
株式会社ソラスト

情報セキュリティ対策基準

目次

1章	はじめに	6
1.1	背景	6
1.2	本書の位置づけ	6
1.3	本書の記載方法	6
1.4	用語の定義	6
2章	組織的管理策	8
2.1	情報セキュリティのための方針群	8
2.2	情報セキュリティの役割および責任	8
2.3	職務の分離	9
2.4	管理層の責任	9
2.5	関係当局との連絡	10
2.6	専門組織との連絡	10
2.7	脅威インテリジェンス	11
2.8	プロジェクトマネジメントにおける情報セキュリティ	11
2.9	情報およびその他の関連資産の目録	11
2.10	情報およびその他の関連資産の許容される利用	12
2.11	資産の返却	12
2.12	情報の分類	13
2.13	情報のラベル付け	13
2.14	情報転送	14
2.15	アクセス制御	15

2. 16	識別情報の管理	16
2. 17	認証情報	16
2. 18	アクセス権	17
2. 19	調達製品サービスや委託先の情報セキュリティ対策の評価と管理	17
2. 20	情報セキュリティ要求事項に基づく外部委託契約	18
2. 21	製品サービスの選定や調達における情報セキュリティの管理	18
2. 22	調達製品サービスや委託先サービスの監視、レビューおよび変更管理	19
2. 23	クラウドサービスの利用における情報セキュリティ	19
2. 24	情報セキュリティインシデント管理の計画策定および準備	20
2. 25	情報セキュリティ事象の評価および決定	21
2. 26	情報セキュリティインシデントへの対応	22
2. 27	情報セキュリティインシデントからの学習	22
2. 28	証拠の収集	22
2. 29	事業の中断・阻害時の情報セキュリティ	22
2. 30	事業継続のための ICT の備え	23
2. 31	法令、規制および契約上の要求事項	23
2. 32	知的財産権	23
2. 33	記録の保護	23
2. 34	プライバシーおよび個人を特定できる情報(PII)の保護	23
2. 35	情報セキュリティの独立したレビュー	23
2. 36	情報セキュリティのための方針群、規則および標準の順守	24
2. 37	操作手順書	24
3章	人的管理策	25
3. 1	選考	25
3. 2	雇用条件	25
3. 3	情報セキュリティの意識向上、教育および訓練	25
3. 4	懲戒手続き	26

3.5	雇用の終了または変更後の責任	26
3.6	秘密保持契約または守秘義務契約	26
3.7	リモートワーク	26
3.8	情報セキュリティ事象の報告	27
4章	物理的管理策	28
4.1	物理的セキュリティ境界	28
4.2	物理的入退	29
4.3	オフィス、部屋および施設のセキュリティ	30
4.4	物理的セキュリティの監視	30
4.5	物理的および環境的脅威からの保護	30
4.6	セキュリティを保つべき領域での作業	30
4.7	クリアデスク・クリアスクリーン	31
4.8	装置の設置および保護	31
4.9	構外にある資産のセキュリティ	31
4.10	記憶媒体	32
4.11	サポートユーティリティ	32
4.12	ケーブル配線のセキュリティ	33
4.13	装置の保守	33
4.14	装置のセキュリティを保った処分または再利用	33
5章	技術的管理策	34
5.1	利用者端末	34
5.2	特権的アクセス権	35
5.3	情報へのアクセス制限	35
5.4	ソースコードへのアクセス	35
5.5	セキュリティを保った認証	35
5.6	容量・能力の管理	36
5.7	マルウェアに対する保護	36

5. 8	技術的脆弱性の管理.....	37
5. 9	構成管理	37
5. 10	情報の削除	37
5. 11	データマスキング.....	37
5. 12	データ漏洩防止	37
5. 13	情報のバックアップ	37
5. 14	情報処理施設・設備の冗長性	38
5. 15	ログ取得.....	38
5. 16	監視活動.....	39
5. 17	クロックの同期	39
5. 18	特権的なユーティリティプログラムの使用	39
5. 19	運用システムへのソフトウェアの導入.....	39
5. 20	ネットワークセキュリティ.....	39
5. 21	ネットワークサービスのセキュリティ	39
5. 22	ネットワークのアクセス制御	40
5. 23	ウェブフィルタリング	40
5. 24	暗号の利用	40
5. 25	セキュリティに配慮した開発のライフサイクル	40
5. 26	アプリケーションセキュリティの要求事項.....	41
5. 27	セキュリティに配慮したシステムアーキテクチャおよびシステム構築の原則	42
5. 28	セキュリティに配慮したコーディング	42
5. 29	開発および受入れにおけるセキュリティテスト	42
5. 30	外部委託による開発	42
5. 31	開発環境、テスト環境および本番環境の分離.....	42
5. 32	変更管理.....	43
5. 33	テスト用情報.....	43
5. 34	監査におけるテスト中の情報システムの保護.....	43

【 改版履歴 】

版数	発行日	改訂者	改訂内容・理由	箇所
1.0.0	2024/4/1		初版	

1	はじめに	発行日	2024.04.01
適用範囲	全社・全従業員		

1章 はじめに

1.1 背景

本書は、株式会社ソラストの情報セキュリティマネジメントシステムを運用するために記述した文書（以下「本書」と記す）である。

なお、医療業務（医療情報を扱う場合）は本書に記載の対策に加え、厚生労働省が策定する「医療情報システムの安全管理に関するガイドライン」の最新版の対策に対応する。

1.2 本書の位置づけ

本書は、ドキュメント体系における上位規程の情報セキュリティ規程（管理策編）の下位文書に相当する。

1.3 本書の記載方法

本書は、当社の情報セキュリティ規程（管理策編）で定義される「組織的管理策」「人的管理策」「物理的管理策」「技術的管理策」の順で記載し、各管理策の具体的な対応方法を示したものである。

なお、本書内で登場する【重要度：高】が記載された対策は、重要度「高」を扱う場合は必須とし、それ以外の場合は任意とする。

1.4 用語の定義

用語は、引用する規格の用語に従うが、下記の定義を追加する。

No.	用語	用語の意味
1	ISMS	情報セキュリティマネジメントシステム（InformationSecurityManagementSystem）の略。
2	情報セキュリティインシデント	望まないまたは予期しない単独または一連の情報セキュリティ事象であって、事業運営を危うくする確率、および情報セキュリティを脅かす確率が高いもの [ISO/IECTR18044:2004]
3	リスク	組織活動の目的から好ましくない方向※に乖離する可能性があること（※：定義上は、より好ましい方向に乖離する可能性も含む） 実際には、組織の目的遂行を阻害する事象発生の可能性や、事象が発生した際に被る損失等で表す
4	情報資産	組織にとって価値があり、適切な保護（セキュリティ対策）が必要な、情報やシステム、組織の構成員など

5	脅威	情報セキュリティインシデントを、引き起こす直接の原因となりうるもの
6	脆弱性	情報資産に脅威が加えられたとき、情報セキュリティインシデントを起こしやすくと考えられる弱点
7	CISO	情報セキュリティの総責任者（CISO）、通常は代表取締役が担当する CISO:ChiefInformationSecurityOfficer の略。
8	研修	各種教育・訓練・社内外のセミナー・防災訓練・他
9	要員	組織の指示の下で仕事をしている人々
10	従業員	社員、嘱託、パート、アルバイト、など、会社と直接雇用の関係にある会社業務の従事者の総称
11	社員	（各社の定義とする）
12	契約社員	（各社の定義とする）
13	派遣社員	社員以外で、社外から派遣されて会社業務に従事する者の総称
14	協力会社社員	社員以外で、会社の業務の一部または全ての従事し、その遂行を支援する会社社員の総称
15	供給者	自社の情報セキュリティマネジメントシステムに対し、サービスを提供している会社や委託先の総称
16	サプライチェーン	供給者からの委託先（再委託先）や ICT 機器部品の調達先の総称
17	顧客（第三者）	会社の業務・サービス・商品等を提供する法人または個人の総称
18	資産	組織にとって価値をもつもの。 会社が守るべき人的資産、物理的資産、NW・情報システム資産、情報資産の全て
19	利用者エンドポイント機器	ネットワークに接続されている終端機器の総称 各種サーバの他、社内で利用するパソコン類やプリンター、社外で利用する携帯電話、スマートフォン、タブレット等が該当
20	MDM サービス	MDM は（Mobile Device Management）の略。 組織や企業が従業員のモバイルデバイスを遠隔で管理し、セキュリティポリシーやアプリケーションの配布、データの保護、デバイスの追跡などを行うことができるサービス
21	記憶媒体	HD・FD・MO・CD・DVD、USB メモリなど、電子化情報を格納・保持できる機器（パソコン類は除く）
22	内部監査	情報セキュリティマネジメントシステムに対して自社で実施する監査
23	部門	会社の部、チーム、の総称
24	部門長	部門の最高責任者
25	利害関係者	顧客、社員、利用者、協力会社社員、派遣社員、監督官庁、業界団体、株主、ビルオーナー、組合、周辺住民、NGO など

2	組織的管理策	発行日	2024.04.01
適用範囲	全社・全従業員		

2章 組織的管理策

2. 1 情報セキュリティのための方針群

- 経営者は、情報セキュリティ基本方針を定義する。また、情報セキュリティ責任者は年度目標およびその他の方針群を定義する。

＜方針群の例＞

アクセス制御方針、バックアップ方針

- 情報セキュリティ責任者は、定義された情報セキュリティ基本方針、年度目標およびその他の方針群を、情報セキュリティ委員会で承認を得る。
- 情報セキュリティ責任者は、従業員に情報セキュリティ基本方針、年度目標およびその他の方針群を情報セキュリティ委員会からの周知や社内ホームページを通じて認識させる。必要に応じて、社外ホームページで外部関係者にも通知する。
- 経営者および情報セキュリティ責任者は、情報セキュリティ基本方針、年度目標およびその他の方針群を、定期的（年1回以上）に見直しをする。
変更の必要性が生じた場合（経営に影響を与えるセキュリティ事件・事故）は情報セキュリティ委員会の承認を得る。

