



ISO/IEC27005 (Information Security Risk Management) 概要

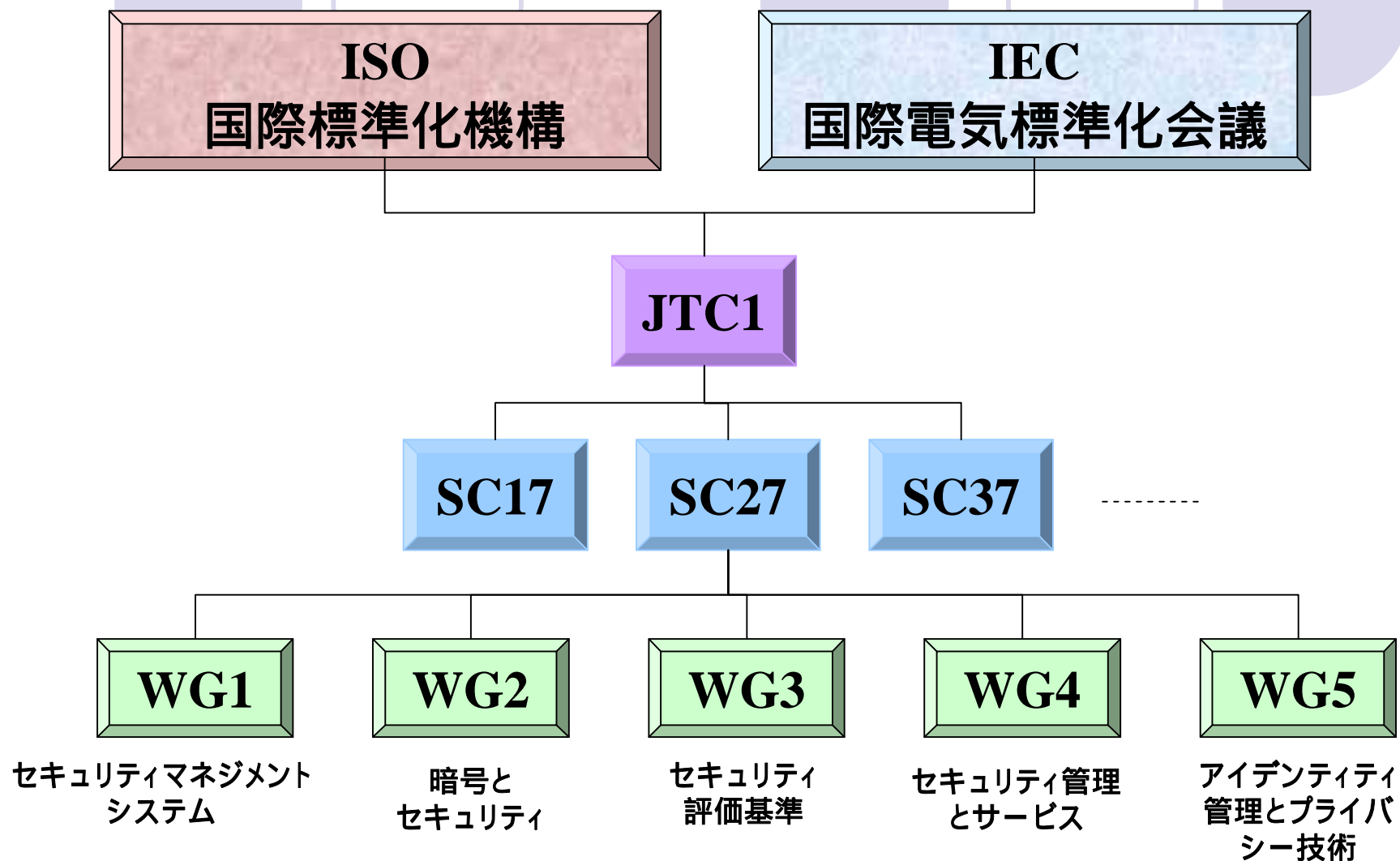
三菱電機株式会社
情報技術総合研究所
中野 初美

内 容



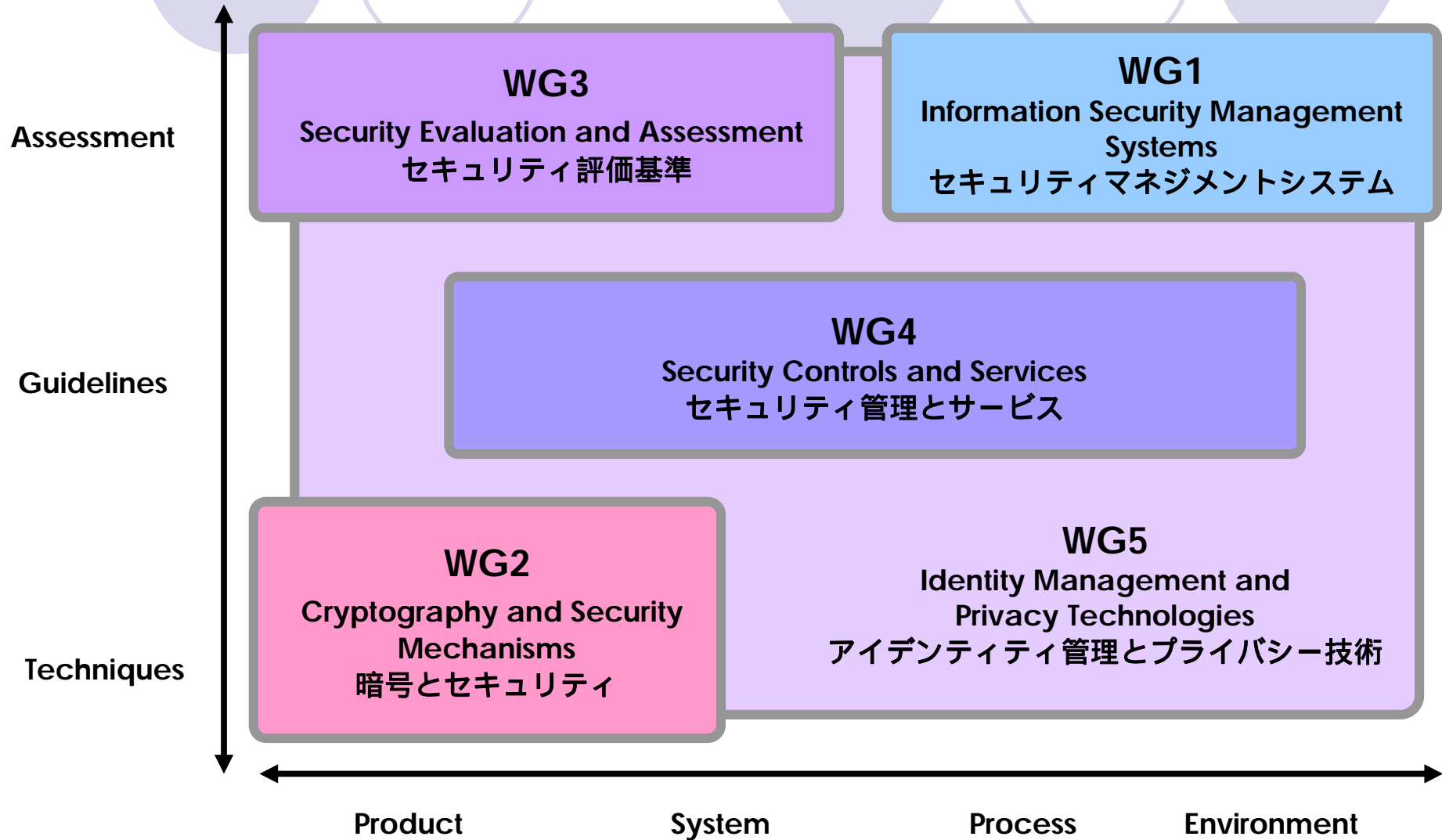
- ISO/IEC27005:2008の概要
 - ISO組織
 - ISO/IEC 27000シリーズ規格
 - 内容の変遷
- ISO/IEC27005:2008の詳細
 - 規格の構成、特徴
 - リスクマネジメントプロセス
 - 各アクティビティの詳細

