AhnLab

百書

最適なランサムウェア対応のための総合セキュリティ戦略

最近発生しているランサムウェア感染事件を見ると、サイバー攻撃が新たな段階に入ったことがわかる。かつて単純なファイル暗号化や金銭要求に留まっていたランサムウェア攻撃は、今やデータ流出、サービス停止、評判毀損を伴う複合攻撃へと進化した。その波及力ももはや単一企業に限定されず、攻撃者は「感染後に恐怖を植え付ける存在」から「侵入後に潜伏する存在」へと変貌している。

このように高度化したランサムウェア攻撃も、表面的には予測不可能に見えるが、実際には明確な流れが存在する。したがって、事故は予測できなくとも、対応は予測可能にすることができる。この哲学こそが、アンラボの「ランサムウェア統合セキュリティ戦略」の出発点である。

ランサムウェアセキュリティの課題

進化を続けるランサムウェア攻撃は、企業に新たな課題をもたらす。課題は多岐にわたるが、大きく次の三つにまとめられる。

#1. 新種/亜種ランサムウェアの対応: ランサムウェアは新種や亜種が絶えず出現し、防御者を苦しめる。こうしたランサムウェアに効果的に対応するためには、単一ソリューションによる遮断を超え、ランサムウェアが引き起こす悪意のある動作を分析し、ソリューション間の連携・連動をサポートするプラットフォームベースの戦略が必要である。

#2. 多様な区間の保護: 最新のランサムウェア攻撃は、エンドポイント、ネットワーク、メールなど多様な区間で発生する。熟練した攻撃者は目的を達成し被害を最大化するため、複数の区間を横断して攻撃を実行することもある。企業が単一の領域のみを保護すると、当該領域のセキュリティソリューションを迂回したり、他の区間から侵入する攻撃の被害を受けることになる。

#3. 再発防止体制の構築: ランサムウェア攻撃は一度遮断しただけでは終わらない。類似した攻撃がいつでも再発する可能性があり、特に潜伏技術が発達した最近の攻撃ではこの傾向が顕著である。ランサムウェアによる連鎖的な被害を予防するためには、検知や遮断を超え、脅威を追跡して予防できるセキュリティ体制を整える必要がある。

セキュリティは製品ではなく「プロセス」によって完成される

新たなランサムウェアセキュリティの課題解決に向け、企業が一般的に提示する解答はセキュリティソリューションの「数」を増やすことである。この傾向は韓国だけでなく世界的に見られる。

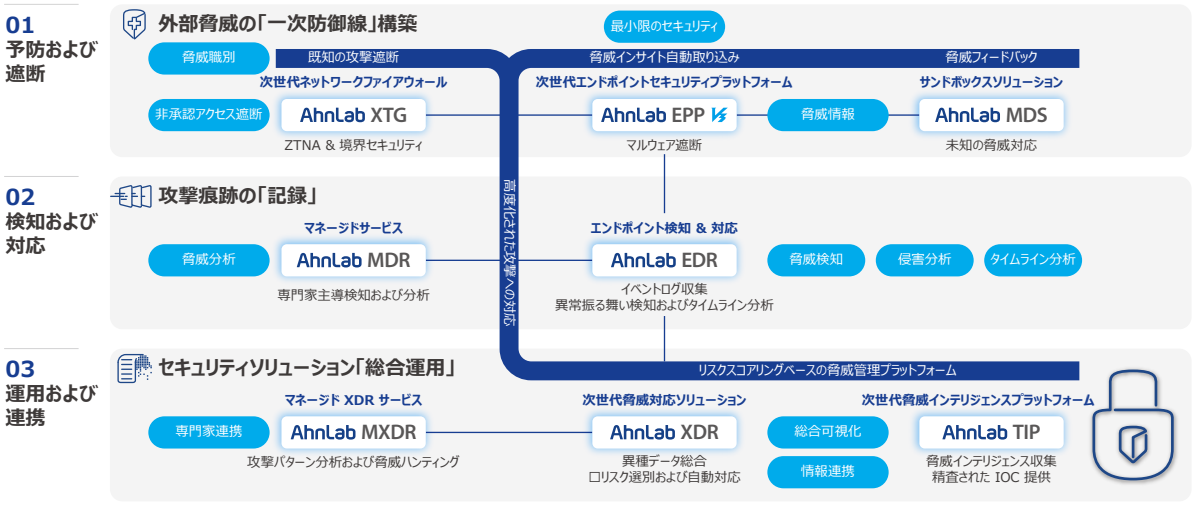
市場調査機関ガートナー(Gartner)が2024年に全世界の大企業162社を対象に行った調査結果によると、回答者は平均45個のサイバーセキュリティソリューションを運用していると答えた。前年度である2023年は平均43個と大きく変わらず、回答者の半数が「ソリューションを十分に活用できていない」と述べた。

セキュリティソリューションの数は企業規模、産業、国によって差があるが、運用上の困難を訴える点は全体的に共通している。そして、アンラボが実際に侵害被害を受けた企業の事例を分析すると、セキュリティソリューションの「不在」よりも「活用不足」によって被害を受けたケースがはるかに多い。

サイバーセキュリティ専門家ブルース・シュナイアー（Bruce Schneier）は、「セキュリティは製品ではなくプロセスである」という名言を残した。セキュリティソリューションを導入し機能を断片的に使用する静的な状態を超え、セキュリティソリューションが有機的に動作しながら人とシナジー効果を生み出せるよう、動的な努力を傾けるべきだという意味だ。

最適なランサムウェア対応のための統合セキュリティ戦略

アンラボは、ランサムウェア攻撃の高度化、現場で企業が直面する課題、プロセス視点の統合セキュリティの重要性を考慮し、ランサムウェアセキュリティに最適化されたプラットフォームベースのソリューションを提供している。アンラボのランサムウェアセキュリティオファリングを構成するソリューションは、それぞれ独自の役割を果たす一方で、相互に柔軟に連携し、プロセス観点から「検知-分析-対応」が有機的に循環する一つのセキュリティエコシステムとして機能する。これにより、顧客が侵害前(Prevention) – 中(Detection) – 後(Response)をつなぐ循環構造を構築できるよう支援する。



