Japan Computer Emergency Response Team Coordination Center

電子署名者 : Japan Computer Emergency Response Team Coordination Center
DN : c=JP, st=Tokyo, l=Chiyoda-ku, email=office@jpcert.or.jp, o=Japan Computer Emergency Response Team Coordination Center, cn=Japan Computer Emergency Response Team Coordination Center
日付 : 2010.03.09 10:36:50 +09'00'

制御システムにおける セキュリティ役割分担の取り組み

制御システムセキュリティカンファレンス 2010
2010. 2. 9

（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 日立研究所
山田 勉

目次

1. 制御システムセキュリティの背景と課題
   - SICE/JEMIMA/JEITAセキュリティ共同WG

2. 制御システムセキュリティのケーススタディ

3. セキュリティ機能と役割分担の検討
   - NIST/PCSRF/SPP-ICS

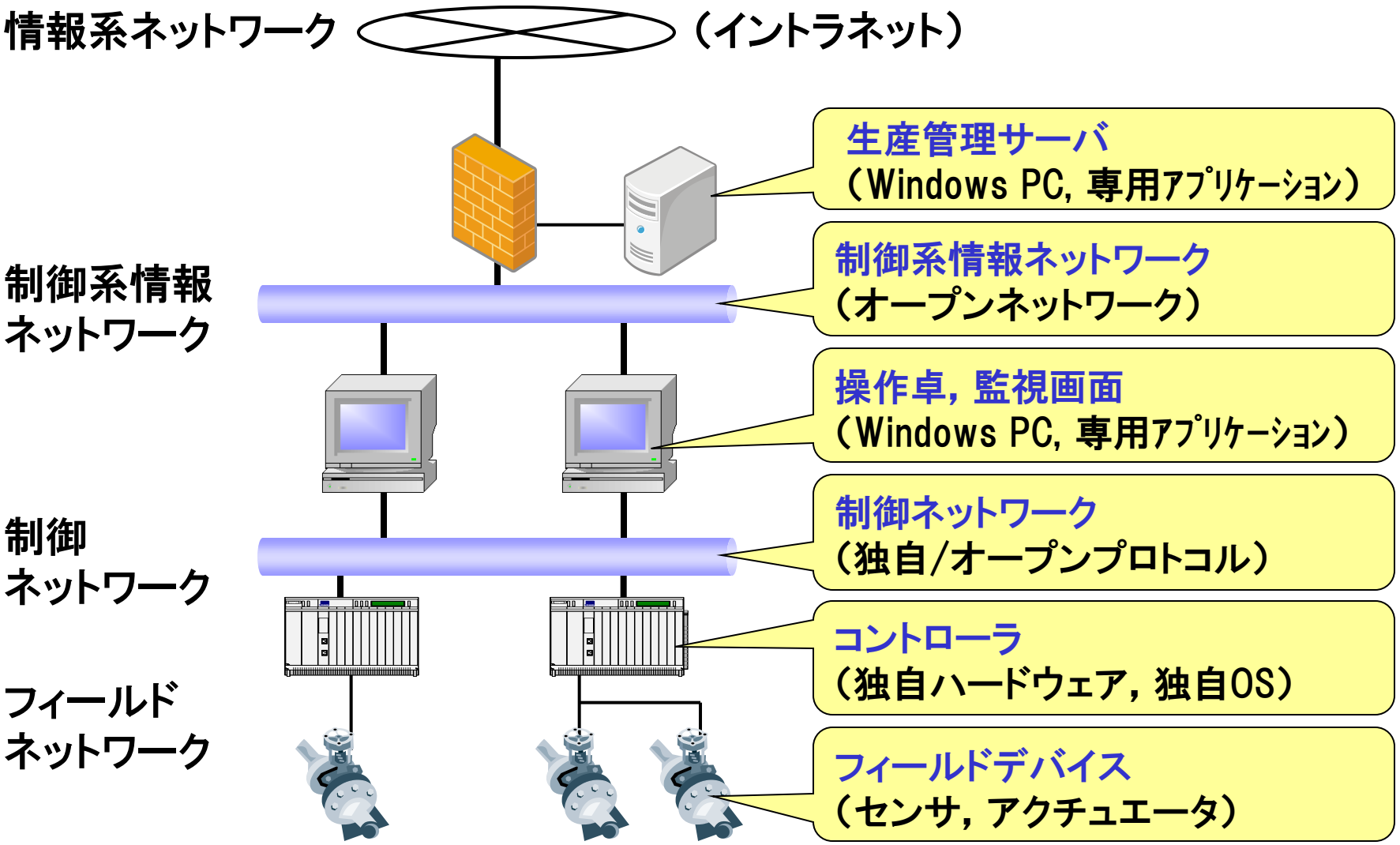
1-1. SICE/JEITA/JEMIMA共同セキュリティWG

- 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(株)，(株)山武，(株)東芝，富士電機ｼｽﾃﾑｽﾞ(株)
  (株)日立ﾊｲﾃｸｺﾝﾄﾛｰﾙｼｽﾃﾑｽﾞ，(株)日立製作所
- 広報活動
  - JEMIMA 計測展，委員会セミナー
  - SICE Annual Conference，産業応用部門大会
  - JEITA 制御システムフォーラム
  - JPCERT/CC 制御システムセキュリティ・カンファレンス
- 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

