MITSUBISHI ELECTRIC
Changes for the Better

ITソリューションで、エコチェンジ。

特定非営利活動法人デジタル・フォレンジック研究会　御中

研究会1
「組織内の重要システムへのサイバー侵害とデジタル・フォレンジック」

「OT領域に対するサイバー侵害（内部侵害）とフォレンジックの重要性」

2020年12月7日
三菱電機インフォメーションネットワーク株式会社
氷見　基治

1．はじめに（市場背景・動向の変化）

新たな脅威、本格的な危機管理経営へ

危機・安全管理に新たな脅威（ヒト）

✓ 接触制限＋行動管理（フォレンジック）、等

＋

サイバー感染拡大（モノ＋カネ）

✓ 新たな感染対応から、IT環境変化に伴い、攻撃多様化
✓ 施設・設備への火災・爆発・操業停止など被害など

2. 日本の危機・安全管理（製造現場の事例）

爆発火災事故から学ぶ（日本の現場力）

1. 保安・品質のカイゼン活動（常に、5なぜ、QC、ヒヤリハット、等を現場で）
2. 原因として、
   - A) 機器・設備は故障する、作業員がルールを守らない（誤判断・誤操作）
   - B) 技術の問題、管理の問題

注：中央労働災害防止協会（中防災、JISHA）などで定義・発表内容を参考

例えば、爆発火災を発生させる要因として、

- A) 作業・操作の不具合（人はミスをする：ヒューマンエラー）
- B) 設備・機器の不具合（機械は壊れる）
- C) 外部要因（自然災害、停電など）
- D) 異常反応（意図していなかった化学反応）

3. 製造現場の危機・安全管理（今後・将来）

サイバー攻撃拡大（モノ＋カネ）

- 海外で不審な爆発事故
  （安全管理の火災・爆発事故に類似）
- 製造停止、操業停止の事故
  （設備トラブル：チョコ停、ドカ停に類似）　等

爆発火災を発生させる要因

A) 作業・操作の不具合（人はミスをする：ヒューマンエラー）

B) 設備・機器の不具合（機械は壊れる）

C) 外部要因（自然災害、停電など）

D) 異常反応（意図していなかった化学反応）

保安・品質の原因に「サイバー攻撃」ならば？？？
真の原因追及となるか？？？？？

発生要因がサイバー攻撃ならば！

A) 機器・設備は故障させる

B) 作業員がルールを意図せず、
誤判断・誤操作させる

C) 技術の問題、管理の問題にすり替え

A) 作業・操作の不正・乗っ取り（Arpスプーフィング）

B) 設備・機器の停止（DOS/DDOS攻撃など）

C) 停電の発生（電力供給網へのサイバー攻撃など）

D) 異常化学反応の発生（異常制御データ投入など）

4. 製造現場のOTとは（規格と日本現場の実態）

規格（海外）のOTとは

OTとは、
Operational Technology
（オペレーショナルテクノロジー）

Operational、即ち
「運用」では。

「運用」とは
「産業用制御システムの運用」

24時間365日安定運用の監視と言えます。

注：産業用制御システム（ICS）は、NISTから
「NIST SP800-82」で開示されています。

日本現場の実態とは

日本の「産業用制御システムの運用」とは、
「現場力、安全安定安心の運用」の
「運用システム」

日本の「運用システム」は、
1970年代初頭から「イーサネット」技術を活用し、
「レガシー(歴史・安定)運用」では。

「レガシー(歴史・安定)運用」とは、
現場の運用者が一目で気付く、
『変化観察型の運用システム』
と言えるのでは。

5. OTで発生するサイバーインシデント影響

3章説明の製造現場の危機・安全管理のサイバーインシデント影響は、NIST SP800-82、で説明されています。

IEC62443だけでなく、NIST SP800-82 Rev.2 産業用制御システム（ICS）ガイドラインがあります。
参照URL：https://www.jpcert.or.jp/research/2016/NISTSP800-82r2_20160314.pdf

- 同ガイドラインの「4.1.2 Potential Consequences (生じ得る結果)、68ページ」で定義されています。

● **Physical Impacts.（物理的影響。）**
- ✓ 最悪の結果として人の負傷や死亡が生じ得る。
- ✓ そのほか資産の喪失（データ等）や環境破壊等がある。

● **Economic Impacts.（経済的影響。）**
- ✓ 物理的影響から派生する二次的影響で、システム運用に影響を及ぼす。
- ✓ その結果施設、組織その他ICSに依存するものに対し、更に大きな経済的損失をもたらす。
- ✓ 重要インフラ（電力、輸送等）が利用不能になると、システムの直接の物理的損害をはるかに越えた経済的影響が生じる。
- ✓ その結果、地元、地域、国家、さらには世界経済に悪影響が及びかねない。

● **Social Impacts.（社会的影響。）**
- ✓ これは別の二次的影響で、組織に対する国民の信頼感が失われる結果生じるが、見過ごしにされがちである。
- ✓ しかし、ICSインシデントから生じ、実に現実的な結果である。

① **国家安全保障への影響—テロ行為を助長する**
Impact on national security—facilitate an act of terrorism.

