2021年度
中小企業における情報セキュリティ対策の実態調査
報告書（概要説明資料）

2022年3月

独立行政法人情報処理推進機構

目次

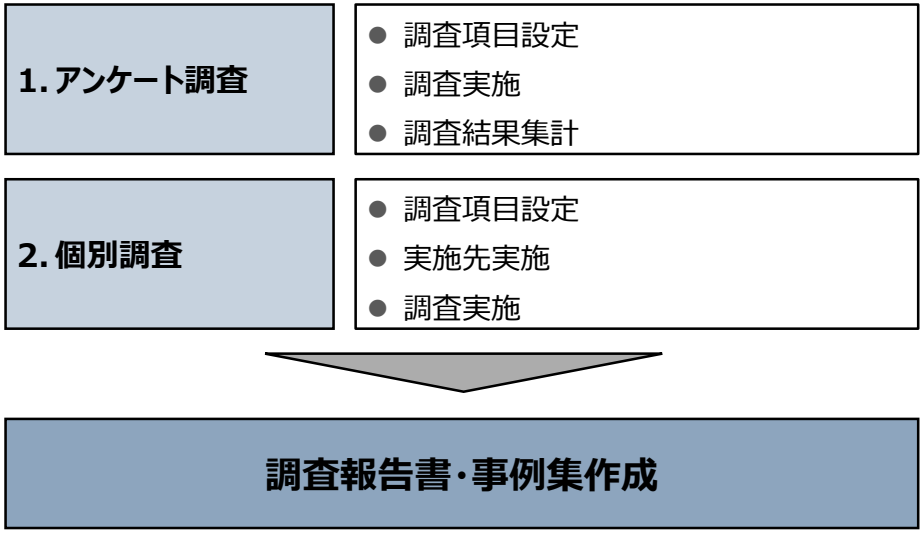
1. 調査目的

- 近年、中小企業においてもIT化が進み、業務の効率化、サービスレベルの向上等が図られている。その一方で、機密情報を狙ったサイバー攻撃は日々発生し、その被害も確認されている。中小企業を取り巻く環境においては、サプライチェーンの関係性を悪用し、セキュリティ対策の強固な大企業を直接攻撃するのではなく、その目的企業が構成するサプライチェーンにある、セキュリティが脆弱な中小企業等の取引先を経由し、最終目的である企業を攻撃するケースも発生している。
- 今般、IPAが事務局を務めるサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）において「発注元企業として取り組むべき課題」等についての議論も行われている。加えて、中小企業においても、2020年以降、急速に普及しつつあるテレワーク等によって、働き方も大きく変化しつつある。
- こうした状況に鑑み、前回調査から5年経過した2021年度に中小企業における情報セキュリティ対策の実情を把握するため、「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」を実施した。
- 本調査報告書は、調査結果をとりまとめたものである。加えて、個別のインタビュー調査に基づく61件の取組事例を事例集として取りまとめた。報告書と併せて、中小企業における情報セキュリティ対策の実態や取組事例等について参考としていただき、今後の中小企業向けセキュリティ対策の強化につなげる一助となれば幸いである。

2. 調査概要

- 中小企業における情報セキュリティ対策の実態や実施時の課題、経営層の認識、今後求められる対策等を把握ため、中小企業を対象としたアンケート調査、及びアンケート調査結果に基づくヒアリング等調査（以下「個別調査」）を実施した。
- アンケート調査及び個別調査を実施のうえ、調査結果を取りまとめた調査報告書と、個別調査実施により得られた中小企業の情報セキュリティ対策の取組例を取りまとめた事例集を作成した。

【調査実施フロー】



2. 調査概要（アンケート調査）

- 中小企業の情報セキュリティ対策への取り組みや被害の状況、対策実施における課題、経営層の関与や認識に関する実態を把握するため、アンケート調査を実施した。
- アンケート調査手法は、ウェブサイトによる回答システム（以下「ウェブ回答システム」）を構築して実施し、ウェブ回答システムを通じ回収することを前提とし、電子ファイルの添付によるメール回答と併用して実施した。
- 調査対象企業について、前回調査の送付数内訳を参考に、企業信用調査会社の企業データベースからランダムに抽出し、右図の内訳で送付し、4,074件の有効回答を得た。

【アンケート調査実施概要】

調査手法	ウェブによるアンケート調査
調査対象	全国の中小企業を対象とし、業種別、企業規模別、で中小企業法の定義に基づいて割付を行い、サンプルを回収。
調査項目	• 企業概要 • ITの導入状況 • 情報セキュリティに関する意識・状況 • 情報セキュリティ被害 • 取引先を含む情報セキュリティ対策
調査期間	2021年10月～2021年12月
有効回答数	4,074人 （内訳：経営層2,819人、ITや情報セキュリティの社内担当者561人、一般社員、役職無回答・不明：694人）

【アンケート送付数内訳】

業種名	中小企業数	小規模企業数	業種別合計数
農業・林業・漁業	746	1,049	1,795
建設業	1,353	3,160	4,513
製造業、鉱業・採石業・砂利採取業、電気・ガス・熱供給・水道業	1,337	3,123	4,460
情報通信業	529	1,229	1,758
運輸業・郵便業	529	1,229	1,758
卸売業・小売業	2,530	6,074	8,604
金融業・保険業	528	1,231	1,759
不動産業・物品賃貸業	1,115	2,599	3,714
サービス業・その他	3,495	8,144	11,639
合計	12,162	27,838	40,000

2. 調査概要（個別調査）

- アンケート調査の有効回答数 4,074件のうち、左図の観点を極力すべて満たすように対象企業をサンプリングし、64件の企業に対し実施した。調査にあたっては、オンライン会議ツールを使用したウェブ会議、もしくは電話での聞き取りにより実施した。
- 調査項目は、中小企業の取組の参考となる事例を収集する観点から、右図の項目を中心に実施した。

【対象企業選定の観点】

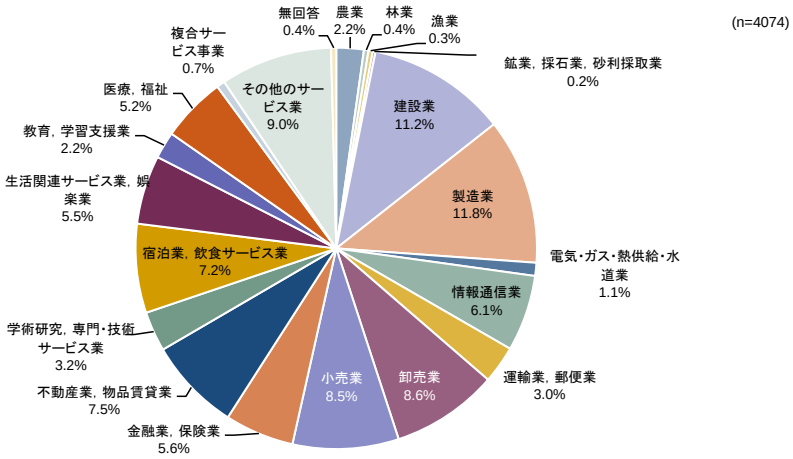
	選定視点の詳細
地域要件からの選定	経済産業省の各経済産業局が所管する地域ごとに一定数の事例が含まれること ※各経済産業局所管都道府県ごとに５件以上 ※内閣府沖縄総合事務局所管都道府県から２件以上
アンケート回答内容からの選定	• 情報セキュリティに関する実施対策が多い、もしくは情報セキュリティ対策投資が多い事例 • 情報セキュリティに関する被害実態等のある事例 • サプライチェーン上での情報セキュリティ対策の要請の多い事例
業種・従業員数要件からの選定	各業種分類において中小企業基本法で定義される「中小企業」と「小規模企業者」を従業員数の観点で極力それぞれ含むこと

【調査項目】

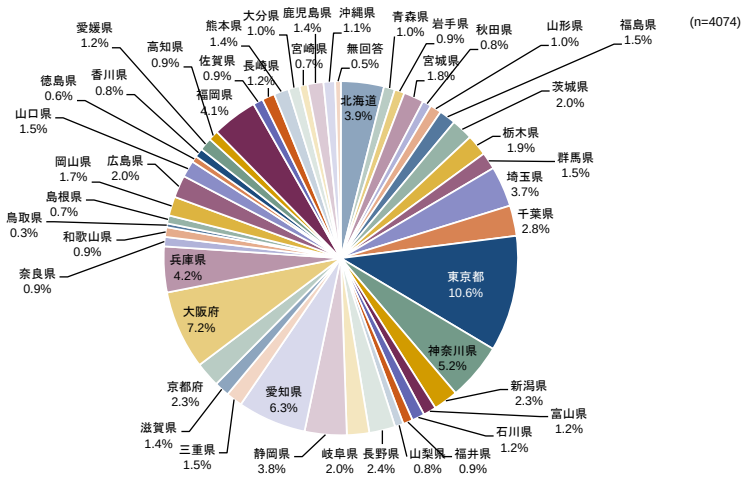
	項目の詳細
情報セキュリティ対策の取組	• 情報セキュリティ対策の必要性を感じたきっかけ • 情報セキュリティ対策として実施している具体的な内容 • 導入または推進する上で特に工夫した点や苦労した点
情報セキュリティ対策の効果	• 対策についての社内外からの声、評判 • 情報セキュリティ対策によって感じられたメリット
情報セキュリティ被害について	• 情報セキュリティの被害の有無 • 被害があった場合、実際に起きた被害によって生じた自社・取引先への影響 • 被害から復旧するまでの要した費用・期間
取引先との関連について	• 取引先との契約や調達仕様等における情報セキュリティに関するルール、取り決め。 • 取引先からの情報セキュリティ対策の要請有無 • 対策を実施する上での課題や費用負担の方法、貴社の方針や社内ルール等の有無等

