【第一部】

ADサーバからはじめる EDR ＋ 遠隔監視

株式会社エアネット

2025.3.27

エアネットについて

商号	株式会社エアネット
代表	代表取締役社長　吉村 隆
事業内容	ビジネスクラウド、マネージドホスティング、ISPサービス
資本金	1億円
設立	2002年12月
拠点	東京都品川区北品川1-10-4　Y.B.ビル　4F
Webサイト	https://www.airnet.jp/

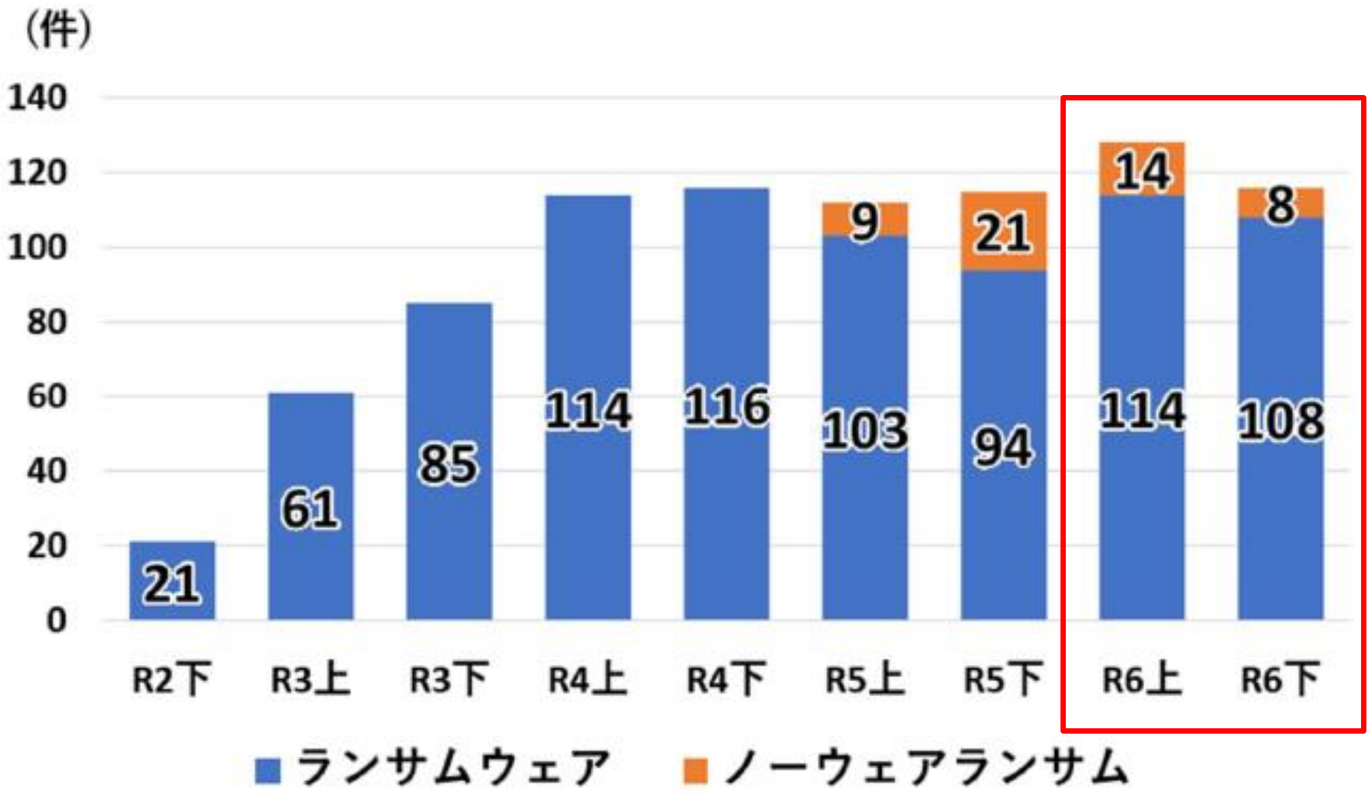
沿革

エアネットはインターネット黎明期より様々なシステムの構築・運用に携わってまいりました。
サービス運用で培ってきた経験をもとに豊富なラインナップでお客様のセキュリティ対策をサポートいたします。

● エアネットサービス 沿革

2025 年1月 DMARCレポート 分析・報告サービス提供開始
2023 年8月 エンドポイントセキュリティサービスで「EDR」提供開始
2023 年6月 クラウドメール障害時に対応「キープメール」オプションサービス提供開始
2021 年7月 標的型メール攻撃対策「セキュリティプラス」サービス提供開始
2015 年8月 メールセキュリティサービス「ALL in Oneメール Gateway」サービス提供開始
2010 年7月 「メール誤送信防止」サービス提供開始
2008 年11月 法人向け専用メールサービス「ALL in One メール Pro」サービス提供開始
2001 年11月 NSPIXP2（現DIX-IE）へのGbE（ギガビットイーサ）による構内接続を追加
1998 年 2月 NSPIXP2（現DIX-IE）へFDDI（100M）にて構内接続
1998 年 1月 WIDE プロジェクト参画
1997 年 6月KDDI大手町ビル内に東京NOCを開設
1996 年 12月 JPNIC 会員となり、ドメイン名およびIPアドレスの割当業務を開始

