清新社会保険労務士事務所

情報セキュリティポリシー

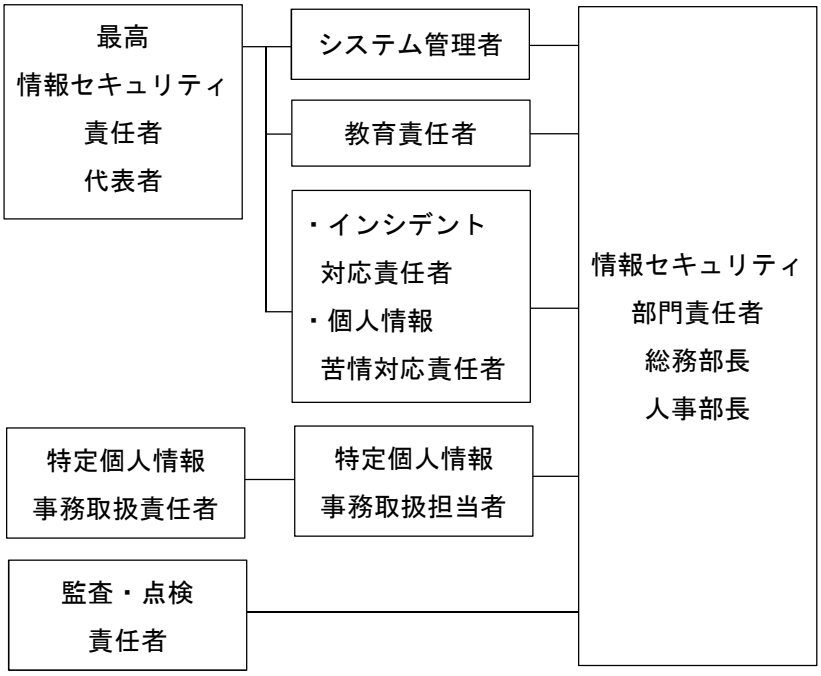
1	組織的対策	制定日	2019.05.01
適用範囲	全社･全従業員		

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	代表者
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 個人情報　苦情対応責任者	総務部長
監査・点検/点検　責任者	総務課長
特定個人情報　事務取扱責任者	代表者
特定個人情報　事務取扱担当者	総務部長

体制図を下図に示す。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。



2.情報セキュリティ取組みの監査・点検/点検

監査・点検/点検責任者は、情報セキュリティ関連規程の実施状況について、３月に点検を行い、監査・点検/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、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、新たな脅威に対する対策として有効でない場合は、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

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。

【専門機関】

- ➢独立行政法人情報処理推進機構（略称：IPA）

[情報セキュリティ]

https://www.ipa.go.jp/security/

[ここからセキュリティ]

https://www.ipa.go.jp/security/kokokara/

- ➢JVN（Japan Vulnerability Notes）

https://jvn.jp/index.html

- ➢一般社団法人 JPCERT コーディネーションセンター（略称：JPCERT/CC）

https://www.jpcert.or.jp/

- ➢個人情報保護委員会

http://www.ppc.go.jp/

2	人的対策	制定日	2019.05.01
適用範囲	全従業員（役員、社員、派遣社員、パート･アルバイトを含む）		

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. 取締役及び従業員の責務

取締役及び従業員は、以下を順守する。

・取締役及び従業員は、当事務所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、当事務所の情報セキュリティ方針及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従い対処する。

※当事務所が営業秘密として管理する情報とは、「情報資産管理台帳」の機密性評価値が 1 以上のものをいう

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・取引先から当事務所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事務所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。

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（関連法令の施行時）

➢特定個人情報の取り扱いに関する留意事項

5. 人材育成

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、公開セミナーへの派遣、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
- 情報処理安全確保支援士試験

3	情報資産管理	制定日	2019.05.01
適用範囲	全社･全従業員		

1.情報資産の管理

1.1 情報資産の特定と重要度の評価

当事務所事業に必要で価値がある情報及び個人情報（以下「情報資産」という）を特定し、「情報資産管理台帳」に記載する。情報資産の機密性における重要度は、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
機密性 1：社外秘	漏えいすると事業に大きな影響がある
機密性 0：公開	漏えいしても事業に影響はない