[図1] アンラボのプラットフォームベースランサムウェアセキュリティオファリング

このため、アンラボは「次世代ファイアウォール（ZTNA）－アンチウイルス（EPP）－サンドボックス－EDR－MDR－XDR－MXDR－脅威インテリジェンス（TI）」へと続く連携体系を構築した。次世代ファイアウォールがユーザーとデバイスの検証を通じてアクセス段階で信頼性を保証し、EPP とサンドボックスが悪意のある動作の検知と事前遮断、EDR と MDR がエンドポイントの動作追跡と専門分析、XDR と MXDR が組織全体の統合可視性と自動対応を担当する。ここに最新の脅威インテリジェンスが加わり、セキュリティ体系を完成させる。

段階	ソリューション	役割
1.予防および遮断	AhnLab XTG	ユーザー/デバイス検証によるアクセス制御 (ZTNA)
	AhnLab EPP (V3)	既存のマルウェアの検知と遮断
	AhnLab MDS	サンドボックスベースの分析－未知のマルウェアの検知と遮断
2.検知および対応	AhnLab EDR	エンドポイントイベントの収集、分析、対応
	MDR サービス	専門家主導のエンドポイント脅威検知、分析および対応
3.運用および連携	AhnLab XDR	リスクスコアリングに基づく統合脅威管理
	MXDR サービス	複数のセキュリティセグメントに対する専門家の統合攻撃パターン分析および脅威ハンティング
	AhnLab TIP	侵害指標(IOC)を含む脅威インテリジェンスの提供

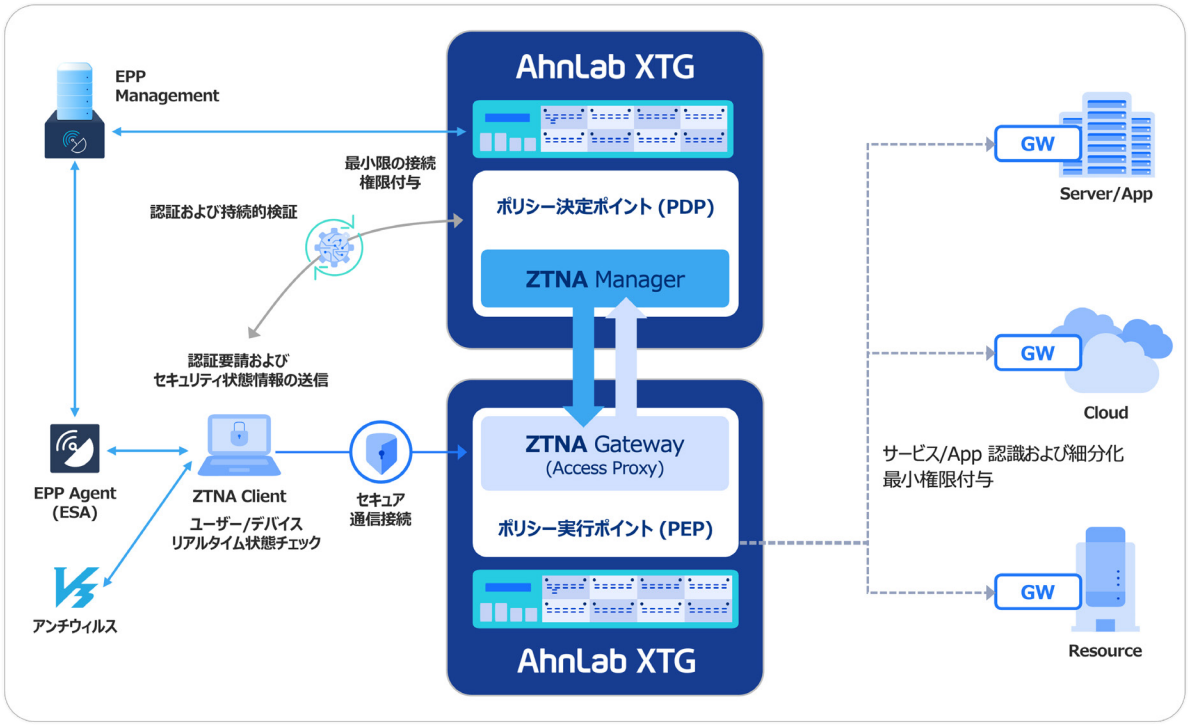
[表1] ソリューション別の役割

セキュリティソリューションが果たす役割に関する詳細は以下の通りである。

1段階：予防と遮断 -「脅威が来る前に防ぐ」

① AhnLab XTG – ZTNA ベースの信頼性検証およびアクセス制御

次世代ファイアウォール AhnLab XTG は、ZTNA（Zero Trust Network Access）を実際のネットワーク運用環境に実装したソリューションである。AhnLab EPP、AhnLab V3 などのエンドポイントセキュリティソリューションと連携し、ユーザーとデバイスの身元を継続的に検証することで、「誰も基本的に信頼しない」というゼロトラストセキュリティモデルを実現する。



[図2] AhnLab XTG - ZTNA ベースのネットワークアクセス制御構造

AhnLab XTG は、未承認ユーザー、セキュリティ状態が完全でないデバイス、権限を超えた内部アクセスをリアルタイムで制御する。ネットワーク区間において内部侵入の最初の関門を根源的に遮断し、ネットワークからエンドポイントに至る統合アクセス制御体系を完成させる。

要約すると、AhnLab XTG は、「認証 – 権限 – 動作」を軸とするゼロトラストセキュリティプラットフォームとして、組織の内外境界を問わない最新脅威防御のために「信頼検証の中心軸」としての役割を果たします。

② AhnLab V3 – 統合セキュリティ体系の「エンドポイント一次防御線」

AhnLab V3 は、30年以上にわたり企業や機関から長期間信頼されてきたアンチウイルス（AV）ソリューションである。基本的に卓越した性能と技術力を備えた製品だが、単純な「インストール有無」を超え、リアルタイム保護の有効化、スキャン周期管理、例外ポリシーチェックなど、ユーザーの運用状況によって防御力が変化する。同じ V3 を使用しても、どれだけ細かく設定し運用するかがセキュリティ効果を左右する。

