アンラボ・セキュリティレター

Press Ahn

2021.10　Vol.94

中小企業をハッキングから遠ざける方法

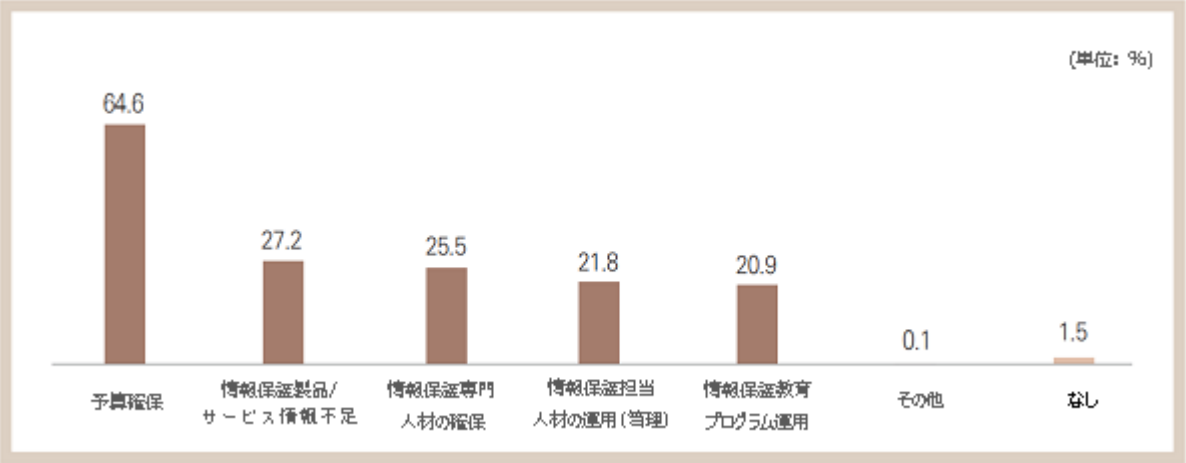
中小企業をハッキングから遠ざける方法

大企業に比べ、中小企業のセキュリティは比較的脆弱だ。そのため、ハッカーの主要ターゲットとなりやすく、攻撃頻度も増加の一途をたどっている。セキュリティの重要性については、徐々に中小企業側にも認知されてきている。しかし、それにも関わらず、様々な制約により、セキュリティを構成する上で困難に直面し頭を悩ませているのが実状だ。

今回は、中小企業にとってネックとなるセキュリティへの問題点を紐解き、正しいセキュリティへのアプローチ法や、アンラボの中小企業向けのカスタマイズソリューション「AhnLab V3 Security for Business」の価値、そして導入事例を紹介していく。

韓国インターネット振興院 (KISA) が発刊した「2021 国家情報保護白書」によると、組織内で情報保護を管轄・運営している韓国内の民間企業は、13.4% にしか満たないことが判明した。また、この 13.4% のうち、87.7%もの割合を占めていたのは、250 名以上からなる大規模事業体であった。このことから、ほとんどの中小企業がセキュリティを組織的に運営できていないという事実が読み取れる。

セキュリティを運営するにあたり悩みを抱える一番の理由に、「予算」が挙げられた。情報保護における難点を問う項目では、「予算確保」が 64.6% と最も高く、「情報保護専門人材の確保 (25.5%)」、「情報保護担当人材の運用 (21.8%)」など、専門性や人材に関する回答も高い割合を占めた。



[図 1] 情報保護にあたり感じる難点 (出典： 韓国インターネット振興院)

統計を基に実際の状況を見てみると、大多数の中小企業は、1 名もしくは 2 名の IT 担当者がセキュリティを管理している。しかし、この IT 担当者にとってセキュリティは、複数ある主要業務のうちの「1 つ」でしかない。社内の IT サポート、インフラ管理など、様々な業務を並行しているためだ。前述の統計にもあったように、セキュリティ専門の人材確保が難しい中、たとえ人材を採用したとしても、セキュリティ業務だけに集中できる企業環境を整えることは、そう容易ではない。

