2. セキュリティーへの取り組み状況

2. セキュリティーへの取り組み状況

近年、各企業での IT 化が進み、業務の効率化やサービスレベルの向上が図られている。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ており、各企業においても被害が確認されるようになった。

企業に対するセキュリティー攻撃は、該当する企業のみにとどまらず、その企業を取り巻く環境やサプライチェーンの関係性を悪用して 、セキュリティー対策の強固な企業を直接攻撃するのではなく、サプライチェーンに存在するセキュリティー対策が脆弱な企業等の取引先を経由して、最終目的である企業を攻撃するケースも発生している。

こうした状況を踏まえ、会員顧客企業ならびに中小一般企業のセキュリティーへの取り組み状況を調査した。

2.1 セキュリティー対策の実施状況と要請

各企業のセキュリティー対策に実施状況と、官公庁や関連団体・企業からのセキュリティー対策の要請状況、そしてそれらの関連について調査した結果を示す。

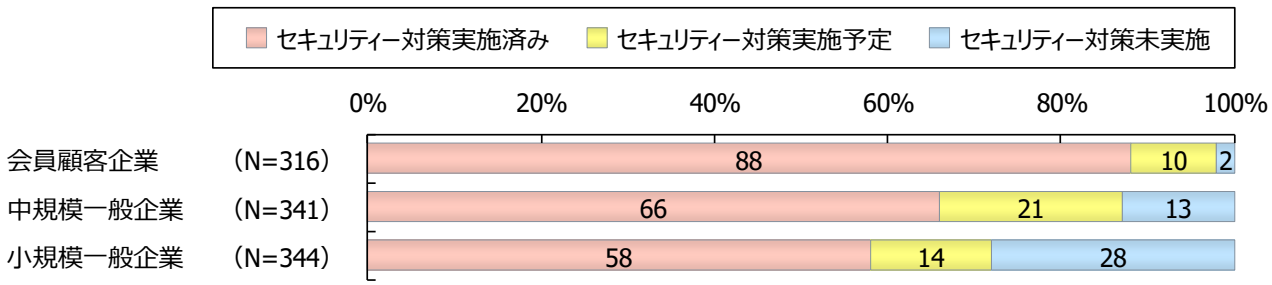
2.1.1 セキュリティー対策の実施状況

今回調査対象とした会員顧客企業 316 社、中規模一般企業 341 社、小規模一般企業 344 社の対策状況を見たのが、図表 2.1.1 である。

会員顧客企業は、会員企業からのセキュリティーに関する働きかけが功を奏して、「セキュリティー対策実施済み」企業が 88%と非常に高い状況であることが分かった。

一方で、一般企業は残念ながら十分な対策が取られているとは言い難い状況である。特に小規模一般企業では「セキュリティー対策未実施」の企業が、全体の 4 分の 1 以上の 28%あり、該当企業のみではなく、サプライチェーン間での連携を含めると、関連する企業に対しても大きな脅威であると言わざるを得ない。

図表 2.1.1　　セキュリティー対策の実施状況



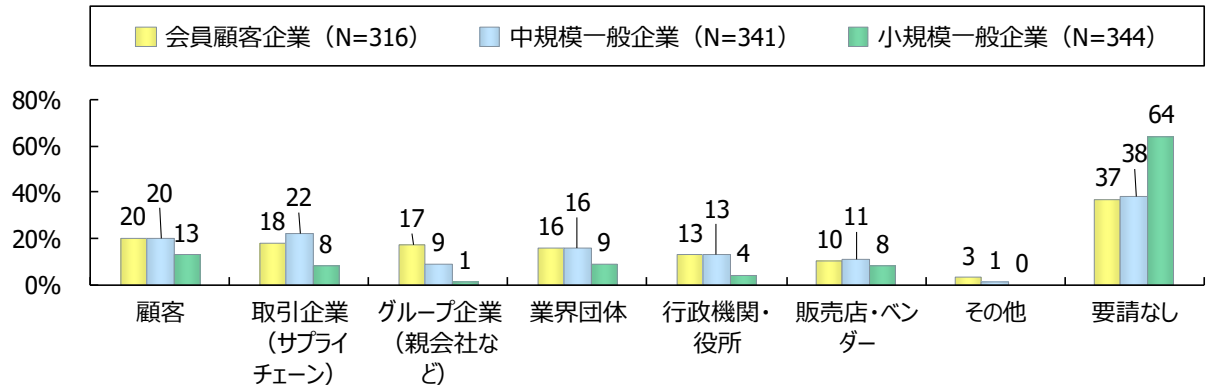
2.1.2 セキュリティー対応の要請状況

セキュリティー対策を進めるにあたって、セキュリティーへの対応の要請元を聞いた結果が、会員顧客企業と中規模一般企業は、各々同様の要請元から 9～22%の比率で要請を受けて、セキュリティー対策を進めてきたことが分かる結果であった。

