中小企業の情報セキュリティ対策
ガイドライン

平成 21 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

目　次

1．はじめに

近年の情報化は、中小企業における業務にも、程度の差こそあれ大きな影響を与えている。例えば、電子メールで顧客からの注文を受けたり、財務会計システムを導入し経理業務の効率化を図ったり、営業報告をワープロで作成したり、会社の HP を立ち上げることで営業に繋げるなど、様々な形で IT が業務の中で活用されている。

従って、情報システムが停止したり、データが壊れたりすることは、中小企業においても業務に大きな影響を与える。また、例えばコンピュータウイルスに感染することで、顧客名やメールでやり取りしていた文書ファイルがインターネットに流出・漏えいする事件などが起こると、顧客からの信頼は大きく失墜してしまう。このように、中小企業であっても、自社の問題として情報セキュリティに取り組むことが必要である。

さらに、サービス業や製造業などでは、中小企業ではあっても、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る。これは、企業規模によらず、個人情報や営業秘密を委託する際の情報管理の重要性への意識が高まってきていることが背景にある。このような企業では、好むと好まざるとによらず、情報セキュリティ対策に取り組むことが求められる。

一方で、中小企業は大企業に比較すると、資金面や人材面での制約から情報セキュリティ対策の実施が難しいといわれてきた。実際の統計からも大企業に比較すれば対策が進んでいない傾向が見て取れる。

しかしながら、中小企業は情報セキュリティ対策を行う上で有利な条件を持っている。それは、経営者を含め「従業員の顔が見える」ということである。情報セキュリティの第一歩は、経営者が情報セキュリティの重要性を自ら認識し、そのことを従業員に伝え、従業員が情報セキュリティ対策を行う意義を理解することである。つまり、「従業員の顔が見える」ということは情報セキュリティ対策を実効的にするためには、この上ない有利な条件なのである。また、この特質を生かすことで、「費用のかからない」対策を実現することもできる。

本ガイドラインは、中小企業に求められる情報セキュリティ対策を、中小企業ならではの視点から実現するための方策を紹介するためのものである。

2.対象読者

本ガイドラインの想定読者は、中小企業の経営者及び中小企業の情報セキュリティ管理者を想定する。なお、ここで情報セキュリティ管理者とは IT 管理者だけではなく、総務・企画部門などで情報管理を担当する者も含む。

また、中小企業に対して業務を委託する企業（大企業・中小企業を問わない）の契約担当者も対象とする。

■中小企業とは

中小企業基本法第２条第１項による中小企業の法令上の定義では下表のようになる。資本金か従業員のどちらか一方がこの定義を満たせば中小企業と判断される。なお、中小企業金融公庫法等の中小企業関連立法においては、政令によりゴム製品製造業（一部を除く）は、資本金 3 億円以下または従業員 900 人以下、旅館業は、資本金 5 千万円以下または従業員 200 人以下、ソフトウェア業・情報処理サービス業は、資本金 3 億円以下または従業員 300 人以下、を中小企業として定義している。

	製造業	卸売業	小売業	サービス業	その他産業
資本金	3 億円以下	1 億円以下	5 千万円以下	5 千万円以下	3 億円以下
従業員	300 人以下	100 人以下	50 人以下	100 人以下	300 人以下

3.中小企業が直面する情報セキュリティ上の課題

3.1.中小企業が置かれた環境

中小企業の情報セキュリティ対策を考えるときに、中小企業に比較的多く見られる問題と、企業一般の問題に分けて考えることができる。

中小企業に比較的多く見られる問題としては、以下のようなものがある。

- 大企業に比較して情報セキュリティ対策にかけるリソース（人・物・金）に制約がある
- 大企業に比較して情報化が進んでいない
- 情報化もしくは情報セキュリティを進める動機がない

これらの問題について、一般的な解決策はなく、また必ずしも解決しなければならない問題ともいえないが、電子メールやウェブなどインターネットに繋がったサービスを使う以上は、他人に迷惑を与えないという意味で、最低限の対策は必要である。

