サテライトオフィスに必要な
セキュリティとは？

～リモートワーク環境整備の落とし穴～

2021/8/4

㈱未来研究所

小林　忍

自己紹介

未来研究所
Future Research Inc.

小林　忍（こばやし　しのぶ）

代表取締役　㈱未来研究所　（2021年1月～）
取締役社長　アライドテレシスアカデミー（株）（2016年1月～2019年12月）
非特定営利活動法人　医療福祉クラウド協会　監事、等
講師　早稲田大学NEO　リカレント教育コース　IT分野での新規事業・起業
講師　神奈川大学　　リカレント教育コース　IT分野での新規事業・起業、サイバーインシデント発生、その時どうする？
（SOHO～中堅企業版）

三重県出身　愛媛大学卒業後、大手電機メーカ、外資企業、起業、会社譲渡を経、現職

【代表的な事業化】
＊サイバーセキュリティ分野でISACA　CSX（クラウド上でインシデント・シナリオ対応を実践学習できるeラーニング）を世界で初めて代理店契約を締結し日本で販売中
＊Extreme（L3 S/W）社の世界で4番目のOEMを締結し、アライドテレシスのS/W事業の基礎を構築
＊日本で初めてNetscapeを販売
等があり、主に海外商材・ソリューションの日本事業展開において多くの実績を有します。

【現職】
IT分野と教育の融合事業を主軸とし、サイバーセキュリティ分野でのCSIRTメンバーに　向けた教育事業、およびコンサルティングを実施。
各種、団体および警察庁・大学等にてサイバーセキュリティ人材育成のセミナーを実施

【履歴概要】
愛媛大学　工学部卒
＊現在：　㈱未来研究所　主にサイバーセキュリティを主軸にした各種ソリューションの提供事業　及び　“未来の学舎”の事業化促進
＊2016 ー　2019/12月 アライドテレシスアカデミー（株）（サイバーセキュリティ教育事業の企画・実施）　ISACA CSXの再販商材等、研修ソリューションを、レベル1～5までを構築。　経済産業省、第四次産業革命スキル習得講座の認定も取得。Level1～2コースは、JMOOCでも採用され第2位 2019年の実績。　警察庁、サイバー系団体にて、サイバーインシデント現状等、セミナー講師を多数実施。　NISC様での種々採用を機に、アライドテレシス（株）への合併が決定（2020年1月）
・アライドテレシスアカデミーにて、サイバーセキュリティ研修マップ、および研修ソリューションをゼロから構築し、実施運営を実施
＊2006-2016 スリーイーグルス（株）代表取締役（ ITソリューション構築、教育事業、人財派遣・紹介事業）、　**日本初のサイバー演習CYDER（総務省）にてJAIST協業にて、サイバーセキュリティ人材育成のためのITSSを参考にしたレベル定義と、各レベルでのスキル項目の洗い出し研修を構築。→　後の経団連・人材定義レファレンスの基となる。**　2016年にアライドテレシスグループに事業転売（M&A）

＊2000-2016 NACSE JPN（株）　代表取締役　（アライドテレシス100%子会社のIT教育会社）、ベンダーニュートラルなネットワーク資格の日本市場・中国市場への展開
＊スリーコムジャパン（株）　シニアディレクター・コア事業部、NC（＝SE）、ダイレクトタッチ営業本部
＊アライドテレシス（株）　プロダクトマーケティング部・部長、開発部課長
＊AMD（ Advanced Micro Devices ）Japan, テレコムエンジニア
＊NEC テレコムシステム（株）エンジニア、 TDM(Time Division Multiplexer)の設計、プログラミング

サテライトオフィスに必要なものは？

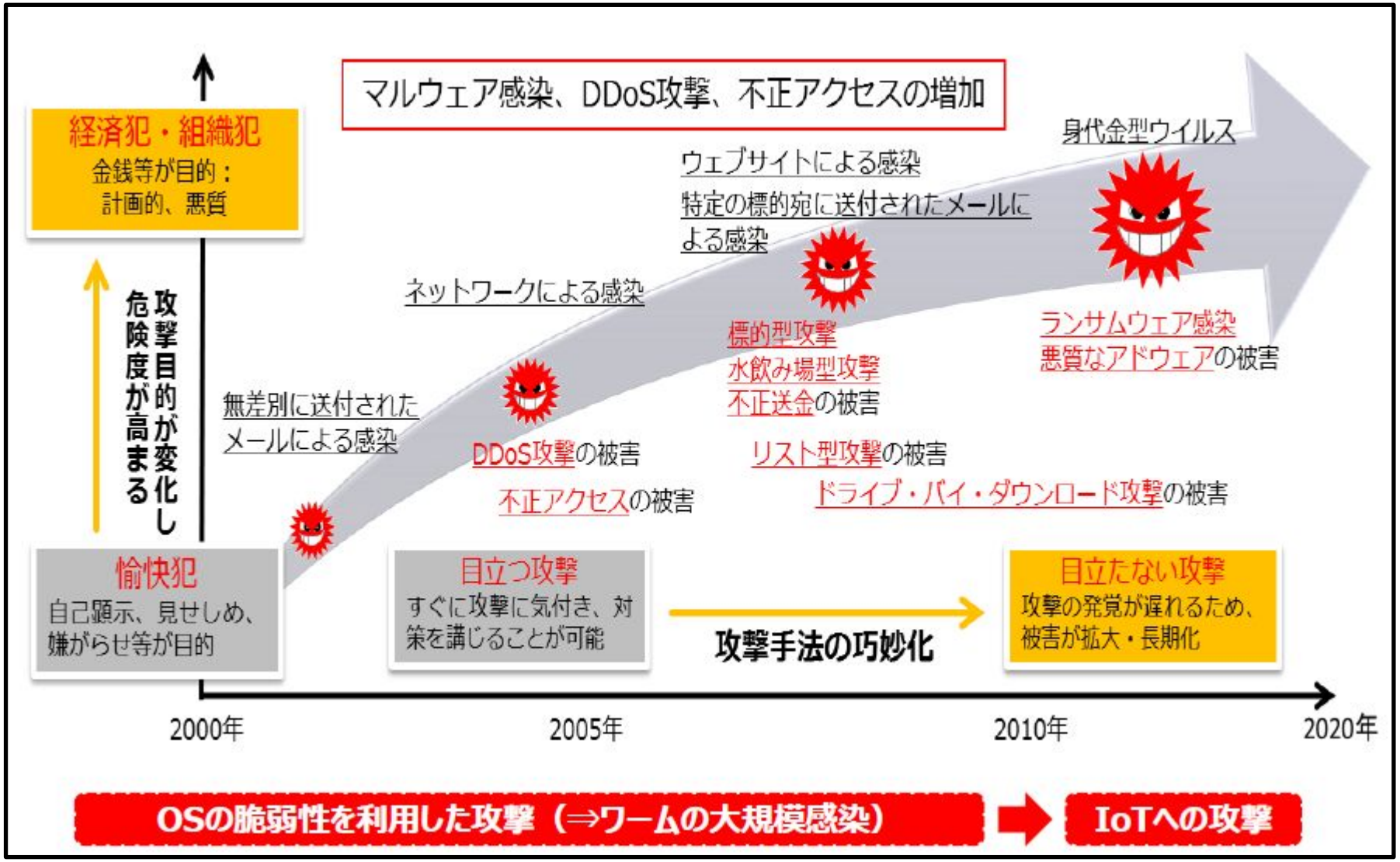
未来研究所
Future Research Inc.

