情報セキュリティ運用規程

1. 目的
本規程は、株式会社シンニチの業務に関連するスタッフが、情報及び情報システムを扱う際に守らなければならない事項を明確にし、会社として情報資産の保護を確実にすること並びに、当社のお客さまの情報セキュリティの確保を確実にすることを目的とする。

2. 適用範囲
本規程の適用範囲は、株式会社シンニチの本社及び各支店業務とする。

3. 所管および実施責任
総務部長は、情報セキュリティ管理責任者として全社の情報セキュリティ管理業務を担任するとともに、各部門の情報セキュリティ責任者を指名する。(別紙　情報セキュリティ管理体制による)
情報セキュリティ責任者は、各部門の情報セキュリティに関する業務を実施し、責任を負う。

4. 基本方針
(1)業務で使用する情報機器(注1)は会社所有のものを使用し、また必要なソフトウェア以外はインストールしない。
(2)個人所有の情報機器は会社に持ち込まず、また業務では利用せず、情報も保管しない。
また会社のメールアドレスを設定したり、会社のメールを転送したりしない。
(3)業務上必要な情報以外にはアクセスしない。
特別な事情からアクセスする必要が生じた場合には情報セキュリティ責任者の許可を得た上で行う。
(4)常に6S(整理・整頓・清掃・清潔・躾・作法)に務め、情報セキュリティのリスクを低減する。
(5)その他会社や部署で決められたルールは厳守する。

注1　情報機器とは、業務で使用するパソコンやPDAを含むコンピュータおよび業務で使用する携帯電話を指す。なお、特例的に個人所有の携帯電話を業務用途で使用する場合(客先等との通話や写真撮影や業務データの送受信などに使用する場合など)には含むものとする。

5. 運用規程
5.1 規程の適用対象者
5.1.1 用語の定義
本規程における用語の定義を以下に定める。
(1)スタッフ
社員および協力会社社員により構成される。
(a)社員
当社の社員
(b)協力会社社員
当社の管理下で業務を行う、他社の社員。
(2)第二者(顧客)
当社のお客さま
(3)訪問者
当社の情報処理施設及び設備に関するアクセス権限を都度与えられる外部の者。
(4)外部委託者
当社の業務を委託されて行う外部の者
(5)情報セキュリティ責任者
部または課、支店の単位で1名、課長職以上のものが選任され、情報セキュリティ業務実施の責任を負う。
(6)情報セキュリティ管理責任者
全社の情報セキュリティ管理業務を統轄、推進する。

5.1.2 スタッフの役割と責任
スタッフは、関係法令、服務規律を遵守し、本規程に基づき情報セキュリティ運用業務を遂行する。

5.2 教育および確認の実施
5.2.1 協力会社との契約
(1)協力会社の決定に当たっては、情報セキュリティの管理上信頼できる会社とする。
(2)契約に当たっては必ず機密保持に関する条項の入った基本契約を締結する。
(3)情報セキュリティに関する管理者を選任して頂き、協力会社社員全体に情報セキュリティ意識を浸透させる。

5.2.2 入社・新規入場時
(1)機密情報保護教育を情報セキュリティ責任者あるいはその指名を受けた代理人が実施する。
(a)機密情報保護教育資料に基づき教育を実施する。
(b)「機密保持誓約書」に記名・捺印後は該当部署が保管し、コピーを総務部に送付する。
(2)同時に服務規律の教育を実施する。
(3)貸与品(パソコン、記憶媒体等)の記録管理をする。
この台帳の保管・運営は情報セキュリティ責任者が責任を持つものとする。

5.2.3 定期教育
(1)年に一度5.2.2(1)(2)の教育を実施する。

5.2.4 退社・退場時確認・点検
(1)情報セキュリティ責任者が貸与品の回収と管理簿のチェックを実施する。
(2)業務を遂行するに当たり付与したID・パスワード・各種権限は全て消去する。
(3)入社・入場教育時に取得した誓約書の内容に違反していないかの確認を行うとともに、
退場後においても、守秘義務を厳守することを確認する。
「機密保持誓約書」は退社・退場後においても、該当部署にて保管する。

