SCUGJ 第45回勉強会

2025/3/15

ロゴ作成中

Entra Private Accessをいじってみた

Windows Server and Cloud User Group Japan
後藤 諭史（Satoshi GOTO）

自己紹介

- 後藤 諭史（ Satoshi GOTO ）
- 国内SIerでプリセールスやっています
- 仮想化製品が主な専門分野です。
  が、基本的には雑用係
- Microsoft MVP - Cloud and Datacenter Management
  （Jul.2012 - Jun.2025）
  Microsoft MVP – Microsoft Azure（Jul.2024 - Jun.2025）

お約束ですが……

本セッション資料ですが、個人で準備した環境において、個人的に実施した検証／結果を基に記載しています。
あくまで個人の意見／見解であり、所属する会社の正式な回答／見解ではない事に留意してください。

お約束ですが……その 2

クラウドサービスを取り扱っているため、セッション当日（2025/03/15）時点の情報となります。
セッション終了直後、いきなり仕様が変更される場合もありますのでご了承ください。

昨今のネットワークレベルのセキュリティー

- 無条件の信用はもう存在しない
  - ゼロトラストネットワーク
    → かならず検証して確認せよ（どうやって？）
  - 境界型ネットワークの限界
    → 境界の内側のデバイスやユーザーを本当に信用していいのか？
    → 境界の外側にいるテレワークユーザーは……？

- VPNをどうにかしたい
  - 境界の外側にいるテレワークユーザーを無条件に信頼していいの？
  - VPN装置という攻撃対象領域（Attack Surface）
    → VPN装置（Firewall）の脆弱性がよく狙われます
    → 攻撃対象となるグローバルIPアドレスをもつ機器を極力減らしたい
  - VPN接続の認証をがっちがちにしてあげれば、あとは信頼してもいいの？ **今回はこちら**

- ほかにもいろいろありますが……

ロゴ作成中
User Group Japan

これって、Microsoftのソリューションで
実現できるんだっけ？

Global Secure Access とは

- Microsoft のセキュリティ サービス エッジ (SSE) ソリューション
- 以下の2つのサービスから構成
  - Microsoft Entra Internet Access（EIA）
  - Microsoft Entra Private Access （EPA）
- Microsoft Entra Internet Access（EIA）は、 Entra IDと連携されたセキュリティで保護されたWebゲートウェイ（SWG）を提供し、ユーザーを安全ではないコンテンツや非準拠コンテンツから守りながら、Webセキュリティを提供
- Microsoft Entra Private Accessは、 Entra IDと連携されたアプリケーションプロキシを提供し、インターネットからのセキュリティが担保された社内リソースへのアクセスを提供

