東京エレクトロン デバイス

Active Directoryを保護する新たなアプローチ

ITDRRで実現する「検知」「修復」、そして即時の「復旧」

昨今のランサムウェア攻撃は、 単なるデータの暗号化にとどまらず、 いまや事業そのものを完全停止させる高度な手法へと進化しています。 企業の「心臓部」ともいえる Active Directory を標的とし、 これを掌握することで重要システムへのアクセス権を奪取し、 組織全体を支配下に置きます。 このリスクに対して、 企業はいかにして事業継続を確保することができるのか――。「ITDRR」（Identity Threat Detection and Response, Recovery）という新たなアプローチに基づく包括的なソリューションを紹介します。

Active Directoryが狙われると事業に与えるインパクトが甚大に

ランサムウェア攻撃はますます悪質化し、大きく姿を変えています。かつては個人のPCを暗号化し、身代金を要求する比較的小規模な攻撃が主流でした。しかし現在では、企業の基幹系を中心とした重要システムを停止させ、事業活動そのものを麻痺させることを目的とした攻撃が一般化しています。

なかでも攻撃者が最優先で狙うようになったのが、Active Directory（以下、AD）です。
ADは、ユーザーや権限、認証情報を一元管理する仕組みであり、企業ITの根幹を支えています。まさに企業インフラの心臓部とも言える存在です。

このADを攻撃者に掌握されてしまうとどうなるでしょうか。「セキュリティ製品を無効化する」「社内のあらゆるシステムへのアクセス権を奪取する」「特権IDを自由に作成・変更する」といった、攻撃者の意のままの行為が可能となります。

結果として、社内のほぼすべてのシステムに自由にアクセスできる状態となり、被害は一部に留まらず全社規模へと拡大します。だからこそADは、攻撃者にとって最もROI（費用対効果）の高い標的となっているのです。

実際に国内でも、ランサムウェア攻撃を受けて操業停止に追い込まれる企業の被害が後を絶ちません。昨年、国内の大手飲料メーカーを襲ったランサムウェアグループ「Qilin（キーリン）」による下記の犯行手口は、まさに昨今の攻撃パターンを象徴しています。

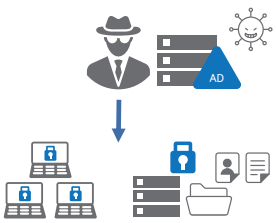
第1段階：VPNや公開サーバーの脆弱性を悪用して企業内部に侵入
第2段階：内部で偵察行動を実施し、ADを特定
第3段階：ADを掌握し、企業の認証基盤全体をコントロール
第4段階：基幹システムや重要サーバーを暗号化し、身代金を要求

この一連の攻撃においても、ADの掌握が決定的な転換点となっていることは、火を見るよりも明らかです。

なぜADが狙われるのか？　ID基盤は、攻めるに易く甚大な被害を与えられるため、非常に狙われやすい

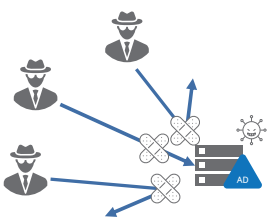
ADを狙う理由

- 認証・権限・アプリ・システムを統括する中枢基盤
- 一度攻撃者が管理者権限を得ると「企業全体の神」に
- 一攻撃成功時のリターンが極めて大きい



ADを取り巻く現状

- 2000年代の設計思想が現在も残存
- Kerberoasting/DCSync/Relay など攻撃手法は高度化
- パッチや設定のみでは防ぎきれない領域が存在



ハイブリッドの落とし穴

- 多くの企業は AD → Entra を同期
- ADが攻撃されると、Entraが踏み台になるケースも
- Entraが健全でも漏えいは防げない構造
- オンプレの脆弱性がクラウドまで波及する

ADからの脱却が難しい理由とは？

ADは今から約25年以上も前に設計された技術であり、当時の設計思想を色濃く残したまま使われ続けています。一方で攻撃手法は日々進化を続けており、パッチ適用や設定変更といった従来型の対策だけでは、防御しきれない状況が生まれています。昨今の攻撃手法やゼロトラスト前提の脅威モデルを十分に織り込んだ設計となっていないため、本質的に攻撃に対してパワーバランスを保てない構造となっているのです。

