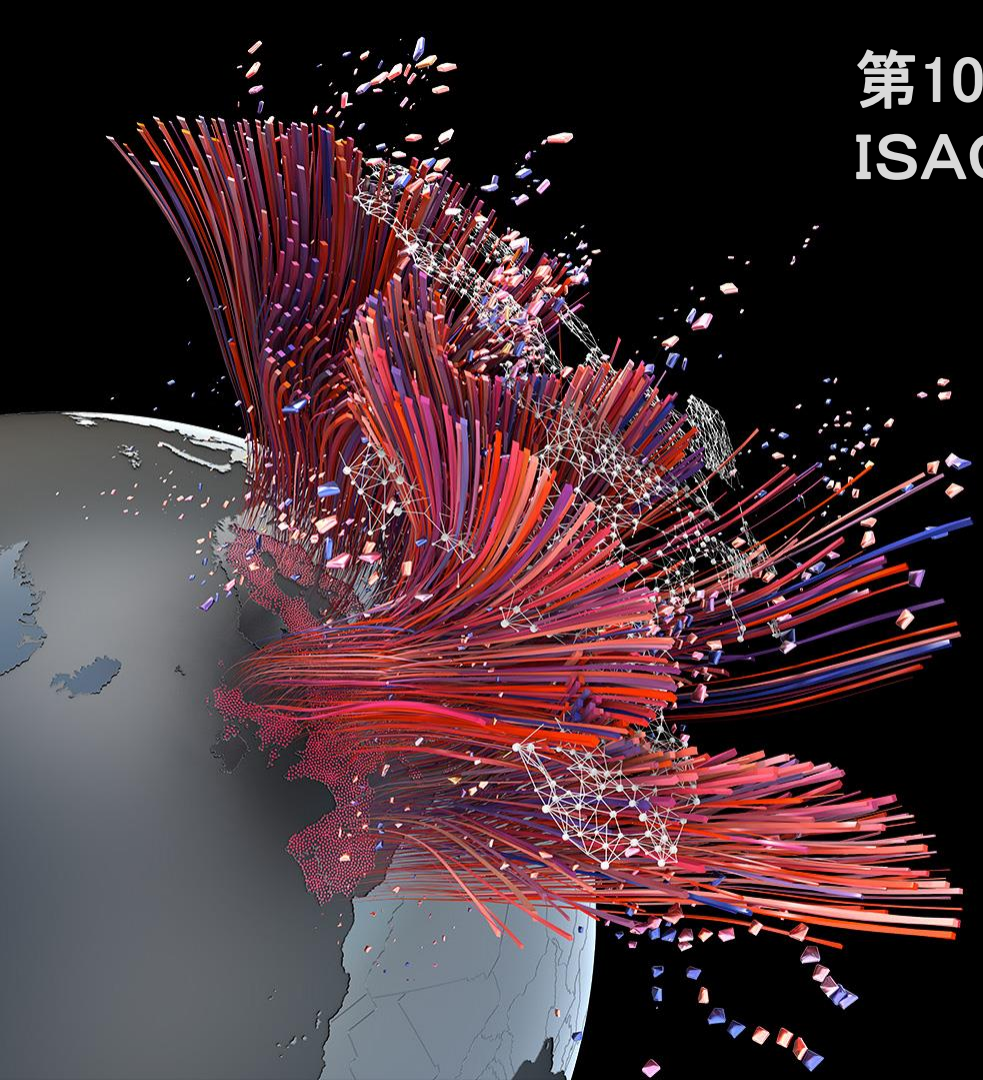


第10回 情報セキュリティマネージャー
ISACA カンファレンス in Tokyo

昨今のサイバー攻撃手法と
インシデント対応事例の紹介

トレンドマイクロ株式会社
インシデントレスポンスチーム
日本Region Leader 田中 啓介

TREND MICRO

Agenda

- インシデントレスポンス概要
- 攻撃手法について
  - 標的型攻撃
  - ランサムウェア
- 当社におけるIR対応業務
- 対応実例のご紹介

自己紹介

田中 啓介
アプライドサイバーセキュリティラボ部
インシデントレスポンスチーム　日本Region Leader
情報処理安全確保支援士,SANS GIAC GCFA,GDAT

期間	所属/業務	役割	備考
2007年-	個人製品サポート	エンジニア	・ウイルスバスター担当(技術/更新)
2009年-	法人製品サポート	エンジニア	・グループウェア製品担当
2012年-	インシデントレスポンス	エンジニア	・中央省庁CSIRTのリード(常駐) ・ログ監視、端末調査、対策立案 （1000件以上未知のマルウェア発見）
2017年-		マネージャ	
2019年-	法人 製品提案SE	コンサルタント	・インシデントレスポンス業務を兼務
2021年-	インシデントレスポンス		・国内のインシデント対応サービスをリード

自己紹介 - 研究活動

- 2020年：2件の論文投稿、研究会発表
  1. セキュリティインシデント実例を元にした各種ガイドラインの対策評価と，効果的なセキュリティ対策の提言(2020/7)
  2. MITRE ATT&CKを用いたセキュリティインシデント実例の分析と,コストを考慮したセキュリティ対策の提言(2020/10)
- 2021年：9月より立命館大学 後期博士課程 入学 (上原研究室)
  - 2022年3月7,8日：IOT研究会にて発表予定
    - 「中小企業における情報セキュリティ対策状況のインタビュー調査」

セキュリティインシデント実例を元にした
各種ガイドラインの対策評価と，効果的なセキュリティ対策の提言

田中啓介[*1]　東結香[*1]　上原哲太郎[*2]

Evaluate security countermeasure from security incident and security guidelines

KEISUKE TANAKA[*1]　YUKA HIGASHI[*1]　TETSUTARO UEHARA[*2]

1. はじめに

MITRE ATT&CK®を用いたセキュリティインシデント実例の分析と,コストを考慮したセキュリティ対策の提言

田中啓介[*1]　東結香[*1]　上原哲太郎[*2]

Proposal for cost effective security countermeasure from recent security incident and MITRE ATT&CK®

KEISUKE TANAKA[*1]　YUKA HIGASHI[*1]　TETSUTARO UEHARA[*2]

1. はじめに

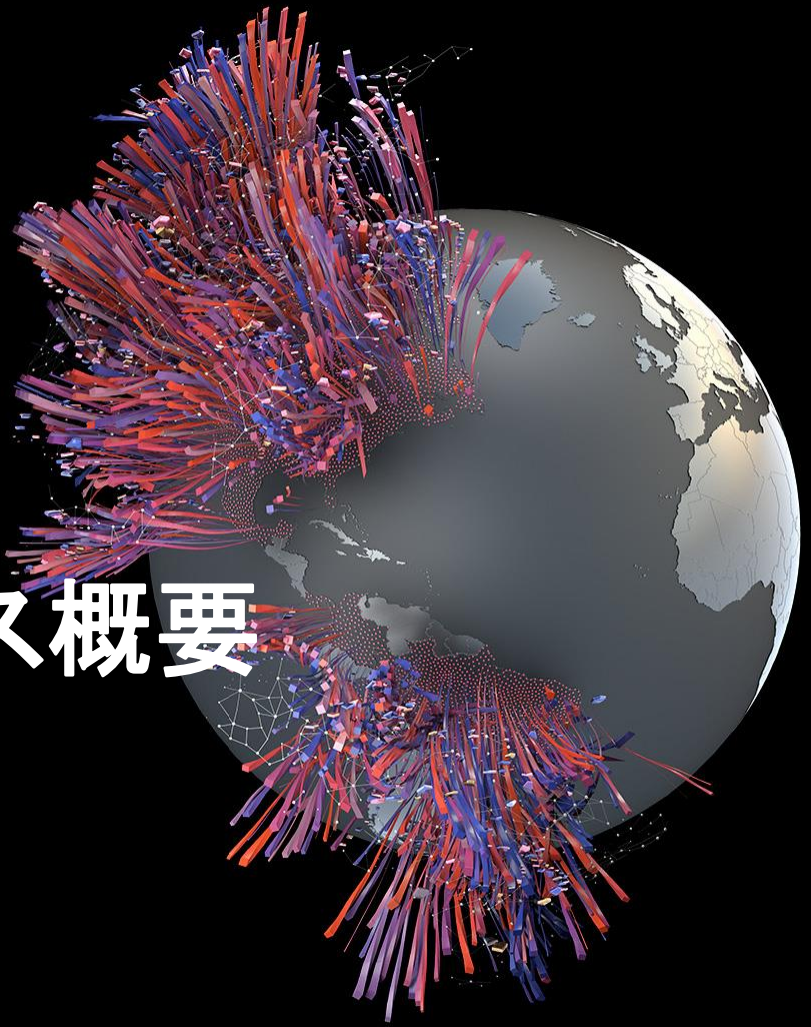
1.インシデント情報をMITRE ATT&CKで整理

- 各事案で利用されたTechniquesの整理
- 各Techniquesが全事案で何回利用されたかの可視化

Tactics > Techniques	Case A	B	C	D	E	F	G	H	I	J	K	L	M	総計
Initial Access	1	1	1	1	1	1	1	1	1	1	1	1	1	13
T1133.External Remote Services		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	11
T1190.Exploit Public-Facing Application				✓										1
T1566.Spearphishing Attachment	✓													1
Credential Access	2	2	3		2	1	1		1	1				13
T1003.05 Credential Dumping	✓	✓	✓		✓									4
T1110.Brute Force	✓	✓	✓		✓					✓				5
T1212.Exploitation for Credential Access			✓			✓	✓		✓					4
Discovery	1	2	2		2	1	1		1		1	1	1	13
T1046.Network Service Scanning		✓	✓		✓	✓	✓		✓		✓	✓	✓	9
T1135.Network Share Discovery	✓	✓	✓		✓									4
Lateral Movement	1	1	3			3	3		2		1	1	1	16
T1021.Remote Services	✓	✓	✓			✓	✓		✓					6
T1072.Software Deployment Tools											✓	✓	✓	3
T1210.Exploitation of Remote Services				✓			✓	✓						3
T1570.Lateral Tool Transfer			✓			✓	✓		✓					4
Impact	1	1	1	1	1	1	1	1	1	1	1	1	1	13
T1486.Data Encrypted for Impact	✓	✓		✓	✓	✓		✓	✓		✓	✓	✓	10
T1529.System Shutdown/Reboot			✓			✓			✓					3

1)https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=206131&item_no=1&page_id=13&block_id=8
2)https://ipsj.ixsq.nii.ac.jp/ej/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=208491&item_no=1&page_id=13&block_id=8

