事務所ニュース News
2026.5
K-081

経営バイタルの強化書 KEIEI VITAL

中小企業の情報セキュリティ対策方法を確認しましょう!

中小企業の情報セキュリティ対策ガイドライン

中小企業の情報セキュリティ対策の確認と経済産業省及び内閣官房国家サイバー統括室が推進する、「サプライチェーン強化に向けたセキュリティ対策評価制度」について確認しておきましょう!

1 中小企業の情報セキュリティ対策ガイドライン

独立行政法人情報処理推進機構（IPA）は、3月27日、中小企業向けに情報セキュリティ対策の考え方や、段階的に実現するための方策を紹介する「中小企業の情報セキュリティ対策ガイドライン」を改訂し、第4.0版を公開しました※。

「中小企業の情報セキュリティ対策ガイドライン」（以下「ガイドライン」）は、情報セキュリティ対策に取り組む際の、(1)経営者が認識し実施すべき指針、(2)社内において対策を実践する際の手順や手法をまとめたもので、経営者編と実践編から構成されており、個人事業主、小規模事業者を含む中小企業（以下「中小企業等」）の利用が想定されています。

今回の改訂（第4.0版への改訂）では、基本的な構成を維持しつつ、最新の環境変化を反映し、企業が適切な情報セキュリティへの認識と実践的な対策を進められるよう、記載内容の見直しが行われています。

2 ガイドライン改訂のポイント

今回の改訂の主なポイントは、大きく下記の3点となっています。

①「バックアップを取ろう!」を追加し情報セキュリティ6か条へ

中小企業がはじめに取り組んでほしい情報セキュリティ5か条に「バックアップを取ろう!」を新たに追加し、情報セキュリティ6か条とし、また「5分でできる! 情報セキュリティ自社診断」の診断項目に、「外部から内部ネットワークへの不要な通信を遮断する」、「ウェブサイトを安全に運用する」を新たに追加する等が行われました。

②「サプライチェーン強化に向けたセキュリティ対策評価制度」の基本的な考え方を取り込む

経済産業省および内閣官房国家サイバー統括室が検討を進める「サプライチェーン強化に向けたセキュリティ対策評価制度（以下、SCS評価制度）」の基本的な考え方に沿った内容となりました。

③「中小企業のための人材確保・育成の実践ガイドブック」を付録として追加

2025年5月に公表された「中堅・中小企業が実施するセキュリティ対策に応じた人材確保・育成の実践的方策ガイドβ版」（経済産業省「サイバーセキュリティ人材の育成促進に向けた検討会」で提示）を踏まえ、中小企業のセキュリティ人材の確保・育成を支援する方策および取組事例が付録として追加されました。

ガイドラインでは、各企業が目指しているセキュリティレベル（成熟度）により、4つのSTEP（STEP1 必要最低限の対策、STEP2 自社の弱み把握と基本的対策、STEP3 組織的な取り組み強化と防御対策、STEP4 高度で広範囲な技術的・包括的取組）が定められており、各企業の方針等により目指すべき取組の範囲を選択できるようになっています。また、各STEPについて、「取組の目安」や「想定している企業の例」が記載されているため、自社の現在の立ち位置を見極め、目指すべき姿を決めたうえで、取り組むSTEPを選択して、実施することができるようになっています。

3 ガイドラインの活用方法

ガイドラインを活用することで、自社の事業の特徴に応じた情報セキュリティ対策を段階的に進めていくことができます。まず、「第1部経営者編」を確認し、取り組むべき情報セキュリティ対策全体像を把握します。次に「第2部実践編」で具体的な対策を行います。

●取り組むべき情報セキュリティ対策全体像の把握

「第1部経営者編」には、経営者が認識すべき「3原則」と実行すべき「重要7項目の取組」が記載されています。まず、経営層が取り組むべき情報セキュリティ対策の全体像を把握し、担当者に任せきりにすることなく、経営者が自社の情報セキュリティについて明確な