3. 調査結果（アンケート調査）
回答企業の属性

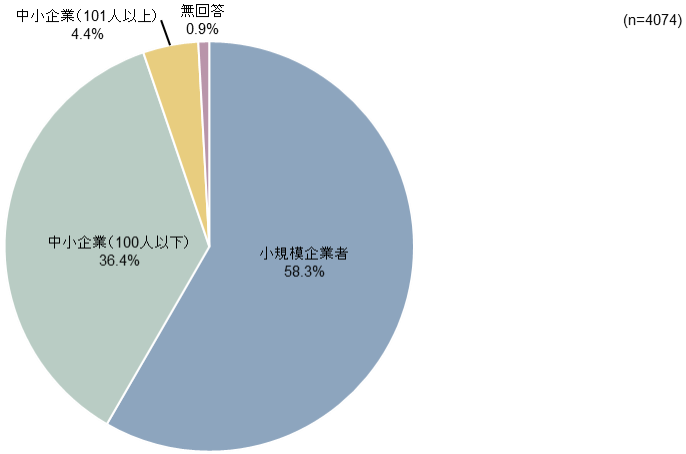
【業種】



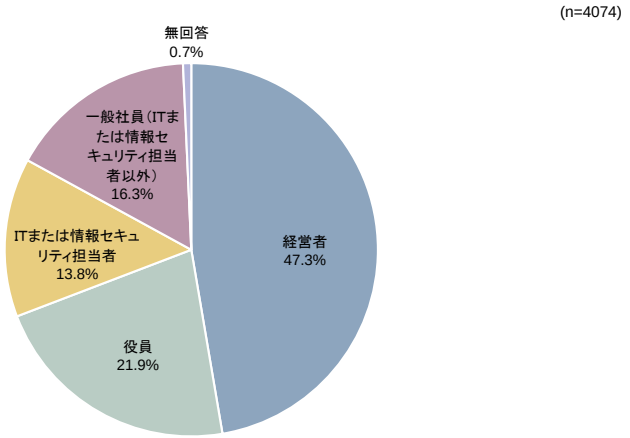
【所在地】



【企業規模】



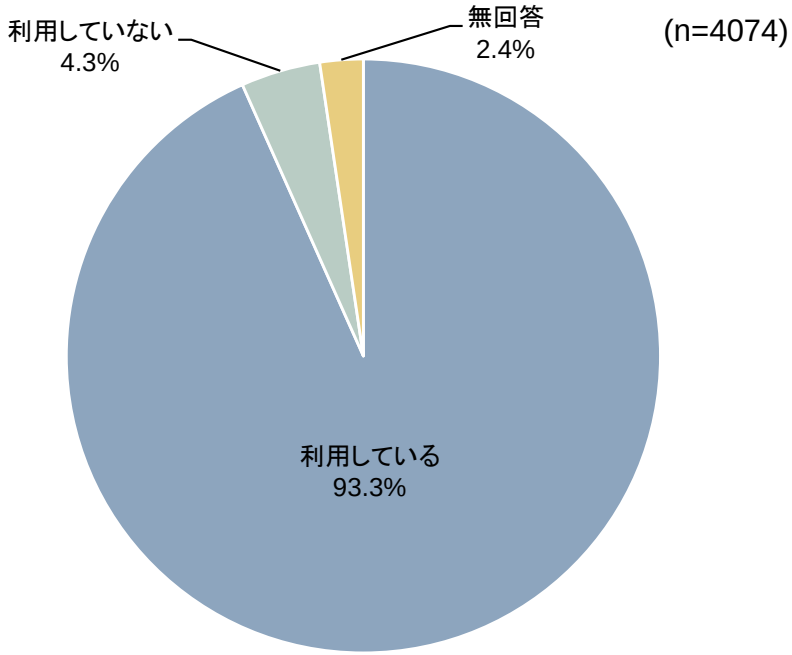
【回答者の役割・担当】



3. 調査結果（アンケート調査）
ITの導入状況

- 業務用パソコン・業務用タブレット端末・業務用スマートフォンを利用状況について、「利用している」の割合が93.3%となっている。

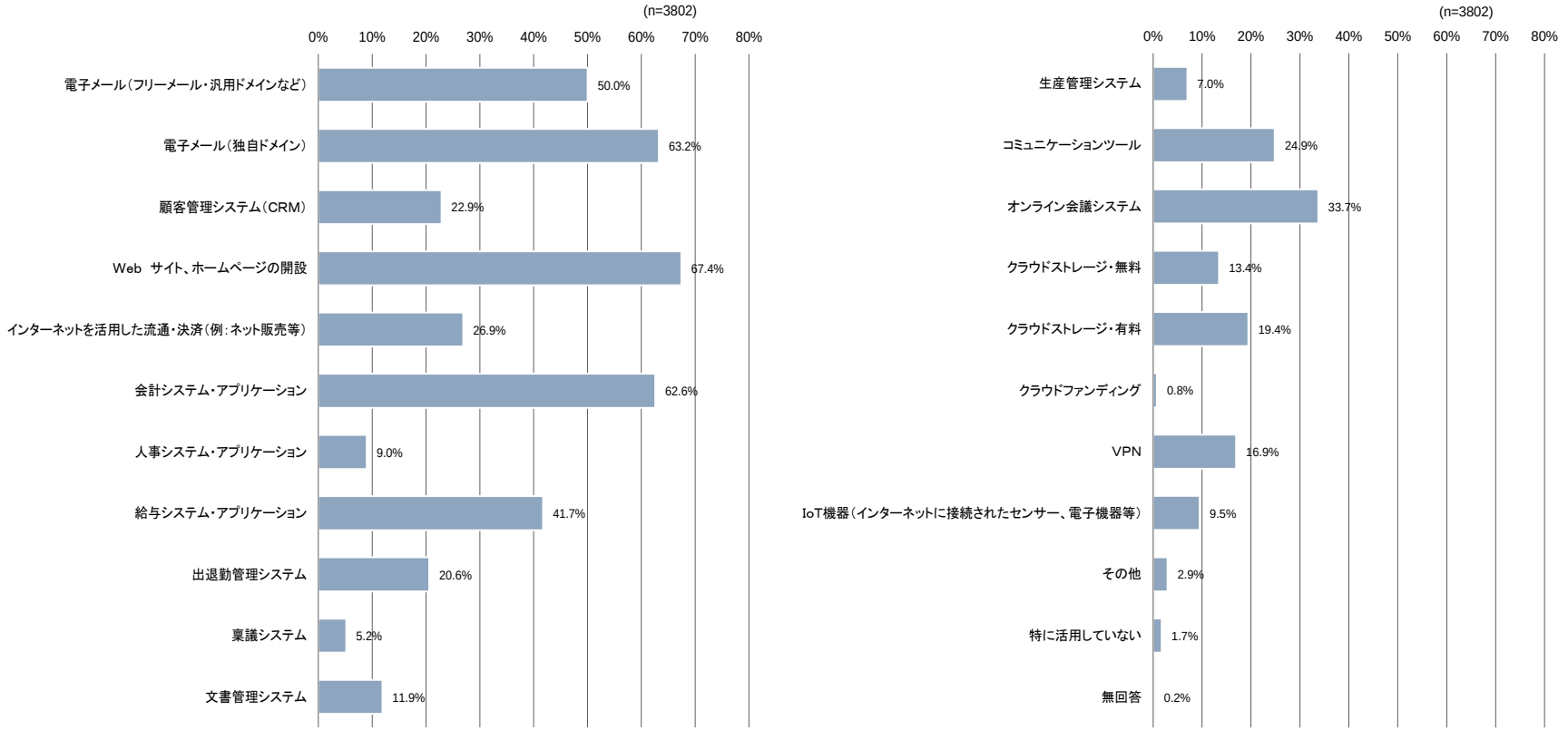
【業務用パソコン・業務用タブレット端末・業務用スマートフォンの利用状況】



3. 調査結果（アンケート調査）
ITの導入状況

- 利用・導入しているサービスやシステムについて、「Webサイト、ホームページの開設」の割合が最も高く67.4%となっている。次いで、「電子メール（独自ドメイン）（63.2%）」、「会計システム・アプリケーション（62.6%）」となっている。

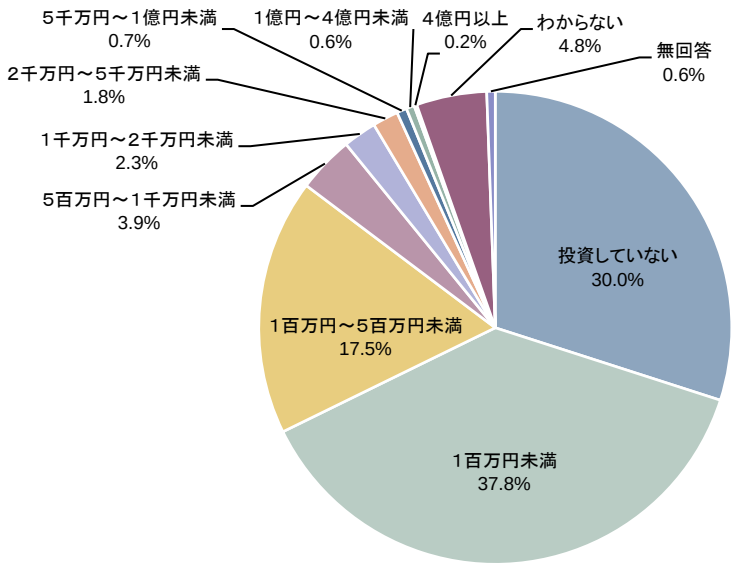
【利用・導入しているサービスやシステム】



3. 調査結果（アンケート調査）
ITの導入状況

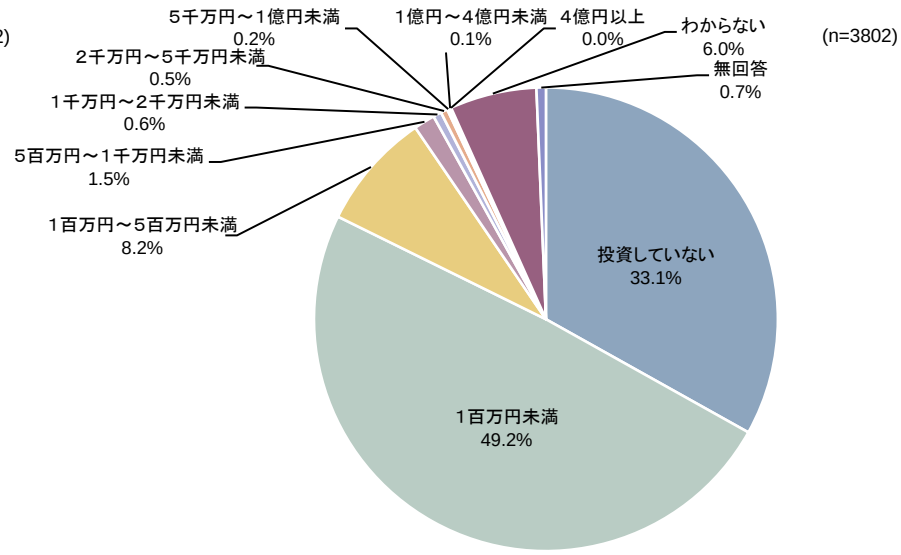
- 直近過去3期のIT投資額について、「1百万円未満」の割合が最も高く37.8%となっている。次いで、「投資していない（30.0%）」、「1百万円～5百万円未満（17.5%）」となっている。
- 直近過去3期の情報セキュリティ対策投資額について、「1百万円未満」の割合が最も高く49.2%となっている。次いで、「投資していない（33.1%）」、「1百万円～5百万円未満（8.2%）」となっている。

