CHECK POINT

セキュリティレポート

サプライチェーンにおけるインシデント事例と対策

Check Point SMB

2024.4.1

YOU DESERVE THE BEST SECURITY

Objective

- サプライチェーンとは
- 一般的なサプライチェーンのインシデント事例
- サプライチェーンにおけるインシデント事例
- サプライチェーン攻撃増加の背景
- サプライチェーンとランサムウェア
- ランサムウェア攻撃を受けやすい業種とその特徴
- ランサムウェア攻撃対策（自社内）

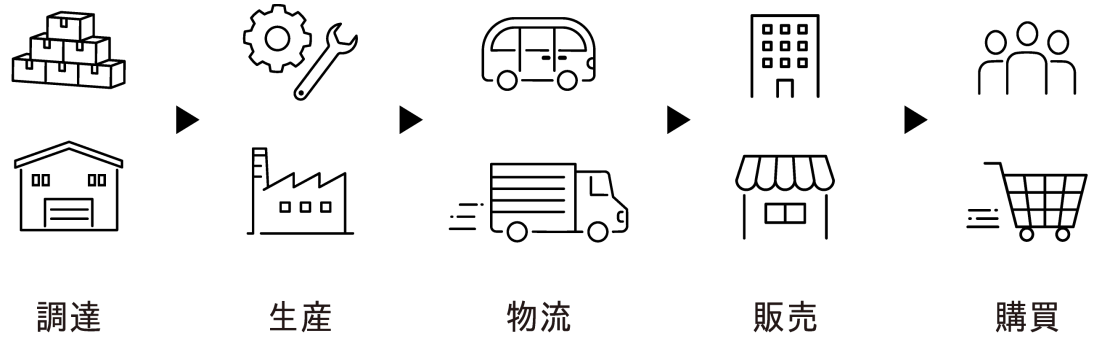
サプライチェーンインシデント事例

サプライチェーンとは

サプライチェーン（Supply Chain）とは、製品やサービスの提供に必要な資源や情報が、原材料の供給元から製造、流通、販売、最終消費者に至るまでの一連の流れやプロセスを指します。

たとえば自社がメーカーである場合、部品メーカーや原材料メーカーなどから製品の製造に利用する部品および原材料を仕入れて製造します。また販売においては、配送業者や卸業者、そして小売業者が関係します。このように、サプライチェーンでは自社の業務だけでなく、モノが製造され販売されるまでのフロー全体を捉えます。

サプライチェーンは、効率的な生産、効果的な流通、顧客満足度の向上などの目標を達成するために重要です。また、競争力の向上やリスク管理の観点からも、サプライチェーンの効率性や信頼性が重要視されます。

