制御システムセキュリティの対策技術紹介
～ホワイトリストスイッチ、サイバー攻撃早期認識支援技術～

CSSC　東北多賀城本部
細川　嵩

制御システムとは

- 発電所やガスプラント、工場、ビル監視など、生活に直結する重要インフラの監視・制御等を行うシステム。
- 企業等の情報システムを支えるサーバやパソコンに加えて、PLCやDCS※などのコントローラが主要な構成要素。
- 重要インフラにおける制御システムのセキュリティ対策では、従来の情報システムとは異なる対策が必要。

※PLC(programmable logic controller)：
プログラム可能なシーケンス制御装置
DCS(distributed control system)：
分散形制御システム

制御システムと情報システムの違い

- 制御システムは社会基盤、産業基盤を支えており、社会的な影響、事業継続上の影響が非常に大きく、24時間、365日稼働を続ける可用性（A）の担保が最重要である。
- 制御システムは利用期間が10年から20年と長く、情報系のOSなどのサポート期限をはるかに超えている。

	制御システム	情報システム
セキュリティ優先度	A→I→C （可用性重視）	C→I→A （機密性重視）
システム利用期間	10～20年	3～6年程度
稼動時間	24時間365日連続稼動（無休）	休止させる場合もある。

C(Confidential)：機密性
I(Integrity)：完全性
A(Availability)：可用性

Chesapeake Bay Program/CC BY 2.0

上記の違いから

情報システムと類似する課題解決策をそのまま制御システムへ適用することは困難

制御システムの脅威

- 攻撃者からの脅威は大きく分けて、技術・物理・人に分類される。
- 上記のセキュリティの脅威を以下に例示する。

  分類の基準はIEC62443-2シリーズ(CSMS)※を参考にした。

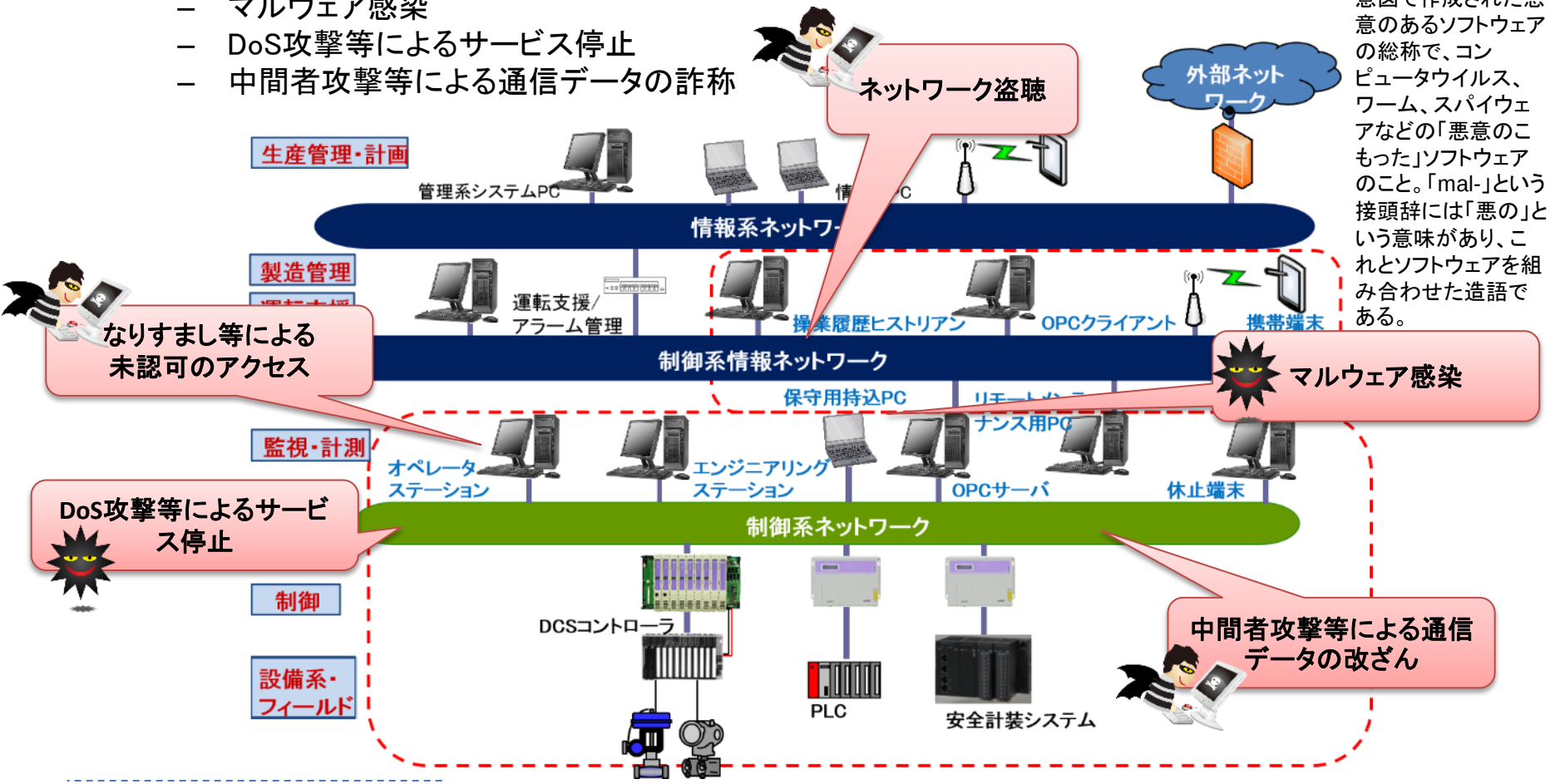
脅威の分類	保護すべき制御資産	脅威の具体例
技術	ネットワークシステム、情報システム、サーバやコンピュータ、OSやソフトウェアなど	不正アクセス、盗聴、マルウェア、改ざん・消去、DoS攻撃、なりすましなど
物理	施設、設備、装置、環境的なもの、記憶媒体など	侵入、破壊、故障、停電、災害など
人	雇用した人の管理(教育)、人的管理上の手続によるもの、パスワード等管理される情報など	誤操作、持ち出し、不正行為、パスワードの不適切管理など

