JEMIMA Japan Electric Measuring Instruments Manufacturers' Association

生産制御システムのセキュリティ

2008.11.26

PA･FA計測制御委員会

セキュリティ調査研究WG

社団法人 日本電気計測器工業会

WGのご紹介

- 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。

- 設立:2005年4月
- 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

- 活動実績
  - 研究活動
    1. SP99　TR2を利用したセキュリティ対策の実践
    2. SPP-ICS ver1.0を利用したセキュリティ要件の分析および役割分担の明確化
    3. セキュリティ標準規格の調査

WGのご紹介

- 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 2008
  - SICE Annual Conference 2008
- 団体との協力関係
  - SICE（計測・制御ネットワーク部会）
  - JEITA（制御システム専門委員会）
  - JPCERT/CC
  - IPA（独立行政法人情報処理推進機構）
- その他の活動
  - IEC/TC65/WG10国内委員会にメンバ登録

Agenda

PART1

生産制御システムセキュリティの現状

PART2

制御システムのセキュリティ規格とセキュリティ俯瞰MAP

PART3

セキュリティライフサイクルを意識した対策の立案
（SP99に基づいたセキュリティ対策立案の紹介）

セキュリティ機能要件の分析と役割分担
（NIST SPP-ICSを利用した分析の紹介）

JEMIMA Japan Electric Measuring Instruments Manufacturers' Association

PART 1

生産制御システム セキュリティの現状

2008.11.26

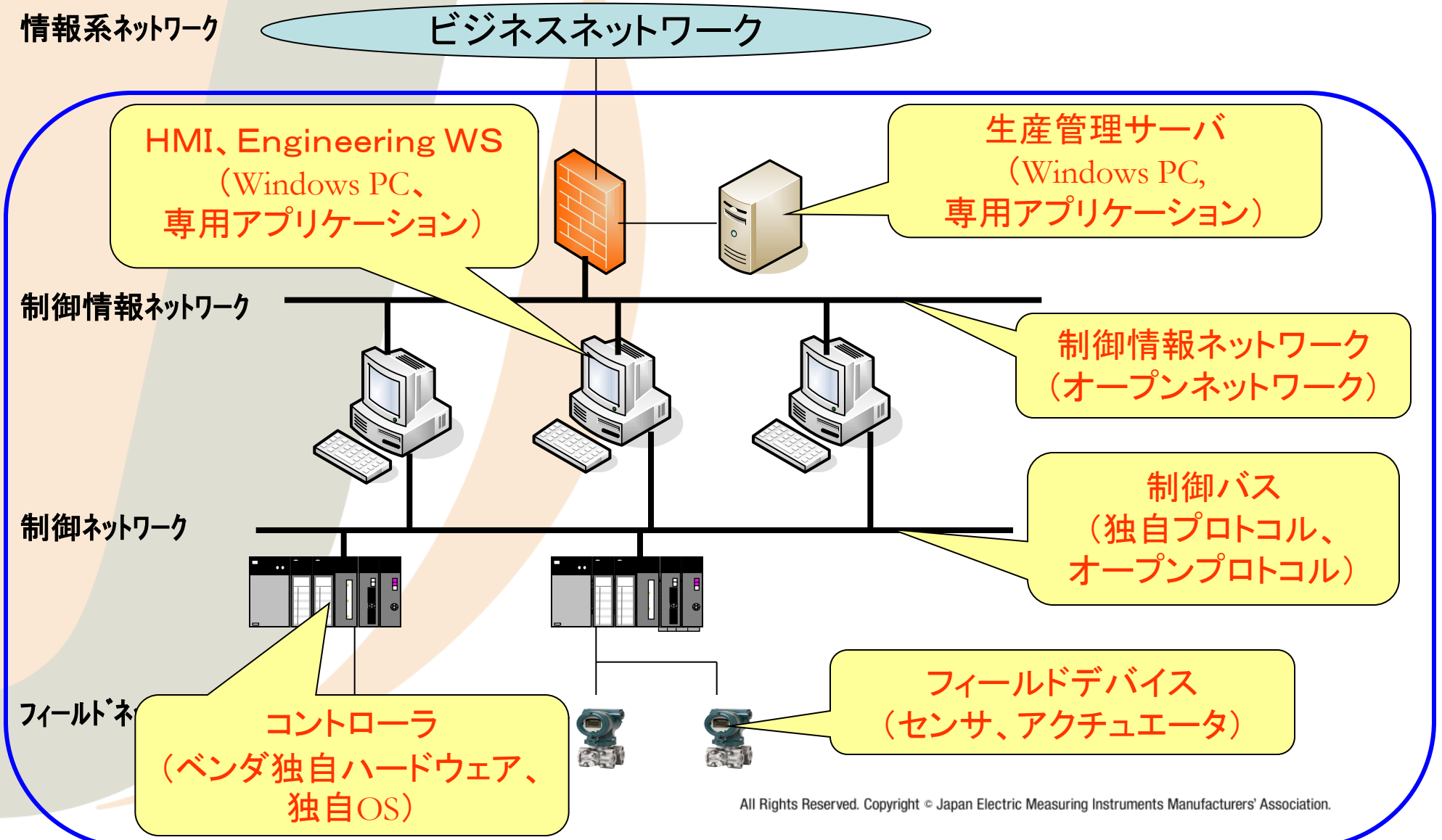
PA･FA計測制御委員会

セキュリティ調査研究WG

社団法人 日本電気計測器工業会

セキュリティの脅威と課題

生産制御システム概要



現実化する脅威

- 生産制御システム（M&CS）のネットワーク化
  - 個々の「島」→　垂直、水平方向へのネットワーク統合。

- 脅威が現実のものになってきている。
  - オーストラリア下水道
    - 元職員による汚水バルブの不正操作
  - オハイオ原発ネットワークダウン
    - ウイルスに感染したことによる
      ネットワーク停止

セキュリティへの脅威

- 第三者の悪意の行為に生じる現象

セキュリティの確保には下記3つの条件をがある。

①機密性

ネットワーク上やコンピュータ内の情報を不適切な人間には決して見せないようにすること

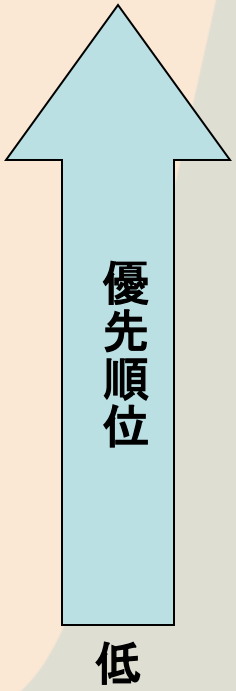
②完全性

ネットワーク上のコンピュータ内の情報が完全な形で保たれ、不正によって改ざんされたり破壊されないこと

③可用性

ネットワーク上のコンピュータ内の情報や資源がいつでも利用できること

セキュリティへの脅威



ITシステム

- **機密性**
- 完全性
- 可用性

●情報の保護が優先

生産制御システム

- **可用性**
- 完全性
- 機密性

●生産の継続が優先

M&CSセキュリティの課題

1. セキュリティパッチ適用時の脅威

Windowsなどの汎用OSや汎用ミドルウェア（データベースなど）を適用している制御システムの課題

1. パッチ適用時にウイルスが混入
2. パッチ適用によるソフトウェアレスポンスの低下、システム停止
3. 古いバージョンのOS等のセキュリティパッチ提供の停止
   （サポート期間が短い）

