はしがき

平成29年（2017年）５月30日に平成27年改正個人情報保護法が全面施行されてから３年が経過し、いわゆる３年ごとの見直しとして、個人情報の保護に関する法律等の一部を改正する法律が令和２年（2020年）６月５日に成立し、同年６月12日に公布された（同年法律第44号）。個人情報保護法が全面施行された平成17年（2005年）４月１日から平成27年改正法が施行され現在に至るまで15年超の期間で、個人情報を含む情報をめぐっての社会環境は激変し、さらに変化を続けている。

現在、事業活動、消費活動、SNSでの情報発信などにより毎分毎秒生み出される多種・大量のデータは、PC、スマートデバイス（電話、タブレット端末、音声認識スピーカー、生活家電等々）等の入力端末からインターネットを通じて収集され、気が遠くなるほど大量のデータに膨れ上がっている。このようなビッグデータは、機械学習、特にディープラーニングといったデータ分析手法の進展とも相まって、各企業にとって、成長力・競争力を維持・発展させるための貴重な資源ともいうべき価値を有するにまで至っていることに、もはや異論を差し挟む者はいないだろう。経済産業省による積極的な後押しなどもあり、デジタルトランスフォーメーション（DX）の重要性は多くの企業が認めるに至っており、近年デジタルへの置き換えが急速に進展することとなった。ビッグデータを適切に活用できなければ、民間企業の産業力ひいては日本の国力の低下につながるとの危機感は、かつてないほど強いものとなっている。この点、上記の令和２年改正法においても、「個人情報の適正かつ効果的な活用」が日本の経済社会等にとって有用かつ重要であるとの基本理念に変更はない。

他方で、個人情報の適正な取扱いに関し、個人情報取扱事業者の遵守すべき義務等を定めることによって「個人の権利利益を保護すること」が、個人情報保護法の中心的な目的であることは疑いようもない。この点、前述のとおりのビッグデータ社会の進展に伴って個人情報を利活用する場面が激増し

ており、その分、違法・不当な取扱いがなされる可能性も相対的に高くなっているといわざるを得ないところ、そのような現状においては、個人の権利利益をいかにして適切に保護していくのかが、個人情報取扱事業者にとって、より一層重要な課題となっていることは明らかである。令和２年改正法では、非個人情報として CookieSync が広く活用されている実態を踏まえ、Cookie およびそれに紐づく行動履歴などを含む概念である「個人関連情報」が新設され、提供元からみて個人情報にはあたらないものであっても、提供先が個人データとして取得することが想定されるときは第三者提供が制限されるなど、平成29年の前回の改正法施行後３年の間に生じた変化を取り込む形となっている。

法執行との側面からみても、ここのところ、個人情報保護委員会は、報告徴収、指導・助言、勧告といった監督活動を積極的に行っており、今後はその傾向がより強くなっていくものとみられ、個人情報の漏洩等、不適切な取扱事案が発生した場合の法的なリスクは一層現実的なものとなっている。そして、ひとたび指導や勧告などの措置を受ければ、それを契機とした報道などによってレピュテーションが低下し、予期せぬ対応費用の出捐を余儀なくされる事態となる。この点、令和２年改正法においては、漏洩等が発生し、個人の権利利益を害するおそれが大きい一定の場合に、個人情報保護委員会への報告が義務化され、法定刑の引上げや法人重科なども行われるなど、罰則も強化されている。

このように、個人情報の利活用はビジネスの遂行にあたって必要不可欠となっている一方で、個人情報を取り扱う企業にとってのリスクは近年ますます現実感を伴った大きなものとなっているといわざるを得ず、当該リスクをいかに低減させるかを検討・準備しておくことは必須である。

本書は、個人情報の違法・不当な取扱いの最たる場面である漏洩事案にフォーカスし、その対応方法について、できる限り実務的な観点から解説を加えることを企図した。本文において繰り返し述べているとおり、漏洩事案においては、初動対応の良し悪しがその後の結果を大きく左右することにな

る。そのため、本書をぜひ参考にしていただき、平時から可能な限り漏洩事故の発生を想定した十分な準備をしておきながら、有事においてはその平時の備えを生かして、迅速かつ適切に対応していただきたい。また、残念ながら平時の備えが十分ではなかった事業者においては、有事における事案の処理にあたり本書をぜひ役立てていただきたい。なお、漏洩事案は時間との闘いであり、対応にあたって迷うことがあれば、弁護士やフォレンジック事業者などの専門家チームの手を借りることを躊躇するべきではない。

本書をより実践的で実務的な内容とするため、デジタルフォレンジック調査業務の分野において数多くの実績があるデロイト トーマツ ファイナンシャルアドバイザリー合同会社のチームにも執筆・編集に参加してもらい、デジタルフォレンジックの概要から個人情報漏洩事案における活用方法に至るまで第6章においてわかりやすく解説していただいた。このことにより、本書のコンテンツが、より読者の皆様のお役に立つものとなったと確信している。

また、情報漏洩の対象となった場合には二次被害発生の可能性が最も高いものの一つであるクレジットカード情報について、漏洩事案発生時におけるクレジット会社との効果的な連携方法等について快くご教示いただいた、高三和之様および稲葉紀之様には、この場を借りて感謝申し上げたい。

そして、本書の企画が持ち上がってから出版に至るまで本当に長い年月を要してしまったが、辛抱強く、最後まであたたかく見守っていただいた株式会社民事法研究会の田中敦司編集部長には、心より感謝申し上げる次第である。

