ASM 診断および事例集作成業務

実施報告書

2026 年 3 月

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目次

1. 本事業の概要

1.1. 背景と課題認識

本事業は、中小企業のサイバーセキュリティ対策強化を目的とした実証事業の一環として実施した。昨今、サイバー攻撃の巧妙化・多様化が進む中、特に中小企業においては、限られたリソースや知見の不足から十分な対策がとられていない現状が指摘されている。そのような状況を踏まえ、ASM（Attack Surface Management）ツールを活用することで、外部から見える自組織の IT 資産や脆弱性を客観的に把握し、リスク低減に向けた適切な対策を促進することを狙いとしている。

本事業では、126 社の中小企業を対象に ASM ツールによる診断を実施し、さらにアンケートやヒアリング調査を通じて効果や課題を多面的に検証したものである。

1.2. 本事業の目的

本事業の主たる目的は、ASM ツールを活用したサイバーセキュリティ診断が中小企業の実態に即してどの程度有効に機能するかを実証的に検証することである。中小企業の現状のセキュリティ対策レベルや課題を把握し、ASM ツールによる診断がどのような気付きや改善行動につながるかを評価した。また、診断を通じて得られた知見を基に、中小企業における今後の効果的なサイバーセキュリティ支援策のあり方を検証し、有効な施策に資することを目指している。

2. 事業実施体制とプロセス

2.1. 実施体制と役割分担

事業を遅延なく遂行するために、事務局では本事業のプロジェクトチームを編成し、各業務分担において複数名の担当者を配置し、余裕を持った体制を構築した。

統括責任者およびプロジェクトリーダーは、ASM ツールによる診断業務経験が豊富な者を配置し、プロジェクトチームの構成メンバーには、情報セキュリティ対策業務経験を有する者および ASM の製品開発や診断業務経験に携わる者、サイバーセキュリティに関するコンサルティングを専門領域とする者を複数名配置した。また、過去に同種の実証事業の経験がある者や、サイバーセキュリティ領域・リスクマネジメント領域に係る文献執筆実績のある者がアドバイザーとして各業務への助言・実行支援を行った。

事業全体の推進にあたっては、プロジェクトリーダーを中心とする事務局が全体の進行管理や関係者調整、問い合わせ対応を担い、診断担当者が ASM ツールを用いた診断実務を実施した。調査担当者はアンケートやヒアリングの設計・実施・集計・分析を担当し、コンサルティング実務経験者が成果物のレビューや助言を行うことで、事業の品質確保と客観性の担保を図った。

参加事業者側とは、必要な情報提供や診断・調査への協力を求められる関係性を構築し、双方向のコミュニケーションを重視した運営体制とした。

2.2. 参加事業者の募集・選定プロセス

本事業の対象として適切な 100 社以上の ASM 参加事業者を確保するため、下表の要件に合致する企業を募集した。

募集要件
1. 中小企業基本法第2条第1項に定める範囲に合致する中小企業者および、小規模事業者
・中小企業庁の定める中小企業者および小規模事業者
2.以下のいずれかに合致する事業者
・経営層が意欲的にサイバーセキュリティに取り組み、対応体制を構築している事業者 ・これからサイバーセキュリティ対策に積極的に取り組みたい事業者 ・取引先などの外部から強くサイバーセキュリティの取り組みを要請されている事業者 ・第三者が行うセキュリティ診断に興味・関心のある事業者 ・必要性は感じているもののサイバーセキュリティ対策の進め方に不安がある事業者 ・過去3年以内にサイバー攻撃や情報漏えいの被害経験がある事業者
3.以下に協力いただける事業者
・ASMツールを使った診断 ・診断後のアンケート回答およびインタビュー

表1　募集要件

事業者の募集においては以下の取組を行った。募集にあたっては、よくある質問(FAQ)を用意し、問い合わせ対応の効率化と応募者の不安解消を図った。

(1) 過去に請負事業者で ASM 診断を実施した企業

請負事業者はこれまでに約 2,000 社に ASM 診断を実施している。このデータベースから
「企業規模(従業員数)」
「業種(製造・建設業、情報通信業、金融・保険業、卸売・小売業、医療・福祉業を中心に5業種以上、偏りがないように抽出)」
「所在地(北海道・東北、関東、中部、近畿、中国・四国、九州・沖縄の6地域から偏りがないよう抽出)」の3軸で本事業の参加候補者を抽出し、参加の呼びかけを行った。

(2) 請負事業者のwebサイト会員、メルマガ会員、既存顧客

請負事業者の web サイト会員、メールマガジン会員、コンサルティング業務等の既存顧客に対しても、本事業の参加事業者となりうる企業を抽出、参加の呼びかけを行った。

なお、上記の他に、中部経済産業局より中部エリアの企業に参加呼びかけを行っていただき、本事業の関心の高い企業が7社参加となった。

2.3. 参加事業者向け説明会の実施

本事業の説明会は、オンライン開催を基本として行った。対象企業が全国各地に所在しており、本業の都合等から、リアルタイム参加できない企業が多数いると想定し、オンライン・リアルタイムで 1 回開催し、当日参加できなかった企業向けにアーカイブ配信(動画視聴および資料ダウンロード)を行う方針とした。

日時	2025 年 9 月 17 日(水)13:00-13:45
開催方式	Zoom によるオンライン開催
説明会内容	1. 本事業の背景・目的 2. 昨今のサイバー攻撃と被害の概況 3. 中小企業・小規模事業者のサイバーインシデント事例 4. ASM ツールによる診断の説明 5. 今後の流れ 6. お問い合わせ・ご質問

表2 参加事業者向け説明会 概要

2.4. 参加事業者の業種・企業規模・エリア分布

参加事業者の選定にあたっては、業種別、規模別、地域別に分類し、特定の業種や規模に偏らないように調整を行い、幅広い事業者が参加できるように努めた。参加事業者の属性は下表のとおり。本事業の正式な参加案内を送付した 1,248 社のうち、126 社が正式に参加を表明した。

※一部、募集要件当てはまらない企業が含まれるが、本事業の主旨を理解し、積極的な協力が見込まれたため許容した。

個数 / 企業名	エリア						
industry	①北海道東北	②関東	③中部	④近畿	⑤中国四国	⑥九州沖縄	総計
製造・建設業	3	14	17	16	2	1	53
情報通信業	1	19			3	3	26
金融・保険業	4	10	1	3	1	1	20
卸売・小売業		7	5	7			19
医療・福祉業		4	2	2			8
総計	**8**	**54**	**25**	**28**	**6**	**5**	**126**

表 3　参加事業者　業種別・エリア別

個数 / 企業名	企業規模					
industry	①20名未満	②～50名	③～100名	④～300名	⑤～500名	総計
製造・建設業	1	4	16	31	1	53
情報通信業	9	4	3	10		26
金融・保険業	8	7	4	1		20
卸売・小売業	1	3	8	7		19
医療・福祉業		1	4	3		8
総計	**19**	**19**	**35**	**52**	**1**	**126**

表 4　参加事業者　業種別・企業規模別

2.5. 実施メニューとスケジュール

本事業の主な実施メニューとしては、まず説明会の開催による事業内容の周知と参加事業者の募集を行った。続いて ASM ツールによる診断を実施し、全参加事業者に対し診断結果のフィードバックを丁寧に行い、特に CRITICAL もしくは HIGH が検知された事業者には、当該脆弱性の詳細と推奨する対策を示した資料とともに解説を行った。その後、全参加事業者へアンケート調査を実施、10 社に対してヒアリング調査を実施、これらを分析した。これらの調査を通じて得られた参加事業者における脆弱性の対応事例や、好取組事例を事例集としてまとめ、本事業全体の総括として実施報告書の作成を行った。

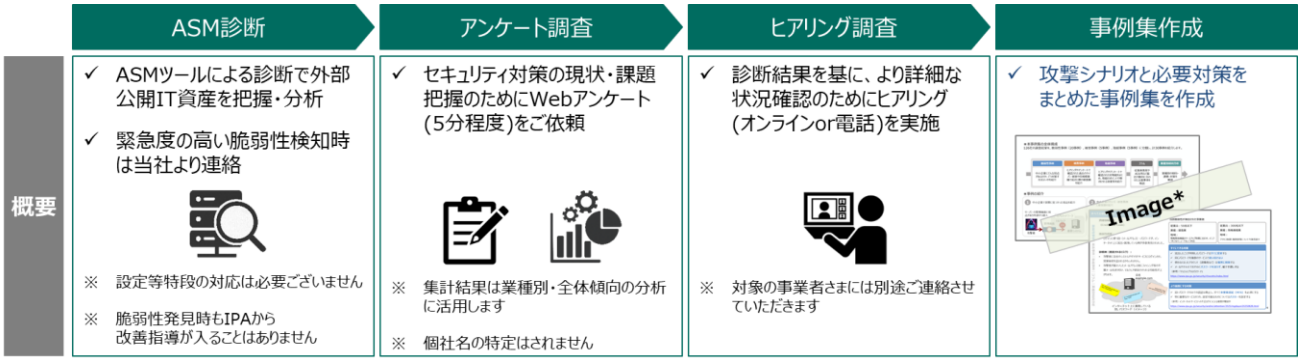

図 1　事業の全体像

全体スケジュールは下図のとおりである。それぞれのメニューで、実施時期や所要期間を明確に設定し、全体進捗や成果物の品質を担保した。主要なマイルストーン(例:アンケート結果集計後の速報報告)や進捗確認会議を開催し、事業運営を円滑に行った。

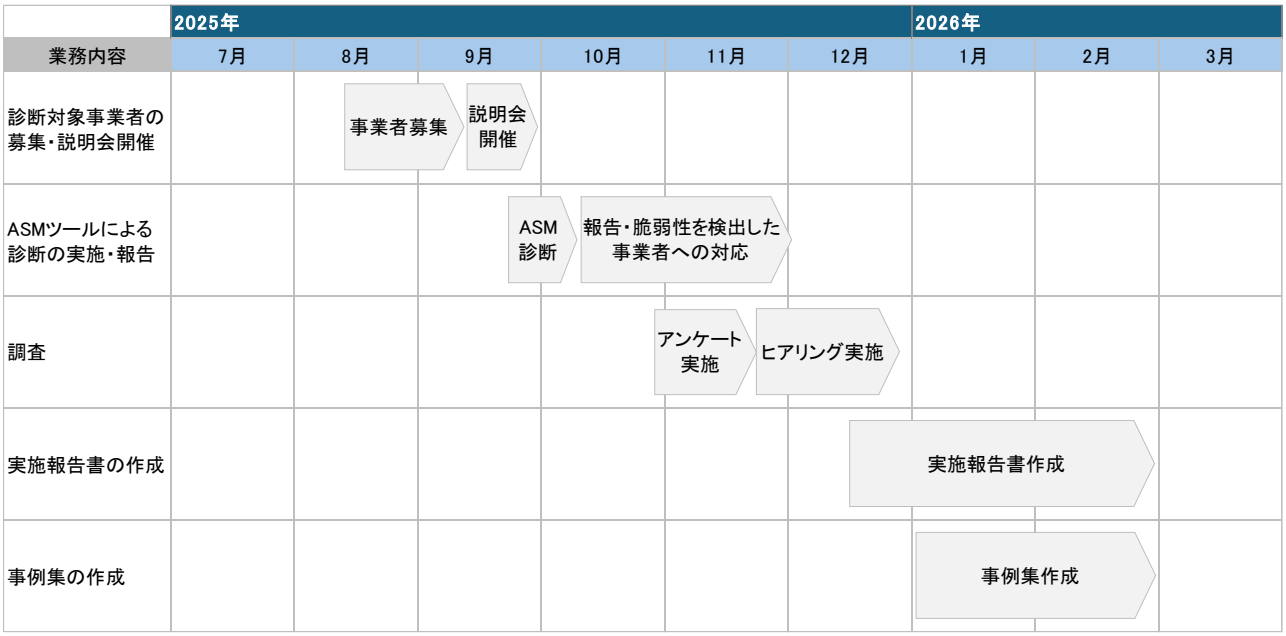

図 2　全体スケジュール

3. ASM ツールによる診断の実施と結果

3.1. ASM ツールの概要

本事業で活用した ASM ツールには、ASM 診断サービス「MS&AD サイバーリスクファインダー」（以下、CRF とする）を活用した。当該サービスは、対象事業者が管理している「ドメイン名」に紐づく IT 資産と脆弱性の有無を検出、分析したうえでリスク評価したものをレポートにまとめる。

CRF は、Coalition 社[1]のもつ世界中から収集したデータベースをもとに、独自の検索エンジンを活用して外部公開資産の自動検出や、脆弱性の洗い出し、リスク評価、レポート自動生成など多様な機能を備える ASM ツールである。

特に、インターネット上に公開されているサーバやリモート接続機器、ウェブサイトなどの資産を網羅的に可視化し、最新の脅威インテリジェンスと連携してリスク度合いを判定する点が特徴である。

また、診断結果を分かりやすく見える化するレポートや、過去の診断結果との比較・傾向分析も可能とするサービスである。こちらを活用して、参加事業者の現状把握を行い、脆弱性の把握や改善行動に資するかどうか検証を行った。

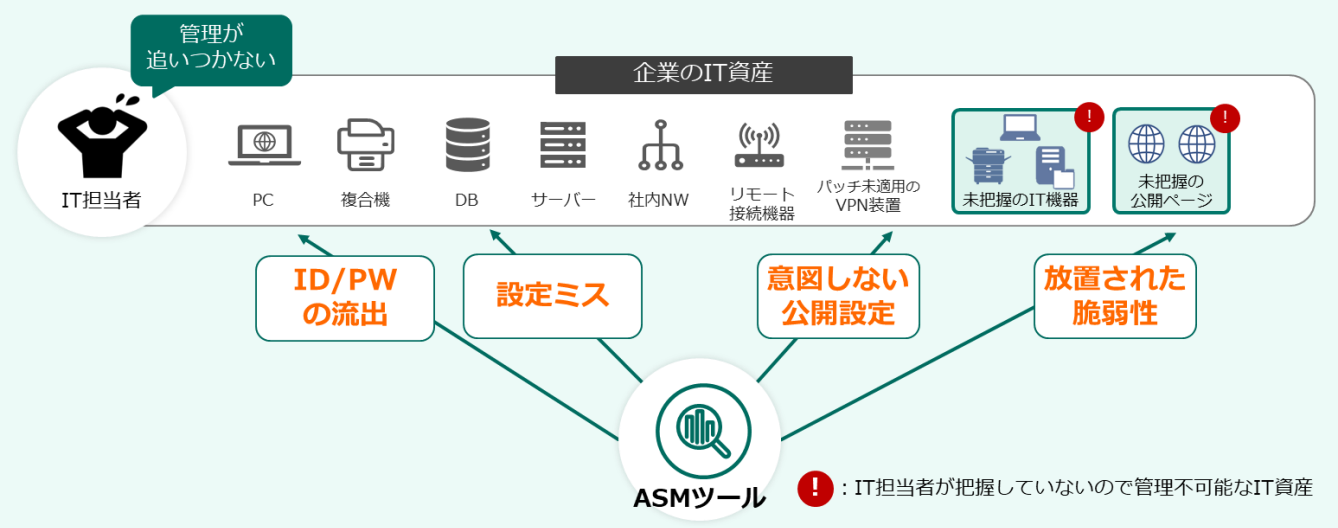

図 3　ASM ツールの概要

3.2. ASM 診断の実施方法

ASM ツールによる診断は、参加事業者のドメイン情報を用いて期間中に全件実施した。具体的には次の手順で行った。診断にあたっては高度な専門知識を要することなく、参加事業者のメールアドレスと最低限の情報を入力するだけで、速やかに診断結果を受領することができ、診断中に発生したトラブ

[1] Coalition 社：カリフォルニア州サンフランシスコに本社をおく「MS&AD サイバーリスクファインダー」の共同開発事業者。2017 年創業。

ルや問い合わせ対応、追加要望にも柔軟に対応し、円滑な診断運用を行った。

STEP1：
・参加事業者は、専用 web サイトにてメールアドレスを登録し、「マイページ」を作成する
・メールアドレスのドメインが、診断対象のドメインとなる
STEP2：
・事務局は、登録された対象事業者のメールアドレスにユーザー認証メールを発信する
STEP3：
・参加事業者は、事務局から発送されたユーザー認証メール本文内に記載された URL から連絡先等の情報を入力する
・登録完了すると「マイページ」へのログインが可能となる
STEP4：
・事務局にて「MS&AD サイバーリスクファインダー」を用いたスキャンを実施する
・スキャン実施後、診断レポートを発行、メールで参加事業者に通知する
STEP5：
・参加事業者は「マイページ」へログインし、診断レポート（PDF ファイル）をダウンロードする

検知した脆弱性はセキュリティ知識のない人にもわかりやすいよう、リスクレベル別で 4 段階（CRITICAL、HIGH、MEDIUM、LOW）に分類したレポートを作成した。リスクレベルは、CVE（Common Vulnerabilities and Exposures）や CVSS（Common Vulnerability Scoring System）などの公知情報に加えて、Coalition 社のインシデントレスポンスチームがフォレンジック調査で得た実際の攻撃手法の分析結果、サイバー保険の保険金請求額に基づく重大度も加味、また、該社が行う年約 48 兆回のネットワークスキャンによる企業のセキュリティデータもかけ合わせて評価する仕組みである。

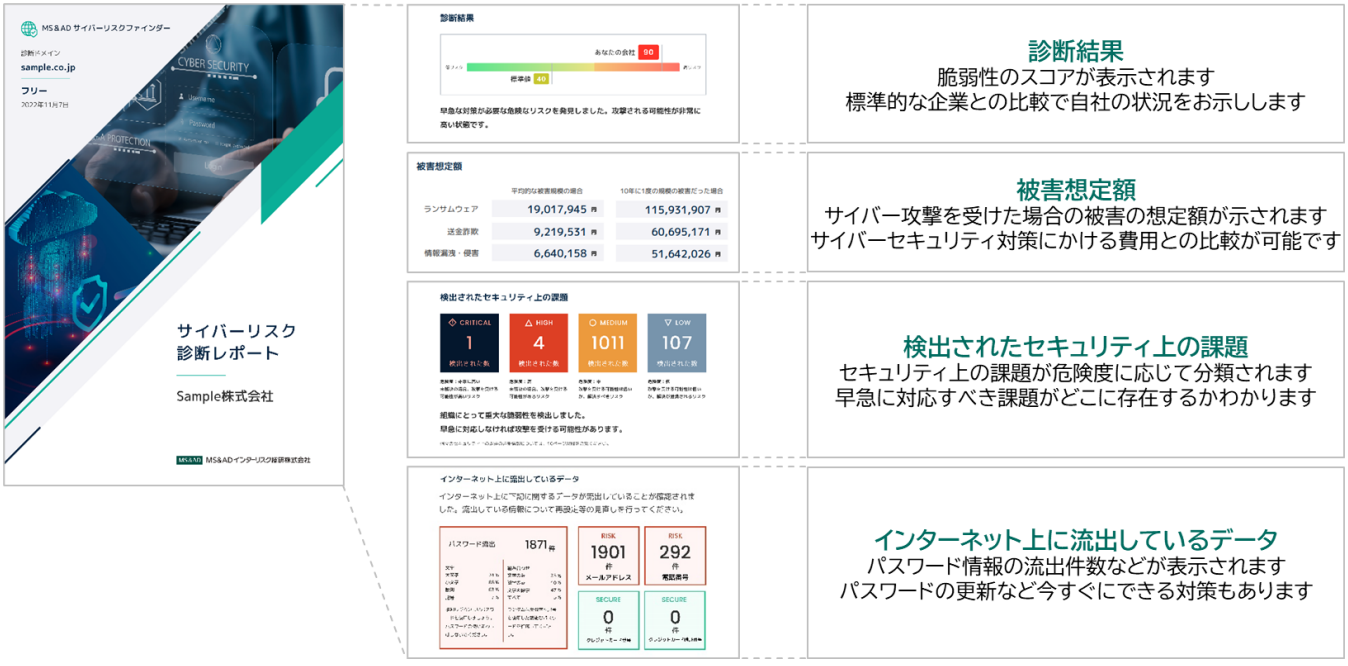

図 4　ASM 診断結果レポートのイメージ

3.3. 診断結果のフィードバック

診断終了後は、企業ごとに診断結果をまとめたレポートを作成し、マイページより確認できる旨メールで案内した。またマイページを見ない参加事業者も想定されたため、事務局からも個別に診断結果レポートと脆弱性の日本語解説資料をメール添付で送付した。それとは別に、緊急度の高い CRITICAL,HIGH の脆弱性を検知した診断先には、該当企業に脆弱性の解説および推奨対応事項を記載した資料を作成し個別に送付した。

診断レポートでは ASM ツールによる診断結果のほかダークウェブ上で取引されている参加事業者の情報や、診断対象ドメインに関係する通信履歴を調査し、不正アクセスやマルウェア感染、メールアカウントの乗っ取りのおそれの有無も報告した。

