

No.218 2018.4 / April

日本データ通信

INFORMATION FROM JADAC AND EXPERTS

» 特集

貴社の 「なりすましメール」対策、 進んでますか？

» トップインタビュー

井山7冠の国民栄誉賞受賞、囲碁とAI、電気通信政策

公益財団法人日本棋院 理事長 團 宏明 氏

» ICTセミナー

総務省3課長が語る電気通信政策の現在

今月の登場企業・組織

公益財団法人日本棋院、東京農工大学、総務省、富士通株式会社、アンテナハウス株式会社、株式会社アイ・コミュニケーション、山梨県立富士北綾高等学校（順不同）

CONTENTS

- 01 | **巻頭言**
一般財団法人日本データ通信協会 理事長 酒井 善則 p.01
- 02 | **トップインタビュー**
井山7冠の国民栄誉賞受賞、囲碁とAI、電気通信政策 p.02
公益財団法人日本棋院 理事長 團 宏明 氏
- 03 | **特集：貴社の「なりすましメール」対策、進んでいますか？**
「なりすましメール」の危険性と「DMARC」の可能性 p.08
一般財団法人日本データ通信協会 迷惑メール相談センター次長 西松 薫
- いま注目される「DMARC」** p.09
東京農工大学 大学院工学研究院 助教 北川 直哉 氏
- 『サイバーセキュリティシンポジウム道後2018』でDMARCの普及促進** p.13
- 04 | **ICT セミナー**
総務省3課長が語る電気通信政策の現在 p.14
総務省 総合通信基盤局 電気通信事業部 電気通信技術システム課 課長 荻原 直彦 氏
総務省 総合通信基盤局 電気通信事業部 データ通信課 課長 内藤 茂雄 氏
総務省 情報流通行政局 サイバーセキュリティ課 課長 木村 公彦 氏
- 05 | **インタビュー**
社内人材を可視化し、モチベーションを高める富士通の『セキュリティマイスター認定制度』 p.20
富士通株式会社 サイバーセキュリティ事業戦略本部 サイバーディフェンスセンター長 奥原 雅之 氏
- 06 | **JADAC Movement**
平成29年度 電気通信主任技術者定期講習を終えて p.24
一般財団法人日本データ通信協会 人材研修部 部長代行 飯田 秀男
- 07 | **challenge！ 工事担任者試験に挑む若者たち**
工事担任者試験、合格に向けたゼロからの出発 p.26
山梨県立富士北稜高等学校 電気情報系列 教諭 楠 秀樹 氏
- 08 | **タイムビジネスの担い手**
国税関係帳簿書類のスキャナ保存で拡大するタイムスタンプ利用 p.28
アンテナハウス株式会社 取締役 e-ドキュメントソリューショングループ
グループリーダー 益田 康夫 氏
- 09 | **Pマーク取得事業者の横顔**
株式会社アイ・コミュニケーション p.30
株式会社アイ・コミュニケーション 代表取締役 目次 真司 氏

教育のICT化となりすまし

一般財団法人日本データ通信協会 理事長 酒井 善則

私は昨年3月まで通信制大学である放送大学に勤務していた。通信制大学の究極の目的は、大学の機能としての質を落とさずに可能な限りICTで実現することだと思う。しかし、現実には放送大学にはスクーリングである面接授業、テレビ、ラジオ等の放送授業の期末試験である集合形の単位認定試験があり、ICTで全ての大学の教育機能を代替することは困難であることを実感した。大学の講義を公開するOCW（Open Courseware）、更にはQ&Aによる習熟度チェック機能も持つMOOCs（Massive Online Open Courseware）等のICT応用が進んでいるが、単位となる講義の全てをICT化するのは現状では困難なのかもしれない。

教育には、何らかの形で学び手に学習させることと共に、学び手の習熟度をチェックする機能の2種類がある。現在の講義形態では、なるべく実際の教師から話を聞く、実際のモノに触ることが良いこととされ、実際の講師が遠隔にいる場合の遠隔講義、実際のモノに触るのが困難な場合のシミュレータによる教育が行われている。すなわち、仕方なくICTを導入しているのが実情かもしれない。AI（人工知能）の進歩により不要となる職業にまだ教員は入っていない。一方、講義そのものの改良も進み、学生からの主体的動きを中心としたアクティブラーニング、ICTの活用を中心として学生の能動性を増す反転授業等の考えが提案されている。当協会においてもeラーニングによる工事担任者養成課程（eLPIT）が行われているが、ICT化で特に困難なのは不正防止であり、なりすましの一種である替え玉受講のチェックも重要である。不正防止さえ実現できれば、能力あるいは習熟度チェックはICTの得意分野であると思う。顔認証、人間の癖等により、リアルタイムに受講者のチェックを行う技術の開発が望まれる。

一方、次世代を担う若者の能力低下は深刻な問題として取り上げられている。AIにより東京大学合格を目指す“東ロボ君プロジェクト”は現状では困難ということで断念した。一方、同プロジェクトのリーダーである新井紀子教授によると、一部の若い人の論理的な能力不足は深刻であり、ソフトウェアを勉強する前に日本語を勉強すべきではないかと述べておられる。同様の話は私の周辺の大学教授からは良く聞き、一部の大学で学生はAIにかなわなくなっているのかもしれない。このままでは、多くの技術者がAIにより代替可能という職業になるかもしれない。

我が国のインフラである電気通信分野を設計管理する技術者については、AIの助けは必要であるが、AIにかなわない方にはなって頂きたい。協会でも多くの資格試験を担当しているが、これらは東ロボ君が簡単に合格するようなものではあってほしくない。ただ、教育、習熟度チェック等は可能な限りICT化して、誰でも学びやすく、受験しやすい資格とする必要がある。ICTを利用してICTに負けない人材を育てる必要がある。ICTの教育への応用は産業としての魅力は十分でないとの意見も聞いたことがあり、電気通信分野の人材を育成する協会の責務も大きいと考えている。

02 トップインタビュー

井山7冠の国民栄誉賞受賞、囲碁とAI、電気通信政策

公益財団法人日本棋院 理事長 團 宏明 氏



〔聞き手〕
一般財団法人
日本データ通信協会
専務理事
井手 康彦



日本棋院理事長の團宏明氏は、郵便・電気通信行政において数々の要職を歴任してこられた。電気通信の世界では、1999年のNTT再編成の際に、郵政省電気通信局電気通信事業部長として今日の電気通信産業における公正競争のあり方にかかわってこられた功績が知られている。