2. リムーバブルメディア利用による脅威

USBメモリやCD－R、DVD－Rなどのリムーバブルメディアの普及により、管理コンソールやオペレータコンソール（HMI）でメディアを利用する場合の課題

1. メディアからのウイルス感染
2. メディアを紛失することによる機密情報漏洩

M&CSセキュリティの課題

3. リモートメンテナンス時の脅威

インターネット回線等を利用するリモート監視システムの増加により、システム外部のコールセンターやリモート保守機器から保守を行う場合の脅威。

1. インターネット回線からの攻撃やウイルス感染

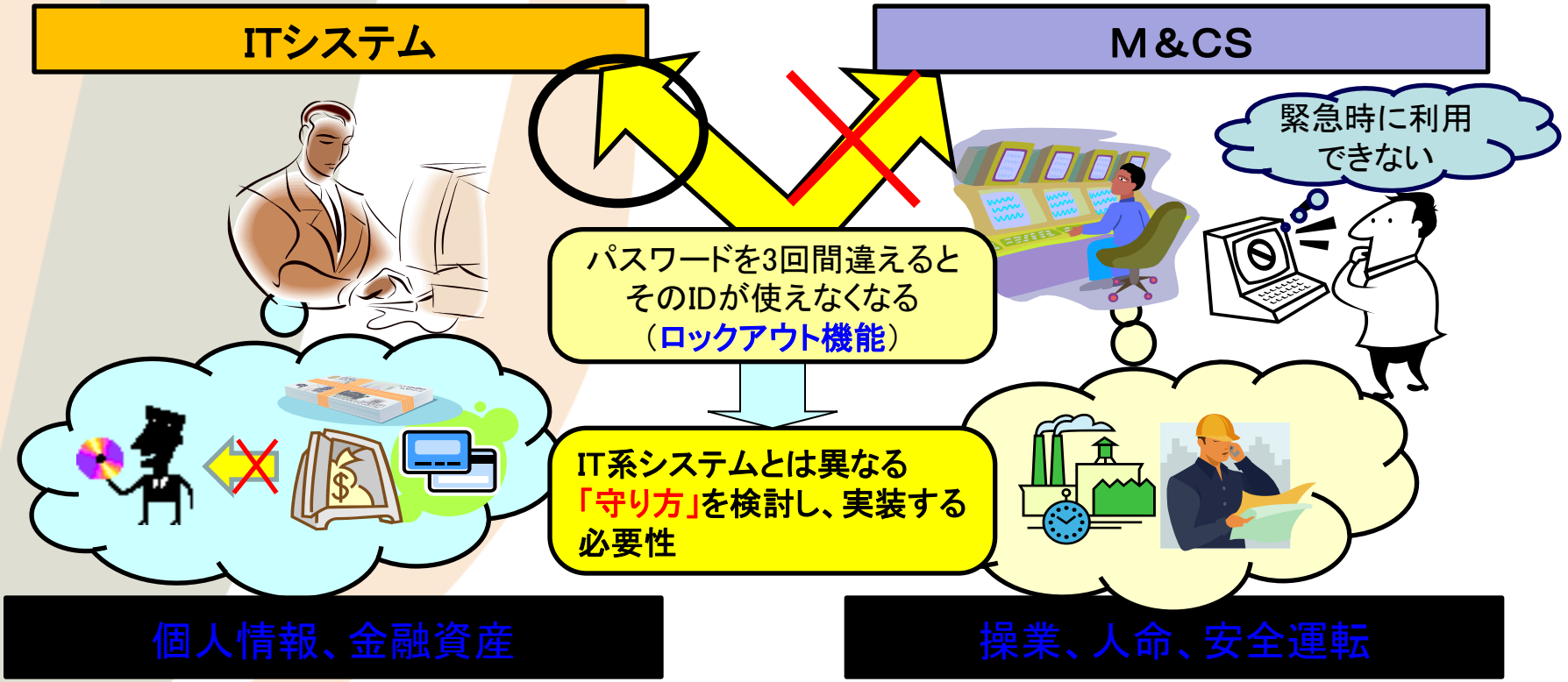
4. メンテナンス用機器など、新たな機器の接続による脅威

機器の増設やメンテナンス目的でシステム設計時に計画していなかった新たな機器を制御システムに接続するときに発生する脅威

1. 機器からのウイルス感染
2. 機器接続によるシステム構成異常

ITセキュリティとM&CSセキュリティ

● ユーザ認証

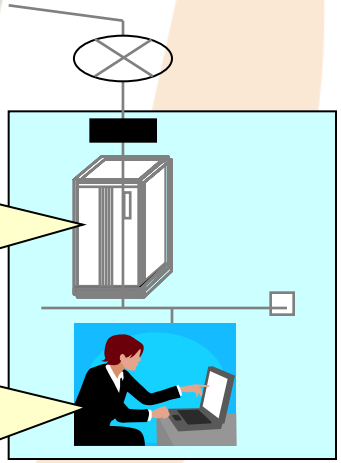


守るべき資産の違い

ITセキュリティとM&CSセキュリティ

●ウイルス対策

ITシステム

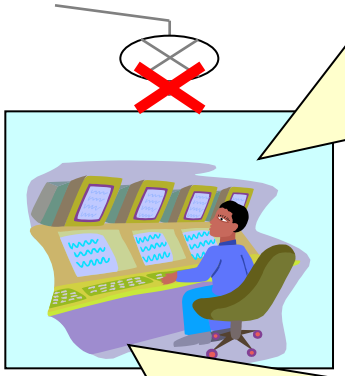


インターネットやイントラネットのパターン更新サーバと接続されている

ウイルス対策、管理されている保守用PCからネットワークを使用して保守を実施

常に高いセキュリティ対策レベルでの運用が可能

M&CS



孤立したネットワーク環境であるため、パターン更新などのセキュリティ対策は保守メンテ時にオフラインで実施。

（リアルタイムに最新パターンへ更新できない）

パッチ適用やモジュール更新は、USBメモリなどを利用してオフラインで実施する。

（紛失、ウイルス混入の危険性）

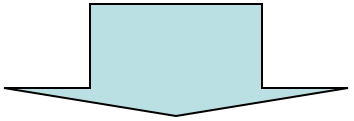
最新パターンで対策がされていない状態でのリムーバブル利用など、運用上考慮すべき課題が多い

ITセキュリティとM&CSセキュリティ

	内　容	IT 系 シ ス テ ム	M&CS シ ス テ ム
1	性能要件	応答性能よりもスループットが要求される。	応答性能が重要。遅延は重大問題。
2	可用性	運用上必要であればシステムの再起動が許容。	システムの再起動は許されない場合が多い。
3	即時性	即時性を要求する緊急処置は少ない。	緊急処置に対する人間の操作を妨げてはならない。
4	ライフタイム	システム、機器のライフタイムは3-5年が中心。	15-20年と長い。
5	守るべき資産	IT資産および情報を第一に保護している。	制御に直接関係する端末装置（プロセス制御装置のようなフィールド装置）を第一に保護。
6	システム運用	汎用OSを用いて設計されており、アップデートは自動化された仕組を利用でき容易である。	独自OSが多く、アップデートの自動化の仕組みが出来ていない。
7	リソース（メモリやディスク容量）	セキュリティ対策などのために、システムは十分なリソースを持っていることが一般的である。	最小メモリやその他リソースで生産プロセスを支援するように設計されており、セキュリティ機能もその範囲内で追加されている。
8	通信	ワイヤレスも含め、標準的な通信プロトコルが使用される。	標準プロトコルの他に専用プロトコル、通信設備が含まれるため、ネットワークは複雑となり、専門の技術者が必要。
9	サポート	機器メーカーによる様々な支援体制がある。	サービスサポートは通常1ベンダーによる。
10	**危機管理**	**データ機密性及び完全性を第一に管理する。**	**人、環境の安全性が第一、次がプロセスの保護である。**

セキュリティへの対応

- 制御システムもオープン化が進み、ウイルス感染や外部からの侵入による情報漏洩など、IT系システムと同様の**セキュリティ脅威**にさらされることが多くなっている
- 制御システムは**安全な運転とシステムの継続稼動を最優先**に運用管理しなければならないため、IT系システムと同じセキュリティ対策をそのまま実施することは、システム運用の妨げになる場合がある



制御システムとしてのセキュリティ標準化が必要

標準化動向

2つの視点

マネージメント視点

- セキュリティ管理システム仕様
- 最適慣例集
  - 実施例の一覧

コンポーネント視点

- コンポーネントの情報セキュリティ機能評価基盤
  - セキュリティ機能要件定義
  - 評価・認証システムのフレームワーク

ITセキュリティ ―― 標準

マネージメント視点

- ISO/IEC 27001 情報セキュリティマネジメントシステム－要求事項
- ISO/IEC 27002 情報セキュリティマネジメント実践のための規範
  （旧 BS7799）

以下予定。

- ISO/IEC27003　情報セキュリティマネジメント実践の手引
- ISO/IEC27004　情報セキュリティマネジメントの測定
- ISO/IEC27005　情報セキュリティリスクマネジメント

コンポーネント視点

- ISO/IEC 15408: Information technology － Security techniques － Evaluation criteria for IT security
  （CC:Common Criteria）

M&CS セキュリティ---- 標準

マネージメント視点

- **ISA-SP99** (M&CSセキュリティ)
- IEC/TC65/WG10
  (Industrial Process Measurement and Control – Net & System Security)

コンポーネント視点

- **PCSRF** (Process Control Security Requirements Forum)
  - SPP-ICS
    (System Protection Profile – Industrial Control System)

JEMIMA Japan Electric Measuring Instruments Manufacturers' Association

PART 2

制御システムのセキュリティ規格とセキュリティ俯瞰MAP

2008.11.26

PA･FA計測制御委員会

（セキュリティ調査研究WG）

社団法人 日本電気計測器工業会

●制御システムのセキュリティ規格

2つの視点

マネージメント視点

- セキュリティ管理システム仕様
- 最適慣例集
  - 実施例の一覧

コンポーネント視点

- コンポーネントの情報セキュリティ機能評価基盤
  - セキュリティ機能要件定義
  - 評価・認証システムのフレームワーク

ITセキュリティの場合

マネージメント視点

- ISO/IEC 27001 情報セキュリティマネジメントシステム(ISMS)要求事項
- ISO/IEC 27002 ISMS 実践のための規範
- ISO/IEC 27006 認証/登録プロセスの要求仕様(2007年3月)

  以下予定。
  - ISO/IEC27000 ISMS規格についての基本用語集
  - ISO/IEC27003 ISMS実践ガイド
  - ISO/IEC27004 情報セキュリティの測定
  - ISO/IEC27005 情報セキュリティのリスクマネジメント
  - ISO/IEC27007 ISMS監査の指針

コンポーネント視点

- ISO/IEC 15408: Information technology − Security techniques − Evaluation criteria for IT security
  (CC:Common Criteria)

M&CSセキュリティの場合

マネージメント視点

- ISA-SP99（M&CSセキュリティ）
- IEC/TC65/WG10

  Industrial Process Measurement and Control – Net & System Security

コンポーネント視点

- PCSRF (Process Control Security Requirements Forum)
  - SPP-ICS

    (System Protection Profile - Industrial Control System)

ISA－SP99

- 名称
  - “Manufacturing and Control Systems Security”
- 目的
  - Manufacturing and Control Systems(以下M&CS)への電子的侵入を防ぐための指針を確立すること
- 参加メンバー
  - システムインテグレータ/コンサルタントが中心にリードしている
  - エンドユーザも参加しており，一部のメンバーはTRの執筆に大きく貢献
  - システムベンダーも一通り参加
- 活動内容
  - TR (Technical Report) を発行(2004年)　2007年改定版発行
    - ISA TR99.00.01: Security Technologies for Manufacturing and Control Systems (TR1)
    - ISA TR99.00.02: Integrating Electronic Security into the Manufacturing and Control Systems Environment (TR2)

ISA－SP99 策定中の標準

- Part 1: Scope, Concepts, Models and Terminology
  - 2007年発行
  - 言葉やモデルの定義
  - Part 2以下の基礎となる共通の理解をまとめる
- 策定中
  - Part 2: Establishing an Industrial Automation and Control System Security Program
    - 2007年10月 委員会内で投票
    - M&CS情報セキュリティのビジネスケースを確立
    - 情報セキュリティ管理に必要な活動を挙げ，その詳細を記述
- 策定予定
  - Part 3: Operating an Industrial Automation and Control Systems Security Program
  - Part 4: Specific Security Requirements for Industrial Automation and Control

IEC/TS 62443

- 2009年～2010年規格化決定
  （2008年5月のTC65東京会議にて決定）

- IEC/TS62443—1, Part1
  - Terminology, concepts and models

- IEC/TS62443—2, Part 2
  - Establishing an industrial automation and control system security program

- IEC/TS62443—3, Part 3
  - Operating an industrial automation and control system program

- IEC/TS62443—4, Part 4
  - Specific security requirements for industrial automation and control system

- IEC/TS62443—5, Part 5 (SP99 TR1)
  - Security technologies for industrial automation and control system

PCSRF

- 名称
  - Process Control Security Requirements Forum（発音: Pic-Surf）
- 位置付け
  - 米国商務省標準技術局:NIST（National Institute of Standards and Technology）の下部組織
- 目的
  - 産業用プロセス制御システム向けの情報セキュリティ要件を定義および適用することで，これらのシステムのセキュリティを強化すること。
  - ベースとして，ISO15408（Common Criteria for IT Security Evaluation）
- メンバー
  - 401の組織，32カ国(2008年10月現在)
  - 制御機器ベンダ(Rockwell, Honeywell,…)，ITベンダ(Cisco, SUN, …)，ユーザ(Exxon Mobil, BP, Dupont, …)，コンサルタント(KEMA, …)，公的機関(NSA, 経産省，…)