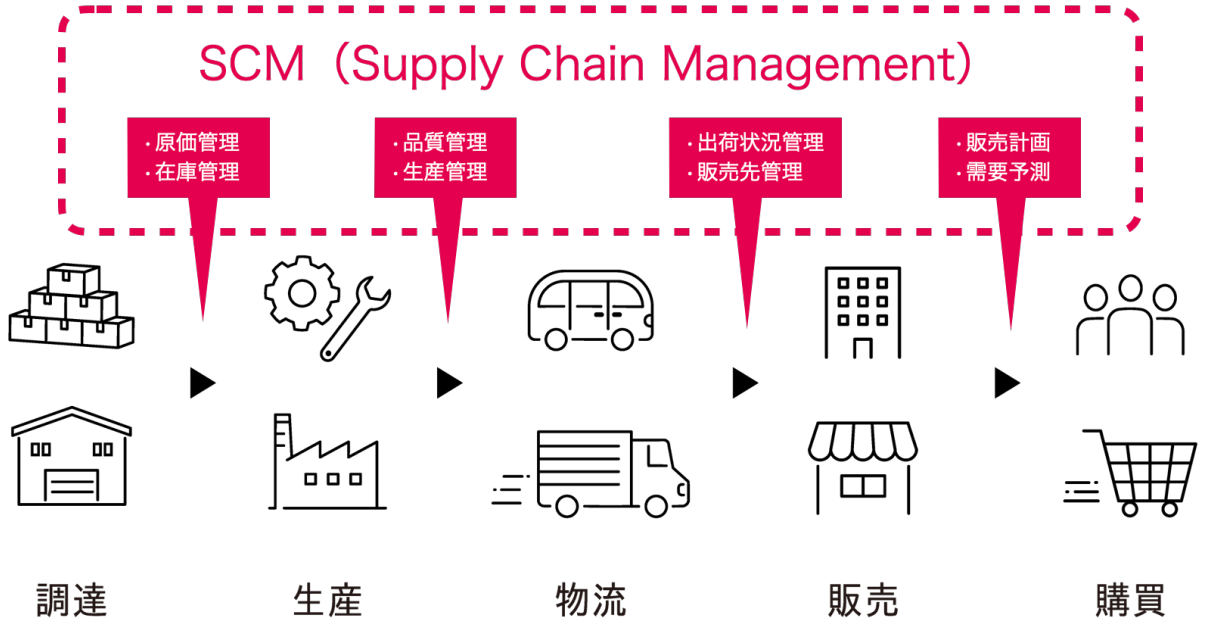


SCM（Supply Chain Management）

サプライチェーンにおいて、製品やサービスの生産・供給プロセスを効率的に管理し最適化しなければなりません。

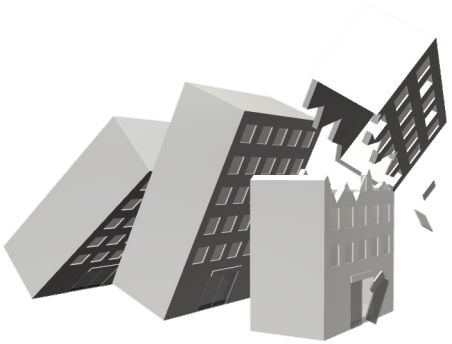
例をあげると、部品・原材料メーカーや卸売業者、販売店などを含めて在庫状況を把握、適正化を図ったりします。

この最適化を実現するためにSCM（Supply Chain Management、サプライチェーン管理）と呼ばれるシステムを導入している企業も少なくありません。



サプライチェーンにおけるインシデント事例（サイバーに関わらず一般的な例）

サプライヤーのデータ漏洩	主要なサプライヤーがハッキングやデータ漏洩に遭った場合、その情報が顧客や取引先企業の機密情報を含む可能性があります。このようなインシデントは、サプライヤーと取引先企業の両方に影響を及ぼす可能性があります。**（取引停止・損害賠償）**
サプライヤーのサービス中断	サプライヤーのシステムやインフラが攻撃や技術的な問題によって中断された場合、取引先企業は製品の生産やサービスの提供に支障をきたす可能性があります。特に、重要な部品や資材を供給するサプライヤーの場合、影響は深刻です。
サプライヤーの不正活動	サプライヤーが不正な活動や違法行為に関与していた場合、取引先企業はその行動によって信頼を失う可能性があります。例えば、賄賂や汚職、知的財産権の侵害などが挙げられます。**（取引停止・損害賠償）**
物流の問題	サプライヤーの物流や運送に問題が発生した場合、製品の供給や配送に遅延が生じる可能性があります。天候の影響、交通インフラの障害、ストライキ、不測の事故などが原因となることがあります。
サプライヤーの破産	サプライヤーが経済的な困難に直面し、破産や倒産を経験した場合、取引先企業は製品やサービスの供給に関する問題に直面する可能性があります。これにより、生産ラインの停止や製品の品質に関するリスクが生じる可能性があります。



