小林勝哉
社会保険労務士事務所

自律的な働き方を実現するための
テレワークの制度設計とは
～就業規則と情報セキュリティ規程のポイント～

2023年1月24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　代表

特定社会保険労務士

元NTTのIT専門家。経済産業省とソフトウェア分野の産官学の交流を推進してきました。
現在、テレワーク相談センター コンサルタント／専門相談員。
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ます。

目次

自律的な働き方を実現するための
テレワークの制度設計とは
～就業規則と情報セキュリティ規程のポイント～

小林勝哉
社会保険労務士事務所

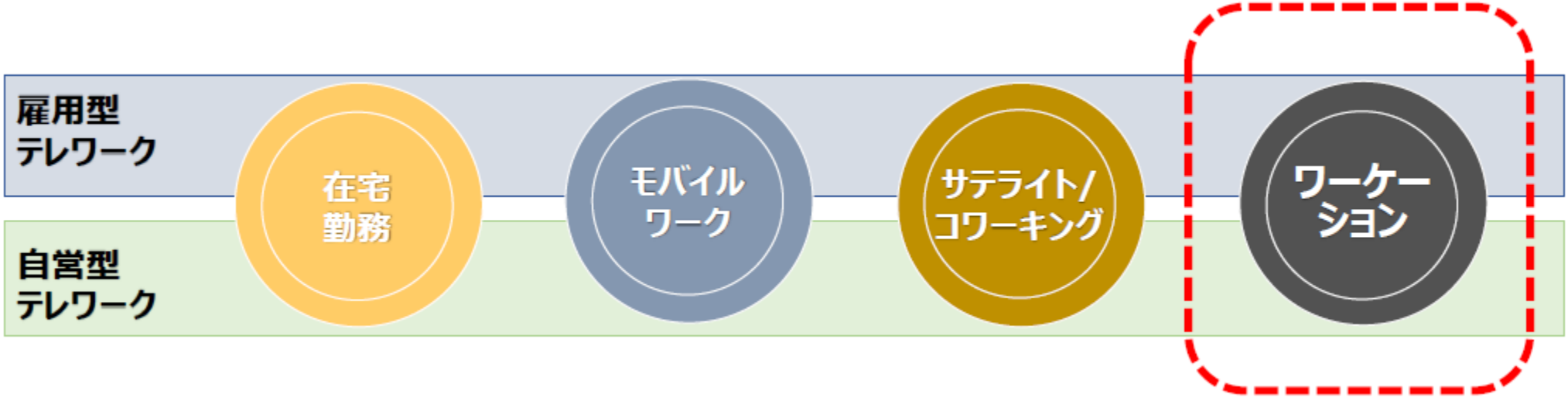
テレワークを通じた
新しい働き方への期待

テレワークワークの実施形態

テレワークとは

ICTを利用し、時間や場所を有効に活用できる柔軟な働き方

※テレワーク:「tele＝離れたところで」と「work＝働く」を合わせた造語



（出典）日本テレワーク協会　テレワーク導入事例の紹介　2022/7/28
https://kagayakutelework.jp/seminar/2022/pdf/seminar03_0728/01_murata220728.pdf

テレワークの導入目的（総務省調査、複数回答）

小林勝哉
社会保険労務士事務所

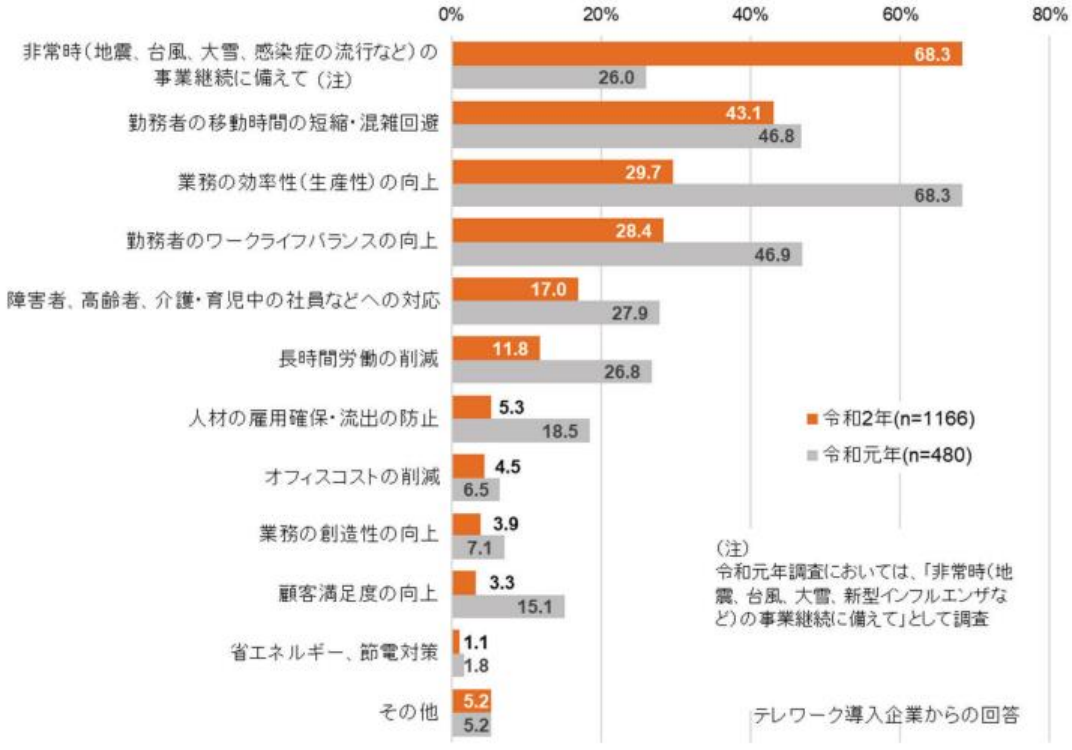
トップ４（導入企業の回答から）

①ＢＣＰ（非常時の事業継続に備えて）

②勤務者の移動時間の短縮・混雑回避

③業務の効率性
（生産性）の向上

④勤務者の
ワークライフバランスの向上

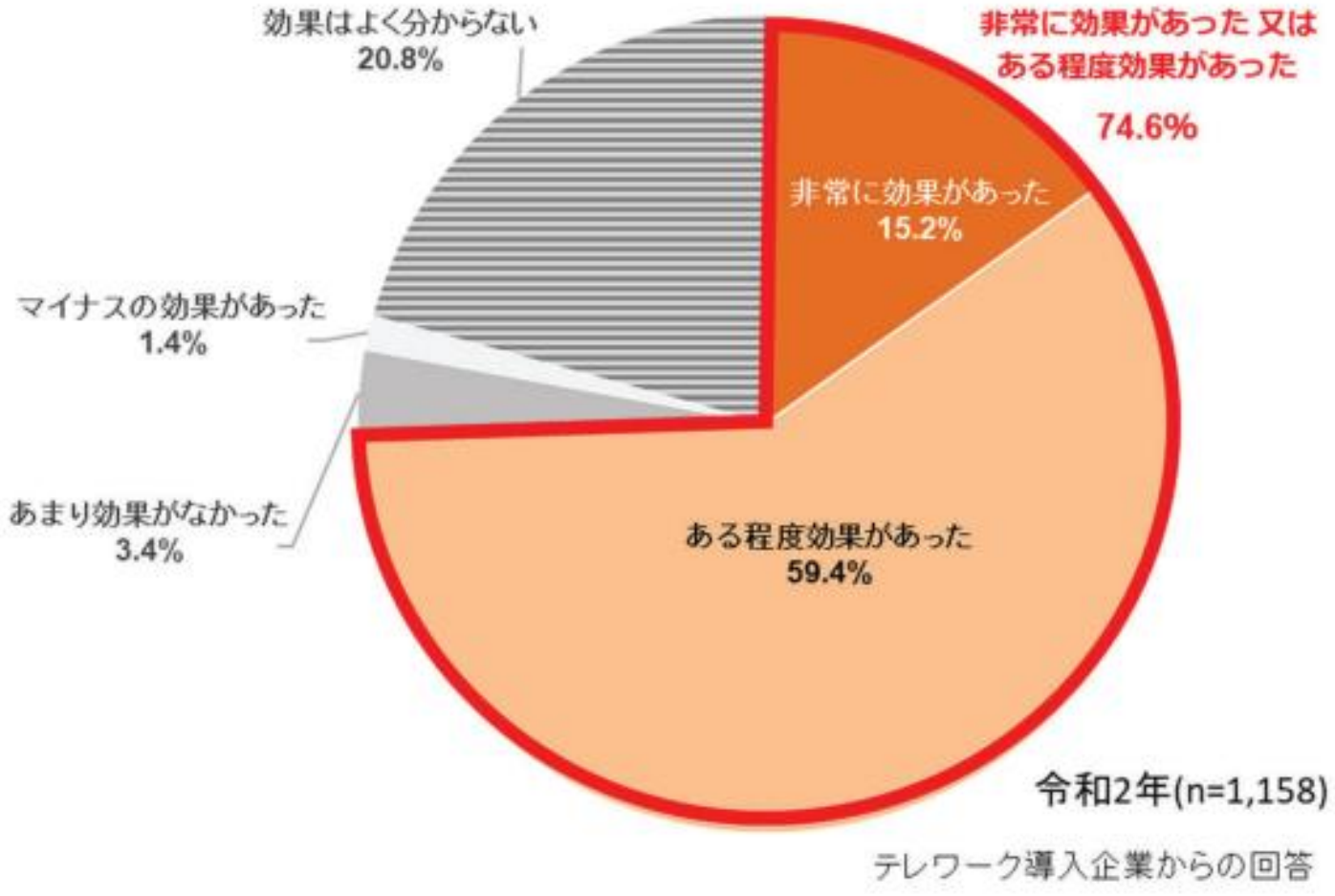


（出典）総務省　令和2年通信利用動向調査の結果
https://www.soumu.go.jp/menu_news/s-news/01tsushin02_02000154.html

テレワークの効果（令和2年、総務省調査）

効果があった（導入企業の回答から）

７４．６％



（出典）総務省　令和2年通信利用動向調査の結果
https://www.soumu.go.jp/menu_news/s-news/01tsushin02_02000154.html