図表 2.1.2 である。

会員顧客企業と中規模一般企業は、各々同様の要請元から 9～22%の比率で要請を受けて、セキュリティー対策を進めてきたことが分かる結果であった。

図表 2.1.2　　セキュリティーへの対応の要請元

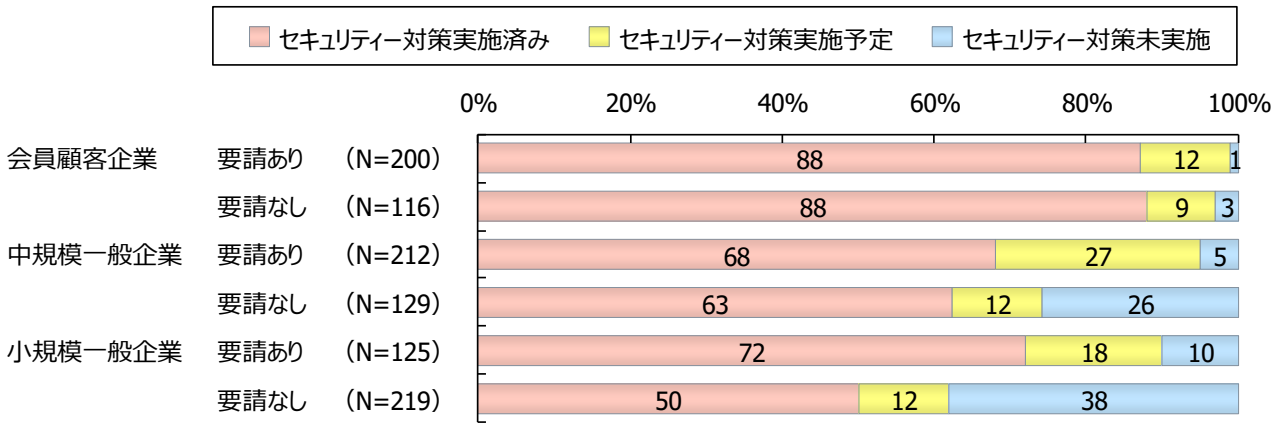


2.1.3 セキュリティー対応要請の効果

セキュリティー対応に対する「要請なし」の比率が、会員顧客企業で 37%、中規模一般企業で 38%、小規模一般企業では 64%あるが、要請がなかった場合のセキュリティー対策の推進に影響があったかを確認するため、「要請を受けた」企業と「要請がなかった」企業のセキュリティー対策の実施状況を比較したのが、図表 2.1.3 である。

「要請がなかった」企業の「セキュリティー対策未実施」の比率は、「要請を受けた」企業に対して中規模一般企業で 21 ポイント、小規模一般企業で 28 ポイント多く、やはり「要請なし」企業では対策が取られていないケースが多いことが分かった。

図表 2.1.3　　セキュリティー対策の実施状況の比較



2.2　セキュリティー対策実施のきっかけ、実施内容と運用状況

各企業のセキュリティー対策に実施状況と、官公庁や関連団体・企業からのセキュリティー対策の要請状況、そしてそれらの関連について調査した結果を示す。

2.2.1 セキュリティー対策実施のきっかけ

「2.1.1 セキュリティー対策の実施状況」で述べたように、「セキュリティー対策実施済み」ならびに「実施予定」の企業は、会員顧客企業で 98%、中規模一般企業で 83%、小規模一般企業でも 72%と高い比率となっているが、対策実施に向けたきっかけは何であったのであろうか。

以下、セキュリティーを考える上で必要なきっかけについて調査した結果が、図表 2.2.1 である。

なお、きっかけとして挙げたのは次の 5 項目である。

① ガイドライン*4 に準拠するため
② 自社で必要性を感じたから
③ 販売店・ベンダーから要請されたから
④ 他団体や取引先が実施しているから
⑤ 未対応で対策の予定はない

ここでは、「バックアップと復旧」、「ユーザー認証・アクセス管理」、「脆弱性管理」、「データ保護」、「ネットワークセキュリティー」、「ログ管理・保存」、「物理的セキュリティー」の 7 項目について、各々「対策のきっかけ」となったのは何であったかを聞いた。

