ITU-T　SG１７

(データネットワーク　およびテレコミュニケーションソフトウェア) における

ISMS-T標準化動向と今後

中尾　康二
KDDI　株式会社　情報セキュリティ技術部
ko-nakao@kddi.com

最新会議の開催情報

開催日程：2004年　3月10日～　3月19日

開催地：　スイス　ジュネーブ

出席国及び出席機関：

21カ国,2国際機関より113名

日本からの出席者（所属）：合計10名

戸田(総務省)、大野（ＣＲＬ）、阿部（横河電機）、渡辺（ＫＤＤＩ）・中尾（総務省参与）、鍛･磯部（日立）、村瀬･石黒（MRI）、日高(SCAT)

SG17のWP構成

WP１：データ網

WP2：開放型システムテクノロジー

WP3：言語及び記述

WP4：品質及び方法

WP5：分散オブジェクト技術

WP2[開放型システムテクノロジー]

＜課題構成＞

課題7/17　IPに関連した下位層プロトコル、およびサービスメカニズム

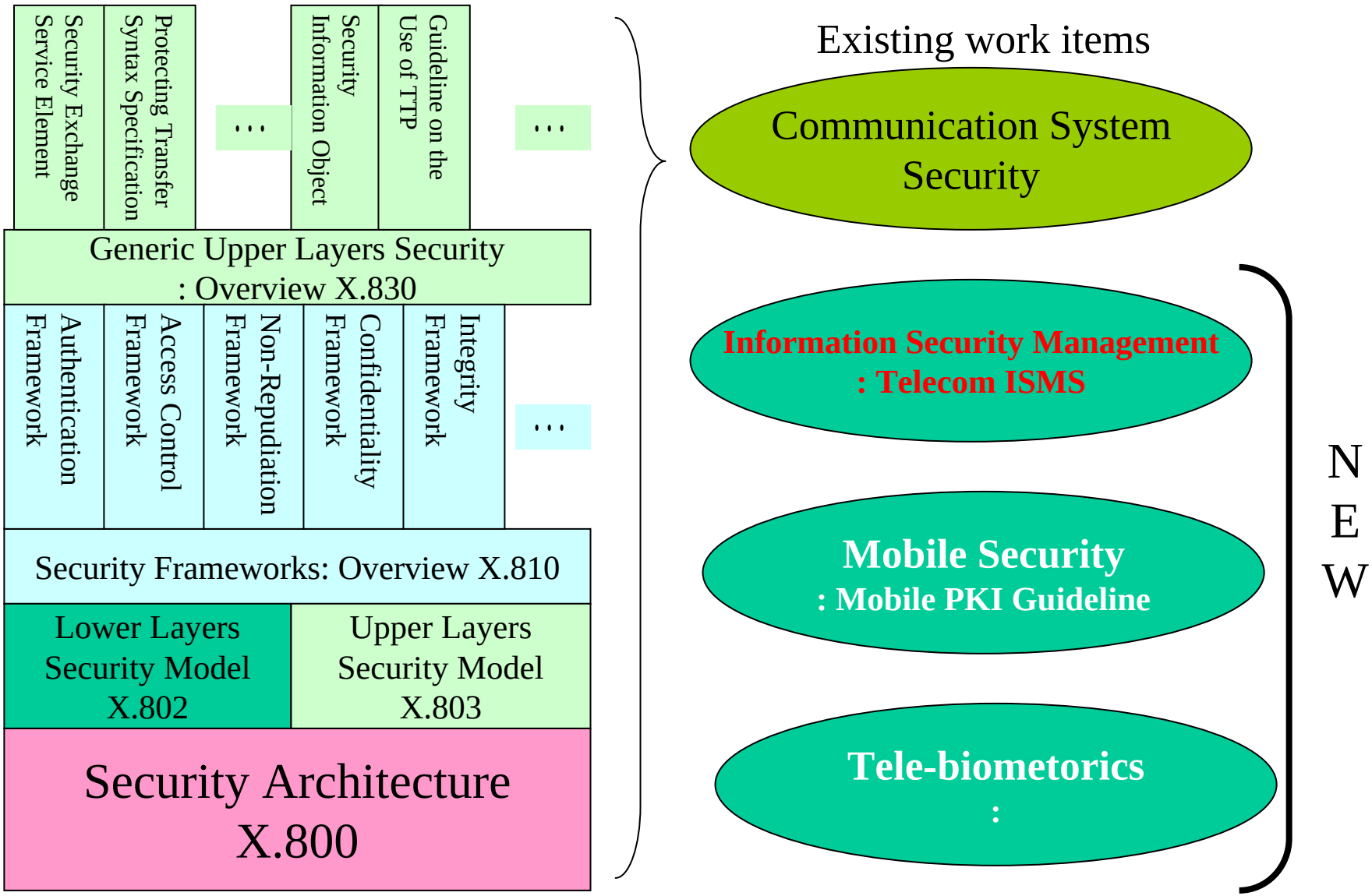
課題8/17　エンド-エンドのQoSマルチキャスト通信

課題9/17　ディレクトリサービスおよびシステム

課題10/17　通信システムおよびサービスのためのセキュリティ要求条件、モデル、ガイドライン

課題11/17　OSI勧告の改版

課題１０の当初の活動目標（２００１年）



課題10/17の活動報告

最終会合にて勧告化申請

Mobile Security

X.m-sec1: Framework of secure technologies for mobile end-to-end data communication

X.m-sec2 : Guideline for implementing secure mobile systems based on PKI

Tele-Biometorics

X.tb : The Telebiometric Multimodal Model – A Framework for the Specification of Security and Safety Aspects of Telebiometrics

ISMS

X.ism : Requirements for Telecommunications of Information Security Management System (T-ISMS)

Security Architecture

前会合にてConsent済み

Security Architecture for Systems Providing End-to-End Communications

先会期（最終会合）にて策定された新しい勧告

1) **X.805**: **Network Security Architecture** (ISO/IEC 18028-2)

2) X.tb (TD 2374 Rev.2) --> **X.1081**
The telebiometric multimodal model - A framework for the specification of security and safety aspects of telebiometrics

3) X.ism (TD 2387 Rev.1) --> **X.1051**
Requirements for telecommunications of information security management system (ISMS-T)

4) X.msec-1(TD 2370 Rev.3) --> **X.1121**

Framework of security technologies for mobile end-to-end communications

5) X.msec-2 (TD 2370 Rev.3) --> **X.1122**
Guideline for implementing secure mobile systems based on PKI

勧告案の概要：

テレコムのための情報セキュリティマネジメント

(ISMS-T)

