Panasonic

製造システムのセキュリティ確保に向けた パナソニックでの取り組み

2017年2月21日

パナソニック株式会社
製造システムセキュリティ室
藤井　俊郎

本日の内容

- 会社概要
- パナソニックのモノづくりの特徴
- 製造システムでのサイバーセキュリティリスク
- 製造システムセキュリティ確保の取り組み
  - ガバナンス
  - 具体的対策
- 最後に

会社概要

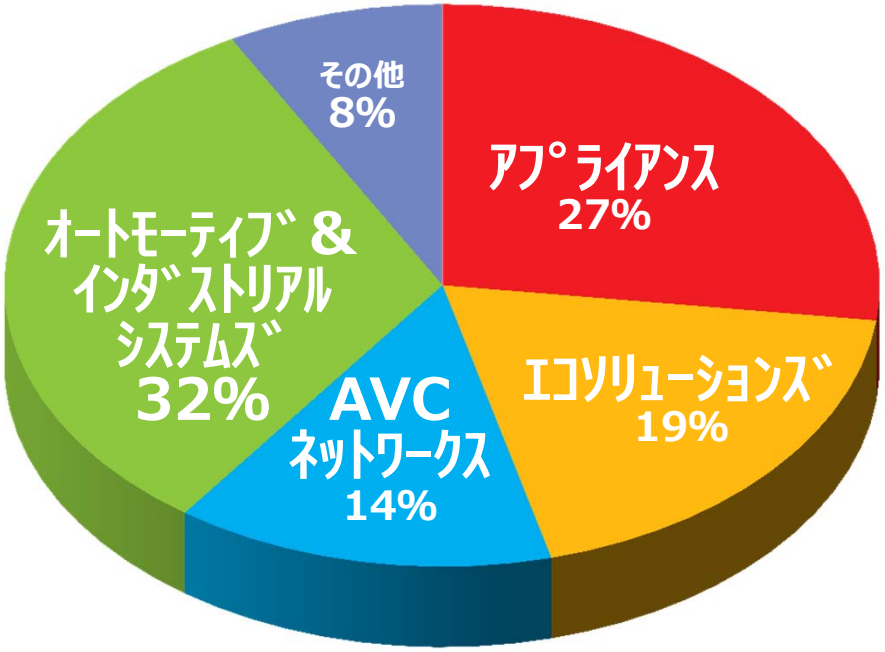
パナソニックグループの概要

本　社　：パナソニック株式会社
創　業　：1918 (大正7) 年 3月
売上高　：7兆5,537 億円
従業員　：25万4,084名 (2016年3月)

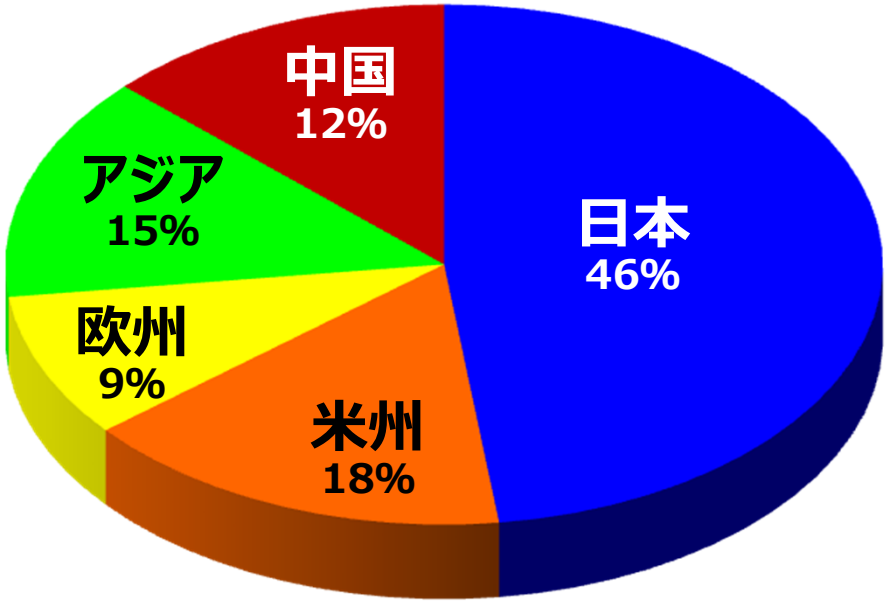
«ブランドスローガン»
A Better Life, A Better World

住宅、社会、ビジネス、旅、自動車など
多様な空間・領域で、様々なパートナーと
お客様一人ひとりにとっての「より良いくらし」
を追求し、拡げていくと共に、地球環境への
貢献をはじめ、グローバルに「より良い世界」
の実現に貢献していきます。