インシデントレスポンス概要



TREND MICRO

インシデントレスポンスとは

インシデント

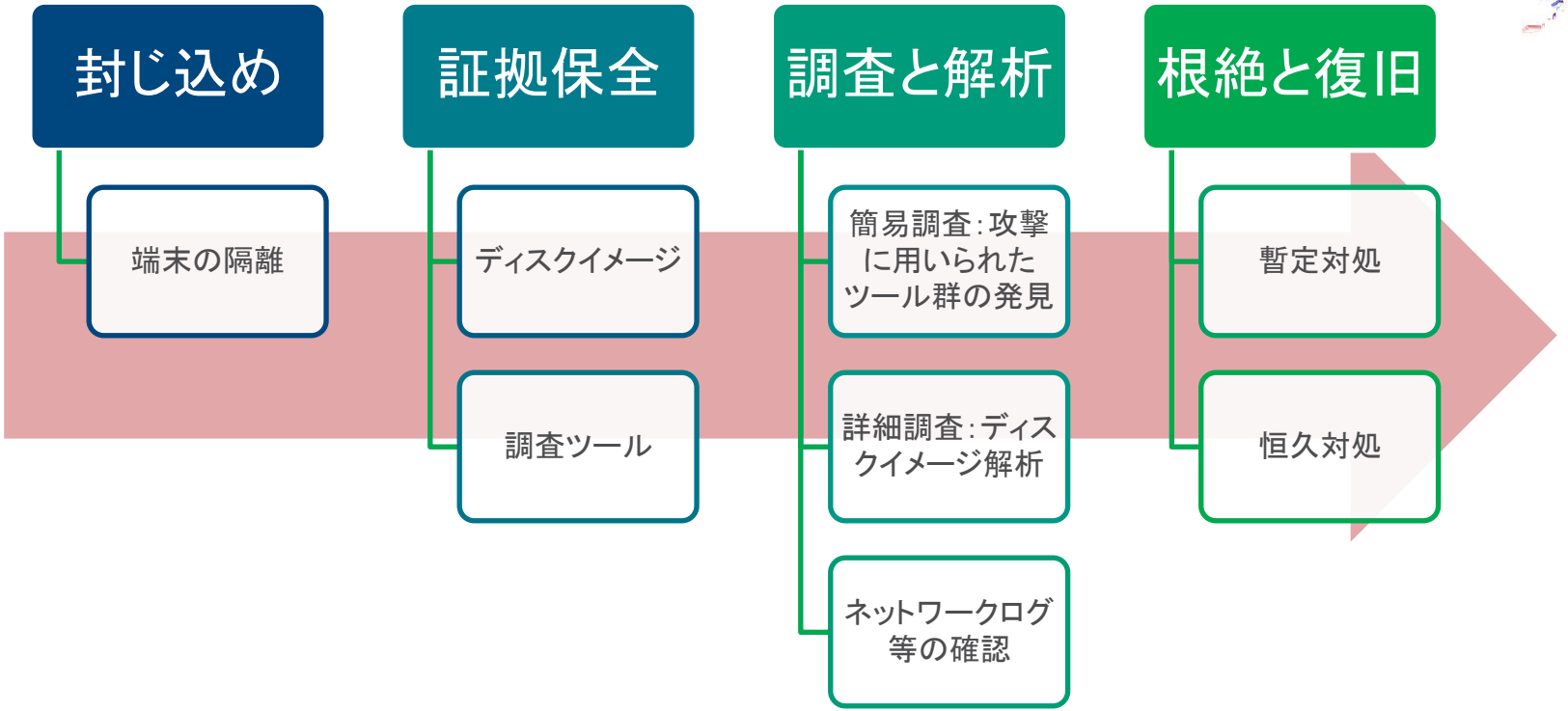
- 情報システムの運用におけるセキュリティ上の問題として捉えられる事象
- 例：情報流出,フィッシングサイト,不正侵入,マルウエア感染 Webサイト改ざん、DoS攻撃等

インシデントレスポンス

- インシデント発生後の被害を最小化するための「事後」対応

出典：JPCERT/CC インシデントとは
https://www.jpcert.or.jp/aboutincident.html

対応の流れ



サイバー攻撃の分類

手法	目的	対象	攻撃者
マルウェア	金銭	個人	犯罪者
標的型マルウェア	情報	企業	犯罪組織
ランサムウェア	業務妨害	公共団体	国家機関
DDoS攻撃	主張	官公庁	国家の支援を受けた組織
Web改ざん			

サイバー攻撃の分類(標的型)

手法	目的	対象	攻撃者
マルウェア	金銭	個人	犯罪者
標的型マルウェア	情報	企業	犯罪組織
ランサムウェア	業務妨害	公共団体	国家機関
DDoS攻撃	主張	官公庁	国家の支援を受けた組織
Web改ざん			

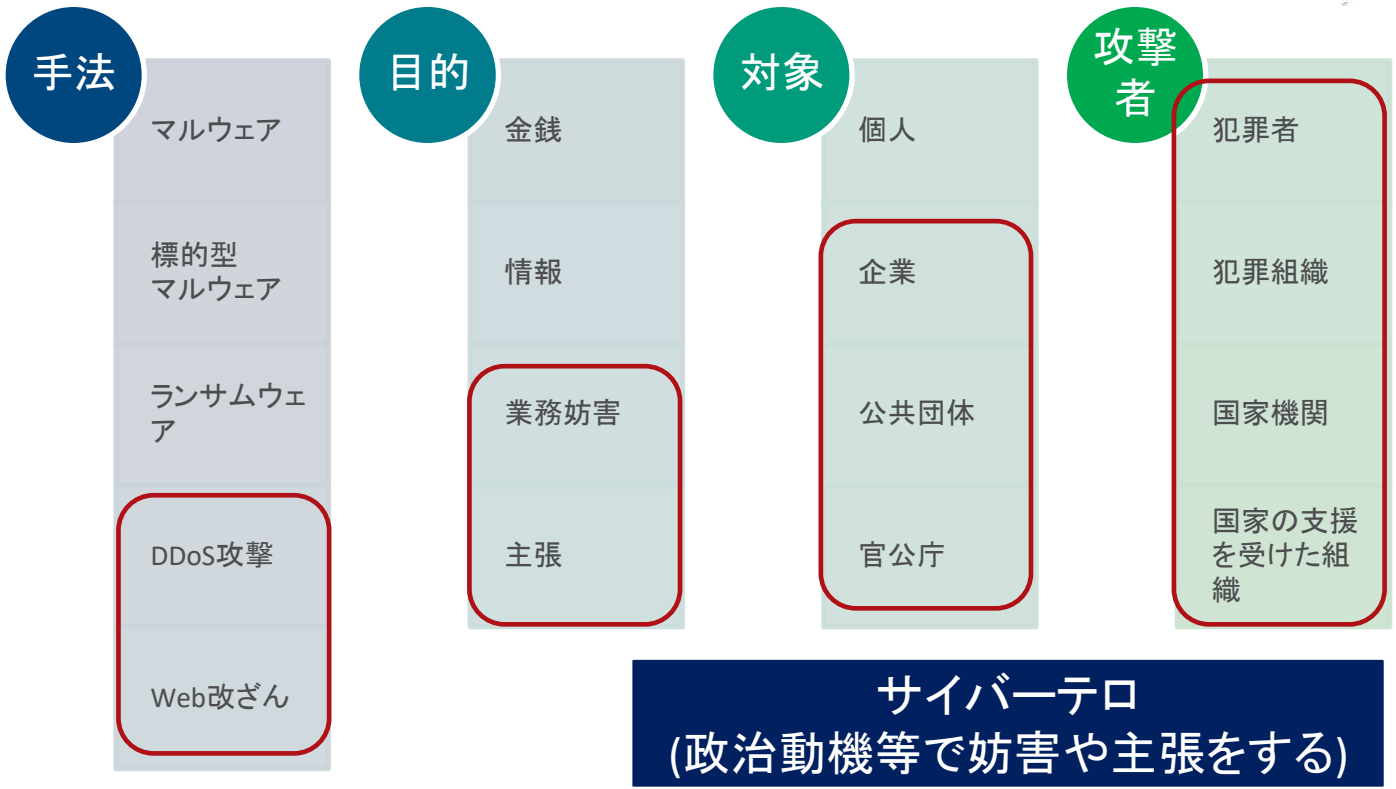
標的型攻撃
(そこにしかない情報を得る)

サイバー攻撃の分類(金銭目的)

手法	目的	対象	攻撃者
マルウェア	金銭	個人	犯罪者
標的型マルウェア	情報	企業	犯罪組織
ランサムウェア	業務妨害	公共団体	国家機関
DDoS攻撃	主張	官公庁	国家の支援を受けた組織
Web改ざん			

金銭を目的とした攻撃
(効率的に多額の金銭を得る)

サイバー攻撃の分類（サイバーテロ）



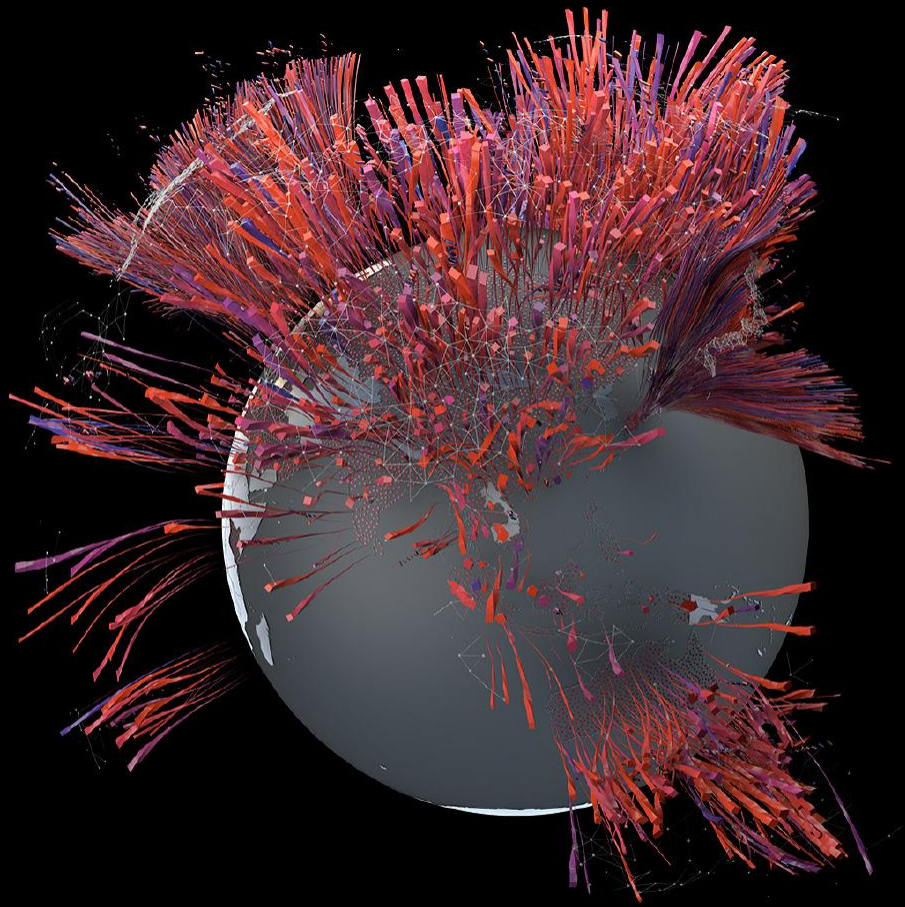
サイバーテロ
(政治動機等で妨害や主張をする)

サイバー攻撃の分類（本日話す内容）

手法	目的	対象	攻撃者
マルウェア	金銭	個人	犯罪者
標的型マルウェア	情報	企業	犯罪組織
ランサムウェア	業務妨害	公共団体	国家機関
DDoS攻撃	主張	官公庁	国家の支援を受けた組織
Web改ざん			