本事業で使用した ASM ツール（CRF）の診断レポートにて記載される項目は以下のとおり。

表 5　ASM ツール（CRF）の診断レポートにて記載される項目

項目	項目の説明
診断結果	診断結果リスクスコア（0～100 点（標準値 40 点））で脆弱性のスコアを表示する。標準値との比較で、自組織の対策が十分か判断できる。
想定被害額	想定被害額を記載する。一般的な企業における、サイバーセキュリティ予測被害額をシミュレーションした金額を記載する。対象事業者の意識向上、注意喚起を目的としている。
検出された セキュリティ上の課題	検出されたセキュリティ上の課題を、リスクレベル（攻撃を受ける可能性）別で4段階（CRITICAL、HIGH、MEDIUM、LOW）に区分し、優先順位を付けた検出数を記載することで、現状と緊急度をわかりやすく表記する。
インターネット上に 流出しているデータ	インターネット上に流出しているデータ（アカウントおよびパスワード、電話番号、クレジットカード番号、クレジットカード暗証番号など）があるかどうかを診断する。パスワードについては、使われている大文字・小文字・数字・記号の使用割合や組合せを表示することで、より強固なパスワード設定ルールに沿ったパスワード再設定の案内など見直しのきっかけとする。
非常に危険度が高い 脆弱性（CRITICAL）	指摘内容のニュアンスが変わらないよう英語での記載となっている。検知された脆弱性に対する「検出名」「検出内容」「対策方法」を、リスクレベルごとに記載した日本語訳の一覧 PDF をマイページからダウンロードし、脆弱性への対策方法を確認できるようにしている。
その他（クリティカル以外） の脆弱性（HIGH、 MEDIUM、LOW）	指摘内容のニュアンスが変わらないよう英語での記載となっている。検知された脆弱性に対する「検出名」「検出内容」「対策方法」を、リスクレベルごとに記載した日本語訳の一覧 PDF をマイページからダウンロードし、脆弱性への対策方法を確認できるようにしている。

項目	項目の説明
不正なソフトウェア（マルウェア）	自組織のネットワーク資産でウイルスやワーム等、悪意のあるソフトウェアによる活動を検出する。本項目を診断することで、ウイルスやワームに感染している可能性や、データの破壊や盗難などの被害が発生する、あるいは発生していた可能性を確認することができる。
迷惑メール（スパム）	自組織のドメインが迷惑メール等の送信に利用されていないかを検出する。本項目を診断することで、迷惑メール送信の踏み台とされているか確認することができる。
不正なインターネット侵入	本来アクセス権限を持たないものによる自組織のサーバや情報システム内部へ侵入の試行、または成功した可能性を検出する。本項目を診断することで、ハッカー（攻撃者）による不正アクセス有無の可能性を確認することができる。
ハッキング検知のおとり（ハニーポット）への攻撃	本サービスで設置しているハニーポットへ攻撃の試みがあったことを検知する。本項目を診断することで、自組織に対してハッカー（攻撃者）が攻撃を試みた、もしくは攻撃が成功した可能性を確認することができる。
ブラックリスト（ブロックリスト）に登録されているドメイン	自組織のメールサーバのドメインや IP アドレスが迷惑メールの発信源としてブラックリストに登録されていないか判定する。本項目を診断することで、自組織内で何らかの不正な活動が発生しているか確認することができる。
違法性の高いダウンロード（トレント）	自組織のネットワーク資産とファイル共有ソフト（Torrents）の通信を検出する。本項目を診断することで、ウイルス感染や不正侵入されている可能性、もしくは従業員によるポリシー違反を確認することができる。
メール送信元確認機能（SPF）	SPF とは、メールを受信した企業がなりすましかどうかを判別するための仕組みである。自組織が送信元ドメイン認証技術を正しく設定しており、送信元ドメインの IP アドレスが正当なものであるかを確認することで、ドメイン偽装によるスパムメールを防止できているかを判定する。本項目を診断することで、なりすましメールの対策がされているか確認することができる。

フィードバック時には、検出されたリスクや脆弱性の内容、優先的に対応すべき事項、ASM ツールの活用ポイントなどを丁寧に解説し、脆弱性の改善対応に資する推奨策を盛り込んだ付属資料を提供し、改善提案を行った。参加事業者からは多くの質問や意見が寄せられ、診断結果を基に実際の改善活動につなげる動きも見られた。

3.4. **診断結果の分析と共通傾向**

本事業では下表に示す 45 の脆弱性が検出された。未管理の公開資産や古いソフトウェアの利用、設定不備などが複数の企業で共通して見られた。各脆弱性によるリスクと対策は、事例集にてまとめているため、そちらを参照されたい。

表 6　検知された脆弱性一覧

No.	脆弱性	レベル	検出社数	脆弱性概要
1	Fortinet FortiGate SSL VPN Panel Exposed	critical	7	Fortinet FortiGate の VPN 機能(SSL VPN)を使用している
2	Exposed Fortinet Device	critical	7	Fortigate(VPN 装置)の存在を外部から確認できる状態
3	DNS Server Zone Transfer Information Disclosure (AXFR)	critical	3	DNS サーバのゾーン転送設定の不備
4	CVE-2025-49113: Roundcube Webmail	critical	1	ウェブベースの電子メールクライアントである Roundcube ウェブメールの脆弱性
5	End-of-life Microsoft IIS Server Found	critical	1	Microsoft 製 Web サーバ IIS のサポート切れ
6	Cisco ASA VPN Panel Exposed	critical	1	Cisco ASA(Adaptive Security Appliance)の VPN 機能を使用している
7	Keycloak Admin Panel Exposed	critical	1	Keycloak(ID 管理やアクセス管理を実現するオープンソースソフトウェア(OSS))の管理パネルを使用している
8	Fortinet FGFM Protocol Exposed	critical	1	Fortinet デバイスの FortiManager(FGFM)プロトコルがインターネットに公開されている
9	Microsoft Remote Procedure Call (RPC) Service Exposed	critical	1	RPC(プロセス間通信(IPC)メカニズムで異なるプロセスに存在する機能のデータ交換と呼び出しが可能)が公開されている
10	GIT Repository found	critical	1	Git のメタデータディレクトリ(プロジェクトのファイルやその変更履歴をまとめて管理する仕組みで、開発の進捗確認や過去の状態への復元などに利用できる)を検出
11	Sophos VPN Login Panel Exposed	critical	1	Sophos VPN(Sophos 社が提供するファイアウォール製品 Sophos Firewall に含まれる VPN 機能)のログインパネルが検出

No.	脆弱性	レベル	検出社数	脆弱性概要
12	Plesk Obsidian Panel Exposed	high	9	Plesk Obsidian(ウェブホスティングおよびサーバ管理のための商用コントロールパネル)の管理パネルを使用している
13	CVE-2024-6387: OpenSSH Remote Code Execution Vulnerability	high	7	OpenSSH リモートコード実行脆弱性(シグナル処理の競合状態に起因しリモートコードを実行)
14	phpMyAdmin Panel Exposed	high	5	phpMyAdmin(MySQL サーバを Web ブラウザで管理するためのデータベース接続クライアントツール)の管理パネルを使用している
15	WordPress Panel Exposed	high	5	WordPress(オープンソースのパブリッシングプラットフォームでさまざまなウェブサイトを構築できるコンテンツマネジメントシステム(CMS))の管理パネルが検出
16	Google API Key Exposed	high	3	Google API Key が公開されている
17	Plesk Onyx Panel Exposed	high	1	Plesk Onyx(ウェブホスティングとサーバ管理を簡素化するための商用ウェブホスティングコントロールパネル)の管理パネルを使用している
18	SNMP Service exposed	high	1	公開されている SNMP(TCP/IP ネットワーク環境の監視・管理を担うプロトコル。ネットワーク機器やサーバの状態を監視)が検出されている
19	HTTP Service without SSL/TLS found	medium	112	通信が暗号化されていない HTTP サービスの検出
20	FTP Service without SSL/TLS found	medium	85	暗号化されていない FTP サービスの検出
21	Email Service without SSL/TLS found	medium	81	暗号化されていないメールサービスの検出
22	Expired Certificate	medium	26	期限切れの証明書の検出
23	Self-Signed Certificate	medium	25	自己証明書の検出
24	MySQL Service found	medium	8	MySQL サービスの外部公開
25	Internal path disclosure	medium	7	アプリケーションや Web サーバのエラーメッセージなどに、サーバ内部のファイルパスがそのまま表示されてしまう状態。
26	Exposed phpinfo() Page	medium	7	phpinfo() を実行するページがインターネットから誰でもアクセスできる状態。

No.	脆弱性	レベル	検出社数	脆弱性概要
27	CVE-2021-3449 - OpenSSL TLS Denial of Service via crafted renegotiation ClientHello message	medium	2	OpenSSL 1.1.1 系に存在する TLS の脆弱性で、攻撃者が細工した「再ネゴシエーション用 ClientHello」を送ることで、サーバ側の OpenSSL が NULL ポインタ参照によりクラッシュし、サービス停止を引き起こす
28	PostgreSQL Service found	medium	1	PostgreSQL の外部公開
29	Directory Listing	medium	1	ディレクトリ内のファイル一覧がブラウザに表示され第三者から閲覧可能になる。
30	Missing Content-Security-Policy Header	low	125	Content-Security-Policy ヘッダーの未設定
31	Missing Referrer-Policy Header	low	123	Referrer-Policy ヘッダーの未設定
32	Missing X-Content-Type-Options Header	low	122	X-Content-Type-Options ヘッダーの未設定
33	Missing Strict-Transport-Security Header	low	121	Strict-Transport-Security ヘッダーの未設定
34	Missing X-Frame-Options Header	low	119	X-Frame-Options ヘッダーの未設定
35	SPF Policy Is Too Broad	low	102	SPF ポリシーが緩い設定になっている
36	Certificate Mismatch	low	100	アクセスしているホスト名と、サーバが返す SSL/TLS 証明書に記載されたコモンネーム(CN)が一致していない状態。
37	DMARC Record Missing	low	55	DMARC Record の未設定
38	HTTP Cookie Max-Age or Expires attribute Missing	low	53	Cookie の Max-Age 属性未設定
39	HTTP Cookie without HTTPOnly flag	low	38	Cookie の HTTPOnly 属性未設定
40	HTTP Cookie without Secure flag	low	29	Cookie の Secure 属性未設定
41	HTTP Cookie SameSite attribute configured with None setting	low	13	Cookie の SameSite 属性が「None」に設定されている
42	SPF Policy Approves Too Many IPv4 Hosts	low	9	SPF ポリシーが多数の IPv4 ホストを承認

No.	脆弱性	レベル	検出社数	脆弱性概要
43	Amazon Web Services (AWS) Access Key ID Exposed	low	5	AWS の Access Key ID / Secret Access Key が公開 Web サイなどに誤って公開されてしまった状態
44	SMTP Sender Policy Framework (SPF) Missing	low	2	SMTP Sender Policy Framework (SPF)の未設定
45	Referrer-Policy Header with insecure value	low	1	Referrer Policy ヘッダーが緩い値になっている

4. 参加事業者に対する調査と分析

4.1. アンケート調査の実施概要

本事業においては、参加事業者への ASM 診断結果の報告にとどまらず、アンケートおよびヒアリングを通じて参加事業者におけるセキュリティ対策の意識の変化や実際の対応行動、対策実施にあたっての課題や工夫などの情報を多角的に把握し、整理・可視化することにより、本事業の成果の社会的波及効果を最大化することを目指した。

参加事業者に対するアンケートの案内および回答の依頼はメールにて行い、未回答の参加事業者へは架電による回答依頼も行った。アンケートの回答は Web 上で行う仕様（Forms を使用）とし、依頼メールにはアンケート Web へアクセスするリンクを添付した。アンケート設計においては、参加事業者の回答負担を最小限に抑えることを重視し、以下の点に留意して実施をし、全参加事業者 126 社から回答を得た。

- 記述式設問は最小限とし、選択肢を中心とした簡易な構成とする
- 回答所要時間（5～10 分程度）を明記し、心理的負担感を軽減する
- アンケート依頼時において、診断結果との関連性や参加の意義を簡潔に伝える説明を実施する
- リマインドとサポート体制を整え、円滑な回答回収を促進する
- 回答締め切り前に、リマインドメールを送付し、必要に応じて個別フォローを実施する
- 回答方法や内容に関する不明点に対応するため、専用の問い合わせ窓口を設置する

実施したアンケート項目は下表のとおり。

表 7 アンケート調査項目

No.	設問	選択肢
1	ASM 診断される前の状況をお伺いします。 貴社で実施している「組織的な」セキュリティ対策内容を教えてください。(複数選択可)	☐ セキュリティーポリシー・規程等の策定 ☐ セキュリティ教育の実施 ☐ セキュリティ対策責任者の設置 ☐ インシデント対応計画の策定 ☐ 外部委託先やサプライチェーンの管理 ☐ その他(記述)
2	ASM 診断される前の状況をお伺いします。 貴社で実施している「技術的な」セキュリティ対策内容を教えてください。(複数選択可)	☐ OS・アプリケーションの更新 ☐ ウイルス対策ソフト導入 ☐ EDR の導入 ☐ ログの収集・監視 ☐ 異常通信検知 ☐ ファイアウォール・境界線防御 ☐ アクセス制御・権限管理 ☐ ワンタイムパスワード、IC カード、USB キー、生体認証などによる個人認証 ☐ ウェブ閲覧のフィルタリングソフト ☐ メールフィルタリングソフト(誤送信防止対策製品、スパムメール対策製品含む) ☐ 暗号化製品(ディスク、ファイル、メールなどの通信/データの暗号化) ☐ バックアップの整備 ☐ ソフトウェアライセンス管理・IT 資産管理製品 ☐ IT 資産台帳の作成・洗い出し・分類・ラベル分け ☐ 脆弱性診断 ☐ 脆弱性管理(システムやプログラムのセキュリティ上の弱点を直すこと) ☐ サイバーセキュリティお助け隊サービスの導入 ☐ その他(記述)

No.	設問	選択肢
3	ASM 診断される前の状況をお伺いします。 組織としてサイバーセキュリティを担う担当部署もしくは担当者を教えてください。（単一選択）	☐ 経営者 ☐ 情報システム部または担当者（専任） ☐ 情報システム部または担当者（他の業務と兼任） ☐ 総務部または担当者 ☐ システム・端末の保有部署の責任者 ☐ 担当部署または担当者はいない ☐ 外部業者に委託 ☐ その他（ 記述 ）
4	ASM 診断される前の状況をお伺いします。 サイバーセキュリティを実施する上での問題は何ですか？（複数選択可）	☐ 専門人材不在 ☐ 教育不足（人材はいるが脆弱性管理の知識がない） ☐ 経営層関与が薄い ☐ 責任体制不明確 ☐ コスト負担 ☐ 費用対効果が不明 ☐ ツールが扱えない ☐ セキュリティ更新（脆弱性修正）プログラム適用管理の手間 ☐ 対象範囲の特定ができない ☐ 優先度が低い ☐ 時間が取れない ☐ 依頼/委託できる業者がいない ☐ その他（ 記述 ）
5	ASM 診断される前の状況をお伺いします。 取引先や関係会社等から脆弱性管理（システムやプログラムのセキュリティ上の弱点を直すこと）の実施を求められたことはありますか？（単一選択）	☐ はい ☐ いいえ ☐ わからない

No.	設問	選択肢
6	ASM 診断される前の状況をお伺いします。 過去にサイバーセキュリティインシデントおよび内部不正（情報漏えい、ウイルス感染等、またその疑いも含む）の経験はありますか？（単一選択）	☐ 過去に経験したことはない ☐ 過去 1 年以内に経験した ☐ 過去 3 年以内に経験した ☐ 過去 5 年以内に経験した ☐ それ以前に経験した
7	前設問で過去にサイバーセキュリティインシデントおよび内部不正の経験があると回答された事業者様にお伺いします。その内容について教えてください。（複数選択可）	☐ 情報漏えい ☐ 不正アクセス ☐ ウェブサイト改ざん ☐ 標的型攻撃 ☐ マルウェア/ウイルス感染 ☐ ランサムウェア感染 ☐ DoS/DDoS 攻撃 ☐ 内部者/委託先による不正持ち出し ☐ その他（　記述　）
8	ASM 診断される前の状況をお伺いします。経営層のサイバーセキュリティへの関心度はどの程度ですか？（単一選択）	☐ 高い ☐ どちらかといえば高い ☐ どちらともいえない ☐ どちらかといえば低い ☐ 低い
9	ASM 診断で、現在使用していない IT 資産もしくは、管理者（会社）が把握していなかった IT 資産は見つかりましたか？（単一選択）	☐ はい ☐ いいえ ☐ わからない

No.	設問	選択肢
10	ASM 診断結果を受けて、「検出されたセキュリティ上の問題の内容」や、「対応すべき優先順位」、「対策の必要性」などについての理解度をお答えください。(単一選択)	☐ 理解できた ☐ どちらかといえば理解できた ☐ どちらともいえない ☐ どちらかといえば理解できなかった ☐ 理解できなかった
11	ASM 診断結果を受けて、検出されたセキュリティ上の問題の対応(修正・改善・対策)を実施しましたか？(単一選択)	☐ はい(1 つ以上実施済) ☐ いいえ(今後実施予定あり) ☐ いいえ(実施の予定なし)
12	前設問で「はい(1 つ以上実施済)」、「いいえ(今後実施予定あり)」と回答された事業者様にお伺いします。具体的にどのような対策を実施または実施予定ですか？(複数選択可)	☐ OS・アプリケーションの更新(脆弱性修正プログラム適用含む) ☐ アクセス制御・権限管理 ☐ 多要素認証の導入 ☐ 強度の強いパスワードへの変更 ☐ 通信/データの暗号化 ☐ 利用していないサービスの無効化・利用停止 ☐ セキュリティ対策ツールもしくはサービスの導入 ☐ その他（ 記述 ）

No.	設問	選択肢
13	前設問で「いいえ（実施の予定なし）」と回答された事業者様にお伺いします。対策を検討・実施する上での問題を教えてください。（複数選択可）	☐ 専門人材不在 ☐ 教育不足（人材はいるが脆弱性管理の知識がない） ☐ 経営層関与が薄い ☐ 責任体制不明確 ☐ コスト負担 ☐ 費用対効果が不明 ☐ ツールが扱えない ☐ セキュリティ更新（脆弱性修正）プログラム適用管理の手間 ☐ 対象範囲の特定ができない ☐ 優先度が低い ☐ 時間が取れない ☐ 依頼/委託できる業者がいない ☐ その他（　記述　）
14	ASM 診断を受けて、今後強化したい「組織的な」セキュリティ対策は何ですか？（複数選択可）	☐ セキュリティーポリシー・規程等の策定 ☐ セキュリティ教育の実施 ☐ セキュリティ対策責任者の設置 ☐ インシデント対応計画の策定 ☐ 外部委託先やサプライチェーンの管理 ☐ その他（　記述　）

No.	設問	選択肢
15	ASM 診断を受けて、今後強化したい「技術的な」セキュリティ対策は何ですか？（複数選択可）	□ OS・アプリケーションの更新 □ ウイルス対策ソフト導入 □ EDR の導入 □ ログの収集・監視 □ 異常通信検知 □ ファイアウォール・境界線防御 □ アクセス制御・権限管理 □ ワンタイムパスワード、IC カード、USB キー、生体認証などによる個人認証 □ ウェブ閲覧のフィルタリングソフト □ メールフィルタリングソフト（誤送信防止対策製品、スパムメール対策製品含む） □ 暗号化製品（ディスク、ファイル、メールなどの通信/データの暗号化） □ バックアップの整備 □ ソフトウェアライセンス管理・IT 資産管理製品 □ IT 資産台帳の作成・洗い出し・分類・ラベル分け □ 脆弱性診断 □ 脆弱性管理（システムやプログラムのセキュリティ上の弱点を直すこと） □ サイバーセキュリティお助け隊サービスの導入 □ その他（ 記述 ）
16	今後、どのような支援や情報提供があれば、セキュリティ対策が進むと思いますか？（複数選択可）	□ セキュリティーポリシーの策定手順書・マニュアルの提供 □ インシデント対応計画の策定手順書・マニュアルの提供 □ サイバーセキュリティ対策のわかりやすい事例集 □ サイバーセキュリティツールの選定・導入支援ガイド □ サイバーセキュリティの周知啓発資料の提供 □ セキュリティ対策製品・サービス導入にかかる金銭的支援 □ 社員向けサイバーセキュリティ教育コンテンツの提供 □ IT 資産台帳の作成手順書・マニュアルの提供 □ 最新の脆弱性情報・注意喚起の定期的な配信 □ テスト環境の管理・閉鎖方法に関するガイドラインの提供 □ 外部ベンダーとの契約に関する手引き書、注意点のまとめ □ セキュリティコンサルティング（専門家によるリスク分析や必要な対策の提案） □ 地元の関係団体等によるサイバーセキュリティの啓発活動 □ その他（ 記述 ）

4.2. アンケート結果の分析

アンケート結果を横断的に分析すると次のようなことが言える。
【ポジティブな回答の共通点】
① インシデント経験がある企業ほど、ASM 結果を具体的な行動に落とし込んでいる
ランサムウェア・Web 改ざん・不正アクセス経験企業は、パッチ適用、多要素認証、不要サービス停止など、実務的な対策を実行・計画している。
② 「不要サービスの無効化」「サブドメイン廃止」など、攻撃面縮小に踏み込む企業が一定数存在する
ASM(外部から見える資産診断)の目的に合致した、理想的な活用の仕方を試行している。
③ 支援ニーズは高度化している企業ほど具体的
「ベンダー契約の手引き」「テスト環境閉鎖ガイド」「経営層向け危機情報」など、単なるセキュリティ啓発を超えたニーズが出ている。

【課題感のある回答の共通点】
④ ほぼ全体で「専門人材不在」「教育不足」が挙がっている
技術的には EDR やログ監視まで入れている企業でも、ツールを使いこなせない、費用対効果が説明できない、という形でボトルネックになっている。
⑤ 経営層関与が薄い企業では、ASM 結果を「やらない理由」にしがち
「重要な問題は検出されなかったため」「対策必要なし」「優先度が低い」などのコメントがみられる。ASM が安心材料として消費され、改善につながらないリスクがみられる。
⑥ 理解度は「どちらかといえば理解できた」が多いが、それでも実施しない層が目立つ
理解と実行の間にある壁は、「コスト」「時間」「優先度」「対象範囲の特定」であることが、自由記述回答から見て取れる。