《事業セグメント別売上比率》



《地域別売上比率》



（2015年度　連結ベース）

パナソニックのモノづくりの特徴

多くの製造拠点と様々な商品

グローバル311拠点　（国内131拠点、海外180拠点）

※２０１６年４月現在

「大量生産から少量生産まで」　「大物から小型デバイス商品まで」

「長Ｌ／Ｔから短Ｌ／Ｔ商品まで」「受注案件物から即納商品まで」

「Ｂ２ＢからＢ２Ｃまで」 **多様な市場・お客様、商品のモノづくりを実践**

IoT活用の世界の潮流

グローバルで進む
IoT活用によるモノづくり高度化、ビジネスモデル変革

ドイツ

インダストリー4.0

Plattform INDUSTRIE 4.0

インターネット、デジタル化
による工場のスマート化

米国

インダストリアル　インターネット

industrial internet CONSORTIUM

IoTを活用した産業の
革新と新しいサービス創造

**IoTで日独連携の
6項目で覚書締結**

中国

中国製造2025

MADE IN CHINA 中国制造 2025

製造情報化を進め
製造大国から製造強国へ

日本

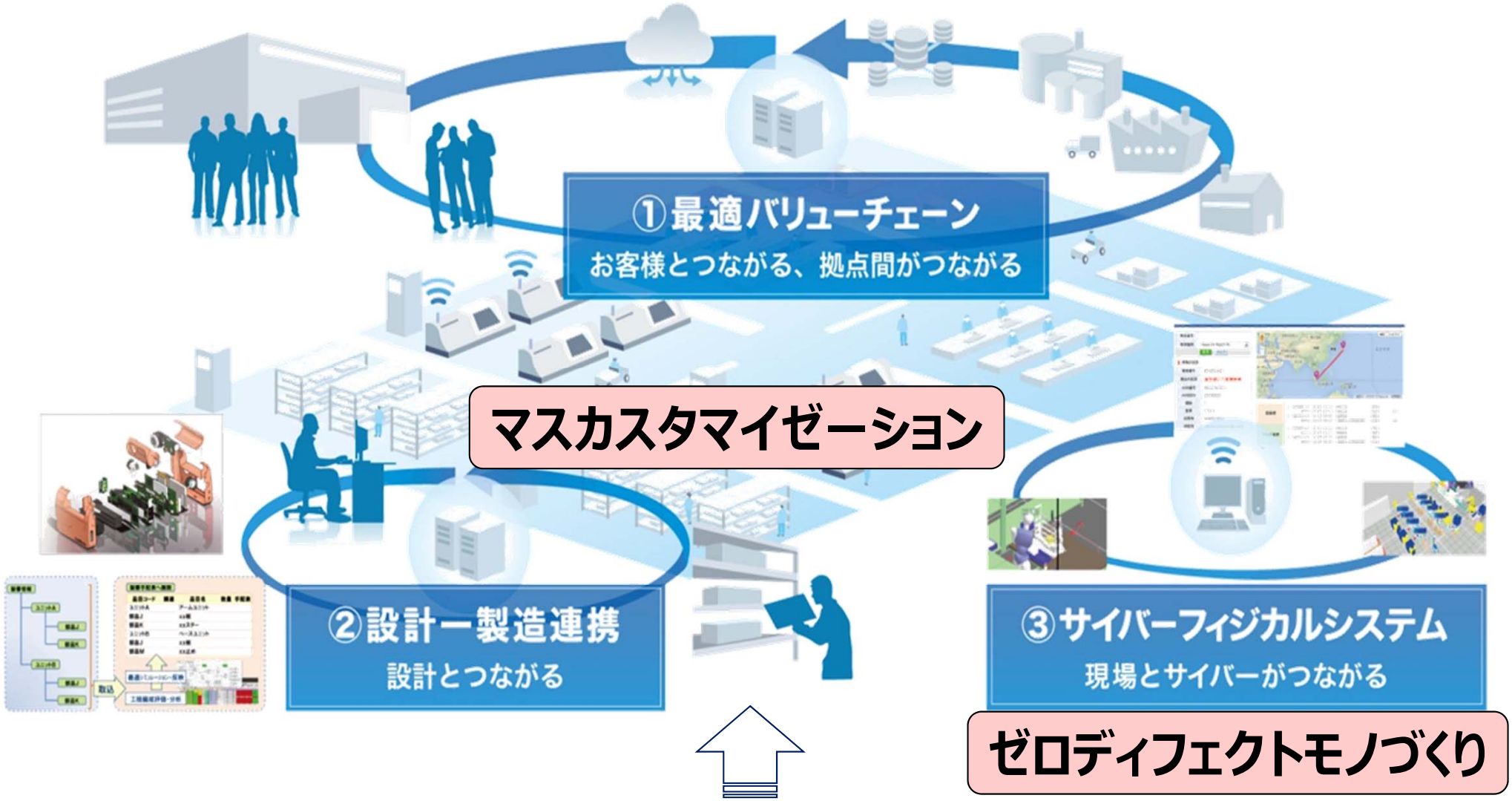
インダストリアル・バリューチェーン・イニシアティブ

IVI Industrial Value Chain Initiative
Connected ! Manufacturing

ものづくりと ICT の
融合による「つながる工場」

IoT時代のパナソニックが目指すモノづくり

ITを駆使したIoTでの『スマートマニュファクチャリング』を構築



IoT、ビッグデータ、AIの利活用で<u>うまくつくる</u>（QCDの飛躍的向上）

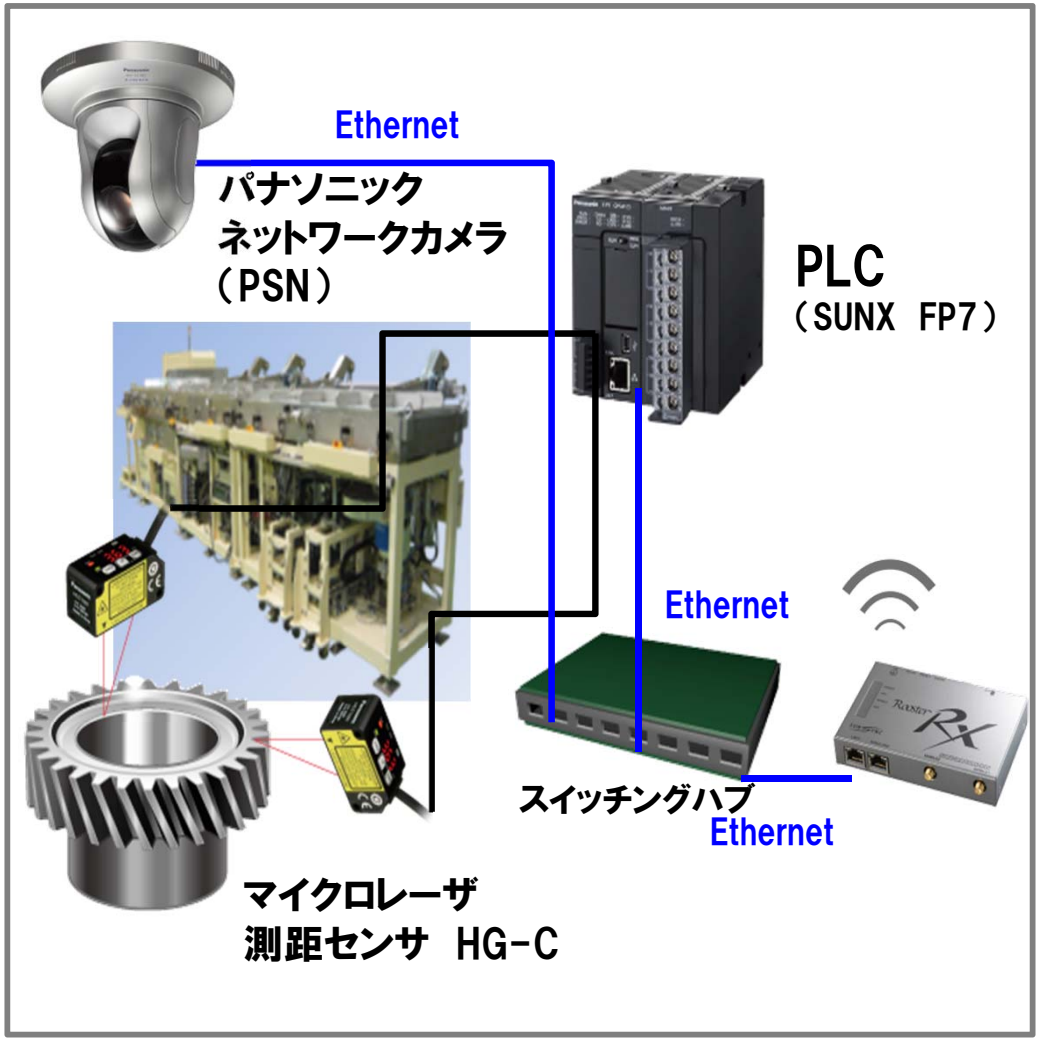
設備のIoT・ネットワーク対応（例）

低コストでIoTネットワーク構築

◆WEBサーバ機能搭載PLCに接続

既存設備をレトロフィット

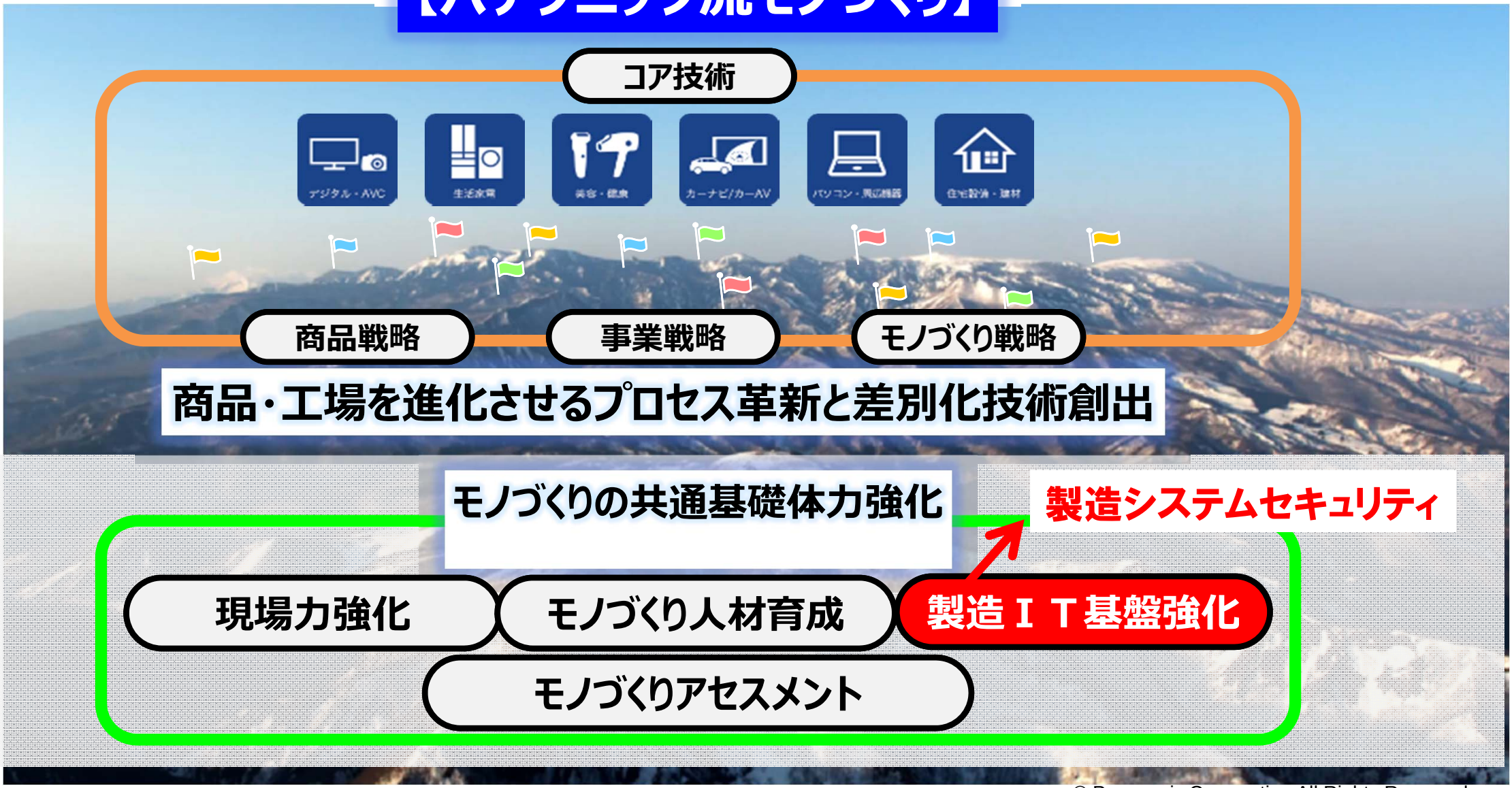
◆センサーやカメラを後付でIoT対応



モノづくりでの製造システムセキュリティの位置づけ

事業特性に適応し、他社と差別化した特長あるモノづくり

【パナソニック流モノづくり】



製造システムでの
サイバーセキュリティリスク

工場でのサイバーセキュリティの取り組み

パナソニックの工場を取り巻くサイバーセキュリティの状況

サイバーリスクの実態

・社内工場で大きな経営ロスが
生じた事例は現在発生していない。

・社外では
IPA等からも情報が出ているように
様々な事例が発生している

スマート工場

