

令和5年度 厚生労働省主催 テレワーク・セミナー

ICT面における留意点

株式会社 テレワークマネジメント
鵜澤純子

1

CONTENTS

1.ポストコロナの
テレワークの
現状と効果

2.情報セキュリティ
インシデントの傾向

3.テレワークの実施
に必要なハードやソ
フトの選び方

4.テレワークの実施
方法に合わせた
セキュリティ対策の
ポイント

2

講師自己紹介: 鵜澤純子 (株式会社テレワークマネジメント)



総務省
地域情報化アドバイザー
テレワークマネージャー
デジタル庁 デジタル推進委員
ITコーディネータ
情報セキュリティ管理士



出産を機に最初の職場を退職し、
2002年から、個人事業主として在
宅での仕事をスタート。
2011年(株)テレワークマネジメント
入社。完全在宅勤務のマネー
ジャーとしてコンサルチームを統括。
2女の母

担当した国・地方自治体の事業:

- 2012年 福岡県テレワーク普及啓発事業
- 2013～2015年 総務省テレワーク全国展開事業
- 2017年～ 総務省地域情報化アドバイザー
- 2014～2020年 厚労省テレワークセミナー講師 (ICT分野)
- 2014～2019年 総務省テレワークセミナー講師 (ICT分野)
- 2016～2019年 総務省テレワークエキスパート講習会講師
- 2016年～ 総務省「テレワークマネージャー」
- 2017～2021年 総務省「テレワークセキュリティガイドライン検討会」構成員
- 2018年 東京都テレワーク活用推進モデル実証事業
- 2022年 千葉県「ちばの新しい働き方検討会」委員

民間企業ご支援例:

住友商事株式会社 日本たばこ産業株式会社 株式会社大塚商会
三井住友海上火災保険株式会社 三菱地所コミュニティ株式会社
株式会社ハンズ(旧東急ハンズ) 株式会社TBSテレビ 株式会社アデランス
YKKAP株式会社 他多数



1. ポストコロナのテレワークの現状と効果

今日ご参加の皆様の テレワーク実施状況を教えてください

投票

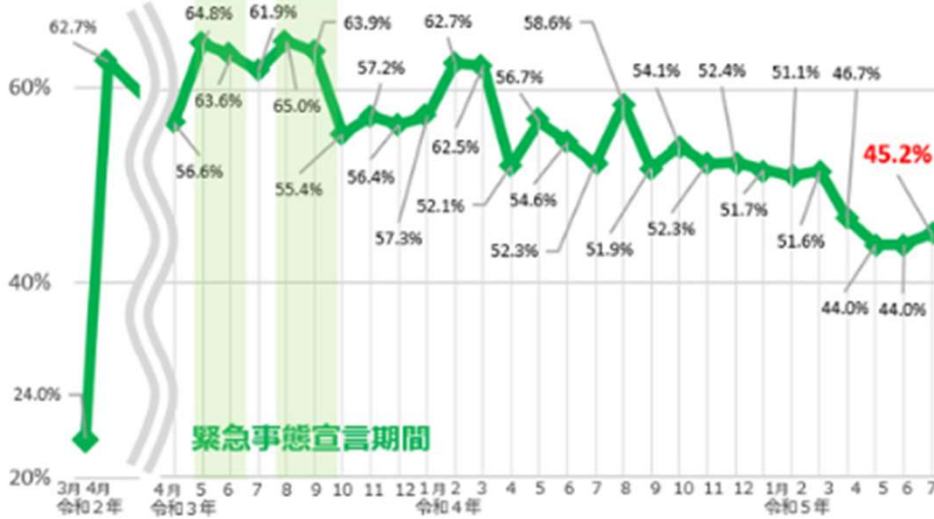
1. コロナ禍中もそれ以降もテレワークを継続して活用している
2. コロナ禍中はテレワークを実施したが、現在はあまり活用していない
3. コロナ禍中はテレワークを実施したが、今は実施していない
4. コロナ禍中も現在もテレワークは実施していない

ポストコロナのテレワークの注目ポイント

経営者と労働者のギャップ
少子化対策としてのテレワーク



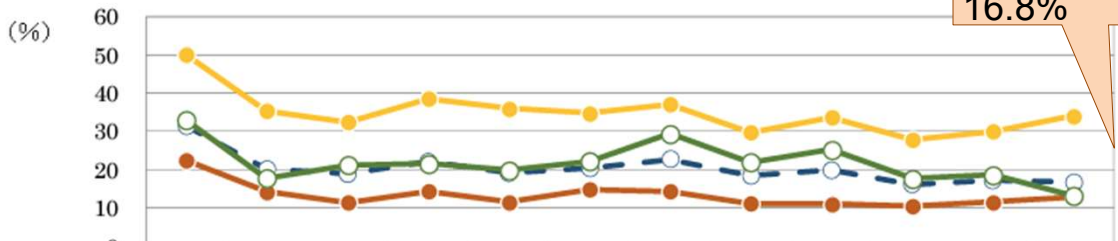
東京都内企業のテレワーク実施率(2023年7月の調査)



(出典)東京都産業労働局 テレワーク実施率調査結果
<https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2023/08/14/09.html>
 Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

全国のテレワーク実施率(2023年1月)

図36 従業員規模別・テレワークの実施率



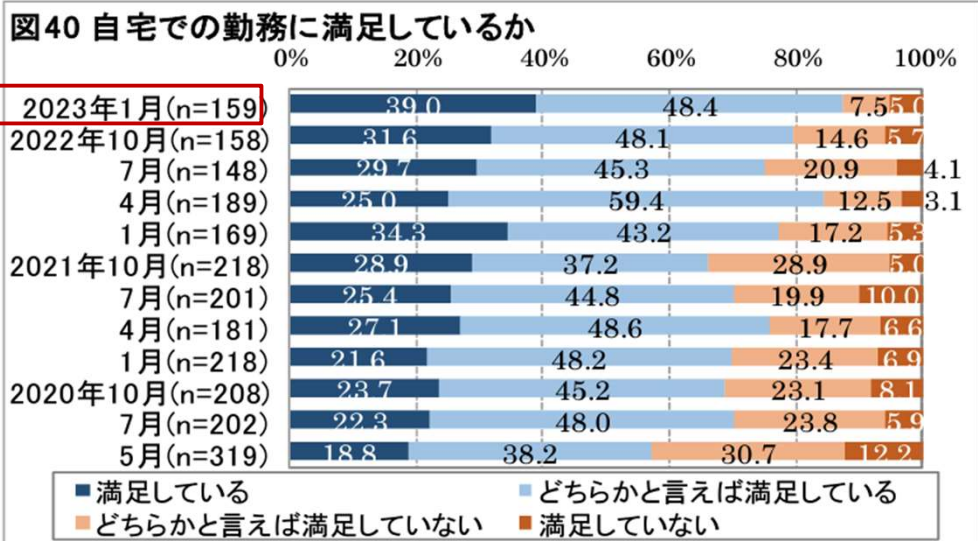
全国平均
16.8%

	2020年5月	2020年7月	2020年10月	2021年1月	2021年4月	2021年7月	2021年10月	2022年1月	2022年4月	2022年7月	2022年10月	2023年1月
全体	31.5	20.2	18.9	22.0	19.2	20.4	22.7	18.5	20.0	16.2	17.2	16.8
100名以下	22.5	14.2	11.4	14.4	11.5	14.9	14.3	11.1	11.1	10.4	11.5	12.9
101~1,000名	33.0	17.7	21.1	21.6	19.8	22.2	29.4	22.0	25.3	17.6	18.7	13.2
1,001名以上	50.0	35.4	32.4	38.6	36.0	34.7	37.1	29.8	33.7	27.9	30.0	34.0

(出典)日本生産性本部「第12回働く人の意識に関する調査」https://www.jpc-net.jp/research/assets/pdf/12th_workers_report.pdf

Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

テレワークを実施している労働者の意見



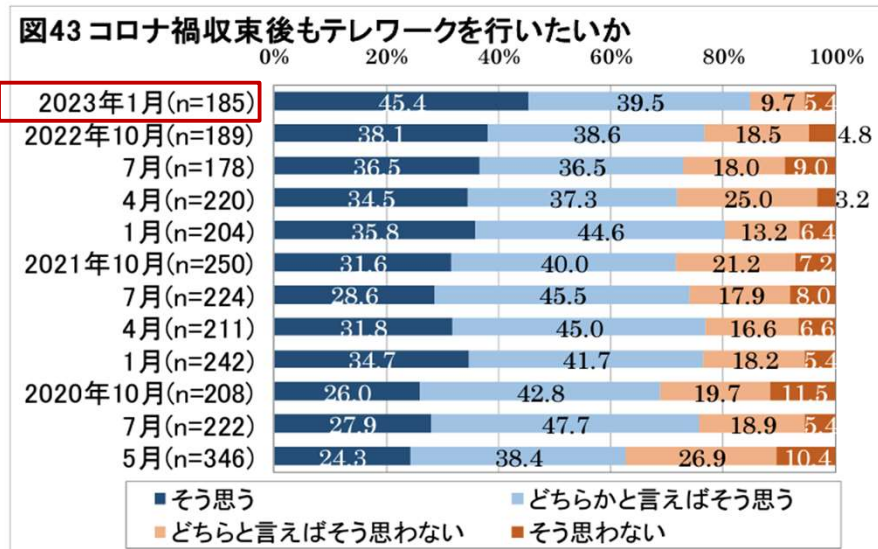
(出典)日本生産性本部「第12回働く人の意識に関する調査」https://www.jpc-net.jp/research/assets/pdf/12th_workers_report.pdf

Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

9

9

テレワークを実施している労働者の意見



(出典)日本生産性本部「第12回働く人の意識に関する調査」https://www.jpc-net.jp/research/assets/pdf/12th_workers_report.pdf

Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

10

10

企業のテレワーク実施率は 下がってきているが、 働く人はテレワークの 継続的な実施を望んでおり、 今後「ミスマッチ」が拡大する恐れも

Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

11

11

政府は「少子化対策」としてテレワークを推進

投影のみ



岸田首相、少子化対策で「テレワーク推進」表明 子が3歳未満なら「努力義務」検討

6/14(水) 16:58 配信 30

JCASTニュース
ビジネス&メディアウォッチ

「こども未来戦略方針」を発表する岸田文雄首相。子育て世代のテレワークの推進も盛り込んだ

岸田文雄首相は2023年6月13日に首相官邸で開いた記者会見で、少子化対策のための「こども未来戦略方針」を発表した。年に3兆5000億円規模を投じ、児童手当の拡充など子育て世代への給付策を多数盛り込んだ。

【画像】「加速化プラン」には3つの柱

方針では、具体的な政策を「こども・子育て支援加速化プラン」の中に列挙。育休取得率の向上やテレワークの推進など、子育て世代の働き方に関する内容も多い。

Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

12

12

制度の導入が遅れる企業は「選ばれなくなる」おそれも

投影のみ



子供3歳まで在宅勤務、企業の努力義務に 厚労省

2023/04/28

日本経済新聞



2023/04/28 10:00

少子化対策として育児の時間を増やす政策の整備が進む。厚生労働省は3歳までの子どもがいる社員がオンラインで在宅勤務できる仕組みの導入を省令で企業の努力義務とする。いまは3歳までとする残業の免除権も法改正で就学前までに延ばす。

少子化対策として育児の時間を増やす政策の整備が進む。厚生労働省は3歳までの子どもがいる社員がオンラインで在宅勤務できる仕組みの導入を省令で企業の努力義務とする。いまは3歳までとする残業の免除権も法改正で就学前までに延ばす。

育児休業後、復帰しても柔軟に働ける環境を整え、希望する数の子どもを持ちやすくする。2024年中にも育児・介護休業法や関連省令の改正を目指す。70歳までの就業機会確保を努力義務とするのと同じような扱いとし企業に行動を促す。

在宅勤務や育児休業の取得は個人の判断だが、制度の導入が遅れる企業は柔軟な働き方を希望する人から選ばれなくなるおそれがある。

育児休業の取得が広がっても復帰後に育児の時間がとれなければ、第2子・3子を持つ気持ちになりにくい。東大の山口慎太郎教授は「テレワークなどで男女がともに柔軟に働き、家事・育児を平等に分担することが少子化対策に欠かせない」と話す。

(出典) 日経新聞 <https://www.nikkei.com/article/DGZXZQOUA050250V00C23A4000000/>

Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

13

13

TELEWORK
MANAGEMENT

今後、企業にとって 「テレワーク」という働き方の選択肢を 整える必要がますます高まる

Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

14

14

働く場所の選択肢が広がれば
会社の中・外どちらにいても
安全に働ける環境づくりが必須

2. 情報セキュリティインシデントの傾向

セキュリティインシデント急増中 被害もより広範囲・より深刻に



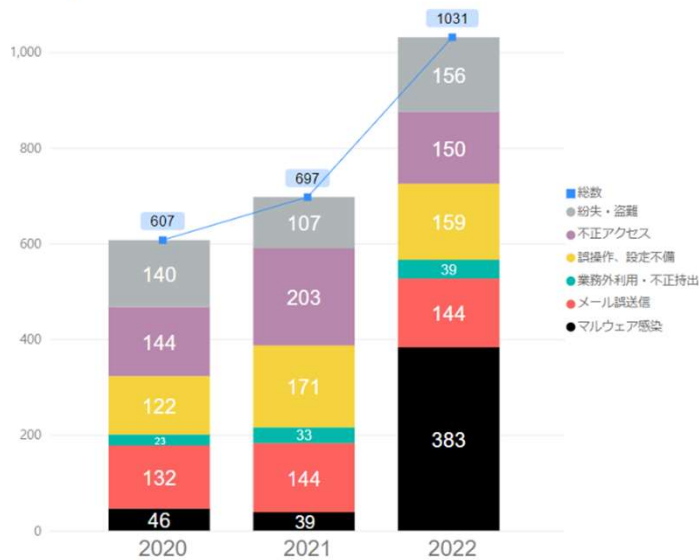
Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

17

17

2022年のセキュリティインシデント発生数は過去最高

2020～2022年国内セキュリティインシデント



(出典) デジタルアーツ プレスリリース (2023年1月)
<https://www.daj.jp/webtopics/960/>

Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

18

18

順位		前年順位
1	ランサムウェアによる被害	1
2	サプライチェーンの弱点を悪用した攻撃	3
3	標的型攻撃による機密情報の窃取	2
4	内部不正による情報漏えい	5
5	テレワーク等のニューノーマルな働き方を狙った攻撃	4
6	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	7
7	ビジネスメール詐欺による金銭被害	8
8	脆弱性対策の公開に伴う悪用増加	6
9	不注意による情報漏えい等の被害	10
10	犯罪のビジネス化(アンダーグラウンドサービス)	圏外

(出典)IPA「情報セキュリティ10大脅威 2023」 <https://www.ipa.go.jp/security/10threats/10threats2023.html>

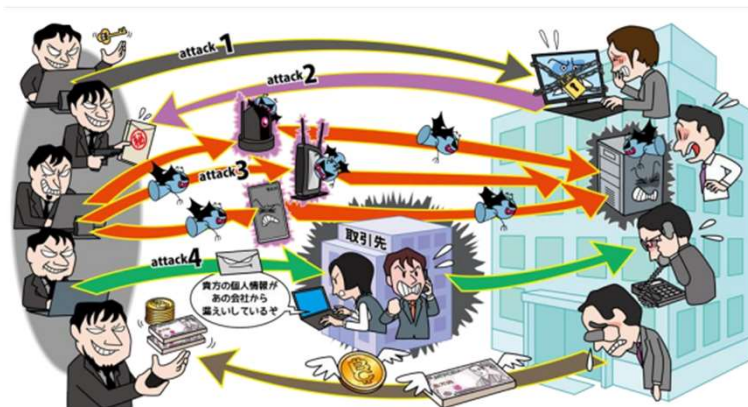
Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