- サテライトオフィスとは？
  - 対象のネットワーク規模
    - 本社 >> 支社・支店 >> **サテライトオフィス（社員数：1~10、NW端末数：20台前後、SOHO・リモートワーク含む）**
  - 従業員の働き方に重点を置いた呼び方
    - 働き方改革
    - 実現方法：リモートワークの環境整備

- 実現に向けて重要なことは、ルールの設定
  - ルール名　＝　セキュリティポリシー
  - セキュリティーポリシーを実現するための機材整備

サイバー攻撃の動向

サイバーセキュリティ脅威の遍歴



※リソース　総務省　　https://www.soumu.go.jp/main_content/000722477.pdf

2020年主なサイバー攻撃事例（日本）

4月　国内高校の半数が利用するClassi社が**不正アクセス**を受け、**IDや暗号化パスワード等が流出**した可能性が判明。

5月　NTTコミュニケーションズ従業員の**テレワーク環境(仮想デスクトップ)に係るアカウント及びパスワードが窃取**され、**顧客情報（防衛省等の政府機関を含む）が流出**した可能性が判明。

6月　ホンダが**サイバー攻撃**を受け、**世界の９工場で生産を一時停止**。

7月　Twitter社で**ソーシャルエンジニアリング**により社内ツールが不正利用され、詐欺投稿が行われ、**データも流出**した可能性が判明。

サテライトオフィスでのセキュリティが狙われる

8月　国内数十社において、**VPN機器の脆弱性を悪用した不正アクセス**が行われVPN接続用のパスワードなどが流出した可能性が判明。

9月　ドコモ口座が悪用され、第三者が**不正に入手した口座番号、暗証番号等を使用**した口座振替による**不正出金**が判明。

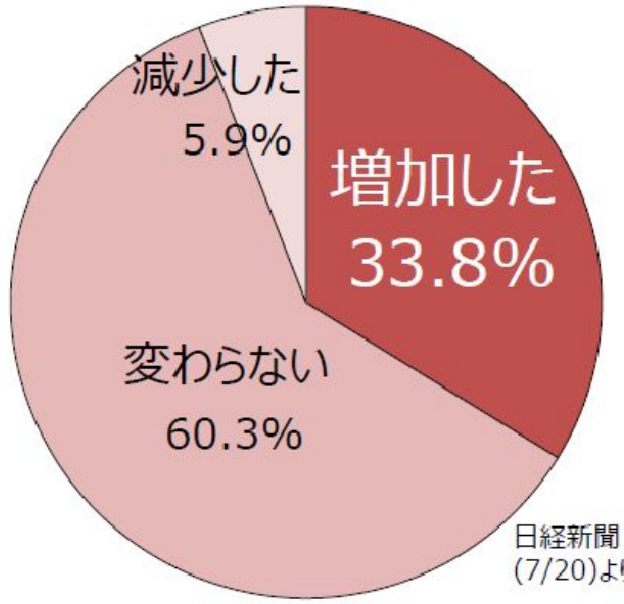
10月　原子力規制委員会が、**不正アクセス**を受け、メール等のやりとりを含む**外部とのアクセスを遮断**。