ランサムウェアの被害状況



令和6年は

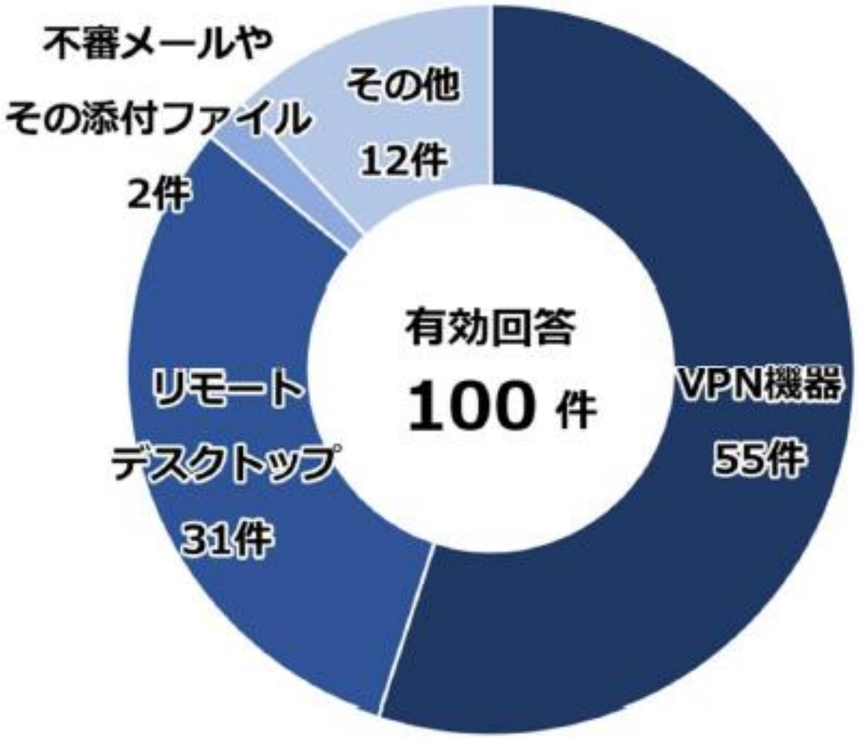
222件

の被害報告件

※「令和６年におけるサイバー空間をめぐる脅威の情勢等について」(警察庁)

多様化する侵入経路

■ ランサムウェアの感染経路



※「令和６年におけるサイバー空間をめぐる脅威の情勢等について」(警察庁)

- メンテナンス用に設定されたVPN
- コロナ禍で作成したが利用者のいなくなったRDP
- アップデートされていないルーターやUTM
- フィッシングメールで漏洩した認証情報

不正アクセスのための情報を扱う

IAB（イニシャルアクセスブローカー）の存在も・・・

サイバー攻撃・ランサムウェアの被害事例

KADOKAWAがランサム攻撃で「ニコニコ」停止、身代金を支払うもデータ復旧できず

動かないコンピュータ取材班

2024.07.05
有料会員限定

全3579文字

【生成AI時代の最新トレンド】注目集
【「AIプライベートクラウド」の可能
【旭プロダクション事例】データ改革

出版大手のKADOKAWAが大規模な
サーバーのデータが暗号化。子会社
ス停止に追い込まれた。KADOKAW
た。取引先や従業員の情報漏洩も確

Active Directoryも乗っ取られ

KADOKAWAは外部専門機関な
正確な情報が得られる見通しで、
し日経コンピュータの取材で、

ＪＡＸＡにサイバー攻撃か、宇宙開発の「機微」閲覧の恐れ…警察から連絡受けるまで気づかず

2023/11/29 05:00

保存して後で読む

宇宙航空研究開発機構（ＪＡＸＡ）が今年夏頃、サイバー攻撃を受けていたことが複数の関係者への取材でわかった。組織内のネットワークを一元管理する中枢サーバーが不正アクセスされ、日本の宇宙開発に関する機微な情報を自由に閲覧できた恐れがある。ＪＡＸＡは政府や警察と連携し、全容解明を急いでいる。

関係者によると、攻撃を受けたのは「アクティブ・ディレクトリ（ＡＤ）」と呼ばれる中枢サーバーだ。組織内の主要なネットワークにつながっており、職員のＩＤ・パスワードや閲覧権限などの情報も管理している。警察当局が今年秋に不正アクセスを感知し、ＪＡＸＡ側に通報した。

ホンダを狙ったサイバー攻撃。ADのドメインコントローラーの脆弱性が利用された可能性も。

大元隆志 エキスパート | CISOアドバイザー
2020/6/21(日) 18:08

一攻撃にあい、一部工場の操業を停止

月上旬、ホンダがサイバー攻
の攻撃に利用されたとされる
ius Group、Enel Groupにも
が高まっている。

地方独立行政法人 岡山県精神科医療センター ランサムウェア事案調査報告書について

HOME » 受診・相談 » 当センターの電子カルテシステムの障害発生について
» 地方独立行政法人 岡山県精神科医療センター ランサムウェア事案調査報告書について

日時	項目	攻撃者Xの推測される手順や行為
03:05~06:28 12:39~12:49	ックアップデーターへのアクセス	
5/19 12:54	AD サーバーの TrendMicro Office Scan Client のフォルダーアクセス	ファイルの削除。 （推測）前後で TrendMicro Office Scan Client のサービスを停止。
5/19 14:31~14:33	Active Director 情報の窃取	サーバー・端末ユーザー、コンピューター、ADサブネット、グループ等の情報を窃取。
5/19 14:42~14:43 14:46~14:47 16:20~16:21	仮想環境サーバー（物理）3台及び仮想環境管理ツールに対するWebアクセス	（推測）VMWare ESXi サーバーの捜索？
5/19 13:10~23:08	サーバー、端末の管理共有のマウントと暗号化 一部サーバーにランサムノート（脅迫状）を表示	Active Directory サーバー、プリンターサーバー、本院サーバー、診療所サーバー、端末の管理共有（C$）をマウント。 （推測）ウイルス対策ソフトを停止し、ランサムウェアによる暗号化を実施。 ランサムノート（脅迫状）は一部のサーバーにのみ表示されていた。DWH サーバーが攻撃を免れた理由は不明。
	ランサムウェアの Autorun 設定	HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run に発見された検体を自動起動設定
	Chrome ブラウザーのインストールとサイトの閲覧	C:¥Users¥xxxx¥Downloads¥ChromeSetup(1).exe ESXi、vSphere、IIS、Fortigate への閲覧を実施。
	仮想基盤の暗号化	SSH 接続による VMWare ESXi サーバーのデータストア

