オンライン・セミナー

リモートワークのセキュリティ エッセンシャル

中小企業向け、はじめてのリモートワーク

INJANET

本セミナーの目標

- 今までリモートワークなどしていなかったけれど、しなければならなくなったシステム管理者
- システム管理者を置く余裕の無い中小企業（組織）の方
- リモートワークによってセキュリティリスクを増やしたくない方

が、最適なリモートワーク環境を決めて、安心してリモートワーク環境を構築できるようになる。

さまざまなセキュリティ上の注意点をまとめました。

ローコストでも安心できるリモートワーク環境の実現

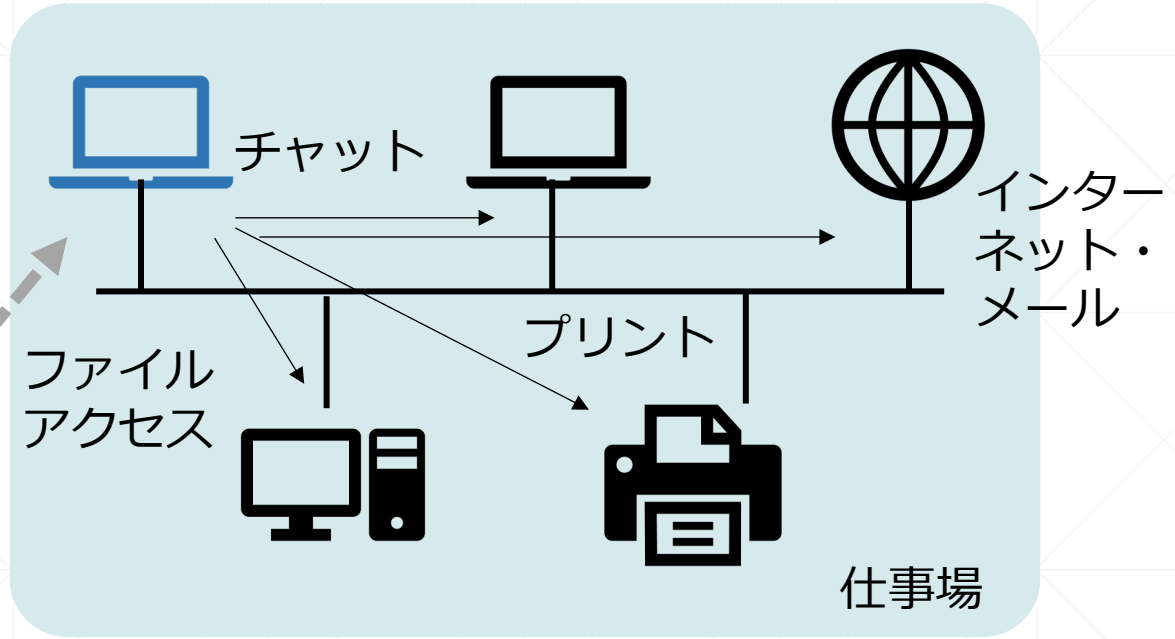
ここで学ぶ内容

1章　リモートワークで何ができるのか？
2章　リモートワークの危険性
3章　リモートワーク環境の形態
4章　ファイル交換
5章　テレビ会議
6章　統合アプリケーション
7章　VPNとリモートデスクトップ
8章　まとめ

当セミナー内容は、INJANET社が調査したOSINTOの手法と、実体験での範囲の内容です。
内容の正確性や、情報の変化については責任は責務を負いかねます。

１章　リモートワークで何ができるのか？

- 理想は、仕事場で行っている仕事がすべて自宅（や仕事場と異なる場所）で遂行できる環境
- 実際は実現コストを考え
  何を制限するかを検討します



１章　リモートワークで何ができるのか？

- メールやインターネットアクセス
- チャットやテレビ会議
- 資料の印刷
- ファイルサーバのアクセス（共有ファイルの編集）
- 勤怠等の申請　など

リモートワークでは何をどのような方式で実現するかで、
環境設定の手間とコスト、セキュリティレベルが変わります

2章　リモートワークの危険性　–守るべきもの

まず、考えてみましょう

- 仕事場でセキュリティが脅かされた時に影響を受けるものは何でしょう？
  - お客様の情報
  - 固有の技術やサービスのノウハウ資料
  - 社員のメールアカウントや人事情報
  - 組織の資産そのもの
  - 組織の提供するサービス