一方、ハッカー側が積極的に攻略するのは、比較的セキュリティが脆弱な中小企業である。韓国ランサムウェア侵害対応センター (RanCERT) が、2019 年上半期を基準にランサムウェアの業種別被害現況を分析したところ、中小企業 (43%) および小規模企業者 (25%) の被害率が、大企業 (1%) を遥かに上回る結果となった。世界的に多くの注目を集めるのは、規模の大きな機関・企業を狙ったサイバー攻撃の被害事例である。しかし、実際の攻撃頻度を見てみると、圧倒的に母数の多い中小企業を狙った攻撃が高い割合を占めていることがわかる。

中小企業のセキュリティ力を底上げするためには、長期的なセキュリティ認識の向上、人材養成、ポリシー強化など、制度面での改善が必要となる。しかし、ここで最も重要なのは、制約のある現在の企業環境で最善のセキュリティ方案を設け、すぐにでも起こりうるサイバー脅威から自社を守ることだ。虎視眈々と攻撃の機会を狙うハッカーは、企業側がセキュリティ態勢を整えるまで待ってはくれない。

こうした観点から、セキュリティに悩みを抱える中小企業が知っておくべきハッキングの経済性原理や、中小企業向けのセキュリティソリューションにおけるニーズを紹介する。

セキュリティの経済性原理：ハッカーも手間がかかることは避ける

一般的に"セキュリティ"を考える際、「どうすればハッカーの攻撃を防ぐことができるのか？」という、防御側の受動的な視点で考えがちだ。これを能動的な視点に切り替えると、次のような質問を投げかけることができる。「どうすればハッカーの攻撃を手間のかかるものにできるのか？」

能動的な視点をもって対応し、セキュリティ脅威の防御に成功したケースがある。「電子金融詐欺予防サービス」がその例だ。2000 年代から 2010 年代の序盤にかけて、最も代表的なセキュリティ脅威の一つは、インターネットバンキング (銀行サービスアプリ) を狙ったマルウェアであった。 防御のための多大な努力もむなしく、金銭的被害が減ることはなく、毎週のように数十万個の新たなマルウェアが配布されていた。

当時、政府や金融機関では、電子金融詐欺予防サービスの実施を全面的に推し進めていた。電子金融詐欺予防サービスとは、公認認証書 (現在は廃止された認証方式) の発行、もしくは一定金額以上を振込む場合、指定された端末でのみ振込みを可能にし、電話やメッセージか

ら再度本人認証を行うよう施行された政策である。この政策が誕生して以降、わずか数カ月の間でセキュリティ脅威が大幅に減少した。その理由は至ってシンプルである。ハッカーが攻撃を成功させることが難しくなったからだ。

上記のケースのように、サイバー攻撃に対し一番効果のある対策案は、攻撃側を最も困らせる方法を見つけることだ。現在のような高度化したサイバー攻撃は、組織化・分業化され行われている。ここで言う攻撃側を最も困らせる方法とは、攻撃する上で多くの時間と資源を投入せざるを得ない状況を作ることだ。市場理論に基づき、攻撃の経済性を悪化させることがポイントとなる。

攻撃側の立場から見ると、現在のサイバー環境は攻撃対象や脆弱箇所が無数に存在する。その上、攻撃対象に定めたターゲットのセキュリティまでもが手薄だったとしたらどうだろう。狙った利益を簡単に手にできる状況で、攻撃を敢行しない理由はないはずだ。限られた資源でセキュリティを構築する中小企業の場合、各自の企業環境にあった最善のセキュリティ態勢を整えることで、自らを難易度の高い攻撃対象にし、ハッカーの攻撃優先順位から自社を遠ざける必要がある。

では次に、中小企業が攻撃側の経済性を悪化させるには、一体どのような方法があるだろうか？まず、アンラボを含めた様々なセキュリティ企業は、常日頃からセキュリティルールの遵守を勧告してきた。ネット上で疑わしいファイルをダウンロードしない、怪しいメールの添付ファイルを実行しない、定期的にセキュリティパッチを行うなどのルールを守ることで、ほとんどの攻撃を予防することができるからだ。

