

サイバーセキュリティ基礎 ～「攻撃」と「防御」を知る～

トレンドマイクロ株式会社
ビジネスマーケティング本部 デマンドマーケティング部
ソリューショングループ マネージャー
浅川 克明

サイバーセキュリティを理解するために…



攻撃を知る

Who	サイバー攻撃は誰が行っている？
Why	なぜ、何を目的に攻撃するのか？
Where	どんな企業のどのポイントを狙うか？
How	具体的にどのような攻撃が行われるか？



防御を知る

Who	誰が守るのか？
What	何を守るのか？
How	どうやって守るか？



攻撃を知る

Who

サイバー攻撃は
誰が行っている？

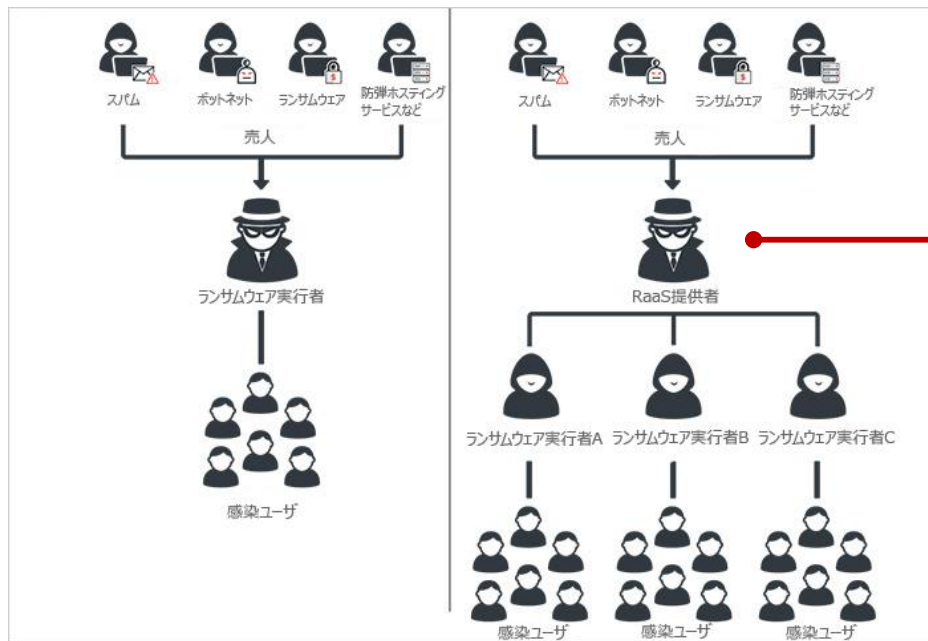
サイバー攻撃を行う者は多岐に渡る

	ローエンド型	ハイエンド型	国家支援型
例えるなら…	コソ泥	絵画泥棒	スパイ
ターゲット	無差別	選択式	指定式
目的	金銭・情報の入手	一攫千金	ミッション次第
特徴	<ul style="list-style-type: none">・ スキルが低い・ リスク&リターンが少ない	<ul style="list-style-type: none">・ 高度な攻撃手法を駆使する・ 時間をかけて大きなリターンを狙う	<ul style="list-style-type: none">・ 非常に高度な攻撃を仕掛ける・ ミッション完了まで特定ターゲットを攻撃し続ける
全体を占める およその割合	80%	15%	5%

図：サイバー犯罪者の三類型

<参考：ENISA Threat Landscape report 2018>

昨今では技術力が乏しい犯罪者でも攻撃が可能に



専門知識が要さず実行
できる形でサービスを提供

図：「ランサムウェア」と呼ばれる不正なウイルスの
利用権利をサービスとして提供するモデル
Ransomware as a Service (RaaS)

