安全・安定操業を脅かした
サイバー攻撃事例
10選

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（ICSCoE）

〔現場向け制御セキュリティ教育プロジェクト〕

本書では、近年国内外で発生した制御システムへのサイバー攻撃の中から、操業の安全・安心を大きく損なった

10 の事例を、影響の大きい順に紹介します。

サイバー攻撃がどのような影響を及ぼす可能性があるのかを
知っていただくために、事例の紹介に留まらず、
発生する可能性のある被害について解説しています。

制御システムは外部からの接続が制限されてるから サイバー攻撃は受けない？

いいえ、そんなことはありません。
2019年には、制御システムへのサイバー攻撃が前年比で20倍に増加したという調査結果が出るなど、制御システムを標的にしたサイバー攻撃が、近年急増しています。

このように、サイバー攻撃はIT分野に限った話や映画の世界の話ではなく、制御システムに対しても身近な脅威になっています。こうした状況において製造現場で働く方のセキュリティ意識の向上は、重要になってきています。

制御システムのセキュリティについて考える 第一歩として、本書をご活用ください。 ご安全に！

（出典）
IBM X-Force 脅威インテリジェンス・インデックス2020

こんな時に使って欲しい

- ✔ 新人配属時に配布
- ✔ 朝礼時に代表者が読み上げ
- ✔ ＫＹ活動（危険予知活動）

本書の読み方


攻撃事例 1.

社会インフラへの影響

電力

発生日：2015 年 12 月
発生場所：ウクライナ

Ukraine

概 要

従業員が不審メールを開封し PC がウイルス感染したことをきっかけに、制御ネットワークに侵入された。攻撃者に制御システムを不正操作され、真冬の最中、約 22 万 5 千の顧客に影響する停電が発生した。同時に、電話システムも攻撃されたため、顧客からの停電に関する問合せも妨害された。

こんな被害が起こる可能性も

安 全

ウクライナの 12月の平均最低気温はマイナス6度であり、極寒の中、停電中は住民たちは暖房を使うことができず、停電時間が長引けば死者が発生する。

品質・操業

電力の安定供給ができなくなることで、顧客や顧客のビジネスに影響を及ぼし、社会的信頼が失墜する。

【参考資料】
CISA(ISC Alert) :
Cyber-Attack Against Ukrainian Critical Infrastructure
https://ics-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01

06.

- ・いつ起きたか
- ・どこで起きたか

- ・何が起きたか

- ・安全、品質・操業にどんな影響が起こるか、可能性があるか

INDEX

社会インフラへの影響 5

電力
浄水場
ダム

操業停止および設備破損 9

核開発
鉄鋼メーカー

操業停止 12

石油化学
自動車メーカー
電機メーカー
半導体メーカー

情報漏えい 17

電力

対策例 19

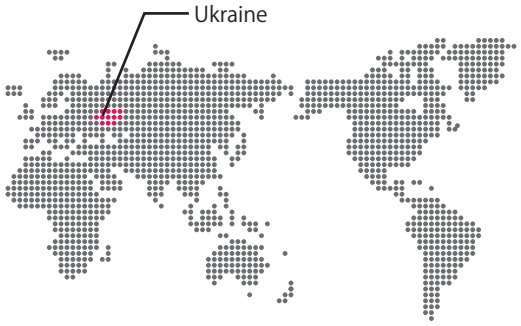
社会インフラへの影響

攻撃事例 1.

社会インフラへの影響

電力

発生日：2015 年 12 月
発生場所：ウクライナ



概 要

従業員が不審メールを開封し PC がウイルス感染したことをきっかけに、制御ネットワークに侵入された。攻撃者に制御システムを不正操作され、真冬の最中、約 22 万 5 千の顧客に影響する停電が発生した。同時に、電話システムも攻撃されたため、顧客からの停電に関する問合せも妨害された。

こんな被害が起こる可能性も

安 全

ウクライナの 12月の平均最低気温はマイナス6度であり、極寒の中、停電中は住民たちは暖房を使うことができず、停電時間が長引けば死者が発生する。

品質・操業

電力の安定供給ができなくなることで、顧客や顧客のビジネスに影響を及ぼし、社会的信頼が失墜する。

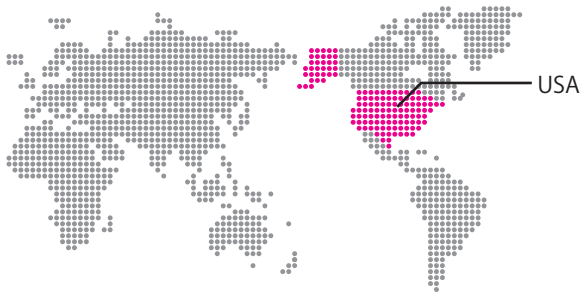
【参考資料】
CISA(ISC Alert)：
Cyber-Attack Against Ukrainian Critical Infrastructure
https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01

攻撃事例
2.