・高効率化・高品質の取り組みの中で
工場のICT化は確実に進んでいる

・サイバーセキュリティを考慮した工場の
ネットワーク/IT設計になっていない

ユーザからの要請

・通常の情報セキュリティ以外に
工場のサイバーセキュリティに
特化した要請は無い

・しかしBCPの視点から
サプライチェーン確保の要請は大きい

その他状況

・リアルタイム処理(＜1ms)が必要
ウイルス対策ソフト等を導入出来ない
・固有の機器（PLC・DCS・製造装置等)は
セキュリティ対策のツール・ソフトが無い
・使用期間が長い(10年以上)ので、
脆弱性への対策が終息

工場でのサイバーセキュリティの取り組み

工場を取り巻くサイバーセキュリティの状況

サイバーリスクの実態

・社内工場で大きな経営ロスが
生じた事例は現在発生していない。

社外では事故は発生

IPA等からも情報が出ているように
様々な事例が発生している

スマート工場

・高効率化・高品質の取り組みの中で

**スマート工場化の取り組みは
もう既に進んでいる**

ネットワーク/IT設計になっていない

ユーザからの要請

・通常の情報セキュリティ以外に

**サプライチェーン・生産の
確保・継続は絶対**

・しかしBCPの視点から
サプライチェーン確保の要請は大きい

その他状況

・リアルタイム処理(<1ms)が必要

**ITで常識的な対策を
OTでは実施できない**

・使用期間が長い(10年以上)ので、
脆弱性への対策が終息

工場でのサイバーセキュリティの取り組み　必要性検討

工場でサイバー攻撃を受けた時に想定されるリスク

- 工場の**稼動**停止
- 検査異常等による**品質**の低下
- レシピ改ざん等による**歩留まり**低下
- **情報の漏洩**
  - お客様情報
  - 設計情報
  - 製造ノウハウ

→ **経営への影響**

BCPの視点　お客様からサプライチェーンの維持を強く求められており、サイバー攻撃を受けてもパナソニックの生産稼動・品質を確保する取り組みが重要となっている。

生産性の向上　生産性・信頼性の向上及びコストダウンの取り組みに、ITの活用が必須となってきており、工場でもサイバー攻撃を考慮しなくてはならなくなってきている。

工場の稼動・品質維持、ユーザーからの信頼確保の為には、対策を始めておく必要がある

製造システムセキュリティの取り組み（ガバナンス）

工場でのサイバーセキュリティの進め方

パナソニック社内では情報セキュリティが行われており、定着してきている

■ 情報セキュリティ

・情報セキュリティを実施していく全社体制
・情報セキュリティ基本規程・基準　ガイドライン等のルールの制定
・ＩＳＯ２７００１認証取得・及び準拠した活動によるＰＤＣＡ活動の定着

