ISSN 0386-7889

No.219 2018.7 / July

日本データ通信

INFORMATION FROM JADAC AND EXPERTS

» 特集

“JIS Q 15001改正”
個人情報保護と Pマーク審査実務への影響

» Seminars

欧州一般データ保護規則（GDPR）の最新動向

ひかり総合法律事務所　弁護士
理化学研究所革新知能統合研究センター　客員主管研究員　板倉陽一郎

サイバー空間における警察活動

警察庁 生活安全局 情報技術犯罪対策課　官民連携推進官　高尾 健一

今月の登場企業・組織

一般財団法人日本情報経済社会推進協会（JIPDEC）、警察庁、日本レコードセンター株式会社、株式会社リグシー、金沢市立工業高校（順不同）

JADAC

日本データ通信
INFORMATION FROM JADAC AND EXPERTS
No. 219
2018年7月号

CONTENTS

01 巻頭言

ICTの進歩と社会

一般財団法人日本データ通信協会　理事長　酒井 善則

「ICT分野の技術進歩は非常に速いため、社会構造自体が近年大きく変わろうとしている」、という主旨の文章を数多く見る機会が多い。確かにコンピュータの処理能力、メモリ容量、通信速度など基本的処理能力（以後処理能力とよぶ）の進歩は非常に早く、ここ10年で大雑把に見てコンピュータ処理能力は10倍以上、メモリ容量100倍以上、通信速度50倍以上となっている。各種能力が10倍になると社会にも大きな影響を与えるのは当然であろう。車、鉄道、飛行機の速度が10倍以上になったら、社会構造は大きく変わると想像される。東京一極集中は更に進むかもしれないし、想像できない社会が実現する可能性がある。耕作地単位面積当たりの食料生産量が10倍以上になっても、農業は大きく変わり、日本の風景も変わるかもしれない。

回線交換中心の電話網からIPによるデータ、映像中心のネットワークへの進歩、AIの進歩、ビックデータによる新しい知識習得等ICT分野の技術進歩が非常に目立っているが、これらの進歩もやはり各種処理能力の進歩に起因する部分も大きい。IPの基礎となるパケット網、映像を含む各種信号処理、AIの基礎である神経回路モデル、データサイエンスの技術的基礎である統計理論は、皆30年以上前に基礎ができている。もちろん最近30年のこれら分野の進歩も大きいが、計算能力、メモリ容量などの進歩を活用する観点で理論も発展して、かつ成果が実用になったことも否定できない。通信事業においても処理能力が進歩したため、電話から映像へ、回線交換からパケット交換へと大きく変わっていったと考えられる。

現在わが国ではAIを中心としたソフトウェア人材、大量データ解析人材の不足が問題視されている。AI等のソフトウェア分野の卒業生は多くの分野の企業で引っ張りだこであるとのことであり、起業して成功する若い人の話も耳にする。一方、私の身近な電気通信事業では、通信そのものは儲からなく、携帯では通信そのものはダムパイプということで新しい付加価値を模索する動きが大きい。これからは教育においても技術だけでなくビジネスが大事であるとの意見も多い。私の専門とする工学は元々物理、化学、数学などの自然科学を応用して社会に役立つ製品設計を行う学問分野である。近年のICT分野の発展も、処理能力の飛躍的進歩を活用したシステム設計の結果であり、システム設計の評価関数に社会あるいはビジネスが入ったとしても応用対象が社会科学まで広がるだけで考え方は変わらない。

日本データ通信協会は人材育成、セキュリティ分野を中心に社会に貢献することを任務としているが、その中で色々な分野での目安を作ることも重要な活動であると思われる。資格等により人材育成の目安作成に貢献して、個人情報保護の指針、タイムビジネス、迷惑メール対策等の活動を通じて、セキュリティ分野からみた製品設計の評価関数の作成にも貢献することが重要と考えている。

特集

“JIS Q 15001改正”

個人情報保護と Pマーク審査実務への影響

改正個人情報保護法が、昨年5月30日に全面施行された。これを受けて民間企業が個人情報保護の仕組みを作り運用するためのよりどころとなっていた「個人情報保護マネジメントシステム」（JIS Q 15001）」が12月20日に改正され、事業者は新しい規格に即した対応を求められることとなった。とくに、この規格に基づいて運用されているプライバシーマークの取得事業者にとって、改正されたJIS Q 15001への対応は火急の課題である。

新しいJISは旧規格と何が異なっており、新規格の下で企業は何をしなければならないのだろうか。本特集では、この改正の背景と目的、実務への影響を3人の有識者に語ってもらった。

最初に経済産業省で個人情報保護政策を担当し、現在は（一財）日本情報経済社会推進協会（JIPDEC）で認定個人情報保護団体事務局長を務める篠原治美氏にJIS Q 15001改正の経緯とその意味を解説していただいた。それを受けて（一財）日本データ通信協会Pマーク審査部主幹研究員の清水政幸が新JIS規格が求める事業者の対応を説明し、最後に日本データ通信協会Pマーク審査部長の小堤康史がプライバシーマーク審査基準への影響を明らかにする。

これまでJIS規格に基づいて個人情報保護施策を行ってきた事業者の皆様にとっても、これから本格的に個人情報保護に取り組もうとする事業者の皆様にとっても、有益な情報が満載である。

JIS Q 15001 改正に至る経緯

一般財団法人日本情報経済社会推進協会（JIPDEC）
認定個人情報保護団体事務局　事務局長
篠原 治美※

「個人情報保護マネジメントシステム－要求事項」（JISQ15001：2017）」は、工業標準化法に基づき、日本工業標準調査会の審議を経て、2017 年 12 月 20 日に改正された。今回の改正は、約 10 年ぶりに個人情報保護法が改正されたことによるもので、改正法に合わせた内容の改正もさることながら、構造的にも大きく変わっている。ただし、個人情報保護の本質は変わらないことから、事業者の対応も大きく変っているわけではない。

1．1999年版JIS制定の経緯

プライバシー・個人情報の取り組みを制度としてどのように保護するかについて日本で議論するきっかけとなったのは、1980年（昭和55年）のOECDの「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」であった。（OECD8原則）

これを受けてわが国では、1988年（昭和63年）に行政機関個人情報保護法が制定され、公的分野の規律が先行されることとなったが、民間分野を対象とする法制化は将来的検討課題となった。

経済産業省（当時通商産業省）から、1989年（平成元年）に民間部門での自主的な取り組みとして、「民間部門における電子計算機処理に係る個人情報の保護について」が公表された。

さらに、1995年（平成7年）EU個人データ保護指令を受けて、より一層の個人情報保護策を求められEU指令に沿った個人情報の推進を図る必要性から1997年（平成9年）「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」が改訂、告示された。

また、1998年には、ガイドラインを基準とした第三者評価認証制度であるプライバシーマーク制度が創設され、それを活用することで個人情報保護の一層の取り組みの促進が図られた。

ただし、このような取り組みが、経済産業省ガイドラインを基準としていたため、経済産業省の管轄する関係業界に限られる恐れを懸念し、業種横断的な取り組みが必要と考え、ガイドラインをJIS化しようということになった。

そのような背景の元、JIS Q 15001は1999年（平成11年）にコンプライアンス・プログラムとして制定された。当初は、民間部門における個人情報の取扱いを規律する法令が存在せず、民間部門の自主的な取り組みに委ねられていた。

コンプライアンス・プログラム版のJIS Q 15001：1999の要求事項の基礎となった基準は、EUの個人データ保護指令である。したがって、JIS規格はEUの個人データ保護指令にならってわが国における個人情報保護へのコンプライアンス、つまり法令遵守に必要な取り組みを定めたものである。

2．2006年版JIS改正の経緯

2003年に個人情報保護法が制定され、法定の義務として個人情報取扱事業者の義務が法律で明記され、従来からの自主的な取り組みとしてのコンプライアンスから、文字通りの法律に基づく法令遵守としてのコンプライアンスへと移行した。

※著者の篠原治美氏は、前職である経済産業省商務情報政策局情報経済課において、法執行専門職員として数々の情報政策に携わり、JISQ15001改正に際しても中心的な役割を果した。

これに伴い、2006年の本規格の改正は、マネジメントシステム規格に準拠する規格として、法令遵守を達成する上で必要な取り組みを組織的、体系的に定める上で必要な指針としてのマネジメントシステムに移行するための改正となった。

当初、法律が制定されていなかった段階においては、コンプライアンスを目的とした「コンプライアンス・プログラム」であった本規格は、その後、個人情報保護法制定後に法令遵守を達成するための「マネジメント・プログラム」へと大きく変化をしたこととなる。

その後、JISには5年に1度の見直し要件があるが、法改正議論を見据えて、本文の改定は行わず、2010年（平成23年）に解説の改訂および表示事項整理票を追加し規格の利便性を向上させるための「確認」として公表された。

3．2017年版JIS改正の経緯

今回の改正は、個人情報保護法が2015年9月に改正され2017年5月30日に全面施行となったことによるものである。

法律に用語の平仄を合わせ、管理策を追加し、マネジメントシステム規格としての位置づけをより明確化にするために、規格の構成を見直すこととなった。

法改正に伴い、各主務大臣が保有していた個人情報保護法に関する勧告・命令等の権限が個人情報保護委員会に一元化され、個人情報保護法に関する問い合わせや漏えい等事案への対応は、包括委任分野を除き、原則、個人情報保護委員会によって行われることになった。

執行権限が個人情報保護委員会に移管されたことにより、経済産業省の個人情報保護法の執行の際の基準となる「経済産業分野ガイドライン」が廃止され、今後経済産業省が作成をするJIS Q 15001に法解釈を盛り込むことができなくなった。

よって、改正個人情報保護法による法執行体制の移行により、本規格は、個人情報保護委員会における法の執行の際の基準となる指針とは別の指針としての位置づけの明確化が必要になった。

2017年版は、個人情報保護法に基づく指針ではなく、工業標準化法に基づくマネジメントシステムであることを明確にしたことになる。

個人情報保護法の上乗せガイドラインとしての役割を担うものではなくなり、改正前のJISとはその存在意義が多く異なることとなる。

4．改正された規格の構造

今回の改正は、本規格のマネジメントシステム規格としての位置づけの明確化、平成29年5月30日に改正個人情報保護法が全面施行されたことを受けて用語の平仄を合わせるとともに管理策等を追加することが主たる目的である。

なお、改正に当たっては、この規格が民間部門の個人情報保護の促進及び消費者保護に重要な役割を果たしていることから、要求事項の基本的な考え方を変更せず、旧規格に基づいて構築された個人情報保護マネジメントシステムがこの規格の改正によって不適合を生じないことに配慮している。

2017年版は、マネジメントシステムに関する要求事項を記載した本文と、管理策を記載した附属書A（規定）とに分離した規格票の構成となっている。さらに、附属書Aの理解を助けるための参考情報を記載した附属書B（参考）及び附属書C（参考）、並びにこの規格と旧規格との対応を示した附属書Dの構成から構成されている。

2006年版までは、規格の本体および解説で構成されており、マネジメントシステム構成要素に加え、マネジメントシステムの対象である個人情報についての取扱いに関する法的解釈が含まれたルールが規定されていた。そのため、今後の個人情報保護法等の改正や技術的進歩による対応を踏まえたメンテナンスの必要性や、他のマネジメントシステム規格との整合性確保の観点から、規格の構成について検討が行われた。

個人情報保護と、情報セキュリティとは安全管理措置の点で共通する事項が多いことから、統合版ISO補足指針の付属書SLに整合したマネジメントシステム規格として先行して制定されているISO27001を参考とした。

ただし、本規格に対応するISO規格は現時点では存在しない。そのため付属書SLに完全に準拠しているわけではない。対応するISO規格が存在しない時点で、ISO規格に近接した規格構成としたことは大きな意義がある。

5．おわりに

JIS Q 15001は、個人情報保護法の存在しない時期のコンプライアンス・プログラムとしての時期から、個人情報保護法に基づくマネジメント・システムへ、そして工業標準化法に基づくマネジメント・システムへと変化をしてきた。

ただし、個人情報の取扱いについてのリスクは情報セキュリティとは違い、法令順守の観点から個人情報保護法上の対応をしなければならないとなること、要するに個人情報保護法に定められた事項を残留リスクとすることはできないというところは注意が必要である。

JIS Q 15001 の改正に伴う実務対応

一般財団法人日本データ通信協会
Pマーク審査部　主幹研究員
清水 政幸

1．はじめに

今回のJIS Q 15001の改正の趣旨は、マネジメントシステム規格としての位置づけを明確化するとともに、平成29年5月30日に全面施行された改正個人情報保護法（以下、「改正法」という）に対応する管理策を追加したことである。

JIS Q 15001:2017（以下、「改正JIS」という）では、①用語を改正法に合わせたこと、②外国にある第三者への提供の制限を追加したこと、③第三者提供に関わる記録の作成・確認などが追加されたこと、④匿名加工情報が追加されたことなどが主な変更点であり、従来からJIS Q 15001:2006（以下、「旧JIS」という）をベースに個人情報保護マネジメントシステム（以下、「PMS」という）を運用してきた企業にとって、改正法との差異が少なくなり、運用がやり易くなった。

2．個人情報の定義

旧JISでは、個人情報の定義がJIS本文に記述されていた。しかし、改正JISでは、「用語及び定義は個人情報保護法による」とされた。そのため、従来はJISのみを参照していればPMSの運用が可能であったが、今回のJIS改正で改正法を含む以下の法令等を参照する必要性が顕在化した。

・個人情報の保護に関する法律
・個人情報の保護に関する基本方針
・個人情報の保護に関する法律施行令
・個人情報保護委員会規則
・個人情報保護委員会ガイドライン
・関係省庁ガイドライン
・認定個人情報保護団体の指針
・地方公共団体が制定する条例
・行政手続における特定の個人を識別するための番号の利用等に関する法律

(1)　個人識別符号

技術の進歩に伴い、個人情報の取扱いについて様々な問題が起こり得る状況が生じている。例えば、Webサイトでの ID登録やCookieの取得によるターゲティング広告の表示など、取扱いによっては、経済的・精神的な被害が発生することも考えられる。そのため、今回の改正法では「個人識別符号」という類型が設けられた。個人識別符号の詳細は政令で定められているが、例えば、DNAの塩基配列、顔貌、虹彩の模様、声紋、指紋・掌紋、旅券番号、基礎年金番号、免許証番号、住民コード、個人番号などがある。

(2)　要配慮個人情報と特定の機微な情報

改正法に要配慮個人情報が導入されたことに伴い、改正JISもこれに準ずることとなり、例えば、旧JISで「特定の機微な個人情報」として規定されていた「勤労者の団結権，団体交渉その他団体行動の行為に関する事項」「集団示威行為への参加，請願権の行使その他の政治的権利の行使に関する事項」などについては改正JIS（改正法）には含まれていないなど微妙な差異が生じている。従来から旧JISに従った運用を実施しているのであれば、実務対応上は、特定の機微な個人情報も要配慮個人情報に含めて管理･運用すれば十分である。

