公 開

平成28年度
情報セキュリティ報告書

第1.00版

初版発行日 ： 2017／08／12
最新改定日 ： 0000／00／00

株式会社サジェコ ISO事務局

公 開

情報セキュリティ報告書

■目次

1. 基本情報 3
2. 経営者の情報セキュリティに関する考え方 4
3. 情報セキュリティガバナンス 6
4. 情報セキュリティ対策の計画、目標 8
5. 情報セキュリティ対策の実績、評価 9
6. 情報セキュリティに係る主要注力テーマ 14
7. 第三者評価・認証 16

公 開

■1. 基本情報

1.1 本報告書の目的

本報告書は、株式会社サジェコ（以下、「当社」といいます。）の情報セキュリティへの取組みをステークホルダー[1)]の皆様に説明し、事業への信頼性を高めていただくことを目的として公表します。本報告書の内容は、公表にあたり、インターネット等による一般公開に問題がないと判断した情報のみを記載しています。ステークホルダーの皆様におかれましては、本報告書の開示内容では意思決定に不十分と判断される場合につきまして、個別開示に応じさせていただく用意がございますので、下記に記した本報告書の責任者（連絡先）または、当社担当者までお申し出ください。

本報告書において「ステークホルダー」とは、お客様、社員、取引先、その他の利害関係者とします。

1.2 本報告書の対象期間

本報告書が対象とする期間は、2016 年 4 月 1 日～2017 年 3 月 31 日とします。

1.3 本報告書の責任者（連絡先）

〒063-0869　北海道札幌市西区八軒 9 条東 5 丁目 1 番 28 号
株式会社サジェコ 本社
代表取締役社長（兼務 ISO 事務局長）　伊藤 直樹
ICT 技術部課長（システム管理責任者）　飯高　司
電話　011-788-7505（代表）
　　011-788-7525（ICT 技術部）

公 開

■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み方針

当社は、「地域に愛され、地域に尊敬される企業活動を行う」という経営理念のもと、本社業務としてソフトウェア開発及びシステム保守、ＩＴソリューション業務等を提供しています。当社の経営はお客様、お取引先との信頼関係の上に成り立っているものであり、その信頼を守るためには、当社が、社内における情報セキュリティを確立し、導入、運用、監視、レビュー、維持及び改善していくことが必要です。当社は、情報セキュリティの重要性を充分に認識し、お客様、お取引先、地域社会のご信頼を得て、より良い総合ビルメンテナンス、ＩＴソリューション業務等をご提供していくため、以下の方針に従うことを宣言いたします。

この方針が対象とする「資産」は、当社が保有するすべての資産、ならびにお客様からお預りするすべての資産といたします。

1. 情報セキュリティ目標の設定

内部及び外部の課題に対応するために、定量化可能な情報セキュリティ目標を年度単位に設定し、その達成状況を評価することにより、情報セキュリティ目的の達成に努めます。

2. 要求事項の特定と満足

情報セキュリティに関する法令及びその他の規制、ならびに契約上のセキュリティ義務を含む利害関係者の要求事項を明確にし、それらを満足します。

3. 体制の整備と責任の明確化

全社的な情報セキュリティを推進していくために ISO 事務局を設置し、ISO 事務局長（情報セキュリティ管理責任者）を任命します。また、各部門の長が部門情報管理責任者として積極的に活動いたします。

4. 資産の保護管理

当社では、情報セキュリティ方針を実行するために内部規定を整備し、取り扱う資産に応じた組織的・人的・物理的・技術的対策により、適切な保護管理を実施いたします。すべての社員（当社の役員、臨時社員を含むすべての社員、常駐の協力会社員が対象）がこの規定を順守いたします。規定にない例外的な状況が発生した場合は、ISO 事務局長の指示により対応し、必要に応じて規定類の見直しを実施します。

