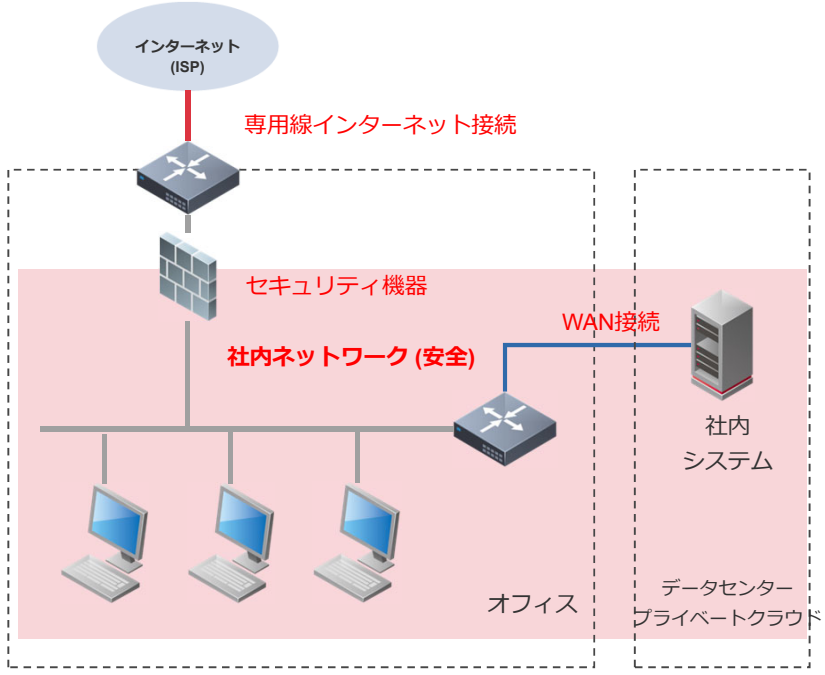
新リモートアクセスサービス説明会

法人(オフィス)インターネット利用の変化

株式会社インターネットイニシアティブ
ネットワーク本部 ネットワークサービス部 インターネット接続サービス課長　原 孝至

2019年頃までの企業の典型的なインターネット利用

- オフィスに集まって勤務
- 「社内ネットワーク」という概念
- セキュリティ境界による防御



近年見られる企業のインターネット利用の変化

DX進展・デジタルワークプレースの普及

- Microsoft 365・Google Workspaceなどパブリッククラウドの利用が急増

→ WAN(社内網)ではなく、パブリッククラウド向けのトラフィックが急増

働き方の多様化・リモートワークの一般化

- 自宅インターネットなど、会社の統制下にないネットワークによる業務が急増

→パブリッククラウドの利用を含めた監査・統制の必要性

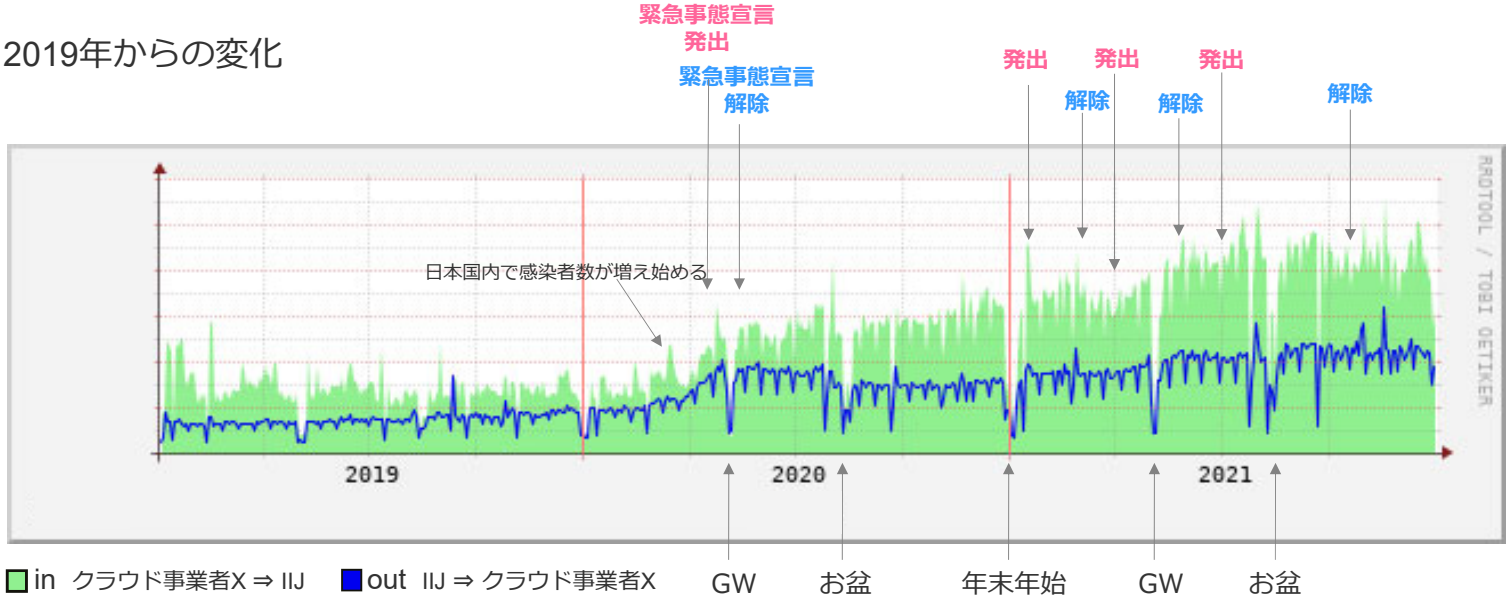
これらの変化はコロナ禍に後押しされた側面もあるが、コロナ禍だけが要因ではない

一過性ではない、継続的な企業活動の変化であり、多くの企業に広がっていくもの

クラウド事業者へのトラフィック増加は止まらない

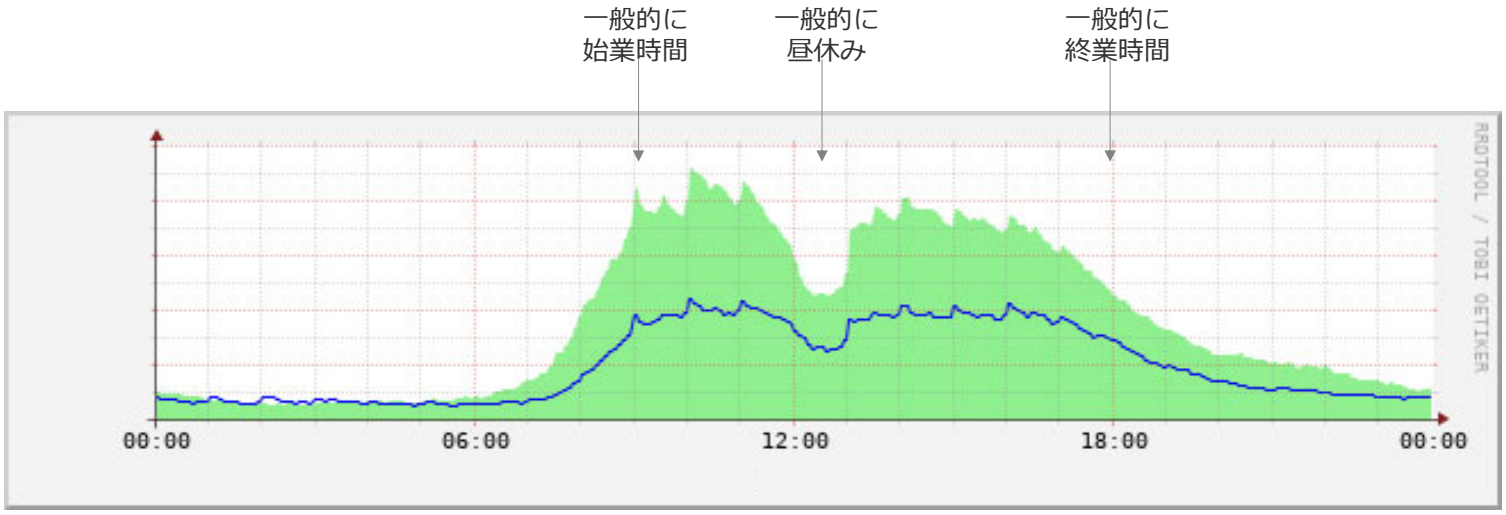
～クラウド事業者XとIIJ間のトラフィック例～

■ 2019年からの変化



- **あるクラウド事業者との接続を見ても2019年→2021年で2倍以上の伸び**
- **複数社のクラウドサービスをご利用であればさらに総量が増加しているのは間違いないと思われる**

