版番号	02
発行日	2024/7/25

情報セキュリティ管理規程

Information Security Management Systems

株式会社 YNP

～　改訂履歴　～

版番号	発行年月日	改　訂　内　容	作　成	承　認
1	2021 年 9 月 1 日	制定	原	社長
2	2024 年 7 月 25 日	規格改訂による全面見直し	原	社長

目次

目的
本規程は、当社の情報セキュリティマネジメントシステムの情報管理を明確にする。
・区分
情報資産は、その内容に応じて以下の３つに区分する。
(1)業務情報：経営、業務上の全ての情報。
(2)個人情報：(1)のうち、氏名、住所、電話番号等、特定の個人を識別できる情報。
(3)機密情報：(1)のうち、経営、業務上の重要で、秘密を保つ必要がある情報。

適用範囲
本規程は、当社の情報セキュリティマネジメントシステムの情報管理について適用する。

責任と権限
各個別の項目に責任と権限を明確にする。
以下の項目立ては、詳細管理策の項番に従う。

5　組織的管理策

5.1　情報セキュリティのための方針群

情報セキュリティ方針及びトピック固有の方針は、これを定義し、管理層が承認し、発行し、関連する要員及び関連する利害関係者に伝達し、認識させ、あらかじめ定めた間隔で及び重大な変化が発生した場合にレビューしなければならない。

・情報セキュリティのための方針群は以下に定める。
「情報セキュリティ方針」
「ISMS マニュアル」
「事業継続マニュアル」
「情報セキュリティ管理規程」
「適用宣言書」

5.2　情報セキュリティの役割及び責任

情報セキュリティの役割及び責任は,組織のニーズに従って定め,割り当てなければならない。

ISMS マニュアル 5.3 に規定する。

5.3　職務の分離

相反する職務及び相反する責任範囲は,分離しなければならない。

・相反する作成者および承認者を「ISMS マニュアル」に記載の情報セキュリティマネジメントシステムにおける役割と責任権限一覧表に明確にする。
・情報資産台帳のリスク所有者やアクセス権設定の基準となる職務分離、部署、グループ等の明確化を行う。

5.4　管理層の責任

管理層は,組織の確立された情報セキュリティ方針,トピック固有の方針及び手順に従った情報セキュリティの適用を,全ての要員に要求しなければならない。

・代表者は、役員・正社員および準社員に対し、情報セキュリティ基本方針及びその他の手順に従って業務上、情報セキュリティを遵守するよう要求すること。

5.5　関係当局との連絡

組織は、関係当局との連絡体制を確立し、維持しなければならない。

・事件・事故発生時に、適切な処置が迅速に取られ、助言を得られることを確実にするために、必要な行政機関、規制機関、情報サービス提供者及び通信業者の連絡先を以下に明確にする。
・関係当局に連絡するかどうかの判断は、管理責任者が判断する。

連絡担当	関係当局
管理責任者	ISMS 審査機関（GCERTI）：06-7662-0441 IPA JPCERT
	通信事業者
	電気関連（電気設備工事、ネットワーク工事）
	警察（110 番） 各都道府県警察本部のサイバー犯罪相談窓口
	ビル管理会社
	顧客
	協力会社

5.6　専門組織との連絡

組織は,情報セキュリティに関する研究会又は会議,及び情報セキュリティの専門家による協会・団体との連絡体制を確立し,維持しなければならない。

・ウイルス感染した場合：IPA　　https://www.ipa.go.jp/
・個人情報に関する事項：JIPDEC　　https://www.jipdec.or.jp/
・HP へアタックされた場合：JPCERT　　https://www.jpcert.or.jp/

5.7　脅威インテリジェンス

情報セキュリティの脅威に関連する情報を収集及び分析し、脅威インテリジェンスを構築しなければならない。

・管理責任者は脅威インテリジェンスについて IPA のメールマガジンから情報収集を行う。
・新たな脅威を発見した場合、リスクアセスメントを実施し、組織の脆弱性に応じて対応を行う。

5.8　プロジェクトマネジメントにおける情報セキュリティ

情報セキュリティをプロジェクトマネジメントに組み入れなければならない。

サービスやプロジェクトの種類に関わらず、情報セキュリティに取り組み、情報セキュリティ管理規定やプロジェクトごとに必要となるセキュリティルールに従う。

5.9　情報及びその他の関連資産の目録

情報及びその他の関連資産の目録を，それぞれの管理責任者を含めて作成し，維持しなければならない。

・情報資産の洗い出し（情報資産の把握）
当社の情報資産は、すべて何らかの業務上の必要性に基づいて保有していることから、業務の流れを参照しながら情報資産を「情報資産リスクアセスメント表」に記載する。

5.10　情報及びその他の関連資産の許容される利用

情報及びその他の関連資産の許容される利用に関する規則及び取扱手順は，明確にし，文書化し，実施しなければならない。

・リスク所有者は、当社の情報資産に関して、その導入、開発、維持、使用及びセキュリティの管理についての権限と責任を負い、「管理責任者」が任命するものとする。
・許容範囲は「情報資産リスクアセスメント表」にてリスク所有者が明確にする。

情報管理区分 / 取扱い	極秘	社外秘	公開
保管（紙媒体）	鍵付きキャビネット、金庫	鍵付きキャビネット	―
保管（データ）	アクセス制限	アクセス制限	HP 等
移送	禁止	中身の透けない郵便	中身の透けない郵便
送信	禁止	通信の暗号化 パスワード設定	―
利用範囲	役職者	従業員	―
委託・提供	原則不可	可能	可能
廃棄	シュレッダー	シュレッダー	―
消去	責任者が実施	責任者が実施	―