一方で、企業一般の問題であって、中小企業にも大きな影響を与える問題としては、以下のようなものがある。

- 情報セキュリティ対策実施を通じた企業競争力の確保

- 法制度からの要請
- 社会・顧客からの要請

以下では、これらについて詳しく見ていく。

3.2.情報セキュリティ対策実施を通じた企業競争力の確保

外部からの要請を考慮して情報セキュリティ対策を実施することは重要であるが、一方で、情報セキュリティ対策を通じて企業競争力の向上やコスト削減につなげることができる。具体的な例としては、以下のような事例がある。

- A 社では情報セキュリティ推進のため、不用な情報資産の洗い出しを進めた結果、書類の保管スペースの削減や、サーバー台数の削減ができた。
- 顧客から重要な情報を預かる B 社は、高度な情報セキュリティ対策を実施し、ISMS 認証を取得することで、顧客からの信頼が高まった。

3.3.社会・顧客からの要請

社会・顧客からの要請とは、自社の必要性に基づくものでも、法律で規定されたものでもなくても、社会一般に期待されるレベルの対策の実施が求められたり、あるいは、顧客との契約などで対策が求められるような場合である。

社会の期待レベルは明確に定められたものではなく、また対策を行っていない事をもって直ちに問題が起こるものではない。しかし、一旦、情報セキュリティに関する事故が起きた場合、近年では、社会的な指弾を受ける傾向が強まっていると考えられる。特に、社会一般に期待されるレベルの対策の実施を怠っていた場合は、場合によっては経営に響く事態になりかねないことは、認識する必要がある。

次に、顧客からの要請とは、簡単に言えば委託関係の中で情報セキュリティ対策の実施が求められることである。IPA の調査によれば、委託関係のある中小企業の実に 2/3 が情報セキュリティ対策を求められたことがあると回答している。

3.4.法制度からの要請

法制度からの要請というのは、簡単に言えば、法律を遵守するために情報セキュリティ対策が必要となる場合である。

法律を遵守するために情報セキュリティ対策が必要となる場合とは、主に以下のような場合がある。

- 個人情報保護法：個人情報の安全管理（情報セキュリティ対策）が義務付けられる
- 会社法：内部統制システム（情報セキュリティも含まれる）の構築の基本方針を決定する
- 金融商品取引法：財務報告に係る内部統制（情報セキュリティも含まれる）を評価し、内部統制報告書として作成・提出する

これらの法律は、主に大企業を想定した法律であるが、中小企業でも該当する場合もある。また、直接該当しない場合でも、情報の委託先として、大企業の子会社として、あるいは重要な事

業拠点として、法律に基づく管理の対象となる場合があることに注意する必要がある。

例えば、個人情報保護法では、個人データを 5000 人分以上持っていない事業者は、「個人情報取扱事業者」としての義務を負わないため、自社としては個人情報をあまり持っていない企業は法律上の義務を負わない。しかし個人情報保護法では同時に、個人情報を委託した場合、委託元に監督責任があると規定している。従って、取引先から個人情報の委託を受けるような事業者は、個人情報保護法に基づく安全管理措置（情報セキュリティ対策を含む）を実施しなければならなくなる。

