生産制御システムにおける セキュリティ調査研究の紹介

―SICE/JEITA/JEMIMA共同セキュリティWG活動より―

制御システムセキュリティカンファレンス 2009
2009. 2. 19

（社）計測自動制御学会 産業応用部門　計測・制御ネットワーク部会
（株）日立製作所
山田 勉

目次

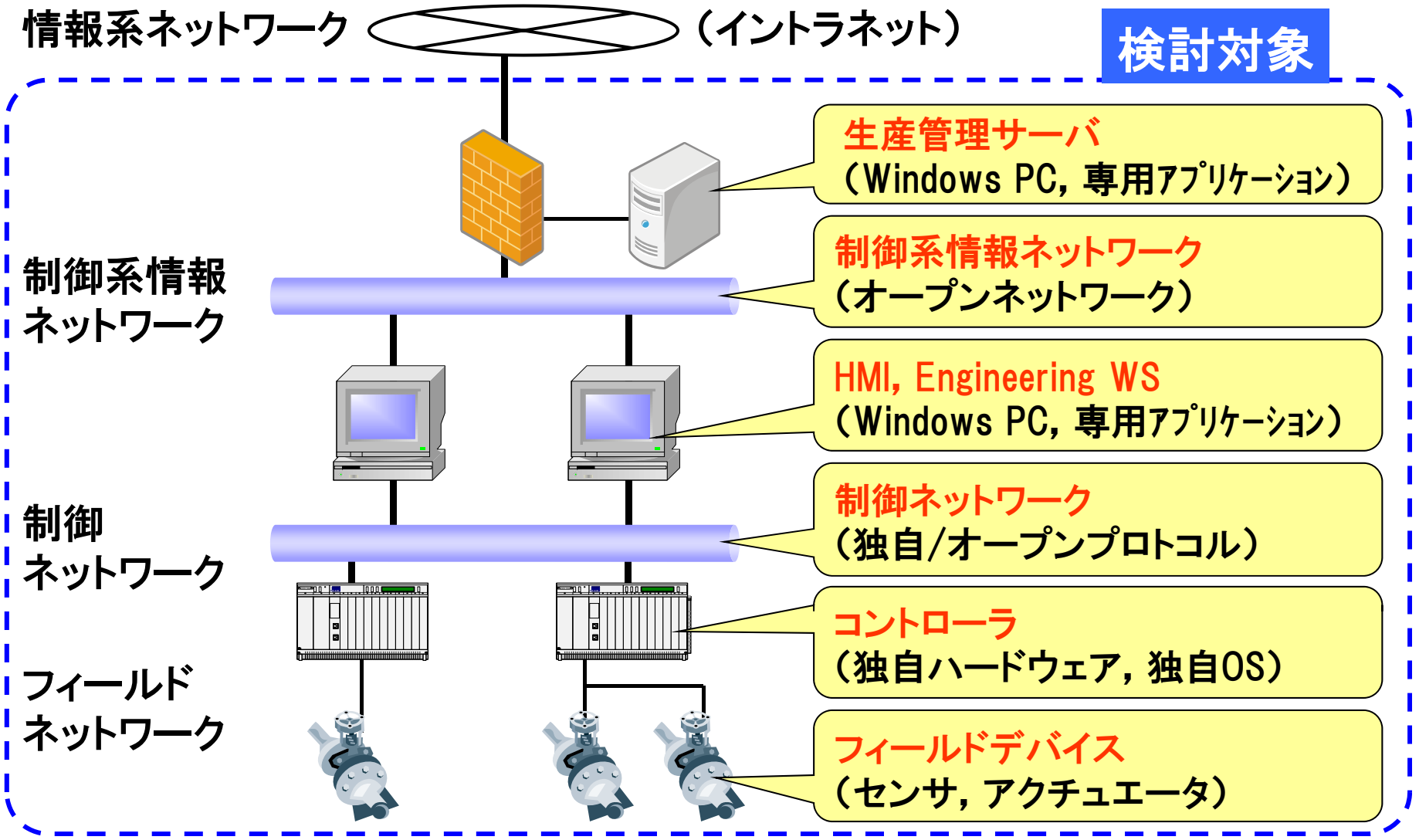
1-1. SICE/JEITA/JEMIMA共同セキュリティWG

- 目的
  - 製造業分野におけるセキュリティ標準化動向，技術等の調査・研究活動を進め，会員企業，ユーザにフィードバックする(JEMIMA)
- メンバ

  横河電機㈱，㈱山武，㈱東芝，富士電機ｼｽﾃﾑｽﾞ㈱
  ㈱日立ﾊｲﾃｸｺﾝﾄﾛｰﾙｼｽﾃﾑｽﾞ，㈱日立製作所
- 広報活動
  - JEMIMA 委員会セミナー，計測展
  - JEITA 制御システムフォーラム
  - SICE Annual Conference
- 団体協力関係
  - JPCERT/CC，IPAと相互に情報交換
  - IEC/TC65/WG10国内委員会にメンバ登録(JEMIMA)

SICE：(社)計測自動制御学会，JEITA：(社)電子情報技術産業協会，JEMIMA：(社)日本電気計測器工業会

1-2. セキュリティ検討対象：生産制御システム



1-3. セキュリティへの脅威

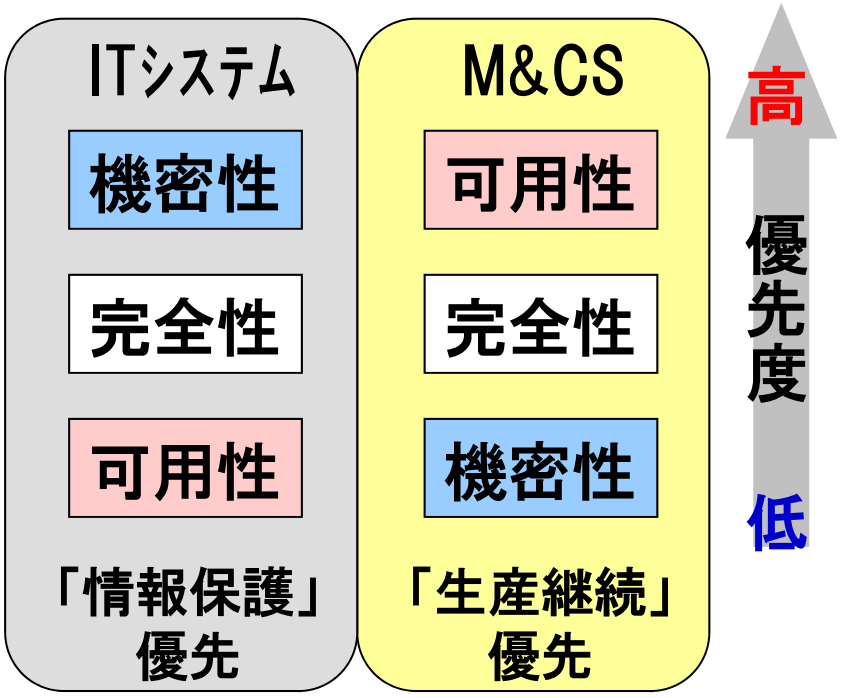
- セキュリティ＝意図的で不当な行為の被害を受けないよう防止
- 生産制御システム(M&CS)のネットワーク化
  ⇒ 脅威が現実のものに（ex. オーストラリア下水道，オハイオ原発）