共通事項として攻撃者はActive Directoryをターゲットにしているケースが多い

ADサーバが狙われる理由

・認証情報が集中管理されている

ユーザーIDやパスワード、アクセス権など企業にとって重要なリソースが一元管理されている情報の宝庫

・特権ID奪取による組織の制御

攻撃者はADの特権アカウントを奪取することで、組織のシステム全体を制御し
グループポリシーによるアンチウイルスの無効化やマルウェアの配布で組織全体を効率よく攻撃できる。

・管理が甘いケース

長期間にわたって利用されていることで構成が複雑化したり、適切なアップデートがされず
脆弱性が放置されているケースがある。（社内NWなので油断しがち・・・）

攻撃者にとってコスパがいい！

理想のセキュリティ対策

SWG、ZTNA、CASB、DLP、IAM、IGA、
EPP、EDR、MDR、UEM、MDM、

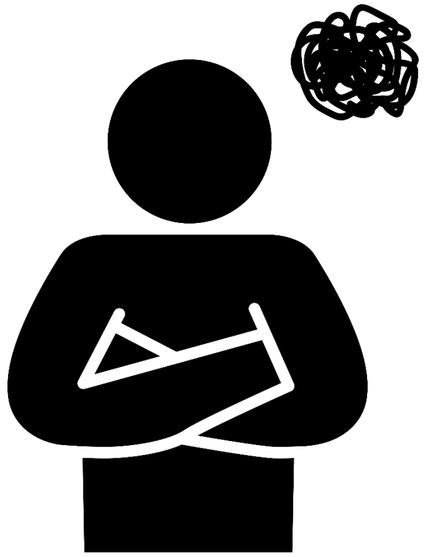
カネ、ヒト、時間があるなら取り組むのがベスト！

DLP、CSPM、CWPP、SSPM、EASM、
SIEM、SOAR、XDR etc.

