中小企業の情報セキュリティ対策に関する研究会

報告書

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

中小企業の情報セキュリティ対策に関する研究会
委員名簿

（委員長）

大木　栄二郎	工学院大学情報学部教授

（委員）

市川　晶久	日本商工会議所 情報化推進部課長
糸井　雅晴	日本アイ・ビー・エム株式会社 GBS 事業 アプリケーション・イノベーション・サービスセキュリティ＆プライバシー 部門長
井上　陽一	NPO 日本ネットワークセキュリティ協会 西日本支部長
岡田　浩一	明治大学 経営学部教授
金子　啓子	パナソニック株式会社 情報セキュリティ本部長
北岡　弘章	弁護士・弁理士
木村　玲美	浜松総務部有限会社 代表取締役
坂田　明	明豊ファシリティワークス株式会社 取締役会長
塩崎　哲夫	富士通株式会社 情報セキュリティセンター長
砂押　以久子	立教大学講師
中尾　康二	KDDI 株式会社 運用統括本部 情報セキュリティフェロー
平山　喬恵	株式会社アクティブブレインズ 代表取締役
星　昌宏	(財)日本情報処理開発協会 ISMS 制度推進室 審査グループリーダー
丸山　満彦	監査法人トーマツ（公認会計士）
南山　智之	シンキングネットワークス株式会社　代表取締役
元橋　一之	東京大学 工学系研究科技術経営戦略学専攻 教授・専攻長
渡部　寿彦	独立行政法人中小企業基盤整備機構 新事業支援部 創業・ベンチャー支援課長

（五十音順、敬称略）

（オブザーバー）

経済産業省

（事務局）

独立行政法人情報処理推進機構セキュリティセンター
株式会社三菱総合研究所

以上

中小企業の情報セキュリティ対策に関する研究会　ＷＧ１
委員名簿

（主査）

塩崎　哲夫	富士通株式会社情報セキュリティセンター長

（委員）

有吉　純	株式会社シマンテック ビジネス開発統括本部エヴァンジェリスト
今田　亘	パナソニック株式会社 情報セキュリティ本部戦略施策チーム
岩間　研二	三菱電機株式会社 総務部情報セキュリティセンター 担当部長
岡村　茂	日産自動車株式会社 Ｒ＆Ｄエンジニアリング・マネージメント本部 プロセス・情報マネージメント部情報企画グループシニアエンジニア
九川　謙一	東京商工会議所 地域振興部　IT 化支援担当課長
杉村　健	日本アキュムレータ株式会社　取締役
西方　弘樹	日本アイ・ビー・エム株式会社 GBS 事業 アプリケーション・イノベーション・ サービス セキュリティ＆プライバシー シニア・コンサルタント
村上　晃	株式会社ラック サイバーリスク研究所 主管研究員
吉川　達也	東京電力株式会社 原子力・立地業務部 情報技術グループ

（五十音順、敬称略）

（オブザーバー）

経済産業省
株式会社三菱総合研究所

（事務局）

独立行政法人情報処理推進機構セキュリティセンター

以上

中小企業の情報セキュリティ対策に関する研究会　ＷＧ２
委員名簿

（主査）

元橋　一之	**東京大学工学系研究科技術経営戦略学専攻教授・専攻長**

（委員五十音順）

岩間　研二	**三菱電機株式会社総務部情報セキュリティセンター担当部長**
大枝　修	**株式会社大塚商会マーケティング部 地域・業界ソリューション推進部**
	地域プロモーション課課長代理
柿本　圭介	**情報セキュリティ大学院大学非常勤講師**
嶋倉　文裕	**特定非営利活動法人日本ネットワークセキュリティ協会西日本支部**
千葉　寛之	**株式会社日立製作所 Hitachi Incident Response Team (HIRT)**
平野　志高	**株式会社富士通ビジネスシステムシステム本部**
	産業流通ソリューション統括部ＩＴコンサルティングサービス部

（五十音順、敬称略）

（オブザーバー）

経済産業省

（事務局）

独立行政法人情報処理推進機構セキュリティセンター
株式会社三菱総合研究所

以上

中小企業の情報セキュリティ対策に関する研究会　ＷＧ３
委員名簿

（主査）

岡田　浩一	**明治大学　経営学部教授**

（委員）

久保寺　良之	**特定非営利活動法人 IT コーディネータ協会 常務理事・事務局長**
佐野　憲	**株式会社シーポイント コンサルティング事業部マネージャー**
高島　利尚	**社団法人中小企業診断協会 副会長**
角田　照彦	**全国商工会連合会 情報・能力開発課長**
宮本　利明	**シーネットネットワークスジャパン株式会社**
柳田　公市	**特定非営利活動法人ナレッジネットワーク理事長**

（五十音順、敬称略）

（オブザーバー）

経済産業省
株式会社三菱総合研究所

（事務局）

独立行政法人情報処理推進機構セキュリティセンター

以上

1．背景と目的

1.1．背景

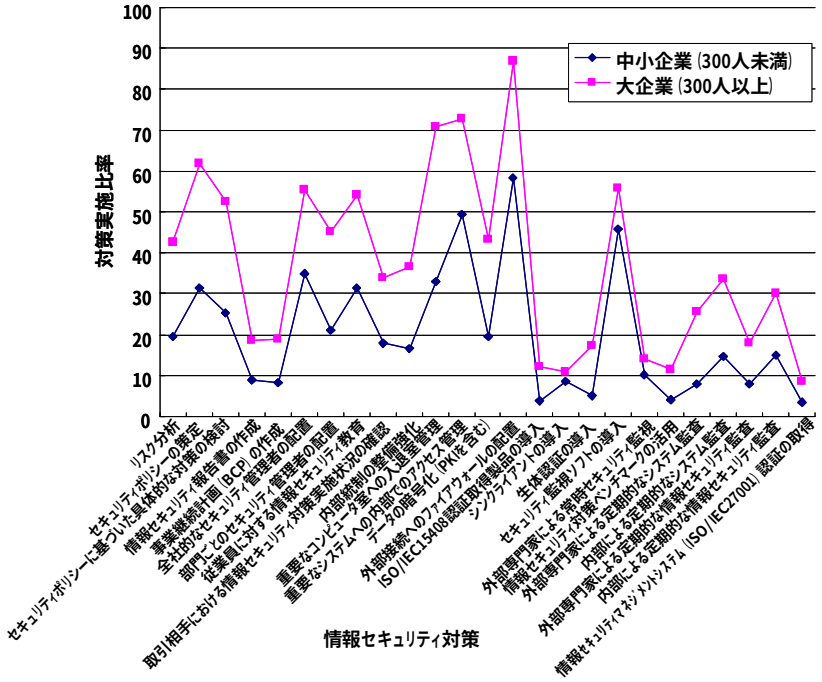
中小企業は我が国の企業の大半を占めている。平成 18 年総務省「事業所・企業統計調査」によれば、300 人以下の事業所の数は全事業所の 99%以上を占めており、従業員数で見ても、約 88%が 300 人以下の事業所の従業員であるなど、中小企業は我が国の産業競争力の根幹を支えている。

中小企業においても情報化は進展しており、例えば従業員 100 人以上 300 人未満の比較的規模の大きい中小企業における企業内通信網の構築率は H19 年に 87.6%に達している（**図 1.1-1**）。全体平均の 90.4%に比較すれば若干低いものの、比較的規模の大きい中小企業においては既に約 9 割の企業で LAN（企業内通信網）が構築されている。このように、中小企業においても情報化が進展していることを踏まえれば、中小企業においても情報セキュリティ対策を実施することが必要である。