3．外国にある第三者への提供

外国にある第三者に個人データを提供する場合には、法令に基づく場合等の例外（法第23条1項各号）を除いて、あらかじめ外国にある第三者への提供を認める旨の本人同意を得る必要がある。

第三者提供に係るフローチャートを**図表1**に示す。

(1) 外国から除外される場合

外国における個人情報の取扱いが日本国内で取り扱われることと同等と認められるのであれば、国内にある第三者提供に関する規則（法第23条）が適用される。

その条件とは次のとおりである。

① 同等性認定による外国：我が国と同水準の個人情報保護制度を有していると個人情報保護委員会規則で定める国に所在する場合

② 基準適合体制を整備：個人情報保護委員会規則で定める基準に適合する体制を整備している場合

①について2018年6月時点では、委員会規則で定められている国はない。なお、現在、日本とEU間の個人データ移転について協議が行われており、今秋までに欧州経済領域（EEA）参加国が指定される模様である。

②については、次の事項が該当する。

- 適切かつ合理的な方法による措置の実施の確保：例えば、個人情報の取扱い規定を含めた契約書や覚書の締結など
- 国際的な枠組みに基づく認定：例えば、APEC越境プライバシーシール（CBPR）の認証を得ていることなど

(2) クラウド型サービスを利用する場合

クラウド型サービス（例えば、Webメールやオンラインストレージなど）を利用する場合、国内であれば、「委託」による第三者提供と解釈され、本人同意は不要（法第23条5項）であったが、海外事業者が提供するサービスを利用する場合、法第24条が適用になり、「委託」は例外事項となっていないため、原則本人同意が必要となる。

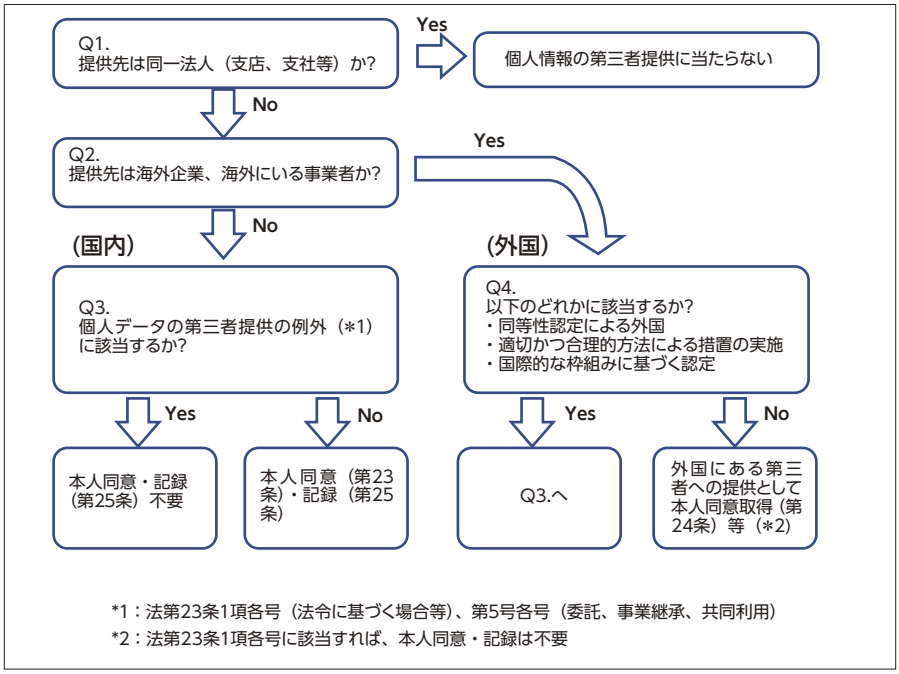
この場合、上述の(1)②基準適合体制を整備しているかどうかが問題となる。個人情報保護委員会のガイドラインによれば、委託契約において委託先（外国の第三者）が個人データを取り扱わない旨が規定されるとともに、適切なアクセス制御が行われていれば、基準適合体制を整備しているものと考えられ、本人同意を得る必要はない。しかし、「個人データを取り扱わない旨」がクラウド事業者の利用契約や約款に定められているか、これを交渉で獲得しない限り、当該サービス利用に係る本人全員の同意が必要となってしまう。実際問題として、既に取得済みの多数の個人情報について本人同意を得ることは膨大な時間やコストがかかり、事実上当該クラウドサービスの利用が不可能であるということもあり得るため、慎重な対応が必要である。

さらに、クラウド事業者においてサーバの場所（国外であるか否か）を明らかにしてもらえない場合は、同等性認定を受けている外国への提供であるか否かも判断できないことになる点にも注意が必要である。

4．第三者提供の確認・記録義務

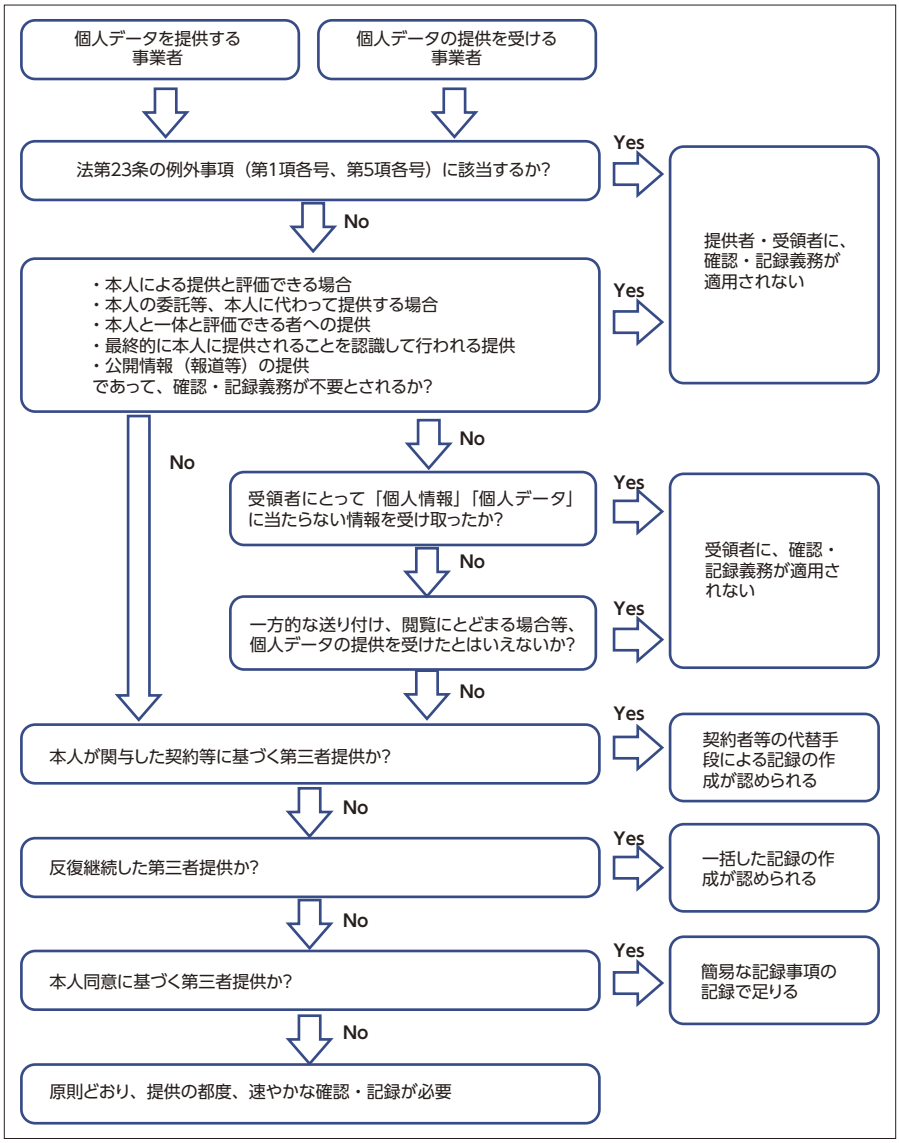
個人データの第三者提供の確認・記録義務は、不正な個人情報の流通を抑止しつつ、個人情報の漏えい等の事故・事件が発生した際に、個人情報保護委員会が、転々

図表1：第三者提供のフローチャート



出所：日置巴美「ビジネスシーンから考える改正個人情報保護法」（経団連出版）

図表2：第三者提供の確認・記録義務のフローチャート



出所：日置巳美「ビジネスシーンから考える改正個人情報保護法」（経団連出版）

流通する個人情報の取得の経路を迅速に把握し、トレーサビリティを確保するためのものである。

第三者提供の確認・記録義務のフローチャートを**図表2**に示す。

⑴　確認・記録義務を不要とする場合

恒常的に個人データの第三者提供を行ってる企業にとっては、都度記録を作成することの負担が大きいことを配慮し、**図表3**の場合には確認・記録義務は不要である。

また、次の場合は受領時には確認・記録が不要である。

・受領者にとって「個人データ」または「個人情報」に該当しない場合
・閲覧のみを行う場合
・一方的に個人データが送られてくる場合

⑵　第三者提供を行う場合の記録など

・記録の作成方法：紙・電子媒体のどちらでもよく、伝送ログ等でも可
・記録の保管期間：3年（施行規則14条2号、3号）、契約書その他の種類は1年（同1号）
・記録事項：提供年月日、第三者の氏名、本人の氏名等、個人データの項目、本人の同意

⑶　第三者から提供を受ける場合の確認

・確認方法：取得の経緯の記述を含む契約書、本人から得た同意書面等
・記録の作成方法と保存期間：⑵と同じ
・記録事項：本人同意による場合は、第三者の氏名、取得の経緯、本人の氏名等、個人データの項目、本人の同意

5．匿名加工情報

個人情報を利用するためには、取得時に特定した利用目的の範囲での取り扱いが求められ、目的外利用や第三者提供を行う場合は、原則として本人の同意が必要であ

る。しかし、既に大量の個人情報を保有している企業が新たなビジネスを検討するため、当該情報を第三者に提供するには本人同意の時間やコストがかかり、情報の利活用に支障が出ると言われていた。これを解決するために匿名加工情報という概念が導入された。匿名加工情報は特定の個人を識別できないように、かつ復元できないように加工した情報である。

⑴　匿名加工情報への適正な加工

匿名加工情報を作成するには最低限次の処理を行う必要がある。

・氏名や住所の一部など、特定の個人を識別できる記述の全部または一部の削除
・運転免許証番号やマイナンバーなどの個人識別符号の削除
・複数のデータベースの情報を連結するためのID（符号）の削除
・一般的に見て珍しい事実（例えば、症例数が極めて少ない病歴など）に関する記述の削除

⑵　匿名加工情報を作成する場合

上記の適正な加工に加え、次の事項が必要である。

・加工方法の情報漏えいを防ぐための安全管理措置の実施
・匿名加工情報に含まれる情報項目の公表
・匿名加工情報を他の情報と照合することによる本人特定の禁止

⑶　匿名加工情報を提供する場合

作成した匿名加工情報を第三者に提供する場合は、次の事項が必要である。

・提供する匿名加工情報の項目とその提供方法の公表
・提供先に対して匿名加工情報であることを明示

⑷　第三者から提供を受けた場合

第三者から匿名加工情報提供を受けた場合は、次の事項が必要である。

・加工方法等情報取得を禁止
・匿名加工情報を他の情報と照合することによる本人特定の禁止

しかし、一般的には匿名加工情報の作成方法が正しいかどうかは、個人情報の性質や利用目的により判断が分かれること、復元されてしまうリスクを的確に認識することは非常に困難であるのが実態であろう。そのため、匿名加工情報の作成に当たっては、自社の所属する認定個人情報保護団体に相談することが望ましい。

6．おわりに

今回のJIS改正が、昨年改正された個人情報保護法に対応したことで、従来からPMSを運用してきた企業にとっては、改正JISに適用したPMSを運用することで法を遵守するための手順を手に入れたと考えるべきであろう。一方、直接書面取得時の同意や、個人情報と個人データなどJISが法の上乗せになっている部分や、今回の改正で追加された部分（外国にある第三者への提供など）の例外事項がJISには記載されていないなど、更なる改正が望まれるところである。幸いなことに改正JISの附属書（参考）には、規格の補足説明（運用上のガイドラインとも言える）が記載されているので、PMS運用実務において参考にされたい。

図表3：確認・記録義務を不要とする場合

・法定例外事項	法第23条1項各号（法令に基づく提供等） 法第23条5項各号（委託、事業継承、共同利用）
・本人による提供	本人によるSNSでの情報発信など
・本人から委託を受けて行われる提供	自社サービスと他社のサービスをセットで提供する契約を本人と締結している場合に、サービス提供のために必要な個人データを他社に提供すること等
・本人と一体と評価できる関係にある者への提供	本人の代理人、家族などへの提供等
・最終的に本人にデータが提供されることを提供者が意図したうえで第三者を介してなされる提供	企業が従業員の口座に給与を振り込むため、個人の氏名、口座番号等を、仕向銀行を通じて被仕向銀行に提供する場合等
・不特定多数の者が取得できる公開情報	Webサイトの公開情報、報道情報等

出所：筆者作成

新 JIS 規格でプライバシーマーク審査基準はどう変わるか？

一般財団法人日本データ通信協会
Pマーク審査部長
小堤 康史

1.「審査基準」とは

ここでいう「審査基準」とは、プライバシーマークの認定を得るための事業者の皆様に対する付与適格性審査において用いられる審査基準のことである。

プライバシーマークの付与適格性審査は、文書審査と現地審査からなる。

文書審査は、事業者の個人情報保護マネジメントシステム（広い意味では事業者の個人情報保護に関する取り組み全体を指すが、ここでは規定類、様式類など、それを説明する資料類をいうこととする。以下PMSという）が、審査基準に合致しているかを確認するものであり、これは事業者から提出された申請書類を閲覧しながら机上で行う。

また、現地審査は、実際に事業者を訪問し、審査基準に合致していることを確認した事業者のPMSが、実際に適切に運用が行われているかを確認するものである。

この2段階によって、事業者の個人情報保護に関する運用が審査基準に合致していることを確認する。

適切であれば付与適格性が確認されたとされ、審査会を経て合格となり、登録手続きを経て、登録の証を公表するなど、用いることができるようになる。その期間は2年間であり、期間終了の前に、更新のための手続き（更新申請）が行われる。

各段階で用いられる審査基準は、JIS Q 15001に基づいて作成されているため、審査基準に合致していることが確認された、ということは、事業者のPMS運用がJIS Q 15001に適合して運用されていることを証することになるのである。

JIS Q 15001という規格は、最初の版が1999年版、次の版が2006年版、さらに本文は2006年版のまま解説のみの差し替え、と見直しの歴史をたどってきた。そして今般、2017年版が登場した。JIS Q 15001が改版されたので、これに対応してプライバシーマーク審査の内容（審査基準）が変更される。これが審査基準の変更である。※1

