# 日本データ通信

ISSN 0386-7889
No.214
2017.3
March

interview　ベネッセインフォシェル 代表取締役社長　丸山 司郎 氏インタビュー
**基本に忠実に、そして矛盾を減らしていくことが重要です**

special issue
**❶ プライバシー影響評価（PIA）の海外動向と日本への応用**
**❷ Pマーク審査の現場から（リスク分析）**

info
**平成28年度 電気通信主任技術者定期講習を終えて**

topics
**インターネットの安心･安全に関する動画フェスタin近畿2016の実施**

challenge　福井県立 奥越明成高等学校
**国家試験「工事担任者試験」に向けての取り組み**

trend
**大学入試改革とICT**

column
**Pマークの事故増加は由々しきことなれど**

JADAC
Japan Data Communications Association

# CONTENTS

2017.3 March No.214

# 情報セキュリティのリスク評価

一般財団法人日本データ通信協会　理事長　**酒井 善則**

情報セキュリティを専門としている方から、一部の企業はセキュリティに費用をかけたがらないという話をしばしば聞く。個人情報漏えい等の事件があるため、情報セキュリティの重要さは理解しているものの、いくら費用をかけたらよいか目安がない。火災、自動車事故等のリスクについては、リスクが現実となった場合の損害、リスク軽減のためにかかる費用、保険制度、保険料等を検討してリスク管理を行っている。保険会社も、統計的手法により保険料設定を行っていると思われる。近年は情報セキュリティ被害が多いためその分析はかなり進んでおり、サイバーリスクに対する保険もできている。

近年、セキュリティ対策の経済学からの評価も研究されており、経済的に最適なセキュリティ対策を見出す手法が提案されている。ただ情報セキュリティの場合、損害額の定量化は難しく、かつ対策を行っても攻撃側は新しい攻撃を考えるため、対策の効果が長続きしない。住宅の火災保険は住宅再建築のための費用をほぼ全額負担するようになってきており、その保険料は住宅の構造によって異なる。従って、個人は住宅の構造にかける費用とそれによる保険料の低下等をもとに、少なくとも金銭面のリスクマネージメントが可能となる。ただ情報セキュリティに関する被害は、それによる社会の被害額と企業が負担すべき損害額が必ずしも一致しない。迷惑メールハンドブックによると迷惑メールによる被害総額は年間7,300億円と推定されているが、この額は社会としての損失額で、企業が負担することになる損害額とは異なる。一方、JNSA資料※によると我が国における個人情報漏えい案件での年間損害賠償総額は2,500億円位とのことであり、この額は明確に企業の負担する損害額である。

保険会社の決算をみると保険会社の保険料収入は、支払い保険金総額より大きく、概ね2倍以下程度である。これを1.5倍とすると、企業の情報セキュリティ関係損害を完全に保証できる保険があるとすると、日本における損害額の1.5倍程度が利用者の支払い保険料の総額でよいのかもしれない。このため、仮に情報漏えいに関して保険で損害額を補填すると考えると、保険料総額は4,000億円位と想像される。同様に、迷惑メールによる被害総額を保険で全部補填する場合は、1兆円以上が保険料総額になる。

セキュリティの被害総額は今後増大するものと予想される。セキュリティ保険がある場合は、保険の支払い保険金総額、更には限度額も増加するかもしれない。火災保険、自動車保険では住宅の構造、あるいは運転者の能力が保険料に反映する。同様に、セキュリティ対策の完全さ、セキュリティ対策にかけたコストが保険料にも反映するはずである。セキュリティポリシー、対策としてのマニュアルは多くの組織で作成するようになっている。Pマーク、迷惑メール防止などの活動を通して、保険業界などとも連携して、セキュリティ対策の効果を定量的に求めることも協会の役割ではないかと考えている。

※　特定非営利活動法人日本ネットワークセキュリティ協会「2015年情報セキュリティインシデントに関する調査報告書」

インタビュー

# 基本に忠実に、そして矛盾を減らしていくことが重要です

## ベネッセインフォシェル 代表取締役社長　丸山 司郎 氏インタビュー

●株式会社ベネッセインフォシェル
代表取締役社長
丸山（まるやま） 司郎（しろう）

《プロフィール》
【職歴】
昭和62年1月　(旧)(株)ラック入社
平成19年7月　内閣官房情報セキュリティセンター出向
平成24年7月　(株)ラック　執行役員
セキュリティ事業本部副本部長　兼JSOC事業部長
平成25年4月　同社　常務執行役員
セキュリティ事業本部長　兼JSOC事業部長
平成25年6月　Cyber Security LAC(韓国子会社)取締役
平成27年4月　(株)ラック　常務執行役員　サイバーセキュリティ本部長
平成28年6月　現職

【聞き手】

●一般財団法人日本データ通信協会
専務理事
井手（いで） 康彦（やすひこ）

セキュリティに対する備えはあらゆる組織にとって基本的な課題ですが、何を、どのようにやれば十分な対応ができるのかを理解している経営者は限られているのではないでしょうか。セキュリティベンダーの老舗的存在である㈱ラックでセキュリティ事業の責任者を努め、内閣官房情報セキュリティセンターに勤務経験もある株式会社ベネッセインフォシェル 代表取締役社長の丸山司郎氏は、こうしたお話を伺うには最適の存在です。業務のお忙しい合間を縫って、同社東京支社に同氏を訪ね、様々な気づきを語って頂きました。

**井手**　今日は㈱ベネッセインフォシェルの丸山社長に、企業のセキュリティをめぐる課題と、それらの課題にどのように対処すべきか、というテーマでお話を伺います。

**丸山**　よろしくお願いします。まず、ベネッセグループの紹介からさせていただきます。ベネッセグループには「国内教育」、「海外事業」、「介護・保育」、「語学」の4つのカンパニーと「その他」の事業領域があります。

「国内教育カンパニー」は、通信教育事業や、学校向け教育事業があり、グループ全体の売上のほぼ半分を占めています。「進研ゼミ」「こどもちゃれんじ」は、会員数243万人（2016年4月）を擁していますので、日本の教育の一端を担うという意味で企業としての社会的責任が大きい分野であると考えています。

「海外事業カンパニー」では、中国で積極的に事業を進めており、「こどもちゃれんじ」は、上海を中心に125万の会員がいて、417ヶ所（2016年9月末）でショップを運営しています。幼児向け通信教育では同国において圧倒的なトップ企業の地位にあります。

「介護・保育カンパニー」は、㈱ベネッセスタイルケアが担っています。国内3大介護・保育事業者の一

つで、高齢者向けホームでは、「アリア」、「くらら」、「グラニー＆グランダ」をはじめとする７つのシリーズを運営しています。規模は15年で約３倍、近年も年10％程度の規模で成長しており、平成28年中に300施設を超える予定です。ビジネスとしては必ずしも容易ではない分野ですが、施設の入居率は92％（2016年９月末）に上り、事業規模の大きい有料老人ホーム事業者の中では唯一黒字で運用ができています。

最後に「語学カンパニー」は、語学教育のベルリッツの事業があります。ベルリッツは語学学校としては世界最古の歴史を誇り、欧米、アジアを含めて世界70以上の国と地域に500を超える拠点を持っています。

## ベネッセの情報システムを支えるベネッセインフォシェル

**丸山**　当社自身は、ベネッセグループの中にある42の連結子会社で唯一、ITを業務として担っている企業で、教育事業を行っているベネッセコーポレーションのデータ運用を行っています。ベネッセインフォシェルという社名は親会社のベネッセにインフォメーションのインフォ、外皮、甲殻、貝殻などを意味するシェルを組み合わせ、ベネッセがお預かりしているお客様の情報をシェルでしっかりと守るという意味をもたせています。

当社はベネッセのお客様情報漏えい事故を機にベネッセホールディングスに設置された情報セキュリティ監視委員会の提言を受け、㈱ベネッセホールディングスが70％、㈱ラックが30％の持株比率で2015年１月15日に設立されました。基本的には情報システムの保守・運用を行う会社ですが、それだけではなく、お客様であるベネッセコーポレーションにITを分かりやすく、安心して使ってもらえるようにすることを目指しています。

組織は３つの本部と監査部門から成り立っています。特徴的なのが監査部門で、ここが業務監査と情報セキュリティ監査を担当しています。この規模の会社としては体制を強化し、かなり厳格な日々のチェックや運用確認を行っています。各本部が行っている仕事をしっかりとチェックするという姿勢を組織として明確にしており、ここに当社の大きな特徴があります。

また、お客様の個人情報については従来以上に厳格に行っています。私たちの感覚では、銀行における預金情報の管理と同等のレベルの管理を個人情報について行っていると認識しています。

**井手**　銀行と同等以上というのはどういう意味ですか？

**丸山**　金融機関の基幹システムは、金融情報システムセンター（FISC）のルールによって厳格な対応を求められています。基本的に外部とつながるネットワークとは分離されてインターネットとはつながらないようにしていますし、人の出入りも厳密に管理していますが、私どもでも同じような管理を行っているという意味です。

**井手**　以前ある銀行で、端末のIDとパスワードを取得した者が本人になりすまして個人情報にアクセスした事故がありましたよね。

**丸山**　当社では、個人情報にアクセスできるのは執務室内でも限定されたエリアの中だけです。そして、そこに入れるのはあらかじめID管理された社員だけですし、入る際にはいくつものセキュリティ施策をパスしなければなりません。

**井手**　監視カメラはもちろん作動している。

**丸山**　はい、それは言うまでもありません。一般的にできることはすべてやっているとお考えいただいて結構です。

## プロ化するサイバー攻撃

**井手**　さて、今日は丸山社長に、ユーザー企業がセキュリティ対策を行う上でどのようなことに気をつけていく必要があるかを教えていただきたいと考えています。

**丸山**　具体的な事例については話をすることができませんので、大きな方向についてお話をしたいのですが、現在セキュリティの分野で起こっていることについては、大きく分けて３つの観点で思うところがあります。

一つ目は「攻撃の高度化、プロ化」の進行です。サイバー攻撃の高度化については一般紙にもニュースが載るようになっているぐらいですが、攻撃を表す単語も新しいものがどんどん出てきています。マルウェアに

感染したシステムに利用者がアクセスできないようにし、それを解除するために身代金を要求するランサムウェア、大量のIoTデバイスを乗っ取って行う大規模なDDoS攻撃、それにスノーデン事件のような情報暴露もあります。

新しいところでは「BEC」というのがあって、まだ日本ではあまり知られていないと思うのですが、「Business E-mail Compromise（ビジネス電子メール詐欺）」の略です。これは何かというと、攻撃者が企業の経理担当者のPCに侵入して密かにメールを読み続けるんです。そして月末になってその企業に取引先から振込み依頼のメールが来ると、それを読んだ攻撃者がすかさず取引先をかたったメールを経理担当者に送り「ごめんなさい、先ほどの口座は間違いで、こちらの口座に振り込んでください」と偽の口座を伝え、振込みをさせる。実はそれは外国にある攻撃者の口座という寸法ですが、入金を待っている会社は「単なるお客さんの入金遅れかな」などと考えてしまい、詐欺であることがすぐにはばれない。お客様に問合せをした時には後の祭りです。米国などでは、こうした新手の詐欺がかなり出てきているようです。

また、「自動化」のトレンドがあります。ビジネスをする側は人工知能を事業に活かせないかを一生懸命考えていますが、攻撃をする側も当然同じことを考えるわけでして、自動化がどんどん行われ始めています。人間が関与する方が間違いを犯して発覚のリスクが増すので、機械にやらせた方が成功率は高いし、逃げるのも簡単なのですね(笑)。

**井手**　国際関係が不安定になって、サイバー空間での犯罪はますます増えてきそうですね。

**丸山**　そのとおりです。ところが、新しい犯罪が次々と海外や国内で起こっていても、日本のユーザー企業ではそうした情報を咀嚼できる人材がいないのが通常です。それが「ユーザーにおける知識・理解の現実とギャップ」という問題です。では、ITエンジニアはどうかと言えば、新しい専門分野の動きを追うのに精一杯なので、そんなにセキュリティのことばかりに構っているわけにはいかないということになります。

## 経営者の思考停止が組織を停滞させる

**丸山**　次に問題だと思うのが、「権限委譲という名の思考停止」です。つまり、企業のトップの方が「お前、ちゃんとやっとおけ」と言って、そこで終わってしまう。

**井手**　ところが本当に問題が起こると「何をやっているんだ！」となる(笑)。

**丸山**　「CISO（最高情報セキュリティ責任者）を作ればよい」という考えは、CEOの逃げの発想、責任逃れの方便ではないかと思うのですが、いかがですか？

**井手**　私は以前の勤め先でCISOをやっていたことがありまして(笑)。

**丸山**　一般的な経営層の方々は、ITのこともよく分からないし、ましてや「Business E-mail Compromise」などと言われても、理解しようという気にもならないのではないでしょうか。

**井手**　セキュリティが重要だということだけはわかるけれども、どうしたらよいかを具体的に考えるのは大変です(笑)。

**丸山**　そうだと思います。そして「お前、なんとかしろ！」になってしまうのが、私には、経営層の思考停止ではないかと感じられてしまうのです。思考停止という言

い方は、もしかしたら失礼に当たるのかもしれないのですが、それがビジネスにとってリスクだとしたら、真剣に考えざるを得ない。必要な投資や経営判断をするのが経営者の責任だと思うのです。そして、お金の投資よりも、能力がある人に必要な権限を与えて責任を持ってやってもらう方がより重要ではないかとも思います。