11月　カプコンが、**オーダーメイド型ランサムウェアによる標的型攻撃**を受け、**個人情報・人事情報・開発資料等が流出**した可能性が判明。

（piyolog、各社公表資料、各種報道等より総務省作成）

2020年４月以降に受けたサイバー攻撃

（前年同月比）



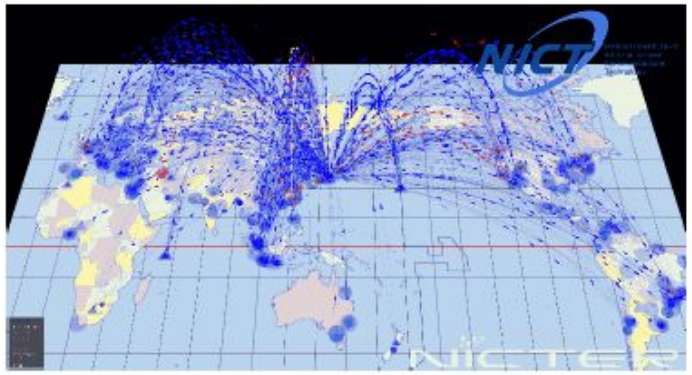
日経新聞
(7/20)より

社内システム・設備の停止や提供しているサービスの停止といった企業活動そのものに影響する攻撃が増加

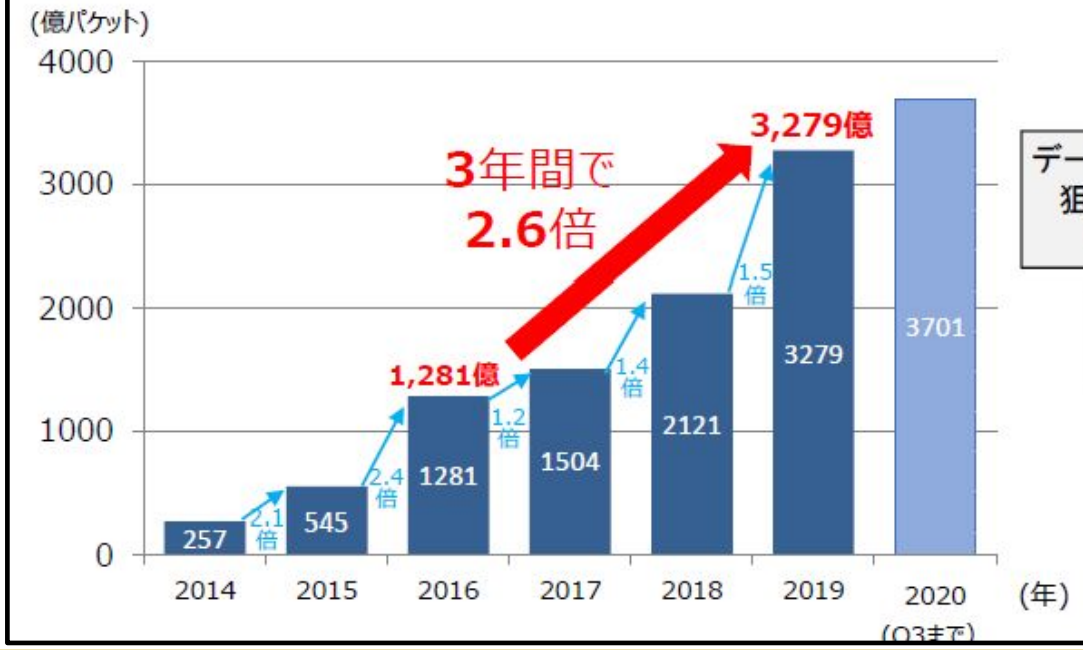
増加するサイバー攻撃

未来研究所
Future Research Inc.

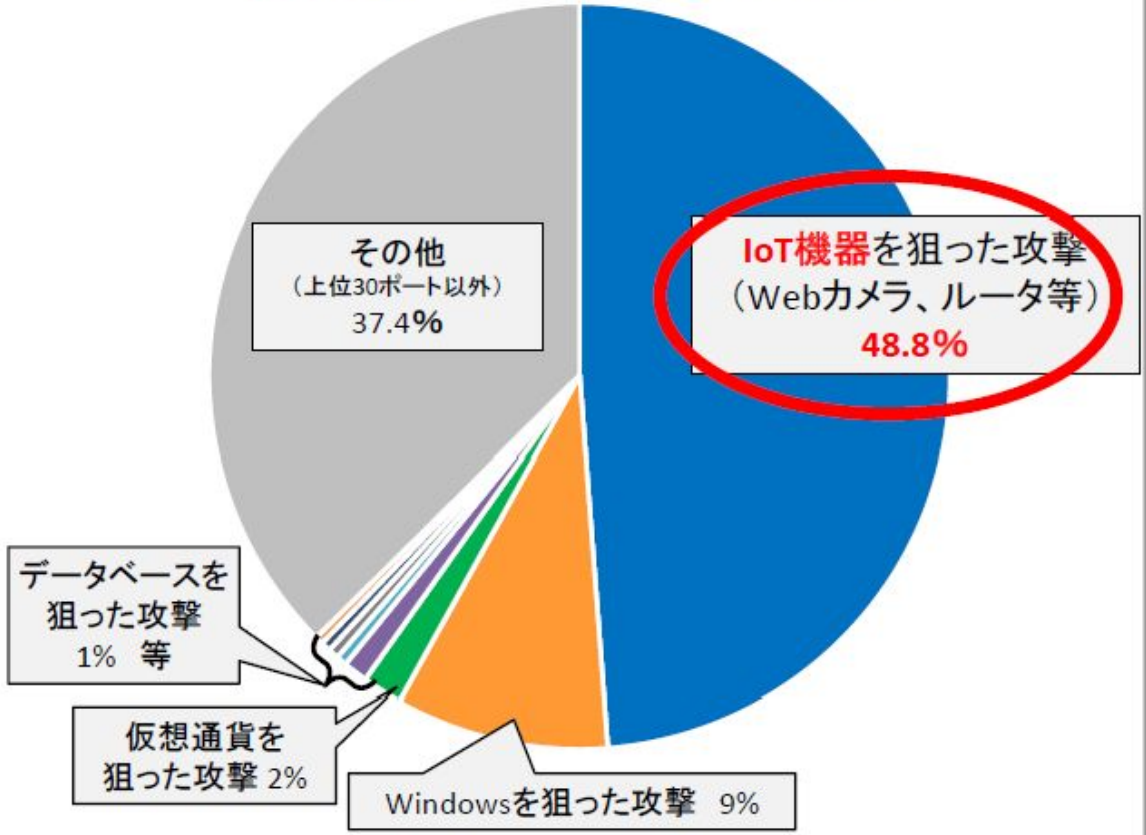
NICTERにより観測されるサイバー攻撃の様子



NICTERで１年間に観測されたサイバー攻撃回数



約半数がIoT機器を狙った攻撃



※ NICTERで2019年に観測されたパケットのうち、調査目的パケット以外についてサービス種類（ポート番号）ごとに上位30ポートまでを分析したもの。

※ IoT機器を狙った攻撃は多様化しており、ポート番号だけでは分類しにくいものなど、「その他」に含まれているものもある。

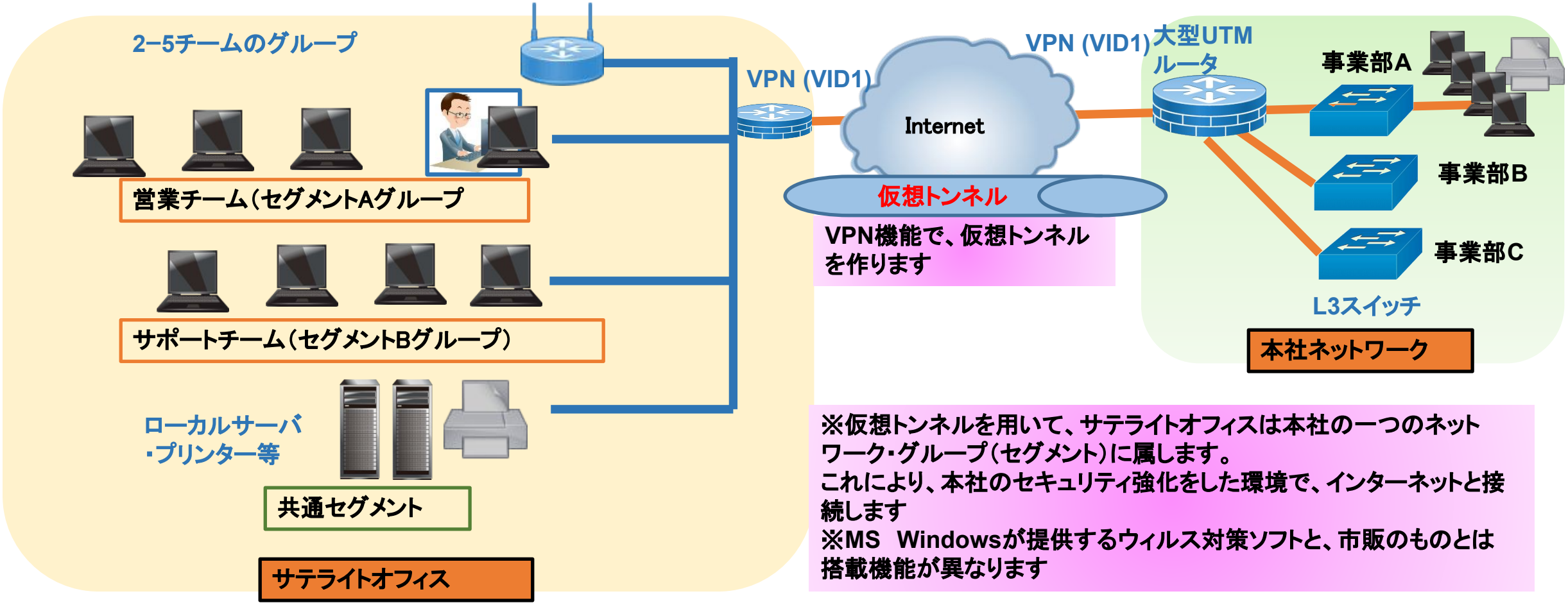
※リソース　総務省　https://www.soumu.go.jp/main_content/000722477.pdf

