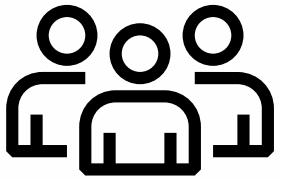
ABB BAILEY JAPAN 3.FEB 2022

制御システムエンジニアによる実践的な制御システム復旧計画

ABB日本ベーレー　デジタル技術部　大石貴之
(情報処理安全確保支援士　登録番号 第018981)

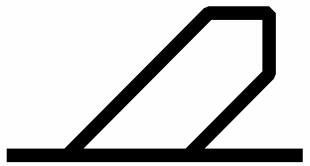
ABB in Japan｜ABBジャパン

技術革新のリーダー企業の1社として



従業員数

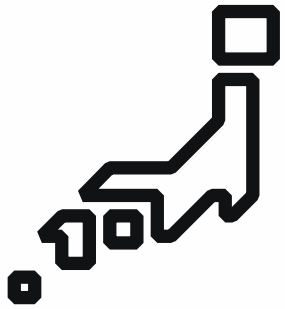
800+ 人



売上（2017）

$456 million

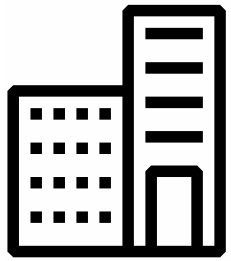
- 約502億円 ($1=¥110)



国内事業拠点

21 拠点

- ABB株式会社本社所在地：
  品川区大崎
- ABBジャパングループとして
  4事業本部、4つの合弁会社
  全国24拠点にネットワークを展開



設立

1907 年

- 日本でのルーツは、114年前。
  前身企業による横浜事務所開設

私たちの事業組織

21の事業部で構成する完全分散型のビジネスモデル

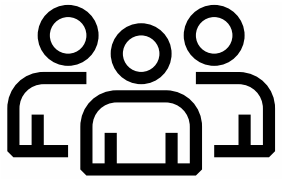
BUSINESS AREA
事業本部

DIVISION
事業部

エレクトリフィケーション	プロセス オートメーション	モーション	ロボティクス＆ディスクリート・オートメーション
			
配電ソリューション	エネルギー産業	大型モータ&ジェネレータ	**ロボティクス**
スマートパワー	プロセス産業	ドライブ	マシンオートメーション
スマートビルディング	マリン＆ポート	システムドライブ	
インストレーション機器	過給機	サービス	
パワーコンバージョン	計測・分析機器	トラクション	
E-モビリティ		MPT	
		IEC LVモータ	
		NEMAモータ	

