情報セキュリティ対策支援（診断）事業の結果について

グローカルビジネスソリューションズ株式会社

2025年3月14日

GBS

事業の背景

近年、デジタル技術の普及とともに、情報セキュリティの重要性が高まっています。2022年2月には、情報セキュリティ対策が強固な大企業に直接サイバー攻撃を行わず、サプライチェーンを構成する企業等を経由して大企業を攻撃する事例が発生しています。一方で、2021年に独立行政法人情報処理推進機構が実施した全国調査によると、情報セキュリティ対策への投資を行っていないと回答した中小企業等が33%に上りました。

中小企業におけるリスクの特定は早急な課題であるとともに、事実と対策を共有していくことは重要な施策となってきています。

こうした状況を踏まえ、中小企業等のセキュリティ対策を支援するため、「情報セキュリティ対策支援（診断）事業」を実施する。

事業の進め方について

事業の概要

1

サイバー攻撃机上演習

・最新のサイバー攻撃の動向や具体的なセキュリティ強化手法等の解説
・情報セキュリティの重要性を理解するための演習を実施

2

情報セキュリティの脆弱性を専門家が診断　（10社）

・ 技術的な情報セキュリティ診断（ツールでの調査によるネットワークやインフラ基盤に対する脆弱性診断を実施）
・ 組織的な情報セキュリティ診断（IPA「５分でできる情報セキュリティ自社診断」や「リスク分析シート」を実施）

3

フォローアップ

・診断結果により、各企業に対して４回以上のフォローアップを実施し、セキュリティポリシー策定等を支援
・診断企業に対する伴走支援後、本事業終了後の改善アクションを取りまとめ、報告書を提出

サイバー攻撃机上演習

サイバー攻撃机上演習

【参加企業数】２会場（岡崎・名古屋）にて合計 64社79名が参加

01. ランサムウェア攻撃の仕組みを理解する
02. ランサムウェア攻撃からの保護方法を学ぶ
03. 攻撃シミュレーションを通じて、実際のセキュリティ対策に対する意識を高める

【演題】ランサムウェアにより社内のパソコンが感染したシナリオ

サイバー攻撃発生時の被害を軽減することが目的

参加企業様には演習を通じて危機意識を高めることができた

演習後、事業の説明会を実施

情報セキュリティの脆弱性診断 及び セキュリティ対策支援に参加する企業を募集
➢１０社を診断参加企業へ選定

情報セキュリティの脆弱性を専門家が診断

情報セキュリティ強化プロセス

選定企業１０社に対し、以下のプロセスにより、情報セキュリティ向上を目指します。

	調査	分析	報告	改善
①技術的情報セキュリティ診断	ツールを使用したネットワークやインフラ基盤に対する脆弱性診断を実施	調査結果をもとに情報セキュリティ対策上の課題と改善策を分析	分析結果を報告	報告した改善策のうち、短期的に実施可能な施策は支援 長期的な課題についてはアクションプランを提示
②組織的情報セキュリティ診断	IPA「５分でできる情報セキュリティ自社診断」や「リスク分析シート」を実施			
③フォローアップ	現状の対策状況に関するヒアリング等			

診断調査結果

調査結果①：技術的情報セキュリティ診断

脆弱性診断結果

・ツールでの調査による対象サーバの開放ポートや、
稼働しているサービスの種類およびバージョン情報の調査、脆弱性スキャンを実施

診断企業	総合評価		脆弱性評価					
	評価	コメント	緊急	高	中	低	情報	内容
A社	A	脆弱性は検出されませんでした。 被害の可能性は非常に低いですが、攻撃者に有益な情報を提供する可能性があり ます。	0	0	0	0	8	情報：NTLM認証の有効化 情報：脆弱なTLSプロトコル、暗号アルゴリズムのサポート 情報：脆弱なDiffie-Hellmanパラメータのサポート 情報：ソフトウェア名、バージョン情報の公開 情報：Content-Security-Policy（CSP）の未設定 情報：X-Frame-Optionsの未設定 情報：Referrer-Policyの未設定 情報：X-Content-Type-Optionsの未設定
B社	D	攻撃される可能性が高いため、早急な対策が必要です。セキュリティ対策の実施を強く推奨します	0	1	0	0	3	高：サポート終了したソフトウェアの利用 情報：脆弱なTLSプロトコルのサポート 情報：管理ログイン画面の外部公開 情報：HTTP Strict-Transport-Security（HSTS）の未設定
C社	A	脆弱性や設定不備は検出されませんでした。 そのため、被害の可能性は非常に低いと考えられます。	0	0	0	0	0	

