ブレインパートナーグループ

情報セキュリティ関連規定

目　次

（Ver.1.6）

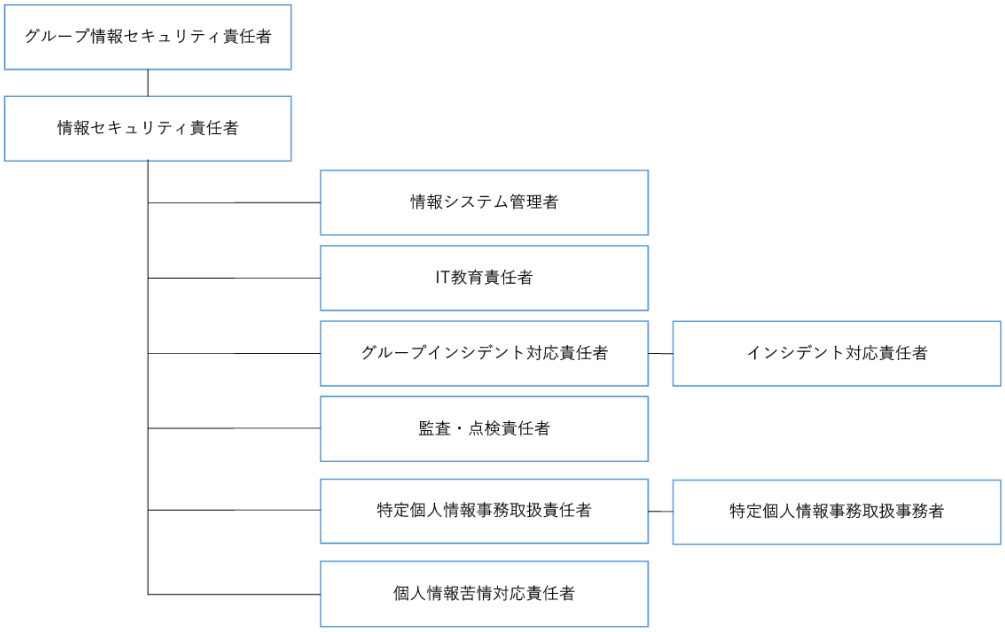
ブレインパートナーグループ情報セキュリティ関連規定

1	組織的対策	改訂日	2024.12.01
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を推進するための組織として、会社組織内にIT委員会を親とする情報セキュリティ分会を設置する。情報セキュリティ分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。

役割名	担当役職	役割と責任
グループ情報セキュリティ責任者	担当役員（IT委員会担当）	情報セキュリティに関する責任者。グループ共通の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 責任者	各部門長及びIT委員長	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。
情報システム管理者	IT委員長及び副委員長	情報セキュリティ対策のための各部門におけるシステム管理を行う。
IT教育責任者	情報セキュリティ委員	情報セキュリティ対策を推進するためにグループの従業員への教育を企画・実施する。
グループインシデント対応責任者	担当役員・IT委員長	事故の影響を判断し、グループ全体の対応について意思決定する。
インシデント対応責任者	各部部課長	事故の影響を判断し、各部門の対応について意思決定する。
監査・点検責任者	IT委員	情報セキュリティ対策が各部門で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評価し、助言を行う。
特定個人情報事務取扱責任者	各部部長	各部門における特定個人情報の情報セキュリティに関する責任者。
特定個人情報事務取扱担当者	特定個人情報事務取扱担当者	各部門における特定個人情報を取り扱う事務に従事する従業員。
個人情報苦情対応責任者	総務部長	個人情報に関する苦情の対応責任者。

＜ブレインパートナーグループ情報セキュリティ分会体制図＞



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、情報セキュリティ関連規程の実施状況について、9月に点検を行い、監査・点検結果を情報セキュリティ分会に報告する。情報セキュリティ分会は、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、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、分会で共有する。

＜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/

4.情報セキュリティ関連規定のグループ内適用範囲

ブレインパートナーグループ
・税理士法人ブレインパートナー
・株式会社ブレインパートナー
・社労士法人ブレインパートナー
・行政書士法人ブレインパートナー
・株式会社bpコンサルティング

2	人的対策	改訂日	2024.12.01
適用範囲	全従業員（役員、正社員、派遣社員、パート・アルバイトを含む）		

1.雇用条件
各グループが従業員を雇用する際には秘密保持契約を締結する。

2.従業員の責務
従業員は、以下を順守する。
- 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。
- 従業員は、当社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、就業規則に準じる。

