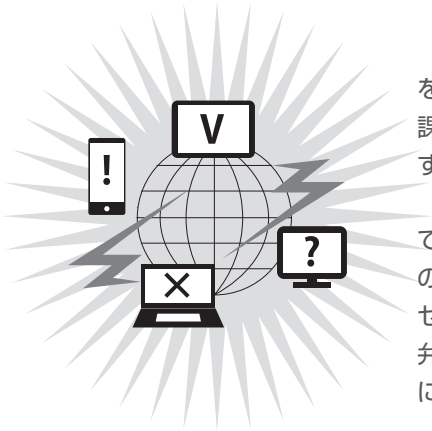
弁護士の情報セキュリティ

第二東京弁護士会会員　平岡　敦（55 期）



弁護士は，日常業務において営業の秘密やプライバシー等のセンシティブな情報を取り扱うので，守秘義務に照らしても，情報セキュリティの徹底が極めて重要な課題であることは異論がないであろう。情報セキュリティの徹底は，各弁護士に対する信頼にも直結するところである。

この点，日弁連は 2013 年に「弁護士情報セキュリティガイドライン」を制定しているが，抽象的な規定から具体的に何をどのように気をつけるべきかを読み取るのは，なかなか難しいと思われる。そこで，本特集では，日弁連内の弁護士の情報セキュリティに関するワーキンググループで同ガイドラインの策定にも関わった平岡敦弁護士に，私たちが日常業務においてどのような点に注意すればよいのかを，具体的にわかりやすく解説していただいた。（伊藤 敬史）

1　はじめに

弁護士がその業務で扱う情報は，センシティブで重要なものばかりである。DV 被害者の住所を漏えいすれば，たちまち生命や身体の危険を招来する。依頼者に送るつもりの電子メールを，誤って相手方代理人に送ってしまったら，それで訴訟の帰趨が決するかもしれない。

多くの弁護士は，そのような危険があることを十分に認識して，リスクを避けるために慎重に行動している。しかし，残念ながら，弁護士の過失による情報セキュリティ事故が発生している。

2　弁護士の情報セキュリティ事故

⑴　どのような事故が発生しているか

近年発生した弁護士が関連する情報セキュリティ事故の一部を**表 1** にまとめてみた。1 ないし 4 番は情報の漏えい，5 及び 6 番は情報の喪失，7 番は情報の毀損を招いた事故である。また，2 ないし 4 番は懲戒処分を受けている事案である。

表 1　情報セキュリティ事故一覧表

	漏えい・紛失・毀損の方法	対象となる情報
1	刑事事件の情報共有のために使用していた掲示板を，本来は非公開設定にすべきなのに公開設定にして利用し，誰でも見られる状態にしていた。	裁判員裁判の事件記録。裁判員候補者リストや被害者の情報を含む。
2	他事件の記録用紙を裏紙として使用して，別事件の記録を印刷し，事件記録としてファイリングしたが，裏紙であることを忘れて，依頼者に交付した。	他事件の事件記録の内容。
3	他事件の記録用紙を裏紙として使用して，FAX 文書を作成したが，送信時に裏表を間違えて送信した。	他事件の事件記録の内容。
4	事件の紹介者に対して，辞任後に訴訟経過など事件の顛末を報告した。その際に準備書面の一部なども交付した。	事件の内容。
5	事務所のサーバのハードディスクが故障し，事務所全体のデータが失われた。復旧に数百万円を要した。	事務所全体のデータ。
6	東日本大震災で事務所が水没し，パソコン内のデータが失われた。	水没したパソコンのデータ。
7	弁護士をメンバーとするメーリングリスト上にマルウェアに感染したメールが流れ，受信者の一部が感染し，パソコン内のデータが改ざんされた。	メール受信者のパソコン内のデータ。

(2) 掲示板誤公開事件の提起した問題

これらの事故の中でも，広く報道されて社会に大きなインパクトを与えたのが，2011（平成23）年に発生した**表1**〔4頁〕の1番の掲示板誤公開事件であった*1。この事件は，以下に挙げるようないくつかの重大な問題をはらんでいた。

① ITを使うべきか，使わざるべきか

この事件を発生させた法律事務所では，複数の弁護人が関与する事件の一部について，弁護士と事務職員をメンバーとする掲示板を事件毎に作成し，事件記録を共有していた。その理由は，担当弁護士が接見などで事務所を不在にしがちだったので外出先からも記録にアクセスする必要性が高かったこと，担当事務職員の関与も必要であったことなどである。この掲示板サービスは，民間業者が無償で運営するもので，データを格納して共有する機能や，メーリングリストの機能を有していた。これらの機能を利用して，事件記録を共有していたのである。この掲示板サービスは，既定の設定が「公開」であったので，開設後に「非公開」に変える必要があった。しかし，一部の掲示板について，過失により「非公開」設定に変えていないものが残っていた。