2. プライバシーマーク制度における審査基準

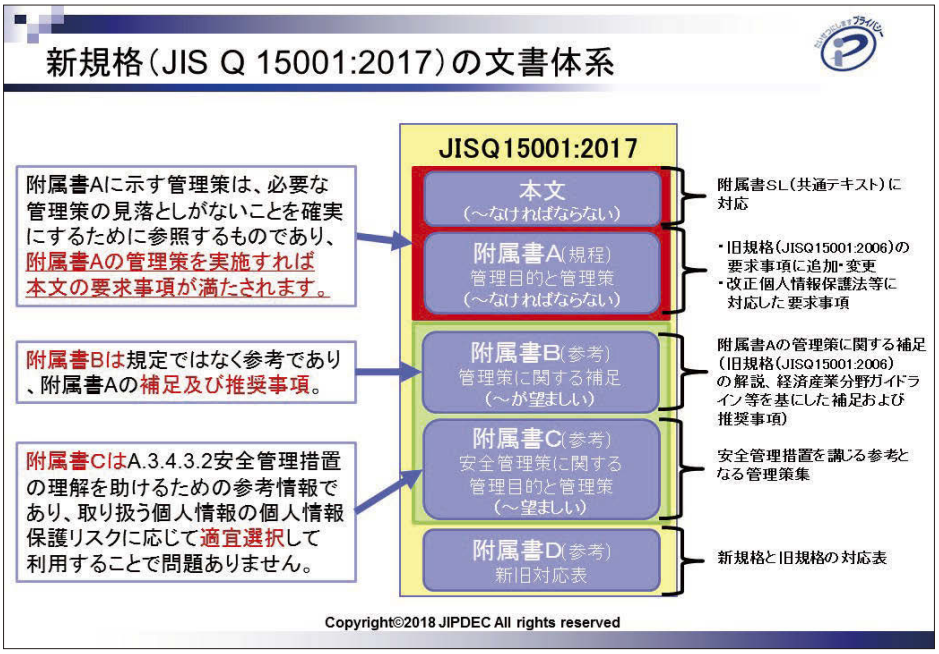
プライバシーマーク制度は、かなり普及してきたが、約300万社とも言われる日本国内企業のうち、約1万6千社程度、0.5%が認証されているに過ぎない。現在もプライバシーマークを取得しようとする企業は多いが、取得総数の伸びは鈍化している。しかし一種のプレミアなマーク制度と考えれば、これはこれで、一つの現在の姿であることは間違いない。

プライバシーマーク制度、という仕組みを決めて運営しているのは一般財団法人日本情報経済社会推進協会（JIPDEC）のため、審査基準についても、JIPDECが決定する。私ども日本データ通信協会はJIPDECに連なっている18の審査機関のひとつに過ぎず、主に電気通信事業者を対象とした業種の範囲で審査業務を行っている。従って、ここで説明する審査基準は、JIPDECから公式に説明されたものがベースとなっている。

プライバシーマークの審査項目は、原則として、JIS Q 15001：2017（2017年版JIS）の附属書Aの各管理策に対応している。

※1 JIS Q 15001：2017は2017年12月20日に公示されたことを受けて、一般財団法人日本情報経済社会推進協会（JIPDEC）は2018年1月12日に、対応の審査基準を公表している。URL（https://privacymark.jp/system/operation/jis_kaisei/index.html）参照。

図表1：新規格の文書体系



出所：一般財団法人日本情報経済社会推進協会（JIPDEC）説明資料より

この2017年版JISの附属書Aは、2006年版JISの本文をほぼ踏襲して作成された。このため、審査項目も、結果としては2006年版JISのときの審査項目に、かなり近似している（本号５ページの篠原論文「４．改正された規格の構造」を参照）。

2017年版JISの附属書Aに対応していることから、見出しは全て、A.x.xの体系となり（Aで始まるのは、JIS Q 15001：2017の附属書Aであることを示す）、その順番に記述されている。

管理策のひとつひとつに対して、審査項目、例えば、対応する手順等を定めていること、意思決定が必要な場合に事業者内で承認する手順を定めていること、定められた手順に従った運用の状況を記録で示すか、または説明できること、等が記述されている。

この新しい審査基準によって、どのように審査が行われるのか、JIPDECは今年の1月15日以降、全国規模で20回近く説明会を開催した。当方もJIPDECの許諾を得て同等内容の説明会を行ってきた。そこで本稿では、その後に明らかにされたことも含め、説明会で説明した内容を要約する。もちろんその文責は全て筆者にある。

なお、この公表された審査基準に対して、今のところ解説・説明が公表されていないが、8月以降に、JIPDECのホームページで公表されるようである。

3．審査基準の概要

すでに述べているように、改正後の審査基準はこれまでの審査基準とは連続性がある。ただし、まったく同じではないので、その差分を確認する必要がある。

手早く確認しようとするならばJIS Q 15001の改正の目的にさかのぼって見ることが妥当である。（篠原論文「３．2017年版JIS改正の経緯」を参照）

4．改正個人情報保護法への対応について

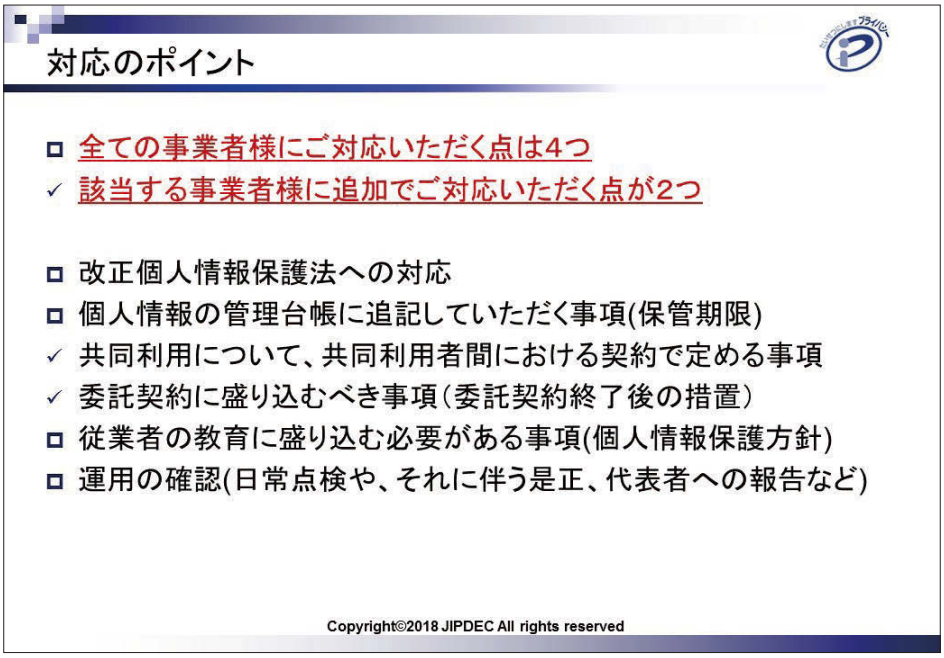
今回のJIS改正の最大の目的は、改正個人情報保護法のキャッチアップであった。

昨年5月30日の改正個人情報保護法の施行以降、日本の個人情報保護のルールは、改正された個人情報保護法に基づいている。JIS Q 15001は、2006年版の策定時には、その時点の個人情報保護法の内容をキャッチアップしていたし、当時の謳い文句として、JIS Q 15001：2006に従っていれば日本の個人情報保護法を守っていることになるのだ、とされていた。その個人情報保護法が改正されたため、その謳い文句がストレートには言えない状況になっていた。そこで今回、改めて改正された個人情報保護法をキャッチアップしたことになった。※2

すると、事業者の皆様への、この点での影響は、そもそも昨年5月30日の施行までに、改正法対応の準備が

※2 ただし、JIS Q 15001：2006の3.3.2には、「法令、国の定める指針その他の規範」という要求事項があった。改正個人情報保護法も、いうまでもなく法令であることから、2006年版JISのままでも、改正個人情報保護法（およびこれに基づくガイドライン等）を特定し、それらを遵守していることが要請されていた。もちろん、大半の事業者の皆様も、これに従い、既に改正個人情報保護法に従った個人情報の取り扱いを行っていることと思う。

図表2：事業者にとっての対応のポイント



出所：一般財団法人日本情報経済社会推進協会（JIPDEC）説明資料より

行われていて、すでに運用も行われているはずであるから、今回のJIS Q 15001の改正による影響は、必ずしも大きくはない、ということができる。

ただし、審査基準として見た場合は、単に新たに改正された個人情報保護法を特定しているか、というレベルではなく、改正された個人情報保護法で示された規範に対応した手順等が定められているか等、確実にレベルアップがされている。

これに属するJISの改正は、A.3.4.2.8界隈に集中しており、第三者提供を巡るルールの高度化に対応できているのか、が主な審査基準の変更ということになる。

ここも、改正個人情報保護法の主旨となるが、名簿提供行為の規制、海外への個人情報移転の規制などがルール化に影響している。

例えば、第三者提供の確認記録義務、国外の第三者への提供、そして匿名加工情報のあたりは、各事業者において、実際に生じる場面があるのか、あるならば、そのときの一連の運用手順、承認手順はどうか、また承認手順に対応した記録様式は整備されているのか等が、その最たるものであろう。

5．要配慮個人情報について

次に、単なる用語の変更とはいえないものがあり、それが「要配慮個人情報」である。2006年版JISでは、「特定の機微な個人情報」という用語で整理されていた領域であるが、ほぼ同等の領域を示しているものの、改正個人情報保護法の定義が、必ずしも、2006年版JISの「特定の機微な個人情報」と完全一致していないので、これへの対応が示されている。

この場合、事業者の皆様は、単に、用語定義を差し替えるだけでは、論理的には不十分であり、特定されている個人情報（いわゆる「個人情報管理台帳」に記載されている個人情報）のすべてに対して、改めて「要配慮個人情報」の定義に従って、対象となるかならないかの判定を行うことが求められる。

6．保有個人データについて

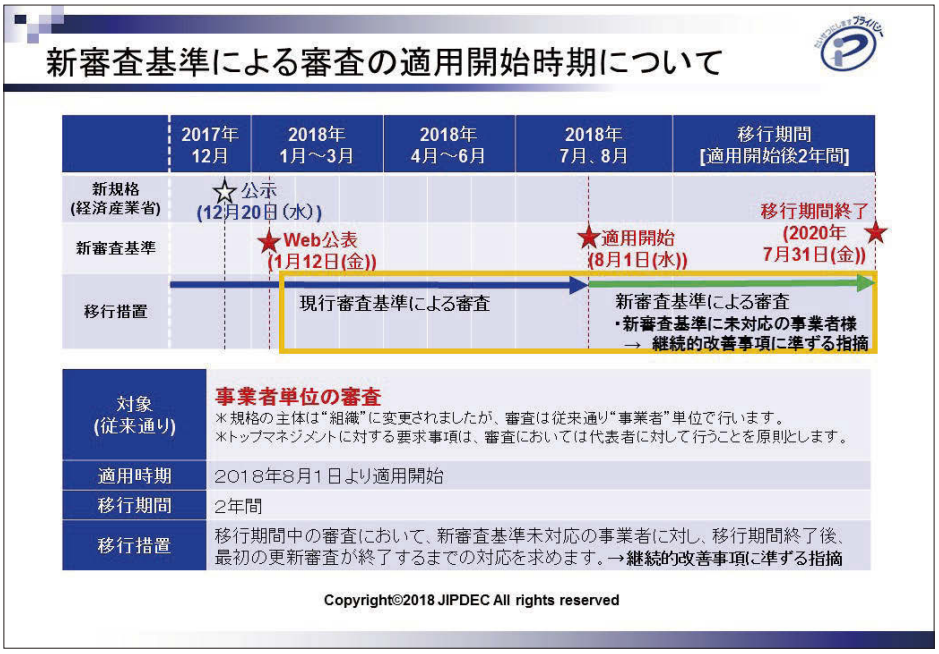
一方、開示対象個人情報という用語は、JIS Q 15001：2017において保有個人データという用語に置き換わったが、これに関しては、個人情報保護法で定義されている保有個人データではなく、引き続きJIS Q 15001：2006の用語である開示対象個人情報と同等である、と説明されているため、単なる用語の置き換えとなる。これは、甚だややこしい。つまり、改正個人情報保護法の用語である保有個人データとは、微妙に定義が異なる、という状態を説明していることになるからである。

しかし、多くの事業者が、自社のホームページで「開示対象個人情報」という用語を用いて、開示等の求めの手順を公表していることに対する影響を考えれば、やむを得ないことであろう。この点については審査基準の改正によって直ちに事業者の皆様に対してホームページの修正を求めないこととなり、この点が救われる。

7．保管期限について

個人情報の保管期限の管理、という審査基準が、今回新たに示されている。

図表3：新審査基準による審査の適用開始時期



出所：一般財団法人日本情報経済社会推進協会（JIPDEC）説明資料より

これは、使われなくなった個人情報はできるだけ速やかに消去等を行うことが望ましい、という努力義務に対応した審査基準となる。いわゆる「個人情報管理台帳」等の管理項目に、この保管期限を設ける、その管理項目に対応して記載内容に、いつからいつまで保管するのか、ということを記載する（定める）、そして、実際に保管期限が到来したら管理手順に従って実際に消去等を実施する、一連の手順が定められているか、実際に運用されているか、ということが示された。

これについては、見かけは地味な審査基準の改正だが、以外と事業者にとって影響が大きいのではないだろうか。単なる、“望ましい”とされる事項から、手順の具体化が要請されたことになるからである。

8．その他

他にも、細々した審査基準の見直しがされているが、全てを網羅してここに記すことは紙面の都合上不可能であるので、この辺で留める。

JIS Q 15001：2017の本文を、自社内でどう取り扱うのか等は、今回の審査基準の中では説明されていないので、迷う向きもあろうかと思う。

附属書Cの使い方もとまどう事業者の皆様は多いと思う。

また、審査基準としては、単なる用語の置き換えは必須ではない、という言い方がされているが、将来のわかりやすさを考えれば、審査基準とは別に、この際、用語の置き換えをしておいたほうが良いと、個人的には思う。

このように、単に審査基準への対応だけでは、次回のプライバシーマーク更新審査対応としては良くても、自社のPMSの改善として見れば不足なところもあるので留意が必要である。JIS Q 15001：2017の全文を、審査基準対応として、だけではなく、何度も眺めることによって、自社のPMSの改善への気づき（ヒント）を得ていただきたいと思う。そして、それができるのは、自社の組織等を知る事業者の皆様ご自身である。

9．対応の方向性

事業者は、取り組みの手順としては、まず、審査基準を熟読すると良い。それを前提に、審査基準を用いて、JIS Q 15001：2017との合致の内部監査を実施することが妥当である。すると、すでにこれまでの取り組みのままで、2017年版への対応としても問題がないところと、それでは不十分なところが浮かび上がってくる。不十分なところを補強すれば、まずは、第一段階としては、最低限の山を越したことになる。

整備された社内ルールを正式化し、そのルールでの運用を積み重ねれば、要するに2017年版JISに対応した運用も実施されていることになる。このタイミングで次のプライバシーマーク更新審査が行われれば、自社内の判断だけではなく、審査に基づく客観的な認証も行われたこととなるので心強い。

