高圧ガス保安法改正に伴う サイバー事故原因究明調査(令和5年改正)と 国内外で発生するサイバーインシデントについて

2026年3月13日

令和７年度 高圧ガス製造事業者保安検査説明会
及びコンプライアンス研修会

独立行政法人情報処理推進機構
産業サイバーセキュリティセンター調査分析部
サイバーインシデント調査室　中山　顕

IPA Better Life with IT

1.自己紹介とIPAの紹介
2.高度化・巧妙化するサイバー攻撃
3.ランサムウェア
4.海外インシデント事例
5.法令関係
6.調査事業
7.普及展開

1.自己紹介とIPAの紹介

2.高度化・巧妙化するサイバー攻撃

3.ランサムウェア

4.海外インシデント事例

5.法令関係

6.調査事業

7.普及展開

1.自己紹介とIPAの紹介

<名前>

なかやま　あきら
中山　顯

■組織
独立行政法人情報処理推進機構（IPA）
　産業サイバーセキュリティセンター（ICSCoE）
　　調査分析部 サイバーインシデント調査室（CIIL）
■担当
・原因究明調査責任者
・ICSCoEに関わる外部向け及び普及啓発活動の責任者　等
■略歴
富山県富山市生まれ

東京工科大学工学部で電子工学（材料）分野の助手、大手Sierを経て現在に至る
IPAでは戦略企画部として制度設計など経産省と連携し政策立案に関与　2018年より現職
2023年12月21日に施行された「高圧ガス保安法等の一部を改正する法律」に伴う組織の設置
2024年より「海事におけるサイバーセキュリティ検討会」委員
2025年「鉄道事業者の重要システムにおける情報セキュリティ対策等検討委員会」オブザーバ
2025年「公益社団法人2025年日本国際博覧会協会が用意する設備制御システムにおけるセキュリティ確保支援」PM　等

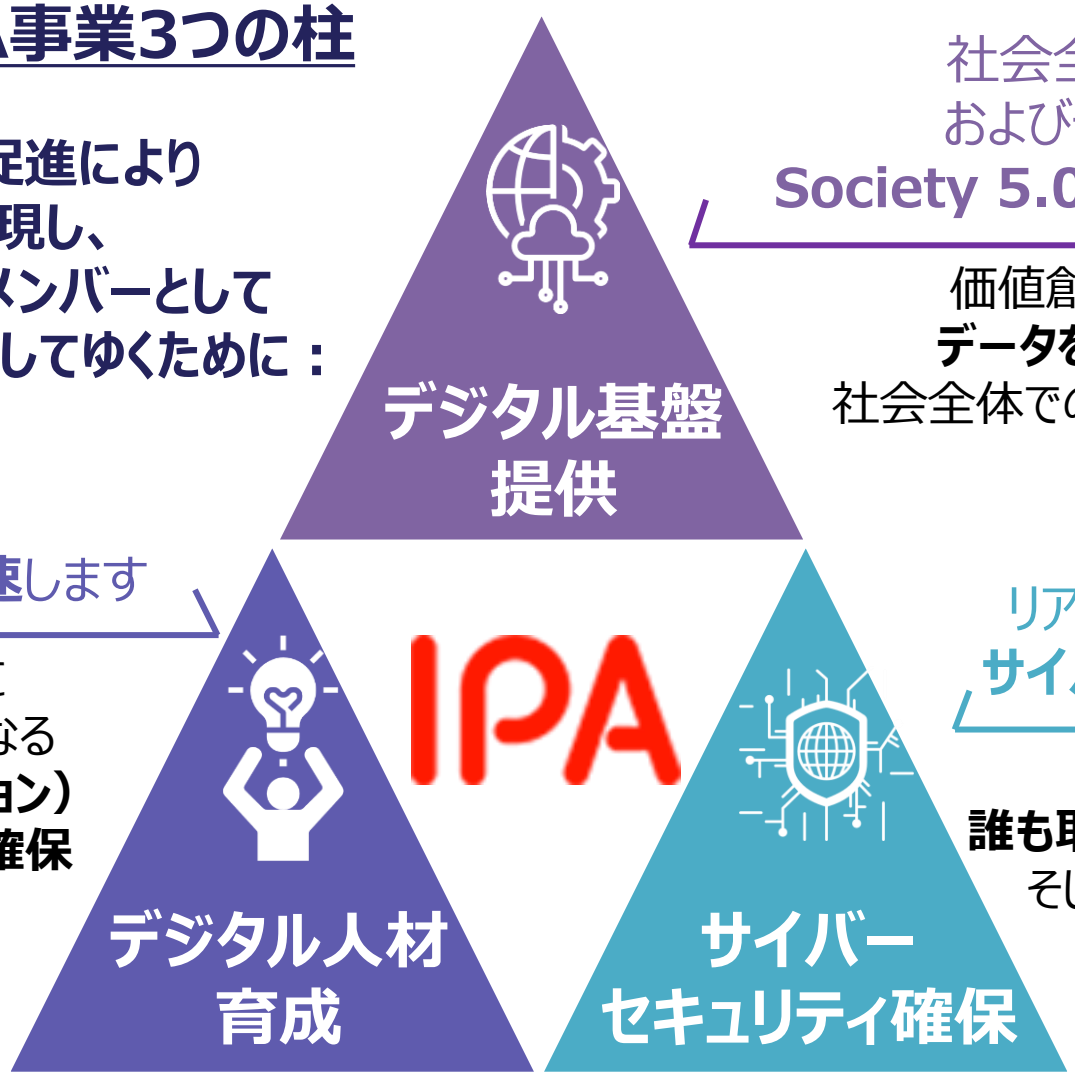
1.自己紹介とIPAの紹介

独立行政法人情報処理推進機構（以下、「IPA」という。）は、
情報処理の促進に関する法律の一部を改正する法律（平成14年法律第144号）
により設立された経済産業省（以下、「経産省」という。）の政策実施機関
情報処理・情報セキュリティに関する政策を産業・社会の基盤強化へとつなげる取組みを推進