サテライトオフィスのセキュリティ

有るべき姿とは？

サテライトオフィスに必要なNW機器＆ルールは？

- セキュアなVPN（Virtual Private Network)機能を有したルータを設置
  - 昨今、ルータ機能を有したUTM・F/Wメーカが台頭
- 使用PC＆サーバには、市販のウィルス対策ソフト（検知・除去ソフト:EDR)をインストール
- リモートワークのためのセキュリティポリシー（使用方法のルール）



※仮想トンネルを用いて、サテライトオフィスは本社の一つのネットワーク・グループ（セグメント）に属します。
これにより、本社のセキュリティ強化をした環境で、インターネットと接続します
※MS　Windowsが提供するウィルス対策ソフトと、市販のものとは搭載機能が異なります

サテライトオフィスのセキュリティ

リモートワーク環境の整備について（コロナ禍対策）

サテライトオフィスを狙うサイバーアタックとは？

未来研究所
Future Research Inc.

◆ IPA発行：情報セキュリティ10大脅威2021

■「情報セキュリティ10大脅威 2021」

NEW：初めてランクインした脅威

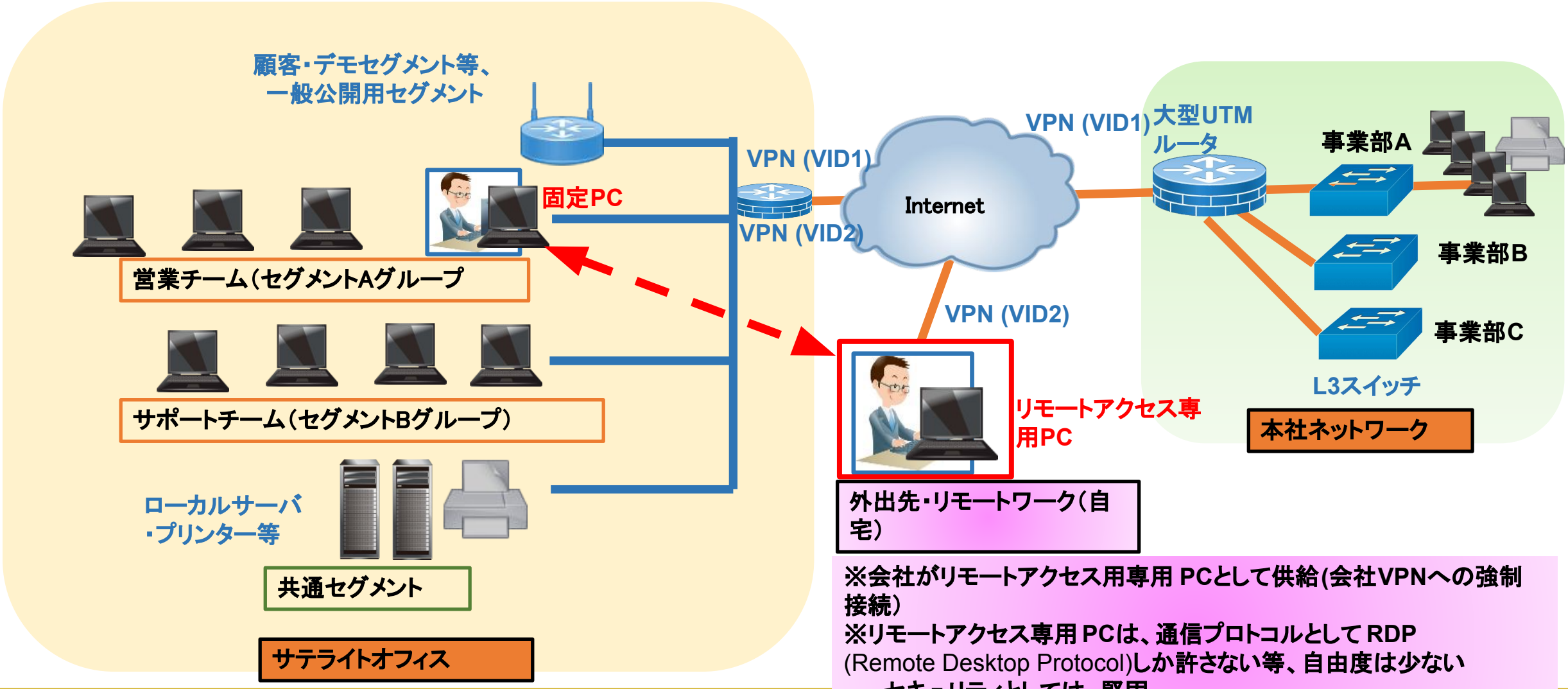
昨年順位	個人	順位	組織	昨年順位
1位	スマホ決済の不正利用	1位	ランサムウェアによる被害	5位
2位	フィッシングによる個人情報等の詐取	2位	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗・中傷・デマ	3位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃	4位
3位	クレジットカード情報の不正利用	5位	ビジネスメール詐欺による金銭被害	3位
4位	インターネットバンキングの不正利用	6位	内部不正による情報漏えい	2位
10位	インターネット上のサービスからの個人情報の窃取	7位	予期せぬIT基盤の障害に伴う業務停止	6位
9位	偽警告によるインターネット詐欺	8位	インターネット上のサービスへの不正ログイン	16位
6位	不正アプリによるスマートフォン利用者への被害	9位	不注意による情報漏えい等の被害	7位
8位	インターネット上のサービスへの不正ログイン	10位	脆弱性対策情報の公開に伴う悪用増加	14位

- 脆弱性の悪用により**VPN** のパスワード流出
  → 古いVPNソフトを使用。常に最新版への移行が必要（情報システム（IS）業務の不備）
- セキュリティポリシーに反し、個人PCを使用し社内ネットにアクセス。感染したSNS使用によりウィルスが社内に伝搬
  → セキュリティポリシー違反
  （セキュリティポリシーの周知徹底不足）
- **Zoom** に非公開会議へアクセスできる脆弱性
  特定アクセス手法に則ると、約100万種類の入力で取得できた脆弱性。既に対処済み
  → 最新ZOOMの使用

サテライトオフィス　VPN　NW構成図A

未来研究所
Future Research Inc.

