

情報通信技術面における留意点

～テレワーク導入時・運営時のセキュリティ対策のポイント～

**Flexible Work,
Flexible Business,
Flexible Life.**



株式会社 テレワークマネジメント

鵜澤 純子

CONTENTS

1. 働き方&ICT
インフラの変遷と
セキュリティ

2. ハイブリッドクラウ
ド環境での
テレワークの方法

3. Underコロナ期
に発生した課題

4. ネットワークの
管理

5. ハードウェアと
ユーザーアクティビ
ティ管理

普及啓発

- ・テレワークに関する講演・研修
- ・テレワークセミナー定期実施
- ・メールマガジン定期配信
- ・自治体テレワーク普及・推進事業

導入支援

300社以上の実績

- ・テレワーク導入コンサルティング
テレワークに関する調査/分析
テレワークツールの開発/販売
テレワーク勤務規則/制度策定サポート
- ・テレワーク研修・講演

ビジネス提案

- ・テレワークを活用した新しいビジネスの提案

政策提言

- ・国の政策提言
- ・自治体の施策提言



ホワイト企業認定

今日のセミナーのゴール

テレワークに
これから取り組む方



社外で安全に
仕事をする方法が
わかる

テレワークを
実施されたことのある方

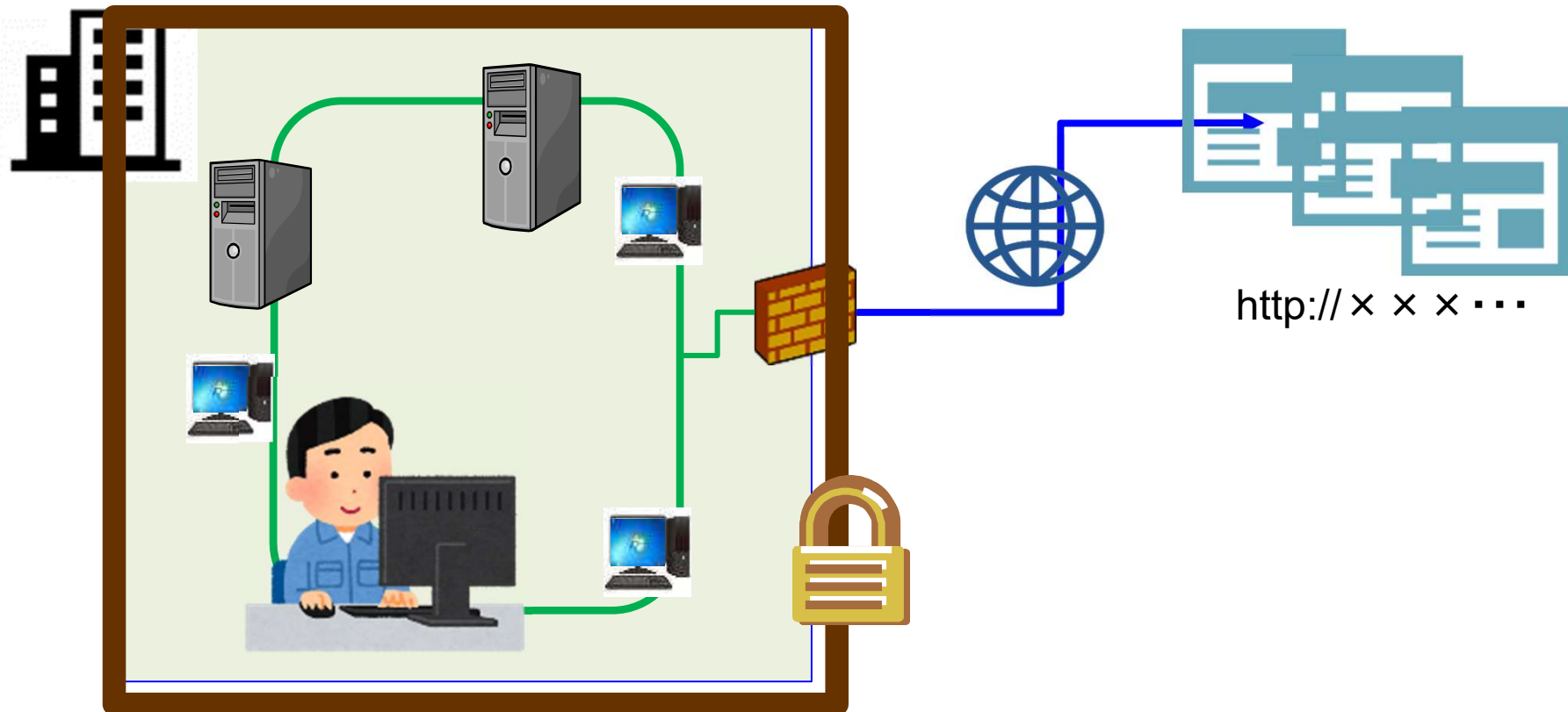


テレワーク実施時の
セキュリティ確保の
ポイントがわかり、
自社状況の確認に
取り組める

働き方 & ICTインフラの変遷とセキュリティ

1.1.働き方 & ICTインフラの変遷とセキュリティ①

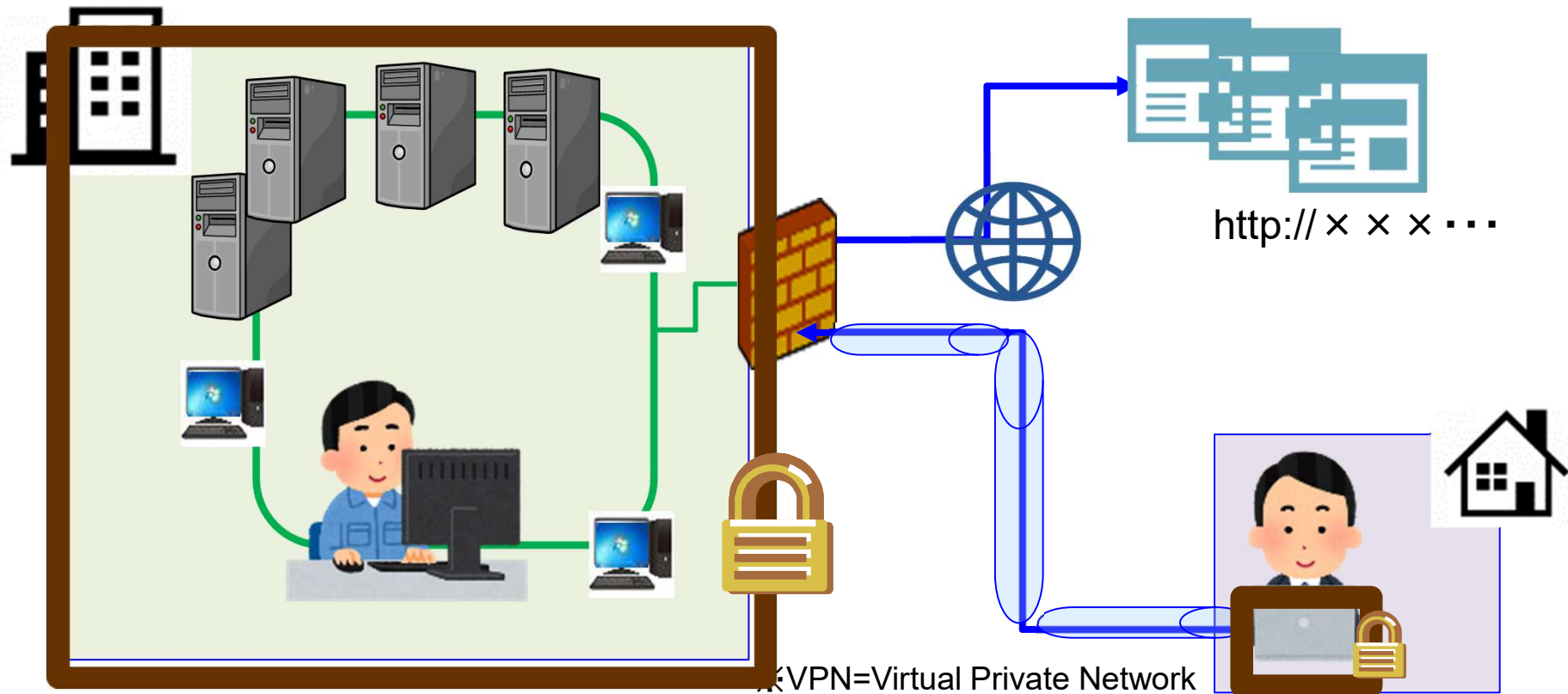
～2000年代：オンプレミス型



パソコンを扱う仕事は会社の建物の中だけで行われ、ICT環境は会社のネットワーク内で閉じていました。

1.2.働き方 & ICTインフラの変遷とセキュリティ②

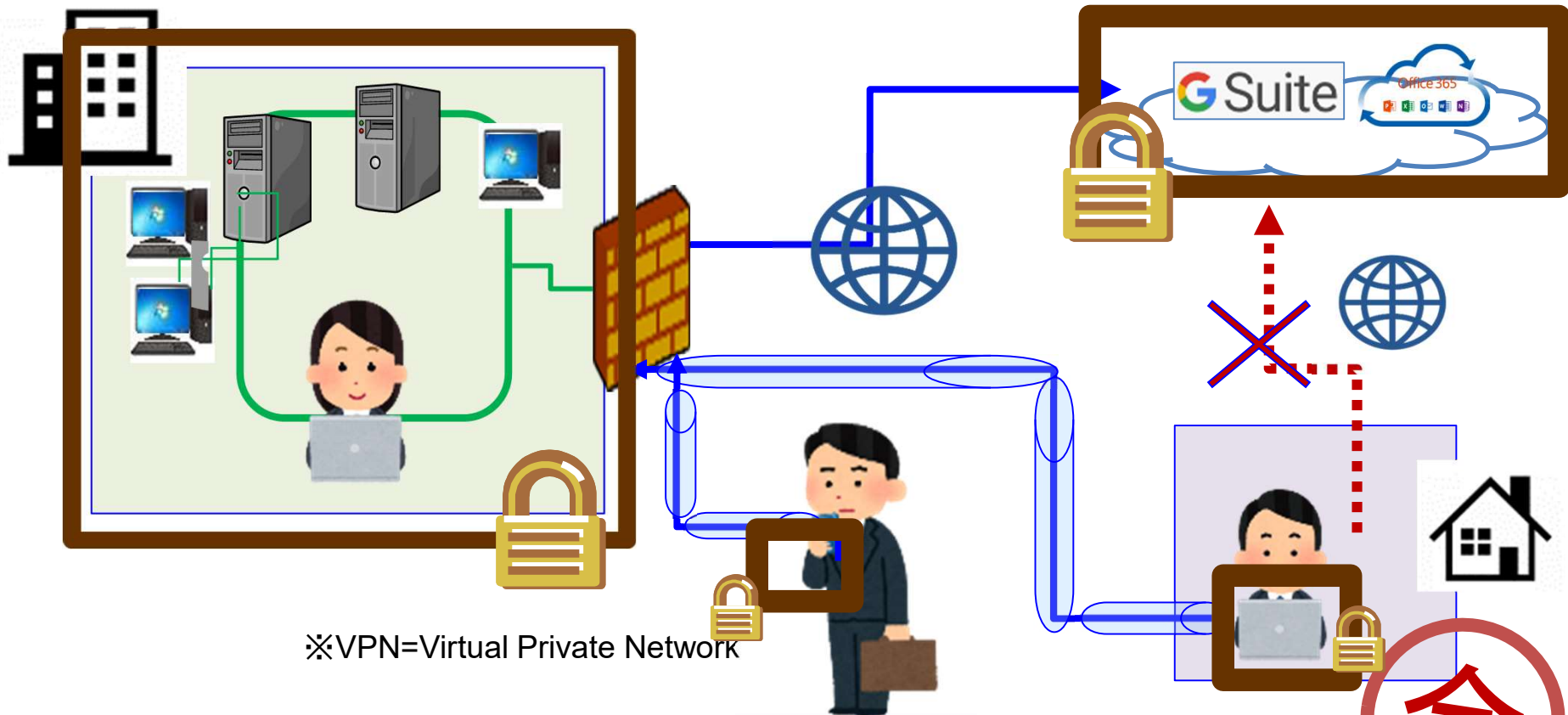
2010年頃～ : オンプレミス + テレワーク型



パソコンを扱う仕事は社外でも行われるようになり、
VPNを使って安全に社内のサーバに接続。

1.3.働き方 & ICTインフラの変遷とセキュリティ③

2017年頃～:ハイブリッドクラウド型

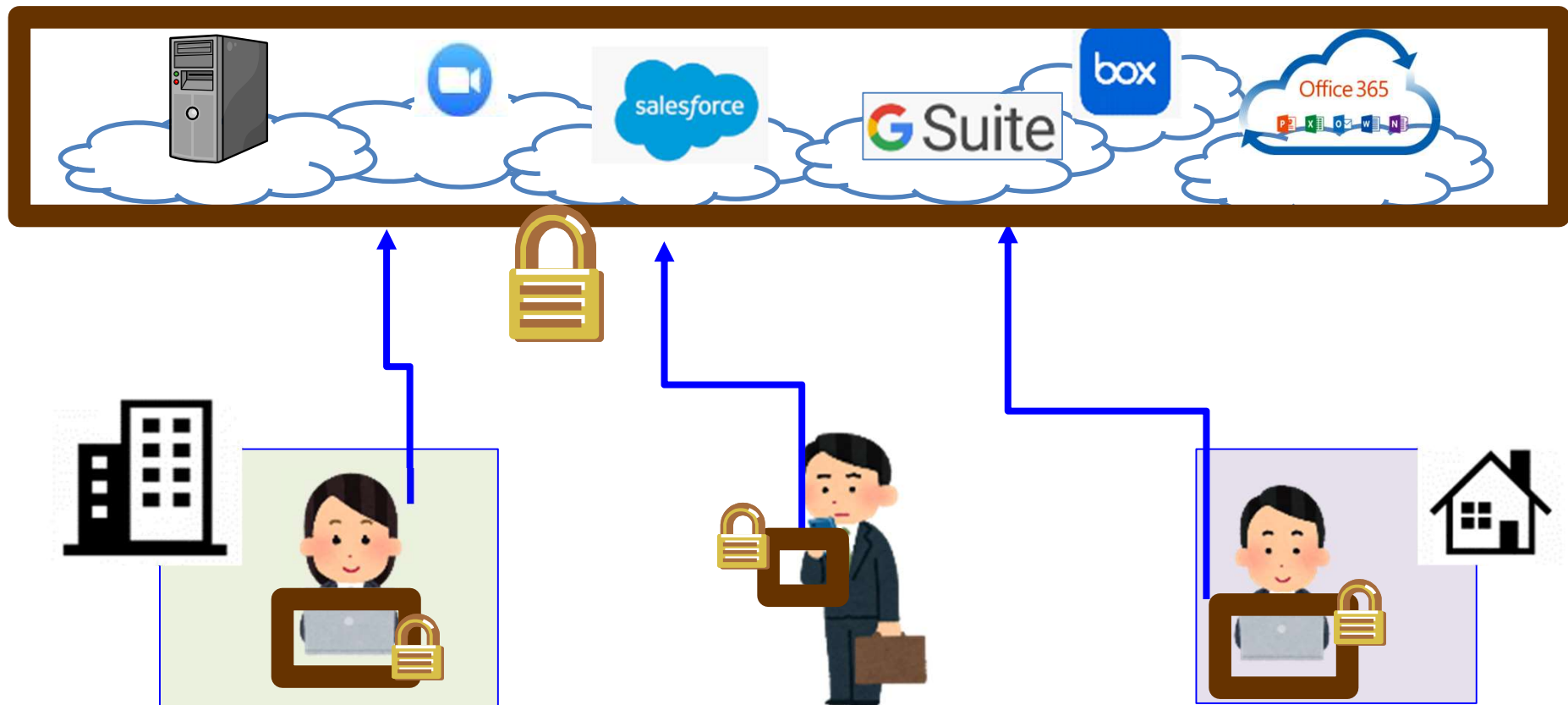


※VPN=Virtual Private Network