社会インフラへの影響

浄水場

発生日：2021 年 2 月
発生場所：アメリカ



概 要

攻撃者がアメリカにある浄水場の制御システムに対して外部より不正アクセスを実施した。その後、攻撃者は水処理に必要な薬品である水酸化ナトリウムの設定値を通常の 111 倍に変更した。オペレータは異常な値の変更にすぐ気がつき、設定値を元に戻した。

こんな被害が起こる可能性も

安 全

この浄水場より給水を受ける人数は約1万5千人とされており、高濃度の水酸化ナトリウムを飲むと口内、食道、胃などの粘膜を破壊するなど健康被害が出る。

品質・操業

浄水場の操業が停止すると約1万5千人に給水の影響が出る。

【参考資料】
CISA(ISC Alert)：
Compromise of U.S. Water Treatment Facility
https://us-cert.cisa.gov/ncas/alerts/aa21-042a
CNN.co.jp：
浄水システムに不正侵入、苛性ソーダ濃度１００倍に設定　米フロリダ州
https://www.cnn.co.jp/usa/35166249.html

攻撃事例 3.

社会インフラへの影響

ダム

発生日：2013 年 8 月～9 月
発生場所：アメリカ

概 要

攻撃者がアメリカにあるダムの制御システムに対して外部より不正アクセスを実施し、水門の状態と運用に関する情報を繰り返し入手していた。ダムの水門を遠隔操作することも可能だったが、この時はメンテナンスのため水門への接続が解除されていたことから、遠隔操作には至らなかった。

こんな被害が起こる可能性も

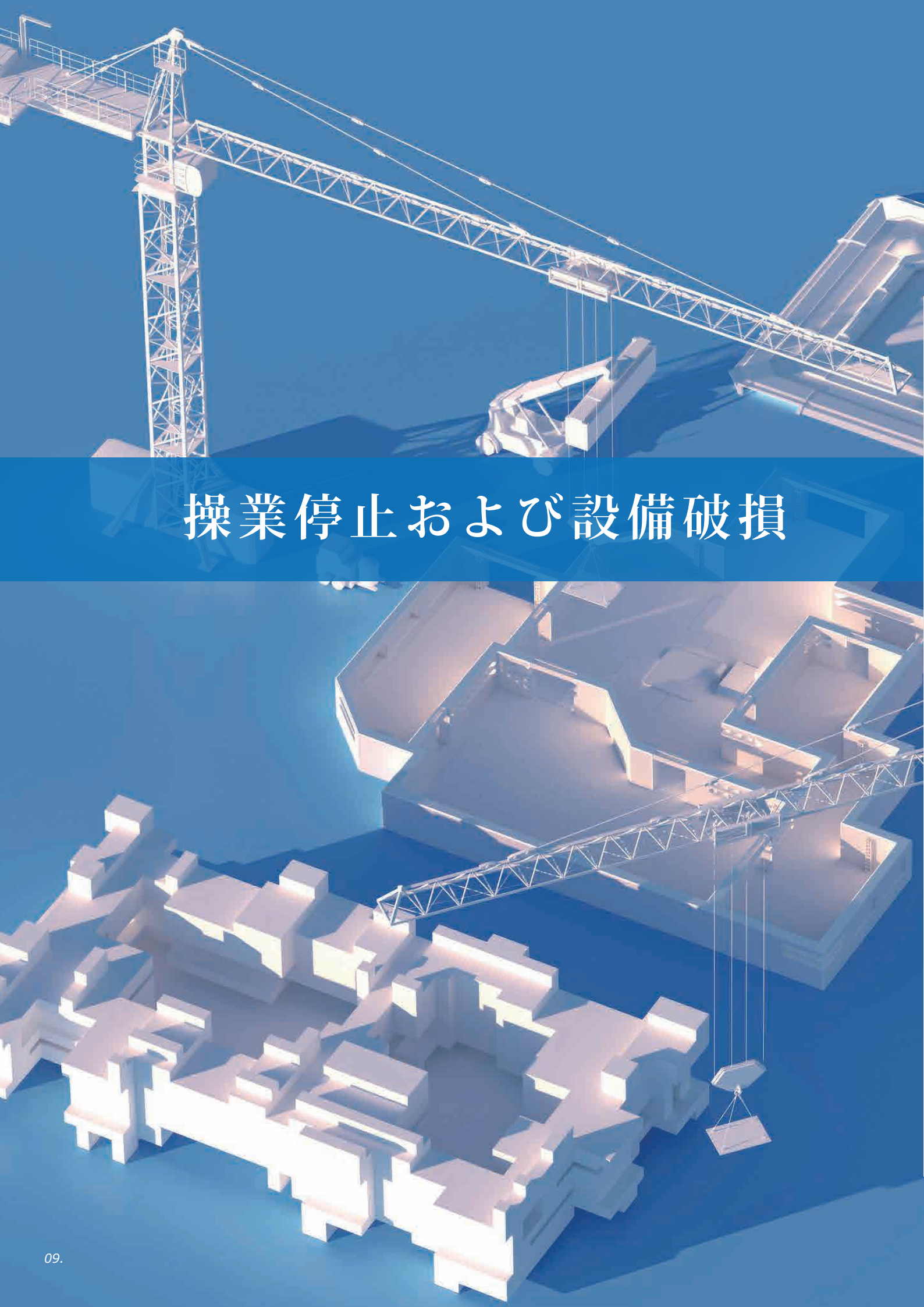
安 全

ダムの下流にある街が洪水に飲み込まれる可能性がある。住民の溺死、家屋の浸水・流出、汚水による感染症、電気や水道などのライフラインなどに影響が出る。

品質・操業

ダムの貯水が無くなることにより、発電、生活・工業・農業用水の供給が停止する。

【参考資料】
U.S. Department of Justice：
Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector
https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged
Itmedia エンタープライズ：
米司法省、大手銀行やダムへのサイバー攻撃でイラン人 7 人を訴追
https://www.itmedia.co.jp/enterprise/articles/1603/25/news068.html