最近、特に中小企業では、社員のメールアカウントが盗まれ、そこから取引先大企業へ標的型メールが送付されるサイバー攻撃の足場となっています

2章　リモートワークの危険性 –被害

まず、考えてみましょう

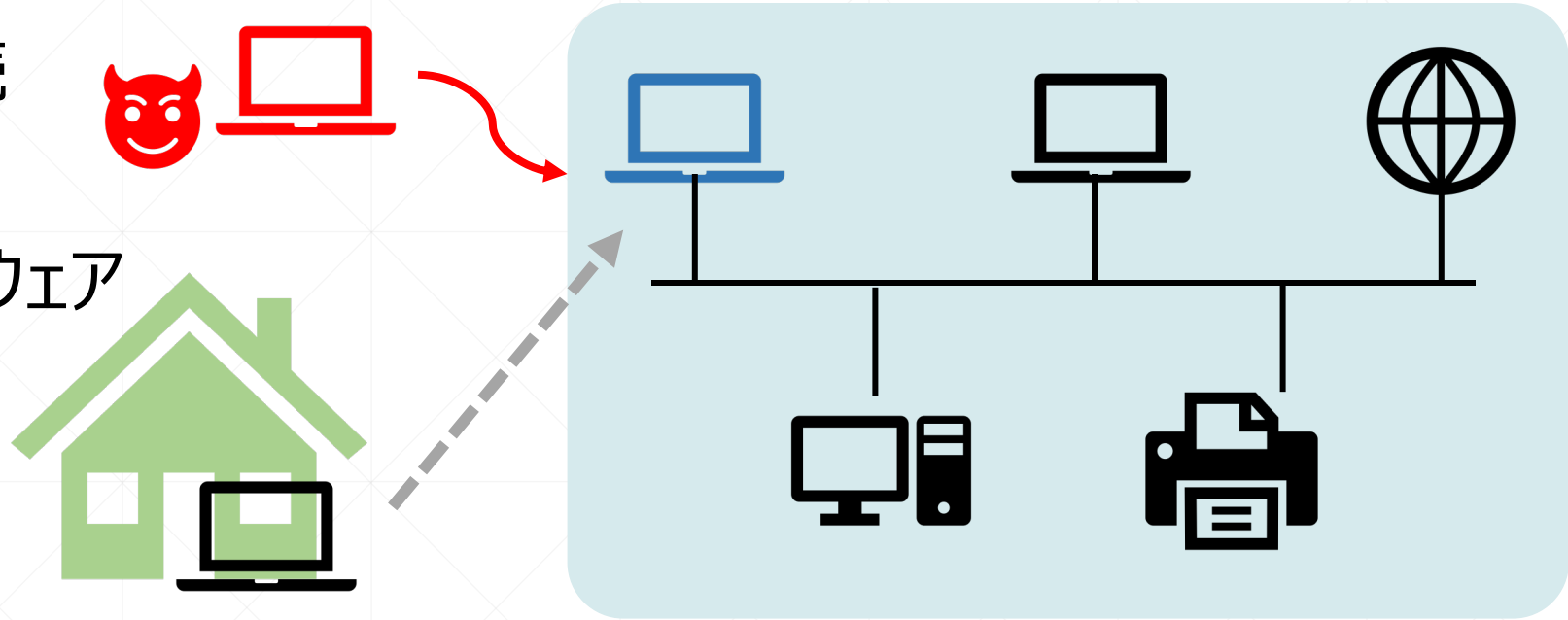
- 仕事場でセキュリティが脅かされた時何が起こるでしょう？
  - お客様の情報：個人情報保護法違反、顧客の喪失
  - 固有の技術やサービスのノウハウ資料：優位性の低下
  - 社員のメールアカウントや人事情報：標的型攻撃の足場、人の引き抜き
  - 組織の資産そのもの：資産（機器）の故障、機能停止
  - 組織の提供するサービス：サービスの停止