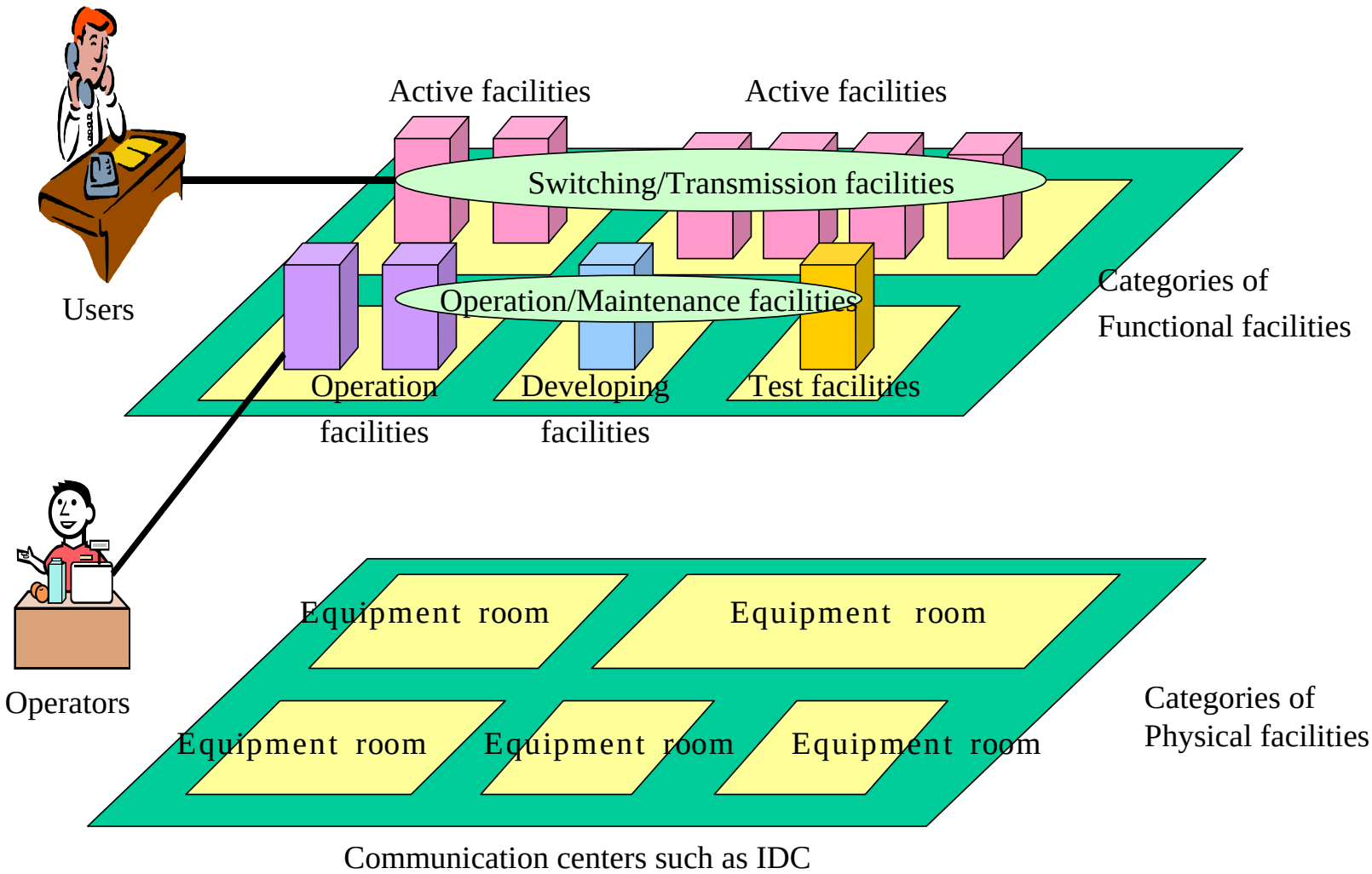
Last Call: June 1st

導入部

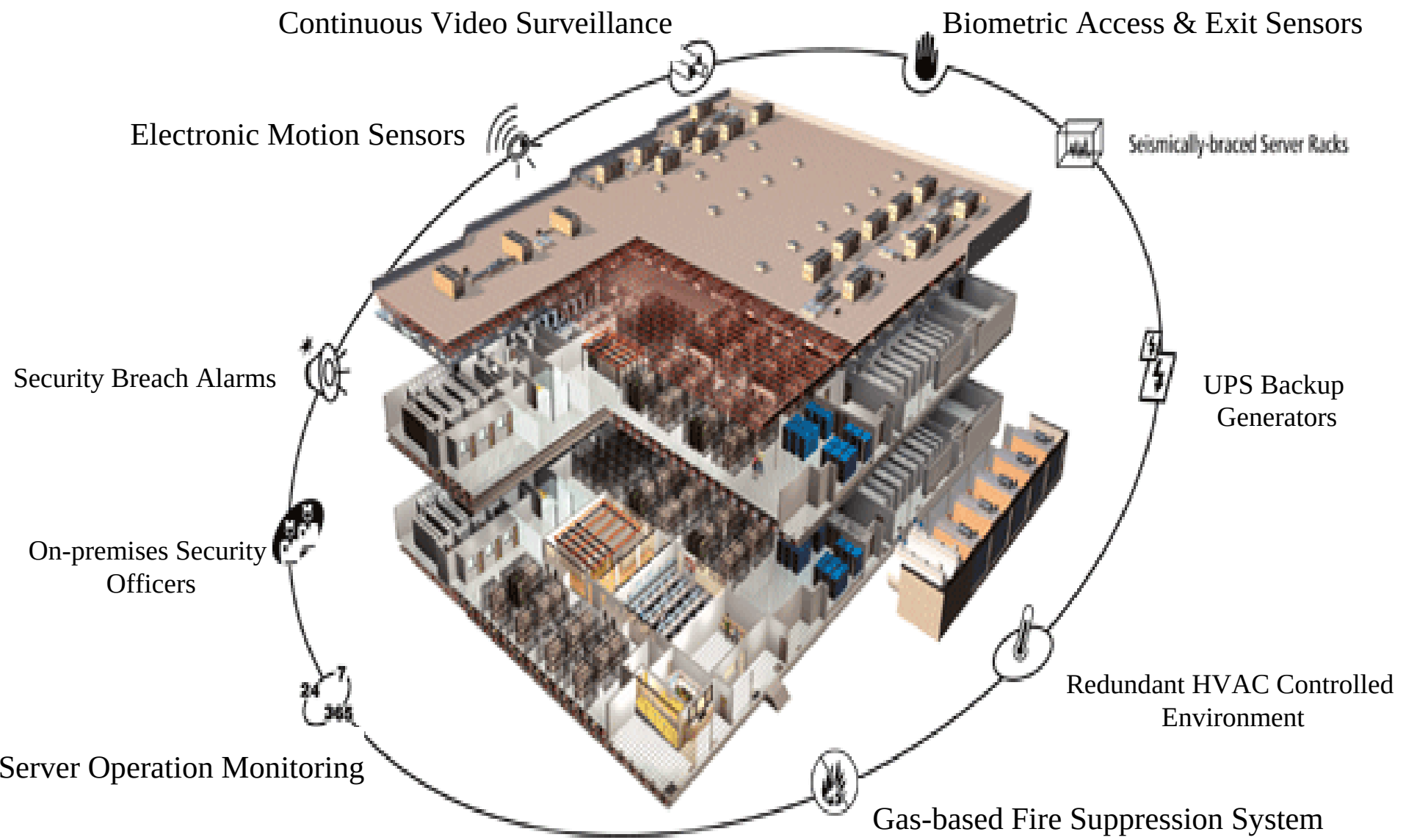
守るものは何？：テレコムの資産は？

- **電話、インターネット、携帯通信における交換設備**：これらは、ルーティング情報、加入者情報、ブラックリスト情報など保有
- **伝送設備**：ケーブル、リレー設備など
- **運用設備**：通信管理システム、課金管理システム、トラヒック管理システムなど（これらは、システム構成情報、顧客情報、課金情報、トラヒックログ情報などを管理）
- **通信サービス資産**：ポータル情報サービス、代理徴収サービス、オペレータ支援サービス、メールサービス、ディレクトリサービス、ローミングサービスなど
- **要員、品質、技術**
- **通信業者の評判、企業イメージ**など

テレコム特有の設備、施設のセキュリティ確保



テレコム特有の設備、施設：iDC 等



移動体サービスにおけるセキュリティ

移動体基地局（BS）の例

*Located outside without strong protections
- Easy to be damaged

*For the Maintenance

- Recovery procedure
- Repairing procedure
- Testing procedure
  ・・・

通信事業者にとって、「情報セキュリティマネジメント」の確保が重要： ISMSの構築

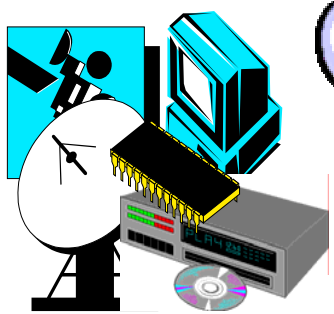
1. セキュリティ基本方針

2. 組織のセキュリティ

10. 適合性 (コンプライアンス)

