# 制御システム・セキュリティの現在と展望

## ～ この1年間を振り返って ～

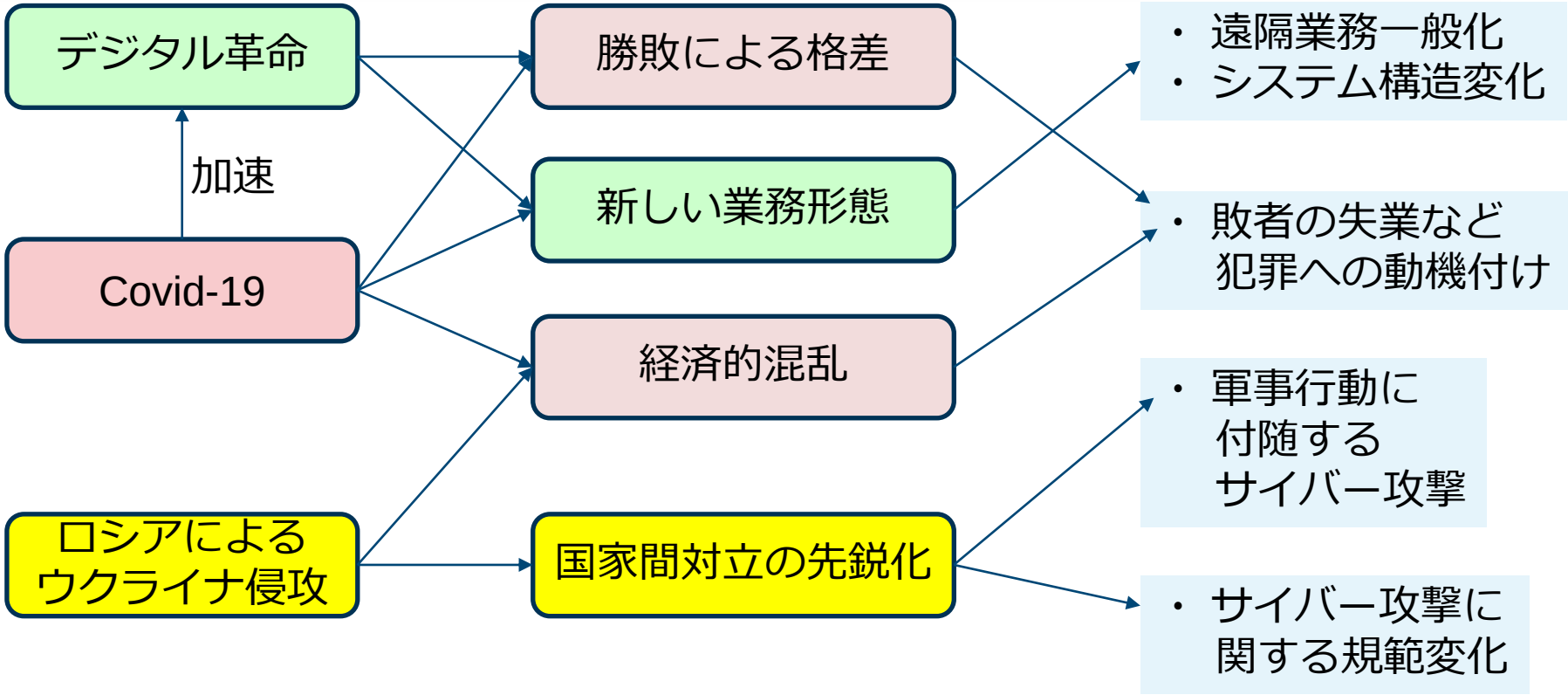
**2023年版**

JPCERTコーディネーションセンター
ICSR　技術顧問
宮地利雄

- ☞ デジタル革命の進展
- ☞ Covid-19パンデミック： 多くの地域で鎮静化へ
- ☞ ロシアによるウクライナへの侵攻
- ☞ 脱炭素やエネルギー危機などICSを取り巻く環境が大きく変動

# サイバー・セキュリティを取り巻く世界情勢

# サイバーセキュリティ脅威を深刻化させる世界情勢

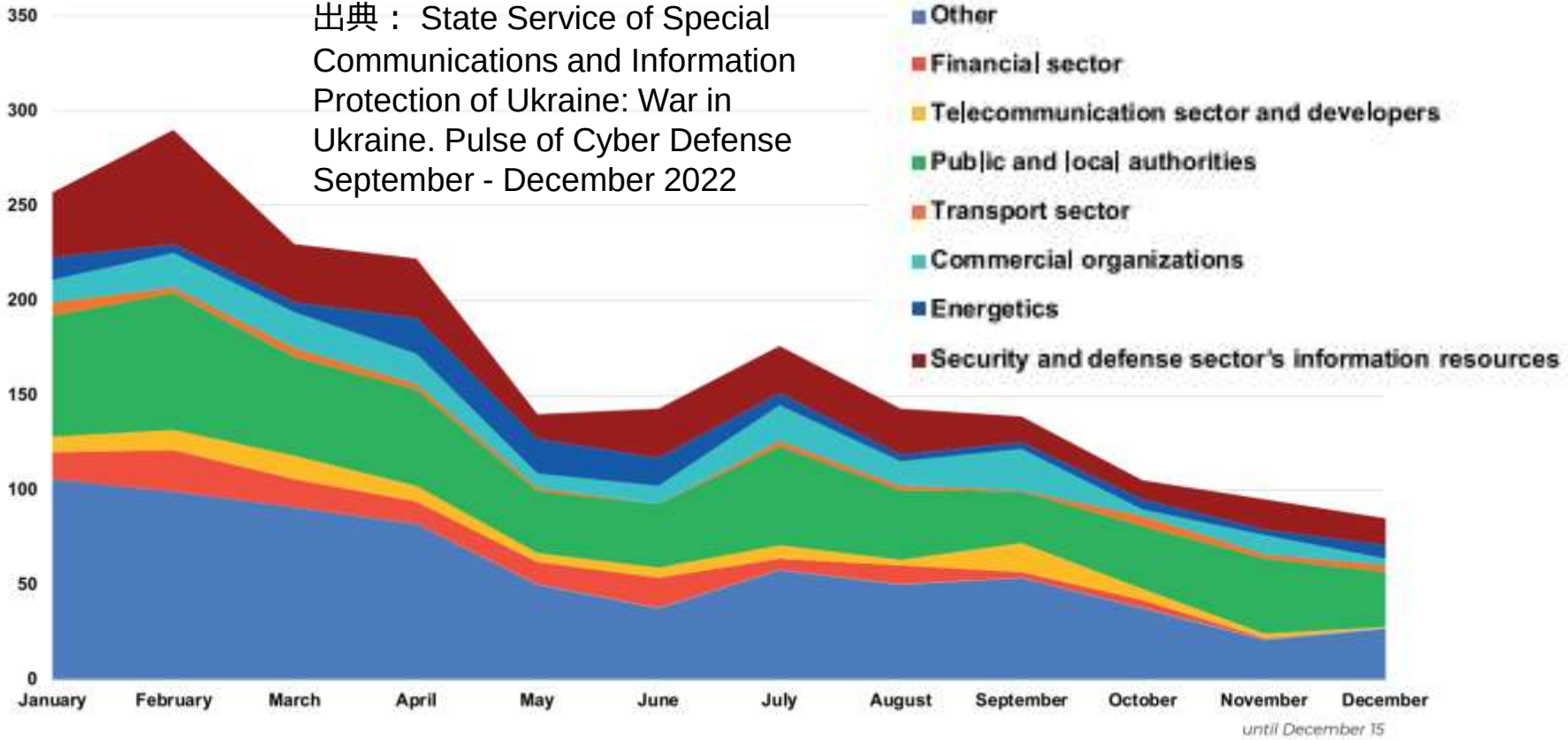


# ロシアによるウクライナへの侵攻に伴うサイバー攻撃

- 2月21日：東部2州の独立を承認する大統領令にプーチンが署名
- 2月23日：ウクライナの多数の組織(防衛，金融，航空，ITサービス等)にサイバー攻撃(HermeticWiperによるシステム消去)
- 2月24日：早朝にウクライナ東部での「特別な軍事作戦」の実施をロシアが発表し，首都キーウなどへのミサイル攻撃や空爆開始
- 2月24日：サイバー攻撃により衛星通信網ViaSatに障害
- 2月26日：ウクライナ軍部隊にベラルーシュからフィッシング攻撃
- 2月27日：ウクライナ政府がボランティアに呼びかけた「ウクライナIT軍」がロシアの数十組織に対してサイバー攻撃
- 2月28日：Anonymousがロシア軍の移動に使われるベラルーシュ鉄道の内部網を侵害しサービスを妨害したと主張
- 3月17日：欧州航空案庁がGNSS(ナビ衛星)の不安定化について警告

# ウクライナでのサイバー・インシデントとサイバー攻撃

出典： State Service of Special Communications and Information Protection of Ukraine: War in Ukraine. Pulse of Cyber Defense September - December 2022