※制御システム:IEC62443-2シリーズ
情報システム:ISO/IEC27000シリーズ(ISMS)

技術的脅威

技術

- ネットワーク及びネットワーク上の資産に対する脅威の例を明示する。
  - なりすましなどによる未認可のアクセス
  - ネットワーク盗聴
  - マルウェア感染
  - DoS攻撃等によるサービス停止
  - 中間者攻撃等による通信データの詐称



＊マルウェア（malware）：不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアの総称で、コンピュータウイルス、ワーム、スパイウェアなどの「悪意のこもった」ソフトウェアのこと。「mal-」という接頭辞には「悪の」という意味があり、これとソフトウェアを組み合わせた造語である。

物理的脅威

物理

- 悪意のある内部者及び外部者による、装置、情報またはソフトウェアの持出や盗難、施設への侵入、設備・装置の盗難や破壊等、さらには停電、災害の脅威により、サービスの障害・停止が発生する。

侵入

資産の管理状態（持出、廃棄等の管理）

人的脅威

人

- 従業員やその候補、契約社員などにかかわるセキュリティであり、誤操作、持ち出し、不正行為、パスワードの不適切な管理などの脅威が想定される。また、外部者による侵入や悪意のある内部犯行やパスワードの管理方法などセキュリティ意識の低い従業員の行為によりリスクが生じる。

外部者による侵入

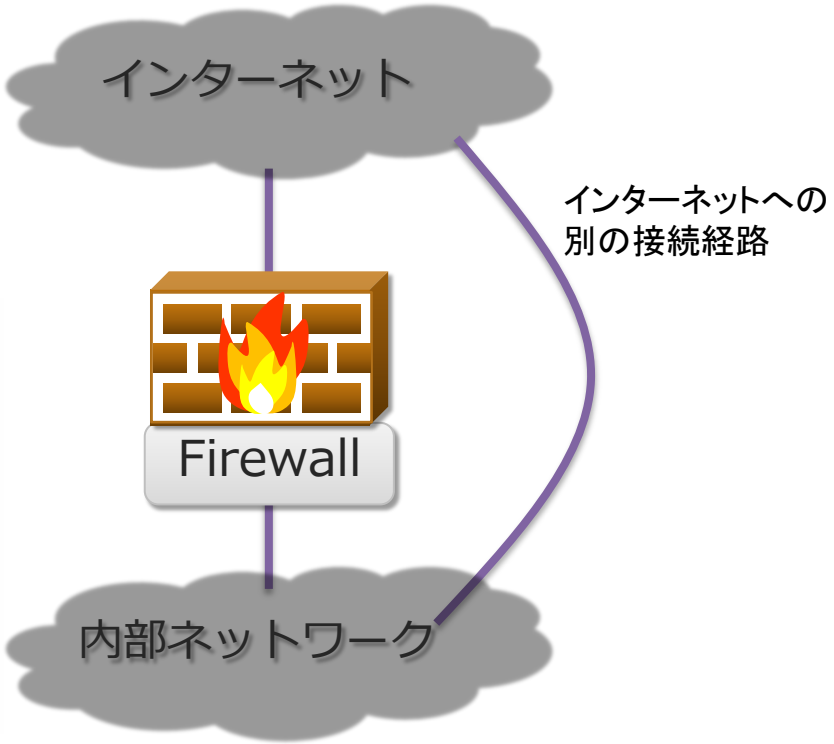
不十分なパスワード管理
持出、不正行為など

盗聴などによる漏洩

鎖の強さは最も弱い輪によって決まる

●セキュリティにも同じことがいえる。

“The strength of the chain is in the weakest link.”（鎖の強さは最も弱い輪によって決まる）ということわざは、どこか1つでも弱い輪があれば、鎖全体の強度がその弱い輪と同じ強度になってしまうという意味である。



