スクリーニング調査

（全員が対象です。）

Ｓ－１　貴社・貴団体ではテレワーク※を導入されていますか。（○は１つ）

1	従前から導入している
2	新型コロナウイルス対策のため導入
3	以前導入していたが、既に導入をやめた
4	今後導入予定である
5	導入していないし、具体的な導入予定もない

※本アンケートでいう「テレワーク」は次のいずれかの形態を指します。

在宅勤務：自宅を就業場所とする働き方。終日在宅勤務のほか、１日の勤務時間のうち、一度オフィスに出勤、もしくは顧客訪問や会議参加などをしつつ、一部の時間は自宅で業務を行う「部分在宅勤務」も該当します。

サテライトオフィス勤務：所属するオフィス以外に他のオフィスやシェアオフィス、コワーキングスペース、遠隔勤務用の施設を就業場所とする働き方。

モバイルワーク：営業活動などで外出中、従業員がオフィスに戻らずに移動中の交通機関や駅・カフェなどでメールや日報の作成などの業務を行う働き方。

Ｓ－２　Ｓ－１で「５　導入していないし、具体的な導入予定もない」と回答された方に伺います。

テレワークを導入しない理由は何ですか。（○はいくつでも）

1	職種としてテレワークが実施不可だから（全員現場での作業が必要な職種など）
2	テレワークに適した仕事がないから
3	情報漏えいなどのセキュリティが心配だから
4	業務の進行管理が難しいから
5	導入するメリットがよく分からないから
6	社員の評価が難しいから
7	社内のコミュニケーションに支障があるから
8	周囲の社員にしわ寄せがあるから
9	労働組合や社員から要望がないから
10	顧客など外部への対応に支障があるから
11	費用がかかりすぎるから
12	労務や給与等の処理が複雑だから
13	文書の電子化が進んでいないから
14	導入や維持に対応できる人材が不足しているから
15	そもそも導入方法が分からないから
16	その他（　　）

Ｓ－３　Ｓ－２で「３　情報漏えいなどのセキュリティが心配だから」と回答された方に伺います。

具体的にどのようなセキュリティに関する心配がありますか。（○はいくつでも）

1	外部からの不正アクセスによる業務影響
2	マルウェア（ウイルス）感染による業務影響
3	端末等の紛失による業務影響
4	テレワーク端末に機密情報を保存すること
5	テレワーク端末から機密情報を閲覧すること
6	会社の管理外の場所で端末を利用すること
7	テレワーク時のセキュリティ対策に自信がない
8	なんとなく心配
9	その他（　　）

Ｓ－４　Ｓ－１で「４　今後導入予定である」又は「５　導入していないし、具体的な導入予定もない」と回答された方に伺います。

テレワークの導入に当たり課題と考えている点について教えてください。（○はいくつでも）

1	セキュリティの確保
2	テレワークに必要な端末等の整備
3	通信環境の整備（通信速度や回線の不足等）
4	テレワークに必要な場所の確保
5	テレワークをする社員の労働時間の管理
6	テレワーク業務に関する就業規則の整備
7	個々の従業員による業務の進捗管理
8	テレワークをする社員への指示・指導・評価
9	文書の電子化が進んでいないことによる業務への支障
10	書類へのサインや捺印ができないことによる業務への支障
11	取引先や顧客への対応
12	社内コミュニケーションの不足、情報共有の困難
13	テレワーク化する業務や対象となる社員の選定
14	テレワーク導入・維持に対応できる人材の不足
15	その他（　　）
16	特になし

Ｓ－５　Ｓ－１で「４　今後導入予定である」又は「５　導入していないし、具体的な導入予定もない」と回答された方に伺います。

職場利用・テレワーク利用に関わらず、会社所有のＰＣ端末のＯＳの種類を全て教えてください。（○はいくつでも）

1	Windows11
2	Windows10
3	Windows8.1（延長サポート契約済）
4	Windows8
5	Windows7
6	WindowsXP
7	MacOS
8	分からない
9	ＰＣ端末を利用していない
10	その他（　　）

Ｓ―６　Ｓ－１で「４　今後導入予定である」又は「５　導入していないし、具体的な導入予定もない」と回答された方に伺います。

Windows8.1（延長サポート契約済）※、Windows8、Windows7、WindowsXPのいずれも、セキュリティ上の公式サポートが切れていることをご存じですか。（○は１つ）

１　知らなかった
２　知っていた／アンチウイルスソフト等を導入しておけばまだ使えるという認識
３　知っていた／アンチウイルスソフト等を導入していても危険だという認識

※Windows8.1の延長サポート契約は2023年1月に終了予定です。

Ｓ－７　Ｓ－５で「４　Windows8」、「５　Windows7」又は「６　WindowsXP」と回答された方に伺います。

使用するＰＣ端末はサポート期限が切れていますが、そのまま使っている理由は何ですか。（○はいくつでも）

１　使用に問題があると思っていない
２　利用するソフトウェアが最新ＯＳに対応していない
３　更新する費用がない
４　危険性を最近認知した
５　更新する方向で検討中
６　更新中・調達中
７　インターネットに接続していない等の特殊な用途である
８　その他（　　）