19

19

第1位:ランサムウェアによる被害

攻撃手口: ウイルス(ランサムウェア)に感染させて金銭を要求



1. メールを利用した手口
・不正な添付ファイルやリンクを開かせる
2. ウェブサイトを利用した手口
・ランサムウェアをダウンロードさせるようにウェブサイトを改ざん
3. 脆弱性を悪用した手口
・ソフトウェアの脆弱性を悪用しウイルスに感染させる
4. 不正アクセスによる手口
・管理用のRDP(リモートデスクトップ)等でサーバーに不正アクセス

(出典)IPA「情報セキュリティ10大脅威 2023」 https://www.ipa.go.jp/security/10threats/ps6vr70000009r3z-att/setsume_i_2023_soshiki.pdf

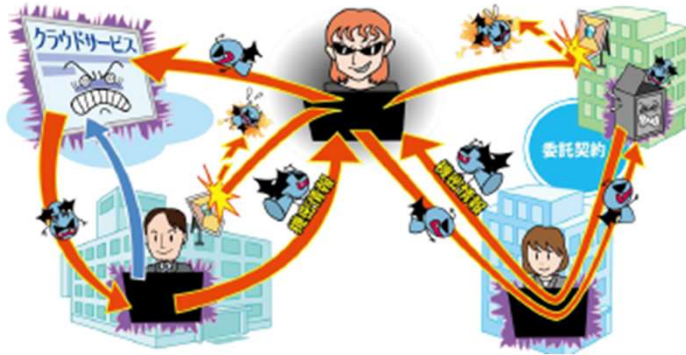
Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

20

20

第2位: サプライチェーンの弱点を悪用した攻撃

攻撃手口: サプライチェーンの中でセキュリティが脆弱な組織を狙う



1.取引先や委託先を攻撃する手口
・それらの組織が保有する、標的組織の機密情報を狙う

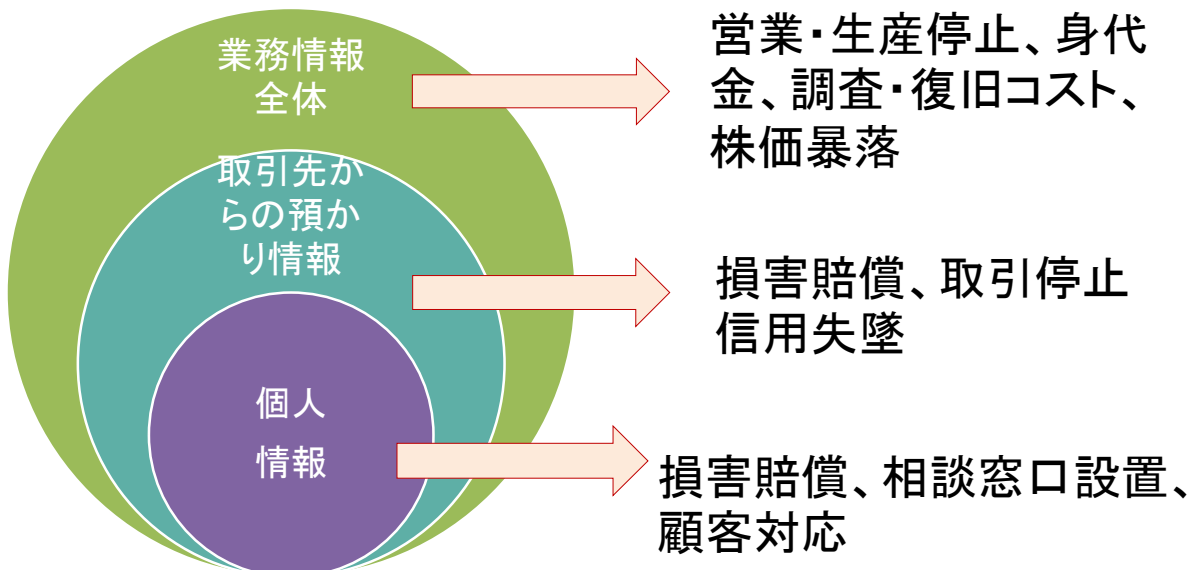
2.ソフトウェア開発元や企業のシステムの運用担当の事業者等を攻撃する手口
・標的を攻撃するための足掛かりとして標的企業のソフトウェアやICT環境に関わる組織を狙う

(出典)IPA「情報セキュリティ10大脅威 2023」 https://www.ipa.go.jp/security/10threats/ps6vr70000009r3z-att/setsumei_2023_soshiki.pdf
Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

