資料２

NTTコミュニケーションズにおけるセキュリティマネジメント体制とセキュリティ人材育成のあり方

2003年1 月24日
NTTコミュニケーションズ
取締役　先端IPアーキテクチャセンタ所長
セキュリティマネジメント室長
飯塚　久夫

1. 情報セキュリティマネジメント実現のための取り組み

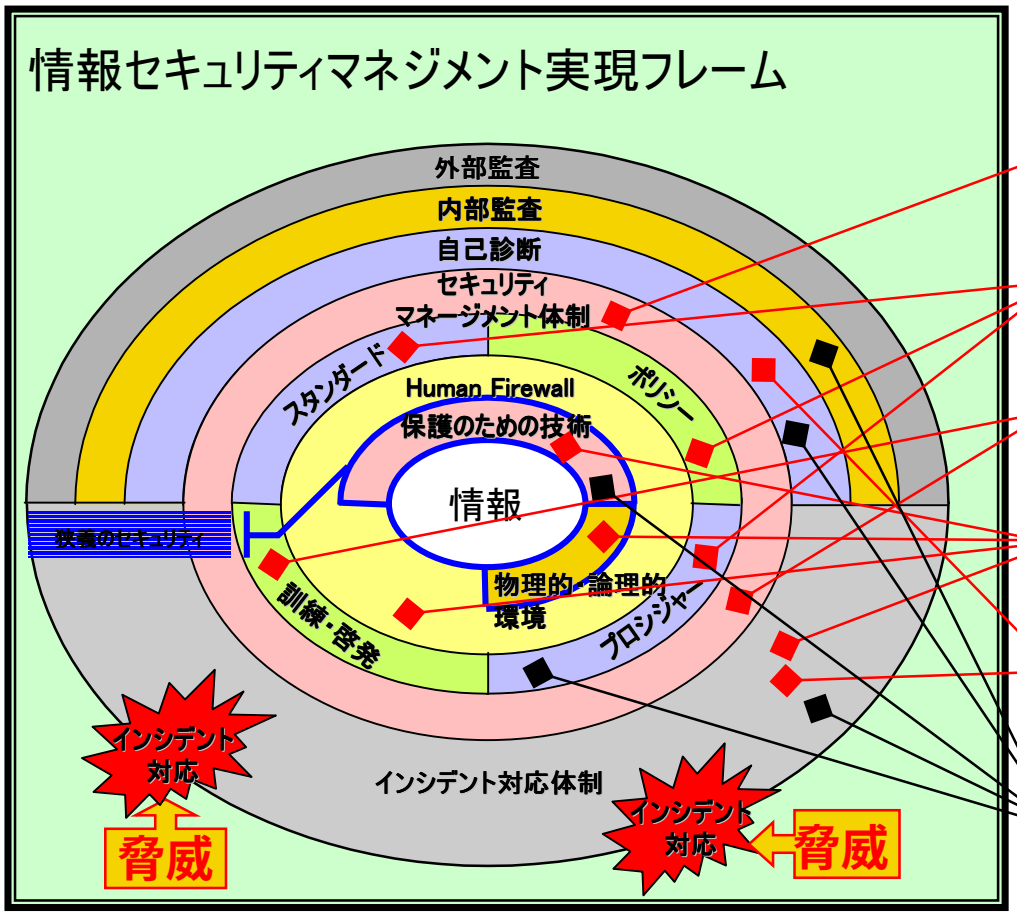
（1）NTTコミュニケーションズの情報セキュリティの平均レベルの底上げ

情報セキュリティマネジメントのグローバルスタンダードである(ISO17799)の要求水準からみて見劣りしないレベル

