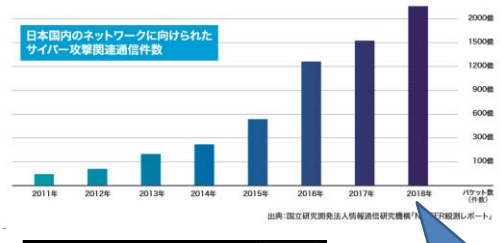
サイバー攻撃の事例集

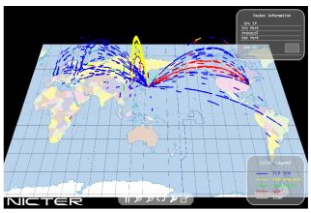
サイバー攻撃事故事例は、沢山あるのですが、ここでは制御システムを標的にした事例の一部を取り上げております。

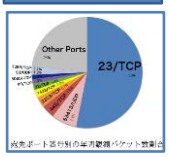
株式会社ICS研究所
https://www.ics-lab.com/e/

1

出典元：NORSE社のWebライブ







http://www.nicter.jp/#
出典元：NICTER　観測レポート

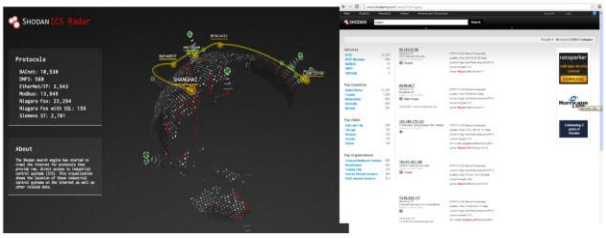
インターネットのサイバー空間の脅威

インターネットのサイバー空間は、常に、サイバー攻撃の脅威にさらされています。

2

悪用されるSHODAN

- インターネットにつながる制御装置や機械を検索して、市場や通信仕様条件別に分類し、サイバー攻撃に必要な情報を提供していることになる。



出典元　https://ics-radar.shodan.io/

出典元　www.shodanhq.com

SHODANやCensysにアクセスすると、インターネットにつながる制御装置や機械を探し出して自動登録する機能ソフトウェアを送り込まれる。

広がるサイバー攻撃ビジネス

プロによる安価なDDOS攻撃サービス

料金
1～4時間　：1時間2ドル
5～24時間　：1時間4ドル
24～72時間　：1時間5ドル
1か月　：1000ドル

高度な攻撃も対応するサイバー攻撃請負業者も登場しています。

最大級のWebサイト・フォーラム・ゲームサービスを攻撃できます。
代金をいただく前にテストをいたします。
ただし、サービスの性質上返金はいたしません

http://www.mcafee.com/de/resources/white-papers/wp-cybercrime-exposed.pdf

https://2ogmrlfzdthnwkez.onion.to/

- サイバー攻撃下請けやサイバー攻撃ツールレンタル業者まである闇市場
- 需要者は、サイバー軍やその下請け企業、犯罪集団やサイバーマフィア、テロ集団など

会員制の闇市場では、30以上のサイバー攻撃請負い業者が確認されている。
高度なマルウェアで指定された標的をサイバー攻撃をする業者も登場している。

悪用されるサイトと拡がるサイバービジネス

出展元：ICS研究所のeICS

3

三菱電機がサイバー攻撃を受ける

防衛・電力・鉄道・交通などの重要インフラに係わる機密情報が狙われる

- 2020年1月20日発表
  - 2019年6月頃、大規模なサイバー攻撃を受けた。
  - 政府機関とのやり取り、取引先企業の情報、8000人以上の個人情報が搾取された可能性がある。
- 攻撃側は、中国系ハッカー集団「Tick」及び別の中国系ハッカー集団「Black Tech」（台湾や日本の製造業企業を標的に）など
- 攻撃は、ゼロDayであった。
- 侵入ルートは、中国の関連企業から三菱電機の中国法人、そこから日本の三菱電機社内ネットワークへ
- 標的は、中間管理職のPCなどに入っている機密情報

4

電力、石油、ガス、化学、水道、医療、金融、クレジット、航空、鉄道、情報通信

重要インフラ

インターネット接続していなくても、業者が持ち込んだPCやベンダーから持ち込まれたソフトウェアから、マルウェアが感染するリスクや交換部品から侵入するリスクがある。
脆弱性は無いと言いながら、新規発注仕様書のコンピュータ仕様にWindowsNT4＋サービスパック6またはそれ以上という条件やXP、Windows7、8などを認めているところがあり、脆弱性に関する認識が間違っているケースも多い。

5

アメリカ

電力システムに対する攻撃

'Russia hacking code' found on Vermont utility computer

31 December 2016 | US & Canada

An electrical company in the US state of Vermont says it has found malware code allegedly used by Russian hackers on one of its company laptops.

The Burlington Electric Department **said it had taken "immediate action to isolate"** the computer, which was not connected to the electrical grid.

The government alerted them to the "Grizzly Steppe" code on Thursday.

時期　2016年12月
(米国大統領選挙 11月)

場所　米国　バーモント州
バーリントン・エレクトリック・デパートメント社
(電力会社)

事象　社内ラップトップPCよりロシアのハッカーが使用しているとされるマルウェアを発見。電力網には接続されていなかった。発見後、直ちにネット環境から隔離。

GRIZZLY STEPPE
同時期に行われていたロシアのサイバー攻撃につけられた名称

出典）http://www.bbc.com/news/world-us-canada-38479179

6

カナダ

電力システムに対する攻撃

時期　2016年12月
(米国大統領選挙 11月)

場所　カナダ　オンタリオ州
ハイドロ・ワン社
(送電・配電会社)

事象　ハイドロ・ワン社の使用しているIPアドレスの一つがロシアのサイバー攻撃に関連するものの一つだった。ここを基点に、電力網にサイバー攻撃を仕掛けることも可能であった。

出典）http://www.ctvnews.ca/canada/exclusive-ip-address-at-ontario-power-utility-linked-to-alleged-russian-hacking-1.3226290

7

アメリカ

電力システムに対する攻撃

時期　2017年7月6日の記事

情報源
米国 国土安全保障省
F.B.I

内容
カンサス州の　Wolf Creek 原子力運営会社の情報システム系ネットワークがハッキングされた。
制御系システムに侵入された痕跡は無い。
将来の攻撃に向けた調査と推定。

出典）https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html

8

ロシア

電力システムに対する攻撃

THE TIMES | Today's sections | Past six days | My articles | Times+ | My account

Ready for more? Get unlimited access by subscribing for less than £1 a week.

Russia-backed hackers try to hijack Britain's power supply

Aaron Rogan, Mark Bridge

July 15 2017, 12:01am, The Times

Hackers targeted control systems operating electricity supplies

GARETH FULLER/PA

Share | Save

Hackers backed by the Russian government have attacked energy networks running the national grid in parts of the UK, *The Times* has learnt.

時期
2017年7月15日の記事

発信者
Ireland's Electricity Supply Board (ESB)

内容
ロシアのGRUが関与するハッカー集団が、北アイルランドの送電システムに侵入。実害は無かったが、停電等の混乱を狙ったと考えられている。
従業員宛の標的型メールが確認されている。

出典）https://www.thetimes.co.uk/article/russia-backed-hackers-try-to-hijack-britain-s-power-supply-55bj9790r

9

イギリス

電力システムに対する攻撃

Hacks 'probably compromised' UK industry

18 July 2017 | Technology | Share

GETTY IMAGES

Some industrial software companies in the UK are "likely to have been compromised" by hackers, according to a document reportedly produced by British spy agency GCHQ.

A copy of the document from the National Cyber Security Centre (NCSC) - part of GCHQ - **was obtained by technology website Motherboard.**

A follow-up by the BBC indicated that the document was legitimate.

時期　2017年7月18日の記事

発信者
National Cyber Security Centre (NCSC)

内容
英国の複数の制御系システムを利用する企業が、国家レベルの組織が支援する敵対的ハッカー集団によって攻撃されている。

また、複数のエネルギー関連企業や製造業企業のIPアドレスが上記ハッカー集団に乗っ取られている。

この様な攻撃は英国に限られたものではなく、全世界的に行われている。

出典）http://www.bbc.com/news/technology-40642962
https://motherboard.vice.com/en_us/article/9kwg4a/gchq-says-hackers-have-likely-compromised-uk-energy-sector-targets

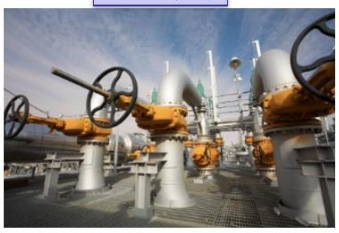
10

サウジアラビア

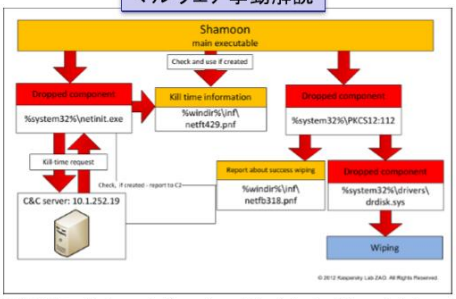
石油化学システムに対する攻撃

- ●2012年、サウジアラビアの石油会社の制御システムで利用されるPC30,000台がマルウェアに感染。マルウェアの攻撃対象は、オイルの流れを止め、オイル製造事業の停止を狙っていた。
- ●攻撃により、内部ネットワークが1週間以上停止し、同ネットワークに接続されていたPCのディスクはすべて削除された。攻撃内容を調査したが、従業員が攻撃へ関与したか否か不明とのこと。

Oil Company



マルウェア挙動解説



出典：http://wired.jp/2012/08/28/worlds-largest-oil-producer-falls-victim-to-30k-workstation-attack/
http://securelist.com/blog/incidents/57784/shamoon-the-wiper-further-details-part-ii/

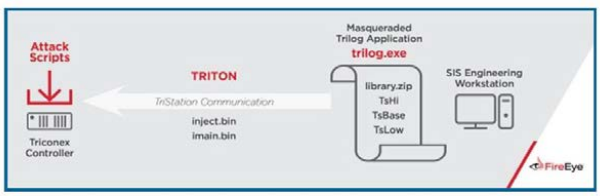
11

中近東プラント

安全計装に対する攻撃

TRITON：Schneider Electricの安全計装コントローラ「Triconex」を標的にしたマルウェア

- 攻撃者はTriconexのEWS（エンジニアリングワークステーション）にリモートからのアクセスを確立してTRITONを仕込み、コントローラのコンフィグレーションプログラムを改竄。
- 改竄したプログラムをコンパイルして、ランタイム版を作成。
- ランタイム版をコントローラに送り込んで差し替え作業を実施。
- コントローラのモードを変えたことで、外部ハードシーケンスが作動して、緊急停止プロセスに強制移行。トリップに至る。



