

「中小企業の情報セキュリティ対策ガイドライン」を公開

IPA（独立行政法人情報処理推進機構、理事長：西垣 浩司）は、中小企業の情報セキュリティ対策に関する検討を行い、より具体的な対策を示す「中小企業の情報セキュリティ対策ガイドライン」を公開しました。<http://www.ipa.go.jp/security/fy20/reports/sme-guide/index.html>

1. 概要

近年の情報化の進展は中小企業にも大きな影響を与え、電子メールでの受発注、財務会計システムの導入による経理業務の効率化、会社のWebサイトを立ち上げての営業活動など、様々な業務でITが活用されています。その反面、例えばコンピュータウイルス感染による顧客データや文書ファイルのインターネットへの流出・漏えいや、情報システムの停止、データの破壊等が発生した場合、顧客からの信頼を大きく失墜することとなるため、中小企業であっても、情報セキュリティ対策に自社の問題として取り組むことが必要となります。

しかし、従来の情報セキュリティ対策の進め方では、リスク分析を基にして、自社に合った対策基準や実施手順を策定することが必要であり、対策未実施の中小企業にとって導入に着手することは容易ではなく、「何をすれば良いか分からない」という状況になる場合があります。

そこでIPAは、中小企業の情報セキュリティ対策として実施すべき具体的な対策事項を選択抽出し、「中小企業の情報セキュリティ対策ガイドライン」としてまとめました。その中でも、特に最初に取り組むべき項目を、下記2種類の別冊ガイドラインとしてまとめました。

- ・5分でできる自社診断シート（「中小企業の情報セキュリティ対策ガイドライン」別冊3）
- ・中小企業における組織的な情報セキュリティ対策ガイドライン（同 別冊2）

また、個人情報や営業秘密など、情報管理の重要性への意識が高まってきており、中小企業であってもサービス業や製造業などは、取引先より情報セキュリティ対策の実施を求められることが多くなってきています。しかし、守るべき機密情報そのものや、その取り扱い方が業務委託時に明確にされていない場合も多く、発注者と受注者それぞれの対策事項が明確でない取引が行われていることから、IPAは「業務委託契約に係る機密保持条項（例）」および「委託先における情報セキュリティ対策事項」についても、下記の別冊ガイドラインとしてまとめました。

- ・「委託関係における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ガイドライン」別冊1）

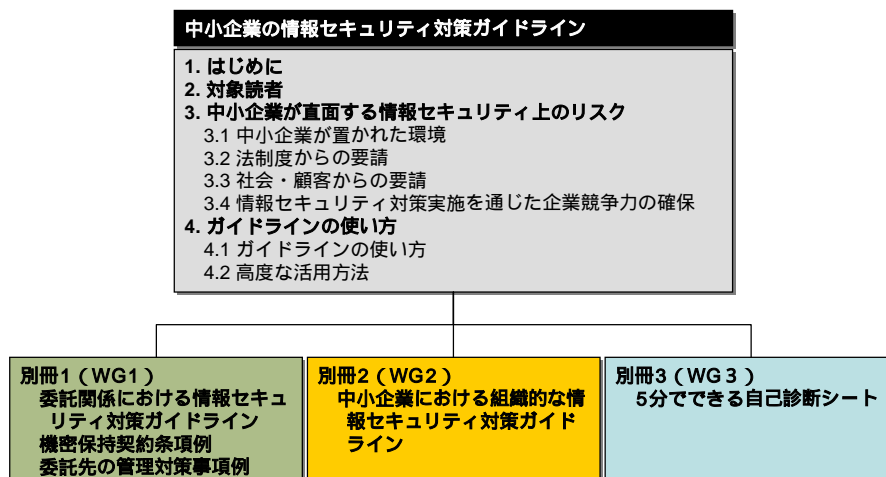


図1. 中小企業の情報セキュリティ対策ガイドラインの構成

2. ガイドラインの内容

1) 5分でできる自社診断シート

「5分でできる自社診断シート」は、中小企業にとって、情報セキュリティ対策が難しいと考えられている要因の一つとして、リスク分析が挙げられることから、最低限実施すべき情報セキュリティ対策を25項目に絞り、経営者や管理者のための自主点検表として作成したものです。



図2. 「5分でできる自社診断シート」

2) 中小企業における組織的な情報セキュリティ対策ガイドライン

「中小企業における組織的な情報セキュリティ対策ガイドライン」は、個人情報や取引先の機密情報を保持し、情報漏えい等でこれらの情報が流出する可能性のある中小企業を対象に策定しました。

中小企業においても、一定のコストをかけて情報セキュリティ対策を行う必要がありますが、中小企業の種類の多さ（規模、業種等）を考えると、具体的にどのような対策を行うべきかについて、一律の基準を示すことは困難です。そのため、本ガイドラインでは“中小企業であれば共通して実施すべき対策”と、“企業毎にそれぞれの特徴を考慮して実施すべき対策”の2つに分けて検討を行いました。共通して実施すべき対策のみでも効果があると考えますが、十分な対策とするためには企業毎に考慮すべき対策についても検討を行い、必要な対策を実施することが望まれます。

