戦略的イノベーション創造プログラム

サイバーセキュリティのインシデント(事件等)に関する事例動向

2020年1月24日作成

株式会社三菱総合研究所
デジタル・イノベーション本部
サイバーセキュリティ戦略グループ

本調査研究は、内閣府が進める戦略的イノベーション創造プログラム（SIP）「重要インフラ等におけるサイバーセキュリティの確保」（管理法人：NEDO)によって実施されました。

目次

用語一覧

用 語	説 明
バックドア	元々の意味は「裏口」。正規アクセス以外の方法で、情報システム等にアクセス可能な経路のこと。システム侵入に成功した攻撃者が継続侵入のため設置する場合や、機器の製造過程で不正に組み込まれる場合等がある。
マルウェア	悪意のあるソフトウェアのこと。Malicious Softwareを略した造語。コンピュータウイルス、ワーム、トロイの木馬等を総称したもの。
エクスプロイト	システム等への侵入や動作妨害を行うために用いる悪性のコードやコマンドのこと。
フィッシング	他人になりすましたEメールを送信し、受信者から情報を騙し取る詐欺行為のこと。フィッシングメールへのマルウェア添付、本文中の不正リンクをクリックするように誘導するといった手口が代表的である。
キーロガー	コンピューターへのキー入力（キーボードのタイプ履歴等）を監視して記録するソフトウェアのこと。正当な目的で用いられることもあるが、ユーザーの入力したパスワード情報の窃取に悪用されることも多い。
ランサムウェア	感染した端末や接続機器のファイルを暗号化し、復号鍵の提供と引き換えに身代金を要求するマルウェア。身代金は匿名仮想通貨で要求されることが多いが、支払いを行っても復号鍵が提供されないこともある。
二段階認証	サービスへのログイン時の認証等に、二段階のプロセスを課す方式のこと。パスワード認証後に、登録したメールアドレスやスマートフォンのプッシュ通知等に送信された認証コードを再度入力する等の実装がある。デバイス認証や生体認証といった性質の異なる認証を要求する場合は、多要素認証と呼ばれる。
P2P	複数の端末が、中央サーバーを介さずに直接通信する方式のこと。近年は、ブロックチェーンの実装に用いられることも多い。
CAN	Controller Area Networkの略。自動車の車載ネットワークで標準的に用いられる他、制御系システムで広く活用されている。通信の安定性が高い等の強みがある低レイヤプロトコル（バス）。セキュリティ機能は基本的にサポートされておらず、高レイヤプロトコルで実装することが必要である。
PLC	Programmable Logic Controllerの略。制御機器のコントロールに主に用いられる。様々な種類の入出力を扱うことが可能。プログラムはラダーと呼ばれる方式で記述され、PLCのメモリに書き込む。
SDK	Software Development Kitの略。ソフトウェアの開発を支援するフレームワーク。SDKには様々な機能が標準で備わっており、アプリケーション開発に用いることが出来る。ただし、不正なSDKの機能をアプリケーションに組み込んでしまうと、知らぬ間にアプリケーションに悪意ある機能が含まれてしまうことにもなる。
CVSS	米国の標準化機関MITREによって開発された脆弱性の深刻度を表す指標。現在はバージョン3が最新版。

1. 調査の概要と調査方法

1.1 調査目的と調査範囲

目 的

変化し続けるサイバー攻撃に対して、セキュリティ事故（インシデント）や脅威について最新の事例動向を把握し、今後の研究開発や対策の方向性の検討に役立てることを目的とする。

調査対象範囲

- 2019年3月～12月に報告されたサイバーセキュリティに係るインシデントについて攻撃手法や被害影響を含む状況に関して整理した。
- サイバー攻撃による事件の他、攻撃者の活動、システムの脆弱性などにより生じる潜在的な脅威も対象とした。
- 報告されるインシデントのうち研究開発の参考となるものについて、攻撃の新規性、被害影響の大きさを優先して選定した。
- 重要インフラ等の制御系に対する攻撃を優先しつつ、情報系に対する攻撃についても参考情報として有用なものを選定した。

分類	主な情報源
インシデント、脆弱性等の警報、動向レポート等	• ICS-CERT/US-CERT Alert • NIST National Vulnerability Database(NVD) • MITRE Common Vulnerabilities and Exposures (CVE)
インターネット脅威観測システムのレポート、国際会議等	• WCLSCAN(MRI)、JPCERT/CC、@police • 国際会議FIRST, APCERT、Blackhat等
セキュリティ情報を専門に扱うサイト等	• krebs on security、SECURELIST、ScanNetSecurity、Darkreading、Security Next等

1.2 インシデント事例に関する調査項目

- 付録のインシデント概要一覧では、インシデントごとに下記の項目について要点を整理した。
- (6)影響・被害、(7)原因・攻撃手法などをもとに、研究開発に参考となるインシデントを抽出した。

調査項目		説 明
(1) 事例名		事例を端的に示す名称
(2) 時期		報告または報道された日時
(3) 国		発生国・地域
(4) ターゲット分類		**[1] 制御システム** [1.1] 産業制御システム(ICS)【管理主体が事業者】 [1.1.1] 重要インフラ [1.1.2] 重要インフラ以外のICS [1.2] コンシューマIoT機器【管理主体が個人】 **[2] 情報システム** [2.1] 重要インフラ分野における事案 [2.2] その他事案
(5) 産業分野		**[1] 重要インフラ** （14分野：情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油） **[2] 重要インフラ以外** [2.1] 制御系 [2.1.1] 産業系ICS（FA、制御システム一般） [2.1.2] コンシューマ 系IoT機器（自動車、家電、ヘルスケア機器等） [2.2] 情報システム(業務システム、予約システム等)
(6) 影響・被害		インシデントによる被害などの影響（情報があれば定量値（損害額、事業停止時間、復旧コストなど）を含む）
(7) 原因・攻撃手法		原因となった脆弱性などの問題やそれに対する攻撃手法
(8) 概要		インシデントの対象、地域、攻撃者等の概要
リスクレベル	**(9) 影響度**	「影響・被害」などから可能なものについては影響度を段階評価する
	(10) 発生可能性	「原因・攻撃手法」などから発生可能性を段階評価する
(11) 攻撃タイプ		抽出した「原因・攻撃手法」全体をもとに、MITRE CAPEC等の攻撃分類を参考に設定した攻撃タイプ
(12) 情報源		URL、文献名など

1.3 攻撃タイプの分類

- 攻撃手法や対策技術の関連性から大きな単位で攻撃タイプを分類した。
- MITRE/NISTによる分類表CAPEC, CWE, ISMS脅威分類、JPCERT/CCインシデント分類などを参考に分類した。
- 本攻撃タイプ分類は排他的ではなく、ひとつのインシデントが複数の攻撃タイプに対応付けられるケースがある。

攻撃タイプ	概 要	対策例
DDoS/DoS等	ネットワークに接続されたサーバやPC、ネットワークを構成する機器や回線等のネットワークリソースに対して、過剰なリクエストやトラフィックの負荷をかけることで、サービスを提供できないようにする攻撃。	ブラックホールルーティング、パケットフィルタリング、CDN、エッジ通信遮断
マルウェア感染	ウィルス、ワームなど不正かつ有害に動作させる意図で作成された悪意のあるソフトウェアの感染等。バッファオーバーフローなどの脆弱性を利用してファイルダウンロードや実行や、メール添付ファイルをユーザに実行させるなどして感染する。	感染防御（経路別：メール添付ファイル、Web脆弱性、USB等）感染検知・隔離・検疫
不正アクセス（アクセス制御侵害）	アクセス制御、認証等を回避する攻撃。パスワード設定の不備、バグ、認証の欠落や、窃取したパスワードや証明書の悪用、計算力を使ってパスワードを破るブルートフォース攻撃、クロスサイト・リクエスト・フォージェリ(CSRF)などを含む。	アクセス制御、IDS、ネットワーク監視、パスワード検査
インジェクション	サーバに対して、細工した入力を与えることで、想定外の動作や情報漏洩を引き起こさせる。SQLインジェクション、OSコマンドインジェクション、HTTPヘッダ・インジェクション、クロスサイトスクリプティング(XSS)などWEB脆弱性攻撃を含む。	入力データ検査、脆弱性対策、ファジング
標的型攻撃・フィシング・APT等(ソーシャルエンジニアリング等)	特定の対象を狙ってウィルス等を添付したメールの送信（標的型攻撃）、メールの読み手を騙し、WEBサイトなどに誘導し詐欺を働く手法(フィッシング）、特定の対象にフィッシングを行う（スピアフィッシング）などメール等により詐欺的な行為を行う。	コンテンツフィルタリング、警告
その他脆弱性攻撃等	上記に分類されないソフトウェアの問題点、設定の不備などに対する攻撃。	サプライチェーンセキュリティ、セキュアコーディング

2. 主なインシデントの全体概観

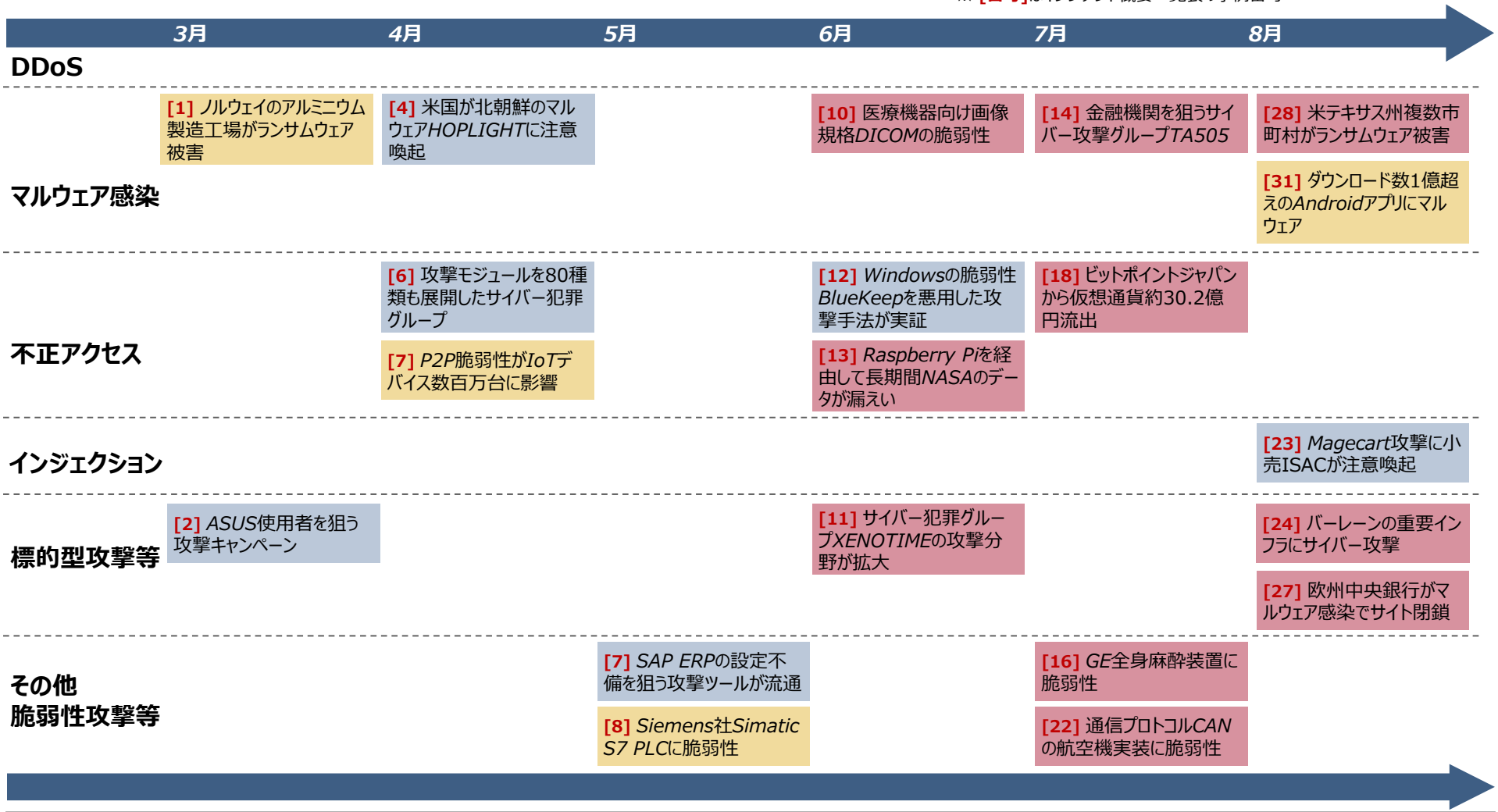
主なインシデントの俯瞰（2019年3月～8月）

- 重要インフラを狙う標的型攻撃が増加、手法も洗練化
- 人命に関わる制御機器の脆弱性によるリスクが拡大
- 管理されていないIoTデバイス経由の不正アクセスの脅威が拡大

凡 例：重要インフラ／その他制御系／情報系

※ 事例は、主な攻撃分類、報告日等で配置

※ [番号]はインシデント概要一覧表の事例番号



主なインシデントの俯瞰（2019年9月～12月）

- 機器脆弱性の発見等、コンシューマー製品が攻撃対象とされる事例増加
- 重要インフラ組織でのランサムウェア被害、フィッシング被害が多発
- ITシステムから制御システムを侵害されるリスクの顕在化

凡例：重要インフラ／その他制御系／情報系

※ 事例は、主な攻撃分類、報告日等で配置

※ 凡例、**[番号]**はインシデント概要一覧表の事例番号

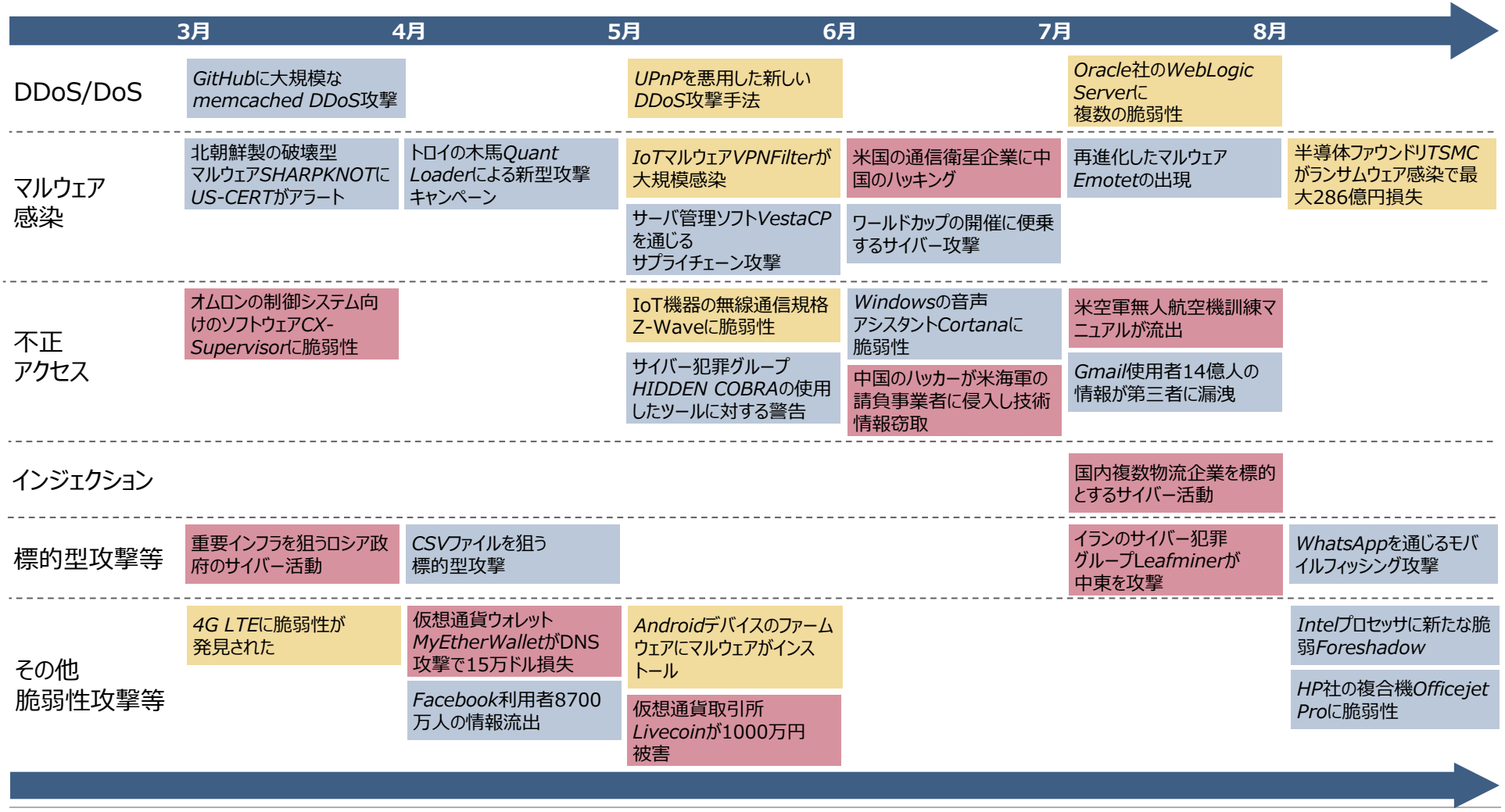
	9月	10月	11月	12月
DDoS			**[59]** *TCP*増幅を利用する*DrDoS*攻撃が増加	
マルウェア感染	**[34]** サイバー犯罪グループ*APT10*が東南アジアの医療関連施設を攻撃 **[44]** ドイツ自動車部品メーカーがマルウェア感染で3億円以上の損失	**[50]** 郵便料金計器メーカーの世界最大手米*Pitney Bowes*社がランサムウェア被害 **[55]** オーストラリアの重要インフラや医療機関がマルウェア*Emotet*に感染	**[60、63]** メキシコ石油公社*Pemex*やニューヨーク警察がランサムウェア被害 **[64]** 悪意のある*SDK*が再び*Google Play*に混入	**[68]** 中東の組織を標的とするディスクワイピングマルウェア
不正アクセス	**[43]** エアバスに対するサプライチェーン攻撃が発生 **[35]** 約30機種の*GPS*トラッカーに脆弱性		**[57]** *Siemens*社*PLC*の悪用可能な隠れ機能が発覚	**[70]** 自動車業界を狙うサイバー犯罪グループ*APT32*
インジェクション				**[67]** バンキング型トロイの木馬*TrickBot*が日本まで蔓延
標的型攻撃等		**[51]** スマートスピーカー*Amazon AlexaとGoogle Home*を悪用する攻撃手法		
その他脆弱性攻撃等	**[36]** 米国の電力網に対する初のサイバー攻撃	**[46]** *IPnet*ソフトウェアの脆弱性が医療分野等の数百万の組込みデバイスに影響 **[47]** *Android*デバイスに影響するゼロディ脆弱性*use-after-free*	**[58]** *Medtronic*社の電気手術器に複数の脆弱性	**[66]** 全てのバージョンの*Android*に影響する脆弱性*StrandHogg*

【参考】主なインシデントの俯瞰（2018年3月～8月）

- サプライチェーンの複雑化に伴う脅威の拡大
- 仮想通貨への脅威の変化、ウォレットへの攻撃の増加

凡例：重要インフラ／その他制御系／情報系

※ 事例は、主な攻撃分類、報告日等で配置



【参考】主なインシデントの俯瞰（2018年9月～2019年2月）

- 検出回避型、自己拡散型などランサムウェアの脅威が多様化
- 攻撃キャンペーンにおける新たな攻撃手法のPoC（概念実証）活動
- サイバー攻撃のサービス化・モジュール化による攻撃ハードルの低下

凡例：重要インフラ／その他制御系／情報系

※ 事例は、主な攻撃分類、報告日等で配置

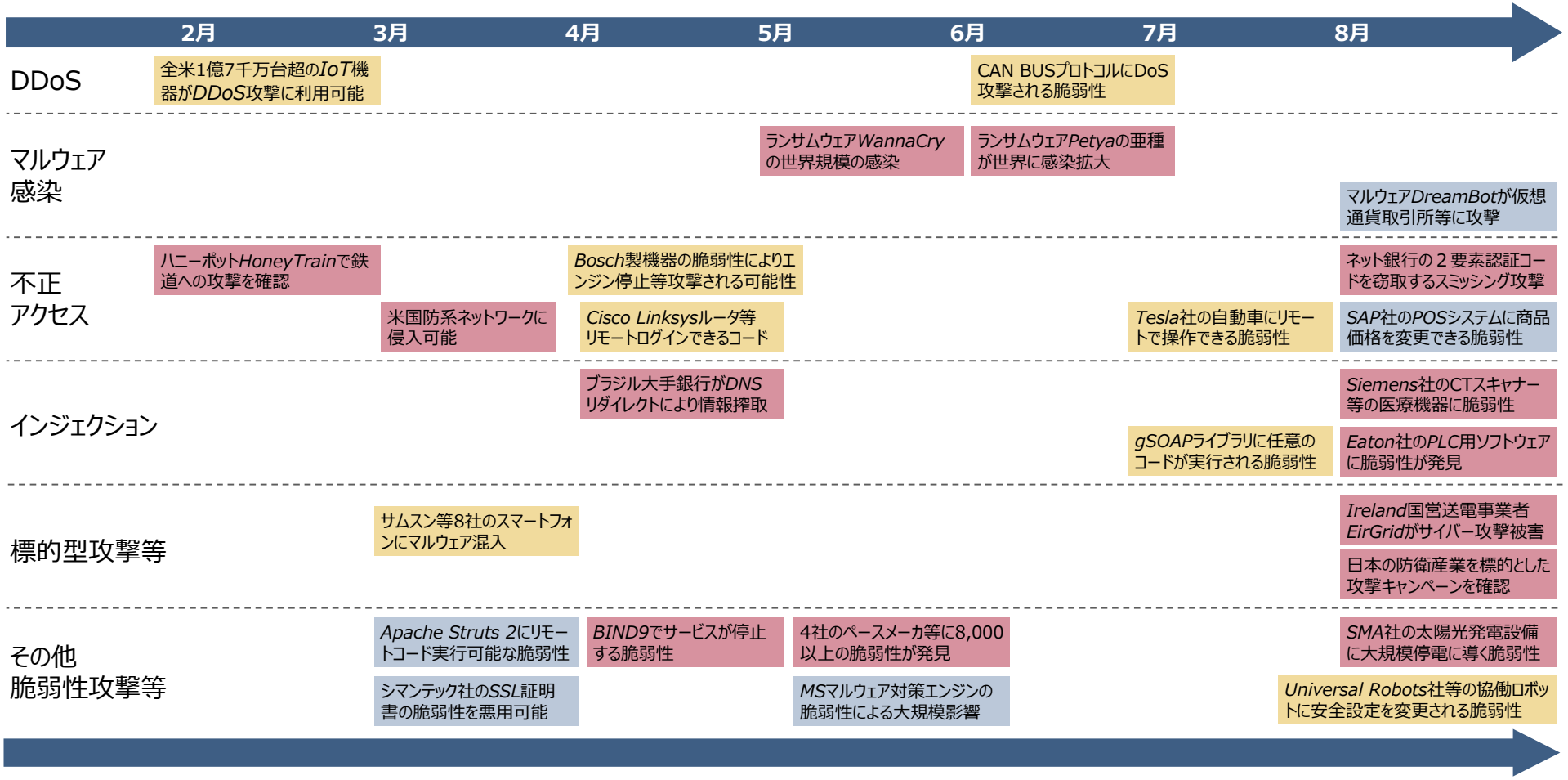
	9月	10月	11月	12月	1月	2月
DDoS/DoS					1秒あたり5億パケットのDDoS攻撃が観察	
マルウェア感染	新たなIoTマルウェアToriiの出現	宇陀市立病院がランサムウェアGandCrab被害		ランサムウェSatanの亜種Luckyの出現	Google Cloud Platformを通じて金融機関を狙う攻撃	EXEファイルを装うMacOSのマルウェア
	東京オリンピックに便乗するマルウェア攻撃	米国下水道局がランサムウェア被害		Adobe Flashの脆弱性を狙うゼロディ攻撃		Linuxサーバを狙うマルウェアSpeakUp
不正アクセス	70種類以上のルータを狙うGhostDNS		自動車Bluetooth通信を狙うCarsBlues	オープンプラットホームKubernetesに脆弱性	横河電機のライセンスマネージャーサービスにアクセス制御の脆弱性	オーストラリアの議会はサイバー攻撃に遭う
	仮想通貨取引所Zaifが不正アクセスにより約67億円損失		複数無線LAN製品のBluetoothチップに脆弱性	Quora社プラットフォームから1億人の個人情報流出	ボーイング757機に対する遠隔のサイバー攻撃	約27億件の情報漏洩を含むファイル群「Collection#1」の投稿
インジェクション					米連邦政府機関でDNSインフラの改ざん	
標的型攻撃等		サイバー犯罪グループCOBALT DICKENSが教育機関を攻撃	サイバー犯罪グループWhite Companyによるパキスタン空軍への攻撃	政府機関狙い攻撃キャンペーンOperation Sharpshooter		
			中東における攻撃キャンペーンNATPionage			
その他脆弱性攻撃等	ボットネットを提供するマルウェアサービスの発見		Intel CPUにサイドチャネル攻撃を受ける脆弱性PortSmash	Google Cloudを介して英米の銀行を標的にするフィッシング攻撃	Microsoft WindowsとWindows Serverの重大な欠陥	暗号化プロトコルTLS 1.2に脆弱性
			Schneider Electric社の制御機器に脆弱性	SQLiteにバッファオーバフローの脆弱性	RFハッキングを経由し建設現場機械へ攻撃	

