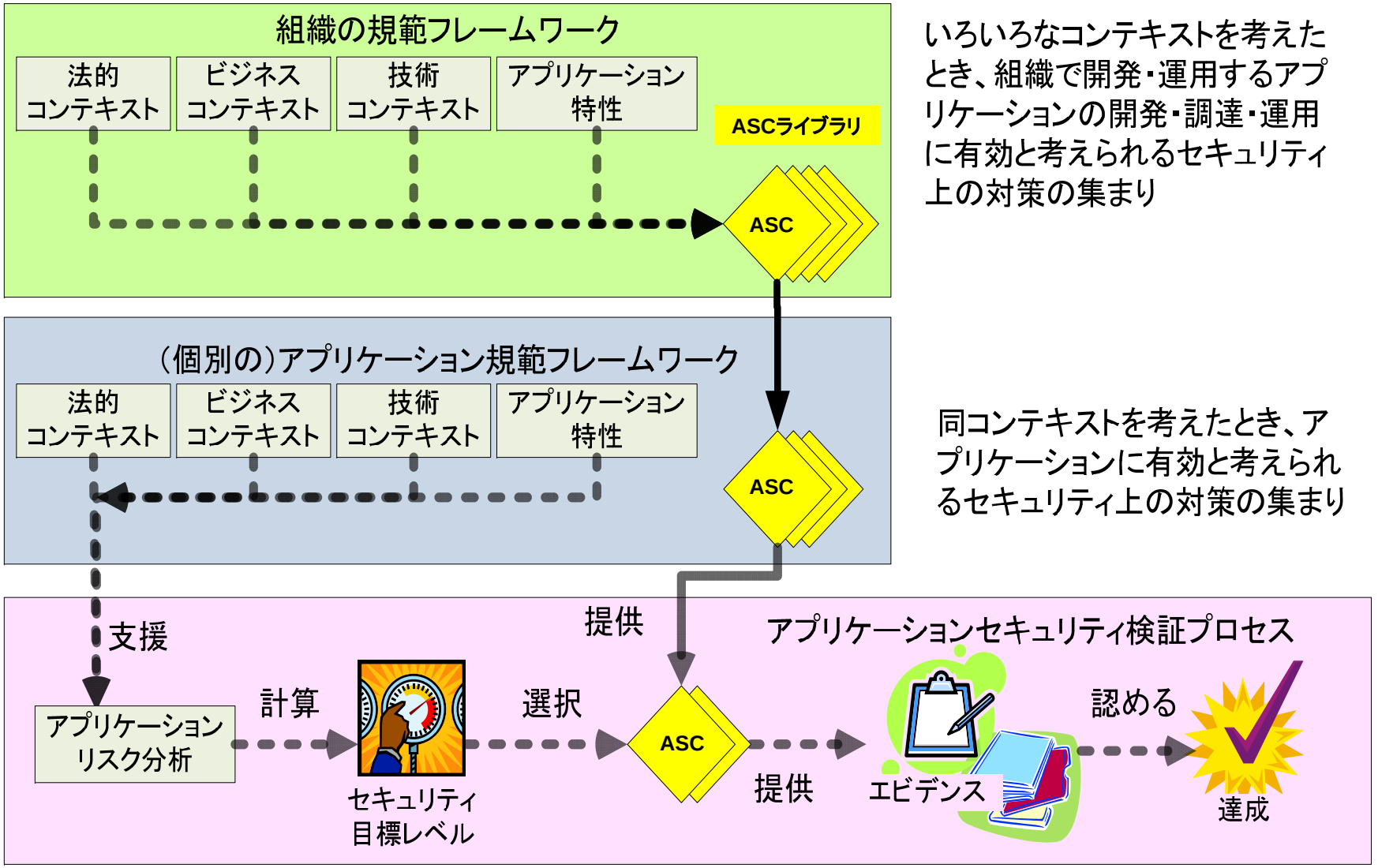
①生産性向上（軽量化）
- 再利用性の向上

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

ASC：Application Security Controls