TRITONは、産業制御システムを手掛ける世界大手Schneider Electricの安全計装コントローラ「Triconex」に干渉する設計になっていた（出典：FireEye）

12

医療機器の脆弱性情報

アメリカ・日本

- 2012年には、医療機器で使われている遠隔操作のソフトウェアについて脆弱性が発覚し、米国のFDA（食品医薬品局）が製品回収情報を公表した。
- 2013年には、ICS－CERTが、医療機器のパスワードの脆弱性について警告しました。40ベンダ約300の医療機器（麻酔器、人工呼吸器、薬物注入ポンプなど）に関係し、機器によっては遠隔操作が可能だという指摘があった。
- 2017年には、岡山大学病院で、患者情報を保有した医療用端末がウィルスに感染し、外部との不正通信が確認された。

13

医療機関に対する攻撃

アメリカ・カナダ

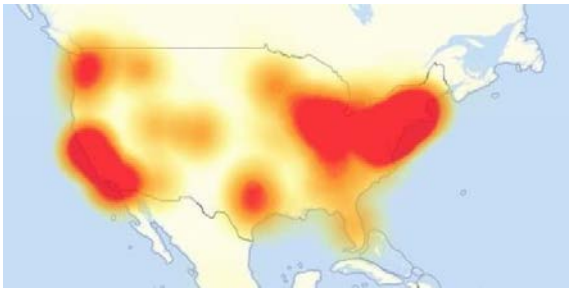
- 2016年には、米国とカナダの医療機関で、ランサムウェアによる暗号化被害が相次ぎました。院内ネットワークに侵入したマルウェアがローカルサーバーを介して院内PCに感染し、PCを使った業務が一切できなくなるなどの影響が発生した。

14

アメリカ

米で大規模サイバー攻撃　ツイッターやアマゾン被害

- 2016年10月22日　防犯カメラなど10万台がマルウェアに感染し、大規模DDOS攻撃。
- ツイッター、アマゾン・ドット・コム、ペイパル、ソニー、エアービーアンドビー、スポティファイ、ニューヨークタイムズ、ウォールストリートジャーナル、ネットフリックスなど多くのネットサービスで21日、数時間にわたり米国で局所的に各社のサイトに接続できずサービスが使えない状態に陥った。



出典：https://newswitch.jp/p/6545
Dynのサーバーダウンによりウェブサービス停止に追い込まれた米国の地域（Downdetector.com）

15

航空機、整備システム
空港
管制システム
衛星通信システム

航空機

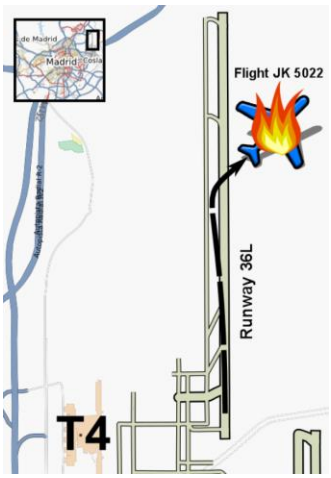
2015年には、米国会計検査院から、航空機や船舶などの脆弱性に懸念があるという報告があった。
2018年8月のBlack hat USA 2018で、航空機に脆弱性があるという公開デモ発表がありました。

16

スペイン

航空機に対する攻撃

- 2008年8月20日：スペインの航空会社で中央システムがUSBメモリを介してウィルスに感染。他の要因もあったようですが、航空機が離陸に失敗しました。この事故では、乗員乗客154名が亡くなってしまいました。
- 2008年10月6日付速報によれば、フライトデータレコーダの記録として、事故機はフラップを展開せずに（0°）離陸しようとしていたこと、およびこの種の離陸時設定異常を知らせる警報が鳴っていなかったことを発表した。

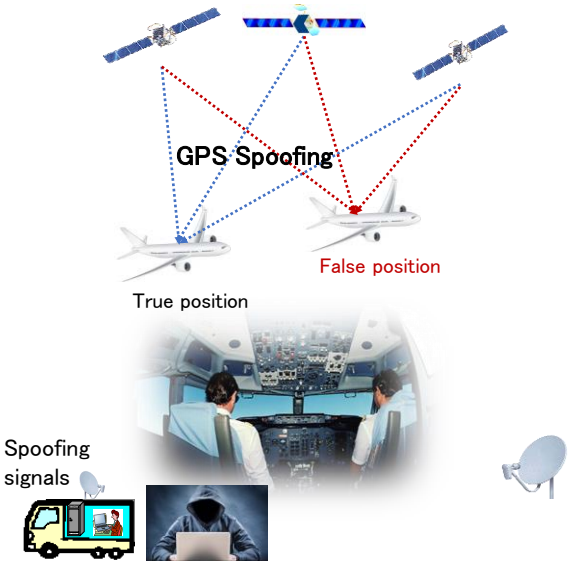


出展：ウィキペディア
スパンエアー5022便

17

航空機／衛星通信に対する攻撃

- GPSは電波が弱く、小さな出力でも妨害が可能なため、テロ等による妨害や悪意あるいたずらによって被害を受ける蓋然性は高い
- 特に現行のGPS信号であるL1、L2は周波数の帯域が狭いため 脆弱である。軍用コードや次世代GPSの信号であるL5は周波数幅が広く、電波出力も高いため、現行の民生コードよりも相対的に脆弱性は低い。ただし、軍用及び民生コードどちらも弱い電波であることから、いずれにせよジャミングを受ける可能性がある
- スプーフィングとは、GPS信号を受信、解読した後、その信号に偽情報を組み込んだものを、あたかも本来のGPS信号のごとく 送信することにより、受信者側に誤った情報を提供することで、正確な測位を妨げる行為をいう。



18

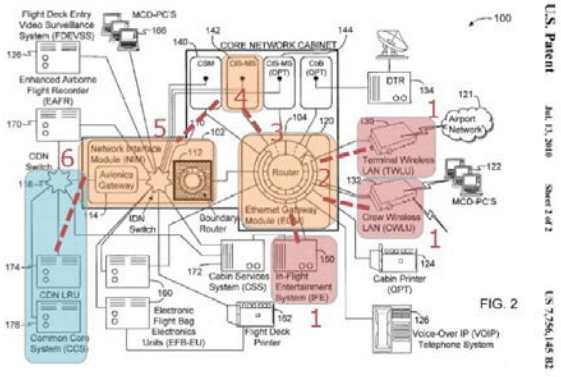
ポーランド

航空会社に対する攻撃

- 2015年6月21日：（CNN） ポーランドの航空会社LOTポーランド航空の地上システムがサイバー攻撃を受け、首都ワルシャワのショパン空港からの出発便が軒並み欠航となるトラブルが起きた。この影響で乗客1400人あまりが同空港に足止めされた。
- LOTポーランド航空によると、このトラブルは21日に発生。同社の地上システムが不正アクセスされて出発便の飛行計画が作成できなくなった。この影響でワルシャワから出発予定だった同航空の20便が欠航となり、さらに数便に遅れが出た。

19

航空機の脆弱性に関するBlack Hat USA 2019での報告



https://www.wired.com/story/boeing-787-code-leak-security-flaws/

- 2018年9月大手航空機メーカーのサーバにおいて、航空機のシステム構成に関する情報がインターネット上に公開されていることが発覚。
- IOActive社(I社)は、特定の脆弱性を用い、機内エンターテイメントシステム等から、機器の操作に関わるネットワークに到達できることを発見し、メーカーに報告。
- メーカーはI社に対して、報告されたのは悪用可能な脆弱性ではなく、緩和策も実施済と回答するも、詳細は不開示。
- これに失望したI社は2019年8月のBlack Hatで脆弱性の詳細を公開。
- これを受けメーカーは、I社は航空機ネットワークの一部を評価しただけで、I社のシナリオで は重要な航空機システムに影響を与えることはできず、発表は無責任だと失望を表明。

20

電車
路線設備管理システム
切符購入・料金システム
決済システム

交通機関

ロンドンの鉄道設備の新規設備購入仕様書の設計条件に、「Windows.NET4サービスパック6又はそれ以上・・・」という条件が今もって入っていたという。
それで脆弱性が無いと言えるのか？　サイバー攻撃の可能性が無いと言えるのか？

21

ポーランド

鉄道のポイント切替システムに対する攻撃

- 2008年：ポーランドで14歳の少年が路面電車システムに侵入。ポイント切替機を不正に操作し、列車4車両が脱線しました。
- 路面電車の運転手がトラムをポイントで右に行こうとしたところ、左に曲がったことで、別のトラムと衝突したとのこと。それによって乗客は床に投げつけられてけが人が出たという。
- 使用したのは、TV用の操作端末（赤外線端末）を加工して、電話などと組み合わせて、路面電車システムに侵入。

22

アメリカ

交通システムの料金システムに対する攻撃

- 2016年：サンフランシスコ市交通局の局内システムへのランサムウェア攻撃により、サンフランシスコ市営鉄道（Muni）地下鉄の料金システムがダウンしました。
- 回復するまでの時間、料金は無料となりました。

23

スウェーデン

交通システムがマヒ

- 2017年10月11日12日　スウェーデンの交通当局のシステムがサイバー攻撃を受けてマヒ。列車の運行停止・遅延が生じた。
- Trafikverket（スウェーデン産業省交通局）の関係者が確認したところによれば、このDDoS攻撃は、同機関の業務に影響を及ぼすために、サービスプロバイダーTDCとDGCを狙って行われた攻撃だった。
- その翌日、別の政府機関であるTransportstyrelsen（スウェーデン交通局）と、公共交通事業者Västtrafikのウェブサイトが、別のDDoS攻撃に襲われた。

出典：https://the01.jp/p0005941/

24

自動車
半導体製造
鉄鋼製造
製紙製造

製造業

サイバー攻撃の手法は、日々高度化していますが、設備は日々替えられません。
情報セキュリティ対策技術だけでは、難しくなっています。
短時間に回復するために何をどのようにしたら良いか、分かっていないケースも多い。