【参考】主なインシデントの俯瞰（2017年2月～8月）

- ランサムウェアWannaCry, NotPetya, BadRabbitなどによる大規模被害、重要インフラ組織への影響
- 自動車、医療機器など安全性に係わるIoT機器で脆弱性が継続的に発覚

凡例：重要インフラ／その他制御系／情報系

※ 事例は、主な攻撃分類、報告日等で配置



【参考】主なインシデントの俯瞰（2017年9月～2018年1月）

- 広範囲に影響する基盤部の脆弱性発見が相次ぐ：WPA2、Bluetooth等の無線通信プロトコル、RSAライブラリ、CPU投機機構
- TRITON, DragonFly2.0など重要インフラへの脅威に対して米国政府(DHS/US-CERT)が公式に関係業界に警告

凡 例　重要インフラ　その他制御系　情報系

※ 事例は、主な攻撃分類、報告日等で配置

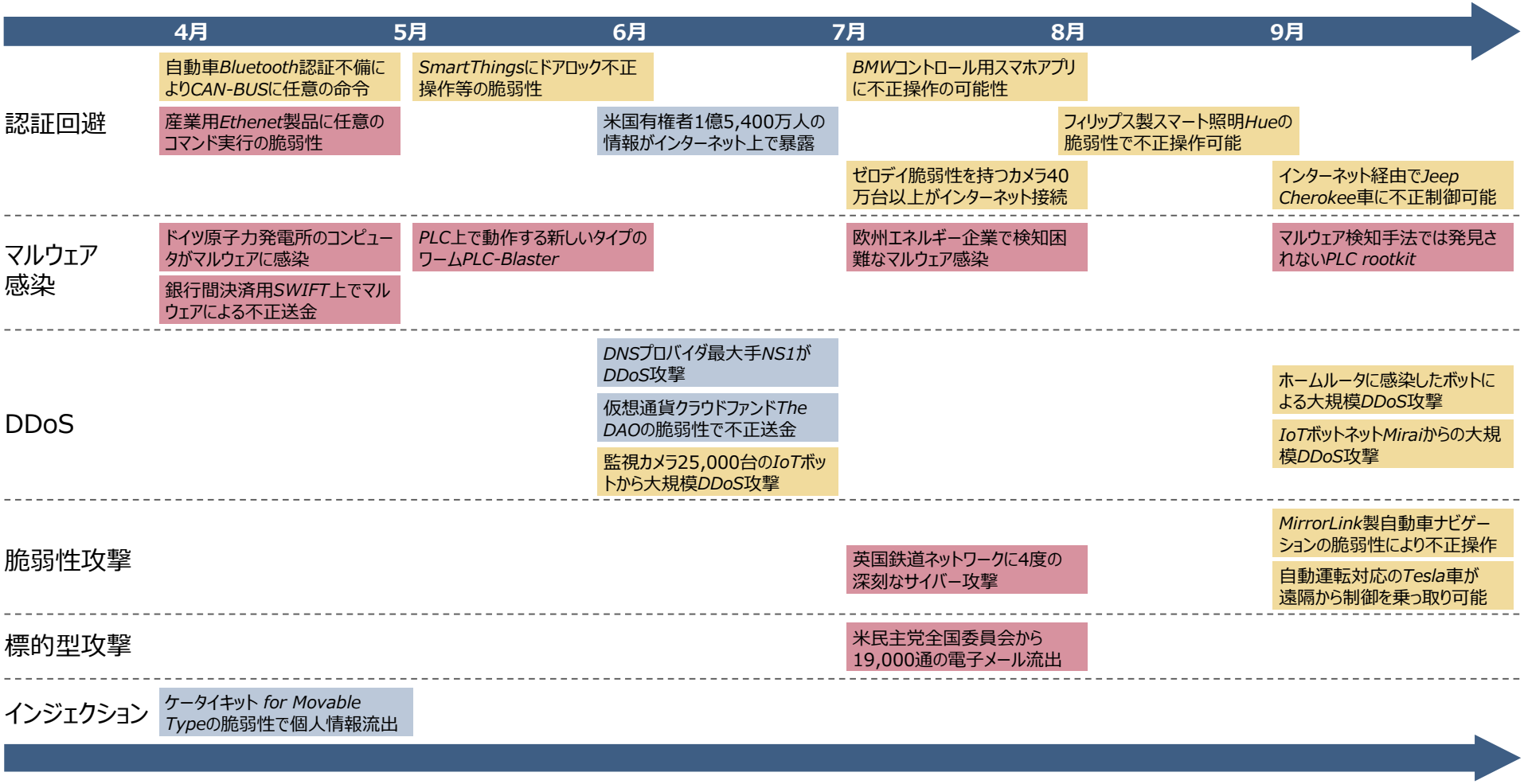
	9月	10月	11月	12月	1月
DDoS		スウェーデン運輸当局のITシステムにDDoS攻撃			
マルウェア感染		ランサムウェアBad Rabbitによりキエフ地下鉄等の機関に影響	google検索のSEOポイズニングによるマルウェアの拡散 MS Officeの脆弱性を悪用するマルウェアCobaltの登場	産業制御系攻撃フレームワークTRITONが重要インフラを攻撃	ARCプロセッサをターゲットするマルウェアSatoriの亜種 医療機関をターゲットにするランサムウェアSamSamの亜種
不正アクセス	ドイツの電子投票システムに選挙結果が操作される脆弱性 スマートホームInsteon HubとWink Hub 2に不正操作の脆弱性 米国21州の選挙システムに不正侵入	ダークウェブでRDPの認証情報36,000件以上が売買される	米Uberから個人情報5,700万件の流出を公表 MacOS High Sierraに容易にroot権限取得できる問題 ボーイング757型機のシステムに無線通信を介して侵入可能	攻撃グループMoneyTakerが米露の銀行から数百万ドルを窃盗 Intel MEの隠し機能God Modeを利用できる脆弱性 53億台のデバイスに影響を与えるBluetoothの脆弱性 医療情報管理システムのオープンソースOpenEMRに脆弱性	Oracle社WebLogicの脆弱性を利用する仮想通貨のマイニング 仮想通貨取引所Coincheckから約580億円分の仮想通貨が流出
インジェクション	Bluetoothにリモートコード実行およびMITM攻撃される脆弱性 Equifax社がStruts2脆弱性により最大1億4300万人分の情報漏洩			データベースをターゲットするHex-Men攻撃 PLCのWAGO PFC200に脆弱性	
標的型攻撃等		米欧重要インフラ事業者等に攻撃キャンペーンDragonFly2.0	カリフォルニア州サクラメント運輸当局へのサイバー攻撃	攻撃ツールCopperfieldは中東の重要インフラ企業を標的に	
その他脆弱性攻撃等		Infineon社組込み用RSAライブラリの脆弱性 無線LANのWPA2におけるプロトコル脆弱性	北朝鮮攻撃グループHIDDEN COBRAによるサイバー攻撃	Bank of America等のアプリに中間者攻撃にされる脆弱性	Intel, AMD,ARM等のCPUの脆弱性により大規模の影響

【参考】主なインシデントの俯瞰（2016年4月～9月）

- 注目事例では、認証回避、マルウェア感染、DDoS攻撃が多い
  重要インフラでは、新たなPLC系マルウェアが登場

凡例：重要インフラ／その他制御系／情報系

※ 事例は、主な攻撃分類、報告日等で配置

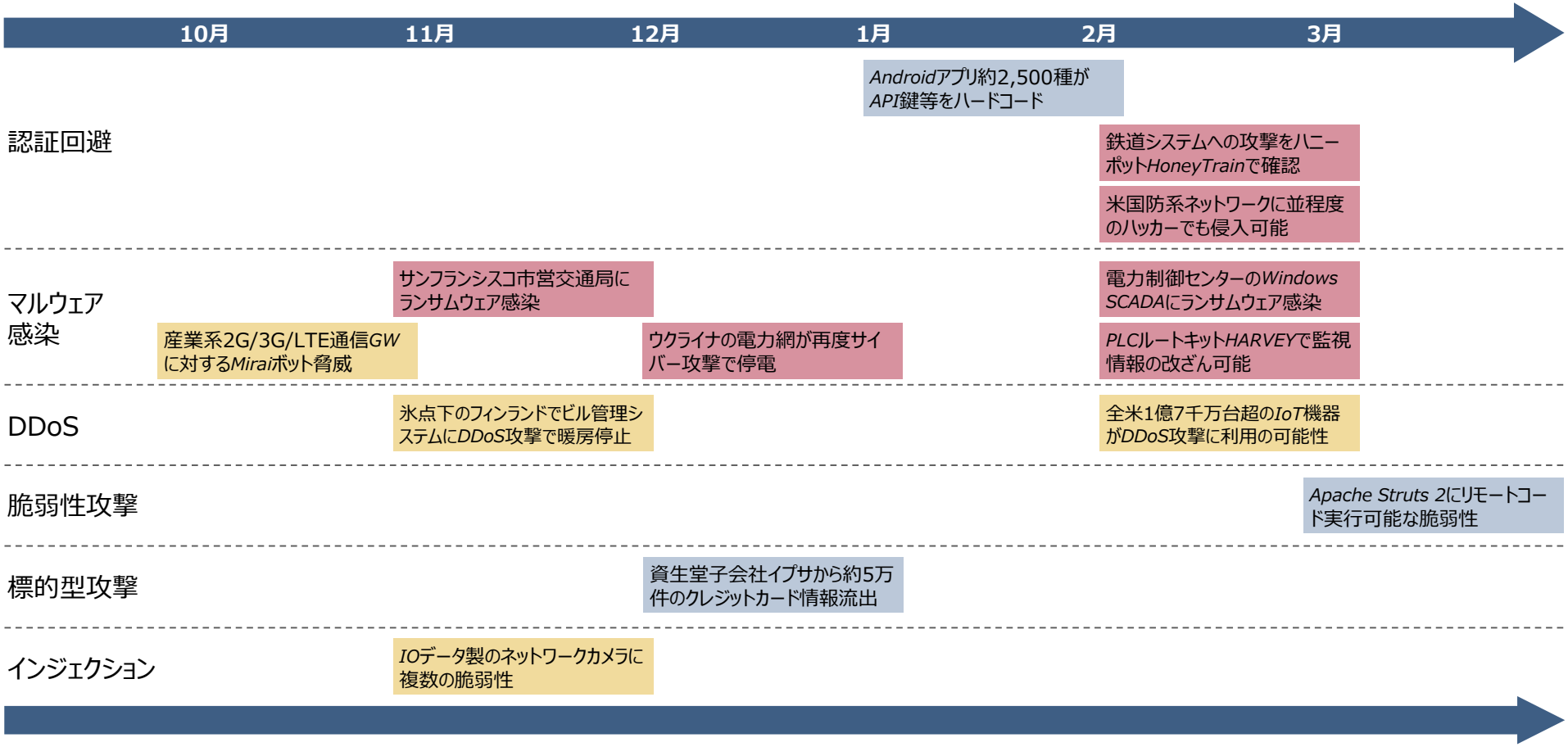


【参考】主なインシデントの俯瞰（2016年10月～2017年3月）

- 利用者に直接影響を与えたインフラ系のインシデントが発生
  （ウクライナ停電、サンフランシスコ市営交通等）
- Mirai等のIoTボットネット系のインシデントが継続的に発生
- 重要インフラにおいてもランサムウェア被害の発生

凡例　重要インフラ　その他制御系　情報系

※ 事例は、主な攻撃分類、報告日等で配置



【参考】脅威トレンドと技術課題 2018年度（1/2）

脅威のトレンド	関連脅威情報	対策区分	今後期待される対策・技術課題（例）
サプライチェーン・セキュリティの脅威の拡大	● 半導体ファウンドリTSMCがランサムウェア感染で最大286億円損失 ● US-CERTはAPT攻撃について警鐘を鳴らす ● 米国政府がHuawei通信機器排除を立法化 ● Androidデバイスのファームウェアにマルウェアがインストール	防御	● **セキュリティ・アシュアランスケースのモデル作成** 検証結果やログなどエビデンスに基づき、論理的にセキュリティが確保されていることを、他のステークホルダーに保証するための体系のモデルを作成する。
		検知 抑止	● **信頼のトレーサビリティ確保** 信頼の起点の創出・検証、信頼チェーンの流通、維持を実現するために、信頼の起点となる対象と記述方法を具体的に体系化し、サプライチェーンにおける組織を横断したトレーサビリティを確保するシステムを開発する。セキュリティ・アシュアランスケースの手段として有効である。
ルータ等のIoT機器への攻撃の多様化	● IoTマルウェアVPNFilterが大規模感染 ● マルウェアslingshotによるMikroTikルータ攻撃 ● 70種類以上のルータを狙うGhostDNS ● 攻撃キャンペーンRoaming Mantisの進化 ● 新型IoTマルウェアの検出数推移（統計情報）	防御 検知	● **包括的なインテグリティ検査** ドロッパーやアップデートにおけるDLLのすり替えなどによる不正なソフトウェアのインストールやネットワーク設定の書換えなどを包括的にシステムや環境の完全性を検証する技術を開発する。
		検知	● **プロトコルベースの異常検知** 汎用情報系のプロトコルや制御系の固有プロトコルなどプロトコルや利用環境に応じた正規通信パターンの情報を用いて、高精度な異常検知を行う手法を開発する。
ランサムウェアの多様化	● TUBAME観測データによるランサムウェアポートへの攻撃の増加（統計情報） ● ランサムウェアSatanの亜種Luckyの出現 ● 米政府はランサムウェアSamSamに対する注意喚起 ● 宇陀市立病院がランサムウェアGandCrab被害	防御	● **サーバ系アップデート技術の高度化** サーバ機能を停止せず、アップデートを実施し、瞬時に切替を行うことで、サーバの脆弱性を狙うマルウェア感染のリスクを低減する。
		検知	● **感染活動の検知・防御技術の開発** ランサムウェアの振る舞いや事前知識をもとに、ランサムウェアの自己増殖、継続的なアクセスなどを早期に検知・防御することで、ランサムウェアの増殖を低減する技術を開発する。

【参考】脅威トレンドと技術課題 2018年度（2/2）

脅威のトレンド	関連脅威情報	対策区分	今後期待される対策・技術課題（例）
サイバー攻撃のビジネス化、モジュール化	● ボットネットを提供するマルウェアサービスの発見 ● US-CERTが主要サイバー攻撃ツールについて警報 ● 新たなIoTマルウェアToriiの出現	検知	● **マルウェアサービスの探索検知技術** インターネット上のトラフィックパターンからボットネットを提供するマルウェアを効率的に検出する技術を開発する。
		適応	● **脅威情報の共有管理システムの構築** サイバー攻撃のビジネス化、モジュール化情報をいち早く共有・管理し、防御のための参考情報として参照できる情報共有システムを開発する。
組織アカウントへの不正アクセスの脅威拡大	● ICS-CERT Monitor（統計情報） ● 米連邦政府機関でDNSインフラの改ざん ● 約27億件の情報漏洩を含むファイル群「Collection#1」の投稿 ● サイバー犯罪グループCOBALT DICKENSが教育機関を攻撃	検知	● **アカウント不正アクセス検知技術** 大学や大規模組織のアカウントについて、網羅的に利用状況やアクセスパターンに基づき不正アクセスの可能性を検知する技術を開発する。
情報系ネットワークからICSへの侵入攻撃の増加	● 横河電機のライセンスマネージャーサービスにアクセス制御の脆弱性 ● RFハッキングを経由し建設現場機械へ攻撃 ● ICS-CERT Monitor（統計情報）	検知	● **ネットワーク接続性検証技術の検証** 制御システムネットワークに接続可能な経路やサービスを網羅的に探索し、アクセスルートの発見と防御のために利用できる技術を開発する。

【参考】脅威トレンドと技術課題 2017年度（1/2）

脅威のトレンド	関連脅威情報	対策区分	今後期待される対策・技術課題（例）
(1)ランサムウェア被害の大規模化	● WannaCry大規模インシデント ● BadRabbit地下鉄等影響 ● Petyaランサムウェア亜種 ● 新型ランサムウェアの増加傾向(McAfee統計情報等)	検知 防御	● **SMB等の脆弱性スキャン・アップデートの自動化** セキュリティ対策の自動化と標準化を目指したSCAPプロトコルなどを活用し、脆弱性情報を早期に流通させ、脆弱性スキャン・アップデートの自動化を進める。
		検知 適応	● **攻撃コードのシグニチャの迅速な流通基盤** WEB上で開示流通する攻撃コードに対してシグニチャベースの検知情報を迅速に流通し攻撃コードを検出する基盤を構築する。
		防御	● **水飲み場攻撃に対応したフィルタリング技術** 水飲み場攻撃サイトの情報を共有管理し、エンドユーザのアクセスサイトに対する警告・フィルタリングによる防御を行う。
(2)IT基盤部の深刻な脆弱性	● CPU投機機構の脆弱性 ● RSAライブラリの脆弱性 ● WPA2、Bluetooth等の無線通信プロトコルの脆弱性 ● macOS root権限脆弱性	適応 検知	● **脆弱性情報の共有管理の自動化・迅速な流通基盤** CPU,ファームウェアを含む広範な脆弱性情報を共有管理し、自動的に迅速に流通管理する基盤を構築する。
		適用 検知	● **ファームウェア等のアップデート手段の共通化** IoT機器のファームウェアのアップデート手段を共通化し、ネットワークを介して安全かつ自動的にアップデートできる仕組みを構築する。
		抑止 防御	● **製品認証の強化** IoT機器の脆弱性対策等の検査を含む製品認証制度の運用を図る。
(3)ファイルレス型マルウェア	● MS Officeの脆弱性を悪用するマルウェアCobalt ● Google Apps Scriptの脆弱性を悪用したマルウェア ● マルウェアLokiの新たな攻撃手法 ● 新型リモートアクセストロイの木馬TelegramRAT ● ファイルレス攻撃がランサムウェアに多用(Security Predictions for 2018　Paradigm Shifts)	検知	● **ファイルレス攻撃に対応したアノマリー検知技術** ファイルレス攻撃で利用されるWindows 管理ツールPower Shellの振舞いを分析することで、悪用に関する兆候を検知する技術を開発する。
(4)重要インフラ事業者への脅威の拡大	● 産業制御系をターゲットにしたマルウェアTRITON ● サイバー攻撃キャンペーンDragonFly2.0	検知 防御	● **シグニチャベースの危険コマンド検知技術の開発** 制御ネットワーク上のマルウェア転送など危険なコマンドを検知する技術を開発する。
		検知 抑止	● **おとりサーバ・偵察行動の検知技術の開発** 制御ネットワーク上のおとりサーバ、マルウェアの偵察行動を検知する技術を開発する。
		抑止 防御	● **内部犯行を抑止・防御する技術の強化** ログ監視、アクセス制御の強化により内部犯行を抑止・防御する技術を強化する。

