Cybersecurity Ethics and Compliance for Law Firms in Japan

Atsushi Okada, Mori Hamada & Matsumoto, Tokyo

1. Key rules in Japan

1.1. General rules

The Basic Act on Cybersecurity provides the basic framework for the responsibilities and policies of the national and local governments to enhance cybersecurity. Further, it obligates operators of material infrastructure (e.g., financial institutions, operators of railroads, airplanes and other means of transportation, and providers of electricity gas and water) and networks (e.g., telecommunication networks) to make efforts to voluntarily and proactively enhance cybersecurity and to cooperate with the national and local governments to promote measures to enhance cybersecurity.

The Act on the Protection of Personal Information ("**APPI**") is the principal data protection legislation in Japan. Its enforcement and application are supervised by the Personal Information Protection Commission ("**PPC**"). Under the APPI, a "Business Operator Handling Personal Information (*Kojin Joho Toriatsukai Jigyosha*)" ("**Handling Operator**") is required to take necessary and appropriate measures for security control of personal data it handles, including preventing leakage, loss or damage of Personal Data (Article 20).

- "Necessary and appropriate measures" refer to security measures in accordance with the PPC guidelines, which include:

  (a) Organizational security measures, including the implementation of an organizational system (for example, establishing rules for handling the personal data, and clarifying the person responsible for supervising the handling of personal data);

  (b) Human resource security measures, including education of employees;

  (c) Physical security measures, including controlling the area where personal data is handled, such as servers and offices; and

  (d) Technical security measures, including control of access to personal data.

- The above four security measures must be conducted as the "necessary and

appropriate measures;" however, the details of each security measure must be determined by each company depending on the degree of risk in case of leakage.

1.2. Specific rules applicable only to lawyers

Attorney Act, Article 23 (right and duty to maintain confidentiality):

'Unless otherwise provided by law, an attorney or a former attorney shall have the right and bear the duty to maintain the confidentiality of any facts which he/she may have learned in the course of performing his/her duties.'

JFBA Model Rules of Professional Conduct

Confidentiality provisions are stipulated in Articles 18 and 23.

2. JFBA Information Security Guidelines for Lawyers

Please refer to the original text in the attachment.

This guideline is not intended to establish any legal obligation. Instead, this guideline is intended to assist practitioners in taking appropriate information security measures (such as understanding what information security seeks to achieve, why it is important for attorneys to safeguard their own and their clients' information, and how an information security management system may be implemented).

3. Examples of recent cybersecurity incidents in Japan

There have been only a few cybersecurity incidents announced to date. However, the impact of cybersecurity incidents has become quite serious across the industries over the past few years. Please see below a few such examples in Japan.

May 2015	A huge number of pension records were leaked due to targeted email attacks.
April 2016	Personal data of 1.4 million individuals were leaked due to cyberattacks to software vulnerability.
April 2017	Personal data of 0.1 million credit card users were purchased on the dark web.
2018	A huge amount of cryptocurrencies were leaked due to unauthorized access to servers of exchange operators

Attachment

Information Security Guidelines for Lawyers

Japan Federation of Bar Associations
Issued on December 19, 2013
Amended on January 17, 2019

第１ 本ガイドラインの目的と利用方法

弁護士法第２３条は，弁護士の秘密保持の権利と義務を規定し，弁護士職務基本規程第１８条は，事件記録中の秘密及びプライバシーの漏えい防止の注意義務を規定している。弁護士は，これらの規定を遵守するため，その責任において情報セキュリティ対策を講じる必要がある。

本ガイドラインはこれらの規定に関する解釈指針を示すものであり，弁護士・法律事務所が行うべき最低限の情報セキュリティ対策を規定するものでも，十分な対策を規定するものでもない。

本ガイドラインは，弁護士の情報セキュリティ対策の取組を支援することを目的としている。弁護士の情報セキュリティ対策のために，強く推奨する取組を「すること」と表記し，物的・人的・経済的環境に応じて推奨する取組を「望ましい」と表記しているが，弁護士に，新たに本ガイドラインが定める取組を行う義務を課すものではない。また，本ガイドラインは綱紀・懲戒の直接の基準とされることも想定していない。

