

日本のサイバーセキュリティを「連携」「学び」「創造」



JNSA全国サイバーセキュリティセミナー2021

新しい働き方の サイバーセキュリティ対策

2021年11月17日

特定非営利活動法人日本ネットワークセキュリティ協会
マーケティング部会 副部会長
持田啓司（株式会社ラック）



本日の講演内容は、持田の個人的見解であり、JNSAおよびラックグループの意見を代弁するものではありません。

本日は広島県より参加しています



自己紹介

- 所属・名前

- 株式会社ラック シニアコンサルタント 持田 啓司 (もちだ ひろし)

- 経歴

- 旧郵政省 ⇒ 米国系IT教育ベンダー ⇒ 国内SIer ⇒ 株式会社ラック

郵政省当時(20年以上前)のテレワーク・オンライン活用

- 在宅等でいかに仕事ができるか
 - オンラインでつながっていない環境も想定
- オンライン会議は可能だが、画像や音声はとぎれとぎれ
 - 大きな拠点間のみ
 - 現地に出張が増える
- メール等で送った文書はすべて印刷して回覧
 - 紙の消費が増える
 - 利用リテラシーの差で、周知徹底の差が発生

ニューヨークの街の変化



1900年



1913年

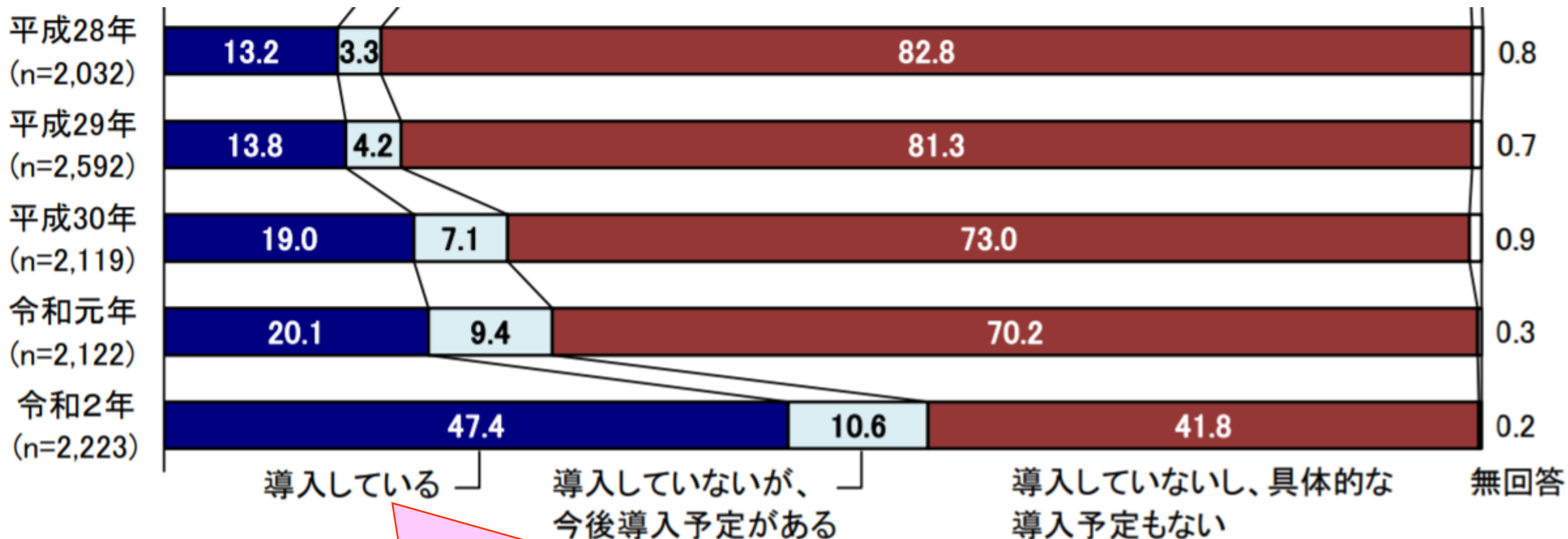
あらためて本日のテーマは！

• デジタル社会推進で更に加速を求められる
DXとサイバーセキュリティ対策

- DX(デジタルトランスフォーメーション)
 - ITの浸透が、人々の生活をあらゆる面でより良い方向に**変化**させる
 - スウェーデン ウメオ大学 エリック・ストルターマン教授が提唱
- 災害は繰り返す
 - 災害が来ることを想定した社会環境に**変化を!**