- リモートワークでの固定PC＋外出・リモートワーク用端末支給PC

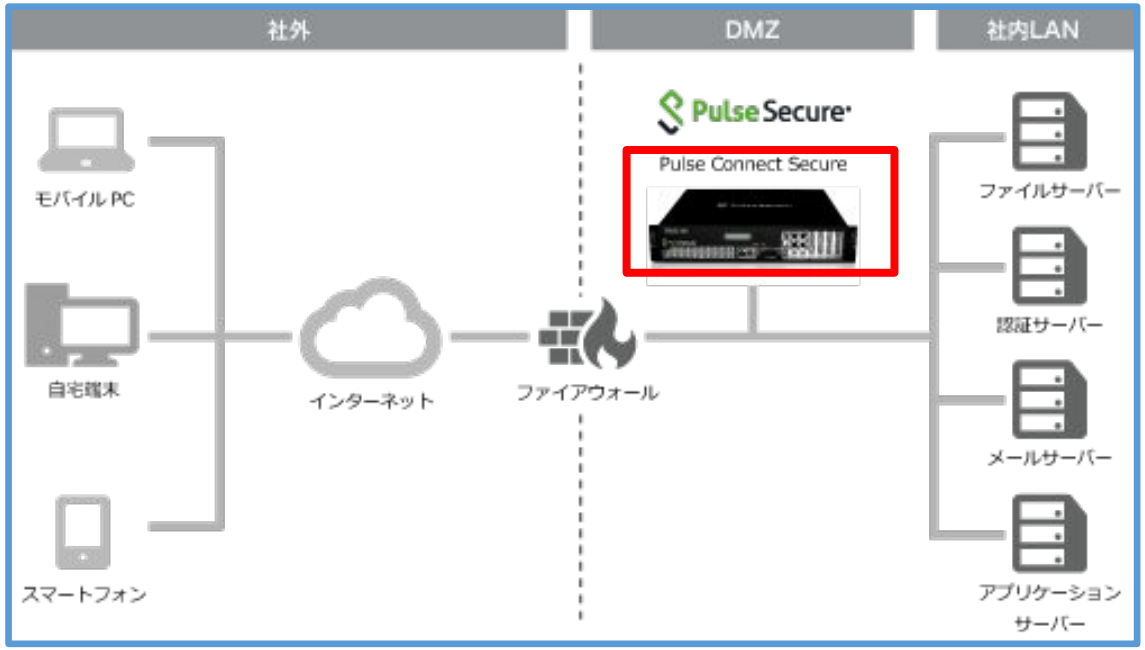


※会社がリモートアクセス用専用 PCとして供給(会社VPNへの強制接続)
※リモートアクセス専用 PCは、通信プロトコルとして RDP (Remote Desktop Protocol)しか許さない等、自由度は少ない
→　セキュリティとしては、堅固

VPN　脆弱性例

- VPNソリューション、Plus Connected Secure での脆弱性を狙った攻撃
  - 対象VPN商材
    - Pulse Secure (IvantiがM&A)社製　VPN Pulse Connect Secure
    - 3件の脆弱性「CVE-2020-11580」「CVE-2020-11581」「CVE-2020-11582」が発表される
  - 原因
    - ゼロディ攻撃、中国ハッカー集団UNC2630,2717が仕掛けたと言われている
- 対策
  - 早急なパッチレベルアップ

