データ侵害への対応措置（サイバーインシデント対応計画）

【方針及び手順の制定】
当社では、サイバーセキュリティ・インシデントに関する方針、手順および体制等を社内管理規則として定めています。

【推進体制】
セキュリティインシデントや大規模システム停止に対応する組織として、情報危機管理部を設置し、その中に、インシデント対応の専任の組織として、CSIRTを設置しています。インシデント発生時には、CSIRTが関係部門と連携し、初動対応、影響範囲の特定及び被害拡大防止等を実施します。また、取締役、CRO、CIO、CISO等で構成する「セキュリティ委員会」に情報を集約し、対応方針を審議・決定する体制を整備しています。

【事前対応】
（重要資産の把握及びリスク評価）
セキュリティ基盤・対策の状況を把握・レビューするとともに、脅威の評価、情報資産に対するリスクの評価を行っています。

（シナリオ分析）
リスク評価を基にシナリオ分析を実施し、特定したシナリオに沿って、定期的に関係者全体を対象とした模擬訓練を行っています。

（脆弱性分析）
新たに発見された脆弱性、新技術の開発、侵入活動及びこれらに関連する動向を確認し、セキュリティリスクの変動が起きていないか判断した上で、必要に応じて対策を実施しています。

（ログ及びアラートの分析）
セキュリティシステムのログやアラートを分析し、異常な兆候を検知するとともに、セキュリティ侵害が発生していないかを確認しています。

（受付及びエスカレーション）
セキュリティインシデントの報告受付窓口、報告・連絡体制及び重大性に応じたエスカレーションルートを含む対応フローを定めています。

（教育・啓発活動）
全従業員を対象として、セキュリティ研修や、フィッシング訓練等のインシデント対応訓練を実施しています。また、セキュリティ情報や事故事例、注意喚起等の発信を行っています。

データ侵害への対応措置（サイバーインシデント対応計画）

【インシデントへの対応】

（インシデントの判定）

各種セキュリティシステムが検知したアラートや利用者からの申告等、セキュリティ上の異常な兆候をイベントとして受理し、インシデントかどうか判定を行います。業務への影響や影響範囲等を特定し、優先順位付けや対応要否の判断を行います。重要な事案に関しては、「セキュリティ委員会」及び「リスクマネジメント委員会」にも報告を行います。

（原因分析）

ログ等の分析を行い、発生経路、脆弱性、攻撃手法及び根本原因を特定します。

（被害拡大の防止及び原因の除去）

アカウント停止、ネットワーク隔離・遮断、感染端末の切り離しなど、被害の拡大防止策を速やかに実施します。また、マルウェア、不正設定、不正アカウント及び脆弱性等を除去または修正し、再発、再侵入の要因を取り除きます。これらの対策により、被害の最小化に努めます。

（復旧）

代替運用、サービスの再開など業務継続のための措置を講じ、原因の除去及び安全性の確認後、システムならびに業務関連データを復旧します。

（報告及び通知）

サイバー攻撃の性質、影響範囲、インシデントの検知から復旧までのプロセスとその対応結果についてとりまとめ、経営層を含む社内関係者への報告に加えて、必要に応じて、顧客や取引先等関係者への報告及び通知を行います。

【事後対応】

（レビューの実施）

インシデントの原因、影響、対応及び復旧結果等を評価し、問題点や得られた知見等を整理します。

（再発防止策及び改善措置）

インシデントの原因やレビュー結果に基づき、セキュリティ強化、プロセス改善、監視ルールの追加など、再発防止策を実施します。必要に応じて、方針や体制、計画の見直しも行います。研修や訓練に関しても、インシデントの事例や得られた知見を反映・更新し、再発防止に努めます。