大規模産業型制御システム模擬装置の整備

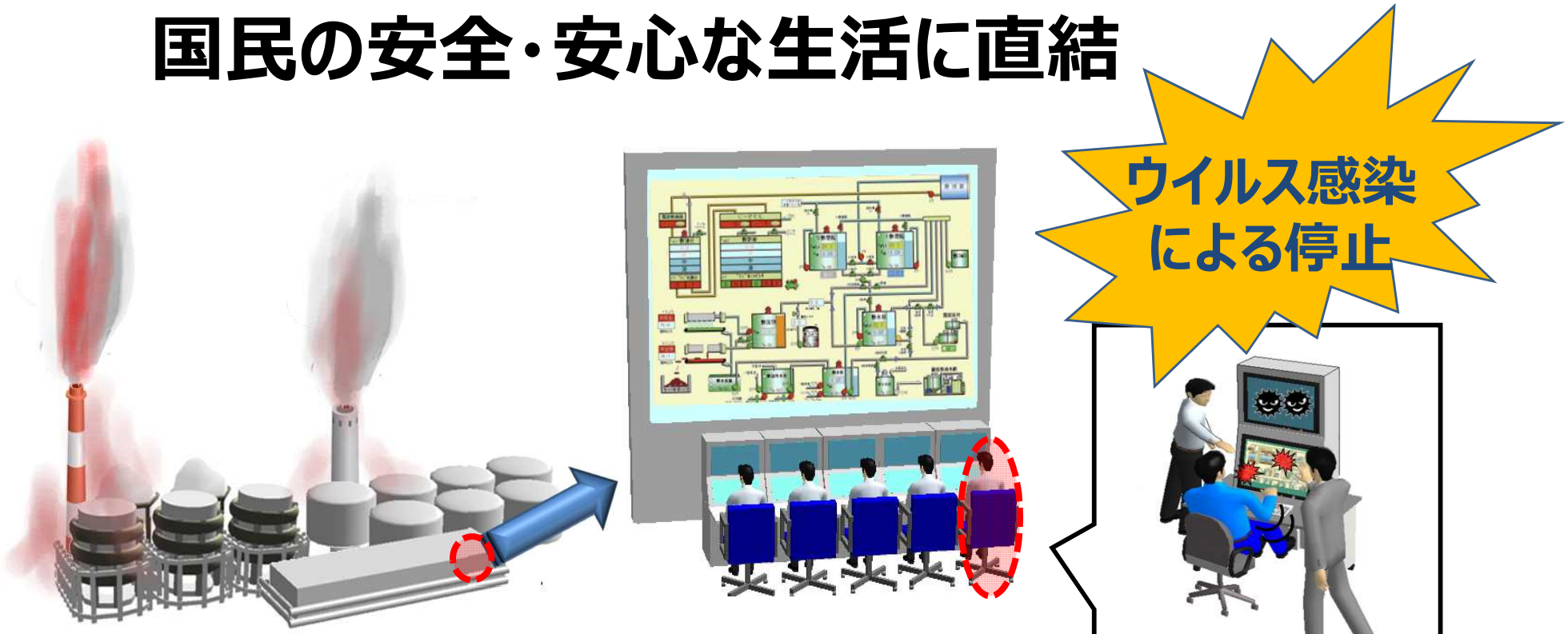
平成29年６月20日

警察庁情報通信局情報技術解析課

産業制御システムとは

○　産業制御システムとは

国民の安全・安心な生活に直結



産業用制御プラント　　監視システム

電力、ガス、石油、化学、水道　等

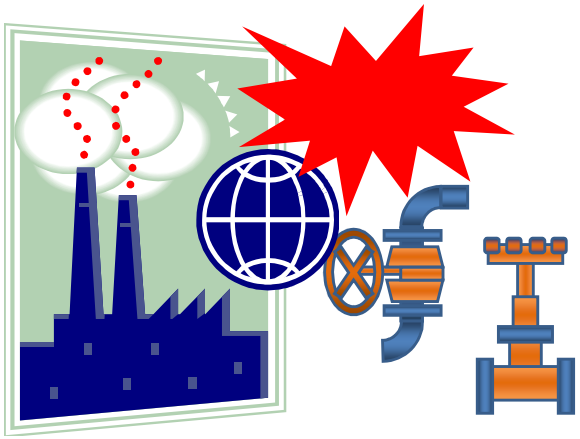
産業制御システムへの脅威

○ 産業制御システムへの脅威の増大

重要インフラと制御システム

電力	原発、火力発電所
ガス	ガスタンク
石油	石油コンビナート
化学	化学プラント
水道	浄水場
鉄道	列車運行管理システム
航空	灯火監視制御システム

等



2010年 イラン核施設 – 遠心分離器停止(スタックスネット)
2012年 イラン石油関連施設 – 端末のハードディスク消去
2012年 サウジアラビア石油会社 – 30,000台の端末停止
2014年 ドイツの鉄鋼工場 – 溶鉱炉制御不能
2015年 国内製制御機器への探索行為を国内で観測