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

表示が困難な場合は、「情報資産管理台帳」に機密性評価値を明記する。

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。

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。

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。

・極秘の場合は代表者の許可を得る。

・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/フォルダー/データを暗号化する。

・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.媒体の処分

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以下の処分を行う。

書類・フィルム	細断/溶解/焼却
USB メモリ・HDD・CD・DVD	破壊/細断/完全消去　※OS の削除・フォーマットは不可

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 ディスク	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
CD-R・DVD-R	再利用不可

4.バックアップ

4.1 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	Windows Server バックアップ	NAS サーバー
給与計算システム	アプリケーションデータ	ファイルコピー	USB メモリ(暗号化機能付)
会計システム	アプリケーションデータ	アプリケーションバックアップ機能	クラウドバックアップサービス
管理システム	アプリケーションデータ	同期ツール	外付け HDD
Web サーバー	ホームページ	同期ツール	NAS サーバー

4.2 バックアップ媒体の取り扱い

バックアップに利用した機器及び媒体の取り扱いは以下に従う。

＜保管＞

・小型媒体：施錠付きキャビネットに保管
・NAS サーバー：施錠付きサーバーラックに収納
＜廃棄・再利用＞
・「3.媒体の処分」に従う

4.3 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、当事務所の情報セキュリティ関連規程に適合している。
・当事務所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こと。

4	アクセス制御及び認証	制定日	2019.05.01
適用範囲	情報資産の利用者及び情報処理施設		

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。対象となるシステム等は「9.1 アクセス制御対象情報システム及びアクセス制御方法」に記載する。

・「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。

2.利用者の認証

社外秘又は極秘の情報資産を扱う社内情報システムは、以下の方針に基づいて利用者の認証を行う。認証方法等は「9.2 利用者認証方法」を参照のこと。

・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を禁止する。

3.利用者アカウントの登録

利用者の認証に用いるアカウントは、代表者又は情報セキュリティ責任者の承認に基づき登録する。アカウント名の設定条件は「9.3 利用者アカウント・パスワードの条件」を参照のこと。

4.利用者アカウントの管理

利用者の認証に用いるアカウントが不要になった場合、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.パスワードの設定

利用者の認証に用いるパスワードは、以下に注意して設定する。パスワードの設定条件は、「9.3 利用者アカウント・パスワードの条件」を参照のこと。

・十分な強度のあるパスワードを用いる。
・他者に知られないようにする。

6.従業員以外の者に対する利用者アカウントの発行

当事務所の取締役又は従業員以外の者にアカウントを発行する場合は、代表者又は情報セキュリティ責任者の承認を得たうえで、秘密保持契約を締結する。

7.機器の識別による認証

社外秘又は極秘の情報資産を扱う情報システムに、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、機器の識別による認証を用いる。認証方法等は「9.4 機器の認証方法」を参照のこと。

8.端末のタイムアウト機能

社外秘又は極秘の情報資産を扱う情報システムの端末もしくは情報機器を、アカウントを付与していない者が接触可能な場所に設置する場合は、接続時間制限やタイムアウト等機能を利用する。

9.標準設定等

9.1 アクセス制御対象情報システム及びアクセス制御方法

情報システム・サービス	アクセス制御方法
ファイルサーバー	Windows Active Directory
給与計算システム	アプリケーションのユーザー認証
管理システム	アプリケーションのユーザー認証
メールサーバー（ホスティングサービス）	ホスティングサービスのユーザー認証
Web サーバー（ホスティングサービス）	ホスティングサービスのユーザー認証

9.2 利用者認証方法

情報システム	利用者認証方法
ファイルサーバー	Windows ログオン認証：アカウント名・パスワード
給与計算システム	アプリケーションのユーザー認証：ID・パスワード
管理システム	アプリケーションのユーザー認証：ID・パスワード

9.3 利用者アカウント・パスワードの条件

	特権アカウント	一般アカウント
アカウント名	・推奨：推測困難であるもの ＜禁止アカウント名＞ WindowsOS：administrator、admin LinuxOS：root ・1 つの特権アカウント名を 2 名以上で共用しない ・Guest 用アカウントは無効化する	・従業員番号 ・従業員コード
パスワード	＜パスワードに使う文字＞	＜パスワードに使う文字＞