脆弱性と脅威

守るべき資産（サービス、システム、ネットワーク、書類、データなど）
を脅かす脆弱性と脅威とは

脆弱性	システムの弱点（セキュリティ・ホールなど）
脅威	・脆弱性を悪用する攻撃者、意図しない故障や災害 ・技術的な脅威、物理的な脅威、人的な脅威に分類

「脆弱性」×「脅威」→「リスク（セキュリティ事故による影響）」の具現化

基礎知識総括

✓制御システムは情報システムと異なり、可用性が最重要

✓制御システムと情報システムは各々特徴があるため、情報システムと同じ対策を制御システムへそのまま適用することは困難

✓脅威は技術・物理・人で分類可能

✓脅威に対し、攻撃者は最も弱い箇所を複数の手段で攻撃

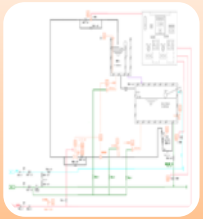
CSSCにおける研究開発の概要

1

[製品]
コントローラ等を対象にして、現状の確認・対策、およびセキュアな製品開発についての研究開発

・ホワイトリストスイッチなど

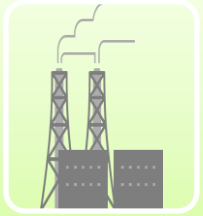
2



[システム]
(IT)システムを中心とした現状のシステムの確認・対策、およびセキュアなシステムを作るための研究開発

・ログ分析技術など

3



[プラント]
現状のプラントの確認・対策、およびセキュアなプラントを作るための研究開発

・サイバー攻撃早期認識支援技術など

4

[テストベッド]
製品・システム・プラントについて、模擬プラント等による確認・対策を実施できる環境そのものに関する研究開発

・遠隔検証環境の構築など

ホワイトリストスイッチ

ブラックリスト型・ホワイトリスト型セキュリティ対策

ブラックリスト型

動作してはいけない通信・プログラムをリスト化

- 最新のパターンファイル更新が必要
  (インターネットなどへの接続を前提)
- **システムへの負荷影響がある**

ホワイトリスト型

動作しても良い通信・プログラムをリスト化

- 機能や構成変更時にパターンファイルの更新が必要
- **システムへの負荷影響は軽微**

多くの制御システムでは・・・

- インターネットに接続されていない or 接続が許可されていない
- 古いOSで運用されており、最新のプログラムが動作保証外の場合がある
- アンチウイルスソフトウエア動作時などの負荷増大が許容されない

制御システムでは**ホワイトリスト型対策が有効**

ホワイトリストの実装検討

対象	内容
端末・サーバ	プロセスの起動順序や、IPアドレスやポートによる制限、ファイルへのアクセス制限をホワイトリストにより制御するツールの研究開発
	アプリケーションコントロールの国産制御システムへの適用可能性の検証
セキュリティ機器（ファイヤーウォール）	正規通信と非正規通信の識別で、ホワイトリストを事前登録無しに利用する機器の実証実験
通信機器（スイッチ）	フロー情報よりホワイトリストを自動作成し、登録するスイッチの実証実験

