TechMatrix

Appgate SDP

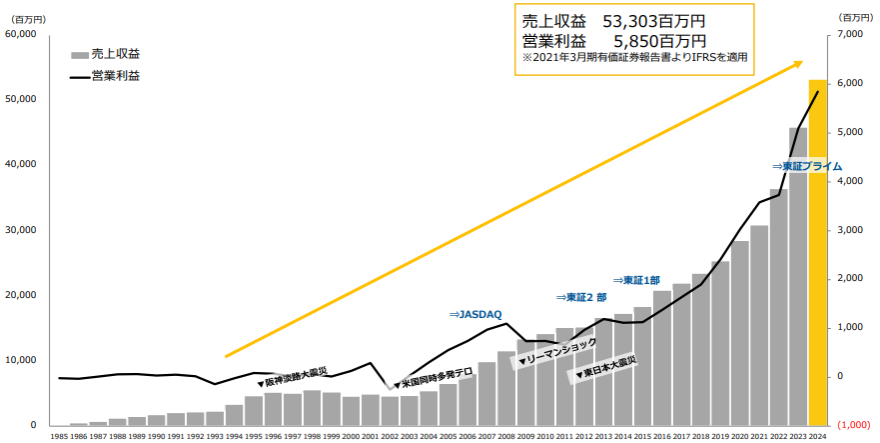
あらゆる人・ものを安全に接続する ユニバーサル・ゼロトラスト・ネットワーク・アクセスを実現

テクマトリックス株式会社
ネットワークセキュリティ事業部
第3営業部　セキュリティプロダクツ営業3課

会社概要

- 商号　テクマトリックス株式会社 (https://www.techmatrix.co.jp/index.html)
- 所在地　東京本社、大阪、名古屋、福岡
- 設立　1984年 8月 30日　(旧社名：ニチメンデータシステム株式会社)
- 上場市場　東京証券取引所プライム市場
- 資本金　12億9812万円
- 売上高　533億3百万円（連結 ’24年3月期実績）
- 従業員数　1,502名（連結 ’24年3月末現在）
- グループ会社

CROSS HEAD	クロス・ヘッド株式会社	CASAREAL	株式会社カサレアル
ARECCIA	アレクシアフィンテック株式会社	TechMatrix Asia Co., Ltd	TechMatrix Asia Co., Ltd
MOBILUS	モビルス株式会社	医知悟LLC	合同会社医知悟
PSP	PSP株式会社	A-Line	株式会社A-Line
OCH	OCH株式会社	M3 AI	エムスリーAI 株式会社



