PI SystemとMcAfee SIEMとの連携による「状況認識」の実現

McAfee サイバー戦略室 兼 ガバメント・リレイションズ
佐々木　弘志 （Hiroshi Sasaki）

アジェンダ

- 制御システムセキュリティ最新動向
- 制御システムセキュリティの基本
- 状況認識の重要性
- McAfee SIEM紹介
- PI SystemとMcAfee SIEMとの連携デモ
- まとめ

●制御システムセキュリティ最新動向

なぜ今、制御システムセキュリティなのか？

制御システムのオープン化

- 制御システム間の通信インタフェースのイーサネット化
- 制御システムの汎用OS化（Windows Embedded, Linuxなどの利用）

制御システムを狙った攻撃の発生

- 2010年 Stuxnetの登場　イランの核施設を破壊。クローズ環境だったがUSBメモリ経由で感染
  SIEMENS社製のPLCプログラミングソフトStep7/Win CCがハッキングされた

世界的に対策が進行中

- 制御システムセキュリティ標準の制定（国際：IEC62443　業界：NERC CIP）
- 国家レベルの取り組み（米国：NIST Framework　EU：DENSEK）

国内の重要インフラセキュリティ（CIP）動向

2013年5月

重要インフラ防護のための制御システムセキュリティ研究開発組織（CSSC)が宮城県多賀城市に開所

2014年4月

CSSC認証ラボラトリーが制御機器の国際的セキュリティ認証であるEDSA認証取得サービスの開始

2014年4月

電力事業者向けに、米国の電力事業者セキュリティ規格NERC CIPを参考とした日本版CIPの制定へ

http://www.css-center.or.jp/ マカフィーも参加

（4月28日電気新聞）

重要インフラのセキュリティ対策が強化、促進される

OPCサーバーを狙ったサイバー攻撃 ～Operation Dragonfly～

McAfee
An Intel Company

› サポート › Japan - 日本 (Japanese) 入力し

個人のお客様　中堅・中小規模企業のお客様　大企業のお客様　パートナー　マカフィーについて

HOME ▸ セキュリティ解析センター ▸ McAfee Blog

McAfee Blog

産業プロトコルを脅かす「Operation Dragonfly」

2014/07/04

最近、ニュースの見出し（「The Register」と「Slashdot」）でStuxnetマルウェアが取り上げられているのを見て、大規模発電所の付近住民は恐怖を覚えたかもしれません。2009年、このマルウェアはナタンツの核施設に重大な損害を与え、イランのウラン濃縮遠心分離機の五分の一を破壊したと言われています。しかし、Operation Dragonflyに関する最近の報告は（少なくとも今のところは）スパイ活動に焦点を合わせているようであり、攻撃範囲はStuxnetよりかなり広いようです。

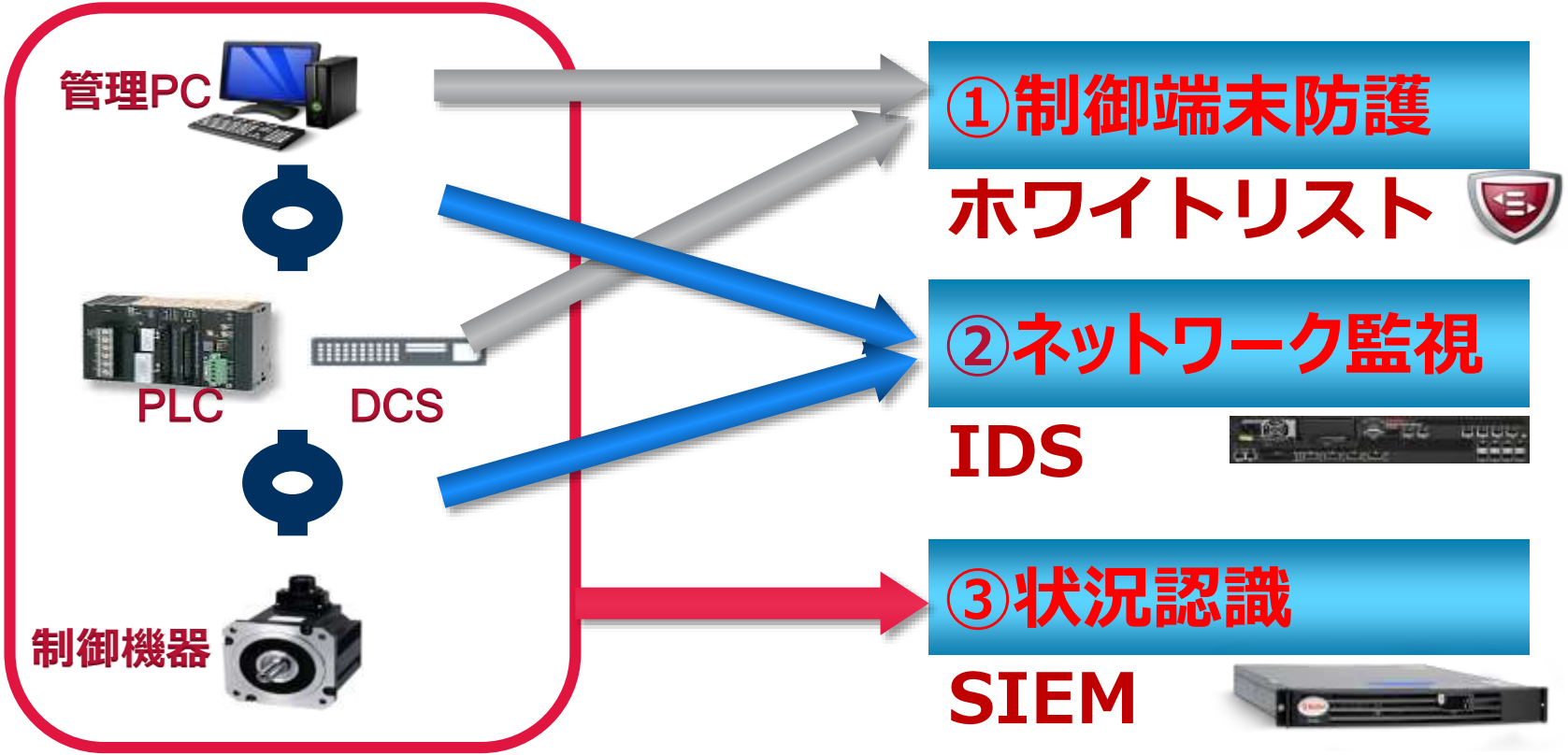
Operation Dragonflyに関するさまざまな要素がOperation Shady RATと比較されています。Operation Shady RATでは、少なくとも最初の段階では、電子メールによって特定の個人が狙われました。ただしOperation Dragonflyは、具体的な動作についてより、重要なインフラストラクチャ、特に拡大し続けるサプライチェーンを構成するシステムの安全性について、非常に大きな懸念を呼んでいます。

http://blogs.mcafee.jp/mcafeeblog/2014/07/1416.html

- 2013年2月より電力業界への攻撃を開始
- 制御システムベンダーのソフトのアップデートサイトをハッキング
- 制御システムベンダーのソフトのアップデータにマルウェアを同梱
- 欧州を中心に電力会社数社が感染
- 感染PCのネットワーク内にあるOPCサーバーの情報を収集し外部へ送信