- ・4.1 情報セキュリティに対する組織的な取り組み
 - ・ 4.1.1 情報セキュリティに関する経営者の意図が従業員に明確に示されている。
 - 経営者が情報セキュリティポリシーの策定に関与し、実現に対して責任を持つこと。
 - 情報セキュリティポリシーを定期的に見直しすること。
 - ・ 4.1.2 情報セキュリティ対策に関わる責任者と担当者を明示する。
 - 責任者として情報セキュリティと経営を理解する立場の人を任命すること。
 - 責任者は、各セキュリティ対策について（社内外を含め）、責任者、担当者それぞれ役割を具体化し、役割を徹底すること。
 - ・ 4.1.3 管理すべき重要な情報資産を分類する。
 - 管理すべき重要な情報を、他の情報と分類すること。
 - 情報資産の管理者を定めること。
 - 重要度に応じた情報の取り扱い指針を定めること。
 - 重要な情報資産を利用できる人の範囲を定めること。
 - ・ 4.1.4 重要な情報については、入手、作成、利用、保管、交換、提供、消去、破壊における取り扱い手順を定める。
 - 各プロセスにおける作業手順を明確化し、決められた担当者が、手順に基づいて作業を行っていること。



図3 組織的な情報セキュリティ対策ガイドライン（一部）

3) 委託関係における情報セキュリティ対策ガイドライン

業務委託において、機密情報を提供する際に、提供元から提供先に対して、機密情報の指定や、その保持に必要な情報セキュリティ対策の具体的な実施内容が示されない場合があります。そのような状況では、機密情報の漏えいを防止する適切な対策の実施は期待できません。

「業務委託契約に係る機密保持条項(例)」は、取引基本契約書や売買契約書、発注書等を通じておこなわれる機密情報の取扱いに係る事項を、委託元が行うべき事項も含めてまとめたものです。

さらに、委託先企業が実施する情報セキュリティ対策事項について、企業で実際に使用している事例を収集し、具体的な対策事項の例として「委託先における情報セキュリティ対策事項」を策定しました。

委託元は、本資料を参考として、委託先と協議のうえ、機密情報の指定およびその保持に必要とされる情報セキュリティ対策の具体的な実施内容を明示することが望まれます。

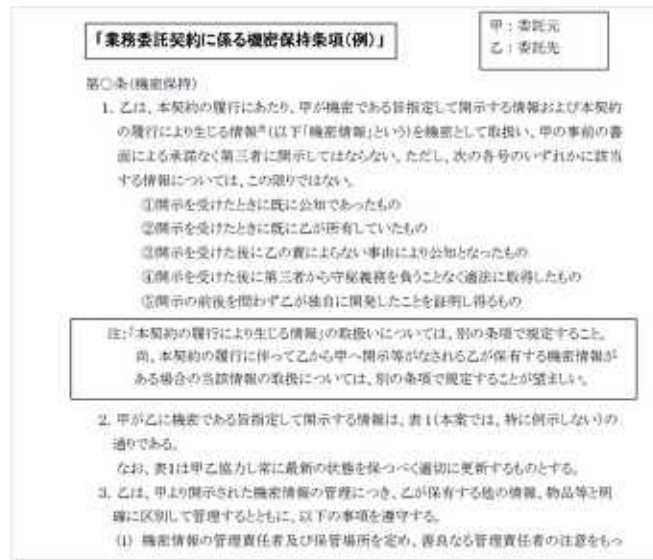


図 4-1 業務委託契約に係る機密保持条項(例)

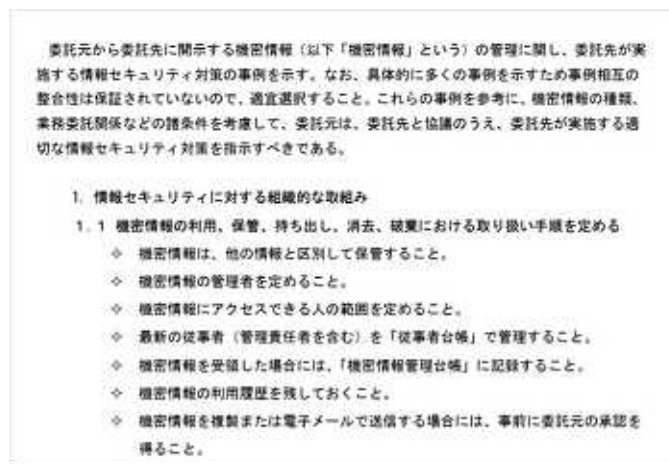


図 4-2 委託先における情報セキュリティ対策事項

3. ガイドラインの使い方

自社で情報セキュリティ対策を実施する場合、まず「5分でもできる自社診断シート」で最低限のセキュリティ対策事項をチェックし、それを満たした場合は、「組織的な情報セキュリティ対策ガイドライン」を実施します。さらに対策が必要と判断した場合は、ISMS等を用いることで最適な情報セキュリティ対策を策定し実施します(図5左)。委託元としての立場の場合は、「委託関係における情報セキュリティ対策ガイドライン」を参照します(図5右)。

