Note for readers of this English translation

This document has been translated from the Japanese original for reference purpose only. In the event of any discrepancy between this English translation and the Japanese original, the Japanese original shall prevail.

Business Briefing on IIJ’s New Remote Access Service

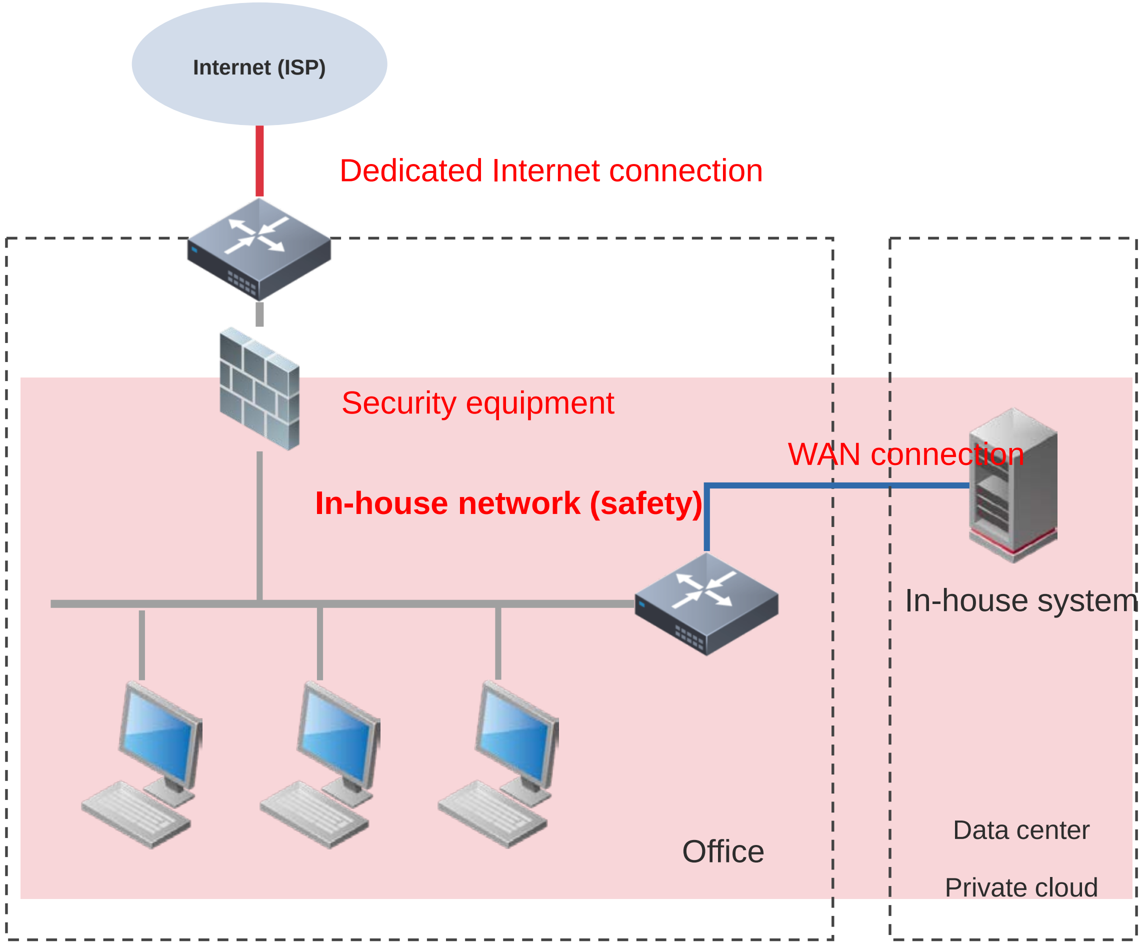
Change in Enterprise Office Internet Usages

IIJ
Internet Initiative Japan

January 25, 2022
Internet Initiative Japan Inc.
Network Division Network Department Internet Access Section, Manager
Takashi Hara

Typical way to use the Internet by companies before 2019

- Employees come to the office to work
- Concept of “in-house network”
- Security through a perimeter defense


Internet (ISP)
Dedicated Internet connection
Security equipment
WAN connection
In-house network (safety)
In-house system
Office
Data center
Private cloud

Recent changes in use of the Internet by companies

Advancement of DX/spread of digital workplace

- Rapid increase in use of public Clouds, e.g. Microsoft 365, Google Workspace

→ Rapid increase in public Cloud-bound traffic instead of WAN (in-house network)

Diversified work styles/ Normalization of teleworking

- Rapid increase in operations using the network outside the companies’ control, e.g. private Internet connections

→ Necessity of auditing/control of connections including use of public Clouds

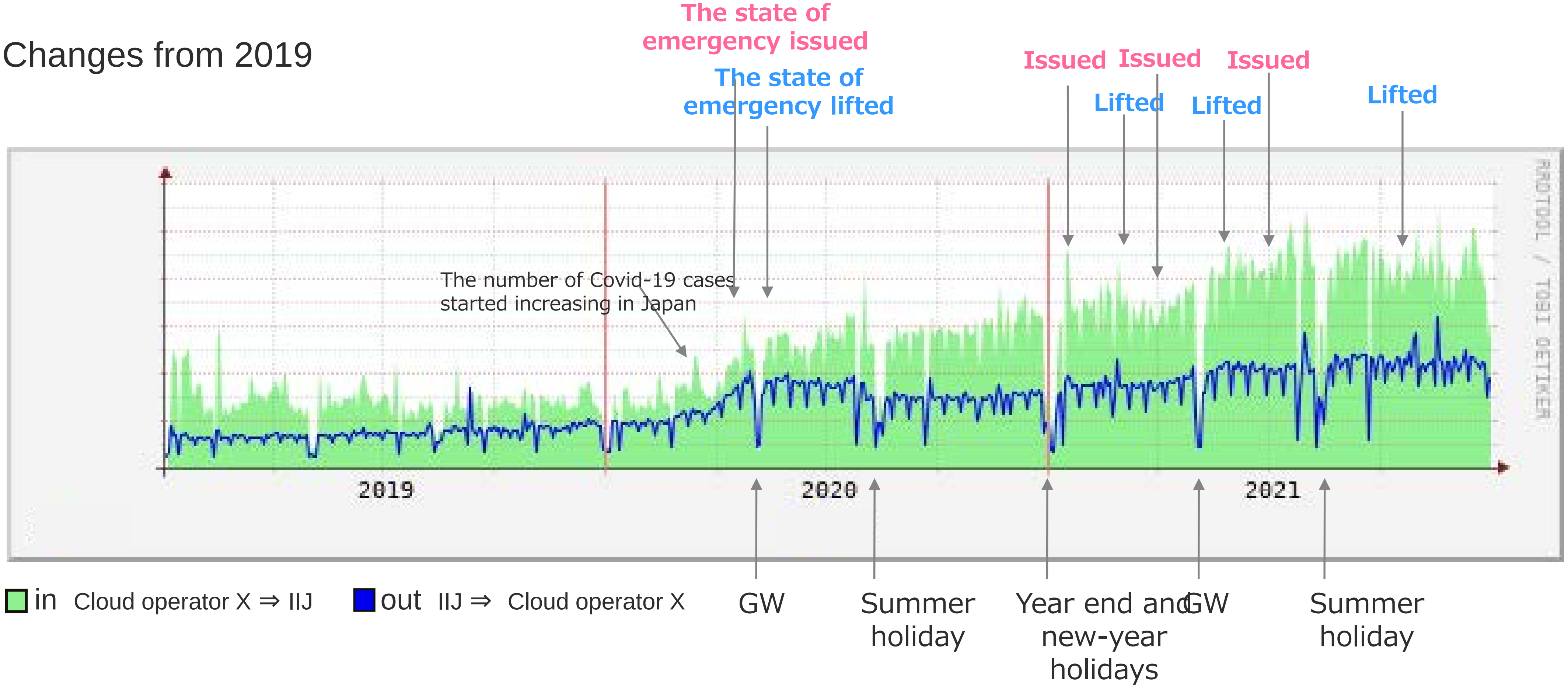
Although these changes were partially provoked by the Covid-19 pandemic, it is not the only cause.

The changes are not temporarily but are here to stay. These changes in the corporate activities will spread among more companies.

No end to the increase in the traffic bound to the Cloud operators

～ Example of traffic between cloud operator X and IIJ ～

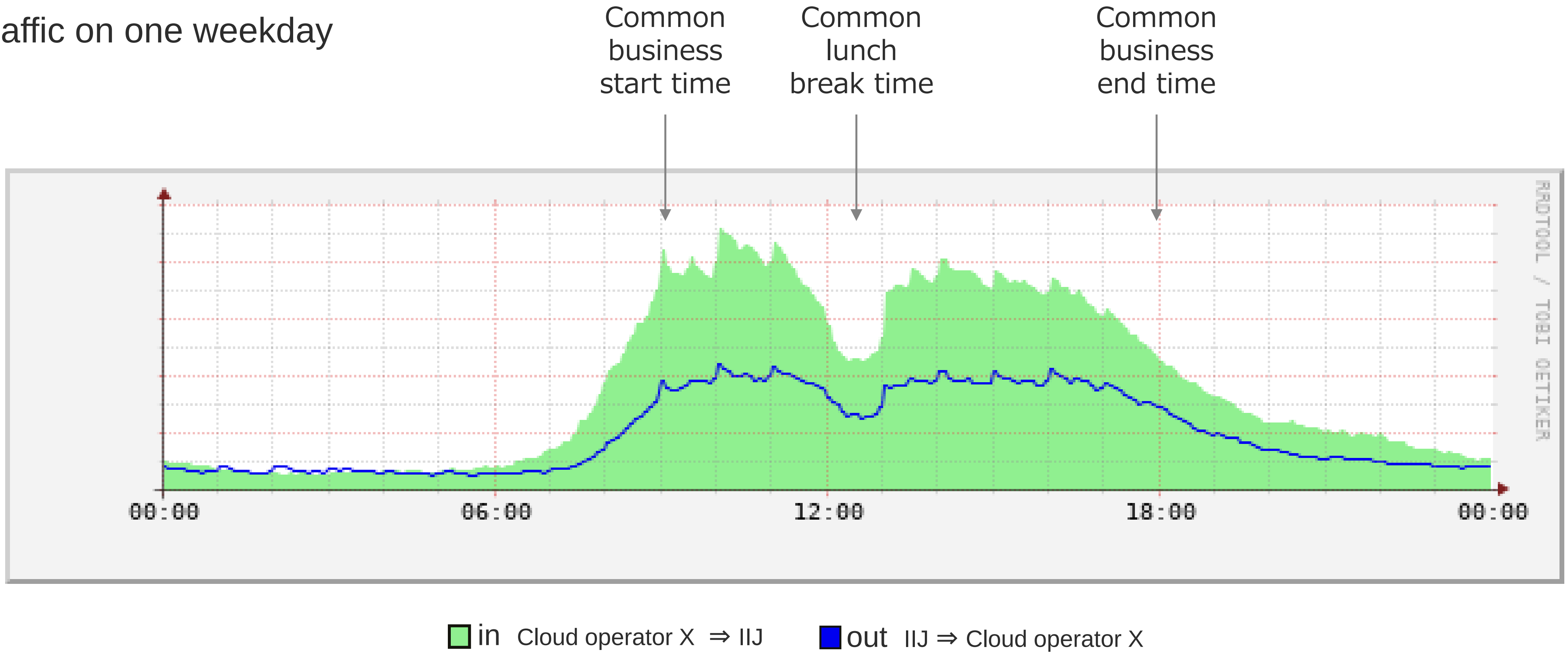
■ Changes from 2019



- **Connection with a cloud operator shows an increase of more than twice between 2019 and 2021**
- **There is no doubt that, if more than one cloud service is used, the total amount has increased even more.**

Spread of Public Clouds

- Traffic on one weekday



Common business start time

Common lunch break time

Common business end time

🟩 in Cloud operator X ⇒ IIJ

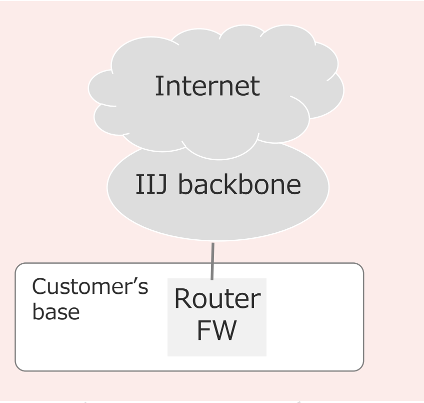
🟦 out IIJ ⇒ Cloud operator X

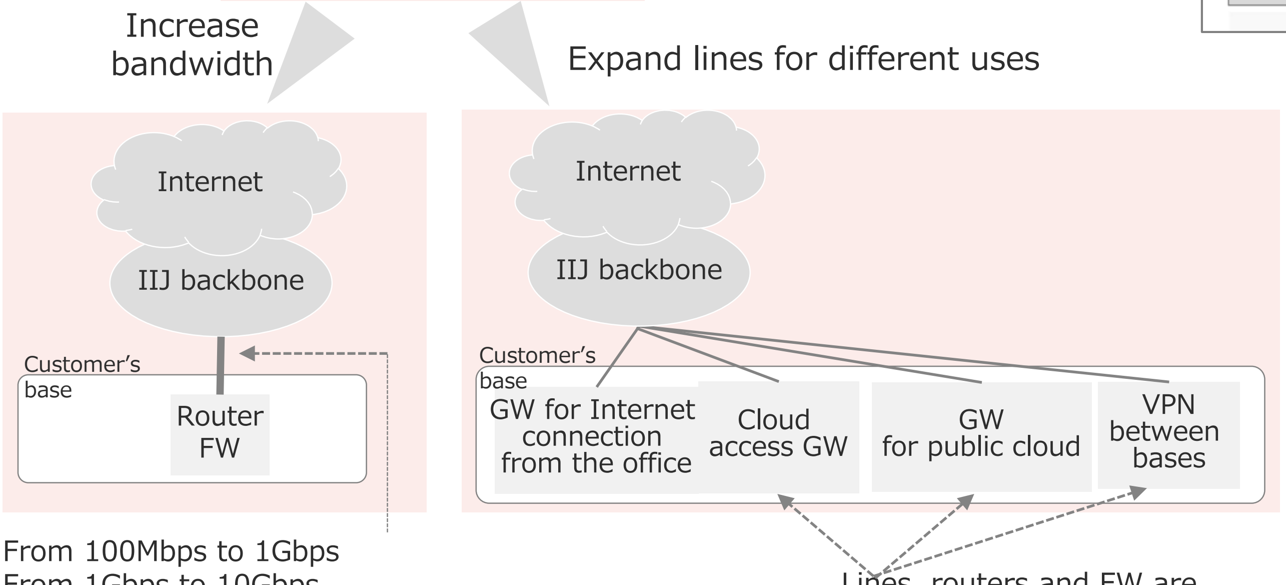
- **Traffic fluctuates according to increase or decrease in the use by corporate customers during the daytime on a weekday**
- **It is clear that use specifically for business increases**

Equipment investment due to the spread of Public Clouds

Increase in customers’ equipment investment in association with the traffic increase

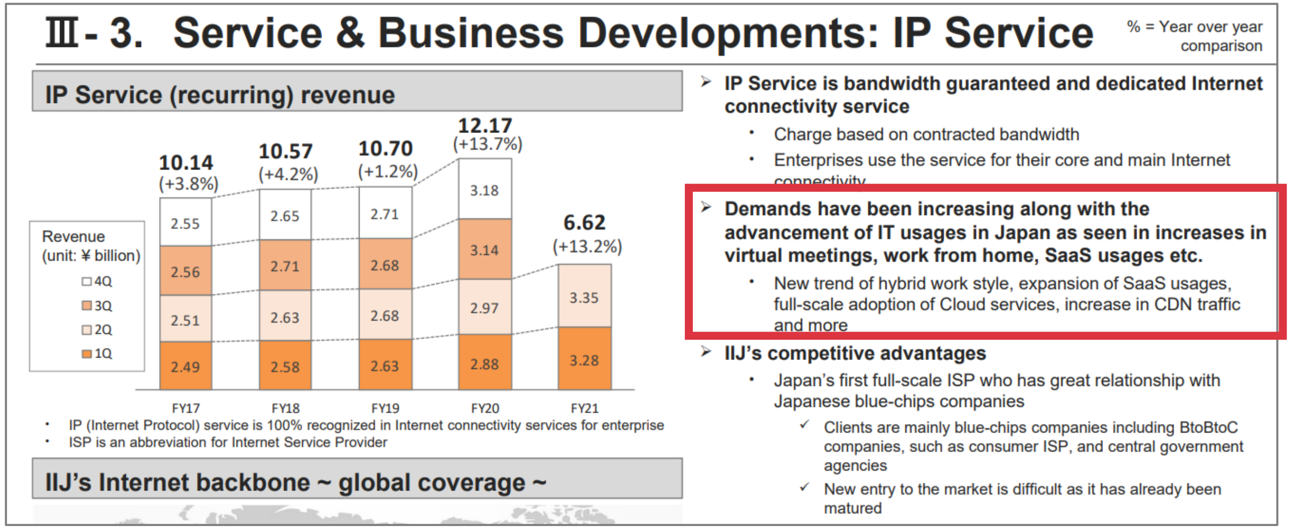
- Enhancement of Internet connection equipment


Internet
IIJ backbone
Customer’s base
Router
FW


Increase bandwidth
Expand lines for different uses
Internet
IIJ backbone
Customer’s base
Router
FW
Internet
IIJ backbone
Customer’s base
GW for Internet connection from the office
Cloud access GW
GW for public cloud
VPN between bases

From 100Mbps to 1Gbps
From 1Gbps to 10Gbps
From a line of 10Gbps to multiple lines of 10Gbps

Lines, routers and FW are prepared for each use



Ⅲ- 3. Service & Business Developments: IP Service

% = Year over year comparison

IP Service (recurring) revenue

Revenue (unit: ¥ billion)

	FY17	FY18	FY19	FY20	FY21
Total	10.14 (+3.8%)	10.57 (+4.2%)	10.70 (+1.2%)	12.17 (+13.7%)	6.62 (+13.2%)
☐ 4Q	2.55	2.65	2.71	3.18	
🟧 3Q	2.56	2.71	2.68	3.14	
☐ 2Q	2.51	2.63	2.68	2.97	3.35
🟧 1Q	2.49	2.58	2.63	2.88	3.28

- IP (Internet Protocol) service is 100% recognized in Internet connectivity services for enterprise
- ISP is an abbreviation for Internet Service Provider

