semperis

ACTIVE DIRECTORY FOREST RECOVERY

Active Directoryのための サイバー・ファースト 災害復旧ソリューション

ADの復旧は、単にサーバーを元に戻すことではありません。**再びその環境を信頼できる状態にする必要があります。**
ランサムウェアやワイパー攻撃によってドメインコントローラーが破壊されると、従来型の復旧プロセスでは
復旧作業が数日から数週間に及ぶことがあります。
Semperisは、完全自動化されたフォレスト復旧プロセスをオーケストレーションします。
これにより、人為的なミスを回避し、数日～数週間かかっていたダウンタイムを数分まで短縮し、本番環境に
ADを戻す前に、侵害後のアイデンティティフォレンジックとADの堅牢化を行うことで、マルウェア再感染の
リスクを排除します。

サイバーファーストな 災害復旧

ドメインコントローラーが
感染・消去されていても
ADを復旧

どこでも 復旧可能

Azureクラウドや
あらゆる仮想/物理
ハードウェアへ

クリーンな状態での リストア

システム状態の
バックアップから
マルウェアを排除

高度な 自動復旧

復旧プロセス
全体を自動化し
ダウンタイムを削減

Azure Cloud Backup による柔軟なリカバリー

ADFRはAzureと連携することで、ADバックアップに追加の保護レイヤーを
提供し、攻撃発生時のシナリオにおける復旧の柔軟性を一層高めます。

- **バックアップの堅牢性**：Azureへのオフサイトストレージを利用して、
  ADバックアップの保護を強化
- **災害復旧(DR)**：攻撃発生時にはAzure Blob Storageからデータを復元し、
  復旧時間を大幅に短縮
- **データセンター復旧**：オンプレミスのデータセンターの障害からADを復旧
- **クラウド分散**：ADFRを従来型のディストリビューションポイントとして
  利用し、バックアップをAzureクラウド上に保管

攻撃後は"再開" ではなく"正常復旧"を

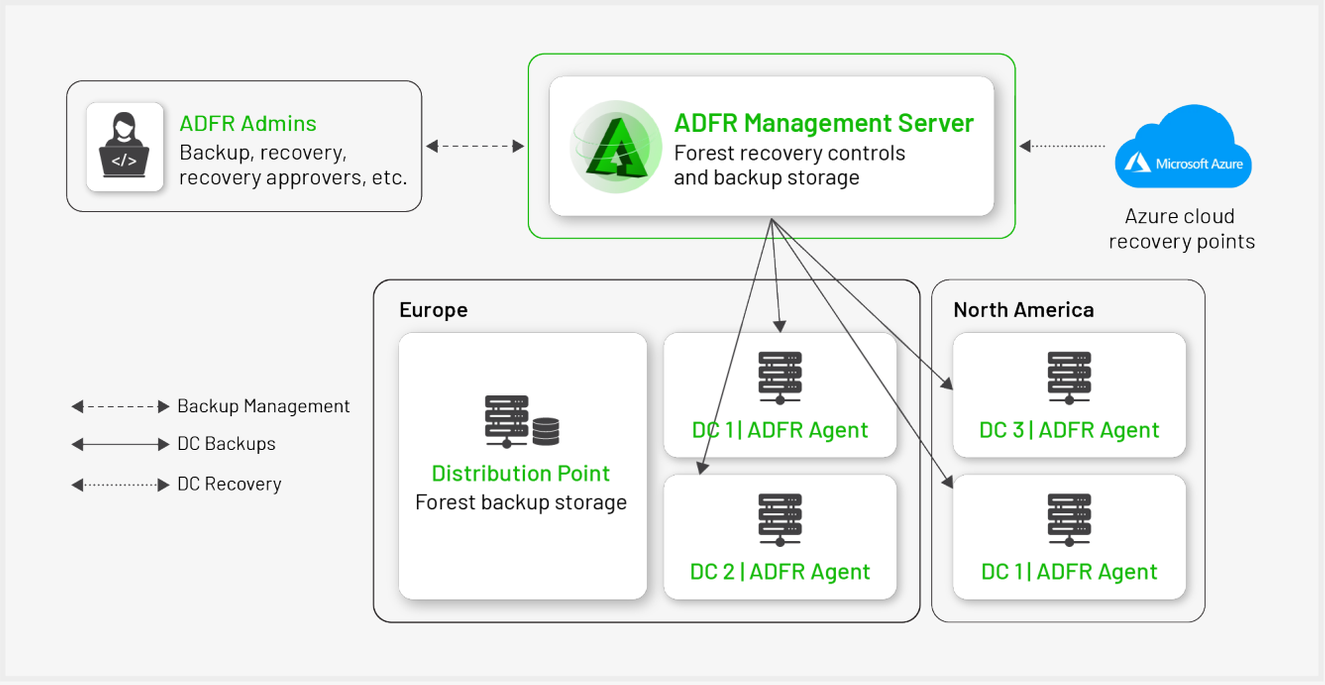
サイバー攻撃の後、多くの企業はとにかく
業務再開を急ぎます。
しかし、包括的かつ十分に検証された
Active Directoryの復旧プロセスと、脅威を完全に
排除し、環境の信頼性を回復する仕組みがなければ、
組織を停止に追い込んだものと同種の攻撃に対して、
システムは再び脆弱な状態に陥ってしまいます。
Semperis ADFRは、完全かつ迅速で、
マルウェアフリーなAD復旧を実現します。

