経済産業省
Ministry of Economy, Trade and Industry

参考資料１

主なインシデント事例

令和４年４月４日

経済産業省　商務情報政策局
サイバーセキュリティ課

高度化・巧妙化するサイバー攻撃の現状

- **昨今のサイバー攻撃は、**企業等の情報を暗号化して金銭をゆすり取る「ランサムウェア攻撃」や、国家支援型の攻撃集団等が特定の企業を執拗に狙う「標的型攻撃」など、**多種多様**。
- 加えて、**サイバー攻撃が高度化・巧妙化**するとともに、あらゆるものがネットワークにつながり、**攻撃の起点が増加**したことで、**サイバー攻撃が社会や産業に「広く」、「深く」影響を及ぼすように**なっている。

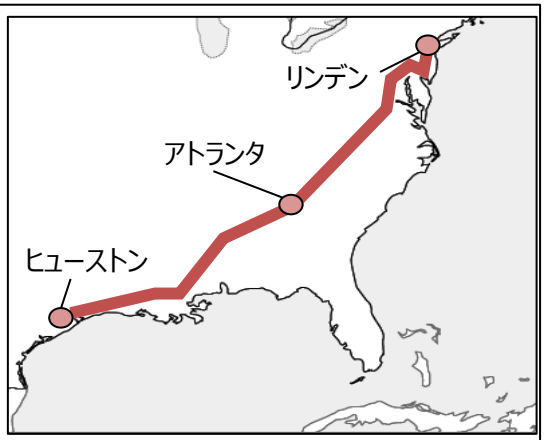
情報セキュリティ10大脅威 2022

順　位	組織向け脅威
1位	ランサムウェアによる被害
2位	標的型攻撃による機密情報窃取
3位	サプライチェーンの弱点を悪用した攻撃
4位	テレワーク等のニューノーマルな働き方を狙った攻撃
5位	内部不正による情報漏えい
6位	脆弱性対策情報の公開に伴う悪用増加
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
8位	詐欺による金銭被害
9位	予期せぬIT基盤の障害に伴う業務停止
10位	不注意による情報漏えい等の被害

<出典：(独)情報処理推進機構(IPA)、2022.1.27>

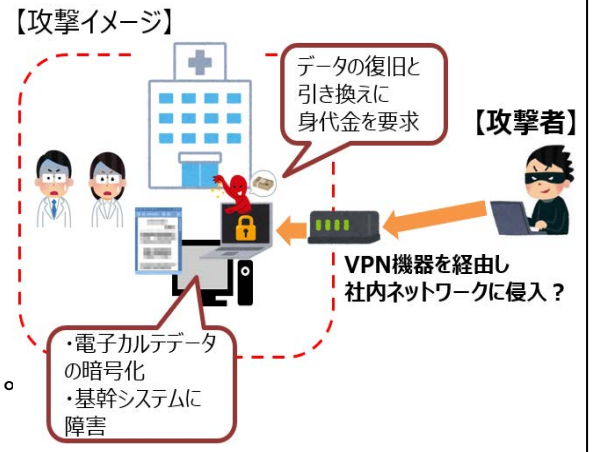
事例（海外）

- 米国の専門機関によれば、米国における重要インフラ事業者等への攻撃のうち、**約1割は制御系システムまで影響を及ぼした**。
- 一例として、2021年5月には、米石油パイプライン大手がランサムウェア攻撃を受け、**全てのパイプラインを一時停止**。米運輸省が燃料輸送に関する緊急措置の導入を宣言する事態に陥った。



事例（国内）

- 2021年10月末、**国内の公立病院がランサムウェア攻撃を受け、電子カルテが暗号化され閲覧不可**になったほか、**診療報酬計算や電子カルテ閲覧に使用する基幹システムが使用不能**になったため、**新規患者の受け入れを停止**。
- 病院は、**身代金要求には応じず**、同年12月29日にサーバーを復旧させ、2022年1月４日から通常診療を再開。



組込み機器に対するランサムウェア攻撃

- 2022年1月、組込み機器向けのセキュリティプロバイダーRed Balloon Security社は、実際のネットワークで使用されている組込みシステムでランサムウェアを展開することが可能であるとの調査結果を発表。
- 同社は、Schneider Electric社製の保護リレーの脆弱性を悪用してランサムウェアのペイロードを展開することが可能で、このプロセスを「高度だが再現可能」と述べている。