3. 資産の分類及び管理

9. 事業継続管理



4. 人的セキュリティ

8. システムの開発及び保守

情報をベースとする
通信事業者の資産

5. 物理的及び 環境的セキュリティ

7. アクセス制御

6. 通信及び運用管理

情報セキュリティマネジメントの必要性（相関図）

1．脆弱性、脅威、資産価値の評価

2．リスク分析・評価

4．インシデント対応

・・・

5．対策技術
- IDS、Firewall
- ウィルス駆除
- インシデント分析
- 暗号・認証技術

等

3．リスク低減・回避のための対策選択

P-D-C-Aに則った情報セキュリティマネジメント（ISMS）の確保

ISMS基準
監査基準

脆弱性共有
ISP連携

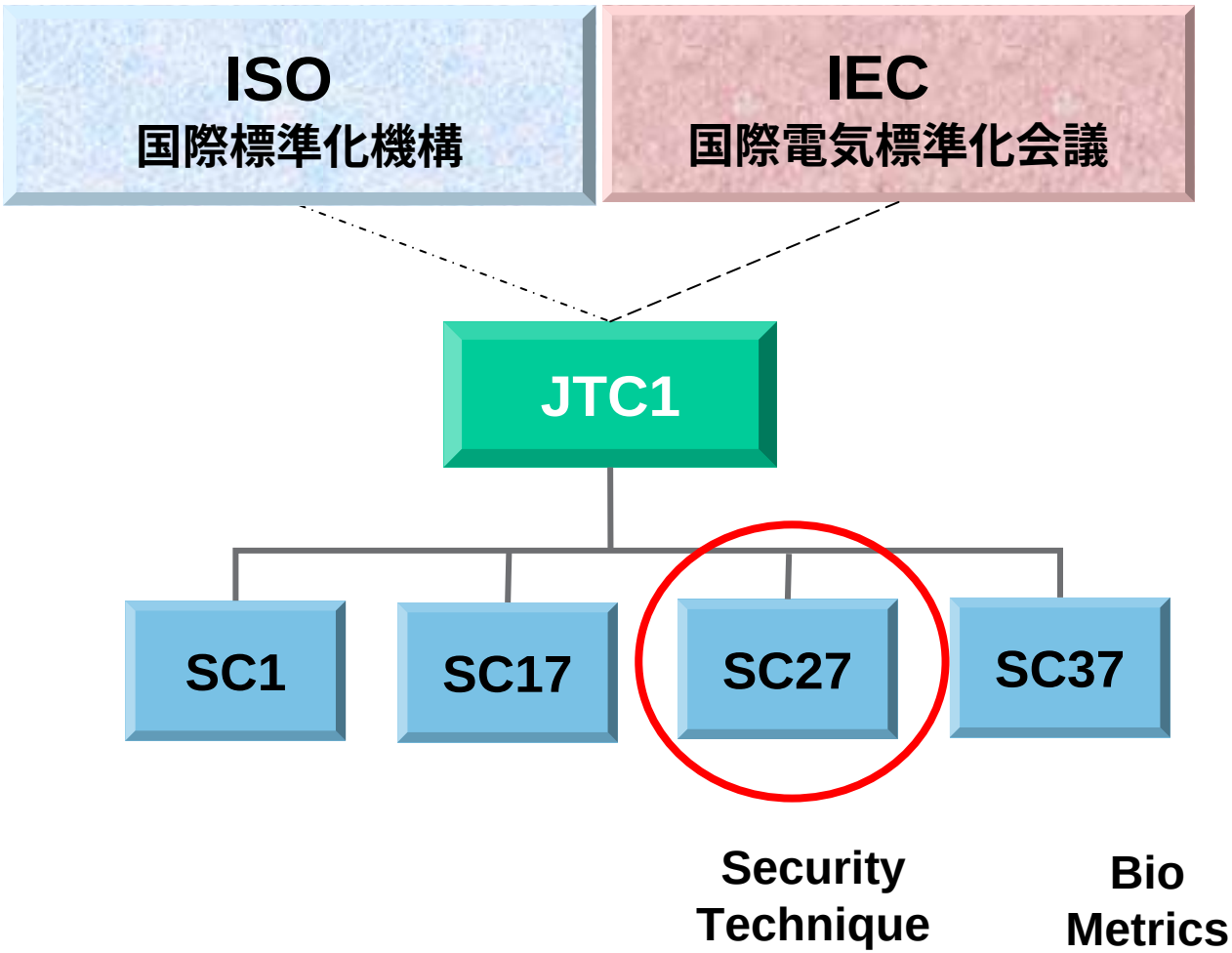
OECD
各種法規制

最新技術
研究開発

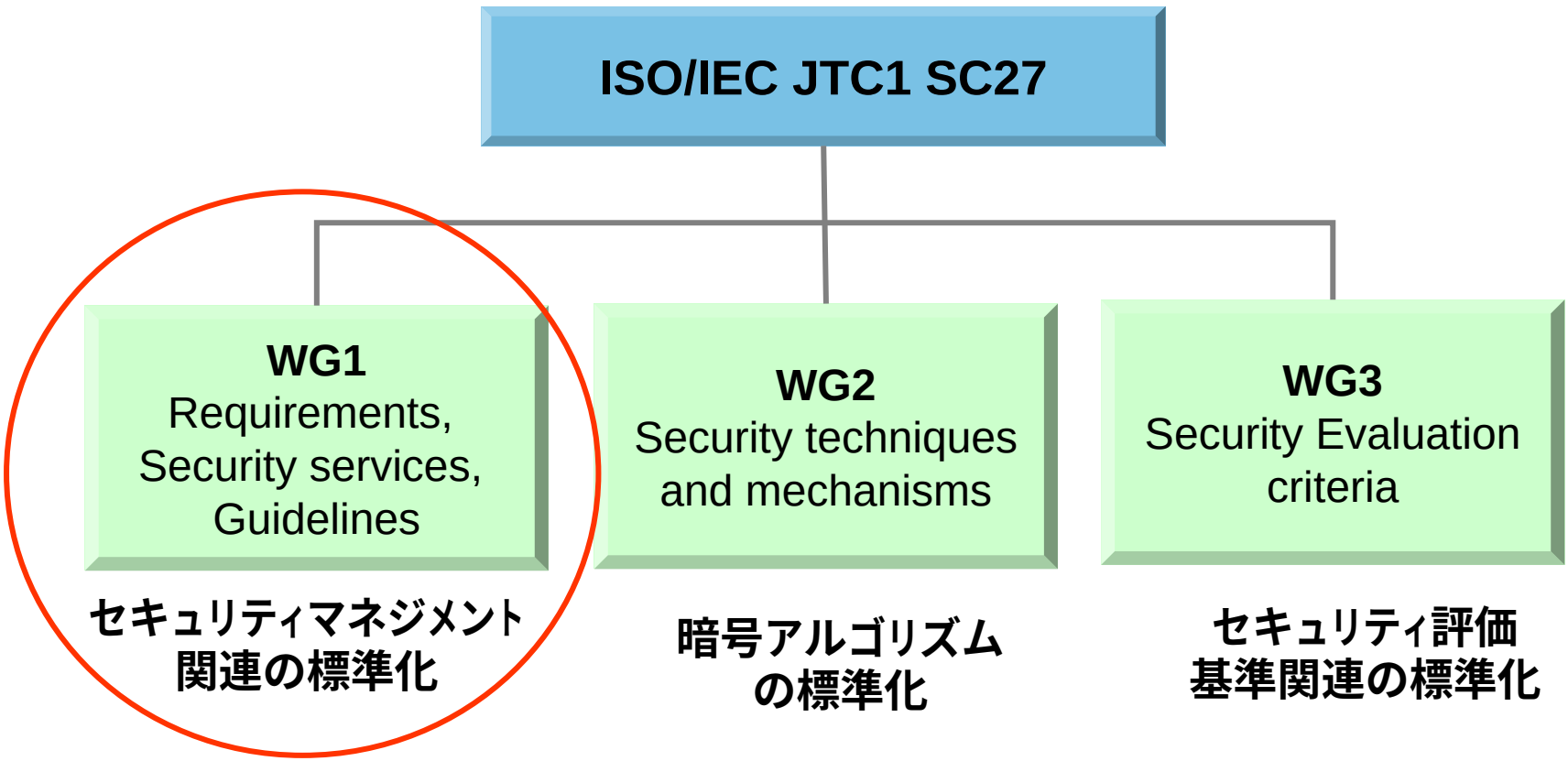
・・・

ISOにおける
情報セキュリティマネジメント
(ISMS)の規格化の現状

ISOの組織（1）


ISO
国際標準化機構
IEC
国際電気標準化会議
JTC1
SC1
SC17
SC27
SC37
Security
Technique
Bio
Metrics

ISOの組織 (2)


ISO/IEC JTC1 SC27
WG1
Requirements,
Security services,
Guidelines
WG2
Security techniques
and mechanisms
WG3
Security Evaluation
criteria
セキュリティマネジメント
関連の標準化
暗号アルゴリズム
の標準化
セキュリティ評価
基準関連の標準化

参加国

- Europe
  - 英、独、仏、伊、ベルギー、スイス、ノルウェー、オランダ、
    フィンランド、オーストリア、デンマーク、アイルランド、
    スウェーデン、ハンガリー、ルーマニア、スロベニア、エストニア、
    ポーランド、スペイン
- Asia & Oceania
  - 韓国、中国、インド、マレーシア、シンガポール、日本、
    オーストラリア、ニュージーランド
- N.America & Latin America
  - 米国、カナダ、ブラジル
- Africa
  - 南アフリカ、ケニヤ

赤字は最近のブラジル会合参加国

ISO/IEC JTC 1/SC27/WG1

- ISO/IEC 13555 Management of ICT security (MICTS)
- ISO/IEC 17799 Code of practice for information security management
- ISO/IEC 18028 IT Network security
- ISO/IEC 18043 Selection, deployment and operations of intrusion detection systems
- ISO/IEC 18044 Information security incident management
- ISMS Requirements specification
- ISMS Metrics and measurements