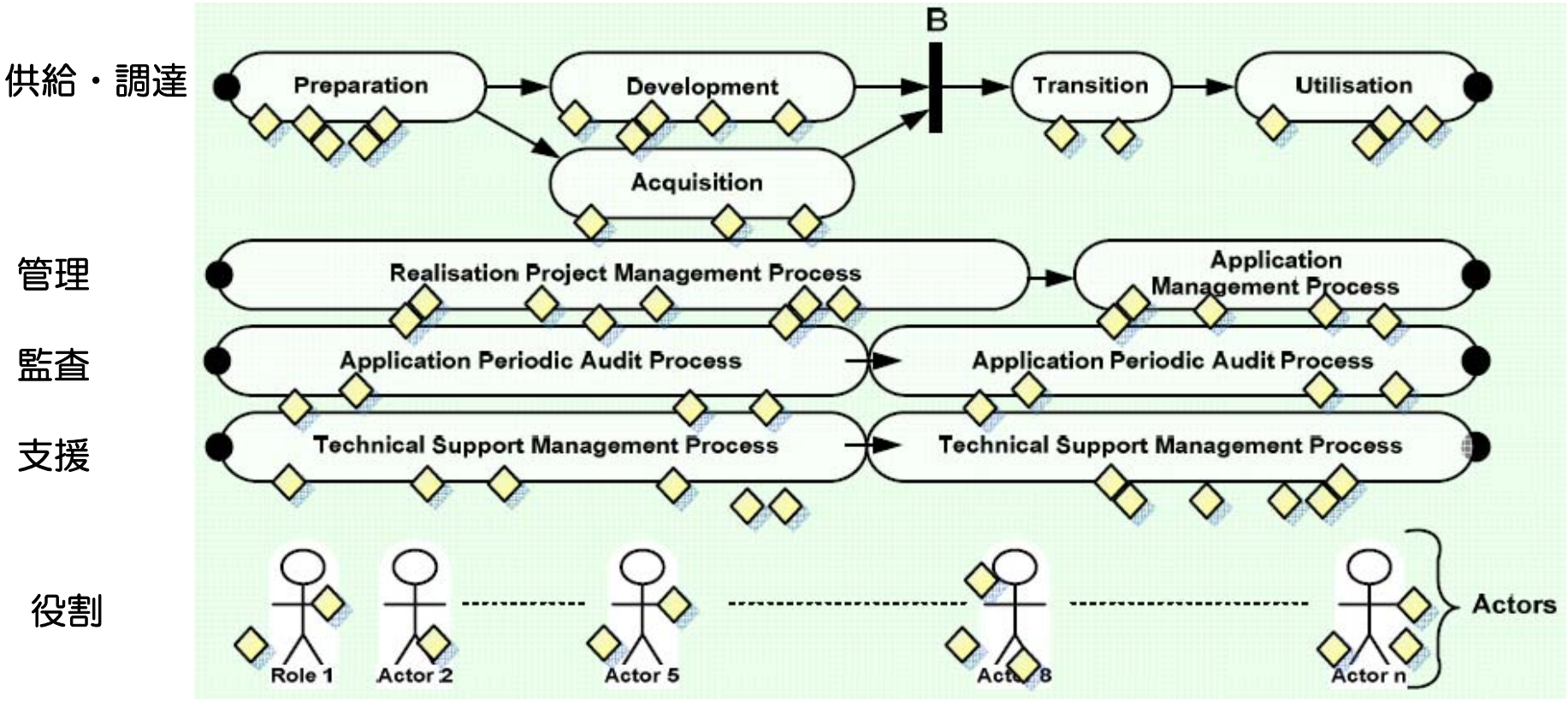


いろいろなコンテキストを考えたとき、組織で開発・運用するアプリケーションの開発・調達・運用に有効と考えられるセキュリティ上の対策の集まり

同コンテキストを考えたとき、アプリケーションに有効と考えられるセキュリティ上の対策の集まり