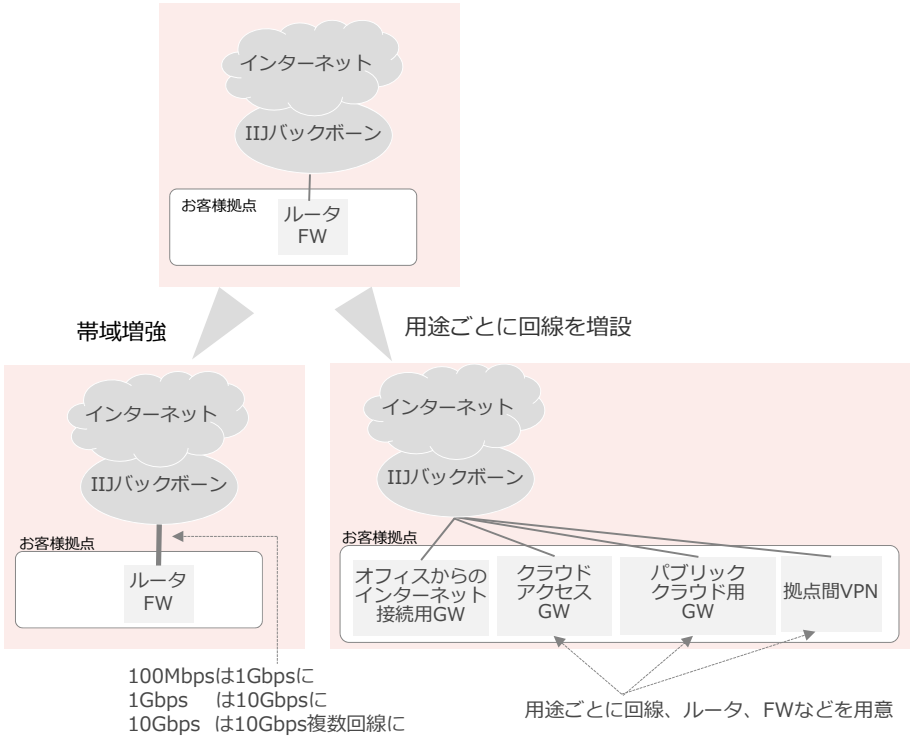
■ ある平日のトラフィック



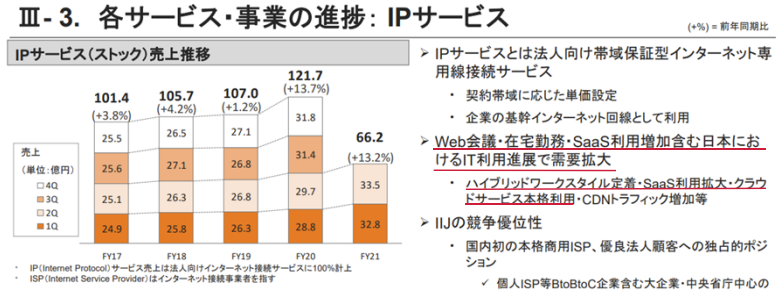
- **平日日中帯は法人のお客様の利用に連動してトラフィックが増減**
- **明らかにビジネス向けに特化して利用が増加**

トラフィック増加に伴う、お客様の設備投資の増加

- インターネット接続設備の増強



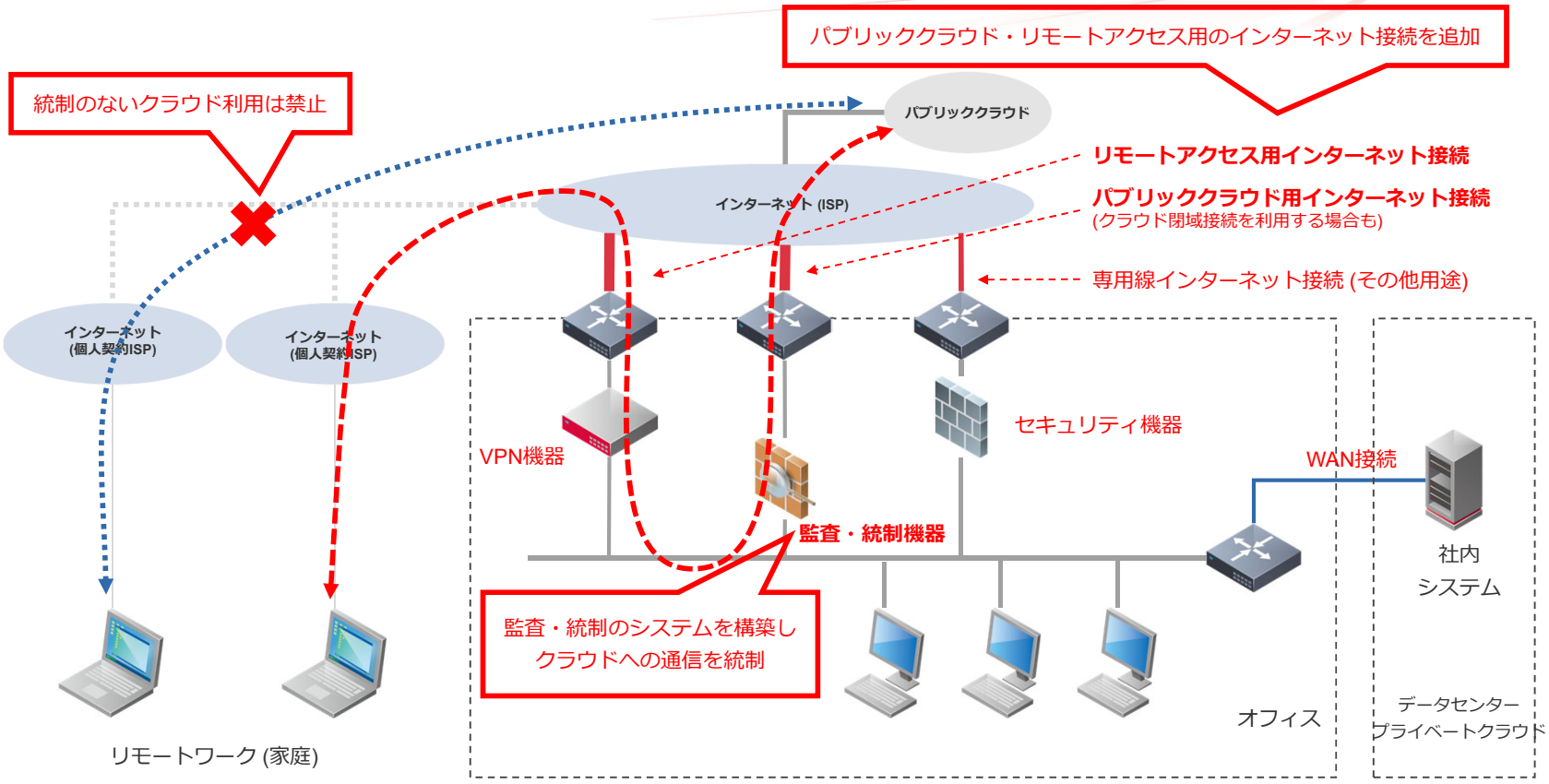
- IIJ業績



2022年3月期 上半期（1H21）連結業績説明資料
https://www.iij.ad.jp/ir/library/financial/pdf/IIJ2Q21J_presentation.pdf

- パブリッククラウド利用の増加により、インターネット接続回線の設備投資増加
  - お客様ごとに多様な方法で増強を実施
- 2020,2021年と継続しており、今後も継続する可能性は考えられる