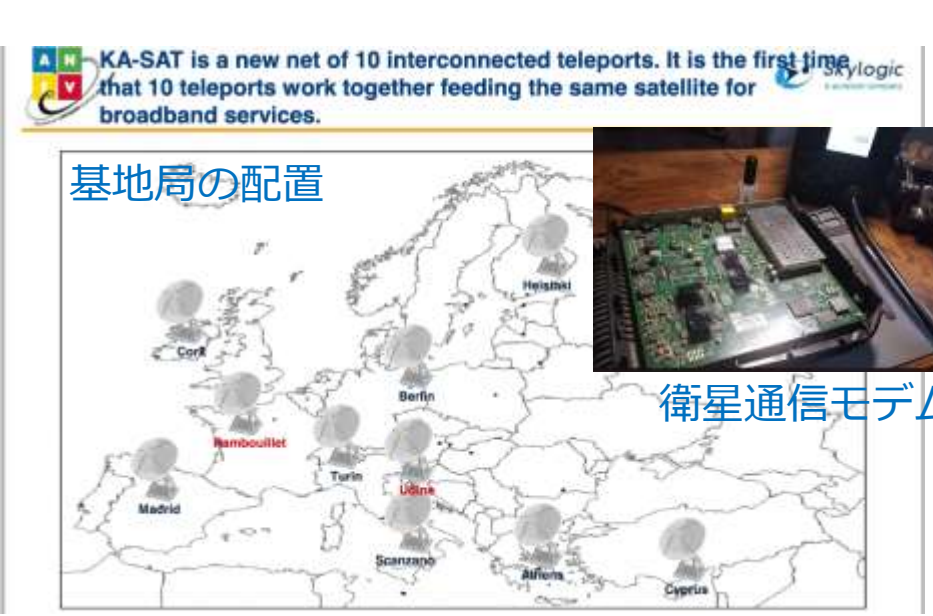
# ViaSat社の衛星通信サービスへのサイバー攻撃

- 2月24日(ウクライナ侵攻初日)に
  ViaSat社の衛星通信モデム約1万台(ドイツ～東欧地域)が障害
  - VPNのご設定を悪用して
    ネットワーク管理用インターフェースに侵入,
    そこから設定を消去するマルウェア(AcidRain)を衛星モデムに
    送りつけた
  - ウクライナ国内の通信を混乱させようとしたと推測される

- ドイツ国内のEnercon社製の風力タービン約5,800台が遠隔制御不能に
  (合計最大発電能力： 11GW)
  - 衛星モデムを1台1台初期化と再設定を行って復旧
    (3週間後(3月16日)までに復旧できたのは15%のみ)

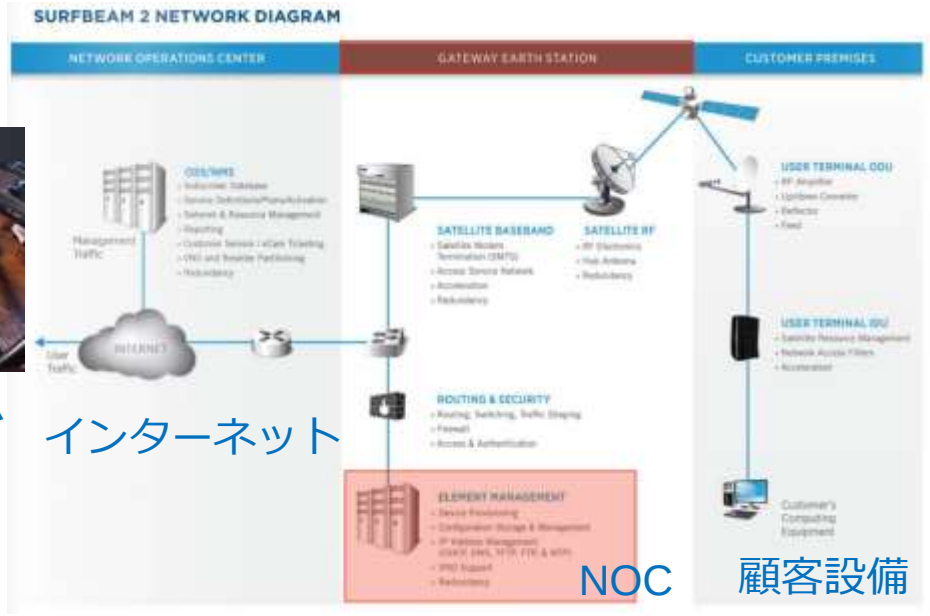
# ViaSat社の衛星通信サービスへのサイバー攻撃 (詳細情報)

[出典] Reverse Mode: SATCOM terminals under attack in Europe: a plausible analysis
https://www.reversemode.com/2022/03/satcom-terminals-under-attack-in-europe.html
Reverse Mode: VIASAT incident: from speculation to technical details
https://www.reversemode.com/2022/03/viasat-incident-from-speculation-to.html






衛星通信モデム



# 衛星システムへのサイバー攻撃への対策アドバイザリ

- 米国CISAとFBIから3月17日にAlert (AA22-076A)
  Strengthening Cybersecurity of SATCOM Network Providers and Customers
  https://www.cisa.gov/uscert/ncas/alerts/aa22-076a
  — 衛星通信事業者に対してサイバーセキュリティ対策を呼びかけ

- 米国NISTから12月30日にNISTIR 8401
  Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control
  https://csrc.nist.gov/publications/detail/nistir/8401/final
  — 人口衛星の管制地上局に向けたCSF(Cybersecurity Framework)の適用

# 全球測位衛星システム(GNSS)信号に対する攪乱

(GNSS: Global Navigation Satellite Systems)

- 様々な地域でGNSS信号に対する攪乱が増加
  - EU航空安全庁(EASA)からは全情報速報
    Global Navigation Satellite System Outage Leading to Navigation / Surveillance Degradation (3月17日)
    https://ad.easa.europa.eu/blob/EASA_SIB_2022_02.pdf
  - CISAからはGPSへの干渉の状況に関する情報の公表
    Global Positioning System (GPS) Interference (12月6日)
    https://www.cisa.gov/sites/default/files/publications/CISA-Insights_GPS-Interference_508.pdf

- GNSSの位置情報はもとより
  時刻情報にICSが依存していないか確認を！

デンバー国際空港で
1月に33時間にわたり
干渉

# ベラルーシュの鉄道会社へのサイバー攻撃

- ハクティビスト集団「アノニマス」がウクライナ侵攻に反対して
  ベラルーシュの鉄道会社の内部ネットワークを侵害し
  同国内に進駐していたロシア軍の鉄道移動を阻止したと
  2月28日にツィート
  - 鉄道会社はマニュアル・モードでの運行に切り替え
    列車が遅延したと報じられた

  [参考] Anonymous breached the internal network of Belarusian railways (Security Affairs)
  https://securityaffairs.co/wordpress/128486/hacktivism/anonymous-breached-belarusian-railways.html

- 親ロシア派，親ウクライナ派双方のハクティビストが
  DoS攻撃でウェブ･サイトをダウンさせる等のサイバー攻撃を実施

  [参考] Russia or Ukraine: Hacking groups take sides (The Record)
  https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/

# 武力による戦時下のサイバー攻撃

（実際の経緯）

- 侵攻と同時に
  衛星通信網にサイバー攻撃
- 電力網へのサイバー攻撃が
  事前に発覚(失敗)
- 世論を操作する情報戦が活発

- ウクライナがロシアへの
  サイバー攻撃を呼びかけ
- 民間のハクティビストの活動
  が活発化

高度なサイバー
攻撃能力がない

(事前の想定)

- 武力行使と並行した
  サイバー攻撃により
  軍の指揮系統と
  重要社会インフラを混乱させる

・ 戦況を変えるほどの影響なし
– イラン製ドローンの方が威力

・ サイバー空間の規範が崩壊

# ウクライナ侵攻と国家支援を受けたサイバー攻撃

- サイバー空間における国家の行動規範に変化 (?)
  - サイバー空間を通じた相手国の世論操作や偽情報による攻撃
  - サイバー攻撃能力を保有することを容認
    (決断時に実際に攻撃できるためには
    平時のうちに侵入しておく等の「事前の仕込み」が必要)

- サイバー犯罪集団による攻撃と
  国家支援を受けたサイバー攻撃がクロスオーバー

- ウクライナの事例はサイバー戦争の典型例ではないとの指摘も
  https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf

# 2018年前後から米国も軍事的なサイバー戦略を見直し

- 米国国防総省が2018年にサイバー戦略を改定し，
  従来からの「自由で開かれたインターネット」を維持しつつ，
  「Defending Forward」や「Persistence」，
  「重要インフラ防御」の考え方を導入