Ｓ－８　Ｓ－５で「４　Windows8」、「５　Windows7」又は「６　WindowsXP」と回答された方に伺います。

貴社・貴団体が使用するＰＣ端末のうち、これらサポート期限が切れたものの割合はどの程度ですか。最も近いものをお選びください。（○は１つ）

１　１割程度／ごく一部
２　２～３割程度
３　半数程度
４　全部／ほぼ全部

本調査（Ｓ－１で１～３と回答された方が対象です。）

１　テレワーク導入状況について

１－１　テレワークはいつ頃から導入されましたか。（○は１つ）

1	2019年以前
2	2020年１月～３月
3	2020年４月～６月（緊急事態宣言１回目）
4	2020年７月～９月（まん延防止等重点措置継続期間１回目）
5	2020年１０月～１２月
6	2021年１月～３月（緊急事態宣言２回目）
7	2021年４月～６月（緊急事態宣言３回目）
8	2021年７月～９月（緊急事態宣言４回目）
9	2021年１０月～１２月
10	2022年１月～３月（まん延防止等重点措置継続期間２回目）
11	2022年４月以降

１－２　Ｓ－１で「１　従前から導入している」「２　新型コロナウイルス対策のため導入」と回答された方に伺います。

今後もテレワークを活用する予定ですか。（○は１つ）

1	活用する予定
2	活用しない予定
3	既に導入をやめた
4	検討中

１－３　１－２で「３　既に導入をやめた」と回答された方に伺います。

テレワークはいつ頃やめられましたか。（○は１つ）

1	2019年以前
2	2020年１月～３月
3	2020年４月～６月（緊急事態宣言１回目）
4	2020年７月～９月（まん延防止等重点措置継続期間１回目）
5	2020年１０月～１２月
6	2021年１月～３月（緊急事態宣言２回目）
7	2021年４月～６月（緊急事態宣言３回目）
8	2021年７月～９月（緊急事態宣言４回目）
9	2021年１０月～１２月
10	2022年１月～３月（まん延防止等重点措置継続期間２回目）
11	2022年４月以降

１－４ １－２で「２　活用しない予定」「３　既に導入をやめた」と回答された方に伺います。

テレワークを活用しない、もしくはやめた理由は何ですか。（〇はいくつでも）

1	職種としてテレワークが実施不可だから（全員現場での作業が必要な職種など）
2	テレワークに適した仕事がないから
3	情報漏えいなどのセキュリティが心配だから
4	業務の進行管理が難しいから
5	導入するメリットがよく分からないから
6	社員の評価が難しいから
7	社内のコミュニケーションに支障があるから
8	周囲の社員にしわ寄せがあるから
9	労働組合や社員から要望がないから
10	顧客など外部への対応に支障があるから
11	費用がかかりすぎるから
12	労務や給与等の処理が複雑だから
13	文書の電子化が進んでいないから
14	導入や維持に対応できる人材が不足しているから
15	セキュリティ事故が発生した際の連絡体制に課題を感じたから
16	情報の取扱い方針・対策に課題を感じたから
17	その他（　　）

１－５ 貴社・貴団体のテレワークの実施状況について、これまで最も多くテレワークが利用された日で、全従業員・職員のうちどのくらいの割合がテレワークを利用しましたか。

最もテレワークを利用した時期、その利用率についてお答えください。（それぞれ〇は１つ）

＜時期＞

1	2019年以前
2	2020年１月～３月
3	2020年４月～６月（緊急事態宣言１回目）
4	2020年７月～９月（まん延防止等重点措置継続期間１回目）
5	2020年１０月～１２月
6	2021年１月～３月（緊急事態宣言２回目）
7	2021年４月～６月（緊急事態宣言３回目）
8	2021年７月～９月（緊急事態宣言４回目）
9	2021年１０月～１２月
10	2022年１月～３月（まん延防止等重点措置継続期間２回目）
11	2022年４月以降

＜利用率＞

1	５％未満
2	５％以上１０％未満
3	１０％以上３０％未満
4	３０％以上５０％未満
5	５０％以上８０％未満
6	８０％以上

２　テレワーク実施における各種対策について

２－１　テレワークの実施に当たり、システム関係について検討・実施したことは何ですか。

（それぞれ○はいくつでも）

検討した事項	1　テレワーク方式（システム構成）の検討・見直し 2　ＰＣ端末の追加調達 3　モバイル端末（スマホ・タブレット等）の追加調達 4　従業員の私用端末の利用許可 5　クラウドサービスの新規導入・追加契約 6　ネットワーク回線帯域の増強 7　リモートアクセス設備（VPN機器、VDI基盤など）の増強 8　サテライトオフィスの活用 9　その他（　　） 10　特に何もしていない
実施した事項	1　テレワーク方式（システム構成）の検討・見直し 2　ＰＣ端末の追加調達 3　モバイル端末（スマホ・タブレット等）の追加調達 4　従業員の私用端末の利用許可 5　クラウドサービスの新規導入・追加契約 6　ネットワーク回線帯域の増強 7　リモートアクセス設備（VPN機器、VDI基盤など）の増強 8　サテライトオフィスの活用 9　その他（　　） 10　特に何もしていない

２－２　テレワークの実施に当たり、テレワークセキュリティ対策について検討・実施したことは何ですか。

（それぞれ○はいくつでも）

検討した事項	1　セキュリティポリシー等のルール（規程）の整備・変更 2　テレワーク利用に特化したルールの新設 3　会社所有端末の持出しを許容するルールの新設 4　従業員所有端末の業務利用を許容するルールの新設 5　機密情報の持出しを許容するルールの新設 6　セキュリティ研修の実施 7　セキュリティに関する注意事項の周知 8　セキュリティ担当者・担当部署の強化（新設を含む） 9　その他（　　） 10　特に何もしていない
実施した事項	1　セキュリティポリシー等のルール（規程）の整備・変更 2　テレワーク利用に特化したルールの新設 3　会社所有端末の持出しを許容するルールの新設 4　従業員所有端末の業務利用を許容するルールの新設 5　機密情報の持出しを許容するルールの新設 6　セキュリティ研修の実施 7　セキュリティに関する注意事項の周知 8　セキュリティ担当者・担当部署の強化（新設を含む） 9　その他（　　） 10　特に何もしていない