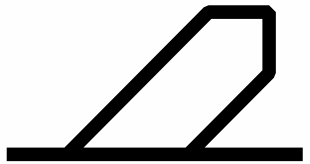
ABB Bailey Japan Ltd.| ABB日本ベーレー株式会社

火力発電向けオートメーションのマーケットリーダー



従業員数

約250 人



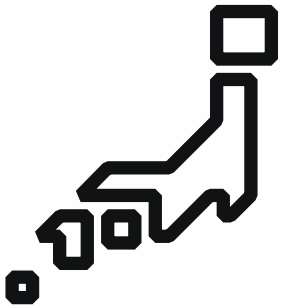
マーケットシェア

50%

- 火力発電所ボイラー制御システム

30%

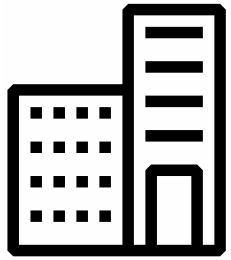
- LNG受入基地制御システム



国内事業拠点

7 拠点

- 本社所在地：**静岡県伊豆の国市**
- 全国7拠点に営業拠点を展開
- 設計・サービス機能に加えて、システム開発、製造機能も併せ持つ



設立

1971 年

- 米Bailey Meter、極東貿易の合弁会社として、50年前に日本ベーレー（株）設立
- 1999年にABBグループの一員となり、2008年より現社名へ

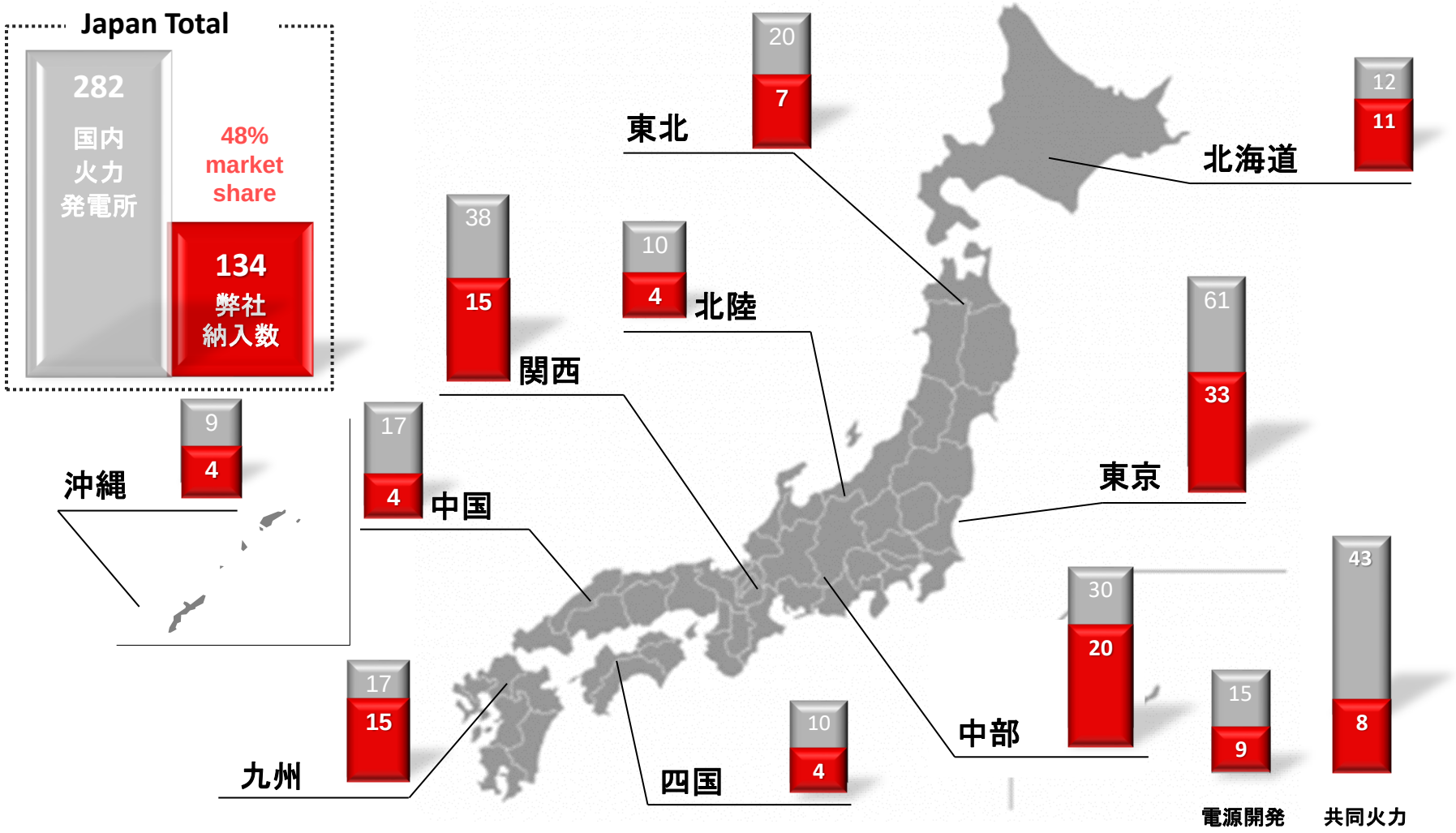
ABB日本ベーレー: 特長

納入実績

事業用発電設備

ボイラ/バーナ制御装置

LNG制御装置



自己紹介

2010 ～ 2018　DCS制御システムの設計・調整・メンテナンス業務を担当

2018 ～ 現在　制御システムのセキュリティ設計・検証・ソリューション提案・制御最適化

1. 制御システムのハーデニング
2. 脆弱性検査
3. IDS,EDRの検証
4. プロセス制御データサイエンティスト

Agenda

本日お話しすること

・制御システムへのサイバー攻撃に備え、

１．事例を知る（ランサムウェア「DARKSIDE」による米国パイプライン攻撃）

２．制御システムの特徴を知る

３．必要な準備を行う

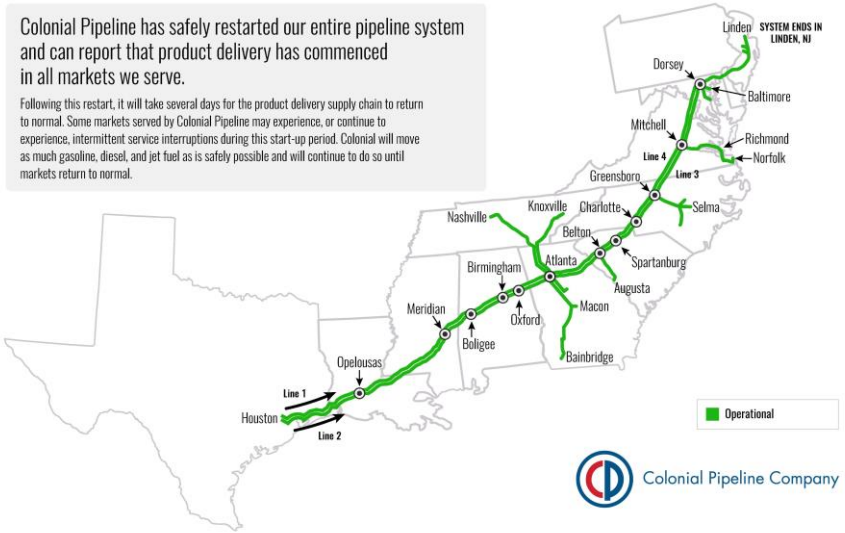
事例を知る

ランサムウェア「DARKSIDE」および米国のパイプラインへの攻撃

事象：2021/5/7 米コロニアル・パイプラインがランサムウェア攻撃によりに全面停止した。