5.2.5 その他
社員は情報保護や漏洩などの事例を関係者に周知し、それがお客様や当社に
与える影響や損害を朝礼やメール等で注意喚起し、情報保護の趣旨徹底を図る。

5.3 ドキュメントおよび媒体の取扱い
5.3.1 管理方針
(1)ドキュメント(データを含む以下同じ)および媒体などの情報資産については事前に
該当部署にて取り扱う情報資産の取り扱いを定め部署内に周知徹底する。
(2)情報機器は資産管理台帳に登録する。
(3)情報資産(ドキュメント、データ、ソフトウェア、記憶媒体)は情報資産台帳に登録する。
(4)次の場合、事前に情報セキュリティ責任者の承認を得る。
(a)情報資産の生成、移動、破棄等、資産リストを変更すべき処置を行う場合。
(b)「5.3.3 分類ごとの取扱い」の範囲を越えた取り扱いの必要が生じた場合。

5.3.2 取り扱い細則
(1)ドキュメントについては情報資産の取り扱い区分に応じた取扱を厳守し、特に定められているドキュメントについては施錠の出来る書棚に収容し、使用の都度開錠と施錠を徹底する。なお鍵については厳重に管理する。
(2)プリンタで印刷したドキュメント、およびFAX等から出力されたドキュメント、
あるいはスキャナーで使用したドキュメントは速やかに収集し放置しない。
(3)個人所有の記憶媒体を持込まず、必ず会社所有の機器・媒体を用いる。会社所有の機器・媒体については「IT資産管理台帳」、または「情報資産台帳」を用い日々管理を行い、また施錠の出来る書棚等で保管する。
会社所有の機器・媒体の支給については会社規程に沿って申請・運用を行う。
利用者間の無断での貸し借りは禁止する。
(4)ドキュメントまたは記憶媒体を社外に持ち出す場合、情報セキュリティ責任者の許可を得た上で行うものとしカバンに入れ携行する。またくれぐれも置き忘れおよび盗難等に注意し、必ず目の届く範囲で取り扱う。
また持ち出す際には必ず「情報資産持出管理台帳」に記録を残し返却時にも記録する。
返却済・未返却の確認も毎月実施すること。
(5)USBメモリー等の外部記憶媒体を使用する際には、セキュリティロック機能を使用する。
また社外に持ち出す場合には必ず暗号化を施し情報漏洩を防止する。
なお返却時には必ずデータを削除した上で返却する。
(6)5.3.3項における社外秘以上の機密性を持つドキュメントはサーバーに保管するものとし、
クライアントである情報機器には保管しない。
情報機器への保管が必要な場合には情報セキュリティ責任者の許可を得た上で行う。
(7)協力会社などにドキュメント・記憶媒体を渡す場合には、双方の間で機密保持契約が
締結されていることを予め確認した上で渡す。なお機密保持契約がない場合には、
必ず情報セキュリティ責任者の許可を得た上で渡す。受渡しの際には必ず「情報資産貸与品管理台帳」に記録を残す。業務が終了した時点での処置についても必ず確認を行う。
(8)必要に応じ、情報のバックアップを作成し保管する。
(9)ドキュメントまたは記録媒体を発送する場合には、二重封筒や開封防止梱包等の対策を講じる。
(10)保存期間を定めているドキュメントを除き、不要となったドキュメント・CD・DVD等の媒体は速やかに、
シュレッダー等を用いて再利用が不可能な形で廃棄する。
(11)公共の場所および人目の多い場所で情報機器および資料などを閲覧しない。
但し、やむを得ず閲覧が必要な場合は、壁を背にする等、十分注意する。
(12)ホワイトボードは使用後に書き込みを全て消去する。
(13)机上には作業に必要なもののみ置き、不要なものは机・書棚・カバンに収納する。
(14)情報資産の入ったカバンを携行する際には、電車の網棚などに放置せず、
常に手元に置いて管理する。また持ち出した状態で、寄り道および遊行しない。
(15)情報資産を所持したままでの帰宅は「情報資産持出管理台帳」に記入し、
情報セキュリティ責任者の承認を得るものとする。外出先等から承認を得たい場合はメール等で連絡し、
後に「情報資産持出管理台帳」に記入してその記録を残すこと。

