小林勝哉
社会保険労務士事務所

情報セキュリティに苦手意識のある方必見!

テレワーク時のセキュリティ対策総点検セミナー

2023年11月28日

小林勝哉社会保険労務士事務所

自己紹介

小林勝哉

小林勝哉社会保険労務士事務所

特定社会保険労務士

元NTTのIT専門家で、経済産業省とソフトウェア分野の産官学の交流推進等にも従事。
現在は、厚生労働省委託事業 東京テレワーク推進センター相談コーナーにて、専門相談員とコンサルタントを担当。
テレワーク専門社労士として、IT×法律で新たな事業価値の創造に取り組んでいる。

目次

情報セキュリティに苦手意識のある方必見!
テレワーク時のセキュリティ対策総点検セミナー

小林勝哉
社会保険労務士事務所

情報セキュリティ事故による企業や社員の損害の増大

情報セキュリティ10大脅威 2023脅威ランキング

小林勝哉
社会保険労務士事務所

「個人」向け脅威	順位	「組織」向け脅威
フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害
ネット上の誹謗・中傷・デマ	2	サプライチェーンの弱点を悪用した攻撃
メールやSMS等を使った 脅迫・詐欺の手口による金銭要求	3	標的型攻撃による機密情報の窃取
クレジットカード情報の不正利用	4	内部不正による情報漏えい
スマホ決済の不正利用	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
不正アプリによる スマートフォン利用者への被害	6	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）
偽警告によるインターネット詐欺	7	ビジネスメール詐欺による金銭被害
インターネット上のサービスからの 個人情報の窃取	8	脆弱性対策情報の公開に伴う悪用増加
インターネット上のサービスへの 不正ログイン	9	不注意による情報漏えい等の被害
ワンクリック請求等の 不当請求による金銭被害	10	犯罪のビジネス化 （アンダーグラウンドサービス）

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

クラウドもランサムウェアで暗号化され情報窃取される時代

株式会社エムケイシステムのクラウドサービスがランサムウェアによる攻撃に

2023年６月21日

各　　位

会 社 名　株式会社エムケイシステム
代表者名　代 表 取 締 役 社 長　三宅　登
（コード番号：3910　東証スタンダード）
問合せ先　取締役 管理統括　吉田 昌基
（TEL. 06-7222-3394）

第三者によるランサムウェア感染被害への対応状況のお知らせ（第２報）

当社は、2023年６月６日付「第三者によるランサムウェア感染被害のお知らせ」及び2023年６月９日付「第三者によるランサムウェア感染被害への対応状況のお知らせ」にて公表しました通り、当社サービスを提供しているデータセンター上のサーバーがランサムウェアによる第三者からの不正アクセスを受けました。

現在も調査及び復旧作業を継続しておりますが、現時点で判明している事実関係及び当社の対応について、以下の通りお知らせいたします。

関係各位の皆様におかれましては、ご迷惑をおかけすることになり、誠に申し訳ございません。深くお詫び申し上げます。

１．発覚の経緯

・６月５日(月)６：00頃、データセンター上の当社サーバーがダウンした事が判明。
・同７：00頃、インフラ担当者がIDCデータセンターへ直行し、状況を確認。調査を開始。
・画面上にランサムウェアらしき警告文を確認。不正アクセスの可能性が高まったため直ちに関連するインターネット回線を切断。その後外部専門家も合流の上、引き続き状況調査を行った結果、ランサムウェアによる第三者からの不正アクセスと断定。

（出典）株式会社エムケイシステム
第三者によるランサムウェア感染被害への
対応状況のお知らせ（第2報）
2023/6/5発生
https://contents.xj-storage.jp/xcontents/AS97180/fd524

クラウドもランサムウェアで暗号化され情報窃取される時代

株式会社エムケイシステムのクラウドサービスの管理する膨大な個人情報

あなたのオフィスへ、革新的な効率をご提供

Providing an Innovative Efficiency to Your Office

株式会社エムケイシステムは社会保険、労働保険の申請手続き業務支援、
給料計算・就業管理・給料明細配信業務支援システムのクラウドサービスを全国の
2700を超える社労士事務所と顧問先企業96万事業所に提供しています。

社労士事務所
2,754
2023年4月1日現在

年間累計電子申請
366万件以上
2022年4月～2023年3月

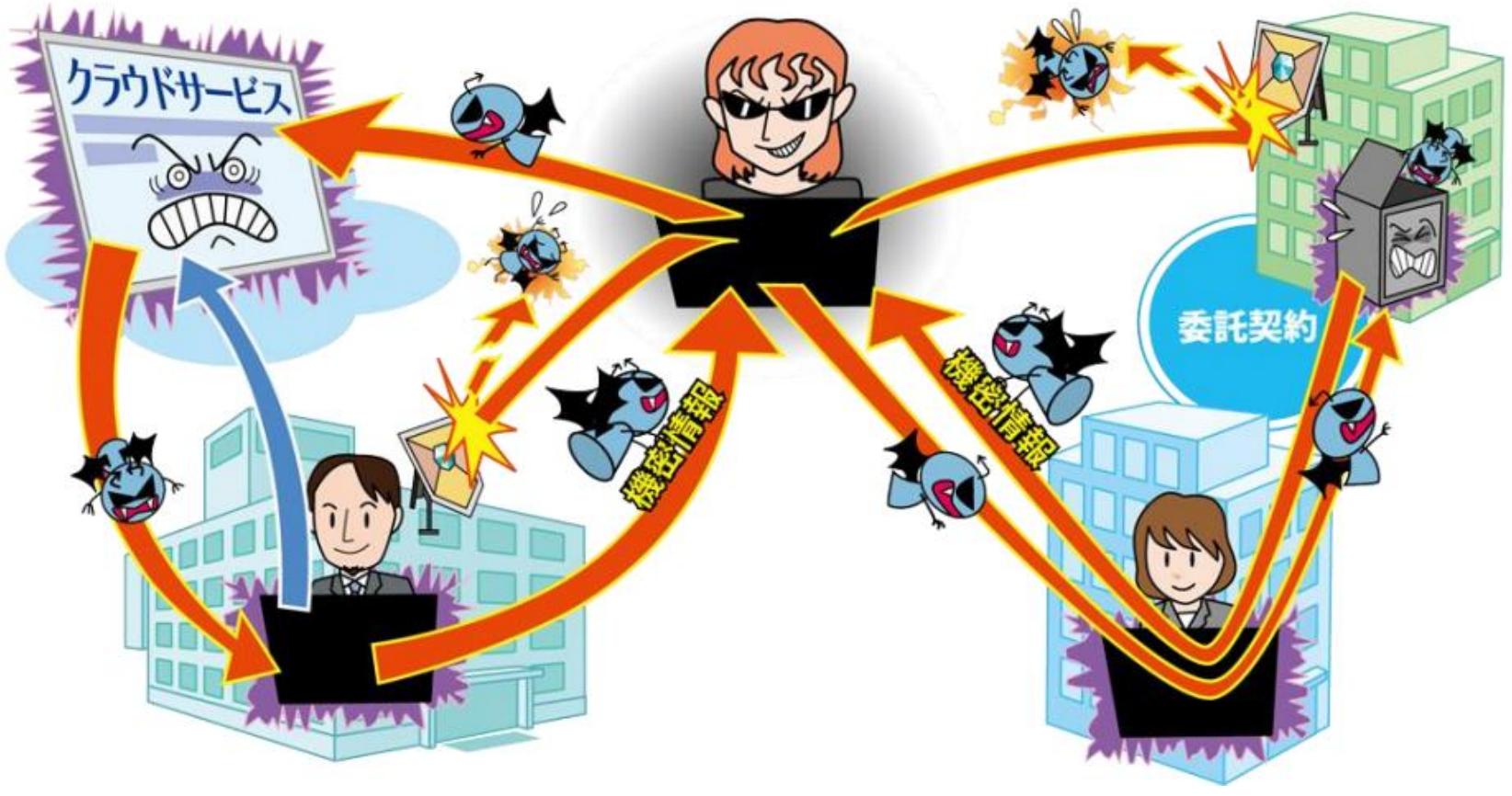
管理事業所
約57万事業所
2023年4月1日現在

社労夢で管理する在職者数
約826万名 （その他退職者数 1,273万名）
2023年4月1日現在

（出典）株式会社エムケイシステム　一目でわかるエムケイシステム　2023/4/1現在
https://www.mks.jp/company/ir-information/ataglance/

サプライチェーンの弱点をついて中小企業が狙われる時代

・自組織だけでなく、委託先や利用しているサービスも適切な管理を



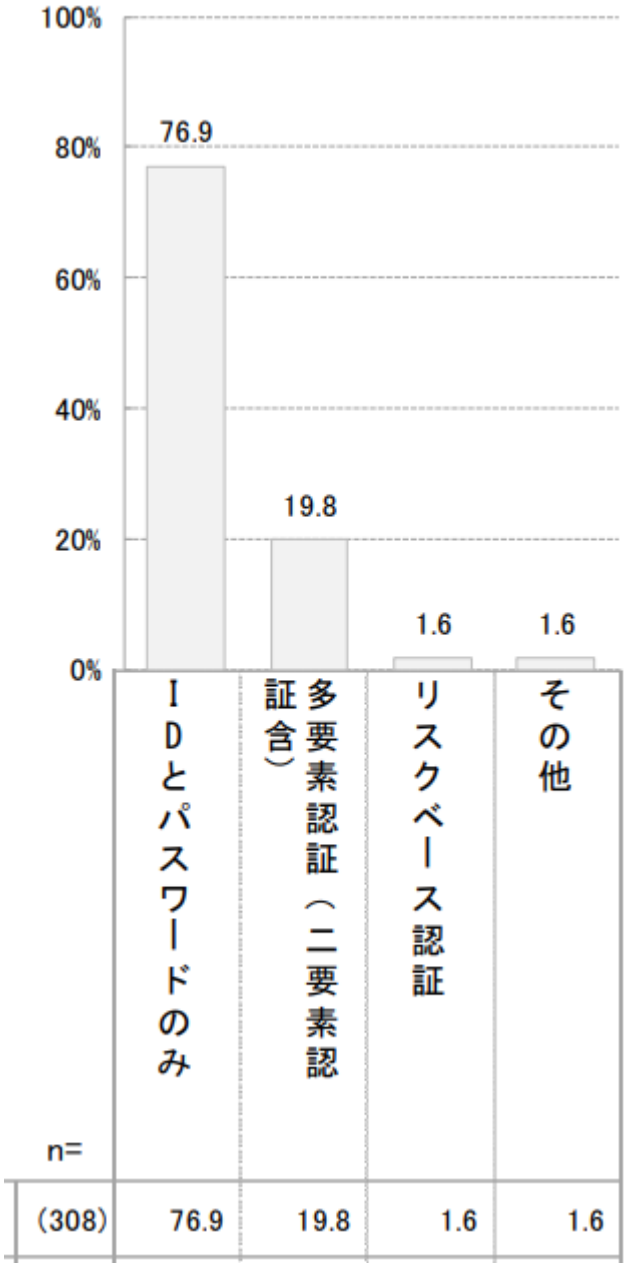
（出典）IPA　情報セキュリティ10大脅威 2023
https://www.ipa.go.jp/security/vuln/10threats2023.html

サプライチェーンの弱点をついて中小企業が狙われる時代

弱点の例　Webサイトの認証方法

2019年の調査では、Webサービス事業者の認証方法は「IDとパスワードのみ」が7割超を占めていました。

各事業者で、多要素認証などのセキュリティ強化が進められていますが、会社で業務利用されているWebサービスの対策強化を踏まえ、認証方法を強化済でしょうか。



（出典）フィッシング対策協議会　インターネットサービス提供事業者に対する「認証方法」に関するアンケート調査結果　2018/7/1
https://www.antiphishing.jp/news/pdf/wg_auth_report01_20190701.pdf