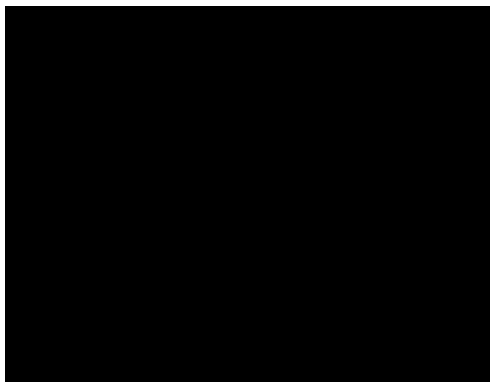


攻撃を知る

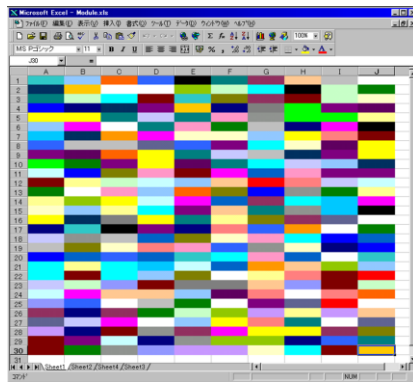
Why

なぜ、何を目的に
攻撃するのか？

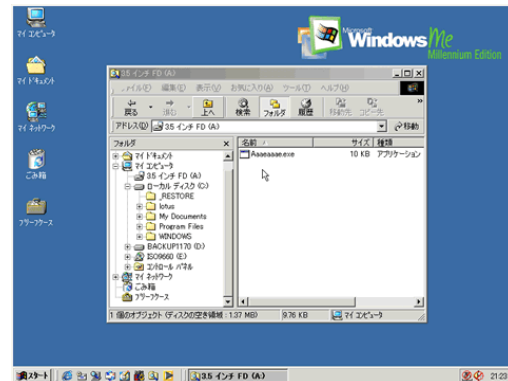
当初は「愉快犯」 目的が多かった



図：フロッピーディスクを介して感染を広げる
MS-DOS向けウイルス「アンビュランス」

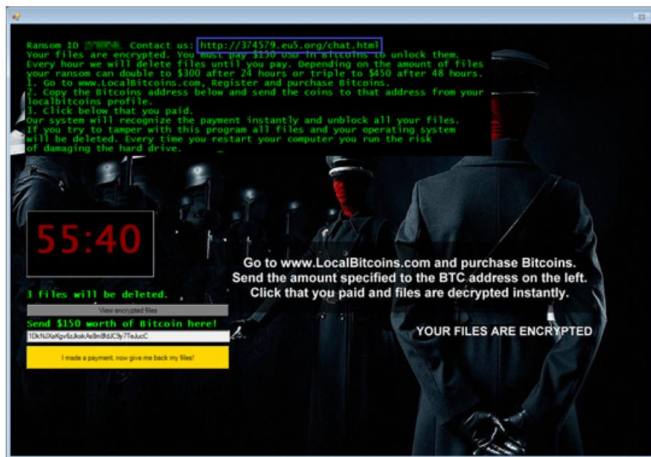


図：Excelのセルがさまざまな色に
変わる不正プログラム「シュガー」



図：画面に渦巻きを表示して端末を
操作不能にする「ハイブリス」

現在では「情報・金銭の窃取」が目的に



図：ランサムウェアによる身代金要求画面

攻撃者は窃取したあらゆる情報を転売している

内容	価格
各種ネットバンキングサービス	5ドルから
Netflix	2ドルから
Spotify	3ドルから
Disney+	1ドルから
McDonalds	1ドルから
Domino's	1ドルから
一般的なカード情報	1ドル
カード情報を含むオンラインストアのアカウント情報	1.5ドルから
使用可能額が高いカード情報	100ドルから
確認済みクレジットカード	10ドルから
偽造のカード明細書	25ドル

Welcome to my brand new account shop!

All accounts are **FRESH** and high quality.


My shop is new, but new sites are being added constantly.

Streaming

1. Netflix Basic/HD Plan - 1,00 €
2. Netflix UHD Plan - 4,00 €
3. Hulu - 1,00 €
4. Hulu (No Ads) - 2,00 €
5. Hulu (Live TV) - 4,00 €
6. Disney+ - 1,00 €
7. --More being added right this second!

Food

1. [USA] McDonald's Account - 1,50 €
2. [USA] Domino's Account + CC - 1,50 €
3. [USA] Domino's Account 60-110 Points - 1,00 €
4. [USA] Domino's Account 120-170 Points - 2,50 €
5. Grubhub Account + CC - 4,00 €

--More accounts and websites are available on my 

左表：アンダーグラウンドで確認された個人情報の取引価格

右図：動画配信サービスと食品関連サービスのアカウント情報を販売する闇市場サイトの広告例

<出典>トレンドマイクロ調査レポート「Shifts in Underground Markets」

攻撃者は窃取したあらゆる情報を転売している

The image shows a screenshot of a dark web marketplace. At the top, there is a red header with the text 'A Fortune 500 US Based Company Network Access'. Below this, there is a table with two columns: 'Author' and 'Message'. The 'Author' column contains a blurred image of a person. The 'Message' column contains the text: 'A Fortune 500 US Based Company Network Access. I am looking for a person or group who would be interested in buying network login information for a large corporation. It is a Fortune 500 company with annual profits of \$2.5B. They are global in nature, but based in the US. Their areas of'. Below the table, there is a light blue header with the text 'Sell admin access to a large online store'. Under this header, there is a row of icons and the date 'Dec 7, 2019'. To the left of the text is a blue square with the letters 'TC' and a green square with a large green letter 'H'. To the right of these squares, the date 'Dec 7, 2019' is repeated. Below the date, the text reads: 'I will sell a log with access to the admin panel of the online store on the shopify platform. Orders for \$ 10-20 thousand are made per day. The turnover for the last month is more than \$ 500k. Write suggestions in PM.'

上図：フォーチュン500企業へのアクセス権の販売例

下図：オンラインストアへの管理パネルへのアクセス権の販売例

<出典>トレンドマイクロ調査レポート「Shifts in Underground Markets」

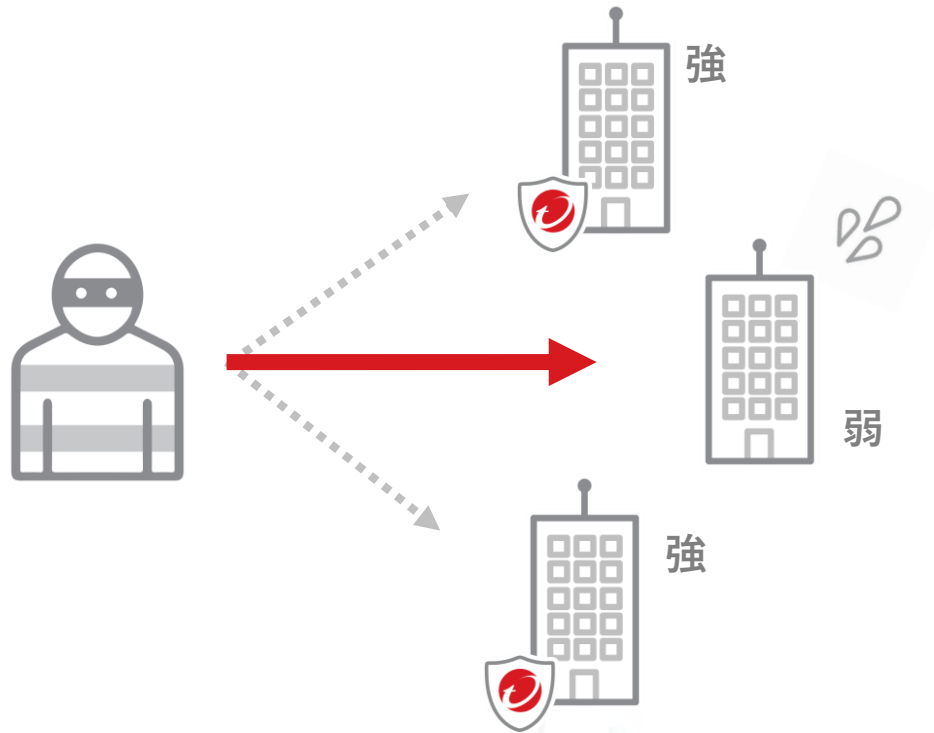


攻撃を知る

Where

どんな企業の
どんなポイントを狙うか？

セキュリティが弱い企業・弱いポイントを狙う



「うちは標的にされない」は間違い

	ローエンド型	ハイエンド型	国家支援型
例えるなら…	コソ泥	絵画泥棒	スパイ
ターゲット	無差別	選択式	指定式
目的	金銭・情報の入手	一攫千金	ミッション次第
特徴	<ul style="list-style-type: none">・ スキルが低い・ リスク&リターンが少ない	<ul style="list-style-type: none">・ 高度な攻撃手法を駆使する・ 時間をかけて大きなリターンを狙う	<ul style="list-style-type: none">・ 非常に技術力の高い高度な攻撃を仕掛ける・ ミッション完了まで特定ターゲットを攻撃し続ける
全体を占める およその割合	80%	15%	5%