5.3.3 分類ごとの取扱い
情報資産の分類は情報セキュリティ責任者が部長の承認を得て行うものとする。
なお、5.4項の規定にかかわらず、業務上の必要によってセキュリティエリア外へ情報を持ち出す場合には、
情報セキュリティ責任者の許可を得た上で行う。
情報セキュリティ責任者は情報の秘密レベルに応じて、社外秘の場合は部長、
極秘の場合は社長の許可を得ることとし、「重要情報資産持出管理台帳」に記録を残す。

5.4 セキュリティエリア

5.4.1 セキュリティエリアの設置

シンニチのセキュリティエリアは執務室内とする。

5.4.2 セキュリティエリアの管理方針

(1)業務に必要の無いものは机上に放置しない(カバン内に収容)

(2)最初の入室者および最終退出者は、玄関通用口にある「入退社」警備カードを使用し
最初と最終の出入りの管理を行う。

(3)執務室内へのスタッフ以外の入室は原則として禁止し、顧客やその他やむを得ない事情がある場合には、
事前に情報セキュリティ責任者の許可を得るとともに朝礼等でフロアのスタッフに周知した上で、
入室をして頂くこと。その際は、社員が立ち会うこと。

(4)見知らぬ人がフロアに入って来た場合、声をかけ用件を伺うようにすること。
(なお応対には失礼のないようにすること。)

(5)直行直帰の際に情報資産を所持したまま自宅や宿泊場所に帰る場合には
情報セキュリティ責任者の許可を得ること。

5.5 情報機器管理

5.5.1 管理方針

(1)物理的に保護された環境に設置する。

(2)電源は、安定供給に配慮する。

(3)電源及びネットワークケーブルは安全な配線を行う。

(4)定期的および緊急時のメンテナンス方法を明確にする。

(5)情報機器の安全な利用について情報セキュリティ責任者から指導する。

(6)敷地外に設置された機器は、その環境に合わせ、適切に保護する。

(7)無人の状態になる機器に対し、情報漏洩を防ぐ為の措置を施す。

(8)機器の廃棄・再利用時には、格納された情報の漏洩を防止する措置を施す。

5.5.2 情報機器運用管理

(1)情報機器に情報を格納する場合可能な範囲でアクセス管理、暗号化等を行う。

(2)ディスプレイ装置は、部外者から表示画面が見えにくい設置場所に配慮する。

(3)利用者がいない情報機器の放置を禁止する。

(4)パソコンはパスワードを設定した上で使用する。
携帯電話についても業務で使用するものは紛失時に備えてリモートセキュリティの設定を施すか、
パスワードロックをかけた上で使用する。

(5)情報セキュリティ責任者の許可のない情報機器の持出しを禁止する。また持ち出す場合には
「情報資産持出管理台帳」に記入の上で持ち出すものとする。

(6)個人所有情報機器の社内持ち込みは禁止する。
やむをえない場合には事前に情報セキュリティ責任者の承認を得る。

(7)執務室からの退出時には情報機器を施錠するか、施錠の出来る書棚等に収容する。

(8)客先から借用している情報機器やデスクトップパソコンはワイヤーロック等を用いて物理的な持ち出しを防止する。
またワイヤーロックキーは情報セキュリティ責任者の管理下に置く。

