# 「フェーズ3時代の到来―弁護士が知っておくべきサイバーセキュリティの12のポイント」
## ―民事裁判手続オンライン化に備えるために

近年進められてきた民事裁判手続のIT化は、いよいよ「フェーズ3」の段階に入った。今後、訴状のオンライン提出などを始めとして、民事裁判手続全体がオンラインで行われていく時代が到来することを意味する。そうなると、我々弁護士にとって、業務の根幹に関わる情報の安全性への配慮と、それを支えるサイバーセキュリティの知識が、これまで以上に重要になってくる。自らが情報管理の不備によりサイバー攻撃の踏み台となってしまえば、他の関係者に多大な損害を与える可能性もあるのである。

東京三会の弁護士業務妨害対策委員会では、2016年にインターネット弁護士業務妨害対策プロジェクトチーム（以下「本PT」という）を立ち上げサイバーセキュリティを調査研究しているが、2024年10月、「弁護士・法律事務所のためのサイバーセキュリティマニュアル（第二版）」*1を公開し、2025年1月には、東京三会の会員向けにサイバーセキュリティ講義を実施した。

本稿では、同講義に登壇した本PTメンバーが執筆者となって、弁護士が最低限押さえておくべきサイバーセキュリティの知識・対策について、12のポイントを挙げて解説する。基礎的な用語の確認やパスワード管理、ソフトウェアのアップデートといった基本的な事項から、生成AI時代における情報の扱い方、万が一の事故に備えるためのサイバー保険の活用法まで幅広く取り上げている。

弁護士業務妨害対策特別委員会

CONTENTS


ポイント❶「情報セキュリティ」「サイバーセキュリティ」って何？ 3頁
ポイント❷ 情報セキュリティの3要素とは？ 3頁
ポイント❸ サイバー攻撃の手口と実例を把握しよう。 4頁
ポイント❹ 日々進化するサイバー攻撃に備え最新の情報を収集しよう。 7頁
ポイント❺ 意識改革！ 8頁
ポイント❻ パスワード管理！ 8頁
ポイント❼ 添付ファイルを安全に送るためにはパスワードの伝え方に気をつけよう！ 9頁
ポイント❽ クラウドサービスに情報をアップロードする前にアップロードしてよいか確認しよう！ 9頁
ポイント❾ 万が一サイバー攻撃を受ける場合に備えて、サイバー保険の加入を検討しよう。 10頁
ポイント❿ サイバー保険の付帯サービスも有用である。 11頁
ポイント⓫ SNSアカウント乗っ取りと弁護士の信用毀損リスク―実務者に求められる備えとは？ 11頁
ポイント⓬ 生成AI活用と情報漏えいリスク―弁護士実務に求められる慎重な姿勢 12頁
「弁護士・法律事務所のためのサイバーセキュリティマニュアル（第二版）」ご利用のご案内 13頁


＊1：当会会員サイト　https://www.toben.or.jp/members/iinkai/gyoumubougai/file/cyber_security_manual_No2.pdf

ポイント❶

## 「情報セキュリティ」「サイバーセキュリティ」って何？

よく耳にする「情報セキュリティ」とはそもそも何を意味する言葉であろうか。

「情報セキュリティ」とは、要は組織や個人の情報を守ることである。より正確に言うと、許された者のみが（「機密性（Confidentiality）」）、正確な情報を（「完全性（Integrity）」）、利用できる（「可用性（Availability）」）状態を維持することとされている。総務省等の公的機関も、情報セキュリティの定義としてこの3要素が維持された状態という定義を採用しており、日弁連の弁護士情報セキュリティ規程もこの定義に従っている（2条1項）。

似た用語として「サイバーセキュリティ」がある。これは基本的には「情報セキュリティ」と異なる意味ではないと解されているが、全く同じではない。「サイバーセキュリティ」という概念はサイバーセキュリティ基本法に定められているところ、同法において保護の対象となる「情報」は「サイバーセキュリティ」の定義上、「データ」に限定されている。よって、例えば、何らかの手段を用いて人の記憶にある機密性の高い情報を引き出そうとする諜報活動を防止するための措置は、「サイバーセキュリティ」の対象ではないが、「情報セキュリティ」の対象とはなり得ることとなる。

**［第二東京弁護士会 会員　阿部 克臣（62期）］**

ポイント❷

## 情報セキュリティの3要素とは？

### ⑴　機密性（Confidentiality）

前述の3要素のうち、「機密性」（Confidentiality）とは、情報へのアクセスを認められた者だけが、その情報にアクセスできる状態を確保することを言う。逆に言えば、認められていない者には情報を使用（アクセス）させないということである。