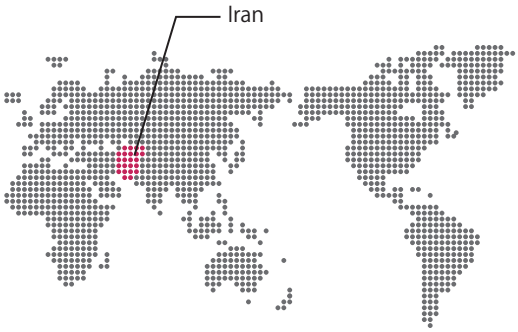
操業停止および設備破損

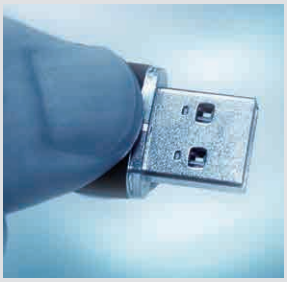
攻撃事例 4.

操業停止および設備破損

核開発

発生日：2009 年 6 月～2010 年 5 月
発生場所：イラン





概 要

ウイルス感染した PC によって、遠心分離機の制御システムの設定が改ざんされた。1 年以上にわたり改ざんに気がつかず、約 8,400 台中、約 1,000 台の遠心分離機が破損し、操業が一時停止した。ウイルスは USB メモリ経由で制御ネットワーク内に持ち込まれたと考えられている。

こんな被害が起こる可能性も

安 全

遠心分離機の破損により放射性物質が飛散し、健康被害が発生する。

品質・操業

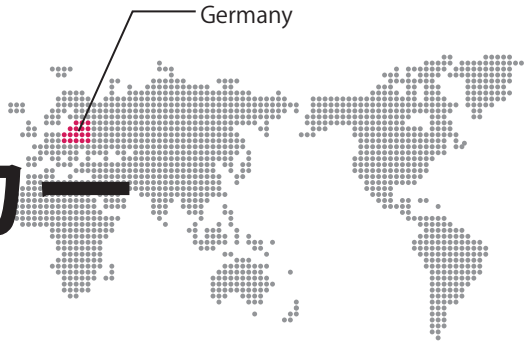
ウラン濃縮に必要な設備である遠心分離機が大量に破損することにより、核開発計画が大幅に遅延する。

【参考資料】
独立行政法人情報処理推進機構セキュリティセンター：
制御システム関連の サイバーインシデント事例 4
https://www.ipa.go.jp/files/000080701.pdf

攻撃事例 5.

操業停止および設備破損

鉄鋼メーカー



発生日：2014 年 12 月
発生場所：ドイツ

概 要

不審なメールを開いてしまった従業員の PC がウイルスに感染した。そこから制御ネットワークに侵入され、制御システムが乗っ取られた。オペレータは溶鉱炉の運転停止を試みるも正常に停止できず、溶鉱炉のシステムに甚大な被害が出た。

