個人まかせではないPCで
安全にテレワークの実現を

Ｓｋｙ株式会社　ICTソリューション事業部　副本部長
金井 孝三

Ｓｋｙ株式会社　会社概要

本社所在地	東京本社　東京都港区港南二丁目16番1号　品川イーストワンタワー　15階 大阪本社　大阪市淀川区宮原3丁目4番30号　ニッセイ新大阪ビル　20階
設立	1985年3月2日
資本金	4億5千万円
売上高	763.6億円（2020年3月期）
従業員数	3,030名（2021年2月1日現在）
グループ従業員数	3,148名（2021年2月1日現在）
拠点所在地	札幌、仙台、東京、横浜、三島、名古屋、 大阪、神戸、広島、松山、福岡、沖縄
グループ会社	株式会社エッグ

アジェンダ

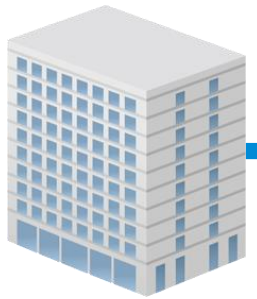
1. テレワークを実現する各種方式
2. テレワーク環境を狙うサイバー攻撃
3. これからのゼロトラストネットワークにも重要なPCの適切管理
4. 安全なPCはIT資産把握とセキュリティパッチの適用の徹底から
5. 組織を守るためには組織がPCを安全に維持することが重要

テレワークを実現する各種方式

「テレワーク（telework）」とは？

「tele = 離れた所」と「work = 働く」をあわせた造語です。ITを活用し、オフィスから離れて、時間や場所の制約を受けずに柔軟に働く働き方を指します。

オフィス



テレワーク

- モバイルワーク

以前からよく行われてきた「テレワーク」

- サテライトオフィス

- 在宅勤務

緊急事態宣言発令中の地域は「出勤者数7割削減」

モバイルワークと在宅勤務の環境の違い

「モバイルワーク」は主に移動時間を有効活用するものです。「在宅勤務」とは大きく異なります。

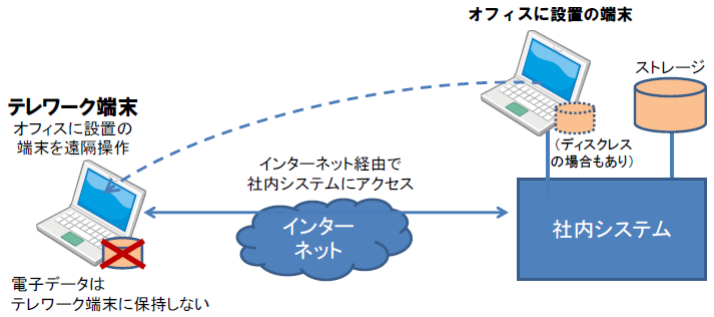
	モバイルワーク	在宅勤務
目的・メリット	業務の効率化 （働く場所を自由に選択、 移動時間を活用 など）	仕事と家庭の両立、 災害／パンデミック対策
対象の職種	移動が多い職種 （主に営業）	モバイルワーカーに加え、 業務をPCで行う職種 （主に事務）
業務で通常使うPC	モバイルPC 	デスクトップPC ／モバイルPC 
テレワークを行う時間	1日の一部の時間 （必要な時は出社する）	テレワーク実施日の 業務時間中（出社しない）

テレワークの6種類のパターン

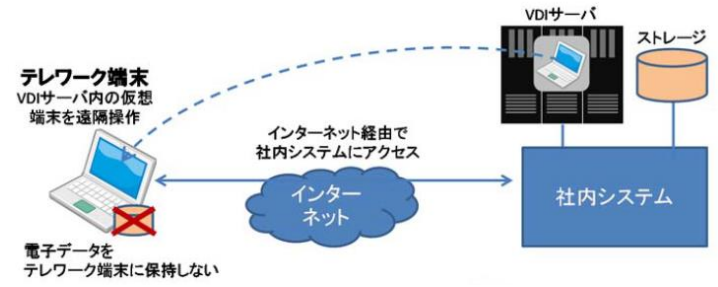
出典：総務省「テレワークセキュリティガイドライン」第4版
https://www.soumu.go.jp/main_content/000545372.pdf