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

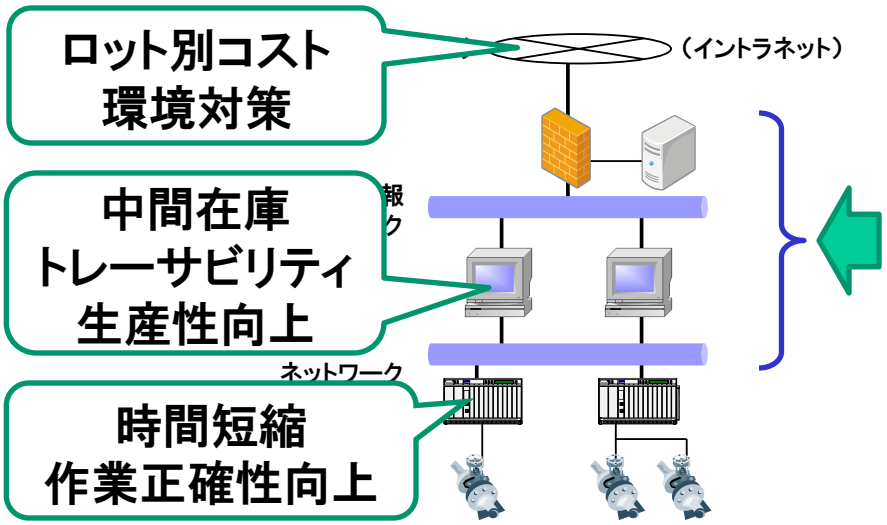
1-2. 制御システムの概要



1-3. 制御システムセキュリティの背景

制御システムにおいて情報連携の重要性が高まる

見える化(経営，生産管理，操業) ＋ 技術の共通化の進展



技術の共通化の進展
- オープン技術
- マルチベンダ

- ハードウェア(x86, LAN用LSI)
- OS(Windows, Linux)
- ネットワーク(Ethernet, 無線LAN)
- プロトコル(OPC, 産業用Ethernet)
- アプリケーション(ﾃﾞｰﾀﾍﾞｰｽ, Web)

外部からの干渉を受けやすくなる

⇒被害を受けないように防止することが必要になる

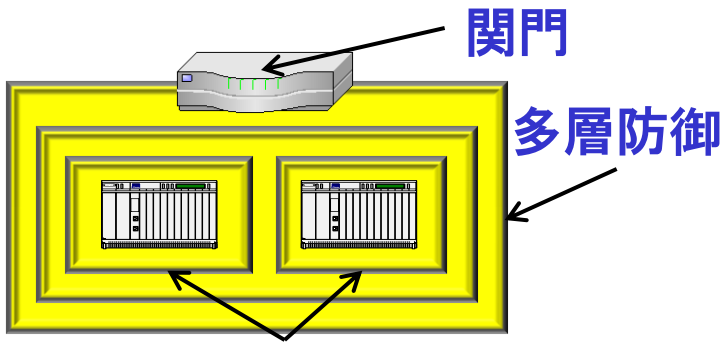
OPC:OLE for Process Control

1-4. 制御システムセキュリティの課題

出典：IPA「重要インフラの制御システムセキュリティとITサービス継続」

- 課題1：オープン化に伴う脆弱性リスクの混入
  - 汎用製品，標準ネットワークの採用
    ⇒ 脆弱性の課題も引き継ぐ（例：USBメモリ，ネットワーク侵入）
- 課題2：長期利用に伴うセキュリティ対策技術の陳腐化
  - 10～20年の間に，対策が更新されない可能性あり
- 課題3：可用性重視に伴うセキュリティ機能の絞り込み
  - ウイルス検査プログラム負荷のシステムに対する影響
  - パッチ導入によるシステム稼働率への影響

基本戦略：
独立した複雑な
セキュリティシステムより，
シンプルな対策を「重ねる」



目次

1. 制御システムセキュリティの背景と課題
   - SICE/JEMIMA/JEITAセキュリティ共同WG

2. 制御システムセキュリティのケーススタディ

3. セキュリティ機能と役割分担の検討
   - NIST/PCSRF/SPP-ICS

2-1. 事例：オーストラリア下水システム侵入

- 2000年，下水処理管理システムが不正に侵入され，河川や公園に何百万リットルもの下水を流出

- 侵入したエンジニア
  - マルーチー市の下水システムを開発した会社に勤務していた
  - クイーンズランド州マルーチー市へ就職を希望したが，不採用で立腹
  - 2000年3月～4月で少なくとも46回侵入し，システムの制御権を奪取