図：サイバー犯罪者の三類型

<参考：ENISA Threat Landscape report 2018>

過去の中小企業におけるウイルス感染事例*

栃木県	加工食品の製造及び卸売	役員のパソコンがウイルス感染し、保存されていた過去の電子メールが勝手に大量発信され、自社及び取引先の重要な情報が漏えいする事態となった。取引先からはクレームが寄せられ、謝罪はしたものの信用が失墜してしまった。
静岡県	薄板鋼板の板金製作	従業員がメールに添付されていたファイルを不用意に開き、ウイルス感染により当社の基幹システムの設定が書き換わる障害が発生した。システムベンダの協力を得て障害の調査を行い、復旧するまでの1週間ほど、基幹システムの一部が使用できなくなった。幸い、他には被害はなかったが、セキュリティ対策の重要性を痛感した。
兵庫県	ゴム製品、加速度センサ等の製造・販売	総務系パソコン2台が「ランサムウェア」に感染し、すべてのデータが暗号化されて元に戻すことができなかった。当社は差分バックアップを行っていたため、データ滅失は一部で済んだが、再作成に時間がとられ、その間、社内の支援業務が遅延しないよう残業等で対応せざるを得なかった。
福島県	和洋菓子店	普段使用しているパソコン画面が突然動かなくなるなど、これまでに経験したことのない妙な動作をするようになった。ウイルス対策ソフトを入れているのでウイルスに感染したなどとは思っていなかったが、日頃からパソコンやFAX等の管理を依頼している地元のシステム会社にメンテナンスを依頼し確認をしてもらったところ、ウイルスに感染していることがわかった。

* 出典：独立行政法人情報処理推進機構

「2016年度 中小企業における情報セキュリティ対策に関する実態調査 事例集」（2017年8月）」より引用

<https://www.ipa.go.jp/files/000060549.pdf>

攻撃者は人とシステムの弱点に付け込む



人の弱点

- ✓ リンクの安全性を考えずにアクセスする
- ✓ メールの添付ファイルをと
りあえず開く
- ✓ パスワードが簡単&使いま
わされている



システムの弱点

- ✓ OS・ソフトウェアのアップ
デートをしていない
- ✓ 脆弱性が放置されている
- ✓ 外部からのアクセスが可能
となっている



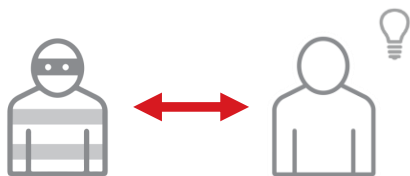
攻撃を知る

How

具体的にどのような
攻撃が行われるか？

目的達成のために多彩な手口で攻撃を仕掛けてくる

詐欺



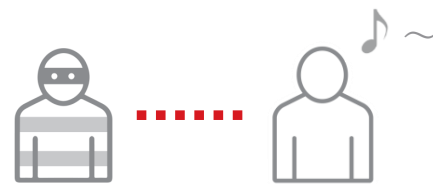
他人になりすましたり、
嘘をついてだまし取る

脅迫



大切なものを人質にとり
解放の対価として金銭を
要求してくる

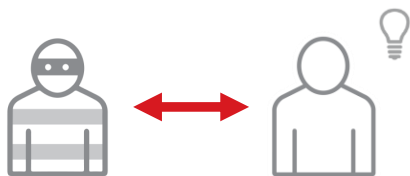
窃取



被害者に気付かれないよ
うにコッソリ盗み出す

目的達成のために多彩な手口で攻撃を仕掛けてくる

詐欺



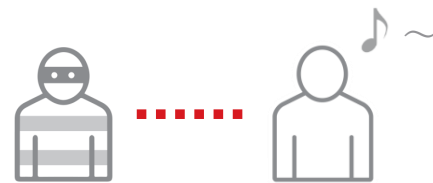
ビジネスメール詐欺

脅迫



ランサムウェア

窃取



EMOTET

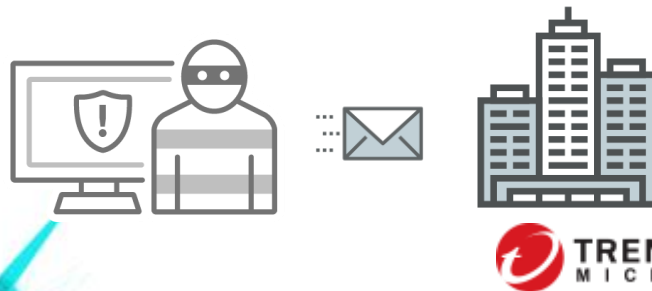
「ビジネスメール詐欺」とは？

ビジネスメール詐欺（Business E-mail Compromise（BEC））

業務メールの盗み見やネット上の情報をもとに、経営幹部や取引先等を騙った巧妙ななりすましメールを送る手口で情報詐取や不正送金を行うサイバー犯罪

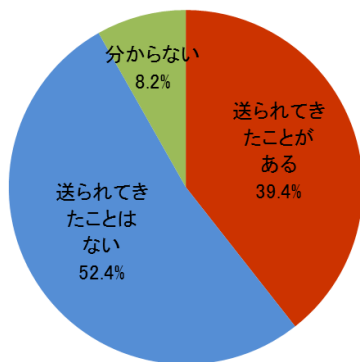
代表的な二つの攻撃シナリオ

- 経営幹部になりすまして、偽の送金指示メールを送る（CEO詐欺）
- 取引先になりすまして、偽の請求書を送る

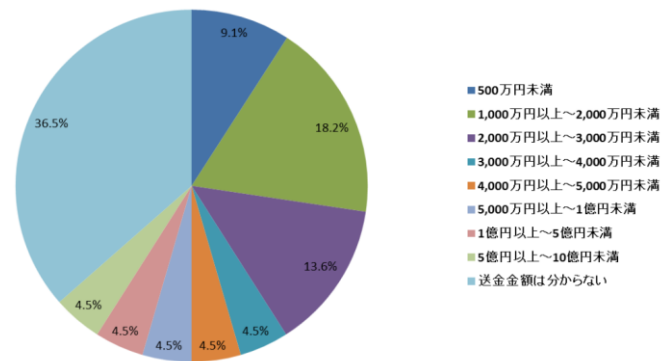


多くの組織が被害を経験している

- ✓ 全体の39.4%にあたる406人が経営幹部や取引先などになりすまし、金銭や特定の情報を騙し取るメールの受信経験がある
- ✓ 送金依頼メールの受信者（253人）のうち、8.7%にあたる22人が騙されて実際に指定口座に送金した