法律事務所では、事務所で管理する顧客に関する様々な情報については、事務所内の所員だけがアクセスでき、外部からアクセスできないことである。機密性が損なわれ、情報が漏えいし、悪用されれば、顧客からの信頼の喪失に留まらず法的な責任を負うリスクも生じてくる。

機密性の高い情報は、できるだけ情報にアクセスできる人を減らすことで漏えいや悪用されるリスクを減らすことができる。例えば、機密性の高い情報を保有しているパソコンやサーバにログインできる人や方法を制限するなどのルールを設定したり、パスワードにより管理したりする方法がある。

### ⑵　完全性（Integrity）

3要素の2つ目の要素である「完全性」（Integrity）とは、情報が破壊、改ざん又は消去されていない状態を確保することを言う。言い換えれば、「正確な情報を」利用できる状態を確保することである。

サイバー攻撃と言うと情報の取得を狙ったものが多いと思われるが、最近は情報の破壊、改ざん又は消去を行う例も少なくない。ウェブサイトの改ざんが典型であり、法律事務所や弁護士会の被害も報告されている。

また、故意による情報の破壊、改ざん又は消去に限らず、過失による情報の消去もあるし、地震や火災などにより情報が消失し業務の継続性が困難になることもある。

完全性を高めるためには、前述の⑴機密性で述べたように、できるだけ情報にアクセスできる人を減らすことが重要である。また、情報にアクセスした者の操作や改変のログを残しておき、あとから変更したことが分かるようにすることにより、過失による変更や

犯罪者による変更を修復し、元に戻すことができることもある。さらに、可用性を確保するための方策の一つでもあるが、情報をバックアップすることにより、情報を消失したり改ざんされたりしても、消失前や改ざん前の状態に修復したり、いかなる情報が消失したか、改ざんされたかを確認したりすることが可能となる。

**⑶　可用性（Availability）**

3要素の最後の「可用性」（Availability）という言葉について、多くの弁護士は、普段、聞き慣れないかもしれないが、情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保することを言う。簡単に言えば、いつでも情報を利用可能な状態にしておくことである。可用性の低下を招く代表例として、情報機器のトラブルやサイバー攻撃がある。前者では、情報を管理しているパソコン、スマートフォン、サーバなどの情報機器に、電源の中断や容量不足、システム変更の失敗などでトラブルが生じると、当該情報機器が管理している情報にアクセスできなくなってしまう。また、後者の例として、パソコンなどの情報を暗号化して読めないようにして身代金を要求する「ランサムウェア」があり、法律事務所の被害も報告されているが、この攻撃を受けると暗号化された情報機器が管理している情報にアクセスできなくなってしまっている。

可用性を維持するためには、複数のパソコンの利用、ハードウェア・ソフトウェアともに安定したシステムの構築、またサイバー攻撃から防御するためにシステムを最新に保つこと、さらに情報を確実にバックアップすることなどが重要となる。

**⑷　3要素を維持するための事前・事後の対応が必要**

以上のとおり、情報セキュリティとは、「許された者のみが（機密性）」、「正確な情報を（完全性）」、「利用できる（可用性）」状態を維持することである。

「機密性」、「完全性」、「可用性」を維持できなかったことにより、事故が生じる。これを維持するためには、事故を未然に防止する事前の対策が必要となる。しかし、事前の対策をいくら取ったとしても、事故の発生を完全に防止することはできない。事故が発生してしまった場合には、「機密性」、「完全性」、「可用性」を回復する事後の対応が必要となる。

また、「機密性」「完全性」の維持の対策に傾きすぎるとルールが厳格になり、効率性が著しく悪くなり、「可用性」を損なうことになってしまうこともあるので、「機密性」「完全性」「可用性」のバランスも重要である。

［第二東京弁護士会 会員　阿部 克臣（62期）］

## ポイント3
## サイバー攻撃の手口と実例を把握しよう。

法律事務所は、弁護士業務を遂行する上で、顧客の個人情報や営業上の秘密に該当する重要な情報を多数取り扱っている。そのため、万が一、法律事務所がサイバー攻撃の被害に遭ってしまった場合には、顧客に多大な損害を与えかねないことはもとより、弁護士に対する信用も失墜する事態も起こり得る。サイバー攻撃の被害に遭わないように備えるためには、まずサイバー攻撃の手口とその実例を知ることから始まる。以下では、法律事務所も狙われるサイバー攻撃の実例を紹介する。

**1　マルウェア**

マルウェアとは、不正かつ有害な動作を行う悪意を持ったソフトウェアのことを指す。マルウェアの中でも、近年では、ランサムウェアとEmotet（エモテット）、サポート詐欺が特に猛威を振るっている。