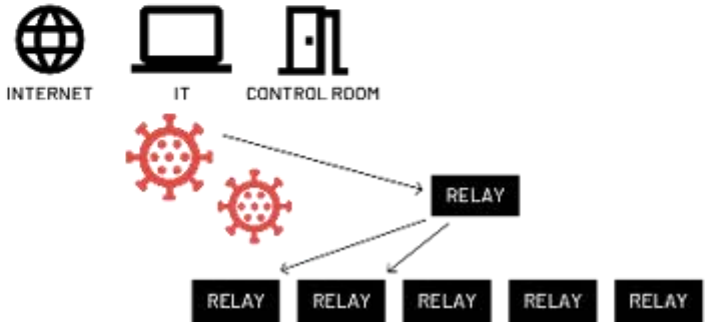
組込み機器に対してランサムウェアを展開する攻撃手法

- Red Balloon Security社は、以下の手法によりランサムウェアの感染等につながる Schneider Electric社製保護リレーの脆弱性を発見。
- 同社は、ミッションクリティカルな機器の完全性や可用性に関して、ランサムウェアが重要な脅威となる可能性を指摘。

物理的なアクセス

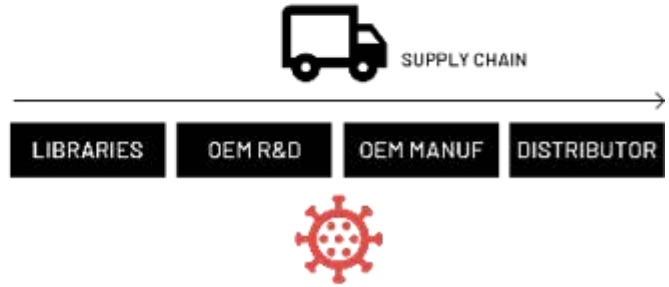
- 実施には、業界内での機器設置状況に関する特定の知識を要するが、現場での機器アクセスによって攻撃が実現し得る。

