Spectrum Technology

V1.0 2026/8/5

抜粋版

はじめてのゼロトラスト・ネットワーク導入キット

～サイバー攻撃により事業停止とならないために～

導入編（Pi5版）

スペクトラム・テクノロジー株式会社

https://spectrum-tech.co.jp

sales1@spectrum-tech.co.jp

導入編　目次

- Pi運用マニュアル　ページ
  1. Piについて　4
  2. 基本コマンド　4
  3. 基本操作　6
  4. 日常運用　7
- 導入キット　全体像　9
- ハード・ソフトウエア概要
  1. ハード概要　10
  2. ソフト概要　11
- ゼロトラスト

1. Cloudflare概要　12
2. ゼロトラスト(ztna)作成手順　16
3. ゼロトラスト(ztna)作成
   - ① 準備　17
   - ② アカウント作成　18
   - ③ ゼロトラスト・ダッシュボード　19
   - ④ プライベートネットワーク接続　20
   - ⑤ 端末側設定　24
   - ⑥ アクセスポリシー設定　29
   - ⑦ トラヒック設定　40
   - ⑧ cloud & saas設定確認　42
   - ⑨ 作成のポイント　45
4. ゼロトラスト(ztna)管理　48
5. ゼロトラスト(ztna)利用例
   - ① 自宅からリモート勤務　51
   - ② 公衆WiFiの安全利用　52

抜粋版のためページは一致しません

導入編　目次

- ゼロトラスト　目次
- ネットワーク監視ツール　54

1. ネットワーク監視ツール　概要　55
2. ネットワーク監視ツール　設定
   - ① Zeek　59
   - ② Alloy　60
   - ③ Loki　61
   - ④ Grafana　62
3. ネットワーク監視ツール　利用例
   - ① Grafana全体　64
   - ② Conn　65
   - ③ Dns　66
   - ④ File　67
   - ⑤ http　68
   - ⑥ Ssl　69
   - ⑦ Time zeek　70
4. ネットワーク監視ツール 警報
   - ① Contact points　71
   - ② Alert：
     - port scan　73
     - file steal　75
     - Weird　77
     - Traverse　79

- 拡張

1. 本導入キットの拡張
   - ① ゼロトラスト・ネットワーク：複数拠点　82
   - ② ネットワーク監視：複数拠点　83
   - ③ ハードウエアの性能向上　84

抜粋版のためページは一致しません

Spectrum Technology

Pi運用マニュアル

Raspberry Pi

1. Raspberry Piについて

既に全世界で1000万台以上販売された手のひらサイズのコンピュータです。LinuxベースのRasbianOSで動作しております。

2. Linux基本コマンド

① システム関係

- 起動：電源を入れると自動で起動します。
- 再起動：# reboot

  又は、アプリケーション>ログアウト>再起動；左上のメニューから
- 終了： # shutdown

  又は、アプリケーション>ログアウト>シャットダウン；左上のメニューから
- ログアウト # logout

  又は、アプリケーション>ログアウト>ログアウト；左上のメニューから
- 日本語／英語の入力切替：キーボードの全角/半角キーで切替ます。

Spectrum Technology

Pi運用マニュアル

Raspberry Pi

2. Linux基本コマンド

② ディレクトリ操作、コピー、移動、削除

root@:~$ cd /root/Documents　　ディレクトリの切り替え
root@:/root/Documents# ls　　ファイルとディレクトリの表示（表示したら操作したいファイルを右クリックでコピペして操作します
root@:~# cp ファイル名　ディレクトリ　　配下のディレクトリのファイルを別のディレクトリへコピー
root@:~# mv ファイル名　ディレクトリ　　配下のディレクトリのファイルを別のディレクトリへ移動
root@:~# rm ファイル名　　ファイルの削除
便利な機能　rm –help　　コマンドのオプションが分からない場合は、ヘルプで問い合わせる。すべてのコマンド共通(マイナスを2個とhelp)

③ ユーザ権限、プロセス他

root@:~ $ su -　　スーパーユーザ（root)に切り替え、パスワードを入力
root@:~# ps a　　現状の動いているプロセスを表示
root@:~# kill　　特定のプロセスを強制終了
root@:~# apt-get install pkg　　パッケージのインストールなどに使用
root@:~# date　　日付、時間の設定を行います。
root@:~# mousepad /etc/network/interfaces　インタフェースに記述内容を変更します。Viよりも使いやすいです。

④ モジュール、usb、メモリ、HDDなどの表示

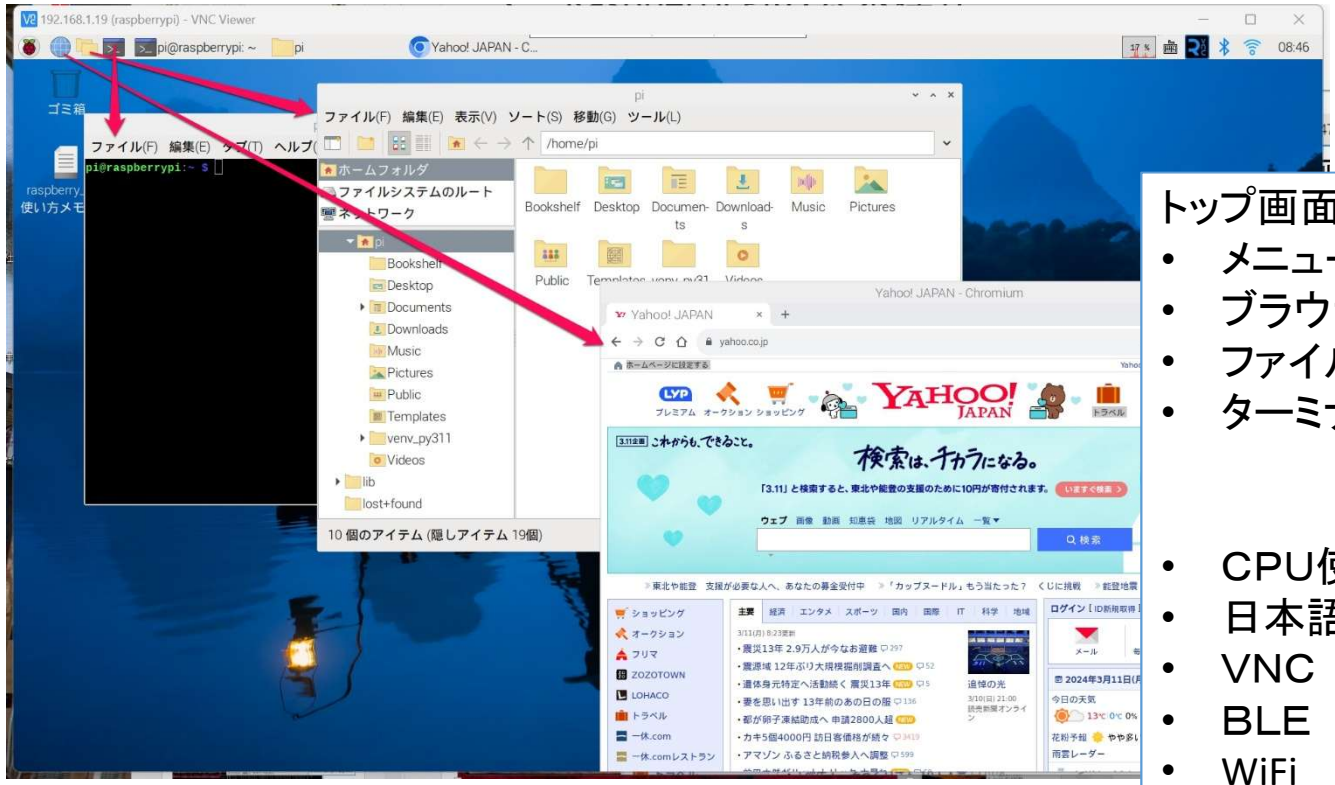
root@:~# lsmod　　linuxのモジュールリスト表示
root@:~# lsusb　　usbのデバイス表示
root@:~# free -mt　　メモリ使用状態表示
root@:~# df -h　　HDD（マイクロSD）の使用状態表示

pi@raspberrypi:~$ sudo
も同様のコマンドになります

RaspberryPi運用マニュアル

3. Raspberry Piの基本操作

① 表示画面と内容



トップ画面（上段のタスクバーで選択）

- メニュー
- ブラウザ
- ファイルマネジャ
- ターミナル

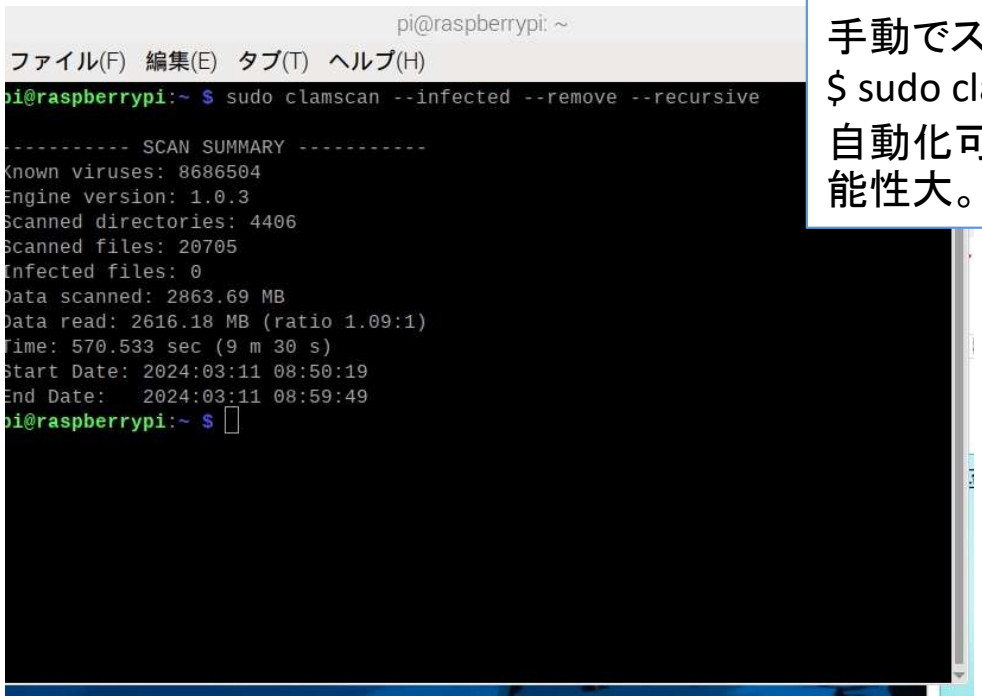
- CPU使用率
- 日本語入力
- VNC
- BLE
- WiFi
- 時刻