アンケート設問ごとに回答結果を以下のとおり示す。なお、アンケート結果の割合の分母は、全てそれぞれの設問における回答企業数である。

（1） 設問１

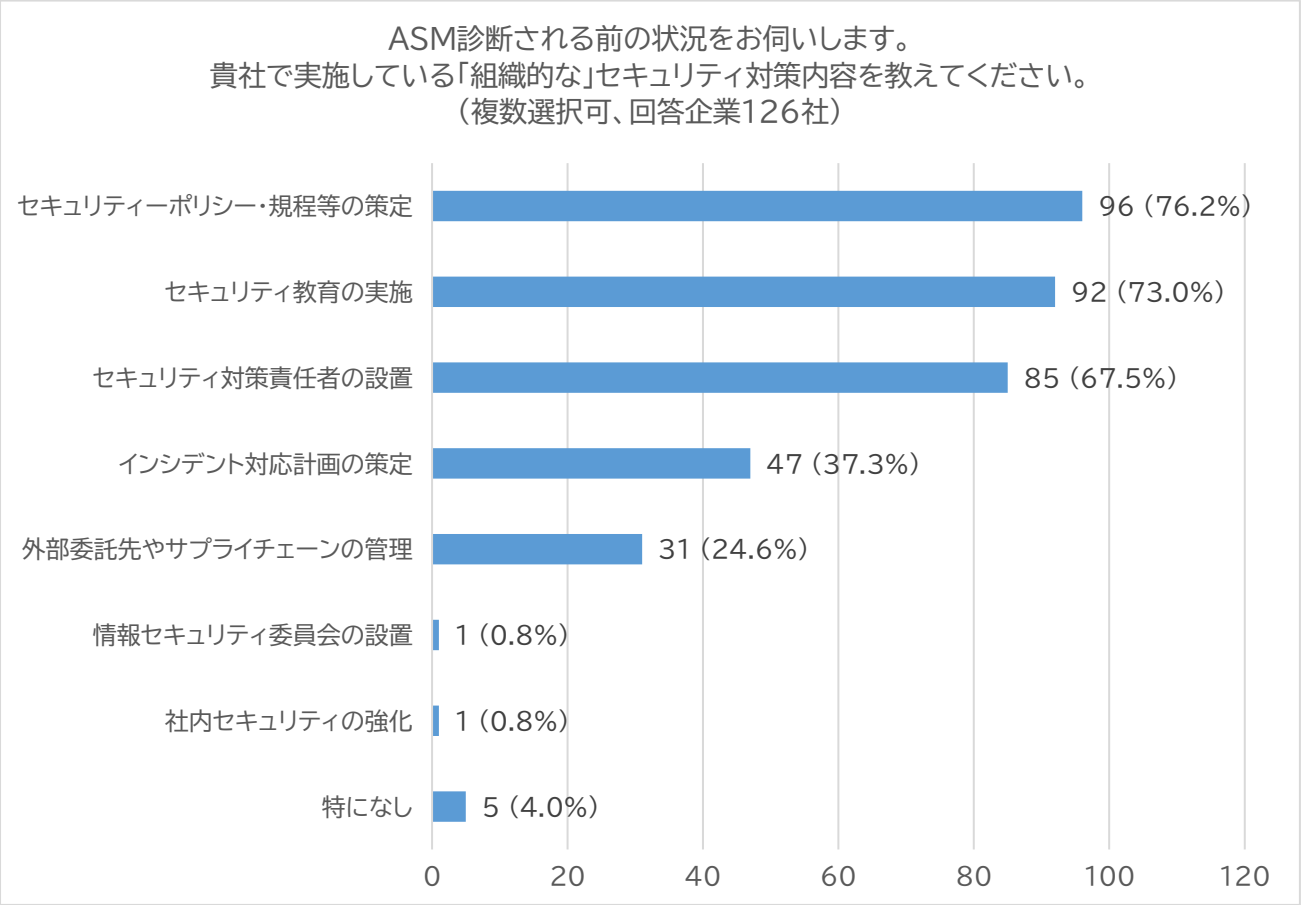

図５ アンケート設問１ 回答結果

（2）設問２

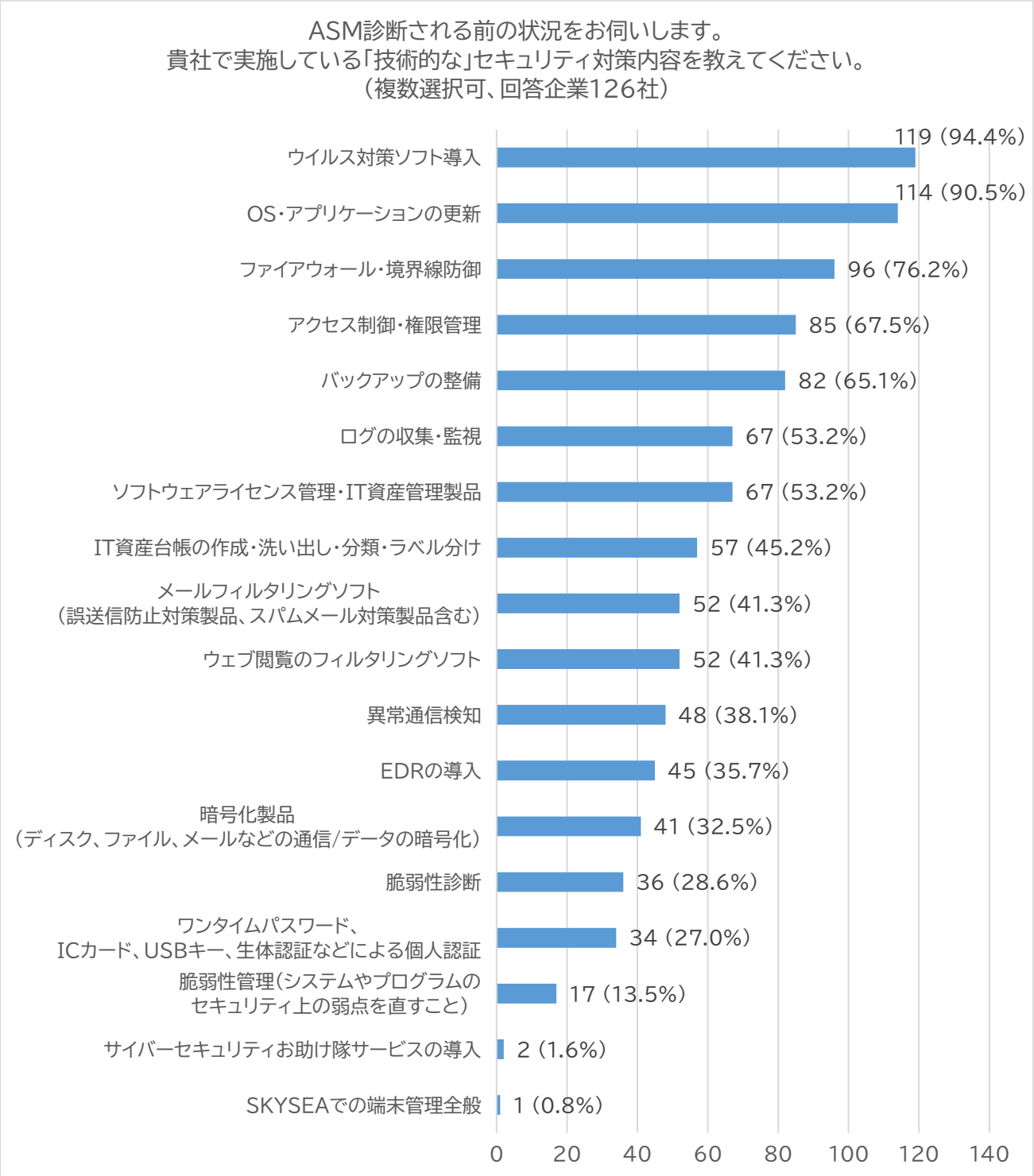

図６　アンケート設問２　回答結果

（3）設問３

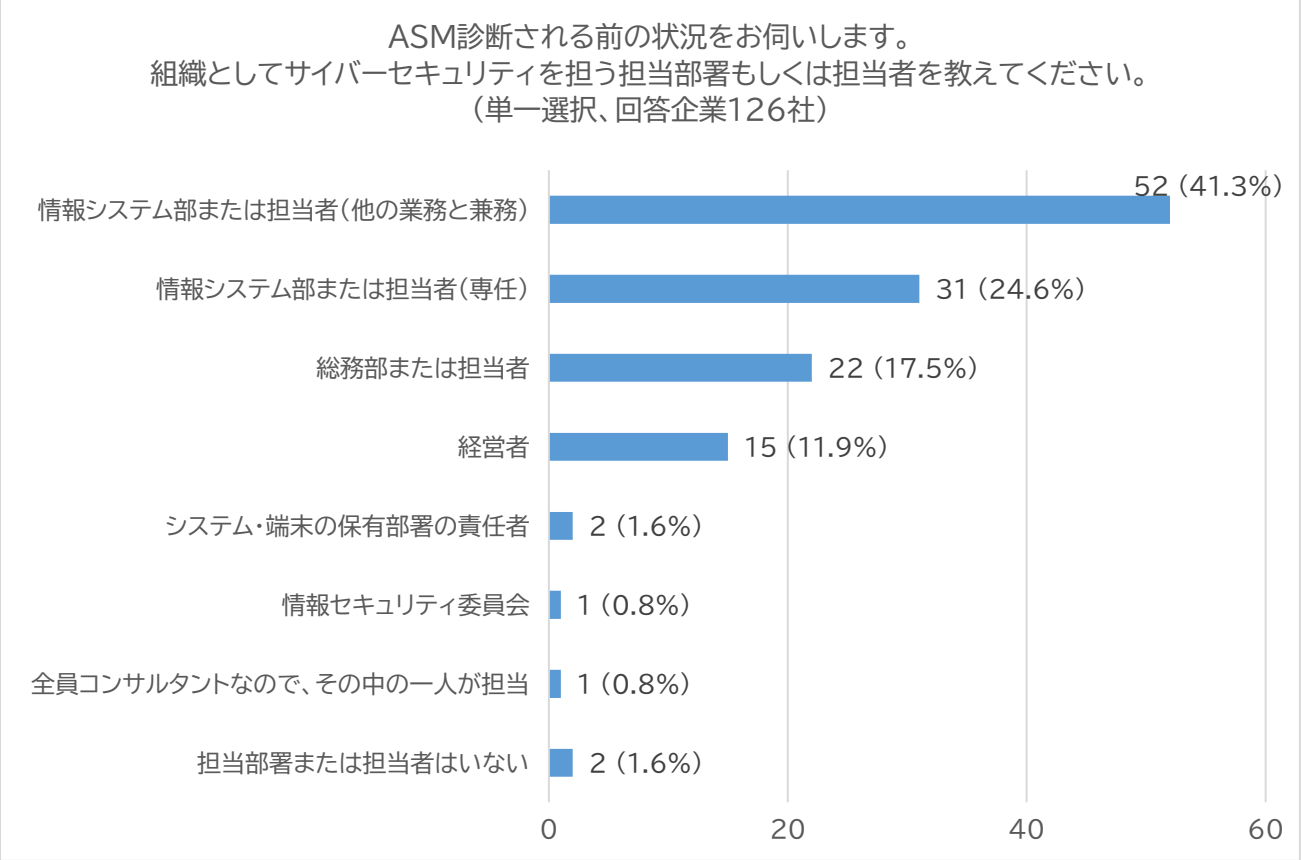

図７ アンケート設問３ 回答結果

（4）設問４

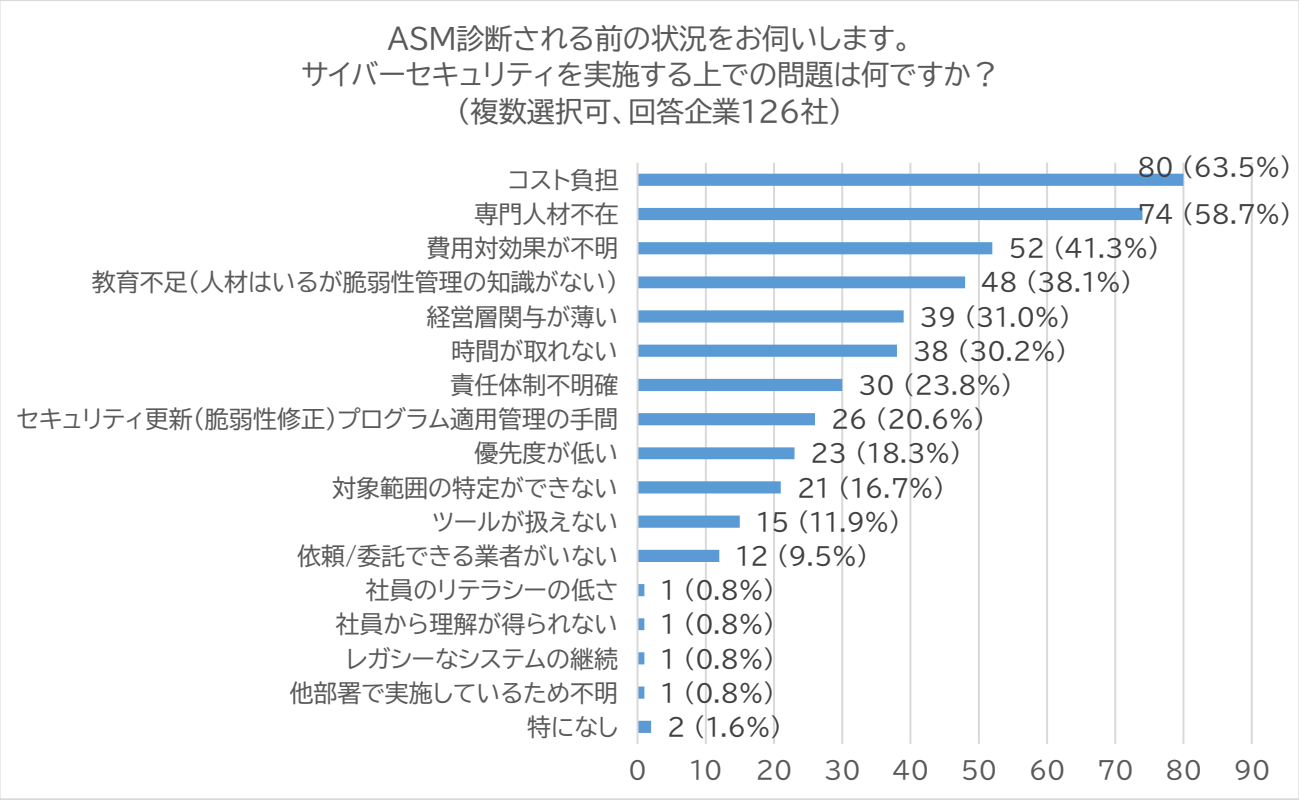

図８　アンケート設問４　回答結果

（5）設問５

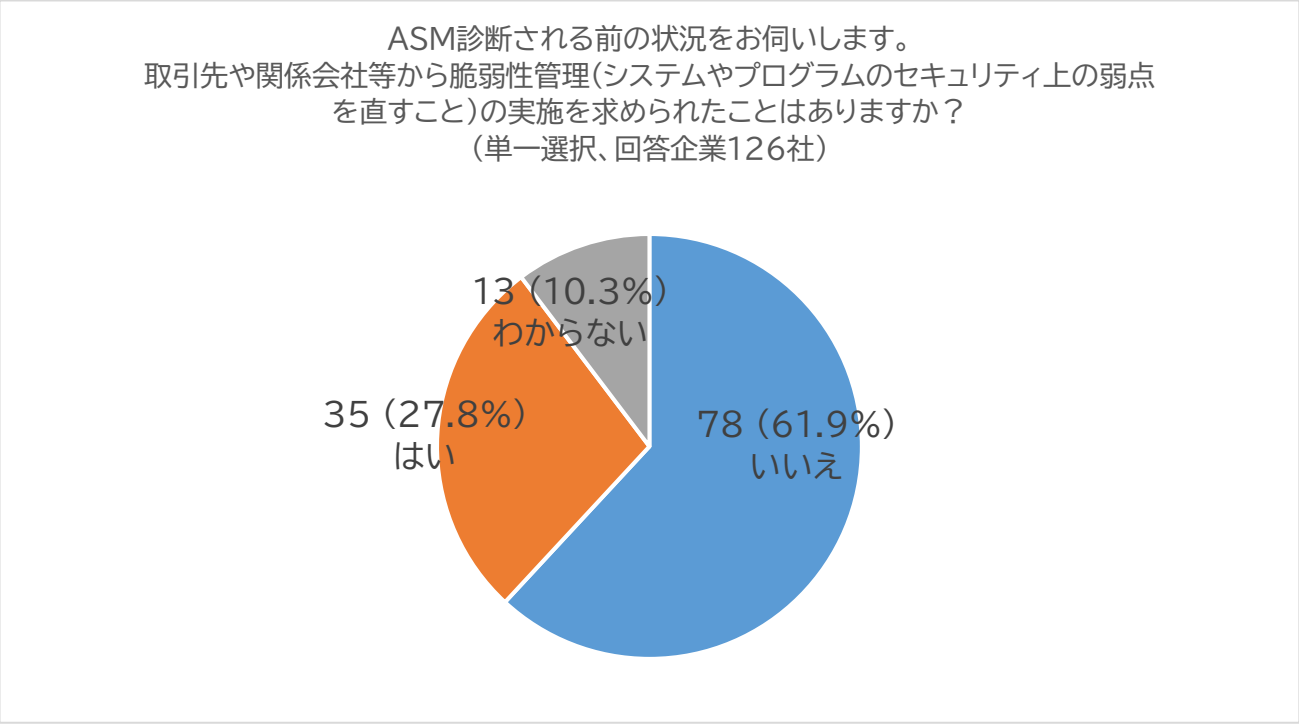

図９　アンケート設問５　回答結果

（6）設問 6

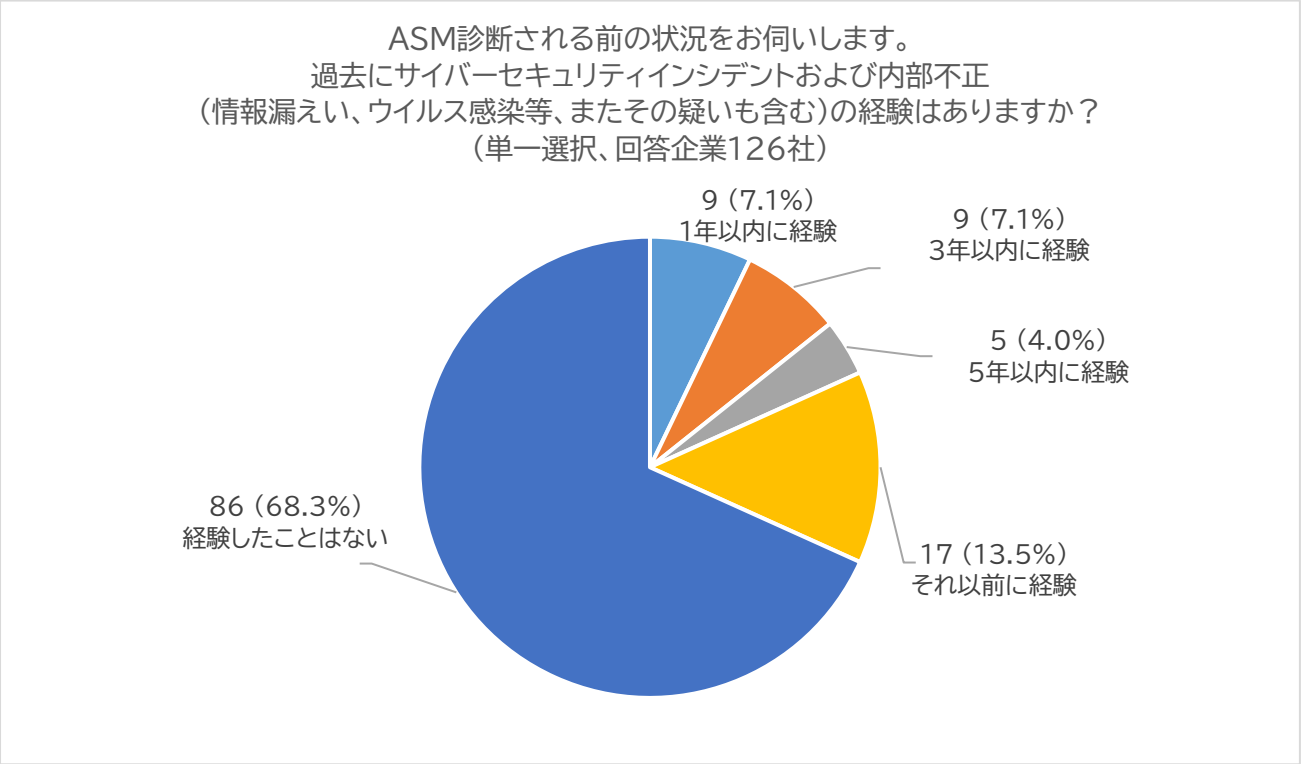

図 10　アンケート設問 6　回答結果

（7）設問 7

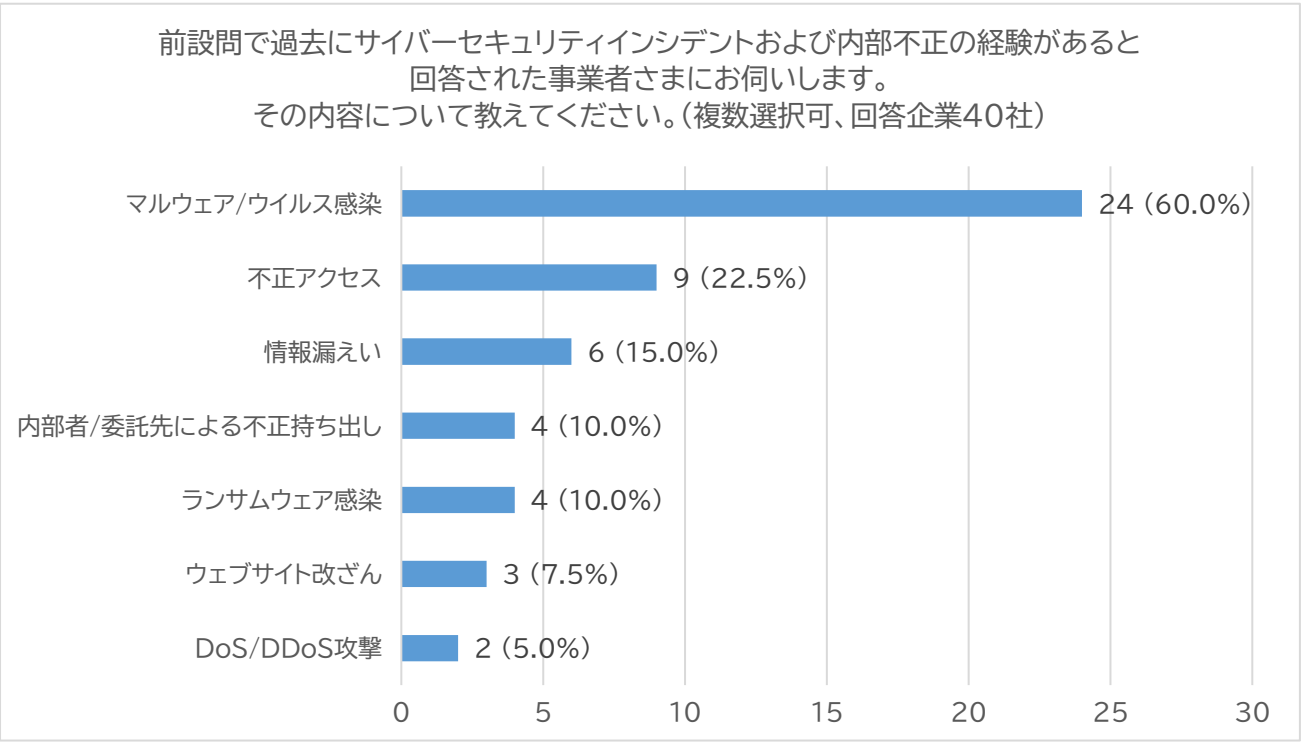

図 11　アンケート設問 7　回答結果

（8）設問 8

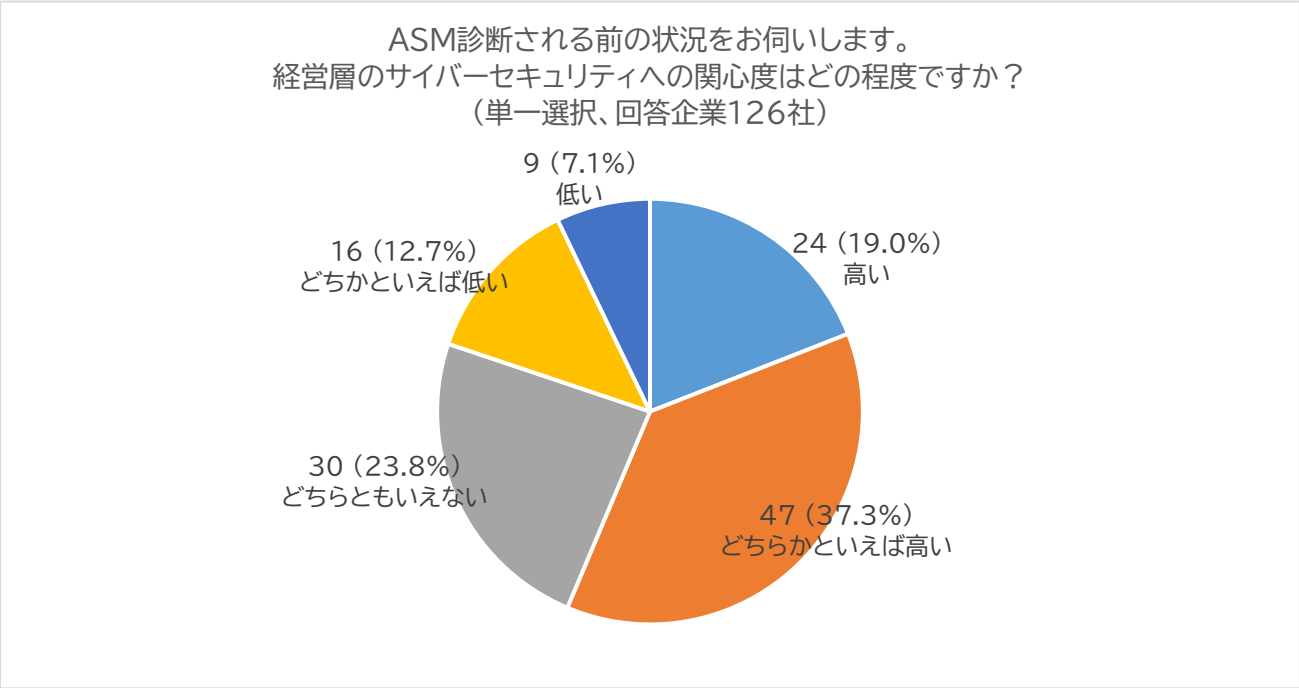

図 12　アンケート設問 8　回答結果

（9）設問 9

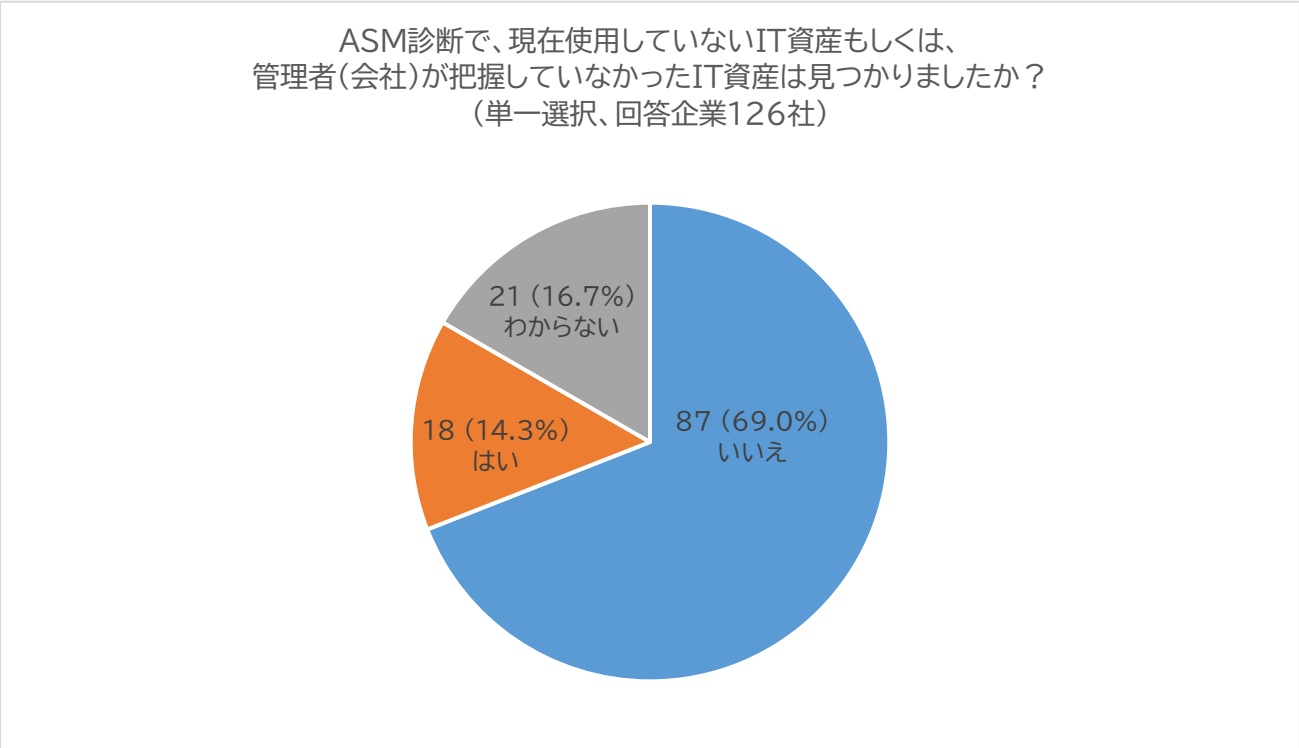

図 13　アンケート設問 9　回答結果

（10）設問 10

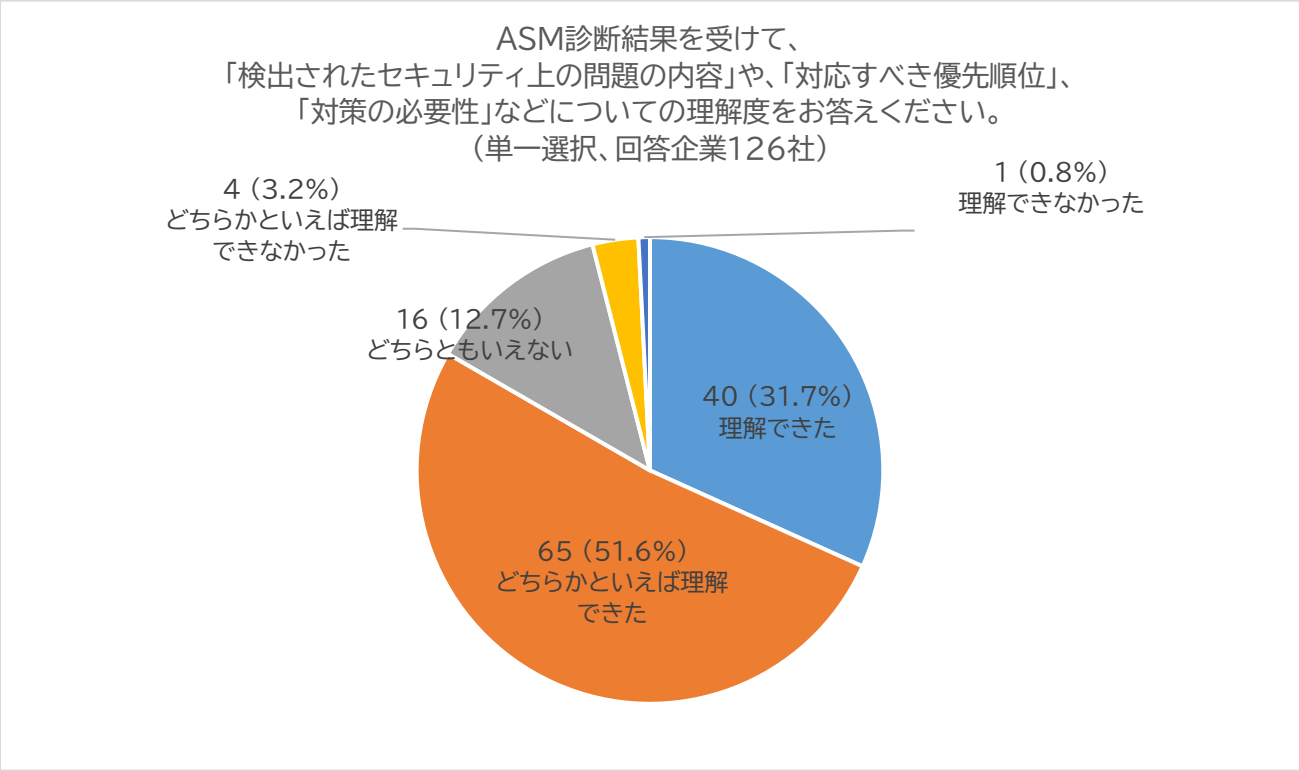

図 14　アンケート設問 10　回答結果

（11）設問 11

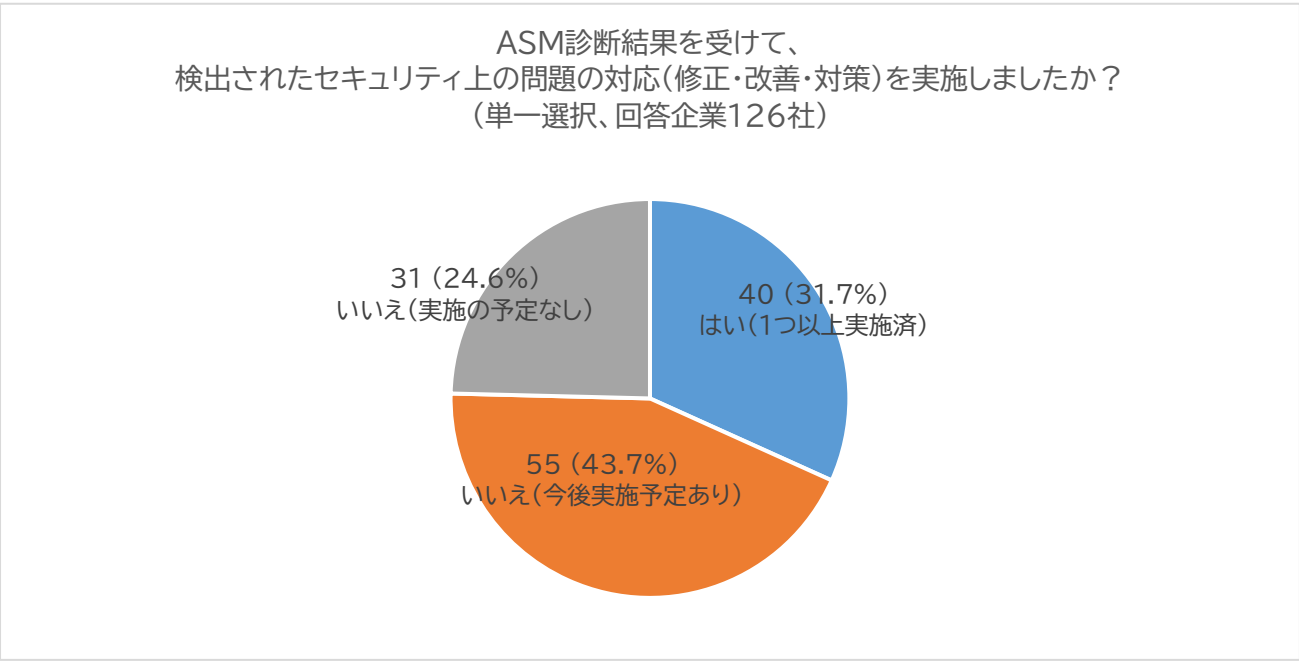

図 15　アンケート設問 11　回答結果

（12）設問 12

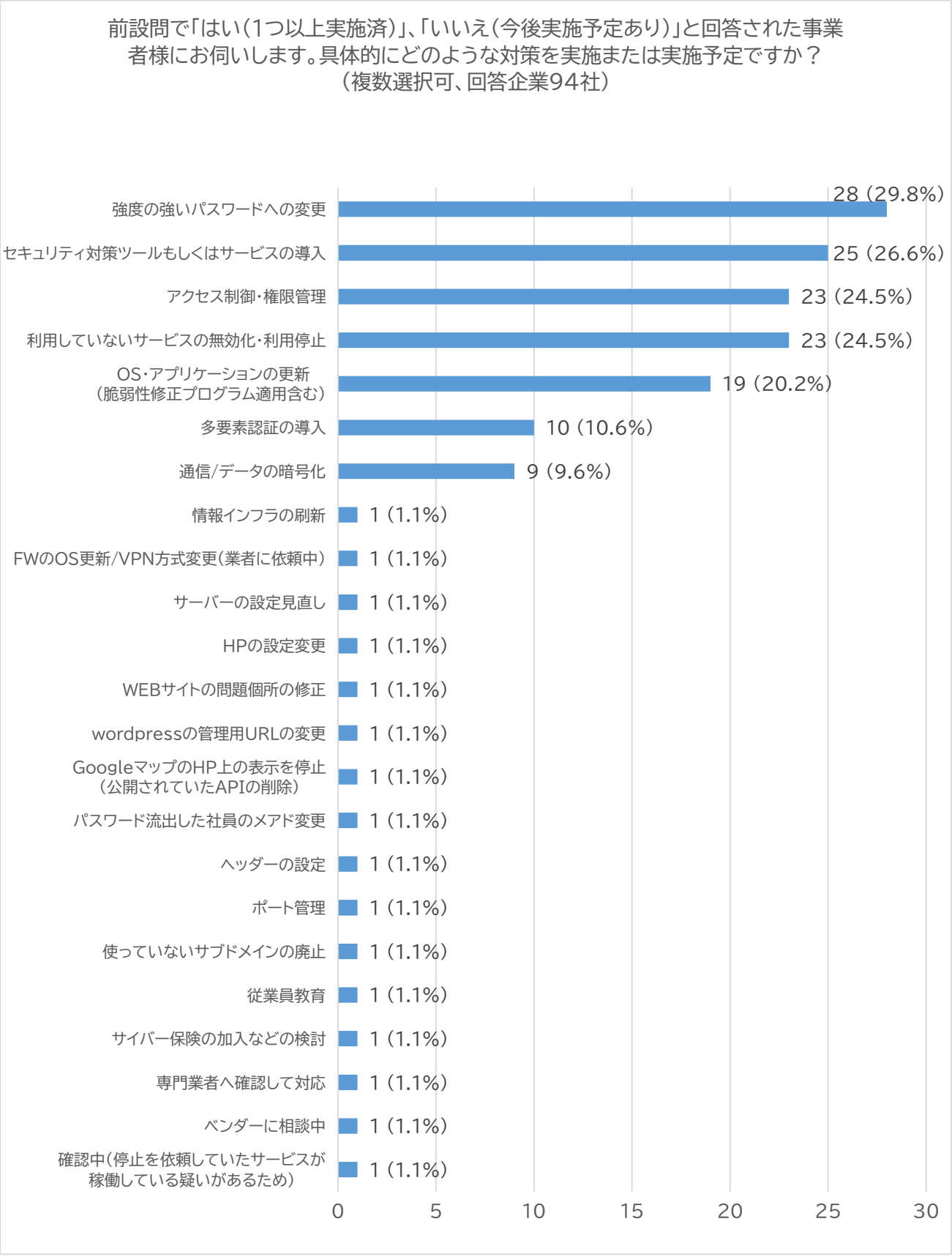

図 16　アンケート設問 12　回答結果

（13）設問 13

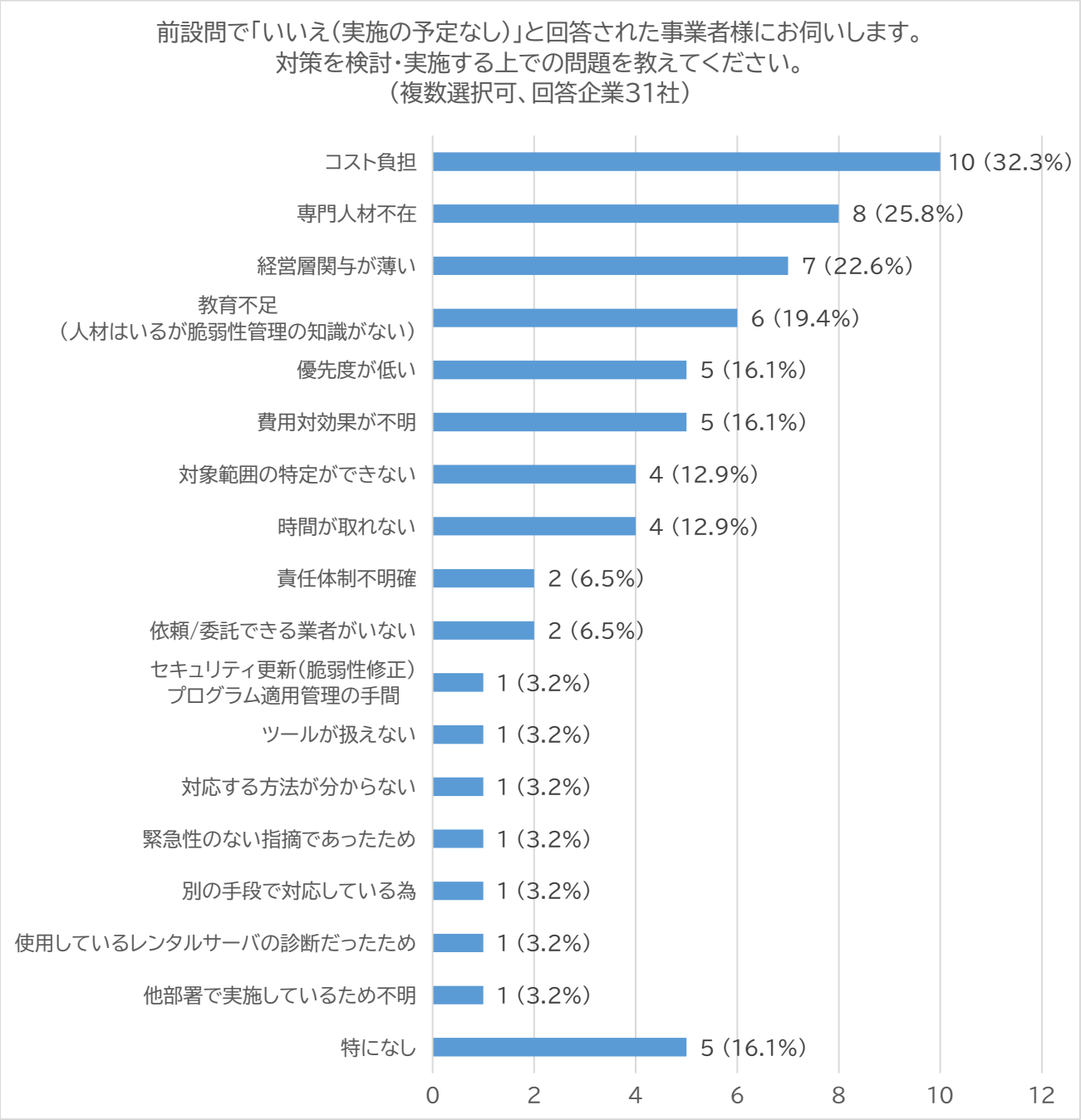

図 17　アンケート設問 13　回答結果

（14）設問 14

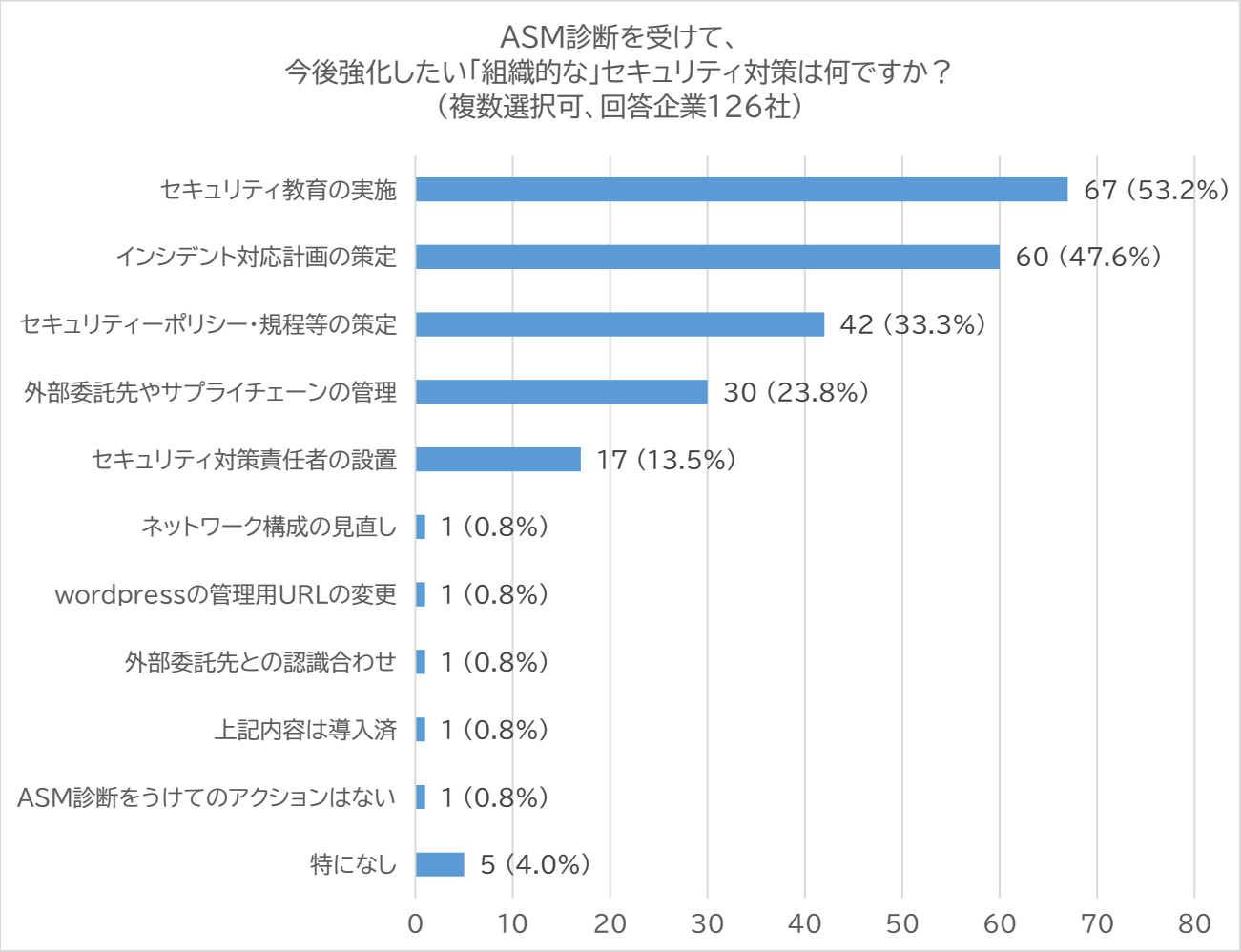

図 18　アンケート設問 14　回答結果

（15）設問 15

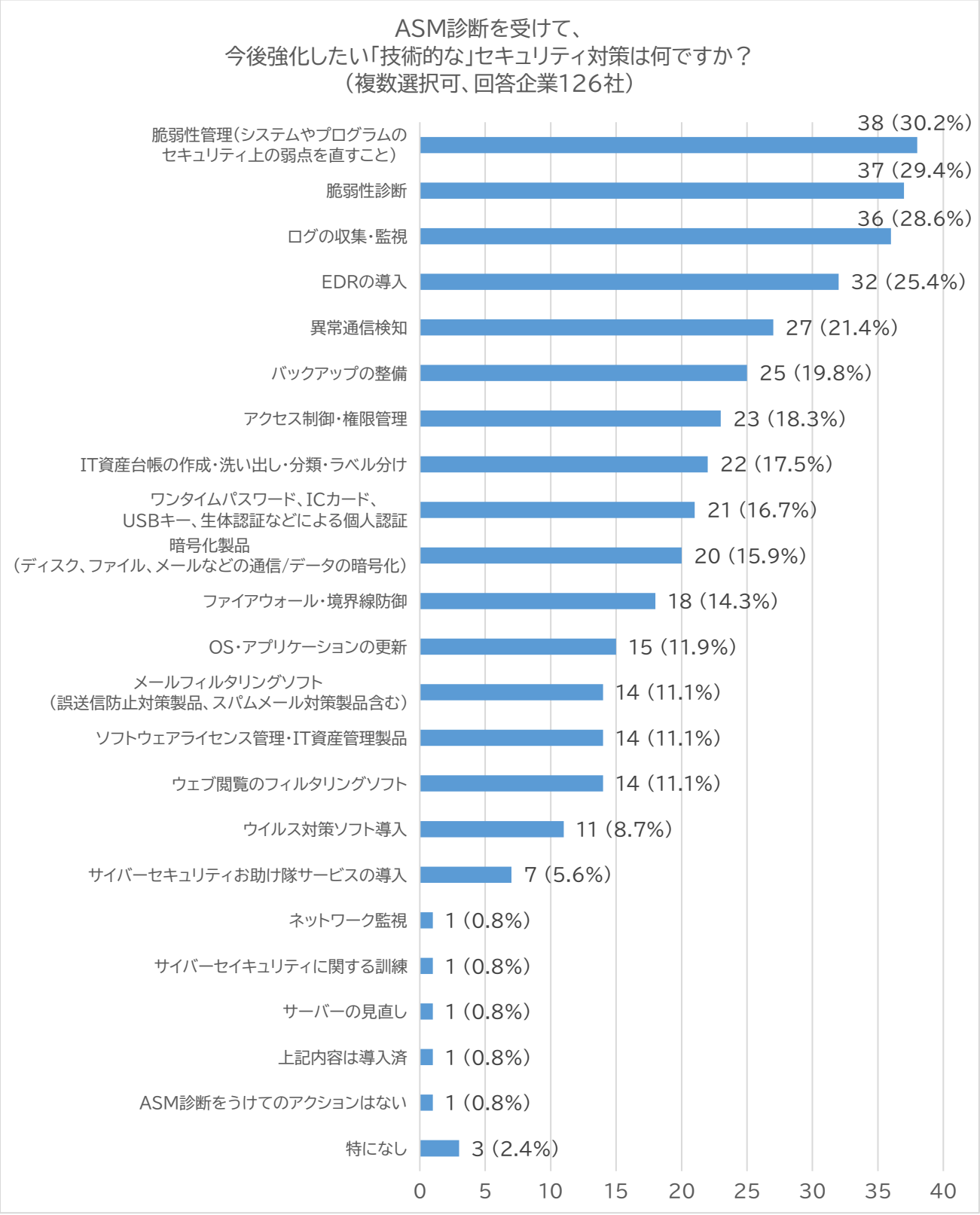

図 19　アンケート設問 15　回答結果

（16）設問 16

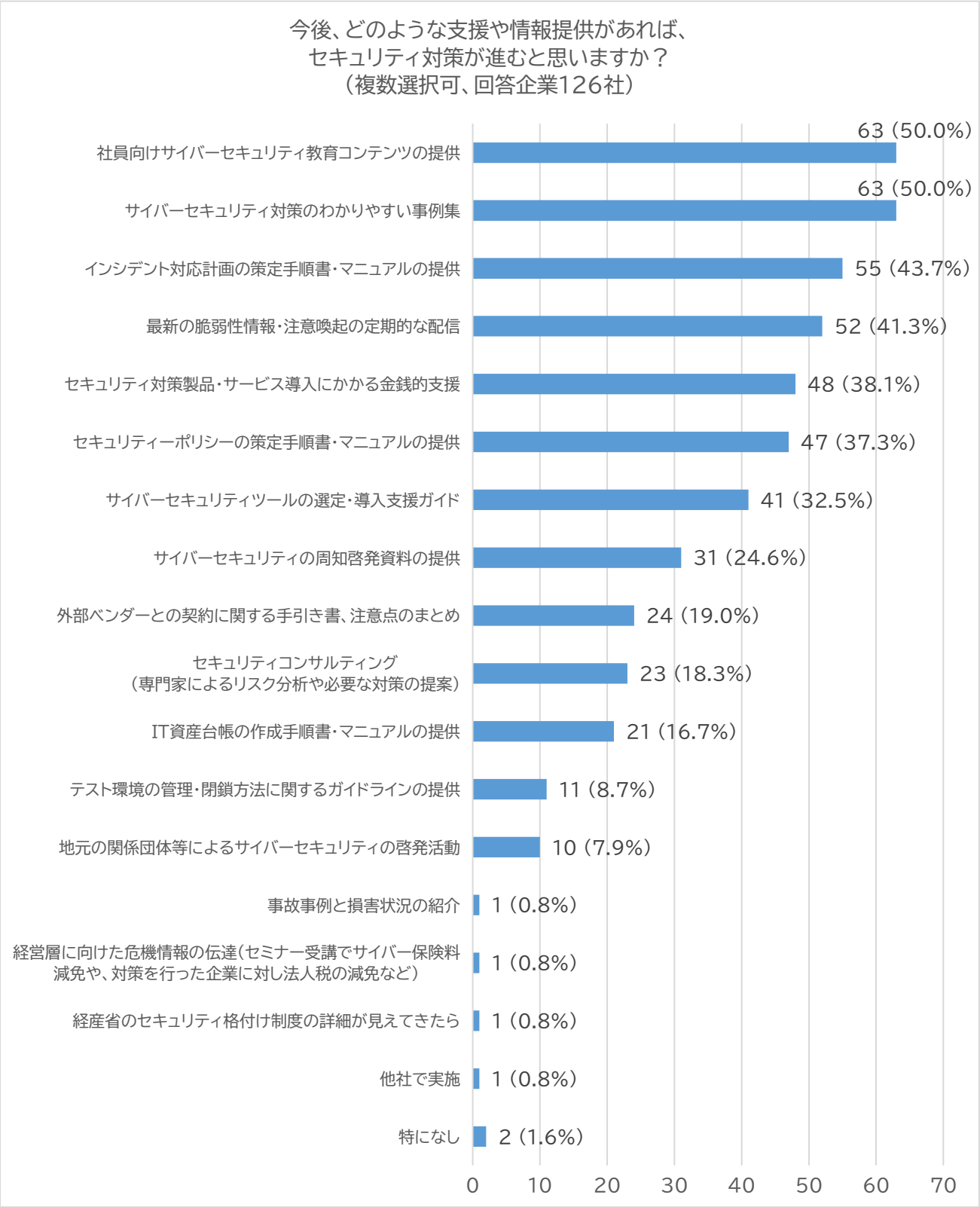

図 20　アンケート設問 16　回答結果

4.3. ヒアリング調査の実施概要

ヒアリング対象企業は、参加企業のうち、アンケート回答状況・ASM 診断のスコア・脆弱性改善取り組みの有無・業種・規模・過去のインシデント経験有無・経営層の関心度・取引先から取組要請有無、などの属性を踏まえ、偏りがないように 10 社に対して調査を行った。

表 8 ヒアリング調査 対象先

属性			アンケート結果(抜粋)							ASM 診断	
企業	業種	規模	担当者 ※1	取引先からの要請	過去インシデント	インシデント内容 ※2	経営層の関心度 ※3	未把握資産有	脆弱性対応	脆弱性検出	改善先
A社	製造業	③~100 名	①	●	●	①	①	●	●	●	
B社	製造業	①20 名未満	③		●	②	②		●	●	●
C社	金融・保険業	非公開	②				③		●	●	
D社	製造業	③~100 名	③		●	③	②		●	●	●
E社	医療・福祉業	③~100 名	①		●	①	②		●		
F社	医療・福祉業	③~100 名	②		●	①	②		●		
G社	金融・保険業	②~50 名	③				②		●	●	
H社	情報通信業	④~300 名	③	●			①		●	●	●