こんな被害が起こる可能性も

安 全

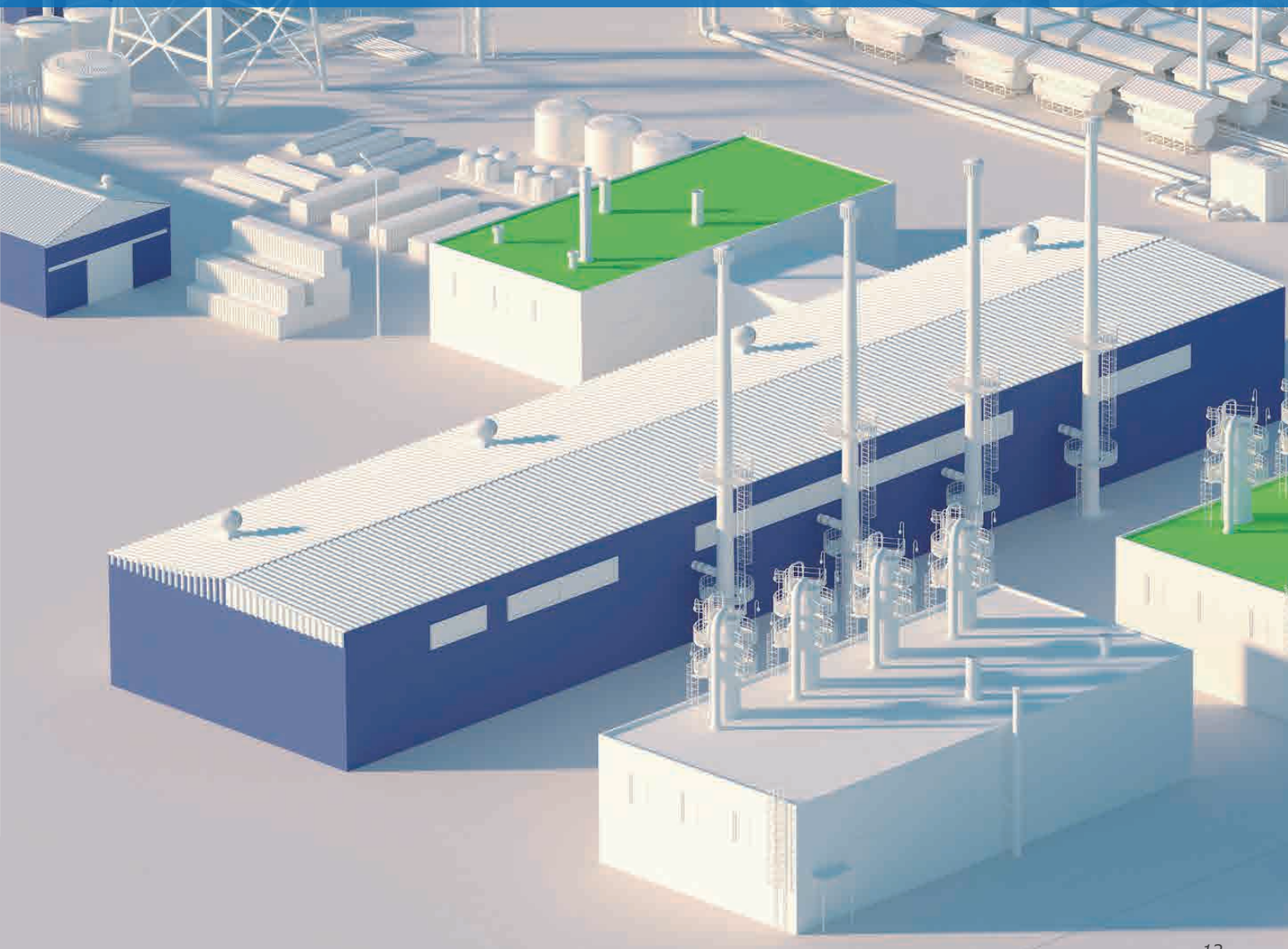
溶鉱炉の破損に繋がった場合、1,400度近い溶けた鉄が流れ出てしまい、付近の社員が重度の火傷を負う。最悪の場合、死者が発生する。

品質・操業

溶鉱炉システムの復旧期間、操業が停止する。製鉄工程の要となるシステムのため、生産機会損失による被害額は甚大となる。

【参考資料】
BSI：
Die Lage der IT-Sicherheit in Deutschland 2014 3.3.1
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

操業停止

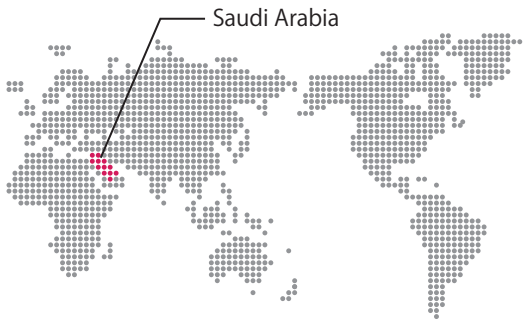


攻撃事例 6.

操業停止

石油化学

発生日：2017 年 12 月
発生場所：サウジアラビア



概 要

安全計装システム (SIS) を不正操作するために開発されたウイルスに感染し、SIS コントローラが不正に操作された。最終的に人命に関わるような事故は発生しなかったが、フェールセーフ機能が自動的に作動し、操業が一時停止する事態となった。

こんな被害が起こる可能性も

安 全

フェールセーフ機能が働かない、もしくはそのような機能が元々備わっていない場合、SISが動作せず、可燃性ガスの漏えいなどに気がつかず、爆発・炎上し、最悪の場合、死者が発生する。

品質・操業

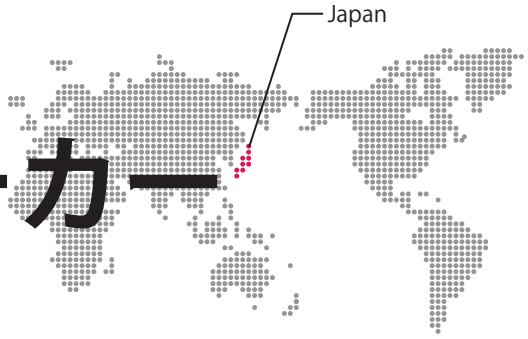
爆発・炎上した場合、プラントに甚大な被害が発生するため、復旧までに数ヶ月単位かかる。

【参考資料】
FIREEYE：
産業制御システム（ICS）への新たな攻撃フレームワーク「TRITON」が重要インフラの運用停止を誘発
https://www.fireeye.jp/blog/jp-threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

