【社内通知】

情報セキュリティ基本方針

制定日	2026 年 4 月 1 日
版　数	Ver.1.0（初版）
発令者	代表　　榊　茂昌
適用範囲	全従業員・役員（パート・アルバイト・派遣社員・業務委託を含む）

1. 趣旨・目的

業務上取り扱う情報資産を適切に保護することを経営上の重要課題と位置付け、情報セキュリティの確保に組織全体で取り組みます。

本方針は、IPA（情報処理推進機構）が策定した「中小企業の情報セキュリティ対策ガイドライン」に基づく自社診断（25 項目）の結果を踏まえ、全従業員が遵守すべき情報セキュリティ対策をルール化し、周知・徹底するために制定します。

2. 情報セキュリティ基本方針

当社は、以下の基本方針に従って情報セキュリティ対策を推進します。

- 情報資産を脅威（ウイルス感染、不正アクセス、情報漏えい、盗難・紛失等）から守り、事業継続を確保する。
- 情報セキュリティに関する法令・規制・契約上の要求事項を遵守する。
- 従業員に対して定期的な教育・訓練を実施し、セキュリティ意識の向上を図る。
- 情報セキュリティ事故の発生に備え、対応手順を整備し、迅速な復旧・再発防止に努める。
- 本方針は定期的に見直しを行い、常に適切な状態を維持する。
-

3. 情報セキュリティ対策ルール一覧（No.1〜25）

以下の 25 項目は、全従業員が日常業務において遵守すべき情報セキュリティ対策です。
自社診断シートの各項目に対応しています。

■ Part 1：基本的対策（No.1〜5）

No.	対策項目	概要・遵守事項
1	**OS・ソフトウェアの最新化**	OS およびソフトウェアは常に最新の状態に保つこと。修正プログラムを速やかに適用する。
2	**ウイルス対策ソフトの導入**	全端末にウイルス対策ソフトを導入し、定義ファイルを常に最新の状態に維持する。
3	**強固なパスワードの使用**	パスワードは 10 文字以上、複雑なものを設定し、使

No.	対策項目	概要・遵守事項
		い回しを禁止する。多要素認証を活用する。
4	**重要情報のアクセス制限**	重要情報へのアクセスは業務上必要な担当者のみに限定し、適切なアクセス権限を設定する。
5	**脅威・攻撃手口の情報収集**	IPA などのセキュリティ機関の情報を定期的に収集し、社内で共有・周知する。

■ Part 2：従業員としての対策（No.6〜18）

No.	対策項目	概要・遵守事項
6	**不審メールへの対応**	身に覚えのない電子メールの添付ファイルを開いたり、URL リンクをクリックしないこと。
7	**メール・FAX 誤送信防止**	電子メール・FAX 送信前に宛先を再確認すること。複数宛先の場合は BCC を活用する。
8	**重要情報の送信時の保護**	重要情報はファイルにまとめパスワード保護の上、メール添付する。パスワードは別手段で通知。
9	**無線 LAN の安全利用**	WPA2/WPA3 等の強固な暗号化方式を設定し、フリーWi-Fi 使用時はファイル共有をオフにする。
10	**インターネット利用ルール**	業務でのインターネット利用に関する注意事項を遵守し、SNS への秘密情報投稿を禁止する。
11	**バックアップの励行**	重要データは定期的にバックアップし、媒体はパソコンと切り離して安全に保管する。
12	**重要情報の安全保管**	重要書類・電子媒体は鍵付き書庫に保管し、机上への放置を禁止する。
13	**重要情報の持ち出し管理**	持ち出しは許可制とし、端末にはパスワードロックおよびデータ暗号化を実施する。
14	**離席時の PC 操作防止**	離席時はスクリーンロックを実施する。のぞき見防止フィルタを公共の場で使用する。
15	**事務所への立ち入り制限**	関係者以外の事務所立ち入りを制限し、重要情報保管場所への無断立入を禁止する。
16	**退社時の機器施錠保管**	退社時はノート PC や外付け記憶媒体等を施錠可能な場所に保管する。
17	**事務所の施錠管理**	最終退出者は施錠を確認し、退出記録を残す。施錠チェックリストを活用する。
18	**重要情報の安全な廃棄**	書類はシュレッダー処理、電子媒体は消去ソフトまたは物理破壊により復元不能にする。

■ Part 3：組織としての対策（No.19〜25）

No.	対策項目	概要・遵守事項
19	**守秘義務の周知**	従業員に守秘義務を説明し、秘密管理している情報を明確に示す。覚書を締結する。
20	**従業員へのセキュリティ教育**	定期的な情報セキュリティ研修を実施し、テレワーク時の対策についても教育する。
21	**私物端末の業務利用ルール**	個人所有端末の業務利用可否を決定し、許可する場合

No.	対策項目	概要・遵守事項
		はセキュリティルールを定める。
22	**取引先への秘密保持要請**	重要情報授受を伴う取引先との契約に秘密保持条項を設け、対策実施状況を確認する。
23	**外部サービスの選定基準**	クラウド等の外部サービスは信頼性・セキュリティ対策・補償内容を確認して選定する。
24	**セキュリティ事故への備え**	情報漏えい・盗難・ウイルス感染等の事故発生時の対応手順書を作成し、従業員に周知する。
25	**情報セキュリティ対策のルール化**	本方針（No.1〜24）を明文化し、従業員全員がいつでも参照できるよう周知・管理する。

4. 責任体制

経営者（代表取締役）	情報セキュリティ対策全体の最高責任者。本方針の承認・改定を行う。
情報セキュリティ担当者	日常的な情報セキュリティ対策の実施・管理・従業員への周知を担当する。 担当者：　　（氏名を入力）
全従業員	本方針・各ルールを理解し、日常業務において遵守する。

5. 本方針への違反

本方針に違反した場合、就業規則に基づく懲戒処分の対象となることがあります。また、違反行為によって会社または第三者に損害が生じた場合、民事・刑事上の責任を問われる場合があります。

6. 本方針の見直し・改定

本方針は年 1 回以上定期的に見直しを行います。また、法令の改正、新たな脅威の発生、業務環境の変化等があった場合には、随時改定します。改定の際は全従業員に速やかに周知します。

7. 関連資料・参考情報

- IPA「中小企業の情報セキュリティ対策ガイドライン」
  https://www.ipa.go.jp/security/guide/sme/about.html
- IPA「5 分でできる！情報セキュリティ自社診断」（本方針の基礎）
- IPA「情報セキュリティハンドブック（ひな形）」（従業員配付用）
- SECURITY ACTION（情報セキュリティ自己宣言制度）
  https://www.ipa.go.jp/security/security-action/