9　弁護士の情報セキュリティ

⑴　情報セキュリティの規則化の必要性

情報通信技術が発達した社会において、組織や社会、企業等において適切な情報セキュリティ対策を採ることが極めて重要な課題になっている。

当然ながら、弁護士は、事件の処理に当たって依頼者だけでなく相手方や事件に関係する多数の第三者の秘密やプライバシーに関する情報を適切に扱い、漏らしてはならないことは職務上の最も基本的な義務であり、この点に関する国民からの揺るぎない信頼があってこそ、初めて弁護士の職業的存立の基盤が確保されることとなる。

弁護士の業務において、従前から、電子メールや、Word、Excel、PDF 形式等の資料を筆頭に、日常的に電子データが取り扱われているという事実は、あえて言及をするまでもないことである。

裁判手続に関しても、まず民事裁判について、オンラインで訴状提出、あるいは口頭弁論でウェブ会議の活用を認めることなどを盛り込んだ民事訴訟法等の一部を改正する法律が、2022（令和 4）年 5 月 18 日に成立した。実務においては、既に IT を活用した手続が段階的に運用され、電子データを取り扱う機会が増えてはいたが、法改正によって書証の写しを含めた事件記録のデータ保管が必須となることから、弁護士業務における電子データの取扱いが、飛躍的に増えることはもはや確実である。

刑事手続についても、法務省の刑事手続における情報通信技術の活用に関する検討会が 2022（令和 4）年 3 月 15 日に報告書を取りまとめられ、その中では、弁護士の防御権や弁護権を不当に制約することがあってはならないとした上で、弁護人として、漏えいリスクを管理するための技術的措置を講じる必要性にも言及されている。近日中に、法制審議会の中で議論が進められ、早ければ 2023（令和 5）年度にも法案が提出される可能性がある。

このような情勢において、全ての弁護士にとって、情報セキュリティへの取組が急務となっている。そもそも、弁護士は、業務の性質上、企業の機密情報、要配慮個人情報等の要保護性が高い情報を取り扱う職業である。また、要保護性が高い情報を取り扱うが故、その情報セキュリティが貧弱であれば、攻撃者の格好の攻撃対象にされてしまうことは論を待たないであろう。さらに、攻撃者によって、弁護士が活用するシステムが踏み台にされ、一般国民に対して弁護士をなりすました攻撃も懸念される。

そのため、十分な対策が講じられないまま、事故やサイバー攻撃による情報の漏えい等が起これば、依頼者や第三者に損害を与えるだけではなく、弁護士全体に対する社会的信用が損なわれ、状況によっては国による干渉を招く危険さえある。弁護士自治と職務の自由を保つためにも、情報セキュリティ対策の強化は避けて通ることができない事項である。

⑵　現行の体制の不十分性

ア　現行の定めの不十分性

弁護士法 23 条（秘密保持の権利及び義務）、弁護士職務基本規程 18 条（事件記録の保管等）、同 19 条（事務職員等の指導監督）、同 23 条（秘密の保持）等において、守秘義務等が定められている。また、弁護士業務における情報セキュリティの確保に関しては、「弁護士情報セキュリティガイドライン」が存在する。

しかし、弁護士情報セキュリティ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、実務的な対策例を記述しているものであり、同ガイドラインに記載された諸々の取組を行う義務を弁護士に課すものではない。

また、弁護士法 23 条や弁護士職務基本規程 18 条等の規定は、守秘義務を中核とした義務を規定しているが、情報セキュリティ対策を講じるべき義務までは定めておらず、情報通信技術が益々発達する社会における弁護士業務や、民事裁判手続や刑事手続等の IT 化に対応するには不十分であった。

イ　情報セキュリティリスクが顕在化した事例

企業に対するサイバー攻撃の被害は数多く報道されているが、法曹関係においても例外ではない。たとえば、弁護士会や国内の法律事務所のホームページに対するサイバー攻撃被害が実際に発生しているほか、USB メモリの紛失や、ファイル共有サーバ又はクラウドサービスに保存したファイルやフォルダの共有設定を誤ったことによる情報の漏えい、ランサムウェアに感染して情報が不正に暗号化された上に漏えいした事案等も発生しているところであり、情報セキュリティリスクは、決して、抽象的なリスクに留まるものではない。

ウ　弁護士情報セキュリティ規程制定の経緯

このような背景から、新たに情報セキュリティ確保のために弁護士等が講ずるべき対策の枠組みとして、弁護士情報セキュリティ規程が定められるに至った。

⑶　弁護士情報セキュリティ規程の概要と「基本的な取扱方法」策定の必要性

日弁連が定める弁護士情報セキュリティ規程は、情報セキュリティに関して、弁護士や弁護士法人、外国法事務弁護士等が服するべき通則的な規範を定めるものである。

ただし、個々の弁護士の独立性、業務の自律性の尊重から、効果的なセキュリティ対策の実施は、それぞれが所属する法律事務所等の規模、業務の種類、対応等によって異なること、さらに技術の変化に伴う柔軟な対応を可能とする必要性等の観点から、同規程では、個別具体的な対策を直接規定に書き込むのではなく、弁護士等に業務の実情を踏まえた自律的な具体的対策指針として、第 3 条第 2 項に基本的な取扱方法を策定することを求め、弁護士業務一般に通用する抽象化された基本的な義務として、第 4 条の安全管理措置、第 5 条の情報のライフサイクル管理、第 6 条の点検及び改善、第 7 条の漏えい等事故が発生した場合の対応を定めている。