サプライヤーが原因で起こった、代表的なサプライチェーンにおけるサイバーインシデント事例①

LINEヤフーが受けたサプライチェーン攻撃

2023年11月にLINEヤフーがサイバー攻撃を受け、LINEの利用者情報など40万件以上の個人情報が流出した可能性があるインシデントは記憶に新しいと思います。

これは関係会社である韓国NAVER Cloudの委託先かつLINEヤフーの委託先でもある企業の従業者が所持するPCがマルウェアに感染したことが原因とされたサプライチェーン攻撃でした。

海外の宿泊予約サービスがサプライチェーン攻撃を受けた事例

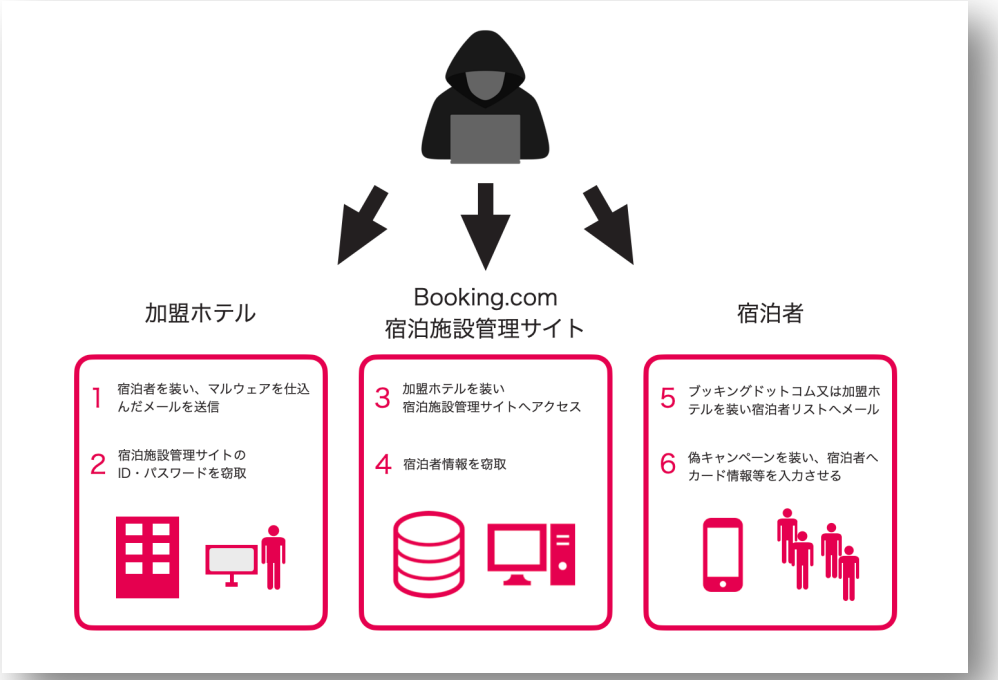
2023年11月には、世界最大級の宿泊予約サービス「ブッキング・ドットコム」にて、宿泊施設の予約を行ったユーザーの個人情報が大量に流出するというインシデントが発生しました。

このケースでも、まず攻撃者は同サービスに登録しているホテルにへ旅行者を装ってフィッシングメールを送り付けてマルウェアに感染させます。

ホテル内システムへ侵入した後、ホテル担当者がブッキング・ドットコムにアクセスする際に利用するアカウント情報（ID：パスワード）を窃取。攻撃者は手にした認証情報を利用してブッキング・ドットコムに対して不正アクセスを実施。

先ほどのLINEの事例と同様、正規のアカウント情報を使っているため、アクセスを受けた側は「それが不正なものかどうか」を容易に判別できず、対応も遅れ、被害の拡大を防げませんでした。

攻撃者はブッキング・ドットコムのシステムを悪用し、ホテル予約者にブッキング・ドットコムを騙ったフィッシングメールを送付。予約者はその不正サイトを通じてクレジットカード情報を含む個人情報を入力し、攻撃者は多くの予約者の個人情報をを窃取することに成功したと言われています。



国内のサプライチェーン攻撃事例としてトヨタ自動車が代表的ですが、上記事例ふまえ大手企業が直接攻撃されずサプライチェーンの中でも比較的サイバーセキュリティ対策が整っていない中小零細企業がターゲットにされやすいことが傾向として大いにあります

