2009 情財第 0127 号

中小企業における情報セキュリティ対策の実施状況等調査

調査報告書

平成 21 年（2009 年）10 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

（調査実施：(株)ノークリサーチ）

アンケート返送先　：　ＦＡＸ　０３－５９７８－７５１８
ＩＰＡセキュリティセンター　企画グループ　宛

「中小企業における情報セキュリティ対策の実施状況等調査」報告書のご利用アンケート

本報告書をご利用頂きまして、誠にありがとうございます。
ＩＰＡの今後のサービス向上に役立てるため、アンケートにご協力下さい。皆様のご意見をお待ちしております。

■ 質問１：　本報告書は、我が国の中小企業における情報セキュリティ対策の実施状況を確認するとともに、ＩＰＡで作成したガイドライン等の活用効果を調査した結果を報告することを目的に作成いたしましたが、どの程度満足されましたか？（○を１つ付けて下さい。）

満足	まあ満足	やや不満	不満

■ 質問２：　上記質問１のように判断された理由をご記入下さい。

■ 質問３：本報告書に関するご感想をご記入下さい。

■ 質問４：本報告書に限らず、ＩＰＡへのご希望・ご意見等ございましたら、ご記入下さい。

■ご連絡先　（差し支えない範囲で結構です。）

お名前	
企業名・団体名	
所属・役職	
会社所在地	
電話	
ＦＡＸ	
e-mail	

● ご記入頂きました個人情報等は適切に管理し、ＩＰＡのサービス向上検討及びご回答者様へのご連絡のためのみに利用いたします。
ＩＰＡの個人情報保護基本方針：http://www.ipa.go.jp/about/privacypolicy/index.html
このアンケートの個人情報保護管理者：セキュリティセンター企画グループリーダー
TEL:03-5978-7508（平成 21 年（2009 年）10 月現在）

●アンケートにご協力頂きまして、ありがとうございました。
ＩＰＡ（独立行政法人　情報処理推進機構）セキュリティセンター
URL: http://www.ipa.go.jp/security/index.html

きりとりせん

目　次

1.はじめに

本報告書は、我が国の中小企業における情報セキュリティ対策の実施状況を確認するとともに、ＩＰＡで作成したガイドライン等の活用効果を調査した結果等をまとめたものです。

ご覧頂く方の目的に応じて、それぞれ該当する箇所を下表にまとめましたので、ご参考にして下さい。

目的	該当箇所
調査結果の概要を知りたい	「3.調査結果概要」（13 ページ）をご覧下さい。
調査結果の詳しい内容を知りたい	「4.調査結果詳細」（17 ページ）をご覧下さい。
調査対象企業のプロフィールを知りたい	「4.1.調査対象企業プロフィール」（17 ページ）をご覧下さい。
企業区分の考え方を知りたい	「2.6.調査手法・区分設定等」（5 ページ）をご覧下さい。
他社のセキュリティ対策の取り組み事例を知りたい	「付録Ｂ．情報セキュリティ対策事例集」（付録 26 ページ）をご覧下さい。
ガイドライン等の概要を知りたい	「6.添付資料」の「6.1.中小企業の情報セキュリティ対策ガイドラインのプレスリリース資料」（30 ページ）をご覧下さい。

2.調査の企画・設計

2.1. 調査の背景

我が国の中小企業における情報化は着実に進展してきているが、それと比較して情報セキュリティ対策が十分に実施されているとは言えない状況にある。中小企業の多くは情報セキュリティ対策に対する認識も十分ではなく、インセンティブやリソースに限りがあることから、大企業に比べて格差が拡大する傾向にある。加えて近年、個人情報保護、営業秘密管理等のさまざまな側面から､取引先から情報セキュリティ対策実施状況の確認が求められるようになってきているが､個々の取引先から異なる情報セキュリティ対策を求められることは、中小企業にとっては大きな負担になりかねない。

このため、我が国において中小企業における情報セキュリティ対策水準の底上げは喫緊の課題である。このような状況を踏まえＩＰＡ（独立行政法人　情報処理推進機構）では、平成 19 年（2007 年）10 月から機構内に「中小企業の情報セキュリティ対策に関する研究会」を設置し、中小企業の負担低減と、中小企業の情報セキュリティ水準向上の観点から、実態に即した中小企業の情報セキュリティ対策のあり方について検討を行った。

平成 21 年（2009 年）3 月に、研究会の検討成果である報告書及び情報セキュリティ対策実施のためのガイドライン、チェックシート等（以下、「ガイドライン等」という。「2.4.調査に使用する報告書、ガイドライン等」を参照。）がとりまとめられ、公表されたガイドライン等は中小企業の情報セキュリティ対策に活用されている。

2.2. 調査の目的

本調査では、上記「1.1.背景」で記載したガイドライン等の活用効果等を確認するため、ガイドライン等が想定した範囲の中小企業群における現行の情報セキュリティ対策の実施状況や、ガイドライン等に対する理解の度合い、ガイドライン等を適用した場合に生じる事象等を直接面接等を通じて調査し、以下のように今後の対策実施に役立てることを目的とする。

- ガイドライン等の活用については、今後ＩＰＡが実施する情報セキュリティセミナーにおいて参加者に紹介する他、経済産業省の事業を通じて、地域における中小企業を対象とした情報セキュリティ対策の指導者等に対して提供されている。これらのガイドライン等の活用効果を具体的な事例を元に紹介することにより、セミナー参加者及び情報セキュリティ対策指導者等に対して、ガイドライン等の活用方法の明確な理解に繋げる。
- 上記研究会は今後も引き続きガイドライン等の改善に向けた検討を継続する予定であるが、検討に際して、現在のガイドライン等を適用した際の反応を分析し、ガイドライン等の改善・向上に役立てる。

2.3. 用語の定義

調査で使用する主要な用語の定義は以下の通りとする。

① 中小企業

中小企業の定義は業種のほか、資本金規模、従業員規模等様々な規模による定義があるが、本件調査においては、情報セキュリティマネジメントに最も影響があると思われる従業員規模に着目し、（法律上の定義とは別に）[1] 便宜的に従業員 300 人以下の企業を中小企業として取り扱う。

② 情報セキュリティ

正当な権利を持つ個人や組織が、情報や情報システムを意図通りに制御できることをいう。情報セキュリティマネジメントシステムの規格である JIS Q 27002 では「情報の機密性、完全性、および可用性を維持すること」と定義されている。この調査においては、ＩＴ（情報技術）の利用を前提とした範囲を主としつつ、広く情報資産の保護まで含めて取り扱う。

2.4.調査に使用する報告書、ガイドライン等

調査に使用するガインドライン等の概略は以下の(1)～(3)に示すとおり。
なお、詳細は以下の URL 掲載の資料及び添付資料の「6.1.中小企業の情報セキュリティ対策ガイドラインのプレスリリース資料」（30 ページ）を参照のこと。

「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

(1)「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（2009）年 3 月版）

上記研究会において、個々の取引先から異なる情報セキュリティ対策実施状況の確認を求められることによる中小企業の負担低減と、中小企業の情報セキュリティ水準向上の観点から、実態に即した中小企業の情報セキュリティ対策のあり方について検討を行った。

平成 21 年（2009 年）3 月に、研究会の検討成果である報告書及び情報セキュリティ対策実施のためのガイドライン、チェックシート等がとりまとめられ、順次公表し中小企業の情報セキュリティ対策に活用されている。

報告書には、ガイドライン等の検討の背景や活用方法について記載。

(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」（平成 21(2009)年 3 月版）

一定の従業員規模以上でＩＴを組織的に活用し、情報システム部門もしくは情報システム担当者等の情報セキュリティ対策を担う人材が存在する企業向けのガイドライン。（以下、

[1]中小企業基本法第 2 条第 1 項によれば、下表の資本金か従業員のいずれか一方を満たせば中小企業とされている。また、株式会社日本政策金融公庫法施行令等の中小企業関連法令においては、個別にゴム製品製造業（一部を除く）は、資本金 3 億円以下または従業員 900 人以下、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、旅行業は、資本金 5 千万円以下または従業員 200 人以下を中小企業と定義している例もある。

	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

「組織的な対策ガイドライン」という）

(3)「5 分でできる！中小企業のための情報セキュリティ自社診断」（チェックシート、平成21(2009)年 3 月版）

ＩＴの活用があまり進んでいないような企業向けの、情報セキュリティの入門レベルの企業向けの対策チェックシート。（以下、「自社診断シート」という）具体的には、以下に示すような特徴を有する企業群を想定して作成。

- 代表者（経営者）が対策方針を直接指示・確認ができる
- 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利用していない
- 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等のように、（ルータを通さず、または DMZ などに設置する等して）インターネットに直接接続しているサーバを利用していない
- 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、自社もしくは発注で開発したアプリケーションソフトがない
- 個人所有 PC を利用する際には、ISP など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
- 情報システム責任者を置かないか兼任である
- 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

2.5. 仮説の設定

以下に掲げるような仮説を想定し、調査を実施した。

a）中小企業の情報セキュリティ対策状況(現状)

