特集《情報漏えい対策と防災対策から見た弁理士の危機管理》

特許事務所の情報漏洩対策

会員　新井　伸太郎

要　約

個人情報の保護に関する法律（個人情報保護法）が施行された平成17年以降，プライバシーポリシーを特許事務所のホームページに掲載するケースが増えているようです。個人情報保護法における「個人情報」とは，簡単に言えば，特定の個人を識別することができる情報のことですが，特許事務所が取り扱う情報には個人情報と同じく重要な情報があります。それは言うまでも無く発明に関する情報等ですが，こうした情報の特許事務所における取り扱いについて議論される機会はあまり多くなかったように思います。これは，弁理士に守秘義務が課されていることから当然という意識が特許事務所にあったからかもしれません。

本稿では，特許事務所が守るべき情報について簡単に見直すとともに，特許事務所における情報漏洩のパターンとその対策について検討します。

目次

1．はじめに
2．情報漏洩の対策
（1）　特許事務所が守るべき情報
（2）　情報漏洩のパターンとその対策
（3）　セキュリティ教育
3．おわりに

1．はじめに

情報化社会の進展に伴い，公的機関や民間企業の個人情報漏洩事件があとを絶ちません。個人情報の保護に関する法律（個人情報保護法）では，5000件以上の個人情報をデータベース等の形態で所持し，事業に用いている個人情報取扱事業者に対して一定の義務を課すとともに，違反があった場合の罰則を規定しています。個人情報取扱事業者に該当する特許事務所が何件くらい存在しているのか調査したことはありませんが，それほど多くないような気がします。

一方で，5000件以上の知的財産権に関する情報を保有している特許事務所はたくさん存在することでしょう。特許事務所にとって知的財産権に関する情報は，個人情報取扱事業者にとっての個人情報以上に重要な情報です。したがって，特許事務所で情報漏洩事件が発生しないように，特許事務所はセキュリティ対策を講じていく必要があります。

筆者は情報セキュリティの専門家ではありませんので情報セキュリティに関する高度な話はできませんが，特許事務所の情報セキュリティ対策を見直す際に，本稿で述べる事項について検討して頂ければ幸いです。

2．情報漏洩の対策

（1）　特許事務所が守るべき情報

特許事務所のセキュリティ担当者が情報漏洩の対策を練る上で初めに考えるべきことは，特許事務所が守るべき情報を見極めることではないでしょうか。

弁理士法の第30条には「弁理士又は弁理士であった者は，正当な理由がなく，その業務上取り扱ったことについて知り得た秘密を漏らし，又は盗用してはならない。」と規定されています。この条文から特許事務所は最低限，所員が業務上知り得た秘密が漏洩しないように対策すべきでしょう。また，秘密として知り得た情報以外の情報であっても，クライアントから得た情報がいかなる価値を持つかを判断することは困難な場合が多いので，クライアントから得た情報はなるべく漏洩しないように努めるべきです。

それでは特許事務所にとって漏洩が問題となる情報とは，具体的にどういった情報なのでしょうか。知財関係者がすぐに思いつくのは公開前の発明や考案の内容でしょう。これに加えて，商標登録を受けようとする商標，指定商品又は指定役務等の商標出願に関する

情報や，調査や鑑定の依頼内容に関する情報も，出願人の将来的な経営方針に関連する事項であるので守るべき情報に当たるのではないでしょうか。

（2） 情報漏洩のパターンとその対策

次に情報漏洩のパターンと対策について考えていきます。

（ⅰ） モバイル PC や USB メモリの置き忘れ

多忙な日々を過ごす弁理士は事務所外で仕事をこなす場面も多いと思います。そんな時，便利なのがモバイル PC や USB メモリ等の記録媒体です。移動中にモバイル PC を利用して仕事をしたり，USB メモリに明細書や発明資料のデータを入れて自宅で仕事をしたりする，といったこともあるかもしれません。このとき注意しなければならないのが，モバイル PC や USB メモリを電車や飲食店に置き忘れることです。情報漏洩の典型パターンとも言えますが，それでもなくならないのがこのパターンです。

（対策）

モバイル PC や USB メモリの置き忘れについては，データを事務所外に持ち出さないようにルール作りをするという対策が考えられますが，それができたら苦労しないというのが弁理士の本音かと思います。現実的には，データを事務所外に持ち出す場合には，モバイル PC にパスワードを設定したり，データを暗号化したりするという対策をとるべきではないでしょうか。