AhnLab V3 は、以下のような核心機能を中心に、ランサムウェアなどの悪意のある動作を検知・遮断する。

A. シグネチャベースの検知

AhnLab V3 の基本検知体系は、シグネチャベースのリアルタイムスキャン（Real-time Scan）と詳細スキャン（Smart Scan）で構成される。既知のマルウェアは即時遮断し、疑わしいオブジェクトは追加スキャンを経て安全性を判断する。シグネチャデータベースは常時アップデートされ、最新の脅威にも迅速に対応する。

B. ランサムウェア保護フォルダー

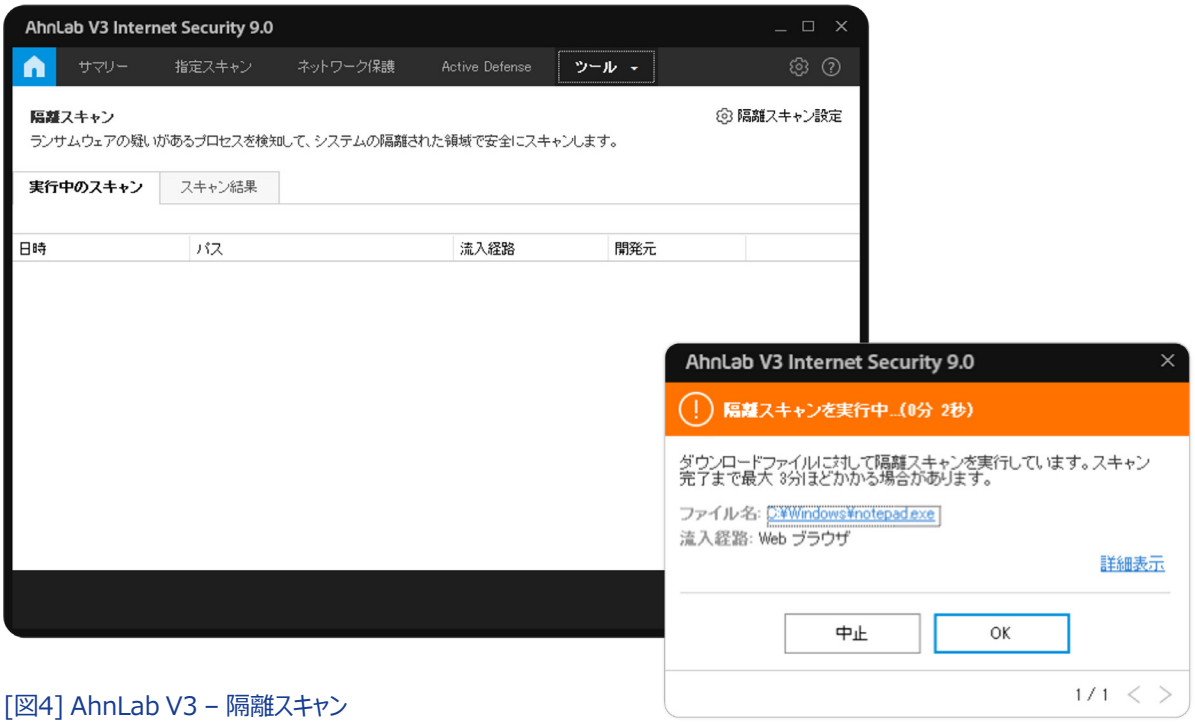
V3 ユーザーは、ランサムウェアなどのサイバー攻撃から必ず保護すべきフォルダーを「ランサムウェア保護フォルダー」として設定できる。ランサムウェア保護フォルダーに指定されたフォルダーには「許可されたプロセス」のみがアクセスできる。例えば、PowerPoint や Excel などの正規アプリのみがアクセスできるように指定すれば、ランサムウェアはそのフォルダーに影響を与えることができない。

アンラボが顧客のセキュリティ運用とランサムウェア侵害事例を分析すると、V3 を導入してもランサムウェア保護フォルダー機能を使用しないケースが多い。ランサムウェア保護フォルダーは、万が一システムがランサムウェアに感染しても重要/機密データを保護できる重要な機能であることを強調する。

[図3] AhnLab V3 – ランサムウェア保護フォルダー設定

C. 隔離スキャン

AhnLab V3 は、PC 内の別個の仮想環境でランサムウェアと疑われるファイルを実行し、隔離スキャン機能を提供する。この機能を活用すれば、ランサムウェアがシステムに侵入しても、行動発現前にスキャンを実行して被害の拡散を防止できる。