※当社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
- 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。
- 従業員は、在職中に知り得た当グループ及びその顧問先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
IT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
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）
- 個人情報の取り扱いに関する留意事項
- 税理士法等の関連業法を遵守するために必要となる事項や管轄団体からの通達

3	情報資産管理	改訂日	2024.12.01
適用範囲	全社・全従業員		

1.情報資産の管理

1.1情報資産の特定と機密性の評価

当社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。情報資産の機密性は、以下の基準に従って評価する。

機密性1：秘密	● 法律で安全管理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 ● 限定提供データ（一定の条件を満たす特定の外部者に提供することを目的とする情報）として指定されている ● 営業秘密（秘密として管理されているもの）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 ● 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ほとんど影響はない

1.2情報資産の分類の表示

情報資産の機密性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表示
- 書類：保管先キャビネット、ファイル、バインダーに表示
- 表示が困難な場合は、「情報資産管理台帳」に機密性評価値を表示する。

1.3情報資産の管理責任者

情報資産の取り扱い関する情報セキュリティ責任者は、当該情報資産を利用する各部門長及びIT委員長とする。

1.4情報資産の利用者

情報資産の利用者の範囲は、「情報資産管理台帳」の利用者範囲欄に示された部門に従事する従業員とする。

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。

- 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、セキュリティロックを設定する。
- 情報の持ち出し、持ち帰りには、可能な限りBOXシステムを利用し、外部媒体等への保存は行わない
- 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、以下の何れかの方法で暗号化を行う
  - 持ち出し情報を暗号化する
  - 持ち出す媒体を暗号化する
  - 暗号化機能付き媒体を使用する
- USBメモリ等の小型電子媒体は、ストラップで体やカバンに固定する。
- 屋外でネットワークへ接続して秘密の情報資産を送受信する場合は、暗号化する。また、顧問先ネットワークや公衆wifi等の、グループが管理しないネットワークへの接続は行わない。
- 携行中は常に監視可能な距離を保つ。
- 携行中の飲酒は禁止する。

3.媒体の処分

3.1媒体の廃棄

秘密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	溶解、クロスカットまたはマイクロクロスカット
USBメモリ・HDD・CD・DVD	破壊 ※OSによる削除・クイックフォーマットは不可

3.2媒体の再利用

秘密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	秘密の情報資産が記載された裏紙は再利用禁止
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による削除・クイック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

情報システム管理者は、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	専用外付けHDD（暗号化機能付）
会計システム	アプリケーションデータ	アプリケーションのクラウドバックアップ機能	クラウドバックアップサービス
Webサーバー	ホームページ	同期ツール	NASサーバー または レンタルサーバー
クラウドストレージ	ユーザーファイル	アプリケーションのクラウドバックアップ機能	クラウドバックアップサービス
グループウェア	ユーザーファイル	アプリケーションのクラウドバックアップ機能	クラウドバックアップサービス

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こと。

4	アクセス制御及び認証	改訂日	2024.12.01
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
秘密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
秘密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は、利用目的を明確にし、その利用目的以外の目的では使用しない。
- 複数の利用者が共有するアカウントは、そのパスワードについて定期的に変更を行う。

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、担当役員又は代表社員もしく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、情報システム管理者は、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
当社の従業員以外の者にアカウントを発行する場合は、担当役員 又は代表社員 もしく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
秘密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、機器の識別または二段階認証を施したID・パスワード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
秘密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
会計システム	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
クラウドストレージ	アプリケーションのユーザー認証
グループウェア	アプリケーションのユーザー認証

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
会計システム	アプリケーションのユーザー認証：ID・パスワード
クラウドストレージ	アプリケーションのユーザー認証：ID・パスワード
グループウェア	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 申告ソフトの顧問先登録を行うアカウント等	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 ● 従業員個人に付与されているメールアドレス
パスワード	＜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	＜パスワードに使う文字＞ ● 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 ● 共有アカウントのパスワードは、利用者の退職があるごとに変更を行う。

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
Windowsのログオン情報	

5	物理的対策	改訂日	2024.12.01
適用範囲	全事業所		

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・応接スペース・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	未使用時に秘密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	－
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	執務室・役員室・書庫
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	あらかじめ許可された者
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。