対象となる情報は、弁護士が職務上取り扱う情報とし、刑事・民事などの限定をせず、事件類型による軽重といった差異も設けていない。弁護士等の情報セキュリティは、職務全般を通じて、確保される必要があるためである。

情報セキュリティの定義については、サイバーセキュリティ基本法に基づき、政府が定めている政府機関等の対策基準策定のためのガイドライン等でも採用されている機密性、完全性、可用性という 3 要素によるものとされた。

なお、3 要素について簡単に説明を加えると、機密性とは、許可された者だけが情報にアクセスできるという特性であり、たとえば、パスワードの漏えいにより許可されていない第三者が情報にアクセスした場合や、事件記録が入ったバックを居酒屋に忘れて第三者

に内容を見られた場合に、機密性が損なわれたということになる。完全性とは、保有する情報が破壊、改ざん、消去等をされていないという特性であり、たとえば、第三者に情報を不正に書き換えられたり、消去されたりした場合に、完全性が損なわれたということになる。可用性とは、許可された者が必要なときに情報にアクセスできるという特性であり、たとえば、ハードディスクドライブが壊れたり、ランサムウェアに感染して情報が不正に暗号化されてしまったりした場合に、可用性が損なわれたということになる。

情報セキュリティ対策の基本的な枠組みは、上記3要素を踏まえながら、セキュリティリスクを把握し、把握したリスクへの対応の方針等取扱方法を策定し、管理体制を構築し、それらに基づいて実際に運用するなどの体制を構築しておくことである。そのため、本規程第3条第2項では、弁護士等に対して取扱情報の情報セキュリティを確保するため「基本的な取扱方法」を定めることを義務付けている。

ここでいう「基本的な取扱方法」は、弁護士等が情報セキュリティを確保するために定めておくべき各自の取扱方法のことであり、リスクの程度は、所属する法律事務所等の規模や業務の種類、対応等によって異なり得るため、日弁連から提示される具体的なモデル案を参考としつつ、各自の実情に応じて取扱方法を策定しておく必要がある。

⑷　具体的な対策について

ア　序論（研修を繰り返し行う必要性）

上述したとおり、弁護士等が各自の実情に応じて「基本的な取扱方法」を策定する必要があるが、弁護士の多くは情報セキュリティの専門家ではない。

そのため、具体的に「基本的な取扱方法」を策定したり、実際に運用を行ったりするためには、東弁や当会においても会員に対して繰り返し研修を行い、会員の知識向上に努めなければならない。

以下、研修を行い会員の知識向上を図るうえで着目すべき重要な視点について、概説をする。

イ　システムを最新の状態に保つこと

システムを最新の状態に保つためには、①ファームウェア（電子機器に内蔵されるソフトウェア。パソコンでいえばBIOS等がこれに当たる）のアップデート、②オペレーティングシステム（Windows、macOS、iOS、Android等）のアップデート、③ソフトウェアのアップデート、④セキュリティ対策ソフトのアップデートの全てが必要である。

情報の公開設定を誤っていたり、パスワードを流出させたりした場合はともかく、システムを最新の状態に保てていれば多くのサイバー攻撃を防ぐことができるため、面倒でも、これら①乃至④のアップデートは怠るべきではない。アップデートの方法が不明な場合は、システムを構築している事業者や、パソコンやスマートフォン、ソフトウェア等の購入元に確認してほしい。

ウ　適切なパスワードを作成して管理すること

ログイン用パスワードとしては「英語大文字、英語小文字、数字、記号の組み合わせで10桁以上」のパスワードを用いることが推奨され、名前、生年月日、地名等の安易な単語を用いるべきではない。短く単純なパスワードや、安易な単語が用いられたパスワ

ードは、ほんの数秒で解析され得るからである。

また、パスワードの使い回しも避けるべきである。たとえば、日弁連と東弁の会員専用ホームページにログインするためのパスワードを同じにしていたり、弁護士会で使用するパスワードと同じパスワードを通販サイトで使用したりすることは避けなければならず、特に、金融機関等の金銭が絡むパスワードについては、その他のパスワードと必ず区別をしなければならない。

なお、パスワードが漏えいした可能性がない限り、パスワードを定期的に変更する必要はなく、パスワード管理アプリや紙のノートを用いてパスワードを管理することが推奨される。

