

アンラボ・セキュリティレター

Press **Ahn**

2021.5 Vol.89

なぜアンラボはクラウドに力を注ぐのか



顧客に必要不可欠なクラウド力を提供

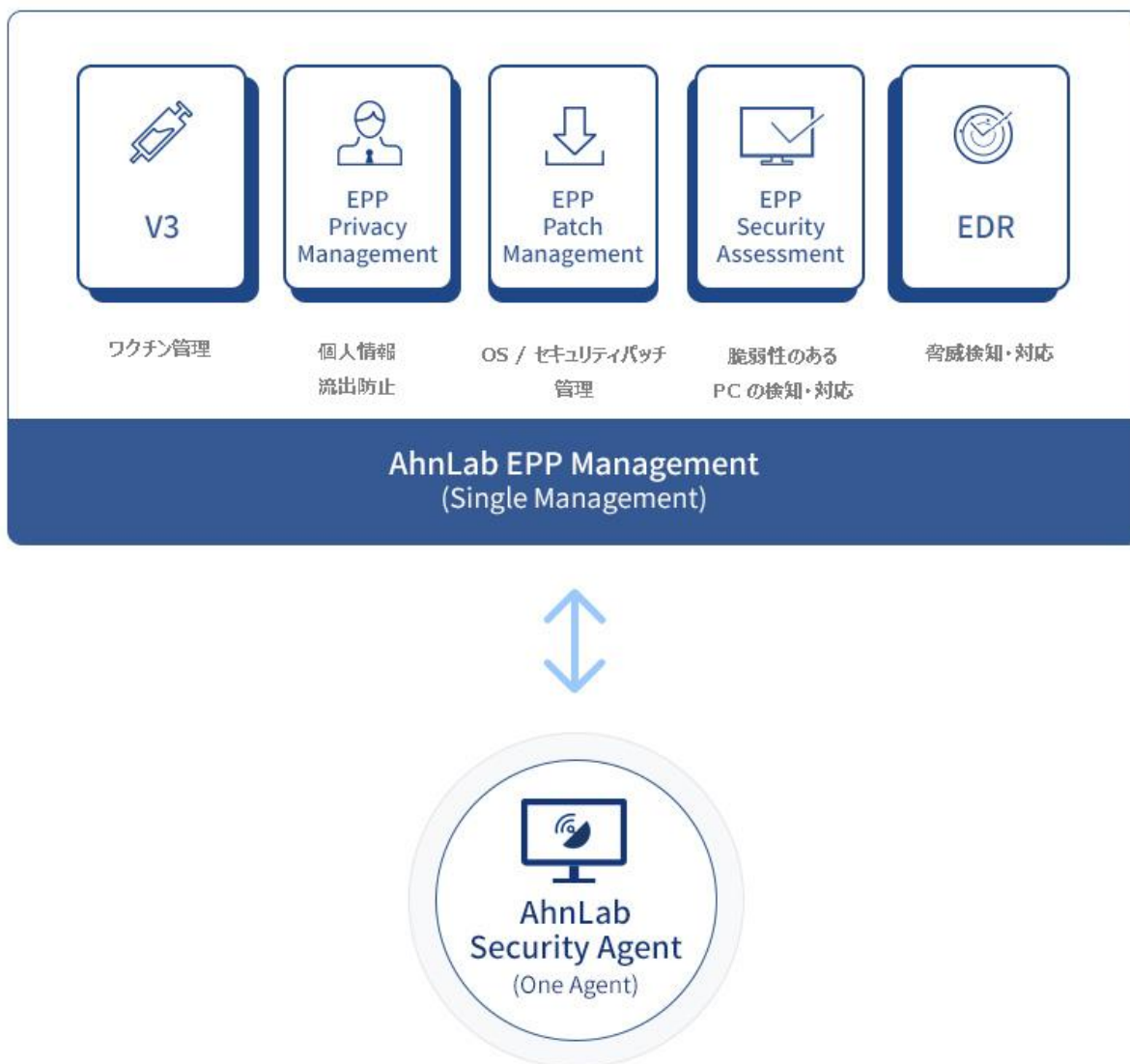
なぜアンラボはクラウドに力を注ぐのか

2021年の幕開けとともに、アンラボは大規模な組織改編を断行した。この断行には、▲顧客中心の経営体系の強化、▲クラウド中心事業の強化、▲オープンイノベーション拡大という組織的な目標が背景にある。このうちクラウド中心事業の強化に関して、研究所内に「クラウド開発室」、またサービス事業部門内に「クラウド事業本部」を新たに編成するなど、事業的かつ技術的力量を集中させている。

クラウドがトレンドであることは今や誰もが知るところだが、アンラボがクラウド領域に力を入れているのは、単にトレンドだからという理由だけではない。今回は、アンラボがクラウド事業に向け掲げる目標や、核心的価値について詳しく紹介する。