- ノートPC＋無線を使い侵入
  ⇒逮捕・禁固2年

Maroochy by Google map

2-2. セキュリティとは

- 『意図的で不当な行為(＝攻撃)の被害を受けないよう防止すること』
  - 意図的で無い行為から資産を守るのは「安全対策」

- オーストラリアの例ではどうすれば良かったか
  - 設計管理，ユーザ管理，リモートアクセス制限 etc.
    ⇒「気付き」が肝心

- シンプル/安易なセキュリティはない。
  繰り返して見直す，PDCAサイクルを回すこと
  が重要

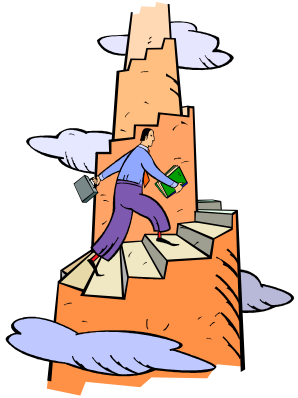
PDCA：Plan Do Check Act

2-3. セキュリティ規格の分類

	管理運用視点 ・セキュリティ管理システム仕様 ・推奨実施例	コンポーネント視点 ・セキュリティ機能要件定義 ・評価・認証の枠組み
情報系セキュリティ	・ISO/IEC 27000シリーズ(27001:情報セキュリティ管理システム(ISMS)要求事項, 27002:ISMS 実践のための規範, 27005:情報システムのリスク管理, 27006:認証/登録プロセスの要求仕様) ・NIST SP800-53他	・ISO/IEC 15408 (Common Criteria;CCと称される。製品がセキュリティに配慮すべき事項)
制御系セキュリティ	・ISA-99 (生産制御システムセキュリティ) ・ISO/IEC 62443 (予定) (Industrial Process Measurement and Control – Net & System Security) ・NIST SP800-82	・PCSRF SPP-ICS (System Protection Profile - Industrial Control System)

2-4. PDCAの具体策

	使えるツール・規格
Plan	各種Good Practice セキュリティ評価ツール ISA-99 NIST SP800-53/82, PCSRF：SPP-ICS
Do	ISA-99 脆弱性スキャナ
Check	ログ監査/侵入検知システム(IDS) 脆弱性情報
Act	ISA-99 NIST SP800-53/82



SPP-ICSを「役割分担」に使うことを検討

目次

1. 制御システムセキュリティの背景と課題
   - SICE/JEMIMA/JEITAセキュリティ共同WG

2. 制御システムセキュリティのケーススタディ

3. セキュリティ機能と役割分担の検討
   - NIST/PCSRF/SPP-ICS

3-1. 確実なセキュリティ対策を行うためには

多層防御
Defense-in-depth

技術や使用方法による
複数の対策（防御壁）で
システムに対する直接攻撃や情報漏洩を退ける

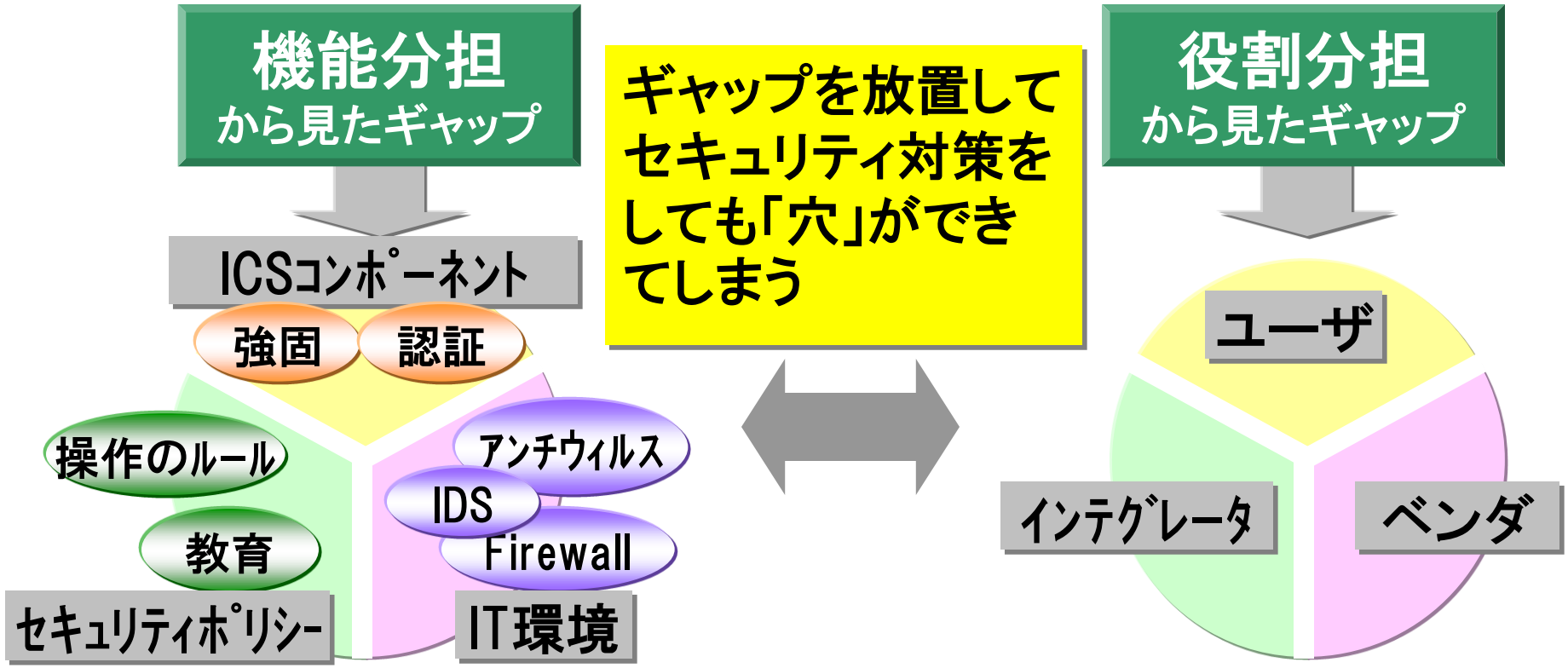
セキュリティに対する攻撃を防ぐだけではなく，
攻撃を見つけ対応するための**時間稼ぎが可能**