調査結果①：技術的情報セキュリティ診断

診断企業	総合評価		脆弱性評価					
	評価	コメント	緊急	高	中	低	情報	内容
D社	C	攻撃の可能性が比較的高く、実害に発展する可能性がございます。セキュリティ対策を講じることを強く推奨します。	0	0	1	0	0	中：Terrapin攻撃の脆弱性
E社	A	緊急に対応が必要な脆弱性は検出されませんでした。被害の可能性は非常に低いですが、攻撃者が利用できる情報が含まれている可能性があるため、注意が必要です。	0	0	0	0	2	情報：ホストの完全修飾ドメイン名（FQDN）解決 情報：IPSEC Internet Key Exchange（IKE）バージョン２の検出
F社	A	脆弱性や設定不備は検出されませんでした。そのため、被害の可能性は非常に低いと考えられます。	0	0	0	0	0	
G社	A	脆弱性は検出されませんでした。 これは、ネットワーク機器が適切に設定され、外部からのアクセス経路が制限されているためと考えられます。この状態を維持することで、今後も高いセキュリティレベルを保つことが可能です。	0	0	0	0	0	

調査結果①：技術的情報セキュリティ診断

診断企業	総合評価		脆弱性評価					
	評価	コメント	緊急	高	中	低	情報	内容
H社	A	緊急に対応すべき脆弱性は検出されませんでした。しかし、攻撃者に有益な情報を提供する可能性があります。	0	0	0	0	1	情報：IPSEC Internet Key Exchangeバージョン2 (IKEv2) の検出
I社	C	攻撃の可能性が比較的高い脆弱性が検出されました。被害に発展する可能性がございますので、セキュリティ対策を講じることを強く推奨します。	0	0	2	1	12	中：クリックジャキングに対して潜在的に脆弱なWeb アプリケーション 中：信頼できないSSL証明書および脆弱なSSL/TLSバージョンの使用 低：SSL/TLS ディフィー・ヘルマンモジュール<= 1024 ビット（Logjam） 情報：SSL / TLS 推奨暗号スイート 情報：使用可能なHTTP メソッド（ディレクトリ毎） 情報：HTTPSサーバでのHSTS未設定 情報：Web サーバ/アプリケーションのfavicon.ico ベンダーフィンガープリンティング 情報：Web サーバで公開されている電子メールアドレス 情報：Content-Security-Policy 応答ヘッダーの未設定 情報：X-Frame-Options 応答ヘッダーの未設定 情報：その他のDNS ホスト名の検出 情報：CGI 汎用の注入可能なパラメーター 情報：IPSEC インターネットキー交換（IKE）バージョン1 の検出 情報：IPSEC Internet Key Exchange（IKE）バージョン2 の検出 情報：Web サーバのオフィスファイルインベントリ
J社	B	攻撃の可能性が比較的低い脆弱性が検出されました。被害に発展する可能性がございますので、セキュリティ対策を講じることを推奨します。	0	0	0	1	2	低：ICMP タイムスタンプリクエストのリモート日付漏洩 情報：ホスト名とIP アドレスの不整合 情報：サービスの検出

集計結果の要点

【脆弱性診断結果】

- 緊急を要する脆弱性は見つからなかったが、
  １０社中４社において、対策を必要とする脆弱性が見つかった。

- 危険度が比較的高い項目としては、サポート終了したソフトウェアの利用や、
  信頼できないSSL証明書及び脆弱なSSL/TLSバージョンの使用などの脆弱性などが見つかった。

