アンラボ・セキュリティレター

Press Ahn

2021.3　Vol.87

在宅勤務時のセキュリティ方案、アンラボの答えとは？

在宅勤務環境におけるセキュリティ方案

在宅勤務時のセキュリティ方案、アンラボの答えとは？

前回、Press Ahn の2月号である「アンラボの2021：顧客とクラウドを見据えて」にて、デジタルニューノーマルのうちの1つである在宅勤務 (Work From Home、WFH) と、これに対するセキュリティ問題について言及している。新型コロナウイルス感染症の影響を受け、非対面 (アンタクト) トレンドが加速化することで、密集度の高いオフィス環境をもつ企業の従業員らを中心に、在宅勤務への需要が増えている。変化する環境下でビジネス資産を守るため、関連セキュリティの必要性もまたクローズアップされている。

では、在宅勤務環境におけるセキュリティはどのように構築するべきか？ありきたりな質問ではあるが、そう容易には答えられないこの問いに対し、今回の記事ではアンラボの回答を紹介していく。

在宅勤務は、セキュリティ統制がおろそかになる他ない"外部"で行われるため、情報流出等のセキュリティ問題への懸念が常に存在している。より具体的に、次の3つの内容を説明しよう。まず、外部端末は物理的統制が相対的に不足するため、紛失または盗難時に端末内のデータが流出する危険がある。さらに、社内共用の有・無線ネットワークを介し内部ネットワークにアクセスすることも、セキュリティを脅かす要素の1つだ。最後に、内部資源に対するリモートアクセスの面からも、不正アクセスなどの脅威が懸念されている。

このように、在宅勤務環境下では様々な経路から脅威が発生・流入してくる。アップデートを適用しない場合、アプリケーションの脆弱性が増加し、新・変種マルウェア感染へのリスクが上昇する。よって、企業にとって端末の管理負担は当然のごとく加重される。

もし、攻撃者がこうした弱点を悪用し攻撃に成功すると、情報流出はもちろんのこと、システム破壊、ビジネス中断など、深刻な打撃を被ることもある。長期的な観点からブランドイメージの低下にもつながるだろう。業務システムへのアクセス前後に関わらず、セキュリティ強化が常に必要とされる理由はここにある。

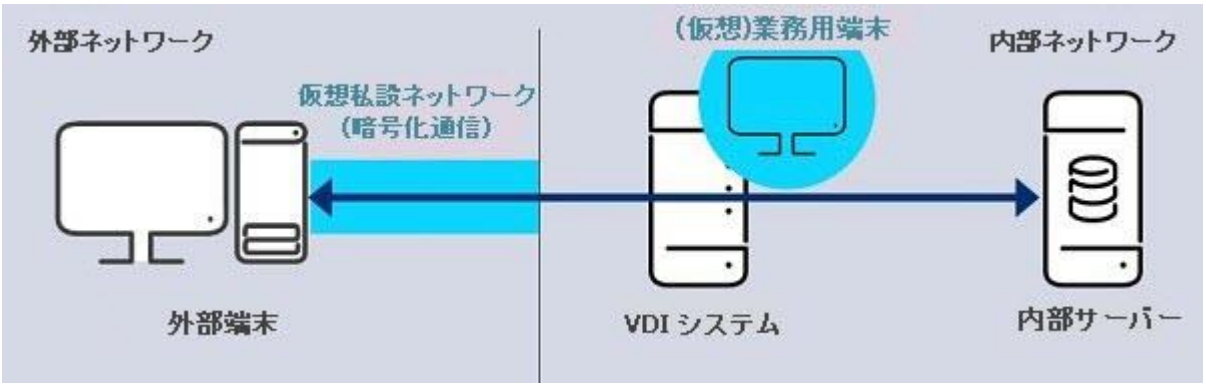
在宅勤務時のリモートアクセス形態

内部ネットワークへのリモートアクセス方式は、「間接アクセス」と「直接アクセス」の2つに区分できる。これはリモート業務の特性と、会社内の環境によって選択することが可能だ。この2つのアクセス方法に関する定義と特徴を簡潔に説明しよう。