中小企業における情報セキュリティ対策状況は、個々の企業により差異があるものの、対策傾向や重点項目については、企業属性によりある程度の類型化が可能ではないか。

b）ガイドライン等の汎用性

ガイドライン等は、汎用的に活用できるよう作成されており、企業属性により傾向の違いはあるものの、組織的な対策ガイドラインまたはチェックシートのいずれかは活用が可能ではないか。

c）ガイドライン等の効果

ガイドライン等は、企業属性により効果の度合いに差異が見られるのではないか。特に、情報セキュリティ対策担当者（兼任も含む）の有無や、地域の身近な情報セキュリティ指導者の有無により、大きな差異が生じるのではないか。また、効果が見られない事例について意見聴取し、今後の検討に繋げることでガイドライン等の改善に活かせるのではないか。

d）中小企業の情報セキュリティ対策事例（模範的事例、トラブル事例）

ガイドライン等の活用を進めるためには、具体的な対策事例の実例の提供が有効ではないか。

2.6.調査手法・区分設定等

2.6.1. 調査手法

調査は、主に直接面接調査により行うこととし、必要に応じて他の調査方法により補完することとした。

(1)直接面接調査を主体とした理由

今回の調査は、情報セキュリティ対策に関する知識を有する者の存在が調査客体の特性として必ずしも期待出来ない中小企業を対象に実施するため、書面記入による調査では対策の実態や背景となる理由が収集出来ない可能性が高いと判断した。また、多数の項目を調査すること、調査対象の負担を出来る限り軽減することにより、情報セキュリティ対策に消極的な企業の実態も把握する必要があること、等も考慮し、直接面接調査を主体とすることが適切であると判断した。

(2)調査件数

直接面接調査を主体とした事から、実施期間及び予算の制限を考慮し、全体で 60 社程度（結果的に合計 66 社）を調査することとした。

2.6.2.企業属性区分の設定

(1)区分の設定

「中小企業における情報セキュリティ対策の実施状況等調査」の調査対象及び企業選定は以下の通りとする。

①従業員規模 300 人以下を 3 区分とする。また、従業員規模に係わらずネット系ビジネス等を行っている「タイプ S」を加え、計 4 区分で比較する。

②業種は製造・建設業、卸・小売など、サービス業など 3 区分とする。また、特別な業種区分としてネット系ビジネス等を行っている「ネット系企業」を加え、計 4 区分で比較する。

③地域は大都市と地方の 2 区分とする

なお、ネット系企業とは、ＩＴ関連企業で SI[2]事業やソフト開発企業群を指すこととした。

各企業属性毎の具体的な区分については、以下のとおり。

①従業員規模（従業員数）属性

－タイプ A:小規模(従業員 20 人未満)

－タイプ B:中規模(従業員 20 人－99 人)

－タイプ C：大規模(従業員 100 人－300 人以下)

－タイプ S: ネット系企業＝ＩＴ関連企業で SI[3]事業やソフト開発企業群。

[2] SI: System Integration。情報システムの企画、構築、運用等を総合的に行うこと。

②業種属性
－製造・建設業
－流通・卸・小売業
－サービス業その他
－ネット系企業（タイプ S）

③地域属性
－大都市圏（首都圏）
－地方圏

(2)区分の考え方

平成 20 年（2008 年）3 月に経済産業省及びＩＰＡが実施した「中小企業のＩＴ活用の実態調査」[4]の結果から明らかになったように、「(1)区分の設定」で示した 3 つの従業員規模に分けた場合、ＩＴの利活用状況、特にサーバを導入した業務システム活用については従業員規模属性でみると差異が見られた。

これは、ＩＴ利活用の進展に伴い、個別に担当者がクライアント PC を用いてデータ処理を行っている段階から、サーバ等を用いて社内でデータを共有し、更に社外とデータの送受信が行われるようになる事と従業員規模との間に何らかの影響が有るものと思われる。

今回の調査も同様に、従業員規模による情報セキュリティ対策の取組みの差異を明確にするために、次の 3 つの属性区分で分けて差をみることとした。同時に取扱う情報の特性に何らかの影響を及ぼすと予想される業種 3 区分と地域 2 区分を同時に分析軸に加える。

①従業員規模＞②業種＞③地域の優先順位で今回の調査の分析フレームとした。

追加で、他の業種区分等と比較するために④の軸として「ＩＴ活用をコアビジネスとするセキュリティ必須企業」をＩＴ依存の度合いが高い特殊な企業群としてタイプ S（ネット系企業）として設定し、①－③のそれぞれの区分との違いを確認することとした。

2.6.3.調査対象企業の選定方法

(1)母集団

調査対象企業の母集団は基本的に帝国データバンクの収録企業から抽出した。表１は、帝国データバンク社による最新の属性別の企業母数を表したものである。

---

[3] SI: System Integration。情報システムの企画、構築、運用等を総合的に行うこと。

[4] 経済産業省及びＩＰＡからの受託により、日本商工会議所とノークリサーチが共同実施。（2007 情財第 0946 号） http://www.jcci.or.jp/2007jittaichosa.pdf

（表１）

【属性別企業母数】　※出典：帝国データバンク社　(2009年3月現在)　　(従業員：人)				
従業員 業種	タイプA： 20人未満	タイプB： 20-99人	タイプC： 100人-300人	合計 （Sタイプ含む）
製造・建設業	455,230	60,676	8,913	524,819
小売・卸・飲食業	326,232	34,702	5,620	366,554
サービス・不動産・運輸・その他	426,069	60,276	14,217	320,562
合計	1,027,531	155,654	28,750	1,211,935

(2)選定方法のポイント

今回のヒアリング調査対象の選定に当たってのポイントは以下の 4 点。

1.従業員規模による差異

2.業種による差異

3.地域による差異

4.上記 1-3 に該当しない企業（企業従業員規模に関係なく）でセキュリティ必須な企業グループ群（タイプ S)。

以上 4 点で対象企業をセル分割して、候補企業を選別する。また関連会社や取引先などの関係で情報セキュリティ対応が必須となるような企業群も全体に分散させて傾向をみるようにした。

（表２）

【対象企業の選定基準】　　（従業員：人）						
分類	企業規模	首都圏	地方	ネット系企業	計	企業母数
タイプA	20人未満	10	10	2	22	1,027,531
タイプB	20-99人	10	10	2	22	155,654
タイプC	100-300人	10	10	2	22	28,750
合　計		30	30	6	66	1,211,935
※タイプA・B・C別に製造・建設業4件、流通・小売・卸業3件、サービス業その他3件（ネット系などタイプSを除く）とする。						

上の表２での首都圏は東京都、隣県 3 県を想定した。地方は、首都圏以外の県庁所在地域や近隣の都市を想定した。ネット系企業（タイプ S）は個別にノークリサーチのパネル企業あるいは一般的な事例として紹介されている企業を抽出した。

(3)参考とした企業区分

ノークリサーチでは、中小企業のＩＴ投資動向等の調査を実施する際に、過去の知見に基づき設定した「SMB 区分」を用いている。(表３参照)

（表３）

「SMB区分定義概要」		
SMB区分	IT部門の特徴	IT導入概要・セキュリティ特性
タイプA： 零細・SOHOクラス	従業員数：20人未満 年商5億円未満 IT部門はなく担当も兼任。ITは必要に応じての購入に留まる。	サーバの導入率は30％未満 クライアント台数：平均5台 ネットワーク環境で利用しているものの、担当者が専任では居ないため、運用管理面での不安は大きい。ウイルス対策ソフトによる対応がほとんど。
タイプB： 中小企業Lクラス	従業員数：20人－99人 年商5億以上～30億円未満 IT部門は存在しない、もしくは3名以下のごく小規模、計画を伴わない部分的かつ短期のIT投資傾向が強い。	サーバの導入率：約70％ クライアント台数：平均60台 サーバを自社運用しているため、必要最低限のセキュリティ対策は行っているが、ネットワーク環境での運用管理面では、レベルは低め。ウイルス対策などの外部対応がメイン。
タイプC： 中小企業Hクラス	従業員数：100人-300人 年商20億以上～60億円未満 IT部門は設置しているが規模は5名以下と小さい。IT投資には計画・戦略がある程度伴うものの部分的最適に留まる。	サーバの導入率：約90％ クライアント台数：平均150台 サーバを複数台自社運用しているため、必要最低限のセキュリティ対策は行っているが、ネットワーク環境での運用管理面では、レベルは低め。ウイルス対策などの外部対応がメイン。
タイプS： IT活用がコアビジネスとなる特定企業	クライアントの個人情報やIT活用などがコアビジネスとなるような業態のため、IT部門は企業規模に関係なく装備率が高く、ITリテラシも高い。	サーバやクライアント、運用管理面などの社内外を問わず、ネットワーク環境で利用しているために、セキュリティ対策の重要性は企業にとって不可欠な要素となる。
※どの企業規模においても、クライアントPCはネットワークでブロードバンド環境にある。		

中小企業（SMB）の企業区分は、ノークリサーチの実施した調査レポート「09 年版中堅・中小企業のＩＴ投資動向」[5]など（脚注の URL 参照）でも用いられ、調査結果には区分毎の明らかな傾向が認められた。

今回のセキュリティ実態調査でも、この区分を参考にして、従業員規模の区分を設定し、区分毎の比較を試みることとした。

2.7.調査実施方針

2.7.1.調査手順

(1)調査手順

対策の実施状況（現状）の確認については、自社診断シートを調査対象企業の担当者等に記入

[5] http://www.norkresearch.co.jp/pdf/2009ittoshi.pdf
http://www.norkresearch.co.jp/pdf/2009server.pdf
http://www.norkresearch.co.jp/pdf/2009clientserver.pdf

を依頼し、結果を回収・分析した。また、自社診断シートの回答結果が 70 点以上の企業[6]には、組織的な対策ガイドライン付録のチェックシートの記入も依頼した。

回収した結果を元に、企業属性別に回答項目毎の平均点を求め、これを比較することで対策項目や重点項目の類型化の可能性の検討等を行った。（付録Ａ①自社診断シート質問項目別平均点数一覧表参照）