- 脅威から守るべき性質

①機密性(Confidentiality)：
情報へのアクセスを，**認可された者だけがアクセスできる**状態を確保

②完全性(Integrity)：
情報が**破壊，改ざん又は消去されていない**状態を確保

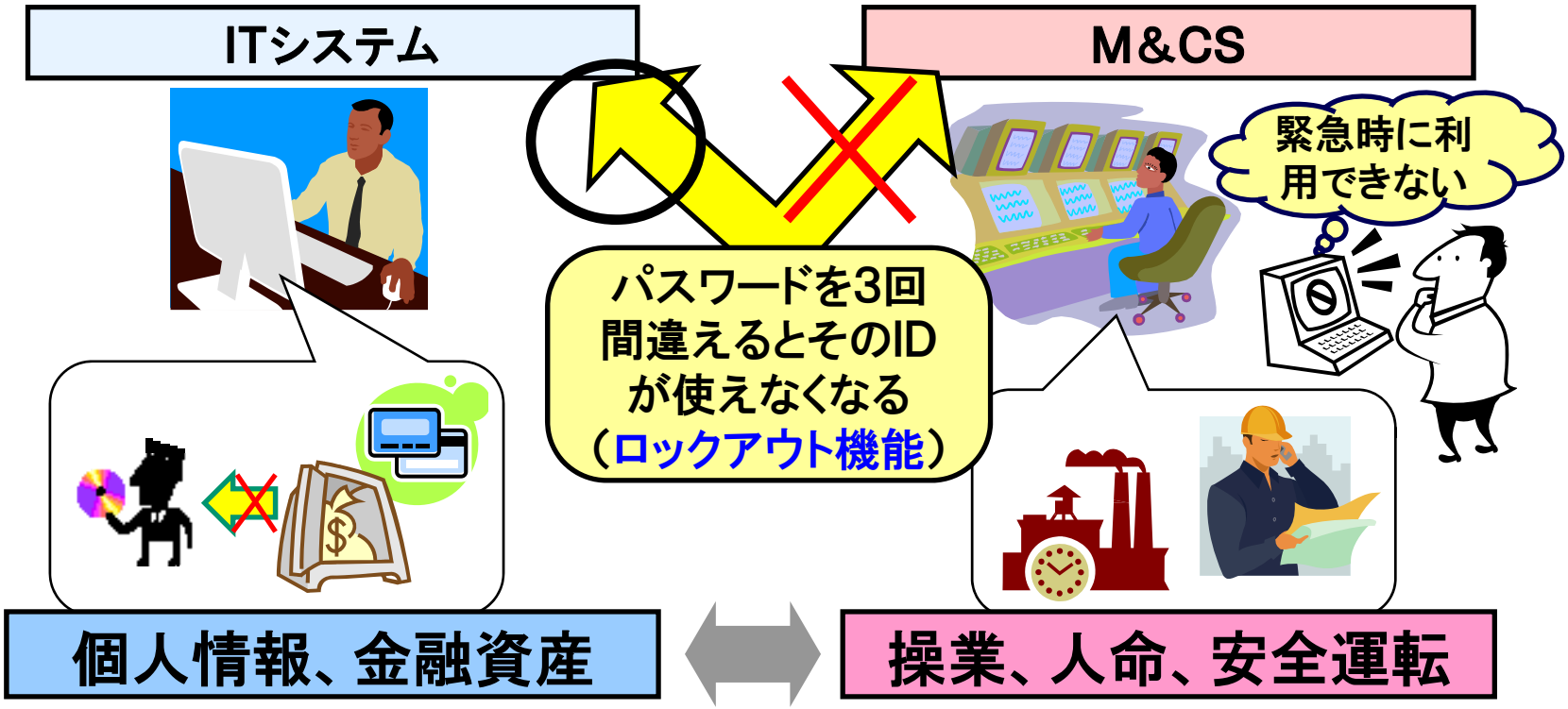
③可用性(Availability)：
認可された者が，**必要時に中断することなく情報にアクセス**できる状態を確保



M&CS：Manufacturing and Control System

1-4. ITセキュリティとM&CSセキュリティ

ユーザ認証での比較例



守るべき資産に違い

異なる「守り方」を検討し実装する必要性ある

目次

2-1. 生産制御システムセキュリティの標準ガイド

- 他システム、上位システムの連携を前提とした生産制御システムのセキュリティ対策をどうすれば？
- セキュリティ管理を体系的に実施するには？

SICE/JEITA/JEMIMA共同
セキュリティWG

生産制御システムとしてのセキュリティ標準・ガイド

◆マネージメント視点では: ISA-SP99, IEC/TC65/WG10, ・・・

◆コンポーネント視点では: NIST/PCSRF/SPP-ICS, ・・・

ISA-SP99を基にセキュリティ管理プログラムの構築実践

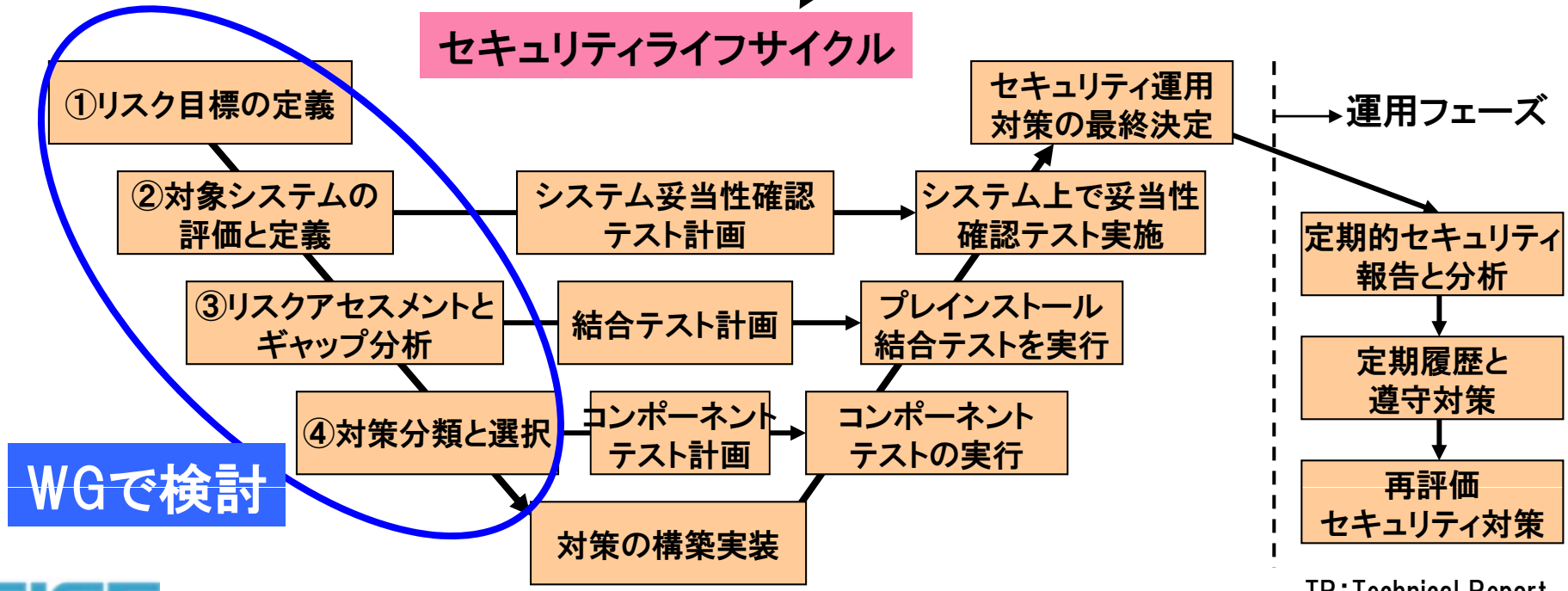
ISA:The Instrumentation, Systems, and Automation Society
IEC:International Electrotechnical Commission, PCSRF:Process Control Security Requirements Forum

