執拗な標的型攻撃のサイクルの全過程に渡り対処する攻撃前（Before）、攻撃中（During）、攻撃後（After）

今こそ新たなセキュリティモデルが求められる時

現在の脅威の状況は、10 年前とは全く異なります。ダメージを封じ込めることができた単純な攻撃はもう過去のものです。今日の脅威は、巧妙化し、豊富な資金に支えられて、企業や国家の基盤に大規模な混乱を引き起こす近代的なサイバー犯罪活動です。これら高度な攻撃は検出が難しいだけでなく、長期間ネットワークに潜伏し、どこか別の場所に攻撃を仕掛けることを目的としてネットワーク リソースの情報を収集します。

今や、検出とブロッキングのみに頼る従来の防御策では対処しきれなくなっています。ここで必要となるのが、攻撃前、攻撃中、攻撃後と、攻撃サイクル全体に対処する新しいセキュリティ モデルです。

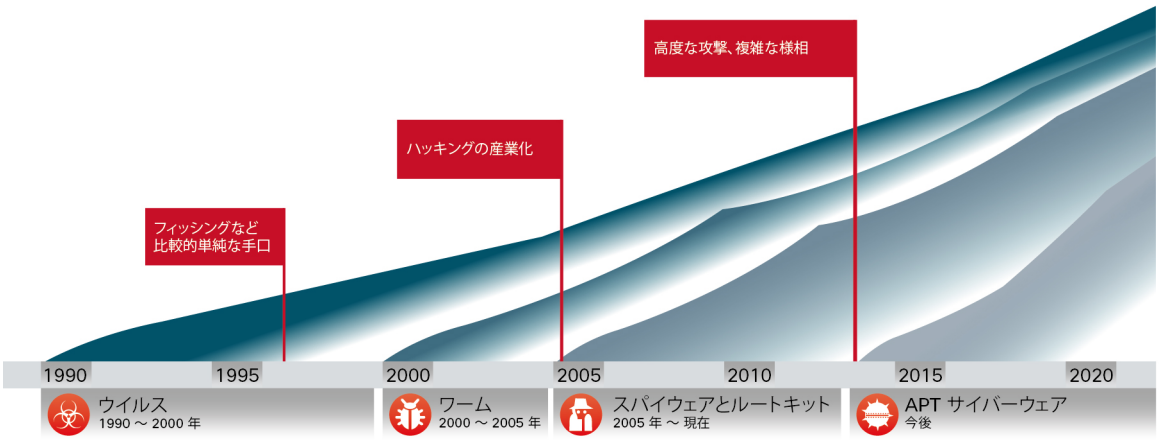
ハッキングの産業化

最初の PC ウィルスが登場したのは 25 年以上も前のことです。当時は、これがハッキングの産業化の序章になるとはだれも想像できませんでした。

ウィルスは、その後約 10 年にわたり、攻撃の主要な手段として使用されてきました。その間、防御者の側でも、ブロックや保護の能力を高め、ウィルスに対抗できるようになりました。名声を得たいという欲求と、新たに発見/公表される脆弱性の情報に突き動かされ、攻撃者たちは攻撃のスキルを磨き続けてきました。その結果として生まれたのが、脅威のサイクル、つまり「軍備拡大競争」でした。攻撃者は約 5 年ごとに、マクロウィルス、ワーム、スパイウェア、ルートキットなど、新しいタイプの脅威を仕掛け、それに対抗する防御側といたちごっこを繰り広げています。

これらのサイクルが大きな技術的転換点と一致し、新たな攻撃のベクトルを生み出してきたことは、驚くべきことではありません（図 1 を参照）。初期のウィルスは主に、オペレーティング システムを標的とし、「スニーカー ネット」を通して広がりました。また、マクロ ウィルスはユーザ間のファイル共有を利用していました。マシンからマシンに移動するワームタイプの脅威は、企業ネットワークや、当時増加傾向にあったインターネットの利用を悪用していました。さらに、新しいアプリケーション、デバイス、オンライン コミュニティなどと共に現れたのがスパイウェアやルートキットでした。今日、私たちが直面しているのは、高度なマルウェア、標的型攻撃、および Advanced Persistent Threat（APT）です。新しい脅威は、攻撃者の動機とツールの点で、これまでとは大きく異なり、攻撃の検出、理解、停止がきわめて難しくなっています。