サプライチェーンの弱点をついて中小企業が狙われる時代

１・サプライチェーンとは

大企業と中小企業とは、インターネットなどで有機的に接続されています。

ハッカーは、大企業は高度な対策と体制をもって防御しているため、対策が進んでいない**中小企業を狙って取引先のメールアドレスなどを取得**。

その後、「なりすまし」や「踏み台」攻撃で取引先の大企業を攻撃します。

２・サイバーセキュリティ保険の必要性

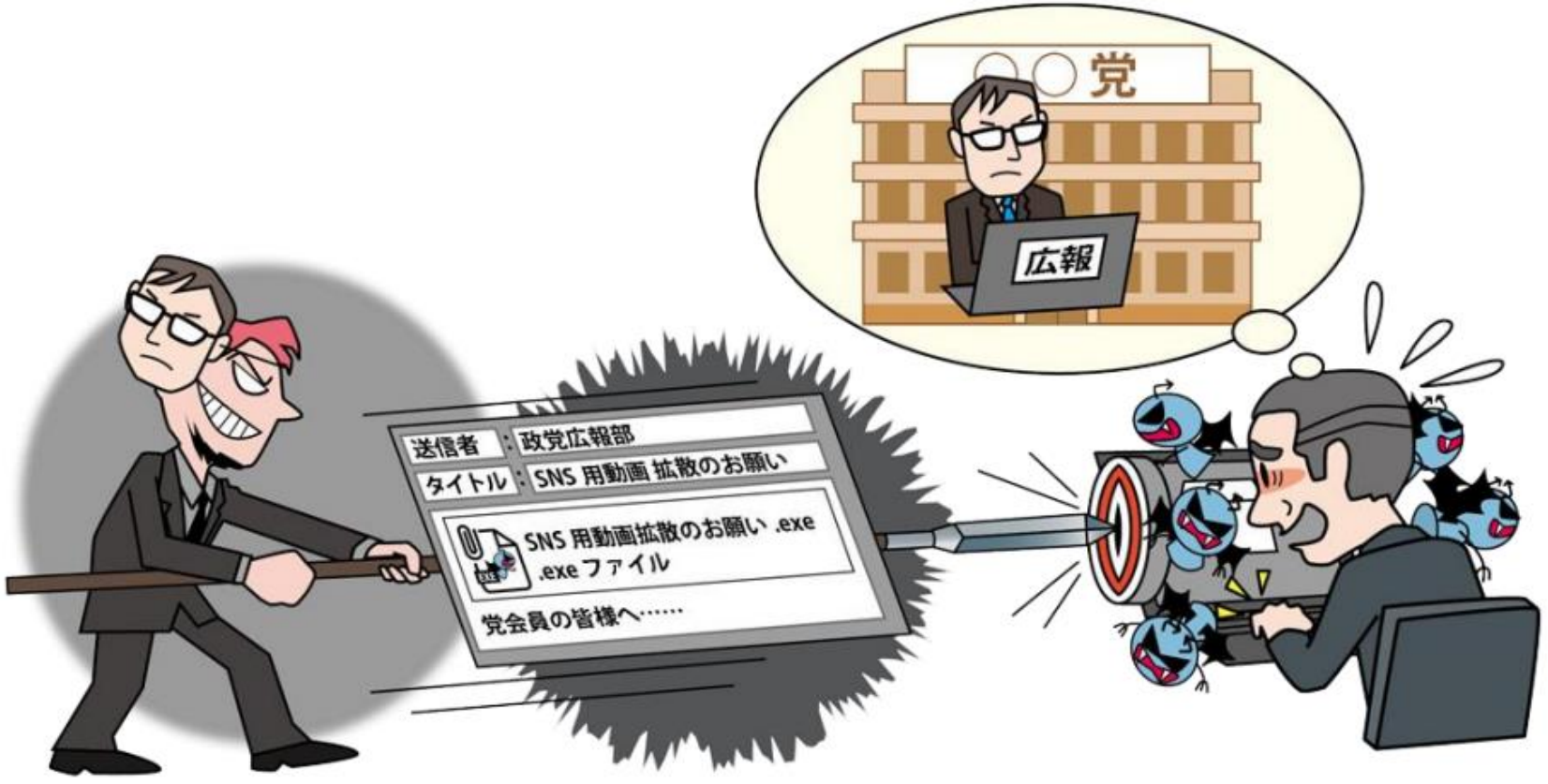
セキュリティ対策を取っていないと、取引先に損害を発生させることとなり、損害賠償や風評被害など**大きなビジネスリスク**を負うこととなります。

このようなリスクに備え、「サイバーセキュリティ保険」が必須の時代に。

標的型攻撃の侵入経路は電子メールが６割

小林勝哉
社会保険労務士事務所

・メールが来たらまず疑え！意識は常に高く



標的型メール訓練は実施していますか？

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

情報セキュリティ被害の侵入経路は電子メールが６割

・過去1年間に情報セキュリティ被害にあったか否か

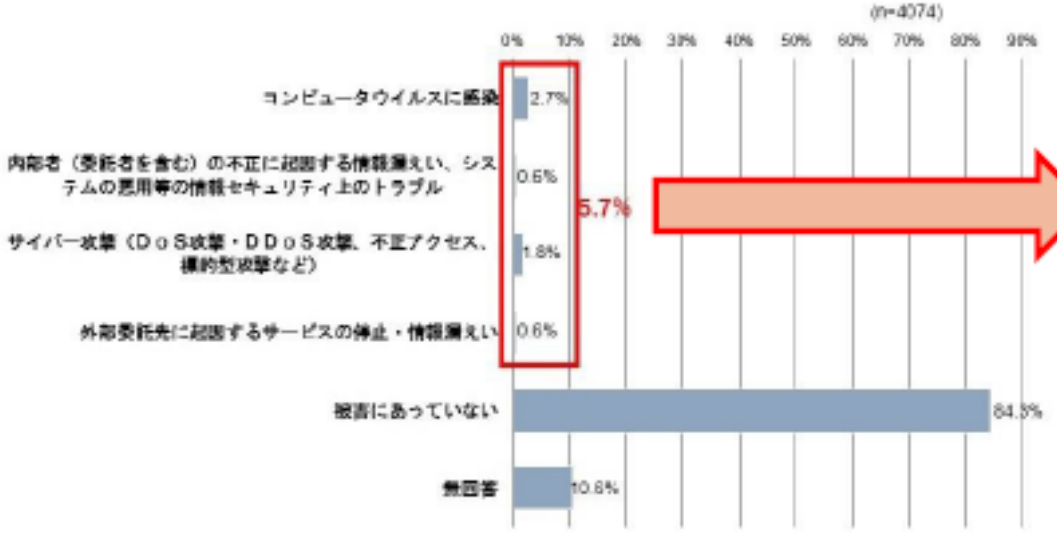
「被害にあっていない」が84.3%、**何らかの被害にあったが5.7%。最多は「ウィルス感染」。**

・コンピュータウィルスの被害を認識している企業のうち

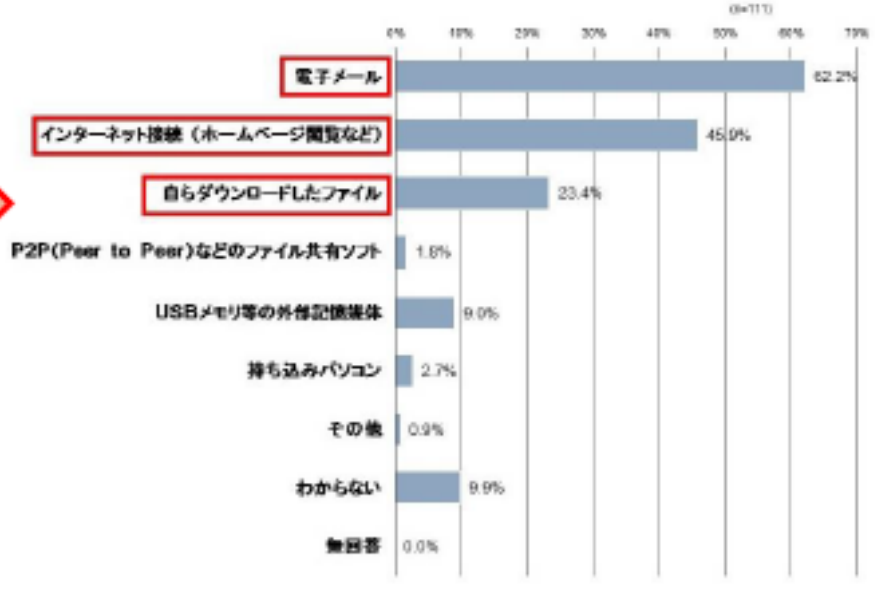
想定される侵入経路は「電子メール」が62.2%、

次いで「インターネット接続（閲覧など）」（45.9%）、「自らダウンロード」（23.4%）。

【2020年度における情報セキュリティ被害の有無】



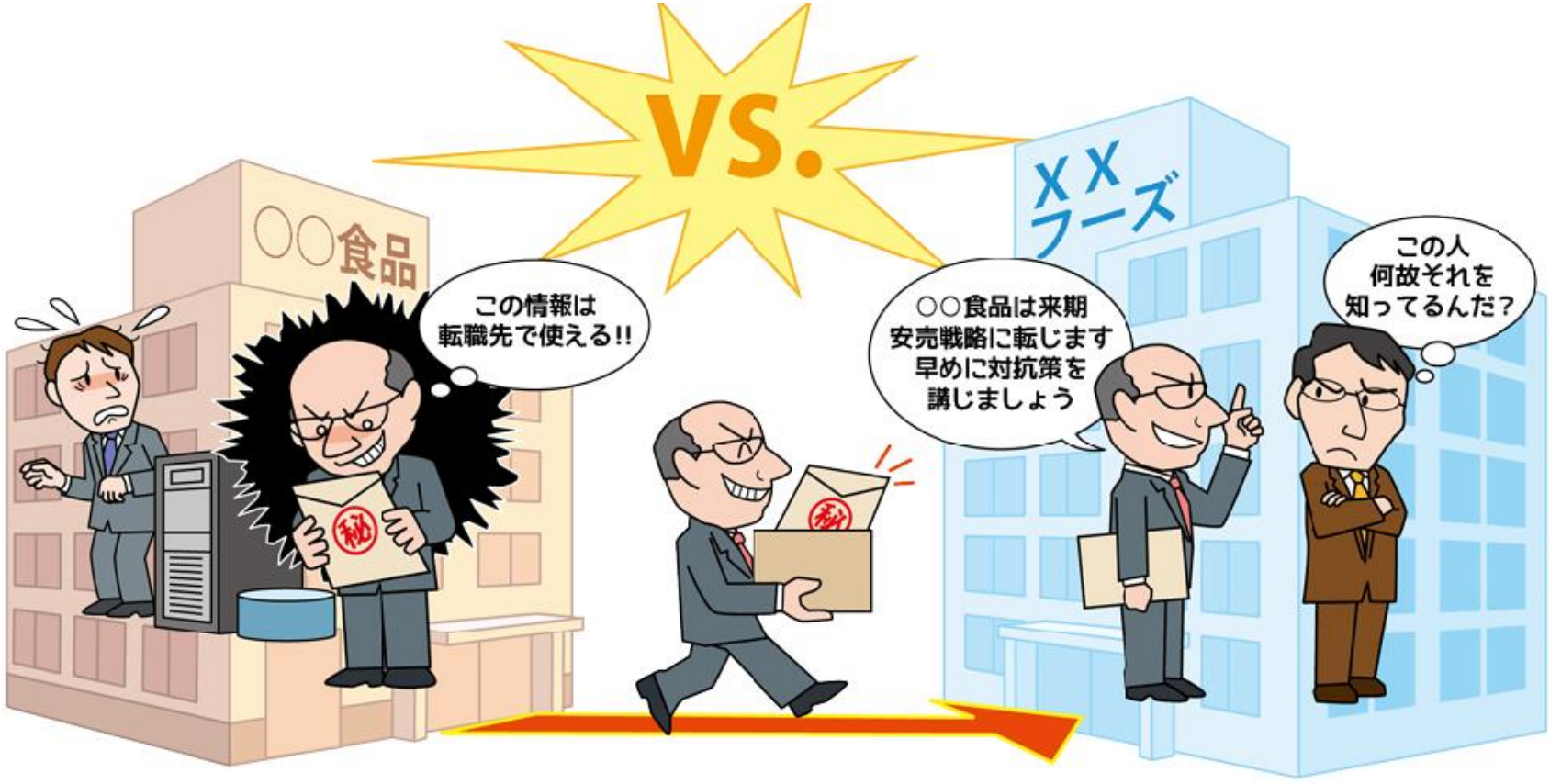
**【感染あるいは発見した
コンピュータウイルスの想定される侵入経路】**



（出典）IPA「2021年度 中小企業における情報セキュリティ対策に関する実態調査」報告書
https://www.ipa.go.jp/security/fy2021/reports/sme/index.html

