FUJITSU
shaping tomorrow with you

FUJITSU
Cloud Service
Tunaclo API Connect

ご紹介資料

2021年7月版

富士通株式会社

目次

- Tunacloシリーズのコンセプト
- Tunaclo API Connectとは
- 利用シーン
- 導入事例
- 利用イメージ
- 商品情報
- 技術情報
- 付録
- コラム

Tunacloシリーズは、
お客様のハイブリッドITの運用を
強力にアシストします。

クラウド活用によりIT基盤のハイブリッド化が進み、
リモートアクセス需要が高まる中、その運用がますます複雑になっています。
Tunacloシリーズは、お客様課題のシンプルな解決策を提案し、
スマートな運用を実現していきます。

Tunaclo API Connect
特別な機器や設定なしで
セキュアーなリモートアクセスを可能に

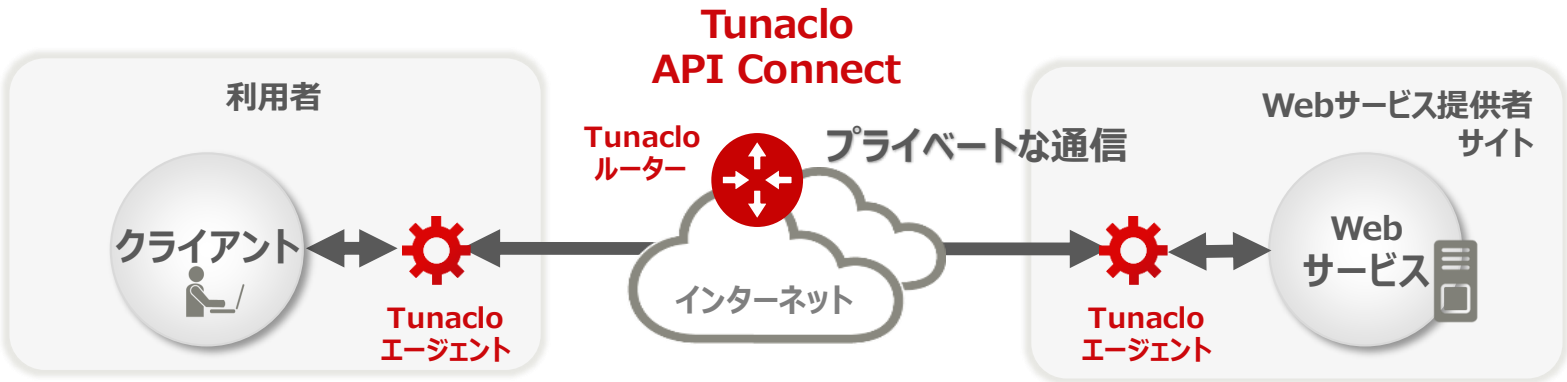
Tunaclo AuthZ Binder
Webサービスへのアクセス制御における
認可設定を 簡単に一元管理

FUJITSU

Tunaclo API Connectとは

Tunaclo API Connect とは

インターネットに公開していないWebサービスを
専用ネットワークを繋がずに安全に利用できるクラウドサービスです



- インターネットを介して非公開のWebサービスにアクセスできます
- 非公開のWebサービスを利用させたいクライアントにのみアクセスを許可できます

特長1：利用が簡単

FUJITSU

✓設定変更不要

お客様環境の設定変更
(ファイアウォールや固定IP
アドレス等)は不要です

※インターネット接続は必要

✓素早いセットアップ

API Connect のセットアップ
は数時間で完了します

※通信元・先にエージェントを配置し、
通信を許可するペアを指定するだけで完了

✓開始・停止が容易

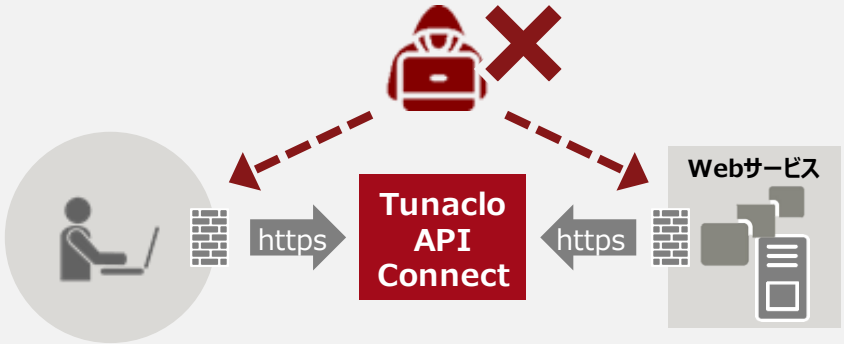
サブスクリプションで提供、
機器導入など初期費用もかからず、
簡単に始められます