このように、セキュリティルールをしっかりと守った上で、さらに検証されたセキュリティソリューションのサポートを受ければ、自社のセキュリティをより一層強化することが可能だ。月刊セキュリティレター・Press Ahn 9 月号の「EDR 導入後の変化」で記述した通り、セキュリティ技術は攻撃の発展にあわせ進化を繰り返している。そして、その進化が反映されたソリューションが市場にリリースされるのだ。企業環境にあわせ、検証済みのソリューションを導入し正しく運営することで、組織自身が遥かに難易度の高い攻撃対象となれる。

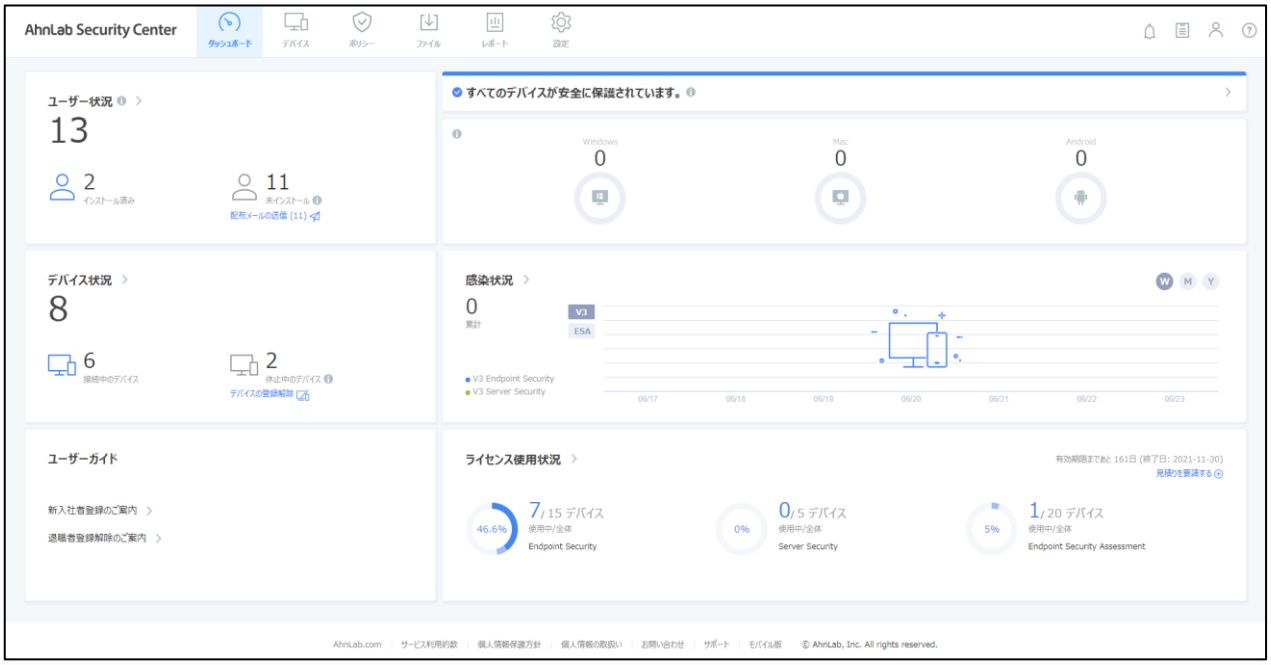
一つ付け加えると、セキュリティソリューションを活用した場合、最初の攻撃を防ぎきれなくとも、追加で発生する被害を最小限に食い止めることが可能だ。一つの例として、ここ数年の間話題となっている「持続的標的型攻撃 (Advanced Persistent Threat：APT)」がある。この脅威は、第一段階の攻撃を成功させた後、内部システムの掌握、情報流出など、段階ごとに細分化され、長期にわたり攻撃を仕掛けてくるのが特徴だ。

APT 攻撃が脅威とされる理由に、被害が一通り発生した後でないと、実際に侵入された事実を発見できないことが挙げられる。セキュリティソリューションの導入により、侵入事実をより迅速に発見し流入経路を遮断することで、内部システムの掌握や情報流出など、追加の被害発生を抑えることが可能だ。こうすることで、攻撃側が多くの資源や労力を投入し、第一段階の攻撃を成功させたとしても、最終目的を果たせないため、攻撃における経済性の低下に繋がる。