1.自己紹介とIPAの紹介

第五期中期計画のIPA事業3つの柱

デジタル技術の利用促進により
豊かな暮らしを実現し、
グローバルコミュニティのメンバーとして
直面する課題の解決に貢献してゆくために：



DX・イノベーションで
新たな価値を生む
デジタル人材の育成を加速します

リテラシー底上げと同時に
課題解決と成長の切り札となる
破壊的な変革（ディスラプション）
をリードできる人材の育成・確保

社会全体のアーキテクチャ設計
およびデータスペース整備による
Society 5.0実現のための基盤を提供します

価値創造と競争力の源泉となる
データを使いこなす環境の整備と
社会全体での**デジタルエコシステムの最適化**

リアルとサイバーの融合でリスクが高まる
サイバーセキュリティの強化を実現します

国家・経済の**安全保障への貢献**、
誰も取り残さないサイバーセキュリティの確保、
そして**自主的なセキュリティ対策**を支える
インフラの提供

1.自己紹介とIPAの紹介

- セキュリティマネジメントからオペレーションまでトータルな施策・対応を実施（施策イメージ※）：
  ①国家・経済の安全保障に貢献し、②誰も取り残さず、③組織・個人自らのセキュリティ対策をサポートします

	特定	防御	検知	対応	復旧
民間事業者向け	・経営/中小ガイドライン 等 ・内部不正防止ガイドライン ・制御システム・リスクアセスメント ・セキュリティ自己宣言制度 ・セキュリティプレゼンター制度	・製品セキュリティ評価・認証 ・暗号モジュール試験・認証 ・CRYPTREC（電子政府推奨）暗号リスト ・脆弱性対策情報DB（JVN iPedia） ・安全なウェブサイトの作り方書 ・セキュリティ啓発コンクール ・セキュリティキャンプ ・中核人材育成プログラム/短期プログラム ・インド太平洋地域向け日米EU産業制御システムサイバーセキュリティウィーク ・脆弱性情報届出制度・脆弱性情報優先提供	・標的型攻撃特定・分析（J-CRAT） ・情報共有枠組（J-CSIP）/ウイルス・不正アクセス届出 ・注意喚起発信（各種メディア活用） ・お助け隊サービス制度	・初動対応支援（J-CRAT） ・サイバーインシデントに関する原因究明調査 ・情報セキュリティ安心相談窓口 ・お助け隊サービス制度（駆付支援、サイバー保険）	
政府機関・自治体等向け	・情報セキュリティ監査（独法等） ・政府機関情報システム監査 ・クラウドサービスセキュリティ評価（ISMAP）	・脆弱性情報優先提供 ・脆弱性簡易診断（自治体等）	・セキュリティ監視（独法等） ・ウェブ脆弱性監視（政府要請主体）	・重要イベント対処調整支援 ・重大事象の原因究明調査	

サイバー情勢研究・分析
情報セキュリティ10大脅威、情報セキュリティ白書
シン・テレワークシステム/自治体テレワークシステム for LGWAN

※ 世界で利用されている米国立標準研究所（NIST）のセキュリティ対策検討・推進フレームワーク、「サイバーセキュリティ・フレームワーク」の各フェーズに沿ったセキュリティ支援サービスを提供