テレワークの企業における効果

トップ５

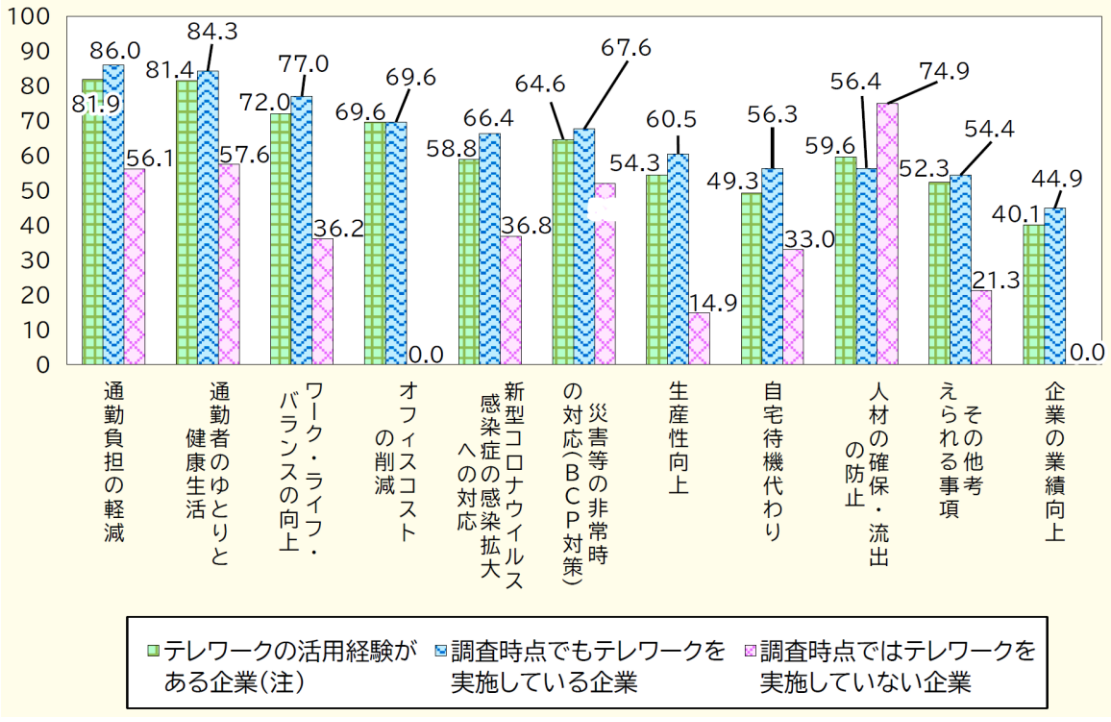
①通勤負担の軽減

②通勤者のゆとりと健康生活

③ワーク・ライフ・バランスの向上

④オフィスコストの削減

⑤新型コロナウィルス感染症
感染拡大への対応



（出典）厚生労働省　令和4年版　労働経済の分析　2022/9/6
https://www.mhlw.go.jp/stf/newpage_27381.html

テレワークの定着に向けた企業の課題

トップ５

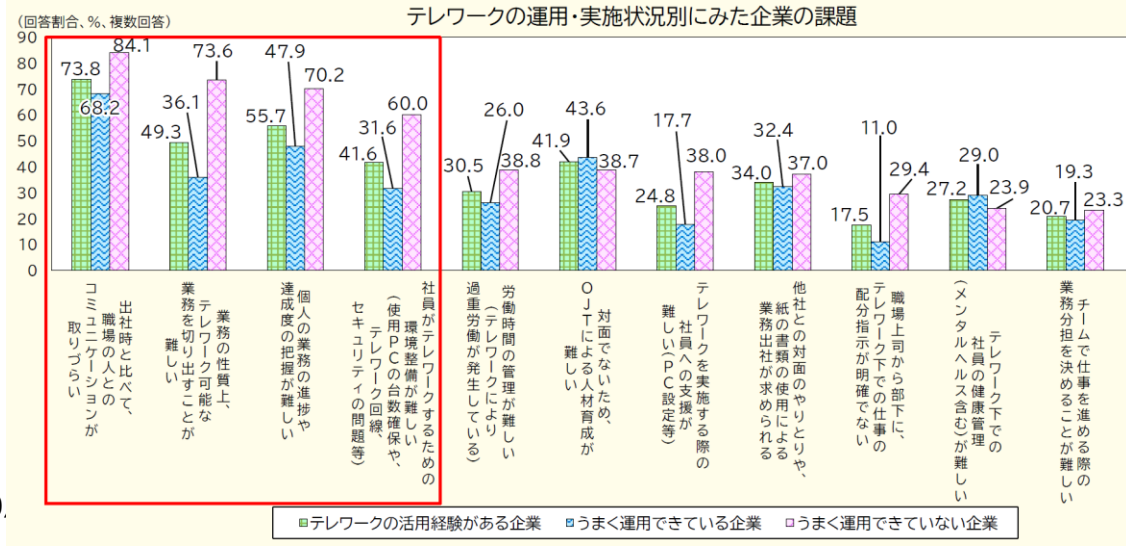
①出社時と比べて、職場の人とのコミュニケーションが取りづらい
　（3割の企業が対応済み）

②業務の性質上、テレワーク可能な業務を切り出すことが難しい

③個人の業務の進捗や達成度の把握が難しい

④社員がテレワークするための環境整備が難しい
　（3割の企業が対応済み）

⑤労働時間の管理が難しい



（出典）厚生労働省　令和4年版　労働経済の分析　2022/9
https://www.mhlw.go.jp/stf/newpage_27381.html

テレワークの定着に向けた厚生労働省の取り組み

【柔軟な働き方がしやすい環境整備への取り組み】

①良質なテレワークの定着・促進

「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」

「人材確保等支援助成金（テレワークコース）」

「テレワーク・ワンストップ・サポート事業」（テレワーク相談センター）

②フリーランスなど個人が安心して働ける環境の整備

「自営型テレワークの適正な実施のためのガイドライン」

「フリーランスとして安心して働ける環境を整備するためのガイドライン」

③障害者の多様な希望や特性等に対応した働き方の選択肢の拡大

障害者のテレワーク雇用に向けた企業向けガイダンス、コンサルティング

（出典）厚生労働省　令和4年版　労働経済の分析
https://www.mhlw.go.jp/stf/wp/hakusyo/kousei/21/index.html

自律的な働き方への期待

テレワークの経験を通じて

自律的な働き方への

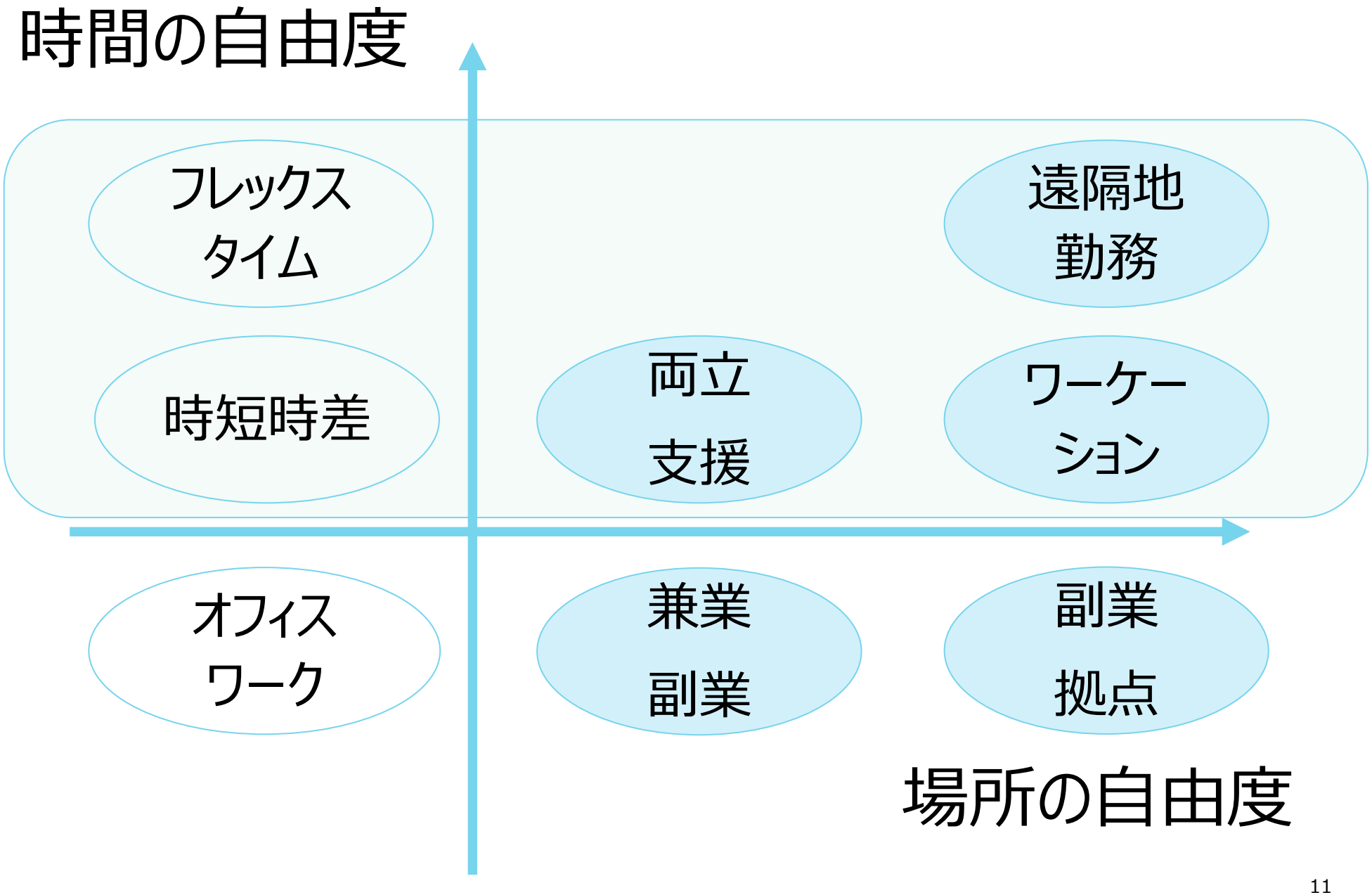
関心が高まっています。

さらに「時間」と「場所」に

とらわれない創造的な働き方への

期待が高まっています。

働く「時間」と「場所」の自由度の関係



小林勝哉
社会保険労務士事務所

テレワークセキュリティの現状と課題

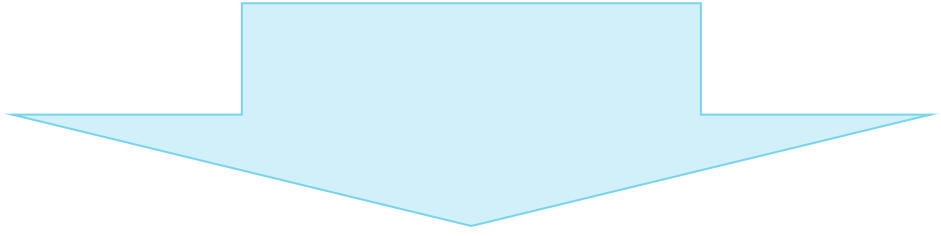
「テレワークセキュリティの現状と課題」

小林勝哉
社会保険労務士事務所

- 情報セキュリティ10大脅威の動向
- 中小企業における情報セキュリティ対策の実態
- 不正競争防止法と内部不正防止ガイドライン

自律的な働き方に対応した、社内制度・ルール作りを

テレワークの制度設計では、自律的な働き方に対応した、
社内制度・ルール作りが大切です。



・内部不正による情報漏えいが、増加しています。
　企業としての基本的セキュリティ対策は行っていますか？
・テレワーク等のニューノーマルな働き方を狙った攻撃は、
　引き続き増加しています。
　テレワークに着目したセキュリティ対策は行っていますか？

情報セキュリティ10大脅威 2022脅威ランキング

昨年順位	個人	順位	組織	昨年順位
2位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位
3位	ネット上の誹謗・中傷・デマ	2位	標的型攻撃による機密情報の窃取	2位
4位	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位	サプライチェーンの弱点を悪用した攻撃	4位
5位	クレジットカード情報の不正利用	4位	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
1位	スマホ決済の不正利用	5位	内部不正による情報漏えい	6位
8位	偽警告によるインターネット詐欺	6位	脆弱性対策情報の公開に伴う悪用増加	10位
9位	不正アプリによるスマートフォン利用者への被害	7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	New
7位	インターネット上のサービスからの個人情報の窃取	8位	ビジネスメール詐欺による金銭被害	5位
6位	インターネットバンキングの不正利用	9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	インターネット上のサービスへの不正ログイン	10位	不注意による情報漏えい等の被害	9位

（出典）IPA　情報セキュリティ10大脅威 2022
https://www.ipa.go.jp/security/vuln/10threats2022.html

5位_内部不正による情報漏えい
～組織は内部不正をさせない、不正情報を利用しない～

小林勝哉
社会保険労務士事務所

【攻撃手口/発生要因】

１・内部の従業員は重要情報にアクセスしやすい

２・悪意をもった場合、情報を外部に提供される

- ■アクセス権限の悪用
- ■内部情報の不正な持ち出し
- ■在職中に割り当てられたアカウントの悪用

【事故の例】

・取引先の顧客情報を不正利用

・元従業員の転職先に対して損害賠償請求

（出典）IPA　情報セキュリティ10大脅威 2022
https://www.ipa.go.jp/security/vuln/10threats2022.html

5位_内部不正による情報漏えい
～組織は内部不正をさせない、不正情報を利用しない～

小林勝哉
社会保険労務士事務所

【対策】

１・組織（経営者、管理者）として

・被害の予防

-基本方針の策定

-資産の把握、対応体制の整備

-重要情報の管理、保護

-物理的管理の実施

・情報リテラシーや情報モラルの向上

・攻撃の予兆／被害の早期検知

・被害を受けた後の対応

（出典）IPA　情報セキュリティ10大脅威 2022
https://www.ipa.go.jp/security/vuln/10threats2022.html

5位_内部不正による情報漏えい
～不正のトライアングル～

小林勝哉
社会保険労務士事務所

【内部不正の要因と対策】

１・要因　不正のトライアングル

内部不正行為の要因は**「機会」「動機」「正当化」の三要素**が揃った時。

アメリカの犯罪学者ドナルド・クレッシー(Donald R. Cressey)氏が提唱。

- 社内システムへの管理用パスワードを意図せず入手できた時、あなたならどうしますか？
- 再発防止策は、「組織的安全管理措置」、「人的安全管理措置」、「物理的安全管理措置」、「技術的安全管理措置」の4つの視点を組み合わせることで、「必要かつ適切な措置」を講じることができます。

（出典）JIPDEC　プライバシーマーク推進センター　2021年度「個人情報の取扱いにおける事故報告集計結果」 2022/10/7　筆者要約
https://privacymark.jp/news/other/2022/1007.html

４位_テレワーク等のニューノーマルな働き方を狙った攻撃
～テレワークのセキュリティは企業と従業員の結束が重要～

小林勝哉
社会保険労務士事務所

【攻撃手口/発生要因】

１・テレワーク環境や管理体制の不備

■急なテレワーク移行による管理体制の不備

■私物PCや自宅ネットワークの利用

※組織のセキュリティ対策が適用されないところからの情報漏えい

■テレワーク用ソフトの脆弱性を悪用した不正アクセス

【事故の例】

・脆弱性の悪用によりVPNのパスワード流出（年間で約1,000社）

・リモートデスクトップへの総当たり攻撃が急増（月に3億件）

（出典）IPA　情報セキュリティ10大脅威 2022
https://www.ipa.go.jp/security/vuln/10threats2022.html

小林勝哉
社会保険労務士事務所

【対策】

１・組織（経営者層）として

・組織としての体制の確立

-テレワークのセキュリティポリシーの策定

-対策予算の確保と継続的な対策の実施

- CSIRTの構築、有事の際の連絡窓口やフローの確立

２・組織（テレワーカー）として

・被害の予防は、組織のテレワークルールを順守
（使用する端末、ネットワーク環境、作業場所等）

・被害を受けた後の対応は、組織の方針に従い各所へ報告、相談する
※上司、CSIRT、関係組織、公的機関等

（出典）IPA　情報セキュリティ10大脅威 2022
https://www.ipa.go.jp/security/vuln/10threats2022.html