[図4] AhnLab V3 – 隔離スキャン

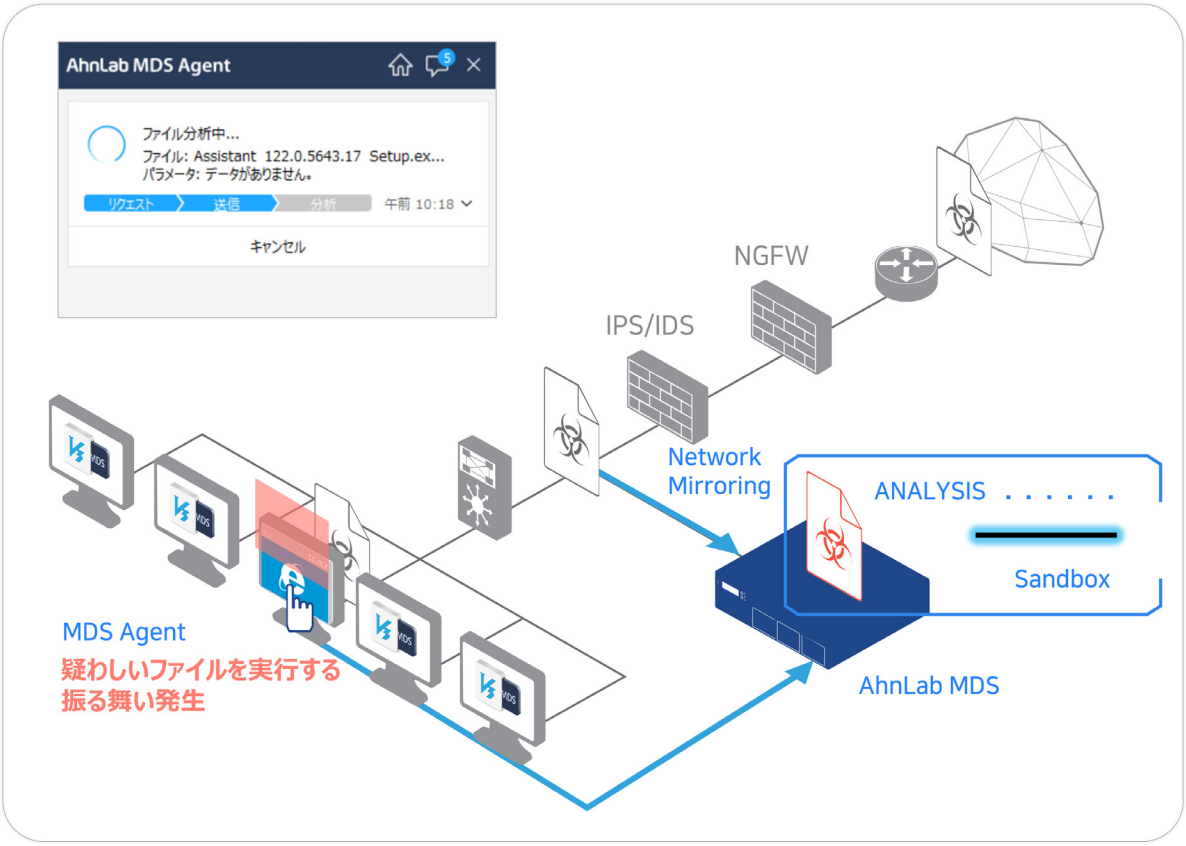
さらに、V3 をエンドポイントセキュリティプラットフォーム AhnLab EPP と併用することで、検知状況、ポリシー、イベントを統合管理し、より迅速な対応が可能になる。EPP は、単一 PC やサーバーを超え、組織内の全エンドポイントのセキュリティ状態を統合モニタリングし、ポリシーを一括適用できる。これにより、セキュリティ担当者は個別デバイスの検知イベントを一つの流れとして把握し、ポリシー管理、パッチ状態確認、デバイス制御など多様なセキュリティ機能間の連携対応を実行できる。

特に最近では、Linux サーバー環境における脆弱性とマルウェアが増加しており、EPP による OS 間の統合セキュリティ管理の重要性が高まっている。AhnLab V3 と AhnLab EPP を併用することで、エンドポイントの検知/遮断能力と中央管理の効率性の両方を確保できる。

③ AhnLab MDS – サンドボックス分析による「ランサムウェア実行前の遮断」

AhnLab MDS は、ネットワーク-エンドポイント-メール区間にわたり未知のマルウェアまで防御し、検知後の対応空白を最小化するサンドボックスソリューションである。

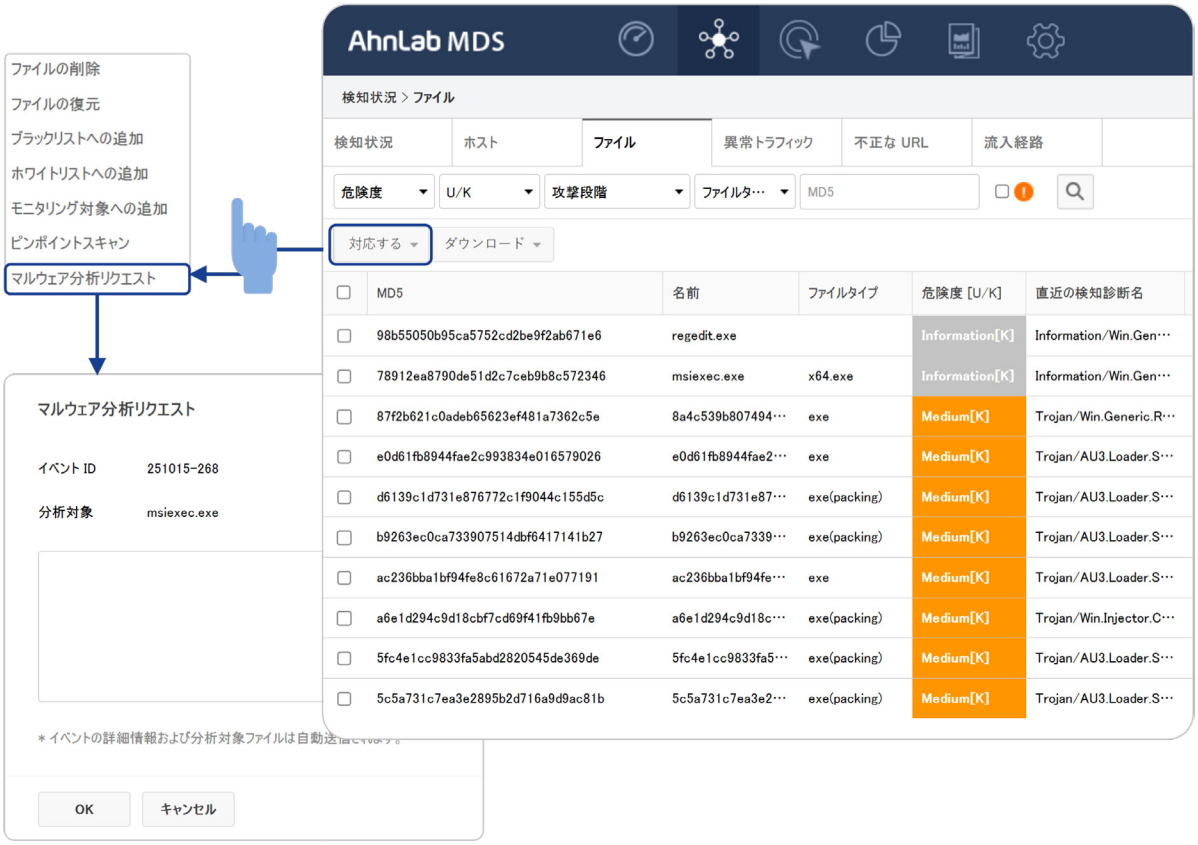
まず、AhnLab MDS はネットワーク区間を行き来するファイルとトラフィックをサンドボックス仮想環境（VM）で分析し、「実行前遮断（execution holding）」、「振る舞い分析（behavior analysis）」などを実行する。エンドポイントにおいても、疑わしいファイルがユーザー PC で検知されると、AhnLab MDS がこれを自動的に収集し、サンドボックス環境で実際の動作を観察する。一定時間内に暗号化、削除、不正アクセスなどの異常動作が確認された場合、直ちに実行を遮断する。また、分析結果を管理者コンソールに送信し、感染の可能性のある他の端末を追跡し、内部拡散を防止する。