2. 2 情報セキュリティの役割および責任

- 経営者は、情報セキュリティ体制を下表に基づき割当て、資産に対する保護責任者や特定の業務（資産の管理、事業継続）に対する実施責任者およびそれぞれの責任範囲を情報セキュリティ体制図で明確にする。
なお、組織・システム・ネットワーク毎の詳細な体制は、情報セキュリティ体制図で明確にする。

役職名	役割と責任
情報セキュリティ責任者 (CISO)	情報セキュリティに関する責任者。情報セキュリティ対策などの決定権限を有するとともに、全責任を負う。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者。各部門における情報セキュリティ対策の実施などの責任を負う。
情報システム部門	社内の情報システムに必要な情報セキュリティ対策の検討・導入を行う。
ネットワーク管理者	社内のネットワークに必要な情報セキュリティ対策の検討・導入を行う。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施する。
インシデント対応責任者	事故の影響を判断し、対応について意思決定する。
個人情報保護管理者	個人情報の取扱いについて関連法令を遵守する責任を負う。
監査責任者	情報セキュリティ対策が適切に実施されているか情報セキュリティ関連規程を基準として検証または評価し、助言を行う。
復旧責任者	自然災害やサイバー攻撃を含む情報セキュリティインシデントが発生した際に、事業継続計画に則りサービスやシステムの復旧を行う。

2.3 職務の分離

- 不正行為が容易にできないように、アクセス権等の要求、承認、実施を行う担当を分離する。
- システム運用を安定的に運用するために、システム運用管理者とシステム運用実施の職務を分離する。

2.4 管理層の責任

- 管理層は、正社員および契約社員に情報セキュリティ方針、情報セキュリティ目標およびセキュリティルールを社内ホームページ等で公表・周知し、遵守を指導する。

2. 5 関係当局との連絡

- 情報セキュリティ責任者または情報セキュリティ部門責任者は、セキュリティ事件・事故の場合、適切な処置が取れるよう下表に示す行政機関、規制機関、情報サービス提供者および通信業者との連絡体制を構築する。具体的な連絡先等は一覧にまとめる。(外部コミュニケーション一覧等)

名称	連絡内容
内閣府	認定こども園業務受託による、行政上必要とされる報告
厚生労働省	医療・介護業務および保育園業務受託による、行政上必要とされる報告
文部科学省	幼稚園業務受託による、行政上必要とされる報告
総務省	医療業務受託による、行政上必要とされる報告
経済産業省	医療業務受託による、行政上必要とされる報告
個人情報保護委員会	個人情報の漏洩等、個人情報に関するインシデントの報告
警察署	情報セキュリティ施設への侵入等、情報セキュリティ事件・事故の通報
消防署	情報セキュリティ施設が火災や要員の怪我・病気等の救急連絡
電気事業者	情報セキュリティ施設・設備への電気の供給に関する問い合わせ
電気通信事業者	ネットワーク経路等、通信状況の問い合わせ
水道局	装置の冷却用設備に対する冷却水供給に関する問い合わせ

2. 6 専門組織との連絡

- 情報セキュリティ責任者または情報セキュリティ部門責任者は、必要に応じて、社内や下表に示す社外の情報セキュリティ専門家による助言を求める。組織全体の調整方法は、情報セキュリティ委員会を利用して調整する。具体的な連絡先等は一覧にまとめる。(外部コミュニケーション一覧等)

名称	連絡内容
独立行政法人情報処理推進機構（IPA）	技術的な内容も含め、情報セキュリティに関する相談全般
一般社団法人 JPCER コーディネーションセンター（JPCERT/CC）	インターネットを介して発生する侵入やサービス妨害等のインシデントについて、日本国内に関するインシデント等の報告受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言
一般財団法人日本情報経済社会推進協会（JIPDEC）	個人情報の漏洩等、個人情報に関するインシデントの報告、個人情報保護に関する好事例の入手
セキュリティベンダ	システムの脆弱性やウイルス対策ソフトウェアの更新情報の入手、インシデント発生時のフォレンジック調査

2. 7 脅威インテリジェンス

- 情報セキュリティ責任者は、2.5（関係当局との連絡）や2.6（専門組織との連絡）に示す外部組織や情報セキュリティ委員会等の内部組織から脅威情報を収集する。
- 情報セキュリティ責任者は、収集した脅威情報が組織に与える影響範囲を分析する。
- 情報セキュリティ責任者は、分析した脅威情報をもとに、必要に応じて関連要員に伝達、対応する。

2. 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

- 情報セキュリティ部門責任者は、プロジェクト計画で、顧客からの情報セキュリティ要求事項について明確にする。

＜顧客からの情報セキュリティ要求事項例＞

- － 機密保持・守秘義務の定義や年数
 - － 個人情報保護法の遵守
 - － 知的財産権に関する合意
- 新規システムまたは既存システム改善に関する業務を実施する場合、システム上のセキュリティ要求事項をプロジェクト計画で明確にする。

＜システム上のセキュリティ要求事項例＞

- － 機密保持・守秘義務の定義や年数
- － 個人情報保護法の遵守
- － 知的財産権に関する合意
- － 業務・サービスクラウドサービス含む外部委託先、供給者等のセキュリティレベル、再委託に関する制限事項、対策・手順等仕様、サービスレベル等

2. 9 情報およびその他の関連資産の目録

- 情報セキュリティ部門責任者は、資産（公開されている情報を除く人的資産・物理的資産・情報資産）について目録を作成する。（「従業員名簿」「物品管理簿（固定資産、小額償却資産、レンタル、リースを含む）」「文書管理簿」「記録管理簿」「顧客支給品管理簿」「情報資産台帳」等）
- 資産が追加、変更、削除された場合、資産目録を更新する。
- 資産目録台帳には、情報・資産の管理責任者（保有者）を記載する。また、ネットワーク・システム等については、ネットワーク管理者、情報システム部門、執務室の管理責任者など、管理責任を有する者を明確に指定する。

2. 10 情報およびその他の関連資産の許容される利用

- 情報に守秘区分を表示することにより利用範囲を明確にする。
- 社内ネットワーク、社内情報システムの利用範囲を利用資格(アクセス権限)の付与基準により明確にする。

<利用資格(アクセス権限)の付与基準>

利用者 NW・システム	従業員		派遣社員	協力会社社員	顧客
	社員	契約社員			
本社、事業所、データセンターなどの全社共通ネットワーク	全て		一部（必要に応じて）		付与しない
特定組織固有のシステム・サービス			一部（必要に応じて）		付与しない
顧客に提供するシステム・サービス			一部（必要に応じて）		全て
上記以外、社外のネットワーク・システム			付与しない (情報資産を社外に持ち出ししない)		付与しない

- 建物、執務室への利用範囲を情報セキュリティ区画図により明確にする。原則、社外には情報を持ち出さない。
- 分類した情報を、守秘区分に従って、扱う。

2. 11 資産の返却

- 正社員、契約社員、派遣社員および協力会社社員は、雇用変更／終了時、契約変更／終了時または合意の変更／終了時に返却または廃棄をする。
- 第三者が返却または廃棄が確実に実施されたことを確認し、記録を残す。(情報資産返却台帳等)

2. 12 情報の分類

- 下表に示す、機密性・完全性・可用性を考慮した分類基準を定める。

<分類基準例>

	機密性 (C) 観点の重要度	完全性 (I) 観点の重要度	可用性 (A) 観点の重要度
重要度: 「高」	情報漏洩等が発生した場合、顧客、社会や事業に重大な影響が及ぶ恐れがある。 例) 医療業務情報、個人情報、営業秘密、機密情報。	改ざんまたは破壊が発生した場合、顧客、社会や事業に重大な影響が及ぶ恐れがある。 例) 請求にかかわる情報、財務情報。	アクセス不可または使用できない状態が発生した場合、顧客、社会や事業に重大な影響が及ぶ恐れがある。 例) 1時間以上のアクセスまたは使用不可状態が許容できない情報。
重要度: 「中」	情報漏洩等が発生した場合、顧客、社会や事業に影響が及ぶ恐れがある。 例) 会社情報、設備情報など社外秘情報。	改ざんまたは破壊が発生した場合、顧客、社会や事業に影響が及ぶ恐れがある。 例) 経営情報、顧客情報。	アクセス不可または使用できない状態が発生した場合、顧客、社会や事業に影響が及ぶ恐れがある。 例) 1日以上アクセスまたは使用不可状態が許容できない情報。
重要度: 「低」	情報漏洩等が発生した場合でも、顧客、社会や事業に影響が及ぶ恐れが少ない。 例) 漏洩しても影響が少ない社内情報。	改ざんおよび破壊が発生した場合でも、顧客、社会や事業に影響が及ぶ恐れが少ない。 例) 改ざんされても影響が少ない社内情報。	アクセス不可または使用できない状態が発生した場合でも、顧客、社会や事業に影響が及ぶ恐れが少ない。 例) 1週間以上のアクセスまたは使用不可状態が許容できない情報。

2. 13 情報のラベル付け

- 電子データや紙媒体、記録媒体については、重要度を識別・伝達できるよう管理することを推奨する。以下に例を示す。
 - システム一覧において、保有している情報の重要度を示す
 - 電子ファイルをファイルサーバやクラウドに格納する場合は、フォルダやファイル名に重要度を示すラベル付けするか、情報を格納しているフォルダの一覧をアクセス容易な場所に示す。

