情報管理規程　JPMA 標準モデル

目 次

0. 基本方針

0.1 情報セキュリティ基本方針

株式会社●●は、情報セキュリティ基本方針を以下のとおり定める。情報セキュリティ基本方針を本社及び各工場に掲示し従業員及び関係者に周知する。また、情報セキュリティ基本方針を顧客の要請の応じ適宜に公表する。

＜情報セキュリティ基本方針＞

当社は、●●事業を中核としてお客様のニーズに応えてきました。今後も、お客様にご満足いただける製品・サービスを提供するために、高度情報化社会における情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、情報セキュリティ基本方針を定め、当社の情報セキュリティに対する取り組みの指針といたします。

1. 社内体制および情報管理規程の整備
当社は、情報セキュリティの維持及び改善のために必要な管理体制を整備し、必要な情報セキュリティ対策を社内の正式な規則として定めます。
2. 経営者の責任および継続的改善
当社の経営者は、本方針の遵守により、当社及びお客様の情報資産が適切に管理されるよう主導します。
3. 法令、契約上の要求事項の遵守
当社の従業員は、事業活動で利用する情報資産に関連する法令、規制、規範及びお客様との契約上のセキュリティ要求事項を遵守します。
4. 従業員の取組み
当社の従業員は、情報セキュリティの維持及び改善のために必要とされる知識、技術を習得し、情報セキュリティへの取り組みを確かなものにします。
5. 違反及び事故への対応
当社は、情報セキュリティに関わる法令、規制、規範及びお客様との契約に関わる違反及び情報セキュリティ事故への対応のための体制を整備し、違反及び事故の影響を低減します。

〇年〇月〇日
株式会社〇〇〇〇
代表取締役社長　〇〇〇〇

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活動を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、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。

情報セキュリティ委員会	
情報セキュリティ責任者	代表取締役
情報セキュリティ　部門責任者	各部長
システム管理者	総務部長
教育責任者	人事部長
インシデント対応責任者	○○○○部長
監査・点検　責任者	○○○○課長

1.2 情報セキュリティ取組みの監査・点検

監査・点検責任者は、情報管理規程の実施状況について、○月に点検を行い、監査・点検結果を情報セキュリティ委員会に報告する。情報セキュリティ委員会は、報告に基づき、以下の点を考慮し、必要に応じて改善計画を立案する。

- 情報管理規程が有効に実施されていない場合、その原因の特定と改善
- 情報管理規程に定められたルールが、新たな脅威に対する対策として有効でない場合は、情報管理規程の改訂
- 情報管理規程に定められたルールが、関連法令や取引先の情報セキュリティに対する要求を満たしていない場合は、情報管理規程の改訂

1.3 情報セキュリティに関する情報共有

情報セキュリティ責任者は、新たな脅威及び脆弱性に関する警戒情報及び営業秘密や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、委員会で共有する。

1.4 文書の改廃

情報管理規程の改廃は、情報セキュリティ責任者の承認を必要とする。対策規程及び対策手順は、情報セキュリティ委員会が承認する。

2. 人的対策

2.1 雇用条件

従業員を雇用する際には秘密保持契約を締結する。

2.2 取締役及び従業員の責務

取締役及び従業員は、以下を遵守する。

- 取締役及び従業員は、当社が営業秘密として管理する情報及びその複製物の一切を許可されていない組織、人に提供してはならない。
- 取締役及び従業員は、当社の情報セキュリティ基本方針及び情報管理規程を遵守する。違反時には就業規則第○条に従い懲戒処分の対象とする。

2.3 雇用の終了

- 取締役及び従業員は、在職中に交付された業務に関連する資料、個人情報、顧客・取引先から当社が交付を受けた資料又はそれらの複製物の一切を退職時に返還する。
- 取締役及び従業員は、在職中に知り得た当社の営業秘密もしくは業務遂行上知り得た技術的機密を利用して、競合的あるいは競業的行為を行ってはならない。

2.4 情報セキュリティ教育

教育責任者は、以下の点を考慮し、情報セキュリティに関する教育計画を年度単位で立案し、教育資料を使用し、情報セキュリティ教育を実施する。

対象者：全従業員、派遣社員、パート・アルバイト
テーマ：以下は必須とする。

- 情報管理規程の説明（入社時、就業時）
- 組織や個人の情報セキュリティの重要性
- 情報セキュリティ対策
- 情報セキュリティ計画
- モラル教育
- 最新の脅威に対する注意喚起（随時）
- 関連法令（不正競争防止法、個人情報保護法等）の理解（関連法令の施行時）
- 法令、規則等の違反、罰則に関する事項

2.5 違反者に対する再教育

教育責任者は、情報セキュリティ違反者に対して、情報セキュリティの再教育を実施し、違反の再発防止に努める。

3. 情報資産管理

3.1 情報資産の管理

3.1.1 情報資産の特定と重要度の評価

当社事業に必要で価値がある情報（以下「情報資産」という）を特定し、「情報資産管理台帳」に記載し、保護の対象とする。特に印刷機製造情報、顧客情報、●●情報について廃棄まで十分な保護を行う。

情報資産の重要度は、以下の基準に従って評価する。

機密性２：極秘	・ 法律で安全管理措置が義務付けられている ・ 守秘義務の対象として指定されている ・ 漏えいすると取引先や顧客に大きな影響がある	顧客からの預託情報、 及びこれらを含んだ自社の印刷機製造情報
機密性１：社外秘	・ 漏えいすると事業に大きな影響がある	自社の印刷機製造情報
機密性０：公開	・ 漏えいしても事業に影響はない	その他の情報

3.1.2 情報資産の分類と表示

情報資産の重要度は以下の方法で表示する。

・ 電子データ：保存先サーバーのフォルダー名に重要度を明示
・ 書類：保管先キャビネット、ファイル、バインダーに重要度を明示
・ 物：製品サンプル等物そのもの、もしくは保管容器に重要度を明示

