Infoblox×TEDが提唱する テレワーク／在宅勤務を実現するために必要なDNSセキュリティとは

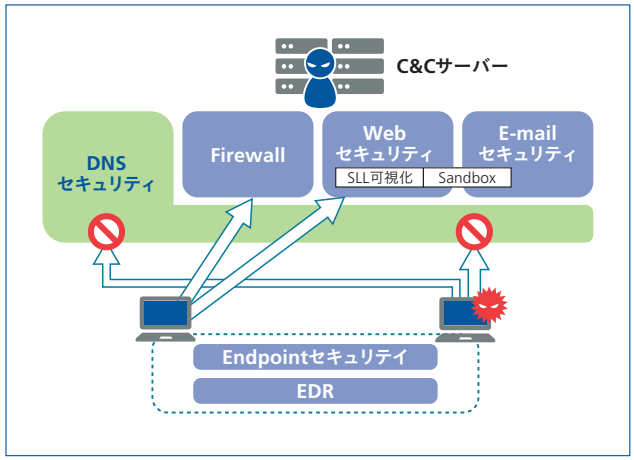
テレワークを推進するにあたって課題になるのがセキュリティだ。しかし、近年はクラウドサービスの利用が進んだことで対策も複雑になりがちである。そうしたなか、低コストで効率的なセキュリティを実現するアプローチとして注目を集めているのが「DNSセキュリティ」だ。

テレワーク／在宅勤務に有効なDNSセキュリティ

ICTを利用して時間や場所にとらわれない働き方を実現するテレワーク。社員の業務効率化と生産性向上を目的に、働き方改革の一環として採用する企業が増えている。「情報通信白書」（平成30年版）によると、テレワークの導入率は13.9%にとどまるが、ゆるやかな増加傾向にある。同白書によると、テレワーク導入企業のうち在宅勤務の導入率は29.9%、モバイルワークの導入率は56.4%、サテライトオフィスの導入率は12.1%となっている。

働き方改革関連法の施行もあり、関心も年々高まるテレワークだが、導入の際にはセキュリティをどう確保するかが課題になりやすい。総務省では「テレワークセキュリティガイドライン」などを公表して支援しているが、多くの企業が予算や手間、リソースの関係でなかなか有効なセキュリティ対策を実施できないのが現実だ。

そうしたなか、テレワークや在宅勤務のセキュリティでDNSの有効活用を提案しているのが東京エレクトロン デバイス（以下、TED）だ。同社は、2006年からDDI（DNS、DHCP、IPアドレス管理）セキュリティソリューション「Infoblox」を取り扱い、通信キャリアや官公庁、大規模企業などへ多数の導入実績を持っている。



DNSセキュリティは標的型攻撃を早い段階で遮断し、Webセキュリティやメールセキュリティの手前のDNSでブロック。91%以上のマルウェアが利用するDNS特有の通信での接続を遮断。またこの仕組みにより、他社セキュリティ製品群からSIEMに出力されるロギング量の軽減も実現する

では、なぜテレワークにDNSセキュリティが有効なのか。TEDによると、DNSセキュリティには、他のセキュリティ製品ではカバーできない領域をカバーしたり、導入/運用コストを最小限にしたりといった多くのメリットがあるという。また、低コストですぐに始められる点もDNSセキュリティの特徴だ。

低コストで効率がよくすべてのアプリを対象にできる

DNSセキュリティやInfobloxの有効性を知るためには、現在の企業を取り巻くビジネス環境でDNSがどのような位置にあるのかを知る必要がある。ポイントとなるのはクラウド環境の複雑化だ。

現在多くの企業はさまざまなクラウドサービスを併用している。例えば、オフィスサービスやファイル共有、チャットサービスなどだ。もっともこれらだけで業務が完結するわけではなく、社内環境で経理システムや生産管理システム、勤怠管理システムなどが稼働している場合が多い。

こうしたハイブリッドなクラウド環境でテレワークを実現しようとすると、社内ネットワークとクラウドネットワークという2つの異なるネットワークをそれぞれ管理する必要がでてくる。この点がテレワークのセキュリティを難しくしている。

例えば、テレワークで自宅からクラウドを利用する場合、VPNなどを使って社内とは異なる方法でセキュリティを確保しなければならない。メールやWeb、マルウェア対策などのセキュリティもそれぞれ実施する必要がでてくる場合もある。結果として、セキュリティ対策の手間やコストがかさんでしまうのだ。

これに対し、DNSセキュリティは、DNSサーバーの振り向け先を変えるだけでいい。コンピューターの通信は基本的にすべてDNSを利用するため、すべてのアプリケーションを対象にセキュリティ対策を容易に実施できる。

また、プロキシやファイアウォールは通信のすべてのペイロードを見るため処理が重くなるが、DNSクエリは接続先のみを見て判断するためパケットサイズが小さく大量に処理が可能という特徴もある。5G時代の大量トラフィックを迎えるいま、DNSセキュリティは最適なソリューションと言える。