RaspberryPi運用マニュアル

4. 日常運用

① セキュリティ対策（アンチウイルス更新、スキャン）

- アンチウイルス対策として無料のclamAVをインストールしてます。
- 手動での運用を基本としてます。



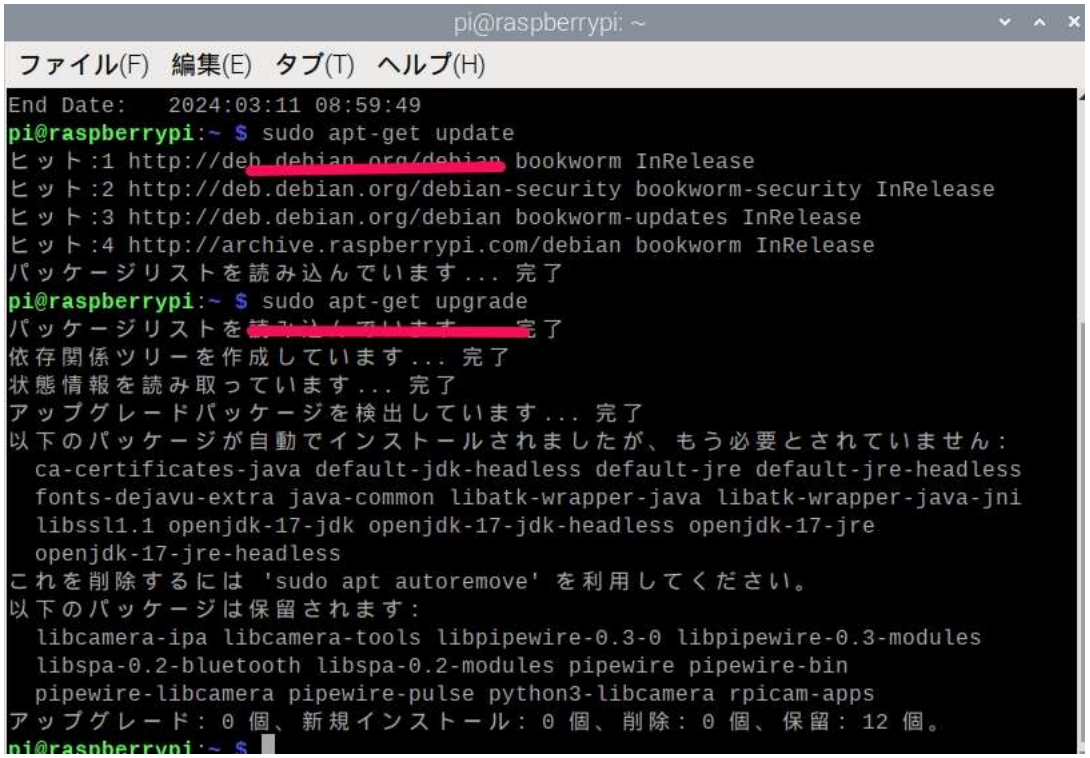
パターンファイル更新
手動スキャン時に更新されます
手動でスキャン
$ sudo clamscan --infected --remove --recursive
自動化可能ですが、バックグランドで重くなる可能性大。コマンド入力後約10分位かかります。

RaspberryPi運用マニュアル

4. 日常運用

② インストール済パッケージの更新リスト、アップグレード

- Linuxの場合は、頻繁に更新が発生します。アップグレードを定期的に実施してください。
- 更新前には、バックアップを取ることをお勧めします。特にアップグレードはまれに動作不良、戻せない状態が発生します。自己責任で実施してください。



更新リスト取得
$ sudo apt-get update
アップグレード実施
$ sudo apt-get upgrade

Spectrum Technology

ゼロトラスト・ネットワーク導入キット　全体像(Pi5版)

ハードウエア

Raspberry Pi5

＋

物品追加

電源アダプタ
（オプション）

HDMIケーブル
（オプション）

OS

Raspbian OS

主な機能

- Ztna(zero trust network access)
  - vpnの脆弱性を排除
  - 端末毎にアクセス制御
- ネットワーク監視
  - ポートスキャン、ファイル持ち出し、異常パケット、横移動等の危険な動きを検出し、slack通知
  - ネットワーク内全トラヒック監視

ZTNA系

CLOUDFLARE

ネットワーク監視系

zeek

Grafana

Grafana Alloy

Grafana loki

弊社提供

Spectrum Technology

1．ハード概要

本体

品名	項目	内容	備考
Raspberry Pi5	CPU	2.4GHz 4コア Cortex-A76（ARMv8、64bit）	
	GPU	VideoCore VII®	
	メモリ	4GB RAM	
	OS	Raspbian bookworm(Debianベース）	
	インターフェース	2.4/5GHz WiFi(802.11 bgnac), Bluetooth 5.0, BLE, 1G ether, USB 2.0x2, USB 3.0x2, micro HDMIx2, microSDカード, 40 GPIO pin	
	電源／消費電力	Micro USB Type C　3.0A	
	サイズ	85x56x18mm	

付属品	内容	備考
ケース	赤白、FAN付。	
microSD 64GB	Raspbian OS, 必要なモジュールをインストールして提供します。お客様が設定するものは必要最低限のパスワード設定、WiFi設定になります。	
プログラム	Cloudflare, zeek等インストール済	
マニュアル	設定編、導入編	

USB電源ケーブル、HDMIケーブルは付属しておりません。
別途オプション品を購入ください

Spectrum Technology

2. ソフト概要

提供するソフトウエアの概要です。

区分	ソフト名	バージョン	備考
OS	Raspbian	Bookworm 64bit	
ZTNA関係	cloudflared	2026.7.3	
ネットワーク監視	zeek	8.2	
	grafana	13.1.1	表示
	alloy	1.18.1	収集
	loki	3.0.0	保存
プログラム言語	python3	3.11.2	仮想化で利用

Spectrum Technology

ゼロトラスト

Spectrum Technology

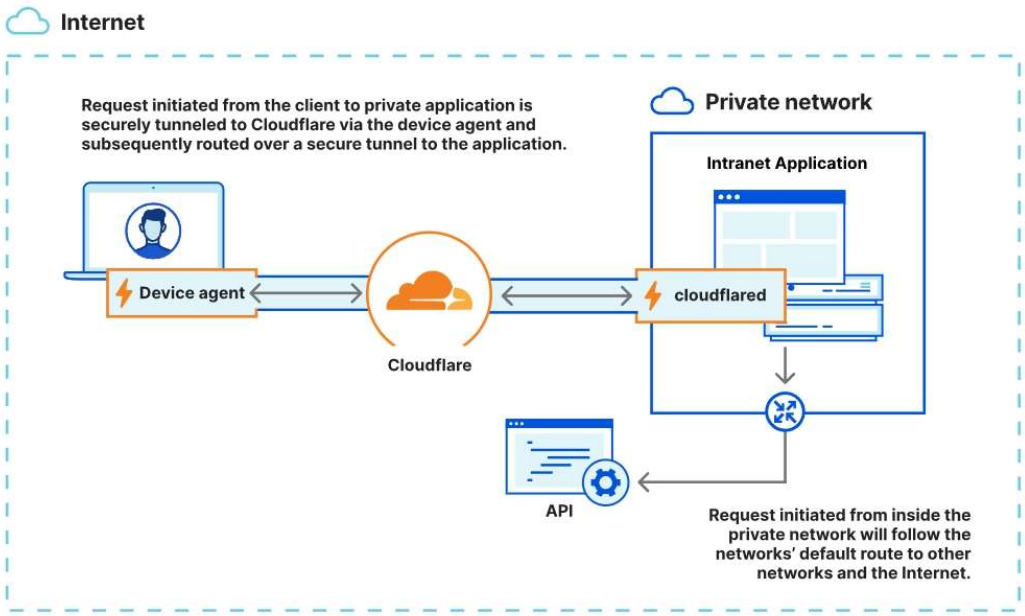
1.Cloudfare概要

- Cloudflareとは？
  - Cloudflareは、世界最大級のコネクティビティ・クラウド・ネットワークの一つです。今日、インターネット上で活動するあらゆる人々が、Cloudflareを利用することで、より高速かつ安全なウェブサイトやアプリケーションを実現できます。
  - Zero trust network accessの代表で、vpnの脆弱性を代替するものになります
  - https://developers.cloudflare.com/learning-paths/replace-vpn/get-started/
  - https://github.com/cloudflare/cloudflared
- 特徴
  - 内部脅威 — ZTNAは、脅威がネットワークの内部と外部の双方に存在し得ることを前提とすることで、セキュリティを強化します。VPNがログイン済みのすべてのユーザーを暗黙的に信頼するのに対し、ZTNAは「最小権限の原則 」を重視し、ユーザーIDの継続的な検証を徹底します。
  - ネットワークセキュリティ — ZTNAアーキテクチャは、ネットワークのマイクロセグメンテーション を促進することで、潜在的な脅威による影響範囲（ブラスト・ラジアス）を縮小します。ユーザーに企業ネットワーク全体へのアクセスを許可するVPNとは異なり、ZTNAは特定のアプリケーションへのアクセスのみを許可し、デフォルトでは他のすべてのリソースへのアクセスを拒否します。
  - パフォーマンス — ZTNAは、オンプレミスのVPNサーバーではなく、クラウド 経由でユーザーを企業ネットワークに接続します。これにより、ユーザーはパフォーマンスの低下を招くことなくどこからでも接続できるようになり、クラウドベースのインフラストラクチャとの統合も容易になります。

