NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

新しい働き方のサイバーセキュリティ対策

2020年11月13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
社会活動部会
冨田高樹（みずほ情報総研株式会社）

紹介する内容

1. 新しい働き方のサイバーセキュリティリスク

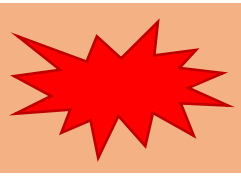
2. 「緊急事態宣言解除後のセキュリティ・チェックリスト」の解説

3. 企業における対策の考え方

１．新しい働き方のサイバーセキュリティリスク

ありがちな事例

■ 機密資料の参照

これまでの運用	機密文書を参照する場合は、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、参照が済んだら施錠して保管
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廃棄され、機密情報が漏えい 

あるべき対策（理想）

■ 機密資料の参照

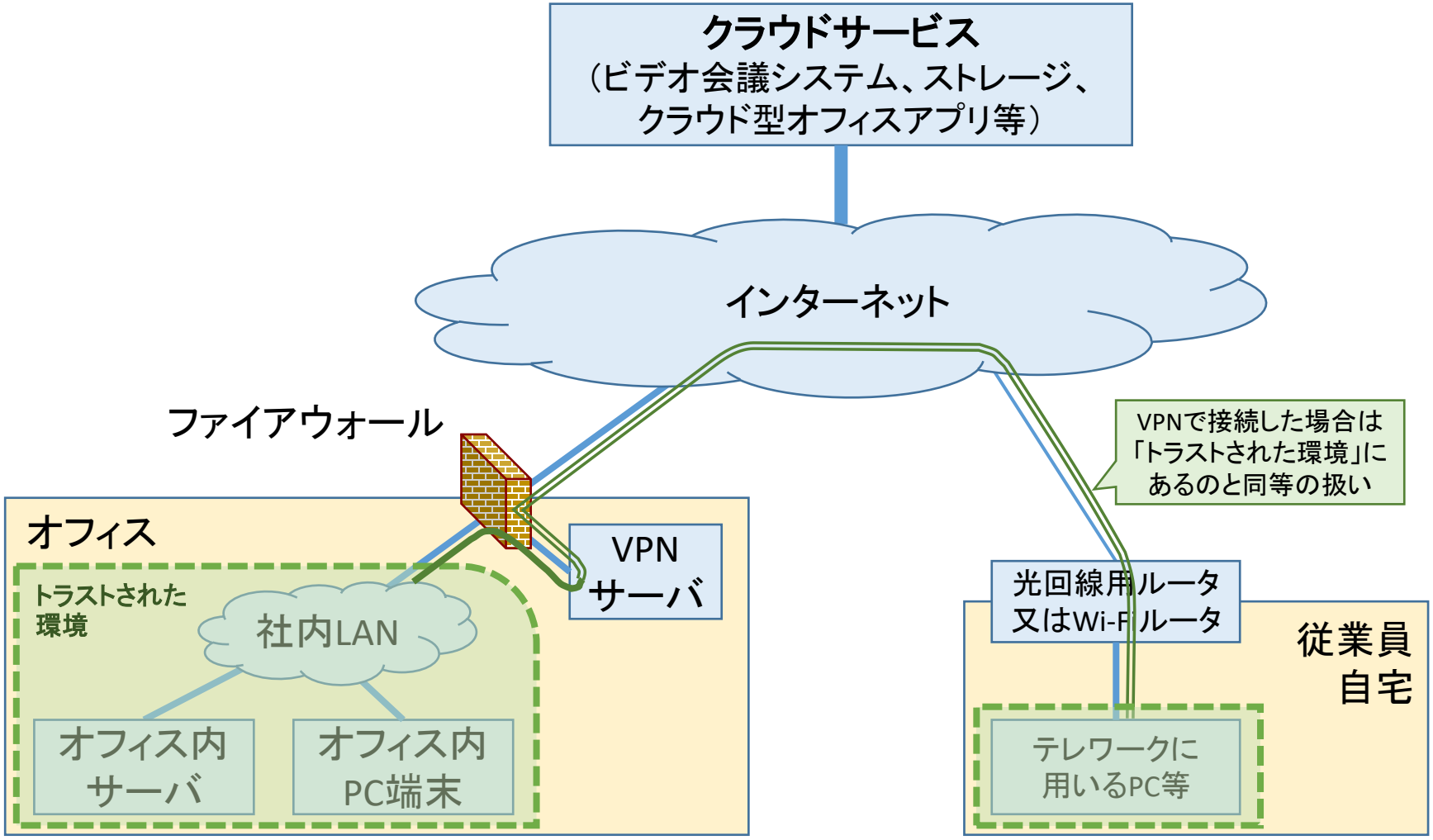
これまでの運用	機密文書を参照する場合は、管理者から鍵を借りて施錠されているキャビネから文書を取り出し、参照が済んだら施錠して保管
テレワークに伴う見直し	機密文書を電子化してアクセス制限をかけて保存。参照する場合は管理者が一時的に利用者に参照権限を付与
その結果	業務上のニーズとセキュリティを両立できた