サプライヤーが原因で起こった、代表的なサプライチェーンにおけるサイバーインシデント事例②

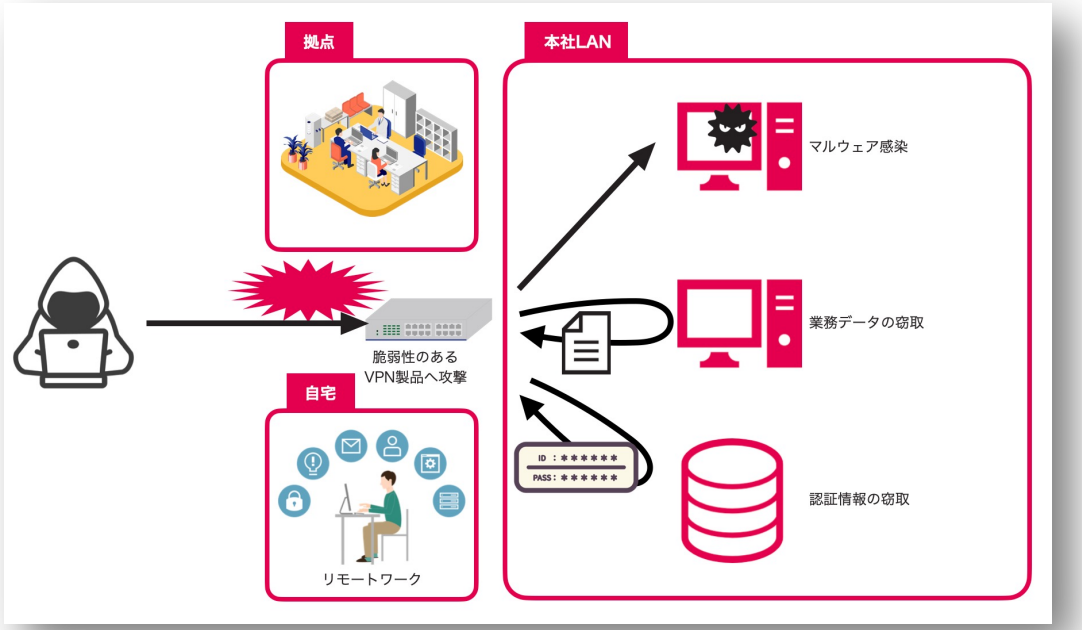
給食を提供するサプライチェーン企業から攻撃

ランサムウェアとみられるサイバー攻撃でシステム障害が起き、大阪急性期・総合医療センター（病床数800超え）の医療サービスが約2ケ月も停止しました。

電子カルテのデータが暗号化されただけでなく、病院システム全体に影響があり、2023年になりやっと復旧できました。サプライチェーン攻撃事例として、復旧までにかなりの時間のかかったケースでした。

給食を委託する給食サプライチェーン企業経由で病院システムに侵入されたのが原因でした。このケースも給食サプライチェーン企業のリモート接続機器の脆弱性を突かれ、ネットワークに侵入された事例と考えられます。

病院への給食は単なるお弁当を届けるだけでありません。患者様のアレルギー対応や健康状態に配慮した食事を提供するために、きめ細かなレシピ等のデータベースと連携しています。密接に病院と接続する給食システムの、ネットワークの脆弱性から攻撃された事例です。



一般的なVPN製品等の脆弱性を狙った攻撃例

サプライチェーン攻撃増加の背景

情報窃取・身代金の要求

情報漏えい時による企業へのダメージ、身代金の要求など、攻撃者にとっての攻撃メリットは総じて高まっています。

そのため、手間をかけてでも攻撃する価値がある対象として狙われると、標的型攻撃が成功するまで執拗に攻撃が繰り返されます。

特に、個人情報を大量に保有していたり、重要な資料、ノウハウなど、機密レベルが高い情報を有している企業は、攻撃者にとってサプライチェーン攻撃を用いてでも攻撃する価値があると言えます。