5. 教育・訓練の実施

当社では、すべての社員に対して情報セキュリティ教育を継続して実施し、意識の向上を図るとともに、資産の保護管理に必要な能力の開発・維持に努めます。

公 開

6. 外部委託

情報セキュリティに関連する業務を他に委託する場合、情報セキュリティに関する適格性を条件に含めた委託先の選定を行い、委託先との間で機密保持条項を含む適切な契約を交わした上で、当社の方針及び内部規定に従った適切な取扱を実施するよう、委託先に対して指導・管理を実施いたします。

7. 監査の実施

当社では、情報セキュリティ方針および内部規定を順守していることを確認するために、内部監査を実施できる体制を整備し、計画的に内部監査を実施いたします。

8. 違反に対する罰則

当社では、社員が情報セキュリティ方針および内部規定に違反した場合、就業規則に基づいた罰則を適用いたします。

9. 継続的改善

当社では、適切な運用が実施されるよう監視を行い、必要な是正・予防処置を実施していきます。また、環境の変化に対応したリスクアセスメントを規定に従って実施し、ISMS を継続的に見直し、改善していきます。

2.2 対象範囲

本報告書が対象とする範囲は、株式会社サジェコ　本社で行うソフトウェア開発及びシステム保守、ＩＴソリューション業務等とし、対象者は、当該業務に携わるすべての社員（役員、臨時社員等を含む）とします。

2.3 報告書におけるステークホルダーの位置づけ、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、取引先様と位置づけています。当社は、ソフトウェア開発及びシステム保守、ＩＴソリューション業務等における設計･製作ノウハウの独自技術、お客様資産の管理･運用保守における技能やマネジメント能力の蓄積･向上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、その技術力と業務を通して蓄積したお客様、お取引先様に係る重要資産の保護と考えます。したがって、情報セキュリティにおいても、技術情報やお客様、お取引先様に係る重要資産の漏洩や棄損、流用を防ぐこと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等の個人情報の保護は、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、普段の営業活動や当社ホームページのご意見窓口等で承り、