エンジニアリング・ワークステーション/SCADA経由の感染



- ITシステムを経由してOTシステムへと侵入する。オペレータのアカウントの侵害や、機器に接続する制御システムへの侵入から攻撃が始まる可能性がある。

サプライチェーン攻撃による感染



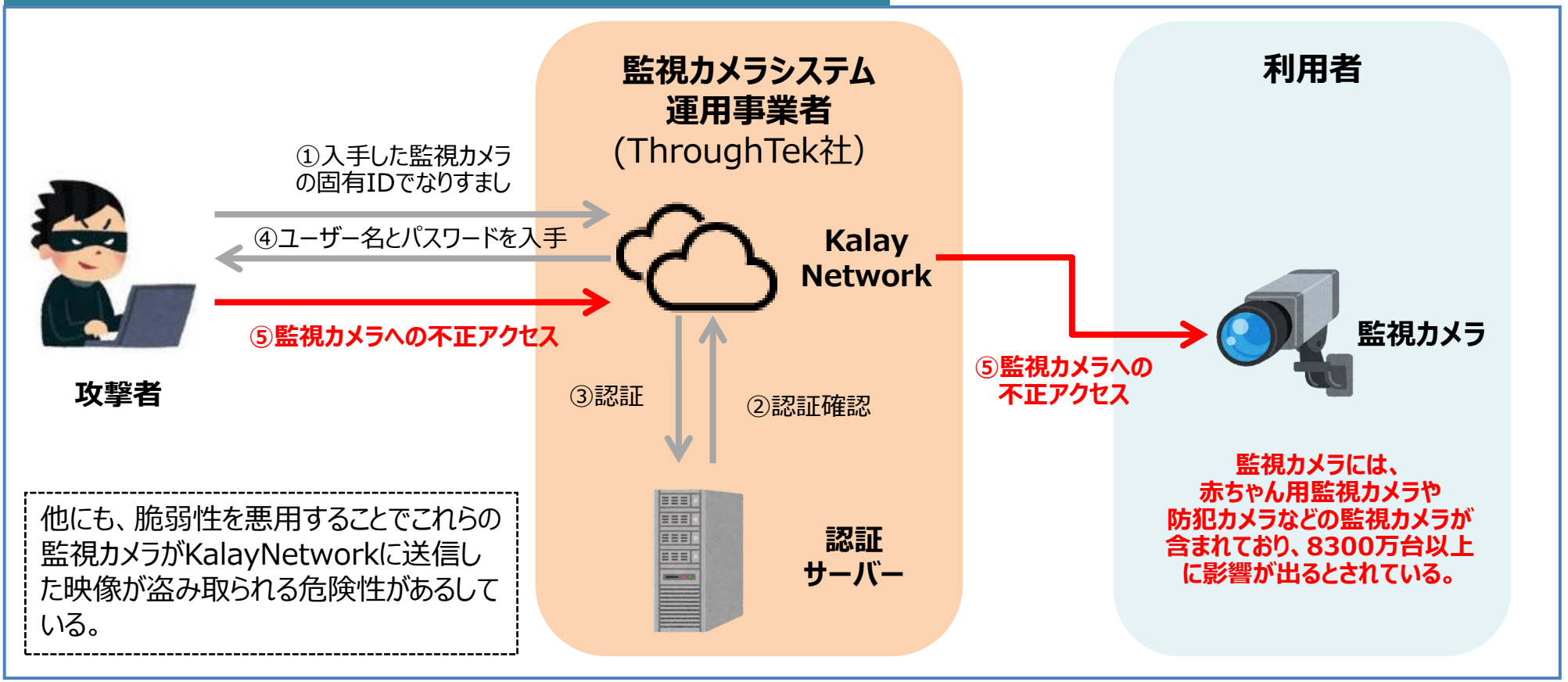
- ライブラリ、製造元の研究開発プロセス、製造プロセス、販売店で出荷を待つ間の機器操作など、様々な段階での侵害が含まれる。

[出典] Red Balloon Security “Ransomware installation on embedded devices is possible, because we’ve done it” を参考に作成

8300万台以上のIoT機器が影響を受ける脆弱性

- 2021年8月、Mandiantは監視カメラを含む8300万台以上のIoT機器が影響を受ける脆弱性「CVE-2021-28372」を発表。KalayNetworkで不適切なアクセス制御がなされる可能性があり、本脆弱性によって、ネットワークカメラの映像を盗み取られたり、家庭内の機器に不正アクセスされる可能性があるとされている。