パソコンを扱う仕事は社外でも当たり前になり、
社内のサーバとクラウドサービスの両方を利用。

1.4.働き方 & ICTインフラの変遷とセキュリティ④

今後はフルクラウド型へ？

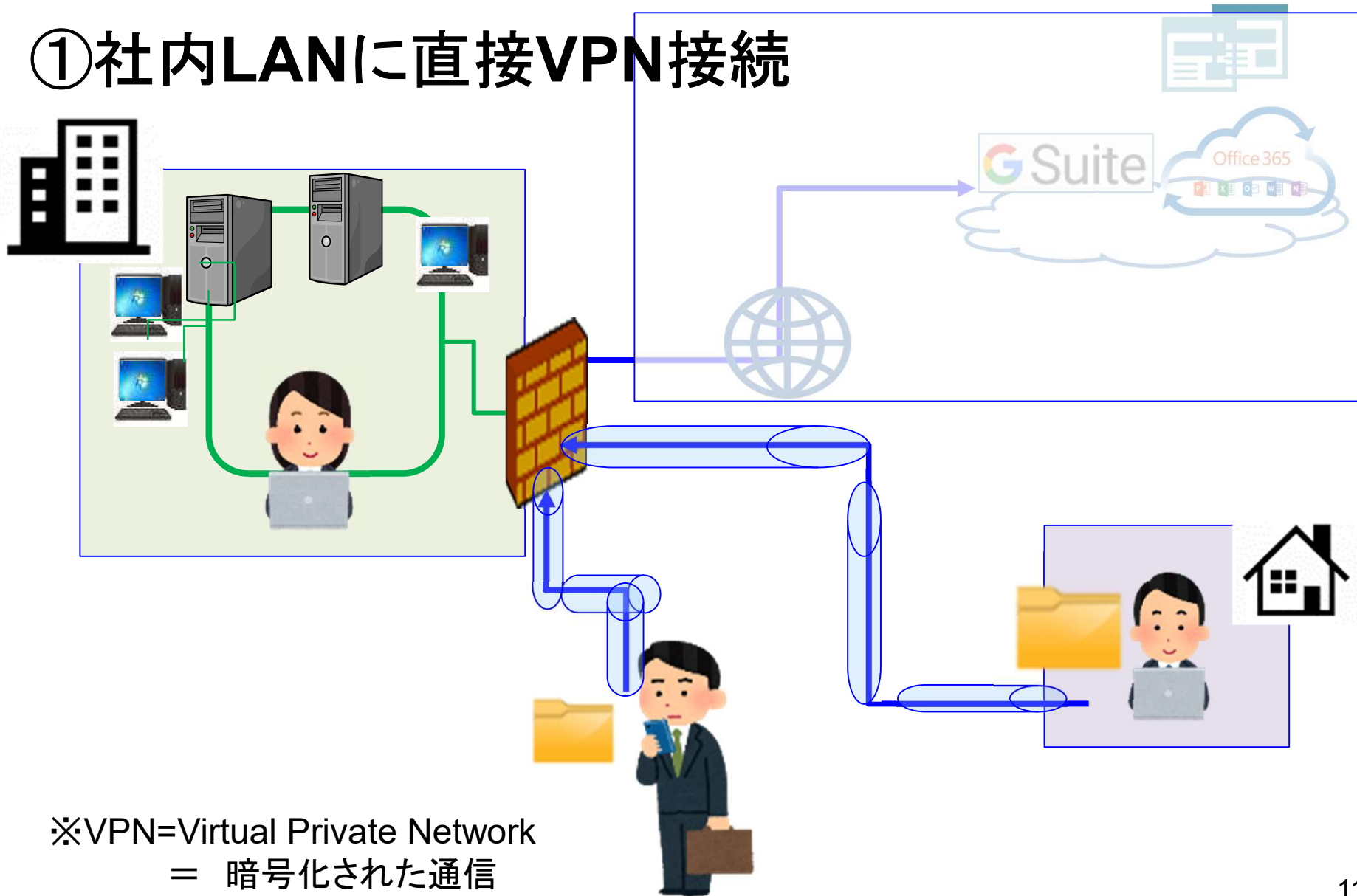


社内LANはなくなり、全ての情報はクラウド内に。

ハイブリッドクラウド環境での テレワークの方法

2.1.ハイブリッドクラウド状態での社内アクセス方法①

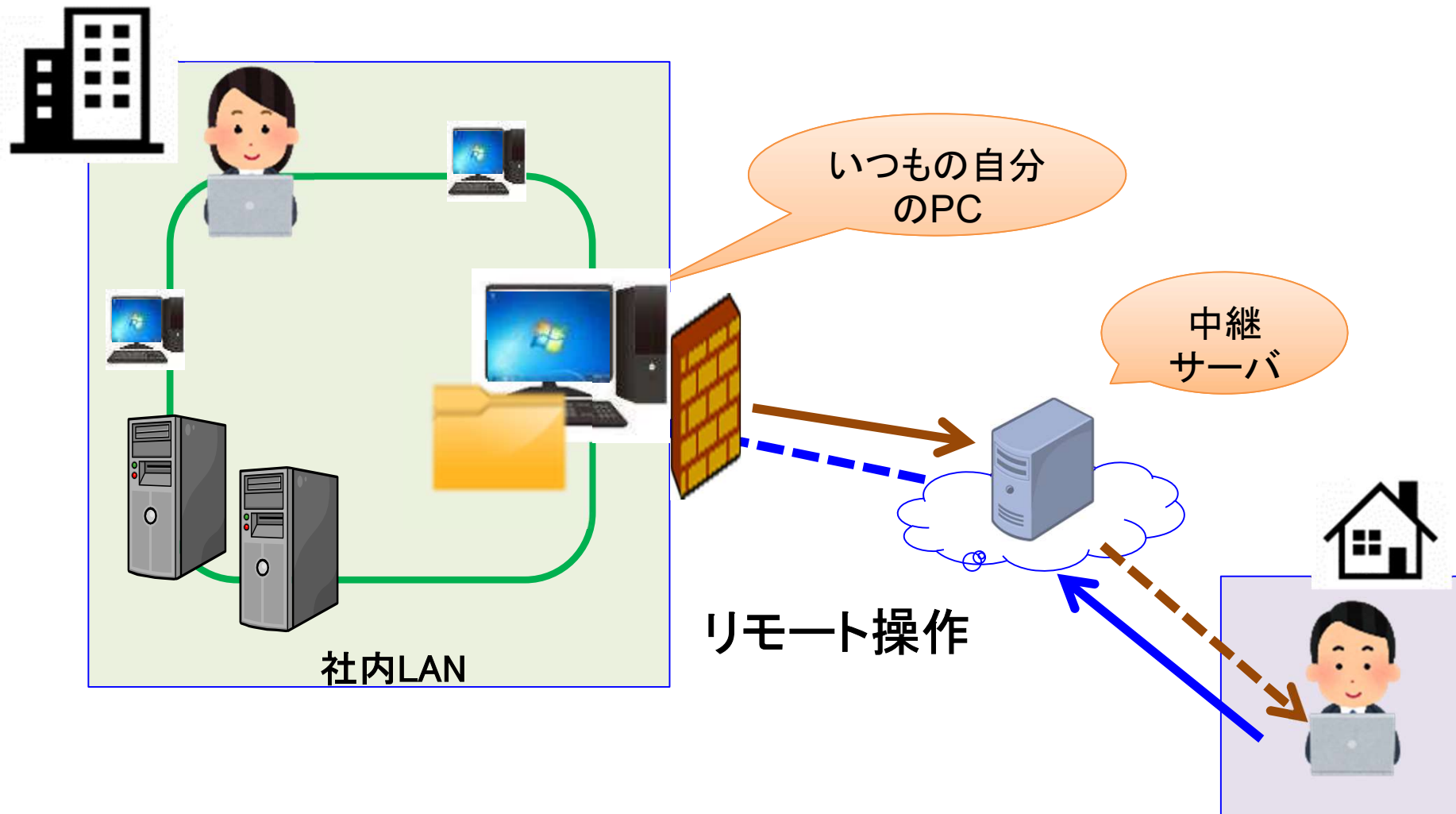
①社内LANに直接VPN接続



※VPN=Virtual Private Network
= 暗号化された通信

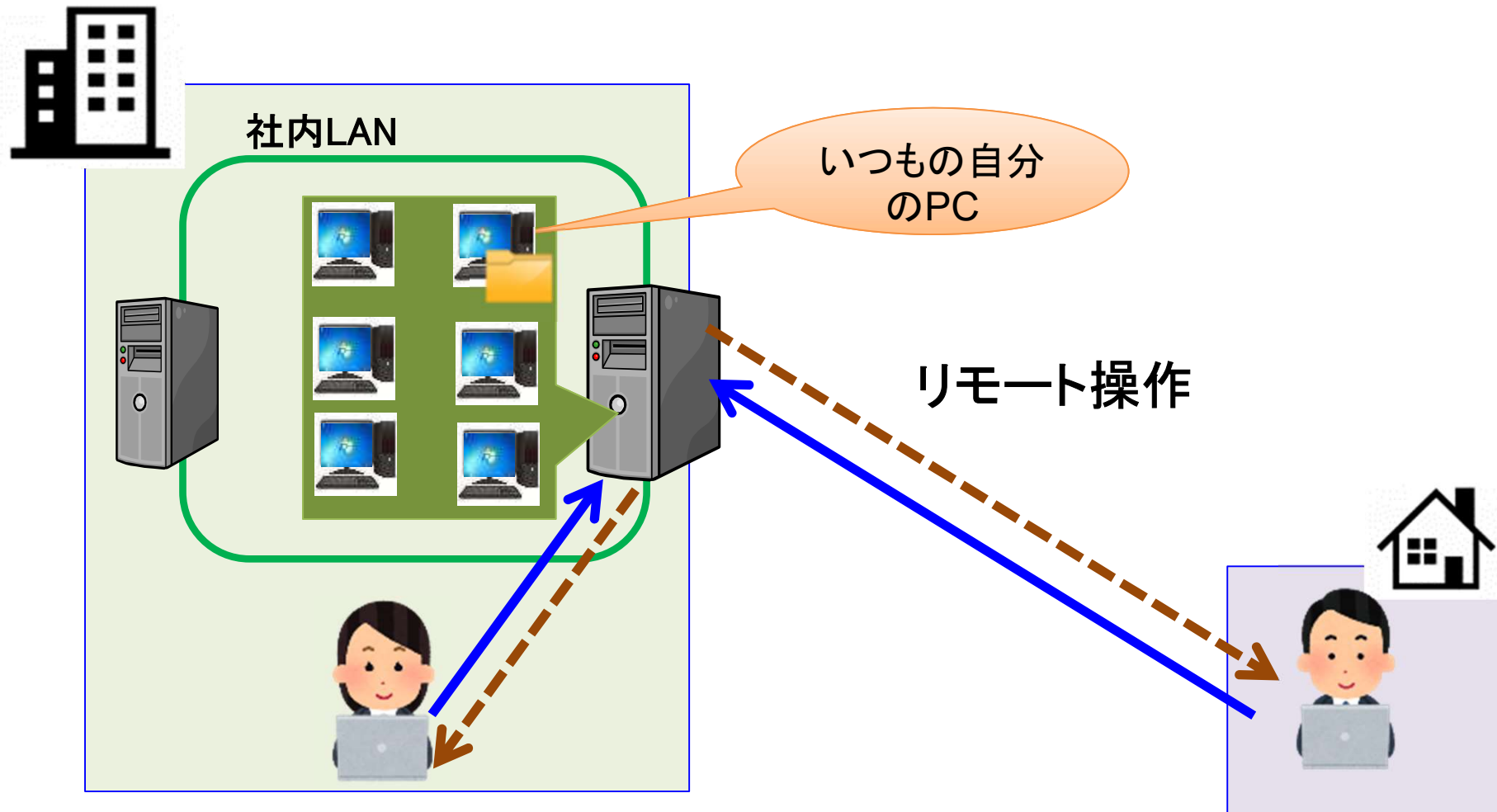
2.2.ハイブリッドクラウド状態での社内アクセス方法②

②リモートデスクトップ



2.3.ハイブリッドクラウド状態での社内アクセス方法③

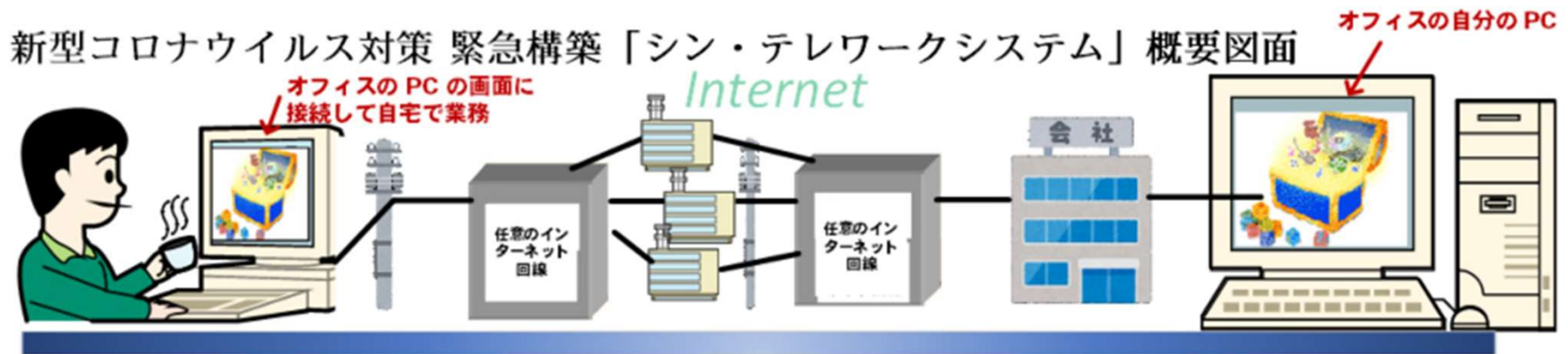
③仮想デスクトップ



2.4.社内システムにアクセスする主な方法のまとめ

接続方法	特徴	情報セキュリティ面でのポイント
