国民のための
サイバーセキュリティサイト

総務省

事前対策

（セキュリティ事故を未然に防ぐためには）

経営層向けの対策

企業や組織にとって、情報セキュリティ対策は、いまや重要な経営課題のひとつです。

情報セキュリティ対策には、組織全体の基本方針の策定や、適切な投資が必要であり、組織幹部の意志決定が欠かせません。組織幹部には、自分たちの組織にはどのような情報資産があり、どのようなリスクがあるかを把握した上で、自ら率先して情報セキュリティ対策の指揮を執ることが求められます。

ここでは、組織幹部（経営層）の向けに情報セキュリティ対策の必要性および、経営層にて主導すべき情報セキュリティポリシーの策定、見直しについて説明します。

経済産業省と独立行政法人情報処理推進機構では、大企業及び中小企業（小規模事業者を除く）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、「サイバーセキュリティ経営ガイドライン」を公開しています。

独立行政法人情報処理推進機構では、中小企業の経営者や実務担当者が情報セキュリティ対策の必要性を理解し、社内において対策を実践する際の具体的な手順を示すため、「中小企業の情報セキュリティ対策ガイドライン」を公開しています。

目次

情報セキュリティ対策の必要性

いまや情報システムやインターネットは、企業や組織の運営に欠かせないものになりました。しかし、現在の企業や組織は、情報システムへの依存による利便性の向上と引き換えに、大きな危険性を抱え持つことになってしまいました。

情報システムの停止による損失、顧客情報の漏洩（ろうえい）による企業や組織のブランドイメージの失墜など、情報セキュリティ上のリスクは、企業や組織に大きな被害や影響をもたらします。また、多くの場合、被害や影響は取引先や顧客などの関係者へも波及します。

サイバーセキュリティは経営課題のひとつとして考える必要がある

企業や組織にとって、情報セキュリティに対するリスクマネジメントは重要な経営課題のひとつと考えなければなりません。特に、個人情報や顧客情報などの重要情報を取り扱う場合には、これを保護することは、企業や組織にとっての社会的責務でもあります。

今日、情報セキュリティ対策は、世界的にも重要な経営課題であると認識されており、情報セキュリティ製品・システム評価基準（ISO/IEC15408）や情報セキュリティマネジメントシステムの認証基準（ISO/IEC27001）が、国際標準として規格化されています。情報セキュリティ対策の重要度が高まるにつれて、日本国内においても、これらの国際基準を採用する企業が増えてきています。

情報セキュリティポリシーの策定

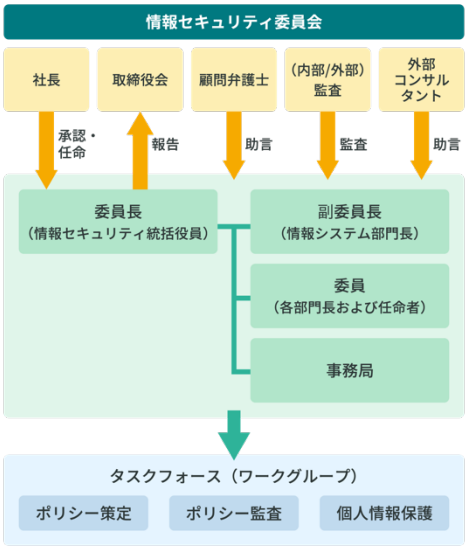
企業の情報資産を情報セキュリティの脅威から守るために情報セキュリティポリシーを策定する必要があります。

情報セキュリティポリシーを策定する際にもっとも大切なことは、担当者、体制、手順をあらかじめ検討しておくということです。また、情報セキュリティポリシーは、企業や組織の代表者が施行するものであるため、可能な限り、代表者や幹部が策定の作業自体にも関わるような体制を作ることが重要です。