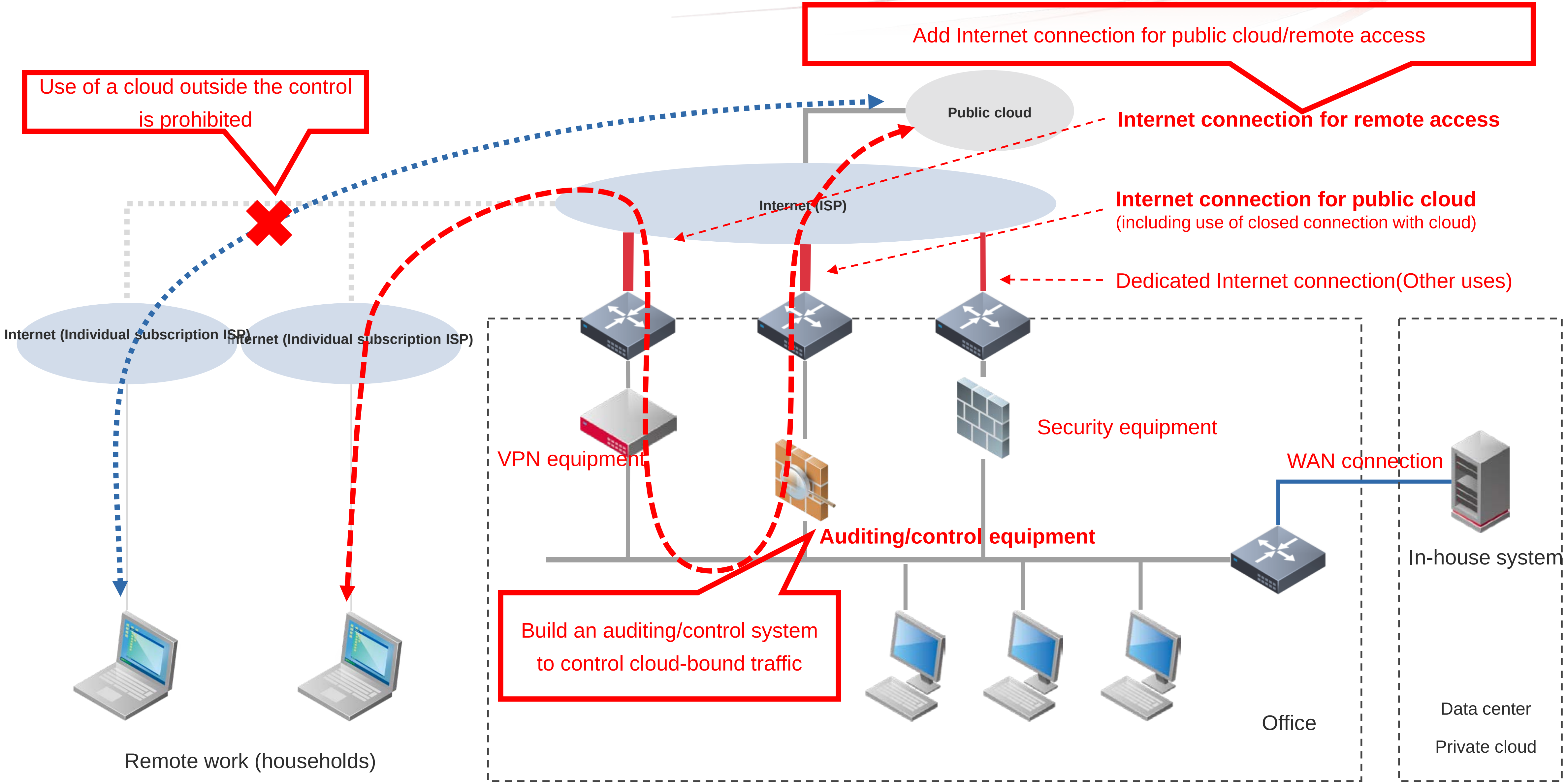
IIJ’s Internet backbone ~ global coverage ~

- ➢ **IP Service is bandwidth guaranteed and dedicated Internet connectivity service**
  - Charge based on contracted bandwidth
  - Enterprises use the service for their core and main Internet connectivity
- ➢ **Demands have been increasing along with the advancement of IT usages in Japan as seen in increases in virtual meetings, work from home, SaaS usages etc.**
  - New trend of hybrid work style, expansion of SaaS usages, full-scale adoption of Cloud services, increase in CDN traffic and more
- ➢ **IIJ’s competitive advantages**
  - Japan’s first full-scale ISP who has great relationship with Japanese blue-chips companies
    - ✓ Clients are mainly blue-chips companies including BtoBtoC companies, such as consumer ISP, and central government agencies
    - ✓ New entry to the market is difficult as it has already been matured

From IIJ’s consolidated financial results for 1H21
https://www.iij.ad.jp/en/ir/library/financial/pdf/IIJ2Q21E_presentation.pdf

- Investment in the equipment of Internet connection lines increased due to the increase in use of public Clouds
  - Customers enhanced their equipment using diversified methods
- The trend has continued since 2020 through 2021 and is likely to continue toward the future.

Case of Internet use by an advanced major company



Add Internet connection for public cloud/remote access

Use of a cloud outside the control is prohibited

Internet connection for remote access

Internet connection for public cloud
(including use of closed connection with cloud)

Dedicated Internet connection(Other uses)

Build an auditing/control system to control cloud-bound traffic

Public cloud
Internet (ISP)
Internet (Individual subscription ISP)
Internet (Individual subscription ISP)
VPN equipment
Security equipment
Auditing/control equipment
WAN connection
In-house system
Office
Data center
Private cloud
Remote work (households)

Remote work and use of public Clouds are accepted as normal, but the uses outside the control are not accepted. (Accelerated shift to zero trust)

- Build a system for auditing/control
- Install an aggregation point of communications within the company's own network

A large-scale and highly advanced network like this can only be implemented by a major company

A medium-sized or semi-major company would not be able to afford installing it on their own

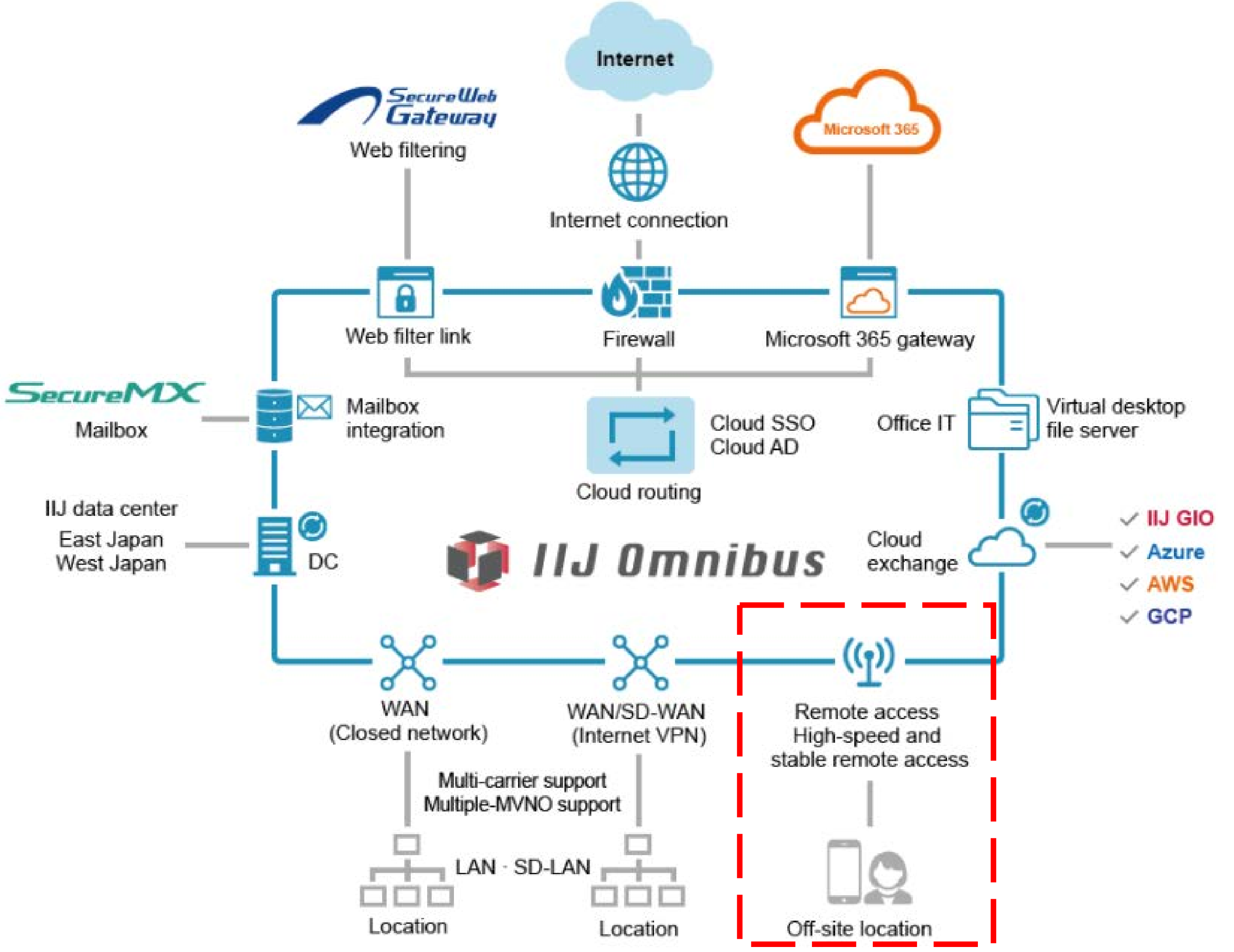
IIJ Omnibus

With the network cloud provided by IIJ Omnibus, a highly advanced network can be implemented through outsourcing.

IIJ Omnibus is a brand of the network cloud that covers an entire corporate network

- IIJ Flex Mobility Service/ZTNA

  One of the services constituting IIJ Omnibus and a remote access service with added function of zero trust network


Internet
SecureWeb Gateway
Web filtering
Microsoft 365
Internet connection
Web filter link
Firewall
Microsoft 365 gateway
SecureMX
Mailbox
Mailbox integration
Cloud SSO
Cloud AD
Office IT
Virtual desktop file server
Cloud routing
IIJ data center
East Japan
West Japan
DC
IIJ Omnibus
Cloud exchange
✓ IIJ GIO
✓ Azure
✓ AWS
✓ GCP
WAN (Closed network)
WAN/SD-WAN (Internet VPN)
Remote access
High-speed and stable remote access
Multi-carrier support
Multiple-MVNO support
LAN · SD-LAN
Location
Location
Off-site location

IIJ Flex Mobility Service/ZTNA

New IIJ Flex Mobility Service that realizes Zero Trust

Internet Initiative Japan Inc.
Network Service Division, Deputy Division Director
Yoshihiro Yoshikawa

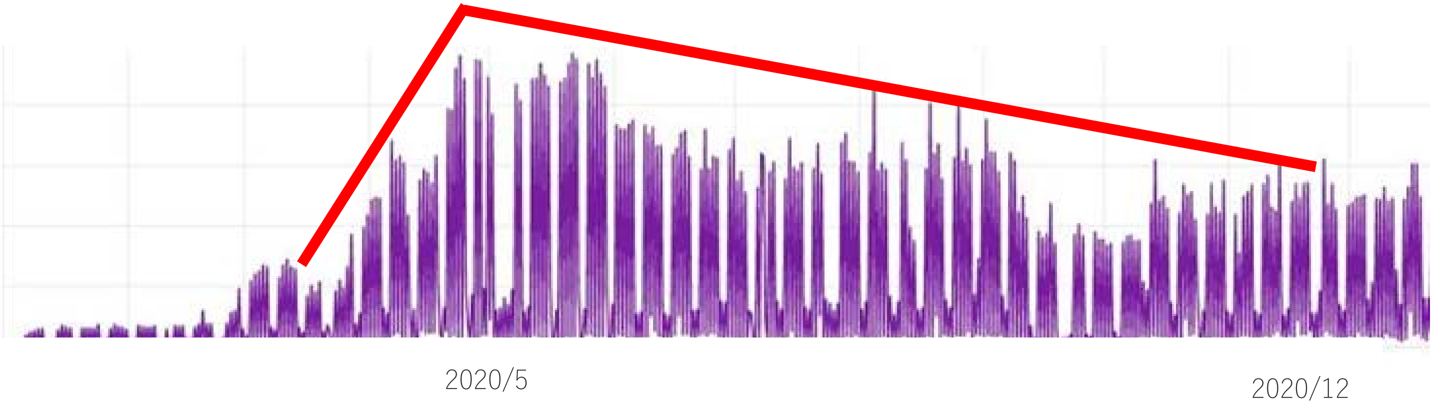
Today’s Topic

Issues emerging with Remote Work and Zero Trust

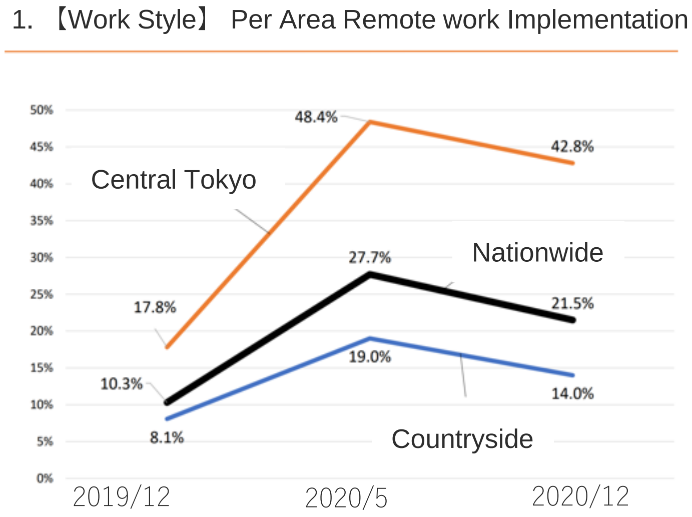
What New IIJ Flex Mobility Services offer

Issues emerging with remote working

IIJ Flex Mobility Bandwidth for 2020



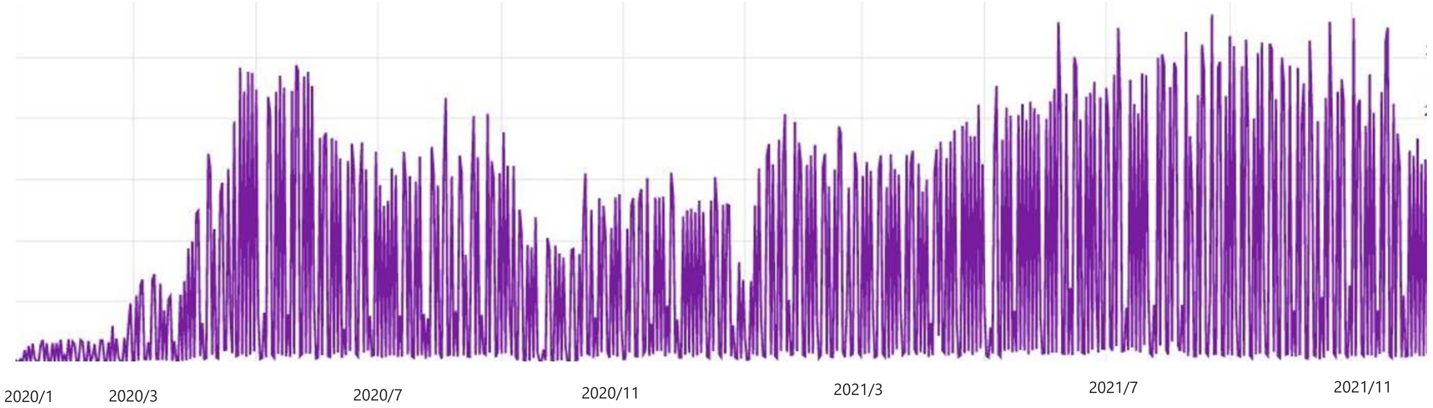
IIJ Flex Mobility Services' Bandwidth for 2020


1. 【Work Style】 Per Area Remote work Implementation

From The Cabinet's Home Page
Survey on change in general views and human behavior under the COVID-19 Pandemic
(https://www5.cao.go.jp/keizai2/keizai-syakai/future2/20210119/shiryou3-1.pdf)

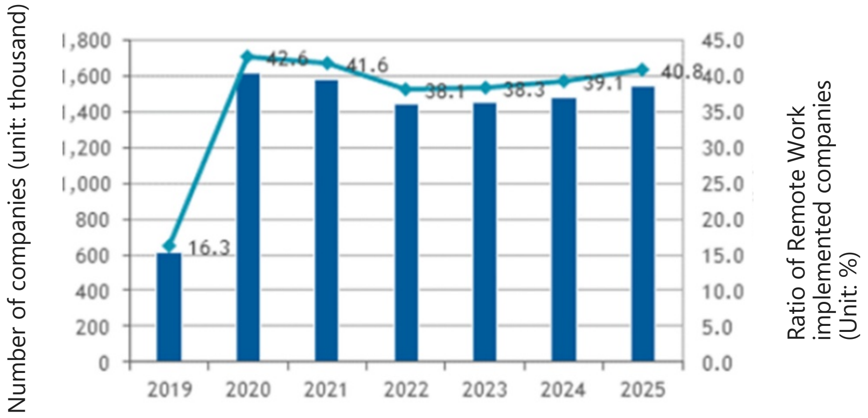
Same Trend seen for Remote work implementation and IIJ Flex Mobility bandwidth

Changes in IIJ Flex Mobility Service/ZTNA bandwidth from 2020 to 2021 (by December 2021)



The VPN traffic has been on a gradual downward trend since the state of emergency was terminated. However, it did not go back to the level before the pandemic.

Market for Domestic Remote Work
Number of companies implementing Remote work (2019 – 2025)

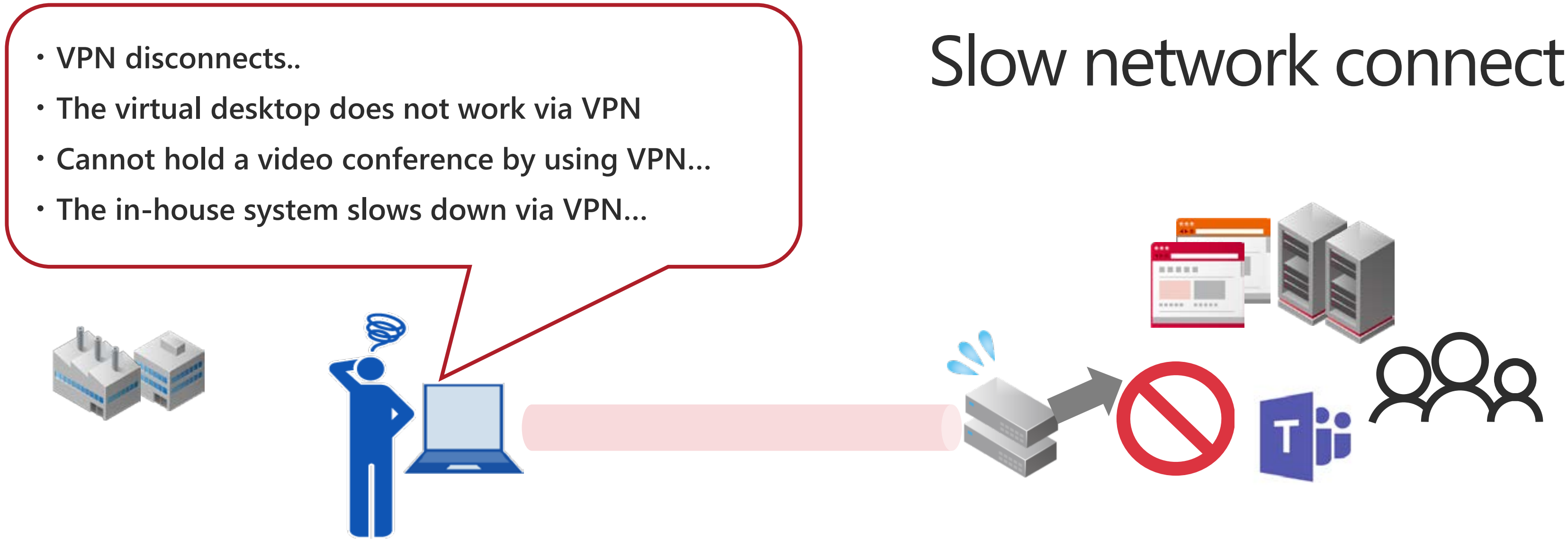


Outlook for the number of companies implementing remote work from 2019 to 2025
Source: Report from IDC

It is likely that the work style will continue transforming and the way of working remotely will remain

Issues solved by IIJ Flex Mobility Services?

