情報セキュリティポリシー

1	対策（基本方針）	改訂日	2017.9.16
適用範囲	当オフィス全体		

1.情報セキュリティ基本方針

情報セキュリティ基本方針を以下のとおり定める。情報セキュリティ基本方針を当オフィスのホームページで公表する。/情報セキュリティ基本方針を顧客の要請の応じ適宜に公表する。

＜情報セキュリティ基本方針＞

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

1. オフィス内体制および情報セキュリティポリシーの整備

当オフィスは、セキュリティの維持及び改善のために必要な管理体制を整備し、必要な情報セキュリティ対策をオフィス内の正式な規則として定めます。

2.リーダーシップにおける責任および継続的改善

当オフィスの経営者は、本方針の遵守により、当オフィス及びお客様の情報資産が適切に管理されるよう主導します。

3.法令、契約上の要求事項の遵守

当オフィスは、事業活動で利用する情報資産に関連する法令、規制、規範及びお客様との契約上のセキュリティ要求事項を遵守します。

4.違反及び事故への対応

当オフィスは、情報セキュリティに関わる法令、規制、規範及びお客様との契約に関わる違反及び情報セキュリティ事故への対応のための体制を整備し、違反及び事故の影響を低減します。

2017 年 9 月 16 日

Half A half

代表　井上明彦

2.特定個人情報の適正な取扱いに関する基本方針

特定個人情報の適正な取扱いに関する基本方針を以下のとおり定める。特定個人情報の適正

な取扱いに関する基本方針を当オフィスのホームページで公表する。/特定個人情報の適正な取扱いに関する基本方針を本社各部署に掲示し、関係者に周知する。/特定個人情報の適正な取扱いに関する基本方針を本人の求めに応じ、通知する。

＜特定個人情報の適正な取扱いに関する基本方針＞

1.関係法令・ガイドライン等の遵守

当オフィスは、特定個人情報の取り扱いに関し、「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。）及び各省庁のガイドラインを遵守します。

2.利用目的

当オフィスは、提供を受けた特定個人情報を、以下の目的で利用します。

(1) 取引先様の特定個人情報等

・報酬、料金に関する支払調書作成事務

(2) 当オフィスの事業サービス上で得たユーザーの特定個人情報等

・支援機関への寄付者情報としての申請書作成事務

・アンケート調査の統計的な信頼度を計るための情報源

3.継続的改善

当オフィスは、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。

4.特定個人情報等の開示

当オフィスは、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

・当オフィス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、および質問苦情等は下記までお願いいたします。

[kiff.tokyo お問い合わせ窓口]

[https://kiff.tokyo/contact/]

2017 年 9 月 16 日

Half A half

代表　井上明彦

1	対策	改訂日	2017.9.16
適用範囲	当オフィス全体		

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に、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
システム管理者	代表
インシデント対応責任者 個人情報　苦情対応責任者	代表
監査・点検　責任者	代表
特定個人情報　事務取扱責任者	代表
特定個人情報　事務取扱担当者	代表

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、情報セキュリティポリシーの実施状況について、適宜点検を行う。情報セキュリティ委員会は、以下の点を考慮し、必要に応じて改善計画を立案する。

- 情報セキュリティポリシーが有効に実施されていない場合、その原因の特定と改善
- 情報セキュリティポリシー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、情報セキュリティポリシーの改訂
- 情報セキュリティポリシー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、情報セキュリティポリシーの改訂

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/

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	情報資産管理	改訂日	2017.9.16
適用範囲	当オフィス事業に必要で価値がある情報及び個人情報		

1.情報資産の管理

1.1 情報資産の特定と重要度の評価

当オフィス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:オフィス外秘	●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代表とする。

2.情報資産のオフィス外持ち出し

情報資産をオフィス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、ハードディスク/データ・フォルダーを暗号化する。

●スマートフォン、タブレットに保存して持ち出す場合は、セキュリティロックを設定する。

●USB メモリ、HDD 等の電子媒体に保存して持ち出す場合は、不要データは全て完全消去専用ツールで消去し、持ち出すデータを暗号化する。

●USB メモリ等の小型電子媒体は、大きなタグを付ける/ストラップで体やカバンに固定する/落としてもすぐに分かるように鈴を付ける。

●屋外でネットワークへ接続してオフィス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

オフィス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

オフィス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(主要 PC)	ユーザーファイル	バックアップツール	外付け HDD
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
Web サーバー	ホームページ	同期ツール	外付け HDD

4.2 バックアップ媒体の取扱い

バックアップに利用した機器およ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

＜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、当オフィスの情報セキュリティポリシーに適合している。
- ●当オフィス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。