【参考】脅威トレンドと技術課題 2017年度（2/2）

脅威のトレンド	関連脅威情報	対策区分	今後期待される対策・技術課題（例）
(5)仮想通貨に係わるサイバー攻撃	● 仮想通貨取引所Coincheckからの仮想通貨流出 ● マルウェアDreamBotが仮想通貨取引所等に攻撃 ● 仮想通貨取引所Zaifにおける不正出金 ● 仮想通貨取引所EtherDeltaのDNSサーバへの不正侵入	防御	● **仮想通貨の効率的な鍵管理方式の開発** 公開鍵暗号ペアの作成、ウォレットアドレス作成、トランザクション作成、トランザクションの署名等のステップを安全に効率行う方式を開発する。
		防御	● **アクセス制御の強化** 組織の情報システムへのアクセス制御の強化により、取引所システムへの不正アクセスを防止する。
(6)DrDoS攻撃の脅威拡大	● 複数の手法を組み合わせたDrDoS攻撃の増加(Arbor) ● 分散キャッシュサーバmemcachedを悪用したGithubサイトへの史上最大級1.35TbpsのDrDoS攻撃	防御 検知	● **DrDoS攻撃の踏み台サーバの設定検査技術の開発** DrDoS攻撃の踏み台のターゲットとなるサーバに対してサービス許可範囲などの設定の不備を検査する技術を開発する。
		検知 防御	● **DrDoS攻撃観測技術の開発** DrDoS攻撃を観測することを目的としたおとりリフレ工ターを運用することにより攻撃の踏み台にされるリフレクタの視点から攻撃を観測する技術を進化させる。
(7)BEC（ビジネスメール詐欺）	● ビジネスメール詐欺によりJALが約3億8千万円の被害 ● 海外取引をする国内企業でもビジネスメール詐欺(BEC)が確認(情報セキュリティ10大脅威IPA)	防御	● **マルウェア感染による情報漏洩をを防ぐ対策** メールアカウントの認証情報だけでなく、標的企業の内部情報を窃取するキーロガーをはじめとするマルウェアの検知・防御技術の向上を実現する。
		防御	● **ソーシャルエンジニアリング攻撃を検知するメール対策技術** メールの内容からBECを検知するような判定技術、フィルタリング技術の精度向上を実現する。
(8)IoT機器のアクセス制御侵害	● SSH(22/TCP)やTelnet(23/TCP)等の認証不備を狙うMirai亜種等からの攻撃観測の増大(JPCERT/CCインターネット定点観測レポート) ● セキュリティ機能が乏しいIoT製品への攻撃(JASA)	防御	● **IoT機器のネットワーク監視・管理技術** 監視カメラ、ホームルーターなどの組込みLinux系IoT機器のTelenetサービス等の必要性に応じたサービス稼動監視・管理技術の確立
		防御	● **IoT機器に係わる認証制度の検討** IoT機器のサービスポートセキュリティ対策に関する基準の策定と認証制度の提供によるユーザへのアシュアランス確保と製品差別化の機会提供
		検知 抑止	● **インターネット観測システムとのシステム連携および情報共有** 国内で稼働中の主要なインターネット観測システムと連携し、IoT機器からの攻撃監視と情報共有による早期警戒システムの整備
(9)自動車、医療機器の脆弱性	● CAN BUSプロトコルにDoS攻撃される脆弱性 ● Siemens社のCTスキャナー等の医療機器に脆弱性	防御	● **セキュアコーディング、脆弱性検査の活用の啓発** インジェクション、バッファエラーなど脆弱性情報に焦点をあてた教材、脆弱性検査ツールの活用に関する教材の作成と教育
		防御	● **ソースコード解析による脆弱性検出技術** ソースコード、Webスクリプトなどのソースコード解析によるインジェクション、バッファエラー等の脆弱性の検出技術の高度化

【参考】脅威トレンドと技術課題 2016年度（1/2）

トレンド	関連脅威情報	対策区分	今後期待される研究開発・対策の方向性（例）
(1)IoTボットネットによるDDoS攻撃の拡大	● IoTボットネットMirai, Hajime等によるDDoS攻撃の拡大 ● 1Tbpsを越えるDDoSの広帯域化 ● インターネット広域観測においてIoTボットネット活動の上昇トレンド	検知抑止	● **インターネット広域観測システムと異常検知システムの情報連携による機能向上** 稼働している広域観測システムと異常検知システムを連携し、IoTボット等の最新の攻撃パターンや特徴などの情報を活用した異常検知技術の開発
		防御	● **IoT機器のサービスポートの体系的な監視・稼動管理技術** 監視カメラ、ホームルーターなどの組込みLinux系IoT機器等への脅威情報を活用したサービス監視・管理技術の整備
		防御	● **IoT機器開発者の意識啓発** Linux系IoT機器の開発者に対するサービス設定のセキュリティ強化に関する教育啓発
		防御	● **IoT機器の脅威に対応した機器認証の基準検討** IoT機器のサービスポートセキュリティ対策に関する基準の策定と認証制度の提供によるユーザへのアシュアランス確保と認証マークによる製品差別化の機会提供
(2)ランサムウェア被害の増加とインフラ事業者への拡大	● サンフランシスコ市営交通局、ブラジル電力、Rockwell等のランサムウェア被害 ● ランサムウェア被害の増加トレンド (McAfee Threat Report 統計情報等) ● ランサムウェアの種類増加トレンド (Symantecレポート)	防御対応	● **ランサムウェア等の脅威動向に対応した意識啓発** 比較的新しいランサムウェア被害の事例集、予防方法、感染時の対処法などについてインフラ事業者を想定した意識啓発の教材開発
		防御	● **最新の脆弱性情報による体系的なマルウェア感染防御** マルウェア感染の原因となるバッファエラー等の脅威の動向に対応したコード検査技術、セキュアコーディング手法の開発
(3)認証不備に関わる脅威の拡大	● 自動車OBD-IIポートに接続する制御機器、IoT機器の認証不備に対する攻撃の増大 ● 制御系における認証・アクセス制御、クレデンシャル情報管理の脆弱性件数の増大 (ICS-CERTレポート)	防御	● **認証・設定不備等に対する体系的な検査技術** IoT系や産業系に特有の認証不備の情報を活用しシステム全体の認証設定に対して、体系的なスキャン、ペネトレーションテスト等による設定不備を検出する技術の開発
		防御	● **認証不備等のインシデントに対応した意識啓発** インフラ事業者に対する認証設定の不備や対策、クレデンシャル情報管理に関する意識啓発のための教材作成と意識啓発の重点化
		検知	● **認証に対する攻撃パターン情報を活用したログ分析による侵入検知技術** 認証不備を悪用した侵入の攻撃パターンを活用した侵入検知やバックドア検知を高度化することにより早期の侵入検知を実現
		防御	● **リソース制約の強いIoT機器に対応した認証技術の高度化** 認証の基盤となる暗号技術、限られたリソースで安全な認証の実現技術、認証設定インタフェースの向上、認証設定の不備の自動検出機能の埋め込みなどによる高度化

※間接的な関連を含む

【参考】脅威トレンドと技術課題 2016年度（2/2）

トレンド	関連脅威情報	対策区分	今後期待される研究開発・対策の方向性（例）
(4)業務情報系から制御系への影響	● サンフランシスコ地下鉄など、業務情報系へのマルウェア感染による重要インフラへの影響 ● ウクライナ電力におけるアクセス権限の奪取 ● トロイの木馬のインシデント増大(MSIRレポート)	検知対応	● **フィッシング・トロイの木馬等の脅威動向に対応したフィルタリング技術** フィッシングメールの検出、トロイの木馬等の不正コード検出などによりユーザにアラートを送信する技術、不正コードの感染を検知する技術の高度化
		防御	● **マルウェア感染防御のための脆弱性対策技術（開発フェーズ）** バッファエラーなどマルウェア感染の原因となる脆弱性対策のためのソースコード検査技術の高度化
		検知対応	● **挙動情報を活用したマルウェアの異常検知技術（運用フェーズ）** マルウェアの感染時の通信やプロセスの動作を監視し異常検知する技術の高度化
(5)入力検証不備に関わる脅威の拡大	● 入力検証不備に関わる脆弱性の増加(ICS-CERTレポート) ● 港湾荷役システム、インテリジェント電力計測機器に対するインジェクション攻撃	防御	● **入力検査不備等の脅威情報を活用したソースコード解析による脆弱性検査技術** ソースコード、Webスクリプトなどの解析によるインジェクション等の脆弱性の検出技術の高度化
		対応	● **脆弱性情報の共有システムの連携インタフェースの基盤整備** インジェクション、バッファエラーなど脆弱性情報をタイムリーに共有し対策に役立てる仕組みの構築
		防御	● **セキュアコーディング、脆弱性検査ツールの活用の啓発** インジェクション、バッファエラーなど脆弱性情報に焦点をあてた教材、脆弱性検査ツールの活用に関する教材の作成と教育
(6) Fintechなど新たな領域の脅威	● 分散型契約管理プラットフォームEtheriumを活用したクラウドファンディングシステムの脆弱性 ● OTA(Over-The-Air)アップデートに関わる脆弱性 ● ドローンを用いたHue照明へのマルウェア感染	防御対応	● **新しい技術の評価検証環境の構築** SIPで開発される技術の検証と共に、IoTなど新たな領域の機能開発に伴い生じる脆弱性を事前に検証するための環境の構築
		防御	● **ブロックチェーン等の新たな機能に関わる設計検証技術** フォーマルメソッド等を活用したアルゴリズム等の設計検証の高度化
		防御	● **IoTなど新領域における人材の意識啓発** IoT化によるオープン化、新たな機能開発分野における技術者に対してセキュリティの意識啓発を行うための教材の作成と意識啓発の実施
		防御	● **OTAアップデート等のセキュリティ強化** 自動車、家電などOTAアップデートが一般的になると予想される中で、OTAアップデートのセキュリティを確保する技術を構築する

※間接的な関連を含む

3. 注目事例の要点

注目事例の一覧（2019年度）

事例1：アメリカ電力網に対する初のサイバー攻撃

事例2：NASAジェット推進研究所の組織内ネットワークに大規模な攻撃

事例3：バーレーンで重要インフラへのサイバー攻撃が継続

事例4：ASUSの自動更新 Live Update にマルウェア混入
（Operation Shadow Hammerとの関係性）

事例5：インドの原子力発電所にサイバー攻撃

事例6：「7pay」への不正アクセスにより5,500万円の被害

事例7：ランサムウェアによりノルウェイのアルミニウム製造工場が操業停止

【事例1】アメリカ電力網に対する初のサイバー攻撃

- 複数の小規模発電施設と中央制御施設をむすぶ通信が外部からの攻撃で短時間不通となる現象が繰り返し発生した[1][2]。
- 設置されたファイアウォールが外部からの間接的な攻撃によりリブートし、機能が復帰するまで通信が不能となる。
- ファイアウォールはインターネット上にあるベンダーのWebポータルサイトの影響をうけてリブートする脆弱性があった。
- 1回5分未満の通信不能な状態が繰り返し発生したが、発電設備や配電設備などには影響を及ぼす停電はなかった。

攻撃対象	アメリカ電力事業者の発電施設、中央制御施設
発生日時	2019年3月5日 9:00-17:00
影響・被害	カリフォルニア州・ユタ州・ワイオミング州の米西部地域にある電力網をコントロールするネットワークの一部に障害が発生したが、発電そのものや配電などには影響を与えなかったため停電などは発生しなかった。
原因・攻撃手法	複数の小規模発電施設と中央制御施設をむすぶネットワーク上にあるファイアウォールは外部のインターネット上のベンダーが提供するWebポータルサイトと連動しており、ファイアウォールの脆弱性によりWebポータルサイトへの攻撃によりファイアウォールのリブートを引き起こすことが可能であった。そのためベンダー側のWebポータルサイトへの攻撃が多数のファイアウォールに影響を与える結果となった。

注目点	脅威の概要と分析
間接的な攻撃	電力の運用で利用しているネットワークや機材への直接攻撃ではなく、（問題が発生した時点では）ファイアウォールの脆弱性によってファイアウォールとベンダーのWebサイトが連動する形になってベンダーWebサイト側からリブートを仕掛けることができた。このようなケースでは利用者である電力会社側での事前の防御はむずかしい。1点を攻撃することで、波状に影響が広がる問題点は概念的にはサプライチェーン攻撃と類似している。
モニタリングの不備	今回はファイアウォールがリブートするのに5分未満と短い時間で復帰していたので、影響は限定的。繰り返しネットワーク障害が発生しているにも関わらずリアルタイムで把握しておらず、問題が発覚後、システムログを精査し同様な攻撃があったことを確認したサイトもあった。死活監視など基本的なモニタリングがされていなかった。

[1] https://www.eenews.net/assets/2019/09/06/document_ew_02.pdf
[2] https://www.eenews.net/stories/1061111289

【事例2】NASAジェット推進研究所の組織内ネットワークに大規模な攻撃

- NASAは宇宙探査などのミッションを担当しているジェット推進研究所(JPL)の主要情報システムやネットワークへの侵入および情報盗取について報告[1]。
- 2019年4月に発覚したケースでは内部ネットワークに接続されている小型組込みコンピュータRaspberry Pi[2]を乗っ取り、情報の収集、外部からの侵入拠点、流出させるための中継点として利用していた。
- この攻撃により23ファイル（約500MB)が流出、うち2ファイルは武器輸出規制に抵触するものであった。

攻撃対象	米NASAジェット推進研究所
発見時期	2019年4月
影響・被害	外部からJPL内部ネットワークに長期間侵入されており、発覚までに10ヶ月は活動していたものと推定される。23ファイル(約500MB)が流出したとされており、2ファイルは武器輸出規制に抵触する内容であった。2019年6月公開のセキュリティ監査報告書において報告
原因・攻撃手法	JPLはシステムやネットワークのセキュリティには必要かつ十分なセキュリティ監査や運用がされておらず、そのため複数の脆弱性を抱えていた。中でも、JPL内ネットワークにカードサイズのコンピュータであるRaspberry Piが許可・登録なく接続されおり、そこが侵入者の活動拠点として使われていた。発覚まで推定10ヶ月にわたる内部ネットワークへの不正な侵入が行われていた。

注目点	脅威の概要と分析
不十分なセキュリティ運用	LANに接続するすべての機器はITSDB(情報技術セキュリティDB)への登録が義務づけられているが、登録されずに利用されている機器もあった。Raspberry Pi(IoT機器として紹介されるが機能はGNU/Linuxサーバーと同等)が許可・登録なく接続される。侵入者は、Raspberry Piの脆弱性を使い乗っ取り、不正活動の内部拠点として長期間にわたり利用していた。尚、インターネットからの不正侵入は外部利用者のアカウントを不正利用していた。
不十分なログ解析・ネットワーク運用	JPLのSOC(Security Operation Center)ではファイアウォールのセキュリティ・ログや、システムのログなどを十分に活用しておらず、長期間にわたり侵入者の活動などを察知することができていなかった。JPL組織内ネットワークには外部研究者や業者などもアクセスするが組織内で適切なネットワークセグメントを構築していなかった。

[1] https://oig.nasa.gov/docs/IG-19-022.pdf
[2] https://www.raspberrypi.org/

【事例3】バーレーンで重要インフラへのサイバー攻撃

- バーレーンの国内重要インフラおよびバーレーン国家安全保安局、内務省、第一副首相官邸といった政府機関に対して同時にサイバー攻撃が行われた（2019年8月7日付けウォール・ストリート・ジャーナル紙(WSJ)）
- 2019年7月にバーレーンの電力局及び水道局の複数のシステムをシャットダウンしたと報告される。
- 今回のサイバー攻撃はイラン政権が支援しておりペルシャ湾岸地域での軍事的緊張が高まっていると指摘している(WSJ)。

攻撃対象	バーレーン国内の政府機関及び重要インフラ
発見時期	2019年8月(WSJ紙で報道)
影響・被害	バーレーン政府の国家安全保安局、内務省、第一副首相官邸、電力局（電力管理システム）、水道局（水道管理システム）への侵入などが発覚した。電力及び水道はいくつかのシステムをシャットダウンした。
原因・攻撃手法	具体的な被害者や侵入されたネットワークなどの情報は開示されていない。内務省スポークスマンによれば2019年前半だけで政府機関に対して6百万回の攻撃、ウイルスなどが検知された電子メールが83万通を検知している。バーレーン当局は、イラン政権が背後にいる集団が引き起こしたサイバー攻撃で、目的は国内攪乱の予行練習もしくはデモンストレーションではないかと考えている。

注目点	中東の重要インフラにおける脅威の概要
活発なペルシャ湾岸地域でのサイバー攻撃事案	ペルシャ湾岸地域では2012年にコンピュータのファイルを破壊するマルウェアShamoonが流行したことで注目されたが、2019年には、さらにアップグレードしたShamoonが発見された。サウジアラビアとアラブ首長国連邦を中心に広まっており、中東に事務所を展開しているイタリアの石油会社 Saipemは300-400台のサーバー、100台のPCが影響を受けたと公表している。
物理的破壊の可能性があるマルウェア	2017年にはサウジアラビアの石油化学プラントで発見されたマルウェアTRITONは安全計装システム（SIS）のTriconexコントローラを不正操作することが可能であった。そのためシステムの停止や機能低下させるだけではなくプラントに対して物理的な破壊も考えられる状況であった。

[1] https://www.wsj.com/articles/high-level-cyber-intrusions-hit-bahrain-amid-tensions-with-iran-11565202488
[2] https://www.symantec.com/connect/blogs/shamoon-7
[3] https://www.fireeye.jp/company/press-releases/2017/attackers-deploy-new-ics-attack-framework-triton.html

【事例4】ASUS社PCの自動アップデートに高度なサプライチェーン攻撃

- ASUS社ノートPCにインストールされている自動アップデートユーティリティが改ざんされマルウェアを埋め込まれていた。
- 2019年1月にマルウェアがセキュリティ・ベンダーによって発見され「ShadowHammer」と命名される[1]。
- 2018年6月から10月までASUS社サイトから配布されていたとみられ推定50万～100万回ダウンロードされる。
- ShadowHammerと同様な仕組みをもつサプライチェーン攻撃が3社に対し行われていた。

攻撃対象	ASUS社自動アップデートユーティリティ
発見時期	2019年1月
影響・被害	ASUS社のノートPC製品にインストールされている自動アップデートユーティリティ「ASUS Live Update Utility」が改ざんされマルウェアが含まれていた。該当アップデーターには正当なASUS社の電子署名がつけられているため「正式版」としてみなされ改ざんは発見できない状態であった。汚染されたアップデーターは最大100万回ダウンロードされた可能性がある。
原因・攻撃手法	ASUS社内で電子署名が行われるまえに、アップデーターが感染されているが感染の過程など詳細は不明。ノートPCに感染した後、マルウェアが持っているMACアドレスのリストと比較し攻撃対象を選別し、不審な通信による発覚を回避している。対象となったノートPCに対する具体的な攻撃内容に関しての公表はなし。

注目点	ShadowHammerの特徴
正当な電子署名が行われている	アップデータに電子署名をおこなう前の開発過程のいずれかの時点でマルウェアが組み込まれているため、正当なASUS製としてインストールされ、セキュリティツールの検知対象とならなかった。汚染されたアップデーターが配布されていた期間は2018年6月から10月後半までとされているが、セキュリティ・ベンダーのKaspersky社が発見できたのは2019年1月と長期間発覚しなかった。2019年3月25日にWebメディアで取り上げられるまでは公開されていない情報だった。
同様なサプライチェーン攻撃を3カ所で確認	Kaspersky社によれば同時期に同様なサプライチェーン攻撃がElectronics Extreme社、Innovative Extremist社、Zepetto社の3社で発覚した。いずれも韓国の会社で、かつゲーム開発に関連している。

[1] https://securelist.com/operation-shadowhammer/89992/
[2] https://blog.kaspersky.co.jp/shadow-hammer-teaser/22850/

【事例5】インドの原子力発電所にサイバー攻撃

- インド最大のクダンクラム原子力発電所(KKNPP)がサイバー攻撃を受けたことを国営印原子力発電公社(NPCIL)が認めた。
- サイバー犯罪グループLazarus(HIDDEN COBRA)が作成した新しいマルウェアDTRACKが使われた。
- NPCILはサイバー攻撃による情報流出の噂を否定したが、Twitter上で原発サイトへのサイバー攻撃の証拠が暴露される。
- NPCILは一転してサイバー攻撃があったことを認めたが、 KKNPPの原子力制御系ネットワークへの侵入は否定した。

攻撃対象	グランクラム原子力発電所(KKNPP)
発見時期	2019年9月3日
影響・被害	マルウェアDTRACKがKKNPPのサイトに侵入・感染、DTRACKによりサイト内のネットワークにあるファイルが外部に流出した。9月3日に第三者がインターネット上で発見、9月4日にCERT-INが当局に通知した。NPCILは最初、サイバー攻撃の被害はなかったとしたが、後に一転して非原子炉プラント制御系ネットワークのみ影響があったと公表した。
原因・攻撃手法	DTRACKは、KKNPP内部ネットワークのファイルサーバに不正にアクセスするコードが含まれていることが分かった。2018年のATM侵入しカードデータを窃取するマルウェアATMDtrackと共通点が多く、2013年にLazarusの手によるスパイウェアDarkSeoulのコードにも類似していることがわかった。

[1] https://www.hindustantimes.com/india-news/cyber-attack-on-kudankulam-plant-network-not-possible/story-4b5QiRVGuTtTi4MlOexadL.html
[2] https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/

注目点	KKNPPへの問題点
DTRACK事件の経緯	2019年9月3日 アンダーグラウンドでKKNPPから流出したファイルが第三者に知られる。 9月4日 インドのCSIRT組織CERT-INからNPCILに通知された。 10月28日 Twitterの匿名アカウントが検体からKKNPP内部ネットワーク内のファイルサーバーにアクセスできるコードがあることを暴露。別にセキュリティ専門家が検体からDTRACKであることを確定させる。また。ネット上で話題になる。 10月29日 NPCILが公式にサイバー攻撃を否定したが、 10月30日 NPCILが一転して肯定。CERT-INからの連絡があったこと、サイバー攻撃があったことを認める。原子炉制御系ネットワークには影響がないとしている。
対策等	• DTRACKは既存のコードを利用しているため、マルウェア対策ソフトで検出できる可能性がある。 • 外部への流出などに関してはトラフィック監視、DLPなどで検知できる可能性がある。 • ナショナルCISRTと連携した迅速な対応が重要である。 • 業務情報系と制御系の境界防御、多重防御は、被害の拡大を抑える上で重要である。

【事例6】「7pay」への不正アクセスにより約3,800万円の被害

- 2019年7月1日に利用開始となったスマートフォン決済システムの7payが72時間も経たない間に不正利用が繰り返された。
- IDとパスワードにより不正ログインし、登録しているクレジットカードから金額をチャージされコンビニ店舗などで利用された。
- 多要素認証などが実装されておらずメールアドレスが不正確でも登録できるなどの不備があり専門家から厳しい指摘が相次いだ。
- 7pay社側は既にどこかで漏えいしているIDとパスワードのリストを使ったパスワードリスト攻撃であると見解を示した。

攻撃対象	7pay（スマートフォン決済システム）
発見時期	2019年7月2日
影響・被害	不正入手したIDとパスワードで7payアプリにログインし、クレジットカードから多額の金額をチャージしたうえで、コンビニ店舗で換金性の高い商品を大量に購入した。7&i社は7月末までで判明した被害者数は808人、被害総額38,615,473円と発表している。[1]
原因・攻撃手法	7&i社は、IDとパスワードを事前に入手するパスワードリスト攻撃である可能性が高いとする。7payの機能である外部 ID 連携・パスワードリマインダー、有人チャットによるパスワードリセット等が、不正アクセスの直接の原因となった事例は見つかっておらず、内部からの流出についても、実査も含め、確認調査を行ったが、明確な流出の痕跡は確認できないとしている。