■ ＩＴセキュリティ

・ＩＴセキュリティを実施していく全社体制（ＣＳＩＲＴ／ＳＯＣ）
・ 情報システムとしてのガイドライン等のルールの制定

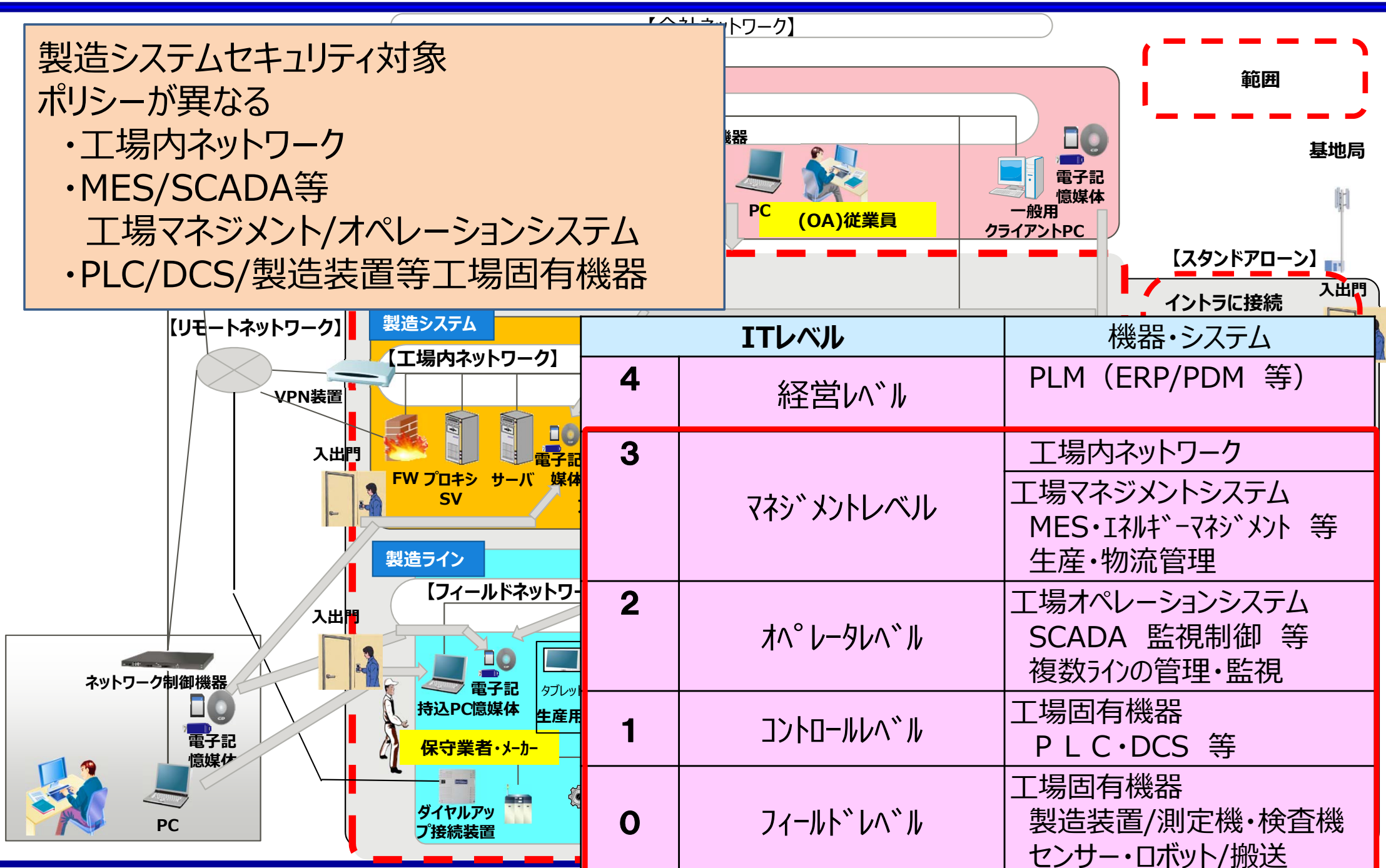
■ パナソニック製品の情報セキュリティ

・製品セキュリティセンターを軸にした全社体制（ＰＳＩＲＴ）
・製品セキュリティ規程・基準　ガイドライン等のルールの制定

既存の取り組みを前提として、重複・矛盾となるような取り組みにしない
製造システムセキュリティのターゲットは
イントラネットと工場との接点及びインターネットと工場の接点から工場側とする。

工場でのサイバーセキュリティの取り組み範囲

製造システムセキュリティ対象
ポリシーが異なる
- ・工場内ネットワーク
- ・MES/SCADA等
  工場マネジメント/オペレーションシステム
- ・PLC/DCS/製造装置等工場固有機器



ITレベル		機器・システム
4	経営ﾚﾍﾞﾙ	PLM（ERP/PDM　等）
3	ﾏﾈｼﾞﾒﾝﾄﾚﾍﾞﾙ	工場内ネットワーク 工場マネジメントシステム MES・ｴﾈﾙｷﾞｰﾏﾈｼﾞﾒﾝﾄ　等 生産・物流管理
2	ｵﾍﾟﾚｰﾀﾚﾍﾞﾙ	工場オペレーションシステム SCADA　監視制御　等 複数ﾗｲﾝの管理・監視
1	ｺﾝﾄﾛｰﾙﾚﾍﾞﾙ	工場固有機器 ＰＬＣ・DCS　等
0	ﾌｨｰﾙﾄﾞﾚﾍﾞﾙ	工場固有機器 製造装置/測定機・検査機 センサー・ロボット/搬送