表示が困難な場合は、「情報資産管理台帳」に重要度を明記する。

3.1.3 情報資産の管理責任者

情報資産の管理責任者は、当該情報資産を保有する部門長とする。管理責任者は、情報を不正な流出、漏えい、盗難、改ざんから保護する責務を負う。

3.1.4 情報資産の利用者

情報資産の利用を許可する範囲は、「情報資産管理台帳」の利用者範囲欄に部署名又は担当者名を記載する。

3.1.5 情報資産の保護

システム管理者は、電子データの閲覧、編集、削除、移動、複写、印刷等の権限を利用者アカウントに付与する。サーバー機器及びクライアント機器のデータは、暗号化を行う。

3.2 情報資産の社外持ち出し

情報資産を社外に持ち出す場合には、以下を実施する。

- 社外秘の場合は所属部門長の許可を得る。
- 極秘の場合は代表取締役の許可を得る。
- ノートパソコンのハードディスクに保存して持ち出す場合は、ハードディスク/データ・フォルダーを暗号化する。
- スマートフォン、タブレットに保存して持ち出す場合は、セキュリティロックを設定する。
- USB メモリ、HDD 等の電子媒体に保存して持ち出す場合は、不要データは全て完全消去専用ツールで消去し、持ち出すデータを暗号化する。
- USB メモリ等の小型電子媒体は、大きなタグを付ける/ストラップで体やカバンに固定する/落としてもすぐに分かるように鈴を付ける。
- 屋外でネットワークへ接続して社外秘又は極秘の情報資産を送受信する場合は、暗号化通信で行う。
- 携行中は常に監視可能な距離を保つ。

3.3 媒体の処分

3.3.1 媒体の廃棄

社外秘又は極秘の情報資産を廃棄する場合は、所属課長に廃棄申請し、情報システム責任者の承認を得る。処分方法は以下に従う。

- 書類、図面等の紙媒体は、シュレッダーによる細断を行う。
- USB メモリ、DVD 等の可搬式記録媒体は、破壊又は専用ソフトウェアによる完全消去を行い、削除、フォーマットは不可とする。
- 媒体や製品サンプル等の物の破壊又はデータの完全消去を、外部に委託する場合は、破壊又はデータの完全消去を実行したことの証明書を取得する。

3.3.2 媒体の再利用

社外秘又は極秘の情報資産を保存した媒体を再利用する場合は、以下の処分を行う。

書類	裏紙再利用禁止
USB メモリ・HDD・CD-RW ディスク･DVD-RW デ	完全消去後再利用 ※OS の削除機能による削除・フォーマットは不可

ィスク	
CD-R・DVD-R	再利用不可

4. バックアップ

4.1 バックアップ

4.1.1 バックアップ取得対象

システム管理者は、以下の機器で処理するデータのバックアップを定期的に取得する。

機器名	対象	方法	保管先
ファイルサーバー	ユーザーファイル アプリケーションデータ	ファイルコピー	外付 HDD
社内データベースＡ	データベース	ファイルコピー	ミラーサーバー 外付 HDD
社内システムＡ	アプリケーションデータ	ファイルコピー	ミラーサーバー 外付 HDD

4.1.2 バックアップ媒体の取扱い

バックアップに利用した機器及び媒体の取扱いは以下に従う。

- 小型媒体は、施錠付きキャビネットに保管する。
- サーバーは、施錠付きサーバー室に収納する。
- バックアップ媒体の処分は、「3. 媒体の処分」に従う。

4.1.3 クラウドサービスを利用したバックアップ

クラウドサービスを利用し、外部のサーバーにバックアップを保存する場合は、以下のサービス要件を確認し、情報セキュリティ責任者の許可を得て導入する。

＜サービス要件＞

- サービス提供者のサービス利用約款、情報セキュリティ方針が、当社の情報管理規程に適合していること。
- 当社事業所がある地域で発生する災害の影響を受けない地域の施設であること。

4.1.4 バックアップスケジュール

システム管理者は、バックアップ取得対象の機器のバックアップを、以下のスケジュールで定期的に取得する。対象となるファイル名、バックアップ方式については、社内システムＡ「バックアップ」に従う。

5. アクセス制御及び認証

5.1 アクセス制御方針

5.1.1 アクセス制御方針

社外秘又は極秘の情報資産を扱う情報システム又はサービスに対するアクセス制御は以下の方針に基づいて運用する。

- 利用者の認証に用いるアカウントは、利用者１名につき１つを発行する。
- 複数の利用者が共有するアカウントの発行は、情報セキュリティ責任者の承認を得る。
- 「情報資産管理台帳」の利用者範囲に基づき、利用者の業務・職務に応じた必要最低限のアクセス権を付与する。
- 特定の情報資産へのアクセス権が、同一人物に集中することで発生し得る不正行為等を考慮し、複数名に分散してアクセス権を付与する。

5.1.2 アクセス制御対象情報システム及びアクセス制御方法

社外秘又は極秘の情報資産を扱う情報システム、又はサービスに対して、以下のアクセス制御方法で認証する。

情報システム	アクセス制御方法
ファイルサーバー	Windows Active Directory
社内システムＡ、 社内データベースＡ	アプリケーションによるユーザー認証
内部メール	内部メールサービスのユーザー認証
外部メール	ホスティングサービスのユーザー認証

5.1.3 無線機器のアクセス制御方法

社外秘又は極秘の情報資産を扱う情報システムに、無線ネットワーク接続によりアクセスする際の制御方式として、以下を用いる。

- 認証方式は、WPA2-PSK 方式とする。
- 暗号化方式は、AES 方式とする。
- 事前共有キーは、アルファベット大文字、小文字、数字、記号の全てを含む１２文字以上の組み合わせとする。
- ANY 接続は、無効とする。
- 接続する無線機器は、MAC アドレスによる追加認証とする。