**井手**　本当の意味での権限委譲ということですね。

**丸山**　おっしゃるとおりです。その人のことを信頼して仕事を任せるということですね。しかし、日本の会社は事業戦略をドライブする側に人を当てるので、守りの仕事であるセキュリティにはなかなか人を当てません。

**井手**　「金は渡さない、人は渡さないが、ちゃんとやれ！」になる（笑）。さらに、なんのためにやっているかわからないので、得てしてルールを厳格にするだけのセキュリティ原理主義がはびこるようになってしまいます。

**丸山**　本来の意味が何なのかを考えない。私が思考停止と呼びたいのは、まさにそこです。

## システム導入の前にまずはルールが必要

**丸山**　三番目の問題はベンダー側にあります。私自身もベンダーにいましたのであまり言いたくないのですが、ベンダーの「恐怖営業」が問題です。つまり脅すんです（笑）。

**井手**　マイナンバー一つで、そこまでというほど脅しますからね（笑）。

**丸山**　脅しますよね。「これが漏れたら会社が潰れます」みたいな言い方を平気でしますから（笑）。さらに別の脅しがあって、「このソフトウェアを入れればセキュリティは完璧です！」と語る営業マンがいます。でも、それはありえないんです。セキュリティにはゴールはありませんから。

**井手**　発送前に宛先チェックをしないと出せない仕組みのメールの誤送信対応ソフトなども「これを入れれば完璧」といった謳い文句を聞きますが、たしかに嘘八百ですね。本来は本当に宛先間違いがないかを確認して、チェック欄をクリックすることを要求しているのですが、使う方が慣れてしまうと、実際には確認していないのにチェック欄をクリックして送るようになってしまう。

**丸山**　そのとおりで、「これを入れれば完璧です」などというソフトなど決してありません。その話を聞いたとたんに、ユーザー側は「ダウト！」と叫ばなければいけないんです。

まずルールをつくる。ルールがなければ、システムを入れても仕方がありません。そのルールを守るためにシステムを入れるわけで、ルールに従った運用のあり方を決めて、それをきちんと行うことが重要なのです。システムはそのためにあるわけです。

そこで次に「例外処理」の問題が出てきます。ルールには例外がつきものですから、例外が生じたときにどうするのか、それを誰がどう判断するのかを決めておく。さらに言うと、次に来るのが監査です。

ルールを決める。そのルールを守るためにシステムを使う。そのシステムをしっかりと動かす。例外が出たときにはきちんと判断を行い、それらがすべて守られているかを第三者が確認する。そうした構造がきちっとできていないと、セキュリティは守れないと思います。

**井手**　貴社では監査部門を監査する仕組みはどうなっているのですか？

**丸山**　ベネッセインフォシェルの監査がちゃんと動いているかは、ベネッセホールディングスが見ています。業務委託をしている親会社が監査を行う仕組みです。

## 基本に忠実に対処し、矛盾を減らしていく

**井手**　お話しいただいた課題に対し、企業はどのように対処していけばよいのでしょうか。丸山さんの考え方と貴社の取組みの例を教えていただけますか？

**丸山**　原則は基本に忠実であること。そして矛盾を減らしていくことだと思っています。つまり、現場でセキュリティ施策を実施する人たちに対して、「こう決まったのだからやれ」と無理強いをするのではなく、本当にできるようにするにはどうすればよいか、適切な手

段を一緒になって考えていく。そして、それを行うよう誘導をしていく。できなかったら、こうしなさいという代替手段を考えてあげて、それでもできなかったら禁止する。このプロセスをやり続けていくわけです。

しかし、どうしてもルールには矛盾が出てきます。例えば、「機密情報の一切持出し禁止」というルールをつくると同時に、それは完璧ではないわけです。そこをどのように解決していくかを現場に委ねるのではなく、矛盾が見つかったら、ルールを決めた側が「では、こうしよう」と決めてあげなければならない。矛盾が生じるかどうかは、やってみなければわからない。それを一つずつ吸収していくしかないのかなと思っています。これが根本的な原則です。

**井手**　矛盾がどこにあるかを見つけていくのですね。

**丸山**　どのような矛盾があるかを見つけ、それをなくしていく。それが現実的な運用だと思います。実行するには金もかかるし、時間もかかります。そのためのロードマップを数年計画でつくり、矛盾をどう減らしていくかを考え続けていかなければなりません。そもそもICT自体がレベルアップしていきます。かつては思いもよらなかったことですが、スマートフォンで企業の仕事ができるというようなことが普通に起こってくる。そのことによって生まれる新たなリスクをどのように吸収するかは現場で考えてくしかないですよね。そうしたことをやり続けなければ駄目かなと思っています。

攻撃の高度化に対して、当社はラックというセキュリティの専門会社との協業という解を求めました。それによって、例えば私のようなセキュリティ分野に人的ネットワークを持っている人間が来ることになりますので、当然これまで以上に情報が入るようになります。このように、セキュリティベンダーと協業をするというようなことを具体的にやってしまう方が現実的なのではないかと思うのです。日本の企業ではしばしば「情報共有を図る」と言う言い回しを使いますが、この言葉はうさんくさいと思っています。というのは「共有」というのは方法に過ぎず、どのような情報をどうやって集めるかが重要だと思いますので、最新の情報を採り続けるためには人間関係を作っていくことが必要なのかなと思います。

**井手**　日本企業のIT人材のレベルは今の水準のままでは駄目ですか？

**丸山**　駄目だと思います。ただ、最近はセキュリティ技術者がユーザー企業に転職するケースが増えています。技術者の側にもニーズが出てきているんです。

ユーザーの側に技術が分かる人がいて、その人がユーザーの言葉を翻訳して仕事を出す、あるいは目利きができるようにならないとスムーズな会話になりません。しかし、日本もこれからそうなっていくのではないでしょうか。

**井手**　中途採用で採るわけですね。社内で育てようという発想はない？

**丸山**　中途採用です。残念ながら育てられる人がユーザー側にはいません。そもそも先生がいませんので、そういう人たちを外から採ってくるということですね。

なお、「セキュリティ技術者育成」という言い方がしばしばなされますが、実はセキュリティ技術の専門家を育成しても駄目で、セキュリティと業務とが分かるIT技術者をユーザー企業の中で育てていくということが重要だと思います。

**井手**　両方が分からないと回らないのですね。

**丸山**　システムだけ語れても駄目なんです。業務が分かり、それを基に何をどう守るのかというルールとシステムと運用と、それら全部を考えられないと守るべきものを守れません。

## ゾーニングで誰もが分かる環境を作る

**丸山**　現実とあるべき姿とのギャップを埋めるために、当社でどのように対処しているのかについてお話をしてみたいと思います。

まず、ユーザーが現実と理論とのギャップをどう理解するかが最初の問題だとすると、人が見てすぐに分かるようにしなければいけません。当社では、ベネッセグループの基準に沿って、エリアを物理的にゾーニングしています。詳細はお話しできませんが、お客様とビジネスの打ち合わせをするエリア、外部の人は入れない一般執務エリア、お客様情報データベースを操作するエリアです。例えば、お客様情報データベースを操作するエリアには、あらかじめアカウントを付与された一部の社員しか入れません。ゾーン内には一切の物品の持ち込み、持ち出しすることができません。食品工場などのクリーンルームをイメージしていただけるとわかりやすいと思いますが、その中でしかお客様の個人情報を取り扱う作業はできません。このクリーンルームを実現するために、ミリ波ボディスキャナなどのセキュリティ施策をいくつか導入しています。

こうした色分けで、どこで何をやってよいのか、よくないのかを目で見て分かるようにしています。物理的に分かりやすく区切って、そこにルールを合わせるようにすると、ここでやるのはまずいということがすぐに理解できるようになります。使う側にすぐに分かるようなゾーニングは大事だと思います。

**井手**　ミリ波ボディスキャナというのは何ですか？

**丸山**　3Dボディスキャナとも言いますが、米国の空港などで金属探知ではない探知機が導入されているのをご存知でしょうか。それと同じものです。物を身につけていると、金属ではなくてもそれを探知できるんです。

**井手**　空港でチェックインをするのと同じようなチェックをしている。

**丸山**　空港より断然厳しいです。空港は私どものチェックに比べたらかなり緩いです（笑）。おまけに24時間、警備会社の警備員が有人で監視をしていますから、普通の会社に比べると格段に厳しいです。

**井手**　警備員が24時間詰めているのですか？

**丸山**　そうです。作業指示書などどうしても持ち込まなければならないものがあれば、警備員がすべてを確認します。

**井手**　おそらく、そこまでしているのを見せるところに意味がありますね。

**丸山**　そう思います。やっている方が見られているのが分かっていますから、悪いことをしようという気が起きません。

## 運用ルールを実現可能なものにし、状況に応じて見直す

**丸山**　次にやっているのが、運用ルールを熟考して実現可能なものとし、状況に応じて見直すということです。運用ルールを本当に考えなければいけないと思います。サンプルポリシーをただ単に持ってくるというのではなく、この会社ではどこまでやればいいのかを考えなければいけません。

例えば、ノートPCのワイヤーロックはどの会社でもしますよね。うちも最初のうちはワイヤーロックを必須にしました。社内であっても持ち運び禁止にしたんです。しかし、それだと実運用上仕事になりません。会議の席にPCを持っていけないし、もちろん自宅にも持ち帰れません。そこで社内では持ち運んでもよい、ただし、自席に座ったときにはワイヤーロックをしな

さいというルールに変えたんです。こうすれば、課長が目で見てチェックができますし、監査チームが週に1回はチェックをしていますから、できていなければ課長が叱られるわけです。

ところが、これをいくらやってもワイヤーロックのし忘れやうっかりして持ち帰りが出てくる。それではまずいので、仮想化端末を導入して持ち帰りも許可できるようにする。

つまり、最初はガッチリと固めてしまうのですが、それを運用ルールで現場に合わせていくということをやっています。

## ルールを守る意味を理解してもらい、本気で監査し、都度指摘する

**丸山**　研修はどこの企業でもやっているとは思うのですが、当社ではテストで100点が取れるまでやり続けるということを徹底しています。研修をしたらOKなのではなく、理解したらOKなのです。監査チームでは「社員が自覚するまでやらせます」と言っています。「やってはいけないんだ」と本人が自覚することが必要なんです。

それでも人間ですから、失敗することはあります。ですから、その時も「再度やったら始末書だよ」といったようなルールを作って自覚をさせるということをやっています。

あと、監査チームではメールは全部チェックをしています。

**井手**　メールの何をチェックするのですか？

**丸山**　一つの例としては、添付ファイルをすべてチェックしています。外部アドレスにはファイルを添付したメールを送ってはいけないという基本ルールがあります。その他にもいくつかのルールがあり、システム上もチェックができるようになっています。引っかかったものを監査部がすべて目視する。やむを得ずファイルを添付して送る際の暗号化は送信者が勝手にしてはならず、サーバ側で自動的に暗号化をして相手に届けます。サーバ側ではそのキーを送信者に渡し、それを送信者に改めて送らせる。これをすることによって、誤送信を防げますし、暗号化のし忘れも防ぐことができます。さらに送られたファイルは監査部が目でチェックをします。

**井手**　それは最もセキュリティの強度が厳しい第3のゾーンの中だけではなくて、すべての社員に適用されるのですか。

**丸山**　はい、全社員に適用しています。そしてもう少し補足すると、第3のゾーンからメールは使えません。お客様の個人情報をメールで外に出すこと自体を例外なく禁止しているのです。

**井手**　貴社の場合、機能子会社の立場だから、そこまで厳密にできるのではないでしょうか。営業マンがたくさんいる大きい会社で全員の添付メールを読むのは難しいように思います。

**丸山**　確かに当社では業務が明確に定義されていますし、やっていいことといけないことが明確に決められています。ですから、もし営業には営業ならではの業務が必要だとしたら、そのためのゾーンを設定して、そこで行う業務を定義すればよいと思います。場所とルールとを合わせ、何をしてよいか、よくないのかを決めていくわけです。それを考え続けることが重要で、この機能について、この業務をこういう風にやっているから、これをここまで制限をして、こうやって運用するんだ、こうやってチェックするんだというのがすべてセットなんです。全部がセットになっていないと、抜け道がたくさん出てきます。

**井手**　ほとんどの組織にはどこかに抜け道がありそうですけれど。

**丸山**　そこで大事になってくるのが、現場からフィードバックをもらい、気づかない弱点の補強とダブルスタンダードをなくす努力を続けることです。百点満点の仕組みはありえないので、弱点を見つけたら皆から言ってもらうし、そもそもルールと運用にギャップがある部分はありますから、それも言ってもらって、次のルールに取り込むことが重要で、その努力を続けています。年に2度ぐらいはそうした見直しをしています。

