探求!

セキュリティ対策の理想モデル

――見えていますか？ 重要情報に忍び寄るサイバー攻撃の“魔の手”――

シスコシステムズ合同会社

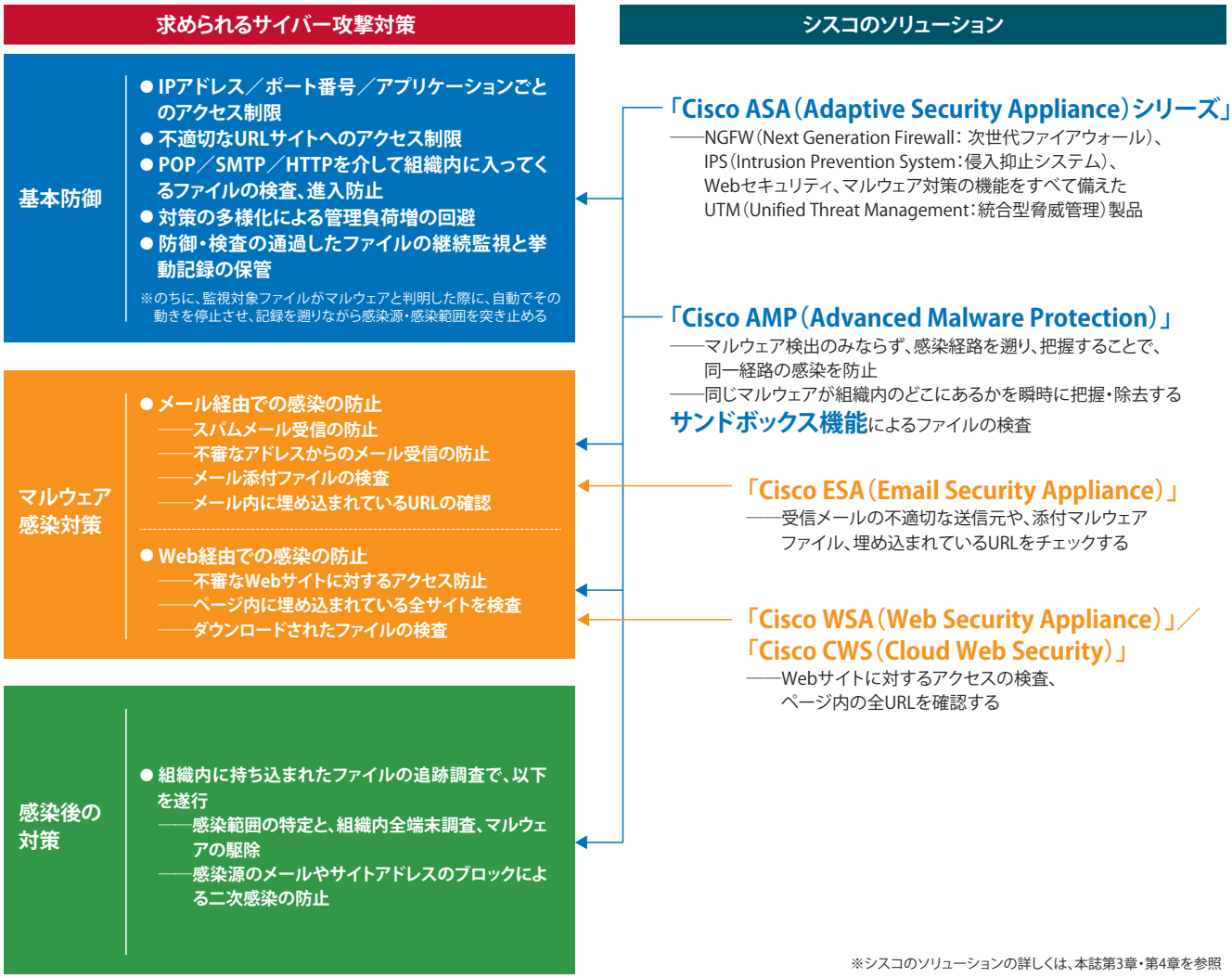
サイバー攻撃の高度化・巧妙化により、従来型のセキュリティ対策だけでは情報漏えい・窃取のリスクを排除するのが至難になっている。会社のIT環境や仕事の進め方、さらには、従業者の特性を調べ上げ、社内のシステムに巧みに潜入し、誰もが気づかぬうちに重要情報を奪い去っていく――そんなサイバー攻撃による情報漏えいの被害が後を絶たない。

シスコシステムズが提案するのは、そうした攻撃のフェーズに応じた総合的なセキュリティ対策だ。このアプローチの下で提供されている製品は、大企業のみならず、セキュリティ対策に潤沢な資金や人的リソースを割くことのできない中堅・中小の企業にも有効だ。

本ハンドブックでは、企業・組織が直面しているセキュリティ・リスクと課題を明らかにしながら、シスコのセキュリティソリューションの実効性について解説する。

CONTENTS

シスコの提案



※シスコのソリューションの詳しくは、本誌第3章・第4章を参照

第1章

脅威の実態をとらえる

サイバー攻撃対策を考えるうえでまず重要なことは、その実態を正しくとらえることだ。
「今、企業・組織の重要情報は、どのようなセキュリティ上の脅威にさらされているのか」
――その実態を知ることが、対策強化に向けた第一歩と言える。
そこでまずは、情報セキュリティを取り巻く脅威の現状・実態について明らかにしておきたい。

