中小企業の情報セキュリティ対策ガイドライン

第2.1版

IPA
独立行政法人**情報処理推進機構**
技術本部 **セキュリティセンター**

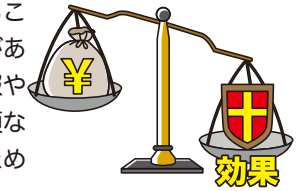
目　次

はじめに

1 経営者の皆様へ

本ガイドラインは、「中小企業の皆様に情報を安全に管理することの重要性についてご認識いただき、必要な情報セキュリティ対策を実現するための考え方や方策を紹介する」ことを目的としたものです。

情報セキュリティ対策は、経営に大きな影響を与えます！

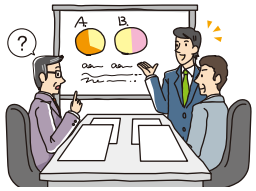


情報セキュリティ対策を実施して対外的にアピールすることで、企業としての評価を高めて売上を伸ばしている企業がある一方、情報セキュリティ対策を疎かにしたために秘密情報や個人情報の漏えいを発生させ、経営を揺るがしかねない高額な賠償金を支払った企業もあります。企業の継続的な発展のために、適切な情報セキュリティ対策を行いましょう。(➡P9)

経営者が法的・道義的責任を問われます！

現代社会では金銭や物品だけでなく、情報にも価値や権利が認められます。これに応じて、情報に関わる法律の整備も進んでいます。例えば個人情報保護法では、事業者に対して個人の権利利益の保護、安全管理措置及び委託先の管理監督が義務付けられており、これらへの違反が認められると行政指導が行われ、それに従わなかった場合には行為者や会社に罰金刑が課されます。また、民法上の不法行為とみなされた場合には、行為者本人が損害賠償責任を負う他、直接に関与していない経営者も原則として損害賠償責任(使用者責任)を問われることになります。さらに、場合によっては取締役や監査役は、別途、会社法上の忠実義務違反の責任を問われることもあります。こうした責任を果たすためには、担当者への丸投げではなく、経営者が自社の情報セキュリティについて明確な方針を示すとともに自ら実行していくことが必要です。(➡P13)

組織として対策するために、担当者への指示が必要です！



情報セキュリティ対策は、経営者が主導し、必要な範囲を網羅し、関係者と連携して組織的に実施しなければ機能しません。経営者はこれらを認識したうえで、必要となる取り組みを担当者に指示する必要があります。(➡P15)

2 対象組織と想定する読者

(1)対象組織

本ガイドラインは、業種を問わず中小企業及び小規模事業者(法人のほか、個人事業主や各種団体も含む)[1]を対象として作成されています。

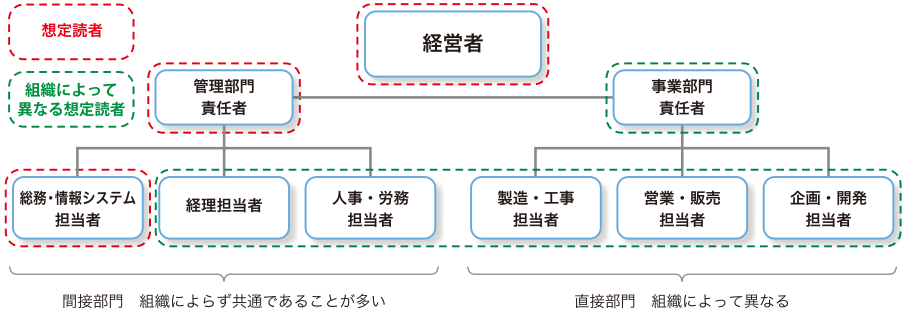
(2)想定読者

組織の経営者と、経営者の指示のもとで重要な情報を管理する方を読者と想定しています。

重要な情報とは、事業に必要で組織にとって価値があり、漏えい、改ざんまたは消失したときに大きな影響がある情報です。例えば自社でウェブサイトを運用したり、顧客情報や取引先の秘密情報をサーバーで管理するなど、ITを業務に活用している場合に、管理責任がある立場の方を読者と想定しています(図1)。

実際にはパソコンやネットワークなどを管理する総務、情報システム担当者や、財務情報や従業員の個人情報などを扱う経理、人事労務などの担当者、設計図や顧客情報などを委託先に提供する際に、情報セキュリティ対策を相手に求める製造や営業の担当者などが該当します。事業内容や組織構成によって読者層は異なりますので、それぞれの事情に応じて適宜に活用してください。

本ガイドラインの活用にあたって、情報セキュリティに組織的に取り組んだ経験は必要ありません。本ガイドラインと付録を用いることで、事業の特徴に応じた情報セキュリティポリシーを策定し、組織的に取り組むことができます。



【図1】本ガイドラインの対象組織・読者例

1 ▲表記上の煩雑さを回避するために、以下「中小企業」と総称します。

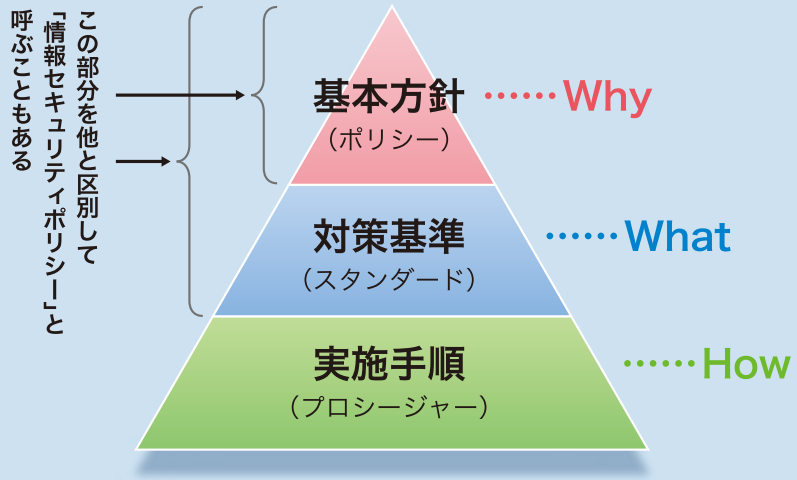
策定したポリシーに従い、組織的に情報セキュリティ対策を実践し、その結果をチェックして、必要に応じてポリシーを見直すことで、組織における情報セキュリティ対策をより高めることが可能です。

コラム

情報セキュリティポリシーとは

「ポリシー」という言葉は狭義の「理念」「方針」「声明」「宣言」などから、広義の「方法」「手段」「手順」などまで幅広い意味で使われています。またパソコンやネットワーク機器等では、セキュリティに関する設定を「セキュリティポリシー」と呼ぶことがあります。本ガイドラインでも、情報セキュリティのための様々な決めごとを総称して情報セキュリティポリシーと表現しています。

広義の情報セキュリティポリシーは、組織全員が情報セキュリティ対策を的確に実行するための共通ルールとして文書で定めたものです。規模の大きな組織では、管理レベルを統一するため、共通原則として基本方針と対策基準とを定め、部署ごとの事情に合わせて実施手順を策定することが多く、階層的な構成になることがあります(図2)。ポリシー策定の目的は、組織全員が情報セキュリティ対策を実行することですので、文書構成によらず実行方法を示す実施手順は不可欠です。



【図2】情報セキュリティポリシー文書構成例

3 全体解説

(1)本ガイドラインの構成

本ガイドラインは中小企業にとって重要な情報[2]を、漏えい、改ざんや消失などの脅威から保護することを目的とする情報セキュリティ対策の考え方や実践方法について説明するもので、本編2部と付録より構成されます(表1)。

【表1】本ガイドラインの全体構成

構成			概要
本編	第1部 経営者編		経営者が自らの責任で対応しなければならない事項について説明しています。
本編	第2部 管理実践編		重要な情報に対する管理責任がある立場の方向けに、組織的な情報セキュリティ管理の進め方について説明しています。
付録	付録1 情報セキュリティ5か条		企業の規模を問わず必ず実行していただきたい重要な対策を5か条にまとめ説明しています。
付録	付録2 5分でできる！情報セキュリティ自社診断		あまり費用をかけることなく実行することで効果がある対策25項目の診断シートです。
付録	付録3 わが社の情報セキュリティポリシー	ツールA リスク分析シート	情報資産管理台帳、脅威の状況、対策状況チェックをもとに自社のリスクを試算できます。
付録	付録3 わが社の情報セキュリティポリシー	ツールB 情報セキュリティポリシーサンプル	ツールAの結果をもとに、自社に適した情報セキュリティポリシーを策定するためのひな形です。

2 ▲**重要な情報** 重要な情報とは事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報のことです。経済的価値を指す“資産”を加え“情報資産”ということがあり、本ガイドラインでも“情報資産”といいます。情報資産には個人情報も含みますが、個人情報保護の目的は個人の人格的、財産的な権利利益の保護であり、企業の損害防止だけではないことに留意する必要があります。

(2)本ガイドラインの使い方

本ガイドラインは読者毎に次のような使い方を想定して作成していますが、読者の職場環境に応じて、参考になる箇所をご活用下さい。

①経営者の方

本編の第１部をお読みください。なお、従業員数が少なく経営者が情報システムの管理も担当されている場合は、②で紹介している本編第２部もお読みください。法人格の有無にかかわらず、個人情報やお客様の情報、自ら重要と考えている情報があるはずですので、このガイドラインに沿って対策を検討することをお勧めします。

②経営者の指示のもとで重要な情報を管理する方

本編第２部と付録をご覧の上、これまでの情報セキュリティへの取り組みに応じて下図のようにご活用下さい(図3)。

取組状況とアクション	本ガイドラインの活用方法
特に意識していない **Step1** まず始める	**「2.情報セキュリティ５か条　P.23」**を参照して、今すぐできる情報セキュリティ対策を実行してください。 進め方　「情報セキュリティ５か条(付録１)」を社内で配付など、まずできるところから開始してください。
できる範囲で実施している **Step2** 現状を知り改善する	**「3.情報セキュリティ自社診断　P.25」**を参照して、自社の状況を把握し、できていない対策の実行に努めてください。 進め方　「5分でできる自社診断シート(付録2)」を各部署に配付集計し、「情報セキュリティハンドブック ひな形」を使って、やるべきことを社内で周知しましょう。
組織的に取り組みたい **Step3** 本格的に取り組む	**「4.情報セキュリティポリシーの策定　P.28」**を参照して、情報資産とリスクを確認し、自社に適した情報セキュリティポリシーを定めてください。 進め方　「わが社の情報セキュリティポリシー(付録3)」を使い、ポリシーを策定して導入してください。
改善し向上したい **Step4** 改善を続ける	**「5.情報セキュリティ対策のさらなる改善に向けて　P.46」**を参照して、情報セキュリティの国際規格や認証制度を参考に情報セキュリティへの取り組みを組織的に改善、向上することで事業に役立ててください。

【図3】本ガイドラインを活用した情報セキュリティ対策の進め方

第１部　経営者編

経営者編では、情報セキュリティ対策に関して、
経営者が認識し、
自らの責任で対応しなければならない
事項について説明します。

1 情報セキュリティ対策を怠ることで企業が被る不利益

ITの普及や利活用により経営効率が向上した反面、ITの普及以前には想定し得なかった秘密情報や個人情報の漏えいによる、高額の賠償請求事例や金銭的損失を伴う事故が増えています。さらに、近年では事故やその影響も多様化し、金銭的損失以外の不利益も顕著になっています。

ここでは、情報セキュリティ対策の必要性に対する理解を深めていただくために、対策が不十分なために起きる事故と、それにより企業が被る主な不利益を次に挙げる４点に要約して説明します。こうした事故による不利益は、後述する情報セキュリティ対策を行うことで、経営上許容できる範囲まで減らすことができます。

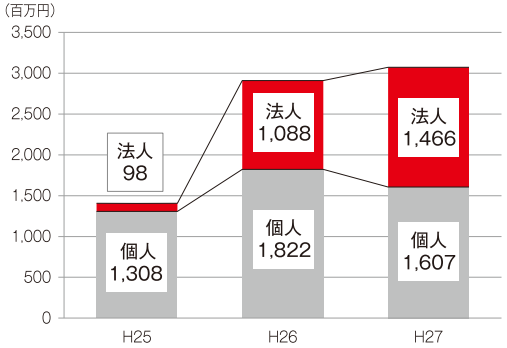
(企業が被る主な不利益)

