Institute of Advanced Sciences
Yokohama National University

YNU YOKOHAMA National University

資料安作2-3

近年のサイバー脅威の動向について
～重要インフラ等への攻撃事例から何が学べるか～

吉岡　克成

横浜国立大学
大学院環境情報研究院/先端科学高等研究院

放送設備安全信頼性検討作業班（2023.1.30）

本日のお話の流れ

- サイバー攻撃の巧妙化・深刻化
  - ランサムウェア攻撃拡大、分業化、組織化
- 重要インフラにおける攻撃事例
- 放送システムのIP化・クラウド化に向けて

サイバー攻撃の巧妙化・深刻化

- **頻度、規模、対象が拡大（量的な脅威の増大）**
  - 脆弱なシステム、IoT機器を狙う攻撃
  - 重要インフラを狙う攻撃
  - 超大規模サービス妨害攻撃
  - なりすましメール（Emotetなど）
  - フィッシング

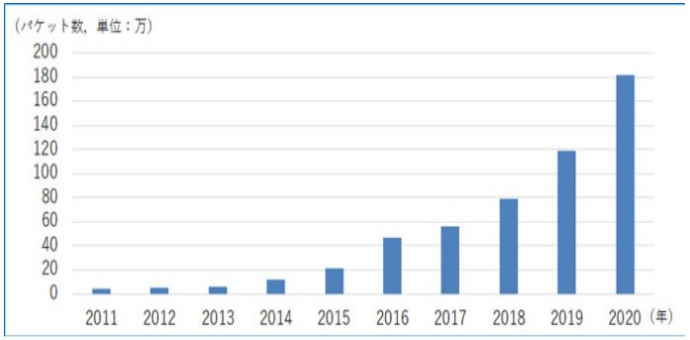


図1.1 IPアドレス当たりの年間総観測パケット数（過去10年間）

- **高度化、組織化、ビジネス化の進展（質的な脅威の増大）**
  - ソーシャルエンジニアリング攻撃
  - サプライチェーン攻撃
  - ゼロデイ攻撃
  - Cybercrime-as-a-Service
  - 世論操作、心理的誘導

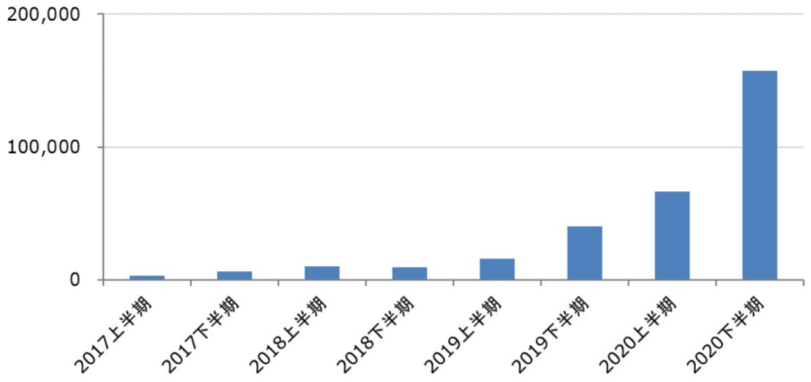


図 1-1　国内のフィッシング情報の届け出件数 [2]

情報通信技術の浸透や国際情勢の緊張を背景に、サイバー脅威が高まっている

情報通信研究機構 NICTER観測レポート2020の公開, https://www.nict.go.jp/press/2021/02/16-1.html
フィッシング対策協議会　フィッシングレポート, 2021 https://www.antiphishing.jp/report/phishing_report_2021.pdf

ランサムウェア攻撃における分業・組織化

- 組織に侵入
- 内部情報の暗号化、外部持ち出し
- 持ち出し情報の評価（価値の値踏み）
- 支払い手段の確保、支払い金の追跡困難性確保
- 脅迫（被害者との交渉）
- 支払い後の対応（暗号化されたデータの復元）
- 支払わない場合の対応（持ち出し情報の暴露・公開・第三者への販売）