なお，本ガイドラインは，使いやすさを考慮して，実務の流れに配慮した。

また，本ガイドラインは，新たなＩＴ機器，サービスの利用だけでなく，紙媒体の不適切な管理による事故も発生していることに鑑み，紙媒体の取扱いなど必要であれば当然の取組についても，重複を厭わず，具体的な手順を可能な限り示すことに配慮した。

弁護士の情報環境及び情報セキュリティリスクは変化する。弁護士は，本ガイドラインを参考として，その責任において，適切な情報セキュリティ対策を構築，実施，点検し，不断に改善を続けることが望まれる。

第２ 定義

１ 「事件情報」とは，法律相談を受け，又は受任した事件に関し，依頼者等（依

頼者その他の事件の関係者をいう。以下同じ。）から受領し，又は自ら取得した情報をいう。

２ 「データ」とは，事件情報，個人情報，その他の弁護士の守秘義務の対象となる情報（以下「事件情報等」という。）を電磁的方式その他人の知覚によっては認識することができない方式で記録したものであって，コンピュータ（以下「ＰＣ」という。）による情報処理の用に供されるものをいう。

３ 「サーバ」とは，法律事務所に所属する弁護士が共有すべきデータを保管する目的で当該法律事務所が管理しているＰＣであって，当該法律事務所に所属する弁護士が各自使用するＰＣとネットワークで接続されているものをいう。

４ 「可搬電子媒体」とは，ノートＰＣ，タブレット機器，携帯電話，スマートフォン，デジタルカメラ，デジタルビデオカメラ，ＩＣレコーダー，ＵＳＢメモリ，ＤＶＤ，ＳＤカードなどデータを収納して容易に携帯できる電子媒体をいう。

５ 「事件記録等」とは，事件情報等を記録した紙をいう。

６ 「外部サービス」とは，ウェブメール（Ｇｍａｉｌなど），大容量ファイル保管サービス（Ｄｒｏｐｂｏｘなど），メーリングリストなどの第三者がインターネットにおいて提供するデータ保管のサービスをいう。

第３ 情報倫理

１ 基本理念

弁護士は，事件情報等の受領，作成・変更，保管，発信・交付，持ち出し・複製（事件記録等をデータに変換すること（以下「データ化」という。）による場合を含む。）及び廃棄・返還に当たっては，法令及び契約を遵守し，事件情報等の利用目的，性質及び内容に相応しい取扱いを行うこと。特に，次に掲げるその性質上漏えいにより深刻な結果を招く恐れのある事件情報等については，事件情報等を保管した媒体の適宜の場所に注意喚起の表示を行うなどの適切な措置を講じること。

(1) 裁判員候補者又は裁判員の個人情報

(2) 特定人の人種，信仰その他のセンシティブ情報

(3) 犯罪被害者の個人情報

(4) その他重大な秘密情報

2 情報共有

弁護士は，外部サービスを利用して事件情報等を他の弁護士と共有するときは，個人情報やセンシティブ情報が漏えいしないよう適切な設定その他の情報漏えいを防止する確実な措置を講じること。

第４ 情報の受領・取得

1 受領・取得（総論）

弁護士は，事件情報等を記載し，又は記録した原本その他の代替性のない物を受領・取得したときは，紛失しないように特に注意して保管すること。

2 受領（ＦＡＸ）

(1) 弁護士は，事件情報等をＦＡＸで受信したときは，直ちに発信者及び内容を確認し，発信者又は内容に不審な点又は間違いがあったときは，速やかに発信者又は正しいと思われる発信者に電話等で連絡し，確認することが望ましい。

(2) 弁護士は，事件情報等をＦＡＸで受信したときは，その受信記録を作成して保管することが望ましい。

3 受領（郵便，宅配便）

(1) 弁護士が，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こと。

(2) 弁護士は，郵便等を受領したときは，適宜の措置を講じること。

(3) 弁護士は，法律事務所の郵便受その他これに相当するものには，錠を付けることが望ましい。

(4) 弁護士は，事件情報等を郵便等により受領したときは，その受領記録を作成して保管することが望ましい。受領した事件情報等が原本その他代替性のないものであるときは，受領記録を作成して保管すること。

4 受領（電子メール）

(1) 弁護士は，電子メールを受信した場合において，送信者に心当たりのないとき又は添付ファイルの形式がセキュリティ上の危険が疑われるものであるときは，電子メール又は添付ファイルを安易に開かないように注意する