情報セキュリティ対策の盲点

従来、企業における情報セキュリティ対策の力点は、「外部からの脅威の侵入をいかに防ぐか」に置かれていた。社内ネットワークとインターネットとの境界線にファイアウォールを設置するといった施策は、その典型例の一つだ。だが、そうした入口対策だけで脅威の侵入を防ぎ切ることはそもそも難しい。

例えば、物理オフィスのセキュリティ対策を想起していただきたい。物理オフィスでは、犯罪者の侵入を防ぐために、入口の施錠や警備員の配備などによって防御を固める。だが、こうした対策をいくら強化したところで必ず“抜け穴”が出来る。窓や裏口から侵入されるかもしれないし、社員が紛失したカギから合鍵が作られるかもしれない。また、何者かが社員になりすまし、正面から堂々と侵入される可能性もある。さらに言えば、社員自身が犯行を起こすケースに対しては入口対策は無力だ。

このようなリスクを未然に回避すべく、物理オフィスでは、いわゆる「内部施策」も厳重に講じる。重要書類・貴重品を金庫や施錠付きのロッカーでガードするのはもとより、監視カメラで人の出入りや現金の出入りをモニタリングしたり、記録したりして、「いつ誰が何を行ったか」をあとからでも追跡できるようにする。さらに、同じ手口が通用しないように、定期的にチェック体制を見直してもいるだろう。

このようなオフィスのセキュリティ対策は、企業資産を守るための当然の施策として大多数の会社が遂行してきた。ところが、情報セキュリティの領域では、もっぱら「侵入防止」の施策のみに力が注がれ、「内部施策」はなおざりにされるケースが少なくなかった。結果として、防御の網を巧みにすり抜けるサイバー犯罪によって、企業の重要情報が窃取されるケースが後を絶たないのである。

デジタル化するビジネス、膨れ上がる脅威

もちろん、入口対策を強化することは大切だ。だが、ビジネスのデジタル化が進行し、企業のIT環境が複雑性を増す今日、攻撃者の侵入経路は拡大の一途を辿っており、「情報の守り手」側はますます不利な状況に追い込まれている。

例えば、旧来、ビジネスパーソンによるIT利用は企業内の業務システムや基幹システムに限定されていた。ところが近年では、日々の業務の中で、メールやスマートデバイス（スマートフォン／タブレット）、各種のクラウドサービス、さらには、ソーシャルメディアを用いるケースが増え、企業内個人が社外のネットワーク（インターネット）を介して業務をこなす場面が増大している。結果、企業が保護すべき対象は以前とは比べものにならないほど広がっていると言えるだろう。

一方で、サイバー攻撃を仕掛けてくる敵の「プロ化」も進行し、攻撃手法の高度化・多様化に歯止めがかからぬ状況が続いている。

旧来のサイバー攻撃は、Webサイトの改ざんにせよ、ウイルスの流布にせよ、「愉快犯」的な犯行が主流を成していた。ウイルスも不特定多数の企業・組織・個人を対象にしたものが多く、ウイルス対策ソフトの網にかかる場合が大多数だった。

ところが、2010年以降、個人・組織の重要情報に狙いを定めた「標的型攻撃」が猛威を振るい始めている。この攻撃を仕掛けてくる犯罪者は、いわゆるプロの「経済犯」であるケースが少なくなく、標的にした企業・組織のシステムやビジネスのありようを入念に調べ上げ、そのセキュリティ上の脆弱性をめがけて執拗に攻撃を繰り返してくる。そのため、いったん標的にされると防御が難しい。しかも、犯罪者が標的企業・組織に潜入させる不正プログラムは、未知のマルウェアであり標的企業・組織のシステ

ム環境に合わせてカスタマイズされている場合もある。そのため通常のウイルス対策ソフトでは不正プログラムが検知できないことが少なくない。結果、脅威の潜伏に気づかず、知らぬ間に、企業・組織の重要情報が抜き取られてしまうケースが多いのである。

さらに、重要情報に対するアクセス権限を持った関係者が情報窃取の犯行に及ぶ場合もある。こうした内部犯行も検知が難しく、企業・組織にとっては極めて深刻な脅威だ。2014年に内部犯行による大量情報の漏えい事件が日本で相次いで発生し、社会を騒然とさせたが、実のところ、情報漏えい事件の多くが内部犯行によるものとされている。また、ITの進化によって、大量データを社外に持ち出す手段が多様化していることも、この脅威の深刻化に拍車をかけていると言えるだろう。

あらゆる業種・業態にマルウェア侵入のリスク

言うまでもなく、サイバー攻撃によるマルウェア侵入のリスクは、あらゆる業種・業態の企業・組織にある。ここで**図1**をご覧いただきたい。これは、業種別にどれほどのサイバー攻撃を受けているかを4つのレベルに分けて表したものだ。シスコの顧客における攻撃のブロックレートから割り出した数値でもあり、ネットワーク上を行き交うトラフィックに対して、どの程度の比率で攻撃が仕掛けられているかを示すものでもある（ノーマル・レベルは1.0）。

この図を見ると、エレクトロニクス業界が最も頻繁に攻撃を受けており、マルウェアの感染リスクがそれだけ高いことが分かる。一方、“ノーマル”のレベル以下にある業界は、サイバー攻撃によるマルウェア感染のリスクが他に比べ相対的に低いように思える。ただし、この分析が2015年上半期のデータのみの分析であることを加味すれば、そう考えるのは早計だ。逆に、あらゆる業界に属す、すべての企業がサイバー攻撃の脅威に等しくさらされており、攻撃は必ず受けると考えるべきだろう。そして万が一、攻撃によって企業の重要情報（例えば、顧客情報や取引情報、知財データ、など）が大量に漏えい・流出すれば、企業は計り知れないダメージを受ける。だからこそ、サイバー攻撃への備えを強化していくことが不可欠と言えるのである。また今後、日本でマイナンバー（社会保障・税番号）制度の運用が本格的に始まれば、マイナンバーもサイバー攻撃の標的にされる可能性が高く、それを保護するための特別な仕組み作りも求められることになる。