ISOの組織

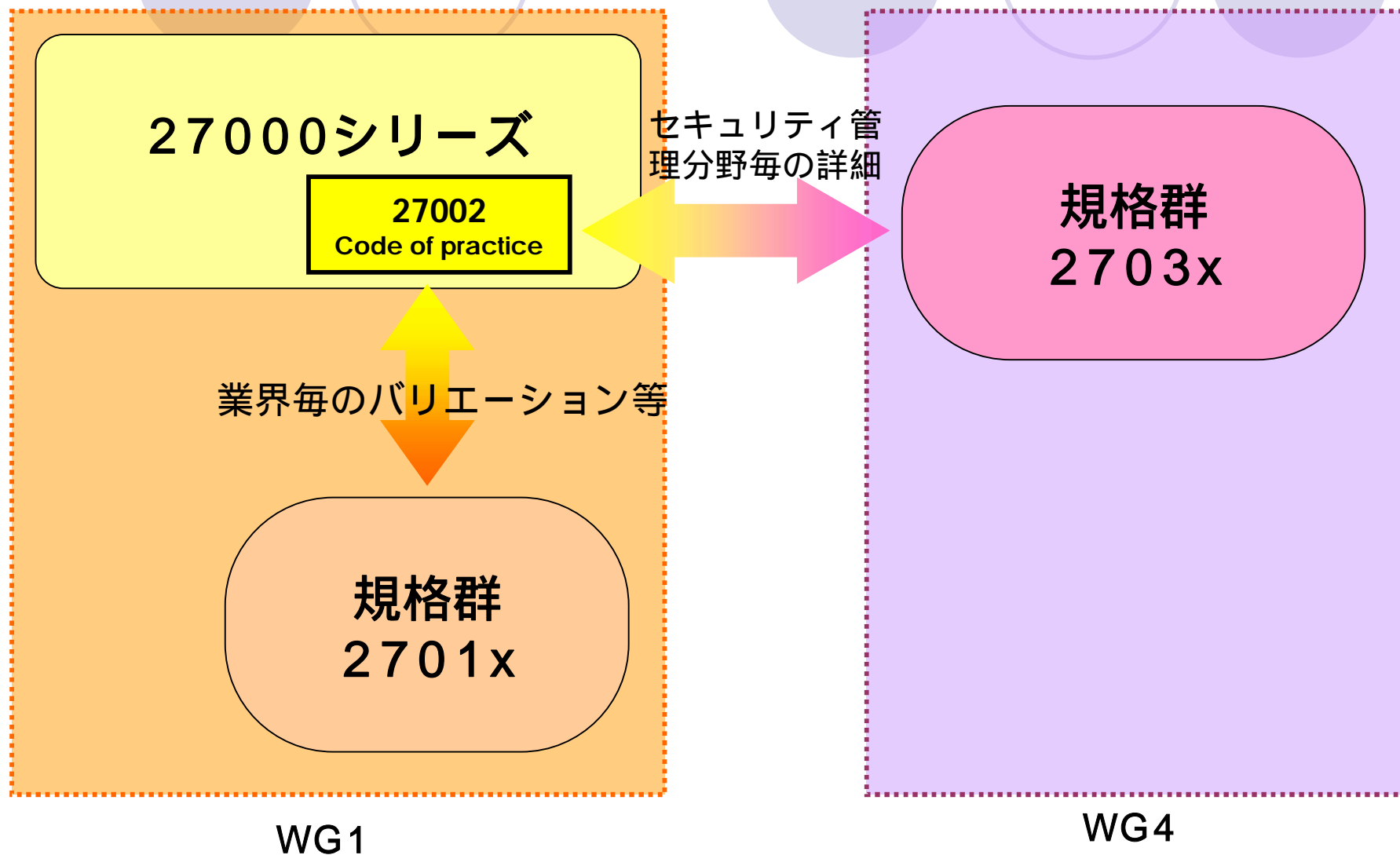


ISOの組織 SC27

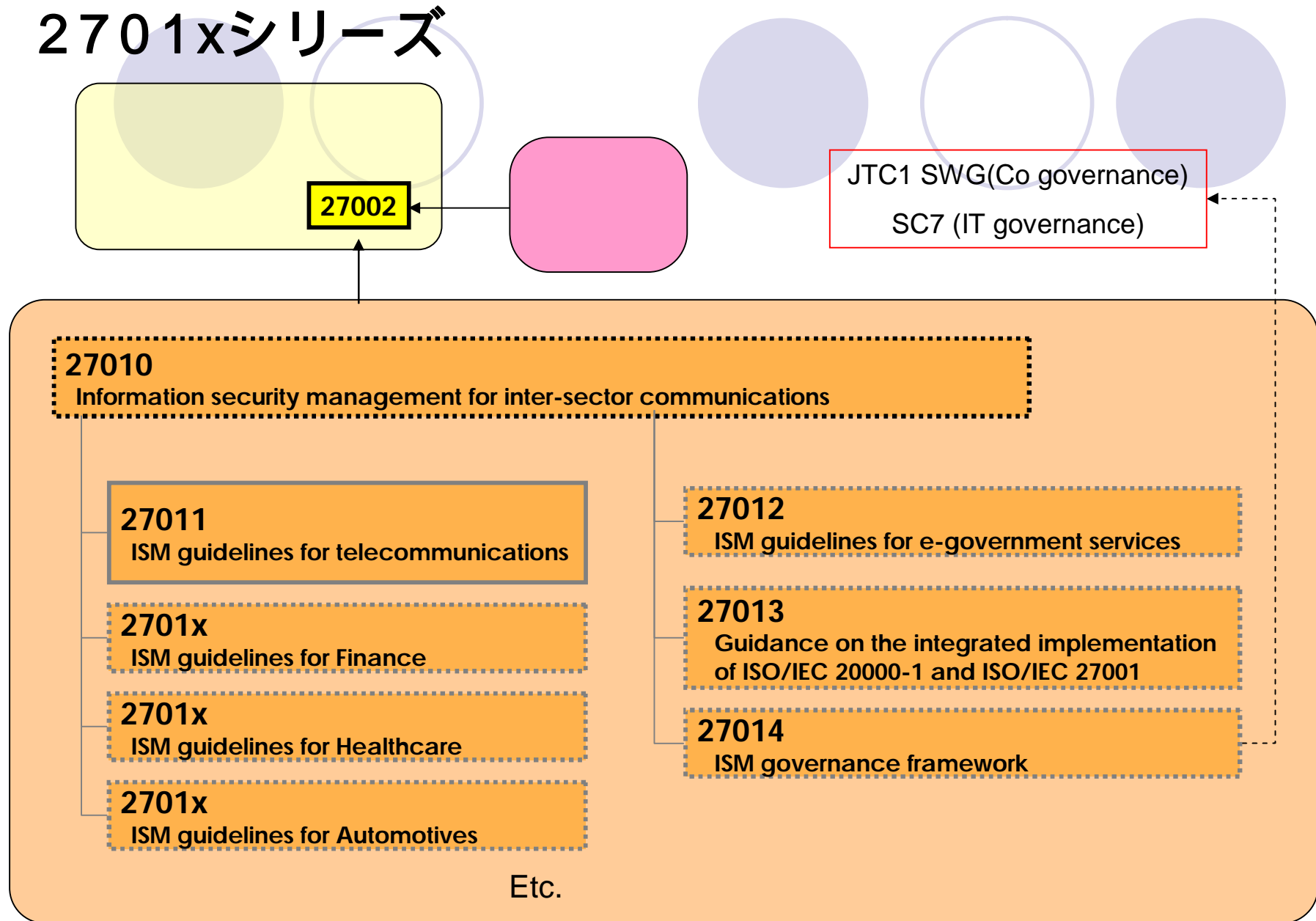
役割：情報セキュリティ技術の国際標準化を担当



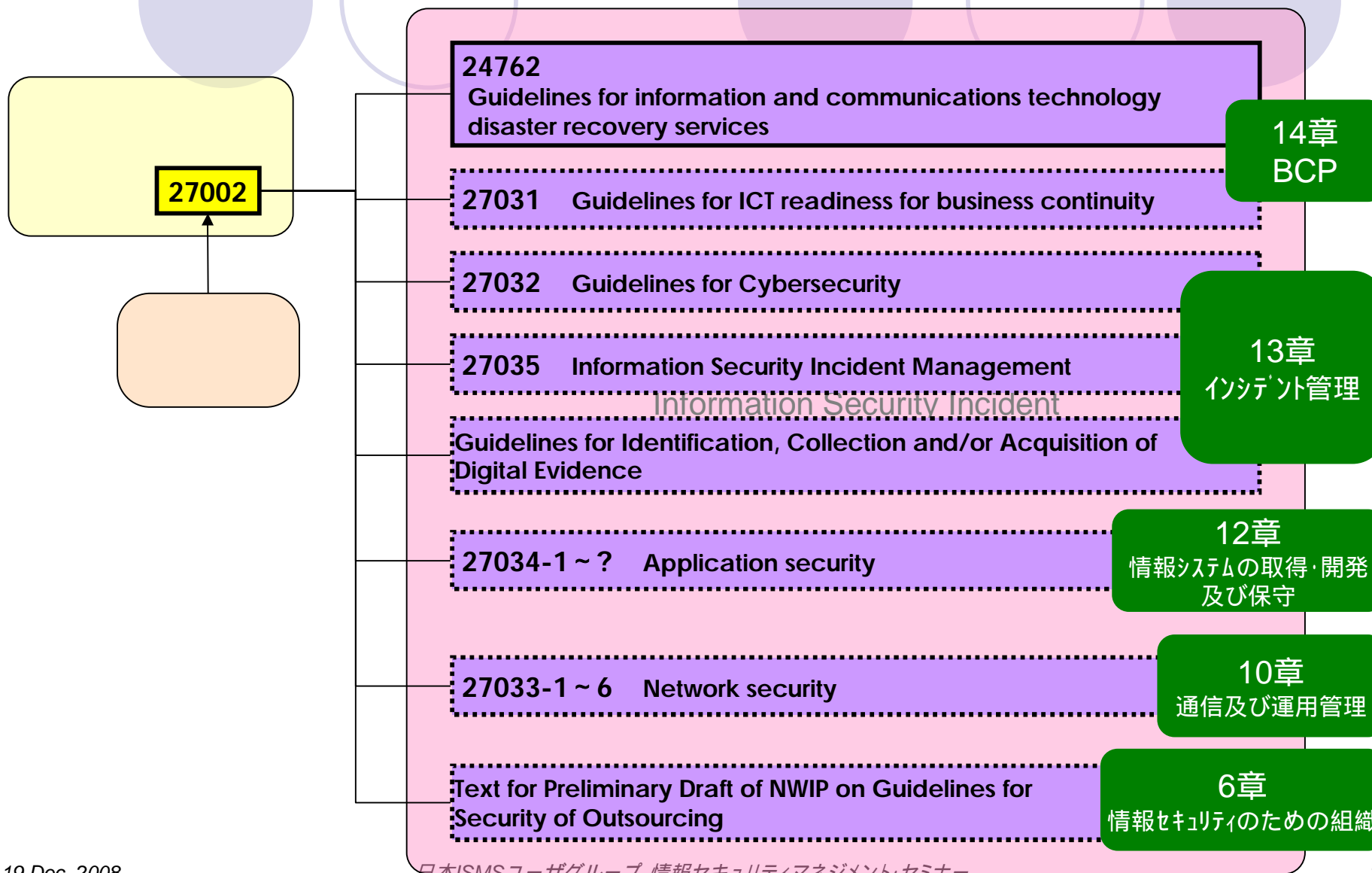
ISMS関連規格 全体像



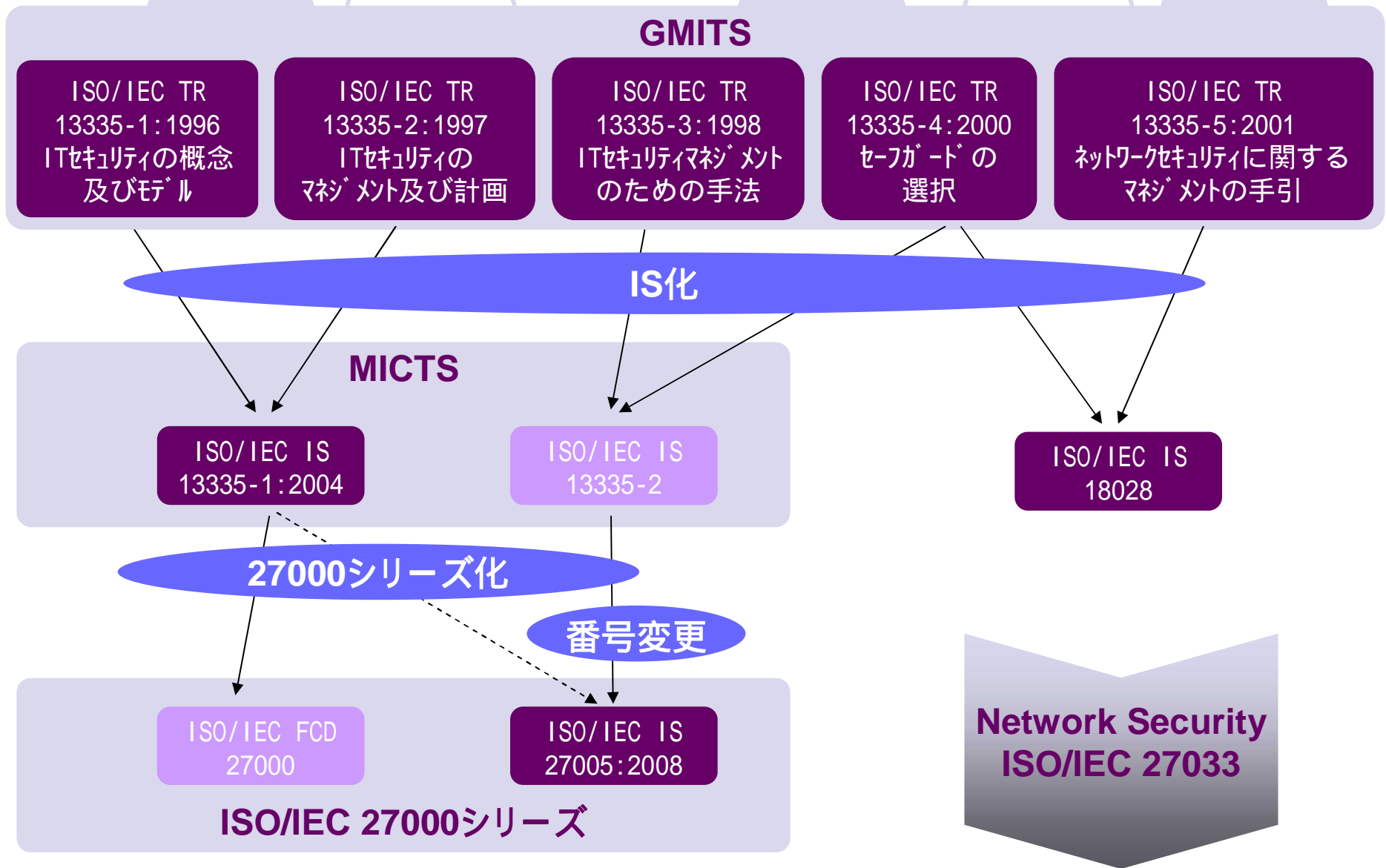
2701xシリーズ



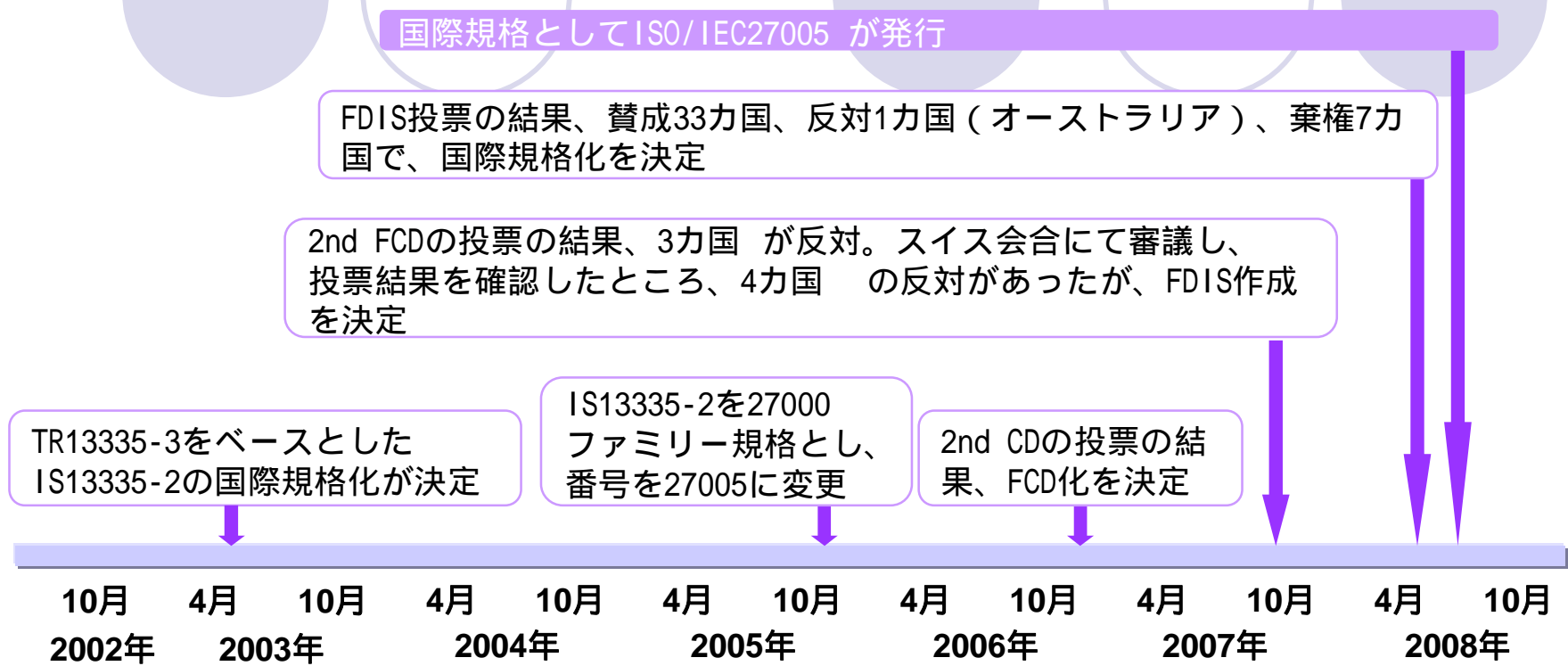
2703xシリーズ



規格内容の変遷



規格化の経緯



反対国

- FCD投票での反対国 : オーストラリア、ノルウェー、スイス、UK、日本
- 2nd FCD投票での反対国 : オーストラリア、オーストリア、日本
- スイス会合審議後の反対国 : オーストラリア、オーストリア、スペイン、ニュージーランド

規格の特徴

- 27000ファミリー規格としての位置づけを明確化
 - ISO/IEC 27001の要求事項へのポイントを追加

7.1

NOTE ISO/IEC 27001 does not use the term “context”. However, all of Clause 7 relates to the requirements “define the scope and boundaries of the ISMS” [4.2.1 a)], “define an ISMS policy” [4.2.1 b)] and “define the risk assessment approach” [4.2.1 c)], specified in ISO/IEC 27001.

- ISO/IEC 27001の要求事項実現のためのガイド情報を追記

8章、9章

NOTE ISO/IEC 27001 does not use the term “context”. However, all of Clause 7 relates to the requirements “define the scope and boundaries of the ISMS” [4.2.1 a)], “define an ISMS policy” [4.2.1 b)] and “define the risk assessment approach” [4.2.1 c)], specified in ISO/IEC 27001.

