「港湾分野における情報セキュリティ確保に係る安全ガイドライン（第2版）」

事案事例集

令和７年３月28日

国土交通省港湾局

目次

(1)港湾における事例.....1
事案1. 名古屋港へのランサムウェア攻撃(2023 年 7 月).....1
事案2. オーストラリア・シドニー港へのサイバー攻撃(2023 年 12 月).....4
事案3. ベルギー・アントワープ港へのサイバー攻撃事案(2022 年 2 月).....5
(2)その他重要インフラにおける事例.....7
事案1. 日本政府 e-GOV へのDDoS攻撃(2022 年 9 月).....7
事案2. 米国コロニアル・パイプラインへのランサムウェア攻撃(2021 年 5 月).....9
事案3. 米国 SolarWinds 社製品を通じたサプライチェーン攻撃(2020 年 3 月).....11
事案4. ウクライナ電力会社への標的型攻撃(2015 年 12 月).....13

(1)港湾における事例

事案1. 名古屋港へのランサムウェア攻撃(2023 年 7 月)

●事案概要

2023 年 7 月 4 日、名古屋港のシステムがランサムウェア攻撃を受け、約 3 日間にわたりコンテナの搬入・搬出作業が停止した。ロシア系ハッカー集団「LockBit」による攻撃とされ、港湾の物流に大きな影響を与えた。名古屋港管理組合はバックアップを活用して 7 月 6 日にシステムを復旧。国内最大級の貿易拠点が標的となったことで、日本の港湾セキュリティ強化の必要性が浮き彫りとなった。

※注－以下の事案の詳細内容は、既往文献を再整理したものであり、各文献発行時点の情報による内容のため、その後の情報精査等により事実関係が一部異なっている可能性があります。

【事案の経緯】

2023 年 7 月 4 日	6:30 頃 NUTS システムにおいてサイバー攻撃による障害が発生
	7:15 頃 システム保守会社及びシステム開発会社へ調査を依頼
	7:30 頃 システム用プリンターからランサムウェアの脅迫文書が印刷される
	8:15 頃 サーバが再起動不可となる
	9:00 頃 愛知県警がランサムウェア攻撃の見解を示す
2023 年 7 月 5 日	2:00 頃 物理サーバ基盤が復旧、仮想サーバの復元作業を開始
	12:00 頃 名古屋港運協会がランサムウェアへの感染をプレス発表
	〃 仮想サーバ全 45 台の復元完了
	21:00 頃 復元した仮想サーバからウイルスが検知される
2023 年 7 月 6 日	2:00 頃 ウイルスチェックにより 130 のマルウェアを検知、ウイルス駆除開始
	7:15 頃 ウイルス駆除終了、バックアップデータの復元と連携作業開始
	14:15 頃 バックアップデータの連携完了
	15:00 頃 各コンテナターミナルが順次再開
	18:15 全ターミナルの作業再開

【攻撃の概要】

- 保守用 VPN を通じて物理サーバにランサムウェアが侵入し、サーバ情報が暗号化されたとみられる。
- 考えられる感染経路は、
  ① 指定ユーザのみ利用可能な仮想専用線たるVPN機器からの侵入
  ② 外部記憶媒体である USB メモリからの持ち込み
  ③ NUTS と港湾運送事業者間とのネットワーク連携で運用している NAT 変換による NUTS への接続からの侵入
  であるが、8 台の物理サーバが全て暗号化され、システムが起動不能となっていたことから、VPN 機器を通じて侵入し、サーバ部へ直接攻撃を行った可能性が最も高い。
- NUTS の保守用 VPN には緊急時に即時に対応するため IP アドレスに制限をかけておらず、ID とパスワードさえ合致すればインターネット上で誰からでもアクセス可能な状態にあった。