- 部外者が立ち入り可能なエリアにおいて、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。または、登録済み電話帳以外からは送信できない。
- 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：施錠ポスト/書留便の場合は総務部
- 宅配便：事務所受付

6	IT機器利用	改訂日	2024.12.01
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、当社の標準ソフトウェアを導入する。当社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、情報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
情報システム管理者は、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。
- 情報システム管理者の利用許可を得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
当社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、情報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
情報システム管理者は、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、秘密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、机の上の書類等が見えないようにカバーをする。
- 不要な電子機器及び資料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
情報システム管理者は、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情報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、情報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＞

- 秘密の情報資産を保存する場合は、情報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。
- 情報システム管理者の利用許可を得ていないサービスの利用を禁止する。

4.3 SNSの個人利用

- 当社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＞

- 秘密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。オンラインストレージ等を利用できる場合は、ダウンロード用URLを共有し、ファイルを直接添付しない。

＜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。（添付ファイルを送信したメールを再利用してパスワードを送付する方法を禁止する）

＜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、情報システム管理者の許可を得る。
- 情報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。

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、情報システム管理者に報告し、情報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RLO4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ことを禁止する。

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	11以降
オフィス系ソフト	Office	Microsoft	2020以降
電子メール	Outlook	Microsoft	2020以降
	Gmail	google	-
スマートフォン用 ウイルス対策	アバスト モバイル セキュリティ	AVAST Software	-
ブラウザ	Chrome	google	-
	Edge	Microsoft	-
その他	定めるもの	-	-

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	Windows11	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	Office2020	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	Chrome	google	自動アップデートを有効にする。
	Edge	Microsoft	自動アップデートを有効にする。
スマートフォンOS	Android	Google	機種毎の情報を常に調べて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	･YARAI ･ITpolicy N@vi TKCサイバーセキュリティーサービス Windows Deffender	FFRI TKC Windows	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	携帯電話キャリアが提供するサービスならびにAvast	-	定義ファイル更新方法を自動に設定する
タブレット用 ウイルス対策	携帯電話キャリアが提供するサービスならびにAvast	-	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	改訂日	2024.12.01
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
情報システム管理者は、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。

2.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。

2.1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、情報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。

2.2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、情報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。

2.3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、情報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。

3.IT基盤の運用
情報システム管理者は、IT基盤の運用を行う際には以下を実施すること。

- 情報システム管理者は、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、情報システム管理者が定期的に確認する。
- 情報システム管理者は、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
- 情報システム管理者は、ウェブフィルタリングソフトを使用して必要に応じて業務に不要なウェブサイト閲覧を制限する。
- 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。

4.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、情報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、情報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。

5.脅威や攻撃に関する情報の収集
情報システム管理者は、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。

6.廃棄・返却・譲渡
情報システム管理者は、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。

7.IT基盤標準
IT基盤で利用する機器及びソフトウェアの情報セキュリティ要件と、それに基づく当社標準を以下とする。

7.1サーバー機器情報セキュリティ要件

対象システム	セキュリティ要件	利用技術・製品
ファイルサーバー	利用者認証機能	Windows Active Directory
	セキュリティログ取得機能	Windows
	システムログ取得機能	Windows
	ユーザーアクセスログ取得機能	SKYSERVER
	ハードディスク：容量2TB以上	RAID構成を必須とする
NASサーバー	利用者認証機能	
	ディスク暗号化機能	
	ハードディスク：容量2TB以上	
BOX	利用者認証機能	BOXセキュリティ設定
	セキュリティログ取得機能	

7.2IT基盤標準ソフトウェア
Windows Server を基幹として、TKCならびにベンダーとの協議により決定する。

7.3標準ネットワーク機器
TKCならびにベンダーとの協議により決定する。

7.4ネットワーク機器情報セキュリティ要件
TKCならびにベンダーとの協議により決定する。

7.5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）
  - 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
  - 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	改訂日	2024.12.01
適用範囲	当社が独自に開発する情報システム		

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。各工程の完了時に情報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

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情報システム管理者が判断し、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

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、情報システム管理者の承認を得る。

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、情報システム管理者の承認を得る。

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。各工程の完了時に情報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	改訂日	2024.12.01
適用範囲	情報資産を取り扱う業務の委託		

