



【緊急配信】 奪われたIDが引き金に— ランサムウェアで止まる企業システム

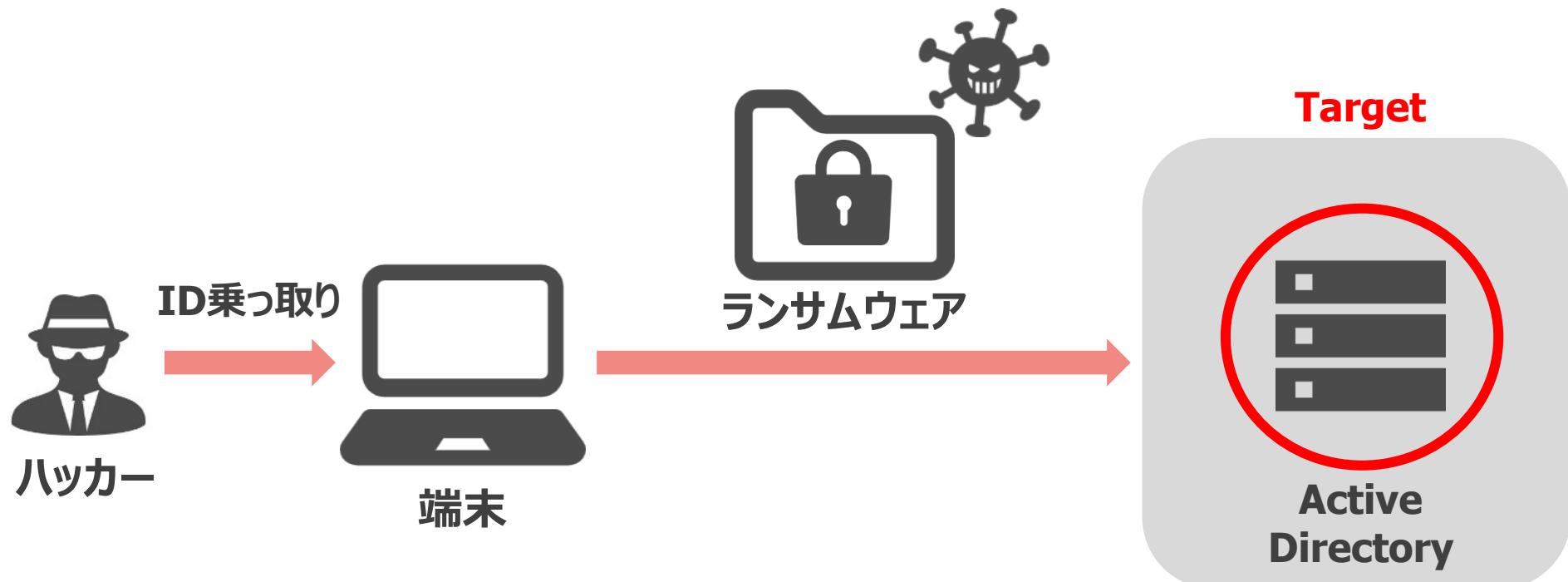
東京エレクトロン デバイス株式会社

2025年11月

Agenda

- はじめに
- ID窃取の現状
- Semperis社のご紹介
- デモ

- 近年、国内でも**システム停止**や**情報流出**のニュースが相次いでいます。
- 製造業や流通、自治体など幅広い業種にて、**ランサムウェアによる業務停止**が発生しています。
- 被害の多くに共通しているのが、「**最終的にID基盤が狙われている**」という点です。