(9)それぞれのソフトウェアには最新のパッチを適用する。また社内ネットワークに社外からアクセスする場合は
ファイアウォールを介して接続するものとし、Windowsとウイルス対策ソフトが最新バージョンであることを確認する。
メーカーサポートの終了したOSは原則として使用せず、止むを得ず使用する場合は、
情報セキュリティ責任者の承認を得る。

(10)ファイル交換ソフトやインスタントメッセンジャーソフト等についてはインストール厳禁とする。

(11)作成者が不明の不審なファイルや業務に必要の無いデータは開封・保管をしない。

5.6 IDパスワード管理

5.6.1 管理方針

(1)システムの利用者登録(および抹消、変更)とその管理に関する基準を明確にする。

(2)システム権限に関する取り決めを明確にする。

(3)ID、パスワードは、秘密を守るように自ら責任を持って管理し、他人に伝えたりせず、
人目に触れないようにする。また他人のIDやパスワードは盗み見せず、聞かず、使わない。

(4)ID、パスワードは、6文字以上とし、類推の困難なものを用いる。
可能なものは3ケ月に一度以上の頻度で変更を行う。

(5)ID、パスワードが不要になった場合は、速やかにその停止や削除を発行元に依頼する。

5.7 コンピュータウイルス管理

5.7.1 ウイルス対策ソフトの導入

(1)情報機器およびファイルサーバを導入対象とする。

(2)情報通信システム部による「ソフトウェア/ハードウェアの購入および導入」に定めている標準製品リストで
指定されたウイルス対策ソフトを選択する。

(3)選択するウイルス対策ソフトは、以下の機能が含まれていなければならない。
(a)定義ファイルの自動更新機能
(b)常時スキャン機能

5.7.2 ウイルス対策ソフトの利用
(1)情報機器に導入されたウイルス対策ソフトを常駐設定にし、ファイルへのアクセスおよびファイルのダウンロード時、電子メールの送受信時には常時スキャンできるよう設定する。
(2)常時スキャンだけではなく、一週間に一度以上、ハードディスク全体に対するスキャンを実施できるよう、ウイルス対策ソフトを設定する。
(3)定義ファイルを毎日一度は更新できるようにウイルス対策ソフトを設定する。

5.8 システムおよびサーバー運用管理
5.8.1 管理方針
(1)操作時に必要なセキュリティ対策を含んだ操作手順書を作成する。
(2)運用変更時は適切な管理を行い、システムのトラブル発生を防止する。
(3)システムの変更手順書を作成し、変更作業を管理する。
(4)オペレーティングシステム変更に際し、レビューフローおよび試験手順書を作成する。
(5)情報セキュリティ責任者がシステム運用管理担当者を任命する。
(6)検証環境と運用環境を分離する。
(7)システムの処理に関わる容量を見積り、管理する。
(8)システムの受入れ基準を確立し、適切な試験を実施する。
(9)システムの情報および設定値のバックアップを適切に行う。
(10)オペレータの操作記録として、運用日報・作業指示書を作成する。
(11)システムに関わる障害は、障害報告書を作成し記録および管理する。
(12)システムの要求事項を記述した文書では、セキュリティ管理対策に関する要求を明確にする。
その際Need To knowの原則(情報を知る必要がある者にのみ権限を与える)に従って権限設定を行う。
(13)ソフトウェア導入に際し、手順書を作成する。
(14)ソフトウェアの購入経路ならびにソフトウェアの利用・修正履歴を適切に管理する。
(15)パスワードは類推困難なものとし、管理者パスワードは厳格な管理を行う。
(16)必要なソフトウェア以外はインストールしない。

5.9 社内ネットワーク接続管理
5.9.1 管理方針
(1)システム運用管理担当者が社内ネットワーク接続の一元的な管理を行う。
(2)機密性、完全性、可用性すべてに配慮し、安全な運用を行う。
(3)最新の構成図等を整備し、状態を把握する。
(4)管理手順を明確にし、管理ミスを防止する。
(5)容量管理およびアクセス制御を適切に行う。
(6)社内のネットワークには会社が所有している情報機器以外の接続を認めない。
やむをえない場合には事前に情報セキュリティ責任者の承認を得る。
(7)サーバーや情報機器を外部ネットワークと接続する場合には、承認を得た上で実施する。