誤って開示されていた掲示板の中には，対象事件が裁判員裁判であり，格納した情報の中には犯罪被害者の情報や裁判員候補者名簿などが含まれているものもあった。

確かにITツールは便利であり，ITツールをまったく使わない弁護士業務を想像することは難しい。ITツールに一定の危険性があるから一切使わない，というのは弁護士業務の高度化や効率化を無視した暴論である。自動車は危険だからいっさい乗らない，医薬品は副作用があるからいっさい飲まない，というようなものである。しかし，自動車も医薬品も利用しないでは現代の社会生活は成立しない。ただ，もちろん安全装置の付いていない自動車や副作用の強すぎる医薬品の使用を避けるべきである。ITツールも同様である。セキュリティ対策のまったく施されていないような，又は明らかにリスクのあるものを用いることは避けるべきなのである。

本件の掲示板誤公開事件でも，文書共有のためにITツールを利用すること自体は否定すべきことではない。しかし，本件で問題となったような掲示板サービスを使うことは避けるべきであった。

② 扱っていい情報といけない情報

本件では，裁判員裁判事件に関する掲示板が設置され，そこでは裁判員候補者名簿や犯罪被害者に関する情報が共有され，結果として漏えいした。

関係者間で必要な情報を共有して高度に活用することは，弁護士業務の質を高め，迅速な処理を行う上で必要なことであり，情報共有のためにITツールが利用されることが否定されてはならない。しかし，裁判員候補者名簿*2や犯罪被害者の個人情報など，

＊1：中央官庁でも2013（平成25）年にGoogleグループという掲示板サービスを使った漏えい事故が起きて，同様の問題を惹起したことは，記憶に新しい。

＊2：裁判員の氏名等の漏示については，裁判員の参加する刑事裁判に関する法律109条に罰則が設けられている（一年以下の懲役又は五十万円以下の罰金）。

弁護士が取り扱う情報の中でも特に慎重な取扱いが求められる性質の情報については，いったん漏えいすると拡散する危険のあるデジタル情報にすること自体を避けるべきであった。

③　サービス規約の問題

本件で問題となった掲示板サービスには，サービス規約上も問題があった。サービス規約では，ユーザがアップした情報について，サービスを提供している企業に，自由に複製・公開などができる権利が留保されていた。企業がアップされている内容をのぞき見することはもちろん，「法律事務所での活用例」などとして広く紹介することも不可能ではなかったのである。これは，被疑者や被告人との関係では，掲示板にアップした時点で守秘義務違反を犯しているとも言える状況であった。

現在，広く使われているサービスの中にも同様の規約を有しているものは多い。弁護士として業務でこのようなサービスを利用することは避ける必要がある。

④　弁護士自治の問題

弁護士自治は，弁護士会が会員に対して必要な監督を行うことによって，弁護士の不祥事について自浄能力を発揮できることが前提となっている。しかし，本件事故のような情報セキュリティ事故について，弁護士会はそれまで十分な対策を講じてこなかった。この点，情報セキュリティに関する一定のルールを有していた裁判所や検察庁には差を付けられていた。弁護士会が十分な監督機能を発揮できないのではないかとの疑いを抱かれても仕方がない状況だったのである。

弁護士自治を守るためには，弁護士会として情報セキュリティに関する対策を講じて会員に対する適切な指導を行う必要がある。そこで，この事件のあと，日弁連内に弁護士の情報セキュリティに関するワーキンググループが設置され，2013（平成25）年には「弁護士のための情報セキュリティガイドライン」が作成され告知された。

このように掲示板誤公開事件は，実に様々な弁護士の情報セキュリティに関する問題提起を生み出した事件であった。

(3)　情報の喪失・毀損型の事故も重要

表1〔4頁〕の5（サーバのハードディスク故障によるデータ喪失），6（災害によるデータ喪失），7（マルウェア感染によるデータ毀損）も，情報セキュリティ事故の一類型である。確かに，情報の漏えいは依頼者などとの関係で弁護士業務にとって大きなリスクである。しかし，情報の紛失や毀損も弁護士業務の大きな阻害要因である。

「記録が見つからない」などという事態は，多かれ少なかれ誰しも経験があることである。また，パソコンやハードディスクの故障や災害によるデータ喪失も無視できないリスクである。ハードディスク関連企業の調査によると，ハードディスクを4年間使用すると，20％に故障が発生するとの報告がある*3。

データが失われると，紙から再現したり，依頼者や相手方からデータを再度受領したりするなど，大きな時間的・経済的コストが掛かり，信用問題にもつながる。したがって，サーバやパソコン内のデータについては，定期的にバックアップを取る必要がある。また，取得したバックアップは，事務所外で保管しないと盗難や災害には対応できない。

＊3：Blackblaze社の2013年の調査結果。

弁護士の事例ではないが，2012（平成24）年に発生したファーストサーバ社（クラウド事業者）の大量データ喪失事件では，親会社が12億1900万円の特別損失を計上していて，その損害の大きさがうかがわれる。