5.1.4 利用者アカウント認証方法

社外秘又は極秘の情報資産を扱う情報システム、又はサービスに対する利用者アカウントの認証方法及び発行条件は、以下に従う。

情報システム	利用者認証方法	発行条件	共有
ファイルサーバー	Windows ログオン認証 アカウント及びパスワード	共有アカウント可	可
社内システムA、 社内データベースA	アプリケーションのユーザー認証 アカウント及びパスワード	利用者１名に 対し１つ	不可
内部メール	平文認証 メールアカウント及びパスワード	利用者１名に 対し１つ	不可
外部メール	STARTTLS 暗号化認証 メールアカウント及びパスワード	利用者１名に 対し１つ	可

5.1.5 利用者アカウントの登録

システム管理者は、利用部門から情報システムへアクセスするためのアカウントの新設又は変更の申請があった場合は、情報セキュリティ責任者の承認を得てアカウントの新設又は変更を行う。

- システム管理者は、申請を受けたアカウントを利用者ごとに作成し、アカウントには情報セキュリティ責任者が承認したアクセス権限を設定する。
- システム管理者は、定期的に利用部門の管理職にアカウント権限の見直しを依頼し、権限の変更が必要な場合は、アカウント権限を変更する。
- システム管理者は、新設又は変更したアカウントを、社内システムA「システムアカウント及び付帯情報管理台帳」に記録する。
- システム管理者は、利用者に対し、アカウントに設定した初期パスワードを推測しにくいものに再設定することを確実に伝達する。

5.1.6 パスワードの再発行

パスワード再発行の申請を受けたシステム管理者は、申請してきた利用者が本人自身であることを確認したうえで、速やかに新規のパスワードを発行して利用者に通知する。

5.1.7 利用者アカウントの削除

システム管理者は、利用部門からアカウント削除の申請があった場合は、申請に従いアカウントを停止、無効化する。

- システム管理者は、定期的に利用部門の管理職にアカウントの棚卸しを依頼し、不要なアカウントは停止、無効化する。
- システム管理者は、アカウント管理システムのアクセスログを確認し、一定期間使用されていないアカウントを停止、無効化する。
- システム管理者は、社内システムA「システムアカウント及び付帯情報管理台帳」に、アカウントの停止、無効化を記録する。
- 利用者の認証に用いるアカウントが不要になった場合は、システム管理者は、当該アカウントの削除又は無効化を、当該アカウントが不要になる日の翌日までに実施する。

5.1.8 利用者アカウント及びパスワードの設定

利用者の認証に用いるパスワードは、以下のポリシーに従い設定する。

- ゲスト用アカウントは、無効化する。
- パスワードは、アルファベット大文字、小文字、数字、記号の全てを含む８文字以上の組み合わせとし、利用者が定期的に変更し発行する。
- 社内システムAのパスワード設定は、初期設定以降の変更を利用者が行う。
- パスワードは、一定期間更新がなければ警告を行い、警告に従わない場合はパスワードは失効するものとする。
- システム管理者は、最初のログオン時に、利用者がパスワードを変更するように設定する。
- アカウントは、他人に貸与してはならない。
- パスワードは他人に教えたり、見えるところに表示してはならない。

5.1.9 従業員以外の者に対する利用者アカウントの発行

取締役又は従業員以外の者に、アカウントの発行を禁止する。

5.1.10 特権アカウントの管理

システム及びアプリケーションを制御するための特権アカウントの使用は、システム管理者及び情報セキュリティ責任者に制限する。

6. 物理的対策

6.1 セキュリティ領域の設定

6.1.1 セキュリティ領域の設定

当社内で扱う情報資産の重要度に応じて社内の領域を区分する。区分した領域内では以下を実施する。

レベル 1 領域	事務所受付・応接室・食堂
利用者	従業員、社外関係者、部外者が立ち入り可
施錠	最終退室者による施錠
設置可能情報機器	ディスプレイ、プロジェクター、ホワイトボード
制限事項	未使用時に社外秘又は極秘の情報資産の放置禁止
部外者管理	従業員の許可を受けて入室可能
管理記録	社内システムA「ホワイトボード」
侵入検知	―
来客用名札	着用不要
火災対策	火災検知器、消火器設置

レベル 2 領域	事務所棟（事務執務室，開発設計室，更衣室，倉庫），工場，検査室
利用者	従業員以外の入室は従業員の許可又はエスコートが必要
施錠	最終退室者による施錠及び警備会社への通報装置作動
設置可能情報機器	ディスプレイ、プロジェクター、ホワイトボード、 パソコン、複合機、電話機
制限事項	情報機器・設備の無断操作禁止・無断持出し禁止
部外者管理	従業員/受付守衛/総務部受付の許可を受けて入室可能
管理記録	社内システムA「ホワイトボード」
侵入検知	センサーによる警備会社通報
来客用名札	要着用
火災対策	スプリンクラー、消火器設置

レベル 3 領域	サーバールーム
利用者	あらかじめ登録された者
施錠	常時施錠及び警備会社への通報装置作動、鍵の管理責任者
設置可能情報機	サーバー、ルーター等のネットワーク機器

器	
制限事項	情報機器・設備の無断操作禁止・無断持出し禁止 スマートフォン、USB メモリ、HDD、CD-R、デジタルカメラその他の情報記憶媒体の無断持込み禁止
部外者管理	保守・点検時等に登録者のエスコート付で入室可能
管理記録	社内システムA「ホワイトボード」
侵入検知	センサーによる警備会社通報
来客用名札	要着用
火災対策	不活性ガス系消火設備、純水ベース消火器、空調設備