21

21

狙われる情報も多様化し、被害額も拡大



Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

22

22

中小企業
だから・・・

テレワークはたまにしか
やっていないから・・・

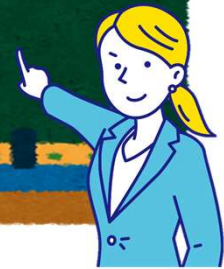
会社の中・外で**安全に働ける**環境づくりが必要

個人情報あまり持って
いないから・・・

3.テレワークの実施に必要な ハードやソフトの選び方

テレワークの主な実施方法は3つ

- ①クラウド利用
- ②VPN
- ③リモートデスクトップ

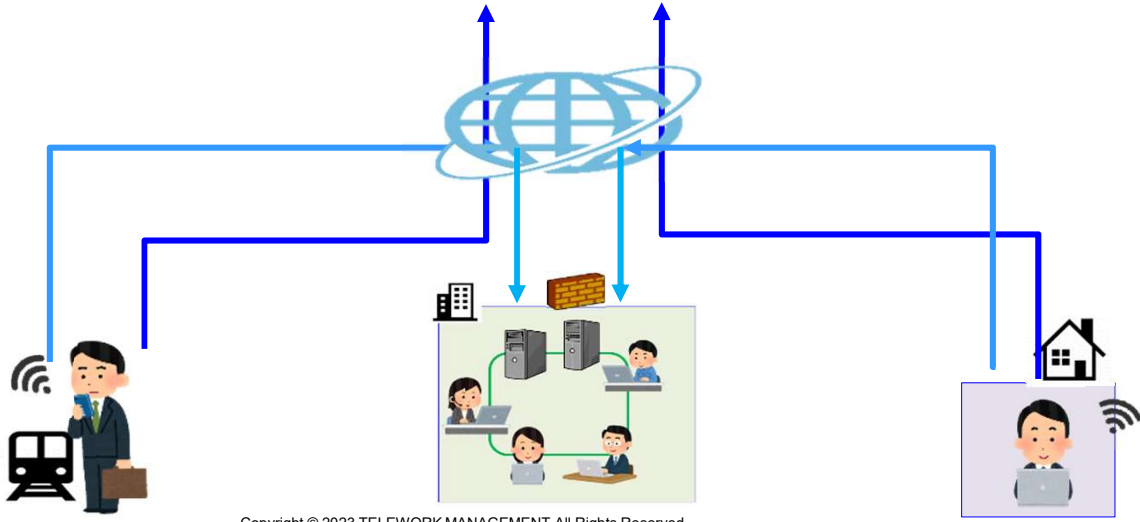


代表的な「テレワークの実施スタイル」



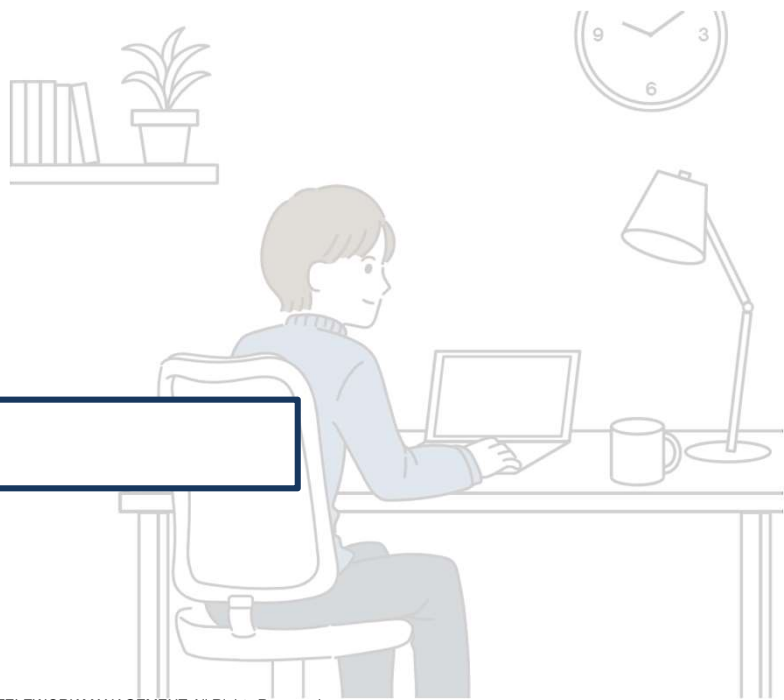
テレワークの実施スタイル

Google Workspace Microsoft 365



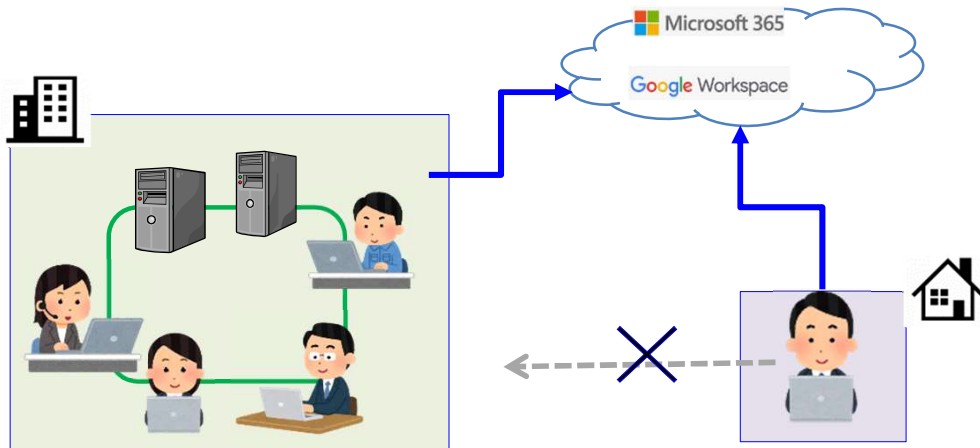
Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

クラウド利用方式



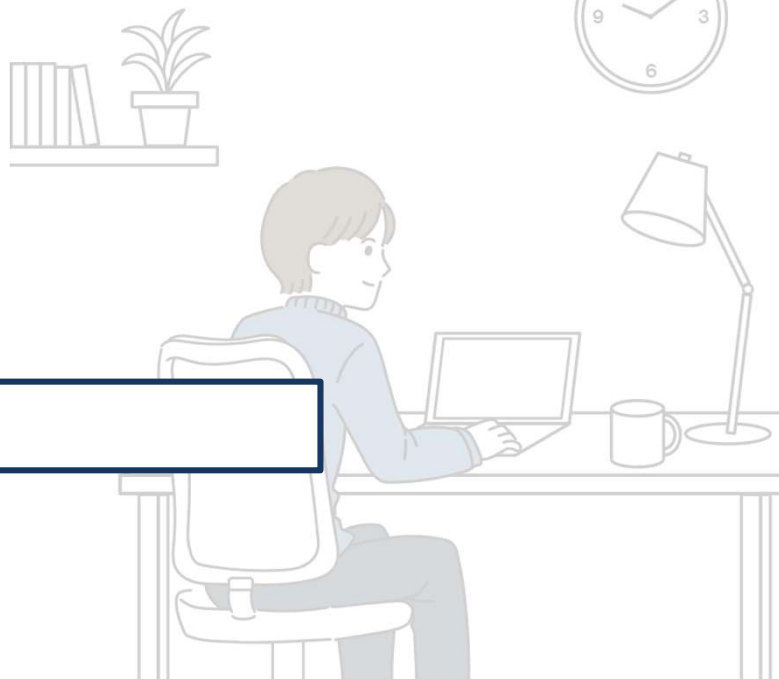
Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

クラウド利用方式の仕組み

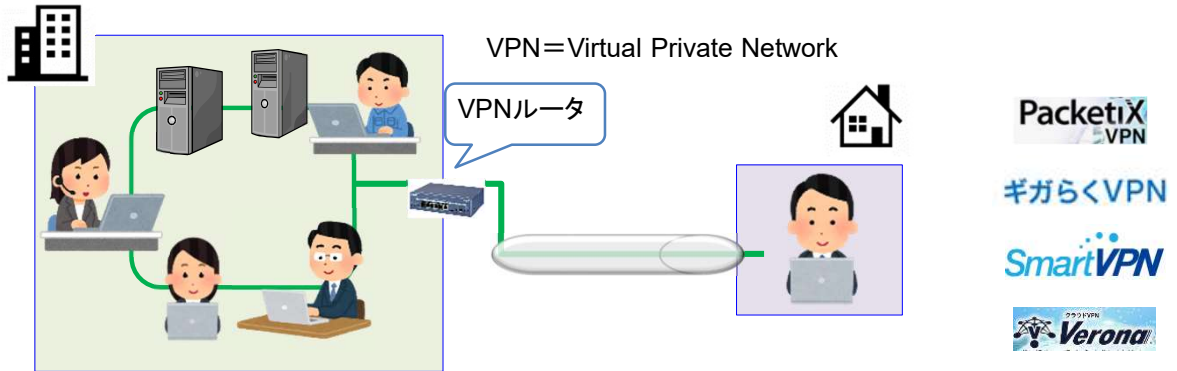


社内LANにアクセスせず、クラウドのみを利用

VPN方式



暗号化された安全な通信を使って、
社内情報にアクセスして業務



Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

31

31

リモートデスクトップ方式



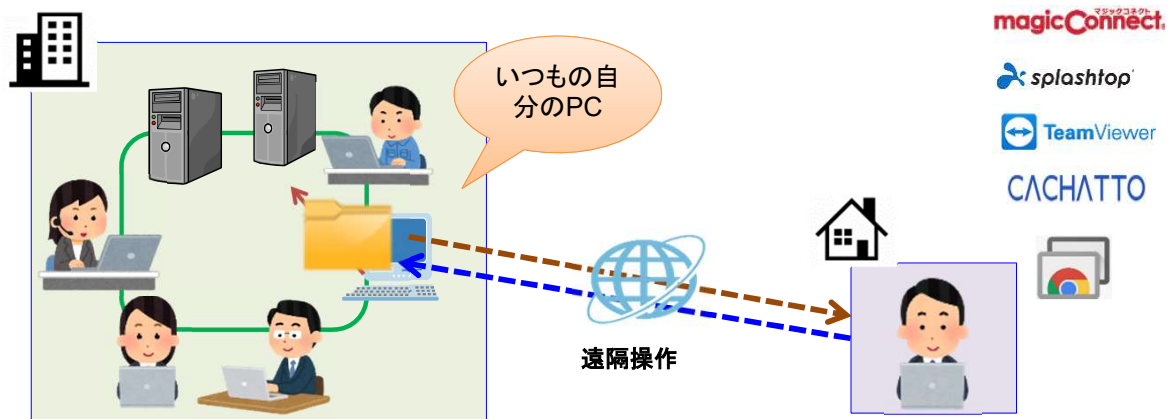
Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