ファイヤウォールで
ネットワーク分割

侵入検知システム

ウィルス検知ソフト
OSのパッチ

3-2. 2つのギャップを考える



「誰」が「何」を担当するか⇒「SPP-ICS」を用いて役割分担を試行

- 産業制御システム(ICS)のためのセキュリティ要件のセット
- ISO/IEC 15408のPP(Protection Profile)をICS向けに拡張

IDS:Intrusion Detection System,　SPP-ICS:System Protection Profile - Industrial Control System

3-3. 機能・役割分担の概要

システム構成を定義

↓

セキュリティ機能要件の分析
（SPP－ICSの活用）

- 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

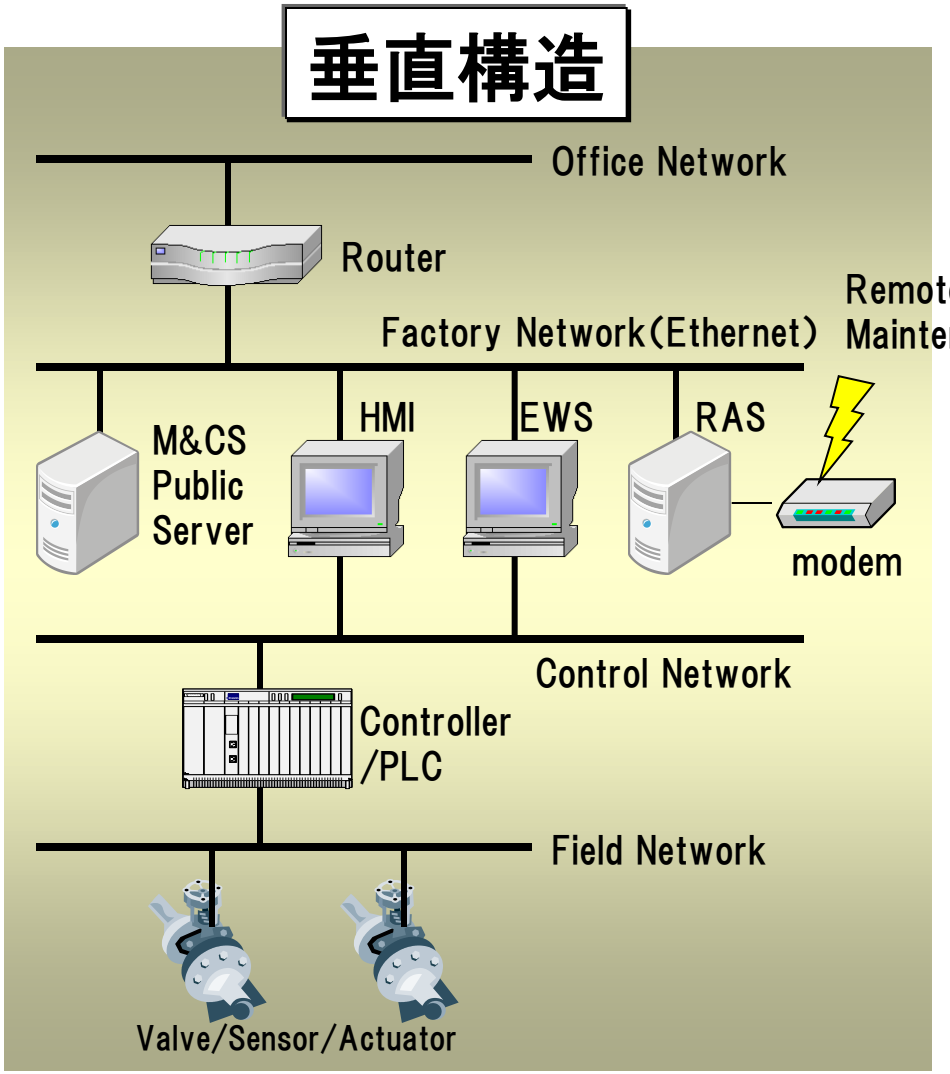
↓

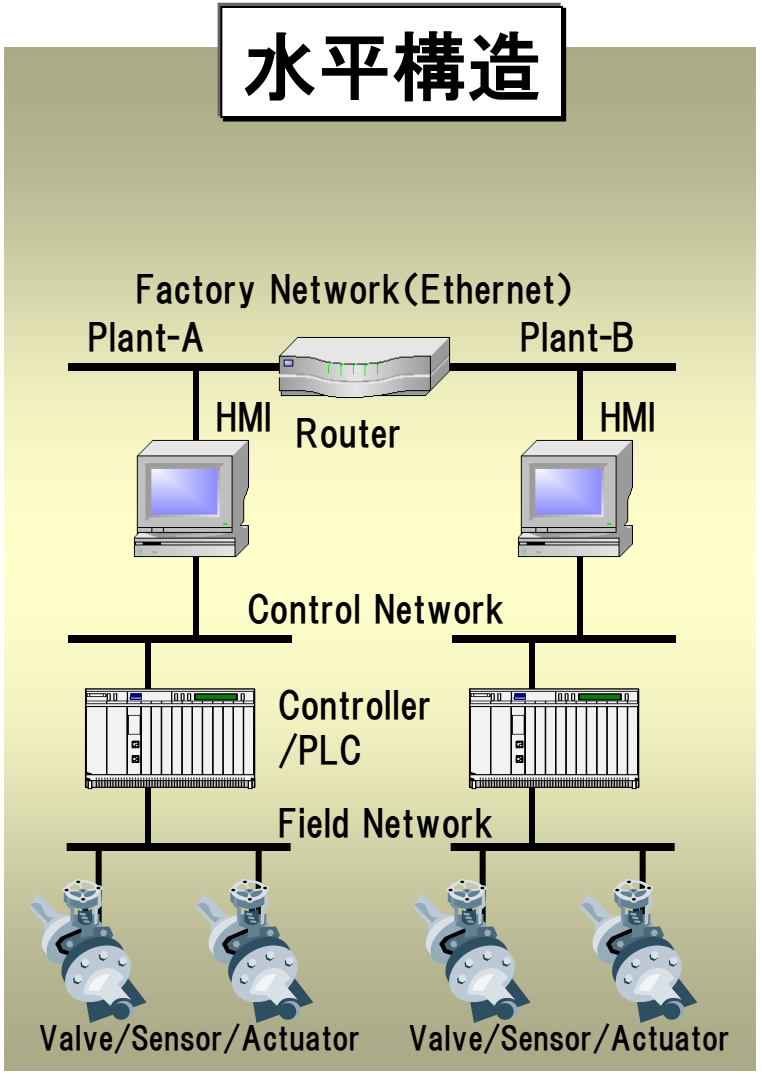
機器・環境のセキュリティ機能分担
＆実装する責任者（役割分担）を明確化

- ICS機器
- IT機器
- 非IT系

- ユーザ
- ベンダ
- インテグレータ

3-4. 役割分担に使用したモデルシステム



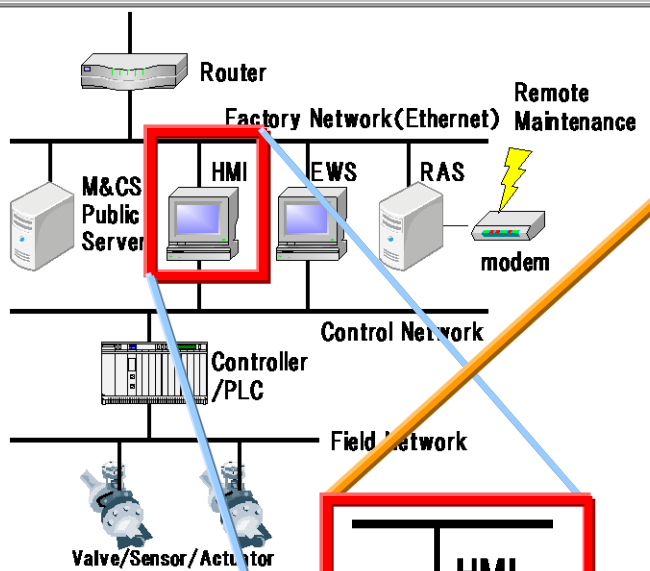


3-5. システムにおける脅威を確定する