6.1.2 セキュリティ領域内注意事項

セキュリティ領域では区分に関わらず以下の点に注意する。

- 図面、書類、印刷物を放置しない。
- ファクシミリ送信時には、誤送信防止のため宛先を複数回確認する。
- 室内での撮影及び録音は禁止する。業務上必要な場合は、情報セキュリティ責任者の承認を得る。
- 応接室及び会議室内では、会話の盗聴を防止するよう配慮する。
- 外線受話時の際に相手が不審な場合は、従業員の個人情報を伝えてはならない。
- 部外者を見かけた場合は、用件を確認する。

6.1.3 搬入物の受け渡し

郵便物及び宅配便の受取り・受け渡しは、以下を介して行う。

- 郵便物は施錠ポスト、書留便の場合は事務所棟受付とする。
- 宅配便は事務所棟受付とする。

6.1.4 保管容器での保管

書類等の紙情報や試作品等、情報資産が金庫等の保管容器に保管することができるものである場合には、当該管理対象情報を保管容器に施錠して保管する。
情報資産を保管容器から持ち出す場合には、その取扱う場所を限定する。

7. IT 基盤運用管理

7.1 管理体制

システム管理者は、IT 基盤の運用にあたり情報セキュリティ対策を考慮し製品又はサービスを選択する。IT 基盤の情報セキュリティ対策及び関連仕様は、情報セキュリティ責任者が承認する。

7.2 IT 基盤の運用

システム管理者は、IT 基盤の運用を行う場合は、以下を実施する。

- システム管理者は、機器の管理画面にログインするためのパスワードは、初期状態のまま使わず推測不可能なパスワードを設定して運用する。
- システム管理者は、通信ログを取得及び保存し定期的に確認を行う。

7.3 IT 基盤の記録

システム管理者は、社内システムA「社内 IT 機材管理」台帳に、IT 機器の設定及びその他の情報を記録する。

- ノード名
- 設置場所（設置年月日、保守年月日）
- 利用機器情報（利用者、機種名、ハードウェア情報、保守番号、IP アドレス）
- 利用目的
- OS とそのバージョン
- ソフトウェアとそのバージョン
- 無線 LAN への接続を認可する機器に関する上記の情報

7.4 標準 OS 及びソフトウェア

業務に利用する PC には、標準 OS として Microsoft 社の Windows OS を導入する。標準ソフトウェアは、情報セキュリティ責任者の承認を得たものを使用する。標準 OS 及びソフトウェア以外のシステムを導入する場合は、情報セキュリティ責任者の承認を得る。

7.5 標準 OS 及びソフトウェアのアップデート

システム管理者は、業務で使用する IT 機器の修正プログラム及びセキュリティパッチの自動アップデート機能を有効にする。

7.6 サーバー機器の情報セキュリティ要件

IT 基盤で利用するサーバー機器に求める情報セキュリティ要件は、システム管理者が決定する。新規にサーバー機器を導入する場合は、情報セキュリティ要件を満たす製品を選択し、情報セキュリティ責任者の承認を得て導入する。

- システム管理者は、サーバー機器の電源及び記憶装置の二重化、又は予備機の設置による冗長化を図る。
- システム管理者は、社内システムAへのアクセス等に使用するアカウントを含む全てのアカウントのアクセス権限に対して、必要最低限のアクセス権限のみ許可する。
- システム管理者は、サーバーの趣旨、用途に応じた必要最低限のアプリケーションサービス及びネットワークサービスのみインストールする。
- システム管理者は、サーバーには、システム管理者あるいはオペレータごとに個別のアカウントを割り当て、推測困難なパスワードを設定する。特にシステム管理者もしくはシステム管理者に類する権限を持つアカウントのパスワードは、厳重に管理する。

7.7 サーバー機器に導入するソフトウェア

IT 基盤で利用するサーバー機器に導入するソフトウェアは、システム管理者が標準ソフトウェアを選定する。新規にソフトウェアを導入する場合は、情報セキュリティ責任者の承認を得て導入する。

- システム管理者は、サーバー機器で使用する OS に、最新バージョン又は保守サポートが受けられるバージョンを使用し、最新のセキュリティパッチを適用する。
- システム管理者は、サーバー機器で使用するアプリケーションソフトウェアに、最新のバージョン又は保守サポートが受けられるバージョンを使用し、最新の修正プログラムを適用する。
- システム管理者は、サーバー機器の認証ログ、アクセスログ、トランザクションログ、アプリケーションログ等、サーバー機器の趣旨、用途に応じたログの取得と分析を行う。
- システム管理者は、サーバー機器を信頼できる標準時刻と同期させたマスタークロックと同期させる。

7.8 クライアント機器の情報セキュリティ要件

IT 基盤で利用するクライアント機器に求める情報セキュリティ要件は、システム管理者が決定する。新規にクライアント機器を導入する場合は、情報セキュリティ要件を満たす製品を選択し、情報セキュリティ責任者の承認を得て導入する。

- 従業員が使用できるクライアント機器は、会社が支給、貸与したもののみとする。
- システム管理者は、会社が支給、貸与するクライアント機器には、使用場所、使用す

る情報の重要度に応じて、アカウント及びパスワードによる認証の他、生体認証、ワンタイムパスワード等の、二段階、二要素認証機能を導入する。

7.9 クライアント機器に導入するソフトウェア

IT 基盤で利用するクライアント機器に導入するソフトウェアは、システム管理者が標準ソフトウェアを選定し、従業員の業務に不要な機能及びサービスをあらかじめ取除いて提供する。新規にソフトウェアを導入する場合は、情報セキュリティ責任者の承認を得て導入する。

- システム管理者は、クライアント機器で使用する OS に、最新バージョン又は保守サポートが受けられるバージョンを使用し、最新のセキュリティパッチを適用する。
- システム管理者は、クライアント機器で使用するアプリケーションソフトウェアに、最新のバージョン又は保守サポートが受けられるバージョンを使用し、最新の修正プログラムを適用する。