２－３ テレワーク時のクラウドサービス利用について伺います。

各クラウドサービスについてお答えください。（それぞれ○は１つ）

① オンライン会議サービス	1　従前から利用している 2　今後利用予定である 3　既に利用をやめた 4　利用していないし、具体的な利用予定もない
② チャットサービス	1　従前から利用している 2　今後利用予定である 3　既に利用をやめた 4　利用していないし、具体的な利用予定もない
③ ファイル共有サービス	1　従前から利用している 2　今後利用予定である 3　既に利用をやめた 4　利用していないし、具体的な利用予定もない
④ メールサービス	1　従前から利用している 2　今後利用予定である 3　既に利用をやめた 4　利用していないし、具体的な利用予定もない
⑤ プロジェクト管理	1　従前から利用している 2　今後利用予定である 3　既に利用をやめた 4　利用していないし、具体的な利用予定もない
⑥ グループウェア	1　従前から利用している 2　今後利用予定である 3　既に利用をやめた 4　利用していないし、具体的な利用予定もない
⑦ 労務管理	1　従前から利用している 2　今後利用予定である 3　既に利用をやめた 4　利用していないし、具体的な利用予定もない
⑧ 会計	1　従前から利用している 2　今後利用予定である 3　既に利用をやめた 4　利用していないし、具体的な利用予定もない
⑨ 電子押印・署名サービス（電子契約を含む）	1　従前から利用している 2　今後利用予定である 3　既に利用をやめた 4　利用していないし、具体的な利用予定もない
⑩ 顧客管理	1　従前から利用している 2　今後利用予定である 3　既に利用をやめた 4　利用していないし、具体的な利用予定もない

⑪ 営業支援	1　従前から利用している 2　今後利用予定である 3　既に利用をやめた 4　利用していないし、具体的な利用予定もない
⑫ 名刺管理	1　従前から利用している 2　今後利用予定である 3　既に利用をやめた 4　利用していないし、具体的な利用予定もない

上記以外に利用しているクラウドサービスがあれば、導入時期を含めて記載ください。

２－４　テレワーク方式の選定に当たって、最も重視した観点は何ですか。（○は１つ）

1　導入費用 2　導入の容易性 3　セキュリティ強度 4　利用者の利便性 5　導入事例の多さ・評判 6　その他（　　）

３　テレワーク端末について

３－１　テレワーク利用を許可している端末の形態は何ですか。（〇はいくつでも）

1　ＰＣ端末：会社支給（通常職場で使用している端末）
2　ＰＣ端末：会社支給（テレワーク用端末を別に用意）
3　ＰＣ端末：従業員所有（USBブート型シンクライアントでの利用）
4　ＰＣ端末：従業員所有（通常利用）
5　モバイル端末(スマホ・タブレット等)：会社支給
6　モバイル端末(スマホ・タブレット等)：従業員所有
7　端末は使用しない（紙出力するなど）
8　把握していない

３－２　３－１で「１　ＰＣ端末：会社支給（通常職場で使用している端末)」又は「２　ＰＣ端末：会社支給（テレワーク用端末を別に用意)」と回答された方に伺います。

テレワークで利用する会社支給のＰＣ端末について、利用しているＯＳの種類を全て教えてください。（〇はいくつでも）

1　Windows11
2　Windows10
3　Windows8.1（延長サポート契約済）
4　Windows8
5　Windows7
6　WindowsXP
7　MacOS
8　把握していない
9　その他（　　）

３－３　（全員に伺います。）職場利用・テレワーク利用に関わらず、会社所有のＰＣ端末のＯＳの種類を全て教えてください。（〇はいくつでも）

1　Windows11
2　Windows10
3　Windows8.1（延長サポート契約済）
4　Windows8
5　Windows7
6　WindowsXP
7　MacOS
8　分からない
9　ＰＣ端末を利用していない
10　その他（　　）

３－４　（全員に伺います。）Windows8.1（延長サポート契約済）※、Windows8、Windows7、WindowsXPのいずれも、セキュリティ上の公式サポートが切れていることをご存じですか。（○は１つ）

1　知らなかった
2　知っていた／アンチウイルスソフト等を導入しておけばまだ使えるという認識
3　知っていた／アンチウイルスソフト等を導入していても危険だという認識

※Windows8.1の延長サポート契約は2023年1月に終了予定です。

３－５　３－３で「４　Windows8」、「５　Windows7」又は「６　WindowsXP」と回答された方に伺います。

使用するＰＣ端末はサポート期限が切れていますが、そのまま使っている理由は何ですか。（○はいくつでも）

1　使用に問題があると思っていない
2　利用するソフトウェアが最新ＯＳに対応していない
3　更新する費用がない
4　危険性を最近認知した
5　更新する方向で検討中
6　更新中・調達中
7　インターネットに接続していない等の特殊な用途である
8　その他（　　）

３－６　３－３で「４　Windows8」、「５　Windows7」又は「６　WindowsXP」と回答された方に伺います。

貴社・貴団体が使用するＰＣ端末のうち、これらサポート期限が切れたものの割合はどの程度ですか。最も近いものをお選びください。（○は１つ）

1　１割程度／ごく一部
2　２～３割程度
3　半数程度
4　全部／ほぼ全部

３－７　３－１で「４　ＰＣ端末：従業員所有（通常利用）」と回答された方に伺います。

従業員がテレワーク時に、サポート期限が切れた端末（Windows8、Windows7、WindowsXP等）を使わないような対策をしていますか。（○はいくつでも）