出典：総務省「H19 年通信利用動向調査報告書（企業編）」

図 1.1-1　従業者規模別企業内通信網の構築状況

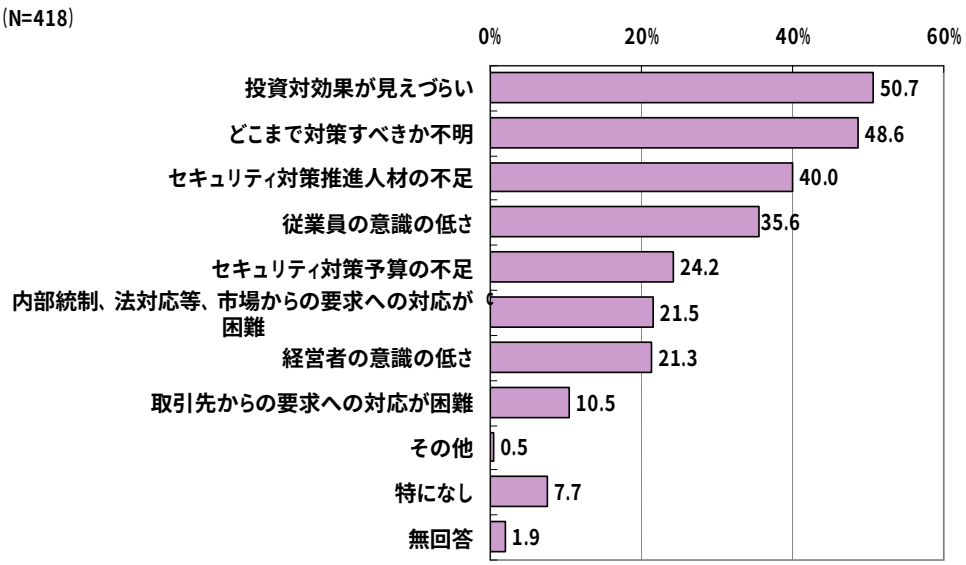
一方、中小企業における情報セキュリティ対策の遅れも報告されている（**図 1.1-2**）。加えて、中小企業の多くは情報セキュリティ対策に対するインセンティブやリソースに限りがあると考えられることから、中小企業については、情報セキュリティ対策に対してより細かい配慮が必要である。



出典：経済産業省　「平成 19 年情報処理実態調査」より作成

図 1.1-2　大企業と中小企業（従業員 300 人未満）の対策実施率の差異

中小企業の情報セキュリティ対策に関する研究会の下、H19 年度に IPA が実施した調査によれば、中小企業における情報セキュリティ対策実施上の問題点としては、「投資対効果が見えづらい」（50.7%）、「どこまで対策すべきか不明」（48.6%）、「セキュリティ対策推進人材の不足」（40.0%）、「従業員の意識の低さ」（35.6%）が高く、業種・規模による差異は少ない（**図 1.1-3**）と報告されている。



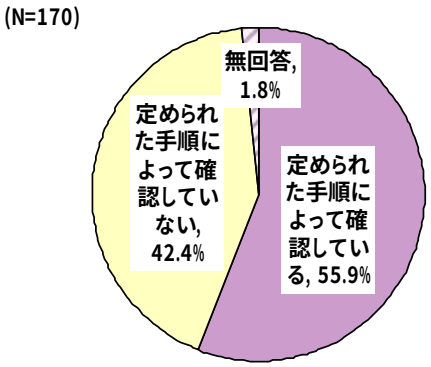
出典：IPA、「中小企業の情報セキュリティ対策確認手法に関する実態調査」

図 1.1-3　中小企業における情報セキュリティ対策上の課題

中小企業の特質に配慮した対策を提示することで負担感の低減に繋げつつ、中小企業における情報セキュリティ対策水準の底上げにつなげる必要がある。

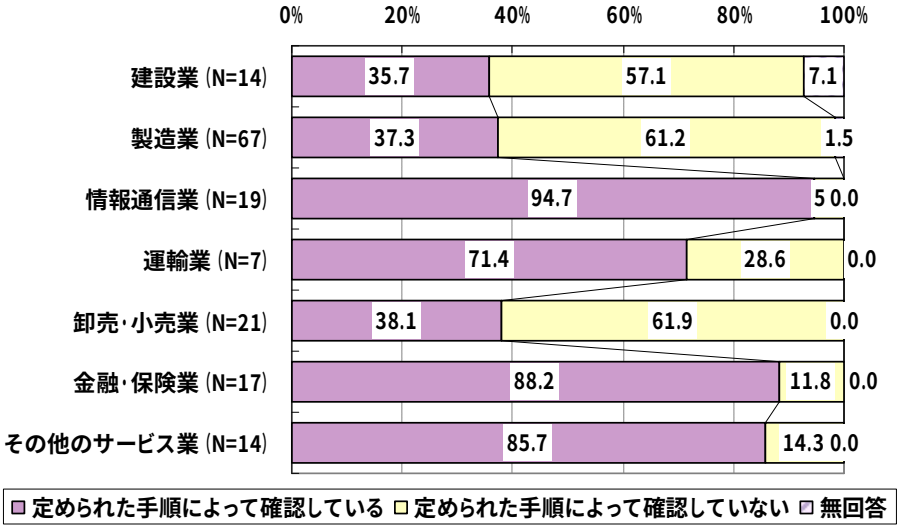
また、近年、個人情報保護や営業秘密管理などの観点から、取引先に対して情報セキュリティ対策を求める事例が多くなってきている。

H19 年度に IPA が実施した調査によれば、大企業の半数以上が取引先の情報セキュリティ対策状況を確認している。業種別では、情報通信業（94.7%）、金融・保険業（88.2%）、サービス業（85.7%）において、確認割合が高い。従業員数が 1,000 人未満の企業による確認割合はやや低い。



出典：IPA、「中小企業の情報セキュリティ対策確認手法に関する実態調査」

図 1.1-4　取引先（業務委託先）の情報セキュリティ対策状況の確認有無



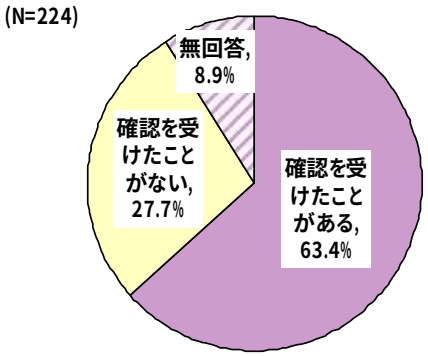
出典：IPA、「中小企業の情報セキュリティ対策確認手法に関する実態調査」

図 1.1-5　取引先（業務委託先）の情報セキュリティ対策状況の確認有無（業種別）

大企業が情報セキュリティ対策状況を確認しているのは個人情報（66.3%）や、重要な技術情報や営業秘密情報等（43.2%）に関わる業務の取引先についてである。業種別では、情報通信・金融保険・サービス業において「顧客に関する個人情報」、「従業員に関する個人情報」、「ビジネスに

関わるノウハウ等」を含む業務の取引先を確認対象とする企業が多い。また、製造業では、「製造方法・部品等に関する技術情報」を含む業務の取引先について確認対象とする企業が多い。また、5,000 人以上の企業では、いずれの情報を含む業務の取引先においても対策確認を実施している割合が高い。

同様に、取引先より情報セキュリティ対策状況に関して確認を受けたことのある中小企業は 2/3 に達しており、特に、情報通信・金融保険・サービス業は、84.3%と高い割合に達する。従業員規模別では、20 人未満の企業で確認を受けたことのある企業が 5 割に留まるが、いずれの規模においても、概ね 5～7 割程度が確認を受けたことがあると回答している。



出典：IPA、「中小企業の情報セキュリティ対策確認手法に関する実態調査」

図 1.1-6　取引先（業務委託元）からの情報セキュリティ対策状況の確認有無

このように、情報セキュリティ対策は単に自社の問題にとどまらず、企業間取引において対応が求められる不可欠の要素となりつつある。このことは企業規模を問わず、共通の問題であるが、特にリソースに限りのある中小規模においては大きな問題になりうる。

1.2. 目的

平成 20 年度中小企業の情報セキュリティ対策に関する研究会では、中小企業における情報セキュリティ対策の促進を目的とした検討を行った。

中小企業における情報セキュリティ対策を考える際に基本となる考え方は、リスクに応じた対策が重要であるということであり、これは大企業におけるそれと変わらない。しかしながら、昨年度調査の結果を踏まえれば、中小企業は、その規模・業種は多様性に富んでおり、一括りに議論を行うことは困難であることに留意が必要である。また、取引関係の中では、大企業から業務委託を受ける中小企業に求められる情報セキュリティ対策の水準は、必ずしもその中小企業が本来実施する必要のある水準の対策とは同一ではない可能性がある。

従って、昨年度の研究会では、中小企業の情報セキュリティ対策の要件を検討するに際しては、以下のような点を基本的な考え方とすることとした。

- セキュリティリスクの大小に応じたマルチレベルの対策。
- 中小企業の多様性と、それに起因するセキュリティリスクの大小への配慮。

・ 中小企業が具備すべき情報セキュリティ水準と、委託関係の中で求められる情報セキュリティ水準は異なるものとして取り扱う。

また、これらを要件としてブレークダウンしていく際に、あまりにも多くのバリエーションが存在することは、中小企業の対応をむしろ困難にすることが考えられることから、多様性に配慮しつつも単純さを重視することとした。

