

三口産業株式会社 セキュリティ規程

(P C ・携帯電話・スマホ等モバイル端末・通信運用 版)

第 1 章 総則

第 1 条 (目的)

本規程は、当社が保有・管理保有する情報資産を、漏洩、改ざん、紛失、破壊、不正利用及び、サイバー攻撃等の脅威から保護し、業務に使用するパソコン、携帯電話、タブレット等を運用すると共に、適切な情報セキュリティ体制を維持・運用することを目的とする。

第 2 条 (適用範囲)

1. 本規程は、役員、社員、契約社員、派遣社員等、当社の業務に従事する全ての者に適用する。
2. 当社の情報資産を取り扱う外部委託先に対しても、本規程と同等のセキュリティ水準の遵守を求めるものとする。

第 2 章 組織・体制とルール整備 (組織としての対策)

第 3 条 (管理体制)

1. 当社は、情報セキュリティ対策を全社的に推進する為、情報セキュリティ管理者を 1 名配置する。
2. 管理者は、本規程の周知徹底、安全対策の実施状況の把握、評価、及び定期的な見直しを行う。

第 4 条 (基本方針とルールの周知)

管理者は、情報セキュリティ基本方針を定め、全従業員等に周知徹底しなければならない。

第 5 条 (教育と啓発)

管理者は、従業員等に対し、情報セキュリティに関する教育や啓発を定期的を実施し、セキュリティ意識の維持・向上を図らなければならない。

第6条（委託先の管理）

1. 業務を外部に委託する場合は、委託先の情報セキュリティ対策状況を確認し、秘密保持やセキュリティ要求事項を盛り込んだ契約を締結しなければならない。
2. 管理者は、委託先の対策遵守状況を定期的に確認する。
3. クラウドサービスやウェブサイト等の外部サービスを利用する際は、サービス規約やS L A（サービスレベル合意書）等からその情報セキュリティ対応能力が適切であることを評価しなければならない。
また、利用中の外部サービスについては、定期的に安全・信頼性を評価すること。

第7条（禁止行為）

以下の行為を行うことを禁止する。

- 機密情報・顧客情報の無断持出や、その内容をS N S投稿すること。
- 許可されていない不正アプリ・クラウドサービスの使用。
- 端末管理ソフトの削除・改変及び停止処置。
- モバイル端末での無断録音・撮影・転送・データ持ち出し。

第8条（処分）

故意または重大な過失により情報漏えい・不正利用・不正通信が発生した場合に於いて、会社に対し損益又は社会的信用低下を招いた場合は、懲戒処分の対象とする。

第9条（教育・啓発）

全社員に対し、年1回以上の研修を実施し、P C・モバイル端末・S N S利用に対するルール及びリスクも含め、周知徹底する。

第3章 情報資産とIT環境の管理（技術的対策）

第10条（情報資産の見える化）

ハードウェアやネットワーク、ソフトウェア、クラウドサービス、データ、アカウント等、機密保護や事業継続等の面から重要と考えられる情報資産については、台帳や図面等により、見える化をしておくこと。

第 1 1 条（会社貸与機器）

1. 会社貸与のデスクトップP C・ノートP C・スマートフォン・携帯電話は、業務目的に限り、使用する事が出来る。
2. 私的利用、第三者への貸与・譲渡、無断持出は一切禁止する。
3. 紛失・盗難・ウイルス感染・不正アクセス等が発生した場合は、直ちに所属長及び、総務課へ報告する。

第 1 2 条（端末設定及び監視）

1. セキュリティ設定（ウイルス対策ソフト、ファイアウォール等）を無効化・削除してはならない。又、対策定義ファイルは常に最新に保つこと。
2. 営業職及び在宅勤務を希望する者の会社貸与のノートP Cには、アクセス管理ソフトを必ずインストールし、操作ログを記録を行い業務履行・不正利用の監視を実施する。
3. 業務上及び会社指定又は承諾得た以外のアプリケーションソフトウェア・クラウドツール（ストレージを含む）の使用は、全て禁止とする。

第 1 3 条（会社貸与のモバイル端末の取扱い）

1. 会社貸与のモバイル端末（スマートフォン等）は、業務連絡及び業務関連アプリの利用に限定する。
2. 会社で認められている以外のアプリのインストール・SNSや個人メールの使用は禁止する。
3. 紛失・盗難時は、直ちに総務課へ連絡を行い、当該端末機器の使用停止処置を依頼すること。
4. 各機器にはロック機能を用い、ロック解除パスコード・生体認証の設定を義務付ける。
5. オペレーションシステム・アプリケーションのアップデートは定期的を実施すること。