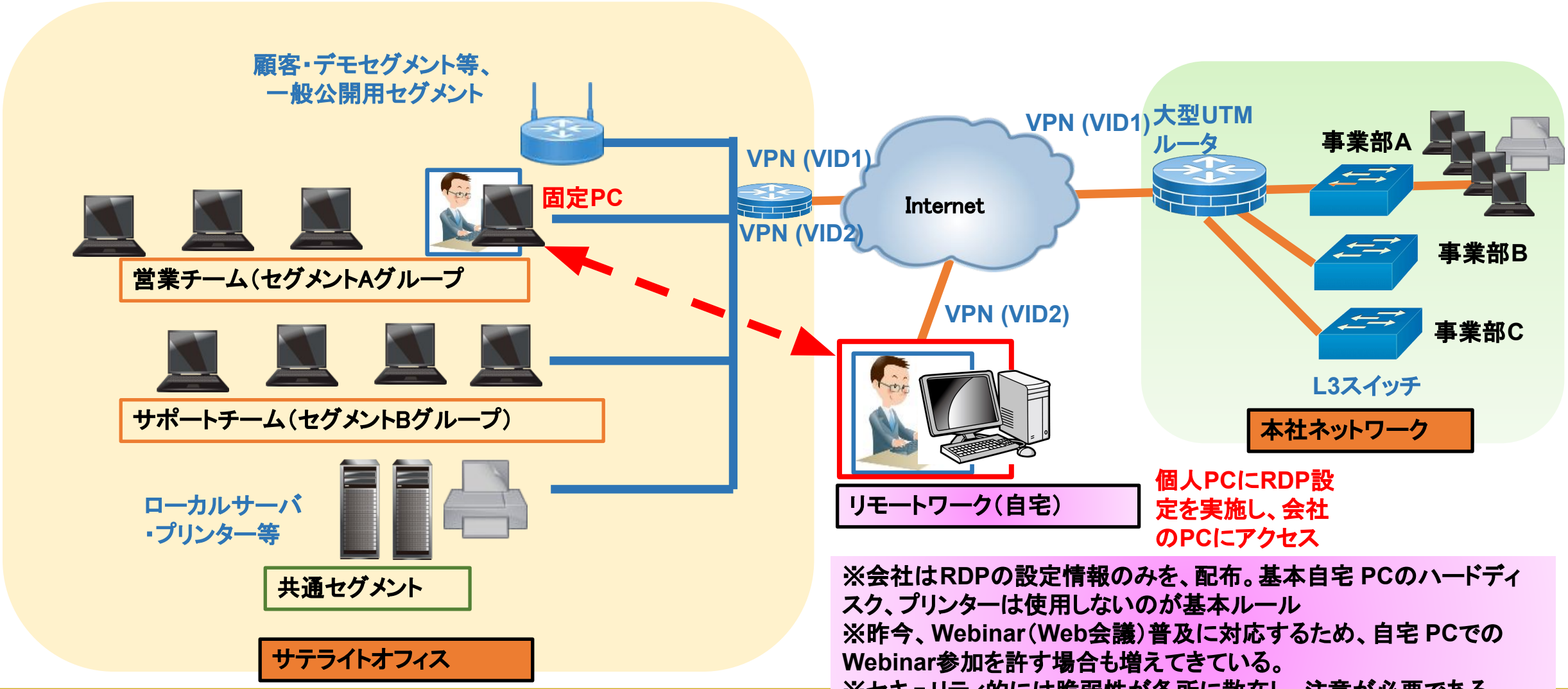
    CSIRT/情報システム部署による管理の徹底



サテライトオフィス　VPN　NW構成図B

未来研究所
Future Research Inc.

- リモートワークでの固定PC＋リモートワーク用PCは個人PCを使用

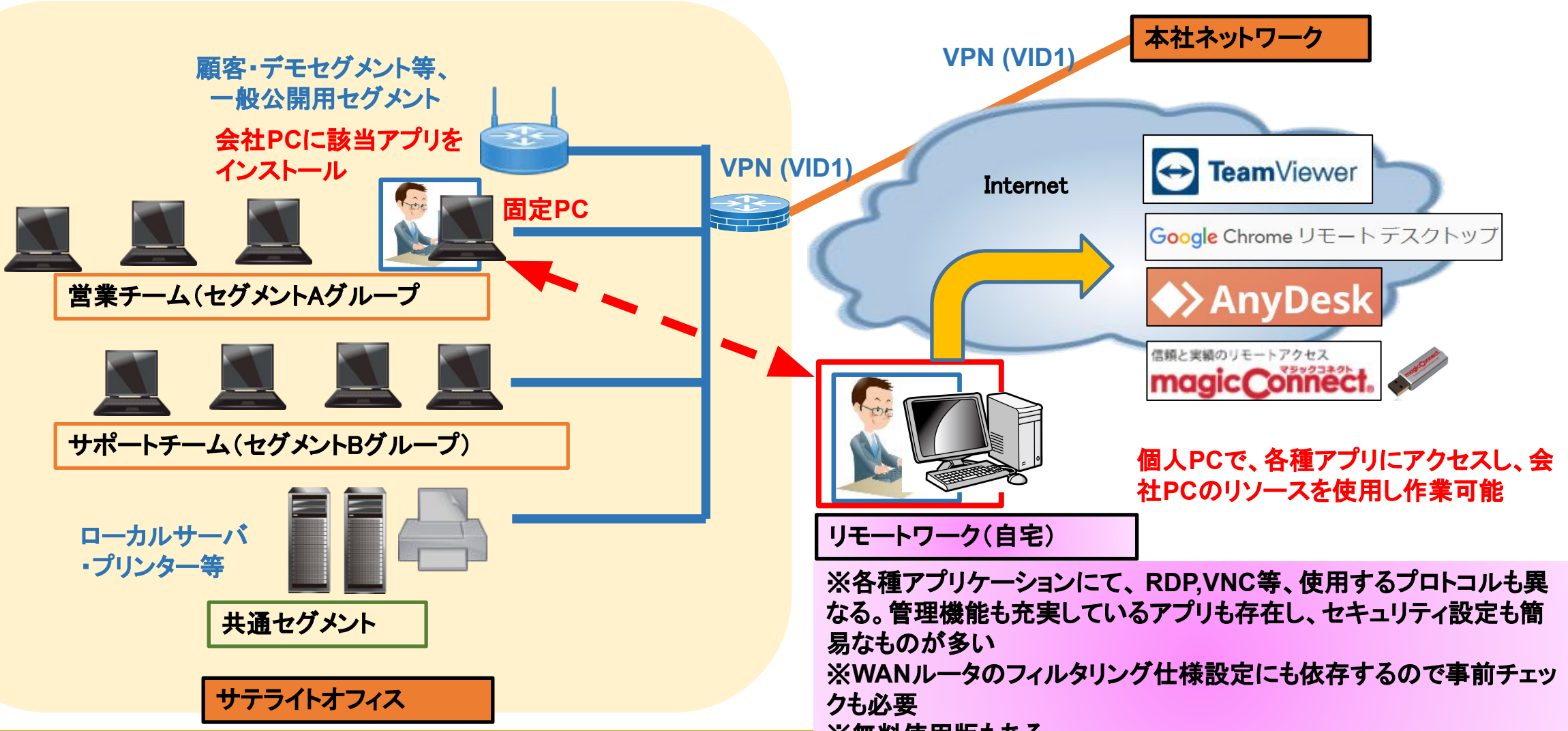


※会社はRDPの設定情報のみを、配布。基本自宅 PCのハードディスク、プリンターは使用しないのが基本ルール
※昨今、Webinar（Web会議）普及に対応するため、自宅 PCでのWebinar参加を許す場合も増えてきている。
※セキュリティ的には脆弱性が各所に散在し、注意が必要である

サテライトオフィス　VPN　NW構成図B‘

未来研究所
Future Research Inc.