※月35,000円～、低価格で利用可能

高度な知識や準備が不要で、契約から数日で利用開始できます

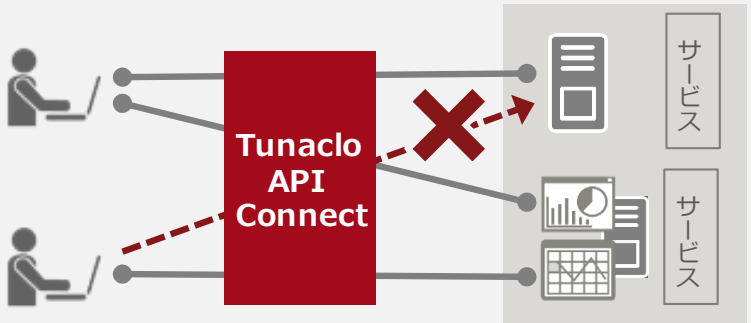
特長2：セキュアな通信

外部からの攻撃を受けない



通信元・先ともに外向きの
https通信だけで接続するため、
Webサービスをインターネットに公開しません

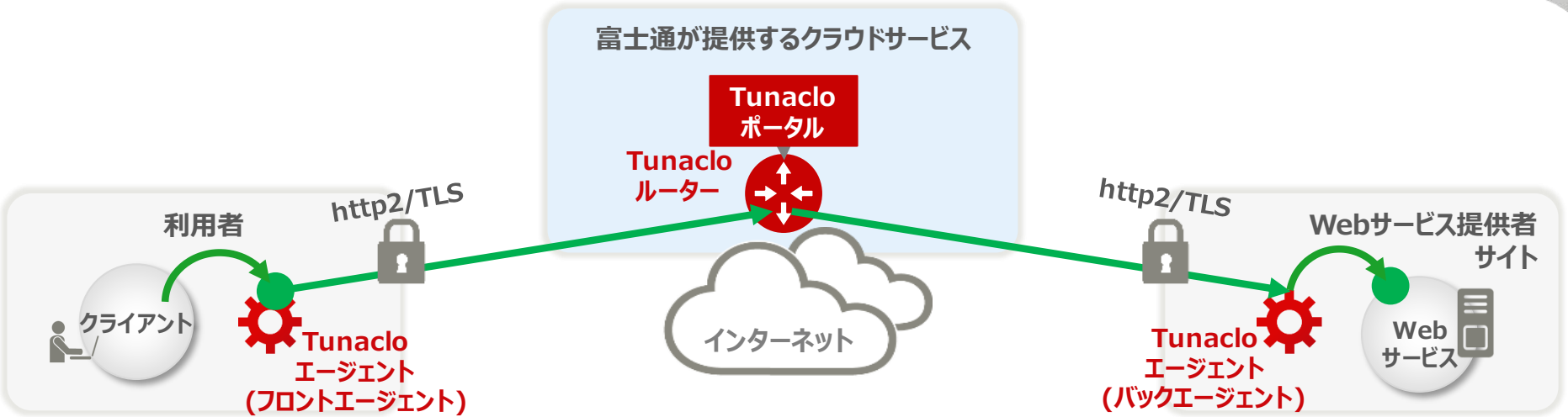
情報漏えいリスクを低減



通信元と通信先(Webサービス)の
通信を組み合わせで管理し、
予期しないアクセスを遮断します

特別な機器やファイアウォールの設定変更なしでセキュアな通信を実現します

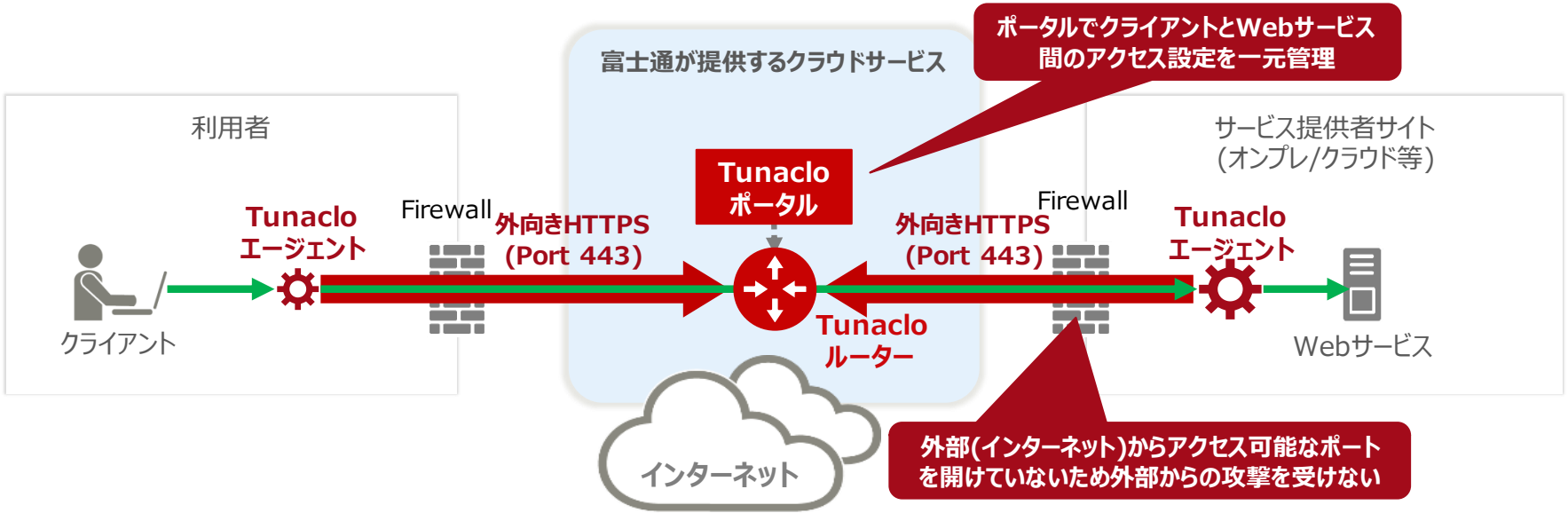
Tunaclo API Connect 構成



コンポーネント	説明
Tunacloポータル	お客様が通信の接続設定を行うGUI
Tunacloルーター	Tunacloポータルの設定に従い、エージェント間の通信を制御して中継
フロントエージェント	クライアント側に設置するエージェントソフトウェア。アクセス要求をTunacloルーターに転送
バックエージェント	Webサービス側に設置するエージェントソフトウェア。Tunacloルーターから中継されたアクセス要求をWebサービスに転送

Tunacloを使った通信の仕組み

- エージェントは外向きHTTPS通信のみをおこないます
  - エージェントが起動するとTunacloルータとHTTPSコネクションを確立し常時接続
  - Webサービスへの通信は確立済みのHTTPSコネクションを使用