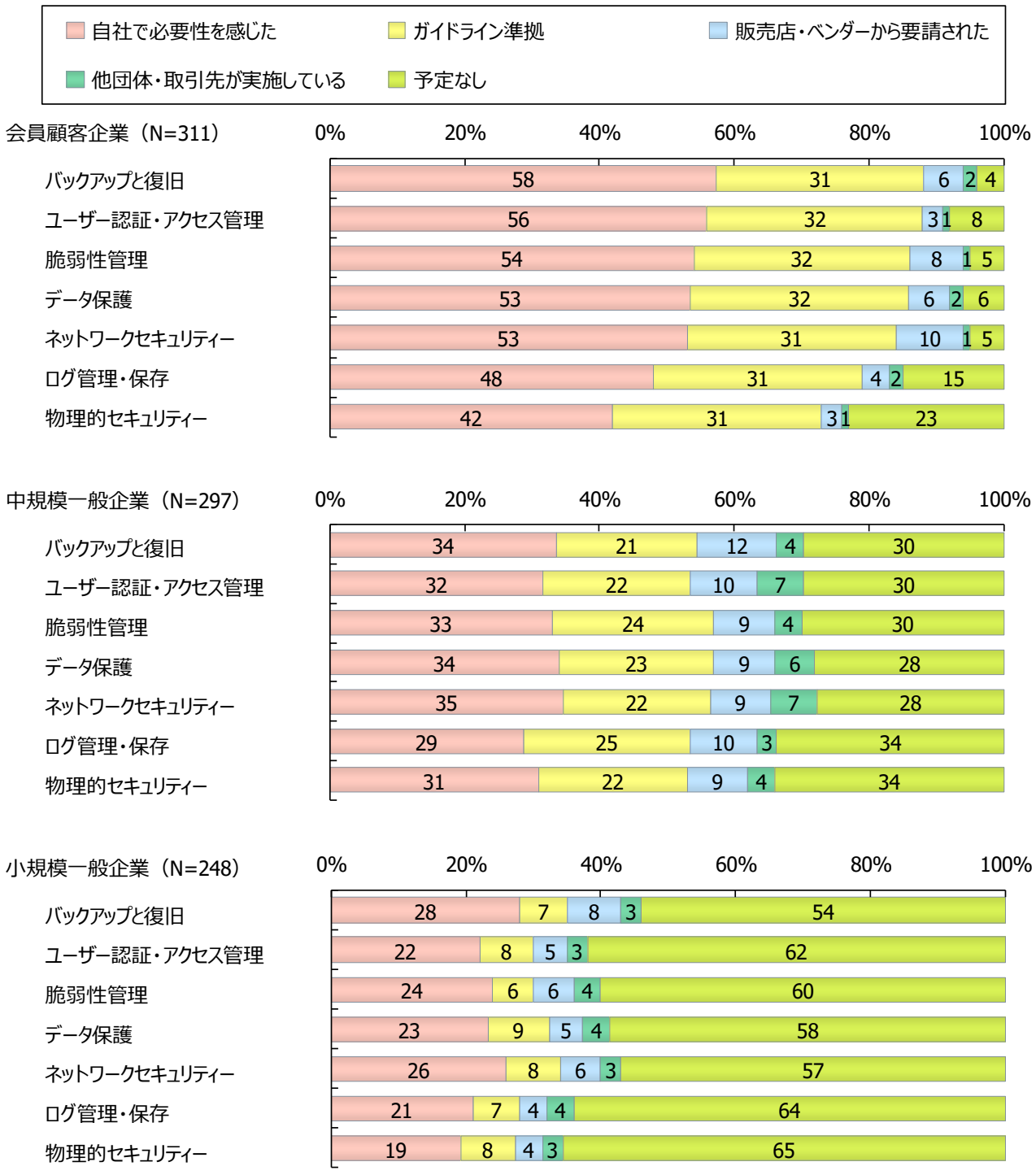
*4　国や各所属団体のセキュリティーガイドライン
例 1:サイバーセキュリティ経営ガイドライン（経済産業省）
https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf
例 2:自工会/部工会・サイバーセキュリティガイドライン（一般社団法人日本自動車工業会・一般社団法人日本自動車部品工業会）https://www.jama.or.jp/operation/it/cyb_sec/docs/cyb_sec_guideline_V02_00.pdf

各項目とも、会員顧客企業、中規模一般企業、小規模一般企業は、ほぼ同様の傾向を示しており、各項目ともに一番多かったきっかけは、「自社で必要性を感じた」で会員顧客企業 42～58%、中規模一般企業 29～35%、小規模一般企業 19～28%であった。

2 番目に多かったのは「ガイドラインに準拠」で会員顧客企業 31～32%、中規模一般企業 21～25%、小規模一般企業 6～9%であった。

いずれの企業群も、この 2 項目が中心であり、他の項目は辛うじて 10%に届く程度であった。

図表 2.2.1　　セキュリティー対策のきっかけ



2.2.2 導入済みあるいは導入予定のセキュリティー製品・サービス

今回の調査で、セキュリティー対策を導入済みあるいは導入予定の企業が、どのような製品またはサービスを導入しているかを聞いたのが、図表 2.2.2 である。

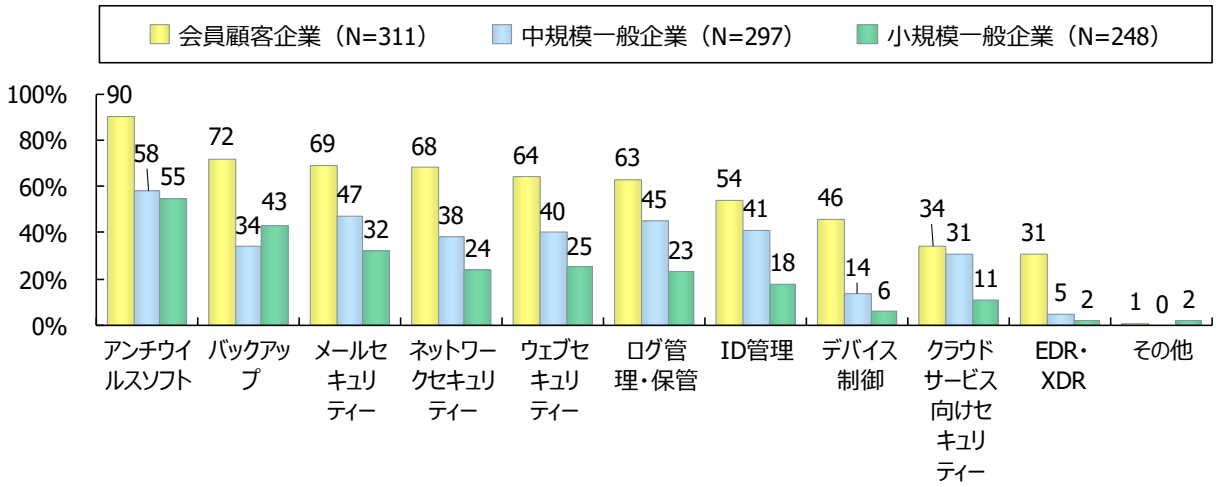
各企業群で最も導入あるいは導入予定されているセキュリティー製品あるいはサービスは、「アンチウイルスソフト」で、会員顧客企業で 90%、中規模一般企業で 58%、小規模一般企業で 55%であった。