7.10 ウイルス感染・フィッシング・情報漏えいの防止

IT 基盤で利用するクライアント機器及びサーバー機器は、標的型攻撃メール等によるウイルス感染、フィッシング、情報漏えいを防止するため、以下を実施する。

- 会社は、ネットワーク経由で入手するファイル及び送受信される電子メールは、UTM 装置[1]の自動検知機能を有効にしてウイルス検知を実施する。
- 会社は、送受信される電子メールは、UTM 装置を使用して送受信の履歴を記録する。
- システム管理者は、クライアント機器及びサーバー機器には承認されたウイルス対策ソフトウェアを導入し、常に定義ファイル、エンジンが最新のものとなるように設定する。
- 可搬式記録媒体を用いてファイルの受け渡しを行う場合は、媒体内のファイルにウイルス検知を実施する。
- ウイルス対策ソフトウェアの導入は、情報セキュリティ責任者の承認を得て導入する。

7.11 ウイルス対策ソフト定義ファイルの更新

従業員は、クライアント機器に導入したウイルス対策ソフトウェアの定義ファイルを随時更新する。持ち出し用クライアント機器は、利用時に定義ファイルの更新を確認する。

[1] ルーター、ファイアウォール、アンチウイルス、リモートアクセス、ウェブフィルタリング、仮想ネットワーク等の機能を有する機器。各社の状況に応じて、適切な機器を記載。

7.12 ウイルス対策の啓発

システム管理者は、適宜ウイルスに関する情報を収集し、重大な被害を与えるウイルスに対しては､対応策及び対応に必要な修正プログラムを社内に公開及び通知する｡従業員は、感染防止策が通知された場合は、速やかに実施、完了すること。

7.13 社外機器の LAN 接続

会社が支給、貸与したクライアント及びサーバー以外の機器を、社内 LAN に接続することを禁止する。業務上必要な場合は、情報セキュリティ責任者の承認を得たうえで、当該機器にインストールされているウイルス対策ソフトの定義ファイルを最新版に更新し、当該機器のフルスキャンを実行し、ウイルスが検知されないことを確認してから接続する。

7.14 クリアデスクポリシー

従業員は、社外秘又は極秘の書類及び電子データを保存したノート PC、スマートデバイス、可搬式記録媒体等の持ち運び可能な機器や媒体の扱いについて、以下のようにクリアデスクを徹底する。

- 利用時以外には、机上に放置しない。
- 離席時は書類を伏せる、又は引き出し、キャビネット等に入れる。
- 退社時又は使用しないときには電源を切り、ノート PC、スマートデバイス、可搬式記録媒体は、施錠保管する。

7.15 クリアスクリーンポリシー

従業員は､離席時に以下のいずれかにより PC の画面をロックし、クリアスクリーンを徹底する。

- スクリーンセーバー起動時間を、5 分以内に設定し、パスワードを設定する。
- スリープ起動時間を、5 分以内に設定し、解除時のパスワード保護を設定する。
- 離席時には、［Windows］＋［L］キーを押してコンピュータをロックする
- ログオフ状態では、システム操作画面は非表示に設定する。退社時又は使用しないときには、PC の電源を切る。
- 外出先で利用する場合は、他者が盗み見できる環境で利用しない。

7.16 ウェブ閲覧

会社は、ウイルス等の悪意のあるソフトウェアに感染するおそれがあると認められる有害ウェブサイト、公序良俗に反するサイトは、UTM 装置を使用して従業員の閲覧を制限

すると同時に、閲覧の履歴を記録する。従業員は、業務でウェブ閲覧を行う場合は、以下に注意する。

- 閲覧が可能なサイトの場合でも、不審なサイトへのアクセス及び社用メールアドレスの登録を禁止する。
- 閲覧が制限されたサイトへのアクセスや、スパムメール扱いされたメールの受信が必要な場合は、情報セキュリティ責任者に対し、閲覧制限、スパム扱いの解除を申請し、承認を得る。
- パスワードをブラウザに保存しない。業務で特定のウェブサービスを利用する場合で、パスワードをブラウザに保存する必要があるときは、システム管理者の承認を得る。
- 業務上、個人情報（メールアドレス、氏名、所属等）を入力する場合は、通信の暗号化、接続先の実在性等を十分に確認したうえで行う。

7.17 インターネットバンキング・電子決済

従業員は、インターネットで提供されているオンライン取引サービスを業務で利用する場合は、情報セキュリティ責任者に利用申請を行い、承認を得る。

- インターネットバンキングを利用する場合は、銀行が公開している URL や銀行が提供する専用アプリケーションソフトを用いる。
- 電子決済を利用する場合は、通信暗号化を採用しているサイトを利用する。
- 電子メールに記載されているリンクや、他のウェブサイト等に設置されているリンクは、正規の URL であることを十分に確認したうえでアクセスする。

7.18 クラウドサービス

従業員は、クラウドサービスを業務で利用する場合は、情報セキュリティ責任者に対し利用申請を行い、承認を得る。

- IT 基盤の一部としてクラウドサービス等の外部サービスを導入する場合は、システム管理者が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。
- クラウド等を管理する者の信頼性を確認する。（例：ＩＳＯ／ＩＥＣ27017 の認証の取得の状況、日本セキュリティ監査協会クラウドセキュリティ推進協議会によるＣＳマークの取得の状況等）
- 社外秘又は極秘の情報資産を保存する場合は、情報セキュリティ責任者の承認を得る。
- メールアドレスの登録が必要な場合は、外部メールアドレスを登録する。
- クラウドサービスの管理者との間で秘密保持契約を締結する。

7.19 SNS の利用

会社の業務において SNS の利用を禁止する。

7.20 電子メールの利用

会社は、業務で使用するインターネットメールアドレスを、情報セキュリティ責任者が承認した従業員にのみ貸与する。社内専用の電子メールサービスを提供するため、社内専用のメールアドレスを従業員に貸与し、インターネットへの送受信は拒否する。従業員は、インターネットメールを利用する場合は、以下を実施する。

