ASM診断および事例集作成業務
実施報告書概要版

2026年　3月

独立行政法人情報処理推進機構
セキュリティセンター

IPA Better Life with IT

事業概要

事業名

- ASM診断および事例集作成業務

実施目的

- 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。
- 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診断がどのような気付き・改善行動につながるか評価する。
- 得られた知見をもとに、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的とする。

背景・課題認識

- サイバー攻撃の巧妙化・多様化が進行している。
- 中小企業では、限られたリソース・知見不足から十分な対策が取れていない。
- ASMツールにより、外部から見える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必要がある。

参加事業者募集プロセス

参加事業者の募集・選定

- 過去にASM診断を実施した約2,000社のデータベース（DB）から、
  - 従業員規模
  - 業種（製造・建設、情報通信、金融・保険、卸売・小売、医療・福祉等、5業種以上）
  - 所在地（全国6地域）

  を軸に偏りが出ないよう抽出し、参加を呼びかけ。
- 請負事業者のWeb会員・メルマガ会員・既存顧客にも案内。
- 中部経済産業局より中部エリアの企業にも声かけをしていただく。

事業説明会

- Zoomによるオンライン開催（リアルタイム1回＋アーカイブ配信）。
- 内容：事業の背景・目的、最近のサイバー攻撃状況、中小企業インシデント事例、ASM診断の説明、今後の流れ、質疑。

参加事業者・スケジュール

参加事業者属性

- 参加案内送付：1,248社
- 正式参加：126社

※偏りが出ないよう調整して選定。

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**

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**

全体スケジュール

※週次での進捗確認会議も実施。

ASM診断

使用ツール

- 「MS&ADサイバーリスクファインダー（CRF）」
- Coalition社の世界中のデータベースと独自検索エンジンを用い、外部公開資産の自動検出、脆弱性洗い出し、リスク評価、レポート自動生成を行うASMツール。

診断手順

- 参加事業者が専用Webサイトでメールアドレス登録・マイページ作成（メールドメインが診断対象）。
- 事務局からユーザー認証メール送信。
- 参加事業者が連絡先等を入力し登録完了。
- 事務局にてCRFでスキャン実施、診断レポート発行。
- 参加事業者がマイページから診断レポート（PDF）をダウンロード。

リスク評価

- 脆弱性はCRITICAL/HIGH/MEDIUM/LOWの4段階で評価。
- CVE/CVSS等の公知情報に加え、Coalition社のインシデントレスポンス・保険金支払い実績・大規模スキャンデータを統合して評価。

診断結果のフィードバック

診断結果のフィードバック方法

- 診断レポート作成完了時にメールで告知。加えて、マイページを確認しない企業も想定し、事務局から診断レポートと日本語解説資料を個別にメール添付で送付した。
- 緊急度の高いCRITICAL/HIGHが検出された企業には、脆弱性の解説と推奨対応事項を記載した資料を個別にメールで提供した。
- レポートには、
  - リスクスコア（0～100点、標準値40点）
  - 想定被害額
  - リスクレベル別の検出数
  - インターネット上の流出データ（アカウント・パスワード等）
  - 不正なソフトウェア、スパム、侵入、ハニーポット攻撃、ブラックリスト登録、違法ダウンロード通信
  - SPF/DMARC等のメール認証設定

  が記載されている。

診断により検出された主な脆弱性例

CRITICAL：

- FortiGate/Cisco/Sophos等VPNパネル露出
- DNSゾーン転送設定不備
- サポート切れMicrosoft IIS
- Gitリポジトリ露出

HIGH：

- OpenSSH RCE脆弱性（CVE-2024-6387）
- WordPress/Plesk/phpMyAdmin管理パネル露出
- Google APIキー露出、SNMP公開

MEDIUM：

- HTTP/FTP/メールの非暗号化（多数）
- 期限切れ証明書、自己署名証明書
- DB（MySQL/PostgreSQL）外部公開、ディレクトリリスティング