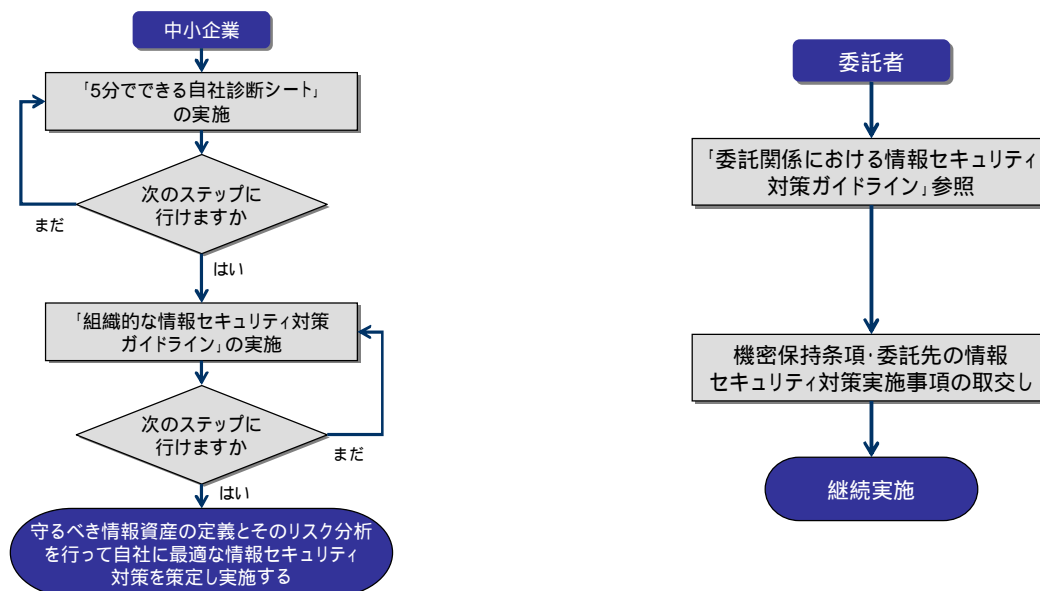


図5. ガイドラインの使い方

本ガイドラインの使用方法は、必ずしもこのような使い方に限定されるものではありません。例えば、委託元からセキュリティ対策を求められた際に「組織的な情報セキュリティ対策ガイドライン」を活用することや、「組織的な情報セキュリティ対策ガイドライン」の補足として「5分でできる自社診断シート」の活用も考えられます（図6）。

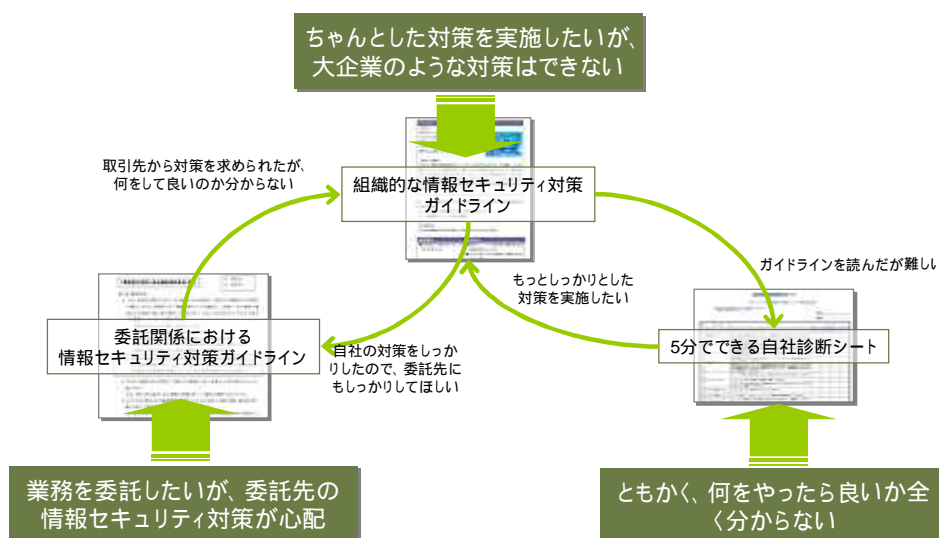


図6. ガイドラインの様々な活用方法

本ガイドラインの詳細は以下の URL をご参照ください。

「中小企業の情報セキュリティ対策ガイドライン」

<http://www.ipa.go.jp/security/fy20/reports/sme-guide/index.html>

本内容に関するお問い合わせ先
 IPA セキュリティセンター 石井
 Tel: 03-5978-7508 Fax: 03-5978-7518 E-mail: isec-info@ipa.go.jp
報道関係からのお問い合わせ先
 IPA 戦略企画部広報グループ 横山 / 大海
 Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: pr-inq@ipa.go.jp