セキュリティ対策の格差

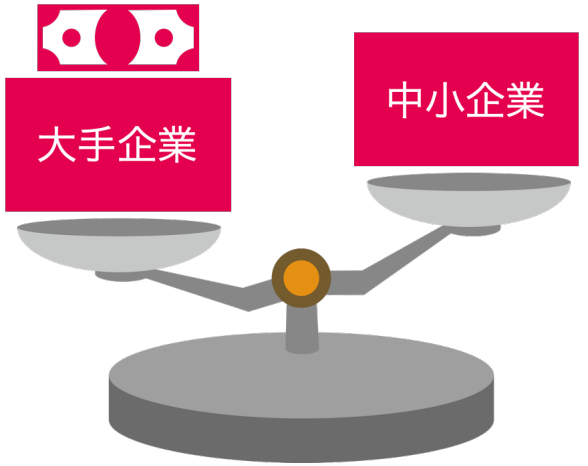
企業におけるセキュリティ対策関連への投資が増加していることもあって、国内の情報セキュリティ市場は年々拡大する一方にあります。

また、コロナ禍以降急速に普及が進むリモートワークにおいて、万全のセキュリティ対策を講じる必要性があることも関係していると言えます。

ただし、経営に余力がある大企業ではこうした対策が進む一方、中小・零細企業では予算や人材の確保などの制約が伴う場合が多く見受けられます。

加えて、経営陣による自社に『重要な情報資産が存在しない』との認識から、セキュリティ対策を怠るケースもあります。

そのため攻撃者視点から、サプライチェーン攻撃によって情報セキュリティ対策が脆弱な中小・零細企業を狙うのは合理的とも言えます。

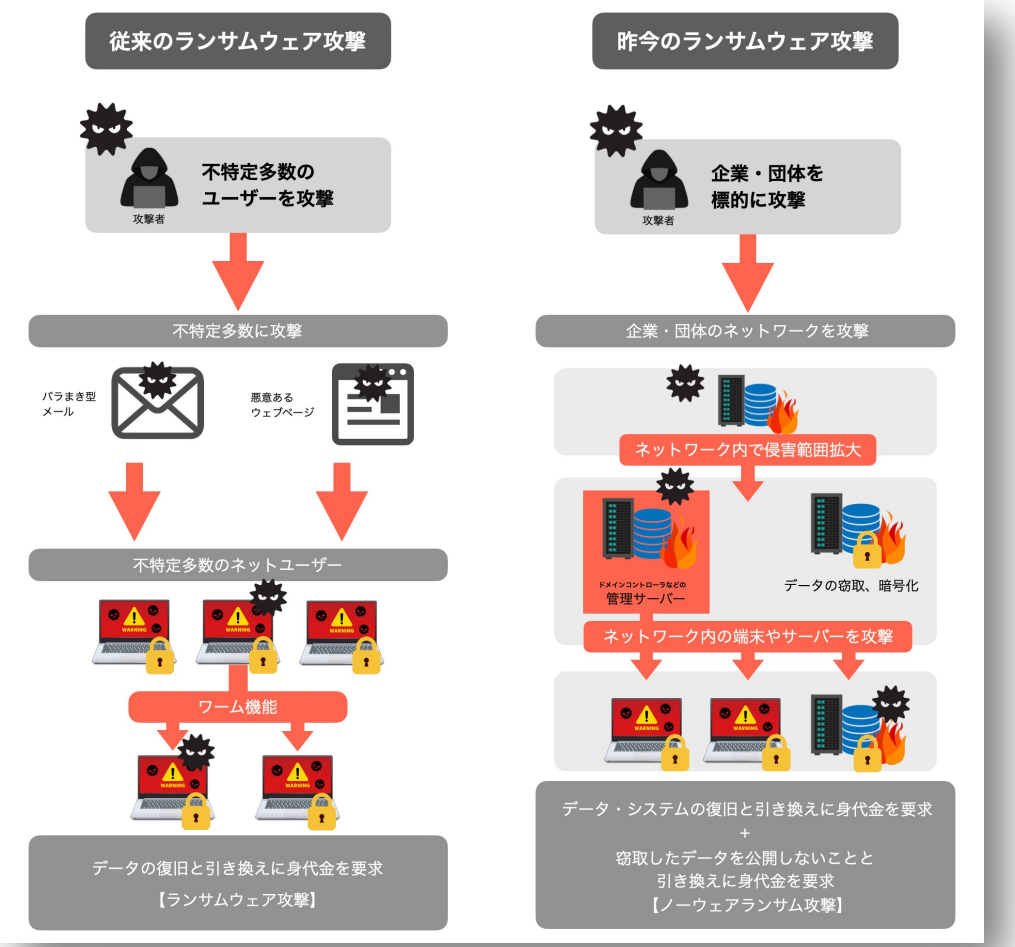


サプライチェーンとランサムウェア

企業や組織に対する攻撃のうち、サプライヤーであるパートナーやサービスプロバイダーを起点としたものが現在増えています。

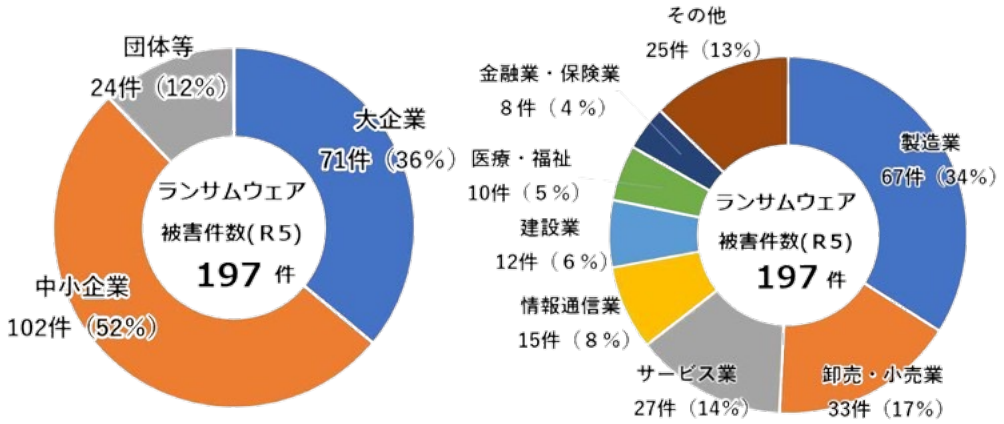
その理由として、攻撃者は1つの企業への攻撃が他のすべての企業への攻撃へとつながるよう、「芋づる式」の攻撃を仕掛けるための脆弱性を探しているからです。