1. この2年での環境変化

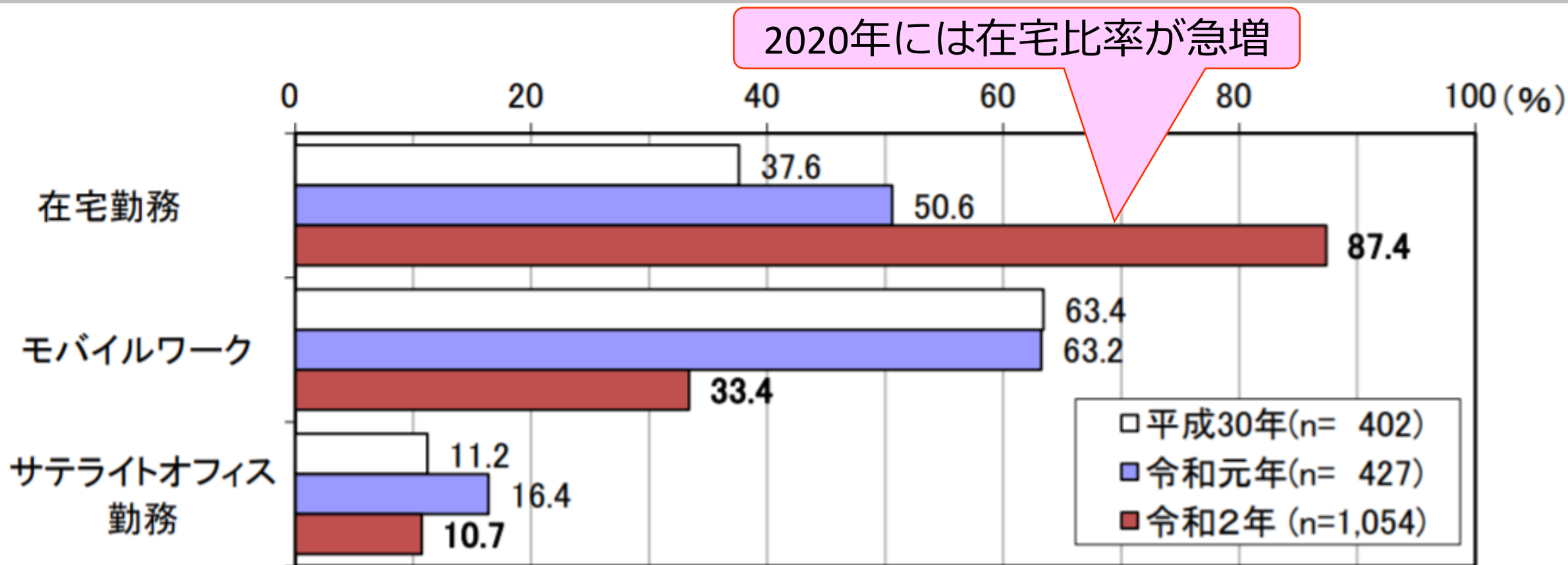
テレワークの導入状況の推移



コロナ禍を機にテレワークが定着

出典：総務省 令和2年 通信利用動向調査報告書（企業編）

テレワークの導入形態の推移



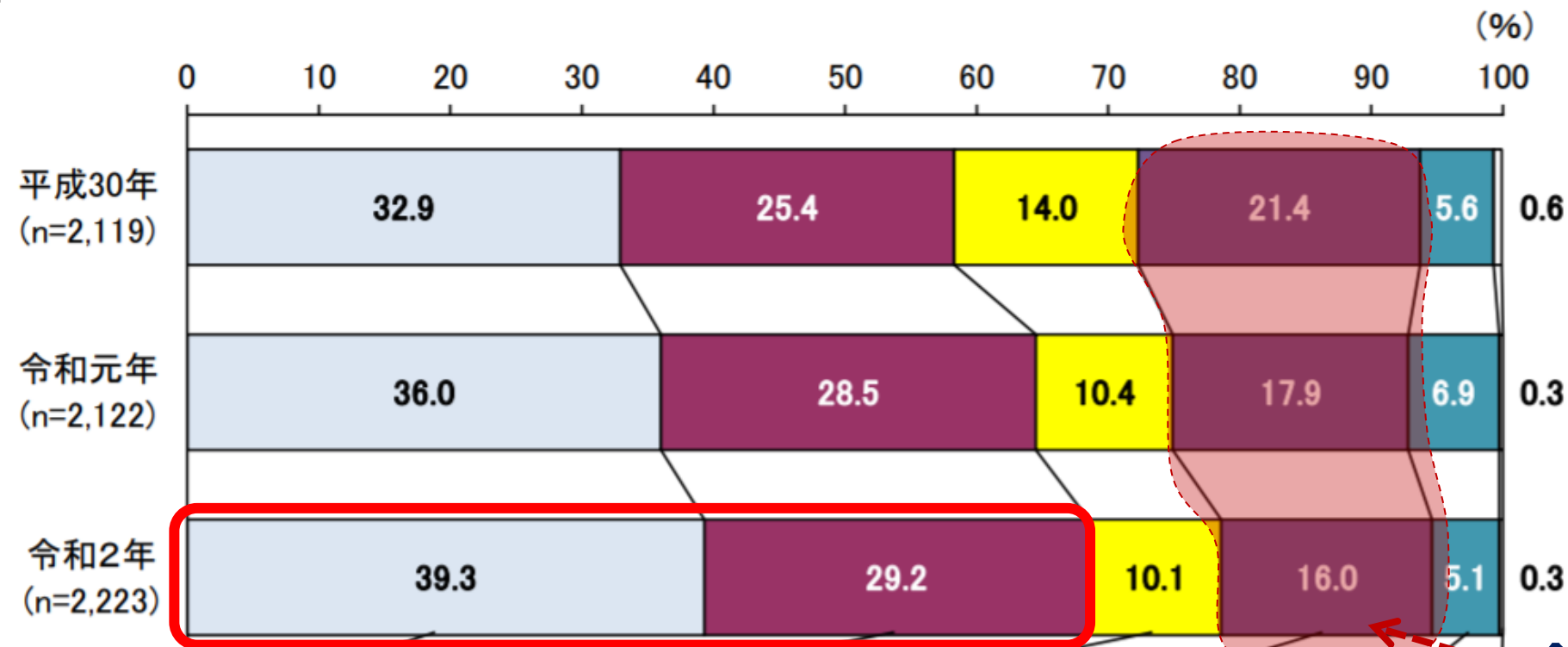
※「無回答」を除いて集計

(複数回答)

※ n値は比重調整後の導入企業数