Spectrum Technology

1.Cloudfare概要

- 構成



- 仕組み

①ユーザーは自身のデバイスでCloudflare One Clientを実行

②管理者はネットワーク内またはアプリケーションサーバー上でCloudflare TunnelまたはCloudflare Meshを運用します。ゼロトラストを導入すると、ユーザーは（インターネットに公開されていない）プライベートリソースにTCP/UDP/ICMP経由で接続できるようになり、管理者はユーザーのID、デバイスの健全性（ポスチャ）、その他の要素に基づいて、それらのリソースへのアクセスを制御できるようになります。

1.Cloudfare概要

- 契約
  - 無料で50ユーザまでを利用

まずは無料で開始

プラン	Free(～50ユーザー)	Pay-as-you-go	Enterprise(Contract)
料金	$0(無料、常設プラン) Zerometric	$7/ユーザー/月(年払い) CostBench	カスタム見積もり(年契約) Zerometric
ZTNA(Access)	フル機能 Zerometric	フル機能	フル機能
Secure Web Gateway(DNS/HTTP/ネットワークフィルタリング)	フル機能(DNS・HTTPフィルタリング) Zerometric	フル機能	フル機能
WARPクライアント / アプリコネクタ	利用可 Zerometric	利用可	利用可
CASB	読み取り専用API連携 2 件まで Zerometric	制限あり	無制限のout-of-band CASB連携 Zerometric
DLP	定義済みプロファイルのみ、限定的 Zerometric	定義済みポリシーのみ Zerotrustcost	カスタムプロファイル・カスタムデータセット・OCR対応のフル機能DLP Zerometric
Remote Browser Isolation(RBI)	対象外	アドオンとして追加課金(目安 $10/ユーザー/月) NearBound	アドオンとして提供 Zerotrustcost
メールセキュリティ	対象外	対象外	アドオンとして提供 Zerometric
ログ保持期間	24時間 Zerometric	30日間 Zerometric	最大6ヶ月(Logpush経由でSIEM連携可) Zerometric
拠点数上限	3拠点まで Zerometric	上限なし	上限なし
サポート	コミュニティのみ Zerometric	SLA付き Zerometric	電話サポート、専任サポートあり Zerometric
SASEネットワーク機能(Magic WAN/Magic Firewall)	対象外	対象外	アドオンとして提供 Zerometric

2.ゼロトラスト(ztna)作成手順

https://developers.cloudflare.com/learning-paths/replace-vpn/get-started/

① 準備
- 端末用ソフトダウンロード：Cloudflare One Client
- ホストサーバ準備：今回は、弊社raspberry pi5

② アカウント作成
- Cloudflareアカウント作成：メール、パスワード、2FAなど

③ ゼロトラスト・ダッシュボード
- ダッシュボードへ
- 契約内容設定
- プロバイダ構成

④ プライベートネットワーク接続
- 接続方法設定：mesh,トンネル

⑤ 端末側設定
- Cloudflare One設定
- 接続
- 接続確認

⑥ アクセスポリシー設定
- awsへのアクセス制限
- nasへのアクセス制限
- saasへのアクセス制限

⑦ トラヒック設定
- firewall設定

⑧ cloud & saas設定確認
- AWS設定

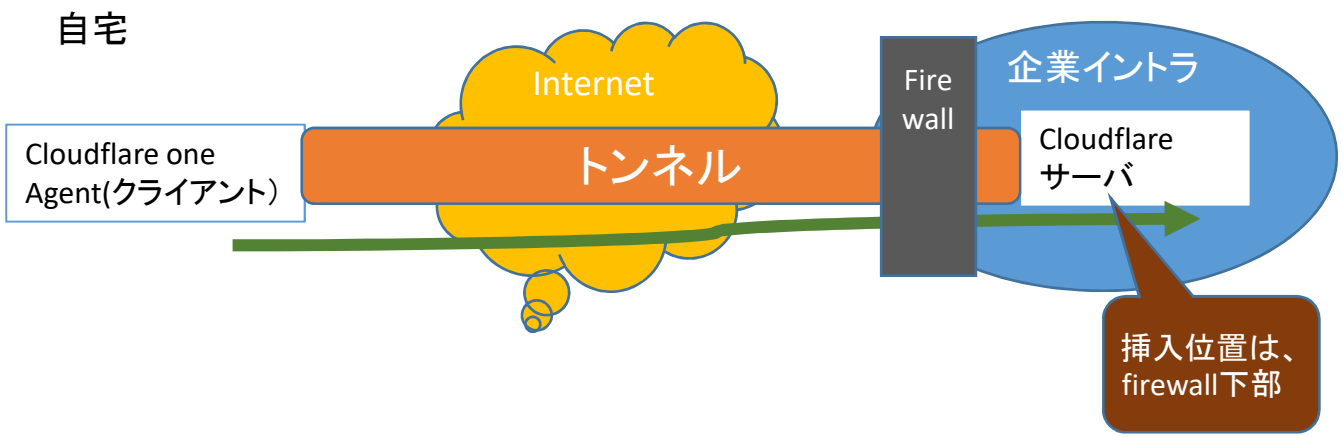
⑨ 作成のポイント
- アクセス制御
- team & resources
- traffic policy

3.ゼロトラスト(ztna)作成

①. 準備

https://developers.cloudflare.com/learning-paths/replace-vpn/get-started/

- 端末用ソフトダウンロード：Cloudflare One Client
  - https://developers.cloudflare.com/cloudflare-one/team-and-resources/devices/cloudflare-one-client/download/
  - 種類を選んでダウンロード：windows, mac,linux,ios,android
- ホストサーバ準備：今回は、弊社raspberry pi5
  - https://developers.cloudflare.com/cloudflare-one/networks/connectors/cloudflare-tunnel/configure-tunnels/tunnel-availability/system-requirements/#recommendations



3.ゼロトラスト(ztna)作成

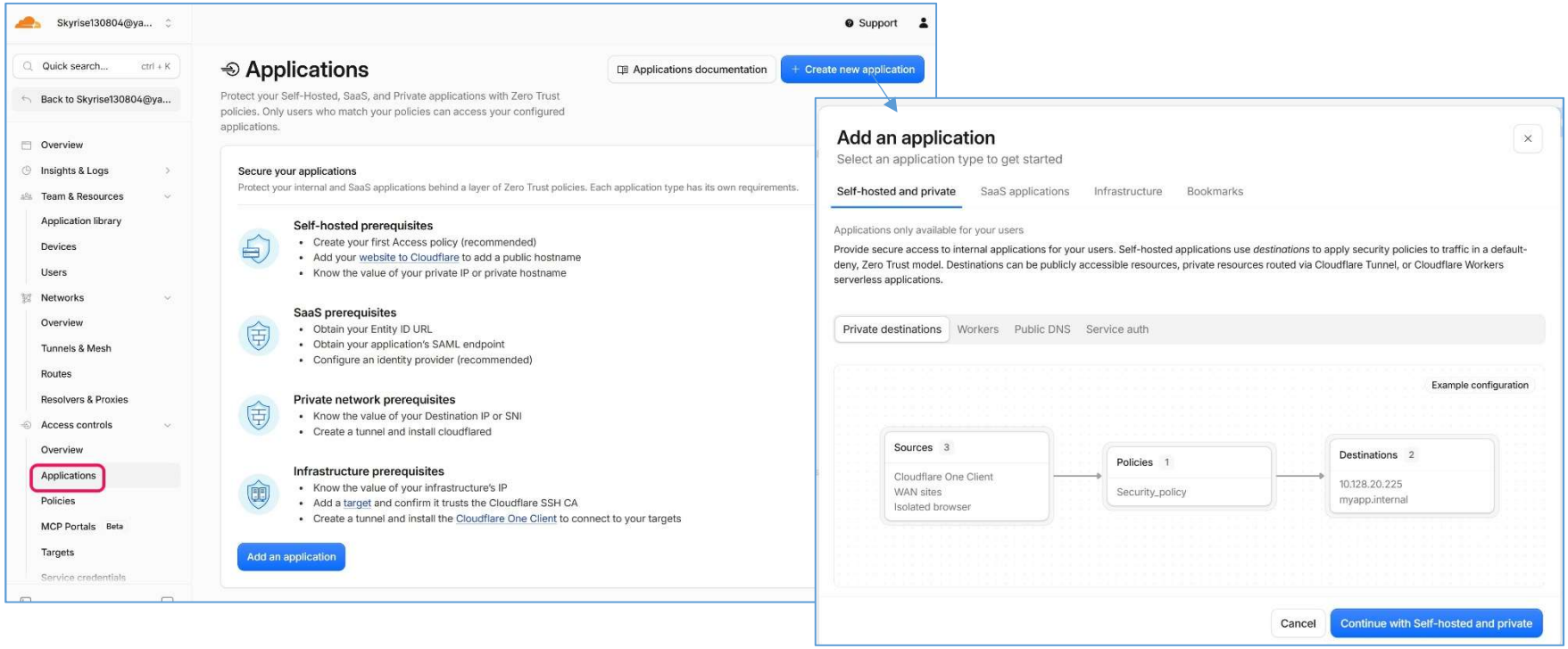
⑤.端末側設定

- https://developers.cloudflare.com/cloudflare-one/team-and-resources/devices/cloudflare-one-client/
- Cloudflare One設定
  - https://developers.cloudflare.com/learning-paths/replace-vpn/connect-devices/install-agent/
  - 端末の種類を選んでダウンロード
  - iphone例
  - Cloudflare one agentをダウンロード
  - プライバシーポリシー：同意
  - チーム名： こちらで設定したものを入力
  - メールアドレス：管理者が招待したメールアドレスこちら
  - メール確認：認証番号6桁入力
  - 設定完了
- 接続
  - スライドするだけ
  - Iphone>設定＞vpnでも確認できます