2章　リモートワークの危険性 –攻撃の手口①

①組織の内部に直接侵入される

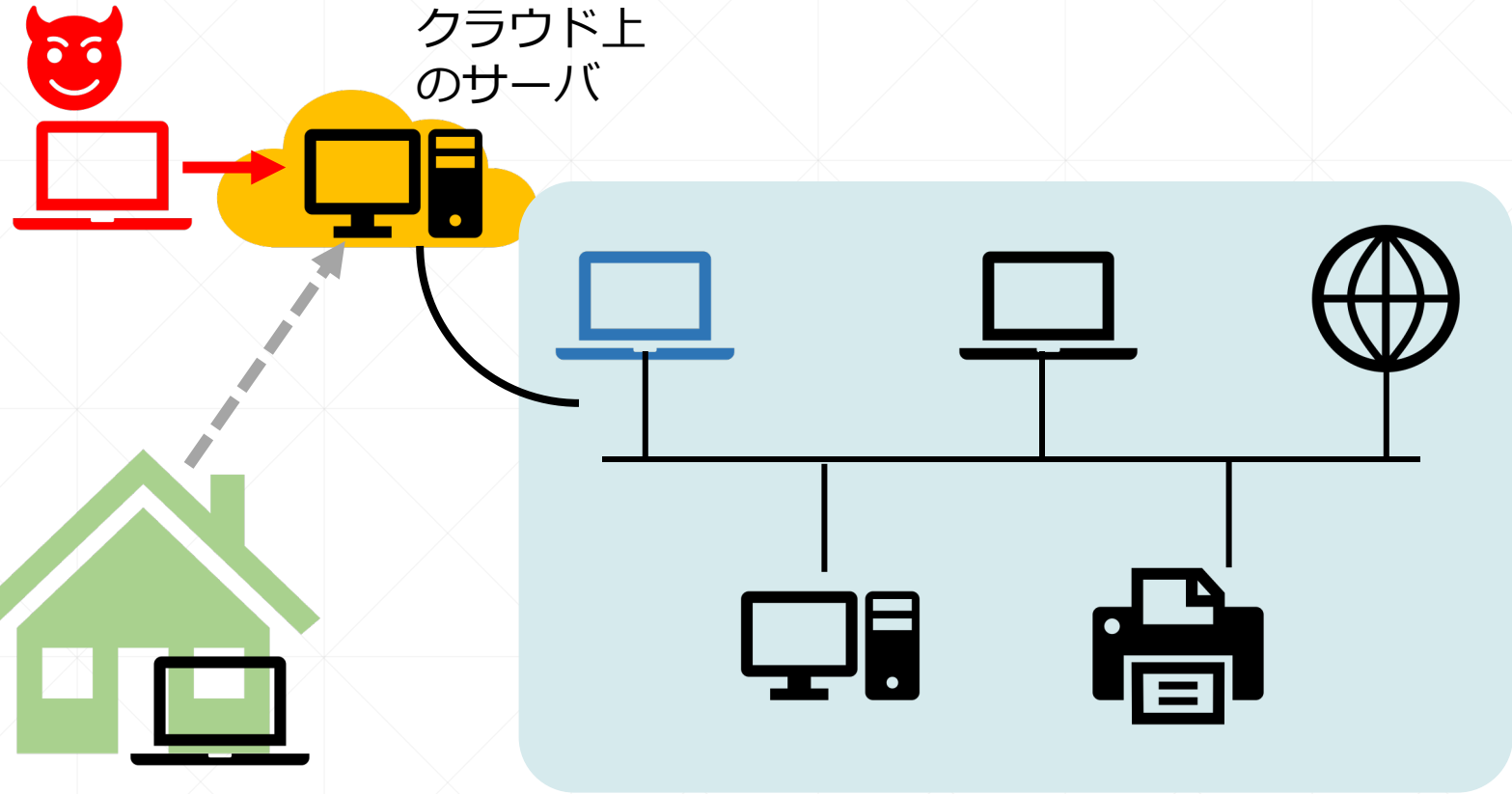
・接続口に悪意ある外部者が接続

・家のPCがマルウェアに感染し内部にマルウェアを持ち込む



2章　リモートワークの危険性 –攻撃の手口②

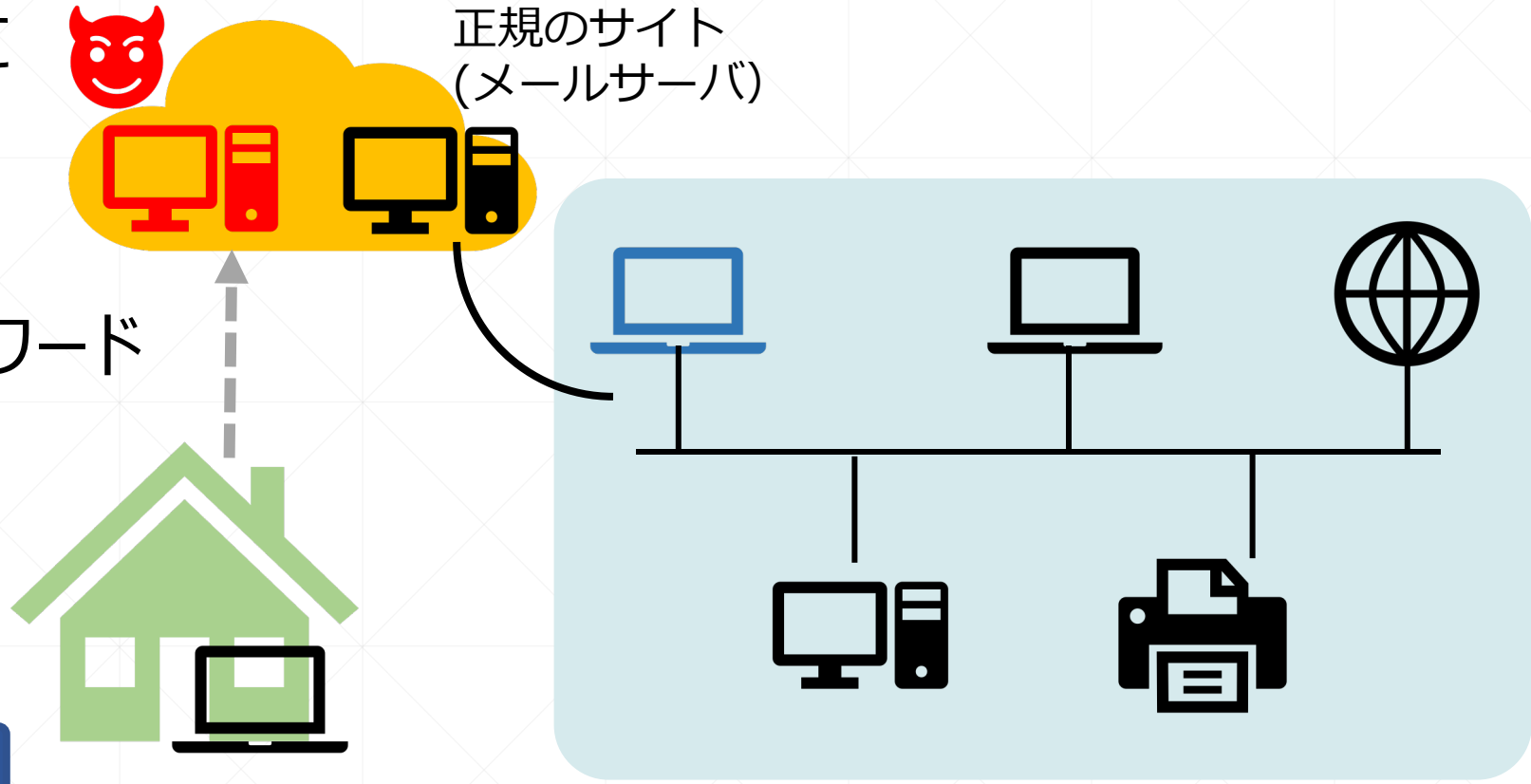
②インターネット上のリモートワークサービスを攻撃



クラウドのセキュリティは利用者側が考えること

2章　リモートワークの危険性 –攻撃の手口③

③インターネット上に
偽のサイトを立て、