業務環境へアクセスする際に用いるIT技術によって、テレワークは6種類のパターンに分けられます。

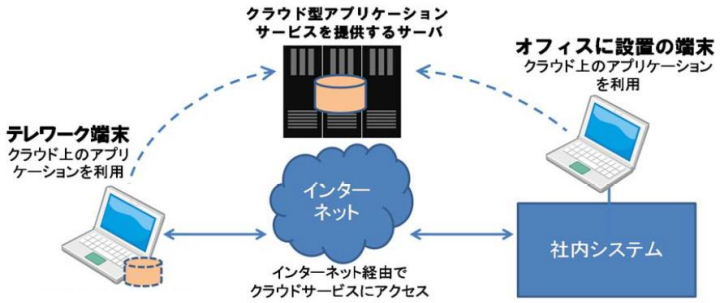
1 リモートデスクトップ方式



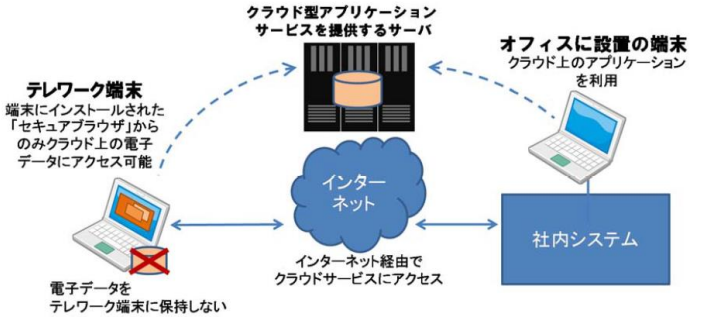
2 仮想デスクトップ方式



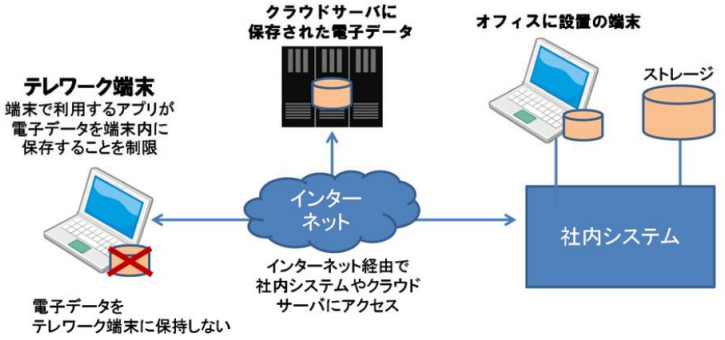
3 クラウド型アプリ方式



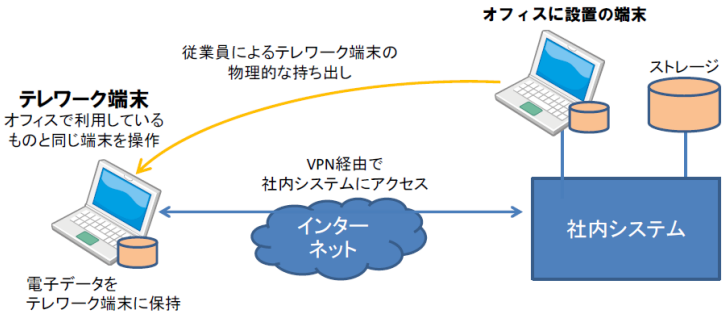
4 セキュアブラウザ方式



5 アプリケーションラッピング方式



6 会社PCの持ち帰り方式



在宅勤務の場合の、各パターンのまとめ

利用シーンを想定して各パターンをまとめると、下表のようになります。

1 リモートデスクトップ方式

- 私物PCにデータがない
- 自宅に高速回線が必要
- オフィスと同じ環境

2 仮想デスクトップ方式

- 私物PCにデータがない
- 自宅に高速回線が必要
- オフィスと同じ環境

3 クラウド型アプリ方式

- 私物PCにデータを保存
- 自宅に高速回線が欲しい
- クラウドのみ使用可能

4 セキュアブラウザ方式

- 私物PCにデータがない
- 自宅に高速回線が欲しい
- クラウドのみ使用可能

5 アプリケーションラッピング方式

- 私物PCにデータがない
- 自宅に高速回線が欲しい
- コンテナ対応しか使えない

6 会社PCの持ち帰り方式

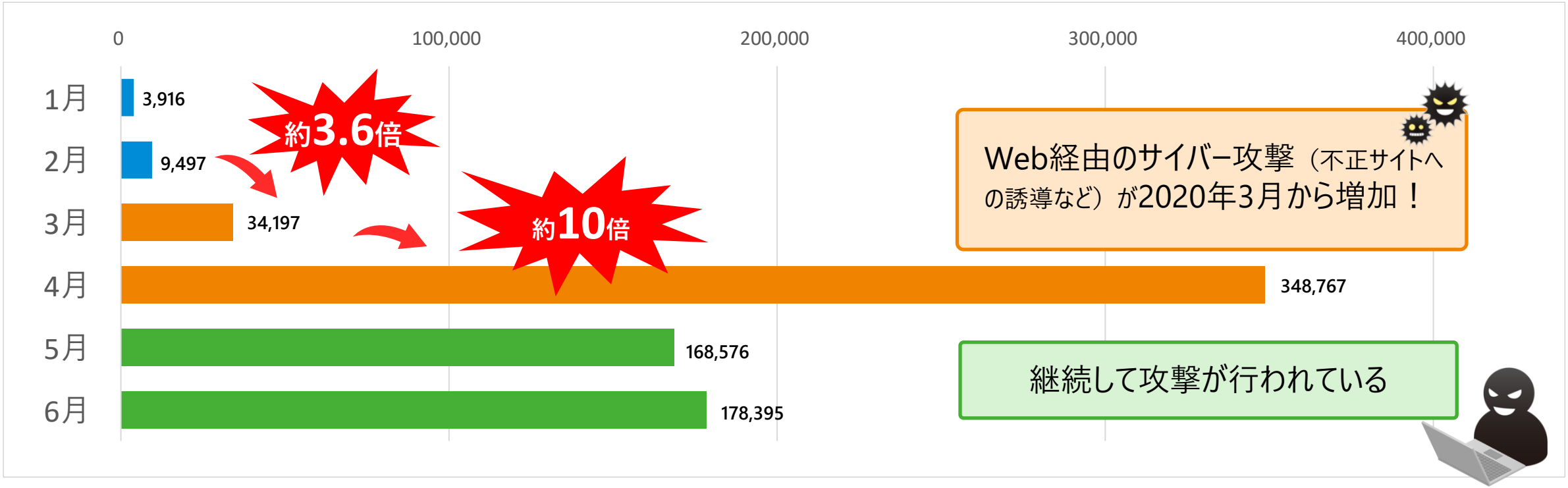
- 私物PCにデータがない
- 自宅の高速回線は不要
- オフィスと同じ環境

テレワーク環境を狙うサイバー攻撃

新型コロナウイルス感染症の拡大に便乗するサイバー攻撃

多くの企業でセキュリティ対策が不十分なままテレワークの導入を余儀なくされ、サイバー犯罪者はこの状況を利用した攻撃を活発化させました。この感染症拡大は、いまだに収束の兆しがみえておらず、今後も攻撃が続くと思われます。

▼全世界における2020年のCOVID-19関連不正サイトへ誘導されたアクセス数の推移



参考：トレンドマイクロ「2020年 上半期セキュリティラウンドアップ」新型コロナウイルスがサイバーセキュリティ業界に与えた影響

テレワークの弱点を利用する攻撃が発生

- VPN製品の既知の脆弱性を突き、取得したと見られる
  認証情報約900件がインターネット上に流出
- 大手製造企業がサイバー攻撃の被害を受け、国内外9工場が生産停止
- 大手IT企業従業員のBYOD端末からVPNを通り、
  VDI経由で社内サーバーに不正アクセス
- 大手製造業の従業員がテレワークで使用するPCで、
  社内ネットワークを経由せずSNSを利用し、マルウェアに感染
- オンライン会議サービス用のソフトウェアインストーラーに、
  マルウェアをバンドルして再配布する攻撃

脆弱性を悪用された事例

VPNの脆弱性を悪用され、暗証番号を含む情報が流出

2020年8月、VPNサーバーの暗証番号を含む情報が、ロシアのハッキングフォーラム上で公開されていることが判明。
対象のVPNサーバーは全世界で900件以上。うち、日本国内のIPアドレスは46社含まれることが確認された。
流出の原因になったのは、2019年4月に公表されたVPNサーバーの脆弱性とされる。

※VPN暗証番号：VPN管理者による新規グループ開設後、参加者の申し込みをするために必要となる番号。VPNに接続する際の認証用パスワードとは異なります。

【脆弱性】とは
コンピューターのOSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した「セキュリティ上の弱点」

**OSやサーバー、ソフトウェアを最新版に
アップデートしないことは非常に危険です！！**

テレワーク中にマルウェアに感染した事例

社内ネットワークを経由せずSNSを利用し、マルウェアに感染＜製造業＞

2020年4月、自宅でのテレワーク時に社内Firewall等を経由せず社員がSNS を利用。その際にマルウェアを含んだファイルをダウンロードして感染。出社時にマルウェアに感染したPCを社内ネットワークに接続したことで、社内ネットワークを通じて感染が拡大した。
機密性の高い技術情報、取引先に係る重要な情報の流出は確認されていない。

ビデオ会議システム「Zoom」へのサイバー攻撃

テレワークによるオンライン会議ツールの使用が増加しました。特にZoomは主要サービスを無料で使えることなどから利用者が急増しましたが、サイバー攻撃の被害も相次ぎ、話題となりました。

過去に発生したZoomへのサイバー攻撃やセキュリティの問題

1 会議に不正侵入する「Zoombombing（ビデオ爆撃）」

関係のない人がZoomによるWeb会議へ乱入して暴言を発したりすることがあった。

Zoom 5.0 以降で解決！

2 チャット機能の脆弱性

Window版のZoomクライアントのチャット機能にUNC （Universal Naming Convention）パスの処理に関する脆弱性が確認されており、PCの情報を不正に取得される危険性があった。