2-2. ISA-SP99とは

- 生産制御システムのためのセキュリティガイド

  【対象】DCS, PLC, SCADA, 運転・操業支援システムなど

  - TR1：標準規格、推奨実装法、技術報告および関連情報
  - TR2：システムのライフサイクル全体に適用できる仕組み及び構築方法、検証、監査および評価



TR：Technical Report

2-3. セキュリティ対策手順：①リスク目標定義

①リスク目標定義
↓
②対象資産の定義
↓
③リスク分析
↓
④対策方針の立案

対象の会社，業務レベルでのリスクと許容範囲を定義

たとえば，悪意の操作を前提として想定していく。

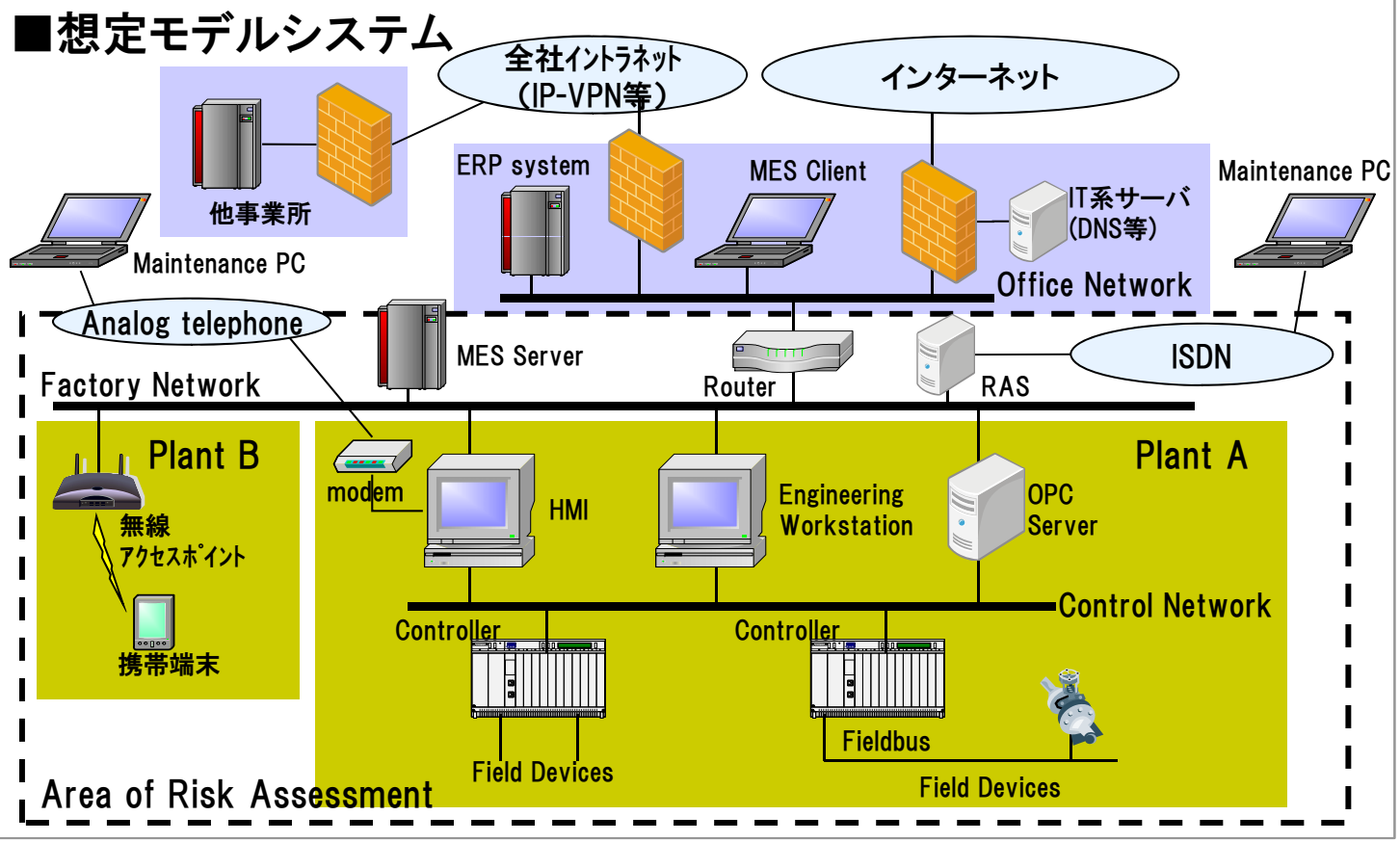
リスクインパクト尺度定義の例

レベル / 分類	インパクト（重要性）			
	1	2	3	無し
身体生命への危害	死亡等重大危害	長期加療/治療	短期加療/治療	傷害無し
金額	＞億円	＞1000万円	＞100万円	小額
環境への影響	永久的	長期的	一時的	殆ど影響無し
生産障害	数週間	数日	数時間	微小時間
会社信用問題	永久的	長期的	一時的	殆ど影響無し

2-4. セキュリティ対策手順：②対象資産の定義

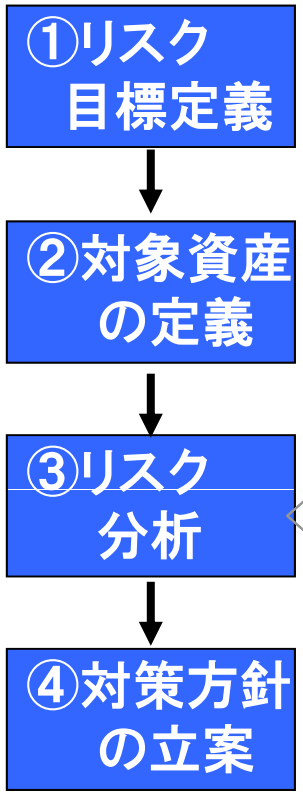
①リスク
目標定義
↓
②対象資産
の定義
↓
③リスク
分析
↓
④対策方針
の立案

正確なネットワーク構成図を作成し、対象システムの資産（装置，アプリ，データ）を漏れなくリストアップ



RAS：Remote Access Server，HMI：Human Machine Interface

2-5. セキュリティ対策手順：③リスク分析



デバイス，アプリ，データ資産について下記を分析

- 脅威の「可能性(Probability)」「重要性(Criticality)」の判断基準を設定
- 進入経路(Remote，Local等)に関する記述

脅威の可能性定義

ネットワークセグメント	脅威の可能性
インターネット 無線LAN ダイアル接続	A＝可能性大
イントラネット コールバック 発信者登録のダイアル接続	B＝可能性中
生産制御システムサイトLAN	C＝可能性小
独立の生産制御システム	D＝可能性無し