ISO/IEC 17799 **改訂の流れ**

*Industry 'Code of practice for information security management' **出版***

1992

1995

*BS 7799 'Code of practice' **出版***

*BS 7799 **改訂版 出版***

1999

2000

*BS 7799 **投票にて早期標準化が決定され、ISO/IEC 17799として出版***

*ISO/IEC 17799 **改訂の開始***

2001

Oct 2004

*Revision of ISO/IEC 17799**がFDIS段階となる***

*ISO/IEC 1779:2005 **(改訂版) の発行***

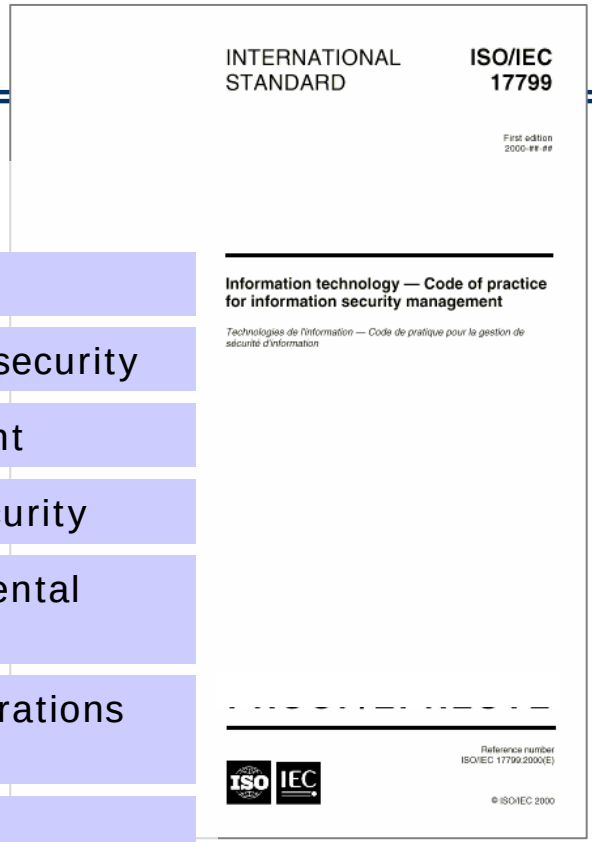
mid-2005

ISO/IEC 17799 改訂作業

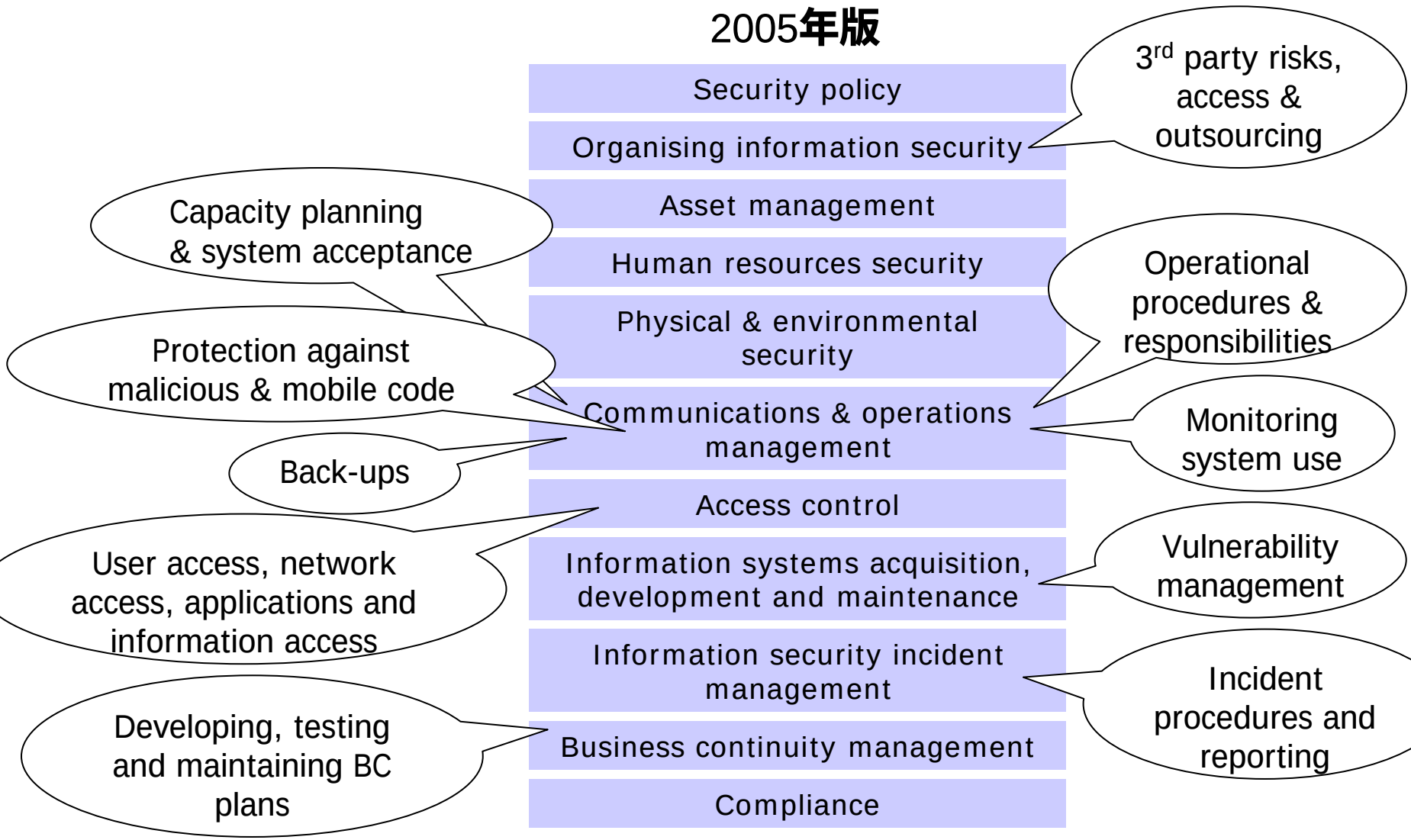
- 23カ国による改訂への貢献
- 2500以上のコメントの提出及び審議（2001-05）
- Technical commentsの審議を2004年10月に終了
- 次回国際会合において、editorial commentsを処理後、最後の投票を実施
- 2005年に出版予定

ISO/IEC 17799 の改訂

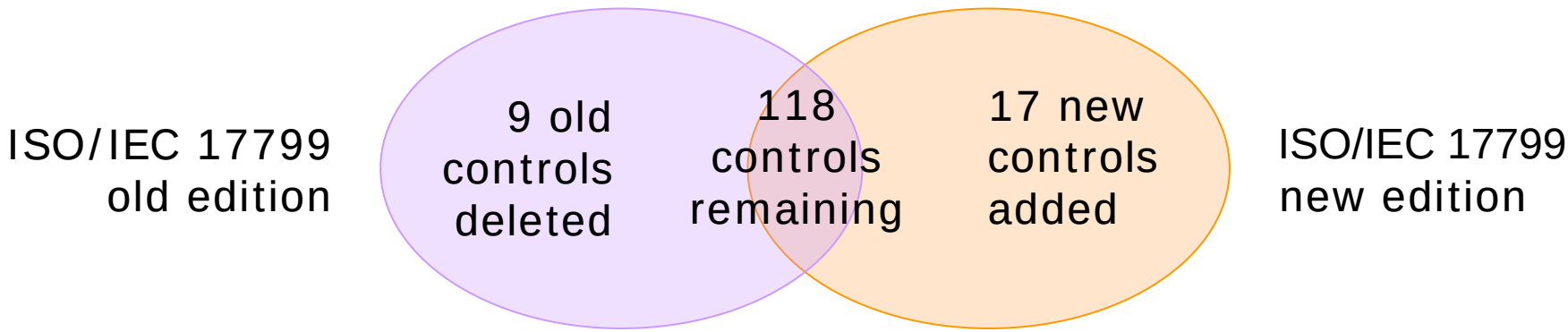
2000年版	2005年版
セキュリティ方針	Security policy
セキュリティの組織	Organising information security
資産の分類及び管理	Asset management
人的セキュリティ	Human resources security
物理的及び環境的セキュリティ	Physical & environmental Security
通信及び運用管理	Communications & operations management
アクセス管理	Access control
システム開発及び保守	Information systems acquisition, development and maintenance
	Information security incident management
事業継続計画	Business continuity management
適合性	Compliance



ISO/IEC 17799の改訂



Control Objectives/Controls



8 new controls objectives

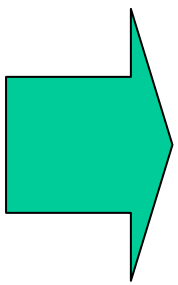
5 control objective **が他の**objectives**に再編成**

改訂版17799の構造

“User friendly interface for control text”