間接アクセス方式

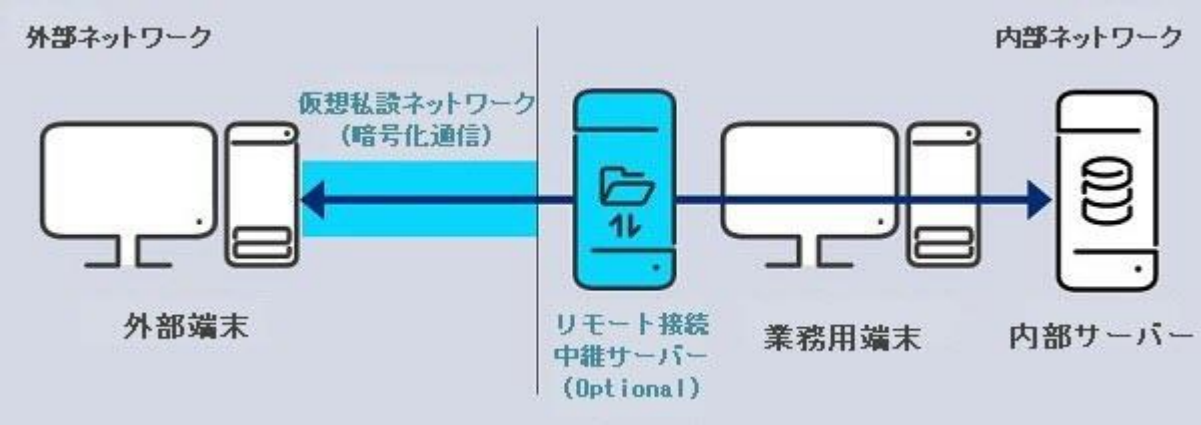
まず間接アクセスとは、外部端末から社内の業務用端末を経由し、内部ネットワークにアクセスすることを言う。仮想デスクトップ(VDI)、もしくはリモートアクセスプログラムの使用によって、そこからさらに2つの方式に区分される。

VDI 方式とは、外部端末から VDI の仮想業務用端末を経由し、内部ネットワークにアクセスするものだ。VDI は社内公開ネットワーク、または内部業務ネットワークに位置づけされ、DaaS (Desktop as a Service) 等のインターネットクラウド基盤の VDI サービスも活用することが可能である。外部端末ではない仮想業務用端末にて業務を処理し、外部端末には仮想デスクトップのイメージのみが表示される。



[図1] 仮想デスクトップ基盤 (VDI) 方式の構造図

リモートアクセスプログラム方式とは、外部端末から業務用端末にリモートアクセスプログラムを利用しアクセスすることである。外部端末および業務用端末間の直接アクセスや、別途のリモートアクセス中継サーバーを介したアクセスも可能だ。VDI とは違い、仮想ではなく実務端末にアクセスし業務を処理するのが特徴である。

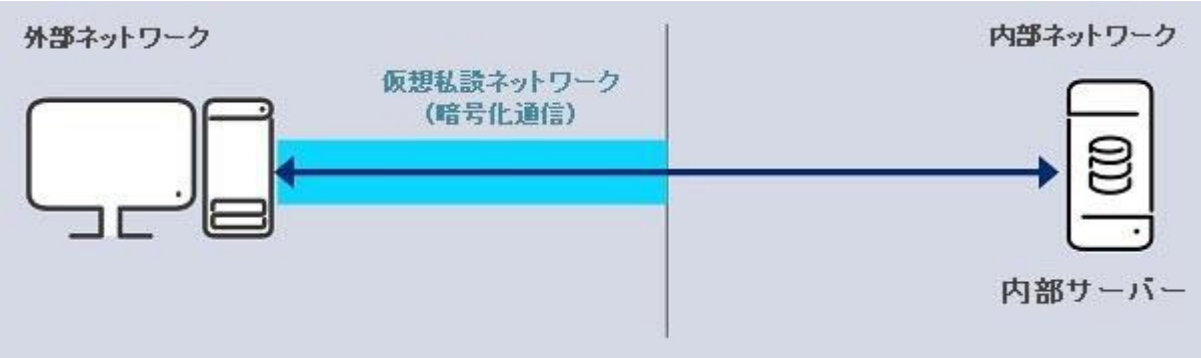


[図2] リモートアクセスプログラム方式の構造図

直接アクセス方式

直接アクセスとは、外部端末から内部業務用端末を経由せず、内部サーバー等に直接アクセスする方式だ。外部端末にて業務を処理する際、業務データが外部端末内にすぐさま保存されるため、情報流出等のセキュリティ問題に格別な注意が必要である。

※ 直接アクセス方式を用いる際の外部端末には、個人端末よりも、会社側で強制的なセキュリティ統制が可能な会社支給端末を使用するべきだ。



[図3] 直接アクセス方式の構造図

在宅勤務環境におけるアンラボのセキュリティ方案

アンラボは、直接および間接アクセスに対するセキュリティ方案をすべて提供している。ワクチンプログラムの設置、APT 遮断対策の樹立、安全なオペレーティングシステムの使用等、各分野ごとのセキュリティニーズを満たしていたこれまでの方式から、統合管理を具現する方向にセキュリティプロセスを進化させた。