ビジネスモデルを持続させるため、攻撃側も組織化・分業・アウトソースにより効率化

重要インフラ†・産業制御システム に関連する攻撃事例（海外）

- コロニアル・パイプライン（2021） 米大手パイプライン会社がランサムウェア攻撃で5日間操業停止，4.8億円の身代金支払い
- ソーラーウインズ（2020） システム管理ツールの開発会社への侵入を発端に顧客（米国政府，米軍，米国大手重要インフラ企業含）が連鎖的に攻撃を受ける．被害の全容は未だ不明．
- ノルスク・ハイドロ（2019） アルミ最大手の生産設備管理システムとITシステムがランサムウェア感染．世界40か国170か所のオフィスや工場のコンピュータが感染．被害額は約65-77億円と見積もり．
- 台湾TSMC（2018） 世界的半導体企業TSMCの工場NWにランサムウェアWannacryが侵入．3日間生産停止による損害額は最大190億円
- WannaCry（2017） 150か国30万台以上（国内600か所以上）がランサムウェアに感染
- ウクライナ大規模停電（2016） サイバー攻撃により変電所の遮断機切断、1時間強の停電
- ウクライナ大規模停電（2015） サイバー攻撃により変電所の遮断機切断、最大6時間停電、22万人以上に影響
- イラン核燃料施設への攻撃（2010） サイバー攻撃によりウラン濃縮用遠心分離機約1000台が稼働不能

†我が国においては、情報通信（主要な地上基幹放送事業者を含む）、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流、化学、クレジット、石油の14分野が重要インフラ分野に位置づけられる

重要インフラ†・産業制御システム に関連する攻撃事例（海外）

- コロニアル・パイプライン（2021） 米大手パイプライン会社がランサ… 業停止，4.8億円の身代金支払い
- ソーラーウインズ（2020） システム管理ツールの開発会社への侵入… 府，米軍，米国大手重要インフラ企業含）が連鎖的に攻撃を受ける… 明．
- ノルスク・ハイドロ（2019） アルミ最大手の生産設備管理システムとITシステムがランサムウェア感染．世界40か国170か所のオフィスや工場のコンピュータが感染．被害額は約65-77億円と見積もり．
- 台湾TSMC（2018） 世界的半導体企業TSMCの工場NWにランサムウ…入．3日間生産停止による損害額は最大190億…
- WannaCry（2017） 150か国30万台以上（…ランサムウェアに感染
- ウクライナ大規模停電（2016） サイバー攻撃により変電所の遮断機切断…
- ウクライナ大規模停電（2015） サイバー攻撃により変電所の遮断機切断…、22万人以上に影響
- イラン核燃料施設への攻撃（2010） サイバー攻撃によりウラン濃縮用遠心分離機約1000台が稼働不能

二重脅迫、RaaS

サプライチェーン攻撃

感染端末持込

自動感染拡大機能をもつワーム型（非標的型攻撃）

執拗な攻撃 妨害目的

破壊目的

USBメモリ経由で持ち込み感染

†我が国においては、情報通信（主要な地上基幹放送事業者を含む）、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流、化学、クレジット、石油の14分野が重要インフラ分野に位置づけられる

海外事例　コロニアル パイプライン攻撃

2021 年 5 月 7 日米国最大手のパイプライン企業 Colonial Pipeline がランサムウェアによるサイバー攻撃を受けた。被害は情報系であり、パイプライン制御システムそのものは直接の影響を受けていなかったが、予め決められていた全社的なインシデント対応プロセスに則って、パイプラインは予防保全的に停止された。[1]

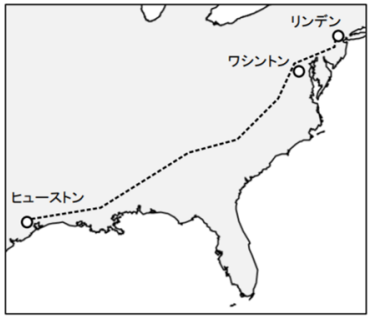


図1　Colonial Pipeline 社の主要なパイプライン

このパイプラインは米国東海岸で消費される燃料の約 45%を扱っており、6 日間続いたパイプラインの停止により、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[2]。また、ランサムウェアを使用する近年のサイバー攻撃は、二重の脅迫[3]と呼ばれる手口が併用され、データの暗号化のみならずデータの窃取が行われ脅迫される。本ケースでは 100GB 近いデータが窃取されたと報道されている。[4]
当該インシデントについて FBI[1]は DarkSide ランサムウェアが関与していると声明を出している[5]。DarkSide はランサムウェアの呼称でもあり、攻撃グループの名前でもあり、ランサムウェアによるサイバー攻撃のクラウドサービスの呼称でもある[6]。