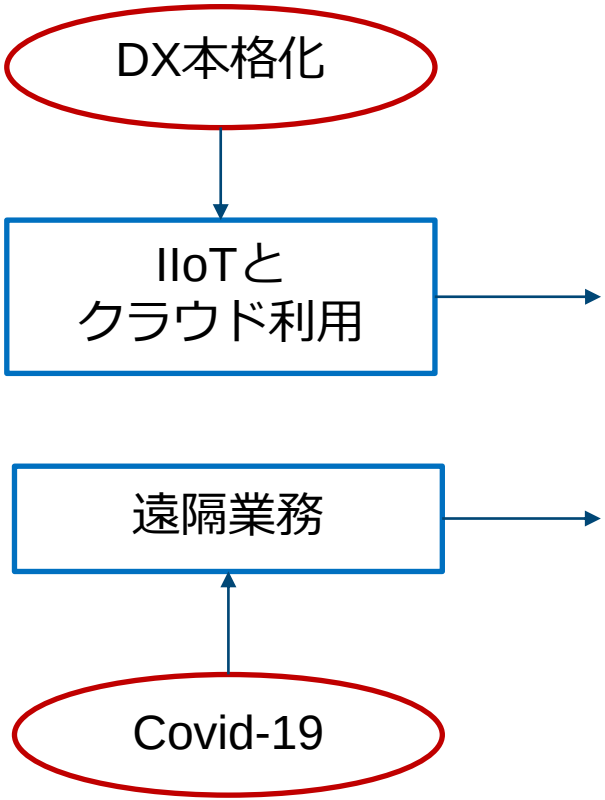
従来型装備より安上がり；
サイバー攻撃の実効性が上昇

- 「Defending Forward」の定義はないが，次を含むとされている：
  - 実戦に備えた諜報活動
  - 悪意あるサイバー活動を根源(攻撃元?)で阻止する
  - 軍事衝突の水準を低下させる

サイバー空間では
迎撃的な防衛では
有効性が低い

[参考] Lawfare: The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes
https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes

# 高度化し進化するICSとサイバー･セキュリティ




- ICSネットワーク･アーキテクチャーが変化
  - 階層的なPurdue大学モデルが陳腐化
- IIoT機器やクラウドのセキュリティ
  - 技術サプライチェーン･セキュリティが課題
- VPNシステムのセキュリティ管理
  - 狙われるVPNシステム
- 遠隔業務下でのセキュリティ管理
  - ルールの徹底と対策の迅速化が課題

# IIoTとクラウドの利用拡大

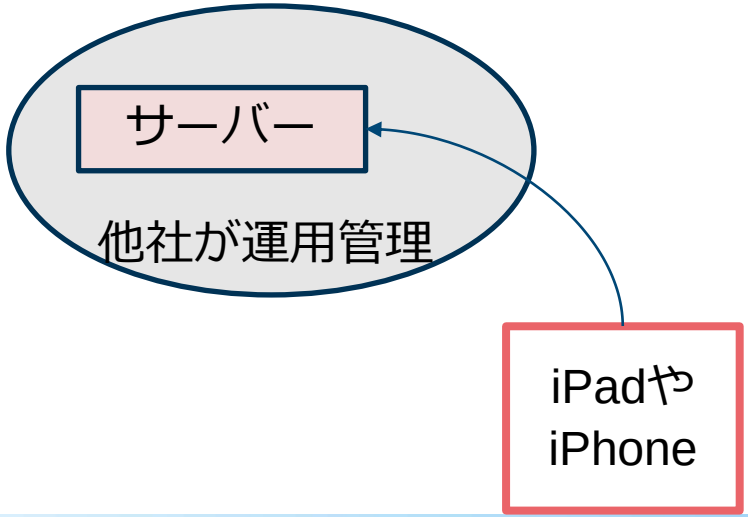
- ICSネットワーク･アーキテクチャーが変化
  - 階層的なPurdue大学アーキテクチャーが過去のものに
  - 新しいネットワーク･アーキテクチャーに整合した
    セキュリティ･アーキテクチャーへの移行が課題に
    - レガシー機器への配慮も必要

- クラウド利用に伴うセキュリティ･リスク
  - クラウドのセキュリティ設定のミス
  - クラウド側で障害発生時の対処

# オンライン電子マニュアルが不調で鉄道が運休

Security Affairs: A cyberattack blocked the trains in Denmark
https://securityaffairs.co/wordpress/138127/cyber-crime/cyberattack-blocked-trains-denmark.html

- 電子マニュアル(運行指示書?)にアクセスできなくなったことが原因でデンマークの最大手鉄道会社DSBで10月29日に列車の運休と遅延




- 電子マニュアルはiPhoneかiPadからサーバーにアクセスして動作
- サーバーは開発会社のSupeo社が運用
  - データセンターでマルウェア感染が見つかりサーバーを停止
- サーバー停止時にはオフライン･モードに切り替わって使えるはずだったが実際にはまったく使えなくなった

- ☞ サイバー攻撃の報告なく北京冬季オリンピックが無事に開催
- ☞ 2種のICSを狙ったマルウェアが4月に報告された
- ☞ 重要インフラへのランサムウェアの脅威が続いた
- ☞ 重要インフラを狙ったワイパー(消去)マルウェアも

# インシデントの動向

# 電力網を狙って開発されたマルウェアIndustoryer2

- 欧州のセキュリティ会社ESET社がIndustroyer 2と名付けたマルウェアを分析し2022年4月12日に公表
  https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

- 2016年末にウクライナで停電を引き起こしたマルウェアIndustroyerを改造したもの
  (技術的には二番煎じ)

- 攻撃(4月8日)に使われる前にワイパー(消去)マルウェアとともに発見されESET社とCERT-UAが共同で分析

詳細が明らかにされていないが国家支援を受けたサイバー空間の活動に対する諜報収集活動の中で探知か？

# 過去にウクライナの電力網に対して行われたサイバー攻撃

| 発生月日 | 被害電力会社 | 操業地域 | 被害 |
|---|---|---|---|
| 2015年<br>12月23日 | PrykarpattyaOblEnergo | Ivano-Frankivsk | 変電所のブレーカの切断で最大約6時間にわたり停電<br><br>ICS用機器の機能を破壊 |
| | AES KyivOblEnergo | Kiev | |
| | ChernivtsiOblEnergo | Chernivtsi | |
| 2016年<br>12月17日 | Ukrenergo | Kiev | 変電所のブレーカの切断で1時間15分の停電 |

BlackEnergy3
KillDisk
Industroyer

**2015年の停電は：**

- **サイバー攻撃により<br>エネルギー供給が停止した初の事例**
- **オフィス網に標的型攻撃をかけて<br>情報収集した後にICSを攻撃**
- **同時に電話網を過負荷状態で利用不能に**

**2016年の停電は：**

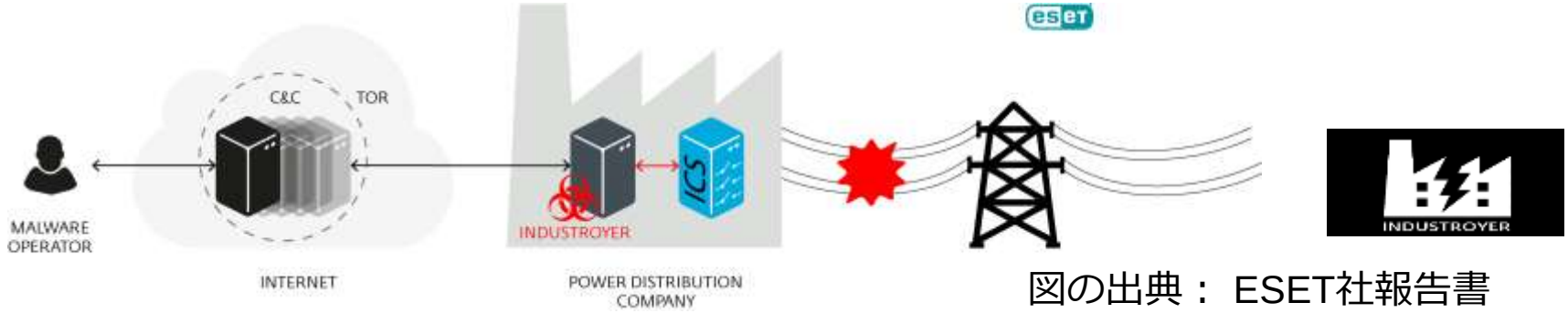
- **官庁や鉄道への攻撃の数日後**
- **前年と似た手口ながら高度化**

(前回(2017年2月)の講演資料から再掲)

# ウクライナで2016年末の停電を引き起こしたIndustroyer

- 報告者
  - スロバキアのセキュリティ企業ESET社(2017年6月12日)：Win32/Industroyer
    https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/
  - 米国のセキュリティ企業Dragos社(2017年6月12日)： CrashOverRide
    https://dragos.com/blog/crashoverride/