[図5] AhnLab MDS - サンドボックスベースの振る舞い分析および実行前の遮断

メール区間においても、AhnLab MDS の MTA（Mail Transfer Agent）はメールのヘッダー、本文、URL、添付ファイルを総合的にスキャンする。本文に含まれる URL は直接アクセスして異常の有無を確認し、添付ファイルはサンドボックス環境で分析する。不正なメールは隔離し、システムに流入しないようにする。

この他にも、AhnLab MDS は、「マルウェア分析リクエスト」機能を提供し、内部で発見された疑わしいファイルをアンラボの専門アナリストに送信・報告できるように支援する。管理者は分析レポートを通じて脅威の種類、感染経路、拡散の有無を確認し、迅速に対処できる。



[図6] AhnLab MDS – マルウェア分析リクエスト

2段階：検知と対応 -「侵入を許容しても拡散は阻止する」

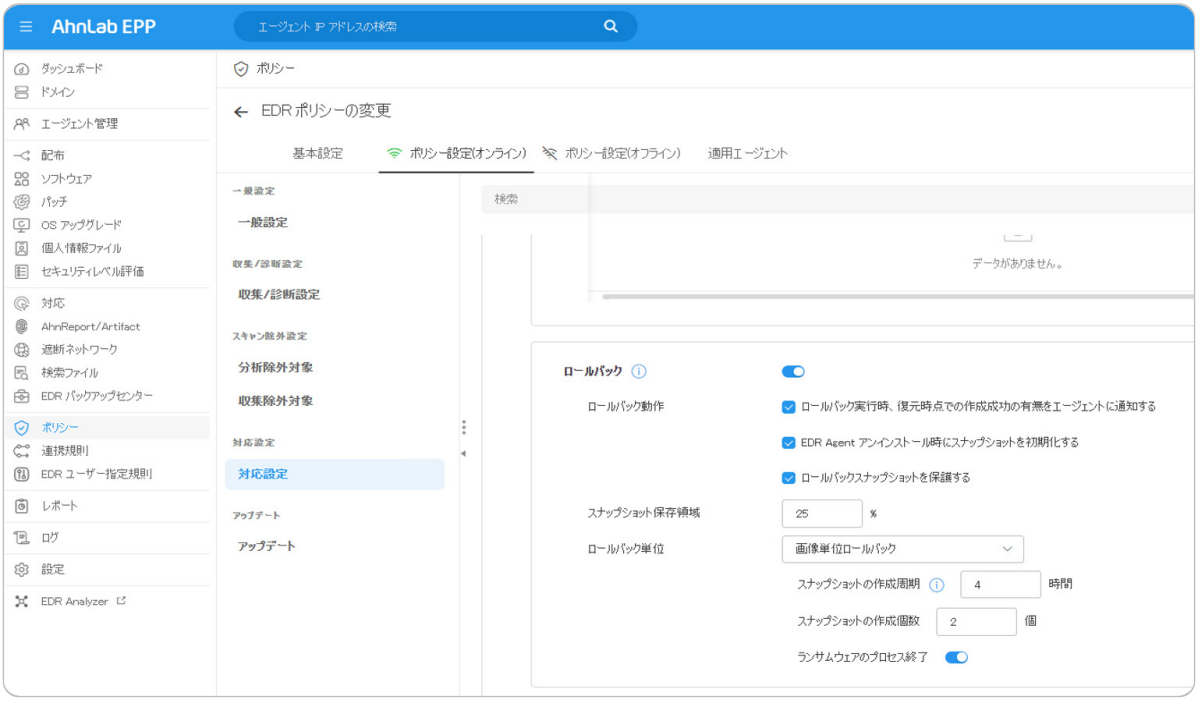
① AhnLab EDR – 脅威の「文脈」を読み取る目

AhnLab EDR は、単なるイベントモニタリングツールではない。各エンドポイントで発生する全ての振る舞いを時間とプロセス単位で記録し、攻撃の文脈を分析して脅威の流れを再構築する。つまり、単一イベントではなく「振る舞い間の関連性」に基づいて脅威を認識する。これにより、ユーザーのエンドポイント脅威管理、未知の脅威の潜伏期間最小化、潜在的な被害及び再発防止を支援する。

また、AhnLab EDR にはランサムウェア対策に特化した機能も搭載されている。代表的な機能は以下の通りである。

A. 自動ロールバック (Auto Rollback)

感染時点以前の状態にファイルを復元できる機能である。従来は管理者が直接ロールバックを実行する必要があったが、現在は自動オプションにより検知即時の復元が可能である。