ちなみに、新審査基準による審査は、この8月から開始となる。そして最終的には2020年7月末までには、更新審査において、新審査基準への適合が求められる。対応を進めていただきたい。

03 Seminars

欧州一般データ保護規則（GDPR）の最新動向

ひかり総合法律事務所　弁護士
理化学研究所革新知能統合研究センター　客員主管研究員 板倉陽一郎

本稿は、去る5月19日に一橋記念講堂（東京都千代田区）で開催された情報法制研究会第7回シンポジウム（主催：日本データ通信協会 情報法制研究会）において、欧州の新しい個人データ保護規則である「欧州一般データ保護規則(GDPR：General Data Protection Regulation)」の最新情報を詳しく解説した板倉陽一郎氏（ひかり総合法律事務所弁護士、理化学研究所AIP客員主管研究員）の報告内容を紹介するものである。欧州における個人情報保護の実態に詳しい板倉弁護士の解説は、日本の企業にも大きな影響があるGDPRを理解するうえで最適の教材である。

実務家としていくつかの企業、企業グループの対応を手伝っているが、GDPRは日本経済新聞の一面で取り上げられるなどしているため、経営陣の関心が高い企業も多い。現場の方々は休日を返上して想定問答を作るなど真摯な対応をしているケースが見て取れる。本日は、前半で事業者の皆さんがGDPRに対応をするにあたって気になるであろうポイントを中心についてお話をし、後半は十分性認定の状況について説明をしたい。

1 GDPRの概要と実務的に重要なポイント

GDPRとは何か

GDPRは欧州の新しい個人データ保護の仕組みである。EU法は憲法のレベルである一次法（Primary Legislation）と、法律のレベルである二次法（Secondary Legislation）に区分され、二次法には規則（Regulation）、指令（Directive）、決定（Decision）、勧告（Recommendation）、意見（Opinion）が含まれる。GDPRはこの中の規則に当たる。従来、EUの個人データ保護は「指令」で律せられ、どのような法令を作るかは加盟各国に委ねられていたが、「規則」は加盟国の国内法に優先して加盟に適用され、加盟国の政府等に対して直接的な法的拘束力を及ぼすため、今後はおおむね加盟国は同じ内容の法令を執行することになる。

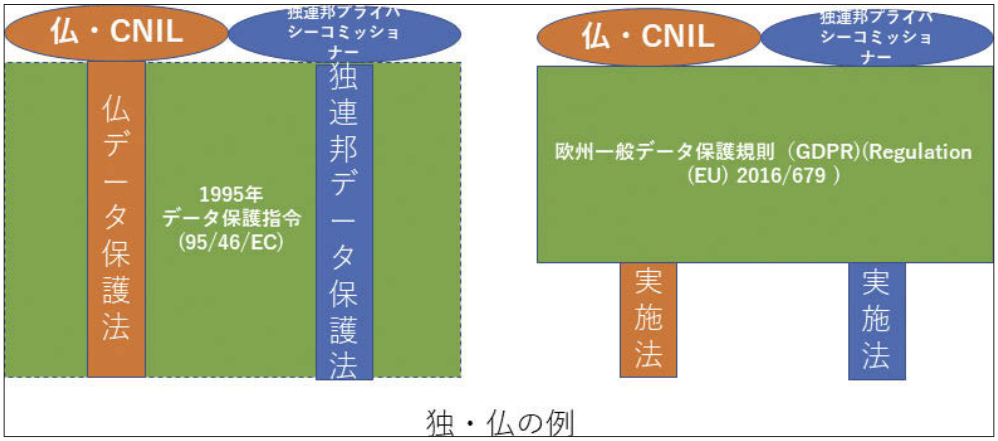
GDPRはデータ保護の改革パッケージの一環である。刑事データ保護もあわせて改革が行われ、決定のレベルで行われていた取り組みが新たに「刑事データ保護指令」と「指令」に格上げされる。刑事データ以外の「一般」のデータ保護の仕組みが「規則」に格上げされることとなった。GDPRの「一般」は刑事データとの比較で「一般」というわけである。

これまでは指令にあわせて、各国が法律を作っていたが、今後は皆で同じ規則を執行することになる。ただし、一部の条項では実施法で例外事由を定めることが各国に留保されている。

EU各国の対応状況

GDPRは5月25日に全面適用される予定だが、直近のニュースでは5月25日に施行が間に合わない国が8カ国ほどあるようである（本報告は5月19日に行われた）。EU加盟国はデータ保護機関の権限や、課徴金の仕組みなど、国内の法律を整える必要があるが、6年前の2012年にはすでにプロポーザルが出ているにもかかわらず、立法が間に合わず施行できない国が31カ国のうち8カ国も出ているのである。したがって企業の準備が間に合わないのは、ある意味当然といえば当然とも言える。

図表1：データ保護指令から一般データ保護規則へ



出所：筆者作成

各国の実施法についてはどうか。欧州の主要法律事務所ですら全体状況を把握できていない状況であるが、今年の2月時点でレイサムワトキンス法律事務所が整理したところでは、成立したのはドイツ、オーストリア、スロヴァキア、ベルギーに限られている。ベルギーなど近年まれに見る大改正を行っている。またいくつもの国で、データ保護機関の名称を変更するなどの対応が進んでいる。

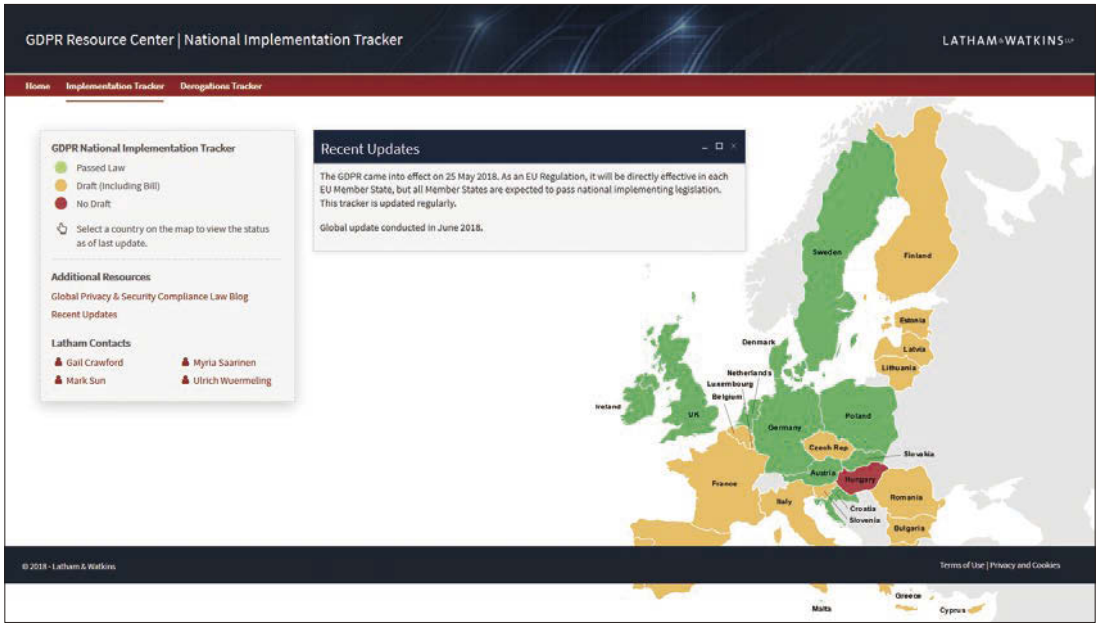
国によって実施法の定め方は千差万別である。例えば、GDPR第89条2項は、「科学的又は歴史的研究目的又は統計目的」についてデータ主体の権利の除外を定めることを規定している。日本では、学術研究例外は個人情報取扱事業者としての義務がすべてかからないというドラスチックな規定をしているが、GDPRは全部の義務がはずれるわけではなく、本人の権利の一部を制限してもよいという開かれた対応になっている。ドイツでは除外するのではなく、安全管理措置を義務付けている。イギリスでは除外について承認のプロセスを設けていたり、アイルランドでは除外は認めるもののデータ最小化の原則を残したりするなど、その定め方は各国で異なる。

EUがGDPRを制定した理由

GDPRを作ったのは何故か。従来の「データ保護指令」は1995年に施行された。当時はせいぜい「Windows95」が世に出て、日本で「テレホーダイ」が人気になっていた頃であり、インターネットの状況が全く違う。指令には本人の権利への配慮が足りていなかった。そこを強化するという狙いがある。

他方で、今回のデータ保護改革パッケージは、「デジタル・シングル・マーケット」、「ワンストップショップ」などのビジネスの流れと密接につながっており、欧州に31の個別の法律があるのはやはり不便である。これ

図表2：GDPRの実施法成立状況（2018年2月現在）



出所：レイサムワトキンス法律事務所ウェブサイト“GDPR Resource Center”より引用（2018年6月現在）

を一つにまとめたいという要求がある。日本やアメリカなど外から見た場合にも、それはあてはまる。

しかし実際には、先ほど説明したように、除外事由の定め方ひとつですら、国によってまったく異なるのが実情であり、日本企業の皆さんが欧州に進出する際に、実施法まで読みこなすのは一筋縄ではいかない作業となる。

GDPRが適用される範囲

GDPRは5月25日から適用される。適用の対象は、EU構成国28カ国と欧州経済地域（EEA）のノルウェイ、リヒテンシュタイン、アイスランドを併せた31カ国である。日本が十分性認定に際して同等性を認定するのも、このEU+EEAが対象となることになっている。したがって日本の事業者から見ると、この31カ国のどこかに拠点があれば、外国にいる第三者へのデータ移転はある程度円滑になるということができる。

①適用の実態的範囲

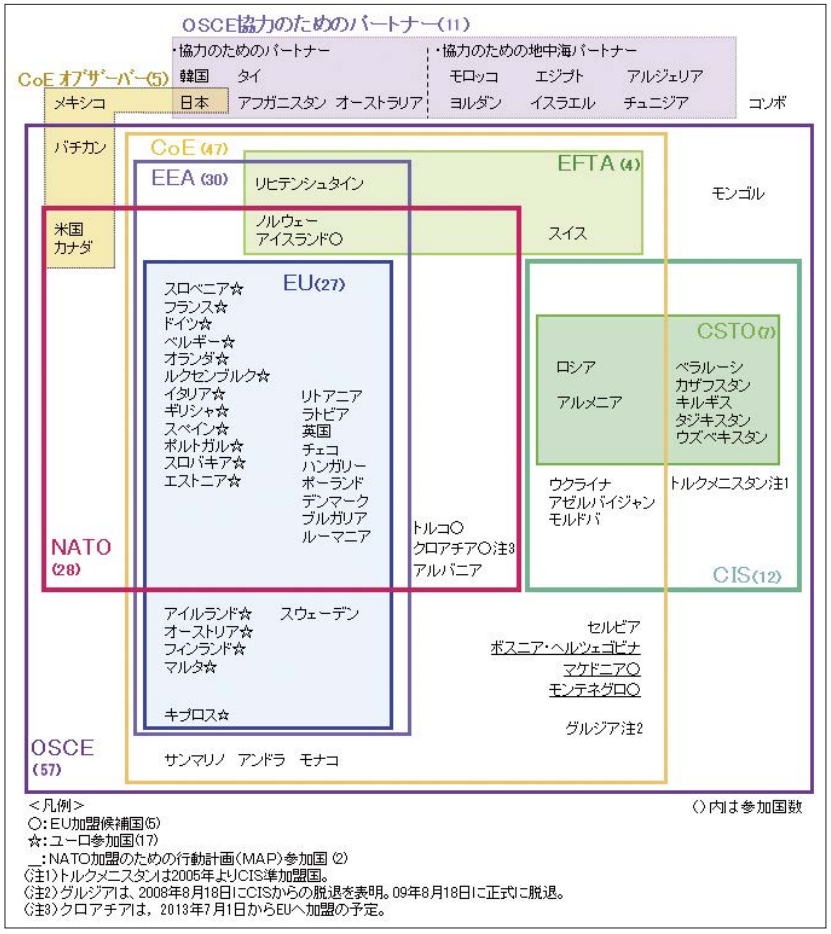
適用範囲については、「全部又は一部が自動的な手段による個人データの取扱いに適用される」とされ、「ファイリングシステム」の一部ではないものには適用されない。データベースの一部に入っている、もしくは入る予定のものが対象となる。ある程度広く取られる傾向はあるので、例えば散在情報である名刺の束も、名刺アプリでデータベース化される「予定」のものはこの中に入ってくる。

②適用の地理的範囲

地理的範囲は域外適用が大きな話題になっているが、現地に拠点がある企業の場合には、第3条1項もかなり問題になるというのが企業の相談を受けての感想である。つまり、「本規則は、EU 域内の管理者又は取扱者の事業所の活動に関連してなされる個人データの取扱いに適用される。この場合、その取扱いが EU 域内又は域外でなされるか否かについては問わない」とされており、EU域内の管理者あるいは処理者の活動に関してなされる個人情報の取扱いには適用されるので、支店の活動の一部を本店が助けているような場合には、その本店の活動にもGDPRは適用される。そこは注意が必要だ。

日本の個人情報取扱事業者がクラウドを活用している場合も、それは日本における処理の一部であり、我が国の個人情報保護法が適用されるとされているのと解釈は

図表3：GDPRの適用範囲



出所：外務省ウェブサイトより引用（ただし、クロアチアが2013年にEUに加盟しているため2018年6月現在、EU加盟国数は28）

同じで、EU側でも同じだと考えればよい。

③行動ターゲティングへの影響が懸念される第3条2項(b)号

域外適用については、皆さんすでに相当程度ご理解されているのではないかと思うが、第3条2項に「(a) EU在住のデータ主体に対する商品又はサービスの提供に関する取扱い。この場合、データ主体に支払が要求されるか否かについては問わない」というものと、「(b) EU域内で行われるデータ主体の行動の監視に関する取扱い」の二つの号があり、後者は主として行動ターゲティング的なものが当たる。(a)号に関し、「グローバルサイトにEUの人がアクセスしてくることがあるがどうすればよいか」という問合せをしばしば受けるのだが、それらはEUを狙っているわけではないので該当しないと整理できるものがほとんどである。例えばEU域内に商品を送る通販サービスは該当するが、単なる英語のグローバルサイトが(a)号に当たるという解釈はないと思う。

他方で、行動ターゲティングなどについては、前文を見ても意図や狙いについては記述がない。そこで、意図せずにEUの消費者に関してタグを貼り解析をしてしまったというものについても対象にする前提であるように思われる。

これについては、EUの消費者のIPは取り除くであるとか、分析をしないで保管だけをしておくという動きが出ている。EUの消費者から見ると、こうした動きは保護が過剰すぎて、排除されすぎという気がしないでもない。EUの消費者のデータを分析しないことによって個人向けに広告がカスタマイズされないとなる程度であればよいが、事業者にとってそのサービスを提供する意味がないので提供を止めるということになると、最終的にはEUの消費者の利益にならないことになってしまう。そうした流れになれば、市民の側から厳格な対応を批判する動きが出てくるということも可能性としてはありえるだろう。