現実的には・・・

中小企業の課題・・・

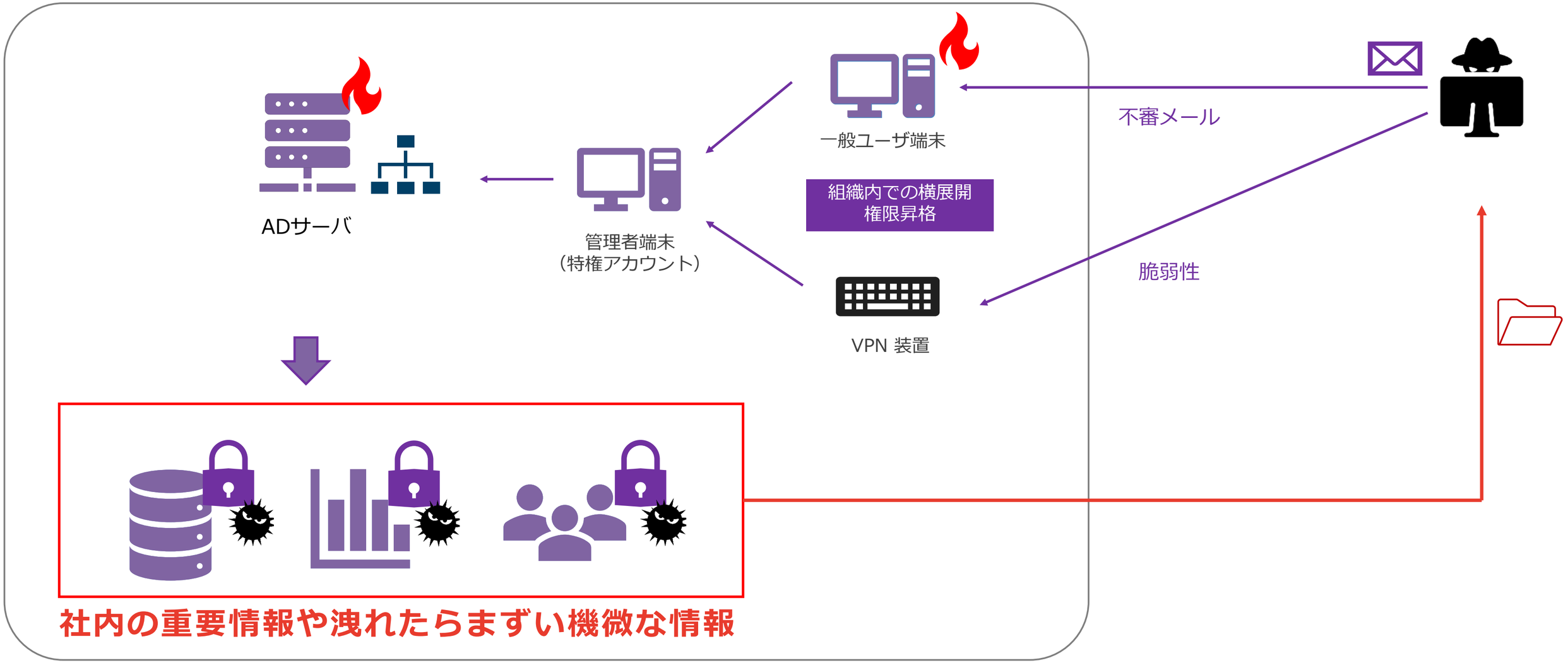
・費用が高い！
・人材がいない！
・工数（時間）が取れない！



できることから始める対策！
Active Directoryに最優先でEDRを入れましょう！

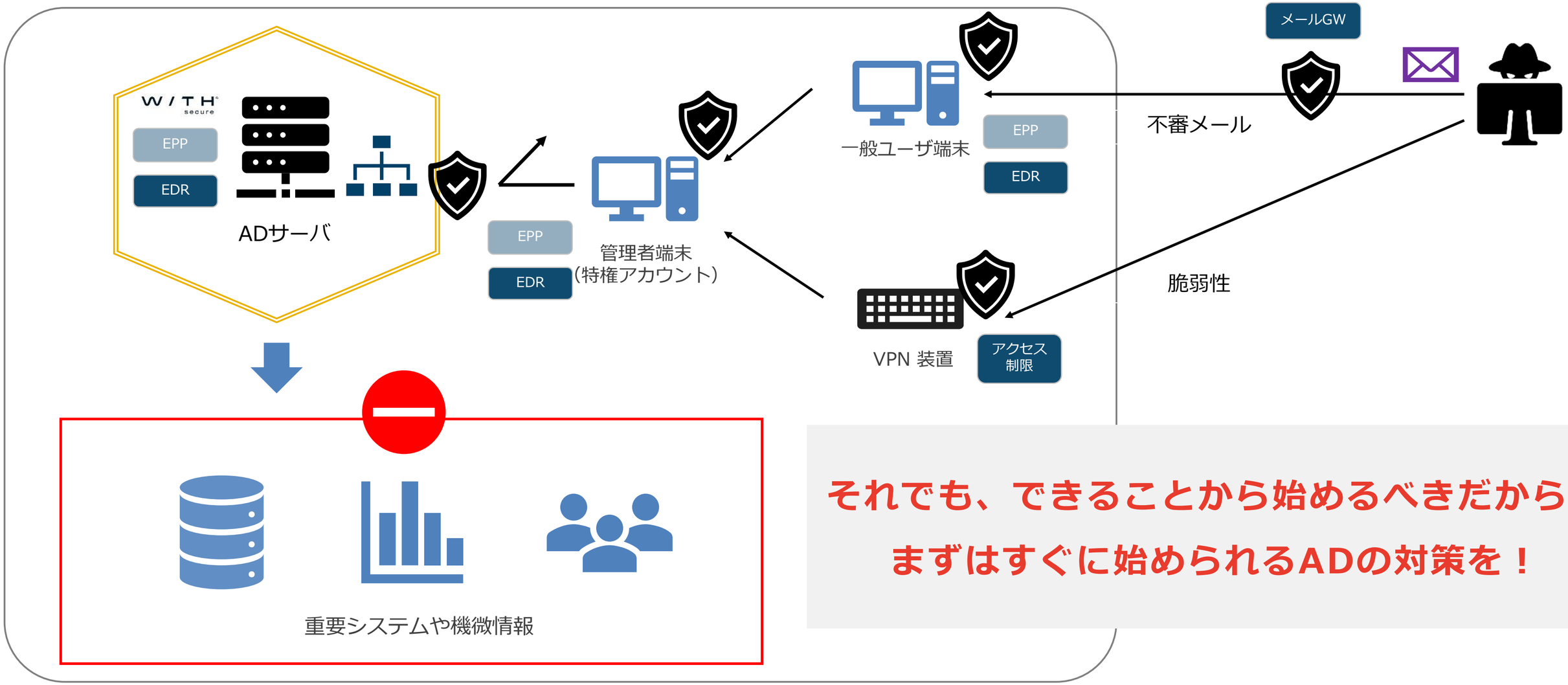
一般的な攻撃のケース

偵察　⇒　初期侵入　⇒　横展開（ラテラルムーブメント）　⇒　攻撃の実行



求められるセキュリティ対策

当然本来は多段式に対応するのがベスト！

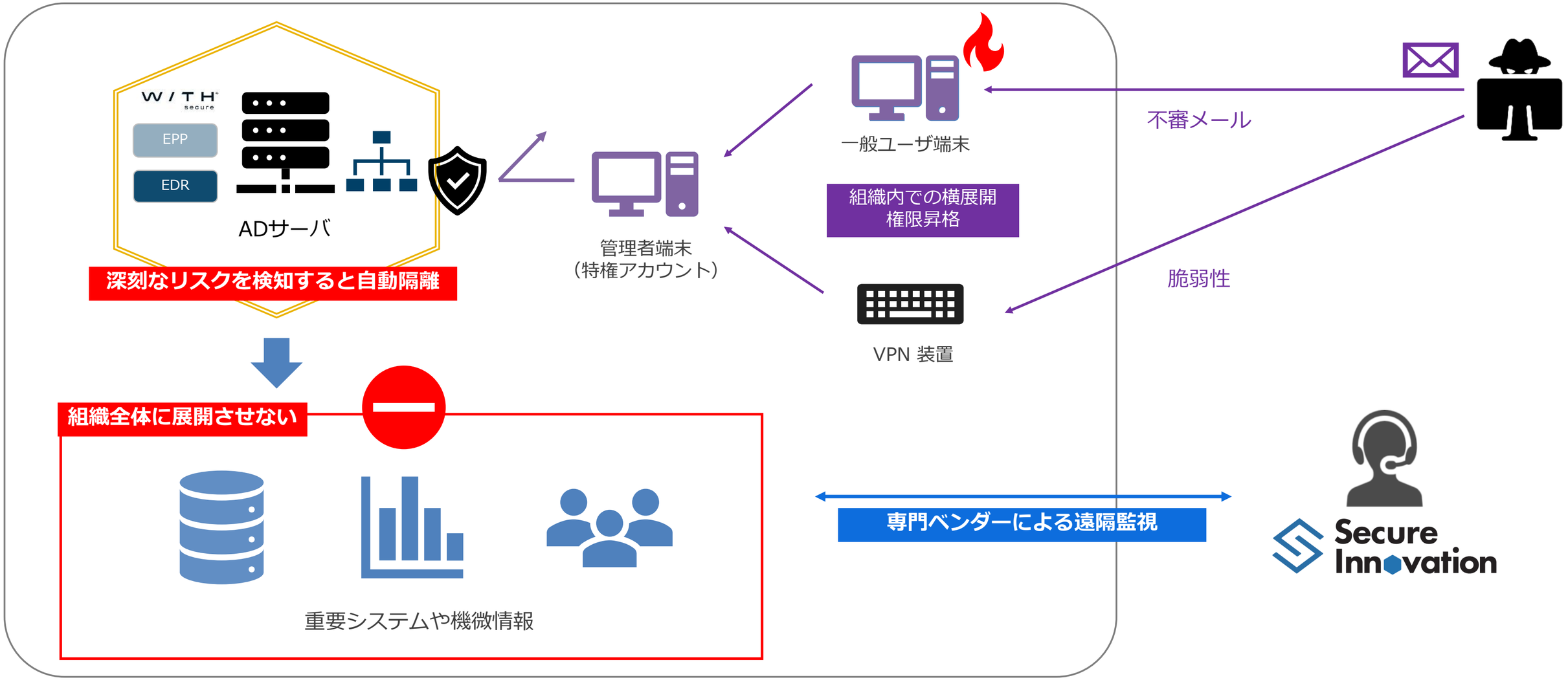


それでも、できることから始めるべきだから…

まずはすぐに始められるADの対策を！

セキュリティ対策の一歩目としてのEDR

ADサーバにEDRを導入することで［ラテラルムーブメント］に効率的に対応



中小企業の課題を解決

中小企業の課題・・・

・セキュリティ対策は費用が高い

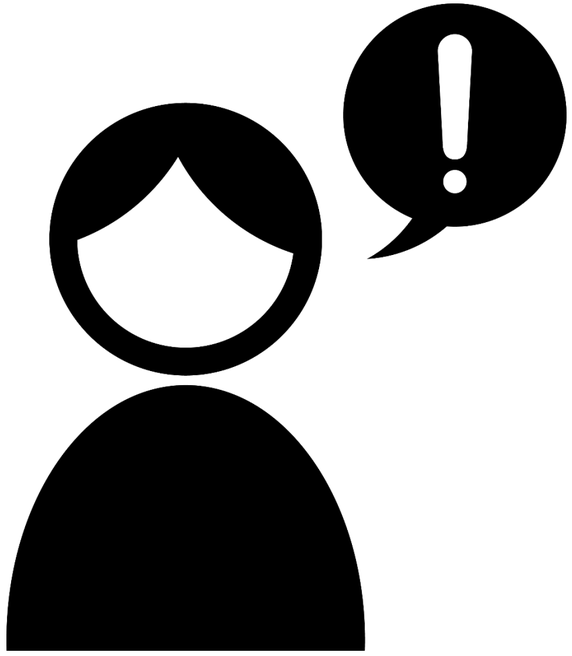
⇒　価格を抑えて導入！17,000円～

・アラート対応できる人材がいない

⇒　専門家の支援を受けられるMSS！

・入れ替えの工数を取れない

⇒　ADサーバ2台～ですぐ導入！



EDRサービス紹介

シンプルで高機能！中堅・中小企業の管理者をサポートするEDR
WithSecure Elements Endpoint Detection and Response

事前対策	ソフトウエアアップデート 脆弱性パッチ管理	デバイスコントロール USB 無線デバイスなど接続制御	EPP / EDR
侵入時の対策	DEEPGUARD 振る舞い検知 マルウェア対策	ブラウザ保護 不審 URL 対策	
侵入後攻撃を受けた場合の対策	ランサムウエア対策 データロールバック	端末の不審挙動検知 インシデントの発見と通知	ネットワーク自動隔離 脅威の封じ込め

ドイツAV-TEST Advanced EDR Testにおいて、
『Approved Advanced Endpoint Detection and Response』を受賞！

