情報セキュリティ規程

社会保険労務士法人さつき

制定日:　　2024年4月1日

目次

1. 適用範囲

本規程は社会保険労務士法人さつき（以下、当法人）の状況の下で、情報セキュリティ運用手順を確立し、実施し、維持し、継続的に改善するための要求事項について規定する。

2. 組織の状況

2.1.組織の役割、責任及び権限

情報セキュリティに関連する役割に対して、責任及び権限を割り当て、伝達する。

役職名	役割と責任
最高責任者 楯本 智久	情報セキュリティに関する責任者。決定権限を有するとともに、全責任を負う。
情報セキュリティ管理責任者 楯本 智久	情報セキュリティ管理責任者。各部門における情報資産に対するセキュリティ実施などの責任を負う。
システム管理責任者 楯本 智久	システム管理責任者。各部門におけるシステムセキュリティ実施などの責任を負う。
教育責任者 楯本 智久	情報セキュリティを運用するために従業者への教育を企画・実施する。
監査／点検責任者 楯本 智久	情報セキュリティが適切に実施されているか情報セキュリティ関連規程を基準として検証または評価し、助言を行う。

2.2.情報セキュリティの取組みの監査/点検

監査/点検責任者は、情報セキュリティ関連規程の実施状況について、毎年12月に点検を行い、監査/点検結果をDX委員会に報告する。DX委員会は、報告に基づき、以下の点を考慮し、必要に応じて改善計画を立案する。

・情報セキュリティ関連規程が有効に実施されていない場合は、その原因の特定と改善
・情報セキュリティ関連規程に定められたルールが、有効でない場合は、情報セキュリティ関連規程の改訂
・情報セキュリティ関連規程に定められたルールが、関連法令や利害関係者の要求や提供できる価値を満たしていない場合は、情報セキュリティ関連規程の改訂

3. 計画

3.1 一般

計画を策定するとき、次の事項のために対処する必要があるリスク及び機会を決定するための手順を以下に定める。

a) 望ましくない影響を防止又は低減する。
b) 継続的改善を達成する。

3.2 情報セキュリティリスクアセスメント

当法人は、次の事項を行う情報セキュリティリスクアセスメントのプロセスを定め、適用する。
a) 管理責任者は、次を含む情報セキュリティのリスク基準を確立し、維持する。
 1) リスク受容基準
 2) 情報セキュリティリスクアセスメントを実施するための基準
b) 管理責任者は、繰り返し実施した情報セキュリティリスクアセスメントが、一貫性及び妥当性があり、かつ、比較可能な結果を生み出すことを確実にする。
c) 管理責任者は、次によって情報セキュリティリスクを特定する。
 1) 適用範囲内における情報の機密性、完全性及び可用性の喪失に伴うリスクを特定するために、情報セキュリティリスクアセスメントのプロセスを適用する。
 2) これらのリスク所有者を特定する。
d) 管理責任者は、次によって情報セキュリティリスクを分析する。
 1) 特定されたリスクが実際に生じた場合に起こり得る結果についてアセスメントを行う。
 2) 特定されたリスクの現実的な起こりやすさについてアセスメントを行う。
 3) リスクレベルを決定する。

 組織は、情報セキュリティリスクアセスメントのプロセスについての文書化した情報として「情報資産台帳」を保持する。

「情報資産台帳」参照

4. 運用

4.1 雇用

雇用または契約する際には、雇用契約書、就業規則および機密保持契約書に、情報セキュリティに関する責任を記載して、雇用または契約する。

4.2 情報セキュリティの意識向上、教育及び訓練

組織の全ての従業員、及び関係する契約相手は、職務に関連する組織の方針及び手順についての、適切な、意識向上のための教育及び訓練を受け、また、定めに従ってその更新を受ける。ただし、組織のマネジメントシステムを構築した経験を有する場合は訓練されたものとする。

4.3 雇用の終了又は変更に関する責任

雇用の終了または変更の際には、以下の事項を実施する。

①アクセス権限の破棄または変更
②引き続き、業務上で知り得た機密情報についての守秘義務があることの確認

4.4 資産の管理責任

管理責任者または一般従業者は、情報資産台帳に従って、資産を管理する。

4.5 資産利用の許容範囲

情報の利用の許容範囲、並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は、情報資産台帳の機密性基準とする。

