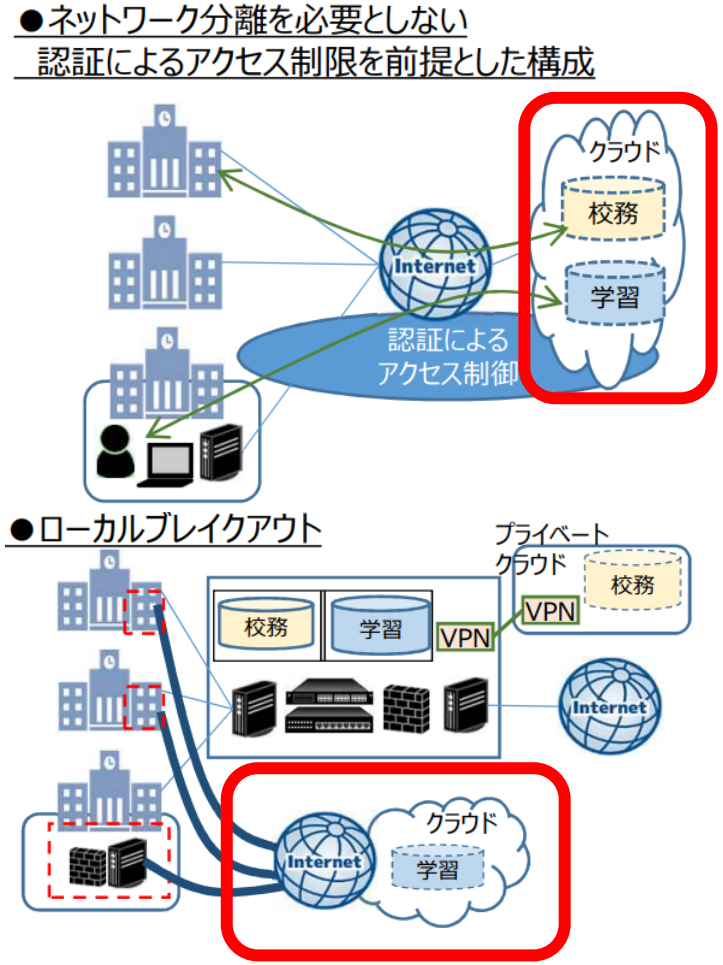
Appgate SDPで行う
『脱・ネットワーク分離』

テクマトリックス株式会社

改定されたガイドライン(令和3年 5月)

【追加された内容】
・ネットワーク分離を必要としない認証によるアクセス制限を前提とした構成
・ローカルブレイクアウト

Appgate SDPを利用することで、
物理的にネットワーク分離をしなくても、
論理的に、「端末」も「サーバ」も分離されます！



認証・認可によって動的なアクセス制御を行うことを
Zero Trust Network Access(Software-Defined Perimeter)と言います。

Appgate SDPはこのSDPを定義している団体のフレームワークに則った、
唯一の製品となっております。
※同団体(CSA)の議長がProductManagerを務める製品であり、
　ワールドワイドで高い評価を得ております。