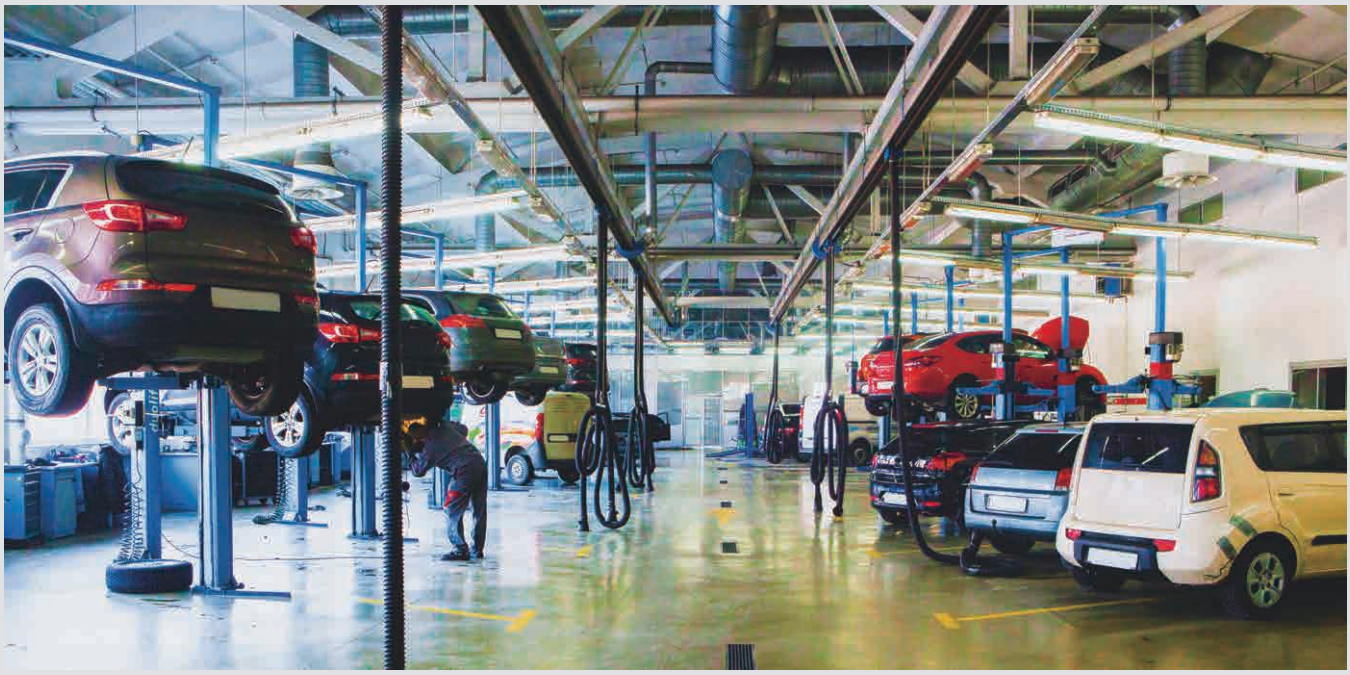
攻撃事例 7.

操業停止

自動車メーカー



発生日：2020 年 6 月
発生場所：日本



概 要

社内システムに感染したウイルスが国内外工場に拡大したことで、出荷停止や生産停止に追い込まれた。全工場の復旧まで約 4 日を要した。本攻撃では、この自動車会社に狙いを定めて作成されたウイルスが使用されたとされている。

こんな被害が起こる可能性も

安 全

製造過程の品質検査の結果を登録するシステムがウイルスに感染し、検査結果の改ざんに気がつかない場合、不具合品の自動車出荷に繋がり、不特定多数の人が危険に晒される。

品質・操業

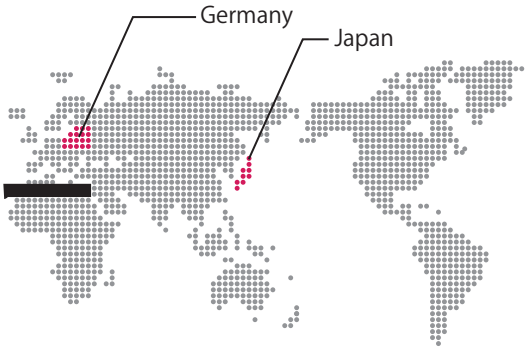
生産設備の制御システムにウイルスが感染し、制御不能になった場合、操業が停止する。

【参考資料】
NHK オンライン：
ホンダへのサイバー攻撃 社内ネット中枢を狙った新たな手口
https://www3.nhk.or.jp/news/html/20200615/k10012471271000.html
日経新聞：
ホンダ、サイバー攻撃で停止の全工場再開
https://www.nikkei.com/article/DGXMZO60280870S0A610C2EAF000/
日経 XTECH：
ホンダの社内ネットで大規模障害、「サイバー攻撃の可能性含め調査中」
https://xtech.nikkei.com/atcl/nxt/news/18/08065/