特に、アンラボの次世代ネットワークセキュリティソリューションである「AhnLab TrusGuard」および「EPP Security Assessment (ESA)」間を連動し、それをもとに在宅勤務環境におけるセキュリティ力を強化した。TrusGuard VPN のクライアントを実行する際、連動した ESA 上で行われるセキュリティ事前スキャンを通過した外部端末は、VPN 接続が許可される。また、事前スキャン結果で「注意」と判断された外部端末の場合、セキュリティ脆弱性に対するソリューションを提供する。

アンラボの間接アクセスセキュリティ方案

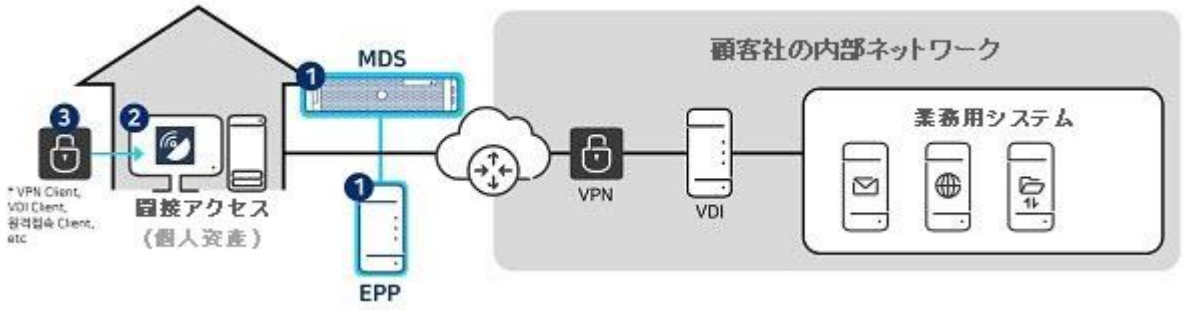
アンラボは、間接アクセスに対し2つのセキュリティ方案をサポートしている。すべて3段階で構成されており、そのうち1段階と2段階に関しては同様の内容だ。

1段階目では、間接アクセスの端末管理用として「AhnLab Endpoint Platform (EPP)」を外部ネットワークに構築し、MDS サーバーを構成する。また、構成後は V3、EPP、ESA、EPP Patch Management (EPM) ポリシーの設定を行う。その後、間接アクセス端末管理のための統合エージェントを準備する。このエージェントは、VPN クライアントの設置時に統合設置を行う必要があるのだが、その統合エージェントの設置が次の2段階目の項目となる。統合エージェントは、EPP エージェント、V3、ESA、EPM、MDS エージェントで構成されている。

最後の3段階目は、それぞれのクライアント、またはサーバー上で事前スキャンを行う以下の2つの方法に分けられる。

第1案 : Client to ESA 連動構成

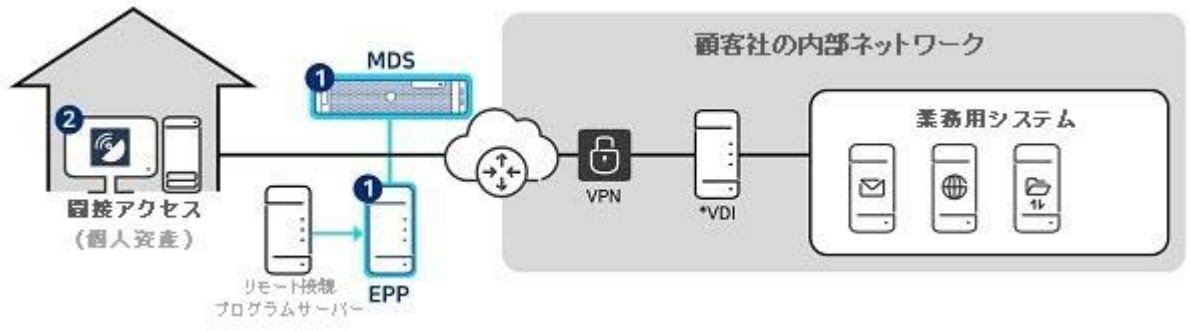
第1案は、間接アクセスのためのクライアント(VPN、VDI、リモートアクセスプログラム等) 上で事前スキャン後、アクセス許可を行う方式だ。これを具現化するためには連動が必要となってくる。この場合、クライアントにて ESA 前回デバイスチェックの点数を確認するのだが、クライアントの提供企業側が連動システムを開発・適用しなければならない。アンラボの場合、ESA 連動のための API を提供している。前回デバイスチェックの点数が低い場合、VPN 接続が遮断される仕組みだ。



[図4] 間接アクセスのセキュリティ方案 - Client to ESA 連動構成の概念図

第2案 : Server to EPP 連動構成

第2案の場合、間接アクセスのためのサーバー(リモートアクセスプログラムサーバー、VDI サーバー等) 上で事前スキャン後、アクセスを許可し連動が必要となる。この場合、間接アクセスプログラムサーバーにて EPP に保存された端末の ESA 前回デバイスチェックの点数を確認する。同様に、間接アクセスプログラムの提供企業が連動を開発・適用しなければならず、アンラボの場合 EPP 連動のための API を提供している。前回デバイスチェックの点数が低い場合、こちらもリモートアクセスプログラムへの接続が遮断される。