- 多数相手に同時に送信する場合は、宛先に自分自身のアドレスを入力し、BCC で複数相手のアドレスを指定する。
- 添付ファイルは、パスワード付きの ZIP 形式で送信する。また、パスワードは、本文とは別に時間差を置いてパスワードをメール送信する。
- 受信したメールを、従業員個人のメールアドレスに転送することを禁止する。
- 情報資産データを、従業員個人のメールアドレスに送信することを禁止する。
- 業務でクラウド型メールを利用する場合は、情報セキュリティ責任者に利用申請し、承認を得る。
- 不審なメールの受信をした場合は、直ちにシステム管理者に報告する。

7.21 ネットワーク機器の情報セキュリティ要件

IT 基盤で利用するネットワーク機器に求める情報セキュリティ要件は、システム管理者が決定する。新規にネットワーク機器を導入する場合は、情報セキュリティ要件を満たす製品を選択し、情報セキュリティ責任者の承認を得て導入する。

7.22 データセンター

従業員は、社外のデータセンターを業務で利用する場合は、情報セキュリティ責任者に対し利用申請を行い、承認を得る。

- 社外のデータセンターに自社のサーバー等を設置する場合は、データセンターの信頼性を確認する。（例：日本データセンター協会のデータセンターファシリティスタンダードのティア１からティア４を取得しているデータセンターのうち自らの管理対象情報の価値等に応じてデータセンターのサービスを適切に提供できるか等）
- データセンターとの間で秘密保持契約を締結する。

7.22.1 対象ネットワーク環境

- グローバルアドレスを利用した、インターネット接続環境。
- 本社、●●工場、●●工場を３つのサブネットに区分した、プライベートアドレスを利

用した、社内 LAN 環境。
- 公衆回線を利用した VPN 接続による、社内 WAN 環境。
- 社外から社内システムへのアクセスを提供する、リモートアクセス接続環境。

7.22.2 対象ネットワーク構成機器

- スイッチングハブ、無線 LAN アクセスポイント
- UTM 装置（ルーター、ファイアウォール、アンチウイルス、リモートアクセス、ウェブフィルタリング、仮想ネットワーク）

7.23 ネットワーク構成装置のセキュリティ実装機能

インターネットと接続するゲートウェイに設置するネットワーク機器には、以下のセキュリティ機能を有する機器を設置する。
- 外部からの不正アクセスを防止、検知する機能を有する機能。
- ウェブ通信や送受信メールにおいて、ウイルス、マルウエアを検知、防御する機能。
- 重要な通信を暗号化する機能。
- 送信メールの添付ファイルについて､サイズ制限､拡張子による送信制限を行う機能。
- 不正なサイトへのアクセスによるマルウエア、不正ソフトウェア感染防止のためのアクセス制限。
- マルウエア、不正ソフトウェア感染を狙った虚偽の Web サイトへの誘導や、宣伝を目的としたメールの利用者への到達制限機能。
- 無線 LAN アクセスポイントは、通信の暗号化が可能なこと。
- 無線 LAN アクセスポイントには、認可した機器及び一意のアカウントで認証した人のみ接続が可能なこと。
- １～8 項までのログの取得機能。

7.24 ネットワーク機器の管理

システム管理者は、ネットワーク機器の追加、撤去や設定の変更、パッチ適用、ソフトウェアのバージョンアップ時においては、その変更における影響を事前に検証し問題が発生しないよう努める。
- ネットワーク機器のソフトウェア、ファームウェア等に対するパッチは、適用による影響、適用しないことによる影響を整理したうえで計画をたて適用する。尚、適用が不可能な場合、代替策を講じる。
- ネットワーク機器のパスワードは定期的に変更を行い、担当者の異動，退職があった場合は、そのアカウント及びパスワードを早期に変更又は削除する。
- ネットワークに接続するクライアント機器の利用者、利用目的あるいは利用形態の変更や廃止の利用者からの申請に対し、変更、撤去の手続きを行う。

- 追加，変更内容及び検証結果は、社内システムＡ「プロダクト保守、管理サイト」に記録を残す。
- トラフィック変化に伴うネットワークの帯域の定期的な見直しを行う。
- 定期的にネットワーク機器の脆弱性検査を行い、検出した脆弱性に対し計画を立て、改善する。

7.25 リモートアクセスの利用

リモートアクセスは、情報セキュリティ責任者から許可を受けたクライアント機器で且つ指定された方法で接続する。端末機器を紛失した場合は、直ちに情報セキュリティ責任者に連絡し、指示に従う。

7.26 リモートアクセス接続環境

リモートアクセス接続は、会社が承認したサービスのみを利用する。

- 公衆 WiFi 回線の利用を禁止する。
- 会社が契約するキャリア回線を利用する。
- リモートアクセスは、原則として勤務時間内とする。

7.27 リモートアクセス制御方法

リモートアクセスにより社内の情報システムにアクセスする際の制御方式として、以下を用いる。

- 通信方式は、IPSec 方式とする
- 認証方法は、事前共有キーによる方式とし、アルファベット大文字･小文字、数字、記号の全てを含む１２文字以上の組み合わせとする。
- 暗号化方式は、AES 方式とする。
- リモートアクセス専用のアカウントとパスワードを発行する。

8. 委託管理

8.1 委託先の評価（クラウドサービスの利用を除く）

8.1.1 委託先評価基準

社外秘又は極秘の情報資産の処理あるいは授受を伴う業務を外部の組織に委託する場合は、委託先の情報セキュリティ管理について、当社が講じている社外秘又は極秘の情報資産に関する管理に係る取組みと同等以上の取組みが行われているかどうかを確認する。
下記の評価基準に基づいて評価する。