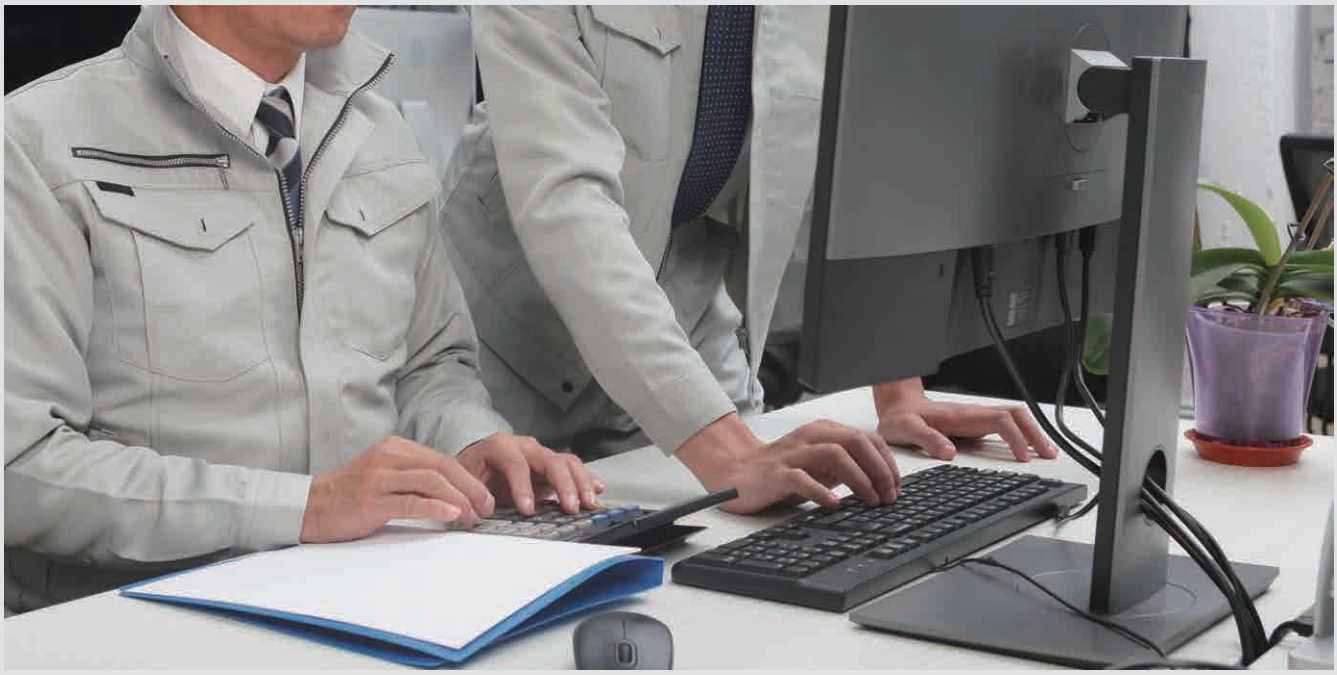
攻撃事例 8.

操業停止

電機メーカー



発生日：2017 年 5 月
発生場所：ドイツ・日本



概 要

社内の PC がウイルスに感染し、工場のシステムが一時停止するなどの被害を受けた。ウイルスはドイツにあるグループ会社の検査機器に何らかの原因で感染し、そこからネットワーク経由で世界各地の事業所の PC に広まった。

こんな被害が起こる可能性も

安 全

安全計装、HMIなどの重要制御機器に感染した場合、制御機器が意図しない動作をして事故が発生する。

品質・操業

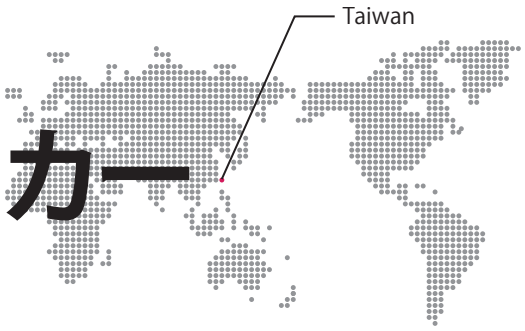
ネットワーク経由でグループ会社全てのPCが感染した場合、復旧まで長期の操業停止に陥ってしまう。

【参考資料】
株式会社 日立製作所：
情報セキュリティ報告書 2018
https://www.hitachi.co.jp/hirt/publications/securityreport/securityreport2018.pdf
日経 XTECH：
日立のセキュリティ担当、WannaCry 感染の反省を語る
https://xtech.nikkei.com/it/atcl/news/17/112102710/

