情報セキュリティに関する基本的な取り扱い方法
（谷田経営法律事務所 弁護士谷田寿人）

本書は、当職が弁護士としての職務を遂行する際に、情報セキュリティを確保するための基本的な取扱方法を定めるものである。当職は、本書に従い取扱情報を取り扱うとともに、当事務所で勤務する事務職員その他取扱情報に接する者（以下「事務職員等」という。）にも基本的な取扱方法を遵守させる。

１　用語

本書で用いる用語は、日本弁護士連合会の弁護士情報セキュリティ規程（会規第１１７号。以下「規程」という。）で定義されたものと同様とする。本書で保護の対象となる「取扱情報」も規程で定義されているとおり「弁護士等がその職務上取り扱う情報」を広く含むが、公開情報等の情報セキュリティを保持する必要のない情報は含まない。

２　安全管理措置

(1) 組織的な安全管理措置

ア　事務職員等に対し、本書をいつでも参照できるようにして、これを遵守することを求め、情報セキュリティを確保するために必要に応じて役割分担を与え、情報セキュリティの確保に関する指揮と監督を行う。

イ　共同受任又は弁護団等で他の弁護士と共同で取扱情報を取り扱う場合には、当該他の弁護士と協議して、取扱情報の授受方法、共有方法等、当該案件の遂行に必要な場合に必要な範囲で、共同の基本的な取扱方法を定める。

(2) 人的な安全管理措置

ア　当職は自ら又は事務職員等に命じて、日本弁護士連合会が発信する情報セキュリティに関する脅威や脆弱性についての情報等の情報セキュリティに関する注意情報を収集する。

イ　当職は、取扱情報の情報セキュリティを維持するために必要な情報セキュリティに関する脅威や脆弱性についての情報収集を行い、教育及び訓練に参加するとともに、事務職員等に対しても、その機会を確保する。

ウ　事務職員等による取扱情報の漏えい等を防止するため、当職の許可なく取扱情報を外部に持ち出すことを禁止する。

エ　事務職員等が退職する際には、保有している取扱情報を返還させ、事務職員等に対し業務用に貸与したもの以外の機器の利用を許可した場合は、当該機器に保存された取扱情報を消去させる。

オ　取扱情報の取扱いを第三者に委託するときは、以下に定めるとおり行う。

①　適切な情報セキュリティ対策を行っている委託先を選定する。

②　委託先との間で、提供する取扱情報に関し、(a)内容、利用目的及び保管方式の定め、(b)第三者提供及び目的外利用の禁止、(c)委託終了時の返還又は消去に関する取り決めを行うか、これらの事項について適切に設定されていることを確認する。

(3) 物理的な安全管理措置

ア　取扱情報がみだりに第三者の目に触れないよう、以下の措置を講じる。

・会議室には取扱情報を置かない。

・取扱情報が存在する部屋には第三者を単独では入室させない。

・取扱情報が第三者から見えないようにパーティションを設置する。

イ　執務スペース等の取扱情報にアクセス可能な場所に立ち入ることのできる第三者を制御するべく、事務所の出入口は常時施錠とする。

ウ　来訪した第三者を取扱情報にアクセス可能な場所に入室させる場合には、来訪者の氏名又は属性の確認を行う。

(4) 技術的な安全管理措置

ア　アカウント管理及びアクセス制御

①　当事務所で用いるソフトウェア、サービス又はハードウェアの利用に際して、必要かつ可能な場合は、ＩＤ、パスワード等を用いた認証及びアクセス権限・範囲の設定等によるアクセス制御を行う。

②　取扱情報にアクセスするためのアカウントは、当事務所が特に定める場合を除き、技術的に可能な範囲で、それを使用する人ごとに発行し、そのＩＤ及びパスワード等を共用しない。