また最近では，事務所外で仕事をするために，データの保管にクラウドコンピューティングを利用している方もいらっしゃるかと思います。クラウドコンピューティングでは，自分の所有する PC や USB メモリ等にデータを保管しなくてすむといったメリットがあります。ただ，データの保管を外部業者に委託することになりますので，サービス提供者側の示す利用規約をよく読み，データが閲覧される可能性がある場合には，データを暗号化した上で保管することも考えておくべきではないかと思います。また，サービス提供者のサーバが攻撃されるリスクも考慮しておくべきでしょう。万一事故がおきた場合に，サービス利用者が直接的に事故の原因や被害状況を把握することは難しくサービス提供者の報告があるのを待つことしかできない可能性もあります。

クラウドコンピューティングの利用については，次の資料が参考になると思います。

情報処理推進機構（IPA）「クラウドサービス安全利用のすすめ」
［http://www.ipa.go.jp/security/cloud/cloud_tebiki_handbook_V1.pdf］

経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」
［http://www.meti.go.jp/press/2011/04/20110401001/20110401001-2.pdf］

（ⅱ） 電子メールや fax の誤送信

特許事務所からクライアントに明細書案や補正書案・意見書案等を送信する形式はいくつかあるかと思います。簡便な形式としては電子メールや fax で送信する形式があります。また，クライアントによっては独自に専用のデータ送受信システムを用意して特許事務所に導入させているケースもあるかと思います。後者の場合であれば，そのシステムの運用方法を間違えないということが前提ですが，そのシステムの欠陥等により情報漏洩が起きた場合，基本的には特許事務所が責任を負うことはないと思います。一方で，電子メールや fax で宛先を間違えたことにより情報漏洩が起きた場合には，特許事務所側が責任の一端を負う場合もあるかと思います。

（対策）

電子メールや fax の誤送信についてはなかなか有効な対策はありませんが，fax の誤送信については，クライアントの fax 番号を予め登録しておき，そこから送信先を選択して送信することで誤入力を防ぐことができます。一方，電子メールの誤送信は，アドレス帳から宛先を選択する際の選択ミスが原因となりやすく，これを防ぐことは難しいと思います。そこで，重要な事項は別途，電子ファイルに記述した上で暗号化して電子メールに添付するという方法も有効かと思います。いずれにしても，誤送信したことに気付いたら直ぐに送信先に連絡して，文書を廃棄してもらうようにすべきでしょう。

（ⅲ） 不正アクセス

現在では特許事務所の業務に関する書類のほとんどが電子データとして管理されています。これらの電子データは一般的に事務所内の LAN に接続されたファイルサーバやコンピュータに保存されており，それら

のマシーンが何者かによって不正アクセス(1)されることにより漏洩してしまうことがあります。一般論で言えばコンピュータ技術を熟知した者からの不正アクセスを完全に防ぐことは難しいでしょう。だからと言って，何の対策も講じなくてよいかというと，そんなことはありません。標的を定めていない不正アクセス者は，セキュリティの甘いシステムを狙います。必要最低限のセキュリティ対策をとっておくのと，そうでないのとでは雲泥の差です。

（対策）

不正アクセスに対する対策として最初に思いつくのがファイヤーウォールです。ファイヤーウォールは，事務所内のLANとインターネットの間に設けられ，予めネットワーク管理者が設定したルールに従って両者間の通信を制御することにより，外部からの不正アクセスを防ぐ役割を果たします。

しかし，ファイヤーウォールも万能ではありません。ファイヤーウォールは適切に運用することで高いセキュリティ効果を発揮しますが，ルールを適切に設定しなければならず，ルールの設定には一定の専門的知識が要求されます。また，設定したルールに適合するデータはファイヤーウォールを通過してしまいますので，そういったデータにコンピュータウイルスが紛れ込んでいる場合には侵入を防ぐことは難しくなってしまいます。別途，データを通過する際にコンピュータウイルスのチェックを行うなどの対策を検討する必要があります。

加えて，不正アクセスの兆候がないかを判断するために，日常的にファイヤーウォールのログを分析するのも効果的です。ファイヤーウォールのログについては，万一不正アクセスされてしまった場合の調査にも役立ちます。不正アクセスが行われたサーバのログは改ざんされている可能性があるのに対して，ファイヤーウォールのログは，ファイヤーウォールが不正アクセスされない限り，信用できる情報となります。したがって，ファイヤーウォールのログは適切にバックアップをとるなどして，消滅しないように注意すべきでしょう。

ファイヤーウォールの他に不正アクセス対策として用いられるのが，IDS（Intrusion Detection System）です。IDSは，予め登録されている不正なアクセスパターン，又は平常時のアクセスパターンと，実際にアクセスがあった際のアクセスパターンを比較することで，不正なアクセスの兆候があった場合に，ネットワーク管理者に通報するシステムです。IDSでは，通信の遮断までは行わないので，ネットワーク管理者は実際に不正なアクセスが行われたかを判断して対応することになります。また，昨今ではファイヤーウォールの機能とIDSの機能を合体させたような製品も出てきていますので，必要に応じて選択するのがよいでしょう。