先進的大企業でのインターネット利用の事例



リモートワーク・パブリッククラウドの利用は当然だが、統制のない利用は認められない（ゼロトラストへのシフト加速）

- 監査・統制のためのシステムを構築
- 自社ネットワーク内に通信の集約ポイントを設置

こういった大規模・高度なネットワークは大企業だからこそ実施できるもの。

中堅企業～準大企業には負担が大きく、自社での導入は困難。

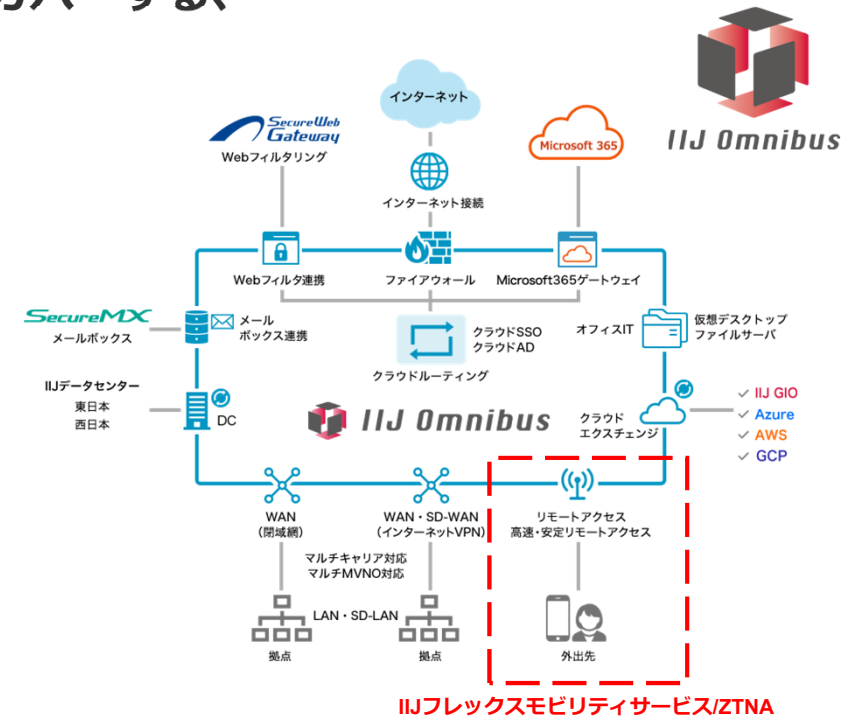
IIJ Omnibus

IIJ Omnibusが実現するネットワーククラウドであれば
高度なネットワークをアウトソーシングで実現可能。

IIJ Omnibusは企業ネットワーク全体をカバーする、ネットワーククラウドのブランド

■ IIJフレックスモビリティサービス/ZTNA

IIJ Omnibusを構成するサービスの中で
ゼロトラストネットワークの機能を追加した
リモートアクセスサービス。



ゼロトラストを実現する
新たなフレックスモビリティサービス

株式会社インターネットイニシアティブ
ネットワーク本部 副本部長　吉川 義弘

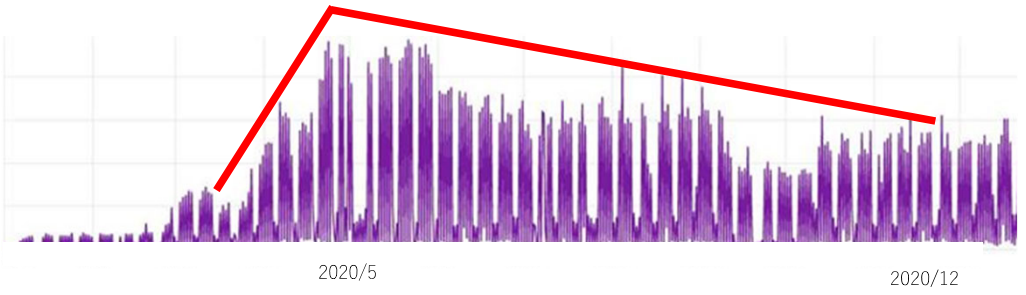
本日お話する内容

リモートワークで顕在化する課題とゼロトラスト

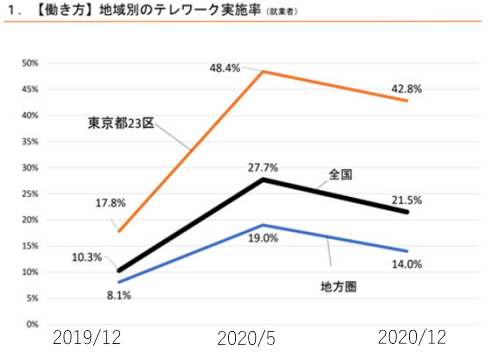
新たなフレックスモビリティサービスで提供するものとは

リモートワークで顕在化する課題

2020年のフレックスモビリティ帯域推移



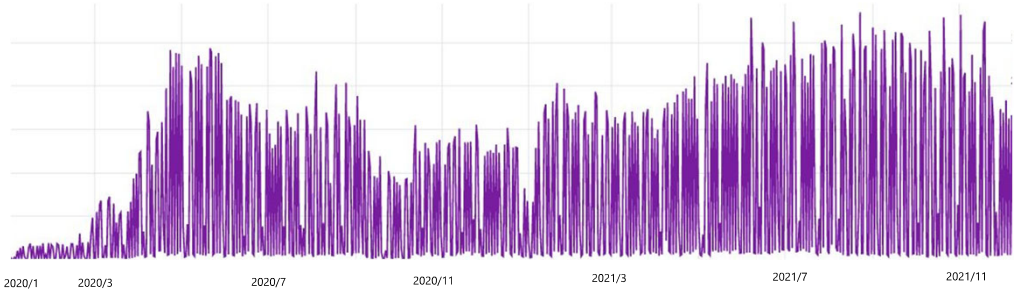
2020年のIIJフレックスモビリティサービスの帯域推移



内閣府HPより
新型コロナウイルス感染症の影響下における生活意識・行動の変化に関する調査
(https://www5.cao.go.jp/keizai2/keizai-syakai/future2/20210119/shiryou3-1.pdf)

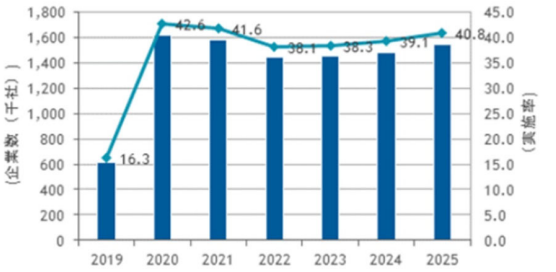
リモートワークの実施とフレックスモビリティ帯域は同様の推移

2020年～2021年の
フレックスモビリティサービス帯域推移(～2021/12)



緊急事態宣言終了後のVPNトラフィックは
ゆるやかな減少傾向ではあるが、コロナ前には戻っていない

国内テレワーク市場 テレワーク 導入企業数予測、2019年～2025年



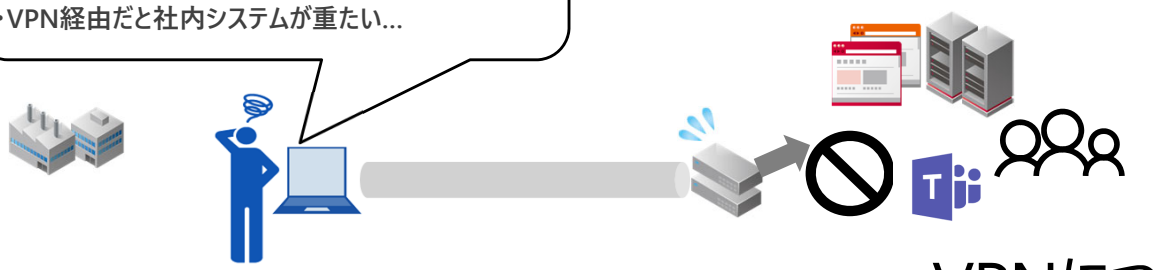
2019から2025年までの国内テレワーク市場 テレワーク導入企業数予測
（出典：IDCの調査資料）

ワークスタイルの変革が進み、
今後もリモートワークを活用した働き方は続く可能性

フレックスモビリティが解決している課題とは

リモートワーク下でのネットワークの課題は何か?

・VPNが切れてしまう…
・VPN経由だと仮想デスクトップがうまく動かない…
・VPNでビデオ会議できない…
・VPN経由だと社内システムが重たい…



ネットワークが遅い

すぐ切れる

VPNにつながらない

リモートワークだと結局仕事にならない・・・

やはり出社しないとだめ・・・

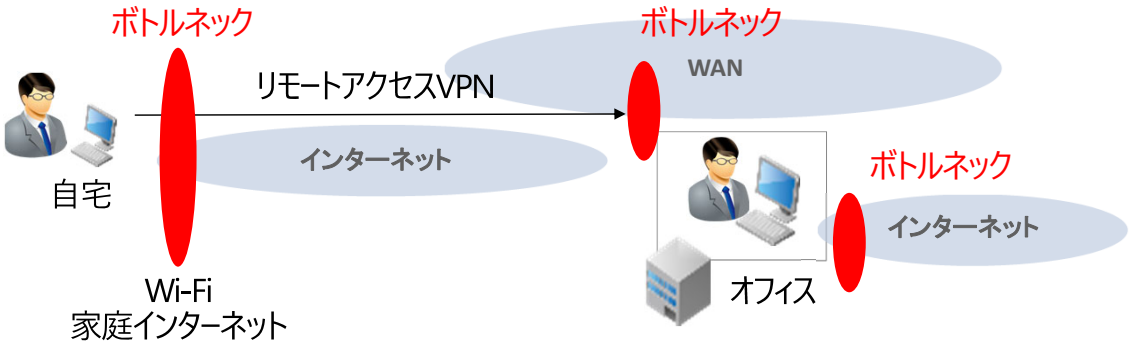
遅い・つながらない主な原因

家庭のWi-Fi環境

家庭のインターネット回線品質

リモートアクセス用VPNサーバやWAN回線

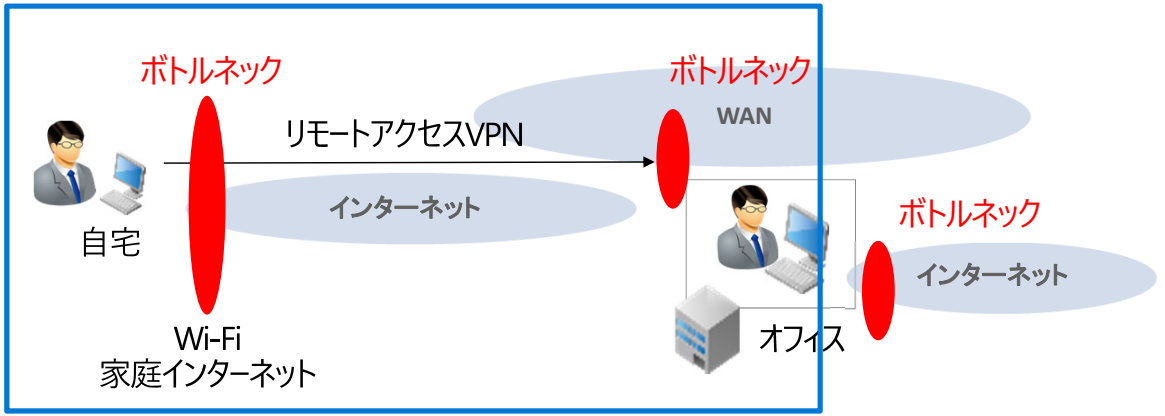
どこがボトルネック?