- 脆弱性がみつかった４社以外についても、IT機器の設定ルールの整備や定期的なチェックを行っているわけではないため、いつ脆弱性が見つかっても不思議ではない運用状況であった。
  IT機器の設定ルールを整備した上で定期的な脆弱性診断を行い継続的な課題抽出や対策を行うことが求められる。

調査結果②：組織的な情報セキュリティ診断

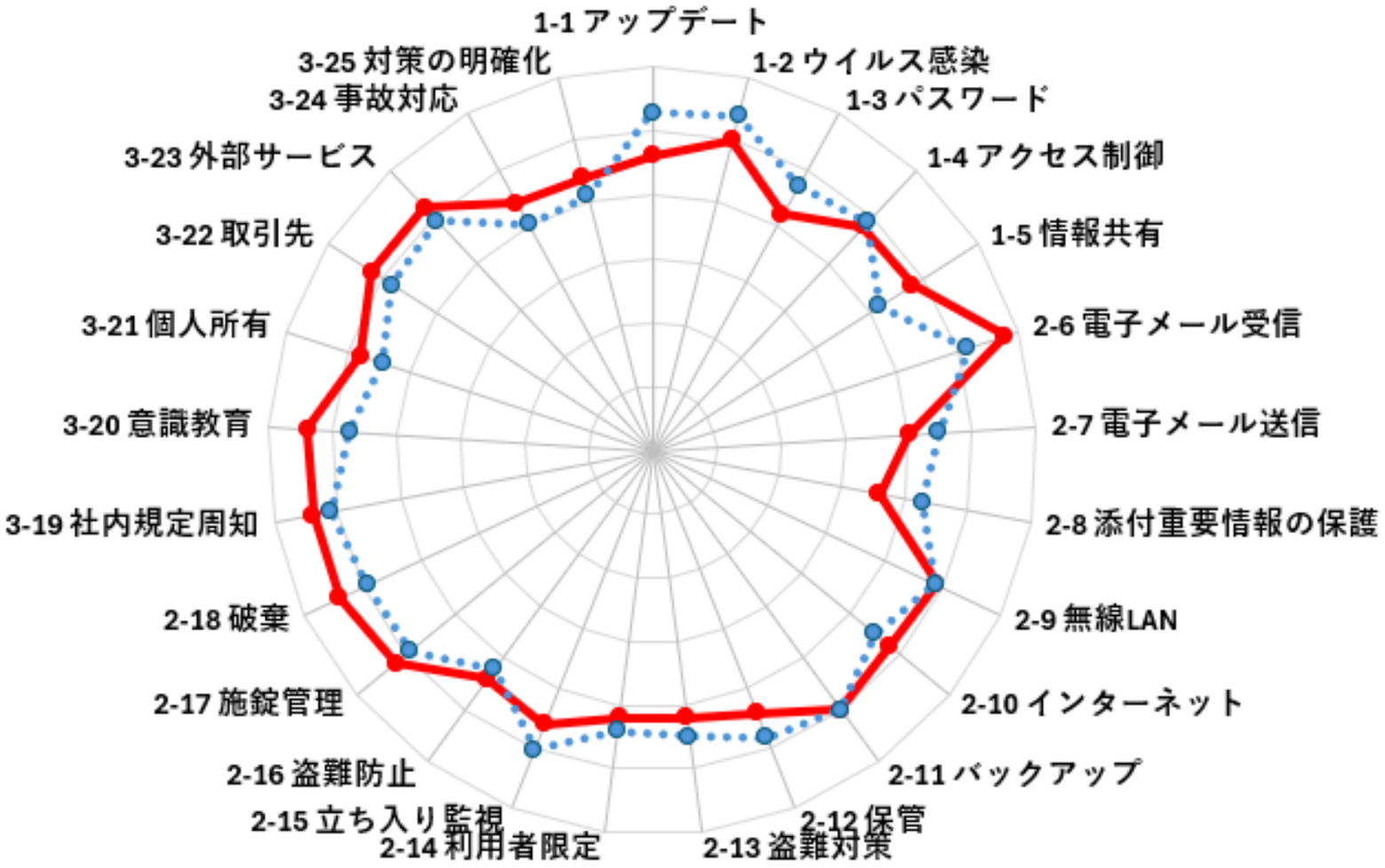
診断結果「IPA　5分でできる！情報セキュリティ自社診断」

診断項目		自社診断スコア										診断企業平均	全業種平均
		A社	B社	C社	D社	E社	F社	G社	H社	I社	J社		
基本的対策	1-1 アップデート	2点	4点	2点	4点	2点	4点	0点	2点	2点	4点	**2.60点**	3.28点
	1-2 ウイルス感染	4点	4点	4点	4点	2点	4点	0点	2点	4点	2点	**3.00点**	3.39点
	1-3 パスワード	2点	4点	0点	2点	4点	2点	2点	0点	2点	4点	**2.20点**	2.71点
	1-4 アクセス制御	4点	4点	2点	4点	2点	4点	4点	0点	0点	4点	**2.80点**	2.89点
	1-5 情報共有	4点	4点	2点	4点	4点	4点	0点	2点	0点	4点	2.80点	2.19点
従業員としての対策	2-6 電子メール受信	4点	4点	4点	4点	4点	4点	4点	2点		4点	3.78点	3.16点
	2-7 電子メール送信	2点	4点	2点	2点	2点	4点	0点	2点	0点	2点	**2.00点**	2.48点
	2-8 添付重要情報の保護	4点	2点	0点	2点	2点	2点	2点	0点	0点	2点	**1.60点**	2.29点
	2-9 無線LAN	4点	4点	4点	4点	4点	2点	4点	0点	4点	-1点	2.90点	2.88点
	2-10 インターネット	4点	4点	4点	4点	4点	4点	0点	4点	0点	0点	2.80点	2.49点
	2-11 バックアップ	4点	4点	2点	4点	2点	2点	4点	4点	2点	2点	3.00点	2.99点
	2-12 保管	4点	4点	0点	4点	2点	4点	2点	0点	0点	4点	**2.40点**	2.81点
	2-13 盗難対策	4点	4点	0点	4点	2点	4点	0点	0点	0点	4点	**2.20点**	2.50点
