社会環境の変化から生じる脅威と
クラウド型セキュリティゲートウェイの有効性

近年、多くの企業でワークスタイルの変革が求められ、テレワークの導入や活用の期待も増加しており、さまざまな働き方を考慮した業務環境の体制整備が重要視されています。

本書では、このような業務の効率化や通信傾向の変化に対する方法のひとつとして、クラウド型セキュリティゲートウェイの有効性について、(株)サイント 岩井氏に解説頂きました。

皆様のセキュリティ対策の一環として、ご一読頂けますと幸いです。

社会環境の変化から生じる脅威とクラウド型セキュリティゲートウェイの有効性

～ 時代の潮流からのセキュリティ対策の一考察 ～

株式会社サイント
代表取締役　岩井博樹

IT環境の変化に伴う脅威の変遷と認識の変化

「サイバー攻撃により機密情報が大量流出」といったセキュリティ事故が紙面を賑わすことが減っていると思いませんか？これは事故自体が減っているのではなく、被害企業が気づいていない（もしくは、そのフリをしている）ことが殆どです。その原因は、社会環境の変化に伴い、サイバー攻撃の手口自体が巧妙化したことに他なりません。現在の日本におけるサイバーセキュリティ対策の多くは、クラウドコンピューティングの普及前の時代から引き継いだものです。サイバー領域における脅威は、IT技術の変化と共に変遷するのが一般的です。その観点では、今私たちは、サイバー攻撃の認識を含めてアップデートしなければならない時期に来ています。その一つが、多様化するオフィス環境に伴い変化するリスク対応です。

サイバー攻撃対策を検討する上で、米ロッキードマーチン社がサイバー攻撃における攻撃者の行動を構造化したフレームワーク「サイバーキルチェーン[1]（Cyber kill Chain®）」の考え方は非常に参考になるものです。同フレームワークを参考にセキュリティ対策を検討した企業も少なくないはずです。このサイバーキルチェーンは、発表から今年で丸10年が経過しました。この歳月は、サイバー領域における脅威の変遷の点においては十分過ぎるものであり、一部のセキュリティ研究者らは、同フレームワークのアップデートの必要性を説いています。その背景として、サイバー攻撃動向の変化がありますが、要因の１つとして各国ともに社会環境の変化が影響していることは容易に想像が付きます。

例えば、７月発表された「認知攻撃ループ[2]（Cognitive Attack Loop）」のようなサイバー攻撃の永続性について説いた攻撃ループの考え方があります。これは、端的に説明すると、サイバー攻撃は目的達成後も、サイバーキルチェーンの一連の流れから抜け出ずに、将来のために標的ネットワークに潜伏し続けるといったものです。これは、攻撃者が標的企業の環境を継続的に調査し、標的企業のネットワークの変更やオフィス環境などを熟知したうえでマルウェアを巧妙に設置することで実現しています。

煩雑化するセキュリティ対策の勘所

IT技術の進歩によりオフィス環境の変化は、マルウェアなどの脅威の侵入経路へも影響を与えました。身近な例では、BYOD（Bring your own device）の利用や在宅勤務制度の利用などはその典型です。また、PaaS（Platform as a Service）やSaaS（Software as a Service）などのクラウドサービス関連のセキュリティ事故も、社会環境の変化が影響したものです。さらには、近年話題となっているソフトウェアのアップデートサーバが踏み台として悪用される「サプライチェーン攻撃」も、10年前は無かった侵入経路です。

何よりも、あらゆるシステムがインターネットに接続されることが前提の社会となってからは、多くのシステムは「暗黙の信頼」で囲まれていることが近年最大の変化です。

---

[1] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[2] https://www.carbonblack.com/resources/threat-research/cognitions-of-a-cybercriminal/

クラウドサービスの普及やBYODの利用の増加は、効率性やコスト削減のメリットがある反面、シャドーITの横行やセキュリティ運用の煩雑化といったデメリットがあります。その一例として、オフィス環境に対するセキュリティ機能の設計と実装とに乖離がある場合が挙げられます。企業が適切に管理のできない箇所でのセキュリティ事故の発生は、発覚までに時間を要し、最悪の場合は事業運営への影響も予想されます。このようなケースは、新たに構築した外部のオフィス環境でしばしば見られます。

このような実状を勘案しますと、近年のセキュリティ対策は、如何に業務システムを一定水準以上のセキュリティ強度を確保するかが課題となります。

従来のセキュリティ対策においては、このような課題に対し、IT運用管理ツールやウイルス対策ソフトウェアが一般的でした。しかし、これらのソフトウェア自体がサイバー攻撃の標的となり始めており、システムの外側での対策も併せて検討する必要が出てきました。

例えば、下図のような環境下において、侵入経路は数多く存在することがわかります。特に多くの組織が頭を悩ませているのは、BYODや自宅PCなどの管理や、外部環境に設置されているサーバ群などへのアクセス管理などです。つまり、これらの端末からサーバ群や企業ネットワークへのアクセスを許可し、さらには企業内と同等のセキュリティ強度を満たす実装の実現が理想的であると言えます。