1　規程・ルールで禁止している
2　注意喚起や研修で周知している
3　テレワーク使用端末を届出させるなどして、サポート切れが使われないよう把握している
4　その他（　　）
5　特に対策をしていない

4　その他のテレワーク利用製品について

4－1　テレワークで利用している端末（PC 端末やスマートフォン/タブレット）側の**ウイルス対策製品**は何ですか。（○はいくつでも）

1	Windows Defender(Microsoft Corporation)
2	Norton360(NortonLifeLock Inc.)
3	ウィルスバスタークラウド(Trend Micro Inc.)
4	Kaspersky Endpoint Security(Kaspersky Lab.)
5	SOPHOS HOME(Sophos Ltd.)
6	Bitdefender(Bitdefender)
7	Microsoft Defender Advanced Threat Protection(Microsoft Corporation)
8	CrowdStrike(CrowdStrike Holdings, Inc.)
9	Symantec EDR Cloud((株)日立システムズ)
10	Trend Micro Apex One(Trend Micro Inc.)
11	McAfee (McAfee, LLC)
12	ESET インターネット セキュリティ (ESET, spol. s r.o.)
13	その他 （　　）
14	ウイルス対策製品を利用していない

4－2　テレワークで利用している端末（PC 端末やスマートフォン/タブレット）側の**デバイス管理製品・サービス**は何ですか。（○はいくつでも）

1	LanScope An(MOTEX Inc.)
2	CLOMO MDM((株)アイキューブドシステムズ)
3	Meraki System Manager (Cisco Systems, Inc.)
4	MobileIron EMM(MobileIron, Inc.)
5	Jamf Pro (Jamf)
6	mobiconnect for Business (インヴェンティット(株))
7	BizMobile Go! (BizMobile(株))
8	Vmware Workspace One(旧：AirWatch) (VMware Inc.)
9	Optimal Biz((株)オプティム)
10	FENCE-Mobile RemoteManager(富士通(株))
11	PC Check Cloud (NRIセキュアテクノロジーズ(株))
12	TRUST DELETE prime(ワンビ(株))
13	たよれーるDMS ((株)大塚商会)
14	Docomo あんしんマネージャー (NTTドコモ(株))
15	SoftBank ビジネス・コンシェル デバイスマネジメント (ソフトバンク(株))
16	KDDI Smart Mobile Safety Manager(KDDI(株))
17	Google エンドポイント管理(Google(同))
18	Microsoft Intune (日本マイクロソフト(株))
19	SKYSEA Client View (SKY (株))
20	その他 （　　）
21	デバイス管理製品・サービスを利用していない

4－3　テレワーク用の端末（PC 端末やスマートフォン/タブレット）で、社内システムやドキュメントにアクセスする際に用いている**ブラウザ等**は何ですか。（○はいくつでも）

1	CACHATTO Securebrowser(e-Janネットワークス(株))
2	Soliton SecureBrowser((株)ソリトンシステムズ)
3	HENNGEOne(HENNGE(株))
4	magicconnectモバイル(ＮＴＴテクノクロス(株))
5	Internet Explorer(Microsoft Corporation)
6	Google Chrome(Google,LLC)
7	Firefox(Mozilla Corporation)
8	Microsoft Edge(Microsoft Corporation)
9	その他 （　　）
10	ブラウザを利用していない

４－４ テレワーク用の端末（PC 端末やスマートフォン/タブレット）でインターネットにアクセスする際に**利用しているブラウザ等**は何ですか。（○はいくつでも）

1	CACHATTO Securebrowser(e-Janネットワークス(株))
2	Soliton SecureBrowser((株)ソリトンシステムズ)
3	HENNGEOne(HENNGE(株))
4	magicconnectモバイル(ＮＴＴテクノクロス(株))
5	Internet Explorer(Microsoft Corporation)
6	Google Chrome(Google,LLC)
7	Firefox(Mozilla Corporation)
8	Microsoft Edge(Microsoft Corporation)
9	その他（　　）
10	ブラウザを利用していない

４－５ テレワークを実施するうえで従業員・職員が利用している**リモートアクセス製品のうちVPN製品**は何ですか。（○はいくつでも）

1	SoftEther VPN(筑波大学大学院研究プロジェクト)(無償)
2	PacketiX VPN(ソフトイーサ(株))(有償)
3	beat リモートアクセスサービス(富士ゼロックス(株))
4	CiscoASA/AnyConnect(シスコシステムズ(同))
5	Pulse Connect Secure（旧：Juniper SAシリーズ、MAGシリーズ）(Pulse Secure, LLC)
6	meraki MX(シスコシステムズ(同))
7	SEIL/SAシリーズ((株)テリロジーサービスウェア/(株)インターネットイニシアティブ))
8	Yamaha　VPNルーター（Yamaha)
9	Arcstar Universal One(NTTコミュニケーションズ(株))
10	マネージドUTM ビジネスセキュリティ((株)USEN ICT Solutions)
11	SmartVPN(ソフトバンク(株))
12	Verona((株)網屋)
13	Master's One（NTTPCコミュニケーションズ（株))
14	FortiClient（フォーティネットジャパン（同))
15	その他（　　）
16	リモートアクセス製品（VPN製品）を利用していない