既存設備へのホワイトリスト型対策適用

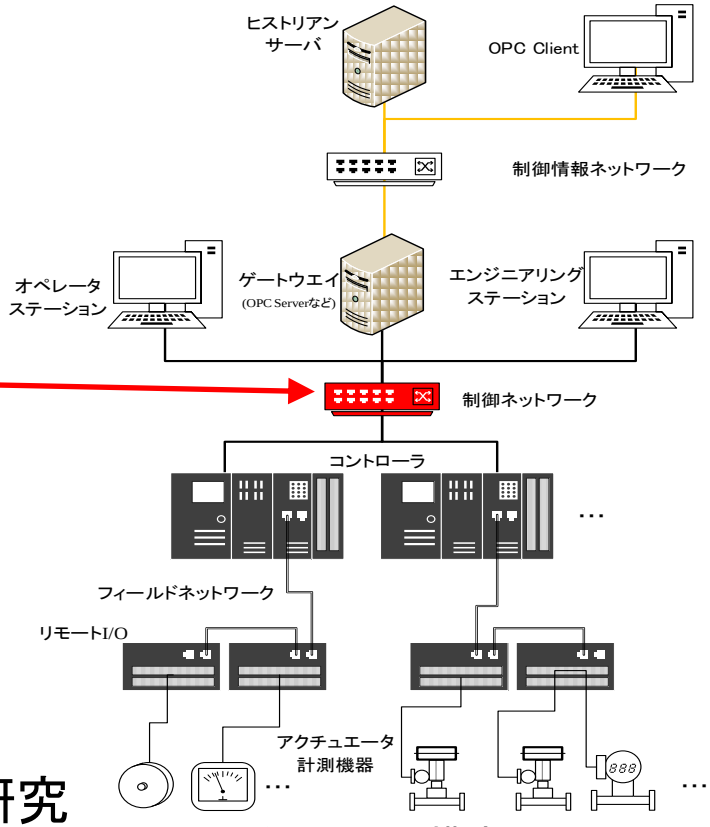
- コントローラ
- オペレータステーションなどのPC

動作台数が多く、既存設備への導入には機器や検証コストが多くかかる

- ネットワークスイッチ

コントローラやPC等に比べて台数が少ないが、制御に
関するデータが必ず通るため高い効果が見込める

制御ネットワークに適したホワイトリストスイッチを研究



制御システム構成

ホワイトリスト自動学習スイッチ

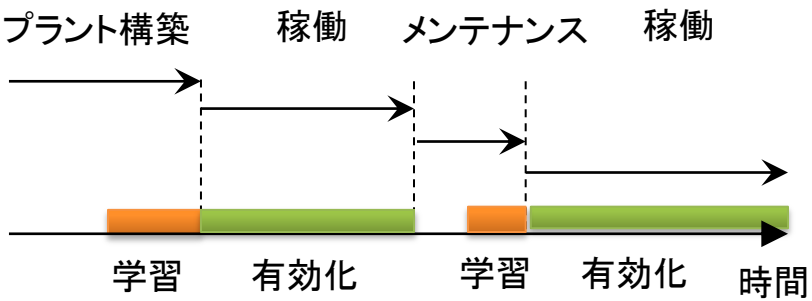
ホワイトリストを実現する技術としてACL（Access Control List)がある。
ACLはファイヤーウオール等でも使用されており、下記のような情報を元に作成される。

IPアドレス(送信元、送信先)、ポート番号(TCP、UDP)、MACアドレス、物理ポート番号など・・・

制御システムへの適用の問題点

制御システムにかかわるエンジニアがネットワークに対する十分な知識を持っているとはかぎらない。
ホワイトリストの維持管理に大きなコストが必要

システム立ち上げやメンテナンス実行時などの
検証作業を実施している時のデータなどから
ホワイトリストとなるACLを自動学習機構を実現する



ホワイトリスト自動学習スイッチの動作

模擬プラントを活用した検証

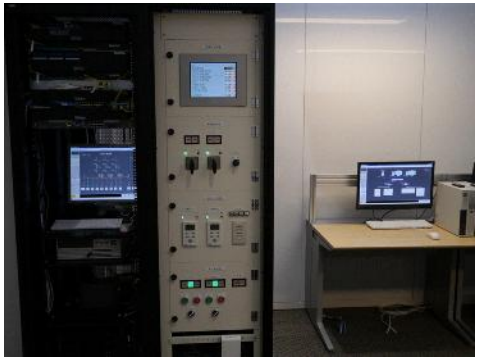
東北多賀城本部の模擬プラント
4式にて検証を実施

既存の制御ネットワークスイッチを
置き換え通常通信を学習して
ホワイトリストを自動生成

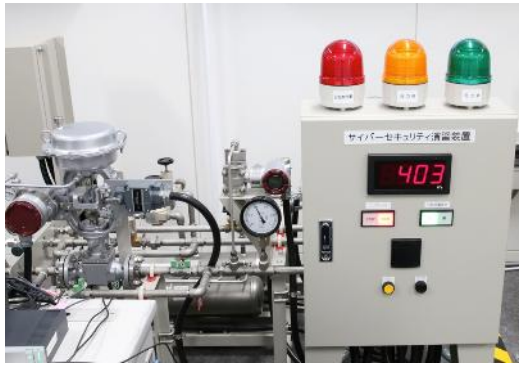
全ての検証プラントにおいて

- 正規通信が阻害されない(通常動作に影響がでない)ことを確認
- ネットワークスキャンやDoS攻撃、などの影響を受けないことを確認

ビルプラント1



ビルプラント2



ガスプラント

スマートシティプラント

まとめ～ホワイトリストスイッチ～

- 制御システムの特徴を考慮して、ホワイトリスト型スイッチについて研究を実施
- 自動学習機能を追加することにより設定コストを低減
- 複数の模擬プラントを使用した検証により、どの分野においても利用できることを確認

研究成果の展開

組合員のAlaxala　Networks社より製品発売※1
上記製品は「Interop Tokyo 2015」の展示会において、Best of Show Award「IoT部門」グランプリを受賞※2

ホワイトリストの自動生成機能をオプションにて追加するAX2530S

他組合員企業も研究成果を活用し、製品化に向けて開発中

※1: http://www.alaxala.com/jp/news/press/2015/20150525.html
※2: http://www.alaxala.com/jp/news/press/2015/20150611.html

