Spectrum Technology

大企業、中小企業のセキュリティ担当の方へ

ゼロトラスト・ネットワーク導入キット
提案書

～サイバー攻撃により事業停止とならないために～

背景：セキュリティの課題

「集中管理された業務基盤が、ひとたび攻撃を受けるとサプライチェーン全体を機能不全に陥らせる」

アサヒビールのサイバー攻撃からの教訓

2025年9月に発生したアサヒビールのサイバー攻撃により、出荷が停止し、復旧まで、半年程度を要し、事業に重大な影響を及ぼしました。詳しくはこちらを参照
その教訓を生かして、同様の事案が発生しないように、対策を講じましょう

主な原因と対策

- リモートアクセスVPNから侵入
- 内部横移動を許すネットワーク構造
- 管理者アカウントの奪取

廃止し、ゼロトラスト・ネットワーク導入
外部と内部用ネットワーク分離、EDR導入、監視強化
認証見直し

赤字が弊社提案

ご提案

EDRで端末を守り、ZTNAでアクセスを制御し、ネットワーク監視で攻撃者の動きを見つける。
なお、今回はEDRについては対象外とします。

注：EDR(Endpoint detection and response)、ZTNA（zero trust network access）

Spectrum Technology

ゼロトラスト・ネットワーク導入キット　全体像

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
- EDR（参考）
  - MS　defender設定、管理

詳細のハード、ソフト仕様は[こちら]

ZTNA系

CLOUDFLARE

ネットワーク監視系

zeek

Grafana

Grafana Alloy

Grafana loki

弊社提供

ST Spectrum Technology

特徴

ゼロトラスト対応

Cloudflareで、VPNの脆弱性を回避した安全なリモートアクセス環境を構築。

ネットワーク監視と自動アラート

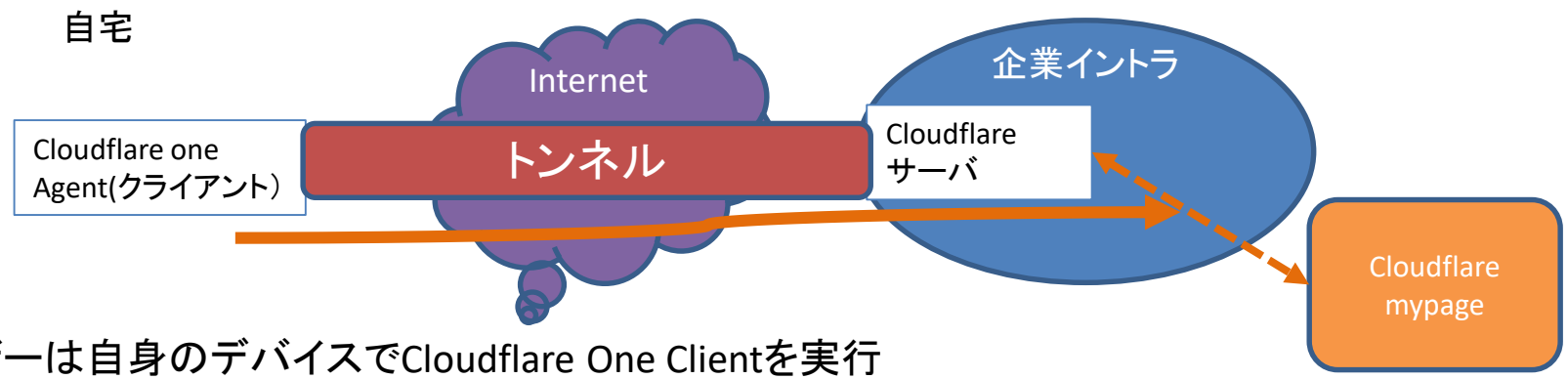
Zeekによるネットワーク監視で異常検知（横移動など）し、Slack等へ即座に通知。専任のセキュリティ担当者が不在でも状況を把握できます。

低コスト導入・拡張

高額な専用アプライアンス不要。Pi5を活用し、限られた予算でも強固なセキュリティ基盤を実現します。また複数拠点、ハードの性能向上などの拡張可能。

ゼロトラスト・ネットワーク：Cloudflare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
- 構成