OLD Control text

Control,
some
implementation
guidance and
other supporting
text



NEW Control text

Control

Implementation guidance

Other information

管理策の記述

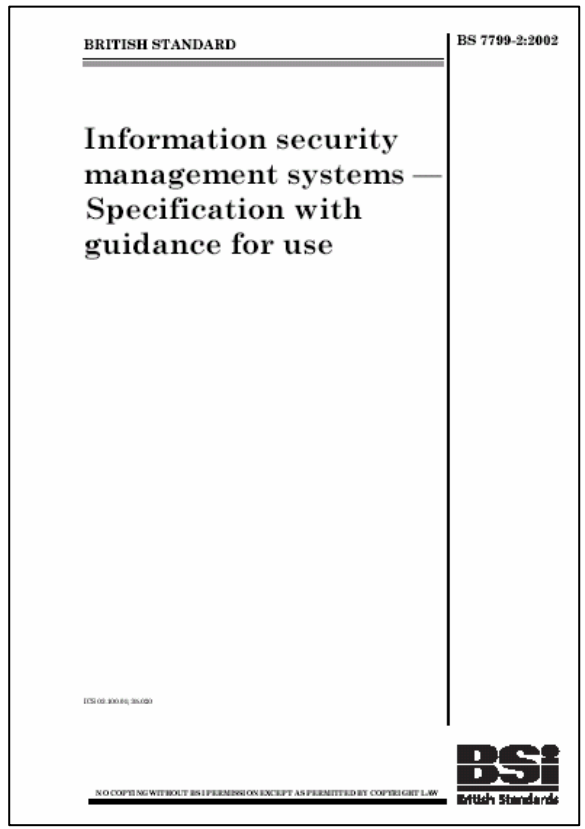
Control Objectives **を満たすための、より詳細な導入のためのガイドライン**

管理策の導入に関連した説明
(管理策の導入時に考慮すべき事項についての説明)
(例:法律への適合性への考慮)

ISMS Specification

- SC27における新プロジェクトの立ち上げ (24743)
- BS 7799 Part 2をベースとした文書の作成
- 次回国際会議にてFinal CD 投票

大きな規格化の進展
→ 国際を跨る認証が可能


BRITISH STANDARD

BS 7799-2:2002

Information security management systems — Specification with guidance for use

BSI British Standards

ISMS Metrics and measurements

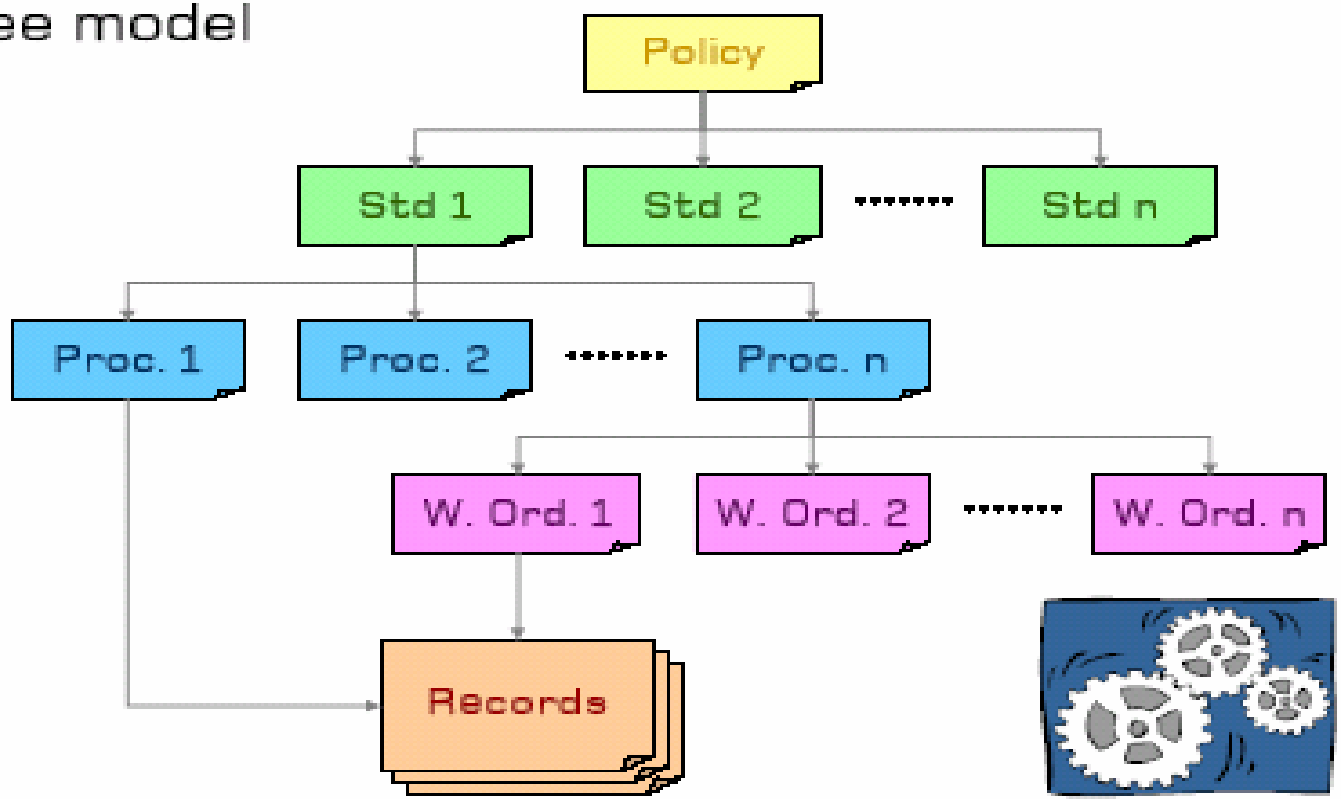
- **SC27 (24742)における新プロジェクトの立ち上げ**
- **Measuring “the effectiveness and performance of ISMS implementations”**
  - **Performance targets**
  - **What to measure**
  - **How to measure**
  - **When to measure**
- **次回SC 27会合（2005年4月）において文書の審議**

M&M Example

Security management model

Records example

It is a tree model



M&M Example

Metrics and indicators

Definition example of indicators

1. **To determine about what do we need information**
   - *Management commitment to security*
2. **To analyze what quantitative data can be collected, the number of….**
   - *M1: Areas or department*
   - *M2: Managers*
   - *M3: Business process*
   - *M4: Areas or departments repreeented at the security committee*
   - *M5: Security committee members*
   - *M6: Managers at the security committee*
   - *M7: Managers at the security committee meetings*
   - *M9: Managers who have received training in security politics and procedures*
   - *M10: Security incidents*
   - *M11: Improvement actions approved by the direction*
   - *Etc., Etc, Etc,*

M&M Example

Metrics and indicators

Definition example of indicators

3. **To establish a relation between the data, which will give out a useful information**

- *I1: M6/M2,* — *Ratio of managers with security responsibilities*
- *I2: M7/M6,* — *Ratio of managers with security responsibilities who usually attends the security committee meetings*
- *I3: M9/M2,* — *Relation of managers who have participated in the training program of corporative security*
- *I4: M4/M1,* — *Horizontality of the security*
- *I5: (I1+I2+I3)/3* — *Management commitment to information security*
- *Etc, Etc.*

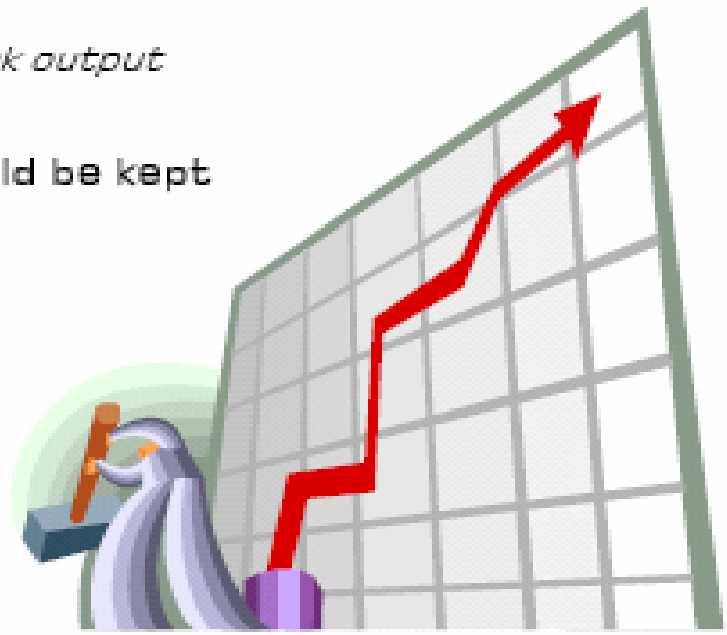
M&M Example

Metrics and indicators

Definition example of indicators

4. **To define de administrative aspects**
   - *Responsible person*
   - *Security objectives and controls related with the indicator*
   - *Actualization period*
   - *Audience*
   - *Action planning with regard to rank output*

5. **To establish the rank within it should be kept**
   - *I1 > 0,75*
   - *I2 > 0,5*
   - *I3 = 1*
   - *I4 > 0,8*
   - *I5 > 0,75*



Risk Assessment

- **ISO/IEC TR 13335:1-5**
  GMITS
  (Guideline for Management of IT Security)
  ITセキュリティ管理の指針
- **MICTS　(新)**
  (IT Security techniques- Management of Information and Communications Technology Security)
  - **ISO/IEC 13335-1: Part1:Concepts and models for managing and planning ICT Security 発行**
  - **Part2:Techniques for information security risk management**