我が国では産業制御システムへの具体的攻撃事例は表面化していないものの態勢を整えておくことが重要

産業制御システムに対するサイバー攻撃対策

○　産業制御システムに対するサイバー攻撃対策

国民の安全・安心の確保のため、
「被害の未然防止」、「緊急対処」及び「実態解明」を実施

被害の未然防止	認知時の緊急対処	実態解明
攻撃に関する情報をシステムを保有する企業と共有し、被害の未然防止を図る。	被害を認知した場合には、企業と共に被害拡大防止等の緊急対処に当たる。	通信履歴等の証拠を保全し、これを基にログ解析を実施する。

産業制御システムの解析等に必要となる
高度な知見等の修得により、緊急対処等に係る能力を強化

産業制御システムの特徴

○　産業制御システムと一般的な情報システムの違い

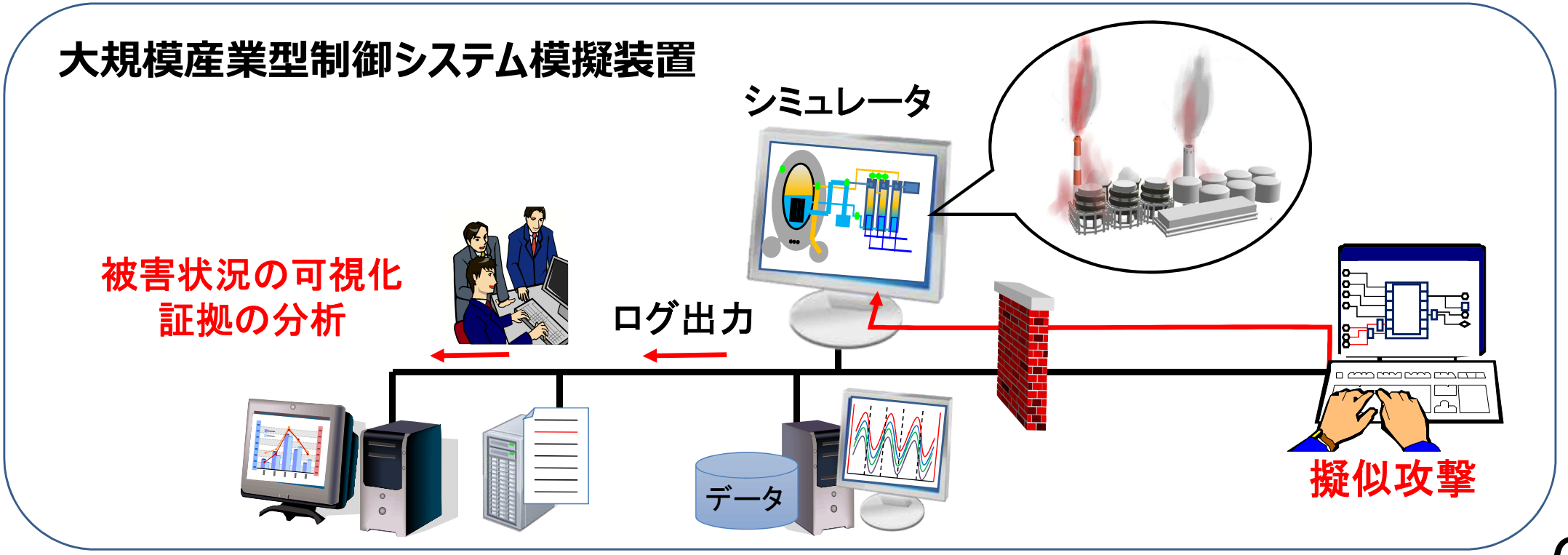
分　類	産業制御システム	一般的な情報システム
用途	物理機器の制御 ・発電所 ・化学プラント	データ処理 ・資料の作成・管理 ・メール
可用性	24時間365日安定稼働 停止できない	再起動は許容範囲
製品ライフサイクル （サポート期間）	10～20年以上	3～5年