What are the issues of network when working remotely?



- VPN disconnects..
- The virtual desktop does not work via VPN
- Cannot hold a video conference by using VPN…
- The in-house system slows down via VPN…

Slow network connections

Constant disconnections

Poor VPN connectivity

After all I cannot have any job done working remotely…

In the end, I have to go to the office..

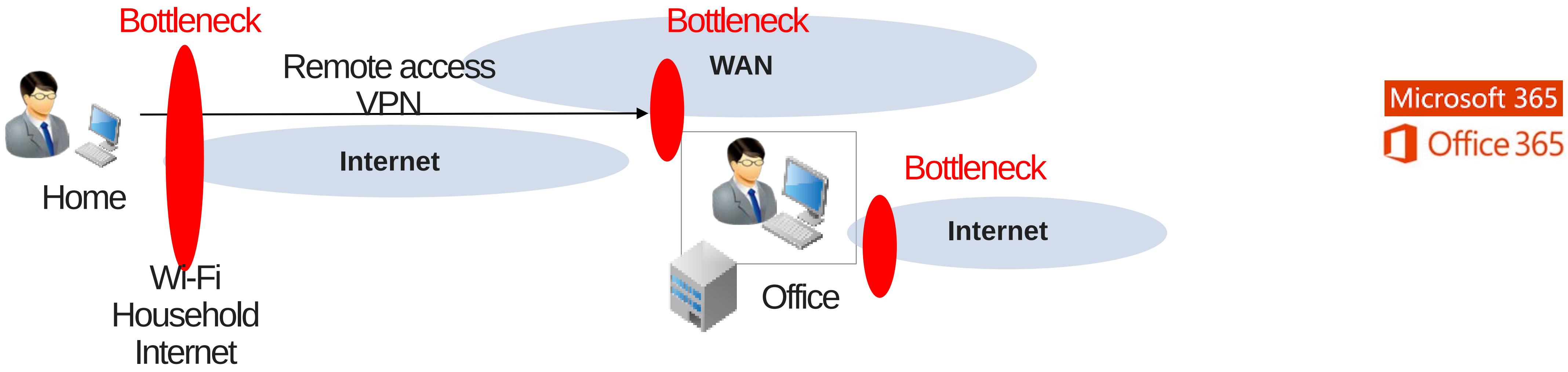
Main reasons for Slow and Poor Connectivity

Wi-Fi setting at home

Internet connectivity quality at home

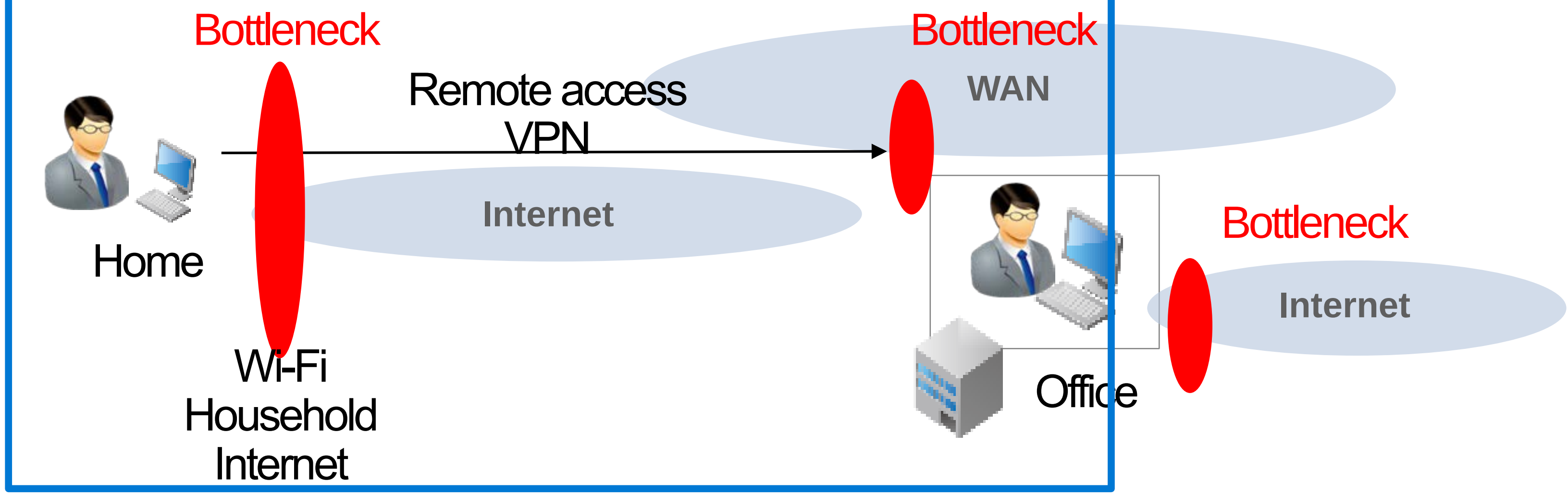
VPN servers for remote access and WAN line

Where are the bottlenecks?


Bottleneck
Bottleneck
Remote access
VPN
WAN
Microsoft 365
Office 365
Internet
Home
Bottleneck
Internet
Wi-Fi
Household
Internet
Office

There are bottlenecks in various places

IIJ Flex Mobility Service Solves the Bottlenecks

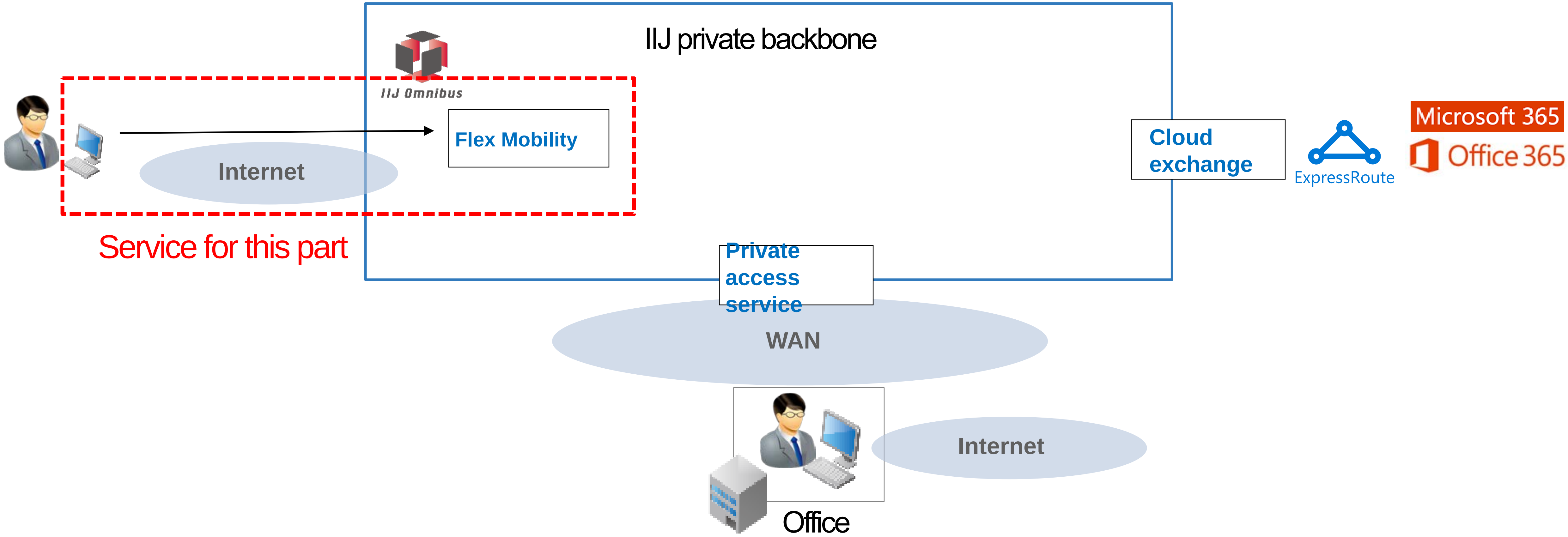

Bottleneck
Bottleneck
Remote access
VPN
WAN
Internet
Home
Bottleneck
Internet
Wi-Fi
Household
Internet
Office

Microsoft 365

Office 365

Bottlenecks

Cloud VPN service


IIJ private backbone
IIJ Omnibus
Flex Mobility
Internet
Service for this part
Cloud exchange
ExpressRoute
Microsoft 365
Office 365
Private access service
WAN
Internet
Office

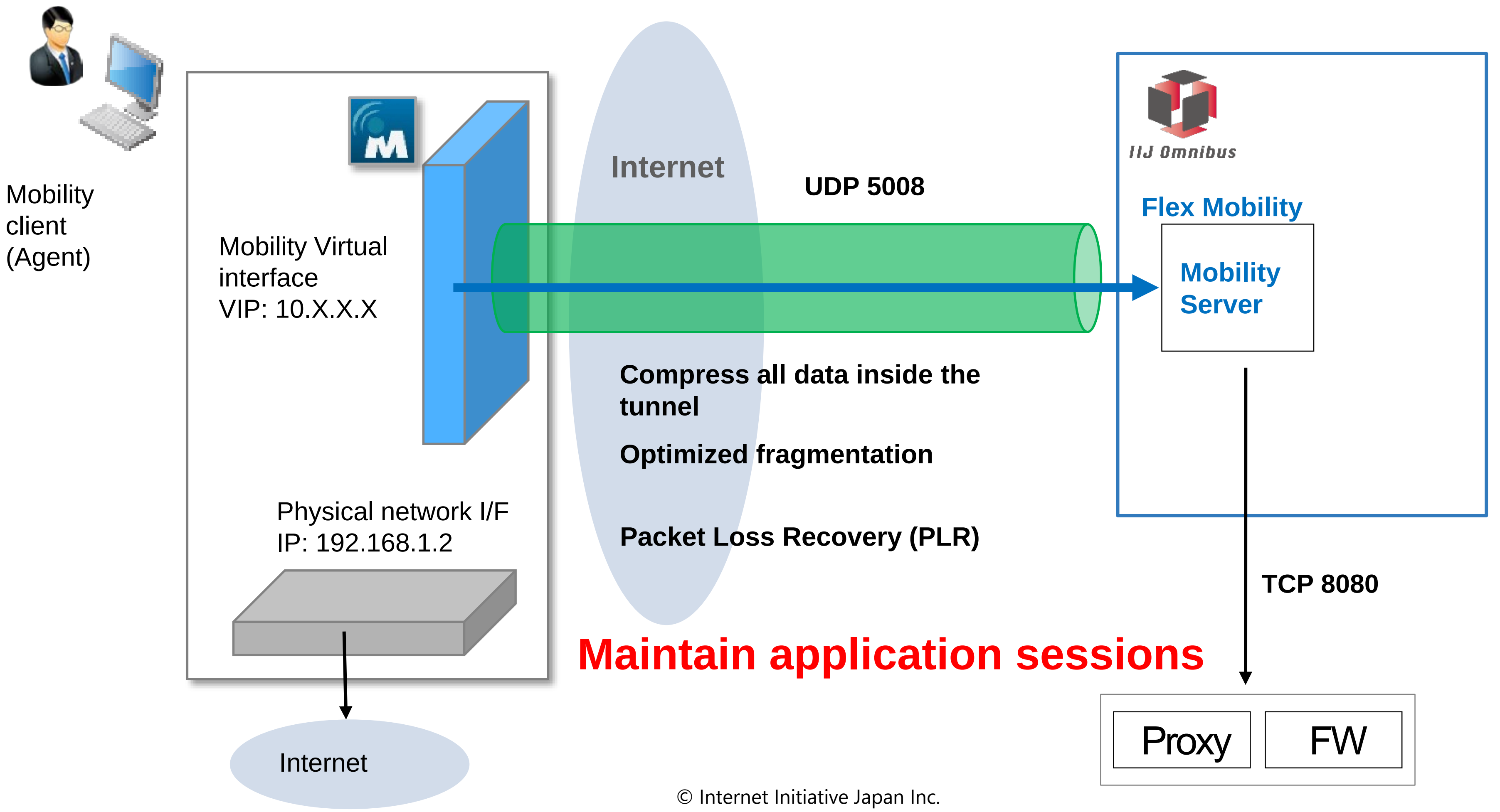
Provide VPN + Network as a service

IIJ Flex Mobility Service

Network based, High Speed, Reliable VPN Service using NetMotion Mobility® as an engine

MOBILITY

Maintain sessions by increasing speed in VPN tunnel and controlling flow



Mobility client (Agent)

Mobility Virtual interface
VIP: 10.X.X.X

Physical network I/F
IP: 192.168.1.2

Internet

Internet

UDP 5008

Compress all data inside the tunnel

Optimized fragmentation

Packet Loss Recovery (PLR)

Flex Mobility

Mobility Server

TCP 8080

Proxy

FW

Maintain application sessions

Frequently occurring situation when working remotely

Connect to the in-house file server via VPN and edit a PPT document

Save the file and close the PC (sleep/lock)

Open the PC and start editing the document again

Start forgetting about VPN

New Issues emerged with Remote Work

Is security in teleworking OK?

Who connects from where?

Is the connecting PC safe?

Isn’t it a public Wi-Fi?

Is there a risk of information leakage?

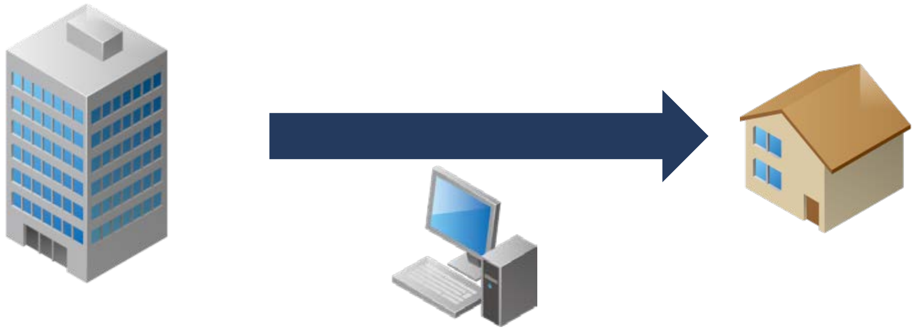
Access status is invisible…

Insecure about the shift to teleworking

What we hear

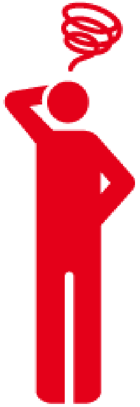
Worry about security when working from home

Sending employee’s desktop to his/her home



Sending PC to home

Network bandwidths are in shortage because of teleworking?

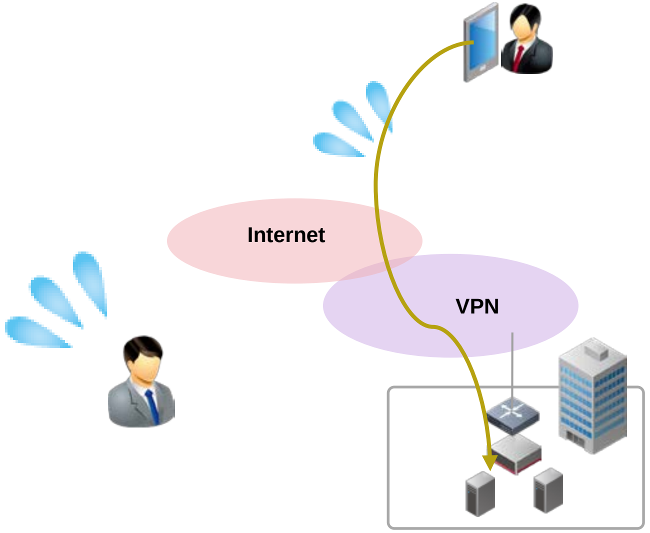


We receive more complaints of slow connections…

Suddenly short of bandwidth?

No idea why…

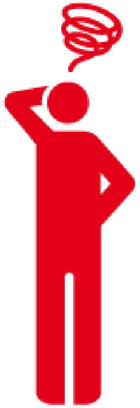
Which part should be spud up?



Usage status is invisible…

No idea what to do…

Inquiries about unstable connections



They blame us for unstable connection, but what about their Wi-Fi connections at home?

There is no way to know about their home Internet connection…

Without knowledge about the users' environments…

troubleshooting is difficult …

What issues of teleworking will come up to the surface in the future?

Security Department
Information Systems Department

Security

Information Systems Department

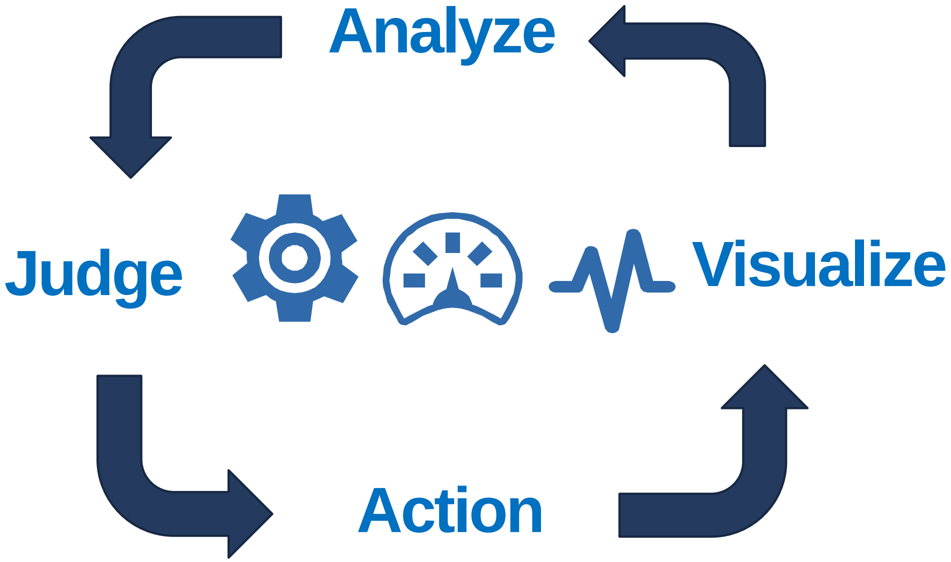
Network bottleneck

Employees
Information Systems Department

Troubleshooting

How to fix?