裏面へ続く→

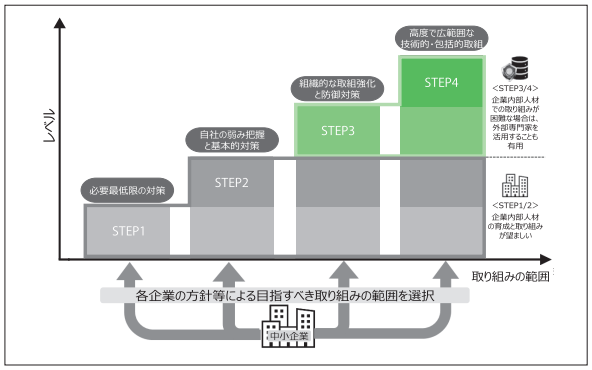
方針を示すとともに自ら実行していくことが必要となります。具体的な対策の実践に当たっては実践編を活用して行うとよいでしょう。

●具体的な対策(第2部実践編の活用)

ガイドラインでは、各企業が目指しているセキュリティレベル(成熟度)により、具体的な対策を行うための4つのSTEPが定められています。

4つの対策とは、**STEP1**(必要最低限の対策)、**STEP2**(自社の弱み把握と基本的対策)、**STEP3**(組織的な取組強化と防御対策)、**STEP4**(高度で広範囲な技術的・包括的取組)となっています。

【図1】情報セキュリティ対策の4つのSTEP



各STEPの取り組みの目安は、

STEP1(必要最低限の対策)

すべての企業が実施すべき基本的なセキュリティ対策であり、「情報セキュリティ6か条」を活用し、自社の業務・情報・従業員・取引先を守る必要最低限の対策から始めます。

STEP2(自社の弱み把握と基本的対策)

基本的なセキュリティ対策を組織的に取り組むために、「5分でできる! 情報セキュリティ自社診断」を活用し、自社の弱みを把握し基本的対策を決定するとともに、組織としての情報セキュリティ基本方針を作成します。

STEP3(組織的な取組強化と防御対策)

組織的な取り組みを強化し、セキュリティ対策に本格的に取り組む企業は、必要に応じて外部専門家を交え、セキュリティに関する体制を整備し、基本的な組織的対策や技術的な防御対策を実施します。

STEP4(高度で広範囲な技術的・包括的取組)

より強固で広範囲なセキュリティ対策のためには、人的・組織的な対策だけでなく、必要に応じて外部専門家を交えてリスク分析を行い、技術的な対策の強化により包括的なセキュリティ対策を実施します。

各STEPで必要な対策の実行に必要な人材の確保と育成については、「中小企業のためのセキュリティ人材確保・育成の実践ガイドブック」(中小企業の情報セキュリティ対策ガイドライン付録1)の解説を参照するとよいです。

4 「サプライチェーン強化に向けたセキュリティ対策評価制度」(SCS評価制度)への準備

経済産業省及び内閣官房国家サイバー統括室が推進する、「サプライチェーン強化に向けたセキュリティ対策評価制度」(以下「SCS評価制度」という)とは、企業のセキュリティ対策レベルを★3(専門家確認付き自己評価)、★4(第三者評価)で評価する仕組みです。主に中小企業の信頼性向上やサプライチェーン対策強化を目的として、2026年度下期の制度開始を目指して整備が進められています。

SCS評価制度で設けられている段階の考え方は、

★3…全てのサプライチェーン企業が最低限実装すべきセキュリティ対策として、基礎的な組織的対策とシステム防御策を中心に実施

★4…サプライチェーン企業等が標準的に目指すべきセキュリティ対策として、組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施

となっています。

★3、★4相当のサイバーセキュリティ対策を行うことで、サプライチェーン強化に向けたセキュリティ対策を実施済みの企業または先進的な企業として自社が認知されることになり、その結果、高いセキュリティレベルと運用力を客観的に示すことができ、取引先・顧客からの信頼向上、取引機会の拡大にも繋がります。

●中小企業の情報セキュリティ対策ガイドライン(付録5)

ガイドラインの付録として提供されている「情報セキュリティ関連規程(サンプル)」(付録5)では、情報セキュリティの具体的な対策(組織的対策、人的対策、物理的対策、技術的対策)や、策定した規程とSCS評価制度の要求事項との対比が記載されているため、参照しながら、具体的な対策を検討するとよいでしょう。