出典：総務省 令和2年 通信利用動向調査報告書 (企業編)

クラウドサービスの利用状況の推移



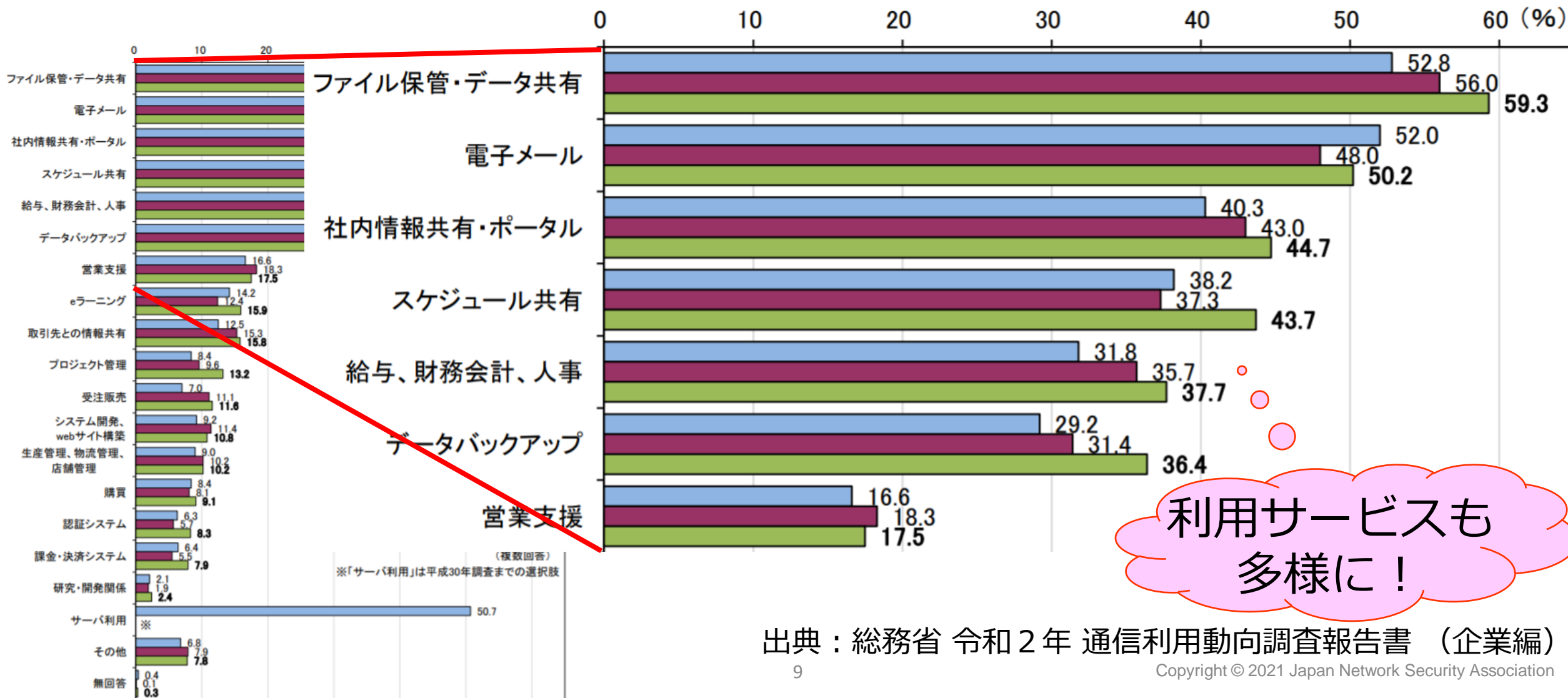
**企業の意思
は刻々と変化する**

- 全社的に利用している
- 一部の事業所または部門で利用している
- 利用していないが、今後利用する予定がある
- 利用していないし、今後利用する予定もない
- クラウドについてよく分からない
- 無回答