PCSRFの活動

- SCP (Security Capabilities Profile)
  - 脆弱性の解析を含めた制御システムのアーキテクチャの分析
  - 安全な制御システムに求められる機能を列挙
  - プロセス制御機器に今後求められるセキュリティ機能を，システムやコンポーネントのベンダに要求する手段とする
  - SPP-ICS作成の基礎とする

- SPP-ICS (System Protection Profile – Industrial Control System) の作成
  - ISO 15408 のPP (Protection Profile)をシステム向けに拡張
  - 下記のベース
    - より特定されたシステム(SCADA, DCSなど)のPP
    - 具体的な制御システムのSST (System Security Target)の基礎
    - 各コンポーネント(コントローラの認証，センサの認証，など)のPP

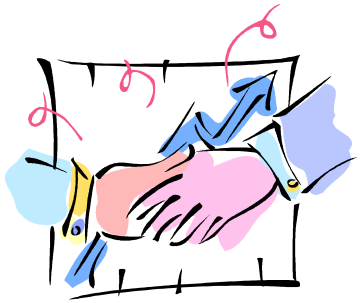
●制御システムセキュリティ俯瞰MAP

セキュリティ規格利用における課題

- 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
    - 分野ごとに独自に作成され、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、どれが自分の目的に合致しているか判断できない
  - 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稼働中のシステムの運用時にやらなければならない事が不明
    - セキュリティに関する専門用語が難しい

解決策

- 利用者が、自身が必要な分野・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MAPを作成する



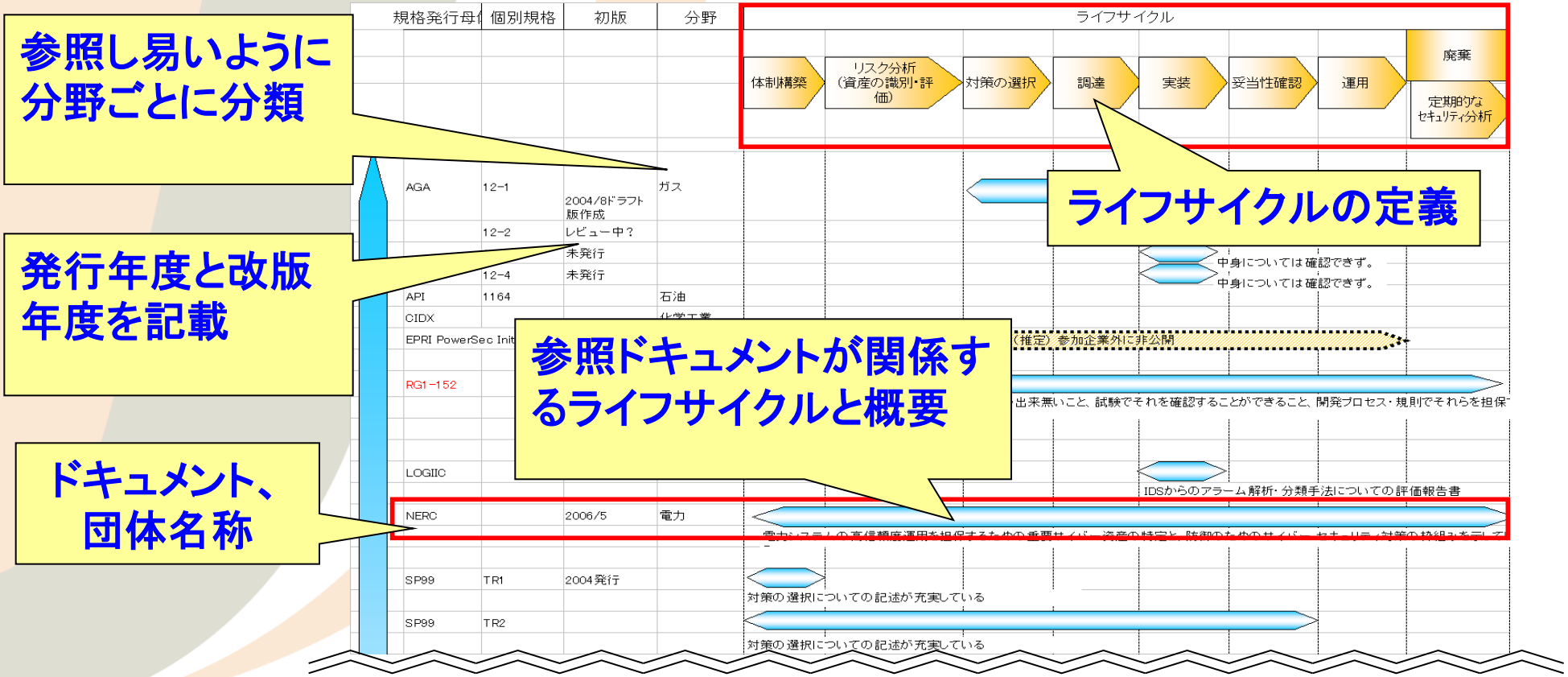
- 「制御システムセキュリティ俯瞰MAP」ドキュメント構成
  - 制御システムセキュリティ規格俯瞰MAP
  - 制御システムセキュリティ規格要約
  - 制御システムセキュリティ規格相関図

俯瞰MAPの特長

- 各分野ごと（電力、ガス・石油）で取り組まれているセキュリティ規格、団体活動を整理
- 作成年度、更新年度を記載
  - 規格としての**「鮮度」**が重要
- 要約
  - 簡単に内容を理解できるように
- **システムのライフサイクル**に合わせて記載
  - 現在自分が担当している業務のフェーズから参照すべき規格が逆引きできる
- 情報系規格との関連を記載

俯瞰MAPのレイアウト

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



セキュリティ規格の要約

- 1つの規格について1ページで要約されている
  - 策定団体、メンバー企業
  - 対象分野
  - 内容
  - 策定団体やドキュメントの参照URL
  - 発行年月日（ドラフト/初版/改版など）
    - 発行日や改訂状況などから**規格としての鮮度**を把握する
  - 対応するJIS規格

セキュリティ規格の要約

●要約例

SP800-42 “Guideline on Network Security Testing"

▪ **策定団体**：

アメリカ国立標準技術研究所(National Institute of Standards and Technology, NIST)

http://www.nist.gov/

▪ **内容**：

ネットワークセキュリティの検査ガイドライン。

効果的なセキュリティテストプログラムの必要性を解説。目的は次の通り。

(1) 最先端システムに存在する脆弱性と実運用のギャップを埋めるため

(2) 組織のセキュリティ運用を理解，調整，記録するため

(3) 組織の取り組みを改善するため

セキュリティ開発ライフサイクルにおいて，実装と，妥当性検証，運用，定期的な監査に適用される。

▪ **発行年月日**：

NIST Special Publication 800-42

Guideline on Network Security Testing

初版：2003 年 10 月

▪ **URL**：

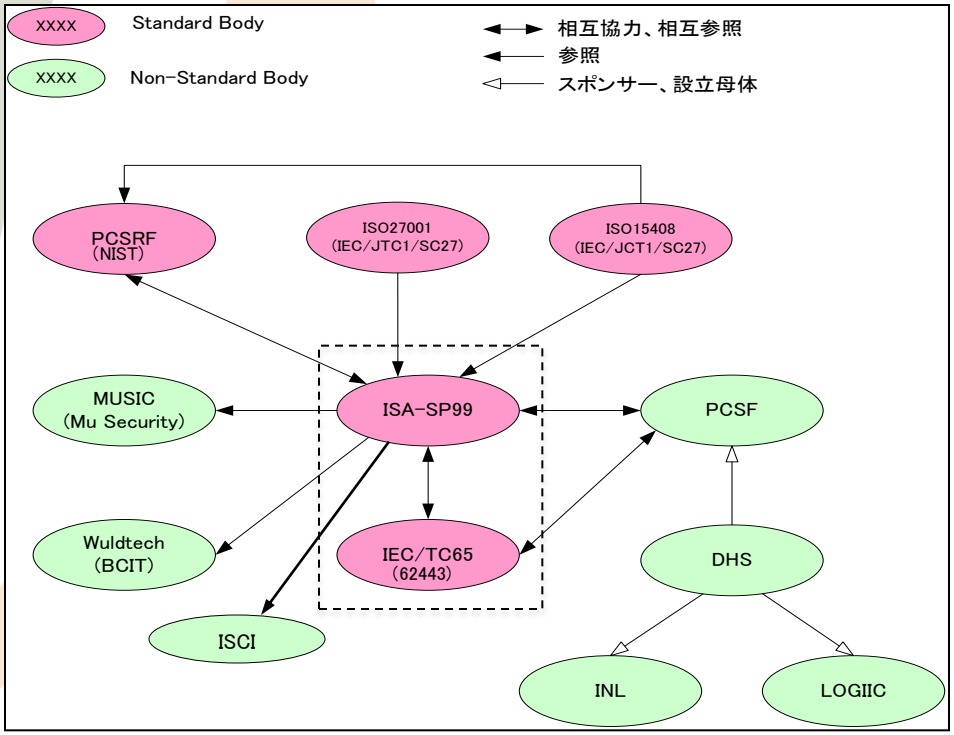
http://csrc.nist.gov/publications/PubsSPs.html

▪ **対応 JIS 規格**：

なし

セキュリティ規格相関図

- 個々の規格、団体間の相関図
  - 各規格の関係、普及の度合いをわかりやすく整理



配布・提供形態

- 俯瞰MAP、要約、相関図をPDF化して冊子としてまとめる
- JEMIMAのホームページからダウンロード(計画)
  - http://www.jemima.or.jp/

JEMIMA Japan Electric Measuring Instruments Manufacturers' Association

PART 3

セキュリティライフサイクルを意識した対策の立案
~SP99に基づいたセキュリティ対策立案の紹介~
セキュリティ機能要件の分析と役割分担
~NIST SPP-ICSを利用した分析の紹介~