Zoom 4.6.10 以降で解決！

3 エンドツーエンド※1の暗号化が行われていなかった

Zoomを使った通信はエンドツーエンドの暗号化によって保護されているはずだったが、サーバー上に保有するデータが復号可能な状態であることが発覚。

※1 通信を行う人同士しか見られないようにすること。

Zoom 5.0 以降で解決！

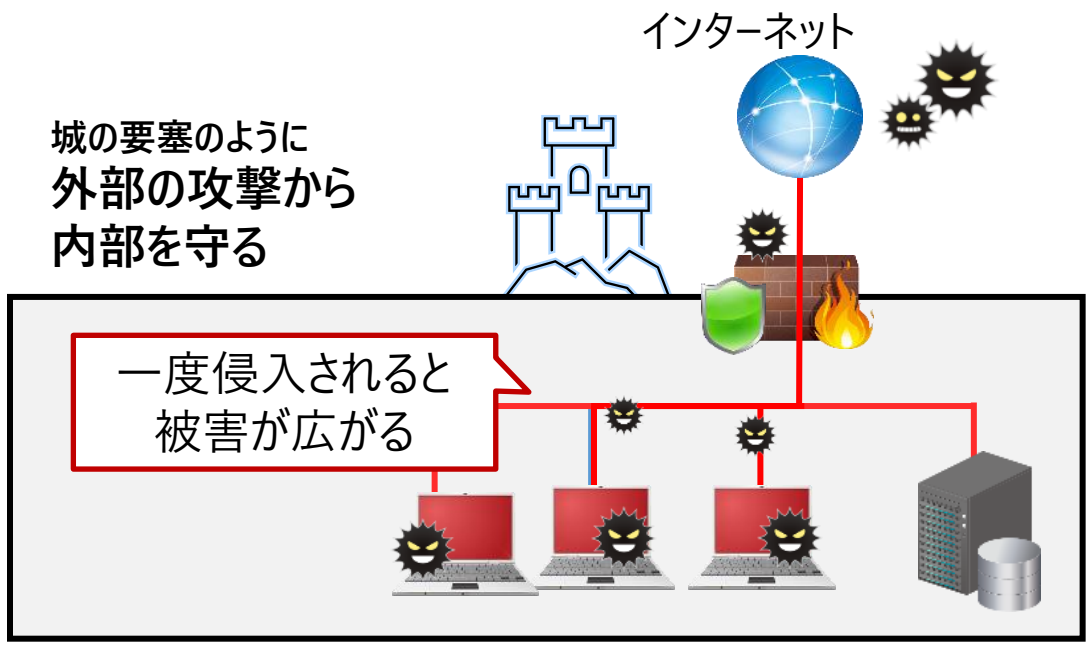
ソフトウェアは最新のバージョンにて使用することをお勧めします

これからのゼロトラストネットワークにも重要な
PCの適切管理

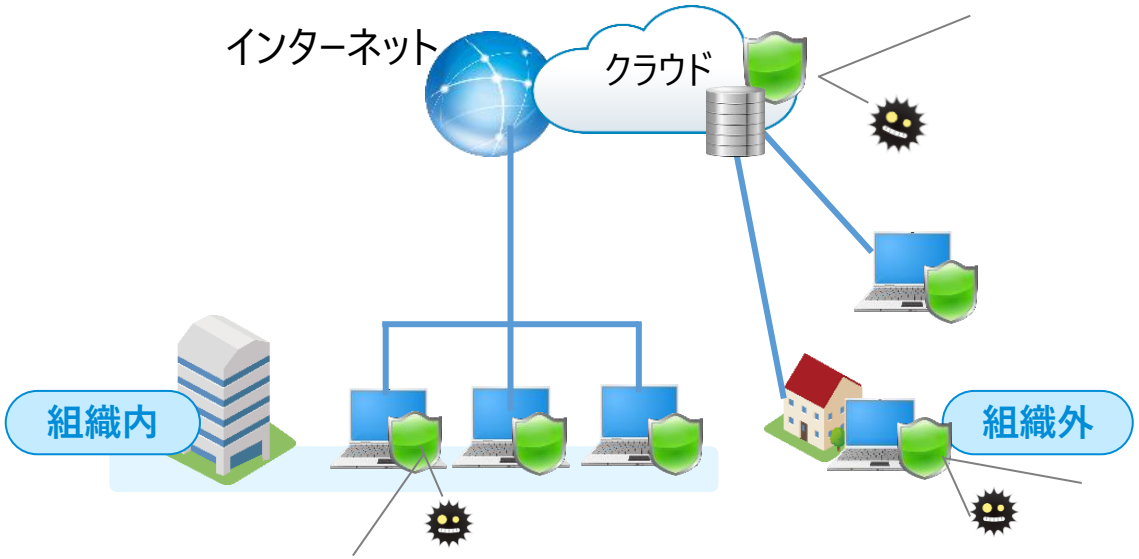
新しいセキュリティモデル「ゼロトラストセキュリティ」

「信頼しない」という言葉の通り、外部も内部も全て疑うという「性悪説」に基づいた考え方です。
ネットワークの内部を守る従来の「境界型セキュリティ」では、安全の確保が難しくなってきたため注目されています。

境界型セキュリティ



ゼロトラストセキュリティ

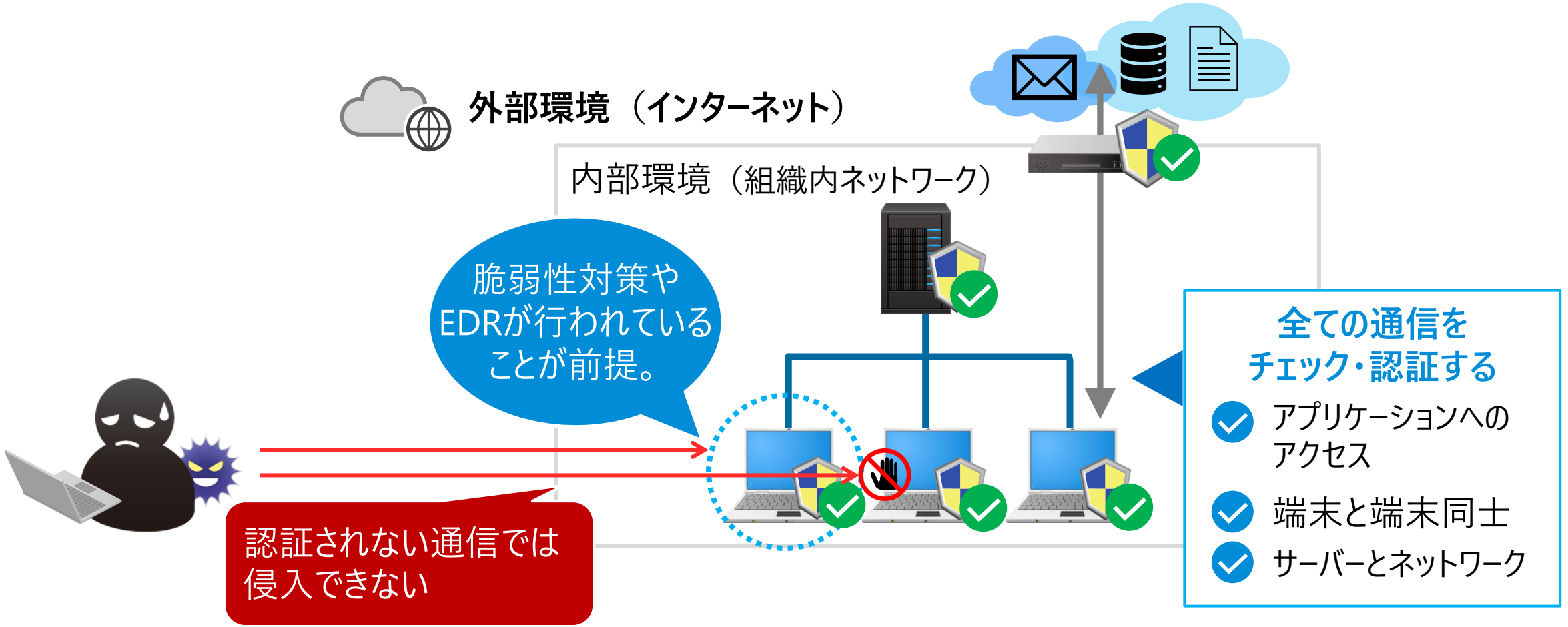


侵入を前提で、各ポイントのセキュリティを強化

- クラウドのセキュリティ
- 認証によるアクセス制御
- 端末のセキュリティ対策

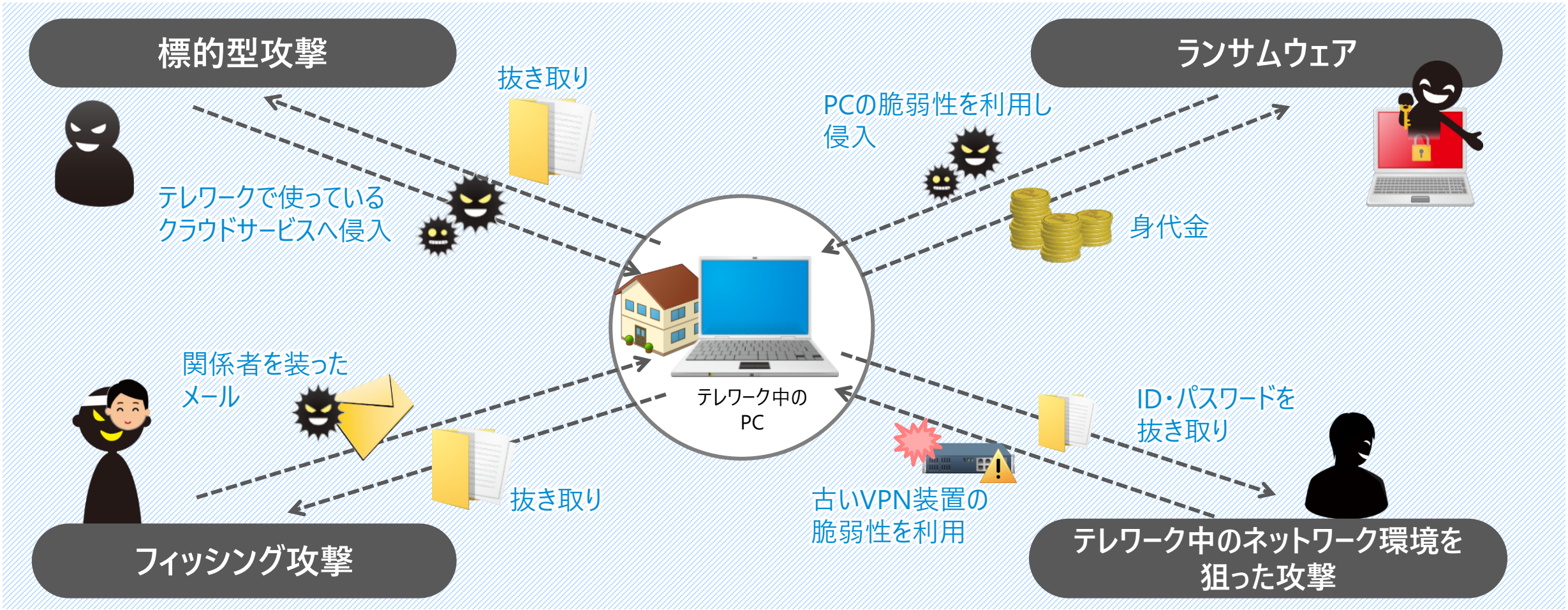
なぜ今、ゼロトラストセキュリティが求められるのか？

在宅勤務の導入などにより、インターネットを経由した組織内ネットワークの利用が求められる今、境界を強固に保つことが難しくなりつつあります。「ゼロトラストセキュリティ」はエンドポイントとの通信を毎回認証し、記録することでマルウェアの拡大感染のリスクを下げることを目指します。



サイバー攻撃の標的となるクライアントPC（在宅勤務）

「クライアントPC」は、さまざまな情報にアクセスできるので、サイバー攻撃のターゲットになりやすいです。そんなクライアントPCが在宅勤務用に急遽、一斉に持ち出されたことで、さらにリスクが高まっています。