操業開始以来、パイプラインの稼働を全面停止させたのは初めて事態となった。
燃料価格は軽微な上昇に留まったが、多くのガソリンスタンドで在庫切れを起こした。

経緯：

2021年4月29日：DARKSIDEがコロニアル・パイプライン社のコンピュータシステムに侵入
2021年5月7日：データの暗号化、身代金の要求を受け、コロニアル・パイプライン社は
パイプライン操業の一時停止を公表、同社CEOが身代金の支払いを承認。
2021年5月12日：パイプラインシステム再開、一部供給網は影響継続。
2021年5月15日：供給網全体の復旧を確認。
2021年6月7日：FBIが身代金の一部を押収。



ランサムウェア「DARKSIDE」および米国のパイプラインへの攻撃

攻撃フェーズ





1.侵入

-VPNシステムのアカウント及び、パスワードが盗まれ攻撃者に侵入されたと報告。

2.探索

数週間から数か月かけて組織のネットワークを詮索。複数の部門のネットワークに侵入

3.情報流出

攻撃者は窃取したファイルをクラウドストレージに100GB程度のデータをアップロード

4.暗号化

攻撃者は拡張子の変更、暗号化を行いコンピュータを操作不能にした。

⇒OTネットワークへの影響範囲が不明であったがパイプライン全停させた。

5.脅迫

暗号化ファイルの復元と情報流出を人質に金銭を要求した。

4重脅迫

1. ファイルを暗号化
2. 情報流出
3. DDosターゲット
4. メール攻撃

事件関係者・有識者のコメント

1. VPNログインは多要素認証を有効としていない従業員のユーザー名とパスワードが使用された。このプロファイルは使用されていないと考えられてた。パスワードは比較的複雑なものであるが、この認証情報は以前に別のウェブサイトで使用していた可能性があり、それを攻撃者が利用したと考えられる。

2. 最終的な復旧にはバックアップデータを使用したが破損しているか、危険に晒されていたのか、使用して安全だったのかが不確かであったとして身代金440万ドルの支払いを決めた。

