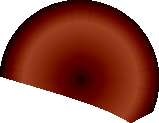
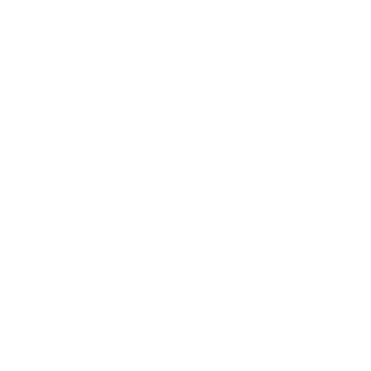
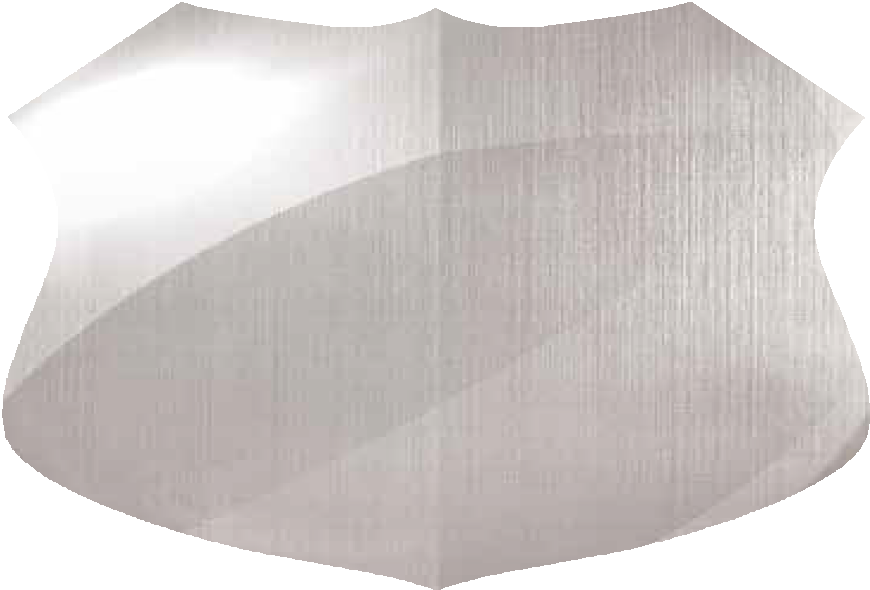
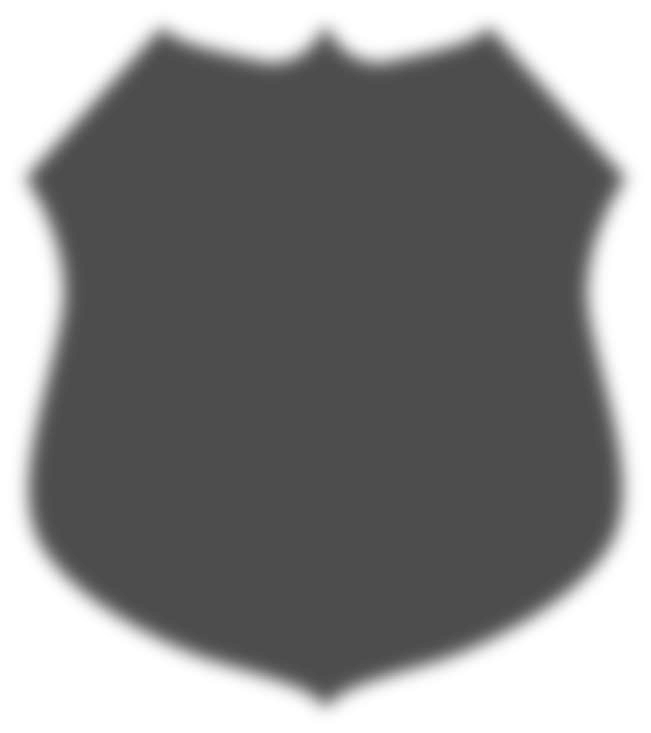
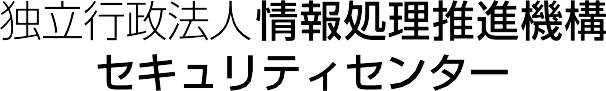
**中小企業の**

**情報セキュリティ対策ガイドライン**

第**3**版





目 次

はじめに 2

1. 経営者の皆様へ 2
2. 本ガイドラインの対象 3
3. 本ガイドラインの全体構成 3
4. 本ガイドラインの活用方法 4

第１部 経営者編 5

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 6
2. 経営者が負う責任 8
3. 経営者は何をやらなければならないのか 10

第２部 実践編 15

1. 実践編の進め方 16
2. できるところから始める 17
3. 組織的な取り組みを開始する 18
4. 本格的に取り組む 22
5. より強固にするための方策 30

情報セキュリティに関する参考情報 55

本書で用いている主な用語の説明 56

付録１ 情報セキュリティ５か条

付録２ 情報セキュリティ基本方針（サンプル） 付録３ ５分でできる！情報セキュリティ自社診断付録４ 情報セキュリティハンドブック（ひな形） 付録５ 情報セキュリティ関連規程（サンプル）

付録６ 中小企業のためのクラウドサービス安全利用の手引き付録７ リスク分析シート



参考情報

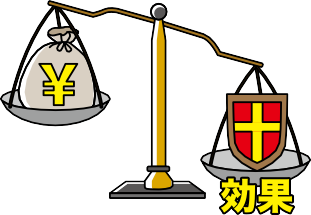
1 経営者の皆様へ

はじめに

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、中小企業にとって重要な情報１を漏えい、改ざん、消失などの脅威から保護するための情報セキュリティ対策の考え方や、段階的に実現するための方策を紹介する 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、企業としての信頼性を確保し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、業績は落ち込み、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。



（➡ 詳細はP6）

対策の不備により経営者が法的・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。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、安全管理措置など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場合によって は会社に罰金刑が課されます。さらに、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。

（➡ 詳細はP8）

組織として対策するために、担当者への指示が必要です！



企業の継続的な発展のために、また、経営責任を果たすためには、担当者に任せきりにすることなく、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。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、情報セキュリティ対策の取り組みを担当者に指示する必要があります。（➡ 詳細はP10）

１▲重要な情報 営業秘密など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” と呼ばれることがあり、本ガイドラインでも“ 重要情報” に加え“ 情報資産” と表記します。

2 本ガイドラインの対象

本ガイドラインは、業種を問わず中小企業および小規模事業者（法人、個人事業主、各種 団体も含む）を対象として、その経営者と情報管理を統括する方を想定読者としています。

3 本ガイドラインの全体構成



本編２部と付録により構成されます（表１）。付録には、情報セキュリティ対策の実施に活用できるサンプルが含まれています。

【表1】本ガイドラインの全体構成



**本 編**

|  |  |  |
| --- | --- | --- |
| **構 成** | | **概 要** |
|  | **第１部 経営者編** | 経営者が知っておくべき事項、および自らの責任で考え  なければならない事項について説明しています。 |
| **第２部 実践編** | 情報セキュリティ対策を実践する方向けに、対策の進め方  についてステップアップ方式で具体的に説明しています。 |
|  | **付録１ 情報セキュリティ５か条** | 組織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２ 情報セキュリティ基本方針**  **（サンプル）** | 組織としての情報セキュリティに対する基本方針書のサ  ンプルです。 |
| **付録３ 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  25 項目のチェックリストです。 |
| **付録４ 情報セキュリティハンドブック**  **（ひな形）** | 従業員に対して対策内容を周知するために作成するハン  ドブックのひな形です。 |
| **付録５ 情報セキュリティ関連規程**  **（サンプル）** | 情報セキュリティに関する社内規則を文書化したものの  サンプルです。 |
| **付録６ 中小企業のための**  **クラウドサービス安全利用の手引き** | クラウドサービスを安全に利用するための手引きです。  15 項目のチェックリストが付いています。 |
| **付録７ リスク分析シート** | 情報資産、脅威の状況、対策状況をもとに損害を受ける  可能性（リスク）の見当をつけることができます。 |

**第3.0 版の主な変更点について**

参考情報

**付 録**

* 第１部



* + IT にあまり詳しくない経営者の方々にも理解していただけるよう、専門用語などをなるべく排して説明するように見直しました。
  + 重要７項目の取組について、「サイバーセキュリティ経営ガイドライン」の改定に伴い、内容を一部更新することで整合性を維持しました。
* 第２部
  + 組織的な対策実施体制を段階的に進めていけるよう、全体構成を見直しました。
  + 「セキュリティポリシー」については多様な解釈があるため、位置づけが明確になるよう、「基本方針」と「関連規程」に分けました。
  + 「ウェブサイトの情報セキュリティ」、「クラウドサービスの情報セキュリティ」に関する解説を追加しました。
  + 「SECURITY ACTION 自己宣言制度」との関連を意図したコラムを追加しました。

■付録

* + 「中小企業のためのクラウドサービス安全利用の手引き」（付録６）を加えました。
  + 旧版で付録「情報セキュリティポリシーサンプル」の一部であった「情報セキュリティ基本方針」を抜き出し、「情報セキュリティ基本方針（サンプル）」（付録２）としました。また、残り部分の名称を「情報セキュリティ関連規程」（付録５）に変更しています。

参考

情報



参考情報

4 本ガイドラインの活用方法

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。本ガイドラインにより、事業の特徴に応じた情報セキュリティ対策を段階的に進めていくことができます。「第１部 経営編」は、全ての経営者に読んでいただきたい内容です。まずはご一読ください。「第２部 実践編」は、あなたの組織にあったSTEP から進めてください。

|  |  |
| --- | --- |
| 取組状況とアクション | 本ガイドラインの活用方法 |
|  | これまで情報セキュリティ対策を特に意識していない場合は  **「２. できるところから始める」**（P.17）を参照して、「情報セキュリティ 5 か条」を実行してください。  **進め方**  「情報セキュリティ 5 か条」を社内で配付するなど、まずできるところから開始してください。 |
| Step1 は実施できていて次に進める場合は  **「3. 組織的な取り組みを開始する」**（P.18）を参照して、「５分でできる！情報セキュリティ自社診断」で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**  ・「情報セキュリティ基本方針（サンプル）」を参考に基本方針を作成してください。  ・「5 分でできる！情報セキュリティ自社診断」で現状の対策を把握し、実施すべき対策を検討してください。  ・「情報セキュリティハンドブック（ひな形）」を参考に具体的な対策を定めて従業員に周知してください。 |
| Step2 までは実施できていて次に進める場合は  **「４. 本格的に取り組む」**（P.22）を参照して、自社のリスクに応じた対策規程を作成し、運用後は点検して改善を図ってください。  **進め方**  ・情報セキュリティ管理の体制を構築し、対策の予算を確保してください。  ・対応すべきリスクと対策を検討し、「情報セキュリティ関連規程（サンプル）」を参考に規程を定めてください。  ・委託時に必要となる対策を検討するとともに、点検や改善に努めてください。 |
| **「５. より強固にするための方策」**（P.30）を参照して、自社に必要な対策を追加実施してください。Step １や Step ２に取り組んでいる企業でも、Step ４を参照して必要な対策があれば実行してください。 |





参考情報

|  |  |
| --- | --- |
| **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、 | |
| 自らの責任で考えなければならない | |
| 事項について説明します。 | |
| 信用失墜、取引停止、 |  |
| 業務低迷、顧客や取引先への迷惑、 |  |
| 刑事罰、損害賠償、  … | とはいえ  何をすれば良いか |
|  | 分からないから |
|  | 部下に任せる？ |

参考情報

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。こうした事故による不利益は、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。



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。

（企業が被る主な不利益）

* + - 金銭の損失 ●顧客の喪失 ●業務の停滞 ●従業員への影響

これらを参考に、自社で起きかねない情報セキュリティ上の事故とは何か、どの業務にそのような心配があるか、自社の経営において最も懸念される事態は何かなどを具体的 に思い描くことが、経営者が情報セキュリティ対策を認識する第一歩です。このような思考実験が経営者によるリスク認識の基礎となります。

（1）金銭の損失

取引先などから預かった機密情報や個人情報を万一漏えいさせてしまった場合は、取 引先や顧客などから損害賠償請求を受けるなど、大きな経済的損失を受けることになり 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に関連した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。

**事例１ ウイルス感染で数日間業務が停止し、数千万円の被害が発生**

（所在地：東京都／業種：情報通信業／従業員規模：101 ～ 300 名）

社内のパソコンやサーバーがウイルスに感染し、数日間に亘った業務停止に至る障害が発生 した。復旧のために徹夜で対応したが、その間の会社としての被害額は推計で数千万円に上る。原因は、被害が発生するまで、セキュリティ対策ソフトを全く導入していなかったことである。その後、ウイルス対策ソフトや技術的な対策の導入、情報セキュリティ規則の制定、プライ バシーマークや ISMS 認証取得に取り組み、再発防止に努めている。







1. 顧客の喪失



重要な情報に関する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。大手メーカーのサプライチェーンに位置する企業の場合は、これまで継続してきた受 注が停止に追い込まれることにもなりかねません。事故を起こした企業は再発防止に努 め、事故を起こさずに事業を続けていくことが必要ですが、低下した社会的信用の回復に は時間を要するため、事業の存続が困難になる場合もあります。

**事例２**

（所在地：東京都／業種：情報通信業／従業員規模：101 ～ 300 名）

**顧客情報の入ったパソコンの紛失事故により取引先の信用を失墜**

従業員が顧客情報の入ったパソコンを持ち出した時に紛失事故が発生した。顧客に対して紛失の報告をしたが信用を失うこととなった。原因は、会社として情報セキュリティに対する意識が高くなかったため、持ち出しに関する明確なルールや手続きを定めておらず、従業員がパソコンを自由に持ち出せる環境であったことである。その後、情報機器の暗号化などの対策を実施するとともに、パソコンの持ち出しルールを含めた情報セキュリティ規程を整備して従業員へ情報セキュリティ教育を行った。

1. 業務の停滞

日常業務で使用している業務システムに事故が発生すると、原因調査や被害の拡大防 止のために、運用中の情報システムを停止したり、インターネット接続を遮断しなければならないことがあります。その結果、電子メールが使えなくなるなど、業務が停滞し、納期遅れや営業機会の損失が生じるなど、事業全体に影響が出てしまいます。



1. 従業員への影響

**事例３ ウイルス感染により基幹システムが一週間停止**

（所在地：静岡県／業種：製造業／従業員規模：51 ～ 100 名）

従業員がメールに添付されていたウイルス付きのファイルを不用意に開いたことで感染し、基幹システムで障害が発生した。システムベンダーの協力を得て障害対応を行ったが、復旧するまでの一週間、基幹システムが使用できなくなった。原因は不審メールを受信した際の対処方法を詳しく教育していなかったことである。その後、朝礼などを利用して従業員へ情報セキュリティ教育を行うとともに、迷惑メール除去ツールを導入した。

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関わらず、従業員

参考情報

のみを罰して管理職が責任を取らないような対応は、従業員が働く意欲を失うおそれが

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。ある経営者は「個別の損害より、職場環境が暗くなっ たことが一番困った」と語っています。



2 経営者が負う責任

情報セキュリティ対策を的確に指揮しなかったことに起因する業績の悪化などが経営者の責任であることは言うまでもありませんが、それ以外の経営者の「法的責任」と「社会的責任」について説明します。



* 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法的な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、担当者は表２に示す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るおそれがあります。 また、個人情報保護委員会２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２】情報管理が不適切な場合の処罰など



|  |  |  |
| --- | --- | --- |
| **法令** | **条項** | **処罰など** |
| **個人情報保護法**個人情報の保護に関する法律 | 40条 報告及び立入検査  83条 個3 人情報データベース等不正提供罪  84条 委員会からの命令に違反  85条 委員会への虚偽の報告など  87条 両罰規定 | 委員会による立入検査、帳簿書類等の物件検査及び質問1年以下の懲役又は50万円以下の罰金  6月以下の懲役又は30万円以下の罰金  30万円以下の罰金  従業者等が業務に関し違反行為をした場合、法人に対しても罰金刑 |
| **マイナンバー法**  **（番号法）** 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 | 48条 正当な理由なく特定個人情報ファ  49条 イルを提供 、個人番  不正な利益を図る目的で  50条 号を提供又は盗用  情報提供ネットワークシステム  51条 に関する秘密を漏えい又は盗用  人を欺き、人に暴行を加え、人を  脅迫し、又は、財物の窃取、施設への侵入、不正アクセス等により個  53条 人番号を取得  54条 委員会からの命令に違反  55条 委員会への虚偽の報告など  偽りその他不正の手段により個  57条 人番号カード等を取得  両罰規定 | 4年以下の懲役若しくは200万円以下の罰金又は併科  3年以下の懲役若しくは150万円以下の罰金又は併科同上  3年以下の懲役又は150万円以下の罰金  2年以下の懲役又は50万円以下の罰金  1年以下の懲役又は50万円以下の罰金  6月以下の懲役又は50万円以下の罰金  従業者等が業務に関し違反行為をした場合、法人に対しても罰金刑 |
| **不正競争防止法**  営業秘密・限定提供データに係る不正行為の防止など | 3条 差止請求  4条 損害賠償請求  14条 信頼回復措置請求 | 利益を侵害された者からの侵害の停止又は予防の請求  利益を侵害した者は損害を賠償する責任 信用を害された者からの信用回復措置請求 |
| **金融商品取引法**インサイダー取引の規制など | 197条の2 刑事罰  207条1項2号 両罰規定  198条の2 没収・追徴  175条 課徴金 | 5年以下の懲役若しくは500万円以下の罰金又はこれらの併科  従業者等が業務に関し違反行為をした場合、法人に対しても罰金刑  犯罪行為により得た財産の必要的没収・追徴違反者の経済的利得相当額 |
| **民法** | 709条 不法行為による損害賠償 | 故意又は過失によって他人の権利又は法律上保護される利益を侵害した者は、これによって生じた損害を賠償する責任を負う |

２ ▲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。３ ▲データベース等不正提供罪 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



参考情報

個人情報データベース等を他者に提供等したり盗用した場合は処罰対象になります。

* 1. 関係者や社会に対する責任



**法務 執行機関**

**個人情報**

**当事者**

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。また、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ますので、会社役員が会社法上の責任（会社に対す る損害賠償責任）を問われ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、企業や団体に個人情報をきちんと大切に取り扱ったうえで、 有効に活用できるよう共通のルールを定めた法律です４。「氏名」、「生年月日」、「住所・電話番号・メールアドレス」などの連絡先、「顔写真」など、事業によって取り扱う個 人情報は様々です。従業員情報や取引先の名刺も個人情報に当たりますので、従業



員名簿やメールのアドレス帳などを作成している事業者は、保有する個人情報が少

なくても、個人情報取扱事業者（個人情報データベース等を事業の用に供している者） となり、この法律が適用されます。

個人情報保護法について詳しく知るには個人情報保護委員会のウェブサイトを 確認してください。

●個人情報保護委員会のウェブサイト  [https://www.ppc.go.jp/](http://www.ppc.go.jp/)

不正競争防止法

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。



参考情報

①秘密として管理されていること（秘密管理性）

②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（有用性）

③公然と知られていないこと（非公知性）

４▲個人情報保護法第1条には「個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。」とあることから、個人情報保護とは企業が被る損害の防止だけではなく、個人の人格的、財産的な権利利益に 対する侵害防止を目的としていることに留意する必要があります。



3 経営者は何をやらなければならないのか

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。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」について認識したうえで（、2）に示す「重要7項目の取組」の実施を指示する必要があります。



1. 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

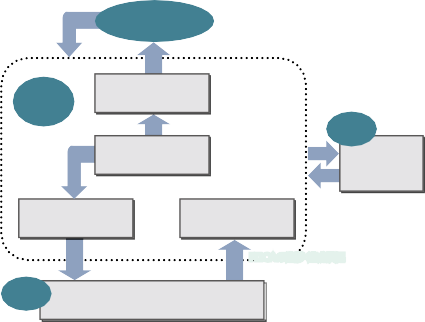
経営者は、IT 活用を推進する中で、情報セキュリティ対策の重要性を認識し、自らリーダーシッ プを発揮して対策を進めます。現場の従業員は、安心して業務に従事できる環境を求める一方、利便性が低下し、面倒な作業を伴う対策には抵抗感を示しがちです。そこで、情報セキュリティ対策は、経営者が判断して意思決定し、自社の事業に見合った情報セキュリティ対策の実施を主導します。











情報セキュリティガバナンス

情報セキュリティガバナンスは、経営者が企業戦略として情報セキュリティ向上 に取り組むための枠組みです。

この枠組みは、経営者が懸念する避けるべき重大事故などを示して「方向付け」を 行い、対策の進捗や点検等により状況を「モニタリング」し、その効果を「評価」して方 向付けを見直すサイクルを骨格としてい ます。

経営者がリーダーシップを発揮する枠組みでもあります。

●経済産業省『情報セキュリティガバナンスの概念』<http://www.meti.go.jp/policy/netsecurity/secgov-concept.html>

企 業

**管理者層** 情報セキュリティ管理Information Security Management

PDCAの進捗・達成状況

モニタリングMonitor

方向付けDirect

経営陣のコミットメント

監督Oversee

評価Evaluate

情報セキュリティガバナンス

のフレームワーク

**監査役**

報告Report

**経営陣CISO**

**利害関係者**

**コラム**

参考情報









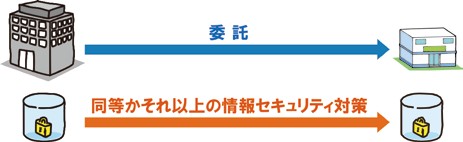


原則 2

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にあたって重要な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 提供した情報が漏えいしたり、改ざんされたとき、それが委託先の不備だったとしても、 事故の影響を受ける者から委託元としての管理責任を問われることになります。そのた め、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ます。また、受託している場合には、委託元の要 求に応じる必要があります。





原則 3

関係者とは常に情報セキュリティに関するコミュニケーションをとる

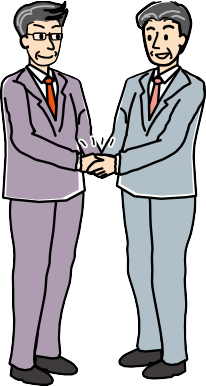
業務上の関係者（顧客、取引先、委託先、代理店、利用者、株主など）からの信頼を高める

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関する取組方針を常日頃より関係者に伝えておくことで、サイバー

攻撃によるウイルス感染や情報漏えいなどが発生した際にも、説明責任を果たすことが

でき、必要以上の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。 

参考情報

1. 実行すべき「重要７項目の取組」



中小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。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、実際に情報セキュリティ対策を実践 するうえでの責任者・担当者に対して指示します。場合によっては、経営者自らが実行す ることも必要になると考えられます。



|  |  |  |
| --- | --- | --- |
|  | 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、従業員や関係者に明確に示すために、どのような情報をどのように守るかなどについて、自社に適した情報セキュリティに関 する基本方針を定め、宣言します。自社の経営において最も懸念される事態は何かを明確 にすることで具体的な対策を促し、組織としての方針を立てやすくなります。

|  |  |  |
| --- | --- | --- |
|  | 取組 2 | 情報セキュリティ対策のための予算や人材などを確保する |

情報セキュリティ対策を実施するために、必要な予算と担当者を確保します。これには事故の発生防止だけでなく、万が一事故が起きてしまった場合の被害の拡大防止や、復旧対応も含みます。情報セキュリティ対策には高度な技術が必要なため、専門的な外部サービス５の利用も検討します。

|  |  |  |
| --- | --- | --- |
|  | 取組 3 | 必要と考えられる対策を検討させて実行を指示する |

懸念される事態に関連する情報や業務を整理し、損害を受ける可能性（リスク）を把握 したうえで、責任者・担当者に対策を検討させます。必要とされる対策には予算を与え、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。実行を指示した情報セキュリティ対策がどのように現場で実施されているかにつき、 月次や四半期ごとなど適切な機会をとらえて報告させ、進捗や効果を把握します。



取組３で指示した情報セキュリティ対策について、実施状況を点検させ、取組１で定めた方針に沿って進んでいるかどうかの評価をします。また業務や顧客の期待の変化など も踏まえて基本方針なども適宜見直しを行い、致命的な被害につながらないよう、対策の追加や改善などを行うように、責任者・担当者に指示します。



参考情報

|  |  |  |
| --- | --- | --- |
|  | 取組 4 | 情報セキュリティ対策に関する適宜の見直しを指示する |

５▲専門的な外部サービスについてはIPA が公開している「情報セキュリティサービス基準適合サービスリスト」を活用することができます。（P.39 コラム「情報セキュリティサービス基準審査登録制度」参照）



|  |  |  |
| --- | --- | --- |
|  | 取組 5 | 緊急時の対応や復旧のための体制を整備する |

万が一に備えて、緊急時の対応体制を整備します。被害原因を速やかに追究して被害の 拡大を防ぐ体制を作るとともに、的確な復旧手順をあらかじめ作成しておくことにより、緊急時に適切な指示を出すことができます。整備後には予定どおりに機能するかを確認 するため、被害発生を想定した模擬訓練を行うと、意識づけや適切な対応のために効果的 です。経営者のふるまいについても、あらかじめ想定しておけば、冷静で的確な対応が可 能になります。



|  |  |  |
| --- | --- | --- |
|  | 取組 6 | 委託や外部サービス利用の際にはセキュリティに関する責任を明確にする |

業務の一部を外部に委託する場合は、委託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委 託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。

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、自社でシステムを構築・運用するよりも、外部サービスを利用したほうが、コスト面から有利な場合がありますが、安易に利用することなく、利用規約や付随する情報セキュリティ対策などを十分に検討するよう担当者に指示する 必要があります。



|  |  |  |
| --- | --- | --- |
|  | 取組 7 | 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、実施を検討するべき対策は目まぐるしく変化します。自社だけで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６などを把握しておき、常時参照することで備えるように情報セキュリティ担当者に指示します。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。



参考情報

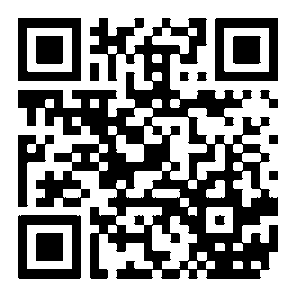




６▲情報セキュリティに関する最新動向を発信している公的機関 IPA（独立行政法人情報処理推進機構）のウェブサイト [https://www.ipa.go.jp/security/index.html](http://www.ipa.go.jp/security/index.html) NISC（内閣サイバーセキュリティセンター）のウェブサイト [https://www.nisc.go.jp/](http://www.nisc.go.jp/)

参考情報

「SECURITY ACTION」一つ星を宣言しよう！



**コラム**

「SECURITY ACTION（セキュリティアクション）」は、中小企業自らが情報セキュ

リティ対策に取り組むことを自己宣言する制度です。取り組み段階に応じて、「一つ 星」「二つ星」のロゴマークを無料で使用することができます。



「一つ星」は、情報セキュリティ５か条に取り組むことを宣言するものです。

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！ ２．ウイルス対策ソフトを導入しよう！

３．パスワードを強化しよう！ ４．共有設定を見直そう！

５．脅威や攻撃の手口を知ろう！

これらの項目は、企業の規模に関わらず、必ず実行すべき重要な対策です。第２部 に進む前に経営者のトップダウンで実行を開始して、自社が情報セキュリティ対策 の取り組みを開始したことを自己宣言しましょう。

宣言方法や制度詳細は公式サイトをご確認ください。

●SECURITY ACTION公式サイト[https://www.ipa.go.jp/security/security-action/](http://www.ipa.go.jp/security/security-action/)













参考情報

|  |
| --- |
| **第 2 部 実践編** |
| 実践編では、情報セキュリティ対策を実践する責任者・担当者を対象に、  実務的な進め方について説明します。 |
|  |

###### 実践編の進め方



1

ここでは、経営者の指示に従い、どのように情報セキュリティ対策を実践していくかについて説明します。情報セキュリティ対策に組織全体で取り組むには、実行すべき対策を決めて、従業員に周知する必要があります。

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な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などを対象に、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。第１部で説明した重要 ７項目の取り組みとの対応を示した表３を参考に、自社の状況にあった進め方をしてく ださい。



実践編の進め方

【表３】重要７項目の取り組みと実践編の対応表







参考情報

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 実践編 | | ページ | 取組  1 | 取組  2 | 取組  3 | 取組  4 | 取組  5 | 取組  6 | 取組  7 |
| **2** | できるところから始める |  |  |  |  |  |  |  |  |
|  | （1） 情報セキュリティ５か条 | 17 |  |  | ● |  |  |  | ● |
| **3** | 組織的な取り組みを開始する |  |  |  |  |  |  |  |  |
|  | （1） 情報セキュリティ基本方針の作成と周知 | 18 | ● |  |  |  |  |  |  |
| （2） 実施状況の把握 | 18 |  |  | ● |  |  |  |  |
| （3） 対策の決定と周知 | 20 |  |  | ● |  |  |  |  |
| **4** | 本格的に取り組む |  |  |  |  |  |  |  |  |
|  | （1） 管理体制の構築 | 22 |  | ● |  |  |  |  |  |
| （2） ＩＴ利活用方針と情報セキュリティの予算化 | 23 |  |  |  |  | ● |  |  |
| （3） 情報セキュリティ規程の作成 | 24 |  | ● |  |  |  |  |  |
| （4） 委託時の対策 | 26 |  |  | ● |  |  |  |  |
| （5） 点検と改善 | 28 |  |  |  |  |  | ● |  |
| **5** | より強固にするための方策 |  |  |  |  |  |  |  |  |
|  | （1） 情報収集と共有 | 30 |  |  |  | ● |  |  |  |
| （2） ウェブサイトの情報セキュリティ | 31 |  |  |  |  |  |  | ● |
| （3） クラウドサービスの情報セキュリティ | 33 |  |  |  | ● |  |  |  |
| （4） 情報セキュリティサービスの活用 | 38 |  |  |  | ● |  |  |  |
| （5） 技術的対策例と活用 | 40 |  |  |  | ● |  |  |  |
| （6） 詳細リスク分析の実施方法 | 44 |  |  |  | ● |  |  |  |



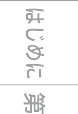






2 できるところから始める

1. 情報セキュリティ５か条



多くの中小企業にとっては、いきなり精巧な対策を開始するのは大変なことだと思い ます。「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、必ず実行すべき重要な対策を５か条にまとめています。

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 なっていますが、対策には共通する部分があります。情報セキュリティ５か条は、共通的 な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。



① OSやソフトウェアは常に最新の状態にしよう！

OS やソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、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。



② ウイルス対策ソフトを導入しよう！

できるところから始める

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。

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流出したID・パスワードが悪用されたりすることで、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。

④ 共有設定を見直そう！

データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違った ために、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。無関係な人が、 ウェブサービスや機器を使うことができるような設定になっていないことを確認しま しょう。



参考情報

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き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。

###### 組織的な取り組みを開始する



3

* 1. 情報セキュリティ基本方針の作成と周知

経営者が定めた情報セキュリティに関する基本方針を、従業員や関係者に伝えるために、簡潔な文書を作ります。基本方針には、決まった書き方はありませんので、「情報セキュリ ティ基本方針（サンプル）」（付録２）を参考にして、事業の特徴や顧客の期待などを考慮したうえで経営者と連携しつつ、自社に適した基本方針を作成してください。



また、基本方針は従業員の指針であり、関係者に対して取り組みを表明するためのものなので、作成した文書は、従業員や顧客などの関係者に周知しましょう。



**情報セキュリティ基本方針の記載項目例**

* 管理体制の整備
* 法令・ガイドライン等の順守
* セキュリティ対策の実施
* 継続的改善 など



* 1. 実施状況の把握

組織的な取り組みを開始する

「５分でできる！情報セキュリティ自社診断」（付録３）を利用して、情報セキュリティ対策が、どれくらい実施できているかを把握します。自社診断は、表４に示す25項目の設問に答えるだけで情報セキュリティ対策の実施状況が把握できるツー

ルです。

具体的な使い方は以下のとおりです。

* + - 経営者または情報システム担当や部門長など実施状況が分かる人が

「５分でできる！情報セキュリティ自社診断」の診断編に記入します。

参考情報

* + - 事業所が複数ある、部署数が多いなど、一人で記入することが難しい 場合には、事業所や部署ごとに記入し、責任者・担当者が集計します。
    - 実施状況が分からない場合は、各従業員に質問して、回答を総合して記入します。



* + - チェック欄の該当するもの１つに〇を付けて、「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 ０点「」わからない －１点」で採点します。

* + - 全項目の合計点で、組織全体のセキュリティ対策の実施状況と、回答 が「わからない」になっている項目を把握します。

【表４】自社診断のための25項目



組織的な取り組みを開始する

**基本的対策**

**従業員としての対策**

|  |  |  |
| --- | --- | --- |
| **No** | | **診断内容** |
|  | **1** | パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？ |
| **2** | パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の  状態にしていますか？ |
| **3** | パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？ |
| **4** | 重要情報※2 に対する適切なアクセス制限を行っていますか？ |
| **5** | 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？ |
|  | **6** | 電子メールの添付ファイルや本文中のURL リンクを介したウイルス感染に気をつけていますか？ |
| **7** | 電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？ |
| **8** | 重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護  していますか？ |
| **9** | 無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？ |
| **10** | インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしていま  すか？ |
| **11** | パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを  取得していますか？ |
| **12** | 紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫など  に安全に保管していますか？ |
| **13** | 重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？ |
| **14** | 離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？ |
| **15** | 関係者以外の事務所への立ち入りを制限していますか？ |
| **16** | 退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？ |
| **17** | 事務所が無人になる時の施錠忘れ対策を実施していますか？ |
| **18** | 重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないよう  にしていますか？ |
|  | **19** | 従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを  守らせていますか？ |
| **20** | 従業員にセキュリティに関する教育や注意喚起を行っていますか？ |
| **21** | 個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？ |
| **22** | 重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？ |
| **23** | クラウドサービスやウェブサイトの運用などで利用する外部サービスは、安全・信頼性を把握  して選定していますか？ |
| **24** | セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備を  していますか？ |
| **25** | 情報セキュリティ対策（上記 1 ～ 24 など）をルール化し、従業員に明示していますか？ |





※ 1 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」とも呼ばれます。



参考情報

**組織としての対策**

※ 2 重要情報とは営業秘密など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。

* 1. 対策の決定と周知



診断結果をもとに、「５分でできる！情報セキュリティ自社診断」の解説編を参考に、実行すべき情報セキュリティ対策を検討します。自社診断には、あまり費用をかけず、効果 があると考えられる対策例が示されているので、診断結果に基づき、実施すべき対策を検討します。



具体的な使い方は以下のとおりです。

* + - 対策の検討と決定は、責任者・担当者と経営者が行います。
    - 診断項目ごとに対策を実施しない場合に考えられる被害・事故や、防止するための対策例が示されているので、参考にして検討します。
    - 検討するときには従業員の意見を聞き、職場環境や業務に適した対策を決定します。



対策が決まったら「、情報セキュリティハンドブック（ひな形）（」付録４）を利用して、従業員が実行するべき事項を周知します。情報セキュリティハンドブック（ひな形）は、自社診

組織的な取り組みを開始する

 断の対策例と連動したひな形です。決定した対策を具体的に記述して、従業員に配付します。具体的な使い方は以下のとおりです。

* + - 情報セキュリティハンドブックは、責任者・担当者が作成します。
    - ひな形に記載された例文を編集して、決定した対策を社内ルールとして明文化します。

参考情報

（例）データのバックアップ

編集前（ひな形）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 機器名 | 対象 | 方法 | 保管媒体 | 頻度 |
| ○○サーバー | システムファイル  ユーザーファイル | Windows バックアップ | 外付け HDD | 毎週 |



編集後



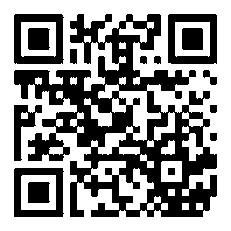
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 機器名 | 対象 | 方法 | 保管媒体 | 頻度 |
| 営業部  ファイルサーバー | 売買契約書ファイル | バックアップソフトによる  増分バックアップ | 外付け HDD | 毎週 |

* + - 完成した情報セキュリティハンドブックを全従業員に配付し、必要に応じて説明する 機会を設けるなどして、情報セキュリティ対策を周知徹底します。

参考情報

**コラム**

「SECURITY ACTION」二つ星へステップアップ！



IT 化社会では、情報の取り扱いに関して安心して利用できる、発注できる、取引で

きる会社であることが求められるようになってきました。しかし、顧客や相手の会

社に、自社が情報セキュリティに取り組んでいるかどうかを具体的に示すのは、と

ても難しいことです。顧客や取引先に情報セキュリティ対策への取り組みを明確に 伝え、信頼を獲得するために「二つ星」を宣言してみませんか。

「二つ星」は、「3．組織的な取り組みを開始する」を実施したことを宣言するものです。

●「５分でできる！情報セキュリティ自社診断」で自社の状況を把握

●「情報セキュリティ基本方針」を定め、外部に公開



宣言方法や「一つ星」からのステップアップについては公式サイト をご確認ください。

組織的な取り組みを開始する

●SECURITY ACTION公式サイト[https://www.ipa.go.jp/security/security-action/](http://www.ipa.go.jp/security/security-action/)







4 本格的に取り組む

自社に適した対策を実行して効果をあげるには、まず、自社にどのような情報セキュリティリスク（事故が発生したとき事業へ損害を与える危険性のこと。以下、「リスク」とい います。）があるかを考えます。経営者が懸念する情報セキュリティ上の重大事故やその 関連業務などを踏まえ、事業へ大きな損害を与える事故を防ぐための対策を決めて、具体的に記述します。（対策を記述した文書のことを、以下、「規程」といいます。）