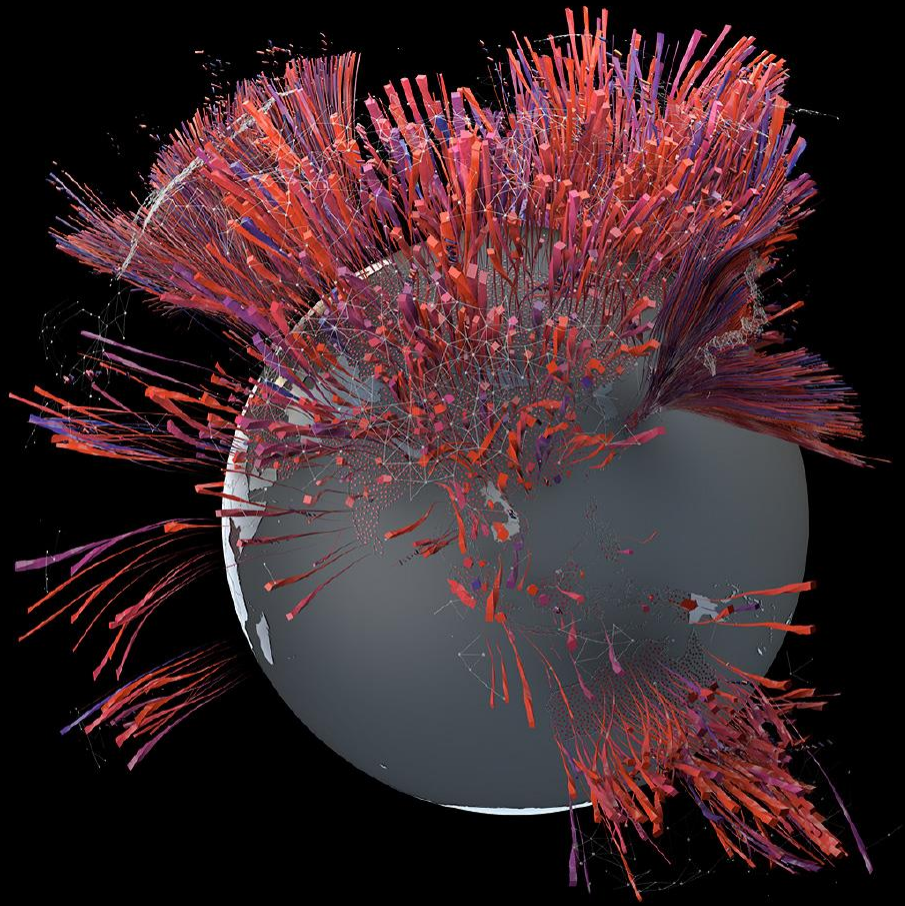
法人向けランサムウェア攻撃の手法や対策をお話しします！

攻撃手法について



TREND MICRO

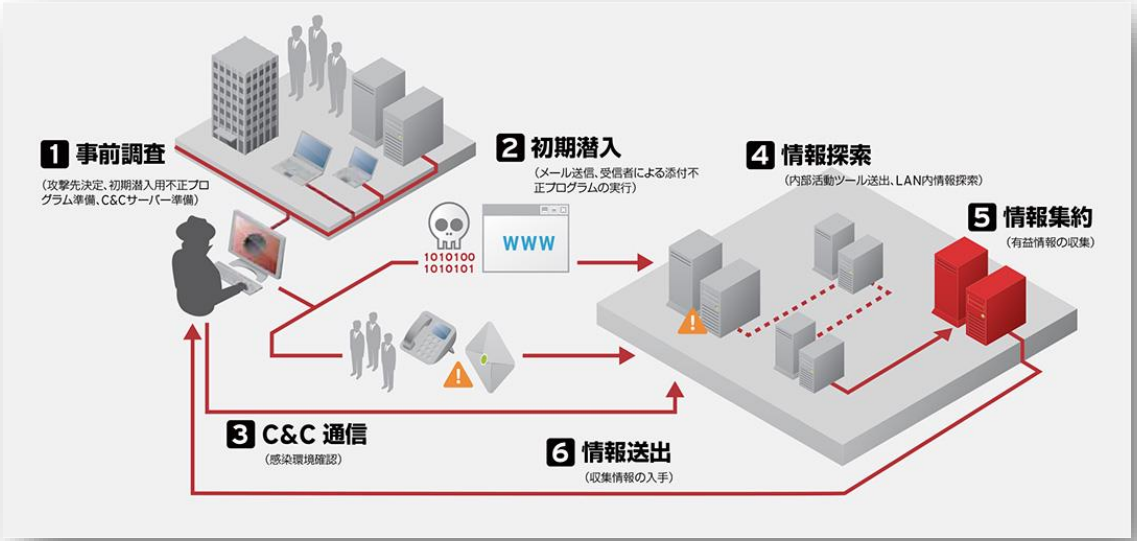
標的型攻撃



TREND MICRO

一般的な攻撃のステップ

攻撃の準備から目的達成までの流れをトレンドマイクロでは6段階に分類



参考:トレンドマイクロ,「標的型サイバー攻撃」, https://www.trendmicro.com/ja_jp/security-intelligence/research-reports/threat-solution/apt.html

※ 一般的にはLockheed Martin社の「Cyber Kill Chain」モデルで説明されることがあります
参考:Lockheed Martin,「Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains」, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