●金銭の損失　●顧客の喪失　●業務の喪失　●従業員への影響

(1)金銭の損失

個人情報の漏えいが発生すると盛んに報道されることからも明らかなように、個人情報の適切な保護は人々にとって重要な関心事となっています。また、取引先などから預かった機密情報を万一漏えいした場合は、取引先や、さらにはその先の顧客などから損害賠償請求を受けたり、漏えい情報を記録していたデータベース等の利用を差し止められて自社業務の深刻な停滞を招くなど、大きな経済的損失を受けることになります。このような、情報漏えい等の情報セキュリティに関わる事故に伴う経済的損失例を表2に示します。

一方、こうした損害賠償などによる損失だけでなく、インターネットバンキング利用時の偽サイトへの不正送金やクレジットカードの不正利用などで直接的な損失を被る企業の数も増えています。警察庁の調査によれば、平成27年度の被害額は合計30億7300万円(法人口座14億6600万円 個人口座16億700万円)にも及んでいます(図4)。



【図４】口座種別毎の不正送金被害状況

警察庁広報資料
「平成27年中のインターネットバンキングに係る不正送金事犯の発生状況等について」

中小企業の情報セキュリティ対策ガイドライン

【表2】最近のサイバー攻撃等による情報漏えい等の経済的損失例

分　類	事故概要	損失額等
情報漏えい	状況 **教育サービス事業者で顧客の個人情報3504万件が漏えい(2014年)** 要因 システム開発・運用を行っているグループ会社の業務委託先の再委託先社員による不正取得と名簿業者への売却	▲お詫び対応の原資として、200億円を準備 ▲漏えいが確認された顧客にお詫びと報告の手紙を送付 お詫びの品として図書カード500円の金券/基金への寄付　いずれかの選択を用意 (当事者の公表資料による) ▲被害者の会集団訴訟による係争中(2016年8月時点) 原告1170名 請求額原告一人あたり55000円、総額6435万円 (2016年8月時点　被害者の会公表資料による)
	状況 **株式を公開している雑貨卸売事業者でインターネット上の株主向けサービスに登録された株主の個人情報6187件(他社の株主個人情報含め総数12014件)が漏えい(2015年)** 要因 サービス運営委託先のサービスサイトへの不正アクセス	▲インターネット上の株主向けサービス導入中止 ▲サービス優待券進呈/クーポン券との交換お詫びとして1000円の金券配付 (当事者の公表資料による)
	状況 **航空会社の顧客の個人情報4131件が漏えい(2014年)** 要因 ウイルスに感染した3台の業務端末が顧客情報管理システムと交信して顧客の個人情報の一部を香港所在の外部サーバーに送信	▲ギフト券への特典交換サービスを一時停止 (当事者の公表資料による) ▲情報漏えいのお詫びとして1名あたり500円の金券配付 (報道資料による)
	状況 **菓子食品製造事業者で顧客の個人情報20万9999件が漏えい(2015年)** 要因 ウェブサイトへの不正アクセス(データベースの不正操作による攻撃)	▲ウェブサイトでの通販・工場見学予約機能の利用停止～全面再開まで約3か月 (当事者の公表資料による) ▲お詫びとして500円の金券配付 (報道資料による)
	状況 **国内半導体製造事業者の技術に関する機密情報が韓国の同業者に漏えい(2014年)** 要因 内半導体製造事業者提携先の元従業員が不正に研究データを持ち出し韓国同業者に提供	▲不正競争防止法に基づく損害賠償等請求で国内半導体製造事業者が韓国同業者と2億7800万米ドル(330億円)の和解金支払いで合意 ▲和解を機に協業拡大を合意 (当事者の公表資料による)
ウィルス感染	状況 **米国の病院で院内ネットワークで共有する電子カルテシステムがウイルスによる攻撃により動作しなくなり診療不能に(2016年)** 要因 電子カルテシステムがランサムウェア[3]に感染し、ファイルが暗号化されたため	▲暗号化を解除するために約1万7000ドル(192万円)相当の仮想通貨であるビットコインを攻撃者に支払い暗号解読キーを入手 (当事者の公表資料による)
情報漏えい	状況 **メガネ販売事業者でオンラインショップ顧客のクレジットカード情報2059件の漏えい(2013年)** 要因 ソフトウェアの脆弱性を利用したウェブサーバーへの不正アクセス	▲流出可能性最大12036名に対して1000円分商品券配付 ※実際の件数は2059件 ▲クレジットカード不正利用最大損害想定額305万3000円 ▲オンラインショップ停止止及びアクセス遮断～再開まで約5か月 (当事者の公表資料による)
ウェブサイト改ざん	状況 **観光バス事業者のホームページが改ざんされ閲覧するとウイルスに感染する恐れ(2014年)** 要因 不正アクセスによりサイトが改ざんされサイトを閲覧すると仕掛けられた不正なプログラムが実行されウイルスに感染	▲17日間のサイト閉鎖により機会損失1億円程度 (報道資料による)

3 ▲ランサムウェア　コンピュータウイルスの一種で、感染したパソコン等に保存されているファイルを外部に流出させるのではなく、暗号化してパソコンの所有者が使えないようにしてしまうものを言います。攻撃者は、ファイルを復号するための暗号鍵を提供する見返りとして金銭を得ることによって目的を達成します。他のコンピュータウイルスと同様、発信者を詐称した電子メールに添付されているファイルや、改ざんされた正規のウェブサイトなどを通じて感染します。

はじめに
第1部
1 情報セキュリティ対策を怠ることで企業が被る不利益
2
3
第2部
1
2
3
4
5
用語
INDEX

(2)顧客の喪失

情報セキュリティ上の事故を発生させると、その原因が何であれ、事故を起こした企業に対する管理責任が問われ、社会的評価は低下します。同じ製品やサービスを提供している企業が他にあれば、事故を起こしていない企業の製品やサービスを選択する顧客が増えるのは自然なことであり、事故の発覚直後には大きなダメージを受けることになります。事故を起こした企業が再発防止に努め、事故を起こさずに事業を続けていく中で、低下した社会的信用は徐々に回復することもありますが、回復もままならずに事業の存続が困難になる場合もあります。

表2の教育サービス事業者の場合、顧客情報漏えいの影響により既存会員の退会が増え、さらに新規営業活動を自粛した結果、前年度比で約25%程度会員が減少しています。(事業報告書・報道資料による)

(3)業務の喪失

情報漏えいに限らず、情報セキュリティ上の事故が発生すると、被害の拡大を防止するため、自社で運用しているサーバーの停止や、インターネットへの接続の遮断などを行います。この結果、インターネットを通じた取引先からみると、営業を停止しているのと同じ状態になるため、措置を講じている間は営業機会の喪失となります。さらに、販売管理、会計などの基幹システムや、電子メールが使えなくなったり、クラウドサービスに接続できなくなったりすることで、社内の業務が停滞してしまいます。

2015年に発生した特殊法人における個人情報漏えい事故の場合、ウェブサイトの一部コンテンツを脆弱性の確認のため約6か月間停止するとともに、職員が使用する外部向け電子メールを使用禁止することになり、業務に大きな支障が出ました。(当事者の公表資料による)

(4)従業員への影響

情報セキュリティ対策の不備を悪用した内部不正が容易に行えるような職場環境は、従業員のモラル低下を招く要因となります。さらに事故を起こしたにもかかわらず、従業員のみを罰して経営者が責任を取らないような対応をとることで、従業員が働く意欲を失う恐れがあります。情報漏えいなどの事故による企業としてのイメージダウンを嫌って転職する従業員も現れます。

また、従業員の個人情報が適切に保護されなければ、従業員から訴訟を起こされることも考えられます。

2 経営者が負う責任

情報セキュリティ対策に関する経営者の責任について、法的責任と社会的責任との観点から説明します。

(1)経営者などに問われる法的責任

企業が個人情報などの管理義務がある情報を適切に管理していなかった場合、経営者や役員、担当者は業務上過失として表3に例示するような刑事罰その他の責任を問われることになります。

- 個人情報やマイナンバーに関する違反の場合は刑事罰が科されます。また、その場合は個人情報保護委員会[4]による立入検査を受ける責任もあります。
- 民法上の不法行為とみなされた場合は、経営者が個人として損害賠償責任を負う場合もあります。

【表3】情報管理が不適切な場合の処罰など

情報の種類	根拠法による規定		処罰など
個人情報 (マイナンバー含む)	個人情報保護法	1)虚偽申告・命令違反	6月以下の懲役又は30万円以下の罰金、業務停止命令
		2)データベース提供罪[5] (83条・改正で新設)	1年以下の懲役又は50万円以下の罰金
	民法(不法行為による損害賠償、709条)		損害賠償
	建設業法		役員または使用人が懲役刑に処せられた場合は営業停止処分
	マイナンバー法(両罰規定)		秘密を漏らし、又は盗用した者は、3年以下の懲役若しくは150万円以下の罰金 行為者を雇用する法人に対しても罰金刑
他社から預かった秘密情報 (外部非公開のデータなど)	不正競争防止法の営業秘密 不正取得・利用行為など		損害賠償、信頼回復措置
自社の秘密情報 (非公開のノウハウなど)	不正競争防止法の営業秘密 不正取得・利用行為など		善管注意義務違反に対する関係者からの損害賠償請求(経営者に対する民事訴訟)
上場会社の株価に影響を与える可能性のある重要な未公開の内部情報	金融商品取引法		内部情報をもとに取引が行われた場合、罰金または課徴金の可能性

4 **▲個人情報保護委員会**　個人情報保護委員会は公正取引委員会と同様の高い独立性を有する機関です。

5 **▲データベース提供罪**　改正個人情報保護法で新設され、役員・従業者等が不正な利益を図る目的で個人情報データベース等を他者にの提供等したり盗用した場合は処罰対象になります。

(2)関係者や社会に対する責任

適切に管理することを前提に預かった情報を漏えいしてしまった場合に問われるのは、前述の法的責任に加え、その情報の提供者や顧客などの関係者に対する責任もあります。さらに、情報漏えい事故は、営業機会の喪失、売上高の減少、企業のイメージダウンなど、自社に損失をもたらし、会社役員は会社法上の責任（会社に対する損害賠償責任）を負っているので、場合によっては株主代表訴訟を提起されることもあり得ます。さらには、取引先との信頼関係の喪失、業界全体のイメージダウンにもなってしまいます。したがって、情報セキュリティ対策は、顧客・取引先・従業員・株主などに対する経営者としての責任を果たすためにも重要です。

コラム

個人情報保護法

個人情報保護法は企業（個人情報データベース等を事業の用に供している者　個人事業主も含む）の個人情報の取り扱いのルールを定めた法律です。保有する個人情報の数が「過去6月以内のいずれの日においても5000を超えない者」は適用除外とされていましたが、平成27年9月9日の改正によりすべての事業者に適用されるため、保有する個人情報が少なくても、法律で定められたルールを遵守しなければなりません。また、人種、信条、病歴などが含まれる個人情報の取得には原則として本人の同意が必要になります。

3 経営者は何をすればよいか

企業で情報セキュリティを確保するための、経営者の役割を説明します[6]。情報セキュリティの確保に向けて、経営者は、(1)に示す「3原則」について認識した上で、(2)に示す「重要7項目の取組」の実施を管理者層に指示する必要があります。

(1)経営者が認識すべき「3原則」

経営者は、以下の3原則を認識し、対策を進める必要があります。

原則1　情報セキュリティ対策は経営者のリーダーシップで進める

経営者は、IT活用を推進する中で、情報セキュリティ上のリスクを認識し、自らリーダーシップを発揮して対策を進めることが必要です。現場の従業員はサイバー攻撃、ウイルス感染、内部不正などの悪意による事故や、メールの誤送信、ノートPCの紛失などの不注意による事故が身近で発生している現状で、安心して業務に従事できる環境を求める一方、利便性が低下し、面倒な作業を伴う対策には抵抗感を示しがちです。そこで、さまざまな脅威がもたらすリスクに対する対策は、経営者が判断して意思決定し、自社の事業に見合った情報セキュリティ対策を実施します。