・・・とはいえ、「電子化してアクセス制限をかけて保存」をいきなりやるのは無理で、結果としてテレワークを諦めた企業が多かったはず
⇒ 今からでも仕事の仕方の見直しを行うことは重要

「新しい働き方」で何が変わったのか

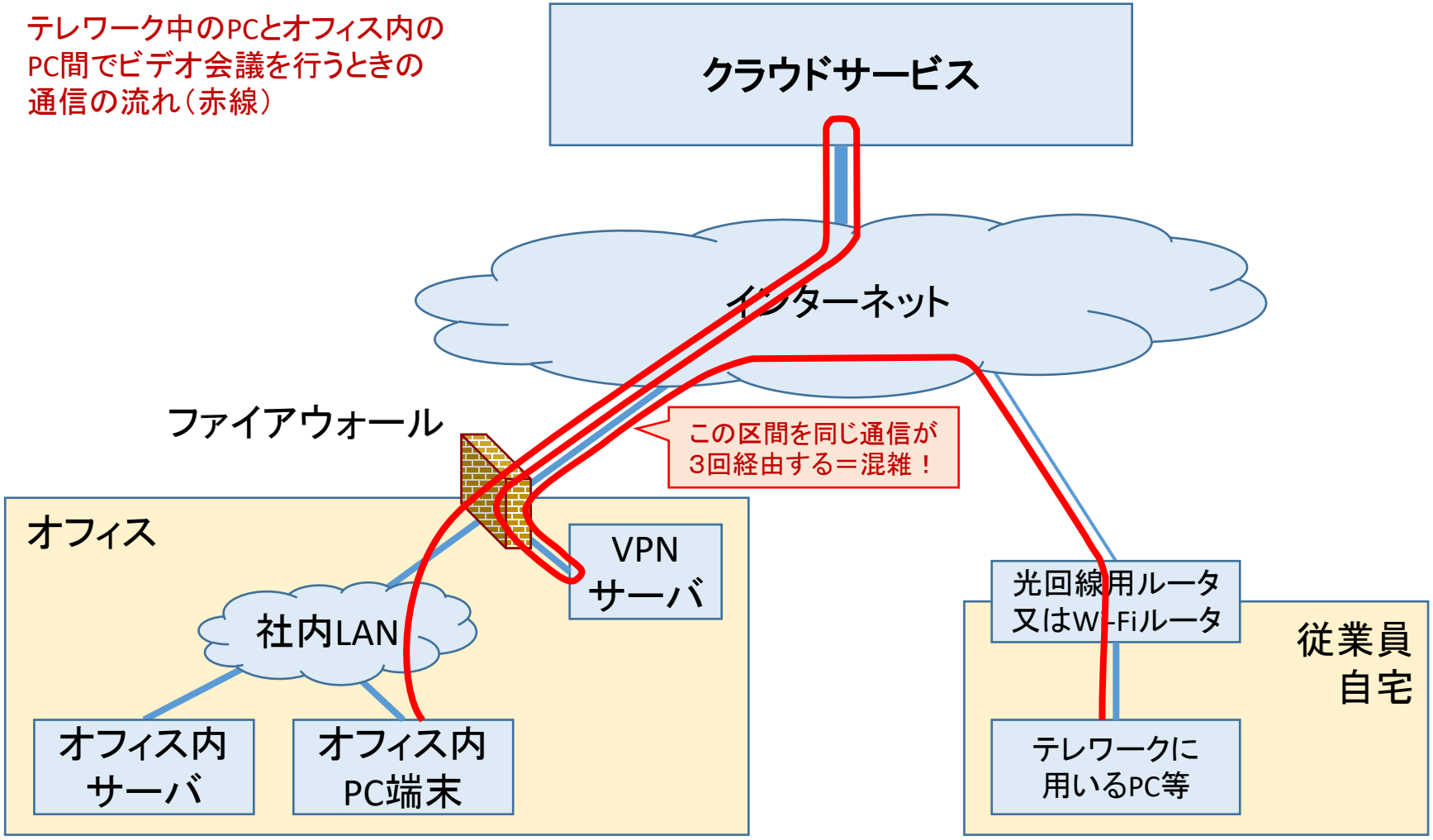
- サイバーセキュリティの観点で見ると：
  - ① オフィスを安全に保つだけでは守れない
    - 「境界防御モデル」の限界
  - ② 業務で利用するIT環境への依存度が高まる
    - ITインフラの性能が業務効率に直結
  - ③ 業務環境の管理主体が多様化
    - 在宅環境のセキュリティ責任者は、在宅でテレワークを行う従業員である