5.10 メール送受信管理
5.10.1 管理方針
(1)パソコンやメールアドレスを含むメールの送受信環境は業務上与えられた会社資産であることを理解し、会社の用件以外でのメールの濫用を禁止する
(2)会社のアドレスから個人所有パソコン／個人メールアドレスへの転送は禁止するとともに、個人所有パソコンでの会社アドレスの使用は禁止する。また業務用であっても外部アドレスへの自動転送は禁止する。
(3)ドキュメント全般の取り扱いは5.3項の扱いに従う。
(4)外部へメールを送信する場合、宛先は必要者にのみ限定した上で間違いの無いよう充分に確認した上で送信する。また複数ドメインのユーザーに送る場合にはbccに宛先をセットして送信する。
(5)社外に添付ファイルをメール送信する場合には、必ずパスワード設定を施した上で送信する。

5.11 インターネット接続セキュリティ
5.11.1 管理方針
(1)情報システム利用者に与えるアクセス権限は、Need To knowの原則(情報を知る必要がある者にのみ権限を与える)に従い制御する。
(2)情報セキュリティ責任者がアクセス権限の登録・変更・抹消の管理を行う。
(3)情報機器にてインターネットに利用する場合は、申請し許可を得た上で行う。
(4)業務目的以外でインターネットを濫用してはならない。
また業務上必要なファイル以外をダウンロードしてはならない。

5.12 システム利用監視
5.12.1管理方針
(1)システムの利用を監視するため、監査ログを取得し、定期的にログのチェックを行う。
(2)監視目的に合わせ、監査ログチェック方針を見直す。
(3)監査ログは、その完全性を維持するために適切に保護する。
(4)監査ログの信頼性を維持するため、システムクロックを同期化する。

5.13 コンプライアンス管理

5.13.1 管理方針

各情報システムおよび組織のすべてに関連する法令、契約上の要求事項、
およびこれらの要求事項を満たすための組織の取り組みを、本規程において定め、最新の状態に保つ。

5.14 その他一般

(1)会話や日頃の言動について

(a)飲食店、電車など公共の場所では業務に関する話題を避けること。

(b)社内であってもオープンな会議スペース、通路等では機密に関する話は周りに注意して行うこと。

5.15 緊急の場合(エスカレーション)

5.15.1管理方針

次の場合には、速やかに直属の上長並びに情報セキュリティ責任者に報告を行い、
情報セキュリティ責任者は「機密情報漏洩報告書」で報告を行う。
休日の場合にも連絡網に従い翌勤務日まで待たず速やかに報告を行うこと。

①情報漏洩(可能性の場合も同様)が発覚した場合。

②情報保護に関連して顧客や外部からクレームを受けた場合。

③情報機器や付属機器を紛失した場合。

④業務に使用したパソコンがウイルスに感染していたり、ファイル交換ソフトウェアが検出された場合。
(なおその場合速やかにLANケーブルを抜くこと。)

⑤その他本規程から逸脱した運用が行われていた場合。

5.16 内部監査

5.16.1 管理方針

(1)内部監査を行い、業務で使用している情報機器の点検と、必要に応じて是正処置を実施する。

(2)「内部監査チェックシート」に基づいた情報保護内部監査を実施し、必要に応じて
部署としての是正処置を実施する。

(3)期毎に1回、内部監査結果を取りまとめ報告する。

6. 有効期限及び見直し時期

本規程は平成30年7月2日より改訂施行され、1年間有効とする。有効期限終了までに、所管部署が見直しを実施した後、1年間有効とし、以後この例にならう。

令和2年4月1日

株式会社 シンニチ

代表取締役 社長 齋藤 修