- 本文はシンプルに、Annexに詳細を
- 他の規格との重複の排除
 - 管理策の実装、リスク対応計画（詳細）策定等は記述の対象外

Vs. Guide73

- “process” と “activity”

- 考え方を整理

- 情報セキュリティリスクマネジメント全体を”process”
- プロセスを構成する要素を “activity”

- Guide73で定義している用語中に “ process”という用語があるものは、注記を追加

risk estimation(3.5), risk identification(3.6)

- “probability” と “likelihood”

- 情報セキュリティリスクでの “発生確率”（数値化）

- Guide73で定義している用語中に “ probability”という用語があるものは、注記を追加

risk estimation(3.5), risk reduction(3.7)

- 27005では、negative riskのみ考慮することをNote
risk retention(3.8), risk transfer(3.9)

規格の構成

タイトル			Annexとの対応
1.	Scope		
2.	Normative references		
3.	Terms and definitions		
4.	Structure of this International Standard		
5.	Background		
6.	Overview of the information security risk management process	リスクマネジメントプロセスの概要説明	
7.	Context establishment	各リスクマネジメントプロセスの説明	AnnexA
8.	Information security risk assessment		Annex B Annex C Annex D Annex E
9.	Information security risk treatment		AnnexF
10.	Information security risk acceptance		
11.	Information security risk communication		
12.	Information security risk monitoring and review		

リスクマネジメントプロセス 用語

リスクマネジメント (Risk Management)

リスクアセスメント (Risk Assessment)
リスク分析からリスク評価までのすべてのプロセス

リスク分析 (Risk Analysis)
リスクの規模の算定

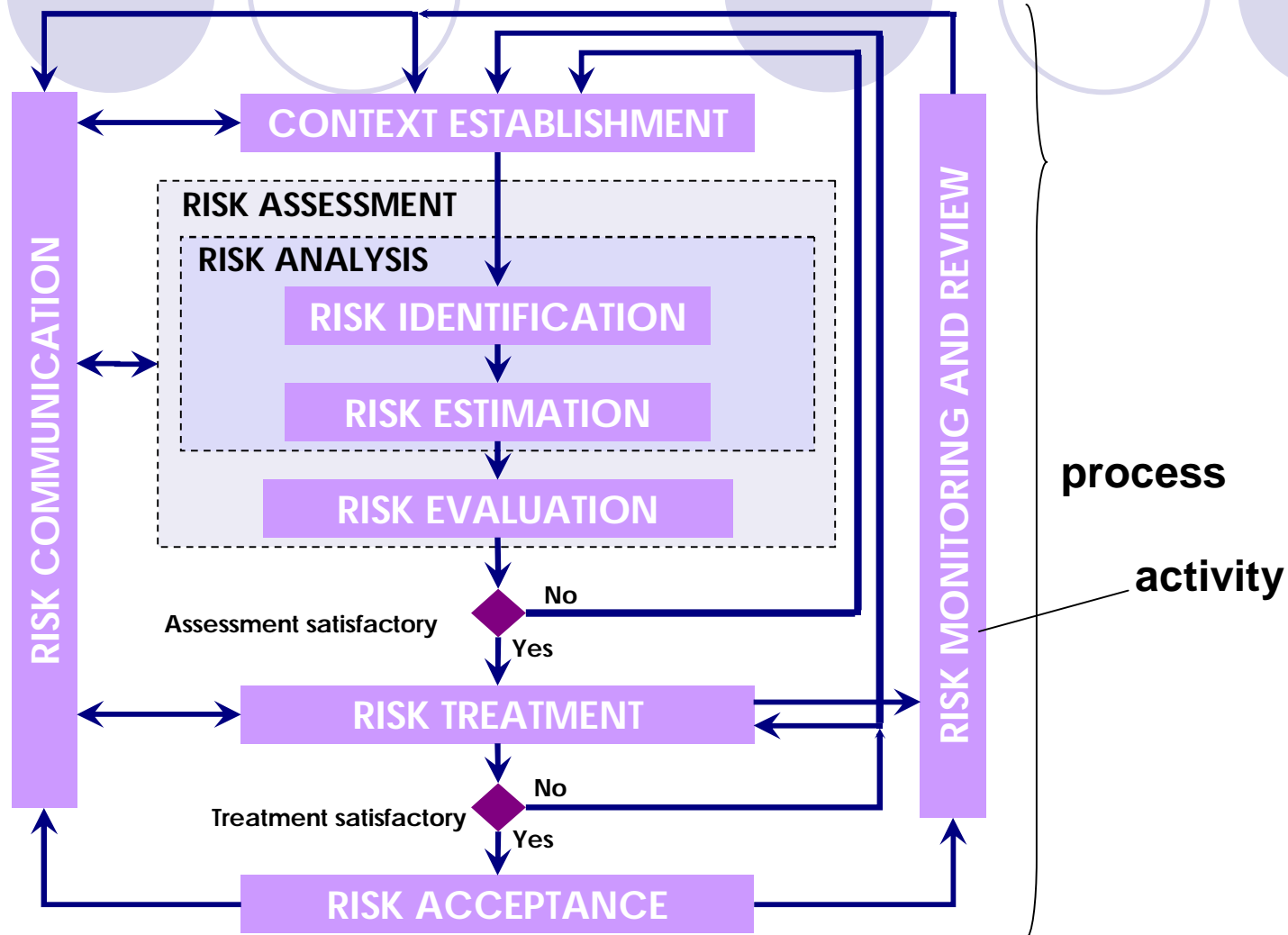
リスク評価 (Risk Evaluation)
リスクの重大さを決定するとともに、算定されたリスクとリスク基準との比較

リスク対応 (Risk Treatment)
リスクを変更させるための方策の選択及び実施

リスク受容 (Risk Acceptance)
リスクを受容する意思決定

リスクコミュニケーション (Risk Communication)
意思決定者と他のステークホルダーの間における、リスクに関する情報の交換、又は共存

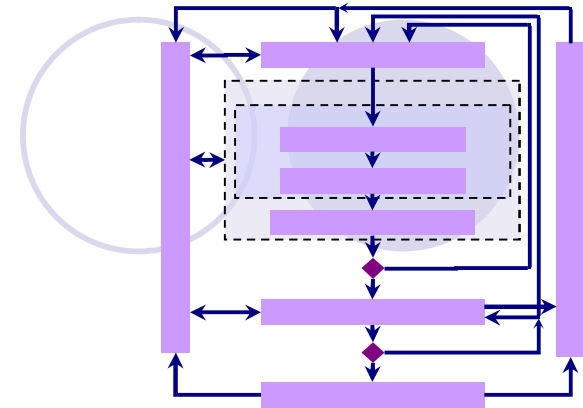
リスクマネジメントプロセス



Context Establishment(1)

- Basic Criteria

リスクマネジメントに必要な各種基準 (CRITERIA)を決める



Risk evaluation criteria

- ✓ **The strategic value** of the business information process
- ✓ The **criticality** of the information assets involved
- ✓ **Legal and regulatory requirements**, and **contractual obligations**
- ✓ **Operational and business importance** of availability, confidentiality and integrity
- ✓ **Stakeholders** expectations and perceptions, and negative consequences for goodwill and reputation

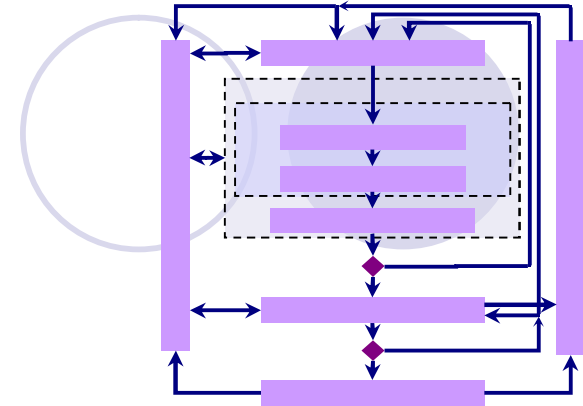
ISO/IEC27001 4.2.1 b) 4)