本書を手に取っていただいた読者の皆様にとって、本書が少しでもお役に立てるものとなることを願ってやまない。

令和2年7月吉日

執筆者代表　TMI総合法律事務所パートナー弁護士　白　石　和　泰

第４章

個人情報漏洩時の具体的アクション

1　総　論

本章では、個人情報の漏洩事件・事故が発生した際の対応について、漏洩原因として主に考えられる下記の四つの類型に分け、それぞれ具体的に論じる（もっとも、これら以外の可能性も排除せず、早期に弁護士およびデジタルフォレンジック会社（専門調査会社）のアドバイスも受けながら調査を進めるべきである。また、漏洩原因を特定しきれない場合もあるが、その場合は、できる限り絞り込んだ漏洩原因に応じた対応を重畳的に行うことが想定される）。

類型１　マルウェアに感染したことによる漏洩（２参照）

類型２　パソコン等の情報端末または個人情報が記録されている書類・外部記憶媒体等の盗難・紛失による漏洩（３参照）

類型３　従業員等内部の者による故意の持ち出し・犯罪行為による漏洩（４参照）

類型４　従業員等の誤操作による漏洩（５参照）

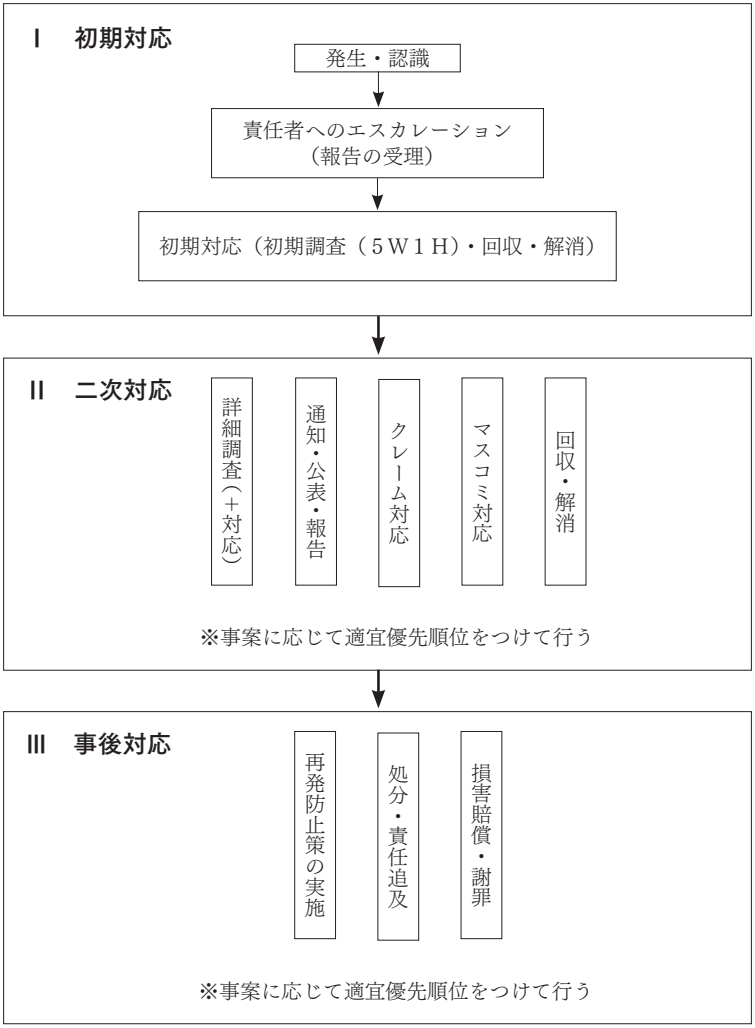
漏洩事件・事故への対応は、その端緒となる事象の認識が早ければ、それだけ、漏洩初期の段階での対応が可能となり、漏洩による被害をより少なくできる可能性がある。よって、いち早く漏洩の端緒となる事象の有無ないし可能性を認識することが重要である。

漏洩の端緒となる事象を情報セキュリティ担当者の報告等により認識したら[1]、いわゆる初期調査を行う必要がある。初期調査においては、被害の拡大防止のために、報告されてきた事実の裏づけを取り、その精度を上げるとともに、漏洩状況を正確に把握するための更なる情報収集を行う。

そのうえで、二次対応として、漏洩した情報の回収措置を講じるとともに、本人への通知（可否および要否の検討を含む）、個人情報保護委員会等・認定

1　漏洩の端緒となる事象に関する、いわゆる５Ｗ１Ｈ（いつ、どこで、誰が、何を、なぜ、どのようにして）の報告であるが、スピードを優先し、報告時点において即座に調査・確認が可能な範囲での報告となろう。

〔図表４－１〕　アクションプランの概要（フロー）



個人情報保護団体に対する報告、事実関係等の公表について各種ガイドラインに従い実施するとともに、顧客等からの問合せおよびクレームへの対応並びにマスコミ対応を行うこととなる。漏洩した情報が膨大であったり、悪用されやすいものであるような重大事案においては、必要に応じて外部調査

チーム等を設置し、漏洩事件・事故の原因等について、初期調査に加えてさらに詳細な調査を行う必要がある。

さらに、事後対応として、謝罪・被害弁償等の本人への対応を行うことになるが、その際、本人から提起される請求、訴訟等の手続への対応が必要となる場合もある。また、漏洩事件・事故の原因等に関する調査結果をとりまとめ、再発防止策を策定および実施する必要もある。この点、本人に対する二次被害を回避する必要性が高い場合や、世間の耳目を集めた事案などの場合においては、調査結果や再発防止策等を公表するべきである。また、個人情報取扱事業者が、漏洩事件・事故に関与した者を社内規則に基づいて処分したり、損害賠償請求を行う等して責任追及することも想定される。