-
-
- － 紙媒体や記録媒体は、保管場所を記載した一覧をアクセス容易な場所に示す。もしくは媒体や保管場所に重要度を示すラベルを貼る。

2. 14 情報転送

＜メール利用時＞

- 電子メールを送信する際は、送信前に必ず宛先と本文を確認する。
- 添付ファイルの内容を確認してから、メール送信する。
- メーリングリストのメンバを定期的に見直す。
- メール自動転送は原則禁止する。
- 業務でクラウド型メールは原則、利用禁止とする。利用する場合は、情報システム部門の許可を得る。

【重要度「高」(機密性)】

- 会社から許可された端末以外で、重要度「高」のメールや情報の閲覧を禁止する。
- 重要度「高」の情報資産を送信する場合は、メール本文には記載しない。
- 重要度「高」の情報を他社(取引先等)とメールで交換をする場合は、送受信メールの管理、メールを受信したことを通知する方法等を決め、あらかじめ合意する。
- メールを利用する上で以下の事項は禁止する。
 - － 業務に支障をきたすおそれがある使用。
 - － 私用電子メールサーバへの接続。
 - － 私用メールアドレスへの転送。

＜物理的媒体の輸送時＞

- 配送業者を利用して記録媒体を配送する場合は、信頼でき、物理的損傷から保護するのに十分な梱包をする業者を選定する。
- 自分で記録媒体を運ぶ場合は、物理的損傷から保護するのに十分な梱包をする。

【重要度「高」(機密性)】

- 紙媒体の個人情報情報を同一建物外に配送する場合は、配達状況が追跡可能で厳重に取扱われる方法で送る。
- 電子媒体の個人情報情報を可搬記録媒体に格納して同一建物外に配送する場合は、電子ファイルを暗号化あるいはパスワード付与して、配達状況が追跡可能で厳重に取扱われる方法で送る。

＜FAX 利用時＞

- FAX の出力用紙を放置しない。
- FAX 送信時は送信先 FAX 番号が正しいことを確認する。(複数名でのダブルチェックを推奨)

【重要度「高」(機密性)】

- FAX 送信する場合は、電話で受信確認を行う。

＜ソーシャルメディア利用時＞

-
- 従業員が業務上、ソーシャルメディア（テレビや新聞等のメディアを含む）に情報を発信する際は、事前に広報・IR 部にその旨を通知し、承諾を得なければならない。またその際は、会社について語ることや自身の発信の影響度を十分理解するとともに、その最終的な責任は企業として会社が負わなければならないことを認識する。
 - 従業員は、業務上(公式アカウント)で facebook、Instagram、YouTube、tiktok、X 等のソーシャルメディアを利用する場合、以下に掲げる事項を理解し、遵守する
 - － 公式アカウントを開設する際は、「ソーシャルメディア利用マニュアル」を一読し、ソラフローより申請。広報課による最終審査後に開設できるものとする
 - － 職務上知り得た秘密（会社外部の人に公開されていない情報）は投稿しない
 - － 会社の従業員として自覚と責任を持って発信をする
 - － 適切なマナーを心掛け、誹謗中傷や第三者の権利を侵害する情報の発信は避け、他人を尊重する発信をする。また、政治的、宗教的な発信も行わない
 - － 発信した情報が長期間公開されること、および瞬時に拡散し得ることがあること等を理解し、発信する情報の内容を慎重に吟味する
 - 従業員は、個人でソーシャルメディアを利用する場合は、原則会社に関連した発信をしてはならない。もし偶発的に配信された場合には、その事実を遅滞なく広報・IR 部に報告する。

<電子署名>

- 法令で署名または記名・押印が義務付けられた文書において、記名・押印を電子署名に代える場合、法令に準拠した条件を満たす電子署名を行う。
- 法定保存期間等の必要な期間、電子署名の検証を継続して行うことができるよう、必要に応じて電子署名を含む文書全体にタイムスタンプを付与する。
- 電子署名に用いる秘密鍵の管理が、認証局が定める「証明書ポリシー」（CP）等で定める鍵の管理の要件を満たして行う。

<その他>

- 公共の場（ビル共用部、エレベータ内等）で、業務に関する話をしない。
- 他社（協力会社や取引会社）とソフトウェアを交換する場合は、必要に応じてソフトウェア交換に関する正式な契約を結ぶ
- 誰でも使える外部サービス（例えば、インスタントメッセージ、ソーシャルネットワーク、ファイル共有またはクラウドストレージ）を利用する際は、事前に上長と情報システム部門の承認を得る。

2. 15 アクセス制御

- 情報セキュリティ責任者は、業務上および関連法規上の物理的・論理的アクセス制御に関する要求事項を定義し、アクセス制御規程を策定する。

<アクセス制御規程に記載する項目例>

- － アクセス制御方針

-
- 利用者アカウントの発行および管理
 - パスワードの設定
 - ゲストアカウントの発行および管理
- ネットワークの利用規程を定める。
＜ネットワークの利用規程に記載する項目例＞
 - 認可手順
 - 利用制限
 - 管理体制
 - 管理手順
 - トラブル発生時の対応

2. 16 識別情報の管理

- 全社共通のネットワーク・システム等、複数人が利用する情報システムおよびサービスにアクセスする場合は、管理者から承認を得る。
- 全社共通のネットワーク・システム等、複数人が利用する情報システムおよびサービスには、アクセス申請・削除・変更の手順を定める。
- 全社共通のネットワーク・システム等、複数人が利用する情報システムおよびサービスのユーザIDは、一意なものを付与する。

2. 17 認証情報

＜システム利用者向け＞

- システム利用開始時に設定された初期パスワードは、速やかに容易に推測できないパスワードに変更する。
- パスワードは10文字以上（英大文字、英小文字、数字、記号のうちの3種類以上が混在）のパスフレーズを用いる。
- 利用者がパスワードを忘れた場合は、利用者の身分証明がなされた後に初期パスワードを発行する。
- 複数の異なるシステム等でパスワードの使い回しをしない。
- パスワードは秘密にする。
- パスワードを紙に記録して保管しない。
- 容易に推測できないパスワードを使用する。
- 初期パスワードは最初のログオン時に変更する。
- 個人用のパスワードは共有しない。

＜システム運用者向け＞

- 利用者へ定期的なパスワードの変更を強制しない。
- 初期パスワードを発行する場合は、社内メールまたは文書によって、確実に本人へ届く方法で送付する。
- 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。

-
- 個人アカウントを他者と共有することを禁止する。
 - 複数の利用者が利用するアカウント（共有アカウント）は、個人を特定できない問題やリスクを理解の上で発行する。
 - 利用者アカウントは、情報セキュリティ責任者の承認に基づき登録する。
 - 利用者アカウントが不要になる場合、情報システム部門は、当該アカウントの削除または無効化を、当該アカウントが不要になった日の翌日までに実施する。
 - 当社の従業員以外の者にアカウントを発行する場合は、部門長の承認を得たうえで、秘密保持契約を締結する。

2. 18 アクセス権

- システムおよび執務室や書庫、情報へのアクセス権の提供および解除は 2.10 に記載の利用資格(アクセス権限)の付与基準に従って、実施する。
- 利用者のアクセス権を定期的に見直し、必要に応じて変更する。
- 社員、契約社員等、協力会社社員、派遣社員の雇用終了時、契約終了時または合意の終了時に執務室、サーバールーム、セキュリティルーム、情報への不要なアクセス権を削除または変更する。
- 執務室、サーバールーム、セキュリティルーム、情報へのアクセス権の変更履歴を残す。

2. 19 調達製品サービスや委託先の情報セキュリティ対策の評価と管理

- 供給者の製品およびサービスを利用する場合には、脆弱性についてリスク評価を行った上で利用する。
- 供給者の製品およびサービスを利用する場合には、SLAを確認し、セキュリティリスクを評価した上で利用する。
- 清掃業者や保守業者（ICT 機器、コピー機、自販機、植栽等の保守業者）が物理的・論理的に組織のエリアや資産にアクセスする場合、事前の許可ならびにアクセス記録を取る。
- 情報セキュリティ部門責任者は情報資産を取り扱う業務を、外部の組織に委託する場合は、委託先事業者の情報セキュリティ管理について、「委託先情報セキュリティ対策状況確認リスト」に記載の委託先事業者評価基準に基づいて評価する。評価結果に基づき委託先事業者を選定し、情報セキュリティ責任者の承認を得る。
- 委託開始後には、「委託先情報セキュリティ対策状況確認リスト」により、委託先事業者における情報セキュリティ対策の実施状況について定期的に評価する機会を設ける。委託先事業者における情報セキュリティ対策の実施に関して不備また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。
- － 委託先事業者の管理責任者にインタビューする。
- － 委託先事業者に「委託先情報セキュリティ対策状況確認リスト」を送付し、実施状況について回答してもらう。

2. 20 情報セキュリティ要求事項に基づく外部委託契約

- 情報システムや情報処理設備の構築、運用管理を利用、委託する場合は、セキュリティ要求事項を明確にし、契約を締結する。
- 供給者のサービスを利用する場合には、組織の情報セキュリティ要求事項を満たすサービスを選定し、契約を締結する。
- 協力会社社員、警備員、清掃員、保守業者が定期的にサーバールームやセキュリティルームに入る場合は、セキュリティ要求事項を明記した契約を締結する。
- 協力会社社員がセキュリティ方針および手順に違反した場合は、必要に応じて協力会社に損害賠償を請求する。
- 委託契約書には、下記に関する事項を明記する。
 - － 当社の情報資産およ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情報資産および個人情報の返却または廃棄、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