② **1か所又は複数同時サイトにおける生産の減少・喪失**
Reduction or loss of production at one site or multiple sites simultaneously.

③ **従業員の負傷・死亡**
Injury or death of employees.

④ **共同体構成員の負傷・死亡**
Injury or death of persons in the community.

⑤ **装備品の損害**
Damage to equipment.

⑥ **危険物の放出・流用・盗難**
Release, diversion, or theft of hazardous materials.

⑦ **環境破壊**
Environmental damage.

⑧ **法的要件の侵害**
Violation of regulatory requirements.

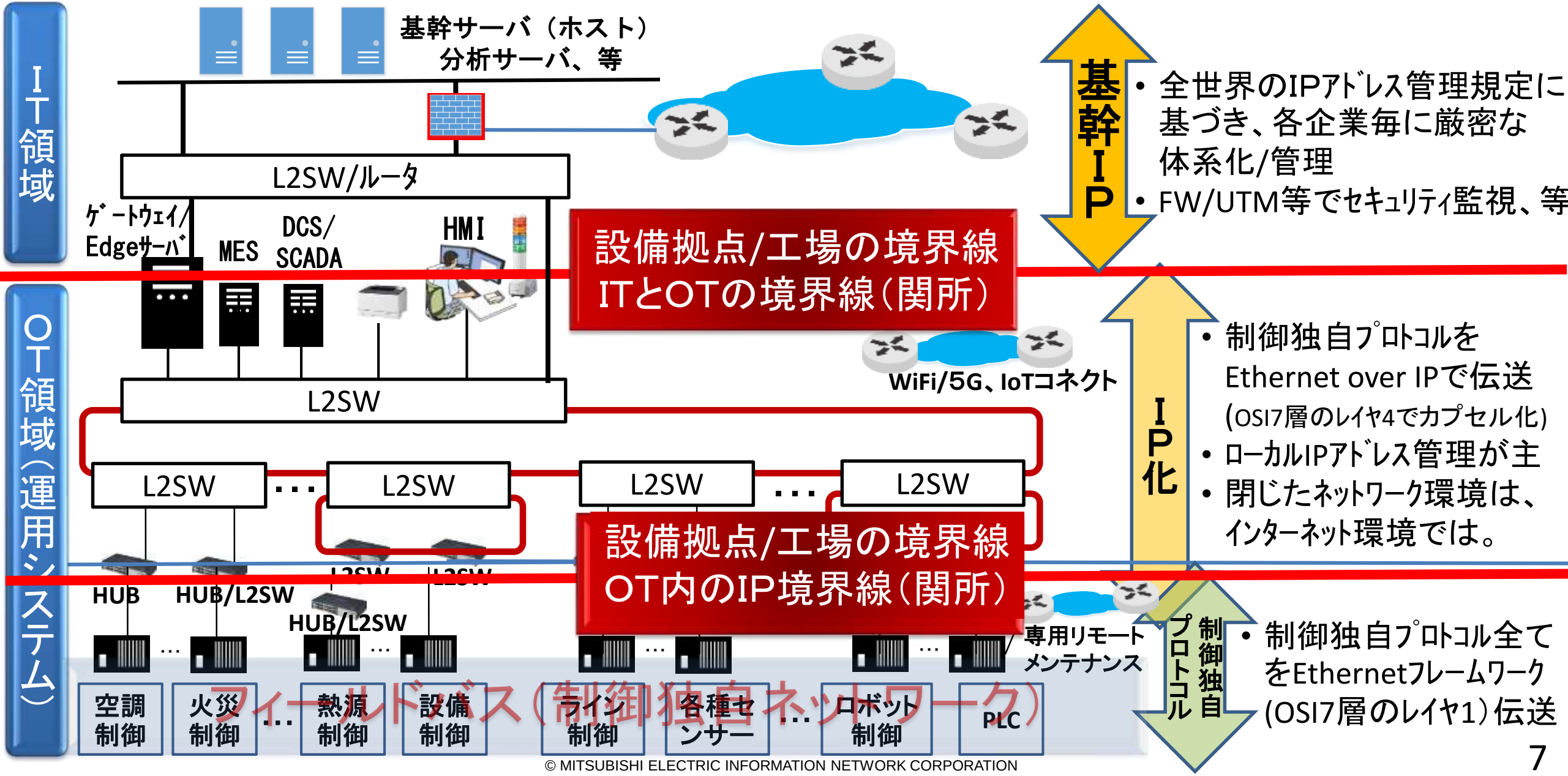
⑨ **製品の汚染**
Product contamination.