４位_テレワーク等のニューノーマルな働き方を狙った攻撃
～事業環境の変化はリスクの変化でもある～

小林勝哉
社会保険労務士事務所

【個人情報の取扱いにおける事故の特徴】

１・プライバシーマーク付与事業者においても事故件数が増大

「テレワークの実施」「新たなコミュニケーションツールの利用」など、
業務環境の変化による影響がみられる

２・事故原因は、「誤送付」（1,938件：63.6%）が最多

内訳は、**「メール誤送信」**（1,128件：37.0%）が最多
（SMSやメッセージアプリ等による誤送信を含む）

３・「プログラム/システム設計・作業ミス 」が前年度から約2.5倍増加

その他、個人情報の「目的外利用」が増加

（出典）JIPDEC　プライバシーマーク推進センター　2021年度「個人情報の取扱いにおける事故報告集計結果」 2022/10/7　筆者要約
https://privacymark.jp/news/other/2022/1007.html

小林勝哉
社会保険労務士事務所

【個人情報の取扱いにおける事故の事例と対策】

４・事例　メール誤送信（業務環境変化に伴う体制構築・手順策定の不備）

A社は、メール送信時に出社している複数人でのダブルチェックを実施。

テレワーク時はメール送信前に各自が複数回チェックするルールを策定。

自身でチェックし送信したが、間違いに気付かず別の事業者に誤送信。

対策例として、メール誤送信防止ツールを導入。

➢再発防止策は「**組織**的安全管理措置」、「**人**的安全管理措置」、「**物理**的安全管理措置」、「**技術**的安全管理措置」の4つの視点を組み合わせることで、「必要かつ適切な措置」を講じることができます。

（出典）JIPDEC　プライバシーマーク推進センター　2021年度「個人情報の取扱いにおける事故報告集計結果」 2022/10/7　筆者要約
https://privacymark.jp/news/other/2022/1007.html

小林勝哉
社会保険労務士事務所

【個人情報の取扱いにおける事故の事例と対策】

５・事例　設定不備（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

「テレワークセキュリティの現状と課題」

小林勝哉
社会保険労務士事務所

- 情報セキュリティ10大脅威の動向
- 中小企業における情報セキュリティ対策の実態
- 不正競争防止法と内部不正防止ガイドライン

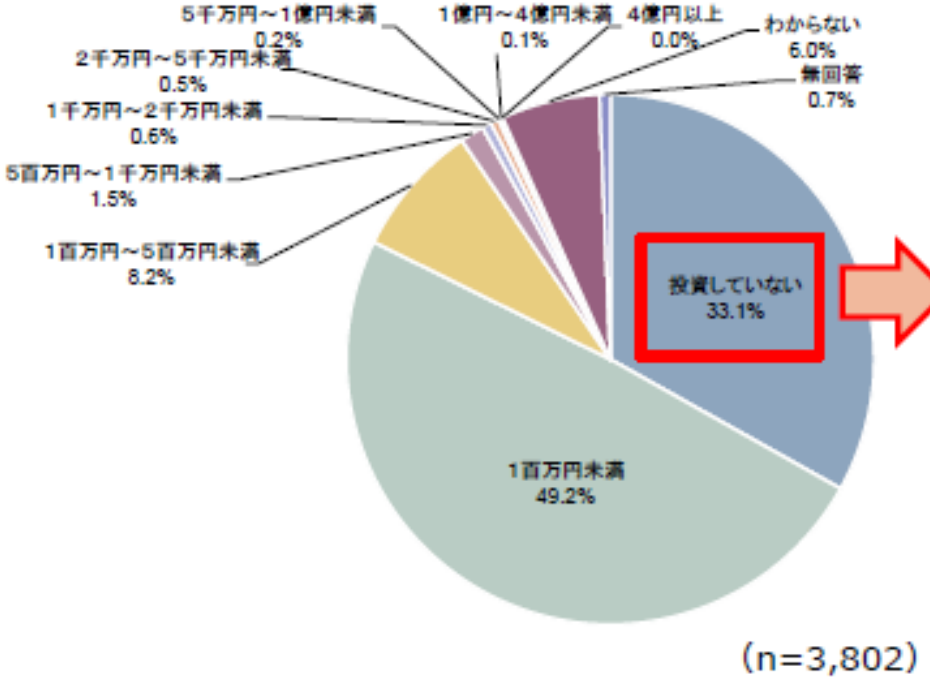
過去3期における「IT投資」「情報セキュリティ投資」を行っていない企業はともに約3割

小林勝哉
社会保険労務士事務所

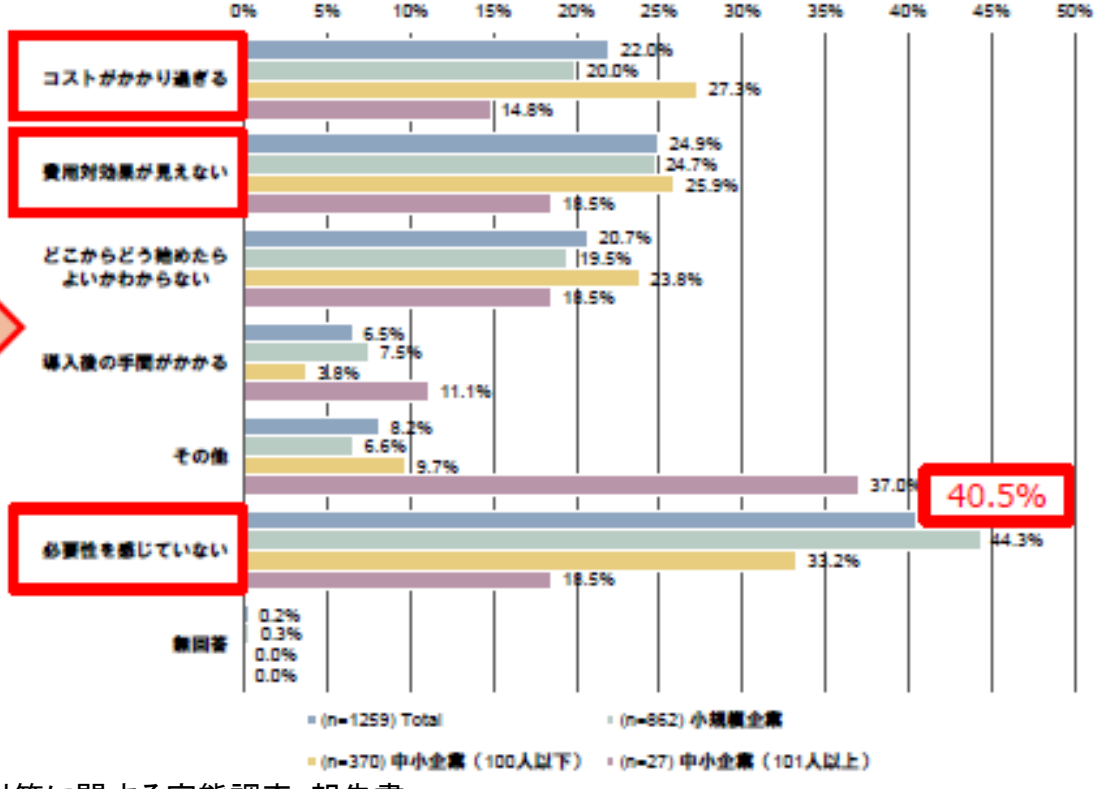
・「情報セキュリティ対策投資」について、**「投資を行っていない」企業は33.1%**

・情報セキュリティ対策**投資を行わない理由は、「必要性を感じていない」が40.5%**、
次いで「費用対効果が見えない」（24.9%）、「コストがかかりすぎる」（22.0%）

【直近過去３期の情報セキュリティ対策投資額】



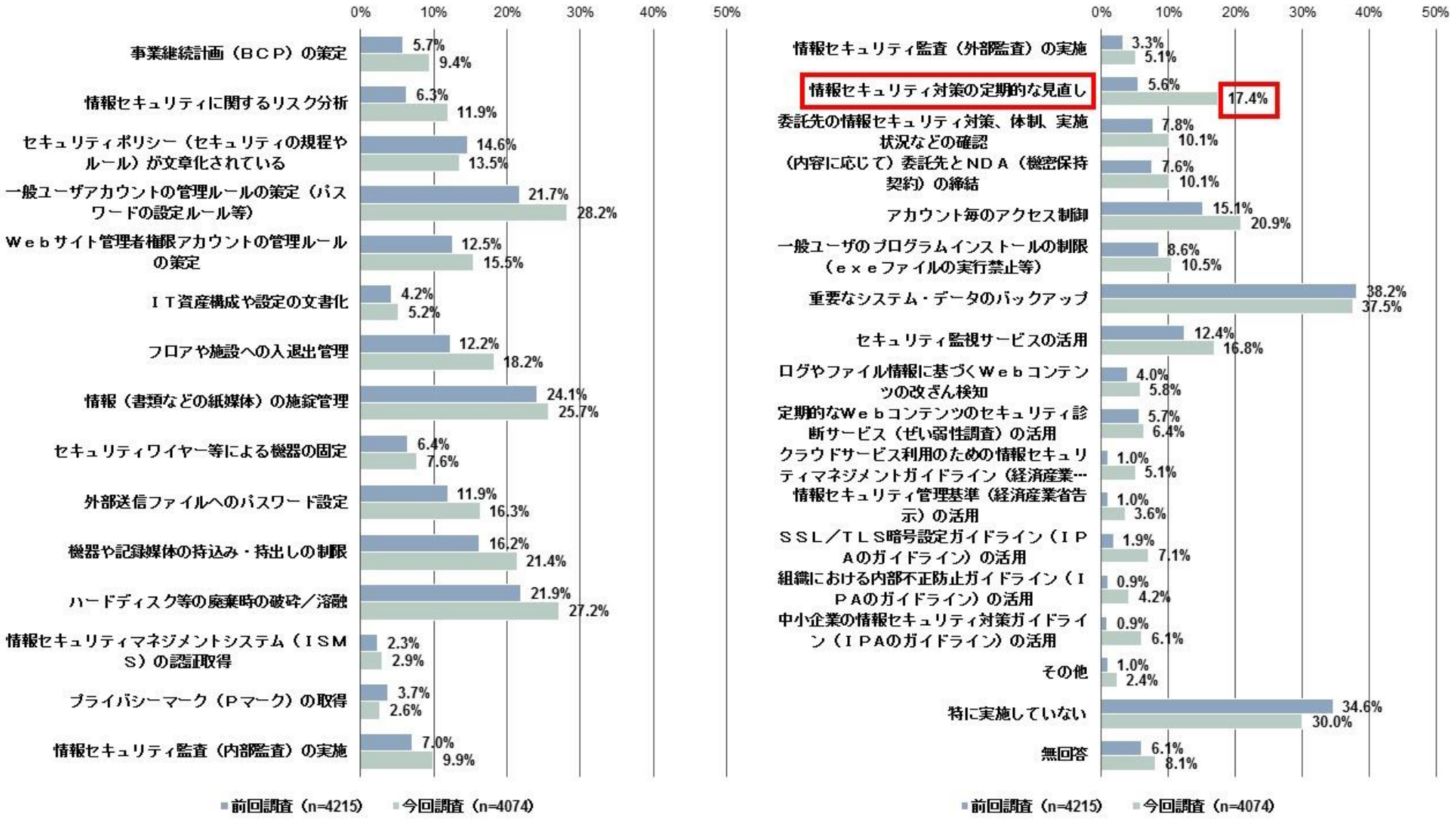
【情報セキュリティ対策投資を行わなかった理由】
（企業規模別）



（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

被害防止のための組織面・運用面での対策は「情報セキュリティ対策の定期的な見直し」が大きく増加

小林勝哉
社会保険労務士事務所



前回調査（2016年） vs 今回調査（2021年） の5年間の変化

（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

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

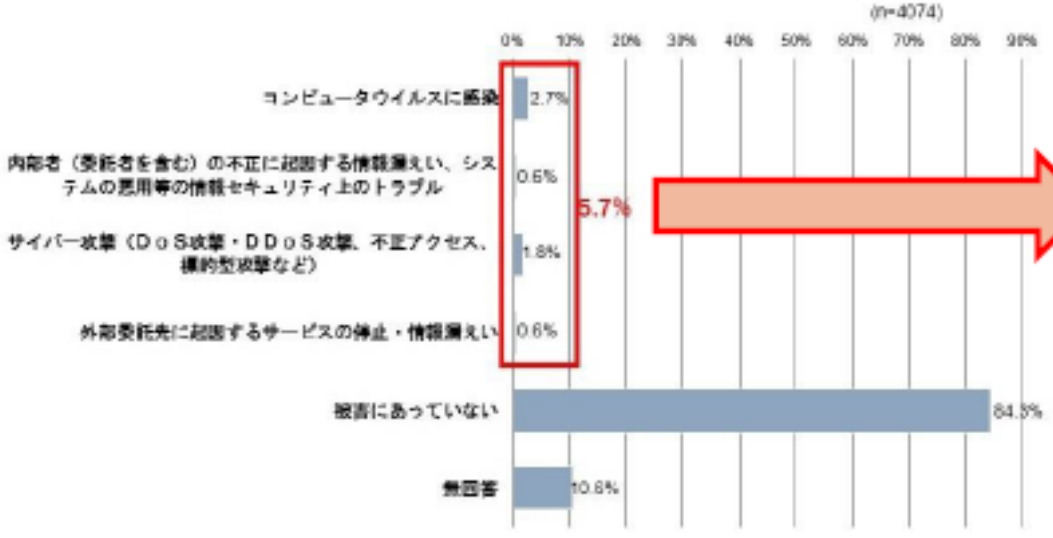
「被害にあっていない」が84.3%、**何らかの被害にあったが5.7%。最多は「ウィルス感染」。**