昨年度の検討を踏まえ、今年度は主に以下の二点について検討を行った。

・ 情報セキュリティに配慮した適正な取引の推進
・ 中小企業の情報セキュリティ対策の底上げ

一点目の「情報セキュリティに配慮した適正な取引の推進」とは、昨年度調査でも明らかなように、中小企業が具備すべき情報セキュリティ水準と、委託関係の中で求められる情報セキュリティ水準は必ずしも同じではない点を考慮しつつ、委託関係の中で情報セキュリティ対策の要求事項とは何かを検討することで、情報セキュリティに配慮した適正な取引の推進を目指すものである。

二点目の「中小企業の情報セキュリティ対策の底上げ」とは、多様な中小企業に配慮しつつ、中小企業でも実施可能な実効性のある対策を提示することで、中小企業の情報セキュリティ水準の底上げを目指すものである。

1.3. 中小企業の定義

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をまとめると**表 1.3-1**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。

表 1.3-1　**中小企業の定義**

	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

2.検討方法

2.1.中小企業の情報セキュリティ対策に関する研究会

本検討に際しては、中立的な立場から検討を行うため、H19 年度に引き続き、情報処理推進機構の中に有識者からなる「中小企業の情報セキュリティ対策に関する研究会」（以降、研究会）を設置した。研究会において実施した検討は以下の通りである。

- 情報セキュリティに配慮した適正な取引の推進
- 中小企業の情報セキュリティ対策の底上げ

これらの検討を踏まえ、「中小企業の情報セキュリティガイドライン」を作成した。

また、研究会の下に 3 つのワーキング・グループ（以降、WG）設置し、ガイドラインについて具体的な検討を行った。

本年度の研究会は計 4 回開催され、ガイドライン案の検討などを行った（表 2.1-1）。

表 2.1-1 「中小企業の情報セキュリティ対策に関する研究会」検討経緯

研究会	主な議題
第 1 回 （平成 20 年 7 月 30 日）	・中小企業の情報セキュリティに関する動向 ・諸外国の情報セキュリティ対策について ・今年度の検討方針
第 2 回 （平成 20 年 12 月 3 日）	・中小企業の情報セキュリティ対策推進に向けた IPA における取り組み状況 ・WG における検討状況について
第 3 回 （平成 21 年 1 月 30 日）	・WG における検討状況について ・研究会報告書骨子案について
第 4 回 （平成 21 年 2 月 26 日）	・ガイドライン（案）について ・研究会報告書（案）について

本年度の研究会は昨年度の研究会の検討を踏まえた検討を行うとともに、経済産業省において検討されている、情報セキュリティ対策に係る法的な側面、アウトソーシングに関する情報セキュリティ対策等の検討と連携を行った**エラー! 参照元が見つかりません。**。

(1)情報セキュリティに配慮した適正な取引の推進

情報セキュリティに配慮した適正な取引の推進では、取引先に求める情報セキュリティ対策について、取引関係における情報セキュリティ対策確認事項の明確化に関し検討を行った。

(2)中小企業の情報セキュリティ対策の底上げ

H19 年度の IPA 調査によれば、中小企業の情報セキュリティ対策は、その業種や規模によって、その水準にかなりの違いが存在することがわかった。いわゆる大企業と遜色ない中小企業から、IT 化自体が遅れており情報セキュリティ以前の問題を抱える中小企業も多い。また一般的な傾向

として、小規模な企業は IT 投資・セキュリティ対策投資ともに進展していない。このため、様々な課題を抱える中小企業の情報セキュリティ対策を底上げするための方策の検討を行った。

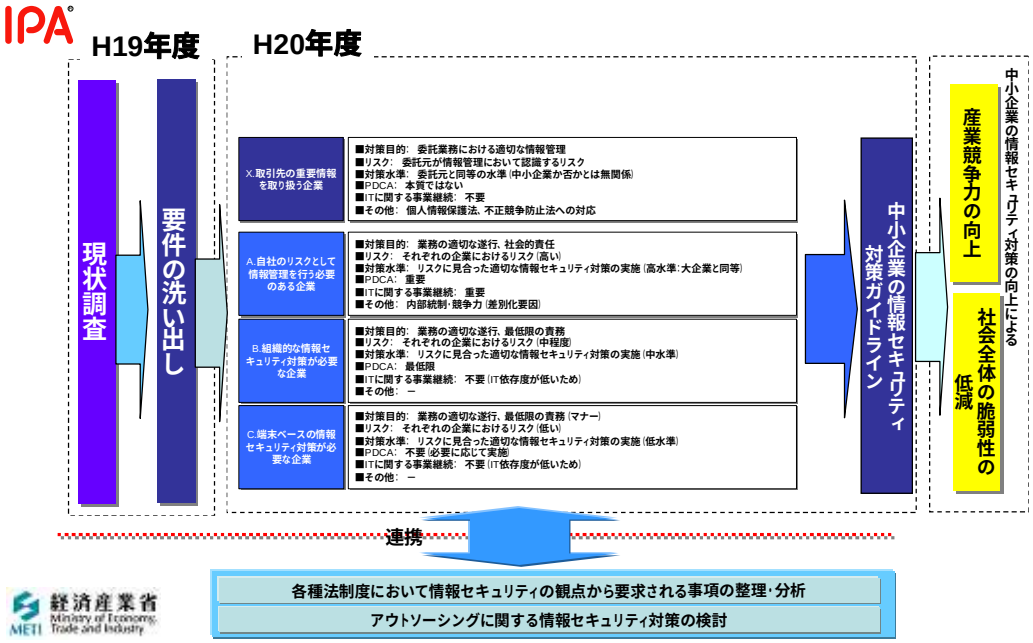


図 2.1-1 「中小企業の情報セキュリティ対策に関する研究会」の検討フレームワーク

2.2.ワーキング・グループ

研究会の下にワーキング・グループを設置した。具体的には、「情報セキュリティに配慮した適正な取引の推進」の検討のため、ワーキング・グループ 1 を、「中小企業の情報セキュリティ対策の底上げ」の検討のため、ワーキング・グループ 2 及びワーキング・グループ 3 を設置した。検討経緯を表 2.2-1に示す。なお、昨年度の研究会において提示した 4 つの企業分類のうち、「X. 取引先の重要情報を取り扱う企業」、「B. 組織的な情報セキュリティ対策が必要な企業」、「C.端末ベースの情報セキュリティ対策が必要起業」は、それぞれ、"X"はワーキング・グループ 1 において、"B"はワーキング・グループ 2 において、"C"はワーキング・グループ 3 において検討を行うこととした。

表 2.2-1 「中小企業の情報セキュリティ対策に関する研究会ワーキンググループ」検討経緯

ワーキンググループ等	主な議題
ワーキング・グループ 1	
第 1 回 （平成 20 年 10 月 22 日）	・中小企業の情報セキュリティに関する動向等 ・検討方針（案） ・事例紹介 ・作業分担とスケジュールについて
第 2 回 （平成 20 年 11 月 27 日）	・事例の収集状況について ・取引先からの要請事項の類型化の検討について ・今後の作業の進め方について
第 3 回 （平成 20 年 12 月 12 日）	・情報セキュリティガイドラインの事例紹介 ・ガイドライン目次の作成 ・執筆分担の決定
第 4 回 （平成 21 年 1 月 6 日）	・機密保持条項（例示案）の検討 ・チェックリスト目次の作成 ・執筆分担の作成
第 5 回 （平成 21 年 1 月 20 日）	・機密保持条項（例示案）の検討 ・委託関係の情報セキュリティ対策事項の検討
ワーキング・グループ 2	
第 1 回 （平成 20 年 9 月 29 日）	・中小企業の情報セキュリティに関する動向等 ・検討方針（案） ・作業分担とスケジュールについて
第 2 回 （平成 20 年 10 月 15 日）	・ポジションペーパーについて ・ガイドライン骨子案について
集中作業 （平成 20 年 10 月 27 日）	・ガイドライン案について
第 3 回 （平成 20 年 11 月 19 日）	・集中作業結果について ・ガイドライン構成案について
第 4 回 （平成 21 年 1 月 23 日）	・ガイドライン案について
ワーキング・グループ 3	
第 1 回 （平成 20 年 11 月 6 日）	・事務局作成資料の概要説明 ・各委員からの意見資料説明 ・スケジュールについて
第 2 回 （平成 20 年 11 月 25 日）	・WG3 のとりまとめ方針について ・事故事例の紹介 ・簡易な自己診断シート（案）について
第 3 回 （平成 20 年 12 月 18 日）	・簡易な自己診断シート（案）について ・来年度以降の検討課題について
主査会	
第 1 回 （平成 21 年 1 月 8 日）	・各 WG 成果の位置づけ、相互関係 ・各 WG の成果報告書の体裁 ・全体スケジュール