事案発生時に必要となる緊急対処等について、
産業制御システムを対象とした手法を確立・検証する必要

大規模産業型制御システム模擬装置の概要

○ 大規模産業型制御システム模擬装置

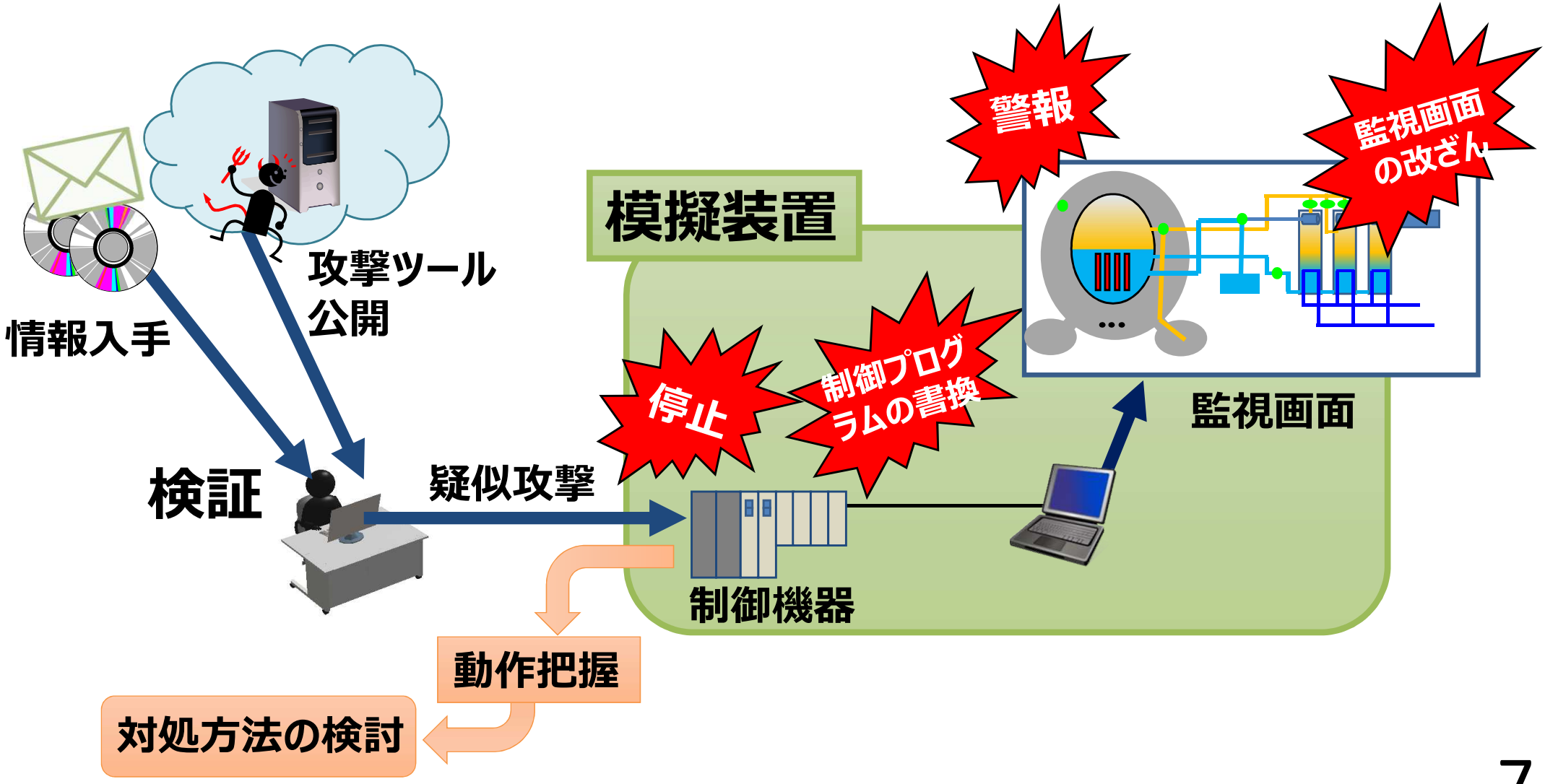
- 産業制御システムに対するサイバー攻撃の再現
  - 疑似攻撃等を行い様々なログ等を出力
- 事案対応時における証拠の検証
  - 被害状況の可視化・証拠の分析による検証の実施