公 開

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

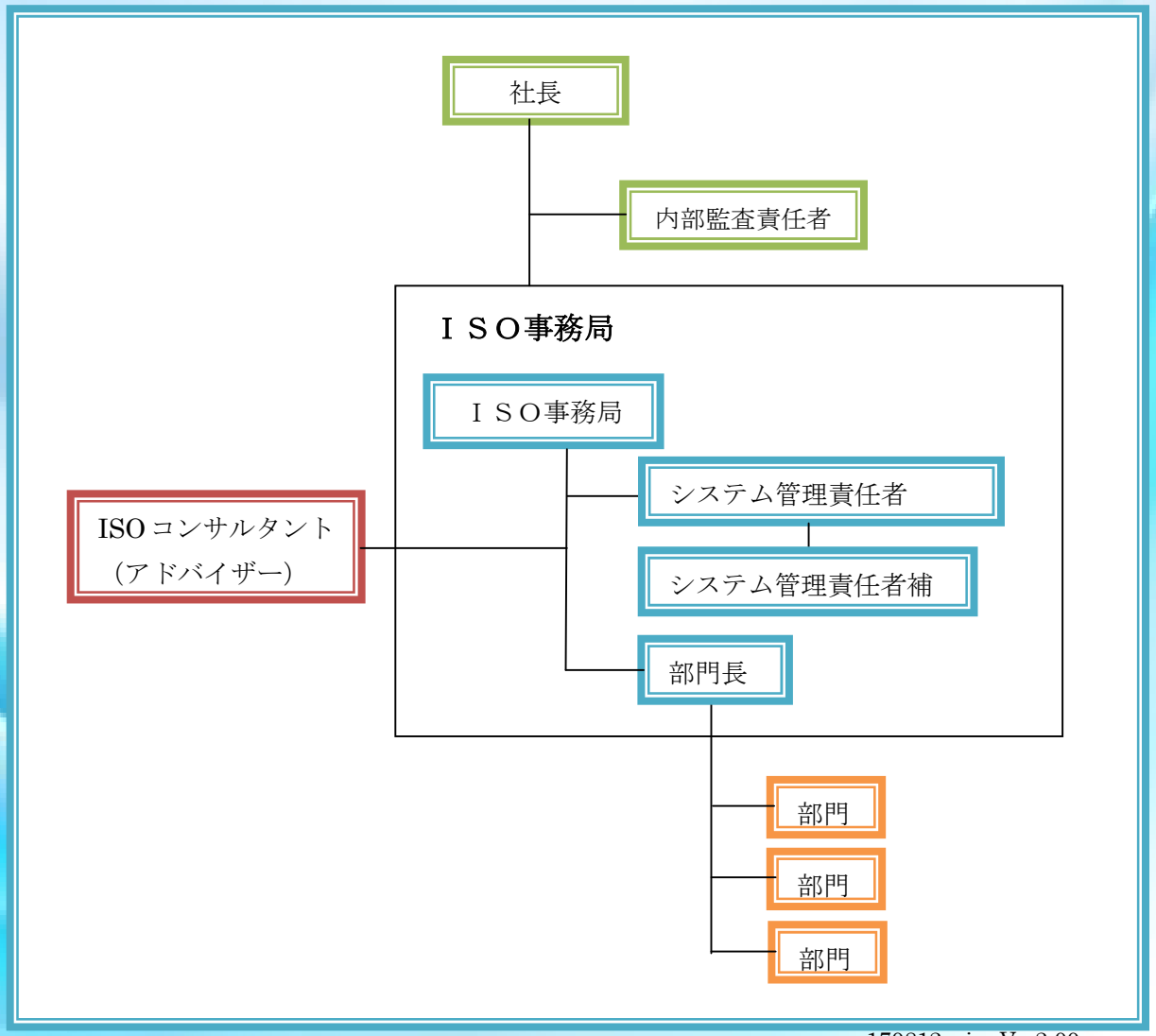
3.1 情報セキュリティマネジメント体制

(1) 推進体制の構造と活動

情報セキュリティ問題は、社内横断的な組織（プロジェクト）である ISO 事務局において取扱っています。

ISO 事務局は、対象範囲における横断的セキュリティ事案を取り扱うため、社長を ISO 事務局長として対象範囲のすべての部門責任者（部門長）および内部監査責任者、システム管理責任者等により構成され、毎月 1 度の会議において社内の情報セキュリティに係るリスク対応策の実施状況等に関して進捗確認・評価及び課題の抽出等を行っている他、外部のセキュリティ事故についての分析および当社への実装の可否等についての協議も執り行っております。

また、必要に応じて外部のセキュリティアドバイザー等、専門家の意見も聴取しています。



⑵ 教育･研修

社員には、営業秘密の取扱いや情報管理方法を主体とした初任時研修の他、情報セキュリティ事故や予兆等に関する事例検証および残留リスクの周知を主体とした定期研修の受講を義務付けており､その受講実績と理解度テスト等の結果が人事異動や昇進昇格に影響する旨をルール化しています。

また、情報セキュリティの取組みをより強力に実践するために就業規則等で罰則規程を定め、悪質な違反者には厳正に対処することとし、その旨をすべての社員に周知徹底しています。

なお、当社のセキュリティ研修は、業務プロセスを踏まえ、派遣社員や必要に応じて業務委託先の社員も受講するルールとなっています。

⑶ 関連法制の順守

当社では、コンプライアンス（法律遵守）を徹底するため、関連法制を要求事項一覧表の一部として整備を行い、ＩＳＯ事務局会議にて情報セキュリティ問題と同様に 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。

当社では情報セキュリティに係るリスク対応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るべきものと考えた活動を行っております。

公 開

■4. 情報セキュリティ対策の計画、目標

⑴ 情報セキュリティ第三者認証の維持

当社における情報セキュリティ第三者認証の推進は段階的に行うものとします。

- 第一期：ISMS の推進体制の整備と本社業務における取得
- 第二期：プライバシーマークの ISMS への取込み・融合
- 第三期：各 MS 統合によるエンタープライズ型 ISO の推進
- 第四期：ISMS,EMS,QMS 最新版への適用・最適化