Define an ISMS policy in terms of the characteristics of the business, the organization, its location, assets and technology that establishes criteria against which risk will be evaluated

Context Establishment(2)

Impact criteria

- ✓ **Level of classification** of the impacted information asset
- ✓ **Breaches of information security**
(e.g. loss of confidentiality, integrity and availability)
- ✓ **Impaired operations** (internal or third parties)
- ✓ **Loss of business and financial value**
- ✓ **Disruption** of plans and deadlines
- ✓ **Damage of reputation**
- ✓ **Breaches** of legal, regulatory or contractual requirements



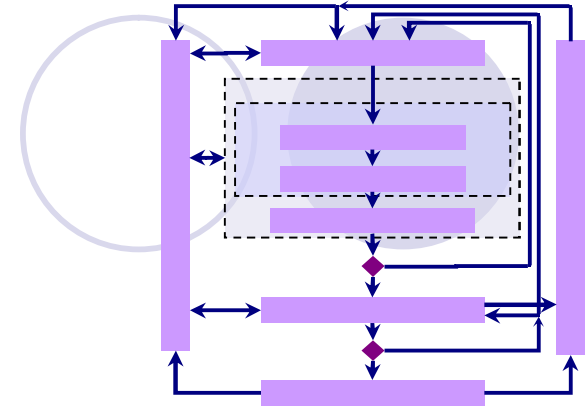
ISO/IEC27001 4.2.1 d) 4)

Identify the impacts that losses of confidentiality, integrity and availability may have on the assets.

Context Establishment(3)

Risk acceptance criteria

- ✓ Business criteria
- ✓ Legal and regulatory aspects
- ✓ Operations
- ✓ Technology
- ✓ Finance
- ✓ Social and humanitarian factors



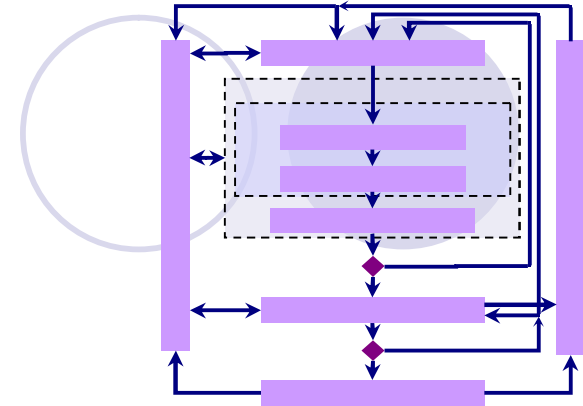
ISO/IEC27001 4.2.1 c) 2)

Develop criteria for accepting risks and identify the acceptable levels of risk.

- *Multiple thresholds*
- *Expressed as the ratio of estimated profit*
- *Depends on the classes of risks*
- *Needs future additional treatment).*

Context Establishment(4)

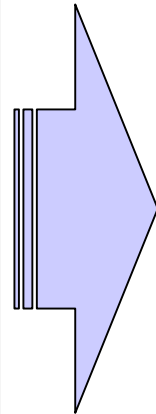
- The scope and boundaries
リスクマネジメントの適用範囲と境界



ISO/IEC27001 4.2.1 a)

The organization shall do the following.

- a) Define the scope and boundaries of the ISMS in terms of the characteristics of the **business, the organization, its location, assets and technology**, and including details of and justification for any exclusions from the scope (see 1.2).



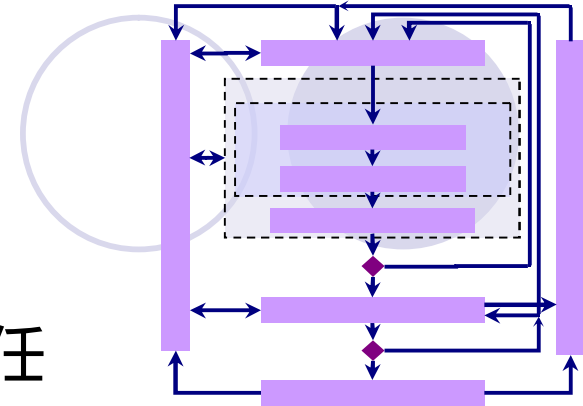
ISO/IEC27005

- The organization's **strategic business objectives, strategies and policies**
- **Business processes**
- The organization's **functions and structure**
- **Legal, regulatory and contractual requirements** applicable to the organization
- The organization's **information security policy**
- The organization's **overall approach to risk management**
- **Information assets**
- **Locations** of the organization and their **geographical characteristics**
- **Constraints** affecting the organization
- **Expectation of stakeholders**
- **Socio-cultural environment**
- **Interfaces** (i.e. information exchange with the environment)

Context Establishment(5)

● Organization for information security risk management

リスクマネジメントのための組織と責任



ISO/IEC27001 5.2.1 a)

The organization shall determine and provide the resources needed to:

- a) establish, implement, operate, monitor, review, maintain and improve an ISMS;