- 制御システムセキュリティの基本

マカフィー
制御システムセキュリティソリューション



ホワイトリストとは？

ブラックリスト型（アンチウィルス）

悪いものをリスト化して検知する。

- 定義ファイル更新必要。メンテナンス要。
- スキャン負荷が高い。
- 未知の脅威には対応できない。

ホワイトリスト型

良いものをリスト化してそれ以外は起動しない。

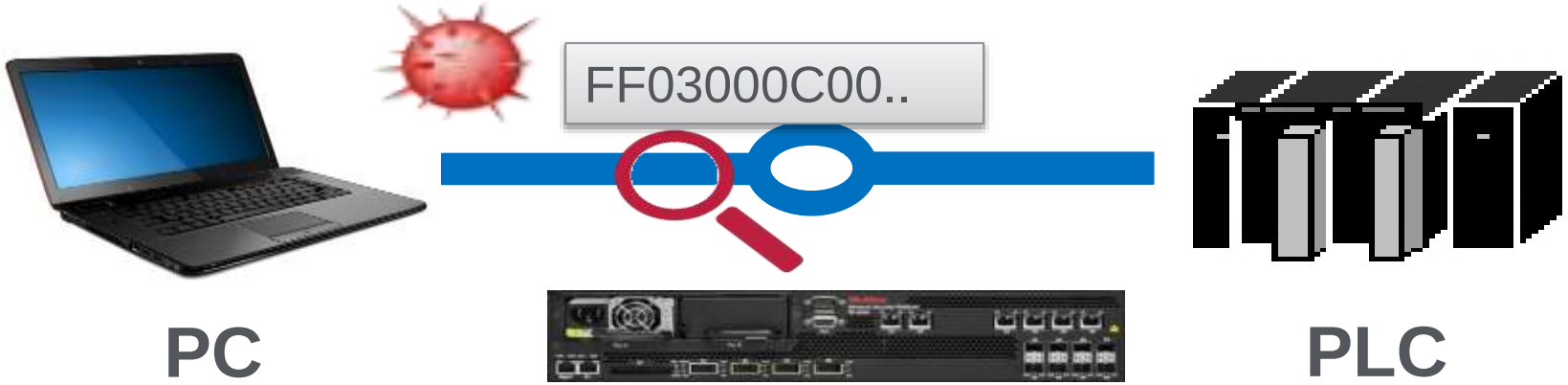
- 変更ないなら放置可能。
- 起動チェックなので負荷がほとんどない。
- 未知の脅威にも対応できる。

ホワイトリストの適用例

ネットワーク監視
IDS (Intrusion Detection System)

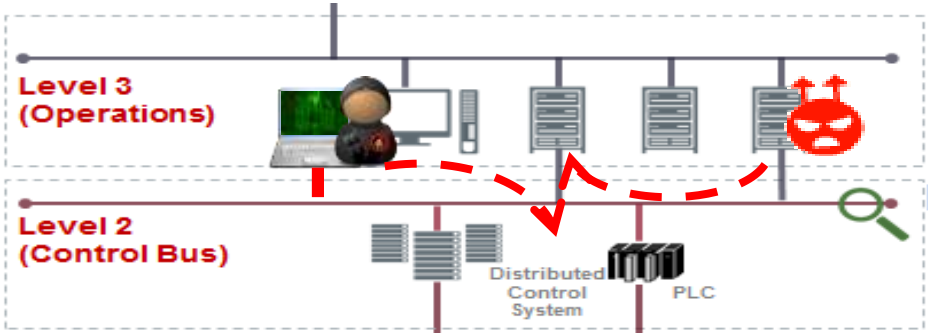
IDS＝「侵入検知システム」

ネットワークを流れるパケットを監視して、不正アクセスと思われるパケットを発見して**検知**する。



ネットワーク監視
IDSの通信制御（ホワイトリスト）

IPアドレスやポートレベル（L3/L4レベル）の通信ホワイトリストの作成が可能。
また、アプリケーションをベースにした通信制御（ACL：Access Control List）を 行うこともできる。例えば**「ファイル共有系の通信を禁止」**というようなポリシー作成ができる。



不正なPCが接続されて通信を行ったり1台のPCがマルウェア感染して、ファイル共有通信などで広がろうとした場合、IDSで通信ホワイトリストを定義しておけば、検知が可能となる。

- 管理されていないPCからの接続を検知できる。
- 該当する制御システムでは使わない通信の使用を検知できる。
- IDSなので実際に通信を止めるわけではない（可用性重視！）

●状況認識の重要性

「状況認識」とは？

古くは第一次世界大戦中の米空軍の考え方にさかのぼると言われており、
軍だけでなく、人間工学、セキュリティなどさまざまな分野で用いられている。
一般的には、1995年のEndsleyの定義が広く知られている。

Toward theory of Situation awareness in Dynamic system (Endsley 1995b) の図より抜粋

「知覚」「把握」「予測」→状況認識 situation(al) awareness

スリーマイル島の教訓①　～状況認識の欠如～

1979年　米国スリーマイル島にある
原子力発電所にてレベル５※1の事故が発生。
事故時の**現場対応のまずさ**により、事前の想定を超えた被害となったことで知られている。

（※1：福島第一原発はレベル７）

スリーマイル島の教訓②　～クリスマスツリー現象～

事故当時
- 137個もの警報灯が点灯
- 30秒間に85回警報音が鳴り響く

現場の混乱が増大

スリーマイル島の教訓③～「状況認識」の重要性～

教訓

オペレータが非常事態に対処するためには、
情報を集めてただ示すだけでは十分ではない。

オペレータが現状を**「知覚」**、**「把握」**し、次に起こることを**「予測」**できなければならない。

「状況認識」の重要性

- McAfee SIEM紹介

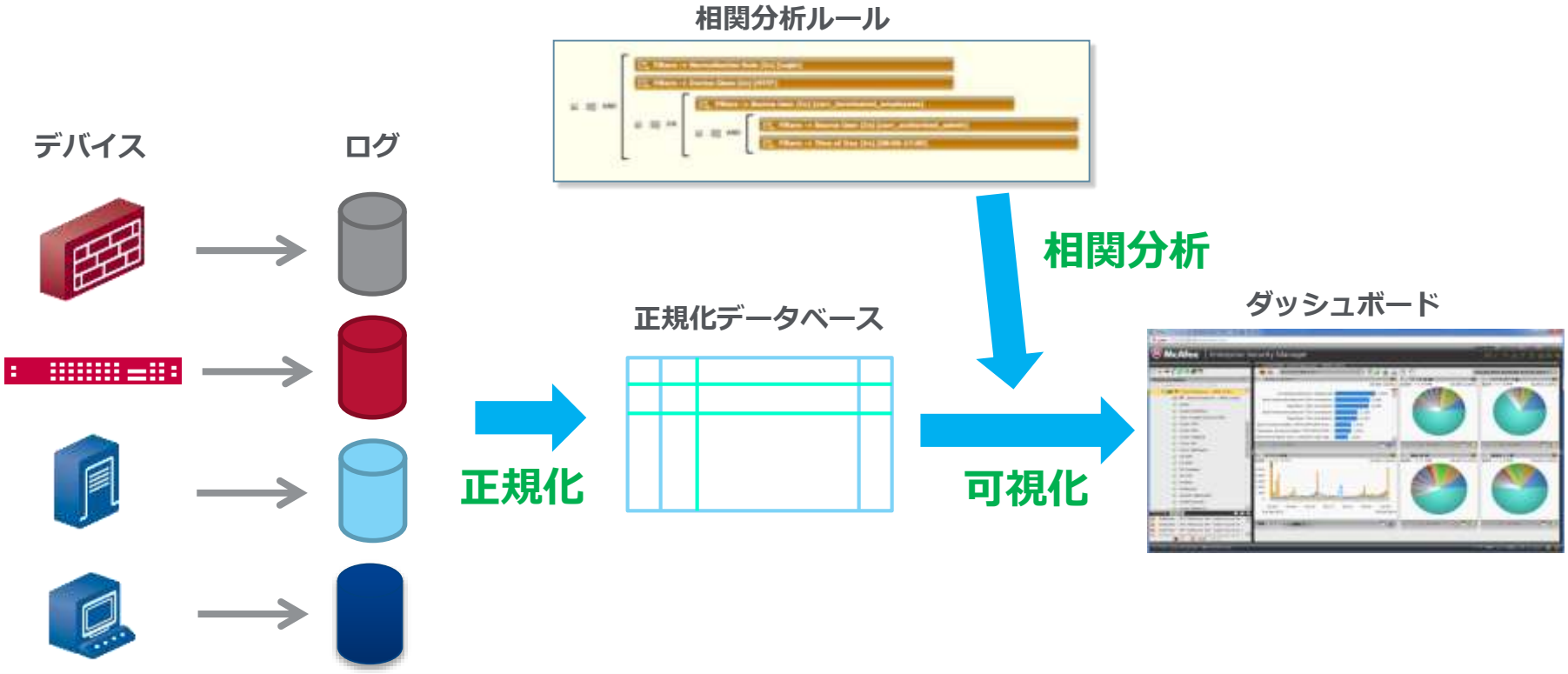
SIEM（Security Information and Event Management）とは？