第3条第2項(a)号については、EU市場を狙う場合に適用されると考えて良い。(b)号については、意思的な要素が加味されていないので、偶発的にデータ主体が加わってくる場合も文言解釈上は排除することは困難であって、トレンドとしては技術的な手段で排除しているように見える。

欧州データ保護会議（EDPB）のガイドラインの重要性

GDPR第68条で各国のデータ保護機関の集まりである「欧州データ保護会議（EDPB)）」が法人格を有するようになる。従来は「29条作業部会」がガイドラインを出していたが、名称が変更されたものである。EDPBがその役割を担うことになる。日本企業もそのガイドラインを見ていく必要がある。

これらのガイドラインの中で、事業者から見て最も気になるのが「同意」のガイドラインではないかと思う。欧州側は、同意によって個人データ移転のスキームを構築すること自体があまり望ましいことではないと考えている。とは言え、同意以外で移転を実現することが難しい場合は多々あるはずなので、その場合にはガイドラインをしっかりと理解しておくことが重要になる。

「透明性」は日本で言うと利用目的等の通知事項に当たり、GDPRでは第13条、第14条、第15条などに該当するガイドラインである。これらについても理解をして必要な準備をしておくのがよいだろう。

「プロファイリング」や「ポータビリティ」はこれらに

図表4：欧州保護会議（EDPB）のガイドライン

- Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679（認証基準）
- Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679（例外事由による越境移転）
- Guidelines on Consent under Regulation 2016/679 (wp259rev.01)（同意）
- Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)（透明性，通知事項）
- Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)（個人の自動的決定，プロファイリング）
- Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01)（データ侵害通知）
- Guidelines on the application and setting of administrative fines (wp253). Now including available language versions.（課徴金）
- Guidelines on the Lead Supervisory Authority (wp244rev.01)（主要監督機関）
- Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)（DPO，データ保護監督者）
- Guidelines on the right to "data portability" (wp242rev.01)（データポータビリティ）
- Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)（データ保護影響評価）

出所：筆者作成

比べれば実務上の優先順位は下がるだろうが、「データ保護責任者（DPO : Data Protection Officer）」を置かなければならない事業者はしっかり見ておく必要がある。

これら9つのガイドラインについては、個人情報保護委員会が積極的に翻訳を行っており、現在のところそのうちの4つが公開されているので、参考にしていただきたい。

制裁金算定における一体性の議論とDPOの範囲の問題

制裁金は経営者が気にする部分であり、「売上高の4%も制裁金を取られてしまうと潰れてしまう」という反応があるが、何をベースに4%を課すのかは現時点では必ずしも明らかではない。「連結売上高の4%」という報道がなされていたりするが、GDPRの前文を見ると、「ここで対象となる企業とは、TFEU の第 101 条及び第 102 条に従う企業として理解されなければならない」とされている。これらは独禁法の規定であり、独禁法での解釈でなされているように経済的な一体性があれば、それが課徴金の分母になると判断するのか、それともデータ処理の一体性を基準とする別の判断をするのかは判然としない。アメリカなどの企業が欧州司法裁判所で争うことになれば、そこで判断がでることになるだろう。

DPOをグループ会社全体で日本側に置こうとした場合、欧州側にDPOを置くと日本側でコントロールするのが難しくなり、解雇などが簡単にはできないという問題もでてくる。そこで、日本側で人を置き、欧州の子会社も含めてその人物が監督をするとなると、今度はデータの処理は日欧で一体ではないかと言われる可能性が出てくる。DPOをどの範囲で置くかは、課徴金とリンクする問題であるという認識が必要ではないかと思う。

個人データ取扱いの権利と義務（同意の取扱い）

GDPRでは第5条、第6条で個人データ取扱いの原則を定めており、これらに基づいて処理の適法性を確保しないとそのデータは使えない。GDPRは日本の個人情報保護法と異なり、処理も移転も原則は禁止で、管理者側でその根拠の妥当性を立証する必要がある。処理をする場合には第6条のどれに当たるのか、移転をする場合には第45条から第49条のどれに当たるのかを考察し、関係するデータをマッピングしなければならない。

例えばダイレクトマーケティングは第6条(f)号の「正当な利益（legitimate interest）」に該当すると推定されうるとしばしば言われるが、実際にはそれほど簡単ではなく、英国の情報コミッショナー事務局（ICO）が三段階テストと呼ぶもの、つまり目的のテスト、必要性のテスト、バランシングのテストなどを越えて認められるものと考える必要がある。

ダイレクトマーケティングについては、はがきを送る、電話をかけるなどといったシンプルな業務は認められるだろうが、クッキーを介した複雑なインターネット上の行動ターゲティングもすべて第6条(f)号で読めると考えるのはリスクがある。

現在は、事業者はクッキーを使用することを利用者に対して表示し、ボタンを押して同意をもらい、その利用を認めてもらうということをしている。そのユーザがサイトに戻ってきたことを確認するためのクッキーの利用であれば、ボタン程度でよいかもしれないが、すべてのケースで大丈夫かといえば疑問が残る。

GDPRが施行される前にベルギーの情報保護機関がフェイスブックを相手取って「いいね」ボタン等の情報収集手段の利用に異議を唱える裁判を起こし、ブリュッセルの第一審裁判所で勝訴した。フェイスブックはきちんと同意を取って個人データを収集しなければならないという判決だが、これぐらい厳しく同意を求められるとアドテク業界には未来がないとまで言われるぐらいの話だ。

GDPRでは、第7条で同意は本人が望めば撤回できなければならないとなっているし、従業員との同意も厳しく見られていると一般的に言われているので、同意に基づいてデータ収集を行う場合には気をつけてスキームを作る必要がある。

なお、ダイレクトマーケティングには「ダイレクトマーケティングへの異議（第21条2項）」という特別な条項があり、処理根拠にかかわらず異議が認められる。また、日本の「要配慮個人情報」に相当する第9条、第10条の「special cathegorized data」については、さらに厳しく「明示的な同意」が必要となる。

「忘れられる権利」などデータ主体の権利

データ主体の権利への対応に関連しては、「消去権」が議論の中でクローズアップされてきたが、条文上は従来の消去権プラスアルファぐらいで落ち着いている。同意を撤回した場合には消去を請求することができる（第17条1項(b)号）。個人データのコピー先に対しては「利用可能な技術及び実施の費用を考慮し、当該個人データを取り扱っている管理者たちにデータ主体が当該個人データのあらゆるリンク又はコピー若しくは複製の消去を要求している旨を通知するために、技術的措置を含む合理的手段をとらなければならない」（17条第2項）となっている。

GDPRの規定とは別に、データ保護指令第12条に基づ

く消去の要求を行った2014年5月のグーグルスペイン事件があり、これに基づいてグーグルは欧州において検索結果削除を行っている。この資料を作成した時点での除外リクエストが約68万件、URLが約263万件で除外請求は右肩上がりで増え続けている。削除されているものには我々の知らない欧州のサイトもあるが、フェイスブック、ツイッター、ユーチューブ、グーグルグループ、インスタグラムなどが目立っている。

ここで問題となってくるのは、世界中のデータを消さないといけないのか、それとも「google.fr」などの、各国向け検索サイトだけ消せばいいのかという点である。

2015年にフランスが世界削除するようにグーグルに求めたが、これをグーグルは断った。グーグルは「それを認めてしまうと、非民主的な国家が、情報を統制するための自国の法律を、国際的に認めるように要求し始めるだろう」と懸念を表明し、フランスの行政最高裁判所であるコンセイユ・デタに上告をした。コンセイユ・デタは2017年7月に欧州司法裁判所に命令が可能か判断を求め、この情報が最近、欧州司法裁判所のWebサイトに掲載されている。域外の削除を求めることができるのか、課題として残っているので注目をしていてもらえればと思う。

データ管理者、データ処理者の義務で重要なのは取扱い活動の記録

義務の中でもっとも重要なのは第30条の「取扱い活動の記録」である。事業者は、自社で行っている個人データの取り扱いをマッピングして把握しなければいけない。このデータの棚卸しはたいへんだが、GDPRに対応するためには不可欠である。事業者の皆さんには、マイナンバーに関連して「第三者提供時の確認・記録義務」への対応をやっていただいたと思うが、それと同様である。全部署でEUに関係する情報にどのようなものがあるのかを把握し、この記録の前提となる記録帳票を作るのがGDPR対応の始まりということになる。

データ保護オフィサー（DPO）設置の必要性

データ保護オフィサー（DPO：Data Protection Officer）は、「管理者又は処理者の中心的業務が、その性質、適用範囲及び/又は目的によって、大規模にデータ主体の定期的かつ系統的な監視を必要とする取扱い作業である場合」（第37条1項(b)号）に設置しなければならないとされている。さらに「管理者又は処理者の中心的業務が、第9条で言及された特別な種類のデータ及び第10条で定める有罪判決及び犯罪に関する個人データを大規模に取扱う場合」（第37条1項(c)号）とも規定されている。ただし、後者は医療情報などを取り扱う場合でない限りはあまり該当するケースはないと思う。

さらに第37条4項で、国内法で要求している場合にはDPOを置かなければならないとされており、ドイツではこれが義務付けられているため、ドイツに拠点がある企業はデータ保護オフィサーを置く必要がある。英国は、BREXITによって将来的にはGDPRはかかってこなくなるが、今の法案では設置義務があるという風に読める。他国について少し調べるてみるとルクセンブルクはないが、ポーランドはあるのではないかと考えられる。実施法については複雑なので、現地に大きな拠点がある場合には、その国の弁護士に確かめるのがよいと思う。

2 EUによる日本の十分性認定と日本側の動き

十分性認定

EUからは、原則的に十分性認定を受けた国にしか個人データを移転できないことが第45条で定められている。さらに第46条で、「標準契約条項（SCC）」や「拘束的企業準則（BCR）」による移転が認められており、それらでは間に合わない場合には第49条の「同意その他の個別的な方法」で対応することになる。米国の「プライバシーシールド」も、この十分性の枠組みになっている。十分性認定は、まだそれほど多くの国で認められているわけではない。

十分な保護措置というのは、米国の「セーフハーバー」が無効になった「マクシミリアン・シュレムス対アイルランド・データプライバシーコミッショナー」の判決の中で判断がなされている。欧州連合基本憲章第7条、8条、第47条の観点からみて、EUの指令で保証されている保護のレベルと実質的に同等である必要があるとされた。

例外事由による移転

企業の皆さんは「標準契約条項（SCC：Standard contractual clauses）」を使って移転の準備をしている場合が多いと思うが、SCCの準拠法は「データ輸出国（Data Exporter）」という表現になっているので、SCCはデータ輸出国の法律で解釈をしなければならない。例えば英国とSCCを結ぶとすると、その準拠法は英国法となり、理論的には英国の契約法を読みチェックをする必要がある。取引先があちこちにある場合、あるいはそれが会社にとって非常に重要性が高い行為であると考えられる場合には、その委任状の代理権授与行為で大丈夫かについて現地で専門家に依頼して調べたほうが良いとは思うし、EU側の提出先はドイツ、フランス、アイルラ

ンドなど何かあった場合に法律を調べやすい国にしておくほうが企業の負担は少ないだろう。

一方、「拘束的企業準則」（BCR：Binding Corporate Rules）の利用状況だが、楽天㈱がルクセンブルクに申請をしてすでに認められている。また、㈱インターネット・イニシアティブは英国に申請し、富士通㈱もオランダに出したようだ。

日本側のガイドライン

十分性認定に基づいて移転をされた場合には、日本法に基づいてそのデータを取り扱えばいいはずだが、そこに上乗せで守るよう要請されるのが、平成30年5月25日までパブリックコメントにかかったガイドライン、「個人情報の保護に関する法律についてのガイドライン（EU域内から十分性認定により移転を受けた個人データの取扱い編）」である。

十分性認定に基づいて移転させる場合には、原則的に欧州と同等だということになるので、GDPR上の義務はなくなるはずである。しかし、昨年の12月にEUと日本の双方は法改正をしないで相互認証をしていくことを合意しており、その結果EUから持ち込まれるデータだけ普通の個人データよりも義務を上乗せして守る仕組みを日本側が定めるという妥結をしたように見える。その結果としてのガイドラインである。

その項目には5項目があり、要配慮個人情報の項目を増やす、保有個人データの6ヶ月をはずす、元の利用目的の範囲内で移転先でも利用目的を定めなければならない、利用目的の記録、外国にある第三者の同意を取る際にインフォームドコンセントを確実にする、匿名加工情報との関係で仮IDを付けた匿名加工情報は認めない、という5つである。

法技術的には、要配慮個人情報が何かについては政令で定めることになっているので、ガイドラインで拡張はできない。ガイドラインの内容をどのように執行するのかという問題がある。何かの条文に引っ掛けて執行するんだと今のところは考えざるを得ないが、行政裁量は非常に広いのでできないことはないと思う。

日本側でもEUの同等性を認定しないと相互認定にならないが、これについては個人情報保護委員会で準備が進んでいる。改正する規則が平成30年個人情報委員会規則第1号として5月9日に施行されており、個人情報の保護に関する法律施行規則の一部を改正し、新たな第11条を加えて、旧11条を11条の2とし、「個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国」を個人情報保護法第24条の規定による個人情報の保護に関する制度を有している外国として個人情報保護委員会が定めるとしている。日本によるEUの同等性認定は、すぐにでもできるように準備がなされている。

マーケティングの関係ではe-プライバシー規則案の行方が気になるところだが、あと1、2年必要となるのではないかという欧州の専門家の声がある。条文案のテキストはしばしば変更されているので、受身で対応をするのであればしばらく様子を見るということになるだろう。

図表5：ガイドラインの内容

EUから十分性認定に基づいて移転した個人データの取扱いに係る規律を定めるガイドライン案

➢ 2017年12月の委員同士の会談において、双方の制度間の関連する相違点に対処するための解決策として、EUから日本へ移転された個人情報に係るガイドラインの策定について合意したことを踏まえ、当該ガイドライン案を作成し、現在意見募集を実施している（募集期間は、平成30年4月25日～5月25日）。