（1）管理体制の構築

①責任分担と連絡体制の整備

P.18（1）情報セキュリティ基本方針の作成と周知にて作成した情報セキュリティ基本方針を具体的に実現するための、情報セキュリティ対策を推進する管理体制を決め ます（表５）。情報セキュリティ責任者から部門責任者を通じて従業員への情報の伝達経路を確立し、また情報セキュリティ上の事故などが発生した場合は、情報セキュリティ責任者へ状況が迅速に報告されるような連絡体制を整備することが重要です。すでに 個人情報保護管理体制（特定個人情報事務取扱責任者、個人情報苦情対応者）などが決 まっている場合は、既存の管理体制との整合をとるようにしましょう。



【表５】情報セキュリティ管理のための役割と責任分担（例）

本格的に取り組む

|  |  |
| --- | --- |
| **役職名** | **役割と責任** |
| 情報セキュリティ責任者 | 情報セキュリティに関する責任者です。情報セキュリティ対策などの決定権限を有するとともに、全責任を負います。 |
| 情報セキュリティ部門責任者 | 各部門における情報セキュリティの運用管理責任者です。各部門における情報セキュリティ対策の実施などの責任と権限を有します。 |
| システム管理者 | 情報セキュリティ対策のためのシステム管理を行います。 |
| 教育責任者 | 情報セキュリティ対策を推進するために従業員への教育を企画・実施します。 |
| 点検責任者 | 情報セキュリティ対策が適切に実施されているか点検します。 |



なお、情報セキュリティ組織の担当者がそれぞれの役割を果たすためには、情報セキュリティに関する知識や経験も必要です。知識の習得や経験には時間も必要になるため、中長期の視点で担当者を育成することも考えましょう。



参考情報

また、小規模な企業などでは、表５の例にとらわれずに、実効的な体制（役割分担）を独 自に考えることもあり得るでしょうが、誰か一人に情報セキュリティ対策の全てを任せ てしまうような体制は望ましいものではありません。

②緊急時対応体制の整備



事業や顧客などに大きな影響がある情報セキュリティ事故が発生した場合に、迅速 に対応するための体制をあらかじめ決めておきます（表６）。対応を誤ったり、遅れると、被害が拡大したり、復旧がうまくいかずに、取り返しのつかないことになるため、誰が 何をするか役割や手順を明確に決めておく必要があります。また、組織内外の緊急連絡



先・伝達ルートを整備し、周知しておくことも重要です。加えて、緊急時対応に関する話

し合いや訓練などを実施し、実際に決めたとおりに動けるのかを確認するようにしま

しょう。関係者やIT 製品のメーカー、保守ベンダー等への連絡先もまとめておきます。

業務システムが使えなくなるような事故においては、メールやweb ブラウザも使えな

くなる可能性があるため、連絡の代替手段も確認しておきましょう。



【表６】緊急時対応体制の役割と責任（例）

|  |  |
| --- | --- |
| **役職名** | **役割と責任** |
| 情報セキュリティ責任者 | 事故の影響を判断し、対応について意思決定する。 |
| 情報セキュリティ部門責任者 | 対応責任者の判断・意思決定に基づき適切な処置を行う。事故の原因を  調べて情報セキュリティ責任者に報告する。 |
| 事故・異常を発見した従業員 | 事故や異常の内容を情報セキュリティ部門責任者に報告する。 |



1. IT 利活用方針と情報セキュリティの予算化



企業運営においてIT の利活用による生産性の向上や業務の効率化を進めることは重要な課題です。従来はIT 機器やソフトウェアを購入して自社内に情報システムを構築することが多かったのですが、現在はレンタルサーバーやクラウドサービスなど外部サービ スも増えたため、IT 利活用のしかたは多様化しています。それに伴いリスクも多様化しているため、自社で利用している情報システムについて、例えば台帳を作成したり図式化したりするなどして把握したうえで、対策を検討するとともに、予算を確保する必要があります。

本格的に取り組む

インターネット



クラウドサービス

社内

ファイルサーバー

（ファイル共有）

ルータ

スイッチングハブ

無線 LAN アクセスポイント

デスクトップパソコン３台

（OS : Windows10）

ノートパソコン 1 台

（OS : Windows10）

レンタルサーバー

（ウェブサイト、メール）

参考情報





1. 情報セキュリティ規程の作成



企業を取り巻くリスクは、事業内容や取り扱う情報、職場環境、IT の利用状況などによっても異なることがあり、汎用的な規程をそのまま使っても、自社に適さないことが考えられます。そこでここでは、効率的に自社に適した規程を作成する方法を解説します。



①対応すべきリスクの特定

経営者が懸念する避けるべき情報セキュリティの重大事故などを踏まえて、何が起 こらないようにするべきかを考えます。この時、以下のような状況を併せて考えることで、対応すべきリスクを把握します。

* 関連する業務や情報に係る外部状況（法律や規制、情報セキュリティ事故の傾向、取 引先からの情報セキュリティに関する要求事項など）
* 内部状況（経営方針・情報セキュリティ方針、管理体制、情報システムの利用状況など）

**個人情報保護法への対応**



**取引先のセキュリティに対する要求への対応**

本格的に取り組む

**報道されている新たなサイバー攻撃**

**への対応**

**テレワーク導入時のセキュリティへの対応**

②対策の決定

全てのリスクに対応しようとすると費用が多額になったり、仕事が非効率になるこ とがあります。そこで、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を優先して対策を実施し、事故が起きる可能性が小さいか、発生しても被害が軽微であるなど、リスクが小さなものについては、現 状のままにするなど、合理的に対応します。

参考情報







参考情報

本格的に取り組む

③規程の作成



②で決定した対策を文書化した規程を作成します。決定した対策を一から文書化す るのは経験がないと難しいため、「情報セキュリティ関連規程（サンプル）」（付録５）を参考に、自社に適した規程にするために修正を加えます（表７）。



サンプル文中の赤字、青字部分を自社向けに修正すれば、自社の規程が完成します。

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、追記を行っ

てください。

|  |  |  |
| --- | --- | --- |
|  | **名 称** | **概 要** |
| 1 | 組織的対策 | 情報セキュリティのための管理体制の構築や点検、情報共有などのルールを定めます。 |
| 2 | 人的対策 | 取締役及び従業員の責務や教育、人材育成などのルールを定めます。 |
| 3 | 情報資産管理 | 情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定めます。 |
| 4 | アクセス制御及び認証 | 情報資産に対するアクセス制御方針や認証のルールを定めます。 |
| 5 | 物理的対策 | セキュリティ領域の設定や領域内での注意事項などのルールを定めます。 |
| 6 | IT 機器利用 | IT 機器やソフトウェアの利用などのルールを定めます。 |
| 7 | IT 基盤運用管理 | サーバーやネットワーク等の IT インフラに関するルールを定めます。 |
| 8 | システムの開発及び保守 | 独自に開発及び保守を行う情報システムに関するルールを定めます。 |
| 9 | 委託管理 | 業務委託にあたっての選定や契約、評価のルールを定めます。業務委託契約書の機密保持に関する条項例と委託先チェック  リストのサンプルが付属します。 |
| 10 | 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 | 情報セキュリティに関する事故対応や事業継続管理などのルールを定めます。 |
| 11 | 個人番号及び特定個人情報の取り扱い | マイナンバーの取り扱いに関するルールを定めます。 |

【表７】情報セキュリティ関連規程（サンプル）の概要













参考情報

1. 委託時の対策



社内業務の一部または全部を外部に委託したり、レンタルサーバーやクラウドサービ スなどの外部サービスを利用することが一般的になっています。重要な情報を渡したり、処理を依頼する場合には、委託先にも情報セキュリティ対策を実施してもらう必要があ ります。



直接指示することが難しい外部の組織に、対策を実施してもらうには、取引条件のひと

つとして契約書や覚書などに具体的な対策を明記します。個別に契約や覚書を交わすこ

とができない場合は、委託先のサービス規約や情報セキュリティに関わる対応方針を確 認したうえで選定します。

また、個人情報保護法では、個人データ７の取り扱いを委託する場合は、委託先にも情報セキュリティ対策を実施してもらうように監督することが義務付けられています。委託 先の状況を把握し、対策が確実に実施されるように委託元が責任をもつ必要があります。

委託先の対策不足で事故が起きた場合には、委託元は管理責任を問われ、委託先は委託元の信頼を失います。重要な情報や個人情報などセキュリティ事故の影響が大きい情報 の授受が行われる場合には、委託元は委託先にセキュリティ対策についての要望や期待 をしっかりと伝え、受託する側はそれをきちんと理解し、実行する必要があります。



・重要な情報

・個人情報

・重要な情報

・個人情報

本格的に取り組む

委託

再委託

情報セキュリティ対策状況の把握

これらを踏まえ、取り扱う情報の種類、委託する業務に適した情報セキュリティ対策を 委託先にも実施してもらいます。機密情報や個人情報を取り扱う場合は、「情報セキュリ ティ関連規程（サンプル）」（付録5）の「業務委託契約に係る機密保持条項」を参考にして、委託先と契約したり、委託先を選定してください。さらに、情報セキュリティ対策が継続 して実施されているか、新たな対策が必要になったときに対応しているかなどを随時確 認して、委託先の情報セキュリティ対策が維持されているか、責任をもって管理します。

７▲個人情報保護法では「個人情報」、「個人データ」、「保有個人データ」、「要配慮個人情報」、「匿名加工情報」等の語を使い分けており、個人情報取扱事業者等に課される義務はそれぞ異なるので、注意を要します。



**コラム**

委託と受託



委託とは他者に業務を行ってもらうことです。外注、委任、準委任、アウトソーシ

ングなどということもあり、受託とは他者の業務を引き受けることで、請負という こともあります。

どのような会社でも事業を行ううえで、全ての業務を自社で行うことは難しいた め、委託している業務があり、委託とそれを引き受ける受託とで成り立っています。 また、業務を委託するときには、委託元と委託先との間で情報の授受が発生します。 例えば、以下のような皆さんの身近な業務で、情報を授受していませんか。

●税理士に帳簿や決算書の作成を依頼 ：売上伝票、出金伝票 

●外部の工場に部品の製造を依頼 ：設計図



●システム開発会社にEC サイトの運用を依頼：住所、氏名など顧客の個人情報

このように重要な情報や個人情報を渡す場合に、委託先が対策を怠っていれば、 漏えいや改ざんなどの事故が起きやすくなります。

本格的に取り組む

業務を受託する場合においては、発注元が求めるセキュ リティ対策を実施できることを示す必要があります。自己 点検の結果や、SECURITY ACTION のロゴマークを提示したり、具体的な規程の内容や、システム上の対策例を閲 覧してもらうことで、相手の信頼を得ましょう。

参考情報



1. 点検と改善



情報セキュリティの点検とは、計画した情報セキュリティ対策が、本当に実行されているか、見落としている対策はないか、対策がセキュリティ事故防止のために役に立っているか、を確認することです。点検の基準には以下を用いることができます。



その１「）情報セキュリティ５か条」や「５分でできる！情報セキュリティ自社診断」に基 づく点検

点検基準例

☑「情報セキュリティ５か条」No.1の対策例を基準にする。

パソコンのWindowsUpdate が「更新プログラムを自動的にインストールする」に設定されていて、更新日が直近の日付であるか

☑「５分でできる！情報セキュリティ自社診断」No.20の対策例を基準にする。

従業員に情報セキュリティ事故のニュースを周知したり、情報セキュリティ啓発サ イトの新着情報を配信するなどしているか

その２）策定した情報セキュリティ対策に関するルール・規程に基づく点検

点検基準例



☑ウイルス感染時の初期対応のルールを基準にする。

社内規程の中で、ウイルス感染時の対応に関する記述を理解しているか

（「情報セキュリティ関連規程（サンプル）」No.10「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」の該当項目を参照）

本格的に取り組む

点検には、以下の方法があります。

* 質問（インタビュー）：従業員や委託先の管理者などに直接質問して回答してもらう
* 閲覧（レビュー） ：関連する文書や記録、パソコンの設定画面など対策を実行した証拠となるものを確認する
* 観察（視察） ：点検の対象となる職場に出向き、従業員が規程や標準規格な どに従った行動をしていることを確認する

参考情報

* 技術診断 ：専用ソフトウェアなどを使ってコンピュータやネットワークのセキュリティ対策が実行されているかを確認する

●チェックリスト ：チェックリストや質問書を配付して回答してもらう

点検の結果を経営者に報告し、経営者の意図するセキュリティ対策が実現できているかの確認と評価をすることが重要です。経営者の評価を得ることで、場合によってはリスクの特定に戻って対策の見直しをするなどにより、取り組みの精度を高めていくことになります。なお、営業秘密や個人情報等の、特に十分な対策が必要な場合には、第三者による情報 セキュリティ監査８を行うことも検討します。



８▲一般に、点検は点検対象業務に従事している関係者自身が実施するのに対し、監査は監査対象業務に従事していない、独立した監査担当者によって実施されるため、より客観的な確認を行う必要がある場合には監査が適しています。



**コラム**

情報セキュリティ点検の実施例



「情報セキュリティ５か条」に取り組んでSECURITY ACTION 一つ星を自己宣言している会社が、「情報セキュリティ５か条」を基準にして点検するときの実施例 です。

① No.1「OS やソフトウェアは常に最新の状態にしよう！」について社員の一人に、

質問と閲覧で点検します。

「情報セキュリティ５か条」では OS やソフトウェアは常に最新の状態にすることに

なっていますが、持出し用のノートパソコンの OS やソフトウェアは最新の状態で

しょうか？」

「ノートパソコンをしばらく使っていないので、分かりません。」





「では、Windows Update の更新プログラムのインストール履歴を見せてください。」

「（ノートパソコンの画面に更新プログラムのインストール履歴を表示）」

「画面を見ると最後のインストール履歴が 2 か月前になっていますが、理由はわかりますか？」

本格的に取り組む

「Windows Update は自動更新に設定していますが、このノートパソコンは社外に出かけるときだけに使うので、普段はネットワークに接続していません。それで更新されていないのだと思います。明日、お客様の事務所に伺い、このノートパソコンをお客様の LAN につないでメールを使いますので、その前に更新しようと思い

ます。」 

②ノートパソコンを持ち出すことがある他の社員に、質問やパソコンの画面を見せてもらい、その回答や観察の結果から総合的に判定します。

参考情報

この例では、「情報セキュリティ５か条」の「OS やソフトは常に最新の状態にしよう！」を実行できていないパソコンがあることを発見しました。その状態で お客様のLAN に接続する予定であったことから、影響が社外におよぶ可能性があり、リスクが大きいと言えます。このようにリスクが大きいと考えられる場合は、すぐに是正するよう助言します。



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。

参考情報

5 より強固にするための方策

IT の普及に伴い情報セキュリティ対策も重要視されています。技術の悪用や技術的な攻撃を防ぐためには、人的な注意や対策だけでは限界があり、技術的対策を強化したり、 外部の専門サービスを利用する必要があります。



ここでは、事業でコンピュータやインターネットを活用している企業が、より強固な情報セキュリティ対策に取り組むために必要とされる技術的対策や、対策の導き出し方な ど以下の６つの区分について説明します。

1. 情報収集と共有

情報セキュリティに関する情報収集の方法と情報共有の枠組みについて説明します。

1. ウェブサイトの情報セキュリティ

ウェブサイトを安全に構築し、運用するためのポイントを説明します。

1. クラウドサービスの情報セキュリティ

クラウドサービスを安全に利用するためのポイントを説明します。

1. セキュリティサービス例と活用

 情報セキュリティに関する外部サービスを説明します。

1. 技術的対策例と活用



IT を活用する際の技術的対策について説明します。

1. 詳細リスク分析の実施方法

「リスク分析シート」（付録７）を活用した詳細リスク分析の実施方法を説明します。

より強固にするための方策









参考情報

1. 情報収集と共有



情報セキュリティに関する脅威や攻撃の手口を知って組織内に共有することは、組織 の対策レベルの向上につながります。また、その情報を社外の関係者と共有することで、 社会全体のセキュリティレベルの向上にもつながります。ここでは、情報セキュリティに 関する情報収集の方法と情報共有の枠組みを説明します。



①情報収集の方法

情報収集で重要なことは、定常的に情報収集ができる方法を整備することです。その

ためには、情報を得る先を理解し、必要な情報が自動的に得られる仕組みを構築します。

例えば、情報セキュリティの専門機関やセキュリティベンダーのメールマガジンやソー

シャルメディアに登録したり、セミナーに参加して積極的な情報収集を行います。

②情報共有の枠組み

近年、取引先や同業者を経由したサイバー攻撃が増加しています。そこで、収集した 情報は社内の関係者だけでなく、取引先や同業者に対しても共有することで、対策の向上が期待できます。共有する情報に機密情報が含まれる可能性がある場合は、守秘義務契約を交わします。情報共有の枠組みとしては日本シーサート協議会の他、業界別のISAC９が組織されている場合があります。



**参考情報**

（情報収集の方法）

■ここからセキュリティ！ [https://www.ipa.go.jp/security/kokokara/](http://www.ipa.go.jp/security/kokokara/)

* IPA セキュリティセンター[https://www.ipa.go.jp/security/](http://www.ipa.go.jp/security/)
* IPA サイバーセキュリティ注意喚起サービス「icat for JSON」[https://www.ipa.go.jp/security/vuln/icat.html](http://www.ipa.go.jp/security/vuln/icat.html)
* JPCERT/CC [https://www.jpcert.or](http://www.jpcert.or.jp/).jp/

■警察庁 @police [https://www.npa.go.jp/cyberpolice/](http://www.npa.go.jp/cyberpolice/)

（情報共有の枠組み）

■日本シーサート協議会[https://www.nca.gr](http://www.nca.gr.jp/).jp/

より強固にするための方策

９▲ ISAC（Information Sharing and Analysis Center）同業界の事業者同士でサイバーセキュリティーに関する情報の共有・分析などを行う組織

* 1. ウェブサイトの情報セキュリティ



自社のウェブサイトを持ち活用することは顧客獲得や売上増に直結するため、多くの 中小企業でもウェブサイトの開設しています。しかし、世界中の誰でもアクセスできるため、攻撃の対象になりやすく、顧客情報の漏えいや、不正サイトに誘導するなどの改ざんによって、自社だけでなく、利用者にも被害が発生することが懸念されます。そのため、ウェブサ



イトを活用する際は同時に対策を講じる必要があります。ここでは、ウェブサイトの運営

形態の検討から実際に運営するまでの３つの段階に分けて検討事項を説明します。

ウェブサイトでの運営形態によって

**ウェブサイト運営形態の検討**

**ウェブサイトの構築**

**ウェブサイトの運営**

ウェブサイトの技術的な脆弱性を認

運用開始後に発覚した情報セキュリ

セキュリティ対策が異なるため、自社

識したうえで、必要なセキュリティ対

ティ上の問題にも適切に対応し、ウェ

の状態に見合った運営形態を検討し ましょう。

策を設計・開発の段階から検討しましょう。

ブサイトの安全性を維持向上しましょう。

①ウェブサイト運営形態の検討

ウェブサイトをどのような形態で運営するかによって、運営にかかる費用が変化す るのはもちろん、運営者が実施する作業内容が異なるため、運営者に求められる技術レベルも変化します。また、運営形態ごとにウェブサイト上でどのような機能を提供できるか、ウェブサイトをどこまで自由に変更できるか、どのような情報セキュリティ対策が必要になるかについても異なります。特に企業のウェブサイトでは個人情報を取り 扱うことも多く、サイト運営者は情報セキュリティが継続的に維持され、最新の脅威に対し対策ができているかどうかに気を配る必要があります。運営者はウェブサイトを 構築する前に表８に示す運営形態ごとの特徴を理解し、組織の状況に応じた運営形態 を選定する必要があります。



より強固にするための方策

【表８】運営形態ごとの特徴

参考情報

|  |  |
| --- | --- |
| **運営形態** | **特徴** |
| サーバー自社設置  （オンプレミス） | ネットワークやサーバーなどの用意から、そのうえで稼動するウェブサイトの構築・運用まで、全て自社で行う運営形態。全ての情報セキュリティ対策を自社で行う必要があります。 |
| レンタルサーバー・ クラウドサービス（PaaS） | ネットワークやサーバーなどは外部サービスを利用し、ウェブサイトの構築・運用のみ自社で行う運営形態。ネットワークやサーバーの情報セキュリティ対策は外部サービスが行うため、ウェブサイトの構築・運用面に関わる情報セキュリティ対策のみ自社で行う必要があります。 |
| モール・ASP | ウェブサイトの開設に必要な機能や運用を一括して外部サービスを利用し、ウェブサイトに掲載するコンテンツだけ自社で準備（登録）する運営形態。外部サービスを利用するための認証情報を、ウェブサイト運営者が適切に管理する必要があります。 |





②ウェブサイトの構築



ウェブサイトの「安全上の欠陥」（脆弱性）が狙われる事件が後を絶ちません。ウェブ サイトの安全を維持するためには、サーバーOS やソフトウェアに対して脆弱性修正パッチの適用や安全な設定などを維持することが重要です。しかし、独自に開発する「ウェ ブアプリケーション10」については、情報セキュリティ上の問題が発覚した場合、サー



ビスの継続提供やコストなどの観点から、設計レベルから修正することは難しい場合

が少なくなく、軽減策で済まさざるをえないこともあります。開発段階において、可能

な限り脆弱性を解消することが望まれます。そこで、ウェブアプリケーションを自社ま

たは委託して開発する場合、参考情報に示す「安全なウェブサイトの作り方」を参照し 脆弱性の対策を実施してください。

③ウェブサイトの運営

安全にウェブサイトを運営するためには、下記図が示す対象ごとに適切な対策を実

施することが必要です。どれが欠けても、ウェブサイトの安全性は確保できません。

参考情報に示す「安全なウェブサイトの運用管理に向けての20ヶ条」を参照して、対

策がとられていない項目があった場合には早急に対策をしてください。



インターネット

ウェブアプリケーション

ウェブアプリケーションフレームワーク

サーバソフトウェア

ウェブサーバ

OS

Check Check

1. ウェブアプリケーションの

のセキュリティ対策

セキュリティ対策

2. ウェブアプリケーションが

稼動しているウェブサーバ

3. ネットワーク（ルータやファイア

Check

ウェブサーバが設置されている

オール）のセキュリティ対策

Check

4. その他のセキュリティ対策

ウェブサイトのセキュリティ対策のチェックポイント

複数のソフトウェアから構成

* + 1. ウェブアプリケーションのセキュリティ対策のチェック例



参考情報

より強固にするための方策

・ウェブアプリケーションを構成しているソフトウェアの脆弱性対策を定期的にしていますか？



**参考情報**

■ウェブサイト開設等における運営形態の選定方法に関する手引き（IPA）

[https://www.ipa.go.jp/security/technicalwatch/20180530.html](http://www.ipa.go.jp/security/technicalwatch/20180530.html)

■安全なウェブサイトの作り方（IPA） [https://www.ipa.go.jp/security/vuln/websecurity.html](http://www.ipa.go.jp/security/vuln/websecurity.html)

■安全なウェブサイトの運用管理に向けての 20 ヶ条（IPA） [https://www.ipa.go.jp/security/vuln/websitecheck.html](http://www.ipa.go.jp/security/vuln/websitecheck.html)

10▲インターネットなどのネットワークを介して使用するアプリケーションソフトウェア

* 1. クラウドサービスの情報セキュリティ



インターネットの普及と技術の進展により、情報システムを所有せず、インターネット上で提供されるサービスとして利用することが増えています。必要なときに利用するだ けという“ クラウド化” によって、所有することで発生していた費用や手間が削減され、柔軟な運用が可能です。その一方で、情報システムの一部が、サービスを提供する事業者の



管理下に置かれることになるため、所有とは異なる観点で情報セキュリティ対策を配慮

する必要があります。ここではクラウドサービスの選定から運用するときのセキュリティ対策まで３つの段階に分けて検討事項を説明します。

**クラウドサービスの選定**

**クラウドサービスの運用**

**クラウドサービスのセキュリティ対策**

クラウド化する業務によって重視すべきセキュリティ対策は異なるため、

 業務のセキュリティ要件に見合った サービスを選定しましょう。

クラウドサービスは提供者と利用者が 連携して運用するため、その特性を理解して運用しましょう。

サービス利用者が対応すべきセキュリテ ィ対策を理解して実施しましょう。

①クラウドサービスの選定

クラウドサービスは、サービス事業者が提供する情報システム（ハードウェアやソフトウェア）の範囲によって、次の３形態に大別されます。



（クラウドサービスの３形態）

* SaaS（Software as a Service サース）：会計アプリケーションやオフィスソフト、ファイルサーバーなど、一般に利用されているアプリケーションソフトをウェブサービスとして提供します。

より強固にするための方策

* PaaS（Platform as a Service パース）：OS やデータベース管理システムなどのミドルウェアを提供します。アプリケーションソフトは別途導入しなければなりません。
* IaaS（Infrastructure as a Service イアース）：仮想のサーバーやメモリなどのハードウェアやネットワークなどのシステム基盤のみを提供します。

本ガイドラインではSaaS の利用を念頭に置いた情報セキュリティ対策について説明します。SaaS 形態のクラウドサービスは、提供されるアプリケーションを複数の組織が利用します。洋服に例えると既製服のようなもので、オーダーメイドのように利用者個別の希望に応じることが難しい部分もあることから、クラウド化する業務に必要 とされるセキュリティ対策を、あらかじめ検討し、それらを備えたクラウドサービスを選定する必要があります。

参考情報

②クラウドサービスをもちいたシステムの運用

自社で所有する情報システムとは異なり、クラウドサービスは他者が提供する情報 システムを利用するため、適切なセキュリティ対策を実施するためには、利用者と提供者とが役割と責任を分担し、それに応じて対策を実施します。

クラウドサービスでは、情報処理は全てクラウド事業者が管理するサーバーで実行 されるため、情報はクラウド事業者に預けている状態になります。このため、サーバー 側の対策は主にクラウド事業者に委ねられます。利用者の事業所にはクラウドサービ スを利用するための、インターネットに接続するパソコンやスマートフォンだけがあり、情報の入出力端末としての機能を果たしています。



このことから、セキュリティ対策のための利用者の役割と責任の範囲は、利用者が直

接管理することができるパソコンやスマートフォンなどの端末機器や、それらにイン

ストールされたソフトウェアに限定されるため、自社所有の情報システムよりも、ハー

ドウェアやソフトウェアへの対策に関する負担は軽減されます。しかし、クラウドサー

ビスはインターネットを介したサービスのため、いつでも、どこからでも、誰でもアク

セス可能であることが、自社所有の情報システムとは根本的に異なり、インターネット

特有の脅威やリスクを考慮して、運用上のセキュリティ対策を検討する必要があります。

③クラウドサービスのセキュリティ対策

クラウドサービスのセキュリティ対策は、以下の観点で検討して、状況に応じた適切な対策を実施してください。

* クラウドサービス事業者のセキュリティ対策を把握し、自社のセキュリティに関す る期待を満たしたサービスを利用する。



* 利用者である自社の役割・責任を把握し、自社でしかできない対策を的確に実行する。

詳細は、表９に示すクラウドサービス安全利用のための15項目を参考に、自社の目的 や運用計画などに適したクラウドサービスを利用してください。15項目の解説は、「中小企業のためのクラウドサービス安全利用の手引き」（付録６）を参照してください。

参考情報

より強固にするための方策

責任分界



自社

**！**

クラウドサービス事業者

わが社の役割と責任はどこまで？

所 有

営業秘密

~~個~~人情報

クラウドサービス

営業秘密個人情報



より強固にするための方策

【表９】中小企業のためのクラウドサービス安全利用のための15項目



|  |  |  |
| --- | --- | --- |
| NO. | 項目 | 内容 |
| **Ⅰ．選定するときのポイント** | | |
| 1 | どの業務で利用するか明確にする | どの業務をクラウドサービスで行い、どの情報を扱うかを検討し、業務の切り分けや運用ルールを明確にしましたか？ |
| 2 | クラウドサービスの種類を選ぶ | 業務に適したクラウドサービスを選定し、どのようなメリットがあるか確認しましたか？ |
| 3 | 取り扱う情報の重要度を確認する | クラウドサービスで取り扱う情報が漏えい、改ざん、消失したり、サービスが停止した場合の影響を確認しましたか？ |
| 4 | セキュリティのルールと矛盾しないようにする | 自社のルールとクラウドサービス活用との間に矛盾や不一致が生じませんか？ |
| 5 | クラウド事業者の信頼性を確認する | クラウドサービスを提供する事業者は信頼できる事業者ですか？ |
| 6 | クラウドサービスの安全・信頼性を確認する | サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービス品質保証は示されていますか？ |
| **Ⅱ．運用するときのポイント** | | |
| 7 | 管理担当者を決める | クラウドサービスの特性を理解した管理担当者を社内に確保していますか？ |
| 8 | 利用者の範囲を決める | クラウドサービスを適切な利用者のみが利用可能となるように管理できていますか？ |
| 9 | 利用者の認証を厳格に行う | パスワードなどの認証機能について適切に設定・管理は実施できていますか？（共有しない、複雑にするなど） |
| 10 | バックアップに責任を持つ | サービス停止やデータの消失・改ざんなどに備えて、重要情報を手元に確保して必要なときに使えるようにしていますか？ |
| **Ⅲ．セキュリティ管理のポイント** | | |
| 11 | 付帯するセキュリティ対策を確認する | サービスに付帯するセキュリティ対策が具体的に公開されていますか？ |
| 12 | 利用者サポートの体制を確認する | サービスの使い方がわからないときの支援（ヘルプデスクや FAQ）は提供されていますか？ |
| 13 | 利用終了時のデータを確保する | サービスの利用が終了したときの、データの取り扱い条件について確認しましたか？ |
| 14 | 適用法令や契約条件を確認する | 個人情報保護などを想定し、一般的契約条件の各項目について確認しましたか？ |
| 15 | データ保存先の地理的所在地を確認する | データがどの国や地域に設置されたサーバーに保存されているか確認しましたか？ |





















※ No15 クラウドサービスのサーバーは日本国外に設置されている場合もありますが、扱うデータによってサーバーの設置国・地域の法規制が適用されることがあります。

参考情報

※ No6・11・12・13 はスマート SME サポーター（認定情報処理支援機関）の開示情報で確認することができます。

**コラム**

クラウドサービス選択時に参考となる制度等



クラウドサービス事業者が適切なデータ保護やセキュリティ対策を実施してい ることをマークとして表示する制度があります。いずれもURL 記載のページ内でそれぞれの条件を満たすサービスが紹介されており、選定時の参考として利用するこ とができます。

●ISMSクラウドセキュリティ認証

（一般社団法人情報マネジメントシステム認定センター）

https://isms.jp/isms.html

ISMS（ISO/IEC27001）認証に加えて、クラウドサービス固有の管理策（ISO/IEC 27017）が適切に

導入、実施されていることを認証するものです。

●クラウド情報セキュリティ監査制度

（特定非営利活動法人日本セキュリティ監査協会）

<http://jcispa.jasa.jp/cloud_security/>

クラウドサービス事業者が基本的な要件を満たす情報セキュリティ対策を実施していることを監査し、

その結果をCS マークの表示許諾を通じて利用者に対し、安全性が確保されていることを公開する制度です。外部監査と内部監査で「ゴールド」と「シルバー」の２種類があります。



●ASP・SaaS 情報開示認定制度

（特定非営利活動法人日本ASP・SaaS・IoT クラウドコンソーシアム）

より強固にするための方策

<http://www.cloud-nintei.org/asp-nintei/>

安全・信頼性に係る比較・評価・選択を行うために必要な情報を、クラウドサービス事業者が開示をし

ていることを認定する制度です。クラウドで扱う情報や環境の種類に応じて、「医療情報」「特定個人情報」「IoT クラウド」「データセンター」など合計７種類の認定マークが定められています。

IT活用を支援する情報処理支援機関

中小企業者等の生産性向上に資するIT ツールや中小企業のIT 活用を支援するIT ベンダーを法令に基づいて認定し、中小企業者がIT ツール選定するために必要となる情報を開示しています。

参考情報

●認定情報処理支援機関（スマートSME サポーター）制度

（中小企業庁）

https://smartsme.go.jp/



中小企業が使いやすいIT ツールの開発促進や中小企業のIT 導入を通じた生

産性向上を図ります。認定を受けたIT ベンダーの情報セキュリティ対策の実施状況を確認できます。

* 1. 情報セキュリティサービスの活用



外部の情報セキュリティサービスを利用することで、より強固で有効な対策を実施す ることができます。昨今では、様々なサービスが提供されています。情報セキュリティ人材が社内に不足している場合や、情報セキュリティの向上に有用です。



①情報セキュリティコンサルテーション

情報セキュリティ管理の体制や対策に関する総合的に支援するサービスです。セキュリティ関連の適合性評価制度等における認証・認定を支援するサービスもあります。

②情報セキュリティ教育サービス

情報セキュリティに関連する知識やスキルの習得、情報セキュリティ対策の解説や 周知などを支援するサービスです。



③情報セキュリティ監査サービス

情報セキュリティのためのマネジメント（組織内のしくみ）やリスク対策の運用状況を、専門的な立場から、国際的にも整合性のとれた基準に従って検証又は評価し、保証や助

 言を行うサービスです。

④脆弱性診断サービス



システムやソフトウェア等の脆弱性に関して知見のある専門家が、システムや ソフトウェア等に対して次のような診断を行うサービスです。

ア Web アプリケーション脆弱性診断イ プラットフォーム脆弱性診断

より強固にするための方策

ウ スマートフォンアプリケーション脆弱性診断

⑤デジタルフォレンジックサービス

システムやソフトウェア等の不正使用、サービス妨害行為、データの破壊、意図しな い情報の開示等、ならびにそれらの兆候について、法的紛争・訴訟に際し、電磁的記録の証拠保全、調査及び分析を行うとともに、電磁的記録の改ざん及び毀損等について次のような分析及び情報収集等を行うサービスです。

参考情報

ア 機器や記録デバイスを対象とするデジタルフォレンジックによる調査

イ デジタルフォレンジックによる調査に付帯する訴訟支援及び電子証拠開示対応

（ｅディスカバリ）等のサービス

⑥セキュリティ監視・運用サービス



システムやソフトウェア等についての情報セキュリティを確保するための監視及び適切な運用についての次のようなサービスです。

ア マネージドセキュリティサービス（セキュリティインシデント又はその予兆の検知、防御を目的とするものをいう。）



イ セキュリティ監視サービス（セキュリティ製品が出力するログの分析、通知、レポー

ト提供を継続的に提供するものをいう。）

ウ マネージドセキュリティサービスやセキュリティ監視サービスを包含する複合

的なサービス。



**コラム**

情報セキュリティサービス基準審査登録制度

これまで、情報セキュリティ対策製品が所定の機能を備えているかどうかを認証 する制度はありましたが、情報セキュリティサービスを対象とする同様の仕組みは なく、サービスを利用したい企業にとっては、品質の悪いサービスを避けようとす れば、他社に利用経験を尋ねるなどするほかなく、不便な状況が続いていました。そ こで、経済産業省では2018年から「情報セキュリティサービス基準審査登録制度」 を開始し、サービスとして最低限満たすべき品質の水準である「情報セキュリティ サービス基準」を満たしているサービスのリストがIPA から公開されるようになりました。これを使うことで、一定の品質維持向上が図られているサービスを、中小企 業でも簡単に選定し、利用することができます。現在は４分野のサービスに限定さ れていますが、今後の対象分野の拡大についても検討されています。



より強固にするための方策

●情報セキュリティサービス基準適合サービスリスト[https://www.ipa.go.jp/security/it-service/service\_list.html](http://www.ipa.go.jp/security/it-service/service_list.html)

参考情報



* 1. 技術的対策例と活用



コンピュータやインターネットを利用するときに施す技術的対策（製品やソフトウェア） を以下に紹介します。自社の環境に合わせて活用してください。



インターネット

VPN

クラウドサービス

IDS/IPS

サーバ

メール

ウェブ

サーバ

WAF

ファイアウォール

メール

フィ グ

ルタリン

ウイルス対策

ウイルス対策

URL

フィルタリング

ファイル

サーバ

ウイルス対策

ウイルス対策

テレワーク等

ウイルス対策

①ネットワーク脅威対策



より強固にするための方策

ネットワークの境界付近に配置して通信の処理や監視を行い、不正な通信の制御と 管理を行うことで対策を実施します。

●ファイアウォール

通信をさせるかどうかを判断し許可する、または拒否する技術。例えば、インターネットと社内LAN との間に設置して、外部からの不正なアクセスを社内のネットワークに侵入させないようにできます。

参考情報

* IDS（Intrusion Detection System：侵入検知システム）

システムやネットワークに対する不正なアクセスなどを検知して管理者に通知する技術。例えば、インターネットとファイアウォールの間に設置することで、不正アク セスと思われる通信を検知して管理者に通知できます。

* IPS（Intrusion Prevention System：侵入防御システム）

システムやネットワークに対する不正なアクセスなどを検知して自動的に遮断する技術。例えば、インターネットとファイアウォールの間に設置することで、不正アク

* WAF（Web Application Firewall）



ウェブアプリケーションの脆弱性を悪用した攻撃からウェブアプリケーションを保 護する技術。例えばファイアウォールやIDS/IPS とウェブサーバーの間に設置することで、ウェブアプリケーションがやり取りするデータを監視して攻撃を検出できます。



* VPN（Virtual Private Network）

インターネットのような公衆ネットワーク上で、保護された仮想的な専用線環境を 構築する技術。例えば、テレワーク勤務者が職場との間で機密性の高い電子データをやり取りする際に、VPN を利用することで暗号化による安全な通信ができます。