インタビューが行われたのは、大きなニュースとなった井山裕太7冠の国民栄誉賞受賞の翌々日。旧知の間柄である当協会専務理事・井手康彦との肩の力を抜いた対談は、囲碁の過去と現在について、さらにNTT再編成当時の思い出についてと縦横無尽な広がりを見せた。

世界に広がる囲碁

井手 一昨日の井山裕太7冠の国民栄誉賞おめでとうございます。

團 井山先生と羽生先生の二人が同時受賞というのは本当によかったです。井山先生は、常日頃から羽生先生のことを尊敬されていて、羽生先生も井山先生の最初の7冠達成の際にお祝いの席でご挨拶を頂いたことがあるなどよい関係を築いてきていましたので、今回の同時受賞は囲碁将棋界にとっても本当によかったと思っています。

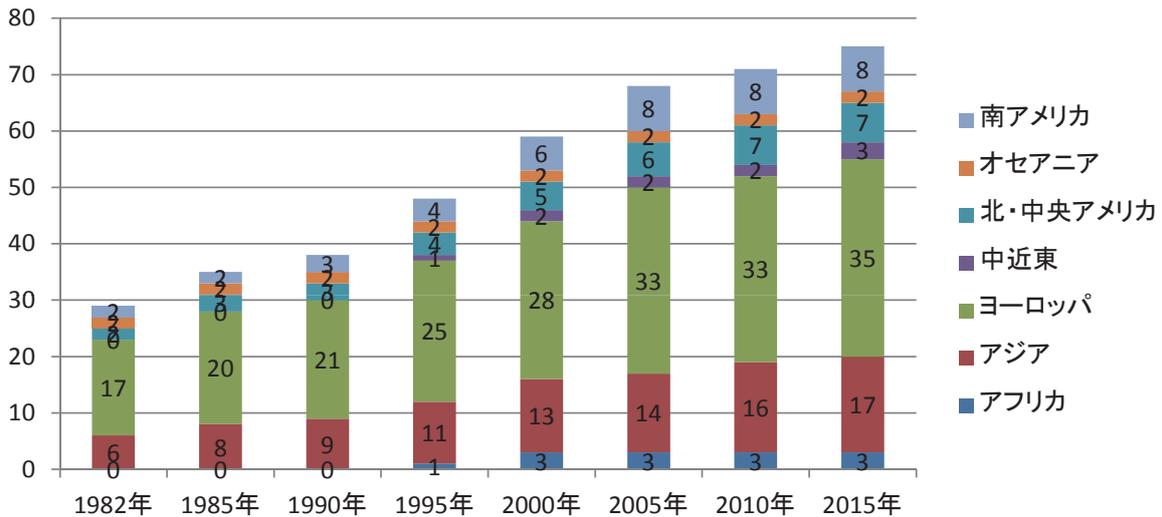
井手 囲碁界にとってはファンの拡大につながる国民栄誉賞受賞ですね。

團 将棋の方がたしなむ方の数は多いのですが、囲碁に将来性があるところは世界的に広がっている点です。国



日本棋院に掲げられた横断幕

図表1：国際囲碁連盟加盟国数の推移（2018年1月現在）



出所：日本囲碁連盟提供資料を基に編集部作成

国際囲碁連盟という組織があり、日本棋院もその発展に関わっています。今では77カ国が参加（2018年1月現在）して、日本、中国、韓国という強豪3カ国ばかりではなく、欧州諸国、米国、中南米、さらにASEAN諸国でかなり囲碁人口が伸びています。

井手 将棋は日本が中心なのですか。

團 将棋は国によってルールが異なります。例えば中国にも将棋がありますが、日本とは異なるものです。それに対して囲碁の世界は万国でほぼ共通です。日本には5世紀頃に中国から朝鮮半島を通じて伝わり、19路盤という今日まで使われている盤面を含めて平安時代にルールができています。当時、寛蓮上人という名人がいて、「碁式」という囲碁のルールや作法を定めたものを醍醐天皇に献上されたとされています。

その後の歴史を見ると、信長も、秀吉も、家康も碁を打っており、皆さんかなり強かったようです。よく大河ドラマなどで彼らが碁を打つ場面が出てきますが、あれは本当の話なのですね（笑）。

徳川家康は天下を治めた後にプロ棋士を作りました。家元制度を作り、俸禄を与えているのです。そこからプロ制度が始まって、その後様々な流派ができてくるわけです。

囲碁は中国伝来とも、もっと古くインドのあたりが発祥だとも言われていますが、きちんとルールを定めたのは平安時代の「碁式」ですし、「棋道」を大事にし、世界に先駆けてプロ制度を始めたのが徳川家康なんです。

井手 ところが、今では日本よりも中国や韓国が腕を上げているんですね。

團 私が碁を始めたのは50年も前の高校生の頃でしたが、その頃は中国にはあまり碁を打つ人がいないという状況でした。韓国も同様でした。そこに日本棋院の先生方が交流をして広めるということをしてきました。趙治勲先生なども韓国から日本にいらっやって勉強をされた。

それが今では、中国も、韓国も、囲碁人口が多く、日本の棋士が簡単には勝てないのが現状です。井山先生はそうした中で、世界で勝つこと、日本の棋道を世界に広めることを目指し、果敢に立ち向かっています。彼の努力は中国や韓国からも非常に評価されています。

今世界戦がとても増えていて、今年の正月早々にも雲南省で大会があり、井山7冠は14時間もかけて現地に行かれました。世界化は囲碁の大きな流れになっています。

こうした趨勢の中、日本棋院としても国際化の流れをさらに加速させようとしています。とくに東京オリンピックが行われる2020年には東京で複数のイベントを開催し、囲碁で世界をつないで『東京2020』を盛り上げていこうと計画中です。

井手 ルールは日本のものが使われているのですか？

團 そうです。中国で勝ち負けを決める石の数え方で少

02 トップインタビュー

し違うやり方をしているなどということはありませんが、基本的なルールは共通です。どこに行っても、同じ碁盤でゲームが楽しめるのは碁の素晴らしさではないでしょうか。

井手 どんどん普及をすると、柔道着がカラフルになった柔道のルール変更のようなことが起こらないですか？

團 それは碁の場合にはあまり心配する必要はなさそうですね。

ただ、今から20年ほど前に郵政省で働いていた頃には碁をやる方は多く、郵政省の全国碁連盟の会長を10年ほど務めました。その頃のことを思い起こすと、日本のメーカーがスポンサーとなって世界戦をやっていました。ところが、現在は棋力が上がった中国や韓国のスポンサーが世界戦を行う時代になっています。そこは印象深いです。井山先生はその中で現状を打破しようとしているわけで、日本の産業も同じように世界で頑張りたいところですね。