Visualize status of communications and security status

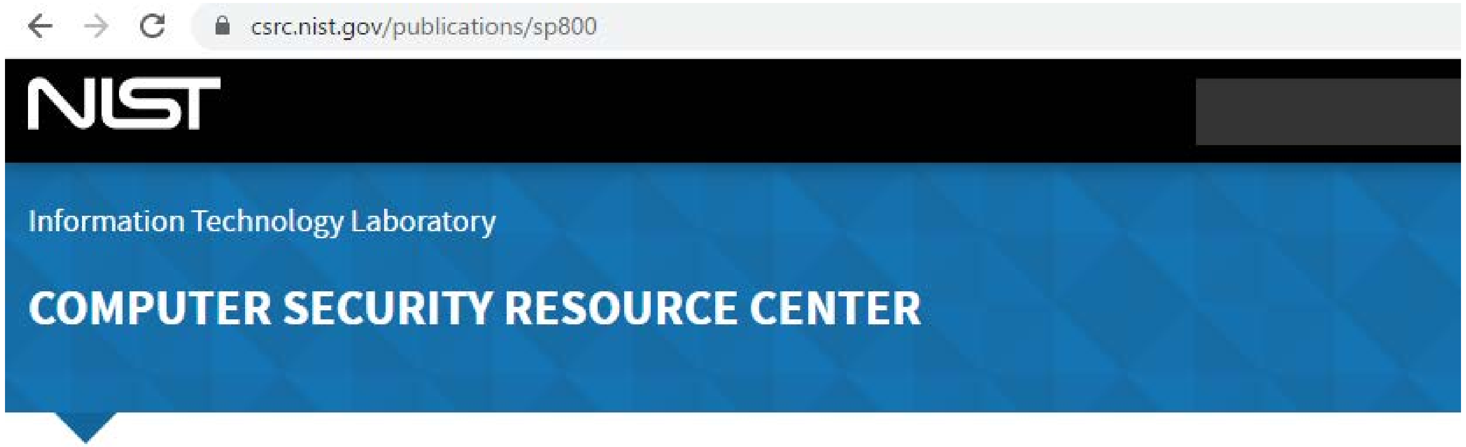

Analyze
Judge
Visualize
Action

Follow the Visualization <-> Action cycle

Zero Trust
Approach toward Security Issues

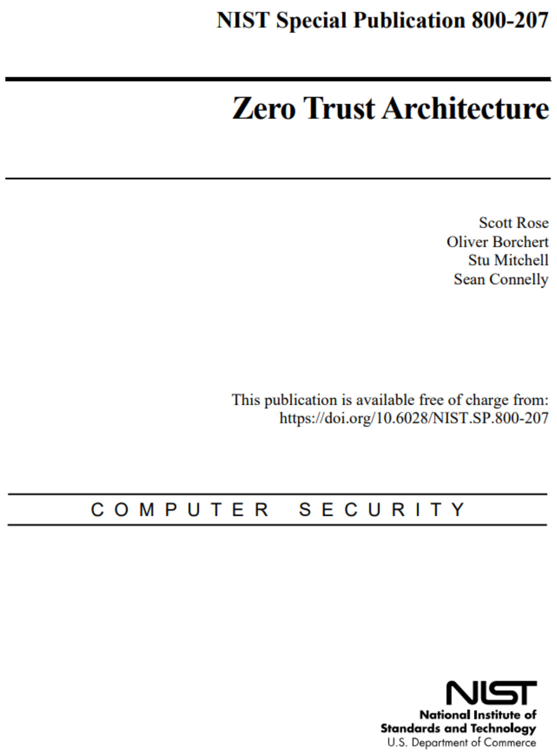
What is Zero Trust Architecture?

“Zero Trust Architecture” is proposed y the National Institute of Standards and Technology (NIST） in its ”SP800-207”


csrc.nist.gov/publications/sp800
NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER



NIST Special Publication 800-207

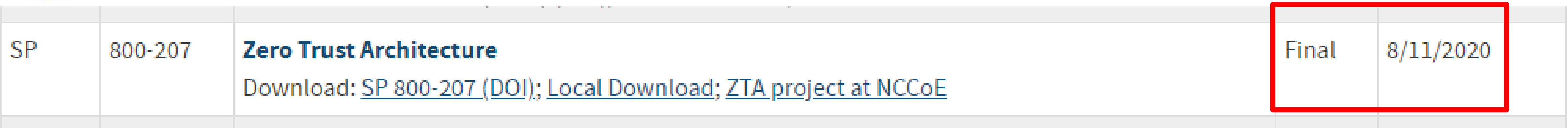
Zero Trust Architecture

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

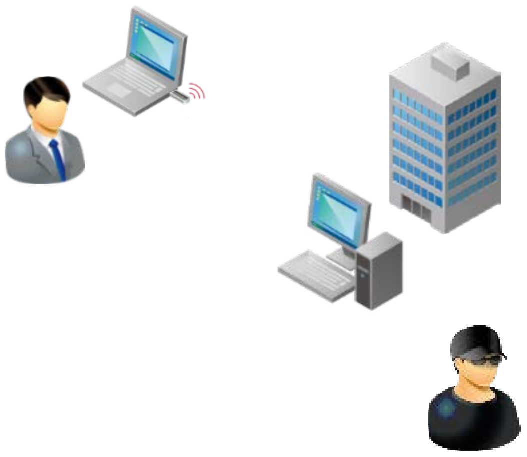


SP	800-207	**Zero Trust Architecture** Download: SP 800-207 (DOI); Local Download; ZTA project at NCCoE	Final	8/11/2020

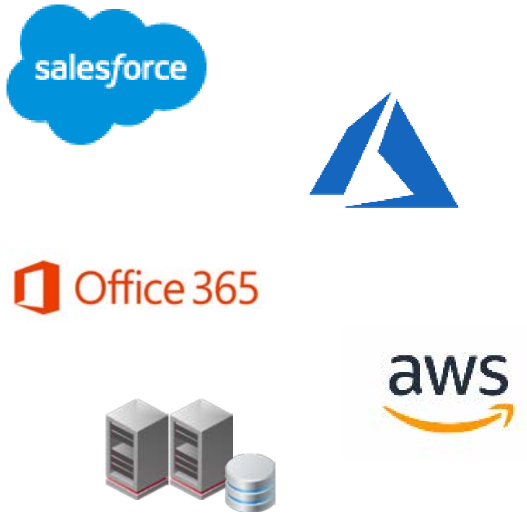
Background for emerging concept of Zero Trust

Flexible working style

Enterprise IT resource everywhere



Office, home, etc.

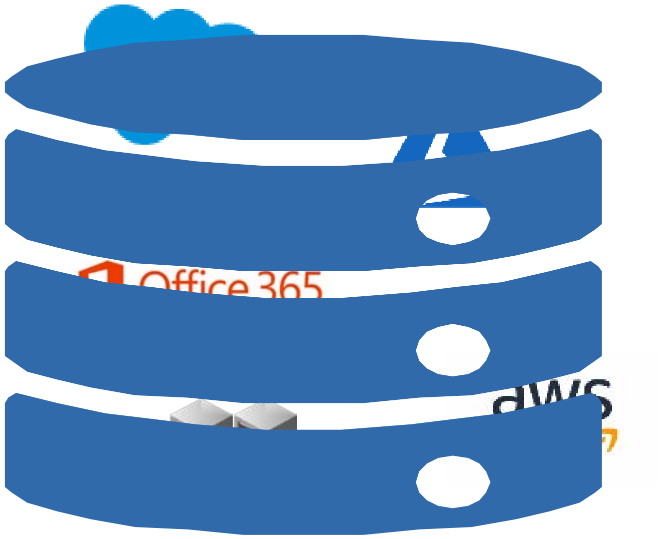

salesforce
Office 365
aws

Cloud, On-premise etc.

Essence of Zero Trust

How to Protect?

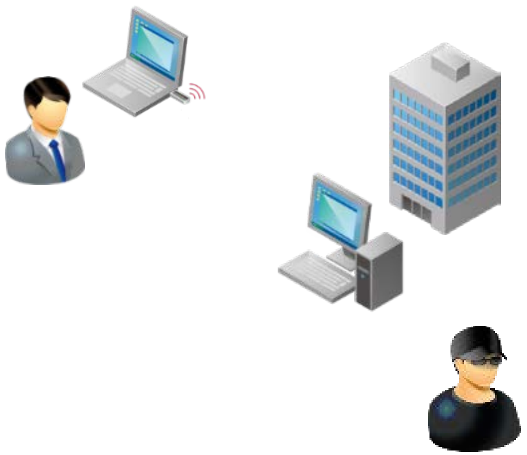
Enterprise IT resource everywhere


Office 365
aws

Data, resource etc.

Essence of Zero Trust

Flexible working style

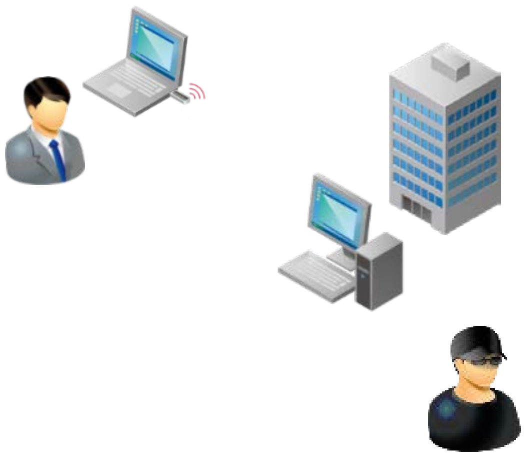


Office, home, etc.

Basically,
Do Not Trust the Origin of Access Point

Essence of Zero Trust

Flexible working style

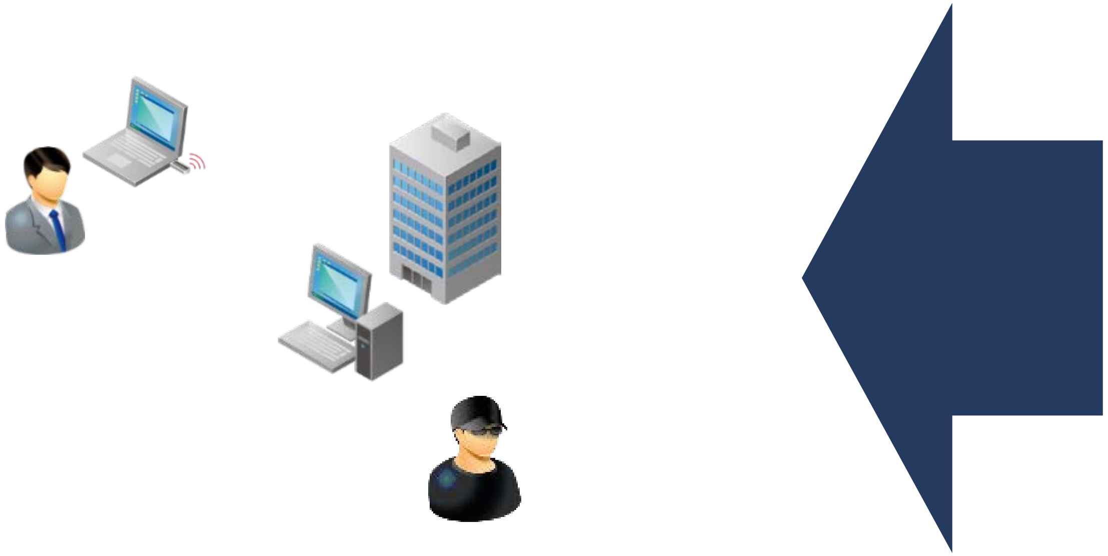


Office, home, etc.

Check the policy every time

Essence of Zero Trust

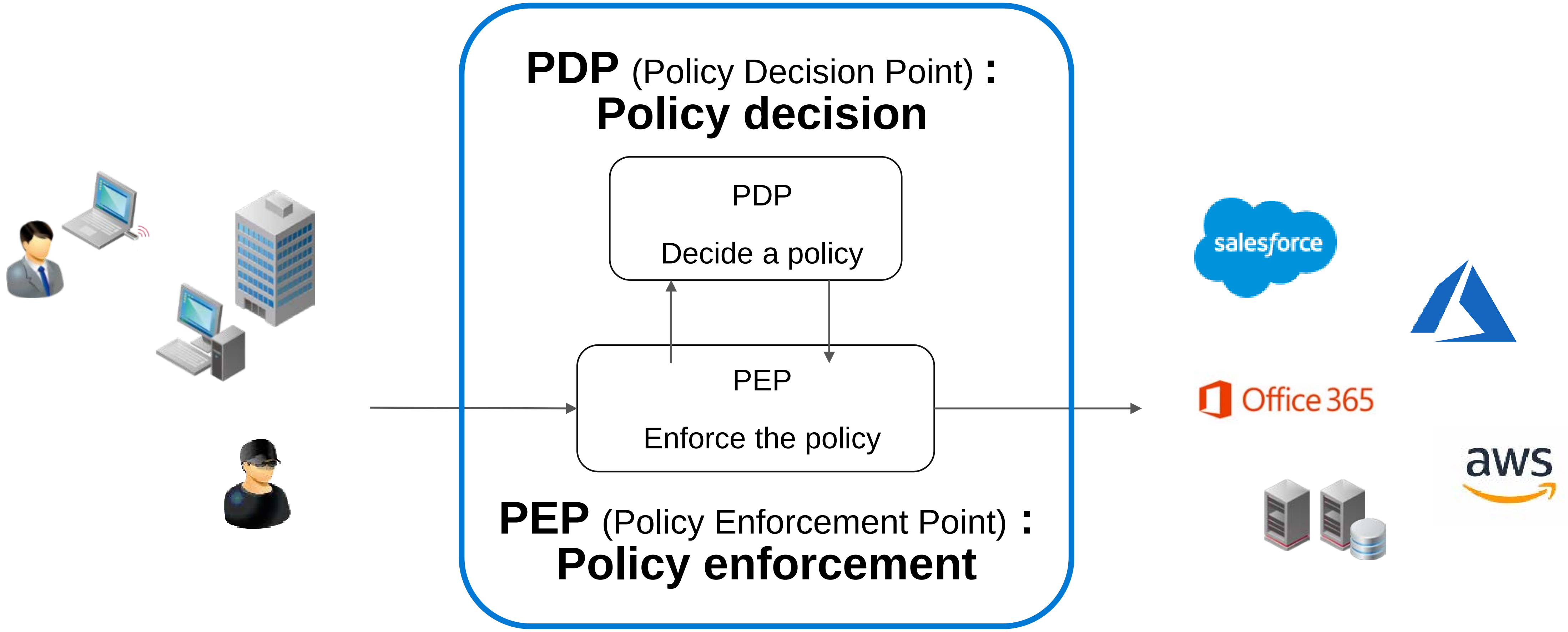
Flexible working style



Approve if match

Office, home, etc.

What you need:



PDP (Policy Decision Point) **:**
Policy decision

PDP

Decide a policy

PEP

Enforce the policy

PEP (Policy Enforcement Point) **:**
Policy enforcement

Concentrate policy decision and enforcement in one place

Basic requirements for Zero Trust

Point) “All” are target for the access destination resource

Point) Do not trust any network location

Point) Check authorization before every session

Point) Dynamically judge authorization in the client’s context

How to determine authorization policies

Basic requirements for Zero Trust

Point) Keep the devices safe

Point) Reflect the status of communications in the policies while always collecting the information

How to operate the authorization policies

➔**Revise/improve the policies based on the collected information**

SASE (Secure Access Service Edge)

Concept proposed by Gartner

Zero Trust based criteria to realize

Define ZTNA (Zero Trust Network Access) to realize PDP/PEP

IIJ Flex Mobility Service/ZTNA

IIJ Flex Mobility Service/ZTNA

Stable VPN

Flexible policies

Stable VPN

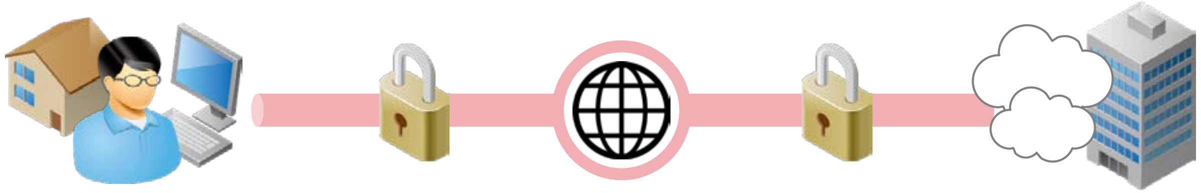
+

ZTNA

Policies

Visualized communications

Reputation



New Flex Mobility Service with enhanced ZTNA functions

Flex Mobility Service /ZTNA Service Menu

Released on
January 31, 2022

Starter

Small start plan

Simple and inexpensive use

*** Succession of FXC**

Items available in this plan:

- Bandwidth: 100Mbps
- Device license: From 100 to 500lic

Released on
January 31, 2022

Core

Enterprise VPN + ZTNA

Comfortable VPN+ZTNA

*** Succession of FXC**

Items available in this plan:

- Bandwidth: From 200Mbps to 2Gbps
- Device license: From 100 to 60,000 lics

To be released in the
end of March 2022

Complete

Digital Experience Monitoring

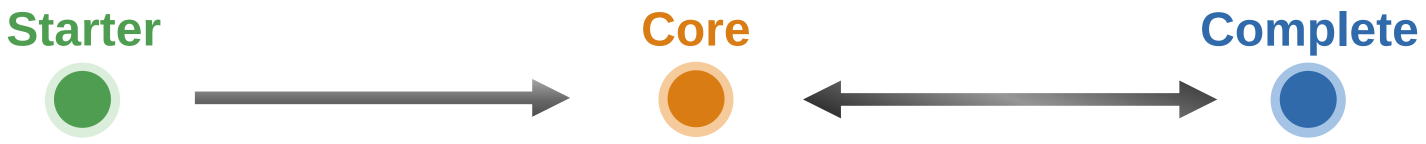
Monitoring function

*** Core+ Visualization**

Items available in this plan:

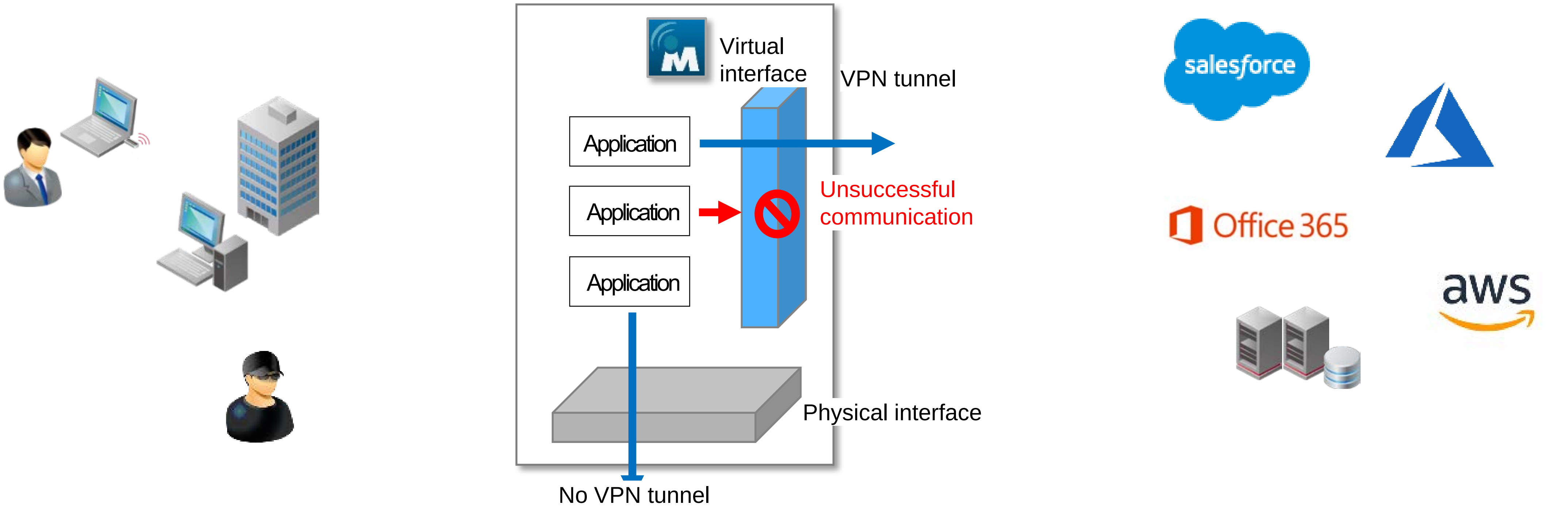
- Bandwidth: From 200Mbps to 2Gbps
- Device license: From 100 to 60,000 lics
- Storage period of visualized logs: 90 days/180 days/360 days