図 1. ハッキングの産業化



ハッキングの産業化により、企業の IT インフラストラクチャに攻撃を仕掛け、犯罪者が短時間で効果的、かつ効率的に利益を上げられる違法なビジネス環境が生まれています。組織化された侵入手口の情報交換が活発化し、利益を生むようになりました。また、オープンな市場の環境によって、単なる情報の不正使用から、盗用、妨害、破壊行為へと深刻度が増しています。莫大な利益を上げる可能性に気付いたサイバー犯罪者は、標準化と自動化を進めたプロセス駆動型の攻撃手法を開発しています。攻撃者は、クラシックなセキュリティ テクノロジーの静的な性質や、それらが一貫性なく導入されることを理解しているため、そのギャップや脆弱性を悪用できます。また、ハッカー グループの間では、ソフトウェア開発プロセスさながらに、品質保証検査や、セキュリティ テクノロジーに対するベンチテストなども広く行われています。これに合格し、一般的な保護対策をすり抜けられることが確認できてから、実際に使用されるのです。

今日では、秘密性に多額の報酬が支払われるため、多くの「Hactivist（ハクティビスト）」グループは、懲罰や起訴の恐れがほとんどない状態で、経済的または政治的影響を及ぼす攻撃を仕掛けています。ポート ホッピング、プロトコル ホッピング、暗号化トンネリング、ドロッパー、ソーシャル エンジニアリングやゼロデイ攻撃を利用した複合脅威/テクニックなどの新しい方法により、ハッカーはより簡単、迅速、低コストで侵入することが可能になった一方、防御側による検出と締め出しはますます難しくなっています。また、攻撃自体が、企業のシステム内で侵入の足場を探しながら機密データを盗み出すまでの間に、その姿を素早く変化させることができるため、検出は一層困難になります。

Any-to-Any の課題

今日の広範なネットワーク環境とそのコンポーネントは、絶えず進化を続けています。そのため、新たな攻撃ベクトルも次々に生まれています。これらには、モバイル デバイス、Web 対応のモバイル アプリケーション、ハイパーバイザ、ソーシャル メディア、Web ブラウザ、組み込みコンピュータのほか、Internet of Everything によってもたらされる、数多くのデバイスやサービスが含まれます。それらの利用者は、ネットワークの内側にも外側にもいます。あらゆるデバイスから、あらゆるアプリケーションにアクセスします。また、さまざまなクラウドを利用します。この遍在性こそが「Any-to-Any」の課題です。この動的な状況はコミュニケーション力を強化しますが、同時にハッカーが付け入るエントリ ポイントや手段が増えることにもなります。残念なことに、セキュリティに対する多くの組織のアプローチは、足並みがそろっていないのが現状です。

大部分の組織では、連携していない、また連携させたくてもできないばらばらのテクノロジーで広範なネットワークを保護しています。また、クラウドのセキュリティやインターネット インフラストラクチャの保護を、それぞれサービス プロバイダーやホスティング会社に頼りすぎているところもあります。こうした中、セキュリティ管理者は一般に、社内ネットワークにアクセスするデバイスやアプリケーションをほとんど把握も管理もできない状況であり、新たな脅威に対応することも困難なのが現状です。