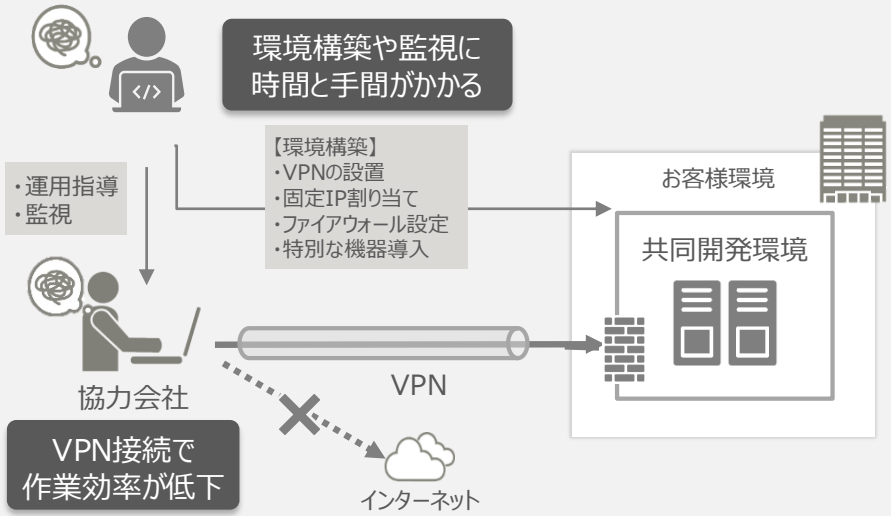
利用シーン

①簡単な導入

リモートアクセス環境を構築するために機器調達や接続に数か月かかる場合があります

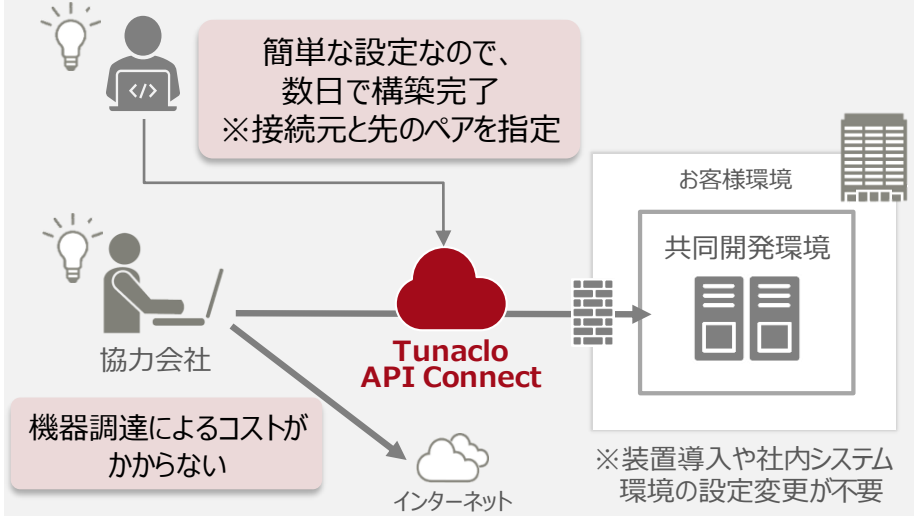
課題

自社セキュリティ基準対策で準備／運用が大変



Tunaclo API Connectで解決

リモートアクセス環境を数日で構築！



Tunaclo API Connectは、自社システムへのリモートアクセスを簡単に実現します

②快適なリモートアクセス

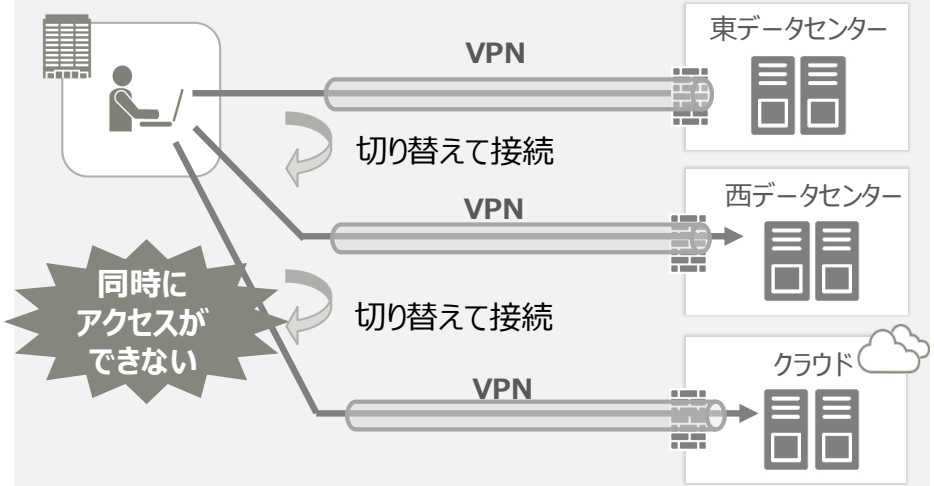
FUJITSU

災害対策などで、業務システムを複数拠点に分散させることが増え、複数サイトへのリモートアクセスが必要となっています

課題

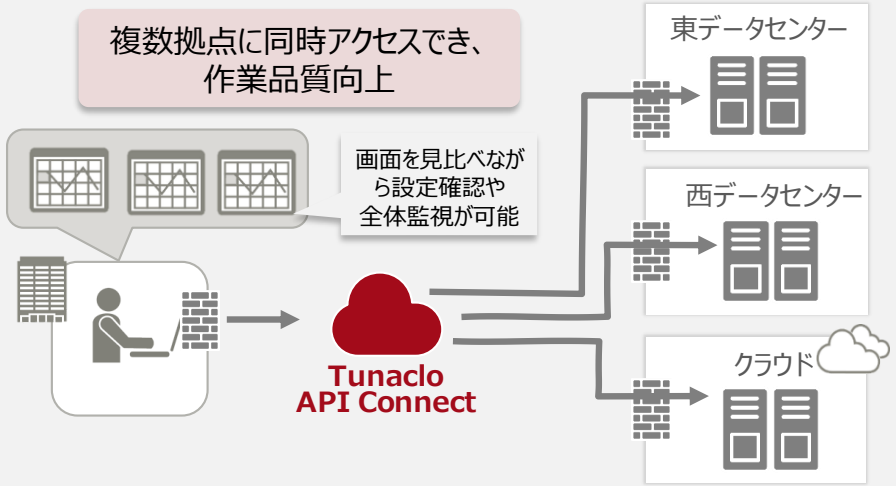
VPNは複数拠点のサーバアクセスが不便

VPNは多くの場合、複数同時接続不可



Tunaclo API Connectで解決

インターネット回線を利用したシンプルなアクセスで効率UP!



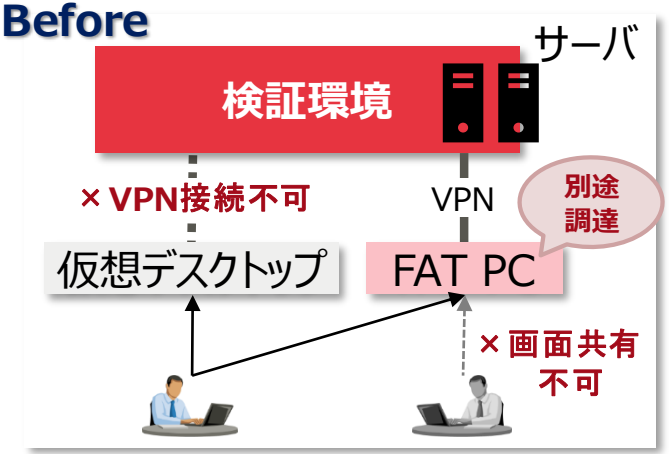
Tunaclo API Connectにより、複数拠点に跨るサーバ・アプリケーションの操作性を改善します

