Confidential

JPX GROWTH
証券コード：7067

ブランディングテクノロジー保守顧客向け資料

サイバー攻撃の脅威に対し 中小企業が行うべきセキュリティ対策 (2023下期版)

2023.12　ブランディングテクノロジー株式会社

Google Partner PREMIER 2022
Google Analytics Certified Partner
Google Marketing Platform Certified
YAHOO! JAPAN Marketing Solutions ★★ Partner

その想いを、たしかな未来へ
Branding Technology

目次

はじめに

中堅・中小企業をおびやかすウイルス。求められるセキュリティ対策とは？

2023年7月、コンピュータウイルス「ランサムウェア」による被害が大きく報道されました。名古屋のコンテナターミナル管理会社のシステムがウイルスに感染し、処理を行う2日以上の間業務が止まってしまった、というものでした。

画像引用：名古屋港システム障害 ターミナルすべてで運用再開 物流混乱も
https://www3.nhk.or.jp/news/html/20230706/k10014120421000.html

このようなサイバー攻撃の被害はコロナ禍以降増加しています。
以前は企業のサイバー攻撃は「大企業が考えるもの」という意識がありました。しかしどの企業でも重要な情報をPCで管理するようになり、ネットに繋がったPCを多用するようになった結果、セキュリティ対策の手薄な中小企業で被害割合が多くなっています。

個人情報の管理が厳しく見られる中、ウイルスによる情報漏洩が起きれば企業の信頼を大きく損ねることにもつながります。
現在では企業の規模によらず対策を考えなければいけない状況になっていると言えます。

本資料では中堅・中小企業のセキュリティリスクについてご説明します。また、求められる対策としてセキュリティのガイドラインと、UTM（統合脅威管理）をご紹介します。御社のセキュリティを見直すためのきっかけとしていただければ幸いです。

中小企業を標的とする攻撃

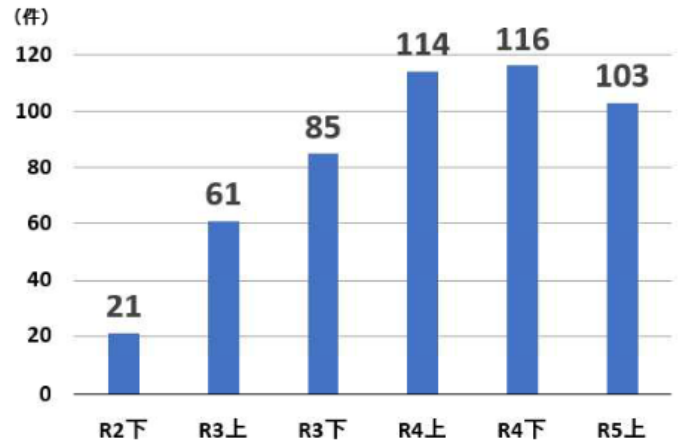
ランサムウェア・ Emotet

2023年最大の脅威「ランサムウェア」

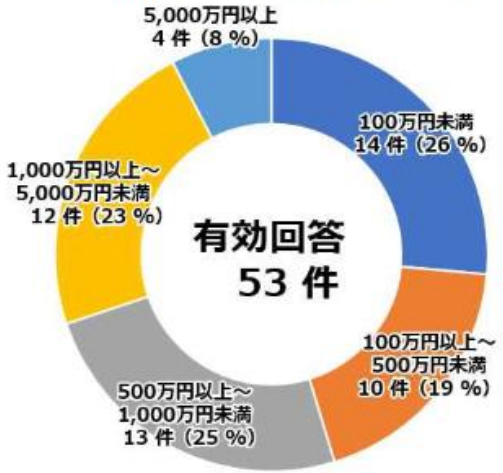
金額の大きい被害が多く、被害件数も増えている最も警戒すべき脅威

- 「ランサムウェア」は被害が続いている悪質なウイルスの一種
- 「身代金要求型」と呼ばれ、感染PCを戻すかわりに対価を要求される
- 一企業だけの被害で終わらずサプライチェーンに感染が広がる場合がある
- 調査・復旧に多額の費用を要することが多い

【図表17：企業・団体等におけるランサムウェア被害の報告件数の推移】



【図表24：調査・復旧費用の総額】



画像引用：https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf
令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について