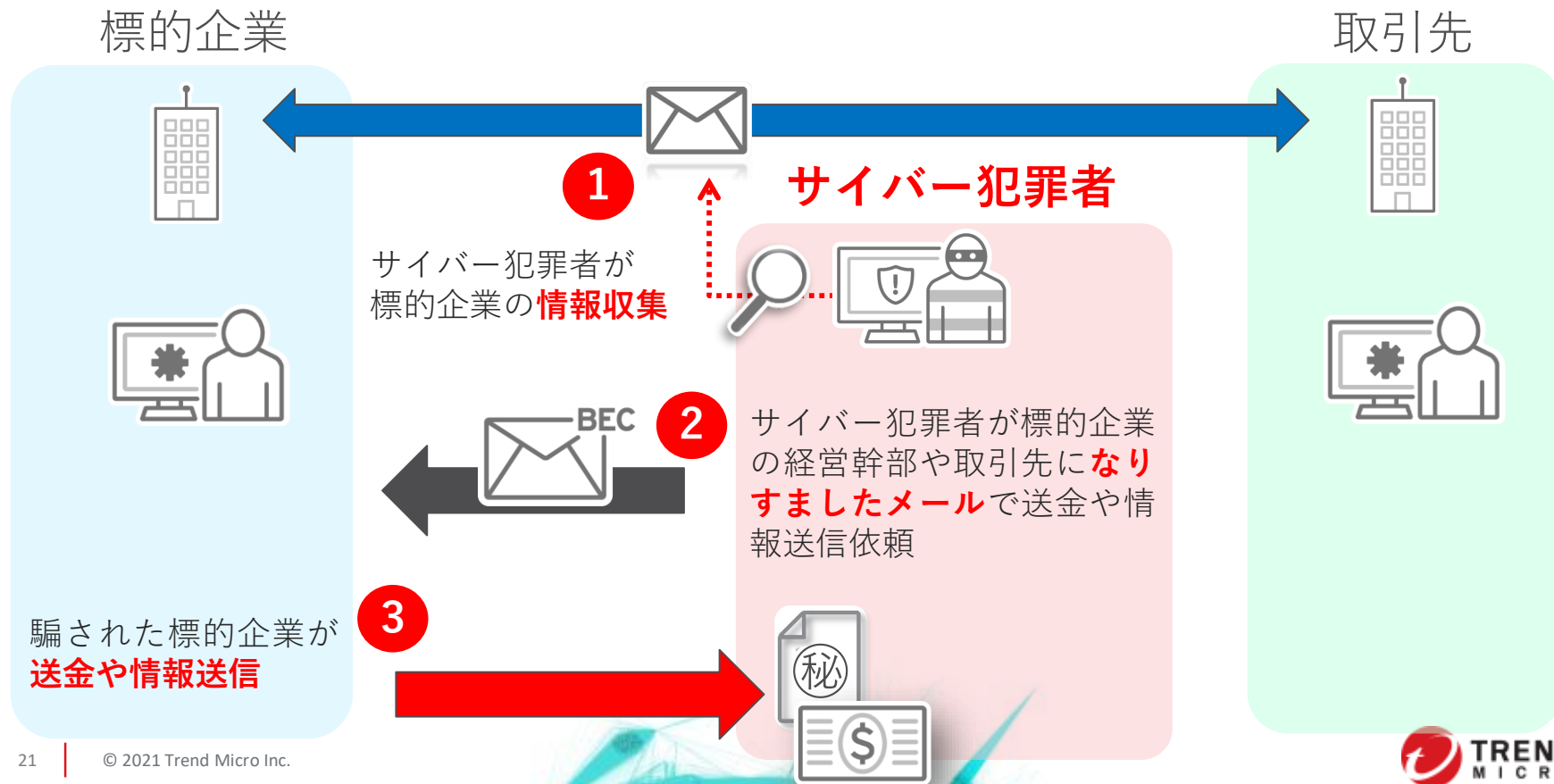
図：経営幹部：取引先などになりすました「ビジネスメール詐欺」メール受信割合（n=1,030）