内部不正による情報漏洩が増加しています

・不正に情報を取得しない、取得させない、使用しない！



異動や離職に際し、利用者ID等は直ちに削除していますか？

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

内部不正による情報漏洩が増加しています

内部不正防止ガイドラインの【10の観点】で規程をチェックしよう！

（主に情報セキュリティ規程に反映すべき規定）

1. 基本方針、2. 資産管理、3. 物理的管理、
4. 技術・運用管理、5. 原因究明と証拠確保

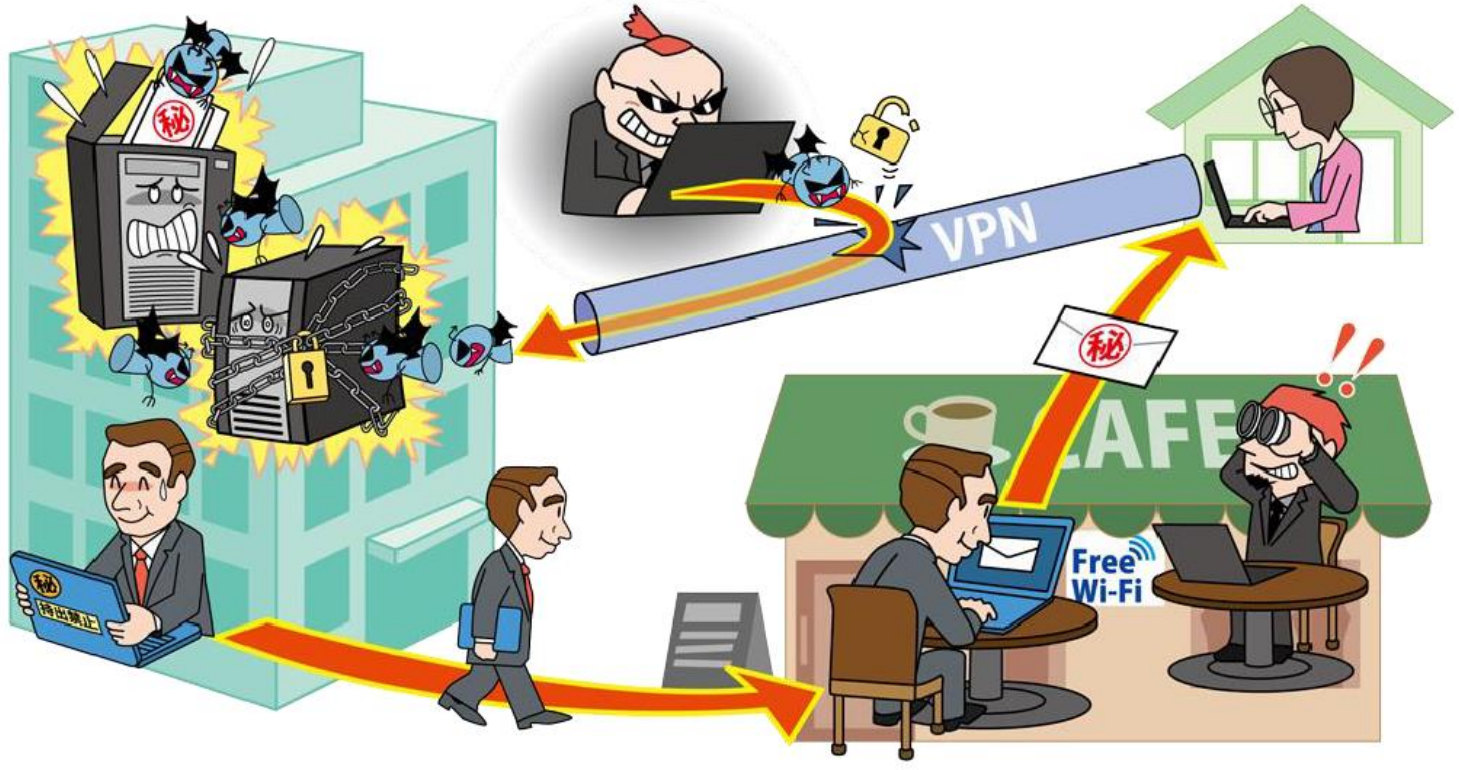
（主に就業規則に反映すべき規定）

6. 人的管理、7. コンプライアンス、8. 職場環境、
9. 事後対策、10. 組織の管理

（出典）IPA「組織における内部不正防止ガイドライン」 2022年4月6日
https://www.ipa.go.jp/security/fy24/reports/insider/

テレワーク等の働き方を狙った攻撃が増加しています

・環境の変化で脆弱な箇所が増えたテレワーク環境が狙われる！



→事例研究してみましょう

テレワーク環境における情報セキュリティ事故の事例

テレワーカーが気を付けたい典型的なシーン別対策

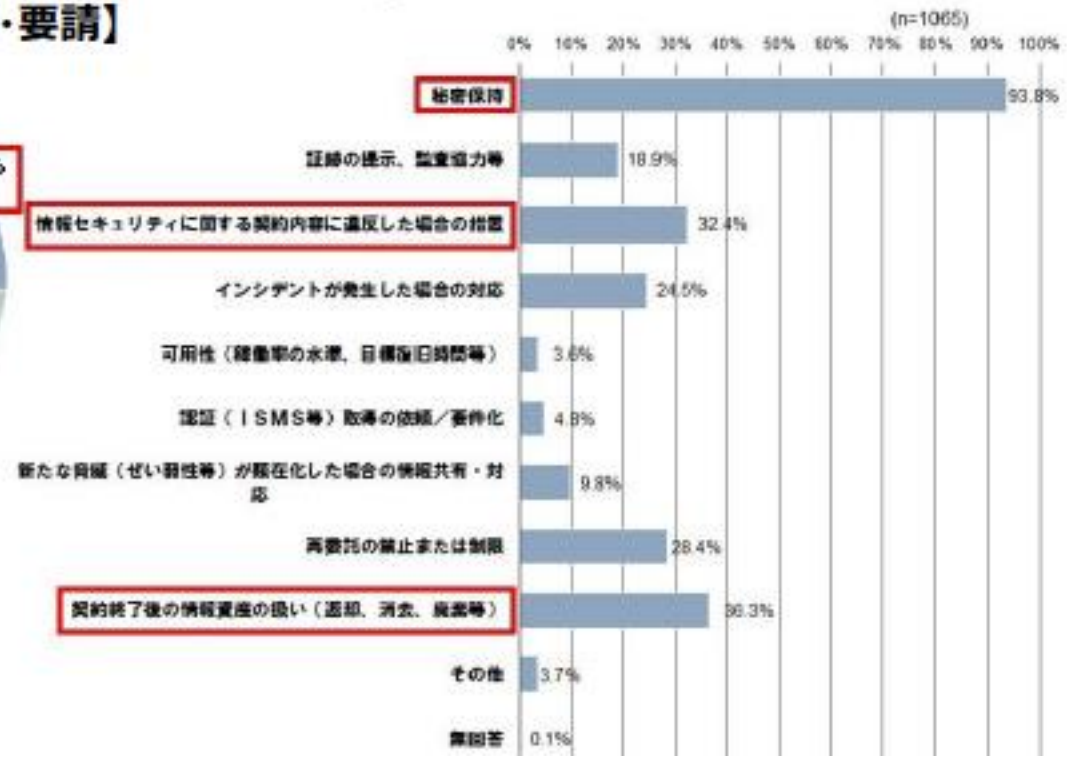
（出典）IPA　情報セキュリティ10大脅威 2023
https://www.ipa.go.jp/security/vuln/10threats2023.html

取引先からの義務・要請は「秘密保持」が９割

・取引先からの情報セキュリティに関する条項・取引上の**「義務・要請はない」が63.2%**。
・「義務・要請がある」企業（26.1%）のうち、**契約時の要請としては「秘密保持」が93.8%**、
次いで「契約終了時の情報資産の扱い（返却、消去、廃棄等）」（36.3%）、
「情報セキュリティに関する契約内容に違反した場合の措置」（32.4%）。

【販売先・仕入先からの情報セキュリティに関する条項・取引上の義務・要請】

【契約時における情報セキュリティに関する要請】



（出典）IPA「2021年度 中小企業における情報セキュリティ対策に関する実態調査」報告書
https://www.ipa.go.jp/security/fy2021/reports/sme/index.html

小林勝哉
社会保険労務士事務所

テレワーク環境における
情報セキュリティリスクの増大

小林勝哉
社会保険労務士事務所

1・テレワークの利用実態（テレワーク人口実態調査）

■勤務地域別の雇用型就業者のテレワーク実施状況

全国平均　26.1%（0.9ポイント減）

首都圏　40.0%（2.3ポイント減）

地方都市　17.5%（ 0.3ポイント増）

■調査の有効サンプル数

26万人に調査票を送り、40,000人回収（うち、テレワーカー10,469人）

■テレワーカー　VS　非テレワーカー

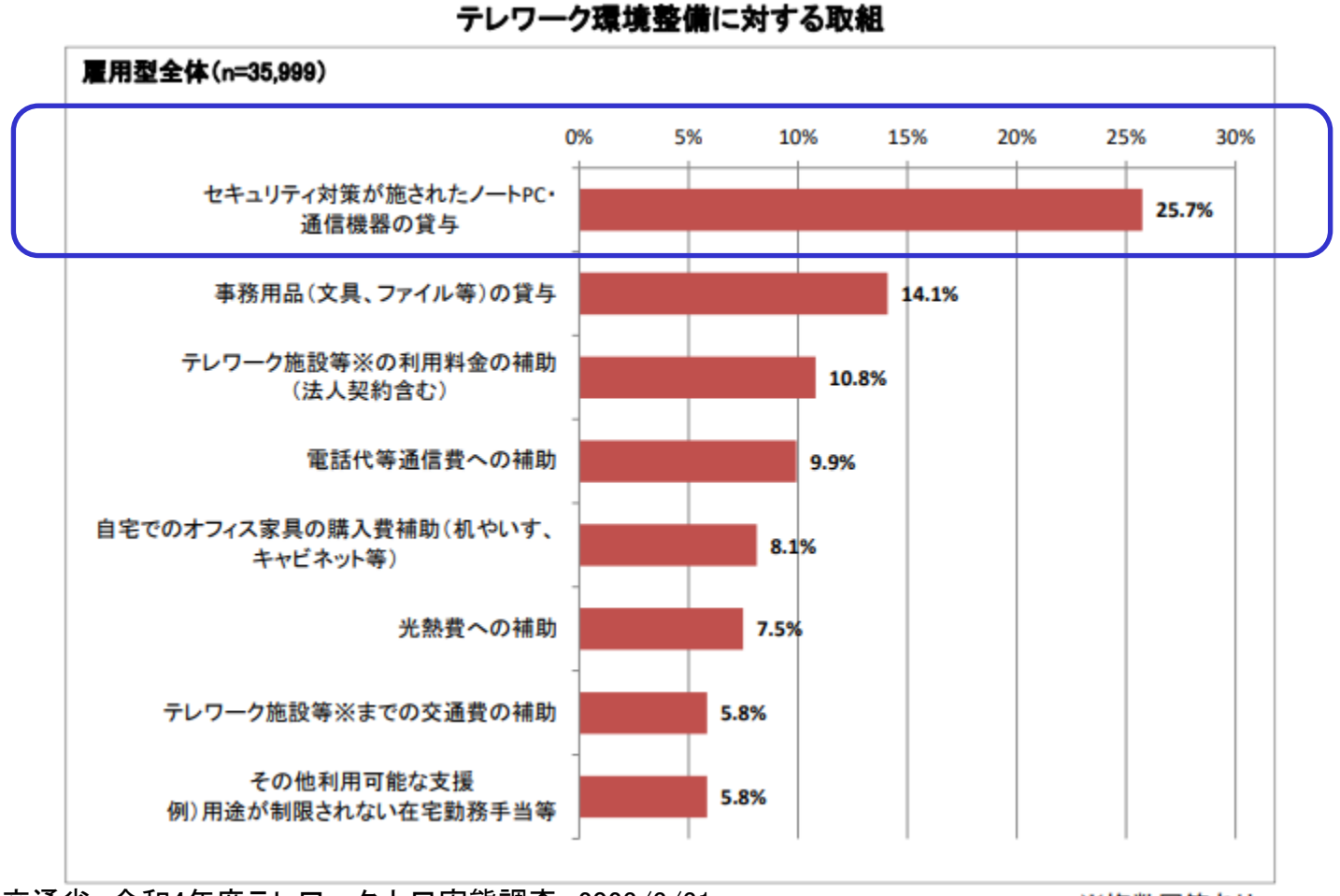
現在の主な仕事でこれまで、テレワークをしたことがある　VS　ない

（出典）国土交通省　令和4年度テレワーク人口実態調査　2023/3/31
https://www.mlit.go.jp/report/press/toshi03_hh_000099.html

小林勝哉
社会保険労務士事務所

2・テレワーク環境整備に対する取組

「セキュリティ対策が施されたノートPC・通信機器の貸与」 25.7%



（出典）国土交通省　令和4年度テレワーク人口実態調査　2023/3/31
https://www.mlit.go.jp/report/press/toshi03_hh_000099.html