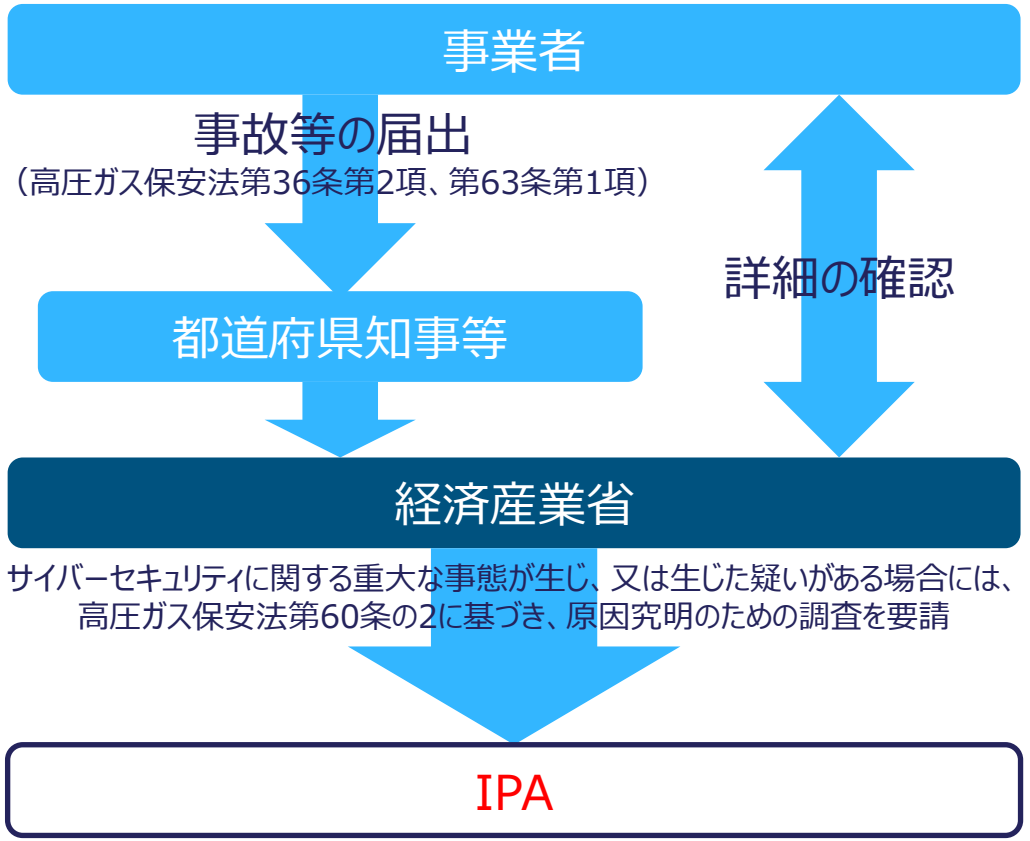
1.自己紹介とIPAの紹介

サイバーインシデントの再発防止に向けた調査

令和5年12月21日(木)より施行された、
「高圧ガス保安法等の一部を改正する法律」の規定により、サイバーセキュリティに関する重大な事態が生じ、又は生じた疑いがある場合には、経済産業大臣からの要請により、IPAにて原因究明調査を実施

再発防止を目的とした調査であり、調査結果を踏まえて、サイバーセキュリティ水準の向上を図るための対策（ガイドラインの見直し等）を講じることを想定

また、事故調査対象企業にも再発防止の観点から調査結果については経産省やIPAから共有することを想定



1.自己紹介とIPAの紹介

2.高度化・巧妙化するサイバー攻撃

3.ランサムウェア

4.海外インシデント事例

5.法令関係

6.調査事業

7.普及展開

2.高度化・巧妙化するサイバー攻撃

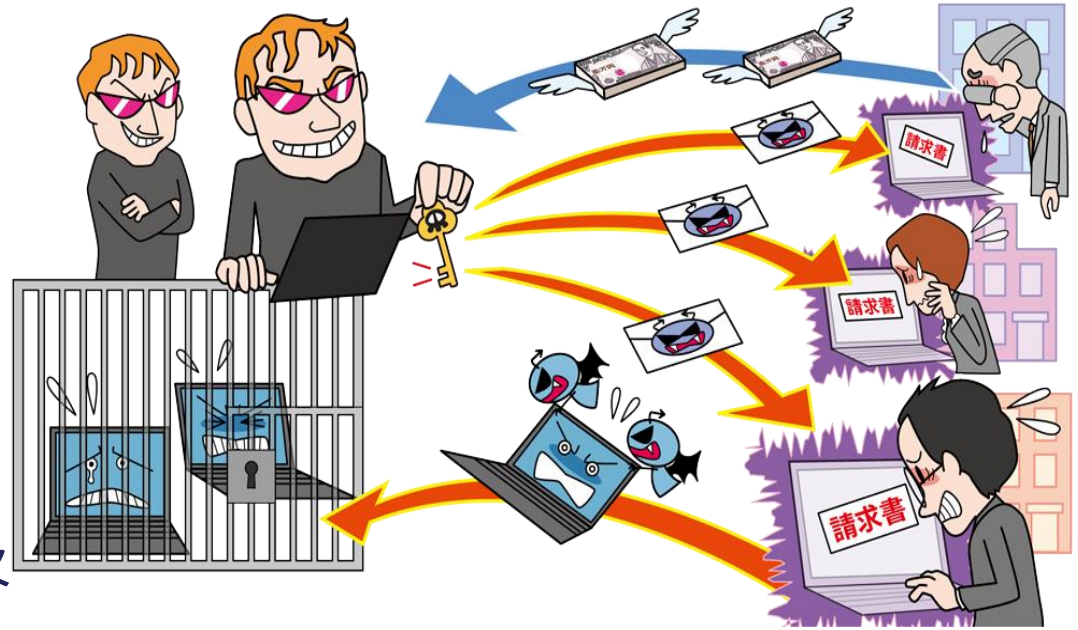
昨今のサイバー攻撃は、企業等の情報を暗号化して金銭をゆすり取る「ランサムウェア攻撃」や、
国家支援型の攻撃集団等が特定の企業を執拗に狙う「標的型攻撃」など、多種多様となっている
加えて、サイバー攻撃が高度化・巧妙化するとともに、あらゆるものがネットワークにつながり、
攻撃の起点が増加したことで、サイバー攻撃が社会や産業に「広く」、「深く」影響を及ぼすようになっている