EDRサービス紹介

特長1：高リスクのアラートが発生した場合はネットワークから自動隔離

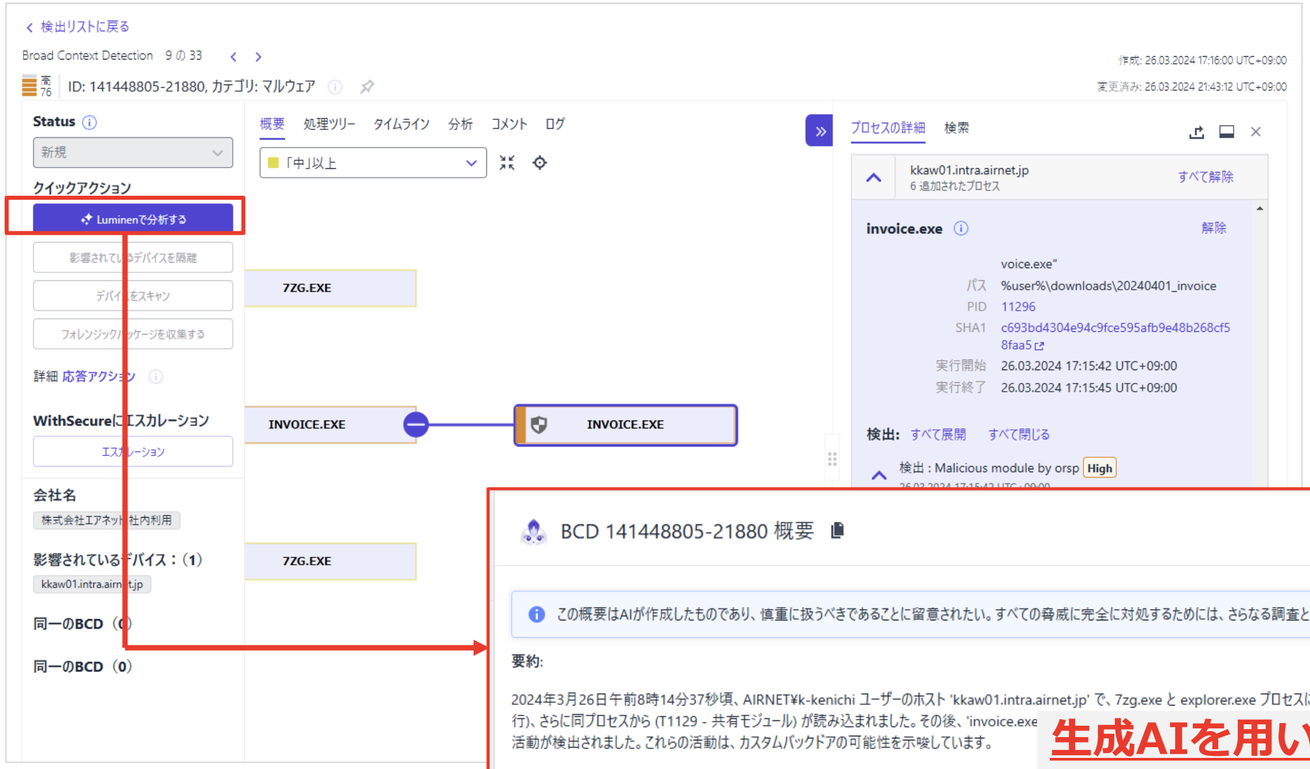
アラート内容を解析し端末の隔離、遮断を判断するEDRですが、判断遅れは命取りに！

本製品ではインシデントをスコア付けし一定以上に達した時点で
強制的に端末を隔離することで被害の拡大を最優先で防ぎます

EDRサービス紹介

特長2：生成AI “Luminen” によるアラート解析

Luminen



生成AIを用いてアラート全体を解析し表示してくれます。

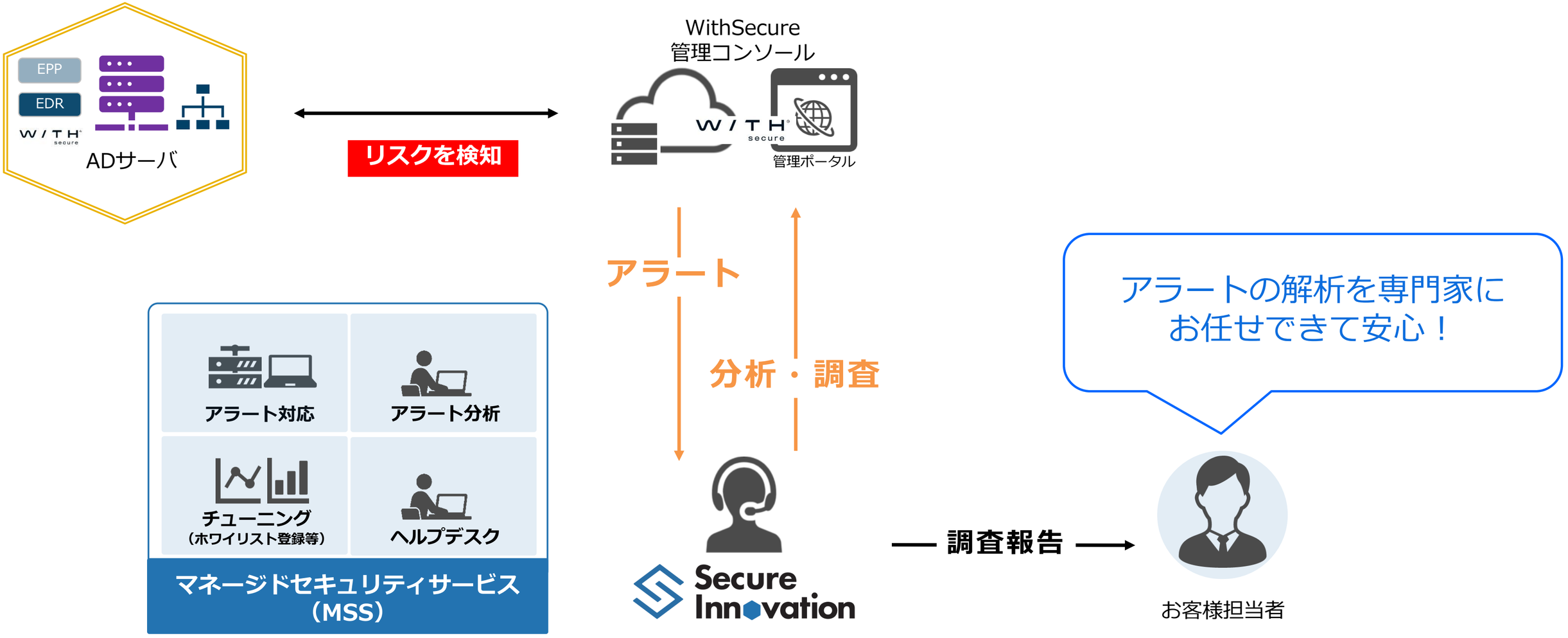
単一のログを確認する従来の機能に比べ
発生時系列やログ同士の関連性が分かりやすく
インシデント調査が効率的行えます。