導入事例

PSLab：仮想デスクトップからPSLabへのアクセス

FUJITSU

Before



状況

案件毎にネットワーク分離された検証環境をリモートから利用するユーザ向けにインターネットVPNを提供

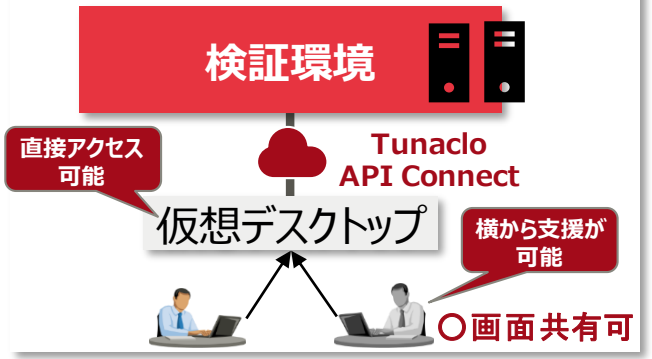
- 社内ルールで仮想デスクトップにVPNソフトをインストールできないため **FAT PCやアクセス用中継サーバが必要**
- VPN接続中はインターネット・イントラネットにアクセスできない

課題

①検証環境へ仮想デスクトップからアクセスしたい

②検証環境へのVPN接続と同時にインターネット接続できず Teams,Skypeでの**画面共有が利用できず検証支援が得づらい**

After



リモートアクセス手段として新たにTunaclo API Connectを導入

① **仮想デスクトップから検証環境を利用可能**
FAT PCの追加準備、中継サーバの設定変更の負担を削減。

② **検証作業の効率化**
検証環境アクセス中もインターネットアクセスが可能なため、画面共有による有識者の支援を得られるようになり、作業が効率化

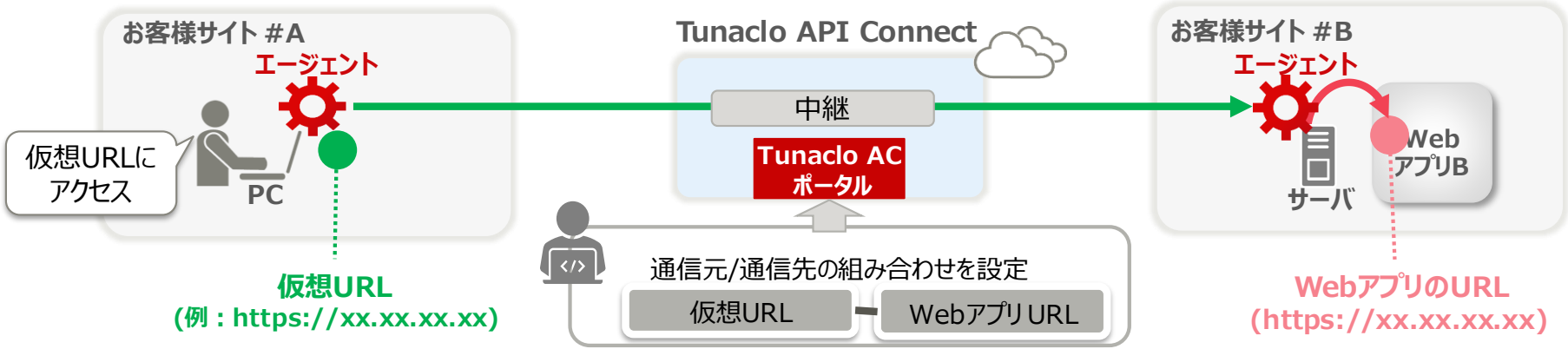
＊ PSLabは富士通が提供する検証環境貸出サービス。案件毎に分離された環境をご提供

利用イメージ

本サービス利用の流れ

1. 通信元、通信先にエージェント(※)を導入
2. 通信元のエージェントに**仮想URL**を設定
   ※仮想URLは通信先との通信に使用する仮想的なURL。通信元環境内の任意のアドレスを設定。
3. 通信元の**仮想URL**と通信先WebアプリのURLの組み合わせをTunaclo ACポータルで設定
4. 利用者は、**仮想URL**にアクセスすることで、Webアプリに接続

利用例



※エージェント： Tunaclo API Connectサービス利用に必要なソフトウェアで、接続元・先に設置します。

エージェントの設置形態

- エージェント形態は２種類あり、それぞれ導入方法を複数用意しており、お客様の利用形態に合わせて選択いただけます。

1. PCに導入するタイプ

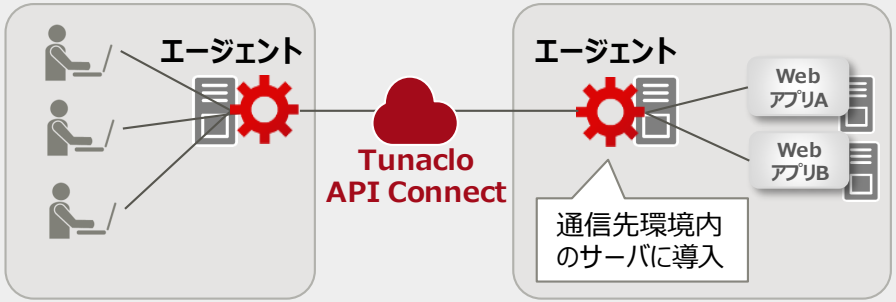
通信元のエージェントとして利用

導入方法(2種類)

①PCに実行形式をダウンロードして展開(Windows)

②PCにインストールしてサービスとして動作 (Windows)

2. サーバに導入するタイプ



通信元で複数利用者が
エージェントを共有して利用

通信先のエージェントとして利用

導入方法(2種類)

①サーバにインストールして導入（Windows）

②コンテナで配備（Linux）

FUJITSU

商品情報

- サービスメニューと価格
- サービス利用までの流れ
- 動作環境
- 製品情報サイト／ドキュメント

サービスメニューと価格

■ 利用目的に合わせて3つのメニューから選択いただけます

メニュー プラン		Basic	Pro 推奨	Enterprise
販売形態		サブスクリプション	サブスクリプション	サブスクリプション
価格（税別）		35,000円/ 月	69,000円から/ 月	お問い合わせください
対象		PoCや開発利用向け	本番利用向け	大規模利用・SaaS事業者向け
ログ保存期間		1カ月	3カ月	12カ月
ルータ	利用形態	共有	共有	占有
	冗長化	なし	あり	あり
サポート手段		メール	メール	メール / 電話
利用できるエージェント数	初期値	35個	70個	200個
	追加	不可	5個 / 月額3,500円 （最大200個）	可能 （価格はお問い合わせください）
備考			年間契約も選択可 （価格はお問い合わせください）	年間契約のみ