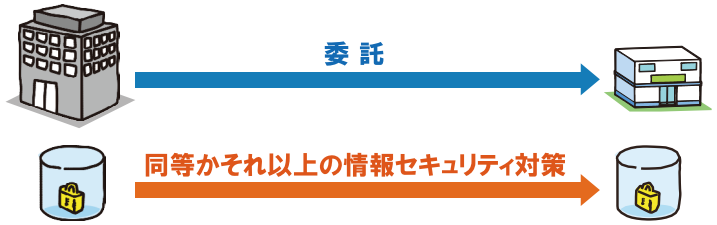
6 ▲本項は経済産業省及びIPAが2015年12月に「サイバーセキュリティ経営ガイドライン」(http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html)として策定した内容を、中小企業向けに編集したものです。

サイバーセキュリティはコンピュータやネットワークで扱う電子情報に対する故意の攻撃から保護すること意味し、情報セキュリティは、電子情報に加え書類やフィルムなどの物理媒体、さらには会話などの音声で扱われる重要な情報を、故意や不注意といった人為的な脅威だけでなく、自然災害や情報機器の故障などの脅威からも保護することを意味します。

パソコンやインターネットが世界中に普及した結果、コンピュータやネットワーク上での攻撃や不正が多発しているため、サイバーセキュリティは、組織の規模や業種を問わず喫緊の課題になっています。なお、「サイバーセキュリティ」と「情報セキュリティ」の定義の違いについては、本書末尾の用語集をご参照ください。

原則 2　委託先の情報セキュリティ対策まで考慮する

業務の一部を外部に委託するのにあたって重要な情報や個人情報を委託先に提供する場合、委託先がどのような情報セキュリティ対策を行っているか考慮する必要があります。委託先に提供した情報が、委託先の不備で漏えいしたり、改ざんされたとしても、事故の影響を受ける者から委託先に対する管理責任を問われることになり、取引停止や損害賠償請求にもなりかねません。そこで、委託先や、共同で仕事を行っているビジネスパートナーなどの情報セキュリティ対策に関しても自社同様に十分な注意を払い、必要に応じて委託先が実施している情報セキュリティ対策も確認し、不十分な場合は対処を検討します。



原則 3　関係者との情報セキュリティに関するコミュニケーションはどんなときにも怠らない

業務上の関係者（顧客、取引先、委託先、代理店、利用者、株主など）からの信頼を高めるには、普段から自社の情報セキュリティ対策や、事故が起きたときの対応について、関係者に明確に説明できるように経営者自身が理解し、整理しておくことが重要です。情報セキュリティに対する取り組み方針を関係者に伝えておけば、周囲にサイバー攻撃などによる事故などが発生した際にも、常日頃の取組み方針を知っている関係者に不安を与えることなく、信頼関係を維持することができます。

(2)経営者がやらなければならない「重要7項目の取組」

経営者は、以下の「重要7項目の取組」について、自ら実践するか、実際に情報資産や情報システムなどの管理を実践する管理者層に対して指示することで、確実に実施することが必要です。

取組 1　情報セキュリティに関する、組織全体の対応方針を定める

情報セキュリティ対策を組織的に実施する意思を、関係者に明確に示すために、情報セキュリティに関する方針を定め、要求に応じて提示できるようにしておきます。

例）

「当社は中小企業の情報セキュリティ対策ガイドラインに基づき情報セキュリティ対策を実践する。」

「当社は顧客情報の流出防止を徹底することから情報セキュリティ対策を開始する。」

取組 2　情報セキュリティ対策のための資源（予算、人材など）を確保する

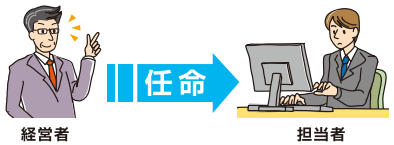
後述する情報セキュリティ対策を実施するために、必要な予算と人材を確保します。これには万が一事故（インシデント[7]）が起きてしまった場合、被害を最小限に止めるために、あらかじめ準備することも含みます。

7 ▲インシデント　リスクが発現・現実化した事故のことを言います。コンピュータやネットワークに関わる事故のことをインシデント（Incident）ということがあり、慣例句として使われます。本ガイドラインでは事故とインシデントとを併用します。情報セキュリティの場合、情報の漏えい、改ざんや消失、情報システムの予期せぬ停止または極端な性能の低下などがインシデントに相当します。

取組３　担当者に必要と考えられる対策を検討させて実行を指示する

事業を行う上で見込まれる情報セキュリティのリスクを把握した上で、必要十分な対策を検討させます。検討した対策ごとに予算を与え、担当者を任命し、実行を指示します。実施する対策は、社内ルールとして文書にまとめておけば、従業員も実行しやすくなり、取引先などにも取り組みを説明する際に役に立つので、併せて指示します。

例）従業員との守秘義務契約
事務所の入退管理
パソコンの管理



人事担当者
総務担当者
情報システム担当者

取組４　情報セキュリティ対策に関する定期・随時の見直しを行う

情報セキュリティ対策を最初から最適な形で実現することはどんな会社でも難しいものです。また情報技術は進化が早く、加えて脅威も変化します。そのため、一度定めた対策がいつまでも有効であるとは限らないので、取組3で定めた情報セキュリティ対策について、定期または随時に見直して、必要な改善や追加の対策を決めるように担当者に指示します。

取組５　業務委託や外部サービスを利用する場合は、情報セキュリティに関する責任範囲を明確にする

業務の一部を外部に委託（共同実施も含む）する場合は、相手先でも少なくとも自社と同等の対策が行われるようにしなければなりません。そのためには契約書に情報セキュリティに関する相手先の責任や実施すべき対策を明記し、合意する必要があります。また必要に応じて相手先を訪問し、対策の実施状況を確認します。

ITシステム（電子メール、ウェブサーバー、ファイルサーバー、業務アプリケーションなど）に関する技術に詳しい人材がいない場合には、外部サービスを利用したほうが、コストと情報セキュリティ対策との両面から有利なときがあります。ただし、無償の外部サービスなど情報セキュリティ対策を求めることが難しい場合や、有償であっても個別契約等でサービス提供者の責任や対策を規定することが難しい場合もあるので、利用規約やサービスに付随する情報セキュリティ対策等を確認したうえで選定するよう担当者に指示する必要があります。

取組６　情報セキュリティに関する最新動向を収集する

情報技術の進化の早さから、脅威やその対策は目まぐるしく変化します。自社だけで全ての脅威や対策を把握することは困難なため、情報セキュリティに関する最新動向を発信している公的機関[8]などを把握しておき、常時参照することで、新たな脅威に備えるようにします。また、知り合いやコミュニティへの参加で情報交換を積極的に行い、得られた情報について、業界団体、委託先などと共有します。

取組７　緊急時の社内外の連絡先や被害発生時の対処について準備しておく

情報セキュリティ対策を実施するとともに、万が一のインシデントに備えて、緊急時の連絡体制を整備します。さらに、その連絡体制がうまく機能するかをチェックするためインシデントを想定した模擬訓練を定期的に行うと理想的です。一方、インシデントにより情報資産の漏えいなどの被害が出た場合には、情報資産の提供元や個人情報の本人などへの連絡も必要となることがあり、速やかに連絡可能なようにあらかじめ準備しておくとともに、経営者の対応についても、あらかじめ決めておけば、冷静で的確な対応が可能になります。

8 **▲情報セキュリティに関する最新動向を発信している公的機関**
IPA（独立行政法人情報処理推進機構）のウェブサイト
https://www.ipa.go.jp/security/index.html
NISC（内閣サイバーセキュリティセンター）のウェブサイト
http://www.nisc.go.jp/

コラム

身近な情報資産と法律

『営業秘密』

企業が持つ営業情報や技術情報などの中には、秘密とすることで他社との差別化や、競争力の源泉となる情報もあります。そのような情報が漏えいすると、研究開発投資の回収機会を失ったり、社会的な信用の低下により顧客を失ったりと大きな損失を被ることになります。秘密としている情報を不正競争防止法により営業秘密として法的保護を受けるためには、次の①～③の要件をすべて満たす必要があります。

①秘密管理性（秘密として管理されていること）
②有用性（生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であること）
③非公知性（公然と知られていないこと）

『ソフトウェアライセンス』

業務で利用している市販のアプリケーションソフトウェアはライセンスの購入により使用権が認められます。その一方、法律では知的財産として開発者（正確には権利保有者）の権利が定められています。このため当該ソフトウェアの不正利用（無断複製、使用許諾条件に反した利用等）を行った場合は、状況如何によって経営者が責任を問われ、著作権侵害による損害賠償請求や、故意に行った場合には犯罪として刑事罰の対象になります。法人が著作権侵害を行った場合には、その法人自体に対して3億円以下の罰金刑とする規定が設けられています。社内で法制度の遵守体制を検討する際に、併せて考慮すべき事項です。

第２部　管理実践編

管理実践編では、情報資産や情報システムなどの管理を実践される方（管理者層）を対象として、情報セキュリティポリシーの策定と実行について説明します。
なお、第２部の説明は、第１部の３で示した「3原則」「重要7項目の取組」について理解していることを前提としています。

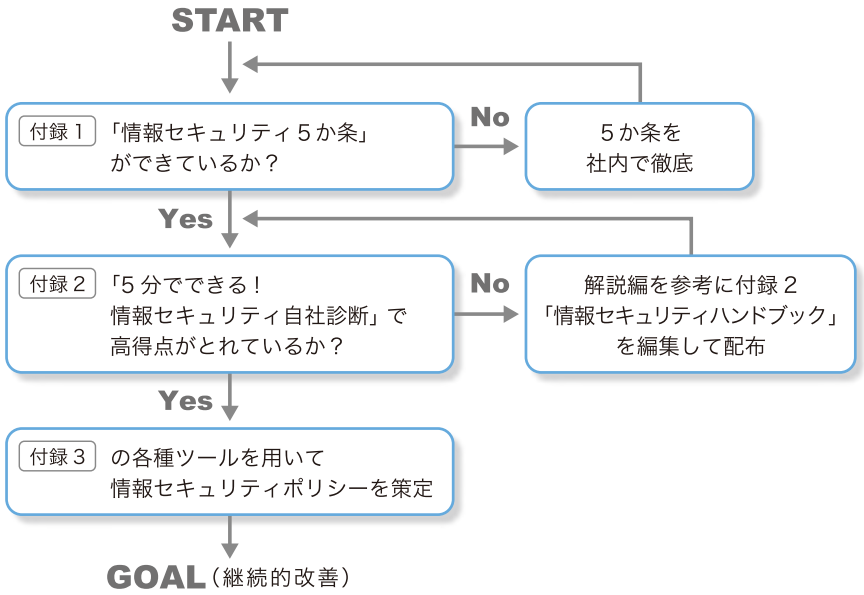
中小企業の情報セキュリティ対策ガイドライン

1 情報セキュリティ管理実践の進め方

ここでは、経営者によって示された情報セキュリティ対策に関する方針のもとで、どのように管理実践を進めていくかについて説明します。有効な対策を組織全体で実行するためには、どのような情報資産があるかをもれなく把握し、想定される脅威を特定した上で、対策を検討し、情報セキュリティポリシーとしてとりまとめる必要があります。

しかし、こうした作業を行うには情報セキュリティに関する知識や経験が必要となるため、それらの知識や経験に長けた人材がいないと対策が進まくなることも考えられます。

そこで、本ガイドラインでは、規模の小さな企業や、これまで十分な情報セキュリティ対策を実施してこなかった企業等を対象に、すぐにできることから開始して、段階的にステップアップすることで、企業それぞれの事情に適した対策が実施できるように進め方を説明するとともに、実践のために各種の付録を用意しました。次図を参考に自社の状況にあった進め方をしてください(図5)。



【図5】本ガイドラインの使用方法

2 情報セキュリティ５か条

情報セキュリティ5か条(付録1)では、企業の規模に関わらず、必ず実行していただきたい重要な対策を5か条にまとめています(表4)。

インターネットの普及に伴い様々な脅威が現れ、攻撃者の手口は年々巧妙かつ悪質になっています。

しかし、攻撃手法には、脆弱性を突く、ウイルスを使う、ソーシャルエンジニアリングを使うなど、共通的な部分があります。情報セキュリティ５か条は、これら攻撃手法の共通部分に対する基本的対策をまとめたものですので、必ず実行しましょう。