[1]https://www.7andi.com/library/dbps_data/_template_/_res/news/2019/20190801_01.pdf

注目点	7payの問題点
7pay事件の経緯	7月1日 サービス開始 / 7月2日 ユーザが不正な利用を発見 / 7月3日 7pay社(当時)がホームページで告知・クレジット及びデビットカードからのチャージ利用を停止・海外IPからのアクセスを遮断 / 7月4日 現金チャージ利用を停止・新規会員登録を停止 / 7月5日 セキュリティ対策プロジェクト設置 / 7月6日 モニタリング体制の強化 /7月11日 外部 ID によるログイン停止 / 7月30日 7payから紐付いているグループ全体で利用するプラットホーム7iD のパスワードリセットの実施 / 8月１日 7payサービス廃止を決定 / 9月30日 サービス廃止
対策等	• 他サイトから流出したIDとパスワードを利用するパスワードリスト攻撃に対しては、多要素認証を取り入れることで防御力を高めることが必要。 • ユーザー側は同じパスワードを使い回さないという原則を守る。 • グループ各社、協力会社などのシステム開発体制が大規模である場合、一部の企業に不備があれば、影響が他に波及するリスクがあるため、セキュリティを確保するための検証体制、組織管理を整える必要性がある。

【事例7】ランサムウェアによりノルウェイのアルミニウム製造工場が操業停止

- ノルウェイのアルミニウム製造企業Norsk Hydroが暗号化型ランサムウェアLockerGogaの攻撃により被害が発生した。
- 米国事業所で発生した感染だが40ヵ国の同社事業所への感染拡大が見られたため社内間ネットワークを遮断した。
- 工場間を結ぶネットワークも遮断されたため、一部の工場は操業停止し、また他も手動に切り替えて操業することになった。
- 従業員35,000人は感染拡大を防ぐため利用しているPCの電源を切って電話とタブレットの電子メールのみで対応した。

攻撃対象	Norsk Hydro (アルミニウム製造会社)
発見時期	2019年3月19日
影響・被害	2019年3月19日夜に同社米国内事業所で感染が発生。翌日朝には40ヵ国に広がる同社の社内ネットワークを通して別の支社・事業所へ感染が拡大したことを確認。感染を防ぐため社内ネットワークを遮断、PC停止を行う。そのため一部の工場は操業停止し、他も手動に切り替え操業することになった。[1]
原因・攻撃手法	暗号型ランサムウェアでPC内のファイルを暗号化したのち、bitcoinでの支払いを求める脅迫文を提示する。管理者権限で暗号化を開始するが、その際、管理者パスワードを変更するため管理者にログインできなくなっている。実行ファイルにはALISA LTD社の正規の有効なデジタル署名がつけられている。外部との通信をしないタイプのため見つけ難い。感染経路は不明とされている。[2]

[1] https://arstechnica.com/information-technology/2019/03/severe-ransomware-attack-cripples-big-aluminum-producer/
[2] https://gblogs.cisco.com/jp/2019/03/talos-lockergoga/

注目点	LockerGogaについて
特徴	● 管理者権限で実行されるexeファイルに正規の有効なデジタル署名がつけられているなど周到な準備がされている。 ● LockerGogaは1つの実行ファイルで複数の機能を持ち実行時オプションで使い分ける。 ● 近年多くのマルウェアがC&Cと通信し、必要なモジュールをダウンロードするが、外部への通信を行わないため通信ログから感染しているPCを発見する方法が使えない。 ● 暗号化する際にランサムウェア検知を回避する工夫がされている。
対策等	• LockerGogaは、これまでのマルウェアやランサムウェアを発見する手法を回避する実装のため既存の方法では対策の有効性が低い。 • また感染経路も明らかにはなっておらず、具体的な境界防御のアプローチからの対策は難しい。 • Norsk Hydro社は全社をむすぶネットワークを遮断し感染の可能性のあるPCをすべて停止することで最低限の対処策を行った。 • データバックアップにより復旧の仕組みを作る。 • 最悪ケースに対する事前の危機管理・事業継続計画を策定し、適切に行動に移すことは必要。

【参考】 注目事例の一覧（2017年度～2018年度）

事例1　：サイバー犯罪グループHIDDEN COBRAの使用したマルウェアに対する警告

事例2　：Githubに対しトラフィック量1.35Tbpsのインターネット史上最大級DRDoS攻撃が「マルウエア

事例3　：マルチステージで感染を広げ攻撃を行うIoTマルウェアVPNFilter

事例4　：分散キャッシュサーバmemcachedを悪用したGithubサイトへの大規模DRDoS攻撃

事例5　：サイドチャネル攻撃Spectre、Meltdownに係わるCPU 脆弱性の脅威

事例6　：重要インフラをターゲットにしたマルウェアTRITONについて警告（米政府）

事例7　：Infineon社組込み用RSAライブラリの脆弱性

事例8　：新種ランサムウェアBad Rabbitによるキエフ地下鉄等への影響

事例9　：米重要インフラ事業者等に対するサイバー攻撃キャンペーン(Dragonfly2.0等)

事例10 ：ランサムウェアWannaCryの世界規模の感染インシデント

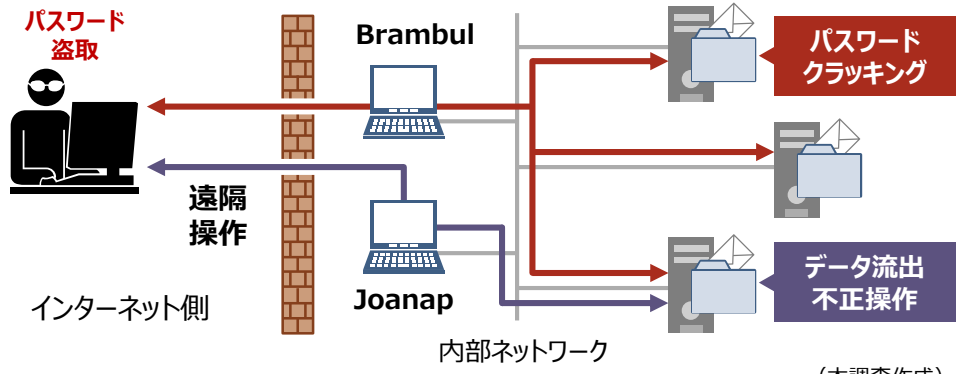
【事例1】サイバー犯罪グループHIDDEN COBRAの使用したマルウェアに対する警告

- US-CERTはサイバー犯罪グループ HIDDEN COBRAによって使われた遠隔操作ツール Joanap 及びSMBワーム Brambulについてテクニカル・アラート文章を公開した。
- 米国土安全保障省（DHS）とFBIの協働によりマルウェアの通信経路追跡や機能・属性の分析(indicators of compromise：IOC) が行われた。

攻撃対象	米国政府
発生日時	2018年5月29日(警告初版公開)
影響・被害	攻撃ツール Joanap及びBrambulを使った米国政府へのサイバー攻撃は北朝鮮政府が支援しているサイバー犯罪グループHIDDEN COBRAによるものと断定している。本アラートでは2009年以降同グループによるマルウェア攻撃が継続していることを警告している。
原因・攻撃手法	Joanapは遠隔操作ツール(Remote Access Tool：RAT)で感染先Windows PCを自由に操作することが可能。それによりファイルの流出だけではなく、さらに侵入先ネットワークを探査することが可能。Brambulは感染先ネットワーク内にあるSMBサーバ（ファイル共有）に対してパスワードを破りアクセスしその上にあるファイルなどを外部に流出させる能力を持っている

攻撃ツールの動作の仕組み

名 称	Joanap	Brambul
機 能	遠隔操作ツール	サーバーメッセージブロック(SMB)ワーム
詳細・特徴	PCに感染後、外部の犯罪グループ HIDDEN COBRAと通信を行いPCを自由に操ることが可能である。外部へファイルの流出をさせる、あるいは外部から新たな機能モジュールのインストールなどが行える。	内蔵のパスワード辞書を使い内部ネットワークのSMBファイルサーバへアクセス、感染した先のホストから電子メールを使いアクセスに成功したユーザ名・パスワードなど情報を外部に流出させる。



（本調査作成）

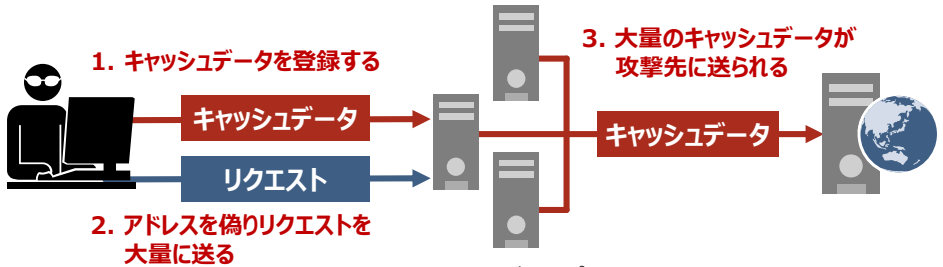
[1] https://www.us-cert.gov/ncas/alerts/TA18-149A

【事例2】Githubに対しトラフィック量1.35Tbpsのインターネット史上最大級DRDoS攻撃が発生

- WEBアプリケーションへのDBアクセスを高速化する分散型メモリキャッシュサーバmemcachedの脆弱性を悪用しデータを増幅した1.35Tbpsという史上最大級のDRDoS攻撃が発生。
- 攻撃を受けたソフト開発プラットフォームGithub[1]はAkamaiを使ってトラフィックを分散させ大きな混乱を回避した。

攻撃対象	米国空軍
発生日時	2018年2月28日 17:28(GMT)
影響・被害	Githubに対してmemcachedをリフレクタ(DDoS増幅サーバ）として使用したDRDoS攻撃が発生し1.35Tbpsの当時最大のトラフィック量を発生させた攻撃が行われた。GithubはAkamaiと協力しトラフィックを分散させるなどした結果、大きな混乱を回避した。
原因・攻撃手法	WebサイトなどのDB応答性能を上げるために利用されるmemcachedに攻撃用データをキャッシュとして事前に登録し、そのデータを攻撃先IPアドレスへ送りつける手法を使った。memcachedに対する不審なパケットの増加が観察されていたためJPCERT/CCは2月21日に注意喚起[2]を発表していた。設定ミスなどによりリフレクターとなるmemcachedがインターネット上に多数存在していた。

リスク要因	概 要
オープンな状態での運用	memcachedは外部からのアクセスを禁じる必要があるが、そのような設定にしていない脆弱なサイトが多数存在している。増幅率は約16,000倍前後(*1)と考えられる。
利用しているサーバサイト	オープンソースのmemcachedはデータベースやWebサーバなどの効率化のために2008年に作られた。処理の効率化を必要とするアクセスの多いサイトで使われるため、そのサイトが攻撃に使われた場合、それだけ脅威度があがる。



（本調査作成）

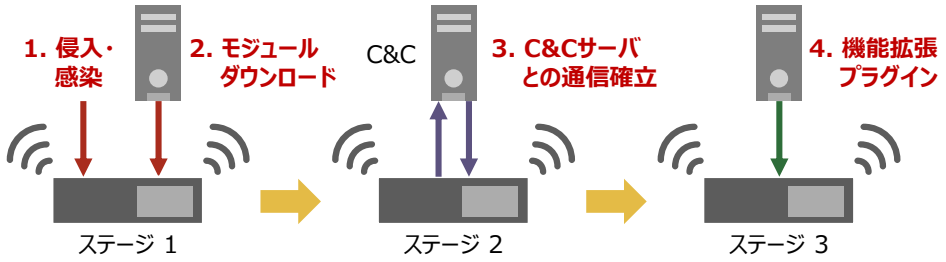
[1] https://githubengineering.com/ddos-incident-report
[2] https://www.jpcert.or.jp/at/2018/at180009.html
*1 本調査試算による

【事例3】マルチステージで感染を広げ攻撃を行うIoTマルウェアVPNFilter

- IoTマルウェアVPNFilterが世界54ヵ国、50万台以上のSOHO・家庭用ルータに感染が拡大（米Cisco System社セキュリティチームTalosが報告[1]）
- VPNFilterはステージによってプラットホームの役割が変化し、またプラグイン・モジュール機能により感染拡大・攻撃・情報収集など柔軟に変化することが可能である。

攻撃対象	米国空軍
発生日時	2018年5月23日(情報公開日)
影響・被害	Mikro Tik、NETGEAR、TP-Linkなどの小規模事業所・SOHO・家庭用ルータをターゲットにしたマルウェアで世界54ヵ国、総計50万台以上に感染を広げた。QNAP社のNASデバイスも感染・攻撃対象である。のちにASUS、D-Link、HUAWEI、Linksys、Ubiquiti、ZTEなどの複数のベンダ機材にも感染が拡張していった。
原因・攻撃手法	ステージ(1)感染初期、(2)拡充期、(3)活動期という3つの段階で変化し、ステージ3では活動目的にあわせたモジュールをプラグインとしてダウンロードし情報収集・DDoS攻撃・感染拡大といった柔軟な拡張が可能である。過去の脆弱性に関しても多くの攻撃方法が用意でき、また新規の脆弱性への対応もすばやく行うことが可能である。

ステージ	機 能
ステージ1（感染初期）	ターゲットであるIoTデバイスに感染したのち、マルウェア・プラットホームを構築するために必要なモジュールをダウンロードし、システムに展開する。
ステージ2（拡充期）	C&Cサーバと通信を行いボットとして活動可能な状態になる。基本的な攻撃や感染拡大の機能はすでに組み込まれている。
ステージ３（活動期）	必要に応じて外部からプラグインをダウンロードし機能として組み込む。攻撃・情報収集・感染拡大など多種多様な活動が可能。Modbus SCADA プロトコルの監視も可能



（本調査作成）

[1] https://gblogs.cisco.com/jp/2018/05/talos-vpnfilter/?doing_wp_cron=1541007439.4221110343933105468750

【事例4】分散キャッシュサーバmemcachedを悪用したGithubサイトへの大規模DRDoS攻撃

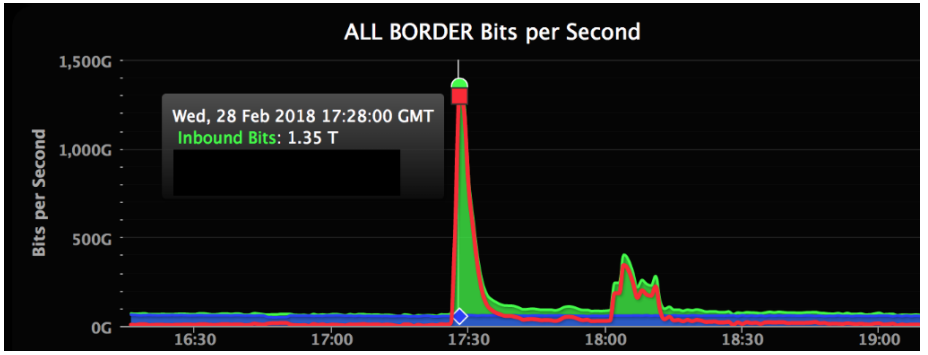
- Githubサイトはインターネット史上最大級である大規模トラフィック量によるDRDoS攻撃を受けた[1]。
- 分散型メモリキャッシュサーバmemcachedがオープンになっているという脆弱性を悪用し**増幅率の極めて高いDRDoS攻撃**を行った。

攻撃対象	Github
発生日時	2018年2月28日
影響・被害	Githubサイトは2018年2月28日17:21-17:30(UTC)にかけて1億2690万パケット・1.35Tbpsのトラフィックが発生した。その後18:00にも400Gbpsを超えるトラフィックが発生した。Githubのトラフィック許容量は攻撃トラフィック量の約2倍であったのでユーザには影響がなかった。
原因・攻撃手法	汎用分散型メモリキャッシュシステムmemcachedサーバのフィルタリングなどのミスによりインターネットから任意のリクエストに応える状態のサーバーに対して送信元IPアドレスを詐称しデータのリクエストを送ると事前にストアされているデータが詐称IPへ送られる。サーバのファイアウォールの設定で防ぐことが可能であるが調査[2]によれば全世界で88000台のサーバに脆弱性が存在していた。日本国内からの攻撃トラフィックもあった。

オープンなmemcachedを使うRDDoS攻撃のポイント

1. memcachedはメモリキャッシュを提供するサーバでWebアプリケーションの高速化など広く利用されている。
2. memcachedはUDPのプロトコルでもストア・リクエストができるので潜在的にリフレクション攻撃に使われる可能性がある。
3. 利用目的がシステムの高速化のためなのでセキュリティなどの機能は持っておらずシステム側でファイアウォールなどの適切な設定が必要である。
4. memcachedが利用しているポート11211に適切なフィルタリングをせずインターネット側からアクセスできるような場合、まず最初にデータをmemcachedに保存し、次に送付元を詐称したUDPパケットによるリクエストを送ると、保存されたデータは詐称先IPアドレスに送ることが可能である。
5. memcachedはデフォルトではキャッシュ最大値は64MBであり、数十バイトのリクエスト命令を送るだけで64MBのデータが送信され送らるため、その**増幅率はアンプ攻撃の中で極めて大きい**。

■ **Githubへの攻撃トラフィック**



（出所）Github Engineering

[1] https://githubengineering.com/ddos-incident-report/
[2] https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/

【事例5】サイドチャネル攻撃Spectre、Meltdownに係わるCPU 脆弱性の脅威

- 2010年以降に製造された主要なCPUのほぼ全てに影響するサイドチャネル攻撃手法 Spectre (CVE-2017-5753、CVE-2017-5715)および Meltdown(CVE-2017-5754)が公開された[1]。
- クラウド環境で他の仮想マシン上のプロセスのデータへアクセス、Webサイトを閲覧したタイミングでPCからデータを窃取される危険性あり

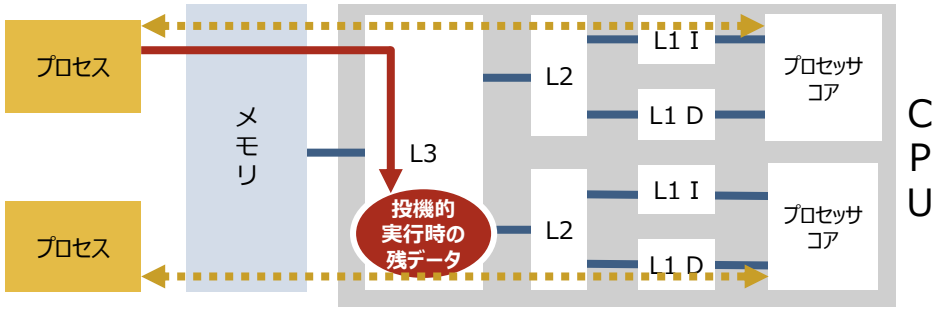
攻撃対象	高性能CPU全般(Intel、AMD、ARM等)
発生日時	2018年1月3日
影響・被害	これらはCPUの投機的実行に起因する脆弱性でCVE-2017-5753、CVE-2017-5715は、Intel、AMD、ARMといったCPUベンダーから現時点で出荷されている主要なCPUはほぼすべて影響を受ける。CVE-2017-5754は、現状ではIntelのCPUのみ影響を確認したが、他の高性能CPUも潜在的に脆弱性が予想され、数十億個レベルと見積もられる。
原因・攻撃手法	投機的実行が行われた際のキャッシュデータをほかのユーザからアクセスを行う手法。キャッシュ上にデータを取り入れるタイミングを作るためサイドチャネル攻撃の手法を用いている。同一ハードウェア上で動作する別の仮想マシンが処理を行ったデータも窃取が可能。JavaScript実装ではWebサーバ上に攻撃コードを用意しユーザがPCからWebサイトを閲覧したタイミングでPC上のデータを抜き取ることも可能。

[1] https://googleprojectzero.blogspot.jp/2018/01/reading-privileged-memory-with-side.html

SpectreとMeltdownの発見及び対応の経緯

1. 2017年6月以前：複数のセキュリティ研究者らが個別にCPUの投機的実行に対する脆弱性を発見し検証していた。
2. 6月1日：Google Project Zero チームからIntel、AMD、ARMに対して脆弱性の報告を行う。
3. 7月：発見者の一員であるグラーツ工科大学（オーストリア）の研究者らがMeltdownに対抗しうるメモリ管理手法KPIT/KAISERを学会で発表する。
4. 12月末：LinuxカーネルにKPIT(旧KAISER)がマージされる。
5. 2018年1月3日：SpectreとMeltdownとして研究者らが情報公開、同時に3つの脆弱性情報が公開される。
6. 1月10日：米MS社Windowsの脆弱性対応のパッチがAMD社CPUで不具合が発生したため取り下げる。
7. 1月22日：Intel社が脆弱性対応としてパッチを配布したが一部メーカーのハードウェアで不具合が発生したため取り下げる。

■ L3キャッシュに残るデータにアクセス



（三菱総合研究所作成）

【事例6】重要インフラをターゲットにしたマルウェアTRITONについて警告（米政府）

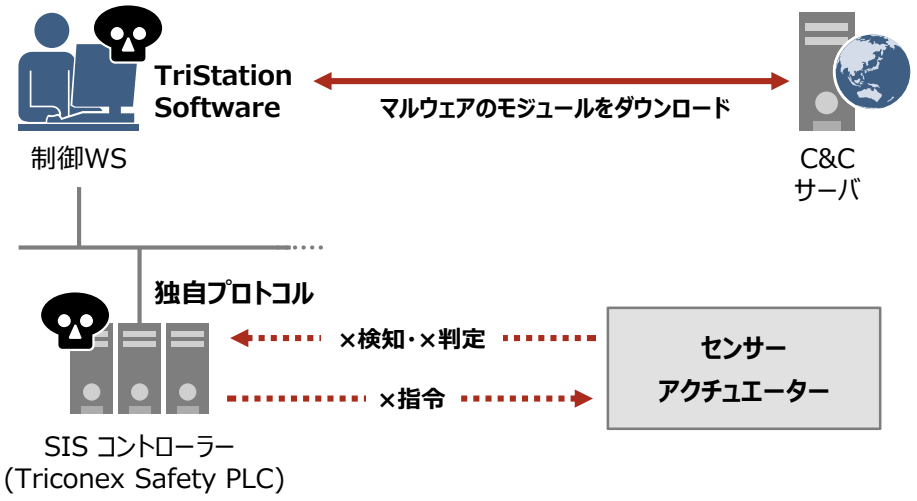
- 米国NCCIC※1 が重要インフラ企業に対し安全計装システム(SIS)をターゲットとしたマルウェアTRITON (HatMan) ※2について警告[1]
- 制御WSに感染し、独自プロトコルによりPLCに偽バイナリをインストール・実行、不正読み書きなどを行う

