情報セキュリティ報告書モデル

１．概要

情報セキュリティ報告書は、企業の情報セキュリティの取組の中でも社会的関心の高いものについて情報開示することにより、当該企業の取組が顧客や投資家などのステークホルダーから適正に評価されることを目指すものである。

情報セキュリティ報告書モデルの基本構成を表 1 に示す。なお、表 1 では、記載項目や内容のフルセットの例を提示しているが、企業はこれらの項目のうちから必要なものを選択できるものとする。このうち、下線がついている項目は、記載することが望ましい基本的な要素である。

表 1　情報セキュリティ報告書モデルの基本構成

①基礎情報

報告書の発行目的、利用上の注意、対象期間、責任部署等

②経営者の情報セキュリティに関する考え方

情報セキュリティに関する取組方針、対象範囲、報告書におけるステークホルダーの位置付け、ステークホルダーに対するメッセージ等

③情報セキュリティガバナンス

情報セキュリティマネジメント体制（責任の所在、組織体制、コンプライアンス等）、情報セキュリティに関わるリスク、情報セキュリティ戦略等

④情報セキュリティ対策の計画、目標

アクションプラン、数値目標等

⑤情報セキュリティ対策の実績、評価

実績、評価、情報セキュリティの品質改善活動、海外拠点の統制、外部委託、情報セキュリティに関する社会貢献活動、事故報告等

⑥情報セキュリティに係る主要注力テーマ

内部統制や個人情報保護、事業継続計画など特に強調したい取組、テーマの紹介、工夫した点等

⑦（取得している場合の）第三者評価・認証等

ISMS 適合性評価制度、情報セキュリティ監査、プライバシーマーク制度、情報セキュリティ関連資格者数、格付け／ランキング等

２．位置付け

情報セキュリティ報告書については、ステークホルダーへの説明責任遂行や新たな事業付加価値創出等、企業それぞれの目的に応じた策定を許容しつつ、企業にとって過度な負

担を避けるという観点から、以下のように位置付ける。

- 記載項目の選択や記載内容のレベルは、企業が自社の事情に応じて選択可能とする。
- 情報開示の方法については、CSR 報告書等の一部として組み込むことも、単体の報告書として公表することも可能とする。
- ただし、CSR 報告書等の一部とする場合、分量も制約があり、読者層・テーマが「CSR」を前提とするため、本来発するべきメッセージを適切な相手に伝えきれない可能性が高いことに留意する必要がある。
- 情報セキュリティ報告書の発行者の意見を踏まえると、
  - 営業秘密に係る情報管理や事業継続性といった観点からの取引先への説明責任
  - 従業員やグループ会社・外部委託先に対する意思統一・意識啓発
  - お客様に対するマーケティング効果やブランドイメージの向上

  といった効果を意図として情報開示を行うのであれば、単体の報告書（情報セキュリティ報告書）としての発行が効果的と考えられる。その場合には、CSR 報告書など他の報告書との連携・整合性を考慮することが望ましい。

３．想定される効果

（1）発行主体にとっての効果

情報セキュリティ報告書の発行主体にとって期待される効果としては、その立場やビジネスモデル等により図 1 のように想定される。

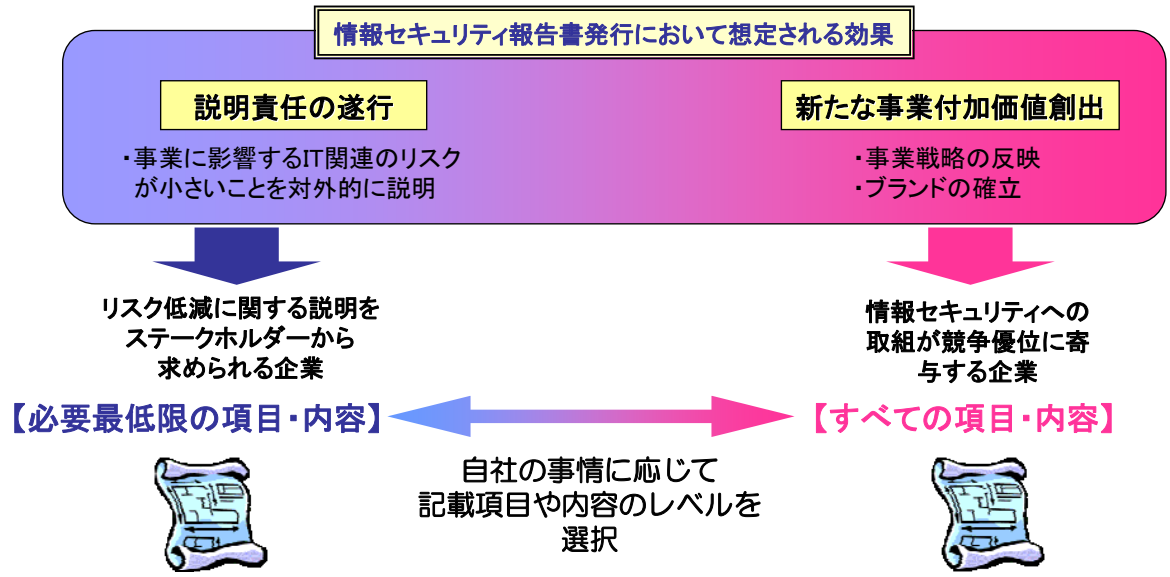


図 1　情報セキュリティ報告書発行において想定される効果

①説明責任の遂行

事業の IT 依存度が高まり、IT 事故が事業の存続すら脅かすリスクとなりつつある中、企業のステークホルダーは、今後 IT 事故に関するリスクに一層高い関心を示すものと見込まれる。このような状況の下、企業としては、情報セキュリティ報告書を通じて、当該リスクへの取組をステークホルダーに対して説明していくこと等が、その発展のために重

要となってくると考えられる。

特に、業界トップランナーと呼ばれる企業は、ステークホルダーからの信頼を獲得し、業界全体の健全な発展を先導するという立場から、情報セキュリティ報告書を率先して開示していくことが強く期待される。

また、セキュリティ報告書を準備･作成し対外的に説明する作業を通じて、経営者自身が情報資産とビジネスプロセスの関係を把握し説明責任を果たすことができるという効果もある。

②新たな事業価値の創出

主な商品やサービスが「IT」や「セキュリティ」に関連する企業や、収集した個人データをマーケティングなどに有効に活用する個人情報取扱事業者にとっては、提供する製品やサービスにおいてセキュリティを確保しておくことは当然のことながら、自社のセキュリティ向上への取組を対外的に公表することで､顧客からの支持を得て､企業価値の向上、競争優位の確保を狙うことができる。

このような効果を期待できる企業は、IT ベンダやセキュリティ関連企業、またネットビジネスやデータセンター等、ビジネスモデルが個人データや IT に強く依存している企業が想定される。

（2）ステークホルダーにとっての効果

情報セキュリティ報告書の読み手であるステークホルダーにとっての効果は、以下のように想定される。

①取引先　－　取引相手の信頼性の把握

取引先は、調達等における相手企業の安定的な事業継続や情報管理の状況に対し高い関心を寄せており、取引条件として第三者認証の取得を求めるケースも見られる。したがって、情報セキュリティ報告書による情報セキュリティの取組状況の開示は、こうしたニーズに合致するものと考えられる。また、個人情報管理について報告書の中で自身の委託先の選定基準を明示することにより、取引先の委託先選定時にアピールすることができる。

②従業員・グループ会社・外部委託先　－　意識の共通化、理解の向上

情報セキュリティ報告書を開示することによって、従業員の情報セキュリティに対する意識･理解を高め、対外的な説明を共通化・統一する効果が期待される。また、グループ会社や外部委託先など、統制が利きにくい領域に対しても、イメージを共有し、啓発する効果が得られる。

③顧客・消費者　－　マーケティング効果、ブランドイメージの向上

製品やサービスの購入者である顧客・消費者の最大の関心事の一つは､「顧客情報・個人情報の保護」である。情報セキュリティ報告書による情報セキュリティの取組状況の開示を通じて、こうした問題に誠意を持って取り組んでいることを訴求し、ブランドイメージを高める効果が期待できる。また、仮に IT 事故が発生した場合も、情報セキュリティ報告書をベースに、情報を隠すことではなく適切に開示することで顧客の信用回復を果たすことが可能になる。

④投資家、アナリスト　－　投資対象の評価

投資家やアナリストは、対象企業の業績や将来成長性を評価する上で、リスク情報やその対策に関する情報を活用する傾向がある。技術資産や営業情報、事業ノウハウといった企業価値を決定付ける主因子を管理するという観点から、情報セキュリティの意義は高まりつつあり、こうした情報発信を通じてリスクコンシャスな投資家・アナリストを育成する効果も期待できる。

⑤格付け機関・メディア・関連団体　－　分析材料の充実

企業の格付けは、一般に公開資料、企業への面接、業界内の情報、取引先からの情報、カントリーリスク等を格付け機関が分析して行うもので、市場にも大きな影響力を持つ。IT リスクが経営に及ぼす影響が今以上に大きくなれば、将来的にリスクマネジメントの視点から格付け機関が情報セキュリティ関連の開示情報を積極的に活用する可能性がある。また、メディアや関連団体から情報セキュリティに関する勝手格付けやランキング等が発表された場合には、上位を目指す企業がより積極的な開示を行う可能性もある。

４．留意事項

情報セキュリティ報告書を発行するにあたり留意すべき点を以下に示す。

①情報開示の範囲

情報開示の範囲や方向について誤ると、リスクを高める可能性もある。例えば、対策ツールの具体的な名称や設定などの情報は、ステークホルダーにとって必要ではない上に、攻撃者に有効なヒントを与えてしまう危険性がある。

また、同じ企業グループ内でも、所属各社の業務内容やセキュリティニーズには通常ばらつきがあることから、企業グループで共通の報告書を発行する場合には、どこまで記載するかについて何らかの基準と合意が必要になる。