- 2016年末のウクライナでの停電でICSに遮断機を開くよう指令

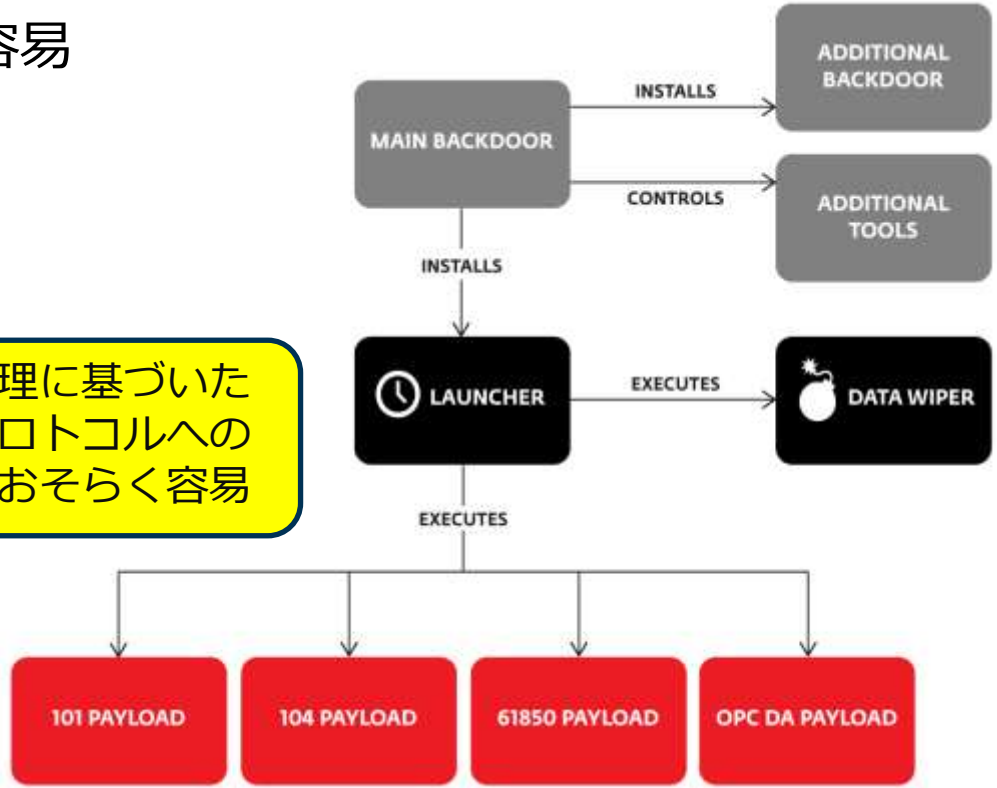



図の出典： ESET社報告書

# Industroyerの構造と機能

- モジュラー構造で機能追加が容易
- ツール
  - ポート・スキャナー
  - DOSツール
- ランチャーで起動
  - データ消去
  - 遮断機の操作
    101用，104用，
    61850用, OPC DA用の
    ペイロードがある

同じ原理に基づいた
他のプロトコルへの
拡張はおそらく容易




図の出典： ESET社報告書

# ICSを狙って開発された多機能マルウェアPipeDream

- 攻撃に使われる前に発見され，Dragos社が分析し2022年4月に公表

  Dragos: PIPEDREAM: CHERNOVITE‘s Emerging Malware Targeting Industrial Control Systems
  https://hub.dragos.com/whitepaper/chernovite-pipedream

  Dragos: Analyzing PIPEDREAM: Results from Runtime Testing
  https://www.dragos.com/blog/analyzing-pipedream-results-from-runtime-testing/

- 5つのコンポーネントをもち多様な攻撃を行う機能を備えている
  - 複数のICS製品に対する攻撃が可能
  - ICSを攻撃する様々な段階で利用できる攻撃ツールを集めたツールセット

# ICSを狙って開発されたマルウェアPipeDream (続き)

- 複数のICS製品(コントローラー)を狙った攻撃が可能
  - 攻撃対象製品を拡大すべく開発中とも推測される

- 外部から指令を受けて，侵入した環境内で実行する機能も
- 侵入した環境に新しいマルウェアなどをダウンロードする機能も

| | |
|---|---|
| EvilScholar | Schneider社製PLCを攻撃する； CodeSysライブラリーも包含 |
| Badomen | Omron社製PLCを攻撃する |
| MouseHole | OPC-UAサーバーと交信し情報を収集する |
| DustTunnel | ホストを偵察し，遠隔からC&C(指令と制御)を実行する |
| LazyCargo | ASRockドライバーを悪用してドライバーをダウンロードする |

# ICSに対するサイバー攻撃モデル

ATT&CK for Industrial Control Systems

https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf

制御システムへのサイバー攻撃についての知識ベース (事典)

- 攻撃技法(technique)を12の攻撃策略(tactic)に分類して列挙
- 12の攻撃策略(tactic)は，1) 最初のアクセス，2) 実行，3) 固着，4) 権限昇格，5) 隠避，6) 発見，7) 水平移動，8) 収集，9) 指令と管理，10) 応答機能の抑制，11) プロセス制御の損壊，12) 究極の衝撃

- 攻撃技法のそれぞれについて，解説と攻撃例，緩和策，参考資料

# これまでにICSを狙って作られたマルウェアの一覧 (1/2)

| マルウェア名 | 報告年 | 概要 |
|---|---|---|
| Stuxnet | 2010 | イランのウラン濃縮工場の遠心分離機に異常な回転をさせて破壊 |
| Havex (DragonFly, EnergeticBear, CrouchingYeti) | 2014 | オフィス網上のPCが感染；OPC関連情報を収集 |
| BlackEnergy2 | 2014 | 複数のベンダーのHMI製品が感染；米国ICS-CERTからアラート |
| BlackEnergy3 | 2015 | 電力およびその関連業界が感染 (情報収集に利用された?)<br>2015年末と2016年末のウクライナでの停電の前段階で多数の感染 |
| Industroyer (CrashOverRide) | 2017 | 2016年末にウクライナで遮断機を開き停電を引き起こした |
| HatMan (Triton, Trisis) | 2017 | Schneider社製安全計装コントローラのプログラムを改竄 |

# ICSを狙って作られたマルウェアの一覧 (2/2)

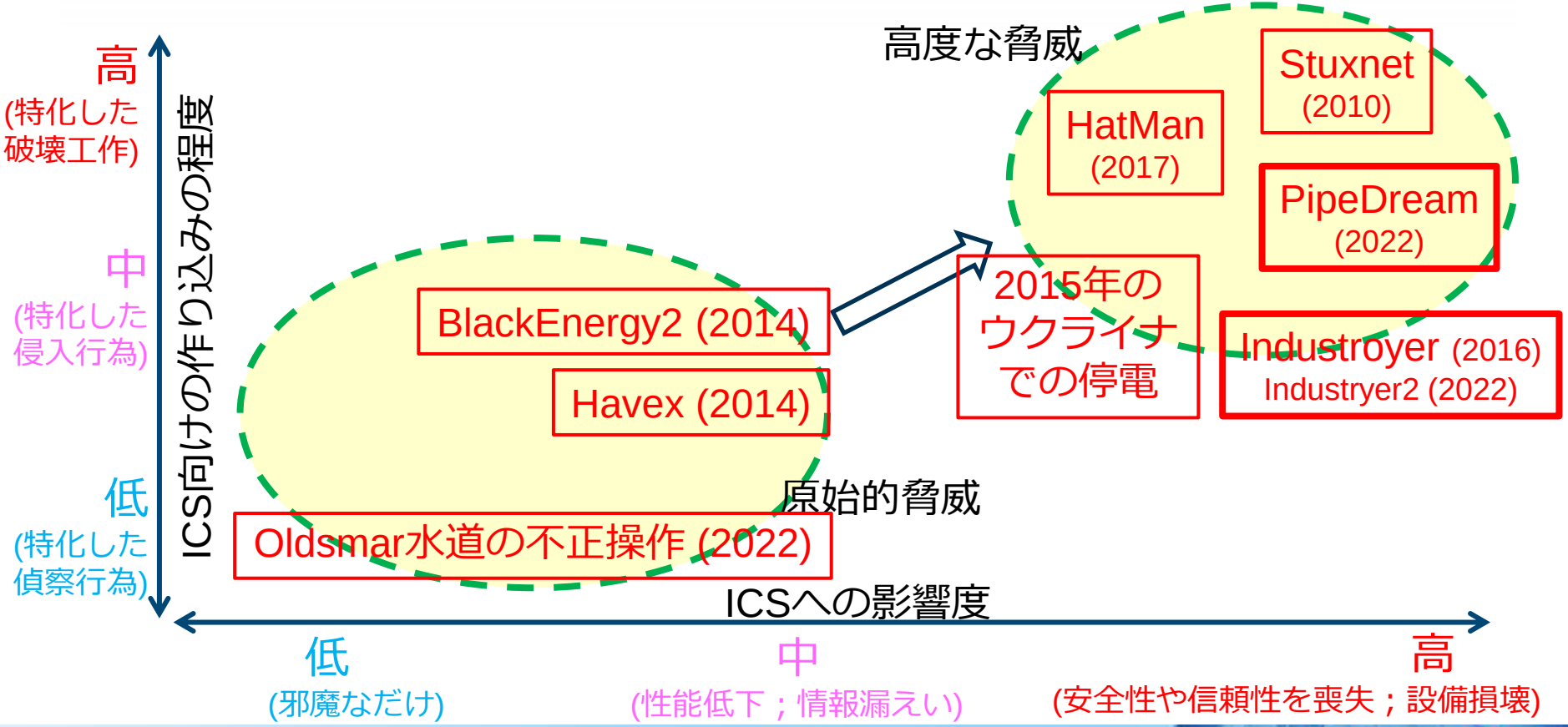
| マルウェア名 | 報告年 | 概要 |
|---|---|---|
| VPNfilter | 2018 | 個人用ルーターに感染<br>Modbusに関する情報を収集する機能 (開発目的不明) |
| Ekans (Snake) | 2020 | ICS関連のプロセスを停止させる機能をもつランサムウェア |
| Industroyer 2 | 2022 | 2022年4月に報告された<br>ロシアによる侵攻下でウクライナの電力網を狙ったとされる |
| PIPEDREAM | 2022 | 2022年4月に報告された<br>5つのコンポーネントを含むモジュール構造で多様な攻撃機能 |