第 1 4 条（私有モバイル端末の取扱い）

1. 原則として、私物であるモバイル端末（スマートフォン・タブレット・ノートP C）を業務に利用してはならない。
2. 会社に事前に申請を行い例外的に許可された場合、以下の条件を順守すること。
 - モバイルデバイス管理登録を行い、社有端末に相当するセキュリティポリシーを適用する。
 - 業務データは、会社指定アプリケーションのみでの取扱とする。
 - 私用アプリへのデータ転送及びスクリーンショットは一切禁止とする。
3. 離職時またはモバイル端末の変更時には、端末内にある会社データを全て削除する。

第 1 5 条（携帯電話のコンプライアンス）

1. 社有端末やアプリケーション上での顧客情報・社内情報の持ち出し及び、共有は禁止する。

2. 商談・会議・相手先での録音・撮影は、相手方の同意を得た場合のみ可能とする。
3. 通話・メール等の記録は、業務上必要な範囲に限定する。
4. 不適切な発言・誹謗中傷・機密漏えい行為が確認された場合は、懲戒処分の対象とする。

第16条（外部記録媒体（USBメモリ等）利用の原則禁止と特例）

1. USBメモリ・外付HDD（SSDを含む）等の外部記録媒体は使用禁止とする。
2. 外部との双方でのデータの交換が必要な場合には、会社指定のクラウドストレージを用い、ダウンロードに当たってはパスワードを設定し、外部に漏洩しない様に行うこと。

第17条（ネットワーク・通信の安全確保）

1. 業務で利用する無線LAN（Wi-Fi）は、暗号化方式（WPA3/WPA2等）を設定し、安全に運用しなければならない。公共のフリーWi-Fi等の安全性が確認できないネットワークでの業務通信を禁止する。
2. 外部ネットワークからの不正侵入を防止するため、ファイアウォール等のネットワーク境界対策を適切に設定・運用する。

第18条（ウェブサイトの安全運用）

当社が運用するウェブサイトや公開サーバーは、脆弱性対策、SSL/TLSによる通信暗号化、及び、改ざん防止対策を講じ、安全に管理しなければならない。

第19条（データ送信ルール）

1. 大容量データの送付はギガファイル便（<https://gigafile.nu>）を使用すること。
 - － ファイルはパスワード付ZIPで、圧縮を行うこと。
 - － パスワードは、ダウンロードリンク記載のメールと別送すること（メール・電話等）
 - － ダウンロード有効期限は7日以内とすること。
2. 無料の外部クラウドストレージ（Google Drive、Dropbox等）への使用・アップロードは禁止。
3. 機密性の高いファイルは、会社指定クラウドストレージ（お任せストレージ）を使用すること。

第20条（マルウェア・ランサムウェア対策）

1. 脆弱性を回避する為に、常に最新のOS・セキュリティパッチを適用すること。
2. 不明なUSBメモリ・メールでのリンク・添付ファイルを開かないこと。
3. 必要と思われるデータは定期的に社内共有サーバーにバックアップを取ること。
4. 感染が疑われる場合は、ネットワークを遮断し、速やかに総務課へ報告すること。

第21（OS・ソフトウェアの更新）

1. 従業員等は、利用するパソコンやスマートフォン等の機器において、OSおよびソフトウェアを常に最新の状態に保ち、脆弱性を解消しなければならない。
2. 「JVN i P e d i a 脆弱性対策情報データベース」などを利用して当社が導入している情報資産に関連する脅威、ぜい弱性及びその対策方法について情報収集し、必要に応じて対策を講じること。

第三者に推測されにくい複雑な文字列（十分な桁数・英数記号の組み合わせ）とし、使い回しをしてはならない。

- パスワード設定は3ワード以内とし、記憶できないパスワードの設定は行わない様にする。
- **可能な場合は多要素認証（MFA）を利用すること。** P I Nコードは4桁以上とすること。
- **他者へのパスワードの共有、貸与、及び付箋等による放置を禁止する。**
- 私用のパスワードと区別すること。
- 紙やメモへの記載禁止する