攻撃対象	産業インフラ・重要インフラ
発生日時	2017年12月18日(警告)
影響・被害	TRITONは仏Schneider Electric社のSIS Triconexシリーズをターゲットにして機能停止・妨害・改ざんを行い安全機能を損なわせ物理的な被害を及ぼす可能性がある。中東地域で1件被害が判明している。 NCCICやFireEyes社は目的や機能などはStuxnetと類似しウクライナ地域をターゲットにしていると分析している。
原因・攻撃手法	TRITONは、(1) 制御ワークステーションTriStationへの侵入、コンポーネントのダウンロード、他デバイスへの感染、(2) 安全系PLCに感染し支配下に置く。 マルウェアは、TriStationプロトコルを用いてPLCに偽命令を送り偽バイナリをPLCにインストールすることでシステムを支配下におく。

TRITONの攻撃ステップ

1. ターゲットはTriconexファミリのTriStationとSafety PLC
2. PCベースのTriStationに感染し外部から必要なモジュールをダウンロードする
3. 感染PCからSafety PLCのファームウェアやアプリを上書き
4. これにより生産プロセスからの情報を改ざん、情報伝達の妨害あるいは機能停止などが可能
5. そのような理由から物理的被害を発生させることも可能と指摘

■ SISコントローラーと制御監視ワークステーションが感染



[1] https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%E2%80%94Safety%20System%20Targeted%20Malware_S508C.pdf
[2] https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

※1: National Cybersecurity and Communications Integration Center
※2: NCCICではHatMan, メディアではTRITONやTRISIS呼ばれる

（三菱総合研究所作成）

【事例7】Infineon社組込み用RSAライブラリの脆弱性（CVE-2017-15361）

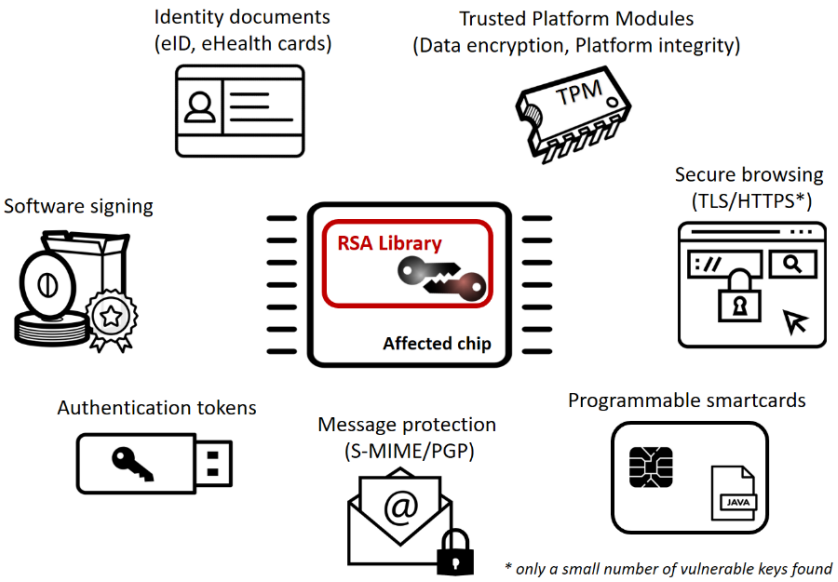
- Infineon社のCC等認証済みのセキュリティチップ向けRSA鍵生成のライブラリに脆弱性がありRSA鍵が素因数分解可能(＝解読可能）と発表される[1]
- たとえば、エストニアの国民eIDは同社のスマートカードを導入しており約75万人が影響をうける可能性がある[2]

攻撃対象	公開鍵インフラ
発生日時	2017年10月15日(発見 2017年2月)
影響・被害	RSALib、同等品を使っているスマートカード、セキュリティ・トークン、TPM、署名ソフトなどに影響がある。エストニアのeIDおよびe-residencyをサンプル調査した結果、前者約55%・後者100%の確率で解読可能性のあるRSA鍵であることが判明した。eIDカードの偽造により投票に悪用されるリスクがある。41種類のノートパソコンのTPM(同社以外のベンダーも含む)のうち10種類(約25%)が解読可能性があった。また同手法で他のRSA暗号を使っている暗号ツールの鍵を調べたところ0.01-0.03%の確率で該当した。 スマートカードやTPMなどに組込まれたファームウェアについて機器ごとに異なる手順でアップデートをする必要であるため、対応が行き渡るまでに期間を要する可能性がある。
原因・攻撃手法	チェコ・マサリク大学のセキュリティ研究者らがRSALibライブラリに含まれる高速素数生成アルゴリズムで作られた素数を使ったRSA鍵に対する高速な素因数分解可能判定および素因数分解手法を開発した。また影響範囲を調べ論文として発表した。

本攻撃が与えるインパクト

1. 組込み系では高速素数生成法を使ってRSA法の素数を生成するケースが多く、そこに対する効果的な攻撃方法が開発された
2. 組込み系はスマートカードのように発行数が多くなり影響範囲は極めて大きい
3. RSAを使う他の公開鍵暗号ツールでも確率は少ないが発見されている

■ 本ライブラリの脆弱性により影響を受ける機器は多岐に渡る



(出所) Masaryk University Centre for Research on Cryptography and Security

[1]https://crocs.fi.muni.cz/public/papers/rsa_ccs17
[2]https://www.schneier.com/blog/archives/2017/09/security_flaw_i.html
[3]https://cyber.ee/en/news/cybernetica-case-study-solving-the-estonian-id-card-case/

【事例8】新種ランサムウェアBad Rabbitによるキエフ地下鉄等への影響

- ランサムウェアBad Rabbitによりウクライナのオデッサ空港やキエフ地下鉄などが影響を受ける[1]
- 大規模なインシデントの原因となったランサムウェアWannaCry、Petyaにより、2017年5月以降ウクライナ・ロシア地域を中心に感染被害が多発しているが、それに引き続き10月に類似の攻撃を行うランサムウェアBad Rabbitが出現

攻撃対象	交通インフラ、メディア企業
発生日時	2017年10月24日
影響・被害	ウクライナのオデッサ空港やキエフ地下鉄などが影響を受ける。ロシアのインテルファックス通信やサンクトペテルブルクに拠点を置くウェブメディアFontanka.ruのサイトが一時閉鎖。
原因・攻撃手法	ウクライナのウェブメディアサイトを中心に（日本のウェブサイトも含む）に水飲み場攻撃を仕掛ける。Flash playerのアップデートに見せかけた侵入モジュールをダウンロード・実行させドライブ・バイ・ダウンロード攻撃を使い侵入。WannaCryやPetyaと同様に侵入後にSMBv1の脆弱性(MS17-010)を悪用し、Petyaと同じリモートよりコードを実行するエクスプロイトEternalRomance手法※を悪用し、組織内ネットワーク経由で感染範囲を広げる[2]。

※ EternalRomanceは、WannaCryptで悪用されたエクスプロイトEternalBlueなどと共に攻撃グループShadow Brokerが4月に公開したエクスプロイト。

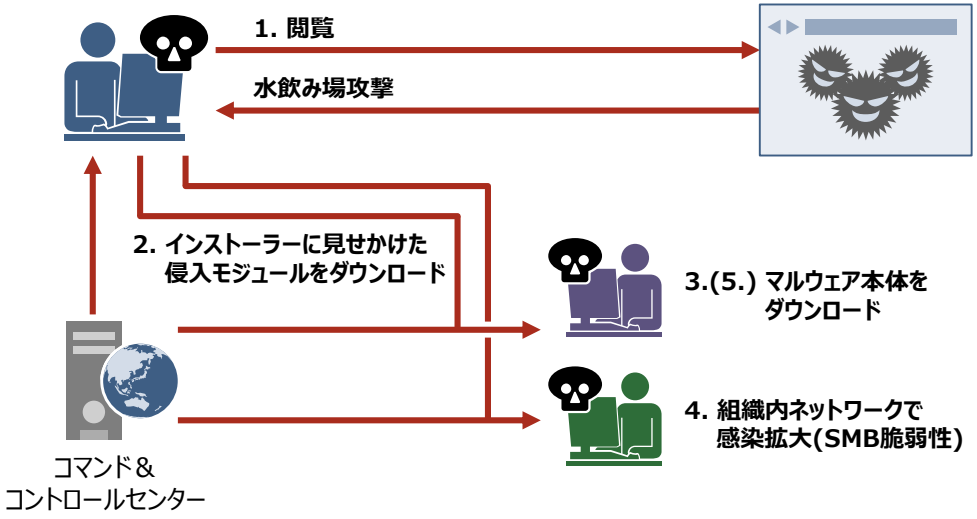
[1] http://www.bbc.com/news/technology-41740768

[2] https://securelist.com/bad-rabbit-ransomware/82851/

ランサムウェアBad Rabbitの感染パターン

1. ニュースサイトなど人の集まるサイトに水飲み場攻撃を仕掛ける
2. 閲覧者にflash playerのアップデータだと偽りトロイの木馬ドロッパーをインストールさせる
3. マルウェア本体や内部感染用のモジュールをダウンロードしSMBv1脆弱性を悪用し感染を広げる

■ ランサムウェアBad Rapidを用いた攻撃パターン



（三菱総合研究所作成）

【事例9】米重要インフラ事業者等に対するサイバー攻撃キャンペーン(Dragonfly2.0等)

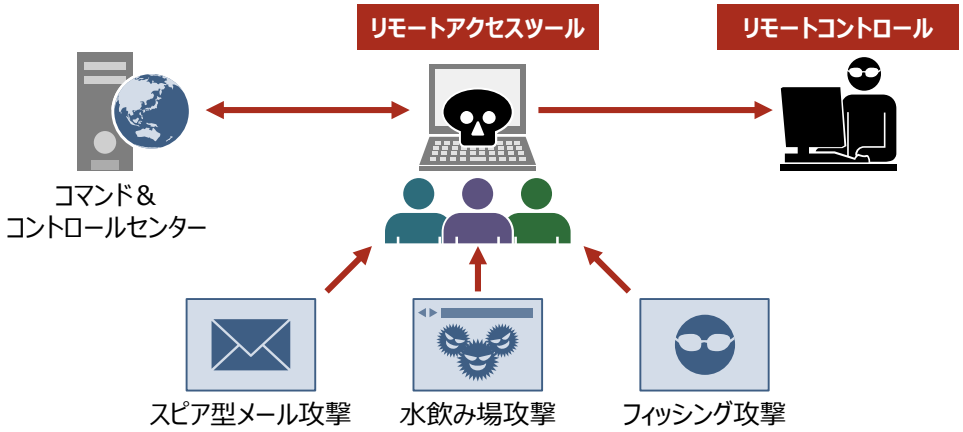
- 米国政府機関、重要インフラ分野（電力・水道・航空など）および重要産業分野（自動車・鉄鋼など）へのサイバー攻撃(APT攻撃)、サイバースパイ活動について米国政府(US-CERT)が公式に警告[1]
- スピア型メール攻撃、水飲み場攻撃、フィッシング攻撃などの手段を使い不正侵入し、コンピュータに遠隔操作ツール(RAT: Remote Access Tools)を設置し長期間にわたり組織内の情報を窃取

攻撃対象	米国政府・重要インフラ・重要産業
発生日時	2017年5月以降活発化 (2017年10月20日公式発表)
影響・被害	米国政府機関、重要インフラ、重要産業の組織内コンピュータに入り込み支配下におき機密情報を継続的に監視・窃取する（サイバースパイ活動）。
原因・攻撃手法	攻撃目標の組織情報を調べ上げ、スピア型メール攻撃、水飲み場攻撃、フィッシング攻撃等の手段を使い不正侵入する。 組織内部に遠隔操作ツールを送り込み長期間にわたり機密情報を継続的に窃取する。これらはスパイ活動の範囲だけではなくシステムを麻痺させる攻撃の準備の可能性もがあると考えられている[1]。 2017年に顕著だったサイバー攻撃チームの活動(キャンペーン)をDragonfly 2.0と命名[2]。

APT攻撃とサイバー・エスピオナージ（スパイ活動）

1. 攻撃目標の組織を公開情報で調べあげ効果的かつ計画的に攻撃準備を行う
2. スピア攻撃、水飲み場攻撃、フィッシング攻撃など多様な攻撃手法を使い執拗に攻撃を継続し続ける
3. C&Cで管理、あるいは外部から手動で遠隔操作し、長期間にわたり組織内の情報を窃取する

■ 多様な手段を使い継続的攻撃するAPTの概要



（三菱総合研究所作成）

[1] https://www.us-cert.gov/ncas/alerts/TA17-293A
[2] https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

【事例10】ランサムウェアWannaCryの世界規模の感染インシデント

- 150ヵ国以上にわたる約30万台のPCが感染し、英国では全体の20%の医療施設で影響があり、緊急を除いて予約の多くがキャンセルという事態が発生。
- 想定する損失総額は生産性低下や損害賠償コスト等を含め世界規模で40億米ドル（約4,412億円）[1]

攻撃対象	一般PC・インフラ・医療機関など
発生日時	2017年5月12日
影響・被害	中国では大学・石油会社・病院・政府機関など約3万の施設が影響を受ける。ホンダ狭山工場では1,000台以上の自動車生産に影響。損失総額は生産性低下や損害賠償コスト等を含め、世界規模で40 億米ドル（約4,412 億円）と推定される。
原因・攻撃手法	PCが感染するとさらに内部ネットワークを探索しMS17-010（SMBv1の脆弱性）を使い感染を広げる。EternalBlueと呼ばれるリモート実行と権限昇格ができる攻撃手法を使い侵入しファイルレスマルウェアDoublePulsarでバックドアを作る。感染するとウィンドウが現れ$300ドル相当のビットコインを要求。時間が経つと$600ドルにアップする。しかし振り込みと感染PCを結びづける管理が見当たらず、また支払って復号したケースも報告されていない。

WannaCryの特徴

1. 感染後、組織内のネットワークをスキャンしWindows SMBファイルサーバの脆弱性MS17-010を悪用して他のPCにさらに感染を広げる
2. 既にサポートが終了しているWindows XPが現在もなお多数利用されているため感染が拡大（英医療機関ケース）
3. マイクロソフトは、WindowsXP用緊急パッチを公開 [2]

■ WannaCryによる身代金要求メッセージウィンドウ

（トレンドマイクロより）

[1] https://www.trendmicro.com/content/dam/trendmicro/global/ja/security-intelligence/research-reports/sr/sr-2017h1/2017h1sr0921.pdf
[2] https://technet.microsoft.com/library/security/MS17-010

4. インシデント概要一覧表

セキュリティ・インシデント・脅威事例概要一覧

I:インシデント、V:脆弱性、C:攻撃キャンペーン

No	注目度	区分	事例名	年月日（報告日等）	発生国	システム区分	産業分野	被害・影響	原因・攻撃手法	注目ポイント（攻撃の新規性、被害規模に注目）	影響度	発生可能性	攻撃タイプ
1	***	I	ノルウェイのアルミニウム製造工場がランサムウェア被害	2019/3/19	ノルウェー	ICS（重要インフラ以外）	製造	大手アルミニウム製造会社Norsk Hydro ASAの製造工場はランサムウェア「LockerGoga」による被害で一時的に停止した。3月18日米国の事務所にあるパソコンが感染したことから始まり、翌日、社内の基幹ネットワークを経由して40カ国にある関連会社まで拡散した。被害予想額は36億円から42億円と予想される。	ランサムウェア「LockerGoga」の実行ファイルには、必要となる機能がすべて含まれているため、外部のC&Cサーバと通信しない。したがって、外部との通信からランサムウェアを検知する手法を使えない。管理者権限で実行される場合、当該アカウントのパスワードを変更し、管理者がログインできなくなるようにする。一般ユーザが実行する場合、脅迫状を表示する。ただし、ランサムウェア「LockerGoga」には、暗号化されたファイルを元に戻す方法がないされ（セキュリティベンダ分析）、ランサムウェアに見せかける破壊型マルウェアとみられる。	アンチウィルスの検知回避、ランサムウェアの偽装など巧妙な手法を組合わせている。	大	中	マルウェア感染
2	***	C	ASUS使用者を狙う攻撃キャンペーン	2019/3/28	各国	情報システム	全分野	ASUS社製ソフトウェアのアップデートを配信するツール「ASUS Live Update Utility」が改ざんされ、バックドアが仕掛けられた形跡が発見された（Kaspersky Labのレポートによる）。計5万7千人以上の使用者が、バックドアを仕掛けられた「ASUS Live Update Utility」をインストールしたと推定される。Kaspersky Labは、本攻撃を過去最大規模のサプライチェーン攻撃とする見解を示し、「ShadowHammer」と名付けた。	攻撃者は、ASUS社の公式ツール「ASUS Live Update Utility」を直接改ざんすることで、バックドアを仕掛けた。改ざんされたソフトウェアは、正規の証明書で署名された後に配信されており、アンチウィルスソフト等で検知されることを回避した。また、感染した端末のMACアドレスを利用し、標的の端末か否かを判断する機能を有していた。	ソフトウェアの製造元に攻撃をしかけることで、正規チャネルからの、不正ソフトウェア大規模配信が実現されてしまった点。	大	大	APT
3	**	C	Verizonのモバイルユーザを標的としたフィッシングキャンペーン	2019/4/5	各国	コンシューマIoT機器	全分野	セキュリティ企業Lookout社のフィッシングAIプロジェクトによって、Verizon社のサービスを利用するユーザを標的としたフィッシングキャンペーンが発見された。セキュリティ企業Cofenseの最高技術責任者兼共同設立者も、モバイルフィッシング攻撃が増加傾向にあると同意し、消費者に直接的な影響を与えると説明した。	Verizon社のカスタマーサービスを騙ったフィッシングメールが、ユーザ宛に送信された。本フィッシングメールは、デスクトップ端末で開封された場合、明らかに不正ドメインから送信されたメールであることが確認できたが、モバイルデバイスで開かれた場合、正当なサイトに見えるものであった。	明らかにモバイル端末を標的とした攻撃であり、モバイルフィッシング攻撃の増加を示す一例である。	中	大	フィッシング
4	**	V	米国が北朝鮮のマルウェアHOPLIGHTに注意喚起	2019/4/10	各国	情報システム	全分野	米国の国土安全保障省及びFBIは、北朝鮮政府が「HOPLIGHT」と呼ばれるマルウェアを展開し、米国企業と政府機関を対象に、サイバー攻撃を実施した事実を特定したと報じた（米国FBIと国土安全保障省の分析レポートによる）。	マルウェア「HOPLIGHT」はトロイの木馬であり、ファイルの読み込み、書き込み、移動、ターゲットシステムに関する情報の収集、プロセスとサービスの操作、リモートホストへの接続をまとめて行うことができる。	北朝鮮を拠点に活動しているとみられるサイバー攻撃グループによる直接的な関与が疑われている。	大	中	マルウェア感染
5	**	V	主要4社のVPN製品に存在する脆弱性への警告	2019/4/11	各国	情報システム	全分野	US-CERTはCisco社、Palo Alto Networks社、F5 Networks社、Pulse Secure社のVPN製品に、深刻な脆弱性が存在するとして注意を呼びかけた。当該脆弱性を悪用すると、攻撃者はシステムをアクセスすることができる。	本脆弱性は、機密データの暗号化不備に関する問題である。攻撃者が、当該VPNユーザのエンドポイントに永続的にアクセス可能である場合、他の方法を使用してCookieを抽出可能であった場合、セッション通信をリプレイし、他の認証の回避を行うことができる。	VPN通信への信頼性の前提であるVPN製品の暗号化機能に関する脆弱性である。	中	大	不正アクセス

