情報セキュリティ規程 第2.0版

はじめに

むすびえはプロジェクト制の元に事業を運営し、プロジェクトやその他組織に関わる情報は全員で共有し、参照できることを前提に事業を進めています。
ただし、扱っている情報の中には、寄付者・支援企業・地域ネットワーク団体・こども食堂など多様なステークホルダーについての個人情報や機密情報も存在し、それらの情報を守ることは、むすびえという組織を守るだけでなく、むすびえと一緒に活動を推進してくれている大切なステークホルダーの皆さんの情報を守ることでもあります。

今回組織が管理している情報資産を守るために、また情報セキュリティに影響を及ぼす事案が発生した場合に備えて、むすびえメンバー全員が守るべきセキュリティ規程を定めました。むすびえの多様な働き方、プロジェクト制での事業運営という点を考慮して、実際の業務を滞らせないことも重要だという観点から、セキュリティ規程としては、最低限これだけは守らなくてはいけない、という項目だけに絞ったものとなっています。

むすびえメンバー一人一人が、このセキュリティ規程を意識し、行動することで、業務を遂行する際に自信を持って情報を管理することができ、結果として、むすびえという組織や関係者を守ることになり、ビジョンの実現につながります。

むすびえの大切な情報資産をみんなでしっかりと守っていきましょう！

なお、この規程は情報セキュリティ対策を推進する上での最上位のルールとなるものであり、具体的なガイドラインやルールについては別途定めます。実際の業務を遂行する上では、各種ガイドラインやルールも確認、順守いただくようお願いします。

1. 組織的対策

1.1. 情報セキュリティのための組織
情報セキュリティ対策を推進するための組織として、ICTチーム内に情報セキュリティ対策室を設置する。情報セキュリティ対策室は、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者。理事長が担う。情報セキュリティ対策などの決定権限を有すると共に、全責任を追う。
情報セキュリティ管理責任者	情報セキュリティの管理責任者。ICTチームリーダーが担う。情報セキュリティ対策の実施や確認、むすびえメンバーへの教育を行う。事故対応については内部ルールに従う。

1.2. 情報セキュリティ取組みの点検
情報セキュリティ管理責任者は、本セキュリティ規程に沿って作成された「別紙：情報セキュリティ状況チェックリスト」を用いて、年1回点検を行い、点検結果を情報セキュリティ対策室に報告する。情報セキュリティ対策室は、報告に基づき、必要に応じて改善計画を立案する。

1.3. 情報セキュリティに関する情報共有

情報セキュリティ管理責任者は、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、情報セキュリティ対策室で共有する。

2. 人的対策

2.1. 契約時

むすびえメンバー（役員・職員・個別の契約関係にあるもの（業務準委任、業務委託、プロボノ、出向等））と業務契約する際には、この情報セキュリティ規程を遵守することを定めた秘密保持条項を含んだ契約を締結する。

2.2. 契約終了時

- 秘密保持契約、休職・退職時の誓約書及び、3.2.3.2、3.2.5.2、3.2.6.3、3.2.7.2の各規定に従い情報の返還、廃棄その他必要な措置を実施する
- 3.2.4.3 を実施する

2.3. 情報セキュリティ教育

情報セキュリティ管理責任者は、情報セキュリティに関する「別紙：情報セキュリティ教育チェックリスト」を年度単位で見直し、教育を実施する。

- 対象者： むすびえメンバー（役員・職員・個別の契約関係にあるもの（業務準委任、業務委託、プロボノ、出向等））で、むすびえアカウントを持つ、D3以上の情報にアクセスできる人
- 内容：情報セキュリティ教育チェックリスト参照
- 実施時期：年1回

3. 情報資産の管理

3.1. 情報資産一覧の管理

情報資産一覧を作成する。作成した一覧を定期的に見直し、更新する。
実施期間：年1回

3.2. 情報資産の取り扱いについて

3.2.1. 情報資産区分

- D1：重要情報（機密情報、個人情報等）
- D2：部門・プロジェクト限定で共有する情報
- D3：むすびえ全体で共有する情報
- D4：外部関係者に共有する情報

3.2.2. 重要情報（D1)

重要情報は原則PJL以上が管理する。PJL以外で取り扱えるメンバーは、情報セキュリティ対策室が別途定める。重要情報資産を業務上取り扱う場合は、以下を実施する。

3.2.2.1. 紙媒体

別途定めたむすびえメンバーのみ閲覧できる。

3.2.2.2. 重要情報を保管するサービス（情報資産一覧内に記載）

別途定めたむすびえメンバーのみアクセスできる。

3.2.2.3. その他

上記以外で、重要情報の取り扱いは認めない。

3.2.3. 紙媒体

紙媒体を取り扱う場合は、以下を実施する。

3.2.3.1. 取り扱いについて

- 公共の場所での作業時、紙の業務書類を出す作業は原則禁止すること。個人情報など秘匿性の特に高い情報については公共の場所では利用しないこと。
- 業務に関係する印刷物を、他者も集まる公共のカフェやコワーキングスペース、公園、各種スペースなどで利用する必要がある場合は、その扱いに十分留意し、情報の秘匿性を守ること。