semperis

Active Directory フォレスト全体の復旧時間を90%短縮

Semperisは、AD専用に設計されたDR、アイデンティティフォレンジックとインシデントレスポンス(IFIR)、さらにAzureクラウドストレージ/仮想ストレージ/オンプレミスストレージへの柔軟な復旧オプションを組み合わせることで、AD関連の攻撃に対する多層防御を提供します。

- サイバーインシデント発生後、信頼できるクリーンな環境へADを**迅速・安全かつ効率的に復旧**
- アイデンティティ侵害の再発を調査・防止するための**専門的なアイデンティティフォレンジックおよびレスポンス機能**により、後続攻撃のリスクを低減
- Azure Cloud Backupを含む**柔軟なストレージオプション**により、バックアップ管理を簡素化し、攻撃発生時のADバックアップからの復旧を迅速化



図：クラウドバックアップを用いたフォレスト復旧

Semperis の優位性

ADをゼロから復旧しなければならないという考え方は、もはや机上の空論ではありません。現在では、インシデントレスポンス計画における重要な要素として位置付ける必要があります。フォレストの復旧は決して容易な作業ではありませんが、SemperisのAD専門家はこの難題に真正面から取り組んできました。その結果、Semperis ADFRは他にはない独自の機能を提供可能となりました。

米国のトップヘルスケア企業

「AD関連のランサムウェア攻撃を受けた後にフォレストを復旧するリスクを考えたとき、Semperisへの投資を決断させたのはADFRの存在でした。
AD復旧プロセスをより効果的かつ効率的に管理できるようになったことが、私たちが導入に踏み切った最大の理由です。」

- ノースカロライナ州拠点 非営利ヘルスケア企業　アイデンティティ管理・エンジニアリング部門 ディレクター

semperis

Active Directoryはサイバー攻撃の格好の標的です。Semperisを使って、迅速かつクリーンな復旧を実現しましょう。

トライアルをご希望の方は、
ぜひお気軽にお問い合わせください。

あらゆる環境へのリカバリー

オンプレミス/クラウドを問わず、
仮想・物理を含むあらゆるハードウェア
環境にADを復元可能

クリーンなリストア

ルートキットなどのマルウェアの
再侵入を防ぐため、ADFRはクリーンな
Windows OSから復旧を開始し、
DCやDNSサーバーなどサーバーの役割
に必要なコンポーネントだけを復元

高度な自動化

DCの復元、グローバルカタログの
再構築、メタデータとDNS名前空間の
クリーンアップ、サイトトポロジーの
再構成、DCの再昇格など、フォレスト
復旧に必要な一連のプロセスを自動化

メンテナンスフリー

スクリプトの作成・保守や、設定情報の
手動更新が不要になり、これらの作業が
適切に行われなかった場合に発生する
復旧失敗リスクも排除

バックアップ完全性

利用可能なサーバーを使って、本番AD
フォレストと同一構成のレプリカ環境を
隔離ラボ上に構築し、復旧手順の検証を
容易に行うとともに、社内外の
コンプライアンス要件に対応した
検証結果の文書化を支援

独立型アーキテクチャ

1台の管理サーバーとWebポータルから、
複数のADフォレストに対する
バックアップ/リカバリーを一元管理し、
初期構成から日常運用までの管理負荷を
大幅に軽減

軽量なADバックアップ

ADコンポーネントのみに特化して
バックアップを取得することで、
バックアップ容量を小さく抑え、復旧時に
取得・処理・転送すべきデータ量を
削減し、リストアにかかる時間を短縮する

容易なDRテスト

利用可能なサーバーを使って、本番AD
フォレストと同一構成のレプリカ環境を
隔離ラボ上に構築し、復旧手順の検証を
容易に行うとともに、社内外の
コンプライアンス要件に対応した
検証結果の文書化を支援