今回はこちら

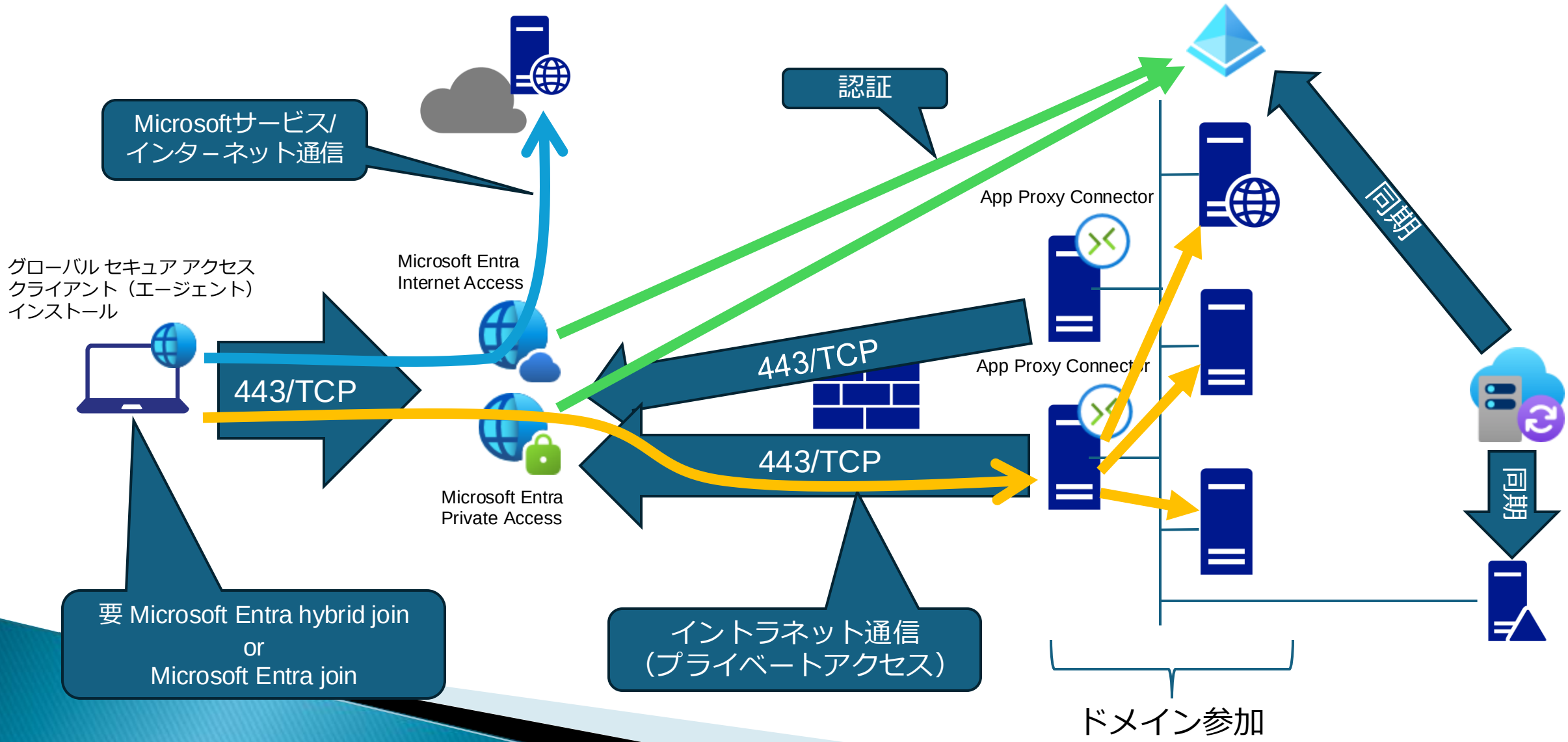
Global Secure Access の有効化（1）

管理者の任意で
ON/OFF可

Global Secure Access の有効化（2）

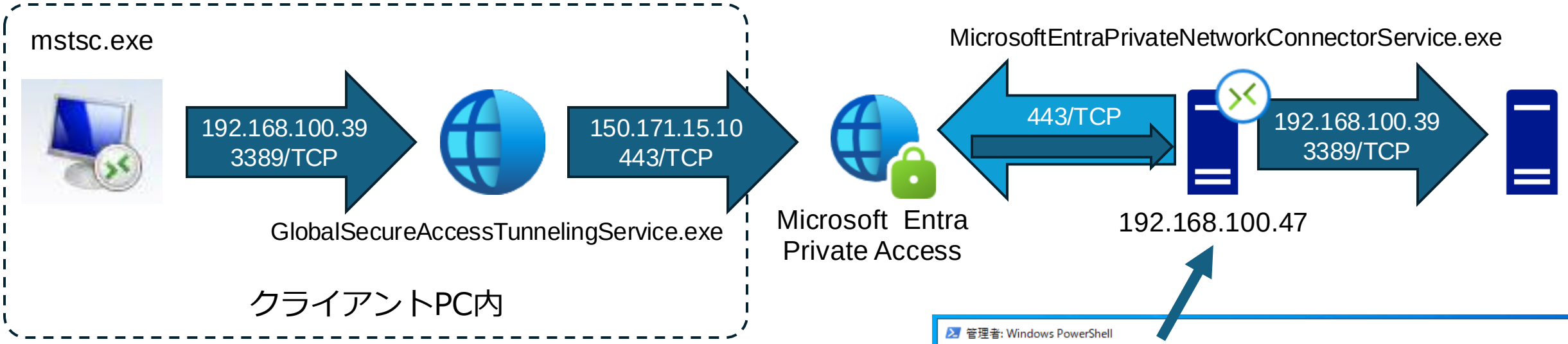
- 基本的にはクライアントにエージェントをインストールする
- サポートクライアントOSは以下の通り
  - Windows 10/11
  - Android （10.0以降）
  - iOS（Preview）（iOS 15.0以降）
  - macOS（Preview）（macOS Ver.13以降）
- **すべてのデバイスで、Microsoft Entraに登録されていることが前提**
  （Windowsクライアントは Entra joinが必要、他はIntune等で管理されたマネージドデバイスであること）