3.ゼロトラスト(ztna)作成

⑥.アクセスポリシー設定

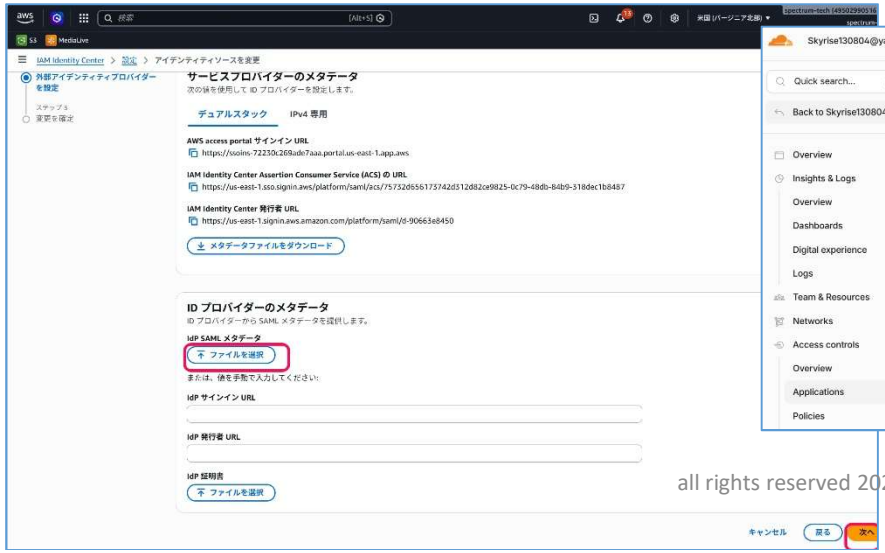
- https://developers.cloudflare.com/learning-paths/replace-vpn/build-policies/
- アプリ毎にアクセスポリシー設定
  - ネットワークおよびアプリのネットワーク情報を登録
  - Zero trust dashboard>access control>application
  - 作成

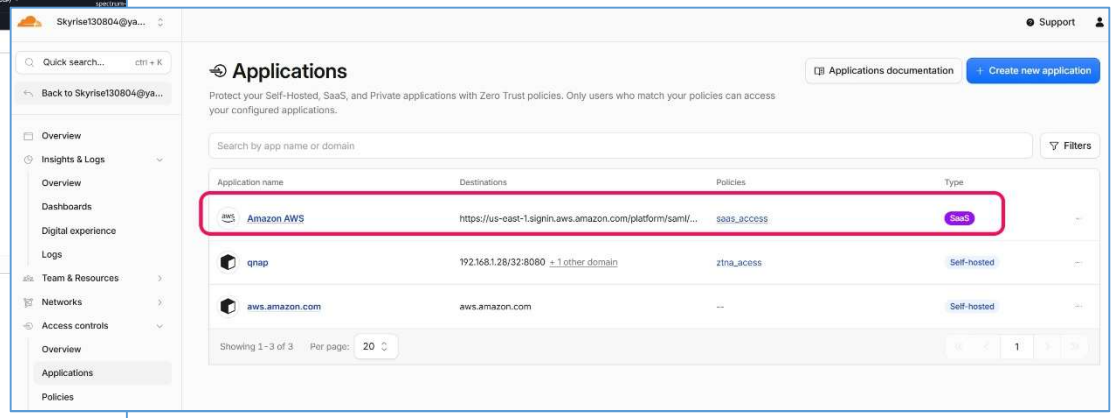


3.ゼロトラスト(ztna)作成

⑥.アクセスポリシー設定　その3

- https://developers.cloudflare.com/learning-paths/replace-vpn/build-policies/
- https://developers.cloudflare.com/cloudflare-one/access-controls/applications/http-apps/saas-apps/aws-sso-saas/
- アプリ毎にアクセスポリシー設定
  - ネットワークおよびアプリのネットワーク情報を登録
  - Zero trust dashboard>access control>application
  - アプリ作成
    - ホスト名：適宜：saasへのアクセス制限
    - Aws設定、small
    - Aws>IAM Identity Center> identity source変更、外部id provider>発行url,acs urlをコピー
    - Entryid:発行url, acs url:acs urlをコピペ、SAML Metadata endpointをコピーして別ブラウザで開き、access_saml_metadata.xmlで保存
    - aws側へxmlファイルをアップロードし完了
    - cloudfare側もアクセスポリシー設定し完了

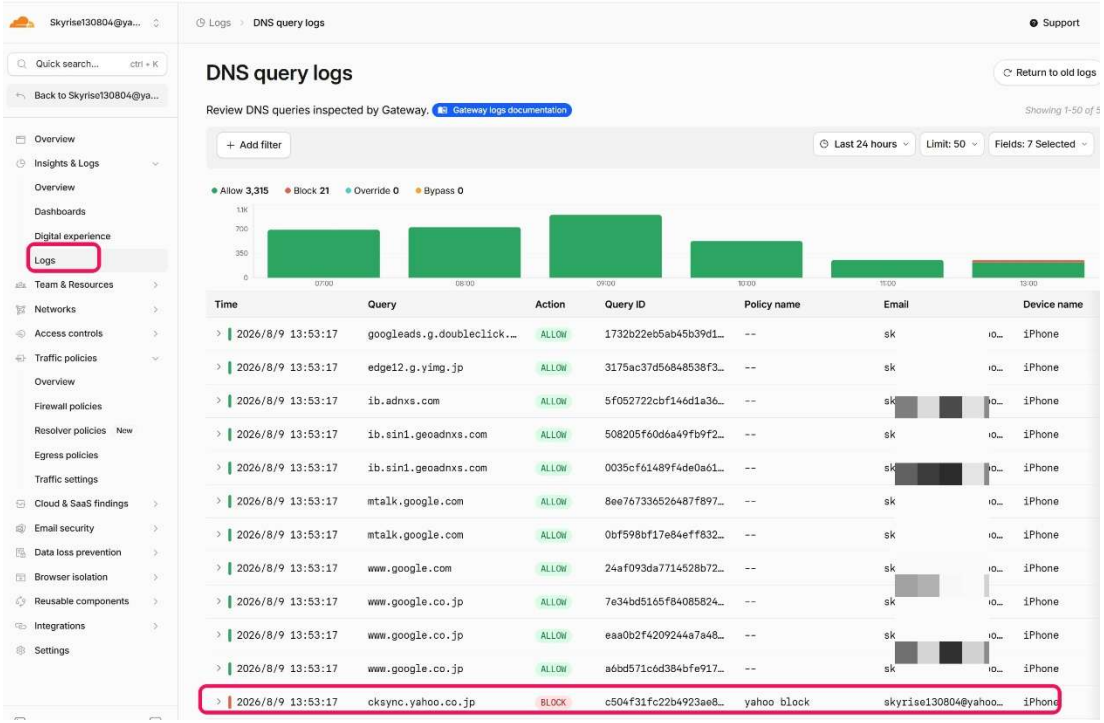




3.ゼロトラスト(ztna)作成

⑦.トラヒック設定

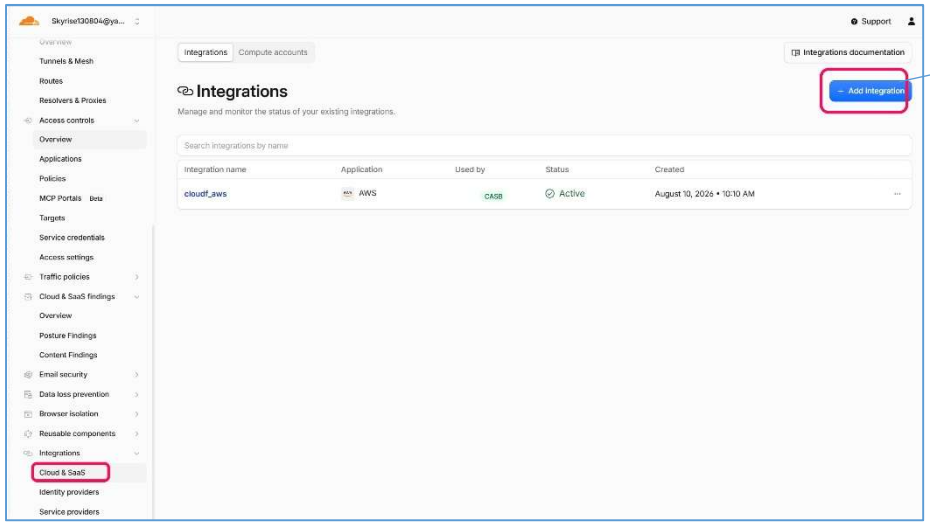
- https://developers.cloudflare.com/learning-paths/replace-vpn/build-policies/
- Dnsポリシー設定
  - ドメインで規制をかける。一番簡単に設定できる
  - Traffic policy>firewall設定
  - dnsポリシー追加
  - ドメイン：yahoo, block
- 確認テスト
  - Log＞dns logで確認。