凡例

情報収集のみ

ICSの動作に影響あり

# ICSに対するサイバー脅威動向のまとめ



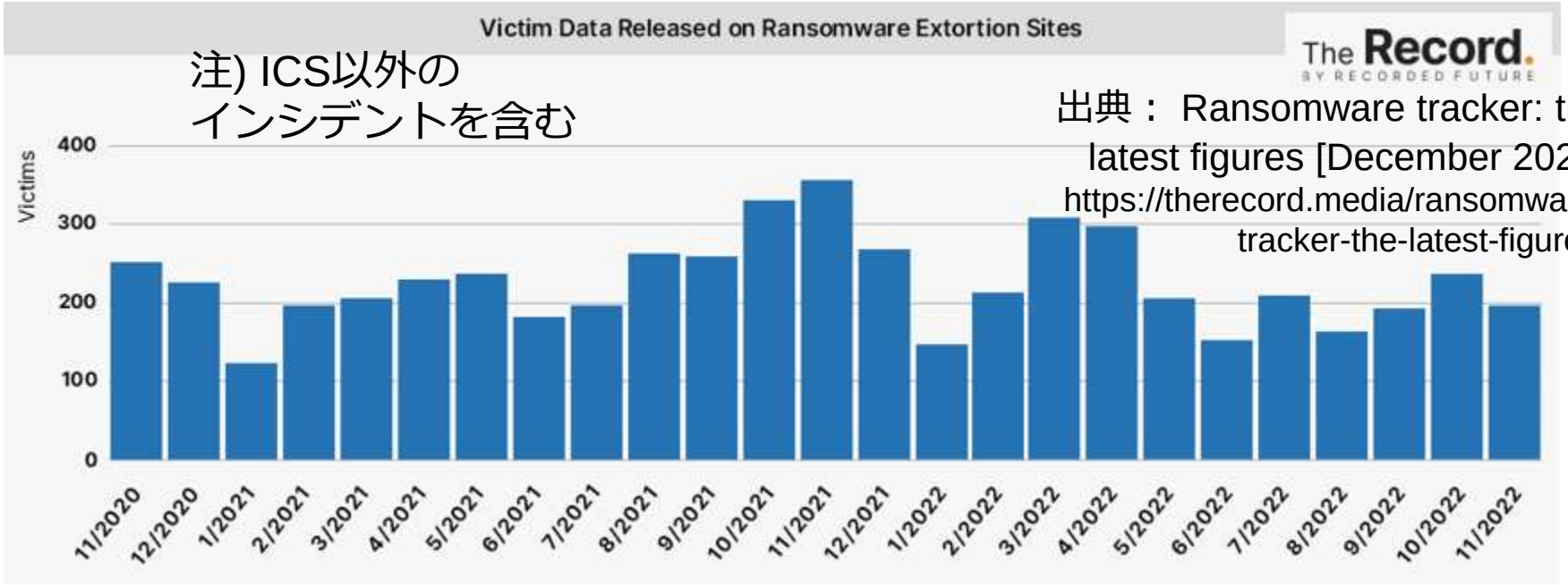
# ランサムウェアの脅威

- ICSを特に狙っているわけではないが
  今のところICSに最も起きそうで大きな損害を伴うサイバー脅威
- 前年(2021年)から引き続きインシデント件数が高止まりしている
- 製造業界が高額の身代金を取れる業界と見られている(?)
  - 身代金の金額は分散が大きい
  - 約1/3の製造事業者が支払いに応じる
  - 支払いにより復旧した割合は6割程度

| 支払った身代金の平均 | 2020年 | 2021年 |
|---|---|---|
| 製造業界 | 15万ドル | 204万ドル |
| 全業界 | 17万ドル | 81万ドル |

情報源：The State of Ransomware
in Manufacturing and Production 2022 (Sophos社)
http://sophos.com/manufacturing2022

# ランサムウェア・インシデントの件数 (2021～2022年)

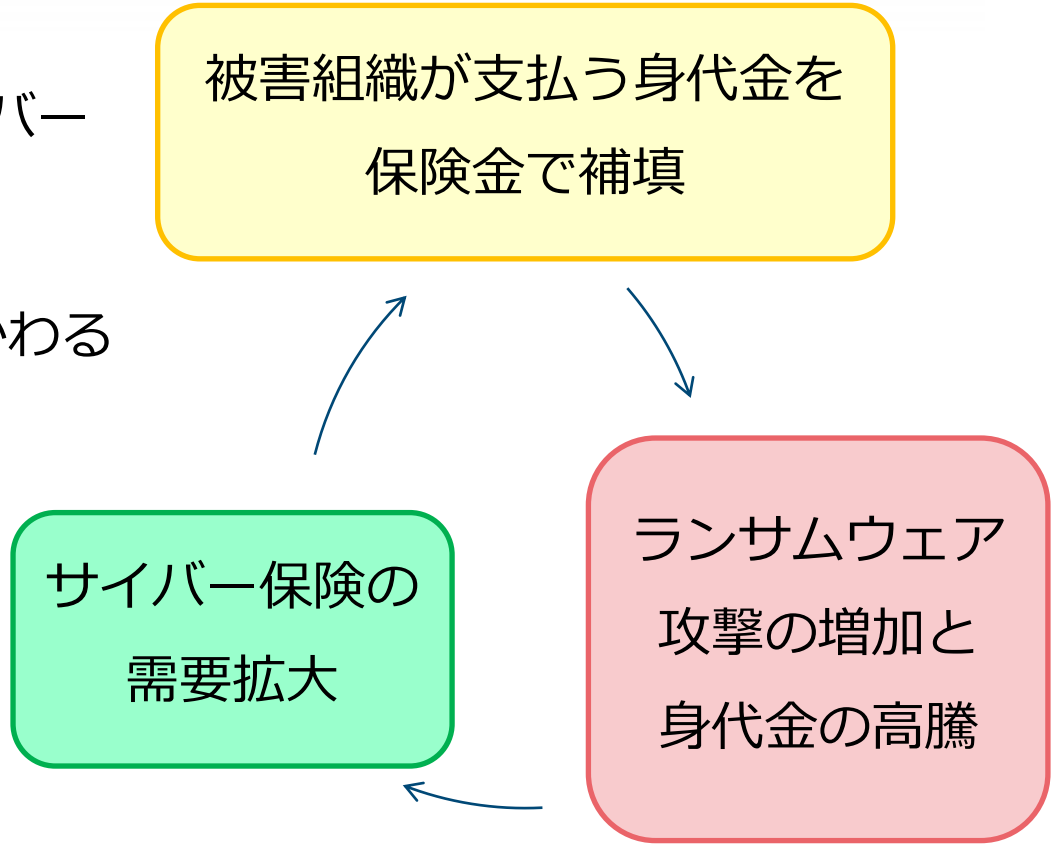



- 重要インフラに対するランサムウェア攻撃事例をTemple大学が取集
  Critical Infrastructure Ransomware Attacks (https://sites.temple.edu/care/cira/)

# ランサムウェアは攻撃者にとって「金のなる木」

- 特に米国やドイツが深刻
- ランサムウェアが最大のサイバー脅威に
  - 事業継続性へのリスク
  - 復旧費用が企業存続にかかわる水準になることも
- 保険会社の利益悪化
  - サイバー保険料の上昇

なお，日本損害保険協会では身代金をサイバー保険の補償対象としていない



# ランサムウェアの典型的な攻撃プロセス

- ネットワーク内に侵害後にランサムウェアを配備

1. フィッシング・メール等を利用して悪意あるサイトに誘導する，
   リモート・デスク・トップ(RDP)を悪用する等の手段で
   最初のコンピュータをマルウェアに感染させる
2. ネットワーク内でマルウェアの感染範囲を拡大しながら，
   ネットワークの情報を収集して狙うべきシステムを特定して，
   又は広範囲にランサムウェアをインストールする
3. データのコピーを外部に送り出す
4. 夜間など気づかれにくい時間帯を狙ってデータを暗号化し，
   その後に身代金要求を表示

# OTシステム関連の重要な情報が漏えいすることもある

Mandiant: 1 in 7 Ransomware Extortion Attacks Leak Critical Operational Technology Information

https://www.mandiant.com/resources/ransomware-extortion-ot-docs

- Mandiant社が2021年に漏えいされた2,600件の情報を分析
  - 重要インフラと製造事業者関連の1,300件を抽出
  - 数百件の情報を実際に入手し，うち70件を人手により分析
  - 10件の情報に技術的に機微な情報が含まれていた

- ランサムウェア攻撃で漏えいされたOT情報の7件中1件に重要情報

# ランサムウェア攻撃者における分業体制 (DarkSideの例)

- ロシア国内に本拠を置いていると見られる
- RaaS (Ransomware As A Service)
  (多くのランサムウェアがRaaS型になっている)
  - DarkSideがランサムウェア攻撃のための基盤を開発運用
  - DarkSideは会員(affiliate)を募集し
    会員が個々の企業に対する攻撃を実行
  - DarkSideは得られた身代金から店賃を差し引いて会員に渡す