2020年には68.5%の企業がクラウドサービスを業務に利用

出典：総務省 令和2年 通信利用動向調査報告書（企業編）

具体的に利用しているクラウドサービスの推移



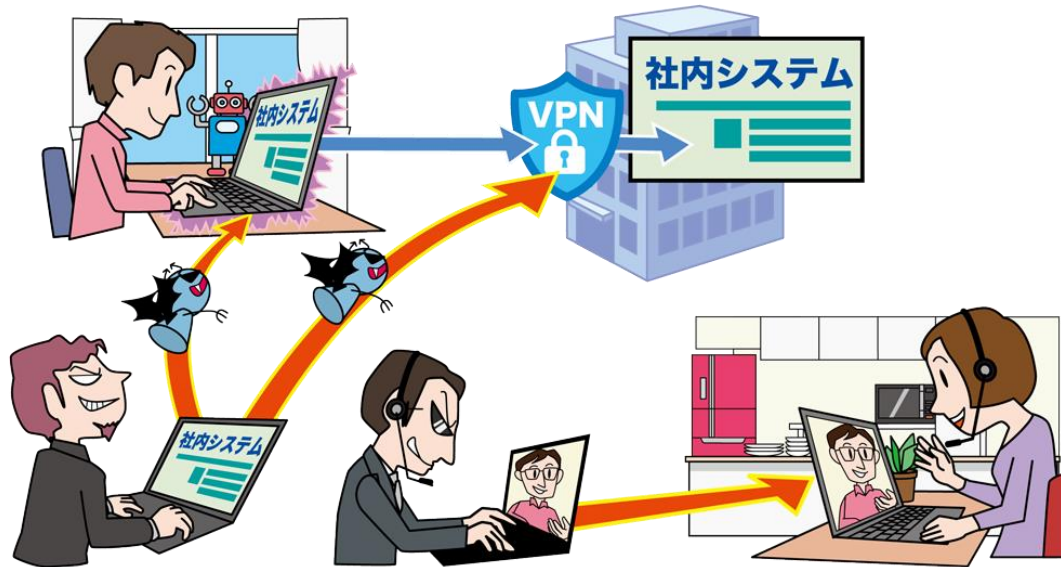
利用サービスも
多様に！

出典：総務省 令和2年 通信利用動向調査報告書（企業編）

2. 新しい働き方のサイバーセキュリティリスク

IPA 情報セキュリティ10大脅威 2021

- 組織編の3位に「テレワーク等のニューノーマルな働き方を狙った攻撃」が初めてランクイン
- ウェブ会議サービスやVPNの本格的な活用の始まりに伴い、それらを狙った攻撃が発生し、ウェブ会議ののぞき見やテレワーク用PCのウイルス感染のおそれ



出典：IPA 情報セキュリティ10大脅威 2021

- テレワーク用ソフトウェアの脆弱性の悪用
 - VPN 等のテレワーク用に導入している製品の脆弱性を悪用し、社内システムに不正アクセスしたり、PC 内の業務情報等を窃取したりする。
 - また、ウェブ会議サービスの脆弱性を悪用し、ウェブ会議をのぞき見する。
- 急なテレワーク移行による管理体制の不備
 - テレワークで利用している PC 内の OS やソフトウェアのセキュリティ管理を組織側から行うのは難しい。その中で、テレワークへの急な移行によりルール整備やセキュリティ対策のノウハウが不十分なまま利用を開始している。
- 私物 PC や自宅ネットワークの利用
 - 私物 PC をテレワークで利用している場合、ウェブサイトや SNS にアクセスしたり、私物のソフトウェアをインストールしたり等の私的利用をすることがある。その際、PC がウイルスに感染したり、攻撃者にソフトウェアの脆弱性を悪用され、テレワーク用の認証情報等を窃取されたりするおそれがある。

