アンラボ・セキュリティレター

Press Ahn

2020.05　Vol.77

ポスト・パンデミック、非接触時代のセキュリティソリューション

コロナウイルスとセキュリティ

ポスト・パンデミック、非接触時代のセキュリティソリューション

リモートワーク、リモート授業、リモートセミナー……

私たちは、これまでは特殊な状況において、ごく少数のための補助的な手段だと考えていた非対面業務環境が、より多くの環境で適用が可能であることがわかった。コロナウイルスの状況で、企業はビジネスの継続性のためにこのような非対面業務環境をサポートする様々なソリューションとサービスを急いで導入した。この過程の中で、一部のソリューションではセキュリティの脆弱性が明らかとなり、これを狙った悪質な攻撃も増加した。しかし、パンデミックの状況ではセキュリティとガバナンスよりもビジネスの継続性が優先せざるを得なかった。しかし、セキュリティこそが時間や場所にとらわれず、業務の生産性とビジネスの継続性を確保するための基本的なインフラであることは、看過できない事実である。ポスト・パンデミック時代では、企業はデジタルトランスフォーメーション加速化のためのクラウド移行、非対面システムの拡充などに、より拍車をかけるものと予想される。現時点では、これまで適用できていなかったセキュリティ衛生(Security Hygiene)の問題を改め、セキュリティを強化するための改善策を準備しなければならない。この記事では、今後加速化していく非接触時代、セキュリティ衛生を強化するアンラボのセキュリティソリューションには何があるかを探っていく。

非接触時代のネットワークセキュリティ

コロナウイルスが長期化し、在宅勤務を行う企業が増えているなか、仮想プライベートネットワーク(VPN)が必須のセキュリティソリューションとなってきている。VPNは、外部からでも社内のイントラネットやデータベースなどにアクセスすることができるため、VPNが構築されている企業は在宅勤務に切り替えるのが容易である。

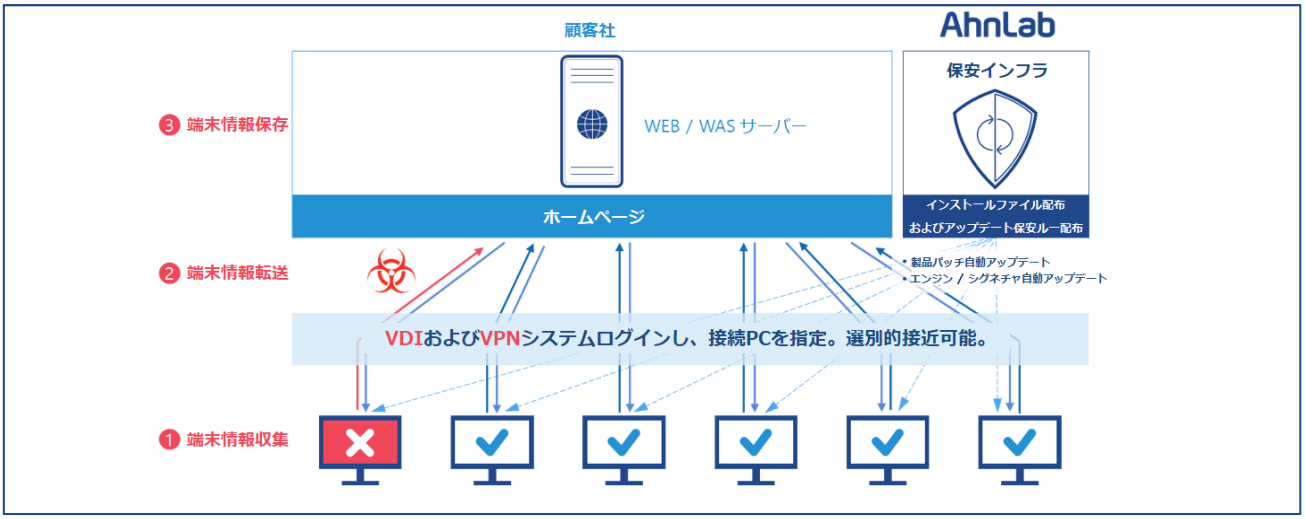
アンラボは、次世代ファイアウォールの「TrusGuard」においてVPN機能を提供している。コロナウイルスのように急速なリモートワークが必要となる状況では、従来のVPNの拡張または新規構築が最も実用的であり現実的な方法だが、TrusGuardを活用すればリモートワーク環境でも社内ネットワーク水準のセキュリティを構築できる。