・胴元の知恵
・店子の数と手間暇

# RaaSに代表される攻撃基盤提供者と攻撃者の分業

- 技術を持つ者と手間暇を惜しまない者とが補完してサイバー攻撃
  - 高度のソフトウェア開発技術を持つ者が攻撃基盤を開発する
  - 低廉の時給で働ける者を闇市場で募集し，手順書を与えて，与えられた攻撃基盤を使わせて，攻撃を実施させる
  - 得られた利益を分割； 満足できる報酬がない場合もある模様で，闇市場には調停制度がある場合も
- 自律的に動作するタイプのマルウェアによらないインタラクティブに(人手で打鍵して)行われるサイバー攻撃が急増
  - 「2019年からの2年間で4倍に増加」とCrowdStrike社が報告 https://www.crowdstrike.com/resources/reports/global-threat-report/
- 一次的侵入の方法を商品として二次攻撃者に販売することにより売上利益を狙っている者も以前から存在している

# Colonial Pipeline社に対するランサムウェア攻撃犯人逮捕

- 2021年5月7日にColonial Pipeline社がランサムウェア攻撃を受けて米国東海岸地域で燃料パニック状態が発生
  - ランサムウェアDarkSideが使われた(攻撃集団はREvil)
  - 身代金75BitCoin(約5百万ドル)が支払われた(63.7BitCoin回収)
- 米国がロシアに犯人の逮捕を要求
- ロシアFSBが1月14日にREvilランサムウェア集団を4都市で一斉捜索
  - 14人のメンバーを逮捕
  - 暗号通貨の他，60万米ドル，50万ユーロ，4.26億ルーブルの現金，20台の高級車を押収した

REvil hacker group liquidated in Russia after US request

В России ликвидировали группу хакеров REvil после запроса США

https://www.rbc.ru/politics/14/01/2022/61e171599a79479dde32112e

# 国家支援を受けた集団によるランサムウェア攻撃も

Microsoft社: Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021
https://www.microsoft.com/en-us/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/
Cyber War Con： Their Own Little War: Iran Adopts Disruptive Ransomware
https://www.cyberwarcon.com/their-own-little-war

- 破壊的な攻撃を行うための手段としてランサムウェアが利用される
  - 高度化しているランサムウェアを流用
  - 金銭目的の犯罪集団の行為に見せつけるなど言い逃れがしやすい

# ICSに対するサイバー脅威動向のまとめ (続き)

- 新しい高度なICSの攻撃手法がこの数年間現れていない状態が続く
  - 攻撃者が「金のなる木」に手いっぱい？
  - ICSにおけるオープン技術の導入とネットワーク接続性が高まっており攻撃界面が拡大していることは確実と見られる

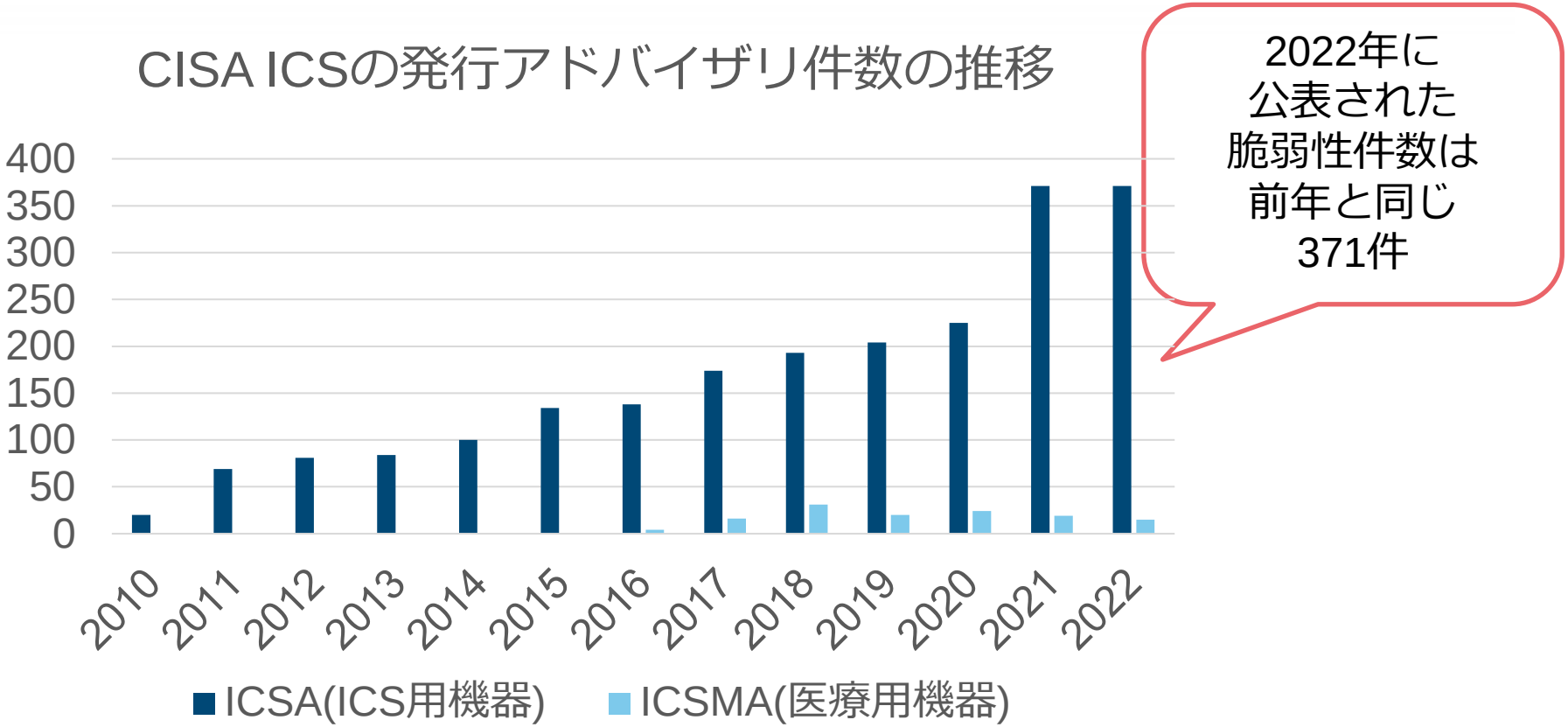
- ロシアによるウクライナ侵攻に伴ったサイバー攻撃が増加
  - 重要インフラを狙ったワイパー(消去)マルウェア攻撃事案が増えた
  - 幸いにして，大きな混乱はなかった
    - ウクライナや米国におけるセキュリティ対策の成果？
    - 攻撃側(ロシア)の準備不足？

- 総じて，社会的に話題になるようなICSのインシデント事案はなかった

- ☞ 2022年は前年と同じ371件(他に医療用機器関連で15件)
- ☞ ICS製品のセキュリティ試験の最高潮年になったとClaroty社が分析
- ☞ 2021年末に公表されたApache Log4jの脆弱性が不気味

# 脆弱性の動向

# 米国ICS-CERTが公表した脆弱性アドバイザリ件数



# 公表されたICS製品の脆弱性のClaroty社による動向分析

公表されたICSの脆弱性の動向をClaroty社(米国)が半年ごとに分析
(2022年8月の公表からX(Extended)IoTの脆弱性にカバー範囲を拡大；
医療用機器等も含む)

https://claroty.com/resources/reports/state-of-xiot-security-1h-2022

- 2022年上半期の動向
  - 86社のベンダー製品に合計747件の脆弱性
    (うち214件は開発者により発見された)
  - CVSS値によれば脆弱性の19%が重大に，46%が深刻に分類される
  - 26%の脆弱性は完全な修正対策手段が提供されていない

# IIoT機器の利用に伴うセキュリティ・リスク： 脆弱性問題

- ソフトウェア･サプライチェーンを通じて継承される脆弱性

  開発に利用されたソフトウェア･ライブラリーについて
  - サポートが，IIoT機器のライフタイム期間中に終了するリスク
  - ライブラリーの脆弱性が公表されても，
    ライブラリーを組み込んだ製品で対策がなされず放置されるリスク

- IIoT機器の脆弱性管理
  - 新たに公表される脆弱性の監視し影響の有無を判定
  - ソフトウェアを更新する機能の具備と更新の実施体制

# IIoT機器に継承された脆弱性への攻撃事例

- インドの電力網に対するサイバー攻撃が続いているとの報告(4月)

  RecordedFuture: Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group
  https://go.recordedfuture.com/hubfs/reports/ta-2022-0406.pdf