2008.11.26

PA･FA計測制御委員会

セキュリティ調査研究WG

社団法人 日本電気計測器工業会

背景

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どうすれば？

■セキュリティ管理を体系的に実施するには？

JEMIMAセキュリティ調査研究WG

生産制御システム（M＆CS）としてのセキュリティ標準・ガイド

◆マネージメント標準化では　・・・IEC TC65 WG10、ISA SP99、CIDX

◆技術／認証では　・・・NIST／PCSRF

セキュリティマネージメントプログラム構築実践

SP99

2. ISA－SP99とは

目的: 生産制御システム（M＆CS）のためのセキュリティガイド

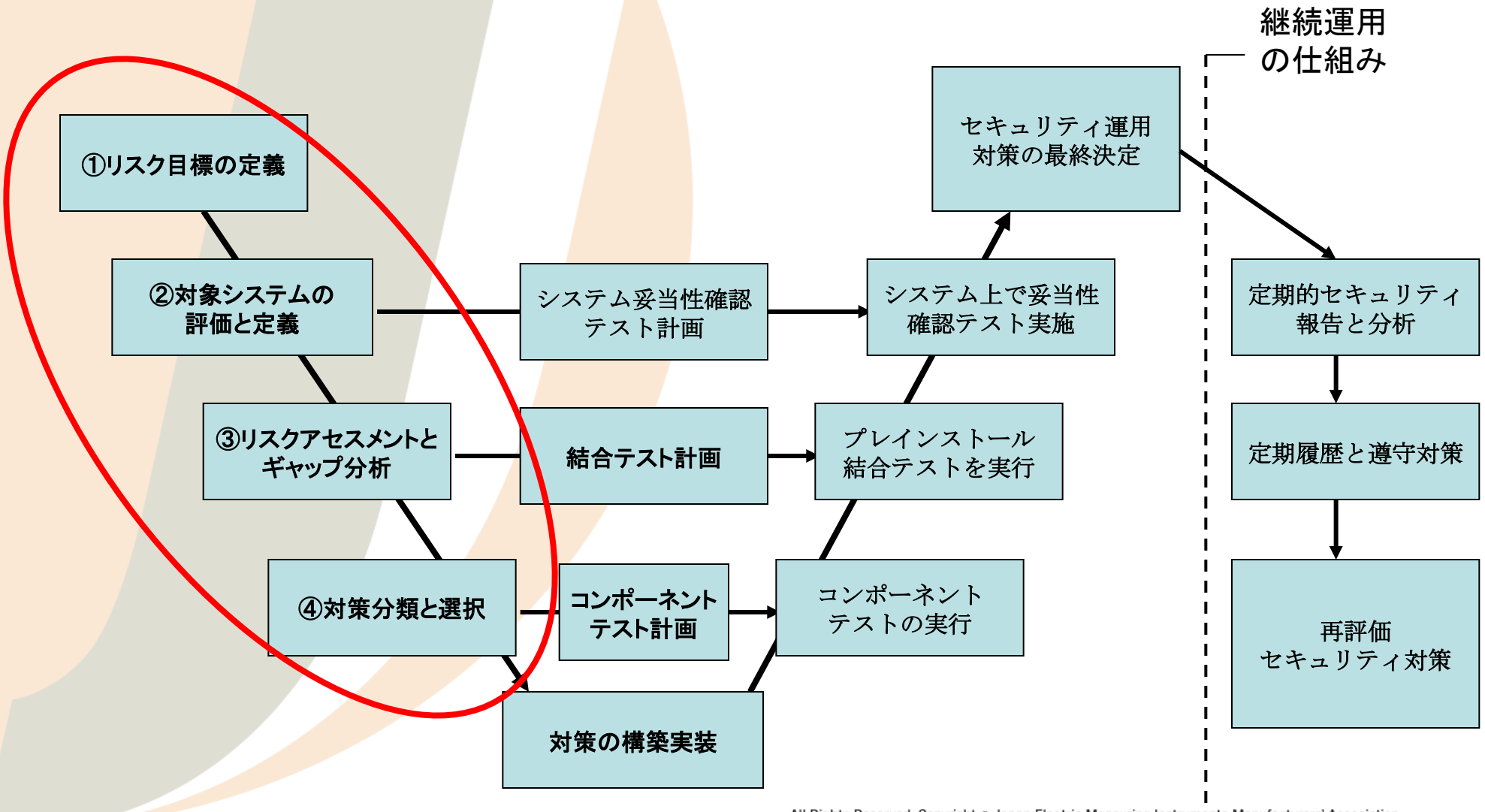
発行:

◆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

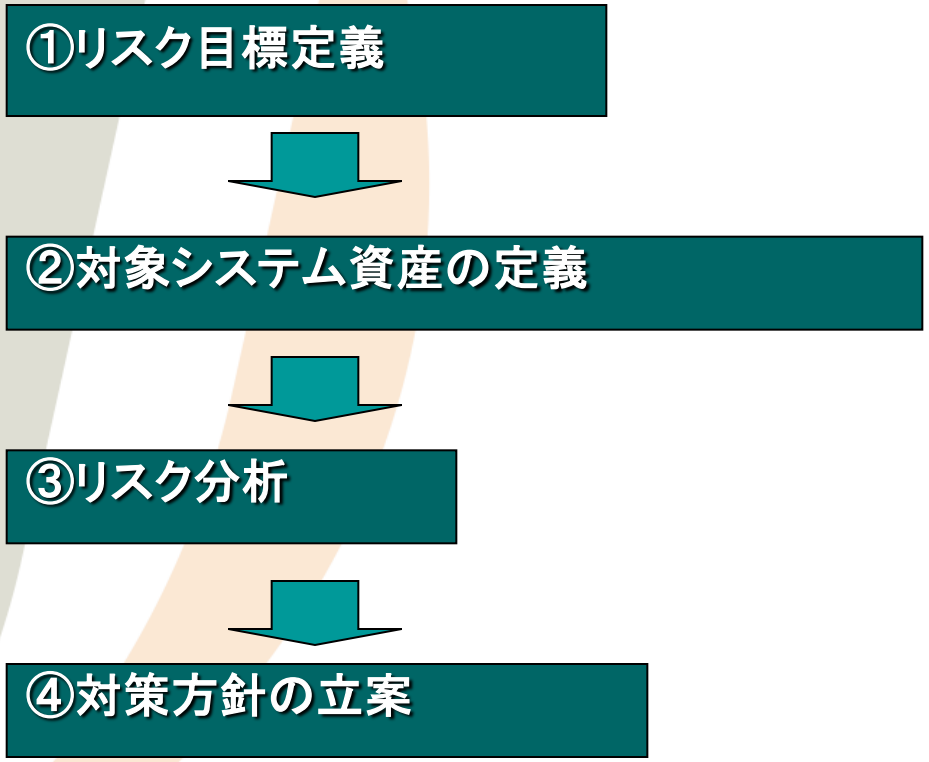
対象:M＆CS（DCS、PLC、SCADA・・）、ネットワークベースの計測、監視および診断システムとその付随するHMI、ネットワークインタフェース、運転・操業支援システムであり、その電子的セキュリテイが対象

3. ISA－SP99セキュリティライフサイクル



設計の手順

4. セキュリティ対策立案までの手順



4. セキュリティ対策立案までの手順－1/4

①リスク目標の定義

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、改ざんあるいは悪意の操作を前提として想定していく。

- プラントの運転全体に直接影響を与え、人命・生活環境に重大な被害
- 一部プラントの運転に影響し、生産・製品に影響（設備、人的被害無し）
- オペレータによるプラントの操作監視を妨害し、運転に支障
- プラントの運転へは直接影響を与えない情報漏洩等

リスクインパクト尺度定義の例

分類＼レベル	インパクト			
	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	殆ど影響なし
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	殆ど影響なし

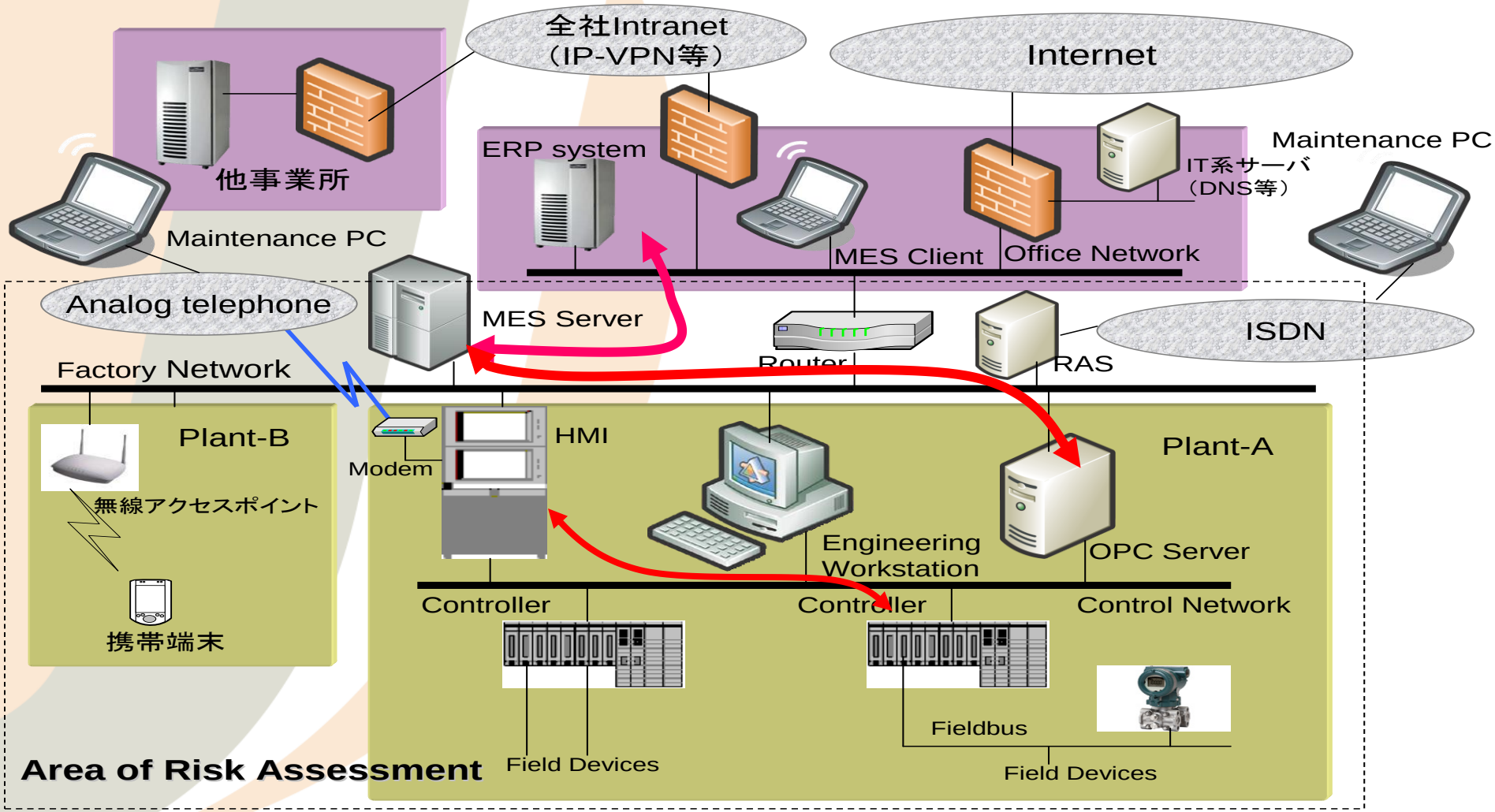
4. セキュリティ対策（管理策）立案の手順－2/4

②対象システム資産の定義

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を漏れなくリストアップ

- ハードウェア
- アプリケーション
- データ

想定モデルシステム



デバイスとデータ資産のリストの例

	FROM	TO	DATA
①	ERP	MES Server	・生産実績 ・KP ・生産スケジュールダウンロード
②	MES Client		・MES server 管理 ・生産実績表示 ・KPI表示
③	RAS		・リモートメンテナンス
④	Engineering WS	HMI	・エンジニアリングデータダウンロード
⑤	Controller		・アラーム通知
⑥	RAS		・リモートメンテナンス
⑦	MODEM		・リモートメンテナンス
⑧	携帯端末		・プロセスデータ収集 ・アラーム収集
⑨	RAS	Engineering WS	・リモートメンテナンス
⑩	MES Server	OPC Server	・プロセスデータ収集 ・プロセスデータ設定 ・アラーム収集
⑪	Engineering WS		・エンジニアリングデータダウンロード
⑫	RAS		・リモートメンテナンス
⑬	HMI	Controller	・プロセスデータ収集 ・プロセスデータ設定 ・アラーム収集
⑭	Engineering WS		・エンジニアリングデータダウンロード