※複数回答あり

小林勝哉
社会保険労務士事務所

３・企業規模別のテレワーク環境整備に対する取組

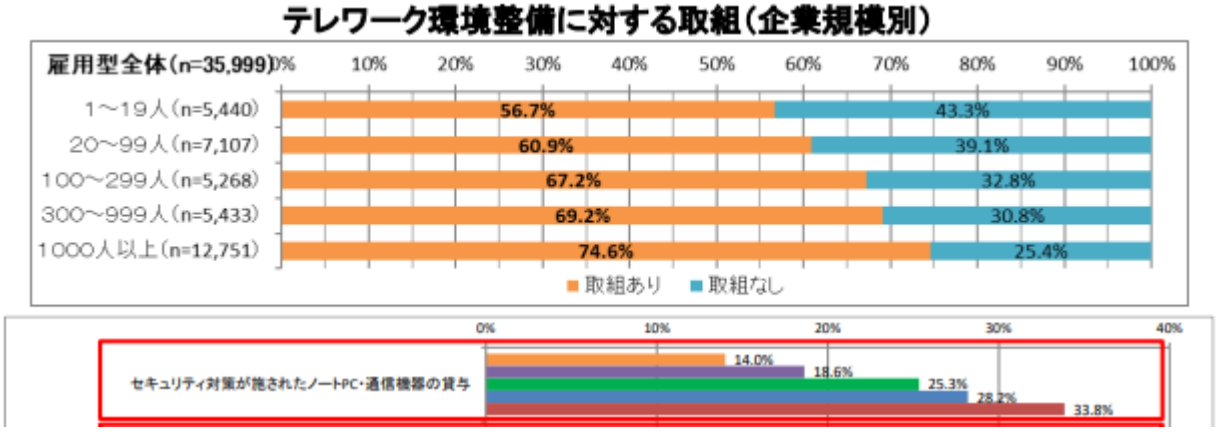
「セキュリティ対策が施されたノートPC・通信機器の貸与」 企業規模で差

平均　25.7%

1000人以上の企業　33.8%

1～19人の企業　14.0%

中小企業のテレワーク・セキュリティ対策の壁



（出典）国土交通省　令和4年度テレワーク人口実態調査　2023/3/31
https://www.mlit.go.jp/report/press/toshi03_hh_000099.html

テレワーク環境で何が変わったのか

１・働く場所

働く場所が、在宅勤務、モバイル勤務、サテライトオフィス勤務、ワーケーションなど、オフィス外に拡大しました。

これにより、情報の持ち出し、情報通信機器の紛失・盗難、ネットワークの接続経路、家族等による秘密情報への接触、オンライン会議の定着などリスクが増大しています。

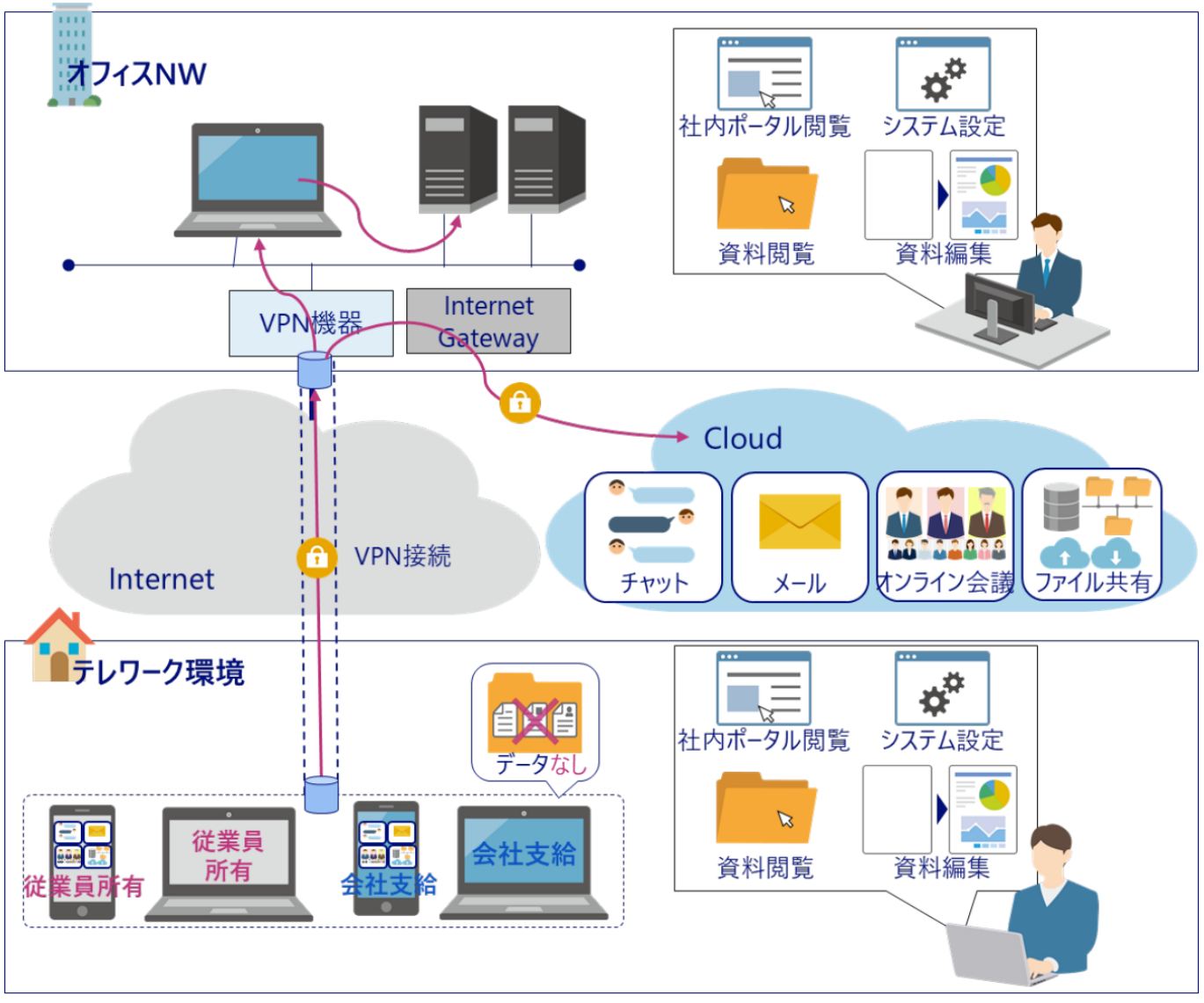
２・情報資産の格納場所

情報資産の格納場所が、社内ネットワークのファイルサーバーや業務システムから、クラウド上のファイルサービスや業務システムへ拡大しています。

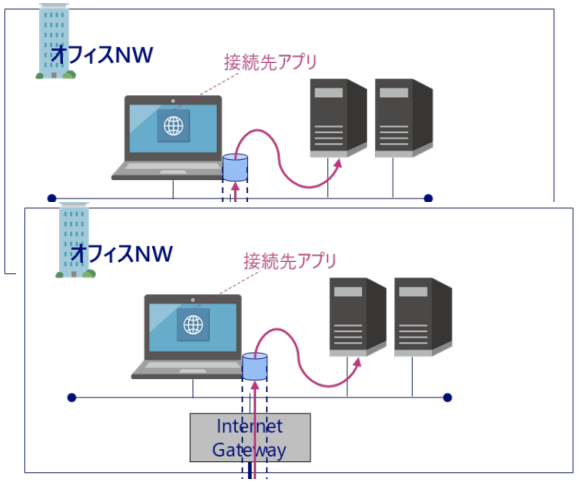
３・情報資産の管理方法

情報資産の管理方法が、書類の電子化、業務のデジタル化により、物理的な鍵管理から電子的なアクセス権管理に管理方法が拡大しています。

テレワーク環境のITインフラの変化



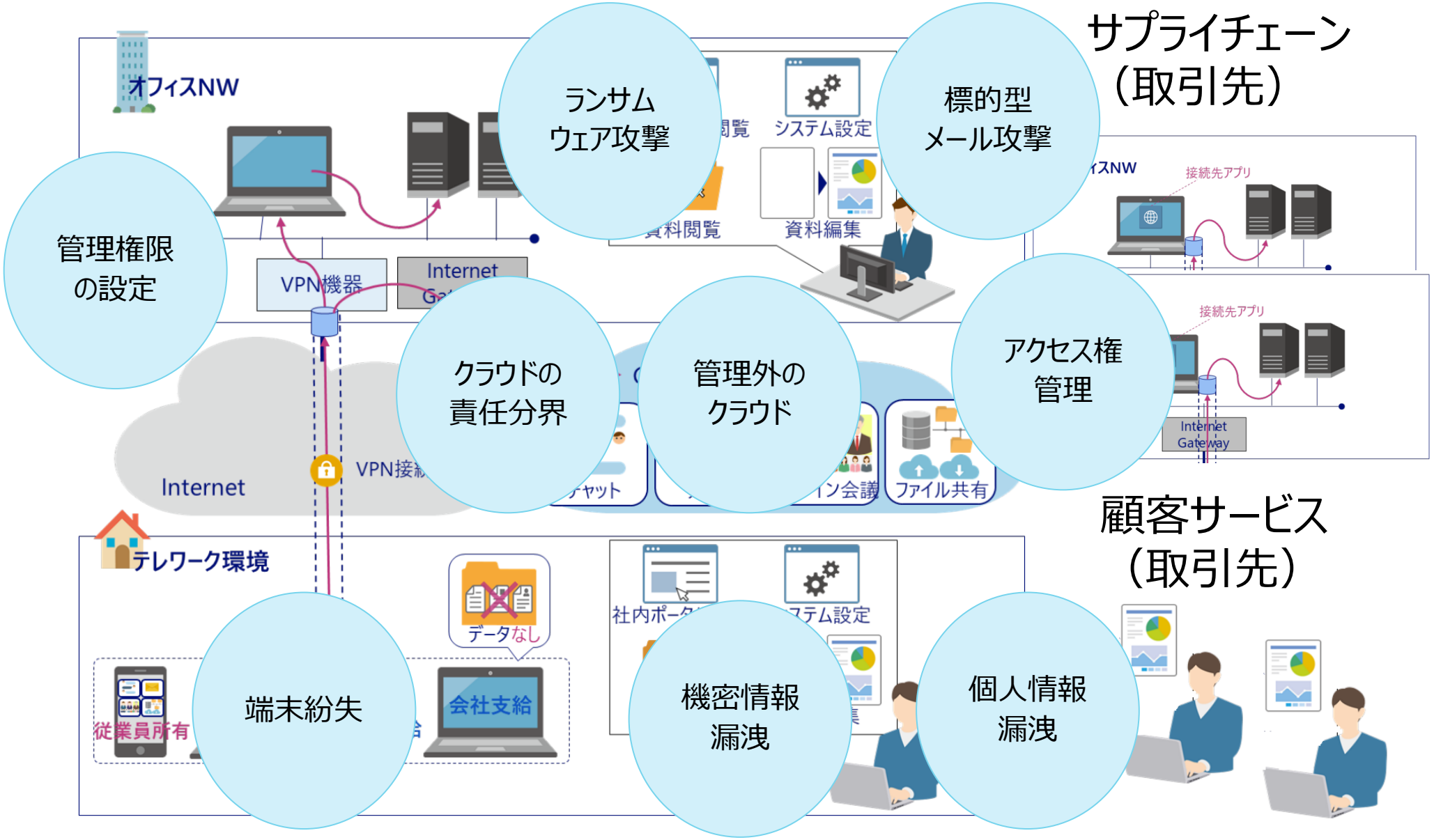
サプライチェーン（取引先）



顧客サービス（取引先）

（出典）総務省　テレワークセキュリティガイドライン（第5版）　2021/5/31　筆者加筆
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

テレワーク環境の情報セキュリティリスクの増大



（出典）総務省　テレワークセキュリティガイドライン（第5版）　2021/5/31　筆者加筆
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

テレワーク環境における情報セキュリティ事故の事例

テレワーク環境における
情報セキュリティ事故の事例を考える

小林勝哉
社会保険労務士事務所

事例１　フィッシングによる個人情報等の漏洩

取締役が偽不在通知SMSにだまされパスワード入力

事例２　PC管理の不備で偽ソフトインストール

業務委託先で偽セキュリティ警告にだまされ情報漏洩か

事例３　VPN、Wi-Fiルータなどのセキュリティの脆弱性

推測可能なVPNパスワードでランサムウェア被害

事例４　クラウドだから安心？会社管理外のクラウドの利用

採用活動に関する個人情報が外部から閲覧可能な状態に

（出典）2023年4月～5月の各社報道発表資料から

取締役が偽不在通知SMSにだまされパスワード入力

小林勝哉
社会保険労務士事務所

事例１　大手出版社

個人情報漏洩に関するご報告とお詫び

このたび、弊社取締役が使用する会社貸与スマートフォンから、同スマートフォンに登録されていた個人情報が漏洩したおそれがあることが判明しました。社内調査のうえ、個人情報が漏洩した可能性がある方々には個別に連絡を差し上げ、お詫びと説明をさせていただいております。

取引先、関係先の皆さまに多大なるご心配をおかけしておりますことを深くお詫び申し上げます。

現時点で判明している事実について、以下の通りご報告いたします。引き続き調査のうえ、新たな事実が判明した場合には、当サイトにてあらためてお知らせいたします。なおこれまでに、個人情報の漏洩による被害発生の報告はございません。

（出典）大手出版社報道発表　2023/4/4発生

取締役が偽不在通知SMSにだまされパスワード入力

1・事象

会社貸与スマートフォンに、宅配業者を装った不在通知のSMSが届き、それを真正の不在通知と誤認してアカウント、パスワードを入力。

スマートフォンに登録されていた302件の「氏名」「電話番号」「メールアドレス」（一部「住所」「会社名」含む）が漏洩したおそれ。

2・原因（推定）

SMSによる攻撃について意識が低く、真正の通知と誤認したため。

会社貸与機器に登録する個人情報を、最小限としていなかったため。

3・再発防止策

あらためて全社に対してアカウントの適切な管理や個人情報の取扱いについて指導を徹底するとともに、セキュリティ対策の継続的な強化に努め、再発防止に取り組む。

（出典）大手出版社報道発表　2023/4/4発生

業務委託先で偽セキュリティ警告にだまされ情報漏洩か

事例２　地方自治体（委託先）

青梅市ファミリー・サポート・センターのパソコンへの不正アクセスによる個人情報の漏えいのおそれのある事故の発生について

このたび「青梅市ファミリー・サポート・センター事業」の委託先において、青梅市ファミリー・サポート・センターの会員情報を管理するパソコンが不正アクセスを受ける事態が発生いたしました。