（2）ビジネス要件からISMS*認証を取得する組織の取得支援

（3）高度スキルをもつセキュリティエンジニアの実践を通じた育成

*ISMS：Information Security Management System



実施プログラム

① CSO/SM室の役割定義および全社セキュリティ体制の設計

② 全社セキュリティ宣言書、ポリシー等の策定

③ セキュリティマネジメント実施担当者等へのセキュリティマネジメント専門知識の集中教育

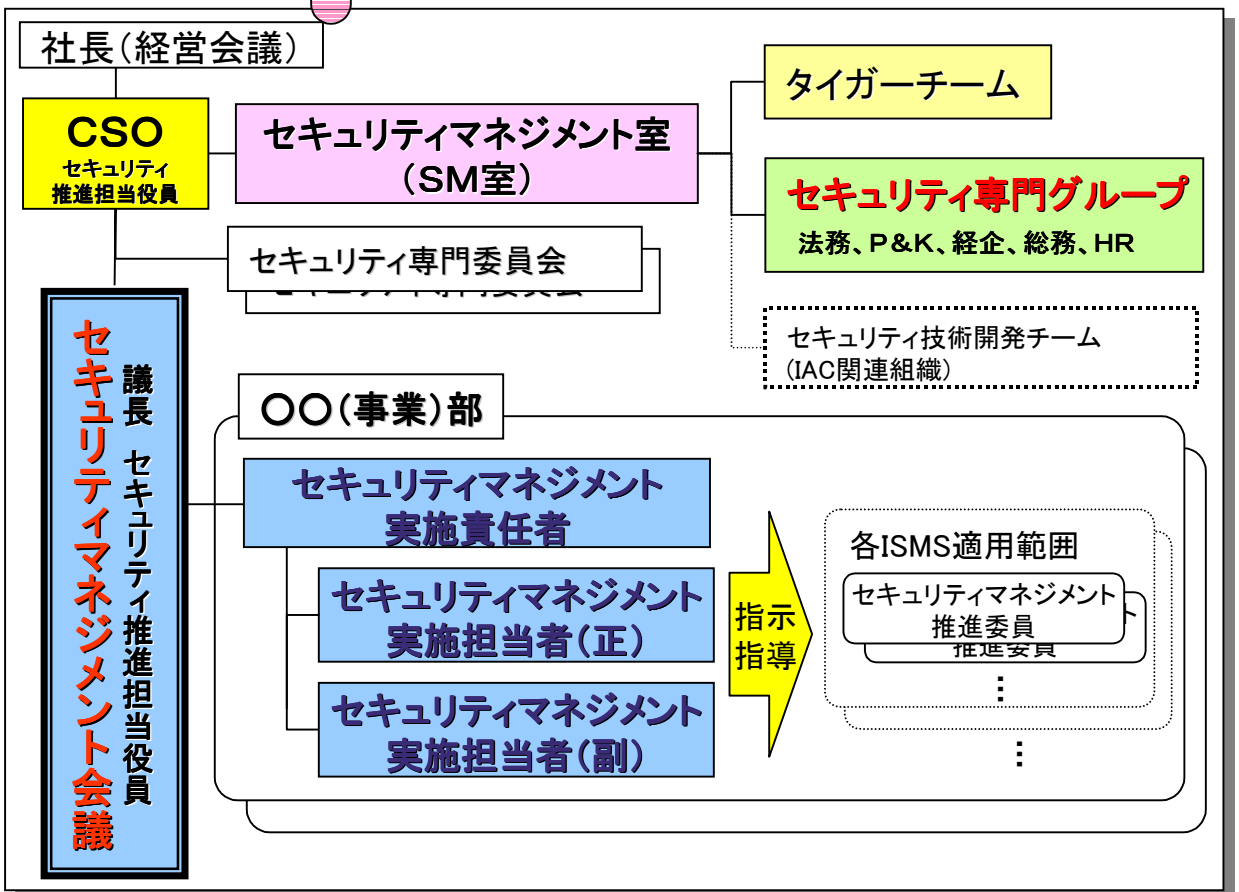
④ セキュリティ対策実施状況に関する現状の把握（ISO17799の要求事項と現状とのギャップ分析）