ID窃取の現状

90%の企業がActive Directoryを利用

- 2000年からある技術のため攻撃手法が確立
- サイバー攻撃の**80%**は認証情報の悪用

被害はEntra IDにも

- ADを掌握されると踏み台にされEntra IDも被害に
- Entra IDがセキュアな設定だとしても攻撃リスク有

**Active Directoryは攻めるに易く、
企業へ甚大な被害を与えることが出来るため標的とされやすい**



ID基盤の掌握後にハッカーが行う攻撃例

- ・EDRの無効
- ・バックアップ削除/暗号化（ランサムウェア）
- ・ハッカー用特権アカウント追加

IDが奪われると全てが停止する



これで全ての資産に
自由にアクセスできる！



特権ID



クラウド



データベース



サーバー



業務アプリ



ID基盤



情報連携
アプリ



開発環境

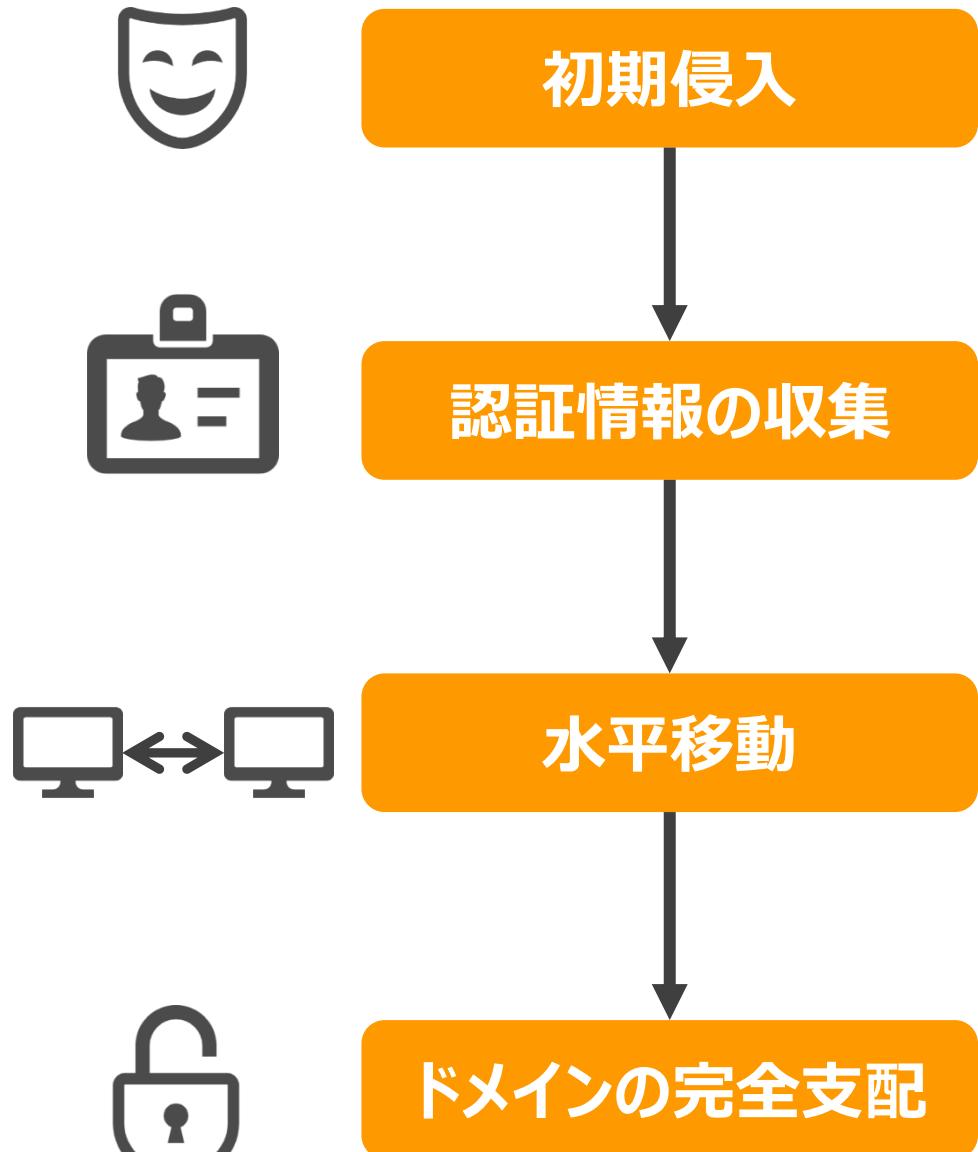


エンド
ポイント



セキュリティ
製品

IDは全ての入口、奪われるとすべてのシステムが攻撃者の手に落ちる



攻撃者が企業ネットワークに最初に入り込む段階

フィッシング、VPN/VDIの乗っ取り、サーバー基盤の脆弱性利用

侵入した端末からAD情報を集める段階

パスワードスプレー、ブラウザやツールの保存パスワードで収集

収集したIDを使って、他のPCやサーバーへ移動

特権IDを求めてRDP、SMB、WinRM、WMI を使った水平移動

特権アカウントを使ってドメインを支配

ランサムウェア混入、データ窃取、バックアップの破壊

どのくらい業績に影響があるのでしょうか？

想定される被害金額



JCIC サイバーリスクの数値化モデルから試算（年商1000億円企業における社内報告資料例）

直接被害	ビジネス停止による機会損失	▼ 20 億円 5営業日あたり	1日の売上 × 事業中断期間
	法令違反による制裁金	▼ 40 億円	現地の法規制に違反したことにより、制裁金や罰金を課せられる場合がある。2018年5月に施行されたGDPRによって違反した企業は高額の制裁金（売上金 4%、または2000万ユーロのいずれか高い方）が課せられる。