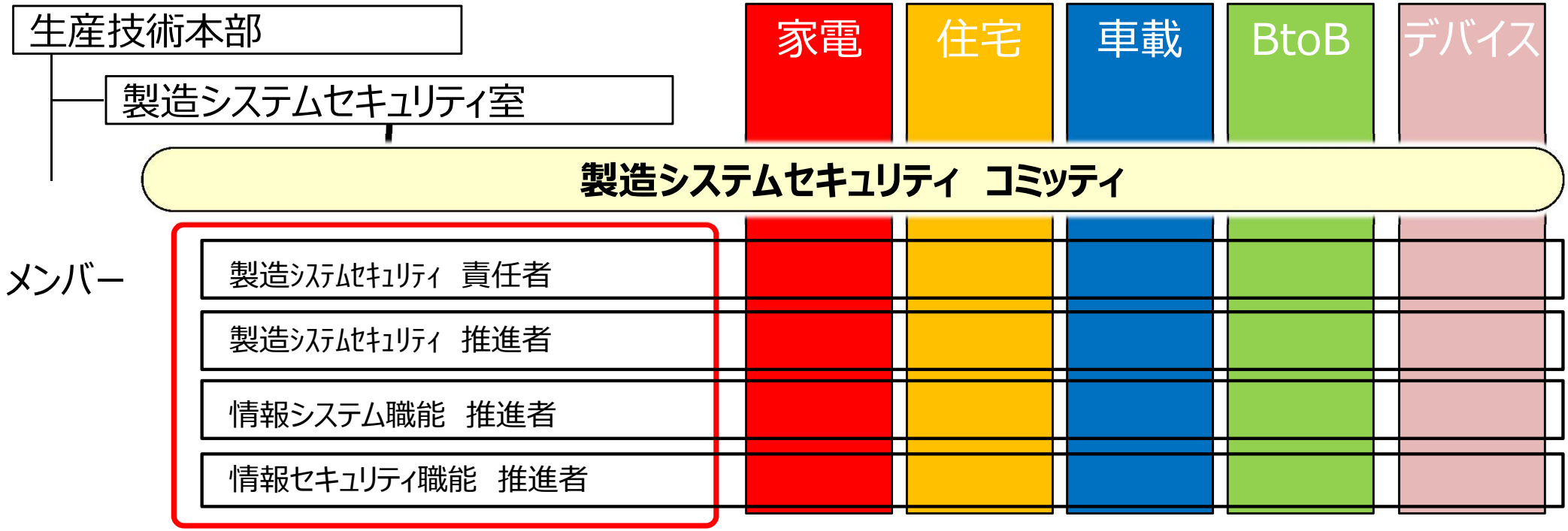
推進体制

工場での自主的改善活動が行えるよう、生産技術者が中心となって推進
ＩＴセキュリティ・情報セキュリティとの接点が多くあるので横断的体制を構築

■ 方針　生産技術本部傘下に「製造システムセキュリティ室」を設置、全社横断の活動を推進する
工場のサイバーセキュリティ対策を高位平準化しＢＣＰリスクを低減する

■ 推進体制

製造システムセキュリティ　コミッティにて方針の決定、推進を進める。



製造システムセキュリティの取り組み
（具体的対策）

考え方

工場に適した製造システムサイバーセキュリティ対策の確立

ガイドラインにより工場として必要なベースラインを明確化

グローバル全拠点への推進による高位平準化の実現

各拠点のBCPリスクに応じた対策を進める

製造システムセキュリティの計画

次の3ステップを3カ年計画で進める

①ウイルス／マルウエア侵入防止の徹底

②工場で異常を検知出来るしくみの導入

③インシデント対応の確立

方針

①ウイルス／マルウエア侵入防止の徹底

技術情報漏洩防止対策として、工場での対策は2009年にガイドライン化していた。
IoTを活用したスマート工場としての変化点を踏まえて、必要な内容に進化させる。
（１）　製造システムがERP等の経営システムと接続
（２）　ビッグデータ解析等に向けて　クラウドの活用
（３）　製造に用いるシステム(SCADA/HMI等)・機器(PLC/センサ/ﾀﾌﾞﾚｯﾄ等)進化

②工場で異常を検知出来るしくみの導入

現在、工場に適した異常検知システムは存在しない。
工場に導入できる異常検知システムを開発又は導入していく。

サイバーセキュリティインシデントも設備故障と同様の考え方で要求レベルを
設定する。（故障率/復旧までの時間等）

③インシデント対応の確立

異常を発見した際に要求レベルを充たすインシデント対応が出来るよう体制を
構築していく

製造システムセキュリティの取り組み（具体的対策）

①ウイルス／マルウエア侵入防止の徹底

①ウイルス／マルウエア侵入防止の徹底

参照できるガイドライン等

- CSMS（IEC62443-2-1）
- NIST SP800-82
- IoTセキュリティガイドライン

情報収集

- JPCERT/CC資料
- 調査・情報収集　他社委託
- CSSC　VEC等の団体

社内の既存規程・ルール

- 情報セキュリティ管理規程
- 情報システム基本規程
- 生産用PCセキュリティガイド

パナソニック工場でのベースラインとなるガイドラインを制定

グローバル311拠点 (国内131拠点、海外180拠点)へ展開

ガイドラインの内容

具体的内容１

物理的セキュリティ	製造現場の物理的管理策
	製造現場への機器の持ち込み
ネットワークセキュリティ	ネットワークセグメント設計
	各セグメントに接続可能な機器
	ネットワークの通信制御
	リモートネットワーク
ネットワークに接続する機器	構成管理

ガイドラインの内容

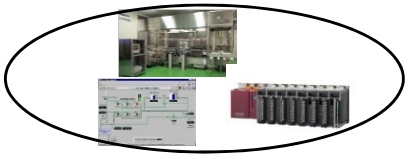
物理的管理・機器の持込による感染対策（再度徹底）

（１）USBメモリー・PCの持込による感染防止
（２）製造・測定装置の持ち込みによる感染防止
（３）セキュリティゾーニングによる入退出のコントロール

USB

PC

設備



持ち込み手順・ルールを決め
日々運用する

セキュリティゾーン（工場）

入退出管理
セキュリティカメラ

入り口

ウイルス
チェック

OSﾊﾞｰｼﾞｮﾝ
チェック実施

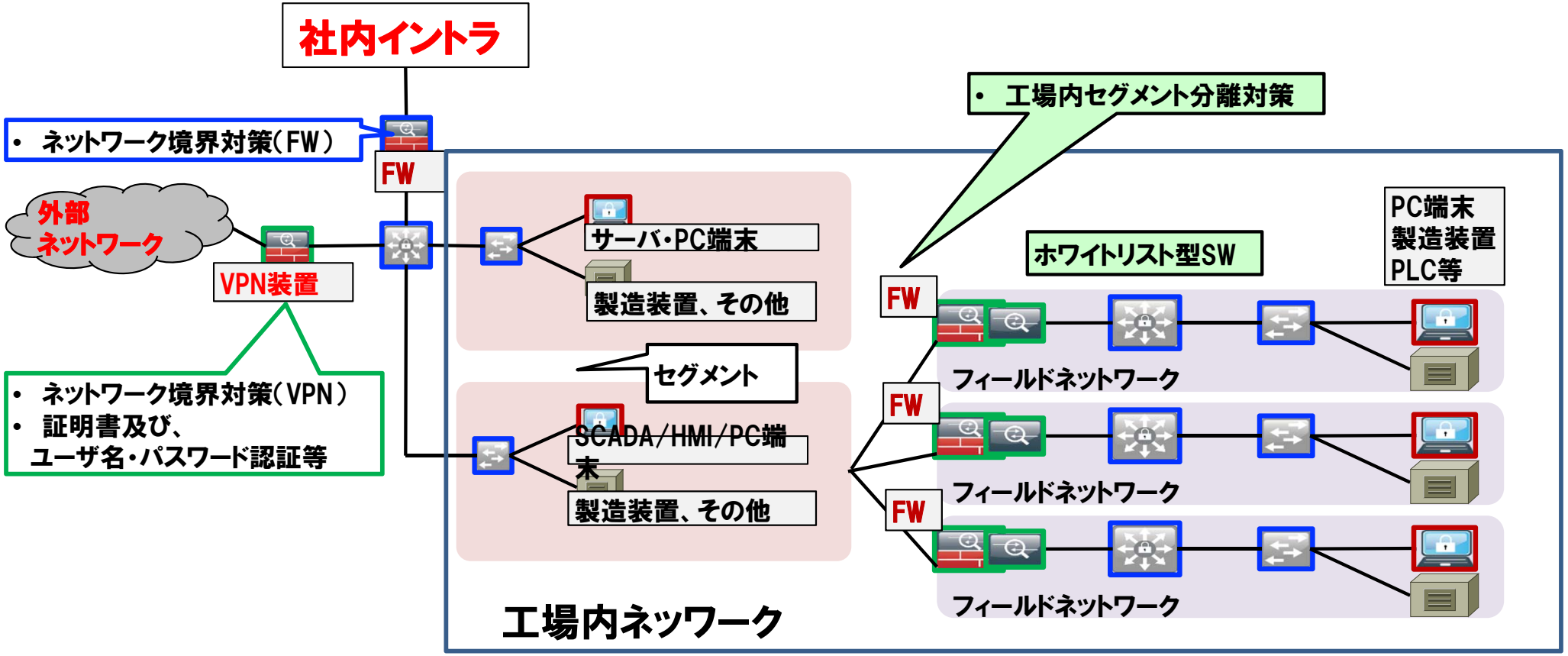
設備導入・ネットワーク接続前に確認

ウイルスチェック
実装したセキュリティ機能の確認

ガイドラインの内容

ネットワークを通じての感染対策

（１） 社内イントラからの侵入 ⇒ FWの設置
（２） 工場の外部接続からの侵入 ⇒ VPN(２要素認証)
（３） 必要に応じてネットワークのセグメントを別ける
（４） 社内イントラとの通信は想定している通信に限定
（５） 工場ネットワークからはインターネットにアクセスしない 等



