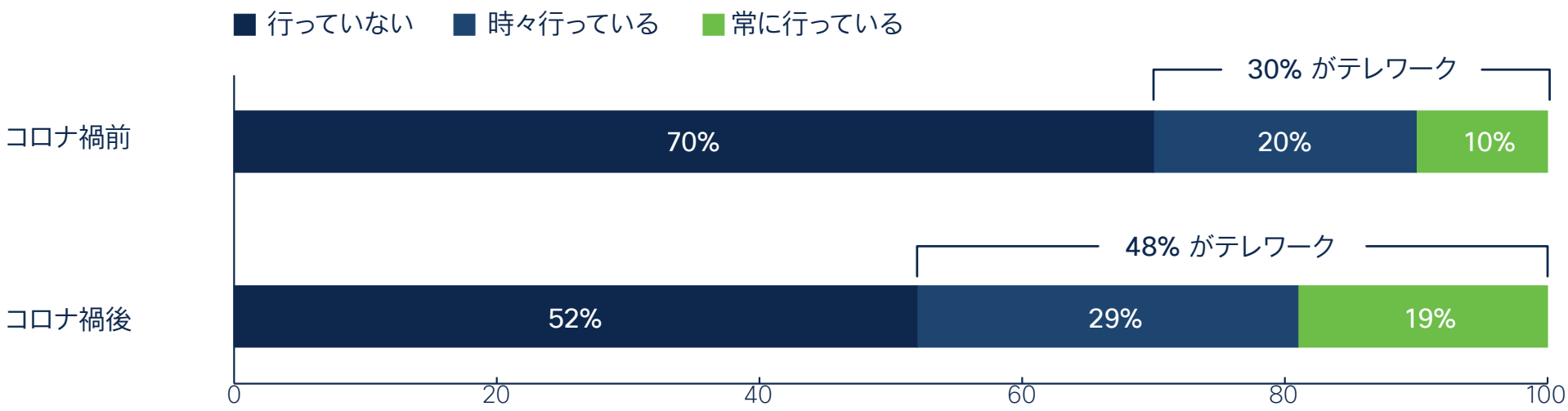
Cisco Umbrella

eBook
Cisco Public

リモートワーカーのためのサイバーセキュリティ

あらゆる場所のデバイスをすべて保護するには

この eBook の内容



コロナ禍の前後でテレワークを行う従業員の割合（予測）

ポストコロナにおける職場のセキュリティ

コロナ禍は私たちの働き方に大きな影響を与えました。その変化は今後も継続すると考えられますが、中には変化したまま二度と元に戻らないものもあるかもしれません。ポストコロナの世界における経営戦略の策定に着手しようとする企業にとって、最大の課題の 1 つは進化し続けるサイバーセキュリティのニーズに対処することです。その背景にあるのは、テレワークが事実上、現代の職場を構成する 1 要素となっていることです。

Gartner 社は 2019 年に、2030 年までにテレワークの需要が最大 30% 増加すると予測しました。コロナ禍がその潮流に拍車をかけたことは言うまでもありません。多くの組織が大半もしくはすべての従業員をテレワークに移行させました。現在、リモート環境での生活に慣れてきた従業員の多くはテレワークを続けたいと考えていて、CFO もそうすることにコスト面でメリットがあると理解しています。その結果、ポストコロナには大企業の従業員の 48% は、少なくとも勤務時間の一部がテレワークでの勤務になると予想されています。そして、そうしたリモートワーカーの保護が必要になります。[1]

従来の防御手段はポストコロナの従業員（テレワーク、オフィス勤務、またはその両方を複合したハイブリッドワークのユーザー）を想定して開発されたものではありません。インテリジェンスを共有しないウイルス対策製品やファイアウォール、独立のセキュリティソリューションでは、十分な効果を得られないということです。今こそサイバーセキュリティを強化し、ユーザーがどこからでも働けるような防御手段を用意して、コロナ禍が生み出した状況から抜け出すための新たな方法を模索する時です。

