JPCERT CC®

ICS関連のセキュリティインシデント対応に備えて

- 製造業を例に対応体制の整備上の課題と対策の第一歩を解説 -

JPCERTコーディネーションセンター
制御システムセキュリティ対策グループ
マネージャー 河野一之

目次

注）
記載内容は本資料作成時のものです。
免責事項：記載内容の活用により生じた責任、負担、損害および損失について、JPCERT/CCは一切責任を負わないものとします。

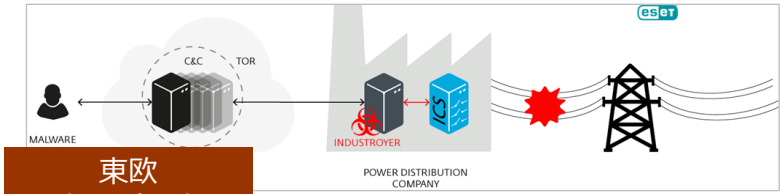
目次

ICSに対するサイバー脅威事案の一例

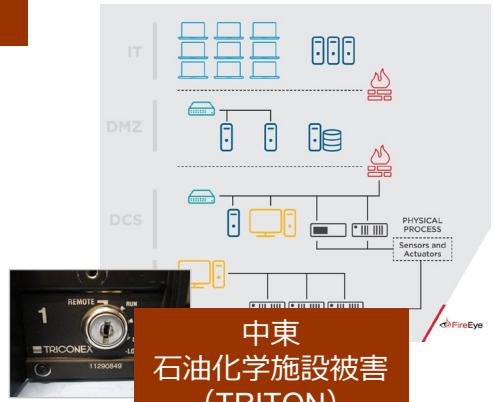
従来のICSに対するサイバー脅威といえば・・・

中東
核燃料施設被害
（Stuxnet）

欧州
製鉄所被害



東欧
変電所被害
（Industroyer）



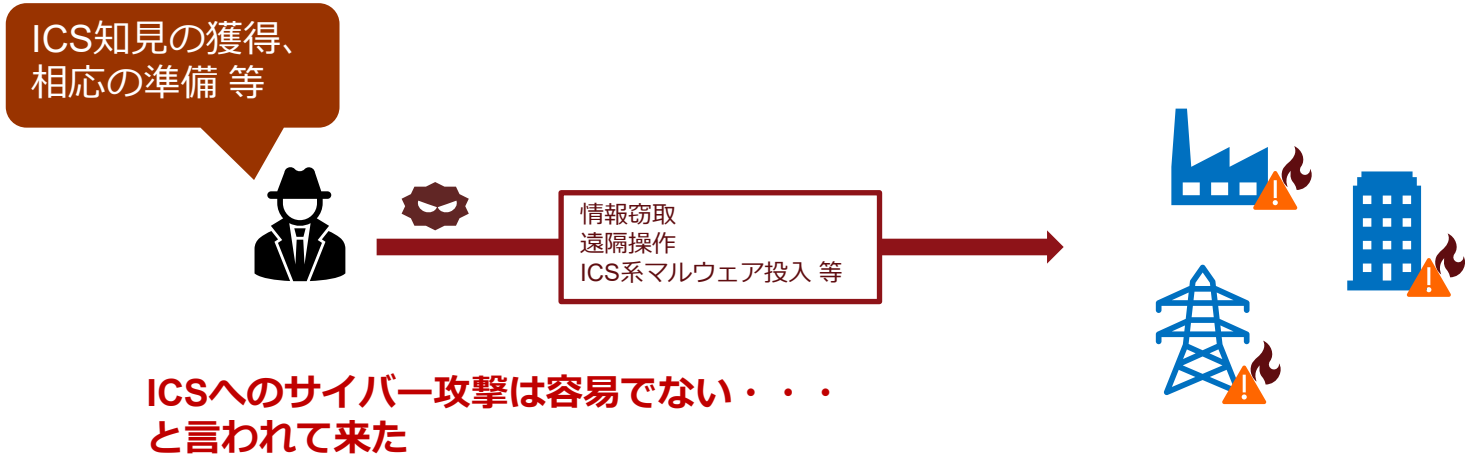
中東
石油化学施設被害
（TRITON）

参考：
JPCERT/CC「Stuxnet – 制御システムを狙った初のマルウエア –」（https://www.jpcert.or.jp/ics/2011/20110210-oguma.pdf）
Bundesamt für Sicherheit in der Informationstechnik「Die Lage der IT-Sicherheit in Deutschland 2014」（https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile&v=2）
キヤノンマーケティングジャパン「産業制御システムに最大級の脅威をもたらすマルウェア「インダストロイヤー」」（https://eset-info.canon-its.jp/malware_info/trend/detail/170620.html）