攻撃者が監視カメラに不正アクセスするイメージ

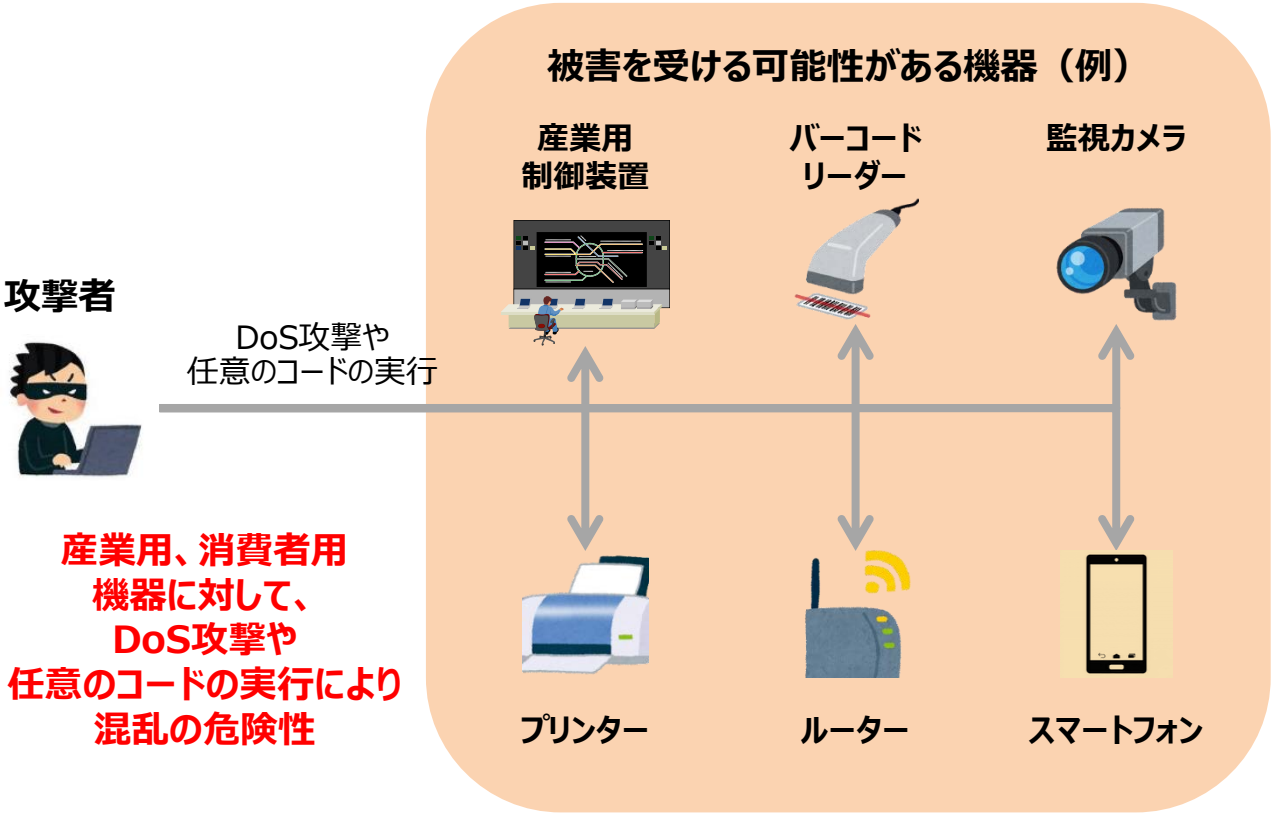


他にも、脆弱性を悪用することでこれらの監視カメラがKalayNetworkに送信した映像が盗み取られる危険性があるとしている。

TCP/IPスタックの脆弱性

- 2020年12月、Forescoutは、複数のオープンソースTCP/IPスタックに「Amnesia33」と呼ばれる脆弱性を発見した。また、2021年4月、ForescoutとJSOFは、複数のオープンソースTCP/IPスタックに「NAME:WRECK」と呼ばれる脆弱性を発表した。
- IoT機器におけるTCP/IPスタックに脆弱性が相次いで発見されており、それぞれの脆弱性が及ぼす影響は100万台から数100万台と言われている。

脆弱性の悪用イメージ



産業用、消費者用機器に対して、DoS攻撃や任意のコードの実行により混乱の危険性

脆弱性「Amnesia33」の影響範囲

以下のTCP/IPスタックを使用している機器

- uIP、Contiki OS、Contiki-NG
- Nut/Net
- FNET
- picoTCP、picoTCP-NG

脆弱性「NAME:WRECK」の影響範囲

以下のTCP/IPスタックを使用している機器

- FreeBSD
- IPnet
- Nucleus NET
- NetXzz

米国上下水道分野における継続的なセキュリティ脅威

- 2021年10月、米国サイバーセキュリティ・インフラセキュリティ庁（CISA）、連邦捜査局（FBI）、環境保護庁（EPA）等は、共同でサイバーセキュリティ勧告を発表し、上下水道への継続的なサイバー脅威について詳述。
- 米国ではこの数年、上下水道施設を対象にしたサイバー攻撃が多数報告されており、地域社会に清潔な飲料水を提供し、効果的に廃水を管理する能力が脅かされているとされる。