近年はMicrosoft 365やMicrosoft Azure関連のサービスの利用拡大に伴い、クラウド型のID・アカウント管理サービスである「Entra ID」(旧Azure AD)を利用する企業も増えていますが、これで問題が回避されるわけでもありません。その多くが、オンプレミスのADとEntra IDを同期させるハイブリッド構成を採用しているためです。この構成ではオンプレミスのADが攻撃者によって掌握された場合、同期を悪用され、Entra ID側も侵害が及ぶおそれがあります。クラウド移行が進んでも、オンプレミスにADが残る限りリスクは解消されないのです。

ならばADをなくせばよいのかといえば、それも簡単ではありません。クラウドサービスへの移行が進む中でも、多くのシステムがオンプレミスのADに依存し続けているからです。社内無線LANやレガシーな業務ソフトウェアなど、ADで認証ができないと通信すらできない設計となっているものも多く、企業にとってADは「なくせないもの」として今後も存続し続ける運命にあります。

なお、万一ADが暗号化されてしまった場合、その復旧は極めて困難です。マイクロソフトが公開している一般的なAD復旧手順は29ステップにも及び、専門知識と多大な時間を要します。途中で一つでも誤りがあれば最初からやり直しになることもあり、手順通り進めたとしても整合性が取れず完全復旧に至らないケースもあります。

年商500億円規模の企業では、AD停止による損失は1日あたり1～2億円に達するとも言われています。復旧に数週間、あるいは数か月を要すれば、その影響は経営レベルの問題へと発展します。ADは、止まること自体が許されないシステムなのです。

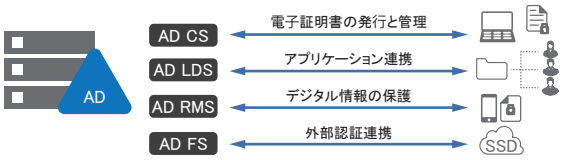
ADが抱える課題　既存対策に加え、ID基盤そのものを守る仕組みが必要

ADをなくせない理由

- 多くのシステムがオンプレADに依存し続けている
- Entraへの完全移行はコスト・改修が膨大
- レガシー資産・工場設備・Wi-FiなどもAD前提で動作
- 結果：ADは「なくせないもの」として存続し続ける

既存対策では止めきれない理由

- 中継攻撃・フィッシングが高度化しMFAを突破
- 正規IDを使われるとEDRでは異常検知が困難
- AD制圧後、EDRを無効化されるケースも
- IDそのものを守る基盤が必要



ID基盤を守る新たなアプローチ「ITDR」

では、どうやってAD基盤を保護すべきでしょうか。まず考えられるのが、MFA（多要素認証）やEDR（Endpoint Detection and Response）といったセキュリティ対策ですが、これだけでは十分とは言えません。

MFAはログイン時の入口対策に有効ですが、正規IDが乗っ取られた後の横展開や権限乱用までは十分にカバーできません。EDRも端末やサーバーのプロセスを監視することはできますが、AD内部の不正な権限変更を網羅的に検知することは困難です。その結果、正規IDを悪用したなりすましログインによって、これらのセキュリティ製品をすり抜ける攻撃が横行しているのです。

そこで東京エレクトロンデバイスが推奨しているのが、ITDR（Identity Threat Detection and Response）と呼ばれるID基盤向けセキュリティ対策の導入です。