昨今の攻撃によるセキュリティ侵害の原因の 68% は、分散拠点とローミングユーザーであったというデータがあります。[2]

この eBook では、セキュリティ担当者が今日直面している課題に目を向け、マルウェアの抑制からセキュリティの簡素化、増え続けるリモートワーカーやローミングワーカーの保護まで簡単に対処できる方法をご紹介します。

最もシンプルなのは、ポストコロナの世界でテレワークを行う従業員や学生を、多機能なクラウドベースのセキュリティソリューションで保護する方法です。このソリューションは DNS レイヤを起点とする保護を提供することで、他のさまざまなセキュリティサービス（ファイアウォール、セキュア Web ゲートウェイ、CASB）を統合し、企業に被害が及ぶ前に脅威を認識し、阻止します。

新たな脅威に対する新たな防御方法

ネットワークが変化すれば攻撃手法も変わります。そしてテレワークへの移行は、間違いなくネットワークの変化の範疇に入ります。攻撃者は驚くべき速さで適応力のある攻撃インフラストラクチャを新たに構築します。そうして新たな攻撃領域が開拓され、より巧妙に防御をかいくぐる悪質な派生形が生み出されるために、悪意のあるトラフィックを識別してブロックするのが困難になっています。最新の脅威には次のようなものがあります。

- 攻撃者が従来型の防御をかいくぐりランサムウェアや悪意のあるコードのインストールを可能にする、詐欺メールを用いたスピアフィッシング
- シグネチャベースのソリューションでは（シグネチャやプロファイルの更新速度が速くても）検出が難しい一度限りのマルウェアパッケージ
- ネットワークベースの防御をかいくぐり、長期間にわたって検出されることなくインフラストラクチャに侵入してデータ窃取を可能にする低速少容量型の攻撃
- 脅威を増殖させるマルウェアキットやサービスとしてのマルウェアリソース。こうした手段を利用すれば、攻撃者や犯罪組織に技術力がなくても、悪意のある仮想通貨マイニングなどのサイバー攻撃に関与することが可能

人材

2022 年までにサイバーセキュリティ職の人材不足が 180 万人規模に [3]

オーケストレーション

79% が複数ベンダーとのアラートの調整に苦戦 [4]

アラート

サイバーセキュリティの専門家の 44% が日々 10,000 件を超えるアラートを認識 [4]

レポート

サイバー犯罪の報告件数は 300% の増加 [5]

テレワークの従業員にも簡単に適用できる DNS レイヤセキュリティ

ポストコロナの世界でオンネットワークのユーザーもオフネットワークのユーザーも同じように保護するには、インターネットをセキュリティの強化に利用します。マルウェアの 91% は、DNS を利用してコマンドアンドコントロールを掌握したり、データの抽出や Web トラフィックのリダイレクトを行ったりしています。しかしインターネットリクエストを再帰 DNS サービスで解決する場合、DNS は悪意のあるドメインや不適切なドメイン、IP をチェックしてブロックするのに最適な場所となります。セキュリティ侵害の兆候を把握する目的で DNS を監視していないセキュリティチームは、重要な機会を逃しているのです。

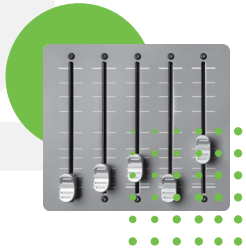
DNS は組織の中で最も貴重なデータソースの 1 つです。侵害を受けたシステムをセキュリティチームがより正確に検出できるように定期的なマイニングと脅威インテリジェンスの相互参照を行い、可視性とネットワークの保護を向上させる必要があります。IT セキュリティのリーダーはプロアクティブな DNS レイヤセキュリティをセキュリティ戦略の中核に据えるべきです。テレワークの従業員を狙った脅威を防御する手段として、DNS は最前線で優れた効果を発揮します。