	2-14 利用者限定	4点	4点	0点	4点	2点	2点	2点	0点	0点	4点	**2.20点**	2.41点
	2-15 立ち入り監視	4点	4点	4点	4点	4点	4点	0点	0点	0点	2点	**2.60点**	3.01点
	2-16 盗難防止	4点	4点	4点	0点	2点	4点	2点	0点	0点	4点	2.40点	2.21点
	2-17 施錠管理	4点	4点	0点	4点	4点	4点	4点	4点	0点	4点	3.20点	2.91点
	2-18 破棄	4点	4点	2点	4点	4点	4点	4点	2点	2点	4点	3.40点	2.93点
組織としての対策	3-19 社内規定周知	2点	4点	4点	4点	4点	4点	0点	4点	4点	4点	3.40点	3.12点
	3-20 意識教育	2点	4点	4点	4点	4点	4点	2点	4点	2点	4点	3.40点	2.73点
	3-21 個人所有	4点	4点	0点	4点	4点	4点	0点	4点	0点	4点	2.80点	2.43点
	3-22 取引先	4点	4点	2点	4点	4点	4点	4点	0点	2点	4点	3.20点	2.82点
	3-23 外部サービス	4点	4点	4点	4点	4点	4点	2点	0点	4点	2点	3.20点	2.91点
	3-24 事故対応	0点	4点	0点	4点	4点	4点	0点	4点	0点	4点	2.40点	2.03点
	3-25 対策の明確化	2点	4点	0点	4点	2点	4点	0点	4点	0点	4点	2.40点	2.10点
	合計（100点満点）	**84点**	**98点**	**50点**	**90点**	**78点**	**90点**	**42点**	**44点**	**28点**	**79点**	**68.68点**	**67.67点**

調査結果②-1

今回の自社診断スコア　「全社業種」の平均スコア

診断結果のレーダーチャート



GBS

集計結果の要点

【情報セキュリティ自社診断結果】

・各社ともにセキュリティ対策の重要性を認識しているため、ルールや意識教育などが含まれる「組織としての対策」については、全業種平均を上回る結果になった。

・ツールで対策できる部分の多い「基本的対策」では、ウイルス対策ソフトが未導入の場合や、ウイルス定義ファイルが最新状態になっていなかったり、パスワードが破られやすい管理となっていた。