LOW：

- 各種セキュリティヘッダ未設定
- SPF/DMARC設定不備・緩いポリシー
- Cookie属性未設定
- AWSアクセスキーID露出 等

アンケート調査の方法と分析の要約

調査方法

- 対象：参加126社全社。
- 形式：Webアンケート（Forms）、メール案内＋リマインド、未回答企業には架電依頼。
- 回答負担軽減の工夫：選択式中心、5～10分程度、専用問い合わせ窓口設置。
- 回答結果：参加126社全社からの回答を集めることができた。

アンケート分析の要約

- ポジティブな傾向
  - インシデント経験企業ほど、ASM結果を具体的な行動（パッチ適用、多要素認証、不要サービス停止等）に落とし込んでいる。
  - 不要サービス無効化・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。
  - 支援ニーズが高度な企業ほど、「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」など具体的な要求が出ている。
- 課題となっている傾向
  - ほぼ全体で「専門人材不在」「教育不足」が課題として挙がる。
  - 経営層関与が薄い企業では、「重要な問題は検出されなかったため」「対策不要」「優先度が低い」としてASM結果を改善に結び付けない。
  - 「どちらかといえば理解できた」が多い一方で、それでも実施しない層が目立ち、壁は「コスト・時間・優先度・対象範囲の特定」にある。

ヒアリング調査の方法

調査方法

- 対象：10社
- 選定条件：アンケート回答状況、ASMスコア、脆弱性改善有無、業種・規模、インシデント経験有無、経営層関心度、取引先からの要請有無等を考慮し偏りなく選定。
- Web会議にてヒアリング調査を実施。
- 主な質問項目：
  - 決裁・意思決定プロセスとハードル（費用・人手等）
  - 実施した対策の内容・コスト・工数・工夫・課題
  - インシデントの実態（内容・被害・原因・改善策・保険加入有無）
  - 他社に伝えたい経験・ノウハウ・最初の一歩のアドバイス 等。

ヒアリング調査の要約

ヒアリング結果の横断的分析

- ポジティブな共通点
  - 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。
  - 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。
  - 生成AIを資料作成やレポート解釈に活用して効率化している事例が出ている。
- 課題の共通点
  - 「どこまでやれば十分か」の基準がない。
  - 取引先からのチェックシート・要請がバラバラで過剰、実態にそぐわない項目も多い。
  - 経営層の意識を変える情報が不足している。

業種別傾向

- 製造・建設／卸売・小売：情報システム担当を兼務する体制が標準。
- 情報通信／一部金融・保険：専任担当・技術系役員が配置され、運用レベルまで踏み込んだ対策を実施。
- 医療・福祉：外部からの具体的要求が少なく、自主的な基準づくりが課題。
- インシデント経験は製造・建設・医療・福祉で一定数あり、対策強化の契機となる例もある。一方、金融・保険・卸売・小売では「大きな被害はない」との認識も多い。
- 経営層の関心度が高い情報通信・一部製造では、ASM結果を受け具体的改善に踏み込む割合が高い。

事例集

事例集の位置づけ

- 本事業のメインメニュー：「ASM診断」「アンケート」「ヒアリング」で得られた
  - 脆弱性事例
  - 被害事例
  - 取組事例

  を計30事例に整理し、別冊「事例集」として作成。
- 目的：中小企業にセキュリティ対策の必要性を理解してもらうための「事例集」として活用することを期待。

考察①　中小企業のセキュリティ実態

全体像

- 「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」。

主なポイント

- 基本的技術対策は広く導入されつつも、HTTP/FTP/メールの非暗号化、期限切れ証明書、メール認証未設定等、設定レベルの不備が多数。
- 「既につかっていないがインターネット上に残る資産」が攻撃面の死角となっている。
- 組織的対策はポリシー等の「最低限整備」にとどまり、インシデント対応計画やサプライチェーン管理まで体系的に運用している企業は限定的。
- 「専門人材不在」「兼務体制」が標準で、EDRやログ監視を導入しても運用・分析まで手が回らない。
- 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。
- 経営層の関心度・理解度が、投資判断と対策レベルを左右。
- クラウド活用＋ローカルデータ削減へのシフトが進む一方、クラウド設定・ID管理・多要素認証など新たな課題も顕在化。