I社	製造業	②~50 名	①				②		●	●	
J社	製造業	②~50 名	③				③	●	●	●	

※1 ①経営者、②情報システム部または担当者(専任)、③情報システム部または担当者(他の業務と兼務)

※2 ①マルウェア/ウイルス感染、②情報漏えい、③不正アクセス、ウェブサイト改ざん

※3 ①高い、②どちらかと言えば高い、③どちらかと言えば低い、④低い

ヒアリング調査では主に次の 2 点を軸に関連する項目について確認をした。

① 今回の ASM 診断で新たに判明した脆弱性への対応

② これまで実施してきた/これから実施したいサイバーセキュリティ対策

具体的な調査項目の例は以下のとおり。なお、参加企業によって特徴が異なるため、全ての設問を網羅的に同じ粒度感で回答を得られたわけではない。

- サイバーセキュリティ対策を行う際の決裁/意思決定プロセス
- 決裁/意思決定の際にハードルになる点(費用、人手など)はあるか
- 実施した対策の内容、またそのコスト感・人的負荷について
- 費用や工数を抑える上で工夫した点、課題
- 過去のサイバーインシデントの実態について(※サイバーインシデントの経験がある場合のみ)

- インシデント発生時の状況（インシデント内容、発生時期、気づいたきっかけ）
- 被害範囲、被害額 、インシデントの原因
- インシデント後、技術面・運用面でどのような改善を行ったか
- サイバー保険への加入有無
- 他企業に対して伝えたい経験・ノウハウ・Tips について
- 過去・今回の取り組みの中で「効果が高かった」「やってよかった」と感じた施策
- これから対策を始める企業に対して、最初の一歩として何を勧めるか
- 取り組む際の注意点、アドバイス

4.4. **ヒアリング結果の分析**

ヒアリング結果を横断的に分析すると次のようなことが言える。
【ポジティブな回答の共通点】
① 経営層に IT・セキュリティ経験者・理解者がいる企業は、セキュリティ投資が進みやすい
② クラウド活用＋ローカルデータ削減を意識している企業が多い
・クラウドの活用によりセキュリティ強化と保有データの削減を両輪で実現
③ 生成 AI を使って資料作成やレポート解釈を効率化している事例が出てきている
・ASM レポートの解説を作成させる
・サイバーセキュリティ教育資料の生成
※ただし、生成 AI の活用は効率化の反面、思わぬ情報漏えいや契約違反につながる可能性もあるため注意が必要である。

【課題感のある回答の共通点】
④ 「どこまでやれば十分か」の基準がない
⑤ 取引先からのチェックシート・要請がバラバラで過剰
・規模や実態にそぐわない項目が多い
・フォーマットがバラバラで負担大
⑥ 経営層の意識を変える情報が不足

ヒアリング結果については、事例集にて詳しく解説をしているので、そちらを参照されたい。
以下は個社のヒアリング結果をまとめたものである。

（1） A社

属性			アンケート結果（抜粋）							ASM 診断	
企業	業種	規模	担当者	取引先からの要請	過去インシデント	インシデント内容	経営層の関心度	未把握資産有	脆弱性対応	脆弱性検出	改善先
A社	製造業	③~100 名	①	●	●	①	①	●	●	●	

（1） サイバーセキュリティ対策実施の決裁/意思決定プロセスについて	
① 自組織の体制・意思決定プロセス等	サイバーセキュリティ・DX 推進は経営者自身で行っている。 中小企業では費用対効果の実感がわかないという声もあるが、当社では経営者自ら理解・推進している。もともとエンジニアで情報系は専門ではなかったが、前職でソフト部門に配属されたことをきっかけに C 言語を学習し、現在の会社に戻った後は中小企業特有の超アナログ状態であることに危機感を覚え、大手企業が当たり前に行っている IT 化を一つずつ進めてきた。
② 取引先関連	取引先の方が古いルール（PPAP など）を求めてくることが多い。大企業のセキュリティルールが更新されていないため、やむなく対応している部分もある。