3. DarkSideには制御システムに関与しパイプラインをシャットダウンする機能はありませんが、この攻撃や他の攻撃では、攻撃の影響や対応方法がわからないため、オペレーターはOTの生産全体をシャットダウンすることになります。

- パスワードポリシー
- アカウントの棚卸
- 従業員への注意喚起

- 日常点検
- バックアップの取得
- 復旧作業のトレーニング

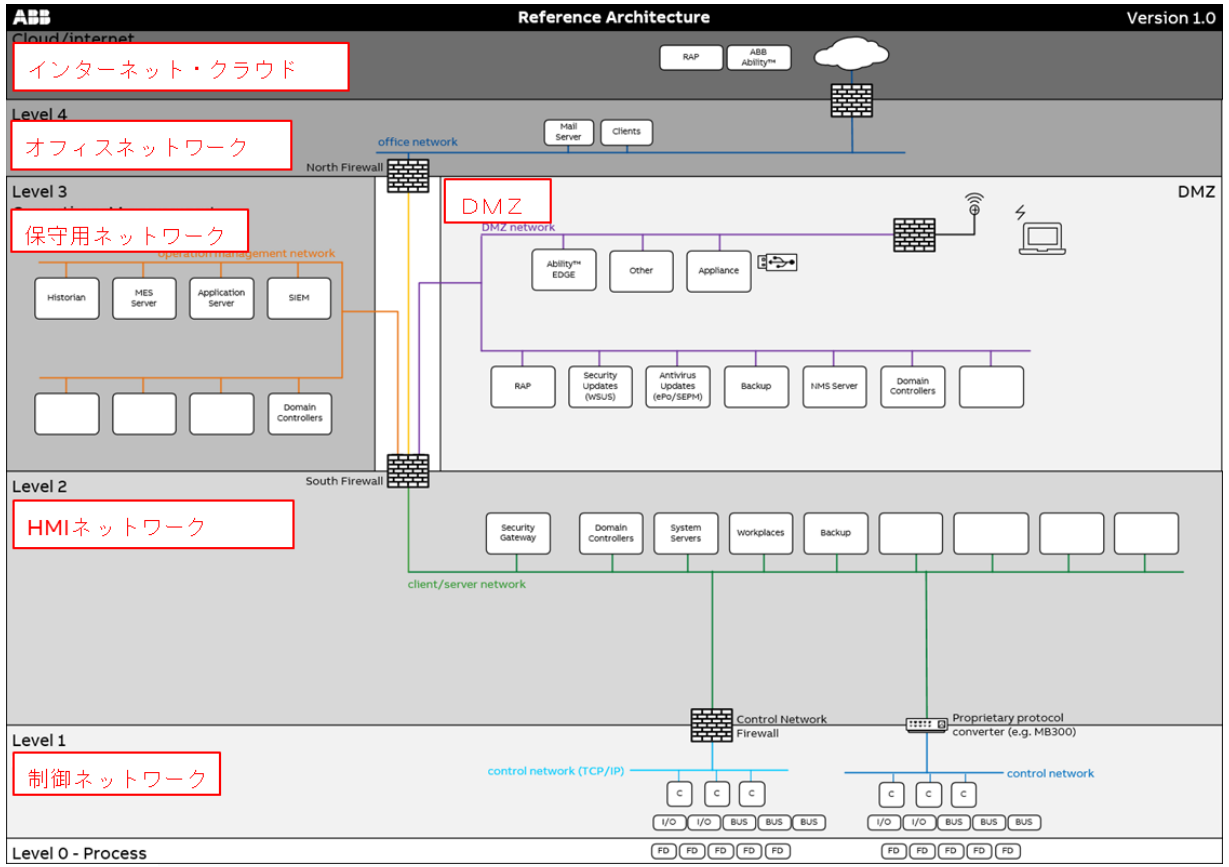
サイバー攻撃を受ける想定と準備、システムの理解が最も重要である。

出典:
https://www.techtarget.com/searchsecurity/news/252502216/Mandiant-Compromised-Colonial-Pipeline-password-was-reused
Colonial Pipeline hack no cause for panic about infrastructure attack (cnbc.com)