ランサムウェアとは、パソコンなどの情報を暗号化して読めないようにして、身代金を要求するマルウェアである。2017年に世界的に流行したWannaCryptor（WannaCry、Wクリプトとも呼ばれる）がその代表である。

ランサムウェアによる被害としては、神奈川県弁護士会所属弁護士の法律事務所がランサムウェアに感染し、法律事務所内の共有サーバ内の電子データが使用できない状態になり、サーバ内のデータが漏えいした可能性も指摘されている実例が挙げられ、自分にはサイバー攻撃なんて無縁であるとは言えない状況にあることが分かる。


**ランサムウェア（WannaCryptor）に感染させられた端末の画面（IPA）**

※図出典：独立行政法人情報処理推進機構「事業継続を脅かす新たなランサムウェア攻撃について～「人手によるランサムウェア攻撃」と「二重の脅迫」～」（P4より抜粋）

また、隣接士業の例ではあるが、2023年6月、「社労夢」というクラウドサービスを提供する会社のサーバがランサムウェアによる攻撃を受け、クラウドサービスが約1か月もの長期にわたって停止し、「社労夢」を利用する多数の社会保険労務士事務所の業務に大きな支障が生じた被害実例も注目される。

次に、マルウェアの一種であるEmotetは、情報の窃取に加え、さらに他のマルウェアへの感染のための足掛かりとして利用されるマルウェアである。Emotetは、業務上開封してしまいそうな巧妙な文面の電子メールにマルウェアが添付されている点に特徴があり、注意が必要と言える。

Emotetによる被害としては、弁護士の利用する端末がEmotetと思われるマルウェアに感染した結果、メールの内容やメールアドレス等が窃取され、メールのやりとりを行ったことのある他の会員や日弁連の職員宛てに、スパムメールが送信されたり、メールのやりとりを行ったことのある他の会員や日弁連の職員の名前を騙って、スパムメールが送信されたりした実例が挙げられる。日弁連では、2020年10月、会員向けウェブサイトに「『Emotet』と呼ばれるコンピュータウイルスに関する注意喚起」を掲載して注意を促している。


※内閣サイバーセキュリティセンター「インターネットの安全・安心ハンドブックVer5.10」より

サポート詐欺とは、ユーザーがインターネットなどを閲覧中に、突然マルウェアに感染したかのような偽の画面を表示させるなどして、ユーザーの不安を煽り、画面に表示されたサポート窓口に電話をかけさせ、遠隔操作ソフト等をダウンロード、インストールさせ、サポートの名目で金銭を騙し取ろうとするものである。

サポート詐欺による被害としては、長野県の教員の業務用端末がマルウェアに感染したとする偽の警告画面が表示されたことから、教員が画面の指示に従って連絡先に電話をかけ指示に従ったところ、生徒の成績・進路資料等の情報が保存されていたパソコンを遠隔操作された実例が挙げられる。

### 2　電子メールやウェブサイトの閲覧による攻撃

標的型攻撃とは、特定の組織や人物を狙って電子メールやSNSを用いてサイバー攻撃を仕掛けるサイバー攻撃である。電子メールの添付ファイルを実行させる、ウェブサイトのURLをクリックさせる、メッセンジャーやチャットから誘導してマルウェアに感染させるという手法が用いられる。

標的型攻撃による被害としては、日本年金機構が攻撃され、日本年金機構の職員が、攻撃者から送信された電子メールを開封し、添付ファイルを実行するなどしたことにより、約125万人分の個人情報が流出した実例が挙げられ、標的型攻撃の被害に遭ってしまうと多大な情報漏えいの被害が発生してしまうことが見て取れる。

次にビジネスメール詐欺とは、海外の取引や自社の経営陣になりすまし、偽の電子メールを送って入金を促したり、個人情報が含まれたリストの送付を促したりする詐欺のことで、BEC詐欺（ベック詐欺）などとも呼ばれている。

ビジネスメール詐欺による被害としては、JAL本社財務部に対して、「ボーイング777型」をリースしている米国の金融会社の担当者を装った者から、リース料の支払先を香港の銀行の別名義口座に変更した旨の偽の請求書が添付された電子メールが届き、当該メールを信じたJALの担当者が、指定された香港の銀行口座に約3億6000万円を振込送金してしまった実例が挙げられる。


**サポート詐欺の画面イメージ（IPA）**

※図出典：独立行政法人情報処理推進機構「偽セキュリティ警告（サポート詐欺）対策特集ページ」より抜粋

### 3　ウェブサイトへの不正アクセスによる攻撃

ウェブサイトへの不正アクセスによる改ざんの被害は世界中で発生しており、日本の弁護士や弁護士会のサイトが改ざんされる事例も多発している。

ウェブサイトへの不正アクセスによる被害としては、札幌弁護士会所属弁護士のウェブサイトがハッキングされ、第一東京弁護士会所属の弁護士への殺害予告やわいせつ画像等がウェブサイトに掲載された実例が挙げられる。もし仮に自己が経営する法律事務所のウェブサイトが不正アクセスによる攻撃を受けてしまった場合を考えると、とても他人事には思えないのではないか。