（2） セキュリティ対策のコスト・工数について	
① 実施した対策、コスト感、人的負荷等について	オンプレミス管理の負担と属人化からの脱却を目指し、Microsoft365 の導入を皮切りに、オンプレミスからクラウドへ移行を進めていった。クラウド化・UTM の導入等は「これが足りないな」と感じる度に順次導入し、クラウド側への攻撃やランサムウェアの対策として、サードパーティのバックアップツールの活用や、従業員のログ取得も実施している。最近では Salesforce を導入し、営業 DX やデジタルツイン実現のために活用している。 費用はクラウド（Azure 等）が約 3 万円/月、UTM はレンタルしており、すべてのサービスを合算しても年間 300 万円ほどに収まっている。経常利益の 5%を情報セキュリティにかけても良いという話もあるが、経常利益率も伸びており、実際は 5%もかかっておらず、得られるメリットの方が大きいと感じている
② 工夫した点もしくは課題	段階的な導入を進めていった。セキュリティに関しては必要経費と捉えているが、経常利益率は同業他社対比で高く推移できている。 セキュリティ費用を必要経費と捉えていない中小企業も多いが、トヨタのような大企業でも取引先のセキュリティ不備からウイルス感染が発生し、サプライチェーンが止まる事態があったが、サプライチェーン全体のセキュリティ担保は難しい。一方でセキュリティ投資ができている会社と仕事をしたいという流れがあるため、セキュリティにお金をかけることは営業材料にもなりうると思料する。攻めながら守る（攻めの DX と守りのDX）ことで利益率向上、属人化脱却・採用力強化につながる。
（3） 今回発見された脆弱性について	

	クラウドへの移行時にバックアップ用の SQL データベースを止め忘れていた。また、Google の API キーも新しく取り直していたが、更新を忘れていた。HP の更新なども自身で行っているため、今回見つかった部分は自身で修正対応を行った。また診断結果レポートは ChatGPT や Copilot に投入して内容を読み取り、効率的に対応できた。
（4） 過去のサイバーインシデントの実態について	
① インシデント発生時の状況	先代社長の PC がメール経由でウイルス感染をした。一方で当該 PC はスタンドアローン状態だったので OS が起動しなくなる（当該 PC が使えなくなる）程度で済み、お客さまや社内への被害はなかった。
② 被害額の程度	PC1 台分（30 万円未満）。これをきっかけに Microsoft365 を導入した。（200 万円ほど）
③ サイバー保険加入有無	未加入である。保険よりもサイバーセキュリティ対策に投資した方が良いと思料。
④ その他	アンケートでは今後導入したい対策・ツールとして EDR を上げたが、未導入となっている理由は、優先順位の問題である。
(5)学び・再現可能な Tips	
① これから対策を始める企業へのアドバイス	中小企業は先行投資の余裕がなく、セキュリティや DX 推進が後回しになっていることが多いが、人手不足の世の中でそれらを推進していかないと、企業としての利益も生まれないと考える。 ベンダー任せではなく、自分たちの DX としてできることからやっていくことが大事。
（6） その他	
① アンケートで「相談できる人がいない」とありましたが、なぜそのように感じますか？	IT も OT（Operational Technology）両方に強い業者が少なく誰に相談したら良いかわからない。DX・セキュリティのコンサル会社・サービスは多いが、費用対効果や前提条件が分かりづらいと感じている。

（2） B社

属性			アンケート結果（抜粋）							ASM 診断	
企業	業種	規模	担当者	取引先からの要請	過去インシデント	インシデント内容	経営層の関心度	未把握資産有	脆弱性対応	脆弱性検出	改善先
B社	製造業	①20 名未満	③		●	②	②		●	●	●