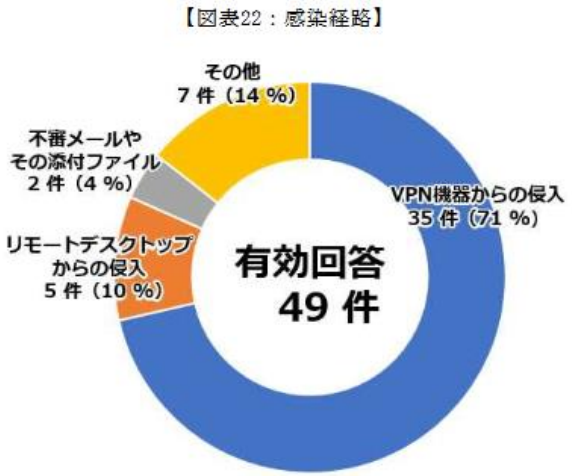
2023年の「情報セキュリティ10大脅威」の1位になっているウイルスが「ランサムウェア」です。
左の棒グラフのように被害件数が高い水準にある脅威で、直近では2023年7月に冒頭に紹介した名古屋港コンテナターミナルで起きた被害のほか、直近でも2023年12月に経済メディア「ダイヤモンド社」が被害を受けたことを公表しています。
https://www.itmedia.co.jp/news/articles/2312/12/news112.html

ランサムウェアは被害額が大きく、左の円グラフのように、被害にあった企業の7割以上が調査・復旧に100万円以上を要したという統計があります。
いまビジネスが最も警戒すべきセキュリティの脅威と言えます。

ランサムウェアの攻撃方法

ウイルスに感染したPCを「人質」に金銭を要求される。ネットワークセキュリティの脆弱性が感染原因

- ウイルスに感染するとPCのデータがロックされ、業務ができなくなる
- 「暗号化されたPCの解除」「窃取されたデータの非公開」で2回対価を要求される
- 流出した情報が闇サイトに掲載されたり販売される場合も
- リモートワークで利用されるVPNやリモートデスクトップからの感染が8割



ランサムウェアはPCだけでなく、流出させたデータも人質にして身代金を要求してきます。PCのデータはその後闇サイトなどで公開されることもあり、重大な被害になる可能性があります。
感染経路の多くはリモートワークで利用されるPC・ネットワークのセキュリティレベルが低いことが原因とされ、コロナ禍後に増えた在宅ワークの流れが狙われていると考えられます。

2023年には暗号化をせず、窃取した情報の公開のみにおいて恐喝を行う「ノーウェアランサム」という脅威も確認され、今後も新しい攻撃方法が現れる可能性があります。最新の情報を押さえ、備えておくことが重要です。

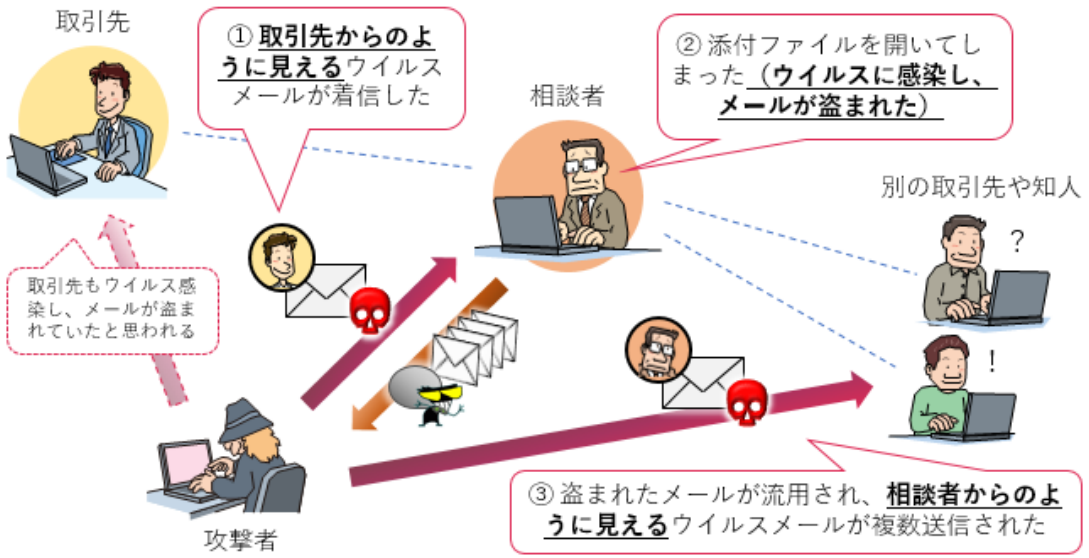
画像引用： https://www.sbbit.jp/article/cont1/65631
ランサムウェアとは何か？手口・対策・事例、気になるポイントをまとめて解説