出典：IPA 情報セキュリティ10大脅威 2021

ありがちな事例：機密資料の参照

これまでの運用



機密文書の参照は、管理者から鍵を借りて施錠されている
キャビネから文書を取り出し、参照が済んだら保管して施錠



テレワークに伴う緊急措置

機密文書の参照が必要な場合は、
コピーして持ち帰ることを許可



その結果

 自宅で他の書類に紛れて誤って
廃棄され、機密情報が漏えい 

テレワークに伴う見直し

機密文書を電子化しアクセス制限を
かけて保存。参照時は管理者が一時的
的に利用者に参照権限を付与

その結果

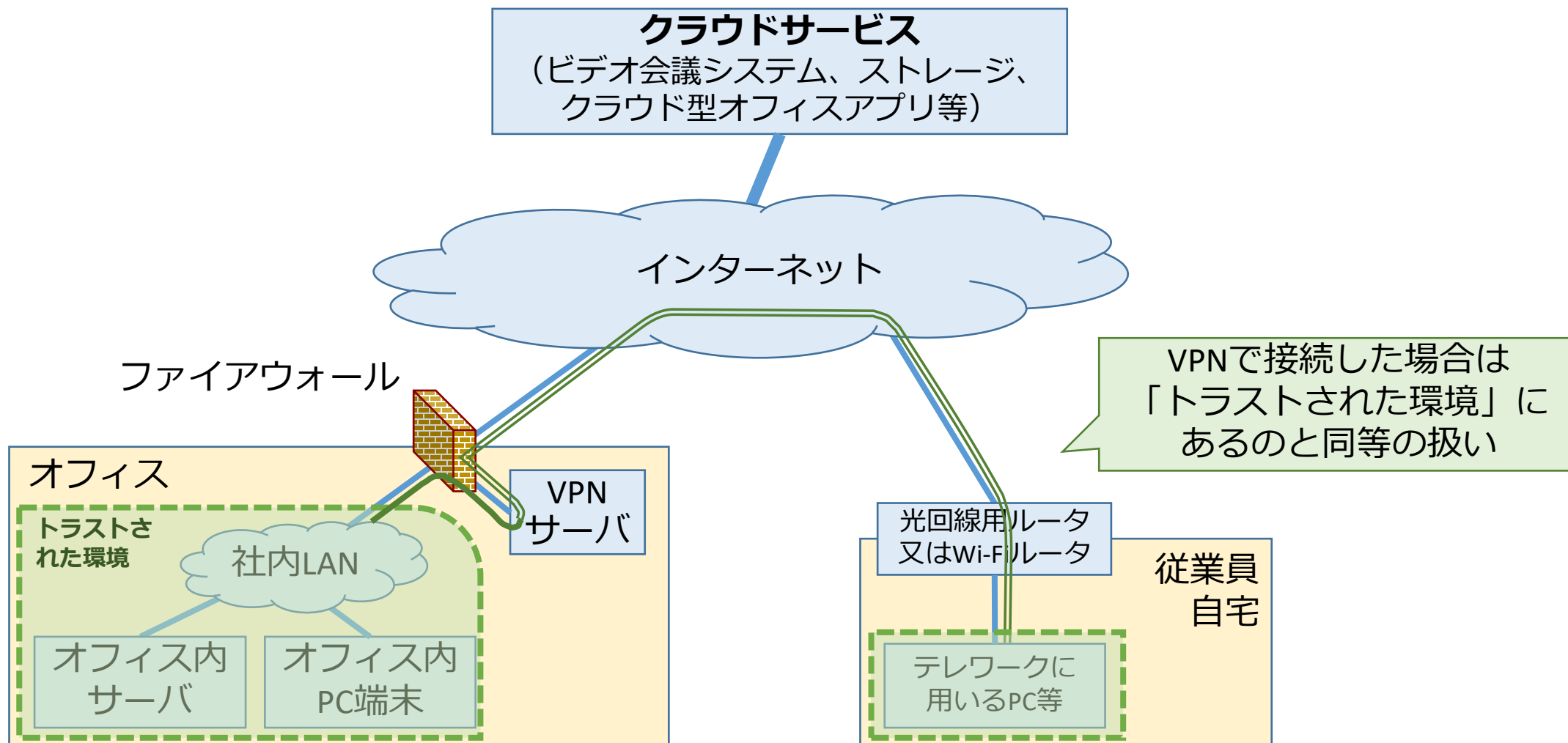
 業務上のニーズとセキュリティを
両立できた 

・・・とはいえ短期間での「文書の電子化」は無理で、結果テレワーク断念企業も多数？
⇒ 今からでも業務のやり方の見直しを行うことが重要

「新しい働き方」で何が変わったのか

- サイバーセキュリティの観点で見ると：
 - ① オフィスを安全に保つだけでは守れない
 - 「境界防御モデル」の限界
 - ② 業務で利用するIT環境への依存度が高まる
 - ITインフラの性能が業務効率に直結
 - ③ 業務環境の管理主体が多様化
 - 在宅環境のセキュリティ責任者は、在宅でテレワークを行う従業員である