4. セキュリティ対策（管理策）立案の手順－3/4

③リスク分析

■脅威の可能性（Probability）,脅威の重要性（Criticality)の判断基準を設定

■進入経路（Remote , Local等）に関する記述

可能性（Probability）

A：IT系から情報へのアクセス可能かつ不正アクセスの前提となる情報・アクセス

B：上記 「A」 の内、比較的取得が困難な情報・アクセス

C：情報の認識に、制御機器あるいはプラント知識が必要となる情報・アクセス

D：専用OSの専門知識が必要な情報・アクセス

重要性（Criticality）　・・当該資産が、改ざんあるいは悪意の操作を前提

1：バルブ開閉、アクチュエータ操作などプラントの運転に直接影響を与えられる

2：オペレータによるプラントの操作監視を妨害を行える

3：プラントの運転に直接影響を与えない

可能性	重要性
A＝可能性大	1＝損失大
B＝可能性中	2＝損失中程度
C＝可能性小	3＝損失軽微
D＝可能性無し	4＝影響無し

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

脅威の重要性　尺度定義

分類＼レベル	インパクト			
	1	2	3	無し
身体生命への危害	死亡等重大	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	殆ど影響なし
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	殆ど影響なし

デバイスとアプリケーション資産に対する脅威の可能性・重要性の分析

機器	アプリケーション	可能性	重要度	リモート接続	ローカル接続	コメント
MES	生産計画機能	B	2	Yes	Yes	OS:Windows
	KPI機能	B	2	Yes	Yes	OS:Windows
	実績収集・管理機能	B	3	Yes	Yes	OS:Windows
	実績分析機能	B	3	Yes	Yes	OS:Windows
	在庫管理機能	B	3	Yes	Yes	OS:Windows
	ロットトレース機能	B	3	Yes	Yes	OS:Windows
	保全管理機能	B	3	Yes	Yes	OS:Windows
	文書管理機能	B	3	Yes	Yes	OS:Windows
RAS	リモートメンテナンス	B	3	Yes	Yes	OS:Windows
	リモートエンジニアリング	B	3	Yes	Yes	OS:Windows
Router	ルーティング機能	A	2	Yes	Yes	OS:Windows
	経路情報設定機能	A	3	Yes	Yes	OS:Windows
OPC	プロセスデータアクセス	B	3	Yes	Yes	OS:Windows
	アラームイベント	B	3	Yes	Yes	OS:Windows

4. セキュリティ対策（管理策）立案の手順－4/4

④対策方針の立案

リスク分析結果から対策の方針を導き出します。
このとき、次のような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。

■緩和策（Mitigation）：停止時間を減少させる為のバックアップ、レイドおよびデータ暗号化など 、ネットワーク切り離し

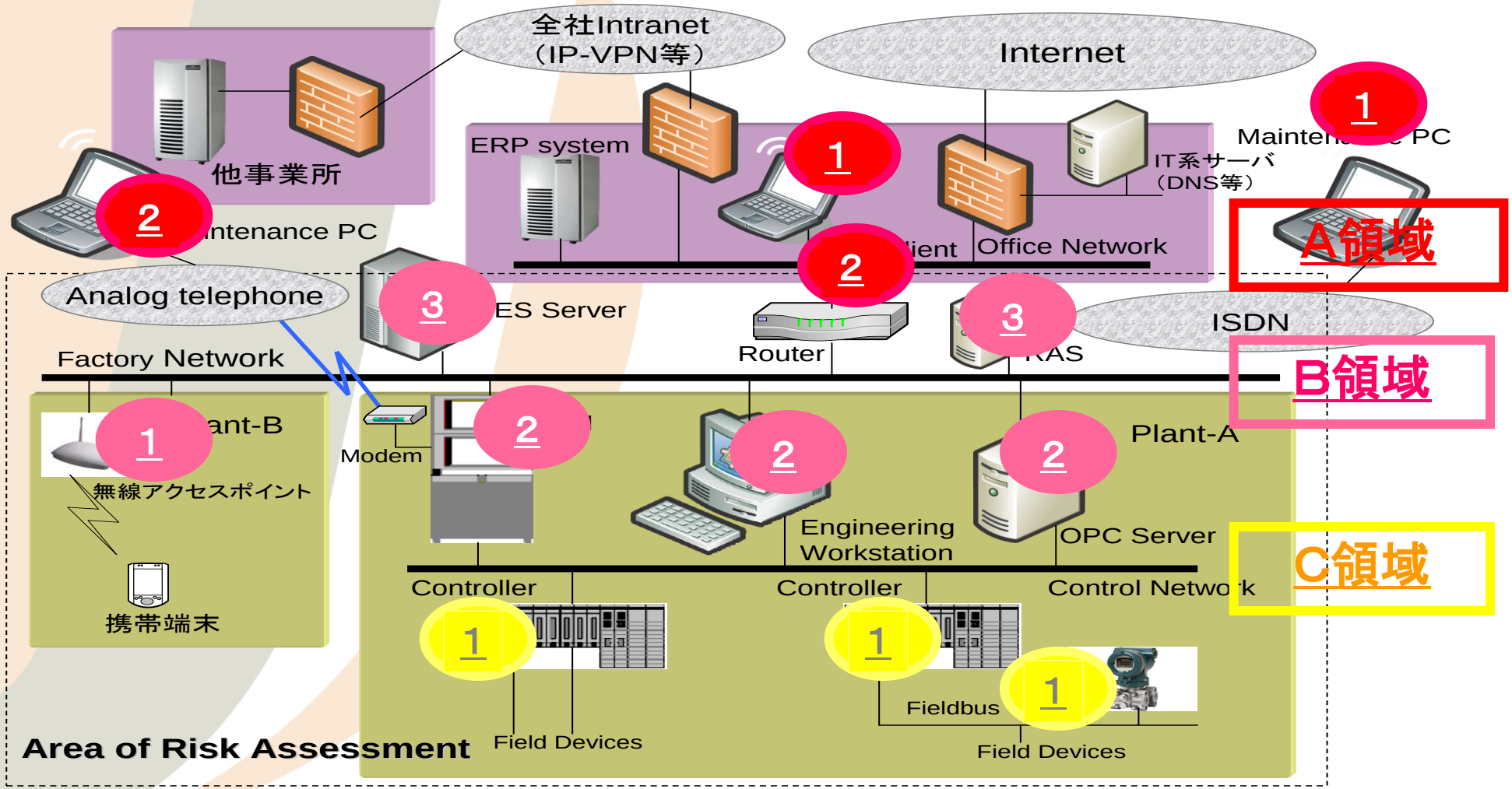
■防御策（Access control）：機器やサービス、ユーザ認証などの利用制限

■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

アプリケーション、デバイス資産に対する戦略マトリックス

脅威の可能性	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
	A	防御策 必須	防御策 必須	防御策 必須	
	B	防御策 必須	防御策 必須	防御策 任意	
	C	防御策 必須	防御策 必須	防御策 任意	
	D	防御策 任意			