2-6. セキュリティ対策手順：④対策方針の立案

①リスク目標定義
↓
②対象資産の定義
↓
③リスク分析
↓
④対策方針の立案

戦略マトリックスを作成し，
下記観点での対策の必要有無を配置する。

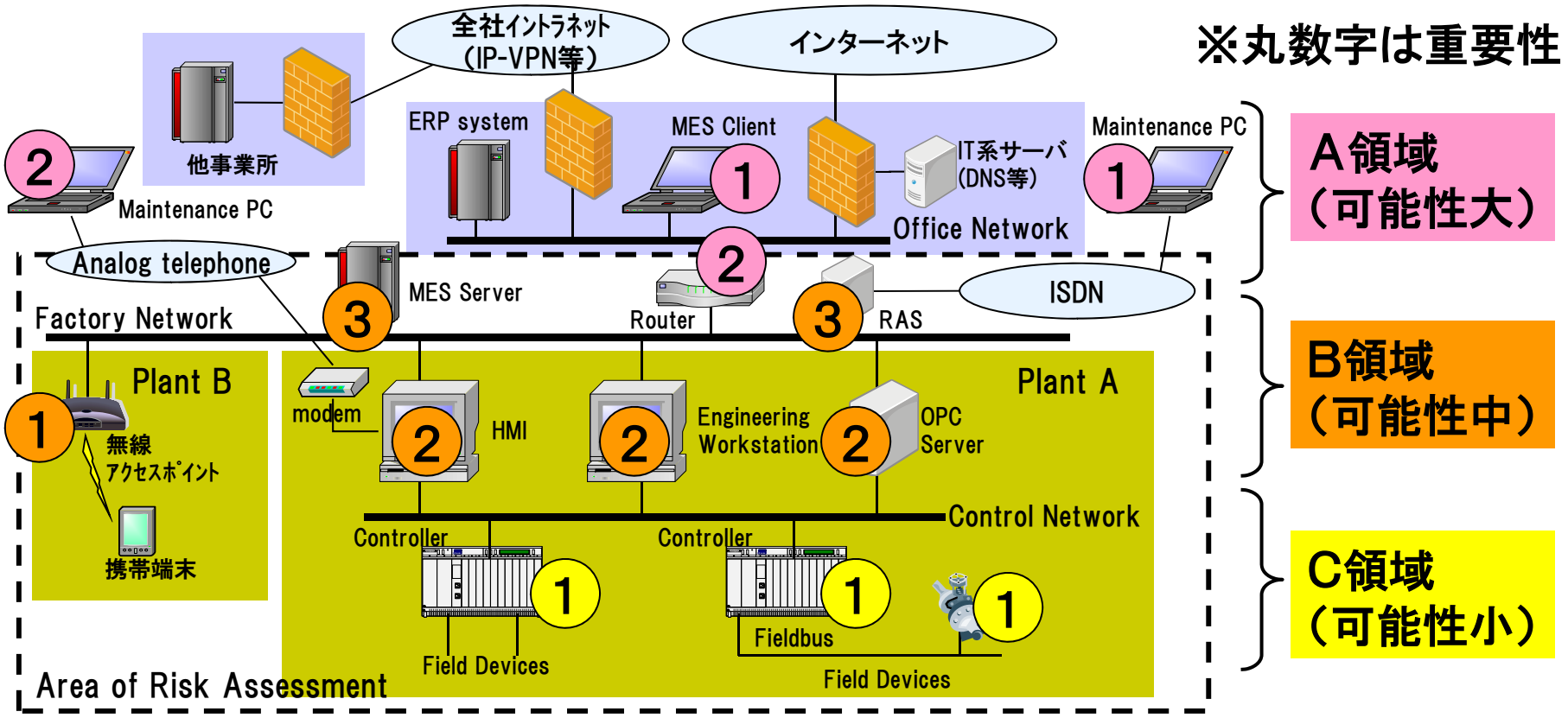
■「防御策要否」戦略マトリックス例

アプリケーションとデバイス資産		脅威の重要性			
		1	2	3	4
脅威の可能性	A（可能性大）	必須	必須	必須	
	B（可能性中）	必須	必須	任意	
	C（可能性小）	必須	必須	任意	
	D（可能性無）	任意			

■対策の観点

緩和策：（Mitigation）	停止時間を減少させる為のバックアップ，RAIDおよびデータ暗号化など，ネットワーク切り離し
防御策：（Access control）	機器やサービス，ユーザ認証などの利用制限
検出策：（Detection）	ログ情報の解析、アンチウィルスソフトによるウィルス検知など

2-7. デバイス資産トポロジーの例



■ 緩和策(Mitigation)

- データのRAIDを導入
- データの暗号化

■ 防御策(Access control)

- DMZを設置しデータ交換
- 無線LANにAES等暗号を導入

■ 検出策(Detection)

- RASのログを監視
- IDSの設置

RAID:Redundant Arrays of Inexpensive Disks, DMZ:DeMilitarized Zone, IDS:Intrusion Detection System