SIEMは「**状況認識**」を実現するためのソリューションである。
「状況認識」とは、システム全体のログやイベント情報をもとに分析を行い、**早期に重要な異常を察知し**対策すること。

SIEM

サーバーやネットワーク機器、
セキュリティ関連機器、
各種アプリケーションから
集められたログ情報に基づいて、
異常があった場合に**管理者に通知**したり
その**対策方法を知らせる**仕組み。

SIEMの仕組み



「正規化」「相関分析」「可視化」で状況認識を実現

①正規化

異なるフォーマットのログをただ集めるだけでは分析の役に立たない。
ログ文字列を解釈してデータベースに取り込む際に「正規化」を行う

2014/01/02 23:34:56

Jan-2 -14 23:34:56

01-02 -2014 23:34:56

2014年1月2日　23時34分56秒

Log-in success

Log-on successful

ログイン成功

異なるフォーマットのログを**意味のある情報**に変換

②相関分析

集めたログを正規化しただけでは、その量は膨大であり、次に何をしなければならないのかの参考にはならない。そこでログデータベースに対して「相関分析」を行う。

不正侵入を検知する相関分析ルール例

①ログインに10回連続で失敗したあとログイン成功した。

↓

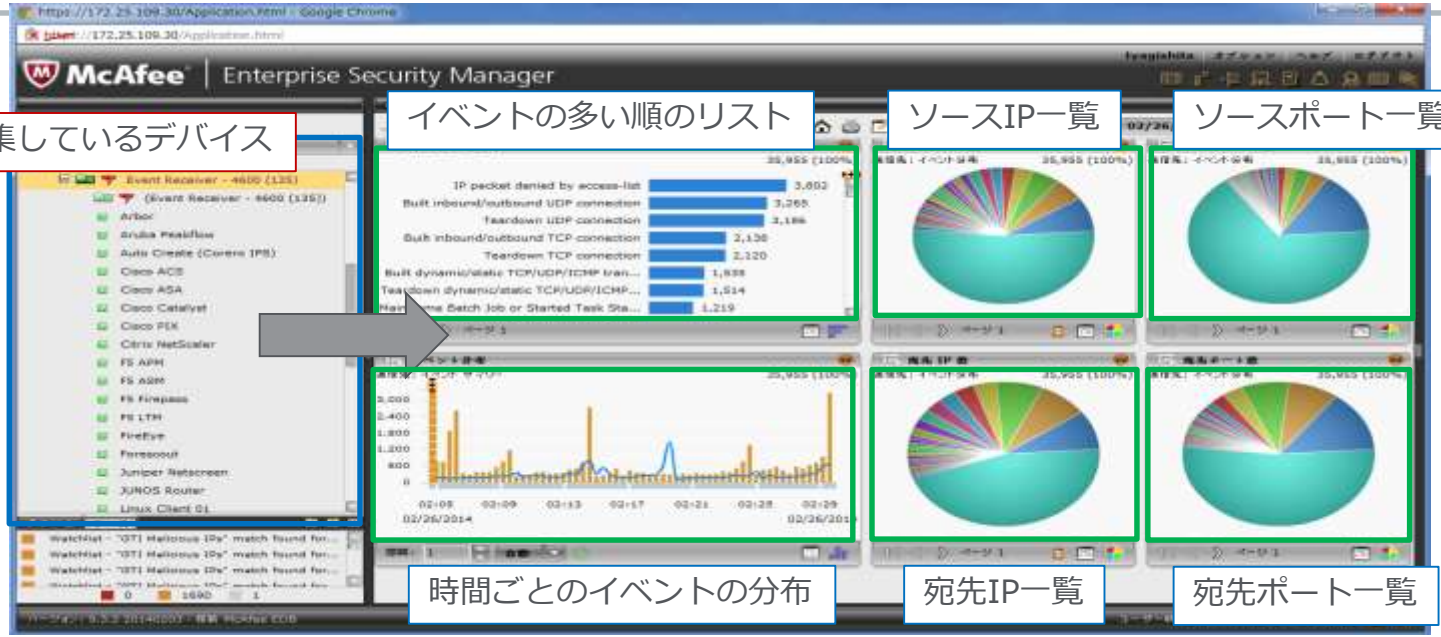
②管理者コマンドを実行した。

↓

大量のログデータから**優先度の高い脅威**を抽出

③可視化

「相関分析」を行った結果をオペレータに分かりやすく知らせる必要がある。
適切な可視化を行うことでオペレータが脅威の予兆を察知することはできる。



ダッシュボードによるログの可視化で脅威の予兆を察知