②コンテンツセキュリティ対策

プログラム実行や電子メール送受信、ウェブ閲覧などを、その内容（コンテンツ）によって制御することで対策を実施します。

●ウイルス対策

ウイルスを検知・駆除することで、ウイルスに感染するのを防ぐための対策。例えば、

利用するパソコンにウイルス対策ソフトをインストールしてウイルス定義ファイル

を最新の状態にすることで、既知のウイルスを検知できます。 

●メールフィルタリング



メールの送受信を監視して、指定した条件によって特定の処理を実行する技術。例えば、メールサーバーでフィルタリング機能を設定することで、迷惑メールやウイルスが添付されたメールをブロックできます。

より強固にするための方策

* URLフィルタリング

ウェブサイトへのアクセスや閲覧について、そのアドレスや内容が所定の条件に合 致もしくは違反する場合に停止や警告などを行う技術。例えば、URL フィルタリング機能を持つ機器を導入することにより、業務に関係がないウェブサイトの閲覧を禁 止し、不正サイトへアクセスしてしまうリスクを減らすことができます。

③アクセス管理

情報システムの利用者を、認可及び制限する機能を提供します。

参考情報

●アクセス制御

利用者や情報機器がデータなどにアクセスすることができる権限や認可を制御する技術。例えば、業務で使用するクラウドサービスなどを事務所のみで利用可能とするアクセス制御を行うことで、事務所外からデータへの不正アクセスのリスクを軽減できます。

●多要素認証



サービス利用時に行う利用者認証を、３つの要素（①知っているもの②持っているもの③本人自身に関するもの）のうち、２つ以上の要素を用いて行う技術。例えば、テレワーク勤務者が職場のシステムを利用する際に、ワンタイムパスワードトークンによって生成されたパスワード認証を追加することで、本人からのアクセスに限定するこ



とができます。

●特権ID管理

情報システムの特権（コンピュータを管理するために与えられた最上位の権限）の利用申請や権限付与、操作ログなどを管理する技術。例えば、サイバー攻撃や内部不正 などによる、特権の不正利用を防止し、リスクを軽減することができます。

④システムセキュリティ管理

組織が保有するIT 資産について、一元的な管理や脆弱性を検出する機能を提供します。

* + IT資産管理

パソコンやサーバーなどのハードウェアやソフトウェアの保有状況・構成情報を取りまとめて管理する技術。例えば、IT 資産管理ツールを導入することで、セキュリティパッチの適用状況を把握することができ、脆弱性に対する攻撃のリスクを軽減することが



できます。

●脆弱性検査

サーバーやアプリケーションに対してスキャニングを行い、脆弱性などを検出する ための検査。例えば、サービス提供前のウェブアプリケーションに対して、脆弱性を 検出するためのリクエストを送ることで、既知の脆弱性の有無を点検することがで きます。脆弱性がある場合は、脆弱性があるサーバーやアプリケーションに対し、脆 弱性修正パッチの適用や安全な設定などの対策を速やかに実施することで、攻撃の リスクを軽減することができます。

より強固にするための方策

●ログ管理

サーバー等に誰がログインしたかや、どのデータに対してアクセスがあったかは、サーバー上にログファイルとして記録されます。ログファイルの内容はサーバー等の運 用期間に応じて増えていくので、一定期間（例：１週間、３か月、１年）などの期間で自動的に削除されるように設定されているのが一般的です。サイバー攻撃があった場 合、このログファイルに書かれている内容をもとに、情報漏えいが生じたかどうかを分析するので、ログファイルをどのように管理するかの方針を、組織として定めておくことは重要です。一方で、ログファイルの内容を十分に理解するには専門的な知識が必要となるため、こうした管理を容易にするためのツール類も提供されています。



参考情報

⑤暗号化



データや通信を暗号化することで覗き見（盗聴）、改ざん、漏えいなどを防止する機能を提供します。



●データ暗号化



特定の法則に基づいてデータを変換し、第三者に内容を知られないようにする技術。例えば、サーバー、パソコン、電子媒体をディスクまたはファイル単位で暗号化する ことで、メール送信時の添付ファイルの盗聴、社外からの不正アクセスによるデータ の持ち出し、パソコンや電子媒体の紛失や盗難などによる情報漏えいのリスクを軽 減することができます。

* TLSまたはSSL

インターネット経由でデータの通信を行うとき、データを保護するために用いられ

る暗号化や認証のための技術規格のうち、最も普及しているものの１つです。過去

にSSL（Secure Sockets Layer）として規格化され、現在はTLS（Transport Layer

Security）という名前で国際標準となっていますが、TLS のことを今でもSSL と呼ん

でいる場合もあります。一般的なウェブブラウザはすべて対応しているので、改めて

導入する必要がないメリットがあり、世界的に広く利用されています。 

⑥データの破棄



情報システムを使わなくなった場合、システム内にデータを保存したまま放置したり、破棄したりするとそれが情報漏えいの原因となるため、速やかにデータの消去を行う 必要があります。またクラウドサービスの場合も、不要となったデータをクラウド上に 保存したままにするのは、情報漏えいのリスクを不必要に高めることにつながります。

参考情報

より強固にするための方策

* 1. 詳細リスク分析の実施方法



P.24（３）情報セキュリティ規程の作成では、経営者の懸念事項を踏まえ外部状況と内部状況から一般的に想定されるリスクを特定し、対策を決めていく方法を紹介しました。しかし、事業規模が大きくなったり、情報システムが複雑になると、想定外のリスクを見 落とし、対策が不十分になることがあります。そこでここでは、もれなくリスクを特定し、



対策を検討する手法として「詳細リスク分析」について解説します。詳細リスク分析は、以

下の手順で行います。

**手順１ 情報資産の洗い出し**

**手順２ リスク値の**

**算定**

**手順３ 対策の決定**



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

手順1 情報資産の洗い出し



 業務で利用する電子データや書類を「リスク分析シート」（付録７）の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きの、事業への影響の観点から重要度を判断します。 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、以下の要領で作業を進めます。

●情報資産管理台帳の作成



より強固にするための方策

パソコンのハードディスクや机の引き出しを見るのではなく、日常どのような電子デー タや書類を利用して業務を行っているかを考えて洗い出すと、作成しやすくなります。

●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場合の事業への影響や、法律で安全管理義務が あるなど、表10の評価基準を参考に評価値11２～０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11 の判断基準に従い、重要度を算定します。

参考情報

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、前項の算定結果に関わらず、重要度は２とします。



情報資産管理台帳の記入要領は、本書の47ページの説明を参照してください。

11▲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わか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10】情報資産の機密性・完全性・可用性に基づく重要度の定義



参考情報

より強固にするための方策

|  |  |  |  |
| --- | --- | --- | --- |
| **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） |
| 守秘義務の対象や限定提供データ 12 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** | 漏えいすると業務に大きな  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** | 漏えいしても業務にほとんど影響はない | ●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** | 改ざんされると業務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ほとんど影響はない | ●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ほとんど影響はない | ●廃版製品カタログ |







12▲限定提供データ 不正競争防止法で次のように定義されています。「第二条 ７ この法律において「限定提供データ」とは、業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その他人の知覚によっては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、及び管理されている技術上又は営業上の情報（秘密として管理されているものを除く。）をいう。」

【表11】情報資産の重要度判断基準



|  |  |
| --- | --- |
| **判断基準** | **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** |

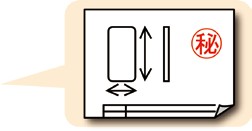
（重要度の判断例）

●『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** |

機密性の２が最大値なので重要度は２

より強固にするための方策

●『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：サーバーの障害など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

参考情報



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



参考情報

より強固にするための方策

付録の利用方法（手順１）



「リスク分析シート」（付録７）は本ガイドラインの手順１～３に示した作業を実施する際のツールです。「手順１」で示した情報資産管理台帳は、「情報資産管理台帳」シートに相当します。記入方法は、「台帳記入例」シートと表12を参考にしてください。



【表12】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** |
| **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。 |
| **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。 |
| **備考** | 必要に応じて説明等を記入します。 |
| **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。 |
| **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。 |
| **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」 |
| **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、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、役職等の属性に関して、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。  **―要配慮個人情報の定義―**  「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り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。 |
| **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１１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。 |
| **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。 |
| **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。 |







記入上のポイント



* 情報資産管理台帳は洗い出した情報資産を「見える化」するための方法の一つです。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。電子化された情報を洗い出すときには「普 段パソコンで見ているこのデータは、どこに保存されているのだろう。」という ように、社内のIT 機器や利用しているクラウドサービスを思い浮かべて記入します。



* 重要度の判断は立場や見識によっても異なることがあるので、記入する前に「重 要ではない」と判断するのではなく、記入した後に組織的に重要度を判断します。
* 電子データや書類を保存する際のまとめ方は様々ですが、管理方法や重要度が 同じ情報は１件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。

【管理方法や重要度が同じ情報の例】

事務所内のパソコンで会計ソフトや表計算ソフトを使って帳簿を作成している場合



* + 仕訳帳
  + 総勘定元帳
  + 現金出納帳

より強固にするための方策

* + 当座預金出納帳
  + 小口現金出納帳
  + 仕訳帳
  + 売上帳

情報資産名称：「会計データ」

「会計データバックアップ」

（バックアップを取っている場合）など媒体・保存先：「事務所 PC」（会計ソフトが保存先）

「可搬電子媒体」

（USB メモリがバックアップ保存先）

* 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。また時間経過に伴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。

参考情報

* 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。







参考情報

**脅威**

**脆弱性**

**× 掛け算**

|  |  |  |
| --- | --- | --- |
|  | **起こりやすさ** | |
| **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** | |
| **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 |

優先的・重点的に対策が必要な情報資産を把握する

手順２ リスク値の算定

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ろいろな方法がありますが、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15）。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13）。

【表13】リスク値の算定基準



算定のしかたは表15参照

より強固にするための方策

|  |  |  |
| --- | --- | --- |
| **重要度** | **情報資産の価値・事故の影響の大きさ** | |
| **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ほとんど影響はない |



|  |  |  |
| --- | --- | --- |
| **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 |

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14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。



【表14】脅威例に応じたリスクのレベル

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 脅威の例 | | 重要度  （a） |  | | 被害発生可能性  （b） |  | |
| 脅威 | 脆弱性 | 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攻撃など不正アクセスによる情報漏えい（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PC 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15】被害発生可能性 換算表



より強固にするための方策

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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

参考情報

付録の利用方法（手順２）



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。

1：通常では発生しな い（数年に 1 回未満）

社内サーバーの故障 による業務に必要な情報の喪失

2：特定の状況で発生する（年に数回程度）

情報搾取目的の社内サーバーでの内部不正

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へのサイバー攻撃

**社内 サーバー**

**媒体・保存先 個別の脅威 脅威の発生頻度（1～3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。



3：実施していない

／わからない

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？

1：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、事務所の施錠をしていますか？

2：一部実施している

業務を行う場所に、第三者が許可なく立入りが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？

**（６）**

**物理的セキュリティ対策**

利用は禁止されていますか？

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・ 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

より強固にするための方策

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

参考情報

* 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）**

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。



リスクの大きな情報資産に対して必要とされる対策を決める

手順３ 情報セキュリティ対策を決定

①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。

②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。

③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やウェブ閲覧に利用せず、USB メモリ、外付けHDD も接続を禁止する、などがあります。

より強固にするための方策

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。

④リスクを移転する

参考情報

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。





参考情報

付録の利用方法（手順 3）



50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  （情報セキュリティ関連規程名称） | 情報セキュリティ関連規程策定の必要性 | 対策状況チェックの診断結果  （対策の実施率） | 付録５  情報セキュリティ関連規程による対策規定の要否 |
| （1）組織的セキュリティ対策 | ◎ | 62.5% | 対策を規定して下さい |
| （2）人的セキュリティ対策 | ◎ | 33.3% | 対策を規定して下さい |
| （3）情報資産管理 | ○ | 14.3% | 対策を規定して下さい |
| （4）アクセス制御及び認証 | ○ | 100.0% | 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。



「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、見舞金など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、不正アクセスなど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、 その他業界団体など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、SECURITY ACTION の宣言や、プライバシーマーク・ISMS などの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。

**コラム**

より強固にするための方策



**コラム**

リスク分析の手法あれこれ

コンピュータやネットワークを利用する時のリスクは、技術的な知識がないと分 かりにくく、見落とすことがありますが、リスクがあることを知らずに対策を怠っ た結果、事故が起きてしまった、ということも多いので、リスク分析を通じて、適切 な対策を導き出す必要があります。

（6）詳細リスク分析の実施方法では、対策の優先順位を判断しやすいように、情報資産の価値と、関連する脅威や脆弱性からリスクを定量的に捉える方法を説明し ています。以下に、広く参照されている「ISO/IEC TR 13335（JIS TR X 0036）ITセキュリティマネジメントのガイドライン」より、４つのリスク分析方法を紹介し ますので、事業やIT 環境に適した手法を選択して活用してください。

①ベースラインアプローチ

既存の標準や基準を参照して対策を検討する方法。

情報資産ごとに「資産価値」「脅威」「脆弱性」を識別しないので、簡単にできる方 法であるが、参照する標準や基準によって、対策のレベルが高すぎたり、低すぎたりする場合がある。

例「）情報セキュリティ5か条「」5分でできる! 情報セキュリティ自社診断」を参照して対策を実施する。

②非形式的アプローチ

より強固にするための方策

組織や担当者の経験や判断によってリスク分析を行い、対策を検討する方法。 短時間に実施することが可能であるが、属人的な判断に偏るおそれがある。 例）システム管理担当者が情報セキュリティに詳しいIT ベンダーにアドバイス

参

考情報

してもらい対策を実施する。

③詳細リスク分析

情報資産ごとに「資産価値」「脅威「脆弱性」を識別し、対策を検討する方法。個々の情報資産に適した対策が可能だが手間がかかる。

参考情報

例）P.43（6）詳細リスク分析の実施方法に従って対策を実施する。

④組合せアプローチ

複数の方法を併用し、それぞれの長所短所を補完する方法。

よく用いられるのは、ベースラインアプローチと詳細リスク分析の組合せ。重 要な情報資産に対する対策とその他の情報資産に対する対策とのバランスが とりやすい。

例）基幹システムに関連する情報資産と個人情報を詳細リスク分析の対象とし て、その他は「5分でできる! 情報セキュリティ自社診断」を参照して対策を実施する。

情報セキュリティに関する参考情報



本ガイドラインを実施するうえで参考となる文献やウェブサイトなどを以下に示します。規格、ガイドラインは改定されますので、適宜に最新版を参照してください。



［1］サイバーセキュリティ経営ガイドライン [Ver.2.0（] 経済産業省/IPA）

大企業及び中小企業（小規模事業者を除く）のうち、IT に関するシステムやサービス等を供給する企業及び経営戦略上IT の利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するため策定された ガイドラインです。 <http://www.meti.go.jp/policy/netsecurity/mng_guide.html>



［2］組織における内部不正防止ガイドライン（IPA）

組織における内部不正を防止するために実施すべき対策として、10の観点（コンプラ イアンス、職場環境など）のもと30項目の対策を提示したガイドラインです。[https://www.ipa.go.jp/security/fy24/reports/insider/](http://www.ipa.go.jp/security/fy24/reports/insider/)

［3］脆弱性対策情報ポータルサイト（IPA/JPCERT コーディネーションセンター）日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供して いる脆弱性対策情報ポータルサイトです。

https://jvn.jp/

［4］JISQ 27001（ISO/IEC 27001）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－要求事項

ISMS（Information Security Management System：情報セキュリティマネジメントシステム）適合性評価制度の認証基準として、要求事項を定めた規格です。

参考情報

※マネジメントシステムとは管理のしくみのことです。

［5］JISQ 27002（ISO/IEC 27002）情報技術－セキュリティ技術－情報セキュリティ管理策の実践のための規範

情報セキュリティ管理策を実施するための手引として用いることを意図して作成された規格です。



※情報セキュリティ管理策とは本ガイドラインでいう情報セキュリティ対策のことです。

［6］JISQ27017（ISO/IEC 27017） 情報技術－セキュリティ技術－ JISQ 27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範 JIS Q 27002を基に、クラウドサービス利用者及びクラウドサービス事業者のための情報セキュリティ管理策の実施を支援する指針を提示した規格です。

［7］情報セキュリティマネジメント試験

情報セキュリティマネジメントの計画・運用・評価・改善を通して組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的なスキルを認定する試験です。[https://www.jitec.ipa.go.jp/1\_11seido/sg.html](http://www.jitec.ipa.go.jp/1_11seido/sg.html)

本書で用いている主な用語の説明



インシデント

リスクが発現・現実化した事象のことをいいます。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いいます。

（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いいます。





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いいます。



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

（情報の）機密性

提供するものをいいます。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。

参考情報

個人情報

①「個人情報」とは、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もの を含む。）」、又は「個人識別符号が含まれるもの」をいう。「個人に関する情報」とは、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。（個人情報保護委員会「個人情報の保 護に関する法律についてのガイドライン（通則編）」）

②「特定個人情報」とは、個人番号をその内容に含む個人情報をいう。（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 ）



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おける定義：「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」をいいます。

②サイバーセキュリティ経営ガイドラインにおける定義：「サイバーセキュリティとは、

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」をいいます。



③ NIST（米国標準技術研究所）における定義：「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」のことをいいます。

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いいます。



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いい、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

など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

参考情報

サイバー保険、サイバーリスク保険などの種類があります。



### おわりに

第2版の公開から約2年が経過し、この度第3版をお届けすることとなりました。この第3版では、「サイバーセキュリティ経営ガイドライン」（経済産業省、IPA）の改訂や、中小企業を取り巻く環境の変化（クラウドサービスなど外部サービスの 利用の増加、ウェブサイトの改ざん被害の増加）へ対応した内容追加を行うとと もに、利用者の皆様からの意見も踏まえ、より解りやすく、より進めやすくなるよう、全面的な見直しを行いました。

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、経営者から「従業員の顔が見える」という有利な条件を備えています。つまり、経営者が直接担当者や従業員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。そうしたなかで 一歩一歩情報セキュリティ対策をすすめていくために、本ガイドラインをご活用いただければ幸いです。

（第3版作成）

中小企業の情報セキュリティ対策ガイドライン改訂に関する研究会 委員

（五十音順、○は委員長）

|  |  |  |
| --- | --- | --- |
| 青山 | 淳 | 全国商工会連合会 組織運営部 部長 |
| ○大木 | 榮二郎 | 工学院大学 名誉教授 |
| 大谷 | 武士 | 全国中小企業団体中央会 総務企画部 部長代理 |
| 小松 | 靖直 | 日本商工会議所 情報化推進部 部長 |
| 下村 | 正洋 | 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 理事／事務局長 |
| 永宮 | 直史 | 特定非営利活動法人日本セキュリティ監査協会 事務局長 |
| 洞田 | 慎一 | 一般社団法人JPCERTコーディネーションセンター |
|  |  | 経営企画室兼早期警戒グループ担当部門長 |
| 松下 | 正夫 | 特定非営利活動法人ITコーディネータ協会 研修制度デザイン部 参与 |

改訂履歴

● 1.0版（2009年3月18日） ● 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

* 3.0版（2019年3月19日）

**はじめましょう情報セキュリティ！**

中小企業の情報セキュリティ対策ガイドライン 第 3 版

2019年3月



〒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 [https://www.ipa.go.jp](http://www.ipa.go.jp/)

電話 03- 5978 -7508 FAX 03 - 5978 -7546

E-Mail [isec-info@ipa.go.jp](mailto:isec-info@ipa.go.jp)

**ウチには秘密なんかないなあ・・・**

**いいえ、こんな情報があるはずですよ！**



**中小企業・小規模事業者の皆様へ**

**情報セキュリティ ５ か条**

* + **従業員のマイナンバー 、住所、給与明細**
  + **お客様や取引先の連絡先一覧**
  + 取引先ごとの仕切り額や取引実績
  + **新製品の設計図などの開発情報**
  + 取引先から“取扱注意”として預かった情報

**サイバー攻撃といっても、被害など知れているのでは？**

**漏れたら大変！ こんなダメージが！**



* **被害者への損害賠償などの支払い**
* **取引停止、顧客流出**
* **ネットの遮断などによる業務効率のダウン**
* **従業員の士気低下**

*情報セキュリティ対策と言っても、何をやれば良いのか分からない組織では、裏面の5か条を守るところから始めてみましよう。*

 **裏面をご覧ください**

**OSやソフトウェアは常に最新の状態にしよう！**

**１**



情報セキュリティ **５** か条

OS やソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、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。

* Windows Update(Windows OS の場合) ／ソフトウェア・アップデート（Mac OS の場合）/OS バージョ

**対策例** 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

#### ウイルス対策ソフトを導入しよう！

**２**

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。

* 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

**対策例** ●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機能を搭載したソフト）の導入を検討する

#### パスワードを強化しよう！

**３**

パスワードが推測や解析されたり、ウェブサービスから流出した ID・パスワードが悪用されたりすることで、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。

* パスワードは英数字記号含めて 10 文字以上にする

**対策例** ●名前、電話番号、誕生日、簡単な英単語などはパスワードに使わない

* 同じ ID・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

#### 共有設定を見直そう！

**４**

データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違ったために、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。無関係な人が、ウェブサービスや機器を使うことができるような設定に なっていないことを確認しましょう。

* ウェブサービスの共有範囲を限定する

**対策例**

* 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**

* lPA 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

セキュリティセンター

IPA セキュリティセンターは誰もが安心、安全な頼れる「IT 社会」を目指して、国民の皆様に情報セキュリティに関する注意喚起や対策情報・対策手段の提供、届出制度や相談窓口を設けるなどセキュアな社会の整備に貢献するための活動を行っています。

[E-mail:isec-info@ipa.go.jp](mailto:isec-info@ipa.go.jp) URL:https://[www.ipa.go.jp/security/](http://www.ipa.go.jp/security/)

**SECURITY ACTION**

セキュリティ対策自己宣言



中小企業自らが情報セキュリティ対策に取り組むことを 自己宣言する制度です。「情報セキュリティ５か条」に取組むことを宣言することで、１段階目「一つ星」を使用 することができます。

URL: https://[www.ipa.go.jp/security/security-action/](http://www.ipa.go.jp/security/security-action/)

2019.3.19 Version 1.2

資料 7

中小企業の情報セキュリティ対策ガイドライン 付録２

情報セキュリティ基本方針（サンプル）

中小企業向けの情報セキュリティ基本方針のサンプルです。必要な項目を選択し、編集することで自社の情報セキュリティ基本方針を作成することができます。

※**赤字箇所**は、自社の事情に応じた内容（役職名、担当者名など）に書き換えてください。

※青**字箇所**は、自社の事情に応じた文言を選択してください。

情報セキュリティ基本方針

株式会社○○○○（以下、当社）は、お客様からお預かりした/当社の/情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組みます。

1. 経営者の責任

当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。

1. 社内体制の整備

当社は、情報セキュリティの維持及び改善のために組織を設置し、情報セキュリティ対策を社内 の正式な規則として定めます。

1. 従業員の取組み

当社の従業員は、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリテ ィへの取り組みを確かなものにします。

1. 法令及び契約上の要求事項の遵守

当社は、情報セキュリティに関わる法令、規制、規範、契約上の義務を遵守するとともに、お客 様の期待に応えます。

1. 違反及び事故への対応

当社は、情報セキュリティに関わる法令違反、契約違反及び事故が発生した場合には適切に対処 し、再発防止に努めます。

発効日:20〇○年○月○日

株式会社○○○○ 代表取締役社長 ○○○○

1

**中小企業・小規模事業者の皆様へ**

**新 ５ 分**

# でできる！

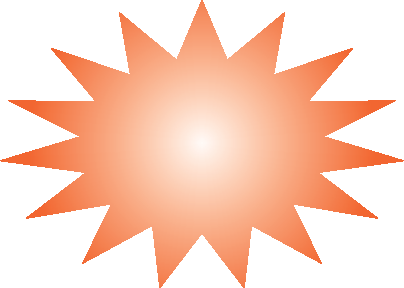
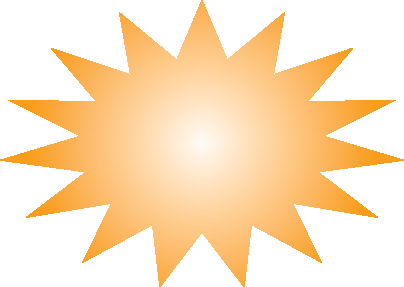
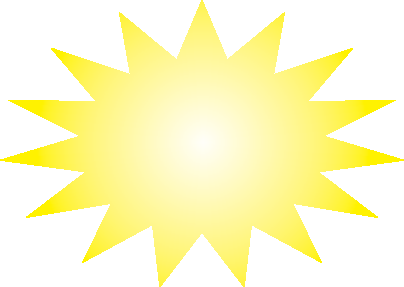
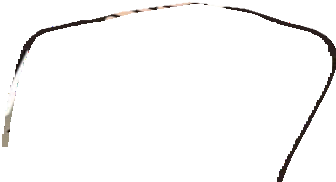
**情報セキュリティ自社診断**

## 最新動向への対応、できてますか？

**脅威や攻撃の変化**

**IT環境の変化**

標的型攻撃



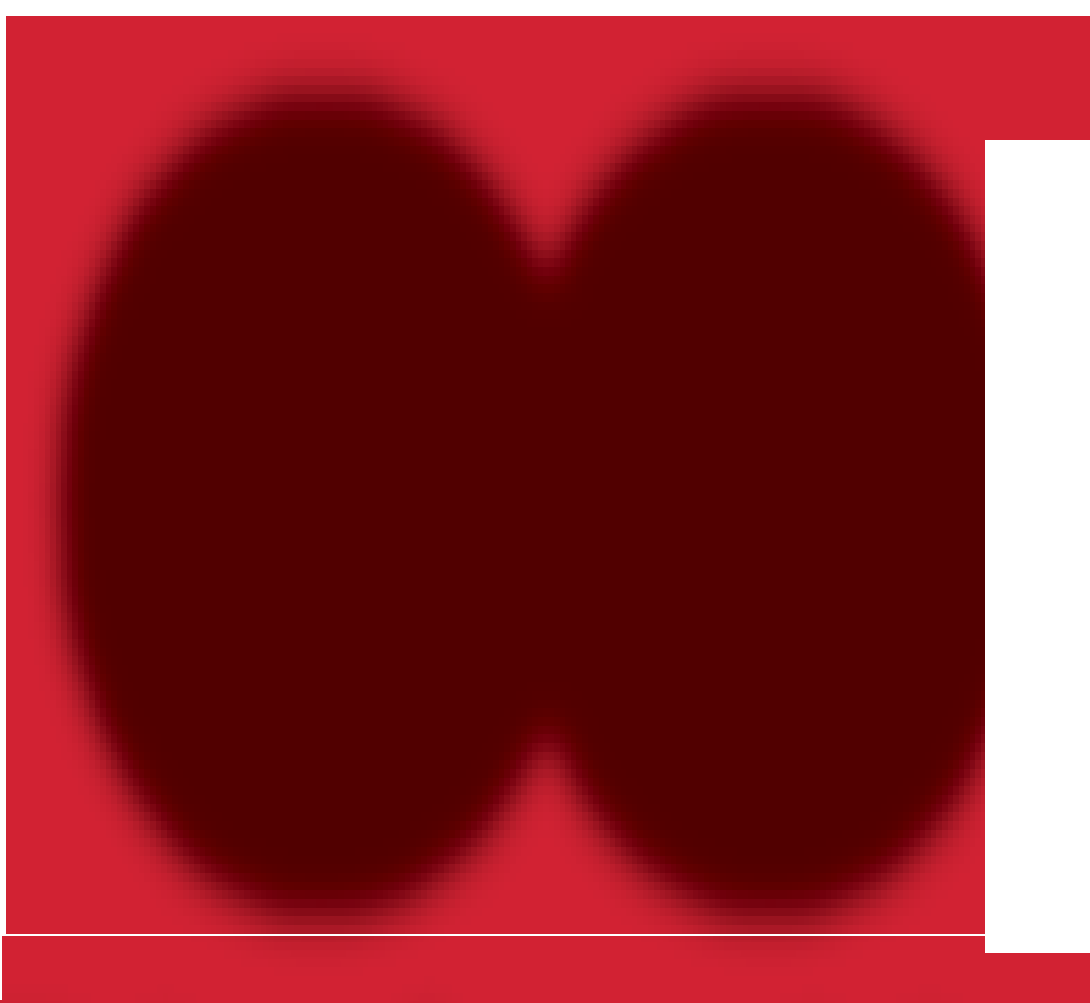
クラウド

ランサムウェア

IoT 機器

パスワードリスト攻撃

スマートフォン



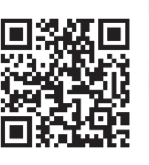
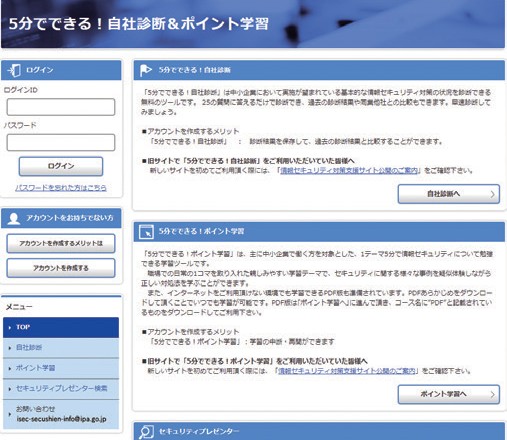
**取り返しのつかないことになる前にあなたの会社のセキュリティ状況を**

**「５分でできる！自社診断」でチェック！**

**使用方法**

診断編（次ページ）25問の質問に回答してください。

情報セキュリティ対策支援サイトでもオンライン診断できます。

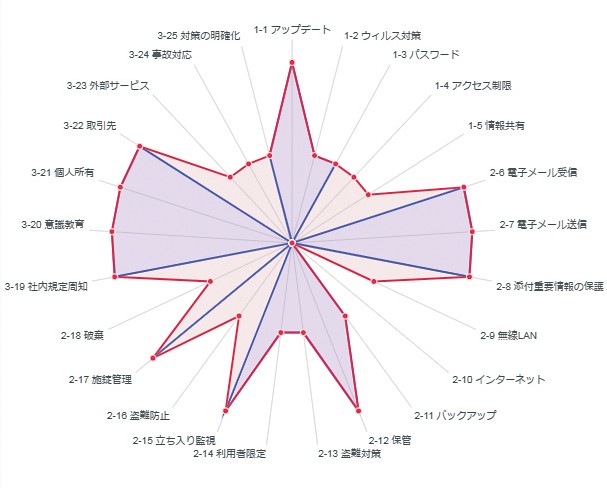


**https://security-shien.ipa.go.jp/learning/**

回答結果をもとに採点し、対策を検討しましょう

|  |  |
| --- | --- |
| 100点満点だった方 | 入門レベルのセキュリティ対策は達成です。ステップアップを検討しましょう。 |
| 70～99点だった方 | ほぼ、出来ていますが、部分的に対策が不十分な点があるようです。 |
| 50～69点だった方 | 対策が行き届いていないところが目立ちます。 |
| 49点以下だった方 | いつ情報流出などの事故が起きても不思議ではありません。 |

|  |
| --- |
| 「中小企業の情報セキュリティ対策ガイドライン」を参照して、情報セキュリティ対策の強化に取り組みましょう。 |
| 小さな隙間から情報が漏えいすることもあります。100 点満点を目指しつつ、「中小企業の情報セキュリティ対策ガイドライン」を参照して対策の強化に取り組みましょう。 |
| 点数が低かった項目について「解説編」を参考に対策を検討し、「情報セキュリティハンドブック」を活用して周知しましょう。 |
| 「解説編」や「対策のしおり」「映像で知る情報セキュリティ」を利用して、分からなかった部分や点数が低かった項目を確認し、対策を施しましょう。 |



**■5分でできる！自社診断 ■5分でできる！ポイント学習 ■普及啓発コンテンツの提供**

25の質問に答えるだけで診断できる 自社診断の質問を1テーマ5分で学べる 講習会や学習用に利用できる資料

中小企業が情報セキュリティ対策を「はじめる」、さらには「強化していく」ことを支援するサイトです。

**情報セキュリティ対策支援サイト**

**https://security-shien.ipa.go.jp/**

2

基本的対策

従業員としての対策

組織としての対策

**診断編**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 診断項目 | No | 診断内容 | チェック | | | |
| 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 |
| Part 1 | 1 | パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態  にしていますか？ | 4 | 2 | 0 | -1 |
| 2 | パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義  ファイル※1 は最新の状態にしていますか？ | 4 | 2 | 0 | -1 |
| 3 | パスワードは破られにくい「長く」「複雑な」パスワードを設定していま  すか？ | 4 | 2 | 0 | -1 |
| 4 | 重要情報※2 に対する適切なアクセス制限を行っていますか？ | 4 | 2 | 0 | -1 |
| 5 | 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできて  いますか？ | 4 | 2 | 0 | -1 |
| Part 2 | 6 | 電子メールの添付ファイルや本文中の URL リンクを介したウイルス  感染に気をつけていますか？ | 4 | 2 | 0 | -1 |
| 7 | 電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していま  すか？ | 4 | 2 | 0 | -1 |
| 8 | 重要情報は電子メール本文に書くのではなく、添付するファイルに書いて  パスワードなどで保護していますか？ | 4 | 2 | 0 | -1 |
| 9 | 無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策  をしていますか？ | 4 | 2 | 0 | -1 |
| 10 | インターネットを介したウイルス感染やSNSへの書き込みなどのトラブル  への対策をしていますか？ | 4 | 2 | 0 | -1 |
| 11 | パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消  失に備えてバックアップを取得していますか？ | 4 | 2 | 0 | -1 |
| 12 | 紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は  机上に放置せず、書庫などに安全に保管していますか？ | 4 | 2 | 0 | -1 |
| 13 | 重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の  対策をしていますか？ | 4 | 2 | 0 | -1 |
| 14 | 離席時にパソコン画面の覗き見や勝手な操作ができないようにしていま  すか？ | 4 | 2 | 0 | -1 |
| 15 | 関係者以外の事務所への立ち入りを制限していますか？ | 4 | 2 | 0 | -1 |
| 16 | 退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をして  いますか？ | 4 | 2 | 0 | -1 |
| 17 | 事務所が無人になる時の施錠忘れ対策を実施していますか？ | 4 | 2 | 0 | -1 |
| 18 | 重要情報が記載された書類や重要なデータが保存された媒体を破棄する  時は、復元できないようにしていますか？ | 4 | 2 | 0 | -1 |
| Part 3 | 19 | 従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏ら  さないなどのルールを守らせていますか？ | 4 | 2 | 0 | -1 |
| 20 | 従業員にセキュリティに関する教育や注意喚起を行なっていますか？ | 4 | 2 | 0 | -1 |
| 21 | 個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確に  していますか？ | 4 | 2 | 0 | -1 |
| 22 | 重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定して  いますか？ | 4 | 2 | 0 | -1 |
| 23 | クラウドサービスやウェブサイトの運用等で利用する外部サービスは、  安全・信頼性を把握して選定していますか？ | 4 | 2 | 0 | -1 |
| 24 | セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順  を作成するなど準備をしていますか？ | 4 | 2 | 0 | -1 |
| 25 | 情報セキュリティ対策（上記 1 ～ 24 など）をルール化し、従業員に明示  していますか？ | 4 | 2 | 0 | -1 |
| ※1 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」とも呼ばれます。  ※2 重要情報とは営業秘密など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。  **診断の後は次ページ以降を読んで対策を検討してください。** | | | A  実施しているの  合計点 | B  一部実施している  の合計点 | C  わからないの合計点 | |
| 点 | 点 | マイナス(－) 点 | |
| **Ａ+B+C**  **合計** | | **点** | |



No.1～5は企業の規模や形態を問わず、必ず対策していただきたい5項目です。いずれも一度やればよいものではなく、継続的な対策実施が欠かせないため、運用ルールとして社内に定着させる必要があります

**基本的対策**

**Part 1**

**Windows Updateを実施する(WindowsOSの場合)、Adobe Flash Player・Adobe Reader・Java実行環境などの利用中のソフトウェアを最新版にするなど。**

対策例

OS やソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、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。

**OSやソフトウェアは常に最新の状態にする**

**脆弱性対策**

**診断編 NO.1**

|  |
| --- |
| **情報セキュリティ対策に役立つツール**  **MyJVNバージョンチェッカ** |
| パソコンにインストールされているソフトウェア 製 品  （ウェブブラウザや動画再生ソフトなど）のバージョンが最新であるかを簡単な操作でチェックできるツールです。MicrosoftのWindows U p da teと併せて、ソフトウェア製品のバージョンアップを行う習慣を身に付けましょう。  「MyJVNバージョンチェッカ」  <http://jvndb.jvn.jp/apis/myjvn/> |

**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の導入を検討す るなど。**

対策例

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。

**ウイルス対策ソフトを導入し適切に利用する**

**ウイルス対策**

**診断編 NO.2**

**パスワードは英数字記号含めて10文字以上にする、名 前、電話番号、誕生日、簡単な英単語などはパスワー ドに使わない、同じID・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など。**

対策例

パスワードが推測や解析されたり、ウェブサービスから流出したID・パスワードが悪用されたりすることで、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。

**強固なパスワードを使用する**

**パスワード管理**

**診断編 NO.3**

**ウェブ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など。**

対策例

データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違ったために、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。無関係 な人が、ウェブサービスや機器を使うことができるよ うな設定になっていないことを確認しましょう。

**共有設定を見直す**

**機器の設定**

**診断編 NO.4**

**lPA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など。**

対策例

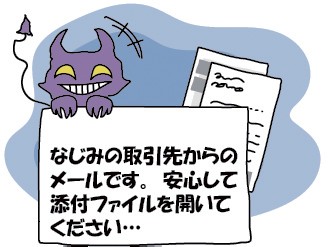
取引先や関係者と偽ってウイルス付のメールを送っ てきたり、正規のウェブサイトに似せた偽サイトを立 ち上げて ID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をと りましょう。

