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

2

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

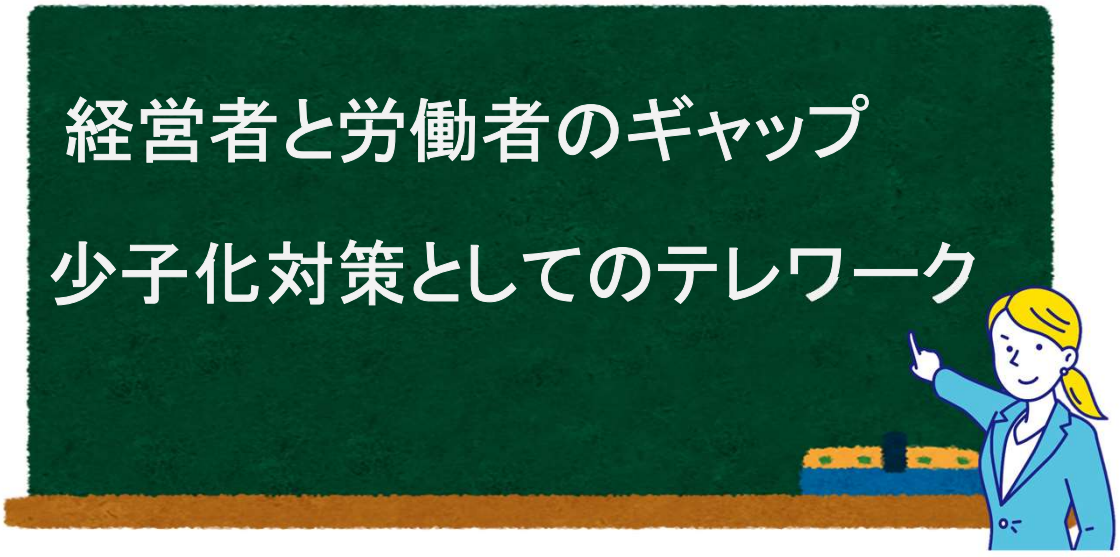
今日ご参加の皆様の
テレワーク実施状況を教えてください

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

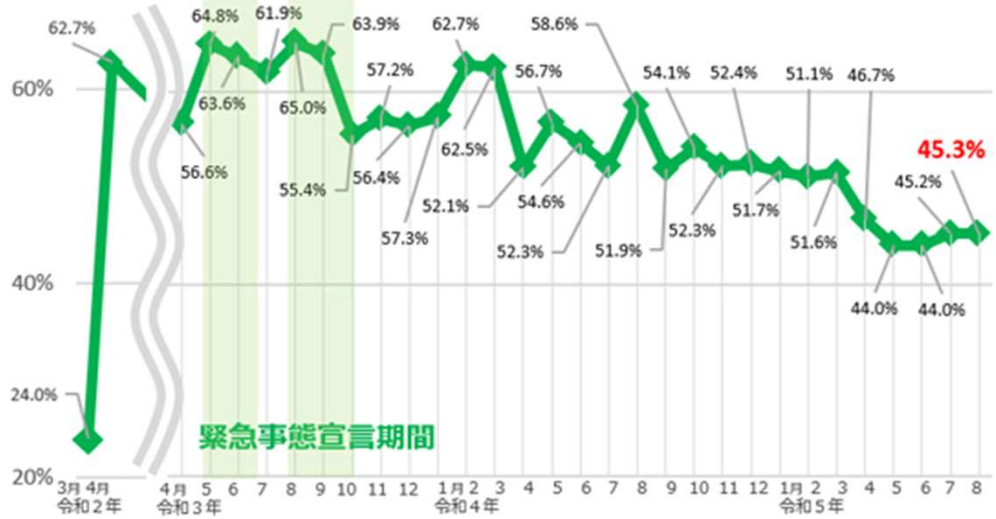
5

ポストコロナのテレワークの注目ポイント



6

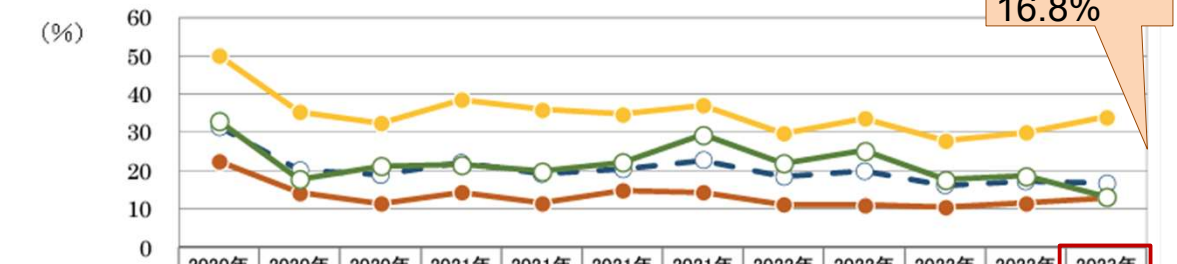
東京都内企業のテレワーク実施率（2023年8月の調査）



(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/2023/09/12/06.html

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

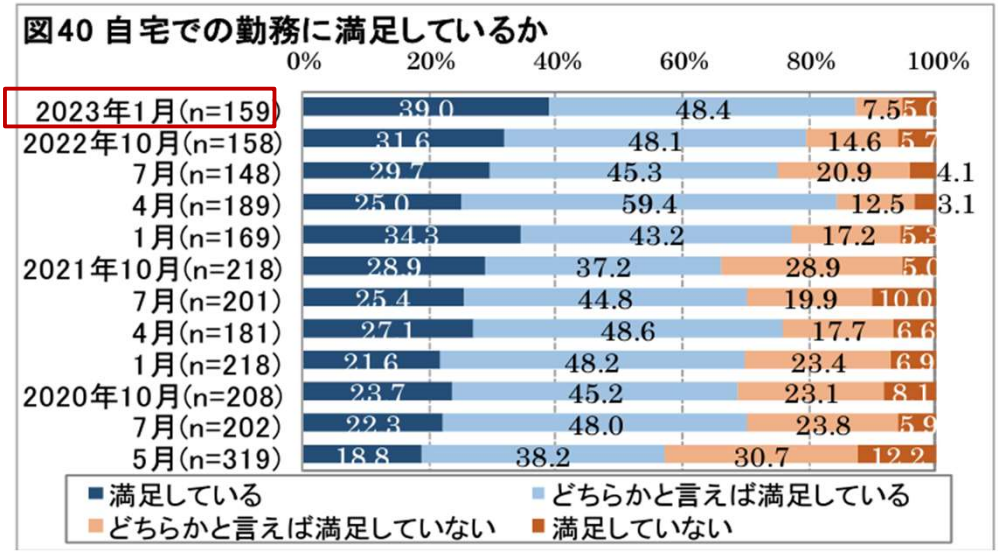


全国平均
16.8%

	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

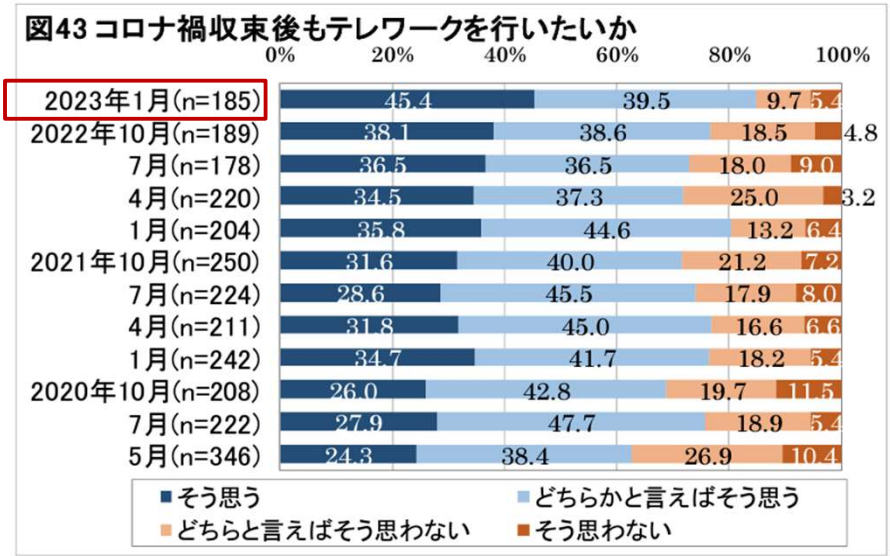
（出典）日本生産性本部「第 12 回 働く人の意識に関する調査 」https://www.jpc-net.jp/research/assets/pdf/12th_workers_report.pdf

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