②報告書の記載内容の信頼性

情報セキュリティ報告書は自己申告であるため、自社にとって不利な情報（例：事故情報等）について一切開示しないという判断もありうる。しかし、「安全性は完璧である」「全く問題はない」としか言わない場合、いざトラブルが発覚すると報告書の信頼性が問われるリスクもある。また、一社の虚偽報告が発覚すると、他社の報告書の内容まで疑われる可能性がある。

一つの考え方として、報告書の記載内容の正確性を担保するため、第三者の監査を受けその内容を保証してもらう方向が考えられる。

５．記載事項の詳細

◆発行主体は、自社の目的や事情に応じて必要な記載項目や内容のレベルを選択できる。ただし、網掛けの項目は記載することが望まれる基本的な項目である。

◆発行形態は、他の報告書の一部として組み込む形も、単体の報告書という形もあり得る。ただし、以下の効果を狙う場合には、情報セキュリティ報告書の発行が効果的である。

・営業秘密に係る情報管理や事業継続性といった観点からの取引先への説明責任
・従業員やグループ会社・外部委託先に対する意思統一・意識啓発
・お客様に対するマーケティング効果やブランドイメージの向上

表 2　情報セキュリティ報告書の記載項目の内容

記載項目（大）	記載項目（中）	主な内容
基礎情報	報告書の発行目的	・発行者側の意図 ・読者に期待すること
	報告書の利用上の注意	・積極的報告事項（特定の目的でつかってほしい）など ・消極的報告事項（意思決定に利用できるほどの詳細な情報ではない）など
	報告書の対象期間	対象とする年度
	報告書の責任部署（連絡先）	部署名のみ表示するケース、電話・FAX・メールを表示するケース、担当者まで明記するケースがある。
経営者の情報セキュリティに関する考え方	情報セキュリティに関する取組方針*1	情報セキュリティポリシーと関連する規程の種類、それぞれの位置付けや内容の概略について記載する。 ・情報セキュリティポリシー宣言、プライバシーポリシー宣言 ・情報セキュリティに関する経営者方針 ・情報セキュリティに係る企業のビジョン（企業理念に基づく情報セキュリティの考え方） ・経営者が認識する具体的課題と社会認識
	対象範囲*2	本報告書で対象とする範囲を規定する。範囲の規定方法としては、例えば以下の方向がある。 ・グループ会社の範囲 ・対象業務 ・対象となる情報（例：営業情報、顧客情報、技術情報、財務情報など） ・対象事業所 ・対象システム
	報告書におけるステークホルダーの位置付け、ステークホルダーに対するメッセージ等	本報告書において想定するステークホルダーの範囲と、それらに対するメッセージについて記載する。 ・経営者が考えるステークホルダーの特定 ・ステークホルダーに向けたメッセージ ・本報告書の開示によるステークホルダーの利益とリスク
	その他の事項	ビジネスに関わる経営指標のうち、情報セキュリティに影響する可能性があるものを記載する。

		＜社会的影響力＞ ・自社の価値（売上規模、ブランドイメージ） ・社会的責任（事業の公益性（国家、社会、経済メカニズム等）、消費者への影響（生命・身体・財産・名誉等）） ・重要情報の保有（国家機密、営業機密、プライバシー等） ＜事業構造上の脆弱性＞ ・基幹業務の情報システム依存（業種特性） ・業務の外部依存性（代理店等への依存度、インターネットへの依存度、正社員･非正社員の比率等） ・関与者の範囲（拠点数、海外拠点の有無、従業者の離職率等）
情報セキュリティガバナンス	情報セキュリティマネジメント体制*3	企業全体の情報セキュリティの推進体制について記述する。この推進体制とは、企業としての情報セキュリティに係る内部統制の核となる社内組織である。中でも、情報セキュリティ統括責任者をはじめとした経営層の意思決定組織（情報セキュリティ委員会など）は、情報セキュリティに係る企業のビジョンやポリシーの決定・承認、情報セキュリティ推進計画の承認や評価結果の承認などの役割を担う。 ・情報セキュリティ統括責任者（CISO）の設置 ・推進体制の構造（委員会方式／ワーキング方式、専門部署や各部署での責任者の設置状況、全体の俯瞰図等） ・各組織の権限と責任（委譲の場合はその内容） ・活動の頻度や主な内容 ・評価・見直し・報告の仕組み ・教育・研修の仕組み ・他の管理組織（リスクマネジメント、内部監査、コンプライアンス等）との関係 ・事業継続計画の策定状況 ・各種ガイドライン等の参照状況
	情報セキュリティに関わるリスク	自社が保有するリスクについて把握し、どのリスクに対して対策を実施し、どのリスクを受容するかを明らかにしておく必要がある。 ・対象となる情報（どのような情報に関してリスクがあるか） - 顧客情報（個人情報、取引情報、会社情報） - 営業機密（戦略情報、技術情報、財務情報） - 株主情報　等 ・情報セキュリティの”CIA”との関連 - 機密性（Confidentiality） - 完全性（Integrity） - 可用性（Availability） ・リスクの特徴（実施しているビジネスによる特異性、一般的なリスクとの違い等） ・リスクの許容度 ・リスクの発生可能性と影響（どの程度の発生可能性があるか、発生した場合どのような影響があるか、影響範囲等）

	情報セキュリティ戦略	ビジョン、ポリシー、リスクに基づき決定・実現される情報セキュリティ戦略（重点テーマ、実施方針等）について記述する。 ・重点テーマは、リスクを管理しビジョンやポリシーを実現するための策の方向性であり、3～5 年の中長期計画において目標とするテーマと考えることもできる。 （例）「当社は業務上多くの顧客情報を保有することから、その漏えいリスクをコントロールすること、すなわち『情報漏えい対策』に重点を置きます」 ・実施方針は、重点テーマの実現手段として選択した情報セキュリティ対策の取組であり、特に強調したいポイントを示す。ただし、実施方針を具体的に示すことで不要なリスクを高めてしまう可能性があるため、慎重かつ適切に開示する必要がある。以下に例を示す。 ＜重点テーマ例＞　＜実施方針例＞ 不正アクセス対策　→　「ファイアウォールと侵入検知装置を要所に設置し、24 時間の監視業務を委託」 情報漏えい対策　→　「重要情報の保管庫に入退室監視装置を設置」 「個人情報を扱うオペレーターに生体認証を義務付け」 システムの安定稼働　→　「システム開発時のバグ・脆弱性排除の徹底」 「各種システム・インフラの二重化」
情報セキュリティ対策の計画、目標	アクションプラン	情報セキュリティ戦略に沿った中長期計画・年次計画をもとに、情報セキュリティ対策に係るアクションプランを記載する。ただし、詳細なアクションプランを示すことで不要なリスクを高めてしまう可能性があるため、慎重かつ適切に開示する必要がある。 ・ISMS、プライバシーマーク等の認証取得計画（対象業務、対象事業所の段階的な拡大等） ・情報セキュリティ監査の段階的実施（対象業務ごとに課題（改善要求事項）の明確化とその対処計画を策定） ・情報セキュリティ要員の段階的増強・配置 ・社員へのｅラーニング研修の実施 ・技術的対策の導入
	数値目標*4	情報セキュリティ対策の実現に際し設定可能な数値目標がある場合には、それを記載する。具体的には、投資規模や、対策実施により得られる効果、情報セキュリティ対策の成熟度の向上/維持を示すデータ等が考えられる。 （例） ・人的投資（専任担当者・兼任担当者の人数、配置等） ・資金的投資（「情報セキュリティ対策」としての明確な意思と戦略を持って行う投資を想定） ・セキュリティテスト（スキャニング、侵入テスト等）の実施回数 ・重要情報の操作要員に対する情報セキュリティ研修の実施頻度 ・セキュリティ担当者に対する情報セキュリティ研修の実施頻度 ・情報セキュリティ対策ベンチマークのスコア ・ポリシーに基づく各種管理事項に関する経営層への報告の有無
情報セキュリティ対策の実績、評価	実績	情報セキュリティ対策のアクションプランや数値目標に係る達成状況を記載する。項目の内容は、「計画、目標」の欄で記載したアクションプランや数値目標と同様になる。

	実績に対する評価	計画・目標と実績の差やその原因についての自己評価を記載する。また、第三者による情報セキュリティ評価または監査の結果を、リスクに配慮した上で記載することも可能である。情報セキュリティ対策ベンチマーク*5の自己診断結果や、自ら設定した効果測定を提示することも可能。 （例） ・「事業環境の悪化により、当初の予算確保が困難となったため、今年度はここまでしかできなかった。」 ・「計画を上回るペースで対策の導入が進展したため、次年度分の事業についても一部着手した。」 ・「情報セキュリティ監査の結果、当社は情報セキュリティポリシーを適切に実現する形で情報セキュリティ対策の実施がなされていることが第三者である監査人から保証された。ただし、改善要求事項として7点の指摘を受けた。」
	情報セキュリティの品質改善活動	情報セキュリティ環境の維持・向上に資する社内の取組について記載する。いわゆるQC活動と同様、現場レベルで実践・浸透する取り組みが望ましい。 （例） ・現場レベルでの問題点・改善点に関するアイディア投稿の仕組み ・事故発生時の現場担当者による原因分析と改善提案 ・研修後のテスト結果の社内公開（部署間競争の促進） ・ヒヤリハット情報の収集・公開
	海外拠点の統制	本社から直接統制することが困難な海外事業所についてどのように対処しているかを記載する。特に海外での活動や管理方法に特徴がある場合、あるいは海外の事業所等に係わる新たな活動を実施した場合などに記載することも可能。 （例） ・海外のグループ会社、事業所に係わる情報セキュリティガバナンスの推進体制 ・情報セキュリティに係わる現地の法令、制度への対応 ・海外での取り組み事例
	外部委託	外部委託を行う場合に、委託先に要請する事項について記載する。 （例） ・情報セキュリティ対策ベンチマークのセルフチェックデータの開示 ・個人情報管理業務に関する委託先選定基準 ・SLAを締結する場合の情報セキュリティの要件定義 ・契約時の追記事項（監査権の確保、事故時の負担、再委託の要件等）
	情報セキュリティに関する社会貢献活動	・自社の情報セキュリティレベルの向上や本業を通じた情報セキュリティへの取り組み以外に、（地球規模で）よりセキュアなIT社会の実現のために企業あるいは社員一人ひとりが取り組んでいる活動を記載する。 ・既に取り組んでいる社会貢献活動の中で、情報セキュリティに関連するものがあれば、それを記載してもよい。 ・情報セキュリティに関する社会貢献活動の例： - 情報セキュリティの啓発のための広告・イベントなどへの協賛 - 情報セキュリティ関連団体への支援 - 小学校等への講師派遣 - こどもセキュリティ教室などのワークショップの開催