25

自動車製造工場に対する攻撃

ドイツ、日本

- 2005年米国で、外部から持ち込まれて接続されたノートPCにより、独ダイムラーの13の工場がWORM_ZOTOBなどの不正プログラムによって操業停止になった。
- 各工場の製造ラインが止まり、5万人の自動車工場の労働者は50分間作業ができない状態になり、1400万ドル（約17億円）の損害を出した。

- 2008年に西日本の自動車会社の工場では、ベンダがエンジニアリング端末（操作パソコン）を入れ替えたところ、エンジニアリング端末にウィルスが混入していた。
- その結果、3日間程度工場の製造ラインの応答が遅くなり、原因究明には1ヶ月を要した

26

日本

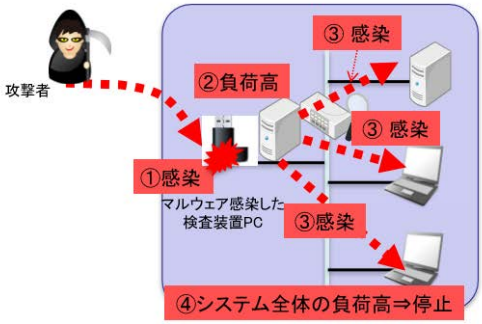
半導体製造工場に対する攻撃

- 2011年に、日本の国内大手半導体メーカでUSBメモリを経由して、品質検査を行う検査装置へマルウェアが感染した。
- 感染により、検査プロセス処理の負荷が異常に高まり、本来不良品として判定すべきものがそのまま検出されずに通ってしまう不具合が発生した。さらに感染元が分からず、感染が飛び火し、最終的には生産ラインが停止した。

半導体工場

出典：写真は参考情報（WEBRONZA）

マルウェア挙動解析



27

ドイツ

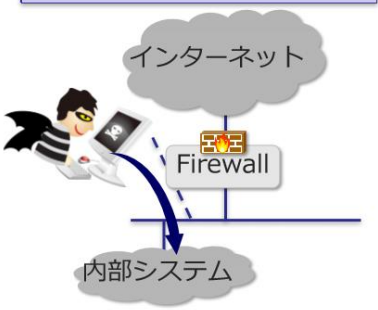
製鉄所に対する攻撃

- 2014年ドイツで、製鉄所の溶鉱炉のコントロールなど内部システムのコントロールを許可するユーザIDとパスワードが、攻撃者に電子メールに添付したマルウェアを使われ、不正入手されてしまう。
- 溶鉱炉を正常に停止できず、生産設備が損傷する大きな被害を受けた。SCADAを攻撃対象として、SCADAの設定ファイルに悪意あるコードを追加した。

Steelworks

写真は参考資料（フェルクリゲン製鉄所-wikipedia）

攻撃者がリモートアクセス経路で内部システムに不正アクセス



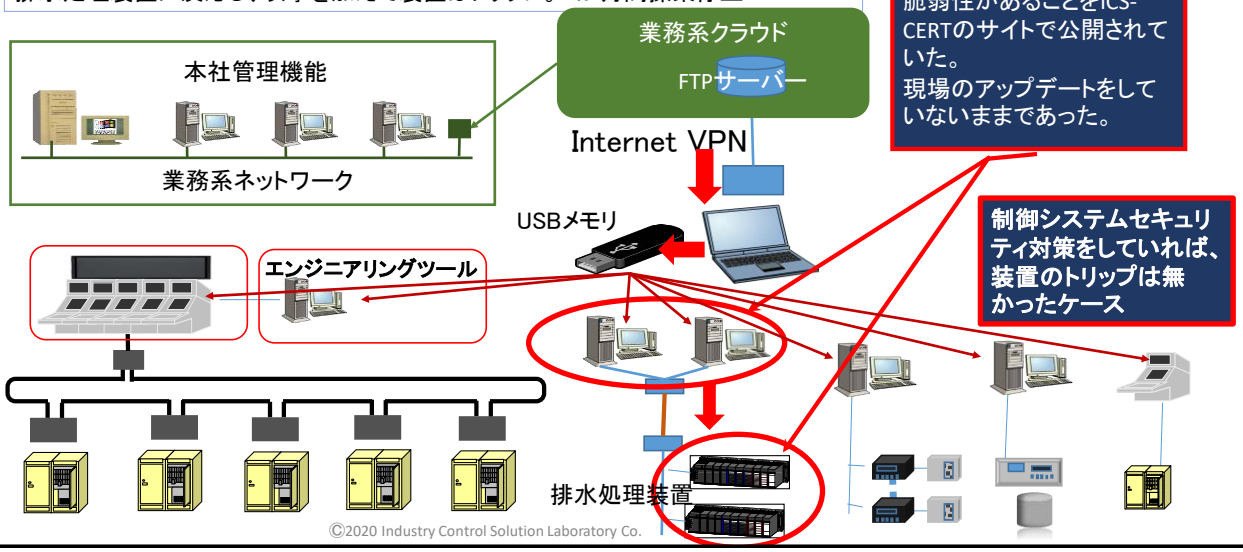
出典：https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf

28

製紙製造工場に対する攻撃

日本

2016年2月　ある制御ベンダ製品を標的にしたStuxnet亜種版マルウェアが侵入して、USBメモリ経由で全てのServerに感染。標的の制御ベンダのSCADAとPLCを使った排水処理装置に反応し、攻撃を加えて装置はトリップ。1か月間操業停止



29

自動車製造工場にWanaCryが拡大感染

日本、北米、欧州、中国

- 2017年6月18日にホンダの狭山工場のネットワークにWanaCryが侵入したことが発覚。操業停止に至った。
- WanaCryは、日本、北米、欧州、中国など複数の地域の工場に侵入された。
- 2017年4月にWanaCryの流行情報を受け、ホンダは5月にセキュリティ対策を実施したが、役に立たなかった。
- 操業停止は、狭山工場のみという。

30

台湾TSMC社のサイバー攻撃事故被害

- 2018年8月3日に台湾のTSMC（Taiwan Semiconductor Manufacturing Company）社がWanaCryランサムウェア（亜種版）攻撃で製造停止に至り、6日までに回復した。
  - 廃棄したウェハーは1万枚以上。
  - 次のデリバリーは、2か月後になるかも知れない。
  - 損害金額約300億円以上

台湾

Taiwan Semiconductor Manufacturing Company Limited

TSMC Details Impact of Computer Virus Incident

Issued by: TSMC
Issued on: 2018/08/05

Hsinchu, Taiwan, R.O.C., Aug 5, 2018 – TSMC today provided an update on the Company's computer virus outbreak on the evening of August 3, which affected a number of computer systems and fab tools in Taiwan. The degree of infection varied by fab. TSMC contained the problem and found a solution. As of 14:00 Taiwan time, about 80% of the company's impacted tools have been recovered, and the Company expects full recovery on August 6.

TSMC expects this incident to cause shipment delays and additional costs. We estimate the impact to third quarter revenue to be about three percent, and impact to gross margin to be about one percentage point. The Company is confident shipments delayed in third quarter will be recovered in the fourth quarter 2018, and maintains its forecast of high single-digit revenue growth for 2018 in U.S. dollars given on July 19, 2018.

Most of TSMC's customers have been notified of this event, and the Company is working closely with customers on their wafer delivery schedule. The details will be communicated with each customer individually over the next few days.

This virus outbreak occurred due to misoperation during the software installation process for a new tool, which caused a virus to spread once the tool was connected to the Company's computer network. Data integrity and confidential information was not compromised. TSMC has taken actions to close this security gap and further strengthen security measures.

31

船舶
航行管理システム
港湾管理システム
衛星通信システム

船舶

ClassNKでは、2018年より、船舶で使用するコンピュータ製品の登録を義務付けした。
セキュリティ対策として脆弱性情報を管理する上で、最低限必要な管理である。
「Guidelines on Cyber Security Onboard Ships Version 2.0」が発行されている。

32

ベルギー、イラン

船舶企業に対する攻撃

ベルギーのAntwerp港における事例

- 薬物を密輸する目的で、密売グループがハッカーを雇ってコンテナターミナル事業者や港湾会 社のコンピュータに不正に侵入していた。

イランの船会社IRISLに対する攻撃

- 2011年8月、イランの船舶会社IRISLのサーバーがハッカーの侵入を受け、輸送料、積み込み、貨物番号、輸送日、輸送先などのデータが盗まれ、コンテナーの場所を特定できなくなる被害に見舞われました。かなりの貨物が間違った目的地に輸送されたほか、なくなった貨物もありました。

海賊が船舶から特定のコンテナの中身だけ奪った事例

- 海賊が事前に船会社が自社開発したCMSを攻撃して、目的のコンテナと、それを輸送する船舶を特定していた。

出典:カスペルスキー

33

韓国、メキシコ

船舶に対する攻撃

韓国の採掘装置船の事例

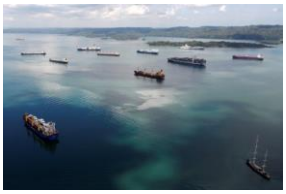
- 2010年、韓国の建設現場から南米へと輸送中の掘削装置が傾く事故がありました。船のコンピューターと制御システムはウイルスだらけ。ハッキングを確認して修正するまで、19日を要した。

メキシコ湾の移動式海洋掘削装置が操業停止に陥った事例

- 労働者がスマートフォンやその他の個人的な機器を掘削装置のナビゲーション制御システムに接続し、その際に感染したマルウェアによって 現場が一時的に中断した。

韓国へのGPSジャミング攻撃

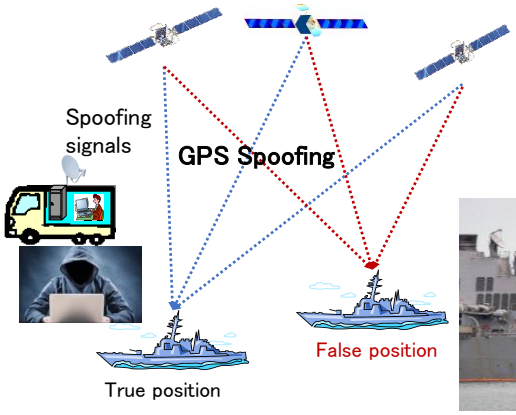
- 2010年以降、北朝鮮によるものと思われる攻撃が 2010年以降に度々発生し、その度に船舶の航行に影響を与えている。