1.委託先評価基準
情報セキュリティ責任者は「情報資産管理台帳」の重要度が1以上である情報資産の取り扱う業務を、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＞
- SECURITY ACTION 二つ星に取り組んでいる。
- 情報セキュリティ監査を定期的に実施している。
- 情報セキュリティに関する方針を公開している。
- 「委託先情報セキュリティ対策状況確認リスト」で全ての対策を実施している。

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。

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。
- 当社の秘密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秘密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
    - ○ *（参考情報：9-1　業務委託契約に係る機密保持条項）*

4.委託先の評価
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。委託先における情報セキュリティ対策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「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。

（参考情報：9-2　委託先情報セキュリティ対策実施状況確認リスト）

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「1.委託先評価基準」「3.委託契約の締結」「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
9-1. 業務委託契約に係る機密保持条項

第1条（機密保持）
1.甲及び乙は、本契約の履行に当たり、相手方が機密である旨指定して開示する情報及び本契約の履行により生じる情報（以下「機密情報」という）を機密として取り扱い、相手方の事前の書面による承諾なく第三者に開示してはならない。ただし、次の各号のいずれかに該当する情報については、この限りではない。
①開示を受けたときに既に公知であったもの
②開示を受けたときに既に自ら所有していたもの
③開示を受けた後に自らの責によらない事由により公知となったもの
④開示を受けた後に第三者から守秘義務を負うことなく適法に取得したもの
⑤開示の前後を問わず自らが独自に開発したことを証明し得るもの

2.甲が乙に機密である旨指定して開示する情報は、別表1（本案では、特に例示しない）、乙が甲に機密である旨指定して開示する情報は、別表2（本案では、特に例示しない）の通りである。なお、別表1及び別表2は甲乙協力し常に最新の状態を保つべく適切に更新するものとする。

3. 甲及び乙は、相手方より開示された機密情報の管理につき、自ら保有する他の情報、物品等と明確に区別して管理するとともに、以下の事項を遵守する。
（1）機密情報の管理責任者及び保管場所を定め、善良なる管理責任者の注意をもって保管管理する。
（2）機密情報を取り扱う従業員を必要最小限にとどめ、上記保管場所以外へ持ち出さない。
（3）機密情報の管理責任者名、機密情報を取り扱う従業員名及び機密情報に関する情報セキュリティ対策を、〇年〇月〇日までに相手方に報告する。また、報告内容に変更が生じた場合には、速やかに当該変更内容を相手方に報告する。
（4）（3）にて報告した機密情報を取り扱う従業員に対して本契約の内容を周知徹底させ、機密情報の漏洩、紛失、破壊、改ざん等を未然に防止するための措置を取る。
（5）甲の書面による承諾を得た場合を除き、機密情報を複写、複製せず、また、機密情報を開示、漏洩しない。但し、政府機関又は裁判所の命令により要求された場合、その範囲で開示することが出来る。なお、その場合には、相手方にその旨を速やかに通知すること。
（6）機密情報は本契約の目的の範囲でのみ使用する。
（7）事故発生時には直ちに相手方に対して通知し、事故再発防止策の協議には相手方の参加を認める。
（8）委託期間満了時又は本契約の解除時、機密情報（（5）に基づく複写、複製を含む）を相手方に返却、又は自己で廃棄の上廃棄の証拠を相手方に報告する。
（9）（8）にかかわらず、相手方から返却また廃棄を求められたときは、機密情報（（5）に基づく複写、複製を含む）を相手方に返却、又は自己で廃棄の上廃棄の証拠を相手方に報告する。
（10）甲及び乙は、相手方に対して、機密情報の以下の具体的管理状況に関する報告を求めることができる。この報告結果をもとに、甲及び乙が相手方の事務所における機密情報の管理状況を確認するために相手方の事務所への立入検査を希望する場合には、当該検査に協力する。また、甲及び乙は相手方に対して是正措置を求めることができ、相手方はこれを実施するものとする。
①委託契約範囲外の加工、利用の禁止の遵守
②委託契約範囲外の複写、複製の禁止の遵守
③情報セキュリティ対策状況

第2条（再委託）
1.乙は、本業務（の全部、又は一部）を第三者へ再委託する場合、甲の事前の書面による同意を得ずに、再委託してはならない。

2.前項の規定に基づき本業務を再委託する場合、乙は自己が負う義務と同等の義務を再委託先に対して書面にて課すとともに、甲に対して再委託先に当該義務を課した旨を書面により報告し、