マルチフォレスト対応

1台の管理サーバーとWebポータルから、
複数のADフォレストに対する
バックアップ/リカバリーを一元管理し、
初期構成から日常運用までの管理負荷を
大幅に軽減

ラボ環境の構築

Semperis ADFRを使用すると、本番環境の
DCのコピーをラボ環境で簡単に作成できる
ため、開発/テスト、ステージング、
トレーニング、サポート用環境の維持に
かかる時間を大幅に短縮可能

安全なバックアップ暗号化

バックアップセット内の各DCに固有の
ワンタイム暗号鍵を生成し、攻撃者が
単一のキーを使用して全バックアップを
復号化することを防止
暗号化が有効になっているバックアップ
ルールも表示可能

分散バックアップストレージ

Azureクラウドの復旧ポイントを含む
配布ポイントサーバーを活用し、DCの
近くにバックアップを分散配置することで、
ネットワークトラフィックを削減し、
バックアップと復旧に要する時間を短縮

ターゲットIPマッピングファイル

IPアドレスの保存と復元を容易にすること
で、復元時の手動によるIP再割り当て
作業を削減
復旧にかかる時間を短縮しつつ、
プロセスを簡素化

SAML認証

SAMLを使用したシングルサインオン
(SSO)をサポートし、ユーザーのログイン
頻度を最小限に抑制
ユーザーは、選択したIdP認証情報を使用
して管理ポータルにログイン可能

段階的リカバリー

まず重要なリソースを優先的に復旧し、
その後ドメインコントローラーの再昇格
を段階的に実施することで、フォレスト
全体の構造を計画的に復元し、復旧
プロセスを細かく制御

AZUREクラウドバックアップ

ADFRを設定することで、
ADバックアップを
自動的にAzureストレージに保存し、
Azure Blob Storageから
迅速にリストア可能

高度な検索

指定した日付範囲のコンポーネントなど
の属性でフィルタリングできる高度な
検索機能により、操作ログのレコード
取得を簡素化

マルチフォレスト配布ポイント

ADFR単一インスタンス内において、
複数フォレスト間で配布ポイントを
共有できるため、アーキテクチャを
合理化し、サーバー管理を簡素化

semperis

GLOBAL TELECOM

「Active Directoryのようなクリティカルなインフラは、完全にセキュアでレジリエントでなければなりません。私たちは、ADFRのバックアップから数時間でADを復旧できます。」

- José Alegria 氏（**Altice Portugal** 元**CSO**）

MANUFACTURING

「Active Directoryが停止すると、必然的にビジネス活動の停止につながります。Active Directory Forest Recoveryを使用することで、こうしたストレスを回避できています。」

- Christian-Martin Schulz 氏（シニアネットワークエンジニア, **Yamaha Music**

Semperis
IT レジリエンスオーケストレーション

5 ★★★★★

出展：Gartner Peer Insights

info@semperis.com
www.semperis.com

Semperis 本社
5 Marine View Plaza
Suite 102
Hoboken, NJ 07030

ハイブリッドおよびマルチクラウド環境の防御を担うセキュリティチームに向けて、Semperisはサイバーキルチェーンのあらゆる段階で、企業にとって重要なディレクトリサービスの完全性と可用性を確保し、復旧時間を最大90%短縮します。
Active Directory、Entra ID、OktaなどのハイブリッドID環境の保護に特化して設計されたSemperis の特許技術は、1億を超えるIDをサイバー攻撃、データ侵害、運用エラーから守っています。
世界有数の企業は、Semperisを信頼し、ディレクトリの脆弱性の特定、進行中のサイバー攻撃の遮断、そしてランサムウェアをはじめとするデータ完全性インシデントからの迅速な復旧を実現しています。
Semperisは米国ニュージャージー州ホーボーケンに本社を置き、研究開発チームを米国・カナダ・イスラエルに分散して国際的に事業を展開しています。
Semperisは、受賞歴のあるHybrid Identity Protectionカンファレンスおよびポッドキャスト（www.hipconf.com）を主催し、コミュニティ向けのハイブリッドActive Directory防御ツールであるPurple Knight（www.semperis.com/purple-knight/）およびForest Druid（www.semperis.com/forest-druid/）を提供しています。
同社は業界最高水準の評価を受けており、近年ではInc. Magazine誌の「2024年の最も働きがいのある職場」リストに選出されたほか、Financial Times紙では「アメリカで最も急成長しているサイバーセキュリティ企業」に選ばれました。
Semperis は Microsoft Enterprise Cloud Alliance および Co-Sell パートナーであり、Microsoft Intelligent Security Association（MISA）のメンバーでもあります。

Microsoft Partner
Enterprise Cloud Alliance
Microsoft Accelerator Alumni
Microsoft Co-sell
Microsoft Intelligent Security Association (MISA)

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 大阪府大阪市北区梅田 3-2-123 イノゲート大阪 17 階