Mandiant「Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure」（https://www.mandiant.com/resources/blog/attackers-deploy-new-ics-attack-framework-triton）

ICSに対するサイバー脅威

■ 従来のICSに対するサイバー脅威の認識・・・

これまで	ICS/OTに直接影響を与えるもの	ICS上の情報窃取／遠隔操作 ICS特化型マルウェア



ICSへのサイバー攻撃は容易でない・・・
と言われて来た

注目した近年のICS影響が想定された事例（抜粋）

	注目したICS関連のインシデント事例（時期）	ランサムウェア事案
2016	東欧：公共電力施設被害（2016）	-
	複数国：自動車製造等製造業被害（2017）	✓
	複数国：製薬、菓子等製造業被害（2017）	✓
	中東：石油生産業被害（2017）	-
	北欧：アルミニウム製造業被害（2019）	✓
	米国：発電機製造業被害（2019）	✓
	米国：自動車製造業被害（2020）	✓
	米国：エネルギー製造供給業被害（2021）	✓
	米国：食肉加工業被害（2021）	✓
	欧州：光学機器製造業被害（2021）	✓
	欧州：製薬製造業被害（2021）	✓
	米国：菓子製造業被害（2022）	✓
	米国：化学製造業被害（2022）	✓
	アジア：電子機器製造業被害（2022）	✓
	欧州：半導体製造業被害（2022）	✓
2022	東欧：公共電力施設被害（2022）	-

出典：MITRE ATT＆CK for ICS等を参考にJPCERT/CC調べ（2023年）
参考：MITRE ATT＆CK for ICS（https://collaborate.mitre.org/attackics/index.php/Main_Page）