かつ乙は当該機密情報開示に伴う全責任を負うものとする。また、乙は次項第3 号の再委託先からの報告を、第1条（機密保持）第3項の具体的管理状況の報告時にあわせて甲に報告する。

3.前項に加え、乙は再委託先から次の各号の同意を得なければならない。また、乙は、当該同意を得た旨を甲に書面で報告する。
①事故発生時には直ちに甲に対しても通知すること
②事故再発防止策を協議する際には甲の参加も認めること
1　再委託先における機密情報の具体的管理状況の報告は、甲の閲覧も可とすること

第3条（権利義務の譲渡）
乙は、本契約によって生じる権利又は義務を第三者に譲渡し、又は承継させてはならない。

第4条（納入物件の知的財産権）
1.納入物件に関する著作権（著作権法第27条及び第28条に定める権利を含む。）、本契約の履行過程で生じた発明（考案及び意匠の創作を含む。）及びノウハウを含む産業財産権（特許その他産業財産権を受ける権利を含む。）（以下「知的財産権」という。）は、乙又は国内外の第三者が従前から保有していた知的財産権を除き、第1条の規定による請負業務完了の日をもって、乙から甲に自動的に移転するものとする。

2.納入物件に、乙又は第三者が従前から保有する知的財産権が含まれている場合は、前項に規定する移転の時に、乙は甲に対して非独占的な実施権、使用権、第三者に対する利用許諾権（再利用許諾権を含む。）、その他一切の利用を許諾したものとみなす。なお、その対価は契約金額に含まれるものとする。

3.乙は、甲及び甲の許諾を受けた第三者に対し、納入物件に関する著作者人格権、及び納入物件に対する著作権法第28条の権利、その他“原作品の著作者／権利者”の地位に基づく権利主張は行わないものとする。

第5条（知的財産権の紛争解決）
1.乙は、納入物件に関し、甲及び国内外の第三者が保有する知的財産権（公告、公開中のものを含む。）を侵害しないことを保証するとともに、侵害の恐れがある場合、又は甲からその恐れがある旨の通知を受けた場合には、当該知的財産権に関し、甲の要求する事項及びその他の必要な事項について調査を行い、これを甲に報告しなければならない。

2.乙は、前項の知的財産権に関して権利侵害の紛争が生じた場合（私的交渉、仲裁を含み、法的訴訟に限らない。）、その費用と責任負担において、その紛争を処理解決するものとし、甲に対し一切の負担及び損害を被らせないものとする。

第6条（損害賠償）
乙は、乙の責に帰すべき事由によって甲又は第三者に損害を与えたときは、その被った通常かつ直接の損害を賠償するものとする。ただし、乙の負う賠償額は、乙に故意又は重大な過失がある場合を除き、第3条所定の契約金額を超えないものとする。

第7条（協議）
本契約に定める事項又は本契約に定めのない事項について生じた疑義については、甲乙協議し、誠意をもって解決する。

第8条（その他）
本契約に関する紛争については、名古屋地方裁判所を唯一の合意管轄裁判所とする。

【コメント】
以下に示すような「機密保持条項に関連する他の条項」については、業務委託期間終了又は本契約の解除後も、合理的な期間にわたり存続させることが望まれます。
第〇条（権利義務の譲渡）
第〇条（成果の帰属）
第〇条（損害賠償）
第〇条（法令等の遵守義務）
第〇条（協議事項）
第〇条（紛争の解決）
また、第〇条（守秘義務）の規定は、「業務委託期間終了又は本契約の解除後〇年間有効とする」の如く有効期間を示すことが適切です。

9-2. 委託先情報セキュリティ対策状況確認リスト

会社名：　　確認者：　　確認日：

区分	No	確認項目	実施状況（〇、×）
社内体制	1	情報セキュリティ管理責任者を定めている	
	2	情報セキュリティ対策を定めた規程を整備している	
	3	情報セキュリティへの取り組み方針を従業員や取引先に周知している	
	4	情報セキュリティ事故に対する対応手順を整備している	
	5	定期的に情報セキュリティに関する内部点検を実施している	
人的管理	6	情報セキュリティに関する教育を定期的に実施し、受講記録を作成している	
	7	従業員と守秘義務契約を交わしている	
物理的管理	8	関係者以外の事務所への立ち入りを制限している	
	9	機密情報の保管について施錠管理をしている	
	10	機密情報を保管している領域に入ることができる人を制限し、入退出記録を取得している	
	11	入退出記録を定期的に確認している	
情報機器・媒体の取り扱い	12	機器・媒体の盗難防止措置を講じている	
	13	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	
	14	媒体の移送、受け渡し時の保護措置を講じている	
	15	媒体の安全な消去、廃棄の手順を整備している	
技術的対策	16	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	
	17	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	
	18	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	
再委託先管理	19	重要情報の授受を伴う委託先との契約書には、秘密保持条項を規定している	
	20	重要情報の授受を伴う委託先には自社と同等の情報セキュリティ対策を求めている	