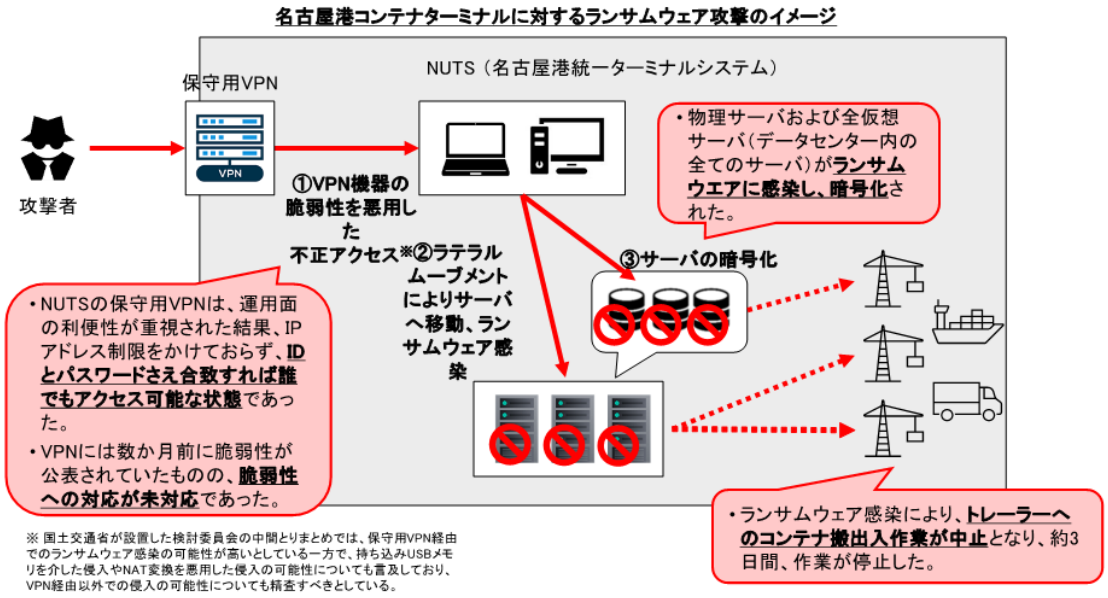


図　ランサムウェア攻撃の攻撃ステップ（イメージ図）

【社会経済への影響】

- 令和５年７月４日から７月６日までの３日間において、計 37 隻の荷役スケジュール（最大24時間）の遅延が発生した。
- コンテナ約2万本の搬入・搬出に影響があった。
- トヨタ自動車は、部品の積込作業ができないため、飛島物流センターなど輸出向け自動車部品梱包工場４カ所のラインを７日間停止した。
  - ✓ 国内外での自動車の生産に影響はなかった。

> ➢ 今年7月、ランサムウェア感染により、名古屋港統一ターミナルシステム(NUTS)が機能停止
> ➢ この結果、トヨタ自動車における4つの部品組立拠点が一時操業停止するなどの影響が発生
> ➢ 事態覚知(7/4 6:30機能停止)から全ターミナル再開(7/6 18:15)まで59時間45分を要した

名古屋港にサイバー攻撃か
コンテナ搬出入停止

トヨタ　愛知と岐阜４つの部品組立拠点停止へ

出典：読売夕刊
(7月5日 11面)

出典：NHK(7月6日)

名古屋港　各ターミナル等の機能と位置関係

出典：名古屋港運協会HP

図　サイバー攻撃による影響の概要

参考文献

- サイバー攻撃から復旧の名古屋港 2日ぶりにコンテナ積み下ろし再開（朝日新聞、2023年7月6日）
- コンテナターミナルにおける情報セキュリティ対策等検討委員会 資料（国土交通省港湾局）
- 電力分野におけるサイバーセキュリティについて（資源エネルギー庁、2024 年 4 月 17 日）
- 名古屋港コンテナターミナルのサイバー攻撃におけるインシデント対応について（国土交通省、2024 年 7 月 26 日）
- サイバーセキュリティに関する国土交通省の取組み（国土交通省、2023 年 11 月） ほか

事案2. オーストラリア・シドニー港へのサイバー攻撃（2023 年 12 月）

●事案概要

2023 年 11 月、オーストラリアの港湾運営会社 DP World Australia がサイバー攻撃を受けた。シドニーをはじめとした国内4港湾のコンテナターミナルにおいて、陸上業務及びトラックの移動を管理するシステムに不正な活動を検知し、システムへのアクセスを遮断、インターネットへの接続を切断した。そのため、これら4港湾のコンテナターミナルの操業がすべて停止した。