【表4】情報セキュリティ５か条

① OS やソフトウェアは常に最新の状態にしよう！	OSやソフトウェアのセキュリティ上の問題点を放置していると、それを悪用したウイルスに感染してしまう危険性があります。お使いのOSやソフトウェアには、修正プログラムを適用する、もしくは最新版を利用するようにしましょう。 **対策例** ●Windows Update(Windows OSの場合)/ソフトウェア・アップデート(macOSの場合)/OSバージョンアップ(Android の場合) ●Adobe Flash Player／Adobe Reader／Java実行環境(JRE)など利用中のソフトウェアを最新版にする
② ウイルス対策ソフトを導入しよう！	ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。ウイルス対策ソフトを導入し、ウイルス定義ファイル(パターンファイル)は常に最新の状態になるようにしましょう。 **対策例** ●ウイルス定義ファイルが自動更新されるように設定する ●統合型のセキュリティ対策ソフト(ファイアウォールや脆弱性対策など統合的なセキュリティ機能を搭載したソフト)の導入を検討する
③ パスワードを強化しよう！	パスワードが推測や解析されたり、ウェブサービスから窃取したID・パスワードが流用されることで、不正にログインされる被害が増えています。パスワードは「長く」「複雑に」「使い回さない」ようにして強化しましょう。 **対策例** ●パスワードは英数字記号含めて10文字以上にする ●名前や誕生日、簡単な英単語などはパスワードに使わない ●同じパスワードをいろいろなウェブサービスで使い回さない

中小企業の情報セキュリティ対策ガイドライン

④ 共有設定を見直そう！	データ保管などのクラウドサービスやネットワーク接続の複合機の設定を間違ったため無関係な人に情報を覗き見られるトラブルが増えています。クラウドサービスや機器が、無関係な人に共有されていないか設定を確認しましょう。 **対策例** ●クラウドサービスの共有範囲を限定する ●ネットワーク接続の複合機やカメラ、ハードディスク（NAS）などの共有範囲を限定する ●従業員の異動や退職時に設定の変更（削除）漏れがないように注意する。
⑤ 脅威や攻撃の手口を知ろう！	取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。 **対策例** ●IPAなどのセキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る ●利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認する

3 5分でできる！情報セキュリティ自社診断

5分でできる！情報セキュリティ自社診断（付録2）は、25の設問に答えるだけで自社のセキュリティレベルを把握することができる自社診断シートと、その解説パンフレットに加え、情報セキュリティ対策を従業員に会社のルールとして周知する時に活用できる情報セキュリティハンドブックのひな形で構成しています。自社診断シートは、あまり費用をかけることなく、実行することで効果がある情報セキュリティ対策を25項目に絞り込んだものです（表5）。

自社診断は、各項目の実施状況に応じて、「実施している：4点」「一部実施している：2点」「実施していない または わからない：0点」で採点し、全項目の合計点によって評価し、自社の弱点を把握します。なお、ネットワーク接続の複合機やハードディスクの共有設定（No.4）、ウェブサービス（No.5）、無線LAN（No.9）、クラウドサービス（No.19）など、自社で利用していないものに関する項目は便宜的に「4点」で計算します。

No.1～18の設問は従業員の情報セキュリティに関する知識や、組織のルールによって実施状況が異なる可能性があります。情報セキュリティは、些細な対策漏れが事故に発展することが多く、対策が不十分な部署や従業員がいた場合には全体の対策レベルが下がってしまいます。そのため従業員一人ひとりが実施すべき対策は、情報セキュリティハンドブックひな形を自社のルールに合わせて編集し、全従業員に配付するなどして周知を高め、全体のレベルアップを図り100点を目指してください。

【表5】情報セキュリティ自社診断のための25項目

の項目は、すべての従業員が実施すべき対策、の項目は、会社として実施すべき対策です。

No.	診断項目	診断内容
1	Part1 基本的対策	Windows Update＊1を行うなどのように、常にOSやソフトウェアを安全な状態にしていますか？
2		パソコンにはウイルス対策ソフトを入れてウイルス定義ファイル＊2を自動更新するなどのように、パソコンをウイルスから守るための対策を行っていますか？
3		パスワードは自分の名前、電話番号、誕生日など推測されやすいものを避けて複数のウェブサイトで使い回しをしないなどのように、強固なパスワードを設定パスワードの設定を強化していますか？
4		ネットワーク接続の複合機やハードディスクの共有設定を必要な人だけに限定するなどのように、重要情報に対する適切なアクセス制限を行っていますか？
5		利用中のウェブサービス＊3や製品メーカーが発信提供するセキュリティ注意喚起を確認して社内共有するなどのように、新たな脅威や攻撃の手口を知り対策を社内に共有する仕組みはできていますか？

中小企業の情報セキュリティ対策ガイドライン

No.	診断項目	内　　容
6	Part2 従業員としての対策	受信した不審な電子メールの添付ファイルを安易に開いたり本文中のリンクを安易に参照したりしないようにするなど、電子メールを介したウイルス感染に気をつけていますか？
7		電子メールを送る前に目視にて送信アドレスを確認するなどのように、宛先の送信ミスを防ぐ仕組みを徹底していますか？
8		重要情報をメールで送る時は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？
9		無線LANを利用する時は強固な暗号化を必ず利用するなどのように、無線LANを安全に使うための対策をしていますか？
10		業務端末でのウェブサイトの閲覧や、SNSへの書き込みに関するルールを決めておくなどのように、インターネットを介したトラブルへの対策をしています
11		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？
12		重要情報を机の上に放置せず書庫に保管し施錠するなどのように、重要情報の紛失や漏えいを防止する対策をしていますか？
13		重要情報を社外へ持ち出す時はパスワード保護や暗号化して肌身離さないなどのように、盗難や紛失の対策をしていますか？
14		離席時にコンピュータのロック機能を利用するなどのように、他人に使われないようにしていますか？
15		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？
16		退社時に机の上のノートパソコンや備品を引き出しに片付けて施錠するなどのように、盗難防止対策をしていますか？
17		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？
18		重要情報を廃棄する場合は、書類は細断したり、データは消去ツールを使ったりするなどのように、重要情報が読めなくなるような処分をしていますか？

はじめに 第1部 1 2 3 1 2 第2部 3 5分でできる！情報セキュリティ自社診断 4 5 用語 INDEX

No.	診断項目	内　　容
19	Part3 組織としての対策	従業員を採用する際に守秘義務や罰則規定があることを知らせるなどのように、従業員に秘密を守らせていますか？
20		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、従業員に意識付けを行っていますか？
21		クラウドサービスなど外部サービスを利用する時は利用規約やセキュリティ対策を確認するなどのように、サービスの安全・信頼性を把握して選定していますか？
22		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、取引先に秘密を守ることを求めていますか？
23		社内外での個人所有のパソコンやスマートフォンの業務利用を許可制にするなどのように、業務で個人所有端末の利用の可否を明確にしていますか？
24		秘密情報の漏えいや紛失、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		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？

＊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　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「パターンファイル」とも呼ばれる
＊3　インターネットバンキング、ソーシャルネットワーキングサービス(SNS)、ウェブメール、カレンダーなどインターネット経由で利用するサービスの総称

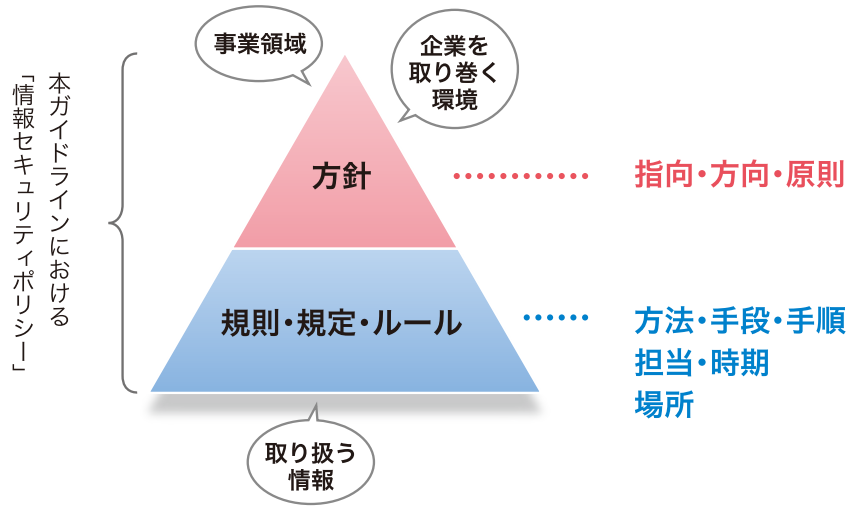
4 情報セキュリティポリシーの策定

自社に適した情報セキュリティ対策を行うには、まず企業が活動を行う際に直面する情報セキュリティ関連のリスクを確認し、組織として実行すべき情報セキュリティ対策を組織の正式な規則として情報セキュリティポリシー（以下、「ポリシー」と言います。）を定め（本書18ページ、取組３）、これに基づいて従業員が行動することでリスクを現実的に問題のないレベルまで封じ込める必要があります。ここでは、中小企業でこうした取り組みを効率よく行うための手順について説明します。

(1)基本的な考え方

① 自社に適合したポリシーを策定

企業が直面するリスクは、事業領域や取り扱う情報、企業を取り巻く環境によっても異なります。したがって、ポリシーのサンプルを入手して社名を変えるだけではうまく機能しません。本章で示す手順に従い、自社に適したポリシーを作成することが重要です。本ガイドラインは、単一事業を営む中小企業を主な対象にしていますので、対策基準と実施手順とを１階層に簡素化したポリシーの策定について説明します（図6）。

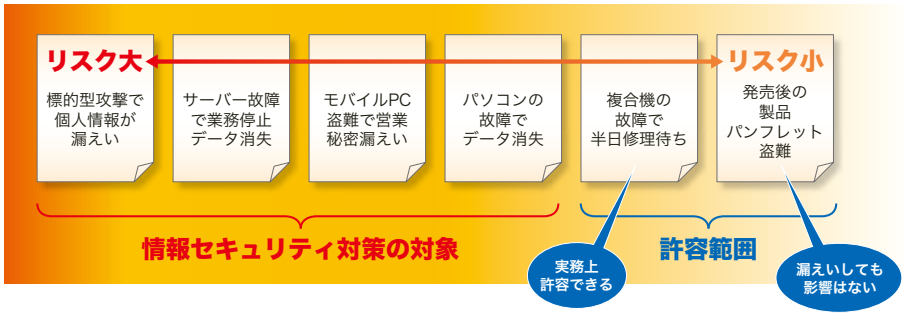


【図6】本ガイドラインで策定する中小企業向けセキュリティポリシー文書構成

② 情報セキュリティリスク[9]の大きなものから重点的に対策を実施

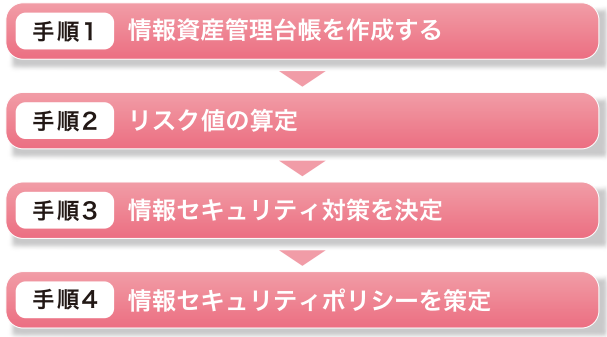
すべてのリスクに完全に対処しようとすると多額の出費が必要です。かといって、「そんな費用は払えない」ことを理由に対策をしないのも問題外です。限られた予算を有効に使うには、あらかじめリスク分析[10]を行い、いつ事故が起きてもおかしくない、あるいは事故が起きると大きな被害になるなど、リスクが大きなものから重点的に対策を定めます。事故が起きる可能性が小さいか、発生しても被害が限定的であるなどリスクが小さなものについては、あえて対策を講じず、リスクが大きなものに対策を講じることで費用対効果を高めるという判断も必要になります（図7）。

【図7】リスク分析の考え方



(2) ポリシー策定までの流れ

ポリシー策定は、わが社の情報セキュリティポリシー（付録３）を使い、以下の手順で行います（図8）。



【図8】情報セキュリティポリシー策定までの流れ

以下では、手順1から4で行う作業について説明します。

9 **▲情報セキュリティリスク**　脅威が情報資産又は情報資産グループの脆弱性に付け込み、その結果、組織に損害を与える可能性に伴って生じる、と定義され（JIS Q 27000:2014（情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語）情報資産に対する脅威の存在により不利益が発生する可能性がある状態のことをいいます。

10 **▲リスク分析**　事故が起きたときの影響とその起こりやすさからリスクの大きさを想定することをいいます。本ガイドラインではリスクの大きさの想定をリスク値の算定といっています。