新しいセキュリティのダイナミクス

高度な攻撃の脅威と Any-to-Any インフラストラクチャという現実に直面しながら、セキュリティ プロフェッショナルは次の 3 つの問いを自問しています。

1. *新しいビジネス モデルと新しい攻撃ベクトルが登場した今、変化を続ける IT 環境において、セキュリティとコンプライアンスをどのように維持していくか?* 生産性、俊敏性、効率性を求めてクラウド、仮想化、モバイル デバイスに移行している組織は、それぞれのセキュリティ インフラストラクチャをそれらのテクノロジーに合わせる必要があります。
2. *脅威をめぐる環境が変化する中、新しい攻撃ベクトルやますます巧妙化する脅威に対抗し続けるため、どのように能力を高めればよいか?* 攻撃者はえり好みをしません。脆弱な部分を見つけたらすぐに攻撃を開始します。多くの場合、狙いを付けた標的のセキュリティ インフラストラクチャに合わせて開発したツールを使い、容赦ない攻撃を執拗に行います。痕跡をほとんど残さないテクノロジーや手法を使い、検出されないために多大な努力を払います。
3. *最初の 2 つの問いに対処すると同時に、セキュリティ ソリューションの複雑化と細分化を避けるにはどうすればよいか?* 保護対策に穴があっては、現在の高度な技術を持つ攻撃者にはすぐに付け入られてしまいます。同時に、統合されていないばらばらのセキュリティ ソリューションを使用することで複雑さが増せば、高度な脅威に対抗できる高いレベルの保護は不可能です。

> *「100 % の企業が、既知のマルウェアの脅威があるサイトのドメインに接続しています。」*
>
> – シスコ 2014 年次セキュリティ レポート

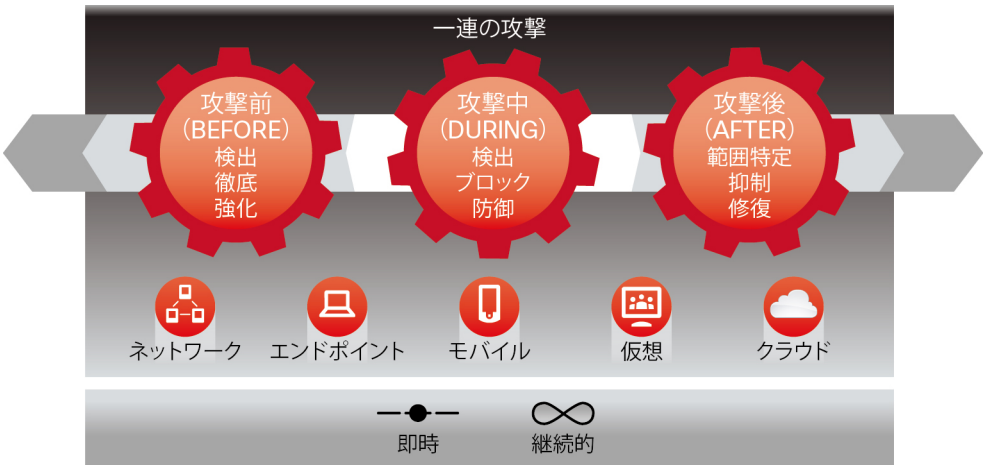
ビジネス モデルの変化、脅威をめぐる環境の変化、セキュリティの複雑化と細分化といった動きが重なることで、セキュリティには穴が生じ、セキュリティ ライフサイクルが破壊されると共に可視性が低下し、新たなセキュリティ管理の問題が増えます。これらの動きに直面しながら組織を確実に保護するには、セキュリティに対するアプローチを抜本的に変える必要があります。今こそ、脅威を中心に据えた新しいセキュリティ モデルが求められる時です。

執拗な標的型攻撃の攻撃前(Before)、攻撃中(During)、攻撃後(After)のサイクルの全過程に対処する

現在使われているセキュリティ ツールのほとんどは、マルウェアを侵入時点でネットワークの可視性を提供し、ブロックすることに焦点を置いています。これらのツールは、ファイルを最初に 1 度スキャンしただけで悪意のあるものかどうかを判断します。しかし、高度な攻撃はある時点だけで終わるものではありません。攻撃は次々と仕掛けられるため、注意して監視を続ける必要があります。現在の攻撃者は、初期の検出をかわすためにポート ホッピング、カプセル化、ゼロデイ攻撃、コマンド & コントロール(C&C)検出の回避、スリープ テクニック、Lateral Movement、トラフィックの暗号化、複合型の脅威、サンドボックス回避などさまざまな手段を講じています。ポイントインタイム方式の検出テクノロジーでは、見逃してしまったファイルが侵入後に進化して悪意のあるファイルになってしまえば、その後の攻撃者の行動の特定にはまったく役に立ちません。