Road Map ISO/IEC JTC 1/SC27 WG1

ISO/IEC 17799

BS 7799 Part 2

ISO Guides 62, EA 7/03

ISO/IEC 18044 Information security incident management

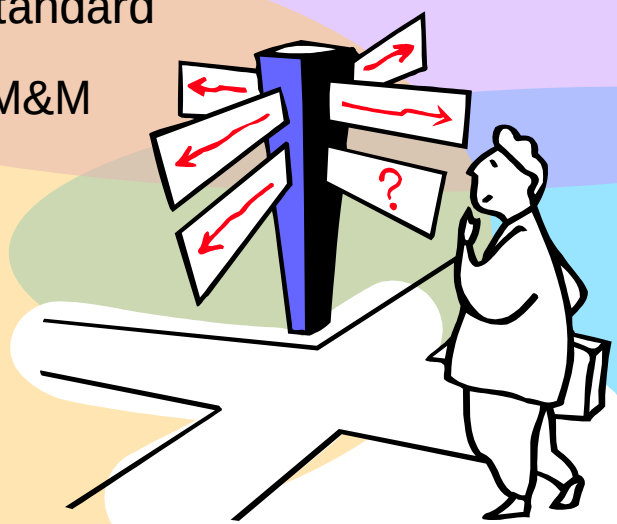
GMITS/MICTS (ISO 13555)

TTP services

IT Network security

ISMS standard

ISMS M&M



New information security standards and guidelines

Future requirements

Road Map ISO/IEC JTC 1/SC27 WG1

ISMS requirements specification standard

current << >> future

TYPE A - Management System Requirements Standards

ISO/IEC 17799

ISMS implementation guidance (Study period)

TYPE B - Management System Guidelines Standards

ISO/IEC 18044 Information security incident management

ISO/IEC 13555 MICTS Parts 1 and 2

ISMS metrics and requirements standard

TYPE C - Management System Related Standards

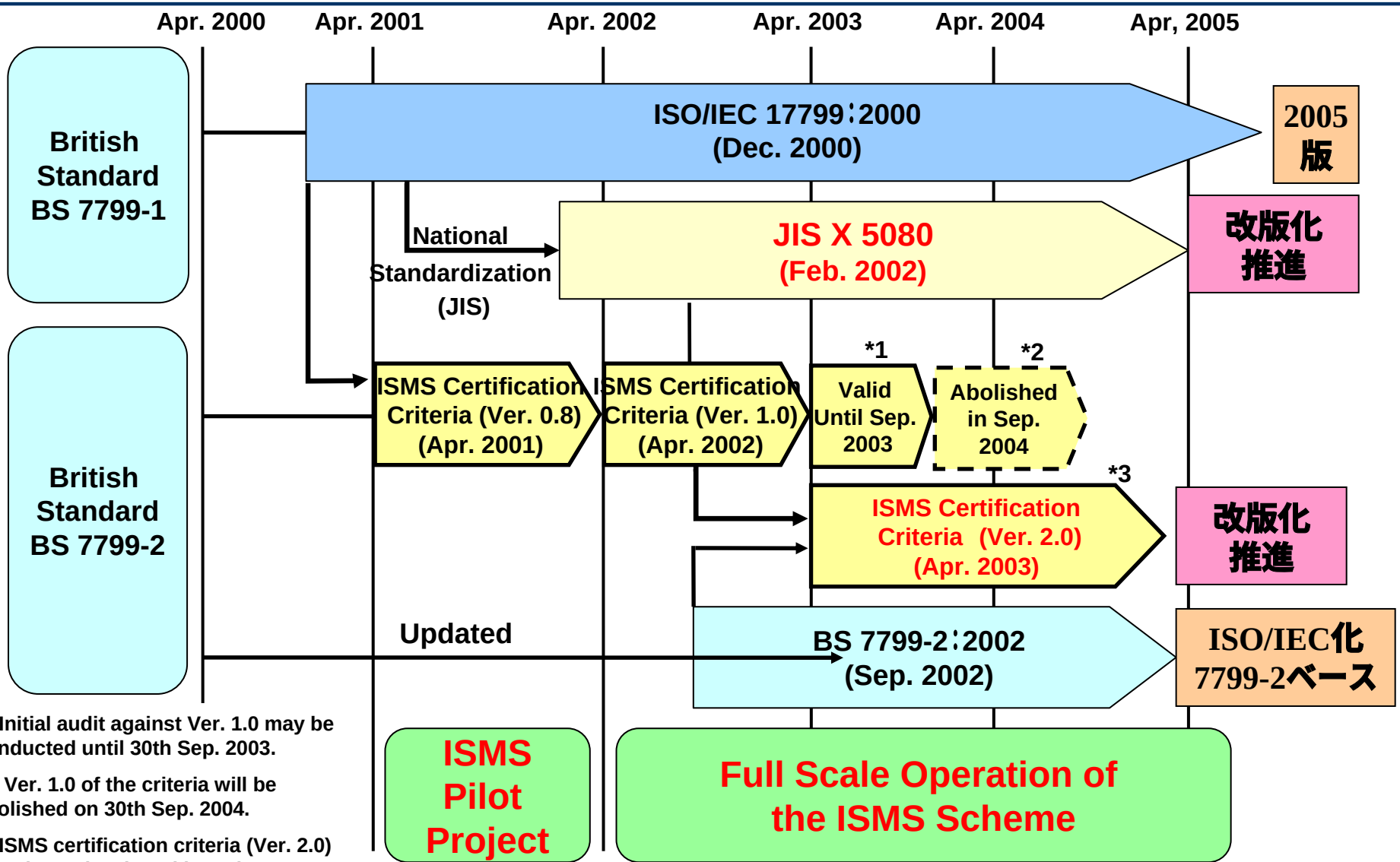
ISMS monitoring and review

ISMS continual improvement

ISMS internal audits

ISMS risk management standards

ISMSに関する規格化の流れ：国際、国内



*1 Initial audit against Ver. 1.0 may be conducted until 30th Sep. 2003.

*2 Ver. 1.0 of the criteria will be abolished on 30th Sep. 2004.

*3 ISMS certification criteria (Ver. 2.0) have been developed based on BS 7799-2:2002, and with regard to terms and expressions the compatibility with JIS X 5080:2002 is ensured.

ISMSの今後

- ISMS国際規格化のさらなる推進
- ISOマネジメント規格策定ロードマップ
  日本からの入力が評価されている
- ISMS構築、運用における
  課題抽出、情報共有
- 課題解決に向けた活動：ガイドライン化？
- セクターベースのISMS Specificationの作成
- 国際的なクロスボーダー認証機構の構築