**井手**　毎回新しい気づきがあるのですか？

**丸山**　システムが新しくなりますから、そこに脆弱性が出てきますし、新しい課題が見つかります。システムが更新される限りはなくならないと思います。

## 施策を本当に考えられるのは現場だけ

**丸山**　次にベンダーへの対応ですが、売る方はこれを入れれば大丈夫ですと言ってくるわけですが、それはありえません。運用ルールを考え、システムで制限をし、監査でチェックをするということを繰り返していくことしかないと思います。

　当社では監査チームがどうやったら守れるのかを考え続けているのですが、そういう人材がいないと守れるものが守れなくなります。外部のコンサルタントは現場の仕事を知らないので、この仕事はできません。

**井手**　得てしてコンサルタントは報告書の見せ方は上手ですが、現場の業務はまるで分かっていませんからね。

**丸山**　考えた策が本当にできるかどうかを判断できるのも現場だけだと思います。コンサルタントは厳しいルールは考えつくかもしれませんし、案はたくさん出せるかもしれません。しかし、考えたルールが実務的に業務時間内でできるかだとか、私たちの能力で処理できるかを判断できるのは当事者である現場だけなのです。

　私どもは機能子会社ですから、そうしたことを理解している社員を増やして、本社の必要な部署に送るといったことも重要な役割になってきます。まだ、そこまでは手が回りませんが、当社の機能の一つとして位置づけて、将来は推進していきたいと考えています。

**井手**　人を育成するのが重要だと。

**丸山**　守らせるのも、守るのも人ですから。最後は人だと思います。

**井手**　貴社の収入は親会社からの委託費でしょうから、そこのコックを親会社に閉められてしまうと、やろうと思っても、やるべきことができなくなる。企業は慣れてくると、得てして掛けているコストが惜しくなる傾向があります（笑）。リーズナブルな対価をもらわないといけないですね。

**丸山**　幸いなことに、ベネッセの場合、実運用の中に仕組みが根付いてきていますので、現状では大きなコストがかからなくなっていますし、如何にコストを下げるかを考えるようにもなってきていますので、今後は大きな投資がなくてもやっていけるようになりつつあるように思います。そこは私どもの強みなのかもしれませんね。

**井手**　企業にとってリスクを把握し対処を考えることがますます重要になってきます。

**丸山**　サイバーセキュリティ基本法が定められ、経済産業省のサイバーセキュリティ経営ガイドラインが出て、今春には改正個人情報保護法の完全施行が迫っています。それに伴ってセキュリティに対する世論が高まっています。私はかつての公害問題と似た部分があるんじゃないかと思っています。

　公害問題も当初はだれも気にかけていなかったわけです。それが、社会問題化することによって法律ができ、皆がそれを守らなければならないと認識するようになりました。セキュリティもそれと同じで、これから数年はかかっても、ある水準まではやらなければならないのは常識だよねという風になってくる、その過程にあるのではないかと思います。

　加えて思うのは、「自分の身は自分で守る」ということです。皆さん、何かあったときに国が守ってくれるとか、保険が守ってくれるんじゃないかとか、なんとなく思ってしまっているところがあるのではないかと思います。しかし、実際には誰も助けてはくれません。そうした環境の中で事業活動を行っているわけですから、お客様を守る、事業を守る、そのためにセキュリティレベルを上げていくということを他人に頼らずにやっていくことこそ求められているのではないでしょうか。

1

# プライバシー影響評価（PIA）の海外動向と日本への応用

株式会社国際社会経済研究所　情報社会研究部　主幹研究員　小泉 雄介

PIAは、事業者における個人情報取扱いの適切性を自ら確認する側面と、自社の事業活動の適切性を消費者にアピールするという透明性向上の側面を持っています。近年、JR東日本SUICA事案やNICT大阪駅ビル実証実験等で顕在化したように、個人情報を取扱う事業を進める上では単なる法令遵守のみならず、当該事業の社会的受容性を常に念頭に置く必要があります。この社会的受容性を高めるための手段としてPIAは優れたツールであると考えられます。本稿では英国を中心とした海外動向について紹介します。

## 1 はじめに

近年、個人情報保護・プライバシー保護の分野でのリスク分析手段として、欧米諸国では広く「プライバシー影響評価」（Privacy Impact Assessment：以下、PIA）が導入されてきています。日本でも社会保障・税番号制度（マイナンバー制度）の導入に合わせて、同制度が国民のプライバシーに与える影響を軽減するために、マイナンバーを取扱う事務を行う行政機関や地方公共団体等に対して、PIAの1つである「特定個人情報保護評価」の実施を義務付けています。またEUでは、2016年4月に採択された一般データ保護規則（General Data Protection Regulation：GDPR）において、民間企業や行政機関に対して個人の権利や自由に高いリスクをもたらす可能性のある個人データ取扱いについて「データ保護影響評価」（PIAに相当）を義務付けることとなりました。

PIAとは、個人情報を取り扱う情報システムやサービスの開発に先立って、プライバシーへの影響を事前に評価し、問題回避のための運用的・技術的な変更を促すための一連のプロセスです。民間企業においては、①自社における個人情報取扱いの適切性を自ら確認し、社内関係者の意識を高めることで個人情報漏洩等のリスクを減らす（自己防衛の側面）とともに、②自社の事業活動の適切性を消費者に対して目に見える形で訴えかけること（透明性向上の側面）を目的としています。

米国、カナダ、オーストラリア、ニュージーランド、英国といった国々では、PIAは行政機関や民間企業が自己評価するための枠組みとして普及しつつあり、とりわけ英国では、データ保護監督機関である情報コミッショナーオフィス（Information Commissioner's Office：以下、ICO）がPIAガイドラインの策定や、PIA実施組織に対する助言等を行っています。他方、日本では、マイナンバー法の枠組み内で行政機関や地方公共団体等が特定個人情報保護評価を実施していますが、マイナンバー制度の一環の取組みとして捉えられている側面が強く、PIAが民間企業で広く自発的に行われるような状況には至っていません。日本で民間企業にPIAが浸透していかない要因としては、企業側でのリスク分析手段としての認知度がそれほど高くないことや、個人情報保護法など法令上でPIAの義務付けがなされていないことが挙げられます。

図表1　PIAとプライバシーマーク制度の比較

| | PIA（プライバシー影響評価） | プライバシーマーク制度 |
|---|---|---|
| 評価の対象、評価の単位 | 個人情報を取扱う特定のシステム、制度、プロジェクト（必ずしも組織毎に行う必要はない。ある制度が複数の組織に跨って導入・実施されるような場合には、1つのPIAで対処することも可能。） | 個人情報を取扱う企業<br>（具体的には、当該企業の個人情報保護マネジメントシステム。） |
| 評価実施のタイミング | 事前<br>（システム・制度等を導入・改修する前。具体的にはシステム設計の前。） | 事前・事後は特に問わない |
| 評価の実施主体 | 当該組織による自主評価 | 審査機関による第三者評価<br>（当該企業による内部監査も実施。） |
| 主に誰に対してアピールするためのものか | 行政機関の場合：国民<br>民間企業の場合：消費者 | 消費者、委託元企業・地方公共団体 |
| 準拠基準 | 第三者機関等が制定するガイドライン | JIS Q15001<br>「個人情報保護マネジメントシステム－要求事項」 |

しかし、個人情報保護の分野は、法令だけ守っていればよいというものではありません。近年、JR東日本SUICA事案（2013年）やNICT大阪駅ビル実証実験（2014年）で顕在化したように、民間企業や組織が個人情報を取扱う事業を進める上では、単なる法令遵守のみならず、当該事業の社会的受容性・コンセンサスを常に念頭に置く必要があります。そして、この社会的コンセンサスを得るための手段として、PIAは優れたツールであると考えられます。

「PIAとは何か」ということについては様々な定義がなされています。例えば『プライバシー影響評価PIAと個人情報保護』[1]では、「個人情報の収集を伴う情報システムの導入または改修にあたり、プライバシーへの影響を事前に評価し、問題回避または緩和のための運用的・技術的な変更を促す一連のプロセス」と定義しています。

PIAは上記の定義にも見られるように、「事前に」（システム等を導入・改修する前に）行うことが重要です。事前に行うことによって、事後的な仕様変更等によるコスト発生が避けられるほか、消費者とのコミュニケーションを十全に行うことによってネットでの炎上等、企業の評判低下・信用失墜のリスクを減らすことができます。PIAはプライバシーマークのような第三者認証制度ではありませんので、基本的には当該企業や組織が自主的に評価を行うことになります。ただ、コンサルタントや監査法人など第三者によるチェックを排除するものではありません。

参考まで、PIAとプライバシーマーク制度とを比較してみます（図表1）。

## 2　海外におけるPIAの状況

米国、英国、カナダ、オーストラリア、ニュージーランドといった英語圏の国々ではPIAの導入が進んでいます。

カナダはPIAの必要性を早期から訴え、1990年代後半、個人情報保護に関する法律を効果的かつ体系的に遵守するためのツールとして、PIAが検討されました。2002年にカナダ財政委員会事務局が発表した「PIAポリシー」において、個人情報を取り扱うITシステムを導入・改修する連邦政府機関に対してPIA実施を義務化しています。2010年には同事務局がPIAポリシーを改定する「PIA指令」を策定、同年4月から施行されています。2011年3月には監督機関である連邦プライバシーコミッショナー事務局（OPC）により、連邦政府機関がPIA報告書をOPCに提出

1　瀬戸・伊瀬・六川・新保・村上著『プライバシー影響評価PIAと個人情報保護』（中央経済社）。

する際のガイドが発行されました。

米国は2002年電子政府法の第208条において、連邦政府機関にPIA実施を義務化しています。政府機関にはPIA報告書の写しを連邦行政予算管理庁（OMB）の長官に提出する義務があります。2003年には、OMBがガイダンスを発行しています。また2010年6月には、国土安全保障省が同省向けのPIAガイドライン(最新版)を発行しています[2]。

オーストラリアでも2006年8月に連邦プライバシーコミッショナー局が行政機関向けの「PIAガイド」を発行しています。

EUに目を向けると、英国では導入が進んでいますが、これまでEUの他の国々では導入が進んできませんでした。ただし、前述のようにEUの一般データ保護規則(GDPR)において、一定条件を満たす民間企業や行政機関に対してPIA実施の義務が盛り込まれたことにより、今後EU各国での導入が一気に進むと考えられます。EU企業等のGDPRへの準備状況に関する2016年の調査では、約56%の企業が「個人のプライバシーに高いリスクを生じさせる可能性のあるプロジェクトについて、既にPIAを実施したことがある」と回答しています[3]。

## 3 英国の状況

### 3.1 英国におけるPIA導入の経緯

英国においてPIA導入の1つの契機となったのは、ICOが2006年に作成した「監視社会に関する報告書」です。この報告書では、英国における監視社会（監視カメラ、国民IDカード等）の進展に対処するための手段としてPIAが取り上げられています。

その後2007年にICOはPIAの国際調査（カナダ、オーストラリア、米国等）とハンドブック作成を公募し、同年12月に「Privacy Impact Assessment Handbook」（PIAハンドブック）を発行しました。ICOは2009年に同ハンドブックの第2版を発行し、この中では、PIAの対象となりうるシステム[4]は個人データ取扱いを伴うもの全般（官民を問わない）とされています。ICOは2014年2月に、更にPIAを導入しやすいものとするために、ハンドブックの後継となる「Conducting Privacy Impact Assessments Code of Practice」(PIA実施行動規範)を発行しています。

また2008年6月には内閣府が報告書「Data Handling Procedures in Government」を発行し、その中で、中央省庁に対して、個人データを取扱う新しい制度・システムに関してPIA実施を義務化しました。同報告書は、2007年の歳入関税局での2500万人分のデータ入りCD-R紛失事件を受けて作成されたものです。

### 3.2 PIA実施の目的

行政機関や民間企業がPIAを実施する目的は、ICOのハンドブックやPIA実施行動規範の内容を整理すると、図表2の3つを挙げることができます。

### 3.3 英国におけるPIAの特徴

ICOによると、英国におけるPIAの最大の特徴は「コンサルテーション・フェーズ」を重視していることです。コンサルテーションとは、利害関係者（内部および外部）との話し合い・意見聴取のことで、想定される影響やリスクの洗い出しを目的としています。当該システムを運用する職員、システム開発に携わるIT企業・セキュリティ企業、当該システムによってプライバシーの影響を受ける市民・消費者、その他有識者などが対象となります。コンサルテーションの方法は様々であり、ICOでは特にその方法を指定していませんが、例えば市民に対するコンサルテーションの方法としては、フォーラムの開催、フォーカスグループでの調査、市民団体への文書による照会、パブリックコメント等が例示されています。

コンサルテーションの実施によって、プロジェクトの早期の段階で設計に変更を加えることが可能になります（図表2の③）。また、市民・消費者に対しては、コンサルテーションで洗い出したリスク[5]に対して、PIAを通じてきちんと解決を図っていることを説明することができるため、これによって反対意見を取り込むことが可能となります（図表2の②）。

2 拙稿「米国・カナダにおけるプライバシー影響評価と日本における検討状況」http://www.i-ise.com/jp/report/PIA_20120131.pdfもご参照ください。
3 Centre for Information Policy LeadershipとAvePointが2016年5月に実施した、主に多国籍企業223社に対する調査。https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/11/cipl_avepoint_gdpr_readiness_survey_report_1107_final-c.pdf。
4 PIAハンドブック等の中では、PIAを実施する対象を指す用語として「project」の語が使われています。これはsystem, database, program, application, service, scheme, initiative, proposal, review, draft legislationを幅広く指す語とされていますが、本稿では主に「システム」と読み替えています。