装置の活用事例(１)

○　攻撃に関する知見の醸成

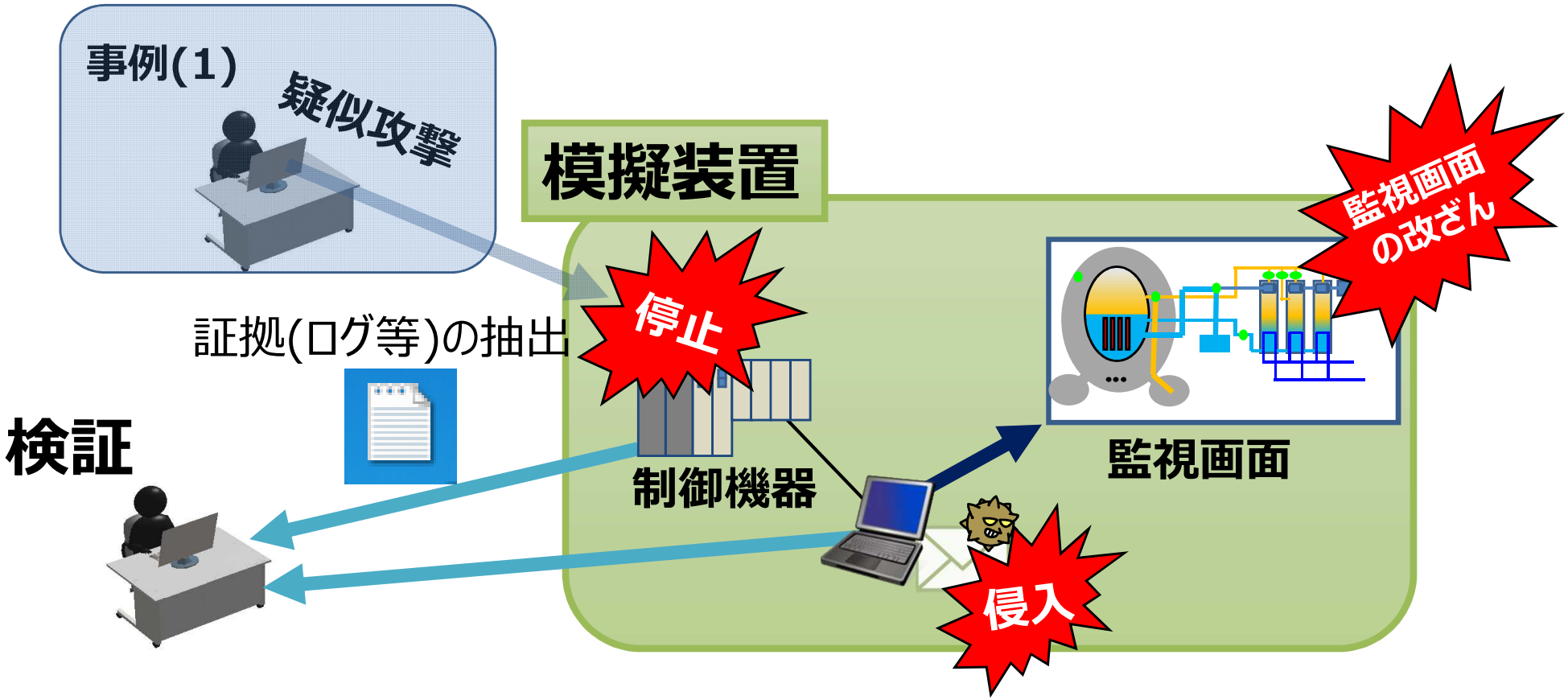
- 情報収集により入手した攻撃ツールの検証



装置の活用事例(２)