画像引用：https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf
令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について

2022年の代表的なサイバー攻撃。ウイルス「Emotet（エモテット）」

中小企業にも大きな感染被害を出したウイルス「Emotet（エモテット）」

- 感染するとPC内の情報を漏洩させるほか、より悪質な他のウイルスにも感染させる「Emotet」は今後も注意すべき脅威
- 2019年から流行が見られたコンピュータウイルスで、メールの添付ファイルを通じて広がる
- 中小企業でも被害が多く、特に2022年3月の流行で大きな感染被害が確認される
- 「実際の取引先のアドレス」を使い「ビジネスで使うような文章」のメールで広がるため判別がしにくい



2022年に中小企業の脅威となったのが「Emotet（エモテット）」というメールで広がるウイルスです。一見して判別が難しく、ウイルスソフトからもすり抜けやすい仕組みを持っています。

年度前半に感染が拡大し、企業・団体の規模を問わず多数の感染被害が発生。Emotetだけで1年間に145件の被害報告がありました。その後感染の沈静化と再拡大を繰り返していますが、2023年春以降大きな感染拡大は発生していないようです。ただ一度感染が拡大すると拡散しやすい性質があり、今後も動向の注意が必要です。

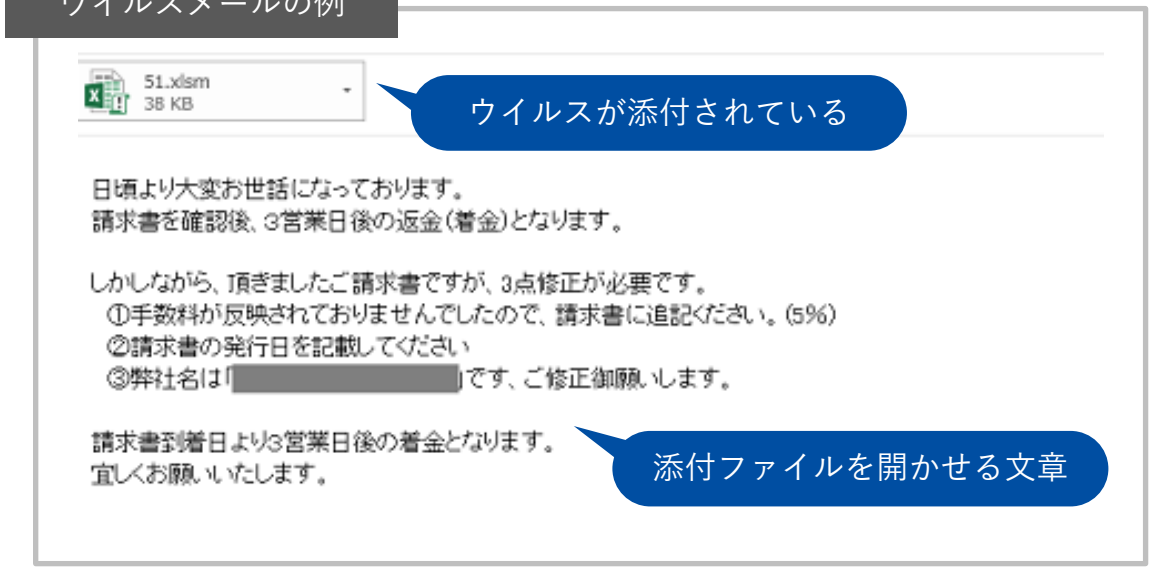
画像引用：https://www.ipa.go.jp/security/announce/20191202.html
Emotet（エモテット）と呼ばれるウイルスへの感染を狙うメールについて

Emotetの攻撃方法

一般メールを装い、セキュリティソフトをすり抜けるウイルスで危険性が高い

- 取引先のメールアドレスを利用し、ビジネスメールのような形でメールを送信するため見逃しやすい
- 普通のメールと同じ形式のため、セキュリティソフトがウイルスと判別できない
- 取引先からのメールだと安心して添付ファイルを開くと感染してしまう
- ビジネスの非常に近くにある脅威