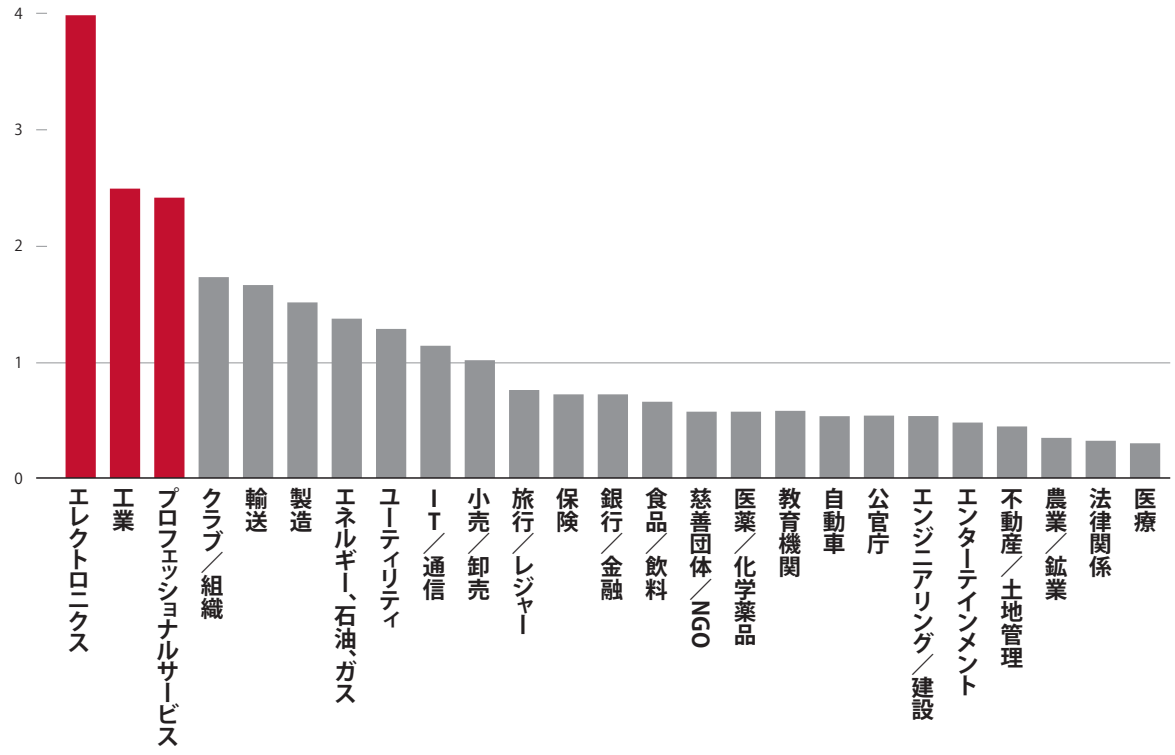


図1：業種別のマルウェア遭遇リスク

（出典：シスコ「2015年中期セキュリティ レポート」）

第2章

防御の課題と具体策

前章では、企業・組織が直面するサイバー攻撃の脅威について概観した。
本章では、その脅威についてさらに具体化させ、
防御の課題と課題解決の施策について掘り下げる。

「既知の攻撃」と「未知の攻撃」

情報セキュリティ上のインシデント（事故）はさまざまな条件が重なって起こるケースが少なくない。

なかでも問題なのは、サイバー攻撃者が検出を回避する能力を向上させ、インシデントの発生を防ぐのが非常に難しくなっていることだ。

言うまでもなく、企業・組織は、こうしたサイバー攻撃の変化・高度化を加味しながら、情報セキュリティ対策、あるいはサイバー攻撃対策を講じていかなければならない。

その具体策を考えるうえで視点を置くべきは、攻撃の手法が「既知」か「未知」かというポイントである。つまり、サイバー攻撃を、既知の攻撃と未知の高度化された攻撃とに分けて、それぞれに適した防御の施策を考えていくことが重要なのである。

サイバー攻撃を既知の攻撃と未知の攻撃に分けた場合、全体の95％程度は既知の攻撃――すなわち、攻撃の手法がすでに知られている攻撃と言ってよい。例えば、不特定多数の企業・組織、個人をターゲットにした「スパムメール」や「マルウェア」、あるいは、DDoS攻撃などが、既知の攻撃に類するものであり、これらに対しては、従来からあるウイルス対策やファイアウォール、IDS/IPS、ネットワークのセグメント化といった施策が有効だ（**図2**）。

また、ソフトウェアの脆弱性を突く攻撃についても、ソフトウェア資産の管理をしっかりと行い、どのシステムで、どのバージョンのソフトウェアが動作しているかを把握しておけば、脆弱性が発見された時点でその影響範囲が特定でき、パッチ（脆弱性の修正プログラム）の適用といった対処をすみやかに講じることができる。

これに対して、未知の攻撃、あるいは高度化されたサイバー攻撃は、従来型の対策では検知・検出が難しく防御のための新しい仕組みが必要になる。

実際、攻撃対象を絞った「フィッシング攻撃」や「トロイの木馬攻撃」、エクスプロイトツール・不正サイトを用いた「水飲み場型攻撃」、あるいは「ソーシャル ネットワーキング攻撃」などを通じて、従来の防御網が突破され、重要情報が窃取されるケースは少なくない。