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

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

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係する内容も多い。

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

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。

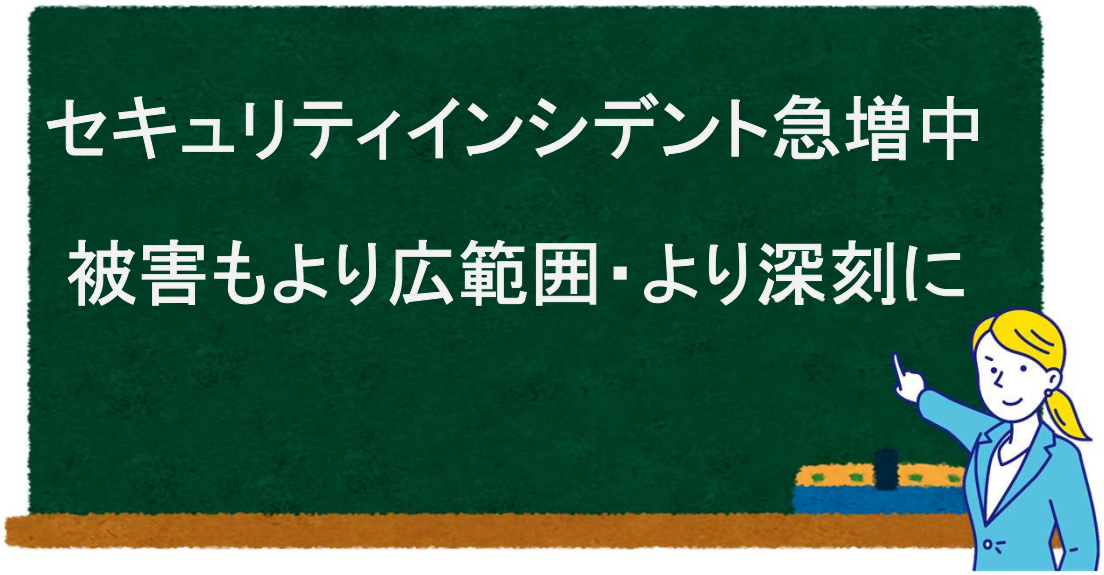
（出典）日経新聞　https://www.nikkei.com/article/DGXZQOUA050250V00C23A4000000/

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

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

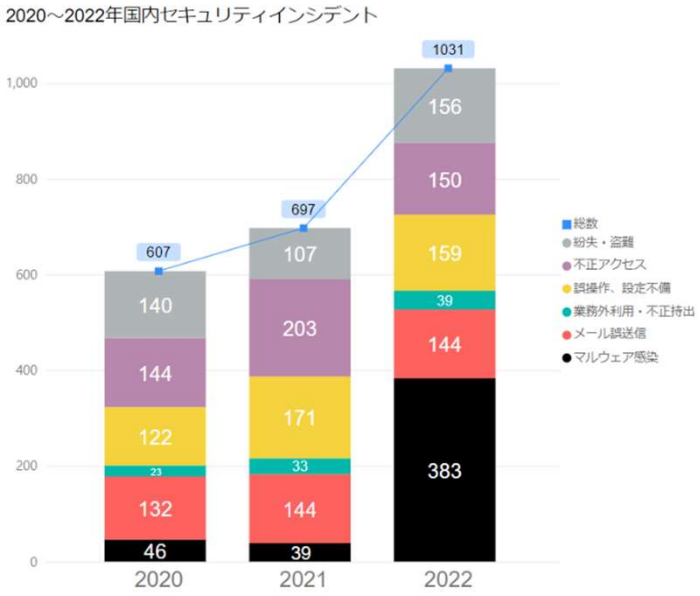
最近の情報セキュリティインシデントの注目ポイント



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



（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/

18

18

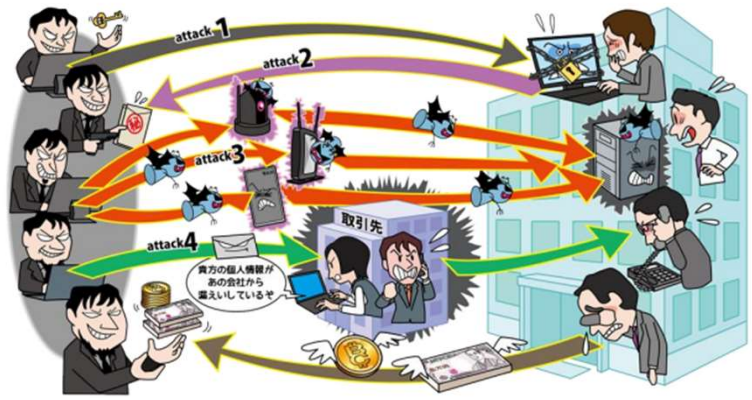
IPA(情報処理推進機構)発表「情報セキュリティ10大脅威 2023」(組織向け)