そこにアクセスした
アカウントID,パスワード
を窃取する



最近の流行です

3章　リモートワーク環境の形態　～方式

- リモートワークの方式にはさまざまな種類があります

　総務省の「テレワークセキュリティガイドライン　第4版」では、4つのパターンが示されています。

パターン①　リモートデスクトップ方式

パターン②　仮想デスクトップ方式

パターン③　クラウドアプリ方式

パターン④　会社PCの持ち帰り方式

小規模の組織では、パターン⑤として、自分のPCでサーバに直接VPNアクセスする形態も考えられます

3章　リモートワーク環境の形態 パターン①

- パターン①　リモートデスクトップ方式

　仕事場に設置されたPC等の端末の画面をそのまま
リモート端末で表示させる方式です。

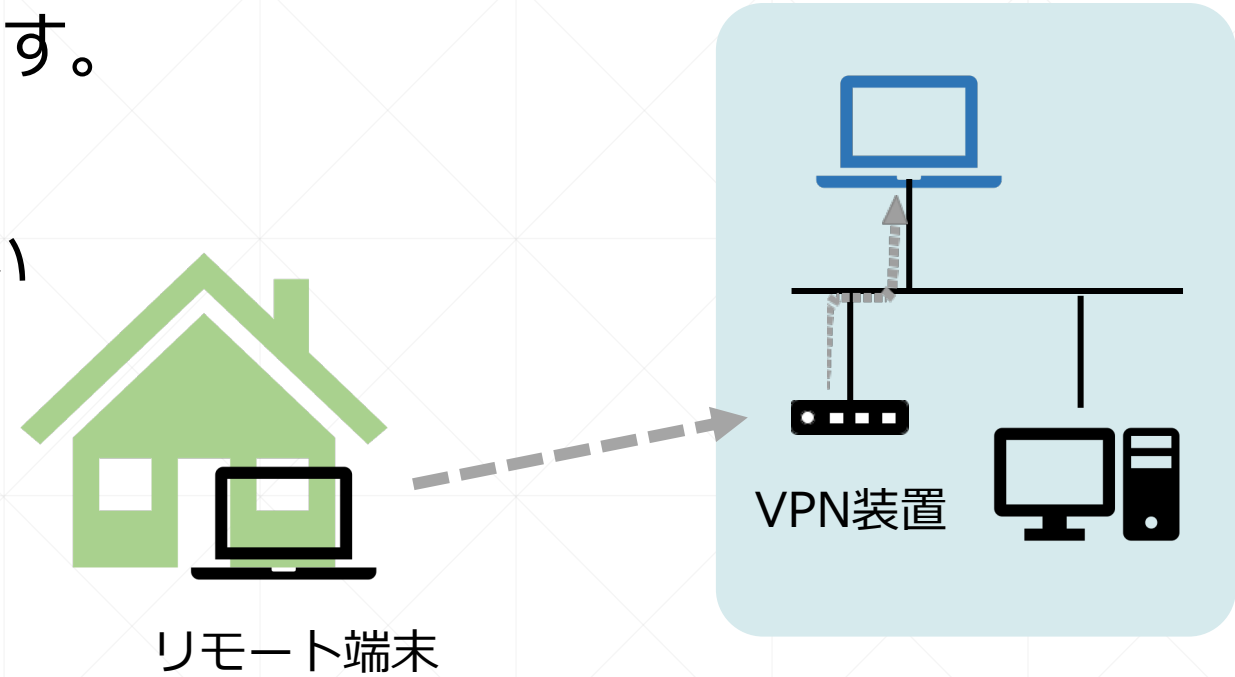
【特長】

リモート端末にデータを保存しない

仕事場の環境がそのまま使える

高速のインターネット回線が必要

VPNに侵入されると仕事場に
接続されたのと同じ危険性あり



3章　リモートワーク環境の形態　パターン②

- パターン②　仮想デスクトップ方式

　仕事場に設置されたサーバ上の仮想デスクトップ(VDI)に接続する。仕事場端末は不要、サーバは必要。