こと。

(2) 弁護士は，事件情報等を電子メールで受信したときは，その電子メールを消去しないことが望ましい。

5 取得（デジタルカメラ等）

(1) 弁護士は，デジタルカメラやスマートフォン等（以下「デジタルカメラ等」という。）により刑事記録等の受任した事件に関連する資料を記録する場合，情報の漏えい・拡散の防止を図るため，使用するデジタルカメラ等は，インターネット等外部のネットワークへの接続ができない状態にしておくことが望ましい。接続可能な状態でデジタルカメラ等を用いるときは，記録前に，記録したデータが外部に漏えい・拡散しない設定となっていることを確認すること。

(2) 弁護士は，記録したデータを保存する記録媒体についても，漏えい・拡散を防ぐため，業務専用の記録媒体を用いることが望ましい。

第5 情報の作成及び変更

1 作成及び変更（事件記録等）

(1) 弁護士は，事件記録等を作成した場合は，作成者，作成日及び当該事件情報等が秘密情報であるときはその旨を明記することが望ましい。

(2) 弁護士は，一旦作成された事件記録等を変更するときは，変更箇所及び変更日を明確にすることが望ましい。

2 作成及び変更（データ）

弁護士は，データを作成し，又は変更するときは，作成し，又は変更したデータの属性（作成者・作成日時などの情報）及び変更履歴（作成者名及び変更者名を含む。）を適正に管理すること。

3 マスキング

弁護士は，事件記録等又はデータを提出する際にその一部をマスキングするときは，確実にマスキングされ提出先において認知できない状態とするように注意すること。特に，画像，ＰＤＦ又は文書ファイル等のデータを加工してマスキングするときは，開示すべきでない情報を確実にマスキングし，提出先においてソフトウェアによりマスキングを除去することができないように注意すること。

第６ 情報の保管

１ 保管（事件記録等）

(1) 弁護士は，事件記録等を机の上等の容易に他人が事件記録等の内容を認識できる場所に放置しないこと。

(2) 弁護士は，事件記録等の紛失・漏えいを防止するため，依頼者，相談者，事件又は案件ごとに編綴するなどの方法で適切に管理し，背表紙等に識別情報を付した上で，錠付きのキャビネットに保管することが望ましい。

(3) 弁護士は，事件記録等の紛失・漏えいを防止するため，その重要度に応じて保管場所，データ化，その他適切な保管方法を定めること。

(4) 弁護士は，事件記録等の所在を把握するため，管理簿を作成するなどの相当の措置を講じること。

(5) 弁護士は，データ化する場合は，パスワードの設定等の適宜のアクセス制限の措置を施すこと。

２ 保管（ＰＣ）

(1) 弁護士は,ＰＣを用いて事件情報等を取り扱うときは,次の措置を講じること。

① 紛失防止 ＰＣの盗難・紛失を防止するための適切な措置

② パスワード管理 ＰＣ及びファイルにパスワードを適切に設定して管理する措置

③ アップデート ＰＣ及びネットワーク機器について，ＯＳ，ブラウザなどのソフトウェアのアップデートファイルを自動で確認するような設定をし，更新ファイルがあるときは，必要な更新を行う措置

④ ウイルス対策 ＰＣにセキュリティ対策ソフトをインストールして最新の状態に保ち，定期的にウィルスチェックを行う措置

⑤ アクセス制御 アクセス権限を有する者だけが必要な情報だけにアクセスすることができるようし，特に退所者がアクセスできないようにする措置

⑥ リモートアクセス制御 通信の暗号化及びログインＩＤとパスワードの設定等，法律事務所外から法律事務所内のＰＣへアクセスする際に第三

者に情報が漏えいしないための措置

⑦ バックアップ ＰＣに収納されているデータのバックアップを定期的に取り，バックアップデータを当該ＰＣとは別に保管する措置

⑧ サーバ管理等 セキュリティ上のリスクを考慮して，サーバを適切に設計して管理する措置

⑨ インストール制御 ＰＣに，管理者の許可なくソフトウェアをインストールさせない措置

(2) 弁護士は，ＰＣに収納されているデータを消去する場合は，消去の可否を慎重に判断し，誤って必要なデータを消去しないように注意すること。

３ 保管（可搬電子媒体）

(1) 弁護士は，可搬電子媒体に収納する目的を超えてデータをみだりに可搬電子媒体に収納しないこと。また，その利用目的を達成したときは，直ちに可搬電子媒体から当該データを消去すること。