また、脆弱性に対する攻撃の速度も増しており、パッチが正式にリリースされる前に、当該の脆弱性が攻撃を受けるケースが多くある。

実際、公開された脆弱性には「CVE（Common Vulnerabilities and Exposures: 共通脆弱性識別子）」という番号が付与されるが、攻撃の傾向を分析すると、CVEが公開された1～2日後には、その脆弱性を悪用した攻撃

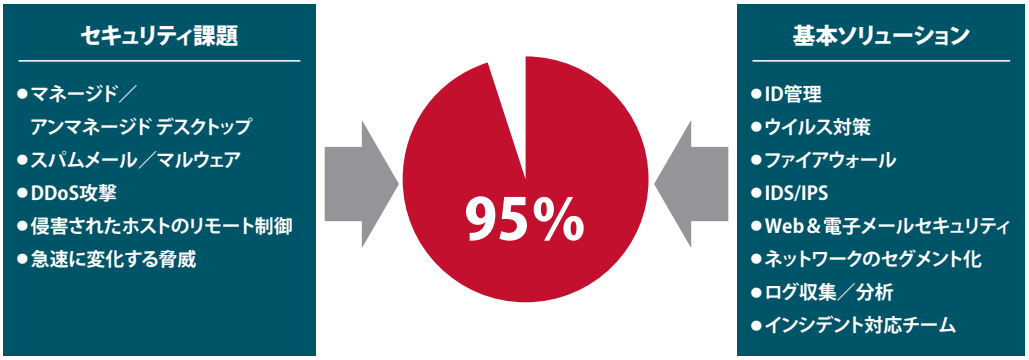


図2：既知の攻撃に対する対処法

（資料：シスコシステムズ）

の発生が確認されているのだ（シスコ「2015年中期セキュリティレポート」より）。

侵入に長期間気づけない

先にも触れたとおり、未知で高度化された攻撃は防御の網の目をすり抜けるのが巧みであり、いったん組織内部への侵入を許すとなかなかその存在に気づけないという恐ろしさがある。例えば、**図3**は、サイバー攻撃の「見えにくさ」、「対応の難度の高さ」を表す調査結果だ（シスコによる調査）。ご覧のとおり、サイバー攻撃によるセキュリティ侵害を受けた企業の「33%」が2年以上、攻撃に気づくことができず、55%がセキュリティ侵害の原因が特定できていない。また、数カ月間にわたりセキュリティ侵害が発見されなかったケースは、全体の54%にも上っている。これは、今日のサイバー攻撃が従来型の検知・検出の網をいかに巧みにかいくぐり、かつ、潜入先での活動の隠ぺい工作にも長けていることを示すものだろう。

また、サイバー攻撃によるセキュリティ侵害に長期間気づけず、原因も特定できなければ、当然、同じ手口による被害の拡大・長期化を許すおそれが強くなるのである。

そこで重要になるのは、以下に示す時間をいかに短くするかだ。

- 攻撃を発見するまでの平均時間：MTTF（Mean Time To Failure）
- 攻撃を封じ込めるまでの平均時間：MTTC（Mean Time To Complete Changes）
- 修復するまでの平均時間：MTTR（Mean Time To Recovery）

繰り返すようだが、今日のサイバー攻撃はプロの犯罪者・犯罪組織によるもので、システムだけではなく、人の弱点も突き、人的エラーを巧みに誘う。そのため、攻撃の侵入を100%阻止することは至難であり、侵入を前提にした新たな施策を展開する必要がある。その施策を講じる際の重要な指標が、上の3つの平均時間というわけだ。

未知の攻撃への対処法

では、高度な攻撃への防御を固め、MTTF、MTTC、MTTRを可能な限り縮小するにはどのようなソリューションが必要とされるのか――。

それは、社内・組織内ネットワーク上の不審な動きを早期にとらえるための「見える化」の仕組みであり、社内・組織内に潜在する脅威をインテリジェントにあぶり出したり、攻撃やその被害範囲を特定したりするためのビッグデータ分析の仕組みである。さらに、標的型サイバー攻撃専任のチームを組織することも高度化する脅威に対抗していくうえでは大切である。

ならば、こうした仕組みをどのように築けばよいのか。また、セキュリティに関する予算や人的リソースに限りがある中で、果たして、これらの仕組みを構築することは可能なのか――。次章では、そうした疑問への解を示す。

図3：企業・組織は「脅威の侵入」になかなか気づけない　（資料：シスコシステムズ）

第3章

サイバー攻撃対策の理想モデル

前章で述べたとおり、高度化する攻撃に対する防御を固めるには、新たな対策を講じなければならない。本章では、シスコシステムズ（以下、シスコ）が提唱しているセキュリティ対策の理想モデルに基づきながら、未知の攻撃に対処するための新たな技術・ソリューションを具体的に示す。

攻撃フェーズに応じた対策

サイバー攻撃への備えを固めるうえでは、攻撃のフェーズを「BEFORE（攻撃前）」、「DURING（攻撃中）」、「AFTER（攻撃後）」という3段階に分けて対策を練ることが重要だ。シスコが提唱しているセキュリティ対策の理想モデルは、この3つのフェーズを包括的にカバーしたものである（**図4**）。

図5からも分かるとおり、BEFORE、DURING、AFTERの3つのフェーズに対応した対策とは、それぞれ、「攻撃を未然に防ぐための対策」、「攻撃を実際に受けたときの対策」、「攻撃を受けた後に、すみやかに封じ込めるための対策」と見なすことができる。そして、これらの対策をバランスよく講じていくことが、サイバー攻撃への防御を固め、前章で触れたMTTF、MTTC、そしてMTTRの最小化につながることになる。