これらを図示すると、前頁〔図表４－１〕のようになる。

以下、２ないし５において、上記各類型に即した対応を具体的に解説する。

２　マルウェアに感染したことによる漏洩

個人情報が記録されている機器等に対して、悪意のある動作を行うウイルスやスパイウェア（以下、総称して「マルウェア」という）が侵入し、当該マルウェア自体が外部へと情報を発信することや、マルウェアにより外部からのアクセスを許すバックドアがつくられること等により、コンピュータ内の個人情報が外部へ漏洩する類型である。

当該類型の具体例としては、たとえば次のような事案が考えられる。

○　会社の業務用電子メールアドレス宛てのメールに添付された「社内人事のお知らせ」と題されたPDF形式のアイコンのファイルを会社の業務用コンピュータ上で開封したところ、マルウェアが侵入し、当該コンピュータ内のプログラムが操作されて個人情報が抜き出され、外部のサーバへと個人情報が送信された（いわゆる標的型攻撃[2]メール）。

○　日頃から業務中にアクセスするWebサイトを訪れたところ、Webサ

イトが改ざんされており、アクセスをしたことで会社の業務用コンピュータ内に遠隔操作マルウェアがダウンロードされてしまい、情報システムを不正に遠隔操作され、個人情報が盗み出された（いわゆる水飲み場型攻撃[3]）。

○　暴露型マルウェアに感染したフラッシュメモリ等を会社の業務用コンピュータに挿入したことにより、当該業務用コンピュータが当該マルウェアに感染し、そこに保存されていた個人情報がインターネットの匿名掲示板やSNSに配信されてしまった。

(1)　Ⅰ初期対応

(A)　漏洩事件・事故の発生・認識

マルウェアに感染したことによる漏洩事件・事故の場合、次のような端緒により発覚することが多い。

・　自社またはセキュリティ管理委託会社が導入している、ネットワークへの不正侵入を検知するアラートシステムによる検知
・　ウイルス対策ソフトによる検知
・　情報管理システムにおけるスローレスポンス（反応が鈍くなること）による発見
・　ウイルスにより送信されたメール等を受信した第三者等からの通報
・　その他第三者からの連絡（たとえば、クレジットカード会社が、同時期に異常な頻度で一定の顧客集団のクレジットカード情報が利用されていることを探知し、調査要請の連絡を入れる場合等）

(B)　漏洩事件・事故の報告

会社として漏洩事件・事故についての必要な対応をとるためには、会社内

2　標的型攻撃とは、金銭や知的財産等の重要情報の不正な取得を目的として特定の標的に対して行われる手法のことをいう。
3　水飲み場型攻撃とは、特定の組織や個人を狙う標的型攻撃の手法の一つで、標的がよく利用すると思われるWebサイトを改ざんし、アクセスした利用者にウイルスなどのマルウェアを導入するよう仕込む手法のことをいう。

の一従業員が漏洩事件・事故を認識しただけでは足りず、その事件・事故の規模に応じて、会社代表者や情報セキュリティ担当役員等、当該対応についての指揮命令権限を有する者にまで必要な情報がいち早く正確に報告されなければならない。

したがって、上記(A)のような端緒を認識した者は、漏洩事件・事故発生に関する、いわゆる５Ｗ１Ｈ（① when（いつ）、② where（どこで）、③ who（誰が）、④ what（何を）、⑤ why（なぜ）、⑥ how（どのようにして）行われたのか）について、直ちにしかるべき部署に報告する必要がある。もっとも、早期の段階においては、まず現状の認識を社内で共有することを優先させ、５Ｗ１Ｈのうち、報告時点において即座に調査・確認が可能な範囲で報告をすればよい（マルウェアによる個人情報の漏洩は、物理的に認識できる盗難・紛失等とは異なり、端緒が発覚した時点では、漏洩状況の現状を分析することが困難である場合も多く、そもそも、個人情報漏洩の実害が発生しているのか、また、その場合に、どの程度の被害が発生しているのかということが容易に判明しない場合も多い）。ここでいう「しかるべき部署」は、会社により異なるが、たとえば、情報セキュリティ担当部署が考えられ、同部署は、会社代表者や情報セキュリティ担当役員等に情報共有を行う。これらの報告フローは、事前に会社として定めておくべきである。

(C)　事実調査

(a)　調査チームの組成・調査の開始

漏洩事件・事故の報告を受けた場合には、直ちに調査チームを組成し、調査を開始する。

調査チームは、調査の過程において、役員・従業員のアクセスログその他プライバシーにかかわる事項に関する調査や高度なセキュリティ情報へのアクセスを行うことが考えられる。そのため、調査チームは、社長直轄ないし情報セキュリティ担当役員を長として、秘密保持の観点から信頼性の高い従業員からなる編成とし、上記のような調査を迅速に行うのに必要十分な権限を付与する必要がある。具体的には、長である社長や情報セキュリティ担当

役員の下で実働する中心メンバー（チームリーダー１名のほかメンバー２～５名程度）を、迅速に選任する必要がある。この点、中心メンバーについては、平時に選任しておき、有事には招集さえすれば即座に組成できるようにしておくことが望ましい。一方、中心メンバー以外のメンバーについては、事案の性質や規模により、適宜必要に応じて選任する。