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

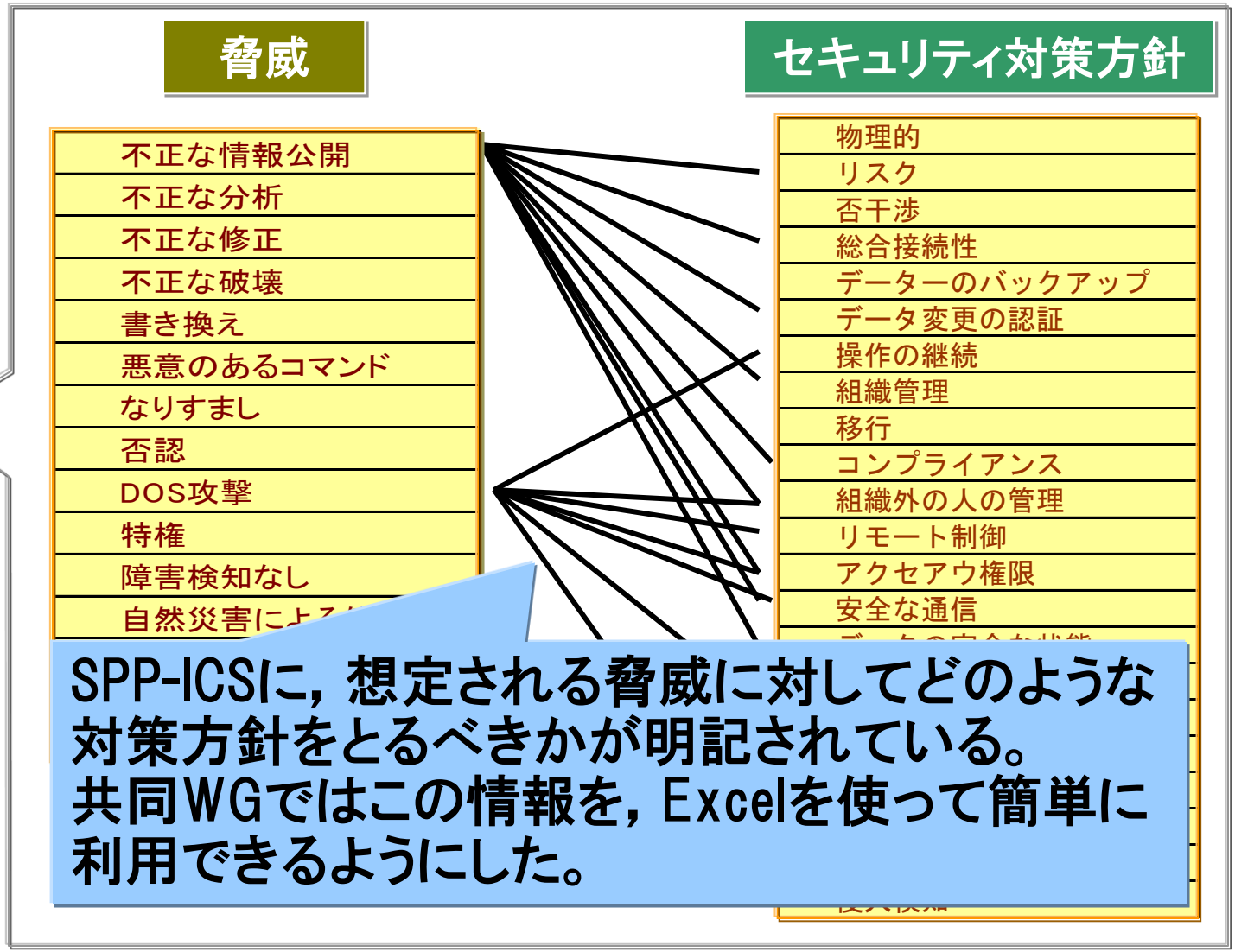
脅威
SPP-ICSで定義されている

3-6. セキュリティ対策方針を決める

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



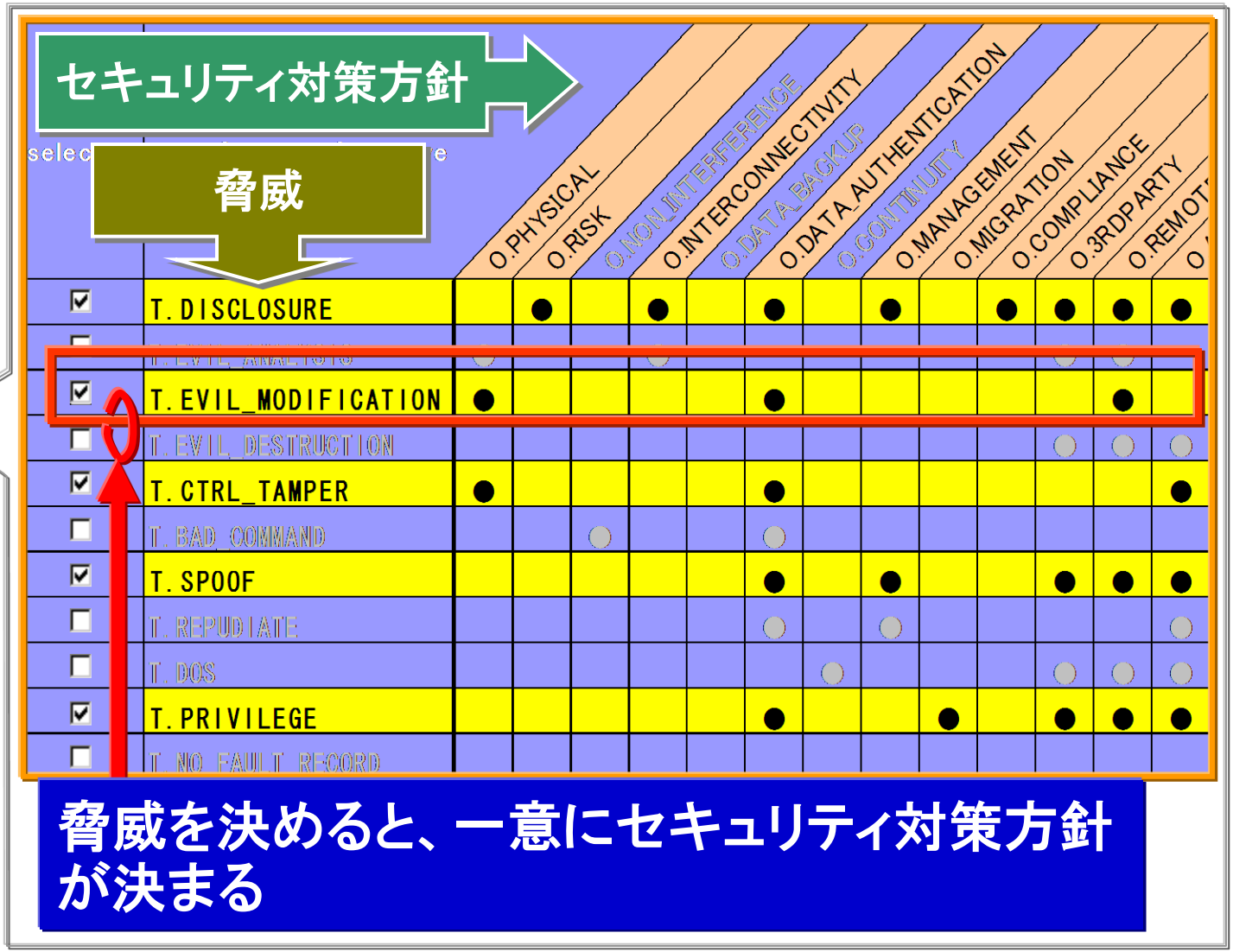
SPP-ICSに，想定される脅威に対してどのような対策方針をとるべきかが明記されている。
共同WGではこの情報を，Excelを使って簡単に利用できるようにした。