3　弁護士を取り巻く情報セキュリティ法規制

われわれ弁護士を取り巻く情報セキュリティに関する法規制や倫理規定には，以下のようなものがある。

(1)　刑事法

秘密漏示罪（刑法134条1項）

故意に業務上知り得た秘密を漏らしたとき，6か月以下の懲役又は10万円以下の罰金

裁判員の氏名等漏示罪（裁判員裁判法109条）

故意に裁判員候補者名簿等を漏らしたとき，1年以下の懲役又は50万円以下の罰金

(2)　民事法

準委任契約上の善管注意義務（民法656条，644条）

不法行為にもとづく損害賠償義務（民法709条）

事件の紹介者に対して，辞任に際して事件の顛末を話し，準備書面の一部を交付したことが不法行為に当たるとされた裁判例がある（**表1**〔4頁〕の4番）*4。

(3)　行政法

秘密保持義務（弁護士法23条）

弁護士又は弁護士であった者は，職務上知り得た秘密を保持する権利と義務を負う。前掲大阪地裁の裁判例では，本条が民事責任の根拠としても機能している。「職務上知り得た秘密」なので，弁護士会活動などで知り得た秘密も含まれる。

安全管理措置義務（個人情報保護法20条）

個人情報取扱事業者*5は，個人データの漏えい，滅失，毀損の防止その他の安全管理措置を講ずる義務を負う。

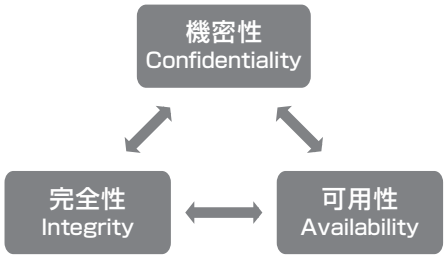
サイバーセキュリティ基本法上の義務

明確に弁護士を名宛人とした規定はない。ただし，国民はすべからくサイバーセキュリティの重要性に関する関心と理解を深め，サイバーセキュリティの確保に必要な注意を払うよう努める義務を負う（9条）。

COLUMN　コラム

セキュリティの3要素

セキュリティ事故を漏えい型と紛失・毀損型に分類したが，これはセキュリティの3要素と言われる分類に対応している。セキュリティというと，一般的には「漏えい」を思い浮かべるが，これはセキュリティの1つの要素に過ぎない。漏えいによって保全されなくなるセキュリティの要素は，機密性（Confidentiality）と言われる。情報へのアクセス権限のある者だけがアクセスできる状態を指す。セキュリティは，この機密性のほかに，完全性（Integrity）と可用性（Availability）という2つの要素があるとされている。完全性とは，情報が改ざんされていない状態のことをいい，可用性とは，必要なときに情報にアクセスできることをいう。これら3つの要素の頭文字を取って，セキュリティの3要素のことをCIAと呼ぶ。



*4：大阪地判平成21年12月4日判タ 1345号196頁

*5：平成27年改正によって個人情報取扱事業者についての「保有する個人データの数が過去6月以内のいずれの日においても5000を超えない」という制限が撤廃されたので，弁護士及び弁護士会もすべからく個人情報取扱事業者に該当することとなる。

COLUMN コラム

サイバーセキュリティ基本法

サイバーセキュリティ基本法は，2015（平成27）年1月に施行された法律であり，サイバーセキュリティに対する脅威の高まりを背景に，サイバーセキュリティの確保を目的として，国・地方自治体，ネットワーク業者などの重要社会基盤事業者，サイバーセキュリティ関連事業者などの義務を定めた法律である。

弁護士や弁護士会の役割は直接規定されていないが，サイバーセキュリティ施策の推進に当たっては，国民の権利を不当に侵害しないように留意しなければならない（3条6項）とされているので，弁護士は国民の側に立って，政府による行き過ぎたサイバーセキュリティ対策によって生ずる権利侵害に対抗する必要がある。

また，いずれは環境権のような請求権的権利として，良好なサイバーセキュリティが保たれたIT環境の生成・維持を求める権利が認められる時代が来るのではないだろうか。

(4) 倫理規定

秘密保持義務（弁護士職務基本規程23条）

弁護士は，依頼者について職務上知り得た秘密を漏えい・利用してはならない。弁護士法23条と比較すると，主体が弁護士に限定され，対象が職務上知り得た秘密に限定されている。

事件記録に関する義務（弁護士職務基本規程18条）

弁護士は，事件記録の保管・廃棄に際して，秘密及びプライバシーに関する情報が漏れないよう注意しなければならない。対象を事件記録に含まれる秘密・プライバシーに限定して注意義務を課している。