セキュリティ対策は、検出だけに集中するのではなく、侵入後の攻撃者の攻撃も緩和できる必要があります。組織は、それぞれのセキュリティ モデル全体に目を向け、広範なネットワークと一連の執拗な攻撃、つまり、攻撃が生じる前、攻撃が行われている最中、システムがダメージを受けた後や情報を盗まれた後について把握し、制御できる必要があります(図 2)。

図 2. 新たなセキュリティ モデル



- **攻撃前**:防御側は、広範なネットワークの防御に必要なポリシーを定めて制御するために、ネットワークで起こっていることを総合的に理解して把握する必要があります。
- **攻撃中**:マルウェアを継続的に検出し、ブロックする能力が不可欠です。
- **攻撃後**:防御側には、攻撃の影響を抑えるためにレトロスペクティブ セキュリティが必要です。侵入経路や範囲を特定し、脅威を抑制して再度感染する危険を排除し、混乱を正す必要があります。

攻撃前

コンテキストを意識する攻撃者には、コンテキスト認識型のセキュリティで対抗する必要があります。攻撃者はしばしば、防御側が保護しようとしているインフラストラクチャについて、防御側よりも多くの情報を得ている場合があります。攻撃前の防御としては、組織が環境全体をしっかり把握する必要があります。つまり、物理ホストと仮想ホスト、オペレーティング システム、アプリケーション、サービス、プロトコル、ユーザ、コンテンツ、ネットワークの動作など(ただしこれらに限定されません)について理解し、攻撃者よりも多くの情報を得るよう努めてください。防御側は、標的の価値、攻撃の正当性、履歴に基づいて、インフラストラクチャに対するリスクを理解してください。保護する対象がわかっていなければ、セキュリティ テクノロジーをどのように構成して防御すればよいのかもわかりません。可視性においては、ネットワーク全体をカバーする必要があります。エンドポイント、E メールや Web のゲートウェイ、仮想環境とモバイル デバイス、さらにはデータセンターも対象になります。この可視性を通してアクションにつながる警告を生成し、防御側が十分な情報を得た上で判断できるようにする必要があります。

攻撃中

容赦ない攻撃はある時点だけで終わるものではありません。攻撃は次々と仕掛けられるため、継続したセキュリティが求められます。従来のセキュリティ テクノロジーが攻撃を検出できるのは、ある特定の時点のみであり、攻撃自身のデータの一点のみに基づくものです。このアプローチでは、高度な攻撃に太刀打ちできません。代わりに必要となるのは、認識(Awareness)という概念に基づいたセキュリティ インフラストラクチャです。この方法では、広範なネットワークでデータを収集して関連付けを行い、履歴データやグローバルな攻撃に関する情報を基に状況を明らかにし、アクティブな攻撃、盗難、偵察などと、単なるバックグラウンド ノイズとを区別することができます。これは、ある時点でのみ実行するセキュリティから、継続して分析と意思決定を行うセキュリティへの進化です。安全だと思い通過させたファイルが後になって悪意のある動作を引き起こすものでもそれが明らかになった時点で、組織は対策を取ることができます。このようなリアルタイムの洞察が得られることで、セキュリティ プロフェッショナルはインテリジェントな自動機能を利用して、手動による介入を必要とせず、セキュリティ ポリシーを適用することができます。

攻撃後

一連の執拗な攻撃に対応するには、レトロスペクティブ セキュリティが必要です。レトロスペクティブ セキュリティでは、ビッグデータが鍵となりますが、この機能を提供できる企業はほとんどありません。継続的にデータを収集および分析してセキュリティ インテリジェンスを構築できるインフラストラクチャを用いれば、セキュリティ チームは自動的に被害の痕跡を特定でき、検出を逃れるために動作を変える高度なマルウェアも検出し、問題を修復することができます。そのままでは数週間、または数ヵ月も検出されない被害を特定し、範囲を絞り込んで抑制および修復することができます。