図表2　英国ICOガイドにおけるPIA実施の目的

①法令遵守に留まらないプライバシー保護

PIAは、当該システムが個人のプライバシーを侵害するリスクを考慮に入れるためのプロセスであり、単に（英国の）データ保護法を遵守するために必要となる措置よりもカバー範囲が広い。

②利害関係者のコミットメントと市民の信頼の醸成

PIAは、利害関係者の見解を集め、適宜フィードバックを行う、透明でコンサルティブなプロセスである。そのため、PIAを実施することによって、一般市民・消費者を含む利害関係者の理解やコミットメントを得ることができる。これによって、当該システムに対する一般市民・消費者のプライバシー面での信頼を醸成することが可能となる。

③事後の仕様変更やコスト発生の回避

PIAは当該システムの設計等のフェーズに先立って、事前に実施するべきである。事前に行うことによって、プライバシーリスクを予見したり、リスクに対する解決策を事前に見出すことが可能となる。システム開発の途中や事後にPIAを実施することは避けるべきである。なぜなら、事後にシステムの仕様を変更したりエラーを直すことは、コストがかかるし、更なるエラーを引き起こす恐れがあるからである。

## 3.4　PIAの実施プロセス

ICOはPIA実施行動規範において、PIAの大まかな実施プロセスとして以下を示しています。

### (0) コンサルテーションを行う

PIAプロセス全般を通じて、適切なタイミングで内部関係者や外部関係者（消費者や有識者）とコンサルテーションを行う。

### (1) PIAの必要性を特定する

スクリーニング質問表への回答等を通じて、当該システムが個人のプライバシーに及ぼしうる影響を考慮し、PIA実施の必要性を判断する。

### (2) 個人データのフローを記述する

当該システムのデータフローを記述する。どのようなデータがどのような目的で利用され、誰から取得され、誰に提供され、誰がアクセスできるか等について説明する。本ステップにより、潜在的な「ファンクション・クリープ」[6]を認識することができる。

### (3) プライバシーに関連したリスクを特定する

個人に対するリスクとして、例えば、不正確なデータやデータ漏洩による損害、不必要なデータ取得による侵害など。組織に対するリスクとして、例えば、データ漏洩、評判低下、信用失墜、金銭的コスト、法令違反など。これらの特定されたリスクを一覧にする。

### (4) 解決策を特定し、評価する

各リスクに対処する方法を決定する。リスクの中には、完全に除去できるものもあれば、軽減できるものもある。また多くの場合、一定レベルのリスクは受容せざるを得ず、ある程度のプライバシーへの影響は残る。いずれにせよ、リスクに対する解決策を決定する際には、プライバシーに対する影響がプロジェクトの目的と比例しているか（釣り合っているか）を検討する必要がある。

**●プライバシーリスクの除去策・軽減策の例**

- 特定の種類のデータを取得・保存しないようにする。
- データの保存期間を必要最小限なものに見直し、保存期間後はセキュアに廃棄する。
- 適切な技術的安全管理措置をとる。
- データを安全に匿名化する方法を開発する。
- 適切な委託先事業者を選定する。
- 新たなシステムの運用方法に関する職員向けガイダンスを作成する。
- 職員を適切に訓練し、プライバシーリスクを認識させる。
- データがどのように利用されているか消費者が十分に認識できるようにする。
- 消費者向けの問合せ窓口を設置する。

### (5) PIAの結果を承認し、記録する

プライバシーリスクが適切なレベルまで対処されたこと

5　ICOによれば、「リスクがないと結論付けるのではなく、あらゆる段階でリスクを特定し、それらの最小化を図った上で、残存するプライバシーリスクが正当化できるものであるかを確認することが重要」とのことです。

6　技術やシステムの利用範囲が当初目的よりも徐々に拡大していくこと。予期せぬデータ利用や意図せぬデータ利用など。

を確認する。これは、プロジェクト承認行為の一環として行うこともできる。PIA報告書には、PIAの全体プロセスや、どのリスクについて除去し、どのリスクについては軽減し、どのリスクについては受容したかという意思決定を記録する。PIA報告書の公表は、透明性やアカウンタビリティを向上させるものであり、消費者とのコミュニケーションにおいて重要である。

### (6) PIAの結果を計画に反映させる

当該システムの開発・実装の様々な段階でPIAに立ち返る。PIA実施後に継続的なモニタリングが必要になる場合もある。今後のために、PIAで得られた知見を記録する。

なおPIAハンドブックでは、「複数のシステムに対して1つのPIAを実施する」ことが合理的かつ経済的であるような場合があるとして、以下の例が挙げられています。

- 複数のシステムに実装されるようなパッケージ・アプリケーションに対して、当該アプリケーションの開発企業がPIAを実施する。
- 複数の政府機関が共通のプラットフォームを導入するような際に、包括的なPIAを実施する。
- ある業界内における共通のアプリケーション(信用情報アプリケーション等)に対して1つのPIAを実施する。

## 4 EUの一般データ保護規則(GDPR)

EUでは近年のインターネット等の急速な技術的進歩やグローバル化の進展によって発生してきた課題に対処するために、従来のEUデータ保護指令を改定する一般データ保護規則(GDPR)が2016年4月に採択されています。2年間の移行期間を経て、2018年5月から各加盟国に適用されます。

GDPRでは新たに第35条でデータ保護影響評価(Data Protection Impact Assessment:DPIA)の実施義務が追加されました。これはPIAに相当するものです。第35条では「特に新たな技術を用いる場合など、個人の権利や自由に高いリスクを生じさせる可能性がある場合」には、民間企業や行政機関は事前にPIAを実施しなければならないと規定しています。とりわけ、以下の3つの場合についてはPIAの実施義務が明記されています[7]。

(a) プロファイリングを含めた自動処理に基づいて自然人に関する個人的側面を体系的かつ広範囲に評価され、その評価に基づいて決定がなされ、その決定が自然人に関する法的効果を生じさせるか又は同様に自然人に重大な影響を与える場合。

(b) 第9 条第1 項で定める特別な種類のデータ、又は第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。

(c) 誰でも立ち入ることの出来る場所において大規模な体系的監視を行う場合。

このPIA(DPIA)の手法やテンプレートに関するガイドラインは、EUの諮問機関である第29条作業部会が2017年に発行する予定です。

## 5 プライバシー・バイ・デザインとの関係

PIAと類似した言葉として、「プライバシー・バイ・デザイン」(Privacy by Design)という考え方があります。このプライバシー・バイ・デザインは「設計段階からプライバシー保護を組み込む」というシステム開発・サービス開発の1つの「哲学」で、企業や組織が果たすべき責任の1つという位置づけです。カナダの前オンタリオ州情報・プライバシーコミッショナーであるAnn Cavoukian博士によって1990年代に提案された理念です(図表3)。あくまで理念ですので、その具体的な実践手段としてPIAやPET(Privacy Enhancing Technology:プライバシー強化技術)を用いることで実現されることになります。

プライバシー・バイ・デザインの考え方は、前述のGDPR、OECDプライバシーガイドライン改定版の補足説明覚書(2013年)、米国のデータ保護監督機関である

7 和訳はJIPDEC「EU一般データ保護規則(仮訳)」https://www.jipdec.or.jp/library/archives/gdpr.htmlより。

図表3　プライバシー・バイ・デザインの7原則 [8]

1. 事後的ではなく事前的、救済策的でなく予防的
2. 初期設定としてのプライバシー
3. デザインに組み込まれるプライバシー
4. 全機能的：ゼロサムではなく、ポジティブサム
5. 最初から最後までのセキュリティ：すべてのライフサイクルを保護
6. 可視性と透明性：公開の維持
7. 利用者のプライバシーの尊重：利用者中心主義を維持する


FTCの報告書（2012年）等に立て続けに盛り込まれています。この背景としては、ICTの発展により個人データ漏洩・濫用時の影響・被害が甚大化したこと、技術進歩に法律制定・法規制が追い付かなくなってきたこと、企業の個人データ取扱いが複雑化し、個人が自分のデータの取扱われ方についてプライバシーポリシーを読んでも必ずしも理解できなくなったことが挙げられます。そのため、企業が果たすべき責任の1つとして、消費者の個人データやプライバシーを「先回りして」守ることが求められているのです。

## 6 日本での応用可能性

前述のように、日本でも民間企業が個人情報を取扱う事業を進める上では、単なる法令遵守のみならず、当該事業の社会的受容性・コンセンサスを常に念頭に置く必要があります。近年、店頭カメラ画像を用いた顔認識技術等の画像解析技術を、防犯・防災・マーケティングなど様々な用途で利活用することが期待されていますが、従来の防犯カメラとしての用途を超えて、店頭カメラ等の画像を活用しようとした場合、まさしく「社会的コンセンサスがどの程度得られているのか」という問題に突き当たることになります。カメラ画像の長所は、アンケート記入やポイントカード提示などで消費者の手を煩わせることなく、消費者の属性や行動などの情報を直接的に取得できる所にあります。しかし、同じ点がまさに「自分の映像がどこで撮られているか分からない」「自分の情報がどのように使われているか分からない」という消費者の不安感につながるのです。また、防犯カメラの画像を万引き犯等の顔照合に使うようなケースも、今の時点では一般的な消費者の予測できる範囲を遥かに越えるような、思いもよらない利用方法ですので、きちんとその旨を告知することが必要でしょう。

政府のIoT推進コンソーシアムでは、JEITA（電子情報技術産業協会）等の産業界からの要望を受けて、カメラ画像利活用サブワーキンググループにおいて一定のルールを検討し、2017年1月に「カメラ画像利活用ガイドブック」を公表しています。ガイドブックでは事業者が配慮すべき事項や消費者に対する透明性担保の方法などが示されています。ただ、ガイドラインではあくまで一般的なルールしか示せませんので、例えば広いショッピングモールのどこで消費者向けの告知を行えばよいのか、近隣の消費者は特にどのような意見や不満を持っているのか、消費者から個人情報の開示請求があった場合（法的には開示義務が無かったとしても）どのように対応すべきなのかなど、具体的な対処方法はシステムやサービスの特徴に合わせて個別に判断する必要が出てきます。事業者がこのような判断に迷う場合には、PIAを自己防衛手段として実施することは1つの有力な選択肢となります。

日本ではまだ民間企業向けのPIAが方法論として確立していないところがありますが、消費者とのコミュニケーションのツールとして、今後広く使われていくことを期待します。

8　和訳は堀部政男/JIPDEC編『プライバシー・バイ・デザイン』（日経BP社）より。

2

# Pマーク審査の現場から（リスク分析）

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

## ● はじめに

ここで言うリスクとは、問題が生じる可能性、のことです。問題そのものではありません。あくまでも可能性、です。もちろん、リスクが高いか、低いか、（あるいはほとんどないか）、ということになります。

個人情報保護の領域においては、ほぼ、個人情報の漏えい、と置き換えることができます。（実際には他にもありますが、話を簡単にするために）

リスク分析とは、漏えいがどこで起きるのか、事前にこれを予測し、事故が起きる前にこれに備え、しかるべき対策を立てておきましょう、というのがその本質ということになります。

Pマークの審査において、このところは最重要事項である、と思うわけですが、これが意外と十分には理解されていないようです。

## ひとつの実例

例えば、近年審査のために訪問したある会社で、審査が始まる前から担当者が待受けていて、こちらが問う前から最近導入したばかりの入退管理システムの説明をしてくれました。

社員全員の入退出の記録が全て取れるようになったのは良かった。しかし、その記録データが相当大量になり、容量が厳しくなってきたので、そろそろ前のデータを消したいのだが、一体どれ位の期間のデータを取っておけばいいのだろうか、と質問されました。

確かに手書きの記録よりは装置で記録を取る方が楽ですが、この時点で、この会社は一体何のために入退管理システムを導入したんだろうか、と思う訳です。

審査に入ってから、実施されたリスク分析の中身を見ても、この会社として気付いたリスクが見当たらないのです。

つまり、そもそもリスクが見えないのに、なぜ最新の入退管理システムを導入したんでしょうか。

想像するに、多分、こういうことをやっておけば、Pマーク審査で良く評価されるのではないか、と、先回りして考えて、システムを導入したのではなかろうか、ということになります。

これは一つの事例ですが、皆さんの組織でも同じような事が起こっていませんか？

お金がかかるこうした事を積み上げると、経営を圧迫しかねず、いわばロスとなります。しかしPマーク審査を乗り越える、という目的を掲げ、ある意味大手を振って、社内でその投資が承認されたのでしょう。

## リスク分析を再考する

このような場合は、考えられるリスクを想定して、これへの対策を考える、という通常の考え方（いわば教科書順）ではなく、（これからやろうとすることか、既に実施していることかに関わらず）この対策は何を目的としてやるものなのか、逆の方向からも分析すべきところとなります。

それぞれの組織にはそれぞれの考え方があって、既にありとあらゆる対策を積み上げていることが多いです。しかし、対策に対応したリスクが分析できていないと、なんのための対策なのか、今後の検討に繋がらなくなってしまうからです。

## 事故は現場で

もうだいぶ前になりますが、「事件は現場で起きている」なる名セリフ（迷言？）がテレビドラマの中で使われていました。あれは既に起きちゃった事件を対象としたセリフな訳ですが、ここでは、「起きそうな事故は現場で起こる」、と読み換えることにしましょう。