事業セグメント（テクマトリックスグループ）

情報基盤事業


デジタル化社会を支える社会インフラとして安心・安全を確保するセキュアな情報基盤・セキュリティ製品・サービスを提供

- 最先端のネットワーク／セキュリティ製品の提供
- 安全な情報基盤を構築
- 24時間365日の運用監視　サービスの提供

アプリケーション・サービス事業

誰にでも使いやすいUI/UXを通してクラウド型の業務アプリケーションを提供

CRM

- コンタクトセンター向け問合せ管理システムの提供
- FAQナレッジシステムの提供

ソフトウェア品質保証

- IoT時代の組み込みソフトウェア品質保証のためのテストツールの販売

ビジネスソリューション

- インターネットサービス・金融分野でのソリューションの提供
- IT技術者向け研修の提供

教育

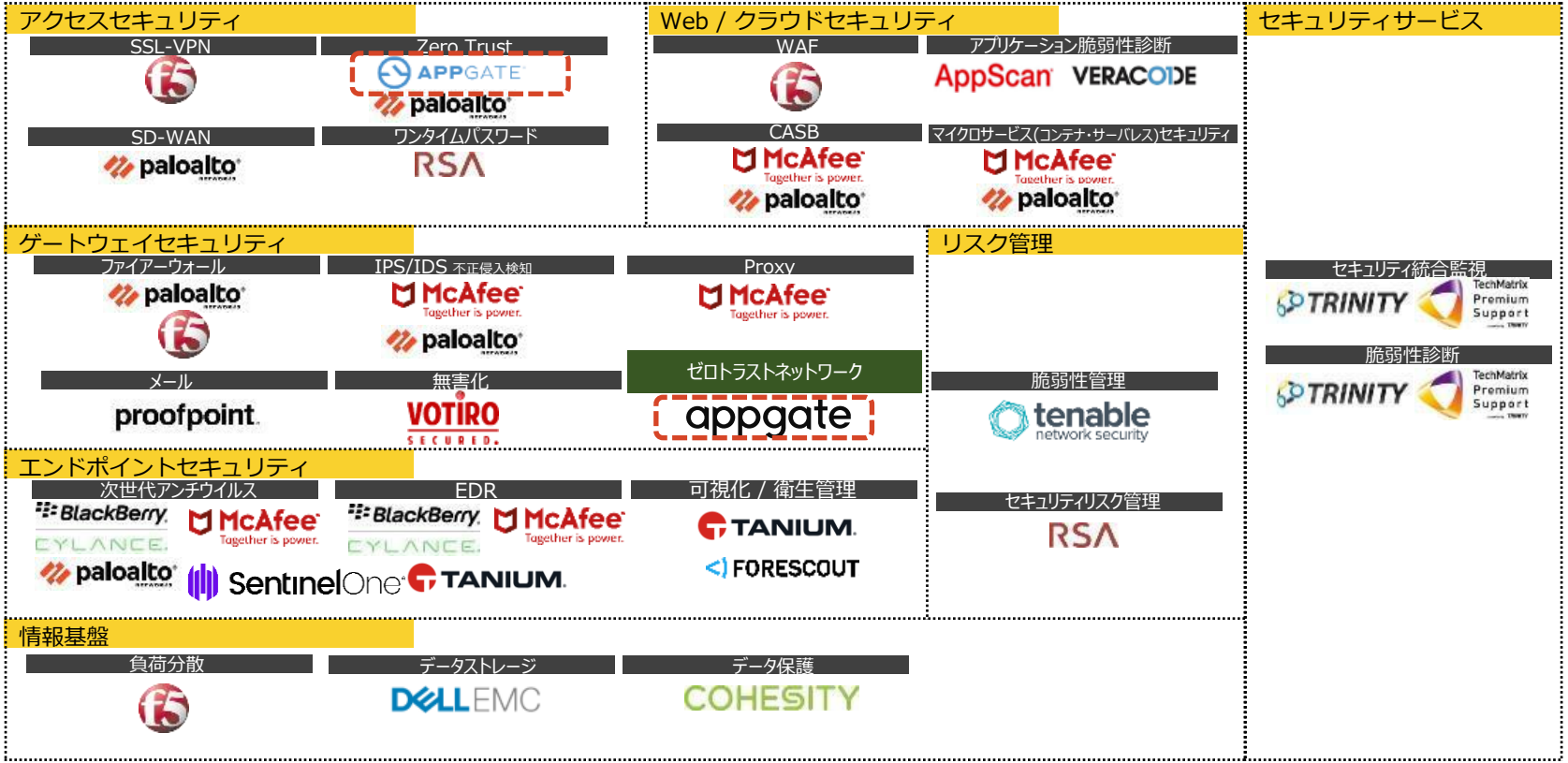
- スクール・コミュニケーション・プラットフォームの提供

医療システム事業

生活者一人ひとりの一生を支える医療情報インフラの構築を目指しアプリケーションやサービスを提供

- 医用画像管理システム（PACS）の提供
- PHRサービスの提供
- 遠隔読影のプラットフォームを提供

情報基盤事業：製品・サービスセグメント



TechMatrix

THE PROBLEM

デジタルの世界は変わった
セキュリティが追いついていない

顧客は多面的な課題に直面している

Cybersecurity must

脅威の増加と攻撃対象の拡大への対応

複雑なクラウドやハイブリッド・インフラストラクチャに対応する拡張性

分散したグローバルおよびリモートワークの保護

The business must

デジタルトランスフォーメーションの加速

市場環境への迅速な対応と適応

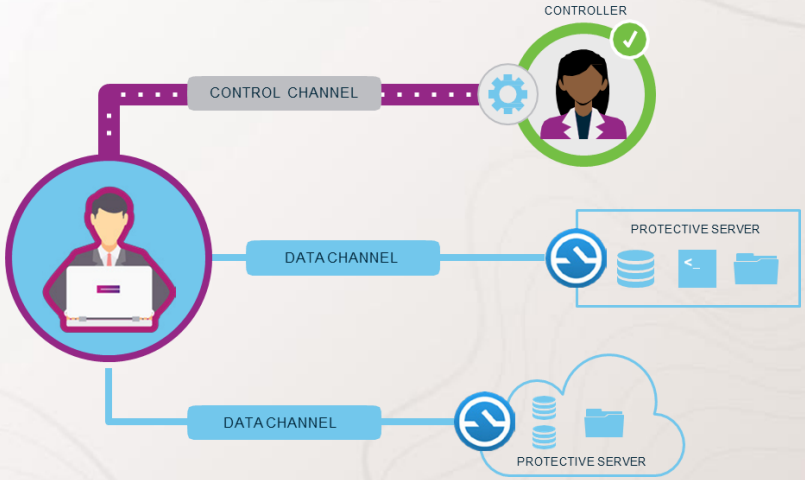
競争優位性を築きながら より大きな価値を創造する

Appgateはその両方を解決し人々につながる力を与え保護します

appgate

新しいネットワークセキュリティ
Software-Defined Perimeter/Appgate SDP

ソフトウエア・デファインド・ペリメーターは境界線（Perimeter）をソフトウェア上で構築、集中的に制御し、アクセス制御に関わる設定を柔軟に動的に変更して安全にデータを転送する技術です。
（出典：Cloud Security Alliance)



- クライアント

  データアクセスを要求するユーザー
- コントローラー

  クライアントを認証し、クライアントとゲートウェイを接続させる
- ゲートウェイ

  クライアントにサーバーのアクセス権を付与する
- ログサーバー

  コントローラーとゲートウェイの監査ログを保存する

Why Appgate Zero Trust Network Access?

TechMatrix

Appgate SDP ZTNA 他サービスとの違い

Direct-Routed

クラウド・プロキシを持たないアーキテクチャは、データがネットワークをどのように通過するかを完全に制御

秘匿化されたインフラ

ネットワーク・アクセス・ポイントは、SPAによって不正行為者から完全に隠蔽

継続的アセスメントによる動的制御

継続的なデバイスおよびアプリケーションのアセスメントによる動的なアクセス制御

プログラマブルで高い適応性

豊富なインバウンドおよびアウトバウンドAPIは、セキュリティイベントやビジネスプロセスとZTNAを統合

ユニバーサルZTNA

人だけでなく、IoT機器やサーバ、マイクロサービスなどのアクセスを一元的に制御・監視・記録

Appgate SDPの仕組み

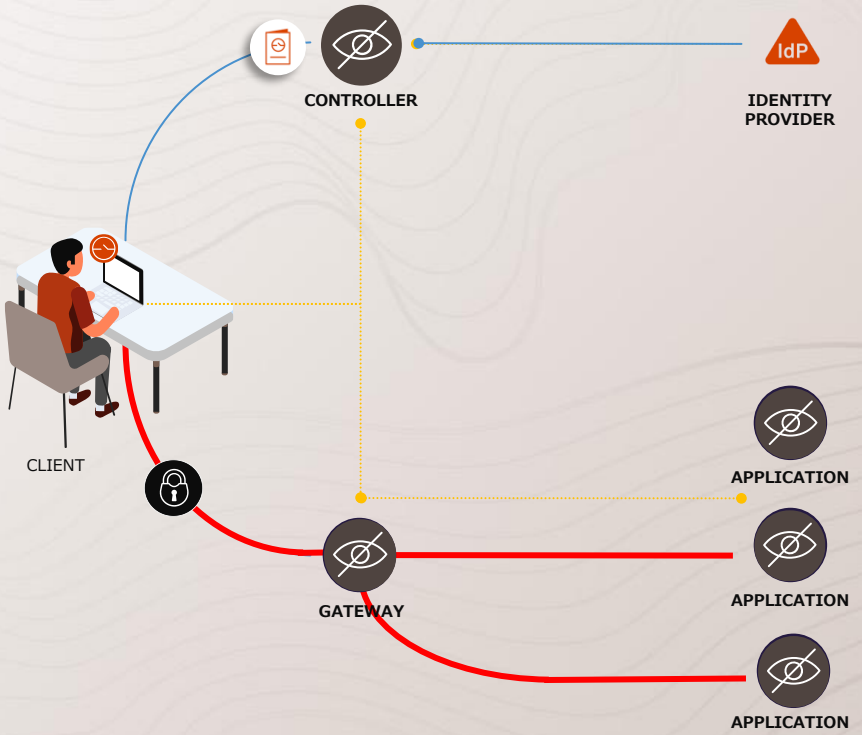
1 クライアントがシングルパケット認証(SPA)を利用し、コントローラーにアクセスリクエストする