ウイルスメールの例



これまでのスパムメール・ウイルスメールは、英語であったり意味不明な内容であったりと判別することが容易でした。Emotetのメールは一見ビジネスメールのような体裁で届くことが多く、ウイルスのファイルを間違えて開きかねない内容になっています。また、通常のビジネスメールと同じ形式のため、セキュリティのチェックですり抜けやすいのも特徴です。これらにより感染が大きく拡大しました。
2023年でも未だにウイルスメールの新種が発見されており、油断できないウイルスです。

画像引用：https://www.ipa.go.jp/security/announce/20191202.html
Emotet（エモテット）と呼ばれるウイルスへの感染を狙うメールについて

コンピュータウイルスによる被害とは

情報流出により信用が失われ、取引先や顧客への対応に追われる

- **個人情報や企業情報、PC内のデータが流出する**
- **関係する連絡先にウイルスを広げる**

- **情報漏洩の対応が必要になる**
  漏洩した情報の精査、漏洩元顧客への謝罪・補償、広報、報告などが必要に
- **回復作業により本来の業務が止まる**
  PC・ネットワークの検査・検疫、再インストール、再設定などが必要に
- **関係先に迷惑をかける**
  ウイルス付きメールを配信したことに対する連絡、謝罪、説明などが必要に
- **自社のブランドが傷つく**
  セキュリティに甘い会社、対応ができていない会社という評価に

コンピュータウイルスの怖い点は、実際の感染症と同様、感染すると自身が感染源となってウイルスを撒き散らすことにあります。

感染後はウイルスを除去するまでネットに繋げず、業務や連絡ができなくなります。発注や納品にも影響が出るほか、会計システムが利用できないことで業務全体が機能不全に陥る可能性もあります。

今年の被害の例として2023年1月、不動産情報を扱う「三春情報センター」が被害にあっています。
https://scan.netsecurity.ne.jp/article/2023/02/06/48869.html

自社には関係のない事柄と考えず、「感染しない」そして「感染させない」ための「感染対策」をPCでも考えることが必要です。

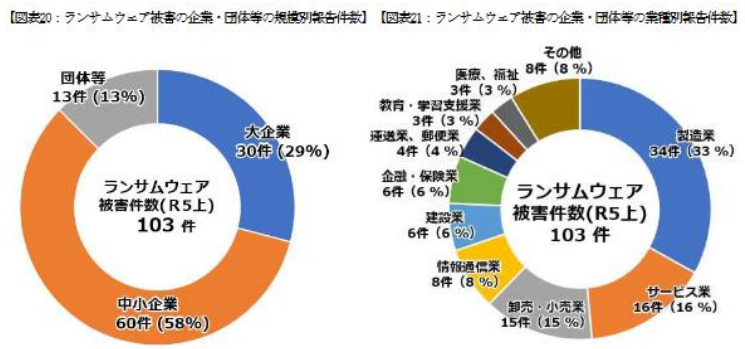
被害が増えている背景

コロナ禍を機に、セキュリティの弱いPCがネットにつながったことが要因の1つ

- コロナ禍以降、ビジネスもネット経由のやり取りが増えた
- セキュリティ設定の弱いPCが増加、狙われやすく
- リモートワークの増加、企業以外のPCでの業務
- 会社がデータ利用やセキュリティの全体を把握できていない

中小企業も狙われている

- **ランサムウェア被害の半分以上が中小企業**
- **セキュリティにコストを掛けていない場合が多い**
- **関係する大企業を狙うための踏み台にされる**



画像引用：https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf
令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について

ランサムウェアやEmotetの被害が増加していることの要因として、コロナ禍以降の業務環境の変化が挙げられます。
リモートワークするため、セキュリティの弱いPCでリモートデスクトップやVPN機器などを利用したことで感染する事例が多いようです。通常業務を行うPCではセキュリティのレベルを管理していても、リモートで利用する自宅のPCについては管理が難しい、という事情もあったようです。

こういった被害の報道では大企業の事例が多く挙げられますが、左のグラフのように、実際の被害件数は中小企業がその半分以上を占めています。
また、製造業が被害の1/3を占めており、攻撃者から「セキュリティの低い企業が多い」と認識されている可能性があります。