3 段階のプロアクティブな DNS レイヤセキュリティ

1

ユーザーと悪意のあるドメインとの間の危険な接続をブロック

2



コマンドアンドコントロール (C2) コールバックとデータ漏えいを簡単に阻止

3

発生前に無力化することでセキュリティインシデントとアラートを低減

脅威を速やかに阻止する優れた方法

可視性を高め、リスクを（仕事の負担も）軽減

ほとんどの企業では、DNS 解決を ISP に依存してします。ところがテレワークの増加に伴って、組織ではインターネットへの直接接続が採用されるようになり、VPN を使わないでネットワークに接続するユーザーが増加傾向にあります。この行為は DNS の死角を生み出します。IP 接続の前に DNS 要求が実施されるため、DNS リゾルバは、接続プロトコルやポートにかかわらず、要求されたドメインをログに記録できます。後続の IP 接続に加えて DNS リクエストを監視することで、侵害を受けたシステムを正確に検出でき、セキュリティの可視性およびネットワーク保護を向上させることができます。

ここで重要なのは、IT セキュリティのリーダーは、セキュリティ運用を複雑にすることのない、より効果的なセキュリティ戦略を求めているということです。そこで効果を発揮するのが、DNS レイヤセキュリティです。

不可欠な DNS レイヤセキュリティ

DNS レイヤセキュリティは、攻撃がどれほど巧妙で独特であっても、必ずどこかに発信源があるという単純な原則に基づいて動作します。DNS レイヤセキュリティは、あらゆるポートやプロトコルを介して不審な「宛先」に送信される、すべてのリクエストを先制的にブロックすることで、コマンドアンドコントロールによるデータ漏えいや、悪意のある仮想通貨マイニング、ランサムウェアなどの攻撃を抑止できます。この方法では、そうした攻撃が持つ特定の性質を最初に識別しなければならないという厄介な問題もありません。不正なドメインは迅速かつ正確に不正ドメインと識別され、ブロックされます。

DNS レイヤセキュリティの特長

- 予測による悪意のあるホストの識別。日々数百億ものDNS リクエストや WHOIS レコード、ボーダー ゲートウェイ プロトコルのルーティング情報などの DNS 関連データを集約して分析することで、不審なドメインをきわめて高い精度で識別できます。
- クラウドサービスとしての DNS リクエストのブロック。クラウド サービス プロバイダーは、随時更新される不審なドメインのリストの提供を受けることでビジネスにとって脅威になりうるドメインや IP へのリクエストを先制的にブロックできます。

3 社のうち
1 社から

DNS[6] によってセキュリティ侵害を抑制できたと報告されています

1,000 ～
2,000 億ドル

という全世界での損失を、DNS[6] で防止できた可能性があります

他のセキュリティでは見逃す脅威も防ぐ DNS レイヤセキュリティ

Cisco Umbrella は DNS および IP レイヤでセキュリティを適用することにより、接続が確立される前にマルウェアやランサムウェア、フィッシング、ボットネットに対するリクエストをブロックします。また、あらゆるポートやプロトコルを利用した脅威がネットワークやエンドポイントに到達する前に阻止します。その過程で遅延が増加することもありません。また、ローミングユーザーを対象に、コマンドアンドコントロールへのコールバックによる直接 IP 接続をブロックすることもできます。こうした機能を備えた Cisco Umbrella はあらゆる場所にセキュリティを適用できるため、オンネットワークで勤務するユーザーとオフネットワークで勤務するユーザーが混在するポストコロナの世界に最適です。

Cisco Umbrella はあらゆるインターネット アクティビティを分類して保持しているため、脅威および攻撃の調査プロセスがシンプルになります。Cisco Umbrella Investigate のコンソールとオンデマンドのエンリッチメント API を使用することで、コンテキストに基づいてインシデントの優先順位を設定し、インシデントに迅速に対応することができるため、Cisco Threat Response で脅威の検出から復旧まで速やかに対処できます。

主要な DNS レイヤ セキュリティ ソリューションを対象に AV-TEST が実施した脅威検出テストでは、Cisco Umbrella は他ベンダーを凌駕するパフォーマンスを見せています。選択的プロキシを利用した場合の検出率は 70% を記録し、市場にある他社のソリューションと比較して 17% 以上効果的という結果が出ています。