また、サプライチェーン攻撃は、大部分がランサムウェア攻撃であり、特定のサプライチェーンを標的に攻撃を実施します。



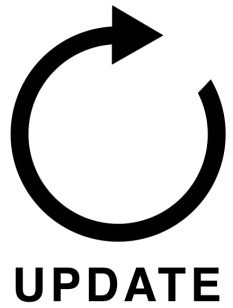
ランサムウェア攻撃を受けやすい業種とその特徴

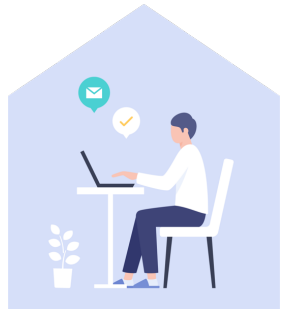
ランサムウェア攻撃を受けやすい業種



ランサムウェア感染しやすい企業の特徴

セキュリティ意識の低さ	従業員や管理層のセキュリティ意識が低い企業は、ランサムウェア攻撃に対する防御が不十分な場合があります。社員が悪意のあるリンクをクリックしたり、添付ファイルを開いたりするリスクが高まります。
セキュリティ対策の不足	アンチウイルスソフトウェアやファイアウォールなどのセキュリティ対策が不十分な企業は、悪意のあるソフトウェアからの保護が不十分であり、ランサムウェア感染のリスクが高まります。
アップデートの遅れ	重要なセキュリティパッチやソフトウェアの更新が遅れている企業は、既知の脆弱性を悪用した攻撃に対して脆弱になります。攻撃者は、古いソフトウェアや未修正の脆弱性を標的にすることがあります。
リモートアクセスの利用	リモートワークや遠隔地からのアクセスが必要な企業は、リモートアクセス用のセキュリティ対策が不十分な場合、攻撃者にとって容易な標的となります。攻撃者は、リモートアクセスを介して企業のネットワークに侵入し、ランサムウェアを広めることができます。