このようにクラウド環境が複雑化するなか、低コストで効率がよく

すべてのアプリを対象としたセキュリティ対策を容易に実施できるのがDNSセキュリティなのだ。

DDI製品Infobloxだけが持つ2つの特徴的な機能

一方、セキュリティの観点からDNSを見ると、近年はDNSがセキュリティの盲点になっているケースが目立つ。ある調査によると、悪意のあるサイトへのリダイレクトやC&Cサーバーとの通信など、DNSを悪用するマルウェアは全体の91%に達しているという。また68%の組織はDNSの監視すらしておらず、46%の企業はDNSを悪用されたデータ漏えいを実際に経験しているという。DNSセキュリティを導入することは、こうしたセキュリティ上の盲点をふさぐ意味もあるのだ。

そうしたなかInfobloxは、DNSセキュリティのメリットを最大化し、他のソリューションでは実現できない2つの特徴的な機能を提供している。

Infobloxの基本的な機能は、DNSを用いて標的型攻撃を遮断したり、DNSトンネリングと呼ばれるDNSを利用した攻撃をブロックしたりするものだ。こうした機能は他のDNSセキュリティ製品でも提供しているが、Infobloxが特徴的なのは、マルウェアの検知においてシグネチャだけでなく、振る舞いベースでの検知が可能なことだ。Infobloxが自社提供する脅威情報とサードパーティの脅威情報を組み合わせ、20〜30分毎に最新情報に更新。1日平均150万件の怪しい宛先を新たに検出できる精度を持つ。

また、もうひとつの大きな特徴として、クラウドとオンプレミスの両方でサービスを提供できる点がある。テレワークのためのセキュリティを確保する場合、クラウドとオンプレミスそれぞれで対策が必要になることが多い。これに対し、Infobloxは、クラウドとオンプレミスを共通のDNSセキュリティの仕組みでカバーできる。

振る舞い検知と、クラウドとオンプレミスのハイブリッド構成ができるDNSソリューションは、他のソリューションにはないInfobloxだけの特徴だ。

機能	他社	Infoblox
シグネチャベースのDNSセキュリティ	あり	あり
振る舞いベースのDNSセキュリティ	なし	あり
自社製脅威情報	あり	あり
自社製脅威情報の1日あたりの新しい怪しいドメイン	6万以下	150万
サードパーティ製脅威情報	なし	あり
お客様作成脅威情報	不可	可能
DNSSEC（DNS通信の暗号化）対応	なし（DNSレコードの検証ができない）	あり
サービス形態	クラウドのみ	オンプレとクラウドの両方を提供

InfobloxによるDNSセキュリティの特徴

すべてのコネクテッドカーに DNSセキュリティを展開する大手自動車メーカー

Infobloxはこのほかにもさまざまな特徴的な機能を提供する。例えば、DNSだけでなくDHCP、IPアドレス情報を管理できるソリューションのため、インシデントレスポンスの際には、それらを「ネットワークコンテキスト情報」として、原因の早期特定や早期究明に役立てることができる。

また、ファイアウォールやSIEM、ID管理、マルウェア対策など、ほかのセキュリティ製品とAPIを通じて連携できるため、セキュリティ運用の自動化や自動復旧といった、「SOAR（Security Orchestration, Automation and Response）」として活用できる。

クラウドサービス利用の増加によりWANの見直しが必要な際には、ネットワークの可視化や制御、ローカルブレイクアウトといったSD-WANのソリューションとしての活用も可能だ。

こうしたInfobloxの機能を有効活用している欧州の大手自動車メーカーがいる。同社は、社内ITセキュリティとコネクテッドカー向けセキュリティとして、4万台のエンドポイント（コネクテッドカー）と、16万台の社内システムのエンドポイントでDNSソリューション「BloxOne Threat Defense」を採用。今後、同社で生産される自動車全てにInfobloxのDNSセキュリティが搭載される予定だ。

TEDのサポートがテレワーク／在宅勤務を後押し

TEDでは、Infobloxの提供とオンサイトサポートを全国12拠点で提供する。20年近い日本展開の実績で培ってきたスキルとノウハウにより、的確かつ迅速なQA対応が可能だ。また、Infoblox製品を専任で担当するエンジニアや日本語ベースの手順書の配布、トレーニングなど、万全のサポート体制を構築している。

テレワーク／在宅勤務を採用する企業は今後ますます増えていく。効果的なセキュリティ対策を実施していくことは、テレワークを成功させるための1つのポイントでもある。InfobloxによるDNSセキュリティのアプローチは、多くの企業にとってテレワーク／在宅勤務を実現するための有効な選択肢になるはずだ。

東京エレクトロン デバイス株式会社
CN BU
https://cn.teldevice.co.jp/

新宿：〒163-1034 東京都新宿区西新宿3-7-1 新宿パークタワー S34階
Tel.03-5908-1990 Fax.03-5908-1991

大阪：〒540-6033 大阪府大阪市中央区城見1-2-27 クリスタルタワー33階
Tel.06-4792-1908 Fax.06-6945-8581

名古屋：〒451-0045 愛知県名古屋市西区名駅2-27-8 名古屋プライムセントラルタワー8階
Tel.052-562-0826 Fax.052-561-5382

つくば：〒305-0033 茨城県つくば市東新井15-4 関友つくばビル7階
Tel.029-848-6030 Fax.029-848-6035

お問い合わせは、Webサイトの下記フォームよりお願いします。
https://cn.teldevice.co.jp/product/infoblox/form.html

September.2019