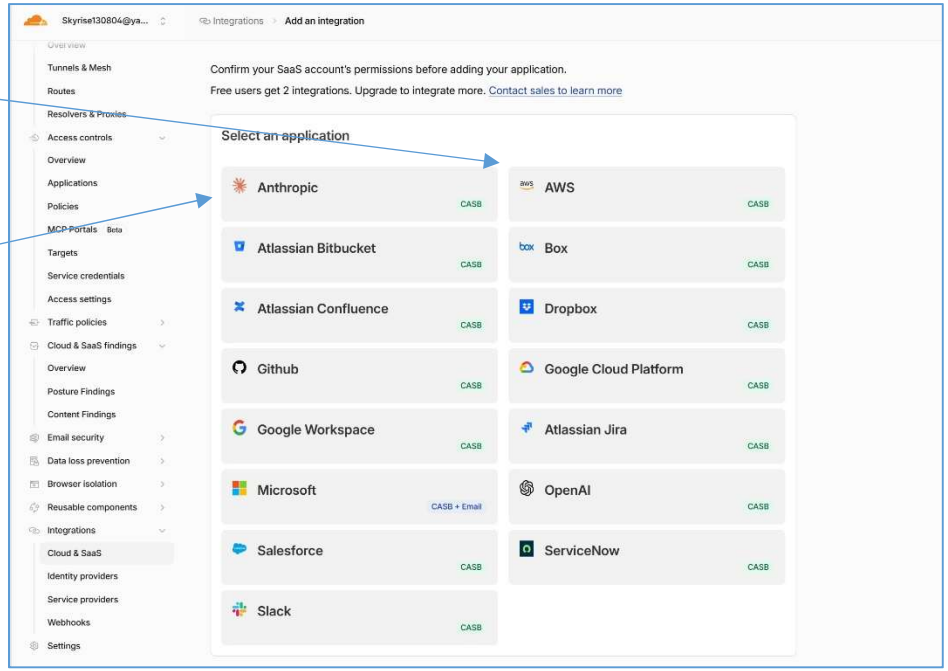


3.ゼロトラスト(ztna)作成

⑧.cloud & saas設定確認

- https://developers.cloudflare.com/cloudflare-one/cloud-and-saas-findings/
- cloud & saasの設定ミスなどを発見できるツール
- cloud設定
  - AWSの設定
  - Integration>cloud & saas：追加
  - AWSを選択
  - AWSのIAMに設定
  - 完了

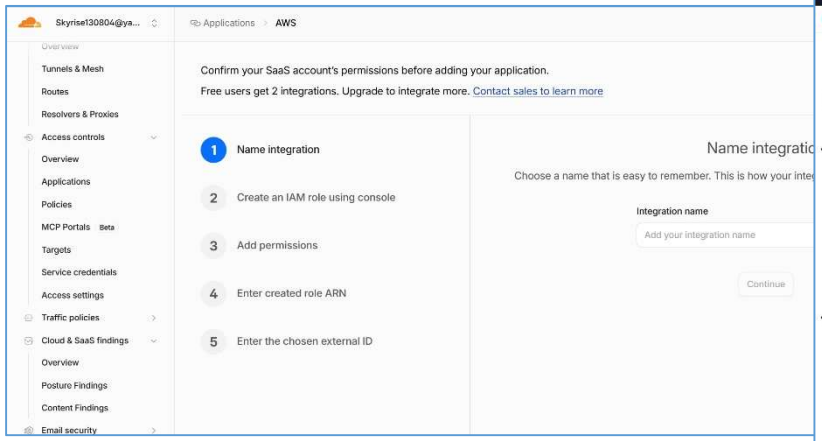


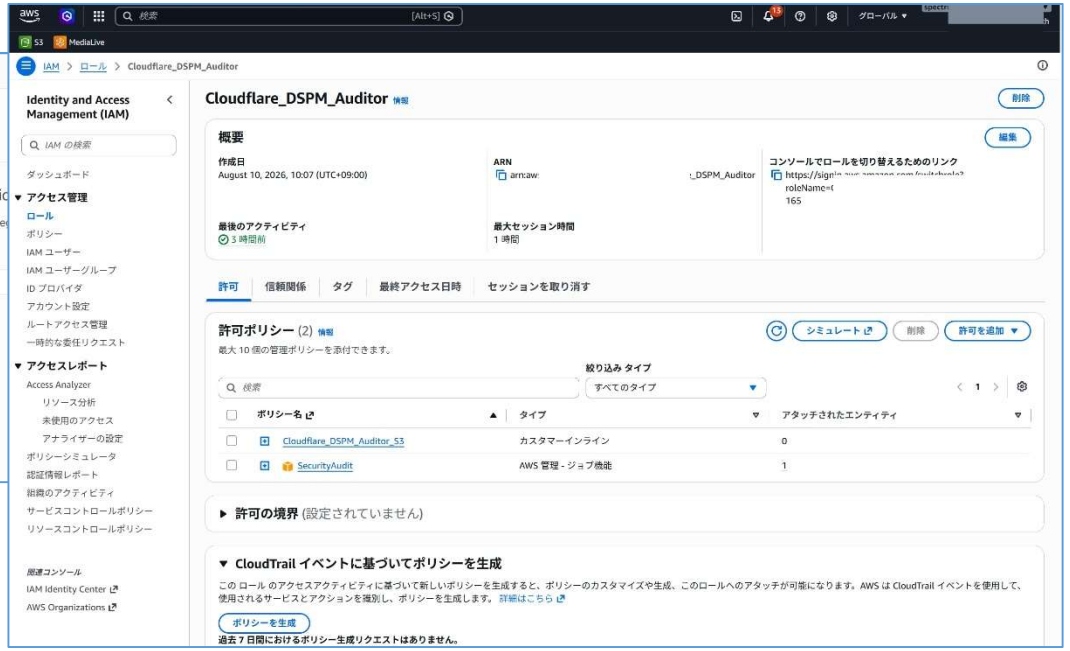


3.ゼロトラスト(ztna)作成

⑧.cloud & saas設定確認

- https://developers.cloudflare.com/cloudflare-one/cloud-and-saas-findings/
- cloud & saasの設定ミスなどを発見できるツール
- cloud設定
  - AWSの設定
  - Integration>cloud & saas：追加
  - AWSを選択
  - AWSのIAMに設定:指示どおりで作成できます。
  - 完了

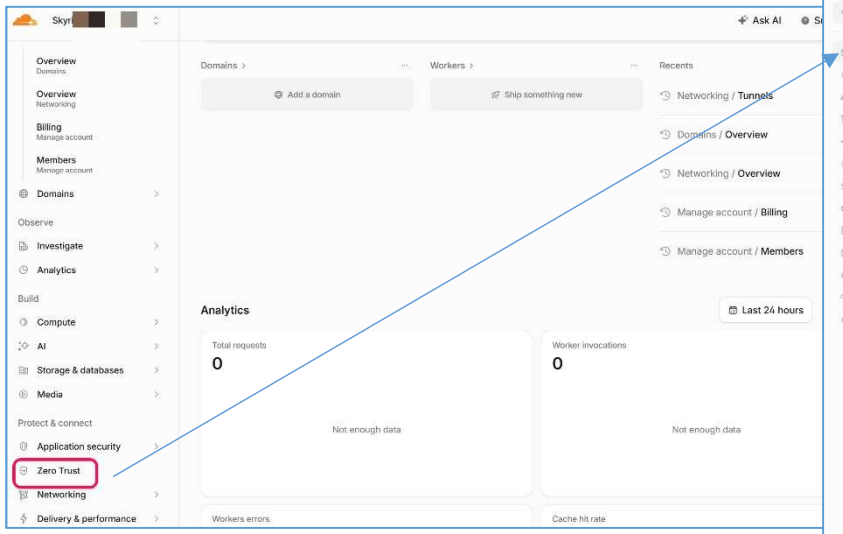


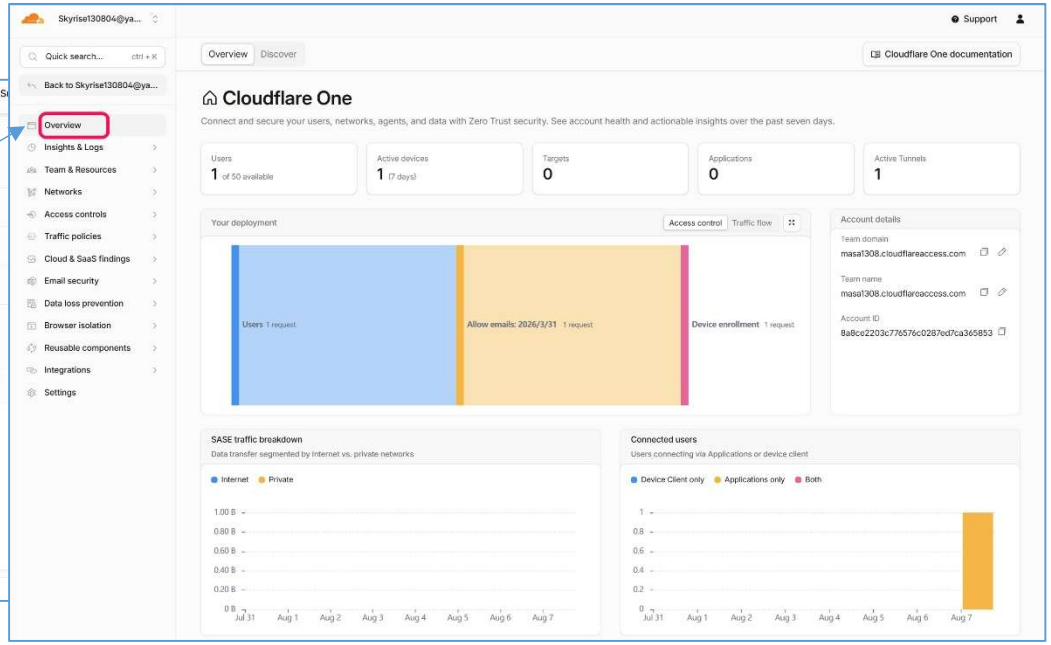


4.ゼロトラスト(ztna)管理

①. ダッシュボード　概要

- https://dash.cloudflare.com/login
- マイページからzero trustのdashboardへ
- 概要：接続ユーザ数、トラヒックなど表示