### 4　フィッシングによる攻撃

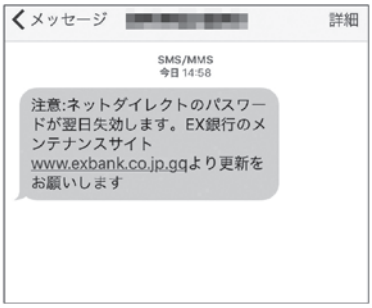
フィッシングとは、金融機関や企業など、信頼できる送信元を装った電子メールなどを不特定多数人又は特定の標的に送って、ID、パスワード、クレジットカード番号、個人情報、財産、企業秘密などを入力させて騙し取るネット詐欺の一種である。

フィッシングの方法としては、金融機関等のお知らせを装った電子メールを送り、「情報確認のため」等と称してURLをクリックさせ、あらかじめ用意した本

**標的型メールとスパムメールの例**

**標的型メールの例**


**スパムメールの例** SMSを使った例



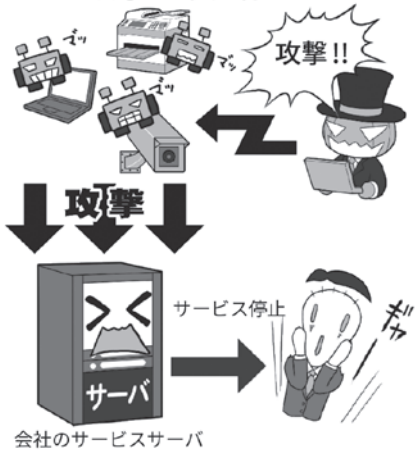

※内閣サイバーセキュリティセンター「インターネットの安全・安心ハンドブック Ver5.10」より

物のサイトにそっくりな偽サイトにユーザーを誘導し、誘導された先の偽サイトでIDやパスワード、クレジットカード情報や口座番号等を入力させ、入力させた情報を盗み取るというものである。

弁護士業務を行う上で、報酬口座や預り金口座でインターネットバンキングを利用している弁護士も少なくないと考えられるが、万が一、インターネットバンキングのIDやパスワードが、フィッシングにより不正に取得されてしまうと、不正送金が行われて多額の被害が発生しかねないことを意識しておくことが必要である。

### 5　DoS 攻撃、DDoS 攻撃

DoS攻撃（Denial of Service Attack）とは、攻撃目標となるウェブサイトやサーバに対し、大量のパケットを送り込むことで、高い負荷を掛けてウェブサイトやサーバをダウンさせて、サービスを妨害するという攻撃手法を指す。DDoS攻撃（Distributed Denial of Service Attack）とは、多数のコンピュータを用いたDoS攻撃を指す。




※内閣サイバーセキュリティセンター
「インターネットの安全・安心ハンドブックVer5.10」より

DoS 攻撃・DDoS 攻撃による被害としては、2024年12月、日本航空や三菱UFJ銀行が同日中に攻撃を受け、空港やネットバンキングに一時不具合が発生した実例が挙げられる。

［会員　服部 毅（60期）］

## ポイント4
## 日々進化するサイバー攻撃に備え最新の情報を収集しよう。

ChatGPTなどの生成AIの性能が飛躍的に向上するのに合わせて、サイバー攻撃も生成AIを悪用するなどして日々進化している。日々進化するサイバー攻撃に備えるには、情報セキュリティに関する最新の情報を収集することが欠かせない。

情報収集先としては、国家サイバー統括室（NCO：旧内閣サイバーセキュリティセンター（NISC））や警察庁のサイバー警察局Webサイト、総務省の国民のためのサイバーセキュリティサイト、独立行政法人情報処理推進機構（IPA）の情報セキュリティページなどが挙げられる。これらのウェブサイトのうち、例えば、IPAのウェブサイトでは、偽セキュリティ警告（サポート詐欺）対策特集ページを設けており、サポート詐欺の画面の閉じ方を体験することができる。事前にサポート詐欺の画面を疑似体験することで、慌てること