上述により把握した内容の背景及びガイドライン等の活用効果等を確認するために、ノークリサーチの研究員による直接面接調査（ヒアリング調査）を実施した。

具体的な調査フローは次頁の図 1（調査プロセスのフローイメージ図）の通りとなる。

(2)自社診断シートを対策実施状況の確認用に用いた理由

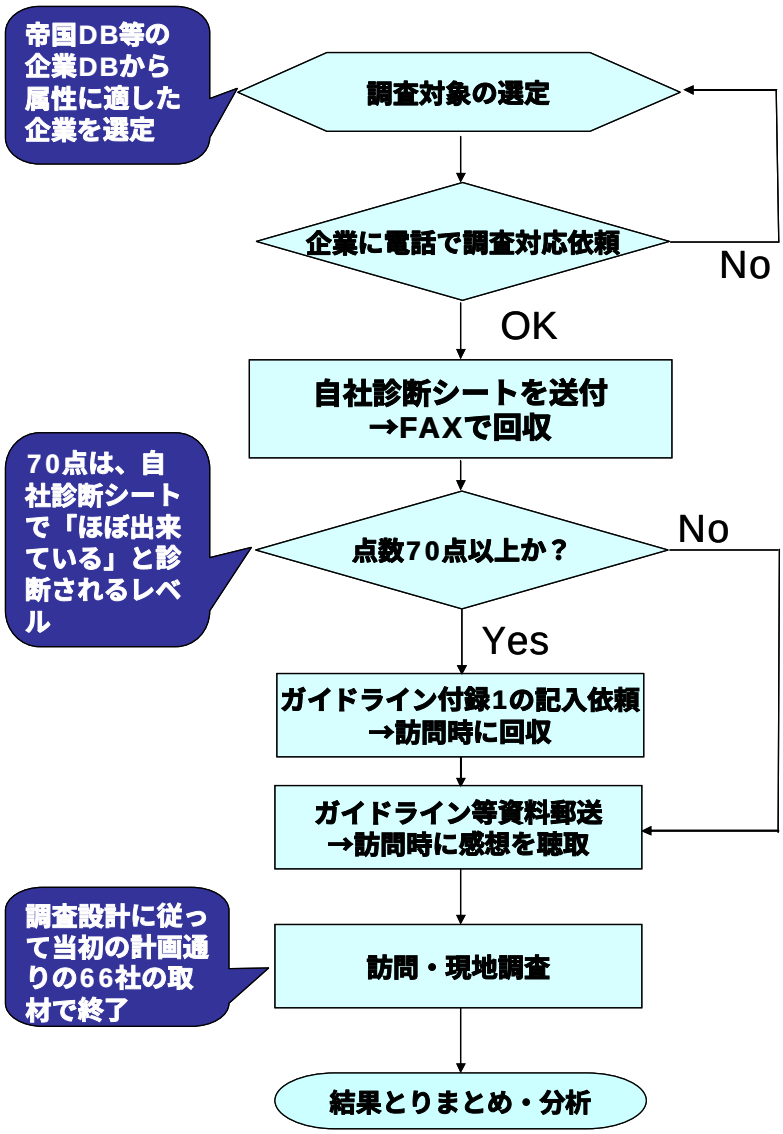
今回の調査では、対象企業の情報セキュリティ対策実施状況を確認するために、上述のとおり自社診断シートを用いている。これは、以下の①～③に掲げるような理由による。

① 自社診断シートは、情報セキュリティ対策の最低限必要となる項目を前提に設計されており、また JIS Q27002 や情報セキュリティ対策ベンチマークシステムの項目を参考にしている事から網羅性があるため。
② 事前に自社診断シートの結果を入手することにより、対策実施状況の概要を知り、ヒアリング調査時の質問項目の絞り込みや調査実施効率の向上を目指すため。
③ 対策項目毎の実施状況の比較をする際に、シート状であることから集計処理がしやすいため。

なお、自社診断シート等は、手軽な情報セキュリティ対策状況確認を目的に作成されたことおから、他者の確認行為が無いまま自己診断により記入される。このため、例えば外部から客観的に見て同等の対策レベルの場合でも、記入者の意識（例えば、記入者が想定している実現すべき情報セキュリティ対策レベル）の違いにより、診断結果に差が生じる可能性が有る事はご理解頂きたい。これは、自署式アンケート調査が等しく直面する特性と言える。

[6]自社診断シートは 100 点満点中 70 点以上を合格レベルと設定している。

(図1) 調査プロセスのフローイメージ図



2.7.2. 調査対象

対象企業は帝国データバンクの収録企業から、表 1、表 2、表 3 の条件に見合う企業を抽出した。

2.7.3. 調査実施件数

合計 66 社

（具体的な属性別の調査件数は「4.1.調査対象企業プロフィール」を参照。）

2.7.4. ヒアリング調査項目及びヒアリングシート

ヒアリング項目については、以下の通りセキュリティの現状、課題、問題点、取り組み意向、ＩＰＡの活動評価等の観点から設定した。（付録Ｃヒアリング調査シート参照）

(1)情報セキュリティ対策の実施状況（現状）

情報セキュリティ対策の実施状況（現状）を確認するための項目として、以下を設定した。

Q1)情報セキュリティに対する組織的な取り組み状況

Q2）物理的セキュリティ対策について

Q3）情報システム及び通信ネットワークの運用管理状況について

Q4）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

(2)ガイドライン等の活用効果

ガイドライン等の活用効果を確認するための項目として、以下を設定した。

Q7）情報セキュリティのガイドラインの効果について

(3)ガイドライン等の感想、意見

ガイドライン等の感想、意見を確認するための項目として、以下を設定した。

Q6）情報セキュリティのガイドラインの内容について

(4)情報セキュリティ対策の事例（模範的事例、トラブル事例）

情報セキュリティ対策の事例を確認するための項目として、以下を設定した。

Q5）情報セキュリティ上の事故対応状況について

Q10）具体的な事例としてのご紹介

(5)その他

その他、現状のセキュリティの課題と今後のセキュリティ投資についての考え方を聞き取るために以下を設定した。

Q8）情報セキュリティについての重要性、課題について

Q9）情報セキュリティについての情報、提案について

Q11）貴社独自の情報セキュリティに関する課題、問題点

Q12）経営層の意識、情報セキュリティ認定、各種資格、その他について（ＩＰＡの認知、ＩＰＡの活動評価、情報セキュリティ対策ベンチマーク[7]の認知等）

2.7.5.調査実施時期（スケジュール）

(1)直接面接調査－実施期間

平成 21 年(2009 年)5 月中旬～6 月下旬

[7] 組織の情報セキュリティマネジメントシステムの実施状況を、自らが評価する自己診断ツール。経済産業省より公表された情報セキュリティガバナンス推進のための施策ツールを、ＩＰＡ が自動診断システムとして開発し、2005 年 8 月より ＩＰＡ の Web 上で提供している。http://www.ipa.go.jp/security/benchmark/index.html

(2)調査の全体スケジュール等

合計 66 社の面接調査なので、担当研究員 4 名を面接要員としてアサインして、約 1.5 ヶ月で調査を実施した。分析も調査の過程で同時に進めることで、最終的に 7 月 15 日に調査を終了した。

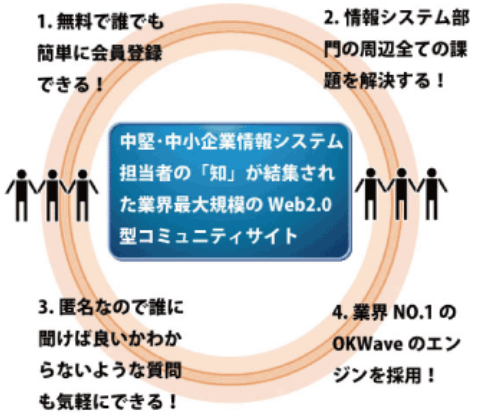
なお、6 月 15 日には中間報告として、成果物（個別ヒアリングシート）と仮説検証の途中確認を行い、最終報告に向けての取りまとめの確認などを実施した。

＜実施スケジュール＞　（全て平成 21 年(2009 年)）

4 月 20 日	調査の設計、対象企業の抽出、アポ取り
5 月上旬	自社診断シート、組織的な対策ガイドライン郵送
5 月中旬	直接面接調査（現地ヒアリング調査）開始
6 月下旬	直接面接調査終了
7 月 15 日	調査終了。報告書提出（ノークリサーチ→IPA）
7 月～10 月	調査結果を IPA「中小企業の情報セキュリティ対策に関する研究会・普及検討 WG」に報告。指摘事項について詳細分析。（10 月公表）

2.7.6.調査を補完するための取組（事業効果を高めるための補完調査）

ノークリサーチで中堅・中小企業向けに実施している「シス蔵」[8]（テクネット社との共同運営）を活用することにより、登録している全国の中堅・中小企業の経営者や情報システム部門の担当者への広報や情報収集がリアルタイムに双方向で行う事が出来る。「シス蔵」を利用してセキュリティへの関心が高い会員に対して、ガイドライン等の周知を実施したほか、一部試験的に「シス蔵」で参加する会員に対してガイドライン等の感想や情報セキュリティ対策実態などの情報提供依頼等の補完調査を行った。



（図 2）「シス蔵」のイメージ図

[5]「シス蔵」は、中堅･中小企業の情報（ＩＴ）システム担当者（登録数約 40 万）を対象としたＱ＆Ａコミュニティ。「質問」と「回答」のやり取りに特化し、知識共有を目的とする Web2.0 型のコミュニティサイト。中堅・中小企業の情報システム部門の助けとなるよう、無料で利用可能で、特定のメーカやベンダに属さない独立運営を行っている。
http://syszo.com/okweb3/_syszo.html

3.調査結果概要

調査結果におけるポイントは下記の通りである。

3.1.ヒアリング調査結果の概要

ヒアリング（直接面接）により、(1)中小企業の情報セキュリティ対策状況、(2)ガイドライン等の汎用性、(3)ガイドライン等の効果、(4)中小企業の情報セキュリティ対策事例、(5)その他の各項目を調査した。

以下に、各項目の調査結果の概要を「2.5.仮説の設定」で想定した仮説に対応する形で記載すると共に、代表的なコメントや見受けられた傾向を＜主なヒアリング結果＞として記載した。
＜主なヒアリング結果＞の冒頭には、ヒアリングシート（付録 C）の該当項目を参考に記載した。