シスコでは、BEFORE、DURING、AFTERの対策強化に必要とされるセキュリティ製品を網羅的に提供しており、それらを用いれば、サイバー攻撃の各フェーズに応じた備えを強化していくことができる（次ページの**図5**）。そこで以下では、BEFORE、DURING、AFTERの各対策の要諦と、その強化に有効なシスコの製品について整理して示すことにしたい。

「BEFORE」対策の要諦とソリューション

BEFORE対策の重要なポイントは、「発見」、「適用」、「堅牢化」である。つまり、「攻撃の芽」を可能な限り早期に発見し、それらの芽を摘み取ることで、システムをより堅牢にするというわけだ。

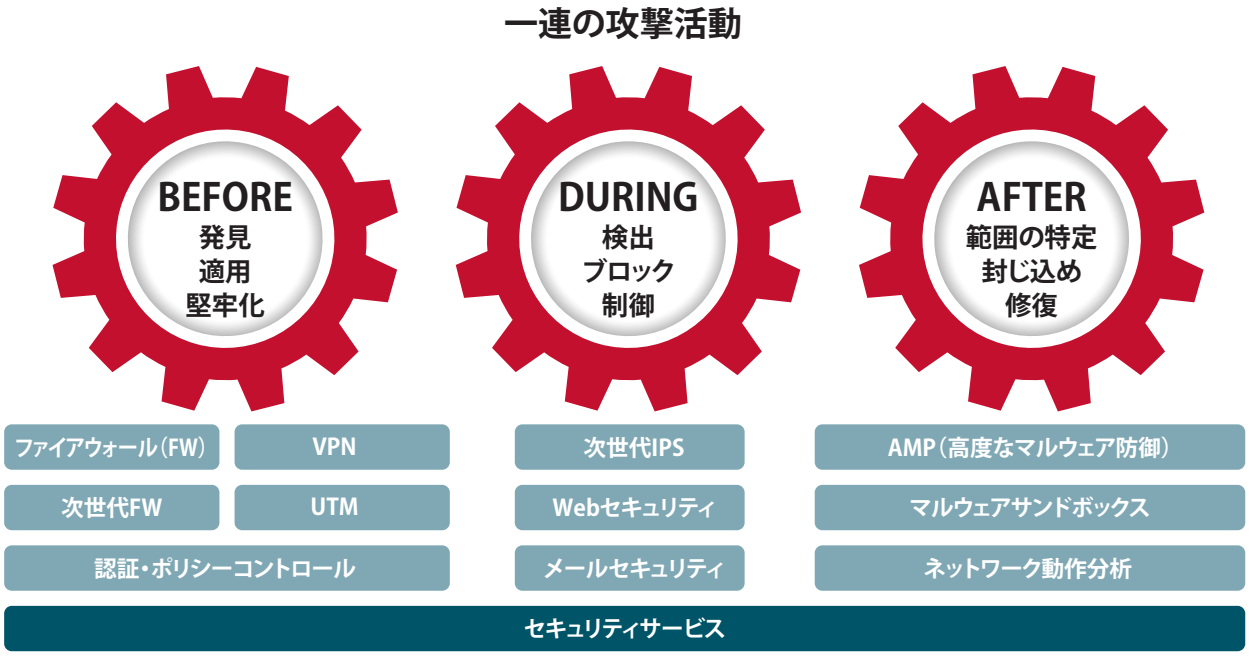


図4：シスコが考えるセキュリティの理想モデル　（資料：シスコシステムズ）

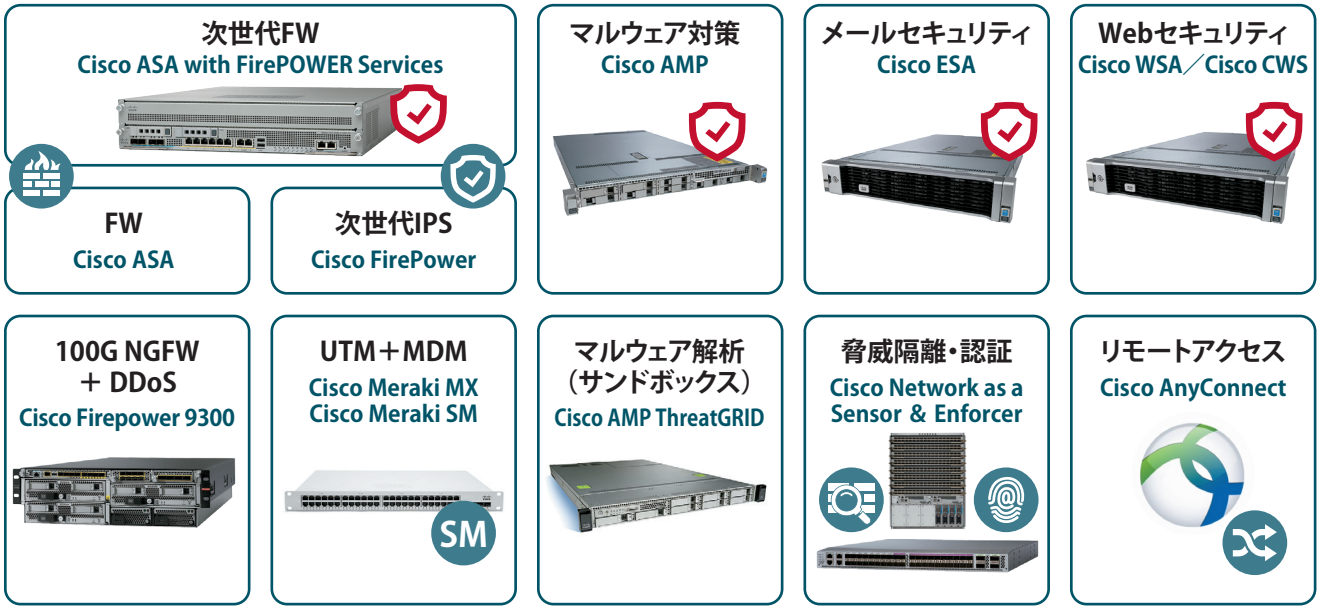


図5：シスコの多彩なセキュリティ製品のポートフォリオ

この対策を支えるセキュリティ製品の分野としては、「ファイアウォール（FW）／次世代ファイアウォール（NGFW）」、「VPN」、「統合脅威管理（UTM）」、さらには、「認証・ポリシーコントロール」などが挙げられるが、シスコでは、そのすべての領域に向けた製品をラインアップしている（以下、主要製品のみ抜粋）。

- FW/NGFW：Cisco ASA / Cisco ASA with FirePOWER シリーズ
- VPN：Cisco AnyConnect
- UTM：Cisco Meraki
- 認証・ポリシーコントロール：Cisco Identity Services Engine（ISE）

もちろん、日々進化し、高度化・多様化するサイバー攻撃の脅威に対して、全方位的な防御の施策を講じようとした場合、投資や運用管理の手間がかさんでいく可能性もある。仮にそうなれば、セキュリティ対策に多くの金銭的・人的リソースが振り向けられない中小規模の企業にとって大きな負担となるだろう。そこで求められるのが、1つの製品で、さまざまな防御の施策が講じられるUTMとなる。

「DURING」対策の要諦とソリューション

一方、DURING対策での重要なポイントは、「検出」、「ブロック」、「防御」の徹底だ。実際、仮に脅威の侵入を許したとしても、それをすみやかに検出し、外部へのアクセスを「ブロック」することができれば、情報の漏えいを阻止する（あるいは、その被害を最小限に食い止める）ことが可能になる。

この対策で必要されるセキュリティソリューションは、「メールセキュリティ」と「Webセキュリティ」、「次世代型IPS／マルウェア防御」の仕組みと言える。