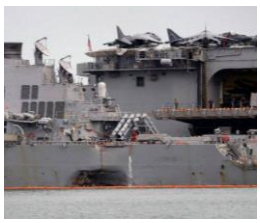


34

船舶に対する攻撃

2017年6月に黒海でGPS通信の操作で、航海中の船20隻のナビゲーション・システムが正常で作動していたにも関わらず、別の位置に誘導されていた事件があった。「スプーフィング」と呼ばれる技術が使われた疑いが高い。





アメリカ

2016年

- 8月19日　大陸間弾道ミサイル搭載の原子力潜水艦ルイジアナが、米ワシントン沿岸で海軍の小型補給艦と衝突。

2017年

- 1月31日　ミサイル巡洋艦アンティータムが横須賀基地の提供水域内で停泊していた際、浅瀬に接触、スクリューの損傷と油圧作動油が流出する事故となる。
- 5月9日　ミサイル巡洋艦レイク・シャンプレインが日本海の公海上で、韓国漁船と衝突する。原子力推進航空母艦カール・ビンソンなどと連合海上訓練中で起きた事故。
- 6月1日　イージス駆逐艦フィッツジェラルドが伊豆半島沖でフィリピン船籍コンテナ船と衝突、乗組員7人が死亡、極めて大きな損傷を受ける。現在横須賀基地のドックに停泊中だが、9月末には米国での修理のため帰国。
- 8月21日　イージス駆逐艦ジョン・S・マケインが、シンガポール沖のマラッカ海峡で石油タンカーと衝突、乗組員5人が負傷、10人が行方不明。

35

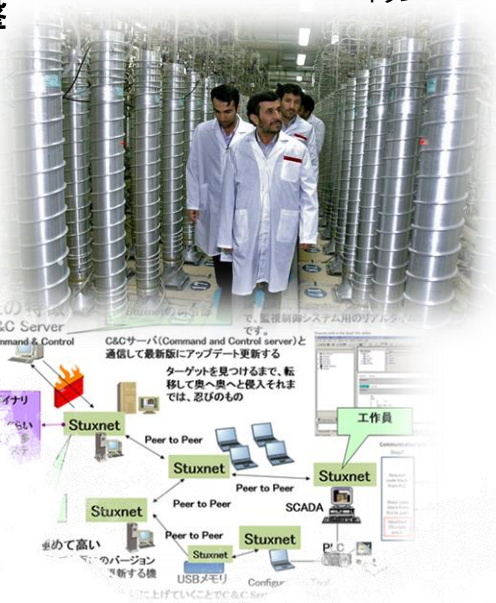
核爆弾開発を遅らせることを目的にサイバー攻撃を実施
軍事介入する戦略としてサイバー攻撃を使用
サイバー軍を陸・海・空・マリン（海兵）の次の軍として登用

国を標的にしたサイバー攻撃

36

ウラン濃縮施設の遠心分離機に対する攻撃

イラン



- 2010年：イランのウラン濃縮施設の遠心分離機を標的にしたStuxnetが発見された。
- Siemens社のWinCC（SCADA）とS7（PLC）の遠心分離機専用のFunction Blockを使用した制御システムを持つ遠心分離機を標的に、ステルス性が高く、シンプルな仕組みで感染力が高いマルウェアを米国とイスラエルで開発し、いろんな手段を使って、イランのウラン濃縮施設の制御システムに侵入させた。
- 4000台以上のウランの遠心分離機の半数近くが破損及び故障。
- 制御システムの構造や仕様が分かれば、制御装置を破壊できる標的型のサイバー攻撃が可能であることを裏付けた事例となった。

37

2013年韓国を標的にしたサイバー攻撃

韓国

- 2013年3月20日、韓国の放送局3組織、銀行3組織、併せて6つの組織のコンピュータシステム（4万8千台）が、サイバー攻撃が疑われる事態の中で同時に使えなくなり、銀行ATMやモバイル決済が影響を受けた。
- コンピュータシステムに被害が生じた組織は、韓国放送公社（KBS）、文化放送（MBC）、YTN、農協、新韓銀行、済州銀行であった。
- このマルウェアは、韓国製のウイルス対策ソフトウェアを無力化する機能を備えており、2013年3月20日午後2時になると、システムを破壊するように設計されていた。
- 具体的には、Windows PCのハードディスクのMBR（Master Boot Record）などの領域を破壊して強制的に再起動させたので、OSが起動しない状態となった。

38

ウクライナの大規模停電

ウクライナ

- 2015年12月23日にウクライナでサイバー攻撃による大規模停電（電力会社2-3社、影響人数 約22万人、停電時間3時間程度）が発生した。
- 当初はBlackEnergy3と呼ばれるマルウェアにより、監視制御システムのサーバのハードディスクが破壊されたことにより停電が発生したと報道されていたが、ハードディスクの破壊が停電に直結することは考えにくい。
- その後、リモート制御により（30カ所、110万ボルト級変電所7か所、35万ボルト級変電所23か所）のブレーカー遮断がなされたことが判明した。（BlackEnergy3の関与は不明）
- ウクライナ政府は、ICS-CERTに調査を要請し、ICS-CERTは以下の調査結果を発表した。

1.約22万5千人の顧客に影響が及んだ。
2.VPN接続を介して電力会社の監視制御システムへアクセスが行われていた。
3.一連の攻撃にBlackEnegryが初期のアクセス手段として用いられたかどうかは定かではない。


http://styknews.info/novyny/ns/2015/12/23/frankivsk-na-pivgodyny-zalyshyvsia-bez-svitla-foto

39

国を標的にしたインフラ攻撃
地下鉄の決済システムに対する攻撃
空港の登場システムに対する攻撃

ウクライナ

- 2017年10月26日：キエフ地下鉄のシステムがランサムウェア（BadRabbit）に感染し、決済システムへの影響が発生しました。
- 2017年10月28日：ウクライナのオデッサ空港のシステムがランサムウェア（BadRabbit）に感染し、搭乗手続きへの影響が発生しました。
- BadRabbitは、サイバー攻撃集団 ”ShadowBrokers” がNSAから流出させたマルウェアのコードを使用していており、CVE-2017-0145でCVE登録されているWindowsサーバーに関する脆弱性をエクスプロイトした攻撃だった。

40

イランの石油施設の対する攻撃

- 2016年10月7日（金）、イランのセムナーン州シャーロードにあるピルージ・オイル＆ガス・リファイナリー社の精油施設で石油貯蔵タンク1基が爆発し、火災となり、4名の負傷者が出た。
- 施設は、天然ガスのコンデンセートや超軽質原油を原料にしてガソリンとディーゼル燃料を生産する精油所で、2016年3月に完成したばかりである。火災があったのは、施設内の石油貯蔵タンクである。
- 8月27日、ジャラリ大将は、イランの石油化学工業がサイバー攻撃の標的にされていることを認めた。問題は施設のために輸入して取付けた部品にあるという。ジャラリ大将は、「ウイルスは石油化学コンビナートを汚染していた。ウイルスによる正規でない指令が危険に陥れる原因になりうる」と語っている。

イラン

- 過去6か月の間、イランの石油、天然ガス、石油化学の施設において同じような悩ましい事故がほぼ12日ごとに起こっており、今回の火災はもっとも新しい事故である。この7月には、フージスタン州のボウアリ・シーナ石油化学コンビナートで大規模な火災が発生し、鎮火までに3日間かかり、9名の負傷者が出た。また、9月には、ブーシェル州の石油化学工場で火災が起こり、4名の負傷者が出ている。さらに、2週間ほど前には、負傷者は出なかったが、ケルマーンシャー州のビスツーン石油化学工場で火災があった。

41

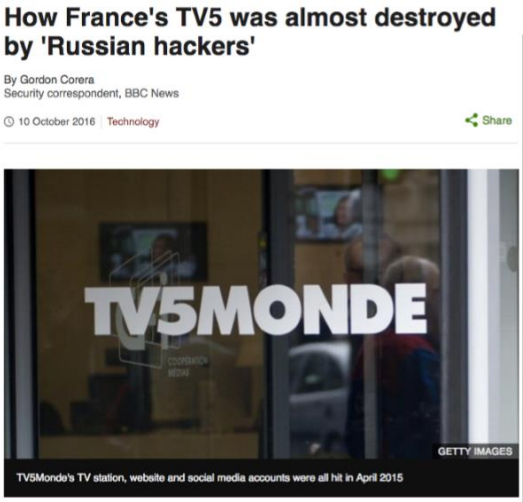
犯罪、恐喝、搾取、報復、詐欺、資金徴収

その他

42

フランス

TV局に対する攻撃



How France's TV5 was almost destroyed by 'Russian hackers'

By Gordon Corera
Security correspondent, BBC News

10 October 2016 | Technology

Share

TV5MONDE

GETTY IMAGES

TV5Monde's TV station, website and social media accounts were all hit in April 2015

A powerful cyber-attack came close to destroying a French TV network, its director-general has told the BBC.

当初、ISのサイバー攻撃と考えられたが、後にロシアのハッカーによるものと判明。
(2015年1月　シャルリー・エブド襲撃事件)

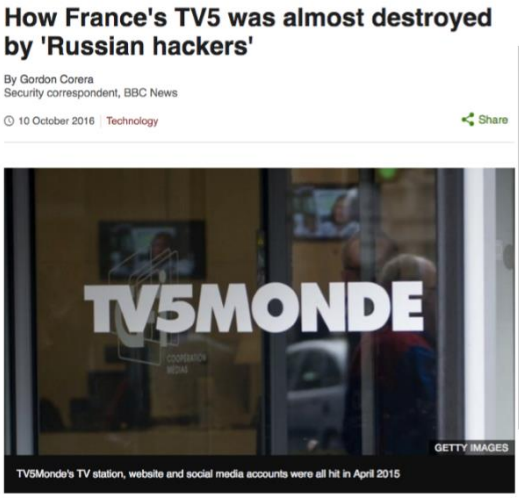
この攻撃は、非常に洗練されたもので、最初のネットワークへの侵入は2015年1月23日。

7つの方法を使って侵入したことが判明しており、そのうちの一つはTV5のスタジオから遠隔操作を行うオランダにあるお天気カメラと判明。

43

フランス

TV局に対する攻撃



How France's TV5 was almost destroyed by 'Russian hackers'

By Gordon Corera
Security correspondent, BBC News

10 October 2016 | Technology

Share

TV5MONDE

GETTY IMAGES

TV5Monde's TV station, website and social media accounts were all hit in April 2015

A powerful cyber-attack came close to destroying a French TV network, its director-general has told the BBC.