	・12 文字以上 ・当人の名前、電話番号、誕生日等、他者が推測できるものを使わない ・アルファベット大文字･小文字、数字、記号の全てを含む ・辞書に含まれる単純な語を使わない ＜パスワードの管理＞ ・システムにパスワードポリシー設定機能がある場合は本項の条件を設定する ･過去 1 年間に使用したパスワードと同一パスワードを使用しない ・ロックアウトのしきい値は 3 回、時間は 6 時間に設定する	・10 文字以上 ・当人の名前、電話番号、誕生日等、他者が推測できるものを使わない ・アルファベット大文字･小文字、数字、記号の全てを含む ・辞書に含まれる単純な語を使わない ＜パスワードの管理＞ ・システムにパスワードポリシー設定機能がある場合は本項の条件を設定する ･過去 1 年間に使用したパスワードと同一パスワードを使用しない ・ロックアウトのしきい値は 5 回、時間は 1 時間に設定する

9.4 機器の認証方法

MAC アドレス	受信側のルーターで設定
IP アドレス	受信側のルーターもしくはサーバー
ドメイン名	受信側のルーターもしくはサーバー

5	物理的対策	制定日	2019.05.01
適用範囲	全事業所		

1. セキュリティ領域の設定

当事務所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	本社受付・応接スペース・商談室・倉庫
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	ー
侵入検知	ー
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	本社執務室・社長室・書庫・工場・営業所
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	入退室を所定様式に記録
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

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

設置可能情報機器	サーバー、ルーター等のネットワーク機器
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	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

2.関連設備の管理

情報機器に関連する設備は以下を設置する。

・サーバー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床下配線とする。

3.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かかわらず以下の点に注意する。

・複合機、プリンタに原稿、印刷物を放置しない。

・FAX 送信時には誤送信防止のため宛先を複数回確認する。

・ホワイトボードは利用後に消去する。

・室内での撮影、録音は禁止する。業務上必要な場合は、情報セキュリティ部門責任者の許可を得ること。

・応接室、会議室内及びエレベータ内では会話の盗み聞き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。

4.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。

＜本社＞

・郵便物：本社施錠ポスト/書留便の場合は総務部

・宅配便：本社 1 階受付

6	ＩＴ機器利用	制定日	2019.05.01
適用範囲	業務で利用する情報機器		

1.ソフトウェアの利用

1.1 標準ソフトウェア

業務に利用するパソコンには、当事務所の標準ソフトウェアを導入する。当事務所の標準ソフトウェア以外のソフトウェアを導入する場合は、システム管理者の許可を得たうえで導入する。標準ソフトウェアは「6.1 標準ソフトウェア」を参照のこと。

1.2 ソフトウェアの利用制限

システム管理者は、利用者の業務に不要な機能をあらかじめ取除いて提供する。従業員は、業務に不要なシステムユーティリティやインストールされているソフトウェアを利用しない。

＜利用を禁止するソフトウェア＞

・インターネット上で、不特定多数のコンピュータ間でファイルをやりとりできるソフトウェア（ファイル共有ソフト）。

・不審なベンダーが提供するソフトウェア。

・正規ライセンスを取得していないソフトウェア。

1.3 ソフトウェアのアップデート

従業員は、業務で使用するソフトウェアを最新の状態で利用する。最新の状態で利用する方法は「6.2 ソフトウェアのアップデート方法」を参照のこと。

1.4 ウイルス対策ソフトウェアの利用

1.4.1 ウイルス検知

従業員は、以下の方法でウイルス検知を行う。

・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。

1.4.2 ウイルス対策ソフト定義ファイルの更新

従業員は、パソコン・スマートフォン・タブレット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。持ち出し用ノートパソコンは利用時に定義ファイルの更新を確認する。定義ファイルの更新方法は「6.3 ウイルス対策ソフトウェアの定義ファイルの更新方法」を参照のこと。

1.4.3 社外機器の LAN 接続

当事務所が管理するパソコン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、システム管理者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。

1.5 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。

2. ＩＴ機器の利用

従業員は、業務に利用するパソコン・タブレット・スマートフォンには、ログインパスワードを設定する。利用するときには以下を実行する。

・ログインパスワードを他者の目に触れる所に書き記さない。
・屋外で利用する場合は、他者が画面を盗み見可能な環境で利用しない。
・退社時又は使用しないときには電源を切り、ノートパソコン・タブレット・スマートフォン・USB メモリ、HDD、CD 等の電子媒体は施錠保管する。