5.11　資産の返却

要員及び必要に応じてその他の利害関係者は，雇用，契約又は合意の変更又は終了時に，自らが所持する組織の資産の全てを返却しなければならない。

・従事者は、雇用、契約又は取決めの終了時に、保有していた当社の資産を全て返却しなければならない。

5.12　情報の分類

情報は,機密性,完全性,可用性及び関連する利害関係者の要求事項に基づく組織の情報セキュリティのニーズに従って,分類しなければならない。

・「情報資産リスクアセスメント表」にて情報資産の分類を実施する。
・　5.10 に基づき分類、またこれに従い、5.13 を参照してラベル付で区分をする。

5.13　情報のラベル付け

情報のラベル付けに関する適切な一連の手順は,組織が採用した情報分類体系に従って策定し,実施しなければならない。

・組織が保有する情報資産の重要性に応じて、ラベル付けを行い「情報資産リスクアセスメント表」にて管理を実施する。

5.14　情報転送

情報の転送の規則,手順又は合意を,組織内及び組織と他の関係者との間の全ての種類の転送手段に関して備えなければならない。

・当社と外部関係者の間で、情報転送する場合には、合意を得て実施すること。

5.15　アクセス制御

情報及びその他の関連資産への物理的及び論理的アクセスを制御するための規則を,事業上及び情報セキュリティの要求事項に基づいて確立し,実施しなければならない。

・管理責任者は、情報システムへの無許可アクセスを防止するため、パスワードによるアクセス管理を実施することを方針とし、利用者や利用者グループごとにアクセス権を設定する。
・システム管理者が認可したネットワークのみを使うこととし、個人が勝手にネットワークを構築してはならない。
・第三者が提供するネットワークサービスに情報を格納する場合には、会社が認可したものだけを使う。

5.16　識別情報の管理

識別情報のライフサイクル全体を管理しなければならない。

■アカウントの発行
アカウントの発行に当たって、以下の事項を実施しなければならない。
・システムを利用する者（あるいは部門長）は、新規にアカウントが必要になった場合、システム管理者にアカウントの発行を申請する。
・システム管理者は、アカウント発行の申請を受けた場合、その事由を精査し妥当と判断した場合、必要最小限のアクセス権限を持つ、新規アカウントを発行する。

■アカウントの変更・削除
アカウントの変更・削除に当たって、以下の事項を実施しなければならない。

・システムを利用する者は、アカウントが不要となった場合、システム管理者に通知し、アカウントの削除を依頼する。
・システム管理者は、アカウントの変更の発行の申請を受けた場合、その事由を精査し妥当と判断した場合、必要最小限のアクセス権限を付与する。また、削除の依頼があった場合、速やかに利用できないよう対応する。

5.17　認証情報

認証情報の割当て及び管理は,認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理しなければならない。

・パスワードは原則として 8 文字以上かつ英字（大文字、小文字を含む）・数字・記号のうち複数種類を用いたパスワードを確実にするための有効な対話的機能を提供しなければならない。
・パスワードの管理はリスクアセスメントの結果に基づき、決定する。
・パスワード変更については、固定のものと変更が必要なものを決定する。
・パスワード等は利用者以外の目に触れないように管理する
・パスワードをシステム内に記憶させないこと
・パスワード管理表を作成する場合は、パスワード保管システム等を利用し、強固なセキュリティ保護を行ったうえで実施すること。

5.18　アクセス権

情報及びその他の関連資産へのアクセス権は,組織のアクセス制御に関するトピック固有の方針及び規則に従って,提供,レビュー,変更及び削除しなければならない。

・アクセス権の設定は、責任権限に基づく許可のもとシステム管理者によりなされるものとする。
・アクセス権のレビューは、各部門責任者が定期的に実施する。
・パスワードの割り当ては、利用者登録の手順に従い設定するものとし、利用者のパスワードの管理は、責任権限に基づく許可のもとシステム管理者が行うものとする。
・管理責任者の退職などにより、後任へ管理責任者が引き継がれた場合は、ファイルサーバなどの管理者用パスワードは、速やかに変更しなければならない。

■アクセス権の変更
・従業員の異動があった場合には、部門責任者等の依頼に基づき責任権限に基づく許可のもとシステム管理者は速やかに変更するものとする。
■アクセス権の削除
・従業員の情報及び施設設備へのアクセス権は、雇用、契約又は取決めの終了時に責任権限に基づく許可のもとシステム管理者が削除するものとする。これに関しても前項に従うものとする。
（　5.11 資産の返却と関連付けて実施すること）
■入退社の確認
・従業員の雇用、契約又は取決め終了時には、部門責任者等の依頼に基づき責任権限に基づく許可のもとシステム管理者は速やかに削除するものとする。

5.19　供給者関係における情報セキュリティ

供給者の製品又はサービスの利用に関連する情報セキュリティリスクを管理するためのプロセス及び手順を定め,実施しなければならない。

・5.22 の規定に従うものとする。

5.20　供給者との合意における情報セキュリティの取扱い

供給者関係の種類に応じて,関連する情報セキュリティ要求事項を確立し,各供給者と合意しなければならない。

・施設の管理要員のアクセスに関わる取決めは、機密の保持を含む正式な契約に基づいて決定する。
・情報処理に関わる業務を外部に委託する場合は、セキュリティ要求事項を明記した契約を取り交わす。
・前記の契約を得られていない第三者の作業には、社員が立ち会うなどの対策をとることでセキュリティの確保を図る。

5.21　情報通信技術(ICT)サプライチェーンにおける情報セキュリティの管理

ICT 製品及びサービスのサプライチェーンに関連する情報セキュリティリスクを管理するためのプロセス及び手順を定め,実施しなければならない。

・組織の資産に対する供給者のアクセスに関連するリスクを軽減させるための情報セキュリティ要求事項について、供給者と合意し、契約書や機密保持誓約書へ文書化しなければならない。

5.22　供給者のサービス提供の監視,レビュー及び変更管理

組織は,供給者の情報セキュリティの活動及びサービス提供の変更を定常的に監視し,レビューし,評価し,管理しなければならない。

■委託先の監督
・業務担当者は、委託先が提供するサービスの取り決めに含まれるセキュリティ管理策、サービスの定義、及び提供のレベルを、委託先が確実に実施、運用、維持していることを監視しなければならない。
・再委託の可否については慎重に検討し、その可否を決定すること。
・委託先が再委託をしている場合は、委託先にも再委託先に対し同等の監視をすることを義務付け、業務担当者は、委託先が確実に監視しているかのチェックをしなければならない。

■委託先の選定
■新規評価
・随時、担当者が面接して当社のセキュリティ要件に適合しているか判断し、基本契約書、秘密保持契約書を締結する。
■継続評価

・セキュリティ講習会に参加しているか、または秘密保持誓約の取り交わしが行われているかを確認する。
・重大な不適合が起こった場合、他にも重大な不適合を発生させていないか、当社のセキュリティ要件に適合しているかを確認し、基本契約書、秘密保持契約書に則り再評価する。