1段階目:事前準備

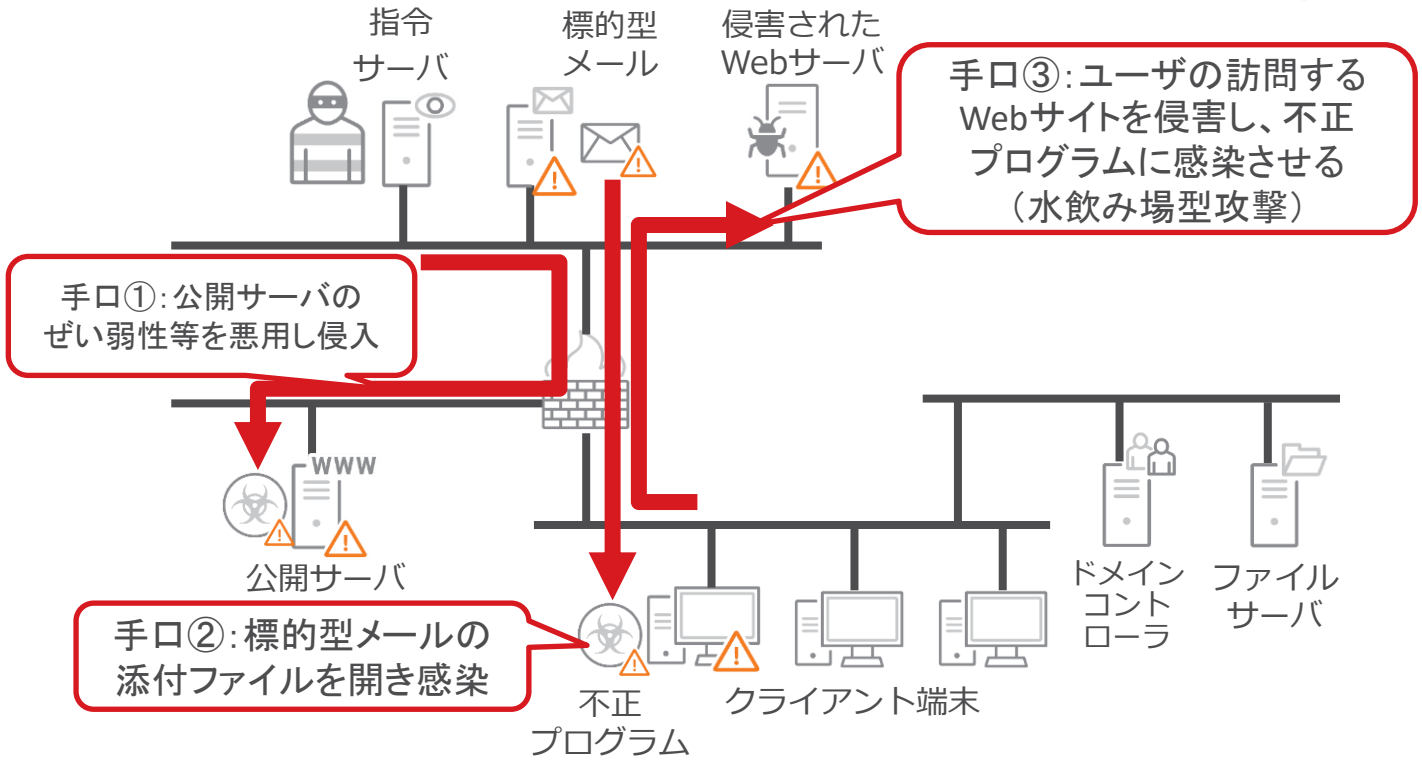
標的の
情報収集


不正プログラムの準備


攻撃先の
環境情報調査

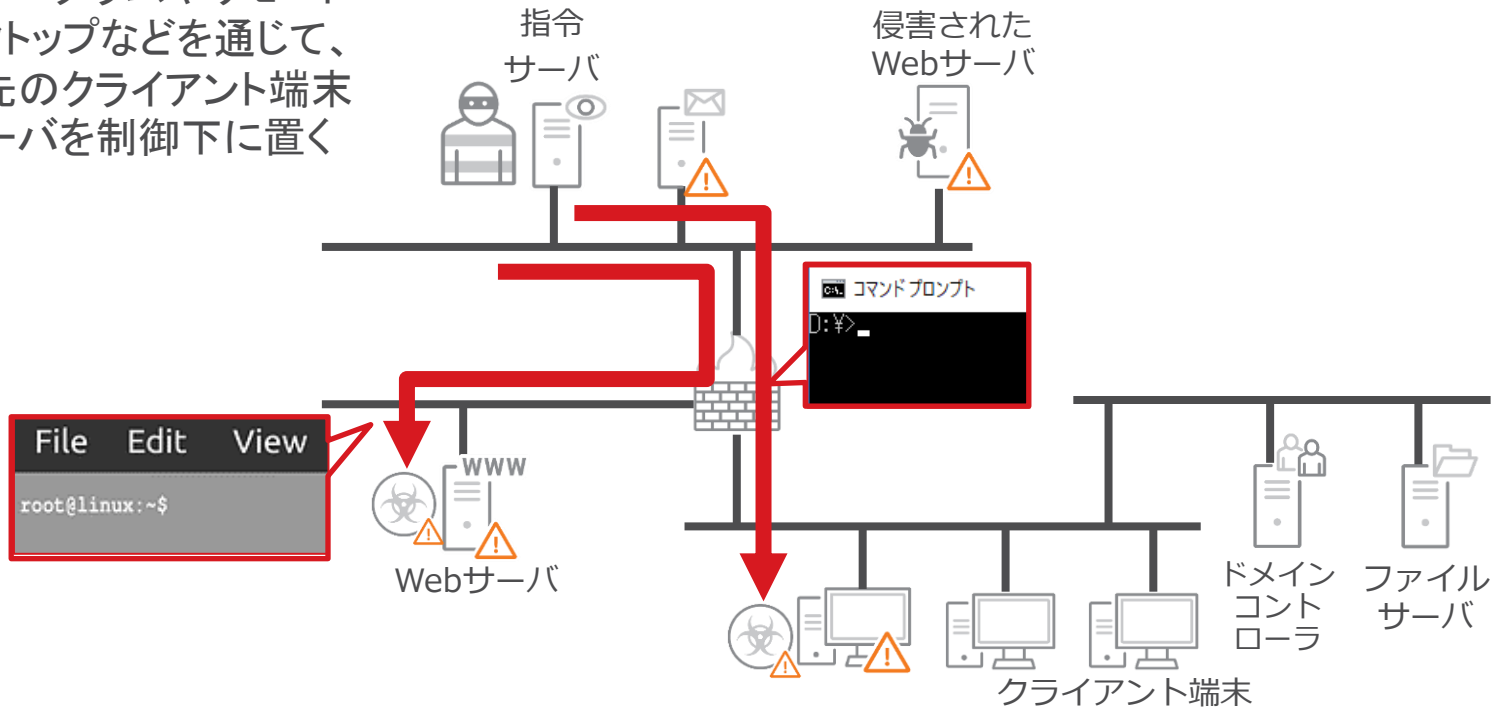
指令サーバの
構築

2段階目：初期侵入



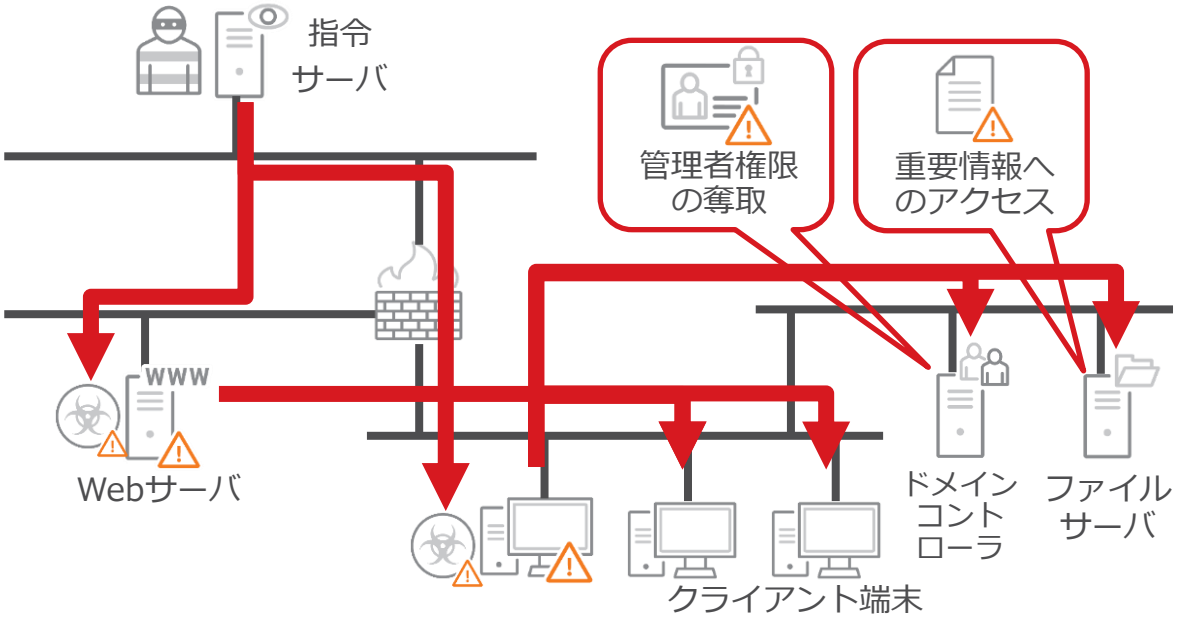
3段階目：端末制御

不正プログラムやリモートデスクトップなどを通じて、侵入先のクライアント端末やサーバを制御下に置く



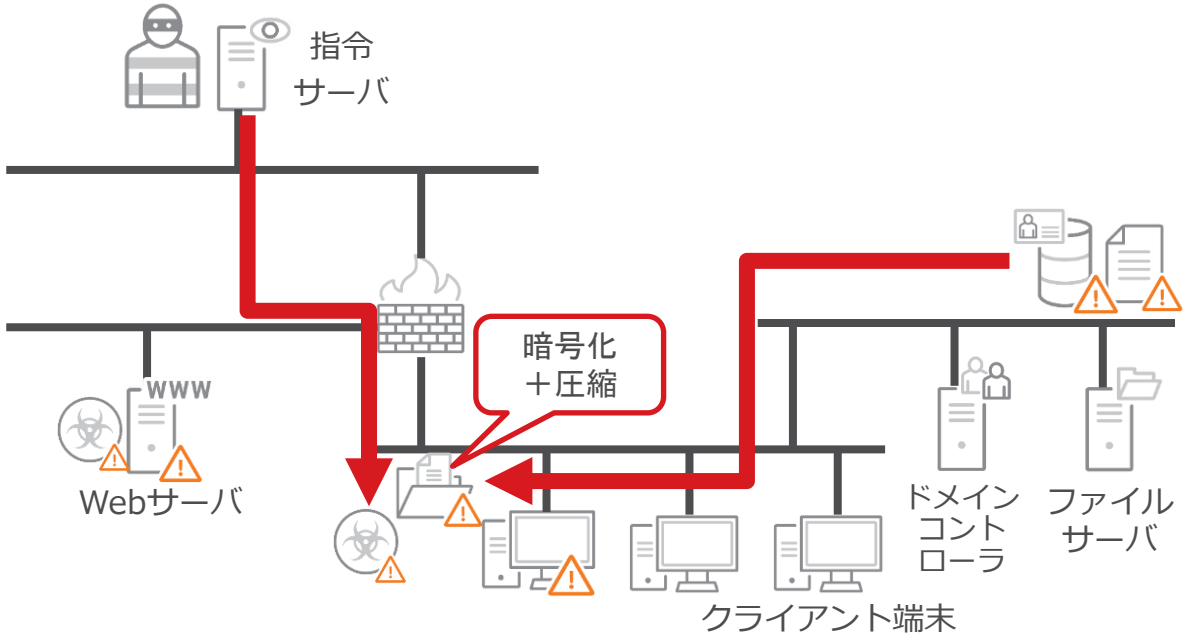
4段階目：情報探索

組織内のサーバ資産や権限などを探索・可視化する



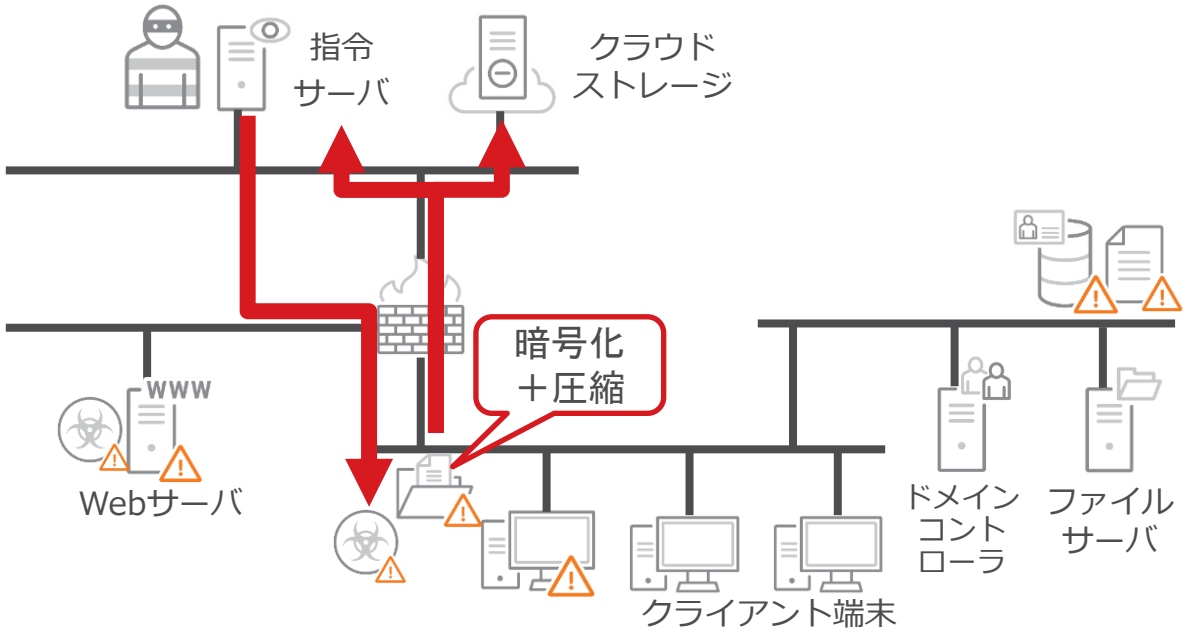
5段階目：情報集約

重要情報を踏み台端末に収集し、暗号化＋圧縮する

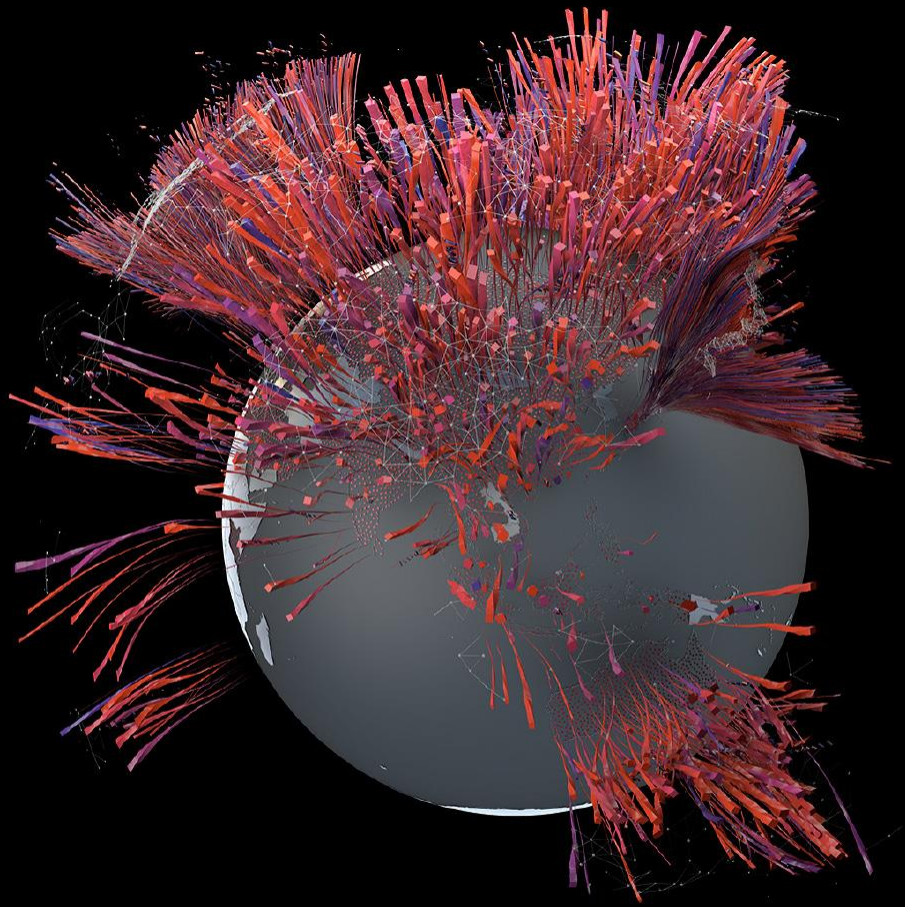


6段階目：データ送出

暗号化＋圧縮したデータをマルウェア×C&C間の通信で直接取得したり、外部サーバにアップロード等して持ち出す



ランサムウェア



TREND MICRO

ランサムウェアの分類

従来型

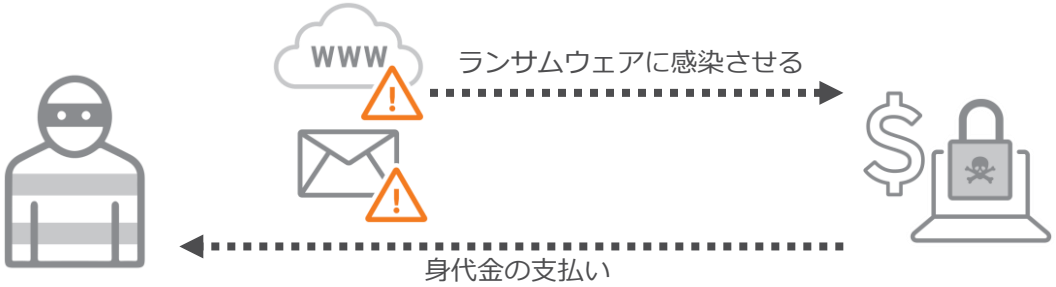
- Worm等で自動拡散
- データ暗号化にて脅迫

二重脅迫型

- 人手による侵入と拡散
- データ暗号化＋情報取得とリークによる脅迫

【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について
https://www.ipa.go.jp/files/000084974.pdf (IPA, 2020年8月20日)