(1)中小企業の情報セキュリティ対策状況

＜仮説 1 について＞
ＩＰＡの作成した自社診断シートの回答を調査対象企業から求めたところ、同シートが合格目標とする 70 点以上の点数を獲得した企業は 3 割程度(66 社中 23 社。35%)であった。
対策項目別の傾向を見ると、社内でのルール化や重要情報の明確化等の組織全体として取り組むべき項目が未実施となっている傾向が確認できた。また、社内への外部者の立入管理や重要情報（資料等含む）の管理については意識が低い企業が多かった。

社内でのルール化については、「情報セキュリティ対策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？」という問に対して、「実施していない」と回答した企業が 66 社中 38 社(58%)であった。

なお、今回の調査では、仮説１で想定した中小企業における情報セキュリティ対策状況の、従業員規模、地域、業種といった企業属性による差は確認出来なかった。ただしＩＴの活用度合の高い企業においては、格段にセキュリティ対策が進んでいることは確認できた。

＜主なヒアリング結果＞

「Q1）情報セキュリティに対する組織的な取り組み状況」の回答内容

- 何らかの枠組みやガイドラインに基づいて体系的に対策を行っている企業は少数であり、経験的に必要と思われる対策のみ実施しているため、網羅性に欠ける傾向がある。
- システム担当者の意識は高いが、社員の意識が低いのが大きな課題。
- 担当者として経営側に進言し、経営側も納得はするが、コストが掛かると分かった時点で、優先順位が下がってしまう。経営側としては積極性が薄い。
- 取引先からセキュリティ対策状況について聞かれることがあるが、取りあえず出来ることはやっている。取引先からも、最低このラインまで、という要望も無い。

・親会社からの指示・指導により具体的な対策を求められている項目については高いレベルで実施されているが、それ以外の項目は必ずしも実施されていない。

(2)ガイドライン等の汎用性

＜仮説 2 について＞
自社診断シートや組織的な対策ガイドラインは、汎用的に活用できるよう作成されており、企業の担当者のスキルによって理解に濃淡はあるにしても、自社診断シート、組織的な対策ガイドラインのいずれかは活用が可能であることが確認出来た。
特に「セキュリティ対策の範囲が思う以上に広く、網羅的な対策が必要なことを気づかされた」という趣旨の声が多かった。

＜主なヒアリング結果＞

「Q6 情報セキュリティガイドラインの内容について」の回答内容

【自社診断シート】

・非常に役立った。内部対策の弱さを感じた。特に対策の不備や不足を改めて感じる良い機会になった。
・「情報」という言葉が、便利に使われすぎてしまって、具体性がなくイメージできないといった可能性もあると思う。もう少し具体的な内容の表記をした方がいいのではないか。

【組織的な対策ガイドライン】

・もっとシンプルに。見やすく。事例は見やすいので、別綴じで良いのではないか？

(3)ガイドライン等の効果

＜仮説 3 について＞
有効なツールとして活用できるという意見は多く、具体的に社内で教育、指導用に活用したいという企業もあった。ただし自社診断シートや組織的な対策ガイドラインは、担当者（面接調査応対者）にとって十分に貴重な情報が得られたが、「実際に自社でセキュリティ対策を展開するについてはその具体的な優先度や必要度合を見極めにくい」などの意見が多かった。
組織的な対策ガイドラインに含まれる事故事例[9]は、具体的で参考になったという評価の声が多かった。さらにもっと自社の従業員規模や業種にあった多くの事例があれば良いという要望も多数の企業で聞かれた。

＜主なヒアリング結果＞

「Q7）情報セキュリティガイドラインの効果について」の回答内容

【自社診断シート】

・自社で最低限やらなければならないことが示されていたので、今後の業務に活かしたいと思う。

【組織的な対策ガイドライン】

9 「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」の第 5 章「企業毎に考慮すべき対策」において、情報セキュリティに関わる様々な脅威や危険について「気づき」を持ってもらうことを狙いとして、KYT（危険予知トレーニング）的なシナリオを提示している。

・ レベルが高く、難しい。組織的な対策ガイドラインは参考になるが、社内回覧をしても関心を示さない社員が多い。診断シートは担当者としては便利だが社員はあまり関心を示さない。担当部門としては参考になるが、社員に徹底させるのは難しい面がある。
・ 責任者はどうやって教育（学習）していけば良いのか？組織的な対策ガイドラインの内容を実施する為にはどういったことが必要なのか判りにくい。責任者がいない場合のセキュリティの向上をどうしたらいいのか、そういったものをガイドしてくれるようなマニュアルが欲しい。

(4)中小企業の情報セキュリティ対策事例（模範的事例、トラブル事例）

＜仮説 4 について＞
66 社のヒアリングで 9 事例をセキュリティ対策が進んでいる事例として得ることが出来た。（付録 B「情報セキュリティ対策事例集」参照）。またトラブル事例としては深刻な事例ではなかったが、66 社中 48 社がウイルス感染や外部アタックなどのトラブル経験があった。

＜主なヒアリング結果＞

「Q8」具体的な事例（模範的事例）」の回答内容

・教育面は定期的に行い、年 1 回の定期的なもの（パートも実施）と入退社時や新入社員への誓約書の締結、個人情報の取り扱いやＩＴの取り扱いに関して行っている。
・会社として「個人情報管理規定」を設けており、個人情報保護方針として社員が顧客の個人情報を守らなければならない旨を社員一人一人に文書で通達している。
・以前より、セキュリティの強化はシステム課発信で徐々に進めていたが、本社と業務提携、資本提携と関係強化をしていく中で、本社よりその要求がなされ、一気に進んだ。

「Q8」具体的な事例（トラブル事例）」の回答内容

今回の調査の中では特に企業の存続に関わるような深刻なトラブル事例は見当たらなかった。しかし、情報漏えいに繋がりかねないようなトラブルは多数確認された。

・ウイルスのアタックが多い。ウイルス感染でトラフィックが増大、システムダウンした。
・海外企業とやり取りしている部署からウイルス感染し、全マシンに広がった。また車内に置いてあった PC が盗まれるという事故もあった。
・ウイルス対策ソフトを最新版にしていなかったことでウイルス感染があった。セキュリティの甘い小規模建設業の孫請会社で使用された USB メモリを社員が持ち込み、使用して起こった。
・退職時にデータの持ち出しをされそうになった（未然に防いだ）。
・社員が持ち込んだ外付けメディア（CD,USB メモリ）からウイルス感染した。

(5)その他（上記以外で判明した事項の概要）

＜仮説の検証以外に判明したこと＞
セキュリティの重要性は多くの企業が理解していても、具体的にセキュリティのために投資や対策をとれないということも聞かれた。経済環境の悪化による投資費用の枯渇ということもある

が、セキュリティの優先度（必須度合）が感覚的に低いということが指摘される。

＜主なヒアリング結果＞

「Q8）情報セキュリティについての重要性、課題について」の回答内容

・ＩＴ投資そのものは行うつもりであるが、セキュリティについては、コストのかからない、社員の教育や啓蒙といった部分の対応を考えて行きたい。

・現場や上層部とコンセンサスがとれていない。投資に関して、セキュリティのみでの投資には上層部も積極的ではない。

・システムの投資は難しい。売上に貢献しないセキュリティ投資は後回しの可能性があるために、投資してセキュリティレベルを上げるというより、まずは意識付けからやっていきたい。

3.2.その他の調査結果の概要

シス蔵による補完調査の結果概要

シス蔵を用いて、「セキュリティガイドラインの投稿」や「トラブル事例」に関する補完調査を行ったところ数件の反応があった。クライアントのパスワード化は難しいという回答が得られたことから、自社診断シートの結果と同様に、定期的なパスワードの変更や暗号化などのクライアント管理については同様に苦労しているということが確認された。また物理的なセキュリティ管理も徹底しにくいなども報告されている。いわゆる企業全体としてのセキュリティ管理の難しさがここでも表れている。

＜シス蔵回答内容＞

・派遣社員用に毎日パスワードを変更してパソコンを使わせているが、パソコンそのものに「本日のパスワード」をメモで貼り付けた。

・出入口にセキュリティガードをつけたが、それとは別の荷物搬入用の倉庫にシャッター付きの出入口が無防備になっており、誰でもそこから簡単に出入りできるようになっている。実際セキュリティ対応が面倒なために、そこから多くの社員や業者が出入りしている。

4.調査結果詳細

調査結果の詳細は以下のとおり。

4.1.調査対象企業プロフィール

今回の調査において、調査対象となった企業のプロフィールは以下のとおり。なお、各分類の考え方については「2.6.調査手法・区分設定等」を参照のこと。

（4.1.1.～4.1.7.については「付録 A－③ヒアリング回答企業属性一覧」も参照のこと）

4.1.1.従業員規模分類の分布

従業員規模別の調査サンプルは、小規模企業が 20 件に満たない結果になった。理由としてはＩＴ担当者がいないことと、調査の対応者が社長になることが多いために、面接調査のスケジュールの都合が合わず、当初の設計よりも少ない件数となった。総数は他の分類を増やすことで調整した。ただし極端な件数減少ではないため、属性別の結果に影響は少ないと判断した。

なお、前述の理由により小規模（20 人未満）の中でも規模が小さな従業員 5 人以下の企業[10]は結果として 2 社となった。

（表４） 「従業員規模の分布（4分布表）実数･構成比」

従業員規模分布	件数	構成比
小規模（20人未満）	15	22.7%
中規模（20人 -100人未満）	24	36.4%
大規模（100人 -300人）	21	31.8%
ネット系企業（タイプS）	6	9.1%
総計	66	100.0%