No	注目度	区分	事例名	年月日（報告日等）	発生国	システム区分	産業分野	被害・影響	原因・攻撃手法	注目ポイント（攻撃の新規性、被害規模に注目）	影響度	発生可能性	攻撃タイプ
6	＊＊＊	C	80種類もの攻撃モジュールを展開したサイバー犯罪グループ	2019/4/16	各国	情報システム	全分野	Kaspersky Labは、同一のサイバー犯罪グループが、2014年からバックドア、ローダー、キーロガーといったハッキングツールを利用し、幅広くサイバースパイ活動を行っている可能性があると報じた。その活動は、TajMahal攻撃フレームワークと呼ばれ、USBスティックから特定のファイルを盗むことができる珍しいも手法を含み、80種類の攻撃モジュールを利用可能と見られる。	膨大な数のプラグインモジュールを備えたTajMahalは、様々な攻撃手法を用いることが可能である。攻撃ツールとして、仮想ファイルシステムも利用されている。	数多くの攻撃モジュールを用いたサイバー攻撃を行いながら、5年間も検知されず、活動を継続していた。	大	中	不正アクセス、マルウェア感染
7	＊＊＊	V	P2P脆弱性がIoTデバイス数百万台に影響	2019/4/29	各国	コンシューマIoT機器	全分野	iLnkP2Pソフトウェアのピアツーピア（P2P）機能に脆弱性「CVE-2019-11220」が報告された（セキュリティ研究者Paul Marrapese）。当該脆弱性は数百万台のIoTデバイス（例：セキュリティカメラ、ベビーモニター、スマートドアベル）に影響を与えている。	多くのP2Pアプリが制御サーバとの通信を確立するために使用する「heartbeat」は、ファイアウォールを通過し、サーバと接続することができる。攻撃者は簡単に推測できるアカウントを利用し、デバイスに直接アクセスすることができる。	数百万台のIoTデバイスに脆弱性があり影響範囲が広い。	中	大	不正アクセス
8	＊＊＊	C	SAP ERPの設定不備を狙う攻撃ツールが流通	2019/5/2	各国	情報システム	全分野	米国土安全保障省のサイバーセキュリティ部門CISAが、ERPパッケージ「SAP」の設定不備を悪用する攻撃ツールの流通に関して、注意喚起を行った。 セキュリティ会議OPCDEでの報告では、アクセス制限などが設定不備状態にあるシステムは、インターネット上に多数あり、影響を受けるシステムは約90万件にのぼる（Onapsis社による試算）。それらのシステムを標的とするエクスプロイト「10KBLAZE」は一般に公開されており、簡単に入手することが可能である。	SAPシステムは、通常インターネットに公開することは想定されていな。しかし、設定不備のままインターネット上に公開されているシステムは多数ある。「10KBLAZE」は、こうした意図せず公開されているシステムを狙う攻撃ツールであり、攻撃者は容易にシステムを侵害することができる。 ①SAPゲートウェイのアクセス制御リスト（ACL）が正しく設定されていない場合、匿名ユーザがOSコマンドを実行することが可能。 ②SAPシステムと外部ネットワークを接続するプログラムSAP Routerは、デフォルト設定では内部ホストとして機能するため、攻撃者によるリモート操作が可能となる。 ③アプリケーション・サーバ間のブローカとして機能するSAPメッセージサーバは、デフォルト設定では認証の必要がないため、攻撃者がメッセージサーバにアクセスすると、アプリケーションサーバ上の操作・実行が可能となる。	「SAP」は、様々な企業で広く導入されているな製品であり、企業の重要情報を多く保持している。「SAP」へのサイバー攻撃は、企業の機密情報保護に深刻な影響を及ぼすものであり、攻撃件数が増加している（2018年にもUS-CERTによる注意喚起あり）。	大	大	その他脆弱性攻撃
9	＊＊	V	Siemens社Simatic S7 PLCに脆弱性	2019/5/17	各国	ICS（重要インフラ以外）	制御システム一般	Siemens社のS7 Simaticアーキテクチャに脆弱性が存在することを、イスラエルのセキュリティ研究チームが発見・報告した。S7 Simaticアーキテクチャは、S7シリーズのプログラマブルロジックコントローラ（PLC）とエンジニアリングワークステーションを接続する用途で使用される。	攻撃者はS7 Simaticの通信アーキテクチャにある脆弱性を利用し、PLCをリモートで起動および停止することが出来る。また、不正なコマンドロジックをS7 PLCにダウンロードさせることで、PLCの制御を奪うことも可能である。更に、これらの不正なコマンドロジックを隠蔽することで、担当者が検査時には、正規のPLCソースコードを表示し、攻撃の痕跡が発覚することを防ぐ事も考えられる。	PLCの脆弱性を悪用する攻撃は、産業システムやプロセスに大きな損害を与える。ファイアウォールの設置、アクセス制御、S7へのインターネット接続の遮断といった対策が求められる。	大	中	その他脆弱性攻撃
10	＊＊＊	V	医療機器向け画像規格DICOMの脆弱性	2019/6/11	各国	ICS（重要インフラ）	医療	医療機器における画像規格DICOMに、脆弱性（CVE-2019-11687）が存在することが、米国セキュリティ企業Cylera Labsの研究者Markel Picado Ortiz氏によって確認された。同時に、概念実証（PoC）エクスプロイトコードも公開されている。DICOM規格は、医用画像情報を送信、保存、検索、印刷、処理、および表示するための国際規格であり、ヘルスケアおよび公衆衛生分野において広く使用されている。米国NCCIC (National Cybersecurity & Communications Integration Center) は、本件に関して注意喚起を行った。	DICOM規格の脆弱性（CVE-2019-11687）は、入力値のバリデーション不備であり、更にリモートコード実行が可能である。攻撃者は、CT／MRIの画像ファイルに悪意のあるコードを埋め込むことが可能であり、患者情報の取得、情報の改ざん、サービス不能攻撃等を行うことが考えられる。	当該脆弱性はCVSSが値高く、1995～2019年に亘りDICOM規格に幅広く影響する。	大	中	マルウェア感染

セキュリティ・インシデント・脅威事例概要一覧

I:インシデント、V:脆弱性、C:攻撃キャンペーン

No	注目度	区分	事例名	年月日（報告日等）	発生国	システム区分	産業分野	被害・影響	原因・攻撃手法	注目ポイント（攻撃の新規性、被害規模に注目）	影響度	発生可能性	攻撃タイプ
11	***	C	サイバー犯罪グループXENOTIMEの攻撃対象分野が拡大	2019/6/14	米国等	ICS（重要インフラ）	石油、ガス、電力、製造	サイバー犯罪グループ「XENOTIME」はシステムの破壊を目的とし、安全計装システム（SIS）を狙う組織とされる。「XENOTIME」は石油分野とガス分野を主な標的として活動していたが、電気事業分野への攻撃活動が確認された。	サイバー犯罪グループ「XENOTIME」が使用しているマルウェア「TRISIS（別名：TRITON）」は、安全システムを不正に操作するよう設計されている。更に、緊急シャットダウン機能を制御することが可能であり、人命の損失又は物理的損傷を引き起こす危険性もある。	電気事業へのサイバー攻撃により、様々な産業への被害が生じ、国家レベルでの混乱を引き起こす可能性がある。	大	大	APT
12	***	V	Windowsの脆弱性BlueKeepを悪用した攻撃への注意喚起	2019/6/17	各国	情報システム	全分野	Microsoftは5月14日にWindowsに使用されているリモートデスクトッププロトコル（RDP）の脆弱性BlueKeep（CVE-2019-0708）に対する修正パッチをリリースした。米国土安全保障省のサイバーセキュリティ部門CISAは脆弱性BlueKeepの動作検証を行い、6月17日に注意喚起を行った。	攻撃者は、RDPが有効になっているWindows端末に対して、BlueKeepの脆弱性を悪用する不正パケットを送信することで、認証を回避しつつ遠隔操作を行うことが可能である。管理者権限を持つアカウントの追加、データの表示、変更、削除といった操作を行ったり、不正プログラムのインストール等を行うといった攻撃が考えられる。また、WannaCry同様、侵害後にワームとして増殖活動を行う懸念が示されている。	遠隔攻撃と自己増殖の機能により、2017年のランサムウェアWannaCry同様、広範囲で被害が生じる起こる可能性があると懸念されている。	大	大	マルウェア感染、不正アクセス
13	***	I	Raspberry Pi経由でNASAのデータが長期間漏えい	2019/6/24	米国	情報システム（重要インフラ）	航空	米国航空宇宙局（NASA）のジェット推進研究所(JPL)は、サイバー攻撃を受け、火星探査に関するデータが漏洩したことを2019年6月24日に発表した。 当該事案を発見したきっかけは、2018年4月にJPLで発生した外部ユーザアカウントの侵害だった。侵害されたアカウントは、主要なミッションシステムの1つから、約500メガバイトのデータを盗むために、使用されていたことが明らかになった。その後の分析の結果、攻撃者はJPLのセキュリティシステムの脆弱性を悪用し、約10ヵ月もの間検知されずに、JPLのネットワーク内で活動していたと考えられている。	JPLは、情報技術セキュリティデータベース（ITSDB）と呼ばれるWebベースのアプリケーションを使用し、ネットワーク上の物理的な資産とアプリケーションを追跡及び管理していた。しかし、適切な運用が行われておらず、JPLのネットワーク環境へは無許可に接続することができた。その結果、攻撃者は無許可に接続されたシングルボードコンピューター「Raspberry Pi」を利用し、JPLのネットワークへ侵入、データを窃取した。	潜伏期間が長く、漏えいした情報も重大なものである（国際武器輸送規制情報も含まれる）。	大	大	不正アクセス
14	**	C	金融機関を狙うサイバー攻撃グループTA505	2019/7/2	各国	情報システム（重要インフラ）	金融	ロシア語を使用するサイバー攻撃グループTA505は、2018年11月に配布したバックドア「ServHelper」に加えて、新しいダウンローダーマルウェア「AndroMut」の使用を開始した。Proofpoint社の分析によると、TA505はシンガポール、アラブ首長国連邦、米国の金融機関のユーザを標的にしている。	攻撃者は、ターゲットへ請求書を装ったフィッシングメールを送付する。細工されたWordやExcelを添付し、ダウンローダーマルウェア「AndroMut」を保存させる。ダウンローダーマルウェア「AndroMut」は、RATマルウェア「FlawedAmmyy」のダウンロードを行い、RATマルウェア「FlawedAmmyy」は権限昇格により管理者権限を奪取、ユーザの行動を監視する。	2018年12月以来、サイバー攻撃グループ「TA505」による活動は活発であり、中南米から東アジアまで、金融業界から小売業界まで、攻撃範囲が広い。	中	大	マルウェア感染
15	***	I	「7pay」への不正アクセスにより5500万円の被害	2019/7/4	日本	情報システム	小売	セブン&アイ・ホールディングスの傘下にあるセブン・ペイ社による決済サービス「7pay」において、サービス開始3日目にして、第三者による不正アクセスが発生したことが判明した。2019年7月4日時点での損害格は、約5,500万円と算出された。セブン・ペイ社はクレジットカード、デビットカードからのチャージ機能の一時停止、パスワードの全初期化等の対策を行ったが、最終的にはサービスの廃止を決断した。	セブン&アイ・ホールディングスの発表では、パスワードリスト攻撃によるアカウント侵害が原因として挙げられた。この手口の場合、不正にログインした攻撃者は、決済用資金をチャージし、商品を購入したものと推測される。 決済サービスでありながら、二段階認証を実装していなかったことを、対策の甘さとして批判する声もあった。	QRコード決済に関する国内最大規模のインシデントであり、他のサービスも含めてセキュリティ対策への信頼性が話題となった。経営層のセキュリティ対策への関与についても議論となった。	大	小	不正アクセス

No	注目度	区分	事例名	年月日（報告日等）	発生国	システム区分	産業分野	被害・影響	原因・攻撃手法	注目ポイント（攻撃の新規性、被害規模に注目）	影響度	発生可能性	攻撃タイプ
16	**	V	GE全身麻酔装置に脆弱性	2019/7/9	各国	ICS（重要インフラ）	医療	GE社の全身麻酔装置 AestivaとAespireの脆弱性（CVE-2019-10966）が、セキュリティ研究チームCyberMDXにより発見された。本脆弱性が悪用されると、麻酔用ガスの種類、濃度、組成、気圧等を遠隔操作で改変されてしまう可能性がある。米国ICS-CERTは、本件に関する注意喚起を行った。	全身麻酔装置 AestivaとAespireがターミナルサーバーを介して病院ネットワークに接続する。攻撃者は、 AestivaとAespireの脆弱性（CVE-2019-10966）を悪用することで、ターミナルサーバとの通信に用いるプロトコルを、安全性の低い古いバージョンに強制的に戻すことが出来る。旧バージョンのプロトコルでは、認証無しでパラメータの変更等を行うことが可能である。	麻酔の投与の遠隔コントロールにより、人体の安全性に係る重大な影響のリスクがある。	大	中	その他脆弱性攻撃
17	**	C	QNAP社のネットワークストレージを狙うランサムウェアeCh0raix	2019/7/10	各国	コンシューマIoT機器／情報システム	全分野	QNAP社のNAS（ネットワーク接続ストレージ）デバイスを狙うランサムウェアeCh0raixが、Anomali社の研究者によって発見された。QNAP社のNASデバイスは、一般消費者向けの製品から、企業向けの製品まで広く展開されているため、米国においては19,000以上のシステムに影響を及ぼす可能性がある。	ランサムウェアeCh0raixの感染ルートは特定されていないが、弱いパスワードを設定しているデバイスへのブルートフォース攻撃、古いQTSファームウェアの脆弱性の悪用といった手段でデバイスにアクセスしたとみられている。 ランサムウェアeCh0raixは、感染したデバイスの所在地を確認する機能を有しており、ベラルーシ、ウクライナ、又はロシアと認識した場合、暗号化を実行することなく、動作停止する。	感染デバイスの所在地による動作の違いから、国家の関与が予想される。バックアップやファイル保存のために使われるNASデバイスは、対応するアンチウィルス製品が少ないため、これを利用した攻撃である可能性がある。	中	大	不正アクセス、マルウェア感染
18	***	I	ビットポイントジャパンから仮想通貨約 30.2 億円流出	2019/7/11	日本	情報システム（重要インフラ）	金融	仮想通貨交換業者ビットポイントジャパンがサイバー攻撃を受け、5種類の仮想通貨「Bitcoin」「Bitcoin Cash」「Ethereum」「Litecoin」「Ripple」が流出した。調査の結果、損害額は30.2億円に上ることが判明した。7月11日に、仮想通貨「Ripple」の送金に関するエラーを検知したことで、調査が開始された。	ホットウォレットの秘密鍵を管理するウォレットサーバが、不正アクセスを受けた可能性があると考えられている。ホットウォレットの秘密鍵が窃取され、不正使用されたものと推測される。詳細な攻撃手法は判明しておらず、調査中である。	仮想通貨流出事案の多発から、仮想通貨への信頼性が揺らぐ事態となった。金融庁により、秘密鍵をコールドウォレットで管理することが義務化される等、規制が強化された。	大	大	不正アクセス
19	***	V	サーバ用ファームウェア MergePoint EMSに脆弱性	2019/7/22	各国	情報システム	全分野	Lenovo社、Acer社、Gigabyte社及びPenguin Computing社のサーバに使用される、ベースボード管理コントローラ（BMC）のファームウェア「MergePoint EMS」に、コマンドインジェクションを可能にするものを含む、深刻な脆弱性が複数存在することが判明した。	第一の脆弱性はシステムのファームウェア更新において、デジタル署名検証が、SPIタイプのフラッシュメモリへの書き込む前に実施されないというものである。これにより、署名検証前に、改ざんした命令をファームウェアに書き込むことが可能となる。 第二の脆弱性は、コマンドインジェクションに関する脆弱性である。本脆弱性を悪用すると、攻撃者は稼働中のシステムに対して、ランダムなコマンドを実行させることができる。	サーバのハードウェアベンダーが、ファームウェアをパートナー企業に外注することが、結果としてサプライチェーンリスクに繋がってしまった事案である。	中	大	不正アクセス、インジェクション
20	**	C	南アフリカの電力会社 City Powerがランサムウェア被害	2019/7/25	南アフリカ	ICS（重要インフラ）	電力	南アフリカ最大の都市Johannesburgにある電力会社「City Power」が、ランサムウェア被害に遭い、電力制限が発生した。City Powerはランサムウェアに関する詳細な情報を公表していないが、顧客の個人情報漏えいはないと説明した。	真冬の南アフリカにあって、Johannesburgはいつも以上に電力を消耗していた。ランサムウェア被害により、プリペイド契約を結んでいた顧客は、チャージを行うことが出来なくなり、結果的に電力の制限が発生した。	制御システム本体への直接的なサイバー攻撃ではなくとも、結果的に制御システムに大きな影響を与える可能性がある。	中	大	マルウェア感染

No	注目度	区分	事例名	年月日（報告日等）	発生国	システム区分	産業分野	被害・影響	原因・攻撃手法	注目ポイント（攻撃の新規性、被害規模に注目）	影響度	発生可能性	攻撃タイプ
21	＊＊＊	C	Apple iOSの脆弱性にSMS攻撃の可能性	2019/7/30	各国	コンシューマIoT機器	全分野	Google Project Zeroの研究者は、Apple社のiOSに、SMS関連の脆弱性（CVE-2019-8646）を発見した。この脆弱性を悪用すれば、SMS経由でターゲット端末へ攻撃を行うことが可能である。Apple社は、Google Project Zeroの脆弱性情報公開ルールへ対応し、脆弱性を修正したバージョンのiOSを公開し、ユーザに対して更新の呼びかけを行っている。	iOSのメッセージ送信方式には、常に暗号化が行われるiMessage と暗号化が行われないSMS/MMSがある。脆弱性「CVE-2019-8646」を悪用することで、iMessage方式で送受信されるコンテンツであっても、外部の攻撃者が読み取ることが可能となる。また、SMS経由で送信されたワンタイムパスワードを、遠隔地から読み取る事も出来る。	多くの利用者を抱えるiOSの脆弱性であり、影響範囲が極めて広い。また、ユーザの個人情報だけでなく、決済用情報等も窃取される可能性があり、深刻度が高い。	大	大	その他脆弱性攻撃
22	＊＊＊	V	通信プロトコルCANの航空機実装に脆弱性	2019/7/30	米国、各国	ICS（重要インフラ）	航空	米国CISAは、航空機のアビオニクス（航空機電子機器）に実装されたCANバスネットワーク（車載ネットワーク標準）が、安全でないことを示すレポートを公開した。当該レポートによると、航空機に物理的にアクセスできる場合という条件はあるが、誤ったデータを入力し、アビオニクス機器が読み取る値を、不正な値とすることが可能である。この時、パイロットは正しい数値を判別することができず、最悪の場合は飛行機が制御を失う可能性があると警告した。	攻撃者が、航空機に物理的に接近することが可能である場合、CANバスネットワークに不正接続し、誤ったデータの入力を行う。	物理的攻撃を妨げるセーフガードの実装を強化する必要がある。	大	小	その他脆弱性攻撃
23	＊＊＊	C	Magecart攻撃に小売ISACが注意喚起	2019/8/1	各国	情報システム	小売	小売およびサービス業ISAC（Retail and Hospitality ISAC；RH-ISAC）とPCIセキュリティ標準評議会（PCI Security Standards Council）は、オンライン決済におけるカードスキミング攻撃について、注意喚起を行った。特に、サイバー犯罪グループ「Magecart」による攻撃の増加に対し、警戒が呼びかけられた。	攻撃者は、ECサイトあるいは広告スクリプトといった機能／アプリケーションへ、不正なJavaScriptコードを挿入し、消費者のクレジットカード情報を抜き出す。	広告スクリプトは、サードパーティの公告配信サービス経由で読み込まれる事も多く、ECサイト運営者側で検知を行うことは容易ではない。	大	大	インジェクション
24	＊＊＊	C	バーレーンの重要インフラにサイバー攻撃	2019/8/8	バーレーン	ICS（重要インフラ）	電力、水道、製造	Wall Street Journalによって、バーレーンにある世界最大の製錬所の1つであるAluminium Bahrain（Alba）が、サイバー攻撃を受けたことが報道された。その他、政府機関や、電気及び水道を管轄する当局への攻撃が確認されている。これらの攻撃の背後には、イランの関与が疑われているという。セキュリティ専門家は、今回の攻撃の洗練度は、以前のイランによるサイバー攻撃よりも高いと分析している。	6月に、100万通以上の悪意のある電子メールの送信や、600万回数以上の攻撃を施行した形跡が残っている。 7月には、電気及び水道を管轄する当局への侵入も、多発していたことが分かっている。攻撃者は、一部のシステムにおいて、シャットダウンの実行、限定的な制御権限の獲得に成功していたと考えられている。	国家レベルのサイバー攻撃が、念入りな準備と共に行われている点。	大	大	APT
25	＊＊＊	V	Siemens社のS7 PLCに脆弱性	2019/8/8	各国	ICS（重要インフラ以外）	制御システム一般	Siemens社の制御機器「S7 PLC」に、認証に関する脆弱性が発見された。全てのS7 PLCが、同じ暗号キーペアを共有していた。1台のS7 PLCを侵害することに成功した場合、全てのS7 PLCへアクセスすることが可能となってしまう。	攻撃者は、エンジニアリングワークステーションを装った機器から、S7 PLCを侵害する不正コマンドを送信する。侵害後は、機器電源のオン/オフ、不正コマンドの実行、不正なコードのダウンロード等を実施可能となる。不正なコマンドをバックグラウンドで実行する、不正コードを隠蔽し正規のPLCソースコードを表示する等、攻撃検知の回避を行う事も出来る。	プラントの制御システムに直接的な被害を与える可能性がある脆弱性であり、深刻度が高い。S7 PLCは市場シェアも高く、影響範囲も大きい。	大	大	不正アクセス、その他脆弱性攻撃

No	注目度	区分	事例名	年月日（報告日等）	発生国	システム区分	産業分野	被害・影響	原因・攻撃手法	注目ポイント（攻撃の新規性、被害規模に注目）	影響度	発生可能性	攻撃タイプ
26	**	V	三菱電機のリモートターミナルユニットsmartRTU に複数の脆弱性	2019/8/13	各国	ICS（重要インフラ以外）	制御システム一般	三菱電機社製リモートターミナルユニット「smartRTU」及び「INEA ME-RTU」に、管理者権限で遠隔コードを実行されるおそれのある、複数の脆弱性が存在することが確認された。米国DHS/CISAは、本脆弱性について注意喚起を行った。	当該機器には、以下の脆弱性が発見された。①認証されていないOSコマンドインジェクション（CVE-2019-14931）；②認証されていない構成ファイルのダウンロード（CVE-2019-14927）；③クロスサイトスクリプト（XSS）の保存（CVE-2019-14928）；④ハードコードされた暗号化鍵の使用（CVE-2019-14926）；⑤ハードコードされたユーザパスワード（CVE-2019-14930）；⑥プレーンテキストパスワードストレージ（CVE-2019-14929）；⑦任意のユーザが読み取り可能な構成ファイル（CVE-2019-14925）。	管理者権限による遠隔コード実行は、非常に強力な攻撃手段であり、危険性が高い脆弱性である。smartRTUは、SCADAシステムと接続し、制御機器等の遠隔監視と制御を担う機器である。不正なコマンドの発行等が実際に行われた場合、制御システムへ大きな影響を及ぼす可能性がある。	中	大	不正アクセス、インジェクション、その他脆弱性攻撃
27	***	C	欧州中央銀行がマルウェア感染でサイト閉鎖	2019/8/15	欧州	情報システム（重要インフラ）	金融	欧州中央銀行（ECB）は、サイバー攻撃によるマルウェア感染事案が発生し、所管するウェブサイトの1つを閉鎖することとなった。ECBは、今回の攻撃による被害には、市場に影響を与えうるデータ漏えいは含まれないと発表した。しかし、ECBの発行するニュースレターの購読者に関する情報（電子メールアドレス、名前、肩書等）は、漏えいした可能性があるとされている。	攻撃者は、何らかの手段で、外部公開サーバへマルウェアを感染させることに成功した。マルウェアは、サーバに保存されていたニュースレターの購読者の情報を窃取可能な状態にあった。ECBは、攻撃者の目的は、フィッシング攻撃へ情報を活用することであったと推測している。 マルウェアへの感染は、2019年8月のサイトのメンテナンス中に発見されたが、2018年12月には、既に感染状態にあったとみられる。	近年、マレーシアやエクアドル等でも中央銀行を標的としたサイバー攻撃が発生しており、警戒が高まっている。	大	大	APT
29	***	V	ビル・オートメーションプロトコルBACnetを利用するビル・デバイスに脆弱性	2019/8/19	各国	ICS（重要インフラ以外）	制御システム一般	スマートビルディングデバイスは、ビル管理者に、温度制御システムや監視システムを、遠隔操作する機能を提供する。セキュリティ研究者Bertin Bervis氏は、スマートビルディングデバイスに新たな脆弱性を発見し、研究成果をDEF CON IoT Villageで発表した。	今回発表された脆弱性は、ビルディングオートメーション用プロトコル「BACnet」を悪用するものである。攻撃者は、本脆弱性を悪用することで、デバイスに不正なjavascriptコードを挿入する。これにより、ビルや産業施設の設備へのアクセスや、データベースを改ざんするパケットの送信等を行うことが出来る。	デバイスとアプリケーション間に、直接的なやりとりがなくても改ざんが成立する新種の攻撃である。スマートビルディングデバイスは、商業施設や工業施設を中心に導入が進んでいる。	中	大	不正アクセス、インジェクション
28	***	C	米テキサス州複数市町村がランサムウェア被害	2019/8/19	米国	情報システム（重要インフラ）	政府・行政サービス	米国テキサス州の22市町村が、ランサムウェアの被害を受けた。本攻撃は、同一人物による仕業だと推測され、テキサスA＆M大学セキュリティセキュリティオペレーションセンター、テキサス公安局、軍事関係者も注目している。	22の市町村に対する攻撃が、一度に発生したことから、攻撃者の手口は、標的システムにランサムウェアを事前にダウンロードさせた後、意図した時間に一斉に起動させたものと考えられている。	攻撃者は、複数の市町村へのランサムウェア感染を成功させており、小規模の地方自治体のみならず、大規模組織へ攻撃対象を拡大していく可能性が懸念される。	大	大	マルウェア感染
30	***	C	APTグループSilenceが金融機関に攻撃拡大	2019/8/21	各国	ICS（重要インフラ）	金融	ロシア語を話すAPTグループ「Silence」による、世界中の銀行や金融機関への攻撃が拡大している。セキュリティ会社Group-IBの分析レポートによると、過去1年間でAPTグループ「Silence」は、20か国以上の組織を標的とし、攻撃頻度が急増している。新たなマルウェアも、武器として用いられている。金融機関の経済的損失は、5倍に急増した。	APTグループ「Silence」の典型的な手口は、マルウェアを埋め込んだフィッシングメールである。感染端末を介して、標的のバンクネットワークへの初期アクセスを試みる。その後、銀行システムにマルウェアを埋め込み、ATMからの不正な引き出し等を行う。また、大量のスパムキャンペーンでは、銀行詐欺ツール「DRIDEX」や、その他のマルウェアを配布する手法も利用されている。	Dutch-Bangla銀行や他の銀行による損失は420万ドルに達しており、被害金額が極めて大きい。	大	大	APT、フィッシング
31	***	C	ダウンロード数1億超えのAndroidアプリにマルウェア	2019/8/27	各国	コンシューマIoT機器	全分野	Kasperskyの研究者チームは、CamScannerというアプリにマルウェアが含まれていることを発見した。CamScannerは、OCR(光学式文字認識)機能を持つPDF作成アプリであり、1億回以上のダウンロード実績があった。本アプリは、Googleの公式アプリストア「Google Play」においても提供されている。	アプリCamScannerに仕込まれたマルウェアには、別のマルウェアをダウンロードするトロイの木馬モジュールが含まれていた。当該モジュールは、アプリのリソースに含まれる暗号化されたファイルから、別の悪意のあるモジュールを抽出して実行する。このため、攻撃者は感染したデバイス上で、更なる操作を行うことが可能である。	1億回以上のダウンロードされたアプリであり、影響範囲が大きい。また、公式アプリストアから配布されたアプリにマルウェアが含まれていたことから、公式アプリストア自体の信頼性に懸念を生じさせた。	中	大	マルウェア感染