中小企業の情報セキュリティ対策ガイドライン

手順1 情報資産管理台帳を作成する

どのような情報資産があるか洗い出して重要度を判断する。

業務で利用する電子データや書類を「情報資産管理台帳」に記入します。記入した情報資産ごとに漏えいや改ざん、誤びゅう(誤記、計算違い)が起きたり、必要な時に利用できないと事業に影響するものについて重要度を判断し、管理責任のある顧客や従業員の個人情報を識別します。

業種、事業内容、IT環境によって保有する情報資産は異なるため、台帳記入例を参考に、自社の情報資産を一通り洗い出し、以下の要領で作業を進めます。

●情報資産の洗い出し

日常業務の流れに着目して、どのような電子データや書類などを利用しているかを考えると、洗い出しがやりやすくなります。

●情報資産ごとの機密性・完全性・可用性の評価

機密性、完全性、可用性が損なわれたときの事業への影響や、法律で安全管理義務があるなど、表6の評価基準を参考に評価値'2〜0を記入します。

●機密性・完全性・可用性の評価値から重要度を算定

重要度は、機密性、完全性、可用性いずれかの最大値で判断します。

前項の作業で「情報資産管理台帳」の所定欄に記入した機密性・完全性・可用性の評価値をもとに、表7の算定基準に従い、重要度を算定します。

なお、事故が起きると法的責任を問われたり、取引先、顧客、個人に大きな影響があったり、事業に深刻な影響を及ぼすなど、企業の存続を左右しかねない場合や、個人情報を含む場合は、前項の算定結果にかかわらず、重要度は2とします。

情報資産管理台帳は情報セキュリティ対策を検討する上での基本資料となるものですので、記入漏れがないようにします。記入量が多いと管理の負荷も大きくなるため、管理方法や重要度が同じ情報は1行にまとめて記入します。また、電子メールや案件ファイルのように様々な情報が混在し、機密性、完全性、可用性を一律に評価することが難しいものは、1行にまとめ、評価値はその中に含まれる情報の最大値を記入します。

情報資産管理台帳の作成方法は、本書の33ページにて説明していますので参照してください。

1▲**評価値**　この他にも数値を使うことがありますが、これは情報資産の重要度やリスクの大きさを定量的に表したほうが、重点的に対策すべき情報資産が解りやすくなるためです。おおよその見当がつけばよく、緻密に計算する必要はありません。

【表6】情報資産の機密性・完全性・可用性評価基準

評価値		評価基準	該当する情報の例
機密性 アクセスを許可された者だけが情報にアクセスできる	2	法律で安全管理(漏えい、滅失又はき損防止)が義務付けられている	●個人情報(個人情報保護法で定義) ●特定個人情報(マイナンバーを含む個人情報)
		守秘義務の対象として指定されている 漏えいすると取引先や顧客に大きな影響がある	●取引先から秘密として提供された情報 ●取引先の製品・サービスに関わる非公開情報
		自社の営業秘密として管理すべき(不正競争防止法による保護を受けるため) 漏えいすると自社に深刻な影響がある	●自社の独自技術・ノウハウ ●取引先リスト ●特許出願前の発明情報
	1	漏えいすると事業に大きな影響がある	●見積書、仕入価格など顧客(取引先)との商取引に関する情報
	0	漏えいしても事業に影響はない	●自社製品カタログ ●ホームページ掲載情報
完全性 情報や情報の処理方法が正確で完全である	2	法律で安全管理(漏えい、滅失又はき損防止)が義務付けられている	●個人情報(個人情報保護法で定義) ●特定個人情報(マイナンバーを含む個人情報)
		改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある	●取引先から処理を委託された会計情報 ●取引先の口座情報 ●顧客から製造を委託された設計図
	1	改ざんされると事業に大きな影響がある	●自社の会計情報 ●受発注・決済・契約情報 ●ホームページ掲載情報
	0	改ざんされても事業に影響はない	●廃版製品カタログデータ
可用性 許可された者が必要な時に情報資産にアクセスできる	2	利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある	●顧客に提供しているECサイト ●顧客に提供しているクラウドサービス
	1	利用できなくなると事業に大きな影響がある	●製品の設計図 ●商品・サービスに関するコンテンツ(インターネット向け事業の場合)
	0	利用できなくなっても事業に影響はない	●廃版製品カタログ

はじめに 第1部 1 2 3 1 2 3 第2部 4 情報セキュリティポリシーの策定 5 用語 INDEX

中小企業の情報セキュリティ対策ガイドライン

【表7】情報資産の重要度判断基準

機密性・完全性・可用性から算定	重要度
機密性・完全性・可用性評価値のいずれかまたはすべてが「2」の情報資産	2
機密性・完全性・可用性評価値のうち最大値が「1」の情報資産	1
機密性・完全性・可用性評価値すべてが「0」の情報資産	0

（重要度の判断例）

●『独自技術に基づいた設計図』（書類）

機密性：主力製品の設計図であり、流出すると他社との差別化ができなくなり、売上が減少する…　**評価＝2**

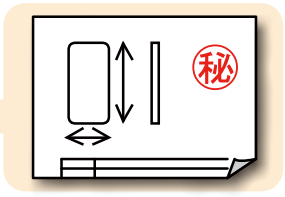
完全性：改ざんや無断の変更があると、製造に支障がある…　**評価＝1**

可用性：原本のCADデータはサーバーに保存してあり、必要なときに閲覧や再印刷が可能なので、利用できなくなっても困ることはない…　**評価＝0**

情報資産管理台帳　重要度欄

評価値			重要度
機密性	完全性	可用性	
2	1	0	2

密性の２が最大値なので重要度は２



●『自社のホームページ』（電子データ）

機密性：公開しているホームページであり、クレジットカード情報など機密情報の保存はしていない…　**評価＝0**

完全性：不正アクセスで価格が改ざんされたり、ウイルスが仕掛けられると顧客や閲覧者に被害が発生し、信用を失う…　**評価＝2**

可用性：サーバーの障害等でアクセスできなくなると、来店客が減少し、売上も減少する…　**評価＝2**

情報資産管理台帳　重要度欄

評価値			重要度
機密性	完全性	可用性	
0	2	2	2

完全性と可用性の２が最大値なので重要度は２

付録の利用方法（手順 1）

付録３は本ガイドラインの手順１～４に示した作業を実施する際のツール集です。「手順1」で示した「情報資産管理台帳」は、＜ツールＡ リスク分析シート＞の「情報資産管理台帳」シートに相当します。「台帳記入例」シートを参考に表８のように記入してください。

【表8】情報資産管理台帳への記入要領

台帳記入欄	記入内容解説
① 業務分類	情報資産に関連する業務や部署名を記入します。情報資産は業務に関連して発生しますので、まず関連業務や部署を特定し、その業務や部署で利用している情報を洗い出すと記入漏れが少なくなります。
② 情報資産名称	情報資産の内容を簡潔に記入します。正式名称がないものは社内の通称で構いません。管理方法や重要度が同じものは1行にまとめます。
③ 備考	必要に応じて説明等を記入します。
④ 利用者範囲	情報資産を利用してよい部署等を記入します。
⑤ 管理部署	情報資産の管理責任がある部署等を記入します。小規模事業者であれば担当者名を記入しても構いません。
⑥ 媒体・保存先	情報資産の媒体や保存場所を記入します。書類と電子データの両方で保存している場合は、それぞれ完全性・可用性（機密性は同一）や脅威・脆弱性が異なるので2行に分けて記入します。 例）見積書「電子データを事務所PCに保存」「印刷物書類をキャビネットに保管」
⑦ 個人情報の種類	各項目が個人情報保護法、マイナンバー法で定義されています。 ＜個人情報＞ 個人情報が含まれる場合は「有」を記入します。 -個人情報- 「生存する個人に関する情報であって当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの、又は　個人識別符号が含まれるもの」 氏名、住所、性別、生年月日、顔画像等個人を識別する情報に限られず、個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表す全ての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化等によって秘匿化されているかどうかを問わない。 ＜要配慮個人情報＞ 要配慮個人情報が含まれる場合は「有」を記入します。 -要配慮個人情報- 「本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報」 ＜マイナンバー＞ マイナンバー（個人番号）が含まれる場合（マイナンバー法で「特定個人情報」と定義されています。）は「有」を記入します。
⑧ 重要度	情報資産の機密性、完全性、可用性それぞれの評価値を記入します。 3種類の評価値から表7に基づき重要度が表示されます。なお⑦でいずれかの個人情報が「有」の場合、重要度は自動的に「２」となります。
⑨ 保存期限	法定文書は法律で定められた保存期限を、それ以外は利用が完了して廃棄、消去が必要となる期限を記入します。
⑩ 登録日	登録した日付を記入します。内容を更新した場合は更新日に修正します。

はじめに 第1部 1 2 3 1 2 2 3 第2部 4 情報セキュリティポリシーの策定 5 用語 INDEX

中小企業の情報セキュリティ対策ガイドライン

記入上のポイント

- 情報資産管理台帳は情報資産を「見える化」するためのものです。特にパソコンやネットワークで利用する電子化された情報は人間の五感で感知することができないため、社外のサーバーや個人のスマートフォンに保存されていると気付かないことがあります。「見える化」は漏れなく洗い出すことが重要なので、電子化された情報は業務で利用しているIT機器やクラウドサービスに留意して記入します。
- 記入する前に「重要ではない」と判断するのではなく、記入した後に重要度を判断します。
- 管理方法や重要度が同じ情報は１行にまとめて記入することで作業負荷を減らすことができます。
  例）管理方法や重要度が同じ情報：事務所内のパソコンで表計算ソフトを使って帳簿をつけている場合

  - 仕訳帳
  - 総勘定元帳
  - 現金出納帳
  - 当座預金出納帳
  - 小口現金出納帳
  - 仕入帳
  - 売上帳

  情報資産名称：「帳簿データ」
  媒体・保存先：「事務所PC」
  「可搬電子媒体（バックアップ）」

- 情報資産の「重要度」は時間経過とともに変化することがありますが、現時点の評価値を記入してください。また時間経過にともなう重要度の変化を台帳上で更新することが難しい場合は、最大値で評価します。
- 中規模企業の場合、管理部署ごとにシートを分けて作成すると、内容の見直しの際に便利です。

手順２ リスク値の算定

対策が必要な情報資産を把握する

手順１で洗い出した情報資産について、対策の優先度を決めるため、リスク値（リスクの大きさ）を算定します。リスク値を算定するにはいくつか方法がありますが、本ガイドラインでは「重要度」と「被害発生可能性」の２つの数値の掛け算で行います。「被害発生可能性」は「脅威の起こりやすさ」と「脆弱性のつけ込みやすさ」の２つの数値から算出します（表11）。これは、脅威が脆弱性を利用して、どの程度被害をもたらす可能性があるかを示す指標です。

リスク値 ＝ 重要度 × 被害発生可能性
重要度 ＝ 手順1にて算定
被害発生可能性 ＝ 脅威・脆弱性から算定

重要度は手順1で算定した2～0の数値、被害発生可能性、脅威、脆弱性は3～1の数値、リスク値は算定結果を大・中・小で表します（表9）。

【表9】リスク値の算定基準

		情報資産の価値・事故の影響の大きさ
重要度	2	事故が起きると ● 法的責任を問われる ● 取引先、顧客、個人に大きな影響がある ● 事業に深刻な影響を及ぼす など企業の存続を左右しかねない
	1	事故が企業の事業に重大な影響を及ぼす
	0	事故が発生しても事業に影響はない

×掛け算

算定のしかたは表11参照

		起こりやすさ
脅威	3	通常の状況で脅威が発生する（いつ発生してもおかしくない）
	2	特定の状況で脅威が発生する（年に数回程度）
	1	通常の状況で脅威が発生することはない

		つけ込みやすさ
脆弱性	3	対策を実施していない（ほぼ無防備）
	2	部分的に対策を実施している
	1	必要な対策をすべて実施している

被害発生可能性	3	通常の状況で被害が発生する（いつ発生してもおかしくない）
	2	特定の状況で被害が発生する（年に数回程度）
	1	通常の状況で被害が発生することはない