制御システムの特徴を知る

制御システムネットワーク

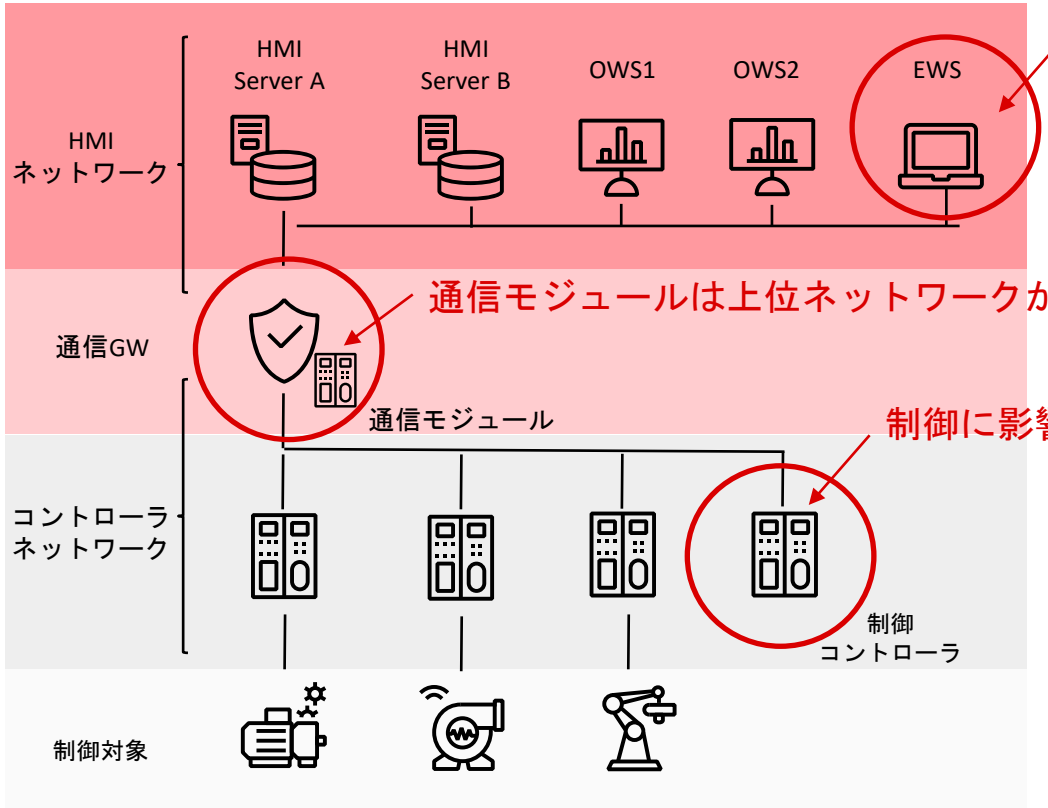
制御装置のシステム構成、動作環境を把握することで復旧に必要な準備をする。



本内容は全ての製品・システム構成に該当するものではありません。

制御システムネットワーク

制御装置のシステム構成、動作環境を知り復旧に必要な情報を知る。

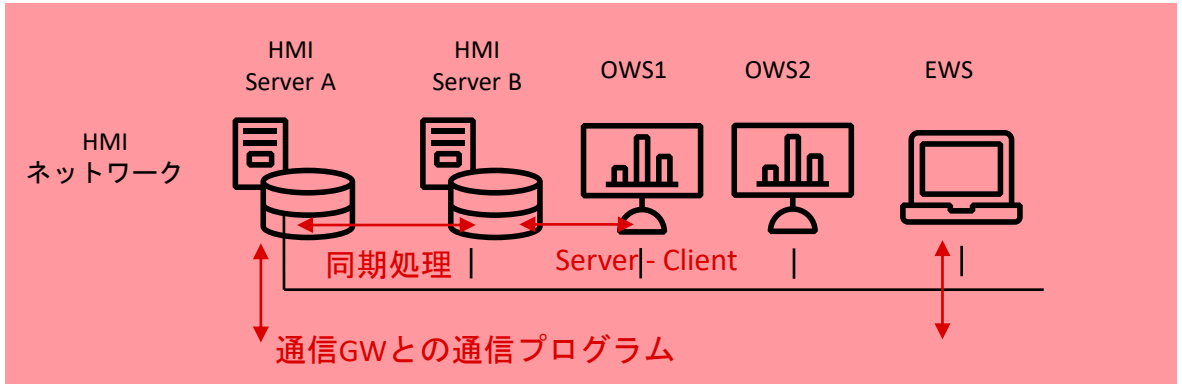


ランサムウェアはどこまで広がるか？

通信モジュールは上位ネットワークからの侵入を防げるか？

制御に影響を及ぼす改変とは？

HMIネットワーク



資産の特徴

- 汎用OS(Linux , Windows)が使用される。
- 冗長化構成のServer A, Bは同期処理のため同一ネットワークに配置される。
- 複数台のOWSもServer A,Bと同一ネットワークに配置される。
- EWS,HMIServerはコントローラへのコマンド発生機能を持つ。

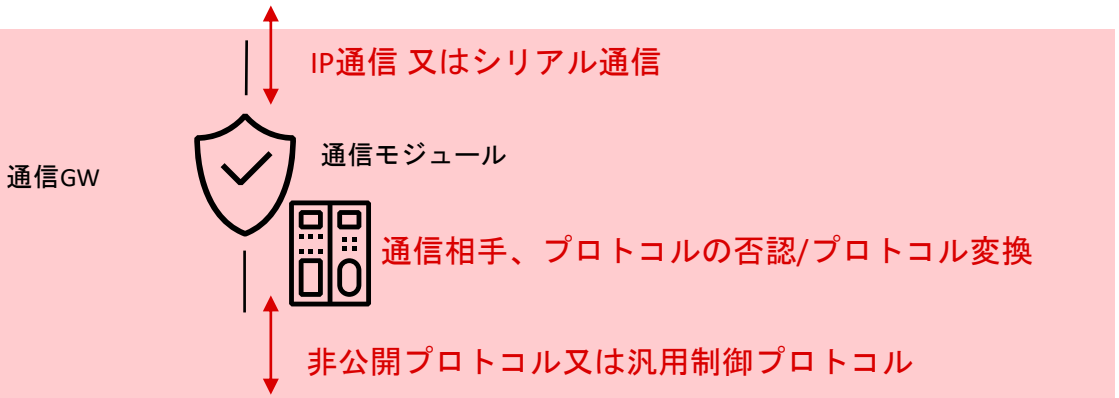
機能・構成

- オペレータはOWSを使用しプラントの状態把握、操作を行う。
- HMIServer – OWS はサーバクライント関係
- EWS – HMIの保守及び、コントローラの保守を行う。
- 可用性を重視し各装置複数台の冗長化構成としている。

注意点

- 様々な脆弱性が発見される汎用OS
- 機能冗長化構成ではあるがホットスタンバイが前提となるため横展開に弱い。
- EWS,HMIServerの既存機能を悪用することでコントローラネットワークに変更を加えることが可能
- セキュリティログがどの程度詳細に取得されているか

通信GW



資産の特徴

- **独自OSではあるが、組み込みRTOSを使用して開発される通信モジュール（VxWorks,codesys等)**
- 特定のプロトコルのみ変換可能であり、実質的なファイアウォール相当の機能を持つ。