こういった現状を踏まえ、どのような対策を取ったら良いか、次のページから解説します。

中小企業が行うべき対策

情報セキュリティガイドライン・UTM（統合脅威管理）

現在のセキュリティ対策で重要な方針

攻撃を完全に防ぐのは難しいという前提で対策を行う

ターゲットにさせないためにもセキュリティ対策は必要

- 基本的なセキュリティ対策を怠らない
- セキュリティの強い企業よりも**弱い企業が狙われる**
- 攻撃のコストがかかる、リスクがあると思わせることが重要

感染時の影響を最小限に抑えることが重要

- 対策をやりきっても続けるのは難しい
- 感染するときは感染する、という前提での対策が必要
- 攻撃があったときも**被害を最小限に抑える施策**が重要

現在のセキュリティ対策の方針としてまず考えるべきは、完全な対策は無いということです。つまり、感染するときは感染してしまう、ということです。中小企業が行うセキュリティのレベルは、大規模な攻撃を想定していません。攻撃側が本気を出せば被害を受けてしまいます。

また、攻撃側はいつ仕掛けてくるかわかりませんが、備える側は常に備えていなければいけません。加えて、人が介在する仕組みでは、イレギュラーが発生したときにリスクのある行動を行ってしまうこともあります。ですから、人の頑張りに頼る施策も避けるべきでしょう。

この前提の上で、「できるだけ狙われないように」する、「攻撃を受けても被害を抑える」ための方策を考えるのが、現実的なセキュリティ対策と言えます。

特に気をつけたい長期休暇（お盆・年末年始・GW）

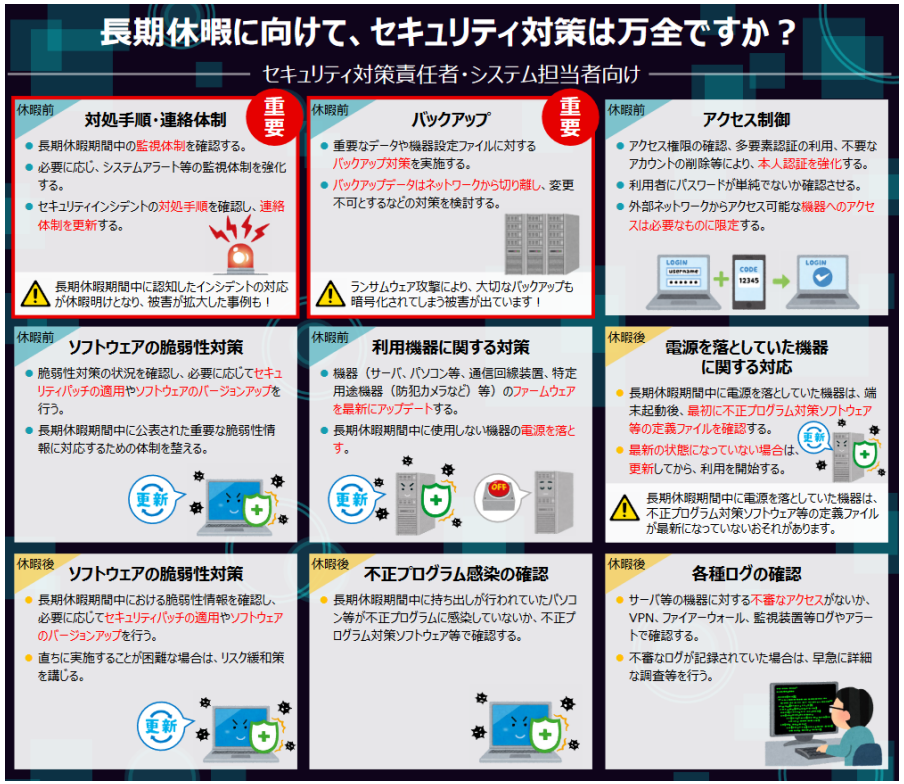
セキュリティの弱い「状況」があることを認識する

セキュリティの弱い企業が狙われるように、
セキュリティの弱い「状況」は攻撃から狙われやすいです。

企業では長期休暇の時期（お盆・年末年始）などがそれにあたり、セキュリティ担当者と連絡がつきにくくなる、通常リモートワークを行わない担当者が顧客対応のためにPCを持ち帰る、などイレギュラーの状況が発生しやすい時期となります。