・ISMS 事務局は、当社の情報セキュリティ基本方針、ISMS マニュアル、規程、手順等の維持及び改善も含め、委託先によるサービスの提供に対する変更を管理する。これには関連する業務システム及びプロセスの重要性と、再度のリスクアセスメントを考慮に入れなければならない。

5.23　クラウドサービスの利用における情報セキュリティ

クラウドサービスの調達,利用,管理及び利用終了のプロセスを,組織の情報セキュリティ要求事項に従って確立しなければならない。

・利用しているサービスについて、「情報資産リスクアセスメント表」「クラウド一覧表」にサービスの使用目的、保管されている組織の情報の内容等の記載対応を行う。
・クラウドサービスを新たに利用する際は組織にて定めた選定基準を満たしたサービスを利用するものとする。

5.24　情報セキュリティインシデント管理の計画策定及び準備

組織は,情報セキュリティインシデント管理のプロセス,役割及び責任を定め,確立し,伝達することによって,情報セキュリティインシデント管理を計画し,準備しなければならない。

・ISMS 関連のインシデントの管理は、管理責任者がその任にあたり、発生したインシデントに対する対応策の検討及び実施と再発防止に関する責任を負う。

5.25　情報セキュリティ事象の評価及び決定

組織は、情報セキュリティ事象を評価し、それらを情報セキュリティインシデントに分類するか否かを決定しなければならない。

・情報セキュリティ事象については、管理責任者はこれを評価し、情報セキュリティインシデントに分類するか否かを決定しなければならない

5.26　情報セキュリティインシデントへの対応

情報セキュリティインシデントは、文書化した手順に従って対応しなければならない。

・情報セキュリティインシデントとは、情報セキュリティ事象からインシデントと分類されるもの。
情報漏洩、情報紛失、ウィルス感染、サイバー攻撃被害、システム障害　他を指す。
・発生時：初期対応、報告、再発防止の処置をとる。「不適合（インシデント）是正処置報告書」を起票し、不適合是正処置の手順に則って是正処置の対応をとること。

5.27　情報セキュリティインシデントからの学習

情報セキュリティインシデントから得られた知識は,情報セキュリティ管理策を強化し,改善するために用いなければならない。

・当社において発生したセキュリティ事故やソフトウェア誤動作の種別、及び大きさ等の影響度を、ISMS 事務局にて可能な限り定量化を行うものとする。
・記録を収集して、次回の教育から実施するものとする。また、情報資産リスクアセスメント表でリスク対策の再検討を行う。

5.28　証拠の収集

組織は,情報セキュリティ事象に関連する証拠の特定,収集,取得及び保存のための手順を確立し,実施しなければならない。

・情報セキュリティインシデント発見後の人又は組織に対するフォローアップ措置が（民事であれ刑事であれ）法的行為にかかわるものである場合、管理責任者によって、証拠は、該当する司法権のもとで定められた証拠に関する規定に適合するように、収集、保管、及び提示できるようにすること。
■盗難・不正アクセス等犯罪による可能性が高いインシデントが発生した場合
（１）　警察などへの連絡
（２）　インシデント関連施設の証拠保全
（３）　情報システムのログ管理
（４）　インシデント関連施設利用の停止、あるいは証拠保全に影響のない利用
（５）　現場の写真撮影
その他外部機関等の指示に従う。

5.29　事業の中断・阻害時の情報セキュリティ

組織は,事業の中断・阻害時に情報セキュリティを適切なレベルに維持する方法を計画しなければならない。

・管理責任者は、組織全体を通じて事業継続のための活動のために、組織の事業継続に必要な情報セキュリティの要求事項を取り扱う管理された手続きを「事業継続計画マニュアル」に策定し維持する。

・管理責任者は、重要な業務プロセスの中断又は不具合発生の後、運用を維持又は復旧するために、また、要求されたレベル及び時間内での情報の可用性を確実にするために、計画を策定し実施する。実施した内容は「事業継続計画・結果」に記録する。

5.30　事業継続のための ICT の備え

事業継続の目的及び ICT 継続の要求事項に基づいて，ICT の備えを計画，実施，維持及び試験しなければならない。

・確立及び実施した情報セキュリティ継続のための管理策が、困難な状況の下で妥当かつ有効であることを確実にするために、１年に１度、「事業継続計画マニュアル」の管理策を検証する。実施した内容は「事業継続計画・結果」に記録する。

5.31　法令、規制及び契約上の要求事項

情報セキュリティに関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組を特定し、文書化し、また、最新に保たなければならない。

・管理責任者は、「関連法規制一覧表」に組織業務に関連するすべての関連する法令、規制及び契約上の要求事項を記載する。
・関連法規制一覧には、要求事項をみたすための組織の取組みを、明確に特定し、文書化し、また、最新化すること。
・法令規制に更新・修正・削除（消滅）があった場合には、直ちにその情報を本規程に反映させ、常に最新の状態で情報を維持するものとし、定期的および随時、更新等の有無について確認するものとする。
・更新などが有った場合は、その情報を当社の役員及び従業者に速やかに通達するものとする。

5.32　知的財産権

組織は、知的財産権を保護するための適切な手順を実施しなければならない。

・情報セキュリティに関連する法令・条令及び業界のガイドライン等（以下、「規則」という）の特定に関しては以下に種類分けすることとする。
（１）必須のもの
必須のものには、下記の法令が含まれなければならない
・知的財産関連
・個人情報保護に関する法律
（２）任意のもの

5.33　記録の保護

記録は，消失，破壊，改ざん，認可されていないアクセス及び不正な流出から保護しなければならない。

・当社の事業活動並びに日常業務に関わる重要な記録は、法令、規則、契約及び事業上の要求事項に従って、消失、破壊、改ざんから保護すること。

5.34　プライバシー及び個人を特定できる情報(PII)の保護

組織は,適用される法令,規制及び契約上の要求事項に従って,プライバシーの保護(preservation)及び PII の保護(protection)に関する要求事項を特定し,満たさなければならない。