2. 21 製品サービスの選定や調達における情報セキュリティの管理

- 情報システム部門は、社内基盤のネットワーク・システム運用にあたり情報セキュリティ対策を考慮し製品またはサービスを選択する。なお、社内基盤のネットワーク・システムにおける情報セキュリティ対策および関連仕様は、情報セキュリティ責任者が承認する。
- 社内基盤のネットワーク・システムで利用するサーバ機器に求める情報セキュリティ要件は、情報システム部門が決定する。新規にサーバ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、情報システム部門の許可を得て導入する。
- 社内基盤のネットワーク・システムで利用するサーバ機器に導入するソフトウェアは、情報システム部門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、情報システム部門の許可を得て導入する。
- 社内基盤のネットワーク・システム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、ネットワーク管理者が決定する。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、ネットワーク管理者の許可を得て導入する。
- 当社が委託する業務を、委託先が他の組織また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事業者を求める。報告には必要に応じて以下の提供を含め、当社と同等の管理を再委託先事業者に行っていることを確認し、部門長の承認を得たうえで再委託を認める。
 - － 委託先事業者と再委託先事業者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）
 - － 再委託先事業者の選定基準

-
- － 再委託先事業者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

- 委託先事業者と契約する際には、再委託に関する制限事項について盛り込む。

【重要度「高」(機密性)】

- 重要な ICT 製品を導入および入替える場合は、構成管理を徹底し、構成要素についても脆弱性情報を収集し、必要に応じて対策する。

2. 22 調達製品サービスや委託先サービスの監視、レビューおよび変更管理

- サービス期間中に、定期的および必要に応じて、業務報告・記録等を取得し、サービス内容およびセキュリティレベルに問題がないことを確認する。
- 定期的および必要に応じて、内部監査や第三者審査等の監査結果を確認する。
- 利用する外部サービスの、サービス内容、サービス提供者のセキュリティ方針、手順・対策等が変更される場合、変更内容を把握する。

2. 23 クラウドサービスの利用における情報セキュリティ

- 業務システム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、情報システム部門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。新規クラウドサービス等の外部サービスを導入する場合は、情報システム部門の許可を得て導入する。
- 業務システムで利用するクラウドサービスの情報セキュリティ要件を以下とする。
 - － サービスプロバイダが公表する情報セキュリティまたは個人情報保護への取組方針が、処理しようとする情報資産の重要度に照らして適切である。
 - － サービス仕様に含まれる情報セキュリティ対策が、処理しようとする情報資産の重要度に照らして適切である。
 - － 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ことが望ましい。

＜適合性評価制度の種類＞

- － 情報セキュリティマネジメントシステム適合性評価制度 (ISMS クラウドセキュリティ認証)
- － クラウド情報セキュリティ監査制度
- － プライバシーマーク制度
- － PCIDSS (クレジットカード業界セキュリティ基準)
- － クラウドサービスの安全・信頼性に係る情報開示認定制度
- － ISMAP 政府情報システムのためのセキュリティ評価制度

2. 24 情報セキュリティインシデント管理の計画策定および準備

- セキュリティ事象（セキュリティ方針違反、事件・事故、重要なシステムのセキュリティトラブル）の対処手順（報告先等の役割および責任含む）があり、要員に社内ホームページ等を通じて伝達している。
- 情報セキュリティインシデントが発生した場合には、以下の体制で対応する。

最高責任者	情報セキュリティ責任者（CISO）
対応責任者	インシデント対応責任者
一次対応者	発見者または情報システム部門

- 事故レベル1以上のインシデントが発生した場合、発見者は「緊急連絡先一覧」に従い、対応者または責任者に速やかに報告し、指示を仰ぐ。

2. 25 情報セキュリティ事象の評価および決定

- 報告された情報セキュリティ事象が、情報セキュリティインシデントかどうか決定する手順を定める。
- 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。

＜情報セキュリティ事故レベル定義＞

事故レベル	ソラスト基準	セキュリティ被害状況	システム障害状況	報告		
		不正アクセス・ウィルス感染・不正メール受信・デバイス紛失・情報持出	インターネット不通・システム利用不可	執行役員会	経営会議	取締役会
3	社会的な問題に発展する可能性	情報漏洩・消失・紛失、システム利用不可により社会への説明責任を果たす必要がある状況 ・ 対象の情報が不特定多数である ・ 個人または他企業が金銭的な被害や不利益を被る ・ 多くの顧客や取引先へ、長い期間にわたりサービス提供に支障が出ている	2日以上利用不可（業務上影響のある場合）	毎週報告	毎月報告（リスク対策アップデート）	毎四半期報告
2	影響が多くの関係者や会社 に及ぶ	情報漏洩・消失・紛失があり、全社への影響がある状況 ・ ほぼ全社で業務継続に影響がある ・ 社員や一部の顧客、取引先に影響があるが、「連絡が取れる」「影響度合い」等により、社会影響をコントロールできる状況				
1	影響が一部の関係者や事業に限定される	情報の漏洩・消失・紛失を伴わない ・ 事業への限定的な影響がある				
0	影響が当該事業に限定される	軽微な事故	3時間以内に復旧	部門内で報告（必要に応じてシステムマネジメント部、ヘルプデスクへ連絡		

- インシデントを以下のとおりに区分する。

区分	事件・事故の状況
情報漏洩・流出	情報資産の盗難、流出、紛失
改ざん・消失・破壊	情報資産の意図しない改ざん、消失、破壊
サービス停止	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

2. 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（セキュリティ方針違反、事件・事故、重要なシステムのセキュリティトラブル）が発生した場合、インシデント対応手順に従い処置する。

2. 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（セキュリティ方針違反、事件・事故、重要なシステムのセキュリティトラブル）の再発防止や被害拡大防止のため、事件・事故および重要なシステムのセキュリティトラブルの種類、被害の大きさ、復旧費用等を明確にし、監視する。
- 教育責任者は、情報セキュリティインシデントから得られた再発防止策を、セキュリティ教育等で、要員に伝達する。

2. 28 証拠の収集

- セキュリティ事象（セキュリティ方針違反、事件・事故、重要なシステムのセキュリティトラブル）の監査証跡（事件・事故の経過を追跡できる記録）およびこれに類する証拠を収集し、アクセス制御（施錠）された場所に保管する。
- セキュリティ事象（セキュリティ方針違反、事件・事故、重要システムのセキュリティトラブル）の証拠、削除、改ざんから保護し、訴訟に関連する作業を実施する場合は、証拠の複製を使用する。

2. 29 事業の中断・障害時の情報セキュリティ

- 情報セキュリティ責任者は、重要な業務の識別および優先順位を決め、これらの業務が中断することによる事業に及ぼすと思われる影響を考慮した情報セキュリティの要求事項を取り扱った事業継続計画を策定する。

<事業継続計画の項目例>

- 想定される情報セキュリティインシデント
- 業務内容
- 資産
- 事業継続の方法
- 復旧許容時間
- 復旧責任者および関係連絡先

-
- 事業の中断・阻害時に情報セキュリティを維持するための計画は経営陣の承認を得る。
 - 情報セキュリティの要求事項を取り扱った事業継続計画は、定期的（年1回以上）に試験を実施し、必要に応じて見直しをする。

2. 30 事業継続のための ICT の備え

- 情報セキュリティ責任者は、事業継続計画において業務の中断等への影響を考慮する際に、業務の継続に必要な ICT サービスの中断等による影響（可用性）を分析、評価する。
- 情報セキュリティ責任者は、事業継続計画において、ICT サービスの中断等による影響の分析結果を元に、ICT サービスに関する対応（予防/検知/復旧等）を検討し、決定する。
- 情報セキュリティ責任者は、事業継続計画の定期的な試験・見直しにおいて、必要に応じて、業務の継続に必要な ICT サービスに関する試験、見直しも実施する。
- インシデント対応責任者は、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および関係者連絡先について、有効に機能するか検証する。復旧責任者は、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。

2. 31 法令、規制および契約上の要求事項

- 情報セキュリティ責任者は、組織の情報セキュリティに関連する関連法規および契約上の要求事項を明確にし、組織としての取り組み方を決定する。また、情報確認を定期的（年1回以上）実施し、最新に保つ。

2. 32 知的財産権

- 著作権、意匠権、商標のような知的所有権があるソフトウェア製品等を使用する場合は、法令、規則および契約上の要求事項を遵守するために適切な手続きを実行する。
- ソフトウェア製品を使用する場合は、使用許諾契約書に従い利用する。

2. 33 記録の保護

- 紙媒体や記録媒体の記録は、劣化、損傷、紛失、破壊、改ざんを防止するのに適した場所に保護し保管する。
- 電子媒体の記録は、削除、改ざん、認可されていないアクセスを防止するためにアクセス制御を行う。
- 記録は保管期間を定めて（法律上必要な期間）管理する。

2. 34 プライバシーおよび個人を特定できる情報(PII)の保護

- 個人情報の取扱い等については、別に定める「個人情報取扱マニュアル」「特定個人情報取扱マニュアル」「個人情報事故対応マニュアル」を参照する。

2. 35 情報セキュリティの独立したレビュー

- 情報セキュリティ基本方針および年度目標が効果的に実施されていることを内部監査や外部監査で確認

する。

- 監査責任者は、情報セキュリティ関連規程の実施状況について、年1回点検を行い、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。
 - － 情報セキュリティ関連規程が有効に実施されていない場合は、その原因の特定と改善
 - － 情報セキュリティ関連規程に定められたルールが、対策として不十分または有効でない場合は、情報セキュリティ関連規程の改訂
 - － 情報セキュリティ関連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、情報セキュリティ関連規程の改訂

2. 36 情報セキュリティのための方針群、規則および標準の順守

- セキュリティ方針、年度目標および規程類に準拠していることを確実にするために定期的に手順を確認し見直す。
- セキュリティ方針、年度目標および規程類に準拠しているかどうかを監査などで定期的に確認する。
- ハードウェア、ソフトウェアのセキュリティ対策が正しく実行されていることを確実にするために、運用システムの点検を行う。なお、点検は、手動でもツールによるものでもよい。