AV-TEST: DNS レイヤでの保護におけるセキュリティ有効性テストの結果 [7]

ベンダー	検出率 | テストケースの数 3,572
Cisco Umbrella (選択的プロキシを使用する DNS レイヤ)	70.7%
Akamai Enterprise Threat Protector	53.6%
Infoblox BloxOne Threat Defense	36.3%

Cisco Umbrella のグローバルネットワークの強み

1 日あたり 6,200 億件の DNS リクエスト

全世界で 1 日あたり 5 億人のアクティブユーザー

900 を超える主要 ISP/CDN とのパートナーシップ

2 万を超える顧客

5 大陸に存在する 35 を超えるデータセンター

Cisco Umbrella を選ぶ理由

Cisco Umbrella は、ユーザー一人ひとりに対して、信頼性、速度の面で非常に優れたインターネット エクスペリエンスを提供することを約束します。ネットワークセキュリティおよび DNS サービスの業界大手であるシスコは、世界中があらゆるデバイスでインターネットに安全に接続できるよう支援しています。私たちはポストコロナの世界に向かって進んでいますが、Cisco Umbrella にはリモートワーカーもローミングワーカーも、オフィスワーカーも保護する、安心のバックグラウンドと技術の蓄積があります。

- **10 年以上にわたる DNS 領域でのリーダーシップ。** 13 年間に及ぶ DNS 技術とデータに関する実地での経験は、攻撃者のインフラストラクチャを理解しそれをブロックするという点に関して、大いなる利点を Cisco Umbrella にもたらしています。
- **DNS の卓越したデータ量と多様性。** Cisco Umbrella は卓越した可視性によって世界中の DNS のアクティビティを把握しています。Cisco Umbrella のグローバルネットワークは、世界 190 か国の 5 億人を超えるユーザーから送信される 6,200 億件のインターネットリクエストを処理しています。
- **予測型インテリジェンスと統計モデル。** Cisco Umbrella は高度に特化したモデルで 700 万もの悪意のある宛先を常時ブロックし、他のどのセキュリティプロバイダーよりも早くそれらを検出します。
- **高い復元力を備えたクラウド インフラストラクチャ。** Cisco Umbrella は 2006 年以来、稼働時間 100% という数値を誇っています。エニーキャストルーティングを使用し、全世界の 35 を超えるシスコのデータセンターに、同じ 1 つの IP アドレスでアクセスできます。リクエストは最も近い最速のデータセンターに透過的に送信され、フェールオーバーも自動的に行われます。
- **投資効果を増幅する統合。** Cisco Umbrella は、複数のセキュリティサービスを単一のクラウドプラットフォームに統合することで、ユーザーの場所を問わずインターネットへのアクセスを保護し、クラウドアプリケーションの使用を制御します。Cisco SD-WAN アーキテクチャや Cisco Meraki MR、Cisco Meraki MX および Cisco ISR ルータ、Cisco Secure Network Analytics (Stealthwatch)、および Cisco Secure Endpoint (Cisco Advanced Malware Protection) との統合により、ユーザーはインフラ全体のセキュリティポリシーの管理と適用を 1 つのダッシュボードで行えます。