・個人情報保護法に従うものとする。

5.35　情報セキュリティの独立したレビュー

人,プロセス及び技術を含む,情報セキュリティ及びその実施の管理に対する組織の取組について,あらかじめ定めた間隔で,又は重大な変化が生じた場合に,独立したレビューを実施しなければならない。

・情報セキュリティおよびその実施のマネジメントに対する組織の取組み（例えば、情報セキュリティのための管理目的、管理策、方針、プロセス、手順）について、あらかじめ計画した間隔で、又はセキュリティの実施に重大な変化が生じた場合に、独立したレビューを実施する。

5.36　情報セキュリティのための方針群、規則及び標準の順守

組織の情報セキュリティ方針,トピック固有の方針,規則及び標準を順守していることを定期的にレビューしなければならない。

・情報セキュリティ教育及びその実施のレビューを実施する。
・必要な場合には、適切なソフトウェアツールによる助けを得て、技術的順守の点検を実施する。

5.37　操作手順書

情報処理設備の操作手順は,文書化し,必要とする要員に対して利用可能にしなければならない。

・管理責任者は、個別情報システムの事業上の重要性を考慮し、当社が定めるリスク許容レベルを満たすために必要な場合、操作手順を文書化するものとする。

6　人的管理策

6.1　選考

要員になる全ての候補者についての経歴などの確認は,適用される法令,規制及び倫理を考慮に入れて,組織に加わる前に,及びその後継続的に行わなければならない。また,この確認は,事業上の要求事項,アクセスされる情報の分類及び認識されたリスクに応じて行わなければならない。

・入社予定の従事者に対して、応募資料の内容が、関連する法律、規制及び倫理に従っているかどうかを選考者が確認すること。また、面談の結果に基づき当社の社員として適切か判断する。この確認は、業務上の要求事項、アクセスされる情報の分類、認識されたリスクに相応したものであること。

6.2　雇用条件

雇用契約書には、情報セキュリティに関する要員の責任及び組織の責任を記載しなければならない。

・誓約書等には、当社の情報セキュリティに対する責任について明記するものとする。
・契約上の義務の一部として、入社予定の役員・正社員および契約予定の準社員は、以下の書面に同意し署名すること。
「**機密保持誓約書**書」
・当社への派遣社員に関しては会社間（当社と派遣会社）の秘密保持契約書をもってこれに代えることとする。

6.3　情報セキュリティの意識向上、教育及び訓練

組織の要員及び関連する利害関係者は,職務に関連する組織の情報セキュリティ方針,トピック固有の方針及び手順についての,適切な,情報セキュリティに関する意識向上プログラム,教育及び訓練を受けなければならず,また,定常的な更新を受けなければならない。

・教育担当は当社の従業員に対し、その職務権限に応じて以下の教育を実施すること。
・情報セキュリティ管理規程等組織の方針、手順の教育を実施すること。
・教育の記録は作成し、保持すること。

6.4　懲戒手続

情報セキュリティ方針違反を犯した要員及びその他の関連する利害関係者に対して処置を講じるために,懲戒手続を正式に定め,伝達しなければならない。

・ISMS に関する定めに対する違反者の対応は、就業規程の定めに従う。

6.5　雇用の終了又は変更後の責任

雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め,施行し,関連する要員及びその他の利害関係者に伝達しなければならない。

・雇用および契約終了時又は、部署異動については、当社代表者の指示に従うこと。
・雇用終了時は　5.11 資産の返却の手続きを参照すること。

6.6　秘密保持契約又は守秘義務契約

情報保護に対する組織のニーズを反映する秘密保持契約又は守秘義務契約は，特定し，文書化し，定常的にレビューし，要員及びその他の関連する利害関係者が署名しなければならない。

関連部門	相手	関連書類	レビュー方法
管理責任者	お客様	・契約書	適宜レビュー、コピーを保管する
	従業員	・秘密保持契約書	適宜レビュー、コピーを保管する

6.7　リモートワーク

組織の構外でアクセス，処理又は保存される情報を保護するために，要員が遠隔で作業をする場合のセキュリティ対策を実施しなければならない。

・リモートワークについて以下に定める。

実施場所	ルール/許可者
自宅	①ＰＣにかならずＩＤ・パスワードを入れる。 ②ＰＣにウィルス対策ソフトを起動させる。 ③フリーWi-Fi を使わない。 ④離席時には必ず PC をログオフする。 ⑤紛失時は管理責任者に即時報告をする。 ⑥個人所有の PC は原則業務での使用はしてはいけない。 ⑦自宅以外で作業を行う場合は、壁側を背に向け、のぞき見されないように防止する。

6.8　情報セキュリティ事象の報告

組織は，要員が発見した又は疑いをもった情報セキュリティ事象を，適切な連絡経路を通して時機を失せずに報告するための仕組みを設けなければならない。

・情報セキュリティ事故やそれに準ずる（疑わしい場合も含む）インシデントを発見、あるいは質問の問い合わせを受けた従業員は、定められた報告経路に基づき、速やかに代表者に報告を行い、指示通りに対応するものとし、報告内容は、「不適合（インシデント）是正処置報告書」にもれなく記載しなければならない。
・尚、インシデントを発見した従業員は、独自の判断で対応してはならない。但し、きわ

めて緊急性を要する場合は、リスク所有者、直属の上司、及び複数の従業者の判断により対応するものとする。

7　物理的管理策

7.1　物理的セキュリティ境界

情報及びその他の関連資産のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いなければならない。

■訪問者の入室・退室手続及び識別
・訪問者が入退できるのはフリースペースに限定するものとする。アポイント無く、やむを得ず会社施設(執務スペース)入室する場合は従業者の立会いのもと同行し、目を離さないようにする。

7.2　物理的入退

セキュリティを保つべき領域は,適切な入退管理策及びアクセス場所【訳注:受付など】によって保護しなければならない。

■出入口の解錠及び施錠
・当社の従業員は施設入り口のセキュリティカードによる施錠によって入退室制限を行い、施錠鍵の使用者は代表者が認めたものとする。
■セキュリティカードによる入退室管理
・必要最低限の要員に配布し、カード№、所持者の一覧表を作成管理すること。
・予備カードがある場合は、その存在を定期的に確認すること。（管理部門）