ランサムウェア攻撃対策（自社内）

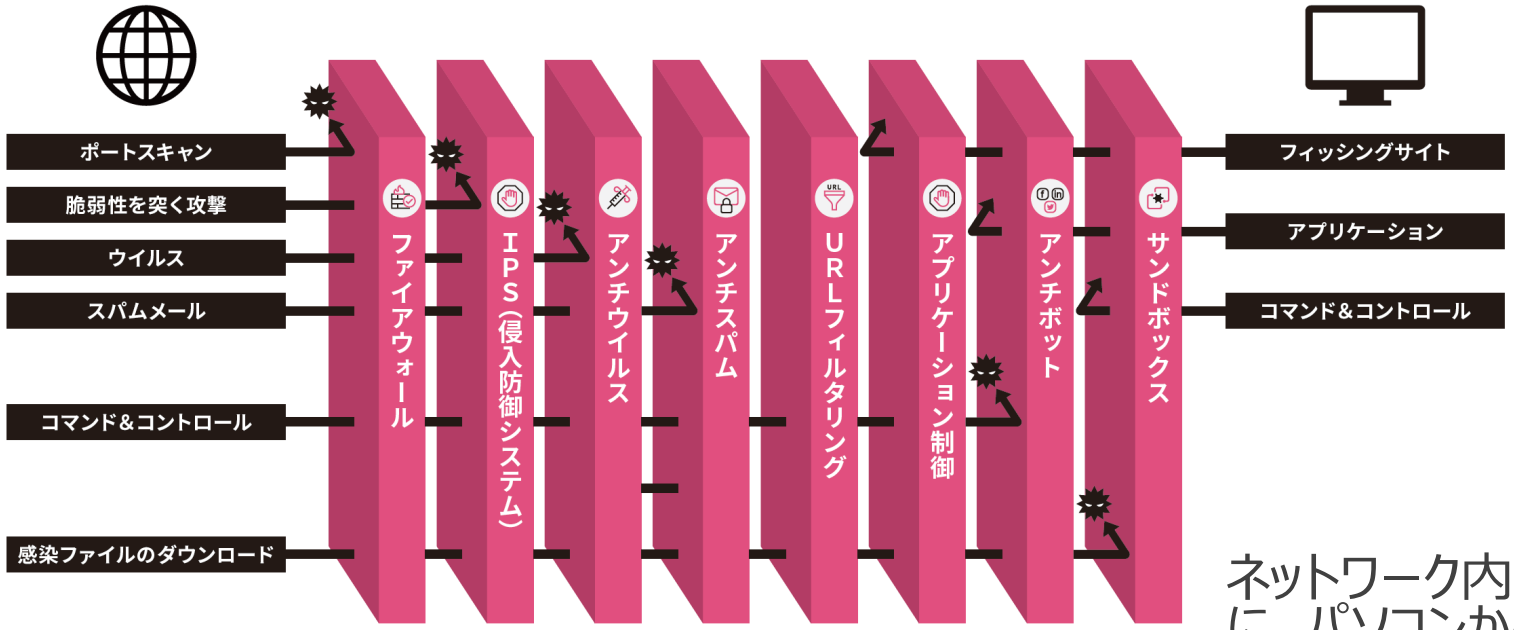
身近に実施出来る対策

1. OSやソフトウェアは常に最新の状態にする。脆弱性は、ソフトウェアを更新して根本的に解消する
2. ウイルス対策ソフトの導入。流行しているウイルスの感染を未然に防ぐ
3. パスワードを強化する。 パスワードは「長く」「複雑に」「使いまわさない」
4. 共有設定を見直す。無関係な人に情報を覗き見られるトラブルを回避
5. 脅威や攻撃の手口を知る。新聞やインターネット等から情報を収集し、被害に遭わないよう手口を事前に知る。

Check Point ソリューションで対策

オールインワンアプライアンス

複雑なサイバー攻撃を防ぐために必要な機能が1筐体に集約されたUTM！
（統合脅威管理：Unified Threat Management）



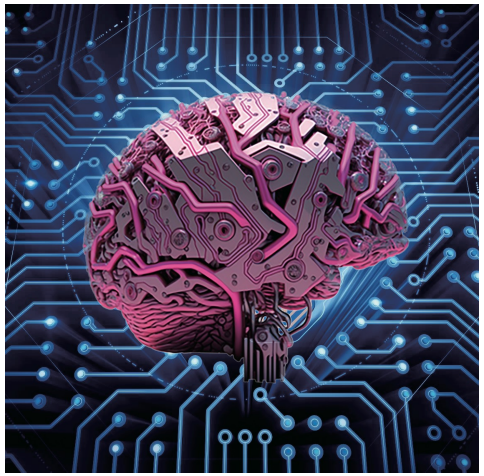
ネットワーク内にある、パソコンをUTMでブロックするとともに、パソコンからC＆C等へのアクセスを遮断します。

外部からの脅威と内部から実施するアクセスを

オールインワンで保護。

あらゆる脅威からの保護

様々なセキュリティ機能に関する脅威対策エンジン



THREATCLOUD

感染ホスト検出
サンドボックス静的解析
サンドボックス動的解析
メール静的解析
フィッシング対策AIエンジン
ネットワークAIエンジンアグリゲータ　などなど

◆世界中の約15万のセキュリティ・ゲートウェイを通過するトラフィックから日々脅威情報を収集
◆脅威情報を防御可能な情報に活用
◆リアルタイムに防御情報をアップデート