中小企業向けのセキュリティソリューションに求められるのは？

中小企業向けのセキュリティソリューションは、基本的に強固なセキュリティを提供した上で、中小企業が直面している現実的な導入課題を解決する必要がある。上記で言及した中小企業にとってネックとなるセキュリティへの問題点をまとめてみると、▲限られた人材、▲少ない予算、▲専門性の不足などが挙げられるだろう。これらをセキュリティソリューションに当てはめると、「セキュリティ専門の人材ではない一般の IT 管理者でも、合理的なコストで手軽に運営が可能であるべき。」という結論に至る。

アンラボはこうしたニーズを反映し、2020 年 9 月、中小企業向けの SaaS 型セキュリティソリューション、「AhnLab V3 Security for Business」をリリースした。この製品は、アンラボが数十年かけ培った技術力とノウハウ、その全てが集約されたアンチウィルスソリューション「V3」をベースとしている。そのため、「AhnLab V3 Security for Business」は最も重要なセキュリティ技術面において、業界随一の技術力を誇る。また、別途で管理サーバーを構築することなく、企業環境や使用用途に応じて、製品ライセンスを購入後すぐに使用できる。さらに、利便性の高い管理機能がサポートされているため、非専門家でも手軽にセキュリティ運営が可能だ。



[図2] AhnLab V3 Security for Business ダッシュボード

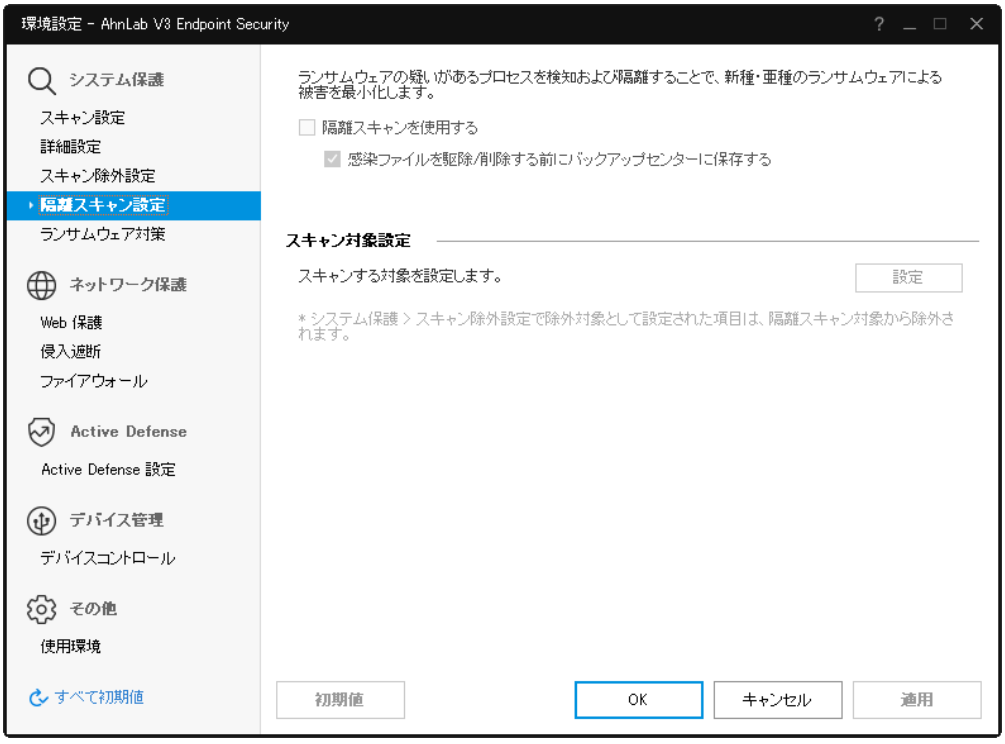
「AhnLab V3 Security for Business」は、中小企業の IT 環境を考慮し、最適化したセキュリティをサポートする 3 種類のソリューションで構成されている。具体的には、「V3 Security for Business：PC・ノートパソコン用統合セキュリティ管理ソリューション」、「V3 Server Security：サーバー専用セキュリティソリューション」、そして「Endpoint Security Assessment：社内 PC 脆弱性点検ソリューション」である。さらに、統合マネジメントを担う「AhnLab V3 Security for Business Center」により、社内機器全般のセキュリティや、使用状況を一目で把握することが可能だ。