2-8. ISA-SP99によるセキュリティ対策まとめ

戦略マトリックスの結果から防御領域と防御方針（トポロジー）が導かれる。

- 資産の重要性レベル
- 可能性度（例ではＡ～Ｄ）領域レベル
- 防御層（多層防御）と境界
- 適切な資産配置

目次

3-1. 確実なセキュリティ対策を行うためには

セキュリティとは最弱点問題～『鎖は最も弱い所から切れる』

多層防御
Defense-in-depth

技術・環境・使用方法などによる**複数の対策（防御壁）**で，
重要なシステムに対して直接攻撃や情報漏洩を退ける

セキュリティに対する攻撃を防ぐだけではなく，
攻撃を見つけ対応するための
時間稼ぎが可能

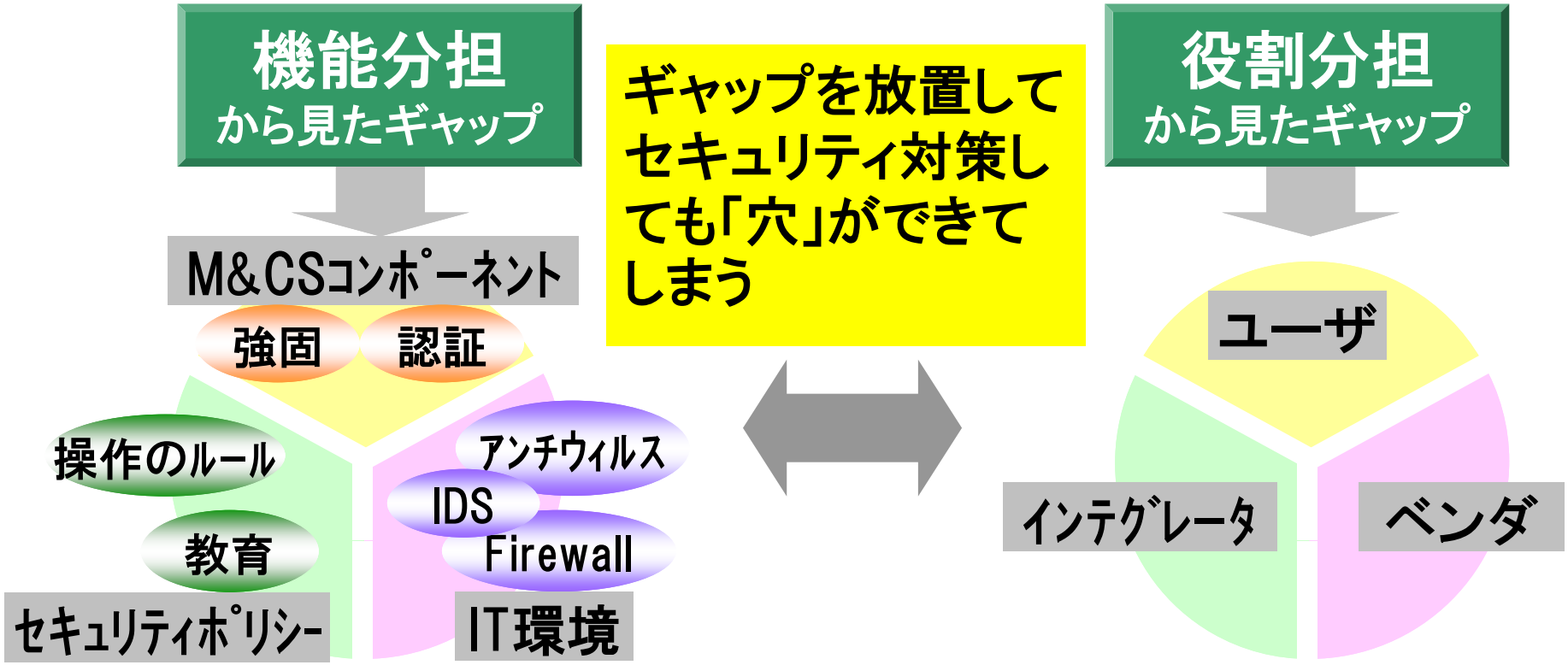
ファイヤウォール・ルータなどによるネットワークセグメント分割

IDS：侵入検知システム
IPS：侵入防御システム

アンチウィルスソフト
Windows等へのセキュリティパッチ

IPS：Intrusion Protection System

3-2. 2つのギャップを考える

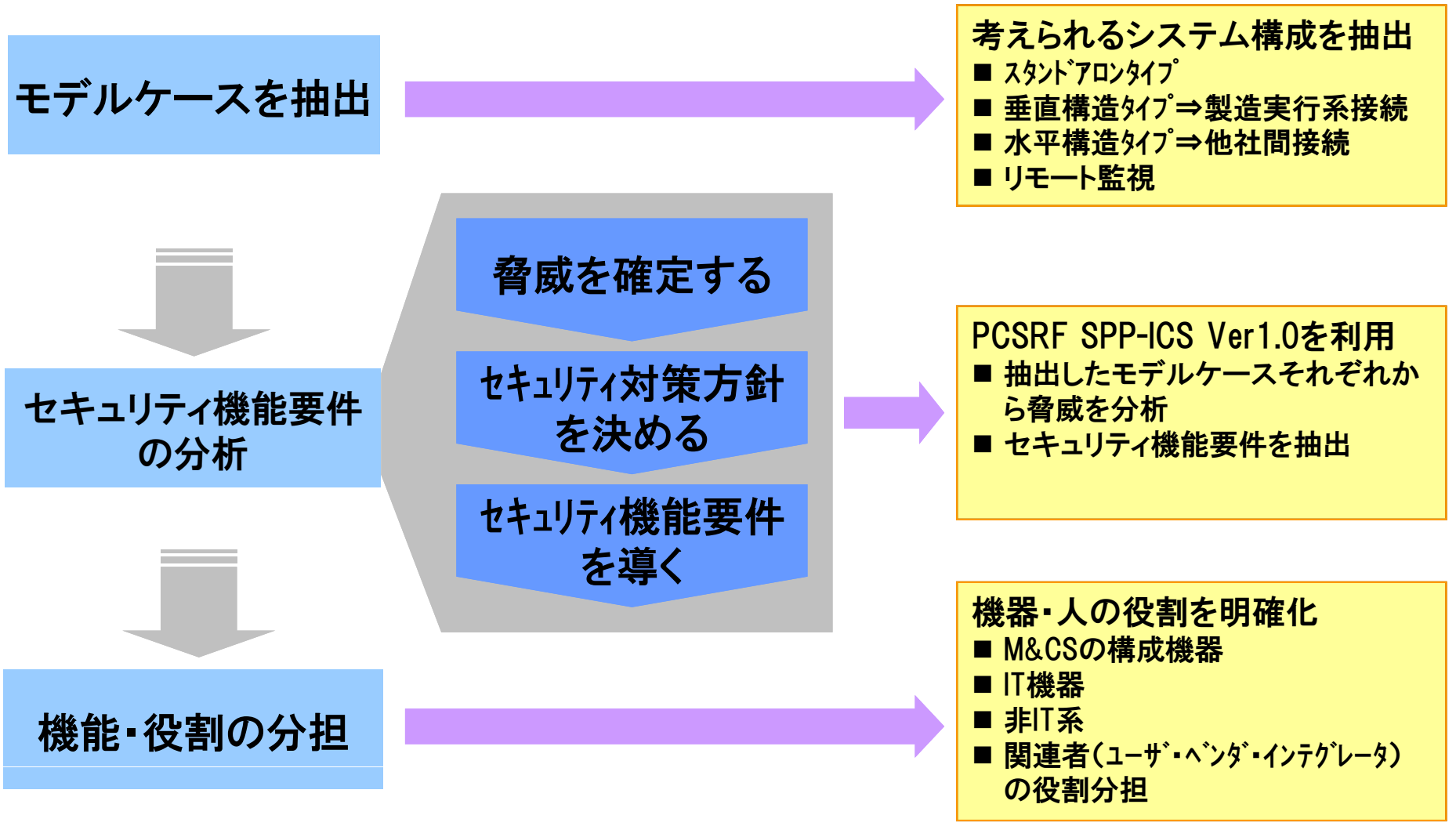


