Japan Electric Measuring Instruments Manufacturers' Association

重要インフラを支える生産制御システムのセキュリティ

～JEMIMA研究活動のご紹介～

JEMIMA
セキュリティ調査研究WG

小川永志樹

PART-1 ：M&CSセキュリティを支える標準化動向
PART-2 ：M&CSセキュリティ機能要件の分析と役割分担

JEMIMAのご紹介

- 社団法人日本電気計測器工業会（JEMIMA）
- 目的
  - 我が国電気計測器産業及び関連産業の健全な発展を図る。
- 活動
  - 電気計測器に関する調査研究、規格の制定等
  - 新しいビジネス展開を目指す事業
  - 環境・安全・セキュリティ事業
  - 日本工業規格（JIS）原案作成事業
  - 国際標準化事業

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㈱、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、㈱東芝、㈱山武

- 活動実績
  - 研究活動
    - SP99　TR2を利用したセキュリティ対策の実践
    - 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

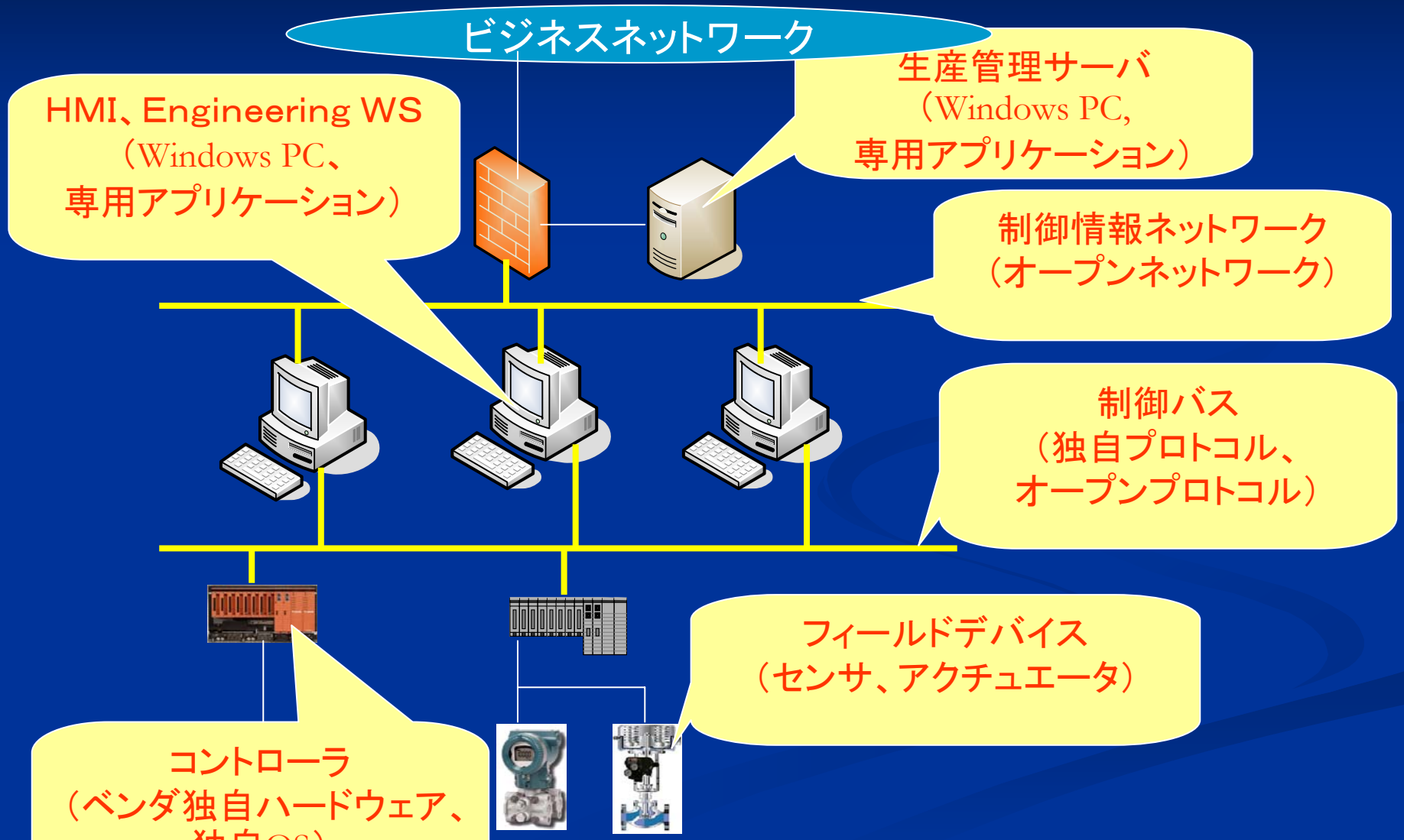
WGのご紹介

- 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 2006
  - SICE MOF (Manufacturing Open Forum) 2006
  - SICE Annual Conference 2007
  - 雑誌記事寄稿