3.クリアデスク・クリアスクリーン

3.1 クリアデスク

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パソコン、USB メモリ、HDD、CD 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。
・離席時に書類を伏せる、引き出しに入れる等する。
・退社時又は使用しないときには机の引き出しに保管し、施錠する。

3.2 クリアスクリーン

従業員は、離席時に以下のいずれかによりパソコンの画面をロックし、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［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パソコンの電源を切る。
・スマートフォン・タブレットを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。

4.インターネットの利用

従業員は、インターネットを利用する際には以下を遵守する。

4.1 ウェブ閲覧

システム管理者は、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/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及び社用メールアドレス登録を禁止する。
・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許可を得る。
・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。
・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。

4.2 オンラインサービス

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、システム管理者の許可を得る。利用する際には以下に注意する。

＜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。

＜オンラインストレージ＞

・社外秘又は極秘の情報資産を保存する場合は、システム管理者の許可を得る。
・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。
・不審なベンダーが提供しているサービスの利用を禁止する。

4.3 SNS の利用

・当事務所の業務に関わる情報の書き込みは行わない。
・取引先従業者と SNS 上で私的に交流する場合、双方の立場をわきまえ、社会人として良識の範囲で交流する。
・SNS 用のアプリケーションが提供するセキュリティ設定を行い、アカウントの乗っ取りやなりすましに注意する。
・使用するパソコン、スマートフォン、タブレット上のデータ、写真、位置情報が、予期せず公開される可能性のあることに注意する。

4.4 電子メールの利用

従業員は、業務で電子メールを利用する際には以下を実施する。

＜誤送信防止＞

・電子メールソフトの即時送信機能を停止する。

＜メールアドレス漏えい防止＞

・同報メール（外部の多数相手に同時に送信するとき）を送信する場合は、宛先（TO）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。

＜傍受による漏えい防止＞

・社外秘又は極秘の情報資産を送信する場合は、メール本文ではなく添付ファイルに記載し、ファイルを暗号化して送信する。

＜添付ファイル暗号化の方法＞

パスワード保護の設定又はパスワード付きの ZIP ファイルにする。/パスワードは先方とあらかじめ決めておくか電話で知らせるなど、パスワードが傍受されないよう配慮する。

＜クラウド型メールの利用＞

・業務でクラウド型メールを利用する場合は、システム管理者の許可を得る。

・システム管理者から許可されたパソコン以外で、メールサーバーからのメールの取り出し及びエクスポートを禁止する。

＜禁止事項＞

・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ーへの接続。

・私用メールアドレスへの転送。

・受信メールの HTML 表示（テキスト形式に変換して表示）。

・HTML 形式メールの中に含まれる不正なコードを実行しないよう以下を設定する。

・プレビューウィンドウを無効化する。

・モバイルコード実行を無効に設定する。

4.5 ウイルス感染の防止

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、以下の内容に複数合致する場合は十分に注意し、添付ファイルを開く、又はリンクを参照するなどしない。受信した場合は、システム管理者に報告し、システム管理者は社内に注意を促す。

メールのテーマ	①知らない人からのメールだが、メール本文のURL や添付ファイルを開かざるを得ない内容 ･新聞社や出版社からの取材申込や講演依頼 ･就職活動に関する問い合わせや履歴書送付 ･製品やサービスに関する問い合わせ、クレーム ･アンケート調査

	②心当たりのないメールだが、興味をそそられる内容 ·議事録、演説原稿などの内部文書送付 ·VIP 訪問に関する情報 ③これまで届いたことがない公的機関からのお知らせ ·情報セキュリティに関する注意喚起 ·インフルエンザ等の感染症流行情報 ·災害情報 ④組織全体への案内 ·人事情報 ·新年度の事業方針 ·資料の再送、差替え ⑤心当たりのない、決裁や配送通知（英文の場合が多い） ·航空券の予約確認 ·荷物の配達通知 ⑥IDやパスワードなどの入力を要求するメール ·メールボックスの容量オーバーの警告 ·銀行からの登録情報確認
差出人のメール アドレス	①フリーメールアドレスから送信されている ②差出人のメールアドレスとメール本文の署名に記載されたメール アドレスが異なる
メールの本文	①日本語の言い回しが不自然である ②日本語では使用されない漢字（繁体字、簡体字）が使われている ③実在する名称を一部に含むURL が記載されている ④表示されているURL（アンカーテキスト）と実際のリンク先のURL が異なる（HTML メールの場合） ⑤署名の内容が誤っている ·組織名や電話番号が実在しない ·電話番号がFAX 番号として記載されている
添付ファイル	①ファイルが添付されている ②実行形式ファイル(exe/scr/cplなど)が添付されている ③ショートカットファイル(lnkなど)が添付されている ④アイコンが偽装されている ·実行形式ファイルなのに文書ファイルやフォルダーのアイコンと なっている ⑤ファイル拡張子が偽装されている ·二重拡張子となっている ·ファイル拡張子の前に大量の空白文字が挿入されている