サイバー攻撃早期認識システム

サイバー攻撃早期認識技術の概要

従来の制御システム

異常発生

1.ユーザ自身による原因究明
- ・プロセス系の異常？
- ・操作ミス？

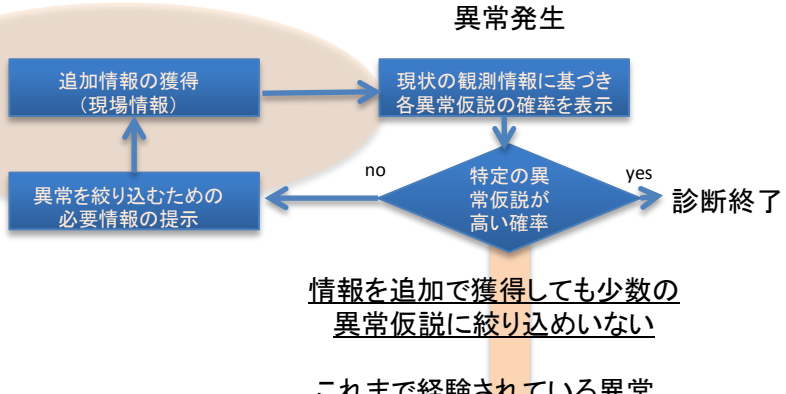
2.ベンダーへ依頼しての原因究明
- ・個別機器の故障？
- ・ソフトウエア異常？

全ての異常の可能性を否定して、
初めてサイバー攻撃の可能性を考える

- サイバー攻撃と認識できるまでの時間が長期化
- サイバー攻撃の認識が困難

サイバー攻撃早期認識技術が導入された場合

Cyber Attack early Recognition System: CAeRS



情報を追加で獲得しても少数の異常仮説に絞り込めいない

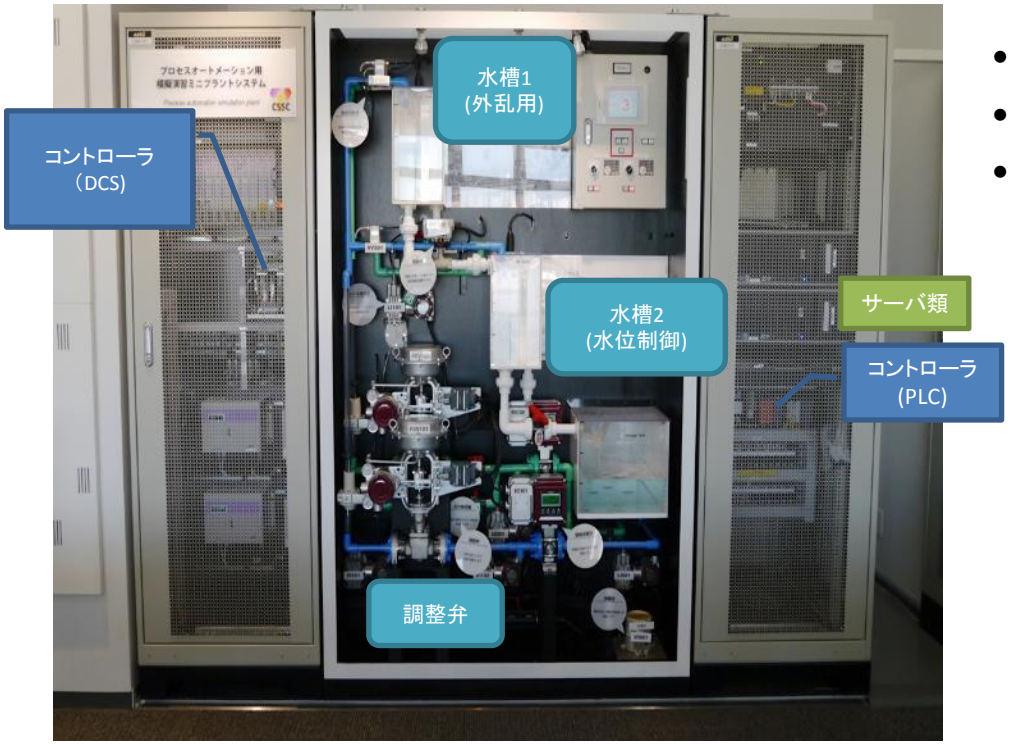
これまで経験されている異常、可能性のある異常の範囲内では現在の状況を説明できない