関係する皆様には、大変ご迷惑とご心配をおかけいたしますことを深くお詫び申し上げます。

青梅市ファミリー・サポート・センターについて

1 概要

令和５年４月２７日午後１時３０分頃、委託先の従業員が本件業務に使用しているパソコンの画面にセキュリティ警告とともに、Microsoftサポートに電話するよう、連絡先が表示されました。
当該従業員は当該連絡先が正規のサポートセンターであると信じて連絡し、電話先のオペレーターの指示に従ってパソコンを操作したところ、身代金を要求するような表示が画面に出たことから、不正アクセスを受けたことが発覚しました。
当該不正アクセスによって委託先の保有する個人情報が漏えいしたかどうかにつきましては、現在調査中です。

2 漏えいしたおそれがある保有個人情報の項目

平成１８年９月２７日から令和５年４月２７日までに会員登録のあった1,695人の方の以下の情報となりま

（出典）青梅市　青梅市ファミリー・サポート・センターのパソコンへの不正アクセスによる個人情報の漏えいのおそれのある事故の発生について　2023/4/27発生
https://www.city.ome.tokyo.jp/soshiki/34/68110.html

業務委託先で偽セキュリティ警告にだまされ情報漏洩か

1・事象

委託先の従業員が、業務用PCの画面にセキュリティ警告とMicrosoft社に電話するよう連絡先が表示され、正規のサポートセンターであると信じて指示に従いPCを操作したところ、身代金要求が表示された。

会員登録のあった1,695人（育児の援助をおこなう人（提供会員）と育児の援助を受ける人（利用会員））の情報が、漏洩したおそれ。

2・原因

正規のサポートセンターであると信じて、攻撃者からの指示で何らかのソフトウェアをインストールしたと思われる。

3・再発防止策

委託先に対し情報管理体制の調査を行ったうえで、適切な指導を行う。

（出典）青梅市　青梅市ファミリー・サポート・センターのパソコンへの不正アクセスによる個人情報の漏えいのおそれのある事故の発生について　2023/4/27発生
https://www.city.ome.tokyo.jp/soshiki/34/68110.html

推測可能なVPNパスワードでランサムウェア被害

事例３　大手建設会社

本件事象の概要

2023年4月2日、当社が運用管理するサーバーの異常を検知するアラートにより、当該サーバーに記録されていたデータの一部がランサムウェアにより暗号化され、使用できない状況となったことが発覚いたしました。

当社は、当該サーバーをネットワークから遮断するなどの被害拡大防止策を速やかに講じたうえで、外部専門家の協力のもと対策チームを設置し、2023年4月5日には、警察当局に被害申告を行いました。また、2023年4月6日には、情報漏洩等の被害の事実は確認されておりませんでしたが、そのおそれがあったことから、個人情報保護委員会への報告を行い、同時に第三者機関に調査を依頼しました。

同調査の結果、現時点において、個人情報やお客様の情報が外部に持ち出された痕跡や外部において不正に公開されているなどの事実は確認されておりません。

本件事象の原因

第三者機関の調査によると、当社が管理運用していたVPN機器の管理アカウントのパスワードが推測可能なものであったため、当社が導入していたVPN機器を経由して当社内サーバー等への不正なアクセスに利用されていたとのことでした。また、従来よりVPN機器による通信の暗号化やクライアント端末のセキュリティ対策は行っておりましたが、当社内サーバー領域にランサムウェア対策セキュリティソフトが導入されておらず、当社内サーバー等におけるランサムウェアの実行や社内システムネットワークでの不正な活動を防ぐことができませんでした。

（出典）大手建設会社報道発表　2023/4/2発生

推測可能なVPNパスワードでランサムウェア被害

1・事象

自社サーバーに記録されていたデータの一部が、ランサムウェアにより暗号化され、使用できない状況に。

自社サーバーで管理の個人情報やお客様の情報が、漏洩したおそれ。

2・原因

自社VPN機器の管理アカウントのパスワードが推測可能なものであったため、VPN機器を経由して不正アクセス。

社内サーバー領域に、ランサムウェア対策セキュリティソフトが未導入。

3・再発防止策

VPN機器を含む管理者アカウントのパスワードの変更、サーバーも含めたXDR（不正アクセスの兆候や不審な挙動を検知）導入など技術的施策、ネットワーク全体の見直しや新システム移行を検討。

（出典）大手建設会社報道発表　2023/4/2発生

採用活動に関する個人情報が外部から閲覧可能な状態に

事例４　ウェブサービス企画運営会社

概要

当社グループの採用に関する情報がインターネット上で閲覧可能になっているとの指摘を受けて事実関係を調査したところ、一部の個人情報がインターネット上で閲覧可能な状態にあったことが社内監査により判明いたしました。クラウドサービス上で作成したファイルで採用に関わる個人情報を管理しておりましたが、閲覧範囲を「このリンクを知っているインターネット上の全員が閲覧できます」と設定したことから、リンクを知っていれば誰でも閲覧できる状態であり、一部の方の「氏名」「学校名」「メールアドレス」「電話番号」「口座番号」などの個人情報がインターネット上において閲覧できる状態でありました。

（出典）ウェブサービス企画運営会社報道発表　2022/5/16発表

採用活動に関する個人情報が外部から閲覧可能な状態に

1・事象

一部の方の「氏名」「学校名」「メールアドレス」「電話番号」「口座番号」などの採用活動に関する個人情報がインターネット上で閲覧できる状態。

学生やグループ従業員の5,800名を超える方の情報が漏洩したおそれ。

2・原因（推定）

一般的に利用できるクラウドを業務利用し、個人情報を管理。

閲覧範囲を「インターネット上の全員」と設定し、リンクを知っていれば誰でも閲覧できる状態に。

3・再発防止策

クラウドのアクセス範囲設定を見直し、個人情報を含むすべてのデータへのアクセス制限を実施。また、会社で管理されているクラウドの利用を徹底。アカウントのIDやパスワードを情報システム部門による厳格な管理に。

（出典）ウェブサービス企画運営会社報道発表　2022/5/16発表

個人情報の取扱いにおける事故の事例

設定不備による事故の事例（クラウドサービスやテレワーク環境の設定不備）

個人情報保護委員会に実際に報告された、**システム環境等で発生**した個人情報の漏えい事案の発生パターンです。

- ✓ 事例１ 本来は非公開とすべきクラウドサービス上の個人情報を誤って公開
- ✓ 事例２ クラウドサービスへのログイン認証が十分でなく不正ログインを受けた
- ✓ 事例３ クラウドのシステム管理者用の認証情報が適切に管理されていなかった
- ✓ 事例４ 不正に入手したVPN認証情報を用い個人情報を狙うサイバー攻撃
- ✓ 事例５ 海外拠点経由のサイバー攻撃で国内ネットワークまで侵入された

（出典）個人情報保護委員会 ～クラウドサービスやテレワーク環境を利用する際の個人情報の漏えい事案に関する注意喚起～ 2021/2/8
https://www.ppc.go.jp/files/pdf/warning_cloud_telework.pdf

個人情報の取り扱いに関する事故の影響

事例１：ウイルス感染で数日間業務が停止し、数千万円の被害が発生

社内のパソコンやサーバーがウィルスに感染し、数日間に亘って業務停止に至る障害が発生した。復旧のために徹夜で対応したが、その間の会社としての被害額は推計で数千万円に上る。
原因は、被害が発生するまで、セキュリティ対策ソフトを全く導入していなかったことである。
その後、ウィルス対策ソフトや技術的な対策の導入、情報セキュリティ規程の制定、プライバシーマークやISMS認証取得に取り組み、再発防止に努めている。

出典：独立行政法人情報処理推進機構（IPA）「中小企業の情報セキュリティ対策ガイドライン第3版」

事例２：テレワーク端末の踏み台化

リモートアクセスを利用した個人所有端末から正規のアカウントとパスワードが盗まれ、オフィスネットワークに不正アクセスされた案件が発生。仮想デスクトップ（VDI）によるリモートアクセスシステムを利用していたものの、個人所有端末自体が攻撃者の踏み台として乗っ取られていたため、VDIサーバ経由で自組織内のファイルサーバーを閲覧されたおそれがあり、180社以上の顧客に影響が出る恐れがあると発表。

出典：総務省「テレワークセキュリティガイドライン（第5版）」

個人情報漏えいインシデント：一人当たり平均損害賠償額　**2万8,308円**
（3か年平均）

出典：NPO日本ネットワークセキュリティ協会（JNSA）「インシデント損害額調査レポート　2021年版」

（出典）JIPDEC　個人情報管理の重要性　2022/12/12
https://privacymark.jp/system/reference/pdf/tools_pms_2022_main.pdf

小林勝哉
社会保険労務士事務所

テレワーカーが気を付けたい典型的なシーン別対策

典型的なシーンを考える

「テレワーク環境における情報セキュリティ事故の事例」から

シーン１　フィッシングによる個人情報等の漏洩

取締役が偽不在通知SMSにだまされパスワード入力

シーン２　PC管理の不備で偽ソフトインストール

業務委託先で偽セキュリティ警告にだまされ情報漏洩か

シーン３　VPN、Wi-Fiルータなどのセキュリティの脆弱性

推測可能なVPNパスワードでランサムウェア被害

シーン４　クラウドだから安心？管理外のクラウドの利用

採用活動に関する個人情報が外部から閲覧可能な状態に

（出典）2023年4月～5月の各社報道発表資料から

典型的なシーンを考える

シーン５　公共の場での盗み見

　カフェなど公共の場でPCを操作し機密情報を盗み見されたり、家族や知人から情報漏洩も

シーン6　出社時に社内ネットワークに接続しウイルス感染

　会社のネットワークを経由せずWebやSNSにアクセスし感染、出社時に社内ネットワークに接続して社内感染も

シーン７　紛失・盗難

　基本動作として持ち出し禁止の情報を許可無く持ち出したり、個人情報や機密情報の入ったPCやUSBを紛失し、生体認証や暗号化も実施されていないケースも

シーン１　フィッシングによる個人情報等の漏洩

・不安を煽る巧妙なフィッシングメールに注意！

最も多い攻撃は、過去の本物の内容を模したフィッシング。

（出典）IPA　情報セキュリティ10大脅威 2023
https://www.ipa.go.jp/security/vuln/10threats2023.htm

シーン１　フィッシングによる個人情報等の漏洩

・不安を煽る巧妙なフィッシングメールに注意！

最も多い攻撃は、過去の本物の内容を模したフィッシング。

・過去の事例

2022年3月、JR東日本「えきねっと」をかたった不審メールの事例

不審メールは過去の「【重要】アカウントの自動退会処理」の内容を模し、「2年以上ログインしていないと自動退会」とリンクからログインを促して、知らずにアクセスすると偽のサイトで個人情報の入力を求められ盗まれる。

・すぐできる対策　被害の予防

-SMSやメールで受信したURLや、SNSのURLを安易にクリックしない

-利用しているサービスの多要素認証の設定を有効にする

-迷惑メールフィルターを利用

（出典）IPA　情報セキュリティ10大脅威 2023
https://www.ipa.go.jp/security/vuln/10threats2023.htm

シーン２　PC管理の不備で偽ソフトインストール

・PC管理は、常にクリーンに、常に最新に！

　警告画面の連絡先に電話しないで！

（出典）IPA　情報セキュリティ10大脅威 2023　筆者加筆
https://www.ipa.go.jp/security/vuln/10threats2023.html