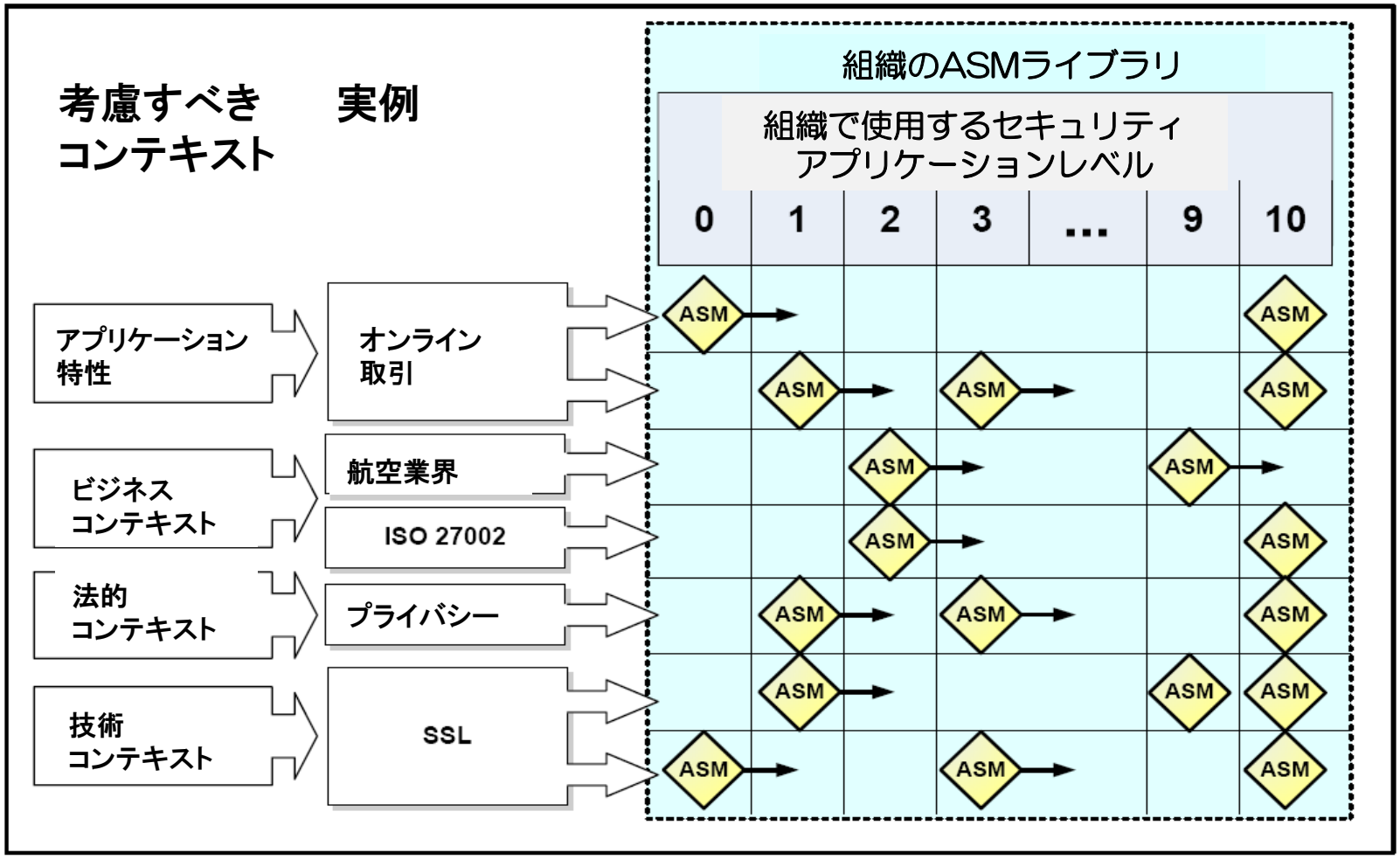
ASCが組織毎に用意される。アプリケーションで必要なものを抽出する。アプリケーションリスクを分析し、セキュリティ目標レベルを決め、アプリケーション毎に集めたライブラリから抽出して使う。設計・開発に使う。また運用時に使うことも考えている。例は、供給者サイドへの適用。