すると、皆さんの組織のリスク分析結果は、どうでしょうか？ 現場で起きそうな事故の可能性を、うまく洗い出せているでしょうか？ ポイントのひとつはこれです。

**（社内の事務局の立場で）**リスク分析のための様式を配り、簡単な記入のための説明を行い、いつまでにやっといて、と作成期限も提示した結果、各部門が渋々書いて提出してきたリスク分析。

それとわかっていても、去年作成されたものをほぼ追認した今年のリスク分析。

それでも形は整っているし、見直日付と部門長の承認印があるからOKとするか？ これではダメです。形ばかりのリスク分析にすぎないからです。魂（心）が入っていませんね。

## マネジメントシステムとして見て

審査員は、審査の冒頭に代表者の方にインタビューを行います。その中で、「御社の事業の中で、個人情報保護の観点から、特に重要と考えている領域（業務）はありますか？」と必ずお聞きしています。

代表者は、言うまでもなく、社内の業務について、経営のレベルで精通していますから、直感的に答えが返ってきます。皆さんの会社のリスク分析結果は、こうした、トップの方の認識を裏付ける内容になっているでしょうか？

ともすると、下から積み上げた資料とトップの認識には、食い違いが生じています。それはやむを得ないとして、そのギャップをどう埋めましょうか？　ここにもひとつのポイントがあると思います。

こうしたギャップは、個人情報保護への取組みに限らず、ありとあらゆる業務において顔を覗かせますし、これを上手く纏める組織・仕組みが、良いマネジメントシステムだ、という訳です。

## —— ではどうするか ——

### 責任者の明確化

まず責任者構造を確保しましょう。大概の会社において出来上がっているはずですが、念のための確認です。代表者を頂点として、各部門の長が従っていますが、大きな組織の場合は、そこに何段階かの階層構造がはいる場合もあります。下位の部門の長と代表者の関係は、フラット組織である場合とピラミッド型の組織の場合と、いろいろです。

リスクの確認は、その組織の中で行うものですから、予め見ておくことが必要です。

（本当は、その各責任者の自覚、という話になっていきますが、それは追い追いと。）

### リスク分析の対象の明確化

個人情報保護の取組みにおいては、一般的には、「個人情報管理台帳」なるものを作成することが多いようです。

ここでの注意事項は、「目に見える」「手元にある」個人情報を洗い出すだけで、本当に良いのか、ということです。

ある部門の責任において関与している個人情報は、もしかすると、必ずしも手元にはない情報もあり得ます。（例えば委託先に預けた状態にある個人情報は、手元にはありません。）

とはいえ、基本的な作業としては、「洗い出し」をしてみないと先に進みません。そのときに、「下限」側の洗い出し労力をほどほどにすることが肝要となります。「より重要な個人情報」を適切に保護することが目的なのに、裾野のほうを見つめすぎ、例えば、経理帳票に押された印鑑は、定義に照らせば個人情報か？ とか、法人間で単なる儀礼的な挨拶の際に交換した名刺も個人情報か？ とかを真剣にやりだすと、「木を見て森を見失う」状態に陥ります。

従い、この取組みにおいても、責任者なり、管理者が関与することが重要です。自部門は、そもそもなにを分担する組織なのか、社内の位置付けはどうか、そしてその役割からして、どういう個人情報を取り扱っているはずなのか、その目つきから見て、十分に洗い出しができているのか、ひょっとして担当者では気づいていない個人情報がありはしないか、そういった方向で、チェックすべきでしょう。

### 業務フローを考える

初期的に洗い出した個人情報（台帳）は、まだ分析の第一歩にすぎません。

実際には、個人情報が、社内をどう流れているのか、業務フローを考える必要があります。

水の流れに例えて考えて見て下さい。ひとつの建物に、上水道から水が引き込まれ、あちこちを経由して、最終的には排出される、という考え方との類似性を考えれば、初期的に洗い出した個人情報は、流れの中では、「輪切り」状態である、とお気づきになることでしょう。「輪切り」である以上は、いくらでも細分化してスライスできますが、それをいくら積み上げても総体として個人情報を特定したことにはなりません。水でいうところのパイプ、ここでは業務フローを洗い出してこそ、個人情報が特定できたことになります。また、「保管してある個人情報」は、水の流れに例えれば、滞留している状態に過ぎませんね。

### そしてリスク分析

業務フローの、それぞれのポイントである、入り口、流れているところ、滞留しているところ、出口、そういった、ポイントごとに、リスクを想定し、対策を検討していきます。

なるべく平易な言葉を用いて、いったいどういうリスクがあるのか、これに対してはどういう対策を実施すれば安全になるのかを考えていきましょう。ここでは、担当者も入れて、「ワイガヤ」精神で参加者意識の向上も狙うところかと思います。

そのときに、前述したように、既に対策が行われている場合は、その基であるリスクを上げることも忘れないようにしましょう。

### 対策

対策には、大別して2種類ある、と考えられます。ひとつは、技術的対策です。なんらかの設備投資などを導入することによって、リスクが除去できるか、の検討です。ただ、設備投資などをするためにはコストがかかります。すぐに実施できるとは限りません。そうなると浮上するのが人的対策です。ルールを決めて、リスクを低減するために、みんなで手順を守るようにしよう、などという対策となります。一般的にはお金があまりかからないですが、人のやることなので、完璧な対策とはならないこともあります。従って、先々には、やはり技術的対策の導入をすべきか、などと将来の再検討を書き残す必要もでてきます。ある意味、これが残存リスクの考え方となります。

また、技術的対策にするのか、人的対策にするのかの選択は、まさに、責任者の判断、ということになるかと思います。

### 対策の実施

人的対策を実施に移すという場合は、一種のルール化・マニュアル化となります。単にルール化・マニュアル化しただけでは十分ではなく、関係者に周知し、守っていただくことが必要です。これが教育、ということになっていきます。

従って、教育は、全社員に一律に教育する内容もあれば、ある個人情報の取扱いの範囲に限定したものもあるでしょう。ここもひとつのポイントとなります。

### 点検

ルールが守れているのかを確認することが必要となります。これが、点検です。点検には、「運用の確認」と「監査」という異なる手法があり、その両方の特徴を掴んで実施することが必要です。

### 代表者の見直し（マネジメントレビュー）

このようにして取り組んできたことを、責任者に報告し、より上位の責任者、最終的には代表者に報告し、そして指示を仰ぐ、というのが、マネジメントシステムの最後であり、次のサイクルの最初となります。PDCAサイクルの輪の完成、ということになります。ここで肝要なことは、「足踏みをしない」精神です。ステップアップを、是非心がけましょう。

### ● 終わりに

駆け足で、リスク分析のあたりを中心に見てきました。

こうした考えが定着しているのか、定着していないとすれば、どこを補強すれば良いのか、といったようなことを考えながら、審査現場に出入りしております。機会があれば、ぜひお目にかかりましょう。

# 平成28年度 電気通信主任技術者定期講習を終えて

一般財団法人日本データ通信協会　事業推進部　部長　飯田 秀男

**平成27年度より電気通信主任技術者定期講習制度がスタートし、28年度の講習は4月に公示、7月より受付を開始し、9月と12月に伝送交換技術・線路技術の各2回(計4回)を200名規模の想定で東京で実施しました。平成28年度までの講習を振返り、取りまとめました。**

日本データ通信協会は平成27年1月に電気通信主任技術者講習の登録講習機関001号として総務省に登録され、同年7月に第1回目の講習を開始して以降東京・大阪・福岡・名古屋の地域で伝送交換技術と線路技術の講習をそれぞれ12回(平成28年は東京で各2回)実施しました。

講習風景


講習テキスト・追補版

## 1 受講者

平成28年度の受講者は192名で、全体の1割ほどが受講時点で非選任の受講者でした。

年齢は、平均年齢が50歳ですが、65歳以上の割合も1割と、高齢の方も多く目につきました。

本講習では、電気通信主任技術者資格者証を取得していて選任されていない方でも受講することが可能で、修了者には選任されている方と同等の修了証を発行しています。将来、選任される予定の方や、知識向上のためにも受講されることをお勧めしています。選任後は講習の有効期限内において受講の必要がありません。

受講者内訳(27+28年度)


受講者の年齢(27+28年度)

| | 平　均 | 最年少 | 最年長 |
|---|---|---|---|
| 選　任 | 50.3歳 | 25歳 | 83歳 |
| 非選任 | 47.5歳 | 26歳 | 76歳 |

## 2 選任事業者(複数社選任)

講習修了者は総務省への報告事項となっており、あわせて選任している電気通信事業者の名称も報告事項となっています。そのため選任している電気通信事業者を確認する必要があります。同じ会社でも名称が不統一であったり、年度途中で会社名が変更されるなどなかなか大変でした。登録事業者は300事業者以上あり受講済み事業者は平成27年度と28年度の合計(以下「累計」と言う)で約80%ほどとなりました。

また、届出事業者の中で選任しているのは累計で60事業者ほどとなりました。

選任受講者中の累計44名が1社ではなく複数の事業者から選任されており（44人で延べ118社から選任）、県間を跨る選任も累計22名ほどありました。

また、この講習は資格者証の種類ごとに、受講する必要があります。両方を兼任されている方の比率は選任の伝送交換技術者で34%と約3分の1ほどでした。

## 3 修了考査

修了考査の合格率は98%で、不合格者は3名でした。省令では「修了考査は、講義の終了後に行い、受講者が講義の内容を十分に理解しているかどうか的確に把握できるものであること」とあります。しかし、1日の短時間の講義ですので、全てを記憶することは大変なことと言えます。修了考査は講義で説明したところを中心に40分間30問、○×式で回答する方式をとっています。また、合格基準は講義に集中できるよう、70%以上としています。

出題者は「落とすことが目的ではない」ので、いわゆる「ひっかけ」の問題を作らないように配意して、正解率が85%～90%の問題となるように作成しており、結果も想定通りとなっています。

実施年度別正解率

| | 平成27年度 | 平成28年度 | 全　体 |
|---|---|---|---|
| 伝送交換 | 88.1% | 88.5% | 88.1% |
| 線　　路 | 85.9% | 89.2% | 86.4% |


修了考査風景

## 4 講習修了者・修了証の発行

平成29年1月末の講習修了者は191名と、講習を受けた方々が全員講習修了とはなりませんでした。

講義にすべて出席し、修了考査に合格した講習修了者には、修了証に次回の受講の期限を記載して発行するとともに、総務省への報告を行っています。次回の受講の期限は「講習の行われた日の属する月の翌月の1日から起算して3年以内」となり、例えば9月の講習修了者は平成31年9月30日までに受講することとなります。

## 5 その他

累計の選任された講習修了者は1,147名です。受講済みの非選任者や最近資格者証を手にされた方がが選任されるケース、異動による新規選任者の受講、また、受講有効期限の切れている方がおりました（28年度は20名以上おりました）。平成29年度も200名程度と想定し、4月に公示、7月より受付を開始し、東京で9月と12月に伝送交換技術・線路技術の各2回（計4回）を計画しています。

また、法改正などに伴い、講習後テキストの内容が変更になるなどのケースがあることから、テキストへの追補版を作成し、修了証をお持ちの方にはご提供する等のアフターフォローをしております。併せて、受講有効期限切れを迎える方には、次期の案内をさせていただければと考えています。

**●お問い合わせ**

協会：電気通信主任技術者講習担当　Tel.03-5907-7575（平日10時～16時）

ＨＰ：http://www.dekyo.or.jp/jinzai/

# インターネットの安心・安全に関する動画フェスタin近畿2016の実施

総務省近畿総合通信局　電気通信事業課長　原　彰宏

## 1 動画フェスタについて

総務省近畿総合通信局では、「スマートフォン時代に対応した青少年のインターネット利用に関する連絡会」（略称：スマホ連絡会）を設立しています。兵庫県立大学の竹内和雄准教授が座長となり、近畿管内の自治体や警察、PTA、学校関係者を中心に、有識者、事業者等も含め、70団体で構成しています。

このスマホ連絡会の取り組みの一環として、平成28年2月、「インターネットの安心・安全に関する動画フェスタin近畿2016」という動画コンテストの実施を発表しました。青少年を対象としたインターネットの安心・安全に関する動画コンテストの実施は、全国的にも少なく、総務省においても、近畿総合通信局のみの取り組みで、今回で2回目となります。

集合写真

## 2 動画制作の目的と募集結果

動画フェスタは、動画の持つ訴求力に着目し、その制作や活動を通じて、インターネットリテラシー向上を図ることを趣旨として、応募者がインターネットリテラシーの必要性、重要性に気づき、考える機会の創出等を目的としています。

応募いただく動画の内容は、インターネットやスマートフォンの安心・安全な利用に関するものであり、視聴の対象は、主に小中学生向け、という条件で、7月1日から9月2日までを応募期間としました。

当局から小中高校や大学に動画フェスタを案内し、学校関係者からも生徒・学生に周知していただいた結果、203作品（生徒部門164作品、学生・社会人部門39作品）もの応募がありました。どの作品も、いわゆる「スマホ世代」である若者の目線で作られている内容で、大人の視点ではなかなか思いつかない、斬新なものもたくさんありました。