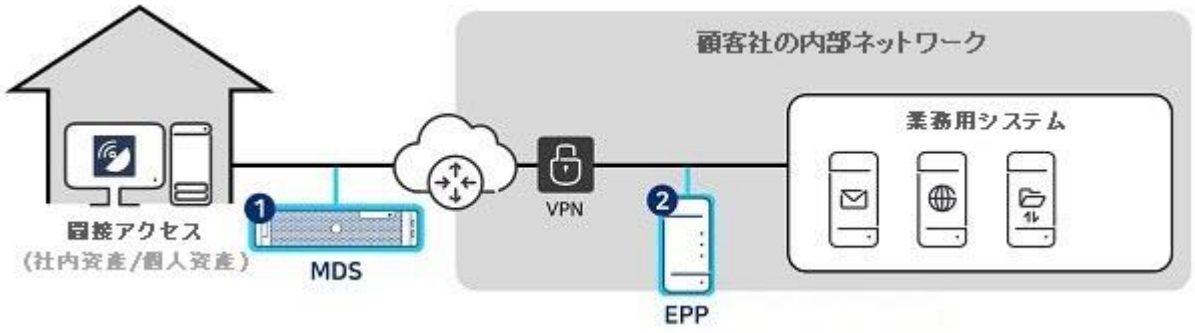
[図5] 間接アクセスのセキュリティ方案 - Server to EPP 連動構成の概念図

アンラボの直接アクセスセキュリティ方案

直接アクセスにに対するセキュリティ方案は2段階で構成されており、その流れは間接アクセスの内容とさほど変わらない。

1段階目では、直接アクセスの端末管理用 EPP を内部ネットワークに構築し、MDS サーバーを構成する。EPP の場合、既存の EMS も活用することが可能だ。その後 V3、ESA、EPM ポリシーの設定を行い、統合エージェントを準備する。

2段階目も同様に、EPP エージェント、V3、ESA、EPM、MDS エージェントで構成された統合エージェントの設置を行うのだが、VPN クライアントを設置する際、ともに統合設置を行う必要がある。



[図6] 直接アクセスのセキュリティ方案概念図

安全な在宅勤務、その答えはプラットフォームに

幅広いセキュリティポートフォリオを保有するアンラボは、ソリューション間の統合・連携を行うことで、プラットフォーム形態のセキュリティカを提供する。各ソリューションが独立的に機能するのではなく、大きな枠組みでのセキュリティプロセス構築に向け、シナジー効果の創出が可能だ。在宅勤務時のセキュリティも同様に、エンドポイントセキュリティプラットフォームの「AhnLab EPP」を中心とした複数のソリューションが、状況や段階に応じて的確な性能を発揮する。

下記の表は、在宅勤務に関するセキュリティ上の考慮点、およびアンラボの全般的な対応案を整理したものだ。

接続方式	区分	対応方案	製品
共通 (間接&直接)	ワクチンプログラムの設置	V3 インストールおよびEPPを介した V3 管理	EPP、V3
	APT 遮断対策の樹立	MDSを介した APT 遮断対策の適用	MDS
	安全なオペレーティングシステムの使用	ESA を介した安全なオペレーティングシステムのチェック	EPP、ESA
	セキュリティパッチ必須適用	ESA を介したセキュリティパッチの適用状況チェックおよび対応 EPM を介したセキュリティパッチの適用状および EPP を介したパッチ管理	- EPP - ESA、EPM
	ログインパスワードの設定	ESA を介したローカルセキュリティポリシーチェックおよび対応	- ESA、EPM
	スクリーンセーバーの設定	ESA を介したスクリーンセーバーの設定チェックおよび対応	EPP、ESA
	リモート接続する場合、 セキュリティ対応の事前スキャン	ESA を介した情報セキュリティ必須事項を事前スキャン	EPP、ESA
間接アクセス	内部ネットワークにアクセスする場合、 インターネット遮断	V3 オフラインファイアウォール機能を介したインターネット遮断	EPP、V3
直接アクセス	インターネット接続を常に遮断	V3 ファイアウォール機能を介したインターネット接続遮断	EPP、V3

[表] 在宅勤務時のセキュリティにおける考慮点、およびアンラボの対応案

在宅勤務は、今後ますます一般化することが予想される。そのため、読者の一人一人がセキュリティ遵守項目を熟知し、対応プロセスを構築することで、ビジネス資産を効果的に保護してもらいたい。

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)