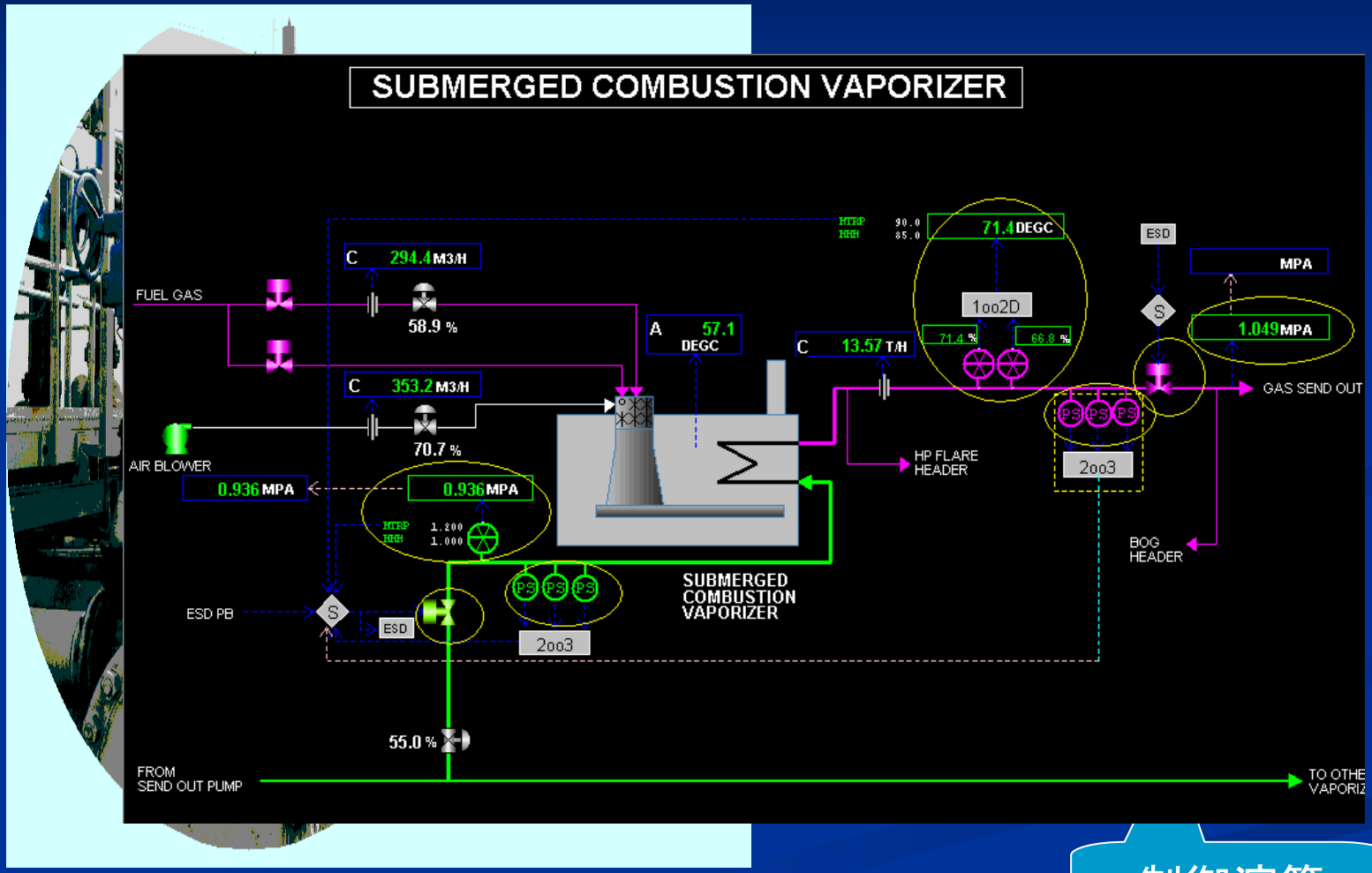
- 団体との協力関係
  - SICE（計測・制御ネットワーク部会）
  - JEITA（制御システム専門委員会）
  - JPCERT/CC

- その他の活動
  - IEC/TC65/WG10国内対策委員にメンバ登録

生産制御システム概要


ビジネスネットワーク
生産管理サーバ
（Windows PC,
専用アプリケーション）
HMI、Engineering WS
（Windows PC、
専用アプリケーション）
制御情報ネットワーク
（オープンネットワーク）
制御バス
（独自プロトコル、
オープンプロトコル）
フィールドデバイス
（センサ、アクチュエータ）
コントローラ
（ベンダ独自ハードウェア、
独自OS）

生産制御システム



制御演算

PART 1

セキュリティを支える標準化動向

JEMIMA
セキュリティ調査・研究WG

Agenda

- 背景
  - 現実化する脅威
  - ITセキュリティとM＆CSセキュリティ
- 標準化動向
- 標準の適用
- 今後の動向
  - デファクト標準

背景

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
    - Slammer　wormに感染したことによるネットワーク停止

ITセキュリティとM&CSセキュリティ

- ターゲット：C・I・A

ITセキュリティとM&CSセキュリティ

	IT セキュリティ	M&CS セキュリティ
守るべきもの	情報 （サーバ）	設備、製品
求められる可用性	低い （rebootは許される）	高い （rebootは許されない）
応答性	分/秒	秒/ミリ秒
リソース	豊富	制約あり

標準化動向

標準　－　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)

マネージメント視点

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) を発行済(2004年） 2007/11月　改定版発行予定
    - 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)
  - 標準の策定中

策定中の標準

- 策定中
  - Part 1: Scope, Concepts, Models and Terminology
    - **ANSI承認待ち　2007年11月発行予定**
    - 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
  - Part 2: Establishing an Industrial Automation and Control System Security Program
    - **委員会内で投票作業中。**
    - 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
  - **Working　Group設立完了**
  - Part 3: Operating an Industrial Automation and Control Systems Security Program
  - Part 4: Specific Security Requirements for Industrial Automation and Control

IEC/TC65/WG10

- 名称
  - "Network and System Security"
- 目的
  - M&CSのセキュリティを確保するための、Policy、Practice、Principleの確立。
- 参加メンバ
  - 12カ国のメンバで構成(ドイツ、フランス、イタリア、イギリス、アメリカ、韓国、中国、日本、オーストリア、スイス、デンマーク、カナダ)
  - ベンダ、出版、コンサルタント、大学などが中心で約30名。活動メンバは10名程度。
  - ベンダとしては、Honeywell、ABB、SIEMENS、Yokogawaなどが参加。
  - リエゾン
    - PCSRF
    - **ISA-SP99**

    などと協力関係を持ちながら活動。(情報提供、人的交流)
- 活動内容
  - 標準規格を策定中。
    - IEC 62443 3分冊。

策定中の標準

- Final Goal（2009年～2010年規格化完了予定）
  - 62443-1 Framework and threat-risk- analysis (IS)
    - リスク分析
  - 62443-2 Security assurance: principles, policy and practice (IS)
    - ポリシー
    - 慣例集
  - 62443-3 Sets of security requirements for security elements in typical scenarios (TS)
    - シナリオ分析
    - 技術的要件セット