現在は井山先生がタイトルを独占している7つの大きな大会があり、これらは新聞社がスポンサーですが、新しいスポンサーによる大会も出てきています。女流棋聖戦のドコモ杯などは、その典型例です。これからは色々な企業さんと一緒にやっていければと思っています。

地域活性化への貢献、若年層への広がり

井手 様々なマーケティング活動（普及活動）を行っているようですね。

團 特徴的な活動の一つが地域への貢献です。千面打ちで有名な『湘南ひらつか碁まつり』はその代表例ですが、川越市の『川越碁まつり』や信濃大町の『アルプ



ス碁村』など多くの自治体で碁が町おこしに活用されています。近年は碁を通じて地域振興を目指す自治体が集まる「碁サミット」という催しを開催しており、各地域の日本棋院支部が自治体とタイアップし、東京の本院からも多くの棋士がサポートに行っています。熱心な自治体はどんどん増えていて、地域の中でのコミュニケーションを活発にするツールとして碁はその有用性を大変認められています。将来的には地方創生の柱の一つになりえるのではないかと思います。

碁のよいところは、若い人からお年寄りまで世代を超えて打てるし、国籍も超えて打てる。先週は静岡で『徳川記念世界碁まつりイン静岡』というイベントがありましたが、日本に加え世界12カ国から参加者がありました。老若男女、皆さんに碁を楽しんで頂きたいと思います。

井手 子供たちも打っているんですか？

團 増えていますね。小中学校でも2万人くらいの方が課内・課外授業として受けていて、大学でも40校ほどが正規の授業として単位が取れるようになっている。前理事長の和田さん（元NTT会長の和田紀夫氏）の貢献が大きかったと思いますが、学校に対する普及活動が実践されているのは以前にはなかったことで驚いたことでもありました。夏場には高校選手権など大会もありますけれども、教育に熱心な学校で取り上げられて、集中力や粘り強さを養い数学的な感覚を育む、あるいは礼儀を学ぶなど、学業にもよい影響を与えているようです。

碁盤も昔は19路盤という正規の大きさしかなかったのですが、13路盤、9路盤、7路盤、6路盤、さらには4路盤というものまで出てきています。少ない升目なのに驚くほど多様な打ち手があって、若い人たちを教える先生の教え方も研究が進んでいます。

面白い話があって、その先生方によると若い人たちは覚え方が違ってきているというんです。子供たちには「よく考えて打て」と言っては駄目だというんですね。感覚で打って、やっているうちに感覚的に覚える。覚え方が昔と全く違うので、教え方も違ってきます。

碁が明らかにするAIの可能性

井手 定石など知識を植え付けるような教え方ではないということですね。

團 そのとおりです。やっているうちに覚えるということですね。この話がAIの話題につながってきます。

井手 今のAIソフトは機械同士の多くの対戦で経験を積み、自ら学習して強くなるようですね。

團 そうなんです。AI囲碁では、グーグルの『AlphaGo』が急速に強くなって、そこで用いられた「ディープラーニング」という方法が話題になっています。従来は人間の棋士が打った棋譜を覚えさせることで強くなっていた。

井手 「ビッグデータ」ですね。

團 「ビッグデータ」の最たるものです。ところが1年ほど前からグーグルは棋譜なしでコンピュータに自ら碁を覚えさせるということを始めました。やってよいこと、よくないことの基本的なルールを示した上で、いわばデータラメにAIに碁を経験させ、AI同士で何十万局も打つことでAIが自分で勝つ方法を覚える。これは先程お話をした子どもたちの覚え方と通じるものがあります。面白いことだなと思います。

「ディープラーニング」の手法を用いると、AIは最終的に勝利する方法を手に入れますが、勝利に至る過程、どうしてその時にその手を打つのかというプロセスについては、人間には十分に説明がつかないことが多い。既存の理論や定石に基づいて打っているわけではないのです。

ということは、「ルールが決まっているものはAIができるようになる」ということではないかと思うのです。ルールがある世界ではAIにはかなわないという風に考えたほうがよいのではないかと。逆に言うと、人間はルールを決めることができるが、機械はルールがないことはできないということでもあります。

つまり、囲碁の魅力は棋士の創造力であるとか、人間的な考え方、思考過程にある。AIが強くなっても、囲碁の魅力がなくなるというわけではありません。AIが打つことによって開拓される新しい手もありますから、AIと人間とはよい関係を築いていると言ってよいのではないかと思います。

井手 機械とはやりたくないという棋士もいそうですが（笑）。

團 現状では、むしろ思いもよらない手が勉強できて面白いと感じる方が多いように思います。王 銘琬先生が、ご著書で「人間は部分を見る」と書いていらっしゃいますが、私もその点には共感します。隅から入って、その



隅で相手とどう戦うかを考え、それから次の隅を考えるとこの風に対戦が進むのですが、王先生によるとAIには“部分”の感覚がないと言います。人間は部分に集中して物事を解決していくけれども、それがAIにはない。ある意味で大局観しかない。部分的に見れば突飛もない手が、全体から見るとよい手だったと終盤になって分かるということが出てきます。棋士がそれを見て面白いと感じるのは、いい関係だと思えます。

井手 囲碁と将棋を比較すると、囲碁の魅力はその宇宙観にあると言われていますね。

團 その宇宙観が重要だと私も思います。そしてAIはその宇宙観に近いものを持っているのかもしれない。

井手 となると、経営もAIができる時代が来るかもしれない（笑）。囲碁は経営判断の訓練になるとよく言われます。

團 確かに経営は多くのことが決まりごとの上に成り立っていますからシミュレーションができます。機械が知らない領域はあるとは思いますが、経営分析のかなりの部分がAIでできるかもしれません。

井手 人間がやると、個人に対する好き嫌いのような人間的な判断が入って間違えることがありますから、AIの方がいいかもしれません（笑）。

團 囲碁と将棋は歴史的に見ると天皇や大名やお坊さんなど権威のある場所で始まっています。それに対して将棋の出自はもっと大衆的で広い基盤を持っています。ですので、囲碁はいわば習い事の世界に近い。文人のたしなみを表す中国伝来の言葉で「琴棋書画」という表現があります。この中の「棋」が囲碁のことで、教養の心得として扱われていた。将棋はもっと気らくな楽しみに近