4.1.2.業種分類の分布

業種分類はほぼ当初の設計どおりの件数を回収することができた。

（表５） 「業種分類の分布（4分類表）実数・構成比」

業種分類	件数	構成比
製造・建設業	24	36.4%
流通・卸・小売業	20	30.3%
サービス業その他	16	24.2%
ネット系企業（タイプS）	6	9.1%
総計	66	100.0%

4.1.3.地域分類の分布

地域分類では当初の設計どおり大都市圏と地方圏[11]を半々で回収できた。

---

[10]従業員規模が 20 人未満の 小規模企業群のうちでも、5 人以下の企業については、ＩＴ業界の SOHO 企業のように業種にも依るが、一般的にＩＴ利活用の様態が進展していないものと考えられる。

[11] 地方圏は、大都市圏（首都圏）に隣接する県を「地方圏 1」、それ以外を「地方圏 2」と分けて、分析した。

（表６）　「地域分類の分布（4分類表）実数・構成比」

地域分類	件数	構成比
大都市圏（首都圏）	30	45.5%
地方圏1	16	24.2%
地方圏2	14	21.2%
ネット系企業（タイプS）	6	9.1%
総計	66	100.0%

大都市圏（首都圏）：東京/千葉/埼玉/神奈川
地方圏：1：茨城/栃木/群馬/山梨/静岡
地方圏：2：新潟/山形/秋田/岩手/福井/三重/岐阜

4.1.4.拠点数

拠点数の分布は以下のとおり。

拠点数は 3 ヶ所以下が 57.5%になっている。1 ヶ所だけが 22.7%、4 ヶ所以上は 42.4%となっている。

（表７）　「拠点数の分布（3分類表）実数・構成比」

拠点数	件数	構成比
1ヵ所	15	22.7%
2～3ヵ所	23	34.8%
4ヵ所以上	28	42.4%
総計	66	100.0%

4.1.5.情報システム部門の人数

情報システム部門の人数の分布は以下のとおり。

情報システム部門 0 人の回答が 42.4%、1 人が 25.8%であり、調査企業の約 7 割が 1 名以下という人数で情報システムを運用している。

（表８）「情報システム部門の人数の分布（４分布表）実数・構成比」

情報システム部門の人数	件数	構成比
0人	28	42.4%
1人	17	25.8%
2～3人	16	24.2%
4人以上	5	7.6%
総計	66	100.0%

4.1.6.ＩＴ導入状況、用途

ＩＴの導入状況、用途では 98.5%の企業が基幹系システムとして利用している。情報系が 25.8%となっている。

（表９）　「IT導入状況、用途の分布（4分類表）実数・構成比」

IT導入状況、用途	件数	構成比
基幹系	65	98.5%
情報系	17	25.8%
フロント系	2	3.0%
その他	1	1.5%

基幹系：基幹業務、経理、人事、販売管理、DB等
情報系：メール、ホームページ、ノーツDB、ファイルサーバ、
アクティブディレクトリ等
フロント系：ウェブオーダーシステム、インターネット通販等
その他：CAD設計
※複数回答

4.1.7.サーバの有無

サーバの有無、台数の分布は以下のとおり。

サーバを導入していないのが 5 社で 7.6%となった。1 台が 25.8%、2-3 台が 15.2%、4 台以上が 51.5%で、サーバは 92.4%の企業が導入している。

（表 10）「サーバの有無、台数の分布（4分類表）実数・構成比」

サーバの有無、台数	件数	構成比
0台	5	7.6%
1台	17	25.8%
2～3台	10	15.2%
4台以上	34	51.5%
総計	66	100.0%

4.2.情報セキュリティ対策の実施状況（現状）

情報セキュリティ対策の実施状況（現状）に関しては、組織的な対策ガイドライン付録のチェックリスト及び自社診断シートの実施結果を回収して、その結果を集計・分析するとともに、いくつかのポイントについて、詳細な聞き取りを実施した。

4.2.1.自社診断シートによる実施結果

自社診断シートをヒアリングの事前に送付・回収して、情報セキュリティ対策実施状況の実態把握を行った。

自社診断シートの点数が合格レベルとされている 70 点以上となった企業は 66 社中 23 社(35%)であり、43 社（65%）が合格レベルに満たない結果となった。

具体的な項目としては、情報セキュリティ対策関連社内ルールの明確化、従業者への守秘義務遵守の徹底や啓発、取引先への機密保持関連要件の明確化、事故対応準備といった企業を挙げて組織的な対応が求められる項目が未実施である企業が多かった。

企業属性（従業員規模、地域、業種等）による差については、今回の調査においては属性の違いによる明らかな傾向は確認が出来なかった。ただし、業務の特性から個人情報を多数保有しているような、ＩＴの活用度合の高い企業においては、セキュリティ対策が進んでいることは確認できた。（詳細は「付録 A－①5 分でできる自社診断シート回答集計結果」参照）

このため、調査に先立ち想定した仮説の一つである、対策項目や重点項目の企業属性による類型化の可能性については、本調査では確認出来なかった。これは、本調査が直接面接調査を重視したために、調査対象企業数が 66 社と類型化の検討のためには少数であった事が影響していると考えられる。

今後、更に大規模な調査により検証することが期待される。

4.2.2.組織的な対策ガイドライン付録のチェックリストの実施結果（参考）

組織的な対策ガイドラインのチェックリストは、「2.7.1.調査手順」で示したフローイメージ図（図１）のとおり、自社診断シートで 70 点以上の企業にのみ実施している。件数も 20 件と少ないため、参考値としてみて頂きたい。

目立った項目としては、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にパスワード設定や暗号化を実施していないという回答が 20 社中 5 社だった。実施していない理由としてパスワード忘れ等によるデータ参照不可に対する懸念が挙げられたほか、そもそも持ち出しそのものを禁止しているので、実施していないという回答もあった。

同様に、無線 LAN のセキュリティ対策（WPA2 の導入等）を 20 社中 6 社が実施していないと回答したが、そのほとんどが情報漏えい等を懸念して無線 LAN そのものを導入していないためであった。

（詳細は「付録 A－⑤組織的な対策ガイドラインの付録チェックシート回答集計結果」参照）

4.2.3.ヒアリング結果

(1)情報セキュリティに対する組織的な取組状況

「4.1.5.情報システム部門の人数」では 0 人の回答が 66 社中 28 社(42%)であり、その他の 38 社(58%)は何らかの形で担当部門または担当者が明確な形で情報システムを運用していた。担当部門が経営層とユーザ部門の間に入る形が大半であったが、経営者や役員自身が担当者という企業もいくつかみられた。

社内でのルール化については、「情報セキュリティ対策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？」という問に対して、「実施していない」と回答した企業が 66 社中 38 社(58%)であった。

情報セキュリティに関連して従業者に対して求める就業ルールの明確化と徹底について今後の課題とする回答が多かった。

(2)物理的セキュリティ対策

物理的なセキュリティについてはＩＴ＝コンピュータについてと、企業の全体に関わることで

は取組状況に差があった。たとえばサーバルームへの出入りについてとかサーバへの施錠とか、配線の引っ掛け防止などは対応が進んでいるが、会社そのものへの出入りや重要書類の管理とかへの意識は薄い。さらに BCP などの対策などは、地域的に地震被害にあった地域の企業などが懸念していたが、ほとんどが未対応であった。概ねサーバルームのある企業では、物理的なセキュリティ対策を施しているようだ。入退室までのログを取る企業は少ない。

(3)情報システム及び通信ネットワークの運用管理状況

ネットワーク管理などは、部分的な対応状況である。特に USB メモリやノート PC などの管理などは仕組みとして制限するというより、指導的に行っているケースが多く、実際は運用管理面での遅れが目立つ。

無線 LAN などは、むしろ情報漏えいを意識して、利用していないか制限を設けていたり、強い暗号化などの対策が目立った。

(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

パスワード管理やアクセス制限、アクセスログ管理などは、自社診断シート 70 点以上の企業で対応が進んでいた。

(5)情報セキュリティ関連の事故対応状況

今回の調査対象企業の中では、特に企業の存続に関わるような深刻な情報セキュリティ上の事故はなかった。情報漏えいに繋がりかねないような機材の盗難や、ウイルス感染によるシステムダウンなどの事例があったが、特に大きな被害には繋がらなかった。むしろ、大きな被害に至らなかったことによる危機認識の過小評価により、セキュリティ対策が進んでいないという見方もできる。そのため事故が起こった場合の連絡事項やエスカレーション（上層部への報告等）なども明文化していない企業が多かった。

4.3.ガイドライン等の汎用性

組織的な対策ガイドラインや自社診断シートは、程度の差は有るものの、どのタイプの企業でも一定の効果があることが確認された。

【自社診断シート】

網羅的な内容で、自社では気づかなかった点が、実はセキュリティとして重要であるという点で参考になったようだ。特にソフトやＩＴネットワークだけでなく、物理的なセキュリティ面など未対応な部分を理解することができた。

【組織的な対策ガイドライン】

このガイドラインは、中小企業向きで内容を網羅的している類似テキストがないので、自社の教育用のテキストとしても使いたいとの意見があった。

4.4.ガイドライン等の活用効果

ガイドラインの活用効果について、以下のような意見が寄せられた。

【自社診断シート】

自社診断シートの結果を受けて、どこまで対策を実施すれば良いかが若干不明な部分がある。要するに 100 点満点の持つ意味が必須で達成すべきことなのか、70 点合格が企業にとってどういう意味を持つかどうかの判断が難しい。

【組織的な対策ガイドライン】

ガイドライン等の活用を進めるためには、具体的な対策事例の提示が有効である事が確認された。特に組織的な対策ガイドラインに含まれる活用事例は、具体的で参考になったという評価の声が多かった。さらにもっと自社の従業員規模や業種にあった多くの事例があれば良いという要望もかなりの企業で聞かれた。活用するには時間も費用も経営者の理解も必要なことから、さらにガイドラインの活用効果を見極めるには時間が必要だ。