以下、会員顧客企業の 2 番目は「バックアップ」で 72%、以下「メールセキュリティー」の 69%、「ネットワークセキュリティー」の 68%、「ウェブセキュリティー」の 64%、「ログ管理・保管」の 63%と続いている。

中規模一般企業の、2 番目は「メールセキュリティー」の 47%、「ログ管理・保存」の 45%、「ID 管理」の 41%、「ウェブセキュリティー」の 40%と続いている。

小規模一般企業の、2 番目は「バックアップ」の 43%、「メールセキュリティー」の 32%、「ウェブセキュリティー」の 25%、「ネットワークセキュリティー」の 24%、「ログ管理・保存」の 23%と続いている。

図表 2.2.2　　導入済みあるいは導入予定のセキュリティー製品・サービス



全体を通じて、ネットワーク関連のセキュリティー製品やサービスが比較的上位に位置付けられており、ネットワークを利用した情報活用やメールのやり取りを担保するためのツールやサービスが重視されている。

2.2.3 セキュリティー対策の運用

導入したセキュリティー対策に対して「セキュリティールールやポリシー」、「セキュリティー教育やトレーニング」、「インシデントへの対応体制整備」、「セキュリティー対策の評価や監査」がどのように運用されているかを聞いた。

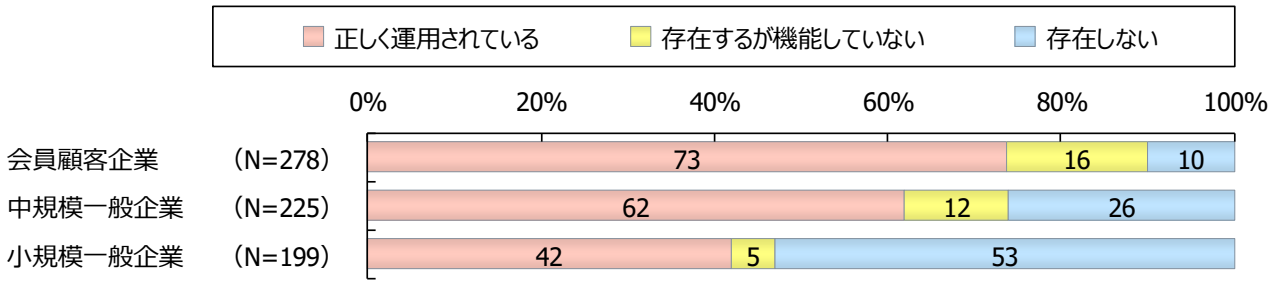
(1)　セキュリティールールやポリシー

「セキュリティールールやポリシー」の状況を聞いたのが、図表 2.2.3 である。

会員顧客企業や中規模一般企業では、「正しく運用されている」が 73%、62%と高い水準であり、ルールやポリシーは企業全体に行き渡っていると考えられる。

ただし、小規模一般企業では、「正しく運用されている」が 42%と半数に届かない状況であり、早急にルールやポリシーを確立させて、正しく運用できるよう改善の必要性が高いと考えられる。

図表 2.2.3　　セキュリティールールやポリシーの状況

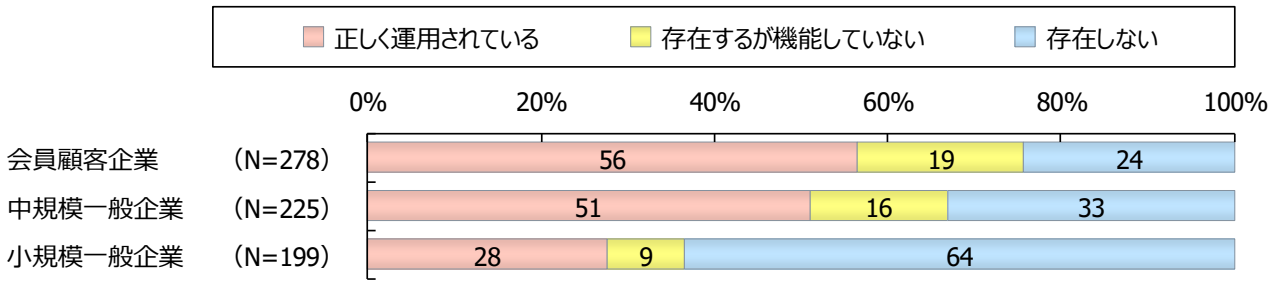


(2)　セキュリティー教育やトレーニング

次に、「セキュリティー教育やトレーニング」の運用状況を聞いたのが、図表 2.2.4 である。

(1)の「セキュリティールールやポリシー」に比べると、「正しく運用されている」は、会員顧客企業や中規模一般企業で 11～18 ポイント少ない 56%と 51%であった。正規社員や非正規社員に対するセキュリティー教育実施の難しさから、運用率が低くなっているものと思われるが、セキュリティー対策の基本ともいえる教育が低調であることは、不測の事態に遭遇するリスクも増加するため、早い時期の教育やトレーニングの充実を期待したいものである。