3-6. セキュリティ対策方針を決める

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



3-7. セキュリティ機能要件を導き出す

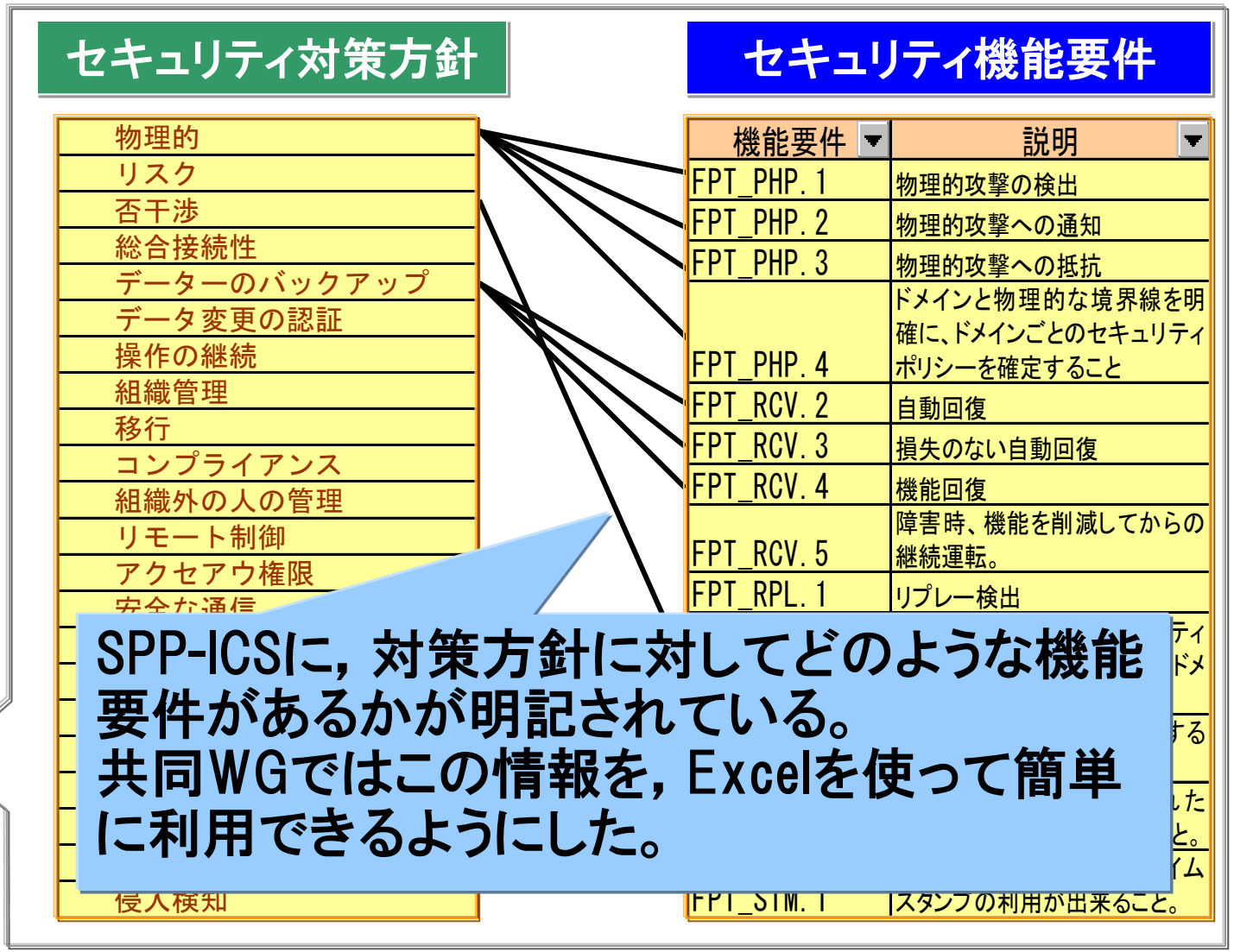
脅威を確定する

↓

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。

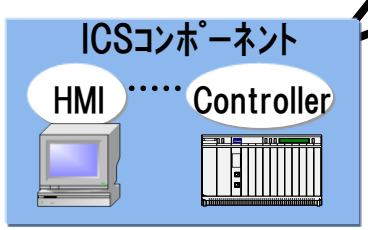
3-8. 機能MAPを作る

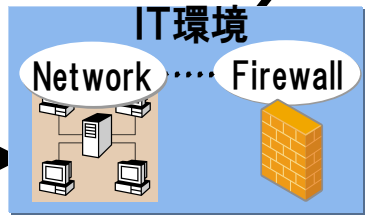
機能MAP

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

=

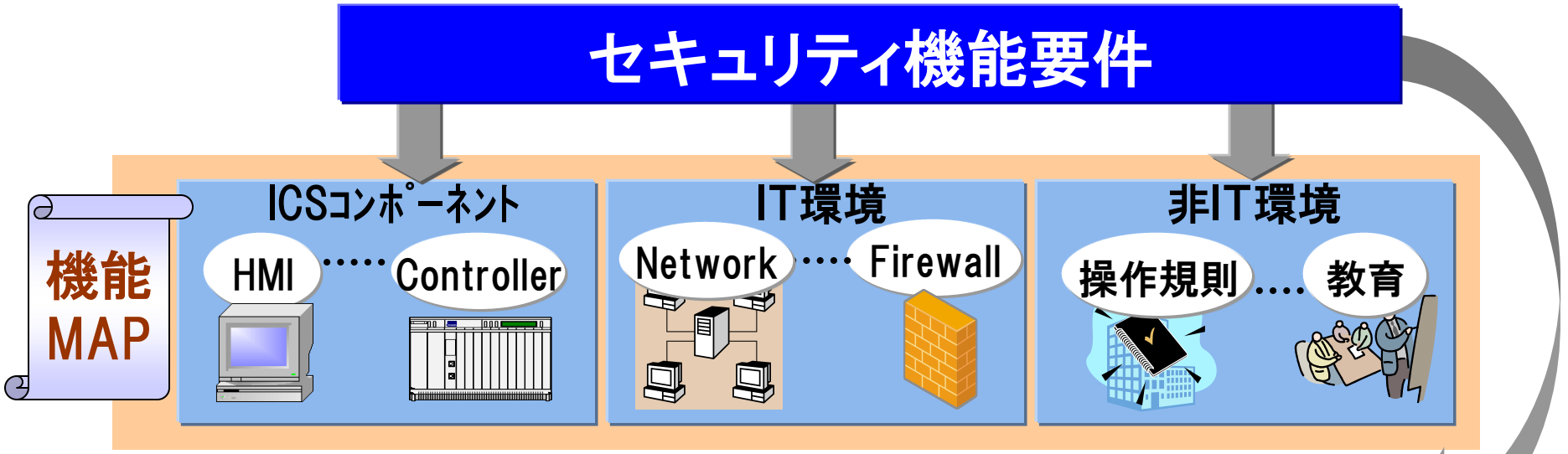
セキュリティ機能要件





実現手段へ割り当てる

3-9. 役割MAPを作る



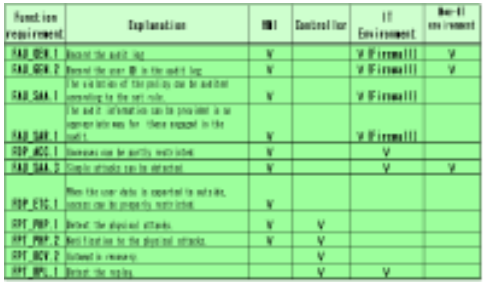
役割MAP

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実行責任者を割り当て

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	The examination of the policy can be analyzed corresponding 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	Usernames can be partly restricted	V		V	
FAU_SAA.3	Simple attacks can be detected	V		V	V
FDP_ETC.1	When the user data is exported to outside, success can be properly restricted	V			
FPT_PHP.1	Detect the physical attacks	V	V		
FPT_PHP.2	Alert function to the physical attacks	V	V		
FPT_RCV.2	Failback is necessary		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	

制御システム構成機器等が持つべきセキュリティ機能を明確にできる

セキュリティ対策する際の制御システム関係者の役割を明確にできる

セキュアな制御システムを構築

まとめ

- SICE/JEITA/JEMIMAでは共同WG活動にて制御システムセキュリティの調査研究を推進中。
  - 制御システムセキュリティは関係者（ユーザ・インテグレータ・ベンダ）の共同が必要。
  - セキュリティ対策の穴を減らすためにNIST/PCSRFのSPP-ICSを用いることで機能分担と役割分担ができることを確認した。

- 今後の活動
  - JPCERT/CCと共同で，セキュリティ評価ツールを試行し，利用上の課題や利点を評価する。