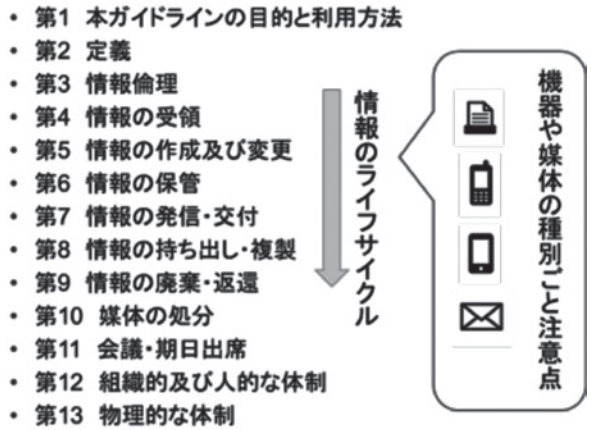
4 弁護士情報セキュリティガイドライン

以上見てきた弁護士に対する法規範は，いずれも抽象的な義務を定めるものである。また，セキュリティ対策は，平面的な規範だけでは実現できない。具体的なリスク評価を行い，それに応じて弁護士ごと・事務所ごとのセキュリティ対策を立て，それを実施・検証していくPlan・Do・Check・Actサイクルを回していく必要がある。その一助となるために2013（平成25）年に弁護士セキュリティガイドラインが作成された*6。

位置づけとしては規程や規則ではなくガイドラインであり，懲戒の直接的根拠となるものではない。ただ，職務基本規程18条などへの違反の有無を判断する際の間接的な資料とされる可能性がある。

対象は，サイバーセキュリティだけではなく，紙媒体の情報も含む。名宛人は弁護士である。強く推奨する取り組みについては「すること」，物的・人的・経済的環境に応じて推奨する取り組みについては「望ましい」という記載をしている。

章立ては以下の通りであり，情報の生成から消滅までのライフサイクルを縦軸に，情報を取り扱う機器（パソコン，FAX，携帯など）や媒体（電磁的記録，紙など）の種別を横軸に，それぞれの場合における情報を取り扱う上での注意点を述べている。



ただ，このガイドラインは抽象的な内容であり，弁護士個々の使用環境に応じた具体的なガイドラインで

＊6：ガイドラインは，日弁連のホームページからダウンロードできる。
https://www.nichibenren.jp/opencms/export/sites/default/news/documentFile/2014/securityguideline.pdf

はない。今後は，代表的な使用環境に応じた具体的なガイドラインを作成していく必要がある。

しかし，どれだけ具体化しても，弁護士や法律事務所との使用環境には個別性があり，それぞれに完全にフィットしたガイドラインを示すことは不可能である。ガイドラインをベースとして，各人が自己の環境に応じたリスク管理とセキュリティ対策を立てて実施する必要がある。情報セキュリティ対策は，一律の基準を示すことができないのである。

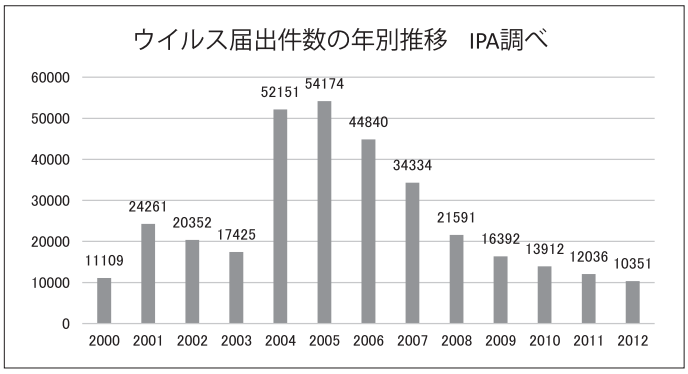
5　具体的な対策方法

上記の通り，セキュリティ対策は個別性が強いので，すべての方にフィットする対策方法を示すことはできないが，代表的なリスクとその対策方法を 情報の受領 → 保管 → 発信･交付 → 持ち出し･複製 → 廃棄 の各場面に沿って概説する。なお，日弁連ではビデオ研修も用意しており，無償で受講できる*7。

(1)　情報の受領の場面

いかなるリスクがあるか？

電子メールの添付ファイルにマルウェア*8が仕込まれていて，それをダウンロードすることによって，ファイルが盗まれたり，毀損されたりするなどの意図しない動作をしてしまうことがあることは，広く知られている。



（独立行政法人 情報処理推進機構，2013 年）

ただ，上右図のように最近はマルウェアの届出件数自体は減少傾向にある*9。ウィルス対策ソフトウェアなどが普及したことが原因であろう。

しかし，マルウェアを使った攻撃でも，より意図的で巧妙な手法が広がりつつある。いわゆる「標的型攻撃」である。今までのマルウェアによる攻撃は，不特定のパソコンを対象として行われていた。しかし，標的型攻撃は，最初から意図して特定のパソコン又はそのユーザを狙い撃ちにするものである。最近では，年金機構に対して標的型攻撃が仕掛けられ，125 万人の個人情報が漏えいしたことが記憶に新しい。以下は，そのときに年金機構の職員に送られた攻撃メールの文章である。この攻撃メールの発信者は，企年協（企業年金連絡協議会）という実在の団体を詐称している。

> 件名:「厚生年金基金制度の見直しについて（試案)」に関する意見
>
> ○○ ○○様
> 5月1日に開催された厚労省「厚生年金基金制度に関する専門委員会」最終回では，厚生年金基金制度廃止の方向性を是とする内容が提出されました。これを受けて，企年協「厚生年金基金制度の見直しについて(試案)に関する意見」を，5月5日に厚労省年金局企業年金国民年金基金の■■課長に提出いたしました。
> 添付ファイルをご覧ください。