⑤ セキュリティインシデント対応用情報共有環境の整備

セキュリティに関する社内関連部門と連携して推進する分野

2. NTTコミュニケーションズの情報セキュリティマネジメント推進体制

CSO/SM室のミッションコンセプト
CSO（Chief Security Officer）とSM室（Security Management Office）の最大のミッションはCSO、SM室をいらなくすることである。
すなわち、全組織、全員が自らセキュリティマネジメントを実施できるような状態にすることである。



ミッションをポリシーに記載して責任体制を明確化

CSO
セキュリティ・レベルの向上に対して責任を持ち、セキュリティマネジメントの定着に向けての指揮を担う。また、セキュリティの全社的有事において対応体制の整備に対する指揮を取ることで対応現場を補完する責任を担う。

SM室
SM室はCSOを補佐し、セキュリティ・レベルの向上、セキュリティマネジメントの定着のための方針、施策、管理策を開発、展開、その順守状況を監査する役割を担う。

セキュリティマネジメント会議
CSOのミッションを具現化し、全社、各組織に展開する上での施策決定機関としての役割を担う。

セキュリティマネジメント実施責任者
各組織の代表者として、セキュリティマネジメント会議へ参画する。CSO/SM室と連携して自組織内のセキュリティ・レベルの向上、セキュリティマネジメントの定着の責任を担う。

セキュリティマネジメント実施担当者
各組織において「セキュリティマネジメント実施責任者」を補佐し、自組織内における各種セキュリティ施策の実質的推進者としての役割を担う。

セキュリティ専門グループ
SM室の指示に基づいて、専門性に応じたセキュリティ関連事項に対する作業の実施する役割を担う。（全社セキュリティポリシー策定等）

タイガーチーム
セキュリティの技術的専門性を有し、脆弱性の発見とセキュリティ問題の解決に対してSM室の指示に基づき実施する役割を担う。

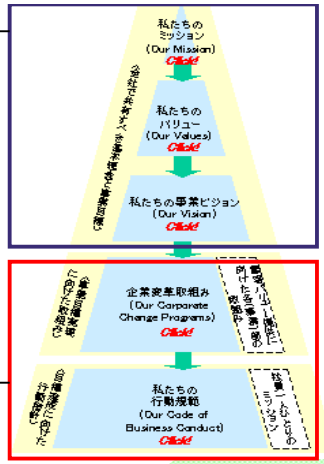
3. セキュリティポリシー体系について

経営理念

OBP

Mission　Vision　Value

Our Business Principle



コーポレートガバナンス

セキュリティ侵犯（情報漏えい　等）

過剰投資　IT競争

人材の流動化　顧客満足の多様化

法的対応　サービス品質

コーポレート
セキュリティ宣言書

品質管理

コーポレート
セキュリティポリシー

コーポレート
セキュリティガイドライン

＜これまでのセキュリティの考え方＞

- ローカルポリシー
- 電気通信事業法をベースとしたテレコム・セキュリティ

＜これからのセキュリティの考え方＞

- コーポレートポリシー
- IP(情報)セキュリティ

情報資産 / セキュリティ要件	情報				設備機器		
	通信の秘密	外延情報	財産情報	その他の情報	交換機	社屋	コンピュータ
機密性	お客様情報の保護に関する規程		財産的情報の守秘管理規程			社屋管理規程	セキュリティ指針
完全性							
可用性					設備管理規程	社屋管理規程	