「何」を「誰」が担当するか⇒「SPP-ICS」を用いて役割分担を試行

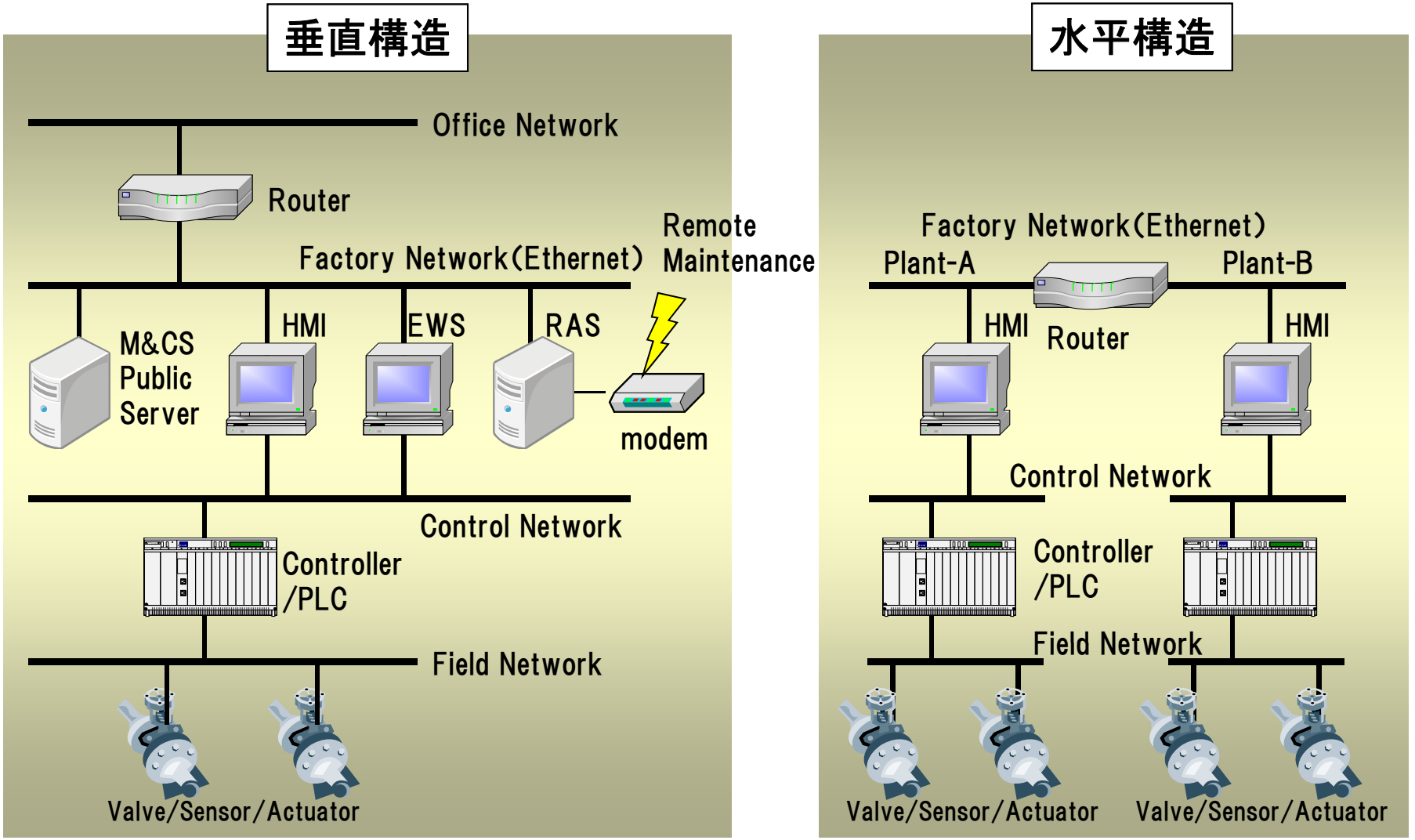
- ISO15408のPP(Protection Profile)をM&CS向けに拡張
- M&CSのためのセキュリティ要件のセット

SPP-ICS:System Protection Profile - Industrial Control System

3-3. 機能・役割分担の概要



3-4. 役割分担に使用したモデルシステム

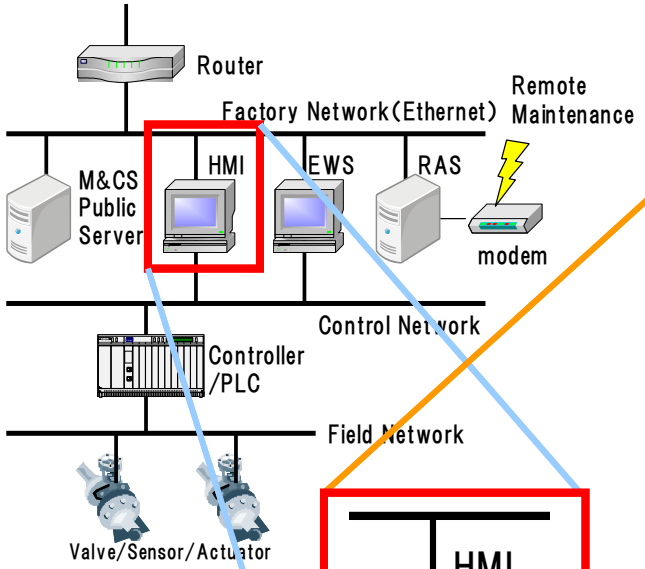


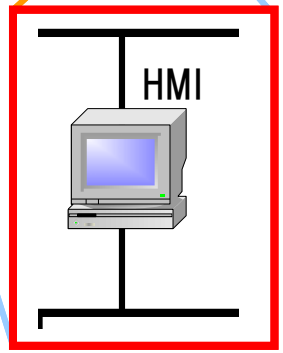
3-5. 脅威を確定する

脅威を確定する

セキュリティ対策方針を決める

セキュリティ機能要件を導く



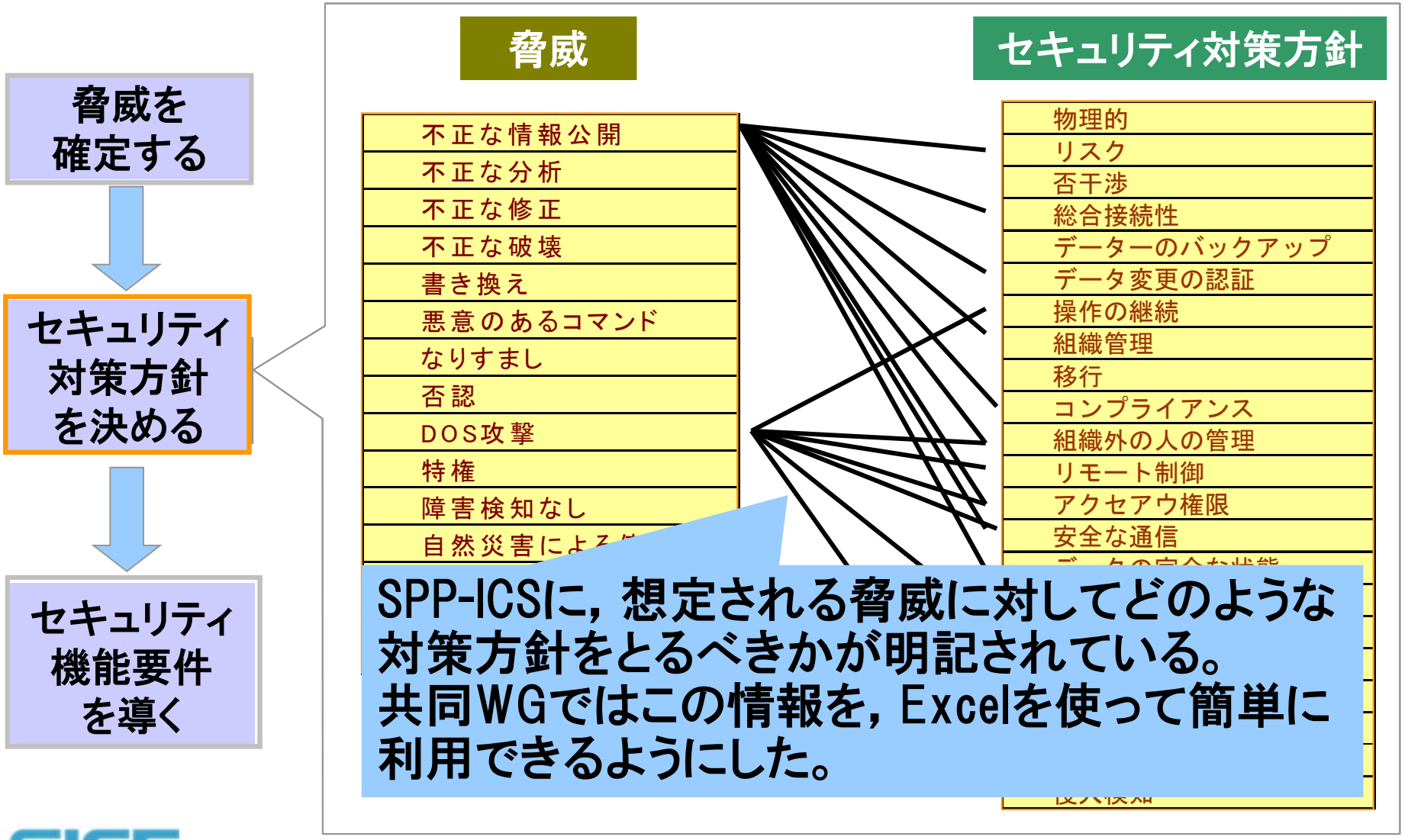


- 不正な情報公開
- 不正な分析
- 不正な修正
- 不正な破壊
- 書き換え
- 悪意のあるコマンド
- なりすまし
- 否認
- DOS攻撃
- 特権
- 障害検知なし
- 自然災害による停止
- 電力停止
- ウィルス感染
- 物理的攻撃