図：送金依頼メールに起因した送金金額内訳（n=22）

<出典>トレンドマイクロ：ビジネスメール詐欺に関する実態調査（2018年）

ビジネスメール詐欺の流れ

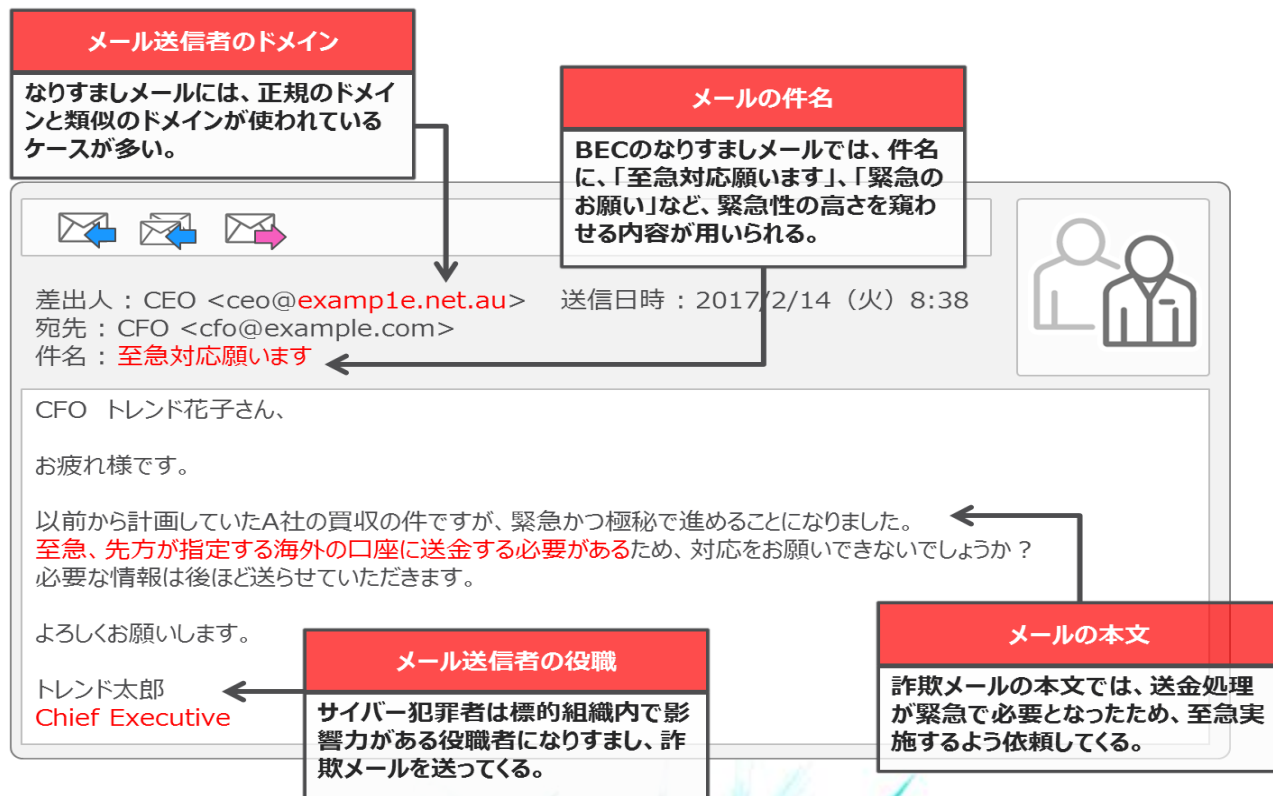


念入りな準備による高度な攻撃手口も存在する

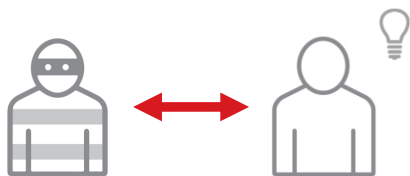
■ 攻撃手口の2つのパターン

- ✓ 公開情報をもとにした安易ななりすまし
 - └ 事前調査に労力をかけないケース
- ✓ 社内情報や取引先情報をもとにした高度ななりすまし
 - └ 本人のメールアドレスを乗っ取り十分な事前調査を行う

なりすましメールの特徴



詐欺



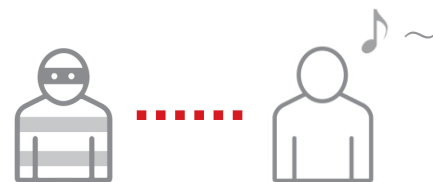
ビジネスメール詐欺

脅迫



ランサムウェア

窃取



EMOTET

「ランサムウェア」とは？

ランサムウェア (Ransomware)

感染したPCを強制的にロックしたり、PC内のファイルや共有ファイルなどを暗号化し、元に戻すことと引き換えに「身代金」を要求する不正プログラム

Ransom (身代金)

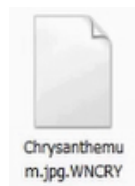


Software (ソフトウェア)



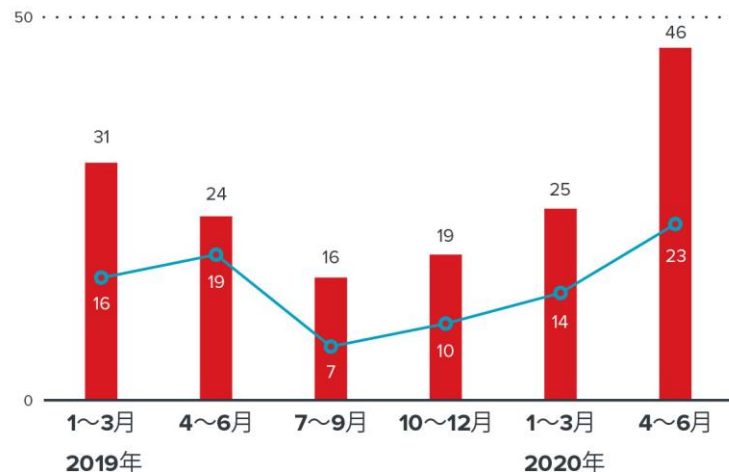
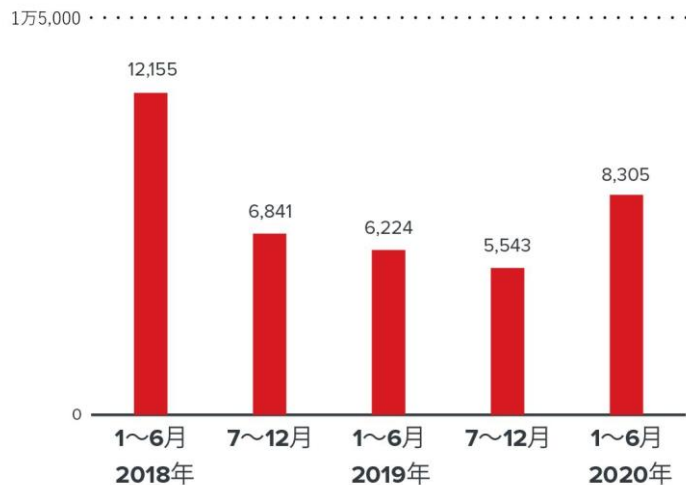
感染の流れの例（最も単純な感染方法）

- ① 正規のメールに偽装してランサムウェアが添付されたメールを受信
- ② 受信者がその添付ファイルを実行することでランサムウェアが起動
- ③ 感染したPCのファイルが次々暗号化され、暗号化されたファイルの拡張子（.pdfや.pptx）が変更される