【EUから十分性認定に基づいて移転した個人データのみに適用】

ガイドライン案の項目	現行法令	ガイドライン案の内容	実務への影響
要配慮個人情報の範囲	「性生活」、「性的指向」、「労働組合」に関する情報は、要配慮個人情報に該当しない。	「性生活」、「性的指向」、「労働組合」に関する情報を、要配慮個人情報と同様の取扱いとする。	そもそもこのような情報がEUから移転されてくることは想定されず、影響は大きくない。
開示請求権	６か月以内に消去することとなる個人データについては認められない。	国内法上は、6か月を越えて保有する個人データのみ対象となっているが、６か月以内に消去することとなる個人データも同様に請求に応じることとする。	保有期間にかかわらず請求に応じている企業は多い。 また、そもそも６か月以内に消去することとなる個人データがわざわざEUから移転されてくることは想定しにくい。
利用目的の承継	－	第三者から提供を受ける個人データを、提供元が特定した利用目的の範囲内で、利用することとする。	企業においては当然対応していると想定される。
日本から外国への個人データの再移転	①本人の同意がある場合、 ②移転先のデータ保護が確保されている場合、 ③提供先が個人情報保護委員会が指定した外国に所在する場合に提供可能。	左記②について、提供先の事業者における体制整備を根拠として、外国へ個人データを移転する場合には、契約等により個人情報保護法と同等の保護を確保することとする。	企業においては当然対応していると想定される。
匿名加工情報	加工方法に関する情報が残存している場合でも、安全に分離保管されていれば匿名加工情報として扱われる。	匿名加工情報として扱う場合、加工方法に関する情報を削除することにより、何人にとっても再識別を不可能とする。	仮IDを付与しての時系列分析を行うことはできなくなるが、現時点において、EUから移転した個人データとの混合分析について強いニーズがあるとは考えにくい。

14

出所：IT戦略本部第14回新戦略推進専門調査会・第10回官民データ活用推進基本計画実行委員会合同会議【資料2-2】個人情報保護委員会「国際的な個人データの移転について」（2018年5月11日）より引用

03 Seminars

サイバー空間における警察活動

警察庁 生活安全局 情報技術犯罪対策課
官民連携推進官　高尾 健一

本稿は6月15日に大阪ビジネスパーク・クリスタルタワーにおいて開催された「第47回ICTセミナー」（主催：日本データ通信協会）における警察庁生活安全局情報技術犯罪対策課の高尾健一官民連携推進官の講演内容を編集部においてとりまとめたものである。
サイバー犯罪への対応は、ICTが社会基盤となった私たちの日常生活において、最優先事項のひとつと言ってさしつかえない重要課題である。警察庁では、今日的かつグローバルな課題であるサイバー犯罪への取り組みを、年を追って強化しており、高尾氏の講演は、私どもがその一端を垣間見る貴重な機会となった。

3つの部署でサイバー犯罪に取り組む警察庁

情報技術犯罪対策課は10年ほど前に設置された。警察庁の中では「サイバー課」と呼ばれている。本日は、最近のサイバー犯罪の傾向、その中でもっとも大きい問題である不正送金の現状、さらにサイバー犯罪対策のための官民連携の実態、そしてネット防犯の試みの4点にわたってお話をしたい。

昨今、警察でもサイバーという言葉がよく使われるようになってきたが、サイバーの名の付く犯罪に対する部署も細分化される傾向があり、現在は警察庁の中に3つの部署が存在している。サイバー犯罪対策を担当しているのが、私が所属する情報技術犯罪対策課（サイバー課）、その他サイバー攻撃や情報窃取等に対する対策を行う警備企画課、それに電子機器に残された電磁的記録の解析（デジタル・フォレンジック）を行う、いわゆるサイバー捜査の鑑識を担う情報技術解析課がある。捜査、攻撃対策、鑑識の3つの組織が警察のサイバー対策のために動いていると理解していただきたい。

最近のサイバー犯罪の傾向

まず、近年のサイバー犯罪に関連する相談件数と検挙件数の推移をご覧いただきたい（**図表1、図表2**）。

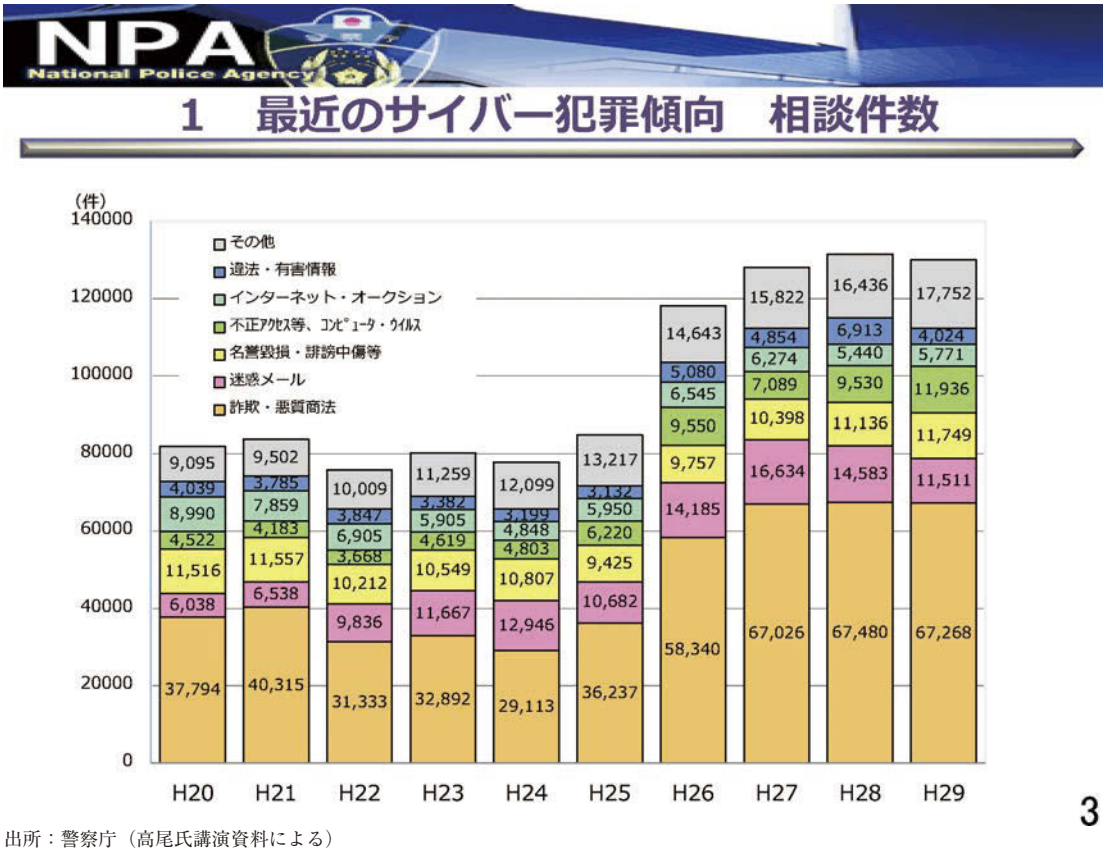
この2つの表から、相談件数は増加しているにもかかわらず、検挙件数は増えていないことがわかる。これについて、我々はサイバー犯罪捜査のキャパシティが限界になっているのではないかと危惧しているところである。

不正送金とその対策

いまサイバー犯罪の中でもっともホットなトピックは何かと言えば、インターネットバンキングの不正送金である。平成27年の被害総額は約30億円に上っていた。私どもでもこれらの被害を防ぐための対策を続けており、その結果、平成28年度は約17億円、平成29年度は10億円と被害額を減少させることに成功している。

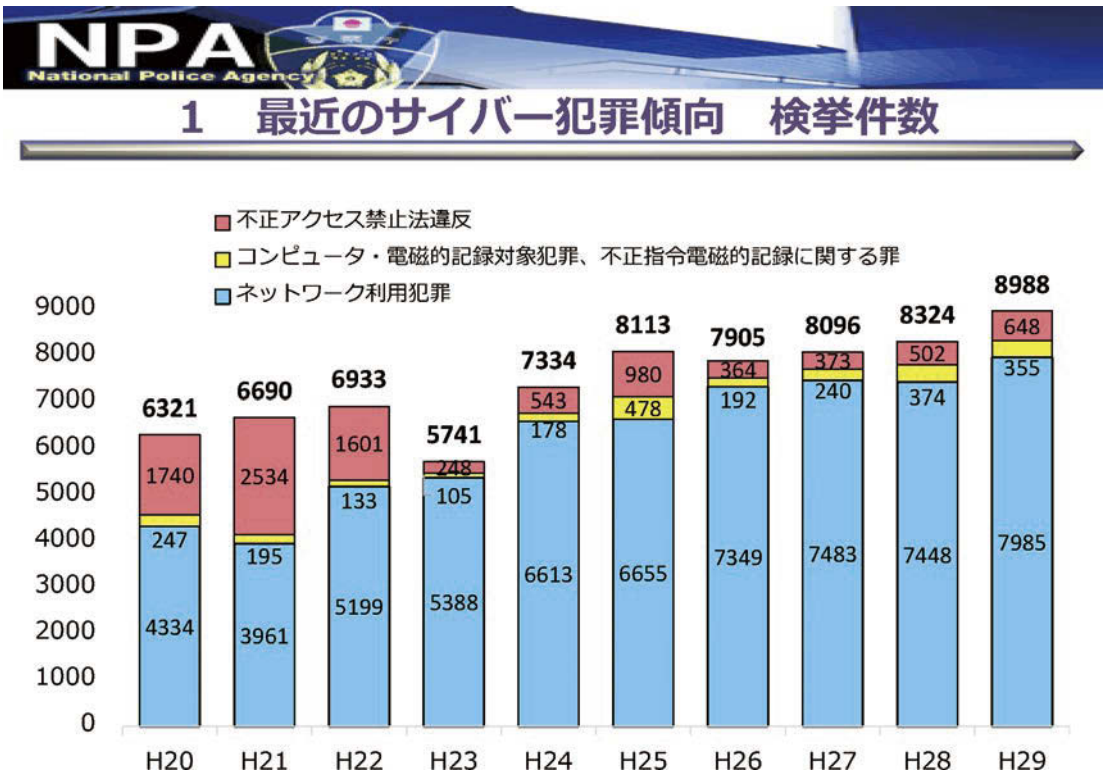
一昨年、昨年と被害額がとくに大きかった原因はウイルス感染によるものである。「至急ご確認ください」という添付ファイル付の電子メールが届き、その添付ファイルを開くとウイルスに感染する、というものがその一例であるが、ウイルスは感染後すぐに動作するわけではなく、例えば、ウイルス感染した端末から、とある銀行のホームページに接続しようとすると動き出す。そして、利用者を偽のホームページに誘導し、IDとパスワードを取ってしまう。そこで金融機関にワンタイムパスワードを採用するという対策等を行っていただき、被害

図表1：サイバー犯罪に関する相談件数の推移



出所：警察庁（高尾氏講演資料による）

図表2：サイバー犯罪に関する検挙件数の推移



出所：警察庁（高尾氏講演資料による）

額はいったん減少した。

その後、犯罪者が編み出した次の手法は「騙しサイト」によるフィッシングである。ウイルスの被害であればアンチウイルスソフトを入れておけば防げる可能性がある。ところが、ウイルスを使わないフィッシングは検知が困難である。例えば、被害者がフィッシングサイトを本物のホームページだと信じてアクセスしてしまったら防ぎようがないのである。警察ではこれらのサイトを発見して潰していく作業を徹底して行った。金融機関のフィッシングサイトが非常に多かったため、金融機関と協力し、フィッシングサイトを発見する方法も共有して排除を行った。

その結果被害は減ったものの、犯罪者たちはまた別の方法を編み出した。IDとパスワードを盗み取って換金性の高い商品を買う手口を用いたのだ。これだと金融機関にお金が送られないので、金融機関が関所として機能しなくなってしまった。例えば5万円のギフトクーポンを100回購入すると500万円になる。そこで、警察はこうした商品を販売している会社への送金を行わないよう、送金を担当する事業者に要請をし、効果を挙げた。

さらに続いたのが自分の身分を明らかにせずに仮想通貨交換業者に口座を作り、当該口座に不正送金を行い仮想通貨に変換して他の仮想通貨口座に送信するという方法である。そこで、あらかじめ登録された入金口座以外からの入金については一定の期間、同等の価値を持つ仮想通貨を含め現金の出金または仮想通貨の送信をできないとする措置を仮想通貨交換業者に取っていただいた。この対策も有効に機能した。

そもそも犯罪者がウイルスを使うか否かで対策は大きく変わる。フィッシングは巧妙で、Webサイトのソース自体は本物と偽物とはまったく変わらない場合が少なくない。そうした例で異なるのはURLだけであり、見破るのは容易ではない。

一方で、メール添付のZIPファイルを開かせる、という方法は、企業内で開くなという教育が普及しているため効果が薄くなっている。以前から「ZIPやPDFは気をつけてください。不用意に開かないでください。」という広報等を行ってきたが、それが効果として表れてきているのだと考えている。

しかし、ウイルスについても安心はできない。現在、不正送金で猛威を振るっているウイルスに「DreamBot」がある。これは通信方式にTorを用いており、またワンタイムパスワードの仕組みすら回避するというものである。こうしたものを自分で防ごうと思っても難しい。警察からも頻繁に情報提供をしているので、それらを見てリスクを減らすようにしていただきたい。

このように山あり谷ありの対応を行いながら、全体的に不正送金の被害額を減しているが、その際、産業界の皆様方の協力が不可欠であったという事実は強調しておきたい。産業界の方々と共に、新しい手口に我々は備えている。

進む官民連携

警察のサイバー犯罪対策能力が飽和している事態にどう向き合えばよいのか。増員は容易ではなく、捜査員の能力を上げる努力はしているものの、一朝一夕に進むものではない。外部からサイバーセキュリティ技術を持った方を採用し、捜査官として育てる制度もあるが、それでも十分な人材を集めるには至っていない。圧倒的にサイバー捜査員の数が少ないのが警察の現状である。そこで取り入れられたのが「官民連携」の推進である。

警察が行っていた仕事の一部あるいは全部を民間と協力してやっていこうという考え方だが、これは警察庁にとって、従来の考え方を180度変えたと言ってよい。持っている情報を民間と共有して、一緒に何かに取り組むという文化は過去の警察にはあまりなかったが、サイバー犯罪の世界では、それではどうしようもないということに気がついたのである。民間の方々と我々の情報を共有し、皆様方のお力を貸していただく、そういう時代に変わったのだと考えている。