アンラボのクラウド事業を説明するにあたり、先に言及しておくべき核心的概念がある。それは「プラットフォーム」形態のサービスだ。アンラボが目指してきたセキュリティプラットフォームとは、ソリューション間の連携や連動をサポートし、顧客の状況に応じて必要なサービスを提供することである。昨今のような多面的かつ高度化した脅威環境において、流入してくる攻撃に対し、単一製品だけで十分な対応力を提供するには限界があるのが実状だ。アンラボは、ポートフォリオのプラットフォーム化を実現させるため絶え間ない努力を重ね、今日までかなりの成果を上げてきた。例えば AhnLab EPP (Endpoint Protection Platform) に関しては、V3、AhnLab EDR (Endpoint Detection and Response) などのエンドポイント領域における単一ソリューションだけでなく、3rd partyソリューションとの連動により、最適化したセキュリティ力を提供している。



[図1] AhnLab EPP 構造図

「プラットフォーム化」を目指すアンラボのクラウド事業

アンラボは、以前よりクラウドセキュリティへの必要性を認識し、具体的なロードマップとともに対応力の強化を続けてきた。そして、数年前にいわゆる「クラウドブーム」が起り、顧客のクラウド使用率が急増し始めることで、それに対するニーズも増えてきた。ここでのニーズとは、クラウドセキュリティだけに限らず、クラウドの使用に関するニーズも含まれている。

顧客の挑戦課題やトレンドを長期にわたり分析した結果、多くの顧客がオンプレミスとクラウドを結合した「ハイブリッドクラウド」を使用していることが判明した。運営環境においてはクラウドに一部を移転し、残りは従来のオンプレミス上で運営を継続する傾向が顕著にあらわれた。顧客は自然とハイブリッド環境下での円滑な運営や、強固なセキュリティへの必要性を訴えることになる。

アンラボは、以前より目指してきた「プラットフォーム化」を基本概念に、クラウドセキュリティの提供へと一層拍車をかけた。その第一段階が、クラウドワークロードセキュリティプラットフォーム (Cloud Workload Protection Platform: CWPP) の「AhnLab CPP」である。

昨年 6 月にリリースされた「AhnLab CPP」は、韓国国内唯一の国産 CWPP ソリューションとして、アプリケーション制御、ホスト IPS (Intrusion Prevention System)、アンチマルウェアなど、クラウドワークロードを保護する上での核心的力量を提供する。またこれに留まらず、リリース後すぐに高度化に向けた作業に着手し、▲サポート OS の拡大、▲コンテナ保護機能の強化、▲多角的なユーザー利便性の向上、▲可用性向上のための性能などを改善した「AhnLab CPP 1.0.2バージョン」をリリースするにいたった。



[図2] AhnLab CPP 概念図

また、クラウドに関する需要が増加するにつれ、ソリューションだけでなく、サービス領域におけるクラウドセキュリティ管制事業も活発に推進してきた。

これまでにアマゾンウェブサービス (AWS)、マイクロソフトアジュール (Azure) など、クラウドサービスのセキュリティ管制に関し様々なリファレンスやノウハウを積み上げている。言うなれば、ソリューションやサービスを網羅したクラウド力を、組織レベルで発展させてきたのだ。

ここからさらにアップグレードしたものが、今年初めにリリースされたマネージドサービスプロバイダ (Managed Service provider、MSP) サービスの「AhnLab Cloud」である。「AhnLab Cloud」は、クラウド構築から運営およびセキュリティにいたるまで、3つの核心的要素を全て備えたクラウドサービスだ。普遍的なクラウド管理サービスに強固なセキュリティ力が追加され、クラウド使用に関するニーズを一気に解決する「次世代 MSP」志向が、このソリューションの特徴である。



[図3] AhnLab Cloud の特長

これにより、アンラボはクラウドワークロードセキュリティプラットフォーム、セキュリティ管制、さらにはクラウド管理サービスにいたるまで、クラウドセキュリティと使用性を併せ持つ統合ポートフォリオの構築を実現した。また、管制や MSP サービスから得たインサイトを、セキュリティプラットフォームの高度化に適用する「好循環システム」も確立することになる。

クラウドポートフォリオの核心は「顧客のユーザー使用性」

アンラボはクラウドポートフォリオを開発・運営するにあたり、「何をどのように保護するか」を常に問い続け、顧客の「ユーザー使用性(Usability)」について悩んできた。

「ユーザー使用性」の概念を、今一度クラウド管理サービスに当てはめてみよう。従来の MSP の場合、クラウドの構築や運営には確固たる強みを持っている。しかしこれとは別に、セキュリティ面において差別化された力量が必要とされている。ただ単に優れたセキュリティソリューションを統合適用するのではなく、顧客にとって本当に必要なセキュリティとは何かを考慮しなければならない。さらに、それがノウハウや技術力によって裏打ちされている必要がある。特に、セキュリティの適用に不備がある場合、性能の低下が懸念されるだけでなく、様々な脅威にさらされる可能性も出てくる。また、これはビジネスに対する脅威にも帰結してくる。

現在の MSP システムでは、クラウドセキュリティ上で問題が発生した場合、顧客の立場からすると原因分析や解決の要請先が不透明である。こう

したニーズの解決、そして顧客側のクラウド管理に対する利便性向上のためにリリースされたのが、この「AhnLab Cloud」だ。「AhnLab Cloud」は現在、他の MSP サービス企業との競争というよりも、純粋に顧客のペインポイント (pain point) を解決し、そのユーザービリティを高めるという観点で運営が行われている。