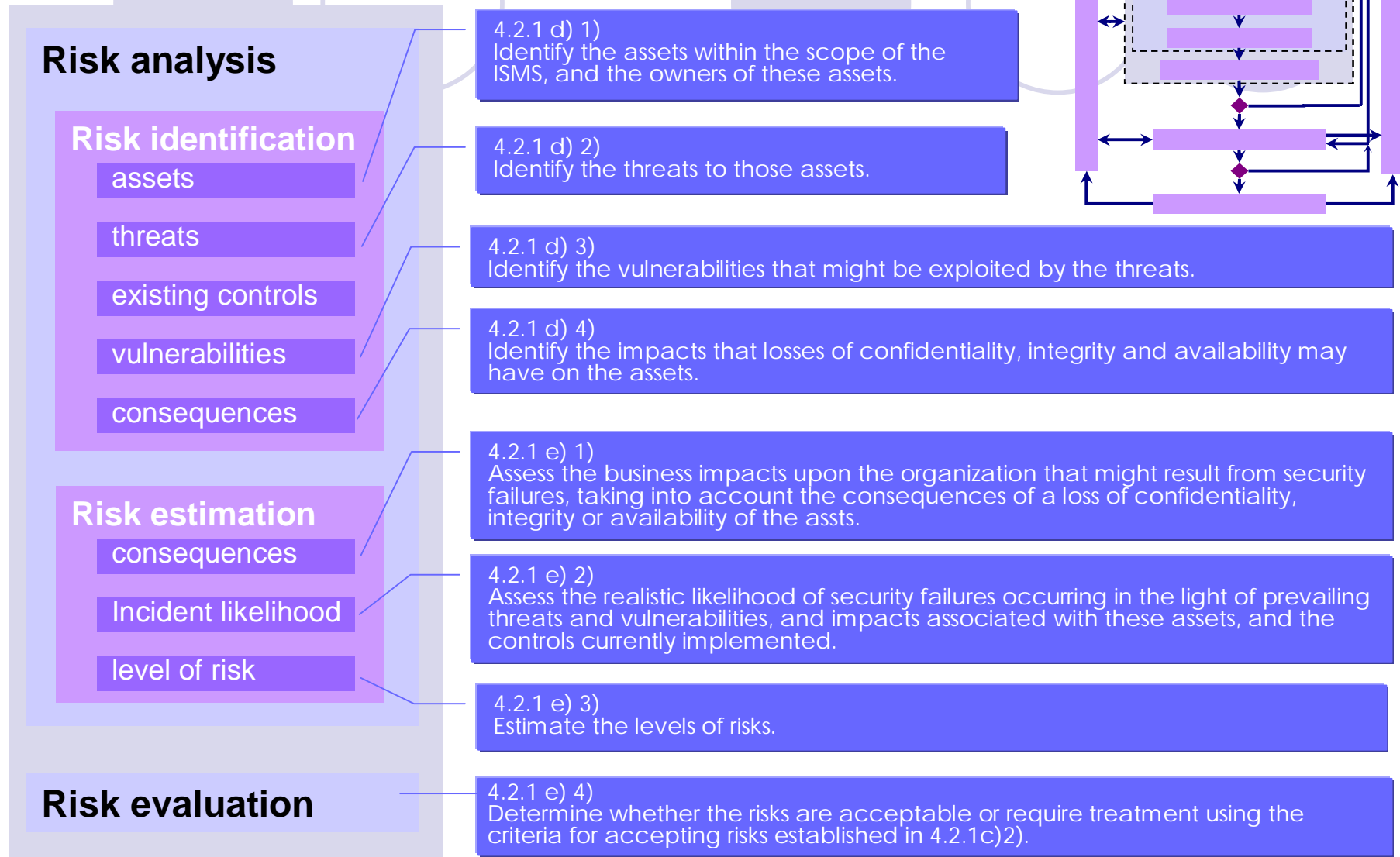
ISO/IEC27005 RESOURCES

- **Perform risk assessment** and establish a risk treatment plan
- Define and implement **policies and procedures**, including implementation of the controls selected
- **Monitor controls**
- **Monitor** the information security risk management **process**

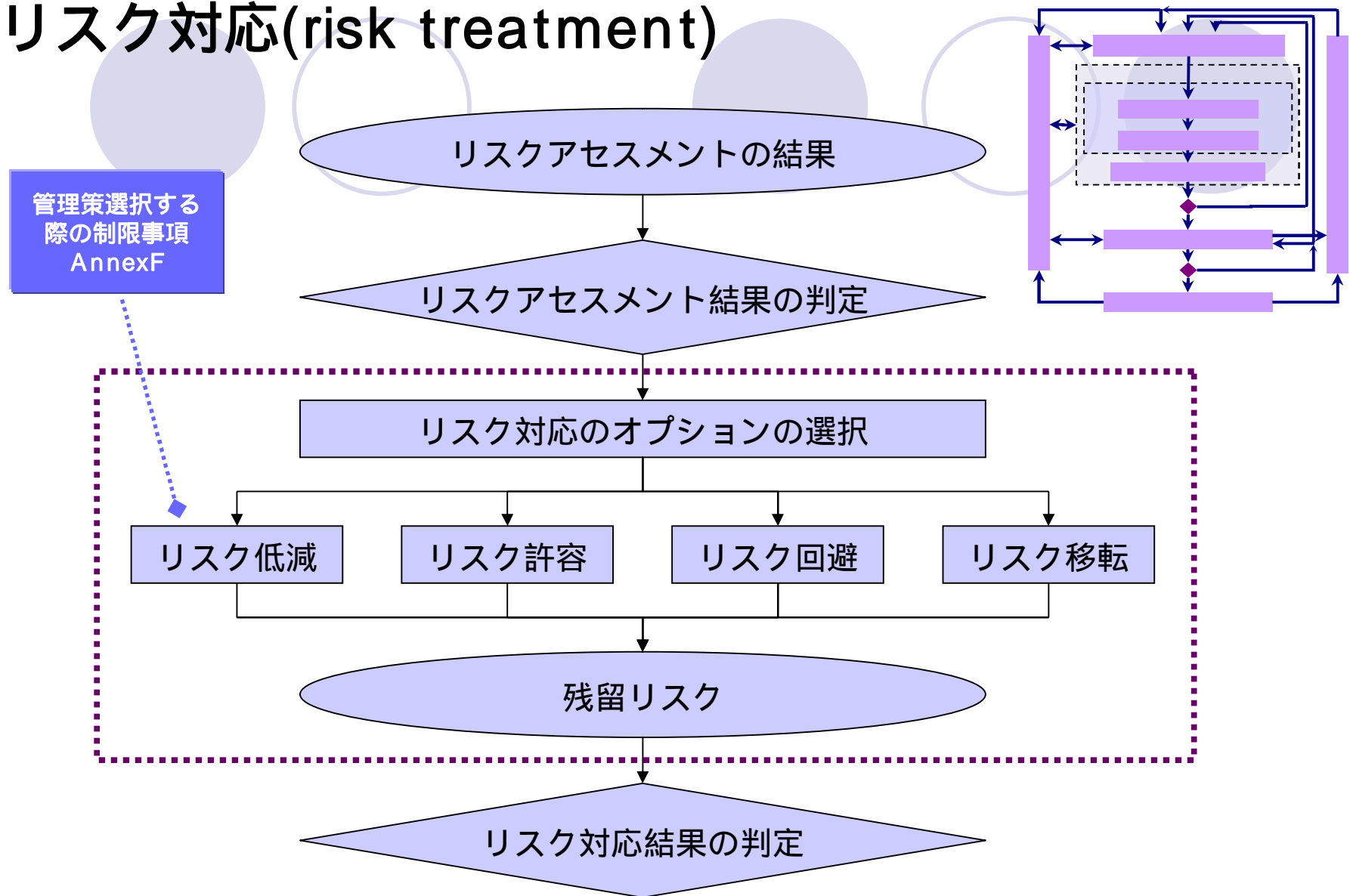
roles and responsibilities of this organization

- **Development of the information security risk management process** suitable for the organization
- Identification and analysis of the **stakeholders**
- Definition of **roles and responsibilities of all parties** both internal and external to the organization
- Establishment of the **required relationships** between the organization and stakeholders
- **interfaces to the organization's high level risk management functions**
- **interfaces to other relevant projects or activities**
- Definition of **decision escalation paths**
- Specification of **records** to be kept

Risk assessment

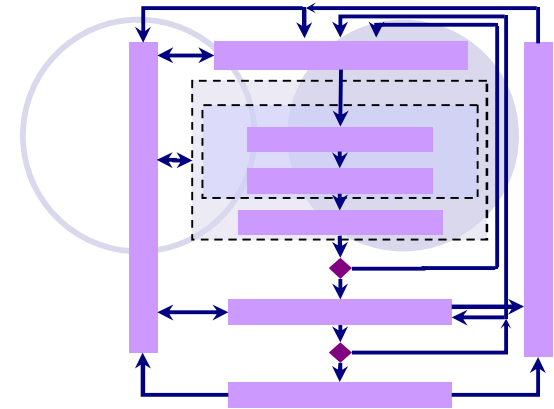


リスク対応(risk treatment)



リスクコミュニケーション

- リスクに関する情報を共有
 - 意思決定者 (decision-maker) - 利害関係者 (stakeholders)
- リスクコミュニケーションプランを策定
 - 通常運用時
 - 緊急時
- 目的
 - リスクに関する情報の収集
 - リスクアセスメント結果及びリスク対応計画の共有

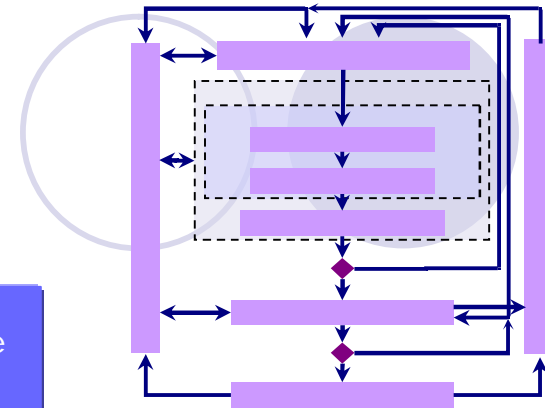


リスクの監視及びレビュー

- Monitoring and review of risk factors
 - リスクの要因についての監視及びレビュー

4.2.3 d)
Review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks, taking into account changes to:

- 1) the organization;
- 2) technology;
- 3) business objectives and processes;
- 4) identified threats;
- 5) effectiveness of the implemented controls; and
- 6) external events,...