※注－以下の事案の詳細内容は、既往文献を再整理したものであり、各文献発行時点の情報による内容のため、その後の情報精査等により事実関係が一部異なっている可能性があります。

【事案の経緯】

2023 年 11 月 10 日	4港湾のコンテナターミナルが不正アクセスによるシステムシャットダウンで操業停止
2023 年 11 月 12 日	システムの安全性確認のテストを実施
2023 年 11 月 13 日	朝頃 操業を再開

【攻撃の概要】

- 4 つの港のターミナル陸上業務を管理するシステムで「不正な活動」を検知。すぐにシステムをシャットダウンしたが、データの漏えいが発覚した。
- 身代金の要求の有無など、攻撃の詳細については明らかにされていない。

【社会経済への影響】

- 不正アクセス被害を受けた 4 つのコンテナターミナルは、オーストラリアの貿易の約 40%を取り扱っており、操業停止となったことで約 3 万個ものコンテナが立往生する事態となった。
- オーストラリア貨物貿易連合（FTA）は、メルボルンでの輸出コンテナ規制、シドニーでの影響、フリーマントルでのトラックアクセスの変更など、日中の問題を挙げている。

参考文献

- DP World Australia Resumes Terminal Ops After “Serious” Cyber Incident（PANAMA Maritime Authority）

事案3. ベルギー・アントワープ港へのサイバー攻撃事案（2022 年 2 月）

●事案概要

2022 年 2 月、石油輸送・貯蔵会社であるドイツの Oiltanking 社、ベルギーの SEA-Invest 社、オランダの Evos 社を標的としたランサムウェア攻撃が発生した。ベルギーでは、SEA-Invest の子会社 SEA-Tank が管理する複数のターミナルでオペレーションが停止した。

※注－以下の事案の詳細内容は、既往文献を再整理したものであり、各文献発行時点の情報による内容のため、その後の情報精査等により事実関係が一部異なっている可能性があります。

【事案の経緯】

2022 年 1 月 29 日	アントワープ港 New Fruit 埠頭において果物貨物の積み下ろしが停止
2022 年 1 月 30 日	SEA-Invest がメディアに対しランサムウェア攻撃を受けたことを発表
2022 年 2 月 2 日	液体バルク部門 SEA-Tank が操業を再開 果物部門がマニュアル作業に切り替えて操業を一部再開
日付不明	コンテナ部門、果物部門が操業を再開

【攻撃の概要】

- ランサムウェア「Blackcat」による石油ターミナルのソフトウェアを標的としたハッキングが発生。
- BBC によると、3 社すべての IT システムがダウンしたか、深刻な障害を受けたとされる。
  - ✓ ただし、専門家は、組織的な攻撃であると考えないよう注意を促している。
- ベルギーの検察当局によると、アントワープ港にある同社最大の石油ターミナル「SEA-Tank」を標的とした攻撃により、SEA-Invest 社全体の端末が影響を受けたとみられる。
- SEA-Invest はハッカー集団との連絡は取っていないと強調した。