（iv） コンピュータウイルス

情報を流出させるコンピュータウイルスとして有名なのが“Antinny”です。“Antinny”は，ファイル交換ソフト「Winny」を介して拡散したコンピュータウイルスであり，感染するとコンピュータ内のデータを「Winny」を利用している他のユーザに勝手に送信してしまいます。“Antinny”により，個人情報のみならず，企業等の機密情報が漏洩してしまう事件が多数発生しました。“Antinny”のようにコンピュータ内のデータを外部に送信してしまうコンピュータウイルスは「暴露ウイルス」と呼ばれています。「暴露ウイルス」は“Antinny”の他にも多数発見されていますので，暴露ウイルスに感染しないよう特許事務所としても何らかの対処を行う必要があると思います。

（対策）

コンピュータウイルス対策としては，アンチウイルスソフトを利用するのが一般的です。当然のことながらアンチウイルスソフトウイルスを導入した場合には，定義ファイルを頻繁に更新する必要があります。また，定期的にコンピュータ内にコンピュータウイルスが存在しないかスキャンするのが好ましいでしょう。いずれも事務所内でルールを決めておき，運用することが重要です。

一方で，所員は自分のコンピュータがコンピュータウイルスに感染したことを認識した場合には，直ちにそのコンピュータを所内LANから切り離し，ネットワーク管理者がいる場合には連絡すべきです。

また，事務所が所員に事務所のメールアドレスを付与しているケースが多いと思います。事務所のメールアドレスは，最終的には事務所内のコンピュータを宛先とするものです。したがって，事務所から割り当てられたメールアドレスをプライベートで利用したり，インターネット上に公開したりするのは極力さけるべきです。仮にスパムメールの宛先に登録されると，毎

日多数のスパムメールを受信しなければならず，コンピュータウイルスに感染するリスクが高まるばかりでなく，業務効率も低下してしまいます。

（v） 事務所への部外者の侵入

ここまでは，情報が電子データとして保存されているケースについて説明しましたが，情報が紙媒体などにより保存されていることもあるかと思います。この場合，特許事務所に何者かが侵入してきて情報を持ち出すといったことも考えられます。侵入は休日など所員がいないときに限らず，平日など所員がいるときにも所員になりすまして行われることもありますので注意が必要です。

（対策）

部外者の侵入に対する対策は，事務所の規模などによって異なってくると思います。大規模事務所であれば警備員を常駐させるといった対策も考えられます。中小規模事務所であれば，セキュリティ会社と契約して，事務所を無人にする際には機械警備を作動させておくなどの対策が考えられます。また，事務所のレイアウトを，出入口付近に所員が配置されるようにデザインすることにより部外者の侵入を防止する一定の効果があると思います。

（vi） 所員による情報漏洩

店員が来店した有名人の様子をインターネット上に公開するといった事件や，自分が行った違法行為についてインターネット上に公開するといった事件があとを絶ちません。また，2011 年には，国土交通省の航空管制官が米国大統領専用機「エアフォースワン」の飛行計画をインターネット上に流出させてしまった事件もありました。管制官は，飛行完了後であれば公開しても問題ないと判断して，機密情報である飛行計画を公開してしまったのです。人間は，自分だけが知っている情報を誰かに知らせたくなる生き物なのかもしれません。そう考えると，事務所の所員であっても悪気なく，情報をインターネット上で公開してしまうことがあるかもしれません。こういった事件は，たとえ本人に悪意がなくても特許事務所の信用問題になりますので注意が必要です。

一方で，事務所員が事務所から情報を不正に持ち出して売却してしまうといったケースについても考えておかなければなりません。自分の事務所の所員が情報を外部に漏洩するといったことを考えるのは嫌なことです。しかし，企業に産業スパイが入り込むといったことがある以上，企業の重要情報を持つ特許事務所に悪意を持った人物が入所する可能性はあるものと考えるべきではないでしょうか。また，所員が何者かに弱みを握られて仕方なくそういった行為を行ってしまう可能性もあるかもしれません。

（対策）

所員による情報漏洩の対策としては所員教育が効果的であると思います。どの情報を秘密として取り扱うべきかを認識させ，秘密情報の取り扱い方について周知徹底すべきでしょう。所員教育により，事務所員が悪意なく秘密情報をインターネット上で公開してしまうといった事態は防止できるのではないでしょうか。

一方で，悪意を持った所員による情報漏洩を防ぐのはとても困難です。全所員について事務所内のファイルサーバへのアクセス制限を設けるなどの対策が考えられますが，仕事効率を著しく低下させる可能性もありますので，情報漏洩のリスクと仕事効率のバランスを考えながら対策をとる必要があります。また，新たに事務所員を採用した場合には，一定期間，情報へのアクセス制限措置をとるといった対策も考えられます。また，事務所に対して何らかの不満を持っている所員が情報を漏洩させる場合もありますので，そういった不満をためさせないように配慮するといったことも大事かもしれません。