- ④ 暗号化が完了すると、デスクトップ画面の変更やポップアップ表示などで脅迫画面を表示して、金銭を要求する

国内で続く被害



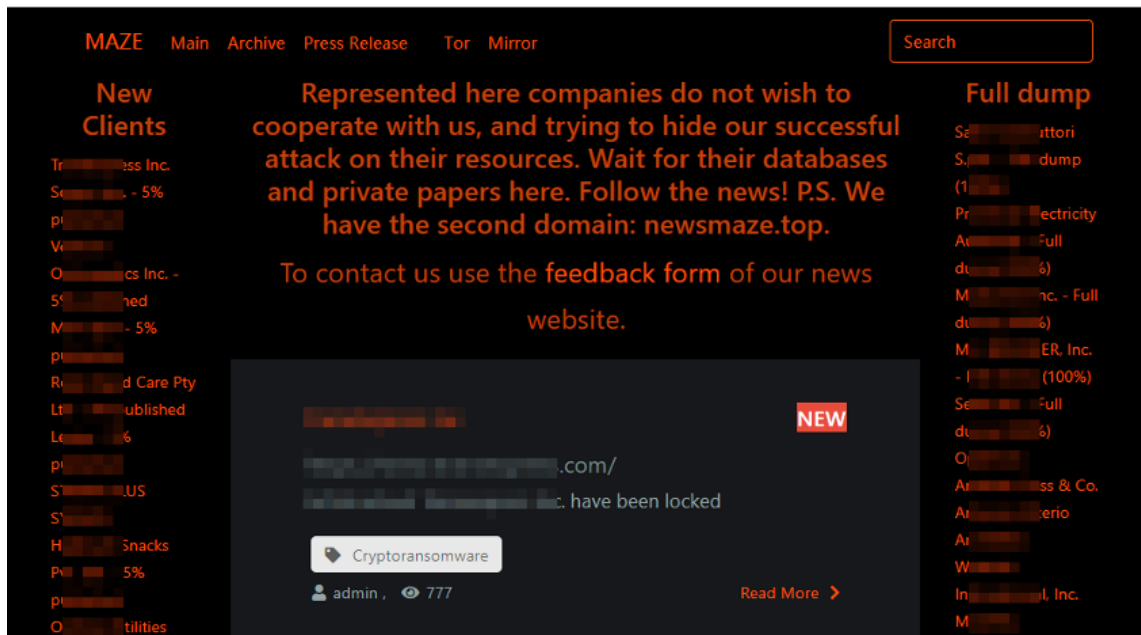
■ 全問い合わせ ● 感染被害あり

左図：国内でのランサムウェア検出件数推移

右図：国内法人からのランサムウェア関連問い合わせおよび被害報告件数の推移（トレンドマイクロ調べ）

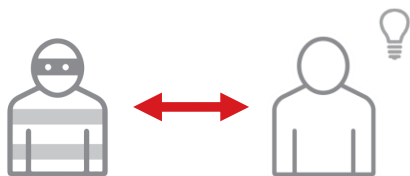
<出典>トレンドマイクロ調査レポート「2020年上半期セキュリティラウンドアップ」

二重の脅迫：「暴露型」ランサムウェアの台頭



図：ランサムウェア「MAZE」の情報暴露サイトの例

詐欺



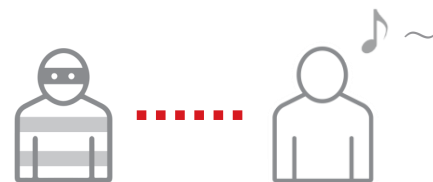
ビジネスメール詐欺

脅迫



ランサムウェア

窃取



EMOTET

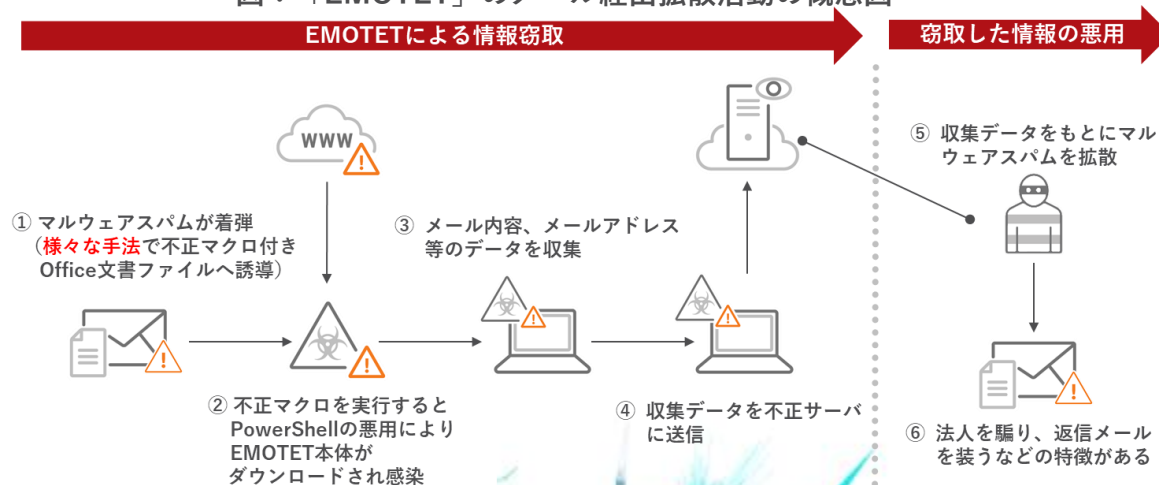
「EMOTET」とは？

EMOTET = メール経由で拡散するマルウェア (ボット)