4.5.ガイドライン等の感想、意見

今回の調査では自社診断シートの結果を受けて、組織的な対策ガイドラインを見てもらう。そしてその内容を自社で当てはめて見た場合の感想や評価を聞くという方法をとった。

【自社診断シート】

「内容的には気付かされることが多く非常に参考になった」という結果で、非常に好印象での意見、感想であった。

【組織的な対策ガイドライン】

今回の調査対象企業のほぼ全てが「参考になった、気付かされた」という高い評価を得ている。ガイドライン等は有効なツールとして活用できるという意見は多く、具体的に社内で教育、指導用に活用したいという企業もあった。ただし、担当者（面接調査応対者）にとって十分に貴重な情報が得られたが、実際に自社で展開する場面では、具体的な対策項目の優先度合や必要度合を見極められると有り難いなどの意見が目立った。

4.6.情報セキュリティ対策の事例

事例としては、セキュリティ対策が進んでいる模範的事例 9 例が得られた。また、トラブル事例としては、企業の存続に関わるような深刻なトラブル事例は見あたらなかったが、情報漏えいに繋がりかねないようなトラブルは多数確認された。

模範的事例 9 社に共通していることは「経営者とＩＴ部門が近いこと」「関連する企業にセキュリティレベルが要求されていること」と「個人情報を経営活動の中心においている」ことの 3 点だ。

模範的事例については、情報セキュリティ対策の検討を進めている企業の参考になると思われることから、個別事例を付録として収録する事とした。（「付録 B．情報セキュリティ対策事例集」を参照。）

なお、トラブル事例については、個別事例を紹介すると悪意有る者に益する情報を公にする可

能性があるほか、企業側も非公開を求める声が強いため、収録を見送る事とした。

【対策事例集として収録した事例】

・A 社（人材派遣業）

--「3 万人の派遣社員の個人情報をセキュアな環境で管理。ＩＴ担当者の高い専門性が強み」

・B 社（医薬品、衛生用品製造販売会社）

--「経営とＩＴ部門が一体となった先進的な事例。自社で独自のセキュリティルールをもつＩＴ部門の高いスキル」

・C 社（ゴミ袋製造）

--「大手親会社の指導のもと、積極的な研修活動。社内のセキュリティレベルの向上に」

・D 社（医療品販売）

--「セキュリティレベルの高さは親会社の強い要請と指導によるもの」

・E 社（美術品販売）

--「コア事業に強い関連を持つ顧客の個人情報の資産管理とセキュリティ対策は経営戦略と一体」

・F 社（放送局系列開発企業）

--「システム開発業を手掛ける情報システム系人材派遣会社。ＩＴ責任者が事業のキーマン」

・G 社（出版・書籍販売）

--「プライバシーマーク取得活動過程にセキュリティ対策を経営として進める。ＩＴ担当が社長の息子」

・H 社（ソフトウェア販売・開発）

--「ＩＴ系企業として自社でポリシーを明確化し、毎年更新、確認してセキュリティ対策」

・I 社（建設会社）

--「少人数の従業員規模で、経営者自らセキュリティ対策を推進。スキルの足りない部分は外部へ委託」

4.7.その他

(1)情報セキュリティ対策に関する認識

セキュリティ対策については、重要であることの認識度合は高いが、具体的に何が必須な項目なのかが把握しきれていない。別の見方をすれば、現在ほとんどの企業で対応しているウイルス対策以外で、何を次に優先すべきかを理解していない。そのため「現状のセキュリティレベルでも特に問題なし」と回答する企業が多い。

今回の調査で初めて「セキュリティというのはそこまで対策を講じる必要があったということが分かった」という回答が多かったことでも、現状は十分にセキュリティを行っていない（その必要性や認識が低い）ということが言えよう。

1 つ共通することは、比較的に情報セキュリティ対策が充実している企業は、経営者や組織がＩＴ活用、セキュリティ対策に積極的に取り組んでいるということだ。さらにいえば個人情報等の機密情報を、適切な保護をしつつ、企業経営にうまく活用出来る企業ということができる。

逆にいえば「B2B なので個人情報の扱いがない（少ない）」ということだけで、セキュリティ

を重要視していない企業が多い点も気になるところだ。

（2）情報セキュリティの投資の意向

情報セキュリティ対策への投資に限らず、情報投資全般に特に優先すべき投資項目が無いという意見が多かった。情報セキュリティ投資への優先度が低いために、現状特に問題となっていないと感じていることから、情報セキュリティへの投資意欲は概ね低かった。

更にＩＴ担当者が問題意識を持っていても、情報セキュリティ対策に対する経営層の認識する投資優先順位が低いため対策が進まないという声もあった。代表的なコメントでは「セキュリティ対策について、ＩＴ担当者としては、経営層に進言している。経営層も納得はするものの、コストがかかるとわかった時点で、優先順位が下がってしまう。」である。つまり重要性の認識が有る場合であっても、具体的なアクションに及ばずという実態が見受けられた。

（3）情報セキュリティの提案主体、情報収集手段について

全般的にＩＴが企業のコアビジネスで活用している企業は、経営者主導や組織方針としてセキュリティ対応しているために、進んで対策を行っている。しかし、多くの企業は「特に外部から提案も受けていないし、自らも積極的に情報収集を行っていない」というのが実態である。

主な情報収集手段として挙げられたのは、雑誌、ベンダー等であった。

また、情報セキュリティ対策を検討する際には、IT 技術に関する知識や企業経営の分析能力が求められるが、多くの中小企業には社内にそうした知識や能力を有する者がおらず、外部の専門家等との接点もほとんど無かった。

（4）情報セキュリティに関して企業が直面している課題、問題点について

課題、問題点については以下のものがあげられる。

- 「属人的」な要素で、セキュリティの対応や充足度合が大きく左右される。特に 300 人以下が対象となる今回の中小企業の情報システム部門は、少ない場合は担当者なし（兼任）から、多くて 3 名、大半が 1～2 名であることから、担当者（兼任者）のスキルや情報セキュリティ対策に対する積極性によって、決定的な差が出る。
- 企業側からは、社内教育の難しさや、対策項目の優先順位等の判断の難しさ、対策ノウハウの欠如が課題としてあげられた。
- 今回の調査を受けて BCP の観点が抜けていた事に気付いたので、今後の課題としたいという回答もあった。

（5）情報セキュリティ認証、各種資格等について

プライバシーマークの付与認定や ISMS 認証の取得などの情報セキュリティに関する組織的な認証を取得している企業は 66 社中 12 社であった。これらの企業の自社診断シートの実施結果を確認したところ、12 社中 6 社が合格点以下（70 点未満）であった。

なお、これらの企業においても、自社診断シートの項目に照らして対策状況を確認した場合に

気付かなかった対策項目が有った事を指摘する声がいくつか見られた。

また、担当者等が情報セキュリティに関連する資格を有している例は 66 社中 9 社であった。会社側で担当者に対して取得を求めている、又は推奨している例は 7 社であった。

(6) ＩＰＡの認知とＩＰＡへの期待について

調査対象企業 66 社中、31 社がＩＰＡのことを知っていた。

ＩＰＡに対する期待や要望については、以下のコメントが得られた。

- ＩＰＡなどの客観的な基準は説得力があるので、今後も基準化などを行って欲しい。ディーラを通じての啓発も良いのと思う。
- ＩＰＡが銀行・信金・地銀など金融機関の担当を通じて啓発するのも、経営者にもダイレクトに伝わって良いと思う。
- 事例はもっと増やして欲しい。また、危険性をもっと PR して欲しい。
- 経営層にセキュリティの重要性を認識させる施策を行って欲しい。
- 中小企業では経営者の意見とやる気が重要なので、使うメディアや手法も、より経営者の眼に触れるもの（雑誌ならプレジデント誌のような経済誌等）を通じて展開して欲しい。
- 経営者向けのセキュリティでのメリット、事業の成功に結びついたなどの点を訴えるようなセミナーなどが効果がある。情報システム部門が社内で上申、プレゼンをするのと、外部の機関が訴えるのとでは、印象がずいぶん違うので是非行って欲しい。
- 「指針」や「セキュリティの項目別の重要度・優先順位表示」「半年程度のスケジュールでの、最新の変化への対策状況と対策の資料」「社員用の教育資料、ビデオ教材など」も実施して欲しい。

(7) 情報セキュリティ対策ベンチマークの認知について

調査対象企業 66 社中、17 社が情報セキュリティ対策ベンチマーク（以下、「ベンチマーク」）を知っていた。ネット系企業の 6 社は積極的に活用していた。

調査で初めてベンチマークを知った企業が多いが、評価は半々であった。「面白い、試してみたい」という肯定派もいるが、「時間が掛かる」「面倒」「そのレベルにない」などの理由であまり積極的に活用しようと思わないという声もあった。

具体的なコメントは以下のとおり。

- やってみたいとは思うが、自社のレベルがまだ低いことを実感したので、更に出来ることを実施した後にやってみたい。
- 結局、出来ることは身の丈にあったことに限られるので、（ベンチマークをしたところで）全ての対策項目は満たせないだろう。
- やってみたいと思わない。システム自体が親会社に合わせるという形であり、求められる具体的な対策レベルを社員教育により実施することがより重要。
- すでに活用している。経営層と実務者の「実行・意識のブレ」を見るためにも活用できる内容である。

5．今後の課題

5.1.中小企業の情報セキュリティ対策の課題

－低いセキュリティ対策の優先度

ヒアリングで目立ったのが「セキュリティの重要性はある程度理解しているが、必要最低限は行っている。緊急に対応が必要とは感じていない。同時に投資する余裕もない。」という回答である。このセキュリティ対策への優先度の低さこそが中小企業へのセキュリティ対策の課題といえよう。