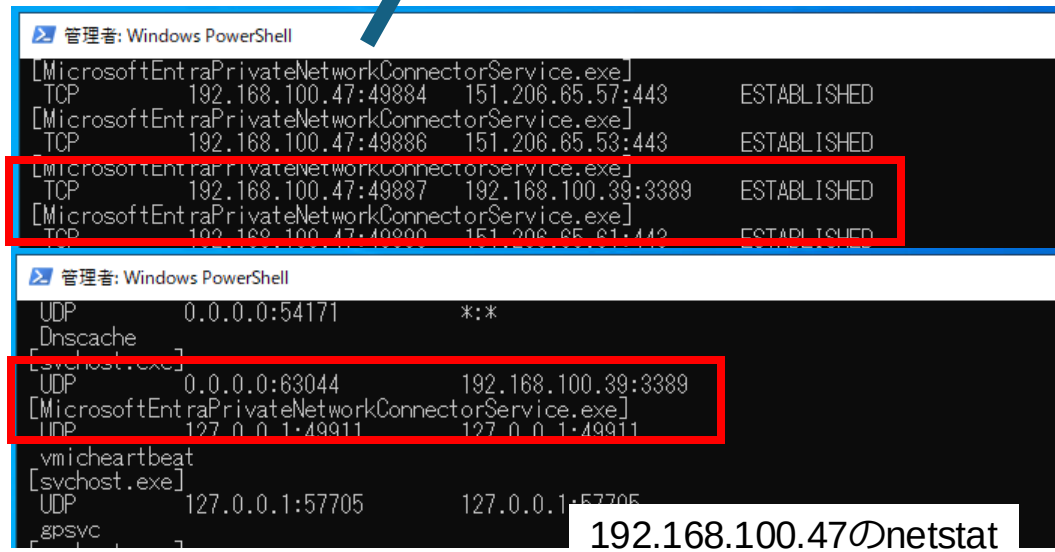
Global Secure Access の基本的な構成



デモ：
イントラネットサーバーへのRDP接続

デモから考えられるEPAの挙動

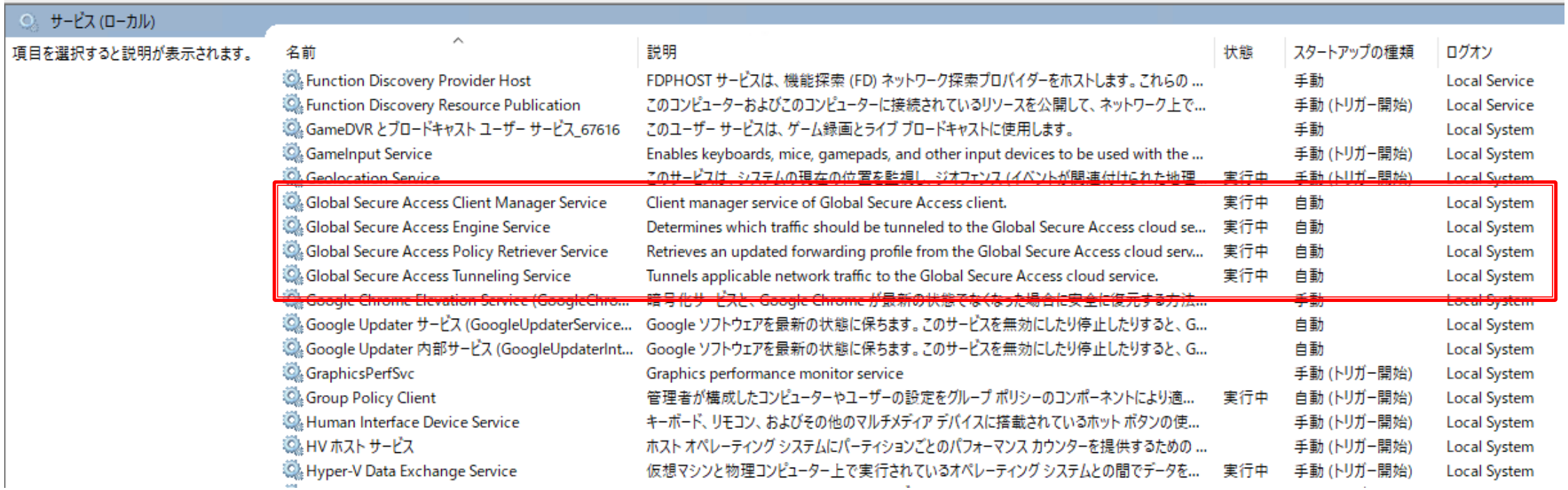




192.168.100.47のnetstat

- ルートテーブルなどは通常通りだったところから、ネットワークドライバーに近いレイヤーで「GlobalSecureAccessTunnelingService.exe」がポリシーにマッチしたパケットをフックし、トンネリング処理を実施していると考えられる。
- プライベートアクセス先は、コネクタ発の443/TCPのトンネルを利用して Microsoft Entra Private Accessサービスから転送されてきたパケットを自身発のパケットとしてターゲットサーバーに転送することで、通信を成立させている。