2 コントローラーがコンテキスト情報を確認し、ライブエンタイトルメントをクライアントに渡す

3 クライアントはSPAを使用しライブエンタイトルメントをゲートウェイに渡し、ゲートウェイはユーザのコンテキストに一致するアプリを検出する。

4 このセッションのために、動的な1対1の接続「セグメントワン」が構築される。

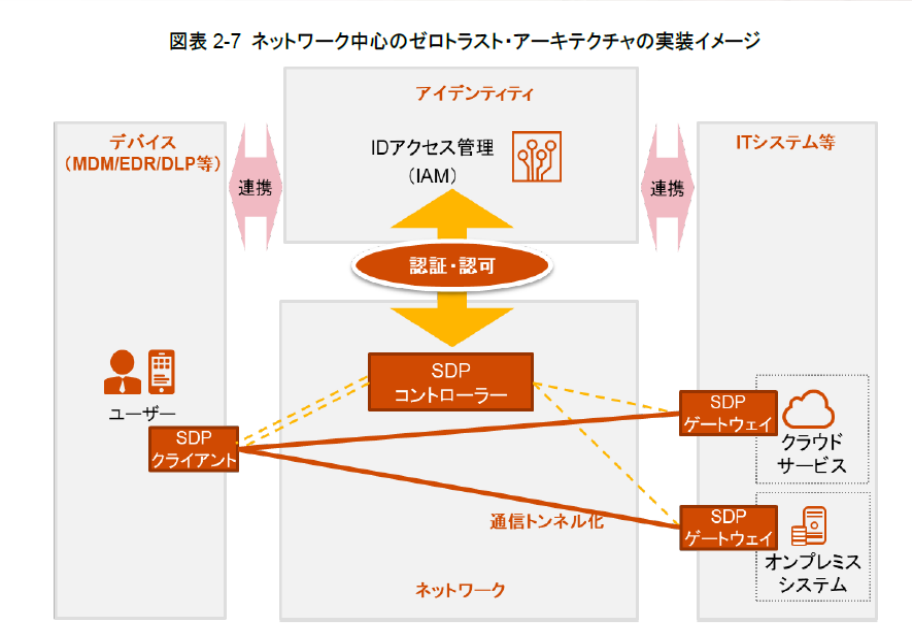
5 コンテキスト情報の変化を継続的に監視し、それに応じてセグメントワンを適応する。



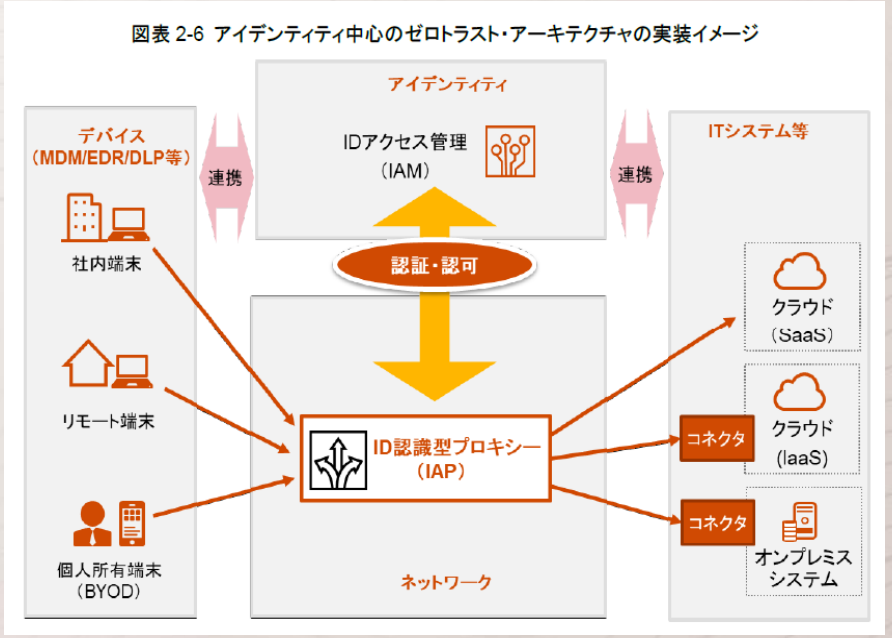
Direct-Routed（SDP）VS Cloud-Routed（IAP）

TechMatrix

SDP (Software defined perimeter)



IAP (Identity Aware-Proxy)



appgate

金融庁報告書を参考に当社作成
https://www.fsa.go.jp/common/about/research/20210630/zerotrust.pdf

Direct-Routed（SDP）VS Cloud-Routed（IAP）

Direct Routed （Appgate）

- ネットワーク・トラフィックを完全に制御
- 低遅延、高可用性のダイレクト・アクセス
- ユニバーサル・アクセス（リモート＆オンプレ）
- レガシーシステム、IoT、OTをカバー
- サーバートリガーの接続に対応
- 幅広い相互運用性
- ネイティブ・ネットワーク・スピードでのユニバーサルZTNAを実現

Cloud-Routed

- マルチテナント型クラウドを強制的に経由するトラフィック
- オンプレユーザーもクラウド経由
- スループット・遅延の問題
- プロキシー・アーキテクチャによるプロトコル・サポートの制限
- 潜在的な隠れた追加費用リスク
- ベンダークラウドのセキュリティ、可用性、拡張性に対する暗黙の信頼
- ユニバーサルZTNAはネットワークパフォーマンスの低下と帯域幅の追加コストを伴う

	Direct-Routed Appgate SDP	Cloud-Routed
ネットワークトラフィックの完全制御	YES	NO
オンプレミスユーザーがインターネットを経由せず直接アクセス可能	YES	NO
広範なネットワークプロトコールが利用可能	YES	NO
オンプレミスユーザーの保護	YES	限定的
レガシー・アプリケーションの保護	YES	限定的
IoT/OTデバイスの保護	YES	限定的
サーバートリガーの接続の保護	YES	NO
直接マルチトンネル、高可用性接続	YES	NO
エアギャップ要件(隔絶している環境)に対応	YES	NO
幅広い相互運用性	YES	限定的

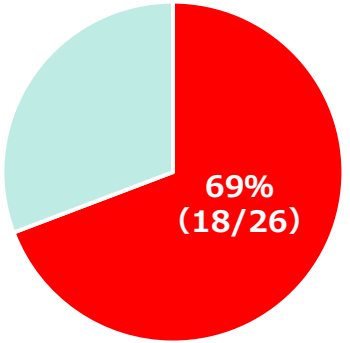
秘匿化されたインフラ

TechMatrix

JP CERT　２０２４注意喚起情報

2024	
公開日	注意喚起内容
2024-02-29	Fortinet製FortiOSの境域外書き込みの脆弱性（CVE-2024-21762）に関する注意喚起 (更新)
2024-02-29	Ivanti Connect SecureおよびIvanti Policy Secureの脆弱性（CVE-2023-46805およびCVE-2024-21887）に関する注意喚起 (更新)
2024-02-15	Fortinet製FortiOSの境域外書き込みの脆弱性（CVE-2024-21762）に関する注意喚起 (更新)
2024-02-14	Ivanti Connect SecureおよびIvanti Policy Secureの脆弱性（CVE-2023-46805およびCVE-2024-21887）に関する注意喚起 (更新)
2024-02-14	2024年2月マイクロソフトセキュリティ更新プログラムに関する注意喚起 (公開)
2024-02-14	Adobe AcrobatおよびReaderの脆弱性（APSB24-07）に関する注意喚起 (公開)
2024-02-09	Fortinet製FortiOSの境域外書き込みの脆弱性（CVE-2024-21762）に関する注意喚起 (公開)
2024-02-09	Ivanti Connect SecureおよびIvanti Policy Secureの脆弱性（CVE-2023-46805およびCVE-2024-21887）に関する注意喚起 (更新)
2024-02-01	Ivanti Connect SecureおよびIvanti Policy Secureの脆弱性（CVE-2023-46805およびCVE-2024-21887）に関する注意喚起 (更新)
2024-01-31	Ivanti Connect SecureおよびIvanti Policy Secureの脆弱性（CVE-2023-46805およびCVE-2024-21887）に関する注意喚起 (更新)