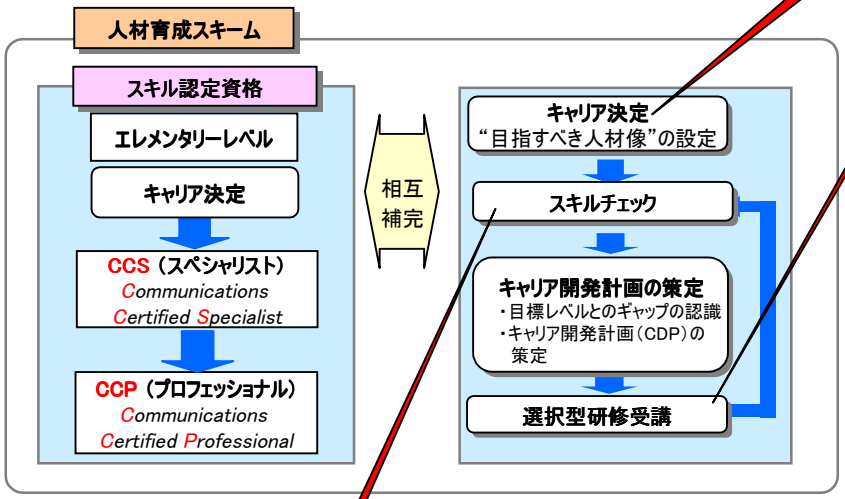
包括的 → 体系的

情報資産 / セキュリティ要件	情報	情報ネットワークシステム
機密性	全体をカバーする新しい情報資産分類の考え方	
完全性		
可用性		

4. 情報セキュリティ人材育成のあり方

1. 全社人材育成スキームに基づく情報セキュリティエンジニア育成

情報セキュリティエンジニアに関する「目指すべき人物像」の設定



スキルチェック対象項目

コアスキル	専門スキル発揮のベースとなり、全社員共通に求められるヒューマンスキル （9項目）		
Product & Service ナレッジ	各キャリアで必要とするビジネスと業務遂行に直結したテクニカルスキル（10～15項目選択）	ビジネススキル	ﾏｰｹﾃｨﾝｸﾞ、調査・統計 等
		SI	ﾌﾟﾛｼﾞｪｸﾄﾏﾈｼﾞﾒﾝﾄ 等
		IPコア技術	LAN技術、WAN技術 等
		IP応用技術	DB構築・管理、ﾐﾄﾞﾙｳｪｱ 等
		NW技術	伝送技術、交換技術 等
		スタッフ機能別	経営企画、財務、人事 等
社外資格	各キャリアで必要とする資格	・マイクロソフト認定資格 ・シスコ認定資格 ・テクニカルエンジニア試験 等	

各項目毎にレベル設定

選択型研修コースにおける情報セキュリティ関連コースの充実

	レベル2	レベル3	レベル4
IPコア技術	◆◆◆◆	◆◆	◆◆◆◆
IP応用技術	-	◆	-
システムインテグレーション	-	◆	-
社外資格（情報セキュリティアドミニストレータ）	-	◆◆	-
情報セキュリティマネジメント	◆◆	◆◆	◆◆