なお、短期間での実効的な事実調査を可能にするため、調査メンバーには、法務部門、広報部門、情報セキュリティ部門、技術部門（内部者が漏洩事件・事故に関与していることが疑われる場合には、これらの部門に加えて人事部門）の各部門に所属する従業員が含まれていることが望ましい。

ただ、マルウェアによる個人情報の漏洩が疑われる場合には、調査に際して専門的な知識が不可欠となるため、マルウェアに対応するための専門的な知識を有する従業員が関与することが望ましく、社内にそのような従業員がいない場合には、事実調査の初期段階から、外部の専門調査会社に調査協力を求める必要がある。

また、事前に作成されていればベストだが、未作成の場合には、調査チームの組成後直ちに、連絡がスムーズにとれるような措置をとる（メーリングリストの作成等）。

(b)　調査チームの役割

調査チームは、報告されてきた事実の裏づけをとり、漏洩事件・事故にかかるいわゆる５Ｗ１Ｈについて、必要十分で正確な事実を把握し（把握するよう努め）、調査結果をまとめる。調査チームが把握した事実が、今後の対応（二次対応および事後対応）を行ううえでの基礎情報となるため、当該調査においては、当初の報告を手掛かりとして、実際に何が起こったのか（起こっているのか）、５Ｗ１Ｈについての正確性を可能な限り上げることが重要となる。

他方で二次被害の防止および類似事案の発生回避のため、漏洩状態の解消、本人への通知、公表等を迅速に行う必要があることから、調査チームによる調査はスピーティーになされる必要がある。したがって、漫然と調査を

第6章

個人情報漏洩とデジタルフォレンジック

ついては、調査対象者単位で実施する場合と、対象者の枠を取り払って全データを一括対象としいて実施する場合がある。なお、メールレビューを含むドキュメントレビュー作業は、eDiscovery[9]対応等有事対応の手法として語られることが多いが、昨今では、平時運用におけるモニタリング機能として実施される事例も増加傾向にある。

(E)　Time Line 解析

Time Line 解析は、OS のもつシステムファイルやログの内容、時間情報を調査目的に応じて時系列で一覧化し、それを基に調査を行う手法を指す。一覧化する情報には、前述の Web 閲覧履歴解析や、USB 接続履歴解析などで抽出した情報も含まれる。Time Line 解析ではさまざまな解析結果を一覧にして俯瞰し調査する。そこから得られた結果をつなぎ合わせて情報漏洩の発生経緯や経過を時系列で追っていく手法であり、昨今では、携帯電話の SMS ／ MMS や SNS アプリの履歴および通話履歴、メール機能をはじめとしたコミュニケーションの履歴を Time Line 化する機能をもったツールも多く存在している。

コミュニケーションの履歴を Time Line 化したサンプルを〔図表６－９〕に記載する。

近年、情報漏洩の調査において携帯電話、スマートフォンおよびタブレット PC などの端末を調査対象とする事例が増加している。これらの端末は数年前と比べて機能、性能が飛躍的に PC に近づいていることから、調査対象者のコミュニケーション履歴を調査する際には、重要な意味をもっている。

9　Discovery（証拠開示）制度において、米国や欧州等では訴訟に関連する情報の開示が求められ、訴訟に関連すると認められた情報は原則としてすべて提出が義務づけられる。eDiscovery とは、この Discovery 制度において電子データに対して行われる証拠開示を指す。

〔図表６－９〕　スマートフォンの Communication Time Line 解析結果の例

Direction	Deleted	Type	Time stamp (Device time +09:00)	Device (Owner name)	Remote party	Coordinates	Text/Description	From	To	Group info	Address (OSM)
Incoming	No	**Line message**	2016/6/8 6:58	Apple iPhone 6 (Takashi Umeda)	機　智久 <eruger5u957796477854bghnmkt>	*N/A*	[GoGoGo!] KIKOLIさんからスターが届いたよ！いますぐPlay	機　智久 <eruger5u957796477854bghnmkt>	梅田 隆	*N/A*	*N/A*
Incoming	No	**Line message**	2016/6/8 16:20	Apple iPhone 6 (Takashi Umeda)	梅田 彩恵 <sdfhwsefkipe4934jkhlvkdjoi4rtjk>	*N/A*	[GoGoGo!] SAEさんからスターが届いたよ！いますぐPlay	梅田 彩恵 <sdfhwsefkipe4934jkhlvkdjoi4rtjk>	梅田 隆	*N/A*	*N/A*
Incoming	No	**Line message**	2016/6/8 18:06	Apple iPhone 6 (Takashi Umeda)	にゃん <nsytrlsnfk4898wqkvj854owfghrilsd>	*N/A*	画像を送信しました	にゃん <nsytrlsnfk4898wqkvj854owfghrilsd>	梅田 隆	*N/A*	*N/A*
Outgoing	No	**Line message**	2016/6/9 18:58	Apple iPhone 6 (Takashi Umeda)	ATSUSHI <udhewsfkjjkcfndkesjgf5468453mnodf>	*N/A*	画像を送信しました	梅田 隆	ATSUSHI <udhewsfkjjkcfndkesjgf5468453mnodf>	*N/A*	*N/A*
Outgoing	No	**Line message**	2016/6/9 18:58	Apple iPhone 6 (Takashi Umeda)	ATSUSHI <udhewsfkjjkcfndkesjgf5468453mnodf>	*N/A*	画像を送信しました	梅田 隆	ATSUSHI <udhewsfkjjkcfndkesjgf5468453mnodf>	*N/A*	*N/A*
Outgoing	No	**Line message**	2016/6/9 18:59	Apple iPhone 6 (Takashi Umeda)	ATSUSHI <udhewsfkjjkcfndkesjgf5468453mnodf>	*N/A*	写真が精いっぱいでした。USBじゃ抜けないので。。。これでいいですか？	梅田 隆	ATSUSHI <udhewsfkjjkcfndkesjgf5468453mnodf>	*N/A*	*N/A*
Incoming	No	**Line message**	2016/6/9 19:01	Apple iPhone 6 (Takashi Umeda)	ATSUSHI <udhewsfkjjkcfndkesjgf5468453mnodf>	*N/A*	ばっちりです。	ATSUSHI <udhewsfkjjkcfndkesjgf5468453mnodf>	梅田 隆	*N/A*	*N/A*
Outgoing	No	**Line message**	2016/6/9 19:06	Apple iPhone 6 (Takashi Umeda)	ATSUSHI <udhewsfkjjkcfndkesjgf5468453mnodf>	*N/A*	ちゃんと数字は伏せてくださいね。	梅田 隆	ATSUSHI <udhewsfkjjkcfndkesjgf5468453mnodf>	*N/A*	*N/A*
Incoming	No				HI sfkjjkcfndkesj53mnodf>	*N/A*	Yes！	ATSUSHI <udhewsfkjjkcfndkesjgf5468453mnodf>	梅田 隆	*N/A*	*N/A*
Outgoing	No				HI sfkjjkcfndkesj53mnodf>	*N/A*	結いなぁww	梅田 隆	ATSUSHI <udhewsfkjjkcfndkesjgf5468453mnodf>	*N/A*	*N/A*