第21条（アカウントとアクセス権限の管理）

1. システムやデータへのアクセス権限は、業務上必要な最小限の範囲で付与する。
2. 退職者や異動者のアカウントは、不要となった時点で速やかに停止又は削除しなければならない。

第22条（バックアップの実施）

1. 重要データやシステムは、ランサムウェア等の被害や障害に備え、定期的にバックアップを取得し、ネットワークから分離した安全な場所等に保管しなければならない。
2. バックアップに使用する装置やシステム、クラウドサービスでは、ランサムウェア検知・ファイル復元などのランサムウェア対策機能が実装されていなければならない。

第4章 利用者行動と物理的対策

第23条（事業所への立ち入り制限）

1. 早朝や夜間、休日など無人や小人数対応になる場合は、部外者の不正侵入への注意や施錠徹底に留意しなければならない。
2. 社員章を常時着用し（★要検討）部外者の識別を図るとともに、来訪者への声がけを行うなど不正侵入しにくい

職場づくりをこころがけること。

第 2 4 条（情報資産の持ち出しと端末管理）

1. 秘密情報や個人情報を含む書類、記憶メディア（U S B メモリ等）、パソコンの社外持ち出しは、管理者の許可を得て行わなければならない。
2. 持ち出すデータは必要最小限とし、原則として暗号化等の安全措置を講じること。
3. 端末の紛失や盗難を防ぐため、移動時や移動先での放置を厳禁とする。会議中など長時間離席する場合でもログアウトと情報書類の施錠保管を徹底すること。

第 2 5 条（クリアデスク・クリアスクリーンの徹底）

1. 従業員等は、離席時には必ず画面ロックを行い、第三者による閲覧・操作を防止しなければならない。
2. 業務終了時や長時間離席時には、机上に秘密書類を放置せず、鍵のかかる保管庫に収納しなければならない。

第 2 6 条（私物端末等の業務利用禁止）

1. 従業員等は、当社が許可または支給した端末及び、記録メディア以外の私有物（個人所有のパソコン、スマートフォン、タブレット、U S B メモリ等）を、業務および当社の情報資産の取扱いに使用してはならない。
2. 私用端末から社内ネットワーク、業務用メール、業務用クラウドサービス等へアクセスすることを禁止する。

第 2 7 条（メールに対するセキュリティ）

1. 不審メール・添付ファイル・U R L を開かない。
2. 外部から届いた不明なメールのリンククリック・返信には注意する。
3. メール送信前に以下を確認すること。
 - － 宛先（To/Cc/Bcc）
 - － 添付ファイルの有無と内容
 - － 件名に【添付あり】【重要】など明記
4. 機密ファイルはパスワード付き ZIP + 別送を原則とする。
5. 自動転送設定・個人メールアドレスへの転送は禁止する。

第 2 8 条（ソーシャルメディア・外部サービスの安全利用）

1. 業務上の秘密情報や非公開情報を、個人のソーシャルメディアや外部掲示板等には書き込んではいけない。
2. 管理者の許可なく、個人所有の I T 機器や未承認のクラウドサービスを業務に利用してはいけない。

第29条（廃棄・消去）

秘密情報が記載された書類はシュレッダー等で物理的に復元不可能な状態にして破棄し、記録メディアやPCを廃棄・譲渡する場合は、復元不可能な方法でデータを完全消去しなければならない。

第5章 インシデント対応と継続的改善

第30条（事故・トラブル発生時の報告と対応）

1. 情報資産の紛失、漏洩、ウイルス感染、不正アクセスの兆候などを発見した従業員等は、直ちに業務を中断し、管理者に報告しなければならない。
2. 管理者は、報告を受けた場合、被害拡大防止（ネットワーク切断等）の応急措置を行い、原因調査、関係機関・被害者への報告、及び再発防止策の策定を行わなければならない。（参考）
 - － I P Aセキュリティセンター（cs-support@ipa.go.jp）
 - － 兵庫県警察イバー犯罪対策課（#9110）
3. システムやデータの復旧を行う際は、専門家や関連業者、関係省庁等の助言や協力を得なければならない。また、その手順や状況について記録し、事後の検証を可能としておくこと。

第31条（点検と見直し）

管理者は、年1回以上、自社の対策状況を点検・評価し、本規程および運用手順の見直し・改善を実施しなければならない。

第6章 附則

第32条（施行）

本規程は2025年10月1日より施行する。社会情勢、運用状況、技術動向に応じて適時改定を行う。