ゼロトラストでは、クライアントPCのセキュリティ対策が極めて重要

―企業・団体向け クライアント運用管理ソフトウェア―
SKYSEA Client View
スカイシー クライアント ビュー

これから（ゼロトラスト）は組織内／外に関わらず
個々のエンドポイント・セキュリティが必要

IT資産管理　ログ管理

利用するエンドポイント（デバイス）の把握

管理するデバイスを把握し、管理外の信頼できないシャドーITを排除

Windows 10、Microsoft 365 アップデート支援

OSやアプリケーションの更新プログラム適用の徹底

脆弱性対策として、OSやアプリケーションを最新の状態に保つ

ITセキュリティ対策強化（連携）

EDR製品等の導入

アンチウイルス機能だけでなく、
未知の脅威に対する振る舞い検知や、
検知後の駆除や調査にも対応

安全なPCはIT資産把握と
セキュリティパッチの適用の徹底から

組織を狙ったランサムウェアの身代金の額は、急騰しています

以前のランサムウェアは主に個人を狙っていたため、感染した場合の被害額は数十万円程度でした。ところが2020年下半期より、さらに攻撃が巧妙になり、より高額の身代金を要求される事例が報告されています。

2020年7月 アメリカ

1,000万ドルを要求。
要求に応じなかったため、
顧客向けサービスが
5日間停止。

2020年10月 欧州

同じ犯罪グループにより、
二度感染。
1,400万ドルを要求

2020年10月 ドイツ

盗み出した顧客データを
ダークウェブ上で公開。
2,300万ドルを要求

Wood Ranch Medical

Phone:(805) 306-0222 Fax:(805) 791-3080

135 Macaw Lane, Suite 210, Simi Valley, CA 9306

Wood Ranch Medical Notifies Patients of Ransomware Attack

SIMI VALLEY, CA – September 18, 2019 – Wood Ranch Medical ("WRM") was the victim of a ransomware attack that resulted in its patients' personal healthcare information being encrypted. As a result, we were unable to restore patients' healthcare records and will be closing our practice on December 17, 2019. Although there is no indication that any information was accessed, in an abundance of caution, we have taken steps to notify all patients and to provide resources to assist them.

On August 10, 2019, we suffered a ransomware attack on Wood Ranch Medical's computer systems. Ransomware is a computer virus that encrypts our computer system until and unless we pay money (i.e., the ransom) demanded by the attackers. The attack encrypted our servers, containing your electronic health records as well as our backup hard drives. These rampant attacks continue to challenge everyone in the business and medical communities. We believe it is likely the attacker only wanted money and not the information on our computers. While we have no reason to believe that anyone's healthcare information was taken, the encrypted system contained electronic healthcare records which included patients' names, addresses, dates of birth, medical insurance and related health information.

ランサムウェア感染で
2019年12月
事業廃止

**ランサムウェアに感染した場合、
倒産のリスクもあります**

※画像引用元：Wood Ranch Medical ホームページ

「テレワークを行う際のセキュリティ上の注意事項」

更新日：2020年9月14日
IPA（独立行政法人情報処理推進機構）
セキュリティセンター

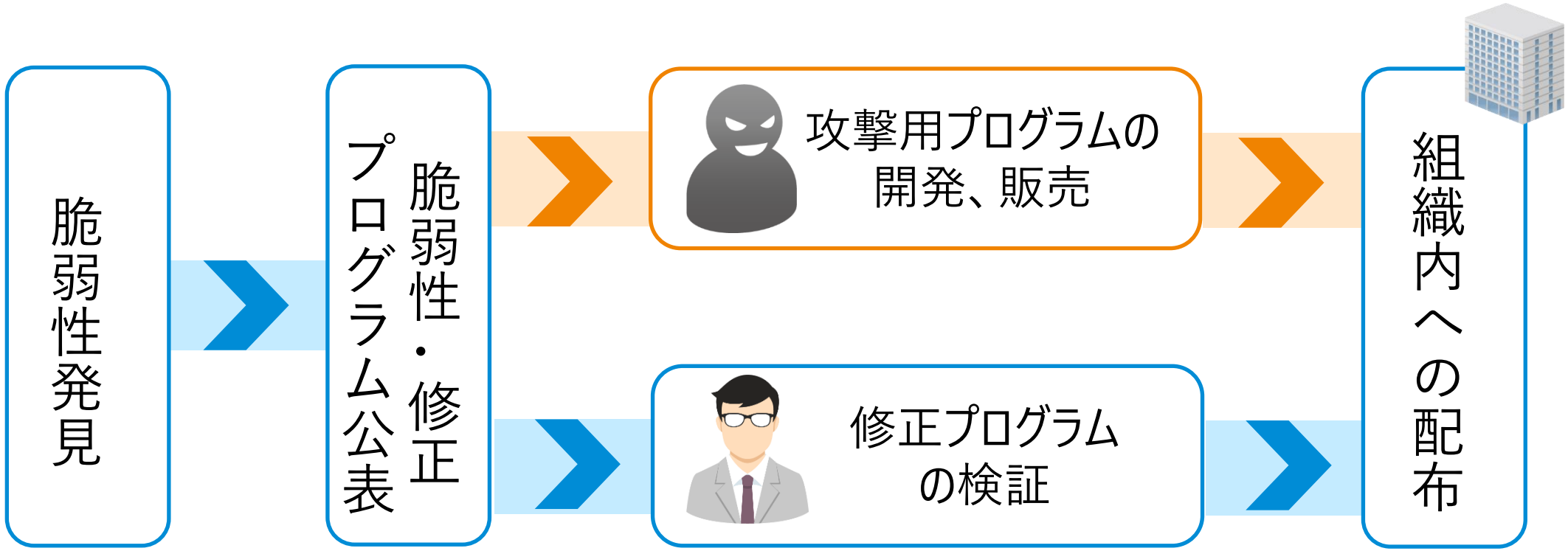
テレワークを行う際のセキュリティ上の注意事項として、IPAより以下の項目が示されています。

1.修正プログラムの適用
2.セキュリティソフトの導入および定義ファイルの最新化
3.パスワードの適切な設定と管理
4.不審なメールに注意
5.USBメモリ等の取り扱いの注意
6.社内ネットワークへの機器接続ルールの遵守
7.ソフトウェアをインストールする際の注意
8.パソコン等の画面ロック機能の設定

真っ先に挙げられているのが「修正プログラムの適用」です

修正プログラムが公開された脆弱性は、狙われやすいです

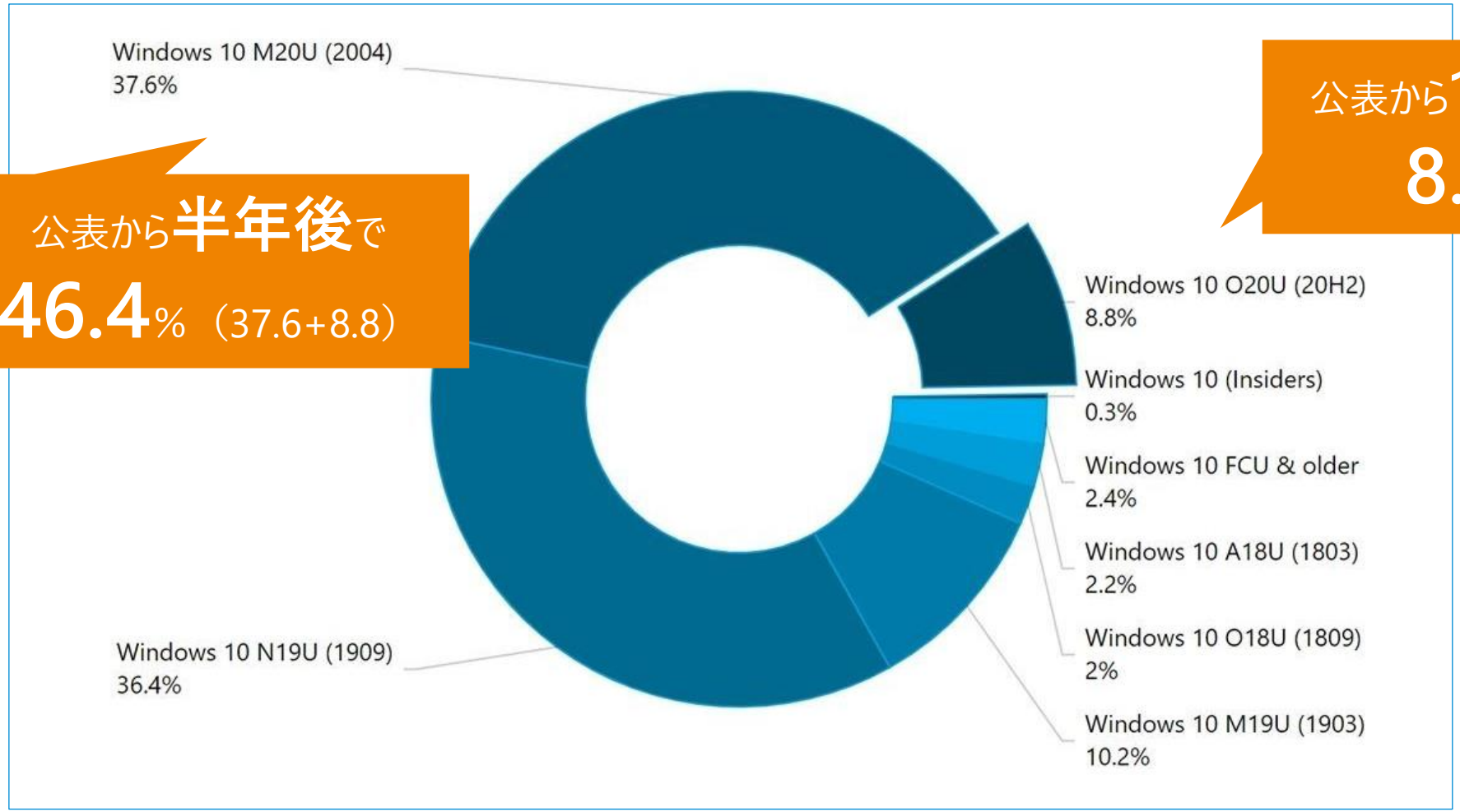
以前はセキュリティパッチが未公表の脆弱性を悪用したゼロディ攻撃が話題となっていましたが、近年は効率よく儲けるために、**公開されてすぐの脆弱性を攻撃するプログラムを開発**することが多いです。そして、開発された攻撃用プログラムは、ダークウェブ上で販売されます。