①社内LANに直接VPN接続	会社のネットワークに直接手元のPCをつなぐ。 社内のPCと同じようにデータを手元に保存できる。	手元機から社内に脅威が入り込んだり、手元にダウンロードした情報が保存される点がリスク。 従って手元機には、セキュリティ対策をしっかりと行った貸与PCを使う。
②リモートデスクトップ	手元PCから、中継するサーバを介して社内の自分のPCを遠隔操作する。 データは手元機には保存できない。	手元機の状態が社内に影響を与えず、情報を社外で保存できないので、私物PC利用も可。 会社のPCが遠隔操作が可能な状態になるので、認証を強化する。
③仮想デスクトップ	手元のPCから、サーバの中に構築された「仮想の自分のPC」を操作する。 データは手元機には保存できない。	同上

2.5.(参考)「シンテレワークシステム」公開中(=リモートデスクトップ)

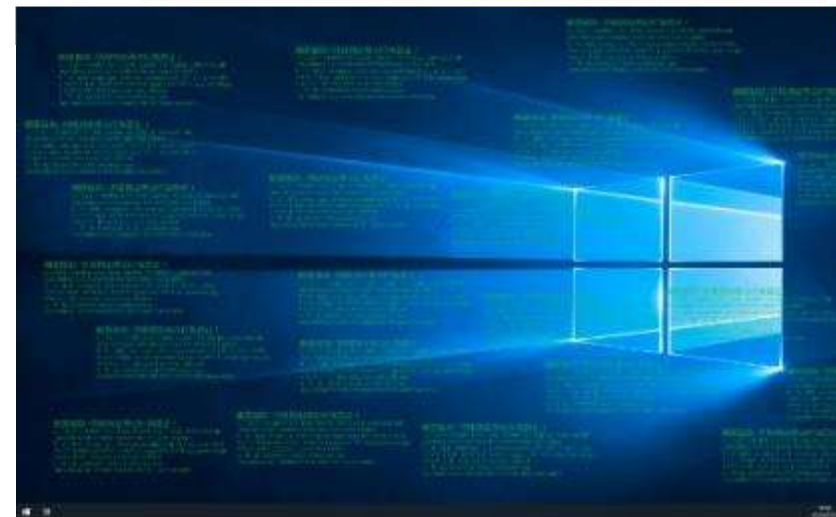


新型コロナウイルス対策 緊急構築 実証実験

・4/21から公開で
利用者7.8万人超

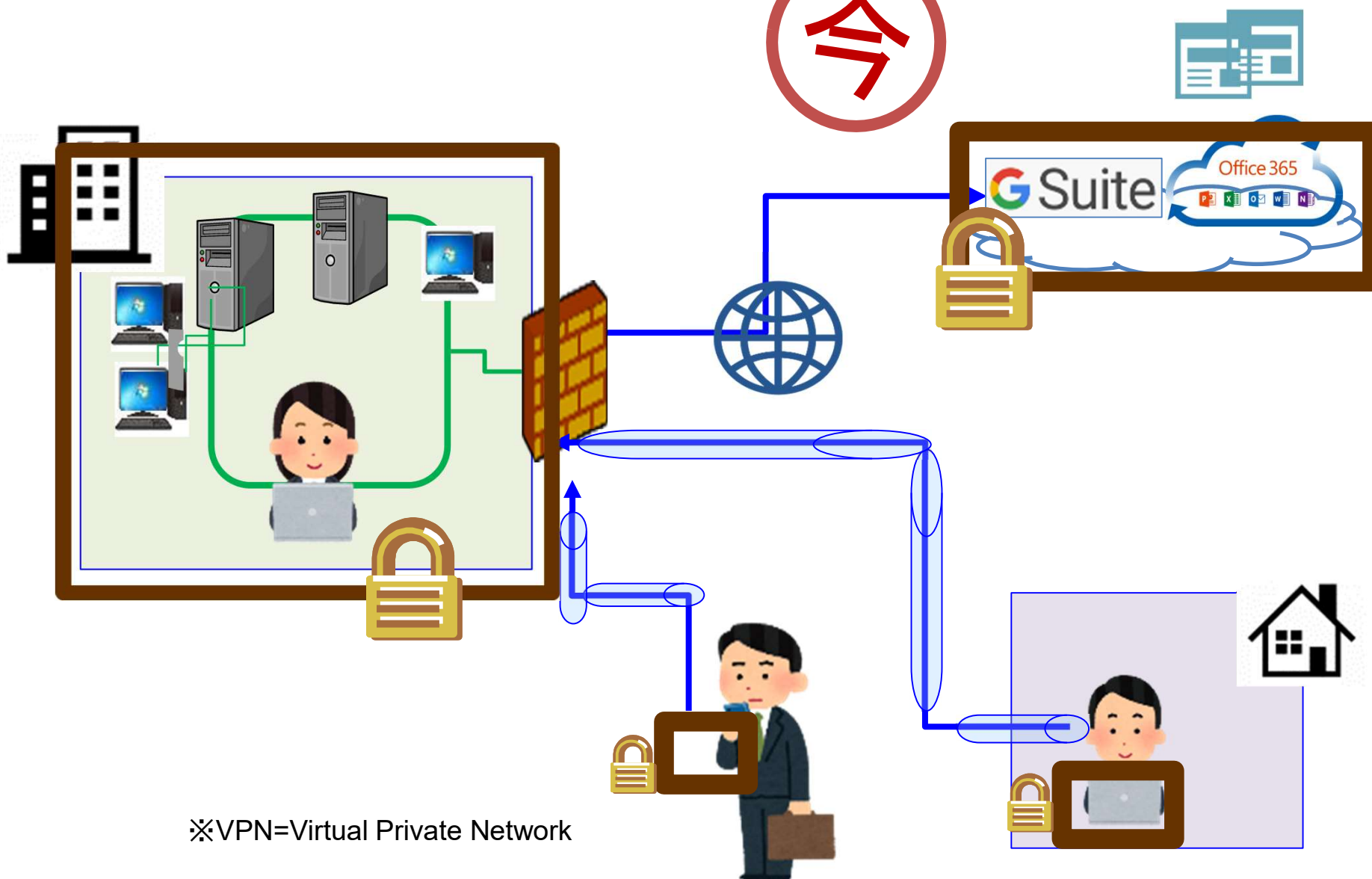
契約不要・ユーザー登録不要、無償の「シン・テレワークシステム」を新型コロナウイルス対策の実証実験として提供中。
2021年10月末までは提供を継続。