コンポーネント視点

PCSRF

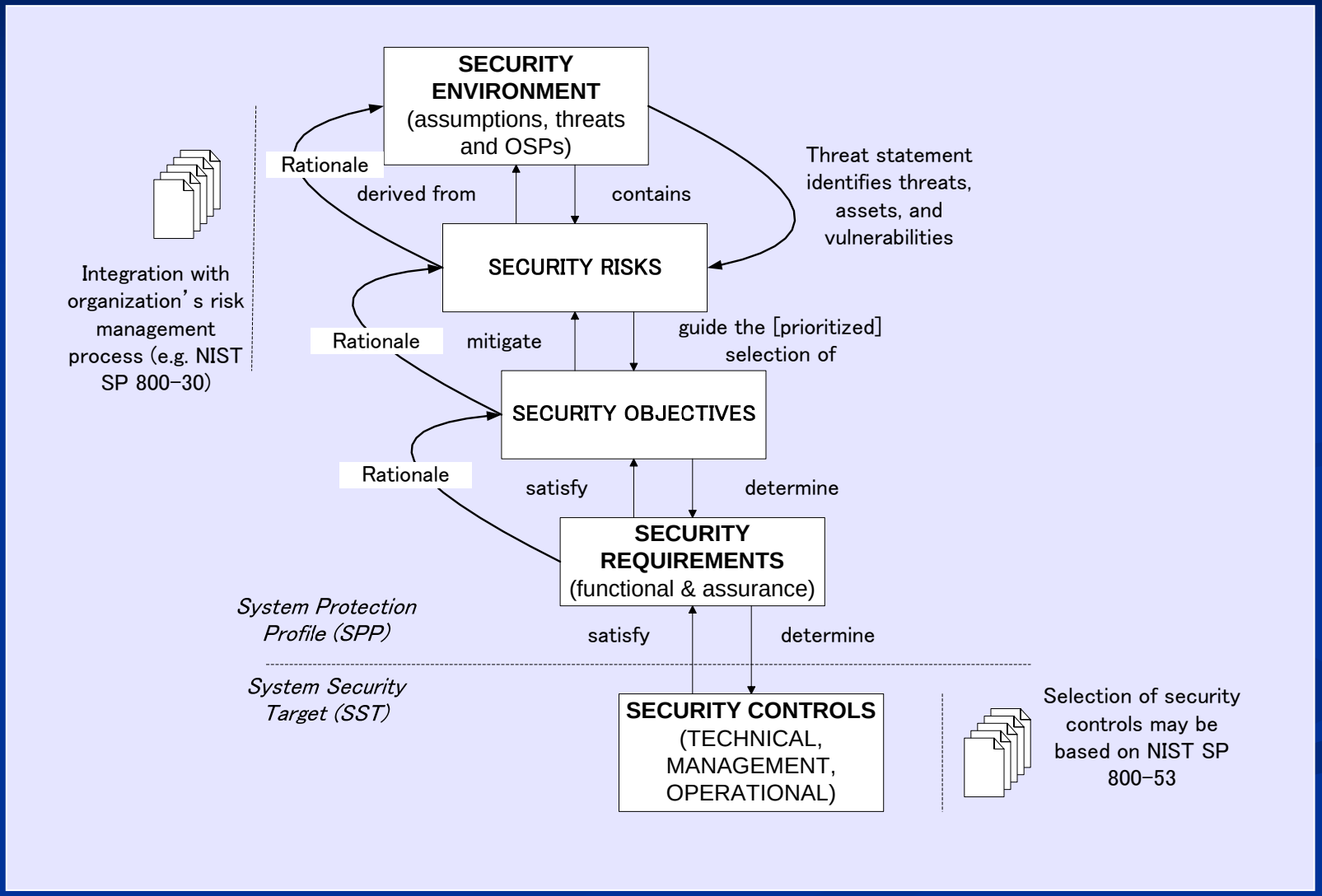
- 名称
  - **Process Control Security Requirements Forum** (発音: Pic-Surf)
- 位置付け
  - 米国商務省標準技術局:**NIST (National Institute of Standards and Technology)** の下部組織
- 目的
  - 産業用プロセス制御システム向けの情報セキュリティ要件を定義および適用することで，これらのシステムのセキュリティを強化すること。
  - ベースとして，**ISO15408** (Common Criteria for IT Security Evaluation)
- メンバー
  - 401の組織，32カ国(2005年8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

SPP-ICSの構造


SECURITY ENVIRONMENT (assumptions, threats and OSPs)
Rationale
derived from
contains
Threat statement identifies threats, assets, and vulnerabilities
SECURITY RISKS
Integration with organization's risk management process (e.g. NIST SP 800-30)
Rationale
mitigate
guide the [prioritized] selection of
SECURITY OBJECTIVES
Rationale
satisfy
determine
SECURITY REQUIREMENTS (functional & assurance)
System Protection Profile (SPP)
satisfy
determine
System Security Target (SST)
SECURITY CONTROLS (TECHNICAL, MANAGEMENT, OPERATIONAL)
Selection of security controls may be based on NIST SP 800-53

標準の適用

ベンダ視点での適用

- ISO15408認証取得
  - PCSRFが定義したPPをベースに自社の製品のセキュリティ保障レベルをISO15408の枠組みで認証。

- 製品開発
  - セキュリティ要件の抽出
    - PPをベースに考える。

ユーザ視点での適用

- 調達要件
  - PCSRFをベースとしたセキュリティ要件
  - ISO15408 EAL指定
- セキュリティ管理システム構築
  - ISA-SP99 TR2のアプローチ

今後の動向

今後の動向

- デファクト標準
  - M&CS コンポーネントのセキュリティ認証
    - **BCIT** - WurldTech
    - **MUSIC** - MuSecurity