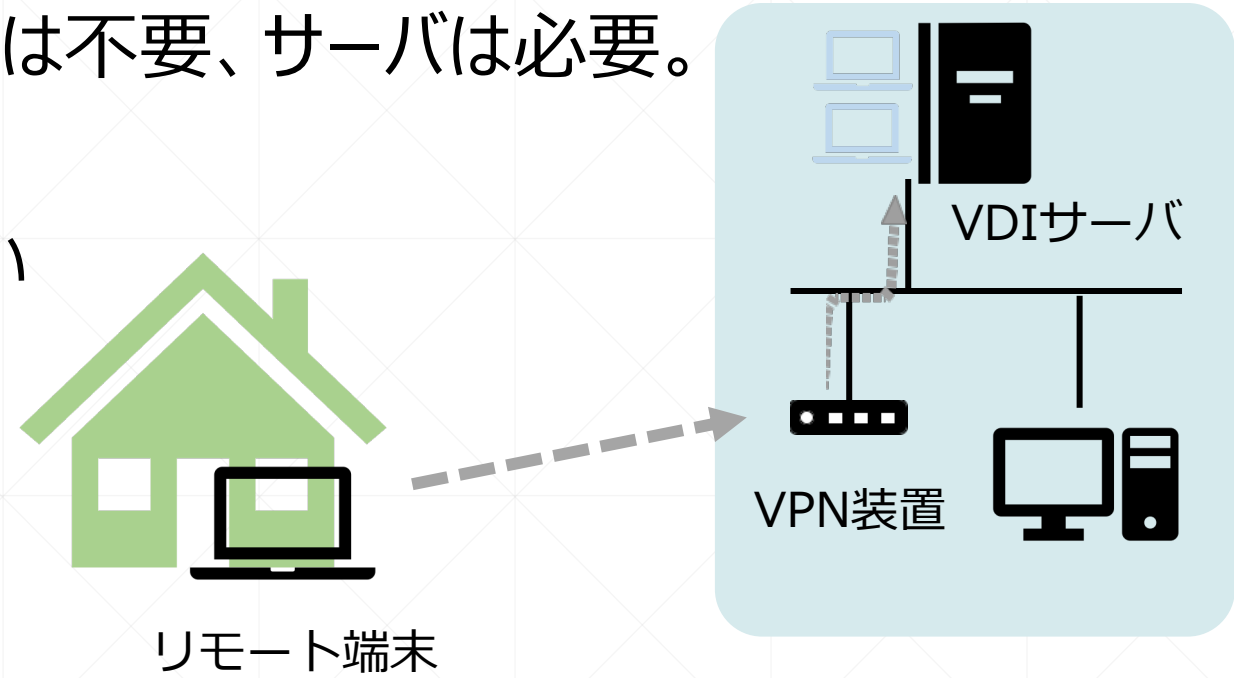
【特長】

リモート端末にデータを保存しない

仕事場の環境がそのまま使える

高速のインターネット回線が必要

VPNに侵入されると仕事場に接続されたのと同じ危険性あり



3章　リモートワーク環境の形態　パターン③

- パターン③　クラウド型アプリ方式
  クラウド上のアプリケーションを社内外から利用

【特長】

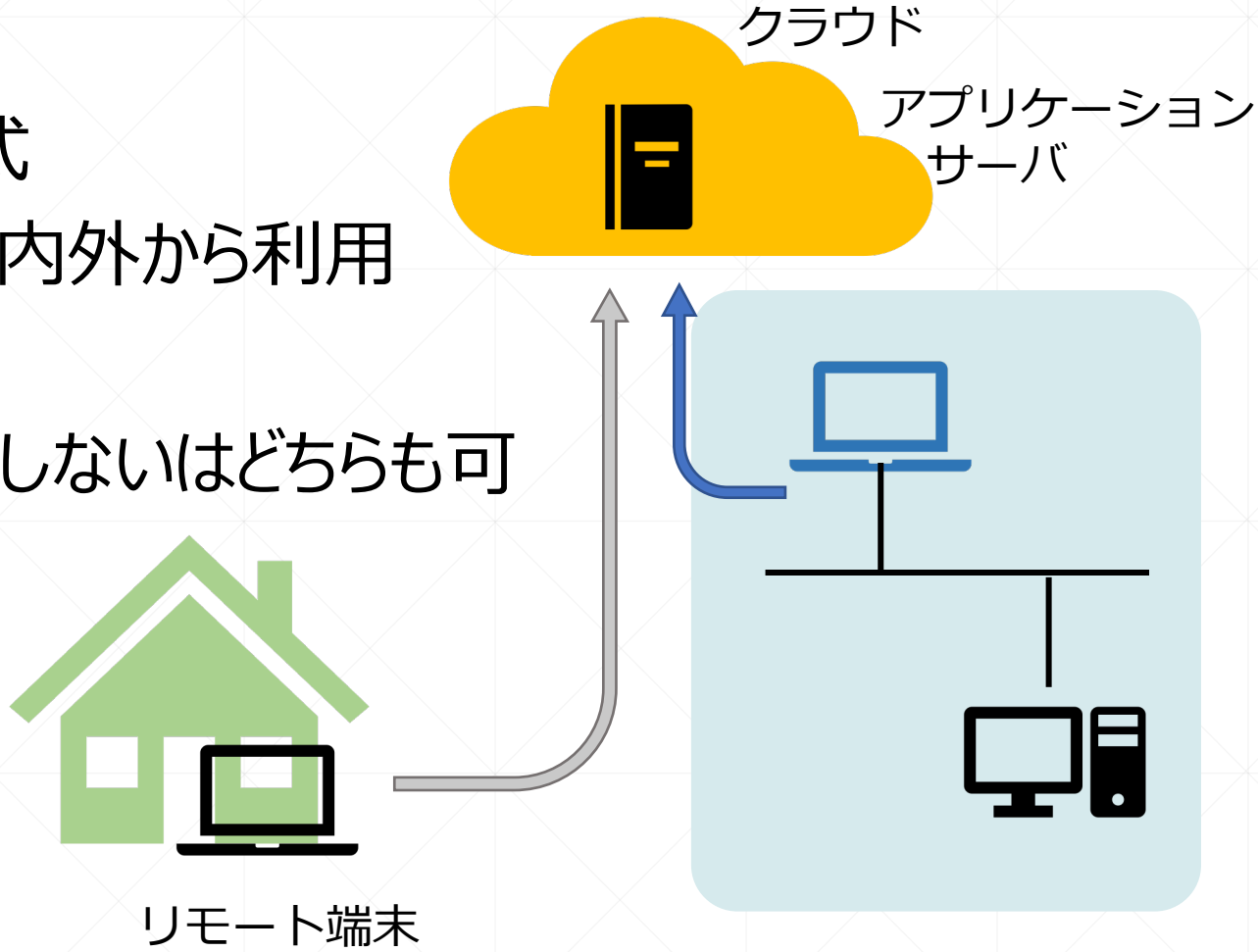
リモート端末へのデータ保存する/しないはどちらも可

サブスク形式が多い