Microsoft 365
Office 365

様々な箇所にボトルネックが出る

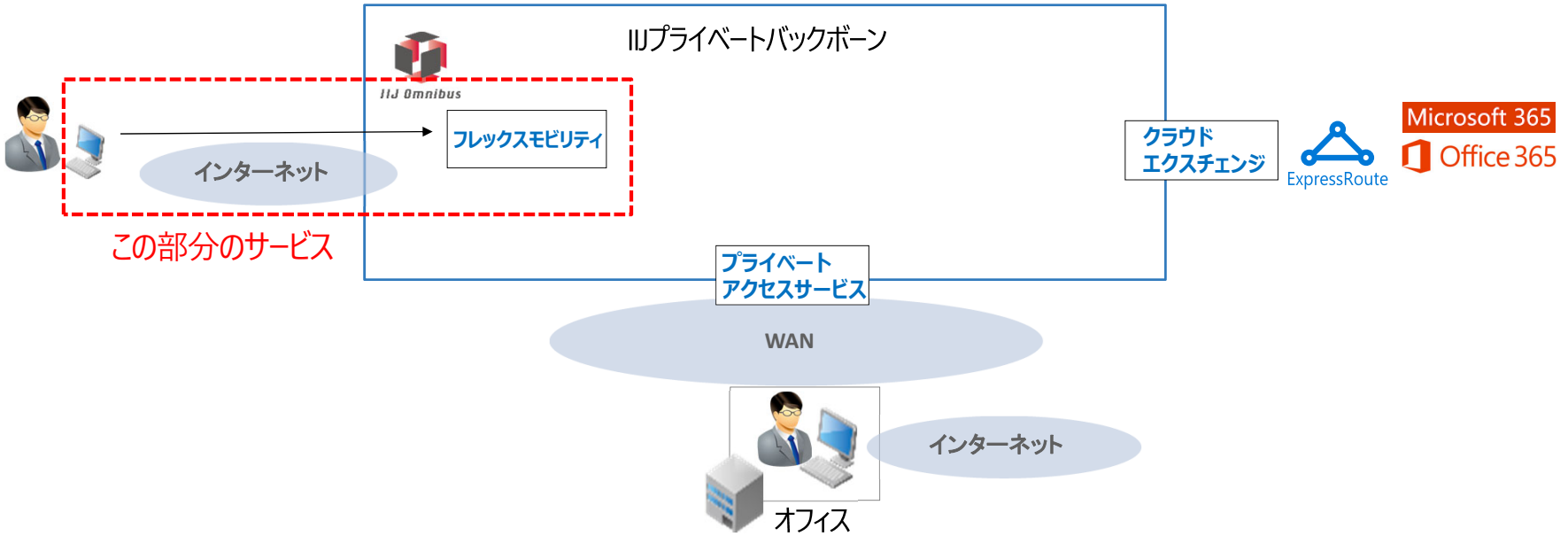
フレックスモビリティが解決するのは



この部分のボトルネック

Microsoft 365
Office 365

クラウド型VPNサービス



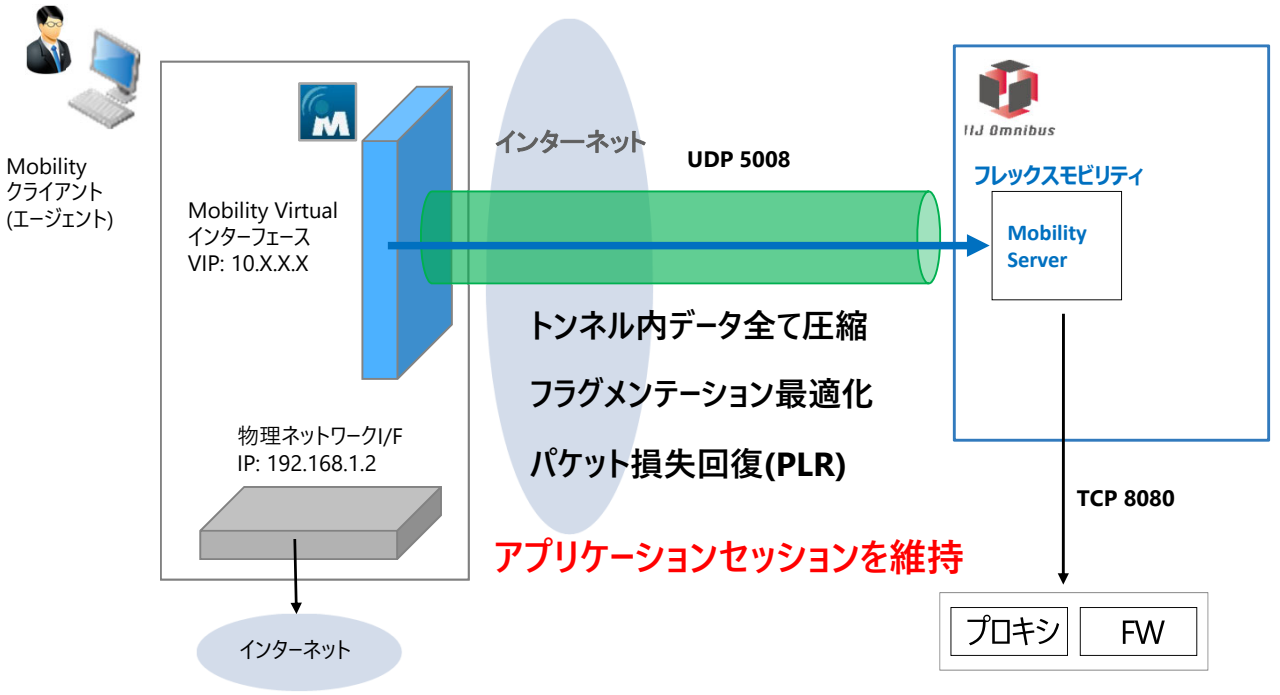
VPN+ネットワークをサービス提供

フレックスモビリティサービス

NetMotion Mobility®をエンジンとして使った

ネットワーク型の高速で切れないVPNサービス

VPNトンネル区間を高速化・フロー制御によるセッション維持



リモートワークでよくあるシーン

社内のファイルサーバにVPN
接続してPPT資料編集

ファイルの保存
そのままPC閉じる(スリープ・ロック)

PC開いて続きから編集再開

VPNを意識しなくなる

リモートワークで浮き彫りとなった新たな課題

リモートワークのセキュリティは大丈夫?

どこからつないでる?

公衆Wi-Fiではない?

接続するPCは大丈夫?

情報漏洩のリスクは?

アクセス状況が見えない・・

リモートワークへの移行に不安が・・

実際にお聞きした話

リモートワーク時のセキュリティが不安

社員のデスクトップPCを自宅に送付してリモートワーク

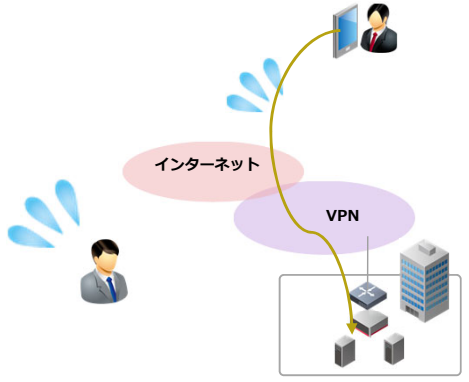
会社PCを郵送

リモートワークでネットワーク帯域が不足?

何か遅いというクレームが増えたが・・

急に帯域不足になった?

理由が分からない・・



どこを増速すればよい?

利用状況が見えない・・・

何を対処すればよいのか分からない・・

つながらないという問い合わせ

つながらないと言われるが、家のWi-Fi環境の問題では?

自宅のインターネット回線まではさすがに分からない・・

ユーザの環境が分からない・・・

トラブルシューティングが出来ない・・

リモートワークで今後顕在化する課題とは?

セキュリティ部門
情シス部門

セキュリティ

情シス部門

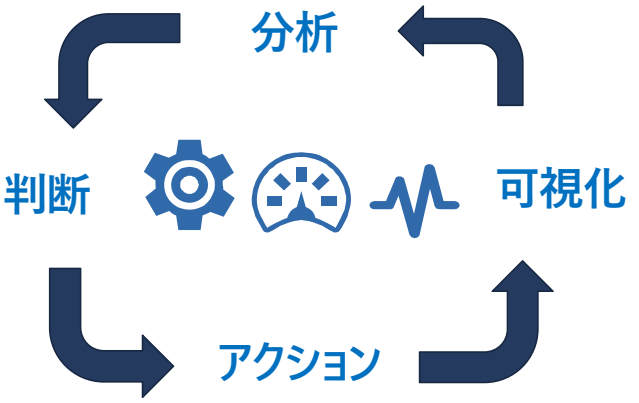
ネットワークのボトルネック

従業員
情シス部門

トラブルシュート

解決への方向性は?

通信の状況、セキュリティ状況を正しく把握して対処

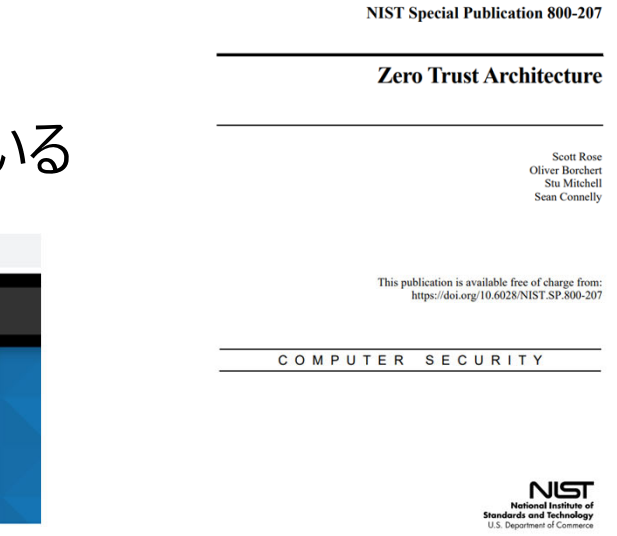


可視化<->アクションのサイクルを回す

ゼロトラスト
セキュリティ課題に対するアプローチ

ゼロトラストアーキテクチャとは

アメリカ国立標準技術研究所（NIST）
が発行する「SP800-207」で
「Zero Trust Architecture」が提唱されている


NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

csrc.nist.gov/publications/sp800

NIST

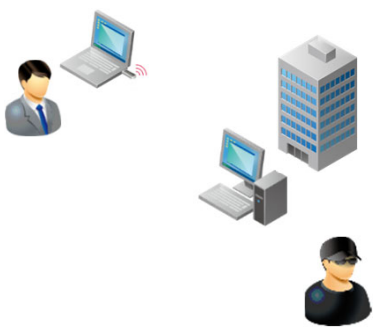
Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

SP	800-207	**Zero Trust Architecture** Download: SP 800-207 (DOI); Local Download; ZTA project at NCCoE	Final	8/11/2020

ゼロトラストの背景

固定化しない利用形態



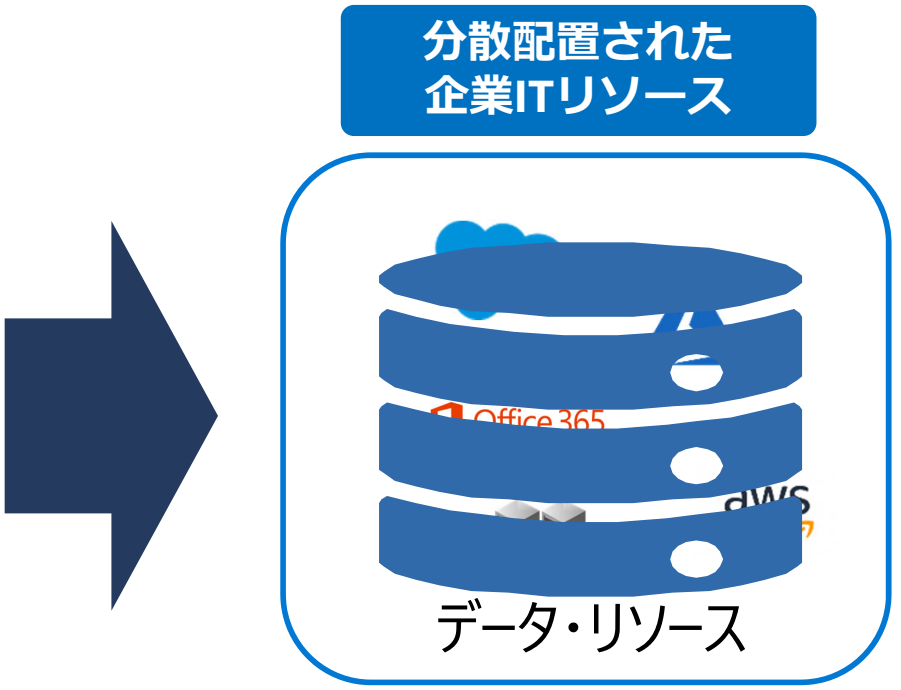
社内・自宅・移動先

分散配置された企業ITリソース

クラウド・オンプレミス

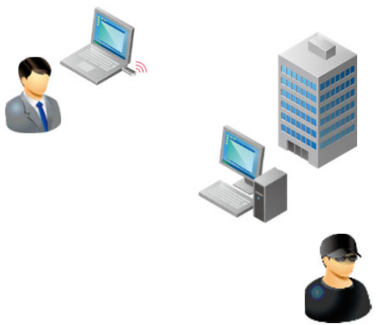
ゼロトラストの本質

どうやって守る?