2. 37 操作手順書

- 社内システムの運用手順書を作成し、必要とする人が利用できるようにする。
- 各組織で重要なシステムを運用している場合は、運用手順を作成し、必要とする人が利用できるようにする。

3	人的管理策	発行日	2024.04.01
適用範囲	全従業員（取締役、社員、契約社員、パート・アルバイトを含む）		

3章 人的管理策

3. 1 選考

- 新規採用、中途採用の応募者が提出した履歴書、推薦状などの内容が正確であることを確認する。
- セキュリティ上の十分な職能や資質について、採用後も継続的に確認する。
- 正社員、契約社員が提出した履歴書、推薦状などの内容が正確であることを確認する。また、十分な職能や資質があることを確認する。
- 派遣会社から要員が提供される場合は、契約書に要員の選考に対する派遣会社の責任を明記する。

3. 2 雇用条件

- 正社員を雇用する際に情報セキュリティに関する社員の役割と責任を明記した雇用契約書（または誓約書）に同意し、署名させる。
- 契約社員を雇用する際に情報セキュリティに関する契約社員の役割と責任を明記した覚書に同意し、署名させる。
- 派遣社員がセキュリティ方針および手順に違反した場合は、必要に応じて派遣会社に損害賠償を請求する。
- 雇用時に情報セキュリティに関する協力会社社員の役割と責任、協力会社の責任を明記した契約書（または誓約書）を協力会社と交わす。
- 業務上知りえた情報を外部に漏らさないよう、社員等を雇用する際に機密保持を誓約させる。

3. 3 情報セキュリティの意識向上、教育および訓練

- 教育責任者は、正社員、契約社員、派遣社員等に対して、入社時に必ずセキュリティ研修を実施する。また、定期的（年1回以上）および必要に応じて（異動・変更時）、セキュリティ教育を実施する。
- 顧客等、利害関係者が常駐する場合などは、定期的および必要に応じて、セキュリティ教育を実施する。
- 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する。
 - － 情報セキュリティ関連規程の説明（入社時、就業時）
 - － 最新の脅威に対する注意喚起（随時）
 - － 関連法令の理解（関連法令の公布・施行時）
 - － 個人情報の取り扱いに関する留意事項
- 教育責任者は、以下に挙げる推奨資格の取得による従業員の情報セキュリティに対する意識向上を年度単位で計画する。計画には関連テキストの配付、公開セミナーの受講、受験費用の予算化を含むこととする。
＜情報セキュリティに関わる推奨資格＞

-
-
- IPA 情報処理技術者試験・情報処理安全確保支援士試験
 - 情報セキュリティマネジメント試験
 - システム監査技術者試験

3. 4 懲戒手続き

- 当社の情報セキュリティ方針および関連規程を遵守する。違反時の懲戒については、就業規則に準じる。
- 情報セキュリティ責任者は、懲戒手続きを社員および契約社員に伝達する。
- 社員および契約社員を懲戒処分する場合は、正式な手順に従って処理する。

3. 5 雇用の終了または変更後の責任

- 雇用終了後、契約終了後、担当業務の変更時に、業務上知りえた情報を関係者以外に漏らさないよう誓約させる。
- 在職中に知り得た当社の営業秘密また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。

3. 6 秘密保持契約または守秘義務契約

- 正社員、契約社員、顧客、協力会社との機密保持契約または守秘義務契約には、組織として規定すべき要求事項を明確に記載する。
- 特定した要求事項は定期的（年 1 回以上）および必要に応じて見直す。

3. 7 リモートワーク

- リモートワーク時のインターネットアクセスは、自宅のネットワーク、会社提供の SIM、社給スマートデバイスのテザリング、信頼された企業やサービス提供元による公衆 Wi-Fi を用いること。
- リモートワークをする場合、住環境を共有する者（家族、友達など）に情報へアクセスさせない。
- リモートワークをする場合、公共の場所における第三者からの盗み見防止のための対策を取る。
- リモートワーク時の書類・印刷物・CD/DVD 等の物理媒体の取り扱いとは原則禁止とし、部門長が許可した場合のみとする。
- リモートワークにおいて物理媒体を利用する場合は、紛失や盗み見を防止するため、適切な保管場所に保管し、破棄は事務所のシュレッダーなど判読不可能な状態にすること。
- リモートワークで貸与品がある場合は貸出・返却手順を明確にする。
- 取引先・レンタルオフィス・カフェ・ホテル・ファーストフード・コンビニ・空港・駅・鉄道・バスなど外出先でリモートワークを行うときには、以下に注意する。
 - 必要な情報以外は持ち出さない。
 - 機器や書類は目の届く範囲に置き放置しない。
 - 取引先やレンタルオフィスなどで一時離席するときはスクリーンセーバーや画面をロックする。
 - 特定多数の人がいる場所では重要情報を画面に表示せず、のぞき見防止フィルターを利用する。
 - 外出先で書類や CD・DVD などの媒体を廃棄しない。

3. 8 情報セキュリティ事象の報告

- パソコン紛失、入館証紛失、メール誤送信、情報漏洩など、情報セキュリティ事象を発見した場合、またはその疑いを発見した場合、手順に従って報告する。
- セキュリティの弱点や脅威に気づいた場合、あるいはその疑いがある場合は報告手順に従って報告する
- インシデント対応責任者は、報告されたセキュリティ事象・弱点は記録する。

4	物理的管理策	発行日	2024.04.01
適用範囲	全事業所		

4章 物理的管理策

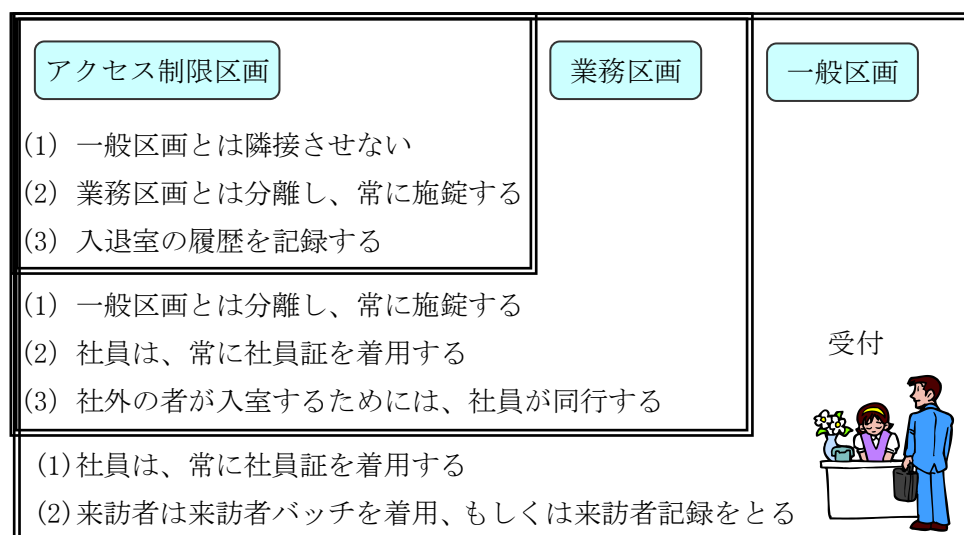
4.1 物理的セキュリティ境界

- 組織の情報と資産がある領域にはセキュリティ境界を設ける。

一般区画	受付・応接スペース
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	プロジェクター、ホワイトボード
制限事項	未使用時に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	—
侵入検知	—
来客用名札	要着用
火災対策	火災検知器、消火器設置

業務区画	執務室 (介護施設や保育施設の居室、書類関係が保管されている事務所等)
利用者	従業員以外の入室は従業員の許可またはエスコートが必要
施錠	最終退室者による施錠および警備会社への通報装置作動
設置可能情報機器	プロジェクター、ホワイトボード、パソコン、複合機、電話機、LAN ケーブルハブ、無線 LAN 中継器
制限事項	情報機器・設備の無断操作禁止・無断持出し禁止
部外者管理	受付の許可を受けて入室可能
管理記録	入退室を所定様式、入退室システムに記録
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

アクセス制限区画	サーバールーム/セキュリティルーム
利用者	あらかじめ許可された者
施錠	常時施錠および警備会社への通報装置作動、鍵の管理責任者
設置可能情報機器	サーバ、ルータ等のネットワーク機器、医療情報や個人情報を扱うパソコン
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・点検時等に社員のエスコート付で入室可能
管理記録	入退室を所定様式に記録、監視カメラによる記録
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



4. 2 物理的入退

- 正社員、契約社員は社員証（入館証）を保持する。
- 来客が入室する場合、受付をし、一般区画での対応とする。
- 保守作業員（コピー機、自販機、植木を含む）などが執務室に入室する場合は、社員が立ち会う。
- 顧客に対する入室制限や情報または資産へのアクセス制御の方針を明確にする
- 執務室へは IC カードにより入室を許可し、誰でも入室できないようにする。
- 執務室の入室は許可された者だけが入室できる。また入退室の記録を取る。
- 物品の受渡しは、原則として一般区画で行う。

【重要度「高」（機密性）】

-
-
- サーバルーム、セキュリティルームへの入室許可は必要最小限にする。
 - サーバルーム、セキュリティルームの入室許可者を定期的に見直す。
 - サーバルーム、セキュリティルームへは IC カードにより入室を許可し、誰でも入室できないようにする。
 - サーバルーム、セキュリティルームの入室は許可された者だけが入室できる。また入退室の記録を取る。
 - パソコン類などの物品を執務室やサーバルーム、セキュリティルームに搬入してもらう場合は、社員が作業に立ち会う
 - 倉庫の入室は許可された者だけが入室できる。また入退室の記録を取る。