上下水道への攻撃事例

2019年から2021年にかけて上下水道システム(WWS)への攻撃が多数発生している。

2021年3月

ネバダ州にてWWS施設のSCADA及びバックアップに対して未知のランサムウェアによる攻撃

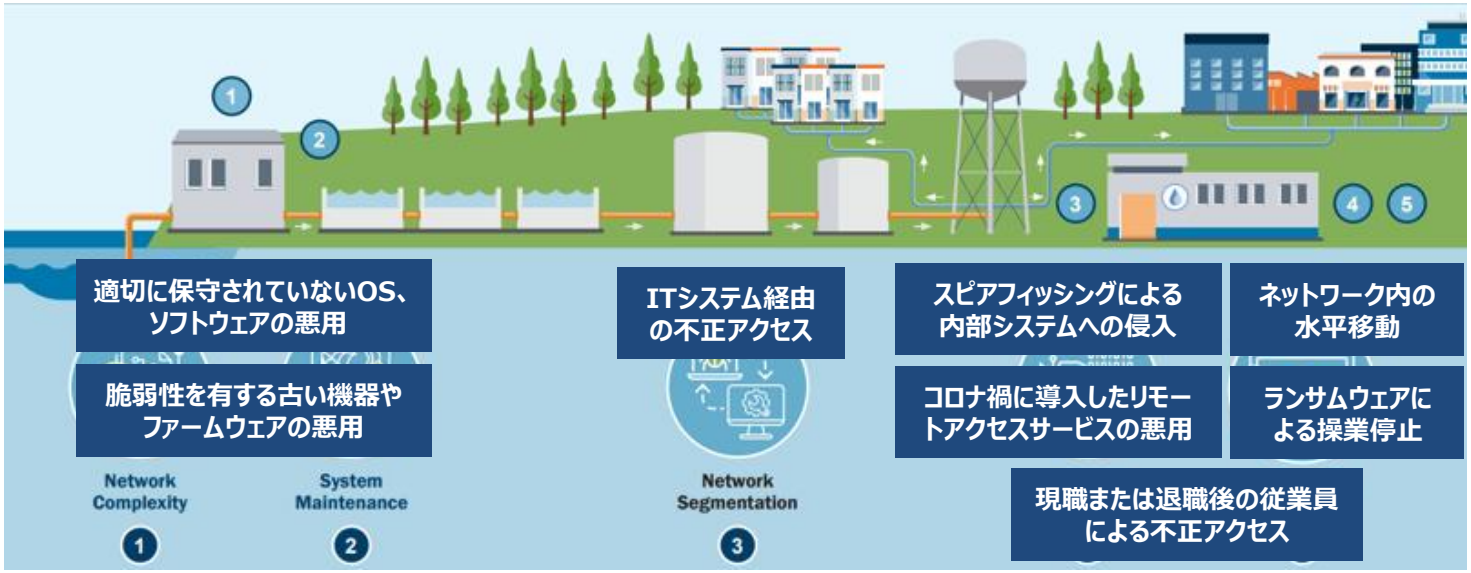
2021年7月

メイン州にてWWS施設のSCADAがランサムウェア ”ZuCaNo”に感染。復旧まで、手動のオペレーションを強制

2021年8月

カルフォルニア州のWWS施設にて3台のSCADAサーバがランサムウェア”Ghost”亜種に感染

共同勧告にて注意喚起がなされている脅威と推奨される対策



推奨される対策

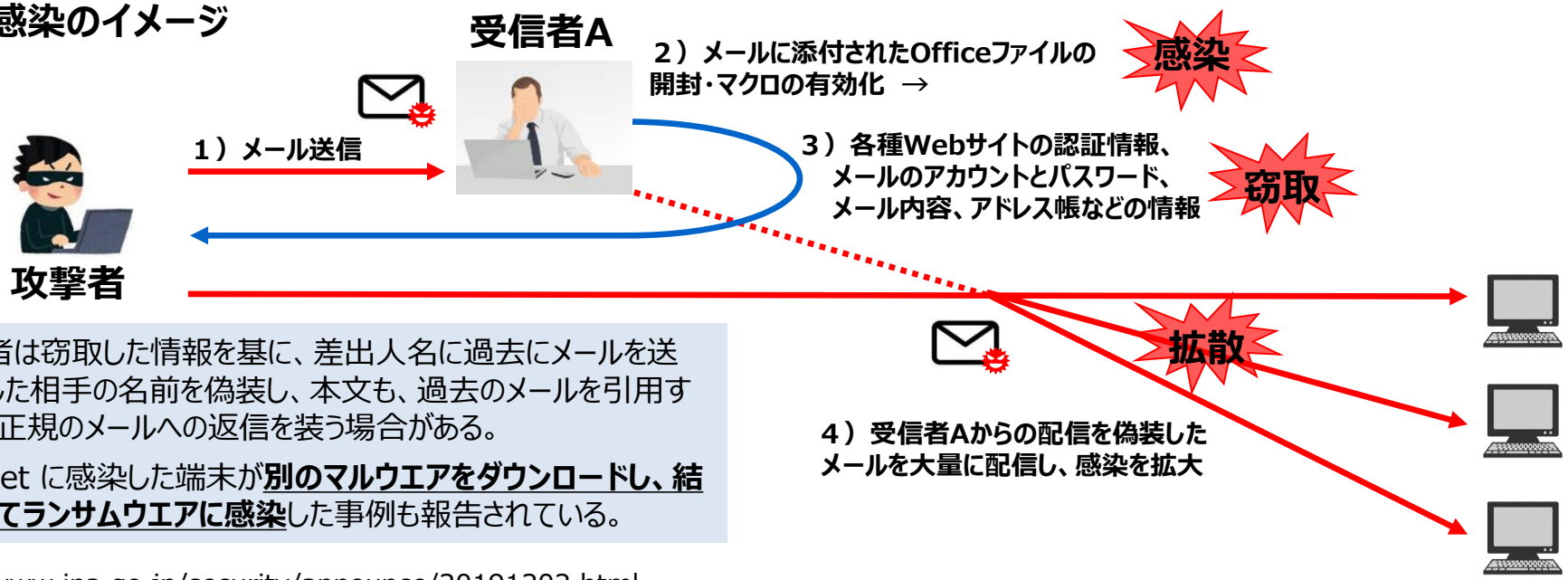
システム監視による不審な活動の検知	リモートアクセスの保護	IT/OTネットワークのセグメント化	対応計画の策定及び訓練等の実施	独立した安全制御システムの設置