【直近過去３期のIT投資額】



【直近過去３期の情報セキュリティ対策投資額】

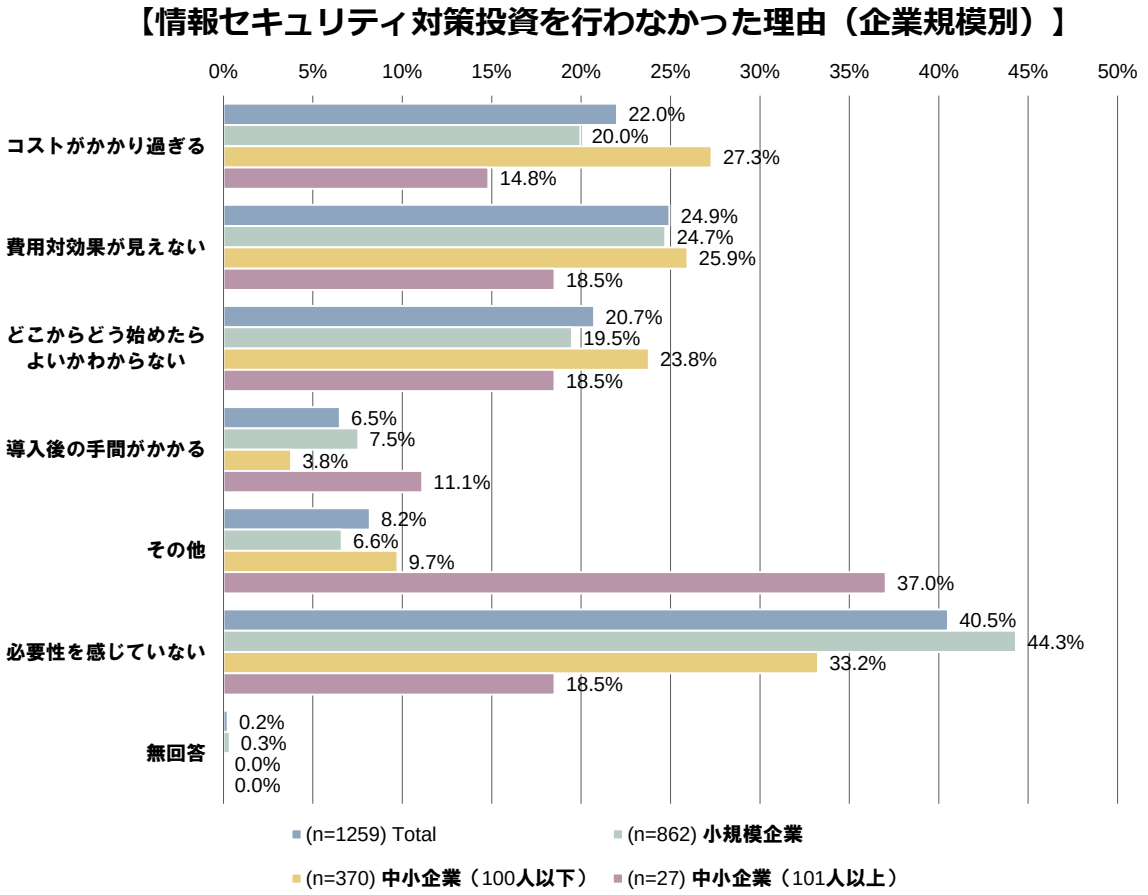
(n=3802)



(n=3802)

3. 調査結果（アンケート調査）
ITの導入状況

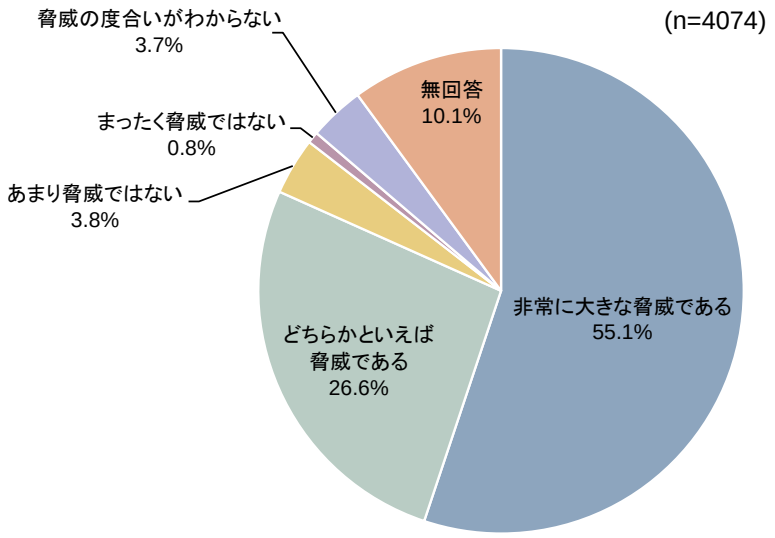
- 情報セキュリティ対策投資を行わなかった理由について、企業規模に関わらず「必要性を感じていない」という回答が最も多く、特に小規模企業や中小企業（100人以下）において回答の割合が多い。



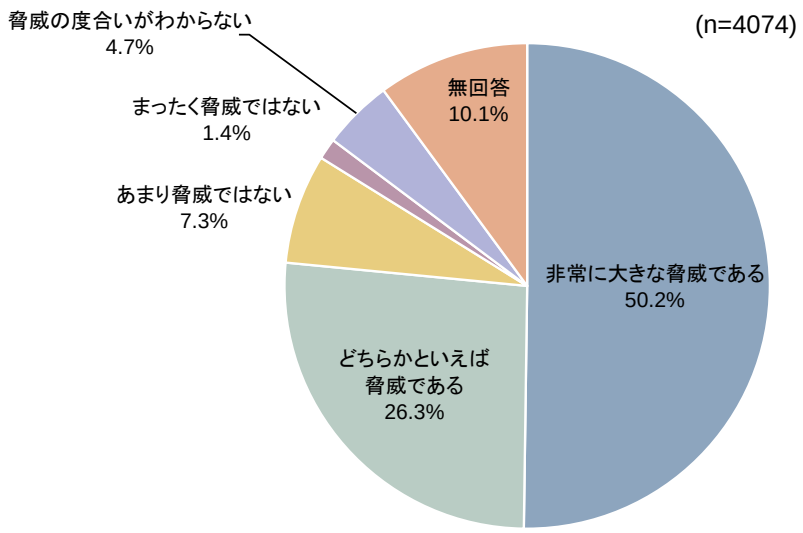
3. 調査結果（アンケート調査）
情報セキュリティに関する意識・状況

- コンピュータウイルスについて、「非常に大きな脅威である」の割合が最も高く55.1%となっている。次いで、「どちらかといえば脅威である（26.6%）」、「あまり脅威ではない（3.8%）」となっている。
- 不正アクセスについて、「非常に大きな脅威である」の割合が最も高く50.2%となっている。次いで、「どちらかといえば脅威である（26.3%）」、「あまり脅威ではない（7.3%）」となっている。

【情報セキュリティに関する脅威（コンピュータウイルス）】



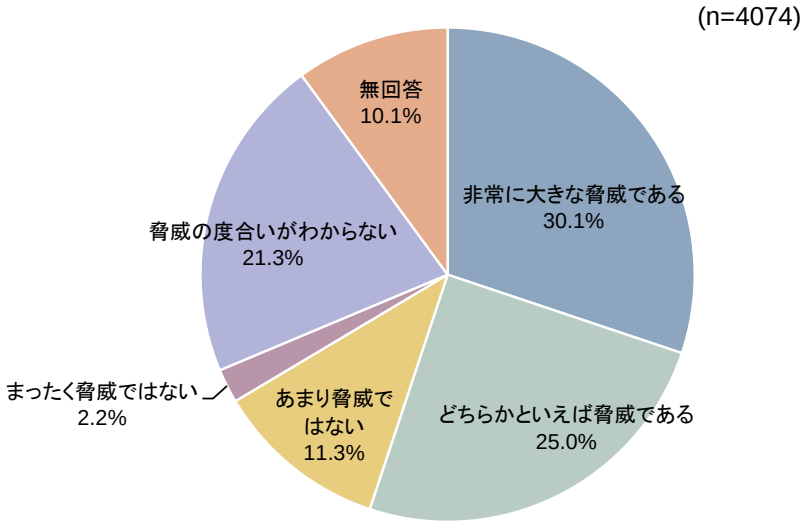
【情報セキュリティに関する脅威（不正アクセス）】



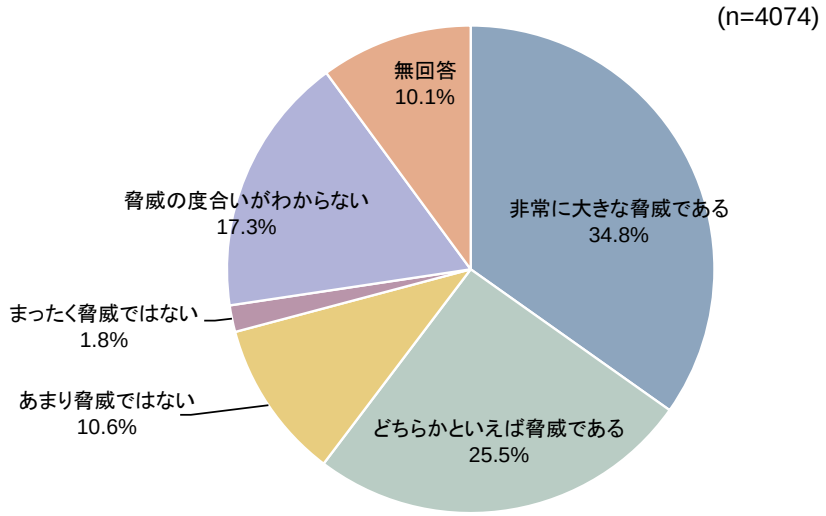
3. 調査結果（アンケート調査）
情報セキュリティに関する意識・状況

- DoS・DDoS攻撃について、「非常に大きな脅威である（30.1%）」「どちらかといえば脅威である（25.0%）」と、脅威と捉えている中小企業は5割を超えている。一方で、「脅威の度合いがわからない」が21.3%となっている。
- 標的型攻撃について、「非常に大きな脅威である（34.8%）」「どちらかといえば脅威である（25.5%）」と、脅威と捉えている中小企業は6割を超えている。一方で、「脅威の度合いがわからない」が17.3%となっている。