・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

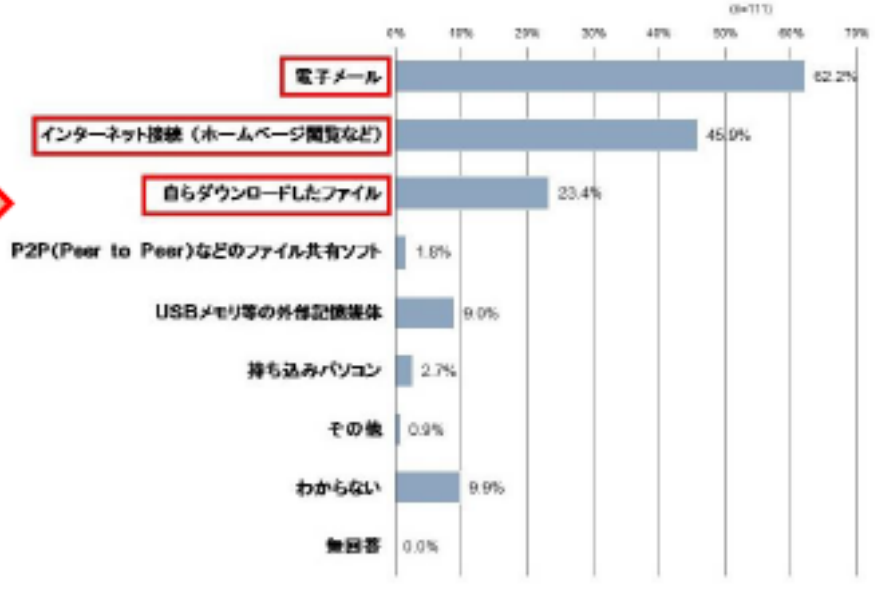
想定される侵入経路は「電子メール」が62.2%、

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】**



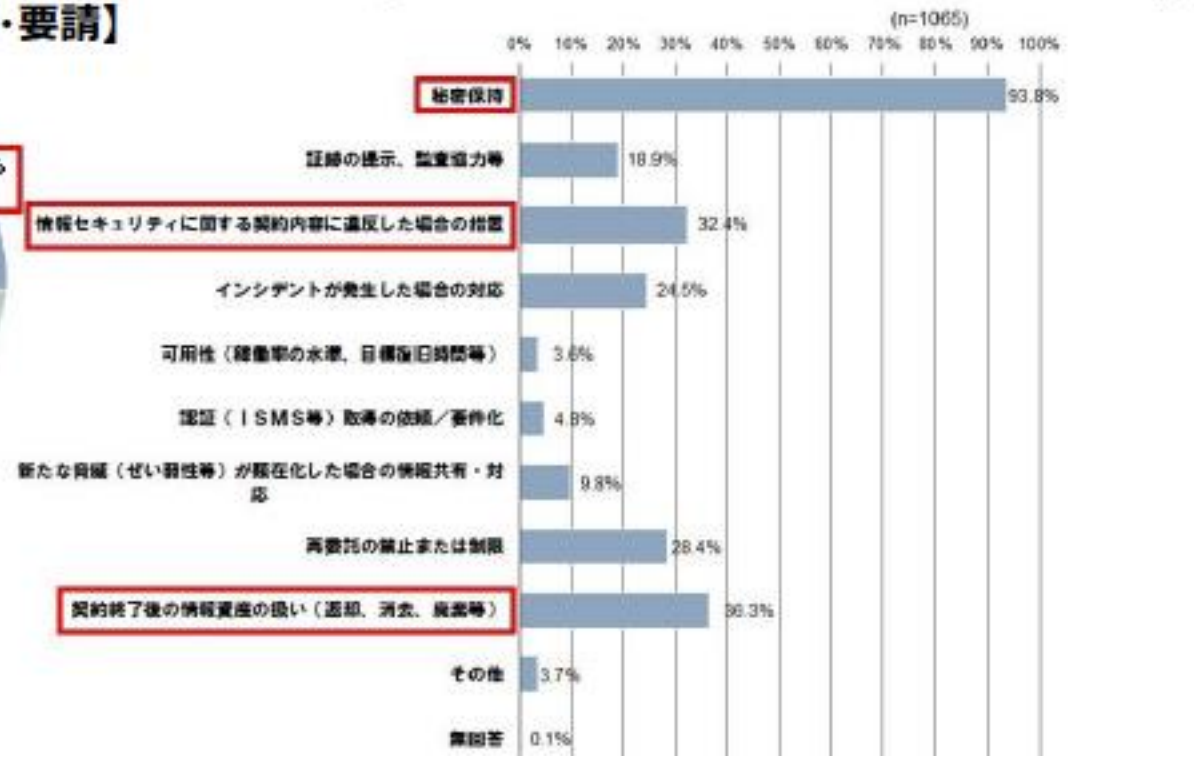
（出典）IPA「2021年度 中小企業における情報セキュリティ対策に関する実態調査」報告書
https://www.ipa.go.jp/security/fy2021/reports/sme/index.html

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

中小企業が狙われる時代

１・サプライチェーン

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

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たることとなり、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」が普及してきました。

一般的な補償内容は、「賠償損害の補償」「事故対応費用の補償」「サービス中断による費用の補償（損失利益）」です。

また、無償の初動相談窓口もあり、いざという時の対応の助けとなります。

「テレワークセキュリティの現状と課題」

小林勝哉
社会保険労務士事務所

・情報セキュリティ10大脅威の動向

・中小企業における情報セキュリティ対策の実態

・不正競争防止法と内部不正防止ガイドライン

ガバナンスとコンプライアンス

➢ ガバナンスとは

「統治」と訳され、**健全な企業経営を行うための管理体制の構築**や企業の内部統治を指します。

具体的には、内部統制やセキュリティなどのリスクマネジメントに特化した専門部署の設置、社外取締役の設置などがあります。

➢ コンプライアンスとは

「法令遵守」と訳され、**全従業員が業務遂行上で守るべき決まりごと**です。

一般的に、倫理規範や就業規則、道徳やマナーまで幅広く含まれます。

コンプライアンスの意識を高めて、管理体制を整えていく活動がガバナンスです。

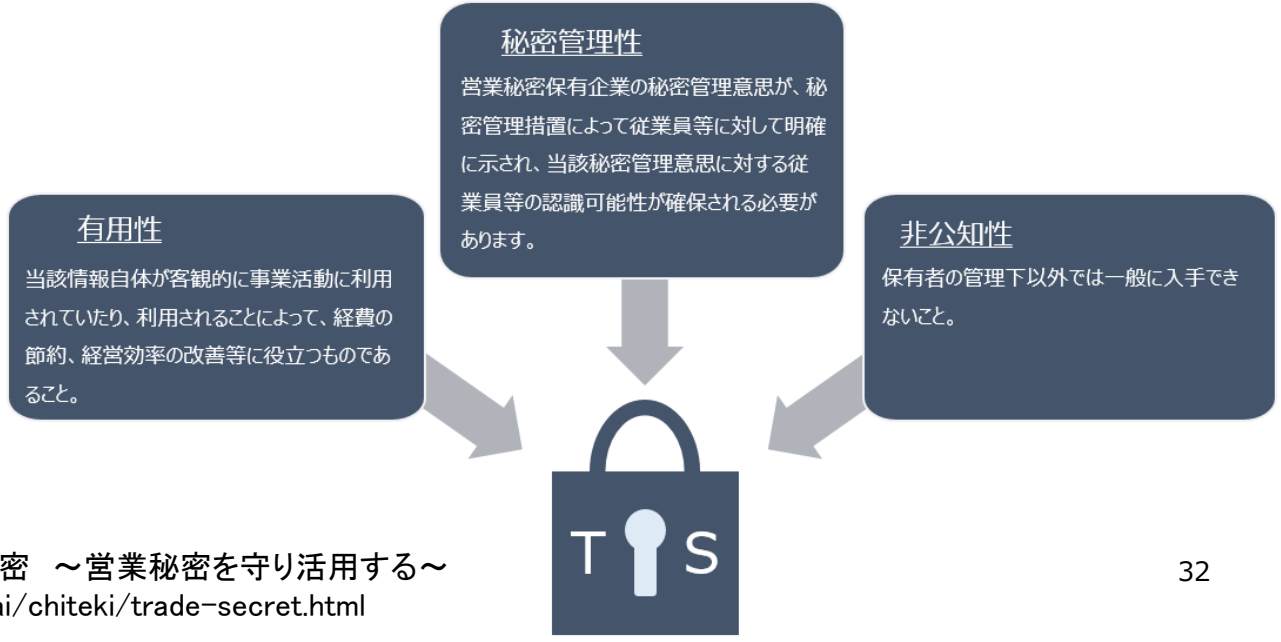
不正競争防止法　営業秘密の取り扱い

経済産業省/公取委では、不正競争防止法における営業秘密の取り扱いを整理し公開しています。

・経済産業省　不正競争防止法 営業秘密のホームページ

～営業秘密を守り活用する～

この中で**「テレワーク時における秘密情報管理のポイント(Q＆A解説)」**が公開されていますので、特に重要な営業秘密の取り扱いをテレワークを通じて行わせる場合には、留意が必要です。（2020年5月）



（出典）経済産業省　不正競争防止法 営業秘密　～営業秘密を守り活用する～
https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html

IPA　組織における内部不正防止ガイドライン

内部不正防止の重要性や、対策の体制、関連する法律等の概要を説明。

10の観点で、合計33項目の対策を示しています。

(2022年4月、第5版)

【改訂ポイント】

1. 事業経営に及ぼすリスクを強調
2. 組織外での秘密情報の取扱増加に伴うリスクを追記
3. 雇用の流動化による退職者増加がもたらすリスクを追記
4. セキュリティ技術の急速な進展と個人情報に配慮した運用を追記
5. 法改正に伴う対策の強化

（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/

IPA　組織における内部不正防止ガイドライン

【10の観点】

（主に情報セキュリティ規程に反映）

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）

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/

IPA　組織における内部不正防止ガイドライン

（主に情報セキュリティ規程に反映）　（主に就業規則に反映）

基本方針	(1)経営者の責任の明確化	**原因究明と証拠確保**	(18)情報システムにおけるログ・証跡の記録と保存
	(2)総括責任者の任命と組織横断的な体制構築		(19)システム管理者のログ・証跡の確認
資産管理	(3)情報の格付け区分	**人的管理**	(20)教育による内部不正対策の周知徹底
	(4)格付け区分の適用とラベル付け		(21)従業員モニタリングの目的等の就業規則での周知
	(5)情報システムにおける利用者のアクセス管理		(22)派遣労働者による守秘義務の遵守
	(6)システム管理者の権限管理		(23)雇用終了の際の人事手続き
	(7)情報システムにおける利用者の識別と認証		(27)雇用終了及び契約終了による情報資産等の返却
物理的管理	(8)物理的な保護と入退管理	**コンプライアンス**	(25)法的手続きの整備
	(9)情報機器及び記録媒体の資産管理及び物理的な保護		(26)誓約書の要請
	(10)情報機器及び記録媒体の持出管理	**職場環境**	(27)公平な人事評価の整備
	(11)個人の情報機器及び記録媒体の業務利用及び持込の制限		(28)適正な労働環境及びコミュニケーションの推進
技術・運用管理	(12)内部不正モニタリングシステムの適用		(29)職場環境におけるマネジメント
	(13)ネットワーク利用のための安全管理	**事後対策**	(30)事後対策に求められる体制の整備
	(14)重要情報の受渡し保護		(31)処罰等の検討及び再発防止
	(15)情報機器や記録媒体の持ち出しの保護	**組織の管理**	(32)内部不正に関する通報制度の整備
	(16)組織外部での業務における重要情報の保護		(33)内部不正防止の観点を含んだ確認の実施
	(17)業務委託時の確認（第三者が提供するサービス利用時を含む）		