脆弱性対策に時間がかかるほど、狙われやすくなります

「修正プログラムの適用」の実態

Windows 10機能更新プログラム公表後の適用率の調査結果では、10日後に8.8%、半年後で46.4%です。



公表から**半年後**で
46.4%（37.6+8.8）

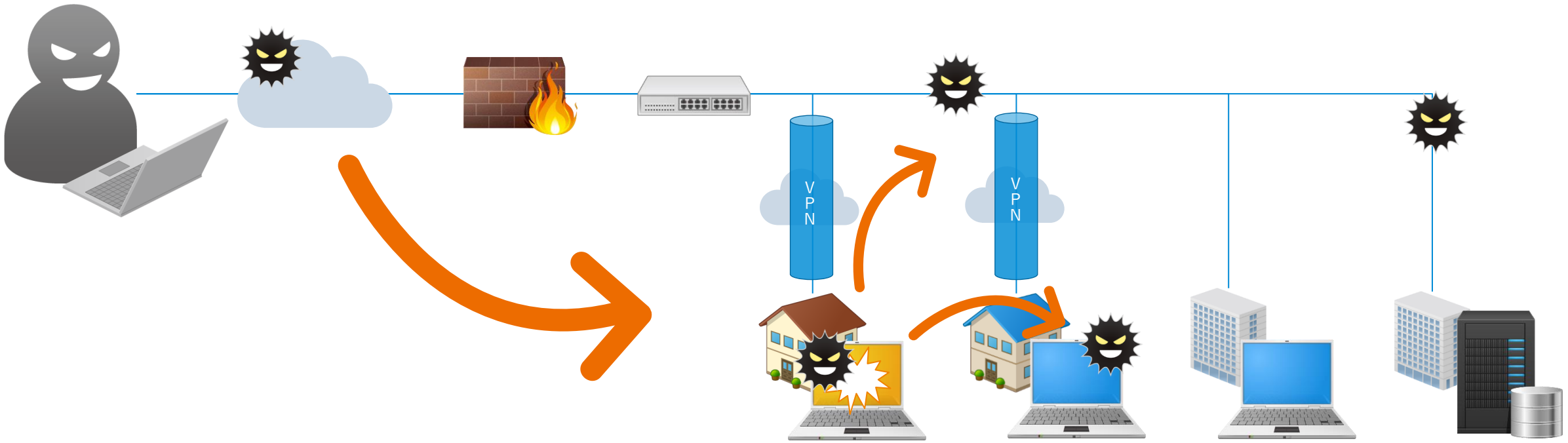
公表から**10日後**で
8.8%

PCを使うときに急に
Windows Updateが始まる
と仕事にならない。
後でやろうと思っていたけど、
つい忘れる…。

※出典：AdDuplex「AdDuplex Report for November 2020」 https://reports.adduplex.com/#/r/2020-11

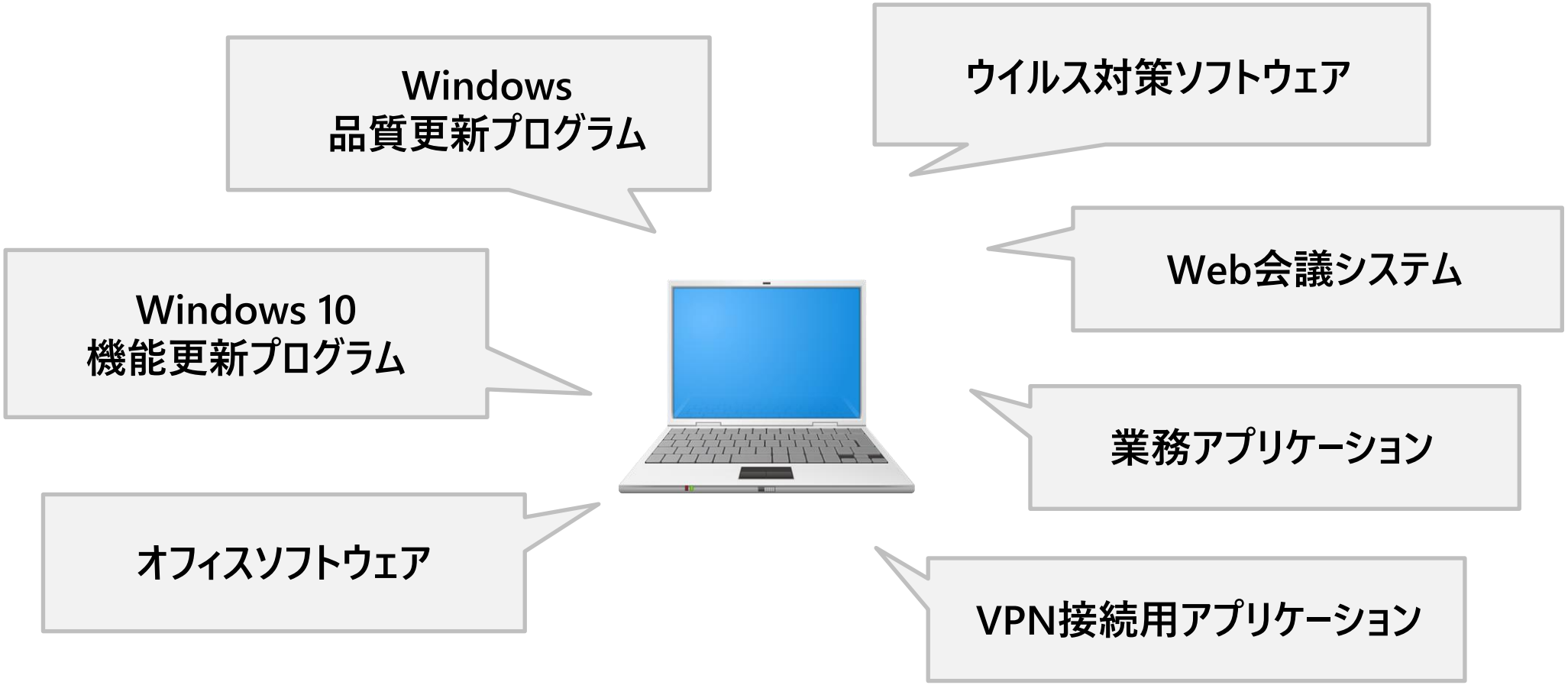
「修正プログラムの適用」は、ネットワーク上の全てのPCに必要

サイバー攻撃において、攻撃者はインターネットを介して組織内のネットワークに侵入し、ハッキング技術を用いて侵入範囲を拡大します。脆弱性があると、攻撃者による侵入や侵入範囲の拡大が行いやすくなります。



OSだけでなく、アプリケーションも最新の状態に

脆弱性が残された状態だと不正アクセスに利用されたり、マルウェアに感染する危険性があります。
脆弱性を利用した攻撃を防ぐためにも、管理しているPCのOS、インストールされているアプリケーションなどは最新の状態にしておく必要があります。