4. 3 オフィス、部屋および施設のセキュリティ

- 執務室での業務内容が屋外から見えないようにする（例えばブラインドを下ろす）。
- 重要書類が保管されている書庫・キャビネットの鍵は施錠可能な場所に保管する。
- 重要書類が保管されている書庫・キャビネットの鍵は 2 本用意し、それぞれ別の場所に施錠管理する。
- 執務室が無人になる時は、施錠する。
- 執務室が無人になる時は、警報装置を稼働させる。
- 執務室では協力会社社員だけで作業させない。
- 許可なしに執務室をカメラ、ビデオなどで撮影することは禁止する。

【重要度「高」（機密性）】

- 重要な設備は、アクセスを許可されていない保守作業員（コピー機、自販機、植木を含む）などがアクセスできない場所に設置する。

4. 4 物理的セキュリティの監視

- 適切な場所に警備員を配置する。

【重要度「高」（機密性）】

- 執務室やアクセス制限区画への入室を目視および記録するために、監視カメラ等のビデオシステムを導入する。
- 監視カメラや警報装置は定期的に試験をする
- 常用する全ての扉や窓からの侵入に備え、警報を使用する。

4. 5 物理的および環境的脅威からの保護

- 自然災害および人的災害による被害を受けにくい立地条件の建物を借用する。
- 火災に備えて、火災警報器や消火システムを設置する。

4. 6 セキュリティを保つべき領域での作業

【重要度「高」（機密性）】

- サーバルームやセキュリティルームでは協力会社社員だけで作業させない。

-
-
- サーバルームやセキュリティルームに入室する協力会社社員には、エリアの利用に関する留意事項を遵守させる。
 - サーバルームやセキュリティルームの入室許可責任者から特別に許可された協力会社社員のみが、当エリアに入室できる。
 - 保守業者がサーバルームやセキュリティルームに入室する場合は、社員が作業に立ち会う。
 - サーバルームやセキュリティルームのへ保守業者などが入室する場合は、アクセスできる範囲を限定する。
 - 許可なしにサーバルームやセキュリティルームをカメラ、ビデオなどで撮影することは禁止する。
 - サーバルームやセキュリティルームで情報処理作業を実施していることが屋外から見えないようにする（例えばブラインドを下ろす）。
 - サーバルームやセキュリティルームが無人になる時は、施錠する。
 - サーバルームやセキュリティルームは、一般区画（建物に入った人が誰でも通れる場所）に面した場所に設置しない。

4. 7 クリアデスク・クリアスクリーン

- ログオンした状態で離席する時はログオフする。またはスクリーンロックをかける。
- 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。
- 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。退社時または使用しないときにはパソコンの電源を切る。
- 離席時や帰宅時は資料を放置しない。
- 会議等で使用したホワイトボードは終了時に必ず消す。
- 社内のノートパソコンや可搬記録媒体は、ワイヤーロックするか帰宅時に引き出し等に施錠保管する。
- プリンター、コピー機の出力用紙を放置しない。

4. 8 装置の設置および保護

- 装置を設置している作業領域への不必要なアクセスは最小限とする。
- パソコン類は安定した場所に設置する。
- 落下、転倒の可能性がある場合は、耐震ベルトなどによりパソコンを固定する。
- 設置機器は施錠管理や監視カメラの設置など、容易に持ち出しがされない工夫等対策がされること。

【重要度「高」（機密性）】

- 重要なネットワーク機器は、施錠可能なラックに収納する。

4. 9 構外にある資産のセキュリティ

- パソコン類・スマートフォン・タブレット端末を社外で利用する場合は、他者に覗き見されないようにする。
- パソコン類の持ち出し、受け入れ時の手順を策定し実施する。

-
- パソコン類を社外に持ち出す場合は、事前に管理者の承認を得る。
 - パソコン類を社外に持ち出す場合は、手元から離さない。
 - 情報資産が格納されているパソコンのストレージは暗号化する。

4. 10 記憶媒体

- パソコン類を返却または持ち込む場合は、手順に従ってセキュリティ上、問題ないことを確認する。
- 記録媒体の持ち出し管理を行う。
- 機密情報を社外に持ち出す場合は、事前に管理者の承認を得る。
- 記録媒体はメーカーが指示する取扱い方法に従い、セキュリティが保たれた環境に保護する。
- 記録媒体の寿命より長く保管する必要がある場合、記録媒体の劣化による情報の消失を避けるために別の記録媒体に移行する。
- 非公開の紙媒体を廃棄する場合は、細断する。
- 非公開の紙媒体は再利用しない。
- 記録媒体を再利用する場合は、格納された非公開の情報を確実に消去する。
- 記録媒体を廃棄する場合は、格納された非公開情報を確実に消去する。あるいは格納された情報が読み取れないよう破壊する。
- 取り外し可能な記憶媒体のポート（SD カード、USB 等）は、必要に応じて無効化する。
- ネットワーク上で遠隔からシステムやデバイスの状態を監視・診断するために使用される遠隔診断ポートの利用は、保守サポートなど必要な場合のみに限定し、認証機能やコールバック機能等を備えるなど、適切なセキュリティ対策を施す。
- USB メモリや外付け HDD に保存する必要がある場合は、会社指定の記憶媒体を使用し、ファイルを暗号化する。
- 記憶媒体を利用する際は、以下を遵守する。
 - － 会社指定の USB メモリは、職務上必要な処理で代替手段がない場合のみ使用を許可するものとする。
 - － 所属長ならびに情報システム部門管理者の許可の得ていない外部記憶媒体を使用しない。また、使用を試みない。
 - － 保管場所や取扱いには細心の注意を払い、貸与を受けた所属部署にて紛失または盗難がないよう適切に管理しなければならない。
 - － 万一、会社より貸与された USB メモリを盗難または紛失してしまったときは、速やかに所属長および情報システム部門担当者に連絡する。
- USB メモリを利用するユーザは、所定の様式に必要な事項を記載して所属長の承認の上、情報システム部門担当者に届け出を行うものとする。また、USB メモリの利用の必要が無くなった場合は、速やかに情報システム担当者に返却するものとする。

4. 11 サポートユーティリティ

- 空調設備が整っており、定期的に保守・点検を実施している建物を借用する。

【重要度「高」(可用性)】

- 一時的にでも停止できない装置については、電源の二重化、無停電装置、自家発電設備などを設置する。

4. 12 ケーブル配線のセキュリティ

- ケーブルは床下に配線したり、ケーブルに保護カバーをしたりする。

【重要度「高」(機密性)(可用性)】

- 重要度の高いケーブルは代替ケーブルを準備する。
- サーバは施錠付き専用ラックに収納する。
- LAN ケーブルは回線盗聴防止のため配線を露出しない。
- 無線 LAN における情報搾取や不正アクセスのリスクを低減するため、暗号を活用する場合は、その時点で安全な暗号方式を利用して、通信を暗号化する。

4. 13 装置の保守

- 保守要員が執務室に入室する場合は、必要最小限のアクセス権を与え、また、保守作業を監視する。
- 記憶媒体を内蔵した装置を修理に出す場合は、格納されている非公開情報を削除する(故障により削除できない場合は除く)。
- 記憶媒体を内蔵した装置を修理に出す場合は、守秘契約を締結した業者に依頼する。

【重要度「高」(機密性)(可用性)(完全性)】

- 継続的に機密性・可用性・完全性を維持する必要がある機器については、ハードウェアの保守契約を結ぶ。

4. 14 装置のセキュリティを保った処分または再利用

- パソコン類を廃棄または社内で再利用の場合やリースバック・レンタルバックする場合は、情報システム部門が指定するツールを使用して情報端末業務で利用したデータを完全に消去する。
- パソコン類を廃棄または再利用する際は、記録を取得する。
- パソコン類を廃棄する場合は、指定業者を通して廃棄し、廃棄証明書を取得する。

5	技術的管理策	発行日	2024.04.01
適用範囲	情報資産の利用者および情報処理施設		

5章 技術的管理策

5.1 利用者端末

- 情報システム部門が指定するウイルス対策ソフトウェアをインストールし、定義ファイルを自動更新する設定にする。
- ストレージ（ハードディスク、SSD 等）、電子媒体に対してウイルスチェックを行う。
- 以下全てのアプリケーションソフトのインストールと利用を禁止する。
 - － 機器ベンダの公式な公開場所（AppStore、GooglePlay など）以外から提供されるもの
 - － 不審なベンダが提供するもの
 - － 正規ライセンスを取得していない違法なもの
- OS やアプリケーションソフトのアップデートが通知されたら速やかに実施する。
- 情報端末や電子媒体を社内に持ち込む場合は、社内 LAN への接続や社内パソコンおよびサーバへ接続しない。
- VPN サービスの利用する場合は情報システム部門の許可を得る。
- VPN サービスの利用する場合は以下を全て遵守する。
 - － 情報システム部門の許可を受け指定された方法で接続する。
 - － 画面の盗み見、不正操作等を防ぐよう、適切な環境で行う。
 - － 情報端末から離れる場合は、情報端末を停止するか他者が利用できないようにする。
 - － リモート接続で利用する情報端末を紛失した場合は、直ちに情報システム部門に連絡し指示に従う。
 - － 業務に関する情報資産の保存を禁止する。
 - － IPSec などを用いて通信経路を暗号化する。
- 執務室や自宅、もしくは会社が許可した Wi-Fi 以外は使用しない。
- 自宅や屋外で利用する場合は以下を全て遵守する。
 - － 信頼できる通信回線のみを利用する。
 - － 機器は原則として勤務時間のみ稼働させる。
 - － 不審なメールの受信など、情報セキュリティで不安がある場合は情報システム部門に問い合わせる。
- データを暗号化し、通信する。