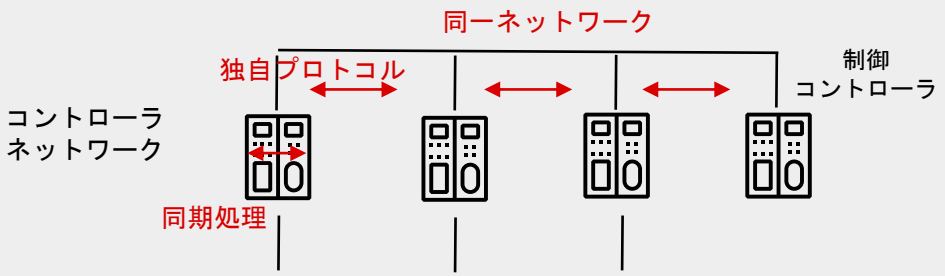
機能・構成

- HMIネットワーク-コントローラネットワークの通信を行う。
- コントローラネットワークとの通信は必ずこのモジュールを経由
- HMIネットワークに対してシリアル通信、IP通信、
  コントローラネットワークに対して非公開プロトコルや
  汎用制御用プロトコルで通信される。
- コンピュータ資産と1対1の構成が多い

注意点

- コンピュータ資産と1対1の構成が多く横展開のリスク低い
- コントローラネットワークが同一ネットワークで構成されるため、1ヶ所から全てのコントローラにアクセス可能。
- 組み込みRTOSで構成され、過去にも脆弱性が発見されている。通信障害やコントローラに対して干渉される可能性がある。

コントローラネットワーク



資産の特徴

- 独自OSではあるが、組み込みRTOSを使用して開発されるコントローラモジュール（VxWorks,codesys等)
- ファームウェアの更新はハードスイッチにより保護される場合がある
- 設定値の変更はリアルタイムに実施できる

機能・構成

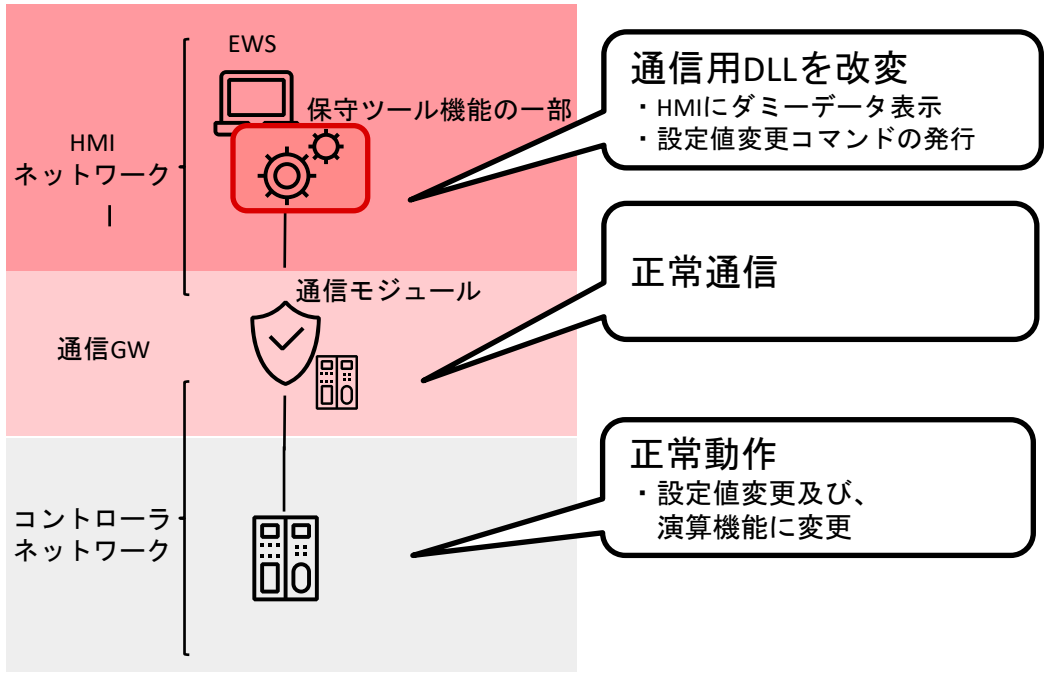
- 内部ロジックの計算、IO処理、冗長化同期処理等を既定時間毎安定的に実行する。
- コントローラ内部の機能構成はプラント毎異なる。
- コントローラ間の通信は独自プロトコルで行われる。