サービス利用までの流れ

FUJITSU

1 手配前の準備

① 必要エージェント数の見積もり
② 契約プランの決定
③ 導入支援サービス利用の検討　[推奨]

2 ご契約

3 サービス開始の手続き

① ユーザー登録

4 サービス開始

① 必要エージェント数の見積もり

FUJITSU

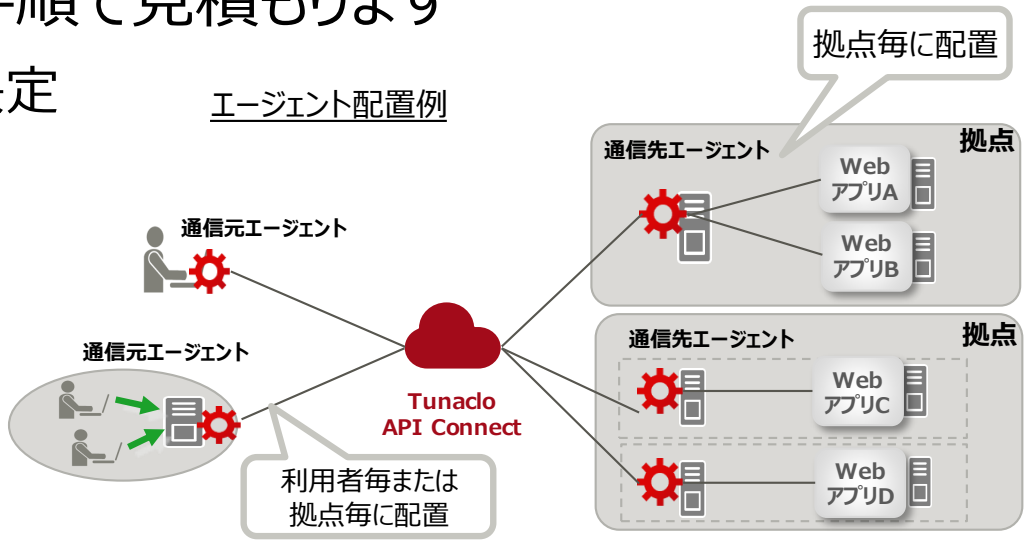
■ 必要なエージェント数は下記手順で見積もります

① 利用者、接続先アプリ数量の決定

② エージェント配置の決定

- 接続元、接続先の利用形態により
  エージェントの配置を決定

エージェント配置例



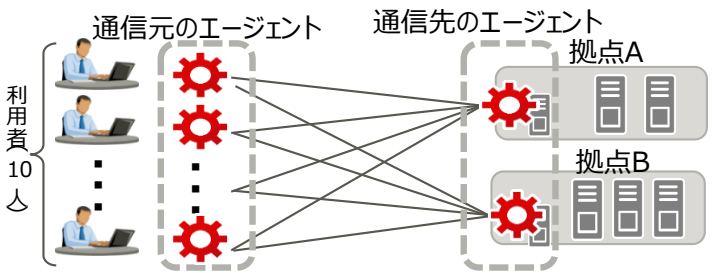
③ 必要なエージェント数算出

必要なエージェント数＝　通信元のエージェント数＋通信先のエージェント数

例）通信元のエージェント数＝利用者数または作業拠点数
　　通信先エージェント数＝接続先拠点数またはドメイン単位

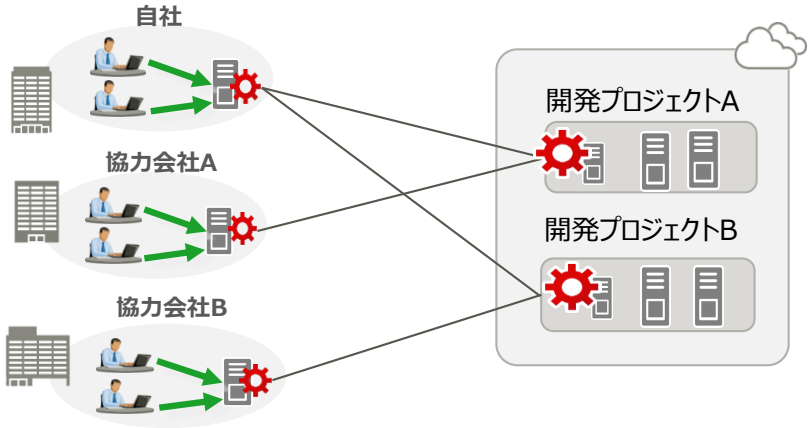
① 必要エージェント数の見積もり例

- 利用者が10人、通信先システムが2つの拠点に分かれている場合
  - 利用者はそれぞれのPCにエージェントを導入、通信先は拠点毎にエージェントを配置



	エージェント数	必要なエージェント数
利用者10人	10	12
拠点2つ	2	

- クラウド上の2つの開発プロジェクト環境を、協力会社から利用する場合
  - 利用者の作業拠点単位にサーバにエージェントを設置、通信先は開発プロジェクト単位にエージェントを設置



	エージェント数	必要なエージェント数
アクセス拠点　3か所	3	5
開発プロジェクト　2つ	2	

② 契約プランの決定

FUJITSU

■ 利用要件により、プランを決定してください。本番環境ではPro以上のプランの利用を推奨します。

推奨

お客様毎
カスタマイズ
可能！

		プラン		
		Basic	Pro	Enterprise
エージェント数	初期値	35個	70個	200個
	追加	不可	5個 単位に追加 最大200個	相談
ルーター	利用形態(※)	共有	共有	専用
	初期値	なし	あり	あり
ログの保存期間		1ヶ月	3か月	12か月
支払い形態		月額	月額／年額	年額

（※）サービス環境を共有している場合、他契約者の負荷の影響を受ける場合があります

注）Tunaclo ACを介した通信の性能はご利用のインターネット環境に準じます

[注意事項]

■ プランの切り替えについて

- 上位プランへの変更 ：利用環境を継続したまま、プランの変更が可能です。プラン変更したい場合は、弊社営業にご連絡ください。
- 下位プランへの変更 ：下位プランに変更する場合は、再契約となり、利用環境を引き継ぐことができません。現契約を解除後、新規契約締結してください。