デバイス資産トポロジーの例



対策案の具体例

■ 緩和策（Mitigation）

・データのRAID(レイド)を導入

・データの暗号化

■ 防御策（Access control）

・Factory NetworkとOffice Networkの間にFirewallを設置

・DMZを設置しデータ交換をはかる

・無線アクセスポイント環境にAESなどの対策を導入

■ 検出策（Detection）

・FirewallやRASのアクセスログを監視

・MESサーバへアンチウィルスソフトを適用、感染の検知、防止

・IDS／IPSの設置

まとめ

5. 設計方針まとめ

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。

■資産への重要性レベル

■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

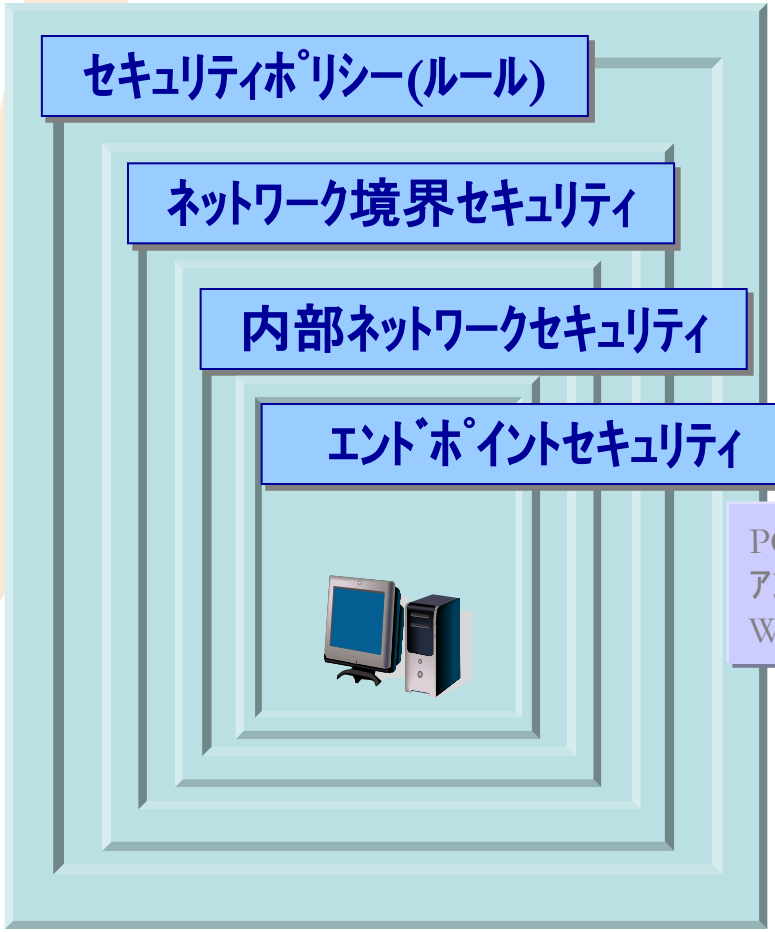
SPP－ICS

完璧なセキュリティ対策を行うために

多層防御
Defense-in-depth

幾層もの防御壁で、技術、環境、使用方法などによる複数の対策によって重要なシステムに対して直接攻撃や情報漏洩を退ける考え

多層防御はセキュリティに対する違反を防ぐだけではなく、攻撃を見つけ対応するための時間を稼ぎます。これにより、違反の影響を軽減します。



ファイヤーウォール・ルータなどによるネットワークセグメント分割

IDS不正侵入検知システム
IPS不正侵入防御システム

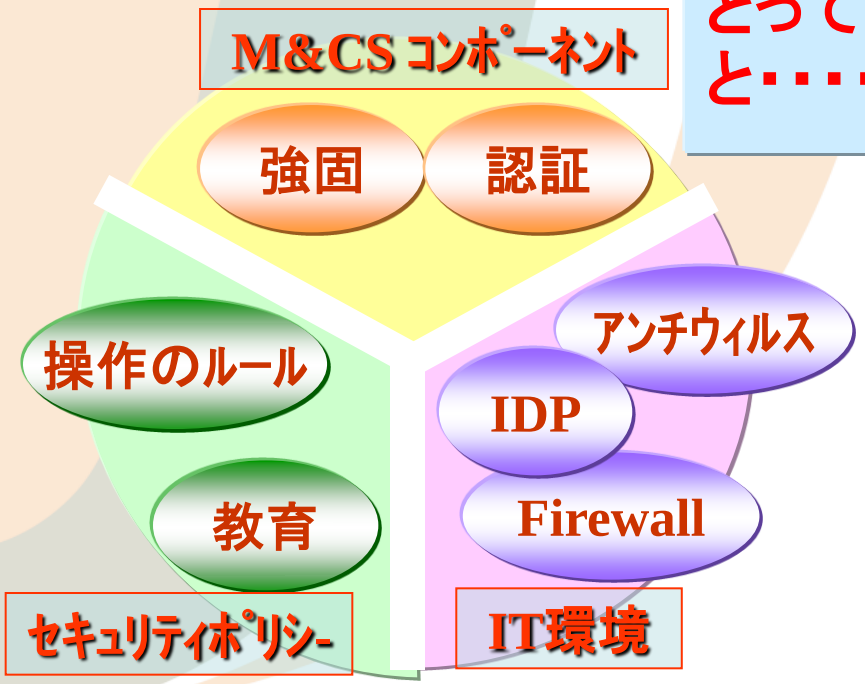
PC等の強化
アンチウィルスソフト
Windows等へのセキュリティパッチ

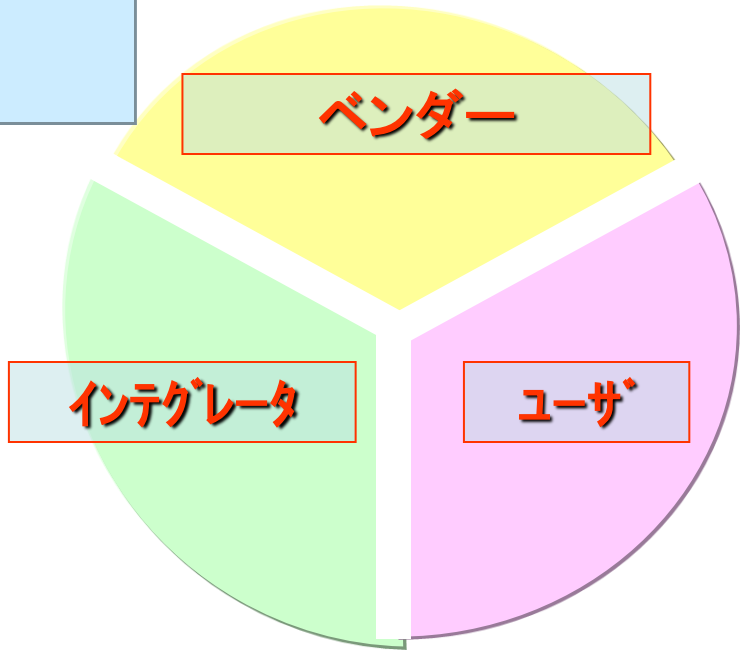
2つのギャップを考える

機能分担
から見たギャップ

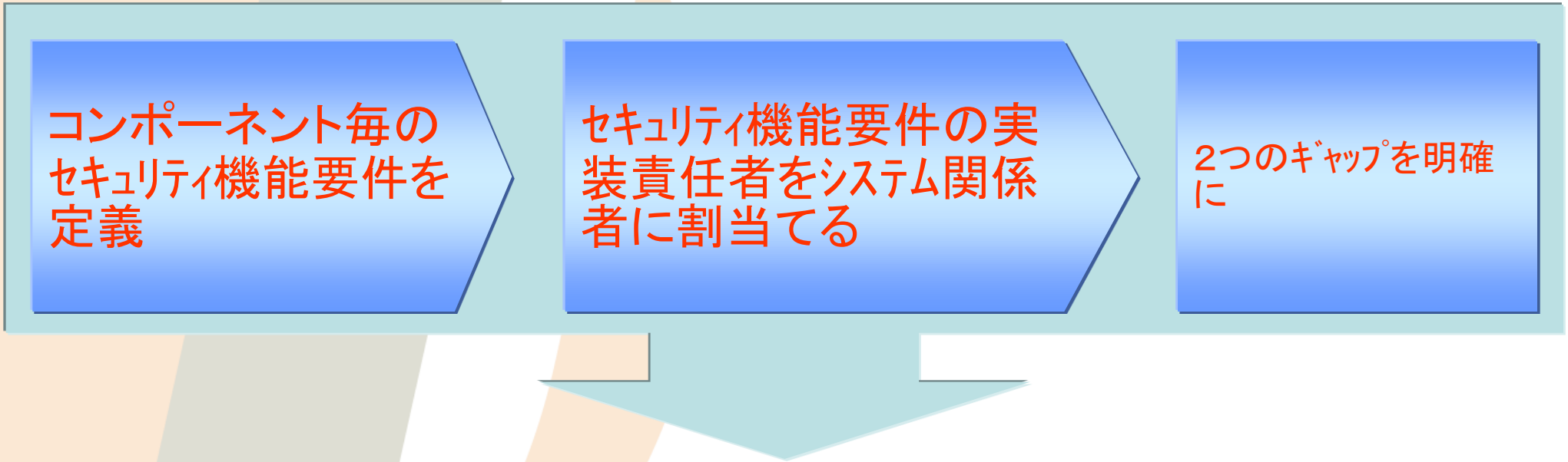
役割分担
から見たギャップ

このGAPを広げたままセキュリティ対策をとっていく・・
と・・・・・・・・・・





2つのｷﾞｬｯﾌﾟを埋めるために



- SPP-ICS (System Protection Profile – Industrial Control System)
  - ISO15408のPP(Protection Profile)をM&CS向けに拡張したもの
  - M&CSのためのセキュリティ要件のセット

JEMIMA セキュリティ調査・研究WGでは
SPP-ICSを使い、
セキュリティ機能要件の分析と役割分担
を実践しました。

実践した全体概要

モデルケースを抽出

考えられるシステム構成を抽出
- ｽﾀﾝﾄﾞｱﾛﾝﾀｲﾌﾟ
- 水平接続ﾀｲﾌﾟ⇒他社間接続
- 垂直接続ﾀｲﾌﾟ⇒製造実行系接続
- リモート監視

セキュリティ機能要件の分析

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

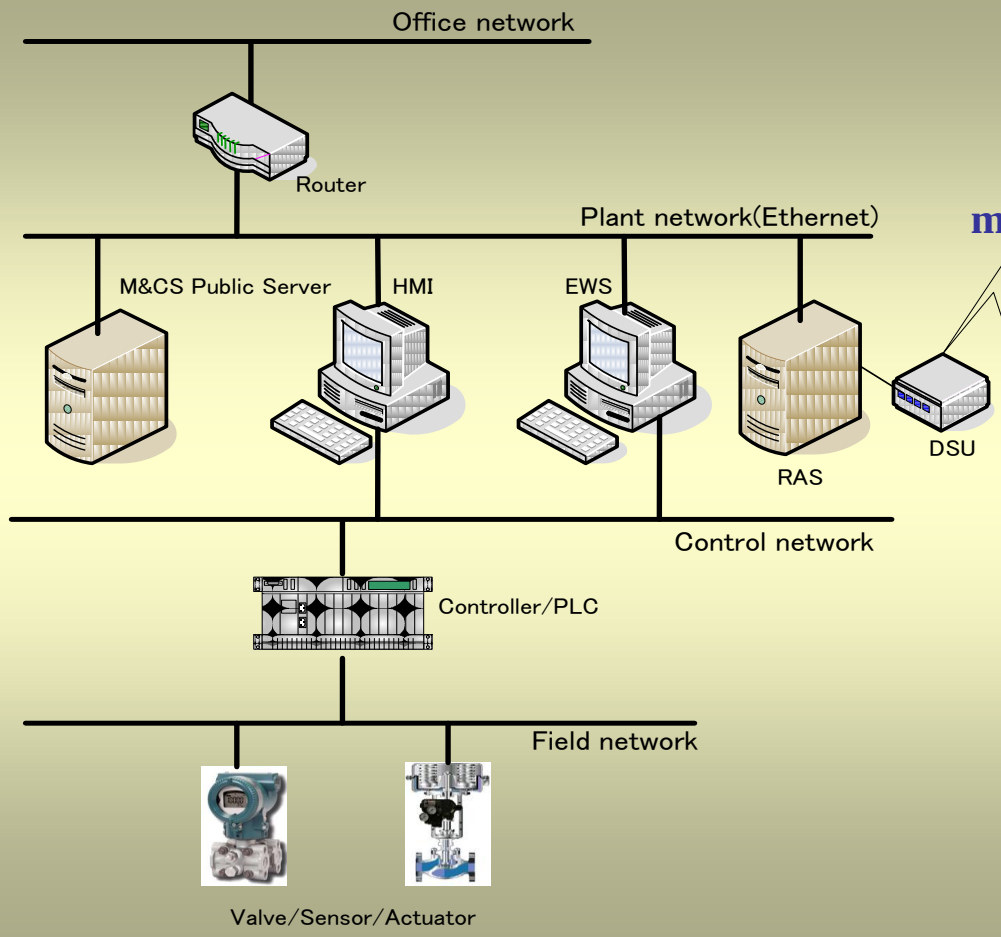
PCSRF SPP-ICS Ver1.0を利用
- 抽出したモデルケースそれぞれでから脅威を分析
- セキュリティ機能要件を抽出