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

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

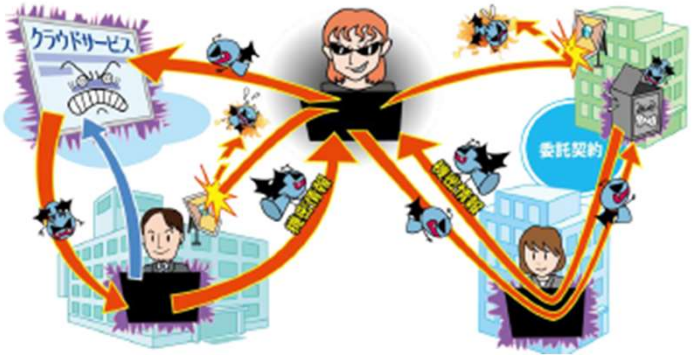
3. 脆弱性を悪用した手口
・ソフトウェアの脆弱性を悪用しウイルスに感染させる

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/setsumei_2023_soshiki.pdf

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

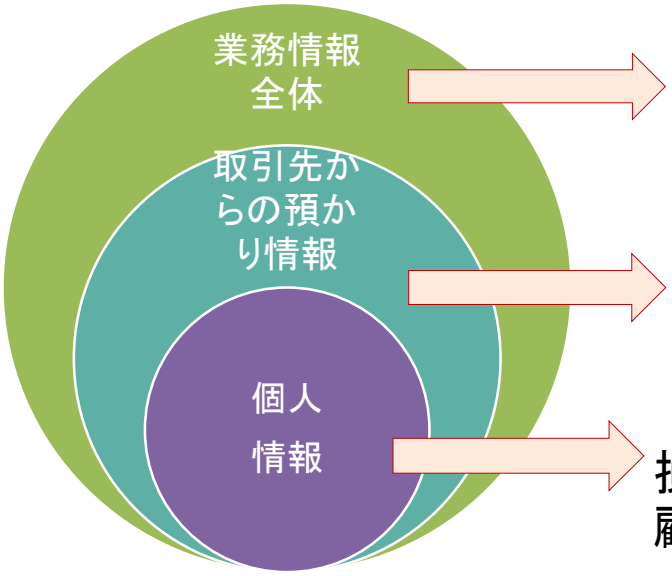


1.**取引先や委託先を攻撃する手口**
・それらの組織が保有する、標的組織の機密情報を狙う

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

狙われる情報も多様化し、被害額も拡大



営業・生産停止、身代金、調査・復旧コスト、株価暴落

損害賠償、取引停止
信用失墜

損害賠償、相談窓口設置、顧客対応

安全にテレワークができる環境づくりが大切

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

個人情報はあまり持って
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3つ

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

25

25

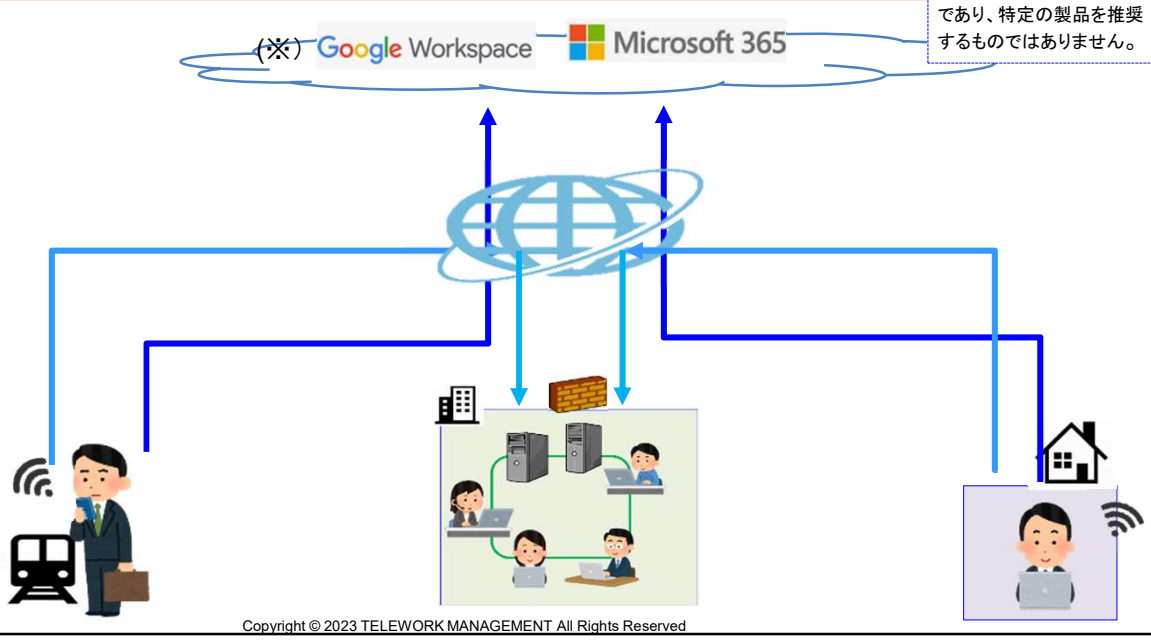
代表的な「テレワークの実施スタイル」

26

26

テレワークの実施スタイル