考察②　ASMツールの有効性と活用課題

ASMツールの有効性

- 外部から見える自社資産の可視化により、未把握資産・設定不備を発見。
- 不要サービス停止・サブドメイン廃止・古いAPIキー削除等、攻撃面縮小の行動変容を促進。
- 一定の対策を実施済み企業にとっては「抜け漏れ」を補完するツールとして機能。
- インシデント経験企業では、再発防止・高度化の指標として活用。
- 一部企業では生成AIと組み合わせ、レポート解釈・社内説明資料作成の効率化にも寄与。

ASM活用の課題

- レポート解釈・優先度判断を担う人材不在。
- 予算制約と費用対効果の説明の難しさ。
- 経営層関与が弱い場合、ASM結果が「やらない理由」に使われるリスク。
- 単発診断では、変化し続けるアタックサーフェスに追随できない。
- 外部ベンダーとの役割分担・契約スキームが不明確。
- 教育・啓発との連動不足。

考察③　今後の支援策の方向性

今後の支援策の方向性

- インシデント経験の有無に応じた二層型支援メニュー。
- 専門人材不在を前提とした外部支援モデル（お助け隊、マネージドセキュリティサービス（MSS）、ASM＋設定変更代行等）の標準化。
- 経営層向け情報提供・インセンティブ設計（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）。
- チェックシート・要請の標準化と負担軽減（サプライチェーン評価制度への期待）。
- クラウド前提のガイドライン・テンプレート提供と、ASM＋クラウド設定診断の組み合わせ。
- ASM結果と教育・啓発コンテンツの連動、生成AI活用時の注意喚起。
- ログ管理・インシデント対応力の底上げ支援。
- 地域・業界団体を活用した「身近な相談窓口」の整備。

本事業の総括①

中小企業の現状

- 多くの企業でウイルス対策ソフト、ファイアウォール、バックアップ等の「基本的な技術対策」は導入されている一方、
  - 非暗号化通信（HTTP/FTP/メール）
  - 期限切れ・自己署名証明書
  - メール認証（SPF/DMARC）未設定
  - 利用していないサブドメインや停止し忘れDB

  など、「見えない資産」や「設定不備」が攻撃面の死角として残存していることが明らかになった。

組織・人材面の課題

- セキュリティポリシー等は一定程度整備されているが、インシデント対応計画やサプライチェーン管理まで運用できている企業は限定的。
- 「専門人材不在」「兼務の情報システム担当者」「教育不足」がほぼ全ての層で共通課題となっており、EDRやログ監視を導入しても運用・分析に限界がある。

行動を分ける要因

- インシデント経験の有無と、経営層の関心度・理解度が、ASM診断結果を「具体的な改善行動」につなげられるかどうかを大きく左右している。

本事業の総括②

今後に向けた方向性

ASMを核とした「支援パッケージ」の必要性

- ASMツール単体ではなく、
  - レポート解釈・優先度付け
  - 設定変更・不要資産の廃止等の実務支援
  - 社員教育・経営層向け説明

  を組み合わせた外部支援モデルとして設計・提供することが重要である。

中小企業支援策への示唆

- インシデント経験の有無に応じた二層型支援メニュー、専門人材不在を前提としたお助け隊・MSS等の標準化、チェックシートの標準化やサプライチェーン評価制度との連動、クラウド前提のガイドライン・テンプレート、ログ管理・インシデント対応力の底上げ、地域・業界団体を活用した相談窓口など、本事業で整理した支援策の方向性は、今後の政策・施策設計の重要な材料となりうる。


IPA