The menu can be changed seamlessly



IIJ Flex Mobility Service

PDP・PEP at Zero Trust Architecture


Virtual
interface
VPN tunnel
Application
Application
Application
Unsuccessful
communication
Physical interface
No VPN tunnel
salesforce
Office 365
aws

Starter Core

Flexible policy control in various contexts

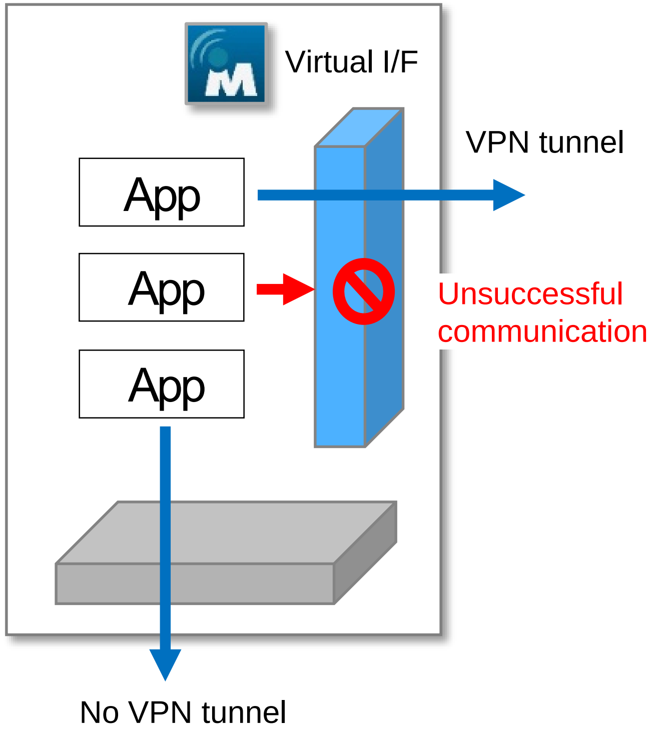
Status

・Policies
SSID /BSSID (Location)
Time
Connection status
Battery
AD group
・・・

・NAC
OS version
Windows program updates
Antivirus programs
・・・

×

Action


Virtual I/F
App
App
App
VPN tunnel
Unsuccessful communication
No VPN tunnel

×

Target (People/device)

Real-time execution on a device

Complete

Provide a function to visualize communications

Conditions

- Location
- Time
- …

In what condition?
For what purpose?

Actions

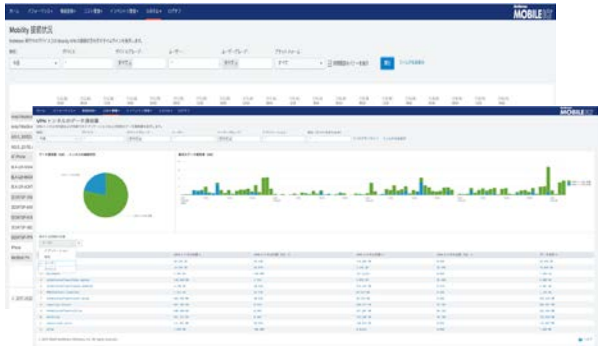
App →

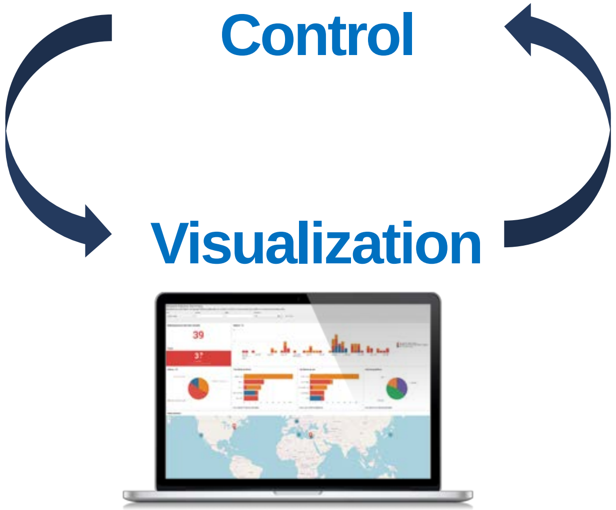
App ↓

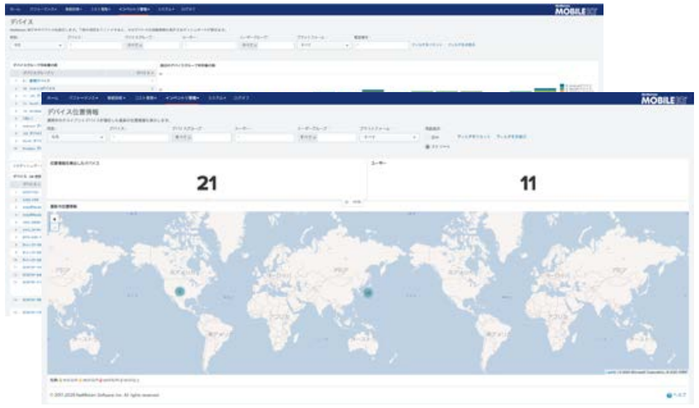
What kind of operation?

Target
(People/device)

Who?

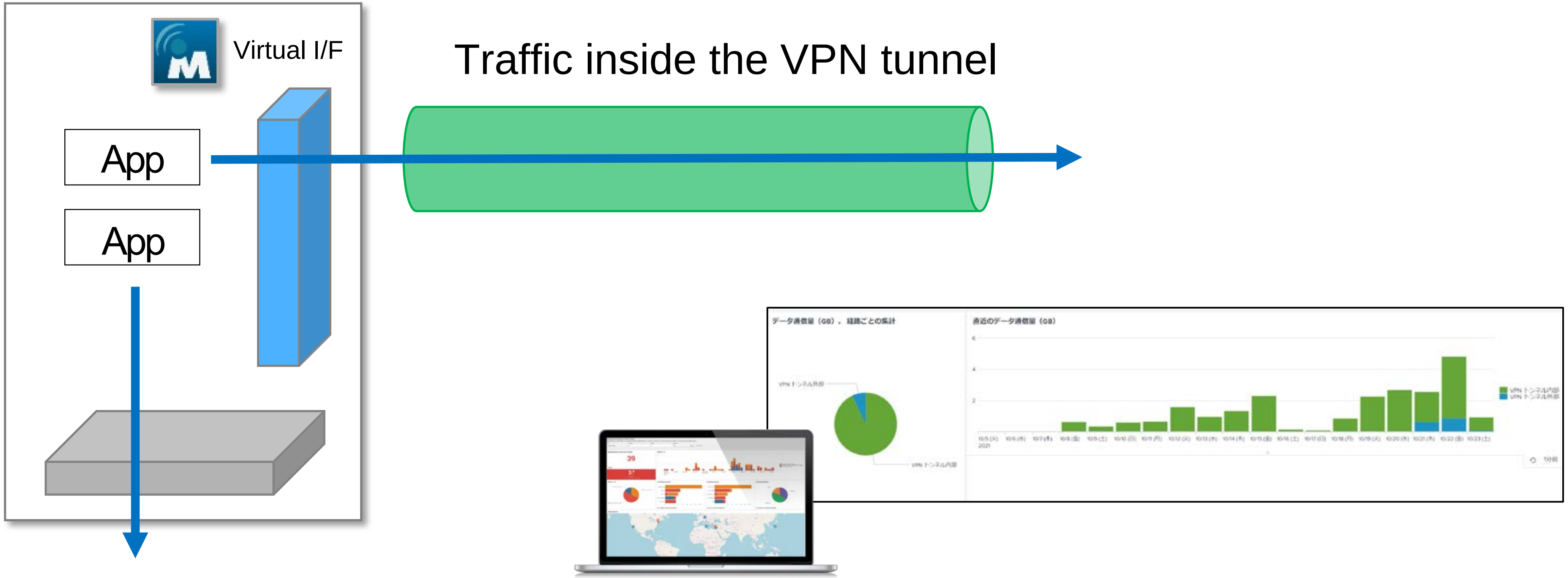



Control
Visualization



Follow the Visualization-Control cycle

Visualization of traffic outside the tunnel, too


Virtual I/F
App
App
Traffic inside the VPN tunnel
データ通信量（GB）、経路ごとの集計
VPNトンネル外部
VPNトンネル内部
直近のデータ通信量（GB）
VPNトンネル内部
VPNトンネル外部

Traffic that is locally broken-out

Visualize/control all the traffic on a device

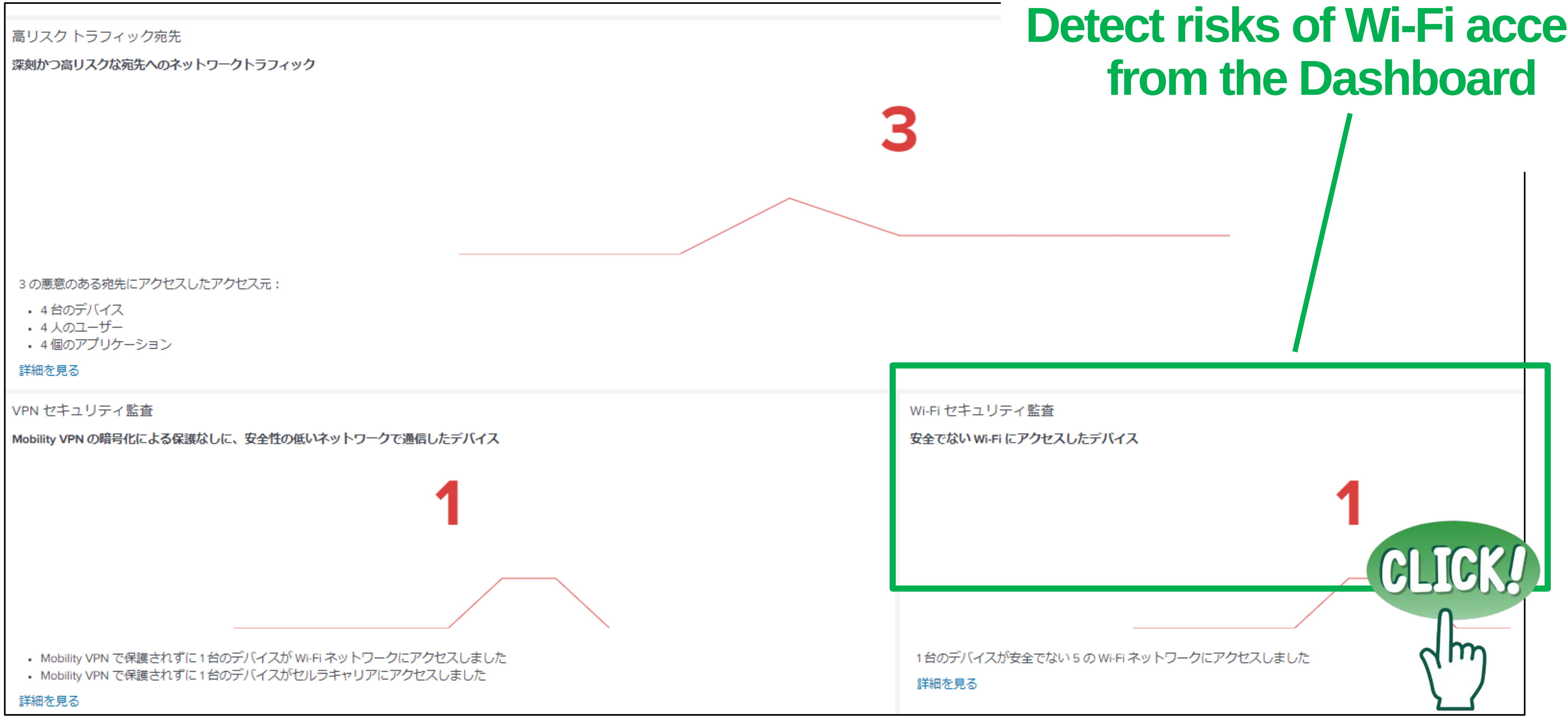
Visualization and Control cycle offered by New IIJ Flex Mobility Service

Security

Control connectivity by visualizing a user’s access situation

Dashboard for Threat Status

Detect risks of Wi-Fi access from the Dashboard



高リスク トラフィック宛先

深刻かつ高リスクな宛先へのネットワークトラフィック

3

3 の悪意のある宛先にアクセスしたアクセス元：

- 4 台のデバイス
- 4 人のユーザー
- 4 個のアプリケーション

詳細を見る

VPN セキュリティ監査

Mobility VPN の暗号化による保護なしに、安全性の低いネットワークで通信したデバイス

1

- Mobility VPN で保護されずに 1 台のデバイスが Wi-Fi ネットワークにアクセスしました
- Mobility VPN で保護されずに 1 台のデバイスがセルラキャリアにアクセスしました

詳細を見る

Wi-Fi セキュリティ監査

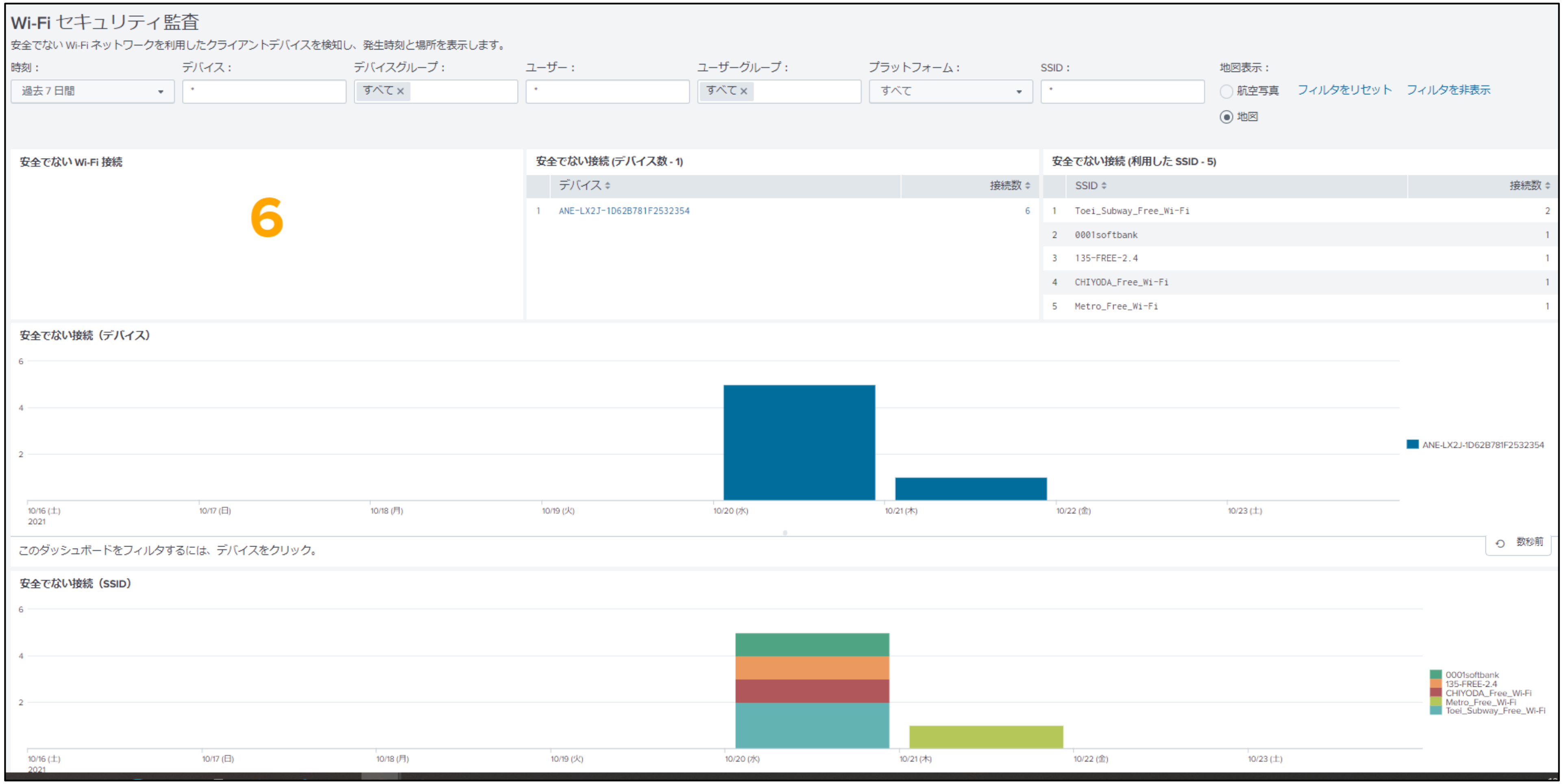
安全でない Wi-Fi にアクセスしたデバイス

1

1 台のデバイスが安全でない 5 の Wi-Fi ネットワークにアクセスしました

詳細を見る

Dashboard for Wi-Fi Security Audit



Wi-Fi セキュリティ監査

安全でない Wi-Fi ネットワークを利用したクライアントデバイスを検知し、発生時刻と場所を表示します。

時刻：過去 7 日間
デバイス：*
デバイスグループ：すべて ×
ユーザー：*
ユーザーグループ：すべて ×
プラットフォーム：すべて
SSID：*
地図表示：○ 航空写真 ● 地図