	事故対応費用	▼ 0.6 億円	サイバー攻撃を受けたかどうかや攻撃を受けた場合の影響範囲や原因を調査するための費用。事項対応費用は数百万円～数千万円が一般的。
間接被害	純利益への影響	▼ 10.5 億円	JCIC調査の結果、セキュリティ事故発生年度は平均21%の純利益減が発生
	時価総額への影響	▼ 300 億円	JCIC調査の結果、セキュリティ事故の適時開示50日後に株価が平均10%減少

JCIC サイバーリスクの数値化モデル

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/pdf/003_04_00.pdf



Semperisご紹介

社名	Semperis Inc.
本社住所	米国ニュージャージー州 ホーボーケン
設立	2014年
代表者	Co-Founder & CEO Mickey Bresman
従業員数	550+
受賞その他	サイバーセキュリティ企業の成長率トップ5 4年連続で二桁成長を達成 Fortune「Cyber 60 2024」リストに選出

アイデンティティセキュリティ基盤への採用

200+ million

アイデンティティをSemperisが保護





ITDR(Identity Threat Detection and Response)

ID基盤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
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

アイデンティティ保護に必要とされる要素を包括的に提供

平時のアセスメント

攻撃のリアルタイム検知

改ざんされた
特権IDの修復

AD/EntraIDの
リカバリ



DSP

- ・ADやEntra IDのセキュリティアセスメントを継続的に実施
- ・特権IDの付与状況やアタックパスを可視化

- ・AD/Entra IDに対する攻撃をリアルタイム検知
- ・不正な権限昇格や認証トラフィックの振る舞い検知も可能
- ・攻撃により改ざんされた権限、及び設定ミスによる誤った権限を元の状態へ修復



ADFR(AD)



DRET(Entra ID)

- ・万が一、AD/Entra IDがマルウェア感染してしまった場合に安全な新環境へ設定を復旧。
- ・自動復元により迅速に業務復旧。(通常復旧と比較し、90%の短縮)