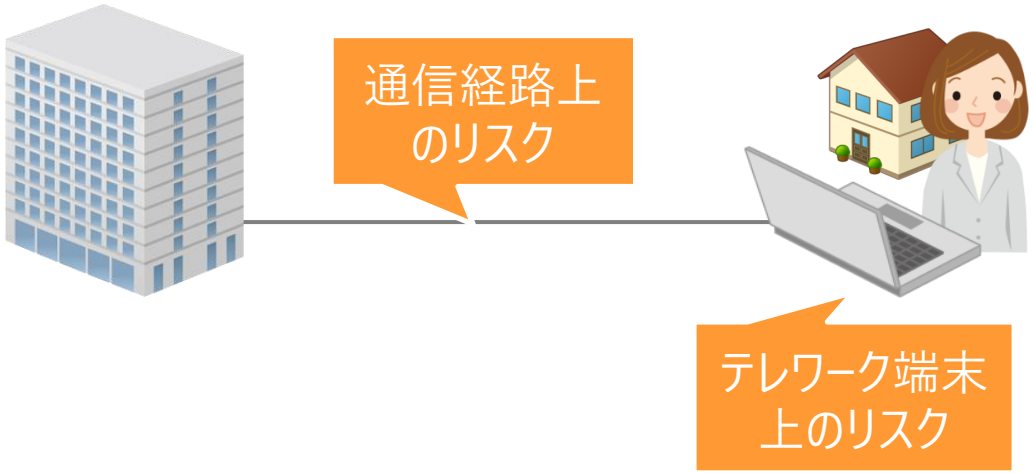


組織を守るためには
組織がPCを安全に維持することが重要

「テレワークセキュリティガイドライン」

テレワークの場合、オフィスと離れた場所で作業を行うため、通信経路上のリスクがあります。また、作業を行う端末から、情報が盗まれてしまう可能性があります。

こういったリスクを考慮して、総務省にて「テレワークセキュリティガイドライン」が定められています。現在の最新版は、2018年4月に策定された第4版です。

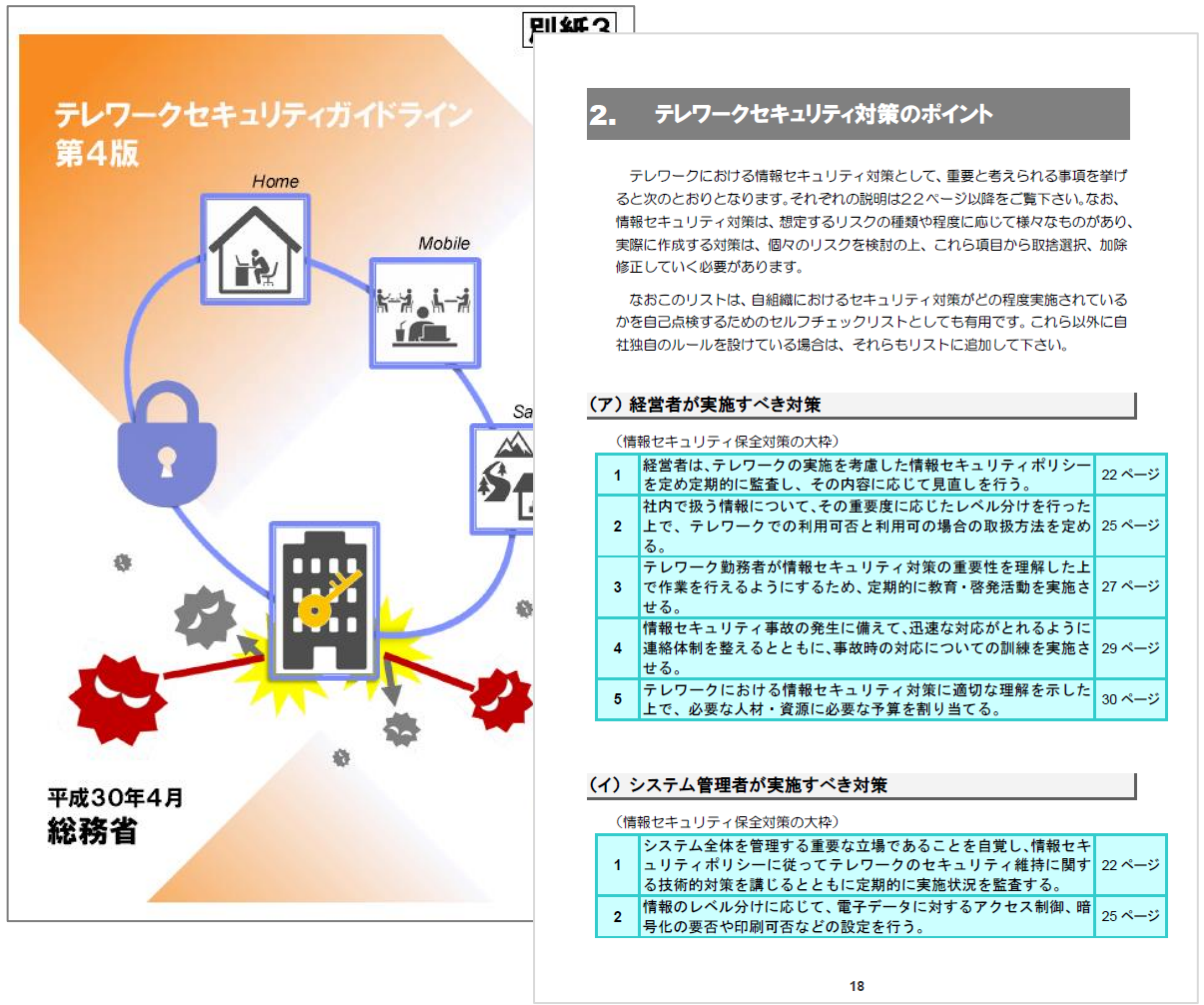


参考：総務省「テレワークセキュリティガイドライン」第4版　https://www.soumu.go.jp/main_content/000545372.pdf

セキュリティ対策のポイント

参考：総務省「テレワークセキュリティガイドライン」第4版　https://www.soumu.go.jp/main_content/000545372.pdf

「テレワークセキュリティガイドライン」では、それぞれの立場ごとにポイントがまとめられています。



2.　テレワークセキュリティ対策のポイント

テレワークにおける情報セキュリティ対策として、重要と考えられる事項を挙げると次のとおりとなります。それぞれの説明は22ページ以降をご覧下さい。なお、情報セキュリティ対策は、想定するリスクの種類や程度に応じて様々なものがあり、実際に作成する対策は、個々のリスクを検討の上、これら項目から取捨選択、加除修正していく必要があります。

なおこのリストは、自組織におけるセキュリティ対策がどの程度実施されているかを自己点検するためのセルフチェックリストとしても有用です。これら以外に自社独自のルールを設けている場合は、それらもリストに追加して下さい。

（ア）経営者が実施すべき対策

（情報セキュリティ保全対策の大枠）

1	経営者は、テレワークの実施を考慮した情報セキュリティポリシーを定め定期的に監査し、その内容に応じて見直しを行う。	22 ページ
2	社内で扱う情報について、その重要度に応じたレベル分けを行った上で、テレワークでの利用可否と利用可の場合の取扱方法を定める。	25 ページ
3	テレワーク勤務者が情報セキュリティ対策の重要性を理解した上で作業を行えるようにするため、定期的に教育・啓発活動を実施させる。	27 ページ
4	情報セキュリティ事故の発生に備えて、迅速な対応がとれるように連絡体制を整えるとともに、事故時の対応についての訓練を実施させる。	29 ページ
5	テレワークにおける情報セキュリティ対策に適切な理解を示した上で、必要な人材・資源に必要な予算を割り当てる。	30 ページ

（イ）システム管理者が実施すべき対策

（情報セキュリティ保全対策の大枠）

1	システム全体を管理する重要な立場であることを自覚し、情報セキュリティポリシーに従ってテレワークのセキュリティ維持に関する技術的対策を講じるとともに定期的に実施状況を監査する。	22 ページ
2	情報のレベル分けに応じて、電子データに対するアクセス制御、暗号化の要否や印刷可否などの設定を行う。	25 ページ

18

	項目数
経営者	5
システム管理者	１８
テレワーク勤務者	２０

離れた・見えない場所で業務を行うため、**テレワーク勤務者に求められる対策**が多いです。

テレワーク勤務者に求められる対策（例）

参考：総務省「テレワークセキュリティガイドライン」第4版　https://www.soumu.go.jp/main_content/000545372.pdf

- テレワーク作業中は、利用する情報資産の**管理責任を自らが負う**ことを自覚し、情報セキュリティポリシーが定める技術的・物理的及び人的対策基準に沿った業務を行い、定期的に実施状況を自己点検する。
- 第三者と共有する環境で作業を行う場合、端末の画面に**プライバシーフィルター**を装着したり、作業場所を選ぶ等により、画面の覗き見防止に努める。
- 作業開始前に、テレワーク端末にウイルス対策ソフトがインストールされ、**最新の定義ファイルが適用されていることを確認**する。

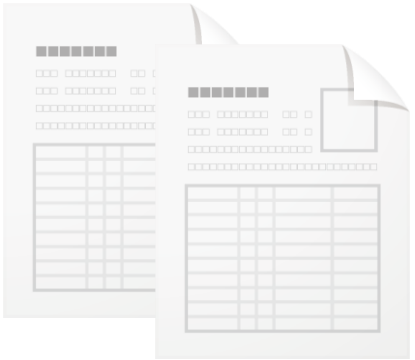
- マルウェア感染を防ぐため、ＯＳや**ブラウザ（拡張機能を含む）のアップデート**が未実施の状態で社外のウェブサイトにはアクセスしない。