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	改訂日	2024.12.01
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	グループ情報セキュリティ責任者
対応責任者	グループインシデント対応責任者 及び インシデント対応責任者
一次対応者	発見者又は情報システム管理者

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	責任者
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	グループ情報セキュリティ責任者
2	事業に影響が及ぶとき	グループインシデント対応責任者 及び 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	グループインシデント対応責任者 及び インシデント対応責任者
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	情報システム管理者

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、発見者は以下の連絡網に従い、対応者または責任者に速やかに報告し、指示を仰ぐ。

対応者または責任者	担当役職	緊急連絡先
グループ情報セキュリティ責任者	担当役員	携帯電話：090-****-**** 電子メールアドレス：president@****.co.jp
情報セキュリティ責任者	各部門長及びIT委員長	携帯電話：090-****-**** 電子メールアドレス：president@*****.co.jp
情報システム管理者	IT委員長及び副委員長	携帯電話：090-****-**** 電子メールアドレス：president@****.co.jp
IT教育責任者	情報セキュリティ委員	携帯電話：090-****-**** 電子メールアドレス：president@****.co.jp
グループインシデント対応責任者	担当役員・IT委員長	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	各部部課長	携帯電話：090-****-**** 電子メールアドレス：president@****.co.jp

監査･点検責任者	IT委員	携帯電話：090-****-**** 電子メールアドレス：president@****.co.jp
特定個人情報事務取扱責任者	各部部長	携帯電話：090-****-**** 電子メールアドレス：president@****.co.jp
特定個人情報事務取扱担当者	各部IT委員	携帯電話：090-****-**** 電子メールアドレス：president@****.co.jp
個人情報苦情対応責任者	総務部長	携帯電話：090-****-**** 電子メールアドレス：president@****.co.jp 携帯電話：090-****-**** 電子メールアドレス：president@****.co.jp

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	秘密情報資産の盗難、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

4.1漏えい・流出発生時の対応

事故レベル	対応手順
3	1. 発見者は即座にグループインシデント対応責任者 及びインシデント対応責任者及びグループ情報セキュリティ責任者に報告する。 2. グループインシデント対応責任者 及び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. グループインシデント対応責任者 及び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. グループインシデント対応責任者 及びインシデント対応責任者は問い合わせ対応を準備する。 5. グループインシデント対応責任者 及び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. グループインシデント対応責任者 及び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. グループインシデント対応責任者 及び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. 代表取締役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
2	1. 発見者は発見次第、情報システム管理者に報告する。 2. 情報システム管理者は漏えい先を調査し、グループインシデント対応責任者 及びインシデント対応責任者に報告する。 3. 情報システム管理者は社内関係者に周知する。
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
3	1 発見者は即座にグループインシデント対応責任者及びインシデント対応責任者及び代表取締役社長に報告する。 2 情報システム管理者は原因を特定し、応急処置を実行する。 3 グループインシデント対応責任者及びインシデント対応責任者は社内に周知するとともに情報システム管理者に連絡する。

	4 電子データの場合は情報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 機器の場合は情報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責任者が可能な範囲で修復する。 7 情報システム管理者は原因対策を実施する。 代表取締役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 発見者は発見次第、情報システム管理者に報告する。 2 情報システム管理者は原因を特定し、応急処置を実行する。 3 グループインシデント対応責任者 及び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情報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 機器の場合は情報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責任者が可能な範囲で修復する。 7 情報システム管理者は原因対策を実施する。
1	発見者は発見次第、情報システム管理者に報告する。 情報システム管理者は原因を特定し、応急処置を実行する。 電子データの場合は情報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。 機器の場合は情報システム管理者が修理、復旧、交換等の手続きを行う。 書類・フィルム等の原本の場合は情報セキュリティ責任者が可能な範囲で修復する 情報システム管理者は原因対策を実施する
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情報システム管理者に報告する。