【情報セキュリティに関する脅威（DoS・DDoS攻撃）】



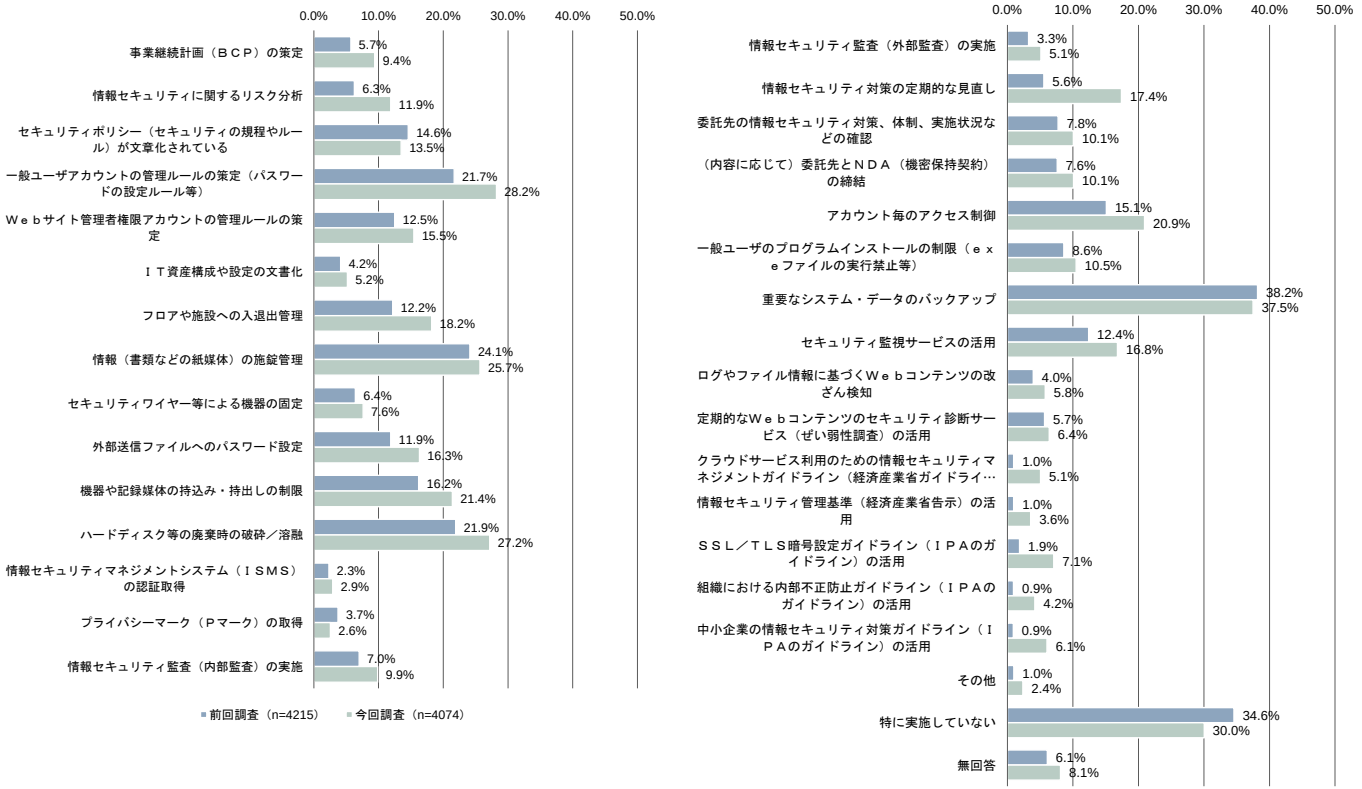
【情報セキュリティに関する脅威（標的型攻撃）】



3. 調査結果（アンケート調査）
情報セキュリティに関する意識・状況

- 被害防止のための組織面・運用面の対策の実施状況について、「重要なシステム・データのバックアップ」の割合が最も高く37.5%となっている。次いで、「特に実施していない（30.0%）」、「一般ユーザアカウントの管理ルールの策定（パスワードの設定ルール等）（28.2%）」となっている。

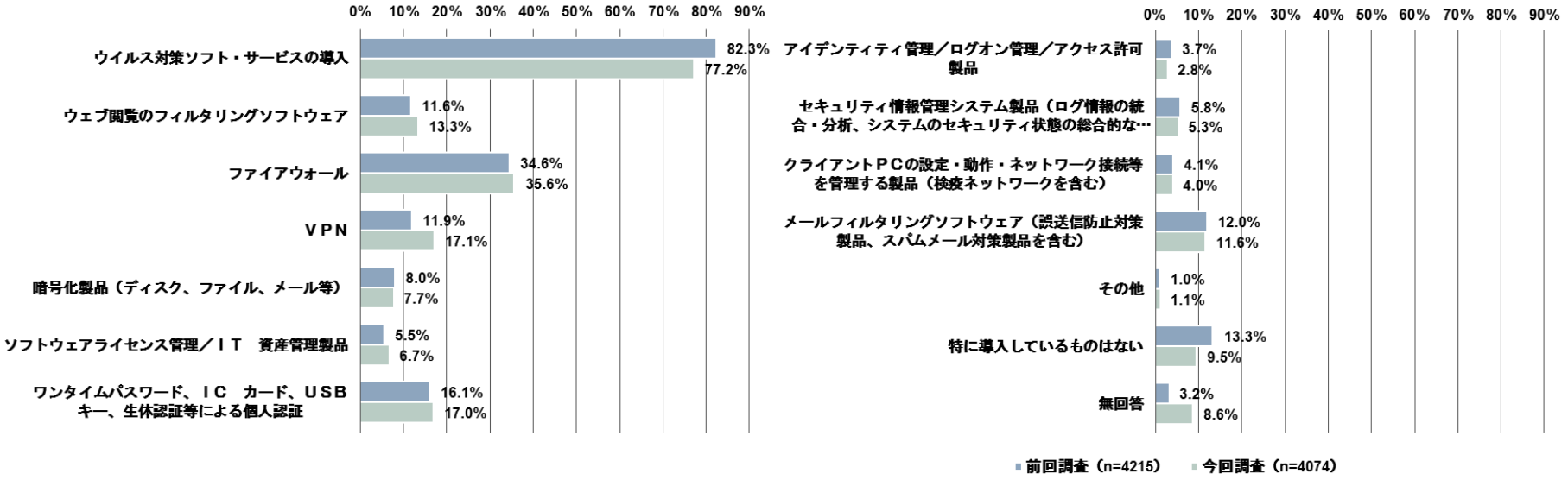
【被害防止のための組織面・運用面の対策（前回比較）】



3. 調査結果（アンケート調査）
情報セキュリティに関する意識・状況

- 情報セキュリティ関連製品やサービスの導入状況について、「ウイルス対策ソフト・サービスの導入」の割合が最も高く77.2%となっている。次いで、「ファイアウォール（35.6%）」、「VPN（17.1%）」となっている。

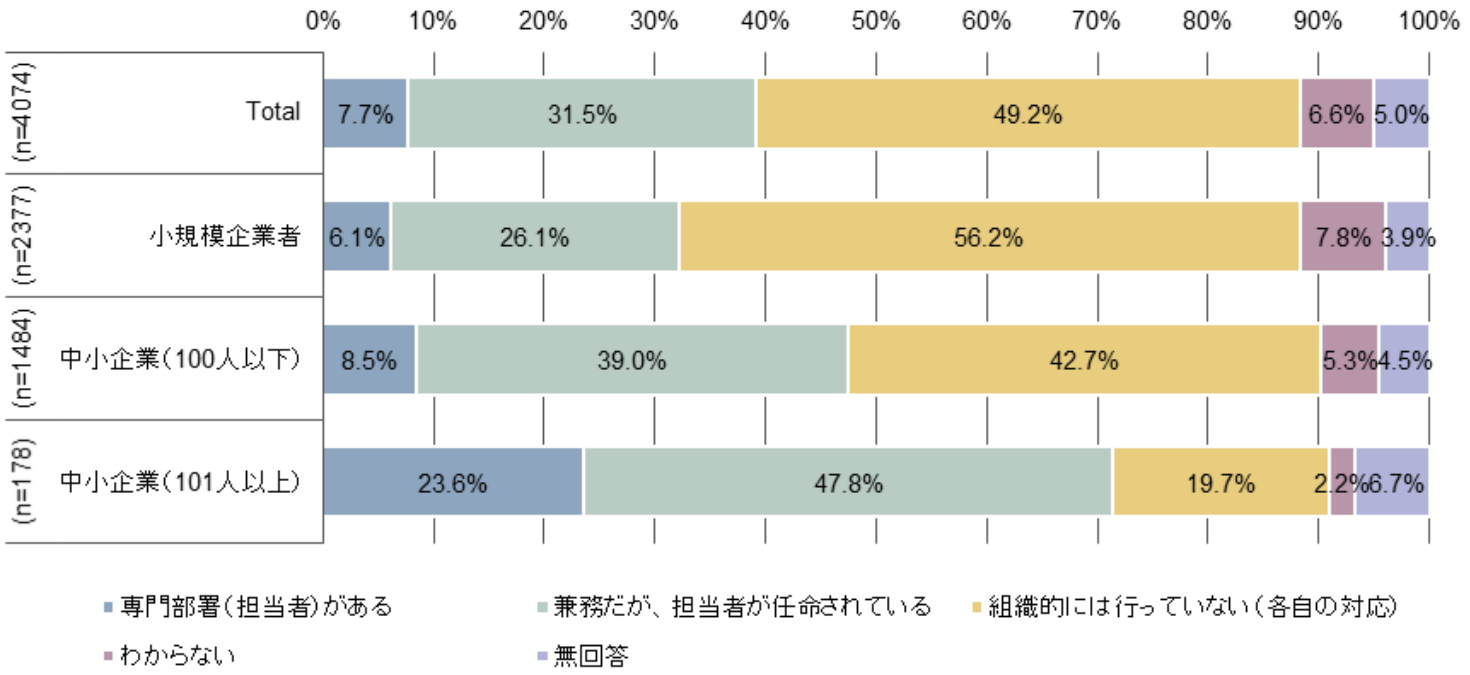
【情報セキュリティ関連製品やサービスの導入状況（前回比較）】



3. 調査結果（アンケート調査）
情報セキュリティに関する意識・状況

- 情報セキュリティに係る組織体制について、「専門部署（担当者が）ある」、「兼務だが、担当者が任命されている」の回答はいずれも企業規模が大きいほど割合が高く、回答の合計は小規模企業者では32.2%、中小企業（100人以下）では47.5%、中小企業（101人以上）では71.4%となっている。

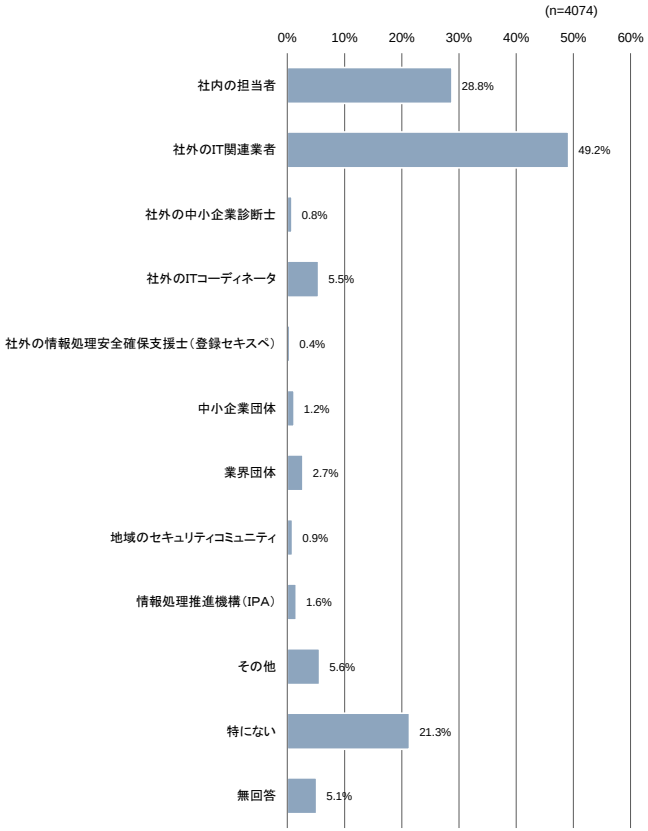
【組織体制（企業規模別）】



3. 調査結果（アンケート調査）
情報セキュリティに関する意識・状況

- 情報セキュリティに係る困ったことがあった際の相談先について、「社外のIT関連業者」の割合が最も高く49.2%となっている。次いで、「社内の担当者（28.8%）」、「特にない（21.3%）」となっている。