いものです。その流れが今に至るまであり、囲碁は先生について習い事をするという世界です。

その流れの先に出てくるのが情報化で、従来は先生について教わらなければ上達しなかったのが、ネットで勉強できるようになっています。

この前聞いた話ですが、高校生の有段者が大会に出てきた。打つのは打てるのだけれども、最後の地の計算ができないのだそうです。どうしてかという、その人はずっとネットでやっていたので計算はソフトが勝手にやってくれる。数え方を覚える必要がないのだそうです。裏返すと、教わらなくてもコンピュータとネットで強くなれるということなんです。情報化による変化の最たるものです。

井手 ゲームでも顔の分からない同士のネット対戦が当たり前になっています。

團 ところが一方では「郵便碁」という遊びがあって、一手ずつ葉書きに書いて碁を打つ愛好者がいまだにいるんです。

井手 それは典雅ですね（笑）。

團 一局で200手もかかりますので、一局打つのに一年かかるという世界ですね。色々な楽しみがある中で、その最先端にネットがあるということです。新しい構図が広がるのはいいことだと思います。

囲碁は「手談」であると言われる。言葉がなくても通じるところが素晴らしいと思っています。国同士、あるいは地域同士、囲碁を打つ同士はお互いが特別の尊敬を持っている。これは囲碁ならではの世界で、人とのつながりを作るのが囲碁だということを確認しています。これはこれからの社会にとってもとても大事なことだと思っています。

井手 人と人をつなげるのが囲碁のいいところですね。

團 そこが囲碁のよいところです。「笠碁」という落語の演目があります。碁敵同士がちょっとしたことで喧嘩別れをするけれど、来なくなると寂しくて仕方がないという人情味ですが、碁敵ほどよい仲間はないという感じがします。

NTT再編のこと — 大事なことはルールに基づく規制

ここで終わるはずだった対談は、流れるままに團理事長が郵政省時代に主導した1998年のNTT再編の話に及んだ。その様子も少々紹介したい。

井手 あの時に100%出資の持株会社方式でNTTを再編するという方向が生まれました。

團 その後いろいろな評価があったと思いますが、当時の大臣以下の判断は妥当だったのではないのでしょうか。ポイントは「完全分割をすれば、独占的企業でも競争になる」という意見です。私は「独占的企業を完全分割しても相互の競争にはならない」と思っていました。他の公益事業の例を見ても、そうはならないと思いました。

何が公正競争なのかということと、技術の進展をどう図るか、国際競争の中で相手国と同じ形態であることも重要だと考えました。

井手 日本では持株方式は独禁法で禁止されたいところ、風穴を開けて頂きました。これはまさに画期的なことですね。

團 前の年に純粋持株会社を許容する制度改正がなされ、NTTの再編で純粋持株会社が初めて設立された。これは政府あがりの施策でしたが、歴史的なことだと思っています。当時、事業の複合化と公正な競争を実現できるという意味で、持株会社が金融分野などにも向いており、生きてくるだろうと思っていましたが、その後、実際にそうになりました。そういう面でもよかったと思っています。

井手 私も当時NTTで、海外の事例を研究したりしながら、持株方式をずっと勉強していました。

團 NTTでもよく研究されていましたね。



当時思っていたのは、海外との競争を考えると、海外の会社と同じ武器を持たないといけないということです。将来どのサービスが伸びるかは分かりませんから、あるサービス分野がだめになったときに、別の分野を伸ばすという余地がないとNTTは大変になったと思います。

井手 電話番号案内はほとんど使われなくなりましたし、当時は高収益だった電話帳も事業としては縮小しました。米国でもAT&Tなど電話会社は電話帳事業を売却してしまいました。

團 重視したのは利用者の利便性が低下する選択肢はよくないという視点ですね。携帯電話の「通話料0円」の

競争など、言ってみれば消費者を混乱させるような競争はしっかりと規制すべきではないかと思います。認可料金である電気通信料金がただなんてことはおかしいですから。

井手 民営化の時に「規制は悪だ」という思想が生まれて、それが当たり前になってしまった観があります。様々な場面で制度が骨抜きになってしまっている部分もあるような気がします。

團 大事なことはルールに基づく規制だと思います。そのルールは恣意的ではなく、しっかりしたものでなくてはならないのですが、規制することが間違っているというのは少し違うと思います。

プロフィール

團 宏明 (だん ひろあき) 氏

東京大学法学部卒。1970年郵政省入省。1996年7月に郵政省電気通信局電気通信事業部長、1999年7月に郵政省貯金局長、官房長、総務省郵政企画管理局长、郵政事業庁長官、日本郵政公社副総裁、郵便事業株式会社代表取締役社長などの要職を歴任。2013年6月から公益財団法人通信文化協会理事長。2016年6月から公益財団法人日本棋院理事長。2017年11月に瑞宝重光章受章。

「なりすましメール」の危険性と「DMARC」の可能性

一般財団法人日本データ通信協会
迷惑メール相談センター次長 西松 薫

欧米で被害が広がっていた「ビジネスメール詐欺」(BEC: Business E-mail Compromise)が日本にも上陸してきた。国内では、2016年3月には大手旅行代理店から約678万人分の個人情報流出し、また、2017年9月には大手航空会社が3億数千万円もだまし取られたと報道されている。

被害に遭ったどの企業も情報セキュリティ対策に注力しているのに、何故、被害にあってしまったのだろうか？ 報道によると、欧米で多く見られている、企業の経営層になりすまして相手をだます、いわゆるCEO詐欺とは異なり、これらはいずれも取引先企業の「なりすましメール」による被害で、2つの事例に共通しているのは、攻撃者による入念な準備と絶妙なタイミングの攻撃メール送信があった点にあると言われている。

攻撃者は、①まず、被害企業に入り込むため「なりすましメール」を送信し、②被害企業の機器をウイルスに感染させて被害企業に入り込む。③その後メールのやり取りをモニターして業務の流れを把握し、④どのタイミングでどのような内容のメールを出せば騙すことが可能か十分に調査したうえで、⑤絶妙なタイミングで被害企業のターゲットとなるメールアドレス宛に「なりすましメール」を送信して被害企業に金銭の振込みを行わせたり、重要な情報にアクセスするためにウイルス感染へと導いたりするのである。もし、「なりすましメール」を完全にブロックすることができていれば、これらの被害は未然に防ぐことができたのかもしれない。

それでは、どのような対応を行えば「なりすましメール」をブロックすることが可能になるのだろうか？ 技術的な観点から送信者ドメインの詐称やメール本文の改ざんを行う「なりすましメール」の検出に対して有効な技術がアメリカを中心に広まってきている。それは「DMARC」(Domain-based Message Authentication,