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

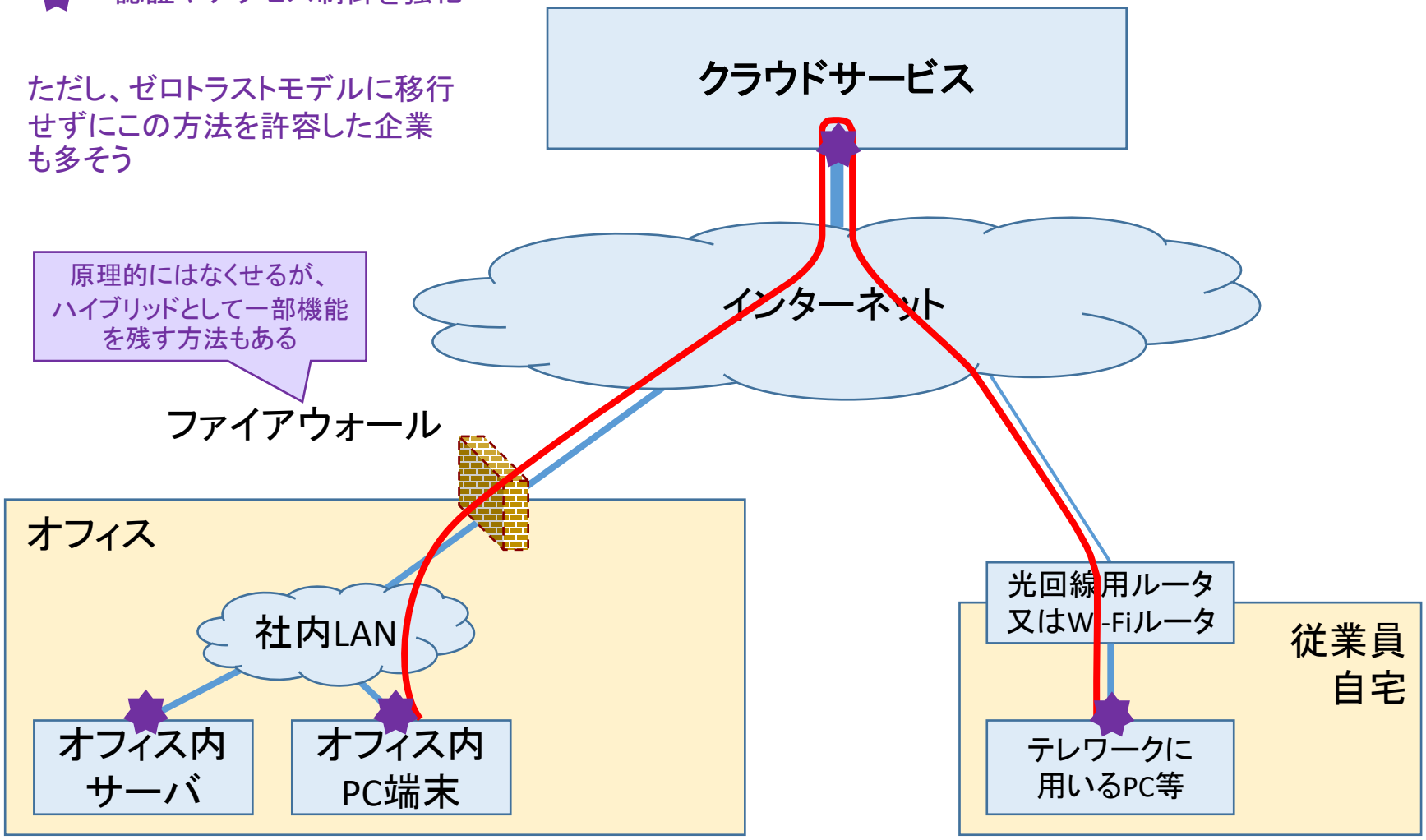
テレワーク中のPCとオフィス内のPC間でビデオ会議を行うときの通信の流れ（赤線）