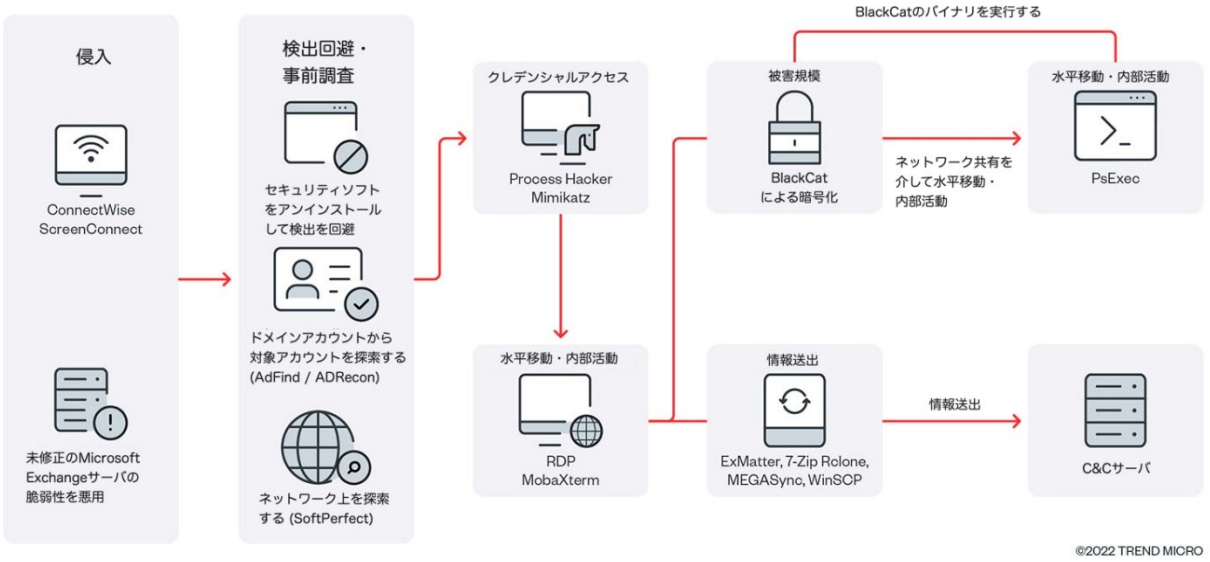


図 ランサムウェア BlackCat の感染フロー（例）

【社会経済への影響】

- ドライバルクを扱うターミナルではマニュアルで作業を行い、荷役は停止しなかった。
- SEA-Invest 社はベルギーの港で食品輸送を担い、スーパーマーケット「Colruyt」などへの供給にも関わっており、食品物流への影響が発生した。
- 港湾ターミナルのシステムが標的となったことで、はしけ船の航行に障害が発生し、タンカーの積卸しができない状況となった。

参考文献

- 新しい国際コンテナ戦略港湾政策の進め方検討委員会最終とりまとめ参考資料（国土交通省港湾局、令和6年2月16日）
- ランサムウェアスポットライト：BlackCat（トレンドマイクロ、2022 年12月23日）
- Cyber Security Assessment Netherlands CSAN 2022
- Antwerps parket onderzoekt cyberaanval op havenbedrijven: tankopslag SEA-invest hersteld, andere activiteiten ondervinden nog hinder（HLN、2022 年）
- European oil facilities hit by cyber-attacks（BBC,2022年2月4日）
- De grootste fruitwinkel van Europa werkt de klok rond（DE TIJD,2022年4月4日）

（2）その他重要インフラにおける事例

事案1．日本政府 e-GOV へのDDoS攻撃（2022 年 9 月）

●事案概要

2022年９月６日、電子政府の総合窓口「e-Gov」などの政府系サイトや東京地下鉄（東京メトロ）などのインフラ企業のウェブサイトが一時閲覧しづらい状態になった。警察庁と内閣サイバーセキュリティセンター（NISC）の分析によると、攻撃の手口は 1 秒間に最大 100 ギガビット程度の大量のデータを断続的に送りつける DDoS 攻撃と判明した。

※注－以下の事案の詳細内容は、既往文献を再整理したものであり、各文献発行時点の情報による内容のため、その後の情報精査等により事実関係が一部異なっている可能性があります。

【事案の経緯】

2022 年 9 月 6 日	「Killnet」が日本の政府機関や民間企業に対するDDoS 攻撃を示唆するコメントや動画を Telegram 上に投稿
	夕方ごろ DDoS 攻撃による e-Gov、eLTAX の閲覧障害が発生
	21:00 頃 e-Gov が概ね復旧完了
2022 年 9 月 8 日	朝ごろ eLTAX が復旧完了

【攻撃の概要】

- 親ロシア派を標榜するハクティビスト集団「Killnet」が日本の政府機関や民間企業に対する DDoS 攻撃を示唆するコメントや動画を Telegram 上に投稿。
- その後、ツールを使用したと推測される DDoS 攻撃が発生し、e-Gov と eLTAX の4つの URL が一時的に閲覧不可の状態になった。
- 攻撃元となる IP アドレスは、約 99%が海外に割り当てられた IP アドレスであり、国内 IP アドレスが約 1%であった。
- DDoS 攻撃では断続的な通信量の増加が認められるが、今回の DDoS 攻撃においては、通信量の増加程度は、最も弱くて7Mbps 程度、最も強くて 100Gbps 程度の通信量の増加が確認された。