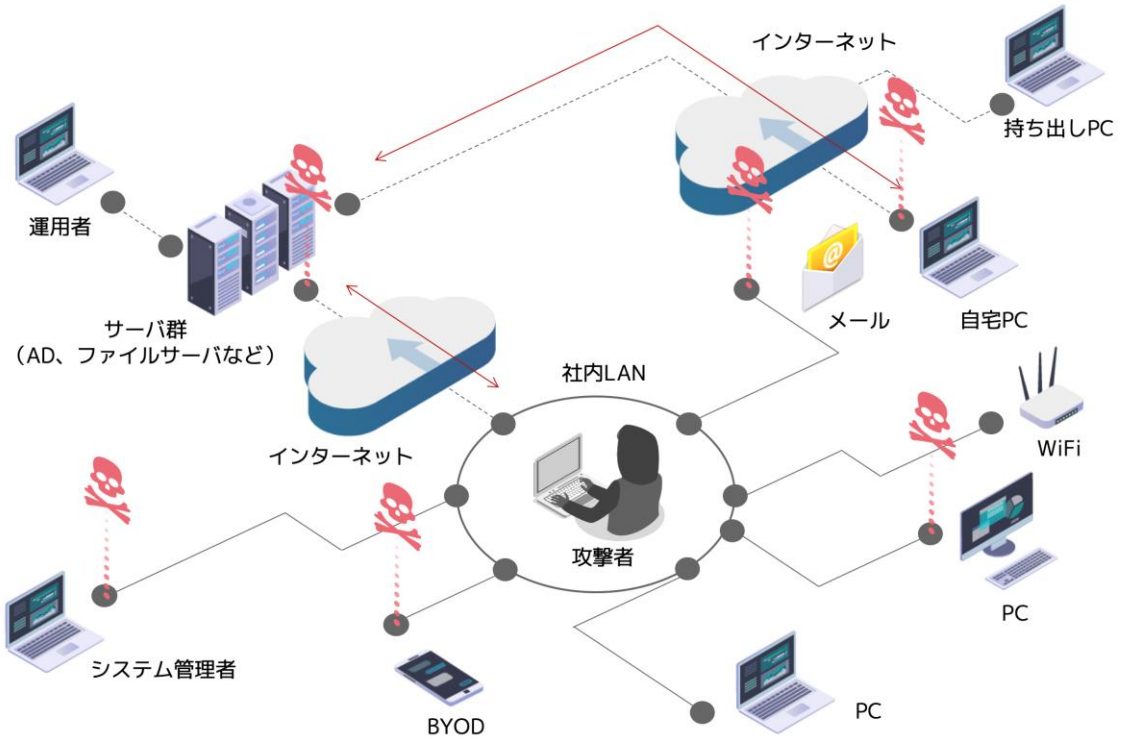

図 近年のIT環境と侵入経路イメージ

多様化するオフィス環境に求められるクラウド型セキュリティゲートウェイ

どのようなセキュリティ対策を実装すれば、現在のサイバー攻撃に耐えうるのでしょうか。まず、現在のサイバー攻撃手口で代表的な経路はメールとウェブです。特にウェブコンテンツは、広告配信に代表されるように、外部からコンテンツを取得していることも珍しくありません。さすがに全てのウェブコンテンツの検査を実施している組織は限られており、セキュリティ製品や外部サービスにお任せすることが現実的です。さらに、ウェブサイトの閲覧やメールの送受信と密接な関係にあるDNSを悪用した攻撃まで考慮しますと、個人や一企業でセキュリティ対策を講じることは中々ハードルが高いと言えそうです。

例えば、次のようなウェブ経由のサイバー攻撃を想定してみますと、意外に対策が厄介であることに気付きます。

・フォームジャッキング（悪性コードを入力フォームが含まれるページに挿入し、機微情報を窃取する攻撃）

・マルバタイジング（広告に悪性コードを挿入しネットワーク広告として配信する攻撃）

・水飲み場型攻撃（標的が習慣的に閲覧するウェブサイトからマルウェアを配信しようとする攻撃）

いずれも企業が一般的に実装しているセキュリティ対策に加え、ウェブブラウザのバージョン管理、設定管理、ユーザのITリテラシーや個別の対策などがなければ、これらの攻撃を未然に防ぐことは難しいと思います。加えて、在宅勤務などの異なる環境下のユーザが企業内と同じセキュリティポリシーの下で対策を行うなど、難易度が高いのではないでしょうか。

このような状況で、解決策の１つとして、クラウド型セキュリティゲートウェイがここ数年で注目を浴びています。その理由の一つは、前述した多様化するオフィス環境への対応が容易だからです。特に、私見ではありますが、下表の機能はどのような環境下のユーザにおいても対策しておきたいところです。