■　策定のための体制作り

情報セキュリティポリシーを策定し運用するには、まず責任者を明確にして、情報セキュリティポリシー策定に携わる人材を組織化することが必要になります。この組織の活動内容が情報セキュリティポリシーの策定・運用の成果に大きく影響するため、企業や組織の実情や現在の社会状況に見合った情報セキュリティポリシーを策定・運用するためには、適切な人材を確保する必要があります。また、情報セキュリティポリシーの品質を高めるためには、外部のコンサルタントや法律の専門家に参加を依頼することも検討するとよいでしょう。

ただし、外部のコンサルタントに策定の全てを依頼することはふさわしくありません。これは、組織内の者によって情報セキュリティポリシーを策定しなければ、その企業や組織に適した内容にすることが困難であるためです。できるだけアドバイザなどの形で協力してもらうようにしましょう。



コラム：個人情報取扱い事業者の責務

情報セキュリティポリシーを策定する上で、法律違反やコンプライアンス違反にならないようにするために組織としてどうすればよいか検討することも重要な要素となります。
少し古い事例にはなりますが、2005 年 4 月に個人情報保護法が全面施行され、個人情報取扱事業者に対し、以下のことを義務付けています。

- 個人情報を取り扱うに当たっては利用目的をできる限り特定し、原則として利用目的の達成に必要な範囲を超えて個人情報を取り扱ってはならない。
- 個人情報を取得する場合には、利用目的を通知・公表しなければならない。なお、本人から直接書面で個人情報を取得する場合には、あらかじめ本人に利用目的を明示しなければならない。
- 個人データを安全に管理し、従業員や委託先も監督しなければならない。
- あらかじめ本人の同意を得ずに第三者に個人データを提供してはならない。
- 事業者の保有する個人データに関し、本人からの求めがあった場合には、その開示を行わなければならない。
- 事業者が保有する個人データの内容が事実でないという理由で本人から個人データの訂正や削除を求められた場合、訂正や削除に応じなければならない。
- 個人情報の取扱いに関する苦情を、適切かつ迅速に処理しなければならない。

※個人情報保護委員会の命令に違反した場合や、報告義務に違反した場合には、罰則が科せられる場合があります。

- 個人情報保護委員会の命令に違反した者に 1 年以下の懲役 又は 100 万円以下の罰金、法人に対しては 1 億円以下の罰金
- 報告義務に違反した場合 50 万円以下の罰金

個人情報の取扱いに関する詳細については、個人情報保護委員会のサイトにガイドラインや相談窓口など有用な情報が掲載されています。
https://www.ppc.go.jp/

情報セキュリティポリシーの見直し

情報セキュリティポリシーは、運用を開始した後にも、社員や職員の要求や社会状況の変化、新たな脅威の発生などに応じて、定期的な見直しが必要です。また、見直しを行った結果、必要に応じて情報セキュリティポリシーを改訂しなければなりません。この作業を継続的に繰り返すことが、情報セキュリティ対策の向上に役立ちます。

以下のような情報セキュリティマネジメントの実施サイクル(PDCA サイクル)によって、実態に沿った内容になっているかを常にチェックし、絶えず見直し、改善を図ることが大切です。

■ 計画(Plan)：

情報資産の洗い出しを行い、リスクや課題を整理し、組織や企業の状況に合った情報セキュリティ対策の方針を定めた情報セキュリティポリシーを策定する。

■ 導入・運用(Do)：

全社員・全職員に周知し、必要に応じて、集合研修などの教育を行う。 社員・職員が情報セキュリティポリシーに則って行動することで、目的とする情報セキュリティレベルの維持を目指す。

■ 点検・評価(Check)：

情報セキュリティ上のリスクは、常に変化するため、常に最新の情報セキュリティ関連の情報を収集する。そして、収集した情報や現場の状況や問題点などを参考にして、現在の情報セキュリティポリシーの内容に不足している項目がないかどうかを評価する。また、遵守されているかどうかの監査も行う。

■ 見直し・改善(Act)：

点検・評価の内容を参考にして、情報セキュリティポリシーの見直し・改善を行う。

情報セキュリティポリシーは、企業や組織の状況、新たな脅威、新しい法律の施行など社会的な状況によっても、定期的に見直さなければなりません。そのためにも、このようなサイクルを継続的に実施することで、常に適切なものにしておくことが大切です。