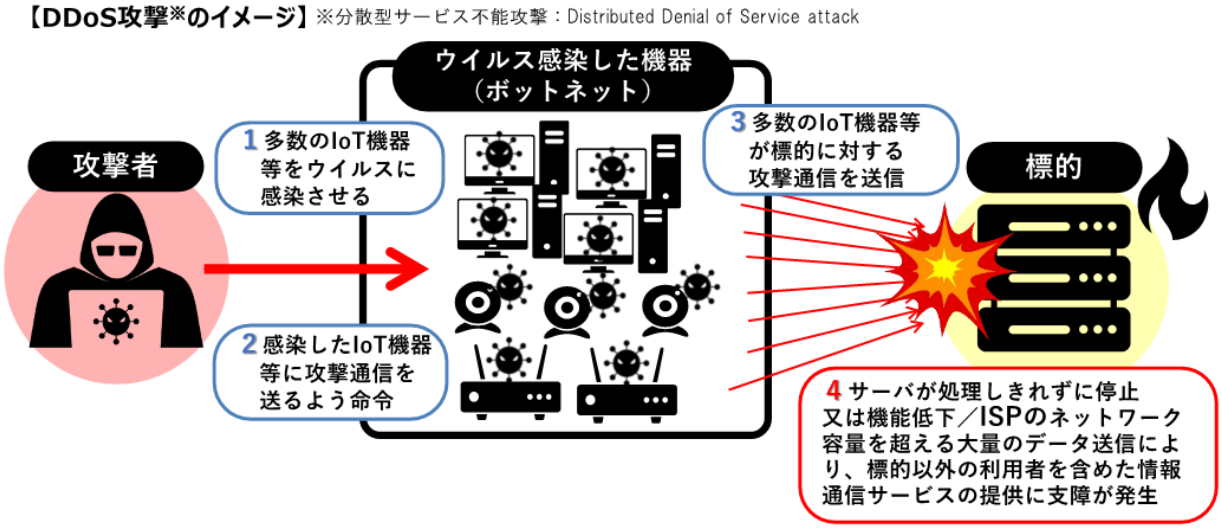


図　DDoS 攻撃のイメージ

【社会経済への影響】

・　政府のオンラインサービスが使用不可能となった。

参考文献

・「e-Gov」などが一時アクセス困難に、親ロシアのサイバー攻撃集団が犯行を示唆（日経 Xtech、2022 年 9 月）
・　総務省のサイバーセキュリティ政策（令和6年2月29日、総務省サイバーセキュリティ統括官室）

事案2. 米国コロニアル・パイプラインへのランサムウェア攻撃（2021 年 5 月）

●事案概要

2021 年 5 月 7 日、米国東海岸の 45%の燃料輸送を担う石油パイプライン企業（Colonial Pipeline 社）は、ロシアに拠点を置くハッカー集団「DarkSide」によるランサムウェア攻撃を受け、5 日間の操業停止に追い込まれ、5 億円相当の身代金を支払う事態が発生した（のちに、身代金の 85%は、FBI が回収したとされる）。

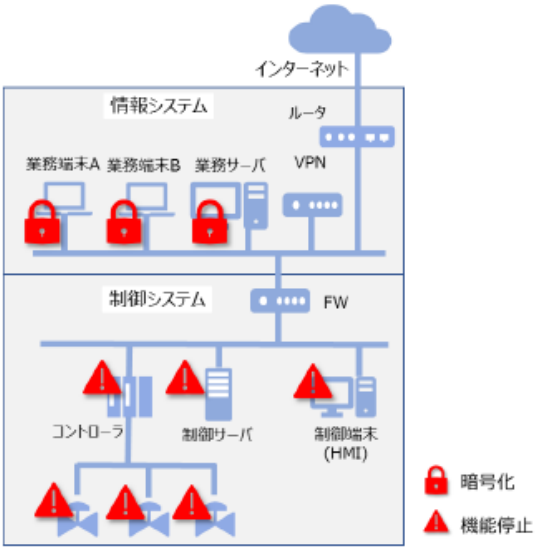
※注－以下の事案の詳細内容は、既往文献を再整理したものであり、各文献発行時点の情報による内容のため、その後の情報精査等により事実関係が一部異なっている可能性があります。