X.1051 の概要

セクターベースのISMS基準

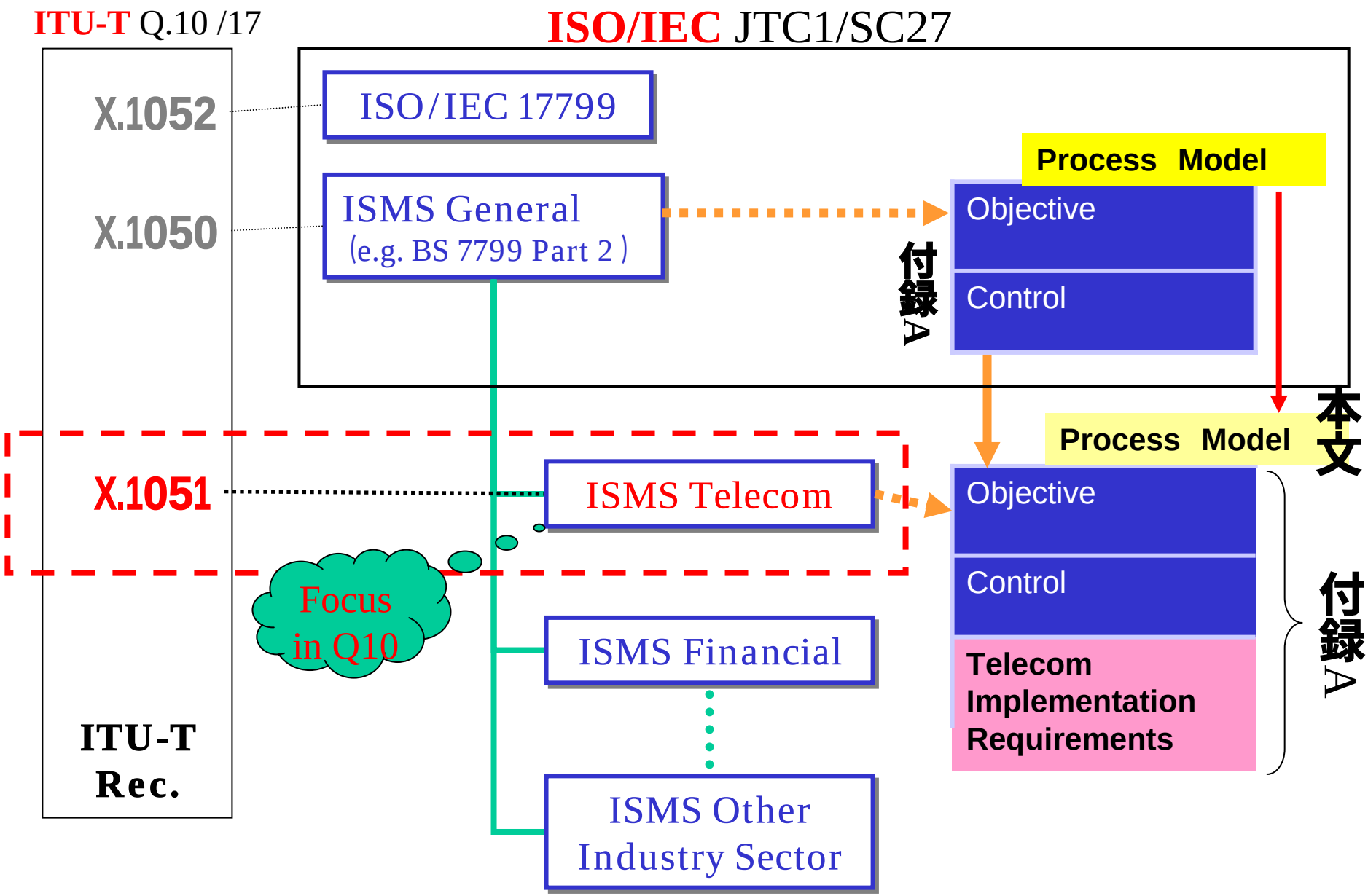
＊医療 → ISO/IEC 27799

＊金融 → ISO/TC68

＊通信 → X.1051 ISMS-T (ITU－T)

＊その他

新しいテレコム用ISMSの位置付け



ISMSプロセスに適用されるPDCA モデル

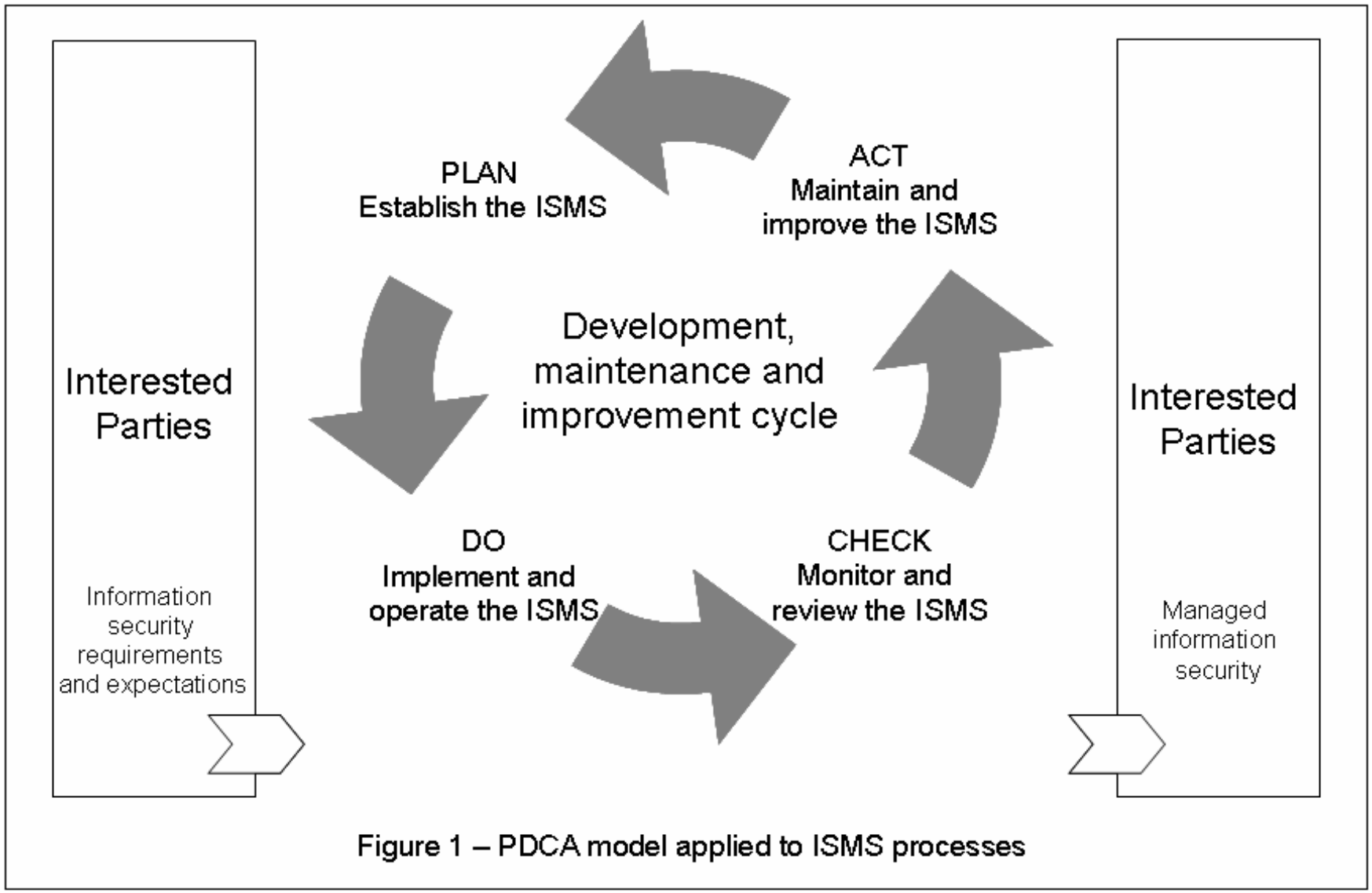


Figure 1 – PDCA model applied to ISMS processes

X.1051 目次

X.1050?

ISMS General
e.g. BS7799-2

Secure areas

Control objective

To prevent unauthorized access, damage and interference to business premises and information.

Securing offices, rooms and facilities

Control

Secure areas shall be created in order to protect offices, rooms and facilities with special security requirements.

ISMS Telecom

X.1051

Secure areas

Control objective

To prevent unauthorized access, damage and interference to business premises for providing telecommunications business and information regarding to telecommunications business.

Securing offices, rooms and facilities

Control

Secure areas shall be set to protect facilities involving special security requirements.

Telecom implementation

Securing communication centers

To protect communication facilities such as switching facilities for providing telecommunications business (hereafter referred to as communication centers), the following shall take place.

…

Securing telecommunications equipment room

X.1051の構造

3 Security policy

3.1 Information security policy

Control objective: To provide management direction and support for Information security.

Controls

3.1.1 Information security policy document

Management, published and communicated, as appropriate, to all employees, shall approve a policy document.

<Telecom Implementation Requirements>

I) An information security policy must be in place over systems supporting wireless internet services to ensure that systems are secured, that security is maintained, and that any suspected security breach is detected, reported, investigated and resolved in a timely manner. These policy documents must include:

§ Corresponding wireless internet security procedures, detailing the regular procedures that need to be performed in order to implement the security policies;

.....

Annex Aの目次

- **2 Organisational Security**
- **3 Asset management**
- **4 Personnel security**
- **5 Physical and environmental security**
- **6 Communications and operations management**
- **7 Access Control**
- **8 System development and maintenance**

通信事業者のための資産

5 Asset classification and control

5.1 Accountability for assets

Control objective: To maintain appropriate protection of organization assets.

Controls

5.1.1 Inventory of assets

An inventory of all important assets associated with each information system shall be drawn up and maintained.

<Telecom Implementation Requirements>

An inventory shall be drawn up and maintained of the important assets associated with each telecommunications facilities. Examples of assets associated with telecommunications facilities are:

a) Routing information, subscriber information and blacklist information, etc. in switching facilities or transmission facilities.

b) Trouble information, configuration information, customers information, billing information and traffic statistical information, etc. in operation facilities or control facilities.

....

通信事業者における資産の例

1) Switching facilities, transmission facilities

- routing information
- subscriber information
- blacklist information, etc.

2) Operation facilities, control facilities

- trouble information
- configuration information
- customers information
- billing information
- traffic statistical information, etc.

4　Personnel security の例

4.1.3　Reporting software malfunctions

Control

Procedures shall be established for reporting software malfunctions.

Implementation requirement for Telecom

Procedures shall be established for reporting software malfunctions existed in telecommunication system. The following actions should be considered.

a) The signs of the problem and any messages appearing on the telecommunication management system should be noted.

b) The telecommunication system should be isolated, if possible, and use of it should be stopped. The appropriate contact should be alerted immediately. If the system is to be examined, it should be disconnected from any telecommunication operating networks before being re-powered.

c) The matter should be reported immediately to the information security manager.

Appropriately trained and experienced staff should carry out to recover it.