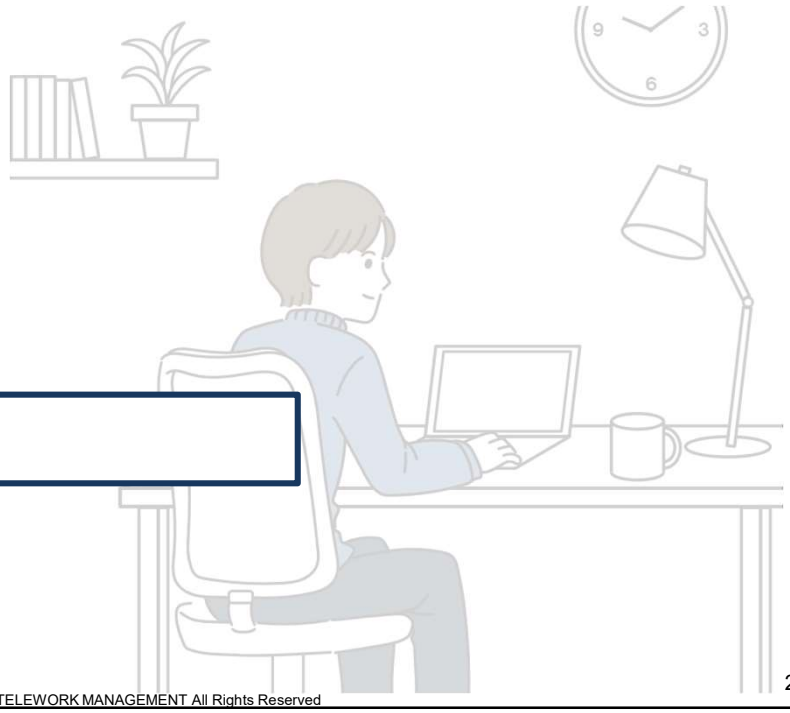
※これらはサービスの一例であり、特定の製品を推奨するものではありません。



27

27

クラウド利用方式

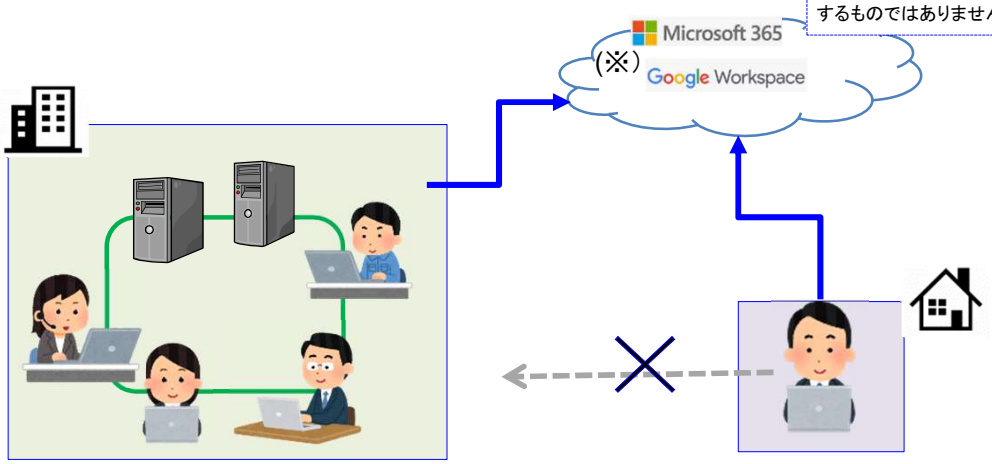


28

28

クラウド利用方式の仕組み

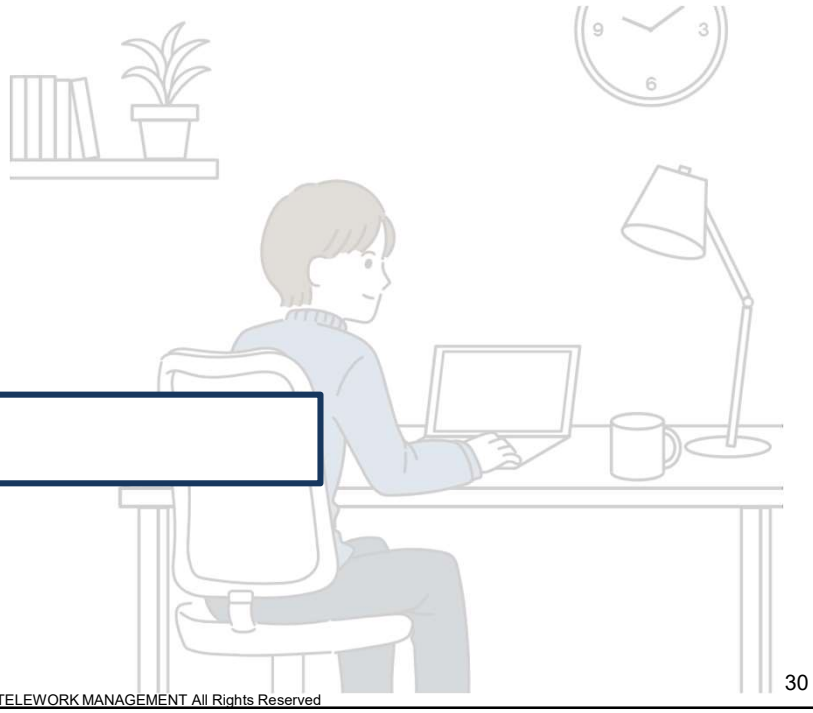
※これらはサービスの一例であり、特定の製品を推奨するものではありません。



社内LANにアクセスせず、クラウドのみを利用

29

29



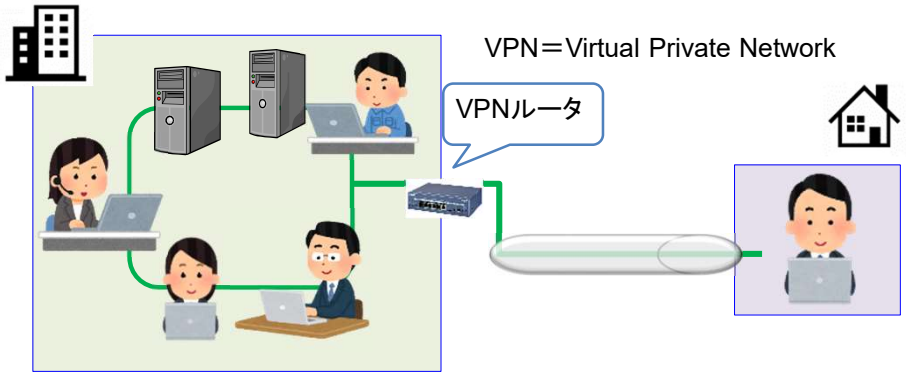
VPN方式

30

30

VPN接続方式の仕組み

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



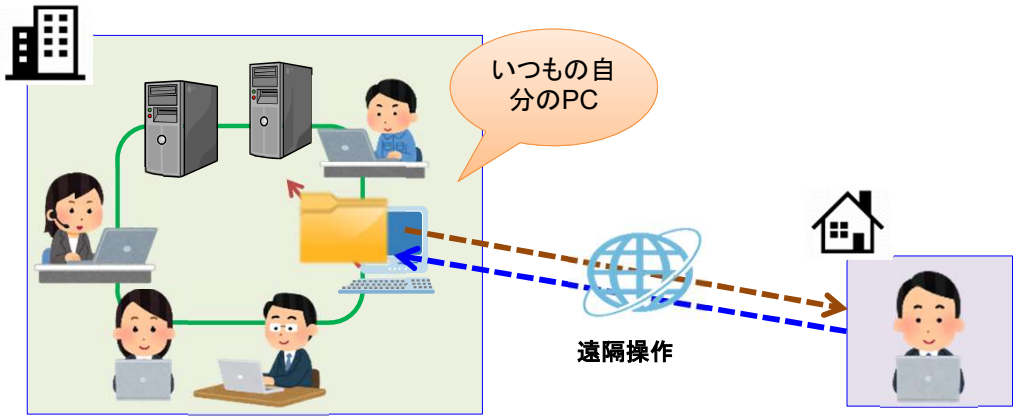
31

リモートデスクトップ方式

32

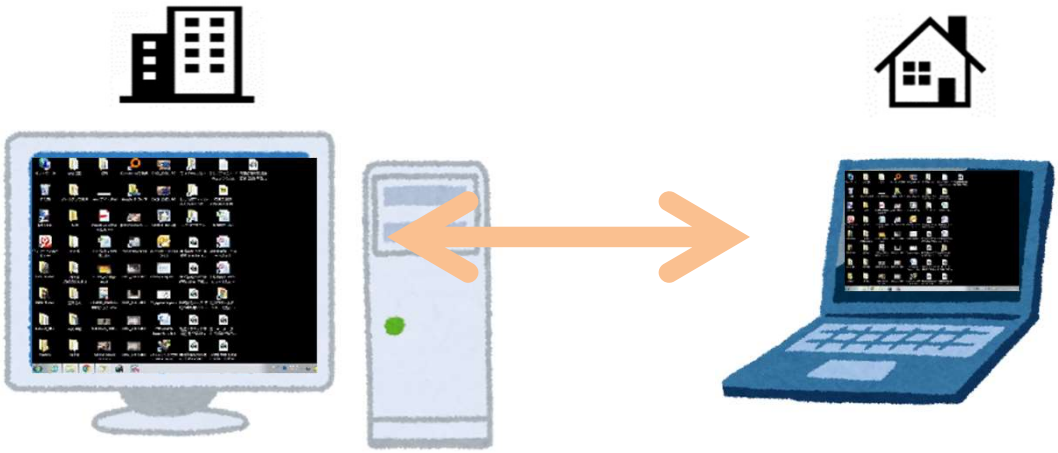
リモートデスクトップ方式の仕組み

社内に置いてある、自分のPCを遠隔操作して業務



33

33

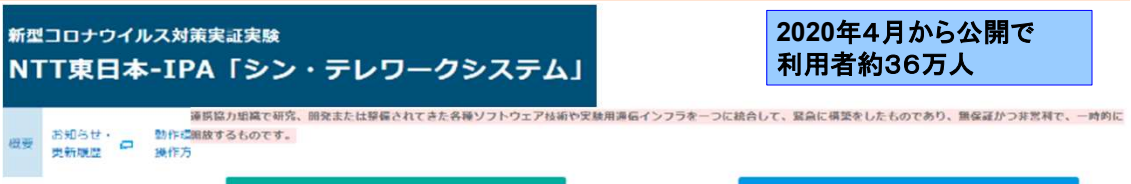


いつもと同じ画面で同じ業務

34

34

無償のリモートデスクトップシステム公開中



2020年4月から公開で利用者約36万人

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

「シン・テレワークシステム」による安全なリモートアクセス

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㈱	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㈱ ㈱バッファローなど	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 月々のサブスク料金が不要の場合もある