ネットワークアクセス制御関連比率



○○はリモートアクセス（VPN）などを提供する機能です。
本脆弱性の悪用により、認証されていない遠隔の第三者がルート権限で任意のコードを実行する可能性があります。

自社管理のVPNだけでなく、クラウドサービス利用でも同等のリスク

秘匿化されたインフラ

Appgate SDPでは認可されたユーザー、端末のみがGWへのアクセスを許可されます。攻撃者がポートスキャンを行ってもすべてのポートは閉じられています。よって仮に脆弱性があったとしても犯罪者は攻撃ポートへのアクセスすらできません。

秘匿化されたインフラ

SPA（Single Packet Authorization）

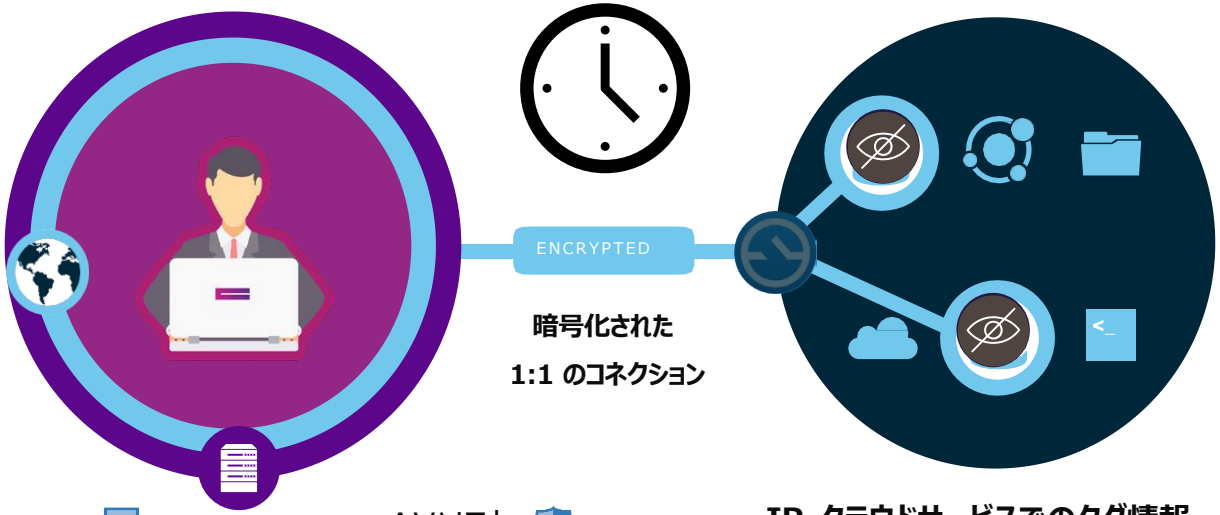
SPA特徴

- 正当で検証されたSPAキーを送信することで接続
- SPAキーが認可されない限り一切の応答がない
- SPAキーはローテーションされ、搾取されても
  なりすましログインができない
- SPAキーはすべてのアプライアンスに対して独立
- 複製防止機能