上記のメールに添付ファイルが付いており，それを

＊7：https://kenshu.nichibenren.or.jp/product/detail.php?pid=19711
＊8：「マルウェア」とは，不正プログラムのことであり，ウィルス，トロイの木馬，スパイウェア，ボットなどの種類がある。
＊9：独立行政法人情報処理推進機構の1990年から2012年までの調査結果。

コラム COLUMN

年金機構事件の問題点

年金機構の事件では，攻撃が数次にわたって行われ，最初の2回の攻撃では被害が発生しなかったにもかかわらず，3回目の攻撃で個人情報の漏えいが発生した。最初の2回の攻撃時点で情報が共有され，注意喚起が十分になされていたら，3回目の攻撃も防止できたかもしれない。

また，個人情報を格納しているデータベースが外部と接点のあるネットワークに接続していたという構造上の問題もあった。掲示板誤公開事件でも問題となった「扱っていい情報と扱ってはいけない情報を切り分ける」という視点が重要であると再認識させられる事件である。

複数の受信者がダウンロードした結果，それらを起点にしてマルウェアの感染が広がり，個人情報が盗取された。同様の標的型攻撃メールを弁護士向けに作成することも容易である。

どのように対応するのか？

予防的対策としては，ウィルス対策ソフトウェアの導入，差出人や件名に不自然さを感じたら開封しない，発信者のメールアドレスがフリーメールではないか確認する，などの方法が考えられる。

しかし，標的型攻撃が巧妙に行われると，それを見破ることは事実上困難である。したがって，事後的な対策が重要となる。感染に気付いたらすぐにLANケーブルを外す，無線LANステーションの電源を切るなどして他のパソコンに影響を与えないようにすることが必要である。

(2) 情報の保管の場面(紙)

いかなるリスクがあるか？

紙の記録は，管理が不十分で所在が分からなくなることによる紛失のリスクと，災害などによる喪失のリスク(CIAでいうところの可用性に関するリスク)。記録の中に綴じ込まれているはずの「あの紙」がない！などという経験は，多かれ少なかれあるものだ。試算だが，全弁護士数約3万5000人(2014年度弁護士白書)が1年に1回15分間書類を探すとすると，その総計は52万5000分(8750時間)にもなる。1時間2万円の損失とすると，合計で1億7500万円もの損失となる。

3万5000人×0.25時間×2万円＝1億7500万円

どのように対応するのか？

紙文書の所在不明事故や災害による喪失をなくすためには，適切な分類と保管が必要である。補助的な対策として，印刷物の元となった電子文書やスキャンして作成したPDFなどバックアップとなるものを適切に分類・保管することが考えられる。IT技術は情報セキュリティ上の災厄をもたらすだけではなく，情報セキュリティ事故を防ぐ道具にもなる。ただ，電子媒体として保管することで増すリスクもある。このような二律背反的な関係は，情報セキュリティを考える上の永遠の問題である。

(3) 情報の保管の場面(パソコン)

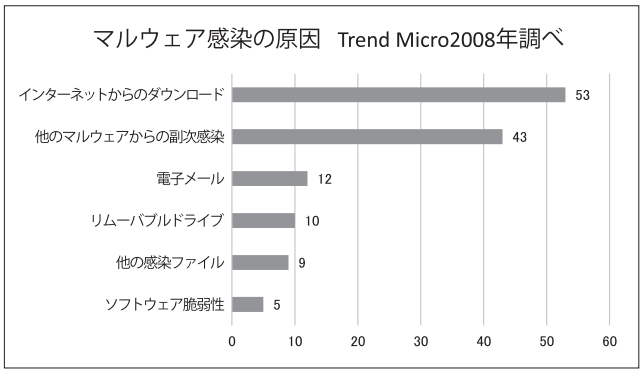
いかなるリスクがあるか？

パソコンに保管中のデータを喪失したり，改ざんされたりするリスクには，いくつかの種類がある。

- マルウェアへの感染
- 機器(ハードディスクなど)の故障
- 誤操作

マルウェアへの感染ルートは，電子メールの受信に伴うものよりも，ウェブサイト閲覧に伴うものや，他の感染源からの副次的感染の方が圧倒的に多い。

また，機器(ハードディスクなど)の故障は，実感よりも頻発している。前述した調査結果では，ハードディスクを4年間使用し続けると，その20％に故障が発生するとのことであったが，パソコンを使用してい



（トレンドマイクロ株式会社，2008 年）

る者の実感としては，それほど多くの故障に出会うわけではない。しかし，それはハードディスクが故障したとしても，ハードディスクの枢要な箇所でなければ，ハードディスク全体のデータが失われることはないからである。運悪く枢要な箇所が故障すれば，全体のデータが失われる。故障は発生しているが，運良く大きなデータ喪失にはつながっていないだけかもしれないのである。