- 仕組み

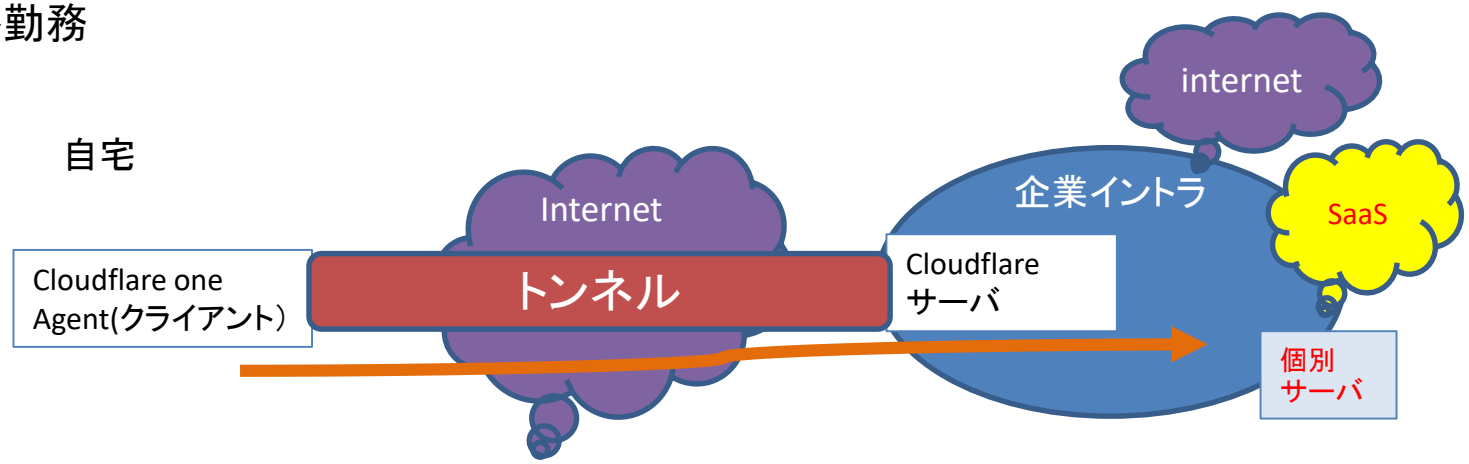
①ユーザーは自身のデバイスでCloudflare One Clientを実行

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。

ゼロトラスト・ネットワーク(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。
- 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）
- Cloudflareは50ユーザまでは無料で利用可能です。