ランサムウェア事案の中で、
ICSが何らかの影響を受ける事案が増加か

ICSに関する深い知見を持たずとも、影響を与えるサイバー攻撃が可能に

ランサムウェアがもたらしたICSに対する脅威の影響

■ ICSに対するサイバー脅威の変化

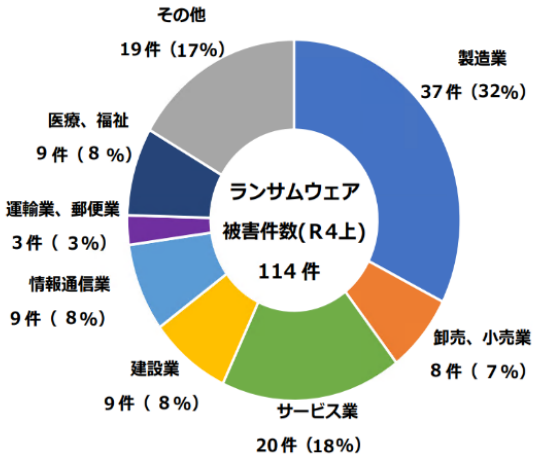
近年	ICS/OTに間接影響を与えるもの	**ランサムウェア**感染

ICS利用組織での「ランサムウェア」事案が取りざたされるケースの増加

- **ICSに直接影響を与えずとも、（生産停止等の）ICSの運用影響を与える**
  - **運用影響を通じて事業影響を与えることも可能であることが顕在化**

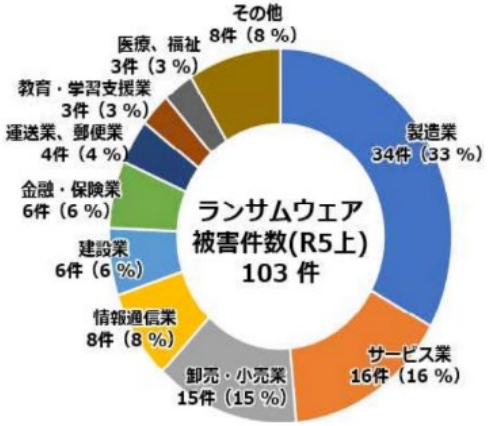
国内製造業の被害状況：ランサムウェア事案統計より

令和4年上半期



注　図中の割合は小数第1位以下を四捨五入しているため、総計が必ずしも100にならない。

令和5年上半期



注　図中の割合は小数点第1位以下を四捨五入しているため、総計が必ずしも100にならない。

— 製造業における被害の割合は、昨年と今年の同時期ともに**トップ**

— **被害の減少は見られない**（注：ICS被害とは限らないが生産影響は起きうる）

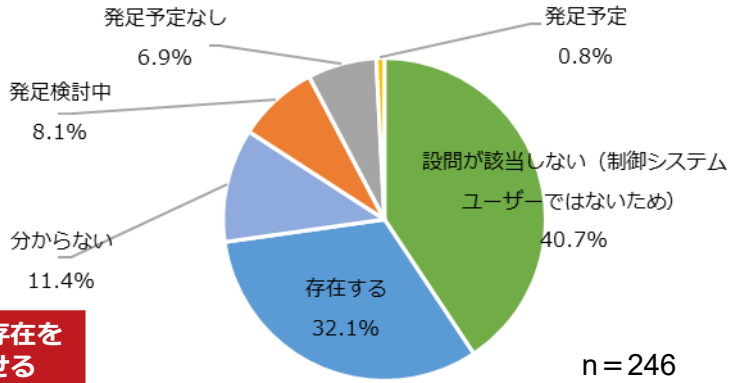
参考：
警察庁「令和４年上半期におけるサイバー空間をめぐる脅威の情勢等について」（https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf）
警察庁「令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について」（https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf）

目次

ICSを対象とするSIRT構築状況 - アンケート結果から

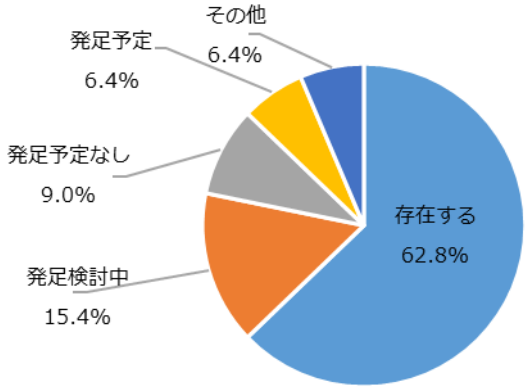
設問：自身の組織内に制御システムを対象とするセキュリティインシデント対応体制（SIRT）が存在するか？