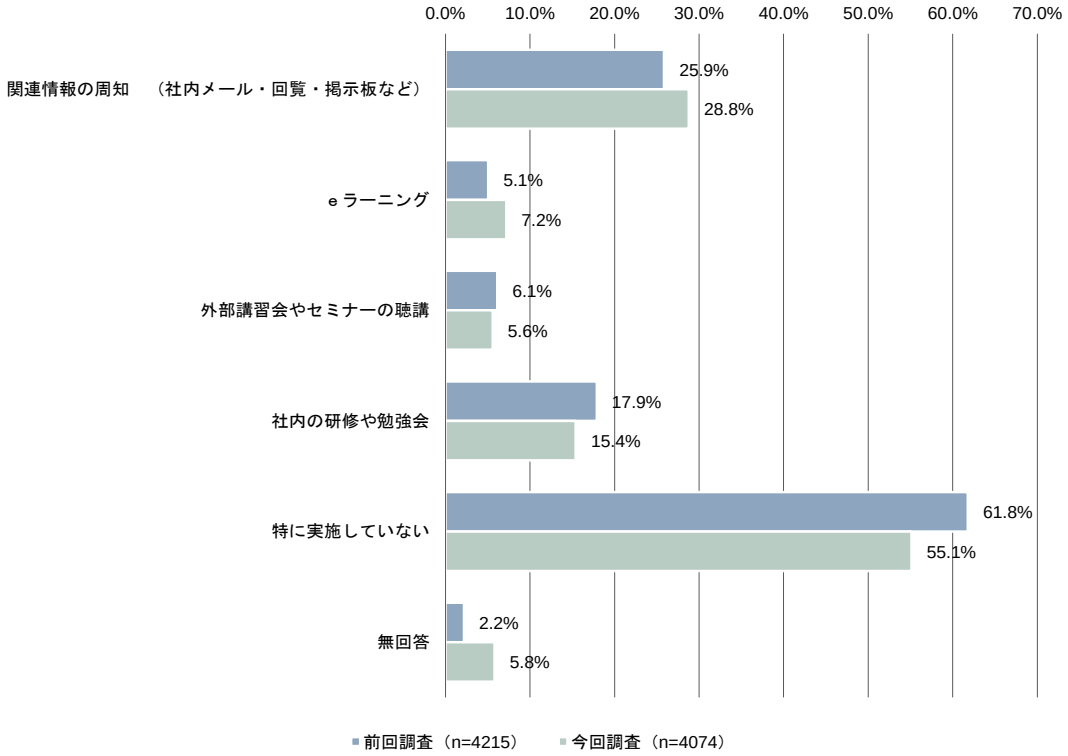
【困ったことがあった際の相談先】



3. 調査結果（アンケート調査）
情報セキュリティに関する意識・状況

- 従業員に対するセキュリティ教育の実施状況について、「特に実施していない」の割合が最も高く55.1%となっている。次いで、「関連情報の周知　（社内メール・回覧・掲示板など）（28.8%）」、「社内の研修や勉強会（15.4%）」となっている。
- 前回調査と比べ、「特に実施していない」の回答が61.8%から55.1%に減少した。

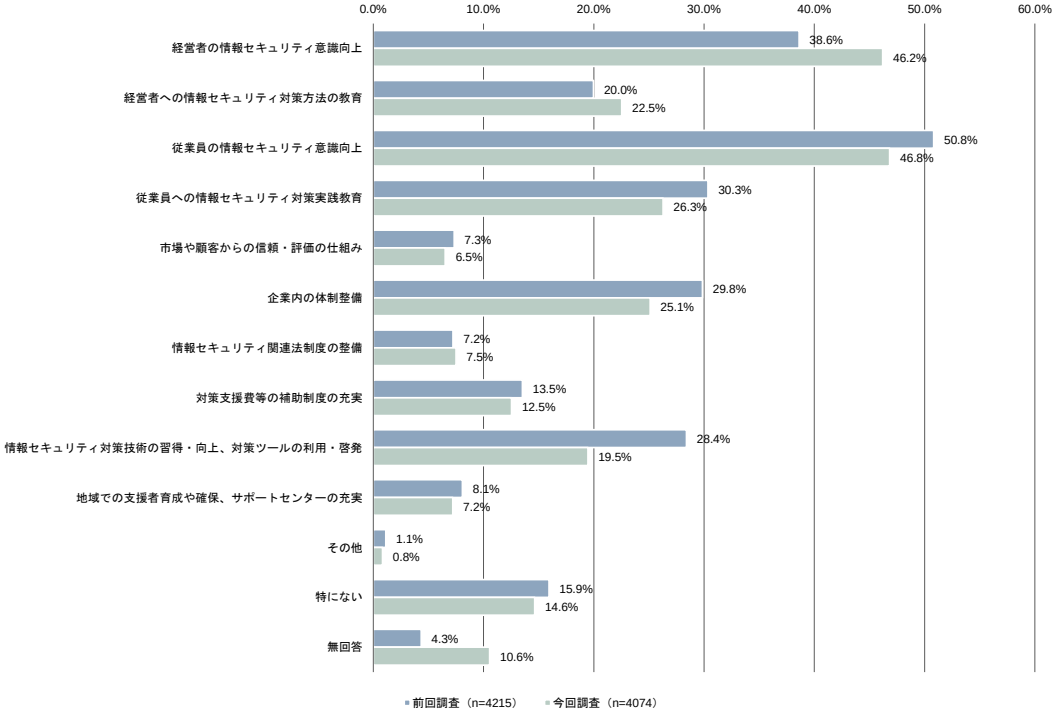
【従業員に対するセキュリティ教育の実施状況（前回比較）】



3. 調査結果（アンケート調査）
情報セキュリティに関する意識・状況

- 情報セキュリティ対策をさらに向上させるために必要と思われることについて、「従業員の情報セキュリティ意識向上」の割合が最も高く46.8%となっている。次いで、「経営者の情報セキュリティ意識向上（46.2%）」、「従業員への情報セキュリティ対策実践教育（26.3%）」となっている。前回調査と比べ、「経営者の情報セキュリティ意識向上」は38.6%から46.2%に増加している。

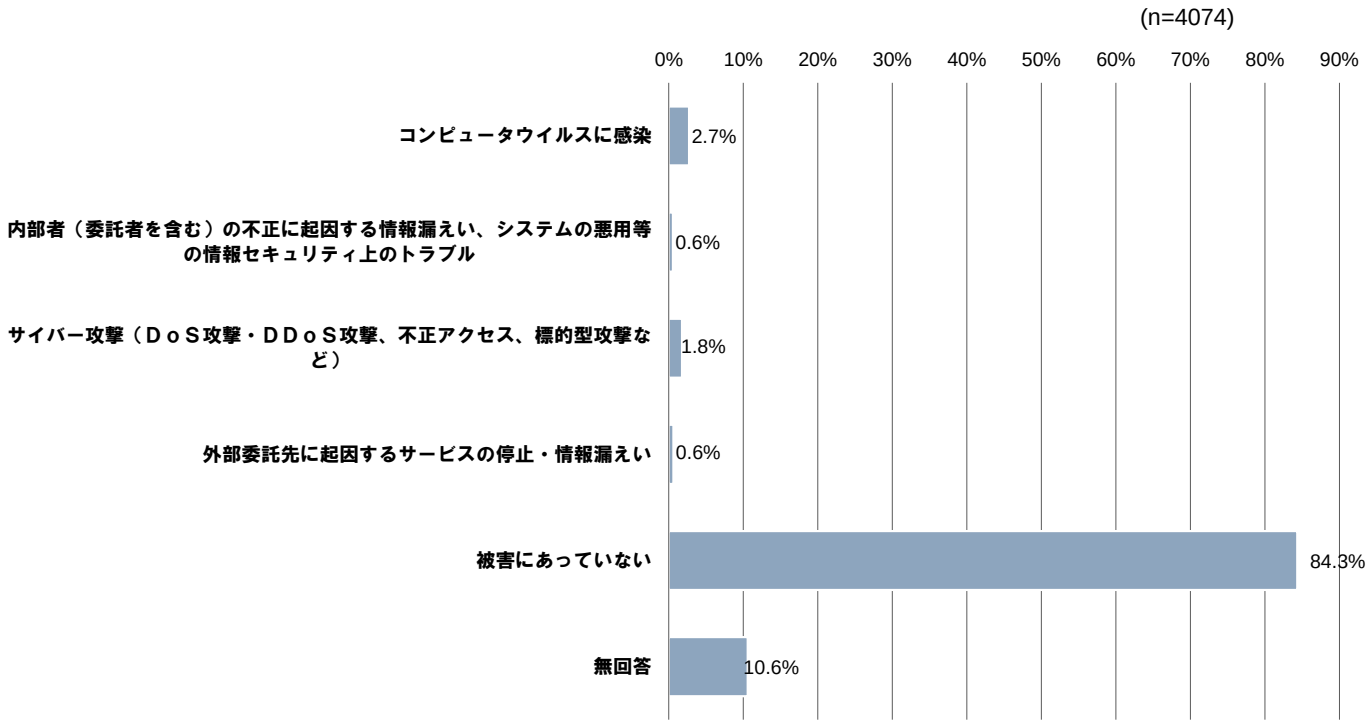
【情報セキュリティ対策をさらに向上させるために必要と思われること（前回比較）】



3. 調査結果（アンケート調査）
情報セキュリティ被害の状況

- 2020年度（2020年4月～2021年3月）における情報セキュリティ被害の有無について、「被害にあっていない」割合が最も高く84.3%となっている。次いで、「コンピュータウイルスに感染（2.7%）」、「サイバー攻撃（DoS攻撃・DDoS攻撃、不正アクセス、標的型攻撃など）（1.8%）」となっている。

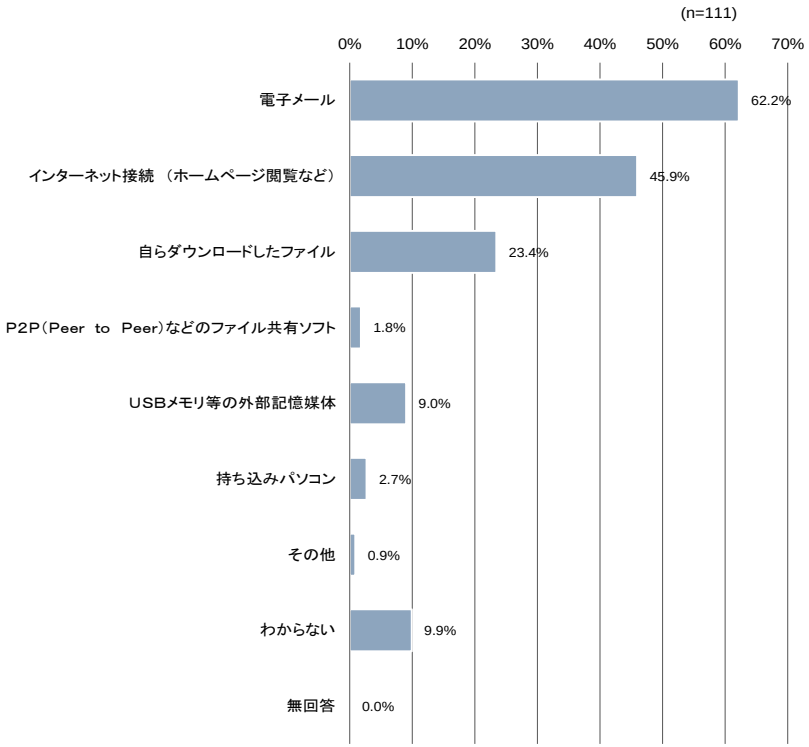
【2020年度における情報セキュリティ被害の有無】



3. 調査結果（アンケート調査）
情報セキュリティ被害の状況

- コンピュータウイルスの被害にあった企業において、感染あるいは発見されたコンピュータウイルスの想定される侵入経路は、「電子メール」の割合が最も高く62.2%となっている。次いで、「インターネット接続　（ホームページ閲覧など）（45.9%）」、「自らダウンロードしたファイル（23.4%）」となっている。