リスク値	4～6 大	深刻な事故が起きる可能性大
	1～3 中	重大な事故が起きる可能性有
	0 小	事故が起きる可能性小、起きても被害は許容範囲

はじめに 第1部 1 2 3 1 2 3 第2部 4 情報セキュリティポリシーの策定 5 用語 INDEX

中小企業の情報セキュリティ対策ガイドライン

中小企業で扱う典型的な情報資産に関する脅威・脆弱性と、それがもたらすリスク値の算定例を表10に示します。この表からも分かるように、重要度と脅威は固定的ですが、脆弱性は対策の有無に応じて変動します。次の手順3で対策を決定し、手順4で対策を社内ルールとして実施することによって、本書29ページ図7の説明のようにリスクを許容範囲内まで小さくします。

【表10】脅威例に応じたリスクのレベル

脅威・脆弱性の例	重要度 (a)	脅威	脆弱性	被害発生可能性 (b)	a×b	リスク値
顧客リスト（個人情報）を保存しているノートパソコン（暗号化せず）の盗難	2	2	3	2	4	リスク大
暗号化すると	2	2	1	1	2	リスク中
お客様の個人情報が登録されたウェブサイトへの（不正な攻撃による漏えい（攻撃対策不十分）	2	3	2	2	4	リスク大
適切な対策を実施すると	2	3	1	1	2	リスク中
標的型攻撃メールを誤って開いてしまった従業員個人パソコンからの、顧客との取引情報の漏えい	2	3	2	2	4	リスク大
地震によるサーバーの損傷によるデータの消失（バックアップ対策なし）	2	1	3	1	2	リスク中

【表11】被害発生可能性　換算表

脅威 ＼ 脆弱性	3	2	1
3	3	2	1
2	2	1	1
1	1	1	1

計算式　脅威÷(4－脆弱性)　小数第1位を切り上げ

付録の利用方法（手順 2）

<ツール A>を用いて、個々の情報資産ごとにリスク値を算定する方法を説明します。

①「重要度」の指定

「情報資産管理台帳」シートに記入した重要度をそのまま使用します。

②「脅威」の指定

「脅威の状況」シートで、媒体・保存先ごとの脅威がどのくらいの頻度で発生する可能性があるかを対策を講じない場合の脅威の発生頻度」欄に表示されるリストから1～3のいずれかを選択します。

社内サーバー	情報搾取目的の社内サーバーへのサイバー攻撃	3：通常の状態で発生する（いつ発生してもおかしくない）
	情報搾取目的の社内サーバーでの内部不正	2：特定の状況で発生する（年に数回程度）
	社内サーバーの故障による業務に必要な情報の喪失	1：通常では発生しない（数年に１回未満）

媒体・保存先　個別の脅威　脅威の発生頻度（1～3から選択）

③「脆弱性」の指定

「対策状況チェック」シートで55項目の「情報セキュリティ診断項目」ごとに自社における実施状況を「回答値」欄に表示されるリストから1～4のいずれかを選択します。

(6)物理的セキュリティ対策	業務を行う場所に、第三者が許可無く立入できないようにするための対策（物理的に区切る、見知らぬ人には声をかける、等）が講じられていますか？	2：一部実施している
	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？	1：実施している
	高いセキュリティを確保する区域には、許可された者以外は接近できないような保護措置がなされていますか？	3：実施していない/わからない
	秘密情報を保管および扱う場所への個人所有のパソコン・記録媒体等の持込み・利用は禁止されていますか？	4：自社に該当しない

情報セキュリティ診断項目（チェック項目）　回答値（1～3+4：該当しない）

④リスク値の算定

以上①から③を入力すると「情報資産管理台帳」シートの右側「リスク値」欄に情報資産ごとのリスク値が表示されます。リスク値に応じて以下のように対応を検討します。

- リスク大　重点的に対策を実施
- リスク中　対策を実施
- リスク小　現状維持

現状の状況から想定されるリスク（入力不要・自動表示）					
脅威の発生頻度（「脅威の状況」シートで設定）	脆弱性（「対策状況チェック」シートで設定	被害発生可能性		リスク値	
3:通常の状態で発生する（いつ発生してもおかしくない）	2:部分的に脆弱性未対策	2	可能性：中	4	リスク大
2:特定の状況で発生する （年に数回程度）	2:部分的に脆弱性未対策	1	可能性：低	2	リスク中

情報資産ごとの脅威の発生頻度　情報資産ごとの脆弱性（対策状況）　情報資産ごとの被害発生可能性（高・中・低の3段階）　情報資産ごとのリスク値（大・中・小の3段階）

手順3 情報セキュリティ対策を決定

対策を決める

続いて、リスク値の大きいものから対策を検討し、自社に適した対策を決定します。なお、対策は以下のように区分して検討します。

ア) リスクを低減する

自社で実行できる情報セキュリティ対策を導入ないし強化することで、脆弱性を改善し、事故が起きる可能性を下げます。

イ) リスクを保有する

事故が発生しても許容できる、あるいは対策にかかる費用が損害額を上回る場合などは対策を講じず、現状を維持します。

ウ) リスクを回避する

仕事のやりかたを変える、情報システムの利用方法を変えるなどして、想定されるリスクそのものをなくします。

例えば、従来は商品の発送先である住所や氏名などの個人情報を発送完了後もパソコンに保存し続けていたが、保存中の漏えいを避けるために、利用後はすぐに消去する、インターネットバンキングに使用するパソコンでメールやウェブ閲覧をしていたが、ウイルスに感染しないようにインターネットバンキング専用のパソコンを設置し、ウイルス感染の原因となるメールソフト、ブラウザをインストールせず、USBメモリ、外付けHDDも接続を禁止する、などがあります。

また、リスク値が大きく自社の対策だけでは不十分であったり、多額の費用がかかり、実施できない場合は以下を検討します。

エ) リスクを移転する

自社よりも有効な対策を行っている、あるいは補償能力がある他社のサービスを利用することで自社の負担を下げます。

例えば、商品を販売するウェブサイトでのクレジットカード決済業務を外部の決済代行サービスに変更する、社内のサーバーで運用していた業務システムをセキュリティ対策の充実した外部クラウドサービスに移行する、情報漏えい、システム障害などの事故発生に伴う損失に対して保険金が支払われる情報セキュリティに関連した保険商品に加入する、などがあります。

はじめに 第1部 1 2 3 1 2 3 第2部 4 情報セキュリティポリシーの策定 5 用語 INDEX

付録の利用方法

<ツールA>を用いて対策を検討する方法について説明します。
34ページで示した、「情報資産管理台帳」シートの右側「リスク値」で「リスク大」と表示されたものから対策を検討します。このとき時参考になるのが「診断結果」シートの「対策状況チェックの診断結果」です。これは「対策状況チェック」シートで回答した実施状況を対策の種類ごとに集計したものです。

対策の種類 (情報セキュリティポリシー名称)	情報セキュリティポリシー策定の必要性	対策状況チェックの診断結果 (対策の実施率)	<ツール B> 情報セキュリティポリシーによる対策規定の要否
(1) 組織的セキュリティ対策	◎	62.5%	ポリシーで対策を規定して下さい
(2) 人的セキュリティ対策	◎	33.3%	ポリシーで対策を規定して下さい
(3) 情報資産管理	○	14.3%	ポリシーで対策を規定して下さい
(4) マイナンバー対応	○	100.0%	ポリシーで対策を規定して下さい

この「対策の実施率」が低いことでリスク値が大きくなっている可能性があります。実施率が低くなっている対策の種類について「対策状況」シートを見直し、対策を行ったと仮定して「3:実施していない / わからない」や「2:一部実施している」となっている項目を「1:実施している」に直すと、リスク値が変化しますので、全てのリスク値が「中」以下になり、かつ自社で今後実施が可能と見込まれる対策について検討してください。この結果に基づき、次の手順4に従い、対策を社内ルールをとして定めます。

コラム

「情報セキュリティに関連した保険商品」とは

個人情報保護法の施行後、個人情報を漏えいしてしまった企業に対して、損害賠償金ならびに法律相談、事故対応、見舞金等の費用損害相当額を支払う保険が登場しました。現在は個人情報以外にも、不正アクセス等により取引先企業の秘密情報の漏えい事故にも対応するものが、「サイバーセキュリティ対策保険」として損害保険各社から提供されています。また、中小企業が加入しやすい団体型の商品として日本商工会議所が会員向けに提供している「情報漏えい賠償責任保険制度」や、その他業界団体等によるサイバー保険の各種団体制度があります。こうした保険では、プライバシーマークやISMS 認定を取得していたり、適切な情報管理体制を導入していたりすると保険料が割引になるため、情報セキュリティ対策を行うことが経済的な利点となっています。

手順４ 情報セキュリティポリシーを策定

対策を社内ルールにする

以上の検討結果をもとに、決定した情報セキュリティ対策を社内の正式なルールとして文書化し、「情報セキュリティポリシー」としてとりまとめます。ルールは実行可能であることが重要ですので、自社で決めた対策が適切に伝わり、確実に実行してもらえるように社内の環境に合わせて策定することが大切です。

付録の利用方法（手順４）

＜ツール B＞には表 11に示す情報セキュリティポリシーサンプル（ひな形）が用意されています。このうち No.1の「組織的対策」には情報セキュリティ基本方針と個人番号及び特定個人情報の適正な取扱いに関する基本方針のサンプルとが含まれます。

＜ツール A＞の「診断結果」シートに従い、「ポリシーで対策を規定して下さい」と表示された項目の「対策の種類（情報セキュリティポリシー名称）」欄のサンプルを使い、文中の赤字、青字部分を自社向けに編集すれば、自社の情報セキュリティポリシーが完成します。なお、サンプルに明記されていなくても必要な対策や有効な対策があれば、追記や更新を行ってください。

【表11】本ガイドライン付録３で用意している
情報セキュリティポリシーサンプル

No.	情報セキュリティポリシー名称	適用条件
1	組織的対策	（原則としてすべての企業）
2	人的対策	（原則としてすべての企業）
3	情報資産管理	（原則としてすべての企業）
4	マイナンバー対応	（原則としてすべての企業）
5	アクセス制御及び認証	（原則としてすべての企業）
6	物理的対策	（原則としてすべての企業）
7	IT機器利用	（原則としてすべての企業）
8	IT基盤運用管理	（原則としてすべての企業）
9	システム開発及び保守	社内でシステム開発を行う場合
10	外部委託管理	業務委託を行う場合
11	情報セキュリティインシデント対応ならびに事業継続管理	（原則としてすべての企業）
12	社内体制図	従業員数２名以上
13	委託契約書機密保持条項サンプル	委託先と秘密情報や個人情報等の重要な情報の授受が発生する場合

(3)委託時の情報セキュリティ対策

業務委託や複数の企業で共同作業を行ったり、あるいは委託先がさらに再委託する場合など、自社と同等またはそれ以上の情報セキュリティ対策を相手方に求める必要があります。委託契約を行う場合、機密情報の取り扱いに関する、必要かつ適切な情報セキュリティ対策について、委託先と合意し、具体的に契約書に明記します。具体的な対策がなく、事故が発生した場合の損害賠償請求のみの規定では、委託先が事故を未然に防ぐための対策を講じないことがあり、望ましくありません。また個人情報を含むデータの処理を委託する場合、個人情報保護法により委託先の監督が義務づけられていることから、監督の具体的な手段について契約書に明記する必要があります。

こうした要件を踏まえた上で、付録３の委託契約書機密保持条項サンプルを参考に、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契約条件に含めて締結します。

コラム

業務委託

業務委託とは自社以外の組織あるいは個人に、自社の業務を行ってもらうことです。請負、外注、委任、準委任などともいいますが、どのような会社でも自社だけで全ての業務が完結することはまれで、必ず委託している業務があります。例えば自社商品を販売するウェブサイトの開発・運用を開発会社に委託する、会計処理を顧問税理士に委任するなど、事業は委託によって成り立っているといっても過言ではありません。委託を行う際には、必ず情報の授受が発生します。ウェブサイトの開発・運用であれば顧客のメールアドレス、氏名や住所などの個人情報が開発会社が管理するウェブサーバーに保存されたり、会計処理をしてもらうには、売上伝票や出金伝票などの帳票を税理士に渡します。この中に自社の重要な情報が含まれる場合、自社だけが情報セキュリティ対策を行っていても、委託先が対策を怠っていれば、事故が発生する可能性が高くなります。実際に起きている情報セキュリティ事故の原因として、委託先の対策不足などに因るものも多いため、委託時の情報セキュリティ対策はとても重要です。