どのように対応するのか？

――― マルウェアへの感染に対応する ―――

マルウェアへの感染を防ぐ方法には，以下の3種類がある。

- 危険に近づかない
- 危険に触れても感染しないようにする
- 事後的な対策を迅速に行う

危険に近づかないようにするためには，作成者の身元がはっきりしないウェブサイトは閲覧しないという方法が考えられる。ただ，職務上，そのようなサイトにアクセスせざるを得ない場合も考えられる。そのようなときには，事件記録などが格納されているサーバとは接続していないネットワークに接続したパソコンからアクセスすることが望ましい。

危険に触れても感染しないようにするためには，WindowsやMacOSなどの基本ソフトウェアのセキュリティアップデートを行う，基本ソフトウェアに組み込まれていたり，別途購入できたりするマルウェアに対抗するソフトウェア（ファイアウォール，ウィルス対策ソフトウェアなど）を機能するようにしたり，インストールしたりしておくなどの措置が考えられる。

なお，感染の原因となる脆弱性は，基本ソフトウェアよりも基本ソフトウェアの上で使われるミドルウェアの方に多く見られる。最近の感染経路の多くが，Adobe Flash Player，JRE，Adobe ReaderなどのMicrosoftやAppleといった基本ソフトウェアメーカーではない会社が作成したミドルウェアに存在するセキュリティ上の弱点を狙ったものとなっている*10。これらのソフトウェアは，基本ソフトウェアに較べてアップデートを怠りがちなので，攻撃者の標的になりやすいのである。したがって，これらのミドルウェアについては，必要がないものは使わない*11，必要があるものはセキュリティアップデートを怠らない，などの措置を執る必要がある。個々のソフトウェアごとのアップデート方法は個別性が強く，ひとつひとつ解説することはできないが*12，多くの場合アップデートを行うようにメッセージが出るので，そのようなメッセージが出たら，それに従ってアップデートを行うべきである。

Adobe Flash，Adobe PDF Reader，
Java（JRE）などのアップデートを忘れずに！

＊10：2015年の日本アイ・ビー・エム株式会社マネージド・セキュリティー・サービスの調査（2015年上半期Tokyo SOC情報分析レポート）によるとウェブサイトの閲覧に伴う感染の99%がAdobe Flash Playerを経由したものであった。なお，脆弱性が発見されるとそのソフトウェアが狙われるので，どのソフトウェアが感染源になるかは，年と時期によって大きく変動する。

＊11：ミドルウェアを使わない方法としては，アンインストール（取り除いてしまう）方法もあるが，ブラウザーでは，それらのミドルウェア（プラグインという）を使用したいときだけ使用するように設定することもできる場合もある。Adobe Flashはアニメーションや音声の再生などを行うウェブサイトで用いられているが，再生の必要はないことの方が多いので，動作しないように設定した方が無難である。

＊12：Adobe Flashに関しては，下記のサイトで最新版か否かの確認ができ，アップデートもできる。
https://helpx.adobe.com/jp/flash-player/kb/235703.html

マルウェアに感染してしまった場合の事後的対策としては，感染を広げないために迅速に当該パソコンとネットワークの接続を切ることが重要である。その上で，マルウェアを駆除するソフトウェアを動かして，感染を除去する必要がある。ただし，最近はゼロデイ攻撃といって，セキュリティ会社が対応を取る前に次々と新しいマルウェアを作成して攻撃する手法があり，そのような攻撃に対しては，駆除は有効ではない。そのような場合には，当面，その感染したパソコンを使わない，という対策を取るほかない。

――― 故障や誤操作に対応する ―――

ハードディスクなどの故障や誤操作を100％防止することはできない。したがって，これに対応するためには，データを喪失したときのリカバリー策としてバックアップを取っておく以外に有効な手立てがない。

COLUMN コラム

無線LAN（Wifi）のリスク

公衆無線LANサービスが普及しており，弁護士会館でも利用できる。しかし，誰でもアクセスできるタイプの無線LANは，同じ回線を見知らぬ人同士で共有していることを忘れてはならない。パソコンにはファイルやプリンタの共有機能があり，既定の設定では一部のファイルについて公開する設定になっている。そのままセキュリティ設定のないホテルや空港などの無線LANサービスに接続すると，公開されたファイルが丸見えとなってしまう。筆者がそのようなサービスに接続して試してみたところ，多くのファイルが公開されていた。各自のパソコンの設定をよく確認して欲しい。

バックアップの方法としては，単純なものとしては，市販のUSB接続のハードディスクを買ってきて，それをつないでコピーするという方法が考えられる。ただそれをパソコンと同じ場所に置いておいたのでは，災害や盗難に対応できない。

もうひとつの方法としては，ネットワークを経由して提供されるクラウドサービスで保管する方法がある。Dropbox，Googleなどが比較的安価な保管サービスを提供している。ただ，無償のサービスには規約上，守秘義務が担保されていないものもあるので，注意が必要である。