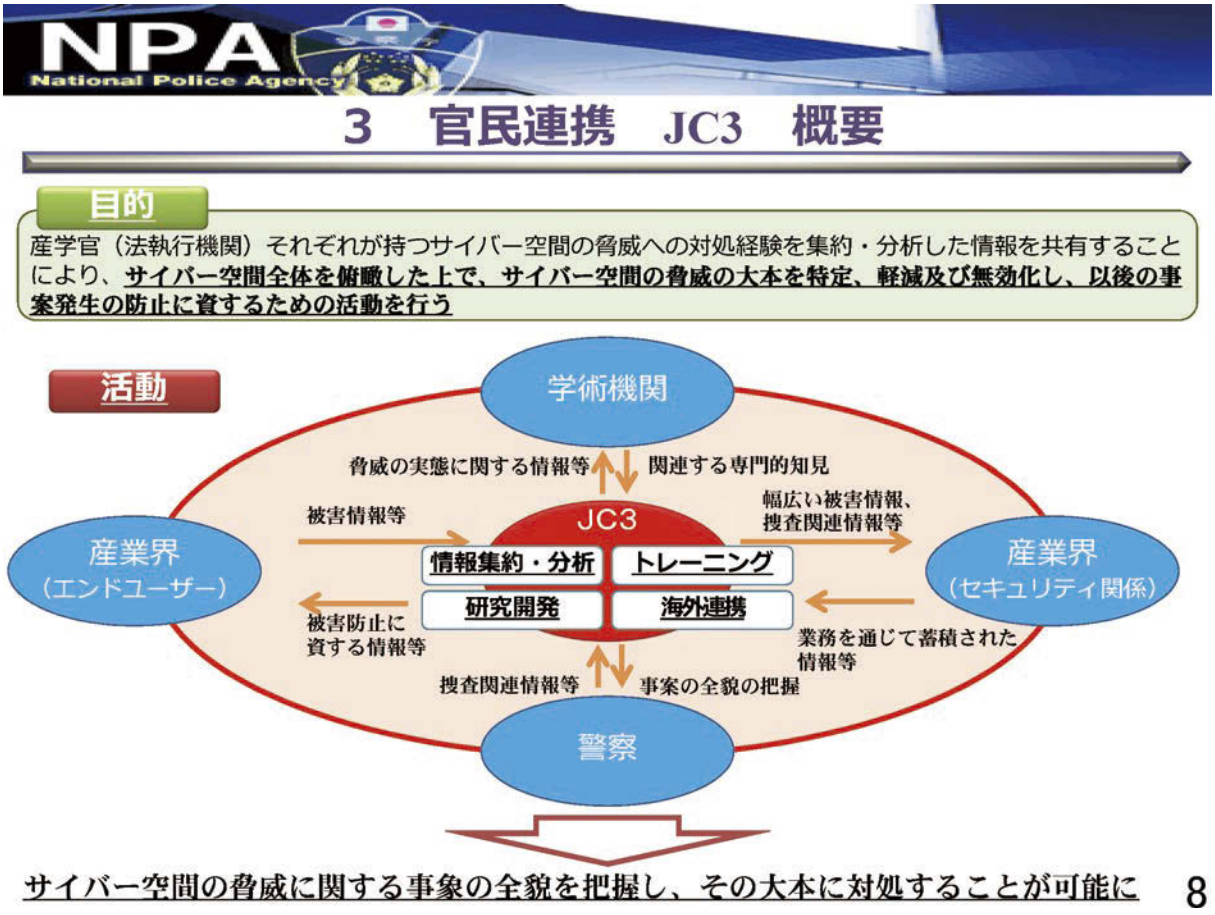
官民連携の要、「JC3」と「IHC」

では皆様方とどのように連携するか。「JC3（Japan Cybercrime Control Center）」という組織を立ち上げ、平成26年11月に業務を開始した。これは平成25年12月10日に閣議決定をした「「世界一安全な日本」創造戦略」に基づいて設立された、警察と民間の方々が同じフロアで協働する組織である。この組織は、米国のピッツバーグにあるNCFTA（National Cyber-Forensic and Training Alliance）という組織を参考にして設立された。

JC3の活動の一例として、詐欺サイトに誘導するフィッシングメールの配信を監視する活動を行っている。この監視結果を警察において速報しているので、ぜひTwitterで警察庁のアカウントをフォローしていただきたい。また、JC3のホームページ内に、PCから訪れていただくと「DreamBot」にPCが感染していないかを判定してくれる仕組みをつくっているので、ぜひ活用していただきたい。

官民連携の2番目の例が「IHC（Internet Hotline Center）」で、インターネット上の違法情報や有害情報を受理し、プロバイダに削除等を依頼する活動である。

図表3：JC3の概要



出所：警察庁（高尾氏講演資料による）

平成28年度には約28万件の通報が来ている。IHCはプロバイダ等に認知されてきており、削除依頼を行うと、H28年度の実績では98%と、かなりの割合で削除が実施されている。

児童ポルノ分野での国際協力

次に、児童ポルノの分野では、国際連携組織である「INHOPE（International Association of Internet Hotlines）」が徹底的な取り締まりを行っている。IHCでは、INHOPEとの間で国際的な情報連携を実施している。

また、この児童ポルノの関連では、日本では「青少年ネット利用環境整備協議会」が平成29年7月に立ち上がっている。これはコミュニティサイトに起因する児童被害を防止しようという目的で設立した組織である。かつて援助交際が社会問題化した際に、出会い系サイト規制法を改正し、出会い系サイトでは身分確認をして18歳以下の者が登録できないように徹底した。その結果出会い系サイトでの被害は減少したが、それに代わってSNS等で被害にあう児童が右肩上がりになってしまっている。これを防ぐために作られたのが「青少年ネット利用環境整備協議会」である。警察は、児童被害に遭う子供たちを救いたいという一心で活動をしている。

ネット防犯に必要とされる様々な対策

日本は日本語で守られているために詐欺サイト被害はまだ限定的と見る向きもあるが、世界的には大きな問題になっている。これに対して「APWG（Anti-Phishing Working Group）」という国際非営利団体が活動している。日本警察も参加し、詐欺サイトを発見するとその情報を提供している。昨年12月には、振込先が日本の口座である詐欺サイトに対する一斉摘発を行った。

詐欺に遭う人は繰り返し遭う傾向がある。どういうことか。例えば、アダルトサイト請求の詐欺等の被害者を狙った消費者被害相談詐欺が存在している。犯罪者は、詐欺の被害者がポータルサイトに「詐欺・被害・取り戻す」などの単語検索を行なったとき、通常の検索結果より上位に表示される広告を出しておく。そして、検索結果の上位にその広告が表示されてしまっているが故にこれをクリックしてしまった被害者を、犯罪者のホームページに誘導する。被害者はそこに書かれた電話番号に電話をしてしまう。すると、犯罪者は「お金を取り戻し

ましょう。最初に手付金を払ってください。」等の言葉を用い、数万円の手数料をだまし取る、という手口である。引っかかったことを隠そうとして、さらにこうした詐欺の被害に遭う方が少なくないのである。

また、「BEC（Business Email Compromise：ビジネスメール詐欺）」は日本でも急速に拡大する傾向があり、実態を知っておく必要がある。多くの場合外国への送金が絡んでおり、英語のコミュニケーションに不得意な場合に引っかかる傾向がある。ぜひ慎重に対応をしていただきたい。

活躍が期待されるサイバー防犯ボランティア

JC3と並んで私どもが官民連携に取り組んでいるのが、「サイバー防犯ボランティア活動」である。町内活動で防犯の取り組みを行うように、サイバー空間でのボランティア活動をお願いするもので、現在、約200団体、約8,600名の方々にご活躍いただいている。ボランティアの皆さんにはサイバー空間をチェックしていただき、何かあればIHCに連絡していただいているほか、小中学校に出向いて教育活動を行うなど、広報活動も行っていただいている。

終わりに

警察ではサイバー犯罪捜査、サイバー攻撃対策捜査、情報解析のそれぞれについて各都道府県警察に設置した警察学校にて教養を行っている。例えば、専門知識を習得する専科の中にサイバー犯罪対策専科を設け、一定数の人材を育成している。また、すべての警察官が受ける教育の中にもサイバー犯罪捜査の科目があり、すべての警察官がサイバー犯罪の基礎について学んでいる。さらに、民間企業やJC3に派遣を行い技術の向上を図ることも行っている。

また、我々は先端の情報通信技術に遭遇したとき、そのような情報通信技術を犯罪者はどのように使用するか、またどうやって捕まえるかに頭を使う、あるいは犯罪者の痕跡がどこに残るかを検討するといった点に注力すべきだろうと考えている。

サイバー技術を使って世の中が豊かになるのは我々の願いである。一方で、インフラストラクチャを安全にしていかなければ、産業も成立していかない。そのために我々も日夜努力しているので、ぜひ産業界の皆様のご協力をお願いしたい。

04 challenge！ 工事担任者試験に挑む若者たち

情報通信産業を支える人材育成を目指して

金沢市立工業高等学校
電子情報科　教諭　中野 克也

学校紹介

本校は、今年で創立90周年を迎える金沢市が設置する唯一の高校です。教育目標として、「高い教養と優れた技能を　責任ある言動と協調の精神を　勤労の喜びと健全な心身を」掲げ、「ものづくり」の感性と工業の基礎・基本を身に付けた地域産業の期待に応える人材を育成し、創立以来、20,000人を超える卒業生を社会へ輩出しています。

幾多の学科改編を繰り返しながら、現在は5科（機械、電気、電子情報、建築、土木）があり、生徒数は717名（平成30年4月現在）です。進路は、就職が6割、進学が4割です。

運動部活動も盛んで、水球部のインターハイ2連覇を始め、相撲、バドミントン、剣道、弓道が全国大会へ出場しています。

工事担任者試験への取り組み

本校では、全生徒に資格カレンダーを配布し、各資格試験や検定試験の受験を積極的に奨励しています。また3年次には、全国工業高等学校長協会が認定するジュニアマイスターの取得を目指して、在学中ひとつでも多くの資格を取得することができるよう推奨し指導しています。

さて、標記にもあります工事担任者DD3種試験への取組ですが、電子情報科の2・3年生の希望者が積極的に受験しています。合格すると本科では専門科目「電子技術」の増加単位になります。したがって「電子技術」の授業で、試験に出題されるような通信技術の基礎理論を学習しています。その他、本科では技能検定3級電子機器組立てを資格取得の大きな柱としています。それら以外に、ITパスポート、第2種電気工事士など、電子、電気、通信、情報の分野を幅広くカバーし卒業後、即戦力に繋がるように資格指導を行っています。具体的な資格取得の流れは、次のとおりです。

(1)　第1学年

ア．６月　計算技術検定3級
イ．７月　技能検定3級電子機器組立て
ウ．１月　情報技術検定2・3級C言語

(2)　第2学年

ア．10月　第2種電気工事士
イ．11月　工事担任者DD3種
　科目「電子技術」「電子回路」「電気基礎」で、基礎関連の学習をします。
　「実践問題集」で、受験者は法規と技術を各自で学習します。
　過去4回分の問題を渡し、過去問題で試験対策をします。
ウ．随時、ITパスポート

(3)　第3学年

ア．4月　基本情報技術者
イ．随時、ITパスポート
ウ．5月　工事担任者DD3種、秋にDD3種合格者は総合種を受験

3年次に科目「電子技術」「電子回路」「電気基礎」があり、クラス全体で基礎関連の学習をします。また、「実践問題集」で受験者は法規と技術を各自で学習します。さらに、過去4回分の問題を渡し、過去問題で試験

対策をします。特に、通信ネットワーク関連企業への就職希望者は、総合種の取得を推奨しています。

電子情報科教員は、工事担任者をはじめ各資格・検定が、生徒の将来や進路に役立つように合格を願いながら、日々指導にあたっています。

最後に、ここ近年、受験希望者が減少傾向にありますす。しかし、インターネットやスマートフォンなど情報通信が急速に普及した現在の社会において、今後さらに情報通信の設備や社会基盤の整備が必須になってくると考えられます。したがって工事担任者の資格や、通信技術に関する知識・技能はますます必要になってきます。その必要性を生徒たちに認識させ、情報化社会で即戦力となる技術者を育成していきたいです。

合格者の声

電子情報科　３年
桑原　誓

私がDD3種を受験しようと思ったきっかけは、就職希望先が情報通信関係だからです。昨夏、地元の情報通信関連の企業で就業体験をさせていただく機会があり、学校で学習した専門科目「電子技術」や「情報技術基礎」などの内容が役に立ったからです。そしてより一層、情報や通信関連に関する知識や技術を習得したいと思うようになりました。

実際に、DD3種の勉強は、試験の約1ヶ月前から真剣に取り組み始めました。参考書として、リックテレコムの「工事担任者DD3種標準テキスト」を活用しました。このテキストを毎日読み続け、残り一週間は過去問を解き続けました。一ヶ月頑張って合格できたので、うれしかったです。次は、AI・DD総合種受験するので、合格目指して頑張ります。

電子情報科　３年
服部　仁哉

私がDD3種を受験した理由は、2年次の夏休みに就業体験があり、通信関係の会社に行きました。そこで授業で学習したような情報関係や通信関係の実物や聞いた用語などが、たくさん出てきたり、触れる機会がありました。これまで学校で勉強してきましたが、さらに知識や技能を高めたいと思いました。実際の試験対策では、基礎の計算、論理回路などの既習事項は、軽い復習程度で済みました。それ以外は未習事項が多く、覚えなければできない問題がたくさんあり難しかったです。参考書を基本にわからないことは繰り返し学習するよう努めました。また最後は、過去問題を何度も繰り返し解くことで、合格へ辿りつくことができました。

05 トラストサービスの担い手

連載企画
第5回

“電子作業場”で契約書業務を効率化する『Holmes』

株式会社リグシー
代表取締役 CEO
笹原 健太

契約書の作成・管理に的を絞ったクラウドサービス『Holmes（ホームズ）』で俄然ビジネス界の注目を浴びている企業が株式会社リグシーである。法務系の人材が乏しい中小企業から契約業務効率化の可能性に気がついた大企業まで、その顧客層は急速に広がりつつある。電子契約の普及を見据え、タイムスタンプも備えた同サービスの現在を、昨年までは弁護士としても活動していた代表取締役 CEO の笹原健太氏に伺った。

「世の中から紛争裁判をなくす」という志が起業につながった

笹原氏は、2017年3月に株式会社リグシーを設立し、8月に契約書作成・クラウド締結サービス『Holmes』を開始するまで、弁護士として顧客企業の裁判を多く担当してきた。その体験から、裁判に勝つよりも紛争そのものが起きないようにすることが重要だと考えるに至った。そして、契約書がしっかりと締結されていないという現実に注目した。

「裁判が何故起こるのかを考えてみると、取引関係の裁判では契約書の不備が大きく関わっています。契約書がないことがままあるし、口約束で行われている実態と契約書の内容とが合致していないことがあります。契約書さえきちんとしていれば、こんな紛争は起きなかったと思うケースが私の体感では8割ぐらいはありました」（笹原氏）

その実感から導かれた最終的な解は、簡単に契約書を作れるシステムの提供だった。

契約書を作成する面倒を解消する

笹原氏が『Holmes』を立ち上げた際のビジョンは「契約書をつくらない理由をなくす」である。

「契約書が整備されていない理由は色々とありますが、そういった企業にとっては、ともかく契約書を作成するのは面倒なんです」と考えた笹原氏は、その“面倒”を解消するために、『Holmes』に数多くのテンプレートを用意し、法律の専門家に依頼しなくても画面上で契約書が簡単に作成できるように工夫した。テンプレートは自社に合わせて容易に修正ができる。条項を足したり、削除したりした際に生じる条ズレなども自動的に修正されるなど､作成の手間を削減する様々な工夫がなされている。

契約にまつわるコミュニケーションのコストを削減

しかし、笹原氏の話を聞き続けると、サービスの付加価値は作成時にだけあるわけではなく、作成後の承認や管理を含めた契約書のライフサイクル全体に及んでいることが分かってくる。

「100人以上の企業だと特に顕著なのですが、我が国では契約を取った後の社内承認フローが長くて、契約書が出来るまでに1ヶ月、2ヶ月とかかる場合が少なくありません」と笹原氏は言う。そして、その観察を基に、解決すべき課題が社内コミュニケーションにあることを突き