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

1.自己紹介とIPAの紹介
2.高度化・巧妙化するサイバー攻撃
3.ランサムウェア
4.海外インシデント事例
5.法令関係
6.調査事業
7.普及展開

3.ランサムウェア

身代金（ランサム）を要求する不正なソフトウェア
業務用端末やサーバへ侵入し、保管されているファイルを暗号化することにより、正常な業務運用を妨げる



- **被害の影響**
  情報システムや制御システムの動作が停止または不具合を起こし、業務全体に大きな支障をもたらす。
- **近年の動向**
  ハッカー集団が開発・提供する「RaaS※」の普及により、専門的な知識がなくともランサムウェアの利用が可能となり、攻撃のリスクは一層増大している。

※RaaS : Ransomware as a Service

3.ランサムウェア

ランサムウェアによる被害

- 2025年9月アサヒグループホールディングス、同年10月アスクルへの連続して各社より公表
- それぞれ、犯行声明がランサムウェアグループから公開されている
- 2021年7月ニップンへのサイバー攻撃以来の犯行声明か、この時は2022年初頭まで復旧時間を要した

RansomHouseが公開した犯行声明

日本経済新聞：https://www.nikkei.com/article/DGXZQOUC30D750Q5A031C2000000/

3.ランサムウェア

ランサムウェアによる被害の増加はAI技術か

- フィッシングメールの高度化
  - AIを活用して標的となる組織の文化や人間関係を分析し、より巧妙で信憑性の高いフィッシングメールを作成
  - 自然な日本語の文章を大量に生成できるため、言語の壁が下がり日本の組織も標的になりやすく

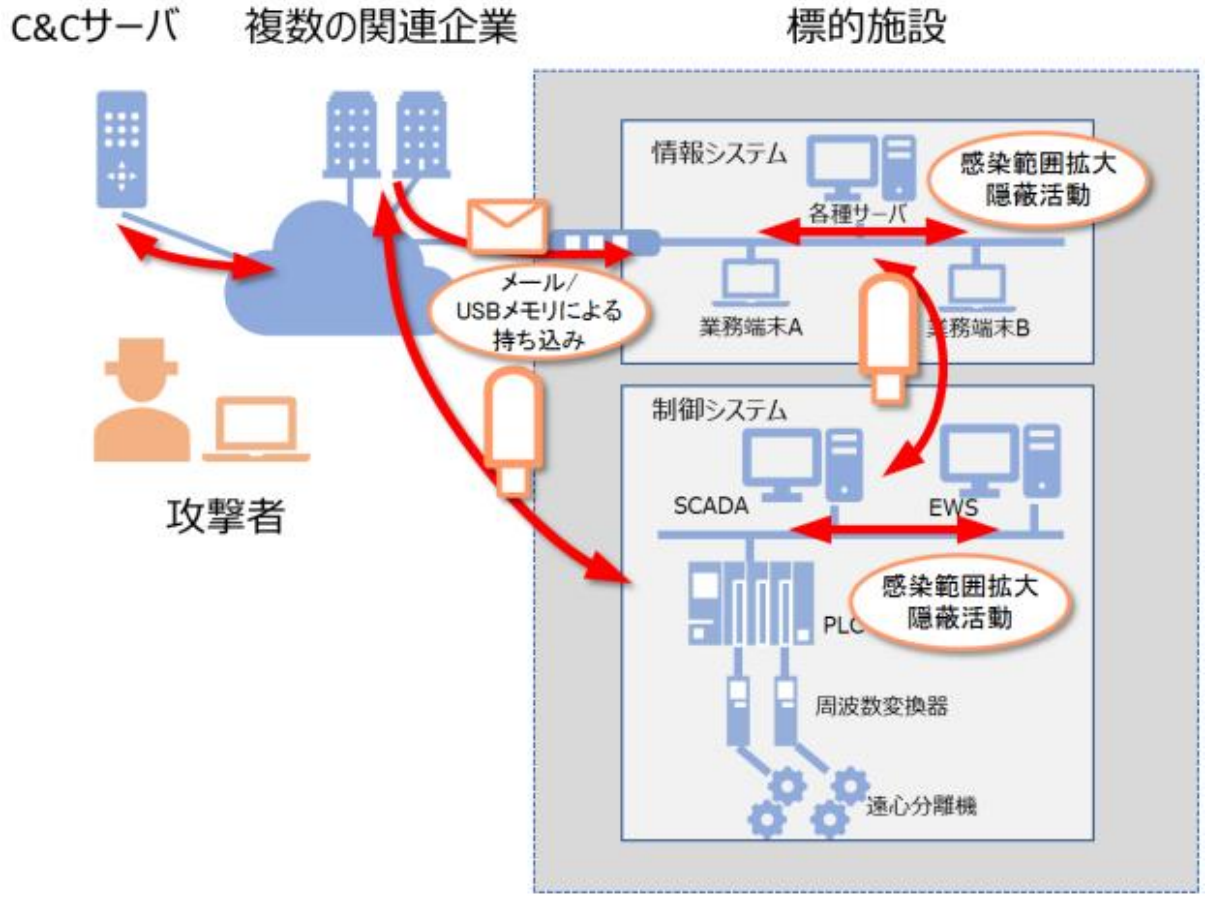
1.自己紹介とIPAの紹介
2.高度化・巧妙化するサイバー攻撃
3.ランサムウェア
4.海外インシデント事例
5.法令関係
6.調査事業
7.普及展開