（1） サイバーセキュリティ対策実施の決裁/意思決定プロセスについて	
① 自組織の体制・意思決定プロセス等	セキュリティは 2 名で担当している。自身の主業務はシステム開発であり、セキュリティに関する工数は全体の 2 割程度である。本来であれば専門家に外部委託を行い、チェックしていきたい気持ちはある。 ネックとなっているのはコスト面。しかし、セキュリティについて我々自身がしっかりと理解して、経営層だけではなく会社全体にセキュリティ対策の重要性を訴求していく必要は不変と考えている。 セキュリティ対策を意識したきっかけは、大きな出来事があったわけではないものの、営業担当者が無意識に不審メールを開封する事案が散見され、危機感を抱き始めたのがスタートだったと記憶している。
② 取引先関連	過去 2 社からチェックシートの提出を求められたことがある。自組織から取引先に要請したことはない。 チェックシートの提出を求めてきた事業者は自組織にとって、売上比率が高いわけではないものの、長く取引をしており、データのやり取りが発生する先である。
（2） セキュリティ対策のコスト・工数について	
① 実施した対策、コスト感、人的負荷等について	IT システム部から役員会に稟議を上げ、決裁を得るフローとなっている。今回の ASM 診断で見つかった脆弱性の対応も役員会に稟議を上げて承認を得た。費用は約 120 万円だった。普段から付き合いのある業者に依頼したため、相見積もりは取っていない。
② 工夫した点もしくは課題	セキュリティをあまりに強固にすると利便性を損なう部分があり、バランスを取る難しさを感じながら対策を行っているのが現状である。 現状かけている費用は FW で年間約 100 万円（5 年契約 500 万円）、UTM が約 30 万円程であり、年間トータルで 200 万円程になっていると思料。 バックアップについて、重要データはサーバ室に保管しているが、大部分はクラウドに移行させている。 サイバーセキュリティにかける費用の基準として、経常利益率に対して何%という目安は特に設けていない。
（3） 今回発見された脆弱性について	
	IT システム部から役員会に稟議を上げ、決裁を得るフローとなっており、今回の

	ASM 診断で見つかった脆弱性の対応も役員会に稟議を上げて承認を得た。
（4） 過去のサイバーインシデントの実態について	
① インシデント発生時の状況	15 年前に会社で使用を禁止していた Gmail を使っていた端末がウイルス感染をし、情報漏えい事案が発生した。損害賠償には至らなかったものの、対策の必要性を実感した。
② 被害額の程度	不明
③ サイバー保険加入有無	不明
④ その他	
(5)学び・再現可能な Tips	
① これから対策を始める企業へのアドバイス	社員教育が重要と考えている。
（6） その他	
① 社員向けのセキュリティ教育として具体的には何をされていますか？	IPA が作成している動画を年 1、2回視聴してもらう機会を設けている。また、教育だけではなく、違反者にはトップ(社長)からトップダウンで直接指導を行っている。個人従業員のログ監視も行っている。 標的型訓練メールを年 1 回程度営業担当者向けに実施している。データ授受に関してもメールに添付することを原則禁止しており、専用アプリ経由でデータ共有を行うようにしている。 コロナ禍以降、セキュリティ対策が追い付いていない部分があり、認証や端末管理などの強化が今後必要と認識している。
② 経営層へ説明される際に工夫している部分は何ですか？	専門用語をそのまま並べても難しいので、かみ砕いて説明している。例えば IPA が出している動画などを経営層に視聴してもらい、その上で脆弱性が利用された場合の危険性共有を図るようにしている。

（3） C社

属性			アンケート結果(抜粋)							ASM 診断	
企業	業種	規模	担当者	取引先からの要請	過去インシデント	インシデント内容	経営層の関心度	未把握資産有	脆弱性対応	脆弱性検出	改善先
C社	金融・保険業	非公開	②				③		●	●	

（1） サイバーセキュリティ対策実施の決裁/意思決定プロセスについて	
① 自組織の体制・意思決定プロセス等	IT 部の部長として、システム開発・サーバ運用保守・社内 PC 管理等を幅広く担当している。現在の会社に中途入社したが、自身の入社前は IT に詳しい人材が社内にいなかったため、外部ベンダーに PC 管理を依頼していた。また、セキュリティ対策もウイルスソフトを導入している程度で、パスワードの使いまわしやセキュリティの穴など、基本的な問題も多かった。 社外取締役はセキュリティ意識が高く、具体的なツールや対策の提案がある。経営層は社外取締役から指摘・アドバイスがあった場合は前向きに検討するが、それ以外ではあまり関心が高くない。
② 取引先関連	セキュリティに関するチェックシートの記入依頼を受けたことはある。 依頼をしてきたのは大手の IFA 法人である。
（2） セキュリティ対策のコスト・工数について	
① 実施した対策、コスト感、人的負荷等について	ウイルス対策ソフトをノートンからウイルスバスター(ビジネス版)に変更し、LANSCOPE を導入して PC の利用ログを取得するようにしている。業務は Google Workspace(G Suite)を中心に運用しており、共有フォルダやスプレッドシートを活用している。 社用 PC をシンクラ環境にはしていない。
② 工夫した点もしくは課題	自組織システムは API サーバにデータを送る形式になっているため、API のレビューをしっかり行うことや、サーバには侵入検知ソフトを導入し、定期的(毎週)にログをチェックしている。 セキュリティの費用は約 50 万円/年である。 費用対効果が高いと感じたセキュリティ対策を 3 つ挙げるとすれば①Google Workspace(G Suite)活用によるクラウドでのデータ集約・管理、②ウイルスバスター(ビジネス版)導入③LANSCOPE 導入によるログ管理である。
（3） 今回発見された脆弱性について	
	経営層には特に説明していない
（4） 過去のサイバーインシデントの実態について	
① インシデント発生時の状況	なし

② 被害額の程度	なし
③ サイバー保険加入有無	不明
④ その他	
(5)学び・再現可能な Tips	
① これから対策を始める企業へのアドバイス	制限をかける部分は早めに実施したほうが良い。例えばGドライブでデータを共有する際に、URL を知っているだけで閲覧できる状態を禁止したいと考えても、これまで使用していた社員にとってはお客さまへの共有など利便性を損なう側面もあり、運用を変更するのは苦労した。
(6) その他	
① 大規模なランサムウェア事案が発生しているが経営層の意識は変わったか。	報道前後で経営層の意識が変化したとは感じない。
② 今後の要望	セキュリティへの意識は今後も高まってくると考えるものの、現状は情報源が限られている印象を受けている。私達のようなセキュリティの専門家でなくても理解できる情報源の拡充が、経営層の意識改革にも有効だと考える。

（4） D社

属性			アンケート結果(抜粋)							ASM 診断	
企業	業種	規模	担当者	取引先からの要請	過去インシデント	インシデント内容	経営層の関心度	未把握資産有	脆弱性対応	脆弱性検出	改善先
D社	製造業	③~100 名	③		●	③	②		●	●	●

（1） サイバーセキュリティ対策実施の決裁/意思決定プロセスについて	
① 自組織の体制・意思決定プロセス等	自身が入社前は、ベンダーに任せており、FW やウイルス対策ソフトを入れている程度だった。自身が中途入社し、社内 SE として働いている。システム部門は上司と 2 名体制である。 EDR の導入等は上司から経営層に上申して承認を得ている。システムが自組織収益の大半を占めるため、セキュリティ対策の導入や意見は経営層も関心が高く、理解を得やすい。 人員不足により、サーバのログ解析などは手が回っていない。
② 取引先関連	
（2） セキュリティ対策のコスト・工数について	
① 実施した対策、コスト感、人的負荷等について	セキュリティの費用は EDR 等諸々含めると年間 100 万円ほどである。 ソフトウェアのバージョンアップの情報や脆弱性の情報はメーカーからの通知で把握している。
② 工夫した点もしくは課題	どれだけの対策を行った方が良いのかの目安は難しいと感じている。
（3） 今回発見された脆弱性について	
	今回 ASM 診断で見つかった脆弱性(SSL/VPN)は来週に業者が対応する予定。本対応は追加依頼となり、費用は 20 万円ほどかかる予定。 ベンダーとは保守契約を結んでいない。パネルの露出については自身で対応した。
（4） 過去のサイバーインシデントの実態について	
① インシデント発生時の状況	SQL インジェクションを受けた。とあるサイトのパスワードリマインダを悪用され、管理用パスワードの改ざん、不審メールの一斉送信が起きた。
② 被害額の程度	一時的にリマインダが使えなくなったが、大きな影響には至らなかった。復旧には 10 日程度を要した。
③ サイバー保険加入有無	インシデント発生後、すぐに加入した。
④ その他	
(5)学び・再現可能な Tips	
① これから対策を始	エラーが起きたときにログがないことがある。何か問題があったときに、3 ヶ月以上

める企業へのアドバイス	前の事象も多いため、ログが残っていないと原因の検証ができない。可能であれば1年はログを保持すべきと考える。
（6）その他	
① やってよかった施策	WAF は安心感も持てるため、必要だと考える。その他では EDR とウイルス対策ソフトを個別から同じベンダーに統一したことは管理が楽になったので良かった。

（5） E社

属性			アンケート結果(抜粋)							ASM 診断	
企業	業種	規模	担当者	取引先からの要請	過去インシデント	インシデント内容	経営層の関心度	未把握資産有	脆弱性対応	脆弱性検出	改善先
E社	医療･福祉業	③~100 名	①		●	①	②		●		

（1） サイバーセキュリティ対策実施の決裁/意思決定プロセスについて	
① 自組織の体制･意思決定プロセス等	サイバーセキュリティ対策の起案･判断は事務長である自身である。形式上は理事会承認だが、実質的には判断を任されている。 ベンダーからの提案を受けて導入を判断。電子カルテは別ベンダーが担当している。他にセキュリティ分野の担当はいない。HP の更新等も自身が担っている。ただ、ブログ更新等の情報発信業務は他職員に引き継ぐ予定である。
② 取引先関連	「何もやっていない」と言われないための説明責任を意識し、最低限の対策を実施している。
（2） セキュリティ対策のコスト･工数について	
① 実施した対策、コスト感、人的負荷等について	主な対策は FortiGate(UTM)の導入である。約 7~8 年間運用しており、5 年ごとに機器を更新。リース料は増加傾向となっている。 年間維持費は約 100 万円(保守･バージョンアップ含む)。他にセキュリティ投資は行っていない。 IT･セキュリティ運用は院内に専任者がおらず、ベンダー任せ。人的な工数は最小限。 電子カルテはクローズドネットワークで運用。USB ポート利用不可などの物理的対策は実施。 費用や工数の抑制は、外部委託の活用と最低限の運用により実現している。
② 工夫した点もしくは課題	決裁の主なハードルは費用対効果の説明と予算確保である。経営資源が限られる中、患者サービス等の目に見える投資と比較してサイバーセキュリティの優先度は下がりやすい。 サイバーセキュリティ対策は必要と認識しつつも、経営が厳しい中では“必要経費”と見なされにくい。医療報酬制度の限界や国民皆保険の維持とも直結した課題。 「何もやっていない」と言われないための“言い訳”として対策を導入しているが、実際の防御効果については不明点が多い。 今後のリスク環境変化や重大インシデント発生時には、必要に応じて投資の優先順位を上げる用意はある。
（3） 今回発見された脆弱性について	

（4） 過去のサイバーインシデントの実態について	
① インシデント発生時の状況	約 10 年前にグループ内拠点で職員が不審メールを開封し、ウイルスに感染。迷惑メールが大量に届くようになった（宅配業者を装ったフィッシング）。
② 被害額の程度	金銭的被害や業務停止等の重大な影響は発生しなかった。
③ サイバー保険加入有無	加入している。
④ その他	
（5）学び・再現可能な Tips	
① これから対策を始める企業へのアドバイス	「何もしていない」と言われないための最低限の対策（UTM 導入、クローズドネットワーク維持）は重要。信頼できるベンダーに相談し、外部委託を活用すべきと考える。また、職員教育は最低限でも継続的に実施することが肝要であり、特に不審メール対応など基本的なリテラシー向上は必須ではないか。 サイバーセキュリティの知識が乏しい場合は、自前で無理にやろうとせず、外部専門家やベンダーの力を借りるべき。一方で、費用対効果が見えにくく、経営的に優先順位が上がりにくい側面はある。
（6） その他	
① 本事業の参加について	無料診断等の外部支援には感謝している。今後も継続的な支援を期待している。 最新情報の入手や業界動向には今後も関心を持ち続けたい。

（6） F社

属性			アンケート結果(抜粋)							ASM 診断	
企業	業種	規模	担当者	取引先からの要請	過去インシデント	インシデント内容	経営層の関心度	未把握資産有	脆弱性対応	脆弱性検出	改善先
F社	医療･福祉業	③~100 名	②		●	①	②		●		

（1） サイバーセキュリティ対策実施の決裁/意思決定プロセスについて	
① 自組織の体制･意思決定プロセス等	IT 系営業職や電子機器メーカー勤務の経験者が IT 担当を担っている。 前職の経験を活かし、現場の技術的サポートも行う。現場の IT 導入･運用、ベンダーとの調整、セキュリティ対策の実務を担う。医療･介護両部門のシステムにも関与し、現場の IT リテラシー向上にも寄与。 対策の起案は現場担当者から行われ、提案は経営層へ直接上申する。経営層（理事長等）が IT･ICT･セキュリティに理解があり、現場の必要性を理解しているため、承認は比較的スムーズである。 費用面がハードルとなる場合もあるが、必要性が高い対策は「仕方がない」と認識され導入される。 組織文化として、経営層･現場ともに IT･セキュリティに前向きであり、現場からの提案が通りやすい環境が推進力となっている。
② 取引先関連	他法人との情報交換は少なく、独自にベンダーと相談しながら運用している。
（2） セキュリティ対策のコスト･工数について	
① 実施した対策、コスト感、人的負荷等について	サイバーセキュリティ関連の年間ランニングコストは約 50 万円。ハードウェア更新時は 100 万円単位の費用が発生している。運用費と更新時にかかる費用をならすと年間 100 万円程度。 ソフトウェアは Microsoft Defender 中心でコストダウン。ベンダー保守委託は最小限とし、自組織で対応することで運用コスト抑制と知識蓄積を両立している。
② 工夫した点もしくは課題	介護系システムは補助金活用で初期費用の約 3/4 を賄う。 人的工数は IT 人材が自組織対応を行い、外部委託を減らし最適化をしている。IT 人材がいることで自組織での運用･対応が可能。知識のない場合は外部委託も選択肢。コストと人材のバランスを見極めることが重要である。 厚労省ガイドラインは「絶対的なもの」として遵守しチェックリストも活用している。
（3） 今回発見された脆弱性について	
（4） 過去のサイバーインシデントの実態について	
① インシデント発生時の状況	約 10 年前に職員メールアカウントが乗っ取られ、大量のなりすましメールが送信された。ホスティング会社からの連絡でインシデント発生に気が付いた。

② 被害額の程度	金銭的・物理的な被害はなかった。ただし、我々から送信したメールが Gmail の迷惑メールフォルダに振り分けられるようになり、ドメインの信用が回復するのに約 1 年を要した。
③ サイバー保険加入有無	不明
④ その他	インシデントの原因は職員の不注意による不審リンククリックと思われるが、本人は自覚なし。改善策としてホワイトリストによる Web 閲覧制限をかけるようになった。
(5)学び・再現可能な Tips	
① これから対策を始める企業へのアドバイス	まずは入口対策(ファイアウォール)、バックアップ体制構築を推奨する。 また、IT リテラシーが低い職員層への教育は難しく、定期的な研修や啓発が不可欠である。コストと人的リソースのバランスが難しい。
(6) その他	
① やっていてよかった対策	ファイアウォール(FortiGate 等)導入、バックアップ体制構築、Web 閲覧フィルタリング(ホワイトリスト)など。

（7） G社

属性			アンケート結果（抜粋）							ASM 診断	
企業	業種	規模	担当者	取引先からの要請	過去インシデント	インシデント内容	経営層の関心度	未把握資産有	脆弱性対応	脆弱性検出	改善先
G社	金融・保険業	②～50 名	③				②		●	●	

（1） サイバーセキュリティ対策実施の決裁/意思決定プロセスについて	
① 自組織の体制・意思決定プロセス等	システム担当の主業務は営業であり、システム管理は兼任している状態である。会社規模が小規模で、専任の IT 人材を配置するのは難しいため、自身がシステム対応も担っている。システムに関する知識は趣味をきっかけに独学で身につけた。 システム関連業務は、通常業務時間外（朝や夜）に対応しており、いわゆる「1 人情シス」状態。 経営層はセキュリティに関して意識が高く、必要な費用はしっかり拠出する方針。
② 取引先関連	外部業者・サプライチェーン管理の一環として、セキュリティのチェックシートを送付している。
（2） セキュリティ対策のコスト・工数について	
① 実施した対策、コスト感、人的負荷等について	昔から付き合いのある業者のサポートを受けている。 契約書等の重要書類は社内の共有サーバで管理し、バックアップも実施している。 コロナ禍をきっかけにノート PC を導入、本社では VPN 経由で外部からのアクセスを可能にした。一方、支店ではノート PC 未導入のため、出社対応が続いた。 クラウド化も検討したが、経営層の意向により付き合いのある業者への委託を継続中。 支店と本社で IT 環境が異なるため、必要性は認識しているが EDR やログ収集は未導入である。 VPN のセキュリティ強化のため、多要素認証の導入検討中。自身が提案し、経営層の承認を得て実施。導入コストは 1ID あたり 7,000 円（買い切り）。 VPN は付き合いのある業者のサービスを利用。 月額 10 万円のフルパッケージプランに含まれている（サーバ保守、PC 不具合対応、UTM アップデート等も含む）。年間のコストは約 120 万円。 アラート発生時は業者から通知があり、対応も業者が実施する。
② 工夫した点もしくは課題	取引業者を比較して相見積もりを取る等コスト削減の意識は持っており、経営層へも報告・相談するが、昔からの付き合いがある取引業者を変更するのは難しい。
（3） 今回発見された脆弱性について	
（4） 過去のサイバーインシデントの実態について	

① インシデント発生時の状況	なし
② 被害額の程度	なし
③ サイバー保険加入有無	不明
④ その他	インシデント発生時の BCP（事業継続計画）策定済み。
（5）学び・再現可能な Tips	
① これから対策を始める企業へのアドバイス	特になし
（6） その他	
① 社員教育について	年に 2 回ほど社員教育を実施している。内容としては総務省などの資料を生成 AI で再構成し配布するなど。以前は自身で資料を作成していた。 サイバー攻撃等のリスクについても、常に社員に注意喚起している。
② サプライチェーン評価制度について	取組予定であり、3 つ星は取れるように対策していきたいという思いはある。

（8）H社

属性			アンケート結果（抜粋）							ASM 診断	
企業	業種	規模	担当者	取引先からの要請	過去インシデント	インシデント内容	経営層の関心度	未把握資産有	脆弱性対応	脆弱性検出	改善先
H社	情報通信業	④～300 名	③	●			①		●	●	●

（1） サイバーセキュリティ対策実施の決裁/意思決定プロセスについて	
① 自組織の体制・意思決定プロセス等	法人向けクラウドサービス提供開始時に本格的な対策を推進し、メールサービスを Google に切り替え、ストレージも Google にしてセキュリティを上げた。 また、ISMS 取得などを順次実施した。 技術部門トップの役員主導で、セキュリティポリシー策定・推進を継続している。 技術者でもある役員の理解があるため、必要な対策を上申して通らないことはない。
② 取引先関連	取引先からのセキュリティチェックシートや脆弱性管理の確認依頼は頻繁に受けている。ISO 27017 取得やホワイトペーパー提出等で対応している。 技術的な対策は概ね実施済みだが、マネジメントシステム面（運用の記録・レビュー・明文化等）で追加対応を求められるケースが多い。NIST SP800-53 など厳しい規格への対応も進めていく。特に大手企業からの依頼事項レベルが高いため対応に苦慮。
（2） セキュリティ対策のコスト・工数について	
① 実施した対策、コスト感、人的負荷等について	年間費用は数百万円～1,000 万円未満。年々増加傾向で、次年度はさらに増額予定である。費用増加の主因はシステム規模の拡大に伴う管理工数削減・自動化対応、陳腐化技術の刷新等。 セキュリティ関連業務は約 10 名体制。現状では人員不足を認識しており、今後は 20 名程度まで拡充したい。各部門にセキュリティ担当者を配置し、全社的な意識醸成を重視している。
② 工夫した点もしくは課題	アンケート調査において「委託できる業者がいないのが悩み」と回答した意図は、基本方針として「自社で対応」を重視している。また、外部委託先は国内法人に限定しており、海外拠点や国外で作業する業者は除外。日本法準拠、国内事業所・作業者を条件とし、リーガルリスク・統制リスクを最小化している。 感情論ではなく、理詰めで考えて判断した結果である。法的リスク（愛国法・パトリオット法）があり、何か起きた場合に顧客情報が取られてしまうことを防げない点や、コストメリット以上に、セキュリティ面のデメリットが大きいと判断している。自社エンジニアの技術力も高いため、外部委託先の選定基準は厳しくなる。
（3） 今回発見された脆弱性について	

