情報セキュリティ規程

特定非営利活動法人

ＩＴＣちば経営応援隊

制定：2020 年 1 月 27 日　　第 1.0 版
改定：2021 年 10 月 1 日　　第 1.1 版

１．情報セキュリティ規程の目的

本規程は、当法人の事業活動を支える情報資産を適切に保護していくために、情報セキュリティ基本方針に基づき、組織的、人的、物理的、及び技術的安全管理措置の内容を定め、当法人の会員並びに会員の管理下で共に事業活動に係わる者に、その遵守を求めることにある。

２．本規程の対象範囲

本規程を適用する情報資産並びに情報システム資源の範囲を以下に定める。

（１）当法人の事業運営に係わる、すべての情報資産（紙データ、電子データを問わず、また受託先などから預かった情報を含む）。

（２）当法人の活動で使用されるすべての情報システム資源（ハードウェア、ソフトウェア、ネットワーク、クラウドサービス、記録媒体などで、会員個人が保有又は使用するものを含む）

3. 組織的対策

3.-1 情報セキュリティに関する組織体制

情報セキュリティの維持・改善を図るために、当法人の組織体制に合わせて、各自が以下の役割と責任を果たすものとする。

当法人の組織体制	情報セキュリティ管理体制
理事長	情報セキュリティ責任者
理事会	情報セキュリティ委員会
事務局	情報セキュリティ委員会事務局
各理事	情報セキュリティ管理者
監事	内部監査担当
会員	情報セキュリティ担当者

【情報セキュリティ責任者】

当法人の理事長が務め、必要な対策について情報セキュリティ委員会に諮り、その実施を通じて情報セキュリティの確保の責任を果たす。

【情報セキュリティ委員会】

当法人の理事並びに監事で構成され、情報セキュリティの確保に必要な対策を協議・決定し、法人内への周知・徹底を図ると共に、実施状況を継続的に把握・改善する。

【情報セキュリティ委員会事務局】

理事会の事務局が担当し、委員会の運営と各種調整を図ると共に、外部からの問い合わせ窓口となる。

【情報セキュリティ管理者】

当法人の理事が務め、各自が担当する役割において、情報セキュリティの確保に必要な対策を実施し、その運営状況を管理する。

【情報セキュリティ担当者】

会員それぞれが情報セキュリティ担当者となり、各自が使用・保有する情報システム資源や使用環境に対して、当法人の事業活動に必要な情報セキュリティを確保し、情報資産保護の責任を負う。

【内部監査担当】

本規程の遵守状況を確認し、必要に応じて監査を実施する。

3.-2 外部への委託について

当法人の事業活動の一部を、外部へ委託する場合は、委託先の情報セキュリティ対策が当法人の要求を満たしているか定期的に確認する。

4. 情報資産の分類と管理方法

当規程で特に保護の対象として管理を徹底する情報資産は、以下に分類される秘密情報と極秘情報とする。また、情報の分類は個々の活動に携わる情報セキュリティ担当者（当法人会員）の判断に委ねる。

尚、ホームページ等の公開情報においても、情報の完全性が損なわれた場合、当法人の信用失墜や被害に発展する可能性に留意し、情報の取り扱いには細心の注意を払う。

（１）秘密情報：当法人内の運営において、閲覧や取り扱い者を限定する情報。機密性や完全性が損なわれると当法人及び当法人会員に被害を与える可能性がある情報で、付表１にて管理する。

個々の秘密情報の管理責任者は、ファイル名等にその旨を表示し、パスワード設定などのアクセス制限や、情報の保管・バックアップ・廃棄などの管理を適切に行う。

（２）極秘情報：秘密情報の中でも、特に事業案件において契約先などから取り扱いについて特別の指示や要請を受けた重要情報で、情報へのアクセスを事業案件の担当者など特定の者に限定する。

極秘情報は、秘密情報と同等の管理を行うことに加えて、案件取り組み時に提出する「プロジェクト理事会申請書」に、該当する情報と具体的な管理方法を記入し、理事会の了承を得る。

５．物理的対策

情報セキュリティ担当者（会員）は、自宅や外出先（移動時を含む）などの作業場所において、自らが使用する PC や記録媒体などの情報機器が盗難などに遭わないよう注意を払う。また収納時は、施錠管理など必要な対策を取る。

6．人的対策

情報セキュリティ委員会は、情報処理推進機構(以下 IPA と表記）の「情報セキュリティ自社診断」をベースとした当法人独自のチェックリストを作成し、情報セキュリティ担当者（会員）に対して自己点検の実施を求める。

また月次連絡会の場やメール送信により、セキュリティマインドの醸成に役立つ情報や最新の脅威情報などを提供すると共に、SECURITY ACTION 自己宣言など、会員の情報セキュリティ対策への積極的な取り組みを促す。

7．技術的対策

当法人は独自に開発・運用する情報システムを保有していないことから、本規程では外部サービスや、パソコン用ソフト等を使用している会員個人の情報システム資源に絞り、当法人の事業活動において以下の点を遵守する。

7.-1 外部サービスやパソコン用ソフトウェア

クラウドサービス等の外部サービスを導入する場合は、情報セキュリティ委員会にてサービスプロバイダの情報セキュリティ対策をあらかじめ評価したうえで選定する。尚、評価に当たっては、IPA の評価基準などを参考にする。

また、業務運用に必要なソフトウェアの導入についても、同様の対応を行う。

7.-2 会員個人の情報システム資源

会員は個人が所有する情報システム資源(ハードウェア、ソフトウェア、ネットワーク、記録媒体など) に対して、前述のチェックリストを用いて、最低年 1 回自己点検を行う。また秘密情報、極秘情報を取り扱う会員は、チェックリストの中で必須とされた項目すべてについて、必ず対策を実施する。

特に事業案件を担当する会員は、案件開始までに改めて自己点検を行い、IPA の「中小企業の情報セキュリティ対策ガイドライン」などの資料を参考に、アクセス管理やウイルス対策の視点から、情報漏えいに対し十分な技術的対策を取る。

尚、極秘情報は、個人や当法人の共有ディスク(OneDrive 等)環境には保管せず、事業案件の担当リーダーが責任を持って保管する。

8．事件・事故発生時の対応

秘密情報や極秘情報の漏えいなど、事件・事故の発生に気付いた会員は（またはその恐れがある場合を含む)、速やかに情報セキュリティ責任者に報告する。

情報セキュリティ責任者は事態の影響を把握するため、関係する情報セキュリティ管理者に発生からの経緯と現状の確認を指示すると共に、速やかに情報セキュリティ委員会を開催し、緊急対策の決定と事態の対応に当たる。

9．運用

9.-1 本規程の改定

本規程は、理事会での検討・承認をもって改定するものとする。

9.-2 付表について

本規程の運用に用いる一覧表などを付表として定める。尚。付表の記載事項に変更がある場合は、本規定の改定と同様、理事会において承認する。

付表 1：当法人の秘密情報の管理責任者一覧表

秘密情報に該当する情報資産	管理責任者（各情報セキュリティ担当者）
入会申込書、会員名簿(個人情報/口座情報)	理事（事務局）
特定個人情報（マイナンバー）	理事（会計担当）
会費請求/入金情報/銀行口座情報	理事（会計担当）
会計関連情報	理事（会計担当）
プロジェクト理事会申請書	理事（事務局）、案件担当リーダー
プロジェクト関連情報	案件担当リーダー