フィルタをリセット
フィルタを非表示

安全でない Wi-Fi 接続

6

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

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

安全でない接続（デバイス）

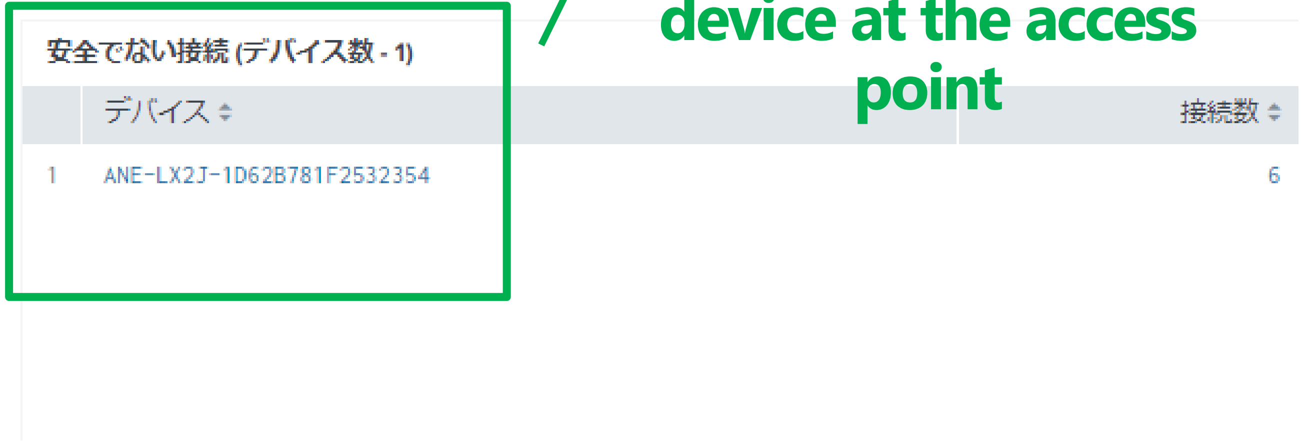
6
4
2
10/16 (土)
2021
10/17 (日)
10/18 (月)
10/19 (火)
10/20 (水)
10/21 (木)
10/22 (金)
10/23 (土)
ANE-LX2J-1D62B781F2532354

このダッシュボードをフィルタするには、デバイスをクリック。

安全でない接続（SSID）

6
4
2
10/16 (土)
2021
10/17 (日)
10/18 (月)
10/19 (火)
10/20 (水)
10/21 (木)
10/22 (金)
10/23 (土)
0001softbank
135-FREE-2.4
CHIYODA_Free_Wi-Fi
Metro_Free_Wi-Fi
Toei_Subway_Free_Wi-Fi

Monitor entire access situation with potential risks

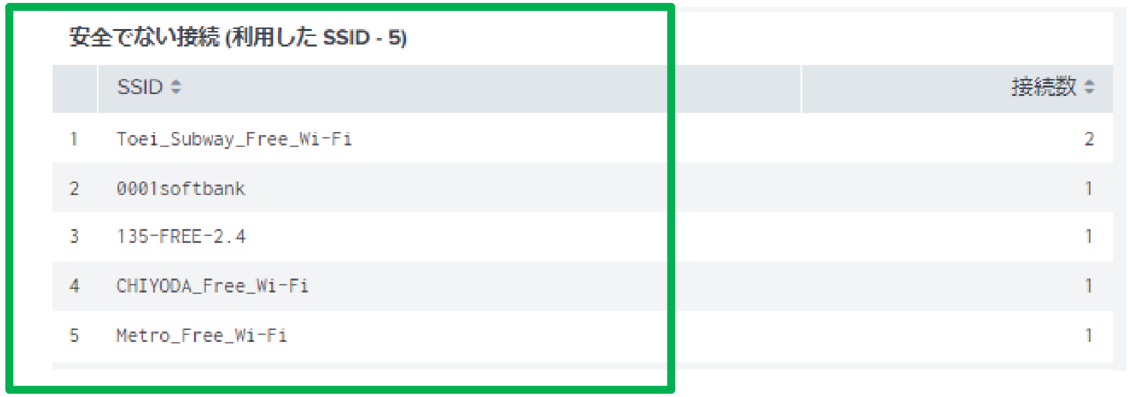


Specify the name of a device at the access point

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

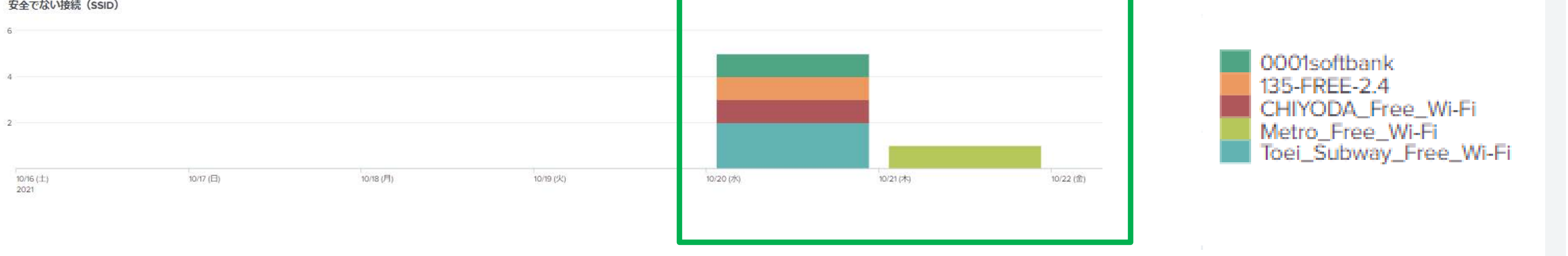
Specify the SSID at the access point



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

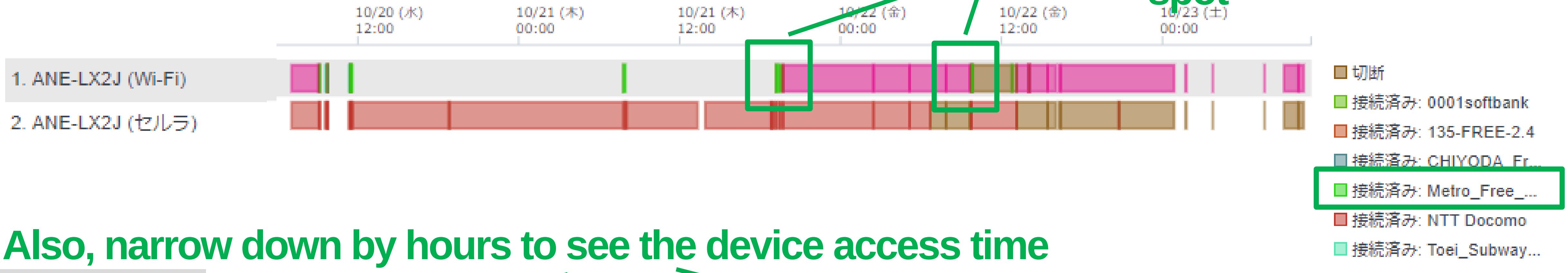
Specify the date of access



Detected that a certain device accessing Free Wi-Fi like access point

Status of a device

Specify the time when accessed Wi-Fi spot

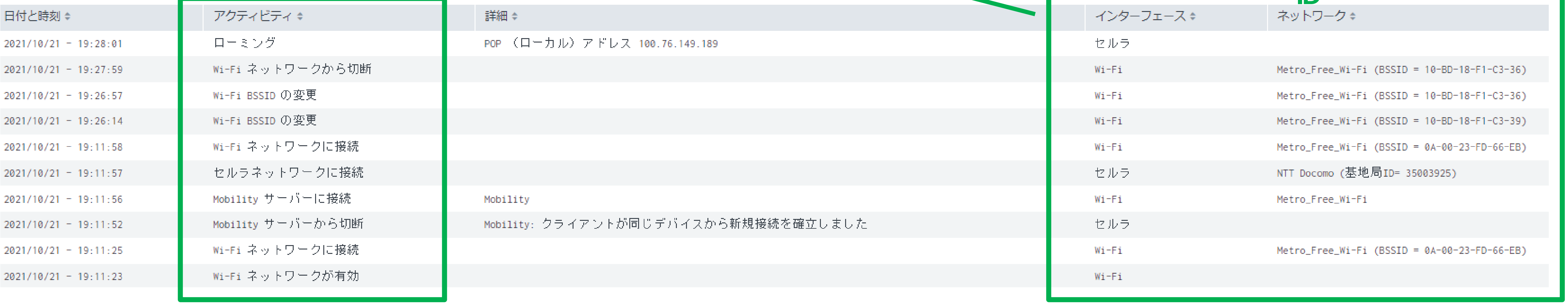


Also, narrow down by hours to see the device access time line

Activity log

Activity

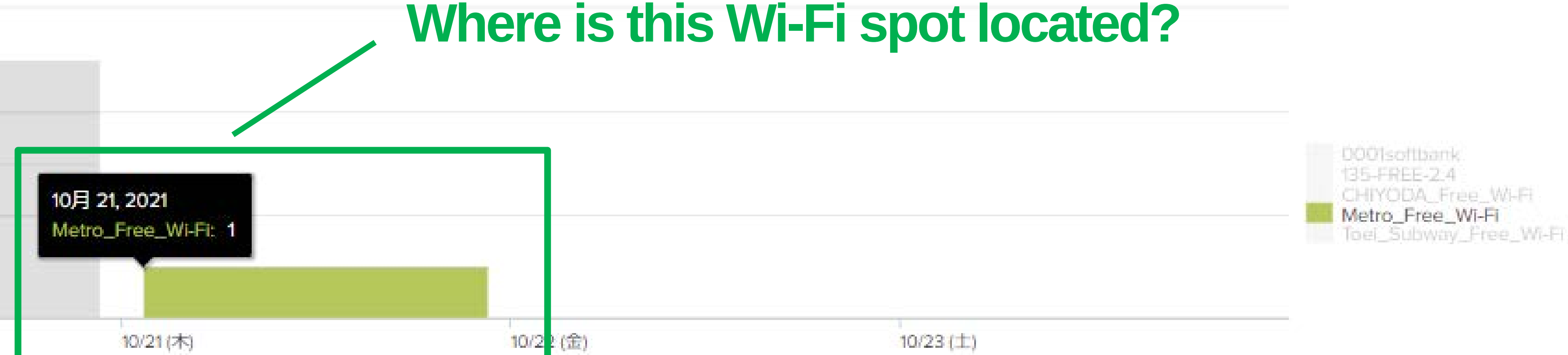
Wi-Fi spot (SSID, BSSID), base station ID



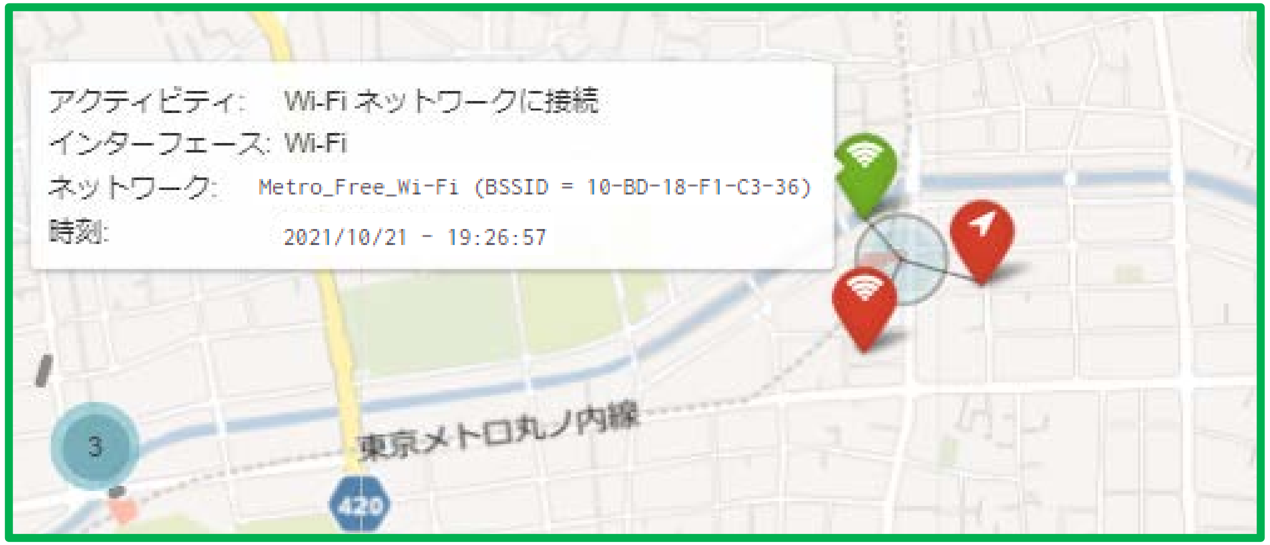
日付と時刻	アクティビティ	詳細	インターフェース	ネットワーク
2021/10/21 - 19:28:01	ローミング	POP （ローカル）アドレス 100.76.149.189	セルラ	
2021/10/21 - 19:27:59	Wi-Fi ネットワークから切断		Wi-Fi	Metro_Free_Wi-Fi (BSSID = 10-BD-18-F1-C3-36)
2021/10/21 - 19:26:57	Wi-Fi BSSID の変更		Wi-Fi	Metro_Free_Wi-Fi (BSSID = 10-BD-18-F1-C3-36)
2021/10/21 - 19:26:14	Wi-Fi 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	

Can it be a vehicle if such is frequently changing BSSID for the same Wi-Fi?

Where is this Wi-Fi spot located?

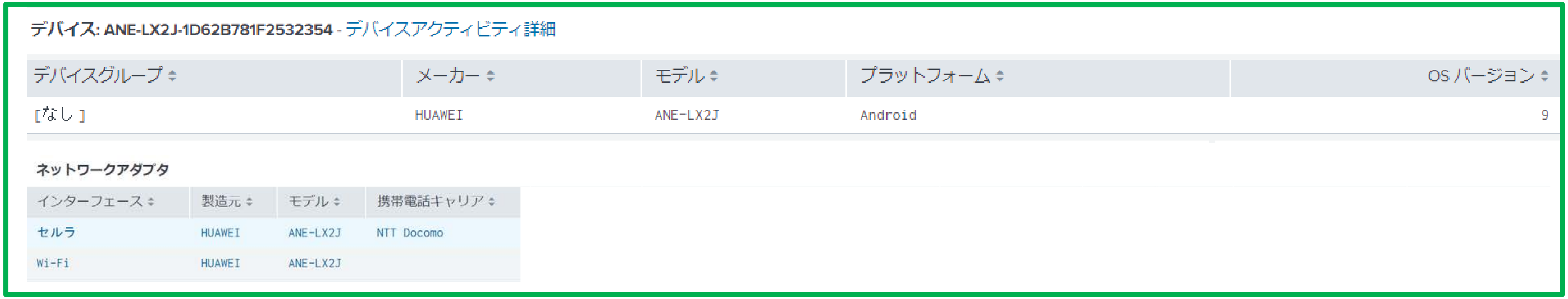

10月 21, 2021
Metro_Free_Wi-Fi: 1

From the access map, learned that it is a subway's Wi-Fi


アクティビティ: Wi-Fi ネットワークに接続
インターフェース: Wi-Fi
ネットワーク: Metro_Free_Wi-Fi (BSSID = 10-BD-18-F1-C3-36)
時刻: 2021/10/21 - 19:26:57

Conclusion:
A certain Android device was connecting to subway's free Wi-Fi spot when moving

Check the details of a device at the origin of access

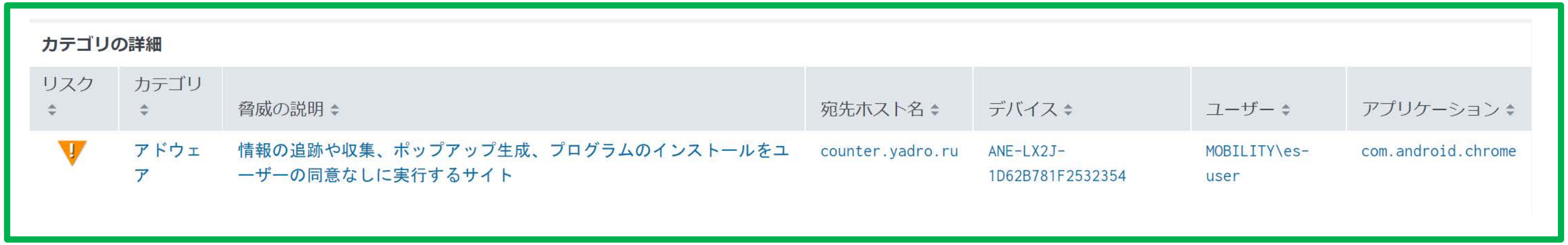


デバイス: ANE-LX2J-1D62B781F2532354 - デバイスアクティビティ詳細

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	

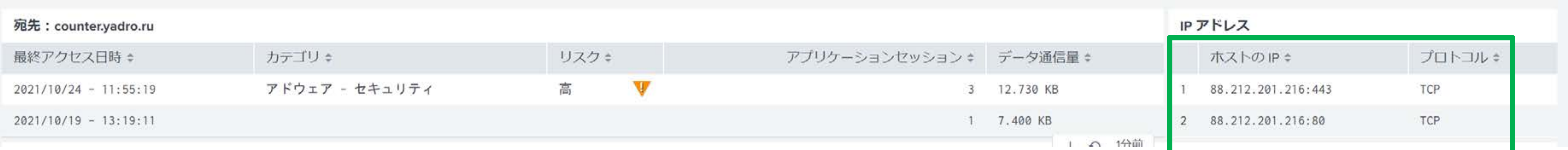


カテゴリの詳細

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

Check where the device accessed

This Android device is accessing via chrome to a Adware website that is highly risky!!