  — RedEchoと呼ばれる攻撃集団(中国に本拠か)が
  IoT機器に脆弱性を悪用して
  ShadowPadと呼ばれるバックドアを造り込む

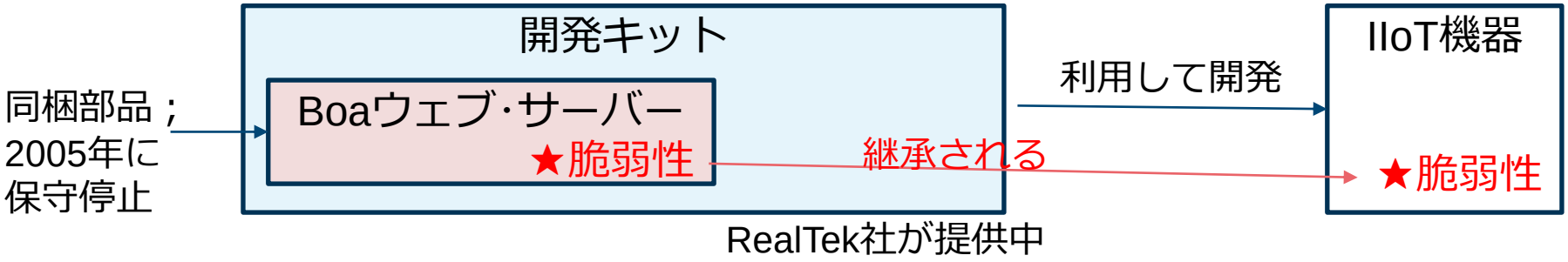
  — 悪用された脆弱性がいわゆるNディ脆弱性であったことが
  後に判明

# IIoT機器に継承された脆弱性への攻撃事例 (続き)

- IoT機器のソフト開発に使われたソフトウェア開発キットが既知の脆弱性をもっていたことが11月に報告された

  Microsoft: Vulnerable SDK components lead to supply chain risks in IoT and OT environments
  https://www.microsoft.com/en-us/security/blog/2022/11/22/vulnerable-sdk-components-lead-to-supply-chain-risks-in-iot-and-ot-environments/

  - 開発キットはRealTek社が提供し広く利用されている
  - 開発キットに含まれるBoaウェブサーバーが2005年に提供打切り
  - Boaウェブサーバーには既知の脆弱性があり放置されてきた



# 継承される脆弱性 (課題)

2021年末に公表された
Log4jの脆弱性(Log4Shell)の例も

- IIoT機器やICSに，開発のエンジニアリング･サプライチェーンを通じ継承される既知の脆弱性が多数存在している
  - OSや通信ライブラリー，CODESYS(PLC開発ライブラリー)など

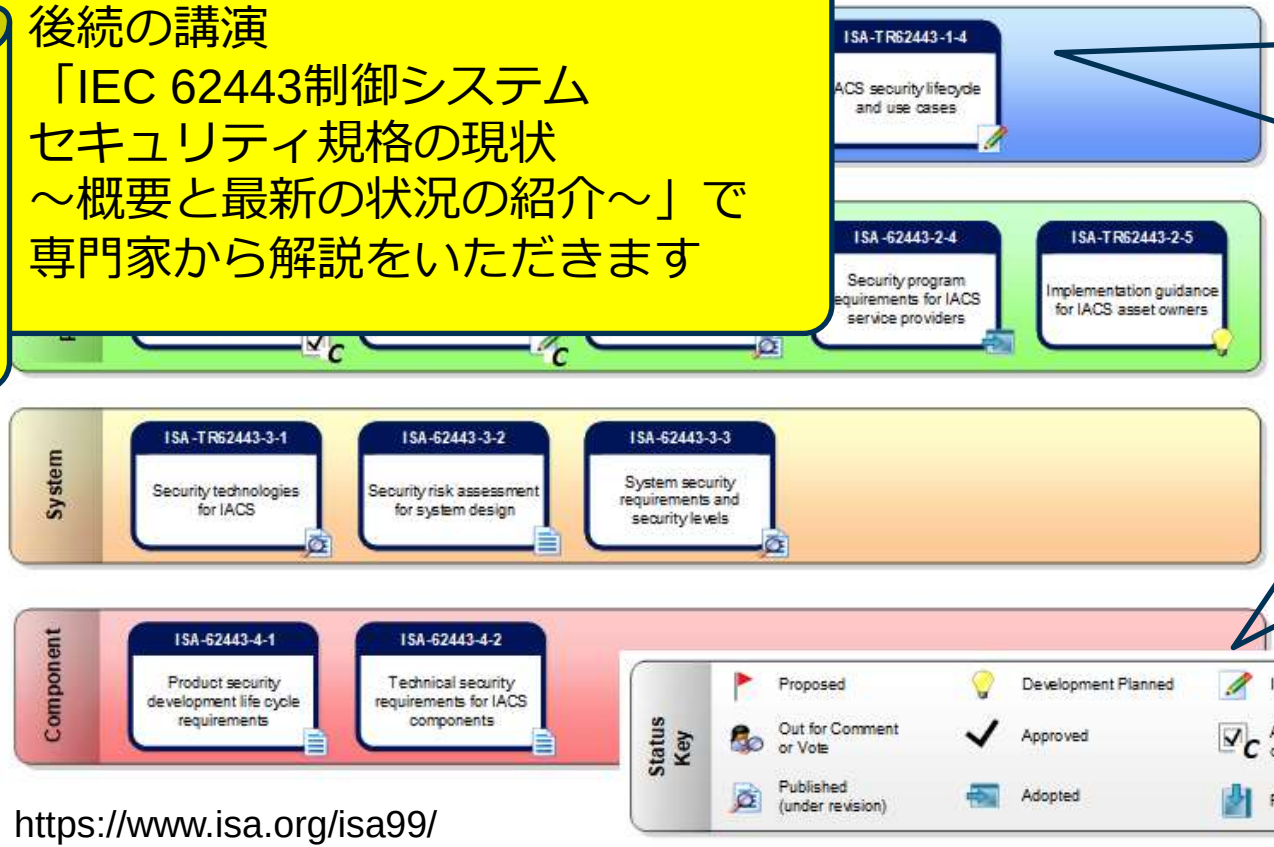
- こうした脆弱性の継承を製品利用者が知るために
  ソフトウェアBOM(Bill of Materials；S-BOM)が求めらている
  - 製品に組み込まれているソフトウェア部品(名称，版番号など)の情報を製品提供者が網羅的に列挙
  - 開示された脆弱性情報とS-BOMから継承された脆弱性を知る
  - 2021年5月の大統領令(14028号)で調達時にS-BOMを要件とすることを連邦政府機関に義務付け