	･ファイル名にRL04が使用されている

5.私有ＩＴ機器・電子媒体の利用

従業員個人が所有するパソコン、タブレット、スマートフォン、携帯電話等のＩＴ機器及びUSBメモリ、HDD、CD 等の電子媒体を業務で利用する場合は、システム管理者の許可を得る/利用することを禁止する。

5.1 利用開始時

利用を開始する前に利用する本人が以下を実行する。

・システム管理者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、定義ファイルを更新する。
・ハードディスク、電子媒体に対してウイルスチェックを行う。
・業務に支障が出る可能性があるソフトウェアを削除する。
・当事務所で契約したサービス以外の Wi-Fi スポットの利用は禁止する。

5.2 利用期間中

利用期間中は、利用するＩＴ機器や電子媒体に以下に該当する機能がある場合には実行する。

・ウイルス対策ソフトウェアの定義ファイルを常に最新版に更新する。
・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。
・社内 LAN へのリモート接続は禁止する/する場合はシステム管理者の許可を得る。
・社外から社内 LAN にリモートで接続する場合は以下を遵守する。
・システム管理者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。
・端末機器から離れる場合は、端末機器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端末機器を紛失した場合は、直ちにシステム管理者に連絡し指示に従う。
・社用メールアドレスで受信したメールを従業員個人のアドレスに転送することを禁止する。
・社内で利用したデータを従業員個人のアドレスに送信することを禁止する。
・社外秘又は極秘の情報資産の保存を禁止する。
・以下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。
  ･機器ベンダーの公式な公開場所（App Store、Google Playなど）以外から提供されるもの
  ･不審なベンダーが提供するもの
  ･正規ライセンスを取得していない違法なもの
・会社で契約したサービス社外の Wi-Fi サービスの利用を禁止する。
・自宅や屋外で利用する場合は以下を遵守する。
・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システム管理者に問い合わせる。

5.2.1 社内での利用

利用期間中にＩＴ機器や電子媒体を社内に持ち込む場合は、システム管理者の許可を得る。社内で利用する場合は以下を実行する。/ことを禁止する。

・社内 LAN への接続は禁止する/する場合はシステム管理者の許可を得る。

・充電を除き、社内のパソコンやサーバーへの接続は禁止する。

5.3 利用終了時

利用を終了する際には、システム管理者が指定するツールを使用してＩＴ機器業務で利用したデータを完全に消去し、復元できない状態にしてシステム管理者の了解を得る。

6.標準等

6.1 標準ソフトウェア

種別	名称	開発・販売元	バージョン
パソコン OS	Windows	MicroSoft	10.0 以降
オフィス系ソフト	Office	MicroSoft	2013 以降
電子メール	Outlook	MicroSoft	2013 以降
パソコン用ウイルス対策	マカフィーリブセーフ	McAfee	Ver.16.0 以降
スマートフォン用ウイルス対策	マカフィーリブセーフ	McAfee	Ver.16.0 以降
ブラウザ	Internet Explore	MicroSoft	Ver.11.0 以降

6.2 ソフトウェアのアップデート方法

種別	名称	開発・販売元	アップデート方法
パソコン OS	Windows10	MicroSoft	更新プログラムを自動的にインストールする を選択する
業務用ソフト	Office2016	MicroSoft	Windows Update の自動更新機能を有効にする
	Adobe Reader	Adobe	自動アップデートを有効にする。
ブラウザ	Internet Explore	MicrOSoft	Windows Update の自動更新機能を有効にする
スマートフォン	Android	Google	機種毎の情報を常に調べて