ISMSに関する
今後の課題（1）
（General）

国際的なクロスボーダー認証機構の構築

- ISMS　Specificationの国際規格化
  2005（春）FCD投票→2005（秋）FDIS
  （中尾の読み）
- 国際的なクロスボーダー認証の実現
- IAF（International　Accreditation　Forum）による国際認証
- 日本における体制の整備・検討
  JIPDEC、JABの役割分担の整理

→　新たな国際間認証の問題の検討も要

ISMSにおける今後の課題

- ISMS国際規格化（ロードマップに沿って）
- ISMS構築、運用の課題抽出、情報共有
  - ＊社内の情報セキュリティのための体制
  - ＊教育、トレーニング
  - ＊大規模化
  - ＊内部監査
  - ＊個人情報保護などとの関係
  - ＊具体的な技術対策との連携、適用方法
  - ＊国際認証のための課題　などなど
- 課題解決に向けた活動：
  - ＊ガイドライン化の検討、**セクターベース検討**

ビジネスの価値を高め、効果的なISMS構築運用、これが究極の狙い！！

ISMSに関する今後の課題 (2)

次会期に向けた

ITU-T SG17

セキュリティ技術に関わる課題

List of Questions of Security in SG17

Q.10G (G/17) - Communications System Security Project
(Question text: TD 2402)

Q.10H (H/17) - Architecture and Framework
(Question text: TD 2382)

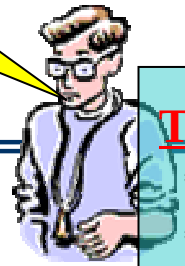
Q.10I (I/17) - Cyber Security
(Question text: TD 2416 Rev.1)

Q.10J (J/17) - Security Management
(Question text: TD 2420)

Q.10K (K/17) - Telebiometrics
(Question text: TD2368 Rev.3)

Q.10L (L/17) - Secure Communication Services
(Question text: TD 2429)

Telecom Systems Users



Q10K

Telebiometorics Technology

*核 Telebiometorics

*Telebiometorics システムメカニズム

Q10J

Security Management

*ISMS-T

*インシデント マネジメント

*リスク評価 手法

* 17799等

Telecom Systems

Applications & Services Security for telecom

Q10L

*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

Q10I

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

*セキュリティ戦略

Security Architecture & Framework

*X.800 series

*新体系

*将来のモデル、フレームワーク

Q10H

Q10G

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

Question 10J/17: Security Management

Task Objectives

1)X.1051の保守、改善、改定作業を実施。

2)既存勧告とISO/IEC国際規格との関係について整理（類似点、相違点などの観点から）。
リスクやインシデントマネジメントの点の検討を優先する

3) 通信におけるリスクマネジメント技術（手法）について検討し、勧告化を進める

4) セキュリティインシデントの対応方法などの手順に関わる検討、および勧告化を実施する

ISMSに関する
今後の課題 (3)

ISMS **ユーザグループ**

これまでのISMS IUG

- ISMS IUG（International User Group)の設立(2000年)：国際ユーザグループ
- 委員長：Edward （Ted) J Humphrey
- 当初の目的：
  - ＊ISMSの啓蒙普及:
    - IUGセミナーの開催：前回はブラジル
  - ＊BS7799-2 の国際規格化
    - ISO標準化活動への参加

仲間を増やす！

ISMS　UGの意義

情報セキュリティマネジメントシステム（BS7799-2）

ISMS
啓蒙活動
セミナー　等

BS7799
規格化への努力
・グローバル化
・国際規格化

ISMS構築・運用に関する情報共有
・国際的に
・構築ツール
・事例紹介
・問題解決

New!

現状のIUGメンバ

＊オーストラリア
ニュージーランド
＊ブラジル
フィンランド
＊ドイツ
インド
ポーランド
アイルランド
韓国
オランダ
ノルウェイ
シンガポール
南アフリカ
スウェーデン
＊英国　　等

＋　日本

New!

日本ISMSユーザグループの発起メンバー等

●日本ISMSユーザグループは、以下の発起メンバーの協力により、2004年7月に任意団体として発足しました。

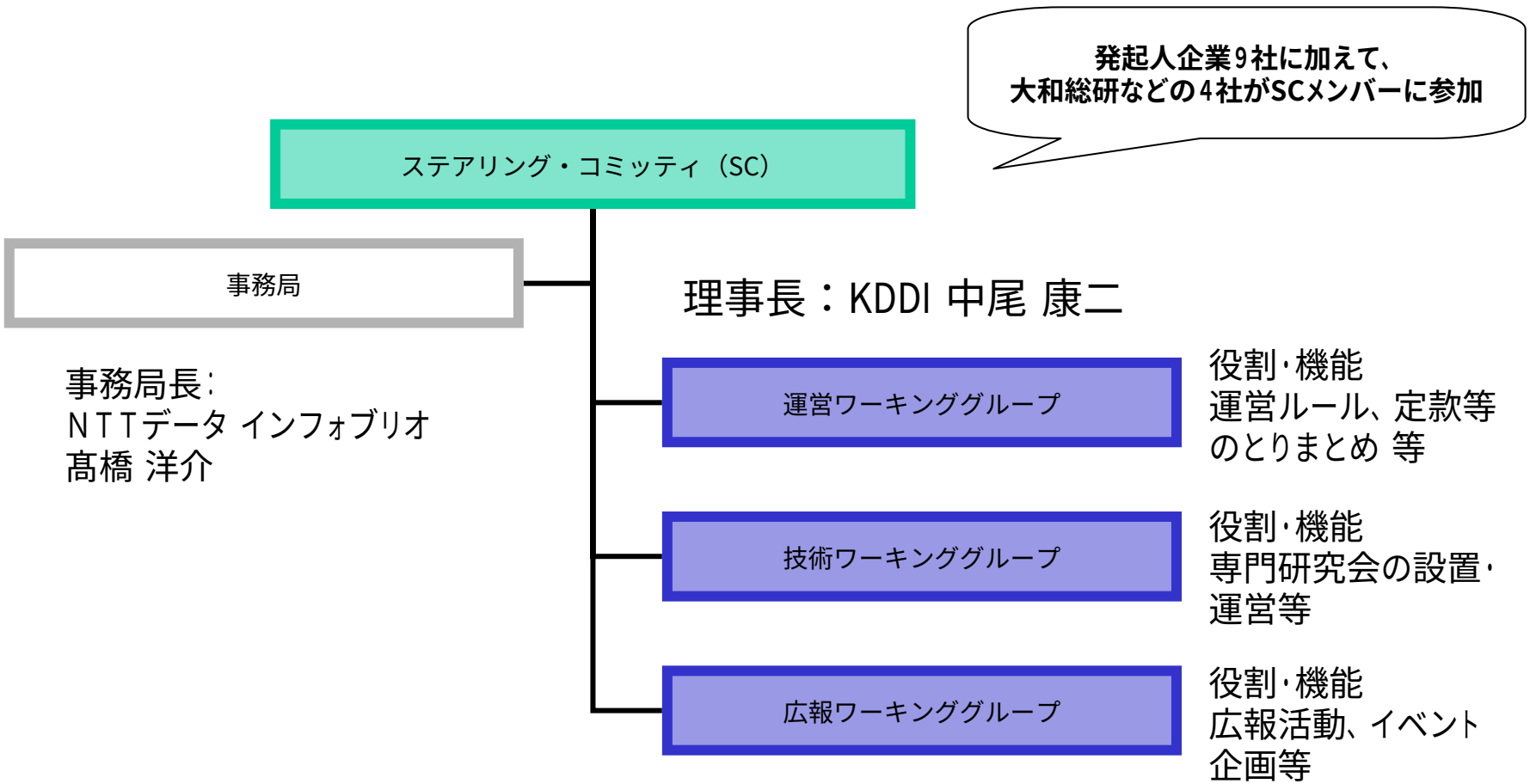
発起メンバー

- IBM ビジネスコンサルティングサービス株式会社
- 株式会社アズジェント
- NTTコミュニケーションズ株式会社
- 株式会社NTTデータインフォブリオ・セキュリティコンサルティング
- グローバルセキュリティエキスパート株式会社
- KDDI株式会社
- 日本電気株式会社
- 株式会社日立製作所
- 松下電器産業株式会社　　以上9社

オブザーバ

- 経済産業省　商務情報政策局　情報セキュリティ政策室
- 財団法人 日本情報処理開発協会（JIPDEC）

日本ISMSユーザグループの運営体制（案）



日本ISMSユーザグループの役割

- ISMS構築、運用における
  課題抽出、情報共有
- 課題解決に向けた活動：ガイドライン化
- セクターベースISMSの構築など

連携の重要性：

ユーザグループメンバ間の連携

JIPDECとの連携

ISMS監査機関との連携

総括 今後の活動の方向性

1）日本における活動が期待される
2）本格的な検討の開始時期にある
3）ISPなど通信事業者のための、
ISMSの検討が必要
4）ISMS-Tの改版を積極的に進める
ことにより、日本発の基準化を
目指す。
5）本セキュリティWGにて活動が
活性化できることが期待される。

世界への浸透、貢献を目指す