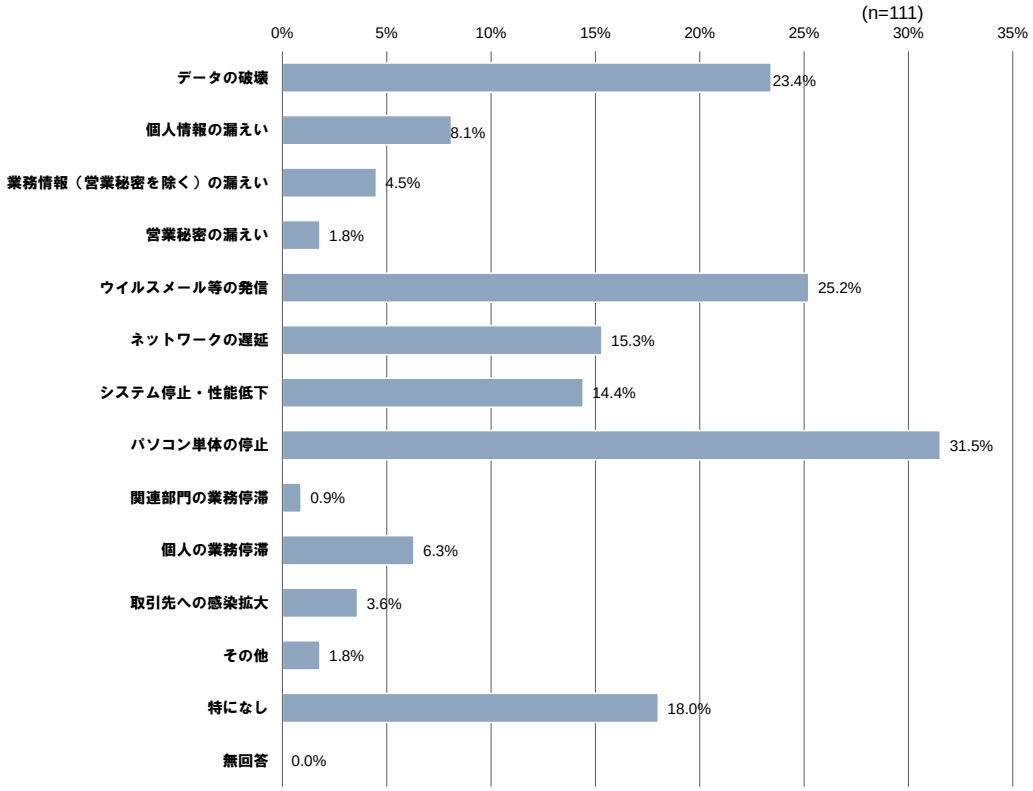
【感染あるいは発見したコンピュータウイルスの想定される侵入経路】



3. 調査結果（アンケート調査）
情報セキュリティ被害の状況

- コンピュータウイルスに感染した影響で生じた被害について、「パソコン単体の停止」という回答が最も高く31.5%となっている。次いで、「ウイルスメール等の発信（25.2%）」、「データの破壊（23.4%）」となっている。

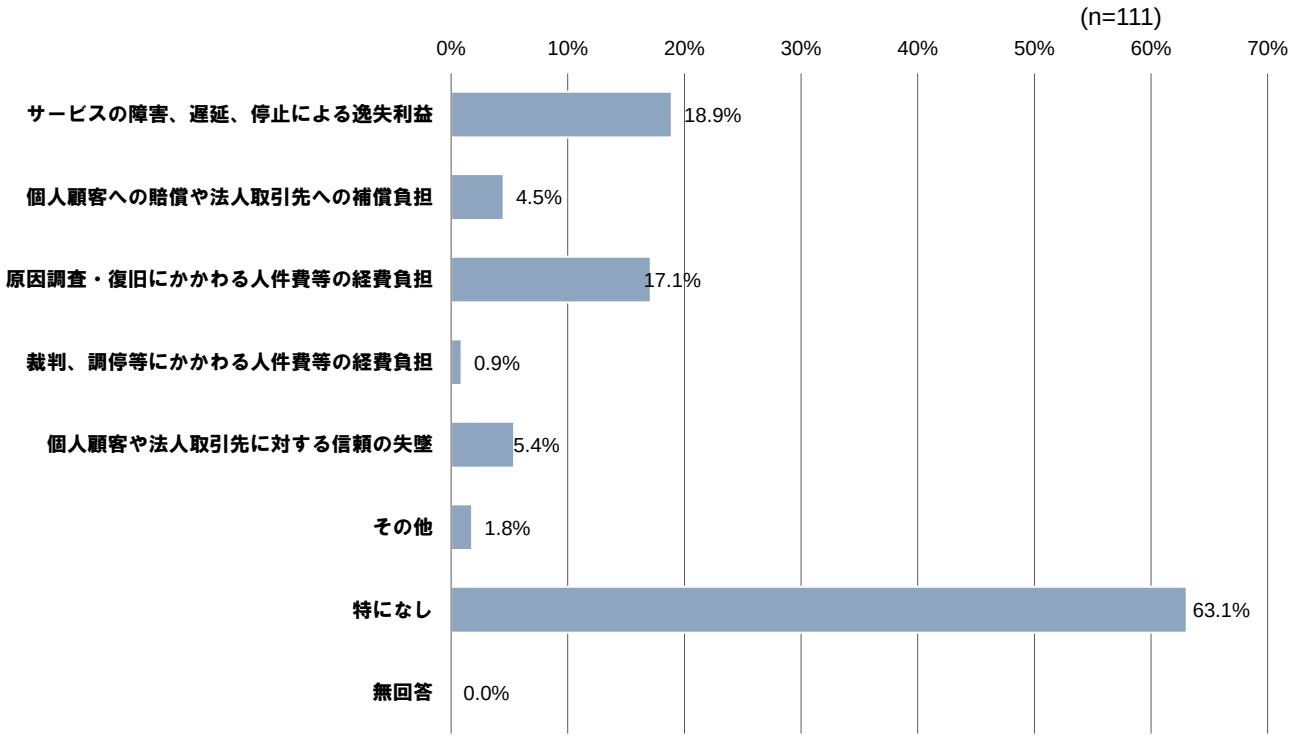
【コンピュータウイルスに感染した影響で生じた被害】



3. 調査結果（アンケート調査）
情報セキュリティ被害の状況

- コンピュータウイルスに感染した影響で、取引先に影響が及んだ内容について、「サービスの障害、遅延、停止による逸失利益（18.9%）」、「原因調査・復旧にかかわる人件費等の経費負担（17.1%）」等が挙げられている。

【コンピュータウイルスに感染した影響で、取引先に影響が及んだ内容】

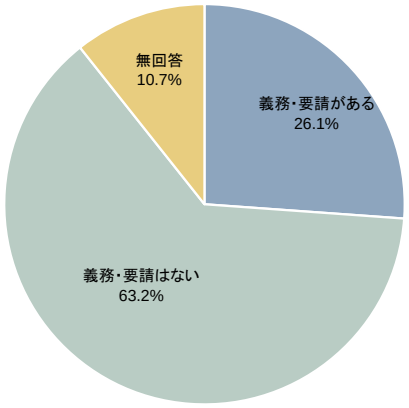


3. 調査結果（アンケート調査）
取引先を含む情報セキュリティ対策

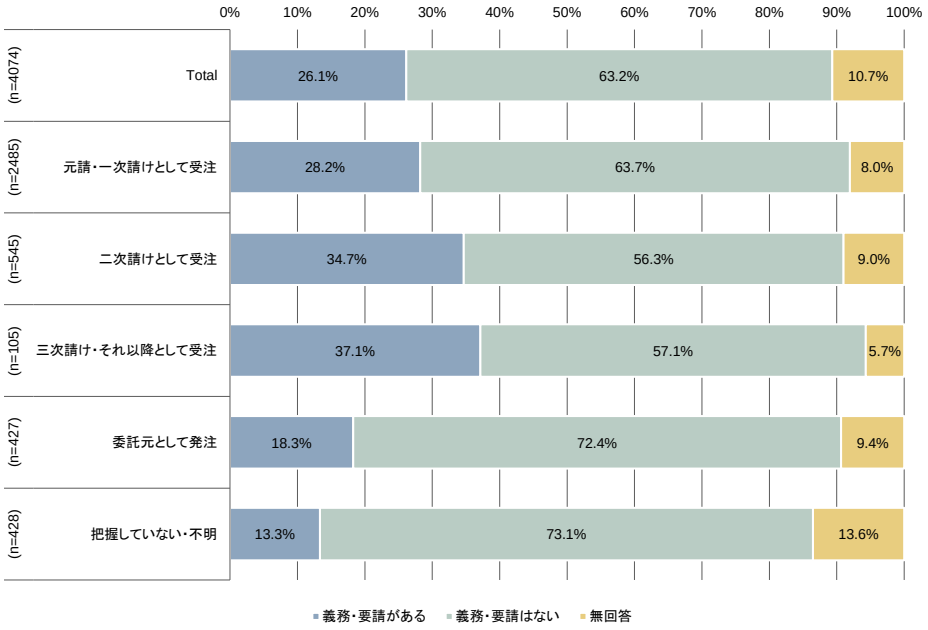
- 販売先・仕入先からの情報セキュリティに関する条項・取引上の義務・要請について、「義務・要請はない」の割合は63.2%、「義務・要請がある」の割合は26.1%である。
- 取引上の立場別にみると、サプライチェーンの上流（元請・一次請）から下流（三次請け・それ以降）にいくにつれ、「義務・要請がある」との回答の割合が増加している。

【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】

(n=4074)