【事案の経緯】

2021 年 4 月 29 日	DarkSide がコロニアル・パイプライン社のコンピュータシステムに侵入。
2021 年 5 月 7 日	攻撃者からの身代金請求書を発見。パイプライン操業の一時停止。
2021 年 5 月 8 日	身代金の支払い。 パイプラインの操業を停止したとの最初の報道発表。法執行機関や連邦機関へ連絡。第三者のサイバーセキュリティ企業に依頼し、調査。
2021 年 5 月 9 日	米国政府が地域緊急事態宣言を発出。 メインラインは停止中であるが、ターミナルと配送地点にある小規模なラテラルラインは稼働中。
2021 年 5 月 10 日	復旧のために膨大なリソースを投入。全てのシステムをスキャンして、マルウェアの可能性や侵害の兆候が無いことを調査。 ノースカロライナ州からミズーリ州までのパイプラインは在庫に限って、手動で稼働中。
2021 年 5 月 12 日	パイプライン操業を再開。通常業務に戻るまで数日を要する見込み。
2021 年 5 月 13 日	パイプライン全体で再開。輸送に係るサプライチェーン全体が正常に戻るまで数日かかる見込み。
2021 年 6 月 7 日	FBI が身代金の一部を押収

【攻撃の概要】

- VPN 装置に不正アクセス。漏えいしたパスワードが利用された。
  - ✓ VPN の正規アカウントを使って侵入（とされている）。パスワードは使いわましされたものが漏洩していた。
  - ✓ VPN は多要素認証が導入済みであったが、一部無効にされていたアカウントが悪用される。
- 情報システムへの侵入後にネットワーク内部を調査し、脅迫のための機密情報の所在調査、攻撃可能な機器に対してランサムウェアを配布。
- 機密情報を窃取し、外部に持ち出し。
- 配布したランサムウェアにより端末内のデータを暗号化。情報システムを機能不全に陥れる。
- 現場担当者が制御システムへの被害拡大を懸念し、制御システムを停止
  - ✓ 予防措置として全てのパイプラインを一時停止。
- 最終的な復旧にはバックアップを取っていたデータを使用。



出典:制御システム関連のサイバーインシデント事例9(IPA、2021 年 10 月)

図 システムへの攻撃の概念図

【社会経済への影響】

- 攻撃によって大規模な供給停止が発生。
  - ✓ パイプラインの操業停止は、アラバマ州、アーカンソー州、コロンビア特別区、デラウェア州、フロリダ州、ジョージア州、ケンタッキー州、ルイジアナ州、メリーランド州、ミシシッピ州、ニュージャージー州、ニューヨーク州、ノースカロライナ州、ペンシルバニア州、サウスカロライナ州、テネシー州、テキサス州、バージニア州など、米国東海岸の複数の州に影響を与えた。
- ガソリン価格の急騰と、国内での燃料不足が広範に報告された。また、消費者の不安感やパニック買いが広がり、交通や物流に支障をきたした。
  - ✓ 例えば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となったなど 市民 生活に大きな影響を与えた。

ガソリンを求める長蛇の車列
(写真提供:©Robin Rayne/ZUMA Wire/共同通信イメージズ)

出典:内外情勢の回顧と展望(令和 4 年版)(公安調査庁、2021 年 12 月)

図 システムへの攻撃の概念図

参考文献

- 制御システム関連のサイバーインシデント事例9(IPA、2021 年 10 月)
- 内外情勢の回顧と展望(令和 4 年版)(公安調査庁、2021 年 12 月) ほか

事案3. 米国 SolarWinds 社製品を通じたサプライチェーン攻撃(2020 年 3 月)

●事案概要

2020 年 3 月 26 日、SolarWinds 社は同社のネットワーク監視ソフトウェア「Orion Platform」に、正規のアップデートを通じてマルウェアが仕込まれたことを公表した。攻撃は 2019 年 9 月に始まっていたとみられ、2020 年 3 月～6 月のアップデートファイルが侵害されたことで、米政府機関等を含む最大約 18,000 組織が影響を受けたとされる。

※注－以下の事案の詳細内容は、既往文献を再整理したものであり、各文献発行時点の情報による内容のため、その後の情報精査等により事実関係が一部異なっている可能性があります。