（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/

IPA　組織における内部不正防止ガイドライン

➢ 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。

◇テレワークに関する対策として追記された項目（2022年4月）

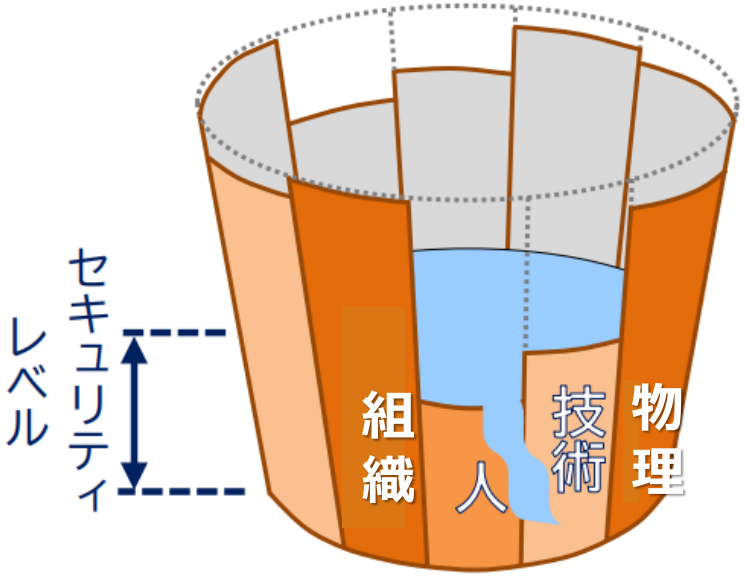
節・項目	対策の指針	関連する対策のポイント（要旨）
4-4.技術・運用管理	(13) ネットワーク利用のための安全管理	■ 組織外部で使用するPC等の対策強化 ■ ローカルブレイクアウト利用時の対策
	(16) 組織外部での業務における重要情報の保護	■ 重要情報と通信の暗号化 ■ テレワーク用PC等のローカル保存、組織内の重要情報への細かいアクセス制御 ■ 採用するテレワーク方式の特性に則した情報漏えい対策の強化 ■ テレワーク時の遵守ルール ■ クラウド等の外部サービス利用時のルール ■ クラウドサービス方式でテレワークを行う場合の対策 ■ 海外からのテレワーク ■ EDRやゼロトラストの概念の適用
	(17)業務委託時の確認（第三者が提供するサービス利用時を含む）	■ 委託先のテレワークセキュリティ対策の確認 ■ 個人情報漏えい事故発生時に委託先が負う義務
4-5.原因究明と証拠確保	(18)情報システムにおけるログ・証跡の記録と保存	■ テレワークに伴う履歴等の取得
4-6.人的管理	(20)教育による内部不正対策の周知徹底	■ テレワークを行う役職員等の実践的な教育・訓練 ■ 組織がテレワークを行う役職員を守ることの周知
4-8.職場環境	(27)公平な人事評価の整備	■ テレワークを行う従業員の公平な処遇
	(28)適正な労働環境及びコミュニケーションの推進	■ テレワークを行う役職員のコミュニケーションの確保
	(29)職場環境におけるマネジメント	■ テレワーク中の単独作業への対策
4-9.事後対策	(30)事後対策に求められる体制の整備	■ テレワーク中の内部不正に対応できるログ・証跡の取得

（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/files/000097371.pdf

セキュリティは「組織」・「人」・「物理」・「技術」のバランス

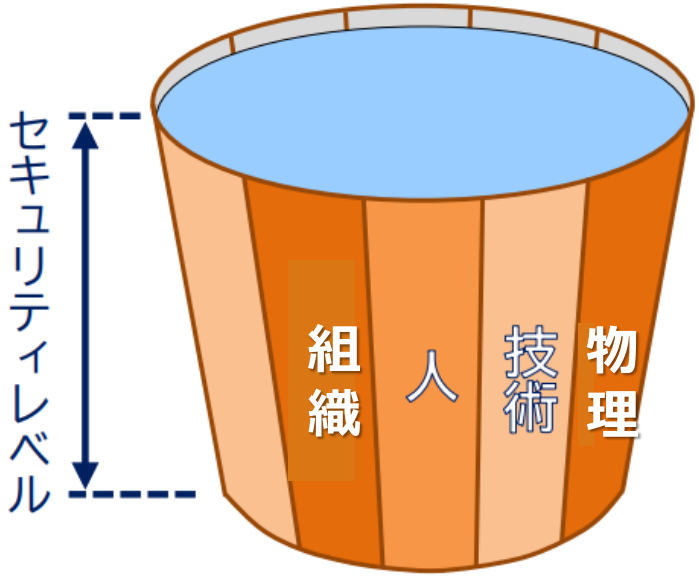
➢ テレワークセキュリティの対策は、技術的対策だけでなく、
人に着目した内部不正防止の組織的ガバナンスが重要。

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）　筆者加筆
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

テレワークにおける就業規則のポイント

「テレワークにおける就業規則のポイント」

小林勝哉
社会保険労務士事務所

- テレワーク制度導入に共通の留意点
- テレワーク勤務規程の規定例
- テレワーク勤務の対象者
- テレワーク勤務時の服務規律

テレワーク勤務に関連する法令遵守のポイント

小林勝哉
社会保険労務士事務所

遵守すべき法令は、オフィスワークと同様です。

■自営型テレワーク

下請法

独占禁止法

フリーランス
ガイドライン
など

■雇用型テレワーク

労働基準法

労働安全衛生法

最低賃金法

労働施策総合推進法

男女雇用機会均等法

育児・介護休業法

テレワークガイドライン、など

■共通

民法

憲法（特に、基本的人権）

テレワーク勤務に共通の留意点

テレワーク勤務制度において改善が必要なことや問題点について、多くの会社で共通の悩みがあげられます。

それらについて、厚生労働省から、ガイドラインとQ&Aが出されていますので、まずは点検してみてください。

- **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（テレワークガイドライン）**

  https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/koyou_roudou/roudoukijun/shigoto/guideline.html

- **テレワークに関するQ&A（テレワーク総合ポータルサイト）**

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

テレワークの活用に必要な取り組み

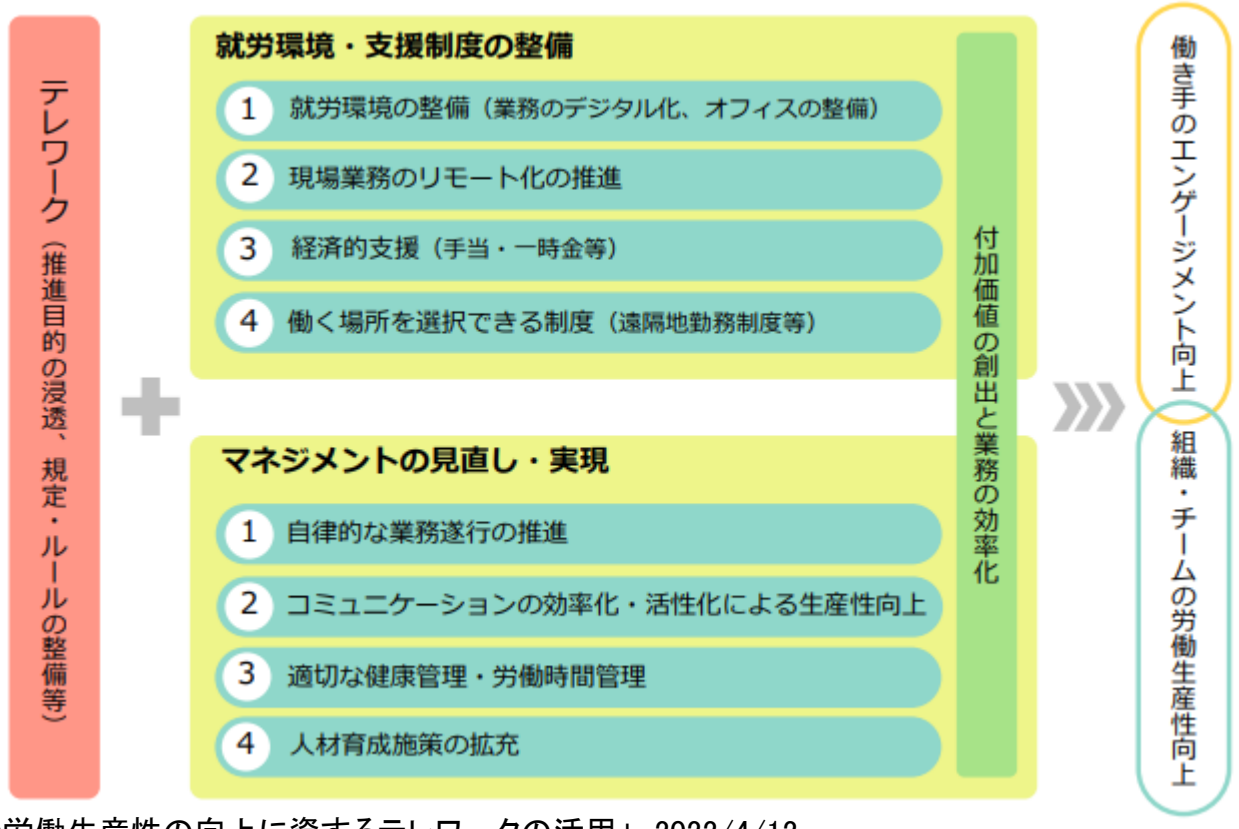
「制度」と「マネジメント」の両面からの取り組みが必要となります。

1・「就労環境・支援制度の整備」

業務のデジタル化や経済的支援など

2・「マネジメントの見直し・実現」

業務遂行や
コミュニケーション、
健康管理など



（出典）経団連　報告書「エンゲージメントと労働生産性の向上に資するテレワークの活用」 2022/4/12
https://www.keidanren.or.jp/policy/2022/036.html

テレワーク勤務制度の導入に共通の留意点

➢ テレワーク勤務制度導入の手順

01　テレワーク勤務制度の全体像をつかむ

02　テレワーク勤務制度導入の方針決定

03　テレワーク勤務のルールづくりと規程、運用、勤怠管理整備

04　実施場面を想定したICT環境とセキュリティの確認/検討/対策

05　制度についての従業員への周知および説明と管理者への教育

06　制度導入実施（トライアル/本格）

07　PDCA

「テレワークにおける就業規則のポイント」

小林勝哉
社会保険労務士事務所

・テレワーク制度導入に共通の留意点

・テレワーク勤務規程の規定例

・テレワーク勤務の対象者

・テレワーク勤務時の服務規律

テレワーク勤務規程の位置づけ

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～　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の規定例

- 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。

「テレワークにおける就業規則のポイント」

小林勝哉
社会保険労務士事務所

・テレワーク制度導入に共通の留意点

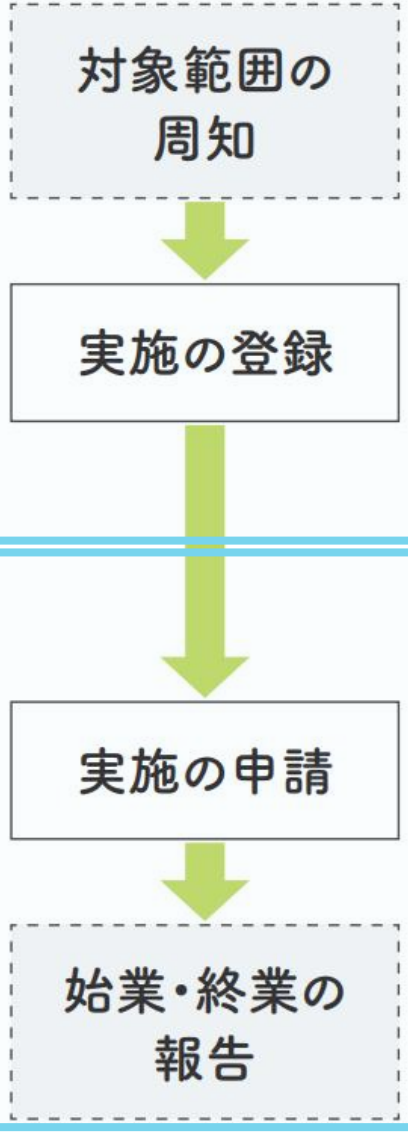
・テレワーク勤務規程の規定例

・テレワーク勤務の対象者

・テレワーク勤務時の服務規律

テレワーク実施までの手続き

【テレワーク実施の申請と承認プロセスの例】



安全衛生/セキュリティ等に関する事前確認
（1年単位など定期確認方法も定める）

ルール策定のポイント

登録
- 誰が（希望者が/希望者の上司が）
- どこに（部署に/上司に）
- どうやって（電子メールで/Webシステム上で/書面で）
- 条件（上司との面談を経て）

承認
- 条件
（対象者の条件を満たしていれば、自動で承認する/面談を経て承認する）

申請
- 誰が（希望者が）
- いつ（当日に/前日までに）
- どこに（上司に/部署に）
- どうやって（電子メールで/Webシステム上で/書面で）

承認
- 条件
（上司の許可を経て/実施する業務を決めた上で）

実際のテレワーク勤務の服務承認
（いつまでにどこに申請するか定める）

（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～　筆者加筆
https://telework.mhlw.go.jp/wp/wp-content/uploads/2022/06/teleworkmodel.pdf

テレワーク勤務の対象者

【対象者に制限を設ける規定例】

第ｘ条　在宅勤務の対象者は、就業規則第〇条に規定する従業員であって次の各号の条件を全て満たした者とする。

（１）在宅勤務を希望する者

（２）自宅での業務が円滑に遂行できると認められる者

（３）自宅の執務環境及びセキュリティ環境が適正と認められる者

（解説）

第２号において、「対象者の自律性」を要件としています。

なお、会社の実情によって勤続年数を設定することもできますし、対象者の自律性には言及しないで勤続年数だけに限定することもできます。

（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～
https://telework.mhlw.go.jp/wp/wp-content/uploads/2022/06/teleworkmodel.pdf