	1 回目診断で脆弱性が見つかったものの、2 回目診断では解消した。 診断で指摘されたドメインは、現在使用していない古いサブドメインだった。DNS に古い情報が残っていたため、診断対象になったと思料している。該当ドメインは既に他社が利用しており、現行サービスとは無関係。利用していないドメインは、DNS から削除する対応を実施した。 WordPress 管理ツールについては、過去に外部から不正アクセスされる被害があったため、10 年以上前から IP アドレス制限や二要素認証を導入済みである。 現在も WordPress は廃止方針で運用しており、リスクのある部分は順次削除している。
（4） 過去のサイバーインシデントの実態について	
① インシデント発生時の状況	なし
② 被害額の程度	なし
③ サイバー保険加入有無	不明
④ その他	
(5)学び・再現可能な Tips	
① これから対策を始める企業へのアドバイス	ID / パスワードのみの認証は危険であり、多要素認証（ワンタイムトークン、SMS 等）を必須化することで不正アクセスの大半を防止可能と考えている。まずは多要素認証の導入を推奨したい。 脆弱性・攻撃事例が多いメジャーな機器（例：FortiGate 等）は選定しない。あえて国内のマイナーな機器を選定している。また、自動パッチ適用もよいと思う。手が回らない機材はそもそも導入しない判断も重要ではないか。
（6） その他	
① 社員教育について	e ラーニング教材の定期配布・管理ツールによる受講管理を実施。外部講師による講演・発表会も開催し、全社的なセキュリティ意識向上に努めている。 添付ファイルの自動検査ツール導入、エンドポイントプロテクション等の仕組みで「気をつけましょう」ではなく、技術的対策でカバーすることが重要である。社内外の事例を全社発信し、危機意識を共有している。
② サプライチェーン評価制度について	ISMS 取得等の認証は一定の効果があるが、上場企業など大手取引先からの要求は年々厳しくなっており、格付け制度のみで対応が容易になるとは考えていない。ガイドライン等への準拠を示すことで一部取引先対応は可能だが、より高い水準の要求には個別対応が必要と捉えている。

（9） I社

属性			アンケート結果(抜粋)							ASM 診断	
企業	業種	規模	担当者	取引先からの要請	過去インシデント	インシデント内容	経営層の関心度	未把握資産有	脆弱性対応	脆弱性検出	改善先
I社	製造業	②～50 名	①				②		●	●	

（1） サイバーセキュリティ対策実施の決裁/意思決定プロセスについて	
① 自組織の体制・意思決定プロセス等	某 IT 企業から転職し入社。IT 担当も代表取締役である自身が務めている。 クラウドを活用した IT 環境の整備を進めている。
② 取引先関連	EC サイトの整備は立ち上げ時期は自身で推進していたが、現在は企画開発室が担っている。前職時代の経験を活かして売り上げを伸ばしている。
（2）セキュリティ対策のコスト・工数について	
① 実施した対策、コスト感、人的負荷等について	サイボウズオフィスから Google Work Space に切り替えた。2014 年からサイボウズオフィスを利用していたものの、kintone を利用していることもあり、不要と判断したため。Google Work Space であればメールやクラウドストレージ等をまとめて利用できるのが利点である。
② 工夫した点もしくは課題	ネット販売を拡大していることから、購買者の個人情報管理・保護は重要ではあるが、Amazon のセラーセントラルで対応しており、我々も個人情報へ常にアクセスできるわけではないことから、個人情報を PC にダウンロードしない、といったルールで対応している。kintone には情報入力するものの、ログイン管理を行えば問題ないため、現状、個人情報管理は十分と認識している。 GoogleWorkSpace については IP アドレス制限や二段階認証はまだ導入していないものの、順次導入することを検討している。 技術的なセキュリティ対策として異常検知やメールのフィルタリングソフトなどは今後も強化していきたいが、GoogleWorkSpace を導入したことで一定改善されたと考えている。
（3） 今回発見された脆弱性について	
	流出していると指摘されたメールアドレスは退職者のものであり、サービスの無効化・利用停止を行っている。
（4） 過去のサイバーインシデントの実態について	
① インシデント発生時の状況	なし
② 被害額の程度	なし
③ サイバー保険加入有無	サイバー保険も提案を受けているが、必要性は低いと判断している。

④ その他	ランサムウェア等で万が一 PC が止まってしまっても、データはクラウドで保管しており、PC 内部にデータを置いていないことから大きなダメージを受けることはないと考えている。
(5)学び・再現可能な Tips	
① これから対策を始める企業へのアドバイス	自社でシステム等を構築しすぎず、クラウドを活用することを推奨したい。技術革新が進む中、一企業での投資には限界がある。 リモートワークのしやすさもクラウド活用が有利。VPN による環境構築は複雑化につながるため、クラウド利用が望ましいのではないか。
(6) その他	
① 社員教育について	社員の年代ごとの教育が必要。特に高齢社員には個別教育が重要。
② IT 人材について	IT リテラシーを有する人間は必要。先日某社の担当者から AI 付帯プランの提案を受けたが、汎用 AI で代替可能と判断し導入を見送った。IT リテラシーがあることで無駄な投資を防げる。 セキュリティ対策だけではなく、kintone やアプリ構築等も含めて任せることが可能な人材を育てていきたい。

（10）J社

属性			アンケート結果(抜粋)							ASM 診断	
企業	業種	規模	担当者	取引先からの要請	過去インシデント	インシデント内容	経営層の関心度	未把握資産有	脆弱性対応	脆弱性検出	改善先
J社	製造業	②～50 名	③				③	●	●	●	

（1） サイバーセキュリティ対策実施の決裁/意思決定プロセスについて	
① 自組織の体制・意思決定プロセス等	主な業務はマーケティングだが、社内の情報インフラ・セキュリティ全般も兼務している。広報、デザイン、メルマガ配信、新規事業、SNS 運用などを幅広く担当している。情報管理課は自身含めて 2 名体制である。 業務の 3 分の 1 程度はセキュリティ・インフラ関連に充てている。業務量は多いものの、生成 AI を活用するなどの工夫をしている。 経営層(社長)はセキュリティに対して一定の理解があるが、他社以上の投資には消極的であるため、自身が必要性を訴求している。 そもそも情報システム部門に配属される人は、バックグラウンドが事務系の人間が多いため、積極的に上申することが難しい。IT ベンダーの営業マン等は情シス部門の担当者を口説こうとするが、情シス部門自体はセキュリティや機器に関する情報も持っており、感度も高い。重要なのは経営者を如何に説得して理解してもらうかではないか。
② 取引先関連	セキュリティチェックシートの記入や、脆弱性管理の要請は多いが、内容が実態や規模にそぐわないものが多く、(データセンターの施錠 等)疑問に感じている。企業ごとにフォーマットも異なるため、対応負担は大きい。 例えば帝国データバンクのように企業を評価する第三者機関が、評価基準を定めて企業ごとのセキュリティ対策を評価するような仕組みができれば良い。 経済産業省が来年度から運用開始を予定している格付け制度についても、企業ごとに取り組むべきセキュリティ対策・範囲が異なる中で、評価基準が見えないと感じている。例えば現在自社で取り組んでいるセキュリティ対策について「そこまでやらなくても大丈夫」と評価された場合、情シス部門が経営層からマイナス評価を受ける可能性もあり、複雑な思いを抱いている。
（2）セキュリティ対策のコスト・工数について	
① 実施した対策、コスト感、人的負荷等について	某ベンダーが IT パートナーとして深く関与しており、万が一の際も代替対応可能な体制を敷いている。UTM や在宅勤務環境は導入済であったが、情報資産管理(LANSCOPE)や EDR の導入を推進した。 セキュリティ機材のリースアップを控えていたことから、情報インフラのフルリニューアルを決めた。Fortigate から CiscoUmbrella へネットワークを全面移行したほ

	か、セキュリティは CrowdStrike に切り替えを実施した。その他、VPN はベンダーのサービスを一時利用し、今後クラウド基幹システムへの移行によって廃止予定である。 今回の情報インフラフルリニューアルで約 500 万円の初期費用がかかっており、ランニングコストで別途 500 万円/年ほどになる。
② 工夫した点もしくは課題	オンプレミスからクラウドへ段階的に移行している VPN 等の「入口」を減らして攻撃対象領域の縮小を図っている。 LANSCOPE の導入によって「会社 PC のログは監視している」ということを伝えており、「抑止力」と捉えている。実際にアラートが出た場合は注意喚起しており、社長に対しても業務用 PC の私的利用は控えるように依頼している。
（3） 今回発見された脆弱性について	
	ベンダーにも相談したところ Fortigate の問題であったため、情報インフラのフルリニューアル時に撤去することから解決済の認識である。大変なのはセキュリティ規定の変更であり、生成 AI 等も活用しながら取り組む予定である。
（4） 過去のサイバーインシデントの実態について	
① インシデント発生時の状況	なし
② 被害額の程度	なし
③ サイバー保険加入有無	不明
④ その他	
(5)学び・再現可能な Tips	
① これから対策を始める企業へのアドバイス	まずはクラウド環境の活用を推奨したい。シングルサインオン（SSO）による ID 管理、クラウドサービスのセキュリティ機能を活用すれば良いのではないか。 端末管理を極力シンプルにして、データのローカル保存を減らすことが大事ではないか。
（6） その他	
① 情報共有について	経営層へ危機感を持たせるような情報がタイムリーに共有されることが重要だと考えている。
② インセンティブについて	「この対策を行うと減税につながる」といったインセンティブがあればセキュリティ対策は一気に普及するのではないか。

4.5. 業種別傾向

製造・建設業や卸売・小売業では、「兼務情シス」が標準で、経営者や営業・総務が片手間でセキュリティを見ているケースが多く見られる。

一方、情報通信業や一部の金融・保険業では専任担当者や技術バックグラウンドを持つ役員が配置され、運用レベルまで踏み込んだ対策が進んでいる。

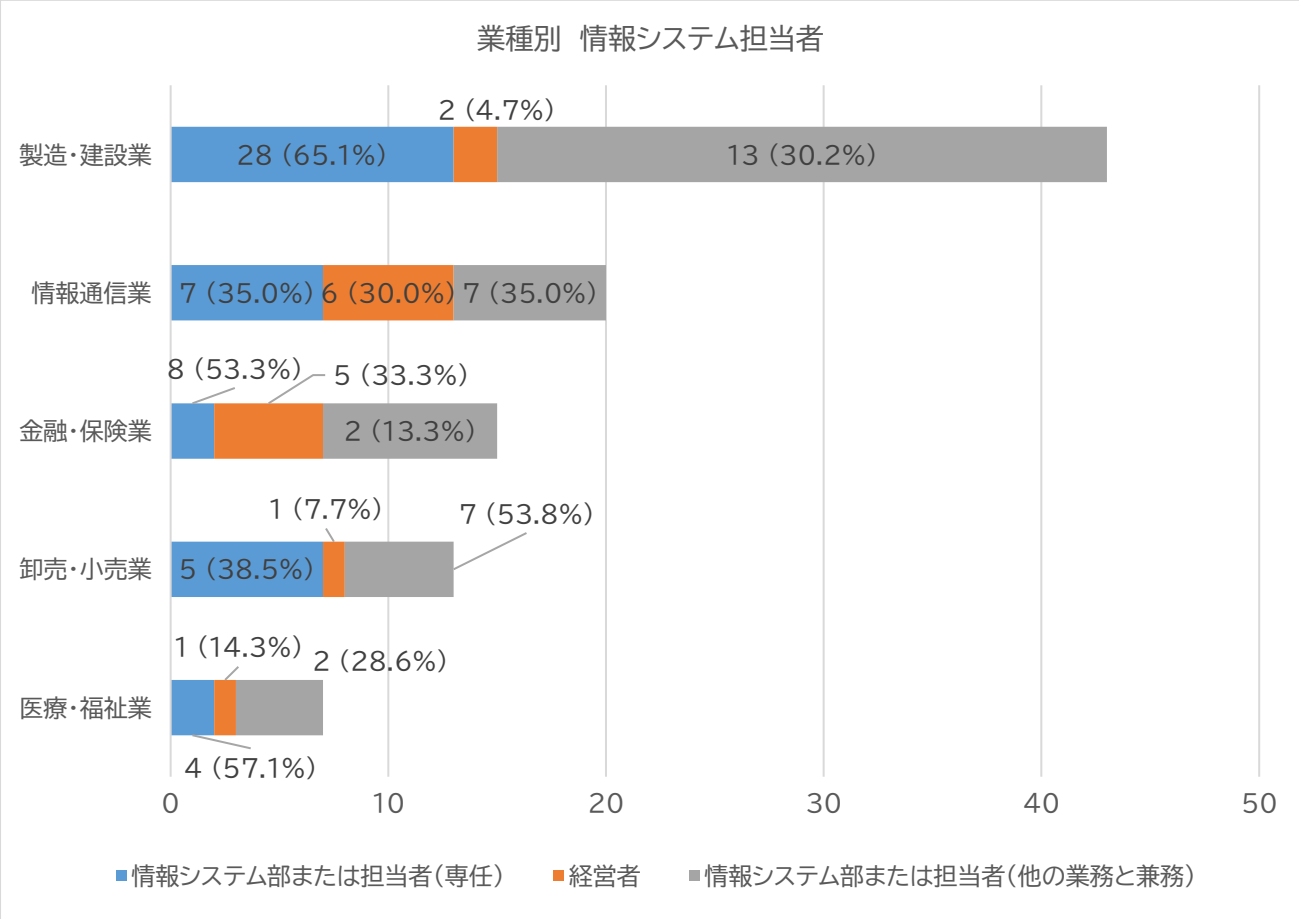

図 21　業種別　情報システム担当者(設問 3 関連)

情報通信業や金融・保険業では、大手顧客からのチェックシートや脆弱性管理要請を日常的に受けており、サプライチェーン要求水準も高い傾向がある。

製造・建設業でも一部で要請が強まる一方、医療・福祉業や小規模な卸売・小売業では、まだ外部からの具体的な要求が少なく、自主的な基準づくりが課題となっている。

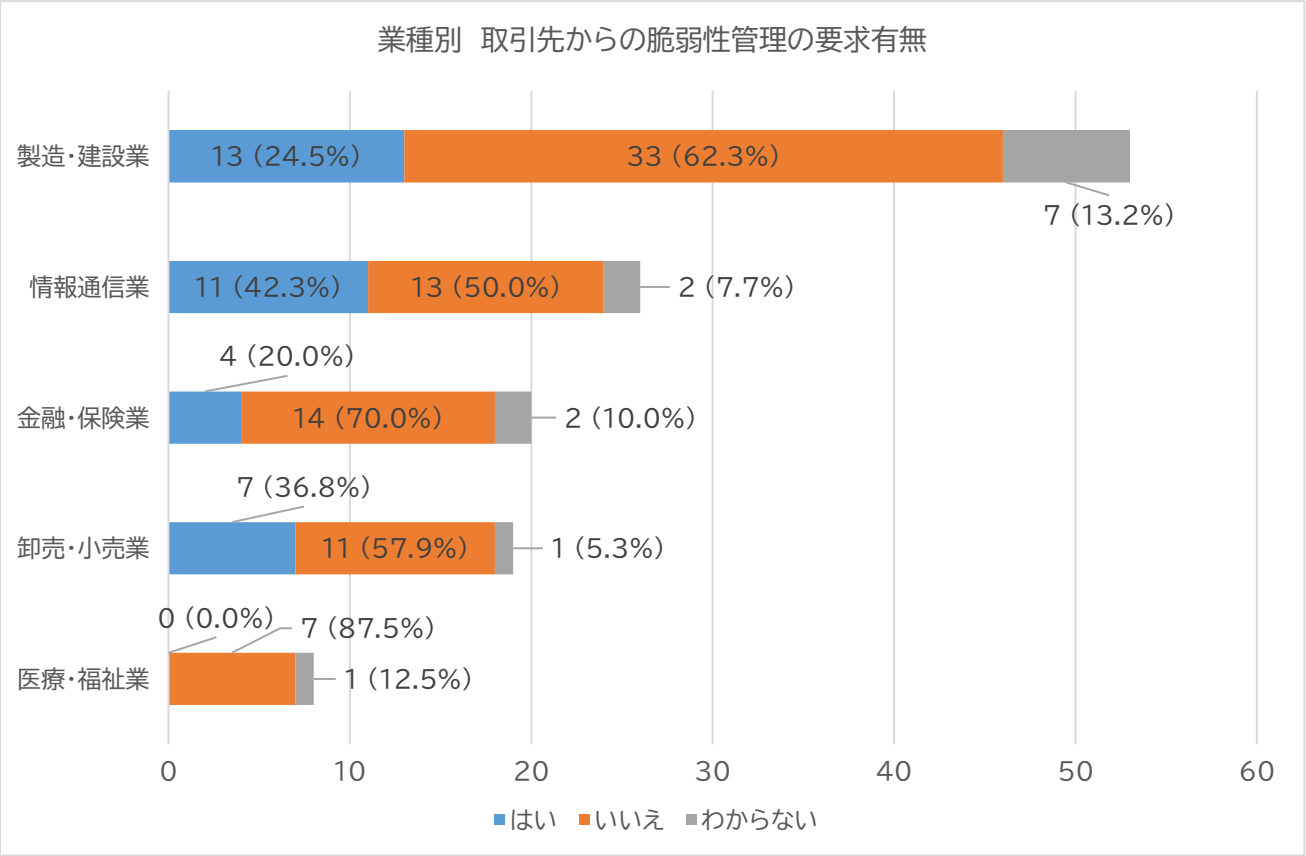

図 22　業種別　取引先からの脆弱性管理の要求有無(設問5関連)

製造・建設業や医療・福祉業では、不審メール開封やウイルス感染、Web 改ざんなどのインシデント経験が一定数あり、それを契機に対策強化へ踏み出した企業も見られる。

一方で、金融・保険業や卸売・小売業では「大きな被害はない」と認識している企業も多く、危機感と投資優先度のギャップが残っている。

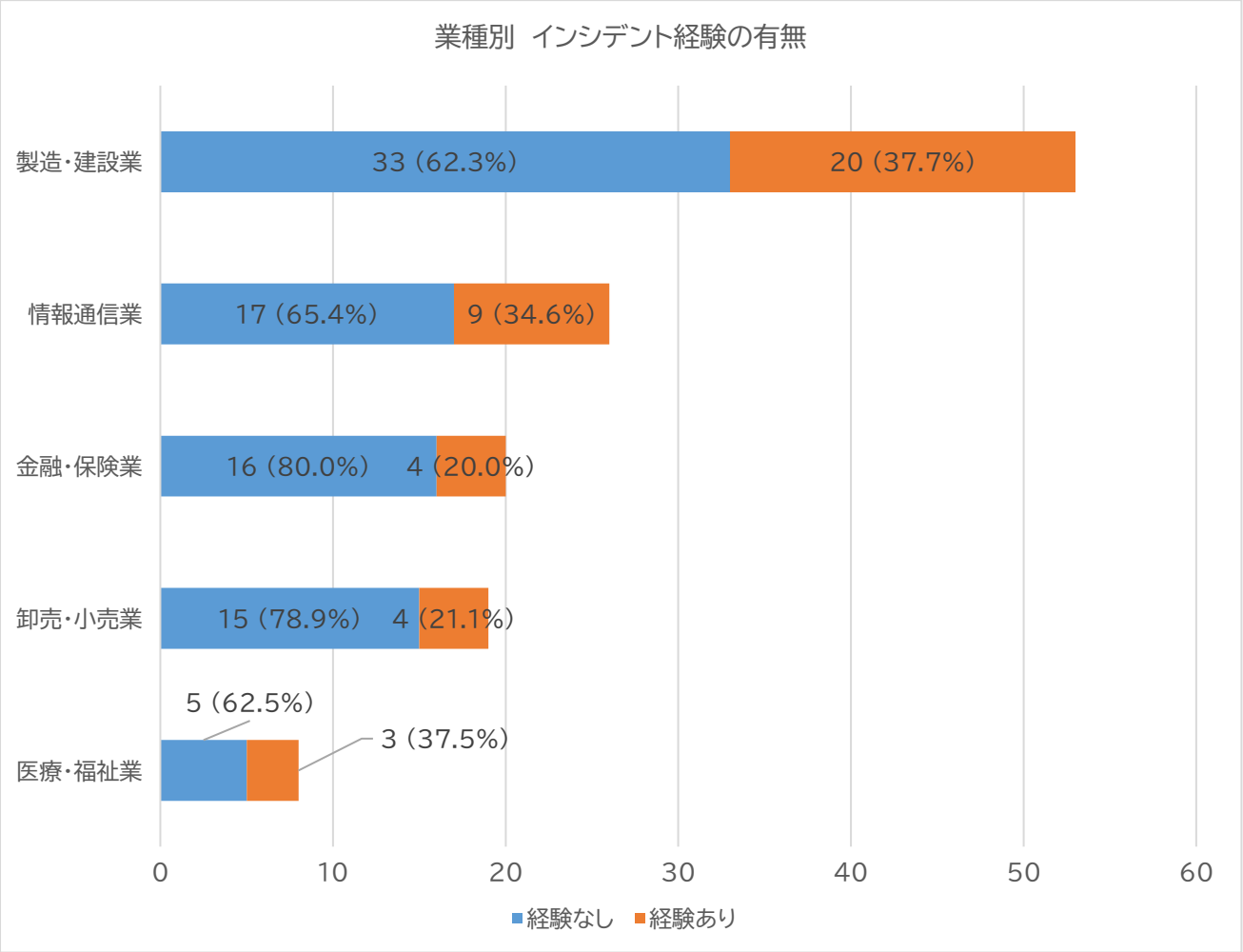

図 23 業種別 インシデント経験の有無(設問6関連)