４－６ テレワークを実施するうえで従業員・職員が利用している**リモートアクセス製品のうちリモートデスクトップ製品**は何ですか。（○はいくつでも）

1	magic Connect(NTTテクノクロス(株))
2	Splashtop Business(スプラッシュトップ(株))
3	Remote View(RSUPPORT(株))
4	DoMobile((株)日立ソリューションズ・クリエイト)
5	ISL Online((株)オーシャンブリッジ)
6	Remote Works(TIS(株))
7	Smart Interwork(インターコア(株))
8	Soliton SecureDesktop((株)ソリトンシステムズ)
9	シン・テレワークシステム(NTT東日本(株))
10	TeamViewer（teamviewer.com)
11	Chromeデスクトップ(グーグル(同))
12	Windows標準 リモートデスクトップ接続(VPN製品と併用)
13	その他（　　）
14	リモートアクセス製品（リモートデスクトップ製品）を利用していない

４－７ テレワークを実施するうえで従業員・職員が利用している、**社内**の打合せで使う**WEB会議システムの製品**は何ですか。（○はいくつでも）

1	Microsoft Teams(日本マイクロソフト(株))
2	Skype for Business（旧：Microsoft Lync）(日本マイクロソフト(株))
3	Zoom(Zoom Video Communications, Inc.)
4	V-CUBEミーティング((株)ブイキューブ)
5	WebEx Meeting Center(シスコシステムズ(同))
6	Googleハングアウト(グーグル(同))
7	GoogleMeets(グーグル(同))
8	MeetingPlaza(NTTテクノクロス(株))
9	LiveOn(ジャパンメディアシステム(株))
10	FreshVoice(エイネット(株))
11	CaféX Meetings(CaféX Communications, Inc.)
12	Cisco Webex(Cisco Systems, Inc.)
13	Chatwork(Chatwork(株))
14	LINE WORKS((Works Mobile Japan(株))
15	Slack(Slack Japan(株))
16	Whereby（Videonor(株))
17	その他（　　）
18	WEB会議システムの製品を利用していない

４－８ テレワークを実施するうえで従業員・職員が利用している、**社外**との打合せで使う**WEB会議システムの製品**は何ですか。（○はいくつでも）

1	Microsoft Teams(日本マイクロソフト(株))
2	Skype for Business（旧：Microsoft Lync）(日本マイクロソフト(株))
3	Zoom(Zoom Video Communications, Inc.)
4	V-CUBEミーティング((株)ブイキューブ)
5	WebEx Meeting Center(シスコシステムズ(同))
6	Googleハングアウト(グーグル(同))
7	GoogleMeets(グーグル(同))
8	MeetingPlaza(NTTテクノクロス(株))
9	LiveOn(ジャパンメディアシステム(株))
10	FreshVoice(エイネット(株))
11	CaféX Meetings(CaféX Communications, Inc.)
12	Cisco Webex(Cisco Systems, Inc.)
13	Chatwork(Chatwork(株))
14	LINE WORKS((Works Mobile Japan(株))
15	Slack(Slack Japan(株))
16	Whereby（Videonor(株))
17	その他（　　）
18	WEB会議システムの製品を利用していない

4－9　テレワークを実施するうえで従業員・職員が利用している**メールサービス**は何ですか。（○はいくつでも）

1	Gmail（無料版）（グーグル(同)）
2	Gmail（有料版）（グーグル(同)）
3	Exchange Online（Office365提供のメールサービス）（日本マイクロソフト(株)）
4	Amazon WorkMail(Amazon.com, Inc)
5	Active! Mail（(株)クオリティア）
6	Zohoメール(ゾーホージャパン(株))
7	BIGLOBEクラウドメール（ビッグローブ(株)）
8	Microsoft Outlook（日本マイクロソフト(株)）
9	さくらインターネット（さくらインターネット株式会社）
10	Garoon（サイボウズ株式会社）
11	その他（　　）
12	メールサービスを利用していない

4－10　テレワークを実施するうえで従業員・職員が利用している**チャットツールの製品**は何ですか。（○はいくつでも）

1	Chatwork(chatwork(株))
2	LINE WORKS(Works Mobile Japan(株))
3	Slack(Slack Japan(株))
4	InCircle((株)DXクラウド)
5	TopicRoom(NTTテクノクロス(株))
6	Microsoft Teams((日本マイクロソフト(株))
7	Skype for Business（旧：Microsoft Lync）（日本マイクロソフト(株)）
8	LINE(LINE(株))
9	Google Chat（Google LLC）
10	Zoom Chat（Zoom Video Communications, Inc.）
11	その他（　　）
12	チャットツールの製品を利用していない

4－11　テレワークを実施するうえで従業員・職員が利用している**ストレージサービスの製品**は何ですか。（○はいくつでも）

1	Google Drive(Google LLC)
2	OneDrive for Business(Microsoft Corporation)
3	Dropbox Business(Dropbox, Inc.)
4	Fleekdrive((株)Fleekdrive)
5	Box((株)Box Japan)
6	セキュアSAMBA(スターティアレイズ(株))
7	DirectCloud-BOX((株)ダイレクトクラウド)
8	Bizストレージ ファイルシェア(NTTコミュニケーションズ(株))
9	KDDI ファイルストレージ(KDDI(株))
10	PrimeDrive(ソフトバンク(株))
11	Fileforce(ファイルフォース(株))
12	firestorage(ロジックファクトリー(株))
13	Smooth Fileクラウド((株)プロット)
14	その他（　　）
15	ストレージサービスの製品を利用していない