セキュリティは重要な課題という認識はあるものの、今後のセキュリティ投資については、現状維持かネガティブな反応。「お金がない。必須度合が低い（優先順位低い）。重要性を認めないわけではないが、必須要件には入ってこない。」など、現在はより経営に響くＩＴ投資に目が向いているのが本音のようだ。「お金を掛けずにセキュリティレベルを上げられる施策､方法なら検討する」ということも聞かれた。

－本質的には企業全体として取り組むべきこと。経営者にどう響かせる、気付かせるか？

セキュリティのクリティカル性を理解していない（怖さを認識していない、事業停止の危機の欠如、経験がないので自社には起こらない出来事と思っている）という面もある。セキュリティの対応度合の高い会社は､経営側（組織として機能）がセキュリティに関わっている場合が多い。言い換えれば、経営のコアビジネスとＩＴが近い企業がセキュリティの対応が進んでいるということが明確になっている。それは個人情報等の機密情報を適切に保護しながらＩＴを利活用して経営に活かす企業に特に顕著である。

それらの企業はＩＴがツールというより、ＩＴが企業の根幹を成しているということなので、セキュリティ対策は対応せざるを得ないということが言える。そのためそのような企業は黙っていても自らセキュリティ対応するため、あまり問題はない。

むしろ多くの「セキュリティは重要だと思うが、企業にとってそれほどクリティカルな問題ではないと思っている」企業に対して、どのように重要性を認識させて、対応させることができるかではないか。組織的な対策ガイドラインに収録された事故事例は問題点が分かりやすいと評判であったが､「事例は分かるが、今ひとつ自社で取り組む必要性が見えない」という声が見受けられた。

別の意見で「B2B なので個人情報の扱いがない（少ない）ので、セキュリティを重要視していない」という点も気になるところだ。まず個人情報が無いということはあり得ないことと、個人情報以外にも重要な情報資産があり得る事に気づいていない視点に甘さが見える。

今回の調査により得られた事例では、ウイルス感染やＰＣ盗難など情報漏えいに繋がりかねないようなトラブルは多数確認されたが、企業の存続に関わるような深刻なトラブル事例は見あたらなかった。そうした事から、保険のように、まさかのために備えて進んでセキュリティ対策を充実させるという動きにつながらないようだ。また、今回は BCP という観点で、天災や火事など

でデータ消失という危険性についても、その意識を聞いているが、部分的に（新潟など）対応している場合もあったが、多くは自分の会社には起こらない出来事として、低い意識にとどまっている。

これは情報漏えいについても性善説で捉えている企業が、自社には起こり得ないこととして、意に介していないとも思える。物理的な障害や事故、天災もケーブルの引っ掛け程度の対応にとどまっており、災害は起こらない、または意識さえしていないという楽観的な見方をしている。

リスクを認識した上で、リスク容認するのは経営判断の一つの結果かも知れないが、現状ではそもそも経営基盤であるＩＴシステムの抱えるリスクが正しく認識されていない可能性が高いと思われる。

－外部専門家等の支援の必要性

情報セキュリティ対策を検討する際には、IT 技術に関する知識や企業経営の分析能力が求められる。しかし今回の調査結果では、多くの中小企業が、社内にそうした知識や能力を有する者がおらず､外部からも提案を受けておらず､自らも積極的に情報収集を行っていない状況であった。

こうした状況を踏まえて、IT や企業経営に詳しい外部専門家（中小企業診断士や IT コーディネータ、地域の SI ベンダ等）との接点を設ける等、支援を容易に受けられるような環境整備が必要と思われる。

また、今回の調査に先立って自社診断シートを入手していたが、全く読んでおらず、今回の調査で初めて内容を知ったという企業もあった。

読んでいなかった理由を確認したところ、１）多忙のため見る時間が無い、２）情報セキュリティは難しい、という２点が挙げられたが、実際に、自社診断シートを読んでもらったところ、特に違和感無く理解出来たという回答が得られた。

このような“喰わず嫌い”のような状況を改善するためには、中小企業を支援する関係団体等の協力を得て、「まずは 1 回試しにやってみよう」という機運を醸成する事が重要と思われる。

5.2.ガイドライン等の活用方策に関する評価と課題

－「内容的には気付かされることが多く非常に参考になった」という結果

今回の調査は自社診断シートの結果を受けて、組織的な対策ガイドラインを見て、その評価を聞くという、2 段階の調査手法で実施した。その総括としてはほぼ 100%近く「参考になった、気付かされた」という高い評価を得ている。

－自社診断シートを社内で配りたいという声も

まずは社内への普及啓発等の人的な対策から取組むという声が多かったが、その場合でも自社診断シートは手軽な教材としても有効であり、勉強になるという指摘が多かった。

－組織的な対策ガイドラインの事例は好評

また組織的な対策ガイドラインは若干レベルが高いという声が多かった。しかし、その中でも

事故事例（５．企業毎に考慮すべき対策）は参考になったという意見が多い。さらに事故事例については自社に似たような業種、従業員規模等の事例がもっと多く含まれていれば良いという意見が多かった。実際に数社のヒアリング先から、社内のテキスト用に組織的な対策ガイドラインを人数分欲しいという要請があったくらいである。

－普及の推進が課題

ただし高い評価の裏側には「知らなかった」という現実もある。しかもそれはＩＰＡが推進しているセキュリティ施策も含め、ＩＰＡそのものの存在を知らない企業も多いという事実がある。

また、今回の調査以前に既に自社診断シートを入手している企業も数社存在したが、いずれも「貰って来たものの、難しそうなので読んでいなかった」と言うように自ら実施するまでに至っていなかった。

情報セキュリティに関連する情報入手手段等についても、たまに地域の SIer 等による提案がある程度という状況であり、情報セキュリティ対策の指導者が身近に存在しない例が多い事が確認された。

5.3.ガイドライン等の改善点、検討課題

－ＩＴ未導入項目の取扱い

自社診断シートには、Ｎｏ６「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？」という問い（確認項目）がある。これに対して、ノートパソコンを導入していない企業が「実施していない」を選択したために、結果的に点数が低くなってしまった例が見受けられた。

ＩＴ未導入項目に対する点数の考慮をした改善が必要と思われる。

－限られた資源の中で、対策の優先順位を知りたい

「参考にはなったが、どこから手をつければ良いのか分からない。そもそも本当に必須で必要な対応なのかが、判断がつかない」という声も見受けられた。自社診断シートを実施して未対策項目が数多く存在している事に気付いた後に、経済的にも人的にも限られた環境の中で、より重要な項目から着手したいが、その判断基準が分からないという声が多かった。

－自社診断シートの実施方法に関する注意事項の記載

今回の調査では、自社診断シートに関するパンフレットを読まずに自社診断シートを実施する例が多い事が判明した。

自社診断シートを作成する際に、確認項目をなるべく汎用性を持たせるために対策項目＋例示という記載方法を用いて、その意図が通じるように同時に配布するパンフレットの説明の中で以下の記載を加えたが、上述のとおり利用者は意に反して読まずに利用していた事になる。

> ＜自社診断シート No.25　ルールについて＞の一部抜粋
> この自社診断シートでは、「○などのように、△していますか？」というように、△という

目的を達成するための実施策の例を○で示しました。△だけでは具体的なことがわからず、○だけでは何のためにやるのかがわかりません。目的と実施策の両方を示すことが必要です。