## 3 入賞作品と表彰式

応募作品については、訴求内容や創造性、表現力、さらには、作品の利活用を想定し、著作権や肖像権の権利処理などにも留意した上で、厳正な審査を行い、入賞作品を決定しました（入賞作品は次頁）。

表彰式

12月10日（土）には、大阪市内において、優秀作品発表会を開催し、入賞作品の上映と表彰状の授与を行いました。参列した中高生、大学生からは、「いい経験ができた」、「自分たちの思いが伝わった」などとても好評でした。当日の模様は、ケーブルテレビの地元チャンネルにも取り上げていただきました。

## 4 トークセッション


トークセッション

表彰式の後、「動画に込めた私たちの想い」をテーマに、応募した生徒・学生と竹内准教授によるトークセッションを行いました。生徒・学生からは、動画を制作する上で楽しかったことやこだわったこと、また、動画を通じて伝えたいことなど、飾らない素直な言葉での発表がありました。

## 5 おわりに

入賞作品については、e-ネット安心講座や各地のイベント等での上映、また、自治体のホームページでのネット配信など、インターネットの安心・安全な利用に向けた啓発活動に積極的に活かしていく予定としています。

さらに、応募者や学校関係者から、「ネットは便利だけど、使う側の意識次第ということを、動画制作を通じて考えさせられた」、「生徒が自分のスマホの使い方を見直すいい機会になった」という声も多くいただいたことから、今後も、継続した取り組みを進めていくこととしています。

# 動画フェスタin近畿2016　入賞作品の紹介

スマちかちゃん

## ～生徒部門～

最優秀賞

「クリック詐欺に気をつけよう！」
奈良朱雀２年映像班
（奈良県立奈良朱雀高等学校）


優秀賞

「スマホの危険性」
松蔭中学校・高等学校 放送部


## ～学生・社会人部門～

最優秀賞

「あなたが見ているのは誰？」
ソーシャルメディア研究会２回生班Ｂ

優秀賞

「秘密を守る、絆を守る」
摂南大学 経営情報学科 久保研究室


## ～審査員特別賞～

「考えよう　やさしい　ＳＮＳ」
豊中市立第十五中学校有志


「金髪姉ちゃん」
園田東中学校１年２組
（尼崎市立園田東中学校）

「ネットに潜む危険」
神戸学院FYNA
（神戸学院大学附属高等学校）

「見逃さないで、小さな日常、素敵な一瞬」
ソーシャルメディア研究会 竹谷東田ペア

# 国家試験「工事担任者試験」に向けての取り組み

福井県立 奥越明成高等学校

電気科　教諭　葛葉 昌彦

## 学校紹介

本校は、平成23年4月、機械科、電気科、ビジネス情報科、生活福祉科（生活コース、福祉コース）の4学科2コースを設置する、本県初の総合産業高校として開校しました。「みがけ心と技」のテーマのもと、新しい時代に求められるスペシャリストとして、奥越地域の産業・文化を担う人材の育成を目指しています。職業系専門学校として「地域に親しまれる学校」「地域に信頼される学校」「地域に必要とされる学校」をモットーに、地域社会とのつながりを大切にした取り組みを続けています。

昨年度の卒業生も数々の国家資格を取得し、奥越地域をはじめとする県内外の企業や施設に就職したほか、大学・短大・専門学校にも数多くの生徒を送り出すことができました。開校6年目を迎えた本校は、「地域を創りだす学校」という自覚を持ち、地域社会の皆様と協力し合いながら、新しい「校風」「伝統」を築き、確固たるものにしていきます。

**校訓**

**自立**：職業系専門教育をとおして、技と心を鍛え、自立した社会人を目指し、自分の仕事を自分の力で責任を持って誠実に成し遂げる力を育成する。

**協調**：工業、商業、家庭、福祉と特徴の違う学科が一つの学校で学ぶことにより、お互いに友愛の心を持って協力し、一つのことを成し遂げる力を育成する。

**創意**：新しいアイディアを生かしたものづくり、ビジネス社会の新たな考え方、食材を生かした調理、新たな感覚のデザイン、創造性豊かな生活環境・福祉環境など、すべての専門教育において独創的な考えを生む力を育成する。

## 電気科紹介

電気を基礎から学習し、携帯電話・モーター・発電所に代表される電子技術・通信技術・電気機器・電力技術など生活を支える幅広い電気エネルギーの活用方法を学ぶとともに、進路実現に必要な多くの国家資格に挑戦します。

### (1)第1学年

電気基礎Ⅰ・情報技術基礎・工業技術基礎を学びます。12月に第二級特殊無線技士を全員受験します。 利用区分別に細分化された周波数帯域の中で電波を使うための無線設備を操作できる資格で、海上と陸上の両方を受験します。この他にも、危険物取扱者試験を受験します。

### (2)第2学年

電気基礎Ⅱ・電子技術・電気機器・実習を学びます。6月にインターンシップに参加します。資格については、5月から第二種電気工事士の筆記について全員で取り組

み、6月に受験、合格者は実技に向けて取り組みます。この他、危険物取扱者試験や第一種電気工事士、工事担任者(AI･DD3種)を受験します。

**(3)第3学年**

通信技術・電力技術・製図・実習・課題研究を学びます。また発電所見学や工場見学にも参加します。資格については生徒一人ひとりが選択して受験し、第三種電気主任技術者・工事担任者(AI･DD1種)・消防設備士・2級電気工事施工管理技術検定など受験します。取り組みについては担当教諭がその都度グループで学習指導し、過去問を中心に学びます。

## 合格体験記

### 工事担任者1種合格

電気科　2年2組　**阿部 成希**

私は後期日程で工事担任者DD1種を受験しました。この資格を取得しようと思った理由は、すべてのデジタル回路への接続工事ができるようになるためです。将来、電気関係の仕事に携わりたいと思うので、単純な電気工事だけでなく、LAN、ルータ等の通信工事もできるように挑戦しました。

工事担任者試験では、基礎、技術＆理論、法規の3科目を1科目につき40分で解答します。勉強の仕方としては、過去問を繰り返し学習しました。基礎については電気基礎で学んだことが多く、理解していることがたくさんあったので、技術＆理論や法規について重点的に学習しました。クラス内に同時に受験する友人がいたので2人で2か月間にわたり勉強しました。本校の電気科では2年生で第1種電気工事士を受験するので電気工事の学習をしながらの勉強でしたが、先生や友達のおかげで合格することができました。3年生ではAI、DD総合種を目指して勉強したいと思います。

### DD3種への取り組みについて

電気科　3年2組　**竹生 祥大**

私は前期日程で、DD3種を取得しました。この資格に挑戦した理由は、ジュニアマイスター制度のゴールドに到達しいと思ったからです。基礎は私が今まで授業で習っていた部分があり、復習程度の内容で特に苦戦することもなく進めることができました。しかし、技術や法規については習ったことがあまりなく、しかも覚えるべき内容も多く、初めて出てきた語句については問題集を繰り返し解いたり、先生に解説してもらって理解しました。また、部活動との両立も大変でした。空き時間を見つけながら毎日少しでも勉強するようにして進めてきました。計画的に学習できたおかげで、DD3種に合格することができました。

現在はDD1種に向けて勉強中です。前回のDD3種挑戦から時間が空いてしまったため、忘れている部分もありますが、授業でさらに詳しく学んでいるので、今後さらに合格に向けて頑張りたいと思います。

# 大学入試改革とICT

株式会社情報通信総合研究所　研究員　**安藤 雅彦**

**日々、暖かくなり春の訪れを感じる季節となりましたが、3月といえば入学試験の最終盤。長くて辛い受験生活もあと少しの辛抱ですね。**

**既にご存じの方もいるかとは思いますが、大学入試改革の目玉として、現在の大学入試センター試験は廃止となり、2021年（2020年度）から新たなテストが導入されます。これは一見、ICTとは無関係に思えますが、実は新テストを支える役割としてICTの活用が期待されているのです。本稿では、大学入試改革とICTの関わり合いについてみていくことにします。**

## 1 大学入試改革の背景

そもそも、なぜ現在の大学入試センター試験を廃止し、新しいテストを導入するのでしょうか。文部科学省の作成資料「高大接続改革について[1]」では、高等教育および大学入試制度の改革の必要性について、次のように述べています。

工業社会から情報社会への転換やグローバル化の進展、成熟化・少子化時代、産業構造や就業構造の変化など大きな社会変動が起こる中、子どもたちは先を見通すことが難しい時代を生き抜いていく必要があります。そこでは、多様な人々と協力しながら主体性を持って人生を切り開いていく力が重要であり、混沌とした状況の中に問題を発見し、答えを生み出し、新たな価値を創造していくための資質・能力の育成が重要であるとしています。具体的には「学力の3要素」として

①知識・技能の確実な習得
②思考力・判断力・表現力
③主体性を持って多様な人々と協働して学ぶ態度

をあげています。

こうした新しい学力観を踏まえ、高等学校の授業も先生が一方的に知識を伝達する講義型のみならず、アクティブラーニングなど生徒が主体となる授業も取り入れ、「学力の3要素」をバランス良く身につけることが求められるとしています。

実はこのような認識や変革の必要性は現在でも叫ばれているのですが、高等学校に関しては十分に浸透していないのが現状です。その要因として考えられているのが、大学入試で求められている学力とのギャップです。大学入試の問題は知識の暗記・再生や暗記した解法パターンの運用の評価に偏りがちなため、高等学校は知識伝達型の授業スタイルからの脱却が難しいという状況に陥っていると考えられています。

そこで単に高等学校の教育課程や授業の在り方を見直すだけではなく、大学入試をも一体化して改革することで、「学力の3要素」を育む仕組みの構築を目指しているのです。

## 2 新テストの概要とICTとの関わり

新テストは「高等学校基礎学力テスト（仮称、以下「基礎テスト」とする）と「大学入学希望者学力評価テスト（仮称、以下「学力評価テスト」とする）の2つが導入されます（**図表1**参照）。

前者は2023年度からの本格実施が予定されている新たなテストです。「基礎テスト」義務教育を含めた高等学校段階における基礎学力の定着度合いを把握することが目的であるため、問題のレベルは基本的な「知識・技能」が中心です。「基礎テスト」の対象者は高校生で、原則、学校単位での受検となります[2]。受験科目や受験時期、受験学年なども学校が判断して利用できる仕組みを想定しています。テスト結果は生徒の学習指導や学校における指導の工夫・充実に活かすといった基礎学力定着度合いの把握と改善に役立てることを目的としていますが、将来的には推薦入試や就職などでの活用も考えられます[3]。

後者は名前のとおり、大学入学希望者を対象に行われる

図表1　新テストの枠組み

| | 高等学校基礎学力テスト（仮称） | 大学入学希望者学力評価テスト（仮称） |
|---|---|---|
| 目　的 | ●高等学校段階における生徒の基礎学力の定着度合いを把握・提示する仕組みを設けること | ●大学教育を受けるために必要な能力について把握すること |
| 対象者 | ●高校生（学校単位での受検が基本）<br>※高等専修学校在籍者、既卒者などの受検も可能とする | ●大学入学希望者 |
| 教科・科目 | ●試行実施では「国語」「数学」「英語」で実施<br>●2023年度からは新学習指導要領における必履修科目を踏まえた教科・科目構成とする | ●学習指導要領下における基本的枠組み |
| 問題レベル | ●基礎的な「知識・技能」を問う問題が中心 | ●「知識・技能」に加え、「思考力」「判断力」「表現力」の評価を重視した問題 |
| 出題方式 | ●マークシート方式<br>●短文記述方式を一部施行実施 | ●マークシート方式<br>●記述方式（当面は国語・数学） |
| 受験回数・時期等 | ●学年や時期、教科・科目等について学校または設置者において適切に判断できる仕組みとする<br>（受検学年や受検科目などは学校等において判断）<br>●学校単位での受検にあたっては原則、学校で実施 | ●複数回数の実施については今後の検討課題<br>●マークシート方式と記述方式の試験日をわけることも検討 |
| ICTの利活用 | ●CBT方式の導入をベースに検討<br>※当面は紙による実施も念頭に置く<br>●IRTを導入する方向で更に詳細に検討 | ●CBT方式導入による資格試験的な取扱の可能性については引き続き検討<br>●採点業務を効率的・安定的に実施する補助として、コンピュータを効果的に活用 |

出典：高大接続システム改革会議「高大接続システム改革会議　最終報告」（2016年3月）を基に筆者作成

テストで、現在の大学入試センター試験と置き換わる形で2020年度からの実施が予定されています。「学力評価テスト」の特徴は、前述した「学力の3要素」の2つめに掲げられている「思考力・判断力・表現力」を中心に評価することです。このため、大学入試センター入試でも採用されている「マークシート方式」に加え、新たに「記述式」回答が導入されます。

こうした新たなテストの導入・実施に際し、期待されているのがICTの活用です。具体的には「CBT」「IRT」「コンピュータによる採点支援」の3つのキーワードがあげられます。

## 3 大学入試改革を支えるICT

### 3-1 CBT

CBTとはComputer-Based Testingの略で、コンピュータを使って実施するテスト方式のことです。国内の入学試験においてCBTを導入している事例はまだ少ない[4]のですが、資格試験や検定試験などに目を向けてみるとCBTは身近な試験になりつつあります。