○　攻撃への対処能力の向上

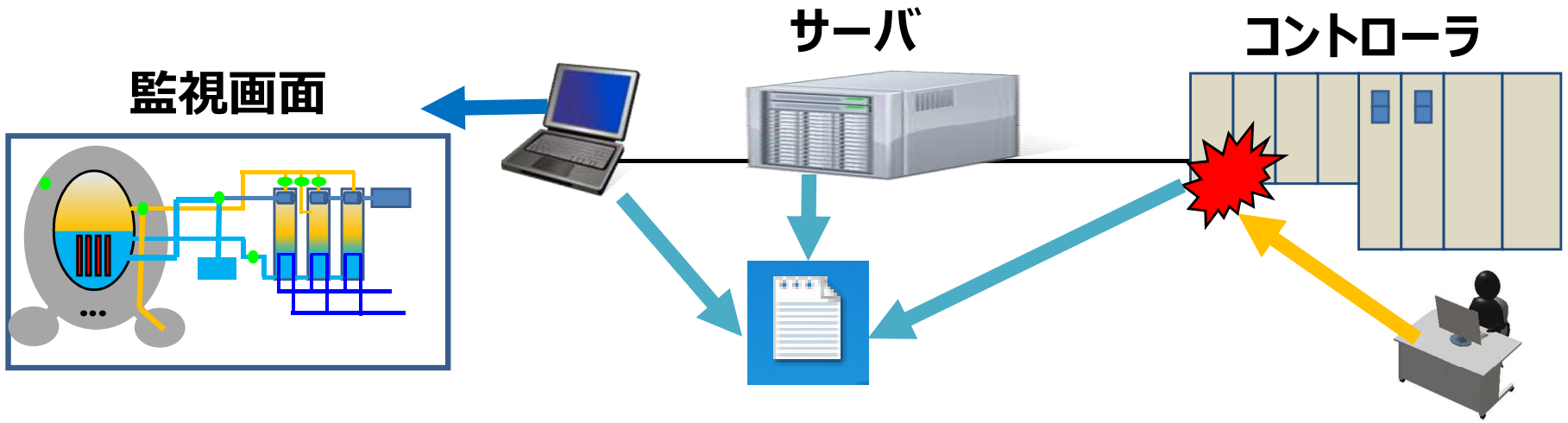
- 攻撃に関する証拠(ログ等)の抽出方法の検証



装置の活用事例(３)

○　実戦的な訓練の実施

- 実機操作を通じた産業制御システムの構造理解
- 事案対処時の状況を再現



産業制御システムのサイバー攻撃に関する対処能力を強化

装置の活用状況

訓練・研修（平成28年度）

実施回数	受講者数
5回	91人

全所属に対する実施割合※1
62.9%

※1　受講所属数（66所属）/全所属数（105所属※2）
※2　警察庁を除く全国情報技術解析課（58所属）及び都道府県警察（47所属）

稼働率（導入後1年間 平成28年2月1日～平成29年1月31日）

稼働率※3
69.0%

※3　検証、環境構築、訓練等における稼働日数（169日）
/勤務日数（245日）

論点

○論点

・実効性のある検証方法について

論点に係る現状と課題

○　現有装置の整備時における背景と対応について

①　重要インフラ（13分野）のうち、主たる対象とする分野の選定

⇒　具体的攻撃事例（海外）等、整備当時の情勢を踏まえて電力・化学分野を優先度の高い分野として選定

②　実装する産業制御システムに係る製品の選定

⇒　電力・化学分野（①）の産業制御システムに係る製品を扱う複数の業者からの聞き取りを基に、シェアが高いと考えられる製品を選定

③　模擬装置の整備形態

⇒　産業制御システムに係る製品のライフサイクルが長いことを踏まえ、検証の継続性を確保するために買取りによって整備

論点に係る現状と課題

○　模擬装置の整備等に係る今後の課題について

①　変遷する脅威への対応

⇒　脅威が刻々と変遷する中で、様々な分野・製品から対象とするものをどのようにして選定していくべきか

②　将来における更新の在り方

⇒　現有装置で検証可能な製品が実際の産業制御システムで使用されている間は現有装置を維持管理する必要があるところ、将来の更新(増強)をどのように行うべきか