DSP



攻撃を検知・修復

- AD・Entra ID を常時監視
- 構成の弱点、不正な変更など発見＆対応
- 攻撃の“前”と“最中”に気づいて止めることが可能に

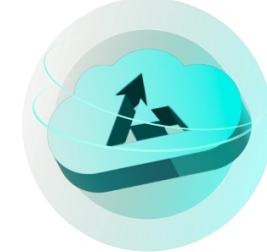
ADFR



ADを復旧

- AD フォレストの復旧手順を自動化
- 数クリックでマルウェアフリーなADを再構築
- ADだけを復旧するので、マルウェアを巻き戻さない

DRET



Entra IDを復旧

- SaaSへのバックアップ
- オブジェクトを柔軟に復元（選択／一括）



Active Directory、Entra IDのリアルタイム監視、変更検知、修復ツール



継続的な脆弱性評価



改ざん防止・追跡

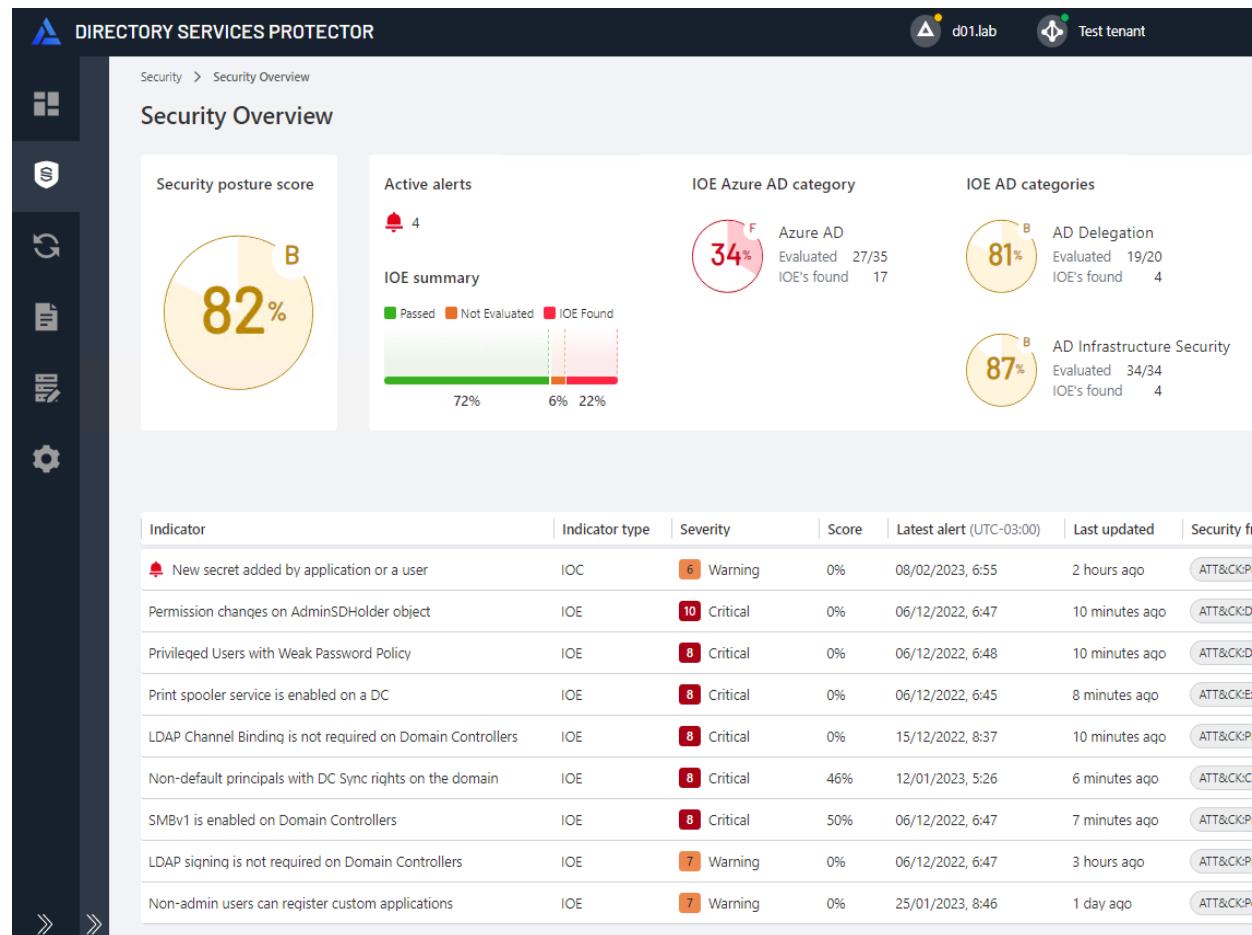


悪意のある変更からのロールバック



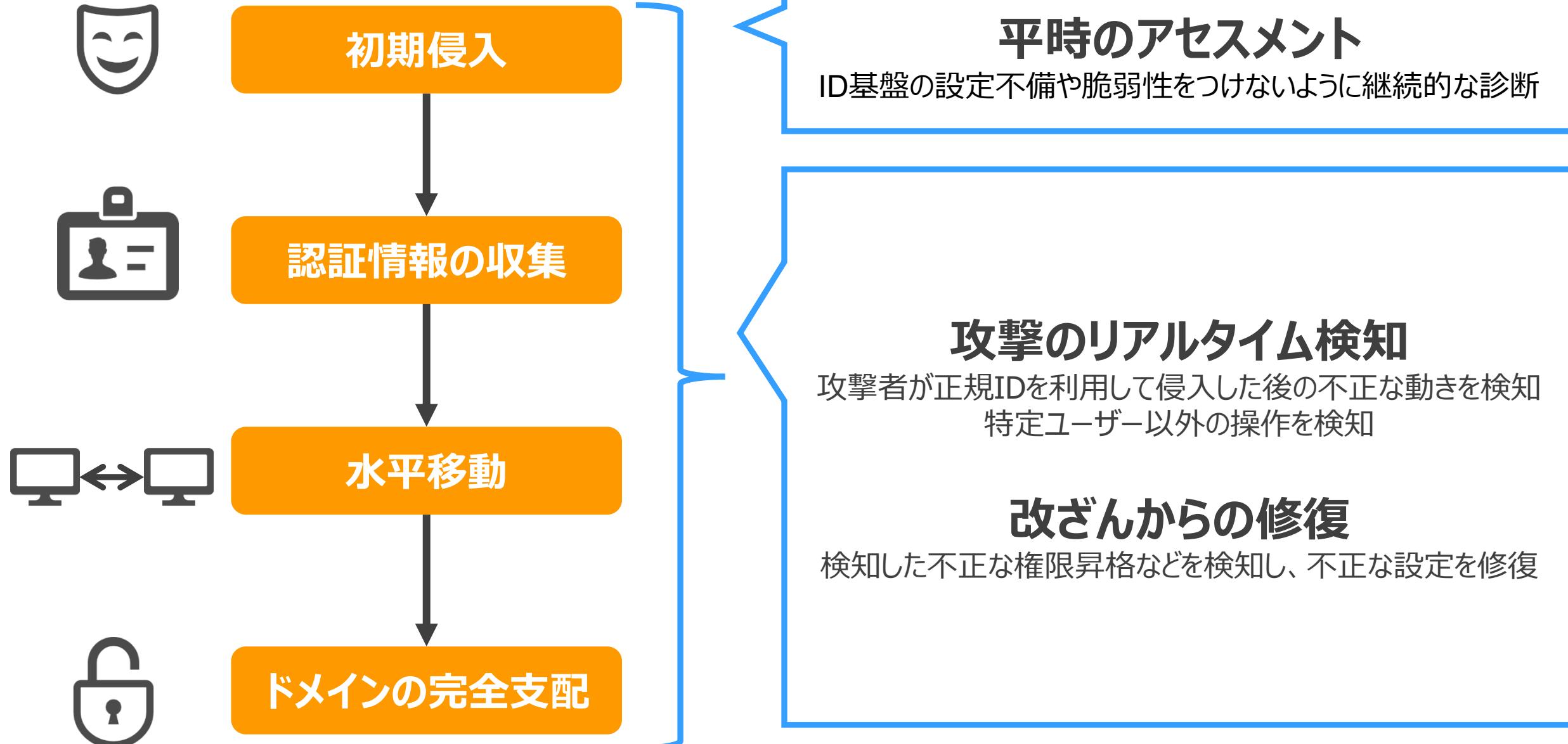
機械学習による高度な振る舞い検知

※追加オプション



The screenshot shows the 'Security Overview' page of the Directory Services Protector tool. At the top, there are two status indicators: 'd01.lab' (green) and 'Test tenant' (grey). The main dashboard features a large circular 'Security posture score' of 82% (B grade), an 'Active alerts' count of 4, and two charts: 'IOE summary' and 'IOE Azure AD category'. Below the dashboard is a table of 'Indicator' details, including type, severity, score, and last updated time.