昨年度は、第四期の二ヵ年目となる年度であり、ISMS（JIS Q 27001:2014）への適応に重点を置いた年となりました。

今年度については第四期の 3 年目として、今年度に移行審査を迎える品質 ISO・環境 ISO の最新版（JISQ9001：2015、JISQ14001：2015）との融合化（スリム化）、最適化に取り組んで参ります。

⑵ 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力を入れています。教育訓練メニューとしては、セキュリティだけでなく、品質、環境、ビジネスマナーや安全衛生（交通安全含む）、メンタルヘルスやハラスメント防止等も含めており、社員自らが考えて適切に動けるよう、事例検討や討論を主体とした社内集合訓練と内部監査活動等による OJT、マネジメントシステムや内部監査員養成に係る外部の高度人材育成研修等の教育訓練計画を策定しております。

また、当社の情報資産を初めて取扱う者については、あらかじめ情報セキュリティを含めた統合マネジメントシステムに関する初任時研修を受講させ、必要な知識やルールを習得し厳守できると評価された者だけに情報資産の取扱いを認めています。

⑶ 社内外コミュニケーションの促進

当社は、リアルコミュニケーションとして毎月 1 回以上開催される ISO 事務局会議や各部門の月例会議にて社内のセキュリティ事象や報道等から外部のインシデント等を取り上げ、管理策実装の要否検討や新しい技術や製品に関するリスク分析を行う等の取組みを行っております。また、バーチャルコニュニケーションとしてグループウェアを導入し、電子掲示板等を活用する等してセキュリティに関する警告や ISO 事務局会議録、内外のインシデント情報等の共有化に努めて参ります。

今後とも、引き続きこの取組みを継続・強化していくことを計画しております。

公 開

■5. 情報セキュリティ対策の実績、評価

5.1 計画に対する実績

(1) 情報セキュリティ第三者認証の維持

ISMS の PDCA サイクルの推進体制に係る人員・能力面の強化、および残留リスクの周知徹底、情報セキュリティ管理策に係るパフォーマンスの注視については、ISO 事務局構成員に部門責任者（部門長）を選出することにより、ISO 事務局を中心としたトップダウン体制の下で整備・強化を推し進めました。

(2) 社員教育の徹底

ヒヤリハット事例（セキュリティ事象）についての検証を主とした定期教育訓練（講習）、座学を主体とした初任時教育訓練は、客先サイト社員を含めて受講率が 100%となり、当初の計画通り認証範囲の対象職員全員の受講を達成しました。

また、システム管理責任者を輩出している ICT 技術部の職員らは、情報セキュリティに係る専門研修等も受講しており、最新のサイバー攻撃対策にも精通しております。

(3) 社内外コミュニケーションの促進

リアルコミュニケーションとしての ISO 事務局会議、各部門の月例会議については予定通りに実施することが出来ました。また、バーチャルコニュニケーションとしてグループウェアについては、電子掲示板等を活用したセキュリティ警告、ISO 事務局会議録や内外のインシデント情報等の参照に努めました。結果として、セキュリティ事象おけるヒューマンエラー割合が引き続き減少傾向を示しております。

5.2 年度実績報告

(1) 法令対応報告

本報告の対象期間中は、セキュリティに係る法的要求事項の変更（改正）等に伴うリスク対応策の見直し等の処置実績はありませんでした。

法令対応状況（平成 28 年度）

法令名	施行期日	主な改正点	見直し内容
—	—	—	—

※平成 27 年度実績：マイナンバー法

公 開

(2) 教育訓練計画及び実績報告

本報告の対象期間中は、情報セキュリティを含む ISO 教育訓練に関して社内集合研修等を実施しました。

社内研修実施状況（平成 28 年度）

研修名	内容	対象者	受講人数	備考
ISO 初任時研修	情報セキュリティを含む、マネジメントシステムに係る社内規定等の解説や理解度テスト	9 人	9(29)人	ﾋﾞﾙﾒﾝﾃﾅﾝｽ業務職員の減少
ISO 定期教育訓練	情報セキュリティを含む、自社および他社のヒヤリハット（事象）・インシデント等の事例検討、残留リスクの確認等	37 人	37(35)人	初任時研修受講者数を含まず。協力会社含む
ISO 臨時教育訓練	ヒューマンエラー等によりセキュリティ事象が再発した者に対する再教育等	0 人	0(2)人	