テレワーク勤務の対象者

【対象者に制限を設ける規定例】（続き）

第ｘ条　在宅勤務の対象者は、就業規則第〇条に規定する従業員であって次の各号の条件を全て満たした者とする。

（１）在宅勤務を希望する者

（２）自宅での業務が円滑に遂行できると認められる者

（３）自宅の執務環境及びセキュリティ環境が適正と認められる者

（解説）

第３号において、「安全衛生」「セキュリティ環境」を要件としています。

自宅等でテレワークを行う際の作業環境整備の留意点がテレワークガイドラインに記載されています。作業環境を確認するためのチェックリスト（労働者用）を活用し、報告を求めるとともに、労使が協力して改善を図りましょう。必要な場合は、サテライトオフィス等の活用も考えられます。

（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～　筆者加筆
https://telework.mhlw.go.jp/wp/wp-content/uploads/2022/06/teleworkmodel.pdf

作業環境を確認するためのチェックリスト（労働者用）

テレワークガイドライン 作業環境を確認するためのチェックリスト(労働者用)

1　作業場所やその周辺の状況について

2　作業環境の明るさや温度等について

3　休憩等について

4　その他

（解説）

1　このチェックリストは、自宅等においてテレワークを行う際の作業環境について、安全衛生の側面から、テレワークを行う従業員本人が確認する際に活用いただくことを目的としています。

2　確認した結果、すべての項目に☑が付くように、不十分な点があれば事業者と話し合って改善を図るなどにより、適切な環境下でテレワークを行うようにしましょう。

（出典）厚生労働省　（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】
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/koyou_roudou/roudoukijun/shigoto/guideline.html

「テレワークにおける就業規則のポイント」

小林勝哉
社会保険労務士事務所

・テレワーク制度導入に共通の留意点

・テレワーク勤務規程の規定例

・テレワーク勤務の対象者

・テレワーク勤務時の服務規律

テレワーク勤務時の服務規律

第ｘ条　在宅勤務者は就業規則第○条及びセキュリティガイドラインに定めるもののほか、次に定める事項を遵守しなければならない。

（１）在宅勤務中は業務に専念すること。

（２）在宅勤務の際に所定の手続に従って持ち出した会社の情報及び作成した成果物を第三者が閲覧、コピー等しないよう最大の注意を払うこと。

（解説）

第１号はテレワーク勤務時の職務専念義務です。就業規則本文で定めていれば十分とも考えられますが、職務専念義務について注意喚起する効果が期待できます。

第２号は持ち出した情報の管理方法について定めていますが、親族でも不用意に情報が目に触れることは望ましくないとする場合、「従業員の親族を第三者とみなす」と規定することもできます。

（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～
https://telework.mhlw.go.jp/wp/wp-content/uploads/2022/06/teleworkmodel.pdf

テレワーク勤務時の服務規律（続き）

（３）第２号に定める情報及び成果物は紛失、毀損しないように丁寧に取扱い、セキュリティガイドラインに準じた確実な方法で保管・管理しなければならないこと。

（４）在宅勤務中は自宅以外の場所で業務を行ってはならないこと。

（解説）

第４号は就業場所を自宅に限定していますが、例えば、「親の介護のために親の家で仕事をしたい」などという要望に応じる対応策としては、「会社が指定する場所」との規定を設ける方法があります。

（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～
https://telework.mhlw.go.jp/wp/wp-content/uploads/2022/06/teleworkmodel.pdf

テレワーク勤務時の服務規律（続き）

（５）モバイル勤務者は、会社が指定する場所以外で、パソコンを作動させたり、重要資料を見たりしてはならないこと。

（６）モバイル勤務者は、公衆無線LANスポット等漏洩リスクの高いネットワークへの接続は禁止すること。

（７）在宅勤務の実施に当たっては、会社情報の取扱いに関し、セキュリティガイドライン及び関連規程類を遵守すること。

（解説）

第５号と第６号はモバイル勤務時の注意事項です。

第７号のセキュリティガイドラインは、各企業の内規です。

- 基本方針：セキュリティ全体の根幹となる方針
- 対策基準：基本方針に基づき実施すべきことや守るべきことの規定
- 実施手順：対策基準に規定された事項を具体的に実行するための手順

（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～
https://telework.mhlw.go.jp/wp/wp-content/uploads/2022/06/teleworkmodel.pdf

内部通報制度は“組織を守る”最後の砦

就業規則　第ｘ条　（公益通報者の保護）

会社は、労働者から組織的又は個人的な法令違反行為等に関する相談又は通報があった場合には、別に定めるところにより処理を行う。

（解説）

法令違反行為を労働者が通報した場合、解雇等の不利益な取扱いから保護し、事業者のコンプライアンス（法令遵守）経営を強化するために、改正公益通報者保護法が2022年6月に施行されました。

新たに、①従事者を指定する義務と②公益通報に対応するための体制を整備する義務等が加わっています。（従業員数が300名以下の事業者については努力義務）

「公益通報」とは、①労働者等が、②役務提供先の不正行為を、③不正の目的でなく、④一定の通報先に通報することをいいます。

（出典）消費者庁　公益通報者保護法と制度の概要
https://www.caa.go.jp/policies/policy/consumer_partnerships/whisleblower_protection_system/overview/

小林勝哉
社会保険労務士事務所

テレワークにおける
情報セキュリティ規程のポイント

「テレワークにおける
情報セキュリティ規程のポイント」

小林勝哉
社会保険労務士事務所

- テレワーク勤務規程に示すセキュリティガイドラインとは
- 情報マネジメントシステムの基本
- 情報セキュリティ対策、まずは何から？
- テレワークにおける情報セキュリティ規程の構成

テレワーク勤務規程に示すセキュリティガイドラインとは

「情報セキュリティ規程」（セキュリティガイドライン）

◆基本方針：セキュリティ全体の根幹となる方針

◆対策基準：基本方針に基づき実施すべきことや守るべきことの規定

◆実施手順：対策基準に規定された事項を具体的に実行する手順

（解説）

セキュリティガイドラインとは、各企業の内規である情報セキュリティ規程です。

内容は、企業ごとに異なります。

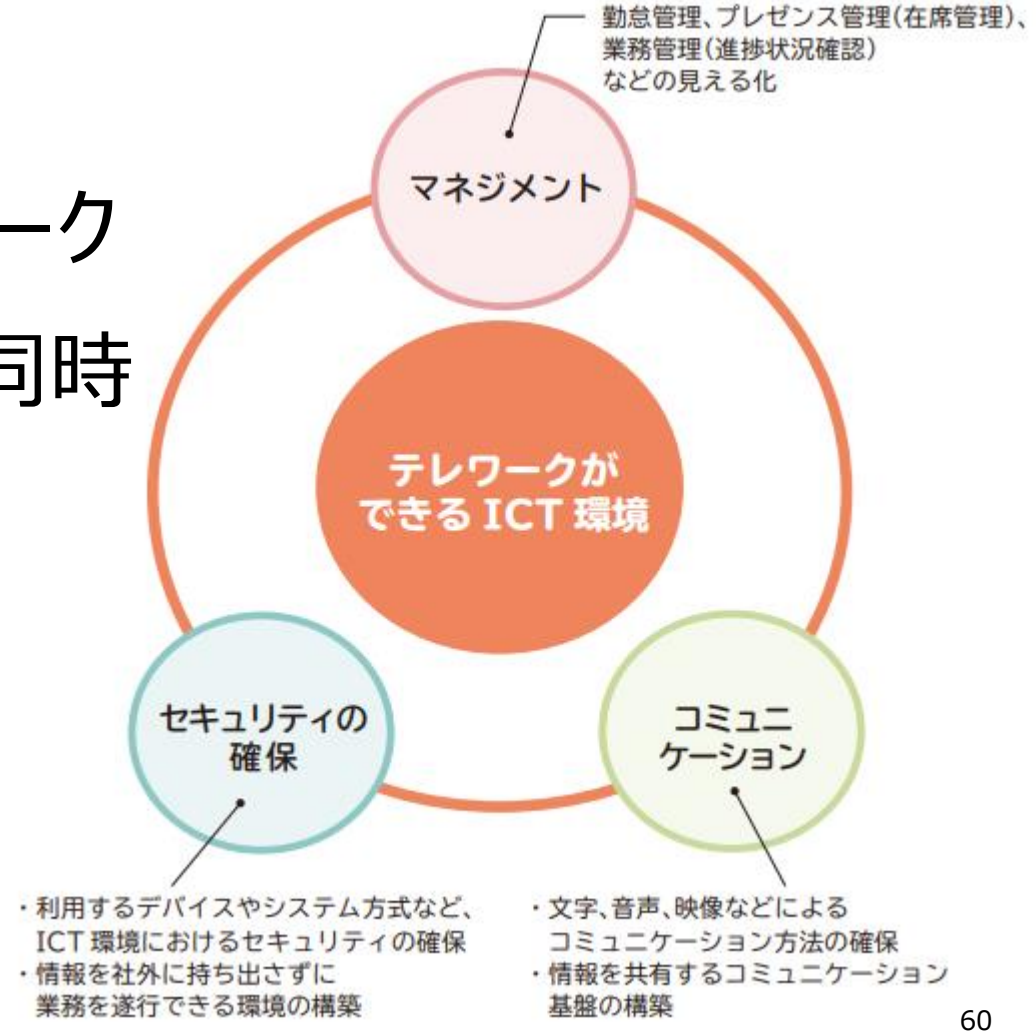
特に、テレワークに着目したセキュリティ対策として、オフィス外からのアクセスや電子メール送受信などに関する制限、顧客との打合せで発生するデータや端末持ち出し手続きなど、業務を行う上で通常順守すべきセキュリティの考え方を具体的に規定しましょう。

（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～
https://telework.mhlw.go.jp/wp/wp-content/uploads/2022/06/teleworkmodel.pdf

ICT環境に適したセキュリティ対策

テレワークの実施形態によってICT環境が異なりますので、ICT環境に適したセキュリティ対策が必要です。

ICT環境は、安全なテレワークのためのセキュリティ対策と同時に検討を進めます。



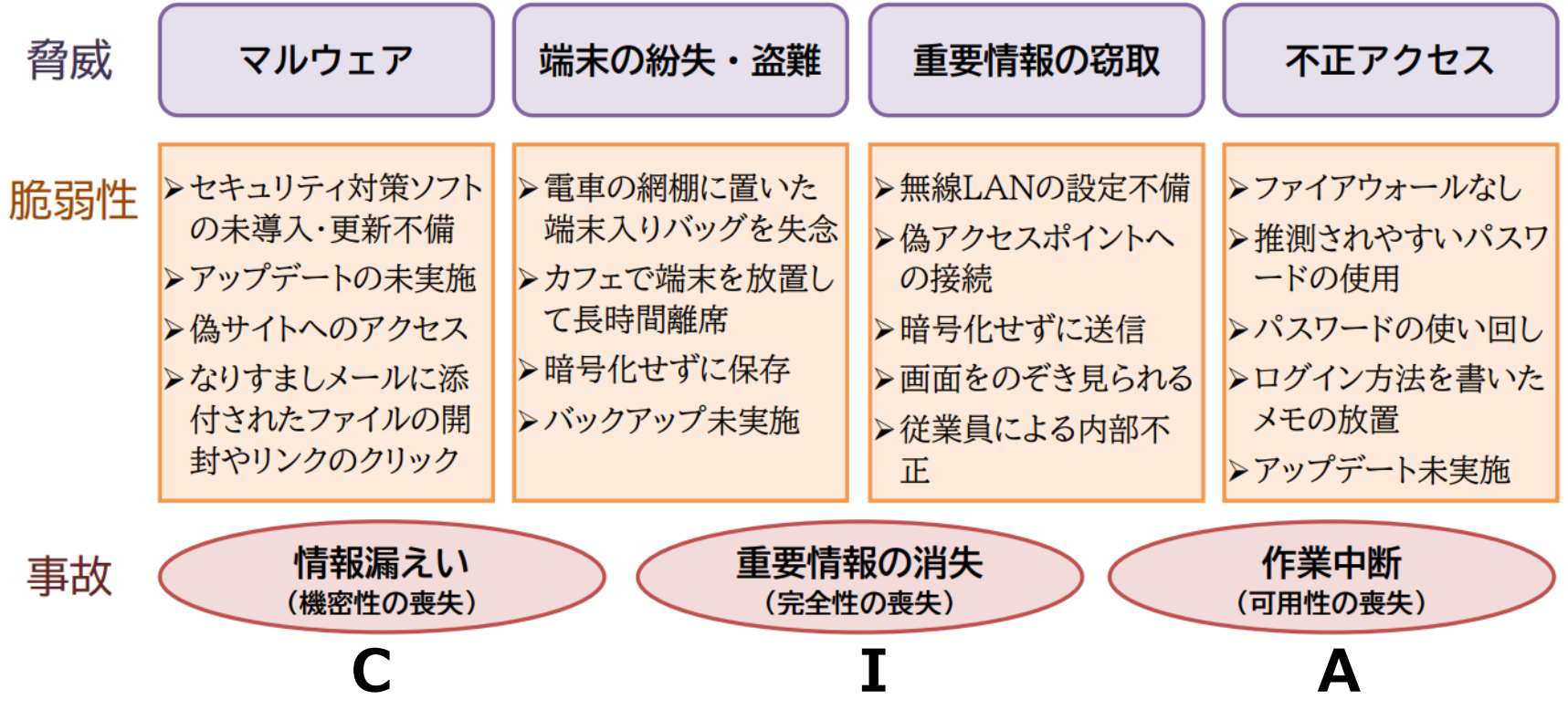
(出典)厚生労働省　テレワークの導入・運用ガイドブック
https://telework.mhlw.go.jp/wp/wp-content/uploads/2019/12/H28hatarakikatakaikaku.pdf