ゼロトラストだとどうなるか

＝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



２．「緊急事態宣言解除後のセキュリティ・チェックリスト」の解説

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

チェックリストの構成

◆＝システム管理者向け、★＝システム管理者＋経営者向け

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に以下の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を行う
- ✓ 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を行う（OS・ソフトウェアの最新化、アンチウイルスソフト定義ファイルの最新化等）

解説書による説明のポイント

- **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

- ✓ 持ち出した機器（端末や外部記憶媒体等）が紛失していないか棚卸し確認する
- ✓ 端末のセキュリティ対策が最新化されているか確認する（OS・ソフトウェアの最新化、アンチウイルスソフト定義ファイルの最新化等）
- ✓ 持ち出した機器（端末や外部記憶媒体等）がマルウェアに感染していないか確認する
- ✓ 無許可のソフトウェアがインストールされていないか確認する
- ✓ テレワーク期間中に、社内システムに不正アクセスされていないかログ等を確認する
- ✓ 社内ネットワークに接続した端末から不審な通信が行われていないか監視を一定期間強化する

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

- ✓ 緊急措置として許可した私物端末利用（BYOD）の利用実態について確認する（私物端末のセキュリティ対策やマルウェア感染の有無、私物端末に保存されていた業務関連資料の削除確認等）
- ✓ 緊急措置としてテレワークを許可していた業務やルールを変更した業務のリスクを再評価する
- ✓ 再評価により、リスクが許容できると判断された業務については、引続きテレワークを継続すべく、必要に応じてセキュリティポリシー等の改訂を行うことを検討する
- ✓ 再評価により、リスクが高いと判断された業務については、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する

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（1／3）

- ✓ 第二波など緊急事態宣言の再要請に備え、業務移行の手順、必要なサービスを整理する
- ✓ テレワークにより負荷が集中した従業員や業務の洗い出しと対応の見直しを行う
- ✓ テレワークにより負荷が集中したサービスの洗い出しと対応の見直しを行う
- ✓ テレワークにより業務効率が下がった業務の洗い出しと対応の見直しを行う
- ✓ テレワークにできなかった業務の洗い出しと今後の対応について検討する