2	PacketiX VPN	ソフトイーサ㈱	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。高額な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 ベーションジャパン㈱	beat/active 初期登録 サービス60,000円/拠点 月額12,800円/拠点 設定さービス30,000円	拠点のネット ワークの状況を ヒアリング、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

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。

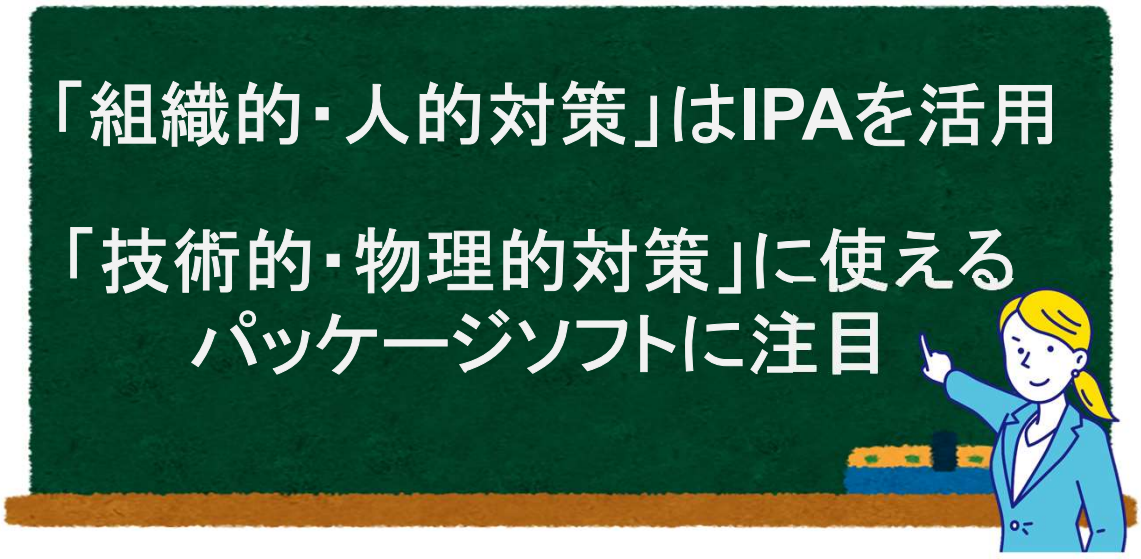
■リモートデスクトップツール

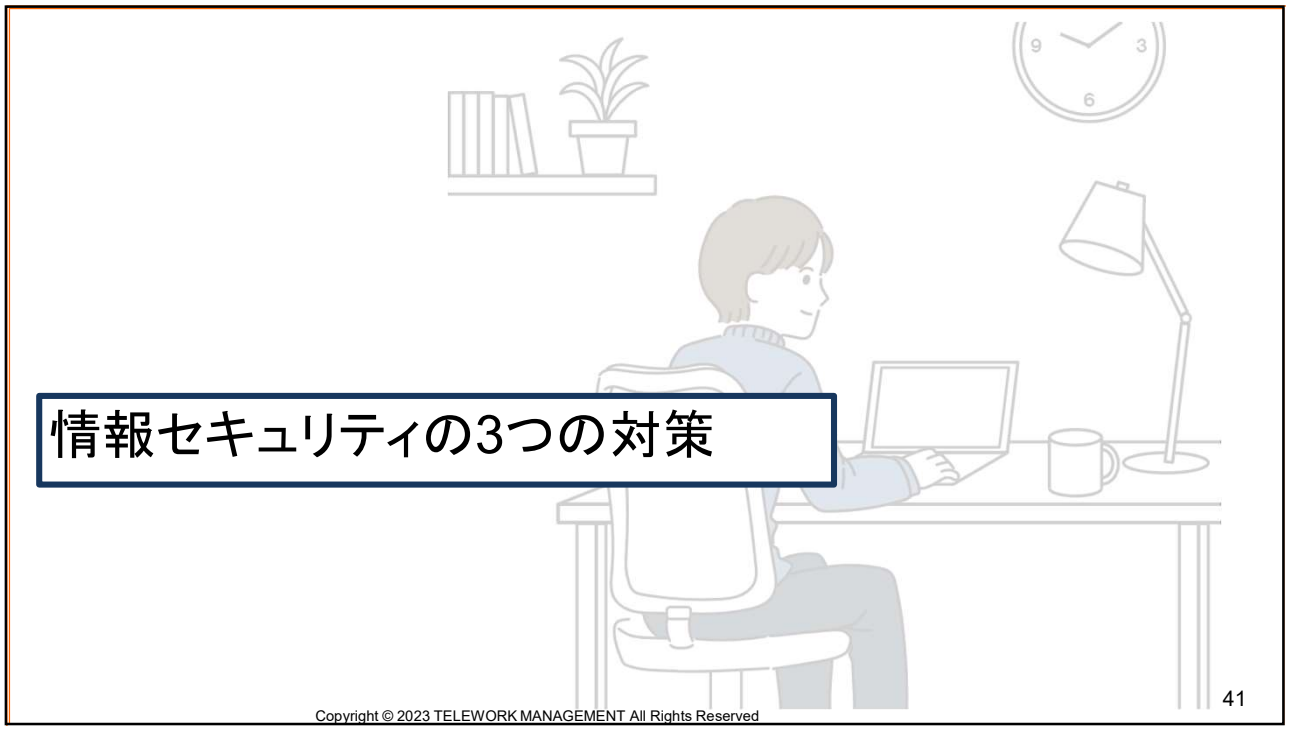
No	製品名	メーカー	価格	所要導入工数	特徴
1	マジックコネクト	NTTテクノクロス㈱	USB1台＋タブレット 初期費用15000円 年額18000円～	約1週間	2004年のサービス開始以来トラブル停止のない実績。国内シェア1位
2	スプラッシュトップ	スプラッシュトップ㈱	初期費用0円 年額15000円～	3営業日程度	PC画面を高速に動画配信する技術を採用
3	リモートビュー	Rサポート㈱	年額12000円	3営業日	低回線速度(128BPS)からも利用可能。接続ログと統計情報を一度に確認
4	DoMobile	㈱日立ソリューションズ・クリエイト	初期費用10000円＋1000円×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