③　アカウント情報は、当該アカウント利用者以外の者の目に触れるところに書き記さない、使い回しをしない等の適切な管理を行う。

④　アカウントのパスワードについては、適切な長さと複雑さを持たせ、第三者から推測されないようにする。

⑤　携帯電話へのコード送信、ワンタイムパスワード等の多要素認証又は生体認証を利用できる場合は、当該アカウントで取り扱う取扱情報の重要度に応じて利用する。

イ　ソフトウェア及びサービス（以下「ソフトウェア等」という。）

①　事務職員等に対し、別途当職が定めた一定のソフトウェア等の使用を禁ずる。ただし、業務上使用の必要がある場合は、事前に報告させ、当職の承諾の上で使用させる。

②　ＯＳを含むソフトウェア等のアップデートを適切に設定し、必要な更新を行う。

③　ウェブサイトを閲覧する際には、マルウェアに感染しないために、業務上必要な範囲を超えての不必要なサイトの閲覧又はファイルのダウンロードは行わない。

ウ　ハードウェア

①　ファイアウォールの設定、セキュリティ対策ソフトのインストール等の適切な防御措置を施して、それを最新の状態に保ち、定期的にチェックを行う。

②　ネットワーク機器、複合機等のファームウェア等のアップデートを適切に設定し、必要な更新を行う。

③　ハードウェアでもパスワードの設定等アクセス制御の機能がある場合は、必要に応じて第三者から容易に推測されない適切な強度のパスワード等を設定する等の措置を講ずる。

④　取扱情報にアクセスできるルータ、ノートパソコン、スマートフォン等のハードウェアを、アクセス制御がなされていない状態で取扱情報へのアクセスが許容されない第三者に使用させない。

⑤　ハードウェアに対し外部からインターネットを経由したアクセスを許す場合に、通信の暗号化及び秘匿化、ＩＤとパスワードの設定等によるアクセス制御を行い、第三者に情報が漏えいしないようにする。

⑥　事務職員等が業務用に貸与されたハードウェア以外の自己所有のスマートフォン等を業務で使用する場合は、あらかじめ当職の許可を得るものとし、使用に際しては本書に規定された安全管理措置と同等の対策を施すものとする。

３　情報のライフサイクル管理

(1) 情報の受領・取得

ア　受領・取得（総論）

取扱情報の受領又は取得に関し、その方法又は利用する情報機器の特性に応じ、次のイからオまでに掲げる対策を取り、情報セキュリティの維持に注意を払う。

イ　受領（FAX）

①　受信がいつでも確実に行われるように機器の整備を行う。

②　受信したFAX文書は、受信日から少なくとも１年間、pdfフォーマットにてクラウドストレージに保存する。

ウ　受領（郵便、宅配便）

①　郵便及び宅配便（以下「郵便等」という。）を受領するときは、みだりに配達人を執務室内に立ち入らせないようにする等、情報漏えいを防止する措置を講ずる。

②　郵便受その他これに相当するものには、ダイヤル式の錠を付し、郵便等の破損又は持ち去りを可及的に防ぐための措置を講ずる。

エ　受領（電子メール）

①　電子メールを受信するコンピュータ又はソフトウェア（ＯＳを含む。）に対し、あらかじめマルウェア等による攻撃を防ぐためのソフトウェア等の適用を行う。

②　電子メールを受信した場合において、送信者（氏名、メールアドレス等）の表示、文面、文面に記載されたリンク、添付ファイルの名称及びファイル形式、メールソフトウェアの警告表示等を注意深く確認する等して、不審であると判断したときは、電子メール又は添付ファイルを安易に開かず、リンクを安易にクリックせずに、発信者に電話、ショートメッセージ等電子メールとは異なる方法で発信の有無、内容等を確認する等サイバー攻撃を回避する措置を講ずる。

オ　取得（撮影、録音又は録画）

①　スマートフォン、デジタルカメラ等の撮影、録音又は録画の機能を有する機器（以下「スマートフォン等」という。）により取扱情報を撮影、録音又は録画する方法により記録する場合、情報の漏えい及び拡散の防止を図るため、使用するスマートフォン等を紛失しないようにする、スマートフォン等のパスワード等を設定する等の措置を講ずる。

②　スマートフォン等をネットワークに接続させるときは、ネットワーク上の第三者からもアクセスできる領域に、写真、動画等の取扱情報がアップロードされないよう適切に設定する等、記録した取扱情報の漏えいを防止する措置を講ずる。

③　スマートフォン等に格納された写真、動画等の取扱情報を、当該取扱情報の性質及び重要度に応じて、適時に、クラウドストレージ等の安全な格納場所に移して保管する。

(2) 情報の保管

ア　保管（紙媒体記録等）

①　紙媒体記録等（取扱情報が記載された紙その他の有体物。以下同じ。）を第三者からのアクセスを適切に制御できる場所に保管し、容易に第三者が紙媒体記録等の内容を認識できる場所に放置しない等、紙媒体記録等の漏えい、改ざん及び紛失を防止するための措置を講ずる。