[出典] CISA “CYBER RISKS RESOURCES FOR THE WATER AND WASTEWATER SYSTEMS SECTOR”等 を参考に作成

ウイルスへの感染を狙う攻撃メール：“Emotet”

- **Emotetは、メールを介して感染する、情報の窃取や他のマルウェアへの感染のため利用されるマルウェア**であり、国内でも2019年10月頃に複数企業で被害事例が相次いだ。
- **2021年11月に攻撃活動再開の兆候が確認**され、**改めて、IPAやJPCERT/CCが注意喚起**を行っている。
- 初期と異なる攻撃手法として、**Emotetが正規のメールから添付ファイルを窃取して Emotetへの感染を引き起こすOfficeファイルとともに送付する事例**や、メール配信経路のセキュリティ製品による検知からのすり抜けを狙って**パスワード付きZIPファイルが添付される事例**が確認されている。
- 2021年1月にテイクダウン（ サーバー等攻撃インフラの接収）が行われ、一時感染は落ち着いたものの、2021年11月後半より活動の再開が確認されており、**特に2022年2月の第一週よりEmotetの感染が急速に拡大**。

攻撃・感染のイメージ

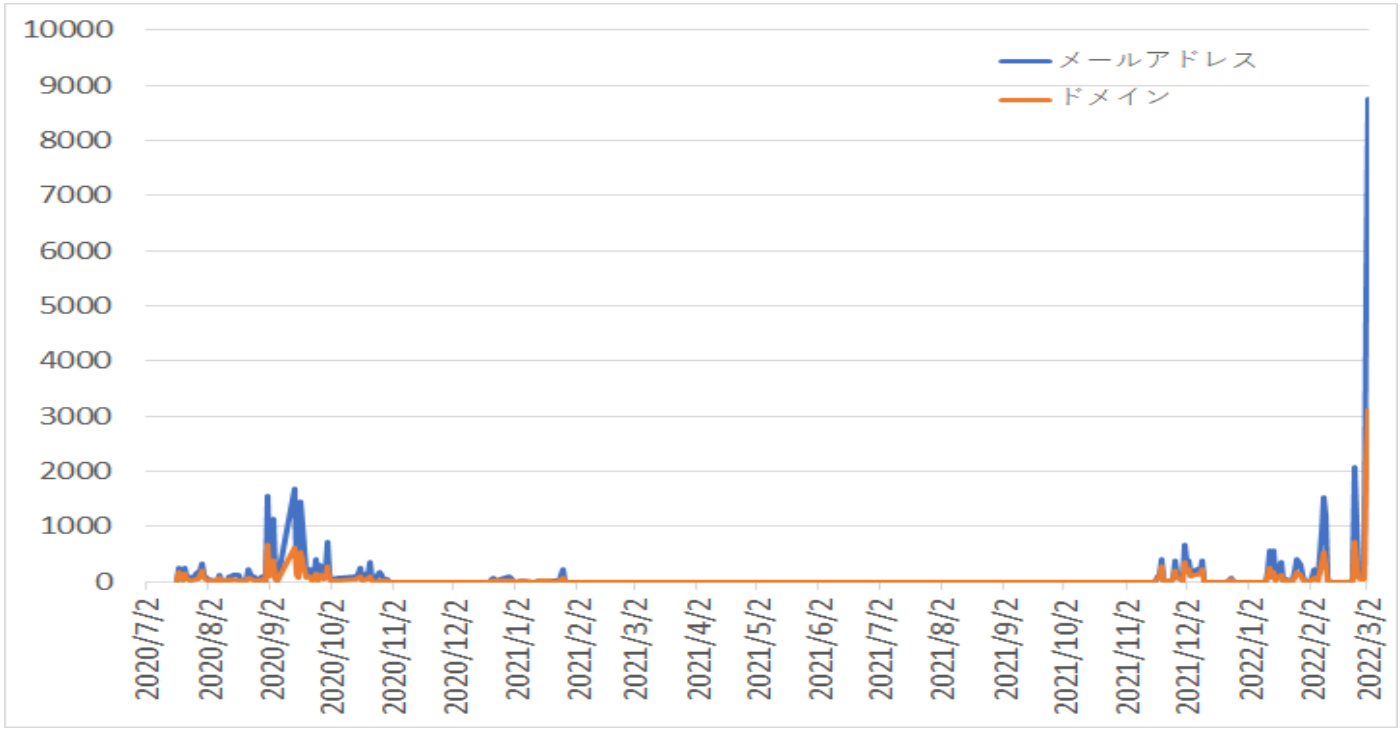


- ✓ 攻撃者は窃取した情報を基に、差出人名に過去にメールを送受信した相手の名前を偽装し、本文も、過去のメールを引用する等、正規のメールへの返信を装う場合がある。
- ✓ Emotet に感染した端末が**別のマルウエアをダウンロードし、結果としてランサムウエアに感染**した事例も報告されている。

https://www.ipa.go.jp/security/announce/20191202.html
https://www.jpcert.or.jp/at/2022/at220006.html

マルウェアEmotetの感染再拡大

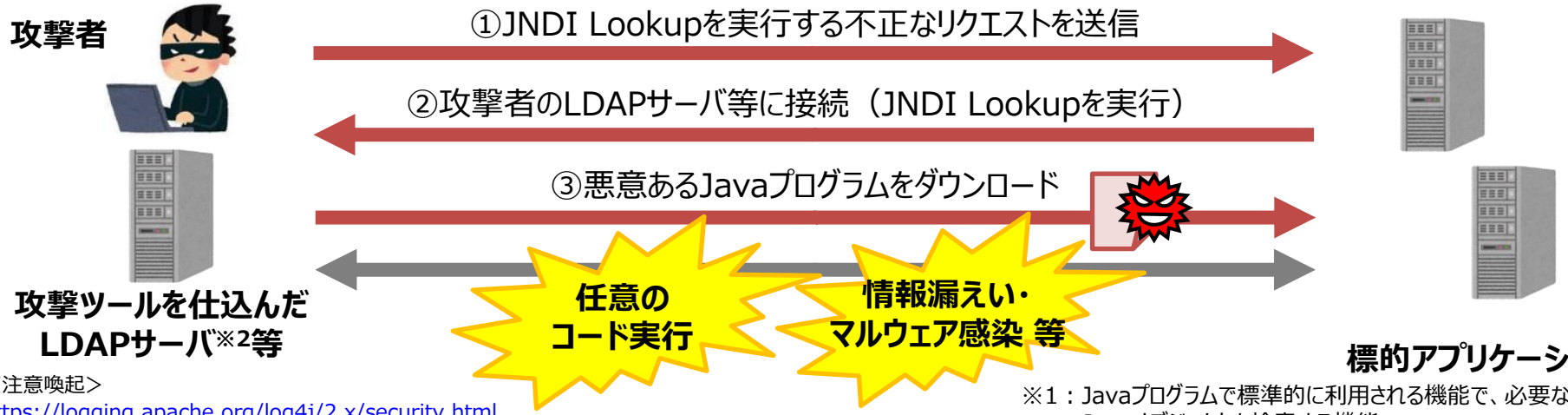
- 2021年11月後半より活動の再開が確認されているマルウェアEmotetの感染が2022年2月の第一週より急速に拡大。
- IPA（2021年11月～）及びJCERT/CC（2022年2月～）から注意喚起等を実施。
  - 正規メールへの返信を装うなどの手口を解説し、身に覚えのないメールの添付ファイルは開かないよう注意喚起
  - 感染が疑われる場合のチェックツール「EmoCheck」を公開