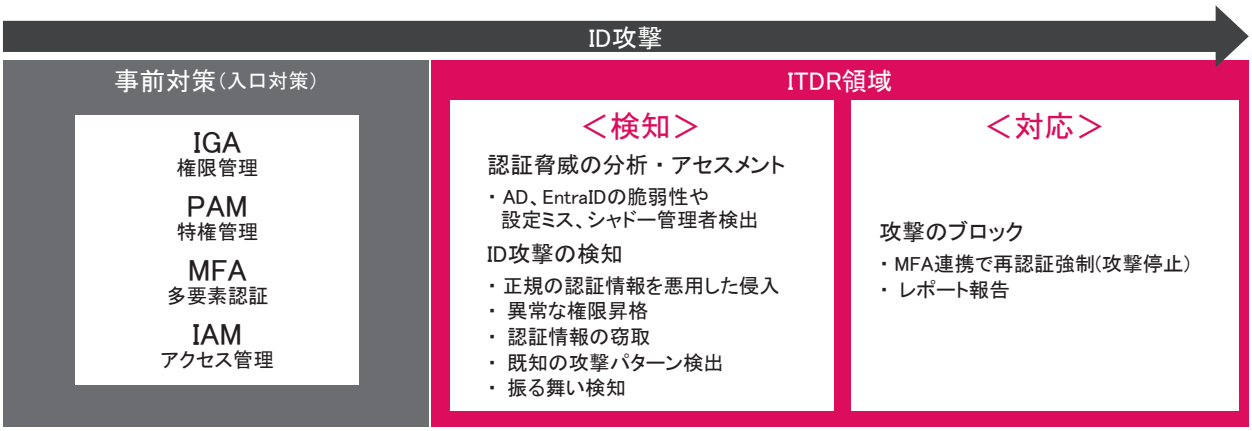
ITDRは、ADやEntra IDなどのIDインフラ上における認証トラフィック等の振る舞いを検知し、対応する新たなセキュリティ対策カテゴリーでのアプローチとなります。

従来の対策として、入口側ではMFAなどが「侵入を防ぐ」ことに、端末側ではEDRが「侵入後の不審プロセスの検知」に注

力します。これに対し、ITDRはそのさらに先の「AD・Entra IDへアクセスされること」を前提とした防御戦略を採用しているのがポイントです。ADに対する不正なアクセスやトラフィックを常時監視し、振る舞いを即座に検知・ブロックすることで被害拡大を防ぎます。

ITDRとは？ ITDR(Identity Threat Detection and Response)

ADやEntra IDなどのIDインフラ上における認証トラフィック等の振る舞いを検知し、対応する新たなカテゴリー
ADなどに侵入されてしまったことを前提に、振る舞い検知＆対応するソリューション。



ITDRを超えるITDR“R”を実現する「Semperis」

ITDRのアプローチを体現する製品として、東京エレクトロンデバイスでは米Semperis（センペリス）社の「DSP・ADFR・DRET」を提供しています。

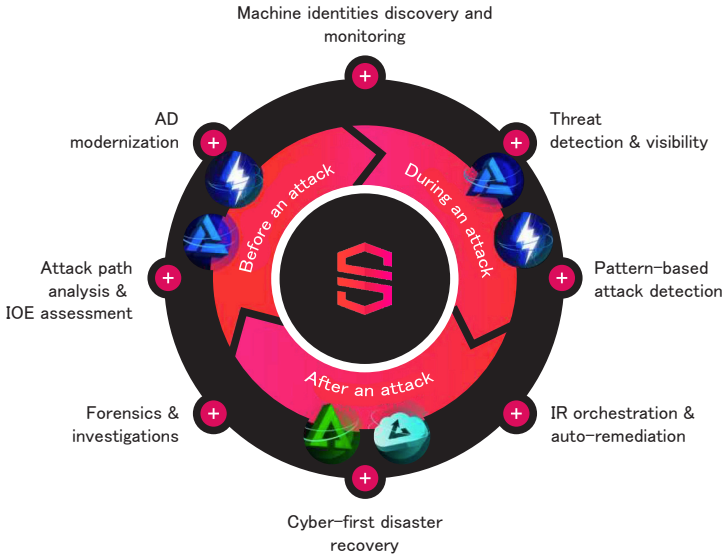
同社は Microsoft MVPや元 Microsoftのフィールドエンジニアなど、AD/ID 分野の専門家が中心となり、2014年に創業した企業です。インシデントレスポンスサービスとして事業を開始し、その豊富な知見を製品化することでSemperisは誕生しました。グローバルではすでに2億を超えるアイデンティティセキュリティ基盤をSemperisが保護しています。

Semperisの最大の特徴は、ADやEntra IDに対する攻撃の「検知」から「修復」「復旧」までを網羅するプラットフォームとして設計されている点にあります。その意味でSemperis は、ITDRを超える「ITDR“R”」(Identity Threat Detection and Response, Recovery)を実現するソリューションとなります。