■一般訪問者との面会
一般訪問者との面会や荷物受取等は、受付スペース、打合せスペースで行われなければならない。
■一般訪問者の入室手続及び識別
一般訪問者が執務スペースに立ち入る場合は、従業員は一般訪問者のみが執務スペースに居る状況をつくらないこと。

7.3　オフィス、部屋及び施設のセキュリティ

オフィス,部屋及び施設に対する物理的セキュリティを設計し,実装しなければならない。

・管理責任者は、セキュリティ境界に応じた物理的セキュリティを設計し、適用する。必要に応じて見直しを行う。

7.4　物理的セキュリティの監視

施設は,認可していない物理的アクセスについて継続的に監視しなければならない。

施設内のセキュリティエリアに侵入を防ぐため、警備会社が提供するセキュリティシステムを利用する。

7.5　物理的及び環境的脅威からの保護

自然災害及びその他の意図的又は意図的でない，インフラストラクチャに対する物理的脅威などの物理的及び環境的脅威に対する保護を設計し，実装しなければならない。

・会社施設は、火災、洪水、地震、その他の自然又は人為的災害による損害に対する物理的な保護を考慮し、適用すること。
■火災
・防火設備が整っていること、ビル管理の場合は適切なメンテナンスが行われているか確認する。
・自社管理の場合は、適切な消火設備の設置点検が行われているか確認する。
■洪水
・浸水等が少ない立地若しくは高層階であること。
■地震
・地震が少ない若しくは一定の耐震強度の建物であること。

7.6　セキュリティを保つべき領域での作業

セキュリティを保つべき領域での作業に関するセキュリティ対策を設計し，実施しなければならない。

■情報機器の安全管理
重要情報/個人情報が保存されている可般型の情報機器は、盗難防止措置を実施しなければならない。たとえば、鍵のかかる机・キャビネット、ワイヤーロック等に保管するものとする。

7.7　クリアデスク・クリアスクリーン

書類及び取外し可能な記憶媒体に対するクリアデスクの規則，並びに情報処理設備に対するクリアスクリーンの規則を定め，適切に実施させなければならない。

・帰宅時・出張時等長時間離席する場合は、クリアデスクを徹底すること。
・パーソナルコンピュータ等を使用中に離席する場合、必ずパスワード付きの画面ロックを行うものとする。
・ただしスクリーンセーバー10 分以内の設定でパスワードロックがかかるものを使用し、スクリーンセーバーの設定をしていれば、この限りでない。

7.8　装置の設置及び保護

装置は、セキュリティを保って設置し、保護しなければならない。

■情報関連機器の設置方法
情報関連機器の設置に関しては、各機器の推奨されている設置方法に従い正しく設置するものとする。設置時には、以下のことを考慮し、そのリスクが当社の定める基準内に収まるよう努める。
【考慮すべきリスク】
（1）窃盗
（2）地震・火災

（３）過度の発熱・煙
　　温度管理（エアコンの設置）
（４）水
（５）ほこり
（６）落下等による衝撃・振動
（７）化学物質
（８）電源障害
（９）電磁放射線
(10) 設置区域（認可されていないアクセス）
(11) その他、情報機器の動作に関わる機器の障害
(12) 損傷/傍受（LAN ケーブル等の損傷）
(13) 情報機器を会社施設外に持ち出す場合の盗難、損傷

7.9　構外にある資産のセキュリティ

構外にある資産を保護しなければならない。

・構外にある資産に対しては構外での作業に伴ったリスクを考慮し、セキュリティを適用する。

■携帯電話・スマートフォン
・緊急時を除き私用での通話は禁止する。
・盗難・紛失等を考慮し、パスワード設定等のセキュリティを設定することが望ましい。
・不特定多数の人間がいる場所（例：駅、公共の場所、レストラン等）での機密情報等の情報レベルが高い通話は禁止する。
・業務上やむを得ない場合を除き、携帯電話で業務用のメールを送受信しないこと。
・不特定多数の人がいる場所でチャットツールを使用する場合は、第三者にのぞき見をされないように工夫すること。
・USBでスマートフォンを会社のネットワークに接続しないこと。

■個人所有の携帯電話の取扱について
・盗難・紛失等を考慮し、パスワード設定等のセキュリティを設定することが望ましい。
・当社内でのカメラ付携帯電話のカメラ機能使用は禁止する。
・不特定多数の人間がいる場所（例：駅、公共の場所、レストラン等）での機密情報等の情報レベルが高い通話は禁止する。
・業務上やむを得ない場合を除き、携帯電話で業務用のメールを送受信しないこと。

7.10　記憶媒体

記憶媒体は,組織における分類体系及び取扱いの要求事項に従って,その取得,使用,移送及び廃棄のライフサイクルを通して管理しなければならない。

・ノート PC を持ち出す場合は、暗号化ソフト（BIOS パスワード、HDD 暗号化等）を導入しているノート PC のみ持出可能とし、管理責任者の承認後、PC 起動時のパスワード認証を必ず行う。
・記憶媒体の利用は責任権限に基づく許可のもとシステム管理者の承認を得て使用すること。

・記憶媒体による情報の移送が終了したら直ちにその内容物を削除または記憶媒体自体を物理的に処分しなければならない。
・HDD 及びサーバ―については、セキュリティに備えて物理的破壊または委託廃棄等を実施する。
・社外等で重要情報あるいはパーソナルコンピュータ、携帯電話、ノート PC 等（以下、PC 等）を取り扱う際には、下記の点に注意しなければならない。