シーン２　PC管理の不備で偽ソフトインストール

・PCの管理は、常にクリーンに、常に最新に！

**　警告画面の連絡先に電話しないで！**

・公開された脆弱性情報を悪用し、修正未実施の機器を狙う

・不正アプリをインストールするとPC内の情報等が漏洩する

　攻撃の踏み台にされることで意図せず加害者になるおそれも

・すぐできる対策　被害の予防

　-資産の把握 、体制の整備

　-脆弱性関連情報の収集と対応

　-ネットワークの監視および攻撃通信の遮断

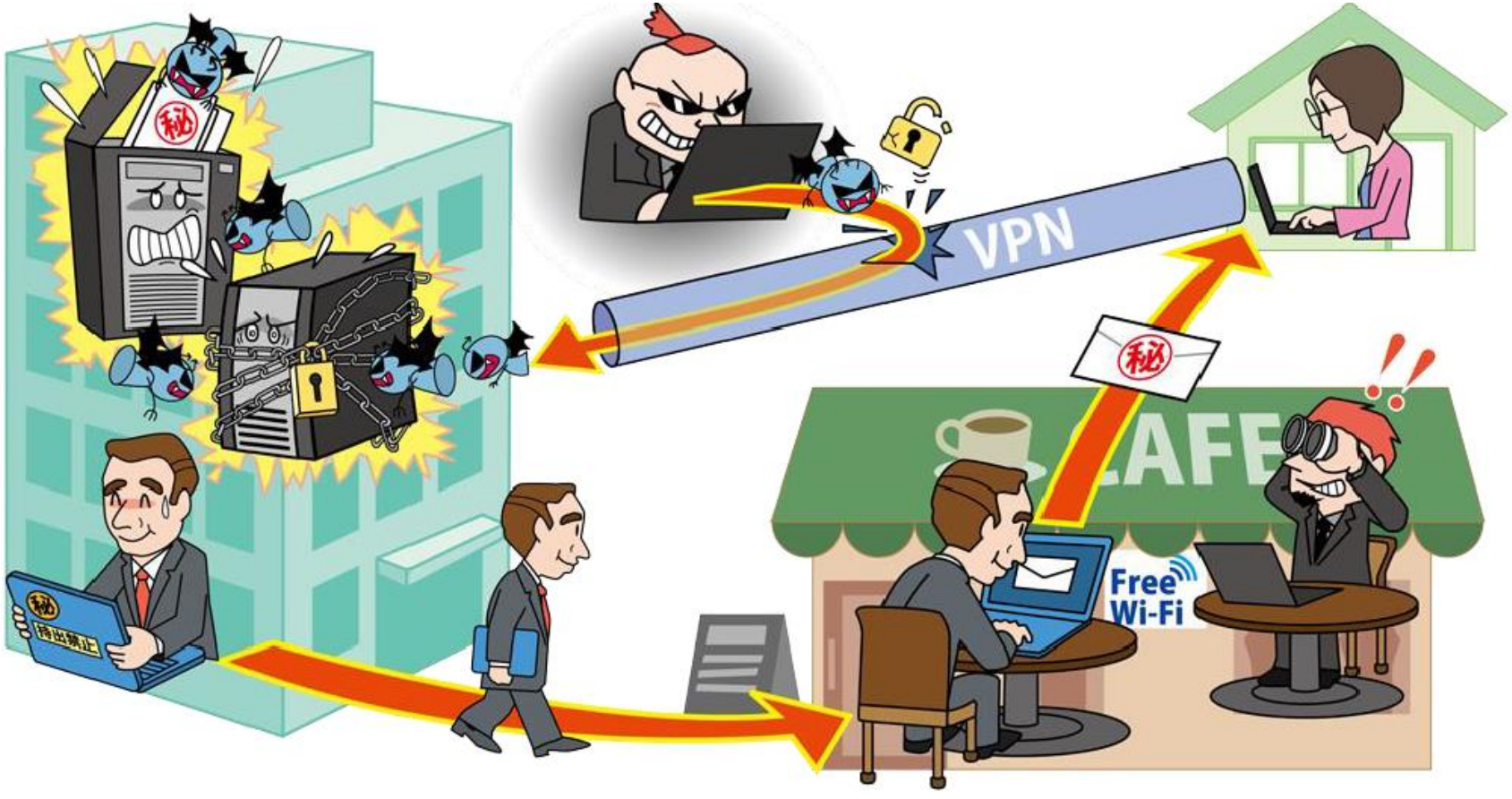
　-セキュリティのサポートが充実しているソフトウェアやバージョンを使う、等

（出典）IPA　情報セキュリティ10大脅威 2023　筆者加筆
https://www.ipa.go.jp/security/vuln/10threats2023.html

シーン３　VPN、Wi-Fiルータなどのセキュリティの脆弱性

・セキュリティ対策が不十分な暫定状態のままの運用に注意！

・組織のセキュリティ対策が適用されない箇所から情報漏えい



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

シーン３　VPN、Wi-Fiルータなどのセキュリティの脆弱性

・セキュリティ対策が不十分な暫定状態のままの運用に注意！

・組織のセキュリティ対策が適用されない箇所から情報漏えい

(1) 見知らぬアクセスポイントの利用

旅行中のＡさんは、旅先でたまたま利用可能であったWi-Fiを利用しました。利用したことのないアクセスポイント名（SSID）でしたが、パスワード入力不要で簡単に接続できたので、利用することにしました。

(2) ID・パスワードの安易な入力

接続したところ、利用に当たってはSNSでの認証が必要であると求められたため、SNSのID・パスワードを入力しました。入力画面のURLはよく確認していませんでしたが、インターネット接続は問題なく利用できたため気にしませんでした。

(3) 悪意の第三者によるなりすまし被害

数日後、SNSに自分の名前で覚えの無い誹謗中傷の投稿がされているのを見つけました。調査した結果、SNSのID・パスワードが盗用されて、第三者のなりすましによる不正アクセスをされたことがわかりました。

（出典）総務省　無線LAN（Wi-Fi）のセキュリティに関するガイドライン
https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

シーン４　クラウドだから安心？管理外のクラウドの利用

・企業管理外のクラウド（Shadow IT）を可視化し制限を
**　1つのうっかりが大事件につながることも**
**　特に、個人情報管理マニュアルの策定・遵守を最重要事項に**

・すぐできる対策　被害の予防（被害に備えた対策含む）

-確認プロセスに基づく運用
-取り扱う情報の重要度を規定し、それに合わせた運用を行う
-情報の保護（暗号化、認証）、機密情報の格納場所の把握、可視化
-DLP（Data Loss Prevention）の導入
　ポリシー設定で重要データと認定された情報の送信やコピーを制限
-外部に持ち出す情報や端末の制限

（出典）IPA　情報セキュリティ10大脅威 2023　筆者加筆
https://www.ipa.go.jp/security/vuln/10threats2023.html

シーン4　クラウドだから安心？

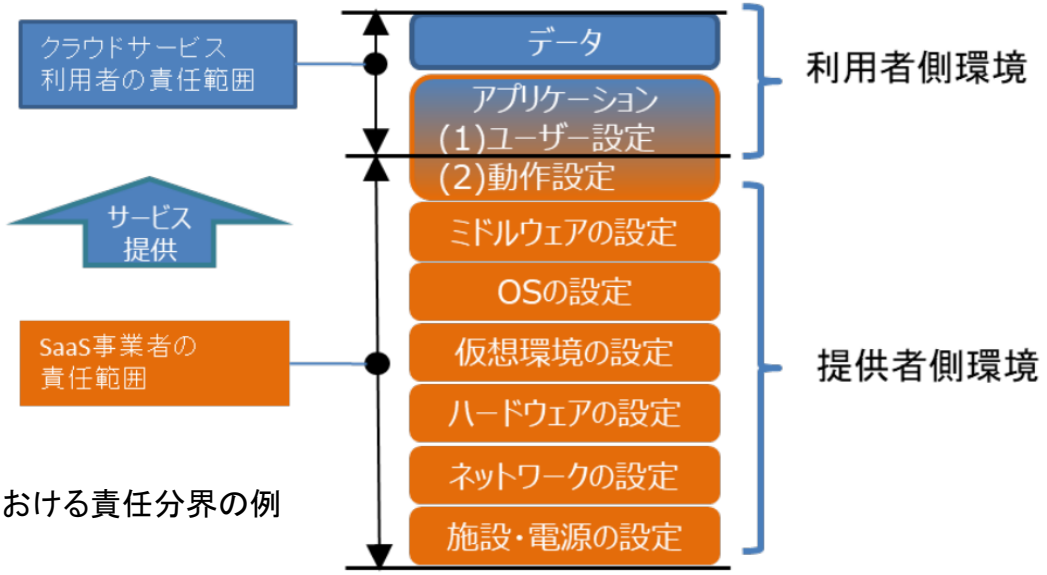
・クラウドの責任分界点

クラウドサービスの多くは、サービスやインフラの管理・保守、トラブル発生時の責任を事業者と利用企業の間で分担する「責任共有モデル」を採用しています。

クラウド利用時に情報漏洩事故が発生した場合、誰が責任を取るのか。契約時に責任を負う範囲が決められていますので、これを踏まえた対策が求められます。

クラウド上のデータの管理責任は、利用者側の企業にあります。

クラウドは安全など過信をせず、BCP（事業継続）の観点から、必要なバックアップを別の場所に持っておくことも必要です。

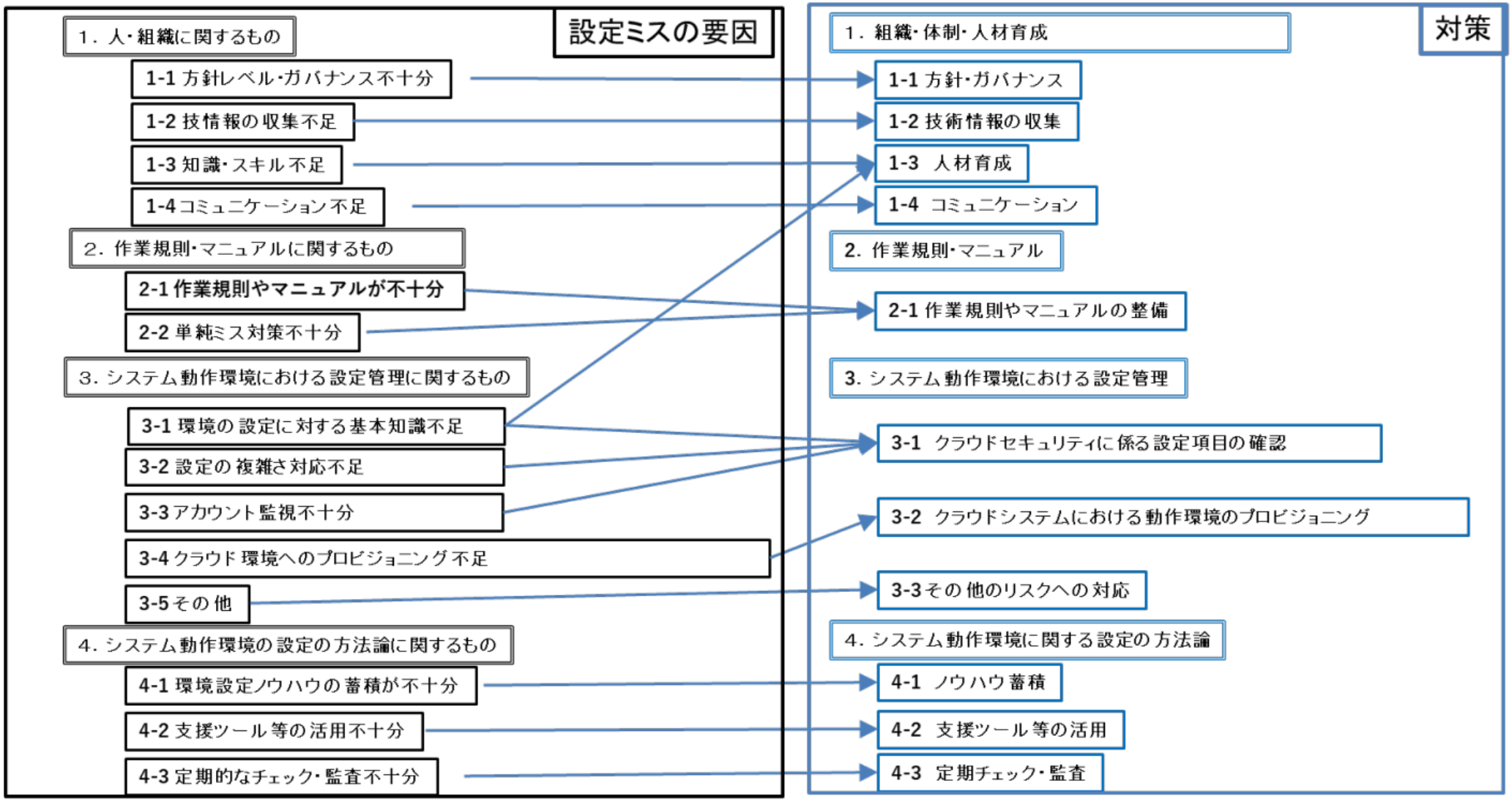


SaaSにおける責任分界の例

（出典）総務省　クラウドサービス利用・提供における適切な設定のためのガイドライン　2022/10/31
https://www.soumu.go.jp/main_content/000843318.pdf

シーン4　クラウドだから安心？

・クラウドサービス利用側の要因と対策の関係



（出典）総務省　クラウドサービス利用・提供における適切な設定のためのガイドライン　2022/10/31
https://www.soumu.go.jp/main_content/000843318.pdf