[図1] リモートワーク必須ネットワークソリューション、AhnLab TrusGuard

アンラボのTrusGuardは、ファイアウォール、IPS、アプリケーションコントロール、VPN、アンチウイルス/迷惑メール、C&Cの検知および遮断など、様々なセキュリティ機能を提供する次世代ネットワーク統合セキュリティシステムである。特にアプリケーションコントロールを搭載することで、APTなど複雑化した最新のセキュリティ脅威に悪用されているP2P、Webハード、インスタントメッセンジャー、SNSなどの数百にわたるアプリケーションデータに対するリアルタイム分析および行為の制御機能を提供する。

非接触時代のエンドポイントセキュリティ

在宅勤務にはSSL VPNが主流だが、暗号化通信がより重要である。外部端末、家庭用PCなどの識別が不可能な端末の場合、セキュリティに脆弱性が生まれる可能性がある。



[図2] AhnLab Safe Transaction 端末情報収集機能

アンラボのセーフ・トランザクション(AhnLab Safe Transaction、ASTx)は、端末情報収集機能によって外部の識別された端末のみアクセスを可能にする。これにより、Webサービスの利用時に発生しうる様々な脅威とハッキング要因に対し、強力なセキュリティ機能を提供する。また、収集された情報は暗号化を通して機密性と完全性を保障する。このほかにも、キーボードセキュリティによってユーザーの取引情報、個人情報などの主要コンテンツの流出や改ざんを防止するだけでなく、マルウェアの検知、ネットワーク遮断、脆弱性の遮断、フィッシング/ファーミング遮断などの総合的なセキュリティ機能を提供する。

社内にアクセスする外部端末の一層強化されたセキュリティを考慮している企業であれば、AhnLab MDSも検討する価値がある。

[図3] AhnLab MDSを活用した端末保安強化

MDSエージェントは、VPN(Virtual Private Network)、VDI(Virtual Desktop Infrastructure)によって内部資産にアクセスする外部端末にインストールされ、3つの重要な端末セキュリティ機能を提供する。この3つの機能は、▲端末PCのリアルタイム監視によって新種・変種のマルウェア感染を事前に遮断▲感染の疑いがある端末の隠されたマルウェアの検出、および収集▲OSおよびアプリケーションの脆弱性を利用して発生する悪性行為の自動遮断などである。

グローバル市場調査機関のIDCによると、70%のセキュリティ侵害事故はエンドポイントで起こっており、エンドポイント・モニタリングとセキュリティが台頭している状況である。これにより、エンドポイントでEPP(エンドポイント保護プラットフォーム)とEDR(エンドポイントでの検出と対応ソリューション)が代案として浮上してきている。

[図4] AhnLab EPP & AhnLab EDR 構築概念図

次世代エンドポイント保護プラットフォームであるAhnLab EPPは、単一エージェント、単一コンソールを基盤として、様々なエンドポイント保護ソリューションの有機的な連携を提供する。有機的なエンドポイントセキュリティ管理および運用によって、強力で効率的な脅威への対応を提供する。また、エンドポイント脅威の検知、対応ソリューションであるAhnLab EDRは、エンドポイント領域に対する持続的なモニタリングを通して脅威の可視性を提供することにより、潜在的な脅威の事前予防効果を提供し、様々なセキュリティソリューションとの有機的な連携によって更に強力なセキュリティを実現することが可能だ。