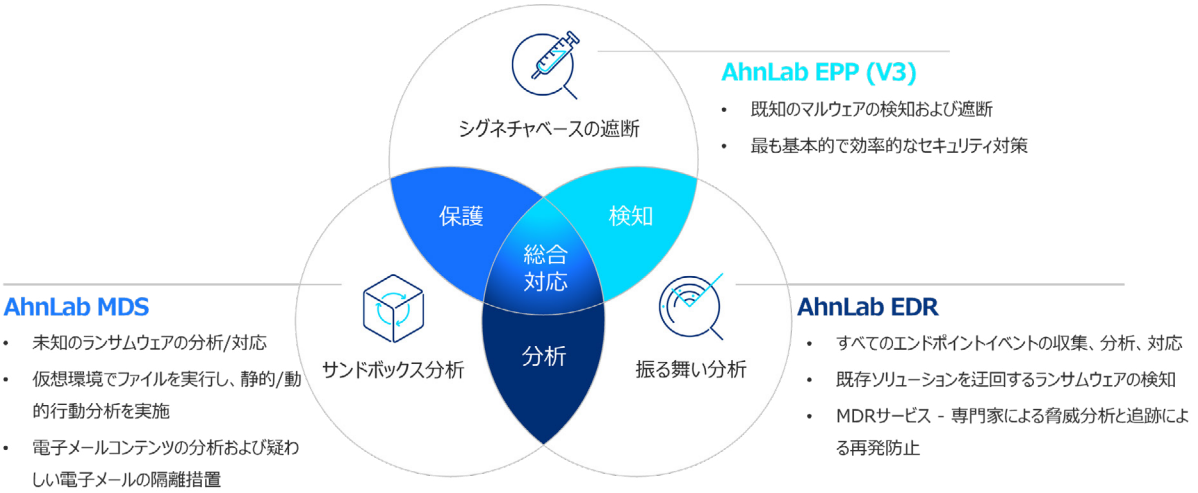


[図7] AhnLab EDR – 自動ロールバック機能画面

B. セキュリティニュース& IOC ウィジェット

AhnLab EDR は、アンラボの脅威インテリジェンスプラットフォームである AhnLab TIP の最新セキュリティ勧告文で提供 IP、URL、ハッシュ値などを自動収集し、内部ログと比較分析する。管理者は「このニュースに関連する危険端末」を即座に確認できるため、対応速度を短縮できる。

これまで説明した AhnLab EPP(V3)、MDS、EDR は、アンラボのランサムウェアセキュリティ提供の中でも核心を担う。EPP(V3)がエンドポイントの第一線防御、MDS がネットワーク-エンドポイント-メールの振る舞い分析および遮断、そして EDR がエンドポイント全体のイベントを分析・対応する体系で構成される。これら3つのソリューションは柔軟に相互連携し、検知 – 分析 – 対応が有機的に連携したマルチレイヤーセキュリティ体制を構築する。

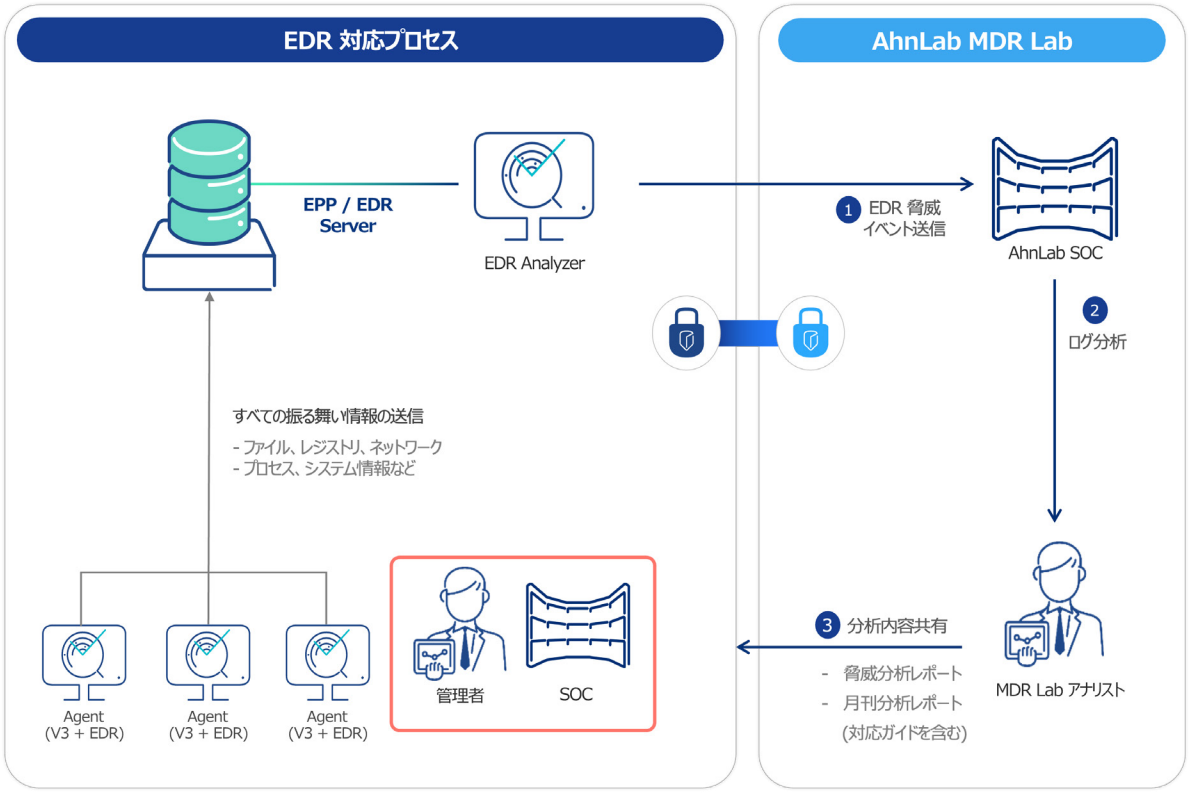


[図8] AhnLab V3-MDS-EDR 連携セキュリティ体系

② MDR – 検知と「人を中心とした対応」

EDR が技術的基盤であるならば、MDR（Managed Detection & Response）は、人間の経験が加わった脅威対応プロセスである。アンラボのセキュリティ専門家は、AhnLab EDR で検知される脅威を24時間モニタリングし、侵害の兆候を事前に追跡（ハンティング）する。異常兆候が発見された場合、迅速な対応と検知を実行する専門的な運用プロセスを通じて、顧客の脅威イベントを常時分析する。