⑩ **刑法又は民法上の責任**
Criminal or civil legal liabilities.

⑪ **専有・秘密情報の喪失**
Loss of proprietary or confidential information.

⑫ **ブランドイメージ・顧客の信用の喪失**
Loss of brand image or customer confidence.

6. ITとOT、設備拠点/工場のシステム構造



- 全世界のIPｱﾄﾞﾚｽ管理規定に基づき、各企業毎に厳密な体系化/管理
- FW/UTM等でｾｷｭﾘﾃｨ監視、等

- 制御独自ﾌﾟﾛﾄｺﾙをEthernet over IPで伝送
  (OSI7層のﾚｲﾔ4でｶﾌﾟｾﾙ化)
- ﾛｰｶﾙIPｱﾄﾞﾚｽ管理が主
- 閉じたﾈｯﾄﾜｰｸ環境は、ｲﾝﾀｰﾈｯﾄ環境では。

- 制御独自ﾌﾟﾛﾄｺﾙ全てをEthernetﾌﾚｰﾑﾜｰｸ(OSI7層のﾚｲﾔ1）伝送

6. OSI7層と「機器、ハッキング検知/遮断」の関係

	NW機器	検知/遮断機器		バックドア/内部侵入後のハッキング手法、等
	HUB/L2SW	FW	UTM	システムコマンドレベル
レイヤ7: アプリケーション層	ー / ○	○	○	
レイヤ6 プレゼンテーション層				
レイヤ5 セッション層	ー / ○		△	
レイヤ4 トランスポート層	ー / ○	△	△	攻撃対象みつける: ポートスキャン:ポート番号(約65,000)
レイヤ3 ネットワーク層	△ / ○	△	△	攻撃対象みつける ポートスキャン:IPアドレス(約37億)
レイヤ2 データリンク層	○ / ○	△	△	機器なりすまし ARPプロトコル応答
レイヤ1 物理層	○ / ○ Ethernet対応	注 ○:レイヤ7で主処理 △:レイヤ7が参照しているレイヤ		

注:ハッキング手法コマンドを検知/遮断できない事もあると言われています。

レイヤ4が設備拠点/工場の境界線
ITとOT、OT内の境界線(関所)

- **第7層 - アプリケーション層**
  HTTP,DHCP,SMTP,SNMP,SMB,FTP,Telnet,AFPX.500
- **第6層 - プレゼンテーション層**
  SMTP,SNMP,FTP,Telnet,AFP
- **第5層 - セッション層**
  TLS,NetBIOS,NWLink,DSI,ADSP,ZIP,ASP,PAP,名前付きパイプ
- **第4層 - トランスポート層**
  TCPUDPSCTPDCCPSPXNBFRTMPAURPNBPATPAEP
- **第3層 - ネットワーク層**
  IP,ARP,RARP,ICMP,IPX,NetBEUI,DDP,AARP
- **第2層 - データリンク層**
  イーサネット,トークンリング,アークネット,PPP,フレームリレー
- **第1層 - 物理層**
  RS-232,RS-422(EIA-422,TIA-422),電話線・UTP,ハブリピータ,無線.光ケーブル