4－12　テレワークを実施するうえで従業員・職員が利用しているクラウドアクセス用の**ネットワークセキュリティ製品**は何ですか。（○はいくつでも）

1	Netskope(Netskope, Inc)
2	Zscaler Internet Access(ノックス(株))
3	i-FILTER（Digital Arts Inc.）
4	その他（　　）
5	クラウドアクセス用のネットワークセキュリティ製品を利用していない

4－13 テレワークを実施するうえで従業員・職員が利用している**仮想デスクトップ方式の製品**は何ですか。（〇はいくつでも）

1	Citrix XenDesktop(Citrix Systems, Inc)
2	VMware Horizon 7(VMware, Inc)
3	Microsoft VDI/Microsoft Virtual Desktop Infrastructure(Microsoft Corporation)
4	その他（　　）
5	仮想デスクトップ方式の製品を利用していない

4－14 テレワークを実施するうえで従業員・職員が利用している**アプリケーション・ラッピング方式*の製品**は何ですか。（〇はいくつでも）

1	CACHATTO Desktop(e-Janネットワークス(株))
2	WrappingBox((株)ソリトンシステムズ)
3	Flex Work Place(横河レンタ・リース(株))
4	@割符plus(ネクスト・シェアリング(株))
5	ZENMU for PC((株)ZenmuTech)
6	その他（　　）
7	アプリケーション・ラッピング方式の製品を利用していない

※アプリケーション・ラッピング方式とは、テレワーク端末内に仮想的な隔離環境を設け、その中でテレワーク業務用のアプリケーションを動作させる方式です。当該方式では、テレワーク端末と仮想的な隔離環境との間でデータのやり取りを制限することが可能です。

５　情報セキュリティ対策について

５－１　情報セキュリティ対策に関する取組（実施状況）として、それぞれ該当するものをお答えください。（それぞれ○は１つ）

①　資産管理 （例：テレワークで使用する端末等を把握・管理している）	1　十分実施している 2　実施しているが不十分と感じる 3　未実施
②　マルウェア（ウイルス）対策 （例：アンチウイルスソフト（セキュリティ対策ソフト）をテレワーク用端末に導入している）	1　十分実施している 2　実施しているが不十分と感じる 3　未実施
③　論理的なアクセス制御 （例：必要な情報へのアクセス権を最小限に限定し、ファイアーウォール等でアクセス制御を実施している）	1　十分実施している 2　実施しているが不十分と感じる 3　未実施
④　物理的なアクセス制御 （例：端末から離れる際にはスクリーンロックをかけている）	1　十分実施している 2　実施しているが不十分と感じる 3　未実施
⑤　脆弱性管理 （例：ＯＳやソフトウェア、ネットワーク機器のファームウェア等を最新の状態にしている）	1　十分実施している 2　実施しているが不十分と感じる 3　未実施
⑥　インシデント対応・管理 （例：マルウェア感染や情報漏えい等が発生した場合に備え、対応方針や関係者の連絡先等を定めている）	1　十分実施している 2　実施しているが不十分と感じる 3　未実施
⑦　データ保護 （例：テレワーク端末のハードディスクを暗号化している／機密情報を暗号化して保存している）	1　十分実施している 2　実施しているが不十分と感じる 3　未実施
⑧　通信暗号化 （例：クラウドサービス接続時にHTTPS通信などを利用している／VPNで暗号化した上で通信している）	1　十分実施している 2　実施しているが不十分と感じる 3　未実施
⑨　認証 （例：第三者に推測されにくいようなパスワードを設定している）	1　十分実施している 2　実施しているが不十分と感じる 3　未実施
⑩　特権管理 （例：システムの管理者権限は限られた従業員のみが必要な場合のみ利用し、厳格に管理している）	1　十分実施している 2　実施しているが不十分と感じる 3　未実施
⑪　規程の整備 （例：セキュリティポリシー等の規程を整備している）	1　十分実施している 2　実施しているが不十分と感じる 3　未実施
⑫　教育 （例：従業員に情報セキュリティに関する研修を実施している）	1　十分実施している 2　実施しているが不十分と感じる 3　未実施
⑬　脅威インテリジェンス （例：脅威動向、攻撃手法、脆弱性等に関する情報を収集している）	1　十分実施している 2　実施しているが不十分と感じる 3　未実施

５－２ ５－１の取組において、どれか一つでも「３　未実施」と回答された方に伺います。

未実施と回答された項目の理由について、最も当てはまるものを教えてください。（○は１つ）

1　該当する対策の内容を検討したことがない
2　該当する対策の必要性を感じていない
3　実施には至っていないが、検討している
4　対策実施を進言したことがあるが、経営判断で実施しない方針となった
5　その他（　　）

５－３　貴社・貴団体における組織体制について教えてください。（○はいくつでも）

1　ＩＴ担当役員（CIO）が存在する
2　セキュリティ担当役員（CISO）が存在する
3　情報システム部門が存在する
4　セキュリティ企画・管理部門が情報システム部門とは別に存在する
5　経営企画・総務部門等がシステムやセキュリティを担当している（専門部門がない）
6　システムやセキュリティに明るい人材が属人的に担当している
7　システム管理業務は外部の専門企業に委託している
8　セキュリティ対策業務は外部の専門企業に委託している
9　テレワーク導入・運営を担う部門が明確になっている
10　テレワークを推進する担当役員が明確になっている

５－４　貴社・貴団体において、最もセキュリティに詳しい方について、最も当てはまるものを選んでください。（○は１つ）

1　高度な資格を有するレベルの者がいる（例：情報処理安全確保支援士、CISSP、SSCP等）
2　高度な資格はないが、相当な知識を有している者がいる
3　社内には適切な者はいないが、グループ会社や関連会社に適切な人材がいる
4　関連会社等を含め適切な者はいないが、外部委託先に適切な人材がいる
5　セキュリティに詳しい者はいない