注意点

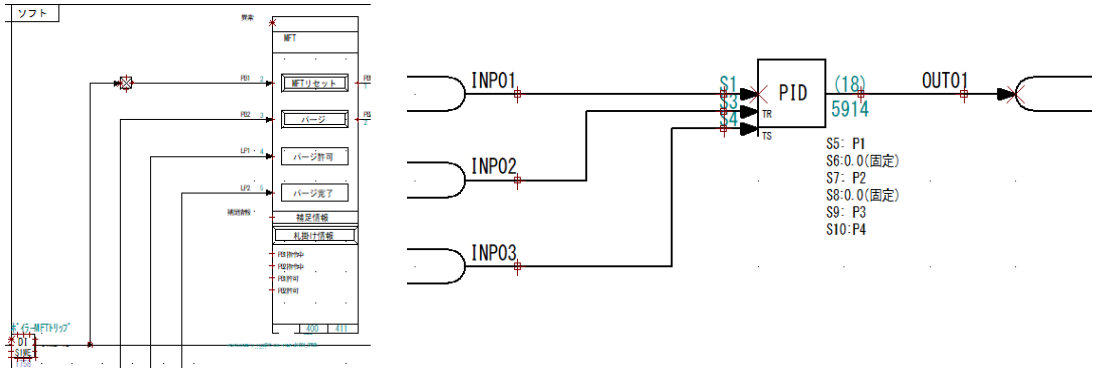
- コントローラは同一ネットワーク上のコントローラと通信可能であり、1つの変更がネットワーク上すべての動作に影響を及ぼす。
- 組み込みRTOSで構成され、過去にも脆弱性が発見されている。通信障害やコントローラに対して干渉される可能性あり。
- 設定値変更であってもプラント運転に多大な影響を与える
- コントローラ側に変更履歴を保持する機能がない。

設定値変更によるプラント運転への影響

STUXNET



PIDコントローラ・インターロック信号



- アナログ制御はPIDブロックを用いて行われる。この設定値を変更することで目標値に対する追従性を悪化させることや急激な動作により機器を破損させることが可能。
- 機器やユニットの保護のためにインターロック回路を構築している。
- 重要なインターロック信号の模擬や、閾値を変更することで、プラントを自動停止や、再起動不可に陥れることが可能。

サイバー攻撃に対しての制御システムの特徴

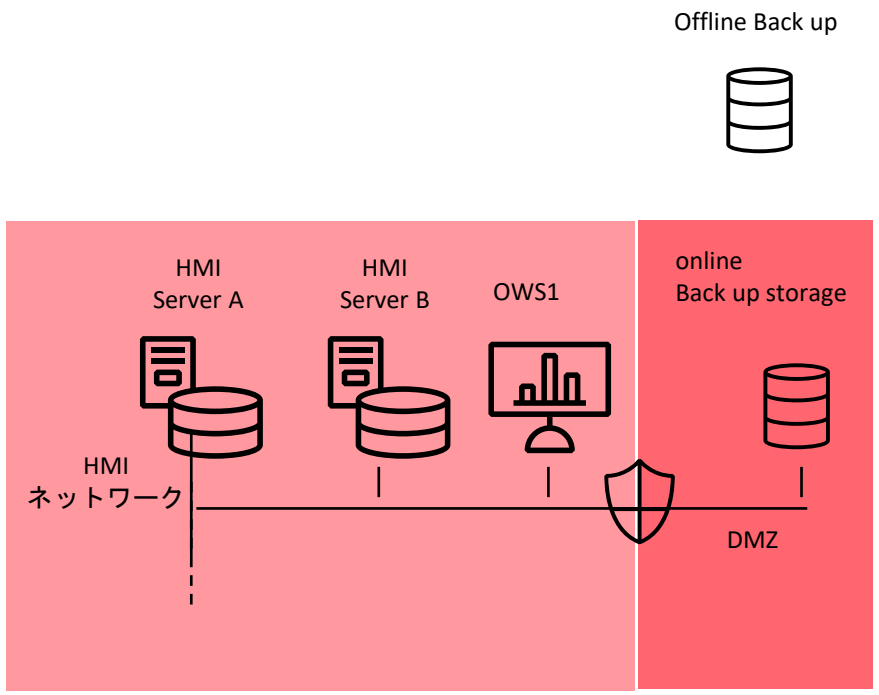
HMIネットワーク	・機能冗長化構成ではあるが資産は同一ネットワーク上に置かれる場合が多く横展開に弱い。 ・保守端末に限らず、コントローラネットワークとの通信プログラムはインストールされており、コントローラネットワークへの侵入口になりえる。
通信GW	・組み込みRTOSで構成され、過去にも脆弱性が発見されている。通信障害やコントローラに対して干渉される可能性がある。 ・HMIネットワーク-通信モジュール間はIPプロトコルで通信されており傍受は可能 ・HMI資産と通信モジュールは1対1の構成であり横展開のリスクは低い
コントローラネットワーク	・コントローラは同一ネットワーク上のコントローラと通信可能であり、1つの変更がネットワーク上すべての動作に影響を及ぼす。 ・コントローラ側に変更履歴を保持する機能がない。 ・設定値変更によりプラント制御動作に大きく影響を与える。

必要な準備を行う

HMIネットワーク

横展開リスクに備えたオンライン・オフラインバックアップの準備

推奨構成



オンラインバックアップストレージ

- HMIネットワーク上の機器について、バックアップをスケジュールする。
- 保存ストレージをHMIネットワーク上に置かない。
- 可能な限りHMIやEWSと異なるOSを利用する。
- バックアップ動作中は通信データ量が増加する。HMI動作に影響を及ぼす可能性があり、メーカとの協調が必要。