Reporting & Conformance) と呼ばれ、国際的な電子メール不正利用対策技術検討グループであるM3AAWG (The Messaging, Malware and Mobile Anti-Abuse Working Group) が推奨している。日本でも日本データ通信協会の迷惑メール相談センターが運営事務を担当する「迷惑メール対策推進協議会」(座長：新美育文 明治大学法学部教授)がその普及・啓発活動を行なっている。

もちろん、この技術を導入したとしても現在拡大しつつあるBECを無くすことはできないが、少なくとも過去に発生した被害事例のいくつかは防止することができたはずだ。また、攻撃側から見ると、ターゲットとなる企業への侵入難易度や金銭・情報の取得難易度が高まることで攻撃者にとっての手数・コストが増加し、最終的に攻撃意欲の減少につながる。

欧米では大手のメールサービス事業者やメール配信事業者の多くがDMARCを導入しているが、日本ではまだわずかなので、今後、DMARCの日本国内での普及によって『なりすましメール』の被害拡大が抑制されることが期待されている。

迷惑メール対策推進協議会の事務局である迷惑メール相談センターでは、このDMARCの普及に向けてリーフレットを作成し各企業の関係者に配布すると共に、ホームページ上に各メールサービス提供事業者の対応状況を示し、その普及状況を皆様にお伝えしているので、ぜひご覧いただきたい。

メールサービスを提供している事業者のDMARC利用状況については、迷惑メール相談センター当該ページ (<https://www.dekyo.or.jp/soudan/contents/auth/index.html>) を参照いただきたい。

いま注目される「DMARC」

東京農工大学 大学院工学研究院 助教 北川 直哉 氏

1. はじめに

標的型攻撃による機密情報の漏洩や、フィッシング詐欺による被害がメディア等でもさかんに取り上げられているが、これらの攻撃の入り口として電子メールが最も頻繁に悪用されている。例えば標的型攻撃では、攻撃者が取引先企業の人物や職場の同僚などになりすまして電子メールを送信し、そのメールの添付ファイルを開封した受信者をマルウェアに感染させる手口がよく知られている。また、フィッシング詐欺では、ショッピングサイトやオンラインバンクなどになりすまして、パスワードの変更を促すなどの内容で受信者にフィッシングサイトに誘導し、個人情報や金銭の奪取を試みる手口が典型的である。

なりすましメールを送信する攻撃者は、本来の送信者に関する情報を様々な手段でなりすまして送信する。その代表的な手口として、以下の3つの方法が挙げられる。

1. 表示名（ディスプレイネーム）を詐称する
2. 本物の送信者のドメイン名と類似したドメイン名を使用する
3. 本物の送信者のドメイン名を詐称する

1. のディスプレイネームの詐称は、受信者のメールソフト上で表示される送信者の表示名（個人名や法人名など）を偽って記述する手口であり、最も容易に詐称が可能な方法である。この手口は、攻撃者はフリーメール（GmailやYahoo!メールなど）のアカウントを取得して送信される場合や、攻撃者が独自に取得した無関係なドメイン名（大量に自動生成したランダムな文字列の羅列であることが多い）を用いて送信する 경우가多いが、以降で解説する2.や3.の手口においても、ディスプレイネー

ムも合わせて詐称するが多い。

2. の本物の送信者のドメイン名と類似したドメイン名（ホモグラフィドメインやカズンドメインなどと呼ばれる）を使用したなりすまし方法では、人間が文字列の違いを見分けるのが難しいドメイン名（例：（正）example.com（誤）example.comなど）や、本物とはトップレベルドメインが異なるドメイン名（例：（正）example.com（誤）example.netなど）などをあらかじめ取得し、そのドメイン名で生成したメールアドレスからなりすましメールを送信する手口である。

3. の本物の送信者のドメイン名を詐称して送信されるなりすましは、本物とは異なるホストから本物の送信者のドメイン名を偽って送信する手口である。この記事で解説するDMARC（Domain-based Message Authentication, Reporting & Conformance）と、これに深く関係するSPF（Sender Policy Framework）およびDKIM（Domainkeys Identified Mail）の2つの送信ドメイン認証は、いずれもこの手口に対して有効な認証技術であり、1. や2. の手口を用いたなりすましを防ぐものではないことに注意されたい。

2. 送信ドメイン認証技術

DMARCは、現在広く利用されているSPF（Sender Policy Framework）とDKIM（Domainkeys Identified Mail）のどちらの認証にも失敗したメールに対して、受信サーバがどのように処理するべきかを、送信側ドメインの管理者が指定することができる仕組みである。まず、DMARCで利用されるSPFとDKIMの2つの送信ドメイン認証技術について説明する。

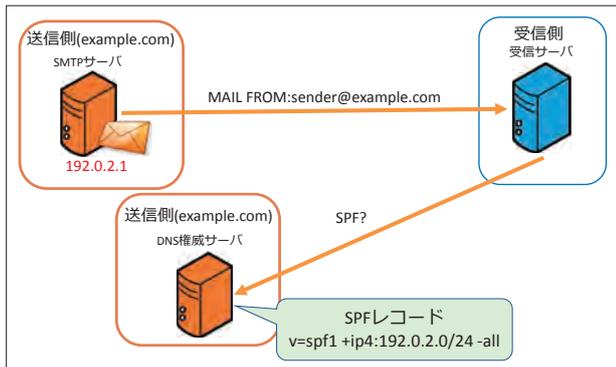
2.1 SPF

SPF（Sender Policy Framework）は、メール送信側

ドメイン名の正当性を検証する機構として広く利用されている。送信側の管理者は、あらかじめ自ドメインのDNS権威サーバでSPFレコードを公開しておく必要がある。SPFレコードでは、レコードを公開しているドメインからメールを送信するSMTP（Simple Mail Transfer Protocol）サーバのIPアドレスのリストを宣言する。

図1に、受信サーバがsender@example.comからのメールを受信した場合のSPFによる送信ドメイン認証の流れを示す。

図1：SPF検証の流れ

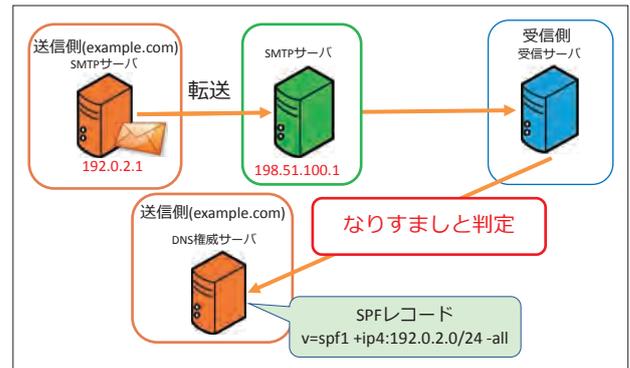


この例では、送信側は「example.comというドメインからのメールは192.0.2.0/24のアドレスブロックに含まれるIPアドレスを持つホストから送信する」旨を宣言していることを示す。受信側では、example.comからのメールを受信すると、当該ドメイン名のDNS権威サーバにSPFレコードを問い合わせる情報を取得し、その送信サーバのIPアドレスと比較する。図1の例では、このメールを送信したSMTPサーバのIPアドレスは「192.0.2.1」であり、SPFレコードで宣言された「192.0.2.0/24」のアドレスブロックに含まれているため、SPF検証は成功する。