②　紙媒体記録等の紛失又は漏えいを防止するため、紙媒体記録等に含まれる情報の秘匿の必要性に応じて、適切な保管場所及び保管方法を選択する。

イ　保管（データ）

データの性質等に応じて必要な場合は、当該データ又はフォルダにアクセスできる者をＩＤ、パスワード等により制限する等、データの漏えい、改ざん及び紛失を防止するための適切な措置を講ずる。

ウ　保管（モバイル機器）

モバイル機器（持ち運びが容易なＵＳＢメモリ、スマートフォン、タブレット、ノートパソコン等の情報機器）に格納して取扱情報を取り扱うときは、イのデータの保管に関する措置を講ずるほか、取扱情報及び使用するモバイル機器の特性に応じて、特に以下で定める措置を講ずる。

① モバイル機器に保存する目的を超えてデータをモバイル機器に格納しない。また、その格納する必要がなくなったときは、速やかにモバイル機器から当該データを消去する。

② データをモバイル機器に格納して外部に持ち出すときは、個別のデータ又はモバイル機器全体にパスワードの設定、暗号化その他データの漏えいを防止する措置を講ずる。

③ モバイル機器の所在を常に把握する等モバイル機器について適切な管理を行い、遠隔操作によるデータの消去が可能な場合はその設定を行っておく等の相当な措置を講ずる。

エ 保管（外部サービス）

① 外部サービス（ファイル転送、クラウドストレージ、メッセージ交換等）を用いてデータを取り扱うときは、当該外部サービスの信頼性を十分に吟味し、外部サービスの利用により守秘義務違反を招かないように注意する。

② 外部サービスの利用を停止するときは、当該外部サービスで保管しているデータを確実に消去する。

(3) 情報の発信・交付等

ア 発信・交付（総論）

取扱情報を発信する際には、宛先違い及び内容違いがないか確認する。

イ 発信（FAX）

① 繰り返し送信することが予定される送信先については、当該送信先の FAX 番号をあらかじめ登録する。

② 取扱情報を FAX で送信したときは、送信に用いた機器に送信ログを保存する。

ウ 発信（電子メール等）

① 電子メール、携帯電話又はスマートフォンのショートメッセージ、ＳＮＳのメッセージツール等インターネット経由の送信方法（以下「電子メール等」という。）により、その性質上漏えいにより深刻な結果を招くおそれのある取扱情報を発信する場合は、宛先違い、内容違いがないか十分に確認し、できるだけ安全な方法を選択する。

② 複数の宛先に電子メールを送信するために同報送信機能を利用する場合は、電子メールアドレスが個人情報に該当する場合があることに留意しつつ、ｃｃ（カーボ

ン・コピー）機能とｂｃｃ（ブラインド・カーボン・コピー）機能を適切に使い分ける。

エ　発信（ＳＮＳ）

情報主体の承諾なく、公衆に向けて送信するＳＮＳにおいて取扱情報及びこれを推知させる情報を書き込まない。

オ　交付

取扱情報が記載又は記録された文書又は物品を交付（直接対面で渡すこと）する場合は、受領者の権限を確認した上で交付するものとし、受領証を取り付ける等当該文書又は物品の交付の事実及び受領者を確認できる措置を講ずる。

カ　マスキング

取扱情報の一部にマスキングを施して相手方当事者や第三者に提示する場合は、開示すべきでない情報を確実にマスキングするように注意する。特に、画像、pdf ファイル等のデータを加工してマスキングするときは、提出先においてマスキングを除去することができないように注意する。

(4) 情報の持ち出し・複製

ア　持ち出し

紙媒体記録等及び取扱情報を格納したモバイル機器を必要な範囲を超えて外部に持ち出さない。

イ　複製（紙媒体記録等のデータ化を含む。）

①　取扱情報を必要な範囲を超えて複製しない。

②　情報漏えい及び目的外利用の危険を考慮し、複製の可否及び範囲を慎重に判断する。

③　複製物を適切に管理し、紛失の防止に必要な措置を講ずる。

(5) 情報の廃棄・返還

ア　廃棄（総論）

①　保有する必要のない取扱情報は、速やかに廃棄する。

②　取扱情報を廃棄する場合は、廃棄の可否を慎重に判断し、誤って必要なデータを廃棄しないように注意する。

③　取扱情報の廃棄を専門業者等に委託する際には、委託先が守秘義務を負っていること及び廃棄方法の適切さ等を確認する等して、委託先から取扱情報が漏えいすることを防ぐ措置を講ずる。