EDRの検出項目

検出項目	内容
マルウェア	コンピュータ、サーバ、クライアント、またはコンピュータネットワークに損害を与えることを意図的に設計されたソフトウェア。
フィッシング	ユーザに個人情報や機密情報（たとえば詐欺メールを利用して）を開示させようとしているプロセス。
権限昇格	ユーザーアクセスを拡張しようとしています。たとえば、管理者として複数回ログインしようとしています。
異常なファイル アクセス	プロセスは異常なファイルにアクセスしています。たとえば、特権なしで複数の種類のドキュメントやシステムファイルにアクセスしたり、同様のことを行ったりしています。
異常なファイル変更	このプロセスでは、ファイルを変更します。たとえば、システムバイナリの変更、ファイルの実行可能ファイルへの変更、ログファイルの削除、シャドウコピーの削除、実行後の実行可能ファイルの削除などです。
異常なネットワーク接続	プロセスの異常なネットワークアクティビティが検出されました。たとえば、プロセスがネットワークポートにバインドされている、Twitterに接続している、データをダウンロードしている、または異常な処理を行っているなどです。
異常なプロセスの実行	不審なパラメータまたは異常なファイル パスを使用しているプロセスまたはスクリプト。
バックドアされたファイル	プロセスはファイルを実行しました。このファイルは、不正アクセスを提供し、システムを制御する可能性があります。
CC ネットワーク接続	プロセスが既知のコマンド & コントロール (C&C) サーバへのネットワーク接続を開いています。
セキュリティの設定を変更する	ファイアウォール ルール、管理者ユーザ、開発者モードのアクセスなどの設定を変更しているプロセス。
アタック ツールの作成	悪質な意図を隠すためにローカル コンピュータ上にツールを構築しているプロセス。
侵入拡大	最終的に攻撃の標的となる可能性のあるデバイスを検索しながら、ホスト間を移動することにより、ネットワーク内でさらにアクセスを取得しようとしているプロセス。
悪意のあるプロセス	悪質として知られているプロセス。
ログの異常	異常なログエントリ。