(1) ワーキング・グループ 1（WG1）

WG1 では、情報セキュリティに配慮した適正な取引の推進方策について検討を行うため、発注者と下請け者それぞれの責任範囲が現状よりも明確になるように、発注者が下請けに実効性のある対策を具体的に示すための手引きを作成した。この内容を実施するのは中小企業だが、それを指示する大企業が発注時に参考とするようなものを想定している。

この検討に際しての要件と課題は以下のようなものである。

- 委託業務における適切な情報管理／情報セキュリティ対策の確認が行えること。
- 業種や委託する業務なども加味する必要。

検討方針としては、ISO/IEC 27001、ISO/IEC 27002、情報セキュリティ管理基準を参照しつつ、既存の情報セキュリティ水準確認チェックリスト等を参考に検討を行うこととした。これらの結果を、「委託関係における情報セキュリティ対策ガイドライン」としてとりまとめた。

(2) ワーキング・グループ 2（WG2）

WG2 では、中小企業の情報セキュリティ対策の底上げを目的として、「組織的な情報セキュリティ対策が必要な企業」について、対策の指針を示すことを目的とした検討を行った。

この検討に際しての要件と課題は以下のようなものである。

- 中小企業における業務の適切な遂行、社会的責任等への対応。
- 中小企業の規模や業種など、直面するリスクの違いへの配慮。
- 抽象的な表現は避けると共に、よくある誤解例や具体的なシナリオの提示。
- 免罪符にならないように留意する必要。
- 情報セキュリティ対策に意欲のある企業への配慮。

検討方針としては、既存のガイドライン（ドイツ BSI　IT Security Guidelines 等）の調査を行うと共に、既存の IPA 策定ガイドライン等との連携を考慮しつつ、中小企業として実施すべきと考えられる情報セキュリティ対策について検討を行った。

これらの結果を、「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」としてとりまとめた。

(3) ワーキング・グループ 3（WG3）

WG3 では、中小企業の情報セキュリティ対策の底上げを目的として、入門的な対策について検討を行った。この検討に際しての要件と課題は WG2 と同様である。

検討方針としては、中小企業における情報セキュリティ対策の入門あるいは入口として、自社の対策状況を簡便にチェックできるようなチェックシート等について検討を行った。

これらの結果を、「5 分でできる自社診断シート」としてとりまとめた。

3.検討結果

3.1. 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に関する研究会では、2.で示した検討を踏まえ、「中小企業の情報セキュリティ対策ガイドライン」を策定した。

「中小企業の情報セキュリティ対策ガイドライン」は、本文において、中小企業が情報セキュリティ対策に取り組む必要性を示すと共に、実質的なガイドラインとなる別冊の使い方を示している（**図 3.1-1**）。別冊は 3 冊から構成され、それぞれ WG1、WG2、WG3 が作成したガイドラインが対応している。

具体的には、別冊 1 として、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、「委託関係における情報セキュリティ対策ガイドライン」をとりまとめた。別冊 2 及び別冊 3 は、中小企業の情報セキュリティ対策の底上げを目的として、「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」及び「5 分でできる自社診断シート」として取りまとめた。

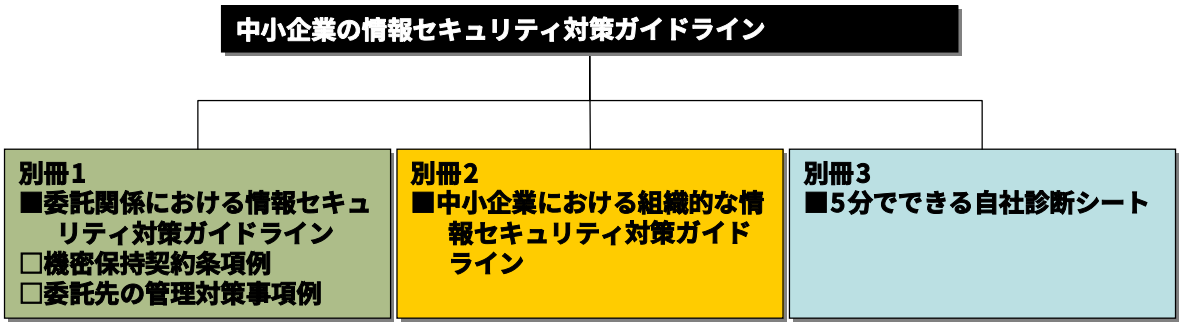


図 3.1-1 「中小企業の情報セキュリティ対策ガイドライン」の全体構成

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 3.1-2のようになる。
まず最初に、読者が中小企業自身（図 3.1-2左）か、委託元としての立場（図 3.1-2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 3.1-2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 3.1-2右）。