ASMのプロセス・役割への適用



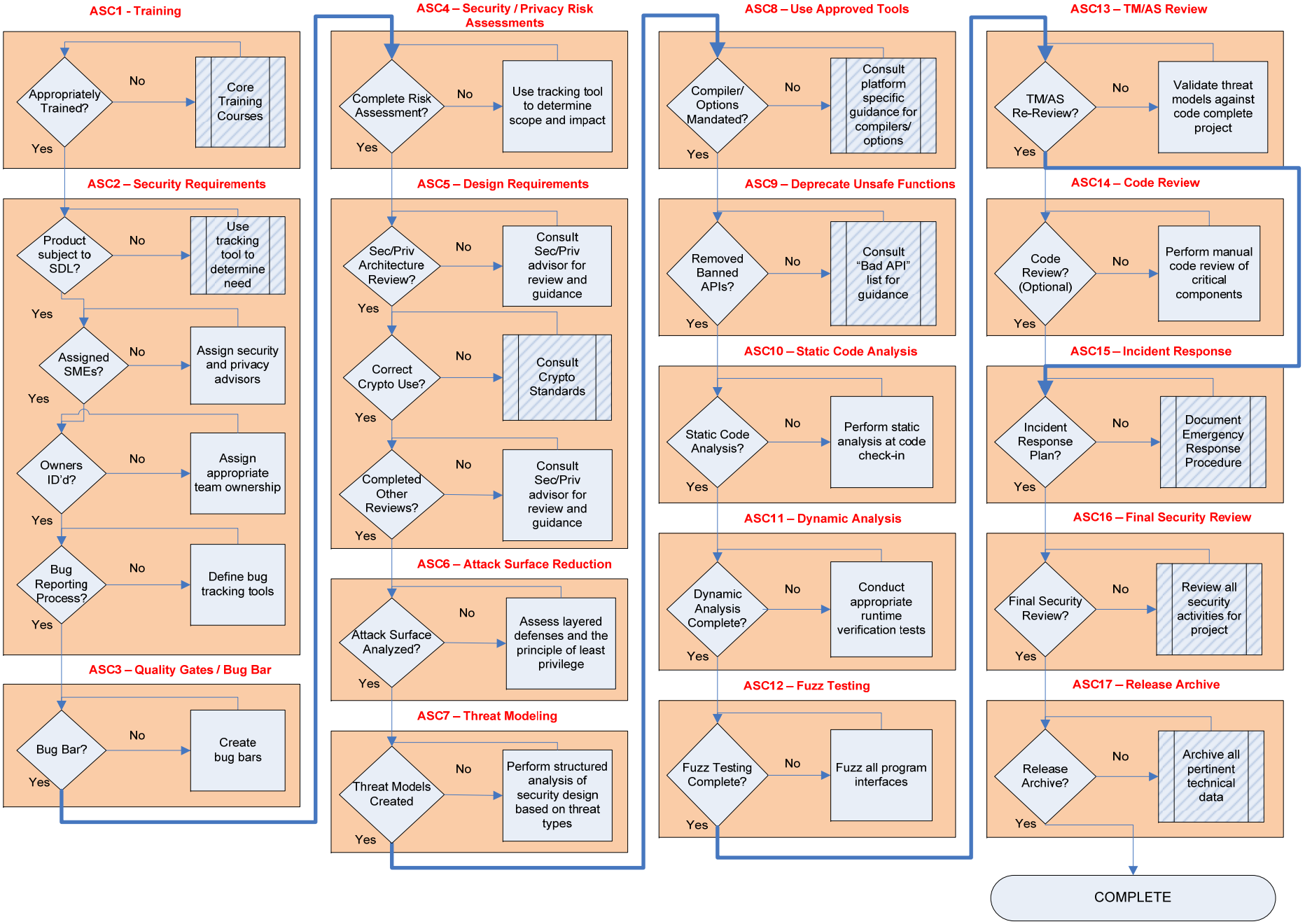
ASC（アプリケーションセキュリティ対策）は、各プロセス（供給・調達、管理、監査、支援）および役割に提供され、エビデンスの生成に利用される。