図表 2.2.4　　セキュリティー教育やトレーニングの状況

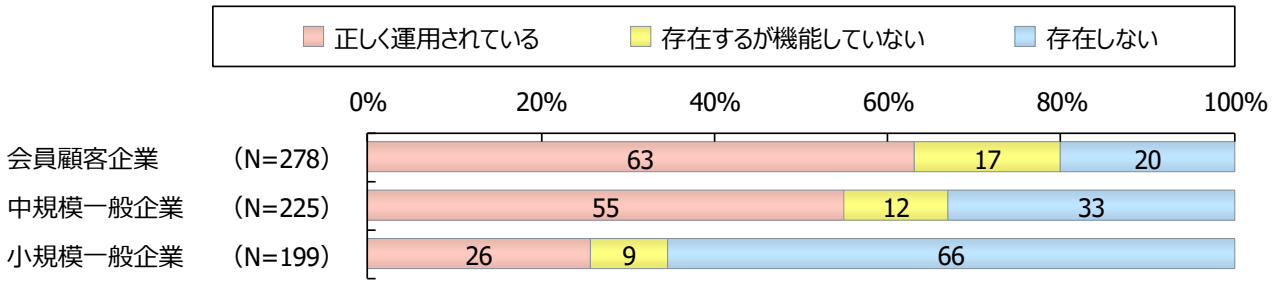


(3)　インシデントへの対応体制整備

3 番目に「インシデントへの対応体制整備」について聞いたのが、図表 2.2.5 である。

(2)の「セキュリティー教育・トレーニング」に比べると、会員顧客企業や中規模一般企業での「正しく運用されている」は 63%と 55%であり、「インシデントに対する対応体制整備」はある程度推進できていると言えよう。ただし、「存在するが機能していない」や「存在しない」が会員顧客企業で 37%、中規模一般企業で 45%あることは、これらの企業でのリスクマネージメントに大きな危惧を感じる。

図表 2.2.5　　インシデントへの対応体制整備の状況



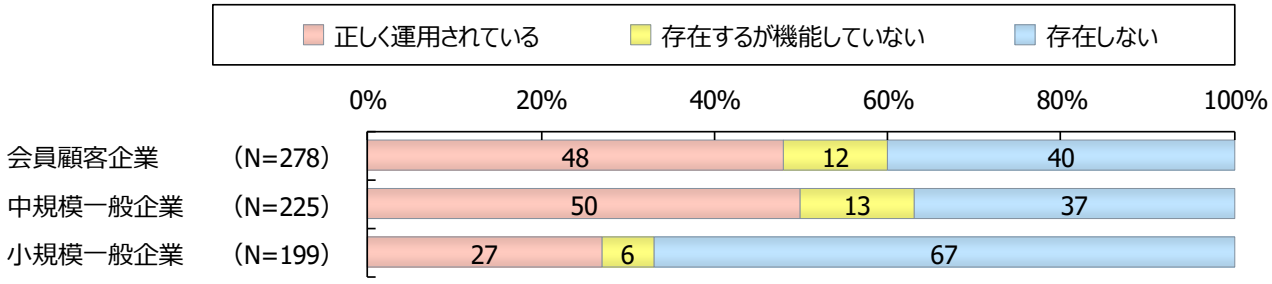
(4)　セキュリティー対策の評価や監査

運用の最後に聞いたのが「セキュリティー対策の評価や監査」で結果が、図表 2.2.6 である。

残念なことに、ここまでは質問ごとに「正しく運用されている」との回答が過半数を占めていた会員顧客企業が 48%と過半数を下回ってしまったこと、中規模一般企業においても、「正しく運用されている」は辛うじて過半数の 50%であり、「対策の評価や監査」については、誠に不十分と言わざるを得ない。

セキュリティー対策を講じて、セキュリティー問題に対応しようという意気込みは感じられるものの、実施した対策に対する評価や監査がなおざりになったのでは、せっかくの対策が有効に機能しない可能性があり、「評価や監査」の対する見直しをぜひ進めてもらいたいものである。

図表 2.2.6　　セキュリティー対策の評価や監査



セキュリティー対策の運用状況全般について、小規模一般企業では「正しく運用されている」は、辛うじてセキュリティールールやポリシーが 42%であったが、他は 26～28%しかなく、「存在するが機能していない」や「存在しない」が 70%近い現状から、全体的に見直しが必要であろう。

2.2.4 セキュリティー対策の見直し

導入済みのセキュリティー対策や現状システムの見直し・評価をどのように行っているかを聞いたのが、図表 2.2.7 である。

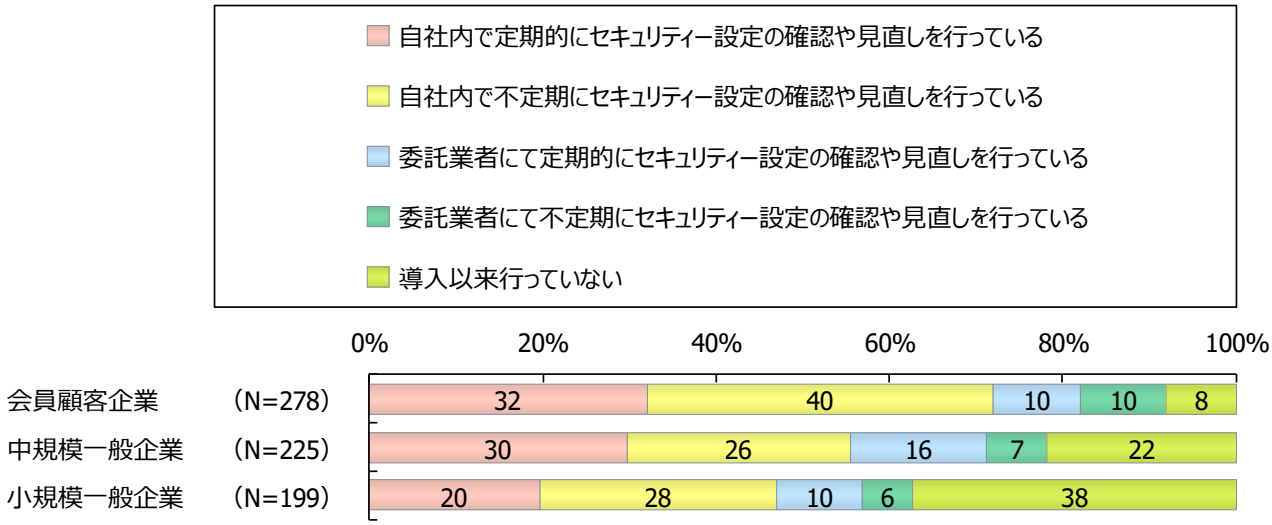
会員顧客企業では、定期的・ 不定期ならびに自社内・ 委託業者を問わずにセキュリティー設定の確認や確認を行っているとの回答が 92%に達しており、非常に安心できる状態であると言える。