ガイドラインの内容

具体的内容２

機器共通の管理策	
ネットワーク機器	ネットワーク機器
	ネットワーク制御機器
	FW（ファイアウォール）
	無線LANアクセスポイント
	VPN装置
情報機器	情報機器共通
	一般用クライアントPC
	生産用クライアントPC
	生産用サーバ（CIM、MES等）
	生産用情報機器（カメラ、スマートフォン、タブレット等）
	持込PC
	電子記憶媒体
製造装置	製造装置共通
	PLC／DCS等の制御装置
	HMI／SCADA等の表示・操作装置
	カメラ
	その他製造装置
その他	通信カード、SIMカード

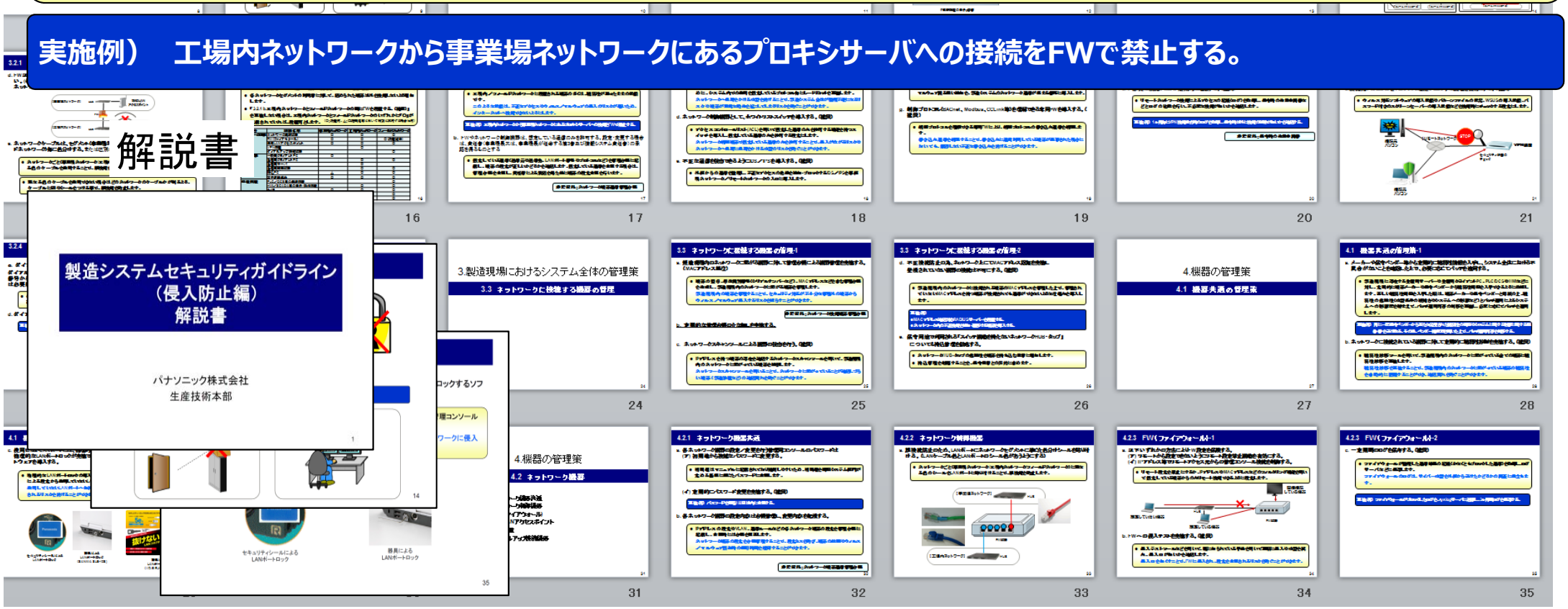
ガイドラインの解説書の作成

ガイドラインの各項目毎に実施内容（例）を簡単に解説し実施例を示す

工場内／フィールドネットワークに設置される機器は、事業場ネットワーク経由でもインターネットに接続できないようにする。

- **工場内／フィールドネットワークに設置される機器の多くは、脆弱性が残ったままの状態です。**
  このような状態は、不正なアクセスやウィルス／マルウェアの侵入のリスクが高いため、インターネットへ接続できないようにします。

実施例）　工場内ネットワークから事業場ネットワークにあるプロキシサーバへの接続をFWで禁止する。



ガイドラインのチェックリストの作成

製造システムセキュリティガイドライン（侵入防止編） チェックシート

チェック対象	
会社名	
部署	
工場名	

最終承認	承認
日付：	日付：

結果（評価点数）

		必須項目の評価							推奨項目の評価						
		点数				はい	いいえ	N/A	点数				はい	いいえ	N/A
3.1	物理的セキュリティ	0	／	7	0%	0	0	0	0	／	0	－	0	0	0
3.2	ネットワークセキュリティ	0	／	11	0%	0	0	0	0	／	8	0%	0	0	0
3.3	ネットワークに接続する機器の管理	0	／	3	0%	0	0	0	0	／	2	0%	0	0	0
4.1	機器共通の管理策	0	／	2	0%	0	0	0	0	／	2	0%	0	0	0
4.2	ネットワーク機器	0	／	7	0%	0	0	0	0	／	5	0%	0	0	0
4.3	情報機器共通	0	／	34	0%	0	0	0	0	／	7	0%	0	0	0
4.4	製造装置	0	／	14	0%	0	0	0	0	／	8	0%	0	0	0
4.5	その他	0	／	2	0%	0	0	0	0	／	0	－	0	0	0
総合得点		0	／	80	0%	0	0	0	0	／	32	0%	0	0	0

チェック実施者		
	部署名	御氏名
代表者		


【資料4－2】製造システムセキュリティガイドライン（侵入防止編） チェックシート

各拠点でチェックシートを用いて
アセスメントを実施

未実施項目に関して
改善計画を立てて実施する。


製造システムセキュリティガイドライン（侵入防止編） 改善計画書

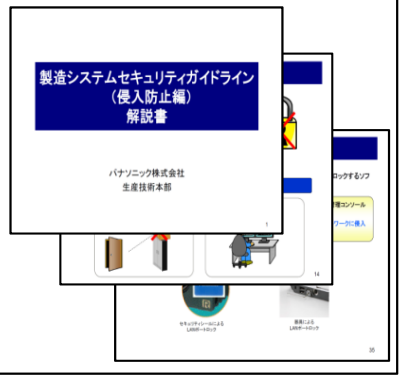
全社への展開

ツールを準備

ガイドライン

チェックシート

解説書



製造システムセキュリティのコミッティを通じて各カンパニーに実施を要請

（１）　各拠点までの体制構築
（２）　チェックリストの実施
（３）　未対策項目の実施計画立案

専務通達で全社方針を徹底

「製造システムにおけるサイバーセキュリティ対策の徹底について」

役員通達 第 11(G)号
2016 年 7 月 29 日

事 業 場 長 殿

専務取締役
技術・モノづくり・調達・IT 革新総括担当

以 上

配 布 先　全 事 業 場

ガイドライン推進での問題点

参照したガイドライン等に記載ある一般的対策のはずですが
実際に工場で実施しようとすると様々な問題が

現場からの声

・FWって何？　どこに置くの？　工場のネットワーク図面がない
・２要素認証？　証明書がいるの？　発行管理って誰が、どうやるの？
・ネットワークセグメントを別ける？
　アプリに組み込んであるのでＩＰアドレス変えれない！
　工場ではレイアウト変更があるので、継続変更管理が大変
・工場ネットワークに接続されている機器が把握できていない
・想定している通信ってどんなの？製造時の通信内容って知らない