（委託先評価基準）

社内管理体制	①経営者による情報セキュリティ基本方針がある
	②情報セキュリティ管理責任者を置いている
	③情報セキュリティ対策を定める規程等を整備している
	④情報セキュリティ事故に対する対応手順がある
従業員の監督	⑤全ての従業者に情報セキュリティに関する教育を実施している
	⑥従業者から秘密保持に関わる誓約書等を取得している
オフィス内のセキュリティ	⑦顧客の情報を扱う領域への入退室を管理している
	⑧顧客の情報の保管について施錠管理を実施している
情報機器・媒体の取扱い	⑨機器・媒体の盗難防止措置を講じている
	⑩媒体の無断複製、不正持ち出しを防止する措置を講じている
	⑪媒体の移送、受け渡し時の保護措置を講じている
	⑫媒体の安全な消去、廃棄の手順を整備している
サーバー・パソコン等の管理	⑬業務で使用するサーバー・パソコンのウイルス対策を行っている
	⑭業務で使用するサーバー・パソコンは利用者認証機能を設定している
	⑮業務で使用するサーバー・パソコンに利用制限等を設け管理している

8.1.2 委託先の選定

評価結果に基づき委託先を選定し、情報セキュリティ責任者の承認を得る。

8.1.3 委託契約の締結

委託契約書には、下記に関する事項を明記する。

- 当社の社外秘又は極秘の情報資産及び個人情報の守秘義務
- 再委託についての事項

・　事故時の責任分担についての事項
・　委託業務終了時の当社が提供した社外秘又は極秘の情報資産及び個人情報の返却又は廃棄、消去についての事項
・　情報セキュリティ対策の実施状況に関する監査の方法とその権限
・　契約内容が遵守されない場合の措置
・　事故発生時の報告方法

8.1.4 委託先の評価

委託開始後には、8.1.1 委託先評価基準の委託先における実施状況について定期的に評価する機会を設ける。委託先における評価基準の実施に関して不備又は変更が認められた場合は、双方協議のうえ、対処を検討し、書面で合意する。
＜委託先評価の方法＞
・　委託先事業所に訪問して現場を観察する。
・　委託先の管理責任者にインタビューする。
・　委託先に書面で確認事項を通知し、実施状況について報告してもらう。

8.1.5 再委託

当社が委託する業務を、委託先が他の組織又は個人に再委託する場合には、事前に書面による報告を委託先に求める。報告には必要に応じて以下の提供を含め、当社の「8.1.1 委託先評価基準」「8.1.3 委託契約の締結」「8.1.4 委託先の評価」と同等の管理を再委託先に求めていることを確認し、情報セキュリティ責任者の承認を得たうえで再委託を認める。
・　委託先と再委託先との契約書案の写し（情報セキュリティに関連する部分のみ）
・　再委託先の選定基準
・　再委託先が情報セキュリティに関する適合性評価制度の認証・認定を取得している場合にはその証書の写し

8.1.6 秘密保持契約の締結

社外秘又は極秘の情報資産の処理あるいは授受を伴う業務を外部の組織に委託する場合は、以下の内容を含む秘密保持契約を締結した後で引き渡す。
・　情報資産の第三者への開示の禁止
・　情報資産の取扱者の限定
・　情報資産の取扱者の氏名等の当社への開示
・　情報資産の取扱者の範囲が必要最小限であることの当社への説明
・　情報資産へのアクセスの記録、及び管理
・　情報資産の複製、廃棄等をした場合の管理簿の作成、及び一定期間の保管

- 情報資産の複製、廃棄等に関する当社への通知
- 情報資産に係る契約の満了時又は解除時の、当該情報資産の速やかな廃棄又は返還
- 情報資産の状況に関する定期的な報告
- 定期的又は不定期な当社からの監査受け入れ
- 情報資産が秘密保持契約等の対象であることの表示
- 情報資産の目録の作成

9. 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

9.1 対応体制

情報セキュリティインシデント(事件及び事故)が発生した際には以下の体制で対応する。

最高責任者	代表取締役
対応責任者	インシデント対応責任者
一次対応者	発見者又はシステム管理者

9.2 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	対応者
3	顧客、取引先、株主、等に影響が及ぶとき 個人情報が漏えいしたとき	代表取締役 インシデント対応責任者
2	事業に影響が及ぶとき	インシデント対応責任者
1	従業員の業務遂行に影響が及ぶとき	システム管理者
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とき	システム管理者

9.3 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、発見者は以下の連絡網に従い、対応者に速やかに報告し、指示を仰ぐ。

最終対応者	緊急連絡先
代表取締役	携帯電話：090-****-**** 電子メールアドレス：president@*****.co.jp
インシデント対応責任者	携帯電話：090-****-**** 電子メールアドレス：incident@*****.co.jp
システム管理者	携帯電話：090-****-**** 電子メールアドレス：system@*****.co.jp

9.4 対応手順

インシデントを以下のとおりに区分し、それぞれの対応手順を示す。

区分	事件・事故の状況
漏えい・流出	社外秘又は極秘情報資産の盗難、流出、紛失
改ざん・消失・破壊 サービス停止	情報資産の意図しない改ざん、消失、破壊 情報資産が必要なときに利用できない
ウイルス感染	悪意のあるソフトウェアに感染