MDR の強みはリアルタイム分析力とコミュニケーションである。単純なログ解釈を超え、「このイベントは単独振る舞いか、それとも連鎖攻撃の始まりか？」を判断し、危険度と拡散可能性、ビジネス影響まで考慮した対応策を提示する。これにより、セキュリティ人材が不足している企業でも卓越した脅威検知・対応プロセスを構築できる。



[図9] MDRサービス – 運用プロセス

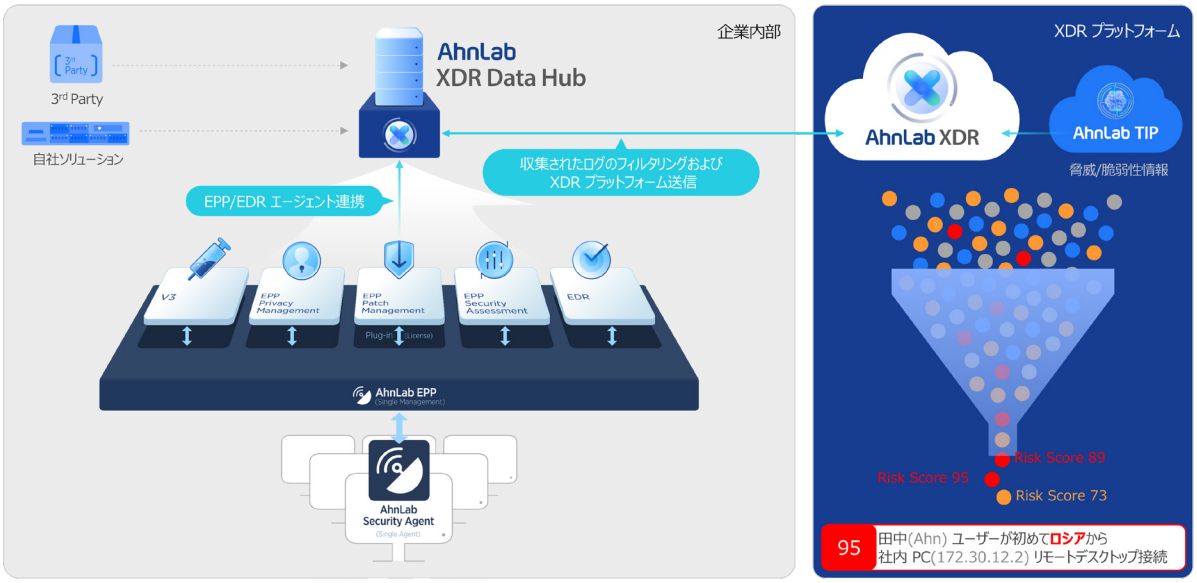
まとめると、EDR と MDR の結合は、人と技術が連携して動作するリアルタイム脅威対応体系を完成させる。攻撃を阻止できなくても拡散は必ず遮断するという哲学を技術的に実現した段階と言える。

3段階：運用と連携 -「セキュリティの最終目標は統合管理」

ランサムウェアを含む最新の脅威は、エンドポイント、メール、クラウド、ネットワークなど、セキュリティ領域を選ばない。したがって、すべてのセキュリティ領域を包括する統合可視性を確保することが最優先課題となった。

① AhnLab XDR – データを繋ぐ「セキュリティハブ」

AhnLab XDR は、エンドポイント、ネットワーク、クラウド、メールなど多様なシステムログを統合して可視化し、イベント間の相関関係を分析して攻撃の全体的な流れを把握する。分散した侵害の兆候を単一の文脈で再構成し、セキュリティ担当者が脅威の展開過程と影響度を容易に把握できるようにする。