4.ガイドラインの使い方

4.1.ガイドラインの使い方

本ガイドラインは、本編の他、3 冊の別冊から構成されている（図 1）。

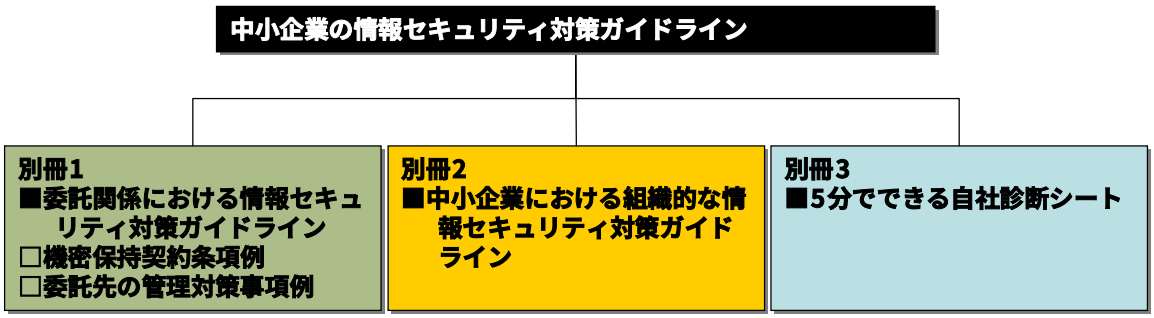

図 1. ガイドラインの構成

別冊 1 は、情報セキュリティに配慮した適正な取引を促進するための、「委託関係における情報セキュリティ対策ガイドライン」である。別冊 1 の主な想定読者は、中小企業等に業務委託をする企業の担当者である。これは、委託元が情報セキュリティ対策の具体的な実施内容を指定しないことが、責任関係の曖昧さに繋がり、結局のところ立場の弱い委託先が多くの義務と責任を負うことに通じるためである。特に中小企業は弱い立場におかれやすいと考えられる。

別冊 2 は、中小企業の情報セキュリティ対策を底上げするための、「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（組織的な情報セキュリティ対策ガイドライン）」である。これは、一定以上の情報セキュリティ上のリスクに曝されており、また、一旦情報漏えい等の事故が発生した場合、自社の業務に影響が及ぶだけでなく、取引先などに対しても大きな迷惑をかける可能性のある中小企業を主な対象としている。

別冊 3 は、同様に、中小企業の情報セキュリティ対策を底上げするための、「5 分でできる自社診断シート」である。これは、中小企業一般の情報セキュリティ対策の入り口として、最低限実施すべき情報セキュリティ対策を経営者か管理者が自主点検するためのものである。

以上をまとめると、図 2 のようになる。

まず最初に、読者が中小企業自身（図 2 左）か、委託元としての立場（図 2 右）なのかで 2 通りに別れる。

読者が中小企業自身の場合は、まず別冊 3 の「5 分でできる自社診断シート」を実施し、十分に対策が出来たと判断した場合は、別冊 2 の「組織的な情報セキュリティ対策ガイドライン」を実施する。さらに十分に対策が出来たと判断した場合は、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する（図 2 左）。