企業内のPCがマルウェアに感染した場合、ネットワークを通じて全社に伝播し、ネットワークの麻痺や主要な情報の流出などの大規模被害が発生する恐れがあるが、企業の有形・無形資産の損失を最小限にするためには、企業用統合PCセキュリティソリューションであるAhnLab V3 Internet Security 9.0が適当である。V3 IS 9.0は、企業ユーザーのシステムを安全に保護することにより、クライアントPCを安心して使用できるようコンピューティング環境を実現し、企業の情報資産を保護する。

POS/キオスクなど非対面システムのセキュリティ

パンデミック以降、POS機器やキオスクを活用した注文決済を超えて、無人化・自動化の波には逆らえない状況となっている。しかしながら、ランサムウェアを通じてPOS機器やキオスクなどでカード情報を盗む攻撃も非対面システムにおいては頻繁に発生している。ダークウェブで取引されているカード情報は、銀行識別コードをはじめとして有効期間、カード暗証番号などを含んでいるが、主にPOSやキオスク、ATM機器などの決済会社システムのセキュリティ脆弱性を利用して流出するケースが多い。POSやキオスクなどは一般的なPCとは全く異なるオペレーティング環境で運用されているにも関わらず、従来のPC環境と同じセキュリティシステムを導入する場合が多く、複雑化した脅威に対して脆弱性があるためだ。

[図5] AhnLab EPSを活用したセルフサービスシステムの保安強化

Ahnlab EPSは、POSシステム、キオスク、重要サーバーなどの特殊目的用途のシステムに最適化した超軽量セキュリティソリューションであり、アンラボ独自のホワイトリストおよびマルウェア遮断技術を基盤として、運用システムに必要なプログラムの実行とネットワーク接続のみを可能にすることにより、不必要なプログラムまたは非業務プログラムの実行をブロックし、マルウェアの侵入やマルウェアによる情報流出を根本的に防止する。

現在、この製品は大型ディスカウントマート、デパート、コーヒー専門店などの大型流通業者の決済システムや鉄道、空港、バス停留所に設置された交通案内電光掲示板などのようなキオスクにおいて検証されたセキュリティソリューションによって運用されている。

非接触時代のセキュリティ監視サービス

企業が在宅勤務ソリューションの導入を推進するなかでSSL VPNを検討しているが、急いで構築したリモートワークのシステムでは、かえってハッカーの攻撃対象になりやすい。また、SSL VPNを導入して在宅勤務システムを構築しても、例外的なイベントが発生するかどうかの24時間のモニタリングが必要であり、ログファイルの管理やアプリケーションのアップデートなど、管理とメンテナンスは必須である。セキュリティインフラを構築して管理する人材がいないため、在宅勤務の導入を考えている企業は、セキュリティコンサルティングが24時間のモニタリング、技術サポートのサービスをあわせて提供するセキュリティ監視サービスの導入も検討すべきだろう。

アンラボのリモートセキュリティ監視サービスは、24時間のモニタリング、ポリシー設定、侵入の検知、分析、対応など、企業が継続的に行うべき一連のセキュリティシステム運用の委託を受けて提供するものである。ファイアウォール、IDS/IPS、UTM、WAF監視サービスおよびDDoS防御サービスを基本として提供し、付加的にアンチスパム、メッセージセキュリティ、脆弱性管理、システムハードニング、侵害事故分析、模擬ハッキングサービスなどを提供する。

特にアンラボは、AWS、Azure、IBMクラウドなどの主要クラウドサービスプロバイダとのパートナーシップを通じてクラウドセキュリティ監視サービスを提供しており、様々な産業群からのクラウドセキュリティ監視顧客を確保し、安定した運用能力を認められている。また、アンラボはオンプレミス環境に提供している情報保護コンサルティングをクラウド環境のために最適化して提供し、クラウドサービスのセキュリティ認証などのコンプライアンス遵守のためのコンサルティングサービスを提供している。