- **サイバー攻撃の可能性を系統的に絞り込み可能**
- **短い時間でサイバー攻撃と認識可能**

サイバー攻撃の可能性

模擬プラントを使用したプロトタイプを作成して有用性の検証を実施する

プロトタイプ実装対象

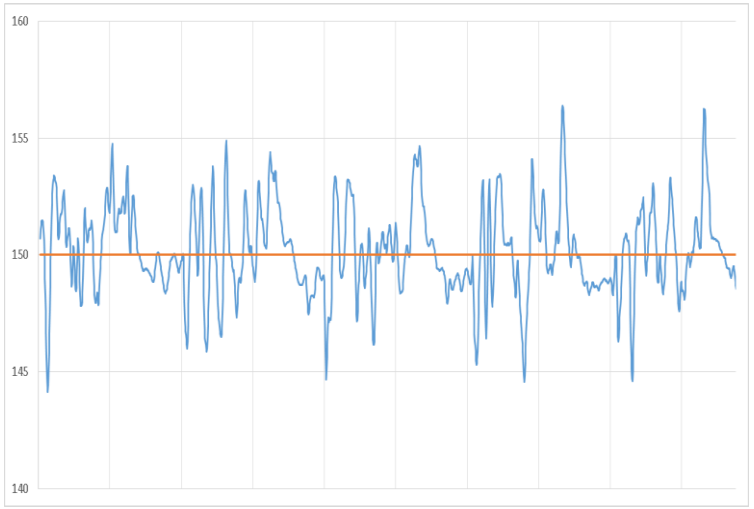


化学プラントテストベッド

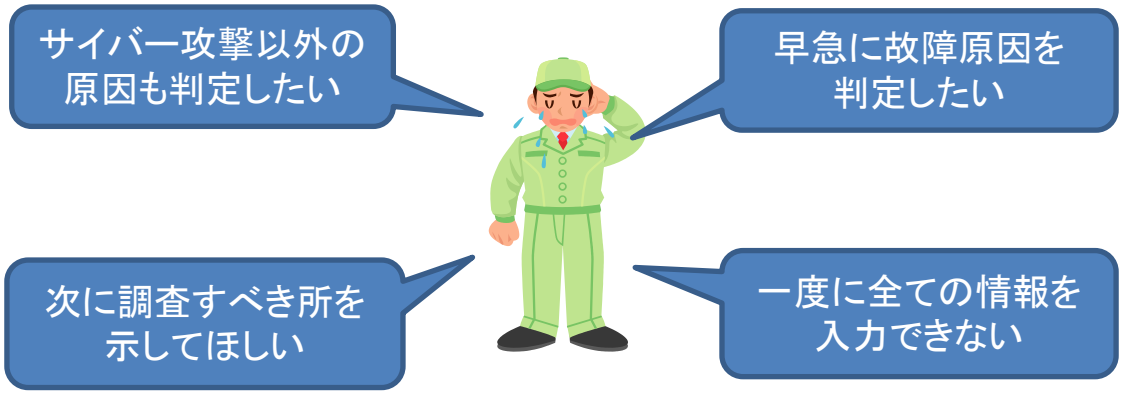
- 実システムと同様の制御機器を使ったテストベッドシステム
- PID制御により水位を一定に制御
- 運転制御卓から遠隔操作可能
- 各種のサイバー攻撃を模擬して、その時の実システムの挙動を再現可能

通常運転時、システム故障、サイバー攻撃を模擬した時のプラントの挙動データを収集して解析

故障診断ロジックへの要求事項



水位変化例



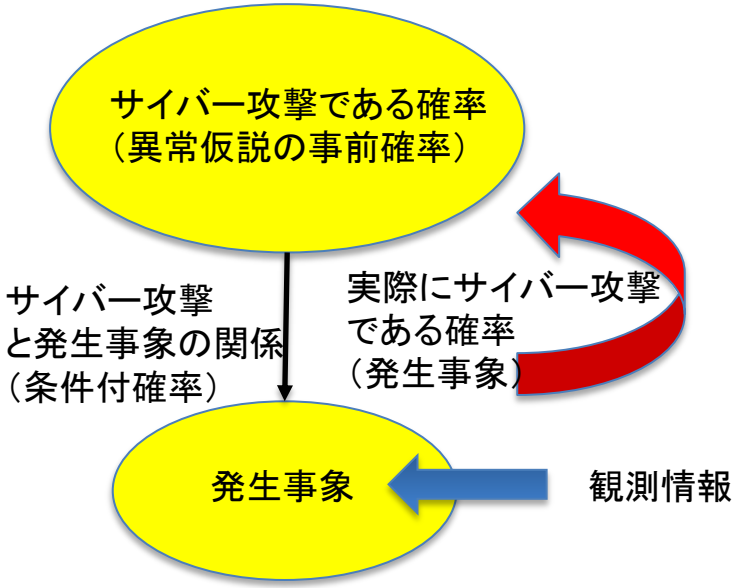
診断ロジックには

- さまざまな原因への対応
- 限られた情報での原因推論
- 補足情報の追加入力
- 推論結果の逐次更新

などが求められる

ベイジアンネットワーク

ベイジアンネットワークは各事象との因果関係を確率によって表現する手法
原因と事象の関連を確率によって定義することにより、発生した事象から原因を推定することができる