読者が委託元としての立場の場合は、別冊 1 の「委託関係における情報セキュリティ対策ガイドライン」を参照する（図 2 右）。

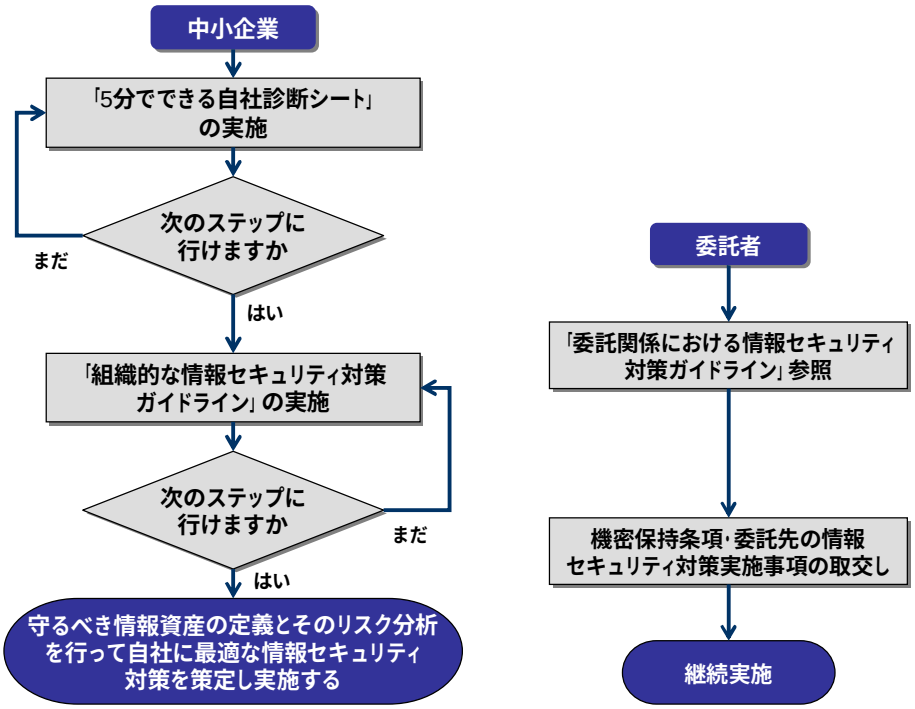

図 2. ガイドラインの使い方

4.2.高度な活用方法

本ガイドラインの基本的な使用方法は 4.1 で示したが、必ずしもこのような使い方に限定されるものではない。例えば、委託元からセキュリティ対策を求められたときに、「組織的な情報セキュリティ対策ガイドライン」を活用することも考えられるし、「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」を活用しても良い（図 3）。

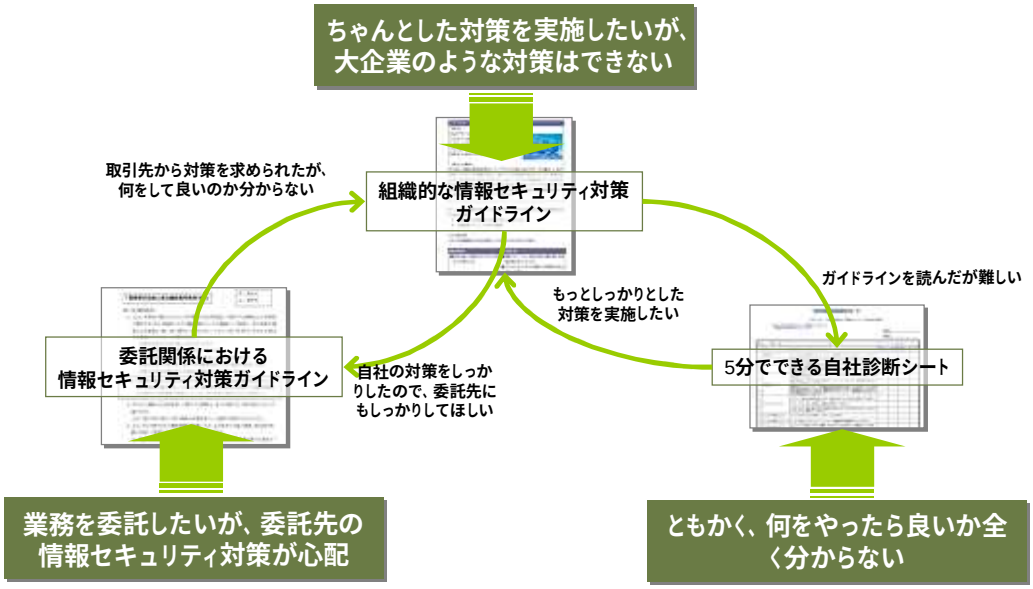

図 3. 様々なガイドラインの活用方法

また、本ガイドラインよりも高度な対策をとりたい場合は、IPA の情報セキュリティ対策ベンチマークや、国際標準である ISMS の利用や認証取得などの利用が考えられる。特に、IPA の情報セキュリティ対策ベンチマークは、中小企業における利用も視野に入れて設計されており、また、本ガイドラインは情報セキュリティ対策ベンチマークとの整合にも留意して作成されているので、本ガイドラインの次のステップとしては最適であろう。

以上