※ 中小企業の情報セキュリティ対策ガイドライン(IPA)
(URL:https://www.ipa.go.jp/security/guide/sme/about.html)

【図2】情報セキュリティ関連規程(サンプル)とSCS評価制度要求事項対応表

項番	目次	SCS評価制度 要求事項
1	組織的対策	
1-1	情報セキュリティのための組織	1-2-1 セキュリティ推進活動部門
1-2	情報セキュリティ取組みの監査・点検/点検	1-4-1 セキュリティ対策推進計画
1-3	情報セキュリティに関する情報共有	1-2-2 サイバー攻撃の監視・分析体制
1-4	情報セキュリティ基本方針の策定・管理	1-3-1 セキュリティ対応方針の策定
1-5	情報資産・IT資産の管理	2-1-1 取引先とのビジネス又はシステム上の関係 3-1-1 情報機器、OS及びソフトウェアに関する情報の把握 3-1-4 機密区分に応じた情報の管理 4-1-9 可搬媒体の制限 4-3-1 データの暗号化 4-3-2 データの保管ルール 4-3-3 取引先との情報共有ルール
1-6	アクセス制御及び認証	4-1-1 ユーザIDの管理手続 4-1-2 管理者IDの管理手続 4-1-3 認証の強度・実装方法の決定 4-1-4 アカウントロック制御 4-1-5 パスワード設定ルール 4-1-6 パスワード管理ルール 4-1-7 アクセス権の管理ルール
1-7	インターネットの利用	
1-8	委託管理	2-1-1 取引先とのビジネス又はシステム上の関係 2-1-2 機密情報の取扱い 2-1-3 取引先のセキュリティ対策状況 2-1-4 セキュリティインシデント発生時の役割・責任 2-1-5 機密情報の回収・破棄 4-3-3 取引先との情報共有ルール
1-9	情報セキュリティインシデント対応及び事業継続管理	5-2-1 セキュリティインシデントのレベルごとの対象範囲 6-1-1 インシデント対応手順
2	人的対策	
2-1	雇用条件	1-2-3 守秘義務のルール
2-2	従業員の責務	1-2-3 守秘義務のルール
2-3	雇用の終了	1-2-3 守秘義務のルール
2-4	情報セキュリティ教育	4-2-1 セキュリティの意識向上のための教育・研修 4-2-2 セキュリティインシデント発生時の教育・訓練
2-5	人材育成	
2-6	テレワークにおける対策	3-1-5 リモートワークにおけるルール
3	物理的対策	
3-1	入室権限およびセキュリティ領域	4-1-8 サーバ設置エリアへの入退室管理
3-2	関連設備の管理	
3-3	セキュリティ領域内注意事項	
3-4	搬入物の受け渡し	
3-5	クリアデスク・クリアスクリーン	
3-6	廃棄・返却・譲渡	
4	技術的対策	
4-1	アクセス制御及び認証に関する標準設定等	
4-2	IT機器利用	4-4-4 セキュリティパッチ・アップデートの手続 4-4-5 マルウェア感染からの保護
4-3	IT基盤運用管理	3-1-1 情報機器、OS及びソフトウェアに関する情報の把握 3-1-2 ネットワークに関する情報の把握 3-1-3 外部情報サービスの管理 4-4-1 情報機器、OS及びソフトウェアの安全な構成 4-4-3 ログの取得 4-4-4 セキュリティパッチ・アップデートの手続 4-5-1 ネットワーク境界防護 5-1-1 ネットワーク接続・データの監視 5-1-2 情報機器及びソフトウェアの挙動監視
4-4	バックアップ	4-3-4 適切なバックアップ
4-5	リストア手順	7-1-1 事業継続要件に沿った復旧準備
4-6	システム開発及び保守	3-2-1 脆弱性の管理体制 4-4-2 サポート期限の切れたOS及びソフトウェアへの対策

※本対応表は要求事項(2027年3月公開)を基に作成しています。