時期　2015年4月8日

場所　フランス　TV5MONDE
(テレビ会社)

事象　午後8時に放送している12チャンネル全てが停止。翌朝5時に1チャンネル復旧。翌朝には完全復旧。

同時に同社のフェイスブック等もハッキングされる。

http://www.bbc.com/news/technology-37590375

44

一般家庭に対する攻撃

フィンランド

boingboing / ANDREA JAMES / 8:20 AM FRI DEC 2, 2016

DDoS attack on Finnish automated buildings disabled heating controls

When the heat goes out during Finnish winter, it's a matter of life and death, so when two automated buildings controlled by Valtia systems suffered DDoS attacks that shut off the heat, Finns were understandably alarmed about the new threat.
Via Metropolitan.fi

時期　2016年10月頃(詳細不明)

場所　フィンランド　ラッペーンランタ

事象　自動制御されている建物少なくとも二棟のヒーティングシステムが停止。

原因　遠隔監視・制御しているValtia社のDNSサーバーがDDOS攻撃をうけたため。

同時期の気温は氷点下のため、人的被害の出る可能性もあった。

http://boingboing.net/2016/12/02/ddos-attack-on-finnish-automat.html

45

ホテルのシステムに対する攻撃

オーストリア

2017年01月31日 08時49分 更新

高級ホテルでランサムウェア被害、宿泊客を部屋から閉め出し

オーストリアの高級ホテルで電子キーシステムがランサムウェアに感染し、宿泊客が自分の部屋に入れなくなった。攻撃側は、ビットコインで1500ユーロの身代金を要求していた。

[鈴木聖子，ITmedia]

"現代の魔法使い"落合陽一氏が語るビジネスのデジタル化
富士通の最新オールフラッシュアレイは速いだけではない？

オーストリアの高級ホテルで客室のカードキーを発行するシステムなどがランサムウェアに感染し、宿泊客が部屋から閉め出される事件が起きた。欧州の英語ニュースサイト「The Local Europe」が1月28日付で伝えた。

オーストリアの4つ星ホテル「Romantik Seehotel Jaegerwirt」（公式Webページより）

記事によると、オーストリアの4つ星ホテルRomantik Seehotel Jaegerwirtで電子キーシステムがランサムウェアに感染した。同ホテルがサイバー攻撃を受けたのは今回が3度目だったという。

客室の扉はカード式のキーを使って施錠と開錠を行う仕組みだったが、サイバー攻撃に遭ってこのカードキーのシステムがダウンしたため、宿泊客は自分の部屋に入れなくなった。新しいカードキーのプログラムもできなくなったという。

http://www.itmedia.co.jp/enterprise/articles/1701/31/news068.html

46

セキュリティベンダの監視システムの脆弱性
OSの脆弱性をついたサイバー攻撃は共通
ハードウェアの脆弱性は、コンピュータ製品全体に及ぶ
サイバー攻撃をビジネスにしている集団が増えている

共通

リモートサポートシステムは、リモート監視することで便利になることは考えても、ウイルスはリモートサポートシステムだから遠慮しようとはならない。
セキュリティ監視システムに脆弱性がある訳ないと勝手に思い込んでいるところがあるが、セキュリティ監視システムを利用して、制御システムをハッキングできるし、マルウェアが侵入できることについては思考停止している。

47

日本

SKY SEAの脆弱性：CVE-2016-7836

- IT資産セキュリティ管理サービスを提供しているSKY SEAに、脆弱性があることが2016年12月21日に報告アップされ、それ以降3回の脆弱性報告がなされた。

出典元：CVEサイト

48

WannaCryが大流行　150ヵ国、25万件以上／日本でも6000台以上に感染

2017年4月からWannaCryが、世界中で大流行した。

- 特に英国の複数の病院のコンピュータシステムがWanna Cryの被害によってロックされ、ネットワークでのオンライン接続を遮断。外来患者の予約、診断、手術をキャンセルする事態となった。
- 一部の病院においては電カシステムにも感染し、停電、透析医療もできなくなった。
- サイバー攻撃手法は、NSAから盗まれたWindowsの脆弱性情報「Microsoft Windows SMB サーバのセキュリティ上の脆弱性 MS17-010」を悪用して作られており、対策の方法が無かった。
- WannaCryに感染すると、コンピュータ上にある170種類以上のデータファイルを読み取りが出来ない形で暗号化します。暗号化されたファイルは「a.jpg.WNCRY」といったように.WNCRYという文字がファイル名の末尾に追加されます。
- 「Killスイッチのドメインアクセス」でWannaCryの活動が停止することはたまたま見つかった。
- パッチ対応で対策可能

対象となるOS

- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT 8.1
- Windows 10
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

49

WannaCry検体について

- WannaCry検体においては、インターネットとのHTTP通信を行う際、機器に設定されているプロキシサーバ設定は利用せず、インターネットと直接通信を行います。この為、**WannaCryに感染した機器が存在するかを確認するには、プロキシサーバのログではなく、DNSサーバのクエリログ、Firewallのログなどを確認する必要があります。**
- **DNSサーバのクエリログを取得している場合は、ウイルス対策ソフトベンダなどから報告されているWannaCryに関連するドメイン名がログに記録されていないか確認してください。**
- また、WannaCryは445/tcpポートを利用し、組織内部だけでなくインターネット上のホストにも接続を試みます。**Firewallのログなどで、組織内からインターネット上のランダムなIPアドレスに対する、445/tcp接続が記録されていないかも確認してください。**

50

Killスイッチの効果の限界

- WannaCryに関するセキュリティ各社の解析結果では、Killスイッチと呼ばれるドメインへのアクセスが成功した場合、WannaCryが動作を停止することが報告されています。当社の検証結果においても、Killスイッチのドメインへ HTTPアクセスが成功した場合は、WannaCryの動作が停止することを確認しています。しかし、実行ファイルなどはそのまま感染機器に残る形となります。
- この為、ファイル暗号化などの被害が発生していない場合でも、WannaCryに関連したファイルがそのまま残っている可能性がありますのでご注意ください。
- なお、**既にKillスイッチが含まれないWannaCryの亜種が確認されています。**この場合は、HTTPアクセスの有無によらずランサムウェアが実行されてしまいます。

51

WannaCryの追跡

- WannaCryはSMB通信（445/tcp）を利用し、横展開を行う特徴があります。この為、感染機器が発見された場合、感染元となった機器も隔離する必要があります。
- WannaCry検体においては、機器A（感染元） → 機器B（感染先）という横展開が行われた場合、機器B（感染先）のセキュリティログには、**ログオン成功（ID 4624）・ログオン失敗（ID 4625）のいずれも記録がされないことを確認しています。**
- また、**機器A（感染元）のセキュリティログには、機器B（感染先）に対するログオンの試行を示すログ（ID 4648）も記録されません。**
- 機器B（感染先）のセキュリティログ（ログオン関連イベント）から機器A（感染元）を追跡することは困難なため、通信ログから追跡を行うか、別途ウイルス対策ソフトやパーソナルファイアーウォールのログなどに、通信の記録が残っていないかを確認します。
- 組織内の機器において、機器B（感染先）から機器A（感染元）の追跡を可能とするログが取得されていない場合は、この機会に取得することを検討してください。
- 例えば、マイクロソフト社が提供しているSysmonツール（https://technet.microsoft.com/ja-jp/sysinternals/bb545027.aspx）を導入している環境では、Sysmonのログから445/tcp通信を追跡することが可能です。

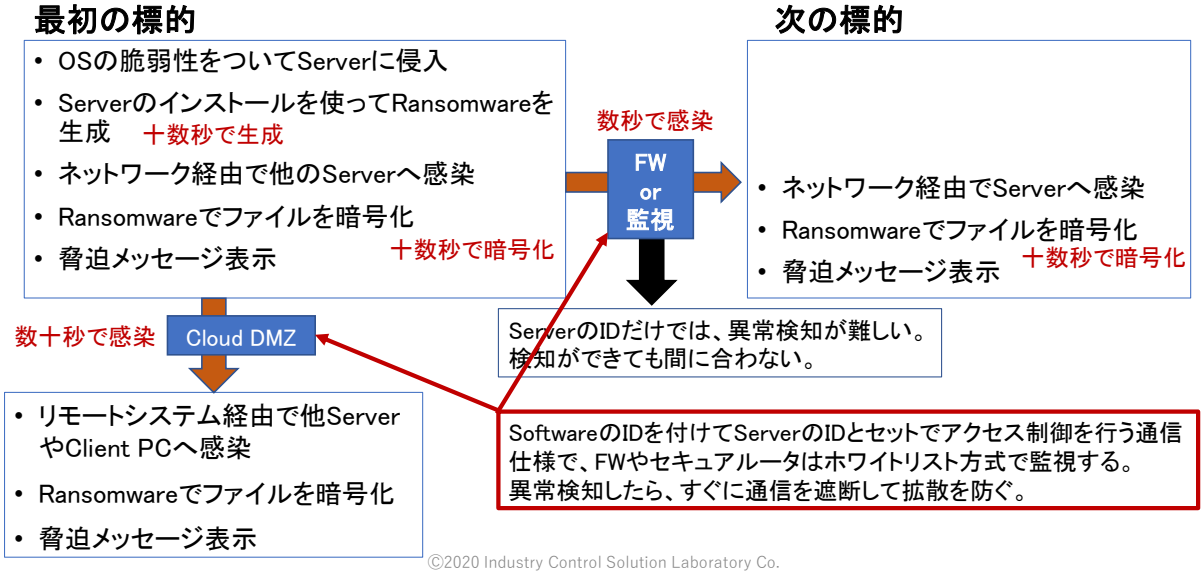
52

スキャン時の注意

- WannaCryが感染時に作成する既知のファイル名を、資産管理ツールやEDR製品などを利用してスキャンすることで感染機器を発見できる場合があります。
- WannaCryに感染した場合、サービスのインストールが発生することから、イベントログ（システム）に、イベントID 7045でサービスのインストールが記録されている場合があります。（例：サービス名: Microsoft Security Center (2.0) Service）
  また、各機器上でセキュリティログにイベントID 4688を取得するように設定している場合は、イベントID 4688のレコード内で記録されているプロセス名に、WannaCryに関連したプログラムの実行（C:¥WINDOWS¥mssecsvc.exeなど）が記録されていないかを確認する方法もあります。イベントID 4688はデフォルトでは記録されない為、設定されていない組織は設定変更を検討してください。
  Sysmonツールを導入している環境であれば、Sysmonのログからプロセス実行の履歴を確認することも可能です。