機能・役割の分担

機器・人の役割を明確化
- M&CSの構成機器
- IT機器
- 非IT系
- 関連者（ﾕｰｻﾞ・ﾍﾞﾝﾀﾞ・ｲﾝﾃｸﾞﾚｰﾀ）の役割分担

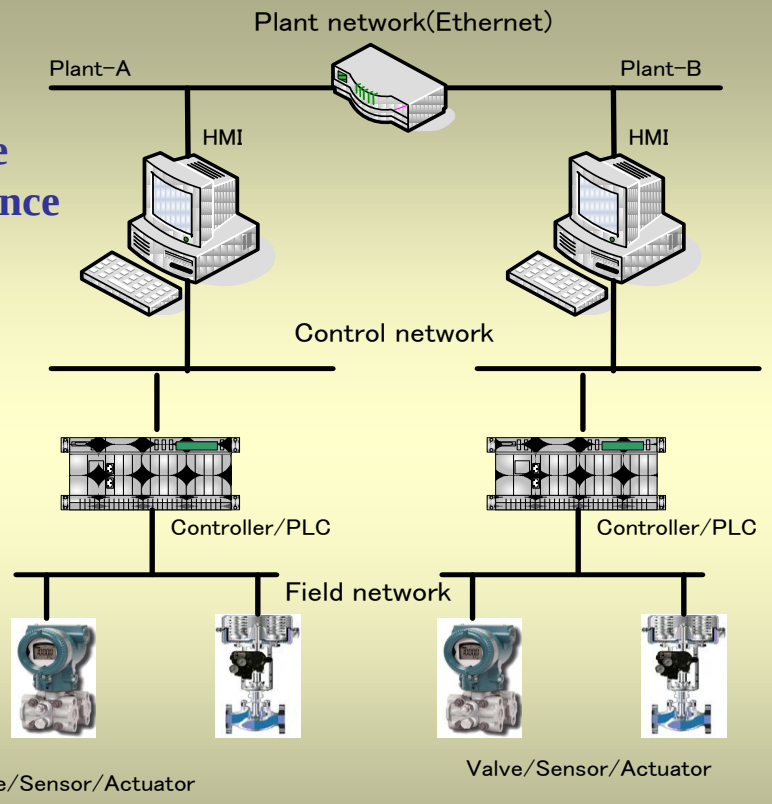
実践に使用したモデルシステム

垂直構造



Remote maintenance

水平構造



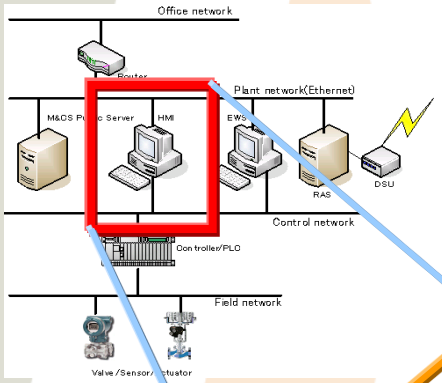
機能要件の分析

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の分析



- 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**を確定していく。

脅威
SPP-ICSで定義されている

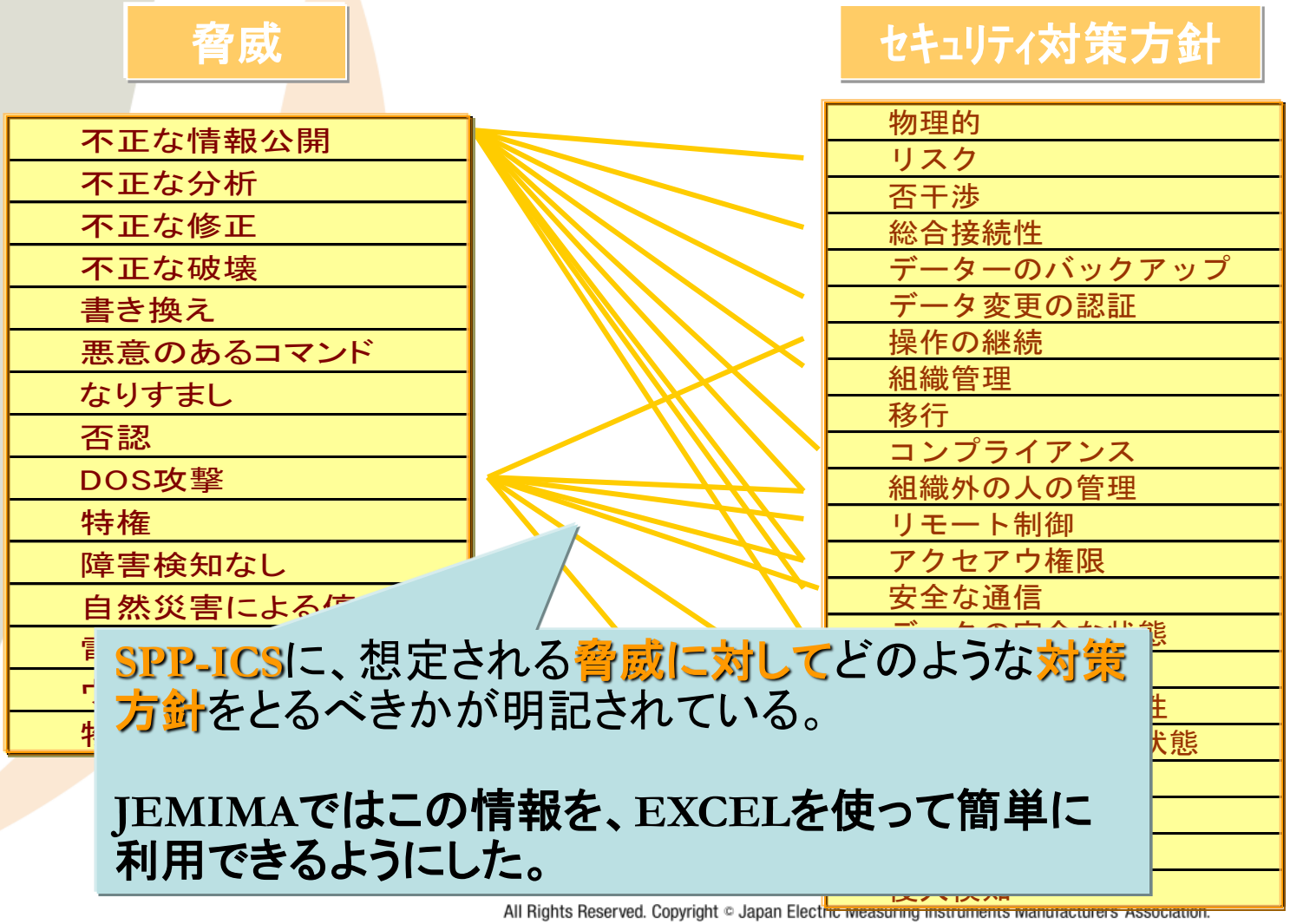
機能要件の分析

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
の分析



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。

JEMIMA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。

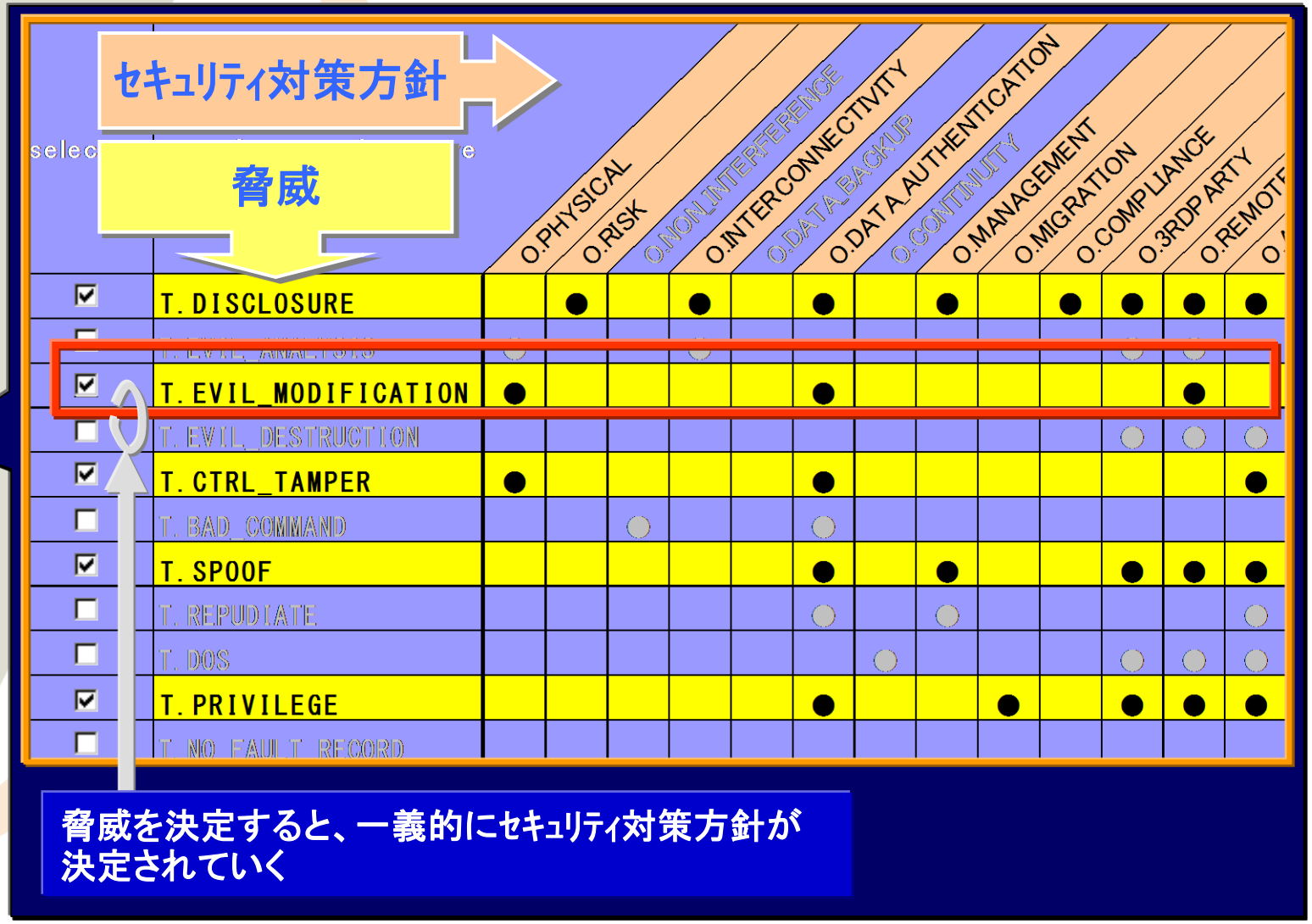
機能要件の分析

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
の分析



機能要件の分析

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

セキュリティ対策方針

- 物理的
- リスク
- 否干渉
- 総合接続性
- データーのバックアップ
- データ変更の認証
- 操作の継続
- 組織管理
- 移行
- コンプライアンス
- 組織外の人の管理
- リモート制御
- アクセアウ権限
- 安全な通信
- データ
- 機密性
- 操作に
- システ
- システ
- 不正監
- 監査
- 侵入検知

