ダイチ通信
今こそ知りたい
＼テクノロジーTips！／
vol.6

最新のセキュリティトレンドをご紹介！

広がり続ける脅威を正しく把握し、セキュリティレベルの向上に繋げましょう！

＼ まずは概要を押さえましょう！ ／

昨今の感染症流行の影響で企業や組織は就労環境の変化を余儀なくされました。当初は大きな混乱があったものの、在宅勤務やハイブリッド勤務が広く浸透してきました。
場所や時間にとらわれず、自由な働き方を可能にする、というプラスの側面が注目されることもありますが、セキュリティ的には攻撃者の攻撃対象領域が拡大することを意味し、一層の注意が必要であると言えます。

TOPICS

トレンドマイクロ社の調査によれば、不正ファイルの検出件数は2020年上半期には10億強程度であったのに対し、2022年半ばには220億強にまで増加し、これにはリモートワークへの移行といった業務体制の変化も影響していると推測されています。ランサムウェア攻撃についてもRaaS（サービスとしてのランサムウェア）を背景として、拡大傾向が見られ、ランサムウェア攻撃への対策も企業や組織にとっての喫緊の課題です。
特に、Linuxシステムはランサムウェアの主要な標的となる可能性が指摘されており、実際に、トレンドマイクロ社によれば2021年上半期との比較で、2022年上半期はLinuxベースの端末を標的としたランサムウェア攻撃は75%増となっています。

攻撃の拡大、巧妙化もさることながら、ユーザー側の脆弱性にも目を向ける必要があるでしょう。
脆弱性の公開件数も増加傾向を示し、さらにはそれらの脆弱性の多くが深刻なものとされています。確実なアップデートを実施することで脆弱性を突いた攻撃のリスクを低減することができますし、前提としてのセキュリティ教育も非常に重要な対策であると言えます。
既にお分かりの通り、セキュリティ脅威は日々進化し、拡大しています。攻撃者は絶え間なく攻撃の機会をうかがい、隙があればすぐに攻撃を仕掛けてきます。
世の中の多くの人々が関心を持つ話題に便乗することもあるそうです。
物理的な対策はもちろんのこと、常に、どこでも脅威に晒されているという意識を持つことも大切です。

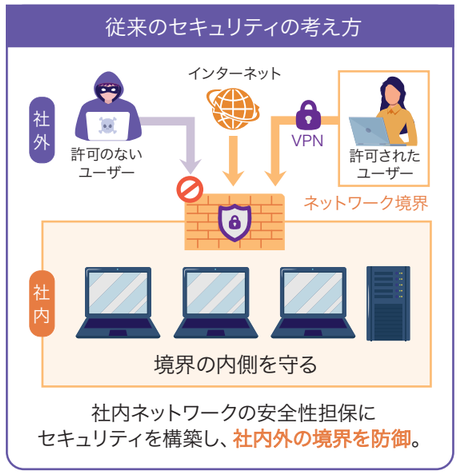
＼ ゼロトラストとは？ ／

先ほど、リモートワークについても述べましたが、
これに関連して「ゼロトラスト」という考え方があります。

ゼロトラストとは・・・・・

Trust（トラスト）は「信頼する」という意味を持ち、
これが「ゼロ」ですから、「すべて信頼しない」ということになります。

ゼロトラストネットワークとは、どういったものなのか、少し見てみましょう。
ゼロトラストはしばしば、従来の「境界型セキュリティ」と対比されます。
境界型セキュリティとは、保護すべき対象が社内ネットワークにのみ存在することを前提として、ネットワークの内と外という境界を設定し、その境界線上にセキュリティ機器を配置するというものでした。
しかしながら、リモートワークやモバイル機器の普及に伴い、境界線の設定自体が不可能となりました。
つまり、保護すべきデータがあらゆる場所に点在するようになったわけです。そういった状況の中で、すべての通信は信用できない、安全な場所など存在しないという「ゼロトラスト」の考え方が注目を集めるようになってきました。

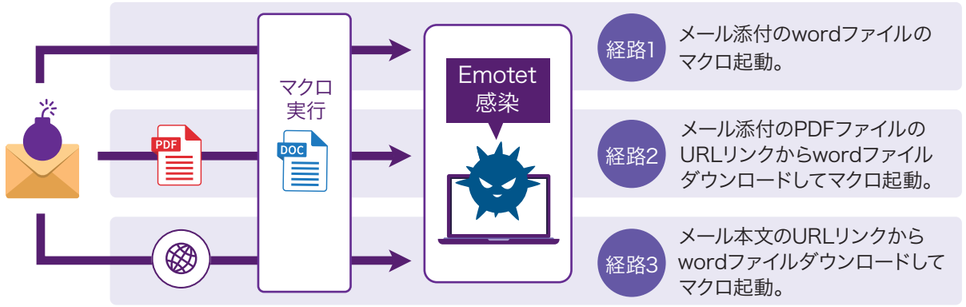


ゼロトラストセキュリティのメリットとしては、セキュリティレベルの向上が挙げられる他、セキュリティに関する設定をクラウドで一元管理できることによる管理効率の向上や社外からのアクセスが従来よりも容易になるといった点も挙げられます。

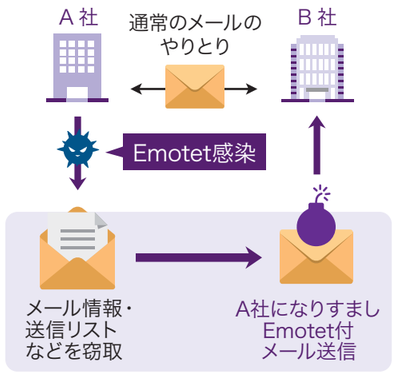
＼ 2022年再燃の脅威！Emotet ／

Emotetとは・・・・・

Emotetは、2014年に発見されたマルウェアの一種です2020年1月頃まで被害が拡大し、その後沈静化されたのですが、2021年11月に活動を再開しました。
関連モジュールを合わせたEmotetの国内総検出台数は2022年第一四半期に過去最高を記録し、国別では日本が最多であったそうです。