**情報収集先ウェブサイトの例**

**国家サイバー統括室（NCO）【内閣官房】**
※旧内閣サイバーセキュリティセンター（NISC）
https://www.nisc.go.jp/

**サイバー警察局【警察庁】**
https://www.npa.go.jp/bureau/cyber/index.html

**国民のためのサイバーセキュリティサイト【総務省】**
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/

**独立行政法人情報処理推進機構（IPA）**
https://www.ipa.go.jp/

**偽セキュリティ警告（サポート詐欺）対策特集ページ（IPA）**
https://www.ipa.go.jp/security/anshin/measures/fakealert.html

**サポート詐欺の電話番号に電話をかけてみた（動画公開）**
https://www.jc3.or.jp/threats/examples/article-570.html

なく適切に対応することができ、サポート詐欺による被害を未然に防ぎやすくなる。

また、一般財団法人日本サイバー犯罪対策センター（JC3）のウェブサイトでは、実際にサポート詐欺の電話番号に電話をかけた際のやりとりを動画にまとめたものが公開されており、サポート詐欺の手口を把握する上で役立つ。

是非本稿をご覧になった方は、前記各サイトを実際に確認することをお勧めする。

［会員　服部 毅（60期）］

## ポイント5
## 意識改革！

サイバーセキュリティ対策の基本として忘れてはならないのは、何よりも意識改革である。往々にして「自分は狙われるような情報を持っていない」「怪しいウェブサイトは見ないから大丈夫」「事務員や業者に任せておけば問題ない」などと考えがちであるが、このような思い込みや油断こそがリスクの源泉と言える。

現代社会においては、誰もが情報を扱う主体であり、弁護士のように個人情報を多く扱う立場では、その漏えいが顧客との信頼関係や事務所の経営、さらには自身の社会的信用まで失墜させる危険を孕む。近年では、個人情報保護法の改正により、漏えい時の報告義務や罰則も明確化され、意識の欠如が法的責任に直結する時代に突入したと言える。

したがって、弁護士は「サイバー攻撃は自分には関係ない」といった思い込みを捨て、自らの業務に対するリスク認識を高める必要がある。「自分には関係ない」という思い込みを捨て去ったとき、今すぐ実行できる対策は、システムやソフトウェア等のアップデートである。これにより、マルウェアに対する脆弱性が修正され、最新の攻撃手法への防御となるとともに、大多数のサイバー攻撃は予防できると言われている。

Windows10のサポートは2025年10月14日に終了した。以降はセキュリティ更新プログラムが提供されないので、もしWindows10を引き続き使用している場合には、安全性を確保するため、Windows11などの最新のOSへの速やかな移行を強くお勧めする。

［会員　坂本 尚志（62期）］

## ポイント6
## パスワード管理！

サイバー攻撃を受ける主要な原因のひとつが、パスワードの不適切な管理である。パスワードに対する主な攻撃手法として、リスト型攻撃（流出済みパスワードを使う）、総当たり攻撃（全通りを試す）、辞書攻撃（よくある単語の組み合わせ）などが存在する。これらを防ぐためには、強固なパスワードの設定が必要である。

本PTでは、英大文字・小文字・数字・記号を含む10桁以上のパスワードを推奨しており、これは理論上、総当たり攻撃によって突破するには数百年単位の時間を要することから、極めて有効な防御策とされている。

一方で、多くの人が複雑なパスワードを覚えることができず、複数のサイトで同じパスワードを使い回しているのが実情である。しかし、1つのサービスで流出したパスワードが他のサービスへの侵入に使われるリスト型攻撃の危険性を考えると、パスワードの使い回しは絶対に避けなければならない。

その解決策として、パスワード管理アプリ（1Password等）の活用や、慎重に保管された紙の記録などが有効と言える。

結局のところ、パスワード管理の質が情報セキュリティ全体の成否を左右するのである。

［会員　坂本 尚志（62期）］

## ポイント⑦
## 添付ファイルを安全に送るためにはパスワードの伝え方に気をつけよう！

メールに添付ファイルを付けて顧客とやりとりをすることが多いと思われるが、ファイルのパスワードはどのように伝えればよいだろうか。

添付ファイル付メールの本文にパスワードを設定する方法に意味がないのは当然として、ファイルにパスワードをかけた上で1通目のメールを送り、2通目のメールでパスワードを送る方法も安全ではなく、ほとんど意味がないと考えられている。メールアカウントを乗っ取られた場合やメールが盗み見られていた場合には、2通のメールが見られてしまうからである。また、2通目のメールでのパスワード連絡は、ほとんどの場合同じ宛先に送信されるため誤送信対策にならないとも言える。

そこで、メールでパスワードを設定したファイルを送る場合、パスワードをメールで伝えるという方法以外の方法で伝える必要がある。例えば、面談時にパスワードを決める、電話やSMSなどメール以外の方法でパスワードを伝えるといった方法が考えられる。後日、パスワードを忘れたので教えてほしいといった連絡があったとしても、メールで送るのではなく、メール以外の方法で伝えることが無難である。