「状況認識」を実現するソリューションSIEM

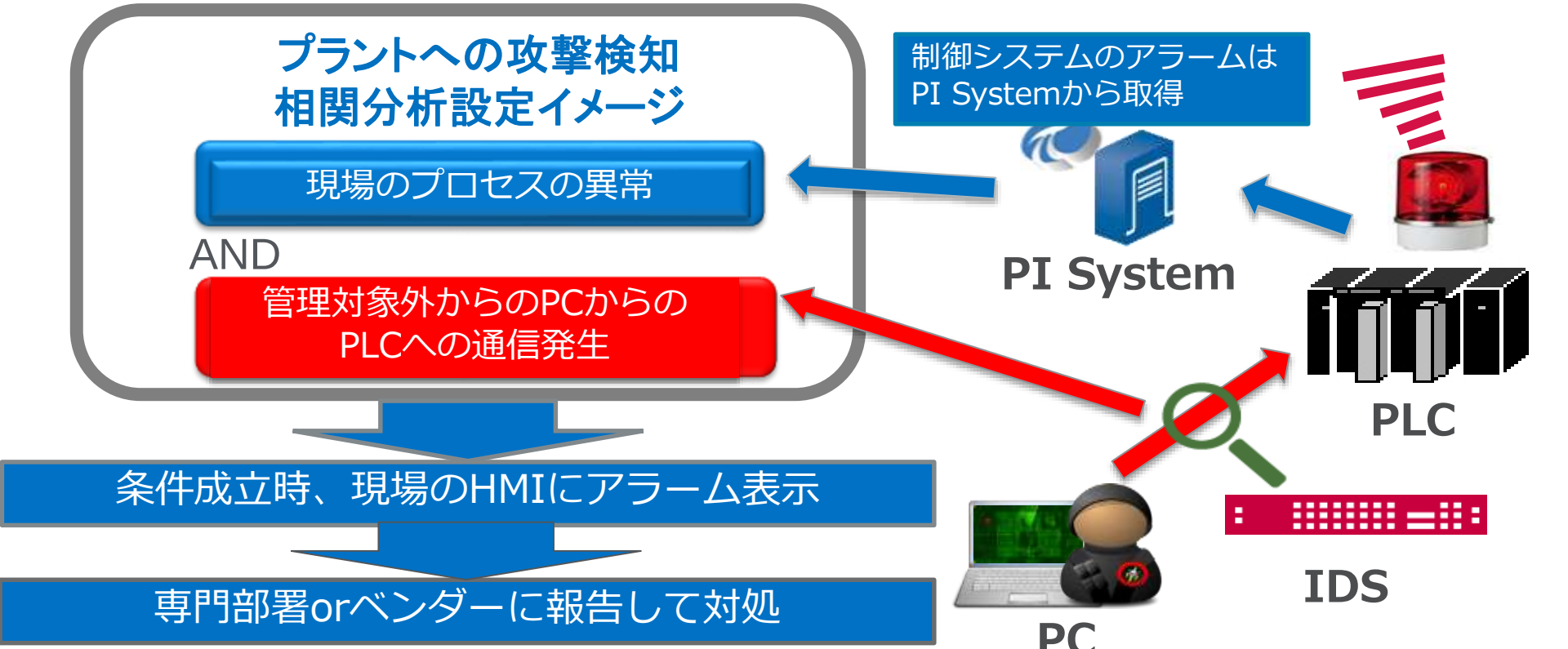
知覚　「正規化」によるログ情報の**収集**

把握　「相関分析」による脅威の**抽出**

予測　「可視化」により脅威の**予兆**を通知

「状況認識」を実現することで**早期の対策**が可能となる！

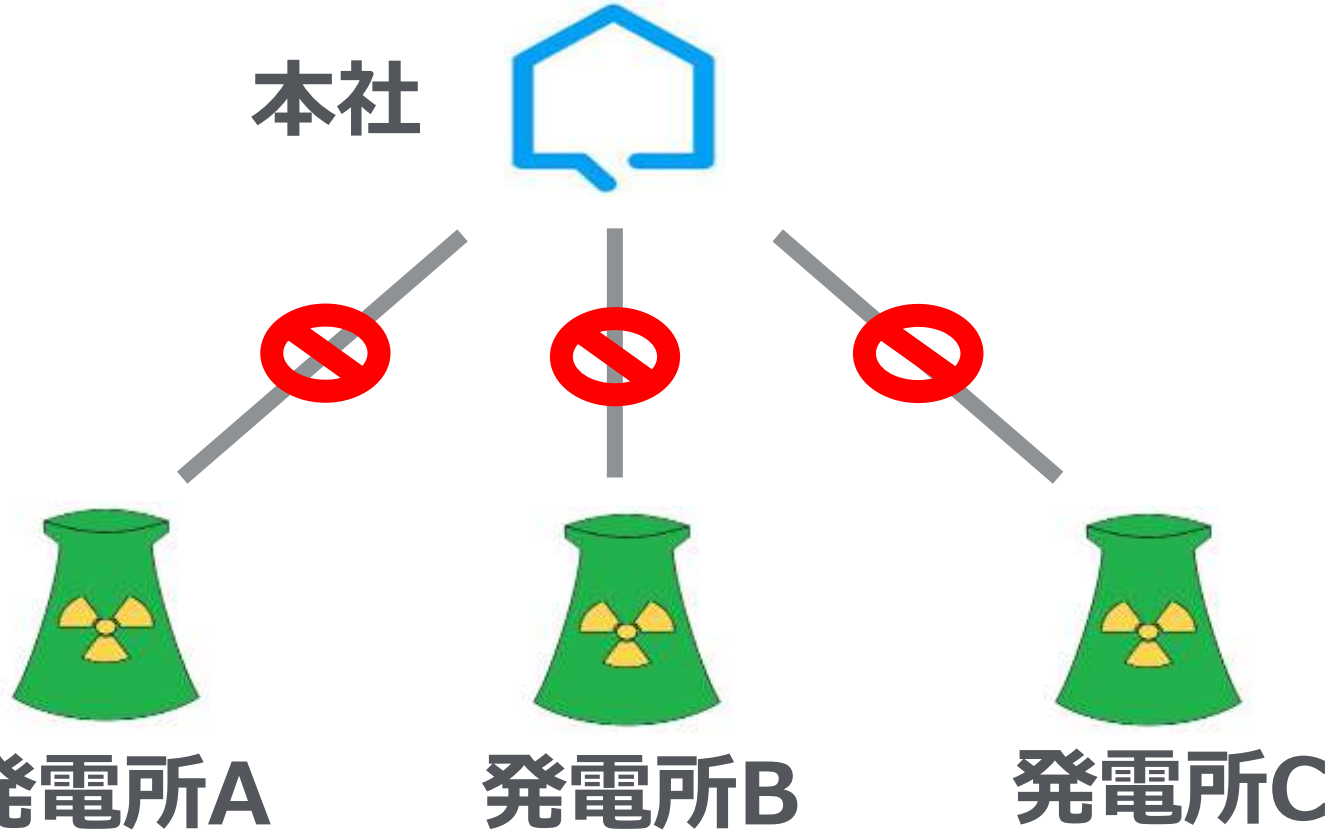
PI System を使用した相関分析例



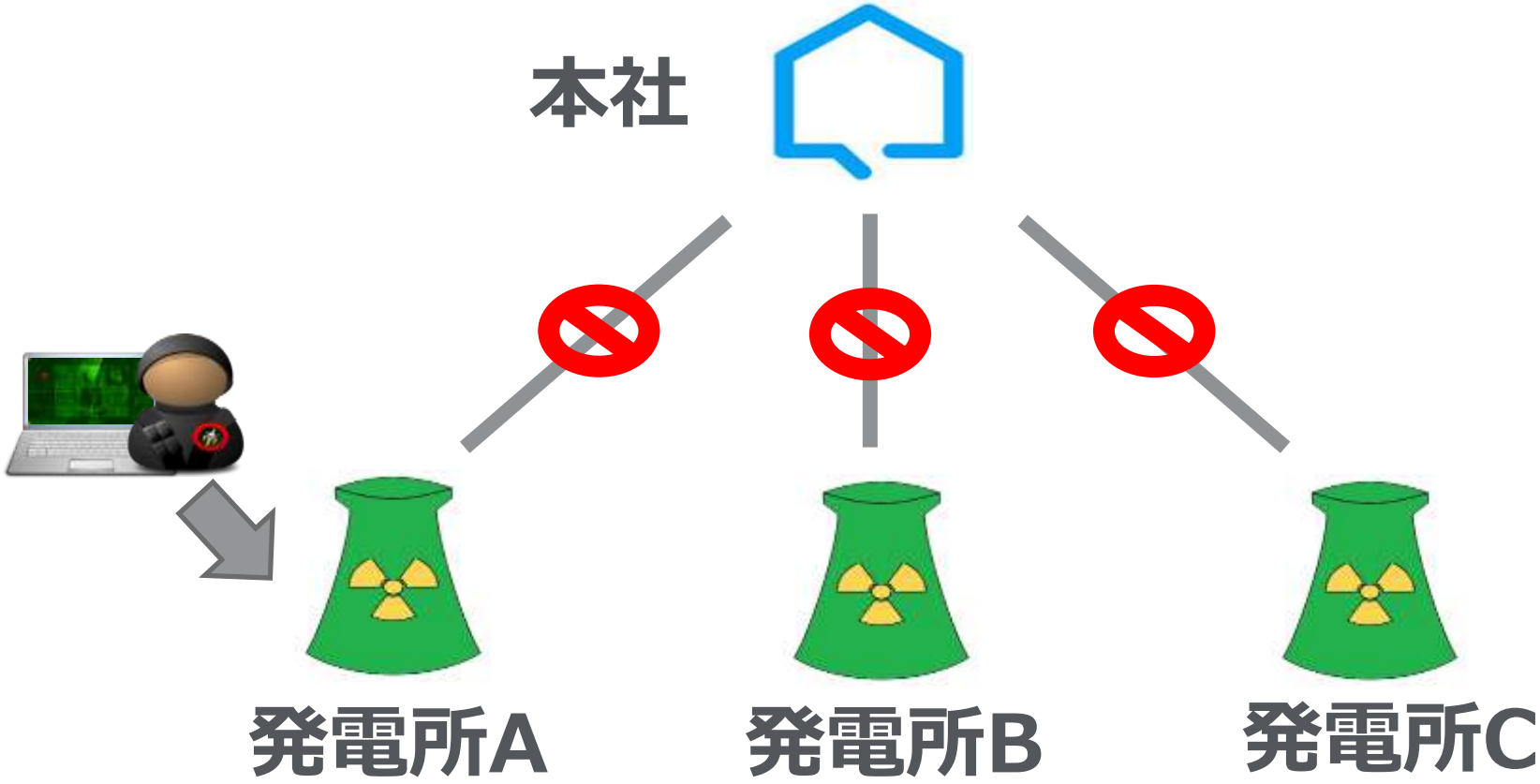
セキュリティの問題である可能性の検知⇒初動が変わる！

- PI SystemとMcAfee SIEMとの連携デモ

Case1: クローズ環境の場合

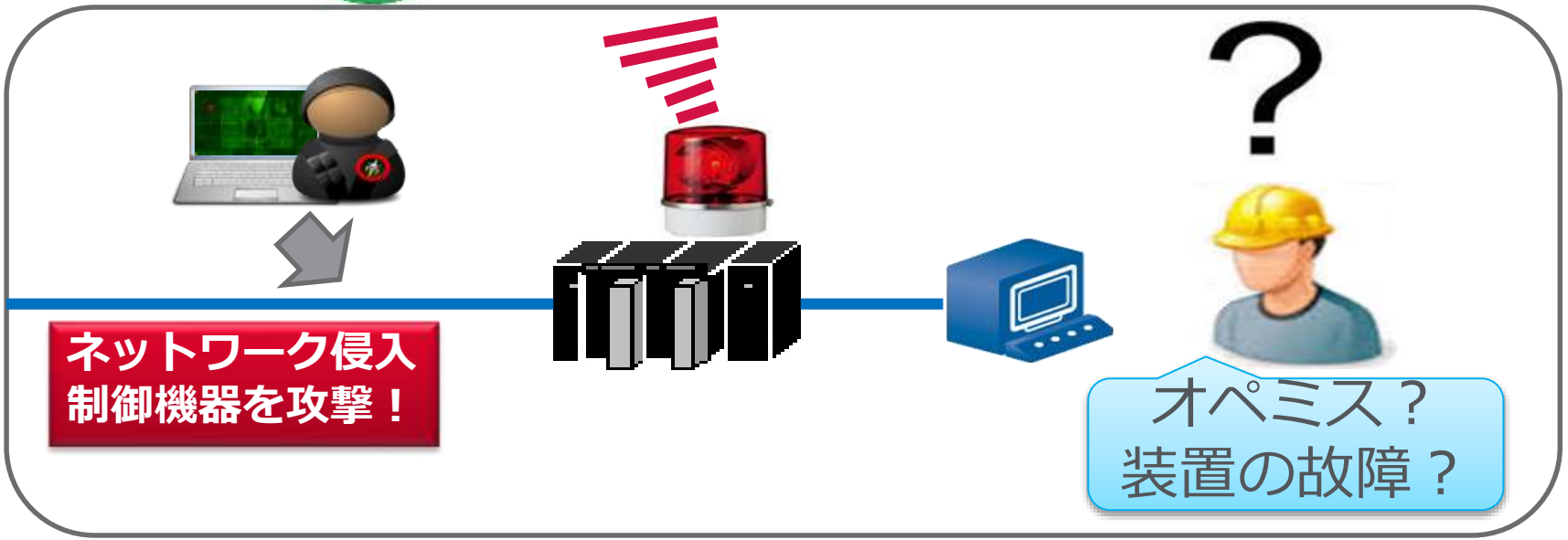


Case1:発電所Aでサイバー攻撃発生！！