4.海外インシデント事例

Stuxnetによるイラン核燃料施設へのサイバー攻撃（2010年）

イランの核燃料施設に、ウイルス（Stuxnet）を仕込んだUSBメモリが持ち込まれた後、制御システムの近くの床に置かれていることに気付いた職員がその**USBメモリを接続**Stuxnetに感染

当該核燃料施設の制御システムは、インターネットに接続されていなかった

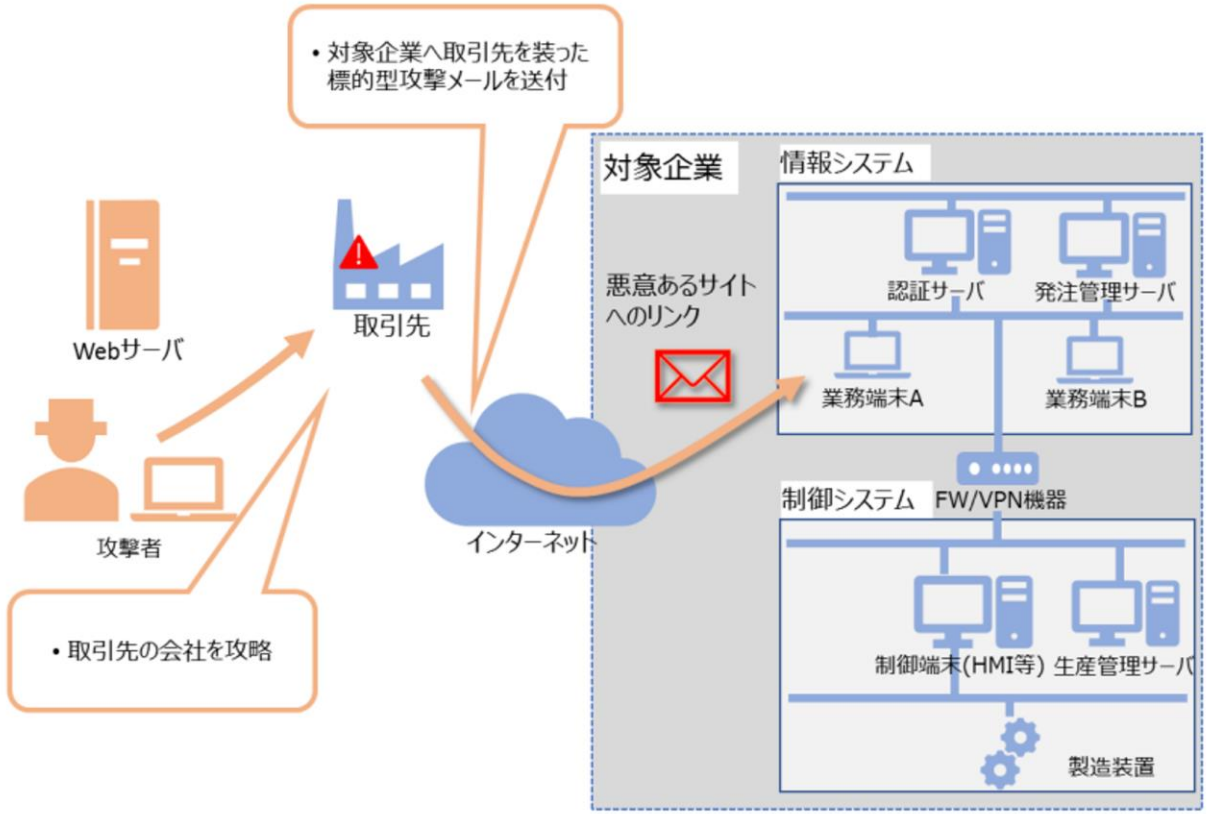


4.海外インシデント事例

アルミ製造企業に対する大規模ランサムウェア攻撃（2019年）

世界有数のアルミニウム生産企業Norsk Hydro社がランサムウェアの被害を受け数カ月の長期間にわたり生産量が低下

攻撃者は取引先の**従業員になりすまし**取引先を装った標的型攻撃メールを企業に送りランサムウェア感染2019年の半期合計の損失は、65-77 億円と見積もられている