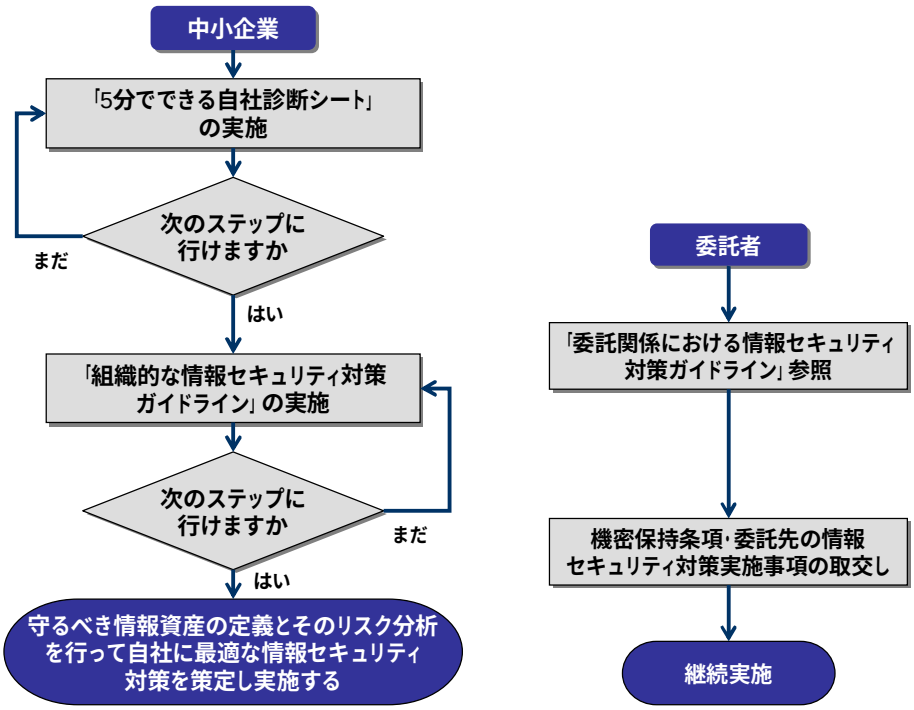


図 3.1-2　「中小企業の情報セキュリティ対策ガイドライン」の使用方法

また、ガイドラインは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 3.1-3）。

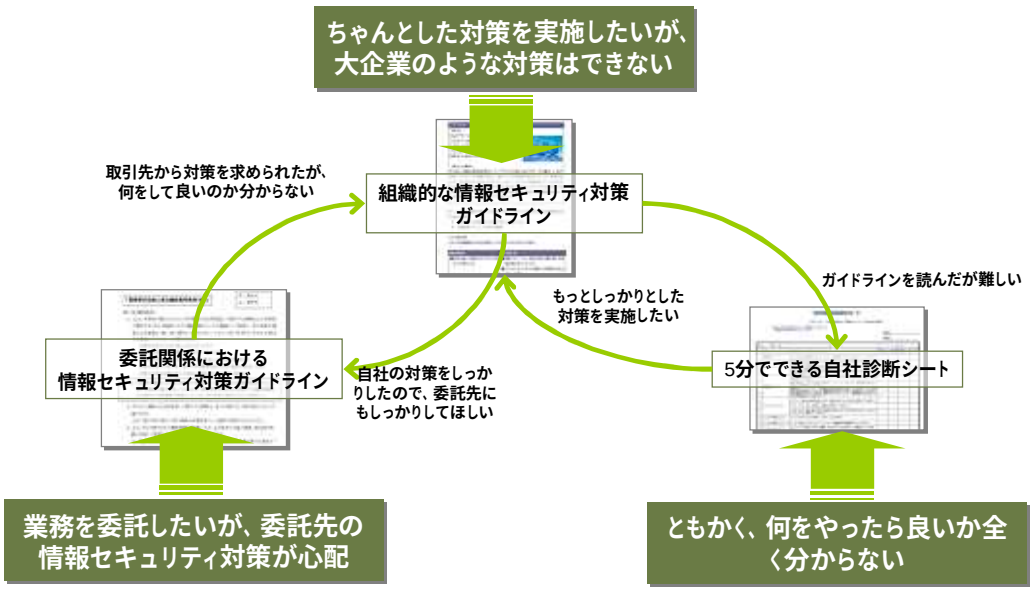


図 3.1-3 「中小企業の情報セキュリティ対策ガイドライン」の使用方法

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ると考えられる。

3.2.情報セキュリティに配慮した適正な取引の推進

(1) 委託関係における情報セキュリティ対策ガイドライン

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、「委託関係における情報セキュリティ対策ガイドライン」をとりまとめた。「委託関係における情報セキュリティ対策ガイドライン」は、「業務委託契約に係る機密保持条項（例）」及び「委託先における情報セキュリティ対策事項」から構成されている。

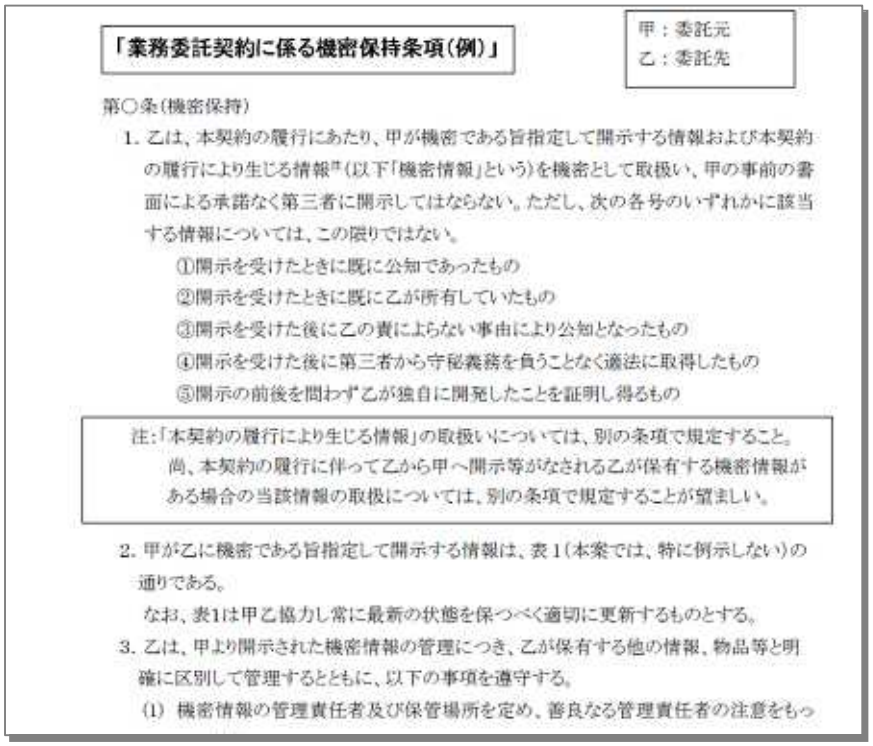
業務委託において、機密情報を提供する際に、提供元から提供先に対して、機密情報の指定またはその保持に必要とされる情報セキュリティ対策の具体的な実施内容が示されない場合がある。そのような状況では、機密情報の漏えいを防止する適切な対策の実施は期待できない。業務委託における機密情報の提供は、委託元から委託先に提供される場合の他、委託先から委託元に提供される場合、相互に提供する場合があるが、ここでは、機密情報を委託元から委託先に提供することを主として検討した。概ね、逆向きの提供でも考え方は同じであるが、委託元から委託先に提供する前提で表現を整理した。

そこで、取引基本契約書、個別契約書、覚書、NDA、打合せや口頭による確認、また売買契約書、代理店契約書等、あるいは発注書、仕様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「業務委託契約に係る機密保持条項（例）」としてまとめた。

さらに、委託元から提供を受けた機密保持に関し、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、いくつかの企業から実務で使用している事例の収集を行い、より具体的な対策事項の例示として「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しい。



「業務委託契約に係る機密保持条項(例)」

甲：委託元
乙：委託先

第○条(機密保持)

1. 乙は、本契約の履行にあたり、甲が機密である旨指定して開示する情報および本契約の履行により生じる情報[注](以下「機密情報」という)を機密として取扱い、甲の事前の書面による承諾なく第三者に開示してはならない。ただし、次の各号のいずれかに該当する情報については、この限りではない。
   ①開示を受けたときに既に公知であったもの
   ②開示を受けたときに既に乙が所有していたもの
   ③開示を受けた後に乙の責によらない事由により公知となったもの
   ④開示を受けた後に第三者から守秘義務を負うことなく適法に取得したもの
   ⑤開示の前後を問わず乙が独自に開発したことを証明し得るもの

注:「本契約の履行により生じる情報」の取扱いについては、別の条項で規定すること。
尚、本契約の履行に伴って乙から甲へ開示等がなされる乙が保有する機密情報がある場合の当該情報の取扱については、別の条項で規定することが望ましい。

2. 甲が乙に機密である旨指定して開示する情報は、表1(本案では、特に例示しない)の通りである。
   なお、表1は甲乙協力し常に最新の状態を保つべく適切に更新するものとする。
3. 乙は、甲より開示された機密情報の管理につき、乙が保有する他の情報、物品等と明確に区別して管理するとともに、以下の事項を遵守する。
   (1) 機密情報の管理責任者及び保管場所を定め、善良なる管理責任者の注意をもっ

図 3.2-1 「業務委託契約に係る機密保持条項（例）」（一部）

委託元から委託先に開示する機密情報（以下「機密情報」という）の管理に関し、委託先が実施する情報セキュリティ対策の事例を示す。なお、具体的に多くの事例を示すため事例相互の整合性は保証されていないので、適宜選択すること。これらの事例を参考に、機密情報の種類、業務委託関係などの諸条件を考慮して、委託元は、委託先と協議のうえ、委託先が実施する適切な情報セキュリティ対策を指示すべきである。

1. 情報セキュリティに対する組織的な取組み

1．1 機密情報の利用、保管、持ち出し、消去、破棄における取り扱い手順を定める

- ✧ 機密情報は、他の情報と区別して保管すること。
- ✧ 機密情報の管理者を定めること。
- ✧ 機密情報にアクセスできる人の範囲を定めること。
- ✧ 最新の従事者（管理責任者を含む）を「従事者台帳」で管理すること。
- ✧ 機密情報を受領した場合には、「機密情報管理台帳」に記録すること。
- ✧ 機密情報の利用履歴を残しておくこと。
- ✧ 機密情報を複製または電子メールで送信する場合には、事前に委託元の承認を得ること。

図 3.2-2 「委託先における情報セキュリティ対策事項」（一部）

3.3.中小企業の情報セキュリティ対策の底上げ

(1) 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

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対象として、「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」を策定した。

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るが、中小企業のバリエーションの多さ（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、一律な基準を示すことは困難である。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った（**図 3.3-1**）。この縦軸で、「水準」とあるのは対策の強度を概念的に示したものである。例えば、アクセス制御において ID・パスワードだけによるのか、IC カードやバイオメトリクスと組み合わせ二要素認証とするのか、などの強度を示している。横軸の「項目の網羅性」とは、情報セキュリティ管理における管理領域の広さを概念的に示したものである。例えば、JIS Q 27001 における管理領域、例えば「物理的及び環境的セキュリティ」や「アクセス制御」、あるいは情報セキュリティ対策ベンチマークにおける「情報システム及び通信ネットワークの運用管理」や「情報セキュリティ上の事故対応状況」などを示す。また、「企業毎に考慮すべき対策」の点線で囲われている領域は、後述する各「シナリオ」に対応している。各シナリオは管理領域