シーン５　公共の場での盗み見

・カフェなど公共の場でPCを操作し機密情報を盗み見されたり、家族や知人から情報漏洩も

・すぐできる対策　被害の予防（被害に備えた対策含む）

-公共の場で操作するテレワーク端末には、覗き見防止フィルターを付ける

-テレワークガイドラインで推奨されている作業環境の確認プロセスを通じて、家族や知人に会社の情報を見せないことや守秘義務の理解について予め社員と合意する

（テレワークガイドライン　（別紙２）自宅等においてテレワークを行う際の作業環境を確認するためのチェックリスト【労働者用】 に、項目を追加してもよい）

（出典）厚生労働省　テレワークの適切な導入及び実施の推進のためのガイドライン　2021/3/25
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/koyou_roudou/roudoukijun/shigoto/guideline.html

シーン6　出社時に社内ネットワークに接続しウイルス感染

・会社のネットワークを経由せずWebやSNSにアクセスし感染、出社時に社内ネットワークに接続して社内感染も

・すぐできる対策　被害の予防（被害に備えた対策含む）

-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

（出典）日本ネットワークセキュリティ協会（JNSA）　緊急事態宣言解除後のセキュリティ・チェックリスト　2020/6/12
https://www.jnsa.org/telework_support/telework_security/index.html

シーン７　物理的な紛失・盗難

・基本動作として持ち出し禁止の情報を許可無く持ち出したり、個人情報や機密情報の入ったPCやUSBを紛失し、生体認証や暗号化も実施されていないケースも

・すぐできる対策　被害の予防（被害に備えた対策含む）

-情報リテラシーや情報モラルの向上

-従業員のセキュリティ意識教育

-組織規程および確認プロセスの確立と定期的な見直し

-確認プロセスに基づく運用

（情報資産台帳の整備、情報持ち出し承認ルールの徹底・記録保持）

-暗号化・閲覧認証機能付きPCやUSBの採用

小林勝哉
社会保険労務士事務所

情報セキュリティ事故発生時の責任と予防措置

テレワーク勤務規程と情報セキュリティ規程の位置づけ

就　業　規　則

○○株式会社

- 給与規程
- 退職金規程
- 旅費規程
- その他の規程
- テレワーク勤務規程

テレワーク勤務規程は
就業規則の一部とされる

- 在宅勤務規程
- サテライトオフィス勤務規程
- モバイル勤務規程
- ワーケーション勤務規程

各企業における内規

- 情報セキュリティ規程
  - 基本方針（セキュリティポリシー）
  - 対策基準
  - 実施手順
- 組織規程
- 会議規程
- 文書管理規程
- その他社内規定

（出典）厚生労働省　テレワークモデル就業規則～作成の手引き～　2022/6/21　筆者加筆
https://telework.mhlw.go.jp/wp/wp-content/uploads/2022/06/teleworkmodel.pdf

テレワーク勤務規程における情報セキュリティの確保

- テレワーク勤務の定義
- 対象者/手続き等
  （自律性/業務適性、安全衛生/セキュリティの確保）
- 勤怠管理の徹底（業務時間、余暇時間の明確化）
- 労働時間把握の徹底（フレックスタイムなどの活用）
- 服務規律（情報セキュリティ、個人情報、営業秘密）
- 費用負担（通信費、光熱費、交通費、施設費用）

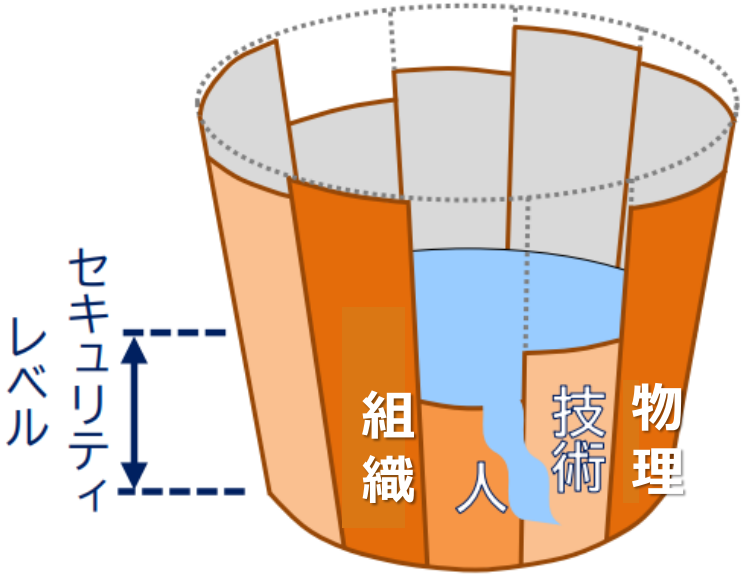
などが考えられます。

小林勝哉
社会保険労務士事務所

セキュリティは「組織」・「人」・「物理」・「技術」のバランス

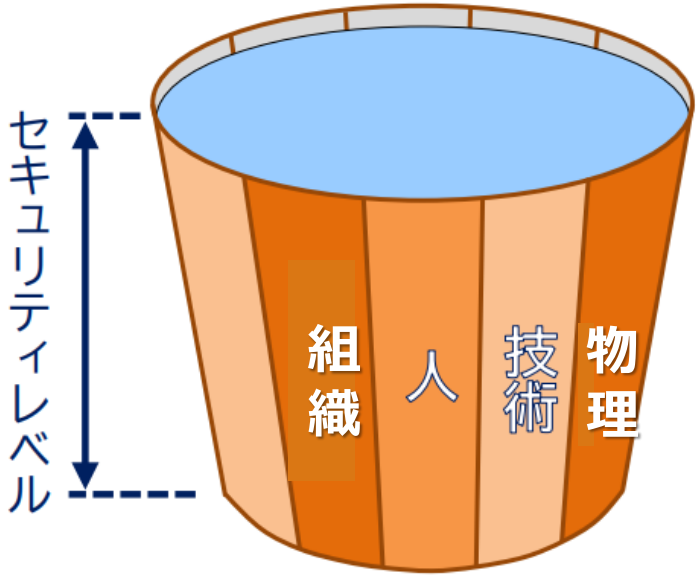
➢ テレワークセキュリティの対策は、技術的対策だけでなく、
人に着目した内部不正防止の組織的ガバナンスが重要。

バランスが悪いセキュリティ対策



バランスが悪いと、対策として不十分となり、全体のセキュリティレベルは低下してしまう。

バランスがとれたセキュリティ対策



バランスがとれた対策で、はじめて高いセキュリティレベルを維持できる。

（出典）総務省　テレワークセキュリティガイドライン（第5版）　2021/5/31　筆者加筆
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

情報セキュリティ規程の基礎となるマネジメントシステム

ビジネスでは、取引相手の情報セキュリティやサービス品質の管理体制を評価する共通の物差しが必要です。

企業活動の良い仕組みを実現するために求められる事項を規定したものが、マネジメントシステム規格です。

・ISMS（情報セキュリティマネジメントシステム）適合性評価制度

（ISO/IEC 27001）

・プライバシーマークにおける

個人情報保護マネジメントシステム構築・運用指針

（JIS Q 15001 個人情報保護マネジメントシステム-要求事項）

（出典）JIPDEC
https://www.jipdec.or.jp/project/smpo/ms_about.html

ISMS（情報セキュリティマネジメントシステム）規格改訂

小林勝哉
社会保険労務士事務所

ISO/IEC 27001:2022

情報セキュリティ,サイバーセキュリティ,プライバシー保護－情報セキュリティマネジメントシステム－要求事項

Information security, cybersecurity and privacy protection - Information security management systems - Requirements

ISMS（情報セキュリティマネジメントシステム）適合性評価制度の認証基準となっている、国際規格ISO/IEC 27001の改訂が発表されました。

（ISO/IEC 27001:2013 → ISO/IEC 27001:2022）

1・目指すものは、情報セキュリティ,サイバーセキュリティ,プライバシー保護。

2・認証の移行期間は、3年間（2025年10月31日まで）。

3・改訂内容は、**附属書Aの管理策（セキュリティ対策）**全面書き換え。

「組織的」「人的」「物理的」「技術的」の4つに再構成。93項目。

（出典）一般社団法人情報マネジメントシステム認定センター ISO/IEC 27001:2022 への対応について 2022/10/25
https://isms.jp/topics/news/20221025.html

情報セキュリティ事故発生時の責任

事故発生時の緊急連絡体制の確保と周知

困ったときにやること

1. 管理部門の担当者へ連絡
   ・メール ： abcdef@xxxx.co.jp
   ・電話 ： 000-0000-0000
2. パソコンをネットワークから切断する。
3. パソコンの電源をOFFにする。

こんなときは、すぐに担当者に連絡！

- 不審なメールの添付ファイルやURLをクリックしちゃった。
- パソコン、携帯電話、USB等を紛失しちゃった。
- アプリケーションをインストールしたら急にパソコンが重くなった。等々

※テレワーク時には、本ハンドブックを常に携行すること。

やらなくてはいけないこと

1. 盗難、紛失防止のためテレワーク端末は、外出時も常に肌身離さず携帯する。
2. テレワーク端末の画面を横や後ろから覗かれないように注意する。
3. 自宅でも席を立つ前にはテレワーク端末にロックをかける。
4. テレワーク端末、無線ルーター、ウイルス対策ソフトに常に最新のパッチ、ファームウェア、定義ファイルを適用する。
5. フリーWi-Fiに接続後、業務をする際はURL「https://」から始まるサービスだけ使う。

やってはいけないこと

1. 業務で取り扱うデータを許可無く私物（テレワーク端末、USB、クラウドサービス等）にコピーしない。
2. 不審なメールの添付ファイルやURLをクリックしない。
3. 不審なウェブサイトにアクセスしない。
4. パスワード等のメモをパソコンに貼らない。
5. 提供元が不明もしくは、よく分からないアプリケーションを安易にインストールしない。

（出典）総務省　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） 従業員向けハンドブック　2022/5
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

情報セキュリティ事故発生時の責任

個人情報漏えい等報告等の義務化

2022年4月施行

●漏えい等が発生し、個人の権利利益を害するおそれが大きい場合に、**委員会への報告及び本人への通知を義務化**する。

改正前	改正後
個人情報保護委員会に報告及び本人通知するよう**努める**（委員会告示）	漏えい等が発生し、個人の権利利益を害するおそれが大きい場合に、**個人情報保護委員会への報告及び本人への通知を義務化**する（§26）

漏えい等報告の義務化の対象事案
（委員会規則で定める要件）

- 要配慮個人情報の漏えい等
- 財産的被害のおそれがある漏えい等
- 不正の目的によるおそれがある漏えい等
- 1,000件を超える漏えい等

これらの類型は件数に関わりなく対象

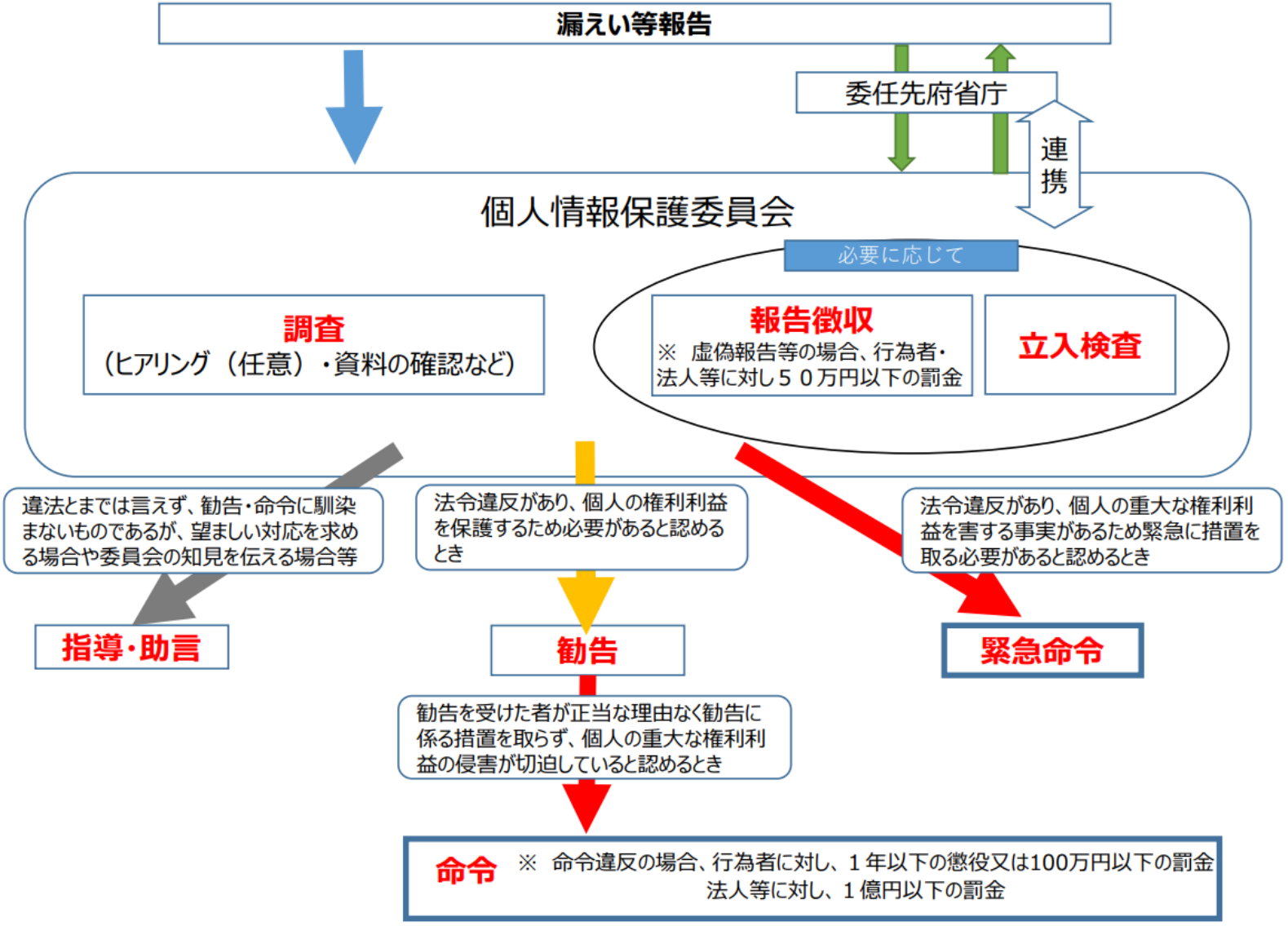
※各類型につき、漏えい等の「おそれ」がある事案も対象。

（出典）個人情報保護委員会事務局　個人情報保護法改正に伴う漏えい等報告の義務化と対応について　2022/5/27
https://www.mhlw.go.jp/content/10808000/000943451.pdf