セキュリティ機能要件

機能要件	説明
FPT_PHP.1	物理的攻撃の検出
FPT_PHP.2	物理的攻撃への通知
FPT_PHP.3	物理的攻撃への抵抗
FPT_PHP.4	ドメインと物理的な境界線を明確に、ドメインごとのセキュリティポリシーを確定すること
FPT_RCV.2	自動回復
FPT_RCV.3	損失のない自動回復
FPT_RCV.4	機能回復
FPT_RCV.5	障害時、機能を削減してからの継続運転。
FPT_RPL.1	リプレー検出
FPT_STM.1	スタンプの利用が出来ること。

SPP-ICSに、想定される**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。

JEMIMA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。

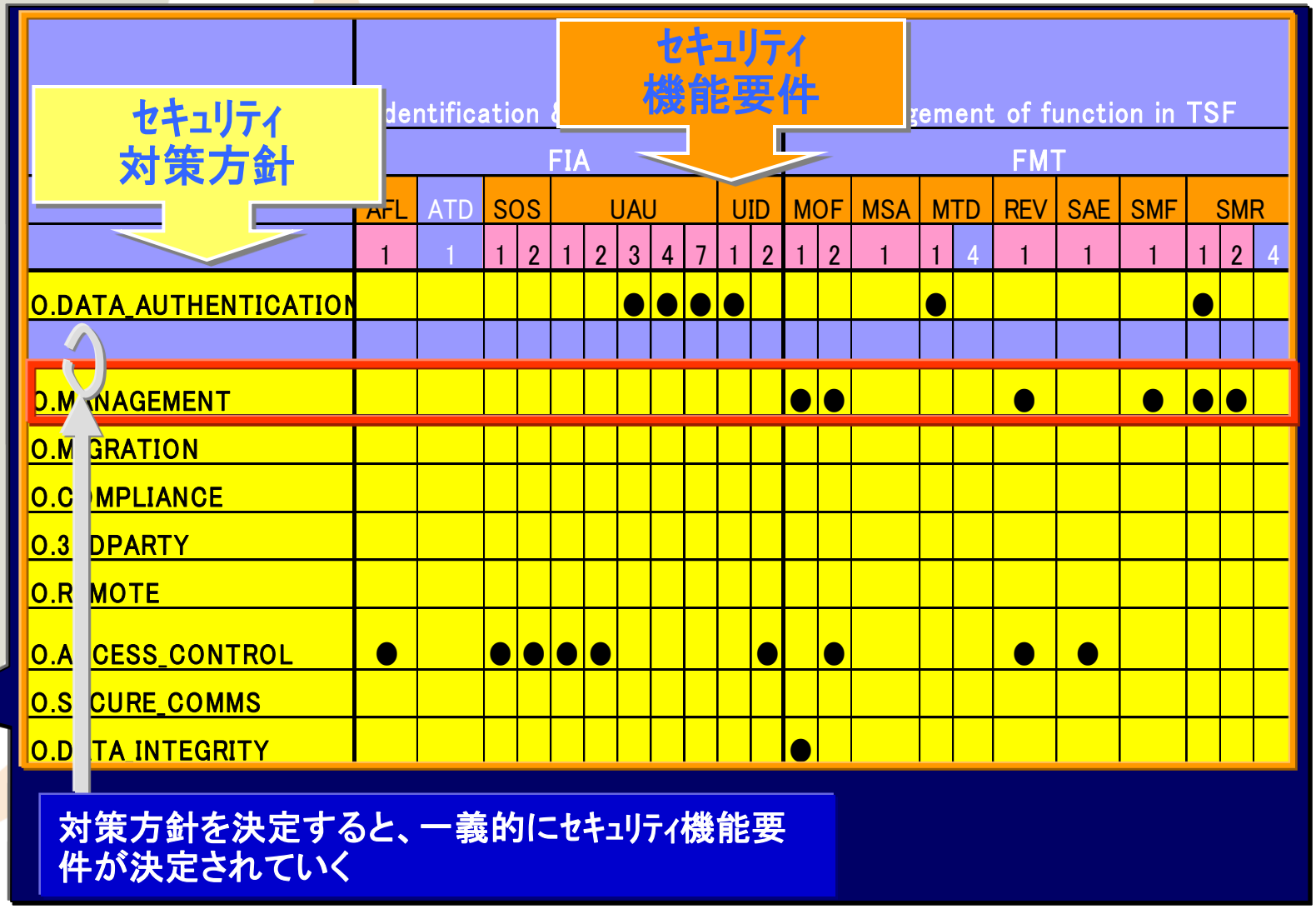
機能要件の分析

セキュリティ機能要件を導き出す

脅威を
確定する

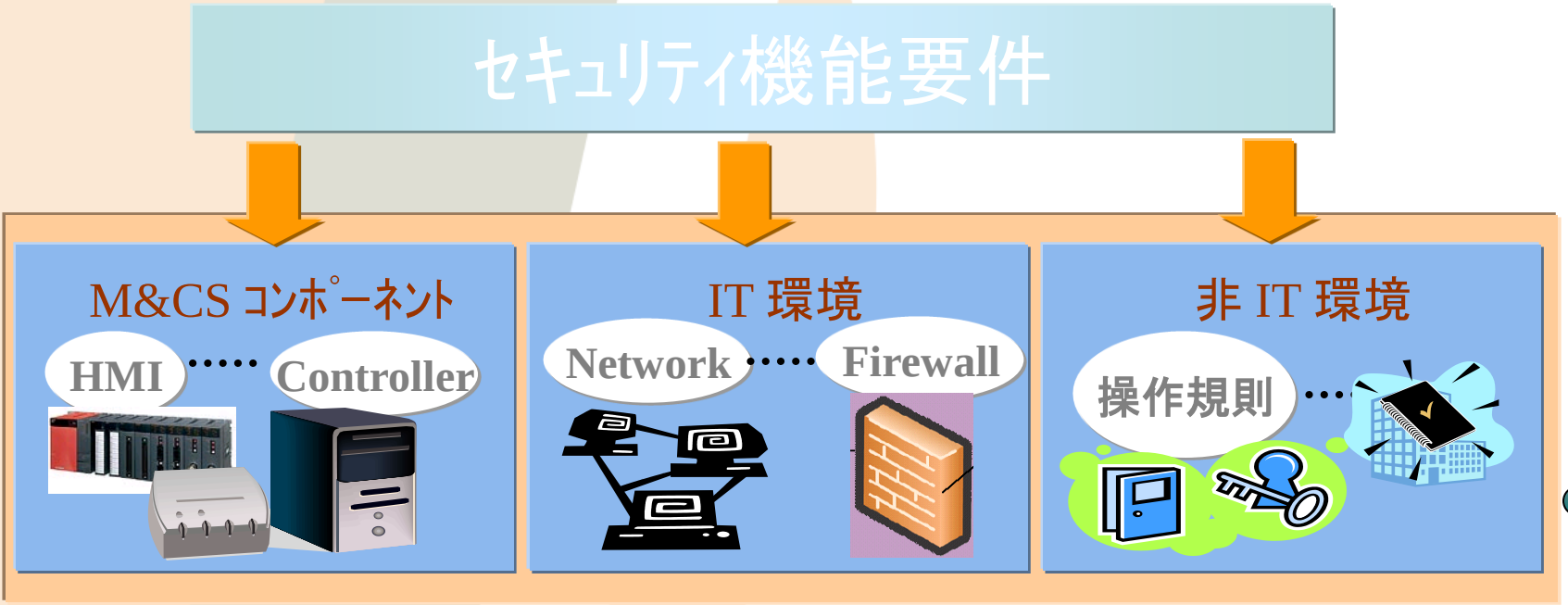
セキュリティ対策方針
を決める

セキュリティ
機能要件
の分析



機能要件の分析

セキュリティ機能要件から分担を決める



機能map

機能Mapを作る

セキュリティ
機能要件

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
FDP_ETC.1	When the user data is exported to outside, access can be properly restricted.	V			
FPT_PHP.1	Detect the physical attacks.	V	V		
FPT_PHP.2	Notification to the physical attacks.	V	V		
FPT_RCV.2	Automatic recovery.		V		
FPT_RPL.1	Detect the replay.		V	V	

機能map

機能要件の分析

セキュリティ機能要件から分担を決める

セキュリティ機能要件

M&CS コンポーネント

HMI …… Controller

IT 環境

Network …… Firewall

非 IT 環境

操作規則 ……

機能map

ユーザ

ｲﾝﾃｸﾞﾚｰﾀ

制御機器ﾍﾞﾝﾀﾞ

役割map

役割Mapを作る

セキュリティ
機能要件

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	

役割map

結果

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	To be a violation of the policy can be audited corresponding to the set rule	V		V (Firewall)	
FAU_SAR.1	To audit information can be provided in an appropriate way for those engaged in the audit	V		V (Firewall)	
FDP_ACC.1	Operations 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, controls can be properly restricted	V			
FPT_PHP.1	Detect the physical attacks	V	V		
FPT_PHP.2	Notification to the physical attacks	V	V		
FPT_RCV.2	Outward is recovery		V		
FPT_RPL.1	Detect the replay		V	V	

M&CSの構成機器等が持っている機能をハッキリさせることができた。

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	

これによりセキュリティ対策を取る上で、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

- M&CSの構築作業時に、ﾕｰｻﾞ・ﾍﾞﾝﾀﾞｰ・ｲﾝﾃｸﾞﾚｰﾀ等の関係者が、どのような作業を分担していくかを明確にしていきます。
  - プロダクトデザイン
  - システムデザイン
  - ｴﾝｼﾞﾆｱﾘﾝｸﾞ
  - テスト
- 関係者間における情報共有と協力体制