SPFはこのような流れで正当な送信サーバの検証を行うしくみとして広く利用されているが、図2に示すようにメールが転送された場合に、なりすましメールではない配送であるにも関わらず検証に失敗してしまう弱点を持っている。

図2の例では、IPアドレスが192.0.2.1であるSMTPサーバから送信されたメールは、IPアドレスが198.51.100.1であるサーバに転送された後に受信者に送信されている。この場合、送信者のアドレス（Envelope-Fromアドレス）は変化しないが、受信サーバから見た送信サーバのIPアドレスは198.51.100.1となり、SPFレコードで示されたIPアドレスブロックに含まれないことから、SPF検証は失敗となる。

図2：転送によるSPF検証の失敗例

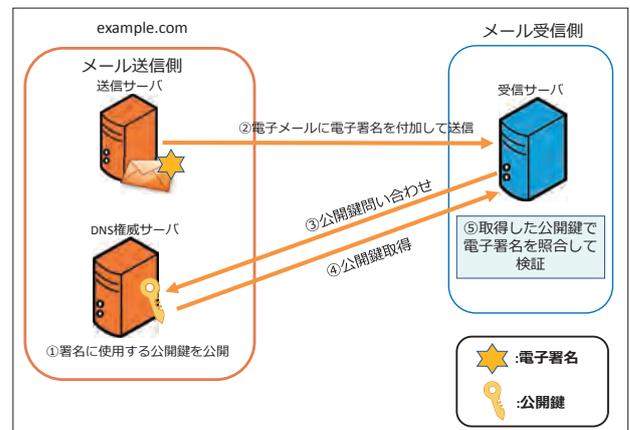


2.2 DKIM

DKIM（Domainkeys Identified Mail）は、電子署名を用いた送信ドメイン認証の機構であり、多くのメールサービスで利用されている。DKIMによる検証では、送信側ではメッセージのヘッダと本文から生成した電子署名をメールヘッダに付加して送信し、受信側でその電子署名を照合することによって送信ドメイン認証を行う。このためDKIMはSPFとは異なり、中継するMTA（メール転送エージェント）で電子メールのデータが変更されない限り、転送メールであっても転送先で正しく認証することができる。

DKIMによる検証の流れを図3に示す。

図3：DKIM検証の流れ



送信側はあらかじめ、署名に使用する秘密鍵と対になる公開鍵をDNS権威サーバで公開しておく（図3-①）。送信側がメールを送信する際には、メールの本文とヘッダを元に作成した電子署名を付与して送信する（図3-②）。受信側のメールサーバでメールを受信すると、メールヘッダ中の「DKIM-Signature」内の「d=タグ」で指定されたドメイン名のDNS権威サーバに対して公開鍵を問い合わせる（図3-③）。ただし、送信側がd=タグで指定するドメイン名はメール送信サーバと同一でなくてもよく、第三者のドメイン名を指定することが可能である。例えば、送信者のドメイン名がexample.com

の場合でも、d=タグではexample.net等、任意のドメイン名を指定することができる。次に、受信側は公開鍵を取得すると（図3-④）、その公開鍵を用いて電子署名を照合し、DKIM検証を実施する（図3-⑤）。

3. DMARC

DMARC (Domain-based Message Authentication, Reporting & Conformance) は、2節で解説した2つの送信ドメイン認証 (SPF・DKIM) を用いたレポーティングおよびポリシー制御の仕組みで、欧米を中心に近年急速に普及が広がっている技術である。DMARCは、SPFやDKIMのような直接的な認証技術とは異なり、SPFとDKIMを利用して、どちらの検証にも失敗したメールに対して、受信側がどのように取り扱うかの方針を送信ドメイン管理者側が宣言するための機構である。このため、DMARCは受信側におけるなりすましメール受信対策ではなく、送信側のドメイン管理者が自ドメインを詐称したなりすましメールを送信されにくくすることで、自ドメインのブランドを保護するための技術であると言える。

DMARCには、このような送信ドメイン認証失敗時の制御ポリシーに従ったメール配送制御の方法を宣言する機能に加えて、レポーティング機能がある。レポーティング機能では、自ドメイン名を名乗って送信されたメールの傾向の集約レポートや送信ドメイン認証の失敗レポートを受信することで、管理者は自ドメイン名の送信ドメイン認証の効果の状況や、自ドメインを騙って送信されたなりすましメールの状況を把握することができる。

DMARCを利用するには、送信側と受信側でそれぞれ次のように対応する必要がある。まず送信側では、SPFおよびDKIMの両方、あるいはいずれか一方に対応する必要がある。これに加えて、送信側では自ドメイン名の先頭に「_dmarc.」を負荷したドメイン名（図6の例では_dmarc.example.com）のTXTレコードとしてDMARCレコードを公開する。DMARCレコード内の「p=タグ」で送信ドメイン認証 (SPF・DKIM) に失敗したメールに対する受信側の処理ポリシーを宣言することができる。宣言可能な処理ポリシーは次の3種類がある。

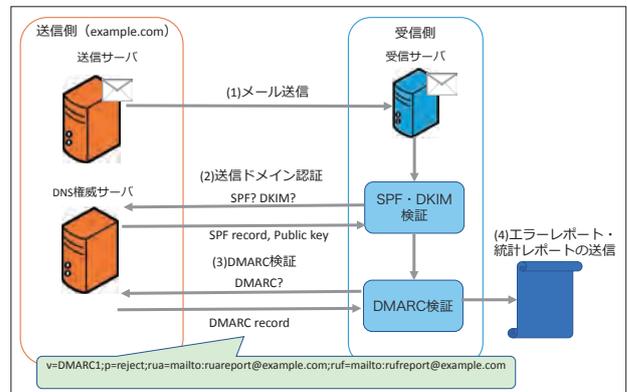
- ・ none (処理方法を指定しない)
- ・ quarantine (隔離する)
- ・ reject (受信拒否する)