6　テレワーク時のセキュリティ対策を推進するに当たって

6－1　テレワークの導入に当たり、課題となった点について教えてください。（〇はいくつでも）

1　セキュリティの確保
2　テレワークに必要な端末等の整備
3　通信環境の整備（通信速度や回線の不足等）
4　テレワークに必要な場所の確保
5　テレワークをする社員の労働時間の管理
6　テレワーク業務に関する就業規則の整備
7　個々の従業員による業務の進捗管理
8　テレワークをする社員への指示・指導・評価
9　文書の電子化が進んでいないことによる業務への支障
10　書類へのサインや捺印ができないことによる業務への支障
11　取引先や顧客への対応
12　社内コミュニケーションの不足、情報共有の困難
13　テレワーク化する業務や対象となる社員の選定
14　テレワーク導入・維持に対応できる人材の不足
15　その他（　　）
16　特になし

6－2　セキュリティの確保に関して、具体的にどのような点で現時点でも課題だと感じていますか。（〇はいくつでも）

1　テレワーク時に使用する端末に、機密情報を保存してよいか
2　テレワーク時に使用する端末で、機密情報を閲覧してよいか
（オンライン会議システムを介した機密情報閲覧を含む）
3　端末の紛失のリスク
4　社内勤務時と同等のセキュリティレベルの確保の是非
5　テレワーク時の通信内容の監視
6　私用端末（BYOD）の使用許可の是非
7　その他（　　）

6－3 以下のセキュリティ対策のうち、貴社で行っているものを教えてください。（それぞれに○は一つ）

	実施している	今後、実施を検討している	実施する意向はない
①テレワークの利用者や利用端末の管理	1	2	3
②テレワーク時に使用した重要情報の把握	1	2	3
③ウイルス対策ソフトを常に最新化	1	2	3
④不審なメールに対する定期的な注意喚起	1	2	3
⑤アプリケーションのインストール制限	1	2	3
⑥重要情報へのアクセス制限	1	2	3
⑦社内システムへのアクセス制限	1	2	3
⑧WEB会議へのアクセス制限	1	2	3
⑨テレワーク端末へののぞき見防止対策	1	2	3
⑩サポート切れのOSやアプリケーションの未利用	1	2	3
⑪ソフトウェアでの最新のセキュリティアップデートの適用	1	2	3
⑫ハードウェアにおける最新のセキュリティアップデートの適用	1	2	3
⑬インシデント発生時の社内対応体制の構築	1	2	3
⑭社内システムへのアクセスログの収集	1	2	3
⑮テレワーク端末の紛失対策	1	2	3
⑯アカウント・認証管理の強固化	1	2	3
⑰管理者権限についての作業制限	1	2	3

6－4 今後もセキュリティ対策を継続するにあたって、具体的にどのような点を検討することが課題だと感じていますか。（○はいくつでも）

1　テレワーク時に使用する端末に、機密情報を保存してよいか
2　テレワーク時に使用する端末で、機密情報を閲覧してよいか
（オンライン会議システムを介した機密情報閲覧を含む）
3　端末の紛失のリスク
4　社内勤務時と同等のセキュリティレベルの確保の是非
5　テレワーク時の通信内容の監視
6　私用端末（BYOD）の使用許可の是非
7　その他（　　）

7　総務省が作成するガイドラインについて

7－1　総務省が発行している「テレワークセキュリティガイドライン※」をご存知ですか。（○は１つ）

※参考URL　https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

1　内容を見たことがあり、参考になった
2　内容を見たことがあるが、参考にならなかった
3　存在は知っていたが、内容を見たことはない
4　知らなかった

7－2　7－1で「１　内容を見たことがあり、参考になった」と回答された方に伺います。

参考になった内容について具体的に教えてください。（○はいくつでも）

1　テレワークにおいて検討すべきこと
2　クラウドサービス活用の考え方
3　ゼロトラストセキュリティの考え方
4　テレワーク方式の種類とその分類
5　適した方式を選定するフローチャートや特性比較表
6　経営者や管理者、勤務者のそれぞれの立場において必要な認識・対策
7　セキュリティ対策のポイントのセルフチェックリスト
8　セキュリティ対策の解説
9　テレワークにおけるトラブル事例と対策
10　その他（　　）

7－3 総務省では、テレワークセキュリティガイドラインの改定検討を行っています。記載を充実させた方がよいと考える内容を教えてください。（〇はいくつでも）

1	テレワーク自体のメリットや意義
2	テレワーク実施に当たって想定されるセキュリティ上の脅威：技術的な解説
3	テレワーク実施に当たって想定されるセキュリティ上の脅威：業務上の影響
4	実際に発生したセキュリティ事故の例
5	テレワークを実現するシステム構成の種類とその解説
6	テレワークを実現するシステム構成の種類ごとのメリット・デメリット（特徴）
7	自社に適したシステム構成の選び方
8	経営層が実施・認識すべきポイント
9	従業員に配布できるような注意喚起ポイント
10	セキュリティポリシー等の社内規程・ルールの事例集
11	従業員向けのセキュリティ教育コンテンツ（動画等）
12	クラウドサービス利用時のセキュリティ対策
13	モバイル端末利用時のセキュリティ対策
14	サテライトオフィスやコワーキングスペース等でのセキュリティ対策
15	テレワークのシステムやセキュリティに関する基礎的な用語集
16	「ゼロトラスト」等の最近流行の単語・概念の解説
17	参考となる他の文献
18	その他（　　）
19	特になし

