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。

(2)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。

(3)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。

(4)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。

(5)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。

(6)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。

(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、セキュリティベンダーなど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ISAC[9]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/

■ IPA セキュリティセンター
https://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

■ JPCERT/CC
https://www.jpcert.or.jp/

■警察庁 @police
https://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.jp/

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

(2) 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**

ウェブサイトでの運営形態によってセキュリティ対策が異なるため、**自社の状態に見合った運営形態**を検討しましょう。

ウェブサイトの**技術的な脆弱性を認識**したうえで、必要なセキュリティ対策を設計・開発の段階から検討しましょう。

運用開始後に発覚した情報セキュリティ上の問題にも適切に対応し、**ウェ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。

【表８】運営形態ごとの特徴

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。

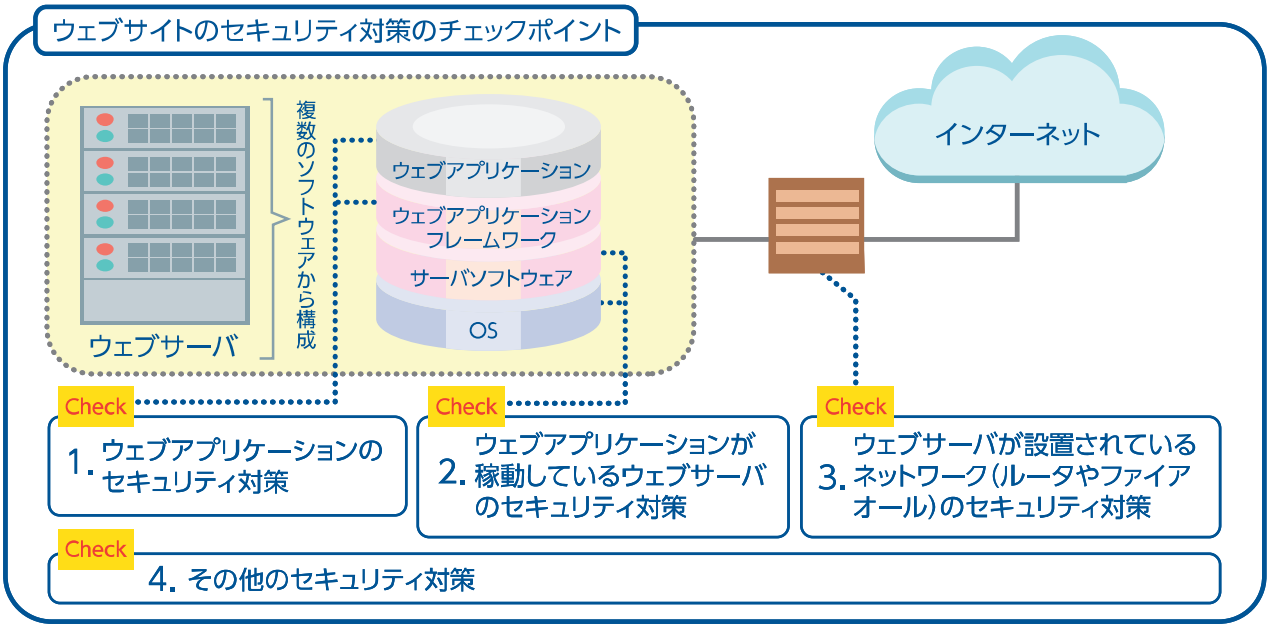
②ウェブサイトの構築

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。



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
・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

■安全なウェブサイトの作り方（IPA）
https://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

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

(3) 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。
- **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。

②クラウドサービスの運用

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。

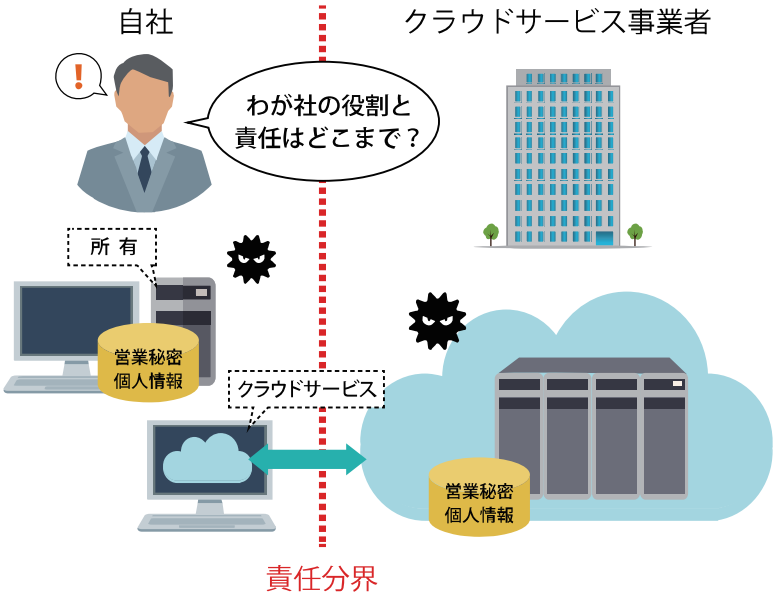
このことから、セキュリティ対策のための利用者の役割と責任の範囲は、利用者が直接管理することができるパソコンやスマートフォンなどの端末機器や、それらにインストールされたソフトウェアに限定されるため、自社所有の情報システムよりも、ハードウェアやソフトウェアへの対策に関する負担は軽減されます。しかし、クラウドサービスはインターネットを介したサービスのため、いつでも、どこからでも、誰でもアクセス可能であることが、自社所有の情報システムとは根本的に異なり、インターネット特有の脅威やリスクを考慮して、運用上のセキュリティ対策を検討する必要があります。