- ☞ IEC 62443の標準化作業の表立った動きはなかったが…
- ☞ ICS関連の認証件数が微増ないし漸増

# 標準化や認証に関する動向

# IEC 62443 (ISA 62443) シリーズ： 2022年の新文書公開なし

後続の講演
「IEC 62443制御システム
セキュリティ規格の現状
～概要と最新の状況の紹介～」で
専門家から解説をいただきます




2つの新文書準備中
- 62443-1-5
  プロファイリング
- 62443-1-6
  IIoTへの適用

新しい層の追加(?)
- 62443-5-*
- 62443-6-*

https://www.isa.org/isa99/

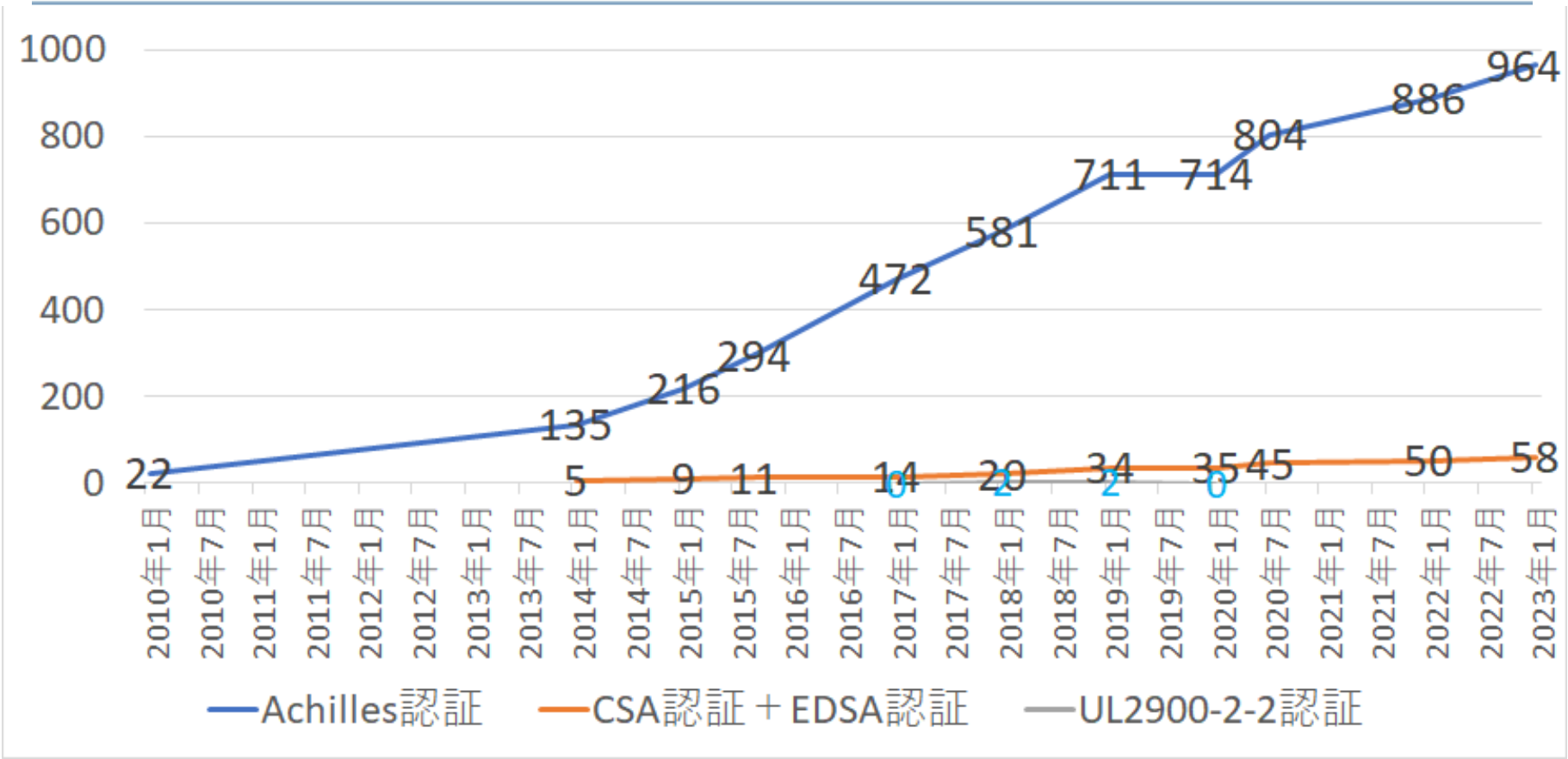
# 認証を受けたICSコンポーネント製品数の動向

- Achilles認証が，1年で約60製品が増えて，946製品に(前年886製品)
  https://www.ge.com/digital/applications/achilles-communications-certified-products
  - GE Digital社が運用している認証制度

- EDSA＋CSA認証は，1年で8製品が認証され，総計58製品に
  https://isasecure.org/end-users/iec-62443-4-2-certified-components
  - ISA SecureがIEC 62443-4-2に基づいて認証
  - うち1製品は国内ベンダーの製品
  - 2022年に新たに認証された8製品の認証水準は
    5製品がCSA 1.0.0 Level 1
    3製品がCSA 1.0.0 Level 2

**EDSA：**
Embedded Device Security Assurance
**CSA：**
Component Security Assurance

# 認証を受けたICSコンポーネント製品数の推移



# ICS(システム)に対する認証の動向

- SSA (System Security Assurance)認証
  https://isasecure.org/end-users/iec-62443-3-3-certified-systems

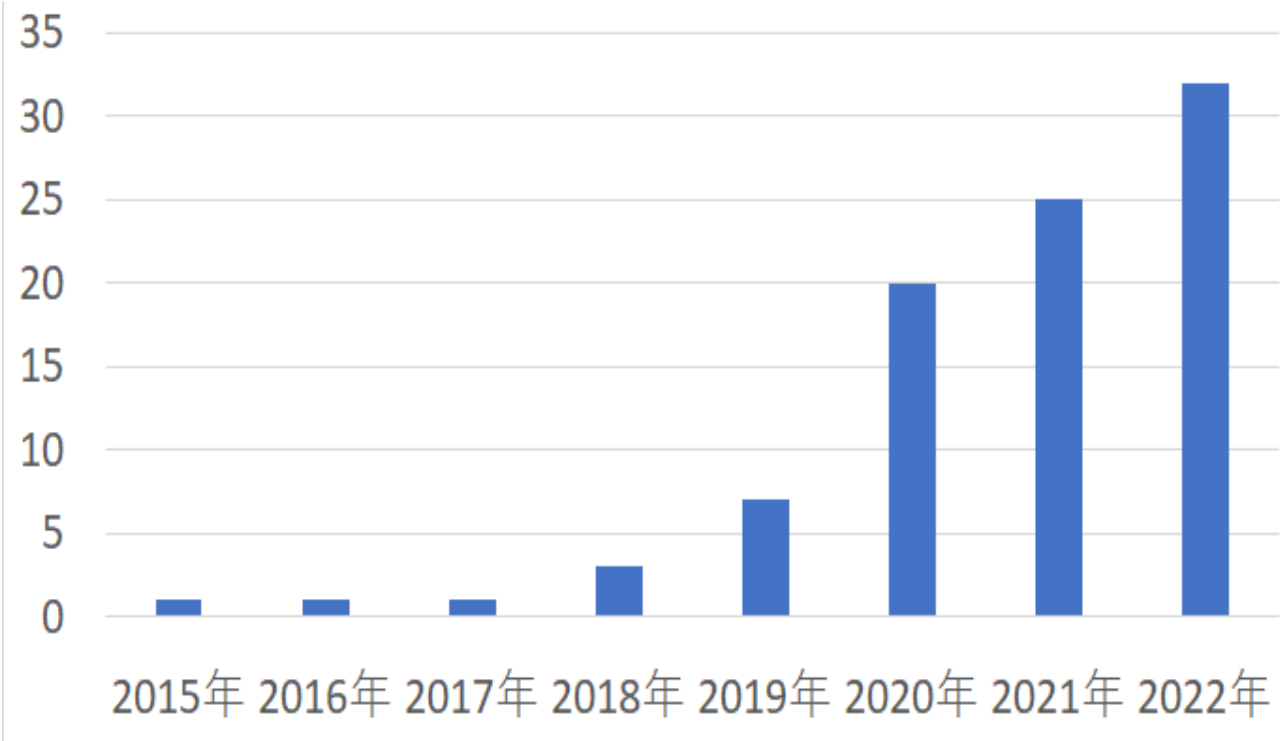
  — ISA SecureがICS(システム)を対象としてIEC 62443-3-3 に照らしてセキュリティを認証

  — 実態はDCSやSISのような製品がシステムとして認証されている

  — 2022年には新たに1システムが認証され，累計で5システムに

# 開発プロセスの認証への関心

- SDLA (Security Development Lifecycle Assurance) 認証




ISA Secureが，
製品/システム開発組織(拠点)を対象として，その開発プロセスにおけるセキュリティ対をIEC 62443-4-1に照らして認証している

☞ EUがNIS2を採択し発行
☞ サイバー保険の動向

# 規制や公的ガイダンスに関する動向

# EUがNIS2を採択し発効へ

正式名： Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2022:333:FULL&from=FR

- 2021年1月16日に指令として発効し，2024年10月17日までに対応する国内法の整備をEU加盟国に義務付け
- 2016年のNIS(Network and Information Systems)指令に置き換わり対策強化

  NISでは加盟国に委ねていたが，NIS２では：

  — セキュリティ対策の共通ベースラインを設定

  — 一定の規模を超える事業者に一律に適用

# 公的ガイダンス

- 米国CISAが業界横断的ベースライン「サイバーセキュリティ実施目標(CPG)」(Cross-Sector Baseline Cybersecurity Performance Goals)を公表
  https://www.cisa.gov/cpg
  — ITとOTのサイバーセキュリティ対策から抽出して優先度付け

- 米国NIST傘下のNCCoEが製造事業者向けのサイバー・インシデント対応と復旧に焦点を絞ったガイダンス作りに向け参加者を募集
  [プロジェクト記述書] Responding to and Recovering from a Cyber Attack -- Cybersecurity for the Manufacturing Sector
  https://www.nccoe.nist.gov/sites/default/files/2022-12/mfg-recovery-project-description-final-r1.pdf

# サイバー保険に関連した動き

- Merck社がAce American保険に対して勝訴
  - マルウェアNotPetya被害(2017年)についてサイバー保険金請求
  - 保険会社は「戦争条項」に該当するとして免責を主張
  - ニュージャージー州最高裁が14億ドルの保険支払いを命じた
    https://www.bloomberglaw.com/public/desktop/document/MerckCoIncvsAceAmericanInsuranCeDocketNoL00268218NJSuperCtLawDivA

    戦争条項への該否は明らかでなく，
    明らかでない条項は保険契約者に有利に解釈することが妥当

- Merck社の判決により保険会社が「戦争条項」の条文改訂検討を開始

# 全体のまとめ

1. 差し迫った脅威としてランサムウェア感染を想定した対策を！
2. 進化するICSに対応したサイバーリスクの再評価と対策を！
   - IIoT機器やクラウド利用をはじめとする<br>ITシステムとICSとの密結合化
   - ICSの新しいネットワーク･アーキテクチャー
   - 新技術に付随する潜在的な脆弱性
3. サイバー戦争に関する今後の国際的動向に要注意
4. 幸いここ数年間はICSに対する攻撃手法の進化が足踏み状態
5. 懸念される継承された脆弱性が蓄積するIIoT機器を含むICS製品

# その他の参考資料

- SANS： [Survey] Survey The State of ICS/OT Cybersecurity in 2022 and Beyond
  https://www.nozominetworks.com/downloads/US/SANS-Survey-2022-OT-ICS-Cybersecurity-Nozomi-Networks.pdf
- ENISA： ENISA Threat Landscape for Ransomware Attacks
  https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks
- Dragos： Six Months Later: Assessing the OT and ICS Risks of the Log4j Vulnerability
  https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_WP_Log4J_05_2022_final.pdf
- CyBeats, Gartner： SBOM Insights: Using SBOMs to strengthen the security of your software supply chain
  https://www.cybeats.com/gartner

# お問い合わせ、インシデント対応のご依頼は

## JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- https://www.jpcert.or.jp/

## インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

## 制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form.html

## 脆弱性に関するお問い合わせ

- Email：vultures@jpcert.or.jp
- https://jvn.jp/

# ご清聴ありがとうございました