3.2.3.2. 削除・廃棄等について

情報資産一覧の廃棄方法に従って、廃棄もしくは返還すること。

3.2.4. 各デバイス

各デバイスを取り扱う場合は、以下を実施する。

3.2.4.1. 取り扱いについて

- 全てのデバイスは一定時間で認証が必要なロックがかかるようにすること。
- デバイス内のデータは暗号化を施して保存すること。
- 業務の情報が通知で出る際はその内容までは表示されない設定にすること。
- 離席時はあらゆる場所において必ずデバイスのロックをかけること。
- 業務に使用する各デバイスは、個人利用にとどめ、他者との共同利用を禁止とする。
- USB、外部接続HDDは可能な限り禁止とする。利用する場合は、登録制かつ自動暗号化機能付きであることとし、情報の共有はクラウドのみとする。

3.2.4.2. OSについて

- OSは常に最新へアップデートする。
- 公式のサポート切れOSの使用禁止。
- サポート切れOSのPCを止むを得ず使用する場合は指定のセキュリティソフトの導入を必須とする。

3.2.4.3. 削除・廃棄等について

秘密保持契約書に従って処分する。

3.2.5. Google Workspace

Google Workspaceを取り扱う場合は、以下を実施する。

3.2.5.1. 取り扱いについて

- アカウント登録は、情報セキュリティ管理責任者が承認し、情報セキュリティ責任者は随時確認すること。
- むすびえメンバーでのプロジェクト単位でのアクセス制限は実施しない。
- 外部と情報を共有する場合は、情報セキュリティ管理責任者の監督の元、情報資産区分に準ずるフォルダ内で、アクセス用のフォルダを別途作成する。

3.2.5.2. 削除・廃棄等について

退職（契約終了含む）、休職が終了した時点で、情報セキュリティ管理責任者は、当該アカウントの削除又は無効化を実施する。

3.2.6. ネットサービス

ネットサービスを取り扱う場合は、以下を実施する。

3.2.6.1. 取り扱いについて

- 個人での契約を禁止とし、情報セキュリティ対策室の確認を経て、むすびえにて購入する。
- 二段階認証の設定を必須とすること
- それぞれのネットサービス間での、パスワード共有及び一定のルールに基づくパスワード設定は禁止。特に、個人で利用しているサービスと共通のパスワードは業務では使用しないこと。
- 情報セキュリティ対策室が定めたパスワードマネージャでログイン情報を管理すること。

3.2.6.2. AIについて

AIツールは個人情報・機密情報の掲載を禁止する。

3.2.6.3. 削除・廃棄等について

退職（契約終了含む）、休職が終了した時点で、情報セキュリティ管理責任者は、当該アカウントの削除又は無効化を実施する。

3.2.7. コミュニケーションツール

コミュニケーションツールを取り扱う場合は、以下を実施する。

3.2.7.1. 取り扱いについて

情報セキュリティ対策室で、使用すると決めたコミュニケーションツール以外は使用しない。

3.2.7.2. 削除・廃棄等について

退職（契約終了含む）、休職が終了した時点で、情報セキュリティ管理責任者は、当該アカウントの削除又は無効化を実施する。

3.2.8. リモートワーク

リモートワークにより情報資産を取り扱う場合は、以下を実施する。

3.2.8.1. 取り扱いについて

- 公共の場所でのオンラインミーティングにおいては業務情報の口頭漏洩を十分に注意すること。
- 公共の場所での作業時、第三者からの画面の盗み見などに十分に注意すること。
- ネットワーク網については、原則、自宅WiFi（有線含む）と各自のスマホ等によるテザリングを推奨（ポケットWi-Fi含む）。外部の施設Wi-Fiを使う場合は、使用するネットワーク名が確実に施設公式のものであるかを十分に確認すること。

4. 情報セキュリティインシデント対応ならびに事業継続管理

別途定めたリスクマネジメント体制のフローに従って対応する。

4.1. 対応体制

情報セキュリティインシデントが発生した場合には、以下の体制で対応する。

最高責任者	情報セキュリティ責任者
対応責任者	各ディレクターと、情報セキュリティ管理責任者
一次対応者	発見者又はプロジェクトリーダー

4.2. 情報セキュリティインシデントの影響範囲と対応者
情報セキュリティインシデントが発生した場合、以下を参考に影響範囲を判断して対応する。

事故レベル	影響範囲	責任者
3	● 顧客、取引先、などに影響が及ぶ時 ● 個人情報が漏洩した時	各ディレクターと情報セキュリティ責任者
2	事業に影響が及ぶ時	各ディレクターと情報セキュリティ責任者
1	むすびえメンバーの業務遂行に影響が及ぶ時	各ディレクターと情報セキュリティ管理責任者
0	インシデントにまでは至らないが、将来においてインシデントが発生する可能性がある事象が発見された時	プロジェクトリーダーと情報セキュリティ管理責任者

4.3. インシデントの連絡及び報告
レベル1以上のインシデントが発生した場合、発見者は各ディレクターと情報セキュリティ管理責任者に速やかに報告し、指示を仰ぐ。

附則

- この規程は、2022年12月26日から施行される。
- この改定規程は、2026年2月1日から施行される。(2026年1月23日理事会決議)