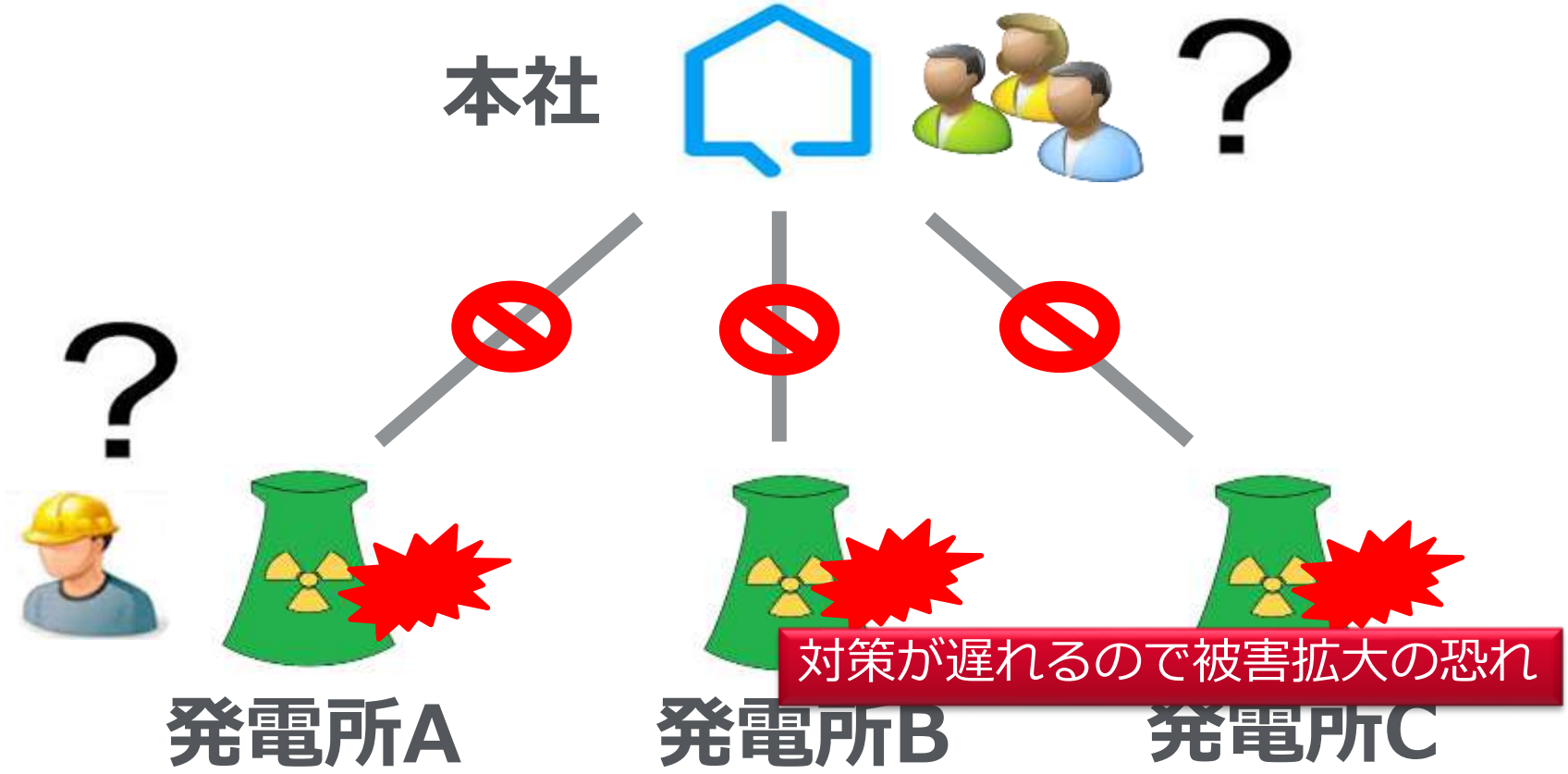
Case1:現場のプロセスの異常発生！

発電所A

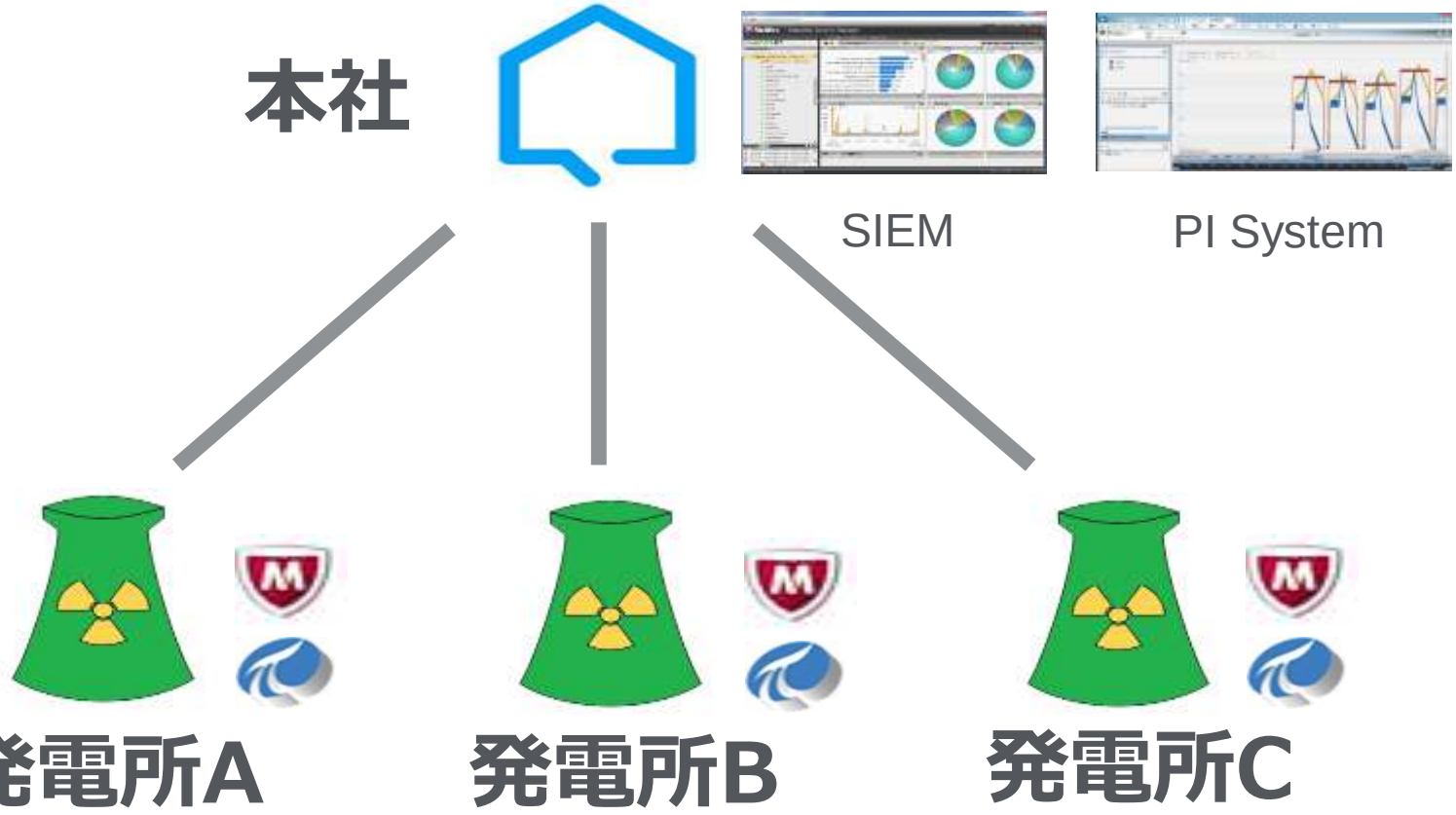


原因不明なので本社に連絡

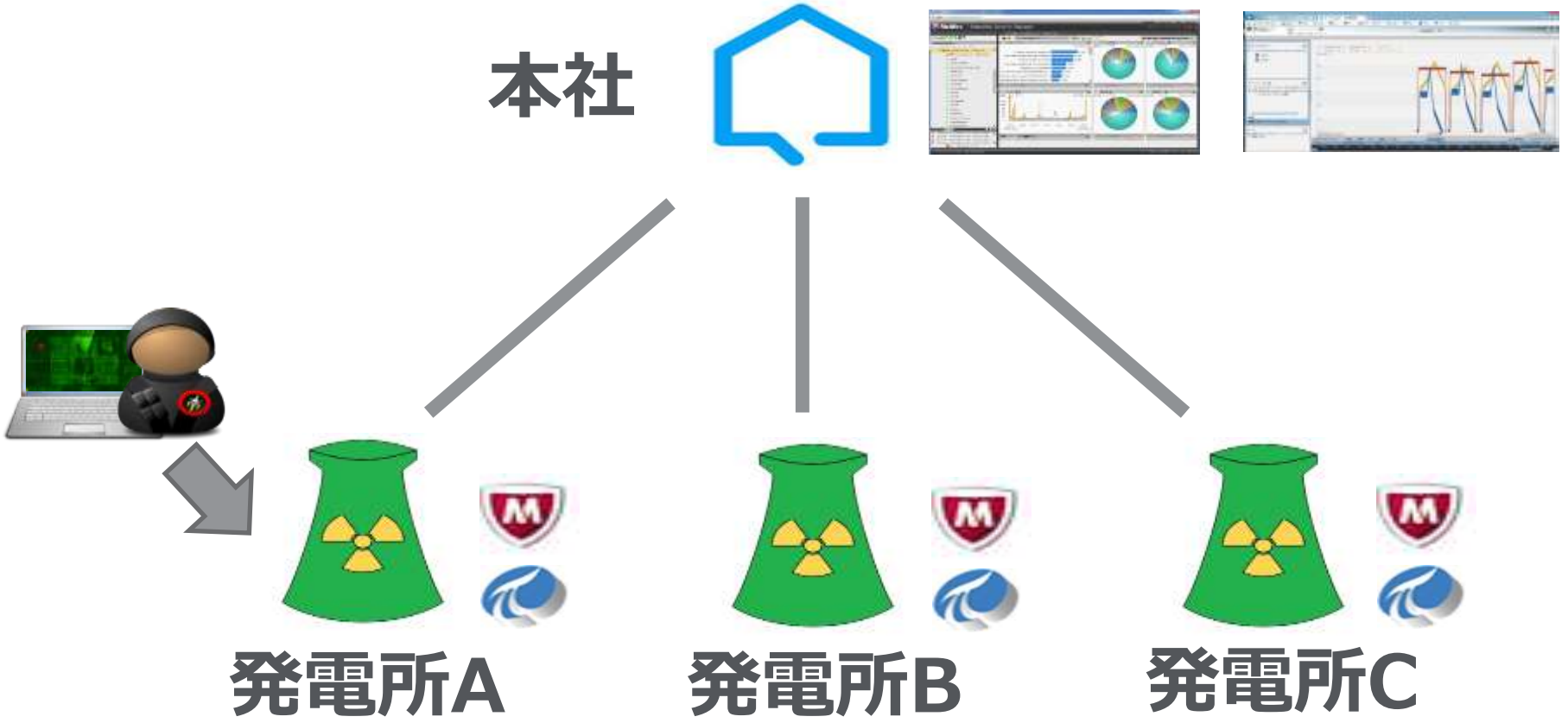
Case1:発電所Aの現状を把握できない！



Case2: 「状況認識」できている場合

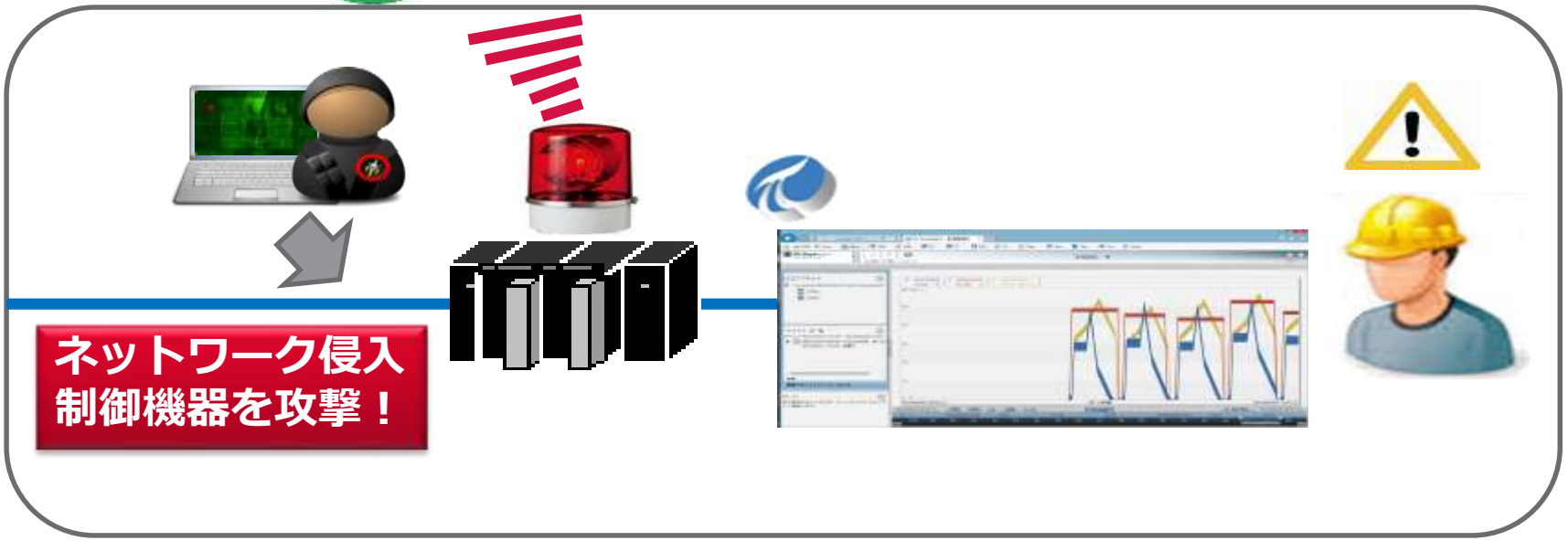


Case2:発電所Aでサイバー攻撃発生！！



Case2:現場のプロセスの異常発生！

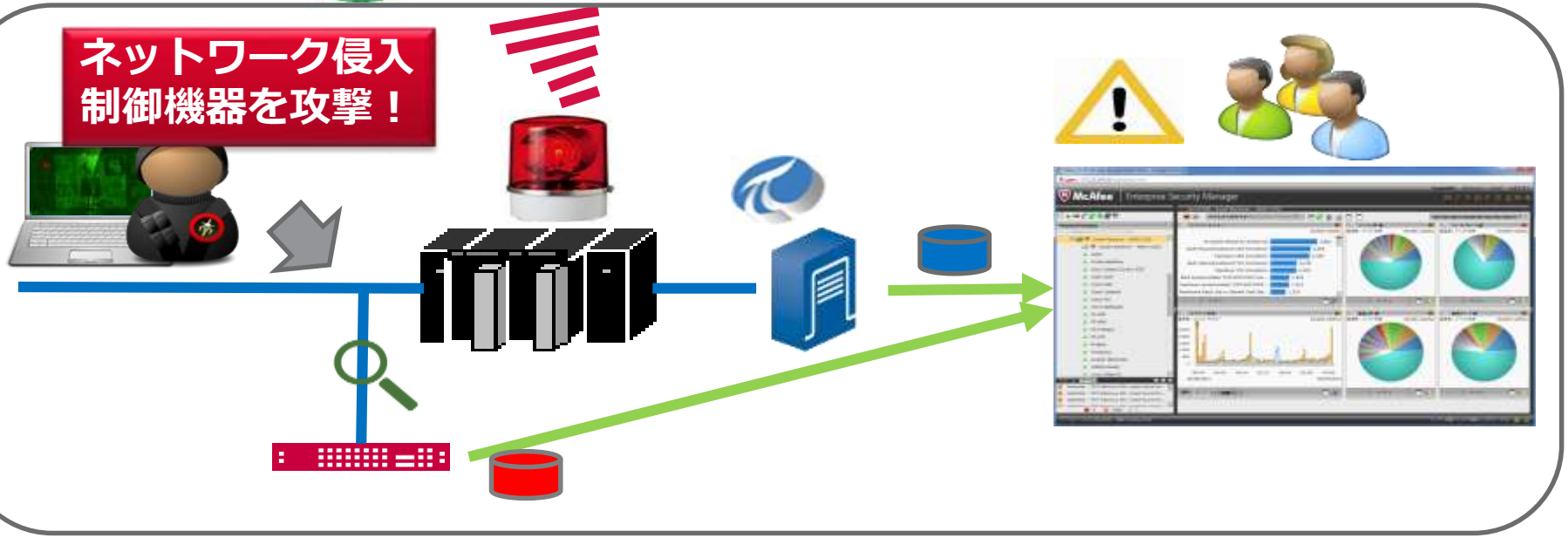
発電所A



メールで即座に通知　→　制御システムの状態を正しく確認

