【SaaS 事業部門セキュリティポリシー】

・環境認識（ちょっとした油断・ミスが重大な危機をまねく）
日々の仕事で、顧客、取引先および自社の重要な情報資産を取り扱っている。
ちょっとした油断やミスなどで、情報資産の誤用、盗難、紛失などを起こせば、顧客、取引先などに多大な迷惑や損害を与え、ひいては、企業、個人の信用を大きく失墜させてしまう。
さらに近年、インターネット経由でほとんどの情報をやりとり出来るようになり、不正アクセス、ウイルスによるデータの破壊、情報の漏えい、サイバーテロなどのネットワーク犯罪が急増しており、企業､個人にとって大きな代償を払うという深刻な事態を起こしかねない。
ネット化された高度情報化社会のなかで、業務で重要な情報を扱う者には、的確な環境認識と適正な行動が厳しく求められている。

・目的（情報資産の保護と企業経営の方針）
株式会社プロシップの SaaS 事業部門である、SaaS 営業部、SaaS 開発本部、製品開発 2 部（以下当部門という）は、情報資産の活用において、セキュリティが欠くことのできない影響を与えることを認識し、情報資産に対する適切な安全対策を重要な施策のひとつとしてこれを実施する。
このセキュリティポリシーならびに各種ガイドラインは、安全対策に対する当部門の基本方針であり、当部門の情報資産を適切に活用、保護するための最低限度の要件及び責任の所在を明確にし、当該資産の誤用と損失などによる物的損害と、さらに誤用、盗難、損失などによる訴追などを未然に防止することを目的としている。
このセキュリティポリシーが有効に機能するよう、従業員がこれに関与し、これを遵守しなければならない。

１．適 用 範 囲 （誰が遵守し、何に適用されるのか）

（１） このポリシーは、当部門に関わる取締役、監査役、顧問、正社員、契約社員、アルバイトを含むすべての従業員に適用される。なお、相当部分は、開発パートナーにも適用する。

（２） このポリシーは、ハードウェア、ソフトウェア、コンピュータネットワーク、各種データファイルのみならず、紙媒体を含む各種ドキュメントや顧客情報を含む、当部門の事業活動に関わるすべての情報資産に適用される。

２．ポ リ シ ー の 遵 守 （誓約書の提出、罰則等）

（１） 従業員は、入社時及び毎年当ポリシー適用後速やかにポリシーを遵守する旨の誓約書を提出しなければならない。開発パートナーについても、業務開始時及び毎年、誓約書の提出を義務付ける。

（２） 従業員は、当部門が随時開催するセキュリティ研修に必ず参加しなければならない。開発パートナー会社は、責任者を当部門セキュリティ研修に参加させ、その内容を当部門の業務に当たる従業員に周知しなければならない。

（３） 当部門は、セキュリティポリシーに反する行為を行った者に対して、就業規則第８章の賞罰の条項により、戒告から解雇の懲戒を課すとともに、その内容によっては法的措置をとることがある。

（４） セキュリティポリシーに反する行為を行った、またはその恐れがある者を発見した場合は、上司に通知しなければならない。
この場合、当該通知者の秘密は保護されなければならない。

３．機 密 保 護 の 原 則

（１） 会社の機密、及び業務上知り得た顧客に関する機密事項（以下、「機密情報」という。）を外部に漏らしてはならない。営業上あるいは法律等により対外的に提出する目的のもの以外の当部門の事業活動に関わる全ての情報資産は、「社外秘」、「マル秘」等の記載の有無に関わらず原則としてコピー・複写・送信・転送を禁じる。

（２） 会社の業務遂行上において発生するいっさいの情報は会社に帰属するものとする。

（３）機密保護の原則に反する行為を行った者に対しては、規定により罰則を課すものとする。

※ケースによっては、会社、個人が訴追される。

４．事 故 発 生 時 の 対 応

情報資産に関する事故が発生した場合には以下の対応を行う。

（１）事故当事者及びそれを発見認知した者は、一人で判断せず、直ちに上司に報告する。直属の上司がいない場合は、その上長等連絡がつく者に報告する。

（２）事故連絡を受けた者はさらにその上長に報告し、所属本部長まで報告する。

（３）報告を受けた本部長は事故対応責任者として、社長、取締役及び他本部長に報告するとともに、二次被害及び被害拡大を防止するため、その時点で取りうる対応をとる。
・紛失・盗難の場合は警察、交通機関に届けを出す。
・入室証、携帯電話等の紛失の場合は失効の手続きを行う。

（４）情報漏えいの恐れがある場合には、直ちに漏えいの恐れのある関係先に第一報を行うとともに、事故の早期解決に向けた対応をとる。

（５）事故の詳細な内容を調査し、被害を受ける或いは受ける恐れのある関係先に報告を行う。

５．マネジメントシステムの運用

（１）マネジメントシステムを実行・維持・改善を行うために管理責任者の任命等、体制を整える。

（２）マネジメントシステムの構築及び情報セキュリティに関する目的を設定し、定期的にレビューし、継続的に改善を実施し、維持する。

６．クラウドサービスに関するセキュリティ

（１）クラウドサービスカスタマとして、クラウド環境に保存される情報がクラウドサービスプロバイダによるアクセス及び管理の対象となる可能性、資産がクラウド環境に保持される可能性、処理がマルチテナントの仮想化されたクラウドサービス上で実行される可能性、クラウドサービスユーザ及びクラウドサービスユーザがクラウドサービスを利用する状況、特権的アクセスをもつクラウドサービス実務管理者、クラウドサービスプロバイダの組織の地理的所在地及びデータを保存する可能性のある国を考慮する。

（２）クラウドサービスプロバイダとして、クラウドサービスの設計及び実装に適用する最低限の情報セキュリティ要求事項、認可された内部関係者からのリスク、マルチテナンシ及びクラウドサービスカスタマの隔離、当部門によるクラウドサービスカスタマの資産へのアクセス制御と手順、変更管理におけるクラウドサービスカスタマへの通知、仮想化セキュリティ、クラウドサービスカスタマデータへのアクセス及び保護、クラウドサービスカスタマのアカウントのライフサイクル管理、違反の通知並びに調査及びフォレンジック（forensics）を支援するための情報共有指針を実施する。

制定日 2026 年 4 月 1 日

株式会社プロシップ
代表取締役 鈴木 資史