情報通信業や一部の金融・保険業では、技術に明るい経営層の主導で関心度が高く、ISMS 取得やログ管理などへの投資が進んでいる。

医療・福祉業や卸売・小売業では「どちらかといえば低い」層も目立ち、患者サービスや売上向上施策と比べてセキュリティ投資の優先度が上がりにくい構造が見られる。

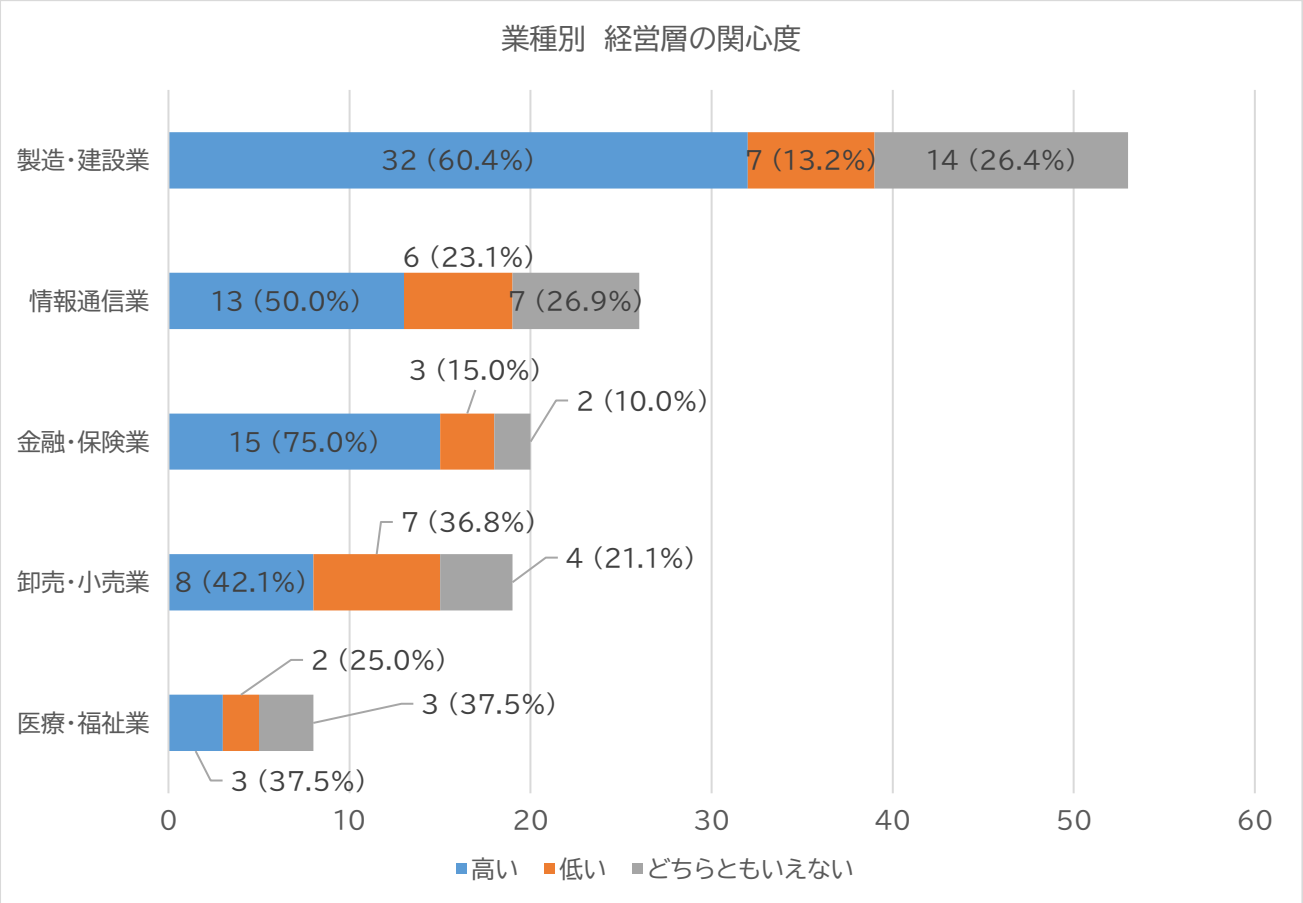

図 24　業種別　経営層の関心度(設問8関連)

インシデント経験があり、かつ経営層の関心が高い情報通信業や一部の製造業では、ASM 診断結果を受けて不要サービス停止や多要素認証導入など具体的な改善に踏み込む割合が高くなっている。

一方、医療・福祉業や卸売・小売業では「問題なし」とみなして対応を先送りするケースも残り、兼務情シス体制や費用対効果の不明確さが行動のボトルネックになっている。

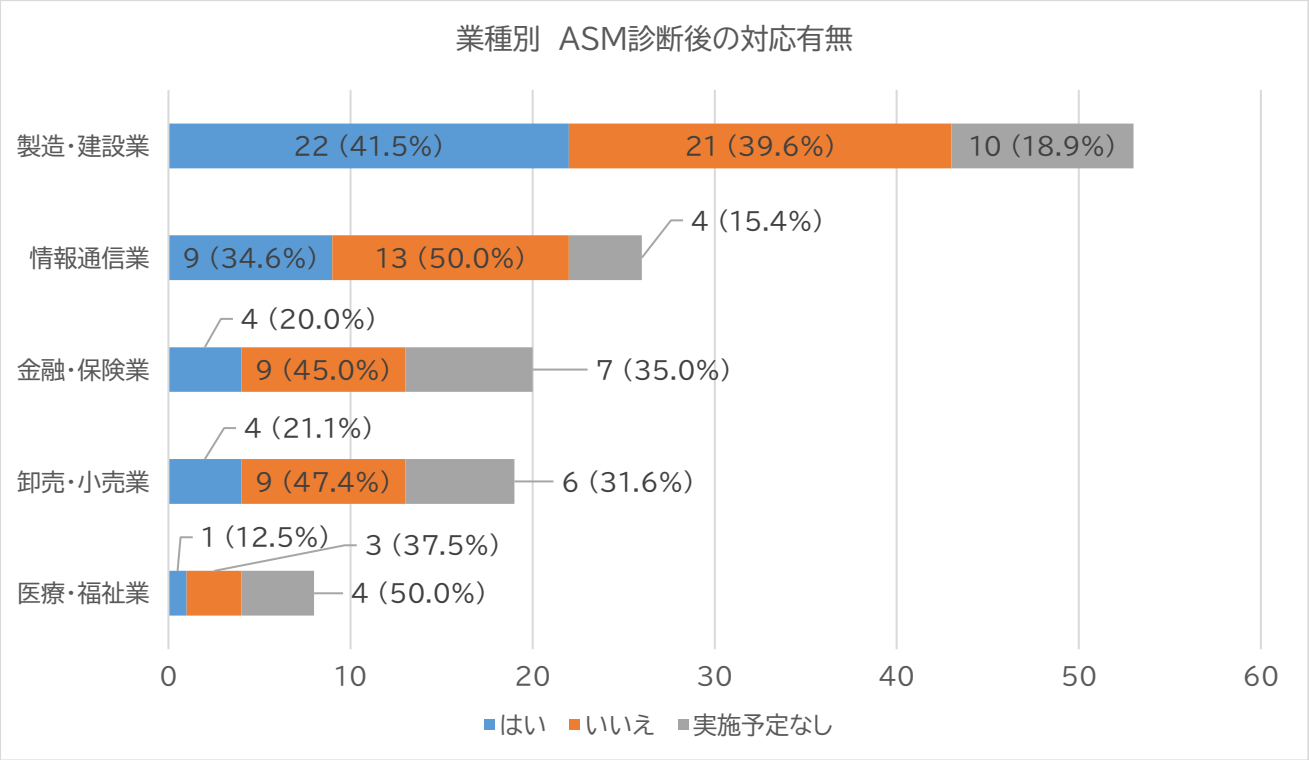

図 25　業種別　ASM 診断後の対応有無(設問11関連)

5. 事例集の作成と活用（別冊）

5.1. 事例集の作成方針

本事業のメインメニューは「ASM 診断」「アンケート調査」「ヒアリング調査」である。本事業を通じて確認できた脆弱性事例、被害事例、取組事例を計 30 事例にまとめて、事例集として作成した。

本事例集は中小企業にセキュリティ対策の必要性を理解いただくための「実践事例集」としての役割を期待している。

詳細は事例集を参照されたい。

6. 事業実施結果から得られた考察

6.1. 事業参加事業者におけるサイバーセキュリティ対策状況の実態

本事業の参加企業 126 社に対する ASM 診断結果、アンケートおよび 10 社へのヒアリング結果を総合すると、中小企業のサイバーセキュリティ対策状況は「一定の対策は講じているが、攻撃面の縮小や脆弱性管理まで踏み込めていない層が厚い」という実態が明らかになった。

（1） 基本的な技術対策は広く導入されつつある一方、「見えない資産」と「設定不備」が残存

ウイルス対策ソフト、ファイアウォール、バックアップなど、いわゆる「三種の神器」は多くの企業で導入されている。

しかし ASM 診断では、暗号化されていない HTTP/FTP/メールサービス、期限切れや不適切な証明書、メール認証（SPF/DMARC）の未設定など、設定レベルの不備が多数検出された。

また、クラウド移行時に停止し忘れたバックアップ用 DB、過去に利用していたサブドメインや API キーなど、「組織としては既に使っていないがインターネット上には残っている資産」が複数の企業で確認され、攻撃面の「死角」となっていることが明らかになった。

（2） 組織的な対策は「最低限の整備」にとどまる企業が多い

セキュリティーポリシーや規程は 8 割弱の企業で整備されているが、インシデント対応計画やサプライチェーン管理まで含めた体系的な運用に至っている企業は限定的である。

特に、取引先からのチェックシートや脆弱性管理の要請に対しては、「回答はしているが、自社の基準や方針を持たないまま個別対応している」ケースが多く、外部要請にやむをえず応える場当たり的な対応をする実態が見られた。

（3） 「専門人材不在」と「兼務体制」が標準であり、運用に限界

アンケートでは、ほぼ全ての層で「専門人材不在」「教育不足」が課題として挙げられた。

実務を担うのは、経営者自身、情報システム担当者の兼務、総務担当者などが中心であり、「1 人情シス」や「本業の合間にセキュリティ対応」という体制が一般的である。

そのため、EDR やログ監視など高度なツールを導入している企業であっても、「ログ分析まで手が回らない」「費用対効果を説明できない」といった運用上の限界が見られた。

（4） インシデント経験の有無が、対策の具体性と行動の差を生む

ランサムウェア感染、Web 改ざん、不正アクセス、情報漏えい等のインシデント経験がある企業ほど、ASM 結果を踏まえた具体的な行動（パッチ適用、多要素認証導入、不要サービス停止、ログ保存期間の延長など）に踏み込んでいる。

一方で、インシデント経験のない企業では、「リスクは理解したが、今すぐの優先度は低い」「現状で十分」といった認識にとどまり、ASM 結果が具体的な改善行動に結びつかない傾向が見られた。

（5） 経営層の関心度と投資判断が対策レベルを左右

経営層に IT・セキュリティの理解者がいる企業では、クラウド活用や UTM・EDR 導入、ログ管理、バックアップ強化など、一定水準以上の投資と運用が進んでいる。

一方で、経営層関与が薄い企業では、ASM 診断結果を「問題なし」と解釈して投資を先送りする、あるいは「最低限の説明責任を果たすための対策」にとどめる傾向が見られた。

特に医療・福祉分野では、「患者サービス等の目に見える投資」と比較した際に、セキュリティ投資の優先度が上がりにくい構造的課題も確認された。

（6） クラウド活用とローカルデータ削減へのシフトが進行中

Microsoft 365、Google Workspace、各種クラウド業務システム等の導入により、「データはクラウドに集約し、端末には残さない」「VPN を減らし、クラウド前提のネットワークに移行する」といった方針を取る企業が増えている。

これはセキュリティ強化と業務効率化を両立させる有効な方向性である一方、クラウド設定の不備や ID 管理・多要素認証の未導入など、新たなリスクも内包しており、クラウド前提のガバナンス整備が今後の課題である。

以上から、本事業参加企業は「基本的なセキュリティ対策は一定程度実施しているが、外部から見える攻撃面の管理、クラウド前提の脆弱性管理、経営層を巻き込んだ継続的な改善プロセス」という観点では、なお発展途上にあると整理できる。

6.2. ASM ツール活用の課題と有効性

ASM ツールは、本事業を通じて中小企業にとって有効な手段であることが確認された一方、その価値を十分に引き出すためにはいくつかの構造的課題がある。

（1） ASM ツールの有効性

本事業で活用した ASM ツールは、以下の点で有効に機能した。

① 外部から見える自社資産の可視化

ドメイン情報を入力するだけで、外部公開されているサーバ、リモート接続機器、Web サイト、メール設定などを自動的に洗い出し、リスクレベル別に提示できた。

クラウド移行時に停止し忘れた DB、利用していないサブドメイン、公開された管理パネルなど、社内では把握されていなかった資産・設定が多数発見された。

② 攻撃面の縮小という行動変容のきっかけ

診断結果を受けて、不要サービスの無効化、未使用サブドメインの廃止、古い API キーの更新・削除、といった「攻撃者から見える入口を減らす」対策を実施した企業が一定数確認された。

③ 一定の対策を実施済みの企業における「次の一手」の具体化

クラウド活用や EDR 導入等を進めている企業にとって、ASM 診断は、VPN 機器の管理パネル露出への対応、メール認証（SPF／DMARC）の強化、証明書管理の徹底、CMS（WordPress 等）の廃止・アクセス制限など、既存対策の「抜け漏れ」を補完するツールとして機能した。

④ インシデント経験企業における再発防止・高度化の指標

過去にランサムウェア感染や Web 改ざん等を経験した企業では、ASM 結果を「再発防止策の棚卸し」として活用し、ログ保全期間の延長、WAF 導入、多要素認証の徹底、クラウドへのデータ集約とローカルデータ削減等の高度化施策につながっていた。

⑤ 生成 AI との組み合わせによる非専門家の活用余地

一部企業では、ASM レポートを生成 AI に読み込ませ、要約や対応方針の整理、社内説明資料の作成に活用していた。これにより、専門用語の多いレポートを「自社向けの平易な説明」に翻訳し、経営層や現場への説明負担を軽減していた。ただし、生成 AI の活用は効率化の反面、思わぬ情報漏えいや契約違反につながる可能性もあるため注意が必要である。

（2） ASM ツール活用上の課題

一方で、以下のような課題も明らかになった。

① 専門人材不在とレポート解釈の負担

多くの企業では、ASM レポートに記載された脆弱性名や CVE 情報を自社環境に引き付けて解釈し、対応優先度を判断する人材がいない。

「どの指摘が自社のどのシステムに関係するのか」「どこまで対応すれば十分なのか」といった判断ができず、「レポートは確認したが、そのまま保管されている」ケースも存在した。

② 予算制約と費用対効果の説明の難しさ

重大な脆弱性が検出されても、「対策費用」と「インシデント発生確率・被害額」を定量的に比較することが難しく、経営層への投資提案が通りにくい。

無料診断や補助金の範囲でのみ ASM を活用し、継続的な有償サービスとしては導入しない利用形態にとどまる傾向がある。

③ 経営層関与の弱さと「やらない理由」としての消費

経営層の関心が低い企業では、ASM 診断結果が「重大な問題は検出されなかった」という安心材料として消費され、「追加投資は不要」という結論に誘導されるリスクがある。

技術的な用語のまま経営層に共有され、経営リスクとして認識されていないケースも見られた。

④ 単発診断では活用価値が半減

今回の実証では期間が限られていたこともアリ、単発の診断による現状把握が中心であり、継続的なモニタリングや PDCA まで踏み込めた企業は限られた。

クラウドや SaaS の導入・廃止が頻繁な環境では、アタックサーフェスは常に変化するにもかかわらず、ASM 診断でその変化を追随できていない。

⑤ 外部ベンダーとの役割分担・契約スキームの不明確さ

ASM 診断で検出された脆弱性への対応を、どこまで自社で行い、どこから外部ベンダーに委託するかの線引きが不明確な企業が多い。IT と OT の両方に通じたベンダーが少ない製造業などでは、「誰に相談すべきか分からない」こと自体が ASM 活用のボトルネックとなっている。

⑥ 教育・啓発との連動不足

ASM 結果を社員教育や社内ルール見直しに活かしている企業もある一方、多くは「技術部門内の情報」にとどまり、組織全体のリテラシー向上にはつながっていない。

以上より、ASM ツールの価値を最大化するためには、「ツールそのもの」だけでなく、レポート解釈・優先度付け・設定変更・教育・経営層への説明を含む「周辺の仕組み・外部支援」と一体で設計することが重要であると言える。

6.3. 中小企業に必要と考える今後のサイバーセキュリティ支援策

本事業の結果を踏まえると、中小企業のセキュリティ対策を実効的に底上げするためには、ASM ツールを核としつつ、以下のような支援策・スキーム構築が有効と考えられる。

（1） インシデント経験の有無に応じた「二層型支援メニュー」の整備

インシデント経験あり企業向けには、ASM 結果を活用した再発防止計画の策定支援、ログ管理・EDR・WAF 等の高度化支援、BCP・インシデント対応計画の高度化支援など、「被害を経験したからこそ踏み込める」高度化メニューを提供する。

インシデント経験なし企業向けには、同業他社の被害事例と ASM 結果を組み合わせた「自社に引き付けた危機感喚起」、不要サービス停止、多要素認証導入、メール認証設定、バックアップ確認等を束ねた簡易対策パッケージを提示し、最初の一歩を明確にする。

（2） 専門人材不在を前提とした外部支援モデルの制度化・標準化

中小企業が自前でセキュリティ専門人材を確保することは現実的でないことを前提に、

① サイバーセキュリティお助け隊
② マネージドセキュリティサービス（MSS）
③ ASM 診断＋設定変更代行＋運用モニタリングをワンパッケージにしたサービス
などを、ガイドラインや認定制度を通じて標準化・見える化する。

特に、IT と OT が混在する製造業などでは、「IT/OT 両方に一定の知見を持つ支援事業者」の登録・紹介スキームを整備することで、「誰に相談すべきか分からない」という課題の解消につなげる。

（3） 経営層向けの情報提供・インセンティブ設計の強化

経営層に対して、最新の被害事例、サプライチェーン全体への影響、自社が被害に遭った場合の想定損失・信用失墜リスクを分かりやすく示す「経営者向けレポート」「経営者セミナー」を継続的に提供する。併せて、一定水準以上のセキュリティ対策を実施した企業に対する税制優遇、補助金加点、サプライチェーン評価制度との連動（一定以上の評価で取引先からのチェックシート簡略化等）
など、「やると得になる」インセンティブを設計することで、投資判断を後押しする。

（4） チェックシート・要請の標準化と負担軽減

取引先ごとにバラバラなセキュリティチェックシートや要請項目が、中小企業の大きな負担となっている実態を踏まえ、業種別・規模別に標準化されたチェックリストの策定、サプライチェーン評価制度や第三者認証と連動した「代替証明」の仕組み（例：一定の格付けを取得していれば、個別チェックシートの一部を免除）を整備する。

これにより、中小企業が「実態にそぐわない過剰要求」に個別対応する負担を軽減し、本質的な対策にリソースを振り向けられる環境を整える。

これについては、現在、経済産業省と IPA が主導している「サプライチェーン評価制度」がまさにこれにあたり、制度の実装に期待をしたい。

（5） クラウド前提のセキュリティガイドラインと実践テンプレートの提供

多くの中小企業がクラウド活用とローカルデータ削減を進めている現状を踏まえ、クラウドサービス選定・設定のベストプラクティス、ID・アクセス管理、多要素認証、共有設定、バックアップ等に関する「クラウド前提」のガイドライン、IT 資産台帳の作成・更新をクラウド環境に対応させたテンプレートを提供する。

これについては、既に IPA から「中小企業のためのクラウドサービス安全利用の手引き[2]」が公開されているので、参照されたい。

併せて、ASM ツールとクラウド設定診断ツールを組み合わせた「クラウド時代の攻撃面管理パッケージ」を普及させることで、オンプレ前提の対策からの転換を支援する。

---

[2] 2024 年 7 月 IPA 中小企業のためのクラウドサービス安全利用の手引き
https://www.ipa.go.jp/security/sme/f55m8k0000001wpl-att/outline_guidance_cloud.pdf

（6） 教育・啓発コンテンツと ASM 結果の連動

ASM 診断で多く検出された典型的な脆弱性（HTTP 未暗号化、メール認証未設定、Cookie 属性不備等）を題材とした、社員向け教育コンテンツ、管理者向け設定手順書、経営層向けリスク説明資料をセットで提供し、診断結果をそのまま教育・啓発に活用できるようにする。

生成 AI を活用した「自社向け教育資料自動生成」のような仕組みも組み込むことで、教育負担の軽減と継続性を高める。ただし、生成 AI の活用は効率化の反面、思わぬ情報漏えいや契約違反につながる可能性もあるため注意が必要である。

（7） ログ管理・インシデント対応力の底上げ支援

ヒアリングでは、「どこまでログを残せばよいか分からない」「3 か月でログが消えてしまい、原因究明ができない」といった課題が複数の企業で確認された。

これを踏まえ、最低限確保すべきログ種別と保管期間の目安、コストとリスクのバランスを踏まえたログ管理の標準モデル、インシデント発生時の初動対応手順（誰に連絡し、何を確認するか）を分かりやすく示す支援策が有効である。

ASM 結果とログ情報を組み合わせてインシデント兆候を検知するようなマネージドサービスの普及も、今後の方向性として重要である。

（8） 地域・業界団体を活用した「身近な相談窓口」の整備

「相談できる業者がいない」「費用対効果が分からない」といった声を踏まえ、商工会議所、業界団体、地場金融機関等と連携した地域の相談窓口、信頼できる支援事業者のリストアップ・紹介スキームを整備する。

特に、IT と経営の両面に一定の知見を持つ「中小企業向けセキュリティ・DX アドバイザー」の育成・配置は、ASM ツールを含む各種支援策の翻訳者として重要な役割を果たし得る。

以上のような支援策を、ASM ツールを中核とした診断・可視化機能と組み合わせて展開することで、中小企業のサイバーセキュリティ対策は、「何をすればよいか分からない」段階から、「最低限の対策を確実に実行できる」段階を経て、「攻撃面を意識的に管理し、継続的に改善できる」段階へと、着実に引き上げていくことが可能になると考えられる。

以上