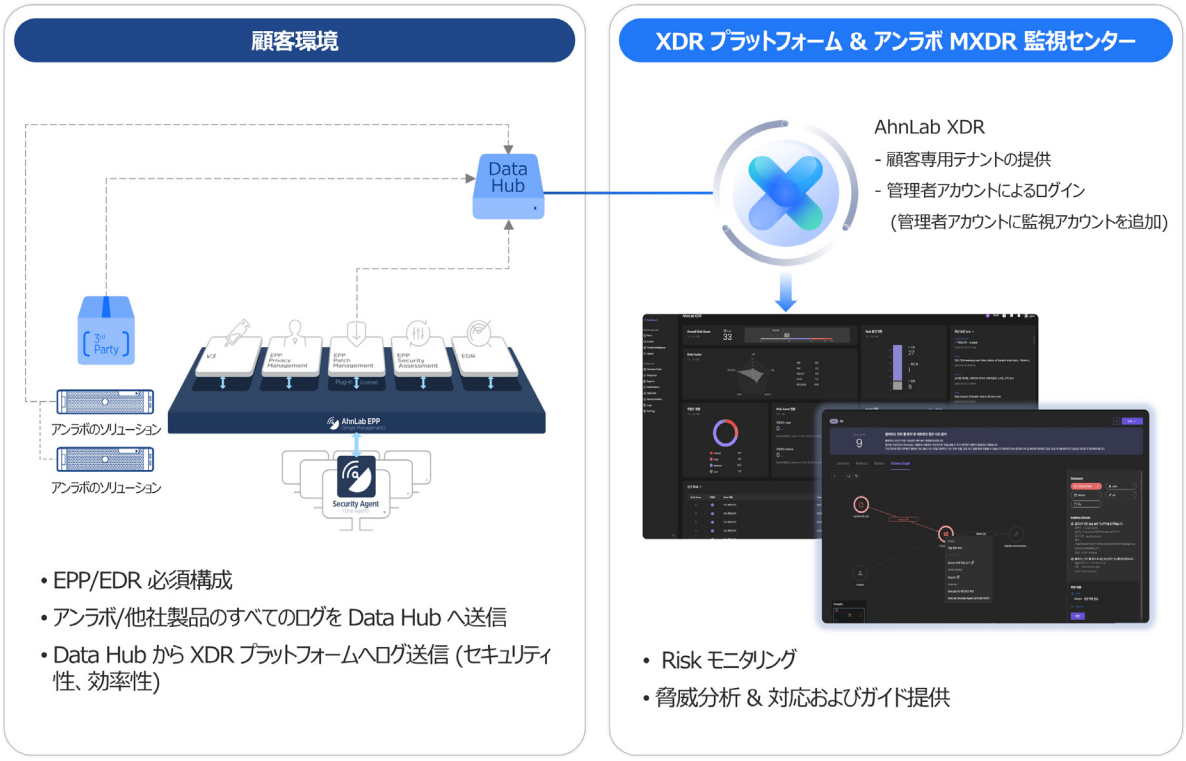


[図10] AhnLab XDR - 統合データプラットフォーム基盤の相関分析

この過程で脅威の深刻度はリスク指数として定量化し、管理者が対応優先順位を明確に判断できるようにする。AhnLab XDR に搭載された生成 AI「AhnLab Annie」は、ユーザーのセキュリティ意思決定プロセス全体を支援する。また、オープン API ベースの Open XDR 構造により、他社ソリューションとも柔軟に連携できる。企業はセキュリティ体制をより拡張可能（スケーラブル）にし、有機的なプラットフォームへと発展させることができる。

② MXDR –「統合運用」を完成させる専門家の手

XDR がデータを統合してリスクを管理するならば、MXDR は、その統合データに基づき専門家が直接セキュリティを運用・対応する段階である。アンラボの MXDR サービスは顧客企業の AhnLab XDR プラットフォームを遠隔管理し、24時間モニタリング、脅威ハンティング、リスク対応などを実施する。専門家が単一イベントの異常兆候から複合攻撃まで分析し、ビジネス影響度を評価して最適な対応策を提示する。



[図11] AhnLab MXDR の統合脅威対応構造（専門家分析サービス + XDR プラットフォーム）

MXDR は単なる監視サービスではなく、セキュリティ専門家が顧客企業のセキュリティチームの一員のように常時連携するハイブリッド運用モデルである。XDRのデータに基づく自動検知能力と人間の分析能力を組み合わせ、「検知 – 分析 – 対応」の全過程を完成形のプロセスとして実現する。

③ AhnLab TIP – インテリジェンスで完成する先制的なセキュリティ

AhnLab TIP は、最新の侵害指標(IoC)、脅威グループ分析、攻撃戦術・手法(TTP)情報を統合して提供する予測型セキュリティインテリジェンスハブである。これにより国内外で収集された脅威情報を標準化し、攻撃者グループの戦術と行動パターンに基づいて「予測可能なセキュリティ」を実現する。

また、AhnLab TIP は、AhnLab EPP、AhnLab XTG、AhnLab EDR、AhnLab XDR など、アンラボの主要ソリューションとリアルタイムで連携し、新たに検知された IoC を各製品の検知ポリシーに自動的に反映する。これは単なる情報提供ではなく、セキュリティイベントの統合可視性と自動対応、関連性分析まで包括する統合セキュリティプロセスの一部である。

この構造のおかげで、アンラボソリューションは脅威インテリジェンスの「収集 – 検知 – 遮断 – 対応」がリアルタイムで循環する自動化された脅威対応システムを備えている。AhnLab TIP は、個別のソリューションの上に存在する「セキュリティプロセスの中心ハブ」として、組織が予測不可能な脅威にも一歩先んじて対応できるよう支援する。

世界的に検証された技術力

アンラボのランサムウェアセキュリティオファリングを構成する核心ソリューションは、グローバルサイバーセキュリティ評価で優れた成績を収め、卓越した技術力を証明し続けている。

まず、AhnLab V3 は、2013年から AV-TEST に参加し、60回以上の認証を獲得した。2025年には「高度脅威防御テスト（Advanced Threat Protection Test、以下 ATP テスト）」で満点を獲得し、高度化された攻撃遮断能力を検証された。ATP テストは MITRE ATT&CK フレームワークに基づいて設計された10種類のサイバー攻撃シナリオを活用し、製品の検知＆遮断能力を評価した。

また、AhnLab EDR と AhnLab XDR は、世界で最も信頼性の高いセキュリティ製品テストの一つである MITRE ATT&CK 評価において優れた成績を収めた。2024年に実施されたラウンド6では、主要ランサムウェアグループである CL0P と LockBit が Windows と Linux を跨いで実行する実際の攻撃手法で構成されたシナリオの95%を検知した。これは世界のセキュリティ企業の中でも上位に相当する成績である。

さらに、検知した56の詳細ステップ（substep）のうち49で最高評価の「Technique」を獲得。これは検知情報を通じてユーザーが脅威振る舞いの「文脈（context）」を包括的に理解できることを裏付けるものだ。

このように、アンラボの主要ランサムウェアセキュリティソリューションは、世界的に着実に検証され、顧客の信頼度を高め続けている。

結論：予測可能なセキュリティ、人と技術のシナジーで完成

ランサムウェアはもはや単一の手法による攻撃ではない。侵入後も情報窃取、内部拡散、外部脅迫が続く複合的な脅威チェーンが存在する。今必要なのはセキュリティソリューションの羅列ではなく、予測可能なプロセスに基づく統合対応体系である。

アンラボのランサムウェア統合セキュリティ戦略は、こうした侵害対応プロセスを現実化したモデルである。「ユーザー及びデバイス検証(XTG) – 脅威検知及び遮断(EPP & MDS) – エンドポイント振る舞い分析及び追跡(EDR) – 専門家主導エンドポイントセキュリティ(MDR) – 統合リスク管理(XDR) – 専門家主導統合脅威対応(MXDR) – 脅威インテリジェンス(TIP)」へと続くマルチレイヤー構造がそれである。このプロセス下で、セキュリティ技術は脅威を迅速に識別し、専門家は攻撃の文脈を解釈する。ここに AI 技術が加わることで、最適な対応が可能となる。

今やサイバー脅威への「いかに迅速かつ正確に」対応するかが鍵となる時代だ。アンラボは今後も自社ソリューションとサービスを緊密に連携させ、人間の洞察と技術の自動化が融合した予測型セキュリティ体制で、お客様のビジネス環境を共に守り続ける。

AhnLab, Japan
〒 108-0014 東京都港区芝 4丁目 13-2田町フロントビル 3階
www.ahnlab.com/jp | jp.sales@ahnlab.com