情報セキュリティ・情報システム屋で常識のコントロールを
そのまま工場へ適用するのは難しい

工場で実行可能な具体的対策になるよう、いくつかの拠点を
モデルに実装・運用方法も含めて検討を継続中。

製造システムセキュリティの取り組み（具体的対策）

②工場で異常を検知出来るしくみの導入

②工場で異常を検知出来るしくみの導入

論文・発表等	情報収集	製造システムの状況
ホワイトリスト型検知 ふるまい検知（IDS/IPS等） 機械学習　etc.	JPCERT/CC/CSSC等の資料 各種セミナー・講演会 ベンダーへのヒアリング	製造装置　OS種類・バージョン 製造システム仕様 製造システム稼働状況

個々の設備毎の検知のしくみ導入対応は工数がかかり無理

接続されている機器に依存せず異常検知が出来るよう
ネットワークレベルで取得出来る情報を利用ししくみを構築

工場調査（物理構成）

物理構成・配線・機器配置
工場にて実地調査

多くの装置がネットワークに接続
エッジスイッチは管理されていない
機器の接続状況が不明

サーバー

製造工場

ＭＥＳ・ＳＣＡＤＡ・ＨＭＩ

フロア
スイッチ

エッジスイッチ

エージングライン

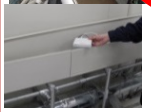
エッジスイッチ

実装ライン

エッジスイッチ

エッジスイッチ

エッジスイッチ



検査ライン

トレーザビリティ

エッジスイッチ

組み立てライン

工場見える化

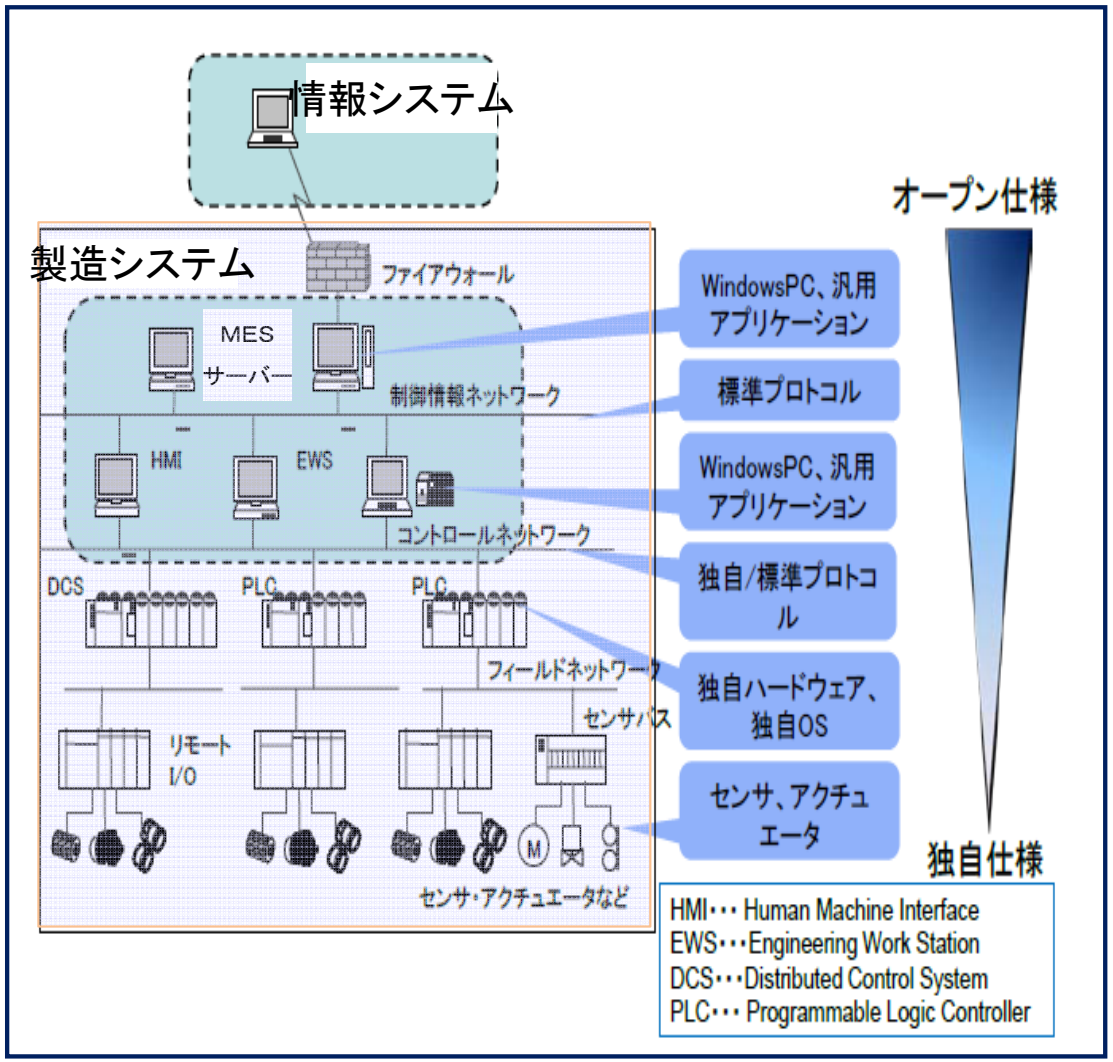
機器リスト