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

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



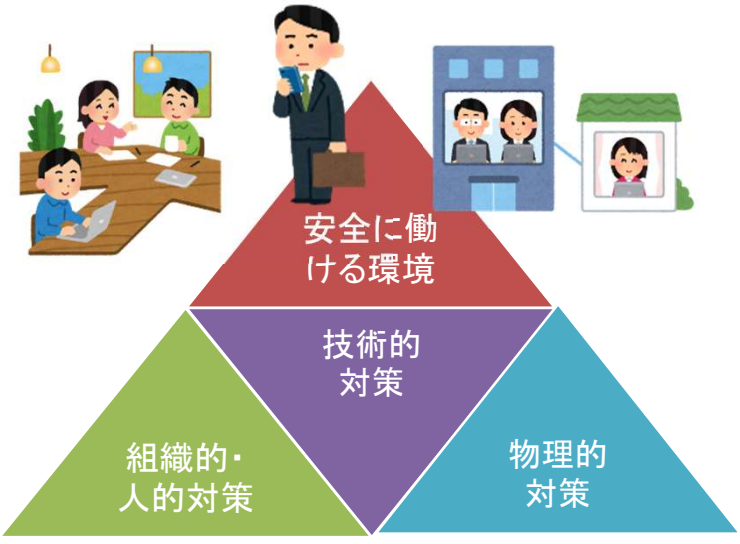


情報セキュリティの3つの対策

41

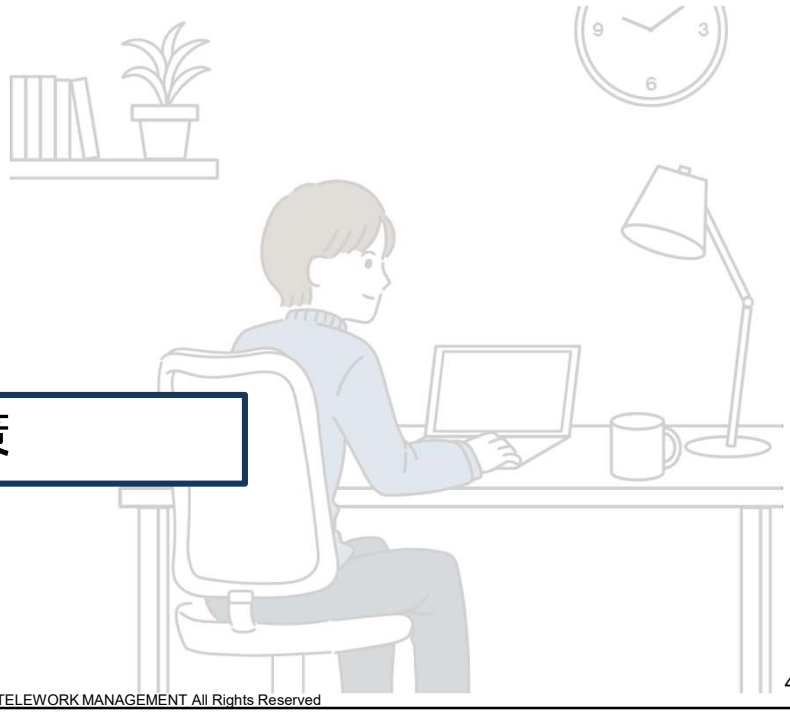
41

オフィスの内外問わず「安全に働ける環境」を作る3つの対策



42

42



組織的・人的対策

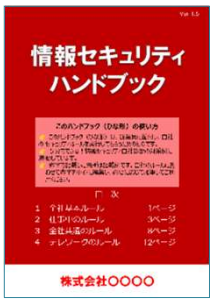
組織的・人的対策に役立つ資料1

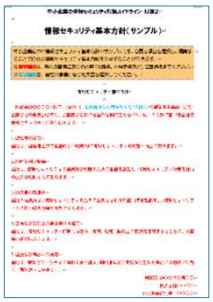
（2023年5月改訂）

目　次

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

組織的・人的対策に役立つ資料2





45

45

46

46

47

47

48

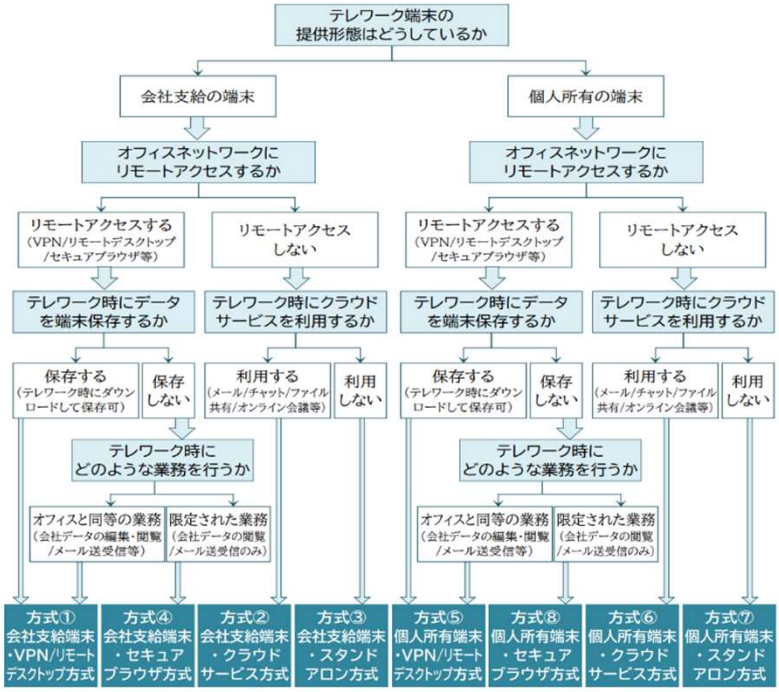
48

技術的・物理的対策に役立つ資料1

「テレワークセキュリティガイドライン（第5版）」

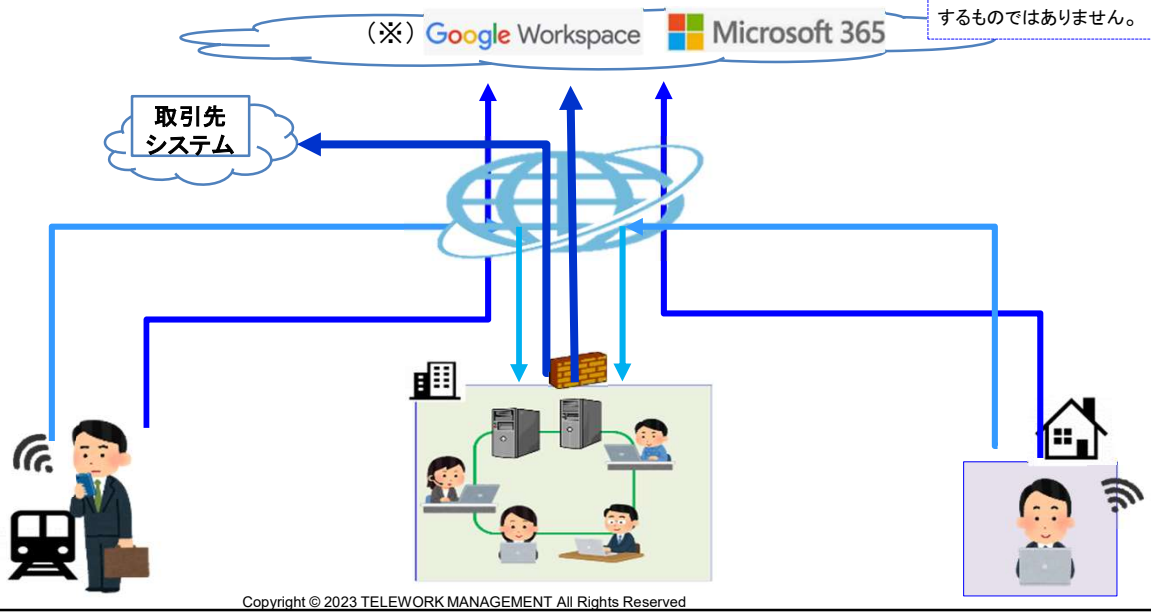
「中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト)」