日常会話の中に、情報漏洩を示唆する履歴が確認される場合も多い。

（出所）　デロイト トーマツ ファイナンシャルアドバイザリー合同会社が作成。

3　個人情報漏洩の抑止とデジタルフォレンジック

昨今では、デジタルフォレンジックの技術を情報漏洩抑止の平時運用として活用する事業者も増加している。本項では、BYOD を採用している企業において、中途入社者を雇い入れる際に行っている施策とその実務を意思決定のポイントも踏まえて記載する。

Case１：個人情報の流出のみではなく、“流入”によるリスクを考慮した事例

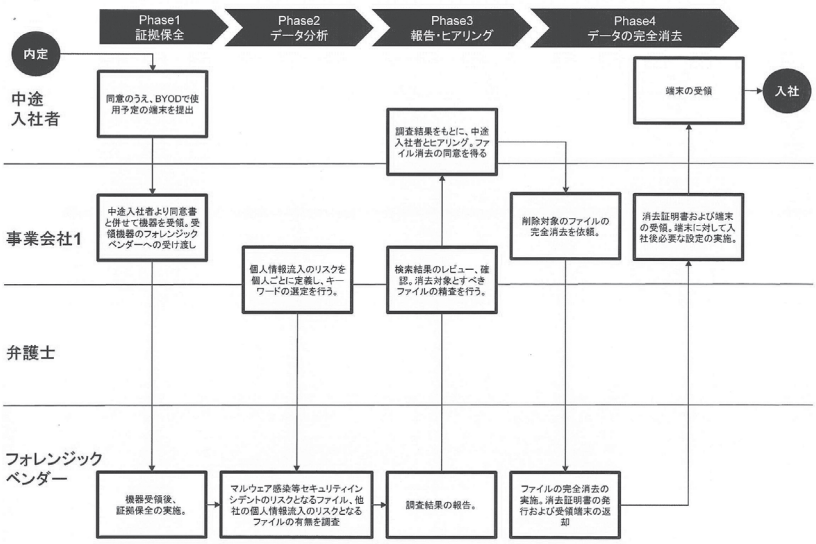
事業会社１はWeb開発事業を手掛ける中堅の事業者である。創立メンバー

の少数精鋭で運営している。業績は好調だが業務負荷が高い状況にあり、現在の従業員だけではこれ以上の事業拡大は難しいという課題を抱えていた。加えて、現在軌道に乗っている事業を継続しつつも、新たなサービスの開発を推し進め、企業を大きく発展させることが事業計画に上がっており、事業会社１は中途採用者を積極的に採用し、人材を確保することとした。

事業会社１は、従業員の利便性を向上させるためにBYODを採用しており、仕事への取組み方は個人の裁量に任せられる部分が多く、従業員は意欲的に業務に取り組んでいた。しかし、気心が知れている仲間で組織された職場環境であるため、情報漏洩などを見据えたセキュリティ対策にはこれまで一般的な対応を除いて行っておらず、これから中途採用を積極的に行うためには、セキュリティ対策の運用と体制を整える必要があった。

事業会社１は、BYODを採用した段階で、セキュアなネットワーク環境やアクセス管理といった対策、従業員がスマートフォン、タブレットPCを

〔図表６－10〕　中途採用者受け入れ時の対応フロー



（出所）　デロイト トーマツ ファイナンシャルアドバイザリー合同会社が作成。

業務使用する場合を見据えたMDM、MCM管理は行っている。しかし、社内から外部に情報が漏洩することを想定された対策はあるものの、外部から情報が持ち込まれ、自社が情報の漏洩先になってしまうリスクは想定されていないことが課題としてあげられた。今後、中途採用者が事業会社1に加わる際に憂慮されることは、中途採用者によって意図しない形で情報が“流入”することにより、自社が情報の漏洩先になってしまうという事態であった。事業会社1は、弁護士、フォレンジックベンダーに相談のうえ、対応策について検討を行った。その結果、中途採用者受入れ時の体制について〔図表6－10〕に示すフローによって整理を行った。