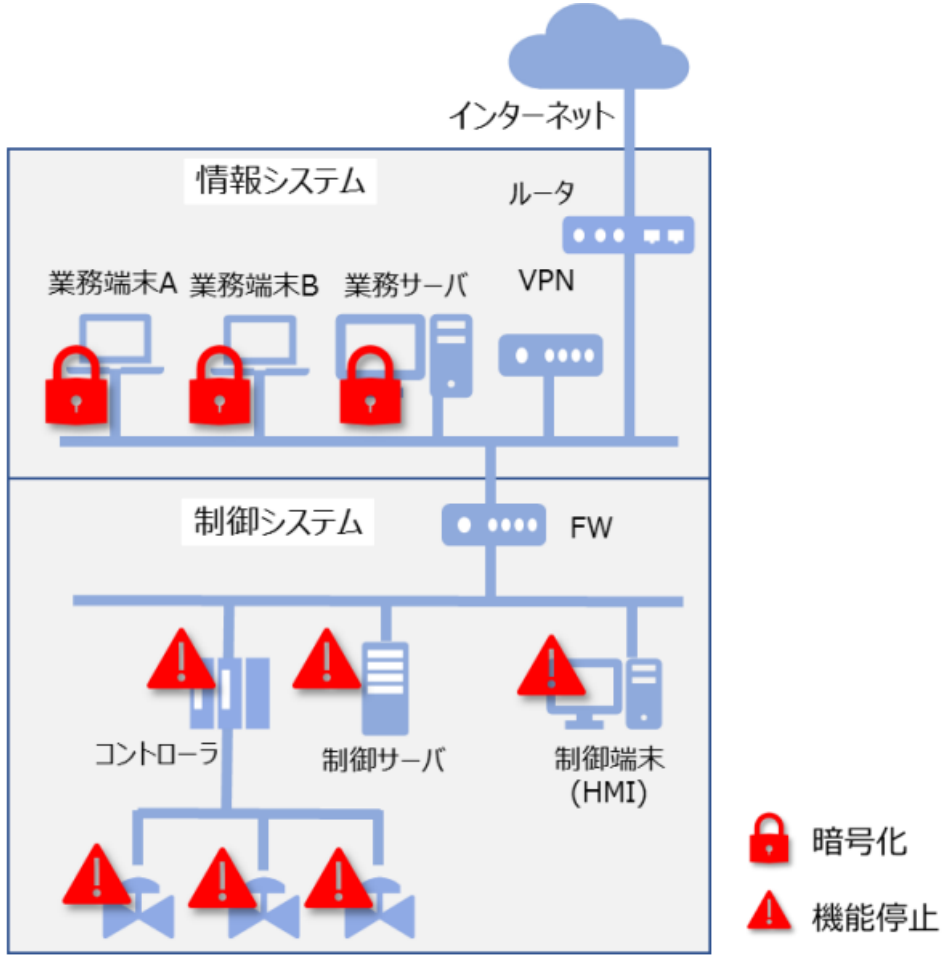
4.海外インシデント事例

米国最大手のパイプラインのランサムウェア被害（2021年）

米国の燃料パイプライン最大手の Colonial Pipeline社 が、サイバー攻撃によりランサムウェアに感染し業務を停止

6日間続いたパイプラインの停止により、首都ワシントンのガソリンスタンドのうち**約81%でガソリンが売り切れ**状態など**市民生活に大きな影響**を与えた

攻撃者はインターネット上から VPN の正規のアカウントを使って侵入してきたと考えられている



1.自己紹介とIPAの紹介
2.高度化・巧妙化するサイバー攻撃
3.ランサムウェア
4.海外インシデント事例
5.法令関係
6.調査事業
7.普及展開

5.法令関係 –法律施行までの経緯-

改正法の閣議決定

令和４年３月４日(金)

「高圧ガス保安法等の一部を改正する法律案」が閣議決定されました （経済産業省）

https://www.meti.go.jp/press/2021/03/20220304004/20220304004.html

第208回通常国会（常会）で成立、公布

令和 4年 6月22日 (水)

「高圧ガス保安法等の一部を改正する法律（令和4年法律第74号）」

https://www.shugiin.go.jp/internet/itdb_housei.nsf/html/housei/kaiji208_l.htm

本法案の施行

令和5年12月21日(木)

認定高度保安実施事業者制度の運用を開始し、燃料電池自動車等の規制の一元化を実施しました（経済産業省）

https://www.meti.go.jp/press/2023/12/20231221003/20231221003.html

5.法令関係 –改正対象法律-

「高圧ガス保安法等の一部を改正する法律（令和四年法律第七十四号）」の改正対象となる法律

- **高圧ガス保安法（昭和二十六年法律第二百四号）**
- ガス事業法（昭和二十九年法律第五十一号）
- 電気事業法（昭和三十九年法律第百七十号）
- 情報処理の促進に関する法律（昭和四十五年五月二十二日法律第九十号）

5.法令関係–改正対象法律-

○高圧ガス保安法（昭和二十六年法律第二百四号）

（調査の要請）

第六十条の二　経済産業大臣は、**認定高度保安実施者**その他の**保安の確保上特に重要な者**として経済産業省令で定める者において保安に係るサイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティ※をいう。）に関する**重大な事態が生じ**、又は**生じた疑いがある場合**において、**必要があると認めるとき**は、独立行政法人情報処理推進機構に対し、その原因究明のための調査を要請することができる。

※サイバーセキュリティ：
サイバーセキュリティ基本法（平成二十六年法律第百四号）
（定義）
第二条　この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。