セキュリティはクラウドに実装され

た機能をユーザがどう利用するか

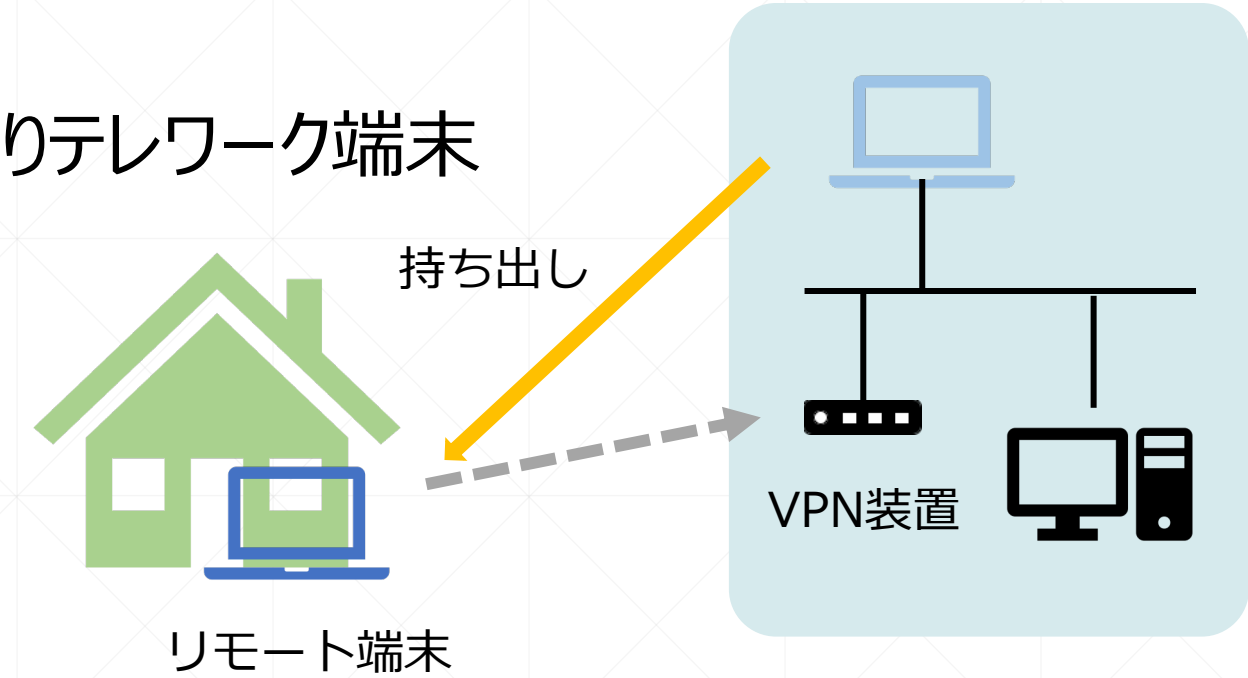
スタート時の負荷が少ない



3章　リモートワーク環境の形態 パターン④

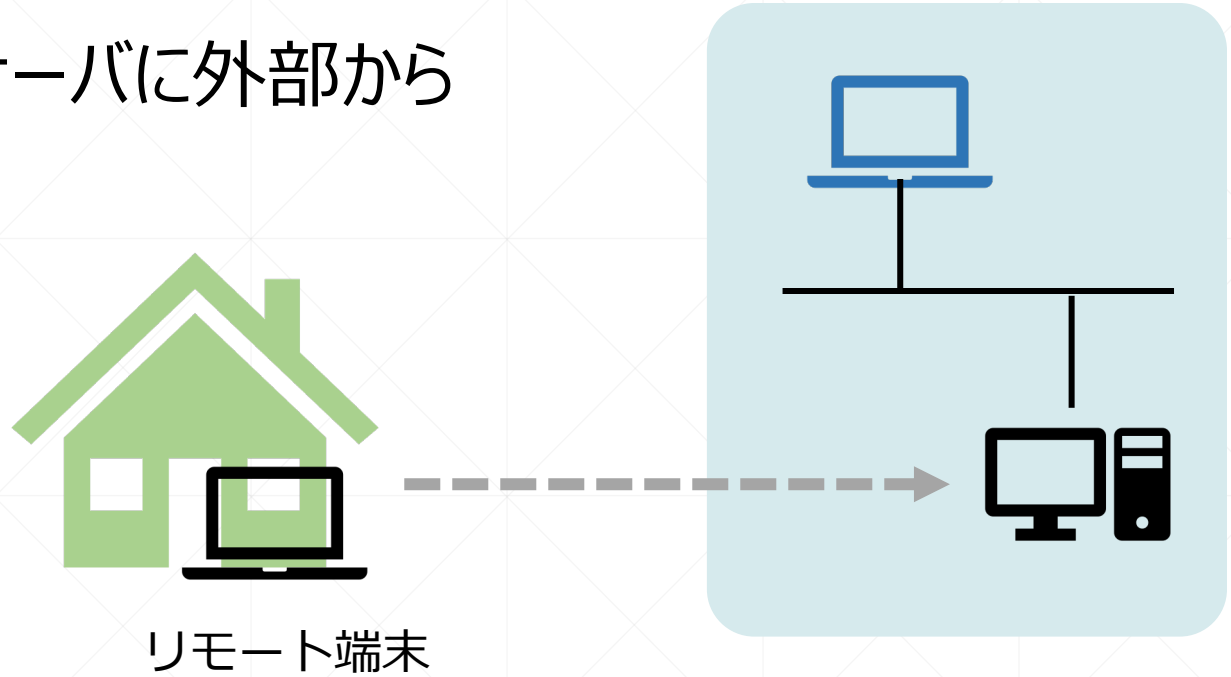
- パターン④　会社PCの持ち帰り方式
  会社PCの持ち帰り方式

【特長】
仕事場のPC（端末）を持ち帰りテレワーク端末として利用する
PCにデータを保存する
仕事場にはVPN接続する
VPNに侵入されると仕事場に接続されたのと同じ危険性あり