③導入支援サービスオプション

FUJITSU

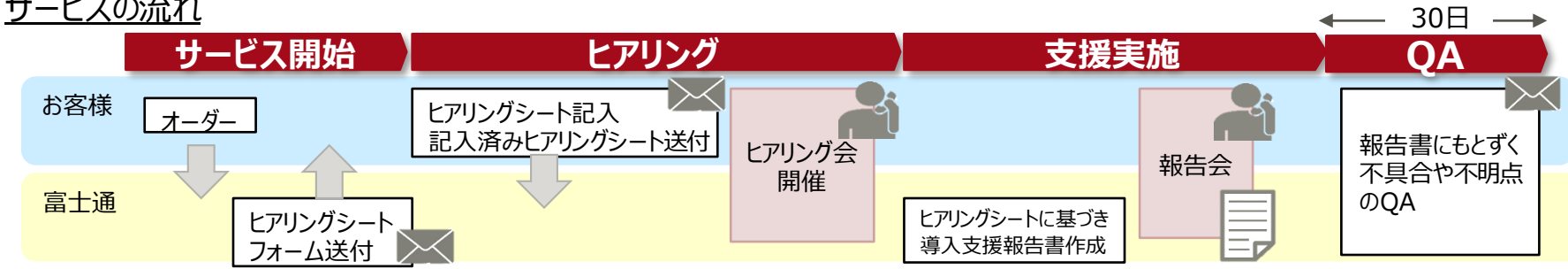
- お客様の環境に沿った導入を支援します。
  - お客様環境のヒアリングに基づき、最適な構成設計と導入手順をレポートします。
  - 30日間アフターフォローしますので安心です。

※本サービスは、Tunaclo API Connectサービス契約と同時にご契約ください。
※個別見積もり製品となっています。価格については弊社営業にお問い合せください

Tunaclo API Connect はインフラに関する専門的な知識なしに簡単に導入できるサービスですが、セットアップに不安がある方はこちらのオプションサービスも併せてご検討ください。

サービス内容	エージェント配置・運用に関する設計支援	エージェントの導入設計、運用設計支援ドキュメント提供 ・インストール方法 ・エージェント起動パラメーターに関する設計 ・エージェントのバージョンアップの運用設計
	サービス活用に関する設計支援	ポータル設定支援ドキュメント提供 ・サービスおよびクライアントの定義 ・ユーザーおよびロールの定義
	アフターサービス（QA）	本サービス結果の報告会後、報告内容にもとづくQAに対応します（期間：30日、対応：平日9:00～17:00、E-mailのみ）

サービスの流れ



動作環境

FUJITSU

エージェント

動作OS	エージェント名称	適用場所	配備方法と備考
Linux	コンテナ版	Front Agent Back Agent	dockerコンテナとして動作します。 ポータル上の公開している起動コマンドを実行して起動します。
Windows	Tunaclo Connect Client	Front Agent	実行形式で提供するエージェントです。 アプリインストール権限がないVDI環境でも利用可能です。
	Tunaclo Agent Service	Front Agent Back Agent	インストールして利用するエージェントです。一度インストールしていただくと、以降は自動で起動するようになります。

動作環境

エージェント種別	OS	装置要件	必須ソフトウェア
Linux（コンテナ版）	CentOS 7.7.1908以上, Ubuntu Server 18.04.3LTS以上	CPU：2GHz 64bit プロセッサ （推奨：インテル Core2 Duo 2GHz 以上） または同等の互換プロセッサ メモリー：推奨：4.0GB 以上 HDD：空き容量 10GB 以上	Docker 19.03 以上
Tunaclo Connect Client	Windows 10		なし
Tunaclo Agent Service	Windows 10 Windows Server 2016		なし

ポータル

- ブラウザー：Google Chrome

※ 上記以外の環境についてはお問合せ下さい

製品情報サイト

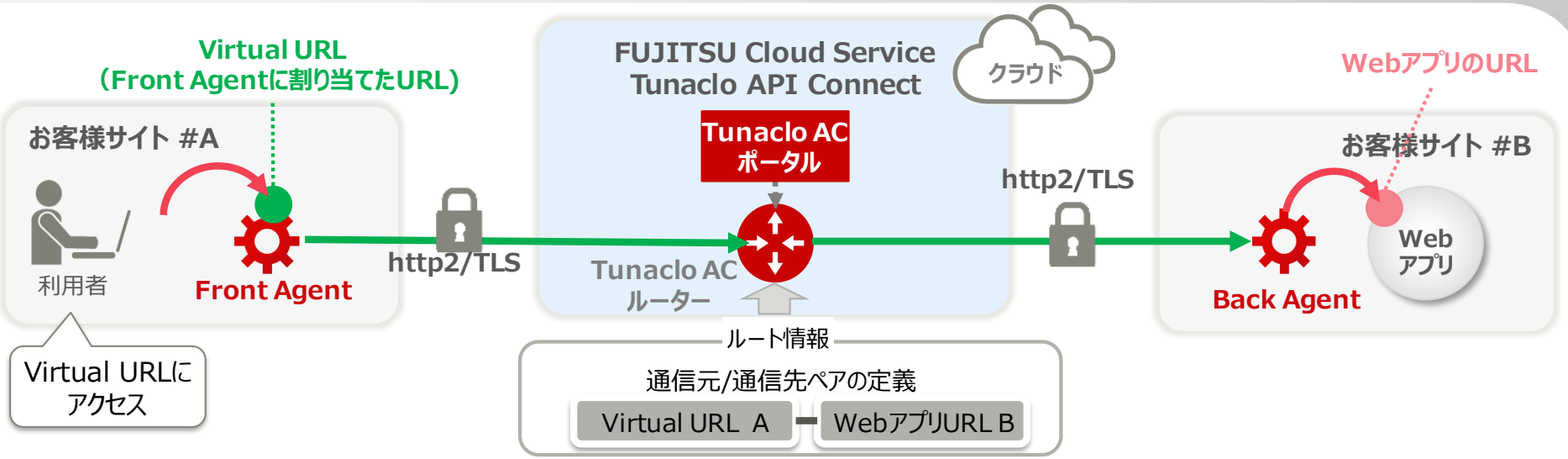
- 製品情報公開サイト
  - https://www.fujitsu.com/jp/tunaclo/
- ドキュメント（ユーザーズガイド、リリースノート）
  - https://support.tunaclo.jp.fujitsu.com/