Phase 1 ：証拠保全

事業会社1が整理したフローにおいて、まず行うことは対象者に合意をとり、BYODで使用する予定の電子機器を受領することである。今回対象となったのは、管理職として内定している人物であった。対象者には可能な限り自身でデータのスクリーニングを実施してもらったうえで、事業会社1の担当者立ち合いのもとフォレンジックベンダーに機器を受け渡してもらった。この際、もし機密情報と定義する条件に合致するデータが確認された場合は、データの完全消去を行う旨の同意書と、CoCの取り交わしを行った。

フォレンジックベンダーは、機器受領後に直ちに機器の状態を写真に収め、証拠保全に取り掛かった。今回のデジタルフォレンジック調査の目的は、意図せぬ機密情報の流入によるレピュテーション低下のリスクの低減および、マルウェア等のセキュリティインシデントを発生させる要因をなくすことであったため、起動しているPCのメモリダンプ[10]、内蔵HDDの物理イメージを取得することとした。なお、この作業を行う際はより揮発性の高いデータから取得する必要があるため、メモリダンプ、HDDの物理イメージの順でデータを取得した。取得したデータはハッシュ値の比較による調査、不良セクター等によるエラーの有無を確認し解析対象とされた。

10　ある時点において、メインメモリの内容の一部または全部をHDD等の記録装置に記録すること、または記録したデータ。

★実務ポイント

✓証拠保全を行う際は、CoC や写真を用いて機器およびデータの受け渡し、作業内容の履歴を残すことが重要である。本件調査は受け入れ時対応のため、直ちにインシデントに直結する可能性は低い。しかし、後日インシデントが発生した際に事前対応として行った作業の内容が適切なものであったことを裏づけるためにも、調査対象機器が誰から誰にいつ手渡され、どのような機器であったかを克明に残しておくことが肝要である。

✓マルウェアの調査では、PC のメモリに残された記録からマルウェアの挙動が確認できる場合がある。証拠保全は対象機器のデータに一切の改変を加えずにデータの取得を行うことが前提であるが、調査目的に鑑み、適切な手法を選定することが求められる。

Phase 2 ：データ分析

証拠保全によって取得したデータは、以下の二つの観点から解析が行われた。

①　他社からの情報流入の有無

②　マルウェア等、セキュリティ上のリスクとなり得るファイル、プログラムの有無

本項では、上記①、②についてとられた手続について記載する。

Phase 2 － 1 ：他社からの情報流入の有無

本調査では、ユーザーが削除したデータの復元を行い、復元されたデータに対してキーワード検索がなされた。検索にヒットしたファイルは、あらかじめ事業会社１と弁護士において検討したレビュープロトコル[11]に従いレビューが行われた。ここでは、弁護士によって法的観点から情報流入のリス

11　ドキュメントやメールのレビューを行う際の方針について記載された指示書。レビューを行う際の観点や、事前のインプット情報が記載されていることが一般的。

クとなる可能性のある個人情報、営業秘密などに該当すると思われるファイルの有無が調査された。その結果、一部の現存するファイルおよび削除ファイルから一部個人情報とみられるデータが確認され、それらは派遣会社の社員リストや、他社の組織図などであった。これらのデータは本人への確認のうえ完全消去がなされる予定である。なお、パスワード付きの圧縮ファイル、画像ファイル等は、対象者とヒアリングのうえ、明確に私用のものと特定できるファイルを除き、本人同意のもと完全削除が行われる予定である。

★実務ポイント

✓情報流入への対策としてリスクとなりうるドキュメントを抽出する際は、今回のようにドキュメントレビューを行う場合と、キーワード検索にヒットした段階ですべてのデータを削除する場合がある。

Phase 2－2：マルウェア等、セキュリティ上のリスクとなり得るファイル、プログラムの有無

本調査では、証拠保全で取得したHDDの物理イメージ、メモリダンプを解析する。

メモリダンプの解析は、プロセスアドレス空間[12]に含まれるコード[13]の分析により、悪性のコードであるか否かの判定等を行う。悪性のコードと推察される痕跡が認められた場合は、取得したHDDの物理イメージ内に感染ファイルがあるかを調査し、当該ファイルの駆除を行う。

なお、取得したHDDの物理イメージは、あくまでOSが起動していない静的な状態であるため、マルウェアの挙動を実際に確認する場合は、取得した物理イメージを仮想的に立ち上げ、実際にネットワーク接続を行い、通信

12　アドレス空間とは、メインメモリの物理的な位置、領域を意味する。ここでいうプロセスアドレス空間は、メモリに対してアプリケーションが情報を書き込むことが可能な領域を指す。

13　プログラミング言語の仕様に準じて書かれたコンピューターに対しての指示、命令を指す。

◆ 執筆者一覧 ◆

［執筆者（TMI 総合法律事務所）］

白石　和泰（しらいし・かずやす）

1996年　早稲田大学政治経済学部政治学科卒業

2003年　司法修習終了（第56期）、弁護士登録（第二東京弁護士会）、TMI 総合法律事務所勤務

2013年　ワシントン大学ロースクール卒業（LL.M.、Intellectual Property Law and Policy コース）、Dorsey & Whitney LLP 勤務（シアトル）、Bracewell & Giuliani LLP 勤務（シアトル）