**脅威や攻撃の手口を知り、対策に活かす**

**情報収集**

**診断編 NO.5**

４



No.6～18は従業員として注意すべき項目です。重要情報を日々扱っていると慣れによる人為的ミスが発生しやすくなります。また、脅威の形が日々変化しているので、油断しないように注意する必要があります。

**従業員としての対策**

**Part 2**

|  |  |  |
| --- | --- | --- |
| **診断編 NO.6** | | **電子メールのルール** |
| **身に覚えのない電子メールは疑ってみる** | | |
| 電子メールに添付されたファイルを開いたり、電子メール本文中に記載されたＵＲＬリンクをクリックしたりするこ とでウイルス感染する事故が続いています。身に覚えのない電子メールの添付ファイルやＵＲＬリンクへのアクセ スに気をつけましょう。 | | |
| 対策例 | **不審な電子メールの添付ファイルを安易に開かない、Ｕ ＲＬリンクに安易にアクセスしない、不審な電子メールの情報を社内に共有するなど。** | |

電子メールやFAX の送り先を間違えて、他人に情報が

漏えいしてしまう事故が続いています。電子メールや

FAX は送り先を十分確認するようにしましょう。また、

電子メールアドレスを誤って他人に伝えてしまうことも情

報漏えいになります。複数の送り先に送信する際には、

**電子メールやFAXを送る前に送信先を再確認する、電子メールはＴＯ・ＣＣ・ＢＣＣを使い分けて指定するなど。**

対策例

送り先の指定方法を十分に確認するようにしましょう。

**宛先の送信ミスを防ぐ**

**電子メールのルール**

**診断編 NO.7**

|  |  |  |
| --- | --- | --- |
| **診断編 NO.8** | | **電子メールのルール** |
| **重要情報を送信する時は保護する** | | |
| 重要情報を電子メールで送る場合は、電子メールの本文に書き込まず、文書ファイルなどに記載してパスワードで保護した後、メールに添付します。パスワードはその電子メールには書き込まず、電子メール以外の手段で通知することが必要です。 | | |
| 対策例 | **重要情報は文書ファイルに書いてパスワードで保護す る、パスワードはあらかじめ決めておくか、携帯電話のショートメッセージサービス（SMS）などの別手段で知**  **らせるなど。** | |

|  |  |  |
| --- | --- | --- |
| **診断編 NO.9** | | **無線LANのルール** |
| **無線LANの盗聴や無断使用を防ぐ** | | |
| 適切なセキュリティ設定がされていない無線 LAN は、通信内容を読み取られたり、不正に接続されて犯罪行為に悪用されたりする被害を受ける可能性があります。無線 LAN の盗聴対策や無断使用を防止するようにセキュリティ設定をしましょう。 | | |
| 対策例 | **強固な暗号化方式（WPA2-PSK）を選択する、パスフレーズ（暗号化キー）は長くて推測されにくいものを使用するなど。** | |

|  |  |  |
| --- | --- | --- |
| **診断編 NO.10** | | **インターネット利用のルール** |
| **インターネットを介したトラブルを防ぐ** | | |
| 悪意のあるウェブサイトやセキュリティ上の問題があるウェブサイトを閲覧することでウイルス感染する可能性があります。また、SNS や掲示板へ悪ふざけした画像を投稿したり秘密情報を勝手に掲載して会社に被害を及ぼすことがあります。業務でのインターネット利用を制限する仕組みやルールにより、被害を防止することが必要です。 | | |
| 対策例 | **インターネットの利用ルールを作る、SNSの利用ルールを作る、Webフィルタリング機能を導入することでシステム的にインターネットの利用を制限するなど。** | |

|  |  |  |
| --- | --- | --- |
| **診断編 NO.11** | | **バックアップのルール** |
| **バックアップを励行する** | | |
| 故障や誤操作、ウイルス感染などにより、パソコンや サーバーの中に保存したデータが消えてしまうことがあります。このような不測の事態に備えて、バックアップを取得しておきましょう。 | | |
| 対策例 | **重要情報のバックアップを定期的に行う、バックアップは別の場所に保存するなど。** | |



**机の上をきれいにする、重要書類は鍵付き書庫に保管す るなど。**

対策例

机の上に放置された情報は、誰かに持ち去られたり、盗み見 られたりする危険にさらされています。関係者以外が見たり、触れたりすることができないように、重要情報は放置せず、管理する必要があります。保管場所を定め、作業に必要な場 合のみ持ち出し、終了後に戻すことを励行するようにしま しょう。

**重要情報の放置を禁止する**

**保管のルール**

**診断編 NO.12**

**重要情報の持ち出しは許可制にする、ノートパソコン・スマートフォン・USBメモリなどはパスワードロックをかける、荷物を放置しないなど。**

対策例

重要情報を社外へ持ち出す場合、思わぬ盗難にあったり、うっかり紛失したりすることがあります。ノートパソコンやス マートフォンの利用にあたってパスワードの入力を求めるように設定したり、データファイルを暗号化するなどの対策を事前に行うことで、盗難や紛失の際に情報を簡単に読み取 られることができないようにしましょう。

**重要情報は安全な方法で持ち出す**

**持ち出しのルール**

**診断編 NO.13**

**離席時にパソコンをロックする、退社時にパソコンを シャットダウンし、他人がパソコンを使うことを防ぐなど。**

対策例

パソコンを使用した作業の途中でそのまま席を離れたり、パスワードなしでログインできるパソコンなど、誰でも操作できる状態のパソコンは、不正に使用される可能性があります。不正使用からパソコンを守るための対策を行いましょう。

**機器を勝手に操作させない**

**事務所の安全管理**

**診断編 NO.14**

**事務所で見知らぬ人は事務所に入れない、受付を設置 するなど。**

対策例

関係者以外の事務所への立ち入りを制限しなければ侵入されてしまい、情報を盗み取られる危険性があります。特にサーバーや書庫・金庫など、重要な情報の保管場所の近くには無断で立ち入りができないようにしましょう。

**見知らぬ人には声をかける**

**事務所の安全管理**

**診断編 NO.15**

**退社時に机の上のノートパソコンやタブレット端末、備品**

**（CD、USBメモリ、外付けハードディスクなど）を引き出しにしまうなど。**

対策例

ノートパソコンやタブレット端末、USB メモリなどは手軽に持ち運べる便利さがある反面、盗難や紛失の危険性も高くなっています。利用しない場合は、施錠可能な引き出し等に保管するなどの対策を講じましょう。

**機器・備品の盗難防止対策を行う**

**事務所の安全管理**

**診断編 NO.16**

**鍵の管理を徹底する、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。**

対策例

最終退出者と退出時間の記録を残すことは、最終退出者による施錠の責任意識を向上させることにも役立ちます。施錠と退出記録の管理をしましょう。

**オフィスの戸締まりに気を配る**

**事務所の安全管理**

**診断編 NO.17**

**書類は細断する、電子データは消去ソフトを利用する、 物理的に壊してから処分する、専門業者に消去を依頼するなど。**

対策例

重要情報が記載された書類をゴミ箱にそのまま捨てると、関係者以外の目に触れてしまい、重大な漏えい事故を引き起こすことがあります。また、電子機器・電子媒体に保存された情報は、ファイル削除の操作をしても復元される恐れがあります。重要情報を廃棄する場合は、シュレッダーや消去用ソフトウェアを利用するなど、媒体ごとに適切な処分をしましょう。

**重要情報は復元できないように消去する**

**情報の安全な処分**

**診断編 NO.18**

|  |
| --- |
| **情報セキュリティ対策に役立つツール**  **対策のしおり** |
| 情報セキュリティ上の様々な脅威への対策をテーマ別にわかりやすく解説した小冊子シリーズです。IPA のホームページからダウンロード(PDF) もできます。 |
| 「対策のしおり」  https://[www.ipa.go.jp/security/antivirus/shiori.html](http://www.ipa.go.jp/security/antivirus/shiori.html) |

6





No.19～25は組織としての方針を定めた上で､実施すべき対策です｡情報 セキュリティのルールは明文化して社内で共有することにより､従業員の意識を高めるようにしましょう。

**組織としての対策**

**Part 3**

**採用の際に守秘義務について説明する、守秘に関する覚 書を交わす、秘密としている情報を具体的に示すなど。**

対策例

従業員の守秘義務や機密保持について就業規則などで 定められていることもありますが、どのような情報が秘密なのか、何をしたらいけないのかなどを、従業員に明確に説明しましょう。

**従業員に守秘義務について理解してもらう**

**守秘義務の周知**

**診断編 NO.19**

**情報管理の大切さや関連する法令などを説明する、定期的な研修の機会を設けるなど。**

対策例

日々の仕事では常に様々な情報を取り扱いますが、日常的であるがゆえに管理の意識がつい疎かになりがち です。従業員に対し繰り返し意識付けを行うことが有効です。

**従業員に情報セキュリティ教育を行う**

**従業員教育**

**診断編 NO.20**

**個人所有パソコン、スマートフォンの業務利用を許可制にする、業務利用する場合のルールを決めるなど。**

対策例

個人所有のパソコンやスマートフォンを業務で使用する場合、管理が行き届かず、セキュリティの確保が難しくなります。個人所有端末の業務利用の可否や業務利用の ルールを定めましょう。

**個人所有端末の業務での利用可否を決める**

**私物機器の利用**

**診断編 NO.21**

**秘密保持や具体的な対策を明記した契約や覚書を交わ す、情報セキュリティ対応方針を公表している取引先を選定する、取引先の情報セキュリティ対策を確認するなど。**

対策例

取引先が情報の内容から判断して「当然秘密にしてくれるだろう」という一方的な期待は禁物です。取引先に機 密情報を提供する場合には、それを機密として取り扱ってもらうことを明確にすることが必要です。

**取引先に秘密保持を要請する**

**取引先管理**

**診断編 NO.22**

**利用規約や補償内容、セキュリティ対策などを確認して 事業者を選ぶなど。**

対策例

クラウドサービスなど外部サービスをコスト優先で選んでしまうと障害等でサービスが利用できなくなっても、補償を受けられない場合もあります。外部サービスを利用する場合は、性能や信頼性、補償内容など十分に吟味しましょう。

**信頼できる外部サービスを使う**

**外部サービスの利用**

**診断編 NO.23**

|  |
| --- |
| **情報セキュリティ対策に役立つツール**  **映像で知る情報セキュリティ** |
| 情報セキュリティ上の様々な脅威と対策が学べる映像コンテンツです。10 分前後のドラマやデモンストレーションを通じて情報セキュリティを学べま  す。YouTube「IPA チャンネル」でも公開中です。組織内研修等でご利用ください。 |
| 「映像で知る情報セキュリティ」  https://[www.ipa.go.jp/security/keihatsu/videos/](http://www.ipa.go.jp/security/keihatsu/videos/) |

**重要情報の流出や紛失、盗難があった場合の対応手順書 を作成し、従業員に周知するなど。**

対策例

実際に事故が起きてからだと、冷静に対応する余裕がなくなってしまいます。また、対応が後手に回り、それが原因でさらに深刻な事態になりがちです。報道されるセキュリティ事故などを参考に「もし、同じことが自分の会社で起きた ら・ ・」を想定して、誰がいつ何をするのかをまとめておきましょう。

**事故発生に備えて事前に準備する**

**事故への備え**

**診断編 NO.24**

**情報セキュリティ対策として、診断シート項目のNo.1から24までをルール化して社内で共有する、一度決めた ルールでも問題があれば改善するなど。**

対策例

経営者が情報セキュリティ対策に関する方針を決めていたとしても、それを具体的なルールとして明文化していなければ、従業員は都度経営者の指示を仰がなければなりません。従 業員が自らルールに従って行動できるように、「企業としてのルール」をまとめて明文化し、従業員がいつでも見られるようにしておく必要があります。

**情報セキュリティ対策をルール化する**

**ルールの整備**

**診断編 NO.25**

解説編で例示した対策の前提は以下のとおりです。

■経営者（代表者）が対策方針を直接指示・確認することができる

■従業員全員が顔見知りである

■複雑な設定を必要とするサーバーやネットワーク機器を自社所有していない

・電子メールやのホームページは外部サービスを利用するなどのように、インターネットに直接接続しているサーバーを自社 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、自社で独自に開発したアプリケーションソフトはない

自社診断の後は

社内ルールの周知に取り組もう！



情報セキュリティハンドブック（ひな形） [https://www.ipa.go.jp/security/keihatsu/](http://www.ipa.go.jp/security/keihatsu/) sme/guideline/

の ッ に しの セキュリティルールを実行してもらうためのものです。

でで セキュリティ の に連動しています。

赤字で記載した箇所 記載 です。 のルールにあわせて赤字を中心に編集し 必要に応じて加筆してご利

い。

目 次

1 全社基本ルール 1ページ

仕事中のルール 3ページ

3 全社共通のルール 8ページ

株式会社0000

中小企業の情報セキュリティ対策ガイドライン付録の「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一人ひとりが実施すべき対策の周知に取り組んでください。自社診断で100点満点が取れ るよう組織全体のレベルアップを図りましょう。

Ver 1.4

< 1 >

x禁止

◎必須

OSとソフトウェアのアップデート 自己診断No.1

<OSのアップデート＞

* パソコンのOSはW ndows Updateの自動更新を有効にして最新の更新プログラムをインストールした状態にする。
* 業務に利用するスマートフォンのOSは以下を参考にして手動で更新する。
  + Andro d端末の場合 機種毎の情報を常に調べて必要に応じて対応する。
  + Phoneの場合 Phone本体（W -F を利用）で OSアップデートを行う。

※アップデート後は元のバージョンに戻せないので、事前にデータのバックアップを取得する。

<ソフトウェアのアップデート＞

* W ndowsの更新 に の roso t の更新プログラム 手しインストールした状態にする。
* Adobe Flash Player、Adobe Reader はアップデートを自動に設定する。

ル 対策ソ もアップデ してください。

い い ください。

ウ ル ソフトの 自己診断No.

* 業務で利用する機器には以下のウイルス対策ソフトを導 し、定義ファイルを随更新する。 し用 ートパソコンは利用 に定義ファイルの更新を する。
  + パソコン 0000ウイルス対策ソフト（定義ファイル更新方法 自動）
  + タブレット端末 0000ウイルス対策ソフト（定義ファイル更新方法 自動or手動）

パ ワー の嘗理 自己診断No.3

* ログインやファイル暗号化に使うパスワードは、以下に従って設定・利用する。

基本ル~~ー~~ル

1~~-~~1 全社



SECURITY ACTION 二つ星

[https://www.ipa.go.jp/security/](http://www.ipa.go.jp/security/) security-action/

（基本方針）

* 情報セキュリティポリシー

情報セキュリティ自社診断

* 5分でできる！

「SECURITY ACTION」は中小企業自らが、情報セキュリティ対策に取組むことを自己宣言する制度です。「5分でできる！情報セキュリティ自社診断」を実施し、「情報セキュリティ基本方針」を定め、公開することで２段階目の「二つ星」を使用することができます。

情報セキュリティ対策の取り組みを外部にアピールしよう！

|  |  |
| --- | --- |
| 10文字以上の文字数で構成されている | 名前・愛称・地名・電話番号・生年月日・辞書に載っている単語・よく使われるフレーズは使わない |
| アルファベットの大文字と小文字、数字や「＠」、  「%」、「&」などの記号を組み合わせる | 同じ文字・数字を連ねただけにしない |
| ID・パスワードの使い回しをしない | 者に見えるところに記さない／教えない |



セキュリティセンター

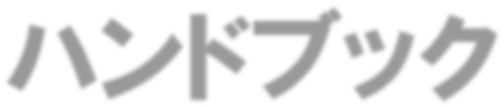
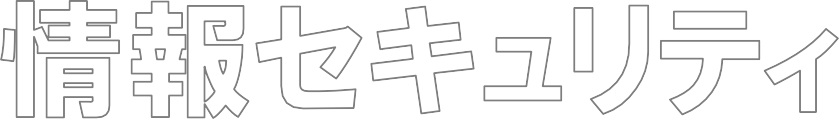
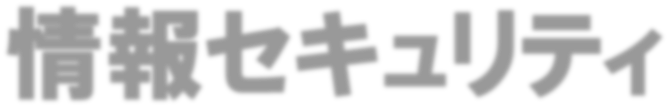
〒113-6591 東京都文京区本駒込二丁目28番8号文京グリーンコートセンターオフィス

TEL: 03-5978-7508 FAX: 03-5978-7546

E-mai[l：isec-info@ipa.go.j](mailto:isec-info@ipa.go.jp)p [URL：https://www.ipa.go.jp/security/](http://www.ipa.go.jp/security/)

2019.3.19 Version 5.0

Ver 1.4



**このハンドブック（ひな形）の使い方**

👉👉 このハンドブック（ひな形）は、従業員に配付し、自社の セキュリティルールを実行してもらうためのものです。

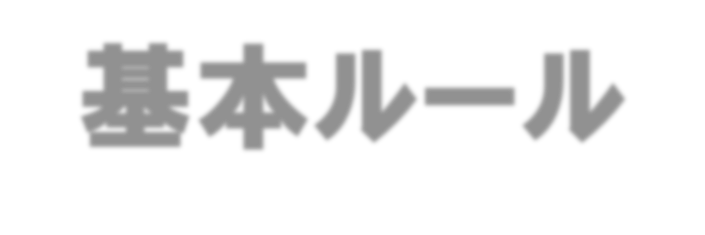
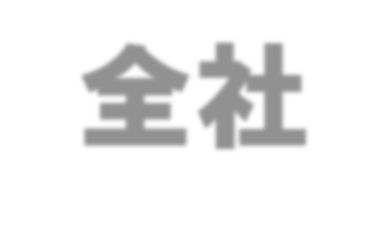
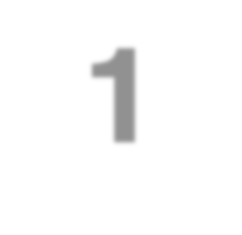
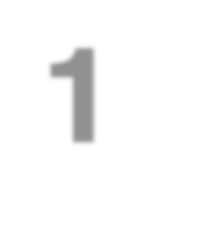
👉👉 ５分でできる！情報セキュリティ自社診断の対策例に連動しています。

👉👉 赤字で記載した箇所は記載例です。自社のルールにあわせて赤字を中心に編集し、必要に応じて加筆してご利用ください。

目 次

|  |  |  |
| --- | --- | --- |
| １ | 全社基本ルール | 1ページ |
| ２ | 仕事中のルール | 3ページ |
| ３ | 全社共通のルール | 8ページ |

株式会社〇〇〇〇



**１-１ 全社基本ルール**

OSとソフトウェアのアップデート

自己診断No.１

＜OSのアップデート＞

* パソコンのOSはWindows Updateの自動更新を有効にして最新の更新プログラムをインストールした状態にする。
* 業務に利用するスマートフォンのOSは以下を参考にして手動で更新する。
  + Android端末の場合：機種毎の情報を常に調べて必要に応じて対応する。
  + iPhoneの場合：iPhone本体（Wi-Fiを利用）でiOSアップデートを行う。

※アップデート後は元のバージョンに戻せないので、事前にデータのバックアップを取得する。

＜ソフトウェアのアップデート＞

* Windowsの更新時に他のMicrosoft製品の更新プログラムも入手しインストールした状態にする。
* Adobe Flash Player、Adobe Reader はアップデートを自動に設定する。

業務でスマートフォンを使う場合は、スマートフォンのOS、ウイルス対策ソフトもアップデートしてください。

やりかたが分からない人は、総務部システム担当までお問い合せください。

ウイルス対策ソフトの導入

* 業務で利用する機器には以下のウイルス対策ソフトを導入し、定義ファイルを随時更新する。持ち出し用ノートパソコンは利用時に定義ファイルの更新を確認する。

自己診断No.２

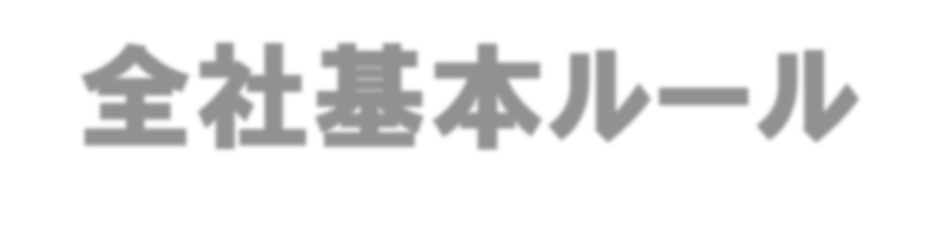
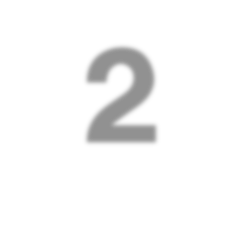
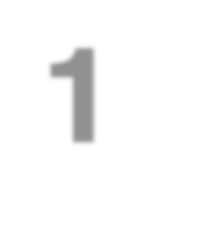
* + パソコン：○○○○ウイルス対策ソフト（定義ファイル更新方法 自動）
  + タブレット端末： ○○○○ウイルス対策ソフト（定義ファイル更新方法 自動or手動）

自己診断No.３

##### パスワードの管理

* ログインやファイル暗号化に使うパスワードは、以下に従って設定・利用する。

|  |  |
| --- | --- |
| **◎必須** | **×禁止** |
| 10文字以上の文字数で構成されている | 名前・愛称・地名・電話番号・生年月日・辞書に載っている単語・よく使われるフレーズは使わない |
| アルファベットの大文字と小文字、数字や「@」、  「%」、「&」などの記号を組み合わせる | 同じ文字・数字を連ねただけにしない |
| ＩＤ・パスワードの使い回しをしない | 他者に見えるところに記さない/教えない |



**１-２ 全社基本ルール**

アクセス制御

自己診断No.４

* 複数名が共有する機器には以下のようにアクセス制御を行う。
* アクセス制限の設定・変更は、総務部システム担当が行う。

|  |  |  |
| --- | --- | --- |
| 機器名 | アクセス制御の方法 | アクセス許可対象者 |
| ○○ファイルサーバー | NAS（ネットワークHDD）  ○○○○ACL | 社長/○○部従業員 |
| 設計図保存サーバー | Windows Active Directory | 社長/技術部従業員 |
| ○○部複合機HDD | 複合機アクセス権設定機能 | 社長/経理部従業員 |
| 本社無線LANルーター | Wi-Fi パスワード設定  WPA2による暗号化 | 社長/取締役/従業員 |

##### セキュリティに対する注意

* 総務部システム担当は毎週月曜日に以下のサイトを参照し、当社で利用するIT製品やサービスに関わる重要なセキュリティ情報、緊急情報などが公表された時には、速やかに社長に報告し、電子メールで対策を全従業員に通知する。

自己診断No.５

* 通知を受けた従業員は速やかに対策を実行する。

👉👉 独立行政法人情報処理推進機構（略称：IPA） 重要なセキュリティ情報

##### https://www.ipa[.](http://www.ipa.go.jp/security/index.html)go.jp/security/

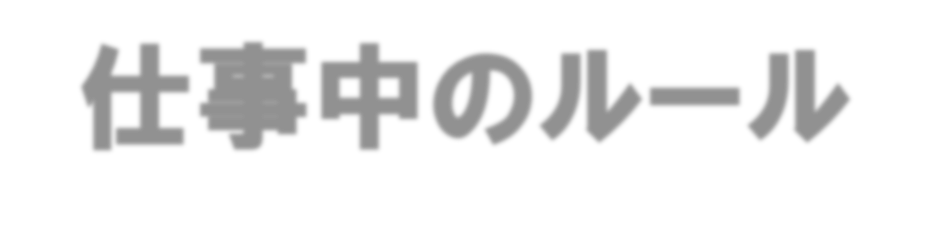
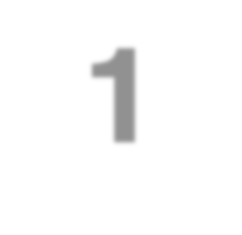
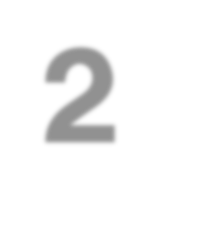
👉👉 JVN （Japan Vulnerability Notes 脆弱性対策情報ポータルサイト）

##### https://jvn.jp/

👉👉 一般社団法人 JPCERT コーディネーションセンター

（略称：JPCERT/CC 技術的な立場における日本の窓口CSIRT）

##### https://[www.jpcert.or.jp/](http://www.jpcert.or.jp/)



**２-１ 仕事中のルール**

電子メールの利用

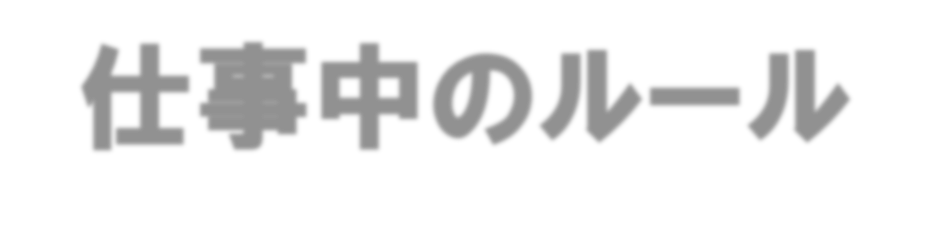
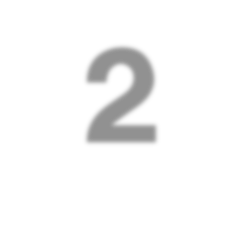
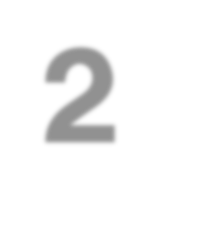
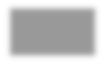
自己診断No. ７・８

* メールソフトを以下のように設定し、宛先のアドレスが間違っていないか確認してから送信する。

（Microsoft Outlookの場合）

* + [ファイル]→[オプション]→[詳細設定]→[送受信]の項目にある「接続したら直ちに送信する」チェックを外す→「OK」
  + 送信トレイに保存されたメールをもう一度確認して「送受信タブ」から[すべてのフォルダーを送受信]をクリックする。
* 複数の外部の人に同時に同じメールを送る場合には、宛先（TO）に自分自身のアドレスを入力し、BCCで複数相手のアドレスを指定する。
* 重要な情報または個人情報を送信する場合は、本文に記入せず、以下の方法で行う。
  + 重要な情報または個人情報を添付ファイルに記載して、パスワードを使用して暗号化、またはパスワード付き圧縮ファイル（ZIP形式）にして暗号化する。
  + パスワードは先方とあらかじめ決めておく、または携帯電話ショートメッセージサービス（SMS）で知らせるなど、パスワードが傍受されないようにする。





**２-２ 仕事中のルール**

電子メールの利用

自己診断No.６

* 標的型攻撃メールによるウイルス感染を防止するため以下の内容に複数合致する場合は十分に注意し、安易に添付ファイルを開いたり、リンクを参照したりしない。
  + **メールのテーマ（件名・見出し）**

①知らない人からのメールだが、メール本文のURLや添付ファイルを開かざるを得ない内容

②心当たりのないメールだが、興味をそそられる内容

③これまで届いたことがない公的機関からのお知らせ

④組織全体への案内

⑤心当たりのない決済や配送通知 （英文の場合が多い）

⑥ID やパスワードなどの入力を要求するメール

* + **差出人のメールアドレス**

①フリーメールアドレスから送信されている

②差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる

* + **メールの本文**

①日本語の言い回しが不自然である

②日本語では使用されない漢字（繁体字、簡体字）が使われている

③実在する名称を一部に含むURL が記載されている

④表示されているURL（アンカーテキスト）と実際のリンク先のURL が異なる（HTML メールの場合）

⑤署名の内容が誤っている

* + **添付ファイル**

①ファイルが添付されている

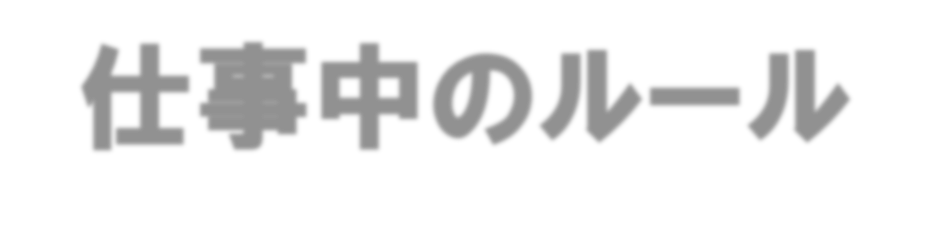
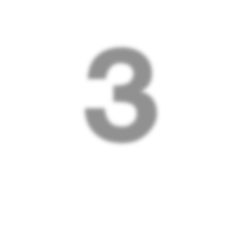
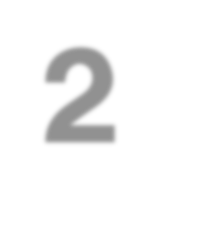
②実行形式ファイル（exe / scr / cpl など）が添付されている

③ショートカットファイル（lnk など）が添付されている

④アイコンが偽装されている

⑤ファイル拡張子が偽装されている





**２-３ 仕事中のルール**

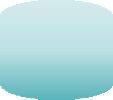
インターネットの利用

自己診断No.１０

* ウェブサイト利用時には以下に注意する。
  + 不審なサイトへのアクセス及び社用メールアドレス登録を禁止する。
  + パスワードをブラウザに保存しない。
* 業務でオンラインストレージサービスを利用する際には以下を順守する。
  + 業務でオンラインストレージサービスを利用する場合は、総務部システム担当の許可を得る。
  + 従業員、もしくは取引先以外との業務関連情報の共有を禁止する。
  + メールアドレスの登録が必要な場合は社用メールアドレスを登録する。
* 業務でSNSを利用する際には以下を順守する。
  + 当社の秘密情報の書き込みは行わない。
  + 取引先従業者とSNS上で私的に交流する場合、双方の立場をわきまえ、社会人として良識の範囲で交流する。
  + セキュリティ設定を行い、アカウントの乗っ取り、なりすましに注意する。
  + 使用するスマートフォン、タブレット端末上のデータ、写真、位置情報が、予期せず公開される可能性のあることに注意する。

##### データのバックアップ

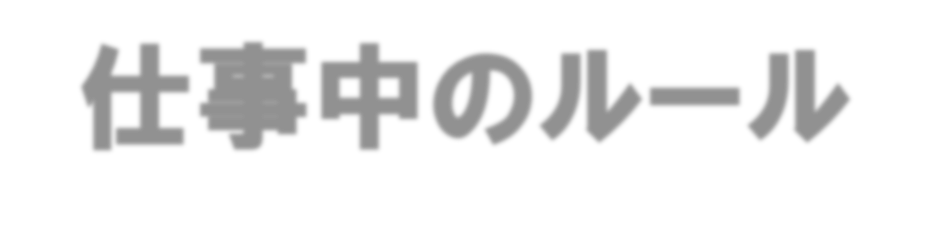
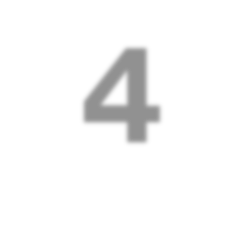
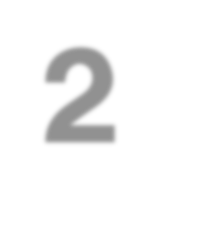
* 重要なデータは以下に指定したサーバーに保存する。



自己診断No.１１

* 重要なデータを保存したサーバーのバックアップは、総務部システム担当が以下の要件に従い取得する。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 機器名 | 対象 | 方法 | 保管媒体 | 頻度 |
| ○○サーバー | システムファイルユーザーファイル | Windows  バックアップ | 外付けHDD | 毎週 |
| 設計図保存サーバー | ファイルバックアップ | ○○同期ツール | 外付けHDD | 毎日 |



**２-４ 仕事中のルール**

クリアデスク・クリアスクリーン

自己診断No.１２・１４

* 重要書類、スマートフォン、携帯電話、重要な情報を保存したUSBメモリ、小型ハードディスク、CD等の電子媒体などを業務利用時以外は机上に放置せず、クリアデス クを徹底する。
* 離席時には以下のいずれかによりパソコンの画面をロックし、クリアスクリーンを徹底する。
  + スクリーンセーバー起動時間を5分以内に設定し、パスワードを設定する。
  + スリープ起動時間を5分以内に設定し、解除時のパスワード保護を設定する。
  + ［Windows］＋［L］キーを押してコンピュータをロックする。
* 退社時、未使用時にはノートパソコン、USBメモリ、小型ハードディスク、CD等の電子媒体及び重要書類を机の引き出しに保管し、施錠する。

自己診断No.１３

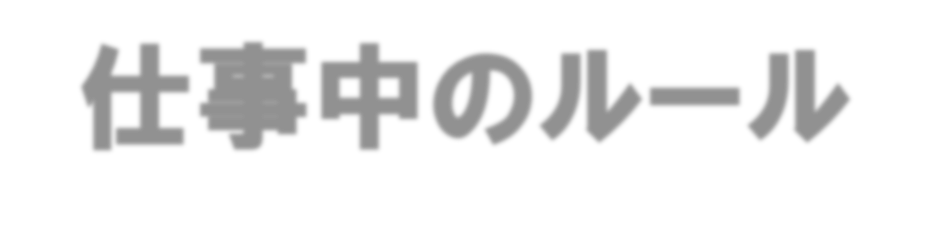
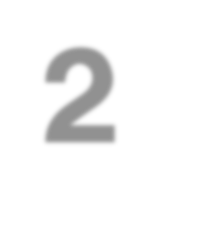
##### 重要情報の持ち出し

* ノートパソコン、タブレット端末、重要な情報を保存したUSBメモリ、小型ハードディスク、CD等の電子媒体及び重要書類を社外に持ち出すときには以下を徹底する。
  + ノートパソコンまたはタブレット端末に保存するデータは必要最小限にする。
  + 電子媒体はケースに入れ、USBメモリはタグ、ストラップ、鈴などを付け紛失を防止する。
  + 書類はひも付き封筒に入れる。
  + ノートパソコンはBIOSパスワードとWindowsログインパスワードを設定する。
  + 電子データはファイル暗号化、またはUSBメモリ暗号化機能により暗号化する。
* 携行時には以下に注意する。
  + 電車内では網棚に置かない。
  + 自動車内に置いたまま車外に出ない。
  + 作業中離席する場合は携行する。
  + 他者が画面を覗き見できない状態で使用する。

##### 重要情報の保管

* 退社時、未使用時にはモバイル用パソコン、USBメモリ、小型ハードディスク、CD 等の電子媒体及び重要書類を机の引き出しまたは所定のキャビネットに保管し、施錠する。

自己診断No.１２



**２-５ 仕事中のルール**

入退室

自己診断No.１７

* 取引先または関係者以外が入室した場合、発見者は声をかけ用件を確認する。
* 最終退室者は以下を行う。
  + 全員のパソコンがシャットダウンされ、プリンターなど周辺機器、暖房器具、湯沸かし器など発熱機器の電源が切られているか確認する。
  + 全ての出入口の施錠を確認する。
  + 退室時刻と退室者氏名を所定様式に記録する。

自己診断No.１８

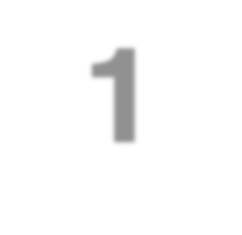
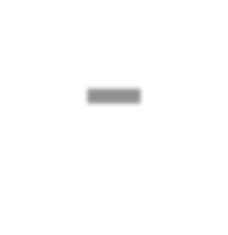
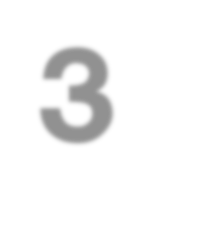
##### 電子媒体・書類の廃棄

* 電子媒体または重要書類の廃棄は以下の手順で行う。

|  |  |
| --- | --- |
| 媒体 | 廃棄方法 |
| サーバー・パソコン  ※リース物件返却・売却含む | * 総務部システム担当がハードディスクを取り出し破壊 * 総務部システム担当がデータ抹消ツールにより完全消去 |
| 外付けハードディスク | * 総務部システム担当が破壊 * 総務部システム担当がデータ抹消ツールにより完全消去 |
| CD・DVDなどのディスク | * 利用者がシュレッダーで細断 * 利用者がCDのラベル面、DVDのディスク内面にカッターでキズを入れる |
| USBメモリー | * 総務部システム担当がデータ抹消ツールにより完全消去 |
| 重要書類 | * 利用者がシュレッダーで細断 * 大量の場合は総務部システム担当が溶解処分を専門業者に依頼し、廃棄証明書を取得 |

< 7 >





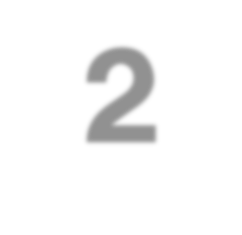
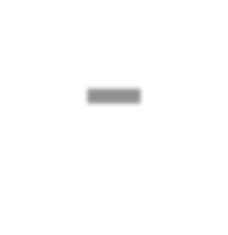
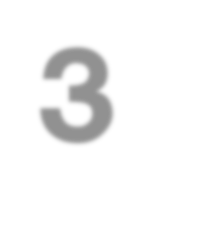
**３-１ 全社共通のルール**