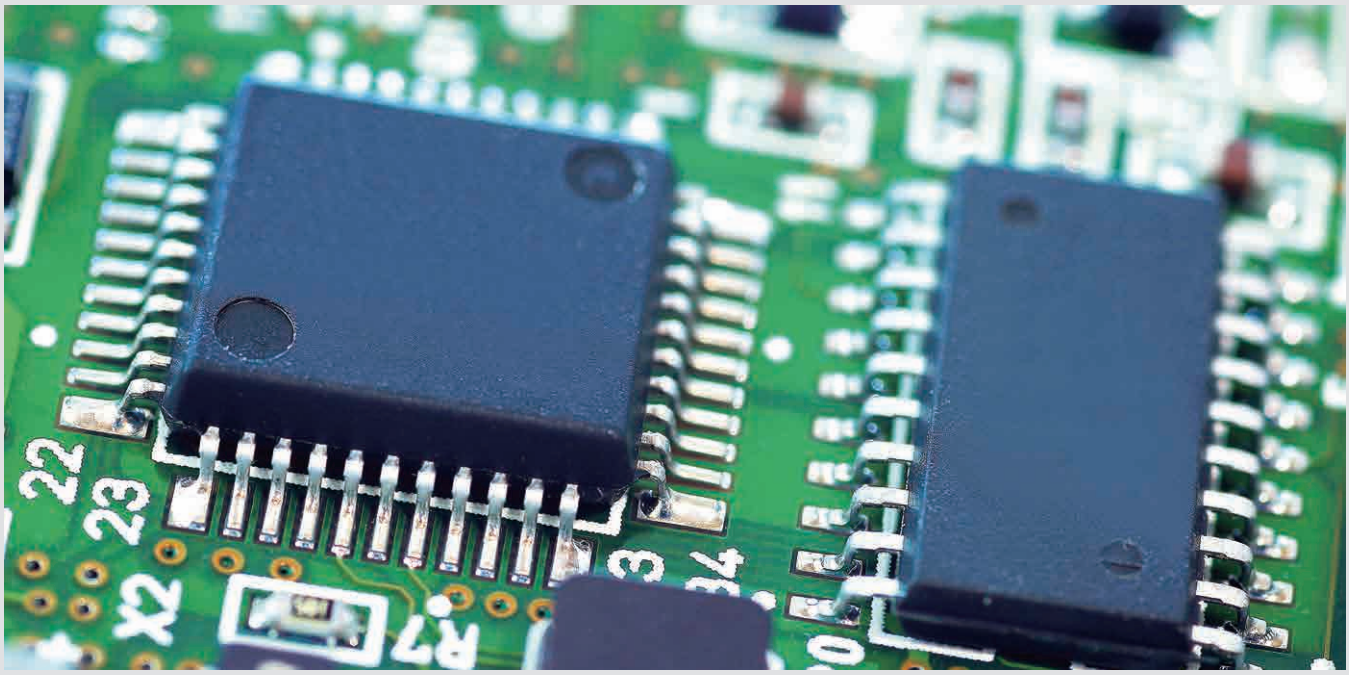
攻撃事例
9.

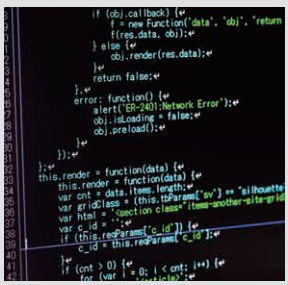
操業停止

半導体メーカー



発生日：2018 年 8 月
発生場所：台湾





概 要

製造用ツールが入った新規 PC がウイルスに感染しており、気がつかないまま制御ネットワークに接続したところ、3 拠点 1 万台以上の PC に感染が広がった。
その結果、各 PC のデータが暗号化されて開けなくなり、生産が停止した。

こんな被害が起こる可能性も

安 全

ウイルスが制御内容を変更するものだった場合、バルブ不正操作により特殊ガスが漏えいすることで、爆発・火災に繋がり、最悪の場合、死者が発生する。

品質・操業

生産が停止すると、自動車・鉄道・家電製造メーカー等、半導体ユーザである各業界への影響が大きい。

【参考資料】
TSMC：
https://pr.tsmc.com/japanese/news/1969
日経新聞：
台湾 TSMC、半導体工場がウイルス感染　生産一時停止
https://www.nikkei.com/article/DGXMZO33846620W8A800C1FFE000/
REUTERS：
Apple chip supplier TSMC resumes production after WannaCry attack
https://www.reuters.com/article/taiwan-tsmc-virus/apple-chip-supplier-tsmc-resumes-production-after-wannacry-attack-idINKBN1KR0B9?edition-redirect=in

情報漏えい

攻撃事例 10.

情報漏えい
電力

発生日：2012 年～2014 年
発生場所：ヨーロッパ各国

概 要

欧州の電力会社数社を中心に、制御システムの保守用 PC がウイルスに感染し、そこから制御サーバの情報が漏えいした。原因は、制御ソフトメーカーの Web サイトが攻撃され、ウイルスが含まれたアップデート用インストーラが公開されており、それをダウンロード＆インストールしたためである。