においてお互いに若干重複している。また水準という観点からは「共通して実施すべき対策」とも重複している。

共通して実施すべき対策だけでも相当な効果があると考えられるが、十分な対策をとるためには企業毎に考慮すべき対策について各自検討を行い、必要な対策をとることが望まれる。

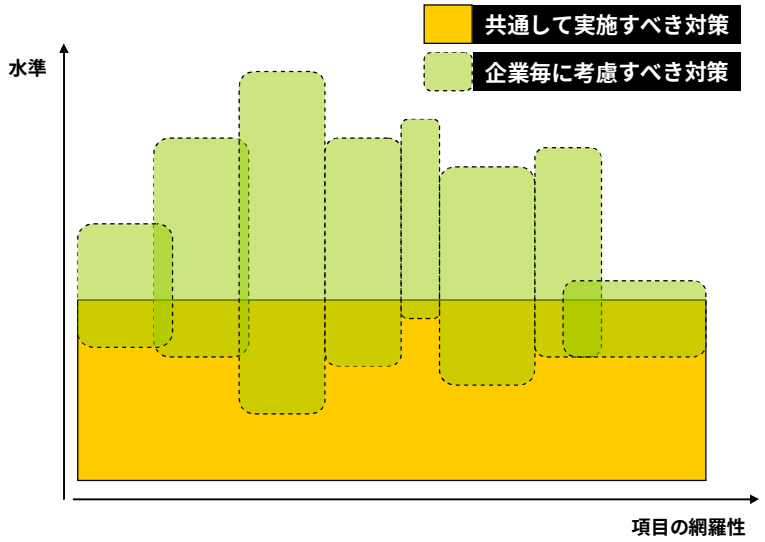
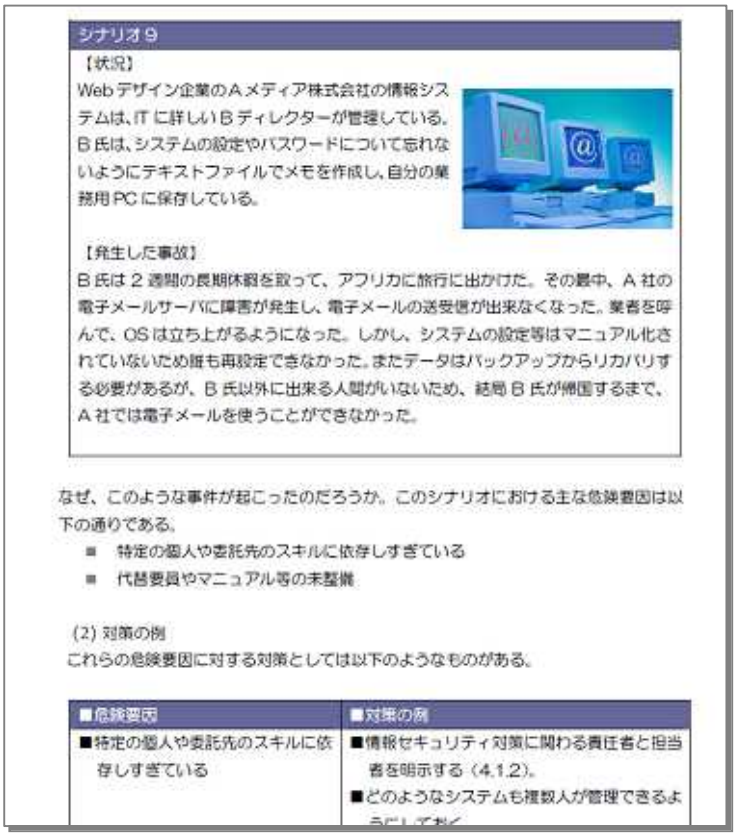


図 3.3-1　共通して実施すべき対策と企業毎に考慮すべき対策のイメージ

なお、一般的な情報セキュリティの教科書においては、まずリスク分析から入ることが推奨されている場合が多い。本ガイドラインでは、「企業毎に考慮すべき対策」が、それに相当する。しかし、中小企業においてリスク分析を行うことが心理的な負担になっているとの指摘もあることから、本ガイドラインでは敢えて「共通して実施すべき対策」を先行して示すことで、心理的ハードルを下げ、脅威への気づきや、リスク分析についてはその後で示すという変則的な構成をとった。



シナリオ９

【状況】

Webデザイン企業のAメディア株式会社の情報システムは、ITに詳しいBディレクターが管理している。B氏は、システムの設定やパスワードについて忘れないようにテキストファイルでメモを作成し、自分の業務用PCに保存している。

【発生した事故】

B氏は２週間の長期休暇を取って、アフリカに旅行に出かけた。その最中、A社の電子メールサーバに障害が発生し、電子メールの送受信が出来なくなった。業者を呼んで、OSは立ち上がるようになった。しかし、システムの設定等はマニュアル化されていないため誰も再設定できなかった。またデータはバックアップからリカバリする必要があるが、B氏以外に出来る人間がいないため、結局B氏が帰国するまで、A社では電子メールを使うことができなかった。

なぜ、このような事件が起こったのだろうか。このシナリオにおける主な危険要因は以下の通りである。

- 特定の個人や委託先のスキルに依存しすぎている
- 代替要員やマニュアル等の未整備

(2) 対策の例

これらの危険要因に対する対策としては以下のようなものがある。

■危険要因	■対策の例
■特定の個人や委託先のスキルに依存しすぎている	■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（4.1.2）。 ■どのようなシステムも複数人が管理できるよう[illegible]

図 3.3-2 「組織的な情報セキュリティ対策ガイドライン」（一部）

さらに、本ガイドラインに基づいた対策を行った中小企業は、情報セキュリティ対策ベンチマークを利用することで、求められる対策の達成状況を把握したり、様々な企業の中での自社の位置づけを把握することができる。これにより、不足している対策が判明した際は、再び本ガイドラインを参考に、必要な対策について検討することが重要である。

(a)共通して実施すべき対策

共通して実施すべき対策で考慮したのは項目のバランスである。というのは、中小企業だからやらなくても良いものがあるわけではなく、また、その形態は多様であり、様々なリスクを考慮する必要があることから、漏れが無く、バランスのある対策セットを提示することは中小企業においても重要であるためである。しかしながら、中小企業の多様性や情報セキュリティ対策に投入できる限られたリソースを考慮すると、高レベルの対策を求めるのは現実的ではない。以上を踏まえ、共通して実施すべき対策では、以下のような方針に基づいて項目を決定した。

1. **項目のバランスを考慮し、経済産業省及びIPAの情報セキュリティ対策ベンチマークの項目に準拠して項目を選定した（表 3.3-1）。なお、情報セキュリティ対策ベンチマークはJIS Q 27001:2006付属書Aの管理策との対応をとって策定されているため、本ガイドラインにおける共通して実施すべき対策の項目も間接的にJIS Q 27001**

付属書 A との対応が取れていることになる。ただし、本対策項目を全て実施したとしても JIS Q 27001:2006 付属書 A で示されている対策が十分に出来ているということは意味しない。

2. 項目のレベルについては、情報セキュリティ対策ベンチマークにおいて各項目において 3 点[1]程度を取得できることを目安に設定した。ただし、ベンチマークにおける中小企業の平均得点を考慮すると共に、中小企業にとって重要な項目と重要でない項目についても考慮している。なお、本来は企業の IT 依存度や業種毎に必要とされるレベルが異なるが、今回は簡単のため業種別のレベルは提示していない。レベルの高い対策が必要な場合は、後述する「(b)企業毎に考慮すべき対策」を各企業において検討することになる。中小企業向けに質問項目自体も情報セキュリティ対策ベンチマークから変更したことにも留意が必要である。

なお、中小企業において「共通して実施すべき対策」を行う事は、中小企業において「必要」な対策であるが、「十分」な対策ではない点に留意すべきである。「十分」な対策を行うためには、以下に示す「企業毎に考慮すべき対策」もあわせて実施する必要がある。

(b)企業毎に考慮すべき対策

「企業毎に考慮すべき対策」では、中小企業において重点的に取り組むべき様々なシナリオを提示することで、「共通して実施すべき対策」の徹底と、場合によっては必要とされる高度な対策について示した。これは企業それぞれが、自身の業務内容などを考え、必要となる対策を選択するための手がかりを与えることを狙いとしている。具体的には、企業が自社の直面する危険や問題点（情報セキュリティリスク）への気づきを与えるため、、危険予知トレーニング（KYT）的な手法を用いながら、幾つかの典型的なシナリオの中から自社に適合するものを選択し、それに対応する対策を自ら選ぶこととした。さらに、典型的な対策について、「共通して実施すべき対策」との関連を明らかにしつつ、紹介している。シナリオ一覧を**表 3.3-2**に示す。