<https://telework.cyber.ipa.go.jp/news/>



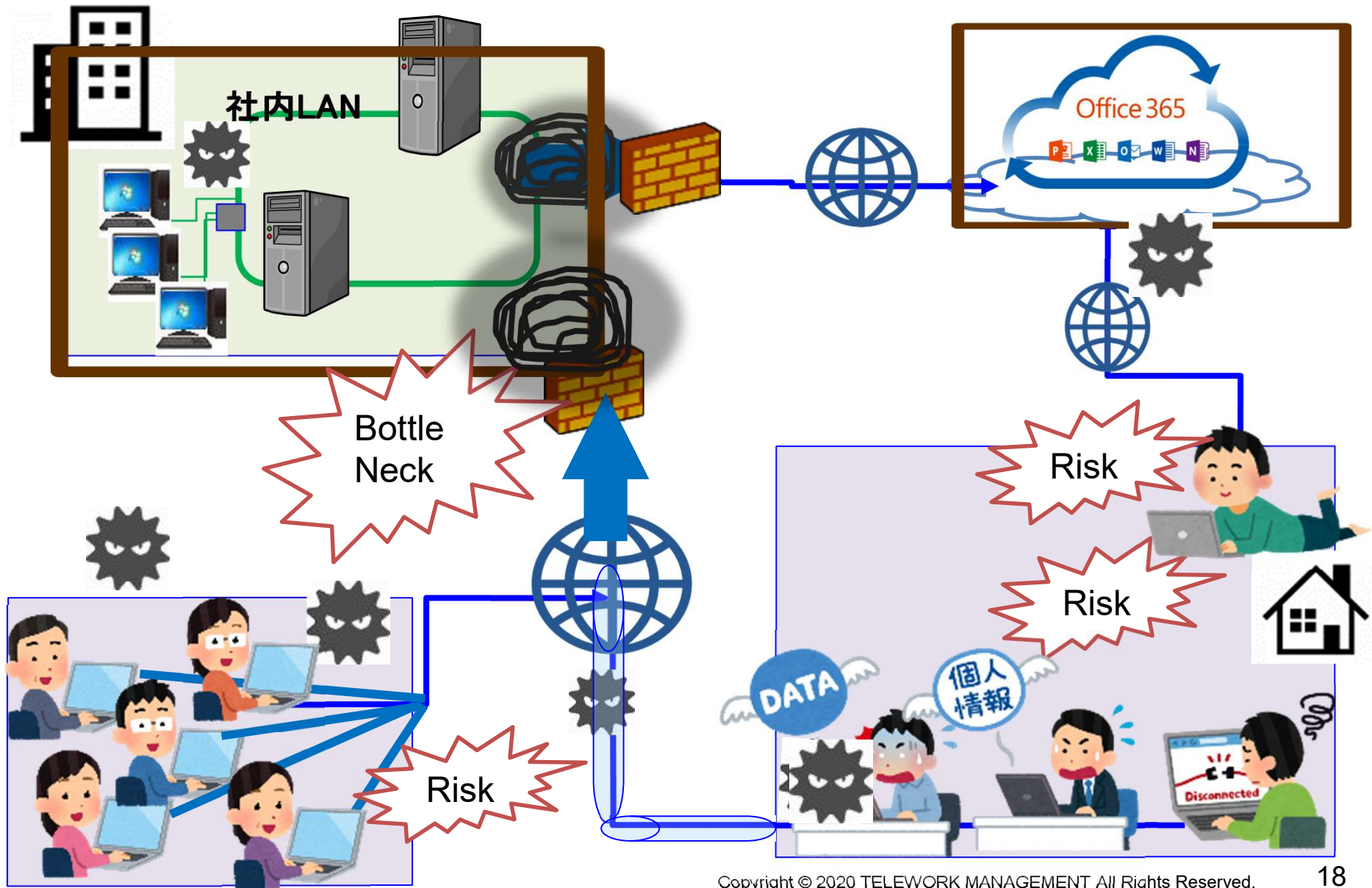
Underコロナ期に発生した課題

3.1.現在はハイブリッドクラウド型



※VPN=Virtual Private Network

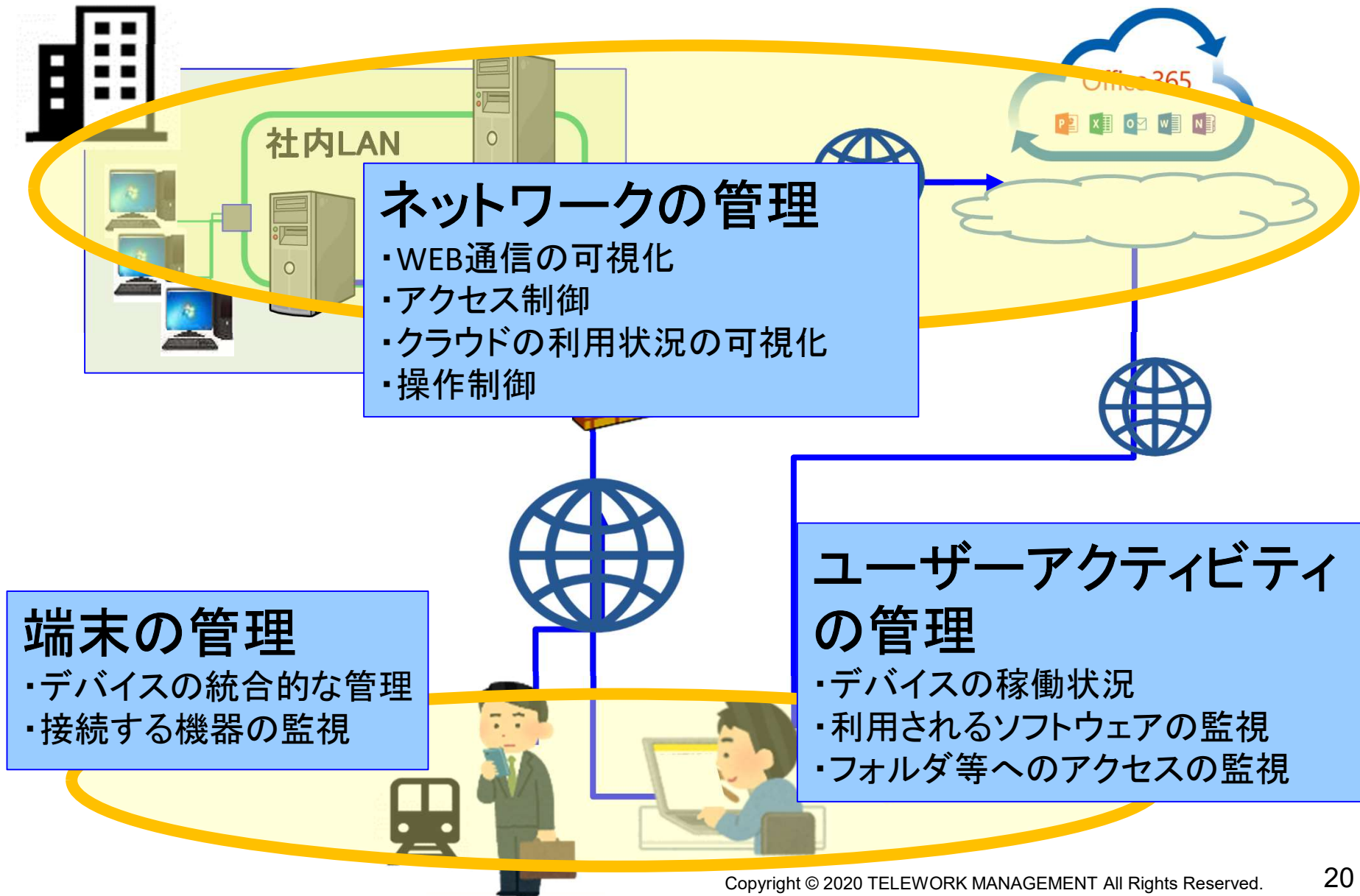
3.2.Underコロナ期の課題



ゼロトラストとは
「すべてのトラフィックを信頼しない
ことを前提とし、検査、ログ取得を
行う」という考え方

もはや、社内と社外の「境界」を守るだけでは
セキュリティは守り切れない

3.4. 管理・監視すべきポイントは3つ



ネットワークの管理