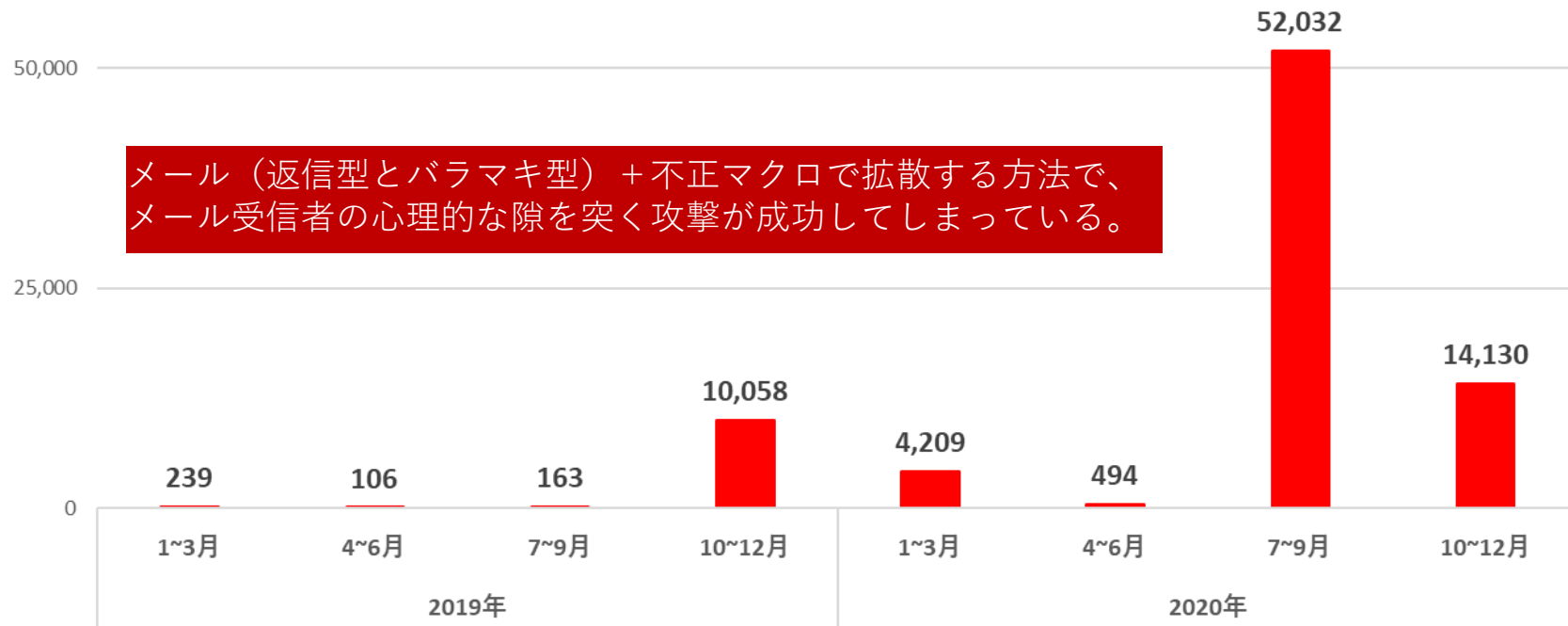
- 感染手法

- ばらまき型マルウェアスパム or 「返信型」攻撃メール
- Office文書ファイルの不正マクロ

図：「EMOTET」のメール経由拡散活動の概念図



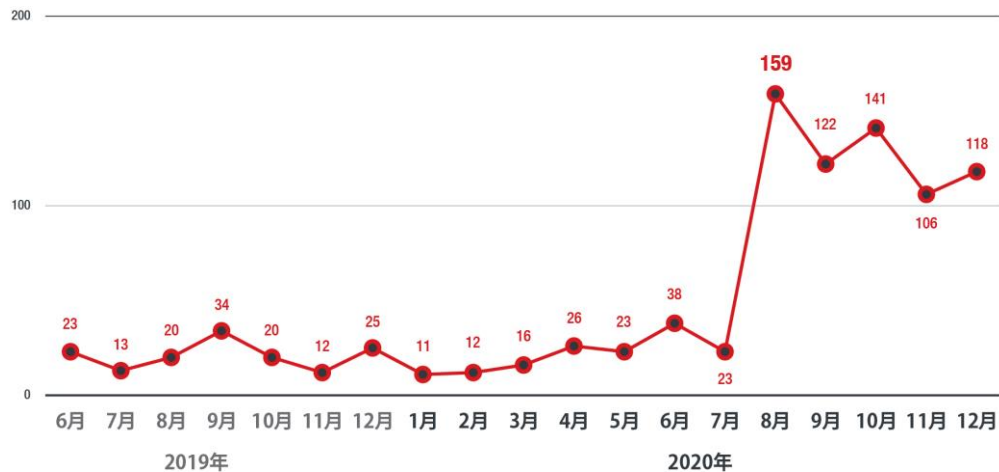
昨年、国内でEMOTET検出台数が過去最大規模



図：国内における「EMOTET」検出台数推移

「EMOTET」の被害

- 情報流出：**メール情報**・感染端末の認証情報・メールクライアントの認証など
- 更なる攻撃の踏み台化：**他組織への攻撃メール送信**・LAN内での感染拡大
- 他のマルウェアの感染：TRICKBOT、QAKBOTなどからランサムウェア、など
 - － 組織内ネットワークのアクセス権を売買される可能性も（Access-as-a-Service）