4.6 情報の分類

管理責任者は、取り扱う情報、重要性、及び影響範囲等の度合いの観点から、適切に情報を分類する。

必要とする情報を容易に識別できるよう、情報のラベル付けについて次に定める。

・電子データは、顧客、プロジェクトごとなど意味のある単位でフォルダにまとめる。

・電子データは、容易に検索ができるよう、ファイル名に共通の接頭辞を付ける、またはそれを含むフォルダ名にその文字列を含める。

・印刷物や記録媒体は、顧客、分類ごとなど意味のある単位で、バインダー、ファイルボックス、ケースにまとめる。

4.7 資産の取扱い

管理責任者または一般従業者は、資産の価値、重要度等によって分類された情報資産台帳に従って、資産を取り扱う。

4.8 媒体の処分

必要がなくなった場合で、かつ、所管法令等において定められている保存期間等を経過したときには、できるだけ速やかに復元できない手段で削除(「米陸軍準拠方式 (AR380-19)」に準拠した全箇所を3回上書き)又は廃棄(断片化、粉砕、焼却、融解)する。

4.9 アクセス制御

・情報に対するアクセス制御は、利用者の職務や役割に応じて最低限の利用範囲を特定し、適切に設定する。

・情報処理施設等へのアクセスは、その情報処理施設等を管轄する事業者が正式に定めた手順に従い、アクセスする。

・外部のネットワーク及びネットワークサービスの利用においては、暗号鍵による認証またはパスワードによる認証を必須とする。また、パスワードは記号1つ以上を含む半角英数字8文字以上とする。

・システム及びアプリケーションへのアクセスは、セキュリティに配慮したログオン手順により、制御する。

・明確に許可を受けていない情報へのアクセス及び操作をおこなってはならない。また、その試みを行うこともしてはならない。

4.10 ネットワーク及びネットワークサービスへのアクセス

管理責任者又は管理責任者が許可した一般従業者は、以下の事項を実施することにより、利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを利用者に提供する。

・業務を遂行するにあたり必要なネットワーク及びネットワークサービスを継続的に利用するにあたっては、広く認知されているネットワーク及びネットワークサービスを除き、管理責任者による許可を必要とする。

・オフィスに設置される無線LAN(アクセスポイント)は、組織の者が利用するネットワークのみとし、社外の者が利用するネットワークは提供しない。

4.11 利用者登録及び登録削除

4.11.1 利用者アクセスの提供

管理責任者又は管理責任者が許可した一般従業者は、利用者の登録及び登録削除の際に、以下の事項を実施する。

【利用者登録手順】

LANの設定
①管理責任者が許可した一般従業者については、社内LANに接続可能なネットワーク名及びパスワードを通知する。

ファイルサービス
①管理責任者が許可した一般従業者については、システム管理責任者にユーザの追加を依頼する。
②システム管理責任者はファイルサービスにユーザを追加し、一般従業者に通知する。
③利用権限（アクセス権）と利用者を結びつけるために、ID及びパスワード又はそれに準ずるものを発行する。
なお、パスワードは記号を1つ以上含む半角英数字8文字以上とする。

【利用者削除手順】
①一般従業者がファイルサービスを利用する理由がなくなった場合、利用者を結びつくID及びパスワード又はそれに準ずるものを削除し、それにより利用できなくなったことを確認する。
社内LANの利用についての割当及び無効は、利用者が管理責任者に申請をし、管理責任者が通知する。

ファイルサービスの利用についての割当及び無効は、利用者が管理責任者に申請をし、管理責任者からシステム管理責任者に申請をする。設定後、システム管理責任者から利用者に通知する。

4.11.2 アクセス権の削除又は修正

管理責任者は、従業員の雇用終了時に、その従業員が保有する情報及び情報処理施設に対する全てのアクセス権を、雇用終了日又は翌日に、システム管理者責任者に依頼し削除する。

管理責任者は、外部の利用者との契約又は合意の終了時に、その利用者が保有する情報及び情報処理施設に対する全てのアクセス権を、契約又は合意の終了日又は翌日に、システム管理者責任者に依頼し削除する。

4.11.3 セキュリティに配慮したログオン手順

システム及びアプリケーションへのアクセスは、可能な限り以下の事項を満たすセキュリティに配慮したログオン手順により、制御する。

・認証情報の推測の助けとなるようなメッセージを表示しない。
・入力したパスワードは伏字になるなど、表示されない。
・パスワードを平文で通信しない。（HTTPS、SSHなどのセキュアプロトコルによる通信）
・ログオログが取得されている。
・総当たり攻撃及び辞書攻撃から保護している。

4.11.4 パスワード管理システム

利用者が設定可能な、対話式のパスワード管理システムを用いてパスワードを設定、管理する。なお、管理責任者又は資産を管理する一般従業者は、必要に応じて利用者のパスワードを無効化またはリセットできなくてはならない。