32

32

リモートデスクトップ方式の仕組み

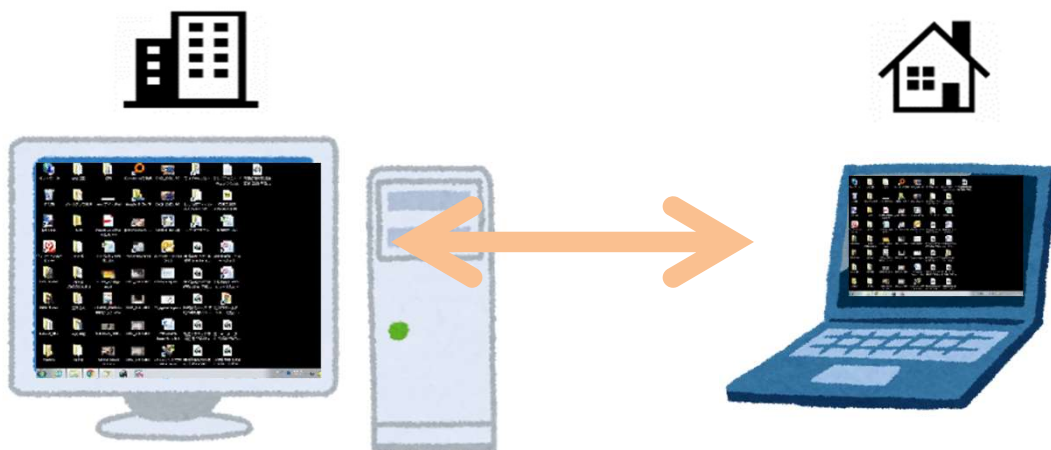
社内に置いてある、自分のPCを遠隔操作して業務



Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

33

33



いつもと同じ画面で同じ業務

Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

34

34

無償のリモートデスクトップシステム公開中

新型コロナウイルス対策実証実験
NTT東日本-IPA「シン・テレワークシステム」

2020年4月から公開で
利用者約36万人

産研協力組織で研究、開発または整備されてきた各種ソフトウェア技術や実験用専用インフラを一つに統合して、緊急に構築をしたものであり、無償かつ非営利で、一時的に提供を開始するものです。

<https://business.ntt-east.co.jp/service/thintelework-system/>



契約不要・ユーザー登録不要、無償のシンクライアント型VPNを活用しテレワークを支援する「シン・テレワークシステム」を提供を開始。当面の間提供を継続。(少なくともこの先6か月間は継続)

テレワークを実現するためのツール例

※これらはサービスの一例であり、特定の製品を推奨するものではありません。

■ 総合的なクラウドサービス

No	製品名	メーカー	価格	特徴
1	Microsoft 365	日本マイクロソフト (株)	1ユーザ 1,360円/月～	Officeやチャット、ビデオ会議のTeamsなど多様なアプリを利用可能 一人当たり2テラのストレージ容量
2	Google Workspace	グーグル合同会社	Google Workspace Business 1ユーザ 1,360円/月	Google Drive(ストレージ)、スケジュール、チャット、スプレッドシート、ビデオ会議など多様なアプリを利用可能

(出典) 日本テレワーク協会「テレワーク関連ツール一覧」
https://japan-telework.or.jp/wordpress/wp-content/uploads/2022/06/Tools_V7.0s_20220623.pdf

テレワークを実現するためのツール例



※これらはサービスの一例であり、特定の製品を推奨するものではありません。

■VPN接続ツール

No	製品名	メーカー	価格	所要導入工数	特徴
1	VPNルータ	ヤマハ(株) パッファローなど	初期導入費数万円～(NASサーバー(Network Attached Storage)は安価)	安価なシステムはユーザーによる設定が必要	初期導入費が安価 月々のサブスクリプション料金が不要の場合もある
2	PacketiX VPN	ソフトイーサ(株)	Standard Edition(小規模企業向け)95,000円～ 1年間のサポートサービスつき	ユーザーが体験版で動作検証・導入。ソフトウェアはWebからダウンロード	年間で5,500社に採用のVPN製品の最新版。高額のVPNルータ無しで、ソフトウェアでVPN接続を可能にする。
3	beat/active	富士フイルムビジネスイノベーション(株)	beat/active 初期登録 サービス60,000円/拠点 月額12,800円/拠点 設定サービス30,000円	拠点のネットワークの状況をリアルタイムで注視、その後 注文から1～2週間	複数の事業所に専用のゲートウェイ装置 (beatbox)を配置することで、メッシュ型のVPNを自動的に構築

(出典)日本テレワーク協会「テレワーク関連ツール一覧」
https://japan-telework.or.jp/wordpress/wp-content/uploads/2022/06/Tools_V7.0s_20220623.pdf

Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

37

37

テレワークを実現するためのツール例



※これらはサービスの一例であり、特定の製品を推奨するものではありません。

■リモートデスクトップツール

No	製品名	メーカー	価格	所要導入工数	特徴
1	マジックコネクト	NTTテクノクロス(株)	USB1台+タブレット 初期費用15000円 年額18000円～	約1週間	2004年のサービス開始以来トラブル停止のない実績。国内シェア1位
2	スプラッシュトップ	スプラッシュトップ(株)	初期費用0円 年額15000円～	3営業日程度	PC画面を高速に動画配信する技術を採用
3	リモートビュー	Rサポート(株)	年額12000円	3営業日	低回線速度(128BPS)からも利用可能。接続ログと統計情報を一度に確認
4	DoMobile	(株)日立ソリューションズ・クリエイト	初期費用10000円+1000円×ユーザー数 年額18000円	3営業日	強固なセキュリティに加えて導入の容易さを兼ね備えている。

(出典)日本テレワーク協会「テレワーク関連ツール一覧」
https://japan-telework.or.jp/wordpress/wp-content/uploads/2022/06/Tools_V7.0s_20220623.pdf

Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

38

38

3.テレワークの実施方法に合わせた セキュリティ対策のポイント

Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

39

39

セキュリティ対策を進める上で知っておきたい注目ポイント

TELEWORK
MANAGEMENT

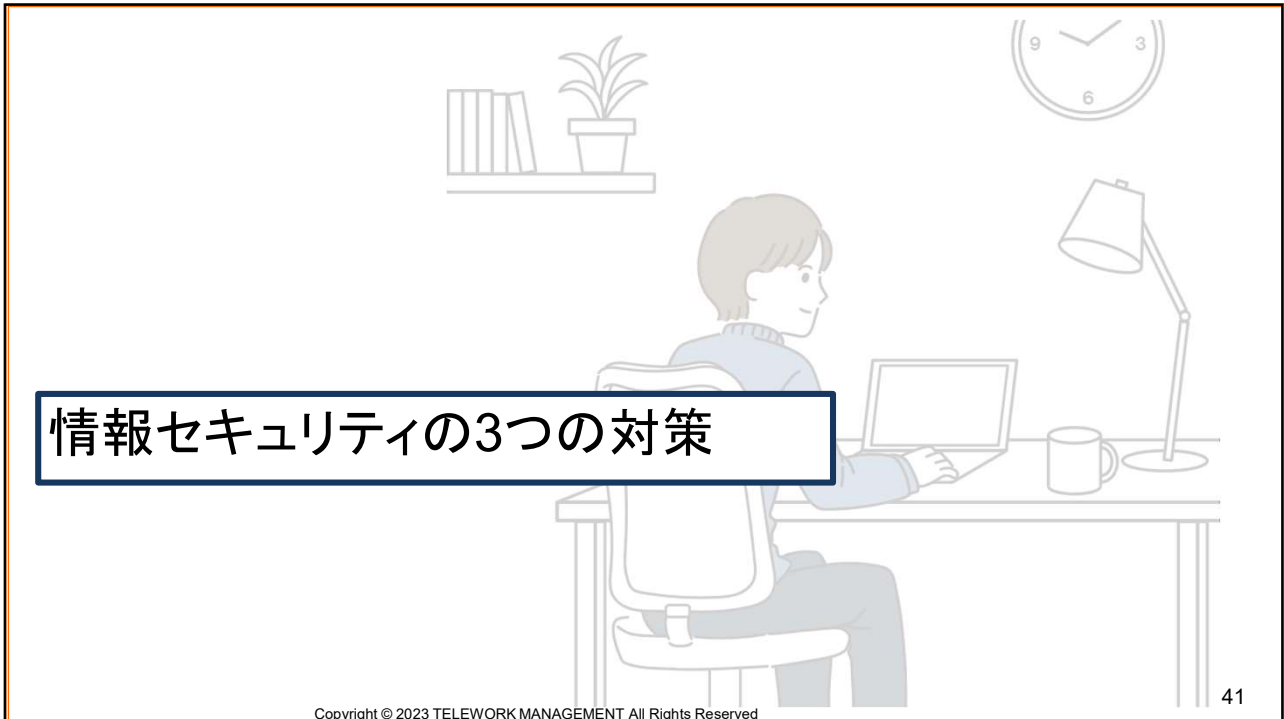
「組織的・人的対策」はIPAを活用
「技術的・物理的対策」に使える
パッケージソフトに注目



Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

40

40



41



42

組織的・人的対策

Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

43

43

組織的・人的対策に役立つ資料1

TELEWORK
MANAGEMENT



(2023年5月改訂)

<https://www.ipa.go.jp/security/guide/sme/about.html>

Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

44

44

目次

はじめに	2
1. 経営者の皆様へ	2
2. 本ガイドラインの対象	3
3. 本ガイドラインの全体構成	3
4. 本ガイドラインの活用方法	4
第1部 経営者編	5
1. 情報セキュリティ対策を怠ることで企業が被る不利益	6
2. 経営者が負う責任	8
3. 経営者は何をやらなければならないのか	12
第2部 実践編	17
1. 実践編の進め方	18
2. できるところから始める	19
3. 組織的な取り組みを開始する	20
4. 本格的に取り組む	24
5. より強固にするための方策	32
情報セキュリティに関する参考情報	65
本書で用いている主な用語の説明	66

組織的・人的対策に役立つ資料2

情報セキュリティ 5か条

「5か条」は情報セキュリティの基本原則です。

1. 重要データのバックアップ、復旧、保護を徹底する

2. 重要データの複製を厳格に管理する

3. 重要データのアクセス権を厳格に管理する

4. 重要データの廃棄を厳格に管理する

5. 重要データの流出防止を徹底する

情報セキュリティ関連規程(サンプル)

目次	ページ
1. 目的	1
2. 用語の定義	2
3. 管理体制	3
4. 基本方針	4
5. 基本原則	5
6. 重要データの保護	6
7. 重要データの複製	7
8. 重要データのアクセス	8
9. 重要データの廃棄	9
10. 重要データの流出防止	10
11. 関係者への啓発	11
12. その他	12

5分でできる! 情報セキュリティ自社診断

最新動向への対応、できていますか?

脅威や攻撃の変化 | IT環境の変化

「5分でできる! 自社診断」でチェック!

情報セキュリティハンドブック

このハンドブック(5巻)は、中小企業・小規模事業者向けに、情報セキュリティの基礎から応用まで、わかりやすく解説しています。

1. 全社共通のルール | 1ページ
2. 仕事のルール | 3ページ
3. 会社共通のルール | 8ページ
4. テレワークのルール | 12ページ

株式会社〇〇〇〇

情報セキュリティ基本方針(サンプル)

本方針は、本社の業務活動において、情報セキュリティを確保するための基本となる方針を定める。本方針は、全従業員に適用される。本方針は、本社の業務活動において、情報セキュリティを確保するための基本となる方針を定める。本方針は、全従業員に適用される。

情報セキュリティ基本方針(サンプル)

目次	ページ
1. 目的	1
2. 用語の定義	2
3. 管理体制	3
4. 基本方針	4
5. 基本原則	5
6. 重要データの保護	6
7. 重要データの複製	7
8. 重要データのアクセス	8
9. 重要データの廃棄	9
10. 重要データの流出防止	10
11. 関係者への啓発	11
12. その他	12

中小企業のためのクラウドサービス安全利用の手引き

クラウドサービスの安全利用、できていますか?

取り返しのつかないことになる前にクラウドサービス安全利用チェックシートで確認!

中小企業のためのセキュリティインシデント対応の手引き

情報漏えい? ウイルス感染? システム障害? どうしたらいいの?!

Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

中小企業・小規模事業者の皆様へ

新 5分でできる! 情報セキュリティ自社診断

最新動向への対応、できていますか?

脅威や攻撃の変化

- 標的型攻撃
- ランサムウェア
- パスワードリスト攻撃
- ビジネスメール詐欺

IT環境の変化

- IoT機器
- クラウド
- スマートフォン
- テレワーク

取り返しのつかないことになる前にあなたの会社のセキュリティ状況を「5分でできる! 自社診断」でチェック!

診断編

診断項目 No.	診断内容	チェック
Part 1 脅威や攻撃の変化への対応	1. パソコンやスマホなどの情報機器の OS やソフトウェアは常に最新の状態で更新されていますか?	A 2 0 -1
	2. パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイルが最新の状態に更新されていますか?	A 2 0 -1
	3. 重要情報に対する適切なアクセス制御を行っていますか?	A 2 0 -1
	4. 新たな脅威や攻撃の手段を知り、対策を社内共有する仕組みはできていますか?	A 2 0 -1
Part 2 IT環境の変化への対応	5. 電子メールの添付ファイルや本文中の URL、リンクを介したウイルス感染に気づいて対応していますか?	A 2 0 -1
	6. 電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか?	A 2 0 -1
	7. 重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか?	A 2 0 -1
	8. 無線 LAN を安全に使うための適切なセキュリティ対策を実施していますか?	A 2 0 -1
Part 3 関係者への啓発	9. インターネットを介したウイルス感染や SNS の書き込みなどのトラブルへの対応はできていますか?	A 2 0 -1
	10. パソコンやサーバーのウイルス感染、盗難や紛失による重要情報の漏えい防止に気を付けていますか?	A 2 0 -1
	11. 紛失や盗難を防ぐため、重要情報が記載された書類や電子媒体は引取りや廃棄など、適切な対応をしていますか?	A 2 0 -1
	12. 重要情報が記載された書類や電子媒体を廃棄する際は、適切な廃棄方法を実施していますか?	A 2 0 -1
Part 4 関係者への啓発	13. 関係者へのセキュリティに関する教育や注意喚起を行っていますか?	A 2 0 -1
	14. 関係者へのセキュリティに関する教育や注意喚起を行っていますか?	A 2 0 -1
	15. 関係者へのセキュリティに関する教育や注意喚起を行っていますか?	A 2 0 -1
	16. 関係者へのセキュリティに関する教育や注意喚起を行っていますか?	A 2 0 -1
Part 5 関係者への啓発	17. 関係者へのセキュリティに関する教育や注意喚起を行っていますか?	A 2 0 -1
	18. 関係者へのセキュリティに関する教育や注意喚起を行っていますか?	A 2 0 -1
	19. 関係者へのセキュリティに関する教育や注意喚起を行っていますか?	A 2 0 -1
	20. 関係者へのセキュリティに関する教育や注意喚起を行っていますか?	A 2 0 -1