2014年　TMI 総合法律事務所復帰、外務省経済局政策課専門員（2015年３月末まで）

2016年　パートナー就任

〔専門分野〕 IT・情報・通信関連法、消費者関連法、一般企業法務、紛争（訴訟）、リスクマネジメント、M&A、労働法務等

〔論文・著書〕『IT・インターネットの法律相談〔改訂版〕』（共著、青林書院、2020年）、「Japan chapter of Getting The Deal Through」Cybersecurity 2020 年１月号（共著、2020年）、『起業の法務――新規ビジネス設計のケースメソッド』（共著、商事法務、2019年）、『AI・ロボットの法律実務 Q&A』（共著、勁草書房、2019年）、「国内企業における GDPR 対応の実務」自由と正義70巻６号（共著、日本弁護士連合会、2019年）、『個人情報管理ハンドブック〔第４版〕』（共著、商事法務、2018年）、「座談会　自動運転社会の法制度設計」ビジネス法務17巻11号12号（共著、2017年）、『セミナー形式 改正個人情報保護法のポイントと対応』（共著、新日本法規出版、2017年）、「匿名加工情報とは？作成時の基準・義務・事例をまとめて解説」The Finance（共著、2017年）、「特集　人工知能の未来と企業法務」会社法務Ａ２Z119号（共著、2017年）、『完全対応　新個人情報保護法－Ｑ＆Ａと書式例－』（共著、新日本法規出版、2017年）、「遺伝子ビジネスと法規制」ビジネス法務15巻11号（共著、2015年）、「『健康食品』の機能性表示」ビジネス法務15巻10号（共著、2015年）、『Q&A 改正個人情報保護法――パーソナルデータ保護法制の最前線』（共著、新日本法規出版、2015年）、「法務部門の積極的な関与が求められるサイバーセキュリティ」ビジネス法務15巻８号（共著、2015年）など

村上　諭志（むらかみ・さとし）

2004年　東京大学法学部第一類卒業
2006年　中央大学法科大学院修了
2007年　司法修習終了（第60期）、弁護士登録（東京弁護士会）
2008年　TMI 総合法律事務所勤務
2013年　ワシントン大学ロースクール卒業（LL.M.、Intellectual Property Law and Policy コース）、モルガン・ルイス＆バッキアス法律事務所勤務（サンフランシスコ）
2014年　ニューヨーク州弁護士資格取得、TMI 総合法律事務所復帰
2018年　Certified Information Privacy Professional / Europe 取得
2019年　パートナー就任

〔専門分野〕 一般企業法務、個人情報、IT・通信、商標、著作権、メディア、エンタテインメント、消費者関連法、不正競争、景品表示法、国際法務、ベンチャー支援

〔論文・著書〕 『IT・インターネットの法律相談〔改訂版〕』（共著、青林書院、2020年）、『起業の法務――新規ビジネス設計のケースメソッド』（共著、商事法務、2019年）、「M&A の専門家とデータの専門家が支援するデータ利活用時代の M&A」Lawyers Guide M&A 2019年 9 月号（共著、レクシスネクシス・ジャパン、2019年）、「ビッグデータの利活用におけるパーソナルデータ取扱い上の法的留意点」知財管理68巻 6 号（共著、2018年）、『個人情報管理ハンドブック〔第 4 版〕』（共著、商事法務、2018年）、『セミナー形式 改正個人情報保護法のポイントと対応』（共著、新日本法規出版、2017年）、「個人情報保護法改正の保険業界への影響」保険毎日新聞（共著、2017年）、「匿名加工情報とは？作成時の基準・義務・事例をまとめて解説」The Finance（共著、2017年）、「遺伝子ビジネスと法規制」ビジネス法務15巻11号（共著、2015年）、「ビッグデータの利活用」ビジネス法務15巻 5 号（共著、2015年）、「最近の連邦商標希釈化改正法に関する重要判決・審決」知財管理65巻 3 号（共著、2015年）、『ソフトウェア取引の法律相談』（共著、青林書院、2013年）など

小林　央典（こばやし・ひろのり）

2006年　東京大学法学部第一類卒業
2008年　中央大学法科大学院修了

2009年　司法修習終了（第62期）、弁護士登録（第二東京弁護士会）、TMI 総合法律事務所勤務

〔専門分野〕 商事関連訴訟、知財訴訟・審判、一般企業法務、消費者関連法、商標、IT・通信

〔論文・著書〕 『IT・インターネットの法律相談〔改訂版〕』（共著、青林書院、2020年）、『AI・ロボットの法律実務 Q&A』（共著、勁草書房、2019年）、『個人情報管理ハンドブック〔第 4 版〕』（共著、商事法務、2018年）、『完全対応 新個人情報保護法－Q＆Aと書式例－』（共著、新日本法規出版、2017年）、『企業のためのサイバーセキュリティの法律実務』（共著、商事法務、2016年）、『Q&A 営業秘密をめぐる実務論点』（共著、中央経済社、2016年）、『知的財産判例総覧2014Ⅱ』（共著、青林書院、2016年）、『Q&A 改正個人情報保護法――パーソナルデータ保護法制の最前線』（共著、新日本法規出版、2015年）、「介護ロボットと法規制」ビジネス法務15巻 8 号（共著、2015年）、「クラウドサービスの利用における法的論点の考察――クラウドセキュリティガイドライン活用ガイドブックのリリースに際して」NBL1013号（共著、2013年）