中小企業の情報セキュリティ対策ガイドライン

(4)情報セキュリティ対策の実行

前章で策定したポリシーを組織全体に理解させ、実行します。

① 通常時の役割

実行する際の、経営者や従業員の役割分担例を表12に示します。セキュリティの性格上、アルバイトなども含めてひとりでも対策を実行しない人がいると、全体のセキュリティが保てなくなってしまいますので、雇用関係のあるすべての従業員は社内規則のひとつであるポリシーを遵守する必要があります。

【表12】各階層の役割(例)

分　類	それぞれの役割
経営者	◎情報セキュリティ対策に必要な予算・人材の確保 ◎情報セキュリティ方針の策定 ◎管理者層への指示、目標達成状況の確認
管理者層	◎部下に対するポリシーの説明 ◎必要に応じたポリシーの改善 ◎異常に関する監視
一般従業員	◎ポリシーで定められた情報セキュリティ対策の実行

② 緊急時の対応

情報セキュリティに関するインシデント(情報の漏えい、改ざんや消失の発生、日常使用している機能の停止または著しい性能低下など)の発生またはそれが疑われる状況では、上述の役割とは異なる対応が必要になる場合があります。

- インシデントが判明した場合は、速やかに所定の担当に報告を行うことを、すべての従業員と経営者ならびに外部の関係者にも周知しておく必要があります。
- 異常事態になってはじめて平常時と異なる対応をしようとしてもうまくいきません。誰が何を担当するかをあらかじめ決めておく必要があります。具体的には以下を実行するための役割を決めておくことが望まれます。

  ① 緊急時の指揮命令と対応の優先順位の決定
  ② インシデントへの対応(インシデントレスポンス)
  ③ インシデントの影響と被害の分析
  ④ 情報収集と自社に必要な情報の選別
  ⑤ 社内関係者への連絡と周知
  ⑥ 外部関係機関との連絡

- インシデントへの対応には専門家の知見が必要となる場合があります。有償でこうした対応を行う民間サービスもありますが、中小企業にとってはコスト負担が難しいケースが多いと思います。

コラム

サイバーセキュリティ

情報化社会といわれる今日、企業活動はコンピュータやインターネットを利用した電子商取引や情報のやりとりに大きく依存しています。インターネットは世界中に普及し、誰でも簡単に利用することが可能なため、悪用することも容易です。このような環境下では詐欺行為やサービス妨害だけでなく、特定の組織を計画的に攻撃して重要なデータを盗み取るなど、企業活動を阻害する事故が絶えず起きています。それら深刻な事故を防ぐために、情報セキュリティ対策の一環として、コンピュータやインターネットを利用する際の安全を確保することを「サイバーセキュリティ」として「情報セキュリティ」と区別することが増えています。サイバーセキュリティ対策が不十分な場合、自社が被害にあうだけでなく、自社のサーバーやIT機器を第三者に対する攻撃の踏み台として利用されてしまうこともあります。メールサーバーが踏み台[1]にされると迷惑メール[2]の発信元としてブラックリストに登録され、メールの送信が不可能となることで、業務に支障が生ずる恐れもあります。このように、社会に対する責任の観点からもサイバーセキュリティ対策は不可欠です。

1 踏み台
不正アクセスを行う際の中継地点として他人のコンピュータを使用する不正行為。迷惑メールの発信に利用されることがあり、踏み台に利用されたコンピュータは、所有者が気付かないうちに、攻撃に加担していることになります。

2 迷惑メール
商用目的かどうかによらず、宣伝や嫌がらせなどの目的で不特定多数に大量に送信されるメールのこと。SPAM(スパム)メールとも呼ばれます。

はじめに 第1部 1 2 3 1 2 2 3 第2部 4 情報セキュリティポリシーの策定 5 用語 INDEX

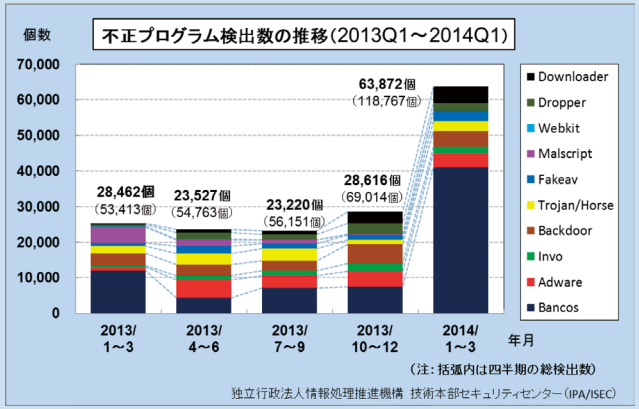
中小企業の情報セキュリティ対策ガイドライン

コラム

ウイルス対策ソフトウェアを入れておけば安心？

2010年以前、コンピュータウイルスによる被害のほとんどは、世界中に大量にばら撒かれた多種多様なウイルスによって生じていました。ウイルス対策ソフトウェアメーカーは次々に出回るウイルスのサンプルを入手し、ウイルスとして検知できるように対策ソフトウェアを更新し、利用者はウイルス対策ソフトウェアを最新状態にすることで、ウイルス感染を防ぐことができたのです。しかし、2010年代に入ってからは、標的型攻撃に代表されるように、特定のウェブサイトやシステムのみを攻撃するウイルス（マルウェア[1]）が多くなり、これらはサンプルの入手が困難なため、ウイルス対策ソフトウェアでは検知できないケースがほとんどです。古いタイプのマルウェアも依然として流通しており、未知のマルウェアの不自然な挙動をブロックする機能を追加した製品などもありますので、ウイルス対策ソフトウェアを導入することは引き続き有効ですが、導入しておけば安心というわけではないことに留意してください。

1マルウェア
コンピュータウイルス、スパイウェア、ボットなどの不正プログラムの総称。経済産業省「コンピュータウイルス対策基準」では「(1)自己伝染機能」、「(2)潜伏機能」、「(3)発病機能」をもつものをウイルスと定義しています。これら以外の不正プログラムを含めて一般にはウイルスと呼ばれることが多く、コンピュータウイルスを発見、またはコンピュータウイルスに感染した場合には、感染被害の拡大と再発防止に役立てるために、IPAへ届け出ることとされています。2011年の刑法改正では、不正指令電磁的記録に関する罪（通称 ウイルス作成罪）として正当な理由もなくウイルスを作成や提供した場合は、処罰対象になりました。ウイルス被害は後を絶たず、深刻な問題となっています。



【図9】コンピュータウイルス・不正アクセスの届出状況および相談状況
（2014年第1四半期(1月～3月), IPA）

(5)チェックと改善

情報セキュリティ対策が適切に実施されることを担保するためには、ポリシーを策定し、全従業員にその遵守を指示するだけでなく、実際に実施されているかどうかのチェックが必要です。チェックの結果、脅威に対して十分な対策が講じられていないと判断される場合は、ポリシーが適切に実践されていないことによるのか、ポリシーを見直す必要があるのかを見極めた上で、状況に応じた改善を行います。

① チェックの方法

ポリシーで要求されている事項に関するチェックシートを作成した上で、遵守状況のチェックを行います。大企業の場合、社内の監査部門が現場部署を対象にチェックを行うのが一般的ですが、中小企業では監査担当者が任命されていないケースが多く見受けられます。こうした場合、部署ごとに自己点検を行い、情報セキュリティの担当者及び経営者がその結果を確認するのが最も効率的な方法です。ただし、こうした監査や点検が形式的なものになっては意味がないため、あらかじめ以下の点を社員に周知させておく必要があります。

- 定められた対策を実施できていないのを咎めることが目的ではないので、実態を正直に回答してよいこと
- 実施できていない場合は、その原因と考えられることを報告すること

なお、こうしたチェックをより効果的に行うためには、情報セキュリティ監査の考え方を取り入れると良いでしょう。概要を次章5.(3)に示します。

② 改善の方法

ポリシーの改善が必要となるのは、以下の場合です。必要に応じて本書29ページ(2)に示したポリシー策定手順を再度実施し、ポリシーの改定を行います。

- ポリシーに欠陥があり、対策を実施しても現場の情報セキュリティに有効ではない場合
- 現場の業務とポリシーで定められた規定が整合せず、ポリシーの遵守が困難な場合
- 新たな脅威が発生したり、会社の業務や情報システムが変化したことで既存のポリシーでは対処が困難となった場合

はじめに 第1部 1 2 3 1 2 3 第2部 4 情報セキュリティポリシーの策定 5 用語 INDEX

5 情報セキュリティ対策のさらなる改善に向けて

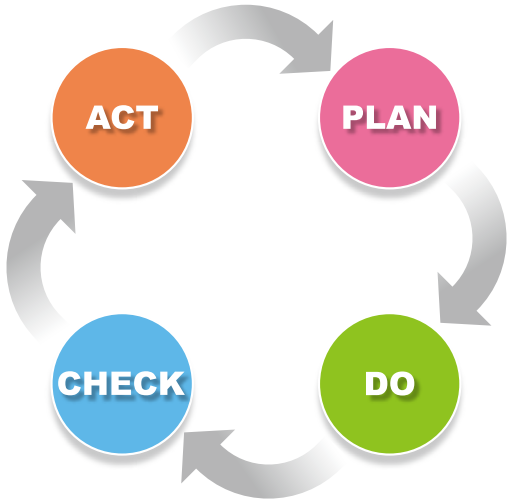
ここでは、これまでの対策を実践済みの組織に向けて、情報セキュリティマネジメントシステムに関する国際規格ISO/IEC27001[12]の考え方をもとに、情報セキュリティ対策をさらに改善するための方法について紹介します。

(1)情報セキュリティマネジメントサイクルによる継続的改善

ISO/IEC27001 が定めているマネジメントシステム（管理のしくみ）の考え方の基本は、Plan（計画）、Do（実行）、Check（チェック）、Act（改善）の４段階の活動（PDCA サイクル[13]）を順に繰り返すことを通じて改善していくことにあります。情報セキュリティ対策で見ると、それぞれ次の活動に相当します。

- Plan：情報セキュリティ対策の計画立案または見直し
- Do：情報セキュリティ対策の実践
- Check：監査・点検による活動の有効性確認と経営者による必要な改善箇所の決定
- Act：改善の実施

Check の機会は少なくとも年１回、インシデントが発生した場合や自社を取り巻く状況が変化した場合には随時行います。Check 及びAct に関する活動の詳細は次項以降で説明します。



12 ▲ISO/IEC27001　日本ではJIS Q 27001 として規格化されています。
13 ▲PDCA サイクル　戦後、品質管理手法として製造業を中心に導入され、大きな成果をあげました。今では事業活動全般の改善手法として広く普及しています。

はじめに 第1部 1 2 3 1 2 3 4 第2部 5 情報セキュリティ対策のさらなる改善に向けて 用語 INDEX

(2)情報セキュリティ対策に関する標準規格

本ガイドラインの、付録３で示す対策は、中小企業でも取り組みやすいように情報セキュリティの国際規格であるISO/IEC 27002（情報セキュリティ管理策の実践のための規範）から抜粋し、解りやすい表現にしています。

情報セキュリティマネジメントの実践に関して国際的な認証制度（ISMS認証　情報セキュリティに対する取り組みを第三者機関が審査して証明する制度）がありますが、どのような対策を実施しているか審査するための基準として、ISO/IEC 27002が利用されていますので、付録３を活用すれば国際規格に準じた管理レベルが実現します。

(3)情報セキュリティ監査・点検の実施

情報セキュリティ監査・点検とは、策定した情報セキュリティポリシーが、実行されているか、あるいは策定した情報セキュリティポリシーがリスク低減に有効かどうかを客観的に評価することを言います[14]。評価の基準となるものは情報セキュリティポリシーに定められたルールそのものか、あるいは定められたルールの根拠となったリスクの確認方法です。監査・点検のやりかたは自由ですが、一般に以下の方法を組み合わせて実施します。

- 質問（ヒアリング）：従業員や委託先の管理者などに直接質問して回答を求める
- 閲覧（レビュー）：情報セキュリティポリシーの関連手続きで申請書などの帳票や、コンピュータのログ、設定内容など実行の証拠となるものを見て確認する
- 観察（視察）：監査・点検者が現場に赴き、情報セキュリティ対策を行う当事者が情報セキュリティポリシーに従った行動をしていることを目視で確認する
- 技術診断：技術的対策の運用状況などについて、監査・点検者が自ら機器を操作することによって検証する（情報システムや社内ネットワークの脆弱性を確認するために、専用ソフトウェアを使い技術的な脆弱性を診断することもある）