こんな被害が起こる可能性も

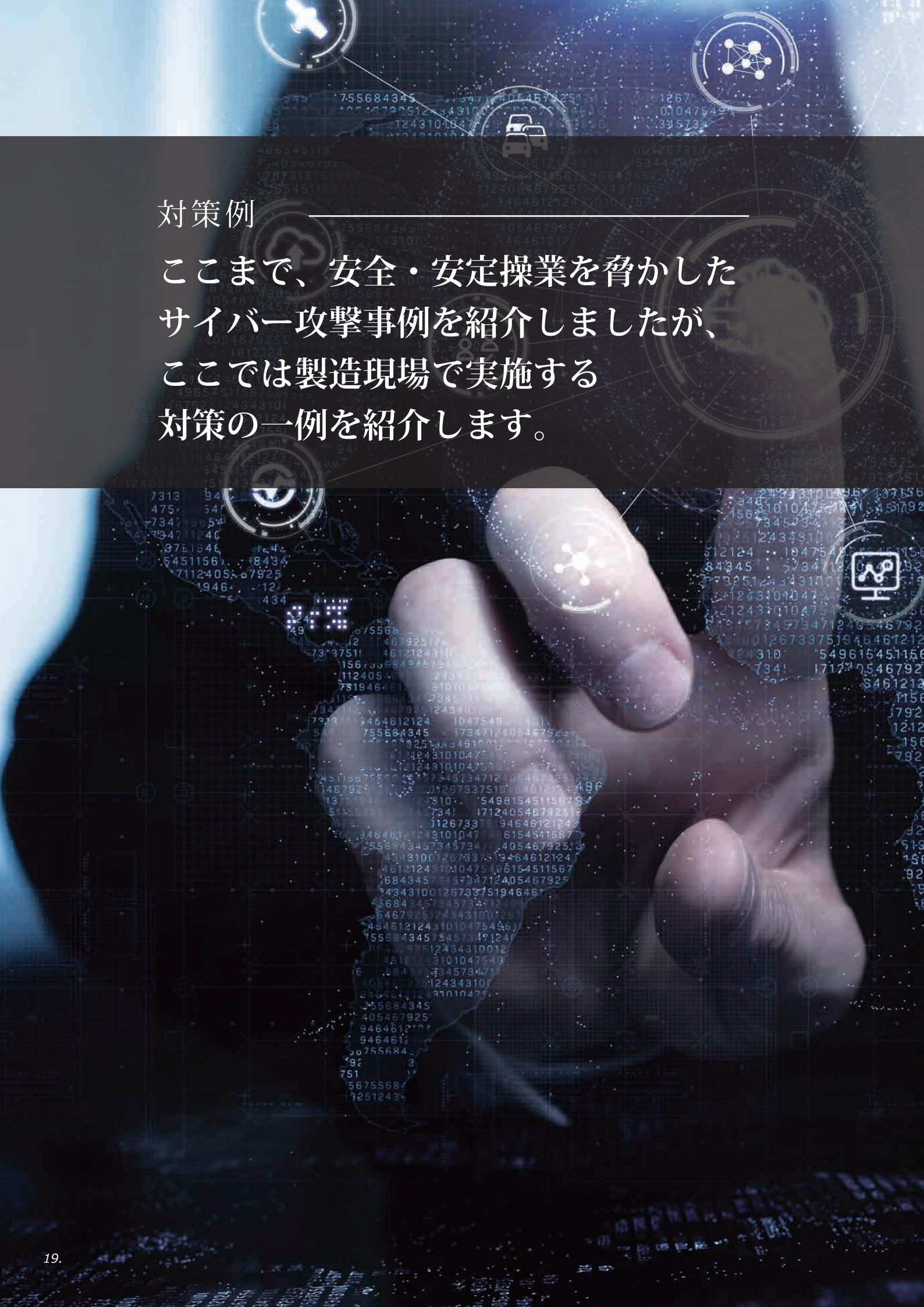
安 全

漏えいした情報を利用して、さらに大規模なサイバー攻撃を受けることで、周辺地域で大規模停電の可能性がある。それにより、病院やその他重要インフラの機能が停止し、人命に関わる事故が発生する。

品質・操業

送配電の設備を不正操作されて大規模停電が発生する。

【参考資料】
BROADCOM「Dragonfly: Western energy sector targeted by sophisticated attack group」
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks
Kaspersky「Energetic Bear — Crouching Yeti」
https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08080817/EB-YetiJuly2014-Public.pdf
MONOist：
制御システム破りの“定石”、「Operation Dragonfly」がもたらす“真の脅威”
https://monoist.atmarkit.co.jp/mn/articles/1409/17/news009.html
McAfee Blog:
産業プロトコルを脅かす「Operation Dragonfly」
http://blogs.mcafee.jp/mcafeeblog/2014/07/1416.html



対策例

**ここまで、安全・安定操業を脅かした
サイバー攻撃事例を紹介しましたが、
ここでは製造現場で実施する
対策の一例を紹介します。**

現場でできる、サイバー攻撃への対策

IT部門やセキュリティ部門と一緒に実施するものだけでなく、製造現場が実施するものもあります。
制御システムのセキュリティを確保する１つの手段として、ご活用いただければと思います。
すでに実施している対策もあるかもしれませんが、これからも継続して実施してください。

対策 1

不審なメールの添付ファイルは開かない、
URL はクリックしない！

対策 2

入退室管理、施錠管理、監視カメラ等の
物理セキュリティ対策を行い不審者を入れない！

対策 3

パスワードは初期設定のものから
推測しにくいものに変更しよう！

対策 4

不要な USB は使わない！
使わない USB ポートはふさごう！

対策 5

保守用 PC や USB などの外部記憶媒体は
制御システムに接続する前にウイルス
チェックをしよう！

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（ICSCoE）

本書の内容は現場向け制御セキュリティ教育プロジェクトの見解であり、
独立行政法人情報処理推進機構の意見を代表するものではありません。

令和３年６月発行