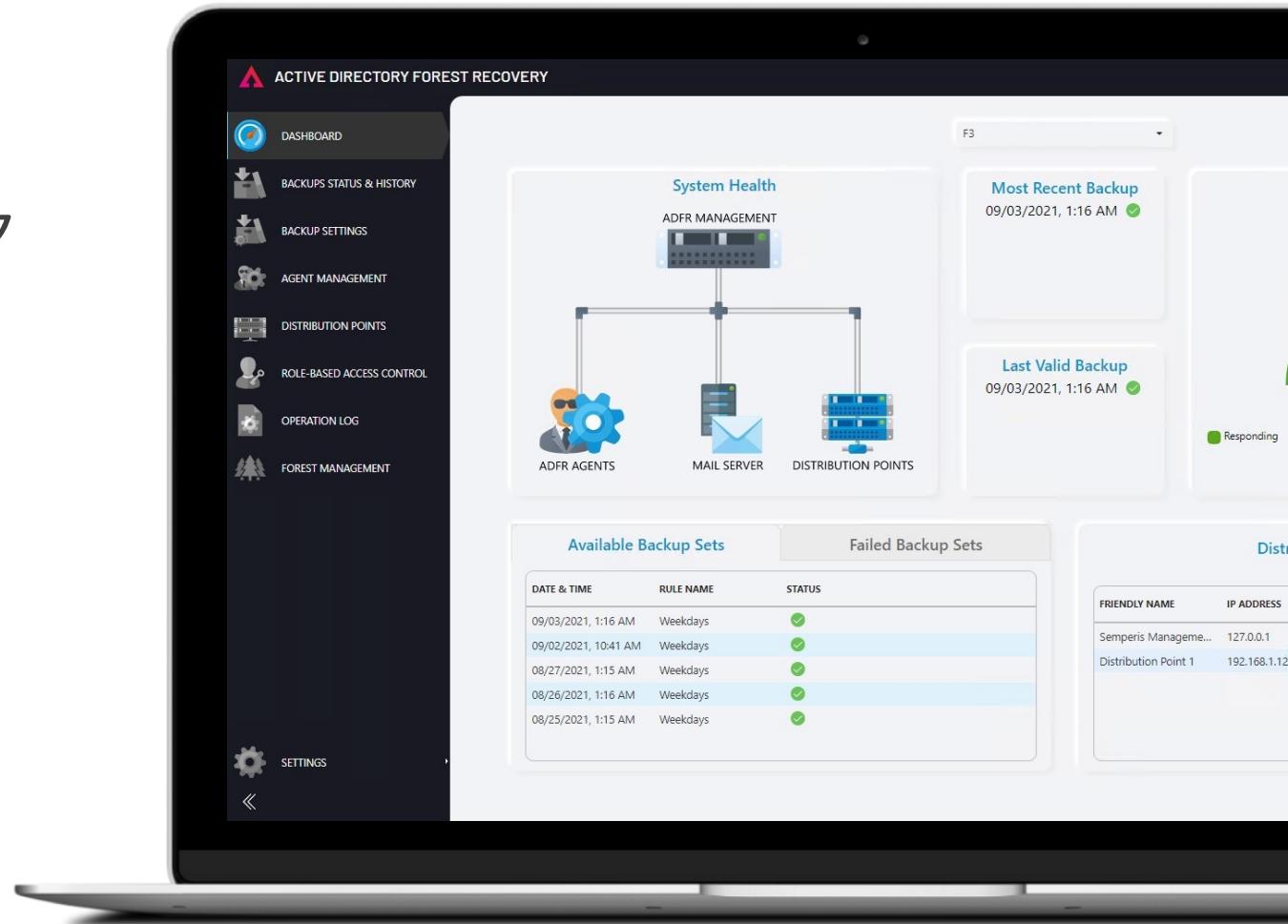
Indicator	Indicator type	Severity	Score	Latest alert (UTC-03:00)	Last updated	Security f...
New secret added by application or a user	IOC	Warning	0%	08/02/2023, 6:55	2 hours ago	ATT&CK: P...
Permission changes on AdminSDHolder object	IOE	Critical	0%	06/12/2022, 6:47	10 minutes ago	ATT&CK:D...
Privileged Users with Weak Password Policy	IOE	Critical	0%	06/12/2022, 6:48	10 minutes ago	ATT&CK:D...
Print spooler service is enabled on a DC	IOE	Critical	0%	06/12/2022, 6:45	8 minutes ago	ATT&CK:E...
LDAP Channel Binding is not required on Domain Controllers	IOE	Critical	0%	15/12/2022, 8:37	10 minutes ago	ATT&CK:P...
Non-default principals with DC Sync rights on the domain	IOE	Critical	46%	12/01/2023, 5:26	6 minutes ago	ATT&CK:C...
SMBv1 is enabled on Domain Controllers	IOE	Critical	50%	06/12/2022, 6:47	7 minutes ago	ATT&CK:P...
LDAP signing is not required on Domain Controllers	IOE	Warning	0%	06/12/2022, 6:47	3 hours ago	ATT&CK:P...
Non-admin users can register custom applications	IOE	Warning	0%	25/01/2023, 8:46	1 day ago	ATT&CK:P...





迅速でマルウェアフリーなADフォレストリカバリ

-  マルウェアフリーなクリーンリストア
-  迅速な回復
-  復旧の自動化



The screenshot displays the Active Directory Forest Recovery (ADFR) software interface. On the left is a dark-themed mobile-style dashboard with a navigation menu:

- DASHBOARD
- BACKUPS STATUS & HISTORY
- BACKUP SETTINGS
- AGENT MANAGEMENT
- DISTRIBUTION POINTS
- ROLE-BASED ACCESS CONTROL
- OPERATION LOG
- FOREST MANAGEMENT

Below the menu is a "SETTINGS" gear icon.