改めて説明するが、標的型のサイバー攻撃では、多くの場合、標的企業・組織の従業者にフィッシングメール――例えば、その企業の顧客や取引先、あるいは従業者を偽ったメール――を送りつけ、添付ファイルを開かせることで、そのPCをマルウェアに感染させる。マルウェアに感染したPCは、外部の不正サーバとの通信を始め、攻撃者に乗っ取られる格好となる。攻撃者は、それを足掛かりに、企業・組織内部のネットワークを縦横に動き回り、重要情報の在り処を突き止め、収集し、不正サーバに送出するのである。

メールセキュリティやWebセキュリティ製品は、こうした攻撃を受けた際に、フィッシングメールを検出したり、外部の不正サーバを検出したりするための仕組みだ。また仮に、これらの検出網が突破され、社内のPCがマルウェアに感染した場合も、マルウェアと社外サーバとの通信を検出し、アクセスをブロックする仕組みがあれば、情報漏えいのリスクを回避できるのである。

シスコでは、メールセキュリティ製品として「Cisco Email Security Appliance（ESA）」を、Webセキュリティ製品として、「Cisco Web Security Appliance（WSA）/ Cisco Cloud Web Security（CWS）」をそれぞれ提供しているが、これに、次世代型のIPS／マルウェア防御の機能を組み合わせれば、サイバー攻撃のDURING対策を大きく強化することが可能となる。

「AFTER」対策の要諦とソリューション

攻撃発生後のAFTER対策では、「範囲特定」、「封じ込み」、「修復」の仕組み作りが重要となる。具体的には、攻撃を受けた際に、すみやかに攻撃の影響範囲を特定し、マルウェアの感染が拡大しないよう脅威を封じ込め、再度、同様の攻撃を受けないようシステム・業務を修復することが必要とされるわけだ。

この施策展開でカギを握るのが、高度なマルウェア分析やネットワーク（上の通信の）解析機能だ。すでに述べたとおり、標的型のサイバー攻撃は、未知の攻撃であるケースが大半であり、攻撃に使用されるマルウェアは通常のウイルス対策ソフトでは検出できない場合が少なくない。そのため今日では、隔離された仮想環境の中で不審なファイルを実行し、その挙動を確認する「サンドボックス」がマルウェア検出のためのツールとして普及し始めている。とはいえ、サンドボックスでも未知のマルウェアが100%検出できるわけではなく、検出漏れが発生する。また、繰り返すようだが、潜入に成功したマルウェアの挙動は検知が難しく、攻撃を見過ごしてしまうことも往々にしてある。さらに、攻撃を発見したのちも、その被害範囲がなかなか特定できず、封じ込めの作業が後手に回るケースも多いのだ。そこで必要とされるのが、マルウェアやネットワークの動きを高度に解析し、マルウェアやその感染範囲を高精度に割り出すためのシステムだ。

その仕組みとしてシスコが提供しているのが、「Cisco AMP（Advanced Malware Protection）」である。AMPは、次章で紹介する脅威解析のインテリジェンスを提供するクラウド基盤「Cisco Collective Security Intelligence」などを活用して、高度なウイルス防御を可能にするソリューションだ。