サイバー攻撃は対応の遅れが深刻な被害の発生を生むこともあり、長期休暇の時期は遅れが発生しやすくなります。警察庁・経済産業省やIPA（情報処理推進機構）は各長期休暇の前に注意喚起を行っています。バックアップや対処の方針など、下記資料を元にできるところから対応を行っていくことが必要です。

長期休暇における情報セキュリティ対策
https://www.ipa.go.jp/security/anshin/measures/vacation.html



画像引用：
https://www.meti.go.jp/press/2023/04/20230424002/20230424002-2.pdf
長期休暇に向けて、セキュリティ対策は万全ですか？

具体的な対策方法1・情報セキュリティガイドライン

IPA（独立行政法人情報処理推進機構）のガイドラインに従う

ガイドラインにそって自社の状況を見直し、対策を講じる

- まず行うべき対策：情報セキュリティ５か条
  https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055516.pdf
- 自社の状況をチェックする：5分でできる！情報セキュリティ自社診断
  https://www.ipa.go.jp/security/guide/sme/ug65p90000019c86-att/000055848.pdf
- 中小企業の情報セキュリティ対策ガイドライン
  https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

セキュリティ対策運用の問題点

- **常に対策を行う必要がある**
- **ネットワークに繋がるすべての機器の状態を把握するのが困難**
- **人の行動を変えるのは限界がある**

画像引用：5分でできる！情報セキュリティ自社診断、
中小企業の 情報セキュリティ対策 ガイドライン

IPA（情報処理推進機構）が中小企業向けの詳しいガイドラインを公表しています（無料）。「どこから手を付けたら良いかわからない」という企業から対応できる易しい内容です。

ただ、左に記載したような問題点もあります。自動で対応できるソフト、システムを導入するのも現実的な対策と言えるでしょう。

具体的な対策方法2・UTM（統合脅威管理）の導入

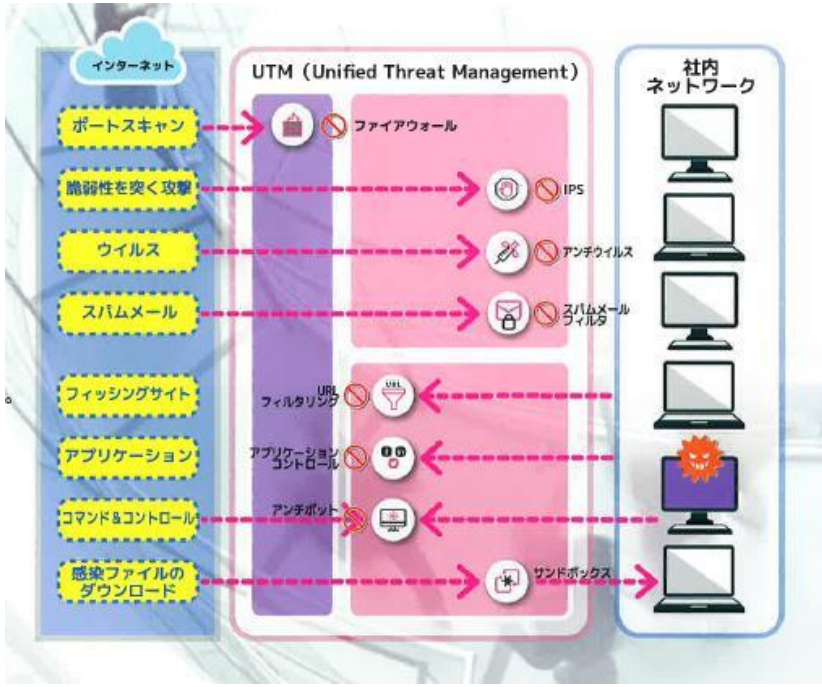
運用では対応しきれない部分を、専用のシステムで管理

UTM（統合脅威管理）とは？

- ネットワーク全体の門番となるシステム
- 社内LANとインターネットの間に物理的に装置を設置する
- ネットワークへのアクセスを監視し、攻撃を防ぐ
- ウイルスソフトより対応範囲が広く、一元的に管理可能

