情報セキュリティ

セキュリティと利便性を両立させる

クラウドサービスの展開では、多くのケースで利便性とセキュリティは相反するものとなりますが、社会や経済の効率性や生産性を上げていくには、双方のバランスを高度にとっていくことが重要です。当社グループは、企業理念において「セキュリティと利便性を両立させる」を掲げており、「安全かつ安定的なインフラサービスの提供」と「データプライバシーの保護と情報セキュリティの徹底」を重要課題として特定しています。安心、安全なサービスの提供に向け、あらゆる対策を講じ、セキュリティリスクの最小化に取り組むことで、各サービスのさらなる成長を追求しています。

情報セキュリティへの考え方と管理体制

当社グループが提供するサービスは、企業や個人のユーザーに対して、顧客情報といった個人情報に該当するさまざまな重要情報の管理や利用を促進するものであるため、情報の取り扱いや保護については、経営の最重要項目に位置付けています。当社グループでは、個人情報保護方針及び情報セキュリティ方針を策定した上で、情報資産を厳重に管理し、あらゆる手段を講じてリスクの最小化に努めています。セキュリティ管理体制においては、プライバシーリスクやセキュリティリスクに対して迅速かつ全方位的に対処できるよう、執行役員がCISO[*1]及びDPO[*2]の役割を担っています。また、グループを横断する情報セキュリティに関する専門部署として、CSIRT[*3]を設置しています。そのほか、2007年の会社設立当初より、個人情報マネジメントシステムを構築しており、社内におけるデータ保護の取り扱いに関する環境を整備するとともに、最新セキュリティ技術を駆使して、さまざまな重要情報を24時間365日監視できる体制を整えています。

*1 最高情報セキュリティ責任者
*2 データ保護責任者
*3 Computer Security Incident Response Team

情報セキュリティに関する主な役割

CISO
情報システムにおけるセキュリティ及びリスク管理に関する責任と権限を有し、情報セキュリティリスク方針並びに管理方法について統括します。

DPO
PMS運用の責任と権限を有する個人情報保護管理者の役割と、GDPRの遵守状況を監視することを主な業務とするデータ保護責任者の役割を担います。

情報システム管理者
情報システム管理業務を所管する組織の長が、CISOと協議の上、組織、分掌及び職務権限規程における承認に基づいた業務を遂行します。

CSIRT
情報セキュリティを脅かす可能性のある事象やシステムの脆弱性に関する情報、サイバー攻撃予兆等を収集し、対応方針や手順を策定します。

インシデントガイドライン

当社グループでは、災害や事故、不正アクセス、脆弱性の問題等のサービス提供に係るインシデントが発生した場合に備え、各部署においてインシデントに対する体制・指揮命令系統や判断基準、対応手順に関するガイドラインを定めています。具体的には、インシデントの種別を機密性・完全性・可用性という3つの観点で種別し、それぞれの対応について優先度を設定した上で、各部署におけるインシデントの判断・対応の意思決定者を定めています。

セキュリティに関する教育

当社グループでは、個人情報保護法と安全管理に関する正しい理解の習得を目的に、全役職員に対して個人情報保護士の資格取得を義務付けています。入社から一定期間が経過しても未合格の場合には、合格するまでは原則、昇給が保留されるルールを設けています。また、入社時と年に一度、情報セキュリティと個人情報保護に関する研修を実施し、定期的な知識習得の機会を設けています。加えて、個人情報・機密情報のPCへの格納を禁止する等、情報資産に関する取り扱い手順の運用を徹底しているほか、内部監査室からの指名で、従業員がセキュリティ委員を務め、従業員間でセキュリティに関する相互監査を行う仕組み等を活用することで、セキュリティ意識を強化しています。

第三者機関認証の取得

当社グループでは、第三者機関によるセキュリティ関連の認証取得及び取得後の定期的な更新対応に取り組んでおり、プライバシーマーク制度や国際規格のISO/IECをはじめとしたさまざまな認定を受けています。これらの認証取得は、情報セキュリティの強化だけでなく、サービスの信頼性獲得にもつながっています。

プライバシーマーク
プライバシーマーク制度は、日本工業規格「JIS Q15001個人情報保護マネジメントシステム―要求事項」に準拠した「プライバシーマークにおける個人情報保護マネジメントシステム構築・運用指針」に基づいて、個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定し、事業活動に関してプライバシーマークの使用を認める制度です。当社は2007年に認定を取得しています。

SOC2 Type1
SOC2報告書は、米国公認会計士協会（AICPA）が定めたトラストサービス規準に従って、セキュリティ、可用性、処理のインテグリティー、機密保持、プライバシーのいずれかに関しての財務報告に関連しない領域を含む内部統制に対して、監査法人が意見を表明した報告書です。有限責任監査法人トーマツにより、「Sansan」におけるType1の「セキュリティ」に関する内部統制について、報告書が発行されています。

電子取引ソフト法的要件認証
公益社団法人 日本文書情報マネジメント協会（JIIMA）の「電子取引ソフト法的要件認証制度」とは、国税関係書類をコンピュータで作成し、電子的にやり取りする場合の当該取引情報の保存を行う市販ソフトウエア及びソフトウエアサービスが、電子帳簿保存法の法的要件を満足している場合に認証を付与する制度です。当社は「Bill One」及び「Contract One」において、2022年4月に認証を取得しました。

ISO/IEC 27001 ／ ISO/IEC 27017
ISO/IECは、セキュリティに関する国際規格です。当社グループが提供する「Sansan」及び「Bill One」において、情報セキュリティマネジメントシステム（ISMS）に関する国際規格であるISO/IEC 27001を2022年5月に取得しました。また、それと同時に、「Sansan」において、クラウドサービスの提供や利用に対して適用されるクラウドセキュリティに関する国際規格であるISO/IEC 27017を取得しました。

技術的なセキュリティに関する取り組み

当社グループでは、安全なサービス提供を目的に、第三者機関や社内専門部署によるサービスの脆弱性診断やペネトレーションテストを実施しているほか、さまざまなセキュリティ対策に取り組んでいます。

データセンターへの通信は全て暗号化
ファイアウォール機能を設置した上で、外部からアクセスされたデータセンターへの通信は、ユーザー認証HTTPSによる高度な暗号化等を行っています。

名刺のスキャン後、端末の画像を削除
外部からの侵入を防ぐソフトをインストールした「Sansan」のスキャナは、名刺画像をスキャンした後、端末から画像データを削除しています。

脆弱性診断とペネトレーションテスト
外部機関を登用し、システムの脆弱性の特定やサイバー攻撃を踏まえた侵入テストを通じて、セキュリティレベルをテストし、問題点の是正をする等、サービスの強化につなげています。

サービスの高可用性
全てのサーバーは負荷分散がなされており、障害発生時には、サービスを迅速に復旧させることが可能です。また、データセンターの二重化を行い、災害時の機能・サービス停止リスクを最小化しています。