（１）　社外等で取り扱う PC 等に、原則として会社の重要情報を保存しない。
（２）　社外でお客様から重要情報を授受する際は、お客様からの要望がある場合などには授受記録の取り交わしを行う。あるいは業務上の必要性において、社外等で重要情報や重要情報を含む PC 等を利用する場合は、下記の事項を遵守しなければならない。
（２）-1 重要情報及び PC 等は、第三者から目に付かないようにカバン等に保管すること。
（２）-2 付近に第三者がいる場合、重要情報及び PC 等が入っているカバン等を手から離さない。
（２）-3 重要情報及び PC 等が入っているカバン等は、容易にひったくり等にあわないようしっかり保持する。
（２）-4 電車内などでは、重要情報及び PC 等が入ったカバンを網棚には置かないようにすること。
（２）-5 重要情報及び PC 等を持って外出した場合は、社外での盗難、紛失などの事故を防止するため、出来る限り直接帰宅せず、社内に持ち帰ること。但し、業務上の必要により PC を持って直接帰宅する場合は、できる限り寄り道をせず帰宅しなければならない。
（２）-6 自動車内等に、重要情報及び PC 等を放置せず、自動車から離れる場合は、重要情報及び PC 等を身に付けて持ち出すようにしなければならない。
（２）-7 重要情報及び PC 等を取り扱う場合、第三者によって、重要情報や重要情報が盗み見等されないように、取扱い場所に十分な注意を払うこと。
（２）-8 社外で重要情報に関する会話をしなければならない場合は、第三者による盗み聞きを防止するため、周囲に第三者がいないことを確認すること。特に携帯電話での会話には注意すること。
（２）-9 PC 等の媒体に保存した重要情報を持ち歩く際には、落下等の衝撃による破損を防止するため、カバン等に入れ、落下等の衝撃を与えないよう注意すること。
（２）-10 カバン等に入れた重要情報及び PC 等が、風雨に遭った際に、水に濡れたりしないように注意を払うこと。
（２）-11 社外で重要情報等を閲覧する際に、風によって吹き飛ばされないよう、周囲の状況を確認してカバン等から取り出すこと。

（３）USB メモリ等の移動可能な記憶媒体による情報の授受は、会社支給による記憶媒体を利用しなければならない。なお、それらの記憶媒体による情報の移送が終了したら直ちにその内容物を削除または記憶媒体自体を物理的に破壊しなければならない。

7.11　サポートユーティリティ

情報処理施設・設備は,サポートユーティリティの不具合による,停電,その他の中断から保護しなければならない。

・システム管理者（管理責任者）は、情報関連機器の電源設備、空調設備など支援ユーティリティの不具合による、停電、その他の故障から保護する方策を立てること。

7.12　ケーブル配線のセキュリティ

電源ケーブル、データ伝送ケーブル又は情報サービスを支援するケーブルの配線は、傍受、妨害又は損傷から保護しなければならない。

・ケーブルは折れたり踏んだりできないよう保護を行う。

7.13　装置の保守

装置は,情報の可用性,完全性及び機密性を維持することを確実にするために,正しく保守しなければならない。

・情報関連機器の保守に関しては、継続的な可用性及び完全性の維持を可能とするため、各機器において推奨されている方法（マニュアル類）に従い正しく保守するものとする。
・装置の保守については、定期的に確認をすること。

7.14　装置のセキュリティを保った処分又は再利用

記憶媒体を内蔵した装置は,処分又は再利用する前に,全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること,又はセキュリティを保てるよう上書きしていることを確実にするために,検証しなければならない。

■情報関連機器の廃棄
・情報関連機器の廃棄に関しては、各機器の推奨されている方法に従い正しく廃棄するものとする。
・内部に情報又はアプリケーションが含まれている機器に関しては、情報やアプリケーションの復元が不可能な方法で情報を消去すること。

■情報関連機器の再利用
重要情報が保持されている情報関連機器を再利用する場合は、再利用の環境に応じて情報関連機器廃棄時と同様に、情報及びアプリケーションを復元不可能な状態にしなければならないものとする。

8　技術的管理策

8.1　利用者エンドポイント機器

利用者エンドポイント機器に保存されている情報,処理される情報,又は利用者エンドポイント機器を介してアクセス可能な情報を保護しなければならない。

・従業員は、書類やコンピュータ媒体について、非使用時や不在時、特に作業時間外には、施錠したキャビネットもしくは引き出し、または他のセキュリティが確保された保管庫に保管する。

8.2　特権的アクセス権

特権的アクセス権の割当て及び利用は、制限し、管理しなければならない。

・当社の情報システムまたはネットワークサービスに対する特権については、責任権限に基づく許可のもとシステム管理者が承認したもののみに与え、管理しなければならない。
・システム管理者が実施・管理する。

8.3　情報へのアクセス制限

情報及びその他の関連資産へのアクセスは、確立されたアクセス制御に関するトピック固有の方針に従って、制限しなければならない。

・情報及びアプリケーションシステム機能へのアクセスは、アクセス制御方針（5.1）に従って、各ファイルにアクセス制御を設定し、各個人ごとに責任権限に基づく許可のもとシステム管理者がアクセス権の付与を行う。必要最低限のアクセス設定を行うことにより不必要なアクセスを防ぐ。

8.4　ソースコードへのアクセス

ソースコード,開発ツール,及びソフトウェアライブラリへの読取り及び書込みアクセスを適切に管理しなければならない。

・システム開発専用のフォルダに管理し、（管理責任者と）開発者のみにアクセス権を付与し、必要最低限のものの利用、加工で済むようにする。

8.5　セキュリティを保った認証

セキュリティを保った認証技術及び手順を,情報へのアクセス制限,及びアクセス制御に関するトピック固有の方針に基づいて備えなければならない。

システム及びアプリケーションには ID、パスワードを設定し管理する。
・パスワードに関しては 8 文字以上に設定を行い、ID は他人に教えたりしないこととする。

8.6　容量・能力の管理

現在の及び予測される容量・能力の要求事項に合わせて、資源の利用を監視し、調整しなければならない。

・個別の情報システムにおいて、当該情報システムの主な管理担当者は、業務上の要求事項に基づく必要なシステム性能を確保するために、情報システムを監視し、将来必要とされる容量・能力を予測した計画を作成するものとする。

8.7　マルウェアに対する保護

マルウェアに対する保護を実施し,利用者の適切な認識によって支援しなければならない。

・使用するウィルス対策ソフト：ディフェンダー

・適用する機器：クライアントPC、サーバ、他

8.8　技術的ぜい弱性の管理

利用中の情報システムの技術的ぜい弱性に関する情報を獲得しなければならない。
また、そのようなぜい弱性に組織がさらされている状況を評価し、適切な手段をとらなければならない。

・利用中の情報システムに関係する技術的脆弱性に関する情報はシステム管理者が入手し、グループウェアの掲示板等で周知し、必要に応じて適切な処置を指示する。情報入手先は、OSはMicrosoft、その他は入手先とする。
・WindowsUpdateの運用：他のアプリケーションとの非互換が無い場合は自動取得
・ウィルス対策ソフトのパターンファイルは常に最新になるようにサポート切れのソフトウェア（OS 含む）の運用は禁止とする。他のシステムとの互換等やむを得ず使用する場合は外部ネットワークからの遮断等、適切なセキュリティ対策を施し使用する。