テレワーク環境におけるセキュリティ・リスクの一例

情報セキュリティの3要素　CIA

「機密性」（Confidentiality）、「完全性」（Integrity）、「可用性」（Availability）を確保できるか、リスクアセスメントを行いましょう。

こちらは、テレワーク環境におけるセキュリティ・リスクの一例です。

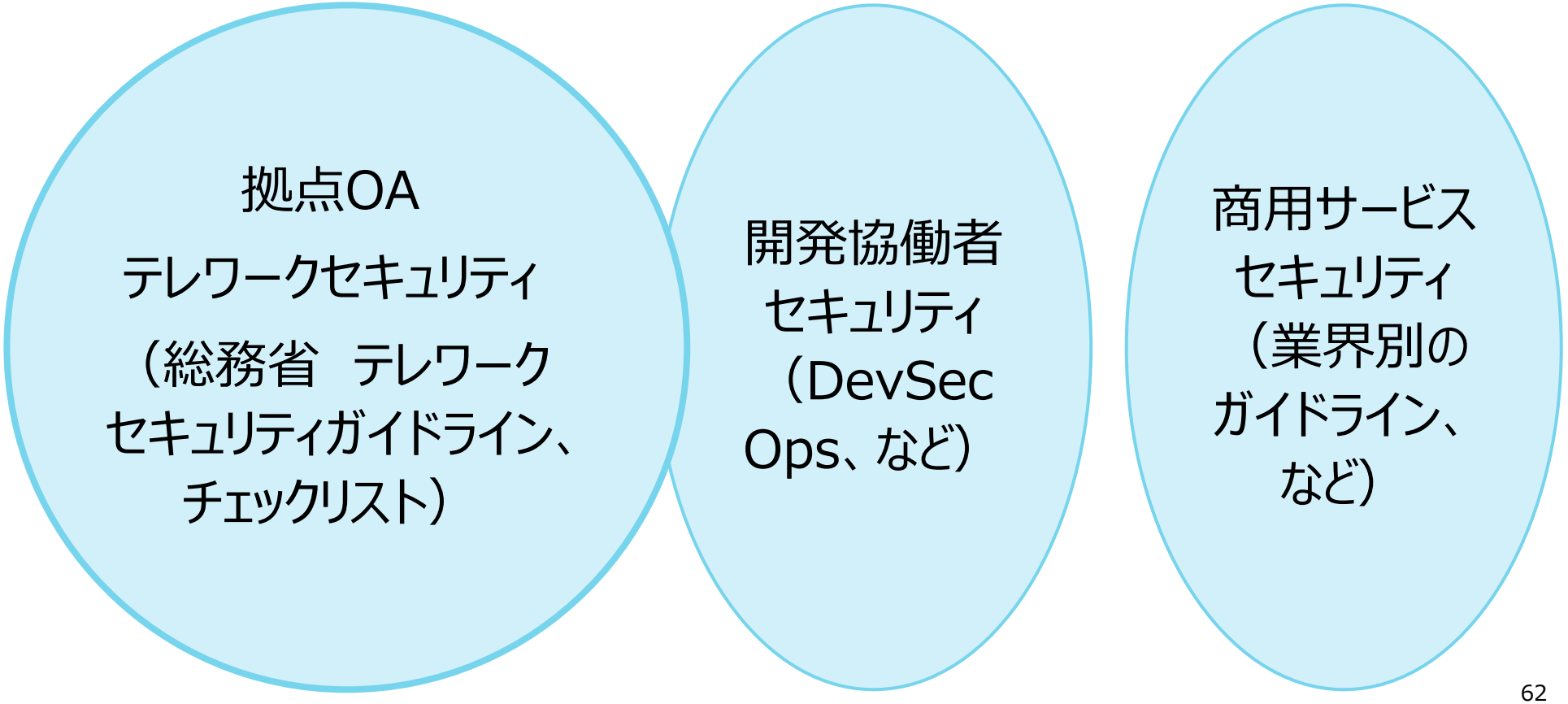


（出典）総務省　テレワークセキュリティガイドライン（第5版）　筆者加筆
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

業務別セキュリティードメインの考え方

テレワークセキュリティを考えるにあたっては、業務別セキュリティードメインの考え方を取り入れて要件を整理することが必要となります。

例えば、次のような業務別のネットワーク構成が考えられますが、テレワークセキュリティでは拠点OA業務が対象となることが一般的です。



「テレワークにおける
情報セキュリティ規程のポイント」

小林勝哉
社会保険労務士事務所

・テレワーク勤務規程に示すセキュリティガイドラインとは

・情報マネジメントシステムの基本

・情報セキュリティ対策、まずは何から？

・テレワークにおける情報セキュリティ規程の構成

マネジメントシステムの着眼点

➢ マネジメントシステムの着眼点＝機会を伸ばし、リスクを管理

１・事業活動との一致、経営層の関与

２・機会をとらえた意図した結果の達成

３・リスクマネジメント活動

４・内外とのコミュニケーション、マネジメントシステム自体がPDCA

➢ 機会とは：意図した結果を達成するのに好ましい状況

（ビジネスチャンス、成長戦略、テレワークの定着、など）

➢ リスクとは：目的に対する不確かさ

（新たな脅威、法令の要求事項、契約上の義務、

内外のセキュリティインシデント、技術の変化、など）

代表的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

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

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

◆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。

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

自社のテレワーク環境の現状と改善点を把握し、テレワークのセキュリティ対策として推奨される対策の中から、対処方法を決定します。

（支援ツールの一例）

「テレワーク環境セキュリティ対策簡易チェック」（株式会社ラック、無料）

https://www.lac.co.jp/telework/security_check.html

自組織の現状を26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。

「テレワークにおける
情報セキュリティ規程のポイント」

小林勝哉
社会保険労務士事務所

・テレワーク勤務規程に示すセキュリティガイドラインとは

・情報マネジメントシステムの基本

・情報セキュリティ対策、まずは何から？

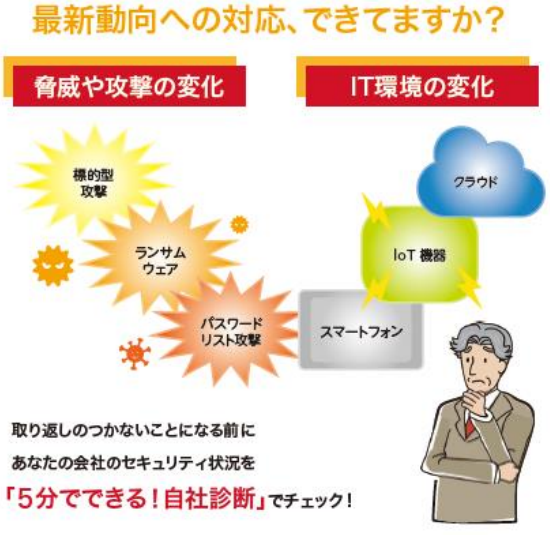
・テレワークにおける情報セキュリティ規程の構成

情報セキュリティ対策、まずは何から？

１・組織として

組織として留意することは、情報セキュリティ規程の整備と教育訓練です。

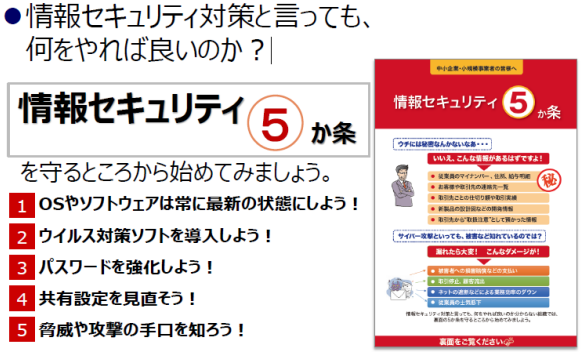
まずは、IPAの「５分でできる！情報セキュリティ自社診断」などを用いて、点検してみましょう。



２・個人として

個人が留意することは、

IPAの「情報セキュリティ５か条」などに明確です。



（出典）IPA　中小企業の情報セキュリティ対策ガイドライン
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

SECURITY ACTION 「二つ星」をめざそう

・SECURITY ACTION（セキュリティ対策自己宣言）「二つ星」とは

「５分でできる！情報セキュリティ自社診断」で自社の状況を把握し、「情報セキュリティポリシー(基本方針)」を定め、外部に公開したことを宣言することです。

・組織として規程の整備や教育訓練に向け、特にこれらの観点を点検しましょう。

Part 3 組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	4	2	0	−1
	20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？	4	2	0	−1
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	4	2	0	−1
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？	4	2	0	−1
	23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？	4	2	0	−1
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	4	2	0	−1
	25	情報セキュリティ対策（上記１～24など）をルール化し、従業員に明示していますか？	4	2	0	−1

（出典）IPA　SECURITY ACTION（セキュリティ対策自己宣言）
https://www.ipa.go.jp/security/security-action/sa/index.html

モバイル、サテライトオフィス、ワーケーションに向けて

テレワーク勤務制度として、モバイル、サテライトオフィス、ワーケーションを行う場合は、特に**無線LAN（Wi-Fi）のセキュリティ確保**の対策が重要となります。

・手引き

総務省「Wi-Fi利用者／Wi-Fi提供者向けのセキュリティ対策の手引き」

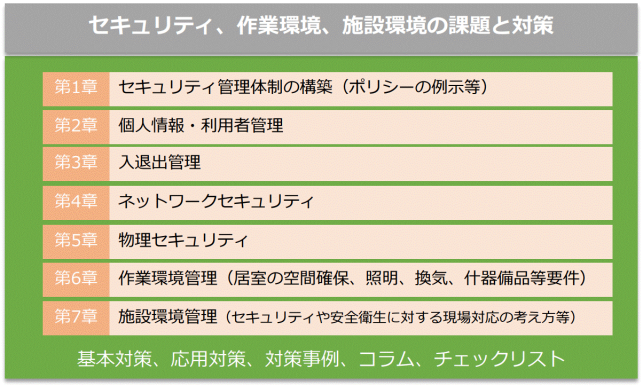
・施設認証

日本テレワーク協会「安心安全テレワーク施設認証プログラム」

テレワーク施設の情報セキュリティおよび

作業環境に係る安全性を検査し、認証。

法人契約の参考となるでしょう。



「安心安全テレワーク施設ガイドライン（第1版）」

（出典）総務省　無線LAN（Wi-Fi）の安全な利用（セキュリティ確保）について
https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/
日本テレワーク協会　安心安全テレワーク施設認証
https://japan-telework.or.jp/workation_top/security/

「テレワークにおける
情報セキュリティ規程のポイント」

小林勝哉
社会保険労務士事務所

・テレワーク勤務規程に示すセキュリティガイドラインとは

・情報マネジメントシステムの基本

・情報セキュリティ対策、まずは何から？

・テレワークにおける情報セキュリティ規程の構成

テレワークにおける情報セキュリティ規程の構成

「情報セキュリティ規程」（セキュリティガイドライン）

１・基本方針（セキュリティポリシー）

セキュリティ全体の根幹となる方針

２・対策基準

基本方針に基づき実施すべきことや守るべきことの規定

３・実施手順

対策基準に規定された事項を具体的に実行するための手順

（解説）

情報セキュリティ規程は、一般的にこれらの3つで構成されます。

テレワーク勤務規程では、セキュリティガイドラインを遵守することを規定します。「情報セキュリティ規程」（セキュリティガイドライン）を作成・点検し、テレワークセキュリティについても対応した表現を反映しましょう。

「１・基本方針」の構成

1.経営者の責任

2.社内体制の整備

3.従業員の取組み

4.法令及び契約上の要求事項の遵守

5.違反及び事故への対応

（解説）

基本方針は、経営者がコミットするセキュリティ全体の根幹となる方針です。テレワークセキュリティについても対応した基本方針を、作成・点検しましょう。

基本方針は、広く社外に公開し、サプライチェーンを構成する発注元企業を含む幅広い取引先などステークホルダーの信頼を得る第一歩とすることが大切です。

（出典）IPA　中小企業の情報セキュリティ対策ガイドライン
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

「２・対策基準」の構成

1.推進組織体制

2.方法論、実行手段、技術等の標準

（解説）

対策基準は、基本方針を実行に移すために必要となる共通の遵守事項や判断基準を定めたものです。情報セキュリティに関するリスクマネジメントが有効に行われているかを評価する基準となるものです。

技術的管理策としてベストプラクティスを整理したものが、国際規格や業界や公的機関でまとめられていますので必要に応じ参照してください。

（出典）IPA　中小企業の情報セキュリティ対策ガイドライン
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

「3・実施手順」の構成

1.組織的対策
2.人的対策
3.情報資産管理
4.アクセス制御及び認証
5.物理的対策
6.IT機器利用
7.IT基盤運用管理
8.システム開発及び保守
9.委託管理
10.情報セキュリティインシデント対応ならびに事業継続管理
11.個人番号及び特定個人情報の取り扱い