エ　多要素認証を活用すること

会員登録をして利用する多くのホームページでは、メールアドレスを ID とし、パスワードを入力することでログインができる「パスワード認証（単一認証)」が提供されている。しかし、中には、「多要素認証」（2 つの要素の場合は 2 要素認証）と呼ばれる複数の認証方式を採用したホームページも存在する。ここで、「多要素認証」とは、①知識認証（パスワード認証、秘密の質問、暗証番号等)、②所有認証（メールアドレスにコードを送付する認証、SMS による認証、トークンを用いた認証等)、③生体認証（指紋、顔認証等）等の、複数の要素を組み合わせて認証を行うことでセキュリティを高める仕組みである。

この多要素認証を用いることで、万が一、１つの要素（たとえばパスワード）が流出したとしても、別の認証方式を突破しなければログインができないため、第三者に不正にログインされて、情報漏えいを防ぐことが可能となる。各ホームページによって多要素認証を提供しているか否かが異なるため、ログインした後に各種の設定画面を確認してほしい。

オ　バックアップを定期的かつ複数行うこと

バックアップは、少なくとも半年から 1 年に一度は行われるべきである。また、①元データに加えて最低 2 つのバックアップを作成することで、データを少なくとも 3 重に保存して、②2 種類以上の異なる種類のメディアに保存そして、③バックアップのうち 1 つ以上は異なる場所で保管するという「3-2-1」ルールを参考にバックアップを行うべきである。

データの消失は、記録メディアの故障のほか、パソコン内のファイルを暗号化してしまうランサムウェアに感染した場合にも起こりうることであるが、バックアップを適切に行っていれば、多くの場合にデータの完全消失を防ぐことが可能である。

カ　公衆無線 LAN（Wi-Fi）の使用を控えること

空港やファーストフード店等に設置された公衆無線 LAN（Wi-Fi）への接続は控えるべきである。空港やファーストフード店等には、公衆無線 LAN サービスの Wi-Fi スポットとも呼ばれるサービスを提供している場合がある。このような公衆無線 LAN サービスは、無線 LAN アクセスポイント機器から送出される無線 LAN の電波の識別名である SSID（Service Set Identifier の略）が付与されている。公衆無線 LAN の利用者は、この

SSIDに接続して同サービスを利用するが、SSIDを選択する際に、暗号化の鍵マークがついていない SSID については、通信が暗号化されておらず簡単にデータを盗聴することが可能であるため、利用は控えるべきである。また、暗号化の鍵マークがついている場合には、公衆無線 LAN の SSID に接続するためのパスワードを入力して利用することになるが、この暗号化の鍵マークがついている SSID であっても、暗号化の種類によっては第三者が暗号を解読し得ることもゼロではないため、データ盗聴の危険性は依然として存在する。さらに、SSID名は誰でも自由に設定することが可能であるため、SSID名からでは公衆無線LANサービスを提供しているSSIDと攻撃者のSSIDとを区別することができない。知らないうちに攻撃者の SSID に接続してしまえば、通信の中身を盗聴されたり、SSIDに接続する端末へアクセスされたりする可能性もある。したがって、自身が取扱う情報の重要性から判断して、安全性を重視した接続が必要な場合には、公衆無線LANを利用するのではなく、自身が用意したポケットWi-Fiやスマートフォンのテザリングの利用等、安全が確保されたインターネット接続を利用すべきである。

キ　プライバシーフィルターを活用すること

カフェや新幹線の車内等の公共の場所で、パソコンやタブレットを用いて作業を行う場合、隣や背後から情報を確認されないためにも、のぞき見を防止するプライバシーフィルターを活用すべきである。

ク　クラウドサービス等の利用規約等を確認すること

メールやファイルの受け渡し等、業務にクラウドサービス等を用いる場合には、その利用規約等の確認を行うべきである。特に、無料のクラウドサービスについては、利用規約等において、利用者が保存した情報の知的財産権の所在や、利用者が保存した情報に対するクラウドサービス事業者によるアクセスを予め承諾するか否か等の点に注意を払うべきである。無料のクラウドサービスは、無料であるが故に利用者の情報を金員に変えていることで成り立っている可能性のあることを心掛けるべきである。

ケ　攻撃手法等を把握すること

各自が情報セキュリティに関する知識を身に着けて、サイバー攻撃の手法についても把握したり、自身が所属する組織や事務所の現状のセキュリティ対策について把握をしたりすることが大切である。多くの攻撃手法を知ることで新たなサイバー攻撃であっても気づくきっかけになり、被害を防止することにつながるからである。

⑸　当会の方針

当会としては、以上で述べた視点に着目しつつ、当会会員に対して、情報セキュリティに関する情報の提供や、研修の機会を提供、「基本的な取扱方法」策定のための支援活動等を行い、弁護士全体の情報セキュリティに関する知識レベルの向上に努めていく次第である。

以　　上