	事故報告*6	実際に発生した IT 事故についての概要を明らかにするとともに、再発防止に向けた取組を記載する。 ・ IT 事故に至る経緯 ・ 被害状況 ・ 影響範囲・規模（取引先、顧客、売上、企業価値、信用・評判等） ・ 対応状況 ・ 事故原因 ・ 再発防止に向けた取組
情報セキュリティに係る主要注力テーマ		発行者がステークホルダーに対して特にアピールしたいテーマを選択する。 （例） ・ 内部統制 ・ 個人情報保護 ・ 営業秘密情報の管理 ・ 事業継続計画（BCP）の策定
（取得している場合の）第三者評価・認証等*7		情報セキュリティの取組において、客観的な評価につながる、第三者による評価・認証に係る取組を記載する。 （例） ・ 認証の取得状況（ISMS 適合性評価制度、プライバシーマーク制度等） ・ 取得した認証の詳細情報（認証基準、認証登録番号、登録範囲、初回登録日・有効期限、認証登録機関等） ・ 情報セキュリティ監査の実施状況 ・ 公表資料 ［ISMS 適合性評価制度］適用宣言書、審査登録証 ［情報セキュリティ監査制度］情報セキュリティ監査報告書（開示可能な部分のみ） ・ 監査結果（リスクに配慮した上で記載） ・ 情報セキュリティ関連資格者数 ・ 情報セキュリティ管理の成熟度評価 ・ 情報セキュリティの格付け／ランキング ・ 今後の計画・予定

*1) リスクを高めるような情報開示をしないように考慮が必要。

*2) ネットワークでつながる全ての部門・事業所・システムを対象範囲とすべきとの意見もあるが、本資料では重点の軽重を意味するものと位置付ける。

*3) 予算や人的資源の配分を示すことも可能。

*4) 例示の数値目標を全て書かなければならないわけでなく、組織によって目標が自由に設定できる。

*5) 情報セキュリティ対策ベンチマークは、独立行政法人 情報処理推進機構（IPA）が公開している情報セキュリティ対策の自己診断サイト。自組織の情報セキュリティ水準について自己診断し、他社の水準と比較することができる。

*6) リスク分析との関連を説明することも可能。

*7) 「計画、目標」「実績、評価」の項で記載することも可能。

６．情報セキュリティ報告書記載イメージ

5.に基づき、具体的な記載イメージ例を策定した。策定に当たり、以下の架空の特徴を有する企業 3 社を想定した。

表 3　記載イメージ例のために想定した企業

A 社：インターネット通販

架空企業	A 社（インターネット通販）
売上高	国内　　200 億円，海外　20 億円
調達高	国内　　150 億円，海外　 0 億円
総資産	500 億円
総資本	300 億円
純利益	30 億円
国内拠点	本社　1
海外拠点	なし
営業形態	ネット販売　　100%
重要情報	[個人情報]・ネットによる取得　　あり ・委託先への提供　　あり ・店頭等での直接取得 なし ・外部からの提供　　なし ・個人 PC での保管禁止 [営業秘密]・リアルタイムの売上　電子データ [知財]　　・特許等　　なし
社員構成	正社員　40%，嘱託・契約　　10%， 派遣社員 40%，アルバイト　　10%
株主数	5
上場先	非公開
認証取得	プライバシーマーク
発行報告書	営業報告書、事業報告書
ステークホルダーとの関係	・顧　客：最重視 ・株　主：顧客を優先 ・取引先：特定先との取引集中 ・ビジネスパートナー：販売提携先 ・従業員：転職率については同業他社と大きな差はない ・環　境：重要性なし ・地域社会：ネットワーク中心
セキュリティ専門部署	特になし
アクセス管理	ID 管理は実施するが、入退出等は特別のチェックなし。
セキュリティポリシー	ネットにて公開
システム開発	外部委託にて開発
研修	入社時及び定期的に実施
顧客等からの情報開示請求	お客様窓口で対応
情報漏えいの有無と対応	・委託先で情報流出事故が発生 ・対応 情報漏えいの該当者に迷惑料支払 謝罪広告 調査結果の公表

B 社：大手家電メーカー

架空企業	B 社（大手家電メーカー）
売上高	国内　　5000 億円，海外　2000 億円
調達高	国内　　1000 億円，海外　3000 億円
総資産	2 兆 1000 億円
総資本	5000 億円
純利益	100 億円
国内拠点	本社　1，　支社　30，　工場　3，　支店　100
海外拠点	（支社）ニューヨーク、シカゴ、カリフォルニア、ホノルル、ロンドン、パリ、北京、上海、香港、シンガポール、ジャカルタ、シドニー　他 30 箇所 （工場）中国 5 箇所、東南アジア 3 箇所、米国 3 箇所、欧州 2 箇所、他 15 箇所
営業形態	メーカー販売　50%、ネット販売　10%、 委託販売　20%、直営店販売　20%
重要情報	[個人情報]・ネットによる取得　　あり ・委託先への提供 あり ・店頭等での直接取得　　あり ・外部からの提供 紙媒体のみ ・個人 PC での保管禁止 [営業秘密]・製品技術情報　電子データ、機密文書等 [知財]　・特許等　　電子データ、紙での保管
社員構成	正社員　80%，嘱託・契約　10%，派遣社員 5%， アルバイト　5%
株主数	1000 人超
上場先	東証一部上場
認証取得	ISMS 認証取得
発行報告書	有価証券報告書、事業報告書、アニュアルレポート、環境報告書等
ステークホルダーとの関係	・顧　客：重視 ・株　主：敵対的買収に備えるため企業価値を高め株価を高値安定させることが必要 ・取引先：厳格な基準によって選定 ・ビジネスパートナー：海外販売提携先 ・従業員：在職期間が長い ・環　境：環境負荷が大きい製品が中心のため重要度は高い ・地域社会：工場や支社等は地域経済に与える影響は大
セキュリティ専門部署	CISO をはじめ、本社で 10 名体制
アクセス管理	ID 管理、入館チェックをともに実施。
セキュリティポリシー	ネット等あらゆる場所で公開
システム開発	自社にて開発。 ベンダより人員の派遣を受けている。
研修	定期的に実施
顧客等からの情報開示請求	カスタマーセンターで対応
情報漏えいの有無と対応	・情報漏えいの経験は　　なし ・現在の取組 - 社員の評価指標として位置付け - 現場担当者による原因分析と改善提案 - 委託先にも契約書により賠償を規定

C 社：部品メーカー

架空企業	C 社（部品メーカー）
売上高	国内　　700 億円，海外　150 億円
調達高	国内　　400 億円，海外　100 億円
総資産	1000 億円
総資本	850 億円
純利益	50 億円
国内拠点	本社　1，支社　2，工場　4
海外拠点	（工場）中国 1 箇所
営業形態	メーカー販売　100%
重要情報	[営業秘密]社内及び顧客の技術情報　　電子データ、機密文書類 [知財]特許等　　電子データ、紙での保管
社員構成	正社員　70%，嘱託・契約　　10%，派遣社員 10%，アルバイト 10%
株主数	100 人超
上場先	東証一部上場
認証取得	とくになし
発行報告書	有価証券報告書、事業報告書、アニュアルレポート、環境報告書等
ステークホルダーとの関係	・顧　客：最重視 ・株　主：敵対的買収に備えるため企業価値を高め株価を高値安定させることが必要 ・取引先：同じレベルの対策を期待 ・ビジネスパートナー：海外生産先 ・従業員：在職期間が長い ・環　境：顧客の要請に応じる ・地域社会：工場と地域の関係は重要
セキュリティ専門部署	CSO を中心に、本社で 5 名体制
アクセス管理	ID 管理、入館チェックをともに実施
セキュリティポリシー	ネットにて公開
システム開発	自社にて開発。 ベンダより人員の派遣を受けている。
研修	定期的に実施
顧客等からの情報開示請求	とくになし（個人情報の保有はわずか）
情報漏えいの有無と対応	・情報漏えいの経験はなし ・現在の取組 - 現場担当者による原因分析と改善提案 - 委託先にも契約書により賠償を規定

情報セキュリティ報告書　記載イメージ１：A社（インターネット通販）

1.　基礎情報

（省略）

2.　経営者の情報セキュリティに関する考え方

2．1　　情報セキュリティに関する取組方針

当社では、「お客様の暮らしを支えるパートナーとしてあるべき姿を追求する」という企業理念に基づき、情報セキュリティについて以下の２つの方向を基本方針としております。

(1) 個人情報保護

当社では、ネット通販業務に関連してお客様の情報を多数お預かりしています。したがいまして、お客様が安心してネット通販取引ができるよう、正確、安心・安全な情報システムの管理体制がお客様の信頼を得る事業遂行の基本であると認識しています。そこで、当社では、個人情報保護ポリシーに基づき、ネット通販事業の遂行によるお客様の情報保護のための体制を構築・運用し、継続的改善に取り組んでいます。