53

WannaCryの感染力



54

WannaCry対策

- 制御セキュリティ対策
  - セグメント／ゾーン設計の境界にホワイトリスト方式のFair Wall設置
  - インシデント検知で通信自動遮断
  - 汚染範囲を特定し、洗浄、回復
  - 被害を受けた後の回復のためのデータバックアップ
- 人材育成
  - 社員へのセキュリティ教育
  - 制御セキュリティ技術者を育てる
- 脆弱性識別管理
  - 使用設備機器の脆弱性識別情報管理
  - 保管交換部品の脆弱性識別情報管理

- 計画的なセキュリティメンテナンス
  - 最新情報入手で亜種版情報や対策情報などを確認
  - セキュリティ監視システムのアップデート管理
  - 定期的に脆弱性有り無し検証
  - サイバー攻撃による被害の検証
  - 事故発生を想定した訓練
- パートナー企業への協力依頼
  - サイバー攻撃に強い装置・機械・ロボットの開発
  - 脆弱性識別情報共有
  - 脆弱性識別検証テストツール整備
  - ペネトレーションテスト実施

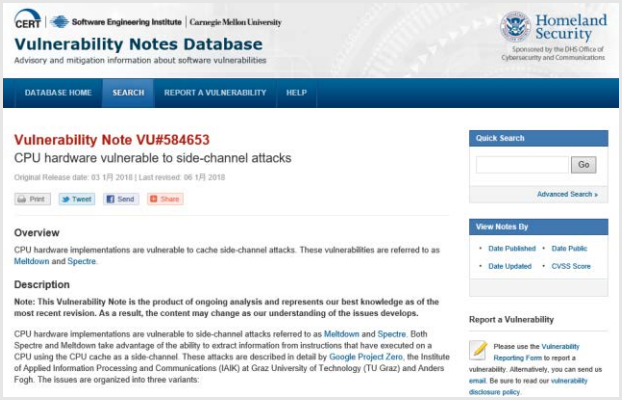
55

CERT情報：Vulnerability Note VU#584653

ハードウェアCPUの脆弱性

2018年1月3日情報公開

- ·Variant 1 (CVE-2017-5753, Specter): Bounds check bypass
- ·Variant 2 (CVE-2017-5715, also Specter): Branch target injection
- ·Variant 3 (CVE-2017-5754, Meltdown): Rogue data cache load, memory access permission check performe after kernel memory read



https://www.kb.cert.org/vuls/id/584653

56

ここまでのまとめ

サイバー攻撃の手法が変わると対策を見直す必要がある。

ファイヤーウォールやプロキシ監視では検知できないスクリプトタイプのマルウェアや暗号化されたマルウェアが2014年以降増えている。

システム内のServerでマルウェアに成長することでインシデント検知場所と対策技術が以前と異なってくる。

制御製品を支配下に置いたり、コントローラ内部を攻撃するマルウェアが登場していることで、サイバー攻撃に強い制御製品であることが必要となっている。

対策技術を学んで、安全なシステムを確保しよう。

注：IEC62443もISA Secure認証もガイドラインも2018年は更新しています。

57

制御システムを標的にしたサイバー攻撃事例

- **サイバー攻撃手法も高度技術を使用しており、組織的サイバー攻撃兵器としても開発し、取引されている。**
- **サイバー攻撃対策を考えるには、攻撃対象、攻撃武器、侵入経路、攻撃内容、被害状況などの具体的サイバーリスクアセスメントが必要となっている。**
- **アンチウイルスソフトやファイヤーウォールで検知できないスクリプトタイプや暗号化マルウェアが急増**

	2010	2014	2014	2015/2016	2016.8～	2017.12
発生場所	イラン	ドイツ	韓国	ウクライナ	イラン	中近東
攻撃対象	核燃料施設	製鉄所	原子力発電所	電力変電所	製油所 天然ガス基地など	プラント
攻撃武器	Stuxnet	トロイの木馬	外部操作を可能にしたマルウェア	スピアフィッシングメールで感染 Black Energy／Industroyer	不明 サイバー攻撃ではないかと疑われている	Triton
侵入経路	USBメモリ	電子メールの添付ファイル	インターネットからの侵入	インターネットからの侵入	不明	リモートサービス
攻撃内容	遠心分離機への過剰な負荷	溶鉱炉の異常停止	マルウェアを使った遠隔操作	UPSを攻撃	不明	SISシステムのEWSからSISコントローラへ
被害状況	遠心分離機を破壊	生産設備の損傷	実被害なし	広いエリアで6時間停電	石油貯蔵タンク爆発火災（10月）	プラント緊急停止

58

サイバーセキュリティ対策の重要性

国内で起きている事故

自動車工場	•現場サポート業者が持ち込んだPCから工場内ネットワークにマルウェア侵入。PC50台に感染 •10日間操業停止⇒1200台出荷できず：年間売り上げから30億円以上が無くなる
半導体製造工場	•現場装置のアップデート作業で持ち込んだデバイスから工場内ネットワークにマルウェア侵入 •1か月間操業停止⇒年間売り上げから340億円が無くなる。
石油精製工場	•MESのネットワークにマルウェアが侵入 •2週間操業停止⇒2週間分の出荷減
工作機械が並ぶ精密機械製造工場	•マルウェアが工場内ネットワークに侵入 •セキュア改善するまでは、年に数回数週間ずつ操業停止
ゴミ焼却場	•従業員が持ち込んだ携帯電話の充電中にインターネットと接続。マルウェアが侵入 •6日間操業停止
高速道路管制システム	•インターネットにつながるPCからマルウェアが侵入し、USBメモリ経由で管制システムに感染 •設備総入れ替え

サイバーインシデントが発生する都度に出てくる損失

何が問題か

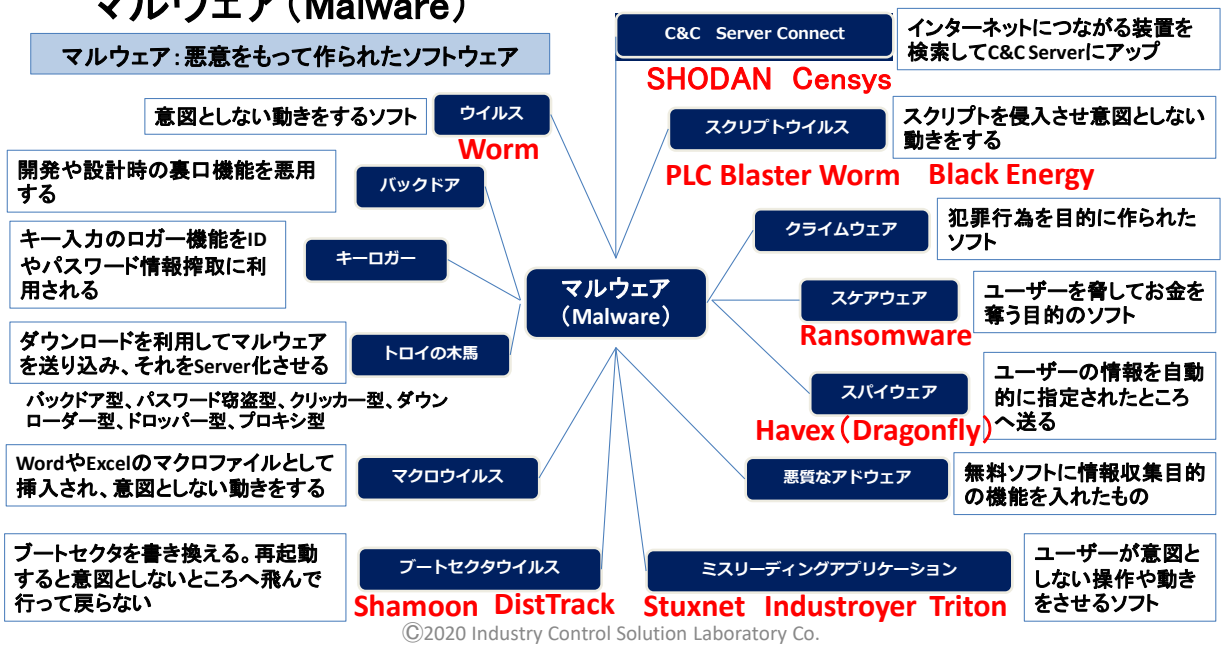
- 年間計画している売り上げが減る。
  - 操業停止している期間の売り上げが無くなる。
- 復旧作業の為にコスト増
  - 緊急対応コスト
    - マルウェア判定：専門家に依頼
    - 洗浄作業：
    - 回復作業：ベンダを呼びだして作業依頼
  - セキュア改善対策コスト
    - インシデント検知システム
    - セグメント設計改造
    - ゾーン設計改造
    - インシデント対応トレーニング