- リモートワークでの固定PC＋リモートワーク用PtoPアプリ

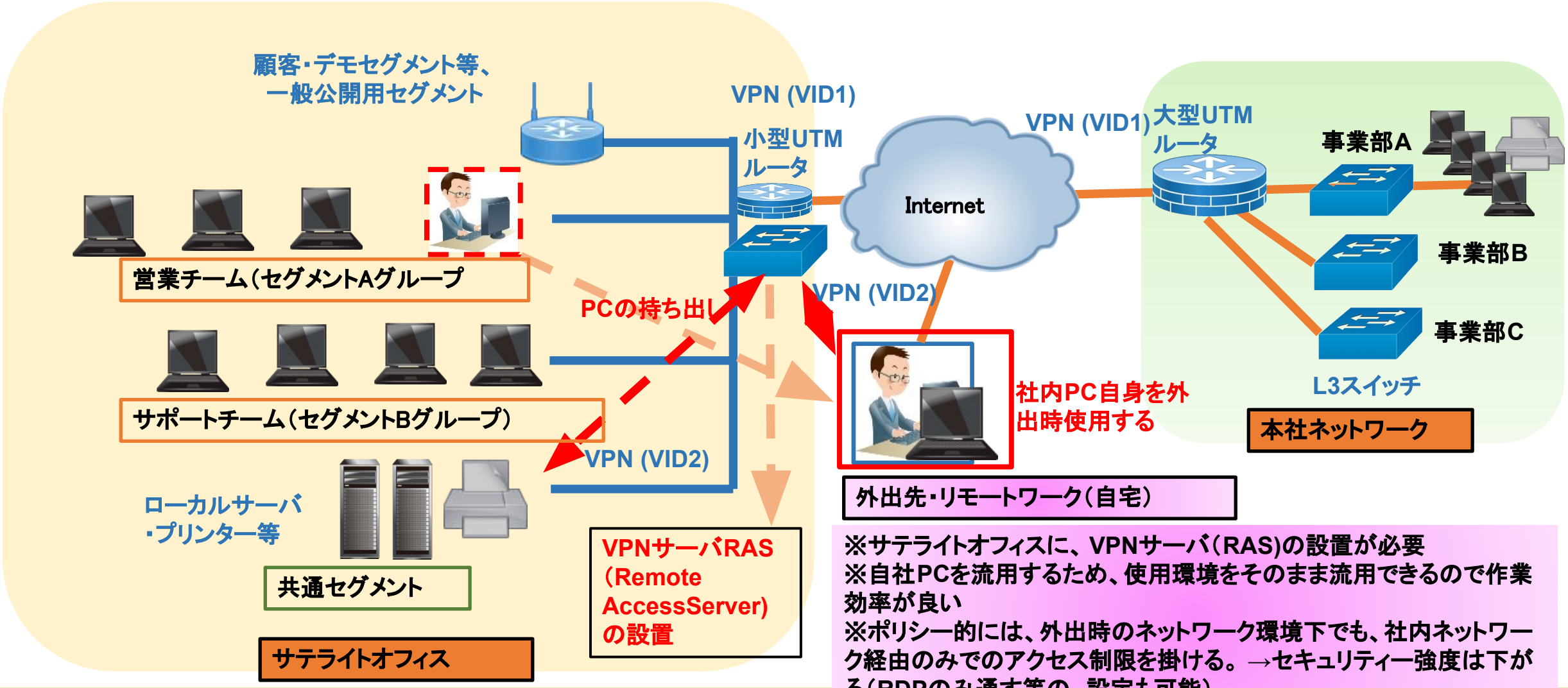


※各種アプリケーションにて、RDP,VNC等、使用するプロトコルも異なる。管理機能も充実しているアプリも存在し、セキュリティ設定も簡易なものが多い
※WANルータのフィルタリング仕様設定にも依存するので事前チェックも必要
※無料使用版もある

サテライトオフィス　VPN　NW構成図C

未来研究所
Future Research Inc.

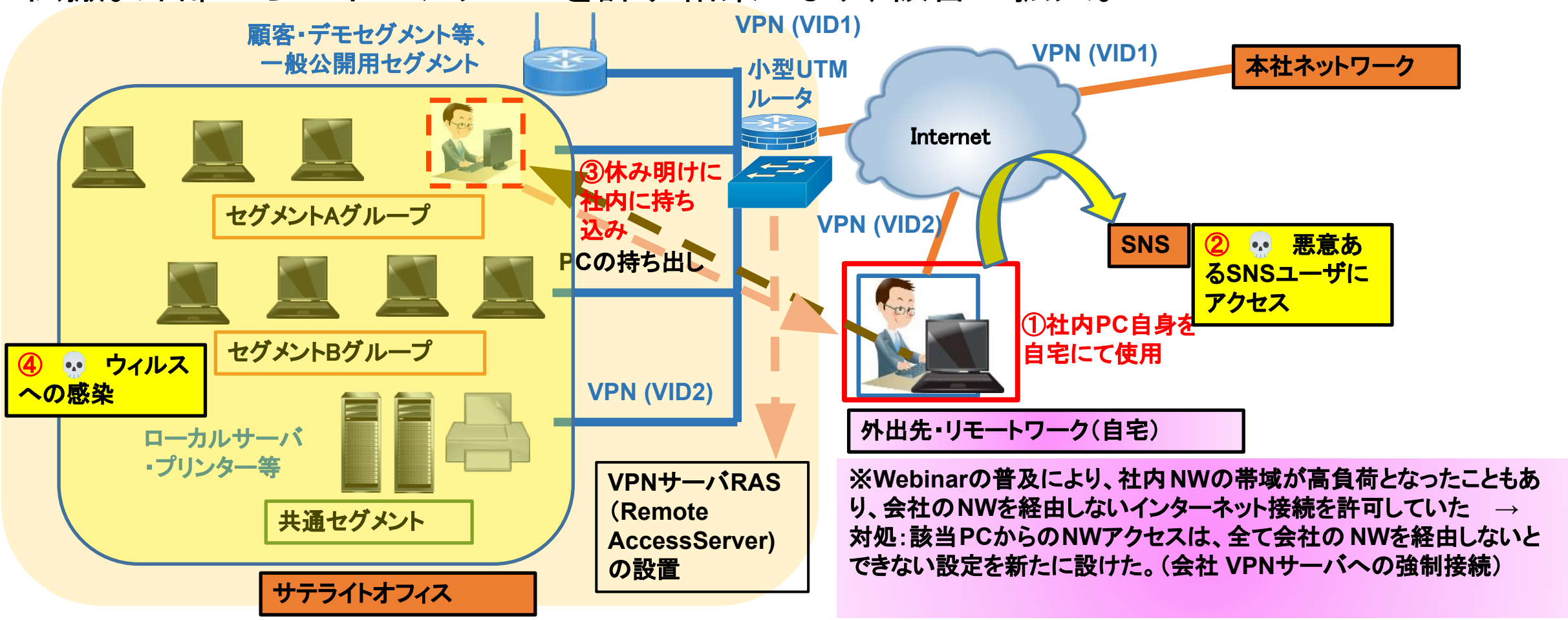
- 社内PCを必要に応じ持ち出すことで、リモートワークを実現する



※サテライトオフィスに、VPNサーバ（RAS)の設置が必要
※自社PCを流用するため、使用環境をそのまま流用できるので作業効率が良い
※ポリシー的には、外出時のネットワーク環境下でも、社内ネットワーク経由のみでのアクセス制限を掛ける。→セキュリティー強度は下がる（RDPのみ通す等の、設定も可能）