  - M&CS システムセキュリティ認証
    - **INL**（Idaho National Laboratory ）

PART 2

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~

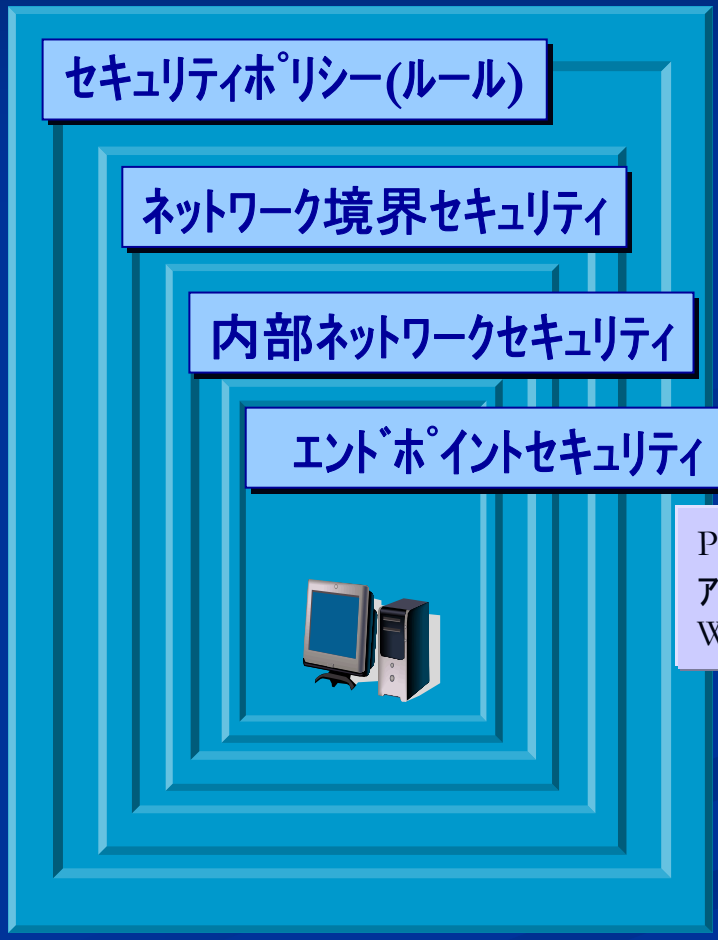
JEMIMA
セキュリティ調査・研究WG

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

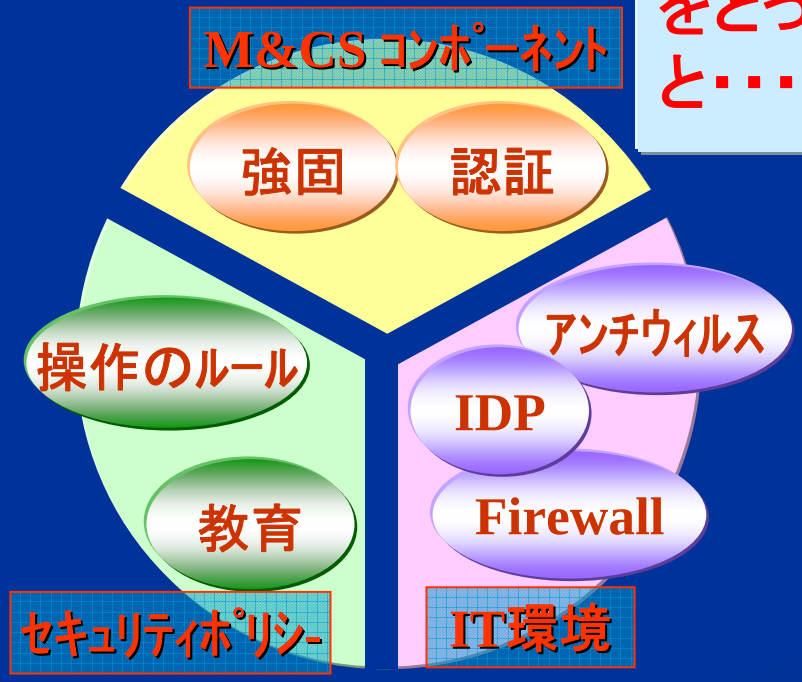
PC等の強化
アンチウィルスソフト
Windows等へのセキュリティパッチ

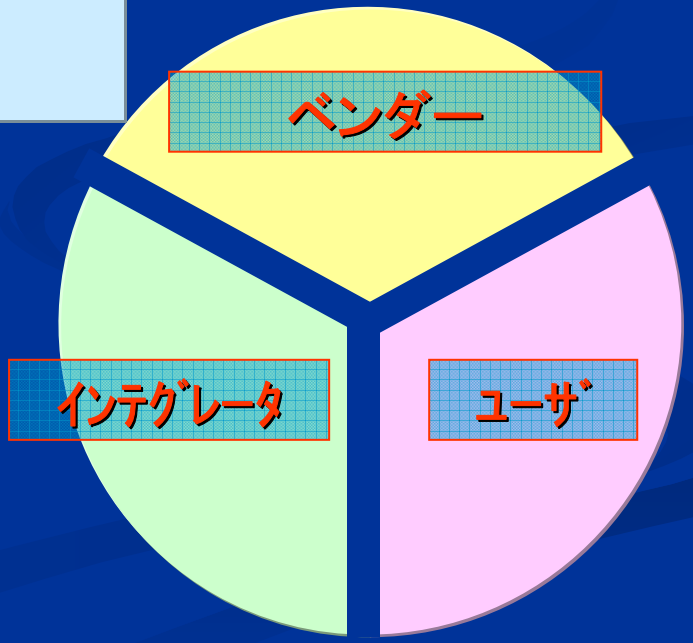
2つのギャップを考える