観測情報が欠けていても、異常原因の信頼性を確率表現により求めることが可能
→**早期の事象にも対応可能**

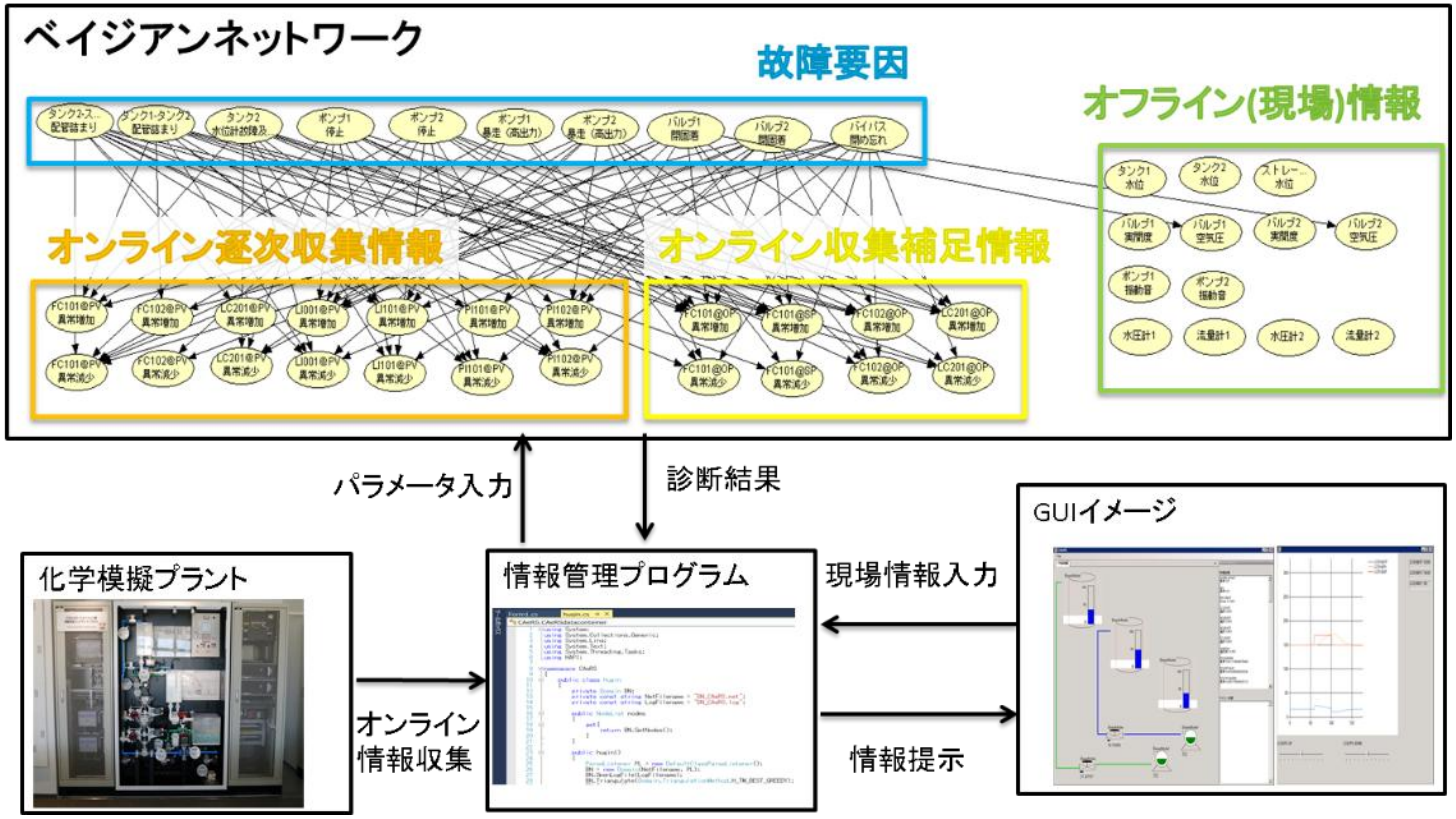
観測を重ねることによる逐次的な推論
→**新たな情報入力による推論結果の更新や動的変化に対応可能**

情報の逐次的獲得

- オンライン情報(1): リアルタイムで常にモニターしている情報
- オンライン情報(2): 必要に応じてオンラインで獲得する情報
- オフライン情報：現場情報を獲得し作業員がシステムに入力する情報