-
- 離席時にはスクリーンロックし、作業終了時にはログオフをする。
 - 情報システム部門は、利用を終了するパソコンや記憶媒体について、データ消去ツールを用いて業務利用したデータを完全に消去するか、磁気破壊または物理破壊し、復元できない状態にする。
 - 業務用のスマートフォンや携帯電話を利用する際は、遠隔で管理する MDM サービス等に参加し、リモートワイプ、リモートロックが可能な状態で利用する。
 - 業務用のスマートフォンや携帯電話は放置せず、参照範囲外の人に見られないように暗証番号などでロックする。
 - パソコン類を社外に持ち出す場合は、手元から離さない。

5. 2 特権的アクセス権

- 特権ユーザの承認手続きを明確にし、承認の記録を残す。
- 特権ユーザ ID は一般ユーザ ID とは別の ID を付与する。(作業によって使用する ID を区別する)
- 特権ユーザの割当ては必要最小限の人数にする。
- 特権ユーザの割当ては、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、複数名に分散する。
- 特権ユーザのアクセス権を定期的に、また変更(人事異動など)があった場合に見直す。一般ユーザより高い頻度で見直す。

【重要度「高」(機密性)】

- 特権ユーザとして作業をするたびに承認を受ける。

5. 3 情報へのアクセス制限

- 利用者の分類(社員、契約社員、協力会社社員、派遣会社社員など)に応じてアクセス権(リード権、ライト権、実行権など)を制御する。
- 識別情報、装置、場所、アプリケーションなどに基づいてアクセス許可を与える。

5. 4 ソースコードへのアクセス

- プログラムソースコード、開発ツール、プログラムソースライブラリへは、プロジェクトなどで決められた者のみがアクセスできるように制御する。

5. 5 セキュリティを保った認証

- ログオン手順に、許可されていない利用者の助けとなるメッセージを表示しない。
- 入力したパスワードを平文で画面表示しない。
- パスワードは暗号化して保存する。
- パスワード入力の失敗回数(3回を推奨)を制限する。パスワード入力を指定回数失敗した場合は、一定時間ロックアウトする、または所定の手続きにより本人確認のうえ解除する。
- ログオンに成功または失敗したログを記録する。
- 重要度「高」の情報を扱う情報システムや、クラウドサービスへのアクセスには多要素認証を用いる。
- ネットワーク接続によりアクセスする際の認証方式として、情報端末の識別による認証または接続元の

IP による認証を用いる。

- ログオン後の接続時間を制限する。

5. 6 容量・能力の管理

- 情報システムの処理能力（CPU やメモリの使用率、HDD 使用量、通信量等）を監視し、将来必要とされる処理能力や容量を予測する。必要に応じて CPU 使用率および記憶容量を調整する。

【重要度「高」（可用性）】

- 処理能力の指標に対して、設備増強等のシステム変更が必要と判断する基準の値（しきい値）を設定する。
- 毎月 1 回、CPU 使用率の利用状況等を監視し、処理能力や容量がしきい値を超えないように調整する。調整しても、しきい値を超えそうな状況の場合は、設備増強も含めた対応を実施する。
- 人的資源の増員や施設の増加についても、必要に応じて、検討している。

5. 7 マルウェアに対する保護

- ウイルス対策ソフトをインストールし、定義ファイルを自動更新する設定にする。
- OS およびソフトウェアを更新する。
- ウイルスに感染した場合は、手順に従い、封じ込め・根絶・復旧する。
- ウイルスに感染した場合またはウイルス感染の恐れがある場合は、速やかに社内ネットワークから切断し、パソコンの電源を切らずに情報システム部門に連絡する。
- 新しい機器を導入する場合は、使用前にウイルス検査を実施する。
- フリーソフトウェアは原則使用を禁止し、使用するソフトウェアは、情報システム部門で承認されたものを購入する。
- 社外とファイル共有可能なソフトウェアは原則として使用しない。使用する場合は、情報システム部門の承認を得て使用する。

【重要度「高」（機密性）】

- 重要なシステムで用いるパソコンでは社外とファイル共有可能なソフトウェアを使用しない。
- ネットワーク経由で入手するファイルは、自動検知機能を有効にしてウイルス検知を実施する。
- 電子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。
- 当社が管理するパソコン、サーバおよび会社貸与のスマートフォン、タブレット以外の機器を社内 LAN に接続する場合は、情報システム部門の許可を得たうえで、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。
- ウイルスに感染した、またはその疑いがある場合の対応方法についての要員教育を行う。
- 標的型攻撃メール等によるウイルス感染を防止するため、不審なメールの添付ファイルを開く、またはリンクを参照するなどしない。受信した場合は、情報システム部門に報告し、情報システム部門は社内に注意を促す。

5. 8 技術的脆弱性の管理

- 使用中の情報システムの技術的脆弱性の情報を入手し、リスクを評価し、必要に応じて対策を講じる。
- 情報システムのソフトウェア開発を行う際には、当該情報システムの利用環境に応じて設計時に技術的な脆弱性を識別し、対策を講じる。脆弱性に対する対策の有効性は情報システム部門が判断し、承認する。
(参考) IPA 情報セキュリティ脆弱性対策
<https://www.ipa.go.jp/security/vuln/index.html>
- 脆弱性の特定、パッチ適用の検証のために、脆弱性スキャンツールを用いる。

5. 9 構成管理

- ハードウェア、ソフトウェア、サービス（クラウドサービス等）およびネットワークに関して、導入した運用システムのセキュリティ設定が正しく構成管理されていることを確実にするために、運用システムの点検を行う。また、構成を変更する場合は、システム変更手順などに従う。
- ハードウェア、ソフトウェア、サービスおよびネットワークの構成を検討する際には、組織のセキュリティ方針、ベンダの推奨事項などを考慮する。

5. 10 情報の削除

- 情報システムや装置からの情報の削除手法（例：物理的破壊、磁気消去、クラウド上の情報削除等）を定め、実行する。
- 削除の結果を証拠として記録する。情報削除を行うサービス業者に委託する場合、削除証明書を取得する。

5. 11 データマスキング

- 必要に応じ、個人情報や要配慮個人情報はマスキングや匿名化・仮名化する等の対策を講じる。

5. 12 データ漏洩防止

- 組織内で保管される情報が外部にアップロードされたりメールで送信されたりすることにより、外部に情報が漏洩の可能性がある場合に検知し、防止するための対策を講じる。または、アクセス制御や暗号化保存を実施する。

5. 13 情報のバックアップ

- バックアップ方針に基づきバックアップを取得する。
- バックアップに利用した機器の取扱いは以下の全てに従う。

＜保管例＞

CD/DVD、外付けHDD、USBメモリ等：施錠付きキャビネットに保管

NAS サーバ：施錠付きサーバラックに格納

＜廃棄・再利用例＞

4.14（装置のセキュリティを保った処分または再利用）に従う。

- クラウドサービスを利用し、外部のサーバにバックアップを保存する場合は、以下の全てのサービス要件を確認し、情報システム部門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、当社の情報セキュリティ関連規程に適合している。
- － 当社事業所がある地域で発生する震災、水害等の影響を受けない地域の施設である。

【重要度：「高」（可用性）】

- 極めて重要な業務情報およびソフトウェアがある場合は定期的にバックアップをする。
- 極めて重要な業務情報およびソフトウェアのバックアップは建物の災害から損傷を免れるために十分離れた場所に保管する。
- バックアップファイルを定期的に検査する。

5.14 情報処理施設・設備の冗長性

- 情報処理システムは、その重要性によって冗長構成、あるいは地域分散を行う。

【重要度：「高」（可用性）（完全性）】

- 継続的に可用性と完全性を維持する必要がある設備・機器については、ハードウェアまたはネットワークを冗長化する。あるいは、予備のハードウェアを用意する。

5.15 ログ取得

- ユーザ ID（特権ユーザも含む）、ログオンおよびログオフ日時、システムやデータへアクセスを試みての成功および失敗の記録を取り、重要度に応じて必要な期間（例えば 1 年）保管する。
- 情報セキュリティ侵害が発生していないかどうか、システムごとに定める間隔で定期的を取得したログを分析する。
- ログ機能の設定は許可された者のみが実施できるようアクセス制御する。
- ログ情報は許可された者のみがアクセスできるように制御する。
- システムを維持管理している場合、運用担当者は、作業名、作業時間、作業内容などを記録し、情報システム部門に報告する。

【重要度：「高」（機密性）】

- 以下の全てに従い、ゲートウェイにおける通信ログを取得および保存する。
 - － 通信ログの保存期間は最低 1 年間とする。
 - － ログファイルの保存状況について、情報システム部門が定期的に確認する。
- 情報システム部門は、通信ログについて以下の全ての確認を定期的に行う。
 - － 管理外のインターネット接続がないか
 - － 許可なく接続された機器や無線 LAN 機器はないか
 - － 不審な通信が行われていないか

5. 16 監視活動

- 社内システムやネットワークの異常なトラフィックや社外からの不審なアクセスを検知し、警告する仕組みを設ける。

5. 17 クロックの同期

- 情報システムで用いるサーバやパソコンは、コンピュータ内の時計を組織が採用した NTP に合わせる。なお、一部のスタンドアロンパソコン等については除く。

5. 18 特権的なユーティリティプログラムの使用

- システムおよび業務プログラムの制御を無効にするシステムユーティリティを使用する場合、使用する人、時間を制限する。
- システムおよび業務プログラムの制御を無効にするシステムユーティリティを使用する場合、使用記録をとる。
- システムおよび業務プログラムの制御を無効にする不要なユーティリティソフトウェアは、アンインストールする。

5. 19 運用システムへのソフトウェアの導入

- システムの維持管理を行う場合、運用プログラムの更新は任命された担当者によって実施する。
- システムの維持管理を行う場合、運用プログラムの構成管理を行う。
- ソフトウェアのインストールは、責任者の承認を得て行う。インストールされたソフトウェアは記録し、管理する。