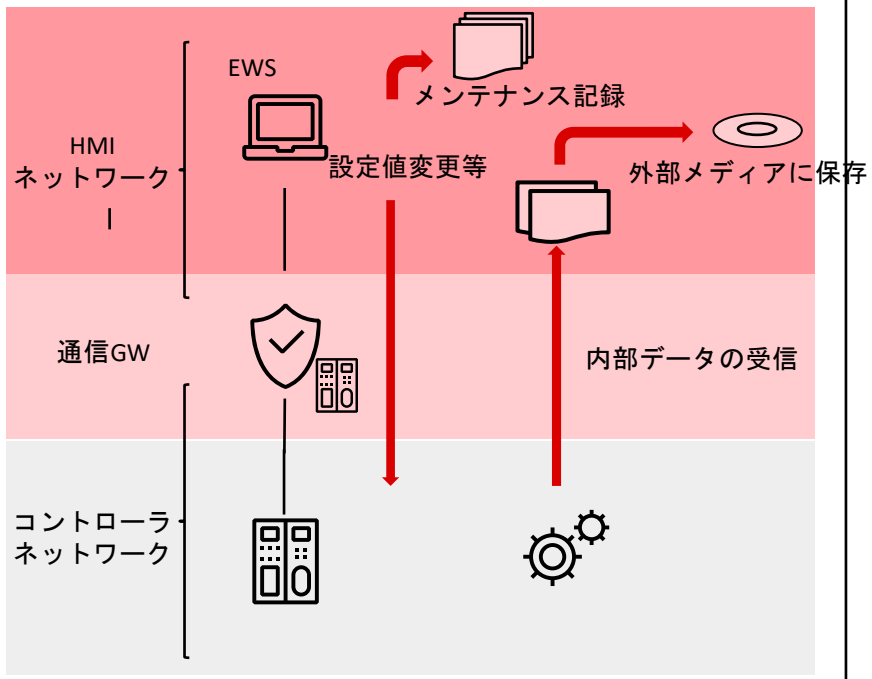
オフラインバックアップストレージ

- 横展開による感染を考慮しオフラインバックアップは推奨。
- 更新頻度は運用次第だが、コントローラ側に変更を加えた際は必ず取得する。
- 使用しているコンピュータに対応するHDDストレージを用意する。
- リストアした状態で保管。
- 最低減のオペレーション可能な構成。

コントローラネットワーク

コントローラ内部への干渉に備えた「定期的な内部データ受信」と「変更内容の比較」

推奨構成



定期的なコントローラ内部データ受信

- コントローラの中のパラメータとEWS内のパラメータを常に一致させる。
- コントローラ内部の演算プログラム及びパラメータは定期的に受信しバックアップデータを作成する。
- バックアップデータは外部メディアに保存し保管する。

変更内容の比較

- 使用機器により受信データとバックアップデータを比較する手順を明確にする。
- 設定値変更等のメンテナンス作業はメンテナンス記録として残す。

メーカやメンテナンス部門との協調

制御システムによって適切なメンテナンス、サポートが異なります。

- 緊急事態発生時に期待できるサポートは?
  - -連絡先や、メーカのサポート体制
  - -メーカ推奨の復旧方法、アイソレーション、証拠保全方法
  - -復旧に必要な機能と期間の把握
  - -どのようなセキュリティログが残るか
  - -予備品の確認
  - -故障との見極め　->　通常制御状態の状態を保存・把握する。

- 日常的に実施すべきメンテナンスは？
  - -推奨される日常保守
  - -保守契約
  - -トレーニング（復旧、システム起動）

セキュリティ対応はメンテナンス業務に含まれる。
他部門、他社と協調できる体制づくりが重要。

制御システム復旧

平常時準備

- **協力体制の構築**
  社外（装置メーカ、メンテナンス業者)
  社内（経営層、他部門）
- **制御システムの把握**
  脆弱性調査
  制御システム機能の知る
- **HMIバックアップ**
  オンラインバックアップのスケジュール
  オフラインバックアップの取得
  ハードウェアの予備品準備
- **コントローラネットワークメンテナンス**
  定期的なコントローラ内部データ取得
  メンテナンス記録
- **作業手順準備とトレーニング**

STEP 1 – メーカへの連絡

事象の連絡

証拠保全の方法

ネットワークのアイソレーション

STEP 2 – HMIネットワーク復旧

バックアップデータからの復元

アイソレーション状態で起動

STEP 3 – コントローラネットワーク復旧

内部データとバックアップデータの照合

必要なら：OS再インストール

オペレーションの段階的な復帰

- **運転状態の比較**
  主要なプロセス値
  制御状態
- **システム状態の確認**
  実行中のタスク
  コンピュータ/コントローラの負荷率
  伝送通信量
- **アイソレーションNWの段階的な復旧**

復旧計画のすすめ

いつでも自分の判断に自信を持てるように必要な準備をしておきましょう。


ABB