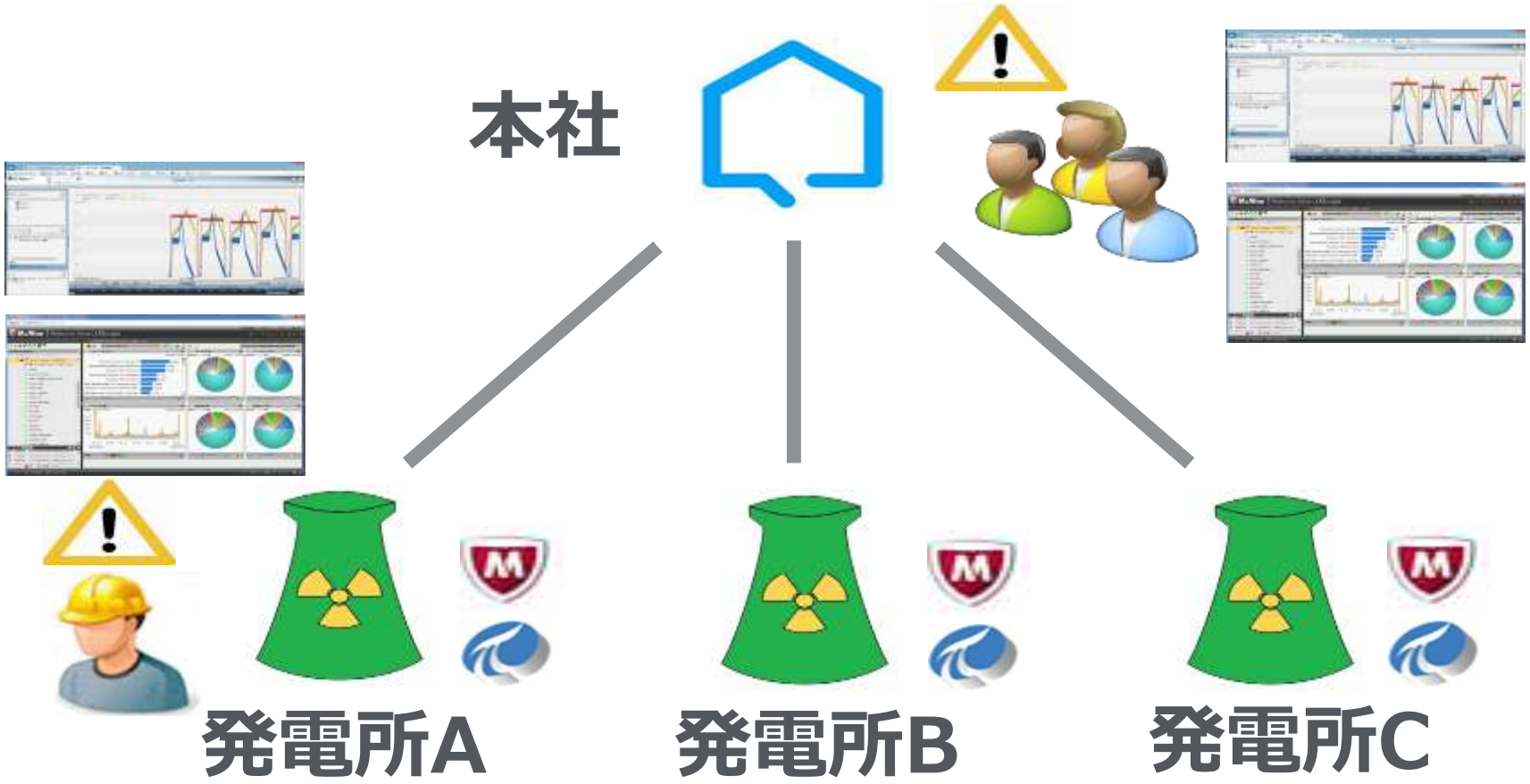
Case2:現場のプロセスの異常発生！

発電所A

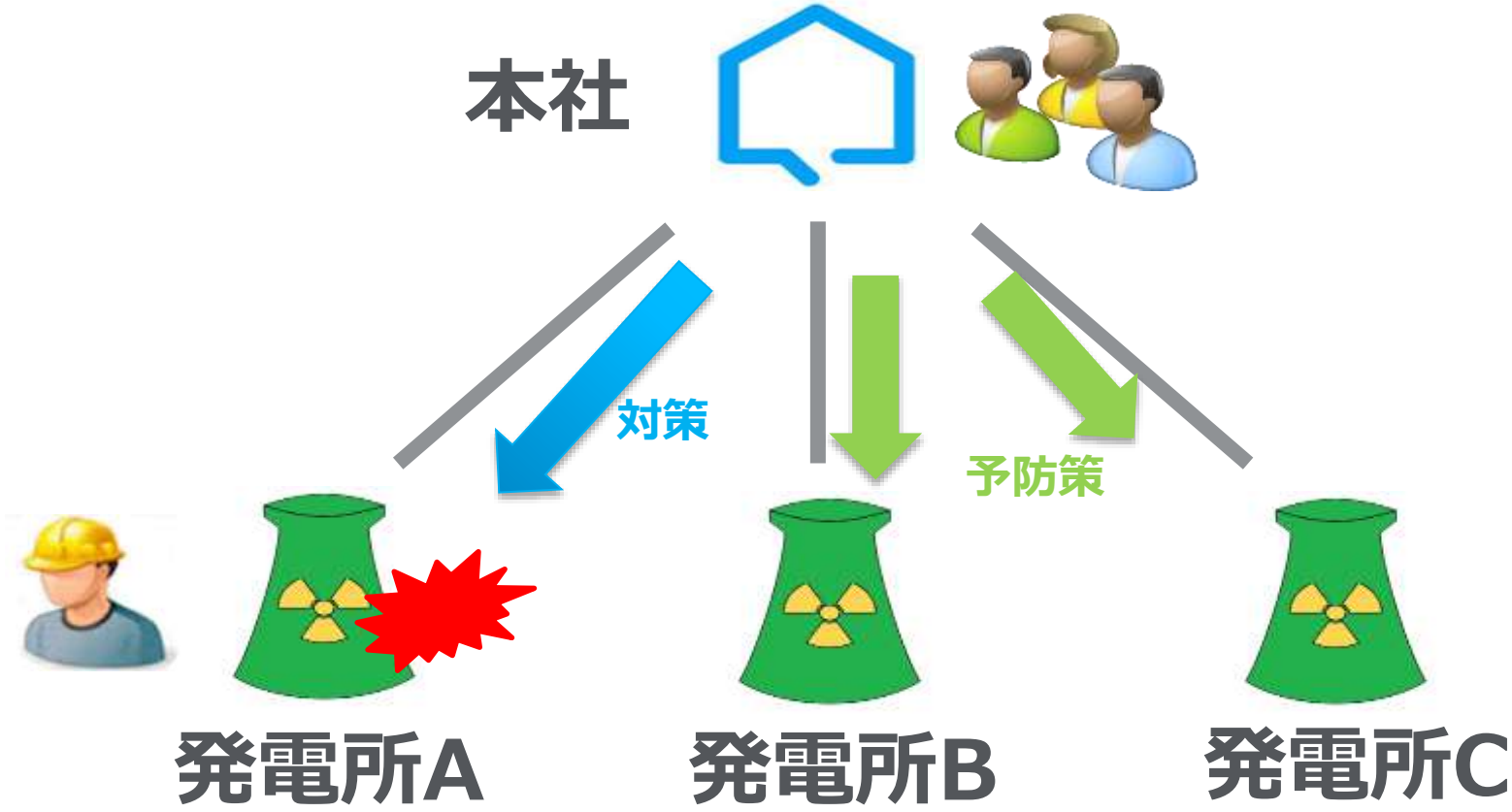


PI Systemやネットワーク監視機器からSIEMにログ送信

Case2: 同じ画面を本社でも共有！（COP）



Case2:「状況認識」により早期の対策可能



PI System＋SIEMが実現する「状況認識」

	Case1：クローズ環境		Case2：PI System × SIEM	
項目	現場	本社	現場	本社
サイバー攻撃で 装置の異常動作発生の 検知	○ HMIやDCSのア ラート等	×	◎ DCSアラート+PIによる 通知 情報共有	◎ PI→SIEM セキュリティ問題として検 知
1次対応・対策	○ →ただし 原因は不明	×	◎ オペレータの 適切で素早い対応 →原因を特定しやすい	◎ 現場と本社の連携 →本社も同じ画面を共有
2次対策・ 他への展開	×	×	◎ 再発防止策	◎ 他プラントに展開

- まとめ

「状況認識」を実現するまでのステップ①

オペレータが非常事態に対処するためには、
情報を集めてただ示すだけでは十分ではない。

「状況認識」の実現が重要である。

PI System × McAfee SIEMで実現可能。

ただし、実現までには課題が…

「状況認識」を実現するためのステップ②

課題

① クローズ環境よりもリスクが増えないか？
② 誰がどうやって見るのか？
③ SIEMの相関ルールをどうやって作るの？

対策

① 脅威の可視化、本社との情報共有でリスク減少
② PI System, McAfee SIEM ともにトレーニングメニューあり。
③ McAfee/パートナーによるハンズオンの支援


intel
Security
OSIsoft.