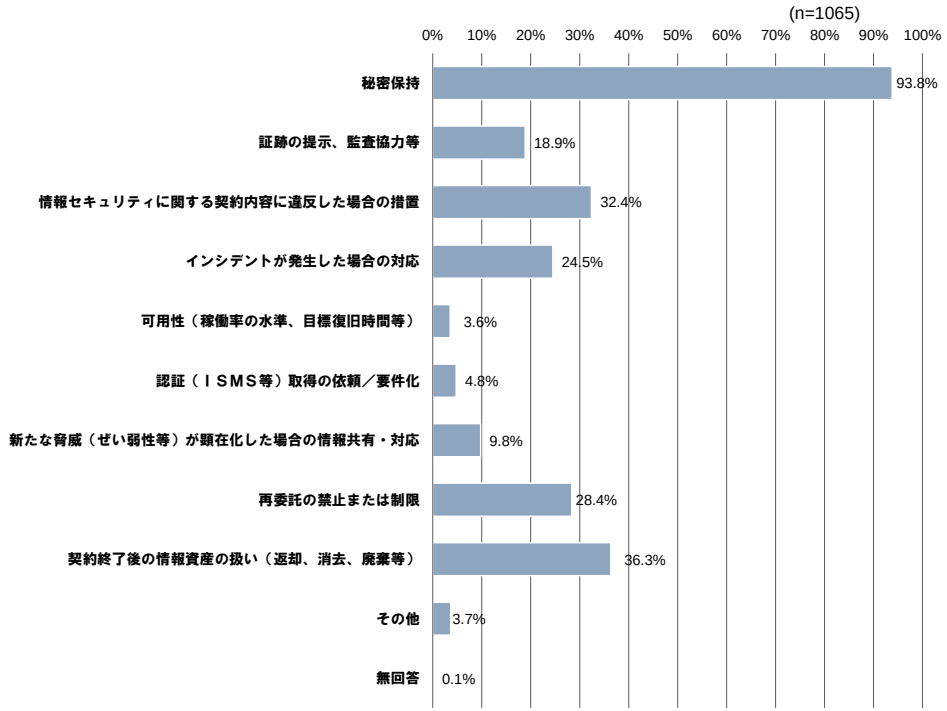
【取引上の立場別】



3. 調査結果（アンケート調査）
取引先を含む情報セキュリティ対策

- 販売先(発注元企業)との契約時における情報セキュリティに関する要請について、「秘密保持」の割合が最も高く93.8%となっている。次いで、「契約終了後の情報資産の扱い（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%）」となっている。

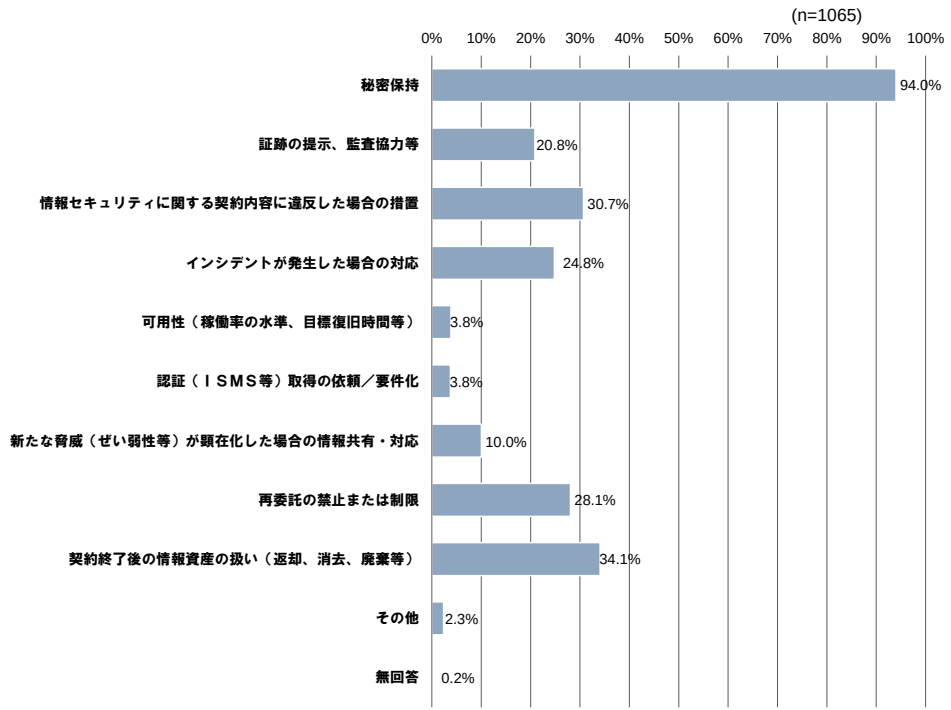
【契約時における情報セキュリティに関する要請（販売先（発注元企業）との契約時）】



3. 調査結果（アンケート調査）
取引先を含む情報セキュリティ対策

- 仕入先(委託・協力企業) との契約時における情報セキュリティの要請について、「秘密保持」の割合が最も高く94.0%となっている。次いで、「契約終了後の情報資産の扱い（返却、消去、廃棄等）（34.1%）」、「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（30.7%）」となっている。

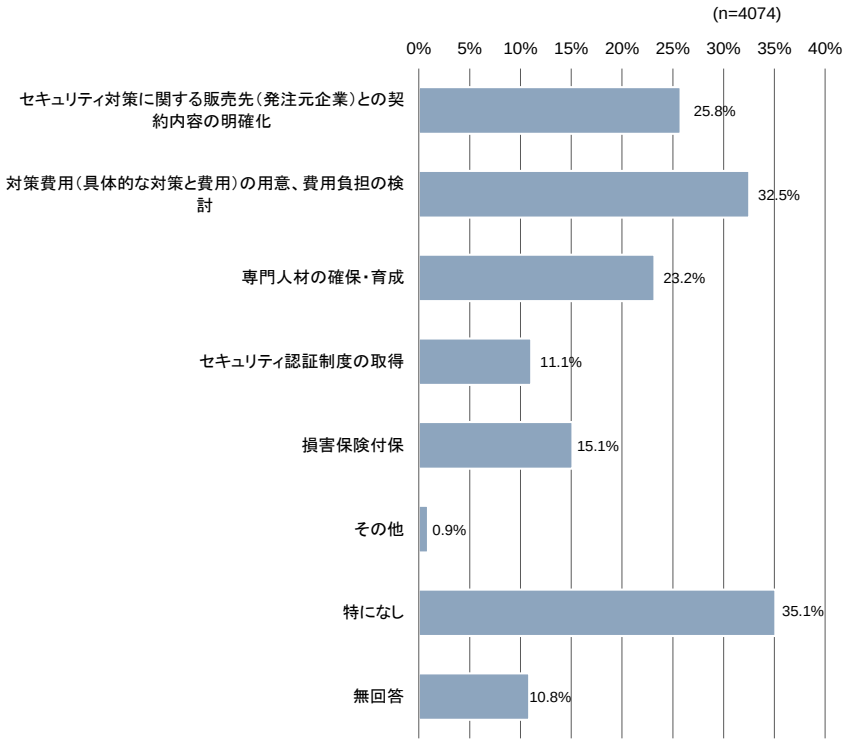
【契約時における情報セキュリティに関する要請（仕入先（委託・協力企業）との契約時）】



3. 調査結果（アンケート調査）
取引先を含む情報セキュリティ対策

- 販売先から情報セキュリティ対策の要請を受けた場合、対策実施に向けての課題について、「対策費用（具体的な対策と費用）の用意、費用負担の検討（32.5%）」、「セキュリティ対策に関する販売先（発注元企業）との契約内容の明確化（25.8%）」等が挙げられている。

【販売先から情報セキュリティ対策の要請を受けた場合、対策実施に向けての課題】

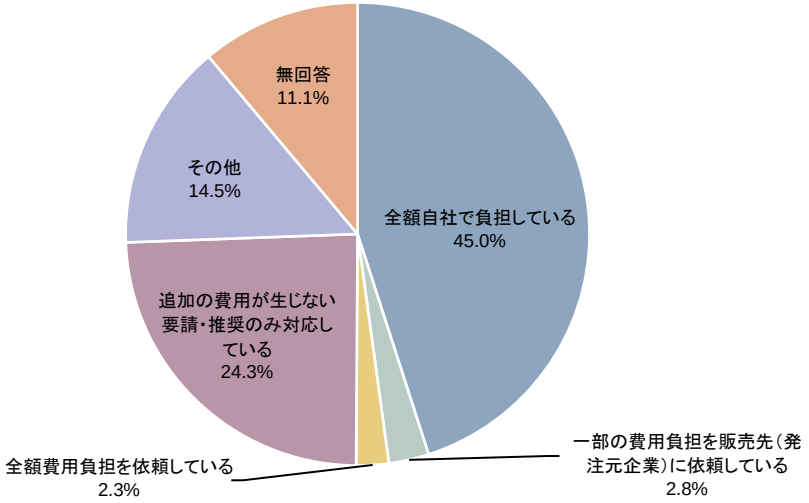


3. 調査結果（アンケート調査）
取引先を含む情報セキュリティ対策

- 販売先からの情報セキュリティに関する要請・推奨に対応するための費用負担について、「全額自社で負担している」の割合が最も高く45.0%となっている。次いで、「追加の費用が生じない要請・推奨のみ対応している（24.3%）」、「その他（14.5%）」となっている。

【販売先からの情報セキュリティに関する要請・推奨に対応するための費用負担】

(n=4074)



3. 調査結果（個別調査）

- アンケート調査の有効回答数 4,074件のうち、64件の企業に対して個別調査を実施し、事例集では61件の事例を取りまとめた。
- 地域ブロック別事例集掲載件数は左図の通りである。なお、事例集に掲載の各事例ごとに、選定時に重視した視点に当てはまる項目がわかるよう右図の通りマークを付している。

【地域ブロック別事例集掲載件数】

地域ブロック	事例件数
北海道ブロック	5件
東北ブロック	5件
関東ブロック	17件
中部ブロック	6件
近畿ブロック	10件
中国ブロック	5件
四国ブロック	5件
九州ブロック	6件
沖縄ブロック	2件
合計	61件

【選定視点※（視点の重複あり）】

	選定視点詳細	件数
対策･投資多	情報セキュリティに関する実施対策が多い、もしくは情報セキュリティ対策投資が多い事例	47件
被害有	情報セキュリティに関する被害実態等のある事例	15件
取引先要請多	サプライチェーン上での情報セキュリティ対策の要請の多い事例	18件

3. 調査結果（個別調査）
事例集

- 個別調査での聞き取りを踏まえ、実施している「情報セキュリティ対策の取組」について、その背景や具体的な内容、対策実施時のポイント、取引先からの対策実施の要請状況について、可能な限り盛り込む形でとりまとめを行った。

【実施している取組例】

（基礎的な対策の実施）
- 業務のIT化推進に伴う、基礎的なセキュリティ対策の実践。
- Windows Updateをすぐに実施。
- データの定期的なバックアップを実施。
- 業界として求められる水準に合わせた対策の実施。

（ルール、社内規定の整備）
- IPAの公開情報も参考とした社内情報の整備を実施。
- 管理者権限を有するアカウントに限定したソフトウェアのダウンロードの許可。
- 個人情報を取り扱う業務を行う施設を限定。

（認証取得・自己宣言）
- Pマーク取得に伴う、各種対策の実施。
- ISMS取得・維持のため、定期的な見直しを実施し、対策の形骸化を防ぐ。
- SECURITY ACTIONを宣言。それをきっかけとして、更に認証取得に向けた取組を開始。

（社内への周知・教育の実施）
- 取引先企業から情報セキュリティ対策に関する情報の提供をうけ、自社従業員への周知・徹底を実施。
- 従業員の意識向上に向けた研修の実施。