悪意のあるユーザーがポートスキャンを実行しても応答がないため、攻撃のしようがありません

継続的アセスメントによる動的制御

ユーザーの属性およびデバイス、アクセス環境に応じた、一度限りのポリシー権限を与えます。
そのアクセス環境は継続的に監視・評価され、アクセス権限に反映されます。

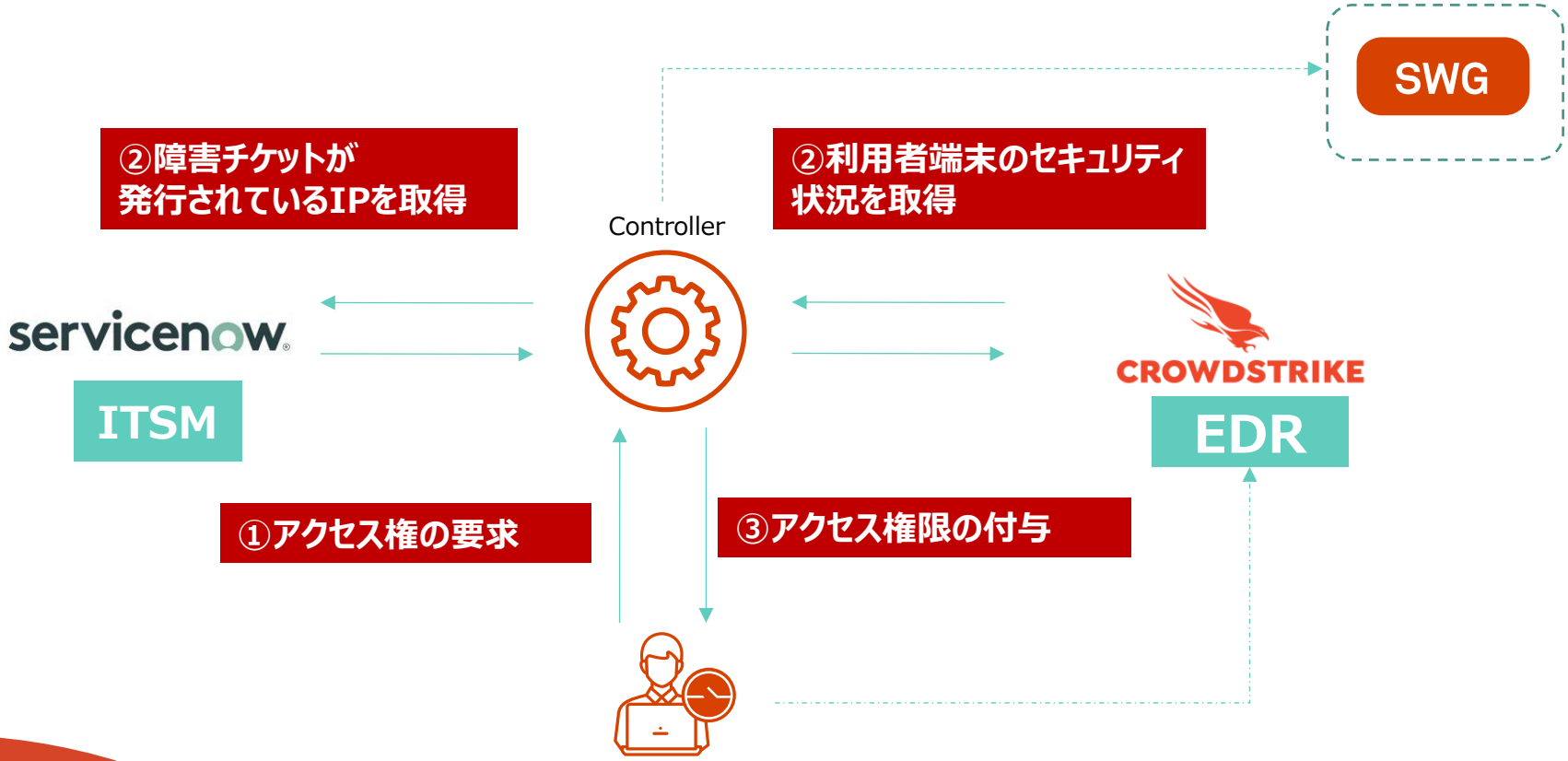


デバイス
多要素認証
リモートアクセス
時間

AVソフト
許可されたアプリ
所属部署
カスタム属性

IP・クラウドサービスでのタグ情報・ドメイン情報により規定された範囲のみにアクセスを許可

プログラマブルで高い適応性



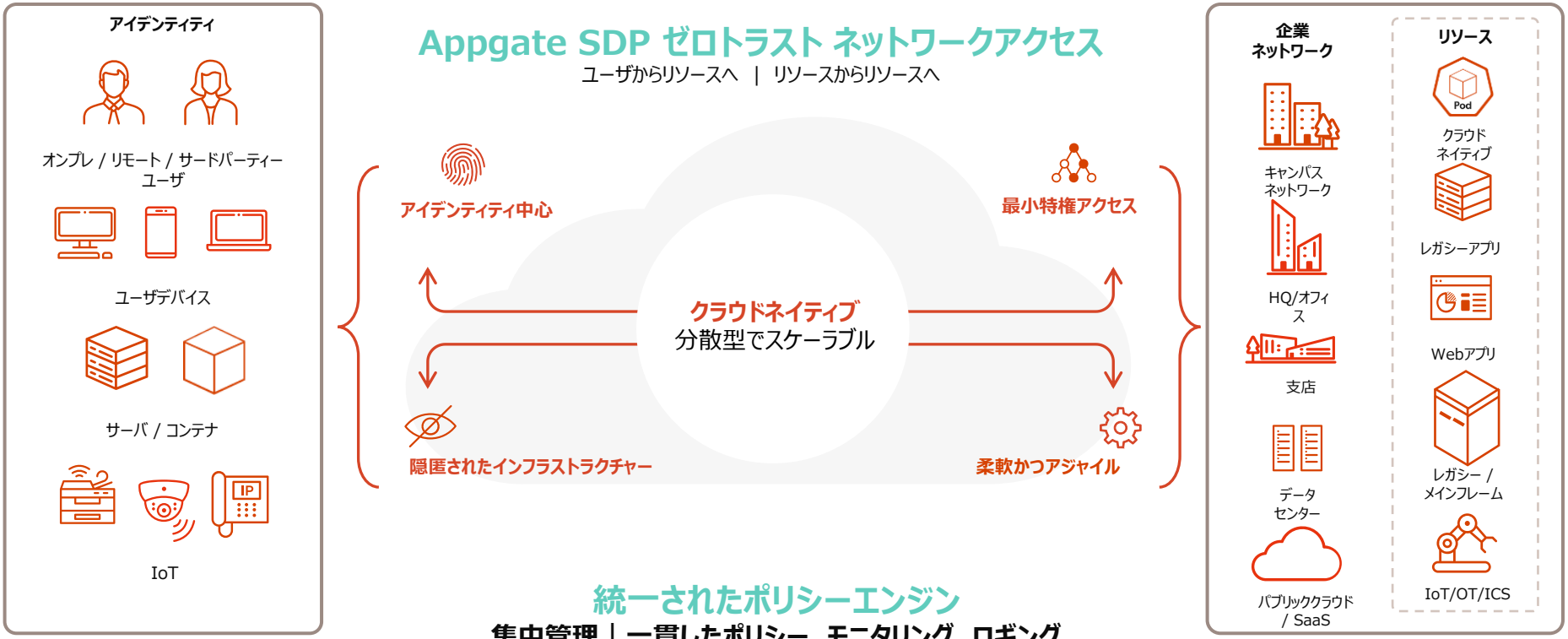
プログラマブルで高い適応性

機能豊富なAPI。最高クラスのアライアンス。ビルドインのリスクエンジン

アイデンティテの統合	エンドポイントの活用	SSEの実現	サーバ間のセグメント
LDAP SAML RADIUS OIDC	SentinelOne* CROWDSTRIKE Trellix Intune*	MENLO SECURITY	illumio

アクセスのアートスケール	TDIRの向上	ITSMの自動化	リスクエンジンの連携
aws Azure Google Cloud	splunk> elastic sumo logic DARKTRACE	servicenow Jira Software	appgate

ユニバーサル・ゼロトラスト・ネットワークアクセス



ユニバーサル・ゼロトラスト・ネットワークアクセス

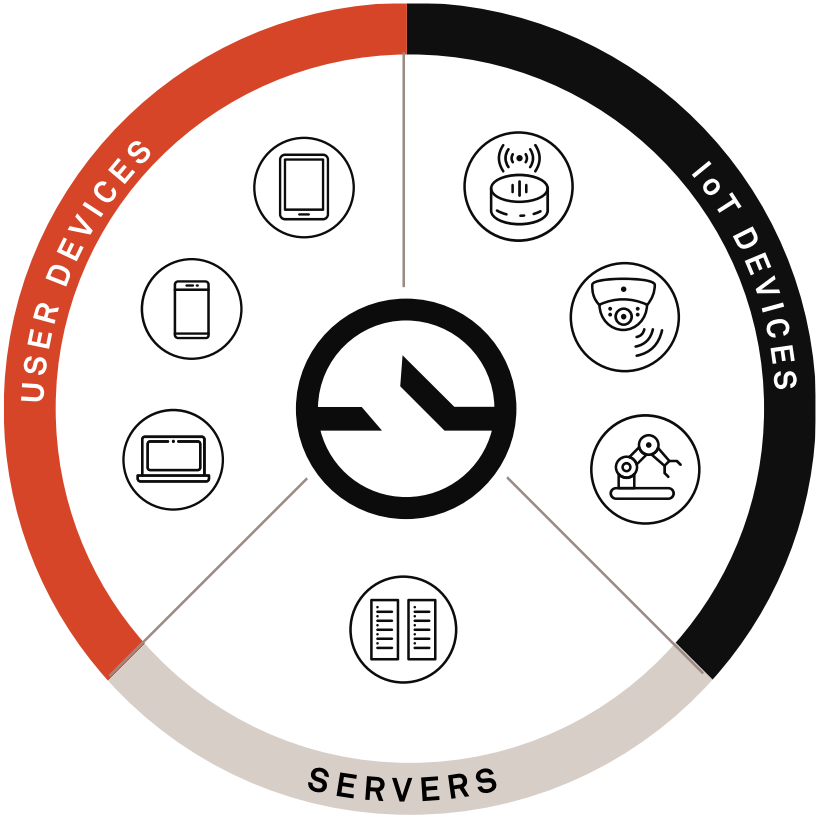
ユーザー、サーバー、マイクロサービス、IoT・OTのための統合セキュリティ・プラットフォーム