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（2／3）

- ✓ 脱押印のためのオンラインワークフローや電子署名サービスの導入について検討する
- ✓ 社内業務だけでなく、顧客や外部委託先との契約上、テレワーク化することができない業務やサービスについて、テレワークができる手段を検討し、顧客や外部委託先と協議の上、必要に応じて契約条件の見直しを検討する
- ✓ 今までのIT投資やセキュリティ対策の優先順位を見直し、テレワークを前提とした社内IT投資やセキュリティ対策について検討する

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（3／3）

- ✓ テレワークを前提としたシステム構成管理やログ設定の見直しを行う
- ✓ クラウドサービスや社内外で安全かつシームレスに業務を実施するためのゼロトラストネットワークの導入を推進する
- ✓ テレワークを前提としたセキュリティインシデント発生時の体制や対応について再検討を行うと共に、そのための教育や訓練を行う
- ✓ これを機会に、リスクの再評価を行い、セキュリティポリシーにおいて形骸化した項目を見直すと共に、社員等への周知やセキュリティリテラシーの向上を行う

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

- ✓ 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こと
- ✓ 持ち出した機器を紛失・破損をしてしまったら、正直に報告すること
- ✓ 在宅勤務中に無断でインストールしたソフトがあれば、全て報告すること
- ✓ 在宅勤務中に、怪しい動きなどの心配なことがあったら、すぐに報告すること
- ✓ 在宅勤務中に私物パソコンを使って業務を行った場合には、その事実を報告すること
- ✓ 在宅に必要な機器を整理し、ハイブリット勤務に備えること
- ✓ 在宅でもできる仕事、在宅ではリスクがある仕事をリストアップして業務を見直すこと
- ✓ 会社のセキュリティルールに課題があれば、リストアップして報告すること

一般従業員がチェックすべき事項のポイント

- 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

企業へのアドバイス

- 「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」の決まりはない
- 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

（参考）テレワークの方式の変遷

■ 総務省「**テレワークセキュリティガイドライン**」に見る方式数の変遷

2013年 3月
第３版
３種類

- **パターン①** オフライン持ち出し型
- **パターン②** オンライン持ち出し型
- **パターン③** シンクライアント型

2018年 4月
第４版
６種類

- **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** クラウド型アプリ方式
- **パターン④** セキュアブラウザ方式
- **パターン⑤** アプリケーションラッピング方式
- **パターン⑥** 会社PCの持ち帰り方式

2020年 9月
中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）
８種類

- **方式①** 会社支給端末・VPN/リモートデスクトップ方式
- **方式②** 会社支給端末・会社非接続方式（クラウドサービス型）
- **方式③** 会社支給端末・会社非接続方式（手元作業型）
- **方式④** 会社支給端末・セキュアブラウザ方式
- **方式⑤** 従業員所有端末・VPN/リモートデスクトップ方式
- **方式⑥** 従業員所有端末・方式（クラウドサービス型）
- **方式⑦** 従業員所有端末・会社非接続方式（手元作業型）
- **方式⑧** 従業員所有端末・セキュアブラウザ方式