OS			必要に応じて対応する。
	iOS	Apple	iOS アップデート

6.3 ウイルス対策ソフトウェアの定義ファイルの更新方法

種別	名称	開発・販売元	アップデート方法
パソコン用 ウイルス対策	マカフィーリブセーフ	McAfee	定義ファイル更新方法を自動に設定する
スマートフォン用 ウイルス対策	マカフィーリブセーフ	McAfee	定義ファイル更新方法を自動に設定する

7	ＩＴ基盤運用管理	制定日	2019.05.01
適用範囲	サーバー・ネットワーク及び周辺機器		

1.管理体制

システム管理者は、ＩＴ基盤の運用に当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。

1.1 ＩＴ基盤の情報セキュリティ対策

ＩＴ基盤の運用の際には以下の技術的情報セキュリティ対策を考慮すること。

1.1.1 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、システム管理者の許可を得て導入する。サーバー機器の情報セキュリティ要件は、「6.1 サーバー機器情報セキュリティ要件」を参照のこと。

1.1.2 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、システム管理者の許可を得て導入する。標準ソフトウェアは「6.2ＩＴ基盤標準ソフトウェア」を参照のこと。

1.1.3 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、システム管理者の許可を得て導入する。ネットワーク機器の情報セキュリティ要件は、「6.4 ネットワーク機器情報セキュリティ要件」を参照のこと。

2.ＩＴ基盤の運用

システム管理者は、ＩＴ基盤の運用を行う際には以下を実施すること。

・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。
・以下に従い、ゲートウェイにおける通信ログを取得及び保存する。
  ➢通信ログの保存期間は 3 年間とする。
  ➢ログファイルの保存状況について、システム管理者が定期的に確認する。

・システム管理者は、通信ログについて以下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
・システム管理者は、必要に応じて業務に不要なウェブサイト閲覧を社内周知/ウェブフィルタリングソフトを使用して制限する。
・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。

3.クラウドサービスの導入

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。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、システム管理者の許可を得て導入する。サービスプロバイダの情報セキュリティ対策の評価基準は「6.5 クラウドサービス情報セキュリティ対策評価基準」を参照のこと。

4.脅威や攻撃に関する情報の収集

システム管理者は、最新の脅威や攻撃に関する情報収集を行い、必要に応じて社内で共有する。

5.廃棄・返却・譲渡

システム管理者は、ＩＴ基盤で利用した機器を返却、廃棄、譲渡を行う場合は、内部記憶媒体の破壊又は専用ツールによりデータを完全に消去し、情報セキュリティ責任者の承認を得たうえ返却、廃棄、譲渡を行う。内部記憶媒体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。

6.クラウドサービス情報セキュリティ対策評価基準

・サービスプロバイダが公表する情報セキュリティ又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こと。
・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こと。
・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。

＜適合性評価制度の種類＞

  ➢ISMS 適合性評価制度（ISMS 認証/ISMS クラウドセキュリティ認証）
  ➢プライバシーマーク制度
  ➢PCI DSS（クレジットカード業界セキュリティ基準）
  ➢ASP・SaaS の安全・信頼性に係る情報開示認定制度
  ➢インターネット接続安全安心マーク

8	システム開発及び保守	制定日	2019.05.01
適用範囲	当事務所が独自に開発する情報システム		

1. 情報システムの開発

1.1 新規システム開発・改修

情報システムの開発・改修を行う際には、以下の工程を経て実施する。各工程の完了時にシステム管理者の承認を得る。

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

1.2 脆弱性への対処

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システム管理者が判断し、承認する。

1.3 情報システムの開発環境

情報システムの開発及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、システム管理者の承認を得る。

1.4 情報システムの保守

情報システムの保守を、開発元又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及びハードウェアの製造者が提供するサポートが終了した場合、他のソフトウェアやハードウェアを用いた再構築又は当該情報システムの利用停止を検討し、システム管理者の承認を得る。

1.5 情報システムの変更

情報システムのハードウェア又はソフトウェアの変更を行う際には、以下の工程を経て実施する。各工程の完了時にシステム管理者の承認を得る。

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

9	委託管理	制定日	2019.05.01
適用範囲	情報資産を取り扱う業務の委託		

1. 委託先の評価（クラウドサービスの利用を除く）

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、委託先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定等を整備している
	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・媒体の取り扱い	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