メール以外に、できるだけ安全にファイルを送る他の方法として、例えば、インターネットを通じてデータを保管できるサービス（クラウドサービス）を利用する方法がある。これは、当該サービスに渡したいファイルをアップロードし、相手に当該サービスからダウンロードしてもらう方法である。

最近のクラウドサービスでは、特定のメールアドレスからのみアクセスを許可するものや、ダウンロード可能期間やダウンロード回数を設定できるものなどもあるので、これらの機能も活用すると良い。クラウドサービスは、間違ったファイルを保存しても相手のダウンロード前ならクラウド上から削除できるし、ダウンロード後にすぐに削除してデータを残さないという対応もできるなど、ファイル共有後もファイルを一定のコントロール下に置けるというメリットもある。アップロードするファイルの注意点については、ポイント⑧「クラウドサービスに情報をアップロードする前にアップロードしてよいか確認しよう！」を参照されたい。

現在でも2通目のメールにパスワードが記載されている例を目にすることがあるが、これを機に、ファイルを安全にやりとりする方法について再検討しておくことをお勧めする。

［第一東京弁護士会 会員　大澤 一雄（64期）］

## ポイント⑧
## クラウドサービスに情報をアップロードする前にアップロードしてよいか確認しよう！

メール以外に、できるだけ安全に情報を送る方法として、クラウドサービスに情報をアップロードし、相手においてダウンロードさせる方法があるが、クラウドサービスを利用するのか、するとして特定の情報をアップロードするのかについて確認する必要がある。

クラウドサーバ内にあるデータは所在地の国の法律が適用される可能性があるため、所在地の法律に基づき、その内容が検閲され、情報が流出する可能

性がある。そこで、クラウドサービス利用にあたっては、事業者の利用規約等を確認して、クラウドサーバの所在地が国内であるか否かを確認しておくことが肝要である。

次に、クラウドサービスの利用は、情報を第三者に預けることを意味するだけではなく、セキュリティについても第三者に委ねることを意味する。そのため、「政府情報システムのためのセキュリティ評価制度」（ISMAP）による認定を受けているクラウドサービスであるか否かを確認し、セキュリティ面で信頼することができるクラウドサービスを選別して利用することが重要である。

ISMAP（イスマップ）とは、政府が求めるセキュリティ要求を満たしているクラウドサービスをあらかじめ評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、政府機関等におけるクラウドサービスの円滑な導入に資することを目的とする制度である。

ここまでで、クラウドサービスを適切に選別できなければ、クラウドサービスを利用しないことも検討すべきである。

それだけではなく、事業者において、セキュリティ対策に万全を期したとしても、攻撃者にクラウドにアクセスされてしまい、情報が流出する可能性は否定できない。そこで、クラウドサービスにアップロードする情報について、たとえその情報が含まれたファイルが流出しても、その内容を閲覧できないようにファイルごとにパスワードをかけておくことが考えられる。

また、セキュリティ対策に完璧というものはない以上、クラウドで保管していた情報が流出する等の事態が生じてしまうと、弁護士が損害賠償責任を負うことも起こり得る。そのため、情報漏えい等の事態が起きたときに、クラウドサービス提供事業者において、どのような対応が行われるかについて利用規約等で確認しておく必要がある。具体的には、かかる事態が発生した場合の報告義務、報告の方法、損害賠償の責任範囲、データのバックアップ設定の有無等を確認しておくべきである。上記事態が発生した際に、クラウド上での情報のやりとりに関する記録（ログ）が保存されていれば、どの情報が流出したのか等を究明できるが、保存されていなければどの情報が流出したのか等を究明できず事後対応に支障が生じかねないため、ログを保存するサービスがついた内容で契約することが考えられる。

クラウドサービスにアップロードする情報については、検討を要する。例えば、刑事弁護の際に謄写した訴訟記録については刑事訴訟法281条の4に定める目的以外の目的での提供等が禁止されていること、犯罪被害者から委託を受けた弁護士が犯罪被害者保護法3条に基づき謄写した訴訟記録についても謄写の際に使用目的を制限し、その他適当と認める条件が付されたりするなど、法令上の要請からアップロードすべきかどうかについて慎重な判断を必要とする場合がある。

また、特定の情報（例：児童ポルノに関する情報）をアップロードすることが利用規約で禁止されている場合があり、こうした場合には利用規約違反を理由に当該サービスの停止等の措置が行われる可能性もあるため、利用規約の禁止事項にも目配りをする必要がある。