今後は自社診断シートの余白部分に該当の記述を追加する等の利用者の活用実態を意識した改善を検討する必要がある。

―以上―

6.添付資料

6.1.中小企業の情報セキュリティ対策ガイドラインのプレスリリース資料

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

プレスリリース
2009 年 3 月 18 日
独立行政法人情報処理推進機構

「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した。

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）

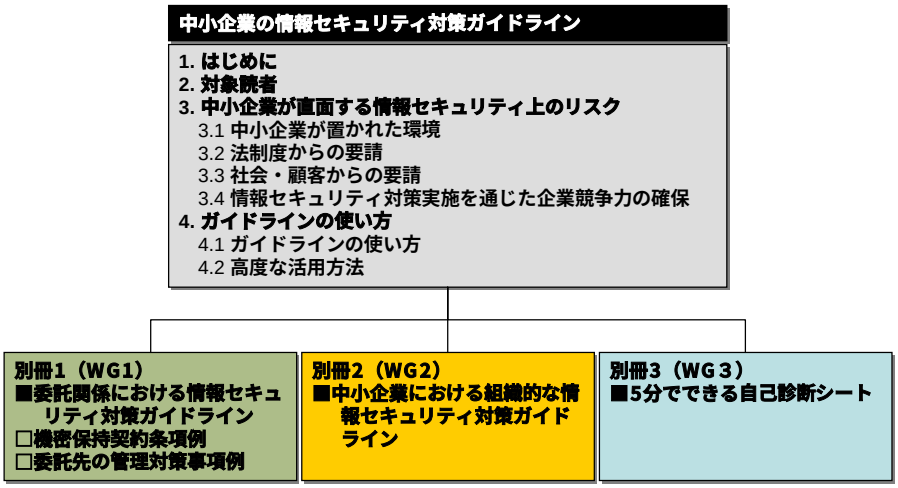


図 1．中小企業の情報セキュリティ対策ガイドラインの構成

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。

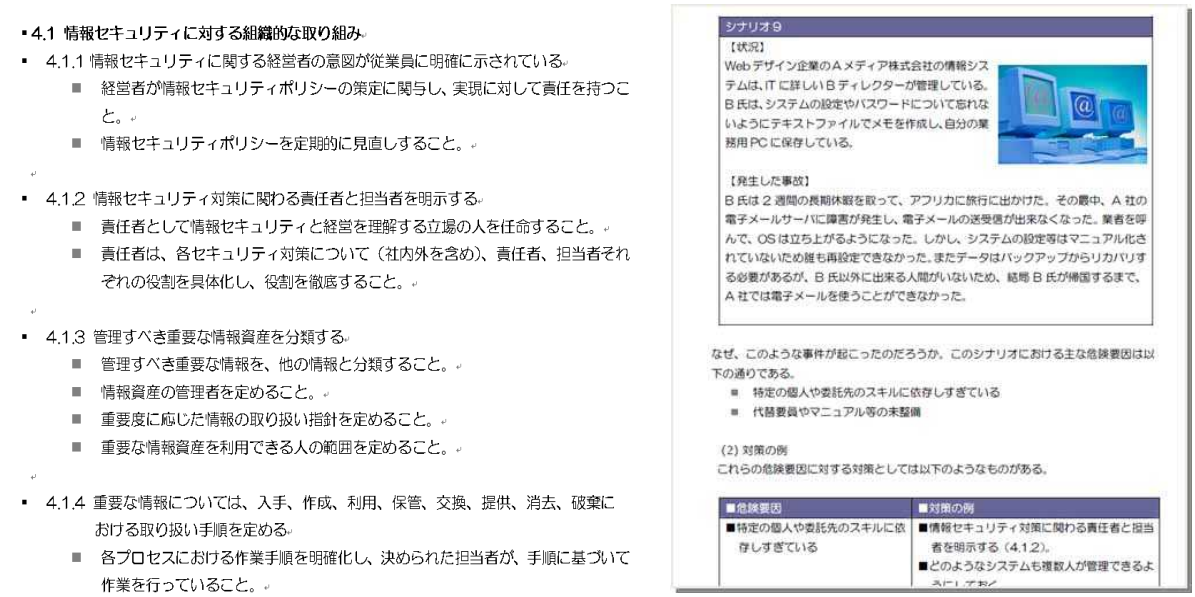
図 2．「5 分でできる自社診断シート」

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、情報漏えい等でそ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、担当者それぞれの役割を具体化し、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、破棄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）

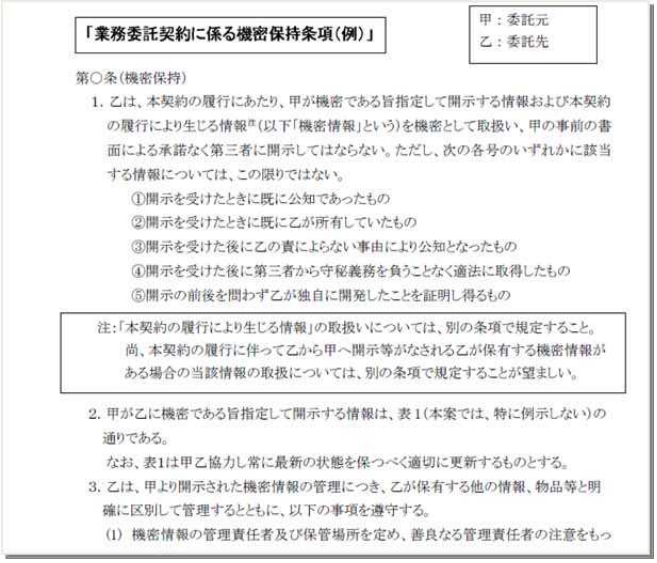
３）委託関係における情報セキュリティ対策ガイドライン

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。



「業務委託契約に係る機密保持条項(例)」

甲：委託元
乙：委託先

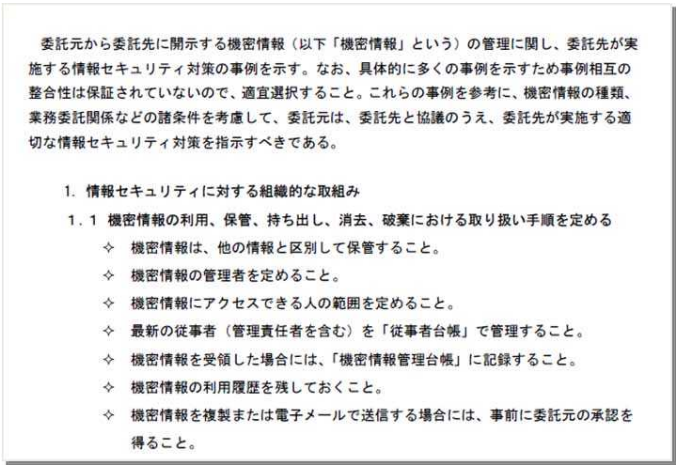
第○条(機密保持)

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 4-1　業務委託契約に係る機密保持条項（例）



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 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)。

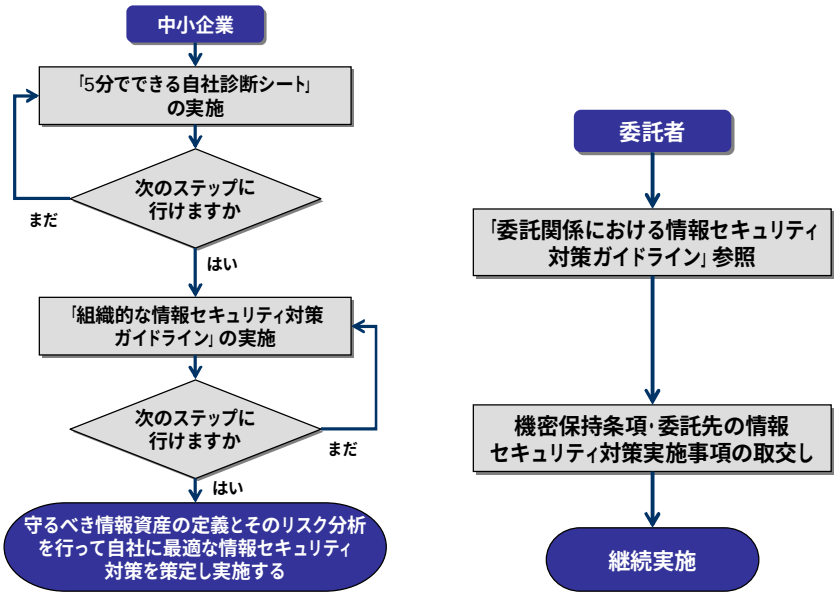


図 5．ガイドラインの使い方

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）。

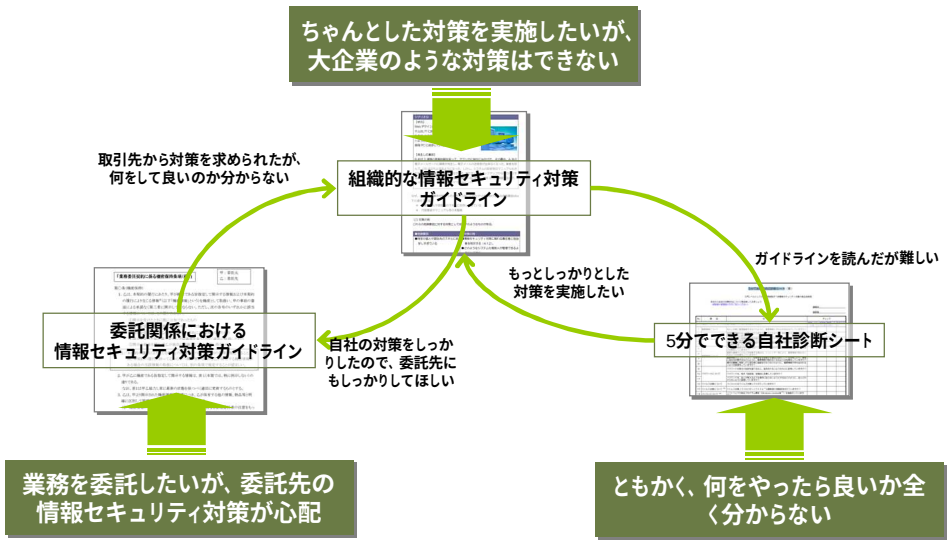


図 6．ガイドラインの様々な活用方法

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

6.2. 自社診断シート

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

6.3.組織的な対策ガイドラインの付録チェックシート

項目番号	内容	チェック
1. 情報セキュリティに対する組織的な取り組み状況		
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ますか？	□
1-2	情報セキュリティ対策に関わる責任者と担当者が明示されていますか？	□
1-3	管理すべき重要な情報資産を区分していますか？	□
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ていますか？	□
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っていますか？	□
1-6	従業者（派遣を含む）に対して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していますか？	□
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ていますか？	□
2. 物理的セキュリティ		
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っていますか？	□
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に配慮し適切に配置・設置していますか？	□
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っていますか？	□
3. 情報システム及び通信ネットワークの運用管理状況		
3-1	情報システムの運用に関して運用ルールを策定していますか？	□
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っていますか？	□
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っていますか？	□
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していますか？	□
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していますか？	
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		
4-1	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）を行っていますか？	□
4-2	重要な情報に対するアクセス権限の設定を行っていますか？	□
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）を行っていますか？	□
4-4	無線 LAN のセキュリティ対策（WPA2 の導入等）を行っていますか？	□
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っていますか？	□
5．情報セキュリティ上の事故対応状況		
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していますか？	□
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していますか？	□

※　「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」（2009 年 3 月版）[12]の付録１から引用。

[12] http://www.ipa.go.jp/security/fy20/reports/sme-guide/index.html

7.参考資料目録

・付録 A.　調査集計結果
  ・付録Ａ－①　【5 分でできる自社診断シート】回答集計結果
　　質問内容別　従業員規模・地域・業種　採点表（平均点）
  ・付録Ａ－②　【5 分でできる自社診断シート】回答集計結果
　　質問内容別　ワースト項目表（平均点）
  ・付録Ａ－③　ヒアリング回答企業属性概要一覧
  ・付録Ａ－④　ヒアリング重点項目コメント一覧
  ・付録Ａ－⑤　【組織的な対策ガイドラインの付録チェックシート】回答集計結果

・付録 B.　情報セキュリティ対策事例集

・付録 C.　ヒアリング調査シート