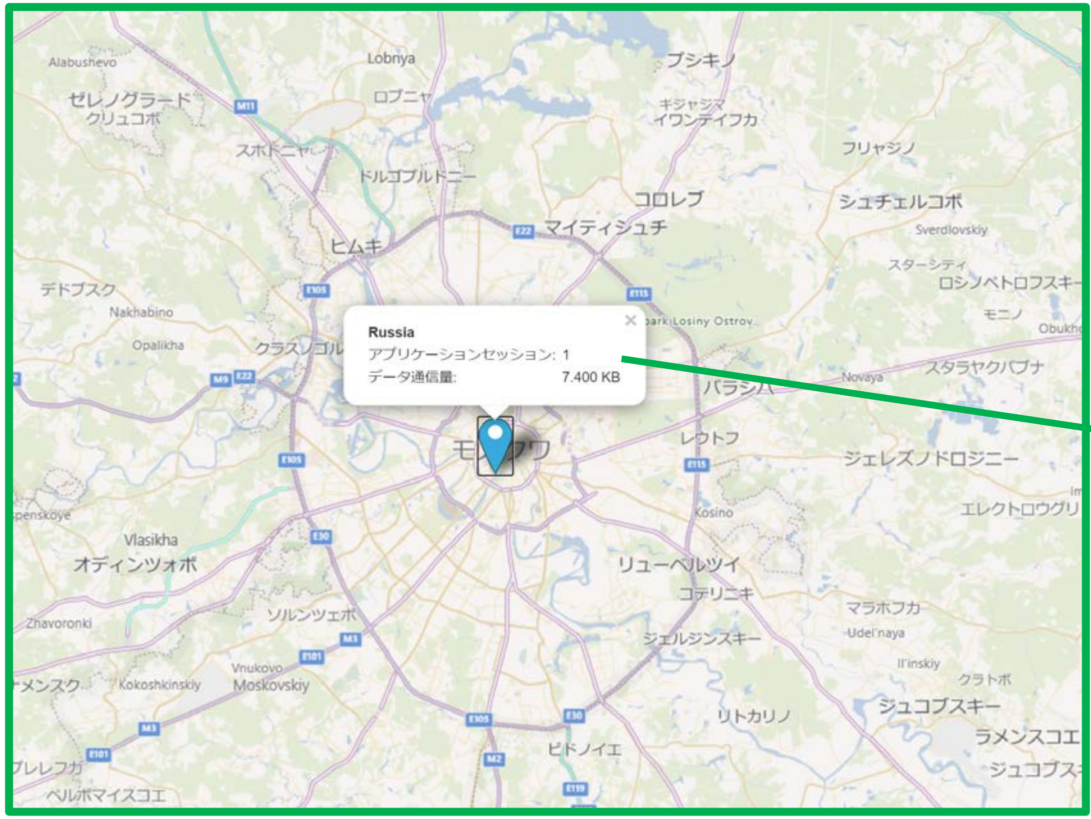
宛先：counter.yadro.ru

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

IP address of destination host:
Learned about the port



Russia
アプリケーションセッション: 1
データ通信量: 7.400 KB

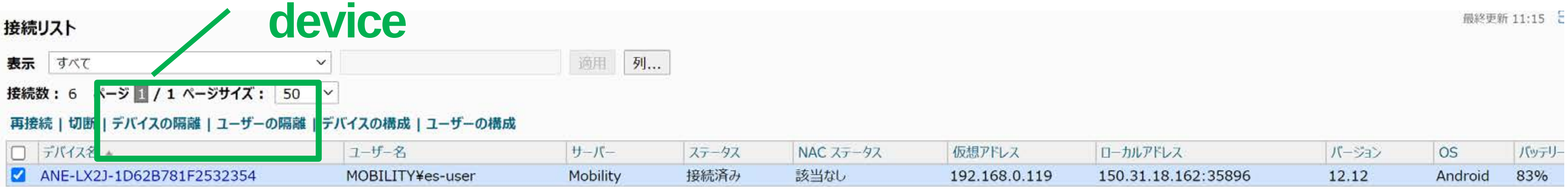
Lobnya
ブシキノ
Alabushevo
ゼレノグラード
クリュコボ
ロブニャ
キジャジマ
イワンティフカ
スホドニャ
フリャジノ
ドルゴプルドニー
コロレブ
シュチェルコボ
マイティシュチ
ヒムキ
Sverdlovskiy
スターシティ
デドフスク
ロシノペトロフスキー
Nakhabino
モニノ
Opalikha
クラスノゴルスク
Obukhovo
スタラヤクパブナ
Novaya
バラシハ
モスクワ
レウトフ
ジェレズノドロジニー
エレクトロウグリ
Vlasikha
Kosino
オディンツォボ
リューベルツイ
コテリニキ
ソルンツェボ
Zhavoronki
マラホフカ
Udel'naya
ジェルジンスキー
Il'inskiy
Vnukovo
Moskovskiy
Kokoshkinskiy
クラトボ
ジュコフスキー
リトカリノ
ラメンスコエ
ビドノイエ
アプレレフカ
ペルボマイスコエ

Learned about the host destination area from the map

Learned about the access point by using IP location!!

Updating Action and Policy

1st step: isolate the device



接続リスト

最終更新 11:15

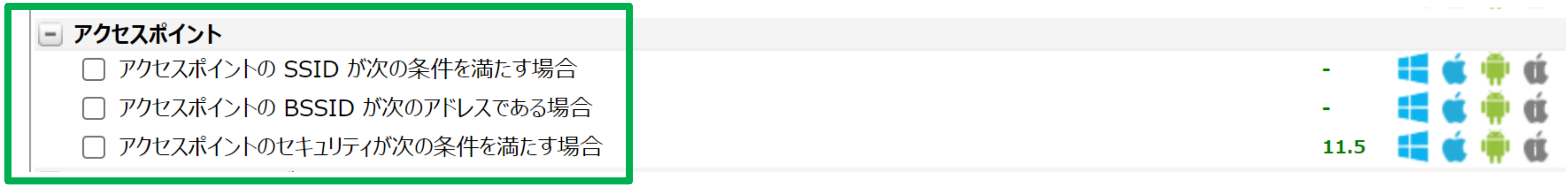
表示 すべて ⌄ 適用 列...

接続数： 6 ページ 1 / 1 ページサイズ： 50 ⌄

再接続 | 切断 | デバイスの隔離 | ユーザーの隔離 | デバイスの構成 | ユーザーの構成

☐	デバイス名	ユーザー名	サーバー	ステータス	NAC ステータス	仮想アドレス	ローカルアドレス	バージョン	OS	バッテリー
☑	ANE-LX2J-1D62B781F2532354	MOBILITY¥es-user	Mobility	接続済み	該当なし	192.168.0.119	150.31.18.162:35896	12.12	Android	83%

2nd step: Set up a policy to block unencrypted Wi-Fi access point



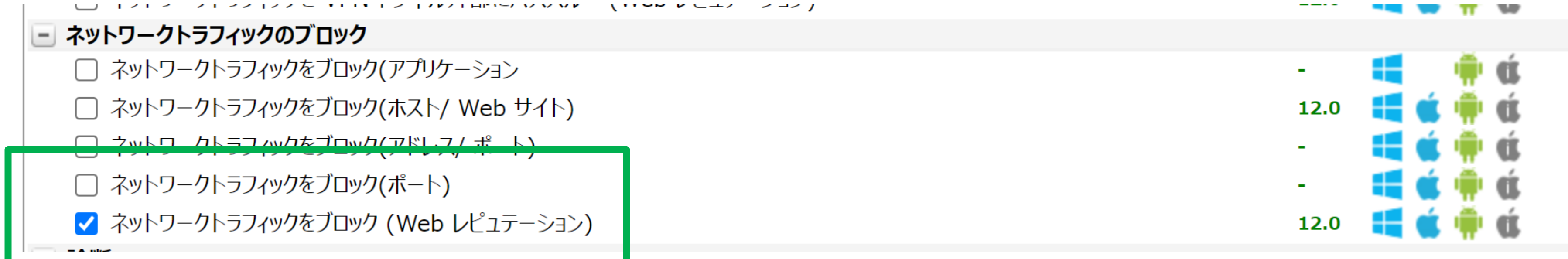
アクセスポイント

- ☐ アクセスポイントの SSID が次の条件を満たす場合 -
- ☐ アクセスポイントの BSSID が次のアドレスである場合 -
- ☐ アクセスポイントのセキュリティが次の条件を満たす場合 11.5

※Additionally, we could think about having the entire communication into VPN tunnel to encrypt etc.

Review connectivity policy based on gathered traffic information

Updating Action and Policy



ネットワークトラフィックのブロック

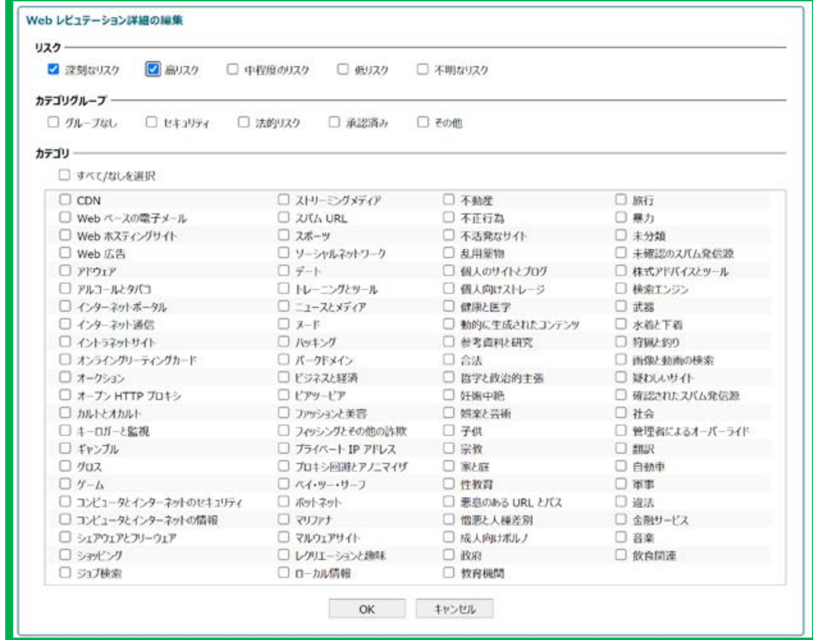
☐ ネットワークトラフィックをブロック(アプリケーション) -

☐ ネットワークトラフィックをブロック(ホスト/ Web サイト) 12.0

☐ ネットワークトラフィックをブロック(アドレス/ ポート) -

☐ ネットワークトラフィックをブロック(ポート) -

☑ ネットワークトラフィックをブロック (Web レピュテーション) 12.0



Web レピュテーション詳細の編集

リスク

☑ 深刻なリスク ☑ 高リスク ☐ 中程度のリスク ☐ 低リスク ☐ 不明なリスク

カテゴリグループ

☐ グループなし ☐ セキュリティ ☐ 法的リスク ☐ 承認済み ☐ その他

カテゴリ

☐ すべて/なしを選択

☐ CDN
☐ Web ベースの電子メール
☐ Web ホスティングサイト
☐ Web 広告
☐ アドウェア
☐ アルコールとタバコ
☐ インターネットポータル
☐ インターネット通信
☐ イントラネットサイト
☐ オンライングリーティングカード
☐ オークション
☐ オープン HTTP プロキシ
☐ カルトとオカルト
☐ キーロガーと監視
☐ ギャンブル
☐ グロス
☐ ゲーム
☐ コンピュータとインターネットのセキュリティ
☐ コンピュータとインターネットの情報
☐ シェアウェアとフリーウェア
☐ ショッピング
☐ ジョブ検索
☐ ストリーミングメディア
☐ スパム URL
☐ スポーツ
☐ ソーシャルネットワーク
☐ デート
☐ トレーニングとツール
☐ ニュースとメディア
☐ ヌード
☐ ハッキング
☐ パークドメイン
☐ ビジネスと経済
☐ ピアツーピア
☐ ファッションと美容
☐ フィッシングとその他の詐欺
☐ プライベート IP アドレス
☐ プロキシ回避とアノニマイザ
☐ ペイ・ツー・サーフ
☐ ボットネット
☐ マリファナ
☐ マルウェアサイト
☐ レクリエーションと趣味
☐ ローカル情報
☐ 不動産
☐ 不正行為
☐ 不活発なサイト
☐ 乱用薬物
☐ 個人のサイトとブログ
☐ 個人向けストレージ
☐ 健康と医学
☐ 動的に生成されたコンテンツ
☐ 参考資料と研究
☐ 合法
☐ 哲学と政治的主張
☐ 妊娠中絶
☐ 娯楽と芸術
☐ 子供
☐ 宗教
☐ 家と庭
☐ 性教育
☐ 悪意のある URL とパス
☐ 憎悪と人種差別
☐ 成人向けポルノ
☐ 政府
☐ 教育機関
☐ 旅行
☐ 暴力
☐ 未分類
☐ 未確認のスパム発信源
☐ 株式アドバイスとツール
☐ 検索エンジン
☐ 武器
☐ 水着と下着
☐ 狩猟と釣り
☐ 画像と動画の検索
☐ 疑わしいサイト
☐ 確認されたスパム発信源
☐ 社会
☐ 管理者によるオーバーライド
☐ 翻訳
☐ 自動車
☐ 軍事
☐ 違法
☐ 金融サービス
☐ 音楽
☐ 飲食関連

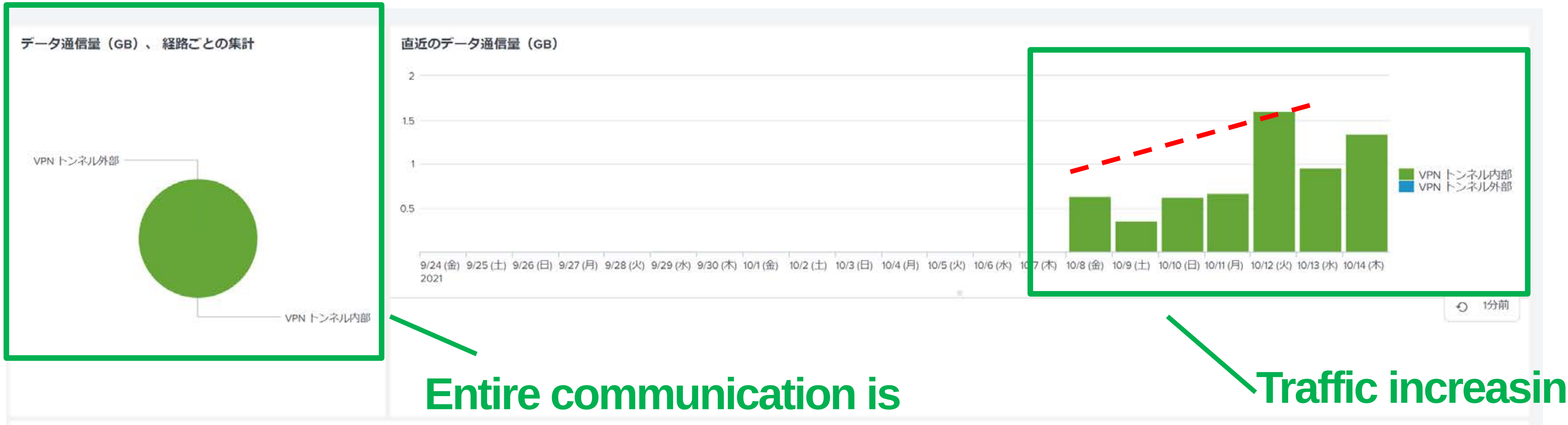
Set up policy that blocks access by designating risks and categories

Review security policy based on gathered traffic information

Learn about Network Bottlenecks

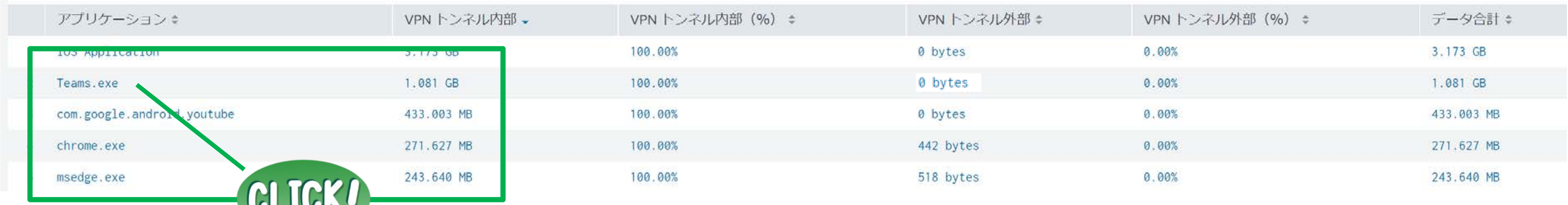
Control communication by visualizing VPN traffic situation

Dashboard for VPN communication situation


データ通信量（GB）、経路ごとの集計
VPN トンネル外部
VPN トンネル内部
直近のデータ通信量（GB）
2
1.5
1
0.5
9/24 (金)
2021
9/25 (土)
9/26 (日)
9/27 (月)
9/28 (火)
9/29 (水)
9/30 (木)
10/1 (金)
10/2 (土)
10/3 (日)
10/4 (月)
10/5 (火)
10/6 (水)
7 (木)
10/8 (金)
10/9 (土)
10/10 (日)
10/11 (月)
10/12 (火)
10/13 (水)
10/14 (木)
🟩 VPN トンネル内部
🟦 VPN トンネル外部
1分前

Entire communication is located inside of VPN tunnel

Traffic increasing?!

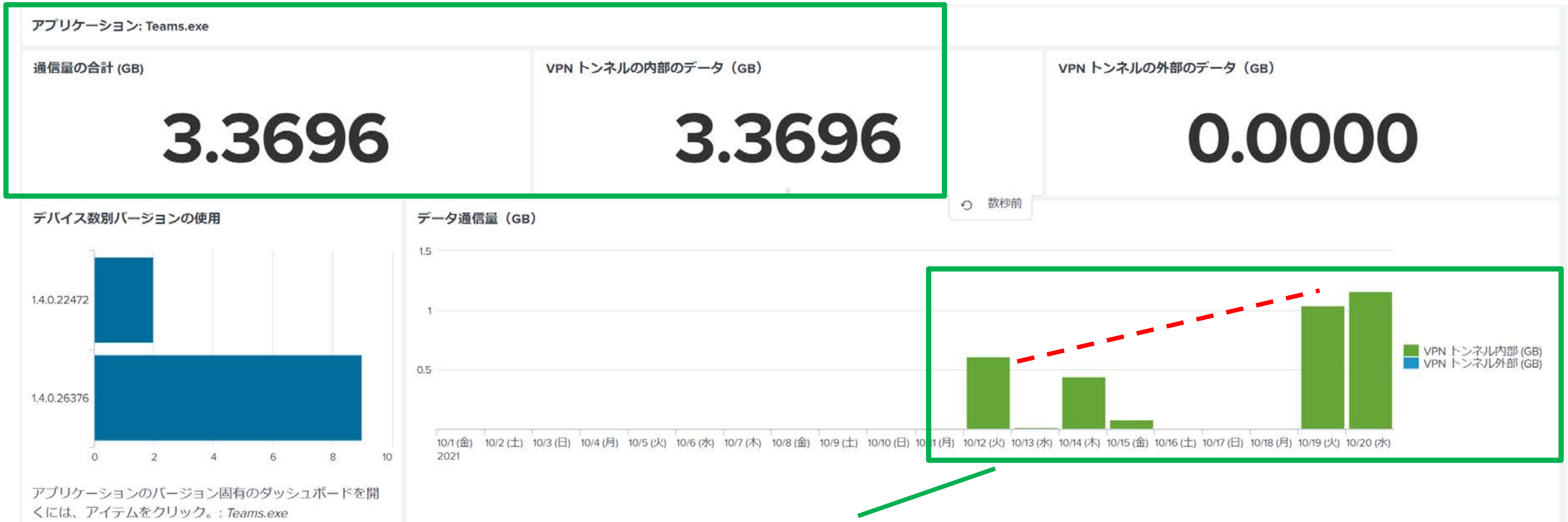


アプリケーション	VPN トンネル内部	VPN トンネル内部（%）	VPN トンネル外部	VPN トンネル外部（%）	データ合計
iOS Application	3.173 GB	100.00%	0 bytes	0.00%	3.173 GB
Teams.exe	1.081 GB	100.00%	0 bytes	0.00%	1.081 GB
com.google.android.youtube	433.003 MB	100.00%	0 bytes	0.00%	433.003 MB
chrome.exe	271.627 MB	100.00%	442 bytes	0.00%	271.627 MB
msedge.exe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

Check to see from Teams, the application using the most traffic

Data traffic volume within VPN tunnel

Gather information about traffics for Teams



アプリケーション: Teams.exe

通信量の合計 (GB)	VPN トンネルの内部のデータ（GB）	VPN トンネルの外部のデータ（GB）
3.3696	3.3696	0.0000

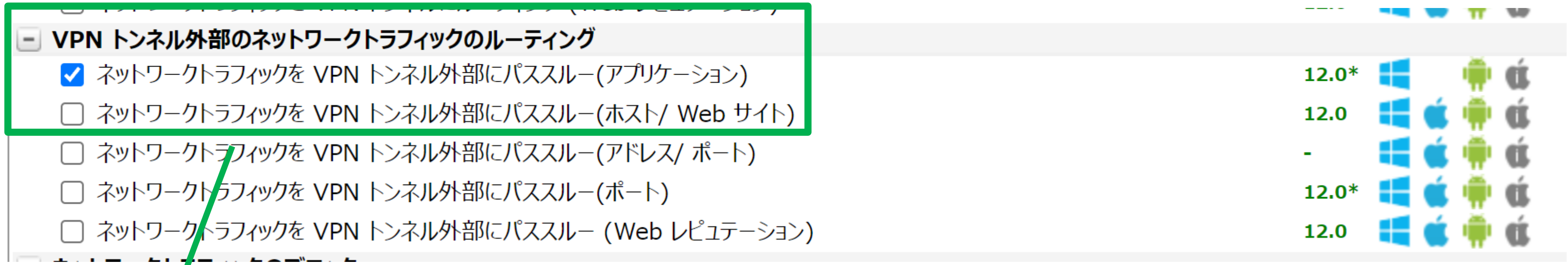
数秒前
デバイス数別バージョンの使用
1.4.0.22472
1.4.0.26376
0
2
4
6
8
10
データ通信量（GB）
1.5
1
0.5
10/1 (金)
2021
10/2 (土)
10/3 (日)
10/4 (月)
10/5 (火)
10/6 (水)
10/7 (木)
10/8 (金)
10/9 (土)
10/10 (日)
10 1 (月)
10/12 (火)
10/13 (水)
10/14 (木)
10/15 (金)
10/16 (土)
10/17 (日)
10/18 (月)
10/19 (火)
10/20 (水)
🟩 VPN トンネル内部 (GB)
🟦 VPN トンネル外部 (GB)

アプリケーションのバージョン固有のダッシュボードを開くには、アイテムをクリック。: *Teams.exe*

Traffics for Teams are suddenly increasing!