Emotetはメール経由で拡散するマルウェアであり、攻撃メールに添付されたファイルを通してEmotetに感染してしまうと、端末に登録されている関係者や取引先のアドレス宛にスパムメールが送信され、感染が急拡大します。
感染による被害としては、感染端末からの個人情報や認証情報の漏えい、社内外への感染拡大とそれに伴う信用失墜など様々です。
また、Emotetはマルウェア媒介機能を有し、攻撃基盤となり得るためEmotetに感染することによって、あらゆる種類のマルウェアに感染するリスクが著しく増大します。



攻撃メールの類型としては、例えば、関係者宛に送信したメールの返信を装った「返信メール型」が挙げられます。差出人や宛先、メールタイトルが偽装されており、過去のやり取りを想起させる情報等によって、誤信してしまうことが多々あるようです。
添付される不正なファイルは zip の他、直接 Word や Excel が添付されることもあれば、リンクをクリックすることによって不正ファイルがダウンロードされるケースもあります。
また、時事的な内容や季節の挨拶を装ったメールで、ファイルを開くように誘導する類型もあり、注意が求められます。

Emotetの対策について

覚えのないメールに添付されたファイルやURLを開かない。

対策としては、まずは覚えのないメールに添付されたファイルやURLを開かない、ということが一番です。常に警戒心を持ち、少しでも不自然な点があれば、送信元に確認しましょう。疑わしいファイルを開いてしまった場合は、マクロを有効化しないことで一定程度の感染予防が期待できます。ただし、有効化の手順を踏まず、ファイルの実行のみで感染してしまう場合があることは理解しておく必要があります。また、OSやアプリケーション、セキュリティソフトを最新の状態に保っておくことは、Emotet対策のみならずセキュリティ全般において重要なことです。
これらの対策をしっかりと実践するための前提として、情報ガイドラインの作成やセキュリティ教育の実施、こまめな注意喚起等が必要になるでしょう。

＼ どんな企業も標的に ／

組織間の業務上のつながりを悪用して行われる攻撃に「サプライチェーン攻撃」があり、近年注目されています。

TOPICS

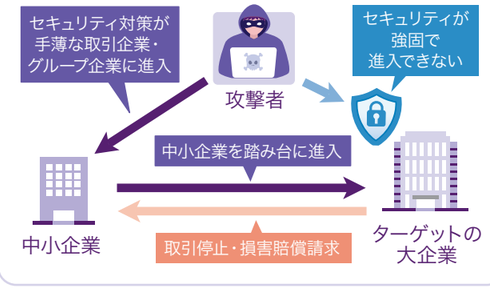
情報処理推進機構が公開した「情報セキュリティ10大脅威2022」では「サプライチェーンの弱点を悪用した攻撃」が、2021年よりも順位を1つ上げて3位にランクインしました。

サイバー攻撃は大企業をターゲットとして行われるものと考えてしまいがちなのですが、実はこのサプライチェーン攻撃は中小企業こそが警戒しなくてはなりません。最終的なターゲットである大企業に侵入するための経由ターゲット（踏み台）として中小企業が狙われるためです。大企業はセキュリティ対策に費やすコストや人員も多く、不正侵入が困難であると考える攻撃者は、セキュリティ対策が手薄な中小企業を狙って攻撃を仕掛けます。

攻撃者が最終的なターゲットまで到達してしまった場合、踏み台となった会社の経営規模を超えるような莫大な被害をもたら可能性が高く、だからこそ、規模の大小に関わらず、セキュリティ対策を徹底する必要があるのです。

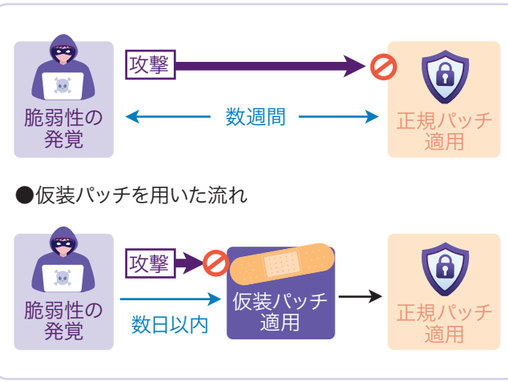
まずは、侵入させない、万が一侵入を許したとしても、ネットワークにおける挙動監視等、内部活動の迅速な可視化によって早期に対応できる体制の構築が必要です。

●サプライチェーン攻撃の仕組み



＼ 仮想パッチとは？ ／

仮想パッチとは、本来のセキュリティパッチがすぐに適用できない場合の暫定的なセキュリティ担保として利用されるソリューションであり、ネットワーク外から脆弱性を突いて攻撃してくるパケットを検知、遮断する仕組みになっています。
ただし、あくまで「暫定的な」脆弱性対策に過ぎません。仮想パッチを使っても脆弱性は残ったままであり、脆弱性を根本的に解決するためには、仮想パッチではなくベンダーから配布される修正パッチを適用しなくてはなりません。



お客様のセキュリティ向上に伴走いたします！
まるっと当社にご相談ください！

Daichi SYSTEM 株式会社 ダイチシステム
〒103-0005 東京都中央区日本橋久松町 12-4
TEL：03-5652-9855　FAX：03-5652-9856
E-mail：info@daichisystem.co.jp
URL https://www.daichisystem.co.jp