4.1. ネットワークを管理するサービス

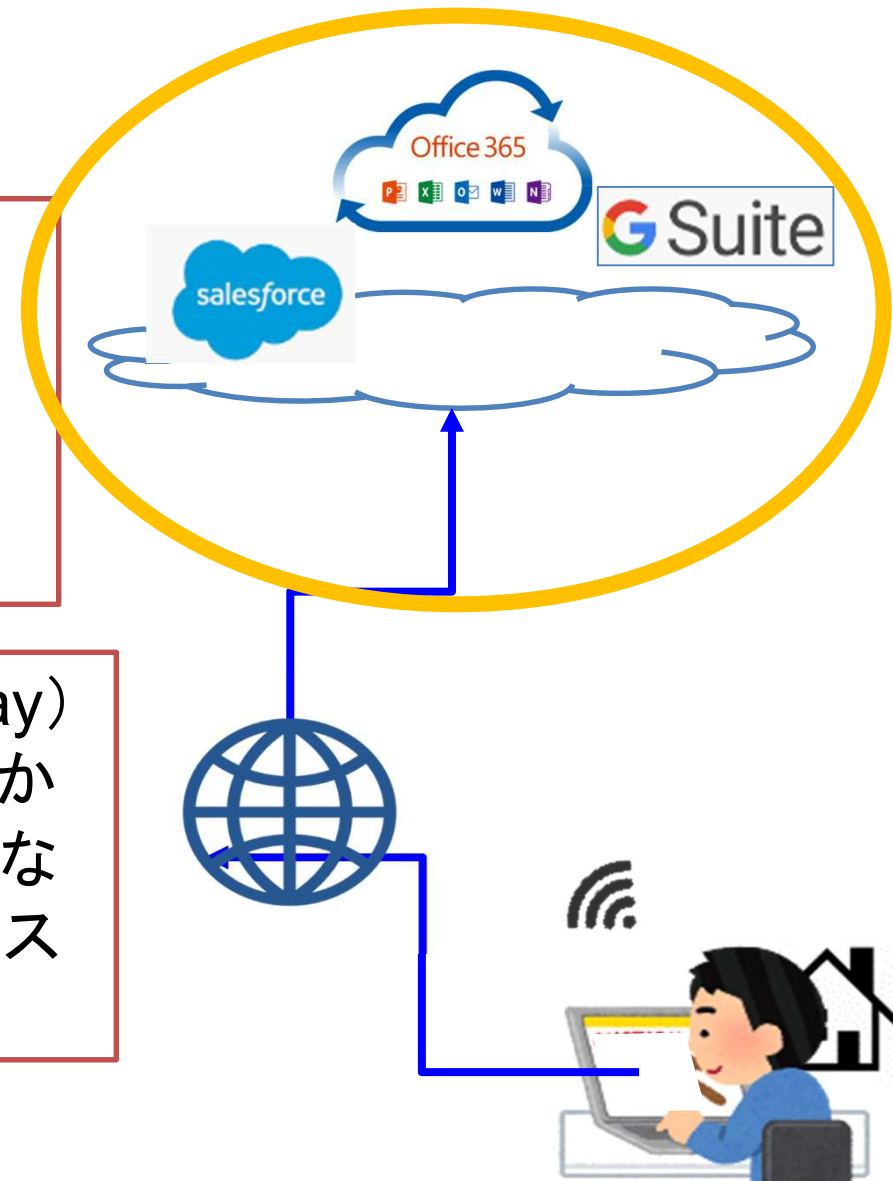
ネットワークの管理

■ CASB (Cloud Access Security Broker)

クラウドの利用状況の可視化、
操作制御

■ SWG (Secure Web Gateway)















アクセス先のURLやIPアドレスからその安全性を評価し、安全でないと評価された場合にはアクセスを遮断



4.2.(製品例) Microsoft365

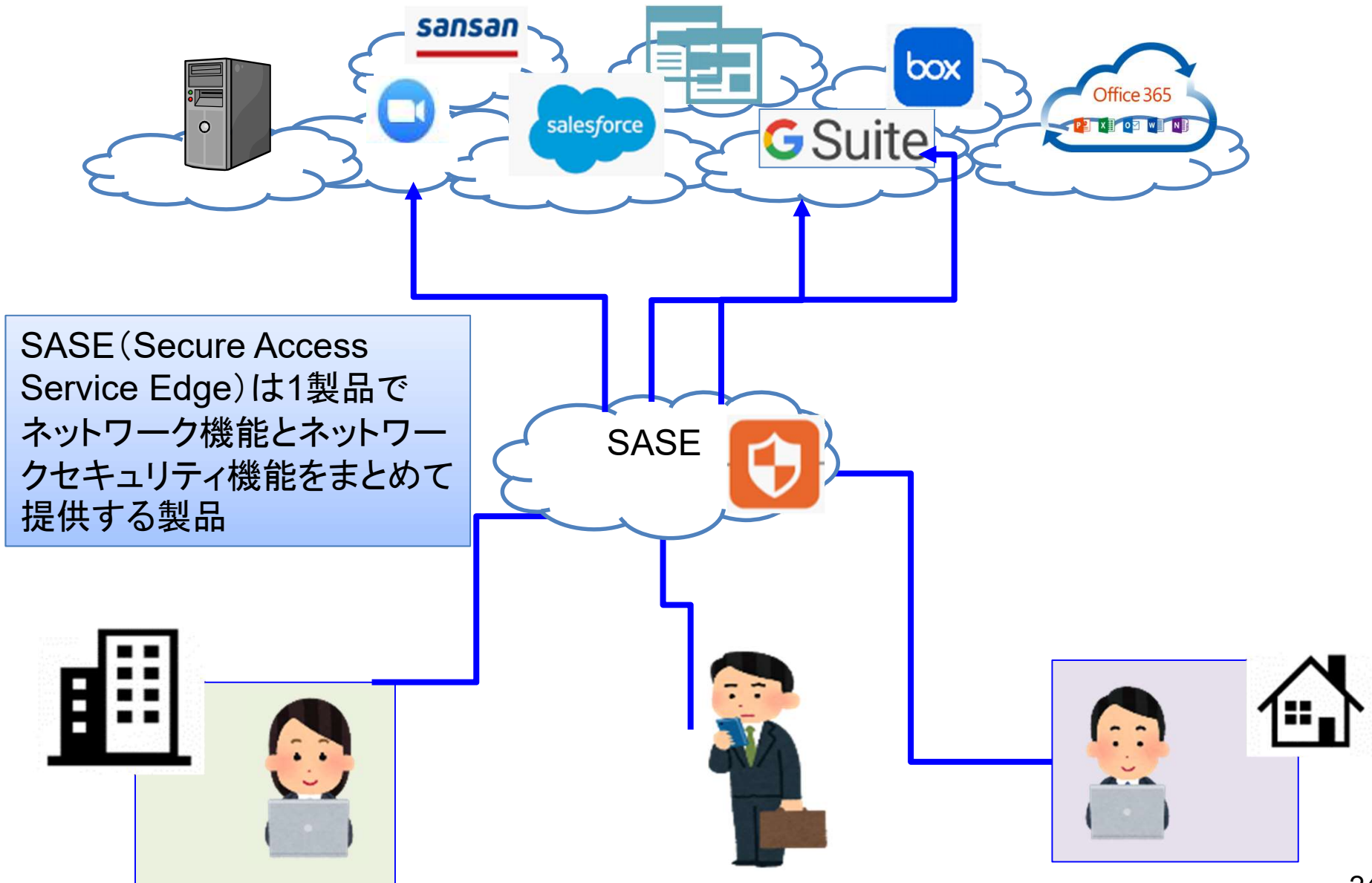
Microsoft365とは、Office製品やOneDrive,teamsなどを含むサブスクリプションサービス。