単一の動的ポリシーモデルですべてのアクセスを制御

従業員、システム、第三者による安全なリモートアクセスが可能

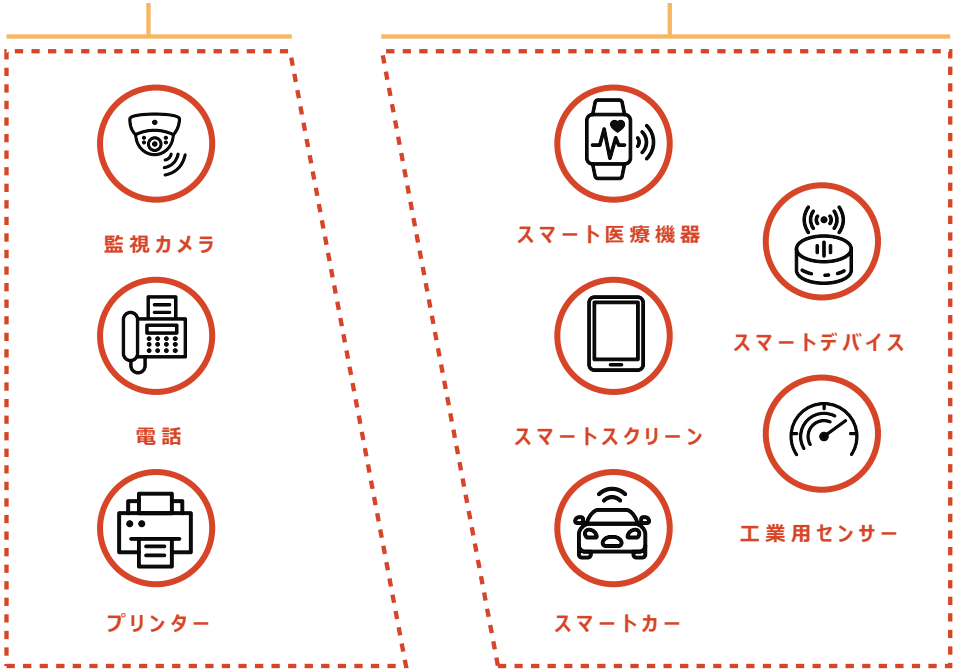
IoTシステムは次のような問題から保護される。

- 侵害された機器
- 悪意のあるネットワークアクセス
- トラフィックの盗聴
- ネットワーク偵察



IoT/OTデバイスにおけるセキュリティー

レガシーデバイスと最新のIoT・OTデバイスを統合する
ゼロトラストセキュリティ



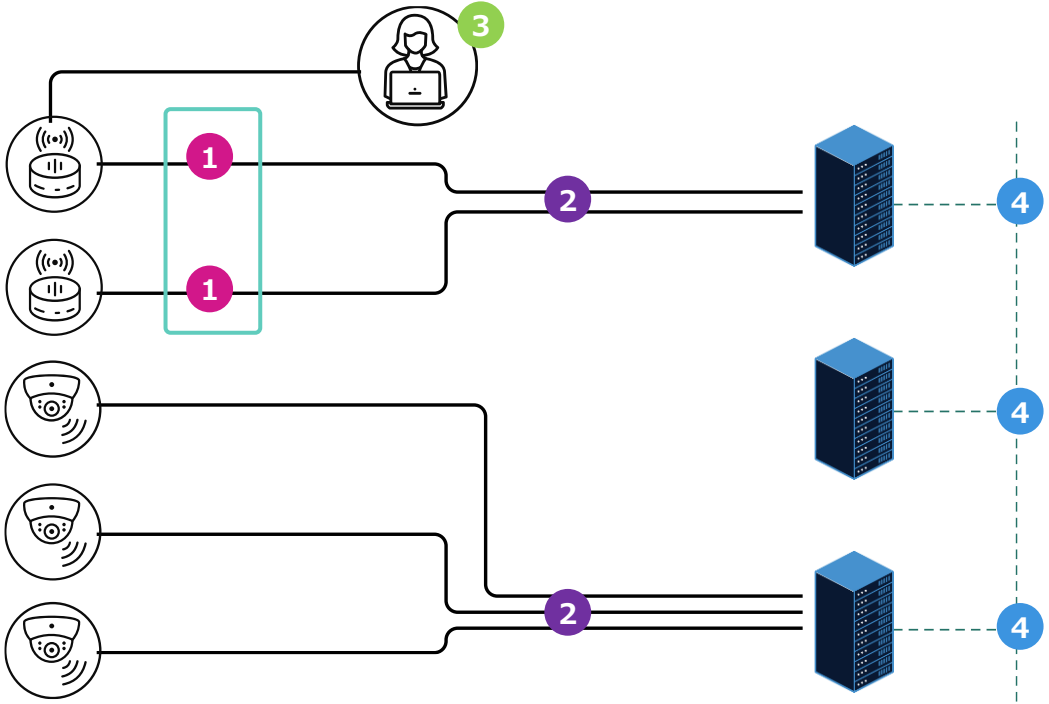
IoT/OT デバイスの特性

通常は閉じたネットワーク環境にある
ユーザインタフェースが無い
ソフトウェアが追加インストールできない
アイデンティティ管理システムと連携できない

リスク

平文のネットワークプロトコル
リモートで操作され、監視されていない
物理的な攻撃(ハードウェアの抜き取り等)
物理的なネットワーク接続

IoT/OTセキュリティー要件



1

ネットワーク接続の
ハイジャックの防止

2

ネットワークトラフィック
の暗号化

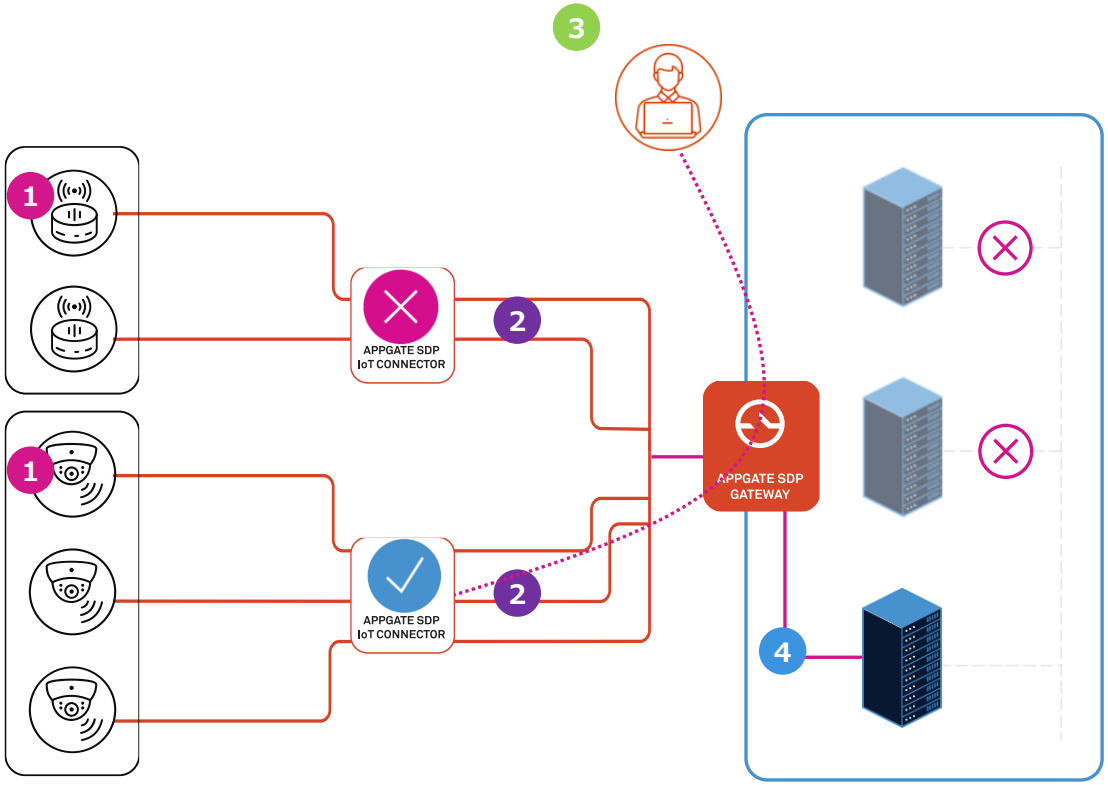
3

IoT/OTデバイスへの安全
なユーザーアクセス

4

ネットワークの偵察または
横移動の防止

Appgate SDPコネクタでIoT / OTの保護



1

セグメント化されたデバイス

2

暗号化された
ネットワークトラフィック

3

ポリシーによって制御される
デバイスへのユーザーアクセス

4

デバイスは許可された
サーバーのみにアクセス

Zero Trust Network Accessの進め方

Zero
Trust
Network
Access

レガシー・テクノロジーの段階的縮小

VPNやFWのような時代遅れで安全ではないレガシー・アクセスとネットワーク・テクノロジーを置き換え、削減する。

企業ネットワークの変革

VLANやNACのようなレガシーな企業セキュリティ管理を置き換え、ネットワーク・アーキテクチャを簡素化

セキュアアクセスの近代化

複雑なハイブリッドインフラストラクチャにおいて、場所を問わず、すべてのユーザーとデバイスおよびリソースに最新のセキュアアクセスソリューションを提供

オペレーション・オーバーヘッドの削減

セキュリティ管理者のオーバーヘッド、納期、運用上の課題を削減し、コスト削減とビジネスROIを向上させます

TechMatrix

米国空軍をはじめ、高度なセキュリティが求められる多くのグローバル企業・政府機関でご採用いただいています

One Compath様

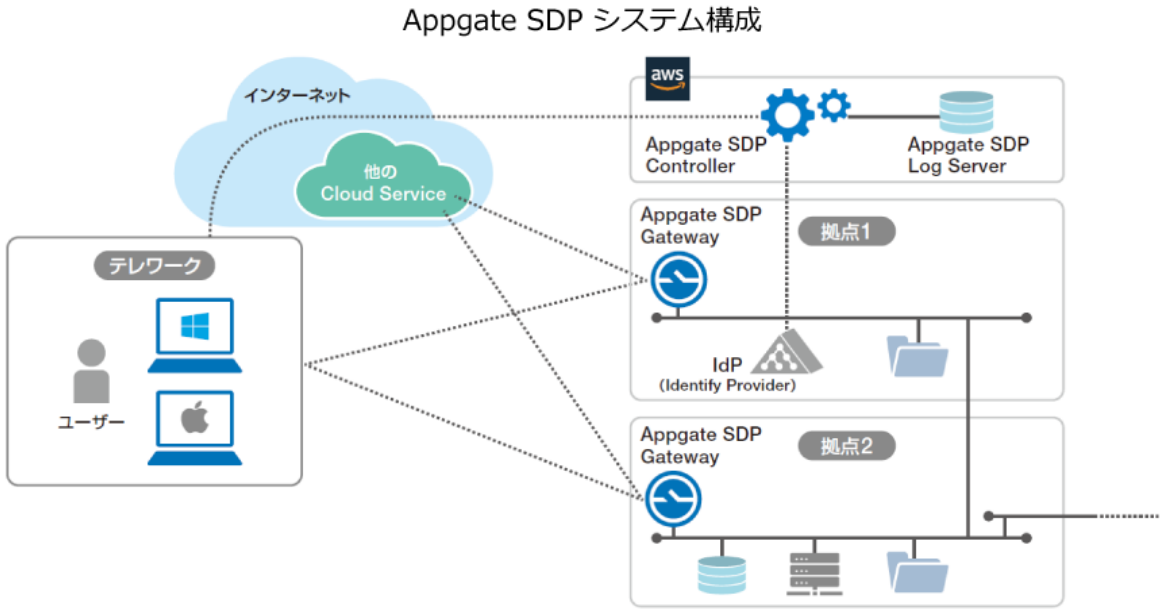
VPNリプレース

ONE COMPATH

緊急事態宣言に伴う全社テレワークでVPNがキャパオーバーに

ゼロトラストネットワークアクセスを実現する「SDP」に注目

大きく改善されたアクセスの安定性とユーザビリティ



appgate

日鉄ソリューションズ様

DevOps

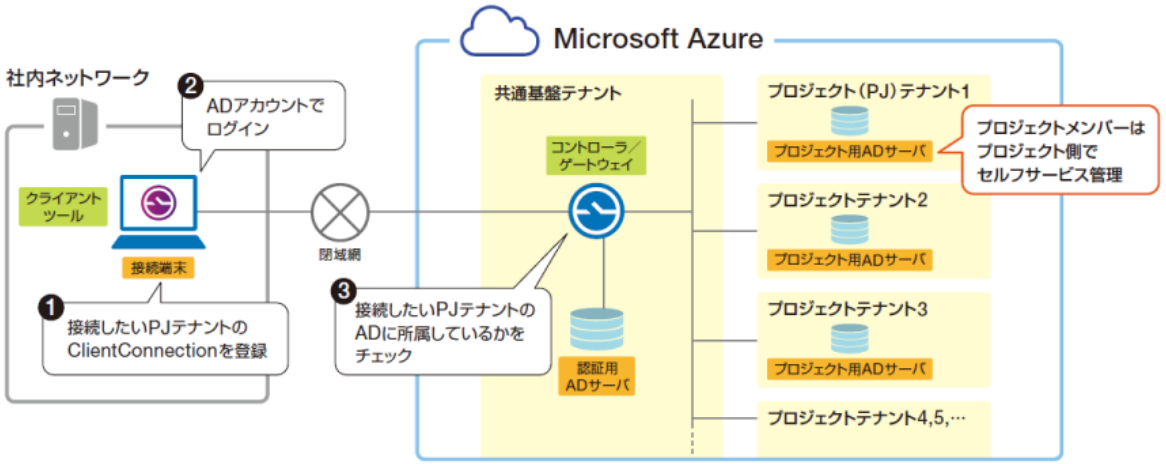
日鉄ソリューションズ株式会社

社外との共同開発環境をクラウド化するにあたり、アクセス制御が課題に

「ゼロトラスト」をキーワードに探したら「Appgate SDP」に行き着く

高アジリティと運用負荷の低減を実現したことからマルチクラウド環境や社内完結の開発環境への導入も検討