国内で比較的古くからCBTを導入しているのは日本漢字能力検定（漢検）です。漢検は2003年よりCBTを導入しており、2級から7級までの試験をCBTによって受検することが可能です。2014年度は約2万人の受検者がCBTを選択しています[5]。漢検でのCBT受検のメリットは自分の都合にあわせて受検できることにあります。既存の紙ベースの試験では年数回の指定日に受検をする必要がありますが、CBTではより多くの受検日が設定されているのです。

漢検では漢字の書き取りなどの記述式問題も出題されますが、キーボートとペンタブレットを用意することで、読み問題や選択問題はキーボード入力し、記述式問題はペンを使ってタブレットに直接文字を記述するという使い分けが行われています。

実用英語技能検定（英検）も2014年から2級と準2級においてCBTを導入、2017年1月の1次試験では全国13都道府県でCBTが実施されました。さらに英検では、面接試験（2次試験）でもCBTでの受検が可能となっています。受検者は遠隔地にいる面接委員とオンラインでつなぎ、ヘッドセットとマイクを使って面接試問が行われているのです。

米国の大学・大学院への留学に必要なTOFEL®も紙のテストからCBTに移行した試験のひとつです。現在でも一部に紙のテストが残っているようですが、世界の受験者の96%がCBTであるTOFLE® iBTテストを利用しています[6]。

こうしたCBT方式のテストは、従来の紙方式のテストに比べてどのようなメリットがあるのでしょうか。主なメリットとして、次の3つが指摘できます。

**① 音声や動画など多彩な出題・回答方法**

CBTでは動画や音声など紙では表現できないコンテンツを使った出題が手軽に行えます。加えて、回答にあたってもマイクを使って音声を録音するといったことが容易に行えるため、英語のスピーキング能力を測るテストなどが実施可能となります。

**② 即時採点**

CBTの場合、選択式などではその場で即時採点が可能です。紙方式の場合、たとえマークシート方式であってもシートを回収してスキャニングする時間やマーク読み取りエラーの対応などCBTに比べると時間を要するといえるでしょう。ちなみに以前の英検CBTでは、受検が終了したその瞬間に1次試験の合否判定が行われていました[7]。

**③ 回答者に応じたフレキシブルな出題**

即時採点をさらに応用することで、回答者の回答状況・正答状況に応じて、個別の試験問題を出題することが可能になります。たとえば、共通問題の正答率が高い回答者は、より高度な問題を出題して応用力を試すといったようなこともCBTなら可能です。したがって、同じ英語の試験といっても、実は隣の人とは全く異なる問題を解いていたということもCBTでは起こりうるのです。こうしたフレキシブルな出題を行うことで、個々人の能力をより詳細に評価、判定することが可能となるのです。

このようなメリットがあるCBTですが、新テストでのCBT導入には課題もあります。

「学力評価テスト」においては50万人超の受験生が対象となることが予想[8]されるのですが、これだけの大規模なCBTをトラブルなく実施できるのかという指摘です[9]。一方の「基礎テスト」においても、学校でのテスト実施が想定されているものの、高等学校のパソコン整備は心許ない状況なのです。文部科学省の「学校における教育の情報化の実態等に関する調査」によると、2016年3月時点での高等学校の教育用コンピュータ1台当たりの児童生徒数は5.0人/台[10]ですが、第2期教育振興基本計画で掲げた「2017年度に教育用コンピュータ1台あたりの児童生徒数3.6人/台[11]」という目標を達成するのは難しい状況です。

CBT導入に向けては、こうしたハード面の整備やセキュリティを含めた安心できる試験環境をどのように整えていくかを検討していくことが必要となるでしょう。

## 3-2 IRT

IRTはItem Response Theory（項目反応理論）の略称で、複数回数受検する場合に回ごとの試験問題の難易度差による不公平を排除するための理論です。理論ですからICTそのものではありませんが、前述したCBTとIRTを組み合わせることで、CBTの価値をより高めることが可能となります。

IRTは複数回のテスト実施における不公平感を軽減することに役立ちます。先ほど、高等学校のハード整備不足をCBT導入の課題のひとつにあげましたが、IRTを導入することで、テスト時期をずらしてCBTを実施してすることができます。また、コンピュータ等のトラブルといったCBTの脆弱性についても、IRTで複数回受検可能という仕組みがあれば安全性の担保に繋がるといえるでしょう。

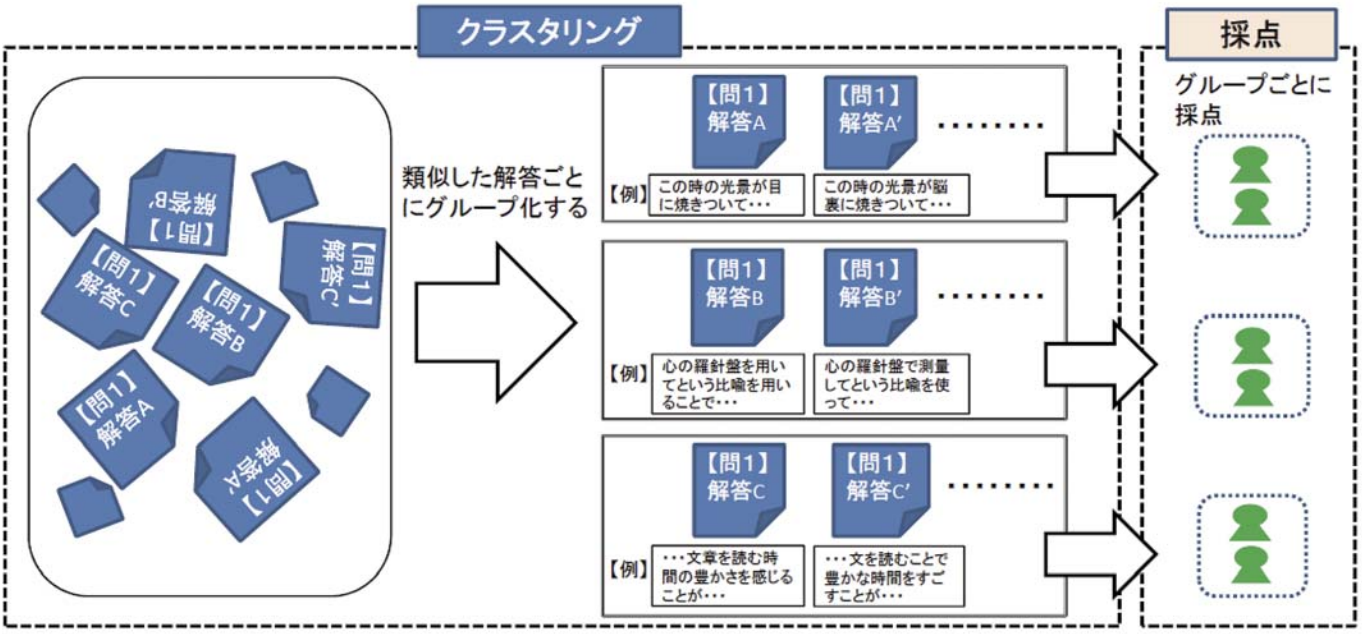
精度の高いIRTの実施を考えた場合においてもICTは強力な味方となります。IRTを行うためには大量のテスト問題の蓄積が必要となるため、ICTの力が必要不可欠となります。さらにCBTでは即時採点が可能であるため、IRTを使って大量の問題データベースの中から回答者のレベルに合わせた問題を即時に抽出、出題することも可能となります。

新テストをいつでも、どこでも受けられる…CBTとIRTを組み合わせることで、そんな便利な時代がくるかもしれません。

## 3-3 コンピュータによる採点支援

「学力評価テスト」では記述式問題が出題されますが、記述式問題の採点には時間と手間が必要となる上、採点の公平性も課題となってきます。こうした課題を解決するため

図表2　クラスタリングによる採点支援のイメージ




出典：高大接続システム改革会議「高大接続システム改革会議　最終報告　高大接続システム改革会議参考資料2」(2016年3月)より引用
http://www.mext.go.jp/b_menu/shingi/chousa/shougai/033/toushin/1369233.htm

に、人工知能などを活用したコンピュータによる採点支援の導入が検討されています。

具体的にはデジタル化した記述式回答を、キーワードや文書構造などを基に自動的にクラスタリング(類似グループに分類すること）した上で、採点者はグループ毎に採点を行うという手法の導入が想定されています（**図表2**参照)。これにより、採点効率が向上、採点時間の短縮や採点のゆらぎを少なくすることにつながると考えられています。

究極的には人工知能やディープラーニングを活用した記述式回答の自動採点も考えられます。しかし、文部科学省では現在の技術水準で実現可能であることを重視し、人工知能等のコンピュータ技術を支援側面として活用することを検討しています。

## 4 おわりに

今まで見てきたとおり、今回の大学入試改革によって、入試におけるICTの存在意義は今まで以上に高まることでしょう。あわせて、文部科学省は、「学力評価テスト」のクラスタリングや「基礎テスト」の運営などにおいて民間事業者の知見やノウハウを最大限に活用していくことが望ましいとしています[12]。大学入試改革はICT事業者に新たなビジネスチャンスをもたらす好機であるとも言えるでしょう。

1　文部科学省高大接続改革PT「高大接続改革について」(2016年1月29日)
http://www.mext.go.jp/component/a_menu/education/detail/__icsFiles/afieldfile/2016/03/15/1367221_4_1.pdf
2　希望する個人(既卒生や社会人など)の受検も可能としています。
3　試行期間中は就職や入試などへの活用は禁止されています。
4　たとえば佐賀県の私立龍谷高等学校では総合コース専願者を対象にCBT入学試験を導入しています。
5　公益財団法人日本漢字能力検定協会webサイト
http://www.kanken.or.jp/kanken/cbt/characteristic.html
6　国際教育交換協議会日本代表部(TOFLEテスト日本事務局）webサイト
http://www.toefl-ibt.jp/toefl_ibt/format.html
7　英検2級に記述式英作文が導入されたことに伴い、即日の合否判定は行われなくなりました。
8　2017年度の大学入試センター試験の志願者は575,967人。
9　産経ニュース「新大学入試文科省素案…「CBT方式50万人」前例なく　課題はシステムの安定性」(2015年6月18日)
http://www.sankei.com/life/news/150618/lif1506180036-n1.html
10　文部科学省「学校における教育の情報化の実態等に関する調査結果(平成２７年度)」(2016年10月)
http://www.e-stat.go.jp/SG1/estat/Pdfdl.do?sinfid=000031462110
11　3.6人/台は①コンピュータ教室40台、②各普通教室1台、特別教室6台、③設置場所を限定しない可動式コンピュータ40台を整備することを目標として算出した数値。
12　文部科学省「高大接続改革の進捗状況について」(2016年8月31日)
http://www.mext.go.jp/b_menu/houdou/28/08/1376777.htm

# Pマークの事故増加は由々しきことなれど

一般財団法人日本データ通信協会　Pマーク審査部　**中山　隆**

**この1月、プライバシーマークの仕事に携わっている同僚の間で話題になった新聞記事がありました。読売新聞が1月10日夕刊に掲載した「Pマーク企業　情報「事故」2000件」と題した記事がそれで、Pマーク取得事業者が1万5千を超えたが、それらの事業者が報告する事故の数も同様に増え、2015年度は前年比で約2割も増加し、1947件にも上っている」というものです。副題には「昨年度　「管理「適切」認定　信頼揺らぐ」とあります。**
**形骸化した制度ほど、ものの役に立たないものはありませんから、この記事の見出しは関係者にとってはショッキングです。Pマークのあるべき方向性について、「事故」と「事故報告」を例に考えて見ます。**

## 報告されている事故の内実はさまざま

前向きに個人情報を保護していこうとする事業者に対して、Pマークはいくつかのツールを提供していますが、その中で重要なのが、今回の新聞の記事で槍玉に挙げられている「事故報告」です。

私ども日本データ通信協会の場合、平成27年度の1年間で92件の事故が認定を行った事業者から報告されました。1社で複数回の事故を報告している事業者もありますので、事業者数で数えると報告をもらったのは40社になります。これまで私どもでPマークを取得した事業者は約1200社ですので、この年、取得事業者の3パーセントの事業者から事故報告が上がってきていることになります（ちなみに平成28年度は第3四半期まで終わった時点で事故件数が52件ですので、1年前よりも報告数は減る傾向にあります）。

明らかに重い事故から、うっかりミスで起こったごく軽い事故まで、私どもには軽重さまざまな事故が報告されます。手練手管を弄したサイバー犯罪者に自社サーバに侵入されて個人情報を盗み見されるのは紛れもない重大な事故ですが、一方では「取引先のA社の佐藤さんに送るべき挨拶メールを、間違えて取引先のB社の佐藤さんに送ってしまった」であるとか、「釣りをしていた社員が取引先の電話番号を保存している会社の携帯電話を海の中に落とした」などといった、影響の及ぶ範囲がごく軽いケースもその中には含まれてきます。

Pマークの運用にまじめに取り組んでいる事業者であればあるほど、一般的に考えて軽いと見られるような事故も丁寧に報告する傾向があり、報告回数も多くなってきます。

## 事業者の報告はどのように処理されるか

Pマーク制度において事故報告が重要なのは、事故を起こした事業者に、事実関係の報告とともに再発防止策を立ててもらい、それも合わせて報告をしてもらうという仕組みを組み入れているからです。