３．企業における対策の考え方

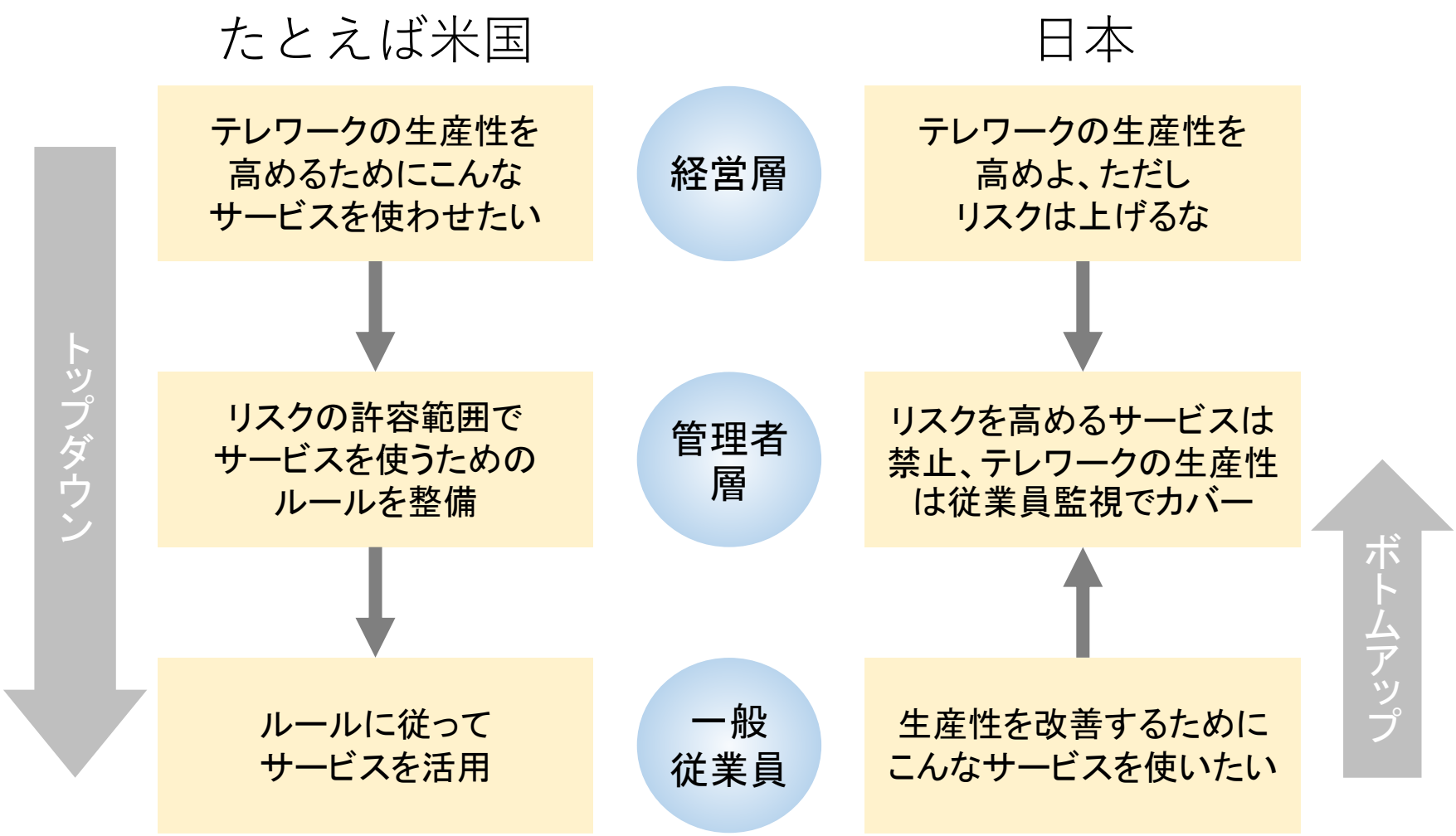
「新しい働き方」をセキュリティが阻害？

- サイバーセキュリティインシデントが起きなければよいのか？
  （例：コラボレーションツールの利用）

自社	競合他社
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	従業員へのサイバーセキュリティ教育をした上で容認
↓	↓
コラボレーションツールを使いたい顧客が離反	コラボレーションツールを使いたい顧客との契約維持
↓	↓
セキュリティは確保されているが業績が低下	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」目標を達成できたかもしれないが、
業績悪化の責任をとれるのか？