クライアントエージェント

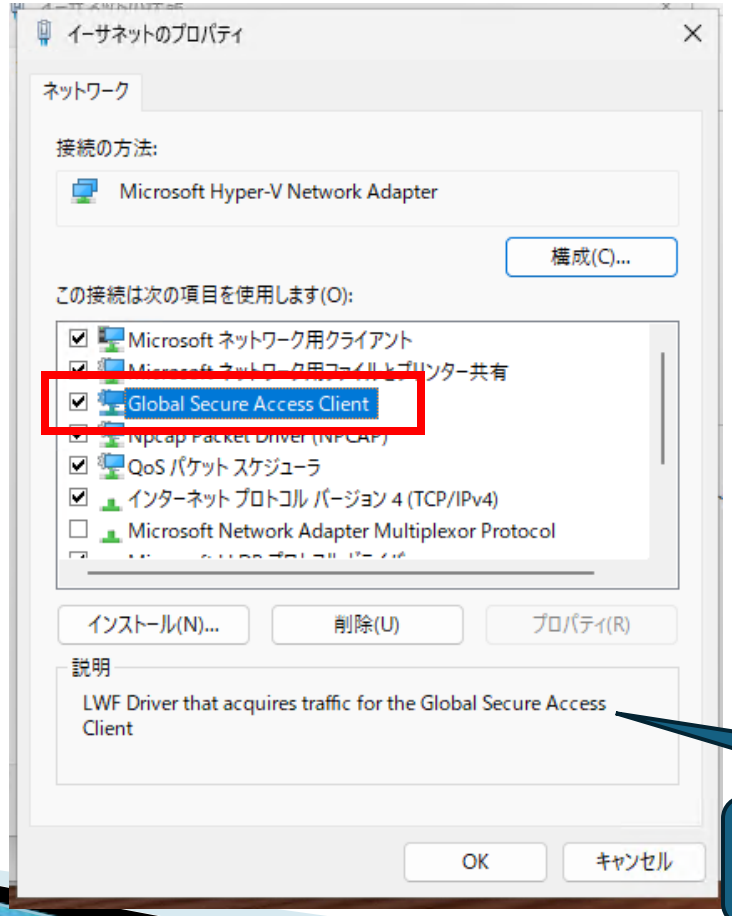


名前	説明	状態	スタートアップの種類	ログオン
Function Discovery Provider Host	FDPHOST サービスは、機能探索 (FD) ネットワーク探索プロバイダーをホストします。これらの ...		手動	Local Service
Function Discovery Resource Publication	このコンピューターおよびこのコンピューターに接続されているリソースを公開して、ネットワーク上で...		手動 (トリガー開始)	Local Service
GameDVR とブロードキャスト ユーザー サービス_67616	このユーザー サービスは、ゲーム録画とライブ ブロードキャストに使用します。		手動	Local System
GameInput Service	Enables keyboards, mice, gamepads, and other input devices to be used with the ...		手動 (トリガー開始)	Local System
Geolocation Service	このサービスは、システムの現在の位置を監視し、ジオフェンス (イベントが関連付けられた地理...	実行中	手動 (トリガー開始)	Local System
Global Secure Access Client Manager Service	Client manager service of Global Secure Access client.	実行中	自動	Local System
Global Secure Access Engine Service	Determines which traffic should be tunneled to the Global Secure Access cloud se...	実行中	自動	Local System
Global Secure Access Policy Retriever Service	Retrieves an updated forwarding profile from the Global Secure Access cloud serv...	実行中	自動	Local System
Global Secure Access Tunneling Service	Tunnels applicable network traffic to the Global Secure Access cloud service.	実行中	自動	Local System
Google Chrome Elevation Service (GoogleChro...	暗号化サービスと、Google Chrome が最新の状態でなくなった場合に安全に復元する方法...		手動	Local System
Google Updater サービス (GoogleUpdaterService...	Google ソフトウェアを最新の状態に保ちます。このサービスを無効にしたり停止したりすると、G...		自動	Local System
Google Updater 内部サービス (GoogleUpdaterInt...	Google ソフトウェアを最新の状態に保ちます。このサービスを無効にしたり停止したりすると、G...		自動	Local System
GraphicsPerfSvc	Graphics performance monitor service		手動 (トリガー開始)	Local System
Group Policy Client	管理者が構成したコンピューターやユーザーの設定をグループ ポリシーのコンポーネントにより適...	実行中	自動 (トリガー開始)	Local System
Human Interface Device Service	キーボード、リモコン、およびその他のマルチメディア デバイスに搭載されているホット ボタンの使...		手動 (トリガー開始)	Local System
HV ホスト サービス	ホスト オペレーティング システムにパーティションごとのパフォーマンス カウンターを提供するための ...		手動 (トリガー開始)	Local System
Hyper-V Data Exchange Service	仮想マシンと物理コンピューター上で実行されているオペレーティング システムとの間でデータを...	実行中	手動 (トリガー開始)	Local System