・個人情報の保護に関する法令等の遵守を前提とした個人情報保護ポリシーを策定し、全社に適用するとともに、その体制を構築・運用します。
・全従業員に定期的に個人情報保護教育を実施し、法律遵守を周知徹底します。
・定期的に個人情報保護体制の評価を行い、その結果を対策に反映します。

(2) 事業継続

当社の使命は、お客様が一番欲しいときに一番欲しいモノをご提供できるよう、ネット通販サービスを通じて可能な限り迅速にご注文に対応することにあります。そのため、当社はサービスを 24 時間維持・運用していくために最大限努力いたします。

しかし、当社の事業は情報システム及びネットワークの存在を前提としているため、それらにトラブルが発生した場合、事業の継続が困難となるリスクを抱えています。したがいまして、そうしたリスクを踏まえた、トラブルに強い情報セキュリティ体制の構築・運用を実現いたします。

・事業継続計画の一環として情報セキュリティの方針を策定します。
・情報セキュリティの事件、事故等に対する危機管理体制を構築します。

××年××月××日
××通販株式会社
代表取締役社長〇〇〇

2．2　対象範囲

本報告書では、当社がネット通販事業で営業上取り扱う情報及び情報システム全般を対象としています。具体的には、お客様情報及びお客様からご利用いただいた受発注情報、商品情報、それらに関わる社外・社内システム、社内イントラネットが主な対象です。

2．3　報告書におけるステークホルダー[1]の位置付け、ステークホルダーに対するメッセージ

当社は、現在のお客様のみならず、将来当社のお客様となられる消費者の皆様もステークホルダーとして捉えております。したがって、本報告書は、まず第一に、現在のお客様をはじめとする消費者の皆様にご覧頂くものとしてご報告いたします。本報告書を通じて、お客様から信頼を得ることこそ、当社の営業基盤を安定させ、株主や投資家の皆様のご期待にお応えすることと認識しています。

また、当社が良好な取引関係を継続するためには、取引先の皆様の信頼を得ることが不可欠と認識しております。

そこで、本報告書では、当社が、お客様にとって「安心なサービス」であることに加え、取引先の皆様にとっても安心な「事業の維持・継続」にも重点を置いていることをお伝えいたします。

3．情報セキュリティガバナンス

3．1　情報セキュリティマネジメント体制

お客様から頂くご注文に 24 時間いつでも対応することが私たちの使命であり、私たちのビジネスの基盤であります。したがって、私たちは以下の取組を通じて、サービスを維持するために最大限努力いたします。

(1) 推進体制の構造と活動

①情報セキュリティ委員会

〇〇年〇月には、「情報セキュリティ委員会」を発足いたしました。この委員会は、代表取締役を委員長、事業部長以上を委員とするメンバー構成で、情報セキュリティポリシーや各種規定・規則の策定、セキュリティポリシーの実践に向けた様々な取組について実施の承認を担当しています。情報セキュリティ委員会での決定事項は会社としての方針であり、各業務責任者を通じて、全社的に対応するよう指示されます。

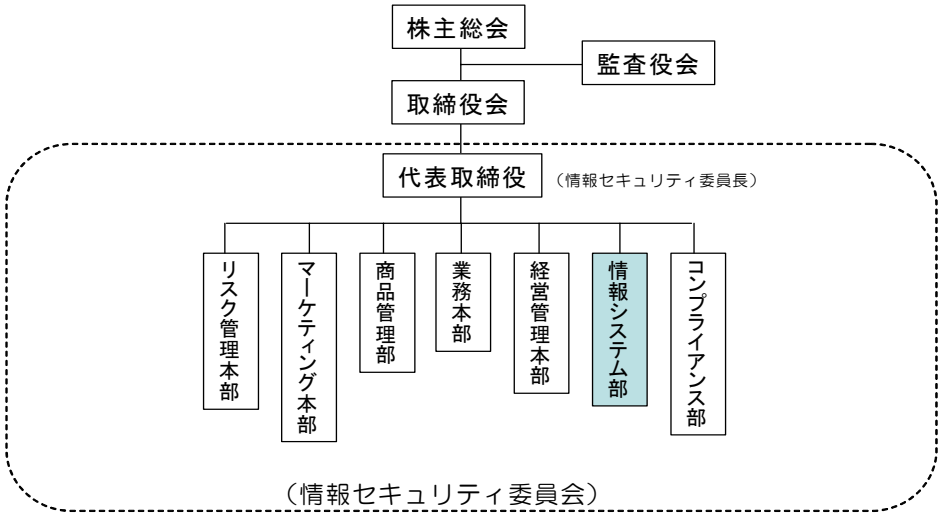
②情報システム部

[1] 株主・従業員・取引先・顧客・地域社会等、企業が事業活動を通じて関係を持つ相手のことをさします。

情報システム部では、セキュリティポリシーの実践に向けた取組について、現場の実施状況を定期的に見直し、問題がある場合にはその改善策を検討した上で、その結果を情報セキュリティ委員会に報告します。

情報セキュリティ委員会は四半期毎に開催し、情報システム部の報告を踏まえ、改善策の実施について審議します。

情報システムのダウン、コンピュータウイルスやワーム、不正アクセス、情報漏えいといった事故が発生した場合には、事業継続計画に則り、情報システム部の主導で適切かつ迅速に対応し、問題の早期解決を図ります。



※本委員会の事務局は情報システム部が担当し、各部間の連携を図る。また、個人情報最高責任者（CPO）を2名おく。
（顧客情報担当CPO：業務本部長、社員情報担当CPO：経営管理本部長）

(2) 教育・研修

情報セキュリティポリシーに基づく社内ルールを定め、社員全員がいつでもアクセスできるようにイントラネット上の情報サーバで社内向けに公開しています。

また、当社の社員は、入社時点から、情報セキュリティやコンプライアンスを含む実践的な情報システム利用研修を定期的に受講しており、そうした問題に係る十分な知見を有しています。

(3) 関連法制への準拠状況

当社は、個人情報保護に係る日本の規格 JISQ15001 を遵守する社内ルールを整備しており、プライバシーマークの認証も取得しています。同ルールでは、ソフトウェアの不正使用禁止や入退出管理への対応、違反に対する罰則を含む具体的な取組も明記しています。同ルールは、情報セキュリティポリシーに基づく項目もカバーしており（(2)参照）、その内容に矛盾・競合する点はありません。

管理面では、顧客データへのアクセスを技術的に監視・記録する仕組みを整備しており、社内ルールの遵守を裏付けています。

3. 2　情報セキュリティに関するリスク

(1) 重要なリスク

当社は、インターネットショッピングサイトで商品の販売を行っていること、それに伴い大量の顧客情報を保有していることから、以下のリスクを重要なリスクと考え対応を行っています。

・顧客の個人情報の漏えいリスク
・Web サイトでのサービスの停止リスク

なお、当社が保有している、顧客情報は次のとおりです。

【顧客情報】

・約 300 万件（累計）
・基本情報
　氏名、住所、メールアドレス、生年月日、性別、お客様 ID、パスワード等
・取引情報（過去 5 年分）
・支払情報（クレジットカード番号含む）

(2) 重要なリスクと事業活動の関連について

当社のサービスはインターネット上の Web サイトを介して取引の環境を提供することであり、当社の事業は情報システムやインターネットに大きく依存している状況にあります。

このため、インターネット経由で不特定多数からの不正アクセスやサービス妨害等の攻撃を受ける可能性、あるいは、Web アプリケーションの不具合等により、インターネット経由で顧客情報が漏えいする可能性があります。

また、お客様との接点は基本的にインターネット経由を通した Web サイトであることから、ネットワークあるいは Web サイトのシステムに障害等が発生した場合にお客様に対してのサービスが提供できなくなる可能性があります。

当社で取り扱う主な顧客情報は、データセンター、カスタマーセンターに集中し保管されております。これらセンター業務はすべて外部へ業務委託することにより運営しています。また、業務システムの開発保守業務も外部に委託しています。

また、当社の正社員比率は約 4 割程度であり、また、派遣社員、契約社員等を含めた従業者の離職率は〇〇%と、ほぼ業界平均並となっています。

(3) 発生した場合の影響

当社では、上記のリスクに対し必要と思われる対策を実施しておりますが、すべてのリスクの発生を回避あるいは防止し得るものではありません。

昨今の状況としては、一般にシステムのダウンや顧客情報の漏えい事件等の IT 事故は多数発生しており、同業他社でも同様の状況です。したがって、不確実ではありますが、当社でも IT 事故が発生する可能性は考えられます。

顧客情報が漏えいした場合、あるいは、Web サイトでのサービスが停止した場合、次のよ

うな影響が及ぶ可能性があります。
・事件、事故等への対応（損害の補填、再発防止策の実施等）のための費用負担
・営業停止した場合の機会損失
・信頼・評判の低下による取引の減少
・漏えいした顧客情報が悪用されることにより、お客様が被る損害
・Web サイトが停止することにより、お客様が取引不能となる
・株価のダウン

3. 3　情報セキュリティ戦略

(1) 個人情報保護
当社のように、業務の性質上、大量の個人情報を抱えざるを得ない業種では、リスクを低減し、個人情報保護を実現することが事業遂行上不可避の課題となります。
個人情報管理上のリスクの一つに、社員が業務遂行のため顧客データを社外に持ち出し、紛失・盗難に遭うケースが挙げられます。そこで当社では、お客様の情報を厳格な環境下で管理運用するため、高水準の情報セキュリティレベルを有し、SLA（Service Level Agreement：サービス品質保証制度）を取り交わしたデータセンター、カスタマーセンターを活用し、原則として個別のお客様情報を社員が直接取り扱うことがないよう、業務フローと情報システムを設計しています。

(2) 事業継続
ネット通販事業を安定的に行う上で焦点の一つが、サービスの中核機能である Web サイトの維持・継続です。そこで当社では、Web サイトをはじめとする情報システムの安全性・信頼性に重点を置くものとして、万が一情報システムに問題が発生した場合にも、可能な限り事業を継続し、迅速に復旧するための事業継続計画（Business Continuity Plan）を策定して、それに基づく対策を実施、トラブルに強いシステム・体制の構築に取り組んでいます。