診断後は次ページ以降を読んで対策を検討してください。

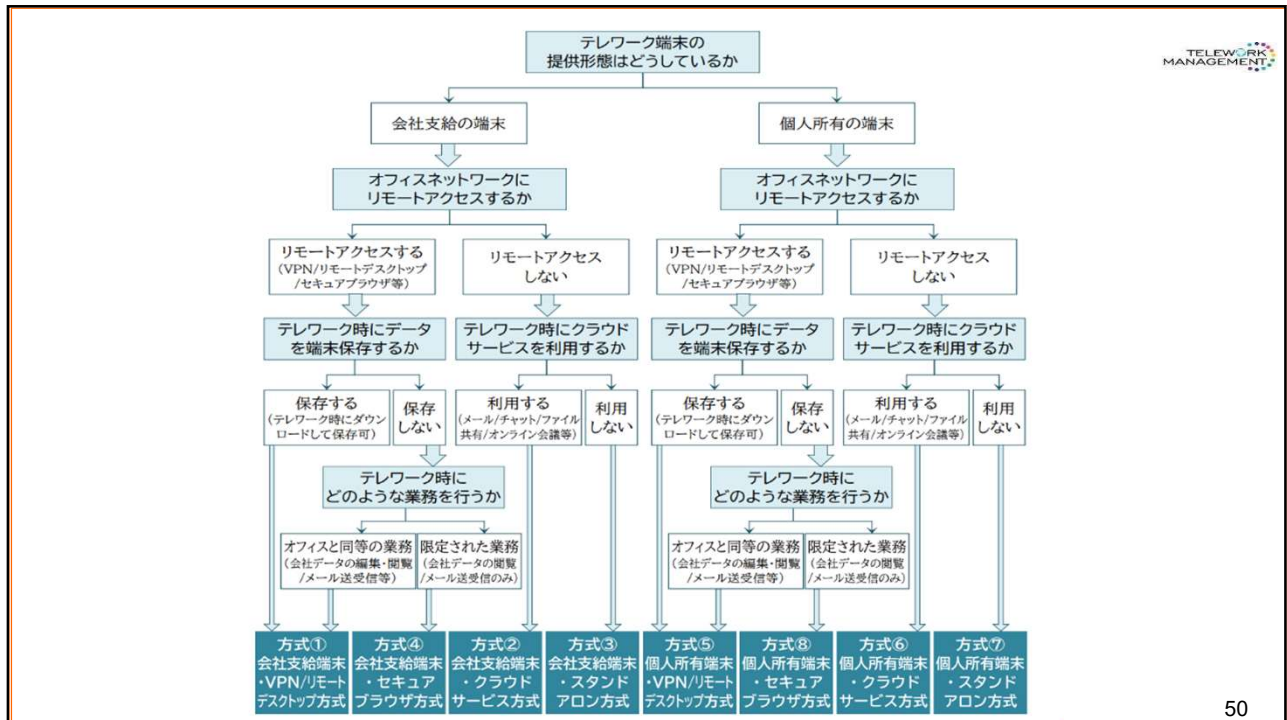
Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

「テレワークセキュリティ
ガイドライン(第5版)」

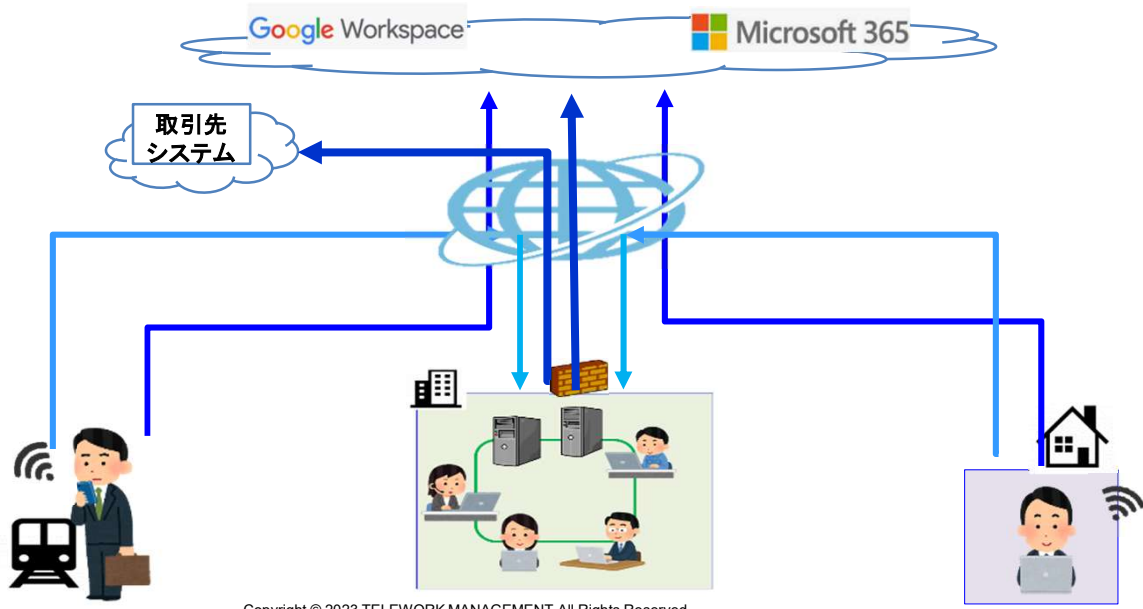
「中小企業等担当者向け
テレワークセキュリティの
手引き(チェックリスト)」



https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

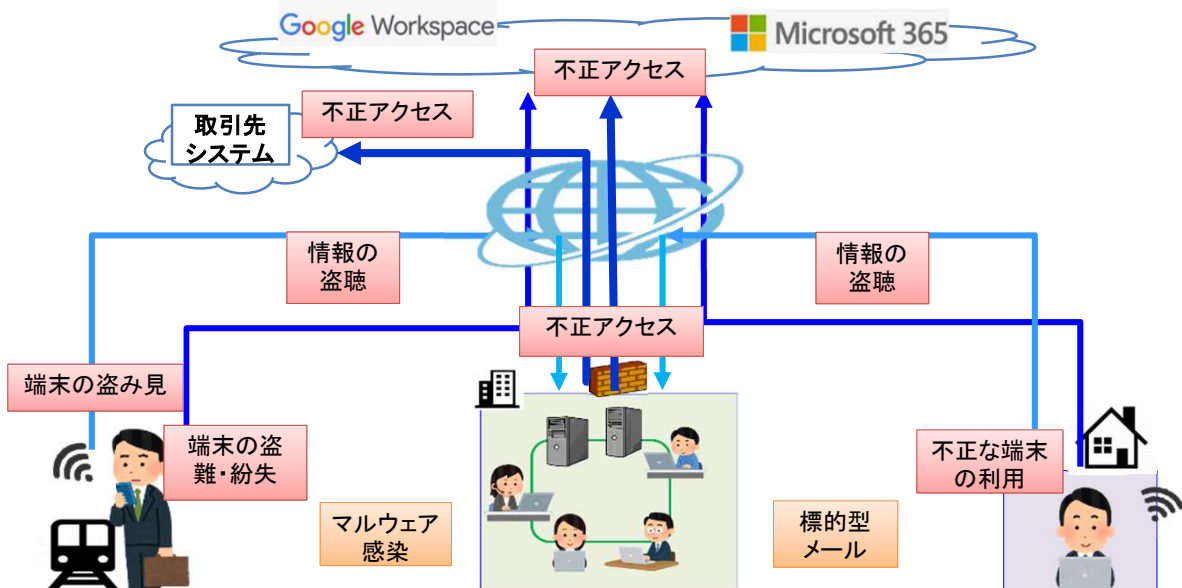


テレワークを含む働き方



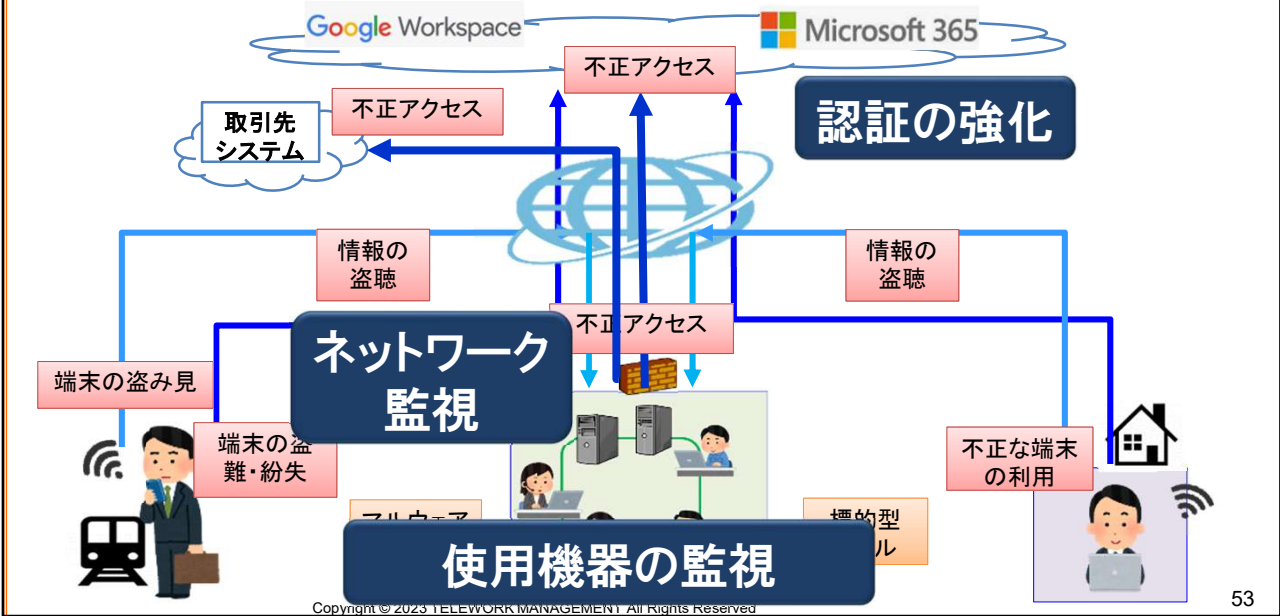
Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