［第一東京弁護士会 会員　大澤 一雄（64期）］

## ポイント⑨
## 万が一サイバー攻撃を受ける場合に備えて、サイバー保険の加入を検討しよう。

どれだけサイバーセキュリティ対策を講じても、サイバーリスクを完全に抑えることは困難である。

そして、サイバーリスクが顕在化すると、顧客の機密情報を流出させてしまったり、一時的に法律業務が滞ってしまったりする。その結果、顧客への賠償責任が発生したり、費用が掛かったり、事業中断により売上が低下したりすることが想定される。

そこで、万が一に備えて、サイバー保険の利用を検

討することも一案である。

サイバー保険とは、サイバー攻撃を受けた場合に発生する損害や費用等を補償する保険である。サイバー保険の補償内容は、加入するプランやオプションとして追加する特約により異なるものの、基本的には、損害賠償補償（例えば顧客に対する賠償責任を補償）・費用損害補償（例えばフォレンジック調査（証拠の収集と分析）に係る費用を補償）・利益損害補償（事業中断に伴う逸失利益を補償）の3本柱からなる。

［第一東京弁護士会 会員　山岡 裕明（63期）］

## ポイント⑩
## サイバー保険の付帯サービスも有用である。

サイバー保険には、金銭的な補償に加えて、付帯サービスとして専門家の紹介サービスが含まれている。

サイバー攻撃を受けた場合、技術的対応が必要となるため、被害を受けた自組織だけで対応を行うことは容易ではなく、様々な専門家のサポートを受けることが重要となる。例えば、サイバー攻撃の原因や被害範囲について調査をする必要があるところ、第三者機関であるセキュリティベンダーにデジタル・フォレンジック調査を依頼することとなる。また、再発防止を策定するにあたっても、技術的な助言が必要となるため、信頼できるITベンダーを探す必要がある。

もっとも、有事の状況下において、これらの専門ベンダーを探すことは容易ではない。

そこで、有用なのは各保険会社が付帯サービスとして提供する専門家の紹介サービスであり、このサービスは保険会社が提携している外部の専門家の紹介を受けることが可能となっている。

また、昨今では、平時からのサービスも充実しつつあり、例えば自組織のセキュリティリスクの診断をしてくれたり、セキュリティ製品を紹介してくれたりもする。

金銭的な補償に加えて、こうした事故前と事故後の付帯サービスを受けることができるのも、サイバー保険の大きなメリットと言える。

［第一東京弁護士会 会員　山岡 裕明（63期）］

## ポイント⑪
## SNSアカウント乗っ取りと弁護士の信用毀損リスクー実務者に求められる備えとは？

### ■ SNSのセキュリティ

SNSは弁護士にとっても日常的なコミュニケーション手段となりつつあるが、その利便性の裏で、アカウントの乗っ取りによる深刻なリスクが顕在化している。特に弁護士は「信頼を預かる職業」であるがゆえに、SNSアカウントが乗っ取られた場合、単なるプライバシー侵害にとどまらず、社会的信用の毀損や守秘義務違反の疑いを招く事態にまで発展する可能性がある。

実際に、SNS乗っ取りによる被害では、アカウントからフィッシングサイトへ誘導するメッセージが無差別に送信されるケースや、偽広告や詐欺サイトのリンクが投稿されるケースが多く見られる。弁護士の名前で送られたメッセージは、一般ユーザーの名前で送られたものよりも開封・信用されやすく、受信者が騙されるリスクは一層高まる。弁護士の名義が「悪用される」こと自体が、周囲に不安と誤解を与え、信用毀損に直結するのである。

加えて、SNSで依頼者とのやりとりを行っている場合、乗っ取りにより事件情報等が第三者に閲覧され、守秘義務違反が問われるおそれもある。弁護士としては、「情報が漏れた」という事実だけでなく、

「情報管理体制そのものに問題があるのでは」と疑念を持たれる点にも自覚的でなければならない。

このような事態を未然に防ぐためには、他のウェブサービスと同様に、SNSにおいても次の対策を講じるべきである。

- 多要素認証の有効化
- 推測されにくい独自のパスワードの使用（サービスごとに別設定）
- 乗っ取りの主な手口（フィッシング、リスト型攻撃、アプリ連携）に関する知識の共有
- 定期的なログイン履歴やアプリ連携の確認と棚卸し

万一、乗っ取りの兆候（身に覚えのない投稿やログイン通知等）に気づいた場合には、即時にパスワードを変更し、必要に応じてアカウント停止・アプリ連携の解除を行い、被害の拡大を防止する必要がある。また、顧客等にも適宜説明・注意喚起を行うことで、信頼維持の観点からも重要なリスク対応となる。