メリット

- **PCごとの設定が不要**
- **スパムメールや、内部からの情報漏洩も防止できる**
- **社内にセキュリティ担当者がいなくても対応可能**



セキュリティ対策のシステムとして現在企業に導入が進んでいるのがUTM（統合脅威管理）です。これは次世代ファイアウォールとも呼ばれ、ネットワークのセキュリティを一元的に管理できるシステムです。
ネットワークに直接設定するため、接続するPC等の機器を個別に管理する必要がありません。また、セキュリティの専門知識が少なくても運用が行えるため、中小企業でも導入が望まれています。

ブランディングテクノロジーのご提供するUTM

統合セキュリティ「CheckPoint」をご提供しております

特徴

- 中堅・中小企業向けに実績あるUTM（統合脅威管理）
- 一台で社内のネットワークすべてを管理
- ウイルスソフト・ファイアウォールでは
  対応できない攻撃からもネットワークごと防御できる

こんなビジネスにおすすめ

- 業務で**複数台**のPCを利用する
- 住所やカード情報のような**個人情報**を扱うPCがある
- セキュリティの**担当がいない**、いるが専門知識が少ない
- WIFIでつながっているPC、スマホを把握できていない

顧客情報を取り扱う観点から、中堅・中小企業でも情報セキュリティへの対応が求められています。しかし、整備するための時間が取れないという企業は多いです。そのような場合でもUTMはほぼ「おまかせ」の対応が可能なため、時間の取れない企業ほど導入をおすすめしております。

詳しいご説明・ご相談をご希望の方は
下記のボタンよりご連絡くださいませ。

ご相談はこちらから »

おわりに

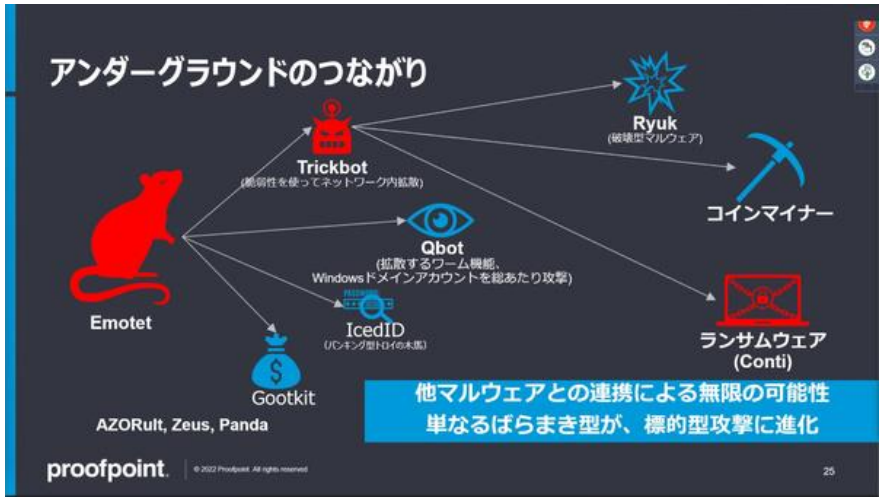
標的にされないためのセキュリティ対策を

ウイルスやランサムウェアといったサイバー犯罪を起こす組織は互いに繋がり、情報を共有しあっています。「セキュリティが弱い企業」という情報は「標的リスト」として共有され、複数の犯罪組織からの攻撃対象になる可能性が高まります。

基本的なセキュリティ対策を行い「セキュリティの強い企業」になることは、犯罪組織から「標的」とされにくくなる「予防策」にもなっていると言えるでしょう。

行うべきは、まだ標的となっていない「今」、対策を始めることです。14ページに掲載したガイドラインは、その対策として基本から役立ちます。ぜひセキュリティを今一度見直していただければと思います。

その上で、もし時間が取れない、自分たちだけでは対応が難しい、とのことであれば、弊社からも「CheckPoint」というソリューションをご提案しております。**お気軽にご相談・お問い合わせくださいませ。**



画像引用：https://ascii.jp/elem/000/004/121/4121172/
なぜEmotetの脅威を軽視すべきでないのか―ランサムウェア犯罪グループの実像を知る

「CheckPoint」の詳しいご説明・ご相談は
下記のボタンよりご連絡くださいませ。

ご相談はこちらから »

Branding
Technology

www.branding-t.co.jp