情報セキュリティポリシー

株式会社ビシィッ

制定日：2026 年 5 月 10 日

---

1. 基本方針

株式会社ビシィッ（以下「当社」といいます。）は、自社の業務・サービス運営において、発注企業・受託者・その他関係者から預かる情報資産を適切に保護することを経営上の重要課題として位置づけます。

当社は、情報の機密性（Confidentiality）・完全性（Integrity）・可用性（Availability）を確保するため、本情報セキュリティポリシー（以下「本ポリシー」といいます。）を定め、全役職員（正社員・契約社員・パートタイマー・業務委託者・派遣労働者を含む。以下「従業者」といいます。）および関係者がこれを遵守します。

2. 適用範囲

本ポリシーは、以下に適用されます。

- 当社のすべての従業者
- 当社が業務を委託・再委託する外部委託先・パートナー
- 当社が管理・利用するすべての情報資産（電子データ・紙媒体・システム・ネットワーク等）

3. 情報資産の管理

3.1 情報資産の分類

当社は、保有する情報資産を以下のとおり分類し、それぞれの重要度に応じた管理を行います。

- 【極秘】：漏えいした場合に当社または顧客・取引先に重大な損害を与える情報（個人情報・営業機密・契約情報・支払情報等）
- 【社外秘】：社内のみで共有される情報（内部報告書・未公開情報等）

- 【社内公開】：社内全体で共有される情報（社内規程・マニュアル等）
- 【公開】：ウェブサイト等で一般に公開される情報

3.2 アクセス管理

- 情報へのアクセス権限は、業務上の必要性に応じて最小限の範囲で付与します（最小権限の原則）。
- 従業者のアクセス権限は、入退社・異動の際に速やかに見直します。
- 特権アカウント（管理者権限等）は厳格に管理し、利用状況を記録します。
- 外部からのリモートアクセスには多要素認証を適用します。

3.3 パスワード管理

- パスワードは 12 文字以上とし、英字・数字・記号を組み合わせたものを使用します。
- パスワードを他者と共有すること、メモ等に平文で記載することを禁止します。
- システムへのログインには、原則として個人に割り当てられたアカウントを使用します。

4. 物理的セキュリティ

- サーバー室・機密情報を扱うエリアへの入退室を管理し、不審者の立入りを防止します。
- 業務上使用する PC・スマートフォン等のデバイスは、紛失・盗難防止のため適切に管理します。
- 机・棚等の書類は業務終了後に施錠管理します（クリアデスクポリシー）。
- 不要になった書類・記録媒体は、復元が不可能な方法（シュレッダー等）で廃棄します。

5. 技術的セキュリティ

5.1 システム・ネットワークの保護

- ファイアウォール・侵入検知システム（IDS/IPS）を導入し、不正アクセスを防止します。
- 通信は原則として SSL/TLS 等の暗号化プロトコルを使用します。

- OS およびソフトウェアは、セキュリティパッチを速やかに適用します。
- マルウェア対策ソフトウェアを導入し、常時最新の状態に更新します。

5.2 データの保護

- 機密性の高いデータは暗号化して保管します。
- 重要データのバックアップを定期的に取得し、復旧手順を整備・確認します。
- クラウドサービスの利用は、当社が認定したサービスに限定します。

5.3 開発・テスト環境

- 本番データをテスト・開発環境で使用することを原則禁止します。
- やむを得ず使用する場合は、適切な匿名化・マスキング処理を施します。

6. 人的セキュリティ

- 採用時・業務委託契約締結時に、情報セキュリティに関する誓約書の提出を求めます。
- 従業者に対して定期的な情報セキュリティ教育・訓練を実施します。
- フィッシング詐欺・ソーシャルエンジニアリングへの対応訓練を実施します。
- 退職・契約終了時には、貸与機器の返却・アクセス権限の即時失効・秘密保持義務の継続を確認します。

7. 外部委託・再委託のセキュリティ管理

当社のビジネスモデルは業務委託および再委託を含むため、委託先のセキュリティ管理に特に注意を払います。

- 外部委託先・再委託先の選定にあたり、情報セキュリティ体制を評価します。
- 委託契約・再委託契約には、情報セキュリティに関する条項（守秘義務・安全管理義務・監査権等）を必ず含めます。
- 委託先・再委託先による情報の目的外利用・第三者提供を禁止します。
- 委託先・再委託先のセキュリティ対応状況を定期的に確認・監査します。
- 委託先・再委託先において情報漏えい等の事案が発生した場合、速やかに当社への報告を義務付けます。

8. インシデント対応

8.1 報告体制

従業者は、情報セキュリティインシデント（情報漏えい・不正アクセス・ウイルス感染・機器の紛失・盗難等）を発見または疑いが生じた場合、直ちに情報セキュリティ管理者に報告します。

8.2 対応手順

1. インシデントの検知・報告
2. 被害範囲の特定と封じ込め（感染・流出の拡大防止）
3. 原因調査・証拠保全
4. 関係者・監督官庁・被害者への通知（要件に該当する場合）
5. 再発防止策の策定・実施
6. 事後検証・ポリシー改訂

8.3 個人情報漏えい等の報告

個人情報の漏えい等が発生した場合、個人情報保護法の規定に従い、個人情報保護委員会への報告および本人への通知を行います。

9. 法令・規制遵守

- 個人情報の保護に関する法律（個人情報保護法）
- 特定受託事業者に係る取引の適正化等に関する法律（フリーランス新法）
- 不正アクセス行為の禁止等に関する法律
- 電子署名及び認証業務に関する法律
- その他情報セキュリティに関連する法令・ガイドライン

10. 監査・見直し

- 本ポリシーの運用状況について、年 1 回以上の内部監査を実施します。
- 外部専門機関によるセキュリティ診断・ペネトレーションテストを定期的に実施します。

- 法令改正・事業環境の変化・インシデントの発生等を踏まえ、必要に応じて本ポリシーを見直します。

11. 違反への対応

本ポリシーに違反した従業者・委託先に対しては、就業規則・委託契約書の規定に基づき、懲戒処分・契約解除・損害賠償請求等の措置を講じます。また、違反行為が法令に違反する場合は、関係機関への通報を含む適切な対応を行います。

12. 体制

当社は、情報セキュリティ管理者を設置し、本ポリシーの運用・教育・監査・改訂を一元管理します。情報セキュリティに関する最終責任は代表取締役が負います。

本ポリシーは 2026 年 5 月 10 日に制定されました。改訂時は版数・日付を更新して再公表します。