https://www.ipa.go.jp/files/000093825.pdf

海外事例　コロニアル パイプライン攻撃

1. VPNの正規アカウントを使って侵入（とされている）．パスワードは使い回しされたものが漏洩していた
2. 脅迫のための機密情報の調査，他の端末へのランサムウェア配布
3. 機密情報を外部へ持ち出し
4. 端末内のデータをランサムウェアにより暗号化し，情報システムを機能不全にする
5. 現場担当者が制御系への被害拡大を懸念して制御システムを停止．顧客への燃料提供がストップし市場の燃料が枯渇

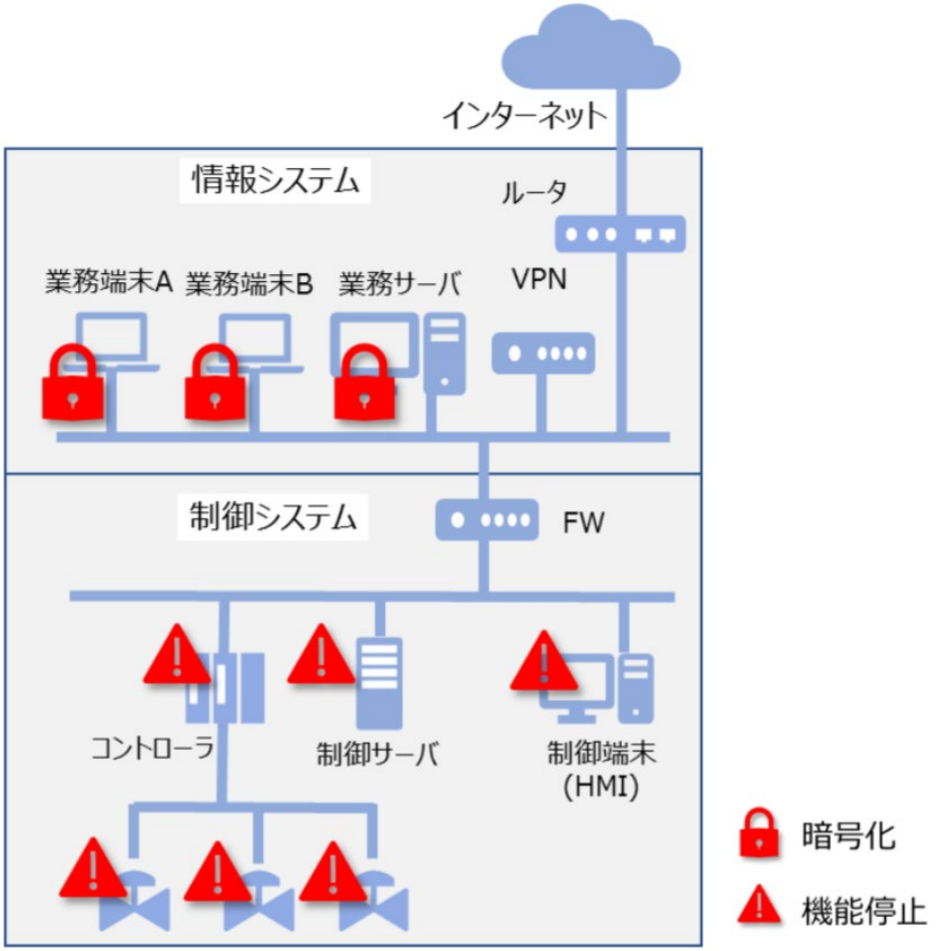


図 1-1　事例理解のための仮想システム構成図（実際のシステム構成とは異なる）

https://www.ipa.go.jp/files/000093825.pdf

海外事例　コロニアル パイプライン攻撃

- VPN装置には多要素認証が適用されていたものの未使用のレガシープロファイルが存在し、ID/パスワードのみでログイン可能だったとされる†
- 利用されたパスワードはダークウェブに漏洩していた†
- 情報系から侵入を受け、制御系に影響が派生するという典型的な攻撃の流れ
- 制御系まで攻撃が到達していなくても、攻撃が発覚した時点で影響を考慮して制御系を止めざるを得なかった
- バックアップは存在していたが破損がないか使用しても安全か短時間で判断がつかず、身代金支払い（4億8千万円）に応じざるを得なかった†
- 身代金の85%はFBIが回収したとされる

†https://www.cloudgate.jp/security-news/colonial-pipeline-ransomware-attack-cause-and-why-it-paid-ransom.html

MITRE ATT&CKによる整理

MITRE ATT&CK: 米国MITREによりサイバー攻撃の戦略、技術、ツール、攻撃グループなどを体系化したナレッジDB（下記はICS版ATT&CK）

攻撃の戦略の流れ

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

初期侵入のフェーズ

内部での展開と拡大フェーズ

攻撃の表面化フェーズ

https://collaborate.mitre.org/attackics/img_auth.php/3/37/ATT&CK_for_ICS_-_Philosophy_Paper.pdf