(2) 弁護士は，データを可搬電子媒体に収納するときは，データ又は可搬電子媒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じること。

(3) 弁護士は，可搬電子媒体の所在を常に把握するなど可搬電子媒体について適切な管理を行い，所在が不明な場合は，遠隔操作によるデータの消去等相当な措置を講じること。

４ 保管（外部サービス）

(1) 弁護士は，外部サービスを用いてデータを取り扱うときは，当該外部サービスを運営する者が規約等で利用者に対し第三者への情報提供をしないことを保証していることを確認し，保証していない場合は当該外部サービスを利用しないこと。

(2) 弁護士は，外部サービスを利用するときは，適切なログインＩＤやパスワードを設定するなど相当のアクセス制限措置を講じ，第三者が自己になりすまして当該外部サービスを利用できないように注意すること。

(3) 弁護士は，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こと。

第７ 情報の発信・交付

1　発信（FAX）

(1) 弁護士は，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ことが望ましい。

(2) 弁護士は，事件情報等をＦＡＸで送信したときは，送信記録を作成して保管すること。

2　発信（郵便等）

(1) 弁護士は，事件情報等に関する郵便等を送付するときは，あらかじめ宛先の住所に誤りがないか確認すること。

(2) 弁護士は，事件情報等に関する郵便等の送付履歴を保存すること。

3　発信（電子メール）

(1) 弁護士は，事件情報等に関する電子メールを送信するときは，あらかじめ宛先のメールアドレスに誤りがないか確認すること。

(2) 弁護士が職務上複数の宛先に電子メールを送信するときは，各宛先同士がメールアドレスを不当に知られることのないよう措置を講じること。

(3) 弁護士が事件情報等を記録したファイルを添付して電子メールを送信するときは，当該ファイルにパスワードを設定し，添付したファイルが正しいものかどうかを確認してから送信すること。この場合においては，当該電子メールにパスワードを記載しないこと。

4　発信（ソーシャル・ネットワーキング・サービス）

弁護士は，依頼者の承諾なく，ソーシャル・ネットワーキング・サービスにおいて事件情報等及びこれを推知させる情報を取り扱わないこと。

5　交付

弁護士は，事件情報等が記載又は記録された文書又は物品を交付する場合は，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など当該文書又は物品の交付の事実や受領者を確認できる措置を講じること。

第８　情報の持ち出し・複製

1　持ち出し

弁護士は，事件記録等及び可搬電子媒体（データを収納したものに限る。以下

この項において同じ。）をみだりに法律事務所の外に持ち出さないこと。やむを得ず法律事務所の外に事件記録等又は可搬電子媒体を持ち出すときは，事件記録等については第１号に掲げる措置を，可搬電子媒体については次に掲げる措置を講じること。

(1) 紛失・盗難防止

(2) データの暗号化

(3) パスワードの漏えい防止

２ 複製（事件記録等のデータ化を含む）

(1) 弁護士は，事件情報等のデータ化に際しては，情報漏えい及び目的外利用の危険を考慮し，データ化の可否及び範囲を慎重に判断すること。

(2) 弁護士は，事件記録等及びデータの複製物を適切に管理し，紛失の防止に努めること。

第９ 情報の廃棄・返還

１ 廃棄（事件記録等）

(1) 弁護士は，事件記録等を廃棄するときは，第三者への事件情報等の漏えいを防止するためシュレッダーによる裁断や溶解処理等の措置を講じること。なお，廃棄業者に依頼するときは，適切な業者を選定すること。

(2) 弁護士は，事件記録等を廃棄するときは，廃棄した事件記録等，廃棄の時期，廃棄に際して講じた措置等を記録しておくことが望ましい。

(3) 弁護士は，事件記録等を裏紙として再利用しないこと。

２ 廃棄（電子媒体）

(1) 弁護士は，データが収納されている電子媒体（ＰＣ，サーバ及び可搬電子媒体をいう。）を廃棄するときは，破壊処理を行うなど当該電子媒体からデータを読み取ることを不可能とする措置を講じること。なお，廃棄業者に依頼するときは，適切な業者を選定すること。

(2) 弁護士は，廃棄した電子媒体，廃棄の時期，廃棄に際して講じた措置の内容等を記録しておくことが望ましい。

３ 返還（依頼者）

弁護士は，依頼者から預かった書類又は物品を返還するときは，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こと。