表 クラウド型ゲートウェイでオススメの対策例

No	機能	備考
1	ファイアウォール ウイルス対策	ファイアウォールは必須の機能です。端末上のファイアウォール機能は、マルウェアや場合によっては管理者の設定不備などにより無効化される可能性があります。
2	DNSセキュリティ	DNSハイジャックをはじめとし、DNSを悪用したサイバー攻撃は度々話題となります。
3	SSLインスペクション	通信の暗号化は攻撃者もセキュリティ製品回避に利用する典型的な手口ですので、SSLの復号機能は多くのサイバー攻撃に対して効果的です。
4	サンドボックス	正規ファイルにさえマルウェアが混入される時代です。実行ファイルや特定のファイル拡張子のファイルは、サンドボックス上で安全確認ができると安心です。
5	ウェブアクセス コントロール	脆弱なウェブブラウザの利用は攻撃者の思う壺です。ユーザごとに好みのウェブブラウザが異なり管理が難しいだけに、一定のセキュリティポリシーを適用したいところです

まず、No.1にファイアウォールとウイルス対策について説明します。実は、私がサイバー攻撃被害を受けた企業にインシデント対応支援に伺いますと、被害システム上のファイアウォールやウイルス対策ソフトウェアが無効化されていることがままあります。攻撃者からすれば、これらのセキュリティ製品の無効化は、マルウェアを潜伏するうえで重要な操作です。この点を考慮しますと、これらの機能は外部にもあるとセキュリティ強度は一層高まると考えられます。

次に、No.2のDNSセキュリティですが、殆どのユーザはネームサーバの存在を特に意識せずにインターネットへ接続しています。つまり、DNSが悪用されたサイバー攻撃被害には気付かない可能性が高いのではないでしょうか。これらのリスク軽減のためにもDNSセキュリティは重要と考えます。

No.3のSSLインスペクション（SSL/TLSの復号化）は、マルウェアの利用する通信の暗号化への対策の他に、シャドーIT対策の観点でも重要であることは言うまでもありません。この機能は、UTMや次世代ファイアウォール製品などにも搭載されている機能ですが、課題としてパフォーマンスの低下がしばしば指摘されていました。同機能がクラウド上で処理されることで、十分なパフォーマンスが期待できることからも、利用価値は高いと考えます。

No.4のサンドボックスは、ウイルス対策ソフトウェアでは検出ができない、もしくは悪性判定が難しいファイルを利用するうえでの確認に役に立ちます。

最後に、No.5のウェブアクセスコントロールですが、これはかなり重要な機能だと思います。しばしば、業務システムの都合で古いバージョンのウェブブラウザの利用を要求する企業を見かけますが、言語道断です。特にウェブ経由でのサイバー攻撃の多くは、ウェブブラウザによるアクセスがトリガーとなるわけですから、しっかり管理すべきソフトウェアの１つだと考えます。

これらの機能を、あらゆる環境下の端末へ一度に実装することができるのは、クラウド型セキュリティゲートウェイの一番の魅力ではないでしょうか。

まとめ

インターネット経由でのデータ管理が一般化し、様々な環境下にあるシステムとの接続が「暗黙の信頼」を前提に行われています。さらに、働き方改革に代表されるように、オフィス環境が多様化し、サイバー領域におけるリスクは増大し続ける一方です。従来は、VPNなどを利用し企業ネットワークへ接続させることで一定のリスク軽減を図ることが一般的でした。しかし、やはり企業内のシステムと同等のセキュリティ対策を実装することは、難しいことが現実です。攻撃者はこの点をうまく利用し、企業ネットワーク外の端末を標的とし、結果的に標的企業の機微情報へアクセスを行いはじめました。

これらの課題に対し、１つの解決策としてクラウド型セキュリティゲートウェイが注目されています。どのような環境下においても一定のセキュリティ機能が実装できることは多くの企業において魅力ではないでしょうか。また、クラウドでのサービスは新たな機能をリアルタイムに実装することができることは、移り変わりの早いサイバーセキュリティ対策では大きなメリットになります。変わりゆく近い未来での社会環境や脅威を見据えてのクラウド型セキュリティゲートウェイの利用の検討は、事業運営とセキュリティの両立を目指す先進的な企業においては１つの選択肢となると思います。

著者紹介

岩井博樹

2000年に大手セキュリティ企業でセキュアサイト構築やセキュリティ監視業務、デジタルフォレンジック業務を担当する。2013年より大手監査法人系のセキュリティ企業へ入社し、技術コンサルティングや脅威インテリジェンスに関連した業務に従事する。
2018年に国内初のインテリジェンスベンダーとして株式会社サイントを設立する。
対外活動として、経済産業省などのセキュリティ関連委員、政府系セキュリティ技術アドバイザー、日本シーサート協議会 専門委員などを精力的に行う。著書として、「動かして学ぶセキュリティ入門講座」「標的型攻撃セキュリティガイド」などがある。