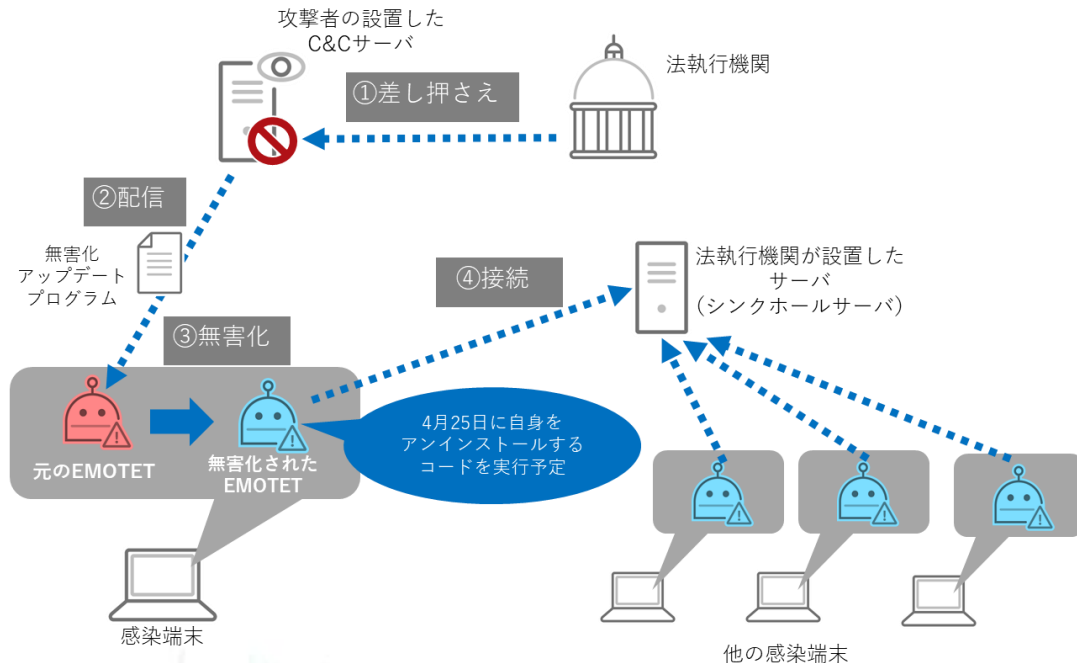


図：「QAKBOT」の国内感染台数推移

2021年・EMOTETボットネットテイクダウン

・ 1月27日EUROPOLによるテイクダウン：

- 関係者の拘束
- C&Cサーバの掌握
- 無害化検体へのアップデート
(4月25日にアンインストール)



ホーム » サイバー犯罪 » サイバー犯罪の根本解決：EUROPOLによるEMOTETテイクダウン

サイバー犯罪の根本解決：EUROPOLによるEMOTETテイクダウン

投稿日: 2021年2月1日
脅威カテゴリ: サイバー犯罪

参考：<https://blog.trendmicro.co.jp/archives/27132>

図：「EMOTET」ボットネットテイクダウンの概念図

EMOTETテイクダウンで利用者は？

- 2021年2月19日：総務省、警察庁、ICT-ISAC
「マルウェアに感染している機器の利用者に対する注意喚起の実施」
(https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00095.html)
- 今後感染が判明した場合の対応：
 - EMOTETが感染させたマルウェアは駆除されない
→ **感染調査と駆除対応**
 - 既にEMOTETが窃取した情報は戻らない
→ **使用している認証情報の変更**
 - **今後もメール経由攻撃に注意**

感染フローに合わせた事前対策のポイント

●EMOTETによる情報窃取

- ① マルウェアスパムが着弾
(様々な手法で不正マクロを含むOfficeファイルへ誘導)



Point 1
メール対策



Point 2
Web対策

- ④ 収集データを不正サーバに送信



- ② EMOTET本体がダウンロードされ感染



- ③ 不正な活動開始。メール内容、メールアドレス等のデータを収集



Point 3
エンドポイント対策

●窃取した情報の悪用

- ⑤ 収集データをもとにマルウェアスパムを拡散



- ⑥ 法人を騙り、返信メールを装うなどの特徴がある

Point 1
メール対策

「 攻撃を知る」 まとめ

Who	✓ 個人から国家支援型の組織まで多岐に渡る
Why	✓ 組織がもつ 金銭・情報を奪う ため ✓ 奪った情報は転売で金銭を得ることもある
Where	✓ セキュリティが 弱い企業・弱いポイントが狙われる ✓ 無差別に行われるため「うちは狙われない」は通用しない
How	✓ ビジネスメール詐欺 ：メールで取引先や経営者を騙り金銭を奪う ✓ ランサムウェア ：ファイルを暗号化した上で身代金を要求する ✓ EMOTET ：メール情報を盗み取り、他組織へも攻撃を行う



防御を知る

Who

誰が守るのか？

「個人」と「組織」の両軸での対策が必要



個人ができること

- ✓ 不審なメール・URLは開かない
- ✓ 文書ファイルのマクロは有効化しない
- ✓ サービスによってパスワードを使い分ける



組織ができること

- ✓ セキュリティポリシーを整備する
- ✓ 最小権限の原則を守る（アクセス権限の適切な管理）
- ✓ ソフトウェアの脆弱性対策を行う
- ✓ 資産を可視化・管理して攻撃のエントリポイントを作らない
- ✓ セキュリティ対策製品を導入して攻撃に関連するファイル・URL・メールなどをブロックする



防御を知る

What

何を守るか？

セキュリティ担当の使命は「重要情報を守る」こと

✓ 重要情報とは？

- 顧客・取引先の情報
- 事業戦略・営業機密情報
- 技術情報 など

✓ 重要情報はどこに保存されている？

- サーバ上（オンプレ/クラウド）
- 従業員の端末
- メールのやり取り など



- ✓ **重要情報が保存されているパソコンなど端末の保護**（エンドポイント対策）
- ✓ **侵入の糸口となるインターネットの出入り口の保護**（ゲートウェイ対策）



防御を知る

How

どうやって守るか？

侵入を前提とした対策



全てのサイバー攻撃を入口で防御することは難しい



万が一入口を突破されても、その次のエリアで止められるように多層で防御する（**多層防御の考え**）



万が一侵入されてしまった場合に、すぐに気付いて迅速な調査・対処ができる仕組みを作る

多層防御＝防犯上の役割分担

それぞれの部屋（PCなどの端末）に鍵をかけて（ウイルス対策ソフトを入れて）不審者（危険なウイルス）を自分の部屋に侵入させない



パソコンの
セキュリティ対策

マンション玄関（インターネットの出入口）のオートロック（出入口での対策製品）で不審者（危険なウイルスや不正メール）をマンション内に侵入させない



インターネット
の出入口対策

多層防御による高度な防犯対策

「 防御を知る」 まとめ

Who	✓ 「個人」と「組織」の両軸での対策が必要
What	✓ 「重要情報」を守る
How	✓ 侵入を前提とした対策 <ul style="list-style-type: none">• 多層防御• 侵入された際に迅速に調査・対処できる仕組み作り



THE ART OF CYBERSECURITY

数千のハイブリッドクラウドワークロードを7日間トレンドマイクロのAPIを通じて自動保護をした結果。実際のデータを使用し、Trend Micro threat researcher またアーティストの **Jindrich Karasek** によって作成されました。