最新の不正ファイル（マルウェア）に対するユーザーアクセスを、クラウドを通じてブロックする「ファイルレピュテーション」の機能や、サンドボックス（Cisco AMP ThreatGRID）による脅威の動的解析・検出を実現しているほか、「ファイルレトロスペクション」と呼ばれる機能によって、過去に遡ってマルウェアの追跡調査が行えるという大きな特徴を有している。レトロスペクション機能を備えたCisco AMPは、監視カメラのように内部ネットワークに入ってきたファイルの動きを監視・記録し、何らかのファイルがマルウェアと判定された時点で、その動きを過去に遡りながら調査・分析、「組織内のどのPCが、いつ、どのような経緯で感染したのか」や「バックドアの潜伏状況」、「攻撃者がどの情報を盗もうとしたか」などを速やかに特定する。これにより、ファイアウォールなどの境界防御の網をすり抜け、組織内に侵入してきたマルウェアに対して、適切、かつスピーディな対処が図れるようになる。また、Cisco AMPのファイルレトロスペクションは、組織内のデータやシステムに対する犯罪行為の証拠保全・調査（デジタル・フォレンジック）にも適用できる。そのため、内部不正による情報漏えいの防止・抑止にも効果的だ。

サイバー攻撃のすべてのフェーズに対応――中小の企業を脅威から守る「Cisco ASA 5506-Xシリーズ」

シスコの「Cisco ASA 5506-Xシリーズ」は、サイバー攻撃の「BEFORE」、「DURING」、そして「ATFER」のすべてのフェーズに対応したUTM製品だ。小規模のネットワークを対象にした省スペース・廉価なローエンドモデルありながら、3,000 種以上のアプリケーションの通信が可視化できるほか、URLフィルタリングによってユーザーの不正サイトへの接続をブロックすることもできる。また、「FirePOWER Services」モジュールを標準で搭載しており、VPN機能や次世代型IPS機能／マルウェア防御の機能もサポートしている。

このうち、次世代型IPSの 機能を用いれば、ソフトウェアの脆弱性に対する即時対応が可能になる。また、Cisco AMPの働きにより、新種のマルウェアの検出・防御がスピーディに行われるほか、外部の不正サーバ（遠隔操作サーバ）と社内システムとの通信の検出・遮断なども可能となる。シスコでは現在、従業員数100 名規模以下の企業に向けたセキュリティソリューション「Cisco Start」も始動させており、このソリューションを成す中核製品の一つとして、Cisco ASA 5506-Xシリーズが位置づけられている。

AFTER対策のもう一つのアプローチ「Network as a Sensor」

もう一つ、シスコならではの「AFTER対策のアプローチ」と言えるのが、「Network as a Sensor」の仕組み作りだ。これは、ネットワーク機器をセキュリティ対策のセンサーとして機能させる試みであり、ネットワーク機器からネットワーク上を行き交う通信フローを読み取り、解析を行うことで、端末に依存しない脅威の自動解析を実現する。解析に用いるのはトラフィック監視で一般に用いられている「Netflow」である。そのため、脅威解析のためにネットワークの構成を変える必要はなく、システムのパフォーマンスにも悪影響を及ぼさない。また、認証機能を組み合せることで、感染端末を特定し、経路制御によるアクセス停止の自動化も可能になる。つまり、Network as a Sensorの働きにより、既存のネットワークが、「脅威の知覚と隔離を自動化する」ツールとして機能するようになるのである。

定期的に健康診断を受ける

上述したBEFORE、DURING、AFTERの対策を強化することは、今日のサイバー攻撃のプロセスに沿った実践的な取り組みだ。それを日々のセキュリティ業務のサイクルに取り込んでいくことで、防御の継続的な改善が可能になる。もっとも、これらは広範な取り組みであるだけに、何から手を付ければいいのか、自社では何が不足していて、何に力を入れるべきかが分からない場合もある。

そこで、シスコが推奨しているのが、自社・自組織のセキュリティ状況がどうなっているかを定期的に診断することだ。つまり、セキュリティに関して定期的に相談できる相手を見つけ、健康診断のように自社のセキュリティ・レベルを定期的にチェック／評価していくのである。

また、診断といっても、侵入テストのようなコストのかかる大掛かりなものではない。日々の健康状態を記録しておき、万が一の際にすぐに相談できる“かかりつけ医”のような存在をつくっておくことが大切なのである。

第4章

次世代の防御を支えるサービスとインテリジェンス

前章で触れたとおり、シスコシステムズ（以下、シスコ）のセキュリティ製品は、中小規模のネットワークを対象にしたローエンド製品から、大規模ネットワーク向けのハイエンド製品に至るまで、すべてが優れた品質と機能が確保されている。また、大規模ネットワークを運用する企業に向けては、高度なセキュリティサービスも提供しており、そうした広範なサービス・製品を支える基盤として、大規模なセキュリティインテリジェンスの仕組みも作り上げている。本章では、そうしたシスコのサービスとインテリジェンスについて紹介し、本誌の締めくくりとしたい。

企業が直面する多岐の課題に対応

今日、あらゆる業種・業態の、さまざまな規模の企業・組織が未知のサイバー攻撃の脅威にさらされている。ローエンド製品からハイエンド製品に至るまで、シスコのセキュリティ製品がすべて優れた品質・機能を備えているのはそのためだ。