3	物理的対策	改訂日	2017.9.16
適用範囲	情報処理設備が設置される領域		

1. セキュリティ領域の設定

業務上支障のない限り、ネットワーク接続を最低限にし、処理する。

また、外付け記憶媒体を適宜利用し、それらを主要 PC に接続の際もネットワークへの切断を実行する。

2. セキュリティ領域内注意事項

セキュリティ領域では区分に関わらず以下の点に注意する。

●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。

4	ＩＴ機器利用	改訂日	2017.9.16
適用範囲	業務で利用する情報処理設備･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、当オフィスの標準ソフトウェアを導入する。当オフィス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、業務に不要な機能をあらかじめ取除いて使用する。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

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

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

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。

1.5 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をする。

2. ＩＴ機器の利用

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。

4.インターネットの利用

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、閲覧を制限する。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

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、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＞

●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。

4.3ＳＮＳの利用

●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

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。

※CC 又は宛先（TO）に複数アドレスを指定すると、送信相手に複数全員のアドレスが通知され、個人情報の漏えいになります。

＜傍受による漏えい防止＞

●メールでの連絡事項は S/MIME や PGP が利用可能な場合はそれらを使用し、使用出来ない場合は取引先にパスワードを設定してもらい、添付ファイルの暗号化を励行する。

●オフィス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 7 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＞

＜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、安易に添付ファイルを開いたり、リンクを参照しない。

また、どうしても内容を確認する必要がある場合はファイルをウィルススキャンしたり、サンドボックを利用するなどする。

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

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	7 以降
オフィス系ソフト	Office	Microsoft	2007 以降
電子メール	Outlook	Microsoft	2007 以降
パソコン用ウイルス対策	Malwarebytes	MalwarebytesCorporation	Ver.2017.9.15 以降
スマートフォン用ウイルス対策	AVG アンチウイルス	AVG TECHNOLOGIES	Ver.6.53 以降
ブラウザ	Chrome	Google	Ver.61.0.3163.91 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	Windows7/10	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	Office2013	Microsoft	Microsoft 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。
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。

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	Malwarebytes	MalwarebytesCorporation	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	AVG アンチウイルス	AVG TECHNOLOGIES	定義ファイル更新方法を自動に設定する

5	ＩＴ基盤運用管理	改訂日	2017.9.16
適用範囲	情報資産を扱うサーバ・ネットワーク等のＩＴインフラ		

1. 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。

2. 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。

3. 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う。

4. 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。

5. 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、それに基づく当オフィス標準を以下とする。

6.1 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	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	Splunk

6	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	2017.9.16
適用範囲	情報セキュリティ事故対応及び事業継続管理		

1. 対応体制

情報セキュリティインシデントが発生した際には以下の体制で対応する。

最高責任者	代表

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、等に影響が及ぶとき ●個人情報が漏えいしたとき	代表
2	事業に影響が及ぶとき	代表
1	業務遂行に影響が及ぶとき	代表
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	代表

4. 対応手順

インシデントを以下の通りに区分し、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	オフィス外秘又は極秘情報資産の盗難、流出、紛失
改ざん・消失・破壊 サービス停止	情報資産の意図しない改ざん、消失、破壊 情報資産が必要なときに利用できない
ウイルス感染	悪意のあるソフトウェアに感染

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。 ②被害者/本人対応を準備する。 ③問合せ対応を準備する。 ④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。 ⑤個人情報の漏えいの場合には監督官庁に届け出る。	代表

2	①漏えい先を調査する。	代表
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原因を特定し、応急処置を実行する。。 ②電子データの場合はバックアップによる復旧を実行する。 ③機器の場合は修理、復旧、交換等の手続きを行う。 ④書類･フィルム原本の場合は可能な範囲で修復する。 ⑤原因対策を実施する。	代表
2	①原因を特定し、応急処置を実行する。 ②電子データの場合はバックアップによる復旧を実行する。 ③機器の場合は修理、復旧、交換等の手続きを行う。 ④書類･フィルム原本の場合は可能な範囲で修復する。 ⑤原因対策を実施する。	代表
1	①原因を特定し、応急処置を実行する。 ②電子データの場合は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。 ③機器の場合は修理、復旧、交換等の手続きを行う。 ④書類･フィルム等の原本の場合は可能な範囲で修復する ⑤原因対策を実施する	代表
0	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に備える。	代表

4.3 ウイルス感染時の初期対応

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。

③ウイルス対策ソフトを実行しウイルス名を確認する。

④ウイルス対策ソフトで駆除可能な場合は駆除する。

⑤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。

4.5 届出及び相談

代表は、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

7	委託契約書秘密保持条項	改訂日	2017.9.16
適用範囲	外部委託契約の締結時		

1. 委託契約時の秘密保持契約条項

オフィス half A half（以下「甲」という。）と貴社（以下「乙」という。）
とは、甲乙間の業務取引（以下「本取引」という。）に関し相互に開示される秘密情報の取扱いに関し、以下のとおり秘密保持契約（以下「本契約」という。）を締結する。