FUJITSU

技術情報

- 仕組み

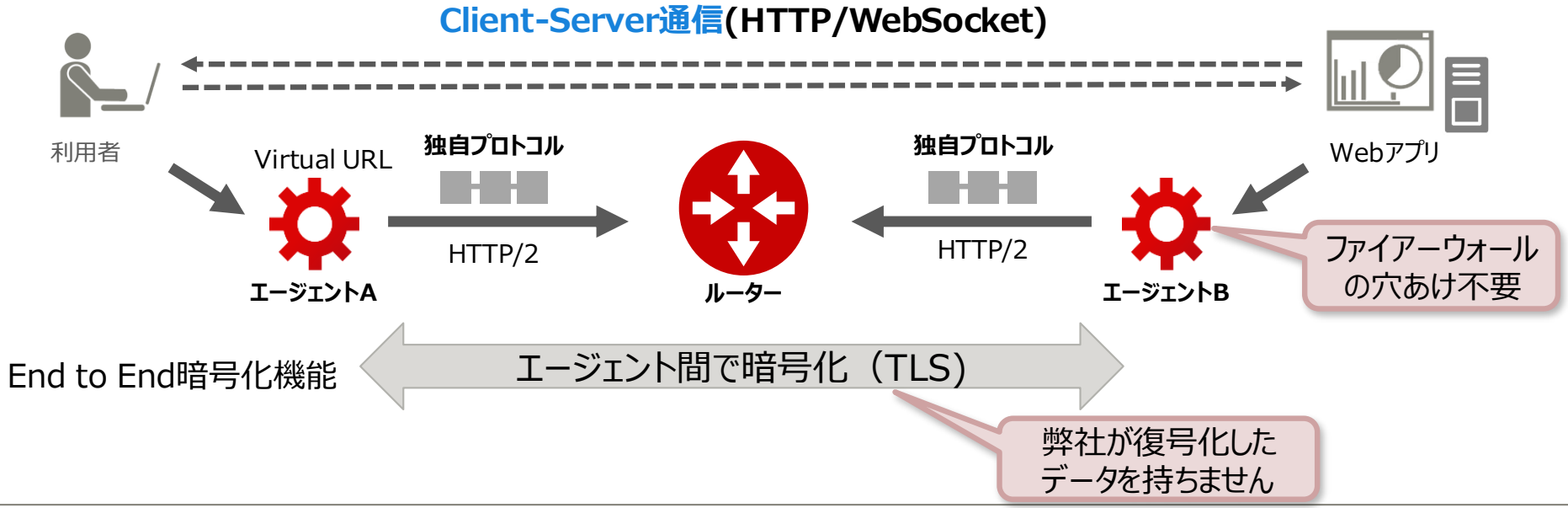
仕組み：通信の流れ



- ルーターは設定したルート情報に従い、Front AgentとBack Agent間の通信を制御し／中継
- 利用者はFront Agentに割り当てられたVirtual URLにアクセスすることで、通信先のWebアプリにアクセス
- Back Agentは、ペアとなっているVirtual URLからの通信をWebアプリのURLに転送
- 各エージェントとルータ間はhttp2/TLSで通信

仕組み：セキュアーな通信

- エージェントからの外向け通信だけなので、Webアプリのインターネット公開不要
- 特定のエージェント間の通信のみが許可され、不当なアクセスは排除
- End to End暗号化でエージェント間の暗号化も提供、お客様のより高いセキュリティ要件に対応



FUJITSU

付録

- 動作アプリケーション

接続実績のあるアプリケーション

FUJITSU

サーバー管理ソフトウェア

PRIMERGY
PRIMERGY iRMC


Apache Guacamole


Windows Admin Center


Linux Cockpit

vmware vSphere
VMware vSphere

監視ソフトウェア

FUJITSU Software
Infrastructure Manager (ISM)

ZABBIX
Zabbix (Web UI)


Prometheus/Node Exporter


Grafana

グループウェア


Redmine


Mattermost


Atlassian JIRA

開発ツール


GitLab

Kubernetes dashboard

docker
Docker Registry

jupyter
Jupyter Notebook

ストレージソフトウェア

ownCloud
ownCloud


Minio

FUJITSU

コラム

リモートアクセスとセキュリティ

セキュリティ事故の99%はユーザーの設定ミス

FUJITSU

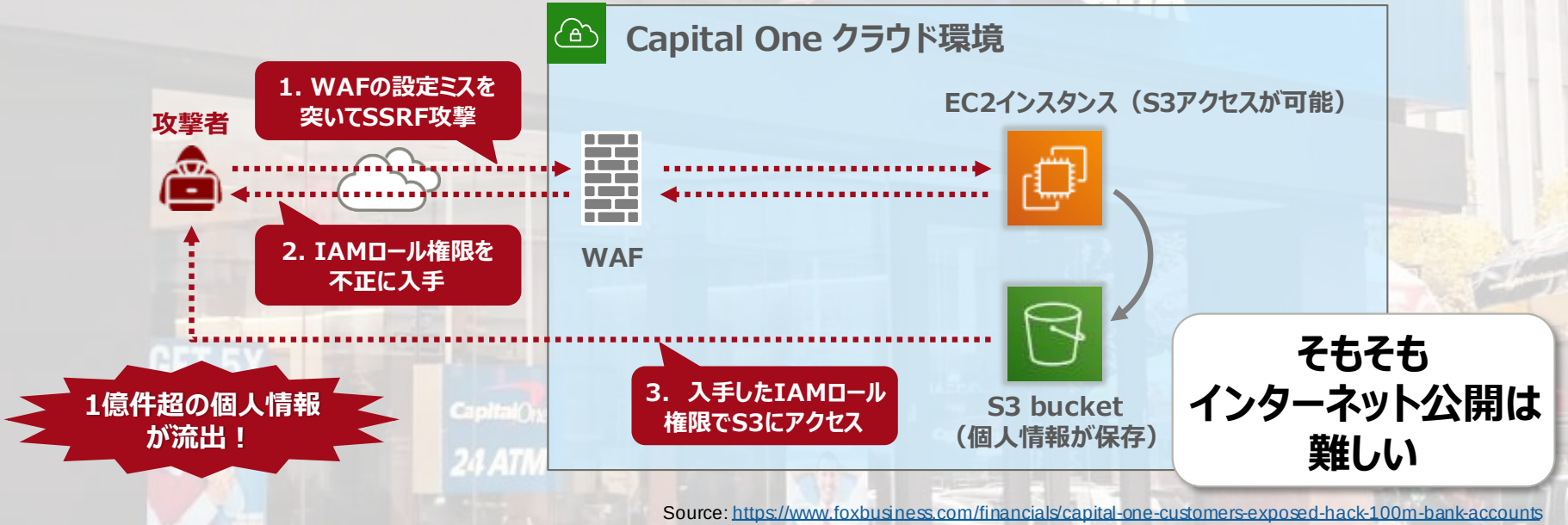
- Gartnerの調査によると、クラウドサービスのプロバイダーにおいてセキュリティインシデントが発生したケースは少なく、サービス損失も部分的にとどまっている場合がほとんど
- 更に同社は、『2025年までに起きる**クラウド関連のセキュリティ事故の99%はユーザの設定ミスに起因**する』と予測