5.法令関係–改正対象法律-

○情報処理の促進に関する法律（昭和四十五年五月二十二日法律第九十号）

第三節　業務等

（業務の範囲等）

第五十一条　機構は、第四十条の目的を達成するため、次の業務を行う。

一　～　九　（略）

十　高圧ガス保安法（昭和二十六年法律第二百四号）第六十条の二に規定する調査を行うこと。

十一　ガス事業法（昭和二十九年法律第五十一号）第百七十条の二に規定する調査を行うこと。

十二　（略）

十三　電気事業法（昭和三十九年法律第百七十号）第百五条の二に規定する調査を行うこと。

1.自己紹介とIPAの紹介
2.高度化・巧妙化するサイバー攻撃
3.ランサムウェア
4.海外インシデント事例
5.法令関係
6.調査事業
7.普及展開

6.調査事業　-調査対象の事業者-

- 対象事業者は各省令で規定されており、現時点でIPAに共有されているのは、次の通り

【高圧ガス関係】

認定事業者、第一種製造者（15,000者）

【ガス関係】

認定事業者、一般ガス導管事業者（193者）、ガス製造事業者（28者）

【電力関係】

認定事業者、一般送配電事業者（大手10社）、発電事業者（14社）

6.調査事業　-調査対象の範囲-

次の①～③のうち、「重大な事態」であると経産省が判断する場合に、IPAに調査要請

「**重大な事態**」については、**供給支障など**が考えられるが、調査を要請する事案については、経産省が個別に判断

調査対象は、**基本的にはOTシステム**※とするが、調査を要請する事案については、経産省が個別に判断

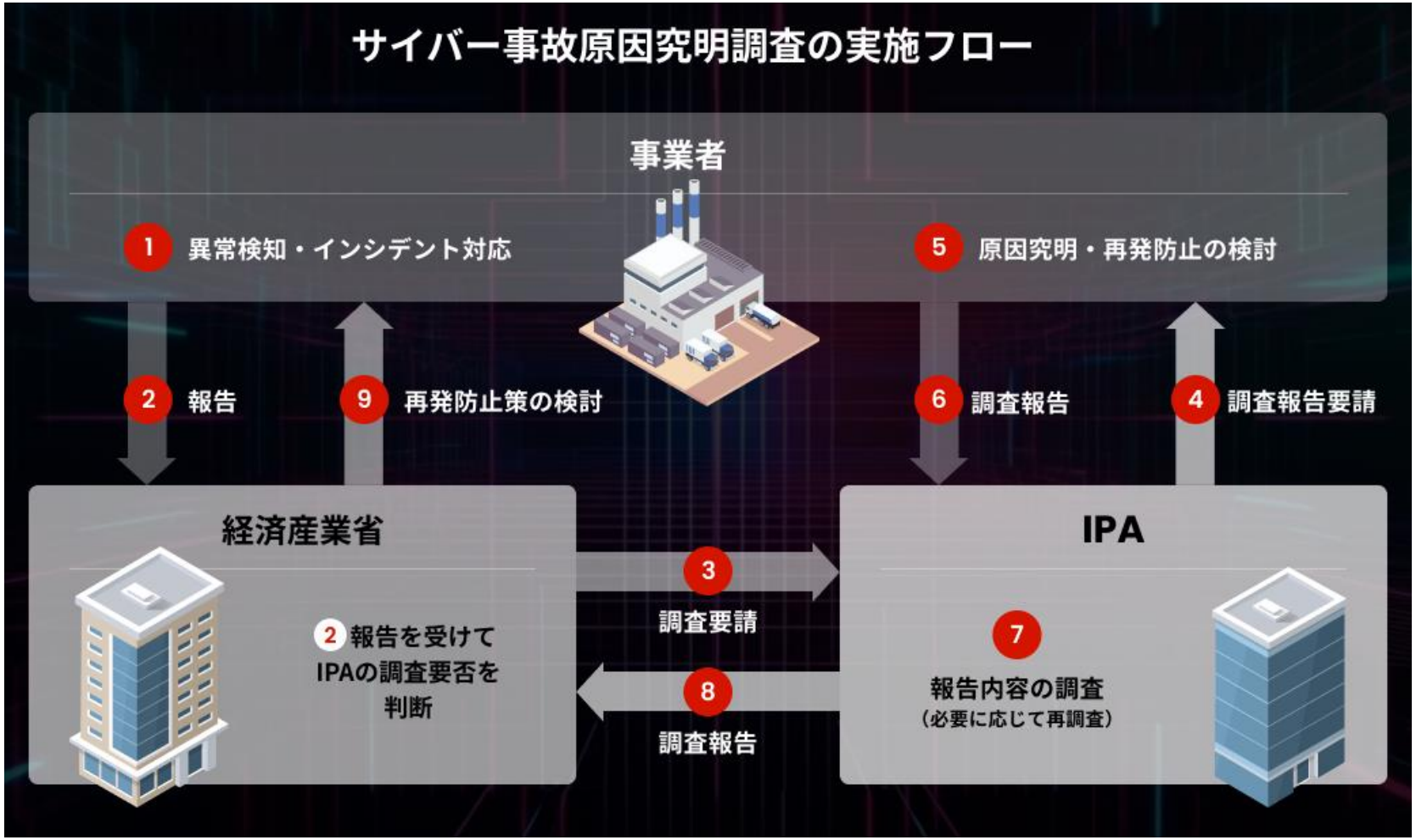
① **報告義務が課されている事故**のうち、**サイバー攻撃に起因するおそれ**があるもの

② NISCの「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報連絡によって報告されるもの

③ その他**サイバー攻撃が疑われる事象**であって、**把握が必要**と経産省が判断するもの

※基本的にOTシステムが対象でありITシステムのみが対象となることはないが、ITシステムへの侵入を通じてOTシステムに影響が及ぼされたケース等においてはOTシステムに加えITシステムも対象となり得る。