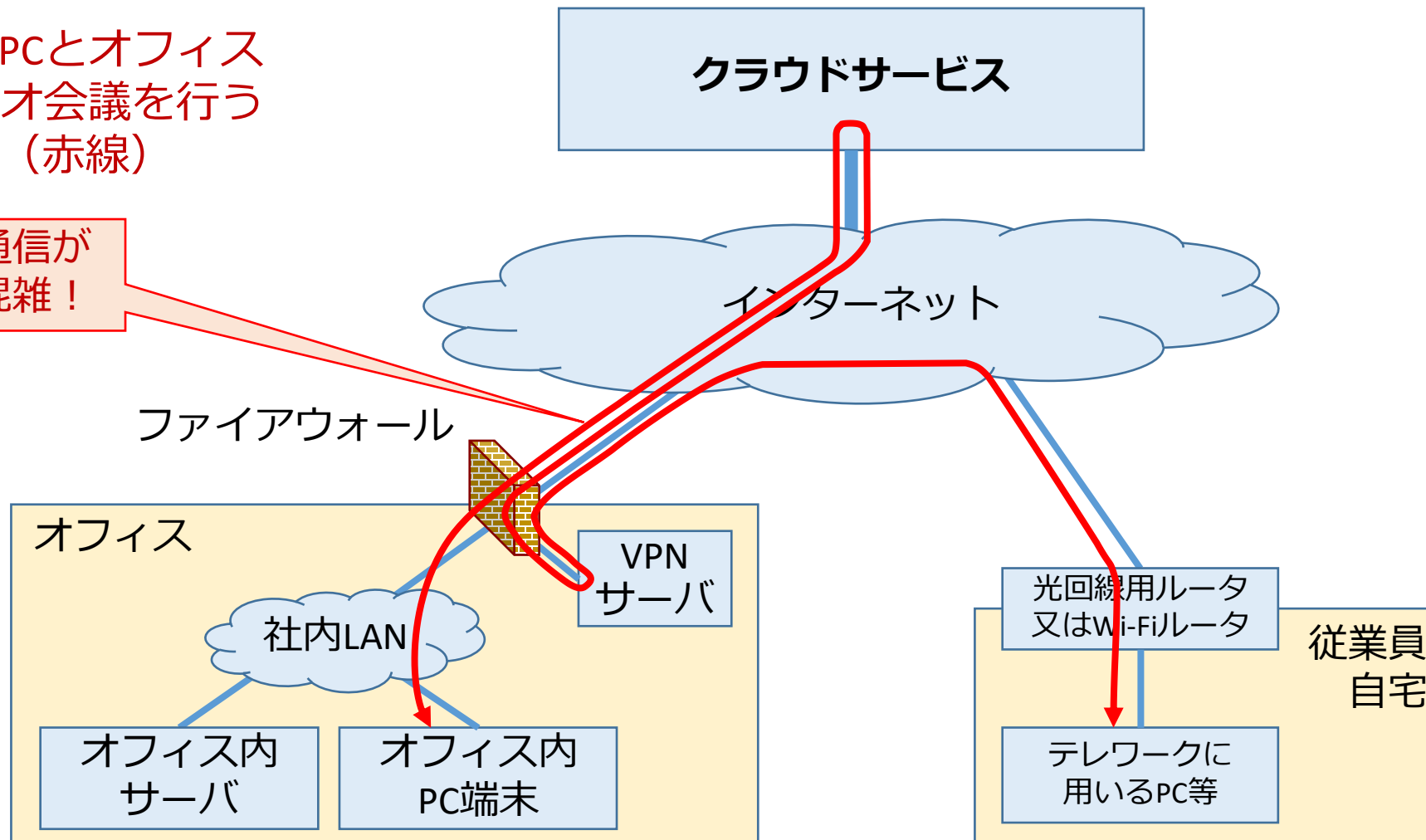
境界防御モデルに基づく典型的なIT環境



テレワークでどうなったか

テレワーク中のPCとオフィス
内のPC間でビデオ会議を行う
時の通信の流れ（赤線）

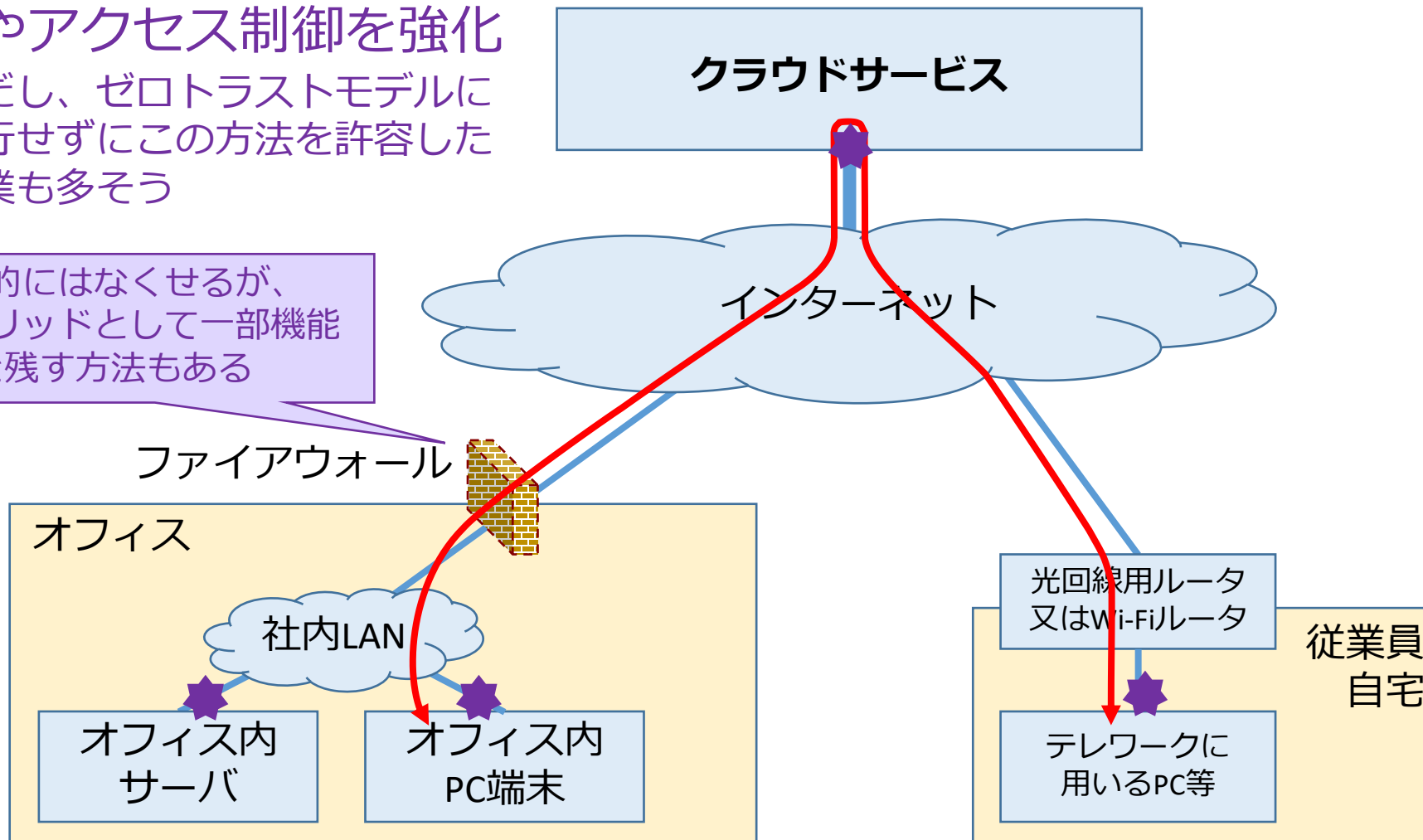
この区間を同じ通信が
3回経由する = 混雑！



ゼロトラストだとうなるか

- ★ = 認証やアクセス制御を強化
ただし、ゼロトラストモデルに移行せずにこの方法を許容した企業も多そう

原理的にはなくせるが、ハイブリッドとして一部機能を残す方法もある



3. 緊急事態宣言解除後のセキュリティ チェックリストで安心・安全に事業継続

https://www.jnsa.org/telework_support/telework_security/index.html

緊急事態宣言解除！ 2021年9月30日



- 2020年6月12日
「緊急事態宣言解除後のセキュリティチェックリスト」公開
- 2020年6月には落ち着くと思われたが！
 - しかし、収束どころか拡大の一途
 - 1年以上経過して緊急事態宣言解除、あらためてチェックリストを確認してみた

【チェックリスト構成】

1. 停止したシステムの再稼働における注意事項
2. テレワークで社外に持ち出した機器を社内ネットワークに接続する際の注意事項
3. 緊急措置としてテレワークを許可した業務やルールを変更した業務の扱い
4. Withコロナフェーズに向けた、業務見直しとセキュリティ対策

※解説書ではこのほか以下の2点を記載

- 一般従業員がチェックすべき事項
- 企業へのアドバイス

1. 停止したシステムの再稼働における注意事項



- 長期間停止していたシステムの動作確認
- 長期間停止していたシステム構成機器のセキュリティ対策の最新化（OS・ソフトウェア、アンチウイルスソフト定義ファイル等）

● 注意事項のポイント

- 従業員による利用開始に先立ち、システム管理部門等での安全確認を実施
- 稼働停止期間中にソフトウェアの脆弱性を悪用した攻撃が発生している場合は、**監視強化等の暫定回避策の併用**についても検討

2. テレワークで社外に持ち出した機器を社内ネットワークに接続する際の注意事項(抜粋)

- 持ち出した機器(端末や外部記憶媒体等)の現物棚卸しや、セキュリティ対策の最新化(OS・ソフトウェア等)、マルウェアへの感染確認
- 無許可ソフトウェアのインストール確認
- テレワーク期間中の社内システムへの不正アクセスログ等の確認や、社内ネットワークに接続した端末からの不審な通信の監視を強化