中規模一般企業では、同様の状況での確認や見直しの実施率は 78%であり、やや不安は残るものの一応は安心できると思われる。

しかし、小規模一般企業になると、同様の状況で確認や見直しの実施率は 62%になっており、見直し回数の不足が懸念される。

今回の調査では、確認や見直しの状況を聞いたものであるため、問題が見つかったときの対応内容については聞いていない。見直し後の対応内容について、今後、継続的な調査により更なる効果検証ができるかもしれない。

図表 2.2.7　　セキュリティー設定の確認や見直し・評価



2.3　セキュリティーへの脅威と対策の理解度

セキュリティーへの脅威とそれらに対する対策についての理解度を調査した結果を示す。

2.3.1 把握しているセキュリティー脅威

独立行政法人情報処理推進機構が公表している「情報セキュリティー10 大脅威 2023*5」 について、最近の脅威ランキングと脅威の種類・内容（要約）を一覧表にしたのが、図表 2.3.1 である。

*5 情報セキュリティ 10 大脅威 2023（独立行政法人　情報処理推進機構）
https://www.ipa.go.jp/security/10threats/10threats2023.html

図表 2.3.1　　情報セキュリティー10 大脅威

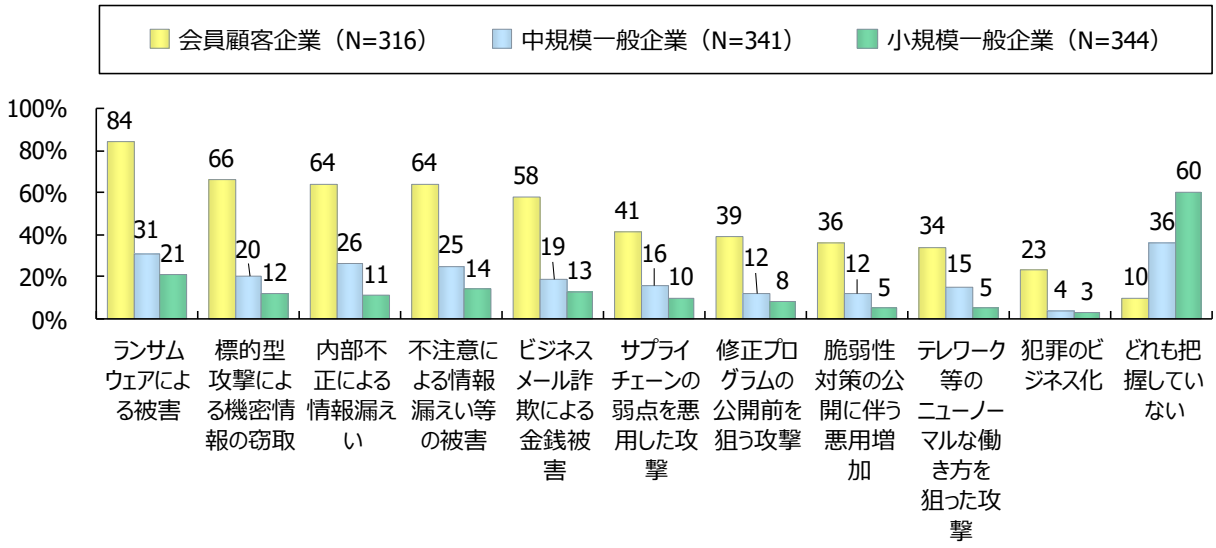
順位	脅威	内容
1	ランサムウェア	ランサムウェアと呼ばれるウイルスにPCやサーバーが感染すると、端末のロックや、データの暗号化が行われ、その復旧と引き換えに金銭を要求される。さらに、暗号化だけで は なく、重要な情報を窃取されることもあり、その情報を公開すると脅す。このように複数の脅しを組み合わせる（四重脅迫等）ことで、ランサムウェアに感染した組織が金銭を支払わざるを得ない状況を作り出そうとする。
2	サプライチェーンの弱点を悪用した攻撃	商品の企画・開発から、調達、製造、在庫管理、物流、販売までの一連のプロセス、およびこの商流に関わる組織群をサプライチェーンと呼ぶ。攻撃者はそのサプライチェーンを悪用し、セキュリティ対策の強固な関連企業・サービス・ソフトウェア等は直接攻撃せずに、それ以外のセキュリティ対策が脆弱なプロセスを最初の標的とし、そこを踏み台として顧客や上流プ ロセスの関連企業等 、本命の標的を攻撃する。また、もう1つのサプライチェーンとして「ソフトウェアサプライチェーン」もある。これはソフトウェア開発のライフサイクルに関与する全てのモノ（コード、ライブラリ、プラグイン、各種ツール等）や人（開発者、運用者等）の繋がりであり、ここを狙った攻撃も行われている。
3	標的型攻撃による機密情報の窃取	標的型攻撃とは、特定の組織（官公庁、民間団体、企業等）を狙う攻撃のことであり、機密情報等を窃取することや業務妨害を目的としている。攻撃者は社会の変化や、働き方の変化に便乗し、状況に応じた巧みな攻撃手法で機密情報等を窃取しようとする。
4	内部不正による情報漏えい	組織に勤務する従業員や元従業員等の組織関係者による機密情報の持ち出しや悪用等の不正行為が発生している。また、組織内の情報管理の 規則 を守らずに情報を持ち出し、紛失や情報漏えいにつながるケースもある。組織関係者による不正行為は、組織の社会的信用の失墜、損害賠償による経済的損失を与える。また、不正に取得した情報を他組織に持ち込んだ場合、その組織も損害賠償等の対象になるおそれがある。