情報セキュリティリスク



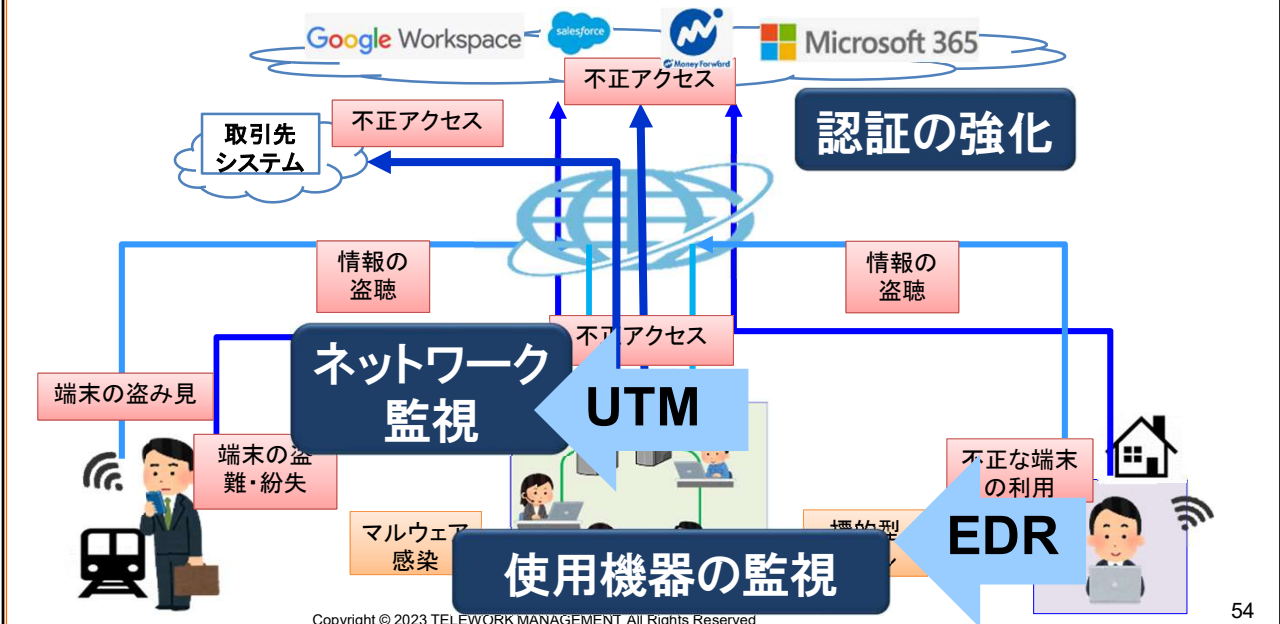
Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

情報セキュリティリスクへの対策



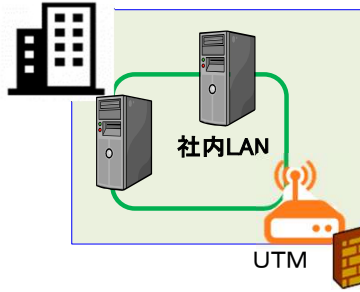
Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

ネットワークや端末を監視するサービスが対象

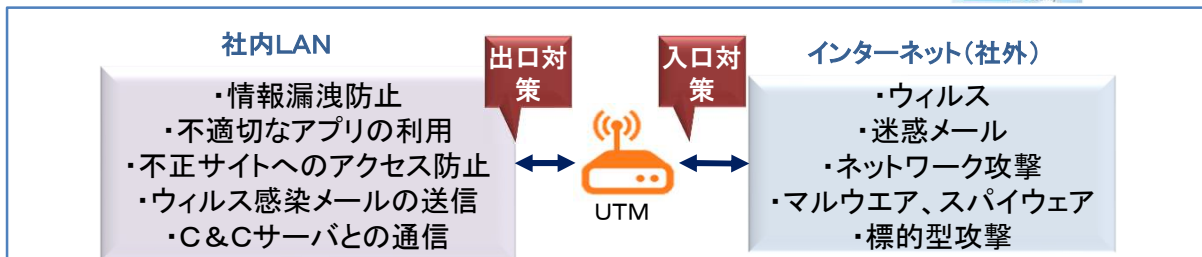


Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

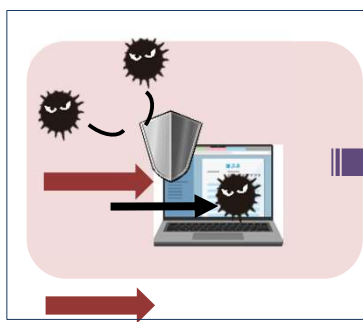
UTMとは？



UTM (Unified Threat Management=統合脅威管理) とは、複数の異なるセキュリティ機能を一つのハードウェアに統合し、集中的にネットワーク管理を行う機器



EDRとは？



EPP

EPPとは「Endpoint Protection Platform」の略で、端末のマルウェア感染防止を目的としたセキュリティツールソフト。



EDR

EDRとは「Endpoint Detection and Response」の略で、各端末の操作状況や通信内容を監視し、異常を検知するソフト。サイバー攻撃による侵入は防げないという考え方を前提として、侵入後の速やかな対応で被害を最小限に抑えるためのもの。



技術的・物理的対策例(ネットワーク・端末監視)

IPAが認定した事業者によるパッケージサービスを紹介

「サイバーセキュリティお助け隊」

<https://www.ipa.go.jp/security/otasuketai-pr/>



OTASUKETAI

手遅れになるまえに、手を打つ。

サイバーセキュリティお助け隊

サイバーセキュリティ問題、起こる前に考えよう！

見守り (異常の監視) 24時間365日監視 挙動や問題のある攻撃を検知しあなたのPCとネットワークを守ります。	駆付け 問題が発生したときに、地域のIT事業者等が駆付け対応します。(リモート支援の場合あり)	保険 簡易サイバー保険で、駆付け支援等インシデント対応時に突発的に発生する各種コストが補償されます。
--	---	--

ワンパッケージで安価に！

Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

57

57

技術的・物理的対策例(端末・ネットワーク監視)

「サイバーセキュリティお助け隊サービス」は経産省「IT導入補助金」の「セキュリティ対策推進枠」の対象

IT導入補助金2023

令和4年度第二次補正サービス等生産性向上IT導入支援事業

セキュリティ対策推進枠

サイバーインシデントを防止するセキュリティ対策強化支援。

補助額
サービス利用料の1/2以内
5万円以上100万円以下



<https://it-shien.smrj.go.jp/>

ITツールの導入費用及び、サービス利用料(最大2年分)

独立行政法人情報処理推進機構(IPA)が公表する「サイバーセキュリティお助け隊サービスリスト」に掲載されているサービスをメインのITツールとした申請(「サイバーセキュリティお助け隊サービス」単品での申請)を行うことができます。

[サイバーセキュリティお助け隊サービスリストはこちら](#)

<申請締切は10/30>

Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved

58

58

テレワークは、
人材不足や業務効率の改善など、
様々な企業課題の解決に
つながる働き方

テレワークを
安全に行うための環境づくりは、
クラウドサービス等を活用すれば
大きな投資をしなくても可能

「子育て中の社員の両立支援」
「台風による交通機関の混乱回避」等
目の前の課題解決の一步として、
テレワークを積極的に
導入・活用してみてください

ご清聴いただきありがとうございました。