尼口　寛美（あまぐち・ひろみ）

2005年　慶應義塾大学法学部政治学科卒業

2008年　慶應義塾大学法科大学院修了

2009年　司法修習終了（第62期）、弁護士登録（第一東京弁護士会）

2010年　TMI 総合法律事務所勤務

〔専門分野〕 一般企業法務、商標、IT・通信、知財訴訟・審判、景品表示法、ブランド

〔論文・著書〕 『個人情報管理ハンドブック〔第 4 版〕』（共著、商事法務、2018年）、『Q&A 営業秘密をめぐる実務論点』（共著、中央経済社、2016年）、『知的財産判例総覧2014Ⅱ』（共著、青林書院、2016年）、『会社法務入門〔第 4 版〕』（共著、日本経済新聞出版社、2011年）

野呂　悠登（のろ・ゆうと）

2011年　東北大学法学部卒業

2013年　東京大学法科大学院修了

2014年　司法修習終了（第67期）、弁護士登録（第一東京弁護士会）

2015年　TMI 総合法律事務所勤務、東京大学法科大学院未修者指導講師
2017年　個人情報保護委員会事務局参事官補佐
2018年　TMI 総合法律事務所復帰
〔専門分野〕 個人情報、IT・通信、知財訴訟・審判、消費者関連法
〔論文・著書〕「ネット広告におけるユーザーデータの取扱いの法的留意点」BUSINESS LAW JOURNAL12巻10号、『起業の法務――新規ビジネス設計のケースメソッド』（共著、商事法務、2019年）、「データが蓄積された企業・事業を取得する『データ M&A』の法的留意点」旬刊経理情報1553号（2019年）、「〈連載〉職場の AI と法律問題」労務事情1376号・1379号・1387号（共著、2019年）、「外国法に対応したプライバシーポリシーの作成・見直し」ビジネス法務2018年12月号、「日本法に対応したプライバシーポリシーの作成・見直し」ビジネス法務2018年12月号、「十分性認定と GDPR における個人データの第三国移転」自由と正義70巻 6 号（日本弁護士連合会、2019年）、「GDPR（EU 一般データ保護規則）対応の最終チェックポイント」ビジネス法務18巻 7 号（2018年）、「AI による個人情報の取扱いの留意点」BUSINESS LAW JOURNAL11巻 6 号（2018年）、『個人情報管理ハンドブック〔第 4 版〕』（共著、商事法務、2018年）、『セミナー形式 改正個人情報保護法のポイントと対応』（共著、新日本法規出版、2017年）、『知的財産判例総覧2014 I II』（共著、青林書院、2016年）

岡辺　公志（おかべ・こうし）

2013年　東京大学法学部第一類卒業
2014年　東京大学法科大学院中退
2015年　司法修習終了（第68期）、弁護士登録（東京弁護士会）
2016年　TMI 総合法律事務所勤務
〔専門分野〕 IT・通信、著作権、メディア、エンタテインメント、不正競争
〔論文・著書〕『個人情報管理ハンドブック〔第 4 版〕』（共著、商事法務、2018年）、「実務解説／ ESG リスク回避のための実践的 CSR 条項」BUSINESS LAW JOURNAL10巻 3 号（共著、2017年）

川上　貴寛（かわかみ・たかひろ）

2013年　東京学芸大学教育学部中等教育教員養成課程英語専攻卒業

2015年　東京大学教養学部中退
2016年　司法修習終了（第69期）、弁護士登録（東京弁護士会）
2017年　TMI 総合法律事務所勤務
〔論文・著書〕『IT・インターネットの法律相談〔改訂版〕』（共著、青林書院、2020年）、「国内企業における GDPR 対応の実務」自由と正義70巻 6 号（共著、日本弁護士連合会、2019年）、【法令ガイダンス】民法改正」LexisNexis AS ONE（共著、2018年）

溝端　俊介（みぞばた・しゅんすけ）

2016年　東京大学法学部第一類卒業
2018年　東京大学法科大学院修了
2019年　司法修習終了（第72期）、弁護士登録（第一東京弁護士会）
2020年　TMI 総合法律事務所勤務
〔論文・著書〕「不法行為法におけるプライバシー」東京大学法科大学院ローレビュー第14巻（2019年）

［執筆者（デロイト トーマツ ファイナンシャルアドバイザリー合同会社）］

デロイトトーマツファイナンシャルアドバイザリー　フォレンジックテクノロジー

【TMI 総合法律事務所】
〒106－6123　東京都港区六本木 6 －10－ 1
六本木ヒルズ森タワー23階
03－6438－5511（代）
http://www.tmi.gr.jp/

【デロイト トーマツ ファイナンシャルアドバイザリー合同会社】
〒100－8363　東京都千代田区丸の内 3 － 2 － 3
丸の内二重橋ビルディング
03－6213－1180（代）
https://www2.deloitte.com/jp/ja.html

個人情報漏洩対策の法律と実務

2020年９月20日　第１刷発行

定価　本体3,700円＋税

編　者　TMI 総合法律事務所
　　デロイト トーマツ ファイナンシャルアドバイザリー合同会社
発　行　株式会社　民事法研究会
印　刷　藤原印刷株式会社

発行所　株式会社　民事法研究会
〒150－0013　東京都渋谷区恵比寿３－７－16
〔営業〕　☎03－5798－7257　FAX 03－5798－7258
〔編集〕　☎03－5798－7277　FAX 03－5798－7278
http://www.minjiho.com/　　info@minjiho.com

カバーデザイン／袴田峯男　　ISBN978-4-86556-287-3 C2032 ¥3700E
本文組版／民事法研究会（Windows10 Pro 64bit+InDesign2020+Fontworks etc.）
落丁・乱丁はおとりかえします。