なお、全ての対策を行うことは不可能であるので、どのような考え方で対策の取捨選択をすべきかについての基本的な考え方も示した。具体的には、脅威や危険について気がついた企業が、どのような対応方針で情報セキュリティ対策の実施の可否を決めるか、という問題に対して、一般的な手法を紹介している。

---

[1] 情報セキュリティ対策ベンチマークにおける 3 点とは、各項目に対して「経営層の承認の下に方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない。」もしくは「方針やルールを定め、全社的に周知・実施しているが、実施状況の確認はできていない。」と回答するレベルをいう。なお、ISMS 取得企業は理論的には 4 点以上を取得するものと考えられる。

表 3.3-1　情報セキュリティ対策ベンチマークとの対応

■情報セキュリティ対策ベンチマーク（全25問）		■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 4. 共通して実施すべき対策（全22問）	
大項目１．情報セキュリティに対する組織的な取組状況		4.1 情報セキュリティに対する組織的な取り組み	
	①情報セキュリティポリシーや情報セキュリティ管理に関する規程を定め、それを実践していますか。		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
	②経営層を含めた情報セキュリティの推進体制やコンプライアンス（法令順守）の推進体制を整備していますか。		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
	③重要な情報資産（情報及び情報システム）を、その重要性のレベルごとに分類し、さらにレベルに応じた表示や取扱をするための方法を定めていますか。		4.1.3 管理すべき重要な情報資産を分類する
	④重要な情報（たとえば個人データや機密情報など）については、入手、作成、利用、保管、交換、提供、消去、破棄などの一連の業務プロセスごとにきめ細かくセキュリティ上の適切な措置を講じていますか。		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、破棄における取り扱い手順を定める
	⑤外部の組織に業務や情報システムの運用管理を委託する際の契約書には、セキュリティ上の理由から相手方に求めるべき事項を記載していますか。		4.1.5 外部の組織と情報をやり取りする際に、情報の取り扱いに関する注意事項について合意を取る
	⑥従業者（派遣を含む）に対し、採用、退職の際に守秘義務に関する書面を取り交わすなどして、セキュリティに関する就業上の義務を明確にしていますか。		4.1.6 従業者（派遣を含む）に対し、セキュリティに関して就業上何をしなければいけないかを明確にする
	⑦経営層や派遣を含む全ての従業者に対し、情報セキュリティに関する自組織の取組や関連規程類について、計画的な教育や指導を実施していますか。		4.1.7 情報セキュリティに関するルールの周知と、情報セキュリティに関わる知識習得の機会を与える
大項目２．物理的（環境的）セキュリティ上の施策		4.2 物理的セキュリティ	
	①特にセキュリティを強化したい建物や区画に対して、必要に応じたセキュリティ対策を実施していますか。		4.2.1 重要な情報を保管したり、扱ったりする場所の入退管理と施錠管理を行う
	②顧客、ベンダーや、運送業者、清掃業者など、建物に出入りする様々な人々についてセキュリティ上のルールを定め、それを実践していますか。		
	③重要な情報機器や配線などは、自然災害や人的災害などに対する安全性に配慮して配置または設置し、適切に保守していますか。		4.2.2 重要なコンピュータや配線は地震などの自然災害や、ケーブルの引っ掛けなどの人的災害が起こらないように配置・設置する
	④重要な書類、モバイルPC、記憶媒体などについて適切な管理を行っていますか。		4.2.3 重要な書類、モバイルPC、記憶媒体などについて、整理整頓を行うと共に、盗難防止対策や確実な廃棄を行う
大項目３．情報システム及び通信ネットワークの運用管理状況		4.3 情報システム及び通信ネットワークの運用管理	
	①情報システムの運用に際して、運用環境や運用データに対する適切な保護対策が実施されるよう、十分に配慮していま		4.3.1 情報システムの運用に関して運用ルールを策定する
	②情報システムの運用に際して、必要なセキュリティ対策を実施していますか。		
	③不正プログラム（ウイルス、ワーム、トロイの木馬、ボット、スパイウエアなど）への対策を実施していますか。		4.3.2 ウイルス対策ソフトをはじめとしたアプリケーションの運用を適切に行う
	④導入している情報システムに対して、適切なぜい弱性対策を実施していますか。		4.3.3 導入している情報システムに対して、最新のパッチを適用するなどの脆弱性対策を行う
	⑤通信ネットワークを流れるデータや、公開サーバ上のデータに対して、暗号化などの適切な保護策を実施しています		4.3.4 通信ネットワークを流れる重要なデータに対して、暗号化などの保護策を実施する
	⑥モバイルPC やUSB メモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などを想定した適切なセキュリティ対策を実施していますか。		4.3.5 モバイルPCやUSBメモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などに備えて、適切なパスワード設定や暗号化などの対策を実施する
大項目４．情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策の状況		4.4 情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策	
	①情報（データ）や情報システムへのアクセスを制限するために、利用者ID の管理、利用者の識別と認証を適切に実施していますか。		4.4.1 情報（データ）や情報システムへのアクセスを制限するために、利用者IDの管理（パスワードの管理など）を行う
	②情報（データ）や情報システム、業務アプリケーションなどに対するアクセス権の付与と、アクセス制御を適切に実施していますか。		4.4.2 重要な情報に対するアクセス権限の設定を行う
	③ネットワークのアクセス制御を適切に実施していますか。		4.4.3 インターネット接続に関わる不正アクセス対策（ファイアウォール機能、パケットフィルタリング、ISPサービス等）を行う
			4.4.4 無線LANのセキュリティ対策（WPA2の導入等）を行
	④業務システムの開発において、必要なセキュリティ要件を定義し、設計や実装に反映させていますか。		4.4.5 ソフトウェアの選定や購入、情報システムの開発や保守に際して、情報セキュリティを前提とした管理を行う
	⑤ソフトウェアの選定や購入、情報システムの開発や保守に際して、セキュリティ上の観点からの点検をプロセスごとに実施するなど、適切なプロセス管理を実施していますか。		
大項目５．情報セキュリティ上の事故対応状況		4.5 情報セキュリティ上の事故対応	
	①万が一システムに障害が発生しても、必要最低限のサービスを維持できるようにするため、情報システムに障害が発生する場合をあらかじめ想定した適切な対策を実施しています		4.5.1 情報システムに障害が発生した場合、業務を再開するために何をすべきかを把握する
	②情報セキュリティに関連する事件や事故が発生した際に必要な行動を、適切かつ迅速に実施できるように備えています		4.5.2 情報セキュリティに関連する事件や事故等（ウイルス感染、情報漏えい等）の緊急時に、何をすべきかを把握する
	③何らかの理由で情報システムが停止した場合でも、必要最小限の業務を継続できるようになっていますか。		⇒4.5.1に統合

表 3.3-2　企業毎に考慮すべき対策におけるシナリオの一覧

番号	シナリオ名称
5.1.1	従業員の情報持ち出し
5.1.2	退職者の情報持ち出し、競合他社への就職
5.1.3	従業員による私物 PC の業務利用と Winny の利用による業務情報の漏洩事故
5.1.4	ホームページへの不正アクセス
5.1.5	アウトソーシングサービスの利用
5.1.6	委託した先からの情報漏えい
5.1.7	在庫管理システム障害の発生
5.1.8	無線 LAN のパスワードのいい加減な管理
5.1.9	IT 管理者の不在
5.1.10	電子メール経由でのウイルス感染

(2)5 分でできる自社診断シート

情報セキュリティ対策が中小企業にとって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。特に情報セキュリティ対策を意識して推進して来なかった中小企業にとっては、「何をすれば良いか分からない」という状態から抜け出すことが難しい状況になっている。

そこで、下記のような企業モデルを前提に、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、経営者か管理者のための自主点検表として、「5 分でできる自社診断シート」を作成した。

- 以下のような状態でもできるような自社診断
  - 情報システム責任者を置けないまたは兼任となる。
  - 経営資源が限られるため、対策経費はあまりかけられない。
- 自社診断で例示した対策の前提
  - 代表者（経営者）が対策方針を直接指示・確認することができる。
  - 社員全員が顔見知りである。
  - 社内に複雑な設定を必要とするサーバやネットワーク機器を自社所有していない。
    - 電子メールやホームページは ISP のサーバを利用しているなどのように、インターネットに直接接続しているサーバを自社所有していない。
    - 市販のアプリケーションソフトだけを利用しているなどのように、自社発注で開発したアプリケーションソフトはない。
    - 個人所有 PC を利用する際には、ISP 等に直接接続するなどのように、個人所有 PC は、職場のネットワークには接続しない。
    - 事業所が 1 箇所で専用線の WAN 回線を持たないなどのように、インターネット以外には社内ネットワークへの接続部分がない。