4.　情報セキュリティ対策の計画、目標

4. 1　アクションプラン

当社では、目標達成のため、以下の取組に着手しています。

(1) 個人情報保護
当社では、3 年前に発生した委託先におけるお客様の個人情報流出事件を踏まえ、業務プロセス全体と社内・社外の業務分担、委託先の選定要件について見直しました。その成果を踏まえ、〇年からリスクの最小化を実現するプロセスとそれを支える情報システムの構築に着手しており、さらなる充実に取り組んでまいります。

また、当社では、社員の高いモラルを確保するため、入社時から定期的に顧客情報の管理に関する研修を実施しています。

(2) 事業継続

事業継続の観点からは、以下の取組が挙げられます。

・ 事業継続計画の策定と継続的な見直し
・ 情報システムのバックアップ体制の整備
・ 定期的な訓練の実施

当社では、特に、当社のみがサービスを維持できず、競合他社との競争に遅れをとる事態を最も恐れるケースとして位置付けています。そこで、事業継続計画の検討においては、情報システムの故障や大量アクセス等によるサービスの極端な低下・停止を脅威として想定し、ビジネスインパクト分析を行ってきました。

〇〇年度は、そうした分析結果を踏まえ、必要となる情報システムのバックアップ体制について見直し、機能面・コスト面から見た最適化を検討することとしました。また、事業継続計画の発動を想定して、関係者による訓練を行い、それぞれの行動の検証と問題点の洗い出しに取り組むこととしました。

4. 2　数値目標

(1) 個人情報保護

4.1 に示したとおり、既存の仕組みについてさらなる改善を図るため、個人情報保護の観点から、受発注処理に係る現在の業務プロセスと情報システムに関する内部監査を一回以上実施することとしました。

また、社員の年一回以上の個人情報保護研修の受講率の目標を 100%としました。

(2) 事業継続

商品情報提供及び受発注処理を行う基幹システムのダウンの年間発生回数について、1 回以下（平均故障間隔　4,380 時間）という目標を設定しました。また、基幹システムのダウンが発生した場合の平均修理時間について、1 時間以内という目標を設定しました。

5.　情報セキュリティ対策の実績、評価

5. 1　実績

(1) 個人情報保護

①顧客情報管理を前提とした業務プロセスと情報システムの設計と見直し

計画に則り、11 月から 12 月の 2 ヶ月間をかけて、受発注処理に係る業務プロセスと情報システムに関する内部監査を実施しました。具体的には、社内の業務部、情報システム部、及び社外の委託先であるデータセンター、カスタマーセンターを対象とし、正式な業務プ

ロセスと実際の作業フローとのギャップや情報システムの実現している環境について検証し、改善すべき点を洗い出しました。

・ 基本的には安全性の高い管理環境を構築できている
・ 情報システムは正式な業務プロセスを適切に反映しているが、作業上システムへの登録が後回しになるケースが見られた
・ 受発注プロセス上、例外的に社員がお客様の情報を直接扱うケースが存在するが、情報システム上はカバーされていない
・ カスタマーセンターから上がった報告が業務部内で共有されにくい

②個人情報保護に関する教育の徹底

社員に対し個人情報保護研修の受講を指示し、年度末時点で在籍している社員の受講率は 100%に達成しました。ただし、年度途中で離職した社員においては、未履行のまま離職したケースが生じていました。

(2) 事業継続

①情報システムのバックアップ体制に関する見直し

バックアップサイトとして必要な機能、通常時の運用・保守、データ転送の頻度、バックアップサイト稼動に要する時間と要員、復旧後の実機への移行工数等を検証した結果、バックアップサイトについてもアウトソーシングサービスの活用が適切と判断し、自社運用から移行することとしました。

②事業継続計画訓練の実施

事業継続計画に基づく訓練を初めて実施しました。サービスを提供している実機にトラブルが発生したという想定のもと、サービスをバックアップシステムに移行、それに伴う各種データの受け渡しや保全、さらに復旧に向けた取組等を検証することを目的としました。ただし、実際にトラブルが発生する危険性を避けるため、訓練は、関係者が一同に集まり、ある想定をもとにそれぞれが役割や行動を確認する机上演習方式を採用しました。その結果、次の点が明らかになりました。

・ 事業継続計画に基づく対処は、お客様にご迷惑をおかけしない水準で実施可能
・ スタッフ間、特に情報システム部と他部門の間の意思疎通にはさらに改善が望まれる
・ バックアップサイトのアウトソーシング化に伴い、計画に若干の改訂が必要
・ 停電が伴う事象の場合、各種対処工程に生じる影響についてさらなる検証が必要

③基幹システムのダウンに係る影響の縮小化

社内の基幹システムの停止に係るトラブルの発生は、今年度は 1 回にとどまり、目標内に収まりました。

ただし、ダウン発生時の修理時間は、原因の切り分けに時間を要したため、約 2 時間かかり、目標内には収まりませんでした。

5. 2　実績に対する評価

(1) 個人情報保護

個人情報保護については、委託先、情報環境、研修の観点から見て、高いレベルの環境を確保していることが確認できました。その一方、例外的なケースではありますが、いくつかの問題点も明らかになり、継続的な見直しと改善が必要と考えられます。

(2) 事業継続

情報システムの監視体制の見直しと自動化により、異常事態の効率化かつ正確な検出を実現するとともに、年間約 300 万円のコスト削減、スタッフの負荷軽減といった具体的な効果が期待できます。

また、訓練の実施により、事業継続計画の実効性について検証できたと考えられます。これは、当社の事業が、情報システムに大きく依存しているにもかかわらず、情報システムのトラブルに対し高い強度を有しており、競合他社に比べても信頼性の高いサービスを提供していると申し上げることができます。

5. 3　事故報告

【システムダウン】

〇月〇日 16 時 30 分過ぎに、受発注用の Web サーバを搭載するサーバマシンにおいて、ハードウェア障害（ハードディスクユニット部分）の原因によるシステムトラブルが発生、バックアップ機も順調に動作しなかったため、受発注サービスが一時的に停止状態に陥りました。

このようなハードウェア障害は常に発生する可能性があります。したがって、メインシステムにトラブルが生じた際の速やかなバックアップサイトへの切替え等を実施できるよう、事業継続計画の発動要件を見直すとともに、その実践的な訓練を繰り返すことで、問題発生時の円滑な対応を目指す必要があります。

また、上記の事故発生時の修理時間は、原因の切り分けに時間を要した影響で約 2 時間かかり、目標内（1 時間以内）には収まりませんでした。

6.　情報セキュリティに係る主要注力テーマ：「事業継続計画について」

(1) 当社における事業継続の考え方

当社は、同業他社に先駆けて、〇〇年〇月にはネット通販サービスを開始しました。それから現在に至るまでに何度か情報システムのトラブルを経験し、そうした事態の発生や収拾の取組方が、お客様のその後のご利用方針に影響することを学びました。事態の収拾に手間取ったり適切な対応がとられなかったりすると、不安を感じたお客様は苦情をおっしゃることなく、他社の類似サービスに移行されてしまいます。当社のようなネットビジネスでは、このような信頼感の喪失は極めて深刻な問題であり、その影響と回復に要する

コストは計り知れません。さらに、今後、チケット予約や株取引のように、処理の遅れがお客様の不利益に直結するような事業を扱う場合、システムダウンは今まで以上に許容できない問題となります。したがいまして、当社は、事業継続について、これまで以上に力を入れていく必要があると考えております。

(2) 事業継続計画の対象

当社において最も回避すべきは、何らかの原因によって当社のシステムがダウンし、サービスを提供できなくなり、お客様が同業他社に移行してしまう事態です。したがって、そのような事態を回避し、発生時にも被害を局限化する取組が求められています。

当社のシステムは、主に顧客管理機能と受発注管理機能で構成されています。そのうち、お客様の個人情報を含む顧客管理機能については、サービス品質が保証される形（SLA）でデータセンター、カスタマーセンターと契約することにより、高い安全性・信頼性を確保しています。そこで、当社の事業継続計画では、当社のサービスの基幹機能である受発注管理機能を主要な対象としています。

(3) 事業継続計画の概要

当社の事業継続計画は次のような構成になっています。

①計画発動段階

緊急事態が発生した場合、まず正確な情報の収集と判定が必要になります。当社の Web システムについては、稼動状況を常時監視し、異常発生時には警報を受ける形で、担当者が異常事態のリアルタイム検出に努めています。異常発生時には、担当者が初期対応に着手するとともに、情報システム部内に速やかに報告し、その深刻度に応じて事業継続計画の発動を含む対応方針を判断します。

②業務再開段階

緊急事態が発生した場合、基本的には 1 時間以内の全面復旧を目標とします。ただし、事態が深刻で、サービスの維持が困難な状況に陥った場合には、可能な限り迅速にバックアップサイトに切り替えるとともに、メインシステムの復旧作業を実施します。バックアップサイトへの移行に伴う各種データの受け渡しや保全については、事業継続計画に則って正確かつ迅速に行います。

また、このトラブルによりお客様の取引に何らかの影響が生じた場合には、この時点でメールやホームページ等を通じて説明します。

③業務回復段階

本システムの障害の原因特定や復旧作業について、作業の進捗状況を正確に把握し、全面復旧に至る手順やスケジュールを検討します。例えば、コンピュータウイルス感染によりシステムダウンに至った場合には、ウイルスの種類の特定やパターンファイルの更新・駆除、社外の関係各所への通知、さらに感染ルートの特定と改善といった作業があり、さらに全面復旧に向けたスケジューリング、段階的なプロセスを必要とする場合にはその手