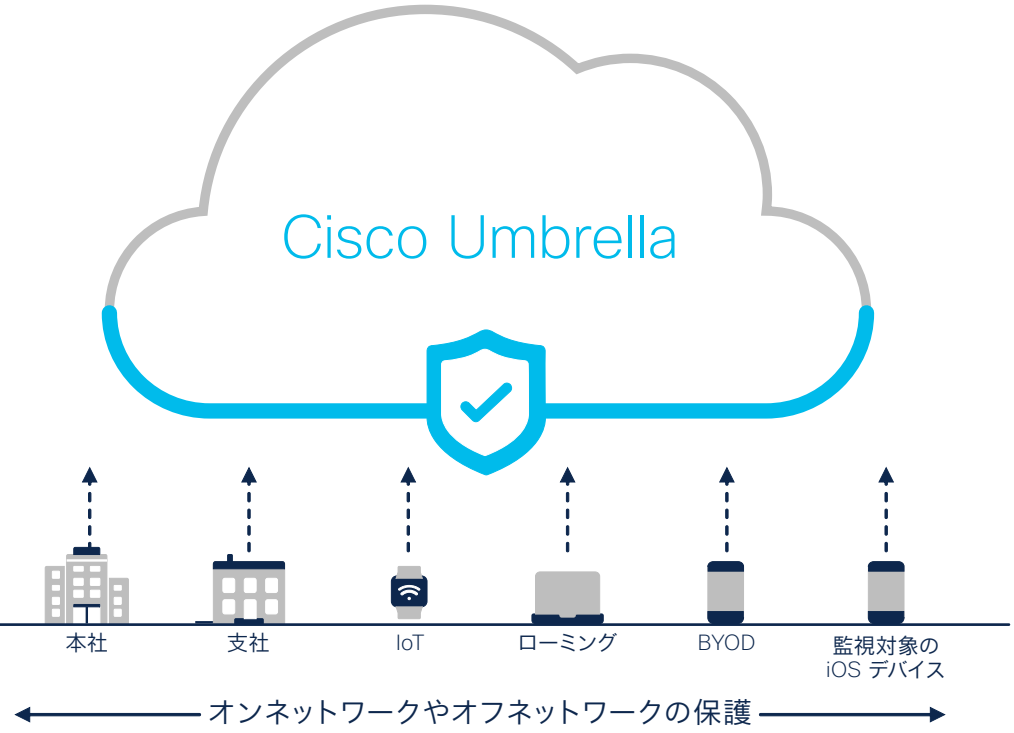
本社、支社、リモートオフィスへのセキュリティ施行

Cisco Umbrella は、民間企業としては世界最大規模の脅威インテリジェンスチームである Cisco Talos の卓越した脅威インサイトを活用することで、攻撃に利用されるさまざまな悪意のあるドメイン、IP、URL、ファイルを検出してブロックします。また、世界中から集められる膨大な量のインターネット アクティビティ データを、統計処理と機械学習を組み合わせたモデルに投入することで、インターネットに出現する新たな脅威を特定できます。

こうした独自の特長によって Cisco Umbrella は、専任のセキュリティ担当者がいない小規模企業から環境が複雑な多国籍企業まで、ポストコロナにあらゆる規模の組織を保護するのに理想的な選択肢となっています。Cisco Umbrella はオンネットワークとオフネットワークのどちらにもより効果的な保護とインターネット全体におよぶ可視性を提供し、リモート環境であるか否かにかかわらず全従業員のセキュリティを保ちます。

汎用性の高い最前線の防御

- すべてのインターネットトラフィックを監視
- 攻撃を早期にブロック
- 侵入したマルウェアの封じ込め
- Web サイトに対してコンテンツフィルタリングを簡単に適用可能
- クラウドアプリケーションの検出、管理、ブロックに対応
- コンテキストの把握による調査の円滑化



30 分であらゆる場所の従業員にセキュリティを適用

ポストコロナにおけるテレワークの従業員のセキュリティをシンプルに

コロナ禍により、これまで以上に柔軟な職場の形が求められる中、自宅やオフィス、外出先など、どの環境にいる従業員にも非常に迅速かつ簡単にセキュリティを適用できるのが Cisco Umbrella です。ハードウェアの設置やソフトウェアの手動更新が不要なため、日常的な管理がシンプルになります。DNS を Cisco Umbrella にリダイレクトする。それだけです。これで Cisco AnyConnect、シスコルータ (ISR 1K および 4K シリーズ)、シスコワイヤレス LAN コントローラ、Meraki MR/MX など、既存のシスコ製品を利用して、数千という単位のネットワークデバイスやラップトップを数分でプロビジョニングできます。シスコならリモートユーザーの保護も難しくありません。

Cisco Umbrella をぜひお試しください

数分で世界中の脅威を防ぐことができます。14 日間無料でお試しください。