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	2020年以降、新型コロナウイルス感染症（ COVID-19）の世界的な 蔓延に伴い、感染症対策の一環として政府機関がニューノーマルな働き方の 1つであるテレワークを推奨している。勤労形態としてテレワークが活用され、ウェブ会議サービスや VPN等の本格的な活用がされる中、それらを狙った攻撃が行われている。
6	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	OSやソフトウェアに脆弱性が存在することが判明し、脆弱性の修正プログラム（パッチ）や回避策がベンダーから提供される前に、その脆弱性を悪用してサイバー攻撃が行われることがある。これをゼロデイ攻撃という。 多くのシステムで利用されているソフトウェアに対してゼロデイ攻撃が行われると、社会が混乱に陥るおそれがある。
7	ビジネスメール詐欺による金銭被害	ビジネスメール詐欺（Business E-mail Compromise BEC）は、悪意のある第三者が取引先等になりすまして偽のメールを送ったり、組織間のメールのやり取りを乗っ取ったりした上で、最終的に偽の銀行口座に送金させるサイバー攻撃である。組織間取引の送金であることから被害額は大きくなる。
8	脆弱性対策情報の公開に伴う悪用増加	ソフトウェアやハードウェア（機器類）の脆弱性対策情報の公開は、脆弱性の脅威や対策情報を製品の利用者に広く呼び掛けられるメリットがある。一方で、攻撃者はその情報を悪用し、当該製品への脆弱性対策を講じていないシステムを狙って攻撃を行うことができる。近年では脆弱性関連情報の公開後に攻撃コードが流通し、攻撃が本格化するまでの時間 もますます短くなっている。
9	不注意による情報漏えい等の被害	メールの誤送信や記録端末や記録媒体の紛失等の不注意による個人情報等の漏えいが発生している。漏えいした情報が第三者に売買されるとさらなる悪用につながるおそれもある。情報漏えいした組織は社会的信頼の失墜や経済的な損失につながるおそれもあり、組織はデータに対して慎重な扱いが求められる。
10	犯罪のビジネス化（アンダーグラウンドサービス）	犯罪に使用するためのサービスやツール、IDやパスワードの情報等がアンダーグラウンド市場で取り引きされ、これらを悪用した攻撃が行われている。攻撃に対する専門知識が無い者でもサービスやツールを利用することで、容易に攻撃を行えるため、サービスやツールが公開されると被害が広がるおそれがある。

各企業が、「情報セキュリティー10 大脅威」の中で脅威として把握しているのが、図表 2.3.2 である。

会員顧客企業が把握している脅威は、「ランサムウェアによる被害」がトップの 84%で、以下「標的型攻撃による機密情報の窃取」が 66%、「内部不正による情報漏えい」と「不注意による情報漏えい等の被害」が 64%、「ビジネスメール詐欺による金銭被害」が 58%と続いた。それ以外の脅威も 23～41 と非常に高い状況であった。