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。



【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。
※ 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）

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。

●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。

Smart SME Supporter

(4) 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
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。

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

多くの情報セキュリティサービスの中から、専門知識をもたないサービス利用者が、サービス事業者の選定時にそのサービスの品質を判断することは容易ではありません。

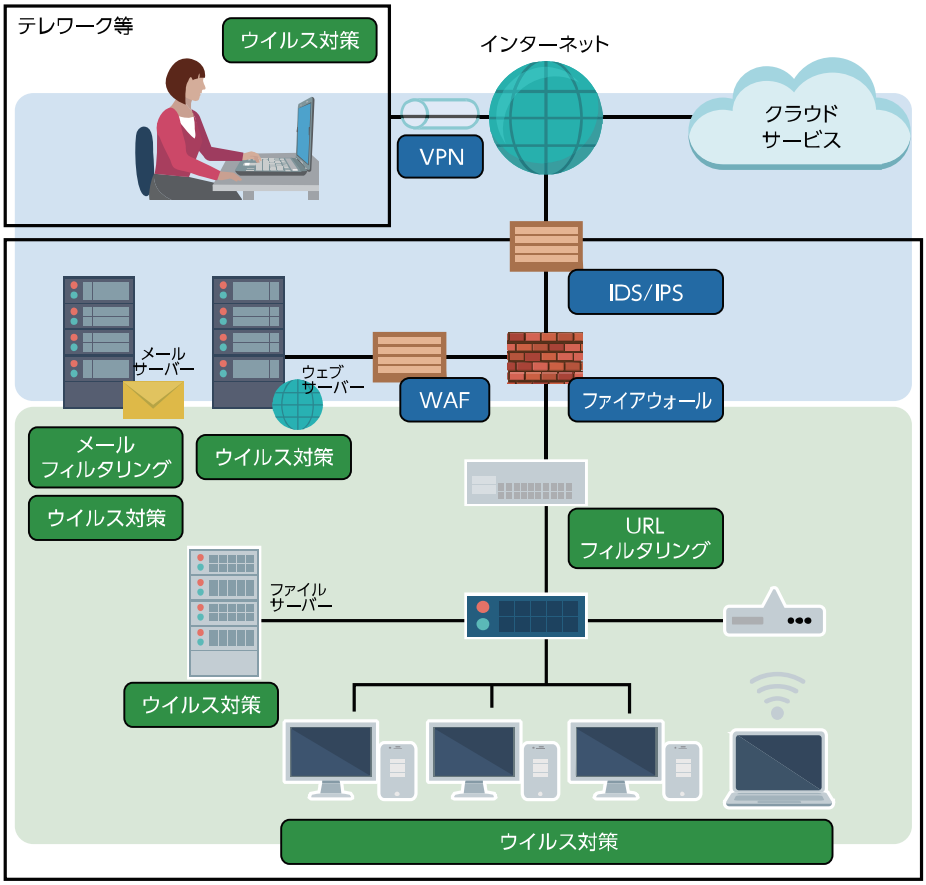
そこで、経済産業省では情報セキュリティサービスに関する一定の技術要件及び品質管理要件を示し、品質の維持・向上に努めている情報セキュリティサービスを明らかにするために「情報セキュリティサービス基準」を設け、この基準に適合するサービスの台帳を公開することで、品質の維持・向上に努めている情報セキュリティサービスを利用者に示し、その普及に結び付けることをねらいとした「情報セキュリティサービス基準審査登録制度」を開始しました。

IPAでは、この「情報セキュリティサービス基準」に適合する情報セキュリティサービスの提供状況について調査を行い、情報セキュリティサービスを利用しようとする者が参照することができるように、「情報セキュリティサービス基準適合サービスリスト」として公開しています。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。

●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

(5) 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。



①ネットワーク脅威対策

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。

●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、不正アクセスと思われる通信を検知して管理者に通知するとともに通信を遮断できます。

●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。

●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。

●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。

●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。

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。

(6) 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

どのような情報資産があるか洗い出して重要度を判断する

業務で利用する電子データや書類を**「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

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[11] 2～0を記入します。

●機密性・完全性・可用性の評価値から重要度を算定

重要度は、機密性、完全性、可用性いずれかの最大値で判断します。前項の作業で「情報資産管理台帳」の所定欄に記入した機密性・完全性・可用性の評価値をもとに、表11の判断基準に従い、重要度を算定します。