まず、「V3 Security for Business」は ▲Windows および Mac OS の新・亜種マルウェア防御、▲有害 / フィッシング Web サイトおよびネットワークの侵入遮断、▲社内 PC の最適化および管理など、社内の PC・ノートパソコンに対する統合セキュリティ管理機能を提供している。「V3 Security for Business」を活用することで、ランサムウェアや各種新・亜種マルウェア、ネットワークへの侵入を図る行為など、様々な脅威から全社の PC・ノートパソコンを安全に保護・管理することができる。

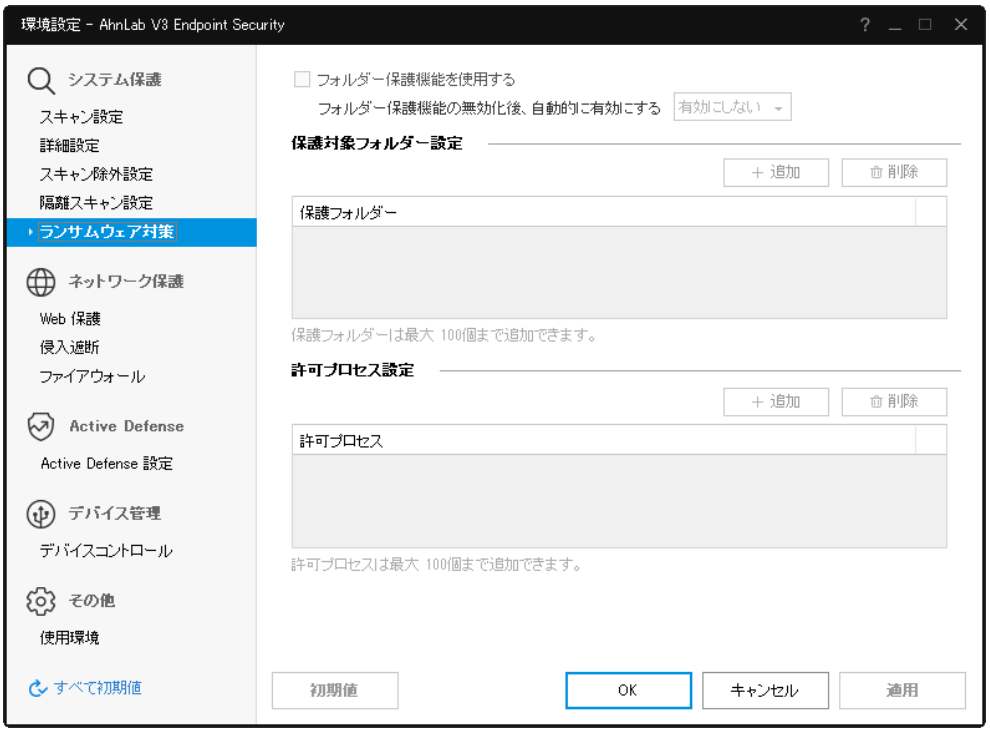
続いて、「V3 Server Security」は ▲Windows / Linux ベースのサーバーに対する強固なセキュリティ、▲サーバー運営環境別の手動・スケジュールスキャン、▲直観的なユーザー画面 (UI) など、強力で便利なセキュリティ機能を提供する。従来のサーバー管理に難点を感じていた IT 担当者も、「V3 Server Security」を活用することで、手軽かつ安定的にサーバーセキュリティを運営することが可能だ。

また、「Endpoint Security Assessment」の場合 ▲社内 PC の脆弱性管理 (定期・不定期)、▲中小企業に最適化したセキュリティ点検チェックリスト、▲OS / SW セキュリティパッチ点検など、組織の PC・ノートパソコンに対するセキュリティ点検機能を提供する。担当者は「Endpoint Security Assessment」を活用し、企業環境に最適化した PC 脆弱性点検ポリシーを設定・実行することができる。