リモート、在宅勤務におけるセキュリティのための実践心得

コロナウイルスの影響により、リモートまたは在宅勤務を行う企業が増加している。これを契機として、リモート・在宅勤務の活性化に対する期待感も高まっており、リモート・在宅勤務を成功に導くための情報保護策が必要な時である。下表は、科学技術情報通信部が発表した「コロナウイルスの影響による在宅勤務時に遵守すべき6つの情報保護実践心得」である。

ユーザー実践対則	保安管理者実践対則
1. 個人PC最新保安アップデート - 在宅勤務の時に個人PCを使用する場合はOSおよびアプリケーションプログラムを最新で維持	1. 在宅勤務システム（VPN）使用勧奨 - 社内保安政策によるVPN使用 - 未保有企業の場合は社内網接続PCのアンチウィルス最新化および随時点検政策実施
2. アンチウィルスのアップデートおよび検査 - アンチウィルス保安パッチ最新アップデートおよび定期的なウィルス検査（リモートワーク接続前および一日1回以上）実施 - アンチウィルス自動アップデート設定およびリアルタイム検査機能解除禁止	2. 在宅勤務対象者の保安指針準備および保安認識を高める - PCの運用体制、ソフトウェア、アンチウィルス最新化、ルーターパスワード設定、ウェブサイト利用自制など保安指針準備および教育実施
3. 家庭用ルーター保安設定（パスワード）および私設WI-FI・共用PC利用自制 - 家庭用ネットルーターを最新ソフトウェアにアップデータし、ルーターのパスワード設定 *パスワードは類推できないように特殊文字などを含む - 個人営業場（カフェ、食堂など）に設置された私設のWI-FI・共用PCを利用して在宅勤務自制	3. 在宅勤務者のユーザーアドレスおよび接続権限管理 - 在宅勤務者のパスワード設定強化および在宅勤務の場合接近検眼を最小化方案準備 - 在宅勤務システム接続しパスワード以外にOTPなど2次認証手段適用必要
4. 会社メール勧奨、個人メール使用注意 - 会社で提供するメールサービス使用勧奨 - 商用メールサービス使用の場合は目的外メール閲覧自制およびURL・ファイル実行注意 *共用PCでメール閲覧後、必ず接続終了	4. 一定時間不在し、ネットワーク遮断 - 在宅勤務者が社内ネットワーク接続後、不在する場合はネットワーク接続遮断設定 *10~30分間不在の場合遮断勧奨
5. 不必要なウェブサイト利用自制 - 業務以外の個人目的ウェブサイトは接続自制	5. リモート接続モニタリング強化 - 在宅勤務者の社内ネットワーク接続現況管理および迂回接続集中モニタリング実施
6. ファイルダウンロード注意（ラムサムウェア感染注意） - メールまたはウェブブラウザを通じてファイルをダウンロードする場合、ラムサムウェア感染可能性があるので、出所が疑わしいファイルはダウンロード禁止 - 業務ファイルは別途のストレージに定期的にバックアップ実施	6. 個人情報、企業情報などデータ保安（ラムサムウェア感染注意） - 企業の重要書類の場合はDRM設定などデータ流出防止対策準備 *データ外部流出の場合は管理者の承認手続きなど - 在宅勤務者の作業ファイル内部搬入の場合はラムサムウェア感染可否などファイル検査必要 - 重要企業のデータはバックアップ勧奨

このセキュリティの心得は、現在国内の一般企業の環境において必ず遵守すべき基本内容を盛り込んでおり、これをサポートするセキュリティソリューションを備えているかどうか、もう一度確認すべきである。さらに、企業ではデジタルトランスフォーメーションの転換によりSASE(Secure Access Service Edge、セキュアアクセスサービスエッジ)、CARTA(Continuous Adaptive Risk&Trust Assessment)のようなソリューションフレームワークを導入するための戦略も策定すべきである。

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)