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

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	漏えいすると事業に大きな影響がある	●見積書、仕入価格など顧客（取引先）との商取引に関する情報
	0	漏えいしても事業に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	改ざんされると事業に大きな影響がある	●自社の会計情報 ●受発注・決済・契約情報 ●ホームページ掲載情報
	0	改ざんされても事業に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**

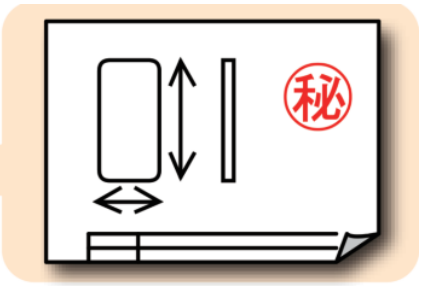
完全性:改ざんや無断の変更があると、製造に支障がある…… **評価＝1**

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



●『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**

情報資産管理台帳　重要度欄

評価値			重要度
機密性	完全性	可用性	
0	2	2	2

完全性と可用性の2が最大値なので重要度は2

付録の利用方法（手順１）

「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
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」 〈特定個人情報〉 個人番号（マイナンバー）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。

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
◆ 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。

●中規模企業の場合、管理部署ごとにシートを分けて作成すると、内容の見直しの際に便利です。

手順2　リスク値の算定

優先的・重点的に対策が必要な情報資産を把握する

手順１で洗い出した情報資産について、対策の優先度を決めるため、リスク値（リスクの大きさ）を算定します。リスク値を算定するにはい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

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

× 掛け算

算定のしかたは表15参照

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

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

被害発生可能性	3高	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中	特定の状況で被害が発生する（年に数回程度）
	1低	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、起きても被害は受容範囲

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)			リスク値	
		脅威	脆弱性		a×b	
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

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

計算式　脅威÷(4－脆弱性)　小数第1位を切り上げ

付録の利用方法（手順２）

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」の分類

「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」の識別

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

社内サーバー	情報窃取目的の社内サーバーへのサイバー攻撃	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）
	情報窃取目的の社内サーバーでの内部不正	2：特定の状況で脅威が発生する（年に数回程度）
	社内サーバーの故障による業務に必要な情報の喪失	1：通常の状況で脅威が発生することはない

媒体・保存先　個別の脅威　脅威の発生頻度（1～3から選択）

③「脆弱性」の認識

「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「実施状況」欄に表示されるリストから１～４のいずれかを選択します。

(6) 物理的セキュリティ対策	業務を行う場所に、第三者が許可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？	2：一部実施している
	最終退出者は事務所を施錠し退出の記録（日時・退出者）を残すなどのように、事務所の施錠をしていますか？	1：実施している
	高いセキュリティを確保する区域には、許可された者以外は接近できないような保護措置がなされていますか？	3：実施していない／わからない
	秘密情報を保管および扱う場所への個人所有のパソコン・記録媒体等の持込み・利用は禁止されていますか？	4：自社に該当しない

情報セキュリティ診断項目（チェック項目）　実施状況（1～3+4:自社に該当しない）

④リスク値の算定

以上①から③を記入すると「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　優先的に対策を実施
- リスク中　対策を実施
- リスク小　現状維持

現状の状況から想定されるリスク（入力不要・自動表示）					
脅威の発生頻度 ※「脅威の状況」シートに入力すると表示	脆弱性※「対策状況チェック」シートに入力すると表示	被害発生可能性		リスク値	
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：部分的に対策を実施している	2	可能性：中	4	リスク大
2：特定の状況で脅威が発生する（年に数回程度）	2：部分的に対策を実施している	1	可能性：低	2	リスク中

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

手順3 情報セキュリティ対策の決定

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

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。

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

事故が発生しても受容できる、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。

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

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はクレジットカード番号を非保持化し、決済業務をセキュリティ対策を十分行っている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。

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。

情報セキュリティ対策の種類（付録5 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）	対策検討・実施の要否
1	組織的対策	◎	62.5%	不足する対策を検討・実施してください
2	人的対策	◎	33.3%	不足する対策を検討・実施してください
3	情報資産管理	○	14.3%	不足する対策を検討・実施してください
4	アクセス制御及び認証	○	100.0%	対策を維持し適切性・妥当性・有効性を継続的に改善してください

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。

コラム

「情報セキュリティに関連した保険商品」とは

個人情報保護法の施行後、個人情報を漏えいしてしまった企業に対して、損害賠償金ならびに法律相談、事故対応、見舞金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

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

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。
例)P.44(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/

[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。

※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

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。

(情報の)機密性

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

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。

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。

③NIST(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

独立行政法人**情報処理推進機構**

〒113-6591

東京都文京区本駒込２丁目28番８号 文京グリーンコートセンターオフィス

URL　https://www.ipa.go.jp

電話　03-5978-7508　　FAX　03-5978-7546

E-mail　isec-pr-nw@ipa.go.jp