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ASCが、レベル3-9で別のASCが、レベル10でさらに別のASCを使うことを示している。

ASCの例（マイクロソフトの提案）



情報セキュリティインシデントマネジメント（27035）

- 本審議は、旧規格のISO/IEC TR18044(インシデントマネジメント：標準資料)のIS化（標準文書化）がトリガーとなり、2008年4月京都会合にて審議が開始された。技術文書（TR）は、参考情報の色合いが濃いため、それを標準文書とするための改修、文書内容の最新化が本課題の目的となっている。インシデントマネジメントとは、情報システムへの不正な侵入、攻撃が成功し、システムへの被害、事故として影響が波及する場合、その被害や事故をどのようにマネジメント（検知、対応など）するか　といった命題である。北京会合では、1st CDに基づき審議がなされ、現在の審議においてインシデントマネジメントは、以下のプロセスにより構成されることが合意されている。
  - 計画と準備のプロセス
  - 検知と報告のプロセス
  - 評価と決断のプロセス
  - 対応のプロセス
  - 教訓、勉強のプロセス
- これらのプロセスに従い、情報セキュリティインシデントについて、具体的なガイドラインを記載していくこととなるが、具体的なコメント処理を実施し、次回の会合で3nd CDの審議がなされる予定である。（課題は次頁）

27035 (Redmondにて）

残存する課題:

①Information security weaknessの定義を明確にすること、

②ISIRTの概念とCSIRT/CERTの違いを明らかにすること、

③インシデントのカテゴリ分け、

④インシデントのインパクトのレベル分け、

⑤インシデント報告様式の整理　等

セキュリティのアウトソーシングのためのガイドライン（27036）

前々回のキプロス会合において、NP（新規課題）の提案がなされた案件で、NPのNB（National Body）投票にかかり、北京会合でプロジェクトとして承認されたものである。本プロジェクトのスコープは、「アウトソースされたサービスの調達や利用におけるセキュリティリスクの評価に関わるガイドラインを企業（組織）に提供すること」としている。さらに、本課題はアウトソーシングのためのISO/IEC 27001/27002の管理策の実施を支援するものであり、アウトソーシングのための戦略目的、ビジネスニーズ、リスク低減技術、保証提供などの内容を含んでいる。また、アウトソーシングの範囲を、ICTに限定しておらず、人的リソース、設備管理などのアウトソーシングも対象範囲としている。

次回の会合にて2nd WDが審議される予定である。

27036：課題（Redmondで）

①本規格の対象範囲（Scope）、
②outsourcingの定義、
③対象とする業務の例とその多様性、
④outsourcingのライフサイクル、
⑤outsourcingの一般的な事項と情報セキュリティに係る事項を区別して後者を記述すべきこと、
⑥ISO/IEC 27002の管理策を要約して引用している部分の扱い、
⑦典型的な業務を取り上げた施策についての具体例の提示の必要性

“Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence” (ISO/IEC 27037)

Scope of 27037 after Redmond(1)

- This International Standard gives guidelines for digital evidence management. It describes the processes of identification, collection, acquisition and preservation of potential digital evidence that may be of evidentiary value.
- The objective is to assist organizations in their disciplinary procedures, and to facilitate the exchange of potential digital evidence between jurisdictions. This standard deals with common situations encountered throughout the digital management process.
- The International Standard intends to provide guidance to those responsible for the identification, collection, acquisition and preservation of potential digital evidence. This includes Digital Evidence First Responders, Digital Evidence Specialists, incident response specialists and forensic laboratory managers. This International Standard intends to inform decision-makers who need make a determination regarding the reliability of any digital evidence presented to them.