・「従業員としての対策」の内、電子メールの送信ミスの防止対策や添付ファイルのパスワードの未保護や書類や電子媒体等の持ち出しに対する盗難・紛失対策などについては、全業種平均を下回る項目が散見されている。

・初めて診断を実施した企業もあり、定期的な診断を行い対策を行うことが求められる。

診断後のヒアリングから抽出した課題

情報セキュリティを4つの観点から分析し課題を抽出

診断後のヒアリングを元に、分析・評価→報告

Input

・脆弱性診断
・「IPA：５分でできる情報セキュリティ自社診断」
・「リスク分析シート」
・ヒアリング

Output

・報告書
（課題と対策）
・アクションプラン
・フォローアップ

分析・評価

報告

観点

物理的環境	従業員
物理的対策	人的対策
入退管理等	セキュリティ教育等
情報システム	**社内規程**
技術的対策	組織的対策
脆弱性管理等	ポリシー整備等

ヒアリングから抽出した課題

分析・評価

No.	区分	検出事項	懸念領域	対策優先度	インパクト	発生可能性
1	人的対策	**情報セキュリティに関する教育訓練**を実施することが望まれた。	**情報セキュリティに関するルールが従業員に浸透していないと外部からの攻撃の足掛かりにされたり、内部不正、ミスを誘発する危険性がある。**	H	H	M
2	組織的対策	**委託先に対する情報セキュリティ管理**を実施することが望まれた。	**委託先が情報セキュリティ事故等を起こした場合、委託元としての監督責任を問われることがある。委託先によるセキュリティ対策が実施されずに委託先に起因したセキュリティ事故が生じるリスクが高まる。**また、委託先がセキュリティ事故を起こした際に、委託元としての管理責任を問われる危険性がある。	H	H	M
3	組織的対策	**個人PCの持ち込み管理**に関してルールの明確化が望まれる。	**不正な業務利用により、情報漏えい等につながる危険性**がある。	M	H	L
4	組織的対策	**情報資産の洗出し**を実施することが望まれた。	**自社にて管理すべき情報資産が正確に把握されないと情報資産に対するリスクが正確に把握できない危険性**がある。	H	H	M

ヒアリングから抽出した課題

分析・評価

No.	区分	検出事項	懸念領域	対策優先度	インパクト	発生可能性
5	組織的対策	情報セキュリティに関する社内規定を自工会ガイドラインへの準拠を踏まえて改定することが望まれた。	業界や発注元からの情報セキュリティに関する要求を満たせない危険性がある。情報セキュリティ対策が前提条件となりつつあるため、取引ができなくなる危険性があります。	M	H	L
6	技術的対策	セキュリティツールの導入において、費用対効果の高いツールを選定するために機能の把握と選定のための適正な評価が望まれる。	セキュリティツール選定を誤ると、必要以上の高額な支出につながる。（機能重複、オーバースペック、運用コスト増大）また機能が不足している場合、セキュリティ対策が不十分になる。	H	H	L
7	技術的対策	バックアップなどのデータ保存の仕組みについて検討することが望まれた。	システム障害、大規模災害、ランサムウェア被害等が生じた際に、事業を継続できなくなる危険性がある。	H	H	M
8	技術的対策	USBメモリや外部クラウドサービスを経由した情報の持出しについて対策が望まれた。	内部不正による情報の漏えいにつながる危険性がある。	H	H	M

フォローアップ：対策とハンズオンによる支援

対策とハンズオンによる支援

主な活動は以下の通りです。

	課題	主な活動
1	情報セキュリティポリシー（規程）のブラッシュアップ	・自工会ガイドライン対応における不足項目の抽出 ・自工会ガイドラインに対応した情報セキュリティポリシーの助言 ・情報セキュリティポリシーの見直し、策定 ・個人情報保護の規定を作成 ・課題や弱点に対してルールを検討し、現状の規程にルールを反映
2	従業員教育	・従業員への情報セキュリティ教育実施（集合型研修） ・インターネット閲覧に関する従業員への注意喚起を助言 ・従業員に対して行う情報セキュリティ教育用資料の見直し
3	情報資産の洗出し	・情報資産台帳を作成支援
4	データ管理の強化	・データの保管方針を助言（提案）