７－４　総務省では、令和２年９月に新型コロナウイルスの感染拡大予防の観点等から中小企業等においてもテレワークの導入が広まる中で、最低限のセキュリティを確実に確保してもらうための手引き（チェックリスト）等を公表しました。

この「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」をご存知ですか。（〇は１つ）

※参考URL　https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

1　内容を見たことがあり、参考になった
2　内容を見たことがあるが、参考にならなかった
3　存在は知っていたが、内容を見たことはない
4　知らなかった

７－５　７－４で「１　内容を見たことがあり、参考になった」と回答された方に伺います。

参考になったのはどの部分ですか。（〇はいくつでも）

1　テレワーク方式の確認
2　テレワーク方式の解説
3　テレワーク環境で想定される脅威の解説
4　テレワーク方式毎のセキュリティ対策チェックリスト
5　テレワーク方式チェックリストの設定例一覧
6　テレワーク環境のセキュリティ対策と想定脅威一覧
7　従業員向けハンドブック（令和４年５月追加）
8　緊急時対応カード（令和４年５月追加）
9　その他（　　）

7－6　総務省では、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の改定検討を行っています。現在の手引きで理解が難しかった内容、または新たに記載を充実させた方がよいと考える内容を教えてください。（〇はいくつでも）

1　テレワーク自体のメリットや意義
2　テレワークを実施しやすい業務と実現方法
3　テレワークを実現するシステム構成の種類とその解説
4　テレワークを実現するシステム構成の種類ごとのメリット・デメリット（特徴）
5　導入・管理しやすいテレワーク方式・ツールの解説
6　テレワーク実施に当たって想定されるセキュリティ上の最新脅威と業務上の影響
7　実際に発生したセキュリティ事故の例
8　経営層が実施・認識すべきポイント
9　従業員に配布できるような注意喚起ポイント
10　セキュリティポリシー等の社内規程・ルールの事例集
11　従業員向けのセキュリティ教育コンテンツ（動画等）
12　クラウドサービス利用時のセキュリティ対策(活用ツール、守らせるルールなど)
13　モバイル端末利用時のセキュリティ対策(活用ツール、守らせるルールなど)
14　サテライトオフィスやコワーキングスペース等でのセキュリティ対策(活用ツール、守らせるルールなど)
15　テレワークのシステムやセキュリティに関する基礎的な用語集
16　「ローカルブレイクアウト」「サテライトオフィス」等のテレワーク関連の最新動向と解説
17　参考となる他の文献
18　その他（　　）
19　特になし

7－7　総務省では、よく使用するテレワーク用ソフトウェア（オンライン会議システムの場合は、Cisco WebEx Meeting・Microsoft Teams・Zoom）に関して、セキュリティ上気をつけるべき点を、具体的な設定画面付きの資料として、前述の手引き（チェックリスト）と同時に公表しています。

この「設定解説資料」をご存知ですか。（〇は１つ）

※参考URL　https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

1　内容を見たことがあり、参考になった
2　内容を見たことがあるが、参考にならなかった
3　存在は知っていたが、内容を見たことはない
4　知らなかった

7－8 以下のテレワーク用ソフトウェアのうち、今後活用したいと思う「設定解説資料」はございますか。（○はいくつでも）

1	CiscoWebexMeetings
2	Microsoft Teams
3	Zoom
4	Windows
5	Mac
6	iOS
7	Android
8	LanScope An
9	Exchange Online
10	Gmail
11	Teams_chat
12	LINE
13	OneDrive
14	Googleドライブ
15	Dropbox
16	YAMAHA VPNルータ
17	Cisco ASA
18	Windowsリモートデスクトップ
19	Chromeリモートデスクトップ
20	Microsoft Defender
21	ウイルスバスター ビジネスセキュリティサービス
22	その他（　　）
23	特になし

７－９ 次のキーワードについて、それぞれ該当するものをお答えください。（それぞれ○は１つ）

① マルウェア	1 意味がわかる	2 聞いたことがある	3 分からない
② ランサムウェア	1 意味がわかる	2 聞いたことがある	3 分からない
③ Emotet	1 意味がわかる	2 聞いたことがある	3 分からない
④ 標的型攻撃	1 意味がわかる	2 聞いたことがある	3 分からない
⑤ DDos攻撃	1 意味がわかる	2 聞いたことがある	3 分からない
⑥ シンクライアント	1 意味がわかる	2 聞いたことがある	3 分からない
⑦ リモートデスクトップ	1 意味がわかる	2 聞いたことがある	3 分からない
⑧ VPN	1 意味がわかる	2 聞いたことがある	3 分からない
⑨ IDS/IPS	1 意味がわかる	2 聞いたことがある	3 分からない
⑩ BYOD	1 意味がわかる	2 聞いたことがある	3 分からない
⑪ ゼロトラスト	1 意味がわかる	2 聞いたことがある	3 分からない
⑫ 多要素認証	1 意味がわかる	2 聞いたことがある	3 分からない
⑬ IaaS/PaaS/SaaS	1 意味がわかる	2 聞いたことがある	3 分からない
⑭ WEP/WPA/WPA2	1 意味がわかる	2 聞いたことがある	3 分からない
⑮ タイムスタンプ	1 意味がわかる	2 聞いたことがある	3 分からない
⑯ eシール	1 意味がわかる	2 聞いたことがある	3 分からない
⑰ eデリバリー	1 意味がわかる	2 聞いたことがある	3 分からない