No	注目度	区分	事例名	年月日（報告日等）	発生国	システム区分	産業分野	被害・影響	原因・攻撃手法	注目ポイント（攻撃の新規性、被害規模に注目）	影響度	発生可能性	攻撃タイプ
32	**	I	米国数百の歯科クリニックがランサムウェア被害	2019/8/29	米国	情報システム（重要インフラ）	医療	米国で、数百の歯科クリニックが、ランサムウェア被害に遭った。本攻撃では、サイバー犯罪グループが、ウィスコンシン州に本拠地を置くソフトウェアプロバイダーThe Digital Dental Record及びPerCSoftを狙い、両社のサービスを利用している歯科クリニックを標的とした。攻撃者は、エンドユーザではなく、サービスを提供する2社に対して、身代金を要求した。	サイバー犯罪グループは、ソフトウェアの稼働するインフラ基盤に侵入し、顧客である歯科クリニックのシステムにランサムウェアREvil/Sodinokibiを感染させた。	マネージドサービスプロバイダーを狙い、一度に大規模の感染を起こす攻撃手法である。	中	中	マルウェア感染
33	***	V	4万7千台以上のSupermicro社サーバが攻撃対象に	2019/9/3	各国	情報システム	全分野	セキュリティベンダEclypsiumは、Supermicro社サーバのベースボード管理コントローラ（BMC）に、意図しないリモート接続を可能とする脆弱性が存在することを発見した。現在、少なくとも47,000台のSupermicroサーバーが、当該脆弱性の影響で攻撃される可能性があると推測されている。Supermicro社は、サーバを外部ネットワークから直接アクセス可能なエリアに配置しないよう、ユーザへ呼びかけている。	攻撃者は、BMCの脆弱性を悪用し、サーバへリモート接続を行う。サーバへの接続後は、仮想USB CD/DVDドライブの乗っ取り、新しいOSの読み込み、設定の変更、マルウェアの設置、デバイスの完全な無効化等の操作が可能である。	BMCへの特権ユーザアクセスを制御する手段は、未だ確立されていない。	中	大	その他脆弱性攻撃
34	***	C	サイバー犯罪グループAPT10が東南アジアの医療関連施設を攻撃	2019/9/5	マレーシア、ベトナム	情報システム（重要インフラ）	医療	Kaspersky社は、サイバー犯罪グループ「APT10」による、医療関連施設を標的とする攻撃を観測したことを公表した。本攻撃は、2018年の10月から12月にマレーシアで、2019年の2月から5月にベトナムで、実行されたと推測されている。 「APT10」は日本をはじめ、少なくとも12カ国以上に対して攻撃活動を行っている。日本外務省談話においても、「APT10」を非難する内容があった。	攻撃者は、バックドア「ANEL」を含むWord文書を、ターゲットに端末に送り込む。バックドア「ANEL」と関連するモジュールは、従来「APT10」が利用していたリモートアクセスツール（RAT）「Redleaves」とは異なり、セキュリティ製品やマルウェア解析による検知を回避するよう設計されている。また、既存技術を統合し、洗練された攻撃手法を用いて医療関連施設を攻撃する。	重要インフラ分野における複数の国・業界を狙うサイバー犯罪グループによる活動であり、攻撃手法が更に洗練されている。	大	大	マルウェア感染、APT
37	***	C	サイバー犯罪グループAPT3が高度なトロイの木馬を開発	2019/9/6	各国	情報システム	全分野	中国を拠点に活動するサイバー犯罪グループ「APT3」が、米国国家安全保障局（NSA)によって開発された、高機能サイバー攻撃ツールのソースコードをリバースエンジニアリングし、高機能なトロイの木馬「Bemstour」を開発したと報じられた。	攻撃者は、トロイの木馬「Bemstour」を使用し、標的デバイスへバックドア「DoublePulsar」をインストールする。これら2つのツール自体は、サイバー犯罪グループ「Shadow Brokers」によって過去使用されたものの亜種とみられる。しかし、セキュリティ企業Check Point社の分析によると、両者のコードには区別すべき違いがあり、エクスプロイトは再設計され、ゼロから構築されたものと考えるべきであるとされる。	他国の攻撃ツールを収集し、再利用・再構築するという組織的展開の手法である。	大	大	マルウェア感染
35	***	V	約30機種のGPSトラッカーに脆弱性	2019/9/6	中国、各国	コンシューマIoT機器	全分野	中国Shenzhen i365 Tech社が製造した、約30機種のGPSトラッカーに深刻な脆弱性が発見された。通信の暗号化機能が実装されておらず、不正な操作や情報漏えいの可能性がある。当該製品は、全世界で60万台以上が稼働していると推定される。	発見された脆弱性は、以下の通りである。 ①初期設定のパスワード「123456」は、非常に推定されやすい値であり、悪用されるおそれがある。 ②通信データが暗号化されていないため、トラッカーのマイクを通じた盗聴、リアルタイムの正確なGPS座標等の漏えい等のリスクがある。中間者攻撃により、不正操作を行われる可能性もある。	低コスト、大量生産のIoTデバイスのセキュリティリスクが顕在化した事例である。	中	大	不正アクセス
36	***	I	米国の電力網に対する初のサイバー攻撃	2019/9/6	米国	ICS（重要インフラ）	電力	北米電力信頼度協議会（NERC）によると、2019年3月5日に、アメリカ西部の電力網において、電力管理センターに対するサイバー攻撃が行われた。この結果、電力管理センターと発電サイトとの間に5分未満の通信障害が発生したが、センター外での停電は起こっていない。本攻撃はおよそ10時間にも及び、ファイアウォールが短時間（5分未満）停止することとなった。	攻撃者は、電力管理センターが利用していたファイアウォールの脆弱性を悪用し、機器を繰り返し再起動することで、予期しない停止を引き起こした。	米国の電力網に対する初のサイバー攻撃事案と位置付けられる。	大	中	その他脆弱性攻撃

No	注目度	区分	事例名	年月日（報告日等）	発生国	システム区分	産業分野	被害・影響	原因・攻撃手法	注目ポイント（攻撃の新規性、被害規模に注目）	影響度	発生可能性	攻撃タイプ
38	***	C	米国が北朝鮮のサイバー犯罪グループHIDDEN COBRAに関する活動を警告	2019/9/9	米国、各国	情報システム	全分野	米国土安全保障省（DHS）及び連邦捜査局（FBI）は、北朝鮮の関与が疑われるサイバー犯罪グループ「HIDDEN COBRA」が、マルウェア「ELECTRICFISH」及びトロイの木馬「BADCALL 」を用いた活動を展開しているとして、警戒を呼び掛けるレポートを公表した。	報告された各マルウェアの動作は、以下の通りである。 ①「ELECTRICFISH」は、攻撃者のIPアドレスとターゲットのIPアドレス間で、セッションを確立するマルウェアである。攻撃者とターゲットマシンの間に、効率的な通信を行うチャネルを構築する。 ②「BADCALL」は、感染したシステムを強制的にプロキシサーバーとして動作させる。トロイの木馬として動作する。	「HIDDEN COBRA」は、既存マルウェアの亜種などを利用した攻撃キャンペーンを展開する等、再び活動量が増しており、警戒が求められる。	中	大	マルウェア感染
39	**	V	Intel CPUに脆弱性NetCAT	2019/9/12	各国	情報システム	全分野	Intel社のサーバ用CPUに、ネットワークパフォーマンス強化機能を悪用したサイドチャネル攻撃の脆弱性「NetCAT」が発見された。当該機能は、Data Direct I/O（DDIO）技術を利用し、周辺機器へ、最高レベルの速度でのキャッシュ読み込み及び書き込みを可能とする。特に、高速ネットワーク環境でサーバのパフォーマンスを向上させる目的で導入されることが多い。Intel社は、本脆弱性への対策方法を公開した。	攻撃者は、脆弱性「NetCAT」を悪用することで、リモート・キャッシュにアクセスし、SSHセッションから個々のネットワークパケットの到着時間を観察するサイドチャネル攻撃を行う。これらのパケットの到着タイミングを静的分析し、SSHセッションの通信内容を推測する。	CPUの機能に関する脆弱性であり、機器調達等に与える影響が大きい。本件は、CVSS基本値も低い（2.6）が、低レイヤの脆弱性は、対策が難しくなるため、特に深刻な脆弱性の情報には注意が必要である。	大	中	その他脆弱性攻撃
40	***	I	4億枚の医療放射線画像がインターネットで公開状態に	2019/9/18	各国	情報システム（重要インフラ）	医療	セキュリティ企業Greenbone Networks社は、医療分野で使用されるPicture Archiving and Communication System（PACS）に、深刻な脆弱性が多数存在することを発見した。インターネットに接続しているPACSを分析すると、約52ヶ国600台のサーバが、不正アクセスを受ける可能性がある状態と判明した。合計で、約4億枚の医療画像がインターネット上に公開され、ダウンロード可能な状態となっていた。	PACSシステムには、数千件もの未対応の脆弱性が存在することが判明した。重大度が最高レベルの脆弱性のみで、500件を超えており、攻撃者はこれらを悪用して様々な手法を組み立てることが出来る。	機密性の高い医療データを取り扱うシステムだが、セキュリティ対策に極めて多くの不備が存在し、重大な情報漏えい事故を生じた事案である。	大	大	不正アクセス
41	***	I	米国の公共サービス業者を狙うフィッシング攻撃	2019/9/24	米国	情報システム（重要インフラ）	電力	Proofpoint社は、4月5日から8月29日までの5か月間に、米国で電力事業に関わる公共サービス業者17社以上が、フィッシングメールの標的となっていた旨を報告した。フィッシングの戦術、手法、及び手順（TTP）から、中国を拠点に活動するサイバー犯罪グループ「APT10」の関与も疑われている。	攻撃者は、グローバルエネルギー認証「GEC」のロゴを使用し、認証テストへの参加を誘うような内容のフィッシングメールを送信した。メールを受信した電力事業会社の従業員に、リモートアクセス機能を含む高機能型トロイの木馬「LookBack」を感染させる。 フィッシングメールの内容から、攻撃者の狙いは、米国の送電網インフラ、原子力発電所、風力発電所、石炭火力発電所と関連する事業者であったと考えられる。	特定の業界を対象とした、完成度の高いフィッシングメールが用いられている。業界内の実在の認証機関になりすまし、当該機関を知る受信者を標的にしている。	大	大	APT、フィッシング
42	**	V	フォーラムサイト構築ソフトウェアvBulletinの脆弱性に対する攻撃	2019/9/24	各国	情報システム（重要インフラ）	全分野	フォーラムサイトを構築するソフトウェア「vBulletin」の脆弱性（CVE-2019-16759）を狙う攻撃が多数検出され、注意喚起が行われた。vBulletinはNASA、SONY、EA、Zyngaといった公的機関、有名企業のオンラインフォーラムにおいても利用されている。修正パッチは、直ちにリリースされたが、本脆弱性の悪用を試みたとみられる攻撃の痕跡は、10,000件以上検出された。	攻撃者は、vBulletinの当該脆弱性を悪用することで、リモート環境から任意のコードを実行可能である。CVSS v3による深刻度の基本値は9.8と算出された。ホストシステムを完全に制御し、マルウェアのダウンロード、他システムへのアクセス、データの窃取、悪意のあるコード実行等を行うことが出来る。	広く普及したソフトウェアやAPIの深刻な脆弱性に対して、パッチ適用前のタイミングを狙った迅速な攻撃を仕掛けている。	中	大	不正アクセス、マルウェア感染、その他脆弱性攻撃等

No	注目度	区分	事例名	年月日（報告日等）	発生国	システム区分	産業分野	被害・影響	原因・攻撃手法	注目ポイント（攻撃の新規性、被害規模に注目）	影響度	発生可能性	攻撃タイプ
44	***	I	ドイツ自動車部品メーカーがマルウェア感染で3億円以上の損失	2019/9/26	ブラジル、メキシコ、米国	ICS（重要インフラ以外）	製造	ドイツの自動車部品メーカー「Rheinmetall Automotive」は、9月24日夜にマルウェア攻撃の被害を受けた。この攻撃は、ブラジル、メキシコ、米国の工場で利用されていたITインフラに影響を与えた。これにより、生産プロセスに大きな混乱が生じた。一連の事象による損失額は、300～400万ユーロと見積もられている。	未公開。（調査中）	製造業の工場では、多くのレガシー組込み機器が用いられている。Forescout社は、管理されていないWindowsデバイスをはじめとして、問題のあるデバイスが利用され続けているケースが多いことを指摘している。	中	大	マルウェア感染
43	***	C	エアバスに対するサプライチェーン攻撃が発生	2019/9/26	欧州	情報システム（重要インフラ）	航空	欧州の航空大手であるエアバスは、サプライチェーンに対する一連の攻撃を受けた。フランス通信社は、攻撃者の目的は、営業秘密を探り出すことにあったと推測され、中国と関連するハッカーによる犯行との見解を報じている。	攻撃者は、英国のエンジンメーカーRolls-Royce社や、フランスの技術コンサルティング企業であるExpleoといった、エアバスからの業務委託を請負う事業者を標的とした。エアバスへ接続可能なVPNを経由した不正アクセスを行い、秘密文書データを不正に入手した。攻撃者の狙いは、エアバス航空機の認証プロセスに関連する技術文書であったとされる。	相対的にセキュリティ対策レベルの低い業務委託先が狙われた結果、委託元の重要機密が漏えいした事例である。典型的なITサプライチェーン攻撃により、攻撃者の狙いが明確である点にも注目すべきである。	大	大	不正アクセス、その他脆弱性攻撃（サプライチェーン）
46	***	V	IPnetソフトウェアの脆弱性が医療分野等の数百万の組込みデバイスに影響	2019/10/1	各国	ICS（重要インフラ）	医療	米国FDAとDHSは、医療、SCADAシステム、産業用コントローラーなどに関係する脆弱性「URGENT/11」について、注意喚起を行った。本脆弱性は、20億以上のデバイスへ組み込まれているリアルタイムOSに関するものであり、医療分野で使用される5つのOSにも影響を及ぼす。	攻撃者は、IPnetのコンポーネントに存在する脆弱性を悪用することで、機器やシステムへ認証を経ずにリモートログインし、制御することが可能となる。その上で、所定のコードを実行することで、機能の変更、データの窃取、DoS攻撃等を行う。	開発者によるサポートが終了したサードパーティ製コンポーネントに発覚した脆弱性であり、対応が難しいサプライチェーンリスクである。医療機器を遠隔操作される危険のある脆弱性でありながら、依然として機器・システムの利用をそのまま継続しているユーザも存在すると報じられている。	大	大	不正アクセス、その他脆弱性性攻撃（サプライチェーン）
45	**	C	米国の石油会社を標的とする攻撃キャンペーン	2019/10/1	米国	情報システム（重要インフラ）	石油	セキュリティ企業Netskope社は、石油業界を狙うマルウェア「ADWIND」の亜種を観測したことを報告した。当該マルウェアは、高度な難読化が行われており、JARファイルまたはJavaアーカイブを利用し、コンパイルされた複数のファイルを1つのファイルに集約する。セキュリティ研究者Abhinav Singh氏は、この手口は複数のOSを標的とする場合に、理想的な選択肢となると分析している。	攻撃者は、マルウェア「ADWIND」の亜種を標的端末に送り込みし、情報の探索を行う。機密情報が記録されたドキュメント以外にも、更なる侵入を実現するため、FTP用のパスワード、SSH鍵等の情報を探索した痕跡が確認されている。	旧来のマルウェアを、高度な難読化やパッケージ化を行うことで、検知の難しい攻撃ツールとして再活用している。	中	大	マルウェア感染

No	注目度	区分	事例名	年月日（報告日等）	発生国	システム区分	産業分野	被害・影響	原因・攻撃手法	注目ポイント（攻撃の新規性、被害規模に注目）	影響度	発生可能性	攻撃タイプ
47	***	V	Androidデバイスに影響するゼロディ脆弱性use-after-free	2019/10/4	各国	コンシューマIoT機器	全分野	Google Project Zeroは、Androidデバイスにメモリ制御の脆弱性「use-after-free」（CVE-2019-2215）を発見したことを報告した。本脆弱性は、ローカル権限昇格を可能とするものであり、何億台ものAndroid OSを搭載したスマートフォンに影響する。	攻撃者は、対象デバイスにローカルアクセス可能な条件下では、本脆弱性を悪用することで権限昇格を行うことが可能である。権限昇格の実施後は、悪意のあるアプリのダウンロード、Webブラウザーを通じた他のデバイスへの感染拡大、外部への攻撃等を行うことが考えられる。	影響の範囲が広さから、メーカーによる対応が間に合っていない部分がある。	中	大	その他脆弱性性攻撃
48	**	C	米国選挙システムを狙うイランによるサイバー攻撃	2019/10/8	米国	情報システム（重要インフラ）	政府・行政サービス	Microsoft社によると、政府組織と関連があると推測されるサイバー犯罪グループ「Phosphorus」（APT25、Charming Kittenとも呼ばれる）が、Microsoft社のメールサービスを利用するユーザアカウントに対して、2,700回以上の侵入を試みたと推測される痕跡が確認された。標的となったアカウントは、米国大統領選挙キャンペーン、米国政府関係者、政治ジャーナリスト、国外に居住するイラン国民が所有するアカウント等である。	攻撃者は、ターゲットに関連する情報（電話番号や予備のメールアドレスなど）を使用して、メールアカウントに侵入しようとした。	政治的意図が明らかなサイバー攻撃である。本件では、実害は発生しなかったが、2020年の総選挙に向けて更なる攻撃の発生が予想される。	中	大	不正アクセス
49	***	I	ドイツPilz社がランサムウェア被害	2019/10/14	ドイツ	情報システム	全分野	ドイツのオートメーション技術ベンダー大手Pilz社は、10月14日に自社のTwitterアカウントから、サイバー攻撃を受け、調査のためにPC群をネットワークから切り離すことを余儀なくされたことを報告した。この結果、受注、配送業務を処理することができなくなり、70ヶ国以上の支社及び取引先に影響が出たとされている。	Pilz社は、感染ルート等の詳細を公表していないが、ランサムウェア「BitPaymer」による被害であるとみられている。ランサムウェア「BitPaymer」は、他のランサムウェアと異なり、厳選されたターゲットのみ送付される。このため、ランサムウェアの特定及び解析が難しい。この戦略は「big-game hunting」と呼ばれる。	世界中の支社に影響を及ぼす事態となっており、自己複製型ランサムウェアの脅威を改めて知らしめる事案となった。重ねて、標的型ランサムウェアの検知が困難であることも大きな脅威である。	大	中	マルウェア感染
50	***	I	郵便料金計器メーカーの世界最大手米Pitney Bowes社がランサムウェア被害	2019/10/17	米国、各国	情報システム（重要インフラ）	物流	郵便料金計器の世界最大手メーカーである、米Pitney Bowes社が、10月12日にランサムウェア攻撃を受け、郵便料金計器の残額補充システム、集計レポートシステム等の機能が停止した。10日後（10月22日）には、主要なシステムが復旧したことを発表したが、対応作業は継続された。	攻撃者は、ランサムウェア「Ryuk」を利用し、米Pitney Bowes社の一部のシステムを暗号化し、サービスへのアクセスを不可能にした。	FBI（米国連邦捜査局）、USPIS（米国郵便監察官）が捜査に動いており、社会的影響の大きさが伺える。	大	大	マルウェア感染
51	***	C	スマートスピーカーAmazon AlexaとGoogle Homeを悪用する攻撃手法	2019/10/21	ドイツ	コンシューマIoT機器	全分野	ドイツの研究者は、スマートスピーカーAmazon AlexaとGoogle Homeを悪用し、会話の盗聴、パスワード窃取等を実行可能なアプリを開発した。このアプリは、Amazon及びGoogleのセキュリティ検証プロセスにも合格している。当該研究は、スマートスピーカーのセキュリティ対策の問題点を示す目的で行われた。	ユーザが、スマートスピーカーに指示を出した後に、フィッシングアプリが、エラーメッセージを返すと同時に盗聴アプリを動作させる。約1分後、Amazon AlexaまたはGoogle Homeの音声をまねて、デイバスの利用を継続するためには、デバイスの更新ファイルをインストールする必要があると説明し、パスワードを要求する。そして、ユーザが回答したパスワードを記録する。	スマートスピーカーを通じたフィッシング攻撃の手法が実証された。	中	中	フィッシング
52	***	C	英国NCSCがロシアのサイバー犯罪グループTurlaに関する攻撃キャンペーンに注意喚起	2019/10/21	英国、各国	情報システム	全分野	ロシアに拠点を持ち、英国の組織を標的とするサイバー犯罪グループ「Turla」の攻撃活動を分析したレポートが、英国NCSCによって発表された。「Turla」が使用しているマルウェアツール「Neuron」、「Nautilus」は、イランの関与が疑われるサイバー犯罪グループ「APT34」が使用したツールから派生した可能性が高いと判断されている。	「Turla」は、「APT34」が使用する攻撃ツールだけでなく、不正コマンドや制御インフラストラクチャに関する情報も手に入れていたと考えられる。他のグループが開発したツール等を利用し、更に多様な攻撃手法を実現している。	APTグループ間で何らかの協力もしくは情報交換等が行われている可能性も考えられる。	中	小	その他脆弱性攻撃