ゼロトラストの本質

固定化しない利用形態



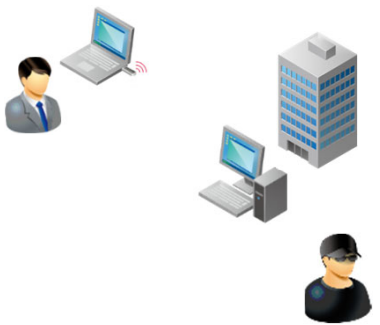
社内・自宅・移動先

アクセス元を
基本

「信用しない」

ゼロトラストの本質

固定化しない利用形態

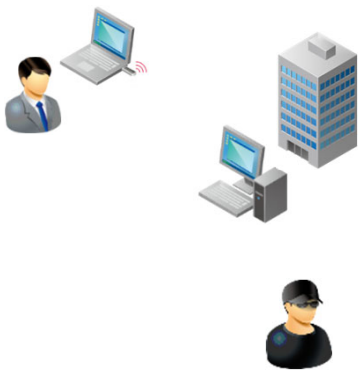


社内・自宅・移動先

都度 条件チェック

ゼロトラストの本質

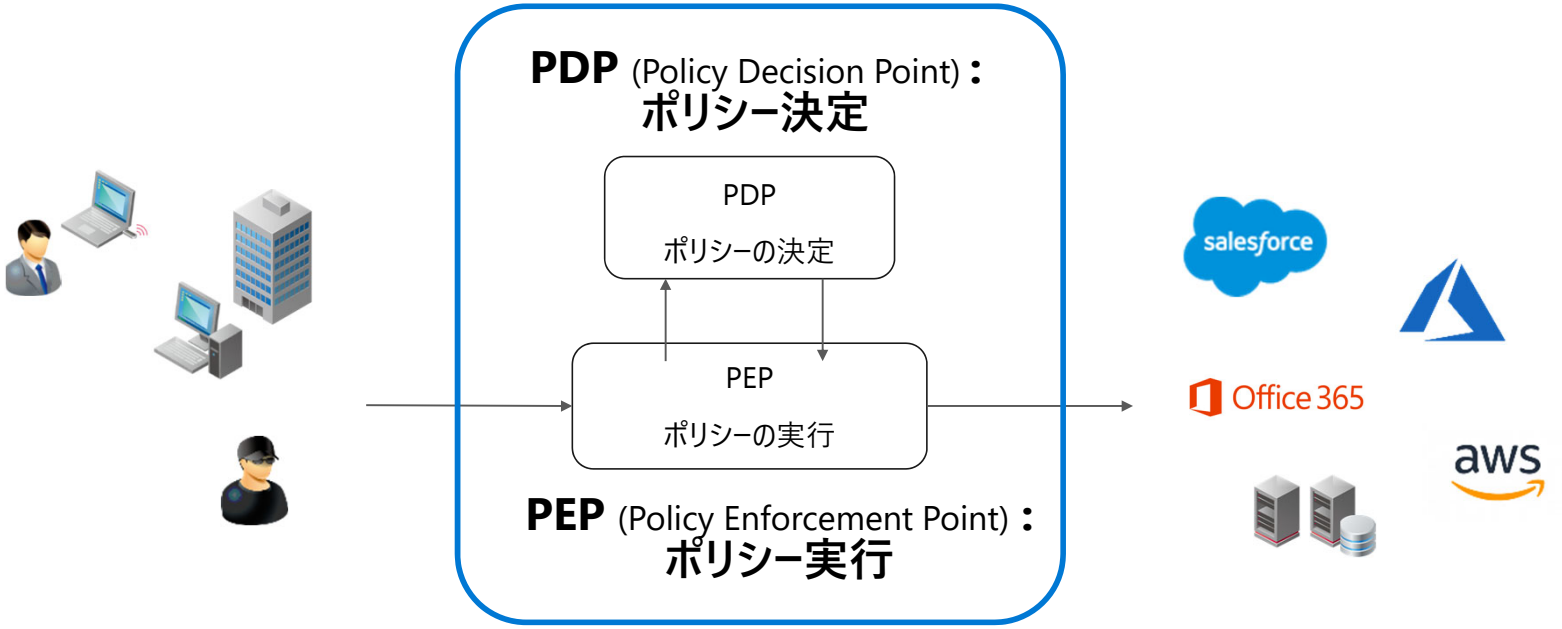
固定化しない利用形態



社内・自宅・移動先

合致すれば許可

そのために必要なこと



ポリシーの決定と実行は一カ所に集約

ゼロトラストの基本要件

ポイント) アクセス先リソースは「全て」を対象に

ポイント) ネットワーク的なロケーションを信用しない

ポイント) セッション毎に認可確認

ポイント) クライアントのコンテキストで動的に認可判断

認可ポリシーの決め方

ゼロトラストの基本要件

ポイント) デバイスはセキュアに維持

ポイント) 通信状況を常に情報収集してポリシーに反映

認可ポリシーの運用の仕方

➔ **収集した情報を基に見直し・改善**

SASE (Secure Access Service Edge)

ガートナーが提唱したコンセプト

ゼロトラストをベースにした実装要件

PDP/PEP の実装として ZTNA を定義

IIJフレックスモビリティサービス/ZTNA

IIJフレックスモビリティサービス/ZTNA

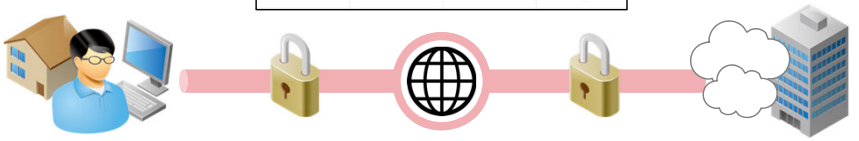
切れないVPN

柔軟なポリシー

切れないVPN
＋
ZTNA
ポリシー

通信 可視化

レピュテーション



ZTNA機能を強化した新たなフレックスモビリティサービス

フレックスモビリティサービス/ZTNA メニュー構成

2022/1/31リリース

Starter
スモールスタートプラン

シンプル・安価に利用
※FXCの後継

契約可能品目

・帯域：100Mbps
・デバイスライセンス：100～500lic

2022/1/31リリース

Core
Enterprise VPN + ZTNA

快適VPN+ZTNA
※FXMの後継

契約可能品目

・帯域：200Mbps～2Gbps
・デバイスライセンス：100～60,000lic

2022/3末リリース予定

Complete
Digital Experience Monitoring

モニタリング機能
※Core+可視化

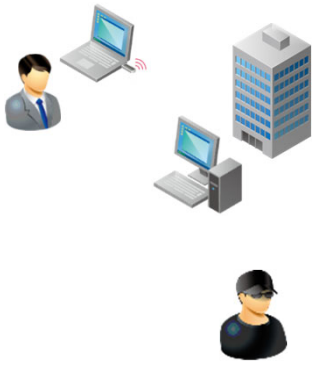
契約可能品目

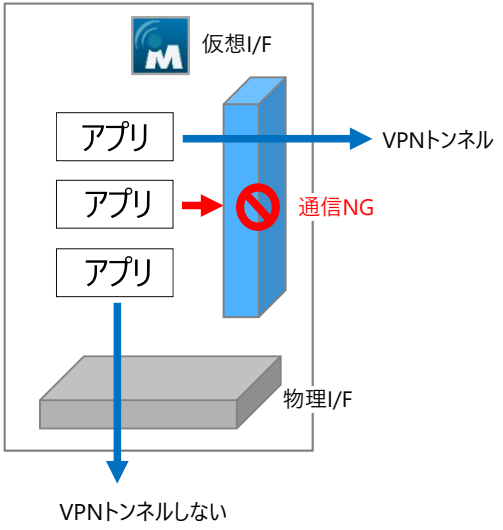
・帯域：200Mbps～2Gbps
・デバイスライセンス：100～60,000lic
・可視化ログ保管期間：90日 / 180日 / 360日

シームレスなメニュー変更が可能

フレックスモビリティサービス/ZTNA

ゼロトラストアーキテクチャにおけるPDP・PEP





Starter Core

様々なコンテキストでの柔軟なポリシー制御

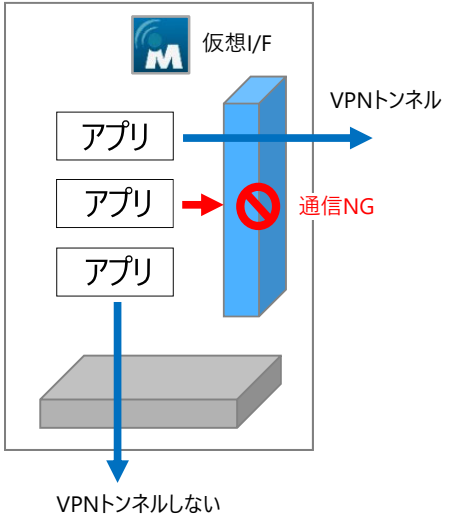
状態

・ポリシー
SSID /BSSID (場所)
時間
接続状況
バッテリ
ADグループ
・・・

・NAC
OSバージョン
Windows更新プログラム
アンチウイルス
・・・

×

アクション



×

対象 (人・デバイス)