➢ **逐次的に情報を獲得していき仮説を絞り込む**

サイバー攻撃早期認知システムのプロトタイプ構成



物理障害における原因推定

結果(1)　異常に対する診断結果

異常状態	オンライン情報(1)のみによる診断結果
ポンプ1高出力	全て低確率
ポンプ2高出力	確率の変動大、時間経過で全て低確率
バルブ1閉固着	低確率
タンク1・タンク2間パイプ詰まり	良
タンク2・ストレージタンク間パイプ詰まり	良
タンク2水漏れ	良
ポンプ1停止	良
ポンプ2停止	良
バルブ2閉固着	良
メンテナンス用バイパス誤って開放	良

結果(2)　追加情報入力時の診断結果

異常状態	変化
ポンプ1高出力	ポンプ1高出力の確率値が上昇
ポンプ2高出力	ポンプ2高出力の確率値が上昇
バルブ1閉固着	バルブ1閉固着の確率値が上昇

オンライン情報(2)とオフライン情報の獲得によって特定可能

ベイジアンネットワークによる診断の有効性を確認

サイバー攻撃に対する診断結果

サイバー攻撃として、内部パラメータ（バルブ1開度上限値）を0に変更

↓

観測徴候：バルブ1開度が0となる

↓

物理的現象は「バルブ1閉固着」と同様

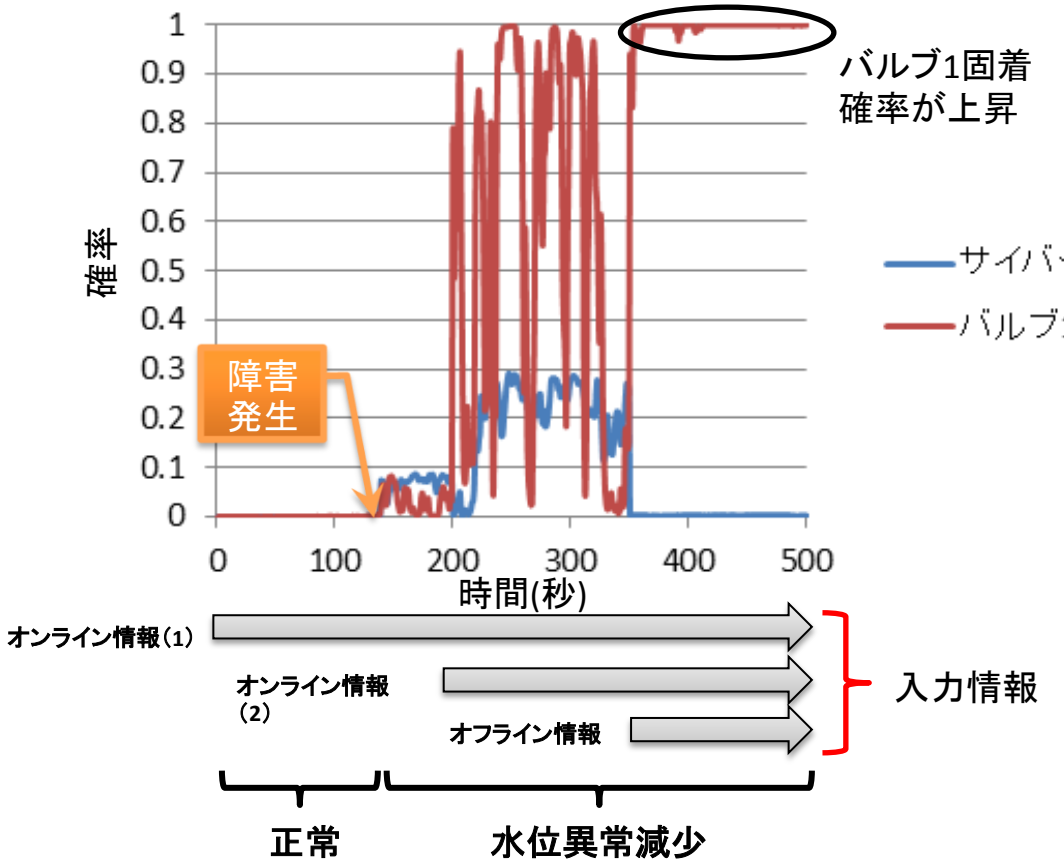
↓

観測徴候としては「バルブ１閉固着」とサイバー攻撃は類似

↓

オンライン情報１だけでは弁別不可能

物理故障とサイバー攻撃の弁別



「サイバー攻撃」と「バルブ1閉固着」の確率の時間的変化

オンライン情報(1)だけでは弁別できないが、情報を追加することで弁別可能

類似の物理現象を持つ物理故障とサイバー攻撃の弁別が可能

まとめ～サイバー攻撃早期認識システム～

・ベイジアンネットワーク技術を用いたサイバー攻撃早期認識システムのプロトタイプを開発
・物理故障と類似した現象が発生するサイバー攻撃の分別が可能であることを確認

今後の研究

- 弁別をするサイバー攻撃バリエーションの追加
- 複数の運転モード切り替え時での推論
- 故障原因診断を行うエンジニアを考慮したユーザインターフェイスの構築