Semperis はITDRではなく“ITDRR”

AD/Entra IDの攻撃検知から
復旧までを網羅するプラットフォーム

- ITDRR = Identity Threat Detection and Response, Recovery
  「アイデンティティ脅威の検知と対応＋復旧」
- AD/Entraの改ざん修復・暗号化時のリストアまで対応
- 攻撃を受けても「業務停止を回避」する設計



具体的にSemperisは、下記のような主要製品のラインナップで構成されています。

1つ目は、「Directory Services Protector（DSP）」。ADおよびEntra IDの変更を常時監視し、不正な権限変更や攻撃の兆候を検知します。検知後は自動的に元の状態へ復元することで、攻撃の影響を最小化します。例えば、一般ユーザーに突然「特権ID」を付与されるといった不審な動きを即座に検知し、自動的に元の権限状態へ戻します。これにより、正規IDを悪用したなりすまし攻撃にも対応することが可能です。

2つ目は、「Active Directory Forest Recovery（ADFR）」。ADを即時復旧するソリューションです。最大の特徴は「マルウェアフリーな復元」を実現する点にあります。ADのデータを定期的にバックアップし、常に保持しています。リストア時にはクリーンな状態の新しいOSへバックアップデータを展開します。なお、復元前にフォレンジック機能でバックドアの有無をチェックします。この仕組みによりランサムウェアの再感染リスクを大幅に軽減しつつ、前述した29ステップを自動化し、マルウェアフリーな環境で復旧します。これにより、手動では数ヶ月かかる復旧作業を数十分～数時間で完了することが可能となります。

3つ目は、「Disaster Recovery for Entra Tenant（DRET）」。誤操作や攻撃によって削除・改ざんされたEntra IDの重要なクラウドIDリソースを、迅速かつ確実に復元するための専用ソリューションです。ユーザー、グループ、ロール、アクセスポリシーなど、ビジネス継続に不可欠な資産を短時間で回復し、長期化するダウンタイムのリスクを低減します。

その他にも「Purple Knight」という製品は、攻撃ベクトルに対して包括的なテストを実行し、ハイブリッドID環境内の危険な構成とセキュリティ脆弱性を可視化します。

また、「Forest Druid」という製品は、ADやドメインコントローラーなどの「Tier 0」を狙う攻撃パスをグラフで表示し、防御境界の再設計を支援します。

このようにSemperisは、単一ベンダーでITDRRの主要な要素をカバーできる点で優位性があります。

Semperis 特徴 【IDを守るための重要事項】

- 社内の中核を担うAD・Entra IDを保護するための4ステップ
- 正規IDによる「なりすましログイン攻撃」への対策。AD内の権限変更を検知・対応＆即時修復
- 企業の業務継続性を維持するための、即時復旧機能

東京エレクトロンデバイスがID基盤保護を全面サポート

繰り返しますが、ADは多くのシステムが依存しているため、「やめる」という選択肢は現実的ではありません。従来のセキュリティ対策だけでは防ぎきれない今、企業に求められるのは、ID基盤そのものをしっかり守り、万一の際にも即座に復旧できる体制の構築です。

ITDRRという新たなアプローチは、この課題に対する答えの一つです。中でもSemperisは、「検知」「修復」「復旧」を一貫して提供できる数少ない優れたプラットフォームとして、企業の事業継続を支えます。東京エレクトロンデバイスは、日本におけるSemperisの正規代理店として、お客様のID基盤保護を全面的にサポートしています。

Semperis に関する
お問い合わせはこちら

東京エレクトロン デバイス株式会社
CN BU
https://cn.teldevice.co.jp/
本社：〒150-6234 東京都渋谷区桜丘町 1 番 1 号
渋谷サクラステージ SHIBUYA タワー 35 階
名古屋：〒451-0045 愛知県名古屋市西区名駅 2-27-8
名古屋プライムセントラルタワー 8 階
大阪：〒530-0001
大阪市北区梅田 3-2-123 イノゲート大阪 17 階

Mar 2026