私有情報機器の利用

自己診断No.２１

* 私有の情報機器を業務で利用する場合は以下を順守する。

|  |  |
| --- | --- |
| **情報機器の種類** | **順守事項** |
| パソコン  ※自宅のパソコンで業務を行う場合も含む | * 社内へ無断で持ち込むことを禁止する * 業務利用を禁止する * 社内LANへの接続を禁止する * ウイルス対策ソフト、アプリケーションソフトは総務部システム担当が指定したものを導入し、許可を得たうえで利用する * 業務終了後に業務用データは総務部システム担当の指定するツールで完全に消去する * 従業員個人のメールアドレスに業務用データを添付して送信することを禁止する * 社用メールアドレスで受信したメールを従業員個人のアドレスに転送することを禁止する |
| スマートフォンタブレット端末携帯電話など記憶・通信機能を備えた機器 | * 会社で貸与した機器を利用する * 地図検索、路線案内を除き業務利用を禁止する * 充電を除き、社内パソコンへの接続を禁止する * ウイルス対策ソフト、アプリケーションソフトのインストールは総務部システム担当が指定したものを導入し、許可を得たうえで利用する * 取引先アドレスを除く業務用データの保存を禁止する。 * 従業員個人のメールアドレスに業務用データを添付して送信することを禁止する * 社用メールアドレスで受信したメールを従業員個人のアドレスに転送することを禁止する |
| USBメモリ  外付けHDDなどの記憶機能を備えた機器・媒体 | * 会社で貸与した機器を利用する * 私有物の利用を禁止する * 総務部システム担当の許可を得て利用する * 業務終了後に業務用データは総務部システム担当の指定するツールで完全に消去する |



**３-２ 全社共通のルール**

クラウドサービスの利用

自己診断No.２３

* クラウドサービスを新たに利用する必要がある場合は以下を入手し、総務部システム担当の許可を得たうえで利用する。
  + サービス提供者が公表する情報セキュリティ方針、プライバシーポリシーなど
  + サービス提供者の情報セキュリティ上の責任範囲を定めたサービス利用規約など
  + サービスにあらかじめまたはオプションで付随する情報セキュリティに関する機能やサービスについて明記したもの
  + サービス提供者が情報セキュリティに関わる適合性評価制度の認証を取得している場合はその証拠となるもの
  + 専門家による監査を実施している場合はその証拠となるもの

＜参考＞※カッコ内は運営組織

情報セキュリティ対策への取組み自己宣言制度

* SECURITY ACTION制度（IPA）

適合性評価制度

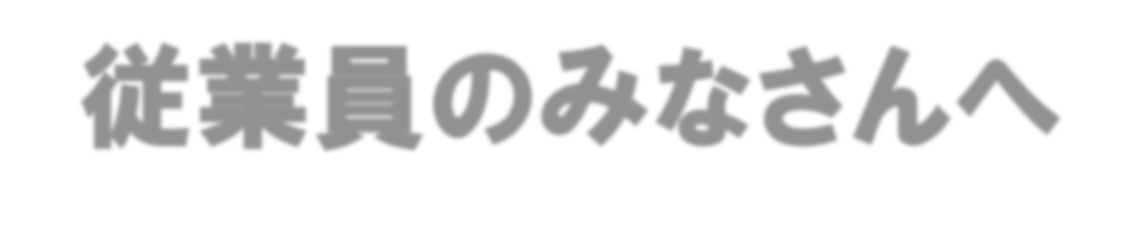
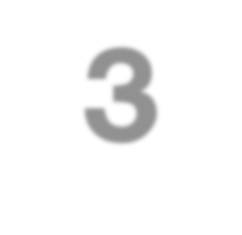
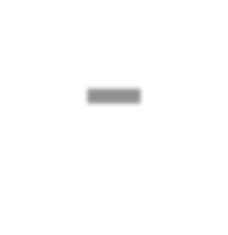
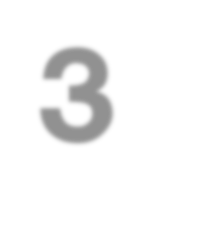
* ISMS適合性評価制度（JIPDEC/JAB）
* プライバシーマーク制度（JIPDEC）
* PCI DSS（クレジットカード業界セキュリティ基準）
* クラウドサービスの安全･信頼性に係る情報開示認定制度（ASPIC）
* インターネット接続安全安心マーク（インターネット接続サービス安全・安心マーク推進協議会）
* TRUSTe（JPAC）

独立かつ専門的知識を持った者に対して情報セキュリティ対策の評価を依頼する制度

* 情報セキュリティ監査制度（経済産業省/JASA）



< 9 >



**３-３ 従業員のみなさんへ**

従業員の守秘義務

自己診断No.１９

* 従業員には当社の就業規則で定められた守秘義務があります。規則を順守し、このハンドブックに定められたルールを守り、情報セキュリティの事故を防ぎましょう。

##### 事故が起きてしまったら

自己診断No.２４

* もしも事故が起きてしまったら、以下の手順に従い、二次被害や事故の影響を最小限に止めましょう。
* 情報セキュリティ事故の定義は以下とします。
  + 情報の「漏えい」「改ざん」の発生または「利用できない」状態になったときに

当社の業務や顧客、取引先、株主、本人（個人情報の場合）に望ましくない影響が及ぶ

１．発見者は社長または総務部システム担当に速やかに連絡する。

**※夜間休日を問いません**

社長携帯電話：090-○○○○-○○○○ 社長内線電話： ○○○○

総務部システム担当携帯電話：090- ○○○○-○○○○ 総務部システム担当内線電話： ○○○○

２．社長/総務部システム担当は以下を実行する。

＜情報漏えい＞

①漏えいした情報の確認

②影響範囲の全ての組織及び本人（個人情報の場合）に事実を報告影響範囲の全ての組織及び本人（個人情報の場合）に対策案を通知

＜改ざん、利用できない状態＞

①原因の調査

②影響範囲の全ての組織及び本人（個人情報の場合）に事実を報告復旧策を実施後、影響範囲の全ての組織及び本人に報告

中小企業の情報セキュリティ対策ガイドライン 付録５

##### 情報セキュリティ関連規程（サンプル）

中小企業向けの情報セキュリティ関連規程のサンプルです。必要な対策を選択し、編集することで自社の情報セキュリティ関連規程を作成することができます。

※**赤字箇所**は、自社の事情に応じた内容（役職名、担当者名など）に書き換えてください。

※青**字箇所**は、自社の事情に応じた文言を選択してください。

**目 次**

|  |  |  |
| --- | --- | --- |
| **1** | 組織的対策 | 1 ページ |
| **2** | 人的対策 | 3 ページ |
| **3** | 情報資産管理 | 5 ページ |
| **4** | アクセス制御及び認証 | 8 ページ |
| **5** | 物理的対策 | 11 ページ |
| **6** | ＩＴ機器利用 | 13 ページ |
| **7** | ＩＴ基盤運用管理 | 21 ページ |
| **8** | システム開発及び保守 | 25 ページ |
| **9** | 委託管理 | 27 ページ |
| **10** | 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 | 34 ページ |
| **11** | 社内体制図 | 39 ページ |
| **12** | 個人番号及び特定個人情報の取り扱い | 40 ページ |

（Ver.1.5）

監査・点検責任者

特定個人情報事務取扱担当者

特定個人情報事務取扱責任者

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | 組織的対策 | 改訂日 | 20yy.mm.dd |
| 適用範囲 | 全社・全従業員 | | |

* 1. 情報セキュリティのための組織

情報セキュリティ対策活動を推進するための組織として、情報セキュリティ委員会を設置する。 情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

|  |  |
| --- | --- |
| 情報セキュリティ委員会 | |
| 情報セキュリティ責任者 | 代表取締役 |
| 情報セキュリティ 部門責任者 | 各部長 |
| システム管理者 | 総務部長 |
| 教育責任者 | 人事部長 |
| インシデント対応責任者  個人情報 苦情対応責任者 | ○○○○部長 |
| 監査・点検/点検 責任者 | ○○○○課長 |
| 特定個人情報 事務取扱責任者 | 代表取締役 |
| 特定個人情報 事務取扱担当者 | 総務部長 |

体制図を下図に示す。組織の変更があった場合は、情報セキュリティ責任者が本体制図の更新を 行う。

・インシデント対応責任者

・個人情報

苦情対応責任者

教育責任者

システム管理者

最高

情報セキュリティ責任者

代表取締役

情報セキュリティ部門責任者

○○部長

△△部長

□□部長

* 1. 情報セキュリティ取組みの監査・点検/点検

監査・点検/点検責任者は、情報セキュリティ関連規程の実施状況について、○月に点検を行い、 監査・点検/点検結果を情報セキュリティ委員会に報告する。情報セキュリティ委員会は、報告 に基づき、以下の点を考慮し、必要に応じて改善計画を立案する。

* + - 情報セキュリティ関連規程が有効に実施されていない場合、その原因の特定と改善
    - 情報セキュリティ関連規程に定められたルールが、新たな脅威に対する対策として有効でな い場合は、情報セキュリティ関連規程の改訂
    - 情報セキュリティ関連規程に定められたルールが、関連法令や取引先の情報セキュリティに 対する要求を満たしていない場合は、情報セキュリティ関連規程の改訂
  1. 情報セキュリティに関する情報共有

情報セキュリティ責任者は、新たな脅威及び脆弱性に関する警戒情報及び個人情報の保護に関す る情報を専門機関等から適時に入手し、委員会で共有する。

【専門機関】

* + - 独立行政法人情報処理推進機構（略称：IPA） [情報セキュリティ] <https://www.ipa.go.jp/security/>

[ここからセキュリティ] https:/[/www.ipa.go.jp/security/kokokara/](http://www.ipa.go.jp/security/kokokara/)

* + - JVN（Japan Vulnerability Notes） https://jvn.jp/index.html
    - 一般社団法人 JPCERT コーディネーションセンター（略称：JPCERT/CC）

https:/[/www.jpcert.or.jp](http://www.jpcert.or.jp/)/

* + - 個人情報保護委員会

<http://www.ppc.go.jp/>

|  |  |  |  |
| --- | --- | --- | --- |
| **２** | 人的対策 | 改訂日 | 20yy.mm.dd |
| 適用範囲 | 全従業員（役員、社員、派遣社員、パート・アルバイトを含む） | | |

1. 雇用条件

従業員を雇用する際には秘密保持契約を締結する。

1. 取締役及び従業員の責務

取締役及び従業員は、以下を順守する。

* 取締役及び従業員は、当社が営業秘密として管理する情報及びその複製物の一切を許可されて いない組織、人に提供してはならない。
* 取締役及び従業員は、当社の情報セキュリティ方針及び関連規程を遵守する。違反時の懲戒に ついては就業規則に従い対処する。

※当社が営業秘密として管理する情報とは、「情報資産管理台帳」の機密性評価値が 1 以上のものをいう

1. 雇用の終了

* 取締役及び従業員は、在職中に交付された業務に関連する資料、個人情報、顧客・取引先から 当社が交付を受けた資料又はそれらの複製物の一切を退職時に返還する。
* 取締役及び従業員は、在職中に知り得た当社の営業秘密もしくは業務遂行上知り得た技術的機 密を利用して、競合的あるいは競業的行為を行ってはならない。

1. 情報セキュリティ教育

教育責任者は、以下の点を考慮し、情報セキュリティに関する教育計画を年度単位で立案する。 対象者：全従業員、派遣社員、パート・アルバイト

テーマ：以下は必須とする。

* 情報セキュリティ関連規程の説明（入社時、就業時）
* 最新の脅威に対する注意喚起（随時）
* 関連法令の理解（関連法令の施行時）
* 特定個人情報の取り扱いに関する留意事項

1. 人材育成

教育責任者は、以下に挙げる推奨資格の取得による従業員の情報セキュリティに対する意識向上 を年度単位で計画する。計画には関連テキストの配付、公開セミナーへの派遣、受験費用の予算 化を含むこととする。

＜情報セキュリティに関わる推奨資格＞

IPA 情報処理技術者試験・情報処理安全確保支援士試験

* 情報セキュリティマネジメント試験
* システム監査技術者試験
* 情報処理安全確保支援士試験

|  |  |  |  |
| --- | --- | --- | --- |
| **3** | 情報資産管理 | 改訂日 | 20yy.mm.dd |
| 適用範囲 | 全社・全従業員 | | |

1. 情報資産の管理
   1. 情報資産の特定と重要度の評価

当社事業に必要で価値がある情報及び個人情報（以下「情報資産」という）を特定し、「情報資産管理台帳」に記載する。情報資産の機密性における重要度は、以下の基準に従って評価する。

|  |  |
| --- | --- |
| 機密性 2：極秘 | * 法律で安全管理措置が義務付けられている * 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 |
| 機密性 1：社外秘 | * 漏えいすると事業に大きな影響がある |
| 機密性 0：公開 | 漏えいしても事業に影響はない |

* 1. 情報資産の分類と表示

情報資産の重要度は以下の方法で表示する。

* 電子データ：保存先サーバーのフォルダー名に重要度を明示
* 書類：保管先キャビネット、ファイル、バインダーに重要度を明示

表示が困難な場合は、「情報資産管理台帳」に機密性評価値を明記する。

* 1. 情報資産の管理責任者

情報資産の管理責任者は、当該情報資産を保有する部門長とする。

* 1. 情報資産の利用者

情報資産の利用を許可する範囲は、「情報資産管理台帳」の利用者範囲欄に部署名又は担当者名 を記載する。

1. 情報資産の社外持ち出し

情報資産を社外に持ち出す場合には、以下を実施する。

* 社外秘の場合は所属部門長の許可を得る。
* 極秘の場合は代表取締役の許可を得る。
* ノートパソコンのハードディスクに保存して持ち出す場合は、ハードディスク/フォルダー/デ ータを暗号化する。
* スマートフォン、タブレットに保存して持ち出す場合は、セキュリティロックを設定する。
* USB メモリ、HDD 等の電子媒体に保存して持ち出す場合は、不要データは全て完全消去専用ツールで消去し、持ち出すデータを暗号化する。
* USB メモリ等の小型電子媒体は、大きなタグを付ける/ストラップで体やカバンに固定する/落としてもすぐに分かるように鈴を付ける。
* 屋外でネットワークへ接続して社外秘又は極秘の情報資産を送受信する場合は、暗号化通信で 行う。
* 携行中は常に監視可能な距離を保つ。

1. 媒体の処分
   1. 媒体の廃棄

社外秘又は極秘の情報資産を廃棄する場合は以下の処分を行う。

|  |  |
| --- | --- |
| 書類・フィルム | 細断/溶解/焼却 |
| USB メモリ・HDD・CD・DVD | 破壊/細断/完全消去 ※OS の削除・フォーマットは不可 |

* 1. 媒体の再利用

社外秘又は極秘の情報資産を保存した媒体を再利用する場合は、以下の処分を行う。

|  |  |
| --- | --- |
| 書類 | 裏紙再利用禁止 |
| USB メモリ・HDD・CD-RW ディ  スク・DVD-RW ディスク | 完全消去後再利用  ※OS の削除機能による削除・フォーマットは不可 |
| CD-R・DVD-R | 再利用不可 |

1. バックアップ
   1. バックアップ取得対象

システム管理者は、以下の機器で処理するデータのバックアップを定期的に取得する。

|  |  |  |  |
| --- | --- | --- | --- |
| 機器名 | 対象 | 方法 | 保管先 |
| ファイルサーバー | ユーザーファイル | Windows Server バ  ックアップ | NAS サーバー |
| 給与計算システム | アプリケーションデ  ータ | ファイルコピー | USB メモリ（暗号化  機能付） |
| 会計システム | アプリケーションデ  ータ | アプリケーションバ  ックアップ機能 | クラウドバックアッ  プサービス |
| ○○管理システム | アプリケーションデ  ータ | 同期ツール | 外付け HDD |
| Web サーバー | ホームページ | 同期ツール | NAS サーバー |

* 1. バックアップ媒体の取り扱い

バックアップに利用した機器及び媒体の取り扱いは以下に従う。

＜保管＞

* 小型媒体：施錠付きキャビネットに保管
* NAS サーバー：施錠付きサーバーラックに収納

＜廃棄・再利用＞

* 「3.媒体の処分」に従う
  1. クラウドサービスを利用したバックアップ

クラウドサービスを利用し、外部のサーバーにバックアップを保存する場合は、以下のサービス 要件を確認し、情報セキュリティ責任者の許可を得て導入する。

＜サービス要件＞

* サービス提供者のサービス利用約款、情報セキュリティ方針が、当社の情報セキュリティ関連 規程に適合している。
* 当社事業所がある地域で発生する震災、水害等の影響を受けない地域の施設であること。

|  |  |  |  |
| --- | --- | --- | --- |
| 4 | アクセス制御及び認証 | 改訂日 | 20yy.mm.dd |
| 適用範囲 | 情報資産の利用者及び情報処理施設 | | |

1. アクセス制御方針

社外秘又は極秘の情報資産を扱う情報システム又はサービスに対するアクセス制御は以下の方 針に基づいて運用する。対象となるシステム等は「9.1 アクセス制御対象情報システム及びアクセス制御方法」に記載する。

* 「情報資産管理台帳」の利用者範囲に基づき、利用者の業務・職務に応じた必要最低限のアク セス権を付与する。
* 特定の情報資産へのアクセス権が、同一人物に集中することで発生し得る不正行為等を考慮し、 複数名に分散してアクセス権を付与する。

1. 利用者の認証

社外秘又は極秘の情報資産を扱う社内情報システムは、以下の方針に基づいて利用者の認証を行 う。認証方法等は「9.2 利用者認証方法」を参照のこと。

* 利用者の認証に用いるアカウントは、利用者 1 名につき 1 つを発行する。
* 複数の利用者が共有するアカウントの発行を禁止する。

1. 利用者アカウントの登録

利用者の認証に用いるアカウントは、代表取締役又は情報セキュリティ責任者の承認に基づき登 録する。アカウント名の設定条件は「9.3 利用者アカウント・パスワードの条件」を参照のこと。

1. 利用者アカウントの管理

利用者の認証に用いるアカウントが不要になった場合、システム管理者は、当該アカウントの削 除又は無効化を、当該アカウントが不要になる日の翌日までに実施する。

1. パスワードの設定

利用者の認証に用いるパスワードは、以下に注意して設定する。パスワードの設定条件は、「9.3 利用者アカウント・パスワードの条件」を参照のこと。

* 十分な強度のあるパスワードを用いる。
* 他者に知られないようにする。

1. 従業員以外の者に対する利用者アカウントの発行

当社の取締役又は従業員以外の者にアカウントを発行する場合は、代表取締役又は情報セキュリ

ティ責任者の承認を得たうえで、秘密保持契約を締結する。

1. 機器の識別による認証

社外秘又は極秘の情報資産を扱う情報システムに、ネットワーク接続によりアクセスする際の認 証方式として、機器の識別による認証を用いる。認証方法等は「9.4 機器の認証方法」を参照のこと。

1. 端末のタイムアウト機能

社外秘又は極秘の情報資産を扱う情報システムの端末もしくは情報機器を、アカウントを付与し ていない者が接触可能な場所に設置する場合は、接続時間制限やタイムアウト等機能を利用する。

1. 標準設定等
   1. アクセス制御対象情報システム及びアクセス制御方法

|  |  |
| --- | --- |
| 情報システム・サービス | アクセス制御方法 |
| ファイルサーバー | Windows Active Directory |
| 給与計算システム | アプリケーションのユーザー認証 |
| ○○管理システム | アプリケーションのユーザー認証 |
| メールサーバー（ホスティングサービス） | ホスティングサービスのユーザー認証 |
| Web サーバー（ホスティングサービス） | ホスティングサービスのユーザー認証 |

* 1. 利用者認証方法

|  |  |
| --- | --- |
| 情報システム | 利用者認証方法 |
| ファイルサーバー | Windows ログオン認証：アカウント名・パスワード |
| 給与計算システム | アプリケーションのユーザー認証：ID・パスワード |
| ○○管理システム | アプリケーションのユーザー認証：ID・パスワード |

* 1. 利用者アカウント・パスワードの条件

|  |  |  |
| --- | --- | --- |
|  | 特権アカウント | 一般アカウント |
| アカウント名 | * 推奨：推測困難であるもの   ＜禁止アカウント名＞ WindowsOS：administrator、admin LinuxOS：root   * 1 つの特権アカウント名を2 名以上で共用しない * Guest 用アカウントは無効化する | * 従業員番号 * 従業員コード |
| パスワード | ＜パスワードに使う文字＞ | ＜パスワードに使う文字＞ |

|  |  |  |
| --- | --- | --- |
|  | * 12 文字以上 * 当人の名前、電話番号、誕生日等、他者が推測できるものを使わない * アルファベット大文字･小文字、数字、記号の全てを含む * 辞書に含まれる単純な語を使わない   ＜パスワードの管理＞   * システムにパスワードポリシー設定機能がある場合は本項の条件を設定する * 過去 1 年間に使用したパスワードと同一パスワードを使用しない * ロックアウトのしきい値は 3 回、時間は 6 時間に設定する | * 10 文字以上 * 当人の名前、電話番号、誕生日等、他者が推測できるものを使わない * アルファベット大文字･小文字、数字、記号の全てを含む * 辞書に含まれる単純な語を使わない   ＜パスワードの管理＞   * システムにパスワードポリシー設定機能がある場合は本項の条件を設定する * 過去 1 年間に使用したパスワードと同一パスワードを使用しない * ロックアウトのしきい値は 5 回、時間は 1 時間に設定する |

* 1. 機器の認証方法

|  |  |
| --- | --- |
| MAC アドレス | 受信側のルーターで設定 |
| IP アドレス | 受信側のルーターもしくはサーバー |
| ドメイン名 | 受信側のルーターもしくはサーバー |

|  |  |  |  |
| --- | --- | --- | --- |
| **5** | 物理的対策 | 改訂日 | 20yy.mm.dd |
| 適用範囲 | 全事業所 | | |

1. セキュリティ領域の設定

当社内で扱う情報資産の重要度に応じて社内の領域を区分する。区分した領域内では以下を実施する。

|  |  |
| --- | --- |
| レベル 1 領域 | 本社受付・応接スペース・商談室・倉庫 |
| 利用者 | 従業員、社外関係者、部外者が立ち入り可 |
| 施錠 | 最終退室者による施錠 |
| 設置可能情報機器 | ディスプレイ、プロジェクター、ホワイトボード |
| 制限事項 | 未使用時に社外秘又は極秘の情報資産の放置禁止 |
| 部外者管理 | 従業員の許可を受けて入室可能 |
| 管理記録 | － |
| 侵入検知 | － |
| 来客用名札 | 着用不要 |
| 火災対策 | 火災検知器、消火器設置 |

|  |  |
| --- | --- |
| レベル 2 領域 | 本社執務室・社長室・書庫・工場・営業所 |
| 利用者 | 従業員以外の入室は従業員の許可又はエスコートが必要 |
| 施錠 | 最終退室者による施錠及び警備会社への通報装置作動 |
| 設置可能情報機器 | ディスプレイ、プロジェクター、ホワイトボード、  パソコン、複合機、電話機 |
| 制限事項 | 情報機器・設備の無断操作禁止・無断持出し禁止 |
| 部外者管理 | 従業員/受付守衛/総務部受付の許可を受けて入室可能 |
| 管理記録 | 入退室を所定様式に記録 |
| 侵入検知 | センサーによる警備会社通報 |
| 来客用名札 | 要着用 |
| 火災対策 | スプリンクラー、消火器設置 |

|  |  |
| --- | --- |
| レベル 3 領域 | サーバールーム |
| 利用者 | あらかじめ登録された者 |
| 施錠 | 常時施錠及び警備会社への通報装置作動、鍵の管理責任者 |

|  |  |
| --- | --- |
| 設置可能情報機器 | サーバー、ルーター等のネットワーク機器 |
| 制限事項 | 情報機器・設備の無断操作禁止・無断持出し禁止  スマートフォン、USB メモリ、HDD、CD-R、デジタルカメラその他の情報記憶媒体の無断持込み禁止 |
| 部外者管理 | 保守・点検時等に登録者のエスコート付で入室可能 |
| 管理記録 | 入退室を所定様式に記録、監視カメラによる記録 |
| 侵入検知 | センサーによる警備会社通報 |
| 来客用名札 | 要着用 |
| 火災対策 | 不活性ガス系消火設備、純水ベース消火器、空調設備 |

1. 関連設備の管理

情報機器に関連する設備は以下を設置する。

* サーバーは施錠付き専用ラックに収納する。
* LAN ケーブルは回線盗聴防止のため床下配線とする。

1. セキュリティ領域内注意事項

セキュリティ領域では区分にかかわらず以下の点に注意する。

* 複合機、プリンタに原稿、印刷物を放置しない。
* FAX 送信時には誤送信防止のため宛先を複数回確認する。
* ホワイトボードは利用後に消去する。
* 室内での撮影、録音は禁止する。業務上必要な場合は、情報セキュリティ部門責任者の許可を 得ること。
* 応接室、会議室内及びエレベータ内では会話の盗み聞きを防止するよう配慮する。
* 外線受話時の際に相手が不審な場合は、従業員の個人情報を伝えてはならない。
* 部外者を見かけた場合は用件を確認する。

1. 搬入物の受け渡し

郵便物及び宅配便の受取り・受け渡しは、以下を介して行う。

＜本社＞

* 郵便物：本社施錠ポスト/書留便の場合は総務部
* 宅配便：本社 1 階受付

|  |  |  |  |
| --- | --- | --- | --- |
| **6** | ＩＴ機器利用 | 改訂日 | 20yy.mm.dd |
| 適用範囲 | 業務で利用する情報機器 | | |

1. ソフトウェアの利用
   1. 標準ソフトウェア

業務に利用するパソコンには、当社の標準ソフトウェアを導入する。当社の標準ソフトウェア以 外のソフトウェアを導入する場合は、システム管理者の許可を得たうえで導入する。標準ソフト ウェアは「6.1 標準ソフトウェア」を参照のこと。

* 1. ソフトウェアの利用制限

システム管理者は、利用者の業務に不要な機能をあらかじめ取除いて提供する。従業員は、業務 に不要なシステムユーティリティやインストールされているソフトウェアを利用しない。

＜利用を禁止するソフトウェア＞

* 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をやりとりできるソフトウェア

（ファイル共有ソフト）。

* 不審なベンダーが提供するソフトウェア。
* 正規ライセンスを取得していないソフトウェア。
  1. ソフトウェアのアップデート

従業員は、業務で使用するソフトウェアを最新の状態で利用する。最新の状態で利用する方法は

「6.2 ソフトウェアのアップデート方法」を参照のこと。

* 1. ウイルス対策ソフトウェアの利用
     1. ウイルス検知

従業員は、以下の方法でウイルス検知を行う。

* ネットワーク経由で入手するファイルは、自動検知機能を有効にしてウイルス検知を実施する。
* 電子媒体を用いてファイルの受け渡しを行う場合は、媒体内のファイルにウイルス検知を実施 する。
  + 1. ウイルス対策ソフト定義ファイルの更新

従業員は、パソコン・スマートフォン・タブレットに導入したウイルス対策ソフトウェアの定義ファイルを随時更新する。持ち出し用ノートパソコンは利用時に定義ファイルの更新を確認する。 定義ファイルの更新方法は「6.3 ウイルス対策ソフトウェアの定義ファイルの更新方法」を参照のこと。

* + 1. 社外機器の LAN 接続

当社が管理するパソコン及びサーバー以外の機器を社内 LAN に接続することを禁止する。業務上

必要な場合は、システム管理者の許可を得たうえで、当該機器にインストールされているウイル ス対策ソフトの定義ファイルを最新版に更新し、当該機器のフルスキャンを実行し、ウイルスが 検知されないことを確認してから接続する。

* 1. ウイルス対策の啓発

システム管理者は、適宜ウイルスに関する情報を収集し、重大な被害を与えるウイルスに対して は、対応策及び対応に必要な修正プログラムを社内に公開及び通知する。従業員は、感染防止策 が通知された場合は、速やかに実施完了すること。

1. ＩＴ機器の利用

従業員は、業務に利用するパソコン・タブレット・スマートフォンには、ログインパスワードを 設定する。利用するときには以下を実行する。

* ログインパスワードを他者の目に触れる所に書き記さない。
* 屋外で利用する場合は、他者が画面を盗み見可能な環境で利用しない。
* 退社時又は使用しないときには電源を切り、ノートパソコン・タブレット・スマートフォン・

USB メモリ、HDD、CD 等の電子媒体は施錠保管する。

1. クリアデスク・クリアスクリーン
   1. クリアデスク

従業員は、社外秘又は極秘の書類及び電子データを保存したノートパソコン、USB メモリ、HDD、

CD 等の持ち運び可能な機器や媒体の扱いについて、以下のようにクリアデスクを徹底する。

* 利用時以外には机上に放置しない。
* 離席時に書類を伏せる、引き出しに入れる等する。
* 退社時又は使用しないときには机の引き出しに保管し、施錠する。
  1. クリアスクリーン

従業員は、離席時に以下のいずれかによりパソコンの画面をロックし、クリアスクリーンを徹底 する。

* スクリーンセーバー起動時間を 5 分以内に設定し、パスワードを設定する。
* スリープ起動時間を 5 分以内に設定し、解除時のパスワード保護を設定する。
* 離席時に［Windows］＋［L］キーを押してコンピュータをロックする。
* ログオフ状態ではシステム操作画面は非表示に設定する。退社時又は使用しないときにはパソ コンの電源を切る。
* スマートフォン・タブレットを外出先で利用する場合は、他者が盗み見できる環境で利用しな い。

1. インターネットの利用

従業員は、インターネットを利用する際には以下を遵守する。

* 1. ウェブ閲覧

システム管理者は、ウイルス等の悪意のあるソフトウェアに感染するおそれがあると認められる 有害ウェブサイトは社内周知/ウェブフィルタリングソフトを使用して、従業員の閲覧を制限す る。従業員は、業務でウェブ閲覧を行う場合は以下に注意する。

* 公序良俗に反するサイトへのアクセスを禁止する。
* 不審なサイトへのアクセス及び社用メールアドレス登録を禁止する。
* パスワードをブラウザに保存しない。業務で特定のウェブサービスを利用する場合で、パスワ ードをブラウザに保存する必要があるときはシステム管理者の許可を得る。
* 業務上、個人情報(メールアドレス、氏名、所属等)を入力する場合は、通信の暗号化、接続先 の実在性等を十分に確認したうえで行う。
* 信頼できるサイトから署名付きのモバイルコードをダウンロードする場合を除き、モバイルコ ード(クライアントパソコン側で動作するプログラム)を実行しない。
  1. オンラインサービス

従業員は、インターネットで提供されているサービスを業務で利用する場合は、システム管理者 の許可を得る。利用する際には以下に注意する。

＜インターネットバンキング・電子決済＞

* インターネットバンキングを利用する際には、自分で設定したブックマークや銀行が提供する 専用アプリケーションソフトを用いる。
* 電子決済を利用する際には、SSL/TLS による通信暗号化を採用しているサイトを利用する。
* 電子メールに記載されているリンクや、他のウェブサイト等に設置されているリンクは、偽サ イトへの誘導である可能性があるためアクセスしない。

＜オンラインストレージ＞

* 社外秘又は極秘の情報資産を保存する場合は、システム管理者の許可を得る。
* メールアドレスの登録が必要な場合は社用メールアドレスを登録する。
* セキュリティポリシーを公表していないサービスの利用は禁止する。
* 不審なベンダーが提供しているサービスの利用を禁止する。
  1. ＳＮＳの利用
* 当社の業務に関わる情報の書き込みは行わない。
* 取引先従業者とＳＮＳ上で私的に交流する場合、双方の立場をわきまえ、社会人として良識の 範囲で交流する。
* ＳＮＳ用のアプリケーションが提供するセキュリティ設定を行い、アカウントの乗っ取りやな りすましに注意する。
* 使用するパソコン、スマートフォン、タブレット上のデータ、写真、位置情報が、予期せず公 開される可能性のあることに注意する。
  1. 電子メールの利用

従業員は、業務で電子メールを利用する際には以下を実施する。

＜誤送信防止＞

* 電子メールソフトの即時送信機能を停止する。

＜メールアドレス漏えい防止＞

* 同報メール（外部の多数相手に同時に送信するとき）を送信する場合は、宛先（TO）に自分自 身のアドレスを入力し、BCC で複数相手のアドレスを指定する。

＜傍受による漏えい防止＞

* 社外秘又は極秘の情報資産を送信する場合は、メール本文ではなく添付ファイルに記載し、フ ァイルを暗号化して送信する。

＜添付ファイル暗号化の方法＞

パスワード保護の設定又はパスワード付きの ZIP ファイルにする。/パスワードは先方とあらかじめ決めておくか電話で知らせるなど、パスワードが傍受されないよう配慮する。

＜クラウド型メールの利用＞

* 業務でクラウド型メールを利用する場合は、システム管理者の許可を得る。
* システム管理者から許可されたパソコン以外で、メールサーバーからのメールの取り出し及び エクスポートを禁止する。

＜禁止事項＞

* 業務に支障をきたすおそれがある使用。
* 私用電子メールサーバーへの接続。
* 私用メールアドレスへの転送。
* 受信メールの HTML 表示（テキスト形式に変換して表示）。
* HTML 形式メールの中に含まれる不正なコードを実行しないよう以下を設定する。
* プレビューウィンドウを無効化する。
* モバイルコード実行を無効に設定する。
  1. ウイルス感染の防止

標的型攻撃メール等によるウイルス感染を防止するため、以下の内容に複数合致する場合は十分 に注意し、添付ファイルを開く、又はリンクを参照するなどしない。受信した場合は、システム 管理者に報告し、システム管理者は社内に注意を促す。

|  |  |
| --- | --- |
| メールのテーマ | ①知らない人からのメールだが、メール本文のURL や添付ファイルを開かざるを得ない内容   * 新聞社や出版社からの取材申込や講演依頼 * 就職活動に関する問い合わせや履歴書送付 * 製品やサービスに関する問い合わせ、クレーム * アンケート調査   ②心当たりのないメールだが、興味をそそられる内容 |

|  |  |
| --- | --- |
|  | * 議事録、演説原稿などの内部文書送付 * VIP 訪問に関する情報   ③これまで届いたことがない公的機関からのお知らせ   * 情報セキュリティに関する注意喚起 * インフルエンザ等の感染症流行情報 * 災害情報   ④組織全体への案内   * 人事情報 * 新年度の事業方針 * 資料の再送、差替え   ⑤心当たりのない、決裁や配送通知 (英文の場合が多い)   * 航空券の予約確認 * 荷物の配達通知   ⑥IDやパスワードなどの入力を要求するメール   * メールボックスの容量オーバーの警告 * 銀行からの登録情報確認 |
| 差出人のメールアドレス | ①フリーメールアドレスから送信されている  ②差出人のメールアドレスとメール本文の署名に記載されたメール アドレスが異なる |
| メールの本文 | ①日本語の言い回しが不自然である  ②日本語では使用されない漢字（繁体字、簡体字）が使われている  ③実在する名称を一部に含むURL が記載されている  ④表示されているURL（アンカーテキスト）と実際のリンク先のURL が異なる（HTML メールの場合）  ⑤署名の内容が誤っている   * 組織名や電話番号が実在しない * 電話番号がFAX 番号として記載されている |
| 添付ファイル | ①ファイルが添付されている  ②実行形式ファイル(exe/scr/cplなど)が添付されている  ③ショートカットファイル(lnkなど)が添付されている  ④アイコンが偽装されている   * 実行形式ファイルなのに文書ファイルやフォルダーのアイコンと なっている   ⑤ファイル拡張子が偽装されている   * 二重拡張子となっている * ファイル拡張子の前に大量の空白文字が挿入されている * ファイル名にRLO4が使用されている |

1. 私有ＩＴ機器・電子媒体の利用

従業員個人が所有するパソコン、タブレット、スマートフォン、携帯電話等のＩＴ機器及び USB メモリ、HDD、CD 等の電子媒体を業務で利用する場合は、システム管理者の許可を得る/利用することを禁止する。

*※編集時注意：利用することを禁止する場合は、5.1～5.3 は削除してください。*

* 1. 利用開始時

利用を開始する前に利用する本人が以下を実行する。

* システム管理者が指定するウイルス対策ソフトウェアをインストールし、定義ファイルを更新 する。
* ハードディスク、電子媒体に対してウイルスチェックを行う。
* 業務に支障が出る可能性があるソフトウェアを削除する。
* 当社で契約したサービス以外の Wi-Fi スポットの利用は禁止する。
  1. 利用期間中

利用期間中は、利用するＩＴ機器や電子媒体に以下に該当する機能がある場合には実行する。

* ウイルス対策ソフトウェアの定義ファイルを常に最新版に更新する。
* OS やアプリケーションソフトのアップデートが通知されたら速やかに実施する。
* 社内 LAN へのリモート接続は禁止する/する場合はシステム管理者の許可を得る。

*※編集時注意：接続を禁止する場合は、5.1～5.3 は削除してください。*

* 社外から社内 LAN にリモートで接続する場合は以下を遵守する。
* システム管理者の許可を受け指定された方法で接続する。
* 画面の盗み見、不正操作等を防ぐよう、適切な環境で行う。
* 端末機器から離れる場合は、端末機器を停止するか他者が利用できないようにする。
* リモート接続で利用する端末機器を紛失した場合は、直ちにシステム管理者に連絡し指示に従 う。
* 社用メールアドレスで受信したメールを従業員個人のアドレスに転送することを禁止する。
* 社内で利用したデータを従業員個人のアドレスに送信することを禁止する。
* 社外秘又は極秘の情報資産の保存を禁止する。
* 以下のアプリケーションソフトのインストールと利用を禁止する。
* 機器ベンダーの公式な公開場所（App Store、Google Playなど）以外から提供されるもの
* 不審なベンダーが提供するもの
* 正規ライセンスを取得していない違法なもの
* 会社で契約したサービス社外の Wi-Fi サービスの利用を禁止する。
* 自宅や屋外で利用する場合は以下を遵守する。
* 信頼できる通信回線のみを利用する。
* 機器は原則として勤務時間のみ稼働させる。
* 不審なメールの受信など、情報セキュリティで不安がある場合はシステム管理者に問い合わせ る。
  + 1. 社内での利用