3章　リモートワーク環境の形態 ⑥

- パターン⑤　サーバのみVPN接続（ガイドラインには記載無し）
- 【特長】
  自社ドメインが無くても手軽にサーバに外部から
  アクセスできる
  ルータの設定は必要
  サーバ自体にVPN機能を
  持つ特定の機器による
  個人所有のPCから接続も



4章　ファイル交換(クラウドアプリケーション方式)

- 少し前まで「宅ファイル便」というサービスがありましたが、セキュリティが確保出来ず廃業しました　→　セキュリティの確保は難しい課題です
- Office 365のOne Drive の認証
- Google Suiteの公開設定

に要注意です。

Offce365では、偽のサイトに誘導されアカウント情報を盗まれる事件が多発しています。

いっぽう、ファイルアクセス時の多要素認証といったセキュリティ強化機能もあります。

5章　テレビ会議①

- リモートワークで今一番注目されているのが、テレビ会議です。
- さまざまなTV会議システムがありますが、手軽、低コストでセキュリティ上安心できるシステムは多くはありません。
- よく利用されているTV会議システム
  - Zoom:とても便利ですが、急成長したためかセキュリティ上問題が多く社用には適しません（Zoom爆弾、IDの漏えいなど）
  - Skype/Slype for Business:Skypeは10人まで、Businessは250人まで　Businessの方はセキュリティは強固と言われていますが、通信自体は不安定になる事もあります
  - Google ハングアウト：10人まで(ハングアウト Meetは250人)。回線の影響は経験上受けにくいです。

5章　テレビ会議②

- テレビ会議では、マイクやカメラ、スピーカーにも注意が必要です。（うまく動作させるためにも、セキュリティ上も両方）
- 快適な環境のためには、ヘッドセットを使ったり、ノートパソコンのマイク、カメラ、スピーカを使うと設定が楽です。
- セキュリティ上は、スマートスピーカーやWebカメラでは、覗かれる危険性が無いわけではありません。Webカメラのシャッターやノートpcのカメラカバーなど、物理的に蓋をするものが確実です。

弊社では、さまざまな形態の会議の経験がございます

6章 統合アプリケーション

- とりあえずリモートワークをしなければ、というケースで投資や時間があまりかからないためお勧めします
- Office 365、G Suite
  - 月数百円/人からのサブスク形式
  - オフィスを既に持っている場合、TV会議などグループ向けサービスの提供あり(Office 365 Business Essentials)
  - Windows, Macの混在可能（一部機能が異なります）
- セキュリティ上設定を誤らなければ安心
- G mail, Google Driveではアンチウイルス有、OneDriveでは世代バックアップ有

7章　VPNとリモートデスクトップ ①

- セキュリティ観点からの注意点
  - クラウド型を除く方式：VPNの接続方式と管理
  - クラウド型：クラウドのセキュリティ設定
- VPN方式とセキュリティ
  - PPTP:低価格のルータなどで持つものがありますが、危険です。（暗号化方式がWiFiのWEPと同じRC4）
  - L2TP/IPSec:ハッキング方法が研究されているとの事で、利用を避けるのが良いでしょう
  - 推奨はSSL-VPNかOpenVPNです。
- 安全のため**UTM**を導入する案もあり

VPNやUTMは知識とノウハウが必要です→ご相談ください

7章　VPNとリモートデスクトップ ②

- リモートデスクトップ
  - WindowsのRDP接続、VM ware、ブラウザ上でリモート環境を実現するなど各種の方法があります。
  - デスクトップの画像情報を送信するため、通信速度を十分確保した回線が必要になります。（特に昇りの速度が遅い回線の場合は注意が必要です）

中大規模向けで、管理工数を減らす事ができますが、投資は必要です。
（弊社ではサポート不可。ベンダーにお尋ねください）

8章　まとめ

- リモートワークを支えるシステムにはいくつかに方式がありますが、そのセキュリティのポイントはいくつかに絞られます。
- ただし、適切にそのポイントを押さえないと、仕事場全体のセキュリティを脅かす事になります。
- 今回書いた以外にも、USBメモリのセキュリティや、リモート端末のセキュリティなど考慮すべき点は他にもあります。

弊社では、無料のツールを極力利用するなど、低価格で手間がかからずセキュアなリモートワーク環境を実現するサポートをしています