VPN　NW構成図C：三菱重工㈱NWへの不正アクセス

- 社内PCを自宅リモートワークで使用し、自宅のインターネット経由で悪意のあるアプリにSNS経由でアクセスし、感染。感染した会社PCを社内に接続したため、感染が他端末に伝搬。外部からの不正アクセスを許す結果となり、被害が拡大。



※Webinarの普及により、社内NWの帯域が高負荷となったこともあり、会社のNWを経由しないインターネット接続を許可していた　→
対処：該当PCからのNWアクセスは、全て会社のNWを経由しないとできない設定を新たに設けた。（会社 VPNサーバへの強制接続）

サテライトオフィスに必要なセキュリティとは？

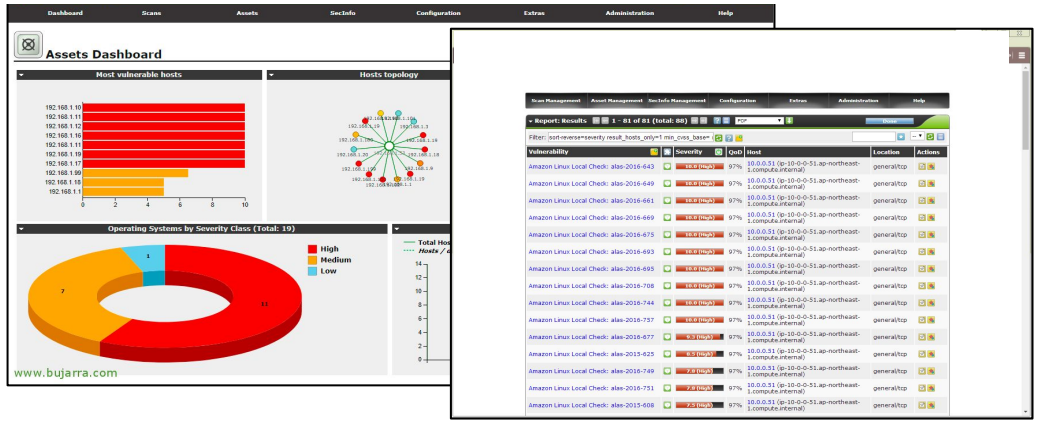
- サテライトオフィス　VPN　NW構成図A　の採用
  - セキュリティが強固　＝　使い勝手が悪い
  - ***セキュリティ強度：　構成A図　＞　構成図C　＞　構成図B***
- 社内向け・セキュリティポリシーの周知徹底
  - 全社員への周期訓練が必須
  - 社外向けセキュリティポリシーの理解
- サイバー保険付きネットワーク機材の選定
  - サイバー保険の検討
    - インシデント発生時の切り分け費用がカバーされるケースが多い
- インシデント発生時の対処方法の習得/訓練
  - 例：日本IT団体連盟「サイバーセキュリティ演習マップ解説書」と「サイバーセキュリティ演習マッピングリスト」
    - https://www.itrenmei.jp/topics/2021/3685/

最後に、各種情報

- セキュリティポリシー（サテライトオフィス規模対応）
  - 情報セキュリティ関連規定
    - 中小企業の情報セキュリティ対策ガイドライン
      - https://www.ipa.go.jp/files/000055794.docx
- サイバーセキュリティ対策を実施する上での実業務は？
  - ISMS(ISO/IEC27001、クラウドサービス版：ISO/IEC27017）の取得 → CSIRTの設置・運用 → PSIRTの設置・運用（IoT向け）
- サイバーセキュリティ対策要員の人材育成
  - 難しいのは、フォレンジック
    （IoC: Indicator Of Compromise)のみ。
    他は、ISO規定アクション業務と略同じ。
    - インシデントの種類によりアクションが異なる。
      明示ガイドラインは、開示されてない。
      → このアクションを訓練することが肝要

御紹介商材・ソリューション

- 各種インシデント発生時における、社内・社外の組織対応訓練ツール
  - アライドテレシス㈱社製、DECIDEPlatformでのIT-BCP訓練→サイバー防災訓練
- 未来研究所：各種コンサルテーション御紹介
  - リモートワーク構築サービス
    - ZOOMでのヒアリング→改善提案→NW再構築
  - 研修・演習
    - サイバーセキュリティ人材育成マップ制作
    - 「サイバーインシデント発生、その時どうする？」
    - 「ISMS情報セキュリティ基礎」
    - 「情報セキュリティ部隊（CSIRT）を新設」
  - 脆弱性チェックサービス
    - 先着3社様　5端末・無料脆弱性チェック



sales@future-research.jp迄、ご連絡ください

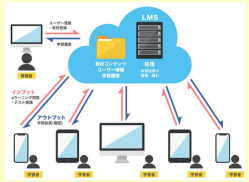
Network@theEdge　ビジネスモデルの全容

未来研究所
Future Research Inc.

- ITサービスを提供する人材を全国で育成・認定し、ITで困っている方々にサービスを提供します

未来研究所
Future Research Inc.

【サービス学習管理システム】
・LMSでの学習者管理
・テストエンジンでの
資格認定制度



学習

【各種サービス・ナビシステム】
・実際のサービス指定コンテンツ
・各種サービスAPIの提供

地域Co-Worker/提携会社・販社
（各地域に存在する・お助け隊）

・地場のITサービス企業
・大手団体（ITコーディネータ協会、CSAJ、IT連盟協会）
・大学の学生（コンピュータクラブ、映画研究会等々）

ITサポート業務
（基本リモート・必要時訪問）

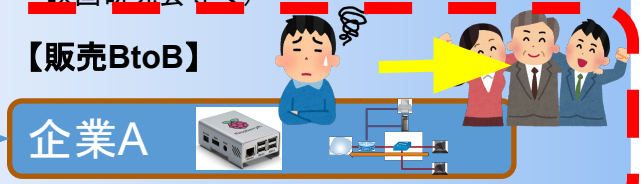
・大学の学生（コンピュータクラブ、映画研究会等々）

ITサポート業務
（基本訪問
・必要時リモート）

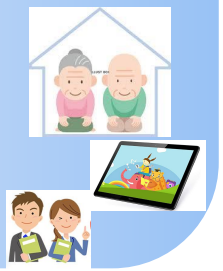
エンドユーザ
（NoneIT・SME企業、コンシューマー）

【販売・サポート協力】
・XX商工会議所
・大手BtoC企業（IOデータ情報機器、IT連盟協会）
・大学の学生（コンピュータクラブ、映画研究会等々）

【販売BtoB】



【販売BtoC】
・葬儀のライブ配信サービス
・結婚式のライブ配信サービス
・ホテルのイベント配信
・老人向け携帯設定サービス



sales@future-research.jp
迄、ご連絡ください

Thank you