4つのサービスが導入される。実行ユーザーはローカルシステム

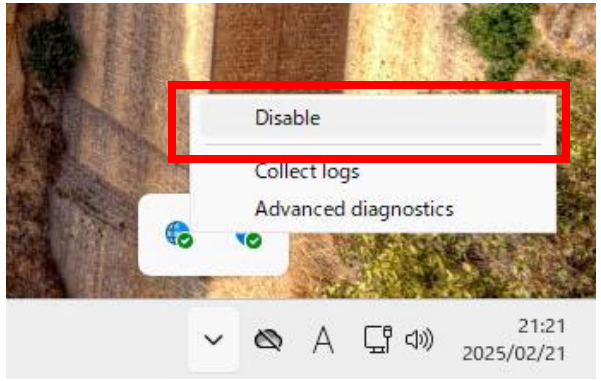
LWF（ライトウェイトフィルター）ドライバー

- グローバルセキュアアクセスのLWFドライバーが導入される

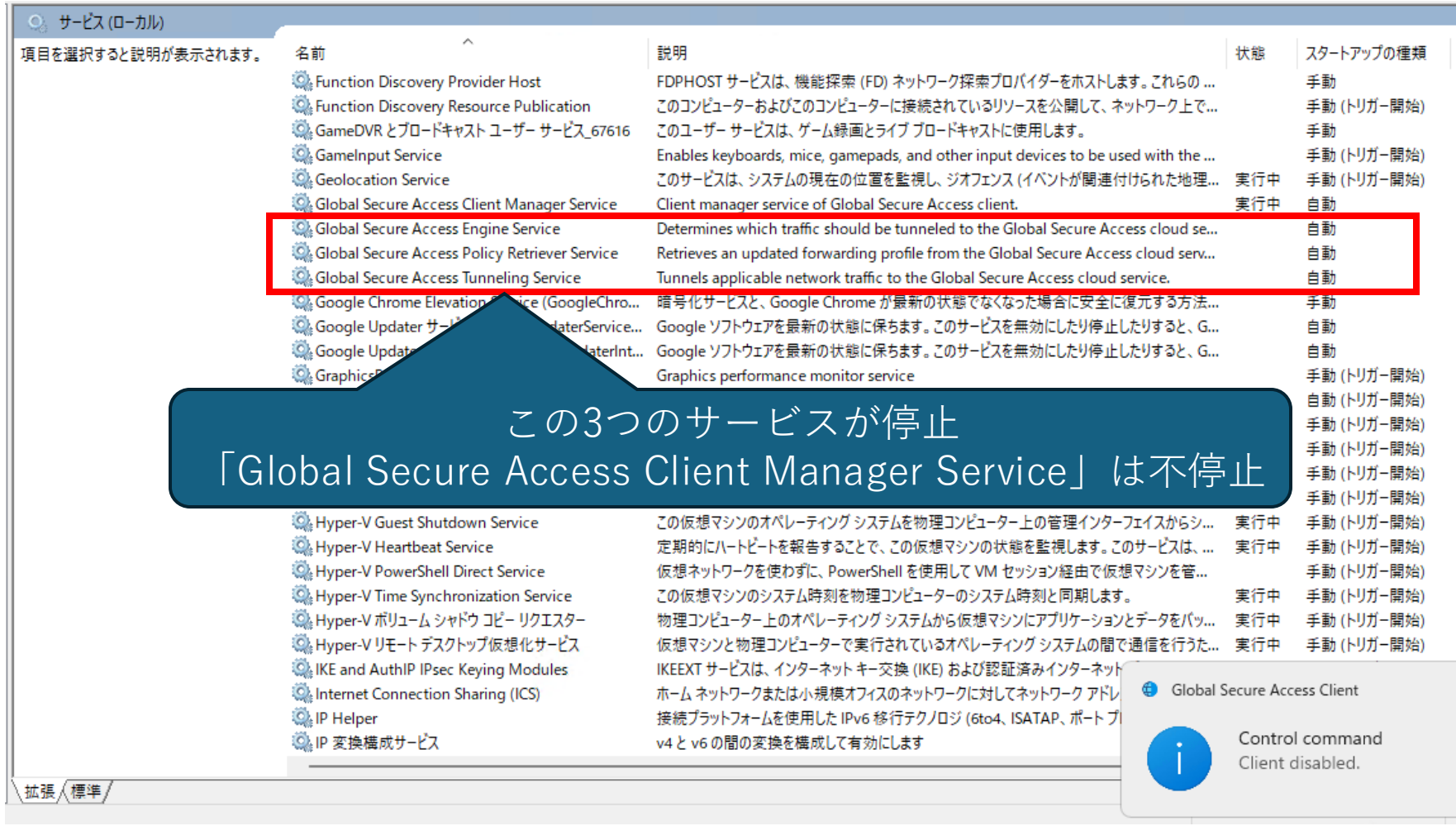


グローバルセキュアアクセスクライアントの
トラフィックを取得する LWF ドライバー

クライアントエージェント

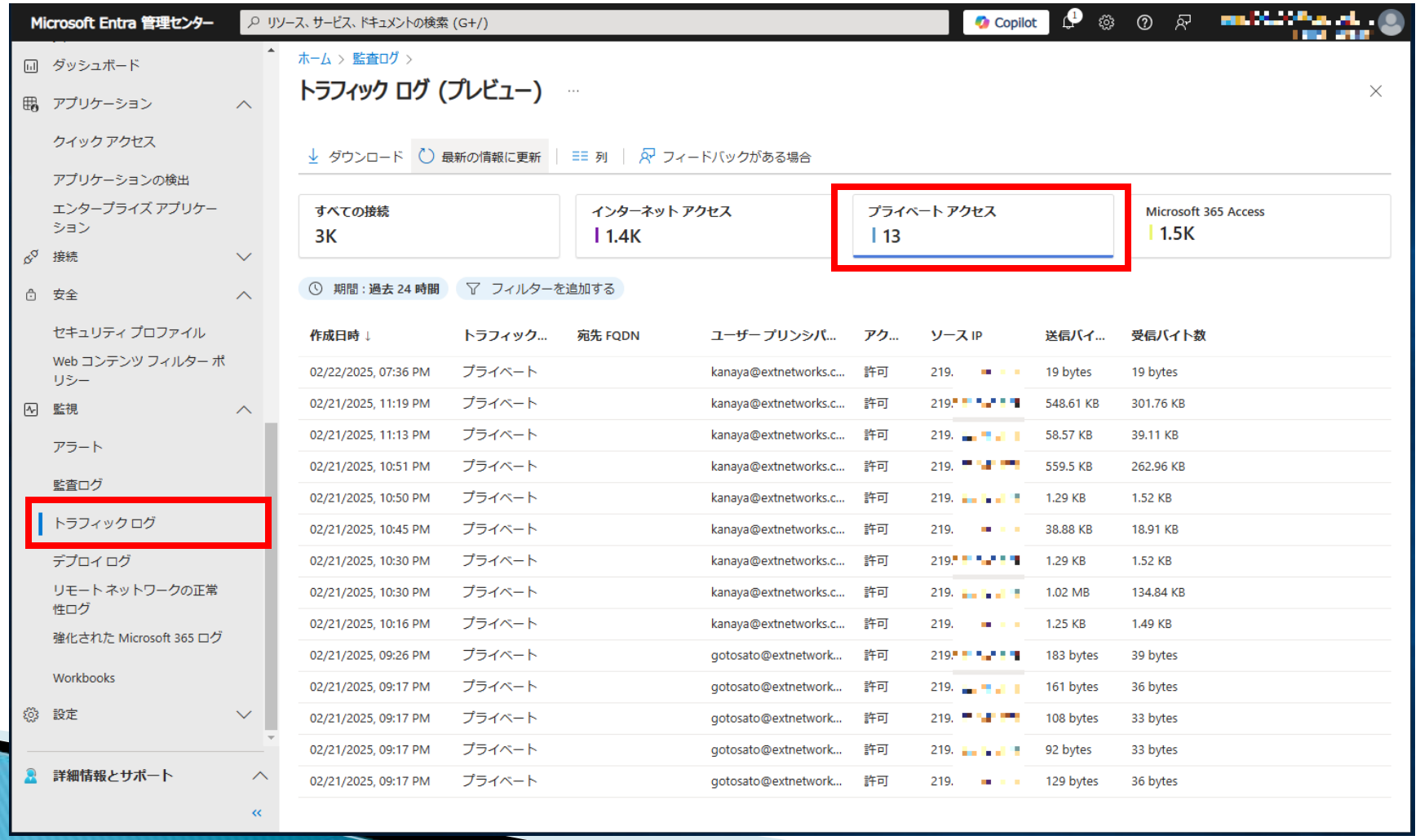


ユーザー権限で、エージェント停止可能
（社内ネットワーク接続時等に、明示的に停止可能）



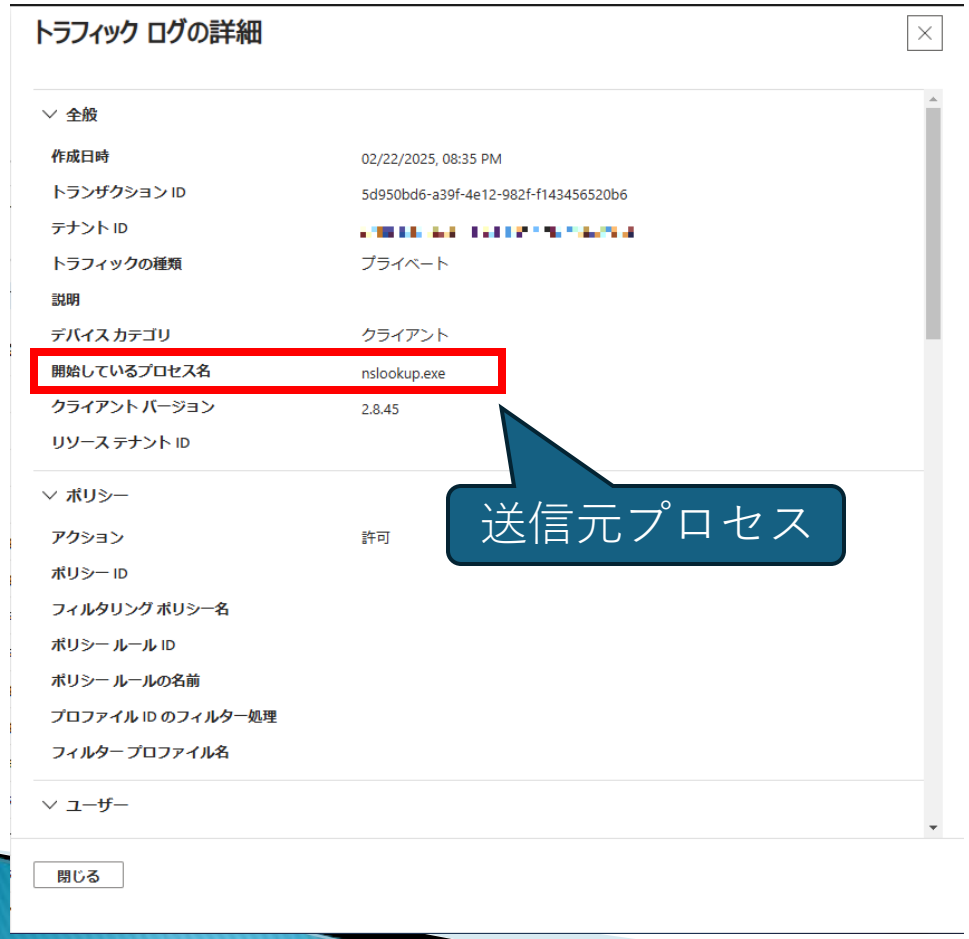
EPAのログ

- 「監視」→「トラフィックログ」→「プライベートアクセス」で参照可能

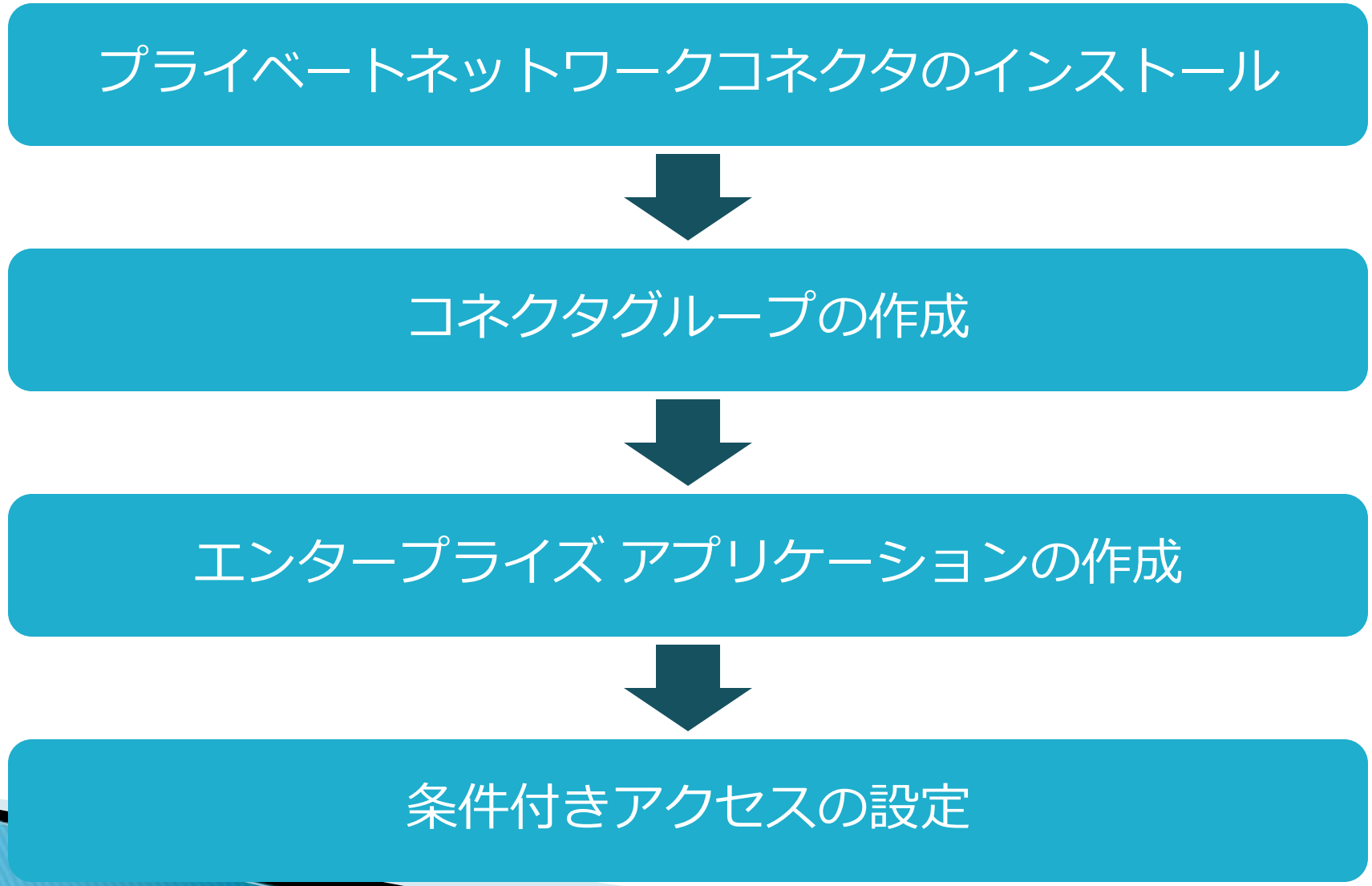


EPAのログ

- 送信元プロセス、通信プロトコルまで可視化



EPAのアプリケーション作成手順



プライベートネットワークコネクタ

- オンプレミスに設置する、Microsoft Entra Private Access及びアプリケーションプロキシサービスへの軽量なエージェント
- プライベートネットワーク上のリソースへのアクセスは、このコネクタを介して実施される
- そのため、高可用性を実現するために2台のコネクタを導入することも可能（本番環境では冗長化を推奨）