米国等と日本の企業カルチャーの違い



「新しい働き方」に対応ないし推進する観点から 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

「新しい働き方」で、陥りがちな罠の例

①	非常事態宣言期間に緊急避難的にテレワークを開始したが、セキュリティ上の問題は特に起きなかった。なので、このまま続けても大丈夫だろう。
②	セキュリティで有名な企業もサイバー攻撃の被害が起きている。費用をかけても結局やられるのなら、対策は安価なものを形だけ入れておけばよい。
③	テレワーク開始にあたり、情報システム部の社員に自社サーバーへのアクセスログの監視を強化するように指示した。なので何の心配もいらない。
④	これまで「標的型攻撃対策製品」や「次世代ファイアウォール」などベンダーの勧めに従って導入したがカモられただけの気がする。今度はテレワークをダシにまたボられるのではないか。

陥りがちな罠①

非常事態宣言期間に緊急避難的にテレワークを開始したが、セキュリティ上の問題は特に起きなかった。なので、このまま続けても大丈夫だろう。

- 問題が生じなかったのは「たまたま」であって、これまでの対策が前提としていた条件が変われば、リスクも変わります。
- テレワークの場合、以下に例示するような条件変化に応じて、組織のセキュリティ関連ルールや対策を見直す必要があります。
  - 秘密情報の社外への持ち出しの有無
  - 通信回線を通じた秘密情報のやりとり
  - 秘密情報に関するビデオ会議でのやりとり
  - 私物PCやスマートフォンの業務利用
  - 組織で契約しているクラウドへの社外からのアクセス

陥りがちな罠②

セキュリティで有名な企業もサイバー攻撃の被害が起きている。費用をかけても結局やられるのなら、対策は安価なものを形だけ入れておけばよい。

- 公知になっていない脆弱性を用いた攻撃（ゼロデイ攻撃）を受けた場合、有名企業でも完全に防ぐことは困難です。しかし攻撃されたことに気付くことはできたとも言えます。
- 中小企業もサイバー攻撃の対象外ということはなく、攻撃が成功したことに気付いていない可能性が高いことが、2019年7月に公表された大阪商工会議所、東京海上日動、神戸大学による実証事業において明らかになっています。
  - 実証対象の中小企業で観測した結果要旨：
    - 調査対象30社のすべてで不審な通信の記録が存在することを確認
    - うち５社においては、悪意のサイトとのデータのやり取りが繰り返されていることが判明

陥りがちな罠③

テレワーク開始にあたり、情報システム部の社員に自社サーバーへのアクセスログの監視を強化するように指示した。なので何の心配もいらない。

- 膨大なアクセスログのうち、何が正当なテレワーク利用で、何が攻撃なのかを区別するのは容易ではありません。
- 罠②に示したように、プロでも気づけないことはありますが、現状において異常を早期発見しようとすれば、商用のセキュリティ監視サービスを利用するほうが、コスト的にも有利な場合が多そうです。
- 経済産業省とIPAでは、民間事業者が提供するセキュリティ監視・運用サービスのうち、一定の品質が確保されていることを審査機関にて確認したものを掲載したリストを「情報セキュリティサービス基準適合サービスリスト」として公表しています。（前掲）

陥りがちな罠④

これまで「標的型攻撃対策製品」や「次世代ファイアウォール」などベンダーが勧めるままに導入したがカモられただけの気がする。今度はテレワークをダシにまたボられるのではないか。

- 実際に悪質なベンダーがこうした売り方をしている可能性はあります。目的に応じて適切なソリューションを導入しましょう。
- 国内の企業がセキュリティ対策にどのくらい投資しているのかは、IPAやJUAS、NRIセキュアテクノロジーズ等が関連するアンケート調査結果を公表していますので、こうしたデータが投資額の参考になります。
- どのような対策が自社にふさわしいかは、様々に公表されているテレワークの導入事例をもとに検討することが考えられます。

https://www.jnsa.org/