また，元所員による情報漏洩を防止するために，外部からファイルサーバへ可能なシステムを有している事務所であれば，アカウントの無効化を確実に行うことが重要です。

（3） セキュリティ教育

情報漏洩の対策は，特許事務所のパートナーやネットワーク管理者など一部の者だけで取り組んでも効果が低いものになってしまいます。いかに重要な情報を自分たちが扱っているかを全所員が共通して理解できるようにセキュリティ教育を行っていく必要があります。

セキュリティ教育は定期的に行うことが重要です。人の注意力というものは徐々に低下していくもので，これまで大丈夫だったから今後も大丈夫だろうといったような慣れが生じてしまいます。得てしてセキュリティ事故はそんなときに起こるものです。そういった

気の緩みは実際にセキュリティ事故が起きればなくなるものですが，だからといってセキュリティ事故を起こすわけにはいきません。そこで，企業等で実際に起きたセキュリティ事故を事案として取り上げて，事務所員に疑似体験させるセキュリティ教育も有効だと思います。

また，情報漏洩を防止するためのルールを事務所内で作成する場合には，現実に即したルールを作成すべきです。所員の行動を束縛しすぎるルール（守ることのできないルール）は，次第に無視されるようになり，ルールの存在自体が忘れ去られることにもなりかねません。したがって，ルールは試験運用をしながら評価と修正を繰り返し，作成していくのが好ましいと思います。

3．おわりに

本稿では，特許事務所における情報漏洩のパターンとその対策を主眼に述べました。ここで挙げた対策の中には，直ぐにでも実施できる対策から実施すること自体が困難な対策までありますが，一つでも実施していただければ，事務所のセキュリティ強度は向上すると思います。また，特許事務所でセキュリティ対策を実施する際には，その目的と各所員が具体的に何をすべきかをトップダウンで所員に告知することが重要です。

本稿を読んだ一人でも多くの方が，自分の事務所のセキュリティについて見つめ直して頂ければ幸いです。

（参考文献）

杉浦司，情報セキュリティマネジメント

相戸浩志，よくわかる最新情報セキュリティ技術の基本と仕組み－情報セキュリティエンジニアリングの基礎－

独立行政法人情報処理推進機構，情報セキュリティ白書 2012

（参考サイト）

独立行政法人情報処理推進機構

http://www.ipa.go.jp/security/sysad/index.html

（注記）

(1)不正アクセスに関する法律として不正アクセス禁止法があります。同法は平成 24 年 3 月に改正され，同年 5 月 1 日に改正法が施行されました。不正アクセス禁止法では，不正アクセス行為を，①アクセス制御機能（ログイン機能）を有する特定電子計算機に他人の ID ／パスワードを入力して不正にログインする行為（同法第 2 条第 4 項第 1 号），②セキュリティーホールを突いて，アクセス制御機能を有する特定電子計算機の制限されている機能を利用可能な状態とする行為（同法第 2 条第 4 項第 2 号），③セキュリティーホールを突いて，アクセス制御機能を有する特定電子計算機とは異なる他の特定電子計算機の制限されている機能を利用可能な状態とする行為（同法第 2 条第 4 項第 3 号））と規定し，不正アクセス行為を行った者に対して，罰則として三年以下の懲役又は百万円以下の罰金に処する旨，規定しています（同法 11 条）。

（原稿受領 2012. 9. 20）

パテント誌原稿募集

広報センター　副センター長
会誌編集部担当　須　藤　　浩

記

応募資格	知的財産の実務，研究に携わっている方（日本弁理士会会員に限りません） ※論文は未発表のものに限ります。
掲　　載	原則，先着順とさせていただきます。
テ ー マ	知的財産に関するもの
字　　数	5,000 字以上厳守～ 20,000 字以内（引用部分，図表を含む）パソコン入力のこと ※ 400 字程度の要約文章と目次の作成をお願いいたします。
応募予告	メール又は FAX にて応募予告をしてください。 ①論文の題名（仮題で可） ②発表者の氏名・所属及び住所・資格・連絡先（TEL･FAX･E-mail）を明記のこと
論文送付先	日本弁理士会　広報・支援・評価室「パテント」担当 TEL:03-3519-2361　　FAX:03-3519-2706 E-mail:patent-bosyuu@jpaa.or.jp 〒 100-0013　東京都千代田区霞が関 3-4-2
選考方法	会誌編集部にて審査いたします。 審査の結果，不掲載とさせていただくこともありますので，予めご承知ください。