【事案の経緯】

2019 年 9 月	SolarWinds のネットワークへの不正アクセスが発生
2019 年 10 月	Orion へのコードインジェクションが発生
2020 年 3 月 26 日	Orion のアップデートファイルにマルウェア「Sunburst」が仕込まれる
	正規のアップデートに見せかけて、18,000 以上の組織にマルウェアが展開
2020 年 12 月	SolarWinds がサイバー攻撃の被害を受けたことを公表
2020 年 12 月 13 日	CISA が被害の対応に関する緊急指令 ED21-01 を発表
2020 年 12 月 14 日	日本の内閣府セキュリティセンター(NISC)が注意喚起を公表

【攻撃の概要】

- 何らかの入り口から、広く使われている IT 監視 / 管理ソフトウェアシステムである Orion にバックドアが設置され、マルウェア「Sunburst」が侵入し被害が発生したとみられる。
- 攻撃者は、Orion が広くサービス展開するのを待ち、導入社が 30,000 社を超えた段階で Sunburst による攻撃を行った。

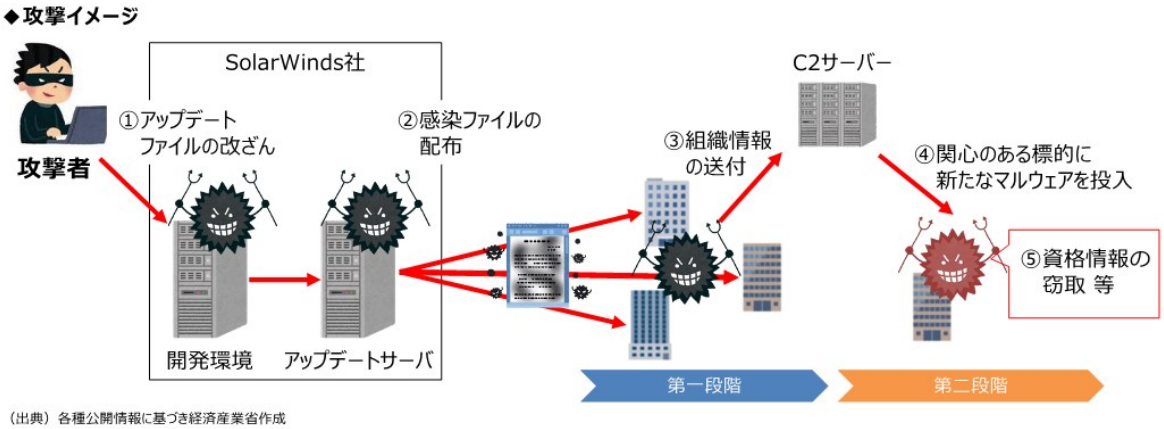


図 Sunburst によるサイバー攻撃のイメージ

【社会経済への影響】

- Orion を使用する 33,000 社のうちアップデートによって 18,000 社が影響を受けた。
- 米国政府や軍も Orion を導入しており、不正アクセス等の被害を受けた。
  - ✓ 米国財務省は、数十の電子メールアカウントの侵害を受けた。また、米マイクロソフトではソースコードの一部の漏洩被害が発生した。
- 事案発覚の半年前に、米司法省が自組織への不正アクセスに気づいて調査を進めていたが、全体としての連携・共有が行われていなかった。
- Orion の日本代理店は、国内においても被害の可能性があることを発表した。

参考文献

- サイバー攻撃の情報共有にかかる取組について（令和6年2月8日、経済産業省サイバーセキュリティ課）
- 第 11 章　ロシアをめぐるサイバー問題―ロシアの情報セキュリティ概念と SolarWinds 社事案（山添　博史）
- 注目されているセキュリティ事故・事件に関する情報＜2021 年 3 月版（第 36 号）＞（選り抜き版）（NTT データ先端技術（株））

事案4. ウクライナ電力会社への標的型攻撃（2015 年 12 月）

●事案概要

2015 年12 月23 日、ウクライナ（イバノフランコフスク、チェルノフツィ、キエフ）で電力会社へのサイバー攻撃が発生し、様々な要因が重なった結果、大規模停電を引き起こした。発生から復旧までに最大で6 時間を要し、22 万5 千人の顧客に影響を与えた。サイバー攻撃によってエネルギーの供給が停止した世界初の事例と言われる。