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・・・・・・・・・



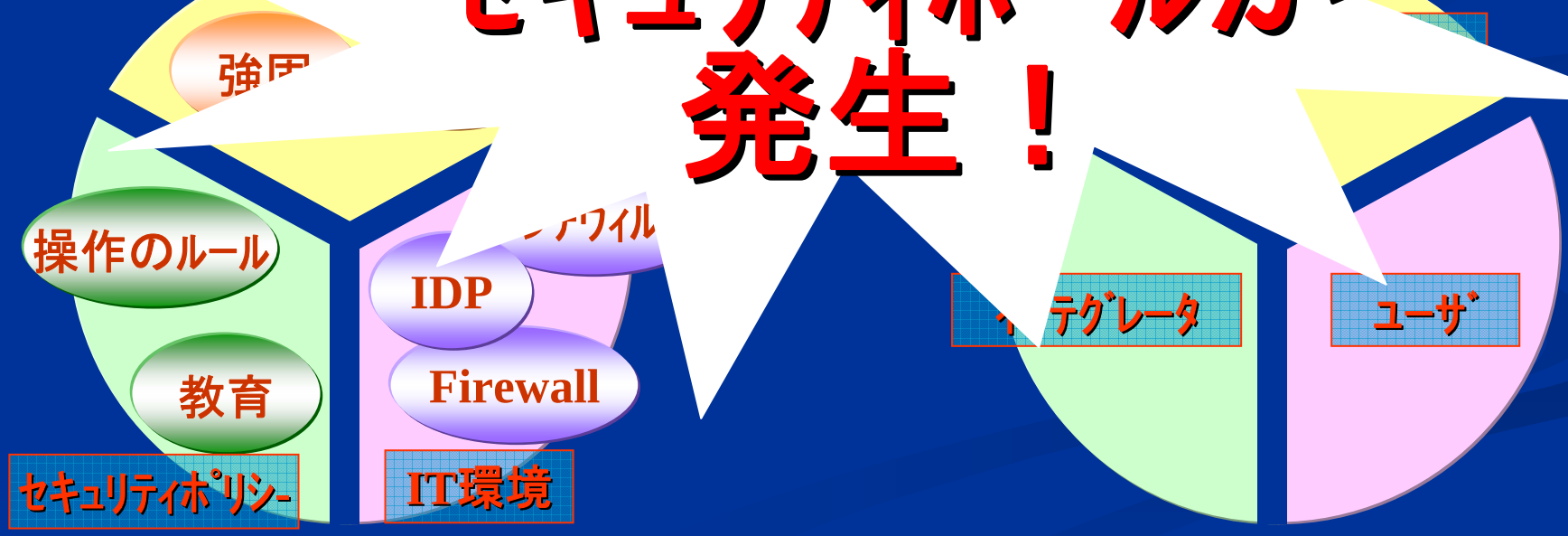


2つのギャップを考える

機能分担
から見たギャップ

責任分担
から見たギャップ

システムに
セキュリティホールが
発生！



2つのギャップを埋めるために

コンポーネント毎のセキュリティ機能要件を定義

セキュリティ機能要件の実装責任者をシステム関係者に割当てる

2つのギャップを明確に

SPP-ICS Ver1.0

- 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

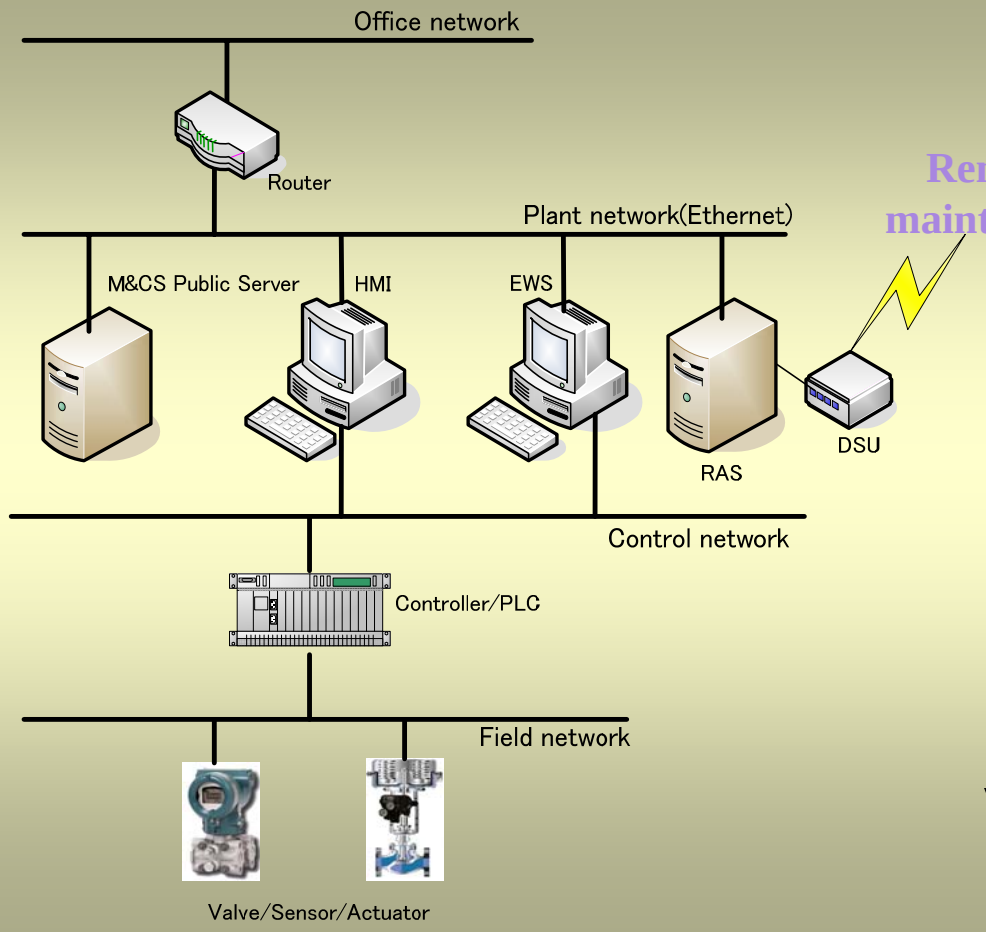
→ **PCSRF SPP-ICS Ver1.0を利用**
- 抽出したモデルケースそれぞれでから脅威を分析
- セｷｭﾘﾃｨ機能要件を抽出