5. 20 ネットワークセキュリティ

- 各ネットワーク（社内基幹ネットワーク、インターネット接続セグメント、エクストラネット接続セグメント、アプリケーションサービスセグメント、OA ネットワーク、開発用ネットワーク、部署基幹ネットワークなど）の境界と管理責任の所在を明確にする。
- ネットワーク管理者はネットワークに流れる情報の保護およびネットワーク基盤（ルータ、ファイアウォール、ゲートウェイ等）を保護（ルータ等の正しい設定を含む）するための対策を講じる。
- ネットワークの運用手順に従ってネットワークを運用する。

5. 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提供者（全社ネットワーク管理者、独自ネットワーク管理者）は、ネットワーク利用者に対してサービスのセキュリティ特性について明確な説明を行い利用者と合意する。
- WAN やインターネットサービスの場合、SLA や報告書を受領し、問題がないか定期的に確認し、合意した SLA の通りのネットワークサービスであるかどうか監視する。（LAN の場合、ネットワークトラフィック等を定期的に確認する。）

5. 22 ネットワークのアクセス制御

- 社内ネットワーク（独自ネットワークを含む）と社外ネットワークを分離し、アクセス制御を行う。
- 利用者用セグメント、サーバ用セグメント、開発用セグメントなど、利用に応じたセグメント分割を行い、不要・不正なアクセスが発生しないようにアクセス制御する。

5. 23 ウェブフィルタリング

- 情報漏洩に繋がるサイトや業務上不要と思われるサイトに対してアクセスを禁止する。
- 情報漏洩に繋がるサイトや業務上不要と思われるサイトに対してアクセスを防ぐための技術的仕組みを構築する。
- アクセスを禁止されたサイトに業務上アクセスする必要がある場合は、例外申請手順に沿った対応を行う。
- 情報システム部門は、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は社内周知またはウェブフィルタリングソフトを使用して、従業員の閲覧を制限する。
- 従業員は、業務でウェブ閲覧を行う場合は以下の全てに注意する。
 - － 公序良俗に反するサイトへのアクセスを禁止する。
 - － 不審なサイトへのアクセスおよび社用メールアドレス登録を禁止する。
 - － 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。
 - － 信頼できるサイトから署名付きのモバイルコードをダウンロードする場合を除き、モバイルコード（クライアントパソコン側で動作するプログラム）を実行しない。

5. 24 暗号の利用

- 暗号技術を利用する規則を定める。（持ち運び可能な若しくは取外し可能な媒体装置または通信によって伝送される情報を、保護するために暗号技術を用いる等。）
- 暗号鍵を使用する場合は、鍵の生成、公開鍵証明書の手入方法、鍵の配布方法、鍵の変更や更新、破棄方法などの手順を作成する。
- 暗号の利用にあたっては、デジタル庁・総務省・経済産業省の暗号技術検討会および関連委員会（CRYPTREC）が推奨する暗号技術を用いる。

5. 25 セキュリティに配慮した開発のライフサイクル

- システムおよびソフトウェア開発のセキュリティに配慮したルールを確立し、実施する。
- 情報システムの開発・改修を行う際には、以下の全ての工程を経て実施する。各工程の完了時に情報システム部門の承認を得る。
 - ① 対象業務の範囲定義
 - ② ハードウェア・ソフトウェア・ネットワーク機能検討
 - ③ 必要なパフォーマンスの検討

-
-
- ④ 情報セキュリティ要件定義
 - ⑤ バックアップ/障害復旧要件定義
 - ⑥ 情報システム運用要件定義
 - ⑦ 運用体制
 - ⑧ 移行計画立案

5. 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または取得する場合、アプリケーションで取引する情報の機密性、完全性および真正性を確保するために情報を暗号化する。
- アプリケーションを開発する際に、設計段階で、セキュリティ要求事項を検討する。
- 電子注文および支払いを伴うアプリケーションの場合、注文情報の機密性、完全性および真正性を確保するために情報を暗号化する。
- トランザクションサービスを提供するアプリケーションの場合は、電子証明書により取引相手の本人確認をする。電子印鑑は該当しない。
- 通信経路を暗号化する。なお、暗号化には、VPN または情報処理推進機構が発行する最新の「TLS 暗号設定ガイドライン」に従って対応する。
- オンライン取引情報を暗号化する。
- 電子署名を用いてオンライン取引情報の正当性を保証する。
- 従業員は、インターネットで提供されているサービスを業務で利用する場合は、情報システム部門の許可を得る。利用する際には以下の全てに注意する。

<インターネットバンキング・電子決済>

- インターネットバンキングを利用する際には、自分で設定したブックマーク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際には、SSL/TLS による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、偽サイトへの誘導である可能性があるためアクセスしない。

【重要度：「高」（機密性）】

- 重要なシステムで用いるパソコンでインターネットバンキング・電子決済を実施しない。

<オンラインストレージ>

- 重要度：「高」の情報資産を保存する場合は、情報システム部門の許可を得る。
- メールアドレスの登録が必要な場合は社用メールアドレスを登録する。
- セキュリティポリシーを公表していないサービスの利用は禁止する。
- 不審なベンダが提供しているサービスの利用を禁止する。

5. 27 セキュリティに配慮したシステムアーキテクチャおよびシステム構築の原則

- システムのセキュリティが侵されにくい構造および防御する機能を考慮する。

<例>

暗号機能、電子署名等

- ゼロ・トラスト原則などのセキュリティに配慮したシステム構築を行う。

5. 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プログラミング手法を用いる。(セキュアコーディング)
- セキュリティ上の課題を早い段階で洗い出し、リスクを顕在化させ、セキュリティの観点からレビューを行う。

5. 29 開発および受入れにおけるセキュリティテスト

- 新規システムを開発した場合、または既存システムを改修した場合は、セキュリティ試験（脆弱性診断、ソースコードレビュー等）を実施する。

【重要度：「高」（機密性）】

➤ 重要なシステムを新規開発または改修する場合は、ペネトレーションテストを実施する。

- 新しい情報システム、改版および変更版を受け入れる場合は、受入基準を明確にし、基準を満たしていることを受け入れ前に検査する。

5. 30 外部委託による開発

- ソフトウェア開発を外部委託する場合は、セキュリティ要求事項を満たすことを確認する。
- ソフトウェア開発を外部委託する場合は、プログラムの所有権と知的所有権についてあらかじめ明確にする。
- 外部委託した作業の提供が合意事項を満たしているかを（開発期間中の打合せや報告にて）継続的に監視し、レビューする。
- ソフトウェア開発を外部委託する場合は、ソースコードの品質、作業の質および正確などを考慮する。
- 情報システムの保守を、開発元または外部の組織に委託することができない場合、以下に挙げる事項に留意し、情報システムに既知の脆弱性が存在しない状態で運用する。
 - － 開発時に用いたソフトウェアに関する脆弱性が公表された場合には、速やかにその影響が顕在化しないための対策を講じる。
 - － 開発時に用いたソフトウェアおよびハードウェアの製造者が提供するサポートの終了が予定されている場合、他のソフトウェアやハードウェアを用いた再構築または当該情報システムの利用停止を検討し、情報システム部門の承認を得る。

5. 31 開発環境、テスト環境および本番環境の分離

- システムの重要度（外部からの要求事項や法規制、委託可否、遠隔バックアップ）等に応じて、適切なセキュリティ環境を確立し開発する。

-
- 開発・試験環境と本番環境は論理的あるいは物理的に分離する。
 - 開発から運用の段階に移行する場合は、移行手順を作成する。
 - 情報システムの開発および改修を行う環境は、運用環境とは分離する。新たに情報システムの開発を行った場合や、情報システムの改修を行った場合は、当該情報システムの運用を開始する前に、必要な情報セキュリティ対策が講じられていることを確認し、情報システム部門の承認を得る。

5. 32 変更管理

- ソフトウェア、ドキュメント、プログラムなどは、プロジェクトなどで決められた構成管理手順に従って変更を管理する。

【重要度：「高」（可用性）】

- 重要な業務用ソフトウェアの OS を変更する場合は、運用中のシステムに障害が発生しないことを試験環境で確認する。

- パッケージソフトウェアは原則として変更しない。
- 情報処理設備やシステムの変更を行う場合は、変更内容を記録する。
- 情報処理設備やシステムの変更を行う場合は、変更による影響を評価した後、実施する。
- 情報処理設備やシステムの変更を行う場合、変更内容を関係者に周知する。
- 情報システムのハードウェアまたはソフトウェアの変更を行う際には、以下の全ての工程を経て実施する。各工程の完了時に情報システム部門の承認を得る。
 - ① 現行システムの問題・課題の把握
 - ② システム変更計画立案
 - ③ システム変更計画書に基づくシステム設計
 - ④ セキュリティ要求と設計の見直し
 - ⑤ 移行計画立案（移行時、運用時の障害対応をあらかじめ検討する。）
 - ⑥ 変更後の仕様書、操作手順書、運用手順書等の関連文書の作成

5. 33 テスト用情報

- 個人情報を含む運用データは試験に使用しない。ただし、顧客の要求により個人情報を使用せざるを得ない場合は、個人情報の使用、保管、返却などの取扱い手順を確認し、その手順に従う。
- 個人情報を含む運用データを試験に使用する場合は、試験完了後、削除する。

5. 34 監査におけるテスト中の情報システムの保護

- 情報システムの監査を実施する場合は、業務が中断するリスクを最小限に抑えるよう慎重に計画を立て、関係者の合意を得てから実施する。
- 情報システムへのアクセスを伴う監査を実施する場合は、運用システムに悪影響がないよう慎重に計画を立て、関係者の合意を得てから実施する。