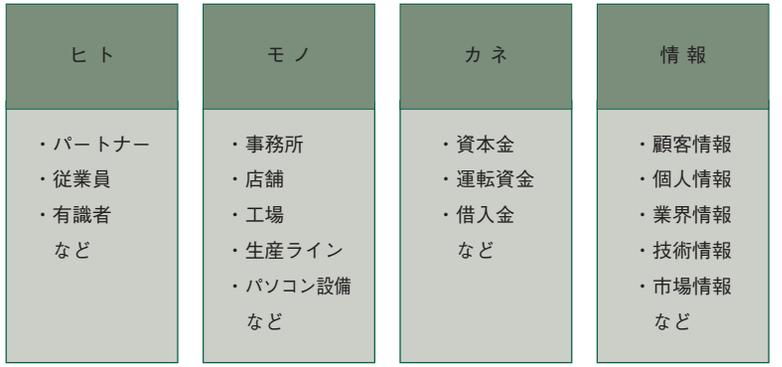
図2-1：企業の経営資源



情報の適切な取り扱いは企業経営の重要課題

企業は、事業活動を行ううえで、製造や開発に関わる設計情報、顧客リスト、個人情報、営業機密、運用マニュアル、著作権などの知的財産など多くの情報を取り扱い、活用することで付加価値あるサービスを顧客へ提供します。また、これら情報の取り扱いを適切に行うことで、顧客や株主、取引先、関係会社といったステークホルダーとの信頼関係を構築し、ビジネスを成長させることも可能です。しかし、万一、情報の取り扱いに関する事故（企業が保有する顧客情報や個人情報といった機密情報の漏えいなどのインシデント）を起こしてしまった場合には、社会的信用を失うなど、企業経営に深刻な影響を及ぼします。

自社の新規プロジェクトに関する情報が外部に漏えいすれば、他社との競争や差別化に影響がでるかもしれません。また、自社の情報のみならず、顧客情報を漏えいした場合には、企業の信用問題に関わる事態となり、契約解除や顧客離れ、サービス停止など、事業への深刻な影響が発生することでしょう。自社が起こしたセキュリティ事故により、顧客や取引先へも被害が影響してしまった場合には、顧客や取引先から損害賠償を請求されることをあり得ますし、法的な責任を問われることもあります。

どんなに順調に成長しているビジネスであっても、社会的信用を失えば、顧客離れや機会損失などにより、あっという間に事業は立ち行かなくなり、事業継続は困難になるでしょう。最悪の場合は、事業停止、倒産も考えられます。情報に関するセキュリティに関する事故は、巨額な損失が発生するだけではなく、社会的信用の低下や失墜といった、企業の事業継続に致命的な影響を与える可能性があります。情報が適切に取り扱われない場合、企業の事業活動に大きく影響を及ぼす可能性があるため、これらリスクを適切に管理することが企業には求められます。情報の適切な取り扱いは、企業経営の重要課題として、また、危機管理の一環として、企業経営にとっては不可欠な取り組みと言えます。

情報セキュリティの推進なき事業活動は、例えるならブレーキやシートベルトのない自動車で、ひたすらアクセルを踏んでいるようなものです。スピードが出る自動車ほど、安全装置はより強固に、より万全にしておくべきです。自社の事業を全力で推進できるよう、全力でアクセルを踏むためにも、情報セキュリティはとくに力を入れて推進することを強く推奨します。

2-2：守るべき情報資産とは

企業の事業活動に欠かせない重要な情報は、価値ある資産であり、守るべき情報です。

こういった企業にとって守るべき価値ある情報のことを「情報資産[注1]」と呼びます。情報資産には、紙媒体である書類や電子データなどの「情報」だけではなく、情報を生成・保管・処理・利用する「情報システム」も含めて考えます。

企業では、事業の内容に応じて、さまざまな情報が活用されます（**表2-1**）。商品を開発や製造する際に得られた技術情報や研究データ、営業活動で得られた顧客情報や取引先情報、経営資源を管理するために必要となる人事情報や財務情報、またこれら情報を利用するために必要となる業務パソコンやサーバシステムといった情報システムなど、企業の中には、非常に多くの情報資産が存在します。

これらの情報が、何らかの理由で、利用不可や改ざん、欠損、漏えいといった事態が発生した場合、情報資産の重要性（価値）に応じて、事業へ影響が発生することになります。

注1）情報セキュリティマネジメントシステム（ISMS）の要求事項を定義している ISO/IEC27001（国際規格）では、「情報」と「情報システム」も含めて「資産（Asset）」という言葉が使用されていますが、JIS Q27001（日本工業規格）では、財務会計等における資産と区別するため、「情報資産」という言葉が使用されています。

●機密性

情報にアクセスして良い人を限定することで、情報の秘匿性を確保することです。つまり「情報を秘密にする状態」を確保することです。企業活動では、従業員だけがアクセスできる社外秘の情報や、特定プロジェクトの関係者だけがアクセスを許可された案件情報などを「機密性が高い情報」や「機密情報」などと言います。機密性が確保されない場合、組織の重要情報が第三者へ漏えいするリスクに繋がります。

●完全性

情報の伝達や受け渡しの際に、「情報に間違いがない状態」を確保することです。例えば、AさんからBさんへ情報を送信する際に、送信経路の途中で情報の改ざんや欠如が発生すると、正しい情報の取り扱いはできなくなります。電子証明書を利用したデジタル署名などの技術を利用して、完全性を確保します。完全性が確保されないと、情報の偽造や改ざんが発生するなど、データの信頼性が欠如し、正しい業務処理ができなくなる可能性があります。