> ***Through 2025, 99% of cloud security failures will be the customer's fault.***

https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

事例：米Capital One社のセキュリティ事故(2019)

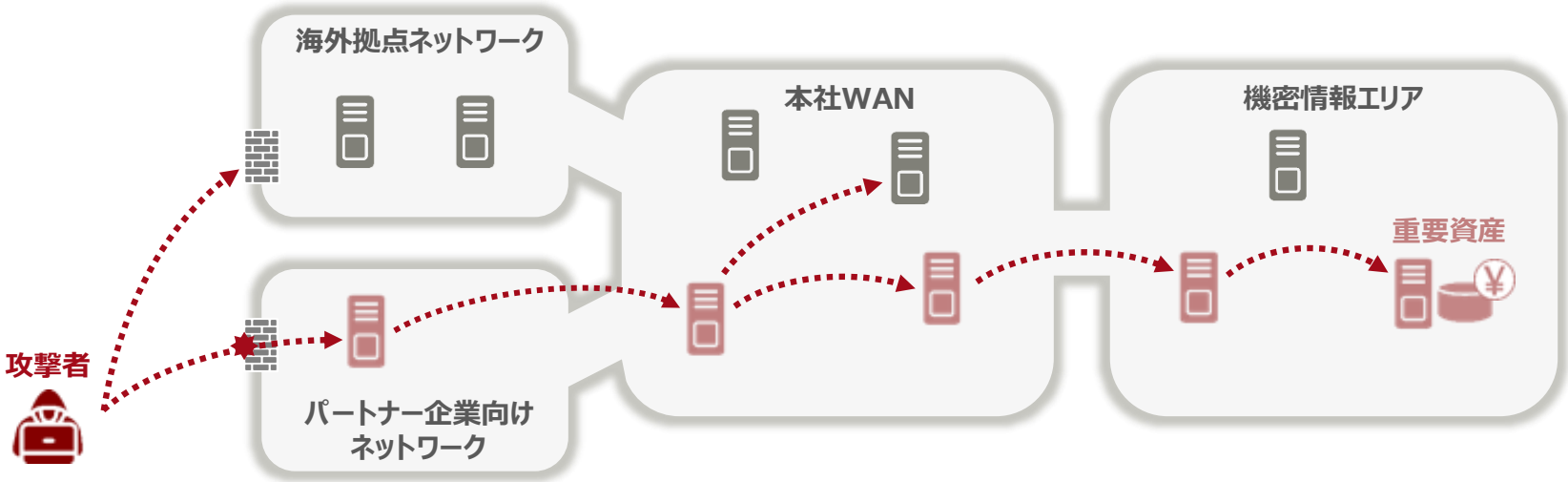
- WAF(OSS)の設定ミスからWeb経由でサーバ情報取得(SSRF攻撃)
- S3 bucketに保存されていた1億件超の個人情報が漏洩



Source: https://www.foxbusiness.com/financials/capital-one-customers-exposed-hack-100m-bank-accounts

近年のセキュリティ脅威：横移動攻撃

- 防御の弱い部分から侵入し横移動を繰り返して組織内部に入り込む攻撃
- 内部からの攻撃には脆弱かつ検知も難しいことが多く被害が深刻化しやすい



例えばシンガポールから日本企業の重要データが盗まれる事件もありました

事例：米Target社の情報漏洩（2013）

- 空調管理システムの監視に利用していたVPNログイン情報が盗まれる
- 攻撃者にネットワーク内に侵入され顧客情報が漏洩

https://dbac8a2e962120c65098-4d6abce208e5e17c2085b466b98c2083.ssl.cf1.rackcdn.com/security-incident-report-data-breach-at-target-corporation-pdf-1-w-1130.pdf

IPA：情報セキュリティ10大脅威 2020

■「情報セキュリティ10大脅威 2020」

NEW：初めてランクインした脅威

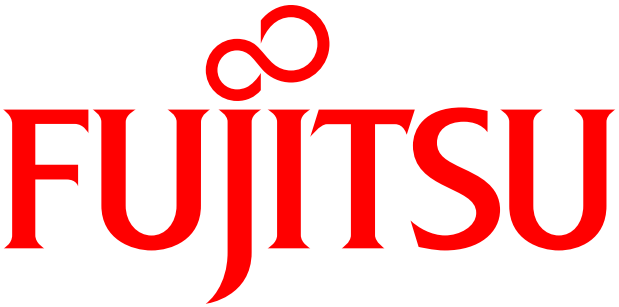
昨年順位	個人	順位	組織	昨年順位
NEW	スマホ決済の不正利用	1位	標的型攻撃による機密情報の窃取	1位
2位	フィッシングによる個人情報の詐取	2位	内部不正による情報漏えい	5位
1位	クレジットカード情報の不正利用	3位	ビジネスメール詐欺による金銭被害	2位
7位	インターネットバンキングの不正利用	4位	サプライチェーンの弱点を悪用した攻撃	4位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	5位	ランサムウェアによる被害	3位
5位	クレジットカード情報の不正利用への被害	6位	予期せぬIT基盤の障害に伴う業務停止	16位
9位	インターネットバンキングの不正利用	7位	不注意による情報漏えい（規則は遵守）	10位
8位	インターネット上のサービスへの不正ログイン	8位	インターネット上のサービスからの個人情報の窃取	7位
6位	偽警告によるインターネット詐欺	9位	IoT機器の不正利用	8位
12位	インターネット上のサービスからの個人情報の窃取	10位	サービス妨害攻撃によるサービスの停止	6位

最初に起きる

被害を拡大

“業務委託先組織が攻撃され、預けていた個人情報が漏えいする 等の被害が発生

https://www.ipa.go.jp/security/vuln/10threats2020.html



shaping tomorrow with you