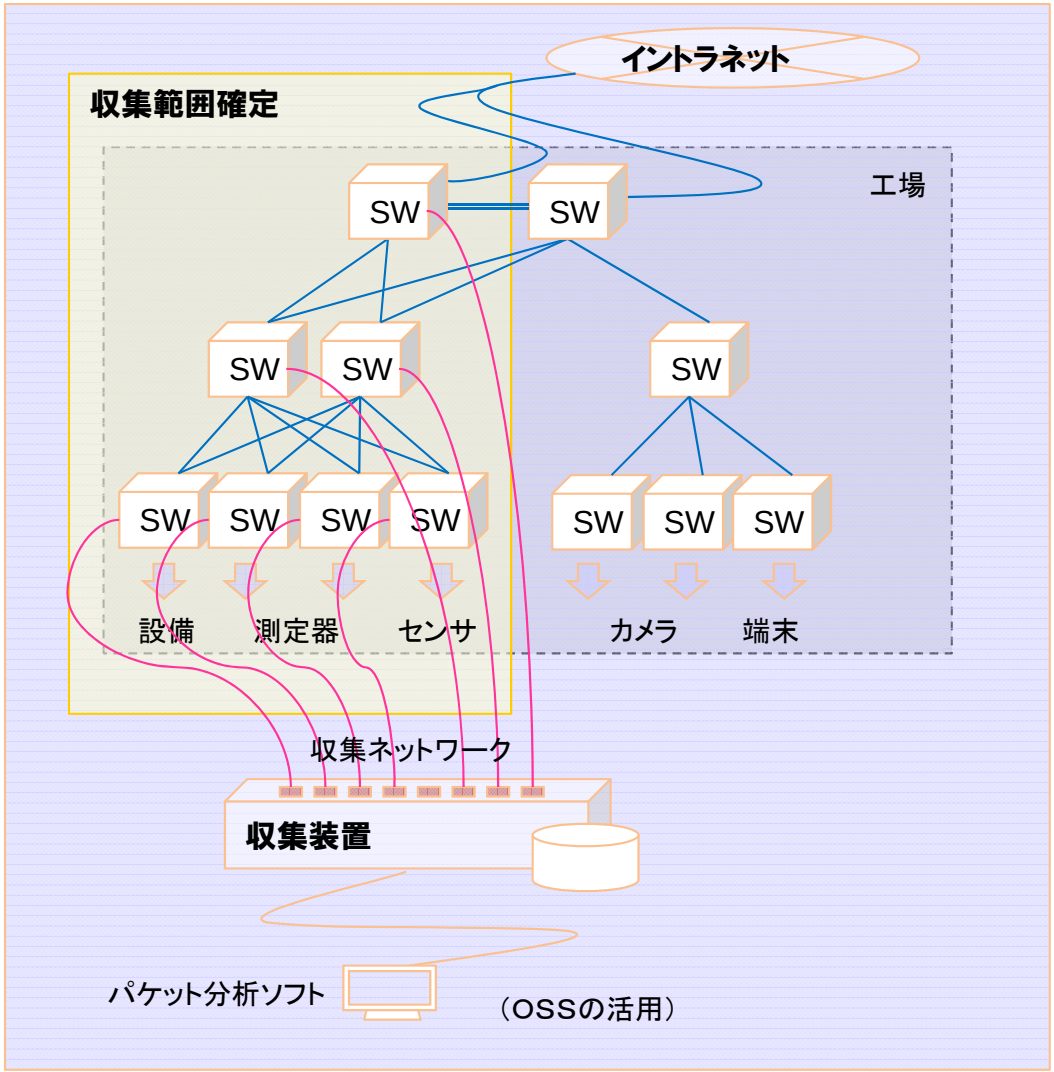
×

工場調査（通信）

工場の通信パケットを収集（7拠点）して通信がどうなっているのか調査

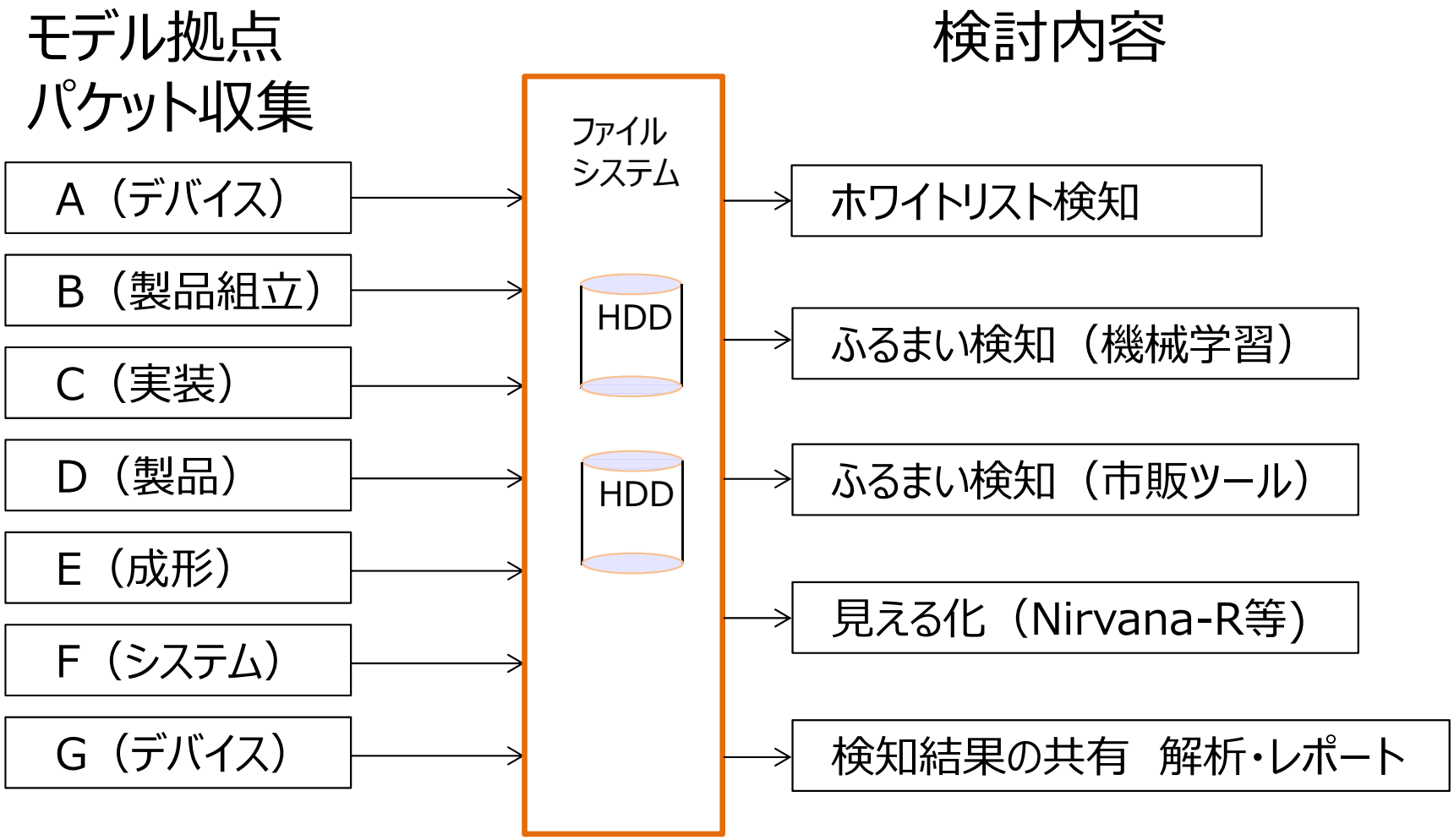
工場での通信状況が見える化
異常検知の検討に活用中





異常検知システムの検討

7拠点を選定
通信パケット取得のしくみ導入



製造システムセキュリティの取り組み（具体的対策）

③インシデント対応の確立

③インシデント対応の確立

異常を検知した際に、早急に工場を復旧・対策できる体制・しくみを構築

インシデント情報の伝達と意思決定のしくみ
インシデント情報を分析・判断できる人材の育成
製造システムセキュリティを推進できる人材の育成

2017年度
より開始

拠点推進人材

教育プログラム・ツール
訓練

カンパニー（４） → 事業部（３７） → 拠点（約311）

エキスパート人材の育成

開発要員？（＊人）
SOC要員？（＊人）
→ 検討中
- 社内育成
- 社外との連携

最後に

終わりに

スマート工場化への取り組みが各社で増加している中
製造システムへのサイバー攻撃のリスクが見えてきている。
被害を受けた時の経営へのインパクトは大きい
スマート工場で経営効果を得るためには今からスタート

生産技術者が製造現場のIT基盤に責任

情報システム・情報セキュリティとの連携体制

サプライチェーン全体での対策・連携

ご清聴ありがとうございました

Worldwide Olympic Partner

Panasonic