MITRE ATT&CKによる整理

前述の重要インフラ攻撃事例群をマッピング

#MITRE ATT&CK for ICSを利用

VPN認証情報の入手
（コロニアル）

悪性サイト誘導
（ノルスクハイドロ）

感染機器持ち込み
（台湾TSMC）

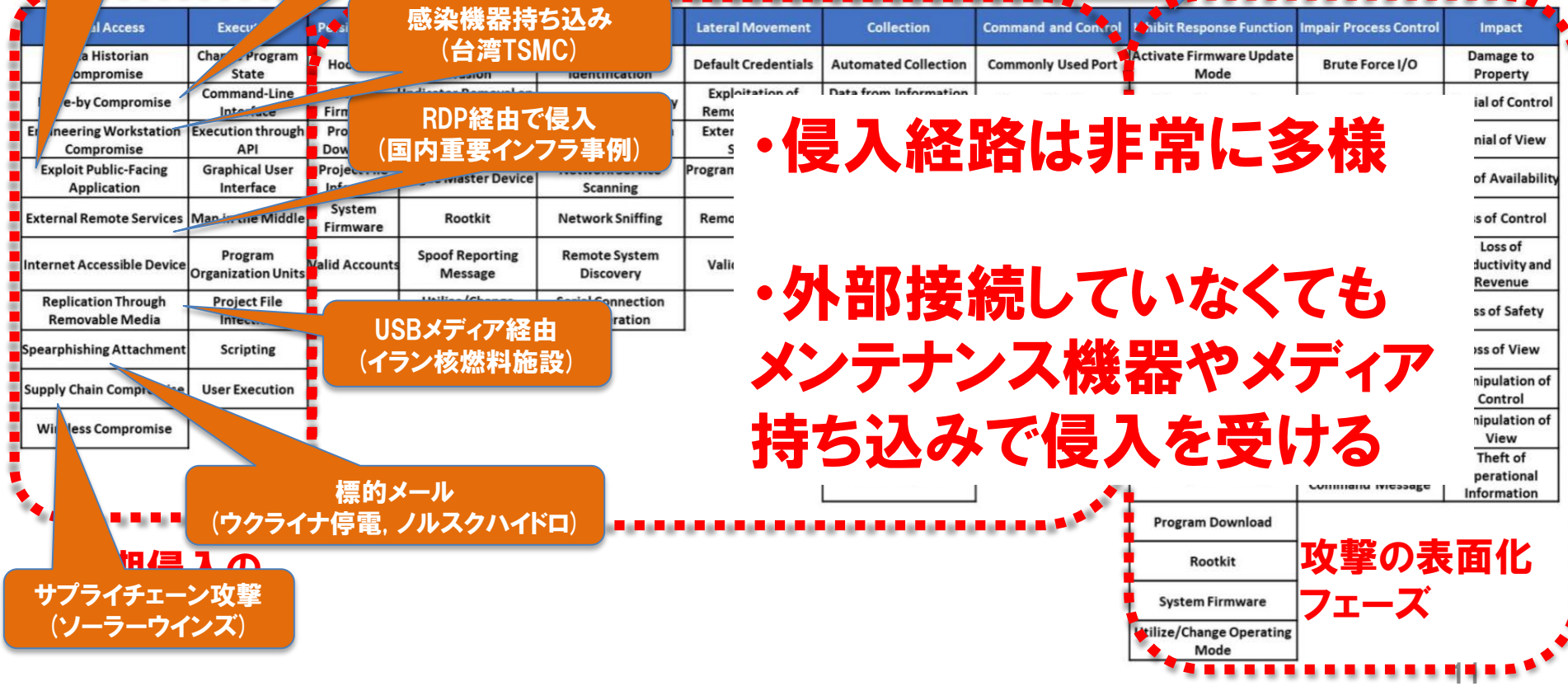
RDP経由で侵入
（国内重要インフラ事例）

USBメディア経由
（イラン核燃料施設）

標的メール
（ウクライナ停電，ノルスクハイドロ）

サプライチェーン攻撃
（ソーラーウインズ）

攻撃の戦略の流れ



・侵入経路は非常に多様

・外部接続していなくてもメンテナンス機器やメディア持ち込みで侵入を受ける

https://collaborate.mitre.org/attackics/img_auth.php/3/37/ATT&CK_for_ICS_-_Philosophy_Paper.pdf

MITRE ATT&CKによる整理

前述の重要インフラ攻撃事例群をマッピング

#MITRE ATT&CK for ICSを利用

攻撃の戦略の流れ

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Im	ss Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode		orce I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Chang	ogram State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Ma	uerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic		Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File			Block Serial COM	Modify Parameter		Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accou			Data Destruction	Module Firmware		Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download		Loss of Safety