制御カンファレンス2022



n＝246

制御カンファレンス2023



n＝78

一定数の存在をうかがわせる

存在する	79
発足予定	2
発足検討中	20
発足予定なし	17
分からない	28
設問が該当しない（制御システムユーザーではない）	100
合計	246

存在する	49
発足予定	5
発足検討中	12
発足予定なし	7
その他	5
合計	78

JPCERT/CCへの問い合わせ・相談の変化

組織A

インシデント対応を想定した、ICSの資産管理部署はどこが担うべきか？

ICSのインシデント対応を想定すると、どういった事象を報告してもらうべきか？

組織B

組織C

ある拠点でインシデントが発生したが、ICSまで調査すべき認識が無かった。
今思えば調査すべきだった。ICS対応準備を進めたい

・・・etc

最近の問い合わせや相談の共通点は
「ICS関連のインシデント対応」の想定

ICSに対するサイバー脅威をどう考えるか？

■ ランサムウェアはICSに対するサイバー脅威の関心を高めたが・・・

近年	ICS/OTに間接影響を与えるもの	**ランサムウェア**感染

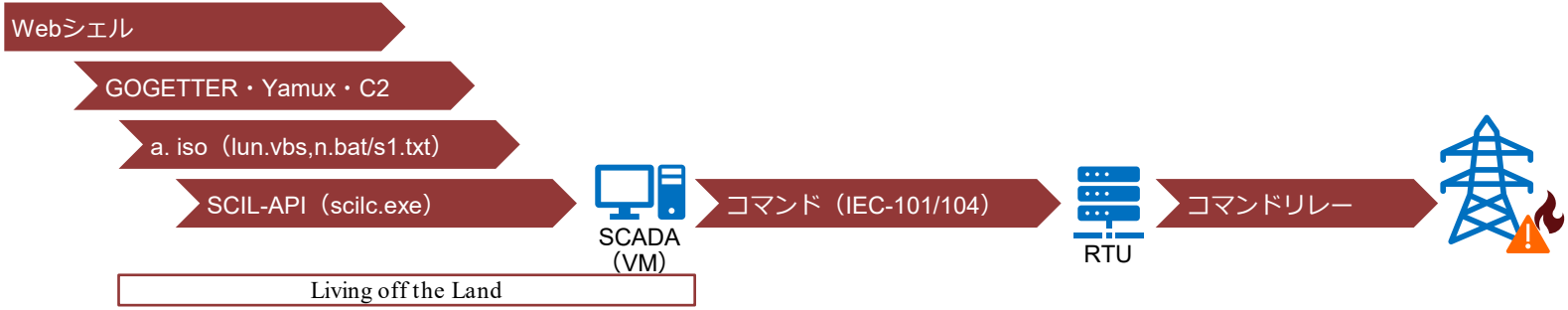
ICS利用組織での「ランサムウェア」事案が取りざたされるケースの増加

➢ **ICSに対するサイバー脅威を、より身近なものとさせたかも知れない**

しかし、ICSに対するサイバー脅威は「ランサムウェア」だけだろうか・・・？

ICSに対する直接的なサイバー脅威は今も（一例）

Sandwormによるウクライナ変電所へのサイバー攻撃（2022/10）



デンマーク変電所へのサイバー攻撃（2023/05）

米国水道施設へのサイバー攻撃（2023/11）

参考：
Mandiant「Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology」（https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology）
Mandiant「SandwormがOT（運用技術）に対する新たな攻撃を使用してウクライナの電力供給を妨害」（https://www.mandiant.jp/resources/blog/sandworm-disrupts-power-ukraine-operational-technology）
SectorCERT「The attack against Danish, critical infrastructure」（https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/sektorcert-the-attack-against-danish-critical-infrastructure-tlp-clear.pdf）
WaterISAC「Water Utility Control System Cyber Incident Advisory: ICS/SCADA Incident at Municipal Water Authority of Aliquippa」（https://www.waterisac.org/portal/tlpclear-water-utility-control-system-cyber-incident-advisory-icsscada-incident-municipal）

見落とされている？- ランサムウェア以外の脅威も

■ ICSに対するサイバー脅威は確かに変化してきたが・・・

これまで	ICS/OTに直接影響を与えるもの	ICS上の情報窃取／遠隔操作 ICS特化型マルウェア
近年	ICS/OTに直接・間接影響を与えるもの	ICS上の情報窃取／遠隔操作 ICS特化型マルウェア **ランサムウェア**感染 等