コンポーネント毎に、SPP-ICSを参照しながら、考えられる脅威を確定する

脅威
SPP-ICSで定義されている

3-6. セキュリティ対策方針を決める



3-7. セキュリティ機能要件を導き出す

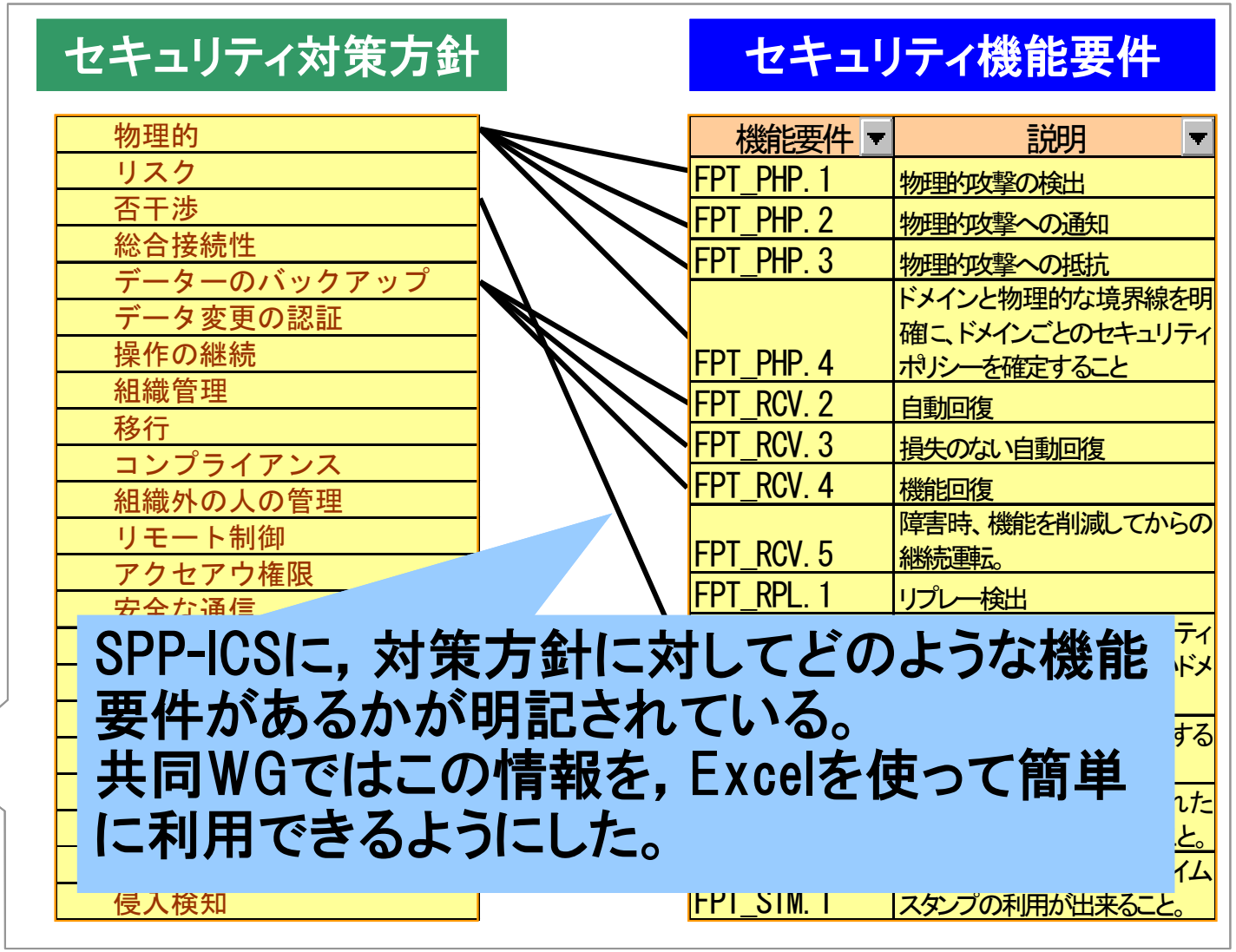
脅威を確定する

↓

セキュリティ対策方針を決める

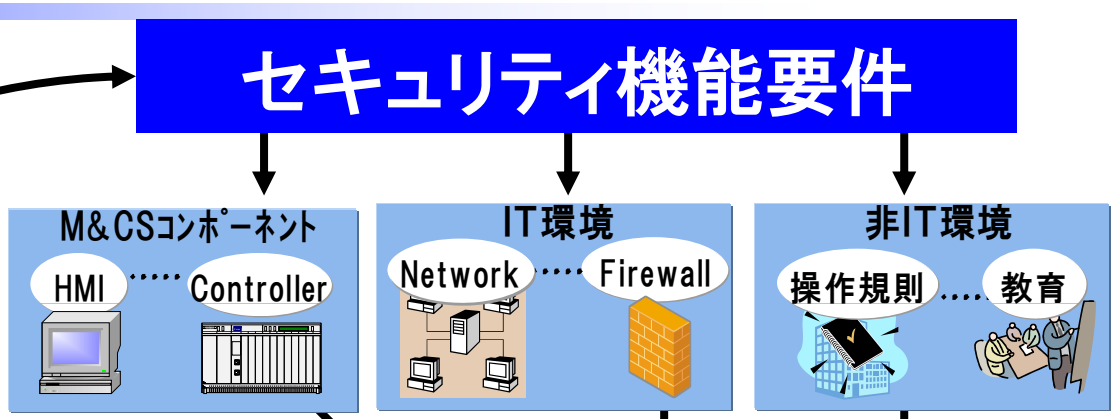
↓

セキュリティ機能要件を導く



SPP-ICSに，対策方針に対してどのような機能要件があるかが明記されている。
共同WGではこの情報を，Excelを使って簡単に利用できるようにした。

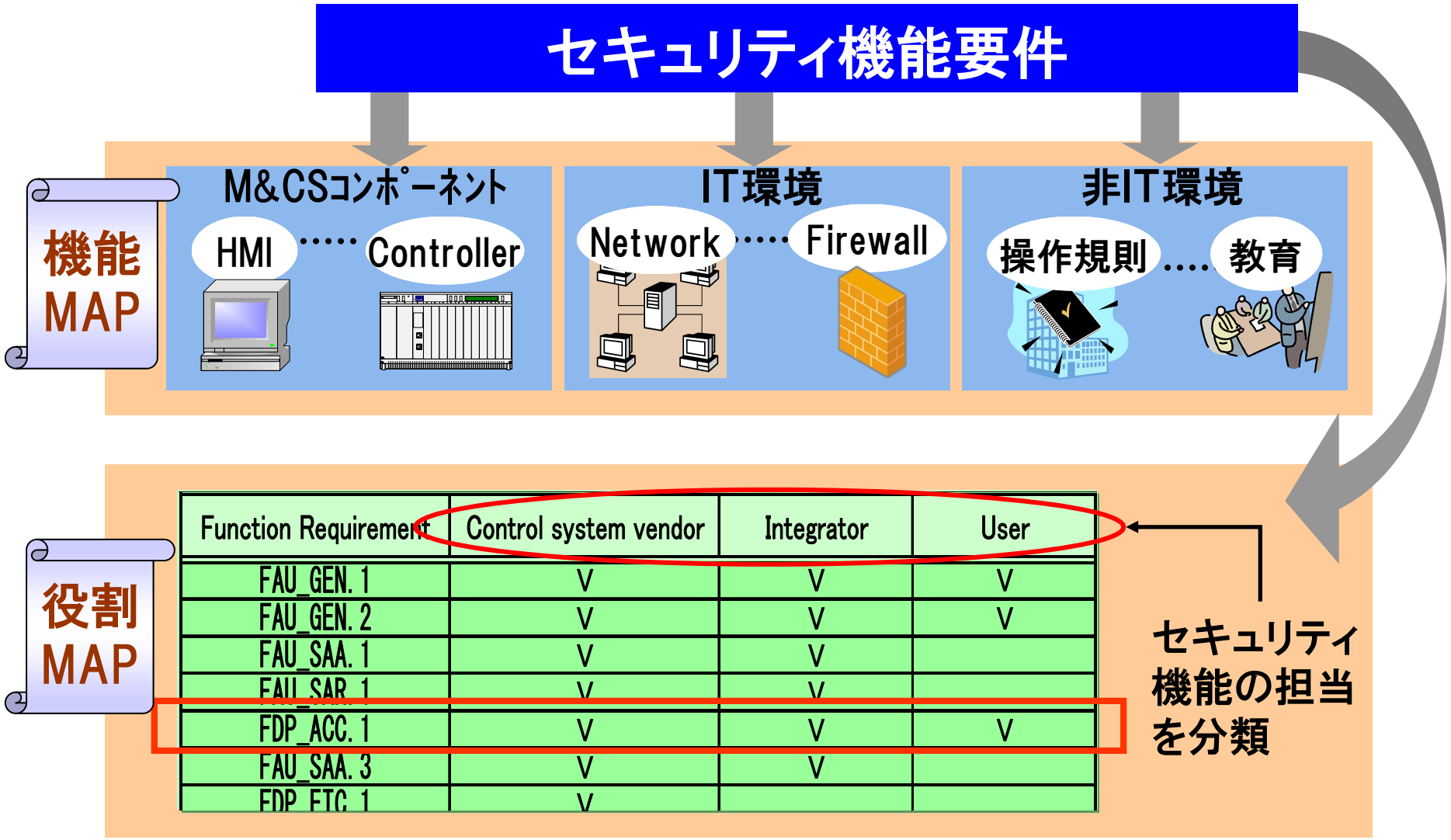
3-8. 機能MAPを作る



機能MAP

Function requirement	Explanation	HMI	Controller	IT Environment	Non-IT environment
FAU_GEN.1	Record the audit log	V		V (Firewall)	V
FAU_GEN.2	Record the user ID in the audit log	V		V (Firewall)	V
FAU_SAA.1	The violation of the policy can be audited according to the set rule.	V		V (Firewall)	
FAU_SAR.1	The audit information can be provided in an appropriate way for those engaged in the audit	V		V (Firewall)	
FDP_ACC.1	Accesses can be partly restricted.	V		V	
FAU_SAA.3	Simple attacks can be detected.	V		V	V

3-9. 役割MAPを作る


セキュリティ機能要件
機能MAP
M&CSコンポーネント
HMI
Controller
IT環境
Network
Firewall
非IT環境
操作規則
教育
役割MAP
Function Requirement
Control system vendor
Integrator
User
FAU_GEN.1 V V V
FAU_GEN.2 V V V
FAU_SAA.1 V V
FAU_SAR.1 V V
FDP_ACC.1 V V V
FAU_SAA.3 V V
FDP_ETC.1 V
セキュリティ機能の担当を分類

3-10. SPP-ICSによる機能・役割分担のまとめ

機能MAP

Function requirement	Explanation	HMI	Controller	IT Environment	Non-IT environment
FAU_GEN.1	Record the audit log	V		V (Firewall)	V