いずれにしろ、やることになる投資

59

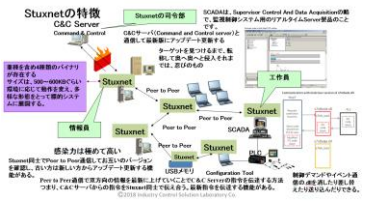
マルウェア（Malware）

マルウェア：悪意をもって作られたソフトウェア



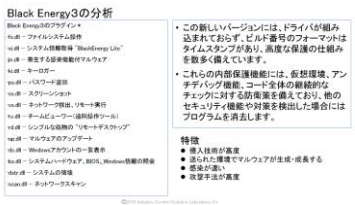
60

Stuxnet：2010年～



標的に制御システムを研究して作られたマルウェア（制御コードを利用）
容易に感染
高度なステルス性

Black Energy：2015年～



サイバーディフェンス級の攻撃ツールを装備したマルウェア

Industroyer：2016年～

リモートServerを利用したサイバー攻撃

制御システムを標的にしたサイバー攻撃

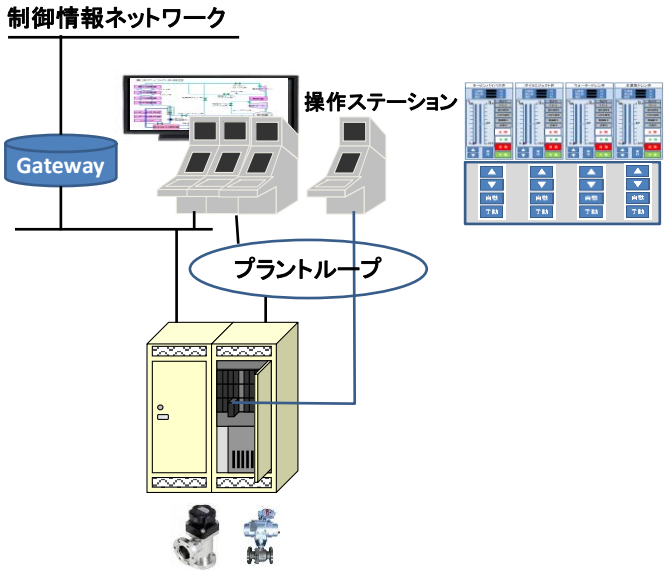
Serverから制御コントローラに.dllコードを送り、コントローラを支配下にするマルウェア

61

DCSやPLCを標的にしたStuxnet攻撃の場合

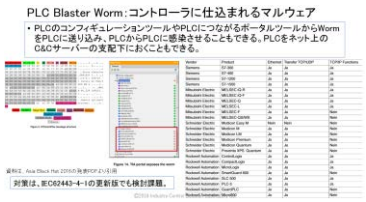
.dllを操作されて何が起きるか
- 警報が消える
- 警報の洪水
- アナログ信号が勝手に動く
- 操作端を操作される
- 自動が手動に移動される
- 制御モードが変わる

Stuxnet攻撃の特徴
- .dllは正規の通信プロトコルなので、通信エラーが出ない
- ステルス機能が強いので起動時のハッシュ検知しかないがハッシュ検知機能をいれると制御に支障が出る



62

PLC Blaster Worm：2016年～

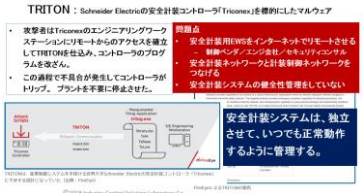


制御コントローラを研究し、ポータル通信を利用したマルウェア

WanaCry／Goldeneye／Petya／Bad Rabbit
＋Ransomware：2017年～

NSAからWindowsの脆弱性情報を盗み出して作ったマルウェア
リモートサポートシステム経由で拡散
ネットワークで接続状態での撲滅が難しい。

Triton：2017年～



安全計装SISのリモートサポートシステムを利用したサイバー攻撃
欧米の制御ベンダの総合サポートソリューションがリスクを高めている。

制御システムを標的にしたサイバー攻撃

制御製品に侵入して中を操作するマルウェア

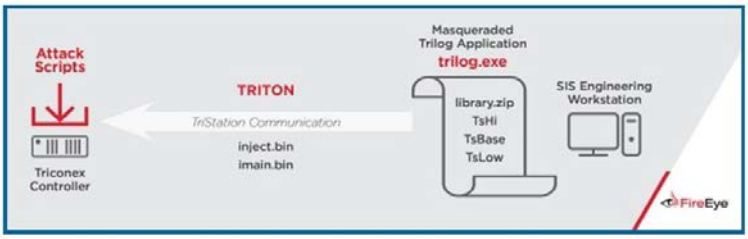
63

TRITON：Schneider Electricの安全計装コントローラ「Triconex」を標的にしたマルウェア

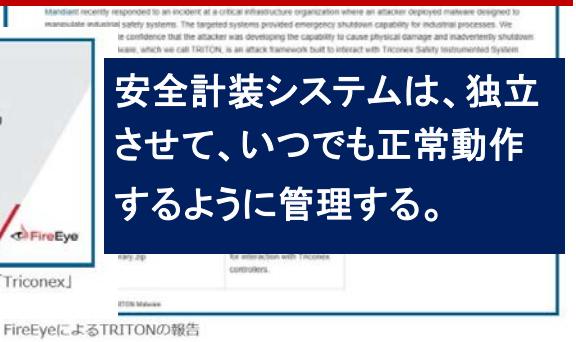
- 攻撃者はTriconexのエンジニアリングワークステーションにリモートからのアクセスを確立してTRITONを仕込み、コントローラのプログラムを改ざん。
- この過程で不具合が発生してコントローラがトリップ。 プラントを不要に停止させた。

問題点

- 安全計装用EWSをインターネットでリモートさせる
  - 制御ベンダ／エンジ会社／セキュリティコンサル
- 安全計装ネットワークと計装制御ネットワークをつなげる
- 安全計装システムの健全性管理をしていない



TRITONは、産業制御システムを手掛ける世界大手Schneider Electricの安全計装コントローラ「Triconex」に干渉する設計になっていた（出典：FireEye）



FireEyeによるTRITONの報告

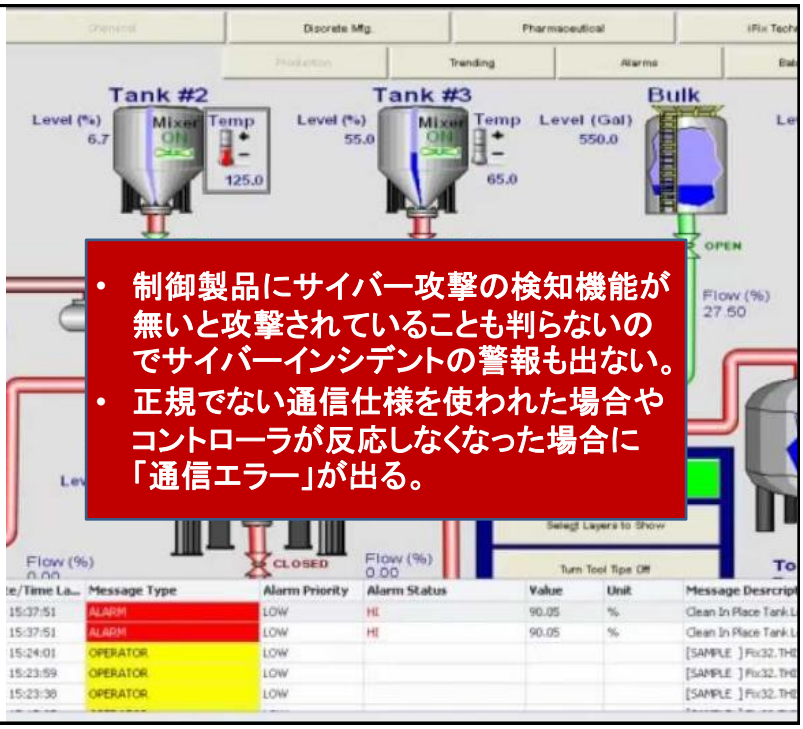
安全計装システムは、独立させて、いつでも正常動作するように管理する。

64

PLC／DCS Blaster Worm

起き得る現象

- いきなりコントローラがトリップ（機能停止）
  - 自動が手動に移動される
  - 手動操作も不能
- スレーブモジュールの異常
  - アナログ信号が激変
  - 検出端異常
  - 操作端異常
- オペレーション不能
  - オペレーションが乗っ取られる
  - 制御モードが勝手に変わる
  - 定常／非定常では出ないパターンの警報が出る
  - 警報が出ても正しいとは限らない
  - 警報が消える
  - レシピが変わる
  - いきなり停止動作



- 制御製品にサイバー攻撃の検知機能が無いと攻撃されていることも判らないのでサイバーインシデントの警報も出ない。
- 正規でない通信仕様を使われた場合やコントローラが反応しなくなった場合に「通信エラー」が出る。

65

制御システムの攻撃方法

- 定常時／非定常時の操作ミス（誤判断・誤操作）を誘発させる攻撃
  - 制御ネットワークを使えなくする
    - ネットワークのServerかPCからDOS攻撃を加えて通信エラーを起こす
  - 現場で発生していないアラームを発報させる
    - DCSやSCADAの監視制御のアラームデータに新しい警報を追加
    - 過去起きたアラームを再度表示
  - 現場で発生しているアラームを監視画面に表示させない
    - アラームデータが上がってきてもデータベースに書き込まない
    - アラームデータを消去
- 制御システムを直接攻撃
  - SCADA／DCSの制御動作をスローダウンもしくは機能停止させる
    - SCADA ServerやDCSのワークステーションにWormを送り込みフル稼働させる：Worm
    - 使用しているファイルを暗号化する：Ransomware
    - 制御データがSCADAに上がってこなくする：通信ドライバを消去、データベースを消去
  - 制御コントローラを操作する
    - コントローラのレジスタを操作する：PLC Blaster Worm
    - コントローラのファンクションを書き換える：PLC Blaster Worm
  - 実際にメカニックストレスを与える
    - 制御コントローラにストレスデマンドを送り込む：Stuxnet

- 操作不能状態
- 現場は正常だけど異常に見せる
- 現場は異常だけど操作は正常に見せる
- 制御不能状態
- 制御乗っ取り
- メカニック破壊

66

生産工場の安全セキュリティ対策
製造システムの制御システムセキュリティ対策
製造している製品の制御セキュリティ対策
システムインテグレート環境のセキュリティ対策
サプライチェーンの脆弱性識別セキュリティ品質情報
サイバーセキュリティ対策の人材育成計画