- Risk management monitoring, reviewing and improving
 - リスクマネジメントプロセスそのものの監視、レビュー及び改善

7.2 Review input
The input to a management review shall include:

- e) vulnerabilities or threats not adequately addressed in the previous risk assessment;
... etc.

7.3 Review output
The output from the management review shall include any decisions and actions related to the following.

- c) Modification of procedures and controls that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to;
- 6) levels of risk and/or criteria for accepting risks.

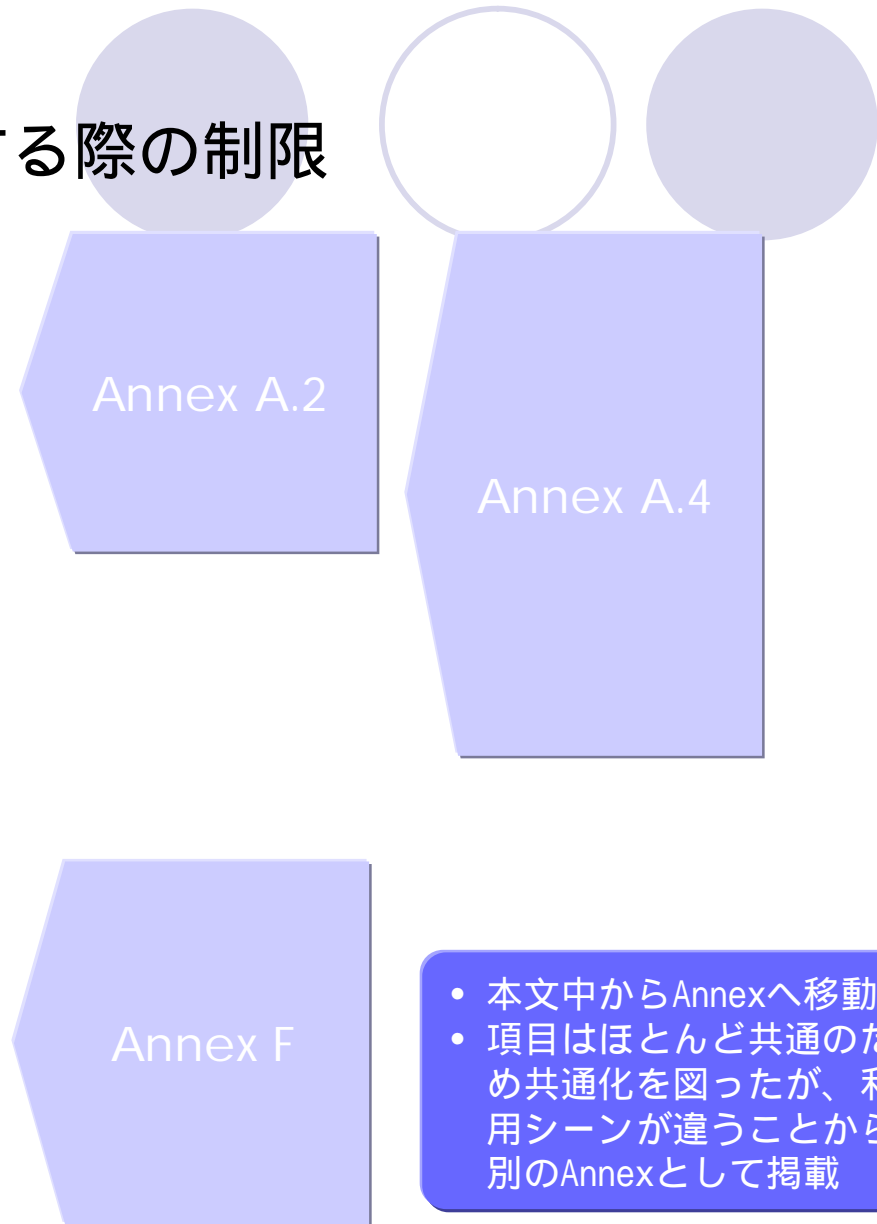
Constraints

- 適用範囲及び境界を決定する際の制限

- Organizational
 - Political nature
 - Strategic nature
 - Concerning personnel
 - Budgetary , etc.
- Technical
- Financial
- Time, etc.

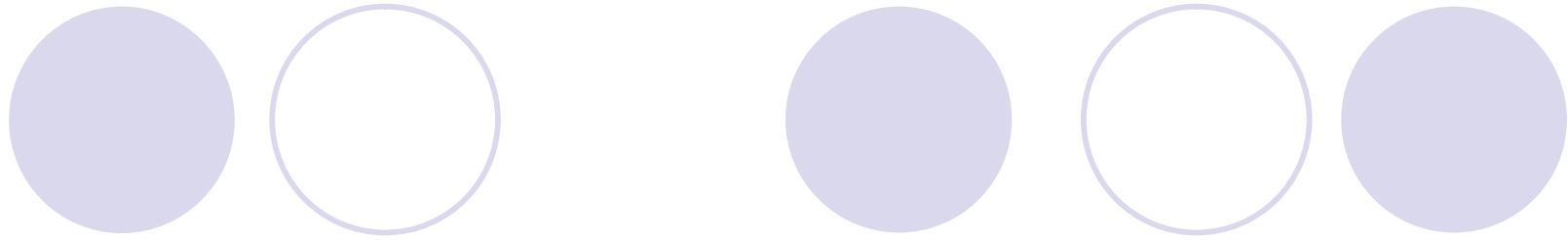
- 管理策選択の際の制限

- Time
- Financial
- Technical
- Cultural, etc.



今後の予定（私見）

- ISO31000、Guide73との整合性
 - ISO31000：DISステージ
 - Guide73：2nd CDステージ
 - 用語定義の違いの吸収
 - risk reduction, risk transfer等の用語は未掲
(risk mitigation, risk sharing)
 - Risk management plan vs. risk treatment plan
- 27000シリーズとの整合性
 - 27003との記述範囲の調整
 - 27001、27002の見直しの動き



ご静聴ありがとうございました

三菱電機株式会社 情報技術総合研究所
主席研究員
中野 初美

Tel: 0467-41-2326

FAX: 0467-41-2312

E-Mail: Nakano.Hasumi@dr.MitsubishiElectric.co.jp

Web: <http://www.MitsubishiElectric.co.jp>