従来型ランサムウェア

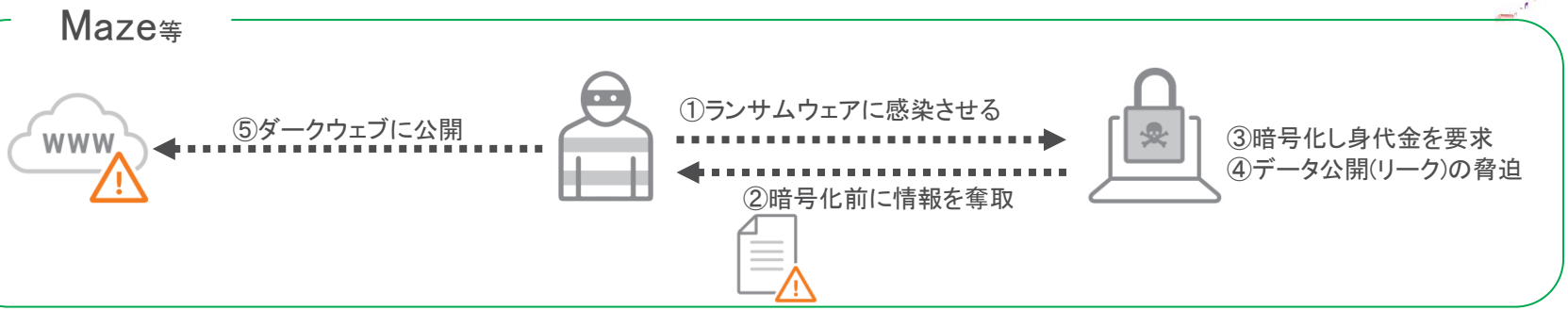


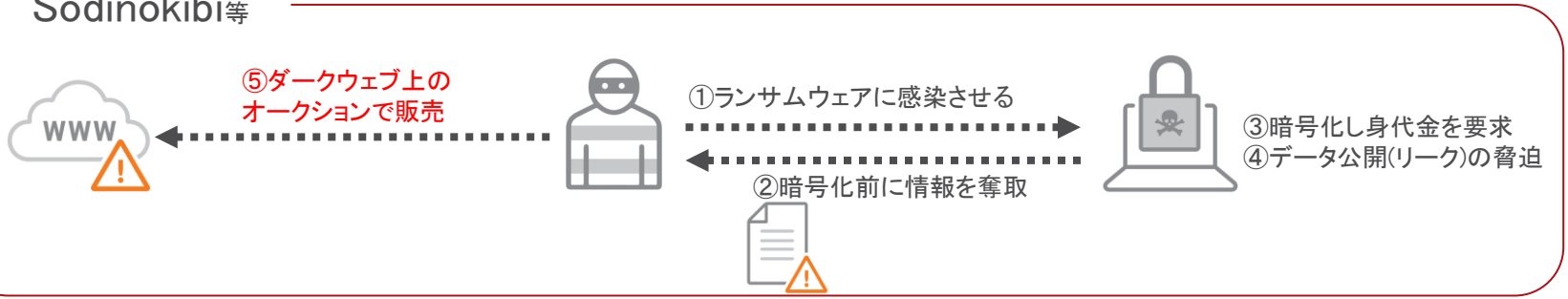
手法

1.改竄したWebサイトやばらまき型のメールにランサムウェアを添付し感染させる
2.ドライブ上に保存されているファイルを暗号化
3.データ復号化のために身代金を請求

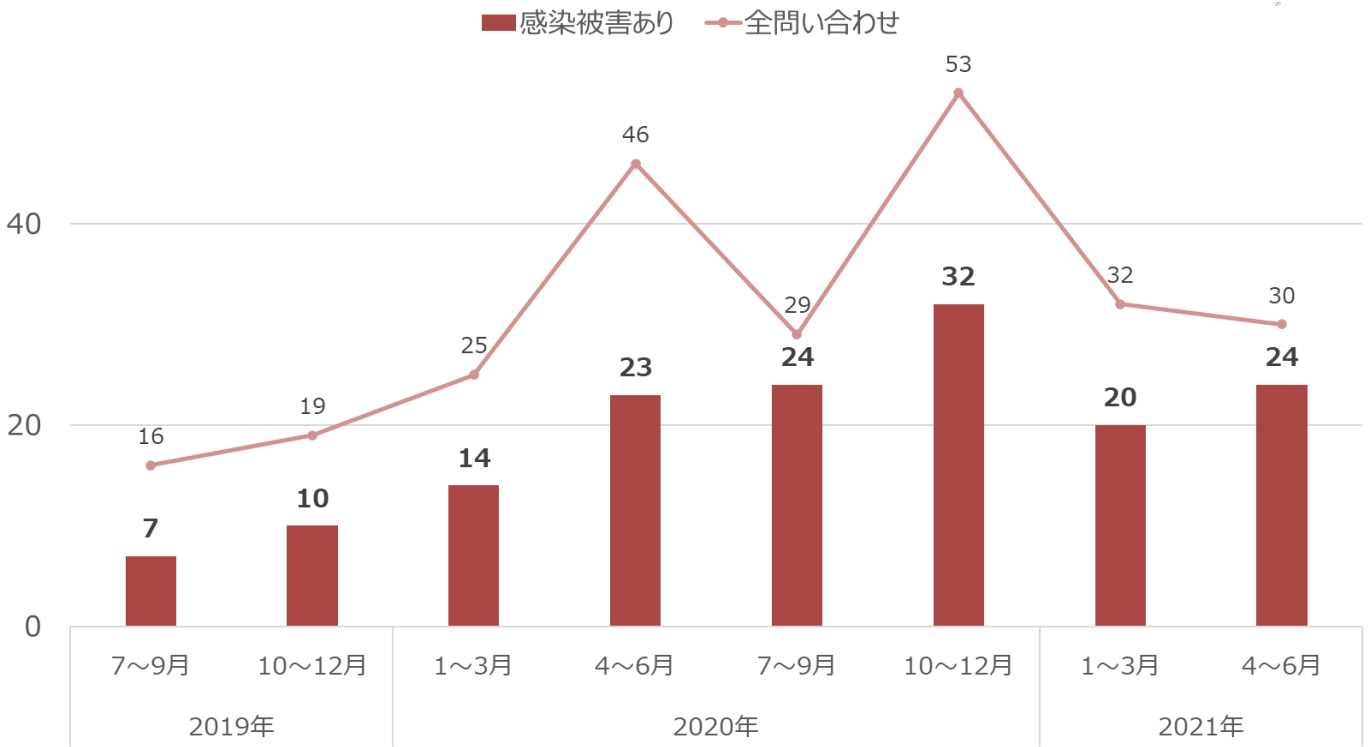
暗号化したファイルの復号のみの要求

二重強迫型ランサムウェア





国内におけるランサムウェア状況



図：国内利用者からのランサムウェア関連問い合わせおよびそのうちの被害報告の件数推移

二重脅迫型ランサムウェア　特徴 (1/3)

1.特定の法人を標的とした攻撃

- 身代金支払い能力がある組織のみを標的にする攻撃団体も存在
  - 逆に「コロナ禍なので医療業界は狙わない」と言っている組織も…

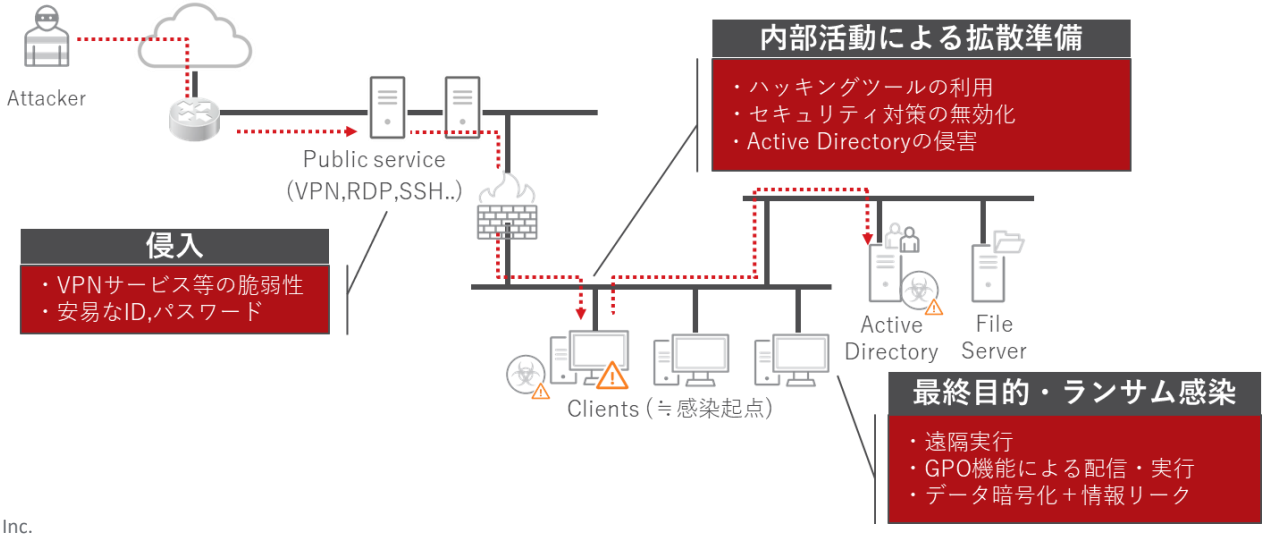
2.情報暴露（リーク）による脅迫

- 以前までは被害者の端末上のデータを暗号化して人質としていたが、昨今は「期日までに支払いを行なわない場合、データを全世界に公開する」という脅迫方法にシフト

二重脅迫型ランサムウェア　特徴 (2/3)

1）特定の法人を標的とした攻撃

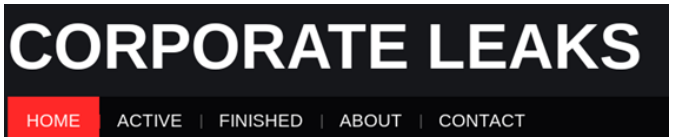
- 従来のメール経由、Web経由による侵入に加え、
  脆弱性攻撃や不正アクセスによる**遠隔からの直接侵入**が顕著化
- 侵入後、**内部活動**により攻撃基盤を拡大した後、ランサムウェア感染
- 遠隔実行による感染に加え、**グループポリシー**による配信・実行



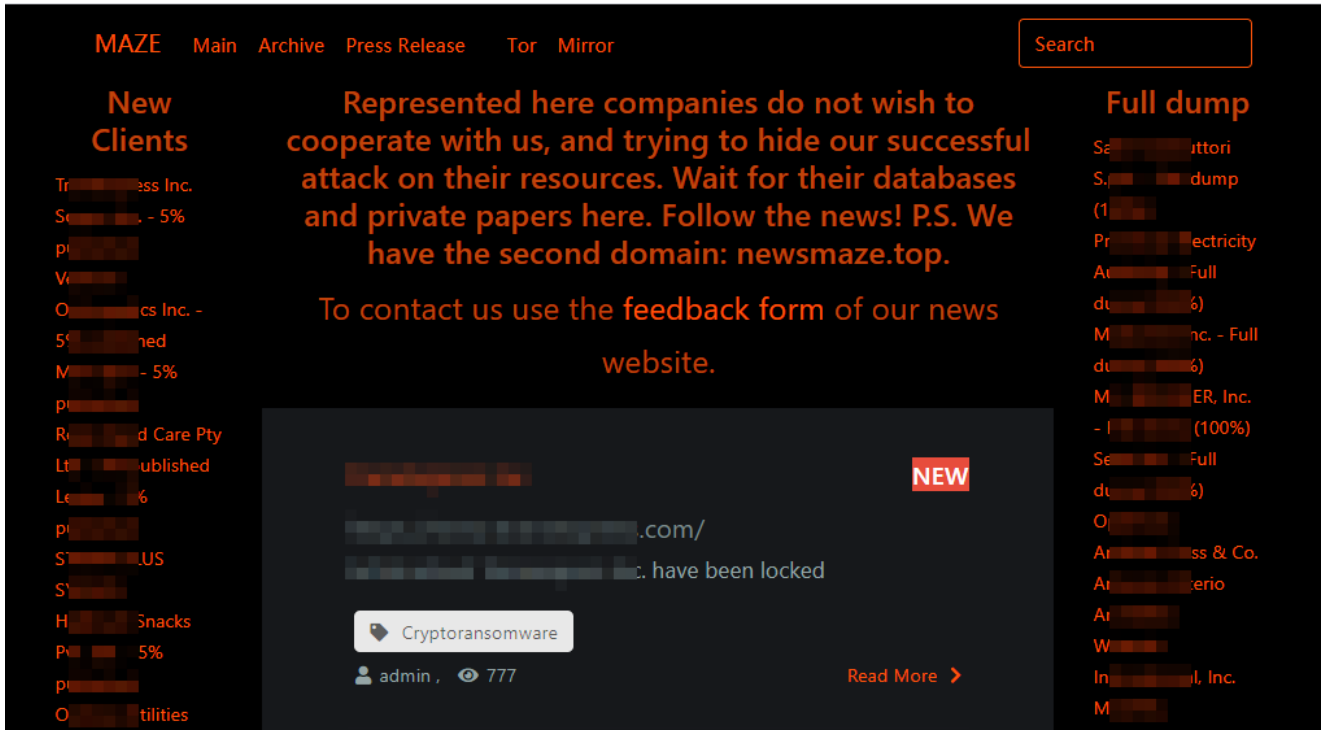
二重脅迫型ランサムウェア　特徴 (3/3)

2）情報暴露による脅迫

- データの暗号化前に**情報を窃取**、身代金を払わない場合には窃取した情報を**暴露**すると脅す
  - 「MAZE」、「SODINOKIBI/REvil」、「NEMTY/Nifilim」、「DOPPELPAYMER」など



参考:リークサイト



参考:リークサイト

Home Mirror Tor search...