弁護士がSNSを利用する以上、個人のセキュリティではなく職業倫理の一環として情報保護の意識を持ち、SNS 運用を「準業務インフラ」と捉えるべきである。

［第二東京弁護士会 会員　田中 健一（74期）］

## ポイント12
## 生成AI活用と情報漏えいリスク―弁護士実務に求められる慎重な姿勢

### ■生成AIサービスを活用する際のセキュリティ対策

ChatGPTやBing AI等に代表される生成AIは、文章作成やリサーチ支援のツールとして弁護士業務にも急速に浸透しつつある。しかし、その利便性の一方で、個人情報の漏えいや偽情報の混入といった実務上深刻なリスクが存在することを十分に認識しなければならない。

生成AIは、大量の学習データを基に自然な文章を出力することに長けているが、他方で、出力内容の正確性は保証されていない。すなわち、表面的にもっともらしい文章であっても、事実関係や法的評価に誤りを含む可能性が常にある。

そのため、生成AIの出力はあくまで参考資料として捉え、事実確認（ファクトチェック）を怠らないことが必須である。実際、米国では弁護士が存在しない判例を引用した結果、裁判所から制裁を受けた事例が報告されている。

さらに重大なリスクが個人情報の漏えいである。生成AIの多くは、ユーザーが入力した情報を今後の学習に利用し、他ユーザーの回答生成に影響を与える仕様となっている。たとえ非公開環境であっても、プロンプトに顧客の氏名、事件情報等の個人データを入力することにより、これが意図せず他者に再利用・露出されるおそれがある。実際に、2023年には生成AIのシステムバグにより、他人の入力内容が閲覧可能となる事例が発生している。

弁護士が本人の同意なく個人データを入力することは、個人情報保護法違反のみならず、弁護士法上の守秘義務違反にも該当する可能性がある。たとえ同意があったとしても、入力目的の限定性や必要性について慎重な判断が求められる。

生成AIがその内部処理を完全に制御・可視化できるわけではない以上、特定の依頼者情報やセンシティブ情報の入力は極力回避すべきである。

また、生成AIを扱う端末が不正アクセス等のセキュリティ被害を受けた場合、入力済のプロンプト履歴等が外部流出するリスクも否定できない。その意味で、生成AIの利用は単なる作業効率化ではなく、情報セキュリティ体制の一部として位置付けて運用管理することが必要である。

生成AIの活用は、あくまで弁護士業務の補助的手段であり、法的判断や情報管理の責任を代替するものではない。倫理と法令を遵守した利用設計が、生成AI時代の専門家としての信頼維持の鍵となる。

［第二東京弁護士会 会員　田中 健一（74期）］

## 「弁護士・法律事務所のためのサイバーセキュリティマニュアル（第二版）」ご利用のご案内

東京三会の弁護士業務妨害対策委員会では、2024年10月に「弁護士・法律事務所のためのサイバーセキュリティマニュアル（第二版）」を公開しているので、ご紹介する。

### ❶「弁護士・法律事務所のためのサイバーセキュリティマニュアル（第二版）」

2024年6月に弁護士情報セキュリティ規程が施行されたこともあり、我々弁護士は、これまで以上にサイバーセキュリティ対策への意識を高める必要が生じている。一方で、サイバー攻撃の手口は日々巧妙化し、その脅威は常に大きくなり続けている。裁判手続等のIT化が進展し、インターネットが弁護士業務に欠かせない現代において、弁護士は常にサイバー攻撃のリスクにさらされており、その脅威から依頼者の個人情報や機密情報を守るためには、最新の情報に基づいた適切なセキュリティ対策が不可欠である。

この度、2021年9月に公開した「弁護士・法律事務所のためのサイバーセキュリティマニュアル（初版）」の内容の見直しを行い、アップデートした。具体的には、初版公開後に新たに発生した具体的なサイバー攻撃の事例を多数追加したり、近年急速に普及しつつある生成AIサービスの利用に伴う新たな問題についても言及したり、万が一サイバー攻撃の被害に遭ってしまった場合の備えとしてのサイバー保険に関する項目を新たに設けたりするなどの情報をアップデートしている。

第二版においては、初版以上に、できるだけ分かりやすい説明を心掛け、具体的な対策・対処法を提示するように努めている。

### ❷ 当会及び日弁連の会員サイトからダウンロード可能

「弁護士・法律事務所のためのサイバーセキュリティマニュアル（第二版）」は、当会会員専用サイトの「ホーム＞会員サポート＞弁護士業務妨害相談」のページのほか、日弁連会員専用サイトの「HOME＞業務関係＞その他弁護士業務＞弁護士業務妨害＞インターネットによる弁護士業務妨害対策マニュアル」のページからダウンロード可能であるので、是非ご利用いただきたい。

「弁護士・法律事務所のためのサイバーセキュリティマニュアル（第二版）」が、会員の皆様のサイバーセキュリティ対策の一助となれば幸いである。