順を検討します。

④全面復旧段階

バックアップサイトからメインシステムへの切り替えを行います。その際、事前に平常運用に移行するためのテストや検証を実施する必要があります。また、各種データの受け渡しや保全に係るチェックリストを策定し、トラブルの発生可能性を減らします。

さらに、全面復旧が完了したことについて、対外的に通知します。その際、障害の原因や影響規模、対応方針、改善策等についても必要に応じて適切に説明することを基本とします。

7. 第三者評価・認証等

当社は、〇〇年〇月に財団法人日本情報処理開発協会より「プライバシーマーク」の認定を受けました。

・ プライバシーマーク付与認定概要

① 認定範囲：ネット通販事業部

② 認定番号：××・・

認定期間：〇〇年〇月 1 日から△△年△月 31 日

併せて、□□年□月には、個人情報の安全管理に関わる状態を把握し改善するため、顧客情報管理を対象に、第三者による情報セキュリティ監査を実施いたしました。指摘事項は 2 箇所で、いずれも軽微な問題であり、すぐに改善いたしました。

情報セキュリティ報告書　記載イメージ2：B社（大手家電メーカー）

1. 基礎情報

（省略）

2. 経営者の情報セキュリティに関する考え方

2. 1　情報セキュリティに関する取組方針

「生活改革促進企業として社会に貢献する」　～　この経営理念のもと、当社は独自開発の製造技術を核として世界各国のお客様の生活に身近なソリューション製品を提供しています。ネットワーク社会の発展に伴い情報セキュリティの重要性が高まる中、お客様の生活革命を推進する当社においても率先して情報セキュリティに関するマネジメントシステム（ISMS）を構築し、その実効的な運用により、お客様、株主様、取引先様から当社の情報セキュリティに対する安心と信頼を得る必要があると考えています。

以下に示す「情報セキュリティ宣言」は、経営者が、企業として情報セキュリティに本格的に取り組むという宣言であり、情報セキュリティマネジメントシステム構築・運用の基本となるものです。

- 当社における情報セキュリティ上の最優先課題は、当社の事業活動関連情報の保護です。すなわち、設計情報や技術情報、研究開発情報、顧客情報や従業員情報等の不正な利用や漏えいの防止と保護に努めます。
- 情報セキュリティポリシーを策定して全社に適用、適切な対策を実施します。
- 全従業員に対し、定期的かつ計画的に情報セキュリティ教育を実施し、周知徹底します。
- 当社の情報セキュリティ対策の基本方針は、リスク管理委員会で決定し推進します。
- 情報セキュリティの推進に当たっては、不正競争防止法、個人情報の保護に関する法令、規則、ビジネスパートナー等との契約を遵守し、それらの変更を反映した対策を実施します。
- 事業の推進には業務の体制、情報技術の進歩を反映した情報セキュリティ対策を実施します。
- 当社は定期的に情報資産の棚卸しを実施し、適正なリスクアセスメントによって情報セキュリティ対策を推進します。
- 定期的に情報セキュリティ体制を見直し、情報セキュリティ対策の維持改善を実施します。
- 情報セキュリティ体制と運用の状況を公表します。

以上

××年××月××日
××株式会社

代表取締役社長〇〇〇

2. 2　対象範囲

本報告書は、当社が事業上取り扱う各種重要情報の保護を中心に記載しています。具体的には、製品の設計情報、製造ノウハウ等の技術情報、研究開発情報、その他ライセンス供給や製品・サービスの提供にかかる重要情報（顧客情報、従業員情報を含みます）が該当します。

2. 3　報告書におけるステークホルダーの位置付け、ステークホルダーに対するメッセージ

当社は、主要なステークホルダーをお客様、株主様、取引先様と位置付けています。当社は独自の技術をもって社会に貢献することを目指しており、ステークホルダーの皆様の当社に対する期待は、まず、この技術開発力によるものと確信しております。したがって、情報セキュリティにおいても、取引先からの技術情報も含んで技術情報の漏えいを防ぐことこそがステークホルダーの皆様の信頼を得るものと考えております。

また、事業において扱うお客様の個人情報等の保護は、皆様に安心して取引をしていただけるための基本であり、ステークホルダーの皆様の信頼確保の入口であると認識し、個人情報保護に取り組んでいます。

ステークホルダーの皆様のお声は、ホームページのご意見の窓口や研究所、工場の近隣住民の方々との対話集会等で承り、当社の持続的な改善につなげています。

3. 情報セキュリティガバナンス

3. 1　情報セキュリティマネジメント体制

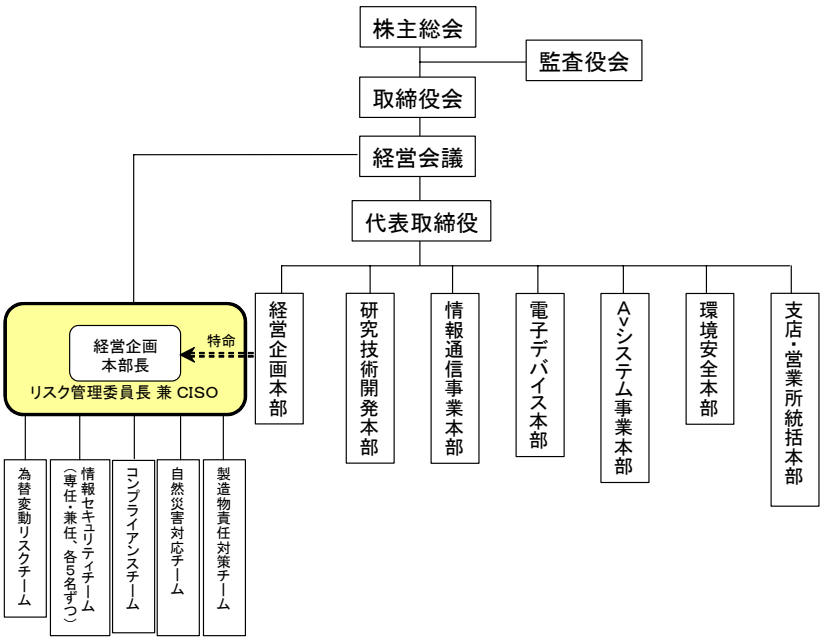
(1) 推進体制の構造と活動

情報セキュリティ問題は、経営会議に直結するリスク管理委員会（〇〇年〇月発足）において扱っています。

リスク管理委員会は、これまで全社的（横断的）な事案を取り扱うため、経営企画本部長をリスク管理委員長として、「為替変動リスクチーム」「コンプライアンスチーム」「自然災害対応チーム」「製造物責任対策チーム」の 4 チームで構成され、各チームが特命事項を担当してきました。しかし、社内の情報セキュリティ推進についても全社的な指揮をとる必要性から、〇〇年〇月、リスク管理委員長を「情報セキュリティ統括責任者」(CISO:Chief Information Security Officer）に併任するとともに、その配下に「情報セキュリティチーム」（専任 5 名と兼任 5 名の計 10 名のスタッフ）を新設し、四半期に一度の会議において社内の情報セキュリティ対策の実施状況に関して進捗確認・評価及び課題の抽出等を行っています。

情報セキュリティチームは、情報セキュリティポリシーならびに関連の規定・規則の策定、コンプライアンスチームや CSR チームとの連携、社内の対応状況の評価と改善策の検討、社員教育等普及啓発策の検討を担当しています。また、外部による情報セキュリティ監査も積極的に活用し、その評価を踏まえた見直しを進めています。

リスク管理委員会では、情報セキュリティチームの報告に基づき、CISO の責任の下、各種承認を行います。



（リスク管理委員会の構成チーム）

(2) 教育・研修

社員には、コンプライアンスと情報管理を中心とした研修の定期的な受講を義務付けており、その受講実績とテストの結果が昇格に影響する旨をルール化しています。

当社では、情報セキュリティ研修を通じて、社員一人一人が、OECD「情報システム及びネットワークのセキュリティのためのガイドライン－セキュリティ文化の普及に向けて」で示されている「セキュリティ文化」の概念を理解することを目指しています。

なお、当社の情報セキュリティ研修は、業務プロセスを踏まえ、派遣社員や関連企業の社員にも受講する形になっています。

(3) 関連法制への準拠状況

当社では、コンプライアンス（法律遵守）の具体的な実践計画であるコンプライアンスプログラムを、情報セキュリティ問題と同様にリスク管理委員会で策定、取締役会で承認しています。したがって、当社では、情報セキュリティ対策とコンプライアンスは整合の取れた形で一律に進められています。

当社のコンプライアンスプログラムは関連企業も含めた範囲で検討されており、PDCA のマネジメントサイクルに基づき毎年度見直され、改善・強化されています。

3. 2　情報セキュリティに関わるリスク

(1) 重要なリスク及び事業活動の関連について

当社は、当社が開発した独自の技術を使った製品を製造販売することにより、他社と差別化を図り、市場競争力を維持拡大し発展を遂げてきております。したがって、技術情報が流出した場合に、技術的優位性が失われ、企業の競争力の低下、さらにはブランド力の低下と、当社のビジネスに大きな影響を及ぼすものと考えております。なお、当社グループにおいては、グループ全体でサプライチェーンを構成しているという事業構造から、これらのリスクはグループ全体に影響を及ぼすものであり、グループ全体で取り組まなければならない課題と認識しております。

【重要な技術情報】

・製品の設計情報
・製造ノウハウに係わる技術情報
・新製品の開発情報
・研究開発情報
・提携先等との共有技術情報

当社の基本的な事業運営はグループ内で行っています。ただし、海外生産拠点があることから、当該拠点から技術情報が漏えいする可能性があります。また、提携先、取引先と共同開発等を行う場合があり相互の技術情報等を共有する場合があります。

当社では、優秀な人材の雇用、育成に力を入れており、正社員比率も高く、セキュリティへの意識も高い企業文化を確立維持しておりますが、人材の流出による情報の漏えいも懸念されます。