● 注意事項のポイント

- 近年のセキュリティインシデントは従業員の端末を通じた侵入事例が多く、すべての端末の利用状況と、利用される端末における対策状況の確認は重要
- セキュリティ対策が適正かどうかを従業員に確認してもらう場合は、**確認方法を示す**必要あり
- すべてのログを確認することが困難な場合、ランダムに抽出した**一部のログについて確認**することも有効

3. 緊急措置としてテレワークを許可した業務やルールを変更した業務の扱い(抜粋)

- 緊急措置で許可した私物端末の利用実態について確認
- 緊急措置でテレワークを許可等をした業務のリスクを再評価
 - リスクが許容できる業務で、引続きテレワークを継続する場合は、必要に応じてセキュリティポリシー等の改訂を行う
 - リスクが高い業務は、一旦元の運用に戻し、テレワークができる手段を検討したうえで、テレワークの可否を判断
- **注意事項のポイント**
 - 緊急措置として実施された内容（私物利用、オンライン会議アプリのインストール等）の実態をまず把握
 - 変更または新規策定したルールやポリシーの適用によるリスクの洗い出しと再評価を実施し、リスクが高いとの結果になった場合は、一時的にもとの運用に戻しつつ、テレワークができる手段を検討
 - ニューノーマル環境では、テレワークとオフィス勤務の混在するハイブリッド勤務におけるセキュリティの担保を目指すことが求められる

4. Withコロナフェーズに向けた、業務見直しとセキュリティ対策(抜粋)

- 緊急事態宣言の再要請に備え、業務移行手順、必要なサービスの整理
- テレワークにより負荷が集中した従業員や業務・サービス、業務効率が低下・テレワーク不可業務の、洗い出しと今後の対応検討
- テレワークを前提とした検討・見直し
 - 脱押印、顧客や外部委託先と契約条件見直し、社内IT投資やセキュリティ対策等、クラウドサービスやゼロトラストネットワークの導入、リスク再評価、セキュリティポリシー見直し、社員等への周知やセキュリティリテラシーの向上
- **注意事項のポイント**
 - 「どのように元の業務のやり方へ戻すか」ではなく、**新しい業務のやり方を考える**ことが大切
 - 見直しの検討にあたっては、自社のみで行うのではなく、様々なステークホルダーとの協議が必要
 - ペーパーレス、脱押印、テレワーク等を前提としたIT投資やシステム構成について再検討
 - 多くの企業でセキュリティポリシーやインシデント対応がテレワークを想定しておらず、見直しだけでなくその教育・訓練実施が必要