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 情報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 情報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情報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

情報システム管理者は、インシデント対応後に以下の機関への届け出、報告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】

- 個人データの漏えい等の事案が発生した場合等の対応
  1. 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
  2. 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
  3. 上記1. 又は2. のおそれ
- 漏えい等事案が発覚した場合は、速やかに下記URを参照して個人情報保護委員会等に対し、報告すること
  - https://www.ppc.go.jp/personalinfo/legal/leakAction/
  - TEL:03-6457-9685
  - 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
- 特定個人情報の漏えい事案が発生した場合の対応
  1. 番号法違反又は違反のおそれ
     a. 番号法違反又は違反のおそれを把握した場合は、速やかに下記URを参照して個人情報保護委員会等に対し、報告すること
     b. https://www.ppc.go.jp/legal/rouei/
  2. 重大事態に該当する事案又はそのおそれ
     a. ≪重大事態≫
        i. 情報提供ネットワークシステム等又は個人番号利用事務を処理するために使用する情報システムで管理される特定個人情報が漏えい等した事態
        ii. 漏えい等した特定個人情報に係る本人の数が100人を超える事態
        iii. 特定個人情報を電磁的方法により不特定多数の者が閲覧することができる状態となり、かつ閲覧された事態
        iv. 従業員等が不正の目的をもって、特定個人情報を利用し、又は提供した事態
     b. 重大事態が発覚した場合は、直ちに下記URLを参照して個人情報保護委員会等に対し、報告すること
        https://www.ppc.go.jp/legal/rouei/
        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
        TEL:03-6457-9680

11	個人番号及び 特定個人情報の取り扱い	改訂日	2024.12.01
適用範囲	特定個人情報（マイナンバーを内容に含む個人情報）		

個人情報保護方針

1.関係法令・ガイドライン等の遵守
当社は、個人番号及び特定個人情報（以下「特定個人情報等」といいます。）の取り扱いに関し、「行政手続における特定の個人を識別するための番号の利用等に関する法律」（以下「マイナンバー法」といいます。）及び「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」、並びに「個人情報の保護に関する法律」（以下「個人情報保護法」といいます。）及び個人情報保護委員会のガイドラインを遵守します。

2.利用目的
当社は、提供を受けた特定個人情報等を、以下の目的で利用します。
当法人は、特定個人情報等を以下の利用目的の範囲内で取り扱います。

（1）従業員等に係る源泉徴収事務、社会保険関係事務および労働保険関係事務
（2）報酬、料金等に係る法定調書作成事務
（3）業務委嘱契約等に基づく年末調整事務および法定調書作成事務
（4）業務委嘱契約等に基づく税務または労務代理
（5）業務委嘱契約等に基づく税務または労務書類の作成
（6）上記（4）および（5）に付随して行う事務

3.安全管理措置に関する事項
当社は、特定個人情報等の漏えい、滅失又は毀損の防止その他の個人番号の適切な管理のために、別途規則を定め、これを遵守します。

4.委託の取り扱い
当社は、特定個人情報等の取り扱いを第三者に委託することがあります。この場合、当社は、マイナンバー法及び個人情報保護法に従って、委託先に対する必要かつ適切な監督を行います。

5.継続的改善
当社は、特定個人情報等の取り扱いを継続的に改善するよう努めます。

6.特定個人情報等の開示
当社は、本人又はその代理人から、当該特定個人情報等に係る保有個人データの開示の求めがあったときは、次の各号の場合を除き、遅滞なく回答します。
・本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
・当社の業務の適正な実施に著しい支障を及ぼすおそれがある場合
・法令に違反することとなる場合

特定個人情報等の開示に関するお問合せ、及び質問苦情等は下記までお願いいたします。

▮特定個人情報事務取扱責任者
総務部長

▮個人情報苦情対応責任者
総務部長

発効日:2024年12月1日
ブレインパートナーグループ
グループ情報セキュリティ責任者

（附　則）

この規定は、令和　6年　12月　1日から施行する。

この規定の改変は、情報セキュリティ分会にて、定期的に協議検討し、役員会の承認をもって改変する。

改定履歴

2024年12月1日

MAC&BPグループより分離、独立したためブレインパートナーグループ情報セキュリティ関連規定を作成。