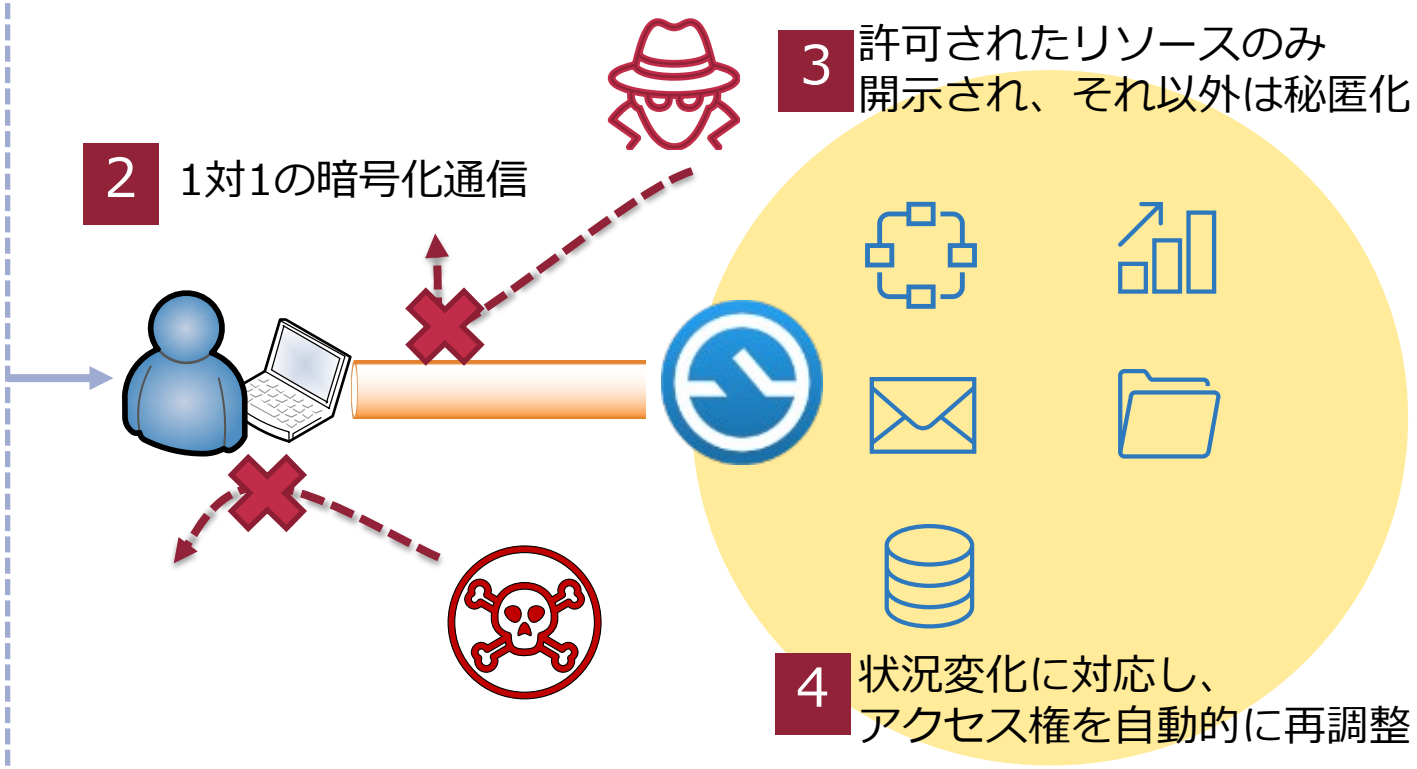
appgate

TechMatrix

「様々な認証・認可」を行い、**「動的」**に、
「リソース単位」のアクセス制御を行う**次世代アクセスプラットフォーム**

1 以下項目に基づいてアクセス制御を実施

- ユーザ
- アクセス端末
- OSバージョン
- エンドポイントエージェント
- レジストリ情報
- 多要素認証
- ロケーション
- ネットワーク
- 時間
- ビジネスシステム
- タグ
- API(例：脅威レベル)



Appgate SDPで行う認証・認可によるアクセス制御

・ネットワーク分離よりセキュアな論理分離の実現

端末へのネットワークを介した**不正なアクセス(ウイルスやハッカーの横移動)を防ぎ**、
サーバも認証認可されたものしかアクセスさせません。
「**クローズドネットワーク内は安全。**」ではなく、全てを妄信せずに厳密な認証認可によるアクセス制御を実施
※閉域SIMを利用しても、SIMを差し替えてしまう、フリーWi-Fiに接続してしまうなどで抜け道が出来てしまいます。
Appgate SDPでは、**インターネットには接続させない**ことや、**強制的にSWG経由にする**ことなども可能です。

・ロケーションやシステム制限無し

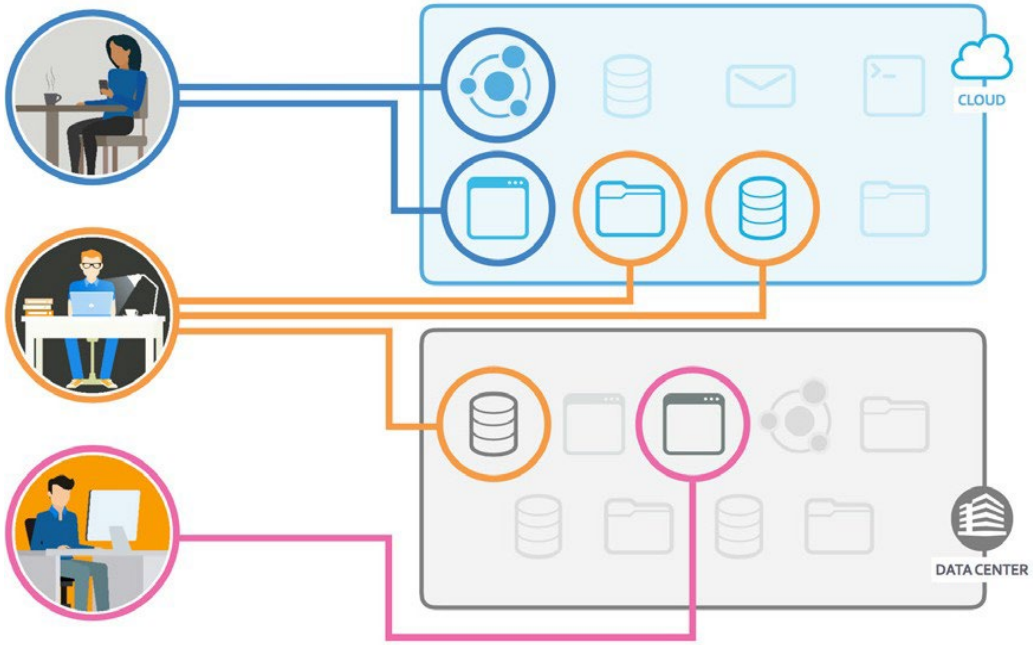
庁内、DC、クラウドなどのリソースの**ロケーションは関係なし！**端末も自宅、庁内どこでも一切関係ありません。
どこから、どこへでも、どんなシステムにもセキュアなアクセスを実現

・ベンダーフリーの豊富な連携

IAMはSAML(AzureAD)だけでなく、ADやLDAP、Radiusも対応！
EPP、EDR、SIEM、SWG、CASB…
既存のシステムを入れ替えずに導入可能であり、連携も実現します。
Microsoft 365 A5 Securityをお持ちであれば、
A5 Securityでは出来ない、「**ネットワーク**」視点や
「**動的なアクセス制御**」を補完して、より厳密な制御が可能

・サーバもIoTも対応

サーバへのアクセスはPCやスマホだけではありません。
サーバからサーバへの通信や、複合機のファイルサーバへのアクセスなど、
IPアドレスが存在するものは全て制御することが可能



教育情報ネットワークのセキュリティ強化やテレワークにもご利用頂けます！

Thank you