8.9　構成管理

ハードウェア,ソフトウェア,サービス及びネットワークのセキュリティ構成を含む構成を確立し,文書化し,実装し,監視し,レビューしなければならない。

・利用するハードウェア、ソフトウェア、サービスについて、「情報資産リスクアセスメント表」にて管理する。
・ネットワークのセキュリティついて、「ネットワーク構成図」にて管理する。

8.10　情報の削除

情報システム,装置又はその他の記憶媒体に保存している情報は,必要でなくなった時点で削除しなければならない。

・情報機器に保存する情報について、削除すべき情報を識別し、必要ではなくなった時点で削除すること。

8.11　データマスキング

データマスキングは,適用される法令を考慮して,組織のアクセス制御に関するトピック固有の方針及びその他の関連するトピック固有の方針,並びに事業上の要求事項に従って利用しなければならない。

・組織での情報利用時には、社内外に情報公開、提供する場合に個人情報や機密情報に関連する項目をダミーデータに変更すること。
・ソフト開発会社がテスト用に情報を受け取る場合は提供される会社に対して、マスキングを要求すること。
・マスキングされていないデータが来た場合は、拒否するか、セキュリティを守ったうえで受け取った側がマスキングをすること。

8.12　データ漏洩の防止

データ漏えい防止対策を,取扱いに慎重を要する情報を処理,保存又は送信するシステム,ネットワーク及びその他の装置に適用しなければならない。

・機密情報を保存している情報機器には、ウイルスソフトの導入等でデータの漏洩を防止する。
・アクセス権を設定する。

8.13　情報のバックアップ

合意されたバックアップに関するトピック固有の方針に従って,情報,ソフトウェア及びシステムのバックアップを維持し,定期的に検査しなければならない。

・管理責任者は、情報資産が保存されているサーバについて、合意されたバックアップ方針として以下に定める。
・バックアップ方針の内容は、システム管理者、管理責任者が、各リスク所有者に確認して合意をとること。

8.14　情報処理施設・設備の冗長性

情報処理施設・設備は,可用性の要求事項を満たすのに十分な冗長性をもって,導入しなければならない。

・情報処理施設・設備は、可用性の要求事項を満たすのに十分な冗長性をもって、導入しなければならない。

8.15　ログ取得

活動、例外処理、過失及びその他の関連する事象を記録したログを取得し、保存し、保護し、分析しなければならない。

・システム管理者、管理責任者は、情報システムについて、利用者の行動、例外事項、情報セキュリティ事象を記録した監査ログを取得し、将来の調査及びアクセス制御の監視を補うために、3ヶ月以上保存すること。
・システム管理者は、ログ機能及びログ情報を改ざん及び認可されていない
アクセスから保護するため、ログ情報を保護しなければならない。
・責任権限に基づく許可のもとシステム管理者及びサーバの作業担当者は、以下の内容のログを記録すること。また、作業ログについては定期的にレビューするものとする。

8.16　監視活動

情報セキュリティインシデントの可能性を評価するために,ネットワーク,システム及びアプリケーションについて異常な挙動がないか監視し,適切な処置を講じなければならない。

・アラートを出してくれるツール（情報資産管理ソフト、EPP）にて監視を行う
・当社で利用しているネットワーク、システムおよびアプリケーションについて、異常事態が発生していないか適宜ログを確認すること。

・アクセスログを取得・監視する（外部・内部）
・システムの稼働状況、ユーザー数

8.17　クロックの同期

組織が利用する情報処理システムのクロックは、組織が採用した時刻源と同期させなければならない。

・責任権限に基づく許可のもとシステム管理者（情報システム部）は、当社のサーバについて、その時刻を外部のタイムサーバと同期をとるものとする。さらに各情報端末は、当社のサーバと時刻の同期をとるものとする。
・外部ネットワークに接続できる機器は自動的にクロック取得できる状態を維持する。

8.18　特権的なユーティリティプログラムの使用

システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理しなければならない。

・特権的なユーティリティプログラム（オペレーティングシステムのチューニングプログラム、ネットワーク監視、制御プログラム　等）において、システム稼働に大きく影響を与えるプログラムは、　使用者の限定（システム管理者、管理責任者等）、使用の管理（申請許可）を厳格に行うこと。

8.19　運用システムへのソフトウェアの導入

運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順及び対策を実施しなければならない。

・市販ソフトウェアパッケージ製品は、システム管理者が管理する。
・運用に当たっては、事前に受け入れテストを行い問題がないことを確認できたことをシステム管理者が判断して使用する。
・フリーウェアを自己判断でインストールしてはならない。
・フリーウェアの導入は、システム管理者・管理責任者の許可・ホワイトリストの運用により管理する。

8.20　ネットワークセキュリティ

システム及びアプリケーション内の情報を保護するために,ネットワーク及びネットワーク装置のセキュリティを保ち,管理し,制御しなければならない。

・システム内の情報を保護するために、以下の手順でネットワークを管理し、制御する。
・ネットワーク全体のログの取得
・リスクに応じたネットワーク保護機器の選定・導入・保全維持（ファイアウォール、UTM 等の導入）

8.21　ネットワークサービスのセキュリティ

ネットワークサービスのセキュリティ機能,サービスレベル及びサービスの要求事項を特定し,実装し,監視しなければならない。

・外部組織が提供するネットワークサービスを利用する場合は、業務委託管理の定めに従いネットワークサービスを選定すること。
・使用するネットワークサービス（クラウドサービス）はネットワーク図に明示すること。
・使用するネットワークサービスの使用目的を明確にし、「情報資産リスクアセスメント表」との整合をとること。

8.22　ネットワークの分離

情報サービス、利用者及び情報システムは、組織のネットワーク上で、グループごとに分離しなければならない。

・社内 LAN、DMZ、インターネットという区分けでネットワークを分離し、それに応じた管理策を講じる。（分離している目的を明確にすること）
・分離された状態をネットワーク図上に明確化する。