(4) 情報の保管の場面（可搬電子媒体）

いかなるリスクがあるか？

スマートフォン，ノートパソコンやデジタルカメラで使われるSDカード，USBメモリなどの持ち運びができる電子媒体（可搬電子媒体という）には，下記のような特徴がある。

- 小さいので紛失しやすい
- 貴重な情報が格納されている

統計*13によると，携帯電話をもっている人の2.6％が携帯電話を紛失した経験を有するとのことである。また，セキュリティ対策会社が模擬試験を行ったところ，スマートフォンを拾得した人の実に96％が中身を見ようとしたそうである。

このようにリスクにさらされている可搬電子媒体であるが，その反面，利便性ゆえに電話帳や電子メールなど貴重かつ秘匿性の高い情報が満載なのである。

＊13：日本ネットワークセキュリティ協会の2011年の調査。

どのように対応するのか？

可搬電子媒体に対するリスクに対応するためには，以下のような方法が考えられる。

- 不必要な情報を入れない
- パスワードロック，暗号化など防御措置

可搬電子媒体に入れる情報は必要最低限のものにしたい。特にUSBメモリやSDカードなどには，本当に必要な情報しか入れないようにしたい。特にUSBメモリを恒久的な保存媒体として使用することは避ける必要がある。なぜなら，紛失のリスクが高いほか，データ破損の危険も高いからである。

また，最近は，刑事記録の閲覧などのときにコピーの代わりにデジタルカメラで撮影することが多く行われるが，撮影したデータはできるだけ早く安全なパソコンに移し，いつまでもSDカード内で保管することは避けたい。

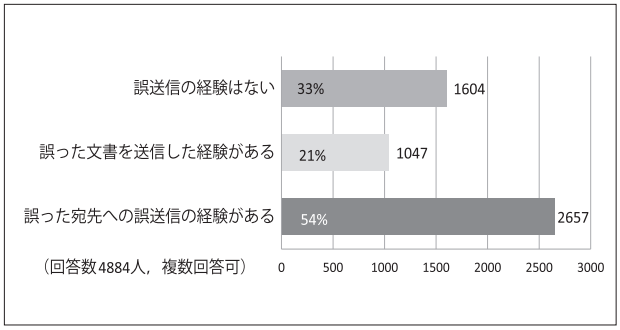
また，ノートパソコンなどを使用する際には，ノートパソコンのハードディスクにはできるだけ情報を格納しないで，サーバに格納してVPN*14経由でアクセスしたり，クラウドサービスで保管してアクセスするなどの方法を取るべきである。

どうしても可搬電子媒体に情報を格納せざるを得ないときでも，必ずパスワードロックを掛ける，情報を暗号化して保管するなどの措置を執る。これらの措置を執ると，可搬電子媒体を使用する際にいちいちパスワードを入れたり，暗号の復号処理で処理速度が落ちたりして，不便である。しかし，セキュリティを確保するために，一定の範囲で効率性が低下することは避けがたい。効率性とセキュリティの確保のバランスをどのように図るのか，これを各人の使用環境やリスクの程度などと相談しつつ，適切に設定していくことが必要である。

(5) 情報の発信・交付の場面

いかなるリスクがあるか？

弁護士がよく使う発信媒体には，FAXと電子メールがある。FAX誤送信による事故は，過去に懲戒事例（**表1**〔4頁〕の3番の事例）もある。2013（平成25）年の日弁連の調査*15によると回答数475人中90人（18.9％）がFAX誤送信の経験を有している。また，民間の調査*16によると，下記のような割合でFAX誤送信が発生しているとのことである。



（NPO日本ネットワークセキュリティ協会，2011年）

＊14：VPNとは，Virtual Private Networkの略称。インターネットは公共ネットワークであるが，それをまたがってLANなどの私的なネットワークを接続させる技術である。ルータなどのネットワーク機器に予め備わっているVPN機能を使用する方法や，VPN用のソフトウェアを導入する方法などがある。いずれも安価に利用でき，外部業者にデータを委託することに伴うリスクを避けることができる。

＊15：第18回弁護士業務改革シンポジウム基調報告書150頁。

＊16：NPO日本ネットワークセキュリティ協会による2011年の調査結果。

COLUMN コラム

リスクへの対応方法の分類

リスクへの対応方法には，①回避，②移転，③低減，④保有の４種類があるとされている。

①回避は，リスクに近づかないことでリスクを取り去る方法である。可搬電子媒体のケースで言えば，スマートフォンを持たない，スマートフォンにはデータを入れない，などの方法が回避に当たる。

②移転は，リスクを取り去ることができないので，他者に移転することである。例えば，情報漏えい保険や弁護士賠償保険に入る，といった方法が考えられる。

③低減は，保有せざるを得ないリスクをできる限り低減させることである。例えば，スマートフォンにパスワードロックを掛ける，データを暗号化する，などといった方法である。