この脅威を中心に据えた新しいセキュリティ モデルにより、組織はあらゆる攻撃ベクトルを対象として一連の執拗な攻撃に、いつでも、継続して、リアルタイムに対応できます。

新たなセキュリティ モデルの実現

シスコでは、新たなセキュリティ モデルを実現するために、現在のセキュリティ テクノロジーは 3 つの戦略的重要課題に注力する必要があると考えています。それは、Visibility-Driven、Threat-focused、Platform-based です。

Visibility-Driven：セキュリティ管理者は発生しているすべてのことを正確に把握できる必要があります。この機能は、広さと深さの両方が必要となります（図 3 を参照）。広さとは、ネットワーク ファブリック、エンドポイント、E メールと Web ゲートウェイ、モバイル デバイス、仮想環境、およびクラウドで想定されるすべての攻撃ベクトルのデータを調べて収集する機能であり、環境と脅威に関する知識が得られます。深さでは、これらの情報の関連付けを行い、コンテキストを理解するためにデータを適用し、より的確な判断を行う、手動または自動でアクションを実行する能力を提供します。

図 3. 広さと深さ

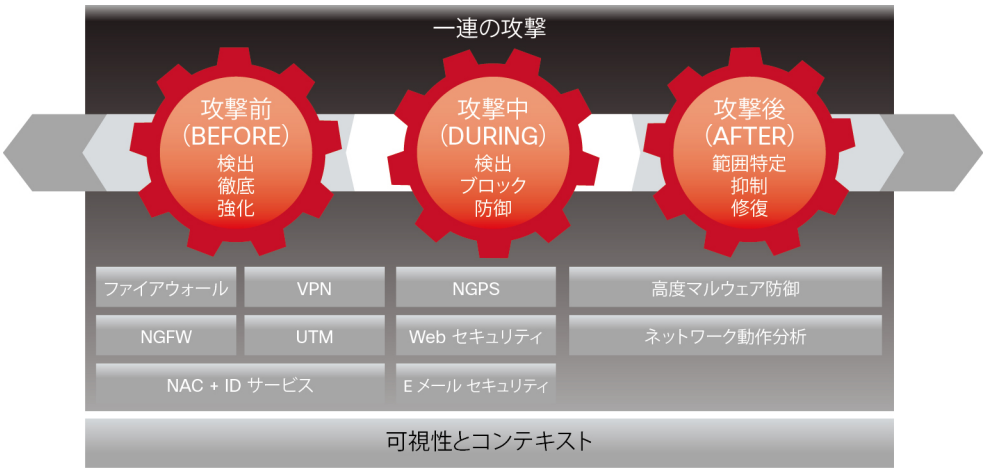
Threat-focused：現在のネットワークは、社員がいるすべての場所、データのあるすべての場所、データにアクセスできるすべての場所に広がっています。絶えず変化を続ける攻撃ベクトルに対応することは、最善の努力をしたとしても、セキュリティ プロフェッショナルにとって困難な課題です。また、攻撃者にとっては格好のチャンスです。ポリシーと管理は攻撃にさらされる領域を小さくするために重要ですが、これだけで脅威を完全に防ぐことはできません。このため、脅威の検出、理解、停止にも焦点を置いたテクノロジーを採用する必要があります。Threat-focused であるということは、攻撃者のように考え、可視性とコンテキストに基づいて環境の変化を理解して適応し、最後には保護機能を進化させて対策を講じ、脅威を停止させることを意味します。高度なマルウェアやゼロデイ攻撃の場合、これは継続的なプロセスであり、クラウドを通して継続的な分析とリアルタイムのセキュリティ インテリジェンスを実現する必要があります。また、効果をさらに高めるためには、あらゆる製品で共有する必要があります。