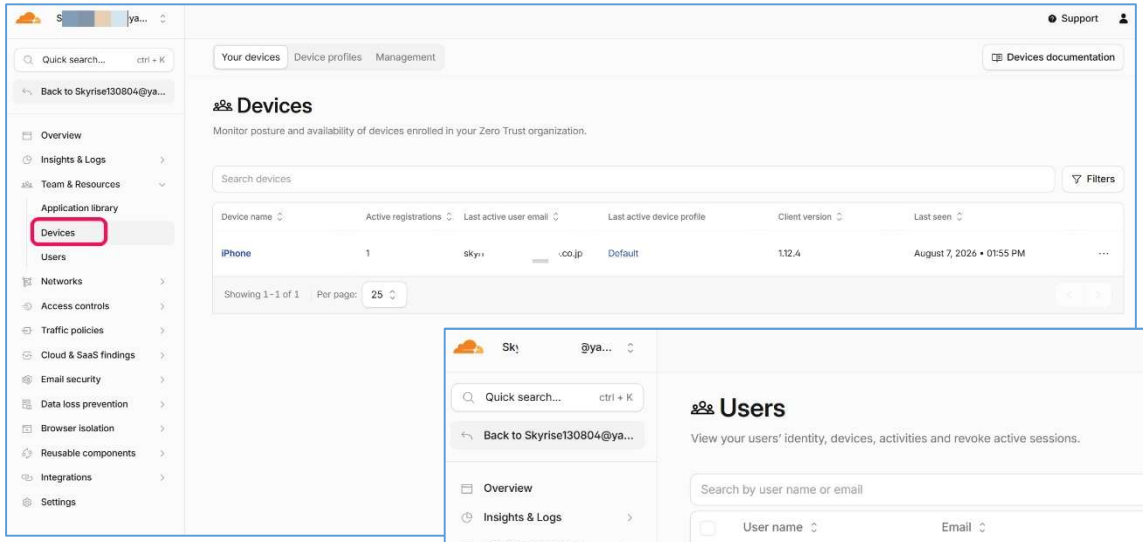


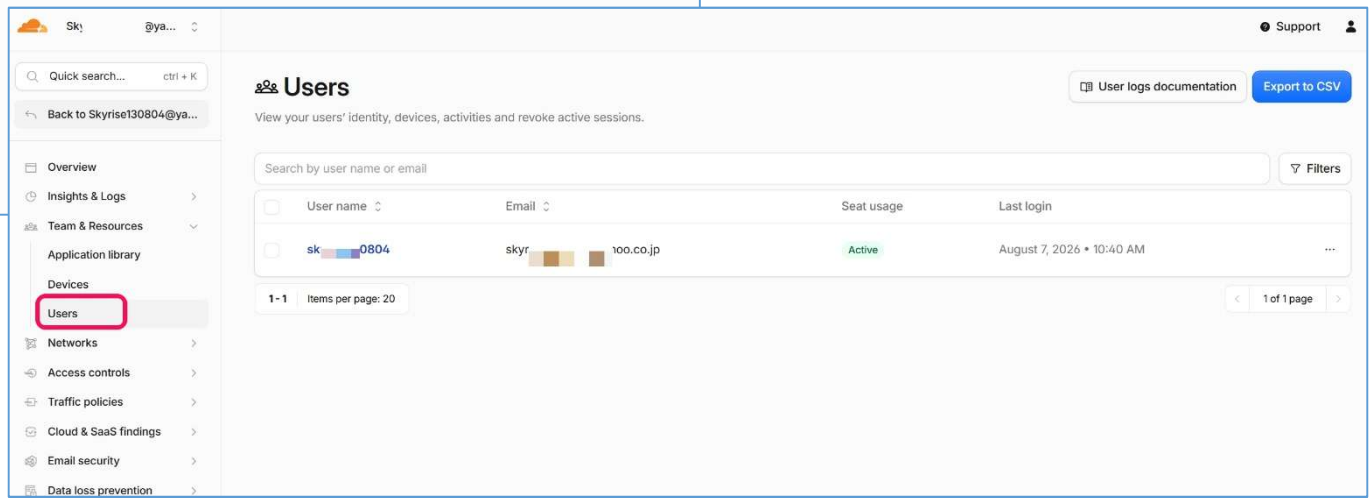


4.ゼロトラスト(ztna)管理

②. ダッシュボード　端末状況

- https://dash.cloudflare.com/login
- マイページからzero trustのdashboardへ
- Team & resource:デバイス、ユーザ

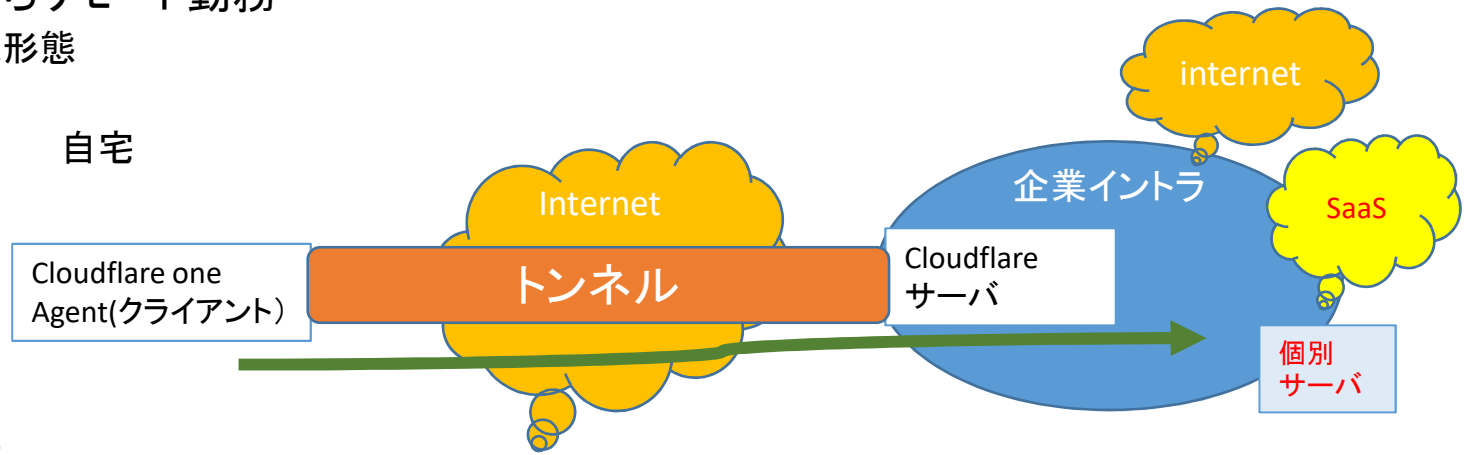




5.ゼロトラスト(ztna)利用例

①.自宅からリモート勤務

- 接続形態

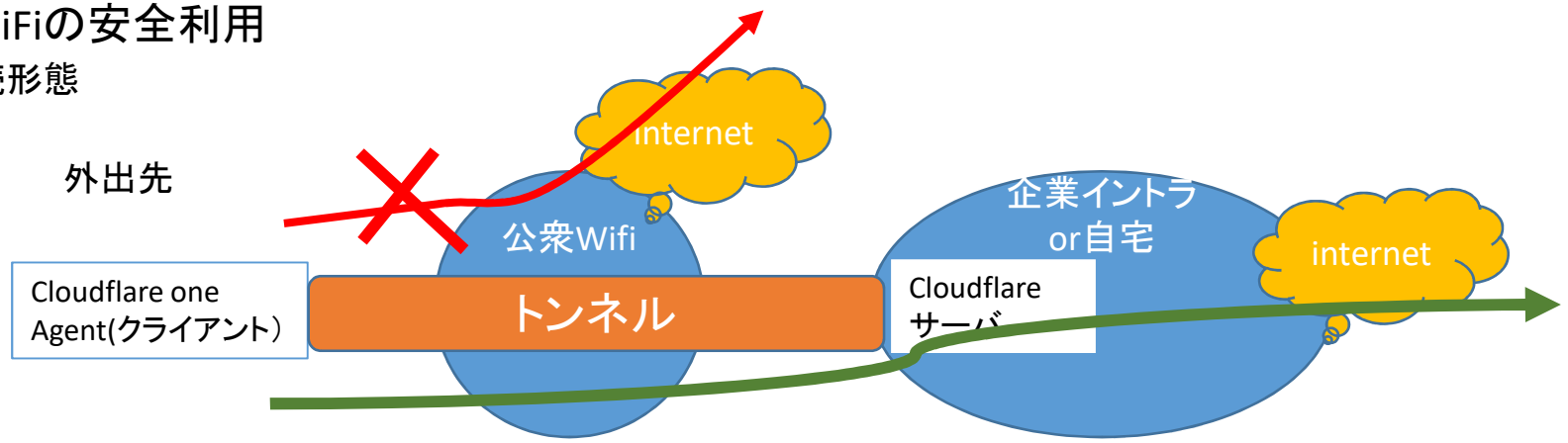


- 特徴
  - 自宅からリモートアクセスも安全に利用、社内システムにも安全にアクセス
  - 各ユーザからは、どのシステムにアクセスできるかポリシーを設定できる。詳細はこちら参照
  - VPNに比較して安全にアクセス（vpnルータ等の脆弱性がない）