The main area is titled "ACTIVE DIRECTORY FOREST RECOVERY". It features a "System Health" diagram showing connections between "ADFR MANAGEMENT", "ADFR AGENTS", "MAIL SERVER", and "DISTRIBUTION POINTS".

On the right, there are several panels:

- "Most Recent Backup": 09/03/2021, 1:16 AM (green checkmark)
- "Last Valid Backup": 09/03/2021, 1:16 AM (green checkmark)
- A table titled "Available Backup Sets" showing five entries with green checkmarks in the "STATUS" column.
- A table titled "Failed Backup Sets" showing three entries with red X icons in the "STATUS" column.
- A "Distribution Points" table with two entries: "Semperis Management" (IP 127.0.0.1) and "Distribution Point 1" (IP 192.168.1.12).



Entra IDをサイバー攻撃から災害復旧



IDの削除/攻撃/構成ミスからの復旧



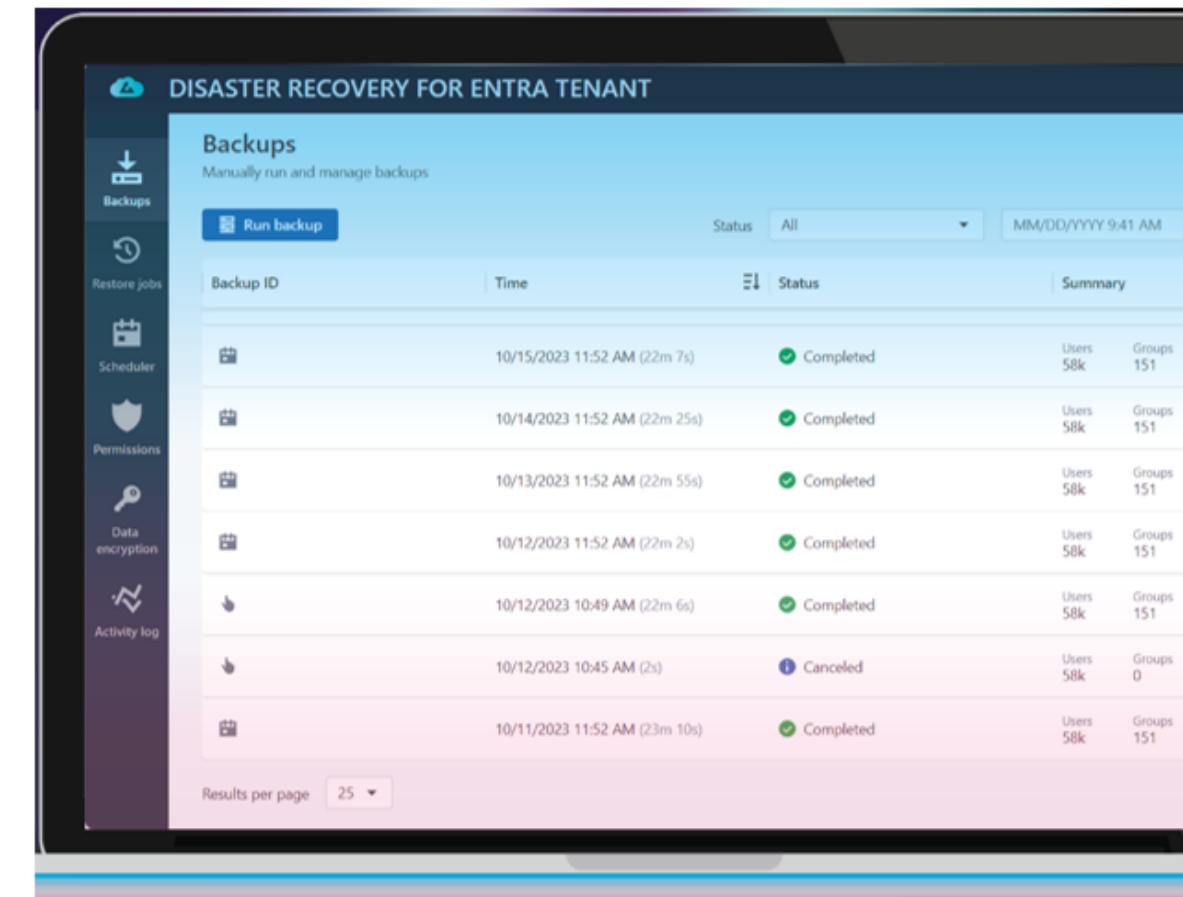
柔軟な復旧（一括、ピンポイント）



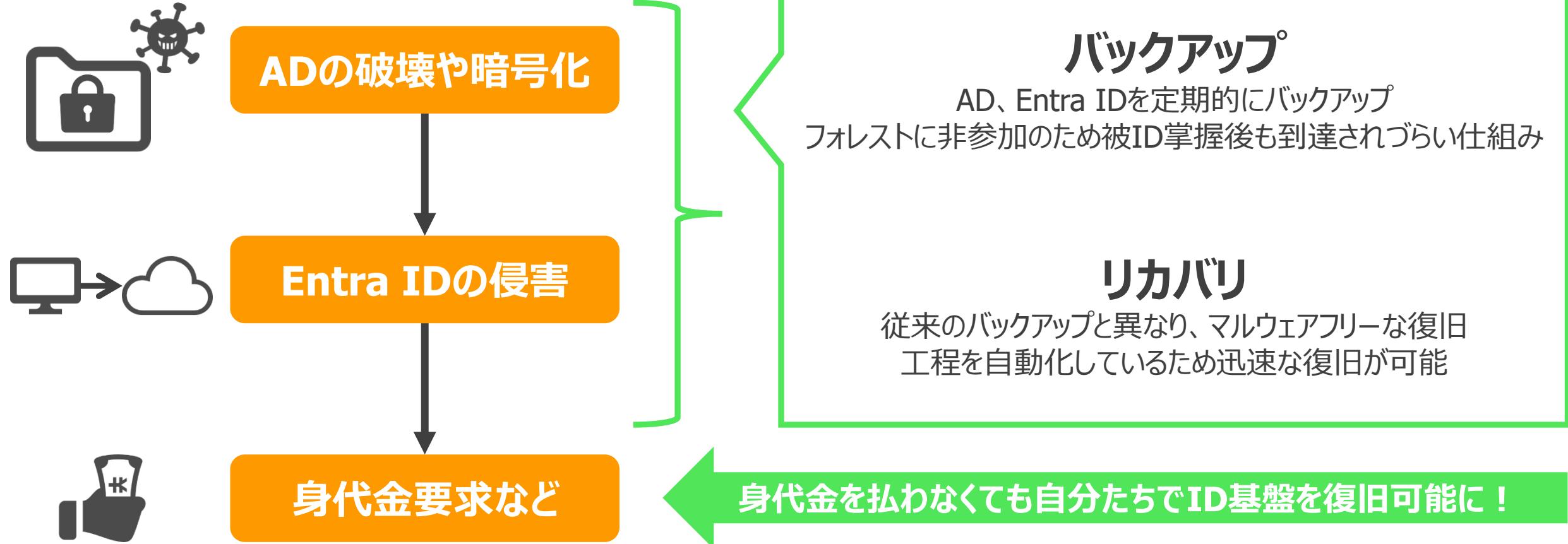
バックアップデータを暗号化可能



SaaSでの提供



Backup ID	Time	Status	Users	Groups
1	10/15/2023 11:52 AM (22m 7s)	Completed	58k	151
2	10/14/2023 11:52 AM (22m 25s)	Completed	58k	151
3	10/13/2023 11:52 AM (22m 55s)	Completed	58k	151
4	10/12/2023 11:52 AM (22m 2s)	Completed	58k	151
5	10/12/2023 10:49 AM (22m 6s)	Completed	58k	151
6	10/12/2023 10:45 AM (2s)	Canceled	58k	0
7	10/11/2023 11:52 AM (23m 10s)	Completed	58k	151



- 社内の中核を担うAD・Entra IDを保護するための4ステップ[°]
- ID基盤への攻撃から企業を守るために、IDを包括的に保護すること
- 企業の業務継続性を維持するためには、リアルタイム検知だけでなく、修復機能による即時復旧が重要



ITDRのベストプラクティスをSemperisで実現



デモ

- DSP : 特権昇格を検知・復旧（手動・自動）
- ADFR : バックアップ取得・リカバリ実施
- DRET : バックアップ取得・リカバリ実施



東京エレクトロン デバイス