- ネットワーク要件としては、インターネット（AzureやGSAのサービス）に対して80/TCP、443/TCPを開けるだけで問題なし。インバウンド（インターネットへの公開）ルールは不要
- 同一プライベートネットワーク内に複数のコネクタ（およびグループ）を展開することも可能。アプリケーション単位で展開することも可能

プライベートネットワークコネクタの要件

- Windows Server 2012R2以降であればインストール可能
- その他のソフトウェア要件は以下の通り
  - 最小 .NET バージョンは v4.7.1 以上
  - Windows Server 2019以降にインストールする場合はHTTP 2.0を無効化
  - TLS1.2を有効化
- ドメイン参加は任意。ただしアプリケーションで統合Windows認証を使用する場合には、要ドメイン参加
- インターネット接続の際にプロキシが必須であるネットワークでもコネクタは使用可能。ただし、以下の点に注意する必要あり
  - 認証機能付きプロキシーは非サポート
  - プロキシーのTLSインスペクション機能は使用不可

参考：HTTP 2.0の無効化とTLS1.2の有効化

ロゴ作成中
User Group Japan

```
【HTTP 2.0 の無効化】
Set-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\' `
    -Name EnableDefaultHTTP2 -Value 0

【TLS 1.2 の有効化】
New-Item -Path 'HKLM:SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2'
New-Item -Path 'HKLM:SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client'
New-Item -Path 'HKLM:SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server'

Set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client' `
    -Name DisabledByDefault -Value 0
Set-ItemProperty ‘HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client’ `
    -Name Enabled -Value 1

Set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' `
    -Name DisabledByDefault -Value 0
Set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' `
    -Name Enabled -Value 1
```