※( )内の数値は前年度（平成 27 年度）実績

社外研修実施状況（平成 28 年度）※情報セキュリティに関する専門研修のみ

研修名	内容	受講人数	備考
ISMS 受審セミナー	情報セキュリティの重要性と ISMS 規格の理解	2 人	

※昨年度実績：マイナンバー法関連研修×4 人、マイナンバーIT 業者向け研修×1 人

(3) 社外インシデントの検討件数と実装状況報告

本報告の対象期間中は、社外の情報セキュリティインシデントを検討して必要に応じたリスク対応策について実装しました。

社外インシデント検討状況（平成 27 年度）

インシデント検討数	うち実装数	実装内容
23(18)件	2(0)件	①ユーザーアドレスで取得されるメールに関する注意・警告等に関する緊急教育を実施。 ②情報資産台帳の臨時見直しを実施。

※( )内の数値は前年度（平成 27 年度）実績

公 開

(4) セキュリティ緩和策の実施状況報告

本報告の対象期間中は、管理策の過剰等による緩和に係る起案実績はありませんでした。

リスク緩和検討状況（平成 28 年度）

リスク緩和検討数	うち緩和数	リスク緩和内容
2(0)件	2(0)件	①音信不通や受取り拒否した者への履歴書等の個人情報書類一式の返還手順見直し（事前に処分に係る同意書取得）。 ②カメラを一定条件下でローカル PC に直に接続して、画像データを取扱うことを容認。

※( )内の数値は前年度（平成 27 年度）実績

(5) マネジメントレビューのインプット・アウトプット報告

本報告の対象期間中は、マネジメントレビュー（MR）を開催しました。

MR のインプット・アウトプット状況（平成 27 年度）

開催日	判断材料（インプット）数	決定事項（アウトプット）数	備考
H29.4 月期	20(20)件	12(12)件	なし

※( )内の数値は前年度（平成 27 年度）実績

(6) 事業継続計画訓練の実施結果報告

本報告の対象期間中は、事業継続計画訓練を実施しました。

事業継続計画訓練結果（平成 28 年度）

実施日	対象事象および試験	前提復旧時間	復旧時間	フィードバック（対応）
H27.8.15	標的型攻撃（発生確率 D、優先順位 D）	3 日間以内	約 20 分	ローカル PC 及びファイルサーバーにテストウィルス「EICAR」を侵入させ、ネットワーク分離やウィルスの隔離手順等を確認しました。テストウィルスは予定時間内かつ適切に除去されました。

※前年度は平成 27 年 7 月 13 日付実施

(7) 施設の選定結果報告

本報告の対象期間中は、施設の選定は行われませんでした。

施設選定結果（平成 28 年度）

公 開

建物名称および住所	調査日	評価項目数	平均点	備考
—	—	—	—	—

(8) 事故等報告

本報告の対象期間中には、事業に影響を及ぼし得るセキュリティ関連の事故（重要資産の盗難・紛失・流用、システムダウン、情報流出等々）は発生しませんでした。

事故等発生件数（平成 28 年度）

	営業部門	ﾋﾞﾙﾒﾝ業務部門	ﾋﾞﾙﾒﾝ業務ｻｲﾄ	IT 業務部門	総務経理部門	ISO 事務局
セキュリティインシデント（事故・事件）	0(0)件	0(0)件	0(0)件	0(0)件	0(0)件	0(0)件
セキュリティ事象（ヒヤリハット事例）	0(6)件	0(1)件	3(2)件	6(3)件	3(2)件	0(3)件
是正要求（内部監査）	2(2)件	2(1)件	12(14)件	1(1)件	0(0)件	0(1)件
是正要求（第二者監査）	実施されませんでした					
是正要求（第三者監査）	0(0)件	0(0)件	0(0)件	0(0)件	0(0)件	0(0)件
観察事項（第三者監査）	0(0)件	0(0)件	0(0)件	0(0)件	0(0)件	2(3)件