第１０ 電子媒体及び事件記録等の処分

弁護士は，事件情報等を記録した電子媒体及び事件記録等を譲渡，貸与，その他の処分を行い，又は第三者に利用させるときは，事件情報等がその目的の範囲で利用され，漏えいしないよう適切な措置を講じること。

第１１ 会議・期日出席

弁護士は，会議，期日等への出席に当たり，第３から第９までの措置を講じるほか，以下の措置を講じること。

１ 打合せ及び会議（依頼者）

(1) 弁護士は，打合せ及び会議に際して，事件情報等が漏えいしないよう相当な措置を講じること。打合せ及び会議を終了したときは，事件情報等が記載され，又は記録された物品を会議室内に放置しないこと。

(2) 弁護士は，打合せ及び会議に際して，ホワイトボード等に事件情報等を記載したときは，当該事件情報等の保存の要否を確認し，保存を要するときは印刷その他の適宜の方法により当該事件情報等を保存した上で，ホワイトボード等の記載を確実に消去すること。

(3) 弁護士は，打合せ及び会議に際して，ディスプレイ等で情報を表示するときは，他の事件に関する事件情報等が表示されないようにすること。

２ 期日出席

(1) 弁護士は，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恐れのある事件情報等が第三者の目に触れないようにする適切な措置を講じること。

(2) 弁護士は，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じること。

第１２ 弁護団事件

１ 弁護団内部での情報管理

(1) 事務所を異にする２名以上の弁護士が共同して受任する事件（以下「弁護団事件」という。）を受任している複数の弁護士ら（以下「弁護団」という。）

の間で事件情報を共有する場合，事件情報が外部に漏えいすることがないよう注意すること。特に，外部サービスを利用して事件情報を共有する場合，その参加者の範囲，授受する事件情報の内容を適切に管理すること。

(2) 弁護団に属する個々の弁護士が知りうる事件情報の範囲（個々の依頼者の個人情報等）を適切に制御し，弁護団内部で事件情報が不必要に拡散することがないようにすること。

2 依頼者に対する情報提供

依頼者が複数である弁護団事件において，期日経過報告等により依頼者に情報提供する際には，当該依頼者以外の他の依頼者の個人情報をみだりに提供しないこと。

3 弁護団同士での情報共有

同種事件のために地域ごとに設立された弁護団の間など異なる弁護団同士で事件情報を授受する場合には，依頼者の同意を得ること及び第三者に漏えいしないように配慮するなど必要な措置を講じること。

第１３ 組織的及び人的な体制

1 情報セキュリティに関する方針等

(1) 弁護士は，弁護士の業務にとって情報セキュリティが重要な意味を持つことを自覚し，業務の性質に応じて適切な情報セキュリティに関する方針を定めること。

(2) 弁護士は，所属する法律事務所において，情報セキュリティ対策を行う体制を定め，各人の役割及び責任を定めること。

(3) 弁護士は，情報セキュリティに必要な具体策を定め，確実に実施すること。

(4) 弁護士は，具体策の実施に必要な経営資源を決定し，提供すること。

2 教育及び訓練

弁護士は，法律事務所に所属する者に対し，前項第２号の体制の下で，情報セキュリティ対策を行うために必要な教育及び訓練を行うこと。

3 委託

弁護士は，事件情報等の取扱いを委託するときは，事件情報等の提供について依頼者の同意を得た上で，当該委託先との間で，次に掲げる内容を含む適切な

守秘契約を締結すること。

(1) 提供する事件情報等（以下「提供情報」という。）の内容，利用目的及び保管方式が特定されていること。

(2) 提供情報の第三者への提供及び目的外利用を禁止していること。

(3) 委託事務が終了したときは，提供情報の全てを返還させ，委託先に残さないものとしていること。

第１４ 物理的な体制

１ 環境整備及び入退室管理

(1) 弁護士は，事件情報等がみだりに第三者の目に触れない環境を整備すること。

(2) 法律事務所の管理者の地位にある弁護士は，法律事務所の入退出者，入退出の日時，入退出した場所等を記録し，及び管理する措置を講じるよう努めること。

２ 防災

弁護士は，所属する法律事務所の事件情報等の保護に必要な範囲で防災のため，適切な方法を講じること。