Current:

Scope of 27037 after Redmond(2)

- This International Standard is applicable to organizations needing to protect, analyze and present potential digital evidence. It is relevant to policy-making bodies that create procedures relating to digital evidence and decision-making bodies need to evaluate digital evidence, often as part of a larger body of evidence. The potential digital evidence may be sourced from any type of media, and refers to data that is already in a digital format. This International Standard does not attempt to cover the conversion of analog data into digital format.
- Application of this International Standard requires compliance with national laws, rules and regulations. The International Standard outlines the minimum requirements necessary for enabling transfer of digital evidence between jurisdictions. It provides a framework for the development of processes and procedures for the identification, collection, acquisition and preservation of digital evidence.

In support of ISO/IEC 27002

- **An implementation guidance of a control of ISO/IEC 27002**

–**13.2.3 Collection of evidence**

–Control

–“Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal) evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).”

–Implementation guidance

–“Internal procedures should be developed and followed when collecting and presenting evidence for the purposes of disciplinary action handled within an organization.

–In general, the rules for evidence cover:

–a) admissibility of evidence: whether or not the evidence can be used in court;

–b) weight of evidence: the quality and completeness of the evidence”

27032- 13.2.3 (日本語）

13.2.3　証拠の収集

管理策

情報セキュリティインシデント後の個人又は組織への事後処置が法的処置（民事又は刑事）に及ぶ場合には，関係する法域で定めている証拠に関する規則に従うために，証拠を収集，保全及び提出することが望ましい。

実施の手引

組織内で扱う懲戒処置のために証拠を収集し提出するときは，内部の手順を定めてそれに従うことが望ましい。

一般的に，証拠に関する規則は，次のことを扱っている。

a)　証拠能力：証拠として法廷での使用可否

b)　証拠の証明力：証拠の質及び完全さ

Content (after Redmond)

- **1 Scope**
- **2 Terms and definitions**
- **3 Abbreviated terms**
- **4 Overview**
- **4.1 Requirements for identification, collection, acquisition and preservation of digital evidence**
- **4.1.1 Auditable**
- **4.1.2 Repeatable**
- **4.1.3 Reproducible**
- **4.1.4 Defensible**
- **4.2 Principle for identification, collection, acquisition and preservation of digital evidence**
- **4.3 Digital evidence management process**
- **4.3.1 Identification**
- **4.3.2 Collection**
- **4.3.3 Acquisition**
- **4.3.4 Preservation**

Content (2)

Redmond meeting

- 27037 “Guidelines for Identification, Collection and/or Acquisition and Preservation of Digital Evidence”は、503件のコメント（GE：88件、TE：289件、Ed：126件）に対し、一部の編集上のコメントを除いた全コメントが処理され、2nd WDに進むことになった。

- 本審議に参加したのは、主に豪、米、スウェーデン、英、FIRST及び日本。2nd WDでは、構成の変更や、ディジタル・エビデンス管理のための能力開発に関する内容の追加、タイトルの変更、法域(jurisdiction)に依存する記述内容の削除等が予定されている。参加国（および組織）間で、特に大きく対立する箇所はなく、今回の審議では、不明確／不適切な記述の解消が主になされた。

NP／SP

Study Period on Redaction

- 本件に関わるSPの審議がなれて、ラポーター（Dr Andreas Fushburger）が目的などを再度レビューし、UK、SG、AT、CA及び日本（5カ国）の賛同により、NPに進むこととなった。ただし、USは最後まで反対の姿勢を貫いた。（上記、日本の賛成は、現地でWG4のMLを用いて皆さんの意見を打診したところ、多くが賛同されたため賛成にまわった。）
- NP文書については、2010年1月5日までにラポーターより提案される予定である。なお、現在のラポーターがActing Project Editor を務め、次会合までにpreliminary draft の作成を行うこととなった。

Proposed Study Periods

1）Storage Security

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

2）Supply Chain Security

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

REDACTION(参考）

A new project proposal was submitted by UK NB on the topic of redaction, which is the procedure for removing sensitive or classified information from documents (electronic or otherwise) to be released publicly. UK NB representative, Dr Andreas Fuchsberger presented the proposal during the 2nd WG 4 plenary meeting in the week and the meeting agreed to initiate a Call for contribution of rapporteur and contents for a new study period on the topic of Redaction.

Thank you for listening Q&A