プランによってはデバイス管理、ID管理、アクセス制御機能などもワンストップで提供

Microsoft 365 Business Basic	Microsoft 365 Business Standard	Microsoft 365 Business Premium
¥540 ユーザー/月相当 (年間契約)	¥1,360 ユーザー/月相当 (年間契約)	¥2,180 ユーザー/月相当 (年間契約)
このプランに含まれる安全なクラウド サービス	このプランに含まれる安全なクラウド サービス	このプランに含まれる安全なクラウド サービス
  Exchange OneDrive	  Exchange OneDrive	  Exchange OneDrive
  SharePoint Teams	  SharePoint Teams	  SharePoint Teams
		  Intune Azure Information Protection

Microsoftのサービスでネットワーク＋
端末・ユーザーアクティビティを一括管理

4.3. 今後はネットワークとセキュリティをまとめた製品も増加



SASE (Secure Access Service Edge) は1製品でネットワーク機能とネットワークセキュリティ機能をまとめて提供する製品

ハードウェアとユーザーアクティビティの管理

5.1.エンドポイントを管理するサービス

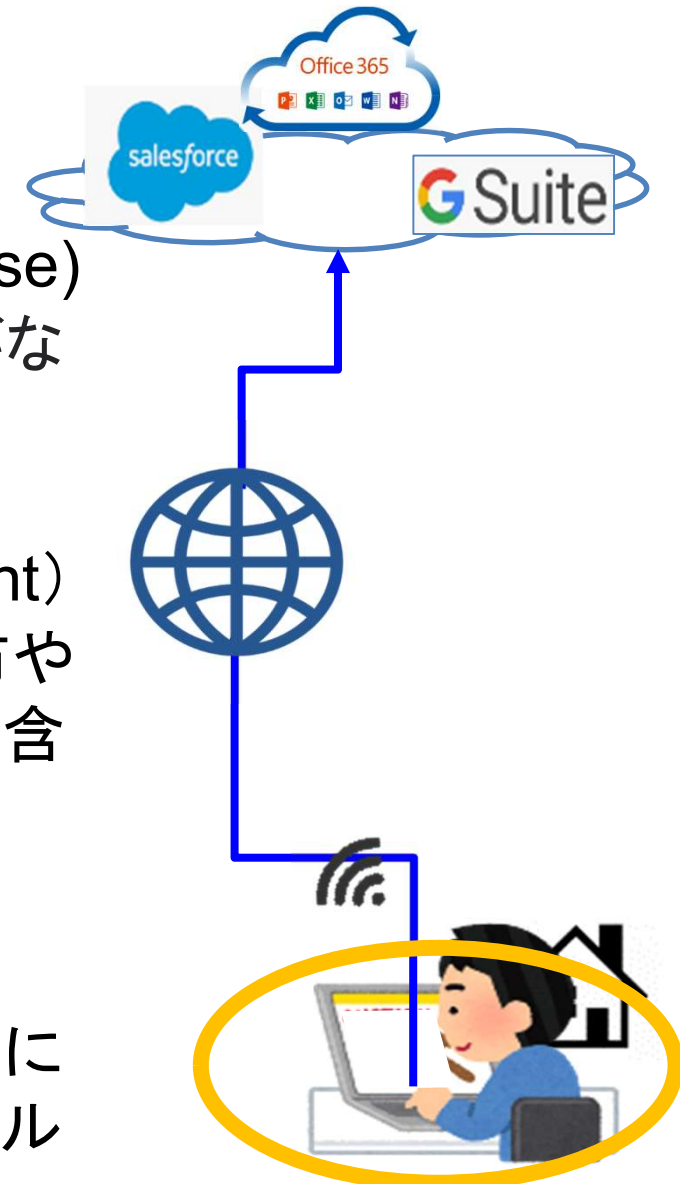
端末の管理

ユーザーアクティビティ
の管理

■ EDR(Endpoint Detection and Response)
端末上でマルウェア等による不審な動きがないか常時監視するツール

■ EMM(Enterprise Mobility Management)
端末に対して、リモート制御、アプリの配布や利用制限、コンテンツの保存の制御などを含む、総合的な管理を行うツール

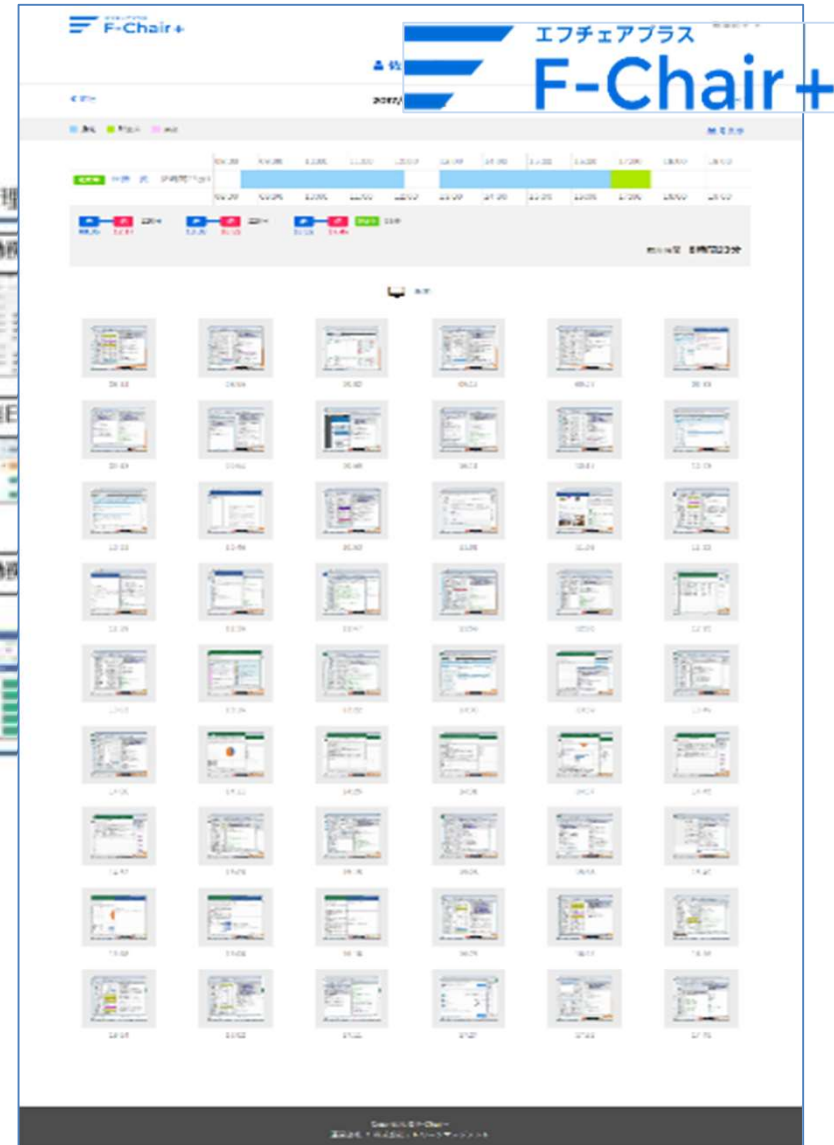
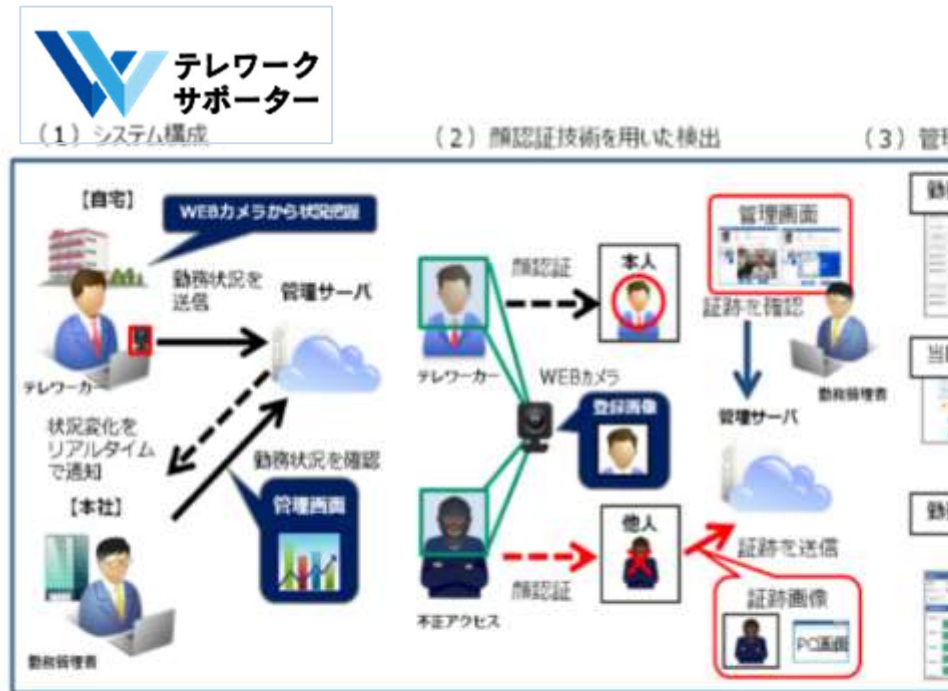
■ MFA(Multi-Factor Authentication)
本人確認のための要素を複数、ユーザーに要求する認証方式(=多要素認証)のツール