- **無線LAN**利用に伴う**リスクを理解**し、テレワークで利用する場合は**確保すべきセキュリティレベルに応じた対策**が**可能な範囲で利用**する。

テレワーク勤務者に、ガイドラインを遵守いただくために

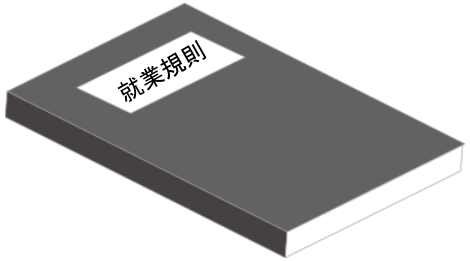
ガイドラインは、方向性を示すものなので具体的な作業については書かれていません。遵守するために具体的にどうすればいいのか、どこまでが必須なのか、手順書や基準を示すことも有効です。

どうすればいいのかわかりません



組織の現状に合わせた手順書

どこまでが必須かわかりません



業界団体等の公開情報を元に
就業規則として基準を整備

例えば介護業界の場合、「令和元年度 業界団体連携によるテレワーク導入促進事業補助金（東京都産業労働局）テレワーク勤務規程」が公表されています。
http://kaiziren.or.jp/wp/wp-content/uploads/2020/03/syuugyoukisoku0318.pdf

組織からの貸与PCをつかうことで、セキュリティ対策の実現へ

普段、情報システム部門が行っているような運用管理を、「全ての」テレワーク勤務者が「もれなく」実施することは困難です。
そのため、テレワークを実施する端末は、SKYSEA Client Viewのような運用管理ソフトウェアをインストールし、会社から貸し出すことが望ましいです。

- サポート中のOSが入っている。
- ウイルス対策ソフトウェアが入っている。
- 会社が把握している機種なので、問い合わせ対応がスムーズ。
- 不要なアプリケーションが入っていない。
- プライベートの個人情報が入っていない。
- クライアント運用管理ソフトウェアを入れて、管理できる。

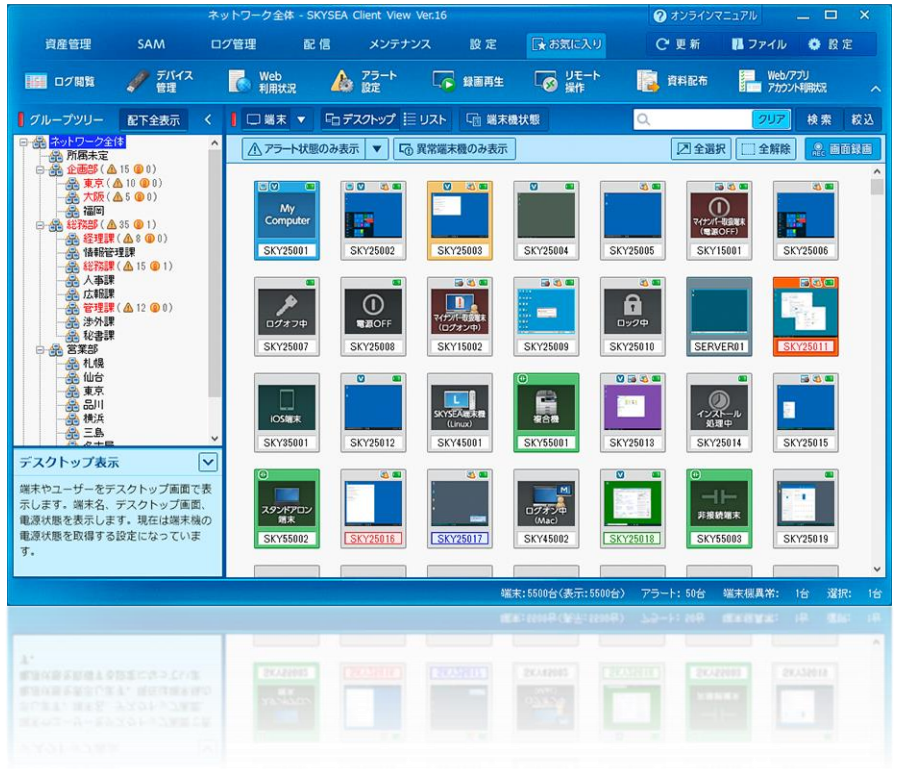
私物のPCを使うより、はるかに安全に業務を行えます

システムでできる対策は、システムで実施を

クライアント運用管理ソフトウェアがあればできること

- インストールする**アプリケーションを限定**できる。
- ルール違反の**操作を制限**したり、アラートを表示できる。
- リモートで更新プログラムの適用や**アップデート**を行える。
- **HDDの暗号化**を徹底できる。
- **業務外の作業を制限**できる。
- 万が一の際の証跡管理のため、**ログを収集**できる。
- 使用する通信を、**VPN等に制限**できる。

など



従業員の私物PCを用いて業務を行う場合

テレワークの方式によっては、私物のPCにデータを残さない仕組みを用いることで、私物PCを用いて安全に業務を行うことができます。業務で用いるシステムによっては利用できないことがあります。

1 リモートデスクトップ方式

- 私物PCにデータがない
- 自宅に高速回線が必要
- オフィスと同じ環境

2 仮想デスクトップ方式

- 私物PCにデータがない
- 自宅に高速回線が必要
- オフィスと同じ環境

3 クラウド型アプリ方式

- 私物PCにデータを保存
- 自宅に高速回線が欲しい
- クラウドのみ使用可能

4 セキュアブラウザ方式

- 私物PCにデータがない
- 自宅に高速回線が欲しい
- クラウドのみ使用可能

5 アプリケーションラッピング方式

- 私物PCにデータがない
- 自宅に高速回線が欲しい
- コンテナ対応しか使えない

6 会社PCの持ち帰り方式

- 私物PCにデータがない
- 自宅の高速回線は不要
- オフィスと同じ環境

私物PCを利用する場合

リスク例

ルールを利用者が守ることができたとしても、
ログの収集や管理を組織で行うことはできません。

OK

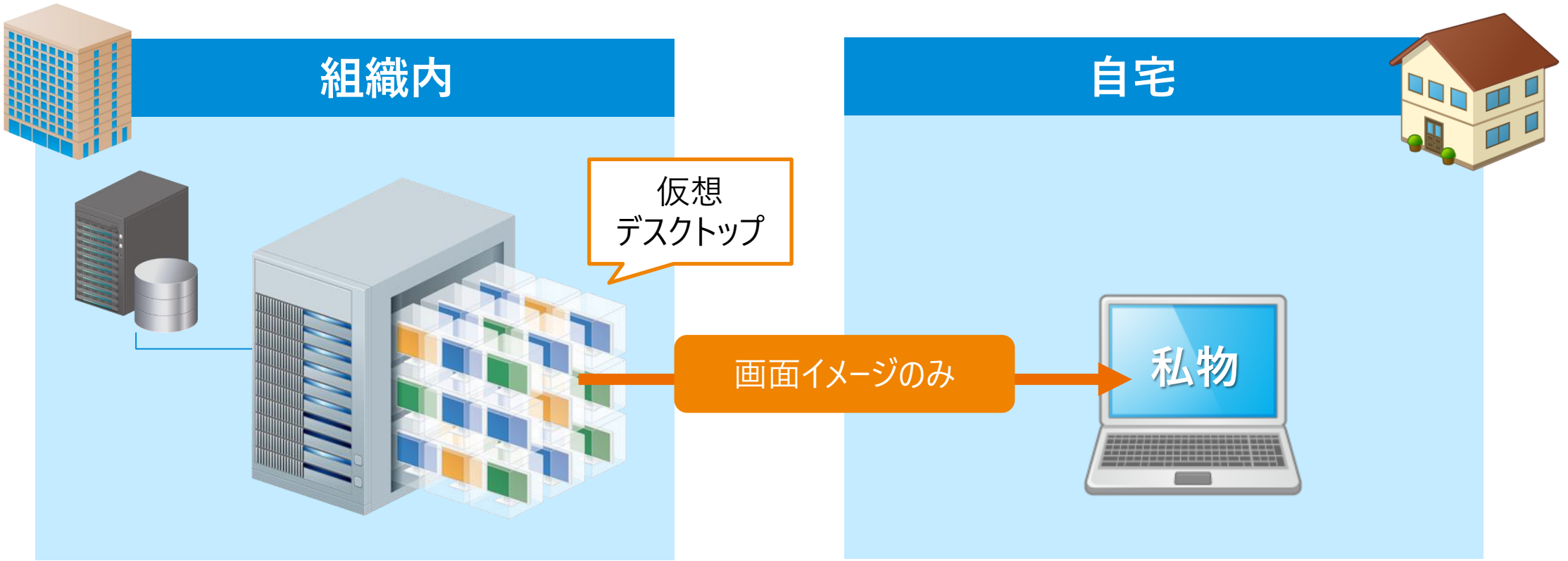
リスクを許容できる
情報資産だけで
行える業務は
私物PCで扱う

NG

リスクを許容できない
情報資産を扱う
業務はデータを
持ち出さずに行う

シンクライアントシステムなら、私物PCで安全にテレワーク

組織内に設置されたサーバー（またはクラウド）上の仮想デスクトップに、遠隔でログインして利用する方法です。
扱うデータはすべてサーバー上に保存されるため、セキュリティ面でメリットが大きい手法です。また、仮想デスクトップはWindows OSを搭載できるので、Windowsの業務システムを使うことができます。