デバイス上でリアルタイム実行

通信の可視化機能を提供

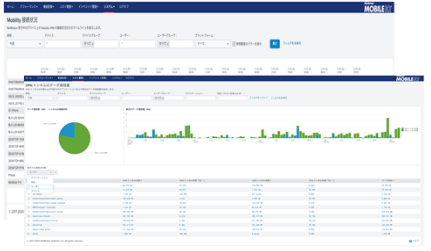
Complete

条件
- 場所
- 時間
- …

どの様な状態で
どの様な目的で

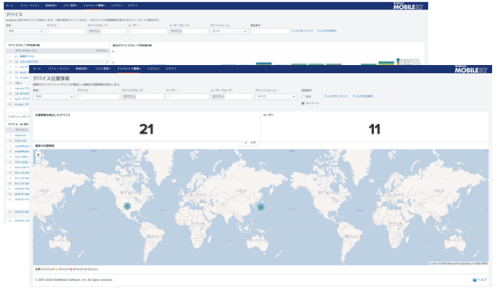
アクション
アプリ
アプリ
どの様な操作を

対象
(人・デバイス)
誰が



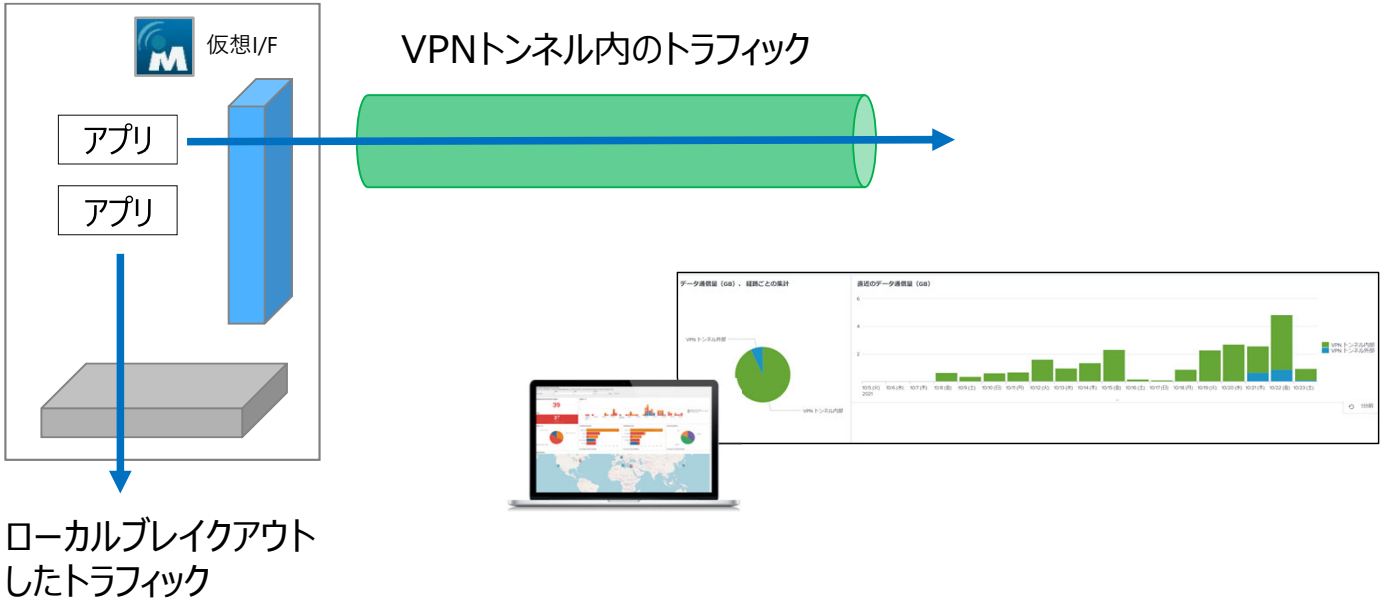
制御

可視化



可視化と制御のサイクルを回す

トンネル外のトラフィックも可視化



デバイスのトラフィックを全て可視化・制御

新たなフレックスモビリティで提供する可視化⇔制御の実例

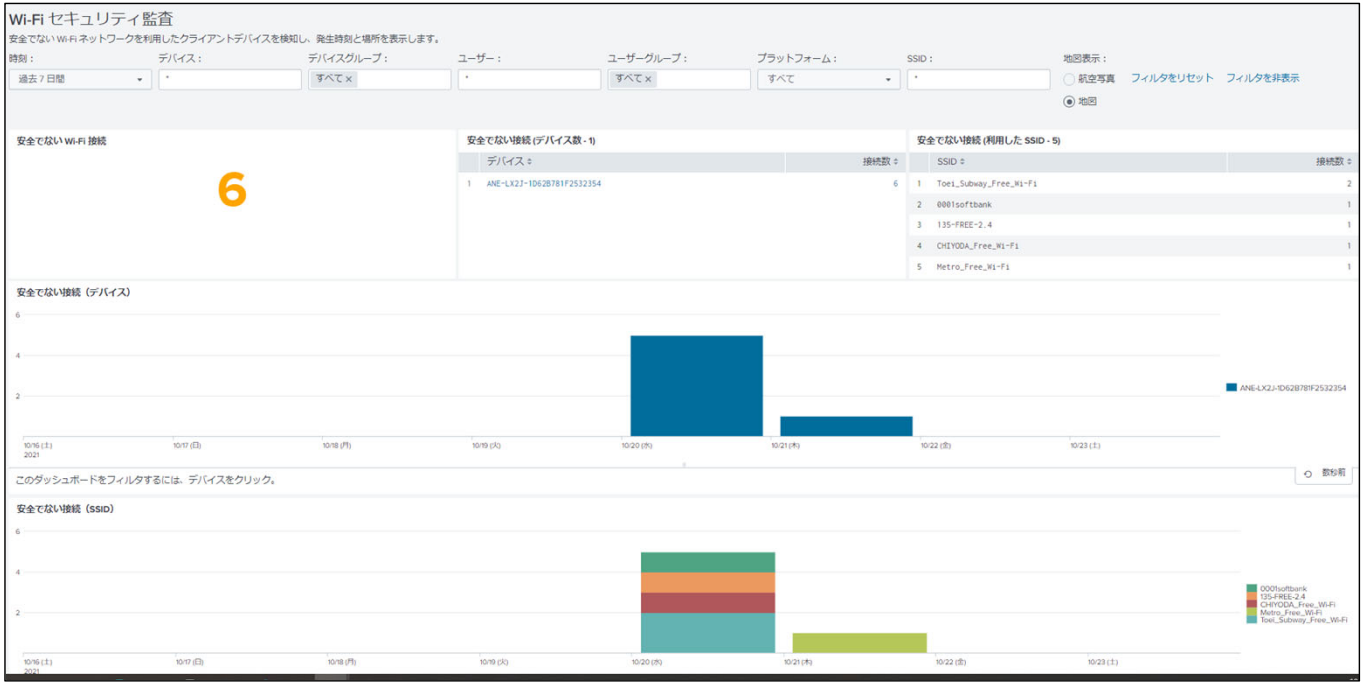
セキュリティ

ユーザのアクセス状況の可視化から
通信を制御する

脅威ステータス一覧 ダッシュボード

ダッシュボードから
Wi-Fiアクセスのリスクを発見

Wi-Fiセキュリティ監査ダッシュボード



リスクのあるアクセス状況の全体を把握する

アクセス元デバイス名を特定

安全でない接続 (デバイス数 - 1)

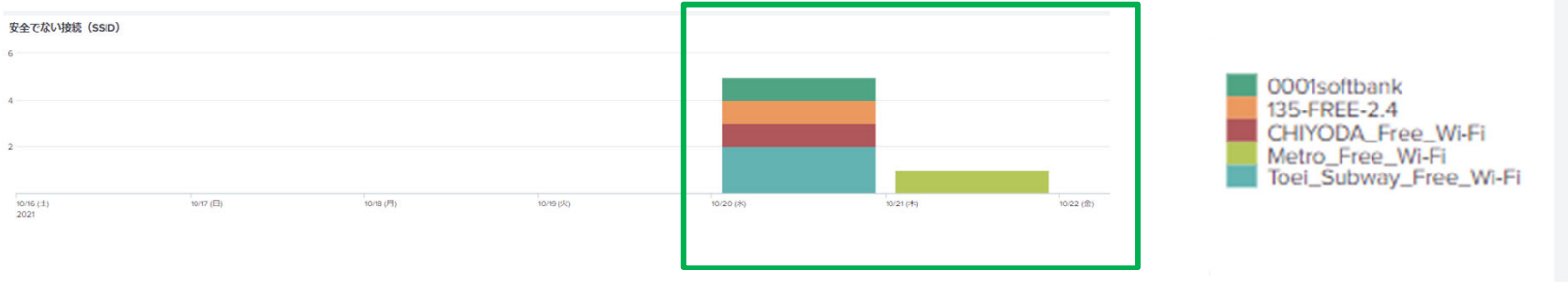
	デバイス	接続数
1	ANE-LX2J-1D62B781F2532354	6

アクセス先SSIDを特定

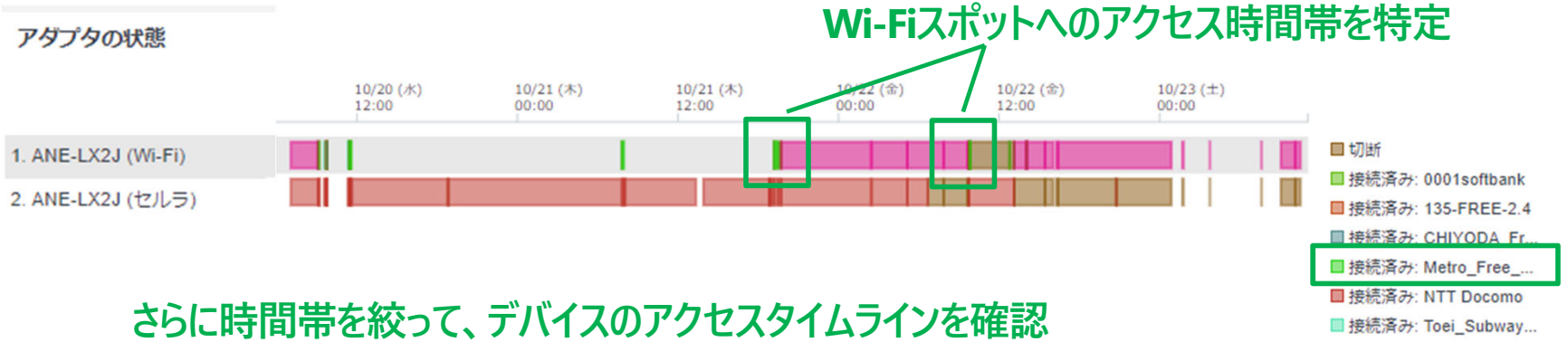
安全でない接続 (利用した SSID - 5)