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



テレワークを含む働き方

※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。

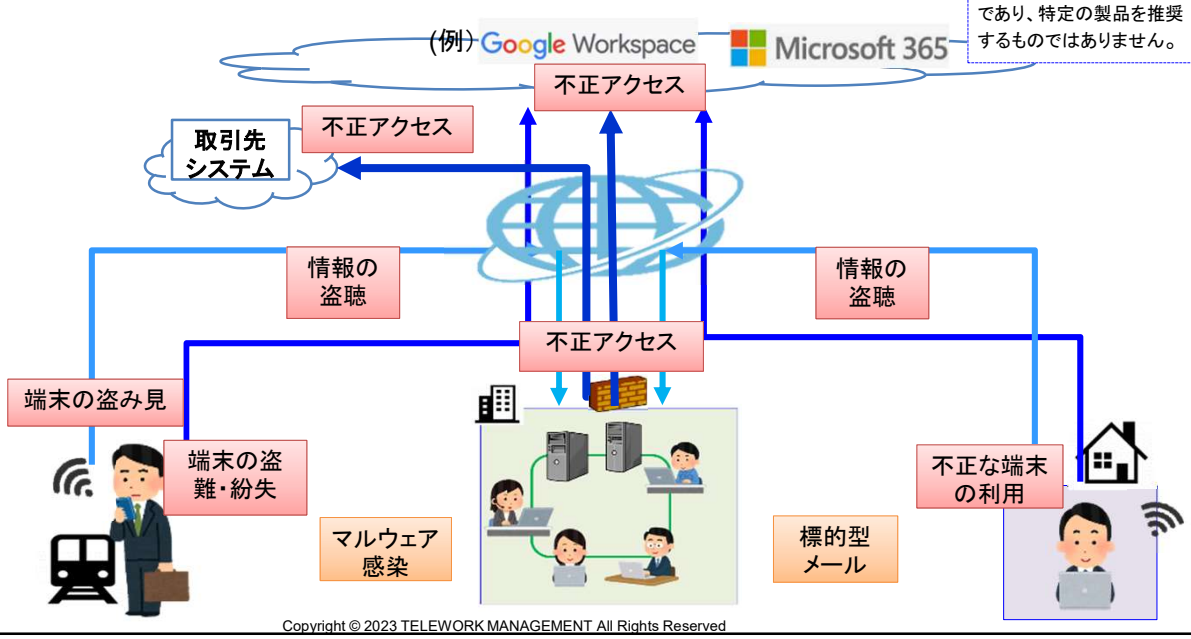


51

51

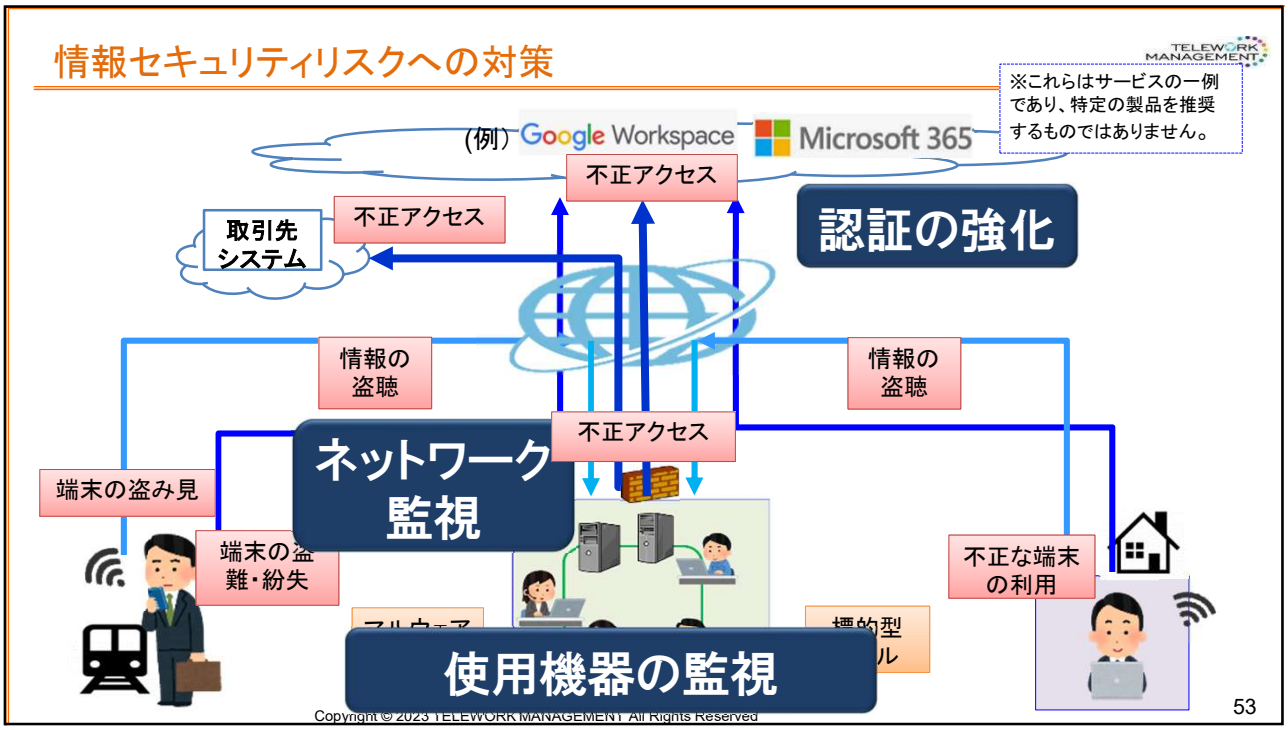
情報セキュリティリスク

※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。

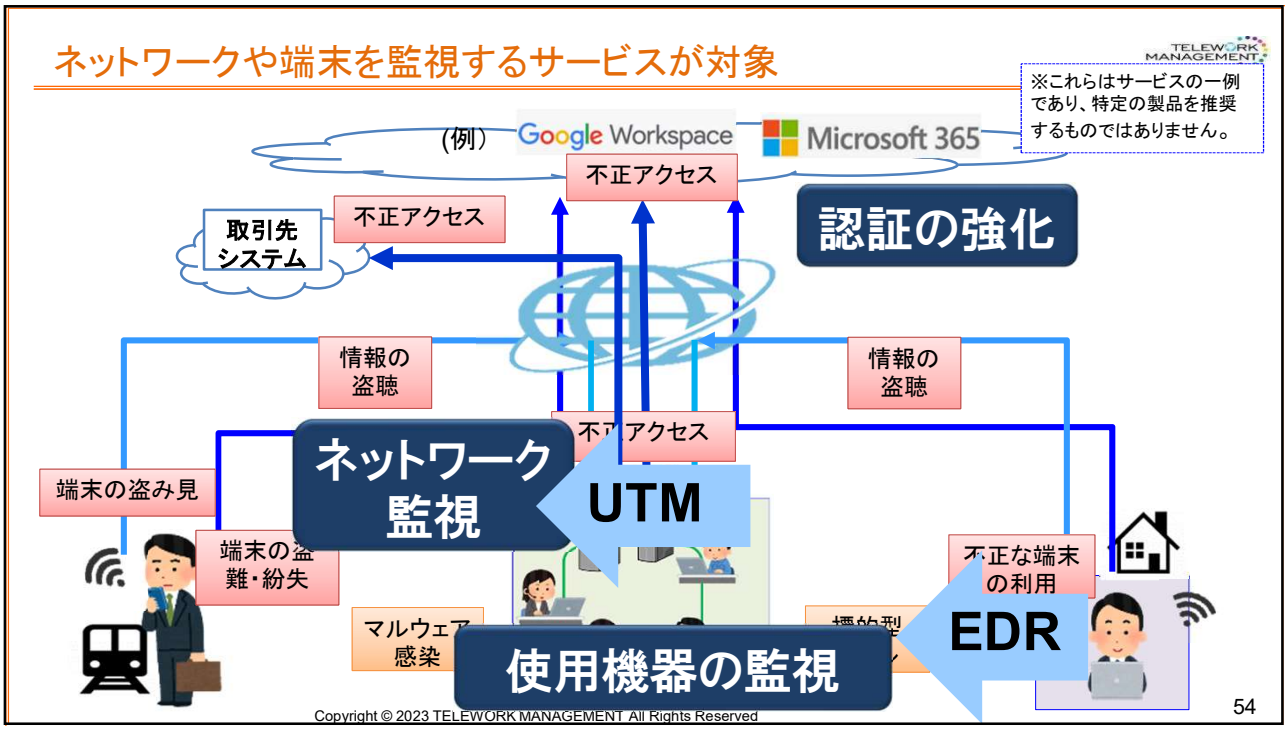


52

52

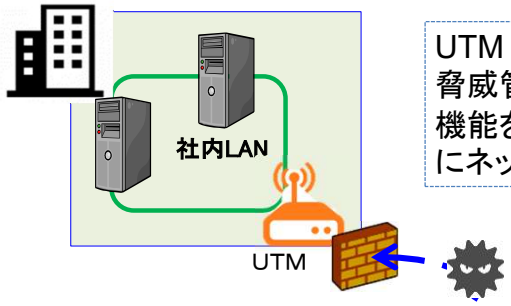

情報セキュリティリスクへの対策
※これらはサービスの一例であり、特定の製品を推奨するものではありません。
(例) Google Workspace Microsoft 365
不正アクセス
取引先システム
不正アクセス
認証の強化
情報の盗聴
情報の盗聴
不正アクセス
ネットワーク監視
端末の盗み見
端末の盗難・紛失
不正な端末の利用
使用機器の監視
Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved
53

53

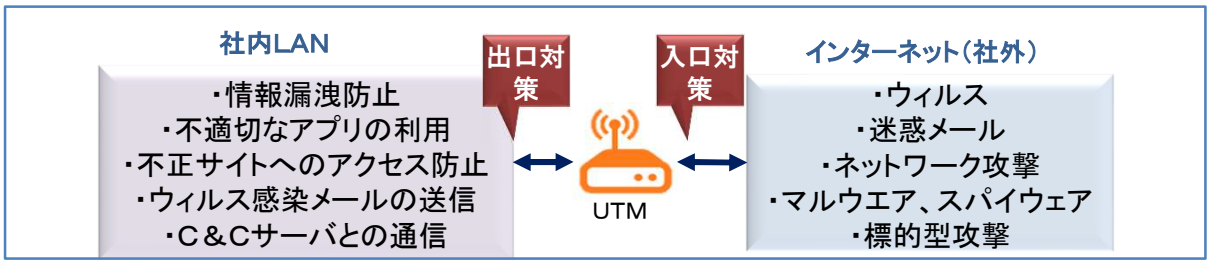

ネットワークや端末を監視するサービスが対象
※これらはサービスの一例であり、特定の製品を推奨するものではありません。
(例) Google Workspace Microsoft 365
不正アクセス
取引先システム
不正アクセス
認証の強化
情報の盗聴
情報の盗聴
ネットワーク監視
UTM
端末の盗み見
端末の盗難・紛失
不正な端末の利用
EDR
マルウェア感染
使用機器の監視
Copyright © 2023 TELEWORK MANAGEMENT All Rights Reserved
54

54

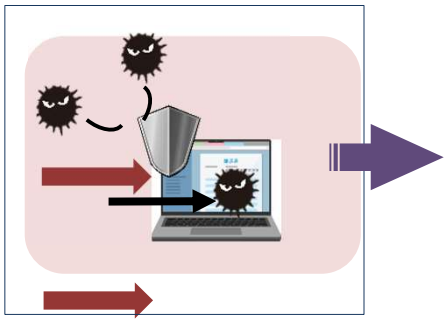
UTMとは？



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）

※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。

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/

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/

サイバーセキュリティ CSお助け隊

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11/27＞

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歩として、
テレワークを積極的に
導入・活用してみてください

61

ご清聴いただきありがとうございました。

62