利用期間中にＩＴ機器や電子媒体を社内に持ち込む場合は、システム管理者の許可を得る。社内 で利用する場合は以下を実行する。/ことを禁止する。

*※編集時注意：社内持ち込みを禁止する場合は、以下の箇条を全て削除してください。*

* 社内 LAN への接続は禁止する/する場合はシステム管理者の許可を得る。
* 充電を除き、社内のパソコンやサーバーへの接続は禁止する。
  1. 利用終了時

利用を終了する際には、システム管理者が指定するツールを使用してＩＴ機器業務で利用したデ ータを完全に消去し、復元できない状態にしてシステム管理者の了解を得る。

1. 標準等
   1. 標準ソフトウェア

|  |  |  |  |
| --- | --- | --- | --- |
| 種別 | 名称 | 開発・販売元 | バージョン |
| パソコンＯＳ | Windows | Microsoft | 8.1 以降 |
| オフィス系ソフト | Office | Microsoft | 2013 以降 |
| 電子メール | Outlook | Microsoft | 2013 以降 |
| パソコン用  ウイルス対策 | ○○○○ | ○○社 | Ver.○以降 |
| スマートフォン用  ウイルス対策 | ○○○○ | ○○社 | Ver.○以降 |
| ブラウザ | ○○○○ | ○○社 | Ver.○以降 |
| ○○○○ | ○○○○ | ○○社 | Ver.○以降 |

* 1. ソフトウェアのアップデート方法

|  |  |  |  |
| --- | --- | --- | --- |
| 種別 | 名称 | 開発・販売元 | アップデート方法 |
| パソコンＯＳ | Windows10 | Microsoft | 更新プログラムを自動的に  インストールする を選択する |
| 業務用ソフト | Office2016 | Microsoft | Windows Update の自動更新  機能を有効にする |
| Adobe Reader | Adobe | 自動アップデートを有効に  する。 |

|  |  |  |  |
| --- | --- | --- | --- |
| ブラウザ | ○○○○ | ○○社 | ○○○○ |
| スマートフォンＯＳ | Android | Google | 機種毎の情報を常に調べて  必要に応じて対応する。 |
| iOS | Apple | iOS アップデート |

* 1. ウイルス対策ソフトウェアの定義ファイルの更新方法

|  |  |  |  |
| --- | --- | --- | --- |
| 種別 | 名称 | 開発・販売元 | アップデート方法 |
| パソコン用  ウイルス対策 | ○○○○ | ○○社 | 定義ファイル更新方法を自  動に設定する |
| スマートフォン用  ウイルス対策 | ○○○○ | ○○社 | 定義ファイル更新方法を自  動に設定する |

|  |  |  |  |
| --- | --- | --- | --- |
| **7** | ＩＴ基盤運用管理 | 改訂日 | 20yy.mm.dd |
| 適用範囲 | サーバー・ネットワーク及び周辺機器 | | |

1. 管理体制

システム管理者は、ＩＴ基盤の運用に当たり情報セキュリティ対策を考慮し製品又はサービスを 選択する。ＩＴ基盤の情報セキュリティ対策及び関連仕様は、情報セキュリティ責任者が承認す る。

* 1. ＩＴ基盤の情報セキュリティ対策

ＩＴ基盤の運用の際には以下の技術的情報セキュリティ対策を考慮すること。

* + 1. サーバー機器の情報セキュリティ要件

ＩＴ基盤で利用するサーバー機器に求める情報セキュリティ要件は、システム管理者が決定する。 新規にサーバー機器を導入する場合は、情報セキュリティ要件を満たす製品を選択し、システム管理者の許可を得て導入する。サーバー機器の情報セキュリティ要件は、「6.1 サーバー機器情報セキュリティ要件」を参照のこと。

* + 1. サーバー機器に導入するソフトウェア

ＩＴ基盤で利用するサーバー機器に導入するソフトウェアは、システム管理者が標準ソフトウェアを選定する。新規にソフトウェアを導入する場合は、システム管理者の許可を得て導入する。 標準ソフトウェアは「6.2ＩＴ基盤標準ソフトウェア」を参照のこと。

* + 1. ネットワーク機器の情報セキュリティ要件

ＩＴ基盤で利用するネットワーク機器に求める情報セキュリティ要件は、システム管理者が決定する。新規にネットワーク機器を導入する場合は、情報セキュリティ要件を満たす製品を選択し、 システム管理者の許可を得て導入する。ネットワーク機器の情報セキュリティ要件は、「6.4 ネットワーク機器情報セキュリティ要件」を参照のこと。

1. ＩＴ基盤の運用

システム管理者は、ＩＴ基盤の運用を行う際には以下を実施すること。

* システム管理者は、機器の管理画面にログインするためのパスワードは初期状態のまま使わず、 推測不可能なパスワードを設定して運用する。
* 以下に従い、ゲートウェイにおける通信ログを取得及び保存する。
  + 通信ログの保存期間は 3 年間とする。
  + ログファイルの保存状況について、システム管理者が定期的に確認する。
* システム管理者は、通信ログについて以下の確認を定期的に行う。
  + 管理外のインターネット接続がないか
  + 許可なく接続された機器や無線 LAN 機器はないか
  + 不審な通信が行われていないか
* システム管理者は、必要に応じて業務に不要なウェブサイト閲覧を社内周知/ウェブフィルタ リングソフトを使用して制限する。
* 遠隔診断ポートの利用は、保守サポートなど必要な場合のみに限定し、認証機能やコールバッ ク機能等を備えるなど、適切なセキュリティ対策を施す。

1. クラウドサービスの導入

ＩＴ基盤の一部としてクラウドサービス等の外部サービスを導入する場合は、システム管理者が サービスプロバイダの情報セキュリティ対策をあらかじめ評価したうえで選定する。新規クラウ ドサービス等の外部サービスを導入する場合は、システム管理者の許可を得て導入する。サービ スプロバイダの情報セキュリティ対策の評価基準は「6.5 クラウドサービス情報セキュリティ対策評価基準」を参照のこと。

1. 脅威や攻撃に関する情報の収集

システム管理者は、最新の脅威や攻撃に関する情報収集を行い、必要に応じて社内で共有する。

1. 廃棄・返却・譲渡

システム管理者は、ＩＴ基盤で利用した機器を返却、廃棄、譲渡を行う場合は、内部記憶媒体の破壊又は専用ツールによりデータを完全に消去し、情報セキュリティ責任者の承認を得たうえ返却、廃棄、譲渡を行う。内部記憶媒体の破壊又はデータの完全消去を、外部に委託する場合は、 破壊又はデータの完全消去を実行したことの証明書を取得する。

1. ＩＴ基盤標準

ＩＴ基盤で利用する機器及びソフトウェアの情報セキュリティ要件と、それに基づく当社標準を 以下とする。

* 1. サーバー機器情報セキュリティ要件

|  |  |  |
| --- | --- | --- |
| 対象システム | セキュリティ要件 | 利用技術・製品 |
| ファイルサーバー | 利用者認証機能 | Windows Active Directory |
| セキュリティログ取得機能 | Windows |
| システムログ取得機能 | Windows |
| ユーザーアクセスログ取得機能 | ○○○○ |
| ハードディスク：容量○TB 以上  RAID 構成 | ○○○○ |
| ＮＡＳサーバー | 利用者認証機能 |  |

|  |  |  |
| --- | --- | --- |
|  | ディスク暗号化機能 | ○○○○ |
| ハードディスク：容量○GB 以上 |  |

* 1. ＩＴ基盤標準ソフトウェア

|  |  |  |  |
| --- | --- | --- | --- |
| 種別 | 名称 | 開発・販売元 | バージョン |
| ＯＳ | Windows Server | Microsoft | 2008 以降 |
| ＲＤＢ | ○○SQL | ○○社 | Ver.○以降 |
| ウイルス対策 | ○○○○ | ○○社 | Ver.○以降 |
| ブラウザ | ○○○○ | ○○社 | Ver.○以降 |
| ○○○○ | ○○○○ | ○○社 | Ver.○以降 |

* 1. 標準ネットワーク機器

|  |  |  |  |
| --- | --- | --- | --- |
| 種別 | 名称 | 開発・販売元 | OS バージョン等 |
| ルーター | ○○○○ | ○○社 | Ver.○以降 |
| ファイアウォール | ○○○○ | ○○社 | Ver.○以降 |
| 監視ツール | ○○○○ | ○○社 | Ver.○以降 |
| ○○○○ | ○○○○ | ○○社 | Ver.○以降 |

* 1. ネットワーク機器情報セキュリティ要件

|  |  |  |
| --- | --- | --- |
| 対象システム | セキュリティ要件 | 利用技術・製品 |
| ルーター | 利用者認証機能 | ○○○○ |
| MAC アドレス認証 | ○○○○ |
| 通信ログ取得 | ○○○○ |
| ○○○○ | ○○○○ |
| ○○監視ツール | ユーザーアクセス監視 | ○○○○ |
| ○○○○ | ○○○○ |

* 1. クラウドサービス情報セキュリティ対策評価基準
* サービスプロバイダが公表する情報セキュリティ又は個人情報保護への取組方針が、処理しよ うとする情報資産の重要度に照らして適切であること。
* サービス仕様に含まれる情報セキュリティ対策が、処理しようとする情報資産の重要度に照ら して適切であること。
* 情報セキュリティに関する適合性評価制度の認証・認定を取得していること。

＜適合性評価制度の種類＞

* + ISMS 適合性評価制度（ISMS 認証/ISMS クラウドセキュリティ認証）
  + プライバシーマーク制度
  + PCI DSS（クレジットカード業界セキュリティ基準）
  + ASP・SaaS の安全・信頼性に係る情報開示認定制度
  + インターネット接続安全安心マーク

|  |  |  |  |
| --- | --- | --- | --- |
| **8** | システム開発及び保守 | 改訂日 | 20yy.mm.dd |
| 適用範囲 | 当社が独自に開発する情報システム | | |

1. 情報システムの開発
   1. 新規システム開発・改修

情報システムの開発・改修を行う際には、以下の工程を経て実施する。各工程の完了時にシステ ム管理者の承認を得る。

①対象業務の範囲定義

②ハードウェア・ソフトウェア・ネットワーク機能検討

③必要なパフォーマンスの検討

④情報セキュリティ要件定義

⑤バックアップ/障害復旧要件定義

⑥情報システム運用要件定義

⑦運用体制

⑧移行計画立案

* 1. 脆弱性への対処

情報システムのソフトウェア開発を行う際には、当該情報システムの利用環境に応じて設計時に 技術的な脆弱性を識別し、対策を講じる。脆弱性に対する対策の有効性はシステム管理者が判断 し、承認する。

（参考）IPA 情報セキュリティ 脆弱性対策

https:/[/www.ipa.go.jp/security/vuln/index.html](http://www.ipa.go.jp/security/vuln/index.html)

* 1. 情報システムの開発環境

情報システムの開発及び改修を行う環境は、運用環境とは分離する。新たに情報システムの開発を行った場合や、情報システムの改修を行った場合は、当該情報システムの運用を開始する前に、 必要な情報セキュリティ対策が講じられていることを確認し、システム管理者の承認を得る。

* 1. 情報システムの保守

情報システムの保守を、開発元又は外部の組織に委託することができない場合、以下に挙げる事 項に留意し、情報システムに既知の脆弱性が存在しない状態で運用する。

* 開発時に用いたソフトウェアに関する脆弱性が公表された場合には、速やかにその影響が顕在 化しないための対策を講じる。
* 開発時に用いたソフトウェア及びハードウェアの製造者が提供するサポートが終了した場合、 他のソフトウェアやハードウェアを用いた再構築又は当該情報システムの利用停止を検討し、

システム管理者の承認を得る。

* 1. 情報システムの変更

情報システムのハードウェア又はソフトウェアの変更を行う際には、以下の工程を経て実施する。 各工程の完了時にシステム管理者の承認を得る。

①現行システムの問題・課題の把握

②システム変更計画立案

③システム変更計画書に基づくシステム設計

④セキュリティ要求と設計の見直し

⑤移行計画立案（移行時、運用時の障害対応をあらかじめ検討する。）

⑥変更後の仕様書、操作手順書、運用手順書等の関連文書の作成

|  |  |  |  |
| --- | --- | --- | --- |
| **9** | 委託管理 | 改訂日 | 20yy.mm.dd |
| 適用範囲 | 情報資産を取り扱う業務の委託 | | |

1. 委託先の評価（クラウドサービスの利用を除く）
   1. 委託先評価基準

社外秘又は極秘の情報資産の処理あるいは授受を伴う業務を外部の組織に委託する場合は、委託 先の情報セキュリティ管理について、委託先評価基準に基づいて評価する。

（委託先評価基準）

|  |  |
| --- | --- |
| 社内管理体制 | ①経営者による情報セキュリティ基本方針がある |
| ②情報セキュリティ管理責任者を置いている |
| ③情報セキュリティ対策を定める規定等を整備している |
| ④情報セキュリティ事故に対する対応手順がある |
| 従業員の監督 | ⑤全ての従業者に情報セキュリティに関する教育を実施している |
| ⑥従業者から秘密保持に関わる誓約書等を取得している |
| オフィス内の  セキュリティ | ⑦顧客の情報を扱う領域への入退室を管理している |
| ⑧顧客の情報の保管について施錠管理を実施している |
| 情報機器・ 媒体の取り扱い | ⑨機器・媒体の盗難防止措置を講じている |
| ⑩媒体の無断複製、不正持出しを防止する措置を講じている |
| ⑪媒体の移送、受け渡し時の保護措置を講じている |
| ⑫媒体の安全な消去、廃棄の手順を整備している |
| サーバー・  パソコン等の管理 | ⑬業務で使用するサーバー・パソコンのウイルス対策を行っている |
| ⑭業務で使用するサーバー・パソコンは利用者認証機能を設定している |
| ⑮業務で使用するサーバー・パソコンに利用制限等を設け管理している |

* 1. 委託先の選定

評価結果に基づき委託先を選定し、情報セキュリティ責任者の承認を得る。

* 1. 委託契約の締結

委託契約書には、下記に関する事項を明記する。

①当社の社外秘又は極秘の情報資産及び個人情報の守秘義務

②再委託についての事項

③事故時の責任分担についての事項

④委託業務終了時の当社が提供した社外秘又は極秘の情報資産及び個人情報の返却又は廃棄、 消去についての事項

⑤情報セキュリティ対策の実施状況に関する監査の方法とその権限

⑥契約内容が遵守されない場合の措置

⑦事故発生時の報告方法

*（参考情報：9-1 業務委託契約に係る機密保持条項）*

* 1. 委託先の評価

委託開始後には、1.1 委託先評価基準の委託先における実施状況について定期的に評価する機会を設ける。委託先における評価基準の実施に関して不備又は変更が認められた場合は、双方協議 のうえ、対処を検討し、書面で合意する。

＜委託先評価の方法＞

* 委託先事業所に訪問して現場を観察する。
* 委託先の管理責任者にインタビューする。
* 委託先に書面で確認事項を通知し、実施状況について報告してもらう。

*（参考情報：9-2 委託先情報セキュリティ対策実施状況確認リスト）*

* 1. 再委託

当社が委託する業務を、委託先が他の組織又は個人に再委託する場合には、事前に書面による報告を委託先に求める。報告には必要に応じて以下の提供を含め、当社の「1.1 委託先評価基準」

「1.3 委託契約の締結」「1.4 委託先の評価」と同等の管理を再委託先に求めていることを確認し、情報セキュリティ責任者の承認を得たうえで再委託を認める。

* 委託先と再委託先との契約書案の写し（情報セキュリティに関連する部分のみ）
* 再委託先の選定基準

再委託先が情報セキュリティに関する適合性評価制度の認証・認定を取得している場合にはその 証書の写し

9-1 業務委託契約に係る機密保持条項

注：このサンプルは、業務委託契約書における機密保持に関する条項を示すものです。委託 元（甲）と委託先（乙）との双方が、相手から機密として提供される情報の守秘義務を負う 双務契約の形式としています。

第○条（機密保持）

1. 甲及び乙は、本契約の履行に当たり、相手方が機密である旨指定して開示する情報及び本契約の履行により生じる情報（以下「機密情報」という）を機密として取り扱い、相手方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自ら所有していたもの

③開示を受けた後に自ら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自らが独自に開発したことを証明し得るもの

1. 甲が乙に機密である旨指定して開示する情報は、別表 1（本案では、特に例示しない）、乙が甲に機密である旨指定して開示する情報は、別表 2（本案では、特に例示しない）の通りである。なお、別表 1 及び別表 2 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。
2. 甲及び乙は、相手方より開示された機密情報の管理につき、自ら保有する他の情報、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。
3. 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て保管管理する。
4. 機密情報を取り扱う従業員を必要最小限にとどめ、上記保管場所以外へ持ち出さない。(3)機密情報の管理責任者名、機密情報を取り扱う従業員名及び機密情報に関する情報セキュリティ対策を、○年○月○日までに相手方に報告する。また、報告内容に変更が生じた場合には、速やかに当該変更内容を相手方に報告する。

(4)(3)にて報告した機密情報を取り扱う従業員に対して本契約の内容を周知徹底させ、機密情報の漏洩、紛失、破壊、改ざん等を未然に防止するための措置を取る。

(5)甲の書面による承諾を得た場合を除き、機密情報を複写、複製せず、また、機密情報を開示、漏洩しない。但し、政府機関又は裁判所の命令により要求された場合、その範囲で開示することが出来る。なお、その場合には、相手方にその旨を速やかに通知すること。(6)機密情報は本契約の目的の範囲でのみ使用する。

1. 事故発生時には直ちに相手方に対して通知し、事故再発防止策の協議には相手方の参加を認める。
2. 委託期間満了時又は本契約の解除時、機密情報（(5)に基づく複写、複製を含む）を相手方に返却、又は自己で廃棄の上廃棄の証拠を相手方に報告する。

(9)(8)にかかわらず、相手方から返却また廃棄を求められたときは、機密情報（(5)に基づく複写、複製を含む）を相手方に返却、又は自己で廃棄の上廃棄の証拠を相手方に報告する。(10)甲及び乙は、相手方に対して、機密情報の以下の具体的管理状況に関する報告を求めることができる。この報告結果をもとに、甲及び乙が相手方の事務所における機密情報の管理状況を確認するために相手方の事務所への立入検査を希望する場合には、当該検査に協力する。また、甲及び乙は相手方に対して是正措置を求めることができ、相手方はこれを実施するものとする。

①委託契約範囲外の加工、利用の禁止の遵守

②委託契約範囲外の複写、複製の禁止の遵守

③情報セキュリティ対策状況

第○条（再委託）

1. 乙は、本業務（の全部、又は一部）を第三者へ再委託する場合、甲の事前の書面による同意を得ずに、再委託してはならない。
2. 前項の規定に基づき本業務を再委託する場合、乙は自己が負う義務と同等の義務を再委託先に対して書面にて課すとともに、甲に対して再委託先に当該義務を課した旨を書面により報告し、かつ乙は当該機密情報開示に伴う全責任を負うものとする。また、乙は次項第 3 号の再委託先からの報告を、第○条（機密保持）第３項の具体的管理状況の報告時にあわせて甲に報告する。
3. 前項に加え、乙は再委託先から次の各号の同意を得なければならない。また、乙は、当該同意を得た旨を甲に書面で報告する。

①事故発生時には直ちに甲に対しても通知すること

②事故再発防止策を協議する際には甲の参加も認めること

①再委託先における機密情報の具体的管理状況の報告は、甲の閲覧も可とすること

第○条（権利義務の譲渡）

乙は、本契約によって生じる権利又は義務を第三者に譲渡し、又は承継させてはならない。

第○条（納入物件の知的財産権）

1. 納入物件に関する著作権（著作権法第 27 条及び第 28 条に定める権利を含む。）、本契約の履行過程で生じた発明（考案及び意匠の創作を含む。）及びノウハウを含む産業財産権（特

許その他産業財産権を受ける権利を含む。）（以下「知的財産権」という。）は、乙又は国内外の第三者が従前から保有していた知的財産権を除き、第〇条の規定による請負業務完了の日をもって、乙から甲に自動的に移転するものとする。

1. 納入物件に、乙又は第三者が従前から保有する知的財産権が含まれている場合は、前項に規定する移転の時に、乙は甲に対して非独占的な実施権、使用権、第三者に対する利用許諾権(再利用許諾権を含む。)、その他一切の利用を許諾したものとみなす。なお、その対価は契約金額に含まれるものとする。
2. 乙は、甲及び甲の許諾を受けた第三者に対し、納入物件に関する著作者人格権、及び納入物件に対する著作権法第 28 条の権利、その他“原作品の著作者／権利者”の地位に基づく権利主張は行わないものとする。

第○条（知的財産権の紛争解決）

1. 乙は、納入物件に関し、甲及び国内外の第三者が保有する知的財産権（公告、公開中のものを含む。)を侵害しないことを保証するとともに、侵害の恐れがある場合、又は甲からその恐れがある旨の通知を受けた場合には、当該知的財産権に関し、甲の要求する事項及びその他の必要な事項について調査を行い、これを甲に報告しなければならない。
2. 乙は、前項の知的財産権に関して権利侵害の紛争が生じた場合（私的交渉、仲裁を含み、法的訴訟に限らない。）、その費用と責任負担において、その紛争を処理解決するものとし、甲に対し一切の負担及び損害を被らせないものとする。

第○条（損害賠償）

乙は、乙の責に帰すべき事由によって甲又は第三者に損害を与えたときは、その被った通常かつ直接の損害を賠償するものとする。ただし、乙の負う賠償額は、乙に故意又は重大な過失がある場合を除き、第〇条所定の契約金額を超えないものとする。

第○条（協議）

本契約に定める事項又は本契約に定めのない事項について生じた疑義については、甲乙協議し、誠意をもって解決する。

第○条（その他）

本契約に関する紛争については、〇〇地方裁判所を唯一の合意管轄裁判所とする。

【コメント】

以下に示すような「機密保持条項に関連する他の条項」については、業務委託期間終了又

は本契約の解除後も、合理的な期間にわたり存続させることが望まれます。第○条（権利義務の譲渡）

第○条（成果の帰属） 第○条（損害賠償）

第○条（法令等の遵守義務） 第○条（協議事項）

第○条（紛争の解決）

また、第○条（守秘義務）の規定は、「業務委託期間終了又は本契約の解除後○年間有効とする」の如く有効期間を示すことが適切です。

9-2 委託先情報セキュリティ対策状況確認リスト

注：このサンプルは、委託先の情報セキュリティ対策の実施状況を確認するためのものです。 必要な項目を加筆修正してご利用ください。

会社名： 確認者： 確認日：

|  |  |  |  |
| --- | --- | --- | --- |
| 区分 | No | 確認項目 | 実施状況  (○、×) |
| 社内体制 | 1 | 情報セキュリティ管理責任者を定めている |  |
| 2 | 情報セキュリティ対策を定めた規程を整備している |  |
| 3 | 情報セキュリティへの取り組み方針を従業員や取引先に周知している |  |
| 4 | 情報セキュリティ事故に対する対応手順を整備している |  |
| 5 | 定期的に情報セキュリティに関する内部点検を実施している |  |
| 人的管理 | 6 | 情報セキュリティに関する教育を定期的に実施し、受講記録を作成している |  |
| 7 | 従業員と守秘義務契約を交わしている |  |
| 物理的管理 | 8 | 関係者以外の事務所への立ち入りを制限している |  |
| 9 | 機密情報の保管について施錠管理をしている |  |
| 10 | 機密情報を保管している領域に入ることができる人を制限し、入退出記録  を取得している |  |
| 11 | 入退出記録を定期的に確認している |  |
| 情報機器・媒体の取り扱い | 12 | ①機器・媒体の盗難防止措置を講じている |  |
| 13 | 媒体の無断複製、不正持出しを防止する措置を講じている |  |
| 14 | 媒体の移送、受け渡し時の保護措置を講じている |  |
| 15 | 媒体の安全な消去、廃棄の手順を整備している |  |
| サーバー・ パソコン等の管理 | 16 | 業務で使用するサーバー・パソコンのウイルス対策を行っている |  |
| 17 | 業務で使用するサーバー・パソコンは利用者認証機能を設定している |  |
| 18 | 業務で使用するサーバー・パソコンに利用制限等を設け管理している |  |
| 委託先管理 | 19 | 重要情報の授受を伴う委託先との契約書には、秘密保持条項を規定して  いる |  |
| 20 | 重要情報の授受を伴う委託先には自社と同等の情報セキュリティ対策を求  めている |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **10** | 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 | 改訂日 | 20yy.mm.dd |
| 適用範囲 | 情報資産及び保有する個人データに関わるインシデント | | |

1. 対応体制

情報セキュリティインシデントが発生した場合には、以下の体制で対応する。

|  |  |
| --- | --- |
| 最高責任者 | 代表取締役 |
| 対応責任者 | インシデント対応責任者 |
| 一次対応者 | 発見者又はシステム管理者 |

1. 情報セキュリティインシデントの影響範囲と対応者

情報セキュリティインシデントが発生した場合、以下を参考に影響範囲を判断して対応する。

|  |  |  |
| --- | --- | --- |
| 事故レベル | 影響範囲 | 対応者 |
| **3** | * 顧客、取引先、株主等に影響が及ぶとき * 個人情報が漏えいしたとき | 代表取締役  インシデント対応責任者 |
| **2** | 事業に影響が及ぶとき | インシデント対応責任者 |
| **1** | 従業員の業務遂行に影響が及ぶとき | システム管理者 |
| **0** | インシデントにまでは至らないが、将 来においてインシデントが発生する可  能性がある事象が発見されたとき | システム管理者 |

1. インシデントの連絡及び報告

レベル 1 以上のインシデントが発生した場合、発見者は以下の連絡網に従い、対応者に速やかに報告し、指示を仰ぐ。

|  |  |
| --- | --- |
| 最終対応者 | 緊急連絡先 |
| 代表取締役 | 携帯電話：090-\*\*\*\*-\*\*\*\*  電子メールアドレス：president@\*\*\*\*\*.co.jp |
| インシデント対応責任者 | 携帯電話：090-\*\*\*\*-\*\*\*\*  電子メールアドレス：incident@\*\*\*\*\*.co.jp |
| システム管理者 | 携帯電話：090-\*\*\*\*-\*\*\*\*  電子メールアドレス：system@\*\*\*\*\*.co.jp |

1. 対応手順

インシデントを以下のとおりに区分し、それぞれの対応手順を示す。

|  |  |
| --- | --- |
| 区分 | 事件・事故の状況 |
| 漏えい・流出 | 社外秘又は極秘情報資産の盗難、流出、紛失 |
| 改ざん・消失・破壊  サービス停止 | 情報資産の意図しない改ざん、消失、破壊  情報資産が必要なときに利用できない |
| ウイルス感染 | 悪意のあるソフトウェアに感染 |

* 1. 漏えい・流出発生時の対応

|  |  |  |
| --- | --- | --- |
| 事故レベル | 対応手順 | 対応者 |
|  | ①発見者は即座にインシデント対応責任者及び 代表取締役社長に報告する。  ②インシデント対応責任者は原因を特定するとともに、二次被害が想定される場合には防止策 を実行する。  ③インシデント対応責任者は被害者/本人対応を  準備する。 | 代表取締役  インシデント対応責任者 |
|  | ④インシデント対応責任者は問い合せ対応を準  備する。 |  |
| **3** | ⑤インシデント対応責任者は影響範囲・被害の大きさによっては総務部に報道発表の準備を申請 する。  ⑥インシデント対応責任者はサイバー攻撃等の不正アクセスによる被害の場合は都道府県警 察本部のサイバー犯罪相談窓口に届け出る。 |  |
|  | ⑦インシデント対応責任者は個人データ\*または |  |
|  | 特定個人情報漏えいの場合には個人情報保護 委員会に報告する。  ⑧代表取締役は社内及び影響範囲の全ての組 織・人に対応結果及び対策を公表する。 |  |
|  | \*個人データ︓個人情報データベース等（特定の個人を |  |
|  | 検索できるようにまとめたもの）を構成する個人情報 |  |
| **2** | ②発見者は発見次第、システム管理者に報告す る。  ③システム管理者は漏えい先を調査し、インシデ ント対応責任者に報告する。  ④システム管理者は社内関係者に周知する。 | インシデント対応責任者 |
| **1** | ※情報漏えい・流出は全て事故レベル 2 以上 |  |

* 1. 改ざん・消失・破壊・サービス停止発生時の対応

|  |  |  |
| --- | --- | --- |
| 事故レベル | 対応手順 | 対応者 |
| **3** | ①発見者は即座にインシデント対応責任者及び 代表取締役社長に報告する。  ②システム管理者は原因を特定し、応急処置を実 行する。  ③インシデント対応責任者は社内に周知すると ともに総務部情報システム担当に連絡する。  ④電子データの場合はシステム管理者がバック アップによる復旧を実行する。  ⑤機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。  ⑥書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する。  ⑦システム管理者は原因対策を実施する。  代表取締役は社内及び影響範囲の全ての組織・  人に対応結果及び対策を公表する。 | 代表取締役  インシデント対応責任者 |
| **2** | ①発見者は発見次第、システム管理者に報告す る。  ②システム管理者は原因を特定し、応急処置を実 行する。  ③インシデント対応責任者は社内に周知すると ともに総務部情報システム担当に連絡する。  ④電子データの場合はシステム管理者がバック アップによる復旧を実行する。  ⑤機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。  ⑥書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する。  ⑦システム管理者は原因対策を実施する。 | システム管理者インシデント対応責任者 |
| **1** | ①発見者は発見次第、システム管理者に報告す る。  ②システム管理者は原因を特定し、応急処置を実 行する。  ③電子データの場合はシステム管理者がバック アップによる復旧もしくは再作成・入手を実行 する。  ④機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。  ⑤書類・フィルム等の原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する  ⑥システム管理者は原因対策を実施する | システム管理者 |
| **0** | 発見者は発見次第、発生可能性のあるインシデン トと想定される被害をシステム管理者に報告す る。 | システム管理者 |

* 1. ウイルス感染時の初期対応

従業員は、業務に利用しているパソコン、サーバー又はスマートフォン、タブレット（以下「コ ンピュータ」といいます。）がウイルスに感染した場合には、以下を実行する。

①ネットワークからコンピュータを切断する。

②システム管理者に連絡する。

③ウイルス対策ソフトの定義ファイルを最新版に更新する。

④ウイルス対策ソフトを実行しウイルス名を確認する。

⑤ウイルス対策ソフトで駆除可能な場合は駆除する。

⑥駆除後再度ウイルス対策ソフトでスキャンし、駆除を確認する。

⑦システム管理者に報告する。

以下の場合など従業員自身で対応できないと判断される場合はシステム管理者に問い合わせる。

* ウイルス対策ソフトで駆除できない。
* システムファイルが破壊・改ざんされている。
* ファイルが改ざん・暗号化・削除されている。

4.5 届出及び相談

システム管理者は、インシデント対応後に以下の機関への届け出又は相談を検討する。

＜届出・相談・報告先＞

【独立行政法人 情報処理推進機構セキュリティセンター(IPA/ISEC)】

* ウイルスの届出https:/[/www.ipa.go.jp/security/outline/todoked](http://www.ipa.go.jp/security/outline/todokede-j.html)e[-j.html](http://www.ipa.go.jp/security/outline/todokede-j.html) TEL: 03-5978-7518

E-mail：[virus@ipa.go.jp](mailto:virus@ipa.go.jp)

* 不正アクセスに関する届出E-Mail：[crack@ipa.go.jp](mailto:crack@ipa.go.jp) FAX：03-5978-7518
* 情報セキュリティ安心相談窓口https:/[/www.ipa.go.jp/security/anshin/index.html](http://www.ipa.go.jp/security/anshin/index.html) TEL:03-5978-7509

E-mail：[anshin@ipa.go.jp](mailto:anshin@ipa.go.jp)

【個人情報保護委員会】

* 個人データ（特定個人情報に係るものを除く。）の漏えい、滅失又は毀損
* 加工方法等情報（匿名加工情報の加工の方法に関する情報等）の漏えい
* これらのおそれ

※次の URL 内の指示（様式等）に従うこと

https:/[/www.ppc.go.jp/personal/legal/leakAction/](http://www.ppc.go.jp/personal/legal/leakAction/)

TEL：03-6457-9685 FAX：03-3597-4560

郵送：〒100-0013 東京都千代田区霞が関３－２－１霞が関コモンゲート西館 32 階個人情報保護委員会事務局 個人データ漏えい等報告窓口宛

* 特定個人情報の漏えい事案等

https:[//www.ppc.go.jp/](http://www.ppc.go.jp/legal/rouei/)l[egal/rouei](http://www.ppc.go.jp/legal/rouei/)/

郵送：〒100‐0013 東京都千代田区霞が関３－２－１ 霞が関コモンゲート西館 32 階個人情報保護委員会事務局 特定個人情報漏えい等報告窓口 宛

※重大事態又はそのおそれのある事案が発覚した場合には、第一報を FAX で報告する

FAX: 03-3593-7962

1. 情報セキュリティインシデントによる事業中断と事業継続管理

代表取締役は、情報セキュリティインシデントの影響により当社事業が中断した場合に備え、以 下を定める。

* 1. 想定される情報セキュリティインシデント

以下のインシデントによる事業の中断を想定する。

* 情報セキュリティインシデント：大型地震の発生に伴う設備の倒壊、回線の途絶、停電等によ る○○システム停止
* 想定理由：当社の事業は、商品の販売から請求回収までの業務を○○システムに依存している ため、停止した場合は事業の継続が困難になり多大な損失が発生
  1. 復旧責任者及び関連連絡先

|  |  |  |
| --- | --- | --- |
| 被害対象 | 復旧責任者 | 関係者連絡先 |
| 電源設備  空調機 | 総務部長 | ○○電力△△支店  (株)○○設備 |
| （○○システム） ハードウェア  ソフトウェア  ネットワーク機器回線サービス  バックアップクラウドサー  バー | インシデント対応責任者システム管理者 | (株)○○システム開発  (株)△△ネットワークサービス  (株)◇◇マネージドサーバー |
| 顧客 | 営業部長 | 営業部取引先リスト参照 |
| 従業員人的被害 | 総務部長 | 従業員名簿参照 |

* 1. 事業継続計画

インシデント対応責任者は、想定する情報セキュリティインシデントが発生し、事業が中断した 際の復旧責任者の役割認識及び関係者連絡先について、有効に機能するか検証する。復旧責任者

は、被害対象に応じて復旧から事業再開までの計画を立案する。

|  |  |  |  |
| --- | --- | --- | --- |
| **11** | 個人番号及び特定個人情報の取り扱い | 改訂日 | 20yy.mm.dd |
| 適用範囲 | 特定個人情報（マイナンバーを内容に含む個人情報） | | |

個人番号及び特定個人情報の適正な取り扱いに関する基本方針

注：このサンプルは、中小企業・小規模事業者のための支援サイト「ミラサポ」の「マイナンバー制度ヘッドライン」が提供する様式「個人情報及び特定個人情報の適正な取扱 いに関する基本方針」を基に作成しています。最新版の様式は下記 URL よりダウンロード可能です。

<https://www.mirasapo.jp/mynumber/style.html>

1. 関係法令・ガイドライン等の遵守

当社は、個人番号及び特定個人情報（以下「特定個人情報等」といいます。）の取り扱いに関し、

「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」（以下「マイナン バー法」といいます。）及び「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」、 並びに「個人情報の保護に関する法律」（以下「個人情報保護法」といいます。）及び個人情報保 護委員会のガイドラインを遵守します。

1. 利用目的

当社は、提供を受けた特定個人情報等を、以下の目的で利用します。

1. 取引先様の特定個人情報等

・不動産取引に関する支払調書作成事務

・報酬、料金、契約金及び賞金に関する支払調書作成事務

1. 株主様の特定個人情報等

・配当及び剰余金の分配に関する支払調書作成事務

1. 当社の従業員等の特定個人情報等

【税務】

・源泉徴収票作成事務

・扶養控除等（異動）申告書、保険料控除申告書兼給与所得者の配偶者特別控除申告書作成事務

【社会保険】

・健康保険・厚生年金保険届出、申請・請求事務

・雇用保険・労災保険届出、申請・請求、証明書作成事務

1. 当社従業員等の配偶者及び親族等の特定個人情報等

【税務】

・源泉徴収票作成事務

・扶養控除等（異動）申告書、保険料控除申告書兼給与所得者の配偶者特別控除申告書作成事務

【社会保険】

・健康保険・厚生年金保険届出事務

1. 安全管理措置に関する事項

当社は、特定個人情報等の漏えい、滅失又は毀損の防止その他の個人番号の適切な管理のために、 別途規則を定め、これを遵守します。

1. 委託の取り扱い

当社は、特定個人情報等の取り扱いを第三者に委託することがあります。この場合、当社は、マ イナンバー法及び個人情報保護法に従って、委託先に対する必要かつ適切な監督を行います。

1. 継続的改善

当社は、特定個人情報等の取り扱いを継続的に改善するよう努めます。

1. 特定個人情報等の開示

当社は、本人又はその代理人から、当該特定個人情報等に係る保有個人データの開示の求めがあ ったときは、次の各号の場合を除き、遅滞なく回答します。

・本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

・当社の業務の適正な実施に著しい支障を及ぼすおそれがある場合

・法令に違反することとなる場合

特定個人情報等の開示に関するお問合せ、及び質問苦情等は下記までお願いいたします。

［窓口名称・担当者名等］

［電話番号・電子メールアドレス・問い合わせ用ウェブページのアドレス等］

発効日:20〇○年○月○日

株式会社○○○○ 代表取締役社長 ○○○○

個人番号及び特定個人情報取扱規程

注：このサンプルは、中小企業・小規模事業者のための支援サイト「ミラサポ」の「マイナンバー制度ヘッドライン」が提供する様式「個人番号及び特定個人情報取扱規程」を 基に作成しています。最新版の様式は下記 URL よりダウンロード可能です。<https://www.mirasapo.jp/mynumber/style.html>