5.ゼロトラスト(ztna)利用例

②.公衆WiFiの安全利用

- 接続形態



- 特徴
  - 公衆WiFiも安全に利用、インターネットも安全利用（第三者による盗聴などがない）

Spectrum Technology

ネットワーク監視ツール

1.ネットワーク監視ツール　概要

①. Zeek概要

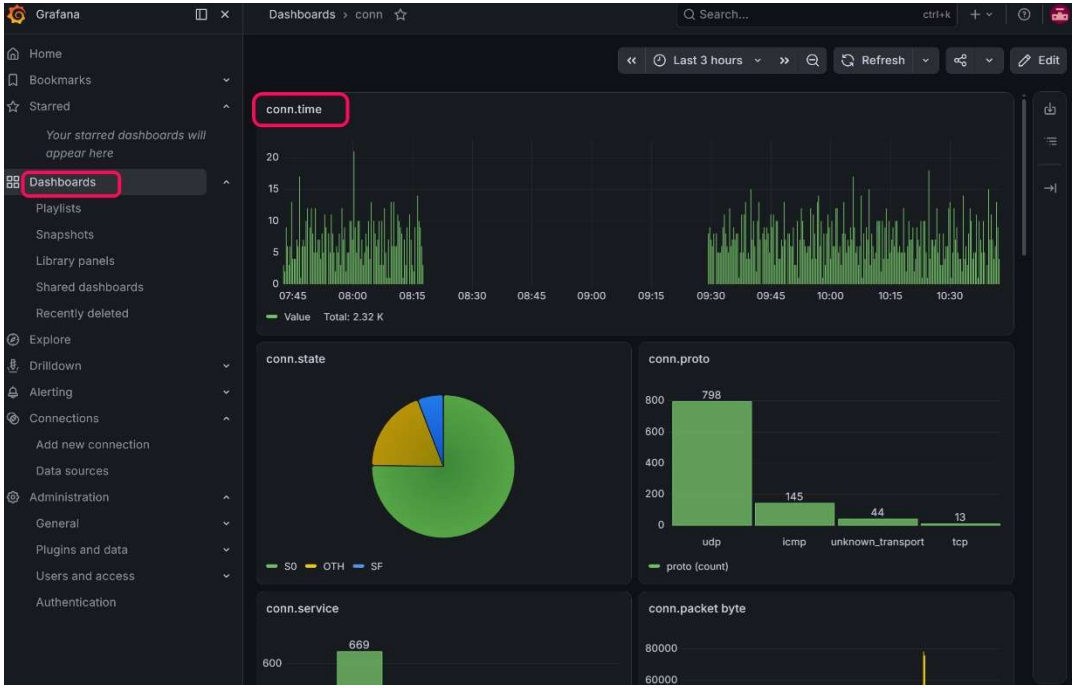
- https://zeek.org/
- https://docs.zeek.org/en/current/install.html
- オープンソースの強力なネットワークセキュリティ監視（NSM: Network Security Monitoring）フレームワークおよびパケット解析ツールです。全トラヒックを記録し、監視します。Zeekは端末の不正侵入などは検知しません。怪しい通信がされていないかを監視します。
- なお、MSのdefenderは主に、端末に対する不正侵入などを検知します。
- 今回は、zeekからの情報をもとに、以下の手順で表示します。
- Zeek → alloy(収集）→ Loki（保存）→ Grafana（表示）

Spectrum Technology

2.ネットワーク監視ツール　設定

④. grafana

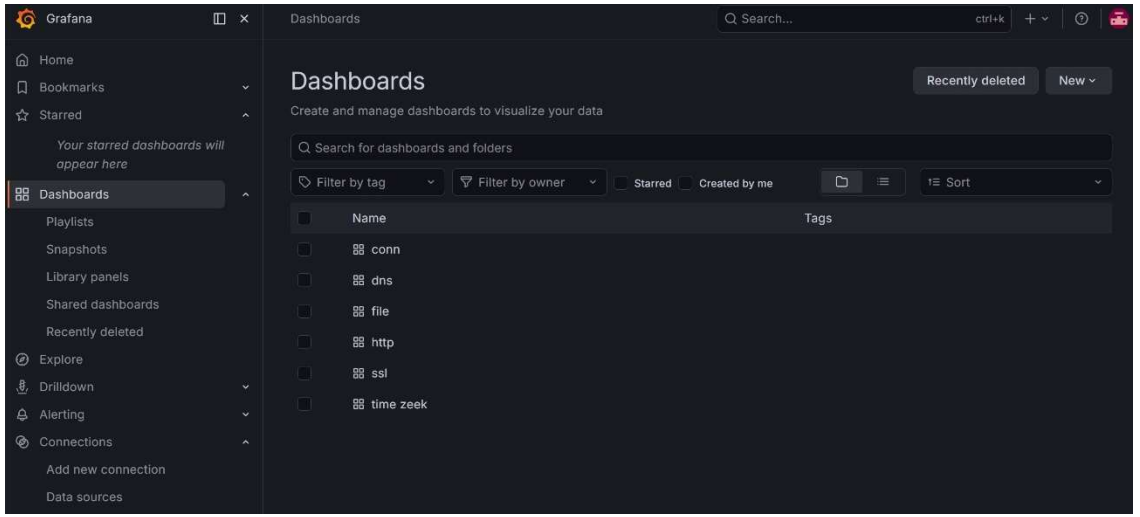
- https://grafana.com/ja/
- https://grafana.com/docs/grafana/latest/visualizations/dashboards/use-dashboards/
- 設定
- 起動
- 各種設定
- 表示
  - Dashboards>conn.time:表示されればok, refreshすると現在時間



3.ネットワーク監視ツール　利用例

①. Grafana全体

- https://grafana.com/docs/grafana/latest/fundamentals/dashboards-overview/
- 表示Dashboards:既に弊社で準備したもの。カスタマイズも可能
  - Conn：conn.logをグラフ化：トラヒック時系列、サービス、ポート、ip addr,table,weird
  - Dns:dns.logをグラフ化：dns query, record
  - File:file.logをグラフ化：file sourceなど
  - http：http.logをグラフ化：http status,ip addr
  - Ssl:ssl.logをグラフ化：server,version,target
  - Time zeek:時間別トラヒック
- Connをモニタすればok

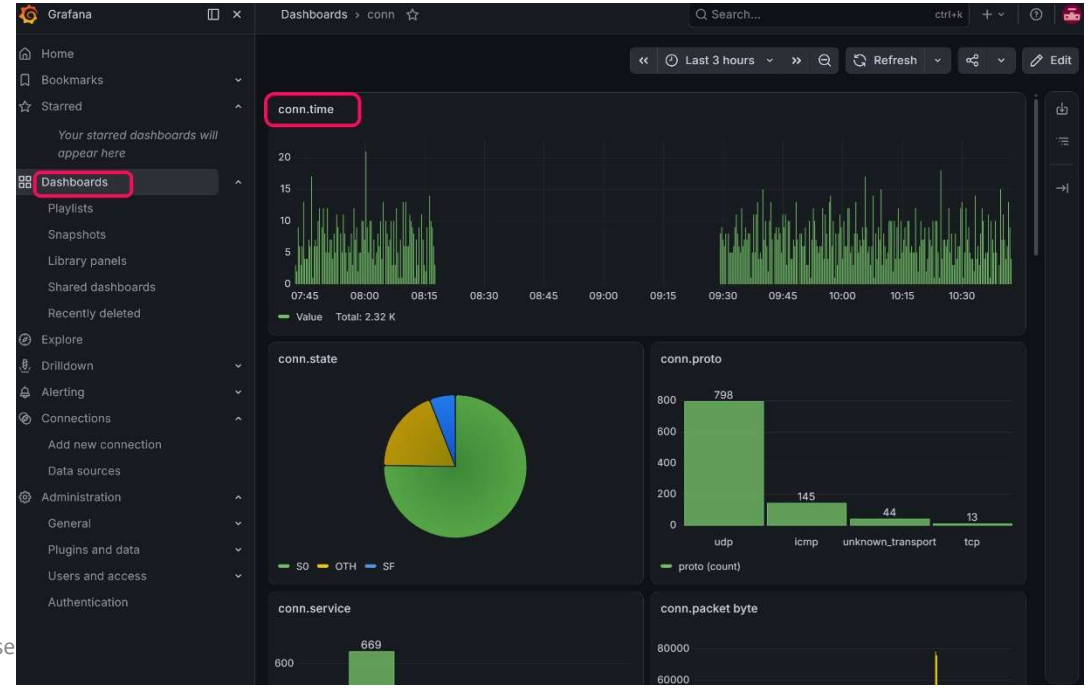


Spectrum Technology

3.ネットワーク監視ツール　利用例

②. Grafana conn

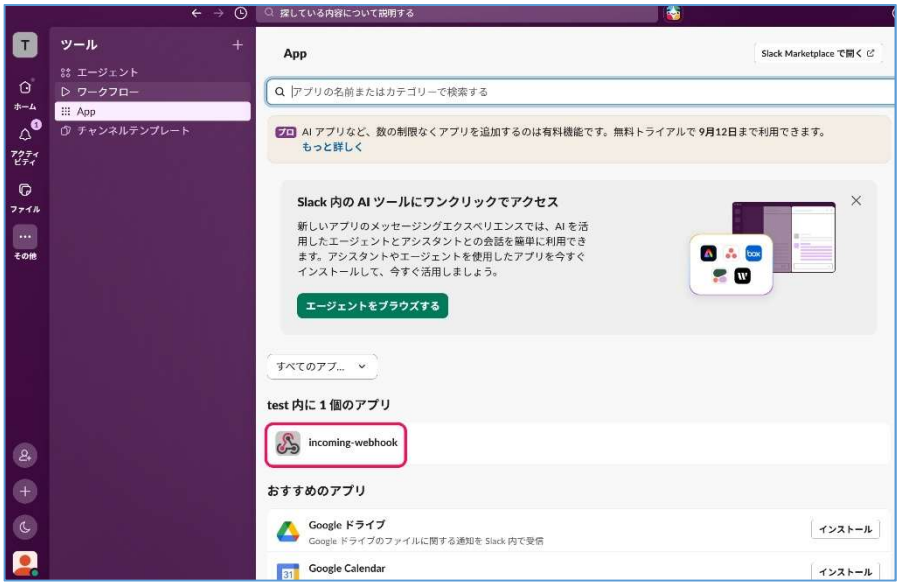
- https://grafana.com/docs/grafana/latest/fundamentals/dashboards-overview/
- 表示Dashboards:既に弊社で準備したもの。カスタマイズも可能
  - Conn：conn.logをグラフ化：トラヒック時系列、サービス、ポート、ip addr,table,weird
  - Dns:dns.logをグラフ化：dns query, record
  - File:file.logをグラフ化：file sourceなど
  - http：http.logをグラフ化：http status,ip addr
  - Ssl:ssl.logをグラフ化：server,version,target
  - Time zeek:時間別トラヒック
- Connをモニタすればok