アンラボが CWPP を最初のクラウドセキュリティソリューションとして選んだのも、このユーザービリティに通じてくる。クラウド環境において、最優先でサポートされるべきはワークロードセキュリティだ。顧客側が最も必要とし、かつ最も多用されているからである。

ユーザー使用性に関しては、クラウドセキュリティソリューションの導入時に、顧客側も綿密に確認しなければならない部分だ。特に回復性 (Resilience) に対する技量を調べ、問題発生時には迅速に修正事項を適用・改善する必要がある。これは、クラウドサービスの使用量とも関係しており、初期設備を支障なく行うことで、使用性・可用性・回復性をすべて備えた上で、コストパフォーマンスや生産性の向上も可能となる。

手軽なようで難しいクラウド、依然として残る挑戦課題

安定的なクラウド環境作りのため、アンラボが注目する2つの挑戦課題は、「複雑性」と「設定ミス」である。

まずクラウドは、必要に応じてリソース使用の柔軟な増減が可能なオートスケーリング (Auto Scaling) や、サービスコストの最適化など、オンプレミスに比べ考慮すべき要素が多い。また、オンプレミス領域では保護価値の低かった資産も、クラウド上では保護対象になりうる。双方の基準が異なるため、その接点やコンプライアンスの適用法に関しても手法を変えていくほかない。こうした複雑性は、マルチクラウドを運営する場合さらに深刻化する。2つ目に挙げられたクラウド上の設定ミス (Misconfiguration) は、クラウド侵害時の主な原因の一つとされている。今後もこの設定ミスにより、多くの被害事例が発生すると予測される。

設定ミスに関する簡単な例として、ある特定の企業がサービスA、B、そしてCへのアクセス権限を全員に付与してしまう設定ミスが発生したと仮定しよう。本来ユーザー認証を全員に付与していても、アプリケーションごとに別途の権限設定が可能である。しかし、こうした措置をとらなかった場合、サービスとは全く関係のない者までが特定のサービスにアクセスし、セキュリティ問題を引き起こす可能性が生じてくる。また別の例として、設定ミスにより必要な人員がサービスにアクセスできず、ビジネスの生産性に支障をきたす場合もある。

このような設定ミスによる被害を予防するためには、まず最低限の信頼度に基づいてアクセス権限を付与する「ゼロトラスト (Zero Trust)」の概念導入が必要となる。市場調査機関である「ガートナー (Gartner)」はゼロトラストについて、「抽象的な信頼を、正確な計算に基づくリアルタイムで適用可能な信頼度に置き換え、企業資源へのアクセス権限を適時適所に付与するもの」と説明している。

顧客側はクラウド初期構築時、ゼロトラストガイドに沿ったセキュリティを構成しなければならない。また、認証 (Authentication) と認可 (Authorization) を明確に区別し設定する必要がある。

ユーザー認証を正確に行ったとしても、認可にミスがあれば不要なアクセス権限を与えることになるからだ。さらに、設定に関する部分は頻繁に変化するため、継続的なモニタリングや管理可能なプロセス・ソリューションが求められる。

クラウド最適化に向けたアンラボのネクストステージ

アンラボは現存する挑戦課題を解決へと導き、クラウドセキュリティやユーザー使用性の最適化に向け努力を続けている。最も代表的なものとして、「AhnLab CPP」へのクラウドセキュリティ態勢管理 (Cloud Security Posture Management, CSPM) 機能の搭載計画が挙げられる。

CSPM とは、クラウドサービスの構成やポリシー設定を評価・管理・モニタリングすることで、人為的過失や設定ミスを防止するソリューションだ。これにより、クラウドセキュリティへの侵害にまつわる根本的な原因を、未然に排除することができる。

さらに、前述したクラウド環境におけるセキュリティの複雑性を解消し、オンプレミス・ハイブリッドクラウド・マルチクラウド環境全般にわたって最適化した技術力をサポートするため、当社が保有するセキュリティポートフォリオの様々な要素をクラウド上で提供する予定だ。

結論

アンラボは今日まで、クラウドセキュリティやユーザービリティ最適化のため邁進してきた。その結果、クラウドセキュリティソリューション、セキュリティ管制および管理サービス領域において、相互補完的な統合ポートフォリオの構築にいたる。さらに、クラウドセキュリティや正しい初期設計、そして可用性の重要性についても顧客から共感を得てきた。アンラボのソリューションを使用しているアジア地域のグローバル顧客層も、クラウドへの転換トレンドにより、今後自社のセキュリティに対する需要が増加すると予想される。

つまるところクラウドとは、顧客が必要とする環境に最適化しサポートするという面で、競争ではなくシナジーが重要なポイントとなってくる。アンラボは、「顧客主導型 (Customer-Driven)」のクラウド力提供という基本概念を堅持し、競争よりも協力や技術力の高度化に焦点を置き、継続的な発展を図っていく意向である。



<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)

© 2021 AhnLab, Inc. All rights reserved.