機能・役割の分担

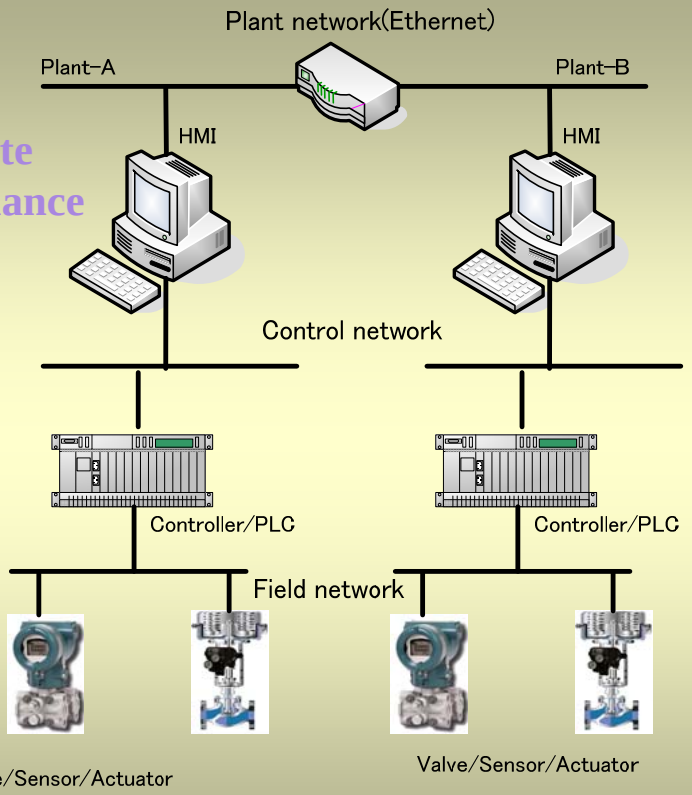
→ **機器・人の役割を明確化**
- M&CSの構成機器
- IT機器
- 非IT系
- 関連者（ﾕｰｻﾞ・ﾍﾞﾝﾀﾞ・ｲﾝﾃｸﾞﾚｰﾀ）の役割分担