ただし、企業・組織のネットワークが大規模になればなるほど、攻撃者にとってのアタックポイントは増え、人的なエラーが引き起こされる可能性も高くなる。

そのため、シスコでは、高度なセキュリティサービスも提供している。

サービスの特徴は、企業・組織のセキュリティ対策のレベルに応じて、計画・構築・運用の適切なメニューが用意されていることだ。

例えば、基本的な対策となるレベル1では、各種製品の

インテグレーションサービスやマイグレーションサービスが用意されている。また、より高いレベルになると、セキュリティアセスメントやリスク分析・評価、セキュリティアドバイザリなどのサービスが提供されるほか、セキュリティの運用サービスや、サイバー攻撃の擬似体験などを通じて、専門家の育成やプロセス整備を支援する「サイバーレンジ」サービスなども用意されている。このうち、セキュリティ運用のサービスでは、ビッグデータ分析によるセキュリティ上の脅威の予見から可視化、防御、復旧に至るまでの運用支援サービスが包括的に提供される。

これらのサービスを活用することで、企業は、セキュリティ対策上の多岐にわたる課題を抜本的に解決することが可能になる。

世界最大規模のセキュリティインテリジェンス

こうしたシスコの幅広い製品やサービスを支えているのが、世界中で展開されているセキュリティインテリジェンスの仕組みだ。

この仕組みにおいて中心的な役割を演じているのが、前章でも触れたCollective Security Intelligence（CSI）である。

CSIは、クラウド上に世界中の脅威情報を収集するネットワークであり、世界中に分散する160万強のデバイスから、1日当たり100TB（テラ・バイト）もの脅威データを収集している。

また、サンプリングするWebリクエストは1,300億件にも上り、電子メール数は10億件に達する。これは、全世界の電子メールトラフィックの35%に相当する規模だ。さらに、CSIで収集された膨大なデータは、研究機関の「Cisco Talos Security Intelligence and Research Group」によって分析され、「BEFORE」、「DURING」、「AFTER」の各フェーズにおいてシスコ製品／サービスが利用する脅威データベースに反映されているのである（**図6**）。

これほど大規模な脅威情報を収集し、分析しているベンダーは、世界的に見ても他に例はないと言える。その意味で、CSIの存在は、シスコ製品の大きなアドバンテージであり、シスコ製品における未知の攻撃・脅威の高い検出力・分析力、あるいは防御の能力を支える力の源でもあるのだ。

シスコのセキュリティ製品やサービスは、先進的な技術や取り組みによって、日々進化している。だからこそ、高度化・巧妙化するサイバー攻撃から企業・組織を守る有効な手だてとなりうるのである。

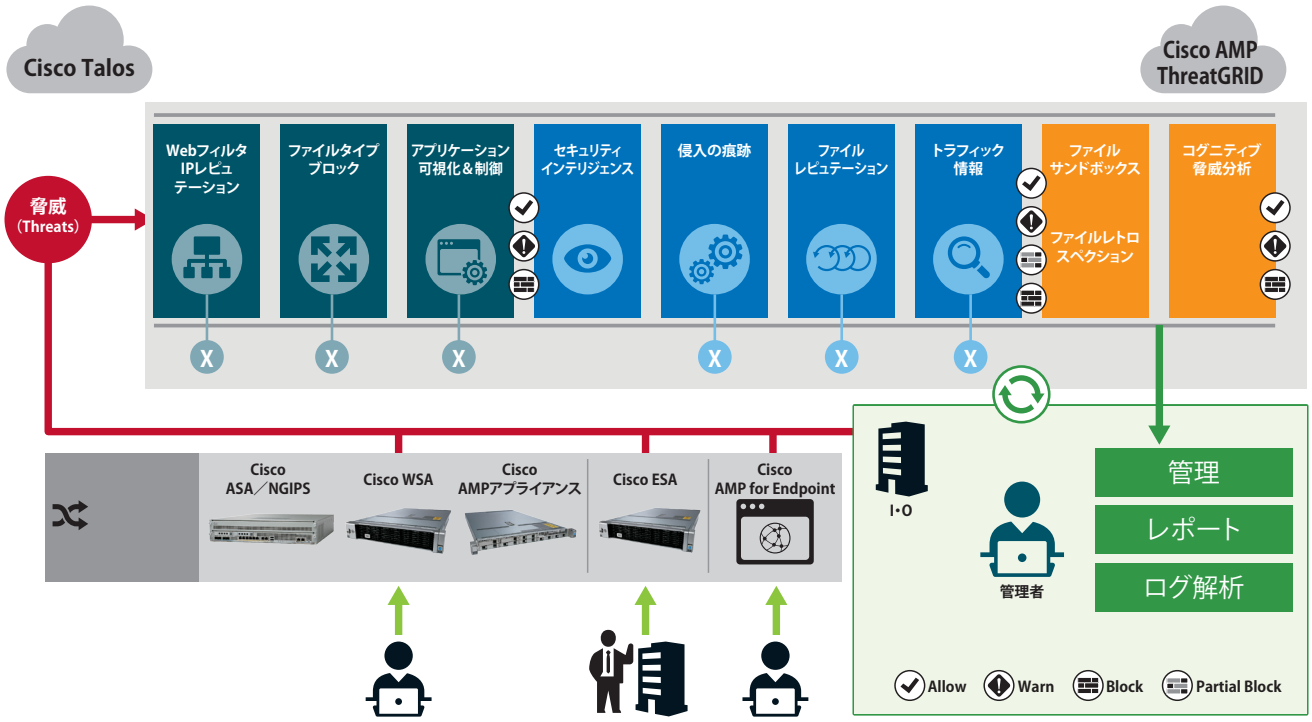


図6：Cisco Talosによるビックデータ分析と、シスコ製品との連携イメージ

お問い合せ先

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

1103-1602-01A-AI