遠隔監視サービス

セキュアイノベーション社のマネージドセキュリティサービス（MSS）でEDRのアラートを遠隔監視



遠隔監視サービス

セキュアイノベーション社　マネージドセキュリティサービス

・専門家による遠隔監視サービス

EDRのアラートはお客様で受け取る必要なし！専門家が代わりに解析し報告だけを受け取れる

・アラートへの対応も支援

実際にアラートの報告を受けても何をすればいいのかわからない…
運用ノウハウをもとに必要な確認事項や対応すべき内容を相談できます！

・コストを抑えたビジネスアワーサービス

24時間365日対応のSOCは高額になりがちで、お客様側の体制構築も必要
受付は24時間、コミュニケーションは平日日中に限定することでコストを抑えてMSSを導入

まとめ

最悪の事態（=組織全体が感染）を防ぐためにまずはADにEDRを入れましょう

・最優先で守るべきはActive Directory

限られた予算・人材の中で優先順位をつけて対応するのであればまずはここから
低コストですぐに始められることが魅力的！

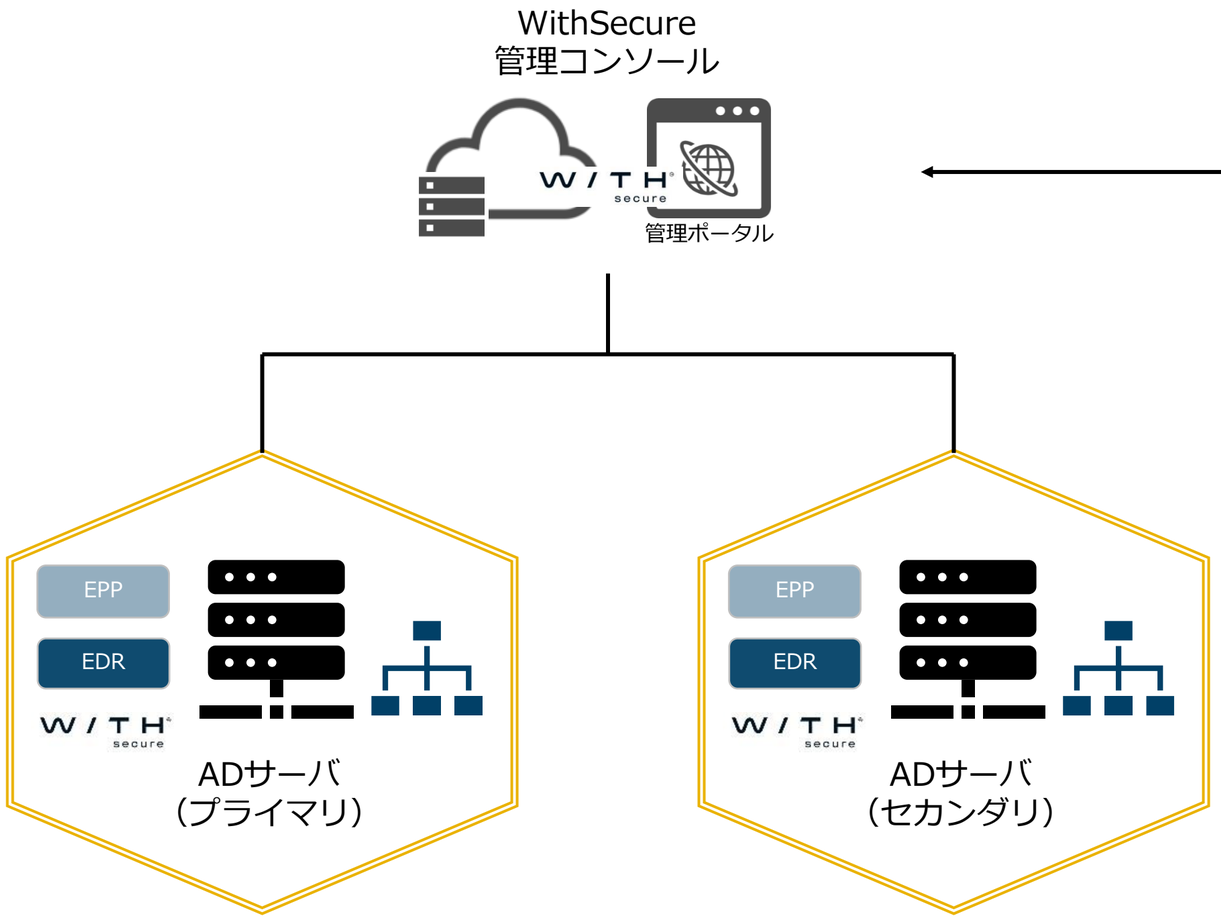
・適切な権限管理や脆弱性対策は必須

EDRを入れたから必ず安全ということではありません
権限やパスワードの管理、アクセス制限、脆弱性管理など基本的な対策は必ず行いましょう

・冗長化や復旧手順、バックアップ手順の確認

EDRの自動隔離機能は被害拡大防止に有効ですが、ネットワークへの復旧も必要です

価格



遠隔監視サービス（MSS）

月額10,000円

EDRサーバ向けライセンス

月額3,500円 × 2台

Active Directory向けEDR + MSSパック

月額17,000円！

価格

■ EDRライセンス費用

	品目	月額費用（税別）
1	エンドポイントセキュリティ プラス EDR（Windows Server）	3,500円 / 1ライセンス

※通常納期5営業日

■ マネージドセキュリティサービス（MSS）

	品目	月額費用（税別）	
		月次レポート無し	月次レポート有り
1	マネージドセキュリティサービス　サーバ 2 台監視プラン	10,000円	25,000円
2	マネージドセキュリティサービス　サーバ 5 台監視プラン	20,000円	35,000円
3	マネージドセキュリティサービス　サーバ 10 台監視プラン	40,000円	55,000円

次のステップ・・・

全社展開も、もちろん承ります！

WithSecure
管理コンソール

管理ポータル

EPP
感染しないための対策

マルウェア対策/ブラウザ保護/USB制御など法人に必須の機能を揃え
ウィルス感染や情報漏洩の脅威から強固にガードします。


PC
（Windows/Mac）


サーバ
（Windows）


モバイル
（Android）

EDR
侵入後の早期発見と被害最小化

イベントログを監視し、不審な動作を検出すると管理者へ通知します。
高リスクの端末はネットワークから自動隔離し被害の拡大を防ぎます。


PC
（Windows/Mac）


サーバ
（Windows）

自由な数量を組み合わせで契約可能

AIRnet SUPPORT OFFICE

AIR Internet Service

電話・メールでの
契約者向けサポート窓口

【対応時間】

平日　10:00 ~ 12:00
　　13:00 ~ 18:00

※管理画面の設定項目や操作方法の
サポートのみ承ります。
アラートの内容や対処方法に関する
ご質問は回答できません。

＋

セキュアイノベーション MSS

Secure Innovation

EDR運用支援サービス

お客様に代わってアラートを受信し
解析と対応支援を行います。

【対応時間】

平日　9:00 ~ 17:30
（祝祭日・年末年始休日を除く）

エアネットのサービス

メールセキュリティを筆頭に多角的なセキュリティ対策をご提案いたします

標的型メール訓練

・訓練による意識向上
・擬似感染者の把握、教育

受信メールに含まれる脅威に対応

セキュリティプラス

・不審メールの URL /添付ファイル対策
・ZIP 暗号化ファイル対策

Active!zone

うっかりミス、情報漏洩対策

メール誤送信防止サービス

・宛先間違い、添付ファイル間違い対策
・ドッペルゲンガードメインなどへの送信制限

Active!gate

送信ドメイン認証 レコードの管理

ドメイン管理・DNSサービス

・自ドメインになりすましされない対策
・DMARC レポート分析

受信メール対策

送信メール対策

Webサーバセキュリティ対策

不正アクセス　サイト改竄対策　DDoS対策

www サービス

・攻撃に利用されないための対策
・加害者にならないための対策

端末まで侵入された場合の最終防壁

エンドポイント セキュリティPC/サーバ

・マルウエア侵入検知
・充実した端末の保護機能

VPN 装置

固定 IP が利用できる ドコモ回線 SIM

・認証に IP アドレスを追加し認証強度を向上

Secure Innovation

感染が疑われる端末の封じ込め

エンドポイント セキュリティ ＋ EDR PC/サーバ

・インシデント発見　通知
・高リスク端末の自動隔離

固定 IPSIM

EPP

EDR

リモートワーク

ありがとうございました