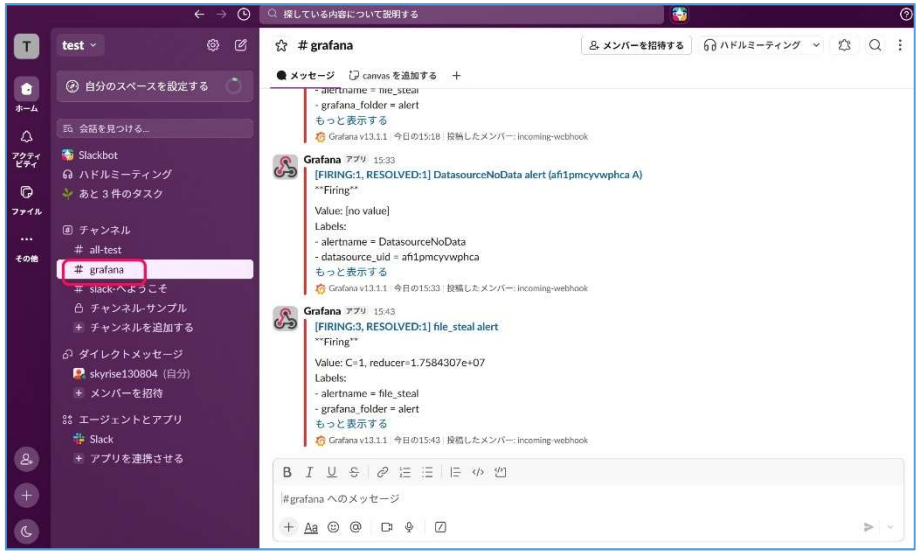


4.ネットワーク監視ツール 警報

①. Contact points

- https://grafana.com/docs/grafana/latest/alerting/configure-notifications/manage-contact-points/
- 警報の通知用の連絡先設定
- 設定
  - Aws sns, slack, emailなどたくさんあります。今回は一番簡単なslack
  - Slack:アカウント作成、チャンネルは#grafana
  - アプリ連携：incoming-webhook選択し、webhook urlをコピペ



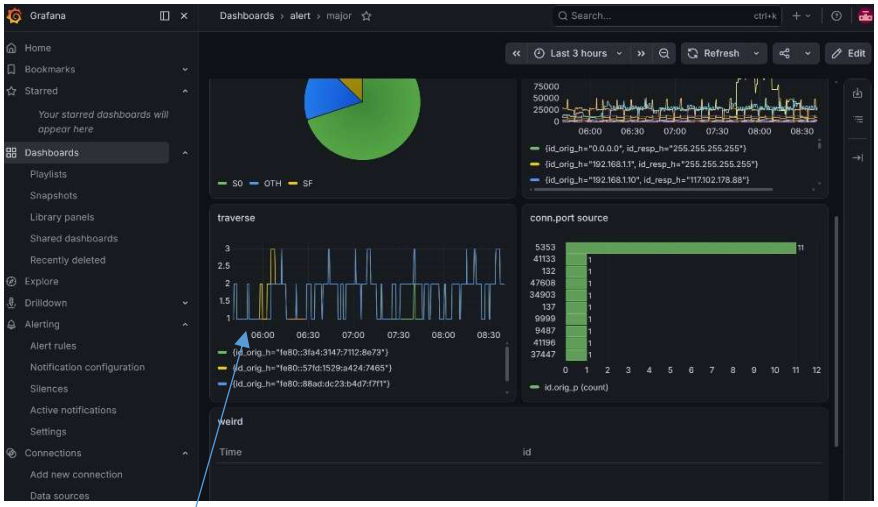


4.ネットワーク監視ツール 警報

②. Alert：traverse

- https://grafana.com/docs/grafana/latest/alerting/fundamentals/
- 設定
  - 例として以下を設定

  ①(ポートスキャン検知) :port scan
  ②(大容量アウトバウンド) :file steal
  ③（異常パケット）:weird
  ④（横移動）:traverse



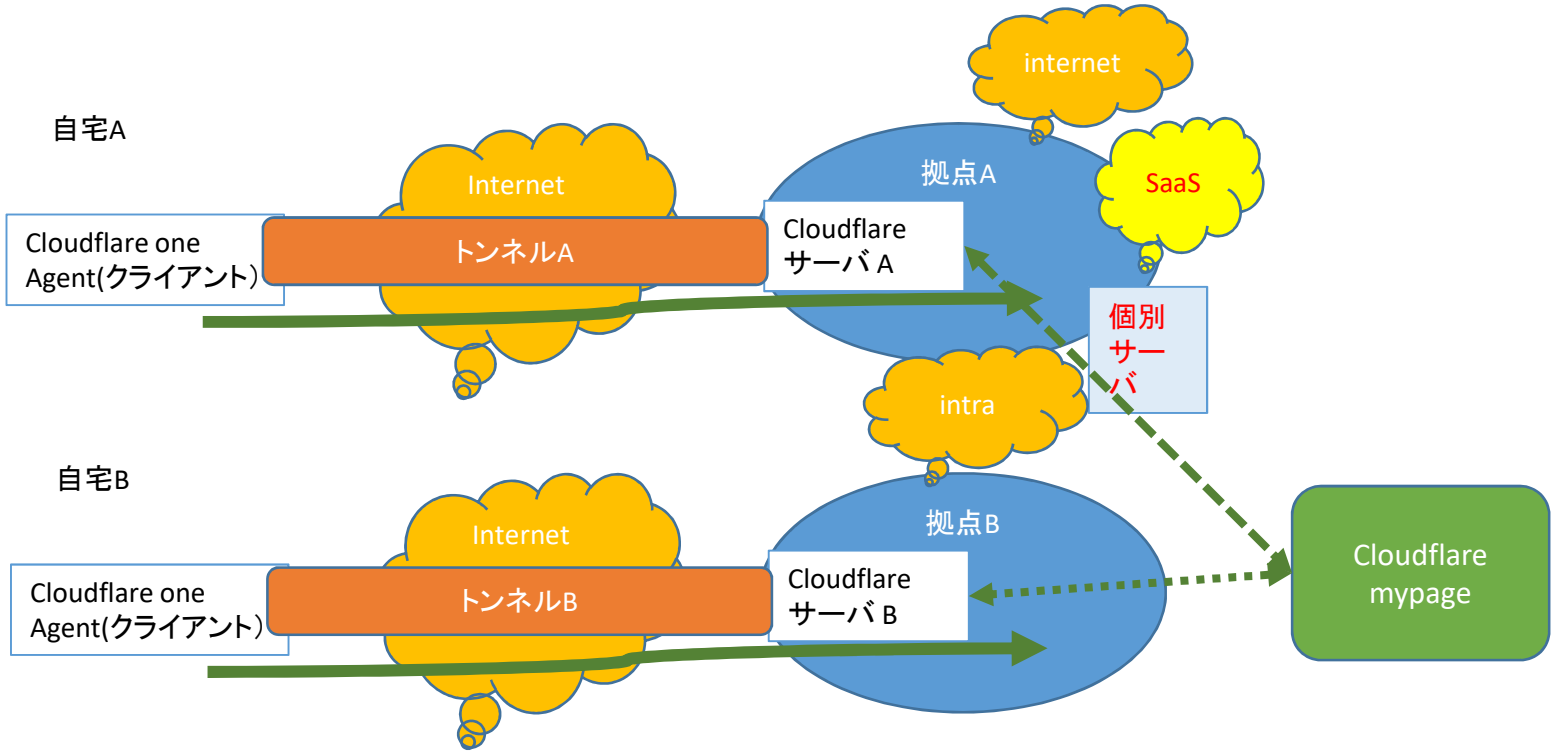
- Traverse
  - count by (id_orig_h) (count_over_time({filename=~".*conn.log"} | json | id_resp_p=~"445|3389|5985|5986|135|22" [10m]))
  - パソコンに不正侵入時に、SMB(ファイル共有/管理共有)、RDP(リモートデスクトップ)、WinRM(PowerShell Remoting)などにより、横移動するパケットを検出
  - Dashboard>alert>majorにtraverse,portを表示

拡張

1. 本導入キットの拡張

①. ゼロトラスト・ネットワーク：複数拠点

- 複数拠点にztnaを導入することが可能です。
- cloudflare側は1か所のmypageで複数拠点の管理できます。



Spectrum Technology

1. 本導入キットの拡張

②. ネットワーク監視：複数拠点

- 複数拠点にzeekを導入し、集約することが可能です。
- Grafana側は1か所で複数拠点からのデータを管理できます。

[拠点A: Pi5+Zeek+Alloy] ─┐
[拠点B: Pi5+Zeek+Alloy] ─┼─→ [中央のLoki/Grafana]　　集約先をlokiのlocalhostからurlへ
[拠点C: Pi5+Zeek+Alloy] ─┘

③. ハードウエアの性能向上

- 本キットは、raspberry pi5で構成しています。Ztnaで10端末、ネットワーク監視は、ひとつのセグメントで、100Mbps程度のトラヒックに対応しています。
- 複数拠点、収容端末数などにより、ハードウエアを更改し、性能向上を図れます。
- 拡張対応のOSは、ubuntuを想定しています。詳しくは問い合わせください。個別に対応します。