これらの処理ポリシーはあくまで送信側が宣言するものであるため、受信側での実際の処理は運用方針によってさまざまである。例えば処理ポリシーがquarantineの場合、

受信側では迷惑メールボックスに隔離する運用が考えられる。また、処理ポリシーがnoneの場合、受信者は通常通りに受信することになるためDMARC導入による受信拒否効果はないが、送信側ではレポーティング機能を活用して集約情報や認証失敗情報を得ることができる。

DMARC検証の流れを図4に示す。

図4：DMARC検証



受信側のメールサーバでメールを受信すると、まず送信ドメイン認証 (SPF・DKIM) を実施する。これらの送信ドメイン認証の両方に失敗した場合、送信側が公開しているDMARCポリシー（図4ではreject）が適用される。また、送信ドメイン認証に失敗した場合には、失敗レポートが「rufタグ」で指定されたメールアドレス（図4ではrufreport@example.com）に対して送信され、送信ドメイン認証の集約レポートは「ruaタグ」で指定されたメールアドレス（図4ではruareport@example.com）に対して送信される。

また、2節で述べたように、DKIMではメール送信者のドメインとは無関係な第三者ドメインによる署名が可能であるが、その署名ドメインが正当であるかどうかを判断するのは極めて困難であるのが現状である。この問題に対して、DMARCではアラインメントと呼ばれる考え方が存在し、第三者署名を禁止している。すなわち、第三者署名によってDKIMに対応しているドメインの配送では、DKIM検証では認証成功となる場合でも、DMARCでは認証失敗となる。

4. DMARCレコードの詳細

DMARCレコードは、図4のDMARCレコードの記述例に示した通り、各パラメータの間をセミコロンで区切って記述する。図4の例では、バージョン情報 (v)、認証失敗時の動作ポリシー (p)、集約レポートの送信先 (rua)、失敗レポートの送信先 (ruf) のパラメータを記述したDMARCレコードの例を示したが、これ以外にも様々なパラメータが存在し、詳細な設定が可能である。これらの概要を表1に示す。

表1：DMARCレポートのパラメータ

パラメータ	概要
v	バージョン情報（現在のところ「DMARC1」のみ）
adkim	DKIM認証のアラインメントモード（r, s）
aspf	SPF認証のアラインメントモード（r, s）
fo	失敗レポートのオプション（0, 1, d, s）
p	受信者に要望する認証失敗時の動作ポリシー（none, quarantine, reject）
pct	ポリシーを適用するメールの割合（0 - 100, デフォルトは100）
rf	失敗レポートの形式（afrf）
ri	集約レポートの送信間隔（デフォルトは86,400秒）
rua	集約レポートの送信先
ruf	失敗レポートの送信先
sp	サブドメインに対するポリシー（none, quarantine, reject）

adkimおよびaspfパラメータは、いずれもDKIMおよびSPF認証におけるアラインメントモードを示し、relaxed mode（r）かstrict mode（s）のいずれかの値を設定する。relaxed modeは、DKIMまたはSPFで認証したドメインとヘッダFromドメインの組織が同じであれば良いことを意味し、組織ドメイン名が同一であればサブドメインでも許可する設定である。一方、strict modeでは、完全にドメイン名が一致している必要があることを意味する。すなわち、いずれの場合でもDKIMとは異なり、組織ドメイン名が異なる署名は認められない。

foパラメータは、失敗レポートを送信する条件を詳細に指定するものである。pctパラメータでは、DMARCポリシーを適用する割合（%）を指定する。rfパラメータでは失敗レポートのフォーマットを指定するが、現在のところafrf（Authentication Failure Reporting Format）のみが指定可能である。riパラメータでは、集約レポート送信の最大間隔時間（秒）を指定する。spパラメータでは、全てのサブドメインに対するDMARCポリシーを指定する。設定可能な値は、pパラメータと同様に、none, quarantine, rejectの3種類である。

5. まとめ

DMARCは従来の送信ドメイン認証とは異なり、送信側のドメイン管理者が受信者に対して受信ポリシーを指定できる仕組みである。海外では大手メールサービスを中心に、DMARCポリシーを最も強い宣言であるrejectに設定している例が多く見られるが、特に国内ではほとんどのドメインでnoneを設定しており、導入に関して慎重な姿勢が見受けられる。実際に、筆者が行なった

調査では、DMARCポリシーを公開しているドメインのうち、およそ80%のドメインが処理ポリシーをnoneとして公開していることを確認している。これは、DMARCポリシーをrejectやquarantineに設定した際に発生する誤判定（False Positive）を防ぐために慎重な設定としていることが多いのが現状であると言えるが、今後の動向の変化にも注目していく必要がある。

また、DMARC導入の重要なメリットとして、DMARCレポートの分析によって、これまで得られなかった自ドメインでの送信ドメイン認証の状況やなりすましの状況の把握ができ、より効果的ななりすまし対策を講じることが可能となることが挙げられる。なりすましメール対策は今後さらに重要視されていくことが予想されることから、DMARCは今後さらに普及していくと考えられる。

プロフィール

北川 直哉（きたがわ なおや）氏

東京農工大学 大学院工学研究院 助教。博士（情報工学）。
 情報処理学会 IOT 研究会藤村記念ベストプラクティス賞（2017/06）、
 IOTS2016 シスコシステムズ賞（2016/12）、ICT-ISPC2016 Best Paper Award（2016/05）、IOTS2015 優秀論文賞（2015/12）等を受賞。
 論文に「A Client Based DNSSEC Validation System with Adaptive Alert Mechanism Considering Minimal Client Timeout」（IEICE Transactions; 2017年8月）、「A spoofed E-mail Countermeasure Method by Scoring the Reliability of DKIM Signature Using Communication Data」（Proc. of IEEE 41st Annual Computer Software and Applications (COMPSAC 2017); 2017年7月）、「Design and Implementation of a DMARC Verification Result Notification System」（Proc. of the 13th APAN Research Workshop; 2016年8月）など多数。

『サイバーセキュリティシンポジウム道後2018』でDMARCの普及促進

—当協会が2講演を提供

3月1日と2日の2日間、松山市で開催された『サイバーセキュリティシンポジウム道後2018』（通称『SEC道後』、主催・サイバーセキュリティシンポジウム道後 実行委員会）において、当協会迷惑メール相談センター主催によるDMARCの講演が行われ、多くの聴衆が熱心に耳を傾けた。

『SEC道後』は、毎年サイバーセキュリティに関わる専門家、各種機関、企業の関係者が一堂に集まるこの分野のビッグイベントである。この『SEC道後』で、日本データ通信協会の迷惑メール相談センターはDMARCに関する2講演を提供し、参加者から好評を得た。