Spearphishing Attachment	Scripting							Device Restart/Shutdown	Rogue Master Device		Loss of View
Supply Chain Compromise	User Execution							Manipulate I/O Image	Service Stop		Manipulation of Control
Wireless Compromise								Modify Alarm Settings	Spoof Reporting Message		Manipulation of View
								Modify Parameter	Unauthorized Command Message		Theft of Operational Information
								Program Download			
								Rootkit			
								System Firmware			
								Utilize/Change Operating Mode			

PLCプログラム書き換え
（イラン核燃料施設）

異常状態の隠蔽
（イラン核燃料施設）

HMIや生産管理
サーバ、業務端末
ファイル暗号化
（ノルスクハイドロ）

ブレーカ遮断コマンド送信
（ウクライナ停電）

機密情報の持ち出し
（コロニアル）

攻撃の表面化
フェーズ

「破壊・妨害」が目的の場合と「情報盗取、身代金」が目的の場合あり

https://collaborate.mitre.org/attackics/img_auth.php/3/37/ATT&CK_for_ICS_-_Philosophy_Paper.pdf

フランス TV5MONDE攻撃

- 2015年4月にフランスの国際テレビネットワークTV5MONDE（TVサンクモンド）の12チャンネルがサイバー攻撃により18時間放送不能になった.
- 同時に同社のSNSアカウントが乗っ取られISのプロパガンダメッセージが表示されたため、当初はISによる攻撃の可能性が疑われた

https://www.bankinfosecurity.com/french-officials-detail-fancy-bear-hack-tv5monde-a-9983