Apache Log4jの脆弱性：Log4Shell（CVE-2021-44228等）

- 2021年12月、Javaベースのオープンソースログ出力ライブラリ**Apache Log4jにおける任意コード実行の脆弱性が発表**された。当該脆弱性はLog4jのJNDI Lookup※1機能に起因するもので、Log4Shellとも呼ばれる。
- この脆弱性を利用することで、**Log4jが動作するアプリケーションに対して外部からの任意コード実行が可能**となり、情報漏えいやマルウェア感染等の被害に繋がる恐れがある。
- 脆弱性の公表をうけて、**NISCから重要インフラ事業者等へ注意喚起を発出。**多くのユーザーへの影響が考えられることから、**一般向けにも注意喚起**を公開。前後して、**専門機関（IPA、JPCERT/CC）からも、Log4jのバージョンアップや回避策を講じることで脆弱性に対処するよう注意喚起**がなされた。
- その後、この脆弱性の悪用を試みる通信が観測されているほか、Microsoft社より本脆弱性を利用したランサムウェアの存在が報告されるなどしている。

◆ **Log4Shell（CVE-2021-44228等）を利用した攻撃のイメージ**



<注意喚起>
https://logging.apache.org/log4j/2.x/security.html
https://www.nisc.go.jp/press/pdf/20211213NISC_press.pdf
https://www.ipa.go.jp/security/ciadr/vul/alert20211213.html
https://www.jpcert.or.jp/at/2021/at210050.html

※1：Javaプログラムで標準的に利用される機能で、必要なデータを含むJavaオブジェクトを検索する機能
※2：特定のキーに対応する情報を返すディレクトリサーバ

「昨今の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）」

●昨今の情勢を踏まえると**サイバー攻撃事案の潜在的なリスクは高まっている。**
●**経営者のリーダーシップ**の下、サイバー攻撃の脅威に対する認識を深め、対策の強化を。
●**不審な動きを把握した場合**は、早期対処のために速やかに経済産業省やセキュリティ関係機関（IPA、JPCERTなど）に連絡、警察にも相談を。

１．リスク低減のための措置

〇本人認証の強化
（パスワードが単純でないか、アクセス権限の確認、多要素認証の利用、不要なアカウントの削除等）
〇IoT機器を含む情報資産の保有状況の把握
特にVPN 装置等へのセキュリティパッチ（最新のファームウェアや更新プログラム等）の迅速な適用
〇組織内での基本の徹底
（添付ファイルを不用意に開かない、URL を不用意にクリックしない、連絡・相談を迅速に行うこと等）

２．インシデントの早期検知

〇サーバ等における各種ログの確認
〇通信の監視・分析やアクセスコントロールの再点検

３．インシデント発生時の適切な対処・回復

〇データ消失等に備えて、データのバックアップの実施及び復旧手順の確認
〇インシデント発生時の対応確認
（インシデントを認知した際の対処手順、対外応答や社内連絡体制等）
➢ 侵入型ランサムウェア攻撃を受けたら読むFAQ　https://www.jpcert.or.jp/magazine/security/ransom-faq.html

経済産業省「昨今の情勢を踏まえたサイバーセキュリティ対策の強化について （2022年2月23日）」 https://www.meti.go.jp/press/2021/02/20220221003/20220221003.html
経済産業省等７省庁「サイバーセキュリティ対策の強化について（2022年3月1日）」 https://www.meti.go.jp/press/2021/03/20220301007/20220301007.html