ネットワーク監視ツール　概要

Zeek概要

- 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）

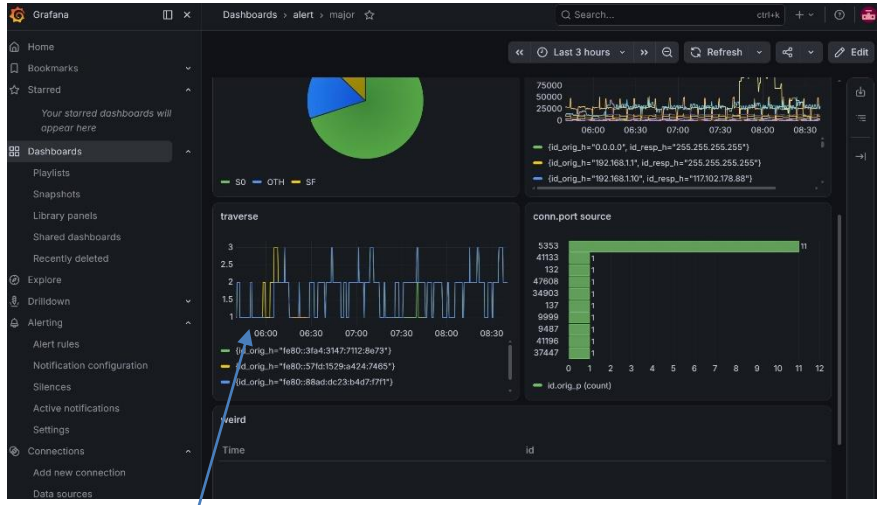
Spectrum Technology

ネットワーク監視ツール 警報例

横移動：traverse

- 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

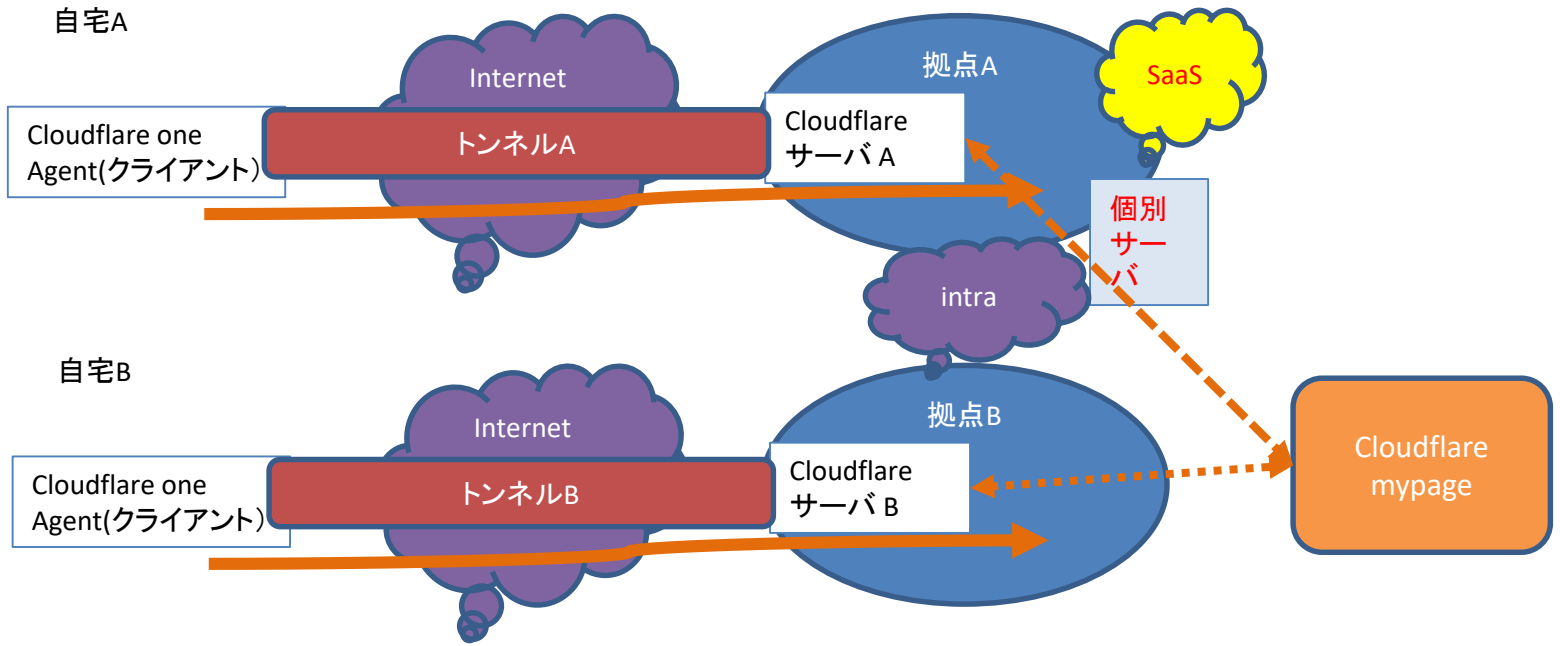
商品比較

項目	EDR単体	UTM/FW	SIEM：Security Information and Event Management	大手NDR	弊社ソリューション（ZTNA＋ネットワーク監視）
主な監視対象	PC・サーバ	通信制御	ログ	ネットワーク通信	アクセス＋ネットワーク通信
ランサムウェア対策	○	△	△	○	△
横移動検知	△	×	△	○	○
データ持ち出し検知	△	△	○	○	○
ゼロトラスト対応	×	△	×	△	◎
リモートアクセス保護	△	△	×	△	◎
通信可視化	×	△	○	◎	◎
専門知識	高い	中	高い	高い	低～中
初期費用	中	中	高	非常に高	低
月額費用	中	中	高	高	-
拡張性	○	○	○	○	△、ハードの性能向上など、準備
中小企業向け	△	○	×	×	◎

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。



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。

お勧めのお客様

- 中小企業のサイバー攻撃対策を実施したいお客様（特に、セキュリティ担当者がいないお客様）
- 大企業でゼロトラスト・ネットワーク、ネットワーク監視の導入を検討しているお客様（試験導入として最適）
- 個人のお客様で、自宅のVPNを更改したいお客様
- サイバー攻撃対策を検証、学習、開発などを行いたい企業、学校の方

安心して導入いただくために

- ゼロトラスト・ネットワーク:　充実したマニュアルで、簡単な設定で、１日で、ゼロトラスト・ネットワークを稼働させます。
- ネットワーク監視：grafanaのわかりやすい表示と、既に設定済の警報、グラフ表示で直ぐに利用
- 安心のサポート: 初心者でも安心の２週間の無料サポート、設定が不安なお客様には、オンサイトでの設定サービスも実施します。

利用するために必要なスキル
- ipネットワーク基礎知識
- linux基礎知識

お問い合わせ

ゼロトラスト・ネットワーク導入キット（Pi5版）について、詳細はお気軽にお問い合わせください。

スペクトラム・テクノロジー株式会社
担当：村上
https://spectrum-tech.co.jp
sales1@spectrum-tech.co.jp

参考

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

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
EDR	Microsoft defender	For business	参考

ST Spectrum Technology

中小企業のみなさまへ

アサヒビールのサイバー攻撃からの教訓

課題
- サプライチェーンが狙われる
  - セキュリティが手薄な中小企業がターゲット
- 利用中のVPNが危ない
  - 多くの企業で使っているリモートアクセスVPNは、たくさんの脆弱性
- 専任者がいない

解決策
- ネットワーク監視
  - 侵入されても、横移動を検知、通知
- ゼロトラスト・ネットワーク(ZTNA)導入
  - VPNに代わるcloudflare
- 専任者がいなくても安心通知
  - Slackなどに警報通知

オンサイト・インストールサービスも提供

ゼロトラスト・ネットワーク導入キット
（all in one, 安価、拡張可能）

PCへの侵入検知などのEDRはMS defenderで参考に記載

詳しくは
スペクトラム・テクノロジー株式会社
担当：村上
https://spectrum-tech.co.jp
sales1@spectrum-tech.co.jp