5MONDE攻撃

1月23日　マルチメディアサーバに最初の攻撃．デフォルトID/PASSWORDを使用していたが内部NWへ接続なし．攻撃失敗

2月16日～3月25日ネットワークインフラ把握、内部文書（wiki）からの認証関連情報取得

攻[illegible]の戦略の流れ

放送不能状態が発生

4月8日ネットワーク機器（ルータとスイッチ）のファームウェア消去によりシステムがダウン

Initial A[illegible]	Execution	Persistence	Evasion	Discovery	Lateral Mov[illegible]nt	Collection	Command and Control
Data His[illegible] Compro[illegible]	Change Program State	Hooking	Exploitation for Evasion	[illegible]ontrol Device [illegible]dentification	Default Credential[illegible]	Automated Collection	Commonly Used P[illegible]
Drive-by Co[illegible]hise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/[illegible] Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Pro[illegible]
Engineering W[illegible]tation Compro[illegible]e	Execution through API	Program Download	Masquerading	N[illegible]twork Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Applica[illegible] Layer Protoco[illegible]
Exploit Publi[illegible] Facing Applicat[illegible]on	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State	
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image	
Internet Acce[illegible]ble Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification	
Replicatio[illegible]ough Removal[illegible]dia	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State	
Spearphishi[illegible]ment	Scripting					Point & Tag Identification	
Supp[illegible]						Program Upload	
W[illegible]						Role Identification	
						Screen Capture	

Inhibit Response Function	Impair Process Control	[illegible]t
[illegible] I/O	[illegible]e to [illegible]rty
[illegible]n State	Den[illegible] Control
[illegible]ing	Deni[illegible] of View
[illegible]l Logic	Loss of Availability
Block Serial COM	[illegible]dify Parameter	Loss of Control
Data Destruction	Module Firmware	Loss of Productivity and Revenue
Denial of Service	Program Download	Loss of Safety
Device Restart/[illegible]down	Rogue Master Device	Loss of View
[illegible]e	Service Stop	Manipulation of Control
[illegible]s	Spoof Reporting Message	Manipulation of View
Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
Program Download		
Rootkit		
System Firmware		
[illegible]ilize/Change Operating Mode		

2月6日　外部組織から漏洩したアカウントによりVPNによりアクセス成功

～2月11日 カメラ管理サーバを拠点化．Active Directoryに管理者アカウント生成

その後、RATのインストール

初期侵入のフェーズ

内部での展開と拡大フェーズ

攻撃の表面化フェーズ

2021年10月には米大手テレビ放送局運営会社Sinclair Broadcast Groupがランサムウェア攻撃を受け、複数の放送局で放送が停止する事態となった

https://www.bankinfosecurity.com/french-officials-detail-fancy-bear-hack-tv5monde-a-9983
https://www.cyberscoop.com/sinclair-broadcast-group-ransomware-ongoing-disruption-macaw/

重要インフラ等への攻撃事例からの気づき

- **高度かつ執拗な攻撃の対象である**

攻撃対象の価値に見合うコストをかけて**周到な準備と継続的で執拗な攻撃**が行われる．影響力の大きい放送設備は対象となり得る

- **あらゆる侵入経路が狙われる**

IP化、クラウド化は利便性を高めるが、**攻撃者にとっても同じ**．番組素材の作成、共有、蓄積、配信、放送のすべてのステップ、関係者が攻撃対象となり得る。テレワークなどを想定するとさらに**侵入経路が増える**．

- **破壊・妨害攻撃が特に脅威**

放送設備を含め、重要インフラは正常に動作していること自体に高い価値があり、**機能の破壊、妨害を目的とした攻撃**が特に脅威となる．一般に不正操作や改ざんより、破壊、妨害活動の方が**実行しやすく防御しにくい**．

放送設備のIP化、クラウド化に向けて

- **放送システムの構成、運用、利用者（内外関係者含む）等全体像の把握とモデル化、脅威分析**

番組制作から放送、配信まで多岐にわたる複雑なプロセス、多様なステークホルダが存在すると予想。共通モデルに基づく脅威分析が可能か要検討。他の重要インフラとの決定的な差異があるか。

- **セキュリティ対策の検討**

脅威分析に基づき、適切なセキュリティ対策を検討する。多重防御やサイバーレジリエンスが中核のコンセプトだが、コストの観点も重要。インシデント時に死守すべき機能は何か。縮退運転が可能か。

- **脅威情報等の収集・共有**

活性化するサイバー攻撃ビジネスにおける重要インフラアクセス情報販売、リークデータ販売など、重大な攻撃の予兆となり得る脅威情報を定常的に収集、共有する努力により、攻撃への準備を怠らない。