URL

https://[redacted].com/

Details

WHITE paper? More to come here, LOT of we still have.

Example files:

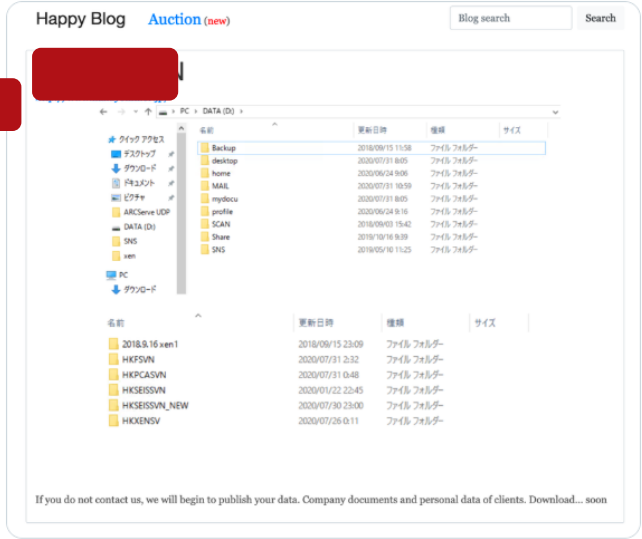
SharedFolders.7z.001 (102400Kb)
SharedFolders.7z.002 (102400Kb)

[redacted]

#Sodinokibi/#REvil claime[redacted]as a victim.

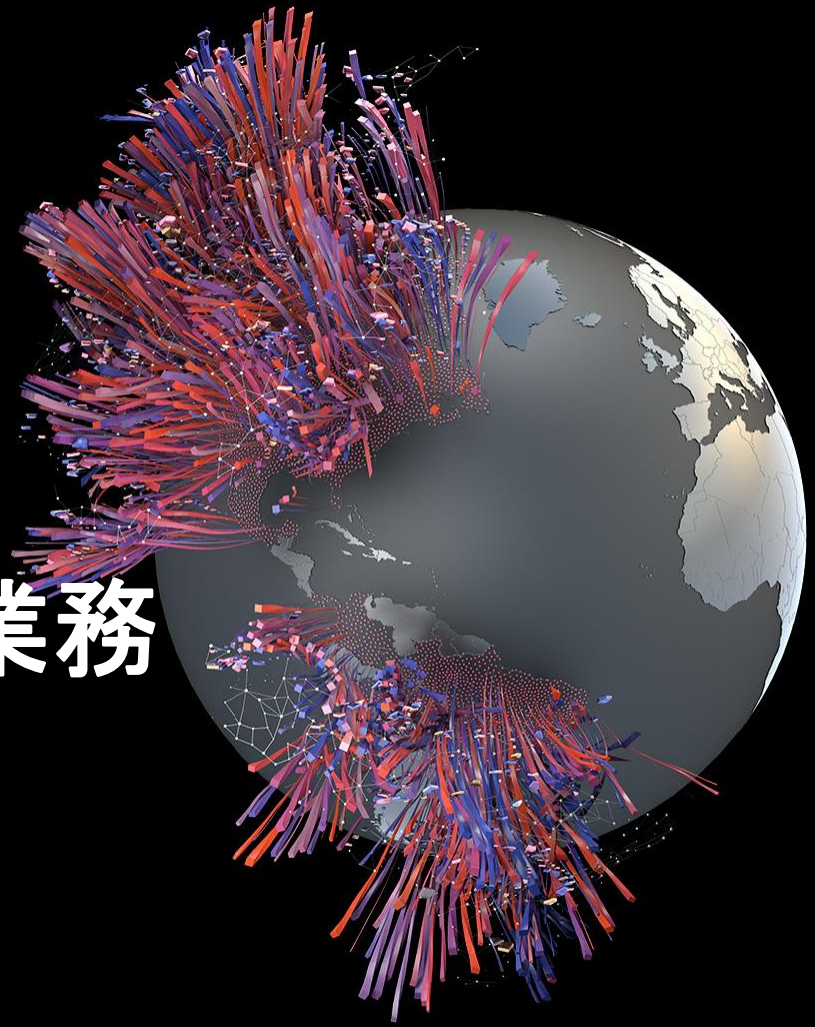
A translation, "[redacted] Association provides verification and inspection services for ship products and contributes to maritime safety and environmental conservation."

ツイートを翻訳



午前3:09 · 2020年8月4日 · Twitter Web App

当社におけるIR対応業務



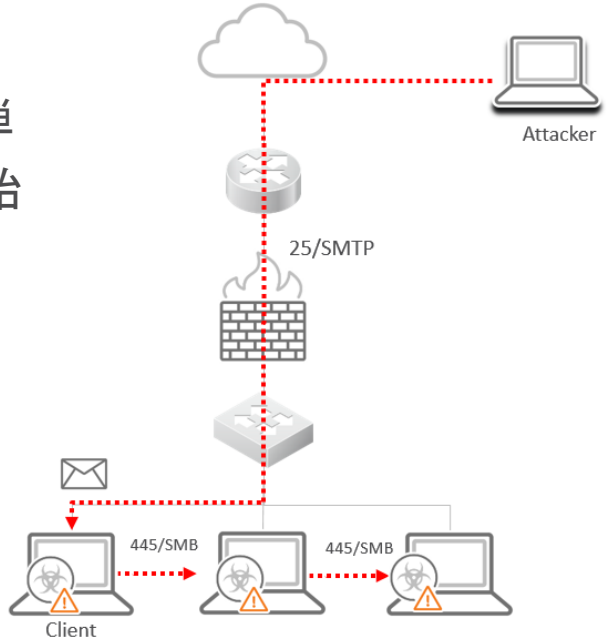
TREND MICRO

インシデント対応サービス概要

名称	**T**rendmicro **C**yber **A**ttack **R**esponse **S**ervice (**TCARS**)
期間	5営業日対応　→　10営業日以内に最終報告
サービス内容	**状況確認支援** ヒアリング、各種ログの確認等によりインシデントのスコープを確認。 スコープに基づいてインシデントレスポンスでの調査事項やゴールについて合意形成を行う
	インシデント復旧支援 インシデント発生前の状態までの回復を支援。弊社ソリューションを用いたマルウェアの駆除、各レイヤでの検出対応、再発有無確認のための監視を実施。
	インシデント調査支援 各種機器(弊社製品以外も含む)のログの解析や、記憶媒体から証跡を抽出しての解析を行い、インシデントの原因等に関する詳細調査を実施
	アフターフォロー 最終報告書の作成および報告会の実施。報告には技術施策、マネジメントに関する助言、製品提案なども含む

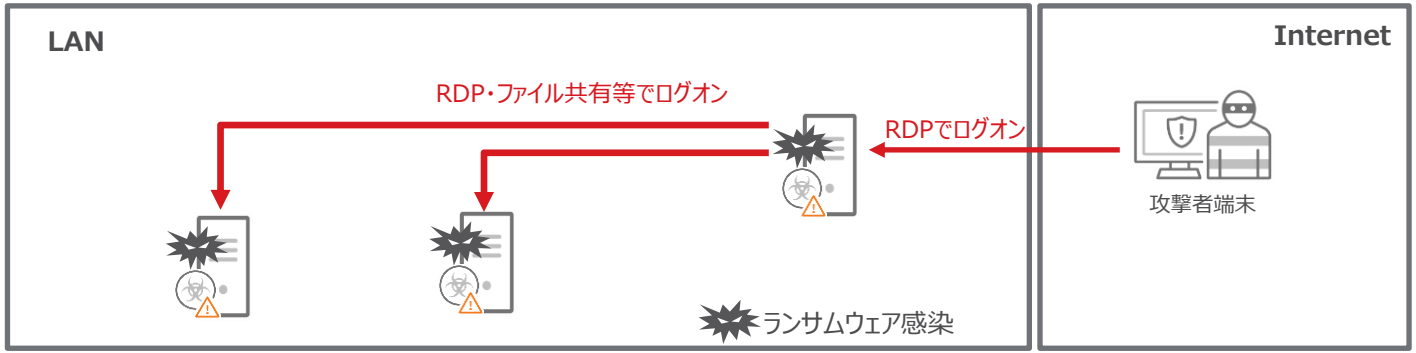
よくある被害事例 (1/2)

- メールで侵入＋内部拡散
  - 不審な添付ファイル付きのメールが着弾
  - ユーザが添付ファイルを開いて感染開始
  - LAN内で横展開、不正通信、別の
    不正プログラムを追加ダウンロード…etc



よくある被害事例 (2/2)

- 外部から直接侵入＋内部拡散
  - 外部（あるいは内部の踏み台）からRDPで侵入
  - 認証情報の窃取
  - LAN内でRDP経由、ファイル共有等で横展開
  - ランサムウェアの感染



主な依頼内容

LAN内の不正通信やウイルス検知を起点とした対応

- ランサムウェア,標的型検体などの挙動調査
- 攻撃手法、感染原因、情報漏洩有無などの調査

公開サーバにおける対応

- 侵入原因（脆弱性）の特定
- 利用された不正プログラムの特定と解析
- 影響範囲の調査

主な依頼内容：補足

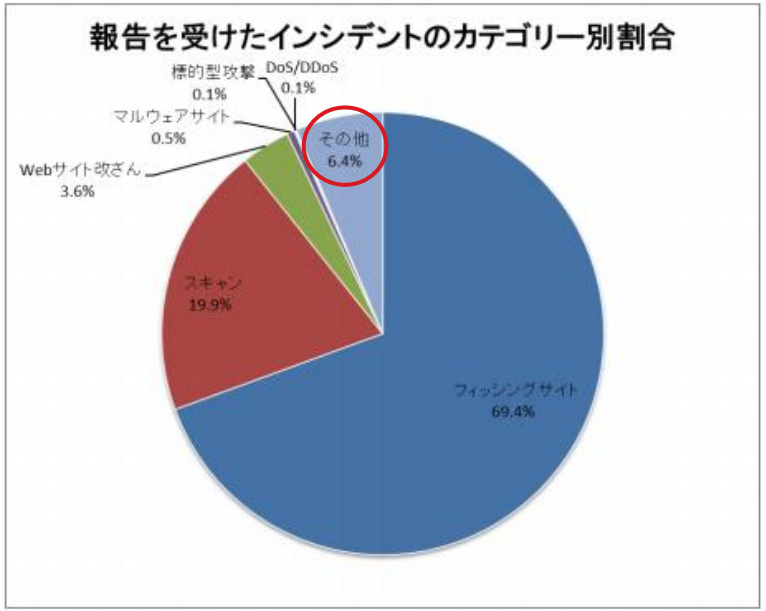
- JPCERT/CCの分類では「その他」が当社インシデント対応サービスの範囲に近い