1. 総則
   1. 目的

本規程は、個人番号及び特定個人情報（以下「特定個人情報等」という。）の適正な取り扱いの 確保に関し必要な事項を定めることにより、当社の事業の適正かつ円滑な運営を図りつつ、個人 の権利利益を保護することを目的とする。

* 1. 定義

本項における用語の定義は、次に定めるところによる。 **個人情報：**

生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。

1. 当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁 的方式（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をいう。） で作られる記録をいう。）に記載され、若しくは記録され、又は音声、動作その他の方法を用い て表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）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。）
2. 個人識別符号が含まれるもの**個人番号：**

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（以下「マイナンバー 法」という。）第 2 条 5 項が定める住民票コードを変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう。

**特定個人情報：**

個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であ って、住民票コード以外のものを含む。）をその内容に含む個人情報をいう。

**個人情報データベース等：**

個人情報を含む情報の集合物であって、特定の個人情報について電子計算機を用いて検索するこ とができるように体系的に構成したもののほか、特定の個人情報を容易に検索することができる ように体系的に構成したものとして「個人情報の保護に関する法律施行令」（平成 15 年政令第

507 号。以下「個人情報保護法施行令」という。）で定めるものをいう。**個人情報ファイル：**

個人情報を含む情報の集合物であって、特定の個人情報について電子計算機を用いて検索することができるように体系的に構成したもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして「個人情報の保護に関する法律施行令」で定めるものをいう。 **特定個人情報ファイル：**

個人番号をその内容に含む個人情報ファイルをいう。 **個人データ:**

個人情報データベース等を構成する個人情報をいう。 **保有個人データ:**

個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提 供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることに より公益その他の利益が害されるものとして個人情報保護法施行令で定めるものをいう。

**個人番号関係事務：**

マイナンバー法第 9 条第 3 項の規定により個人番号利用事務（行政機関、地方公共団体、独立行

政法人等その他の行政事務を処理する者が同条第1 項又は第2 項の規定によりその保有する特定個人情報ファイルにおいて個人情報を効率的に検索し、及び管理するために必要な限度で個人番 号を利用して処理する事務）に関して行われる他人の個人番号を必要な限度で利用して行う事務 をいう。

**個人情報取扱事業者:**

個人情報データベース等を事業の用に供している者（国の機関、地方公共団体、独立行政法人等 及び地方独立行政法人を除く。）をいう。

**本人：**

個人番号によって識別され、又は識別され得る特定の個人をいう。 **従業員：**

当社の組織内にあって直接間接に当社の指揮監督を受けて当社の業務に従事している者をいう。 具体的には、従業員のほか、取締役、監査役、理事、監事、派遣社員等を含む。

* 1. 当社の責務

マイナンバー法その他の個人情報保護に関する法令及びガイドライン等を遵守するとともに、実 施するあらゆる事業を通じて特定個人情報等の保護に努めるものとする。

1. 特定個人情報等の取り扱い
   1. 利用目的の特定

* 特定個人情報等を利用できる事務の範囲を、社会保障、税及び災害対策に関する特定の事務に 限定するものとする。
* 利用に当たっては前項で定めた事務の範囲の中から、具体的な利用目的を特定したうえで、利 用するものとする。
* 特定した利用目的を超えて利用する必要が生じた場合には、当初の利用目的と相当の関連性を 有すると合理的に認められる範囲内で利用目的を変更して、本人に通知を行い、変更後の利用 目的の範囲内で利用するものとする。
  1. 取得に際しての利用目的の通知等
* 特定個人情報等を取得した場合は、あらかじめその利用目的を通知又は公表している場合を除 き、速やかに、その利用目的を本人に通知し、又は公表するものとする。
* 前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電 子的方式等で作られる記録を含む。）に記載された当該本人の特定個人情報等を取得する場合 その他本人から直接書面に記載された当該本人の特定個人情報等を取得する場合は、あらかじ め、本人に対し、その利用目的を明示するものとする。ただし、人の生命、身体又は財産の保 護のために緊急に必要がある場合は、この限りでない。
* 前 2 項の規定は、次に掲げる場合については、適用しない。
  + 1. 利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産 その他の権利利益を害するおそれがある場合
    2. 利用目的を本人に通知し、又は公表することにより当社の権利又は正当な利益を害する おそれがある場合
    3. 国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要が ある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行 に支障を及ぼすおそれがあるとき
    4. 取得の状況からみて利用目的が明らかであると認められる場合
  1. 取得の制限
* 特定個人情報等を取得するときは、適法かつ適正な方法で行うものとする。
* マイナンバー法第 19 条各号のいずれかに該当する場合を除き、他人の特定個人情報等を収集しないものとする。
  1. 個人番号の提供の求めの制限

マイナンバー法第 19 条各号に該当して特定個人情報の提供を受けることができる場合を除くほか、他人に対し、個人番号の提供を求めないものとする。

* 1. 本人確認

本人又はその代理人から個人番号の提供を受けるときは、マイナンバー法第 16 条の規定に従い、本人確認を行うものとする。

* 1. 利用目的外の利用の制限
* 「2.1 利用目的の特定」の規定により特定された利用目的の達成に必要な範囲を超えて、特定

個人情報等を取り扱わないものとする。

* 合併その他の事由により他の法人等から事業を継承することに伴って特定個人情報等を取得 した場合は、継承前における当該特定個人情報等の利用目的の達成に必要な範囲を超えて、当 該特定個人情報等を取り扱わないものとする。
* 前 2 項の規定にかかわらず、次の各号のいずれかに該当する場合には、「2.1 利用目的の特定」の規定により特定された利用目的の範囲を超えて特定個人情報等を取り扱うことができるも のとする。
  + 1. マイナンバー法第 9 条第 4 項の規定に基づく場合
    2. 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意があり、 又は本人の同意を得ることが困難であるとき
  1. 特定個人情報ファイルの作成の制限

マイナンバー法第 19 条 11 号から 14 号までのいずれかに該当して特定個人情報を提供し、又はその提供を受けることができる場合を除き、個人番号関係事務を処理するために必要な範囲を超 えて特定個人情報ファイルを作成しないものとする。

* 1. 特定個人情報等の保管

マイナンバー法第 19 条各号に該当する場合を除くほか、特定個人情報等を保管しないものとする。

* 1. データ内容の正確性の確保

「2.1 利用目的の特定」により特定された利用目的の達成に必要な範囲内において、特定個人情報等を正確かつ最新の内容に保つよう努めるものとする。

* 1. 特定個人情報等の提供

マイナンバー法第 19 条各号に該当する場合を除くほか、特定個人情報等を提供しないものとする。

* 1. 特定個人情報等の削除・廃棄

個人番号関係事務を処理する必要がなくなった場合で、かつ、所管法令において定められている 保存期間を経過した場合には、個人番号をできるだけ速やかに廃棄又は削除するものとする。た だし、その個人番号部分を復元できない程度にマスキング又は削除した場合には、保管を継続す ることができるものとする。

* 1. 特定個人情報等を誤って収集した場合の措置
* 従業者は、誤って特定個人情報等の提供を受けた場合、自ら当該特定個人情報等を削除又は廃 棄してはならず、速やかに所属長、「3.1 事務取扱担当者・責任者」に定める事務取扱責任者

に報告しなければならない。

* 前項の報告を受けた際、「5.3.4 個人番号の削除、機器及び電子媒体等の廃棄」に従って、当該特定個人情報等をできるだけ速やかに削除又は廃棄したうえで、その記録を保存するものとす る。
  1. 安全管理措置

特定個人情報等の取り扱いに関し、「4.委託先の監督」及び「5.安全管理措置」に定める安全管 理措置を講じるものとする。

1. 組織及び体制
   1. 事務取扱担当者・責任者

* 別途定めるとおり、特定個人情報等を取り扱う事務の範囲を明確化し、明確化した事務におい て取り扱う特定個人情報等の範囲を明確にしたうえで、当該事務に従事する従業員（以下「事 務取扱担当者」という。）を明確にするものとする。
* 別途定めるとおり、前項により定められた各事務における事務取扱責任者を明確にするものと する。
* 事務取扱責任者は、次に掲げる業務を所管する。
  + 1. 特定個人情報等の利用申請の承認及び記録等の管理
    2. 特定個人情報等を取り扱う保管媒体の設置場所の指定及び変更の管理 (3)特定個人情報等の管理区分及び権限についての設定及び変更の管理(4)特定個人情報等の取扱状況の把握

(5)委託先における特定個人情報等の取扱状況等の監督(6)特定個人情報等の安全管理に関する教育・研修の実施(7)特定個人情報等管理責任者に対する報告

(8)特定個人情報等の安全管理に関する規程の承認及び周知(9)事務取扱責任者からの報告徴収及び助言・指導

(10)特定個人情報等の適正な取り扱いに関する事務取扱担当者に対する教育・研修の企画 (11)その他特定個人情報等の安全管理に関する事項

* 1. 苦情対応
* 特定個人情報等の取り扱いに関する苦情（以下「苦情」という。）の対応について必要な体制 整備を行い、苦情があったときは、適切かつ迅速な処理に努めるものとする。
* 苦情対応の責任者は、○○○○部長とする。
  1. 従業員の義務
* 当社の従業者又は従業員であった者は、業務上知り得た特定個人情報等の内容をみだりに他人 に知らせたり、不当な目的に使用したりしてはならない。
* 特定個人情報等の漏えい、滅失もしくは毀損の発生又は兆候を把握した従業員は、その旨を事 務取扱責任者に報告するものとする。
* 本規程に違反している事実又は兆候を把握した従業者は、その旨を事務取扱責任者に報告する ものとする。
* 事務取扱責任者は、前 3 項による報告の内容を調査し、本規程に違反する事実が判明した場合には遅滞なく代表取締役に報告するとともに、関係部門に適切な措置をとるよう指示するもの とする。

1. 委託の取り扱い
   1. 委託

特定個人情報等の取り扱いの全部又は一部を当社以外の者に委託するときは、委託先において、 マイナンバー法に基づき当社が果たすべき安全管理措置と同等の措置が講じられるか否かにつ いてあらかじめ確認したうえで、原則として委託契約において、特定個人情報等の安全管理について委託先が講ずべき措置を明らかにし、委託先における特定個人情報の取扱状況を把握するものとする。

* 1. 再委託

委託先が特定個人情報等の取り扱いの全部又は一部を再委託する場合には、当社の許諾を得るも のとする。また、再委託が行われた場合、当社は、委託先が再委託先に対して必要かつ適切な監 督を行っているかについて監督するものとする。

1. 安全管理措置

特定個人情報等の漏えい、滅失又は毀損の防止その他の特定個人情報等の安全管理のために、以 下に定める措置を講ずるものとする。

* 1. 組織的安全管理措置

特定個人情報等の適正な取り扱いのために、次に掲げる組織的安全管理措置を講じる。

* + 1. 組織体制の整備

安全管理措置を講ずるために、「3. 組織及び体制」に従い、組織体制を整備する。

* + 1. 取扱規程等に基づく運用

「情報資産管理台帳」に、以下を登録する。

|  |  |
| --- | --- |
| 情報資産管理台帳の項目 | 登録内容 |
| 情報資産名称 | 特定個人情報ファイルの種類、名称 |
| 備考 | 対象者及び個人情報の項目  明示・公表等を行った利用目的削除・廃棄状況 |
| 管理部署 | 責任者、取扱部署 |
| 利用者範囲 | アクセス権を有する者 |

|  |  |
| --- | --- |
| 媒体・保存先 | 保管場所・保管方法 |
| 保存期限 | 保存期間 |

なお、「情報資産管理台帳」には個人番号は記載しない。

* + 1. 取扱状況を確認する手段の整備

本規程に基づく運用状況を確認するため、以下の項目をシステムログ又は利用実績として記録す る。

・特定個人情報ファイルの利用・出力状況の記録

・書類・媒体等の持出しの記録

・特定個人情報ファイルの削除・廃棄記録

・削除・廃棄を委託した場合、これを証明する記録等

・特定個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者の情報システムの利用 状況（ログイン実績、アクセスログ等）の記録

* + 1. 情報漏えい等事案に対応する体制の整備

情報漏えい等の事案の発生又は兆候を把握した場合には、事務取扱責任者は「情報セキュリティ 関連規程」に定める安全管理措置に従って対応を行う。

* + 1. 取扱状況の把握及び安全管理措置の見直し

特定個人情報等の取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組むため、事 務取扱責任者が、毎年○月、取扱状況を点検し、安全管理措置を見直す。

* 1. 人的安全管理措置

特定個人情報等の適正な取り扱いのために、「情報セキュリティ関連規程２ 人的対策」に従い人的安全管理措置を講じる。

5.2.1 従業者の監督・教育

特定個人情報等の安全管理のために、従業者に対する必要かつ適切な監督・教育を行うものとす る。

* 1. 物理的安全管理措置

特定個人情報等の適正な取り扱いのために、「情報セキュリティ関連規程５ 物理的対策」の物理的安全管理措置を講じる。

* + 1. 特定個人情報等を取り扱う領域の管理

特定個人情報ファイルを取り扱う情報システムを管理するセキュリティ領域（以下「レベル○領 域」という。）及び特定個人情報等を取り扱う事務を実施するセキュリティ領域（以下「レベル

* 領域」という。）を明確にし、「情報セキュリティ関連規程５ 物理的対策」に定める安全管理措置を講ずる。
  + 1. ＩＴ機器及び電子媒体等の盗難等の防止

管理区域及び取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は 紛失等を防止するために、「情報セキュリティ関連規程６ ＩＴ機器利用」に定める安全管理措置

を講ずる。

* + 1. 電子媒体等を持ち出す場合の漏えい等の防止

特定個人情報等が記録された電子媒体又は書類等を社外に持ち出す場合、「情報セキュリティ関 連規程６ ＩＴ機器利用」に定める安全管理措置を講じる。

* + 1. 個人番号の削除、機器及び電子媒体等の廃棄

個人番号を削除又は廃棄する際には、「情報セキュリティ関連規程６ ＩＴ機器利用」に定める安全管理措置に従って、復元できない手段で削除又は廃棄する。

* 1. 技術的安全管理措置

特定個人情報等の適正な取り扱いのために、以下の技術的安全管理措置を講じる。

* + 1. アクセス制御

事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切な アクセス制御を行う。

* + 1. アクセス者の識別と認証

特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であ ることを、識別した結果に基づき認証するものとする。

* + 1. 外部の不正アクセス等の防止

情報システムを外部からの不正アクセス又は不正ソフトウェアから保護するため、「情報セキュ リティ関連規程６.ＩＴ機器利用」「情報セキュリティ関連規程７ ＩＴ基盤運用管理」に定める安全管理措置を講じる。

* + 1. 情報漏えい等の防止

特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するため、「情報セキュリティ関連規程６ ＩＴ機器利用」に定める安全管理措置を講じる。

1. 特定個人情報等の開示、訂正等、利用停止等
   1. 特定個人情報等の開示等

本人から、当該本人が識別される特定個人情報等に係る保有個人データについて、書面又は口頭 により、その開示（当該本人が識別される特定個人情報等に係る保有個人データを保有していな いときにその旨を知らせることを含む。以下同じ。）の申出があったときは、身分証明書等によ り本人であることを確認のうえ、開示をするものとする。ただし、開示することにより次の各号 のいずれかに該当する場合は、その全部又は一部を開示しないことができる。

* + 1. 本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合 (2)当社の事業の適正な実施に著しい支障を及ぼすおそれがある場合

(3)他の法令に違反することとなる場合

開示は、書面により行うものとする。ただし、開示の申出をした者の同意があるときは、書面以 外の方法により開示をすることができる。

特定個人情報等に係る保有個人データの開示又は不開示の決定の通知は、本人に対し、遅滞なく

行うものとする。

* 1. 特定個人情報等の訂正等
* 本人から、当該本人が識別される特定個人情報等に係る保有個人データの内容が事実でないと いう理由によって当該特定個人情報等に係る保有個人データの内容の訂正、追加又は削除（以 下「訂正等」という。）を求められた場合には、その内容の訂正等に関して他の法令の規定に より特別の手続が定められている場合を除き、利用目的の達成に必要な範囲内において、遅滞 なく必要な調査を行い、その結果に基づき、当該特定個人情報等に係る保有個人データの内容 の訂正等を行うものとする。
* 前項の規定に基づき求められた特定個人情報等に係る保有個人データの内容の訂正等を行っ たとき、又は訂正等を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨（訂正 等を行ったときは、その内容を含む。）を通知するものとする。
* 前項の通知を受けた者から、再度申出があったときは、前項と同様の処理を行うものとする。
* 前第 2 項の規定により、本人から求められた措置の全部又は一部について、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合は、本人に対し、その 理由を説明するよう努めるものとする。
  1. 特定個人情報等の利用停止等
* 本人から、当該本人が識別される特定個人情報等に係る保有個人データが「2.6 利用目的外の利用の制限」の規定に違反して取り扱われているという理由又は「2.3 取得の制限」の規定に違反して取得されたものであるという理由によって、当該特定個人情報等に係る保有個人データの利用の停止又は消去（以下「利用停止等」という。）を求められた場合、又は「2.10 特定個人情報等の提供」の規定に違反して第三者に提供されているという理由によって、当該特定個人情報等に係る保有個人データの第三者への提供の停止（以下「第三者提供の停止」という。） を求められた場合で、その求めに理由があることが判明したときは、遅滞なく、当該特定個人情報等に係る保有個人データの利用停止等又は第三者提供の停止を行うものとする。ただし、 当該特定個人情報等に係る保有個人データの利用停止等又は第三者提供の停止に多額の費用 を要する場合その他の利用停止等又は第三者提供の停止を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。
* 前項の規定に基づき求められた特定個人情報等に係る保有個人データについて、利用停止等を行ったときもしくは利用停止等を行わない旨の決定をしたとき、又は第三者提供の停止を行ったときもしくは第三者提供の停止を行わない旨の決定をしたときは、本人に対し、遅滞なく、 その旨を通知するものとする。

前項第 3 項及び第 4 項は本項に準用する。

**中小企業・小規模事業者の皆様へ**



**取り返しのつかないことになる前に… クラウドサービス**

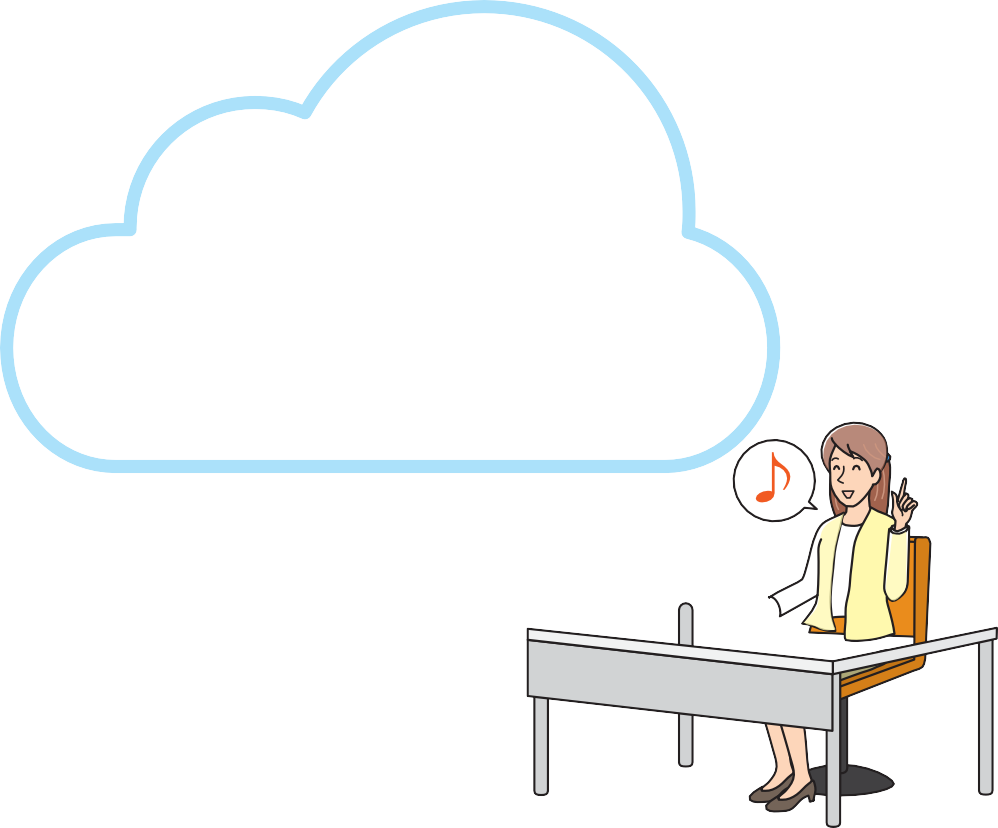
**安全利用チェックシート で確認！**

## 中小企業のための

**クラウドサービス**

# 安全利用の手引き

**クラウドサービスの安全利用、できてますか？**



**財務会計勤怠管理**

**文書作成表計算**

**データ保管情報共有**

**クラウドサービスとは？**

* インターネットを通じてソフトウェアやハードウェアを利用する情報システムサービスをクラウドサービスといいます。インターネットが普及し、コンピュータの仮想化技術※など、関連技術が進展したことで、身近になってきました。コンピュータが、雲の向こうのように、利用者から見えない所にあることから“クラウド”（cloud 雲）と呼ばれています。

※物理的に少数のコンピュータを、論理的に多数のコンピュータのように使うことができる技術

* 情報システムを自社で所有・運用することなく、サービスとして利用するだけのクラウドサービスは、メリットも多く、企業の業務処理だけでなく、個人の生活にまで利用が広がっています。



**身近なクラウドサービスの例**

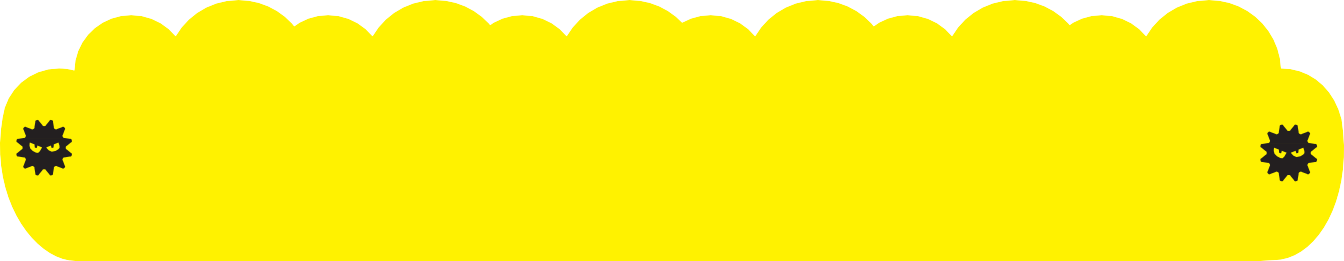
**財務会計、税務申告、給与計算、労務管理** などの経営管理アプリケーション

**顧客管理、販売管理、名刺管理、ホームページ作成、ECサイト** などの業務アプリケーション

**ワープロ、表計算、グループウェア、電子メール、オンラインストレージ** などのオフィスアプリケーション

**クラウドサービスを利用する前に確認しましょう！**

* 情報セキュリティ対策について、情報システムを所有する場合には、自社が対応すればよいのですが、“利用するだけ”のクラウドサービスではサービスを提供する事業者に委ねる部分が発生します。
* 事業者に委ねる部分については、利用者が直接管理することはできないので、サービスの機能だけではなく、サービスに付随するセキュリティ対策についても、きちんと確認したうえで利用する必要があります。
* クラウドサービスのセキュリティ対策は、自社で所有する場合との共通点もありますが、以下のようなクラウドサービス固有のリスクを考慮して検討します。

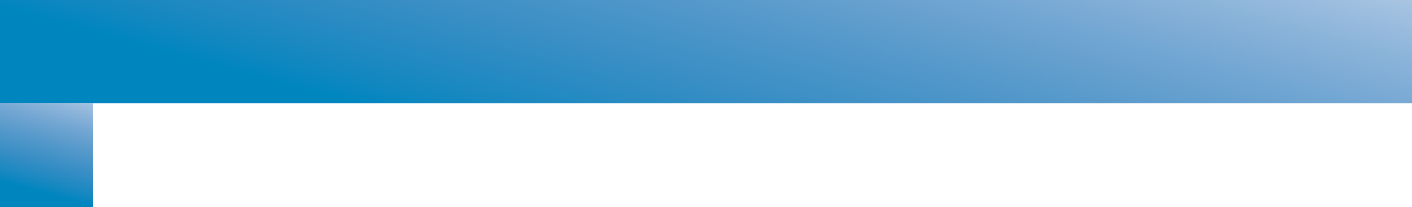


**インターネットを使う ➡外部からの攻撃を受けやすい １台のコンピュータを多数で共用する ➡１台のインシデントが多数に影響する１つのサービスが複数事業者で構成される※ ➡すべての対策を把握することが難しい**

**※サービスを提供するための、データセンター・ネットワーク回線などの設備、サーバー・ルーターなどの 機器、OSやアプリケーションなどのソフトウェアは、それぞれ別の事業者が運営していることがあります。**

**利用者がやるべきことを知っておきましょう！**

* クラウドサービスのセキュリティはサービスを提供する事業者と利用者との両者が、それぞれの役割・責任を分担し、必要とされる対策を実施することで維持・向上します。
* 次ページ以降の「クラウドサービス安全利用チェックリスト」と「解説編」を参考に、利用者としての役割・責任を認識して、今後ますます便利になる、クラウドサービスを活用してください。



**クラウドサービス安全利用チェックシート**

|  |  |  |  |
| --- | --- | --- | --- |
| **Ⅰ．選択するときのポイント** □✔ | | | |
| 1 | **どの業務で利用するか明確にする** | どの業務をクラウドサービスで行い、どの情報を扱うかを検討し、業務の切り分けや運用ルールを明確にしましたか？ | □ |
| 2 | **クラウドサービスの種類を選ぶ** | 業務に適したクラウドサービスを選定し、どのようなメリットがあるか確認しましたか？ | □ |
| 3 | **取扱う情報の重要度を確認する** | クラウドサービスで取扱う情報が漏えい、改ざん、消失したり、サービスが停止した場合の影響を確認しましたか？ | □ |
| 4 | **セキュリティのルールと矛盾しないようにする** | 自社のルールとクラウドサービス活用との間に矛盾や不一致が 生じませんか？ | □ |
| 5 | **クラウド事業者の信頼性を確認する** | クラウドサービスを提供する事業者は信頼できる事業者ですか？ | □ |
| 6 | **クラウドサービスの安全・信頼性を確認する** | サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービス品質保証は示されていますか？ | □ |
| **Ⅱ．運用するときのポイント** | | | |
| 7 | **管理担当者を決める** | クラウドサービスの特性を理解した管理担当者を社内に確保していますか？ | □ |
| 8 | **利用者の範囲を決める** | クラウドサービスを適切な利用者のみが利用可能となるように 管理できていますか？ | □ |
| 9 | **利用者の認証を厳格に行う** | パスワードなどの認証機能について適切に設定・管理は実施できていますか？（共有しない、複雑にするなど） | □ |
| 10 | **バックアップに責任を持つ** | サービス停止やデータの消失・改ざんなどに備えて、重要情報を手元に確保して必要なときに使えるようにしていますか？ | □ |
| **Ⅲ．セキュリティ管理のポイント** | | | |
| 11 | **付帯するセキュリティ対策を確認する** | サービスに付帯するセキュリティ対策が具体的に公開されていますか？ | □ |
| 12 | **利用者サポートの体制を確認する** | サービスの使い方がわからないときの支援（ヘルプデスクやFAQ） は提供されていますか？ | □ |
| 13 | **利用終了時のデータを確保する** | サービスの利用が終了したときの、データの取扱い条件について確認しましたか？ | □ |
| 14 | **適用法令や契約条件を確認する** | 個人情報保護などを想定し、一般的契約条件の各項目について 確認しましたか？ | □ |
| 15 | **データ保存先の地理的所在地を確認する** | データがどの国や地域に設置されたサーバーに保存されているか確認しましたか？ | □ |

※No15 クラウドサービスのサーバーは日本国外に設置されている場合もありますが、扱うデータによってサーバーの設置国・地域の法規制が適用されることがあります。

※No6,11,12,13はスマートSMEサポーター（認定情報処理支援機関）の開示情報で確認できます。



**解説編**

**Ⅰ．選択するときのポイント**

クラウドサービスの機能や情報セキュリティ対策はサービスを

提供する事業者の対応に依存する部分が多いため、必要な機能やセキュリティ対策を確認して選択します。



**チェックシートNo.1**

**どの業務で利用するか明確にする**

クラウドサービスでどの業務を行い、どの情報を扱うかを検討し、業務の切り分けや運用ルールを明確にしましょう。

**例えば**

**社内の情報共有のために、**

**●グループウェアを利用し、社員のスケジュール 管理を行う**

* **オンラインストレージに製品カタログを保存し て営業部門で共有する…など**



**チェックシートNo.2**

**クラウドサービスの種類を選ぶ**

業務に適したクラウドサービスを選び、メリットについて確認しましょう。

**例えば**

**社外でも業務ができるようにして、コストを削減 するために、**

* **経費精算にクラウドサービスを利用することで 外出先や自宅などどこでも業務ができるように する**

**●経費精算に関わる社内の作業時間を短縮し、サービス利用料を上回るコストを削減する… など**



**チェックシートNo.3**

**取扱う情報の重要度を確認する**

クラウドサービスで取扱う情報が漏えい、改ざんされたり、消失、サービスが停止したときの影響を確認しましょう。

**例えば**

**お客様の個人情報をクラウドサービスに保存して いて、サイバー攻撃で個人情報が漏えいした場合 の影響は、**

**●悪用などで本人に多大な迷惑がかかる**

* **本人への謝罪、補償や関係者への連絡が必要に なる**

**●個人情報保護委員会に報告が必要になる**

* **被害拡大防止や再発防止のために多額の費用が**

**かかる…など**



**チェックシートNo.4**

**セキュリティのルールと矛盾しないようにする**

セキュリティのルールとクラウドサービス活用との間に矛盾や不一致が生じないようにしましょう。

**例えば**

**給与計算をクラウドサービスで行うにあたり、従 業員のマイナンバーを登録する必要があるが、**

* **マイナンバーを記載した書類やデータを社外に 保存することは社内ルールで禁止されている**
* **そこで暗号化登録ができるサービスを利用し、 暗号化した場合のみ社外の保存を許可するルー ルに変更する…など**

**解説編**



**チェックシートNo.5**

**クラウド事業者の信頼性を確認する**

クラウドサービスを提供する事業者は信頼できる事業者を選択しましょう。

**例えば**

**会計業務をクラウドサービスに移行するにあたり 長期間利用できて、セキュリティ対策を常に改善 しているサービスを選択するため、**

**●事業者が公表している財務情報を確認する**

**●利用者数などの実績を問い合わせる**

* **事業者の情報セキュリティ方針や関連した認証・認定制度※1の取得状況を確認する…など**

**※1）以下のクラウドサービス選択時に参考となる制度等を参照してください。**



**チェックシートNo.6**

**クラウドサービスの安全・信頼性を確認する**

サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービス品質保証を確認しましょう。

**例えば**

**店舗にクラウド型POSレジを導入するにあたり サービスが常時に動いている必要があるため、**

* **事業者またはプラットフォーム事業者が公表し ている品質保証基準（SLA※２）を確認する**
* **システムの障害でデータ消失などの被害が発生 したときに、どこまでが事業者の責任で、どこ からが利用者の責任なのか利用規約で確認する**

**…など**

**※２）SLAService Level Agreementサービスレベルに関する合意書**

**「サービス及び合意されたサービスレベルを文書化した、サービスプロバイダと顧客間の書面による合意。(ISO/IEC20000-1)｣**

☛**クラウドサービス選択時に参考となる制度等**



クラウドサービス事業者が適切なデータ保護やセキュリティ対策を実施していることをマークとして表示する制度

があります。いずれもURL記載のページ内でそれぞれの条件を満たすサービスが紹介されており、選定時の参考と して利用することができます。 **ISMSクラウドセキュリティ認証**（一般社団法人情報マネジメントシステム認定センター）

**https://isms.jp/isms.html**

通常のISMS(JIS Q 27001)認証に加えて、クラウドサービス固有の管理策(ISO/IEC 27017)が適切に導入、実施

されていることを認証するものです。

**クラウド情報セキュリティ監査制度**（特定非営利活動法人日本セキュリティ監査協会） [**http://jcispa.jasa.jp/cloud\_security/**](http://jcispa.jasa.jp/cloud_security/)

クラウドサービス事業者が基本的な要件を満たす情報セキュリティ対策を実施していることを監査し、その結果を

CSマークの表示許諾を通じて利用者に対し、安全性が確保されていることを公開する制度です。外部監査と内部監 査で「ゴールド」と「シルバー」の２種類があります。

**ASP・SaaS情報開示認定制度**（特定非営利活動法人日本ASP・SaaS・IoTクラウドコンソーシアム） [**http://www.cloud-nintei.org/asp-nintei/**](http://www.cloud-nintei.org/asp-nintei/)

安全・信頼性に係る比較・評価・選択を行うために必要な情報を、クラウドサービス事業者が開示をしていること

を認定する制度です。クラウドで扱う情報や環境の種類に応じて、「医療情報」「特定個人情報」「IoTクラウド」

「データセンター」など合計７種類の認定マークが定められています。

☛

IT活用を支援する情報処理支援機関

中小企業者等の生産性向上に資するITツールや中小企業のIT活用を支援するITベンダーを法令に基づいて認定し、

中小企業者がITツール選定するために必要となる情報を開示しています。

**情報処理支援機関（スマートSMEサポーター）制度**（中小企業庁） **https://smartsme.go.jp/**

中小企業が使いやすいITツールの開発促進や中小企業のIT導入を通じた生産性向上を図ります。

認定を受けたITベンダーの情報セキュリティ対策の実施状況を確認できます。



**チェックシートNo.9**

**利用者の認証を厳格に行う**

パスワードなどの認証機能を適切に設定・管理しましょう。

**例えば**

**なりすましや不正ログインを防ぐために、**

* **パスワードは破られにくい安全なパスワードを 利用する**

**●ID・パスワードの共有はしない**

* **サービスで以下の認証方式が提供されている場 合は利用する**
  + **特定のパソコンでしか利用できないように電 子証明書※3をインストールする**
  + **パスワードを不正利用されてもログインはで きないように「2段階認証」※4を用いる…など**

※3）電子証明書インターネットでクラウドサービスを利用するときに特定のPCからしかアクセスできないように制限するための「身分証明書」です。

※4）複数の要素（記憶、所持、生体情報）を用いた認証方式である「多要素認証」や、同じ要素の認証を多段で実施する認証方式である

「多段階認証」などがあります。



**バックアップに責任を持つ**

サービス停止やデータの消失・改ざん等に備えて、重要情報を手元に確保して、必要なときに使えるようにしましょう。

**例えば**

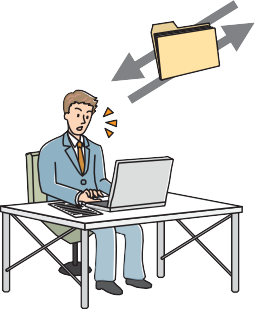
**会計データやホームページなど、消失や改ざんの 影響が大きいものは、**

* **クラウドサービスの拡張機能にバックアップが ある場合は利用する。**

**●定期的に社内の専用ハードディスクなどにもバックアップを取得する**

* **直前のバックアップよりもさらに過去の状態に 遡って復元できるように複数世代※5 のバックアップを取得する…など**

※5）毎月バックアップを取得する場合に前月だけでなく2ヶ月前、３ヶ月前のように複数のバックアップを取得しておくことです。



**解説編**

**Ⅱ．運用するときのポイント**

クラウドサービスを安全に利用するために、

利用者側の体制やセキュリティ対策を決めます。



**チェックシートNo.7**

**管理担当者を決める**

クラウドサービスの技術的な側面などの特性を理解したうえで、業務に適した運用や設定・操作・ヘルプデスクを行うことができる、管理担当者を社内に確保しましょう。

**例えば**

**クラウド型顧客管理システムの運用にあたり、**

* **入力項目やその活用については営業部長が担当 する**
* **技術的な設定や社内のヘルプデスクはシステム 管理者が担当する…など**



**チェックシートNo.8**

**利用者の範囲を決める**

クラウドサービスを利用する人の範囲を決め、どのような権限を与えるか適切に管理しましょう。

**例えば**

**販売管理をクラウドサービスで行うにあたり、**

* **社長と販売部門従業員だけに利用者アカウント を作成する**

**●承認権限は従業員の上司に付与する…など**

**チェックシートNo.10**



**解説編**

**Ⅲ．セキュリティ管理のポイント**

クラウドサービス特有のリスクや関連する法令について

対応できているか確認します。

法令違反？

**チェックシートNo.11 チェックシートNo.12**



**付帯するセキュリティ対策を確認する**

クラウドサービスにおけるセキュリティ対策が具体的に公開されているか確認しましょう。

**例えば**

**サイバー攻撃や通信傍受に対する対策が十分され ているか、**

**●通信の暗号化**

**●ファイアウォールや侵入検知**

**●ウイルス対策**

**●サービスで使っているOSやソフトウェアの脆 弱性対応・セキュリティパッチの適用について 公開されているか確認する…など**



**利用者サポートの体制を確認する**

サービスの使い方がわからないときの支援

（ヘルプデスクやFAQ）が提供されているか確認しましょう。

**例えば**

**クラウドサービスを社内のシステム担当者不在の 週末も利用するため、**

**●サポートの受付時間（週末夜間も受付可能か）**

* **連絡方法（メール、電話、チャット、オンライ ン、のうちパソコンがない事務所から週末も電 話連絡可能か）**
* **料金（頻繁に問い合わせた場合に料金はどのぐ らいか）を確認する…など**