※( )内の数値は前年度（平成 27 年度）実績

(9) 外部の利害関係者からの苦情・クレーム

本報告の対象期間中に、当社のセキュリティ上の不手際等によるクレーム・苦情が以下の通りに発生しました。

苦情・クレーム等発生件数（平成 28 年度）

	営業部門	ﾋﾞﾙﾒﾝ業務部門	ﾋﾞﾙﾒﾝ業務ｻｲﾄ	IT 業務部門	総務経理部門	ISO 事務局
クレーム	0(1)件	0(0)件	0(0)件	0(0)件	0(0)件	0(0)件
苦情	0(1)件	0(1)件	0(1)件	0(0)件	0(0)件	0(0)件

※( )内の数値は前年度（平成 27 年度）実績

公 開

5.3 実績に対する評価

(1) 情報セキュリティ第三者認証の維持

昨年度は、最新版規格（ISO/IEC 27001:2013（JIS Q 27001:2014））の適合性と有効性等に重点を置いた審査が行われました。ICT 技術部においては、当該部門長が別組織（ISMS 認証組織）から転職して就任した直後のタイミングとなったことから、当社の ISMS への理解度に不安が残りましたが、ISO 事務局長がフォローする方法等により、結果的として、数点の改善余地事項があったものの無事に合格することができました。

(2) 社員教育の徹底

昨年度については企業に対するサイバー攻撃が急増している状況を踏まえ、定期教育訓練（講習）時に標的型サイバー攻撃の事例紹介、及びその対策に係る演習等を行いました。当社における PC メールの受診は平均して 1 日 300 通を超えるところですが、未だに全てのローカル PC においてコンピュータウィルスを一度も検出していない状況を維持しているのは、これまでの物理・論理的な対策等と相まって、本教育が有効に働いている賜物と考えております。

初任時研修については、昨年度に引き続き各マネジメントシステムとのバランスを意識した教育内容としました。これにより、引き続き情報セキュリティへの過剰反応等により、本来業務へ支障を来たすような事態にならなかったものと評価しています。

(3) 社内外コミュニケーションの促進

ここ数年間、リアルコミュニケーションとバーチャルコニュニケーションを合わせた運用に取り組んでおりますが、昨年度におきましてもヒューマンエラーは漸減していることから、取り組みは引き続き有効であると評価しています。一方、外部コミュニケーションにおきましては、一昨年の ISO/IEC 27001:2013（JIS Q 27001:2014）移行審査において、審査員より「本書に関する発信状況については、改善の余地がある」とされたことから、昨年度中に環境報告書に倣って、当社 HP のトップページに専用バナーを配置する等、サイト訪問者の誰もが目に付くようなデザインといたしました。また、本報告書につきましても、今公開分からページ背景にデザイン性を取り入れる等して、外部コニュニケーションを意識した仕上げといたしております。

公 開

■6. 情報セキュリティに係る主要注力テーマ

6.1 情報セキュリティ対策に係る主要注力テーマ:「お客様資産の保護」

(1) 基本的な考え方

当社は、ソフトウェア開発及びシステム保守、ＩＴソリューション業務等を通じてお客様自身の個人情報を含め、お客様の大切な資産をお預かりしています。これらお客様資産の保護は当社の生命線であり、こうした資産を保護するために当社では資産台帳を作成し、リスク分析し、必要な管理策を講じ、合わせて資産を取扱う社員に対する教育が適切に行われていることについて、ISO 事務局活動等を通じて監視することとします。

(2) お客様資産の管理方法

①物理的・技術的管理

・社外との通信手段として電子メールを利用しますが、重要（秘密）とされたデータ等については伝送時にパスワードにより保護するか、暗号化の上でパスワード保護する措置を義務付けています。最重要（極秘）とされたデータ等は、原則、電子メールでの伝送を禁止しております。