Before bottlenecks are realized, consider split tunnel

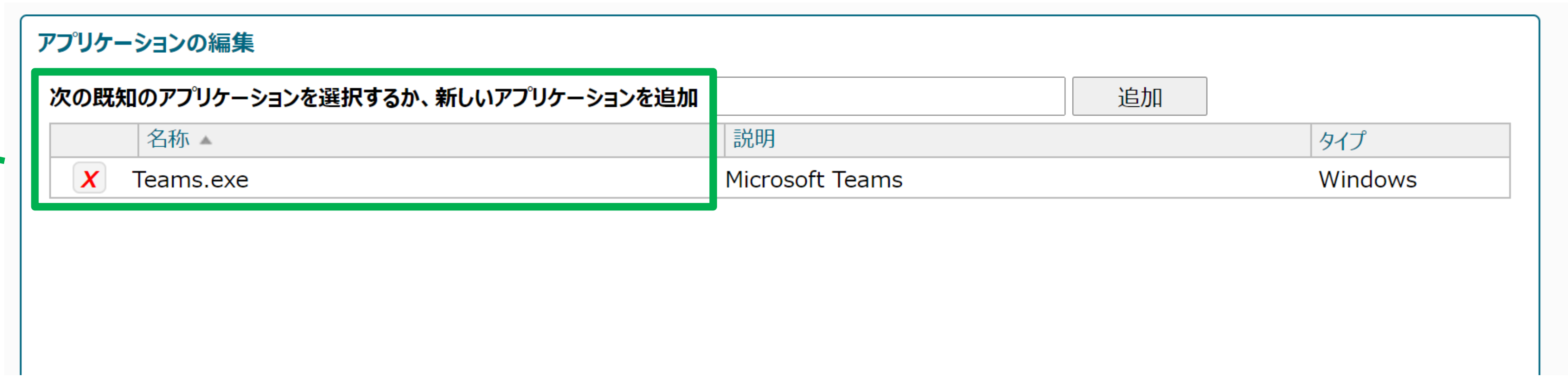
Updating Action and Policy



VPN トンネル外部のネットワークトラフィックのルーティング

☑	ネットワークトラフィックを VPN トンネル外部にパススルー(アプリケーション)	12.0*
☐	ネットワークトラフィックを VPN トンネル外部にパススルー(ホスト/ Web サイト)	12.0
☐	ネットワークトラフィックを VPN トンネル外部にパススルー(アドレス/ ポート)	-
☐	ネットワークトラフィックを VPN トンネル外部にパススルー(ポート)	12.0*
☐	ネットワークトラフィックを VPN トンネル外部にパススルー (Web レピュテーション)	12.0

Pick Teams Application and check pass-through at outside VPN setting



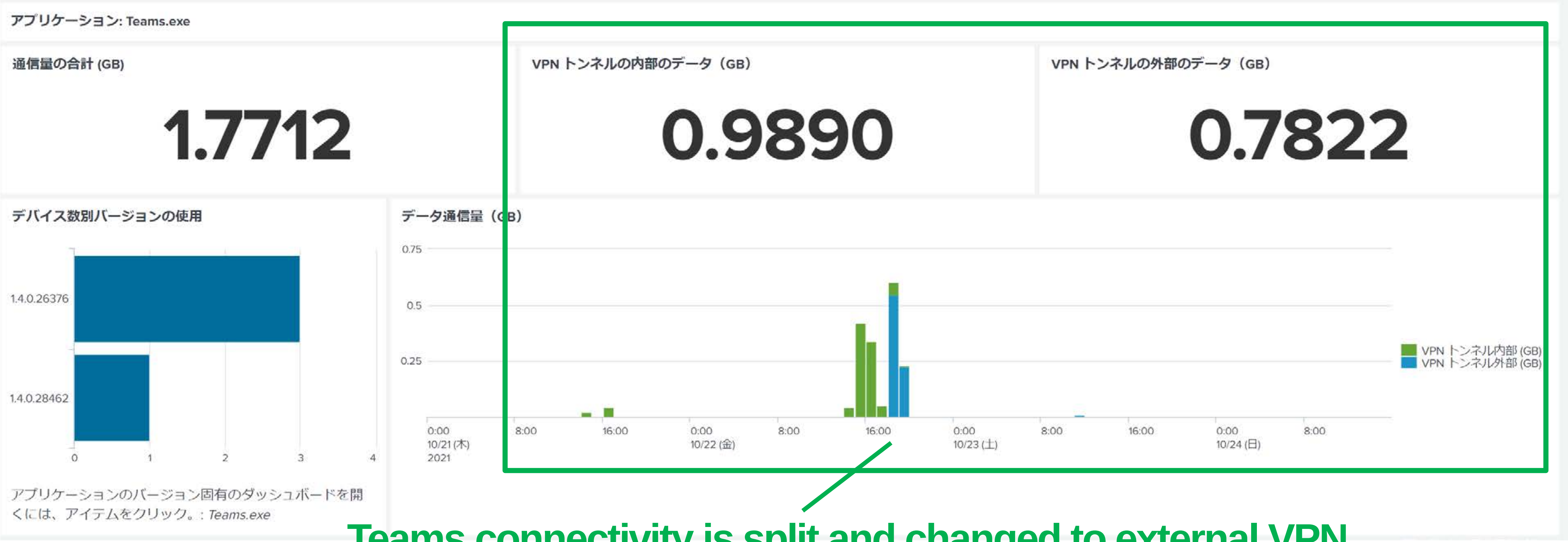
アプリケーションの編集

次の既知のアプリケーションを選択するか、新しいアプリケーションを追加

名称	説明	タイプ
Teams.exe	Microsoft Teams	Windows

Review connectivity policy based on gathered traffic information

Data traffic volume within VPN tunnel



アプリケーション: Teams.exe

通信量の合計 (GB)

1.7712

VPN トンネルの内部のデータ（GB）

0.9890

VPN トンネルの外部のデータ（GB）

0.7822

デバイス数別バージョンの使用

1.4.0.26376
1.4.0.28462
0
1
2
3
4

アプリケーションのバージョン固有のダッシュボードを開くには、アイテムをクリック。: *Teams.exe*

データ通信量（GB）

0.75
0.5
0.25
0:00
10/21 (木)
2021
8:00
16:00
0:00
10/22 (金)
8:00
16:00
0:00
10/23 (土)
8:00
16:00
0:00
10/24 (日)
8:00
🟩 VPN トンネル内部 (GB)
🟦 VPN トンネル外部 (GB)

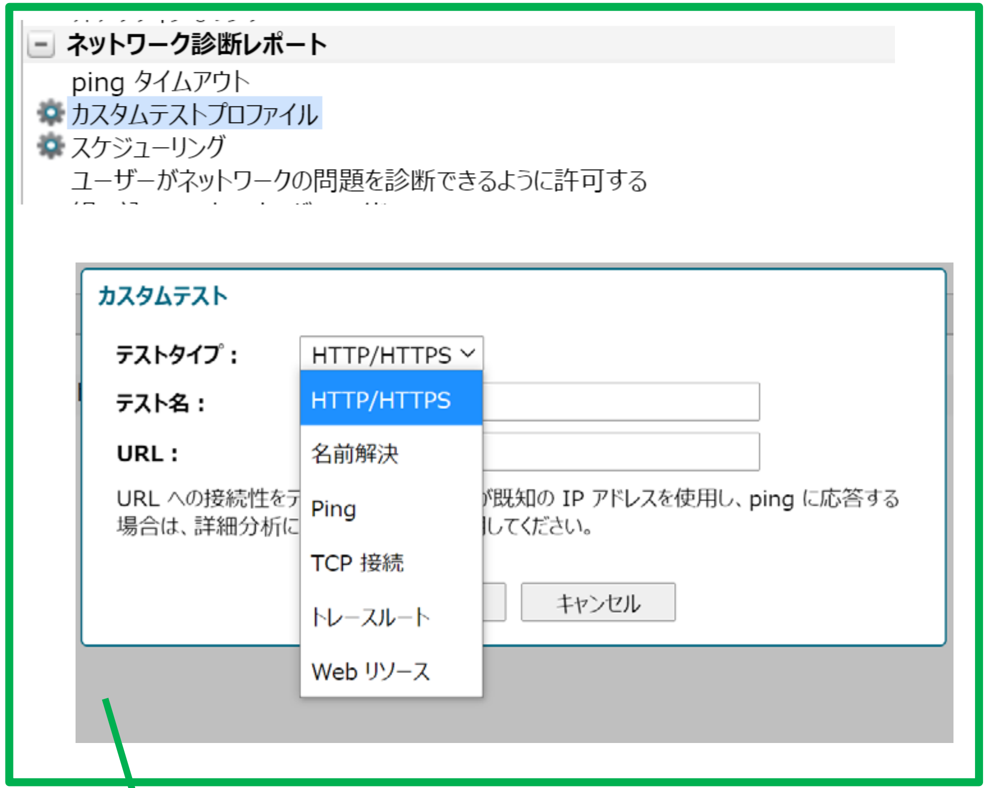
Teams connectivity is split and changed to external VPN

Able to prevent bottle neck risks!!

Trouble shooting

User inquires about “unstable connectivity”

Connectivity test from a user setting

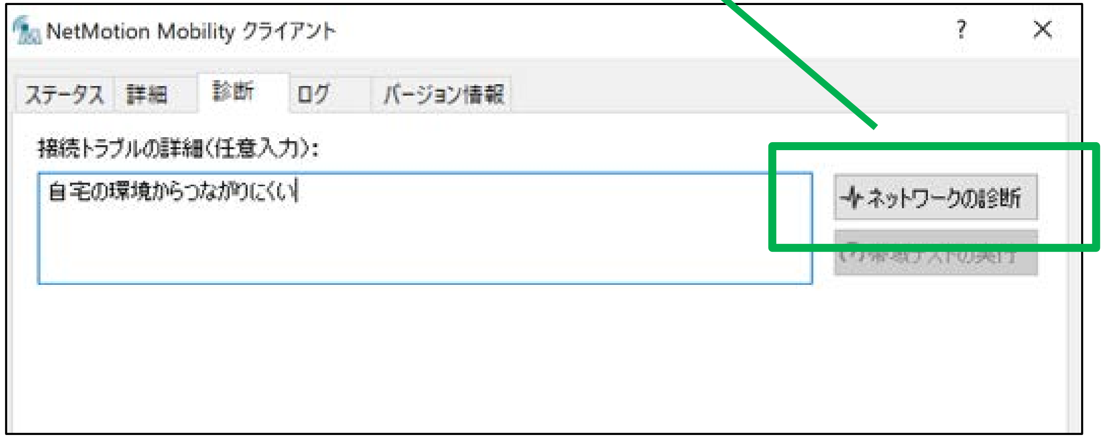

ネットワーク診断レポート
ping タイムアウト
カスタムテストプロファイル
スケジューリング
カスタムテスト
テストタイプ：
HTTP/HTTPS
HTTP/HTTPS
名前解決
Ping
TCP 接続
トレースルート
Web リソース
テスト名：
URL：
キャンセル

ユーザーがネットワークの問題を診断できるように許可する

URL への接続性をテ が既知の IP アドレスを使用し、ping に応答する
場合は、詳細分析に してください。

Administrator arranges test

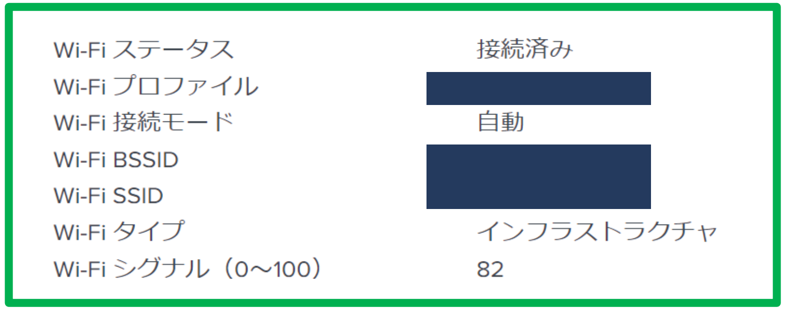
Once a user clicks on a "check Network," connectivity test is implemented


NetMotion Mobility クライアント
?
ステータス
詳細
診断
ログ
バージョン情報
ネットワークの診断

接続トラブルの詳細(任意入力):

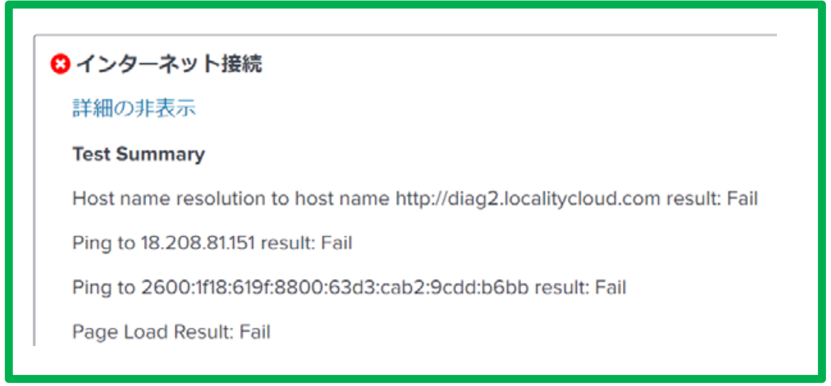
自宅の環境からつながりにくい

No issue at Wi-Fi signal level



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	[redacted]
Wi-Fi タイプ	インフラストラクチャ
Wi-Fi シグナル（0～100）	82

Failed to Ping Traceroute at the designated host



インターネット接続

詳細の非表示

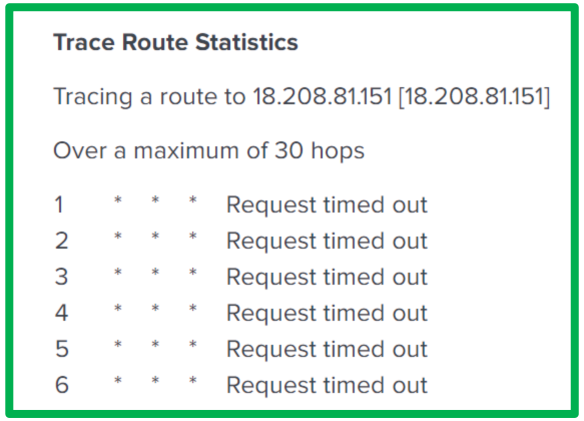
Test Summary

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
```

Seems like my home Internet connectivity is the issue…

Trouble shooting based on connectivity test

What issues of teleworking will come up to the surface in the future?

Security Department
Information Systems Department

Security

Information Systems Department

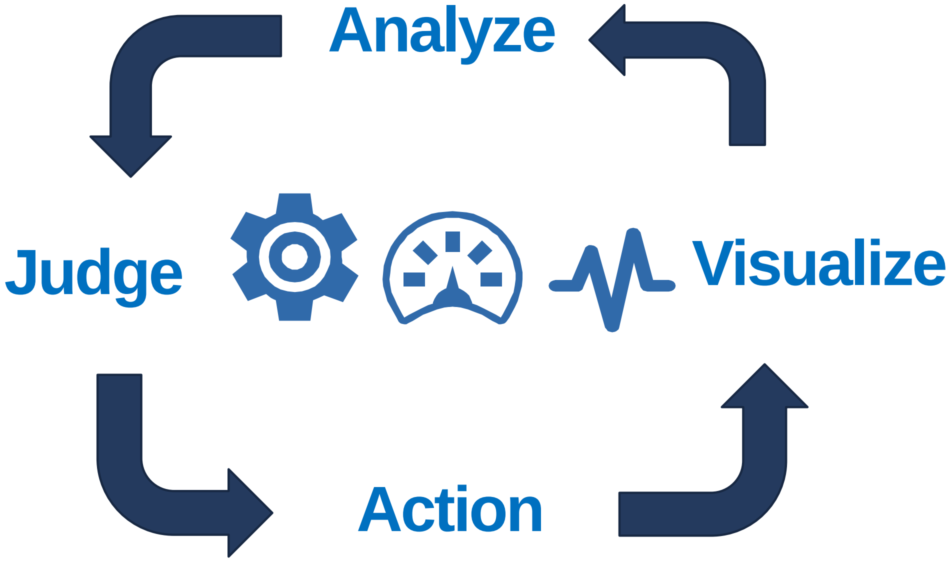
Network bottleneck

Employees
Information Systems Department

Troubleshooting

Solve them with the new Flex Mobility

Visualize status of communications and security status


Analyze
Judge
Visualize
Action

Follow the Visualization <-> Action cycle

IIJ
Internet Initiative Japan

The internet started in Japan in 1992, along with IIJ. Since that time, the IIJ Group has been building the infrastructure for a networked society, and with our technical expertise, we have continued to support its development. We have also continued to evolve our vision for the future and innovate to make it a reality. As an internet pioneer, IIJ has blazed the trail so that others could realize the full potential of a networked society, and that will never change. The middle "I" in "IIJ" stands for "initiative," and IIJ alway starts with the future.

Disclaimer

Statements made in this presentation regarding IIJ’s or managements’ intentions, beliefs, expectations, or predictions for the future are forward-looking statements that are based on IIJ’s and managements’ current expectations, assumptions, estimates and projections about its business and the industry. These forward-looking statements, such as statements regarding revenues, operating and net profitability are subject to various risks, uncertainties and other factors that could cause IIJ’s actual results to differ materially from those contained in any forward-looking statement.