Platform-based：今やセキュリティはネットワークだけの問題ではありません。ネットワーク、デバイス、そしてクラウドをカバーできる俊敏でオープンなプラットフォームによる統合システムが必要です。これらのプラットフォームに必要な条件は、拡張可能であること、規模に応じて構築できること、集中管理によって統一的なポリシー適用や制御が可能であることです。簡単に言えば、敵の攻撃に負けない広範な防御が必要です。これは、単純なポイント的なセキュリティ機器の導入から、拡張性に優れた、導入しやすいサービスとアプリケーションを統合した真のプラットフォームへの移行を意味します。プラットフォームベースのアプローチは、セキュリティの有効性を高めるだけでなく、サイロ化やそれに伴うセキュリティの穴を排除すると共に、検出にかかる時間を短縮し、エンフォースメントを合理化します。

攻撃サイクル全体に対処

現在のセキュリティの課題を克服し、高い保護機能を得るためには、一連の攻撃全体を対象にし、Visibility-Driven、Threat-focused、Platform-based を基本として設計されたソリューションが必要です。シスコは、一連の攻撃全体を視野に入れた脅威中心型のサイバーセキュリティ ソリューションを幅広く提供しています。

図 4. 脅威を連続的に防ぐ



これらの、プラットフォームベースの各種ソリューションは、脅威が出現した攻撃ベクトルにおいて、業界で最も充実したエンフォースメントと修復オプションを提供しています。各ソリューションは一連の攻撃を通じて保護機能を提供するために連携し、さらにセキュリティ システム全体を補完するソリューションとして統合されます。

- 攻撃前：ファイアウォール、次世代ファイアウォール、ネットワーク アクセス コントロール、アイデンティティ サービスなどのソリューションは（これらはほんの一例です）、セキュリティ プロフェッショナルに、脅威の検出やポリシーの徹底および強化に必要なツールを提供します。
- 攻撃中：次世代侵入防御システム（NG-IPS）や E メールおよび Web セキュリティ ソリューションは、ネットワークに侵入して進行しつつある攻撃を検出、ブロック、防御する機能を提供します。
- 攻撃後：組織は Cisco Advanced Malware Protection（AMP）およびネットワーク挙動の分析を活用して、迅速かつ効果的に攻撃の範囲特定、抑制、修復を行い、損害を最小限に抑えることができます。

これらのソリューションは、大規模なグローバル組織にも対応できる拡張性を備えており、組織が必要とするときに、必要とする方法で（物理アプライアンス、仮想アプライアンス、クラウドベースのサービスとして）利用することができます。また、これらを統合することにより、広範なネットワークとすべての攻撃ベクトルに対して継続的な可視性と制御を提供することができます。

まとめ

ハッキングの産業化は、Any-to-Any の課題と相まって、システム保護のために必要な方法を大きく変えつつあります。私たちは、この機会に、サイバーセキュリティの新しいアプローチについて考える必要があります。水際で防御するだけのセキュリティ戦略では、いったんネットワークの内部に侵入されると、攻撃者は野放しの状態になります。

ビジネス モデルの変化、脅威をめぐる環境の進化、セキュリティの複雑化と細分化によりセキュリティには穴が生じ、セキュリティ ライフサイクルが破壊されると共に可視性が低下し、新たなセキュリティ管理の問題が増えます。今求められているのは、広範なネットワークをカバーできる可視性と制御を提供する、新しい脅威中心のセキュリティ モデルです。これによって、企業は攻撃サイクル全体に対応することができます。

シスコは、一連の攻撃全体を通して優れた可視性、継続的な制御、高度な脅威に対する保護を提供すると同時に、複雑化を緩和できる、脅威中心型の独自のセキュリティ アプローチを提供できます。この新しいセキュリティ モデルを使用すれば、攻撃前、攻撃中、攻撃後を通して、よりスマートに、そしてより迅速に脅威に対応できます。

お問い合わせ先

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

14.08

Printed in USA

C11-731741-01　06/14