5.2.貸与PCはしっかり対策

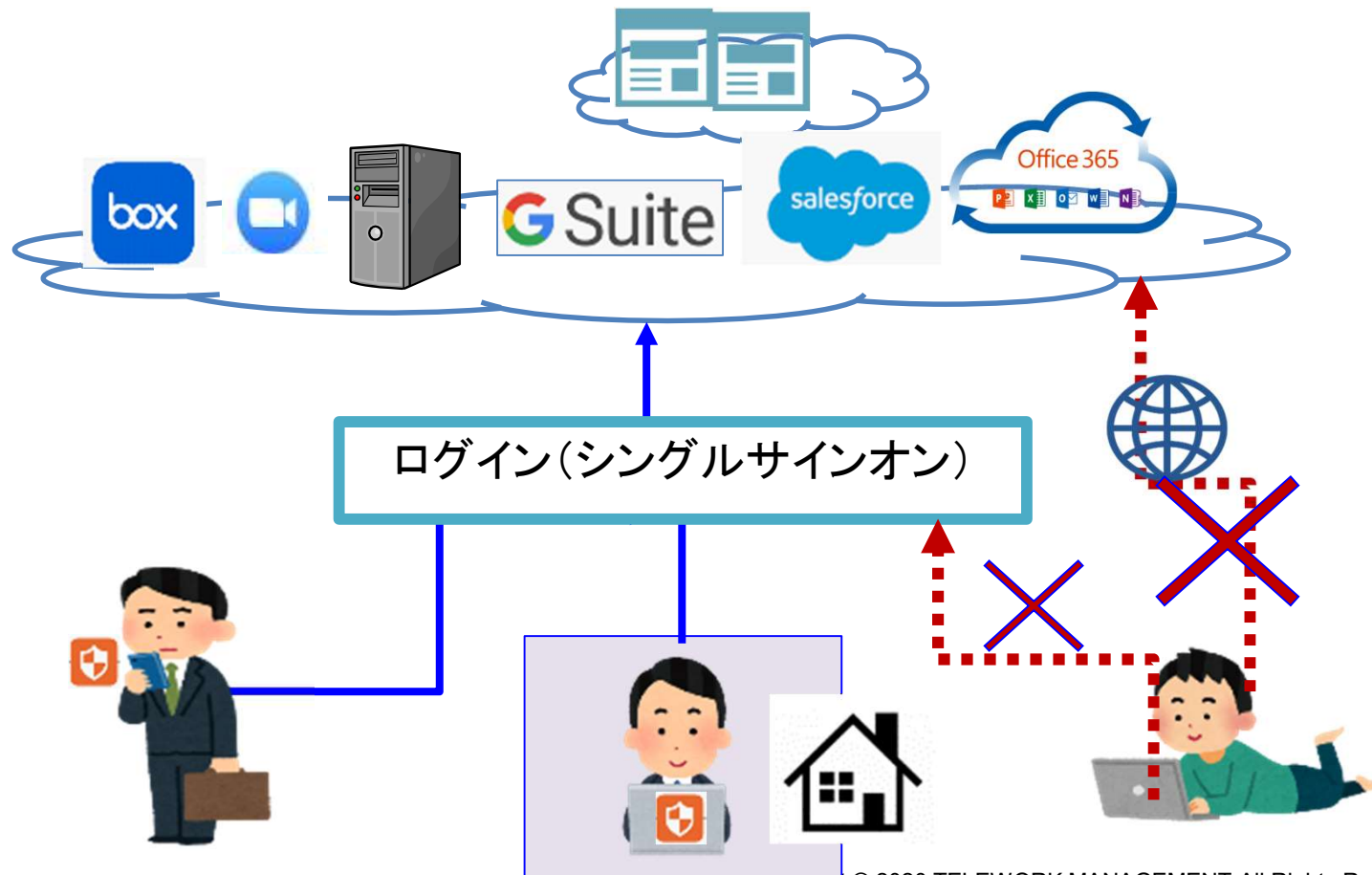


5.3.内部不正防止、ショルダーハック対策



5.4.私物端末利用の場合でもできる対策

セキュアブラウザを利用し、必要な情報に安全にアクセス。しかも手元に情報が残らない



5.5.今、必要なこと

まずは今のテレワークの状態をチェック

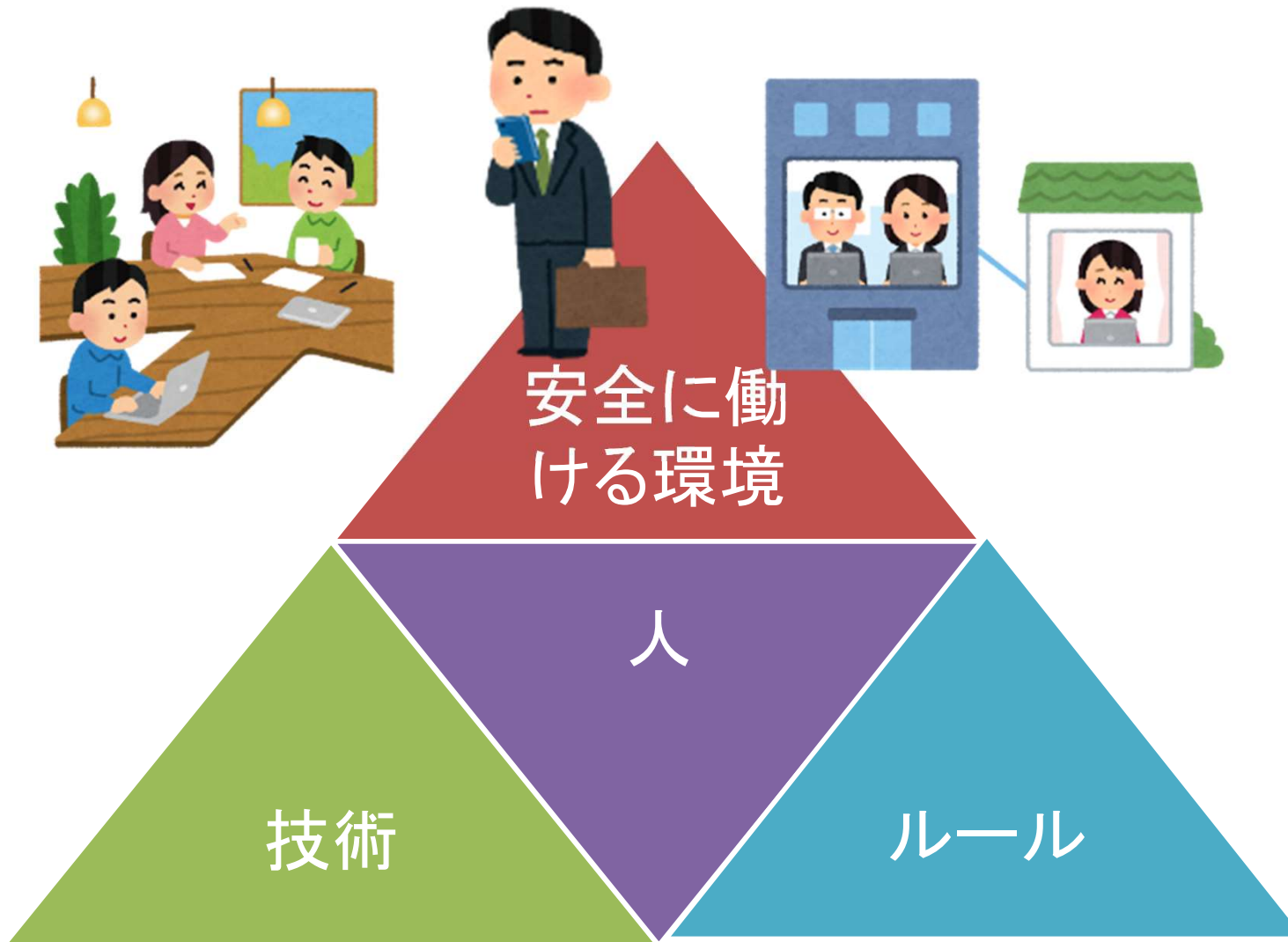


誰がどこで何を使って、どんな業務をするのかを整理



情報のアクセス権やテレワーカーの環境を管理
＜ネットワーク内＞ ＜エンドポイント＞

5.6.「技術＋ルール＋人」への対策が重要



ご清聴いただきありがとうございました。