第１条（目的）

甲及び乙は、本取引に関し、相互に相手方に開示する情報の保護を目的として本契約を締結するものとする。以下、本契約において、情報を開示する当事者を「開示当事者」、情報を受領する当事者を「受領当事者」とする。

第２条（秘密情報）

１ 本契約において「秘密情報」とは、本取引に関して、開示当事者が受領当事者に対して開示した営業上・技術上の情報で、書面（電磁的記録を含む、以下「文書等」という。）
であると口頭であるとを問わず秘密とすることを明示されたものをいう。

２ 前項にかかわらず、次の各号のいずれかに該当する情報は、秘密情報から除外されるものとする。

（１）受領当事者が開示当事者より受領した時点で既に公知であった情報

（２）受領当事者が開示当事者より受領後、受領当事者の責めに帰すべき事由によらずに公知となった情報

（３）受領当事者が開示当事者より受領後、守秘義務を負うことなく第三者から適法に入手した情報

（４）受領当事者が、秘密情報によらず独自に開発した情報

第３条（受領当事者の秘密保持義務）

１ 受領当事者は、受領した秘密情報に関する秘密を第三者に開示、漏洩してはならない。

２ 受領当事者は、秘密情報を、本取引に必要な最小限度の範囲を除き、開示当事者の事前の書面による承諾なく秘密情報を複製してはならない。

３ 受領当事者は、前各項の義務を履行するため、秘密情報につき必要かつ合理的な保護手段を講じなければならない。

第４条（事故報告）

受領当事者は、秘密情報に関し、前条に違反し、又は違反するおそれがある事態が生じたと判断するときは、直ちに、その旨を開示当事者に報告し、開示当事者の指示を仰がなけ

ればならない。
第５条（監査）
受領当事者は、開示当事者より秘密情報の取扱いの状況について報告を求められたときは、遅滞なくその状況を文書等により報告しなければならない。
第６条（有効期間）
１ 本契約の有効期間は、契約締結日より１年間とし、有効期間満了日の２ヶ月前までに何れの当事者からも解約の申し出がない場合には、更に１年間延長し、以後も同様とする。
２ 本契約が終了した場合といえども、本契約第２条ないし第４条で定める義務は本契約終了後５年間存続する。
第７条（契約終了後の措置）
１ 受領当事者は、本契約が終了したとき、又は、開示当事者より請求があったときは、直ちに秘密情報の記録された文書等及びそれらの複製物の一切を、開示当事者の指示に従い返還し、又は廃棄するものとする。
２ 受領当事者は、前項による開示当事者の指示に基づき秘密情報の記録された文書等及びそれらの複製物を廃棄した場合において、開示当事者の請求があったときは、遅滞なく廃棄に関する証明書を提出するものとする。
第８条（損害賠償）
受領当事者は、本契約に違反することにより開示当事者に損害を与えたときは、これにより開示当事者に生じた損害を賠償しなければならない。
第９条（反社会的勢力との取引排除）
１ 甲及び乙は、次に定める事項を表明し、保証する。
（１）自己及び自己の役員・株主（以下「関係者」という）が、暴力団、暴力団関係企業もしくはこれらに準ずる者又はその構成員（以下総称して「反社会的勢力」といいます）でないこと
（２）自己及び自己の関係者が、反社会的勢力を利用しないこと
（３）自己及び自己の関係者が、反社会的勢力に資金等の提供、便宜の供給等、反社会的勢力の維持運営に協力又は関与しないこと
（４）自己及び自己の関係者が、反社会的勢力と関係を有しないこと
（５）自己が自ら又は第三者を利用して、相手方に対し、暴力的行為、詐術、脅迫的言辞を用いず、相手方の名誉や信用を毀損せず、また、相手方の業務を妨害しないこと
２ 甲及び乙は、相手方が前項に違反したと認める場合には、通知、催告その他の手続を要しないで、直ちに本契約の全部又は一部を解除することができる。この場合、相手方は他方当事者に発生した全ての損害を直ちに賠償するものとする。
第１０条（合意管轄）
本契約に関する一切の紛争については、訴額に応じて東京地方裁判所又は東京簡易裁判所

を第一審の専属的合意管轄裁判所とする。

第１１条（協議）

本契約に規定のない事項又は本契約の規定の解釈に疑義を生じたときは、甲乙協議の上、解決するものとする。

本契約締結の方法として、電子証明書を伴うクラウド上のサービス（クラウドサイン）使用することとする