7．OODAループのObserve（観察）とフォレンジック機能

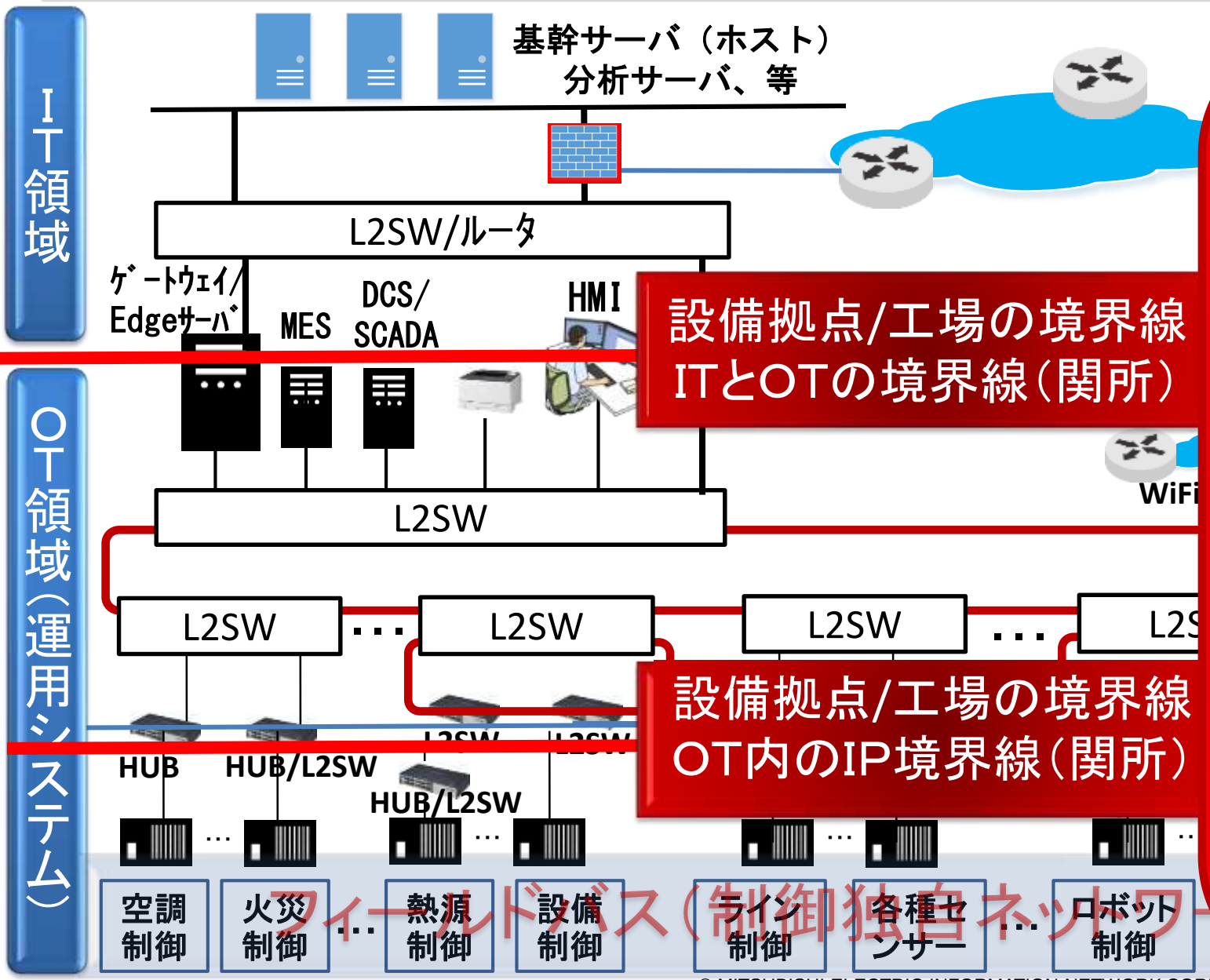
OODAループの第一歩「**Observe（観察）**」の考えは、日本現場力のOT領域で日々実施されている『**変化観察型の運用システム**』と同じと言えるのでは。

「レガシー(歴史・安定)運用」とは、
現場の運用者が一目で気付く、
『変化観察型の運用システム』
と言えるのでは。

観察方式は？

OT領域の特性、OSI7層のレイヤ2～4、を中心に観察（変化を捉え、五感通知）の『**ネットワーク型のフォレンジック機能**』ではないか！

8. OT領域のObserve（観察）型ﾌｫﾚﾝｼﾞﾝｸﾞ機能（想定）



実現方式（想定）

① 境界線（関所）/ｺﾈｸﾄ部分のL2SW間でﾌｫﾚﾝｼﾞﾝｸﾞ監視NWを新設(既設NWならNW分離/優先制御など)。

② ﾌｫﾚﾝｼﾞﾝｸﾞ監視NWは、接続L2SWをRSPAN機能などで接続し、ﾌｫﾚﾝｼﾞﾝｸﾞ分析機器にNWﾃﾞｰﾀを伝送

③ 伝送NWﾃﾞｰﾀと該当L2SWのｺﾝﾌｨｸﾞﾚｰｼｮﾝ情報と相関分析など自律型分析ｴﾝｼﾞﾝと検知表示型方式(気付き方式等)

④ IT領域のCSIRT/SOCがObserve（観察）型ﾌｫﾚﾝｼﾞﾝｸﾞ機能で運用

FIN