	SSID	接続数
1	Toei_Subway_Free_Wi-Fi	2
2	0001softbank	1
3	135-FREE-2.4	1
4	CHIYODA_Free_Wi-Fi	1
5	Metro_Free_Wi-Fi	1

アクセス日時を特定



ある特定のデバイスがFree Wi-Fiらしきアクセスポイントにアクセスしている事を把握



Wi-Fiスポットへのアクセス時間帯を特定

さらに時間帯を絞って、デバイスのアクセスタイムラインを確認

アクティビティログ

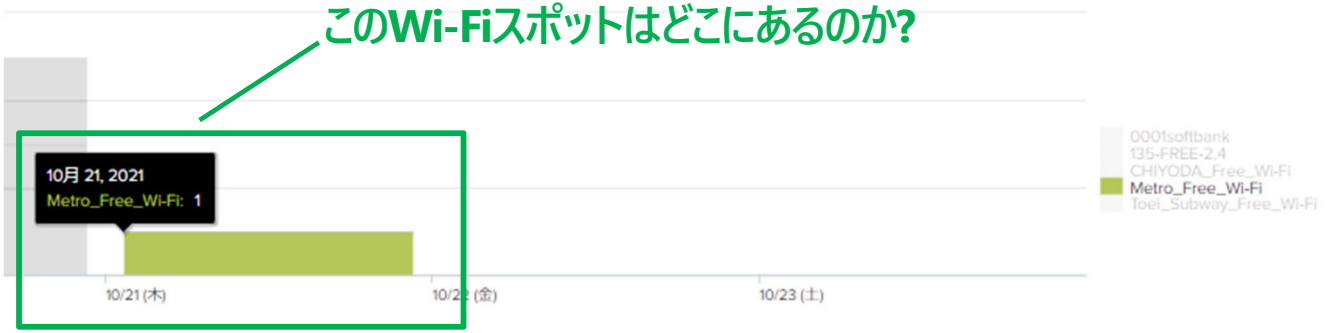
アクティビティ

Wi-Fiスポット (SSID, BSSID)、基地局ID

日付と時刻	アクティビティ	詳細	インターフェース	ネットワーク
2021/10/21 - 19:28:01	ローミング	POP （ローカル）アドレス 100.76.149.189	セルラ	
2021/10/21 - 19:27:59	Wi-Fi ネットワークから切断		Wi-Fi	Metro_Free_Wi-Fi (BSSID = 10-BD-18-F1-C3-36)
2021/10/21 - 19:26:57	Wi-Fi BSSID の変更		Wi-Fi	Metro_Free_Wi-Fi (BSSID = 10-BD-18-F1-C3-36)
2021/10/21 - 19:26:14	Wi-Fi BSSID の変更		Wi-Fi	Metro_Free_Wi-Fi (BSSID = 10-BD-18-F1-C3-39)
2021/10/21 - 19:11:58	Wi-Fi ネットワークに接続		Wi-Fi	Metro_Free_Wi-Fi (BSSID = 0A-00-23-FD-66-EB)
2021/10/21 - 19:11:57	セルラネットワークに接続		セルラ	NTT Docomo (基地局ID= 35003925)
2021/10/21 - 19:11:56	Mobility サーバーに接続	Mobility	Wi-Fi	Metro_Free_Wi-Fi
2021/10/21 - 19:11:52	Mobility サーバーから切断	Mobility: クライアントが同じデバイスから新規接続を確立しました	セルラ	
2021/10/21 - 19:11:25	Wi-Fi ネットワークに接続		Wi-Fi	Metro_Free_Wi-Fi (BSSID = 0A-00-23-FD-66-EB)
2021/10/21 - 19:11:23	Wi-Fi ネットワークが有効		Wi-Fi	

同じWi-FiでBSSIDを頻繁に変更しているという事は、移動している物体？ 乗り物？

このWi-Fiスポットはどこにあるのか?



アクセスマップから
地下鉄のWi-Fiである事を把握

特定のAndroidデバイスが、移動中に地下鉄のフリーWi-Fiスポットに接続していた!!

アクセス元のデバイスの詳細を確認

デバイス: ANE-LX2J-1D62B781F2532354 - デバイスアクティビティ詳細

デバイスグループ	メーカー	モデル	プラットフォーム	OS バージョン
[なし]	HUAWEI	ANE-LX2J	Android	9

ネットワークアダプタ

インターフェース	製造元	モデル	携帯電話キャリア
セルラ	HUAWEI	ANE-LX2J	NTT Docomo
Wi-Fi	HUAWEI	ANE-LX2J	

カテゴリの詳細

リスク	カテゴリ	脅威の説明	宛先ホスト名	デバイス	ユーザー	アプリケーション
!	アドウェア	情報の追跡や収集、ポップアップ生成、プログラムのインストールをユーザーの同意なしに実行するサイト	counter.yadro.ru	ANE-LX2J-1D62B781F2532354	MOBILITY\es-user	com.android.chrome

デバイスのアクセス先を把握

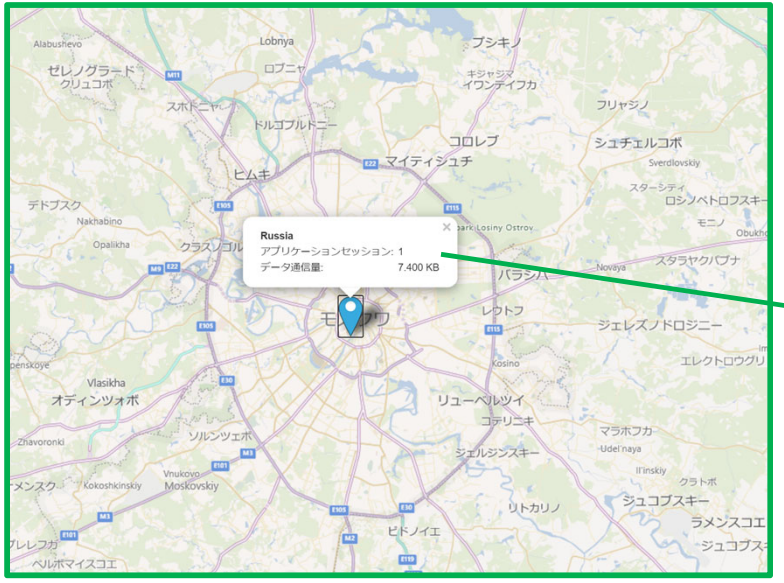
このAndroidデバイスが、chromeでリスクの高いアドウェアサイトにアクセスしている!!

宛先：counter.yadro.ru

最終アクセス日時	カテゴリ	リスク	アプリケーションセッション	データ通信量
2021/10/24 - 11:55:19	アドウェア - セキュリティ	高	3	12.730 KB
2021/10/19 - 13:19:11			1	7.400 KB

IP アドレス

	ホストの IP	プロトコル
1	88.212.201.216:443	TCP
2	88.212.201.216:80	TCP



宛先ホストのIP:ポートを把握

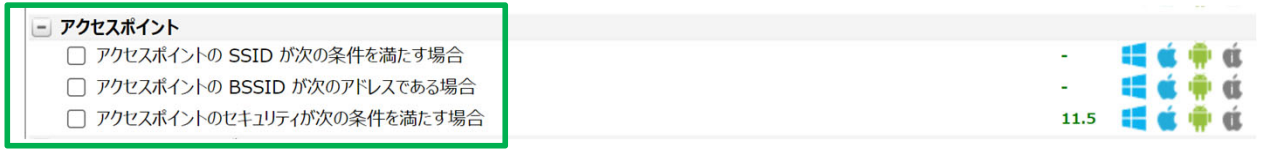
宛先ホストの地域をマップから把握

通信先の場所をIPロケーションを利用して把握!!

アクション・ポリシーへの反映

当該デバイスを隔離する(1st)

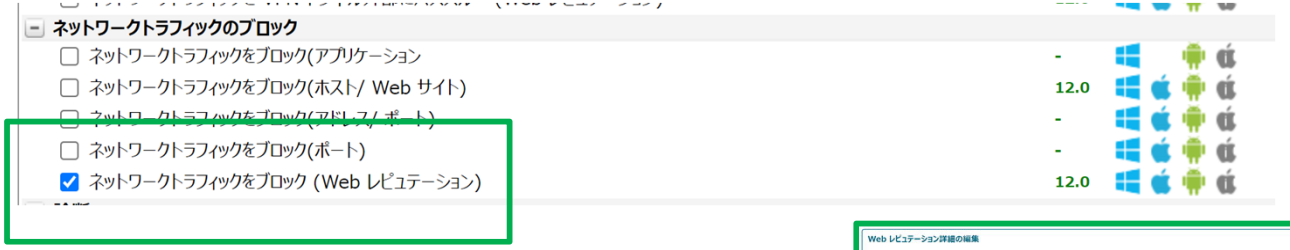
暗号化していないWi-Fiアクセスポイントをブロックするポリシーを設定(2nd)