・社外との搬送手段として社外便を利用しますが、重要（秘密）とされた書類等については二重封筒にて書留（郵便事業会社）とするか、運送業務委託先として選定した業者にのみ厳重な梱包をした上で　引き渡すこととしています。最重要（極秘）とされた資料等は、原則、社外便の利用を禁止し、手渡しによることとしています。

・重要（秘密）の資産である場合は、資産そのものに対して「秘密」または「機密」ラベルを貼り付ける等して、一般資産と区別を図っています。

・重要（秘密）資産を取扱える者を限定し、その取扱いに関する履歴を可能な限り記録しております。

・重要（秘密）資産の保管場所を特定し、また管理者が施錠する等して管理しております。

・重要（秘密）資産の廃棄時には、お客様の同意を得るとともに特定の管理者が漏えい・流用等が無いように適切に処理しております。業者に委託する場合は、セキュリティに関する認証を取得している業者の中から廃棄業務委託先として選定した先のみに取り扱わせることとしています。

・お客様の所有する建物等の鍵をお預かりする場合は、鍵預り証を発行するとともに、鍵を保管する社員について身元保証書の提出を義務付けている他、厳正な取扱いルールを規定し毎月１回以上は、その取扱いに係る点検等の監視活動を行っています。

・情報機器や基幹系ソフトウェア等については、そのログインパスワードを会社側が一定期間で強制変更するルールとなっています。

・各情報機器に設定された OS 等のアップデートは、毎月 1 回以上、会社側が強制的にセキュリティパッチを適用すること等により、脅威に対して常に最新の状態を保てるようにしています。
・当社は、建物における物理セキュリティも強化しております。具体的には、施設の休日・夜間早朝の無人状態時用の機械警備の他、執務用スペースと来客用スペースは非接触型 IC カードロック方式、またはタッチパネル・デジタルロック方式によるセキュリティドア等により隔離しております。

②人的・法的管理

・社員と秘密保持契約を締結しているほか、重要（秘密）資産を取扱う者については身元保証書の提出を義務付けています。
・新たに ISMS の認証スペースにおいて丸 1 日を超えて業務を行うこととなった者につきましては、社員かどうかに関わらず、ISO 初任時教育訓練の受講（実習含む）および確認テストへの合格等を義務付けております。
・重要（秘密）資産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。
・退社に当たっては、重要（秘密）資産を持ち出されることのないよう、重要（秘密）資産を全て当社に返還するような仕組みを構築しております。またその際、何が重要（秘密）資産かということを特定してあるため、社員とのトラブルは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

・重要（秘密）資産を保有する組織全体のマネジメントに取組み、セキュリティ管理体制の整備を行っております。
・社内コニュニケーションとして、リアルコミュニケーションとバーチャルコニュニケーションを取り入れ、情報セキュリティ事故等に関する情報の共有、社員の意識付けを図っています。

公 開

■7. 第三者評価・認証

当社は、2008 年 6 月に ISMS 適合性評価制度に基づく認証を取得しました。

・ ISMS 適合性評価制度承認取得概要

①認　証　範　囲：建築物及び付帯施設に対する清掃、設備保守、衛生管理業務、並びにアプリケーションソフトウェア開発、システム保守サービス等ＩＴソリューション業務の提供

②取 得 認 証 規 格：ISO/IEC27001:2013（JIS Q 27001:2014）

③最 新 登 録 番 号：IC13J0364

④登　　録　　日：2008 年 6 月 24 日

⑤最新登録審査機関：株式会社 日本環境認証機構（JACO）

⑥認　証　機　関：一般財団法人 日本情報経済社会推進協会（JIPDEC）

更新審査

2016 年 8 月 29～30 日に株式会社 日本環境認証機構により更新審査が実施され、重大および軽微な指摘事項共に有りませんでした。「改善余地有り」とされた 2 件については、速やかに対応計画を策定して、既に対処済みとなっております。