○ その他

「その他」とは、上記以外のインシデントを指します。

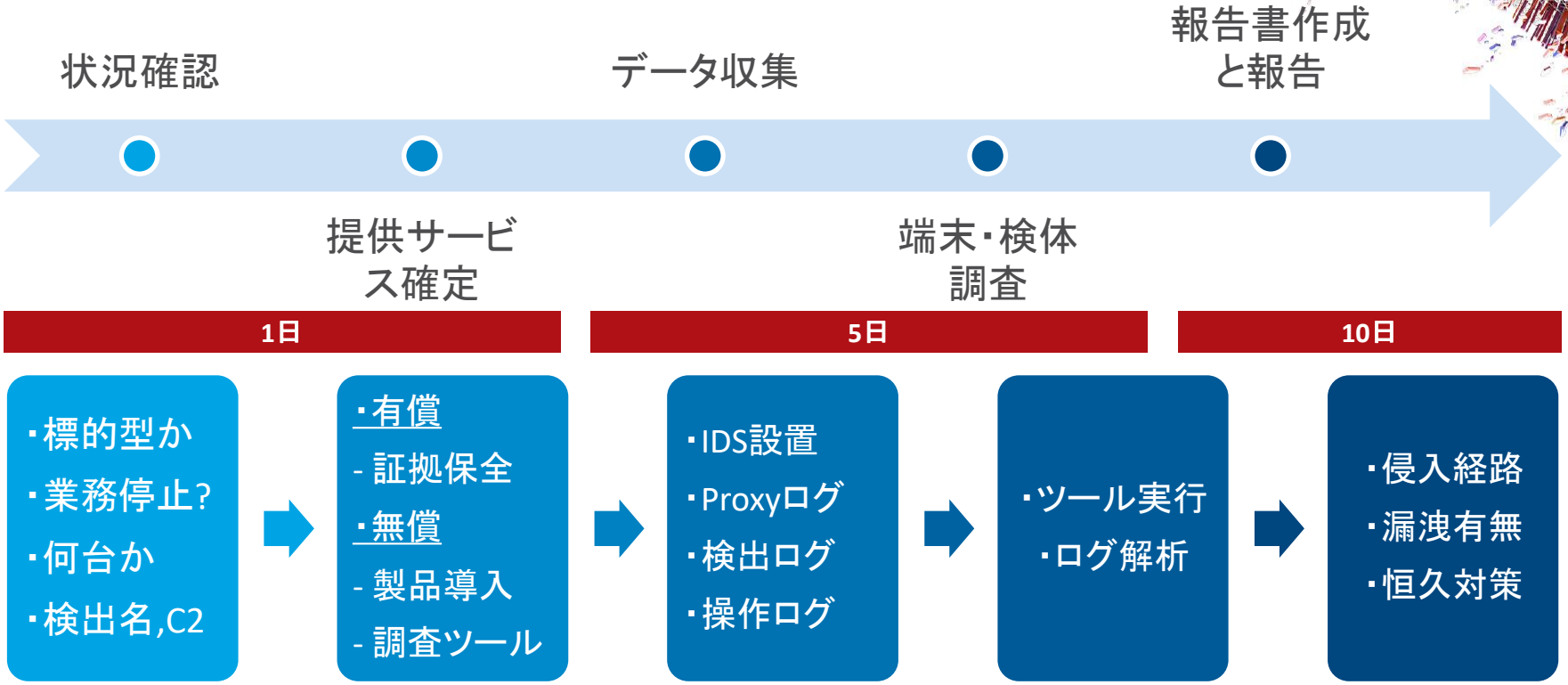
JPCERT/CC が「その他」に分類しているものの例を次に掲げます。

- 脆弱性等を突いたシステムへの不正侵入
- ssh、ftp、telnet 等に対するブルートフォース攻撃の成功による不正侵入
- キーロガー機能を持つマルウェアによる情報の窃取
- マルウェア（ウイルス、ボット、ワーム等）の感染



出典：JPCERT/CC インシデント報告対応レポート［2021年4月1日～2021年6月30日］
https://www.jpcert.or.jp/pr/2021/IR_Report20210715.pdf

ヒアリングから報告までのフロー



Tips:”通常”を知る(Know Normal)

- “通常”を把握することにより、異常に気付けるようにする
  - ネットワーク
  - プロセス
  - レジストリ
  - サービス
  - ファイル
  - アカウント
  - ログ

https://digital-forensics.sans.org/media/SANS_Poster_2018_Hunt_Evil_FINAL.pdf

Tips:フォレンジックの概要と限界を知る

・ディスク/メモリに残った情報(MFT、ファイル、レジストリ、ログ等)の作成・更新・削除のタイムスタンプから、攻撃者の行動履歴を洗い出す
・FWやProxyの外部ログ等も参照する
・SkySea等の操作ログの方が詳しく証拠が残っていることも多い

▼ログ等

日付	概要
6月1日 10:00	ユーザAが端末1でWEBアクセス
6月1日 10:00	端末1のレジストリ変更
6月2日 10:00	ユーザAが端末1でメール開封
6月2日 10:00	端末1でファイル生成
6月3日 10:00	ユーザAが端末2にリモート接続
6月5日 10:00	**端末1が暗号化(不正)**

タイプスタンプから攻撃者の行動履歴を整理

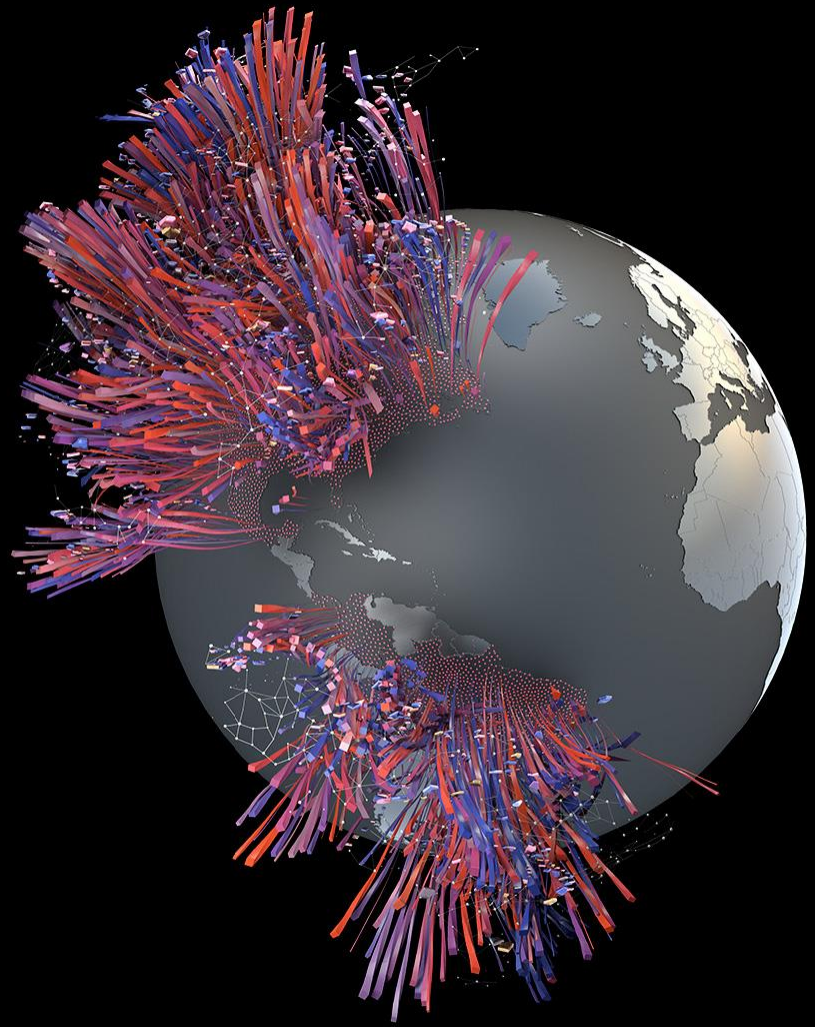
▼攻撃シナリオ

日付	概要
6月2日 10:00	ユーザAが端末1でメール開封(不審)
6月2日 10:00	端末1でファイル生成(不審)
6月3日 10:00	ユーザAが端末2にリモート接続(不審)
6月5日 10:00	**端末1が暗号化(不正)**

▼Executive向け報告

6月2日にユーザが不審メールを開き、
攻撃者が侵入。
6月3日に端末Bへ横展開を行い、
6月5日に端末Aが暗号化された。

対応実例のご紹介

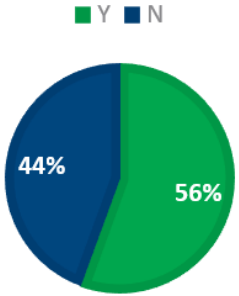


TREND MICRO

当社への相談状況 - 概況

- ランサムウェア感染のご相談が6割
  - ランサムウェアケースの内7割がランサムウェアCring

期間：2021年1月1日～5月31日



ランサムウェアの割合

二重脅迫ランサムウェア

RDP,VPNで侵入

ハッキングツール利用

EPP無効化

対応実例のご紹介

- 過去1年程の間に当社で支援したインシデントを整理

No	ランサム種別	侵入	主な攻撃ツール(TTPs)
1	[redacted]	RDP	Mimikatz,Advanced Port Scanner,Process Hacker
2		RDP	Mimikatz,Advanced Port Scanner,Process Hacker
3		RDP	Mimikatz,ADRecon,GMER
4		VPN	Cobalt Strike
5		不明	Powertools
6		RDP	PCHunter
7		メール?	QAKBOT,PSExec

Case 1,2

- RDPで侵入&拡散
- ハッキングツールの実行
- セキュリティ機能の停止

Eyes Only

Case 3

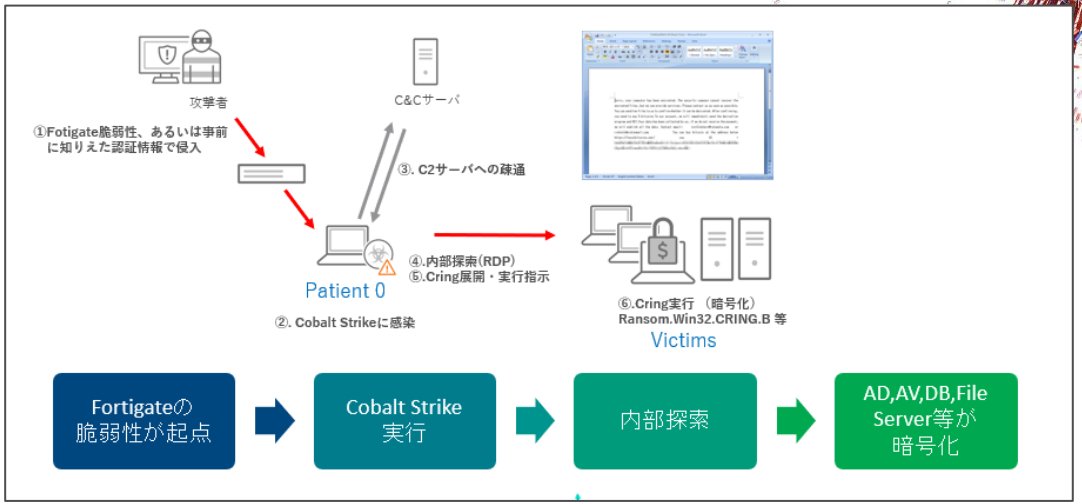
- 4以上の攻撃者が並列作業

Eyes Only

Case 3 (セキュリティ製品のアンインストール)

Case 4

- Fortigateの脆弱性で侵入
  - CVE-2018-13383
  - 初期潜入手法は普段判明しないことが多いが、Cring感染×Fortigateあり=Fortigateが起点と推測できる状況だった
  - ログからFortigateのIPが不正接続元として見えたことも多数あった



ランサムウェア「Cring」の被害が国内で拡大、VPN脆弱性を狙い侵入（2021/5/20）
https://blog.trendmicro.co.jp/archives/27830

※調査協力：田中啓介（スレットリサーチチーム）、濱口裕介（ジェネラルビジネスSE部）、サイバーセキュリティ・イノベーション研究所 スレット・インテリジェンス・センター