止める。顧客と現場と管理部門、さらには顧問弁護士の存在など何層にも重なる関係者の存在が手間と時間とを要求する。そして契約締結後には、契約条件の確認や見直し時に過去の承認履歴を確認する必要が出てくるが、そこにかかる稼働は思いのほか大きい。

「私は、これを社内コミュニケーションの問題だと考えました。何故コミュニケーションの問題が起こるかと言えば、顧客と複数の社内部門とのやりとりがあり、場合によってはそこに顧問弁護士が加わるなど煩雑なやり取りが発生するからです。これが1つめの課題設定です。

2つ目の課題に、そもそも契約書や関連書類を探すのが大変だということがあります。例えばある上司から「A社さんとの契約書はどこにある？」と尋ねられた管理部門では、契約書をファイルの山から探すのに手間がかかることが少なくありません。さらに「ここの条件はなんでこうなっているんだっけ？」などと訊かれ、慌てて過去の書類や電子メールなどに一所懸命に当たるということが起こっています。契約書と契約に関する情報の管理が一元化されていないということです。」（笹原氏）

『Holmes』は数々の手間を解消する「デジタル・ワークプレイス」

こうした課題を解決するために『Holmes』では、いくつもの機能を装備しているが、この時笹原氏が『Holmes』を「デジタル・ワークプレイス」と呼び、契約書に関する作業場だと捉えることによって筋の通ったストーリーが生まれている。

この「場所」では契約書の作成と承認が行えると同時に、契約書の原本ないしそのコピーに常にアクセスでき、承認過程での関係者のコメントがすべて記録されている。アクセスはURLで一本化されており、関係者はこのURLを知ることによって、その契約にまつわる過去と現在のすべてを簡単に知ることができる。煩雑な業務が一挙に簡素化されるのである。

「“レビュー”という機能があって、例えば作成者が上司に対して契約書のサマリーを知らせたり、コメントしたりすることができます。上司はだいたいサマリーしか見ませんから（笑）。上司がそれに対してコメントをすると、それが履歴として残ります。一つのURLを共有するだけでそれらのやりとりができてしまい、添付ファイルを送るなどの手間がいりません。契約書自体とサマリーを別個に送る必要がないのも利点です。上司はURLを開けば、「ワークプレイス」上でその契約に関わるすべての情報が一覧でき、誰がコメントをし、誰が承認をしたかも記録が残ります。」（笹原氏）

ワークフローやワークプレイスの電子化が電子契約のニーズを顕在化する

『Holmes』では電子契約にも対応しており、システム上で契約書の締結を行うことができる。紙にも電子にも顧客の要望に応じて自由に対応が可能な仕組みが用意されている。締結の際にはタイムスタンプが押され、改ざんのリスクに対応している。タイムスタンプの料金は最初からサービスに含まれているため、面倒な契約手続は発生しない。契約業務の電子化への対応について笹原氏は述べる。

「電子契約は取引相手がいることなので紙での契約がまだ主流ですが、あらゆるモノが電子化していますから、契約書にも電子化の流れは確実に来るはずです。まずは「管理部門の課題解決を目的に使い始めた『Holmes』で電子契約が出来るらしい」となるのが自然な成り行きではないかと思います」

電子的なワークフローや、『Holmes』のようなワークプレイスが普及すれば、自ずから契約業務も電子化への道を歩み始める。その時にタイムスタンプが有用なのは火を見るより明らかである。

「導入していただいている企業としては上場企業も多く、サイバーエージェント系の会社にもかなりお使い頂いていますが、業種ではとくに大きな偏りはありません。それよりも、会社規模で、100人以上の企業で興味を持たれる場合が多いのが特徴です。もちろん、社長さんが自ら契約書を作成しているような中小のお客様からも多くお使いいただいているのですが、従業員が100人を超える企業では、契約業務量が飛躍的に増えて、契約に対する課題観が大きくなってきます。なんとか効率化を進めたいと考えている企業様からメディアで記事を読んでお問い合わせをいただくケースが増えています。当事者である管理部門から声が上がっているのは、当社としては嬉しいかぎりです。」（笹原氏）

『Holmes』は、新規サービス開発の一部分をタイムスタンプの機能が後ろで支えている例である。こうした新しい取組みをタイムビジネスを含めたトラストサービスが後押しする事例が今後も登場することを願いたい。

企業プロフィール

LegSea

会　社　名　：株式会社リグシー
本社所在地　：東京都千代田区大手町 1 丁目 6?1
代　表　者　：代表取締役　笹原 健太
設　　立　：2017 年 3 月 31 日
ホームページ：https://www.holmes-cloud.com

※連載企画「タイムビジネスの担い手」は、タイムビジネス協議会の改組によるトラストサービス推進フォーラム（TSF）の設立に伴い、本号より「トラストサービスの担い手」にタイトルを変更します。

06 Pマーク取得事業者の横顔

日本レコードセンター株式会社

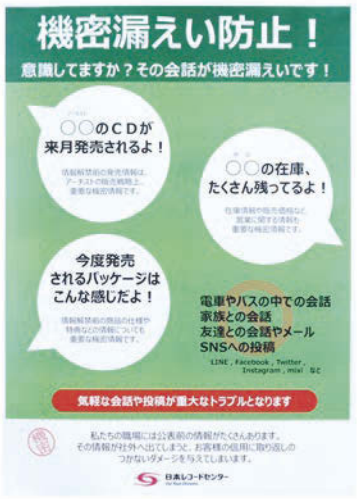
日本レコードセンター株式会社
執行役員人事総務部長
菅野 一郎

物流の規模はGDPの大きさと高い相関があると言われており、情報通信産業などとともに一国の経済活動を支える基幹産業である。今回登場いただいた日本レコードセンター㈱は、物流の中でも音楽、映画、ゲームなどのパッケージを専門に取り扱う会社として40年の社歴を誇っており、この分野では高い競争力を有するサードパーティ・ロジスティクス事業者として確固とした地位を築いている。

――貴社の業務について教えて下さい。

当社は、ビクター音楽産業（現ビクターエンタテインメント）の子会社として、レコードメーカー各社と共同で音楽パッケージソフトの受注・出荷・配送を行う物流に特化した業務を行うことを目的に、1978年3月、神奈川県厚木市に設立されました。

設立当初は、アナログレコード、VHSビデオ、ミュージックテープ（カセット、8トラック）が主でしたが、現在は、CD、DVD、カセットテープ、ゲーム（ハード、ソフト）、ポスターやアーティストのグッズ等を取り扱っています。



2011年4月からは、SBSロジコムの子会社となり、総合物流会社であるSBSグループの一員として、音楽パッケージソフト物流一筋で創立40周年を迎えました。

音楽ソフトパッケージの物流は、創業時期から変わらないサービスレベルを維持しています。それは、今日のお昼（12時）までに頂いた注文であれば、CDを1枚からでも全国のお店に翌日配送（離島除く）するというものです。

この様なサービスレベルを提供し続けるには、物量変化に即応しつつ高品質の作業レベルを維持できるマンパワーマネジメント力、全国を網羅する独自の配送網、物流工程だけでなくレコードメーカー各社との情報連携から販売店様の業務まで自社開発が可能な情報システム力を駆使した精度の高い物流オペレーションが必要となり、これが当社の強みとなっています。

――組織としてはどのような特徴がありますか？

従業員数は約750名で、そのうち約450名は短時間のパートタイマーです。これらの方々は当社の出荷作業の重要な担い手となっています。そこで、パートタイマーの皆さんには、子育てや介護といったご家庭の都合に合わせて、比較的自由に勤務日、時間等を決めることができるようにしています。

貴重な戦力となるパートタイマーの方々を採用するために、労働条件以外にもいろいろな取り組みをしています。社内向けには、夏休みにパートタイマーの子どもさんやお孫さんたちを対象に絵手紙教室を開き、夏休みの自由研究の手助けをしています。絵手紙教室終了後には、お母さん、おばあちゃんの働く様子を見学するツ

アーも実施しており、好評をいただいています。

また、近隣自治会を通じて、健康増進のために、パワーウォーキング講習会や未病サポーター養成研修等を開催し、毎回多くの近隣住民の方々に参加いただいています。

これらの活動は、創業以来厚木市で事業活動を続けている当社として、地域との共生が一番重要であると考え、従業員を含めた地域の皆様に当社を少しでも理解して頂けるよう努力しています。

――Pマークを取得しようと考えたのは何故ですか？

当社の業務は永くCDショップ等の店舗向け配送が主であったため、取扱う個人情報はそう多いものではありませんでした。しかし、2015年5月より一般消費者向け通販を含む物流業務を受託することになりました。そこで、荷主様に安心して仕事を任せていただけるように、しっかりした個人情報管理体制を構築する必要があると思い、認知度の高いプライバシーマークの取得に取り組みました。

個人情報にはマイナンバー等も追加され、今まで以上に管理をしっかり行っていかなければならず、プライバシーマークがあることで、従業員の個人情報管理に対する意識がさらに高まっていると思います。

――仕組みを整備する上で難しかったこと、力を入れたことは何ですか？

最初に取り組んだのは、「個人情報保護マネジメントシステム（略称PMS）」を整備し運用して行く上で重要となる、運用組織を明確に定めることでした。事務局だけで整備ができるわけではありませんので、仲間を増やす目的で、職制に合わせ各部単位で責任者、推進者を任命し、会社を上げてPMS整備に取り組む体制を構築しました。

運用面では、部署ごとのPMS運用状況をチェックするため、共通チェック項目と、部署ごとの特性を考慮したチェック項目を合わせた、運用確認チェックリストを作成し運用しました。これにより、各部署での個人情報管理に対する意識を高めて行くことができました。

――審査を通じて感じたことを教えて下さい。

今年2月の最初の更新審査を終えて感じたことは、個人情報管理台帳を作成し管理する重要性です。個人情報は個人情報管理台帳を用いて特定をしますが、特定した個人情報の流れが正確に記載されていない箇所がありました。原因は、各部署で記載する担当者が、様式の記入要領を十分に理解していないためでした。

個人情報を取扱う作業については、従業員に対して教育を実施してきましたが、PMSの運用に関して、特に用途に応じて作成した様式について、その様式の持つ意味と記入要領についての教育が十分では無かったと痛感しました。

また、新たに事務局に加わったメンバーのPMSの理解度も十分とはいえませんでしたので、日本データ通信協会様の研修や個別相談等を積極的に活用して、全体の管理レベルを向上させる必要があると感じています。

――今後の取り組みについて教えて下さい。

CDショップ向けの配送が減少傾向にある中、一般消費者向けの配送が増加しています。一般消費者向けは、配送ミス＝個人情報漏洩となってしまうので、配送ミスを起こさない作業手順の確立と定着が重要なポイントとなります。単純に生産性を追求するのではなく、個人情報保護という品質を追求して行けるように、管理監督者への教育を進めて行きます。

もう一つは、新たな荷主様が増えることで取り扱う個人情報の件数が増えますので、新規の個人情報取得からリスク分析までをしっかり行い、PMS運用を行うことが荷主様の信頼を得る近道であると思っています。

企業プロフィール

日本レコードセンター
For Your Dreams.

会　社　名　：日本レコードセンター株式会社
本社所在地　：神奈川県厚木市三田 47-3
代　表　者　：代表取締役　菊地 和彦
設　　立　：1978 年 3 月 21 日
ホームページ：http://www.nrc-jpn.net/

編集後記

本号の特集は「JIS Q 15001」改正です。プライバシーマークの審査基準である「JIS Q 15001」の改正は、私どもの審査業務にとっても一大事なのですが、それ以上に実際にプライバシーマークを取得している事業者の皆様にとっては十分な理解と、それに基づくしっかりとした対応が必要になっています。特集では、この分野での経験豊かな3人の著者を得て、実務家にとって有益な情報を提供できたのではないかと考えています。

さらに本号では「GDPR」に関する板倉陽一郎弁護士の講演を紹介しています。これも情報通信分野で事業を営む企業様にとって、第一人者による貴重な情報です。

なお、私ども日本データ通信協会では、6月5日に「タイムビジネス協議会」を改組し、「トラストサービス推進フォーラム（TSF)」を設立しました。タイムビジネスのみならず、電子署名やeシールなど、より幅広い技術やサービスを視野に入れながら、私たちが活用するサービスの信頼性を高める「信頼基盤」を構築していこうという試みです。これを受けて、好表裏に連載を行ってきた「タイムビジネスの担い手たち」は、本号より「トラストサービスの担い手たち」とタイトルを新たに継続していくことにしました。「信頼」を重視してサービスを提供する様々な事業者、「信頼」のためにサービスを提供する様々な事業者を紹介していきます。（中山）

日本データ通信　【通巻219号】

発行所：一般財団法人日本データ通信協会
発行人：高嶋　幹夫

平成30年7月発行
〒170-8585　東京都豊島区巣鴨２-11-１　巣鴨室町ビル６F・７F
TEL：03-5907-5139
HP:https://www.dekyo.or.jp

JADAC

国家試験 電気通信設備 工事担任者試験

平成30年度 第1回 試験実施日

平成30年5月27日(日)

申請受付期間

申請区分	申請内容	申請受付期間	試験手数料払込期間
インターネット申請	実務経歴の申請がない場合	平成30年2月1日(木)～3月7日(水)	平成30年3月8日(木)まで
郵送申請	実務経歴の申請がない場合	平成30年2月1日(木)～3月7日(水)	
	実務経歴の申請がある場合	平成30年2月1日(木)～2月20日(火)	

合否発表 平成30年6月18日(月)

平成30年度 第2回 試験実施日

平成30年11月25日(日)

申請受付期間

申請区分	申請内容	申請受付期間	試験手数料払込期間
インターネット申請	実務経歴の申請がない場合	平成30年8月1日(水)～9月5日(水)	平成30年9月6日(木)まで
郵送申請	実務経歴の申請がない場合	平成30年8月1日(水)～9月5日(水)	
	実務経歴の申請がある場合	平成30年8月1日(水)～8月20日(月)	

合否発表 平成30年12月17日(月)

試験実施地 全国37ヶ所を予定
(注)平成30年度から「富山」及び「大分」の2試験地での試験は実施いたしません。

科目免除 科目合格者、一定の資格又は実務経歴等を有する者及び認定学校の単位修得者等は、申請により試験が免除される科目があります。

試験種別 AI･DD総合種　DD第一種～第三種
AI第一種～第三種

試験手数料 8,700円(全科目免除5,600円)

試験に関する重要事項は当協会から配布する、「試験実施要領」、「受験の手引き」、または下記協会ホームページでご確認ください。

申請書の請求、試験に関してのお問い合わせは
一般財団法人 日本データ通信協会 電気通信国家試験センター
〒170-8585 東京都豊島区巣鴨2-11-1 巣鴨室町ビル6F TEL 03-5907-6556 FAX 03-5974-0096
ホームページ http://www.shiken.dekyo.or.jp/ メールアドレス shiken@dekyo.or.jp

情報通信の現在、そして未来のために

一般財団法人

日本データ通信協会

Japan Data Communications Association