④保有は，低減策を講じても保有せざるを得ず，かつ，回避するわけにもいかないリスクを甘受することである。

これは，情報セキュリティのみならず，あらゆるリスクへの対処方法に当てはまる。弁護士は，リスクを見極め，回避，移転，低減そして保有を選択していく必要がある。

電子メールの誤送信も日常よく目にする。前述の2013（平成25）年の日弁連の調査によると，弁護士の12％が電子メールの誤送信を経験している。

また，最近はTwitterやFacebookなどのソーシャルネットワーキングサービス（SNS）で情報発信する弁護士も増えているが，誤って守秘義務の対象となる事項をアップしていわゆる「バカッター」にならないように気をつけなければならない。守秘義務の対象事項を第三者に分かる形で漏えいしたわけではないが，事件の依頼者には自分のことを述べていると分かる内容の投稿をブログで行ったことが，弁護士の品位を害するとして懲戒の対象となった事例もある。

どのように対応するのか？

FAXや電子メールの誤送信を防ぐためには，まずリスクを回避する方法として，重要な文書はFAXや電子メールでは送らないという対処方法が考えられる。

しかし，迅速性・利便性の要求などからFAXや電子メールを使用しないわけにもいかないのが現実である。そこで，FAXについては，宛先の番号を分かり易く大きく書いておく，送信前に自分以外の人に確認してもらう，送信開始後もFAX機器の側を離れず，正しく送信されているかを確認する，などの方法で可及的に誤送信を防止する。

電子メールについても，重要な内容はメール本文には記載せず，パスワードロックを掛けた添付文書に記載するなどの方法がある（パスワードは電子メール以外の方法で伝える必要がある。面談時に予めパスワードを決めておくといった方法が有効である）。そうすれば，仮に誤送信したとしても，肝心の部分を見られずに済む。また，メール本文は公衆回線を裸の状態で流れるので，傍受などのリスクにもさらされている。

また，Gmailには，わずかな時間であるが送信保留をしてくれる機能があり，送信直後に誤送信に気付いたときは，送信を取り消すことも可能である。

弁護士がSNSに投稿する場合も細心の注意が必要である。SNSは意見表明の場でもあり，弁護士のクチコミマーケティングの最良の媒体であるとも言えるので，SNSの使用自体が回避されるべきというわけではない。ただ，守秘義務違反につながったり，依頼者や事件の相手方に対する誹謗中傷につながるような投稿は避けるべきである。

また，SNSに写真を投稿する場合があるが，スマートフォンで撮影した写真にはジオタグという撮影場所情報が付加されている。ジオタグを除去しないで投稿することで，弁護士の所在情報が漏えいすることが

あり，それが守秘義務違反を構成することもあり得るので注意が必要である。スマートフォンの設定で，写真撮影時にジオタグを付けないように設定することができる。iPhoneでの設定は，下記のように行う。弁護士の場合，既定の設定ではジオタグを付けないように設定しておくべきではなかろうか。

なお，IBAは，IBA International Principles on Social Media Conduct for the Legal Professionを発表して，弁護士とSNSの関わり方について原則を提示している*17。

(6) 情報の廃棄の場面

いかなるリスクがあるか？

紙媒体についてシュレッダーや溶解処理を行わないと漏えいの危険が生ずることは，多くの人が既に知っている事実であろう。デジタルデータについても，単にパソコン上の「ゴミ箱」に入れるだけでは漏えいの危険がある。容易に復元ができるからである。

また，廃棄すべき印刷物を廃棄せずに裏紙として使用し，それを誤って第三者に交付することで情報が漏えいすることもあるので，注意が必要である。**表1**〔4頁〕の3番で挙げたような懲戒事例も生じている。

どのように対応するのか？

パソコンやハードディスクを廃棄する際には，データを単に削除するだけではなく，復元できないような処理をしてから廃棄する必要がある。データを完全に消去するためのソフトウェアが，フリーソフトウェアとして無償でたくさん提供されている。CDやDVDならば，ハサミなどで切断してから廃棄する必要がある。

また，裏紙は，例外的な場合を除いて，法律事務所においては使用しない方がよい。

6 さいごに

以上，情報セキュリティに関する事故事例，弁護士を取り巻く情報セキュリティに関する法規制やガイドライン，具体的なリスク対応方法について述べてきた。通常，このような記事を読むと，しばらくの間は情報セキュリティに関する関心が高まり，リスクにも適切な対処がなされる。しかし，時間が経つと徐々に関心が失われ，次第に情報セキュリティに関する脅威に鈍感になって行く。そして，忘れた頃に事故が起きる。

情報セキュリティを保つための最大にして唯一の方策は「気をつけること」である。しかし，情報セキュリティに対する関心を維持することは困難である。個人の努力だけで退屈な情報セキュリティ対策を講じつづけることは困難である。だからこそ弁護士会や法律事務所の代表者は，構成員の情報セキュリティへの関心を喚起・維持し，情報セキュリティレベルを保つための施策を講じる義務がある。情報セキュリティは人為的な努力によってしか維持されないのである。

＊17：http://www.ibanet.org/Document/Default.aspx?DocumentUid=27EBAC25-0D13-4318-A1C4-6B751ACA935F