情報セキュリティ規則

制定　令和５年３月４日
最近改正　令和５年３月４日

第１章 総則

（目的）
第１条　この取扱規則は、勧永町内会（以下「本会」という。）が保有する情報資産に関して、適正な情報セキュリティ対策が実施されることを目的として定める。

（周知）
第２条　本会は、この取扱規則を、電磁的公示方法により会員に周知する。

（管理者）
第３条　本会における、情報資産の管理者は町内会会長とする。

（取扱者）
第４条　本会における、情報資産の取扱者は理事及び班長とする。

第２章 組織的セキュリティ対策

（点検）
第５条　各部担当者は、情報セキュリティ規則の実施状況について、９ 月に点検を行い、点検結果を理事会に報告する。理事会は報告に基づき、以下の点を考慮し、必要に応じて以下の各号に掲げる改善計画を立案する。

(一) 情報セキュリティ規則が有効に実施されていない場合は、原因の特定と改善
(二) 情報セキュリティ規則に定められたルールが、新たな脅威に対する対策として有効でない場合は、情報セキュリティ規則の改訂
(三) 情報セキュリティ規則に定められたルールが、関連法令や取引先の情報セキュリティに対する要求を満たしていない場合は、情報セキュリティ関連規則の改訂

（情報共有）
第６条　町内会会長は、新たな脅威及び脆弱性に関する警戒情報及び個人情報の保護に関する情報を専門機関等から適時に入手し、理事会で共有する。

(一) 独立行政法人情報処理推進機構（略称：IPA）
https://www.ipa.go.jp/

(二) JVN（Japan Vulnerability Notes）
https://jvn.jp/index.html
(三) 一般社団法人 JPCERT コーディネーションセンター（略称：JPCERT/CC）
https://www.jpcert.or.jp/
(四) 個人情報保護委員会
http://www.ppc.go.jp/
(五) 国民のためのサイバーセキュリティサイト（総務省）
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/index.html

第３章 情報システムの管理

（クライアント）

第７条　本会で使用されるデバイス（例：PC、スマートフォン等）は、情報セキュリティ対策が実施されていなければならない。

(2) デバイスは下記に掲げる各号を満たし、保たなければならない。
(一) パターンファイルが最新化され、マルウェア対策ソフトウェアの常駐化
(二) オペレーティングシステム、及びインストールされている全てのソフトウェアに対する最新パッチ適用
(三) ソフトウェアベンダーがサポートを終了したソフトウェアのアンインストール

(3) 本会がデバイスを理事・班長に貸与するときは、台帳管理を行わなければならない。

(4) 日本国政府又は米国政府が安全保障上の問題から調達を禁止している製品は、利用を許可しない。

（オンプレミス）

第８条　本会において、勧永町内会の保有並びに賃貸している施設の構内に機器を設置し、サーバーとして運用することは禁ずる。

(2) 施設管理に必要な情報収集を目的とした、一時的な情報収集を行う目的において使用される中継サーバーについては、情報セキュリティリスクアセスメントを実施することで設置することができる。

（クラウドサービス）

第９条　本会で使用されるクラウドサービスは、信頼できる監査機関によってクラウドサービス事業者、並びに導入しようとするサービスが、情報セキュリティ対策及び個人情報保護が実現されていることを認証されていなければならない。

(2) 認証規格は以下に掲げる各号のいずれかを満たさなければならない。
(一) 国際規格（ISO/IEC 27001、ISO/IEC 27017）による認証
(二) 米国公認会計士協会（SOC1-3、WebTrust）による認証
(三) 一般社団法人日本プライバシー認証機構（TRUSTe）による認証

(四) 米国連邦情報処理規格（FIPS 140-2, 3）による認証

(3) 個人情報及び経理情報等の機密情報を保存するクラウドサービスは、以下に掲げる各号を満たさなければならない。

(一) データ保存先は日本国内とする

(二) 準拠法を日本国法とする

(4) クラウドサービスの情報セキュリティ対策状況は、少なくとも毎年一回会確認を行わなければならない。

第４章 文書保存

（情報資産の管理）

第１０条　本会で使用される情報資産は原則として、指定されたファイル共有サービス上に原本を保存しなければならない。

（情報資産台帳）

第１１条　情報資産は台帳管理を行い、台帳には以下の各号を記載しなければならない。

(一) 情報資産の名称

(二) 保管場所

(三) 保存期限（年数、有効期間中、永年）

(四) 所管部門

(五) 媒体（データ、紙、その他）

(六) 公開レベル

(2) 前項に定める公開レベルは文書に記載を行う。

レベル	基準
公開（PUBLIC）	規約や広報誌といった、会員及び周辺地域に周知して良い情報
部外秘（INTERNAL）	立替経費精算書や会員名簿といった、町内会活動を行うにあたり必要であり、会員に限定されるべき情報
秘（CONFIDENTIAL）	総会委任状や入退会届といった、個人情報といった機微情報が記載される情報で、役員並びに担当者に限定されるべき情報
極秘(STRICTLY)	安否確認グループ別世帯人数表といった、経歴や病歴等が記載された機微情報で、役員並びに担当者に限定されるべき情報

（保管場所の安全対策）

第１２条 情報資産を活用に、情報メディア（CD、USB メモリ、外部 HDD 等）または紙を使用する場合は、以下に定める各号の対策を行う。

(一) 保管場所の施錠

(二) データの暗号化

(三) 情報資産の分割（単体では情報を解読できない保存方法）

（廃棄方法）

第１３条　保存期間を経過した文書は、該当年度終了時に担当部が町内会会長の承認を受けた後、シュレッダー（クロスカット細断）、破壊、溶解等により廃棄処分を行う。

第５章 アカウント管理

（登録）

第１４条　利用者の認証に用いるアカウントは、町内会会長の承認に基づき登録する。

（配付）

第１５条　情報資産を扱う情報システムは、以下の方針に基づいて利用者の認証を行う。

(一) 利用者の認証に用いるアカウントは、利用者１名につき１つを発行する

(二) 複数の利用者が共有するアカウントの発行を禁止する

（アクセス制御）

第１６条　情報資産を扱う情報システム、又はサービスに対するアクセス制御は以下の方針に基づいて運用する。

(一) 利用者の業務・職務に応じた必要最低限のアクセス権を付与する。

(二) 特定の情報資産へのアクセス権が、同一人物に集中することで発生し得る不正行為等を考慮し、複数名に分散してアクセス権を付与する。

(三) 付与されたアクセス権が不要になった場合は、アクセス権の削除、又は無効化を当該のアクセス権が不要になる日の翌日までに実施する。

（アカウントの管理）

第１７条　利用者の認証に用いるアカウントが不要になった場合、情報システム管理者は、当該アカウントの削除、又は無効化を当該アカウントが不要になる日の翌日までに実施する。

（パスワード）

第１８条　本会で使用されるデバイス、サービスにはパスワードが設定されなければならない。

(2) パスワードは以下に掲げる各号を満たさなければならない。

(一) 文字数は 10 文字以上とする

(二) 文字種は英数字記号の混合とする

(三) 有効期限は設定しない

(3) 多要素認証が使用できる場合は、これを原則として有効とする。

(4) パスワードリセット機能がセルフサービスで利用できる場合は、これを提供する。

(5) アカウント連携が利用できる場合は、これを原則として利用する。

(6) パスワード水準は NIST SP800-63B をベースラインとする。

第６章　その他

（附則）

この取扱規則は、令和５年３月４日から施行する。