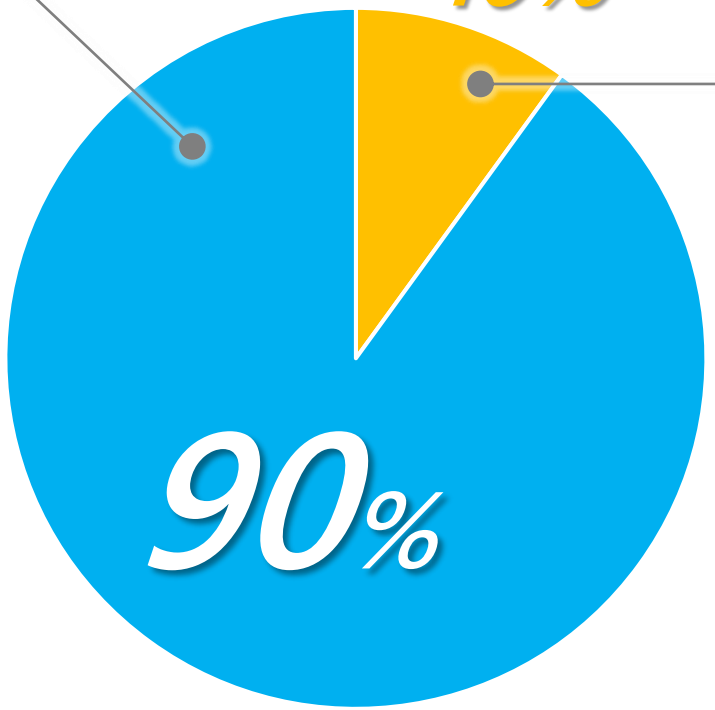


個人まかせではないPCで安全にテレワークの実現を

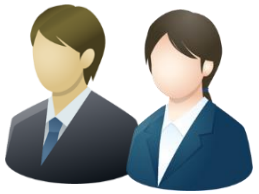
在宅勤務の増加でPCはこれまで以上に狙われています。そのため、求められる情報セキュリティ対策は、より複雑になっています。PCを組織から支給してシステムで管理したり、BYODの際にはPC内にデータを残さないようにしたりすることで、必要な情報セキュリティ対策の徹底を支援できます。

システムでカバー

- 脆弱性対策
- USBメモリの管理
- 業務システム、操作ログの収集
- HDDの暗号化の徹底
- 使用する通信をVPNに制限
- インストールするアプリケーションを限定
- エンドポイントセキュリティなどによる多層防御
- PC内のデータ非保持　など



個人の意識リテラシー



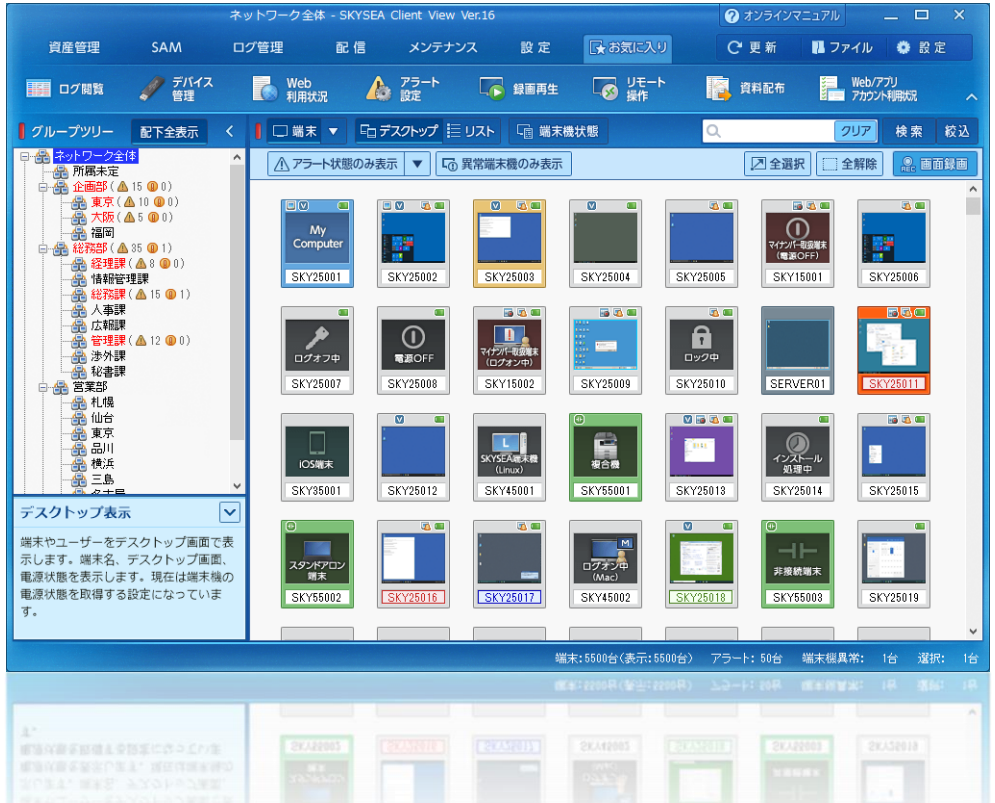
- セキュリティ研修　など

お客様のワークスタイルに合った「安全・安心」なIT活用を

組織から支給するPCの

情報漏洩対策とIT運用管理に

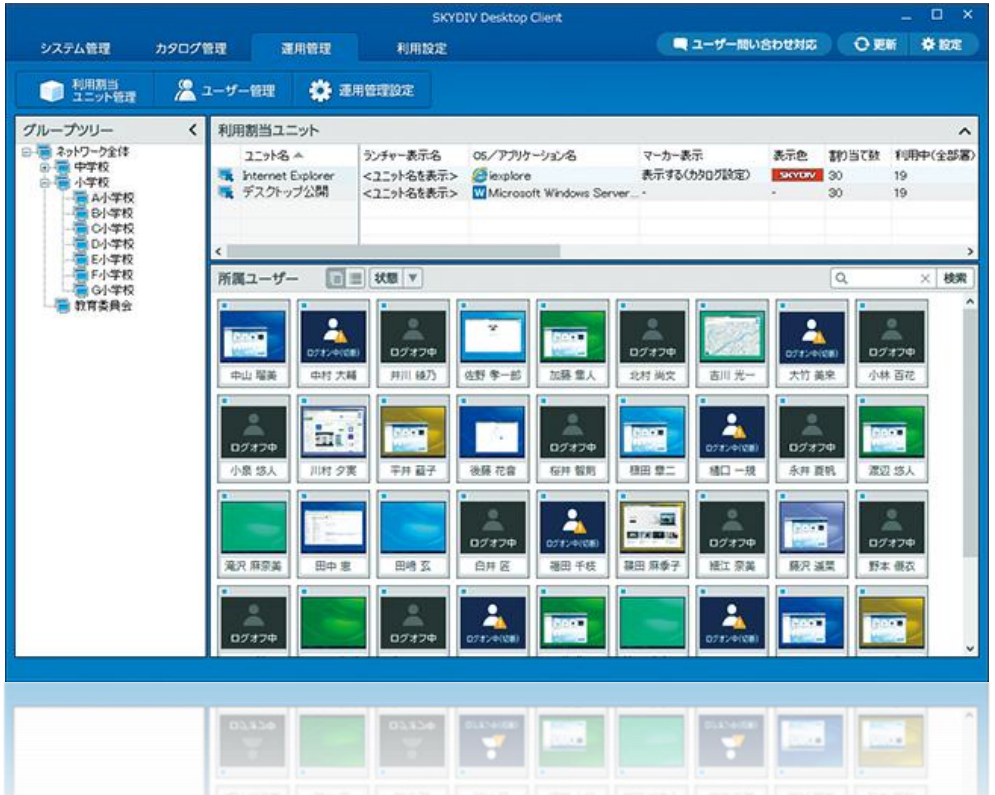
SKYSEA Client View



私物PCにデータを保存しない

安全なBYODの実現に

SKYDIV Desktop Client



ご清聴ありがとうございました

Sky株式会社　https://www.skygroup.jp/

東京本社　〒108-0075　東京都港区港南二丁目16番1号 品川イーストワンタワー15F
TEL : 03-5796-2752　FAX : 03-5796-2977

大阪本社　〒532-0003　大阪市淀川区宮原3丁目4番30号 ニッセイ新大阪ビル20F
TEL : 06-4807-6374　FAX : 06-4807-6376

札幌支社　仙台支社　横浜支社　三島支社　名古屋支社　神戸支社　広島支社
松山支社　福岡支社　沖縄支社