また、システム及びアプリケーションが一定のパスワード強度を要求しない場合においても、パスワードは記号を1つ以上含む半角英数字8文字以上とする。

4.12 暗号利用

・機密情報を電子メールで送信する場合においては、相手と予め取り決められた方式によってデータを暗号化する。なお、可能な限り、公開鍵暗号方式の利用を推奨する。暗号化されたメールの送受信が困難な場合おいては、代替手段としてパスワードを施した圧縮ファイルも許容するが、パスワードは記号を1つ以上含む半角英数字8文字以上とする。

・メールに添付ができないファイルサイズの機密情報を送信する場合は、セキュアなファイル伝送サービスを利用する。送信先がダウンロードしたことを確認した時は、速やかに削除することを推奨する。

・機密情報の伝送においては、SSH、HTTPS、SFTPなどのセキュアプロトコルを用いて暗号化通信を行い、漏洩から保護する。

4.13 モバイルセキュリティ

・ノートPCの利用には指紋認証、パターン認証、またはパスワードの入力を必須とする。また、パスワードは記号を1つ以上含む半角英数字8文字以上とする。
・ノートPCを利用する場合には、ハードディスクの暗号化を推奨する。
・ノートPCを社内ネットワークに接続する場合は、WPA2等の暗号化方式で接続する。
・ノートPCを持ち出す場合は、公共の場での紛失を防ぐために、必ず保持することとする。
・スマートフォンの利用には指紋認証、パターン認証、またはパスワードの入力を必須とする。また、パスワードは半角数字4文字以上とする。パスワードの入力に10回失敗した場合はすべてのデータが消去される機能をオンとすることを推奨する。
・スマートフォンを利用する場合には、ハードディスクの暗号化を最も推奨し、次点で、通信事業者等が提供する遠隔操作による機器の無効化、データの抹消サービスの契約を推奨する。

4.14 テレワーキング

クリアデスク・クリアスクリーン方針及びモバイル機器セキュリティ方針を参照のうえ、以下に留意する

・公共のWi-Fiスポットを使用しない
・やむを得ず公共のWi-Fiスポットを利用する際はVPNを利用すること
・ショルダーハックに気をつける
・借りた機器は使用しない
・社内サーバ及びクラウドストレージからダウンロードしたファイルを保持する場合は「情報資産台帳」の機密性に従うこととし、保持の必要性がなくなり次第、削除すること

4.15 セキュリティを保つべき領域での作業

取扱区域内の作業については、情報漏洩を防ぐため、以下の事項を実施する。

・PCやモバイル機器については、長時間・短時間に関わらず離席する場合においては、スクリーンロック等を掛け、情報の漏洩から保護する。なお、スクリーンロック等の解除には指紋認証、パスワード入力を必須とし、パスワードを用いる場合は記号を1つ以上含む半角英数字8文字以上とする。
・機密情報を扱う書類については、長時間・短時間に関わらず離席する場合においては、施錠可能な引き出しに保管し、漏洩や紛失から保護する。
・訪問者の記録装置（モバイル機器が搭載するカメラなど）の利用を禁止する。

4.16 マルウェアに対する管理策

ウイルス対策ソフト、又はそれに準ずるものをインストールし、それが推奨する頻度で定義ファイルを更新する。

4.17 情報のバックアップ

バックアップ用ツール等を活用し定期バックアップを行い、データの損失を防ぐ。

4.18 ソフトウェアのインストールの制限

業務で使用する以外のソフトウェアを無断でインストールしてはならない。必要な場合は、管理責任者の判断によってインストールを行う。

4.19 責任及び手順

当法人は、情報セキュリティインシデントに対し迅速かつ効果的な対応を行い、また、管理者としての責任を果たすため、以下の手順に従う。

・従業員は、インシデント発生時等、必要に応じて最高責任者または情報セキュリティ管理責任者に報告する。
・最高責任者または情報セキュリティ管理責任者は、発生したインシデントについて、必要に応じて、関連する従業員、機関または専門組織等に連絡する。
・最高責任者または情報セキュリティ管理責任者は、関連する機関または専門組織等から得た助言・情報等を、関連する従業員に伝達する。
・具体的な連絡先については、最高責任者または情報セキュリティ管理責任者が定義する。

4.20 情報セキュリティインシデントへの対応

情報セキュリティインシデントは、以下の手順に従い、適切に対応する。

従業員は、インシデントや漏えい等発生時には、組織内においては24時間以内に情報セキュリティ管理責任者まで報告をし、協議する。
【協議内容】
①事実関係の調査及び原因の究明、②影響を受ける可能性のある本人、取引先、顧客等への連絡、③警察等の外部関係者への報告、④再発防止策の検討及び決定、⑤事実関係及び再発防止策等の公表