具体的対策は、できていますか？

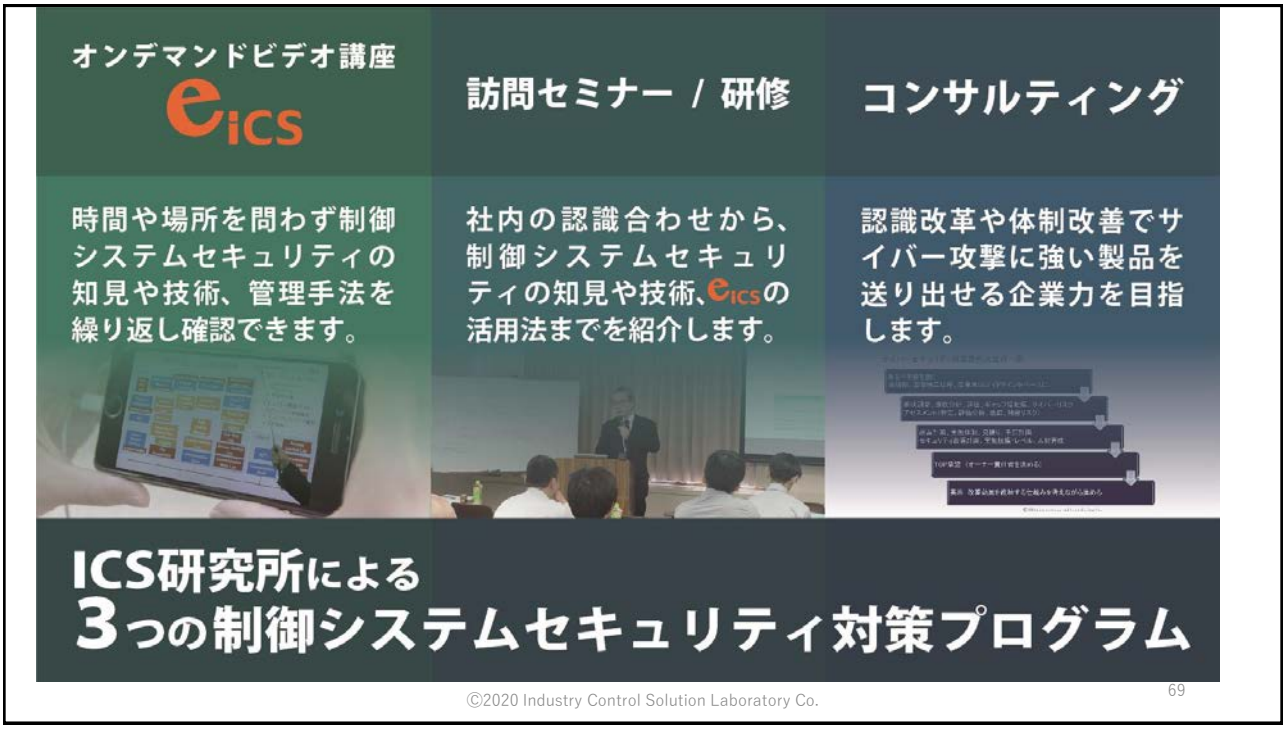
内閣サイバーセキュリティセンターNISC「重要インフラの情報セキュリティに係わる第4次行動計画」など
経済産業省「サイバーセキュリティ経営ガイドラインV2.0」
各産業別サイバーセキュリティガイドライン
国際標準規格／国際認証／NIST／NRC／ICS-CERT
制御システムセキュリティ／制御セキュリティ／安全セキュリティ／ISMS／CSMS
リスクアセスメント／ネットワーク設計／制御システム設計／装置・機械設計／制御システム仕様／制御製品仕様
制御システムセキュリティ設計指針（規範）、インシデント検知・警報設計、緊急時対応マニュアル、
設備脆弱性識別情報管理指針（規範）など

67

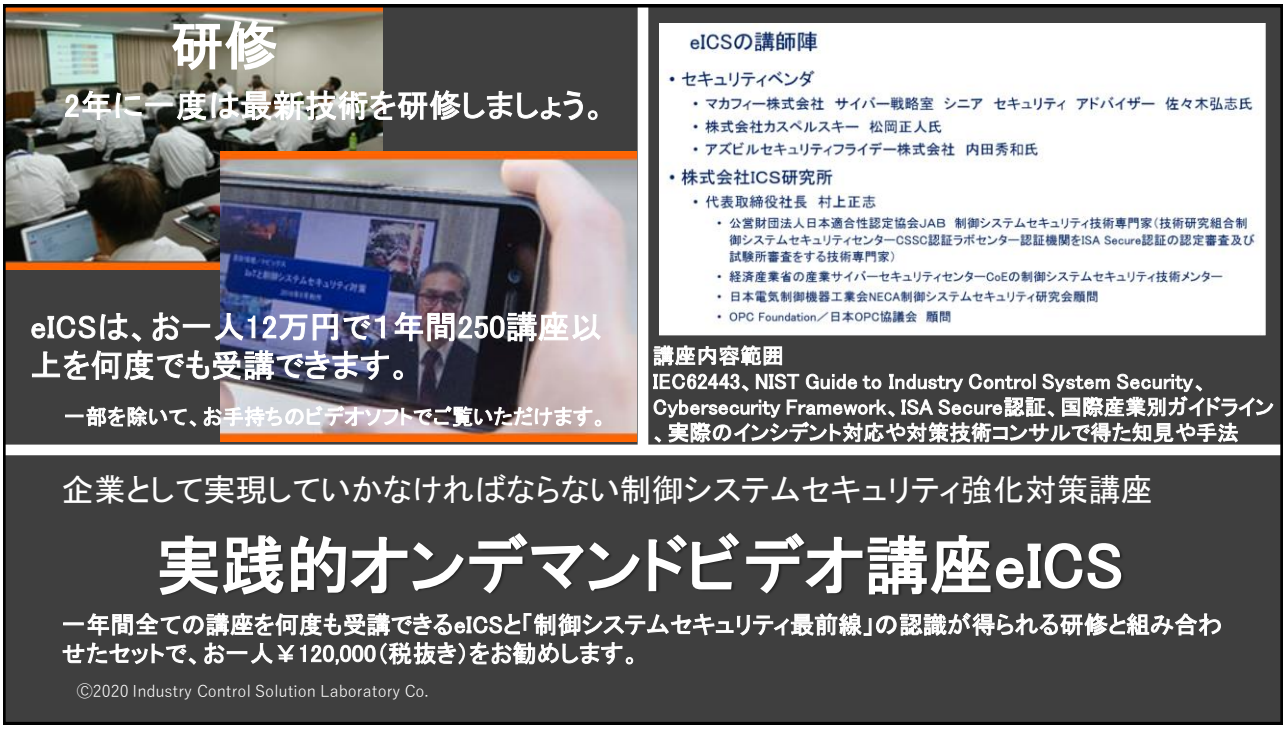
自社の生産工場の制御システムに適合した制御システムセキュリティ対策規範関係のドキュメントは、できていますか？

- 生産工場の制御システムセキュリティ対策基本方針（規範）
  - サイバーセキュリティ経営ガイドライン、産業別サイバーセキュリティガイドライン
  - ISMS（ISO27000）、CSMS（IEC62443-2）、制御セキュリティ（IEC62443-3,-4）、安全セキュリティ（IEC63069）
  - 出入り業者（工事業者含む）のコンピュータ製品／工具（PCやデバイス含む）のセキュリティ管理基準
- 制御系システムのセキュリティ対策要領（規範）
  - 制御システム利用におけるセキュリティ対策要領
  - 制御システム設計における対策要領
  - 制御系セキュリティ緊急時対応マニュアル
  - 設備管理における脆弱性識別に基づく管理要領
  - 制御システムエンジニアリング、制御装置、機械、発注におけるセキュリティ対策要綱
  - 受け入れ検査（立会試験）要綱

68


オンデマンドビデオ講座
eICS
時間や場所を問わず制御システムセキュリティの知見や技術、管理手法を繰り返し確認できます。
訪問セミナー / 研修
社内の認識合わせから、制御システムセキュリティの知見や技術、eICSの活用法までを紹介します。
コンサルティング
認識改革や体制改善でサイバー攻撃に強い製品を送り出せる企業力を目指します。
ICS研究所による
3つの制御システムセキュリティ対策プログラム
©2020 Industry Control Solution Laboratory Co.
69

69


研修
2年に一度は最新技術を研修しましょう。
eICSは、お一人12万円で1年間250講座以上を何度でも受講できます。
一部を除いて、お手持ちのビデオソフトでご覧いただけます。
eICSの講師陣
• セキュリティベンダ
• マカフィー株式会社 サイバー戦略室 シニア セキュリティ アドバイザー 佐々木弘志氏
• 株式会社カスペルスキー 松岡正人氏
• アズビルセキュリティフライデー株式会社 内田秀和氏
• 株式会社ICS研究所
• 代表取締役社長 村上正志
• 公営財団法人日本適合性認定協会JAB 制御システムセキュリティ技術専門家（技術研究組合制御システムセキュリティセンターCSSC認証ラボセンター認証機関をISA Secure認証の認定審査及び試験所審査をする技術専門家）
• 経済産業省の産業サイバーセキュリティセンターCoEの制御システムセキュリティ技術メンター
• 日本電気制御機器工業会NECA制御システムセキュリティ研究会顧問
• OPC Foundation／日本OPC協議会 顧問
講座内容範囲
IEC62443、NIST Guide to Industry Control System Security、Cybersecurity Framework、ISA Secure認証、国際産業別ガイドライン、実際のインシデント対応や対策技術コンサルで得た知見や手法
企業として実現していかなければならない制御システムセキュリティ強化対策講座
実践的オンデマンドビデオ講座eICS
一年間全ての講座を何度も受講できるeICSと「制御システムセキュリティ最前線」の認識が得られる研修と組み合わせたセットで、お一人￥120,000（税抜き）をお勧めします。
©2020 Industry Control Solution Laboratory Co.

70

eICSの活用と効果

eICSを受講しながら、

- **制御システム設計及び制御システム利用における規範作成**
- **業務系ネットワークと製造系ネットワークのセグメント設計防御技術**
- **セキュリティ監視システムの構築設計（SIEMの機能・性能仕様と使い方、アイソレート仕様）**
- **緊急時対応マニュアル作成**
- **被害最小にするゾーン設計**
- **インシデント検知設置及びインシデント警報設計**
- **OT現場従業員セキュリティルールと教育ビデオコンテンツ （ビデオ制作はICS研究所で対応）**
- **制御コントローラに求められる機能・性能仕様、脆弱性情報管理方法**
- **装置・機械発注仕様書のセキュリティ機能・性能仕様**
- **製品開発プロセスにおける脆弱性撲滅方法**
- **試験方案作成など**
- **セキュリティ評価ツール選択基準書作成**
- **サプライヤ企業のセキュリティ監査基準書作成**

などの実務を進める時に必要な知見を取り込んで成果を出している技術者が増えています。

71

サイバー攻撃の事例集

eICSのパンフレットや講座一覧及び見積もり、お問い合わせについては、
eICSのWebページより、ご用命ください。

https://www.ics-lab.com/e/

株式会社ICS研究所

72