9.4.1 漏えい・流出発生時の対応

事故レベル	対応手順	対応者
3	①一次対応者は即座にシステム管理者、対応責任者及び最高責任者に報告する。 ②対応責任者は原因を特定するとともに、二次被害が想定される場合には防止策を実行する。 ③対応責任者は被害者/本人対応を準備する。 ④対応責任者は問い合わせ対応を準備する。 ⑤対応責任者は影響範囲・被害の大きさによっては総務部に顧客及び取引先への公表準備を申請する。 ⑥対応責任者はサイバー攻撃等の不正アクセスによる被害の場合は都道府県警察本部のサイバー犯罪相談窓口に届け出る。 ⑦対応責任者は個人情報の漏えいの場合には監督官庁に届け出る。 ⑧最高責任者は社内及び影響範囲の全ての組織・人に対応結果及び対策を公表する。	代表取締役 インシデント対応責任者
2	①一次対応者は発見次第、システム管理者、対応責任者及び最高責任者に報告する。 ②システム管理者は漏えい先を調査し、対応責任者及び最高責任者に報告する。 ③システム管理者は原因を特定し、防止策を実行する。 ④対応責任者は社内関係者に周知すると共に総務部に連絡する。	インシデント対応責任者
1	※情報漏えい・流出は全て事故レベル 2 以上	

9.4.2 改ざん・消失・破壊・サービス停止発生時の対応

事故レベル	対応手順	対応者
3	①一次対応者は即座に対応責任者及び最高責任者に報告する。 ②システム管理者は原因を特定し、応急処置を	代表取締役 インシデント対応責任者

	実行する。 ③対応責任者は社内に周知するとともに総務部に連絡する。 ④電子データの場合はシステム管理者がバックアップによる復旧を実行する。 ⑤機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。 ⑥書類等の原本の場合は部門責任者が可能な範囲で修復する。 ⑦システム管理者は原因対策を実施する。 ⑧最高責任者は社内及び影響範囲の全ての組織・人に対応結果及び対策を公表する。	
2	①一次対応者は発見次第、システム管理者及び最高責任者に報告する。 ②システム管理者は原因を特定し、応急処置を実行する。 ③対応責任者は社内に周知するとともに総務部情報システム担当に連絡する。 ④電子データの場合はシステム管理者がバックアップによる復旧を実行する。 ⑤機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。 ⑥書類等の原本の場合は部門責任者が可能な範囲で修復する。 ⑦システム管理者は原因対策を実施する。	システム管理者 インシデント対応責任者
1	①一次対応者は発見次第、システム管理者及び最高責任者に報告する。 ②システム管理者は原因を特定し、応急処置を実行する。 ③電子データの場合はシステム管理者がバックアップによる復旧もしくは再作成・入手を実行する。 ④機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。 ⑤書類等の原本の場合は部門責任者が可能な範囲で修復する ⑥システム管理者は原因対策を実施する	システム管理者
0	①一次対応者は発見次第、発生可能性のある状況と想定される被害をシステム管理者及び最高責任者に報告する。	システム管理者

9.4.3 ウイルス感染時の初期対応

従業員は、業務に利用しているパソコン、サーバー又はスマートフォン、タブレット（以下「コンピュータ」といいます。）がウイルスに感染した場合には、以下を実行する。

・　一次対応者は、発見次第、LAN ケーブルを抜く、Wi-Fi を OFF にする等、ネットワークからコンピュータを切断する。

・　一次対応者は、システム管理者及び最高責任者に連絡する。
・　一次対応者は、ウイルス対策ソフトの定義ファイルを最新版に更新する。
・　一次対応者は、ウイルス対策ソフトを実行しウイルス名を確認する。
・　一次対応者は、ウイルス対策ソフトで駆除可能な場合は駆除する。
・　駆除後再度ウイルス対策ソフトでスキャンし、駆除を確認する。
・　システム管理者に報告する。
・　システム管理者は、原因を特定し、情報漏えいや不正なサイトへのアクセスが行われていないか確認する。
・　システム管理者は、感染を確認すると共に、感染の拡大を防止するため、必要に応じてインターネット回線を遮断する。

以下の場合等、一次対応者自身で対応できないと判断される場合はシステム管理者に問い合わせる。
・　ウイルス対策ソフトで駆除できない。
・　システムファイルが破壊・改ざんされている。
・　ファイルが改ざん・暗号化・削除されている。

9.4.4 攻撃の検知、防御、駆除の通知等発生時の対応

システム管理者は、UTM 装置の自動検知機能によって処理された攻撃、防御、駆除の結果について、自動通知されるログを確認し、感染、攻撃、侵入等の疑いがないか確認する。

9.5 情報セキュリティインシデントによる事業中断と事業継続管理

代表取締役は、情報セキュリティインシデントの影響により当社事業が中断した場合に備え、以下を定める。

9.5.1 復旧責任者及び関連連絡先、対応方法

災害及び事故の発生に伴う設備の倒壊、回線の途絶、停電等による情報システムのサービス停止を想定し、以下の基準に従い対応する。システム管理者ならびに情報セキュリティ責任者は、関係部門に適切に指示を行い復旧に当たる。

被害対象	対応方法	復旧責任者	関係者連絡先
電力	障害状況の連絡と復旧依頼	XXX	XXX
受電設備	障害状況の連絡と復旧依頼	XXX	XXX
キャリア回線	障害状況の連絡と復旧依頼	XXX	XXX
電話・LAN 設備	障害状況の連絡と復旧依頼	XXX	XXX
UTM 機器	障害状況の連絡と復旧依頼	XXX	XXX

インターネット	障害状況の連絡と復旧依頼	XXX	XXX
Web・メール サービス	障害状況の連絡と復旧依頼	XXX	XXX
社内システムＡ	１．障害状況の把握 ２．データのリカバリ作業 ３．バックアップ機への切替	XXX	XXX

9.5.2 事業継続計画

情報セキュリティ委員会は、想定する情報セキュリティインシデントが発生し、事業が中断した際の復旧責任者の役割認識及び関係者連絡先について、有効に機能するか検証する。情報セキュリティ責任者は、被害対象に応じて復旧から事業再開までの計画を立案する。

10. 社内体制図

10.1 情報セキュリティのための組織

「1. 組織的対策」における「2. 情報セキュリティのための組織」を下図に示す。組織の変更があった場合は、情報セキュリティ責任者が本体制図の更新を行う。