情報セキュリティ事故発生時の責任

個人情報漏えい等事案の基本的事務フロー

2022年4月施行



（出典）個人情報保護委員会事務局　個人情報保護法改正に伴う漏えい等報告の義務化と対応について　2022/5/27
https://www.mhlw.go.jp/content/10808000/000943451.pdf

情報セキュリティ事故の予防に向けた取り組み事例

東京都　中小企業サイバーセキュリティ対策継続支援事業から

１・テレワーク時の情報セキュリティ事故の予防事例

事例1　信頼性の高いセキュアな開発環境を構築

事例2　柔軟な働き方と情報セキュリティ強化を両立

事例3　運用を刷新し可用性の高いセキュリティ対策に

２・情報セキュリティ事故発生時の初動体制の事例

事例4　インシデントへの組織的な対応体制を構築

（出典）東京都産業労働局　令和4年度中小企業サイバーセキュリティ対策継続支援事業　事例集
https://security-keizoku.metro.tokyo.lg.jp/r4/

事例１　信頼性の高いセキュアな開発環境を構築

業種等　**情報通信、E社、101～300名、管理は兼務で社員3名**

事業内容　ITインフラやシステム構築などのSE派遣やソリューション提供

背景　**複数拠点間の接続やリモート・クラウド環境移行でリスク増大**

課題　エンドポイントのウィルス対策の強化

リモート環境、クラウド環境の対策

クラウド利用ルールを盛り込んだセキュリティ規程の最新化

対策　**ウィルス対策ソフトから次世代のEDRやMDMの導入・運用へ**

VPN経由のクラウドアクセスがあるため多要素認証を導入

急な在宅勤務など例外ルールを含めたセキュリティ規程の整備

情報システム担当者や社員のセキュリティ意識の底上げ

今後　ゼロトラストの実現を中長期目標に、課題に一つずつ取り組む

（出典）東京都産業労働局　令和4年度中小企業サイバーセキュリティ対策継続支援事業　事例集　筆者抜粋
https://security-keizoku.metro.tokyo.lg.jp/r4/

事例2　柔軟な働き方と情報セキュリティ強化を両立

業種等　**出版業、K社、101～300名、管理は兼務で外部委託数名**

事業内容　雑誌、書籍、Web、ECコンテンツなどの制作・販売

背景　**柔軟な働き方やクリエイティブな発想と情報セキュリティの両立**

課題　BYOD（個人所有端末の業務利用）のルールが明確でない

個人のメールアカウントを仕事のデータ授受に頻繁に利用

クリエイティブな業務のためWebアクセス制限やログ監視が困難

対策　**個人のメールアカウントで事故が発生した時のプロセスを整理**

実情に合わせ、BYODを認めるがセキュリティ規程遵守とする

情報セキュリティ規程改定について社員説明会を実施

BYODのログ監視についても責任の有無を明確にする旨説明

今後　入稿管理のクラウド化や、トップダウン＆ボトムアップで改善展開

（出典）東京都産業労働局　令和4年度中小企業サイバーセキュリティ対策継続支援事業　事例集　筆者抜粋
https://security-keizoku.metro.tokyo.lg.jp/r4/

事例3　運用を刷新し可用性の高いセキュリティ対策に

業種等　**エネルギー管理、H社、6～20名、管理は兼務で外部委託数名**

事業内容　熱供給プラント保守、熱エネルギー供給、太陽光発電所運用

背景　**テレワーク運用ルールが古く現状と乖離、内部監査への対応**

課題　リモートデスクトップ方式を利用しているが細かなルールが不足
テレワークの本格導入後に自社サーバのクラウド移行の変更あり
年々ハードルが上がっている内部監査への対策が必要

対策　**テレワークの接続パターンについて直接かクラウド経由か整理**
テレワーク運用ルールにインシデント発生時の対応フロー追加
自社へのクラウド導入基準を自社のシステム管理基準相当に
端末の使い勝手に支障のないよう社員のアクセス権限に幅を

今後　機密性重視のセキュリティ対策から可用性重視のバランス型へ

（出典）東京都産業労働局　令和4年度中小企業サイバーセキュリティ対策継続支援事業　事例集　筆者抜粋
https://security-keizoku.metro.tokyo.lg.jp/r4/

事例4　インシデントへの組織的な対応体制を構築

業種等　**電気機器製造、L社、101～300名、管理は兼務で社員数名**

事業内容　配線器具や電子機構部品を製造、国内複数拠点と海外拠点

背景　**取引先で発生したサイバー攻撃事例を受けて危機感が高まる**

課題　サーバー攻撃などを検知した後の対応手順が確立していない

IPAのガイドライン準拠の規程と実際の業務に乖離がある

拠点ごとのシステム担当者の個別対策を全社的に統括が必要

対策　**実際の業務に合わせ情報セキュリティ規程を実効的に再整備**

社内の情報資産をとりまとめ、保有する情報資産を整理

取りまとめた情報資産の管理方法を定めた要領を作成

全社員が理解・実践しやすいセキュリティ・ガイドブックを作成

今後　情報セキュリティ委員会を中心にインシデント対応フローを整理

（出典）東京都産業労働局　令和4年度中小企業サイバーセキュリティ対策継続支援事業　事例集　筆者抜粋
https://security-keizoku.metro.tokyo.lg.jp/r4/

最後に

本日のまとめ

１）情報セキュリティ事故による企業や社員の損害の増大

情報セキュリティ10大脅威 2023脅威ランキングのトップ5を理解。

２）テレワーク環境における情報セキュリティリスクの増大

働く場所、情報資産の格納場所、情報資産の管理方法の拡大によりリスクが増大。

３）テレワーク環境における情報セキュリティ事故の事例

2023年に起きた情報セキュリティ事故の事例1～事例4を紹介。

４）テレワーカーが気を付けたい典型的なシーン別対策

シーン1～シーン7のリスクとすぐできる対策を紹介。

５）情報セキュリティ事故発生時の責任と予防措置

就業規則と情報セキュリティ規程を整備し、情報セキュリティの確保を。

企業の社会的責任から初動対応、個人情報保護の対応が重要に。

私の考える未来のテレワークの姿

～　IT×法律で新たな価値創造を　～

①新しい働き方とはアンビエントなチームワーク
　遠隔地勤務で離れていてもすぐそばに感じる
＝ambientROOM

②どこまでいっても人と人が触れ合えるITS
　遠く離れた大切な人の温もりが伝わる
＝In Touch

③B2B2X、DXからその先の価値へ
　オープンイノベーションの可能性
　新しい企業価値の創造へ
　DX法務の必要性の高まり

（出典）MIT Media Lab Tangible Media Group
https://tangible.media.mit.edu/projects/

小林勝哉
社会保険労務士事務所

ご清聴
ありがとうございました

【参考資料】
・略語
・テレワークにおける就業規則に関する支援情報
・テレワークにおける情報セキュリティに関する支援情報
・総務省テレワークセキュリティガイドライン等の適用場面
・セキュリティ対策の優先度の検討支援ツール例

参考　略語

- CSIRT（Computer Security Incident Response Team）
  セキュリティ上の問題事象のインシデントが発生した際に対応するチーム。
- DLP（Data Loss Prevention）
  機密情報や重要データの紛失、外部への漏えいを防ぐシステムで、あらかじめ設定したポリシーをもとに機密情報を識別し、重要データと認定された情報の送信やコピーを制限。
- EDR（Endpoint Detection and Response）
  ユーザーが利用するパソコンやサーバー（エンドポイント）における不審な挙動を検知し、迅速な対応を支援するソリューション。
- UTM（Unified Threat Management）
  複数の異なるセキュリティ機能を統合し、集中的にネットワーク管理する機器、機能。
- VPN（Virtual Private Network）
  仮想プライベートネットワーク。 送/受信側でカプセル化処理を行い通信経路を保護。
- XDR（Extended Detection and Response）
  エンドポイントだけでなく、ネットワーク、クラウド、アプリケーション全体を可視化・分析し、脅威を検出し、分析・修復を支援するソリューション。

参考
テレワークにおける就業規則に関する支援情報

小林勝哉
社会保険労務士事務所

➢ テレワーク相談コーナー

https://japan-telework.or.jp/sodan/

電　話：0120-861009

➢ テレワーク総合ポータル

ひと、くらし、みらいのために
厚生労働省
Ministry of Health, Labour and Welfare

https://telework.mhlw.go.jp/

参考
テレワークにおける情報セキュリティに関する支援情報

小林勝哉
社会保険労務士事務所

➢ 令和5年度東京都事業の例

➢ サイバーセキュリティ対策促進助成金

https://www.tokyo-kosha.or.jp/support/josei/setsubijosei/cyber.html

SECURITY ACTION「二つ星」の中小企業に対する機器等の導入、およびクラウド利用に係る経費の助成

1,500万円、助成対象経費の1/2以内

（令和6年1月募集あり）

➢ 中小企業サイバーセキュリティ向上支援事業

https://security-kojo.metro.tokyo.lg.jp/

[支援①UTM機器設置コース]

セキュリティ環境の事前診断とセキュリティ対策機器の体験機会の提供

およびSECURITY ACTION「二つ星」宣言を目指し、サイバーセキュリティに関する基本方針や社内規定の策定等のサポートを実施（令和5年12月8日まで募集）

参考
テレワークにおける情報セキュリティに関する支援情報

小林勝哉
社会保険労務士事務所

➢ 令和5年度IT導入補助金の例

「セキュリティ対策推進枠」

https://www.it-hojo.jp/security/

IPAの「サイバーセキュリティお助け隊サービス」に特化

サービス利用料の1/2以内、最大100万円を補助

サービス利用料 最大2年分補助

➢ IPA事業の例

経営者向けインシデント対応机上演習

https://www.ipa.go.jp/security/seminar/sme/ttx-e.html

経営者を対象に、サイバー攻撃によるインシデントの対応（担当者への指示・判断、顧客対応等）について机上演習し、実際にインシデントが起きた時に経営者が対応するべきポイントや事前の備えについて学ぶ

参考
総務省テレワークセキュリティガイドライン等の適用場面

小林勝哉
社会保険労務士事務所

◆総務省　テレワークセキュリティガイドライン

（総項目数　98、基本対策　78、発展対策　20）

セキュリティの**専任組織がある企業**のテレワークのセキュリティ対策についての考え方や対策例を示したもの。

◆総務省　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

（総項目数　34、優先度◎　14、優先度－　20）

セキュリティの**専任担当がいない中小企業**のシステム管理担当者が、テレワークの最低限のセキュリティを確実に確保するためのもの。

◆IPA　新５分でできるセキュリティ自社診断

（総項目数　25）

小規模事業者がSECURITY ACTION（セキュリティ対策自己宣言）に向け、組織活動をチェックするためのもの。「二つ星」を目指しましょう。

（出典）総務省　テレワークにおけるセキュリティ確保
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

参考
セキュリティ対策の優先度の検討支援ツール例

小林勝哉
社会保険労務士事務所

セキュリティ対策の優先度の検討

　自社の対策状況を把握し、NISTサイバーセキュリティフレームワークなどに基づき推奨される対策の中から、対処方法を検討できます。

（支援ツールの一例）

「ランサムウェア対策簡易チェック」（株式会社ラック、無料）

https://www.lac.co.jp/security/ransomware_check.html

　自組織の現状を25問の設問に回答することで、優先的に対処すべきセキュリティ対策の分野と理由などのレポートが無料で取得できます。

小林勝哉
社会保険労務士事務所

ご清聴
ありがとう
ございました

全国各地域をオンラインで結んでご支援させていただいております。

テレワークのことなら何でもお気軽にお問合せ下さい。