●可用性

情報の利用を許可された人が、「いつでも利用できる状態」を確保することです。システム障害やサイバー攻撃などにより、システムやサービスが停止すると、情報の利用ができなくなります。その結果、製造販売ができなくなる事態や、顧客サービスが提供できなくなるなど、事業活動の売上低下に直結する深刻な事態が懸念されます。

情報資産の評価

情報資産の価値（重要度）を評価するには、機密性・完全性・可用性の3要素を指標とします。3要素の影響度は、それぞれ「情報資産が侵害された場合の組織や事業への影響度」を考慮して定義します。例えば、機密性が侵害された場合の影響度は**表2-3**のように定義できます。

他の要素も同様に、事業への影響に基づいて影響度を定義します。侵害を受けた場合に事業活動の影響が大きい資産ほど、企業にとっては重要な資産と言えます。機密性・完全性・可用性の3要素を基準として評価することで、情報資産の価値（重要度）を識別することが可能になります。

例えば、ダイヤモンドの鑑定では、「カット（輝き）」「カラット（重さ）」「カラー（色）」「クラリティ（透明度）」の4つのC（4C）で評価が行われますが、情報セキュリティにおける情報資産の評価は、機密性・完全性・可用性の3要素で評価されるとイメージするとよいでしょう（**表2-4**）。

表2-3：機密性が侵害された場合の影響度（例）

影響度	事業に対する影響（説明）
低	影響はほとんどない（社内の一部に影響が留まる場合など）
中	影響が一部発生する（全社で影響が出る場合など）
高	深刻な影響が発生する（顧客や取引先へも影響が出る場合など）

表2-4：宝石の鑑定と情報資産の評価（比較）

項目	宝石	情報資産
対象（例）	ダイヤモンド	顧客情報
評価指標	4C（カット、カラット、カラー、クラリティ）	3要素（機密性、可用性、完全性）
結果	A+など	重要度（1〜3など）
報告書／台帳	鑑定書	情報資産管理台帳

●情報セキュリティの目的

情報資産の価値が、機密性、完全性、可用性の3要素（CIA）で示されることは、情報セキュリティの目的も表しています。「情報を正常に維持すること」とは、3要素が侵害されずに、維持される状態を確保することです。つまり、情報セキュリティとは「情報の機密性、完全性、可用性を維持すること」なのです。

この3要素が維持されている状態であれば、情報セキュリティは侵害されていない、と言えます。また、3要素のいずれかが一部でも欠けた状態となると、情報セキュリティは侵害された状態となり、この侵害された事象のことを「情報セキュリティインシデント（セキュリティ事故）」と呼びます。

情報セキュリティインシデントが起こることで、企業の事業活動は影響を受けます。情報セキュリティインシデントによる企業の事業継続への影響を最小限とするために、情報セキュリティ対策が必要となります。

基本方針書のサンプル

実際に基本方針書を作成する場合に、一から文面をすべて考えるのは大変です。そこで、すでに作成されているサンプルを参考に、自社版の基本方針書を作成しましょう。ここでは、組織トップによる宣言をすることが重要な意味を持ちますので、記載内容そのものは、既存サンプル文書を流用し、作成する形で問題ありません。サンプルが自社に遭わない場合などは、文面を修正してください。

本書では、情報処理推進機構（IPA）から「中小企業の情報セキュリティ対策ガイドライン」の「付録2」として提供されているものをサンプルとして紹介します（図6-1）。

・中小企業の情報セキュリティ対策ガイドライン

URL https://www.ipa.go.jp/security/keihatsu/sme/guideline/

図6-1は、一般的な文面となっていますが、基本的な内容が簡潔に押さえられていて、非常によくできた基本方針書です。

とくに「経営者の責任」では、「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。」と力強く宣言しています。経営者は、先頭に立ってセキュリティ対策を行う責務がでてくるので、非常に良いです。また、「社内体制の整備」では、情報セキュリティのために「組織を設置すること」「社内の正式な規則とすること」が記載されており、「従業員の取組み」では従業員に対する「情報セキュリティの知識や技能を習得させること」まで記載されています。

方針書は、対外的にも宣言しますので、こういった「体制や規定類の整備」や「従業員への教育」の取り組みが記載された方針書を、組織のトップの名前で宣言することは、組織的な対策推進を行ううえでは、非常に重要な意味を持ちます（組織のトップに対して、セキュリティに取り組む責任を認識してもらう、良い機会にもなります）。

情報セキュリティ対策は、基本方針書を作成し、自社の情報資産だけではなく、事業活動で取り扱う顧客の重要情報を適切に保護することや社会的責任を果たすことなどを明確に宣言することから始めましょう。

図6-1：情報セキュリティ基本方針（サンプル）

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。
2. 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。
3. 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。
4. 法令およ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。
5. 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。

制定日：20○○年○月○日
株式会社○○○○
代表取締役社長　○○○○

出典：IPA（独立行政法人情報処理推進機構）、URL https://www.ipa.go.jp/files/000072146.docx

6-3：体制図／組織図

続いて推進体制を作りましょう。基本方針書でも「社内体制の整備」として、組織の設置を宣言しています。セキュリティを推進するための「体制整備」は、経営層の責務です。組織一丸となって取り組むためには、次のような観点が重要になります。

・経営者が積極的に参画すること（経営者を巻き込むこと）