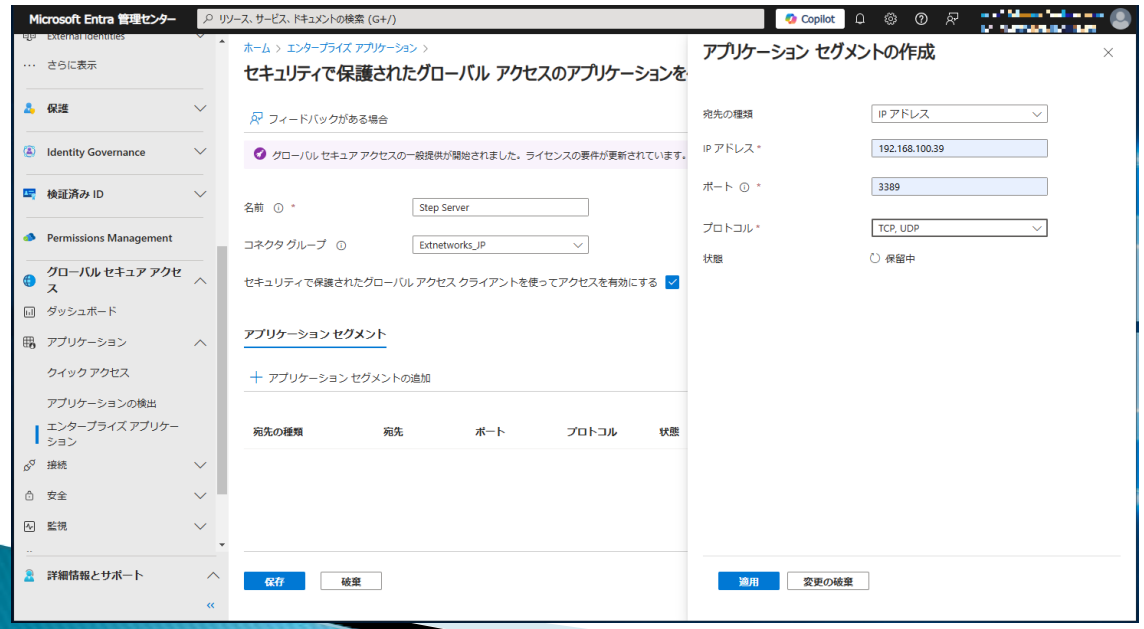
※ レジストリキー追加後は、要再起動

コネクタグループの作成

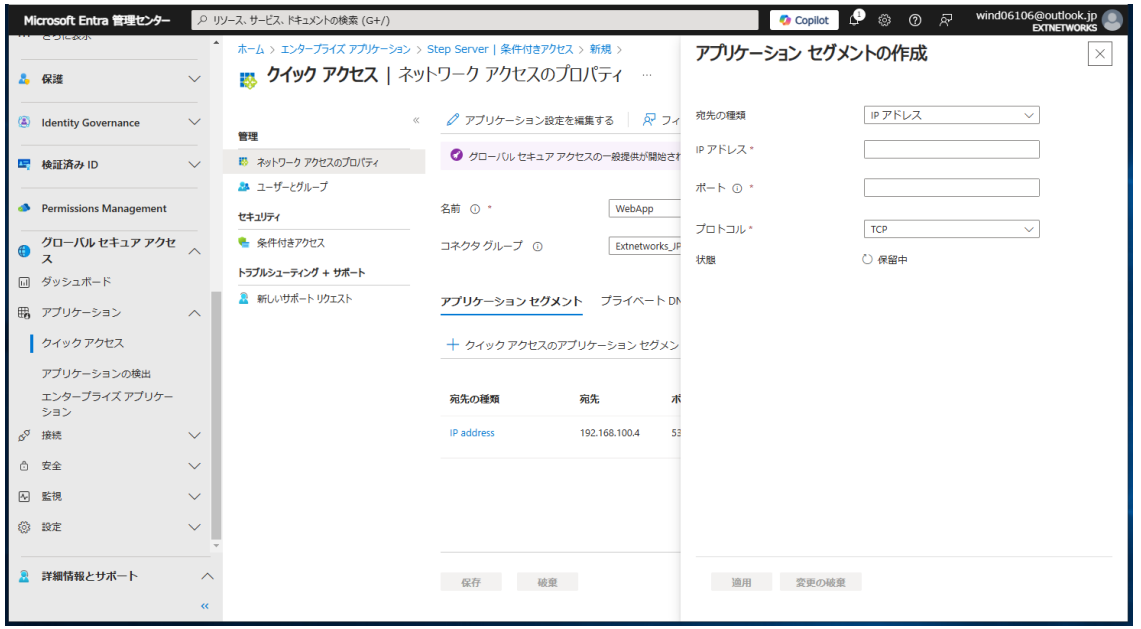
- エンタープライズアプリケーションに接続するための単体もしくは複数のコネクタをまとめるグループを作成
- 同一コネクタグループに複数のコネクタが存在する場合、すべてのコネクタが使用されるために可用性が向上する
- 作成時に地域を指定することでトラフィックフローを最適化可能。無指定の場合はテナントの場所に従って設定
- アプリケーション単位、地域単位等でグループを作成し、適用

エンタープライズアプリケーションの作成

- アプリケーション名、接続するためのコネクタグループを指定し、アプリケーションの接続先とプロトコルを指定して作成
- ささっとテストしてみたい場合は、「クイックアクセス」にアプリケーションをセグメントを作成することで使用可能



エンタープライズアプリケーションの作成



クイックアクセス設定

エンタープライズアプリケーションの作成

- 条件付きアクセスは、エンタープライズアプリケーション作成後に改めて作成

まとめ

- HTTPSのアウトバウンド通信のみで実装可能で、Entraの条件付きアクセスでコントロールできるため、VPNの代替として非常に有用です
- UDPも使用可能なので安心（Previewの時はTCPオンリーでした）
- Entra P1とEntra SuiteないしはEPAのスタンドアロンライセンスが必要なので、若干ライセンス的なハードルが高いかも……。すでにM365 E3やBPなどを使用中であれば、Entra SuiteないしはEPAのスタンドアロンライセンスでOKなのでおすすめ

リファレンス

- Global Secure Access に関するドキュメント
  https://learn.microsoft.com/ja-jp/entra/global-secure-access/

- Microsoft Entra Private Access について学習する
  https://learn.microsoft.com/ja-jp/entra/global-secure-access/concept-private-access

- グローバル セキュリティで保護されたアクセスに関する既知の制限事項
  https://learn.microsoft.com/ja-jp/entra/global-secure-access/reference-current-known-limitations

ご清聴、ありがとうございました。

ご不明点等ございましたら、
お気軽にご質問ください。