8.23　ウェブフィルタリング

悪意のあるコンテンツにさらされることを減らすために,外部ウェブサイトへのアクセスを管理しなければならない。

・社内の PC にはウェブフィルタリングを設定し、制限すること。
・プロバイダーを設定し、制限すること。
・社内あるいはデータセンターに置いたネットワークサーバかクラウドサービスを全面利用しているか　で対策が変わってくる

8.24　暗号の利用

暗号鍵の管理を含む,暗号の効果的な利用のための規則を定め,実施しなければならない。

・インターネットで重要情報の送信をする場合には、SSL 等の秘匿化された通信経路を利用すること。
・無線 LAN を使用する場合は、WPA2 以上の暗号化をするものとする。

・Web アプリケーション等で、暗号化通信が必要な場合は、暗号プロトコルを適切に選択、採用、運用すること。
・暗号鍵を応用するアプリケーションの開発、運用時には、適切な鍵管理ができるように留意する。SSL/TLS（通信の暗号化）などの標準的なセキュリティプロトコルを活用すること。

8.25　セキュリティに配慮した開発のライフサイクル

ソフトウェア及びシステムのセキュリティに配慮した開発のための規則を確立し,適用しなければならない。

・ソフトウェア及びシステムの開発のための規則は、組織内において本マニュアルに確立し、開発に対して適用する。

8.26　アプリケーションセキュリティの要求事項

アプリケーションを開発又は取得する場合,情報セキュリティ要求事項を特定し,規定し,承認しなければならない。

・公衆ネットワーク上におけるセキュリティを、不正行為および認可のない開示・変更要求から保護するものとする。
■アプリケーションサービスの実施者
・通信上のセキュリティ（認証、経路、データ保護トランザクション管理）
■アプリケーションサービスの使用者
・サービス事業者の安全性（上記確認：SLA 等）

・アプリケーションサービスのトランザクションに含まれる情報を、未然の対策により、不完全な通信経路および認可のない開示等から保護するものとする。
・通信プロトコルの管理（タイムアウト、切断時の復旧）
・電子署名
・暗号化等による管理

8.27　セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則

セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの開発活動に対して適用しなければならない。

・セキュリティに配慮したシステムを構築するための原則を本マニュアルに確立し、文書化し維持し、全ての情報システムの実装に対して適用する。
・　8.25 参照

8.28　セキュリティに配慮したコーディング

セキュリティに配慮したコーディングの原則をソフトウェア開発に適用しなければならない。

・当社はセキュリティに配慮されたフレームワークを使用すること。

8.29　開発及び受入れにおけるセキュリティテスト

セキュリティテストのプロセスを開発のライフサイクルにおいて定め,実施しなければならない。

・セキュリティ機能の試験は、システム開発の試験要件に取り込むこと。

・単体テスト、結合テスト、システムテスト、運用テストすべての工程で行う。

・新しい情報システム、改訂版及び更新版を受け入れる際は、責任権限に基づく許可のもとシステム管理者（情報システム部）の指示により、当該情報システムの主な管理担当者は、業務上の要求事項を明確にした受け入れ基準を確立し、その基準に基づき受け入れ前に適切な試験を実施する。あるいは、新規または改訂版、更新版の情報システムが受け入れ基準を満たしていることを確認すること。

8.30　外部委託による開発

組織は、外部委託したシステム開発に関する活動を指揮し,監視し,レビューしなければならない。

・業務用システムの開発を外部委託する場合は、「5.20 供給者との合意におけるセキュリティの取扱い」に従い、業務委託を行うこと。

8.31　開発環境,テスト環境及び本番環境の分離

開発環境、テスト環境及び本番環境は、分離してセキュリティを保たなければならない。

・試験設備は、運用設備から分離し、社内において顧客環境を設定する場合は、社内のネットワークとは分離した環境で行うこと。

・全てのシステム開発ライフサイクルを含む、システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し、適切に保護する。
・開発プロジェクトの機密性に応じた開発環境を整備すること

8.32　変更管理

情報処理設備及び情報システムの変更は、変更管理手順に従わなければならない。

・情報処理設備及び情報システムを変更する際は、これを明確にし、管理責任者が全ての関係者に周知させるものとする。
・情報処理設備及び情報システムを変更する際は、変更計画のもと、管理された状態で実施すること。管理された状態とは下記を指す。
- ・システム変更の内容の具体化
- ・システム変更に関する責任権限
- ・申請及び許可
- ・実施前の技術的検証
- ・実施後の技術的検証
- ・これらの文書化された情報の整備

・業務用システムを変更する際、管理責任者は、業務用システムの変更に関する要求事項を明確にし、各部門責任者と管理責任者の承認を得て、その変更内容を記録し、その変更の実施を適切に管理するものとする。
・システム変更依頼書、変更仕様書等の使用による管理をおこなう
・システム変更による既存システムへの影響を分析し、対応する。

・オペレーティングプラットフォーム（主にオペレーティングシステム）を変更する際、当該オペレーティングシステム上で運用されている業務用システムの運用又はセキュリティに悪影響がないことを確実にするために、重要な業務用システムについては、システム管理者は一定期間の情報を収集し、適用試験等の検証を実施し、記録しなければならない。

・パッケージソフトウェアの変更は原則として行わない
・変更が必要となる場合は、それに伴うリスクを考慮し、その実施は、システム管理者・管理責任者の承認する内容で試験を行ったうえで、管理責任者の管理のもと行わなければならない。

8.33　テスト用情報

テスト用情報は、適切に選定し、保護し、管理しなければならない。

・プログラムソースコード及び試験データ等については、システム開発責任者が当社のアクセス制御方針に基づき、適切なアクセス権を利用者に付与し、適切に保護および管理するものとする。
・試験データは、原則としてダミーデータを使用すること。ダミーデータはシステム試験の要件を満たすが業務実態上意味のないデータにすること。
・既存システム等の本番データを試験データに使用する場合は、適切なマスキングを実施すること。

8.34　監査におけるテスト中の情報システムの保護

運用システムのアセスメントを伴う監査におけるテスト及びその他の保証活動を計画し，テスト実施者と適切な管理層との間で合意しなければならない。

・システムへのアクセスに関する監査は、適切な管理層の承諾を得る。
・システムの可用性に影響を及ぼす監査内容の場合は、業務時間外に実施する。