なお、自社診断で取り上げた項目範囲では、例えば以下の事項については今回は対象としなかった。これらは本来であれば禁止にすることが望ましいが、禁止にできない場合もあると想定し

たためである。ただし、実施する場合には別途の対策が必要になる点に注意する必要がある。

- **テレワーク（自宅 PC や携帯端末等による外部からの利用）で電子メール等を用いて仕事をすること**
- **外部媒体（USB、CD-ROM 等）によるデータの持ち出し、持ち込みをすること**

さらに、「5 分でできる自社診断シート」をより活用してもらうための小冊子である「自社診断パンフレット」を作成した。25 項目について、簡単な解説を加えている。中小企業の情報セキュリティ対策の入門編として、今後広く普及を図るものとする。

5分でできる自社診断シート

入門レベルとして最初に取り組むべき情報セキュリティ対策の自社診断シート

あなたの会社の対策状況について再点検してみましょう
（経営者または管理者の方がご記入ください）

チェック欄は設問に対する回答をひとつ選んで"○"を記入してください。

No.	項　目	内　容	チェック			
以下の項目について、すべての社員が実施しているかをお答えください。 一部の社員が実施している場合には「一部実施している」を選択してください。			実施している	一部実施している	実施していない	わからない
1	保管について	重要情報を机の上に放置せず鍵付き書庫に保管し施錠するなどのように、重要情報がみだりに扱われないようにしていますか？				
2	持ち出しについて	重要情報を社外へ持ち出す時はパスワードロックをかけるなどのように、盗難・紛失対策をしていますか？				
3	廃棄について	重要な書類やＣＤなどを廃棄する場合は、シュレッダーで裁断するなどのように、重要情報が読めなくなるような処分をしていますか？				
4		重要情報の入ったパソコン・記憶媒体を廃棄する場合は、消去ソフトを利用したり、業者に消去を依頼するなどのように、電子データが読めなくなるような処理をしていますか？				
5	事務所について	事務所で見知らぬ人を見かけたら声をかけるなどのように、無許可の人の立ち入りがないようにしていますか？				
6		ノートパソコン利用者は、退社時に、机の上のノートパソコンを引き出しに片付けるなどのように、盗難防止対策をしていますか？				
7		最終退出者は事務所を施錠し退出の記録（日時、退出者）を残すなどのように、事務所の施錠を管理していますか？				
8	パソコンについて	Windows Update[*1]を行うなどのように、常にソフトウェアを安全な状態にしていますか？				
9		ファイル交換ソフト[*2]を入れないようにするなどのように、ファイルが流出する危険性が高いソフトウェアの使用を禁止していますか？				
10		社内外での個人パソコンの業務使用を許可制にするなどのように、業務で個人パソコンを使用することの是非を明確にしていますか？				
11		退社時にパソコンの電源を落とすなどのように、他人に使われないようにしていますか？				
12	パスワードについて	パスワードは自分の名前を避けるなどのように、他人に推測されにくいものに設定していますか？				
13		パスワードを他人が見えるような場所に貼らないなどのように、他人にわからないように管理していますか？				
14		ログイン用のパスワードを定期的に変更するなどのように、他人に見破られにくくしていますか？				
15	ウイルス対策について	パソコンにはウイルス対策ソフトを入れるなどのように、怪しいWebサイトや不審なメールを介したウイルスから、パソコンを守るための対策をおこなっていますか？				
16		ウイルス対策ソフトのウイルス定義ファイル[*3]を自動更新するなどのように、常に最新のウイルス定義ファイルになるようにしていますか？				
17	メールについて	電子メールを送る前に、目視にて送信先アドレスの確認をするなどのように、宛先の送信ミスを防ぐ仕組みを徹底していますか？				
18		お互いのメールアドレスを知らない複数人にメールを送る場合は、Bcc[*4]機能を活用するなどのように、メールアドレスを誤って他人に伝えてしまわないようにしていますか？				
19		重要情報をメールで送る場合は、暗号メールを使うか、重要情報を添付ファイルに書いてパスワード保護するなどのように、重要情報の保護をしていますか？				
20	バックアップについて	重要情報のバックアップを定期的に行うなどのように、故障や誤操作などに備えて重要情報が消失しないような対策をしていますか？				
以下の項目について、あなたの会社で実施しているかをお答えください。			実施している	一部実施している	実施していない	わからない
21	従業者について	採用の際に守秘義務があることを知らせるなどのように、従業者に機密を守らせていますか？		－		－
22		情報管理の大切さなどを定期的に説明するなどのように、従業者に意識付けを行っていますか？		－		－
23	取引先について	契約書に秘密保持（守秘義務）の項目を盛り込むなどのように、取引先に機密を守ることを求めていますか？		－		－
24	事故対応について	重要情報の流出や紛失、盗難があった場合の対応手順書を作成するなどのように、事故が発生した場合に備えた準備をしていますか？		－		－
25	ルールについて	情報セキュリティ対策（上記1～24など）を会社のルールにするなどのように、情報セキュリティ対策の内容を明確にしていますか？		－		－

A ← 実施している○の数	B ← 一部実施している○の数	合計点 ← C + D
A 個	B 個	合計点
C ← A × 4点	D ← B × 2点	
C 点	D 点	点

＊1　マイクロソフト社が提供しているウインドウズパソコンの不具合を修正するプログラム
＊2　WinnyやShareなど、インターネット上で不特定多数のコンピュータ間でファイル（データ）をやり取りできるソフトウェア
＊3　コンピュータウイルスを検出するためのデータベースファイル
＊4　Blind Carbon Copyの略で、他の受信者にメールアドレスを伏せて送信する機能

この自社診断シートで例示している対策方法については、これらだけで十分ということを保証するものではありません。

IPA

図 3.3-3　「5 分でできる自社診断シート」

4.今後の課題

H19 年度の実態調査等を踏まえ、本年度の中小企業の情報セキュリティ対策に関する研究会では、情報セキュリティに配慮した適正な取引の促進と中小企業の情報セキュリティ対策の底上げを目的とした「中小企業の情報セキュリティ対策ガイドライン」を策定した。
研究会では、ガイドラインの策定にあたって中小企業の情報セキュリティ対策が抱える問題点について様々な側面から検討を行い、重要と考えられる問題について優先的に対応した。今後、ガイドラインを用いた中小企業の情報セキュリティ対策水準の向上に向けたプロセスを回していく上で、以下のような課題を考慮しつつ、引続き検討を行うことが望まれる。

(1)中小企業の情報セキュリティ対策水準向上にむけたプロセス

- 中小企業の気づきの喚起
  - 中小企業の経営者の自覚を促す方策について検討する必要。
  - ガイドラインの利用、ひいては中小企業が情報セキュリティ対策に取り組むモチベーションをどのように喚起するかが重要。
- 支援方策と体制
  - 中小企業の対策を進めていくために、ガイドライン等の成果を今後どのように活用していくかが重要。
  - 中小企業の情報セキュリティに対する意識付けまでを視野に入れ、支援体制と一体の普及策が必要。
- 取引関係における情報セキュリティ対策
  - 情報セキュリティ対策に要する費用負担の問題をどのように捉えるべきか検討が必要。
  - 取引関係などに典型的に見られる安全を重視する企業文化を、わが国の国際力向上につなげるための方策について検討が必要。
- 改善プロセス
  - ガイドラインの活用等を通じた普及啓発活動を行った結果を踏まえ、適宜ガイドライン等にフィードバックをかけることで、継続的な改善が必要。

(2)今後ガイドライン等に盛りこむことを検討すべき項目

- 中小企業にとって情報セキュリティ対策の必要性をより認識してもらうために、トラブル事例の収集などが必要。また、情報セキュリティ対策を実施したことによる効果を示す必要はないか。
- 情報セキュリティの観点から、クラウドコンピューティング・SaaS・ASP などの新しい情報サービスを中小企業がどのように活用すべきかの検討が必要。また、中小企業におけるデータセンター等の積極的な外部サービスの活用について検討が必要。

以上