Appgate SDP　システム構成図



appgate

大成建設 様

TechMatrix

大成建設 TAISEI
For a Lively World

課題

- 端末起動時から通信制御を行いたい
- 常に最新の端末情報をもとにアクセス制御を行いたい
- ゼロトラストを内製化し運用過程で各部門の要望に応えたい

効果

- インバウンド通信を遮断し端末をステレス化することで、起動時にサイバー攻撃者から端末が見えない状態に
- 5分ごとに個人識別情報とデバイスポスチャ情報などをもとに、動的にアクセス拒否/許可を実施。なりすましや標準外デバイスの使用などの不適切なものを徹底的に排除
- 構築パートナーのテクマトリックスからスキルトランスファーを受けて内製化を実現。例外設定など運用過程で生じる様々な要望に柔軟かつ迅速に対応できる体制を整えている。

導入のプロセス

スキルトランスファーにより内製化を実現
運用過程で生じる様々な要望に柔軟かつ迅速に対応

PoCにより同社が目指すゼロトラストをAppgate SDPが実現できることを確認。採用にあたり、大きく2つのポイントがあったと山田氏は話す。「1つめは、クラウドとオンプレミスの両方に対応できること。当社の場合、クラウドへの全面移行は現実的ではないからです。2つめは、グループ会社、個別要件にも展開するため、既存ネットワークはそのままに、導入しやすいこと。この2点をクリアできたことでAppgate SDPの採用を決断しました」

Appgate SDPによるゼロトラスト環境の実現は、冗長化されたコントローラーとゲートウェイ、アプリケーションをインストールした端末で構成される。2021年3月に第一弾として、インターネットVPNからAppGate SDPへの切り替えを実施。2022年5月に全社展開し、順次グループ会社、個別要件にも展開。ゼロトラストの運用で重要なポイントとなるのが内製化だ。「検証段階では、テクマトリックスに当社の要件を設定に落とし込んでもらいました。しかし日々業務を行う中で、ゼロトラストに関して寄せられる様々な要望に対し、すべてを外部に依頼していては手間も時間もかかります」と植野氏は話し、こう続ける。「各部門で使用しているアプリケーションは様々です。なかには、起動時のインバウンド遮断を例外にしないと利用できないものもあります。全社展開するまでに、当社と、グループのITを担う株式会社大成情報システムの担当者が、テクマトリックスからスキルトランスファーを受けました。Appgate SDPに対する豊富な知見とノウハウを有するテクマトリックスの説明は、わかりやすくとても丁寧でした」

appgate

岩国市教育委員会 様

TechMatrix

課題

- 校務系と学習系間でも安全にデータのやりとりができるようにして利便性を向上させたい
- 職員室以外の場所でも安全に校務用PCを利用できるようにし、利便性を向上させたい
- オンプレミス環境のセキュリティ確保と共に、将来的にそれらのシステムがクラウド環境に移行してもセキュリティを確保したい。

効果

- ネットワーク統合により校務用PCから学習系へのデータ送信も容易に
- リアルタイムの動的な制御や、端末の論理的な分離などセキュリティ機能のさらなる向上やロケーションフリーな運用
- 各認証システムが直接アクティブディレクトリ(AD)からユーザ情報を取り込むことができるため、ICT教育推進室だけで運用できるようになり、人為的なミスはほぼなくなり、ミスがあっても速やかに対応できるように

導入の経緯

これまでと同等の予算感でクラウド化