No	注目度	区分	事例名	年月日（報告日等）	発生国	システム区分	産業分野	被害・影響	原因・攻撃手法	注目ポイント（攻撃の新規性、被害規模に注目）	影響度	発生可能性	攻撃タイプ
53	***	I	ホテル予約システムAutoclerkから米国政府に関する情報漏えい	2019/10/22	米国	情報システム	全分野	ホテル予約システムAutoclerkのデータベース（Elasticsearchを利用）から、約179GB、計数十万件のホテル予約情報が漏えいしたことが発覚した。vpnMentor.comは、漏えいした情報には、米国政府、米軍や国土安全保障省（DHS）に勤務する職員の個人情報や旅行手配情報等も含まれていたと報じている。	当該データベースが、インターネット上に公開されていた具体的な理由は明らかになっていない。ただし、vpnMentor.comが当該事象を発見した際、US-CERTに報告したにもかかわらず、US-CERTからの反応はなかった。漏えいした情報の性質を考慮すれば、深刻な被害が発生する可能性もあった。	重要インフラへのサイバー攻撃による被害ではないが、設定ミス等の瑕疵であっても、国家安全保障という観点からの重大な事故となりうる。	大	－	不正アクセス
55	***	C	オーストラリアの重要インフラや医療機関等がマルウェアEmotetに相次いで感染	2019/10/25	オーストラリア	情報システム（重要インフラ）	政府・行政サービス、医療	オーストラリア・サイバーセキュリティセンター（ACSC）は、オーストラリアの重要インフラや医療機関等が、相次いでマルウェア「Emotet」に感染したと発表した。少なくとも19以上の企業や機関が被害を受けたとみられ、広範囲に影響を及ぼした。Emotetマルウェアキャンペーンに対して、US-CERTも注意喚起を行った。	マルウェア「Emotet」は、電子メールに埋め込まれたURLまたはWordファイルを介して拡散することが多い。悪意のあるURLやファイルを開いた際に、Microsoft Officeスイートのマクロ機能を利用し、標的端末にマルウェアをダウンロードさせる。 「Emotet」には、感染端末の情報を収集し、他のターゲットに過去のやりとりを模した、返信型メールを送付する機能がある。返信型メールを見破ることは難しく、感染拡大力の強さの一因となっている。	感染端末の情報を利用し、ソーシャルエンジニアリングの手口による感染拡大を行うことから、フィッシングメールであることを見破ることが極めて難しい。	大	大	マルウェア感染、フィッシング、ソーシャルエンジニアリング
54	**	I	三菱UFJ銀行海外拠点の認証システム不備による情報漏えい	2019/10/25	台湾	情報システム（重要インフラ）	金融	三菱UFJ銀行が台湾で提供するネットバンキングサービス「ローカルキャッシュマネジメントサービス」の認証システムが、利用していた通信暗号化装置（東京に設置）の脆弱性が原因となり、台湾拠点に開設された口座番号等1305件の情報が流出したことが判明した。	攻撃者は機器のに脆弱性を悪用し、通信の暗号化を実質無効化し、不正アクセスを行ったと考えられる（製品情報、脆弱性は公開されていない）。	本件との直接的関係性は言及されていないが、9/6に複数メーカーのVPN製品の脆弱性に関する注意喚起がなされている。仮に、当該脆弱性が悪用されていた場合、脆弱性情報の公開から短期間で攻撃を行い、対応の間に合っていない企業を狙った可能性が考えられる。	小	中	不正アクセス
56	***	I	インド原子力発電所にサイバー攻撃	2019/10/31	インド	情報システム（重要インフラ）	電力	インドのKudankulam原子力発電所において、情報搾取を目的としたマルウェアが組、織内のPCから検出されたことをインド原子力発電公社が認めた。原発公社によると、マルウェアが検出されたのは、管理業務に使用されるPCで、原子力発電の制御に関係する重要な内部ネットワークとは隔離されていたという。攻撃者は、情報システムに保管された大量のデータへのアクセス可能であったとみられる。	北朝鮮に活動拠点を持つと見られる犯罪グループ「Lazarus」が、本件に関与していると疑われている。今回のサイバー攻撃で使用されたのは、「Dtrack」と呼ばれるマルウエアである。「Dtrack」は、2016年に、同じくインドにおいて、個人の金融情報を狙い、ATMを標的とした攻撃に使われた事例がある。	原子力発電所を狙った攻撃であり、被害が生じた場合の影響が極めて大きい。過去の「Stuxnet」事例のように、窃取した発電所内の情報を利用し、標的型マルウェアを作成、内部ネットワークに何らかの手段で送り込むといった継続攻撃がなされる可能性もあり、注意が必要と考えられる。	大	中	マルウェア感染
57	**	V	Siemens社PLCに悪用可能なバックドアが発覚	2019/11/5	各国	ICS（重要インフラ以外）	全分野	Siemens社製の小中規模のシステム向けPLC「SIMATIC S7-1200」に、ドキュメントへの記載がないアクセス機能（バックドア）が発見された。当該機能を悪用すれば、非正規のユーザが、PLCのプロセス制御機能をコントロールすることが可能となる。	攻撃者は、バックドアを経由してPCへアクセスする。そして、PLCの起動から0.5秒以内にブートローダのファームウェア整合性チェックをバイパスし、PLCのプロセス制御を操作するコードをロードする。ただし、本アクセス機能を使用することで、PLCメモリの内容を表示することができ、悪意のあるコード発見することも可能である。	メンテナンス機能等は、正式リリース製品に残存していた場合、権限の強い操作を実行可能な脆弱性となってしまうことが分かる。	中	中	不正アクセス
58	***	V	Medtronic社の電気手術器に複数の脆弱性	2019/11/7	各国	ICS（重要インフラ）	医療	US-CERTは、Medtronic社製の電気手術器「Valleylab FT10」及び「同FX8」に複数の脆弱性（CVE-2019-13543、CVE-2019-13539、CVE-2019-3464）が存在するとして、注意喚起を行った。	攻撃者は、リモートから特定の攻撃コードを送信することで、ファイルの上書き、不正コードの実行等を行うことが可能である。また、本手法は、必要とされる技術レベルが低いため、容易に悪用することが可能であり、危険度が高い。	容易に実行可能でありながら、医療手術の安全性に影響する危険性がある。	大	中	その他脆弱性攻撃等

No	注目度	区分	事例名	年月日（報告日等）	発生国	システム区分	産業分野	被害・影響	原因・攻撃手法	注目ポイント（攻撃の新規性、被害規模に注目）	影響度	発生可能性	攻撃タイプ
60	***	I	メキシコ石油公社Pemexがランサムウエアに感染	2019/11/12	メキシコ	情報システム（重要インフラ）	石油	メキシコの国営石油公社Pemexは、ランサムウェアの被害に遭い、490万ドルの身代金を要求された。Pemex社は、ランサムウェアによる影響を受けたコンピュータは全体の5%以下であり、燃料の生産、供給、在庫への影響はなかったと発表した。しかし、職員又はサプライヤーへの支払業務に影響が出る可能性も報道されている。	Pemex社は、感染したランサムウェアについての詳細は公表していない。セキュリティベンダCrowdstrike社は、ランサムウェア「DoppelPaymer」による攻撃であった疑いがあると分析している。	多額の身代金が要求されたランサムウェア感染事例である。	大	大	マルウェア感染
59	***	C	TCP増幅を利用するDrDoS攻撃が増加	2019/11/12	各国	情報システム	情報通信、金融	セキュリティベンダRadware社は、TCP増幅を利用した大規模なDrDoS攻撃の観測レポートを公表した。ヨーロッパのスポーツギャンブルサイトEurobet、トルコの金融サービス企業Garanti、韓国企業Telecom及びSK Broadbandの公式サイトが、本攻撃の影響を受けたと報告された。	攻撃者は、SYNパケット（ターゲットネットワークのIPアドレスから発信されたように見えるよう偽装されたもの）を、多数の外部IPアドレス又はリフレクションサービスに送信し、SYN-ACKパケットの応答をさせた。ターゲットネットワークからの返答がない場合、外部IPアドレスからは、SYN-ACKパケットが送り続けることになり、DoS攻撃の増幅率が上がる。	DrDoS攻撃は、ターゲットだけに被害を与えるだけでなく、増幅に利用されたネットワーク周辺にも影響を及ぼす。	中	大	DDoS/DoS等
61	**	C	ショッピングサイトを狙うマルウェアPipka	2019/11/13	米国	情報システム	小売	ショッピングサイトに潜み、顧客の入力データを収集するマルウェア「Pipka」が、Visaのセキュリティ研究者により発見された。マルウェア「Pipka」は、JavaScriptプログラミング言語で記述されたスキマー（クレジットカードの情報を抜き取るもの）である。	マルウェア「Pipka」は、以下の理由から検知が難しいという特徴がある。 ①webページの読込後に実行されるJavaScriptを利用し、webページをリロードせずデータを抽出可能 ②侵害されたサイトのHTMLソースコードから、自身の痕跡を削除することが可能	JavaScriptの普及拡大に伴い、スキマー等の電子商取引を狙った攻撃等への悪用も進展している。	中	大	マルウェア感染
62	***	C	イランのサイバー犯罪グループが重要インフラに対する攻撃キャンペーン	2019/11/20	各国	情報システム（重要インフラ）	電力、石油	マイクロソフトのセキュリティ研究者Ned Moranがイランのサイバー犯罪グループ「APT33」が重要インフラへの物理的な破壊を伴うサイバー攻撃を企んでいる可能性について警告した。その中には、電力会社、製造業、石油精製業界の制御システム含まれると考えられる。	イランのサイバー犯罪グループ「APT33」が、過去1年間に、何万もの組織のユーザアカウントに対してパスワードスプレー攻撃（ブルートフォース攻撃の一種）を実行したことが確認された。 攻撃対象となるアカウントは、産業用制御システム機器のメーカー、サプライヤー、または保守業者の電話番号であるため、制御システムを狙い攻撃していると推測される。	重要インフラに対するAPT攻撃の前段階と考えられる。	大	中	不正アクセス
63	***	I	ニューヨーク警察がランサムウェア被害	2019/11/24	米国	情報システム（重要インフラ）	政府・行政サービス	ニューヨーク警察（NYPD）は、所管する指紋追跡システム「LiveScan」に接続された23台のマシンが、ランサムウェアに感染したことを受け、システムを一時的に停止した。NYPDは、影響を受けた端末は、署内全体の0.1%程度であったと発表した。しかし、NYPDのデータベースは、州全体のシステムとリンクしており、二次被害の可能性も懸念されている。	保守請負業者が、ランサムウェアに汚染された端末を、署内のシステムに接続したことが感染経路と考えられている。保守業者の端末が、汚染された経緯の詳細は不明（調査中）。	公共機関の保有する機密情報データベースへの侵害であり、影響範囲が大きい。	大	中	マルウェア感染

No	注目度	区分	事例名	年月日（報告日等）	発生国	システム区分	産業分野	被害・影響	原因・攻撃手法	注目ポイント（攻撃の新規性、被害規模に注目）	影響度	発生可能性	攻撃タイプ
64	***	C	悪意のあるSDKが再びGoogle Playに混入	2019/11/25	各国	コンシューマIoT機器	全分野	2019年1月から3月にかけて、Google Playにおいて、広告詐欺を行うAndroid向けゲームアプリが発見された。広告詐欺は、アプリ開発に用いられたSDK（Software Development Kit）が原因で表示されていた。このSDKは、中国企業1tu1shuによって開発された「Tushu SDK」と呼ばれるもので、White Ops Threat Intelligence Teamは、当該ゲームアプリ以外にも、本SDKを用いたアプリには、マルウェアに近い挙動があることを指摘していた。今回、同SDKに新たに検知回避機能を加えたバージョンが、「Twoshu SDK」という名称で再びGoogle Playに存在していることがわかった。	攻撃者は、Tushu SDKを用いて開発されたアプリを通じて、ユーザ送信データの収集、詐欺広告の配信を通じた収益獲得を狙う。Tushu SDKは、アプリの挙動と関係なく、広告のフルスクリーン表示を行い、ユーザによるクリックを誘発する。加えて、Twoshu SDKでは、XOR暗号法を用いた難読化が行われている。これにより、アプリ解析に多くの時間を要するようになり、不正機能としての検知が難しくなっている。	アプリそのものではなく、開発に用いるSDKに不正機能が実装されている。依存コンポーネントに存在するサプライチェーンリスクに関する事案と解釈することができる。	中	大	マルウェア感染、サプライチェーン
65	***	C	JPCERT/CCがマルウェアEmotetの被害拡大に注意喚起	2019/11/28	各国	情報システム	全分野	JPCERT/CCは、マルウェア「Emotet」による被害の増加について注意喚起を行った。マルウェア「Emotet」は、盗み出した情報を利用した高精度のなりすましメールを送信することで、感染対象を拡大させる。アパレル商社であるサンウェル社等が、なりすましメールによる被害を受けた。	マルウェア「Emotet」は、感染端末から情報を窃取し、更なる感染拡大に利用するマルウェアである。フィッシングメールに添付された、悪意のあるマクロを含むWordファイルを通じて、端末内に保存されるパスワードやメール情報等の収集を狙う。更に、取得した情報を利用することで、これまでやりとりされた文脈を踏まえた返信型メールの送信等を行う。見破ることが非常に難しい高度なフィッシングをであり、感染拡大能力が極めて高い。	感染拡大能力の高さから、二次被害の広まりが懸念される。	中	大	マルウェア感染
66	***	V	全てのバージョンのAndroidに影響する脆弱性StrandHogg	2019/12/2	各国	コンシューマIoT機器	全分野	Promon社の研究者によって、全てのバージョンのAndroidに影響する脆弱性「StrandHogg」が発見された。攻撃者は、正当なアプリを悪用し、マルウェアの配信や不正な情報収集を行うことができる可能性がある。既に、60社の金融機関を標的となり、本脆弱性を悪用したアプリは36種類発見されている。	攻撃者は、Android OSのマルチタスクシステムを悪用し、正規アプリの見た目を模した不正アプリへ権限を要求する。ユーザが気づかずに同意してしまうと、メッセージ履歴、写真、資格情報、電話での会話内容等を取得する権限を与えてしまう可能性がある。	見た目を模すという手段によって、ユーザ自身が狙われ、正当な手続きで不正アプリに権限を与えてしまっている。	中	大	その他脆弱性攻撃
67	**	C	バンキング型トロイの木馬TrickBotが日本まで蔓延	2019/12/3	各国	情報システム	全分野	IBM X-Forceによれば、バンキング型トロイの木馬「TrickBot」は、最も活発なトロイの木馬の一つである。一般的な攻撃対象に加えて、モバイルデバイスやヘルスケア企業を標的とする。今までは、英語圏を中心に検知されていた「TrickBot」だが、日本の銀行を標的とした攻撃事例が確認された。ECサイトや仮想通貨交換所等を運営する組織に向けて、「TrickBot」への注意喚起が出されている。	「TrickBot」は、様々な方法での感染が試みられてきたマルウェアであるが、2019年に入ってからは、メールへ不正ファイルを添付する方式に替わり、URLリダイレクト方式が用いられはじめていた。 日本企業を標的とした攻撃キャンペーンでは、「Emotet」によるスパムメールによって、「TrickBot」への感染を狙う手法が用いられている。「TrickBot」は、銀行のwebサイトに対してインジェクション攻撃を行い、個人情報やカード情報等を窃取する。また、「TrickBot」を用いた攻撃が、ランサムウェア「Ryuk」による攻撃へ発展する可能性が懸念されている。	主要なマルウェアが、言語の壁を越えて活動を拡大している。	中	大	マルウェア感染、インジェクション
68	***	C	中東の組織を標的とするディスクワイピングマルウェア	2019/12/4	中東	情報システム（重要インフラ）	石油	イランの関与が疑われるサイバー犯罪グループ「APT34/OilRig」が、中東のエネルギー関連企業を標的とした攻撃キャンペーンを展開している。攻撃には、Windowsシステムのデータを破壊するマルウェア「ZeroCleare」が用いられている。「ZeroCleare」は、2012年にサウジアラビアの石油会社Saudi Aramcoに対し、同社が保有する35,000台以上のWindowsシステムを破壊した「Shamoon」に類似した挙動をする。	マルウェア「ZeroCleare」は、ディスクの内容を破壊的に消去するマルウェアである。本マルウェアは、正規のツールキットであるEldoS RawDiskを使用し、Windowsシステムのマスターブートレコード（MBR）及びディスクパーティションを上書きする。EldoSはファイル、ディスク、及びパーティションを管理するドライバであるため、Windows OSのセキュリティ機能を回避することが可能である。	破壊目的のDoS攻撃であり、エネルギー安全保障上のリスクにつながる攻撃の可能性もある。	大	中	APT、マルウェア感染、DDoS/DoS等

I：インシデント、V：脆弱性、C：攻撃キャンペーン

No	注目度	区分	事例名	年月日（報告日等）	発生国	システム区分	産業分野	被害・影響	原因・攻撃手法	注目ポイント（攻撃の新規性、被害規模に注目）	影響度	発生可能性	攻撃タイプ
69	***	C	US-CERTがマルウェアDridexについて注意喚起	2019/12/5	各国	情報システム（重要インフラ）	金融	金融セクターを狙うマルウェア「Dridex」及びその亜種を用いた攻撃が、継続的に観測されている。US-CERTは、財務省金融情報局サイバー情報グループ（CIG）と財務省金融犯罪執行ネットワーク局（FinCEN）と協力し、これらの活動を分析したレポートを公表し、注意喚起を行った。	マルウェア「Dridex」には、顧客データの不正収集、業務プロセスやシステムの動作を妨害する機能等がある。攻撃者は、主にフィッシングメールを用いて、マルウェア「Dridex」への感染を狙う。このフィッシングメールには、攻撃対象の事業名、ドメイン、専門用語、及び緊急性を唆す言葉等が用いられ、添付ファイルを開くよう誘引する。	マルウェア「Dridex」には、多くの亜種が観測されている。	大	大	マルウェア感染
70	***	C	自動車業界を狙うサイバー犯罪グループAPT32	2019/12/6	ドイツ	情報システム	製造	Bayerische Rundfunkによると、ドイツの自動車大手BMWのネットワークが、ベトナムを拠点とするとみられるサイバー犯罪グループAPT32（別名OceanLotusもしくはCobalt Kitty）によって、長期的の侵入及び監視を許していた事実が発覚した。本事案は、機密情報の収集を目的とした攻撃であったと考えられている。 BMW社の他にも、韓国のHyundai、日本のトヨタも標的とされていた疑いがある。	攻撃者は、BMWの情報システムに不正侵入し、「Cobalt Strike」というツールをインストールした。このツールでは、端末へのアクセスや、リモート操作等を行うことが出来る。 「Cobalt Strike」は、本体となるペイロードをディスク上には保存せず、メモリ上で実行する。これにより、攻撃の痕跡を検知することが難しくなっている。	「Cobalt Strike」は一般的な商用ソフトウェアであるが、その機能を悪用するサイバー攻撃が多く存在する。	大	中	不正アクセス
71	***	I	米国沿岸警備隊がランサムウェア被害	2020/1/2	米国	ICS（重要インフラ）	政府・行政サービス	米国沿岸警備隊（USCG）のシステムがランサムウェアに感染し、産業用制御システムを操作するために必要となるファイルまで感染したことによりシステムが30時間以上停止した。米国沿岸警備隊（USCG）は2019年12月16日にセキュリティ速報を発行し、さらなる攻撃を防ぐための対策を講じるよう促した。	当該ランサムウェアは電子メールを経由して感染したものである。職員が電子メールに埋め込まれた悪意のあるリンクをクリックしたことによって、ランサムウェアが米国沿岸警備隊（USCG）のネットワークファイルにアクセスすることができた。	フィッシング攻撃により国家安全を揺るがす危険性がある。	大	大	マルウェア感染、フィッシング
72	***	I	外貨両替サービス会社Travelexがランサムウェア被害	2020/1/2	各国	情報システム（重要インフラ）	金融	大みそかに外貨両替サービス会社Travelexがランサムウェア「Sodinokibi」の被害を受け、全ての取引が手動で行わなければならなくなった。またTravelex社内メールのシステムもダウンさした。Travelex社が27カ国にある1200以上の店舗が影響を受けた。	攻撃者がTravelex社の7つのPulse Secure VPNサーバーに脆弱性があるにもかかわらず、パッチを当てていないことを利用し、ランサムウェアを感染させた。	Travelex社は27カ国に拠点があり、ユーザに関する個人情報を多く持っているにもかかわらず、脆弱性対策が不十分である。	中	大	マルウェア感染、その他脆弱性攻撃
73	**	V	Microsoft Accessデータベースに脆弱性MDB Leaker	2020/1/7	米国、各国	情報システム	全分野	Microsoft Accessデータベースに脆弱性「MDB Leaker」（CVE-2019-1463）が発見され、85,000社以上に影響を及ぼす可能性がある。	攻撃者が脆弱性「MDB Leaker」を悪用し、機密データまたはプライベートデータを収集することができる。	MDBファイルに保存される個人情報や機密情報まで漏えいする可能性がある。	中	大	不正アクセス

住所　〒100-8141　東京都千代田区永田町2-10-3

組織　株式会社三菱総合研究所
デジタル・イノベーション本部
サイバーセキュリティ戦略グループ