事故の内実は、実際にはそれぞれのケースで個別具体的です。事業者が実施する安全管理措置の内容や程度も違っていますし、従業者の管理の仕方や日常講じている保護施策もそれぞれ異なります。そもそもセキュリティや個人情報保護にかけることができる社内資源の多少も事業者によってさまざまです。その中で事業者には、身の丈にあった、しかし実効性のある施策を重ねて個人情報保護の程度をスパイラルアップしてもらうことが重要です。

事故報告を受けると、月に一度の審査会において有識者の委員が対応の妥当性を審議し、審議結果を事業者に報告します。審査会では、事故を起こした事業者が意味のある対策を講じようとしているかを観察し、施策が不十分だと思われたり、的外れだと考えられたりする場合には、当該事業者には、よりしっかりとした対応を行ってもらうよう指導を行っています。さらに次のPマーク更新審査の際にも、担当審査員が事故対応施策の実効性の確認を行っています。

こうした意思疎通を通じて、事故報告が単なる報告だけに留まることがないように心がけています。

## 必要とされるのは改善につながる報告

事故は少ない方がいいに決まっています。最終的には事故や苦情がなくなることが個人情報保護の理想郷ですが、現実には、生身の人間の行いにミスはつきものですし、情報システムが高度化されれば、そこに新たなリスクも生まれます。攻撃を考える側の技術も進歩します。ですから、対策をまじめに採り続けている組織ですら、どこかで事故を起こすのは不思議ではありません。事故は残念ながら起こるものだとすれば、まず重要となるのは、事故の発生を組織が確実に把握することです。そこが対策の一里塚だと言ってもよいでしょう。

そうすると、アイロニカルな話なのですが、まじめに対策をしようとしているPマーク取得事業者が、「事故報告」を繰り返すということが起こりえます。

私がすぐに思い出すのはA社さんの例です。私どもでPマーク審査を継続しているA社さんは、新しい社長の号令の下、セキュリティや個人情報保護関連の事故に本腰を入れ始めました。すると、同社からの事故報告は増え、一昨年には年に十数件と、私どもの審査企業では突出した報告件数を数えることになってしまいました。

これで終われば、A社さんは単に事故が多い企業だ、けしからん会社だという話になりそうなのですが、こうした取組みを通じ、A社さんは真摯な事故の原因追究と効果のある対策を地道に進め、続く1年では事故報告がほとんどないぐらいまでに成果を出したのです。

## 事故を隠さない覚悟が大切だ

A社さんの例は、もしかしたら、よい意味で特異な例かもしれず、いずれの企業も同じように理想的な結果を得られるとは言えませんが、それでもここには、単純だけれど大事な教訓が示されています。

事故を隠さないのが大事だということです。事故の報告は、それ自体が面倒な作業ですし、ことさら自社のマイナス面をさらすようで格好悪いですし、あとで事務局である私どもからどんな沙汰があるかもしれないと考えたりすると、報告を避けたがる事業者が出てくるのは想像に難くありません。

これは単なる個人の感想に過ぎないので、（幸い）間違っているかもしれないのですが、事故報告の記録を数年にわたって眺めてみると、複数回の報告を行っている企業がいくつもある半面、一度も事故を報告していない企業がその何倍も、何十倍もあります。これを文字通りにとれば、事故を経験している企業の方が稀なわけで、これはなかなかたいしたものだとは思いますが、報告されていない事故がないのかどうかは、やはり心配になります。

Pマークは、参加する事業者が自組織で個人情報保護の取り組みを向上させるための仕組みをJIS規格に基づいて提供する民間の制度ですので、参加する事業者自身、もっと言えば、その組織の代表者に本当のやる気がないかぎり、マークには意義も有難味もなくなってしまいます。その一環である「事故報告」も同様で、これは参加する事業者の皆さんが自ら率先して報告するところに最初の意義があります。審査機関等が事故の発生がないかを見張って、法令違反を取り締まっている訳ではありません。

つまり、事故自体は由々しきこととは言え、事故報告を行うことは奨励されるべき事柄なのです。Pマーク制度によって事故報告が義務付けられ、それによって客観的な状況が明らかになり、次に打つべき施策が明確になって、そのやるべきことが社内全体で意識される。事故報告は、そのように運用されることによって、本来期待される効果を発揮します。

## Pマーク審査部も事業者の皆様と一緒にがんばります

日本データ通信協会Pマーク審査部では、マネジメントシステムの原則に則って自発的な改善の努力を推進する事業者の努力を、審査の場を通じ、また、事故報告や苦情処理の制度を通じ、あるいはPマーク取得事業者向けイベントの開催やホームページ等による情報発信を通じて支援し続けていきたいと考えています。

事故報告はサボろうと思えばサボれる。それをしない事業者の存在がある。あらゆる事業者がそうした誠実さを体現するようになる時が来ることを理想に、私どもも事業者の皆様のお力になれるよう今後も精進していく所存です。

2016年1月号から1年少々の間、個人情報保護の話題をめぐって書き続けてきたこの連載コラムは、これが最終回となります。私どもの機関誌は、今後情報発信の場を当協会ホームページにも拡大し、新しい体裁と内容で皆様にとって意義のある情報発信を続けていく所存ですので、読者の皆様におかれましては、引き続きご愛顧のほどよろしくお願いいたします。

## Report 1 総務部

### ●平成28年度第3回理事会開催

平成29年3月7日に、平成28年度第3回理事会を開催しました。

議題として「平成29年度事業計画」及び「平成29年度収支計画」の提案がなされ、原案どおり議決されました。

平成29年度においても、より一層の公益の増進に寄与すべく、協会の2本柱である「情報通信セキュリティ対策」と「情報通信分野における人材育成」に取り組んでいきます。

## Report 2 迷惑メール相談センター

### ●2017年度版「撃退！ 迷惑メール」「撃退！ チェーンメール」を配布します

迷惑メール相談センターでは、ホームページで迷惑メール・チェーンメール対策資料「撃退！ 迷惑メール（迷惑メール対策BOOK）」、「撃退！ チェーンメール（チェーンメール対策BOOK）」の無償配布を受け付けています。

「撃退！迷惑メール」では、騙されないように気をつけたい「メールde詐欺」のメールや被害事例をもとに作った「ヒヤリ・ハット体験SONG」、急速に普及しているスマートフォンのセキュリティやインターネットを利用する際の注意点などを紹介しています。

「撃退！チェーンメール」では、チェーンメールの実態などを詳細に説明するとともに転送してはいけない理由をわかりやすく解説しています。

どちらも配布は無償です。お申し込みは、次の迷惑メール相談センターホームページでお願いいたします。

http://www.dekyo.or.jp/soudan/


迷惑メール詐欺被害防止啓発キャラクター：サギかもファミリー


## Report 3 Pマーク審査部

### ●プライバシー（P）マーク認定事業者が1,394社になりました（平成29年2月10日現在）

認定事業者一覧は、Pマーク審査部のホームページよりご覧ください。

http://www.dekyo.or.jp/pmark/ninteijigyousha/a.html

## Report 4 電気通信国家試験センター

### ●電気通信主任技術者試験（28年度第2回）の実施結果

平成28年度第2回電気通信主任技術者試験（1月22日実施）の結果が2月13日に発表されました。

今回試験の受験者数は、3,855名で、そのうち720名が合格（合格率18.7%）しました。

合格率については、前回試験（平成28年度第1回）に対し、1.4%減となっています。

なお、次回試験（平成29年度第1回・7月実施予定）の申請受付は、4月1日からですが、受験用試験申請書類は3月から頒布しています。

### ●工事担任者試験（29年度第1回）の試験実施

平成29年度第1回工事担任者試験は5月28日（日）に実施します。

## Report 5 人材研修部

### ●工事担任者養成課程eLPIT（エルピット）

- 平成29年2月1日から教育担当者の方も受講者と同じようにWindows版アプリが使えるようになりました。USBキー使用時とメニューは同じですが、インストール等使い易くなりましたので、受講者の学習状況把握などより一層のご活用をお願いいたします。
- 総受講者数は、12,523名になりました。（平成29年1月23日現在）

今後の開講予定（平成29年）

4月3日、11日、21日／5月1日、11日、22日／6月1日、12日、21日

eLPIT受講申込みは、eLPITホームページをご覧ください。

http://www.elpit.dekyo.or.jp/elpit/

## Report 6 事業推進部

### ●電気通信主任技術者定期講習の公示

電気通信主任技術者講習の登録講習機関として、平成29年度講習の公示を4月4日に行います。平成29年度は9月と12月に東京で予定しています。

最新情報は次のURLでご確認ください。

http://www.dekyo.or.jp/jinzai/

### ●「情報通信エンジニア」団体別ランキングの公開

平成29年3月末現在の情報通信エンジニア資格者の団体別ランキングを協会ホームページに4月10日頃アップの予定です。

3月末と9月末の2回実施しております。下記のURLでご確認ください。

http://www.dekyo.or.jp/engineer/contents/ranking.html

# 読者の皆様へのお知らせ
# （編集後記に代えて）

## ◆今夏、機関誌『日本データ通信』がリニューアルオープンします

『日本データ通信』は、これまで多くの皆様に支えられ、本号で214号を迎えることができました。これもひとえに読者の皆様のご愛顧とご支援の賜物と、編集部一同厚く御礼申し上げます。

さて『日本データ通信』は、皆様のご期待にさらに充実した内容で応えるべく、新年度に久々のリニューアルを敢行します。

**■コンテンツをWebでも提供します**

A4判の印刷物で提供を行ってきたコンテンツを、従来の紙メディアに加えて当協会のホームページで電子版としても提供していきます。

これまでも毎号のpdfを日本データ通信協会のホームページに掲載して来ましたが、今後は協会ホームページに連動したWebマガジンの形で提供しますので、読みやすさは格段にアップします。また記事はアーカイブ化していく予定ですので、過去記事への参照が容易になるなど、利便性も向上します。

**■季刊の紙媒体と随時更新のWebマガジンとで機動性を発揮します**

隔月刊だった印刷版は年4回の季刊になります。紙での提供回数は減りますが、Webでの記事掲載は、定時の提供にこだわらず、新しい記事が準備でき次第ご覧頂く予定ですので、機動性は向上し、より新鮮な記事提供をご覧いただけます。

**■特集記事を充実し、新しいシリーズも準備します**

コンテンツは、ご好評を頂いてきた識者へのインタビューや特集記事をさらに充実させていくとともに、当協会の活動を紹介する読み物をシリーズで提供していきます。

データ通信やセキュリティ、個人情報保護にまつわる分野の最新の情報をご提供すると同時に、私どもの活動について広くご理解頂くよう努める意味で、目指すところはこれまでと何ら変わりませんが、従来の編集方針に一工夫を加え、より分かりやすく、読者の皆様にとって有益な機関誌となるよう尽力していく所存ですので、一層のご支援をお願い申し上げます。

## ◆当協会のロゴが変わりました！

目ざとい読者の方は、本号の表紙や裏表紙の変化にすでにお気づきかもしれませんが、この3月から当協会のロゴが新しくなりました。新しいロゴはご覧のとおり。従来のロゴに右上がりの成長を象徴するウェーブを加え、データ通信分野のダイナミックな営みを表しています。

今後、様々な機会に新しいロゴを用いて当協会を紹介させて頂きますので、こちらもどうかご贔屓のほどお願い申し上げます。


旧ロゴ　　新ロゴ

**【訂正とお詫び】**

前号コラム内のグラフ「位置情報に対する許容度」の項目ラベルのテキストに誤りがありました。内容を以下のとおり訂正するとともに、謹んでお詫びを申し上げます。

（誤）どんな場合でも許容できる　→　（正）どんな場合でも許容できない

**日本データ通信【通巻214号】**

発行所：一般財団法人日本データ通信協会　発行人：井手 康彦　平成29年3月発行
〒170-8585　東京都豊島区巣鴨2-11-1　巣鴨室町ビル6F・7F　☎03-5907-5139

JADAC 国家試験

# 電気通信主任技術者試験

## 平成29年度 第1回 試験実施日

**平成29年7月9日(日)**

**申請書受付期間**

| 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29年4月1日(土)～5月10日(水) | 平成29年5月11日(木)まで |
| 郵送申請 | 実務経歴の申請がない場合 | 平成29年4月1日(土)～5月10日(水) | |
| | 実務経歴の申請がある場合 | 平成29年4月1日(土)～4月20日(木) | |

**合否発表** 平成29年7月31日(月)

## 平成29年度 第2回 試験実施日

**平成30年1月28日(日)**

**申請書受付期間**

| 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29年10月1日(日)～11月8日(水) | 平成29年11月9日(木)まで |
| 郵送申請 | 実務経歴の申請がない場合 | 平成29年10月1日(日)～11月8日(水) | |
| | 実務経歴の申請がある場合 | 平成29年10月1日(日)～10月20日(金) | |

**合否発表** 平成30年2月19日(月)

**試験実施地** 全国15ヶ所を予定

**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科目履修者等は、申請により試験が免除される科目があります。

**試験種別**
- 伝送交換主任技術者試験
- 線路主任技術者試験

**試験手数料** 16,600円～18,700円 *受験科目数による
(全科目免除9,500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

http://www.dekyo.or.jp/