EWSや他のICS機器におけるマルウェア感染も散見される等、
ランサムウェア以外のICSへの脅威も依然として存在

目次

SIRTの構築要件 - ICSを考慮するには・・・

■ 一般的なSIRT構築の要件には次のものがある（一例）

組織要件

- 例：要員および予算の確保、活動方針（「安全の確保」等の対応上の留意点整理を含む）の検討、チームおよび要員の役割りの検討等

機能要件

- 例：インシデント管理（未然防止活動、インシデント検出活動および対応等）

CSIRTに関する上述の要件を記した参考文献は種々公開されているが、
「ICSを考慮したポイント」が記載されているものはごくわずか

ゆえにICSを考慮した構築検討や運用を行う組織は手探り状態
（JPCERT/CCへの相談等で解決へ）

ICSを対象とするSIRT構築の課題-コミュニティー紹介

■ 製造業のICSセキュリティ担当者コミュニティーを形成して推進

コミュニティー概要（JPCERT/CC主催）

20
組織以上
（発表時点）

複数業種
機器製造・化学鉄鋼・製薬
光学・食品 等

ICS セキュリティ 担当者

■ 次の点を主なモチベーションとして活動してきた

- ICSセキュリティの共通課題をともに考える
- 実務者ベースでの実践的な検討を行う
- JPCERT/CCの知見を共有し実務的な協力関係強化
- 個々でなく協力することで攻撃者への対抗力を醸成
- 「ICSを対象とするSIRT」の適切な構築を後押し

取り組み例

➢ 取り組み例：

実績：

✓ ICSにおけるセキュリティアセスメントについて

✓ 近年のICS関連インシデントにみるマルウェアの傾向と対策

直近：

✓ **サイバー要因を想定すべきICS特有事象の検討**

✓ **ICSを対象とするインシデント対応体制に関する要件の検討**

ICSを対象とするSIRTの機能構築の課題 - 取り組み例

■ サイバー要因を想定すべきICS特有事象の検討

— 「ICSを対象とするSIRT」構築の実務的な着手ポイントは種々あるが
「事象把握」の仕組みづくりは適切なSIRT構築の重要な一歩である

— ランサムウェアばかりではない着目すべき「ICS特有事象」とは

— 判別は容易ではないが業種を問わず製造業での共通的な着眼点

No	ICS特有の事象例	サイバー要因の判別
1	制御機器の異常検知（パラメーターの異常な値の表示等）	比較的困難
2	制御機器自体の動作遅延（HMIの応答が遅い等）	
3	制御機器の故障（機器の一部の損傷等、交換が必要な事態）	
4	製品の不良率の増加（品質基準を満たさない製品の増加等）	
5	工場のPCやHMI／SCADA等の画面に不自然な表示（身代金要求等）	比較的容易
6	原因が物理損傷等でなく、かつ原因特定が不明確な事象	比較的困難
7	複数箇所で何らかの事象が同時多発する場合	
8	同一事象が任意の期間で頻発する場合	

ICSを対象とするSIRTの機能構築の課題 - 取り組み例

■ ICS特有事象の検知能力の開発 - ICSを対象としたSIRT機能の装備

— ランサムウェアばかりではない「サイバー要因のICS特有事象」を早期に捕捉

— 前スライドの事象をどのようにして検知するのか？

➢ **前スライドの事情には実際のインシデントケースもあり参加組織では相応の意識をもって取り組み中**

取り組みの一例 製造業におけるサイバー要因となり得るICS特有事象の収集と評価の試行

Case1：現場で**一定のフィルタリングをしてSIRTへ報告**

- **報告対象：**1～4のうち6～8の一部または全部に該当するケースおよび5のケース
- **評価の試行：**報告事象のサイバー要因の有無の確認、サイバーインシデントの判定等
- **長所：**不要な報告の削減、特定事象の評価に注力等