14 ▲客観的な立場で第三者機関が情報セキュリティに対する取り組みを評価する制度(第三者認証制度といいます) として国際規格 ISO/IEC27001 を基準としたISMS 適合性評価制度があります。また、監査基準や監査手続きのモデルを公表した経済産業省の情報セキュリティ監査制度などがあります。第三者認証制度は利害関係のない第三者の評価により偏りや利益相反を防ぎます。本ガイドラインの監査・点検は従業員が実施することを想定していますが、監査・点検を行う従業員自らの業務を対象とせず、他の業務を対象とすることで、監査結果の偏りや利益相反を防ぐことが可能です。

中小企業の情報セキュリティ対策ガイドライン

コラム

情報セキュリティ監査・点検の実施例

□ 情報セキュリティポリシーのIT機器利用を基にチェックシートを作成する。
□ チェックシートに従い、従業員に質問する。

監査人　「IT機器利用では、業務で利用するパソコンにはログインパスワードを設定する、と規定されていますが、モバイルパソコンにもログインパスワードを設定していますか？」

相　手　「はい。設定しています。」

監査人　「では、ログインしてみてください。」

相　手　「(ログイン)」

監査人　「ログインパスワードは４桁でしたが、その通りですか？」

相　手　「はいそうです。忘れないようにパスワードは名前のアルファベットにしています。」

□複数相手に質問や観察を行い、その回答から総合的に評価・判定する。
この場合は、ポリシーをきちんと実行している人がいましたが、ポリシーにパスワードの強度まで規定していないため、リスクの確認が不十分（パスワードに関して桁数、使用する文字、推測しにくいなど強度に関して規定されていない）という評価・判定になり、ポリシーの改訂が必要になります。

監査・点検というと難しく思えるかもしれませんが、スポーツの審判のように、ルールを基準とし、選手が基準を満たしているか判定することと同じです。客観的に評価、判定することで、気付かなかった不備が明確になりますので、情報セキュリティのレベルアップにはとても役に立ちます。

(4)改善の実施

ISO/IEC27001では、監査・点検の結果や、関係者から提供された情報をもとに、情報セキュリティマネジメントが適切に行われていることを経営者が判断し、意思決定することを「マネジメントレビュー」と呼び、その決定に従い、不備や不十分なところを改善することが求められています。企業の規模によらず改善が必要になったときには、経営者または経営者に権限を委譲された人が、改善の必要性を判断し、実行する必要がありますので、改善を実施するにあたっては、経営者のほか、少なくとも情報セキュリティ対策の運用担当者や、インシデント対応の担当者、監査・点検担当者が参加するとよいでしょう。

経営者や管理者層での議論、検討を通じて、情報セキュリティポリシーや具体的な対策に関する従業員や関係者の理解を促し、不備を改善し、今後に向けた改善につなげていきます。

はじめに
第1部
1
2
3
1
2
3
4
第2部
5 情報セキュリティ対策のさらなる改善に向けて
用語
INDEX

おわりに

本ガイドラインの初版は、2009年に策定されました。当時、中小企業でも自社のウェブサイトの立ち上げ、電子商取引の活用、財務会計システムの導入などのIT活用が進む一方、Winnyなどのファイル共有アプリケーションを経由した情報漏えいが問題となるなど、中小企業においても取引先から情報セキュリティ対策の実施を求められる場面も増えていました。こうした状況において、IPAが中小企業を対象として作成したのが本ガイドラインの初版です。

作成から7年を経て、IT環境や情報セキュリティに関する脅威は大きく変化しています。標的型攻撃の巧妙化により、適切な対策を実施していても被害を完全に防ぐことが困難になる中、異常事態の発生を素早く検知し、被害を最小限に抑制するための体制が注目されるなど、対策面も変化しています。また、マイナンバー法の施行、個人情報保護法の改正などに伴い、企業規模を問わず情報セキュリティに対する社会的要請、法的責任が拡大し、中小企業においても情報セキュリティへの取り組みは優先課題となっています。

一方で、中小企業では依然として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おり、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認められます。こうした状況を踏まえ、近年、変化・増大する脅威に対する情報セキュリティ対策を、適切かつ有効なものとすることを目的として、本ガイドラインの初版の内容を抜本的に見直し、改訂版を作成することとしました。

中小企業は情報セキュリティ対策に十分な経営資源を割り当てることができないという不利を抱える一方で、経営者を含め「従業員の顔が見える」という有利な条件を備えています。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、従業員がその対策を行う意義を理解することです。つまり、「従業員の顔が見える」ということは経営者が直接管理者・担当者に対策を指示することができ、対策の結果についても直接報告を受けることができるなど、大企業に比べて迅速に対応ができるという有利な条件を備えています。また、この特質を生かすことで、大企業では必要となるセキュリティ監視や情報共有のための設備が不要とできるため、大企業よりも費用をかけずに対策を実現することも可能です。そうした工夫を行うためのヒントとして、本ガイドラインをご活用いただければ幸いです。

本書で用いている用語の説明

インシデント

リスクが発現・現実化した事故のことを言います。コンピュータやネットワークに関わる事故のことをインシデント（Incident）ということがあり、CSIRT（Computer Security Incident Response Team）のように慣例句として使われます。本ガイドラインでは事故とインシデントとを併用します。情報システムの場合、情報の漏えい、改ざんや消失の発生、日常使用している機能の停止または極端な性能の低下などがインシデントに相当します。

（情報の）可用性

許可された者が、必要な時に、情報や情報資産にアクセスできることを確実にする特性のことを言います。

（情報の）完全性

情報や情報の処理方法が正確で完全であるようにする特性のことを言います。

（情報の）機密性

アクセスを認可された者だけが、情報にアクセスできるようにする特性のことを言います。

クラウドサービス

サーバーなどを自前で所有する代わりとして、インターネット経由で同様の機能を提供するものを言います。レンタルサーバー、SaaS（Software as a service）、ASP（Application Service Provider）などはいずれもクラウドサービスの一種です。

個人情報

①広義の個人情報：「個人に関する情報」のことを言い、特定の個人を識別できなくても、当該個人がプライバシーに関わると考える情報を含みます。

②個人情報保護法の定義：「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」とされています。

③特定個人情報：マイナンバー法（行政手続における特定の個人を識別するための番号の利用等に関する法律）が定める「個人番号（マイナンバー）」をその内容に含む個人情報のことを言います。

中小企業の情報セキュリティ対策ガイドライン

サイバーセキュリティ

①サイバーセキュリティ基本法による定義:「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式(以下本項において「電磁的方式」という。)により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置(情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。)が講じられ、その状態が適切に維持管理されていること」を言います。

②サイバーセキュリティ経営ガイドラインの定義:「サイバー攻撃により、情報の漏えいや、期待されていたITシステムの機能が果たされない等の不具合が生じないようにすること」を言います。

③NIST(米国標準技術研究所)による定義:「攻撃を防止し、検知し、攻撃に対応することにより情報を保護するプロセス」のことを言います。

CSIRT(シーサート、Computer Security Incident Response Team)

サイバー攻撃による情報漏えいや障害など、コンピュータセキュリティにかかるインシデントに対処するための組織のことを言います。

情報セキュリティ

情報の機密性、完全性、可用性を維持することを言います。

情報セキュリティインシデント

情報セキュリティ分野において、情報セキュリティリスクが発現・現実化した事象のことを言います。

情報セキュリティに関連した保険商品

情報セキュリティ上の損害が生じた場合に保険金が支払われるものを言い、個人情報が漏えいした場合の賠償責任などに備える個人情報取扱事業者保険や、不正アクセス等のサイバー攻撃による被害を受けた企業が事業を存続できるように備えるためのサイバー保険、サイバーリスク保険等の種類があります。

情報セキュリティポリシー

企業・組織の情報セキュリティに関する理念である意図と方針を、経営者が正式に表明したものです。本ガイドラインでは、中小企業向けであることを踏まえ、情報セキュリティ対策に関する基本方針、対策基準のほか、実施手順まで含めたものを付録に例示しています。

情報セキュリティマネジメントサイクル

Plan(計画)、Do(実行)、Check(チェック)、Act(見直し)の4段階の活動を順に繰り返すことを通じて、企業で行う情報セキュリティ対策を継続的に改善していく取り組みのことを言います。

ソーシャルエンジニアリング

ネットワーク技術やコンピュータ技術を用いずに、人間心理や社会の盲点を突いて、機密情報(パスワードなど)を入手する方法のことです。たとえば、ことば巧みにパスワードを聞き出す、廃棄物から重要情報を読み取る、社員になりすまして盗み見や盗み聞きをすることなどを言います。

ランサムウェア

コンピュータウイルスの一種で、感染したパソコン等に保存されているファイルを外部に流出させるのではなく、暗号化してパソコンの所有者が使えないようにしてしまうものを言います。攻撃者は、ファイルを復号するための暗号鍵を提供する見返りとして金銭を得ることによって目的を達成します。他のコンピュータウイルスと同様、発信者を詐称した電子メールに添付されているファイルや、改ざんされた正規のウェブサイトなどを通じて感染します。

CD-ROMに収録されているファイル

ファイル名	形式	文書名
本編_中小企業の情報セキュリティ対策ガイドライン第2.1版.pdf	Adobe PDF形式	中小企業の情報セキュリティ対策ガイドライン第2.1版
付録1_情報セキュリティ5か条.pdf	Adobe PDF形式	情報セキュリティ5か条
付録2_5分でできる!情報セキュリティ自社診断パンフレット.pdf	Adobe PDF形式	5分でできる!情報セキュリティ自社診断
付録2_5分でできる!情報セキュリティ自社診断シート.pdf	Adobe PDF形式	5分でできる!情報セキュリティ自社診断シート
付録2_情報セキュリティハンドブック(ひな形).pptx	Microsoft PowerPoint形式	情報セキュリティハンドブック(ひな形)
付録3_わが社の情報セキュリティポリシー.pdf	Adobe PDF形式	わが社の情報セキュリティポリシー
付録3_ツールAリスク分析シート.xlsx	Microsoft Excel形式	リスク分析シート
付録3_ツールB情報セキュリティポリシーサンプル.docx	Microsoft Word形式	情報セキュリティポリシーサンプル

CD-ROM使用にあたっての注意事項

1. 本CD-ROMに収録されている文書及びひな形の著作権および関係する全ての権利は、独立行政法人情報処理推進機構(IPA)に帰属します。
2. 本CD-ROMは、情報セキュリティポリシー作成にお役立てください。
3. 営利目的の使用はご遠慮ください。
4. ことわりなく本CD-ROMに収録されている文書及びひな形の全部または一部を非営利に複製・再配布・上映することを許可します。ただし、その場合であっても免責事項の規定は配布の相手に対して効力を有します。
5. 本資料を掲載する場合は、外部からアクセスできないイントラネット内のサーバとしてください。
   外部からアクセスできるWebサイトへの掲載はご遠慮ください。
6. 複製・再配布に関して、本CD-ROMに収録されている文書及びひな形は改編せずに載せてください。
7. 本ガイドブック及び付録CD-ROM内で記載の会社名、製品名、サービス名は各社の商標または登録商標です。

免責事項

1. 独立行政法人情報処理推進機構(IPA)は、本CD-ROMに関して一切動作保証を致しません。
2. 独立行政法人情報処理推進機構(IPA)は、本CD-ROMに起因してご使用者に直接または間接的被害が生じても、いかなる責任をも負わないものとし、一切の賠償等は行わないものとします。
3. 独立行政法人情報処理推進機構(IPA)は、本CD-ROMの不具合等について、修正する義務は負わないものとします。

動作環境について

- OS:Windows Vista、Windows7、Windows8、Windows10
- アプリケーションソフト:以下のいずれか(Microsoft Office 2007、Microsoft Office 2010、Microsoft Office 2013、Microsoft Office 2016)及び、Adobe Acrobat Readerを標準搭載していること。

改訂履歴

- 1.0版(2009年3月)
- 2.0版(2016年11月15日) 全面改訂
- 2.1版(2017年1月24日)　用語、図の修正

中小企業の情報セキュリティ対策ガイドライン　第 2.1 版
2017 年 1 月

独立行政法人**情報処理推進機構**
〒113-6591
東京都文京区本駒込 2 丁目 28 番 8 号 文京グリーンコートセンターオフィス
URL　http://www.ipa.go.jp
電話　03-5978-7508　　FAX 03-5978-7546
E-Mail　isec-pr-nw@ipa.go.jp