**チェックシートNo.13 チェックシートNo.14**



**利用終了時のデータを確保する**

サービスの利用が終了したときの、

データの取扱い条件について確認しましょう。

**例えば**

**利用中のクラウド型会計システムを他のクラウド サービスに変更するにあたり、**

**●過年度データを含む全データを返却または社 内のパソコンなどにダウンロードできるか**

**●データのフォーマットは他のサービスと互換 性があるか**

**●移行先のサービスは返却されたデータを一括 して取り込む機能があるか**

**●返却後にシステム上に残るデータは完全に消 去または再利用されないことが保証されてい るかを確認する…など**



**適用法令や契約条件を確認する**

個人情報保護など関連法規制の遵守などを 規定した利用規約等について確認しましょう。

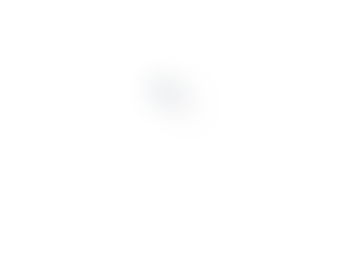
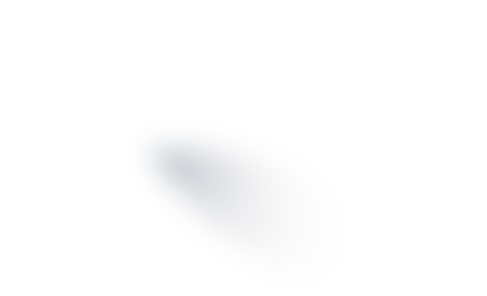
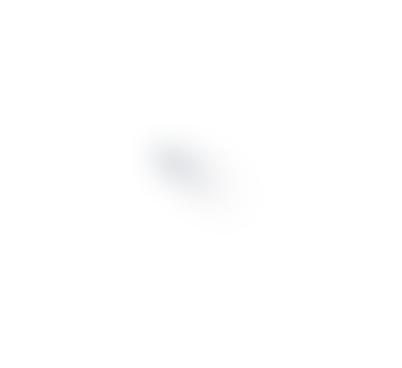
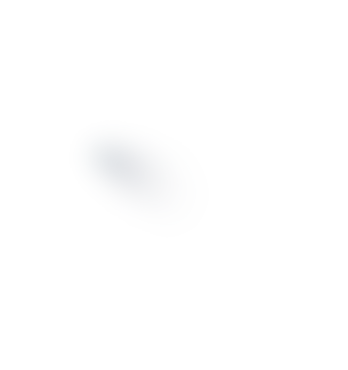
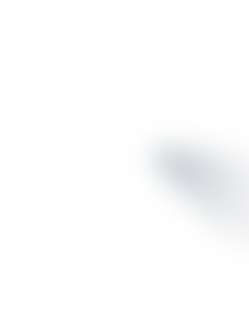
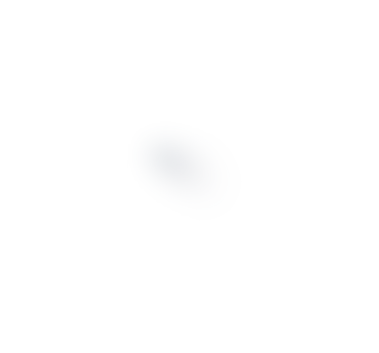
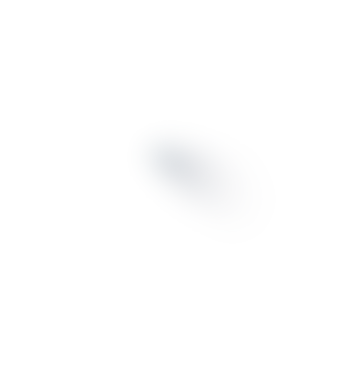
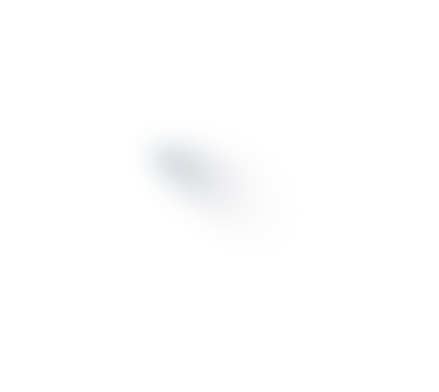
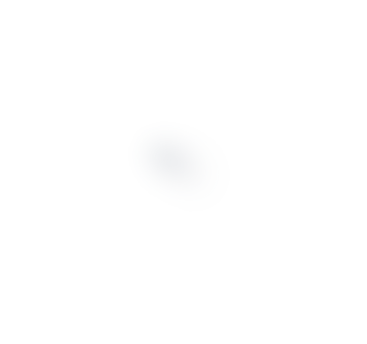
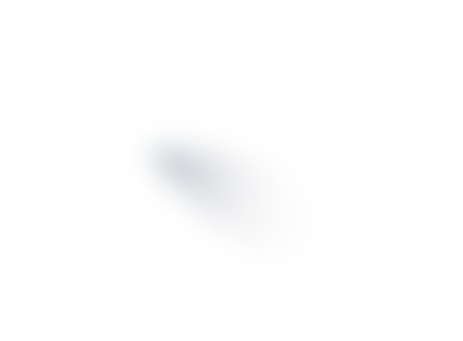
**例えば**

**クラウドサービスに秘密情報や個人情報を保存す るため、**

* **利用者が入力したデータにサービス事業者がア クセスする場合の条件や責任について明記され ているか**
* **設備の保守等を再委託している場合の再委託先 の管理監督責任について明記されているか**
* **利用者が入力した個人情報に関して個人情報保 護法に準拠することが明記されているか（安全 管理措置、委託先の監督）を確認する…など**

**解説編**

**チェックシートNo.15**



**データ保存先の地理的所在地を確認する**

データがどの国や地域に設置されたサーバーに保存されているか確認しましたか？

**例えば**

**海外から受注し、外国のメーカーから直送しても らうECサイトを運用するにあたり各国の個人情 報保護に係わる法律を遵守するため、**

**●事業者または事業者が利用しているプラットフォーム事業者・インフラ事業者が公表するデータセンターが所在する国・地域**

* **個人情報保護に係わる国内および海外の法律・ 規制※6を確認する…など**

※6）以下のような法律・規制があります。

・個人情報保護法 第24条 外国第三者提供個人データを外国にある第三者に提供する場合は、あらかじめ本人の同意を得なければならないことがあり ます。

・EU一般データ保護規則（General Data Protection Regulation：GDPR） 日本国内の企業でも欧州経済領域（European Economic Area：EEA、EU加盟国28カ国、ノルウェー、アイス ランド、リヒテンシュタイン）と個人データをやり取りする場合に適用対象となります。



**情報セキュリティ対策に役立つ情報**

**クラウドサービス利用のための情報セキュリティマネジメントガイドライン（経済産業省）**

クラウドサービスの利用にかかわるリスク対応のために JIS Q 27002（実践のための規範）から適切な管理策を選択し，導入するための

助言とその最適な実施のための手引を提供している

[**http://www.meti.go.jp/policy/netsecurity/downloadﬁles/cloudsec2013fy.pdf**](http://www.meti.go.jp/policy/netsecurity/downloadﬁles/cloudsec2013fy.pdf)

**クラウドセキュリティガイドライン活用ガイドブック（経済産業省）**

実際に発生した事故や、事業者が抱える様々なセキュリティ上の課題をベースに、ITサービスとしてのクラウドサービスに関するリスクと

対策を、事業者と利用者のそれぞれについて解説している

[**http://www.meti.go.jp/policy/netsecurity/downloadﬁles/cloudseckatsuyou2013fy.pdf**](http://www.meti.go.jp/policy/netsecurity/downloadﬁles/cloudseckatsuyou2013fy.pdf)

**クラウドサービスの安全・信頼性に係る情報開示指針（総務省）**

クラウドサービスの安全・信頼性を向上させることを目的として、利用者のサービス選定における情報収集の負担を軽減する観点から、

クラウドサービス事業者によるクラウドサービスに係る情報開示のあり方を示した指針

[**http://www.soumu.go.jp/main\_content/000477838.pdf**](http://www.soumu.go.jp/main_content/000477838.pdf)

**SECURITY ACTION セキュリティ対策自己宣言（独立行政法人情報処理推進機構）**

中小企業自らが情報セキュリティ対策に取組むことを自己宣言する制度で、自社の状況に応じて「一つ星」と「二つ星」の2段階の取組み

目標を用意している

[**https://www.ipa.go.jp/security/security-action/**](http://www.ipa.go.jp/security/security-action/)

独立行政法人情報処理推進機構セキュリティセンター

〒113-6591 東京都文京区本駒込二丁目28番8号文京グリーンコートセンターオフィス

TEL: 03-5978-7508 FAX: 03-5978-7518

E-mail：[isec-info@ipa.go.jp](mailto:isec-info@ipa.go.jp) URL：https://[www.ipa.go.jp/security/](http://www.ipa.go.jp/security/)

2019.3.19 Version 2.0

**「リスク分析シート」の利用方法**

1. シートの構成

この「リスク分析シート」は、自社で扱う情報のセキュリティに関する詳細リスク分析を行うために使用します。それぞれのシートの役割と使い方は次表の通りです。

|  |  |
| --- | --- |
| **シート名** | **役割と使い方** |
| **台帳記入例** | 「情報資産管理台帳」の記入見本です。このシートに入力しても分析はできませんのでご注意下さい。 |
| **情報資産管理台帳** | 情報資産管理台帳の実体となるシートです。自社で管理している情報資産の種類ごとに1行ずつ、その特徴（誰が管理しているか、保存場所はどこか、個人情報を含むかどうか）などを後述の手順に従って記入します。なお、「重要度」の列と右側のオレンジ色の部分は自動的に表示される部分ですので記入しないで下さい。 |
| **脅威の状況** | 自社をとりまく脅威の状況を記入するためのシートです。企業で扱う情報資産についての代表的な脅威を表形式で列挙しています。「対策を講じない場合の脅威の発生頻度」の列に自社における状況をメニューから選んで記入します。それ以外の列に記入の必要はあり ません。 |
| **対策状況チェック** | 自社における情報セキュリティ対策の実施状況を記入するシートです。対策の種類ごとに、「回答値」の列に自社の状況に最も近いものをメニューから選択します。 |
| **診断結果** | 上記の各シートに記入した内容をもとに、詳細リスク分析の結果が表示されるシートです。このシートには何も記入せず、結果を参照するためだけに利用します。 |

1. シートの利用方法

本シートを用いた詳細リスク分析の手順を以下に示します。なお、それぞれの手順の背景となる考え方などを中小企業の情報セキュリティガイドラインの本編のP44～P53で説明していますので併せて参照して下さい。

**［手順１］ 情報資産の洗い出し**

「台帳記入例」シートと下表を参考に、自社で管理している情報資産について情報資産の種類ごとに１行ずつ、「情報資産管理台帳シート」の各列を埋めていきます。一部の列についてはメニューから選択することで入力できます。

|  |  |
| --- | --- |
| **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、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、役職等の属性に関して、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。  ―要配慮個人情報の定義―  「 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り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１１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。 |

**［手順２］ リスク値の算定**

個々の情報資産ごとにリスク値を算定します。リスク値は「重要度」「脅威」「脆弱性」の３種類の要素をもとに決定されますが、重要度は手順１で算出されているものを使うので、ここでは次の２種類をそれぞれのシートで指定します。

1. **「脅威」の指定**

「脅威の状況」シートに列挙されている代表的な脅威のそれぞれについて、自社において発生する可能性があるかどうか、以下の３種類の選択肢から最も近いものを１つ選択します。

|  |  |
| --- | --- |
| **選択肢** | **意味** |
| **1:通常では発生しない（数年に１回未満）** | 通常の業務を行っている範囲内では発生することが考えにくいものに相当します。これには、モバイル機器を使っていない場合のモバイル機器の脅威に関する項目のように、そもそも発生するはずがないものも含みます。 |
| **2:特定の状況で発生する（年に数回程度）** | 1と3のいずれにもあてはまらないと考える場合は2を選んでください。また、過去に起きたことがない事故でも、今後起きる可能性があると感じている場合は1でなく2を選択してください。 |
| **3:通常の状態で発生する（いつ発生してもおかしくない）** | 自社でこれまでに何度か発生したことがあり、今後も発生することが懸念されるものに相当します。 |

1. **「脆弱性」の指定**

「対策状況チェック」シートに示されている11種類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」欄に表示される下記の選択肢１～４のいずれかを選択します。

|  |  |
| --- | --- |
| 選択肢 | 意味 |
| **1:実施している** | 情報セキュリティ診断項目に記載の通り、あるいはそれ以上の対策を実施している場合に相当します。 |
| **2:一部実施している** | 情報セキュリティ診断項目に記載されている項目の一部であったり、近い内容だがやや効果が不十分と考えられる対策を実施している場合に相当します。 |
| **3:実施していない/わからない** | 情報セキュリティ診断項目に記載されている対策を全く実施していない場合、あるいは対策として書かれている内容を実施しているかどうかわからない場合に相当します。 |
| **4:自社に該当しない** | 情報セキュリティ診断項目に記載されている状況が自社にあてはまらない場合に相当します。例 えば、自社でサーバーを運用していない場合の、サーバーに関する項目などがこれにあたります。 |

1. **リスク値の算定**

手順１と手順２の(1)(2)の記入が完了すると、「情報資産管理台帳」シートの右手の「現状から想定されるリスク」欄（オレンジ色の部分）に、情報資産ごとのリスク値に関する分析結果が表示されます。

|  |  |
| --- | --- |
| **「現状から想定されるリスク」欄の項目** | **各項目に表示される内容が意味するもの** |
| **脅威の発生頻度** | 「脅威の状況」シートにおける「対策を講じない場合の脅威の発生頻度」欄に記入した3段階の値のうち、「媒体・保存先」の種類に応じてもっとも大きい値を示しています。 |
| **脆弱性** | 「対策状況チェック」シートで設定した情報セキュリティ診断項目ごとの対策の実施状況をもとに、情報資産管理台帳における「媒体・保存先」の列で指定した内容を考慮した結果が表示されます。 |
| **被害発生可能性** | 脅威の発生頻度と脆弱性に表示されている内容をもとに、当該情報資産を対象とした被害が発生する可能性を高・中・低の３段階で表示します。 |
| **リスク値** | 情報資産の「重要度」と「被害発生可能性」の積をもとにリスクの大きさを大・中・小の３段階で表示します。 |

**［手順３］ 情報セキュリティ対策を決定**

手順１と手順２が完了すると、「診断結果」シートに「診断結果」として、対策の種類ごとに次の結果が示されます。

|  |  |
| --- | --- |
| **情報セキュリティ関連規程策定の必要性** | 以下の４種類の記号により、当該対策に関連した情報セキュリティ関連規程を策定する必要があるかどうかを示します。  ◎ 情報資産台帳の内容にかかわらず必要〇 リスク値算定の結果必要  △ 情報資産管理台帳からは判断不可能  — リスク値算定の結果不要 |
| **対策状況チェックの診断結果（対策の実施率）** | 「対策状況チェック」シートへの記入結果をもとに、対策すべき項目がどの程度実施されているかをパーセント形式で表示します。なお、扱う情報資産の種類によっては不要な対策もあるので、すべての対策を実施していなくても実施率が100%になることがあります。 |
| **<付録6>情報セキュリティ関連規程による対策規定の要否** | 上記２つの診断結果をもとに、対策を規定する必要があるかどうかが次の２種類のいずれかで表示されます。  対策を規定して下さい： リスクを減らすための対策を実施することを規定する必要があることを表しています。  対策の規定は不要です： 該当する情報資産がない、リスクが小さいなどの理由で、対策の必要がないことを表しています。 |

また、「診断結果」シートの「情報資産管理台帳に基づく管理すべき情報資産の状況」欄には「情報資産管理台帳」に記入した情報資産のうち、媒体・保存先ごと、個人情報を含むもの、重要度別などの条件ごとの情報資産の件数が表示されますので、情報資産が多い場合は確認用に利用して下さい。

中小企業の情報セキュリティ対策ガイドライン 付録7 リスク分析シート「台帳記入例」

情報資産管理台帳

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 業務分類 | 情報資産名称 | 備考 | 利用者範囲 | 管理部署 | 媒体・保存先 | 個人情報の種類 | | | 評価値 | | | | 保存期限 | 登録日 | 現状から想定されるリスク（入力不要・自動表示） | | | | | |
| 個人情報 | 要配慮  個人情  報 | マイナンバー | 機密性 | 完全性 | 可用性 | 重要  度 | 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 | |
| 人事 | 社員名簿 | 社員基本情報 | 人事部 | 人事部 | 事務所PC | 有 |  |  | 2 | 0 | 0 | **2** |  | 2019/3/1 | 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 |
| 人事 | 社員名簿 | 社員基本情報 | 人事部 | 人事部 | 書類 | 有 |  |  | 2 | 2 | 2 | **2** |  | 2019/3/1 | 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 |
| 人事 | 健康診断の結果 | 雇入時・ 定期健康診断 | 人事部 | 人事部 | 書類 |  | 有 |  | 2 | 2 | 1 | **2** | 5年 | 2019/3/1 | 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 |
| 経理 | 給与システムデータ | 税務署提出用源泉徴収票 | 給与計算担当 | 人事部 | 事務所PC |  |  | 有 | 2 | 2 | 1 | **2** | 7年 | 2019/3/1 | 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 |
| 経理 | 当社宛請求書 | 当社宛請求書の原本  （3年分） | 総務部 | 総務部 | 書類 |  |  |  | 1 | 1 | 1 | **1** |  | 2019/3/1 | 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 | 1 | リスク中 |
| 経理 | 発行済請求書控 | 当社発行の請求書の控え（3年分） | 総務部 | 総務部 | 書類 |  |  |  | 1 | 1 | 1 | **1** |  | 2019/3/1 | 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 | 1 | リスク中 |
| 共通 | 電子メールデータ | クラウド型メールをローカル同期・閲覧 | 担当者 | 総務部 | 事務所PC | 有 |  |  | 2 | 2 | 2 | **2** |  | 2019/3/1 | 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 |
| 共通 | 電子メールデータ | クラウド型メール(重要  度は混在のため最高値で評価) | 担当者 | 総務部 | 社外サーバー | 有 |  |  | 2 | 2 | 2 | **2** |  | 2019/3/1 | 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 |
| 営業 | 顧客リスト | 得意先（５年分） | 営業部 | 営業部 | 社内サーバー | 有 |  |  | 2 | 2 | 2 | **2** |  | 2019/3/1 | 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 | 2 | リスク中 |
| 営業 | 顧客リスト | 得意先（５年分） | 営業部 | 営業部 | 可搬電子媒体 | 有 |  |  | 2 | 1 | 1 | **2** |  | 2019/3/1 | 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 | 1 | リスク中 |
| 営業 | 顧客リスト | 得意先（５年分） | 営業部 | 営業部 | モバイル機器 | 有 |  |  | 2 | 1 | 1 | **2** |  | 2019/3/1 | 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 | 2 | リスク中 |
| 営業 | 受注伝票 | 受注伝票（10年分） | 営業部 | 営業部 | 社内サーバー |  |  |  | 1 | 1 | 1 | **1** |  | 2019/3/1 | 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 | 2 | リスク中 |
| 営業 | 受注伝票 | 受注伝票（10年分） | 営業部 | 営業部 | 書類 |  |  |  | 1 | 1 | 1 | **1** |  | 2019/3/1 | 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 | 1 | リスク中 |
| 営業 | 受注契約書 | 受注契約書原本  （10年分） | 営業部 | 営業部 | 書類 |  |  |  | 1 | 2 | 1 | **2** |  | 2019/3/1 | 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 |
| 営業 | 製品カタログ | 製品カタログ一式 | 営業部 | 営業部 | 社内サーバー |  |  |  | 0 | 1 | 1 | **1** |  | 2019/3/1 | 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 | 2 | リスク中 |
| 営業 | 製品カタログ | 製品カタログ一式 | 営業部 | 営業部 | 書類 |  |  |  | 0 | 1 | 1 | **1** |  | 2019/3/1 | 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 | 1 | リスク中 |
| 営業 | 製品カタログ | 製品カタログ一式 | 営業部 | 営業部 | 可搬電子媒体 |  |  |  | 0 | 1 | 1 | **1** |  | 2019/3/1 | 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 | 1 | リスク中 |
| 営業 | キャンペーン応募者リスト | 2018年のキャンペーン応募者情報 | 営業部 | 営業部 | 社内サーバー | 有 |  |  | 2 | 1 | 0 | **2** |  | 2019/3/1 | 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 |
| 調達 | 委託先リスト | 外部委託先（５年分） | 総務部 | 総務部 | 社内サーバー |  |  |  | 0 | 1 | 1 | **1** |  | 2019/3/1 | 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 | 2 | リスク中 |
| 調達 | 発注伝票 | 発注伝票（10年分） | 総務部 | 総務部 | 社内サーバー |  |  |  | 1 | 0 | 0 | **1** |  | 2019/3/1 | 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 | 2 | リスク中 |
| 調達 | 発注伝票 | 発注伝票（10年分） | 総務部 | 総務部 | 書類 |  |  |  | 1 | 0 | 0 | **1** |  | 2019/3/1 | 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 | 1 | リスク中 |
| 技術 | 製品設計図 | 現行製品の設計図 | 開発部 | 開発部 | 社内サーバー |  |  |  | 2 | 2 | 2 | **2** |  | 2019/3/1 | 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 |

中小企業の情報セキュリティ対策ガイドライン 付録7 リスク分析シート「台帳記入例」



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 業務分類 | 情報資産名称 | 備考 | 利用者範囲 | 管理部署 | 媒体・保存先 | 個人情報の種類 | | | 評価値 | | | | 保存期限 | 登録日 | 現状から想定されるリスク（入力不要・自動表示） | | | | | |
| 個人情報 | 要配慮  個人情  報 | マイナンバー | 機密性 | 完全性 | 可用性 | 重要  度 | 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 | |
| **1**  技術 | **2**  製品設計図 | **3**  現行製品の設計図 | **4**  開発部 | **5**  開発部 | **6**  書類 | **7** |  |  | **8**  2 | 2 | 2 | **2** | **9** | **10**  2019/3/1 | **11**  2:特定の状況で発生する（年  に数回程度） | **12**  2:部分的に脆弱性未対  策 | **13**  1 | 可能性：低 | **14**  2 | リスク中 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **＜記入内容についての解説＞** | | |
| ① | **業務分類** | 情報資産と関連する業務や部署を記入します。情報資産が少なければ省いても構いません。 |
| ② | **情報資産名称** | 情報資産の名称や内容を表すものを簡潔に記入します。正式名称がないものは社内通称で構いません。 |
| ③ | **備考** | 情報資産名称だけでは個人情報の有無や重要度が判断できない場合に説明を記入してください。 |
| ④ | **利用者範囲** | 情報資産を利用してよい部署等を記入してください。アクセスコントロールに利用できます。 |
| ⑤ | **管理部署** | 情報資産に対して情報セキュリティ上の管理責任がある部署等を記入してください。小規模事業者であれば担当者名を記入することでも構いません。 |
| ⑥ | **媒体・保存先** | 情報資産の媒体や保存場所をリストから選択してください。書類と電子データの両方を保有している場合は２行に分けて記入してください。この項目から脅威と脆弱性を想定します。 |
| ⑦ | **個人情報の種類** | 個人情報※1、要配慮個人情報※2、マイナンバーが含まれる場合は、該当欄に「有」を記入します。 |
|  |  | ※1要配慮個人情報もマイナンバーも個人情報ですが、ここでは要配慮個人情報とマイナンバー以外の個人情報に「有」を記入してください。※2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等が含まれる個人情報 |
| ⑧ | **重要度** | 情報資産の機密性、完全性、可用性のそれぞれの評価値（0～2）を選びます。3種類の評価値を計算した重要度（2～0） が表示されます。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** | 法律で定められた保存期限または利用目的が完了して廃棄や消去が必要となる期限を記入します。必要な期間以上に保有し続けるより廃棄・消去したほうがリスクが小さくなる場合に利用します。 |
| ⑩ | **登録日** | 情報資産管理台帳に登録した日付を記入します。内容に変更があった場合はその更新日に修正します。 |
| ⑪ | **脅威の発生頻度** | 「脅威の状況」シートにおける「対策を講じない場合の脅威の発生頻度」欄に記入された3段階の値のうち、媒体・保存先ごとにもっとも大きい値を示しています。（記入の必要はありません） |
| ⑫ | **脆弱性** | 「対策状況チェック」シートで選択された対策状況をもとに、脆弱性への対策状況を３段階で表示します。（記入の必要はありません） |
| ⑬ | **被害発生可能性** | 「脅威」と「脆弱性」をもとに、現状の対策状況で被害が発生する可能性を高・中・低の３段階で表示します。 |
| ⑭ | **リスク値** | 情報資産の「重要度」と「被害発生可能性」の積をもとにリスクの大きさを大・中・小の３段階で表示します。 |

6 / 11 ページ

中小企業の情報セキュリティ対策ガイドライン 付録7 リスク分析シート「情報資産管理台帳(Ver.1.4)」

情報資産管理台帳

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 業務分類 | 情報資産名称 | 備考 | 利用者範囲 | 管理部署 | 媒体・保存先 | 個人情報の種類 | | | 評価値 | | | | 保存期限 | 登録日 | 現状から想定されるリスク（入力不要・自動表示） | | | | | |
| 個人情報 | 要配慮  個人情  報 | マイナンバー | 機密性 | 完全性 | 可用性 | 重要  度 | 脅威（「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 | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

中小企業の情報セキュリティ対策ガイドライン 付録7 リスク分析シート「脅威の状況」

脅威の状況シート

|  |  |  |  |
| --- | --- | --- | --- |
| **媒体・保存先** | **個別の脅威**  （考えられる典型的な脅威） | **対策を講じない場合の脅威の発生頻度**  （1～3から選択） | **対策状況**  （対策状況チェックシートに入力すると自動で表示） |
| **書類** | 秘密書類の事務所からの盗難 |  |  |
| 秘密書類の外出先での紛失・盗難 |  |  |
| 情報搾取目的の内部不正による書類の不正持ち出し |  |  |
| 業務遂行に必要な情報が記載された書類の紛失 |  |  |
| **可搬電子媒体** | 秘密情報が格納された電子媒体の事務所からの盗難 |  |  |
| 秘密情報が格納された電子媒体の外出先での紛失・盗難 |  |  |
| 情報搾取目的の内部不正による電子媒体の不正持ち出し |  |  |
| 業務遂行に必要な情報が記載された電子媒体の紛失 |  |  |
| **事務所PC** | 情報搾取目的の事務所PCへのサイバー攻撃 |  |  |
| 情報搾取目的の事務所PCでの内部不正 |  |  |
| 事務所PCの故障による業務に必要な情報の喪失 |  |  |
| 事務所PC内データがランサムウェアに感染して閲覧不可 |  |  |
| 不正送金を狙った事務所PCへのサイバー攻撃 |  |  |
| **モバイル機器** | 情報搾取目的でのモバイル機器へのサイバー攻撃 |  |  |
| 情報搾取目的の不正アプリをモバイル機器にインストール |  |  |
| 秘密情報が格納されたモバイル機器の紛失・盗難 |  |  |
| **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 |  |  |
| 情報搾取目的の社内サーバーでの内部不正 |  |  |
| 社内サーバーの故障による業務に必要な情報の喪失 |  |  |
| **社外サーバー** | 安易なパスワードの悪用によるアカウントの乗っ取り |  |  |
| バックアップを怠ることによる業務に必要な情報の喪失 |  |  |

中小企業の情報セキュリティ対策ガイドライン 付録7 リスク分析シート「対策状況チェック」

対策状況チェックシート

|  |  |  |
| --- | --- | --- |
| **情報セキュリティ対策の種類** | **情報セキュリティ診断項目** | **回答値** |
| **(1) 組織的対策** | **経営者の主導で情報セキュリティの方針を示していますか？** |  |
| **情報セキュリティの方針に基づき、具体的な対策の内容を明確にしていますか？** |  |
| **情報セキュリティ対策を実施するための体制を整備していますか？** |  |
| **情報セキュリティ対策のためのリソース（人材、費用）の割当を行っていますか？** |  |
| **(2) 人的対策** | **秘密情報を扱う全ての者（パートタイマー、アルバイト、派遣社員、顧問、社内に常駐する委託先要員などを 含む）に対して、就業規則や契約などを通じて秘密保持義務を課していますか？** |  |
| **従業員の退職に際しては、退職後の秘密保持義務への合意を求めていますか？** |  |
| **会社の秘密情報や個人情報を扱うときの規則や、関連法令による罰則に関して全従業員に説明しています か？** |  |
| **(3) 情報資産管理** | **管理すべき情報資産は、情報資産管理台帳を作成するなど何処にどのようなものがあるか明確にしています か？** |  |
| **秘密情報は業務上必要な範囲でのみ利用を認めていますか？** |  |
| **秘密情報の書類に㊙マークを付けたり、データの保存先フォルダを指定するなど識別が可能な状態で扱って いますか？** |  |
| **秘密情報を社外へ持ち出す時はデータを暗号化したり、パスワード保護をかけたりするなどの盗難・紛失対策 を定めていますか？** |  |
| **秘密情報は施錠保管やアクセス制限をして、持ち出しの記録やアクセスログをとるなど取り扱いに関する手順 を定めていますか？** |  |
| **重要なデータのバックアップに関する手順を定め、手順が順守されていることを確認していますか？** |  |
| **秘密情報の入ったパソコンや紙を含む記録媒体を処分する場合、ゴミとして処分する前に、データの完全消 去用のツールを用いたり、物理的に破壊したりすることで、データを復元できないようにすることを定めていま すか？** |  |
| **(4) アクセス制御及び認証** | **業務で利用するすべてのサーバーに対して、アクセス制御の方針を定めていますか？** |  |
| **従業員の退職や異動に応じてサーバーのアクセス権限を随時更新し、定期的なレビューを通じてその適切性 を検証していますか？** |  |
| **情報を社外のサーバーなどに保存したり、グループウェアやファイル受渡サービスなどを用いたりする場合 は、アクセスを許可された人以外が閲覧できないように、適切なアクセス制御を行うことを定めていますか？** |  |
| **パスワードの文字数や複雑さなどを設定するＯＳの機能などを有効にし、ユーザーが強固なパスワードを使 用するようにしていますか？** |  |
| **業務で利用する暗号化機能及び暗号化に関するアプリケーションについて、その運用方針を明確に定めてい ますか？** |  |
| **(5) 物理的対策** | **業務を行う場所に、第三者が許可無く立ち入り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、など）を講じていますか？** |  |
| **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？** |  |
| **重要な情報やIT機器のあるオフィス、部屋及び施設には、許可された者以外は立ち入りできないように管理し ていますか？** |  |
| **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・記録媒体などの持込み・利用を禁止しています か？** |  |
| **(6) IT機器利用** | **セキュリティ更新を自動的に行うなどにより、常にソフトウェアを安全な状態にすることを定めていますか？** |  |
| **ウイルス対策ソフトウェアが提供されている製品については、用途に応じて導入し、定義ファイルを常に最新 の状態にすることを定めていますか？** |  |
| **業務で利用するIT機器に設定するパスワードに関するルール（他人に推測されにくいものを選ぶ、機器や サービスごとに使い分ける、他人にわからないように管理する、など）を定めていますか？** |  |
| **業務で利用する機器や書類が誰かに勝手に見たり使ったりされないようにルール（離席時にパスワード付き のスクリーンセーバーが動作する、施錠できる場所に保管する、など）を定めていますか？** |  |
| **業務で利用するIT機器の設定について、不要な機能は無効にする、セキュリティを高める機能を有効にする などの見直しを行うことを定めていますか？** |  |
| **社外でIT機器を使って業務を行う場合のルールを定めていますか？** |  |
| **個人で所有する機器の業務利用について、禁止するか、利用上のルールを定めていますか？** |  |

1. / 11 ページ

中小企業の情報セキュリティ対策ガイドライン 付録7 リスク分析シート「対策状況チェック」

|  |  |  |
| --- | --- | --- |
| **情報セキュリティ対策の種類** | **情報セキュリティ診断項目** | **回答値** |
|  | **受信した電子メールが不審かどうかを確認することを求めていますか？** |  |
| **電子メールアドレスの漏えい防止のためのBCC利用ルールを定めていますか？** |  |
|  | **インターネットバンキングやオンラインショップなどを利用する場合に偽サイトにアクセスしないための対策を 定めていますか？** |  |
|  | **IT機器の棚卸（実機確認）を行うなど、社内に許可なく設置された無線LANなどの機器がないことを確認して いますか？** |  |
| **(7) IT基盤運用管理** | **サーバーには十分なディスク容量や処理能力の確保、停電・落雷などからの保護、ハードディスクの冗長化な どの障害対策を行っていますか？** |  |
| **業務で利用するすべてのサーバーに対して、脆弱性及びマルウェアからの保護のための対策を講じています か？** |  |
| **記憶媒体を内蔵したサーバーなどの機器を処分または再利用する前に、秘密情報やライセンス供与されたソ フトウェアを完全消去用のツールを用いたり、物理的に破壊したりすることで、復元できないようにすることを 定めていますか？** |  |
| **業務で利用するすべてのサーバーやネットワーク機器に対して、必要に応じてイベントログや通信ログの取得 及び保存の手順を定めた上で、ログを定期的にレビューしていますか？** |  |
| **重要なITシステムに脆弱性がないか、専用ツールを使った技術的な診断を行うことがありますか？** |  |
| **ファイアウォールなど、外部ネットワークからの影響を防ぐための対策を導入していますか？** |  |
| **業務で利用しているネットワーク機器のパスワードを初期設定のまま使わず、推測できないパスワードに変更 して運用していますか？** |  |
| **クラウドサービスなどの社外サーバーを利用する場合は、費用だけでなく、情報セキュリティや信頼性に関す る仕様を考慮して選定していますか？** |  |
| **最新の脅威や攻撃についての情報収集を行い、必要に応じて社内で共有していますか？** |  |
|  | **情報システムの開発を行う場合、開発環境と運用環境とを分離していますか？** |  |
| **(8) システム開発及び保守** | **セキュリティ上の問題がない情報システムを開発するための手続きを定めていますか？** |  |
|  | **情報システムの保守を行う場合、既知の脆弱性が存在する状態で情報システムを運用しないようにするため の対策を講じていますか？** |  |
|  | **契約書に秘密保持（守秘義務）、漏洩した場合の賠償責任、再委託の制限についての項目を盛り込むなどの ように、委託先が順守すべき事項について具体的に規定していますか？** |  |
| **(9) 外部委託管理** | **委託先との秘密情報の受渡手順を定めていますか？** |  |
|  | **委託先に提供した秘密情報の廃棄または消去の手順を定めていますか？** |  |
|  | **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、事故の発生に備えた 準備をしていますか？** |  |
| **(10) 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** | **インシデントの発生に備えた証拠情報の収集手順を定め、運用していますか？** |  |
|  | **インシデントの発生で事業が中断してしまったときに再開するための計画を定めていますか？** |  |
|  | **個人番号及び特定個人情報の取り扱いルール（管理担当者の割当て、収集・利用・保管・廃棄の方法）を定 めていますか？** |  |
| **(11) 個人番号及び特定個人情**  **報の取扱い** | **個人番号や特定個人情報に関する漏えいなどの事故に備えた体制を整備していますか？** |  |
|  | **個人番号や特定個人情報の安全管理についてルールや手段を定めていますか？** |  |

1. / 11 ページ

中小企業の情報セキュリティ対策ガイドライン 付録7 リスク分析シート「診断結果」

診断結果

＜凡例＞

**◎** 情報資産台帳の内容にかかわらず必要**〇** リスク値算定の結果必要

**△** 情報資産管理台帳からは判断不可能

**—** リスク値算定の結果不要

|  |  |  |  |
| --- | --- | --- | --- |
| **対策の種類**  **（情報セキュリティ関連規程項目）** | **情報セキュリティ関連規程策定の必要性** | **対策状況チェック**  **の診断結果**  **（対策の実施率）** | **<付録6>**  **情報セキュリティ関連規程による**  **対策規定の要否** |
| **(1) 組織的対策** | **◎** |  |  |
| **(2) 人的対策** | **◎** |  |  |
| **(3) 情報資産管理** | **－** |  |  |
| **(4) アクセス制御及び認証** | **－** |  |  |
| **(5) 物理的対策** | **◎** |  |  |
| **(6) IT機器利用** | **－** |  |  |
| **(7) IT基盤運用管理** | **－** |  |  |
| **(8) システム開発及び保守** | **△** |  |  |
| **(9) 外部委託管理** | **△** |  |  |
| **(10) 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** | **◎** |  |  |
| **(11) 個人番号及び特定個人情報の取**  **扱い** | **－** |  |  |

**情報資産管理台帳に基づく管理すべき情報資産の状況**

|  |  |  |
| --- | --- | --- |
|  | | **情報資産の件数** |
| **媒体・保存先ごとの件数** | **書類** | **0件** |
| **可搬電子媒体** | **0件** |
| **事務所PC** | **0件** |
| **モバイル機器** | **0件** |
| **社内サーバー** | **0件** |
| **社外サーバー** | **0件** |

|  |  |  |
| --- | --- | --- |
|  | | **個人情報の件数** |
|  | **個人情報** | **0件** |
| **個人情報の**  **種類別件数** | **要配慮情報** | **0件** |
|  | **マイナンバー** | **0件** |

|  |  |  |
| --- | --- | --- |
|  | | **情報資産の件数** |
| **情報資産の重要度** | **重要度：2** | **0件** |
| **重要度：1** | **0件** |
| **重要度：0** | **0件** |