Case 5

- 侵入起点は不明
- RDPで侵入・拡散
- セキュリティ機能の停止

Eyes Only

Case 6

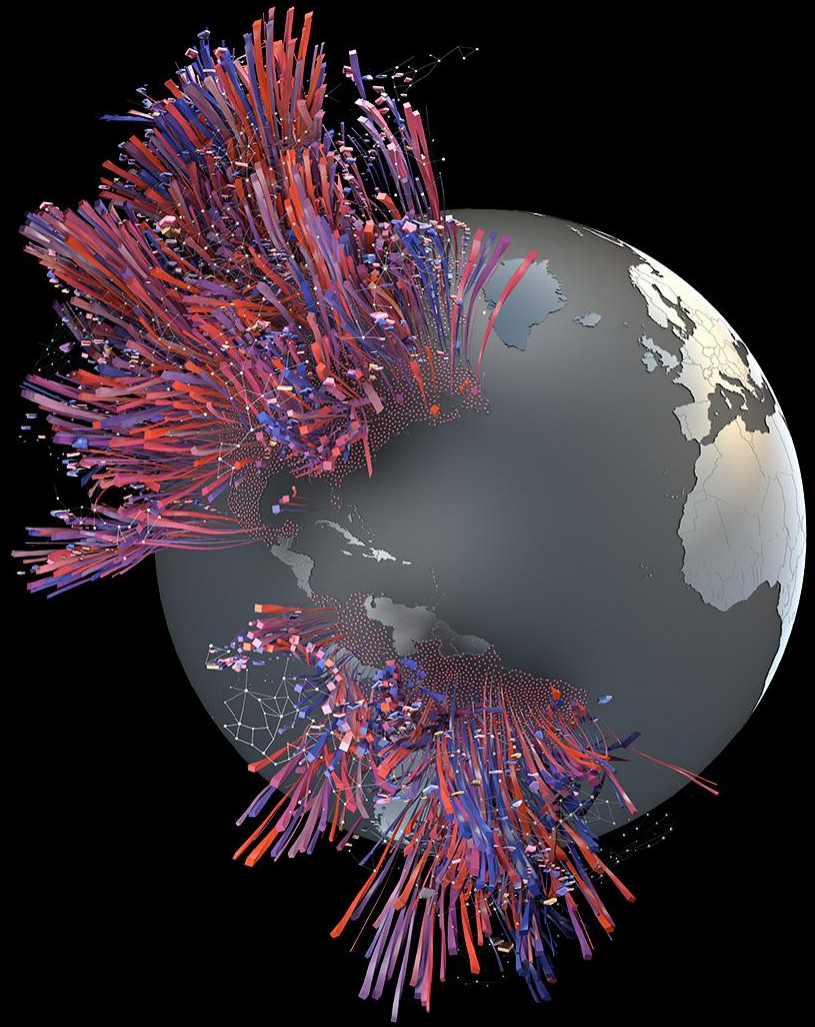
被害概要	特徴
ランサムウェア感染による重要サーバ暗号化	運用上不要なポート(3389)を悪用して感染拡大した事象

Case 7

Eyes Only

被害概要	特徴
ランサムウェア感染による業務停止	脆弱なパスワード設定、運用上不要なポートの解放。

Wrap up



TREND MICRO

本日お話ししたこと (Agenda再掲)

- インシデントレスポンス概要
- 攻撃手法について
  - 標的型攻撃
  - ランサムウェア
- 当社におけるIR対応業務
- 対応実例のご紹介

頻繁に観測されている手法・ツール

外部公開している正規サービスの悪用

- リモートデスクトップ,VPNでの侵入

ハッキングツールの利用

- Mimikatz
- Advanced Port Scanner

セキュリティ製品の無効化

- Process Hacker,PCHunter,GMER

インシデント実例を踏まえた対策

抑止
事前にインシデント発生の要因を断つ

- RDP制限
- パスワード複雑化
- 二要素認証検討

緩和
被害発生時の拡大を最小限に止める

- 挙動監視系機能の有効化
- 共有フォルダアクセス権整備
- セキュリティ製品の最新化

復旧
インシデント発生後に業務を迅速に再開

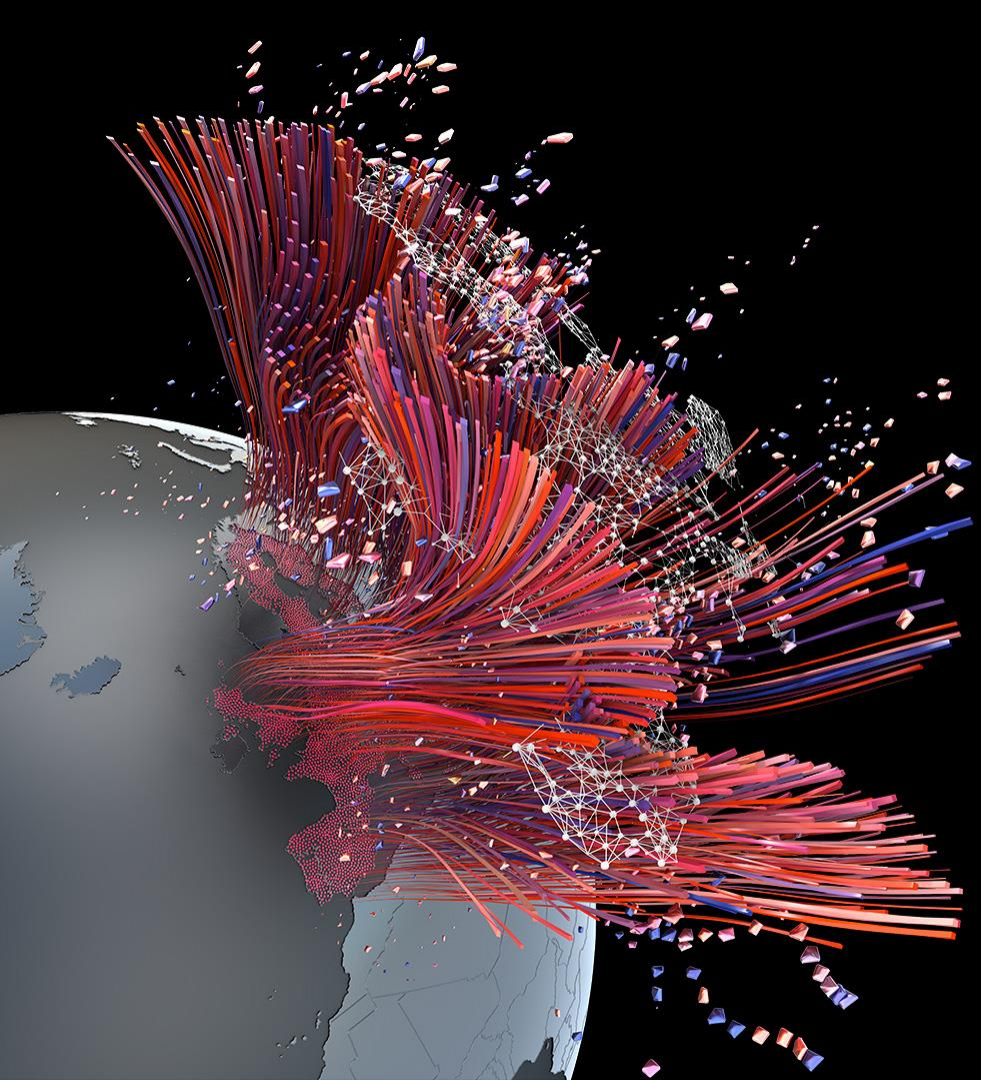
- オフラインバックアップ取得
- ADサーバとセキュリティ管理サーバの分離

参考：対策チェックリスト

- 全て〇がつけばここまで話したようなインシデントの発生を防げる

分類	チェック項目	評価
出入口	VPN装置やファイアウォール機器等ネットワーク機器のパッチ適用を定期的に行っている。	
	VPN装置で必要に応じて接続元の制限を行っている（例：海外からのVPN接続は禁止する など）	
	ネットワーク機器で退職者のアカウントや一時的なメンテナンスアカウントなどを適宜削除している。	
	ネットワーク機器のID/パスワードを推測されにくい複雑な文字列にしている。	
	スパムメールのフィルタリングサービスを導入しており、不審なメールは自動で削除されるようになっている。	
	Webサイト閲覧時にプロキシサーバ等を経由してセキュリティチェックが行われている。	
サーバ	退職者のアカウントや一時的なメンテナンスアカウントなどを適宜削除している。	
	各サーバでは異なるパスワードを設定しており、全台共通のパスワードを利用していない。	
	各サーバのサービス提供に必要なポートのみ解放するようにしている。	
	Windows以外にLinux等のサーバにもウイルス対策ソフトを導入している。	
	OSやミドルウェアのパッチ適用を定期的に行っている。	
クライアント	ウイルス対策ソフトのパターンファイルが最新になっている。	
	ウイルス対策ソフトの機能を把握し、最大限活用している。	
	ウイルス対策ソフトのアラートメールを確認し、必要に応じて調査を行っている。	
	OSやソフトウェアのパッチ適用を定期的に行っている。	
	USBメモリの私用を制限している(私物のUSBを接続できないようにしている)。	
その他	共有フォルダ等のアクセス権限を定期的に見直し、必要最小限のアクセス権限を付与している。	
	バックアップされたデータが同一LAN内にない、もしくはオフライン化されており、外部からアクセスしにくい状況で運用されている。	

〇・・・実施できている
△・・・ある程度できている
×・・・実施できていない/不明

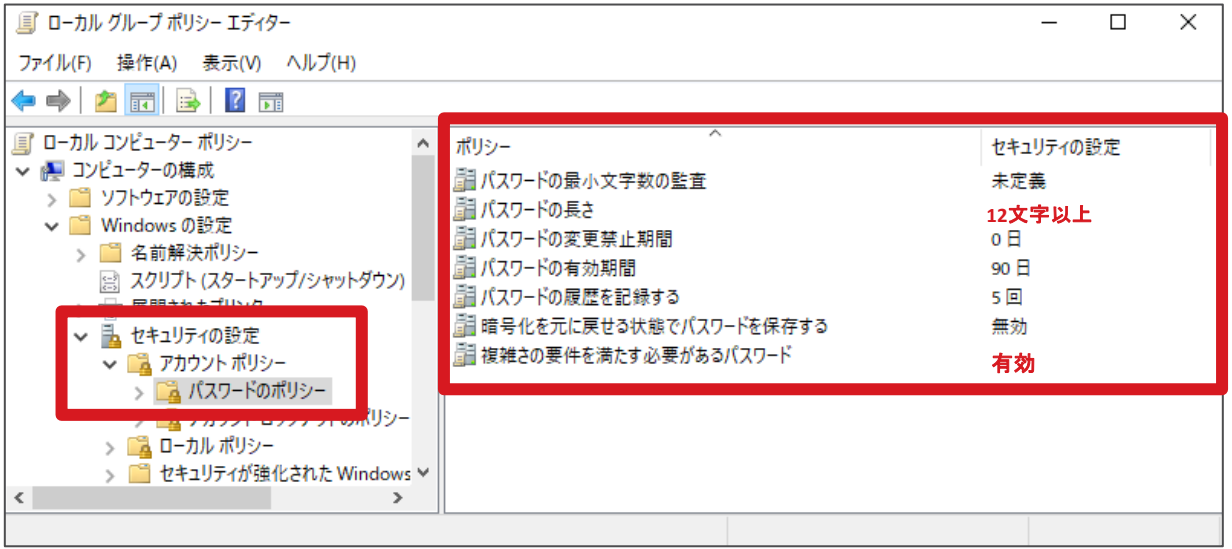


THANK YOU!

TREND MICRO

参考：パスワードの複雑化

- 12文字以上の複雑性を満たすパスワードで運用する
- Active Directoryサーバのグループポリシー>パスワードポリシー等で一括制御可能



参考：ワークステーション間の通信制御

A) Port445(SMB),3389(RDP)などクライアント端末同士では不要なポートをWindows Firewall等で制御

B) 「ネットワーク経由のアクセスを拒否」にAdministrators追加