※注－以下の事案の詳細内容は、既往文献を再整理したものであり、各文献発行時点の情報による内容のため、その後の情報精査等により事実関係が一部異なっている可能性があります。

【事案の経緯】

被害発生以前	マルウェアによる標的型メール攻撃が発生 ※検知されないまま、長期間の偵察を実施
2015 年12 月23 日	15:50 頃 SCADA システムを制御し、変電所を遠隔で停止
	〃 電話系統に対する DOS 攻撃が発生
	〃 マルウェアによるデータ破壊が発生
	〃 UPS（非常用電源）を遮断

【攻撃の概要】

- ウクライナの電力会社に対し、ハッカー集団「Sand Worm」によるサイバー攻撃が発生。
  行われた攻撃は以下のとおり。
  ① 標的型メール攻撃（IT 系への攻撃）
  事前にマルウェア「BlackEnergy3」を含む添付ファイルをメールで送付
  →検知されないまま長期間の偵察を行った
  →攻撃実行日、マルウェア「KillDisk」によりシステム内部のデータを破壊
  ② DOS 攻撃で電話システムに支障発生（IT 系への攻撃）
  →復旧活動を妨害
  ③ 遠隔操作で変電所の遮断機を切断（OT 系への攻撃）
  →最大6 時間の停電が発生（22 万5 千世帯）
  ※UPS（非常時電源）が動作しないように設定
- 電力制御システムを遠隔から手動操作することで停電を発生させた。
- 攻撃者は、対象となる企業のシステムやネットワークを 6 ヵ月以上前から入念に調査した上で、サイバー攻撃を計画していたとされる。
  - ✓ 最終攻撃に向けた段階で、対象企業のアカウント情報（ID やパスワード）を入手し、VPN による接続やリモート管理ツールの使用など正規の通信経路をたどり、リモートから制御システム環境へ接続したと考えらえる。
- 本事例に関して、詳細なシステム構成情報は公開されていない。

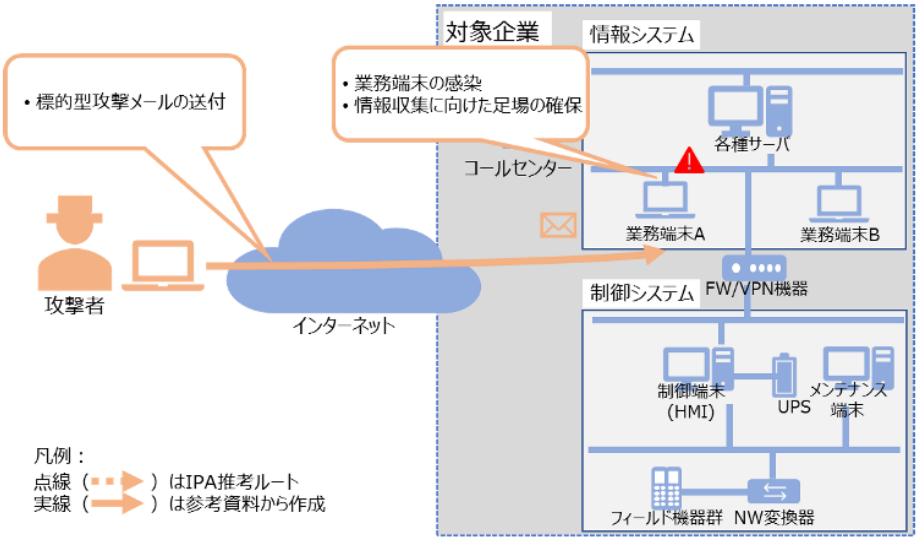


図 マルウェアへの感染誘導

【社会経済への影響】

・ 複数地域において最大 6 時間の大規模停電が発生し、22 万 5 千人に影響を与えた。

図 ウクライナにおけるインシデント発生地域

参考文献

・ 制御システムのセキュリティリスク分析ガイド補足資料 制御システム関連の サイバーインシデント事例1（IPA）

・ 電力制御システムへのサイバー攻撃 – ウクライナの電力網を狙う Industroyer2（TOiNX）