（◆：既存コース，◆：新設コース）

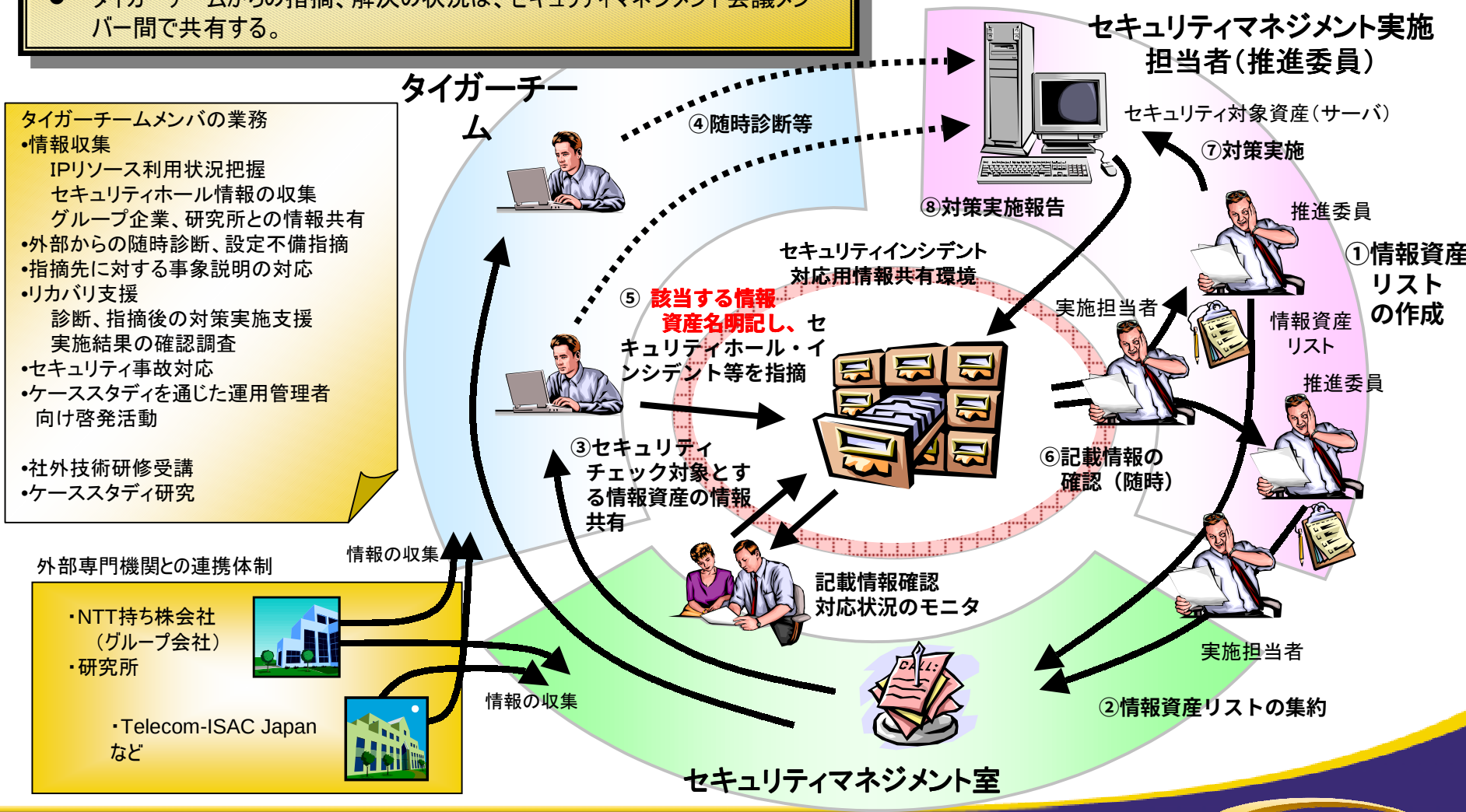
2. 高度スキルを持つセキュリティエンジニアの育成

■高度な最先端のセキュリティ技術を有し、トータルな観点から施策を 実施・管理できる人材 [レベル5相当] の育成

■タイガーチーム（後述）メンバーとしてのOJTを通じたスキルアップ

5. セキュリティインシデント対応用情報共有環境のイメージ

- タイガーチームはセキュリティの高度な技術的専門性を有し、脆弱性の発見とセキュリティ問題の解決に対してSM室の指示に基づき実施する役割を担う。
- セキュリティマネジメント実施担当者は、タイガーチームからうけたセキュリティ上の問題点指摘に対処する。
- タイガーチームからの指摘、解決の状況は、セキュリティマネジメント会議メンバー間で共有する。



6.Telecom-ISAC Japan*の紹介 *Telecom Information Sharing and Analysis Center Japan

- インシデント情報共有・分析センター（Telecom-ISAC JAPAN)の設立(2002.7.15)
- 設立目的（インシデント情報共有・分析センター規約より）
  - センタは、情報セキュリティの確保を図る上で情報通信事業者による取り組みが極めて重要であることを鑑み、わが国の情報通信業界における情報セキュリティ対策の充実を図るため、情報通信事業者を中心として会員を募り、インシデント情報を収集・分析し会員に提供するとともに、会員の情報セキュリティ対策に資するその他の事業を行うことにより、わが国の情報セキュリティの向上を促し、もって、わが国における高度情報通信ネットワーク社会の形成に寄与することを目的とする。
- 重要インフラ部門における官民連携のあり方のひとつ

Telecom-ISAC Japanの活動概要イメージ