FAU_GEN.2	Record the user ID in the audit log	V		V (Firewall)	V
FAU_SAA.1	[illegible]	V		V (Firewall)	
FAU_SAR.1	[illegible]	V		V (Firewall)	
FDP_ACC.1	[illegible]	V		V	
FAU_SAA.3	[illegible]	V		V	V
FDP_ETC.1	[illegible]	V			
FPT_PHP.1	Detect the physical attacks	V	V		
FPT_PHP.2	Notification to the physical attacks	V	V		
FPT_RCV.2	Automated recovery		V		
FPT_RPL.1	Detect the replay		V	V	

役割MAP

Function Requirement	Control system vendor	Integrator	User
FAU_GEN.1	V	V	V
FAU_GEN.2	V	V	V
FAU_SAA.1	V	V	
FAU_SAR.1	V	V	
FDP_ACC.1	V	V	V
FAU_SAA.3	V	V	
FDP_ETC.1	V		
FPT_PHP.1	V		
FPT_PHP.2	V		
FPT_RCV.2	V		
FPT_RPL.1	V	V	

M&CSの構成機器等が持つべきセキュリティ機能を明確にできた

セキュリティ対策する際のM&CS構築関係者の役割を明確にできた

セキュアなM&CSの構築に重要な役割を果たす

まとめ

- SICE/JEITA/JEMIMAでは共同WG活動にて次のセキュリティ規格の調査研究を行いました。
  - 制御系ネットワーク装置の「重要度と可能性に応じた」防御方針を，ISA-SP99を用いて抽出しました。
  - 制御系セキュリティの要件分析と役割分担をNIST/PCSRFのSPP-ICSを用いて試行し，セキュリティ対策の穴を減らす提言をしました。

- 今後の活動
  - 各種セキュリティ規格のライフサイクルとターゲットを一覧する俯瞰マップを作成しています。

A-1. セキュリティ規格利用における悩み

- セキュリティ規格、標準化団体は増えてきているが・・・
  - 現状
    - 欧米を中心に様々な規格、ガイドライン、団体が乱立している
    - 分野ごとに多数存在。互いに参照しあっているものもあるが，実際に適用する際に何を参照したら良いのか判断できない
  - ベンダーの立場
    - 製品の設計や評価検証時にどの規格を採用したら良い？
  - ユーザーの立場
    - システムの検討フェーズや運用フェーズでやるべき事が不明

解決策として

必要な分野や開発フェーズ（ライフサイクル）から
必要な規格を参照可能とするための俯瞰マップを作成する

A-2. 俯瞰マップのレイアウト

- 参照するドキュメントが、セキュリティライフサイクルのどの部分について書かれているかを容易に確認可能