(2) 発生した場合の影響

当社では、上記のリスクに対し必要と思われる対策を実施しておりますが、すべての IT 事故の発生を回避あるいは防止し得るものではありません。したがって、当社でも IT 事故が発生する可能性は考えられます。

重要な技術情報が漏えいした場合、次のような影響が発生する可能性があります。

①自社及びグループ会社への影響

・情報漏えい事故に対応するため、事故処理、再発防止策に実施等の費用負担
・情報漏えいに関わる損害賠償等の支払
・競争力低下による収益減少、シェア減少
・取引先からの信頼低下による取引停止、取引量の減少
・信頼・評判等ブランド力低下による売り上げ減少
・株価への影響

②取引先への影響

・取引先と共有する情報が漏えいすることにより、取引先に損害が発生する可能性があります。

・当社の信頼、評判が低下することにより、取引先からの信頼を低下させる可能性があります。

③株主への影響：

・株価のダウン

3. 3　情報セキュリティ戦略

当社では、前述の情報セキュリティポリシーに基づき、製品の設計情報、技術情報、研究開発情報、顧客や従業員等の個人情報といった重要情報の管理を最優先課題と位置付け、グループを挙げて取り組む方針です。そうした取組の実現手段として、当社では、以下の目標を設定いたします。

目標：『全事業所ならびに子会社を含めたグループ全体における ISMS 認証の取得推進』

技術情報や個人情報といった重要情報の安全な管理を実現するためには、情報セキュリティマネジメントシステム（ISMS）のプロセスを導入・運用することが効果的です。当社では、これを一部の事業部門や事業所だけではなく全事業所、さらには子会社を含めたグループ全体で取り組むべき事業と位置付け、その実現に向けた中期計画を策定しました。

また、こうした取組をより実効的なものとするために、当社として注力すべき 3 つの方針を定めました。

① 情報資産の洗い出し

情報資産の洗い出しは ISMS の導入において前提となるものですが、特に当社が目指す情報セキュリティ環境、すなわち重要情報の安全な管理の実現に当たっては、情報資産の正確な把握と管理が生命線となります。そこで当社では、情報資産の洗い出しを綿密に行うものとします。

② 社員教育の徹底

重要情報の保護対策を追及していくと、最終的には技術ではなく人の問題となります。どれだけセキュリティツールを強化しても、その情報を扱う人間のモラルが貧弱であれば、重要情報の保護を実現することはできません。そこで当社では、社員教育に注力するものとします。

③ ビジネスパートナーとの情報共有ルールの明確化

社外のビジネスパートナーと共同作業を行う場合、共有する情報の取り扱いが問題となるケースが生じます。そこで当社では、社外のビジネスパートナーとの情報共有に際し明確なルールを提示し、その遵守を働きかけることとします。

4. 情報セキュリティ対策の計画、目標

4. 1　アクションプラン

(1) ISMS の認証取得

当社における ISMS の全社的な推進は段階的に行うものとします。

・ 第一期：ベースとなる推進体制の整備と先行部門における取得
・ 第二期：自律的な推進体制の強化と国内の主要部門における取得
・ 第三期：国内全事業所及び主要子会社への拡大
・ 第四期：国内･海外のグループ全体への拡大

昨年度の時点では、この第一期の取組が終了し、先行部門である乙研究所、A 事業部、B 事業部において ISMS の認証を取得することができました。

それを受けて、当社では、今年度を第二期の初年度と位置付けております。具体的には、第一期に整備した ISMS の PDCA サイクルの推進体制に係る人員・能力面の強化と、国内の主要部門（研究開発部門、顧客対応部門、ソフトウェア開発部門）を対象とした ISMS 認証取得に向けた活動を年次計画として取り上げました。

(2) 情報資産の洗い出し

情報資産の洗い出しは(1)の取組と連動するため、ISMS 認証取得の対象部署において、既存の業務で扱われている情報の抽出と、その情報の取得・利用・保管・開示・消去など一連の業務工程に応じたアクセス範囲の特定を綿密に行い、現状を正確に把握するとともに、その情報やアクセス範囲が適正なものであるかを検討することとしました。

(3) 社員教育の徹底

3.1(2)で記載したとおり、当社では社員教育にも力を入れています。今年度は、特に重要情報の取り扱いについて問題となり得るケースを整理し、そうした事態の回避策と併せて、社員教育の場で啓発していくこととしました。

(4) ビジネスパートナーとの情報共有ルールの明確化

ビジネスパートナーと共有する情報の取り扱いについては、契約後は契約に則ったルールに基づき相互に情報の外部流出を制限することができますが、契約前の段階では、曖昧に済ませるケースが多いのが事実です。当社ではこの部分を改善し、契約前の仕様説明の段階から NDA(秘密保持契約)を結び、開示した技術情報について契約の成否に関わらず、それを他に流すことを禁止する方針を採ることとしました。

4. 2　数値目標

(1) ISMS の認証取得

ISMS の PDCA サイクルの推進体制に係る内部スタッフを現在の 4 名から 6 名まで補充するとともに、社外の専門家を招聘して能力面の強化を図るものとしました。

また、研究開発部門、顧客対応部門、ソフトウェア開発部門を対象とした ISMS の認証取得を目指しました。

(2) 情報資産の洗い出し

(1)の推進に基づき、研究開発部門、顧客対応部門、ソフトウェア開発部門における情報資産とそのアクセス範囲について洗い出すとともに、その妥当性について評価することとしました。

(3) 社員教育の徹底

重要情報の取り扱いについて問題となり得るケースを取り上げた講習を、今年度内に全社員に受講させることを目指しました。

(4) ビジネスパートナーとの情報共有ルールの明確化

情報システム及びネットワーク関連の外部委託案件において、契約前の仕様説明の段階から NDA(秘密保持契約)を結び、開示した技術情報について契約の成否に関わらず、それを他に流すことを禁止する方針とし、その履行率を 100%とすることにしました。

5. 情報セキュリティ対策の実績、評価

5.1 実績

(1) ISMS の認証取得

ISMS の PDCA サイクルの推進体制に係る人員面の強化については、社外のコンサルタントと、社内の情報セキュリティチームとの共同タスクフォースを設置する形で強化するとともに、実際の推進活動を通じて社内スタッフの能力面の強化を図ることにしました。

本タスクフォースは当社の国内主要部門を対象として、ISMS の認証取得に向けた活動を遂行しました。

ただし、研究開発部門、顧客対応部門、ソフトウェア開発部門を対象とした ISMS の認証取得に向けた活動は、一部の部署で情報資産の洗い出しと、取得・利用・保管・開示・消去など一連の業務工程に応じたアクセス範囲の特定に予定以上の時間を要したため、作業進捗がそれらの見直しや保護手段にかかる検討の段階に留まり、ISMS の認証取得に至りませんでした。

(2) 情報資産の洗い出し

(1)にも記したとおり、結果的には本作業に時間を要したため、(1)の目標自体は達成できませんでしたが、(1)の工程の一部として、研究開発部門、顧客対応部門、ソフトウェア開発部門における情報資産とアクセス範囲の正確な把握と、その妥当性についての評価は目標どおり実施しました。その結果、約 1 割の情報についてアクセス範囲が不用意な設定になっていたことが明らかになりました。

(3) 社員教育の徹底

重要情報の取り扱いについて問題となり得るケースを取り上げた講習の受講率は 100%

となり、計画とおり全社員の受講を達成しました。

(4) ビジネスパートナーとの情報共有ルールの明確化

情報システム及びネットワーク関連の外部委託案件において、契約前の仕様説明の段階から NDA(秘密保持契約)を結び、開示した技術情報について契約の成否に関わらず、それを他に流すことを禁止する方針とし、その履行を推進したところ、今年度の 7 案件のうち 6 案件についてはその方針が受け入れられました。残り 1 件については、継続予定だった委託先が交渉段階で難色を示したため、当該企業を外部委託先リストから外し、改めて委託先の選定を実施しました。

5. 2　実績に対する評価

(1) ISMS の認証取得

ISMS の認証取得に向けた活動を通じて、共同タスクフォースに参加している社内スタッフは、様々なノウハウを吸収し、能力的に大幅な向上を果たすことができました。

しかし、当初の計画どおり、研究開発部門、顧客対応部門、ソフトウェア開発部門について ISMS の認証を取得することはできませんでした。この原因は、研究開発部門の研究開発情報を一律のルールのもとに洗い出すことが難しいこと、また、ソフトウェア開発部門において、他社から供給を受けている部品ソフトウェアの扱いが一律ではないことから、作業が予定時間を超過したことにあります。ただし、こうした活動を通じて、これまで「情報管理」の思想が必ずしも十分に徹底していなかった研究開発部門や、部品ソフトウェアの取扱いルールが明文化されていなかったソフトウェア開発部門においては、一種の教育効果があったといえます。また表面的な作業で ISMS の認証取得を目指すのではなく、本質的な取組を優先させたことで、本来あるべき ISMS の実装に向けた活動を進めることができた点は評価に値します。

(2) 情報資産の洗い出し

本工程を経て、約 1 割の情報についてアクセス範囲が不用意な設定になっていたことが明らかとなり、その改善策が適用されることとなりました。これにより、当社が目指す情報の適正な管理に向けた改善に大いに寄与したと考えられます。

(3) 社員教育の徹底

研修を通じて、昨今問題化しつつある、社員による重要情報の持ち出しがどのような影響を及ぼし得るかを社員に理解させることができました。したがって、本研修の結果、こうしたトラブルの発生リスクを低減化する効果が得られたと考えられます。

さらに今後、本テーマについて社員にテストを行い、その理解度の把握とさらなる改善の検討に活用することも考えられます。

(4) ビジネスパートナーとの情報共有ルールの明確化

本件のルールを新たに契約前から適用することで、一時的に大きなコストが発生しました。また、新ルールの適用を拒んだ委託先をリストから外すことで、それまでの継続的な委託を通じて蓄積された知見やノウハウの活用が困難となりました。