④　外部業者に委託して廃棄したとき（例えば、業者に委託して紙媒体記録等を溶解したとき、業者に委託してパソコン、モバイル機器等のデータを消去したとき等）は、

当該業者が発行する廃棄完了証明書を適切な期間保管することで、廃棄処理事項の記録に代える。

イ　廃棄（紙媒体記録等）

①　取扱情報が記載された紙媒体記録等を廃棄するときは、漏えいを防止するためシュレッダによる裁断、溶解処理等の措置を講ずる。

②　取扱情報が記載された紙媒体記録等の裏面に印刷をして、他事件の記録への編綴、FAX 送信等をしない。

ウ　廃棄（データ）

取扱情報に該当するデータが格納されている電子媒体を廃棄するときは、消去ソフトウェアを利用する、破壊処理を行う等データを読み取ることを不可能とする等の措置を講ずる。

エ　返還

情報主体から預かった書類又は物品を返還するときは、必要に応じて、返還する書類又は物品の内容を確認して記録し、その返還記録を適切に保管する。

(6) 会議・期日出席

ア　総論

会議又は期日等（以下「会議等」という。）に際して、取扱情報が漏えいしないよう、盗み見、盗み聞きができない環境・設備で会議を実施し、以下で定める措置その他の相当な措置を講ずる。

①　会議等から離席するときは、取扱情報が記載され又は記録された物品を、施錠又は監視等の情報セキュリティを保持する措置が講じられていない会議室内に放置しない。

②　会議等に際して、ホワイトボード等に取扱情報を記載したときは、当該取扱情報の保存の要否を確認し、保存を要するときは撮影その他の適宜の方法により保存した上で、ホワイトボード等の記載を確実に消去する。

③　会議等に際して、ディスプレイ等で取扱情報を表示するときは、表示するべきでない取扱情報が表示されないようにする。

イ　期日

①　期日への出席に際して、その性質上漏えいにより深刻な結果を招くおそれのある取扱情報が第三者の目に触れないように適切な措置を講ずる。

②　期日への出席に際して、持参した証拠の原本を紛失しないよう適切な措置を講ずる。

ウ　ウェブ会議

① 取扱情報にアクセスさせることが適切でない第三者との関係で、盗み見、盗み聞き、背景の映り込み、周囲での会話等により取扱情報の漏えいが発生しない環境及び設備でウェブ会議に出席する。

② ウェブ会議の参加者の中に出席が予定されていない者が紛れ込んでいないかを、可能な範囲で確認する。

③ ウェブ会議が許された者以外によって録音又は録画されないような措置（ウェブ会議ソフトウェアの録音・録画機能の停止等）を可能な範囲で講ずる。

④ ウェブ会議において画面共有により取扱情報を共有するときは、表示するべきでない取扱情報が表示されないようにする。

４　点検及び改善

(1) 毎年４月に、基本的な取扱方法の実施状況を点検する。

(2) 前号の点検の結果、基本的な取扱方法が有効に実施されていないことが分かった場合は、その原因を特定し、改善計画を立案し、必要がある場合は基本的な取扱方法を改訂する。

５　漏えい等事故が発生した場合の対応

(1) 取扱情報の漏えい、滅失、毀損等の事故（以下「漏えい等事故」という。）が発生した場合には、当職がその対応を指揮し、事務職員等の役割分担を決定する。

(2) 漏えい等事故が発生した場合、発見者は、当職に対し、速やかに報告し、指示を仰ぐ。

(3) 原因を調査し、情報主体への連絡、マルウェアに感染した情報機器の停止若しくはネットワークからの遮断又はセキュリティ対策ソフトウェアによる検査若しくは駆除等の応急措置を実行する。

(4) 必要に応じ、外部の情報セキュリティの専門家等の助言又は補助を得る。

(5) 調査の結果判明した原因についての対策を実行する。

以　上

(附則)本書に従った取り扱い方法は、令和５年７月１日から実施する。