（解説）
実施手順は、IPAの情報セキュリティ関連規程（サンプル）をもとに、必要な対策を選択し、編集することで自社の情報セキュリティ関連規程を作成することができます。

（出典）IPA　中小企業の情報セキュリティ対策ガイドライン
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

「３・実施手順」の組織的対策

1.情報セキュリティのための組織

情報セキュリティ責任者

情報システム管理者、教育責任者

インシデント対応責任者、監査・点検責任者

特定個人情報事務取扱責任者／担当者、個人情報管理責任者

（解説）

組織的対策では、情報セキュリティ対策を推進するための組織として、情報セキュリティ責任者をトップとする情報セキュリティ委員会を設置することが望ましいとされています。

（出典）IPA　中小企業の情報セキュリティ対策ガイドライン
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

「３・実施手順」の人的対策

2.人的対策

・雇用条件　　（秘密保持契約の締結など）

・従業員の責務（営業秘密の守秘義務）

・雇用の終了　　（情報資産の返還、守秘義務）

・情報セキュリティ教育、人材育成（年度単位で計画する）

（解説）

人的対策では、全従業員（取締役、社員、派遣社員、パート・アルバイトを含む）を対象とするリスクマネジメントの手順を明確にします。

必要に応じて、就業規則の懲戒処分の規定内容との整合性を点検します。

（出典）IPA　中小企業の情報セキュリティ対策ガイドライン
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

小林勝哉
社会保険労務士事務所

テレワークの
成功事例

中小企業における情報セキュリティ対策事例から

「不正アクセス被害」をきっかけにぜい弱性診断や対策強化を実施！

会社概要　東京都、従業員数 20名弱、情報通信業

（特徴）

・ハッキングによる不正アクセス被害の対策

性善説では情報セキュリティは成り立たない！との意識で対策実施。

外部事業者を活用した自社サービスのぜい弱性診断を実施し、お墨付き。

・効果

業界的には内部者からの情報漏えいが多く、内部マネジメント体制を整えた。

兼務者3名の担当者で、セキュリティワイヤー設置、社内の体制整備、取引先の要請への対応などを行っている。加えて、自社の体制・仕組みが機能していることを、内部監査や外部監査等を通じチェックし改善している。

最近では、基幹業務のクラウド化と情報セキュリティ対策強化の結果、テレワークを増やした際も比較的スムーズに対応することができ、対策に取り組んだメリットの1つでもある。

（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」事例集　P26　筆者要約
https://www.ipa.go.jp/files/000098149.pdf

都内企業に学ぶテレワーク実践事例集から

生産性向上とセキュアな環境の確保を実現！

お客様情報を扱うためセキュアな環境を重視し、サテライトオフィスの積極活用を推奨。

株式会社東急エージェンシー

（発表資料）

https://www.hataraku.metro.tokyo.lg.jp/hatarakikata/telework/16_jirei.pdf

（特徴）

・経営課題　長時間労働の改善を含む生産性向上とワーク・ライフ・バランスの推進
　　クライアント情報の漏洩を防ぐためセキュアな業務環境の構築

・導入概要　カフェ等のモバイル勤務を禁止し、サテライトオフィスを活用することで
　　セキュアな業務環境を構築
　　事前申請、当日報告の徹底による労務管理を実施

・セキュリティ　ノートパソコン、モバイルルーターの貸与
　　クライアントからのプリントは禁止

・通信方式　本社のサーバーとはVPN経由のインターネット接続とログイン認証で接続

（出典）都内企業に学ぶテレワーク実践事例集　平成29年度テレワークの活用促進に向けたモデル実証事業　2018/5
https://www.hataraku.metro.tokyo.lg.jp/hatarakikata/telework/telework_jirei.pdf

都内企業に学ぶテレワーク実践事例集 Vol2から

自律的な時間管理による生産性向上と優秀な人材の確保を実現！

東洋製罐グループホールディングス株式会社

（発表資料）
https://www.hataraku.metro.tokyo.lg.jp/hatarakikata/telework/02_30jirei.pdf

（特徴）

・経営課題　自律的な時間管理による生産性向上
　　優秀な人材の確保

・導入概要　在宅勤務及びサテライトオフィス勤務
　　海外の出張先とサテライトオフィスをつないだWeb会議を実施

・セキュリティ　ノートパソコンの貸与（データを保管できないシンクライアント端末）
　　取り扱える情報を制限、紙資料の持ち出しは禁止
　　（4段階ある基準のうち最上位を除く情報に限定）

・通信方式　本社の仮想デスクトップサーバーとはVPN経由で接続

（出典）都内企業に学ぶテレワーク実践事例集 Vol2　2018年度テレワークの活用促進に向けたモデル実証事業　2019/6
https://www.hataraku.metro.tokyo.lg.jp/hatarakikata/telework/telework_30jirei.pdf

日本テレワーク協会　第22回テレワーク推進賞　&
経団連　ワーケーション実施事例から

小林勝哉
社会保険労務士事務所

「旅なかテレワーク」を推進し、ワーケーションを制度化！

横河電機株式会社

（発表資料）
https://japan-telework.or.jp/wordpress/wp-content/uploads/2022/03/2022_suishin06.pdf

（特徴）

・勤務場所　対象者：全社員、就業場所：制限なし、利用頻度：制限なし。
ただし事前（当日朝まで）に上司へ勤務場所の連絡が必要。
勤務時間の50%以上をテレワークとすることを希望する社員：83%

・費用　ワーケーション費用は自己負担。ただし自治体補助金活用サポートを行う。

・労働時間　フレックスタイム制（コアなし）、時間年休可。

・通信方式　環境整備　SSL-VPNサービス増強。
公衆Wi-Fi利用不可。ポケットWi-Fi等を活用し、VPNを利用する。

・その他　「旅なかテレワーク」は社員の判断で、どこで働いても良い制度。
新たな出会いを創出し、ストレスを解消し生き生き働いてほしい。

（出典）日本テレワーク協会　第22回 テレワーク推進賞表彰式＆事例発表会 2022/2/22
https://japan-telework.or.jp/associationactivities/suishin/

最後に

本日のまとめ

１）テレワークを通じた新しい働き方への期待

自律的な働き方への関心の高まり。

２）テレワークセキュリティの現状と課題

取引先からの義務・要請は「秘密保持」が９割。テレワークの定着により、組織外での秘密情報の取扱増加に伴うリスクが増大。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。

３）テレワークにおける就業規則のポイント

テレワーク勤務規程で、対象者/手続き等と服務規律を明確に。

４）テレワークにおける情報セキュリティ規程のポイント

組織的対策として、情報セキュリティ規程でテレワークセキュリティに対応。

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規程に関する支援情報
・個人としての情報セキュリティ対策、まずは何から？

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。
- DevSecOps
  開発(Development)、セキュリティ(Security)、運用(Operations)の手法を組み合わせた広範な技術的フレームワーク。
- 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。
- ICT（Information and Communication Technology）
  情報通信技術。
- SSL-VPN（Secure Sockets Layer – Virtual Private Network）
  VPN接続をする2点間をSSL暗号通信で接続する方式。
- 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。

参考　テレワークにおける就業規則に関する支援情報

➢ テレワーク相談センター

https://www.tw-sodan.jp/

電　話：0120-861009

（東京都の企業の方は、自動応答で「１」を選択）

➢ テレワーク総合ポータルサイト

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4年度東京都事業の例

➢ 令和4年度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/

社内セキュリティ規程整備

機器導入サポート（UTM）

➢ 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

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

サイバーセキュリティ人材育成・社内体制整備支援

➢ 令和4年度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

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4年度中小企業サイバーセキュリティ向上支援事業　参加企業の声から

学術研究、
専門・技術サービス業
従業員数1～5名程度

Q 本事業に参加する以前は、社内のサイバーセキュリティについてどのような課題がありましたか。

A テレワークを通じて新たな価値創造をしたいと考えていたため、テレワークに対応したセキュリティ対策の必要性を認識していました。サイバー保険には加入したものの、事業所としての基本方針を策定し体系的にセキュリティ対策に取り組むために、マネジメント系の運用ルールの検討稼働が十分とれずにいたことが課題でした。

Q UTMの設置など本支援事業をきっかけにセキュリティ意識に変化はありましたか。また、その他具体的な対策は講じましたか。

A 設置期間中にUTMが取得した広告で埋め込まれたURLへのアクセス等の検知状況のレポートを見て、テレワーク環境では多様なデバイスを通じて不正アクセスの可能性が存在することを認識することができました。また、メールセキュリティの高度な監視設定の提案なども届き、逐次必要な設定確認を行っています。

Q セキュリティマネジメント指導支援を通じて、情報管理に関する基本方針や関連規定等を策定いただきましたが、その効果（例：社員に周知できた、対外的にセキュリティに取り組んでいることを示せた等）はございましたか。

A 専門家の方に業態に合ったセキュリティマネジメントの考え方をご助言いただき、事業所としての基本方針を策定・公開し、SECURITY ACTION 二つ星宣言を実施しました。また、個人情報を取扱う事業所として必要なセキュリティ対策を策定できたことから、個人情報保護事務所の認証を申請できました。

（出典）東京都「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/#voice

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4年度東京都事業の例

➢ 中小企業サイバーセキュリティ対策強化緊急サポート事業

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

EDR（侵入を防げなかった脅威を検知・対処するセキュリティ対策）環境を導入し、サイバー攻撃の実態把握やインシデントへの対応を支援

➢ 令和4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

➢ IPA事業の例

講習能力養成セミナー

https://www.ipa.go.jp/security/keihatsu/sme/seminar.html

社内での情報セキュリティ研修会の基本を学ぶ

参考　個人としての情報セキュリティ対策、まずは何から？

１・個人として

　個人が留意することは、

「情報セキュリティ５か条」

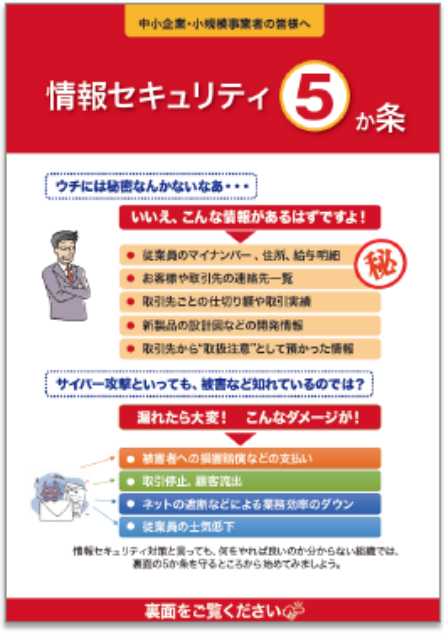
などに明確です。

● 情報セキュリティ対策と言っても、
何をやれば良いのか？

情報セキュリティ 5 か条

を守るところから始めてみましょう。

1. OSやソフトウェアは常に最新の状態にしよう！
2. ウイルス対策ソフトを導入しよう！
3. パスワードを強化しよう！
4. 共有設定を見直そう！
5. 脅威や攻撃の手口を知ろう！



２・組織として

　組織として留意することは、

情報セキュリティを守るための規程の整備と教育訓練です。

　そのために、まずはリスクアセスメントを実施、またはチェックリストで点検するなどしてみましょう。

（出典）IPA　中小企業の情報セキュリティ対策ガイドライン
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

参考　個人としての情報セキュリティ対策、まずは何から？

小林勝哉
社会保険労務士事務所

個人が留意することは、こちらの「情報セキュリティ５か条」のテレワーク環境におけるセキュリティ対策です。

１・ＯＳやソフトウェアは常に最新の状態に

テレワーク時のポイントは、自宅のルータは、メーカーのサイトを確認のうえ、最新のファームウェアを適用（ソフトウェア更新）することです。

２・ウイルス対策ソフトを導入

テレワーク時のポイントは、通信環境や端末の利用状況によっては、定義ファイルの更新が遅れる場合があるので、更新の確認を怠らないことです。

３・パスワードを強化

テレワーク時のポイントは、（１）クラウドサービス等を活用してテレワークを行う際は、強固なパスワードを設定すること。（２）可能な場合、多要素認証を利用すること。（３）自宅のルータの管理用パスワードが脆弱ではないか確認し、強固なパスワードを設定することです。

（出典）IPA　テレワークを行う際のセキュリティ上の注意事項
https://www.ipa.go.jp/security/announce/telework.html

参考　個人としての情報セキュリティ対策、まずは何から？

個人が留意することは、こちらの「情報セキュリティ５か条」のテレワーク環境におけるセキュリティ対策です。（続き）

４・共有設定を見直す

テレワーク時のポイントは、（１）テレワークで使用するパソコン等は、できる限り他人と共有して使わない。共有で使わざるを得ない場合は、業務用のユーザーアカウントを別途作成すること。（２）社外のネットワークではパソコンのファイル共有機能をオフにすることです。

５・脅威や攻撃の手口を知る

テレワーク時のポイントは、（１）自ら最新の脅威や攻撃の手口を知る。（２）システム管理者からの社内通達は必ず確認するとともに、テレワーク時に気付いたセキュリティに関する懸念点は報告することです。

（出典）IPA　テレワークを行う際のセキュリティ上の注意事項
https://www.ipa.go.jp/security/announce/telework.html

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。