【取引先からの要請・取引先への要請例】

（取引先からの要請）
- 取引先企業から情報セキュリティ対策に関する情報の提供をうけ、自社従業員への周知・徹底するよう要請を受ける。
- 取引先企業から、情報セキュリティ対策に関するチェックシートを受領し、そのチェックシートを活用した自己点検の実施が求められる。
- 業界別のセキュリティガイドラインの内容に基づき、各種対策の実施が求められる。
- 取引にあたり、情報管理に関する認証取得の要請を受ける。
- 取引先企業による監査の実施の要請を受ける。
- 行政事業を受託する際に、情報セキュリティ上の要件に対応する必要がある。
- 再委託先に対しても、取引先から求められる水準と同様のセキュリティ対策が実施されていることが要請される。

（取引先への要請）
- 委託先への情報漏えい対策実施の誓約書の提出を依頼。
- 委託先企業に対し、現地確認を行い、情報管理体制等を確認。
- 廃棄PC等は、ハードディスクを物理的には破砕し、その様子を従業員が写真や目視で確認できるよう要請。
- 業務終了時の情報の破棄を依頼。
- 情報セキュリティ対策に関する研修を取引先従業員に行ってもらうよう要請を実施。
- 委託先企業に対して実施してほしいセキュリティ対策のマニュアルを作成し、順守を求める。

3. 調査結果（個別調査）
事例集

- また、「情報セキュリティ対策の効果」について、対策実施による具体的なメリットや今後実施していきたい取組を中心にとりまとめを行った。

【実施によるメリットの例】

（被害の未然防止）
- これまで被害にあっていない、と考えられることがメリットである。

（従業員の意識向上）
- 従業員向けの研修を実施したことで、従業員のセキュリティ意識が向上した。
- 継続して各種対策を続けたことで、IPAが提供する「5分でできる！情報セキュリティ自社診断」の点数も、上昇傾向にある。

（取引先からの信頼獲得・取引の継続）
- 対策実施や実施状況の丁寧な説明により、信頼関係の構築につながっている。
- ビジネスを行う上での要件として、情報セキュリティ対策を取引先に求める企業は増えつつあり、対策実施が必須となっている。
- 認証を取得していたことで、取引先に信頼感を与えることができ、取引が継続している。

（コロナ禍の業務継続に寄与）
- クラウド化を進めるにあたっての情報セキュリティ対策を強化しており、コロナ禍に対応して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た。

（デジタル化の推進に寄与）
- デジタル化を積極的に推進し、デジタル化によって享受できるメリットを情報セキュリティ対策により守る、という認識で取り組んでいる。

【今後実施していきたい取組の例】

（経営者の意識向上）
- 経営者自らがより情報セキュリティに係るリスクを深く理解していくべきであると考えている。

（従業員の意識向上）
- 従業員全体の情報リテラシー向上は今後の課題だと感じている。
- 従業員により情報セキュリティ対策に関する意識を高めてもらえるような社内教育を実施し、全社的なセキュリティレベルを向上させていきたい。
- IPAからの情報発信等も参考にしつつ、実際に起きた情報漏えい、サイバー攻撃の事例や、そうした事例が生じた際に、過去の事例では、どういった対処を行ってきたのか、というケーススタディを充実させたうえで、従業員に周知していきたい

（PC以外の端末への対策の実施）
- PCの対策に加えて、スマートフォンへの対策やGPSを用いた管理等も行うなどの取り組みを進めていきたい。

（社会動向を踏まえた対策の実施）
- 情報管理に対する目も厳しくなっているため、法令順守を超えた積極的な対策に取り組んでいくことが、今後必要になると考えている。
- デジタル化のメリットを守っていくための取組の一環としてセキュリティ対策を進めていきたい。

4. 考察
ITの導入状況

- ITの導入状況
  - 業務用パソコン・タブレット端末・スマートフォンの利用があると回答している企業は93.3%となっており、中小企業にとっても必須のツールとなっている。
  - 一方で、利用・導入しているサービスやシステムについて、利用率は相当にバラツキがあり、6割を超える利用率が確認されたのは「Webサイト、ホームページの開設（67.4%）」、「電子メール（独自ドメイン）（63.2%）」、「会計システム・アプリケーション（62.6%）」に限られる。テレワークやコロナ禍における非対面のコミュニケーションに有用な「オンライン会議システム（33.7%）」「コミュニケーションツール（24.9%）」は必ずしも中小企業全般に浸透しているとは言えない実態が改めて確認された。

- 直近過去3期におけるIT投資・セキュリティ対策投資の状況
  - 直近過去3期におけるIT投資の状況について投資を行っていないと回答している中小企業が30.0%、同じく直近過去3期の情報セキュリティ対策投資の状況について投資を行っていないと回答している中小企業が33.1%となっている。
  - 情報セキュリティ対策投資を行わなかった理由としては、「必要性を感じていない」の割合が最も高く40.5%となっている。次いで、「費用対効果が見えない（24.9%）」、「コストがかかり過ぎる（22.0%）」という結果となっている。
  - 後述の情報セキュリティに関する意識・状況の調査結果を踏まえると、コンピュータウイルスや不正アクセス等の情報セキュリティに関する脅威認識はあるものの、自社は情報セキュリティ被害にあわないと考えている中小企業や必要性を感じつつも金銭的リソース配分の優先順位を高めるまでに至っていない中小企業が多いと考察される。

4. 考察
情報セキュリティに関する意識・状況

- 情報セキュリティに関する脅威の認識
  - コンピュータウイルスについて、「非常に大きな脅威である（55.1%）」「どちらかといえば脅威である（26.6%）」と脅威と捉えている中小企業は8割を超えている。同様に、不正アクセスについて、「非常に大きな脅威である（50.2%）」「どちらかといえば脅威である（26.3%）」と脅威と捉えている中小企業は7割を超えており、情報セキュリティに関する脅威を認識している中小企業は多い。

- 情報セキュリティ対策の実施状況
  - 被害防止のための組織面・運用面の対策実施状況について、前回調査の結果と比較すると、大半の項目で対策実施の割合が増加している。特に、「情報セキュリティ体制の定期的な見直し」については前回調査と比較して10%以上増加している。
  - 一方で、情報セキュリティ関連製品やサービスの導入状況について、「VPN」の導入が11.9%から17.1%に増加しているものの、その他の選択肢については前回調査と大きな差はない。
  - 情報セキュリティ対策の実施状況は、5年前と比べて改善はわずかと考えられる。

4. 考察
情報セキュリティに関する意識・状況

- 情報セキュリティに係る組織体制・相談先
  - 情報セキュリティに係る組織体制は、「組織的には行っていない（各自の対応）」の割合が最も高く49.2%となっている。アンケート調査の回答者属性を見ると4割が5名以下の事業者であることを考えれば、妥当な結果であると考えられる。また、困ったことがあった際の相談先が「特にない」と回答している中小企業が21.3%となっている。
  - 社内に相談できる担当者を配置できていない場合でも、社外のIT関連事業者を含めて相談できる先を持つことは、情報セキュリティ対策を行う上で重要であり、組織的な対応が出来ていない中小企業であっても身近に相談できる相手を持つことが望まれる。

- 従業員に対する情報セキュリティ教育の実施状況
  - 従業員に対する情報セキュリティ教育の実施状況については、前回調査と比べ「特に実施していない」企業の割合が6.7%減少したものの、55.1%と依然高い状況にある。
  - しかし、情報セキュリティ対策をさらに向上させるために必要と思われることについて、前回調査と同様に、「従業員の情報セキュリティ意識向上」と「経営者の情報セキュリティ意識向上」を挙げた企業が多い。
  - この点、個別調査において、同様の問題意識をもつ企業がIPAの提供するコンテンツを活用した情報セキュリティ教育・意識啓発を実施している事例が複数確認されている。
  - 今後、事例集等の他社の取り組みも参考にして、情報セキュリティ教育・意識啓発のさらなる実施が望まれる。

4. 考察
情報セキュリティ被害の状況

- 2020年度（2020年4月～2021年3月）における情報セキュリティ被害の有無
  - 「被害にあっていない」という回答が84.3%となっている。被害の認識があったものとしては、「コンピュータウイルスに感染（2.7%）」、「サイバー攻撃（DoS攻撃・DDoS攻撃、不正アクセス、標的型攻撃など）（1.8%）」をあげる中小企業が相対的に多いことが明らかとなった。
  - しかし、令和2年度の「中小企業サイバーセキュリティ対策支援体制構築事業（サイバーセキュリティお助け隊事業）成果報告書（全体版）」では、中小企業1,117社に設置した機器が外部からの不審なアクセスを181,536件も検知したことが明らかになっている。
  - 先述の情報セキュリティ関連製品やサービスの導入状況を踏まえると、中小企業においてサイバー攻撃を認識できていない可能性も否定できない。

- コンピュータウイルスに感染した影響で生じた被害
  - 「パソコン単体の停止」という回答が31.5%と高い結果であったが、「ウイルスメール等の発信（25.2%）」、「データの破壊（23.4%）」等、組織全体や取引先への影響も懸念される項目についても高い比率の回答があった。
  - コンピュータウイルスに感染した影響で、取引先に影響が及んだ内容については、「サービスの障害、遅延、停止による逸失利益（18.9%）」、「原因調査・復旧にかかわる人件費等の経費負担（17.1%）」等を上げる中小企業が多い。
  - 中小企業に対する情報セキュリティの意識啓発に際しては、こうした被害事例が相当程度存在することも発信することも有用であると考えられる。

4. 考察
取引先を含む情報セキュリティ対策

- 販売先・仕入先との契約締結時における情報セキュリティに関する条項・取引上の義務・要請の有無
  - 「義務・要請がある」と回答したのは26.1%となっている。この点、サプライチェーンの川上に位置する企業よりも、川下に位置する企業の方が「義務・要請がある」と認識している比率が高いことも確認された。

- 「義務・要請がある」と回答した中小企業にその内容
  - 販売先(発注元企業)との契約時の要請としては、93.8%の中小企業が「秘密保持」が明確に義務付けられていると回答している。その他、「契約終了後の情報資産の扱い（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%）」等をあげる中小企業も多い結果となった。
  - 仕入先(委託・協力企業) との契約時の要請としても、94%の中小企業が「秘密保持」が明確に義務付けられていると回答している他、「契約終了後の情報資産の扱い（返却、消去、廃棄等）（34.1%）」、「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（30.7%）」をあげる中小企業が多いという結果であった。
  - 取引先に対して契約上の秘密保持義務を要請することが定着してきており、中小企業においても契約上の義務を履行するために情報セキュリティ対策を実施する必要性が高まっていると考えられる。

4. 考察
取引先を含む情報セキュリティ対策

- 販売先から情報セキュリティ対策の要請を受けた場合、対策実施に向けての課題
  - 情報セキュリティ対策の要請に対して、対策を実施する際の費用の負担や人材の確保等の面で課題があると認識している企業も少なくない。
  - また、要請に対応するために追加的な費用の負担が発生する場合であっても、「全額自社で負担している」と回答している企業が45.0%で最も高い比率となっている。
  - 基本的な情報セキュリティ対策は中小企業であっても必要であるが、先述の情報セキュリティ対策投資を行わなかった理由も念頭に置く必要がある。
  - 特定の業界や特殊な業務の発注にあたり、一般的な中小企業にとって高度な情報セキュリティを求める場面やサプライチェーン全体としての情報セキュリティを高めなければならない場面において、情報セキュリティの必要性を訴えたり、取引上の立場を利用して要請をしたりするだけでは、十分な対策とはならない可能性がある。