実践に使用したモデルシステム

垂直構造



水平構造



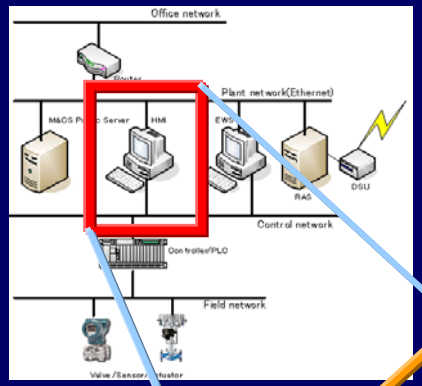
機能要件の分析

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

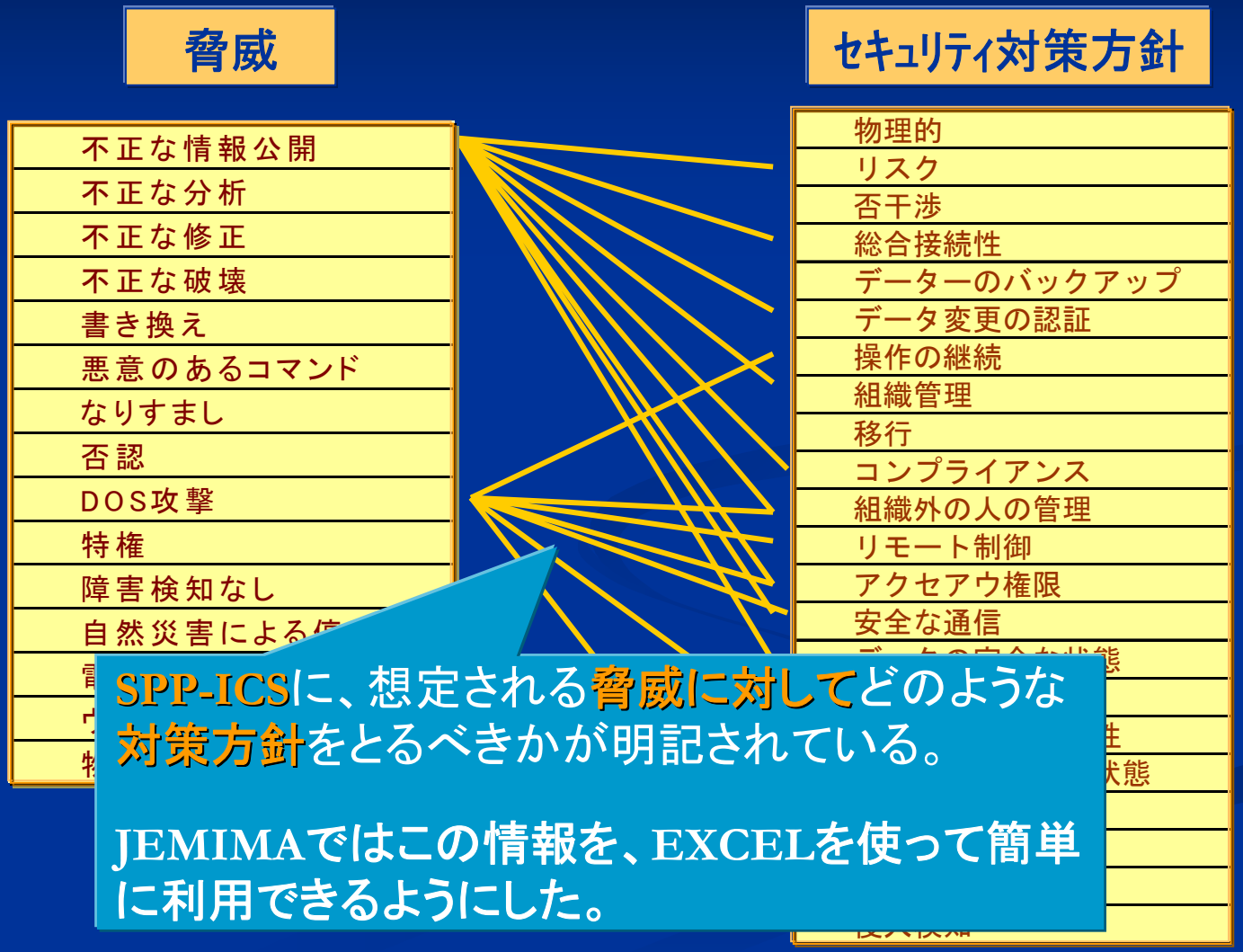
機能要件の分析

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。

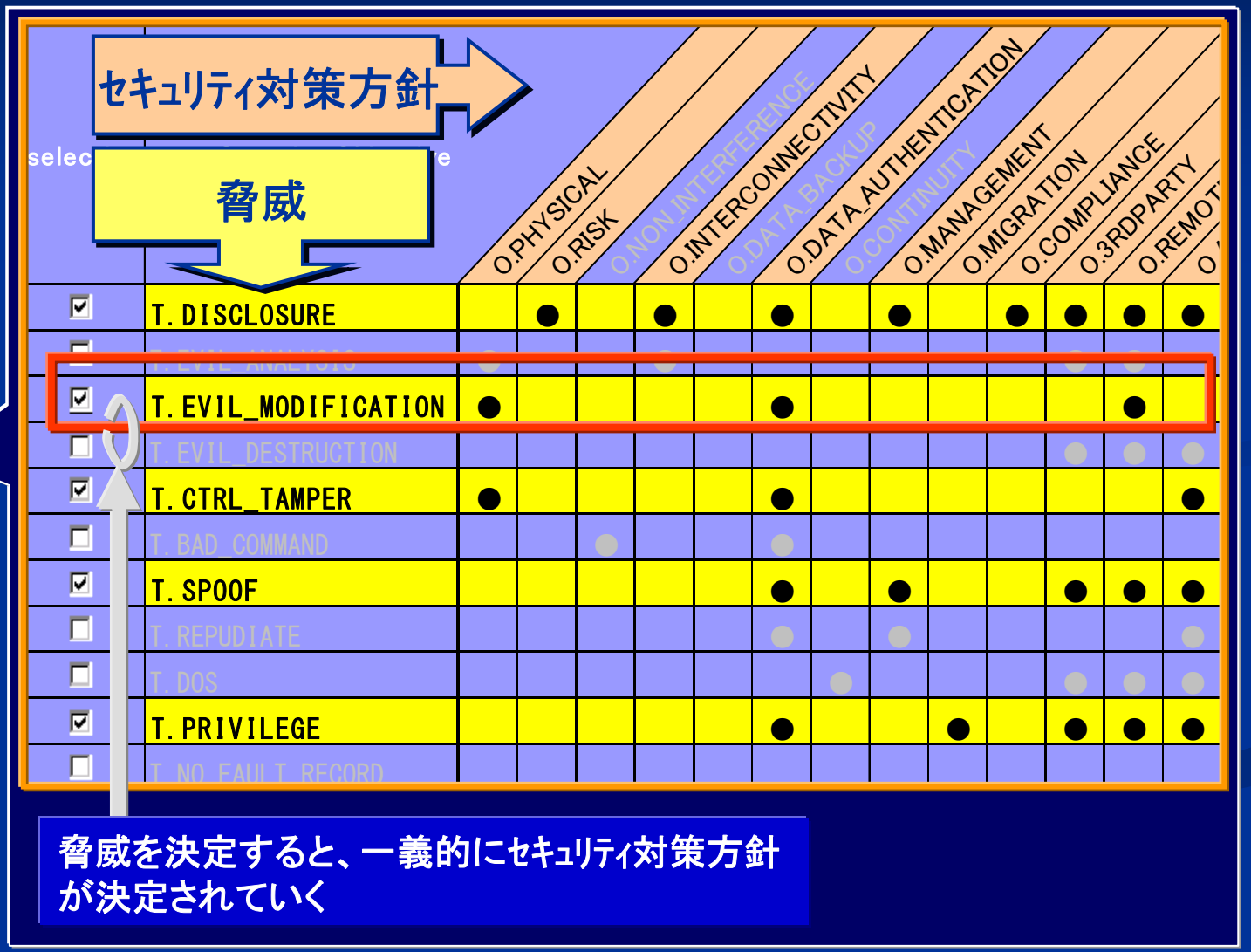
機能要件の分析

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

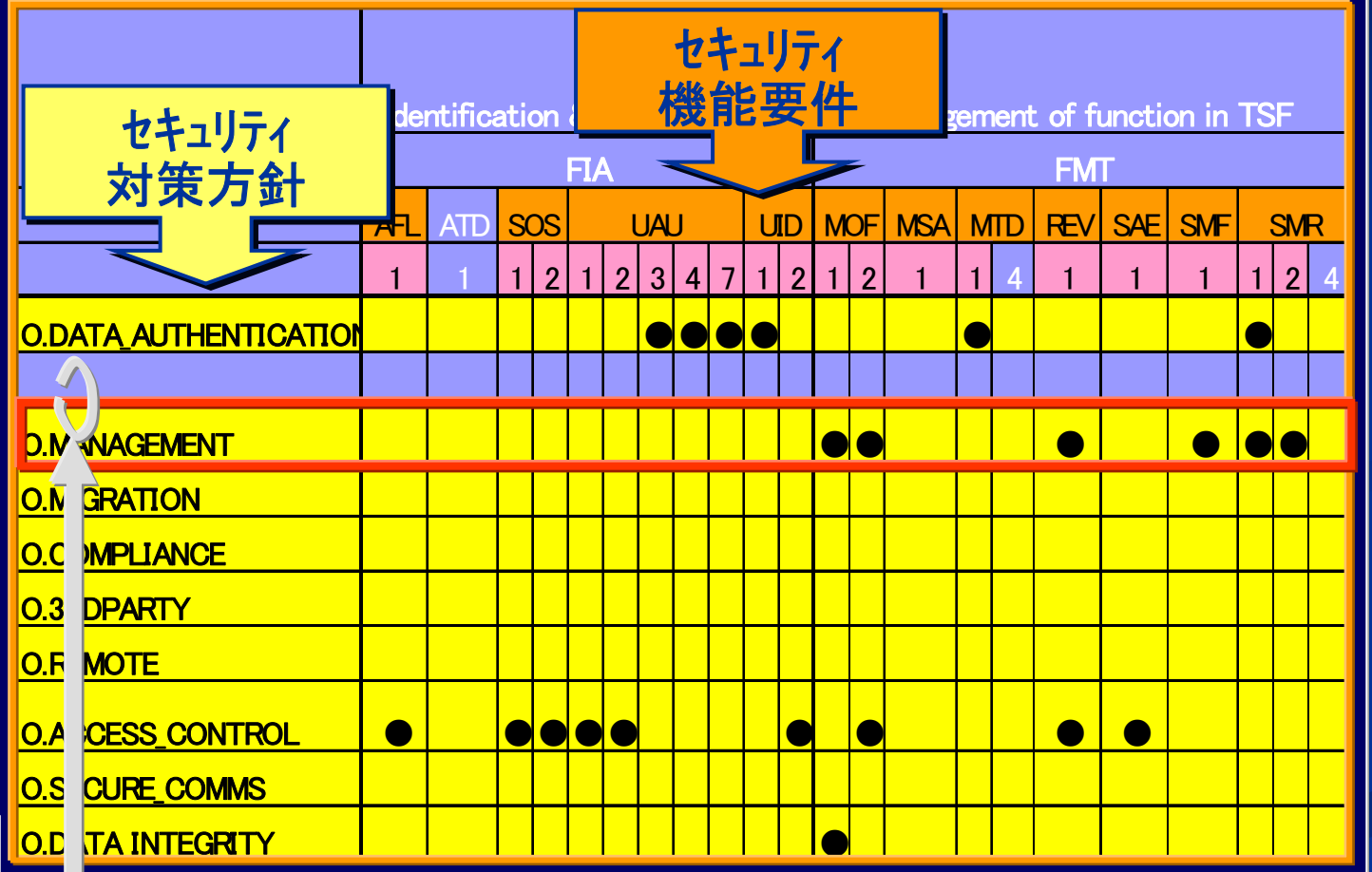
脅威を確定する

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

セキュリティ対策方針

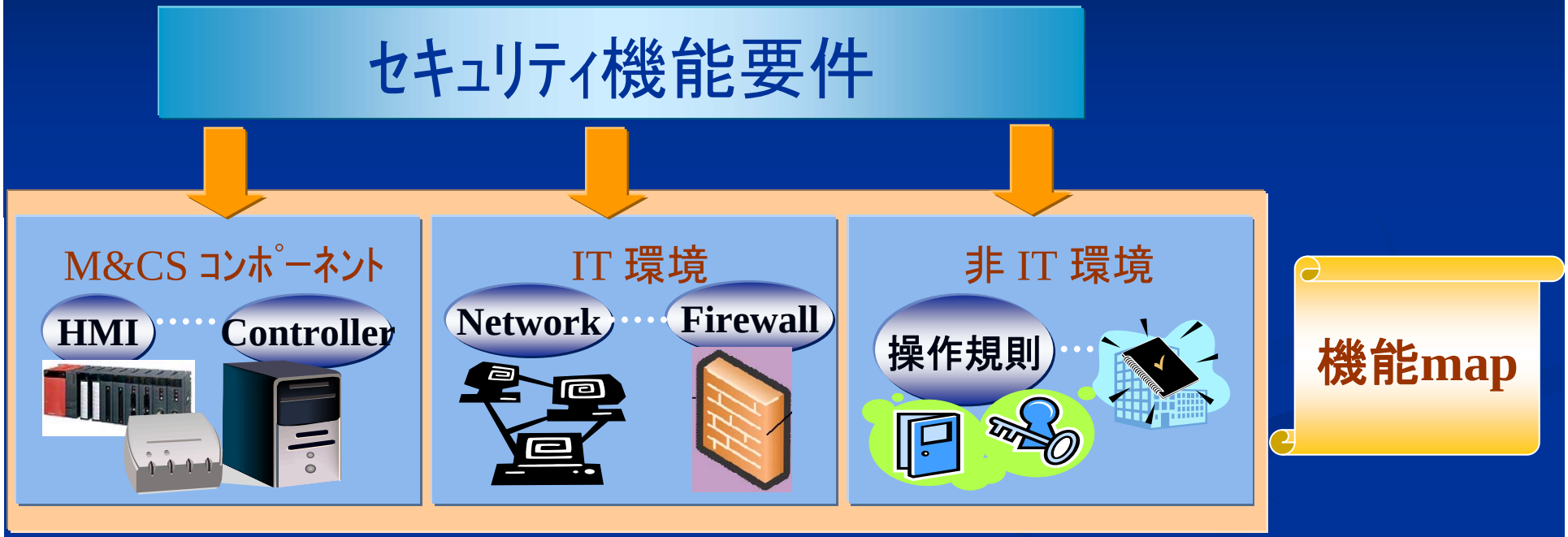
セキュリティ機能要件



対策方針を決定すると、一義的にセキュリティ機能要件が決定されていく

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

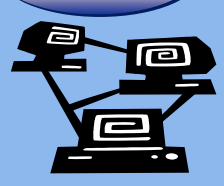
セキュリティ機能要件

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　インテグレータ　制御機器ベンダ

役割map

役割Mapを作る

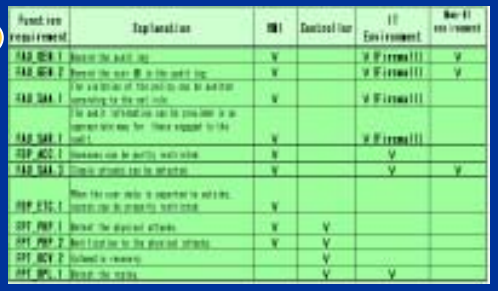
セキュリティ
機能要件

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



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

今後の作業

- M&CSの構築作業時に、ユーザ・ベンダー・インテグ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
  - エンジニアリング
  - テスト
- 関係者間における情報共有と協力体制

本日は、ありがとうございました。

JEMIMA

セイキュリティ調査・研究WG