本市では一部オンプレミス環境(校務支援システムやファイルサーバ等)の仕組みを継続しながらデータを連携したいと考え、当初は首長部局が採用しているVDI(仮想デスクトップ)方式を想定してMicrosoft 365 A3による仮想デスクトップ環境を検討しました。しかし既存の仕組みと比較すると数倍の導入コストとなり、財政面での理解が得られませんでした。

次に検討したのが、Microsoft 365 A5とSDP(Software Defined Perimeter)コンセプトを採用したゼロトラストネットワーク環境です。

オンプレミス環境のセキュリティ確保と共に、将来的にそれらのシステムがクラウド環境に移行してもセキュリティが確保できることが重要で。SDPコンセプトを採用したゼロトラストネットワーク環境ではこれが実現する点が魅力的でした。

本仕組みは、実際のデータに対して、安全で信頼のおけるアクセスかどうか様々な要素を確認した上で許可するもので、アクセス先のシステムがクラウドに移行した際も保護ができます。

校務用PCを現状よりハイスペックにしても既存の仕組みとほぼ同等の予算感で構築が可能であることもわかりました。首長部局への説得には、これまで以上に役立つ仕組みであることに加えて予算を大幅に増やさない工夫も必要です。

このような条件で入札を行った結果、「Appgate SDP(以下、アップゲート)」の導入が決まりました。契約締結から構築・運用まで3~4か月と短期間で構築が完了し、2022年9月から運用をスタートすることができました。

appgate

Industry Validated. Gov't Approved. Enterprise Trusted.

FORRESTER®	Gartner®	CSA cloud security alliance®	NCCoE	U.S. DEPT OF DEFENSE
Named a Leader in the latest Forrester New Wave, positioned highest for current offering	Peer Insights 4.8 out of 5 stars Representative Vendor, ZTNA Market Guide	Aligned to Software-Defined Perimeter (SDP) Reference Architecture	National Cybersecurity Center of Excellence NIST SP800-207 Collaborator Zero Trust Architecture Project	DoD Authorized to Operate & CNAP Aligned to DoD Reference Architecture

DXC TECHNOLOGY · Secureworks® · U.S. AIR FORCE · FINRA · ManTech Securing the Future

- **Fortune 10** Oil & Gas Company
- **Fortune 500** Bank
- **Fortune 500** Health Insurance Company
- **Fortune 500** Chemical Company

Thank You

テクマトリックス株式会社
ネットワークセキュリティ事業部　第3営業部
セキュリティプロダクツ営業3課
E-mail：appgatesdp-sales@techmatrix.co.jp
URL　　：www.techmatrix.co.jp