一般従業員がチェックすべき事項(抜粋)

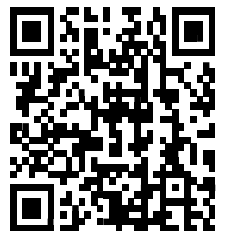


- 会社のネットワークにつなぐ前に、セキュリティ対策を最新にする
- 全て正直に報告する
 - 持ち出した機器を紛失・破損、無断でソフトをインストール、怪しい動きなどの心配なこと、私物パソコンで業務、会社のセキュリティルールの課題
- 在宅に必要な機器を整理し、ハイブリット勤務に備える
- 在宅でもできる仕事、リスクがある仕事をリストアップして業務を見直す

●注意事項のポイント

- 従業員は正直に、ありのままの状況を会社や上司と共有すべき（隠すのは自分の過失を増大させる）
- 自宅ではPCの怪しい挙動に気付いても気軽な相談相手が近くにいないが、躊躇せず上司や情報システム部門に報告
- 在宅で行うのはリスクがある仕事について、会社や上司と情報共有
- セキュリティルールの矛盾や不都合に気付いたら、生産性向上のための改善提案に活かす

- 機密情報を扱うかどうかなど「テレワークでどこまでできるようにするか」で必要な投資額は大きく変わる
- テレワークには多くの方法があり、「必ずこうしなければならない」という決まりはない
- 自社でやるべき対策とプロにアウトソースできる対策を明確にし、限られたリソースを効率的に活用すべき
- 経済産業省とIPAが、一定の品質を満たすサービスを「情報セキュリティサービス基準適合サービスリスト」として公開している
https://www.ipa.go.jp/security/it-service/service_list.html



3. 企業における対策の考え方

「新しい働き方」をセキュリティが阻害？

サイバーセキュリティインシデントが起きないことを追及すればよいのか？

(例：コミュニケーションツールの利用)

変化を否定

悪用の恐れのあるクラウド
サービスの利用はすべて禁止

コミュニケーションツールを
使いたい顧客が離反

セキュリティは確保されて
いるが業績は低下

変化を容認

従業員へのサイバーセキュリ
ティ教育をした上で容認

コミュニケーションツールを
使いたい顧客との契約維持

他社の契約まで確保できて
増収増益



・・・「事故を生じさせない」という目標は達成できたかもしれないが、業績悪化の責任は？

欧米等と日本の企業カルチャーの違い

欧米

テレワークの生産性を高めるためにこんなサービスを使わせたい

リスクの許容範囲でサービスを使うためのルールを整備

ルールに従ってサービスを活用

日本

テレワークの生産性を高めよ、ただしリスクは上げるな

リスクを高めるサービスは禁止、テレワークの生産性は従業員監視でカバー

生産性を改善するためにこんなサービスを使いたい

経営層

管理者層

一般従業員

トピダウン

ボトムアップ

「新しい働き方」に対応・推進する観点から セキュリティ管理者が認識すべきこと



① ルール見直しは必須と覚悟する

- 「境界防御モデル」が前提としていたものが崩れた以上、過去のルールを維持するほうが危険
- ルールの形骸化こそが事故を招く

② ルールはリスクと便益のバランスを体現するもの

- 禁止で防げるリスクと失われる便益を比較
- シャドーITとして把握不可能になるリスクも
- ログがとれるなら、抑止効果として使える場合も多い

③ 見直しの障害突破には外部の力を活用

- リスクアセスメントは専門家の知見活用で説得力が増す
- 公的機関やJNSAの公表物・他社事例等も活用

- 総務省「テレワークセキュリティガイドライン（第5版）」
- https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/
 - テレワークにおいて検討すべきこと
 - 「ルール」「人」「技術」のバランスがとれた対策
 - 7種類のテレワーク方式について、詳細解説と考慮事項
 - 対策一覧と解説
 - トラブル事例と対策
- IPA「ニューノーマルにおけるテレワークとITサプライチェーンのセキュリティ実態調査」
- <https://www.ipa.go.jp/security/fy2020/reports/scrm/index-final.html>
 - コロナ禍でやむを得ず認めたセキュリティ対策の例外や特例が現状も継続している組織がある
 - 規定・規則・手順などが取り決められていても、委託元の半数以上が、従業員が規定・規則・手順を守れているかどうかの確認を実施していない
 - ニューノーマルに関する業務委託契約は進んでいない

新しい働き方とは？

- テレワークなどの環境変化後の働き方と、旧来の働き方には、得意な点と不得意な点がある。
- それぞれの利点を考えて、ハイブリッドな社会環境に変化を!



JNSA

<https://www.jnsa.org/>

ご清聴
ありがとうございました