中規模一般企業や小規模一般企業では、把握している脅威は比較的比率が低く、中規模一般企業で4～31%、小規模一般企業では、3～21%であった。

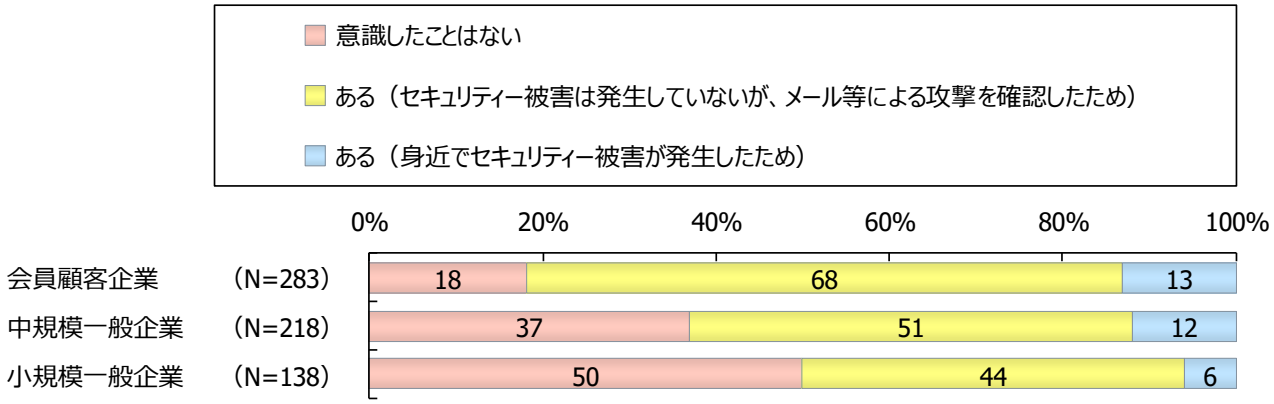
図表 2.3.2　　把握しているセキュリティー脅威



2.3.2 セキュリティーへの脅威経験

次に、10 大脅威に対して「どれも把握していない」以外の回答を寄せた企業に対して 3 年以内に身近な脅威として意識したことがあるかを聞いたのが、図表 2.3.3 である。

図表 2.3.3　　3 年以内に意識したセキュリティー脅威
（把握している脅威がない企業を除く）



会員顧客企業では、「意識したことはない」はわずか 18%しかなく、「具体的被害は発生していないがメール等による攻撃を確認した」が 68%、「身近で被害が発生した」が 13%であった。一般企業では、会員顧客企業に比べれば比率は低いが、あると答えた企業は中規模一般企業で「具体的被害は発生していないがメール等による攻撃を確認した」が 51%、「身近で被害が発生した」が 12%、小規模一般企業で「具体的被害は発生していないがメール等による攻撃を確認した」が 44%、「身近で被害が発生した」が 6%であった。独立行政法人情報処理推進機構が調査した「2021 年度中小企業における情

報セキュリティー対策の実態調査」*6 では、2020 年 4 月～2021 年 3 月の 1 年間に「被害にあっていない」の回答が 84.3%あり、対象期間が 1 年と 3 年であることを差し引いても、近年はセキュリティー被害が増加してきていると言える。

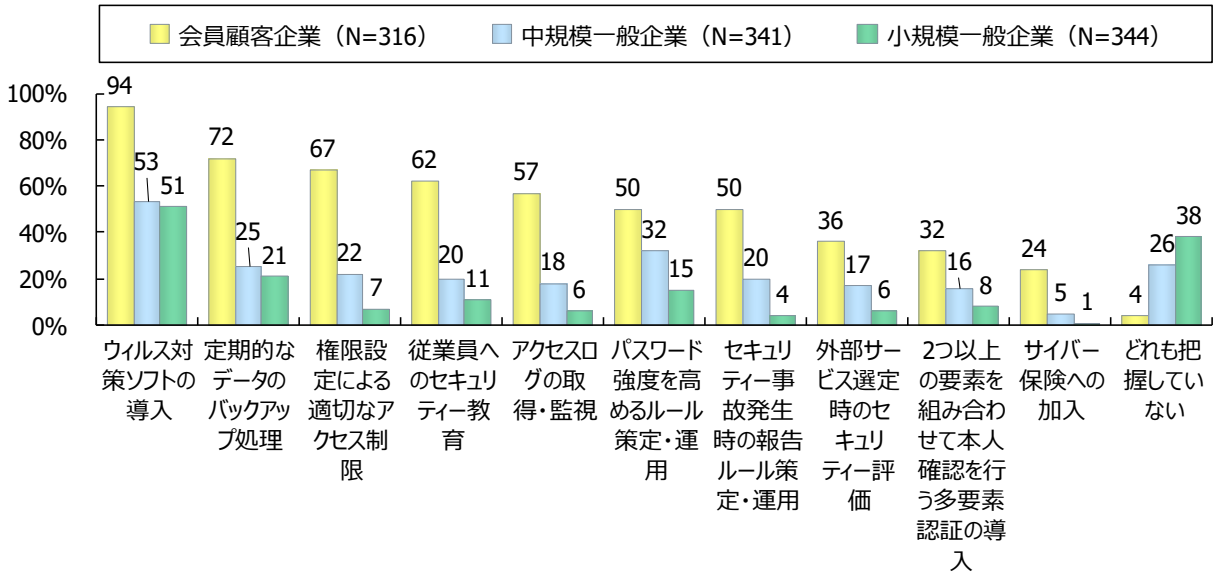
2.3.3 把握しているセキュリティー対策

こうした脅威に対して、各企業が採っているセキュリティー対策を聞いたのが、図表 2.3.4 である。

会員顧客企業、中規模一般企業、小規模一般企業を通して、最も把握している対策は「ウィルス対策ソフトの導入」で、会員顧客企業で 94%、中規模一般企業で 53%、小規模一般企業でも 51%であった。ネットワークに接続された IT 環境下では、何らかの形でウィルスが侵入する可能性があり、侵入前に対応できる対策ソフトが導入されているものと思われる。

それ以外の対策としては、「定期的なデータのバックアップ処理」や「権限設定による適切なアクセス制限」などが上位に挙げられた。

図表 2.3.4　　セキュリティー脅威に対する対策



2.4　セキュリティーに対する要請に対応できていない理由

最後に、図表 2.1.2 で示した「セキュリティー対応の要請元」に対して、十分対応ができていない理由は何かを聞いたのが、図表 2.4.1 であるが、回答企業が会員顧客企業 1 社、中規模一般企業 11 社、小規模一般企業 13 社しかないため、分析は割愛する。

*6 出典：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（独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/reports/sme/about.html

図表 2.4.1　　セキュリティーに対する要請に対応できていない理由