Case2：現場で**全くフィルタリングをせずにSIRTへ報告**

- **報告対象：**1～5のすべてのケース、6～8の一部または全部に該当するケース、その他判断に迷うケース
- **評価の試行：**報告事象のサイバー要因の有無の確認、サイバーインシデントの判定等
- **長所：**報告対象の漏れの低減、報告基準を検討するためのより的確なデータ収集の期待等

これらの取り組み例も含めた**「ICSを対象とするSIRT」の構築を支援するコンテンツを準備中**

目次

まとめ - ICSを考慮したSIRTを構築するには・・・

ポイント①

■ **ICS関連のインシデント事案の捉え方**

- ランサムウェア事案のICSにおいても脅威であるがそれ以外の事案にも着目
- ICS関連事案には、「間接影響（ICSに被害が無くとも主として生産や業務の遂行に影響）」と「直接影響（ICS関連機器自体が被害を受ける）」があり、対策検討においては、両方を踏まえる必要がある

ポイント②

■ **ICSを対象としたSIRT構築の第一歩 - ICS関連のセキュリティインシデントに備える**

- 構築には「組織要件」と「機能要件」がある
- ICSの特有事情（「安全確保」等の考え方、運用事情、特有事象等）を踏まえる必要がある
- 実務的な構築の着手ポイントは種々あるが、**「事象把握」の仕組みづくりは適切なSIRT構築の実践的で重要な一歩である**

- JPCERT/CCは、ICSのステークホルダーの方々とこれまで以上に連携・協働を進めます
- 「ICSを対象とするSIRT」の構築を検討／運用中の**ICSセキュリティ担当者は、JPCERT/CC主催の「ICSセキュリティ担当者コミュニティー」へ参加をご検討ください**
- **参加メリット等は次のスライドをご参照ください**

ICSセキュリティ担当者へ - 関心のある方はご連絡を

■ 製造業のICSセキュリティ担当者コミュニティーの参加組織を追加募集

コミュニティー概要（JPCERT/CC主催）

20
組織以上
（発表時点）

複数業種
機器製造・化学鉄鋼・製薬
光学・食品 等

ICS セキュリティ 担当者

参加メリット

➢ **参加メリットの例：**

- **個人での奮闘からの脱却：**
  ✓ 取り組む仲間を得られる
- **ICSにおけるSIRT活動（構築/運用）をより適正化：**
  ✓ 「ICSを対象とした場合の考慮点」の知見が得られ、より適正化した活動が可能に
- **ICSにおける脅威・脆弱性の対応能力の向上：**
  ✓ JPCERT/CCからICS関連のセキュリティの知見を得る、他社と取り組みの情報交換も可能

・・・等々

■ コミュニティーに関心のあるICSユーザー組織のセキュリティ担当者へ

コミュニティー参加希望で概要説明をご希望の方は次の宛先へご連絡ください

- JPCERT/CC「**ICSセキュリティ担当者コミュニティー係**」（icsr@jpcert.or.jp）
- **コミュニティー参加には条件あり（参加費：無料）**

ICSベンダー／エンジニアリング担当者へ - 脆弱性対応

■ 納品／構築先の「ICSにおける脆弱性対応」に関する意見交換希望者の募集

➢ **募集背景：**

JPCERT/CCでは、次のテーマに関して「ICSベンダー／エンジニアリング」担当者から問い合わせを受けることがあり、同様の関心を持つ「ICSベンダー／エンジニアリング」担当者との意見交換を行いたいと考えております。

テーマ
納品または構築・保守先のICSにおける脆弱性対応の要望に応えるためのポイント

※本件は「ICSを対象とするSIRT」のサポートを前提とした意見交換です

■本テーマの意見交換をご希望のICSベンダー／エンジニアリング担当者へ

ご希望の方は次の宛先へご連絡ください

➢ JPCERT/CC「納品／構築／保守先の**ICSにおける脆弱性対応係**」（icsr@jpcert.or.jp）

ご清聴ありがとうございました