しかし、こうした取組を運用することによって、長期的には情報漏えいリスクを低減し、あるべき姿に近づくことができたという意味で、有益であったと考えられます。

5. 3　事故報告

本報告の対象期間中には、事業に影響を及ぼし得る情報セキュリティ関連の事故（システムダウン、情報流出等）は発生しておりません。

6. 情報セキュリティ対策に係る主要注力テーマ:「営業秘密の保護」

(1) 基本的な考え方

当社は製品の設計や製造ノウハウ等における独自の技術により、競合他社との差別化に成功しています。これらの情報はいわば当社の生命線であり、当社グループ外への流出が許されないものです。こうした情報を保護するため、当社では、経済産業省「営業秘密管理指針」(2003 年 1 月）に則り、不正競争防止法における「営業秘密」として保護を受ける要件を満たすよう、法務専門家のアドバイスを踏まえ、上記の重要情報を適切に管理しています。

※企業の秘密情報が不正競争防止法上の営業秘密の保護を受けるためには、次の３つの要件を満たすことが要求されています。

・秘密として管理されていること（秘密管理性）

・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）

・公然と知られていないこと（非公知性）

これにより、当社の重要情報を対象とした不正競争防止行為に対する差止請求権（第 3 条)、損害賠償請求権（第 4 条)、信用回復措置請求権（第 7 条）が認められると考えられます。

(2) 営業秘密の管理方法

具体的な情報の管理方法は次のとおりです。

①物的・技術的管理

・秘密情報であることがわかるように、書類に「秘」の文字をいれ、一般情報との区別を図っています。

・秘密情報へアクセスできる者を限定し、アクセス権者の履歴を記録しております。

・秘密情報の保管場所を特定し、また管理者が施錠をして管理しております。

・秘密情報の廃棄時には特定の管理者が焼却またはシュレッダーにより処理します。

・パスワードを定期的に変更するように義務付けております。

・ビルや研究所におけるセキュリティの徹底にも力を入れています。

②人的・法的管理

・社員と秘密保持契約を締結しております。

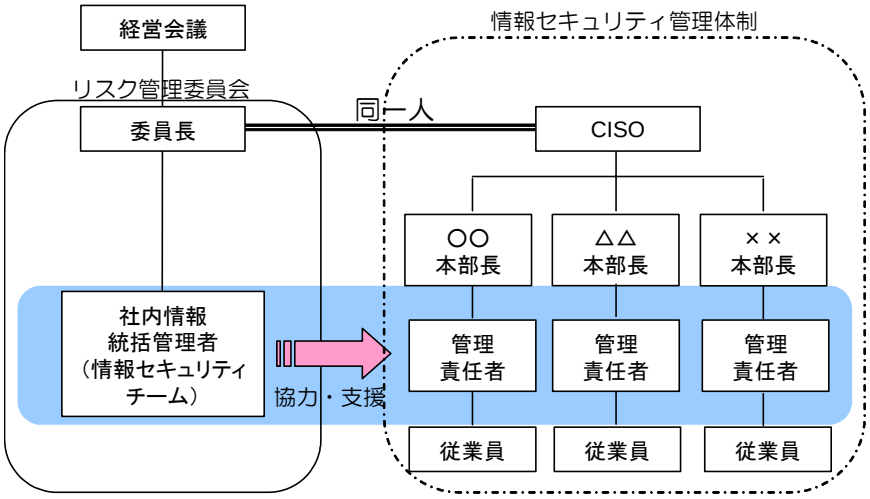
・秘密情報管理の社内でのルールを構築し、社内教育を定期的に行い社員の情報に対する認識の共有化を図っています。

・退職に当たって、秘密情報を持ち出されることのないように秘密書類や資料を当社に返還するよう義務付けております。またその際、何が秘密情報かということを特定してあるため従業員とのトラブルを最小限に抑えることができると考えております。

③組織的管理

・営業秘密を保有する組織全体のマネジメントに取組むことにより、情報セキュリティ管理体制の整備を行っております。

情報セキュリティ管理体制図



7. 第三者評価・認証等

当社は、〇〇年〇月に ISMS 適合性評価制度に基づく認証を取得しました。

・ ISMS 適合性評価制度認証取得概要

① 認証範囲：乙研究所、Ａ事業部、Ｂ事業部

② 取得認証規格：ISMS 認証基準（Ver.2.0）

③ 登録番号：×××００・・

④ 登録日：〇〇年〇月〇日

⑤ 登録審査機関：〇〇〇株式会社

⑥ 認定機関：△△△

サーベランス

△△年△月に□□株式会社よりサーベランスが実施され、重大な指摘事項はなく、軽微な指摘事項 3 件については、即時に改善しました。

情報セキュリティ報告書　記載イメージ３：C 社（部品メーカー）

1. 基礎情報

（省略）

2. 経営者の情報セキュリティに関する考え方

2. 1　情報セキュリティに関する取組方針

当社では、自動車を中心とする部品製造の立場から社会の発展を支えるべく、日々努力しております。当社の競争力の源泉は、当社の伝統である「独創性」と「粘り強さ」で勝ち取った技術力にあり、その技術力を駆使して当社は他に真似のできない「オンリーワン」のユニークな地位を築いていると自負しています。

したがって、当社においては技術情報が生命線であり、その適切な管理と保護は、当社の技術力を守るために、また会社と従業員を守るために、さらにお客様や株主の皆様の利益を守るためにきわめて重要な取り組みであると考えております。そこで、当社では、技術情報をはじめとする各種重要情報の管理･保護を現場レベルで徹底することを基本方針として位置付けるとともに、次の 2 つの目的のために本報告をとりまとめました。

1) 技術情報の管理・保護に関する当社の基本方針を従業員や取引先等関係各所に対して明示し、意思統一を図るとともに、自らの問題としての自覚を促す
2) お客様と株主の皆様の利益を第一に考え、そのための適切な取り組みがなされているということをご理解いただく

当社が、重要情報の管理･保護に関する基本方針に則り、適切に情報セキュリティ対策に取り組むことをお約束します。

××年××月××日
××株式会社
代表取締役社長〇〇〇

2. 2　対象範囲

本書で対象とするのは、以下の事項です。

・ 当社製品に関する機密情報（研究開発、設計、生産における公開していない技術情報）
・ 契約に基づきお預かりしたお客様の機密情報（設計、発注仕様、生産時の調整指示等）
・ その他の重要情報（顧客情報、従業員情報等）

なお、対象とする「情報」には、情報システム上の電子データだけでなく、機密文書類や従業員の知識も含まれます。

3. 情報セキュリティガバナンス

当社が取り組むべき情報セキュリティの適用範囲は、情報システムやネットワーク等にとどまらず、文書管理や従業員の雇用契約まで含めて考えなければなりません。

そこで当社では、〇〇年〇月、情報セキュリティ問題について全社横断的に扱う「セキュリティ統括責任者」(CSO:Chief Security Officer) を設置するとともに、CSO 直属の部隊として「セキュリティ管理部」(5 名) を立ち上げました。

セキュリティ管理部は、総務部、法務部、人事部、情報システム部と協力して、情報セキュリティに関する諸問題の解決に取り組んでいます。

セキュリティ管理部のミッションは、以下の 2 つです。

・ 機密情報・重要情報に関する物理・電子両面に係る安全性確保
・ 機密情報・重要情報保護とコンプライアンスとの整合

4. 情報セキュリティ対策の実績、評価

〇〇年度の主な取り組みとして、以下の 5 項が挙げられます。

(1) 機密情報・重要情報管理方針及びルールの策定

当社では従来、情報管理方針がありましたが、セキュリティ管理部の発足を機に、機密情報･重要情報保護の観点から管理方針や情報管理ルールについて改訂しました。特に、機密情報の流出に関わる問題については、データのアクセスログ管理の強化、解雇や訴訟を含む罰則規定を設け、社として機密情報を保護する意思を明確に提示しました。

(2) 雇用契約の見直しと教育・研修の実施

機密情報・重要情報保護の観点から、もっとも扱いが難しいのは、従業員の知識をどのように統制するかです。現在は、雇用契約における記載に、機密情報・重要情報保護に係る誓約を盛り込み、離職時にもそうした情報の利用に制限を加える形をとっています。

また、従業員に対し、機密情報・重要情報保護が自らの問題であることについて自覚を促し、適切な情報管理の実施を進めるため、研修プログラムの策定を進めています。その際、単なるモラル教育に留まらず、ルールの遵守こそ顧客と自分自身を守る方法であること、技術情報の流出に関する知識不足からトラブルを招く事態が起こらないよう、従業員全員が受講することを想定しています。

さらに、派遣社員についても、同様の研修の実施を派遣元に要請しています。

(3) 物理セキュリティの改善

機密情報・重要情報保護の観点から、施設、設備の安全面、バックアップ環境の確保などを全面的に見直しています。具体的には、入退室管理における生体認証等の採用、施設出入口の管理体制の見直し、複数拠点間の相互バックアップ体制の構築などがあがっています。

(4) 情報セキュリティの品質改善活動

当社では、長年、現場主導の品質改善活動に取り組んできました。こうした経験を踏まえ、情報セキュリティの品質改善活動として「情報セキュリティ目安箱」を設置しました。これは、社員が日々の業務を通じて気づいた問題点・失敗事例、改善に関するアイディアを投稿する仕組みで、有益な投稿については実際に採用しています。例えば、(3)に挙げた複数拠点間の相互バックアップ体制は、この投稿をきっかけとして検討が始まりました。

(5) 外部委託ルールの見直し

トラブル事例の多くは、外部委託先からの情報漏えいが原因になっています。そこで、機密情報･重要情報保護の観点から、情報流出のリスクを低減すべく、外部委託のルールについて見直しを進めています。

5. 第三者評価・認証等

当社は、〇〇年度の ISMS 適合性評価制度に基づく認証取得に向けて、現在準備作業を進めています。