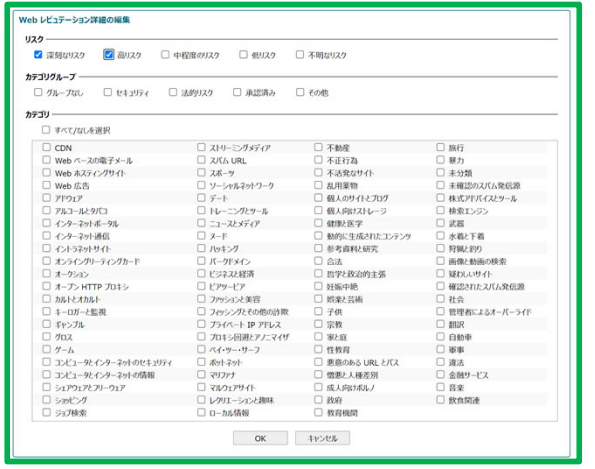


※その他、全通信をVPNトンネルに入れて暗号化させる、等も考えられる

把握した情報をもとに、セキュリティポリシーを見直す

アクション・ポリシーへの反映





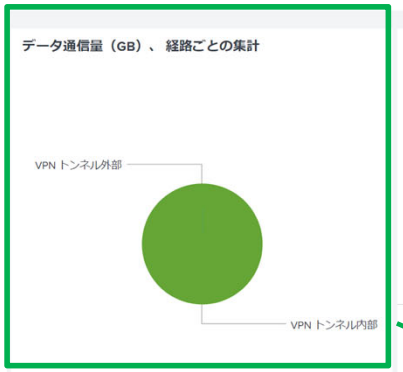
リスク、カテゴリを指定して通信をブロックする
ポリシーを設定

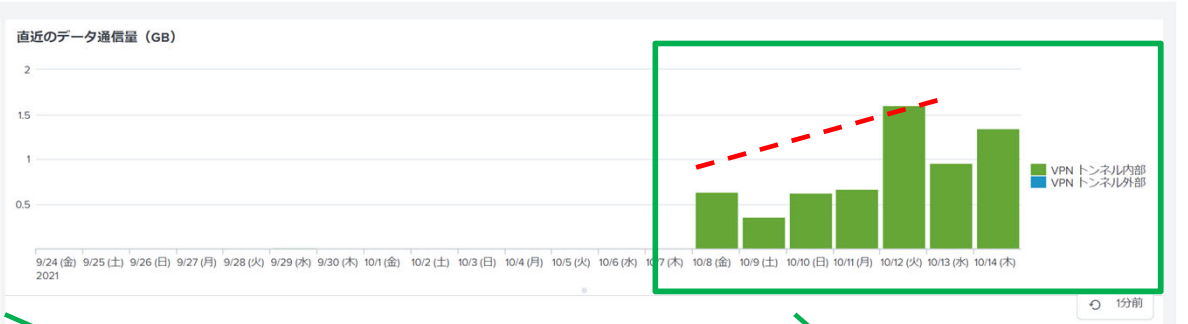
把握した情報をもとに、セキュリティポリシーを見直す

ネットワークボトルネックの把握

VPNトラフィック状況の可視化から
通信制御する

VPN通信状況 ダッシュボード





全通信がVPNトンネル内部

通信量が増加傾向!?

アプリケーション	VPN トンネル内部	VPN トンネル内部（%）	VPN トンネル外部	VPN トンネル外部（%）	データ合計
iOS Application	3.173 GB	100.00%	0 bytes	0.00%	3.173 GB
Teams.exe	1.081 GB	100.00%	0 bytes	0.00%	1.081 GB
com.google.android.youtube	433.003 MB	100.00%	0 bytes	0.00%	433.003 MB
chrome.exe	271.627 MB	100.00%	442 bytes	0.00%	271.627 MB
msedge.exe	243.640 MB	100.00%	518 bytes	0.00%	243.640 MB

通信しているアプリケーション上位からTeamsをチェック

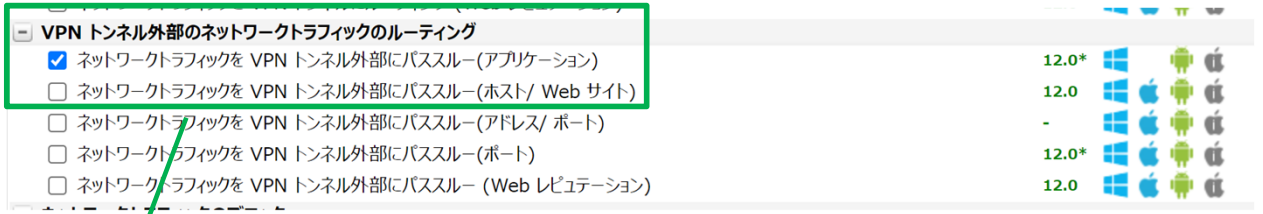
VPN トンネルのデータ通信量

Teamsのトラフィックを把握

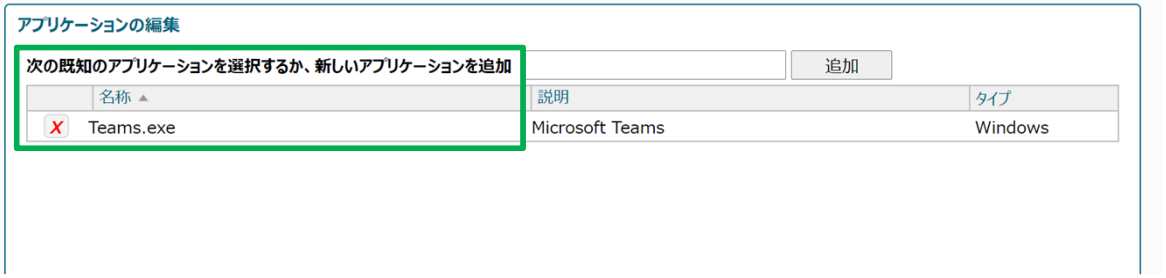
Teamsのトラフィックが急増傾向!

ボトルネックが顕在化する前に、スプリットトンネルを検討しよう

アクション・ポリシーへの反映



Teamsアプリを指定して
VPN外部にパススルーする
設定を入れる



把握したトラフィック情報をもとに、通信ポリシーを見直す

VPN トンネルのデータ通信量

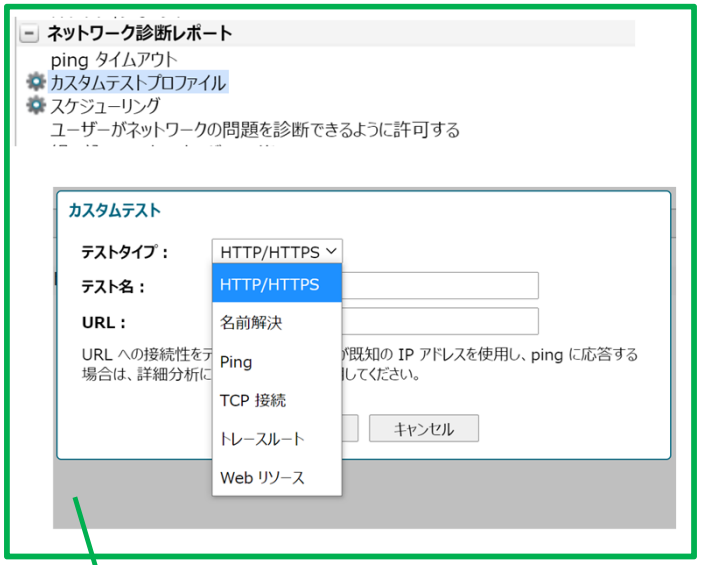
Teams通信がスプリットされてVPN外部に変わった!!

ボトルネックのリスクを未然に対策する事ができた!!

トラブルシュート

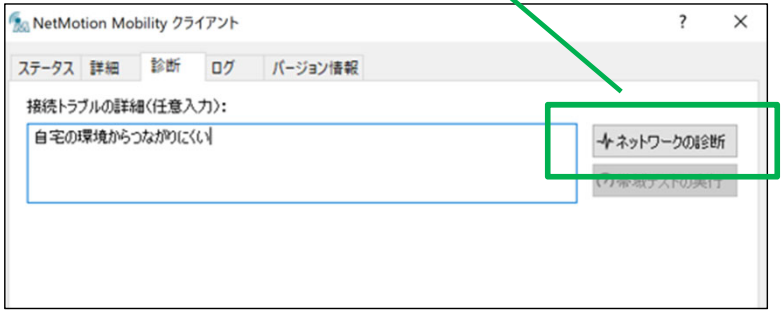
ユーザからの「つながらない」問い合わせ

ユーザ環境からの通信テスト



管理者がテスト設定をする

ユーザがモビリティクライアントの診断ボタンを押すとテスト実施



Wi-Fiのシグナルレベルは問題なし

Wi-Fi ステータス	接続済み
Wi-Fi プロファイル	[redacted]
Wi-Fi 接続モード	自動
Wi-Fi BSSID	[redacted]
Wi-Fi SSID	
Wi-Fi タイプ	インフラストラクチャ
Wi-Fi シグナル（0～100）	82

自宅のインターネット接続の問題っぽいな

指定ホストに対してPing Traceroute失敗

インターネット接続

詳細の非表示

Test Summary

Host name resolution to host name http://diag2.localitycloud.com result: Fail

Ping to 18.208.81.151 result: Fail

Ping to 2600:1f18:619f:8800:63d3:cab2:9cdd:b6bb result: Fail

Page Load Result: Fail

Trace Route Statistics

Tracing a route to 18.208.81.151 [18.208.81.151]

Over a maximum of 30 hops

1	*	*	*	Request timed out
2	*	*	*	Request timed out
3	*	*	*	Request timed out
4	*	*	*	Request timed out
5	*	*	*	Request timed out
6	*	*	*	Request timed out

通信テストの情報から、トラブルシュートする

リモートワークで今後顕在化する課題とは?

セキュリティ部門
情シス部門

セキュリティ

情シス部門

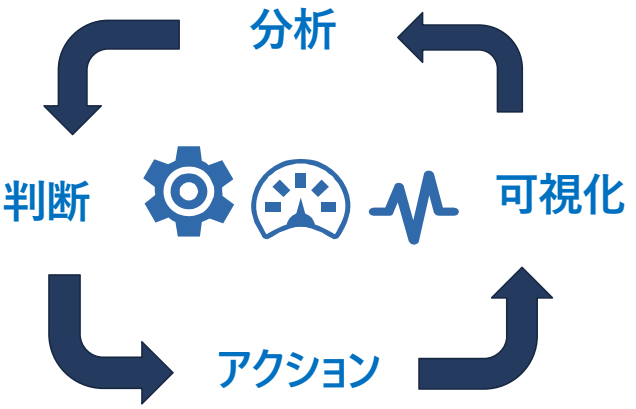
ネットワークのボトルネック

従業員
情シス部門

トラブルシュート

フレックスモビリティ/ZTNA で解決

通信の状況、セキュリティ状況を可視化



可視化<->アクションのサイクルを回す

フレックスモビリティ/ZTNAとは

「**切れないVPN**」をベースに、「**ゼロトラスト**」を実現する

快適、**セキュア**を両立するVPNサービス

フレックスモビリティ/ZTNAの強み

Point 1.　切れないVPN

Point 2.　デバイスのトラフィックを全て可視化・制御

Point 3.　小規模から大規模まで利用可能

・100デバイスからスモールスタート可能

・最大60,000デバイス、広帯域(最大2Gbps)に対応

ご視聴ありがとうございました。

IIJ
Internet Initiative Japan