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。

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。

①当事務所の社外秘又は極秘の情報資産及び個人情報の守秘義務

②再委託についての事項

③事故時の責任分担についての事項

④委託業務終了時の当事務所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

⑤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
⑥契約内容が遵守されない場合の措置
⑦事故発生時の報告方法

1.4 委託先の評価

委託開始後には、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。

1.5 再委託

当事務所が委託する業務を、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、当事務所の「1.1 委託先評価基準」「1.3 委託契約の締結」「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

10	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	制定日	2019.05.01
適用範囲	情報資産及び保有する個人データに関わるインシデント		

1. 対応体制

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	代表者
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

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	代表者 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

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、発見者は所定の連絡網に従い、対応者に速やかに報告し、指示を仰ぐ。

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	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

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発見者は即座にインシデント対応責任者及び代表者社長に報告する。 ②インシデント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インシデント対応責任者は被害者/本人対応を準備する。 ④インシデント対応責任者は問い合せ対応を準備する。 ⑤インシデント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報道発表の準備を申請する。 ⑥インシデント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インシデント対応責任者は個人データ*または特定個人情報漏えいの場合には個人情報保護委員会に報告する。 ⑧代表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。 *個人データ：個人情報データベース等（特定の個人を検索できるようにまとめたもの）を構成する個人情報	代表者 インシデント対応責任者
2	①発見者は発見次第、システム管理者に報告する。 ②システム管理者は漏えい先を調査し、インシデント対応責任者に報告する。 ③システム管理者は社内関係者に周知する。	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	

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発見者は即座にインシデント対応責任者及び代表者社長に報告する。 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インシデント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・フィルム原本の場合は情報セキュリティ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。 代表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。	代表者 インシデント対応責任者
2	①発見者は発見次第、システム管理者に報告する。 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インシデント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・フィルム原本の場合は情報セキュリティ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発見者は発見次第、システム管理者に報告する。 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・フィルム等の原本の場合は情報セキュリティ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	発見者は発見次第、発生可能性のあるインシデントと想定される被害をシステム管理者に報告する。	システム管理者

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。

①ネットワークからコンピュータを切断する。

②システム管理者に連絡する。

③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。

④ウイルス対策ソフトを実行しウイルス名を確認する。

⑤ウイルス対策ソフトで駆除可能な場合は駆除する。

⑥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。

⑦システム管理者に報告する。

以下の場合など従業員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。

4.5 届出及び相談

システム管理者は、インシデント対応後に以下の機関への届け出又は相談を検討する。

＜届出・相談・報告先＞

【独立行政法人 情報処理推進機構セキュリティセンター(IPA/ISEC)】

➢ウイルスの届出

https://www.ipa.go.jp/security/outline/todokede-j.html

TEL: 03-5978-7518

E-mail：virus@ipa.go.jp

➢不正アクセスに関する届出

E-Mail：crack@ipa.go.jp

FAX：03-5978-7518

➢情報セキュリティ安心相談窓口

https://www.ipa.go.jp/security/anshin/index.html

TEL:03-5978-7509

E-mail：anshin@ipa.go.jp

【個人情報保護委員会】

➢個人データ（特定個人情報に係るものを除く。）の漏えい、滅失又は毀損

➢加工方法等情報（匿名加工情報の加工の方法に関する情報等）の漏えい

➢これらのおそれ

※次の URL 内の指示（様式等）に従うこと

https://www.ppc.go.jp/personal/legal/leakAction/

TEL：03-6457-9685
FAX：03-3597-4560
郵送：〒100-0013 東京都千代田区霞が関３－２－１霞が関コモンゲート西館 32 階
個人情報保護委員会事務局　個人データ漏えい等報告窓口宛
➢特定個人情報の漏えい事案等
https://www.ppc.go.jp/legal/rouei/
郵送：〒100 - 0013 東京都千代田区霞が関３－２－１ 霞が関コモンゲート西館 32 階
個人情報保護委員会事務局　特定個人情報漏えい等報告窓口 宛
※重大事態又はそのおそれのある事案が発覚した場合には、第一報を FAX で報告する
FAX: 03-3593-7962

5.事業継続計画

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及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。