6.調査事業　-調査方法と体制-



6.調査事業　-調査方法と体制-

IPAによる調査は、書面調査と現地調査の２段階で実施

書面調査のみで十分に原因を特定できた場合には、**現地調査は行わない**

※例えば、原因分析、再発防止策の検討が十分である場合は現地調査を行う必要はないものと考えられる一方で、報告書の記載や再発防止策が十分でない場合は、現地調査を行う必要があるものと考えられる。

書面調査は、「インシデント調査報告書」を事業者がIPAに提出することにより実施

6.調査事業　-調査方法と体制-

現地調査について、内容や日数等については、個別事案ごとに経産省・IPAと調査対象事業者で協議の上で決定

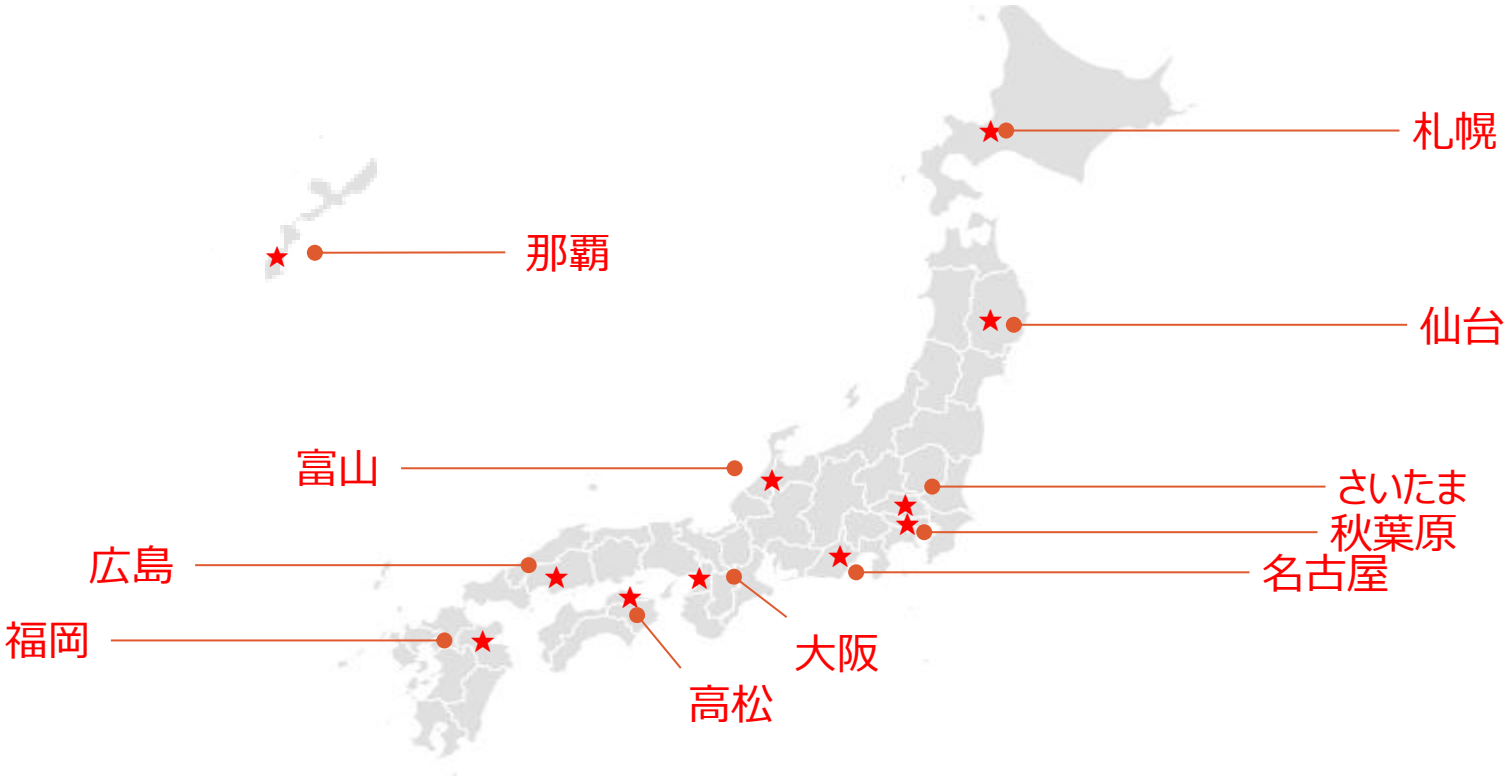
競争領域への立ち入りを含め、現地調査を行う際、情報処理の促進に関する法律上の守秘義務がかかったIPAの職員や契約ベースでの守秘義務がかかったIPAのサイバーセキュリティアナリスト（CSA）が調査を実施

なお、調査体制は事前に事業者に通知するものとする

1.自己紹介とIPAの紹介
2.高度化・巧妙化するサイバー攻撃
3.ランサムウェア
4.海外インシデント事例
5.法令関係
6.調査事業
7.普及展開

7.普及展開

- 2025年では「ガス事業者」「高圧ガス事業者のうち認定事業者」を対象に、高圧ガス保安法等の改正に伴う法律改正（2023年12月21日施行）の内容及びサイバー攻撃の事例等を紹介するため、全国各地11箇所を巡回して説明会を開催。



・述べ 400 者以上が参加
・三重県内の認定事業者（4者）が参加