対策とハンズオンによる支援

主な活動は以下の通りです。

	課題	主な活動
5	バックアップ方針の 妥当性検証	・バックアップの方針（手順）について、 ベストプラクティスとなる他社事例を収集・共有 ・他社事例と照らし、自社のバックアップ方針の見直しの要否を判断
6	委託先管理の実施	・委託先に対するセキュリティ要求事項の明確化 ・委託先を管理する管理表やチェックシート、委託情報資産に関わる覚書の提供 ・秘密保持契約書のレビューと更新
7	情報区分と取り扱いルール	・情報の取扱い区分について助言
8	セキュリティツールの導入	・ツールの導入に関する方針作成の支援

まとめ

（１）基本方針、対策基準、規定の策定支援

　参加企業の半数において、対策基準や規定の策定に不備がある状況であった。これらの企業は自力では、対策を行う人的リソースや知見を持ち合わせていないため、自社だけで対策を行うのは困難であり継続的な支援が必要な状況にある。

　参加企業はセキュリティに対する意識は高いレベルにあったにも関わらず、半数の企業において対策が必要なレベルにある現状を考えると、県内全体でも同じ課題を持つ企業が全体の半数いることが想定されることから、IPAのガイドラインの策定支援、横展開を図るという取組は一定のニーズがあり継続することが重要である。

（２）情報セキュリティ教育

　全ての参加企業がセキュリティ対策の重要性を認識しているため、ルールや意識教育などが含まれる「組織としての対策」については、全業種平均を上回る結果になった。一方で「破られやすい単純なパスワードを設定」「電子メールの添付ファイルの保護」「アップデート漏れ」など、セキュリティの基本事項について対策できていないケースもあり、教育の継続性や教育内容の網羅性がないという課題が見受けられる。

　前述の通り、参加企業は対策の重要性については理解しているので、定期的なセミナーの開催やメールでの注意喚起など、教育を継続することの重要性を常に意識させるような機会を提供することが有効と思われる。

まとめ

（３）対策ツールの活用

診断結果の評価が高い企業においてもツールで対策できる部分の多い「基本的対策」「従業員としての対策」について全業種平均を下回る診断結果となっている。フォローアップ時のヒアリングからは情報システム担当者は対策ツールで対応できることを理解しているが、必要性や重要性を経営者に対して説明できずツールを導入できていないケースが多くみられた。

警察庁「令和6年上期におけるサイバー空間の脅威情勢について」によると、直近のランサムウェアの被害件数114件のうち、中小企業が被害あった件数は73件と64％を占めており、中小企業においてもセキュリティ対策が必須の状況にある。

中小企業の経営者層向けのセキュリティセミナーを定期的に開催しセキュリティ対策に投資することの必要性を経営者自身が認識する機会を提供することが、今後の中小企業のセキュリティレベル向上に必要な施策と考える。

（４）技術的診断の定期的な実施

参加企業全てにおいて、ネットワーク及びサーバーの構築やセキュリティ対策の対応をSier（システムの開発や運用を請け負う企業）に一任しており、設定内容や変更方法を理解せず運用している企業や設定内容は理解しているものの脆弱性が指摘されている古いバージョンのまま利用している企業もあった。

ISMS(情報セキュリティマネジメントシステム)の新規格で要求事項に脅威インテリジェンスの導入が追加されたように、脅威情報を収集し、常に自社のセキュリティ対策の課題をみつけ対策を行う必要性が高まっている現状と社内に専門化がいない中小企業の運用体制を考えると、定期的な脆弱性診断を行い自社の課題を発見、対処することは投資対効果の面で有効な施策であると考える。

GBS

グローカルビジネスソリューションズ株式会社

IS 780237 / ISO 27001