この他にも、「AhnLab V3 Security for Business」は脅威の代表格とされるランサムウェアに関しても、隔離スキャン、フォルダーやファイルの変造・暗号化防止など、強固なセキュリティ機能をサポートし顧客企業を保護してくれる。



[図3] 隔離スキャンによる新種ランサムウェアへの対応



[図4] フォルダー保護機能による重要ファイルの保護

上記の各種機能は、ランサムウェアへの対応がベースとなる、アンラボ「マルチレイヤード (Multi-Layered)」のセキュリティ技術を基に具現化された。「AhnLab V3 Security for Business」を含めた V3 製品ラインナップには、アンラボのアンチランサムウェアツールが適用されている。これにより、フィッシングメールの添付ファイル、または有害サイトから流入する疑わしいファイルの検知や、ASD (AhnLab Smart Defense) クラウドシステムを介した安全性の診断が可能だ。安全性が確保されていないファイルは、PC 内の仮想環境で実行し、安全を確認することでランサムウェアへの感染を予防する。

顧客から見た「V3 Security for Business」の長所

「AhnLab V3 Security for Business」は今年 7 月、リリース後わずか 10 ヶ月で 2 千件余りの顧客企業を確保し、市場への早期安着に成功した。中小企業がこれほどまでに積極的にアンラボのソリューションを導入する理由とは何か？

「AhnLab V3 Security for Business」を実際に使用している、Web エージェンシー社「bstones (ビストンス)」のソル・ドンウク デジタル事業部本部長は、ソリューションの最大長所として、セキュリティを一目で管理できる利便性と、アンラボの差別化されたセキュリティ技術力を挙げた。導入前、ソル・ドンウク本部長は、企業環境上セキュリティに全力を注ぐことができない状況で、顧客企業および提携企業の情報流出防止、社内機器のランサムウェアセキュリティ、派遣職の多い事業状況を考慮したセキュリティ管理に悩んでいた。そんな中、「AhnLab V3 Security for Business」の無料体験後、最終的に導入を決断したと語る。

ソル・ドンウク本部長は、ソリューションを使用した感想や長所について、「検証されたアンラボ V3 のセキュリティ力だけでなく、セキュリティ専門家でなくとも手軽にセキュリティ管理が行える利便性、そして合理的なコストが中小企業の立場から見た最大の長所。」であるとし、「社内機器の全体的なモニタリングをサポートしてくれる 'AhnLab V3 Security for Business Center' により、セキュリティプログラムの配布・管理も便利に行え、リモートワークの環境作りも安心して行えるようになった。」と述べている。

この他にも、様々な産業グループの顧客企業が「AhnLab V3 Security for Business」について、中小企業のニーズがしっかりと反映されており、セキュリティ運営の負担が大幅に減ったと評価している。また、管理上の利便性、ブランドへの信頼、ニーズにあわせた統合レポートなどに関しても共通して満足の声を上げている。

► AhnLab V3 Security for Business の顧客事例を詳しく見る

終わりに

ビジネス環境が益々デジタル化していくこの時代、中小企業にのしかかるセキュリティへの負担はさらに大きくなっている。こうした状況で、効果的なセキュリティを構築し、ビジネスのサステイナビリティ (持続可能性) を守るためには、経済性原理に基づき、「攻撃側に手間をかけさせ、攻撃の優先順位から遠ざかる」という能動的なアプローチ法を堅持し、基本的なセキュリティルールを徹底して守る必要がある。加えて、「AhnLab V3 Security for Business」のような中小企業向けに最適化したセキュリティソリューションを活用すれば、最小限のサポートで最大限のセキュリティ効果をもたらし、組織的なセキュリティシステムを確立することが可能だ。

実際の様々な制約によりセキュリティに悩みを抱える中小企業が、正しいセキュリティ戦略を樹立し合理的なソリューションを導入することで、大切なビジネス資産を安全に保護していけることを願う。

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)