容易な導入と管理

クラウド管理によって導入から運用フェーズまでのコスト削減を実現

簡単デプロイ

- ✓ 事前定義された設定ウィザードにより数分でのセットアップが可能

モバイル・クラウド管理

- ✓ クラウドからの一括管理・設定変更が可能なため、保守運用のアウトソースが可能
- ✓ モバイル管理にも対応、インシデントをリアルタイムに確認可能

セキュリティレポート

- ✓ シンプルで直感的なレポートを標準で提供
- ✓ 通信量や検出したセキュリティ脅威等の情報を確認可能

Check Point1500Proシリーズラインナップ

10名規模の企業から400名まで幅広くサポート可能！

	1535	1555	1575	1595	1600	1800
参考ユーザー数 (NGTX全て有効時)	20	50	100	200	300	400
NGTX スループット ※エンタープライズトラフィック ※スマートアクセル有効	440Mbps	600Mbps	650Mbps	900Mbps	2.0Gbps	2.6Gbps
ファイアーウォール スループット ※試験環境トラフィック	1.5Gbps	2.0Gbps	4.8Gbps	6.4Gbps	8Gbps	17Gbps

※NGTX：サンドボックス含む全てのセキュリティ機能を有効にした状態

差別化ポイント！他社のUTMスループットは理想環境でセキュリティ機能を全て有効にしていない数値の場合が多いですが、チェック・ポイントのスループットは全てのセキュリティ機能を実環境で有効にした数値です

CHECK POINT

Thank You!

YOU DESERVE THE BEST SECURITY