行った講演は、初日に行われた株式会社インターネットイニシアティブネットワーク本部アプリケーションサービス部 担当部長の櫻庭秀次氏による「送信ドメイン認証技術 DMARC によるなりすましメール対策」と2日目に行われた株式会社TwoFive開発マネジャーの加瀬正樹氏による「送信ドメイン認証技術 DMARC の導入とその利用方法」。

櫻庭秀次氏による講演は、DMARCの基礎に始まり、日本での導入に際しての注意点、国内外の普及状況について説明するもの。2日目の加瀬正樹氏による講演は、送信ドメイン認証技術 DMARCの詳細、利用方法、さらには、ドメインレピュテーションといった応用技術の解説という内容であった。質疑応答では、多くの参加者からドメイン認証技術の普及率について質問があり、聴衆の高い関心が見て取れた。

今回の講演について櫻庭氏は、「なりすましメール対



会場となった愛媛大学城北キャンパス・グリーンホール

策としての送信ドメイン認証技術 DMARC は、認知度の低さが普及への課題となっていることがこれまでの調査で明らかでしたが、今回の講演では質問も活発にあり、関心を高めることに貢献できたと感じました」と語った。

一方、加瀬氏は、「今回のシンポジウムは初めての参加でした。DMARCという技術の解説を中心に話ししましたが、SPF や DKIM というそれぞれの技術についての解説にも重要性を感じました。また、技術解説だけではなく、各企業のニーズにあった設定方法について指南できると、DMARC が一層広がるのではないかと思います」と答えてくれた。

講演を主催した当協会迷惑メール相談センター所長の松田和男は、2つの講演について、「セキュリティの専門家や地元の企業に対し、ある程度まとまった時間でしっかりとDMARCを説明できたことは、大変有意義でした。今後も積極的に普及活動を行っていきたいと考えています」と手応えを感じた様子だった。

（文責：編集部 木梨安奈）



講演の講師を務めた櫻庭秀次氏（左）と加瀬正樹氏（右）

総務省 3 課長が語る電気通信政策の現在

本年3月6日に開催された第46回ICTセミナー（主催：日本データ通信協会）は、総務省で電気通信政策を主導する3人の課長をお招きし、各課が取り組む重要課題についてお話を頂いた。本稿はその内容をかいつまんで紹介するものである。当日は、総合通信基盤局電気通信事業部の電気通信技術システム課、同データ通信課、情報流通行政局サイバーセキュリティ課の3つの課が所管分野する電気通信分野の動向、それに対応する各課の取組が凝縮して語られ、聴衆の熱心にメモを取る姿が会場のここかしこで見られた。

講演 1：「ネットワークインフラに関する政策動向について」



総務省 総合通信基盤局 電気通信事業部 電気通信技術システム課
課長 萩原 直彦 氏

電話網のIPネットワークへの移行に向けた対応

NTTは、2025年頃には現在の電話ネットワークを支える交換機を維持・運用することが困難になることから、現行の公衆交換電話網（PSTN）をIP網に移行すると発表している。こうした状況を踏まえ総務省では、2016年2月に「固定電話網の円滑な移行の在り方」について情報通信審議会に諮問を行い、これを受けた同審議会の電話網移行円滑化委員会が平成29年3月に一次答申「移行後のIP網のあるべき姿」を、同年9月には二次答申「最終形に向けた円滑な移行の在り方」を取りまとめた。

一次答申では、IP網に“移行後の電話網のあるべき姿”を描くことを目的に議論が行われ、メタルアクセス回線をそのまま残しつつ、従来PSTNが担ってきた各種電話会社を結ぶ“ハブ機能”を今後作っていくにあたっての個別課題を、利用者及び事業者の視点から必要な課題を整理し、大きな方向性を打ち出した。

2次答申では、1次答申で明らかにした個別課題（電話番号の管理の在り方、緊急通報の確保、ユニバーサルサービスとしての固定電話の確保等）について具体的な方向性を明らかにするとともに、2025年1月までの完了

を目指したIP網への移行スケジュールを示した。

電気通信技術システム課では、情報通信審議会の答申を受け、平成28年12月から「IPネットワーク設備委員会」において、IP網への移行に向けて、電気通信事業者のネットワークの技術基準の検討を開始していた。

電気通信事業法は、ネットワークを自ら構築して運用する回線設置事業者と、有料で100万人以上にサービスを提供する回線非設置事業者に対しネットワーク設備の技術基準への適合を義務付けるとともに、設備の管理規程の届出並びに電気通信設備統括責任者及び電気通信主任技術者の選任・届出を行うこと等を規定している。

これらの規定を踏まえ、同委員会では、メタルIP電話の設備に対する技術基準、音声品質の技術的要件と品質測定方法“電話を繋ぐ機能”に必要な技術的要件、などの課題について取りまとめを行い、平成29年7月に情報通信審議会から答申を受けた。

将来のネットワークインフラに関する検討

我が国のブロードバンド契約者の総トラヒックは急激に伸びており、そのペースが鈍るとは当面考えられない。IoTサービスも本格化しつつあり、2020年までに現在の約2倍の304億個のデバイスが稼働するとの予測もあ

る。また、政府は「4K・8Kの推進」を掲げており、伝送にブロードバンド網が活用されることも想定されている。さらに、LTEの100倍の速度を実現する第5世代移動通信システム（5G）も2020年の実用化を目指して急速に検討が進んでいる。

こうした環境変化を受けて、2030年頃までを見据えて、ネットワークインフラに求められる機能と、安全で信頼性のあるネットワークインフラを実現するための課題を検討するため、2017年1月に「将来のネットワークインフラに関する研究会」を立ち上げ、同年7月に取りまとめと結果の公表を行った。

報告書では将来実現されるサービスのイメージを、「超リアルタイムサービス」、「超高精細映像配信サービス」、「IoTサービス」の3領域に分類したうえで、それらのサービスを実現するためにネットワークインフラに求められる要求条件を、①大容量、②省電力化、③超低遅延、④柔軟性・高弾力性、⑤高効率データ流通、⑥安全・信頼性の6つの機能に整理し、実現に向けた技術的課題を明らかにした。

2030年頃にIoTが我が国の隅々まで普及し、ネットワークが「社会システムの神経網」進展していくためには、光伝送技術等の研究開発の促進、オープンソースなどを効果的に活用取り入れたネットワークの高度化、インフラ事業者、OTTや主要サービス提供事業者とのWin-Winの関係の構築、保守・運用人材不足を見越した

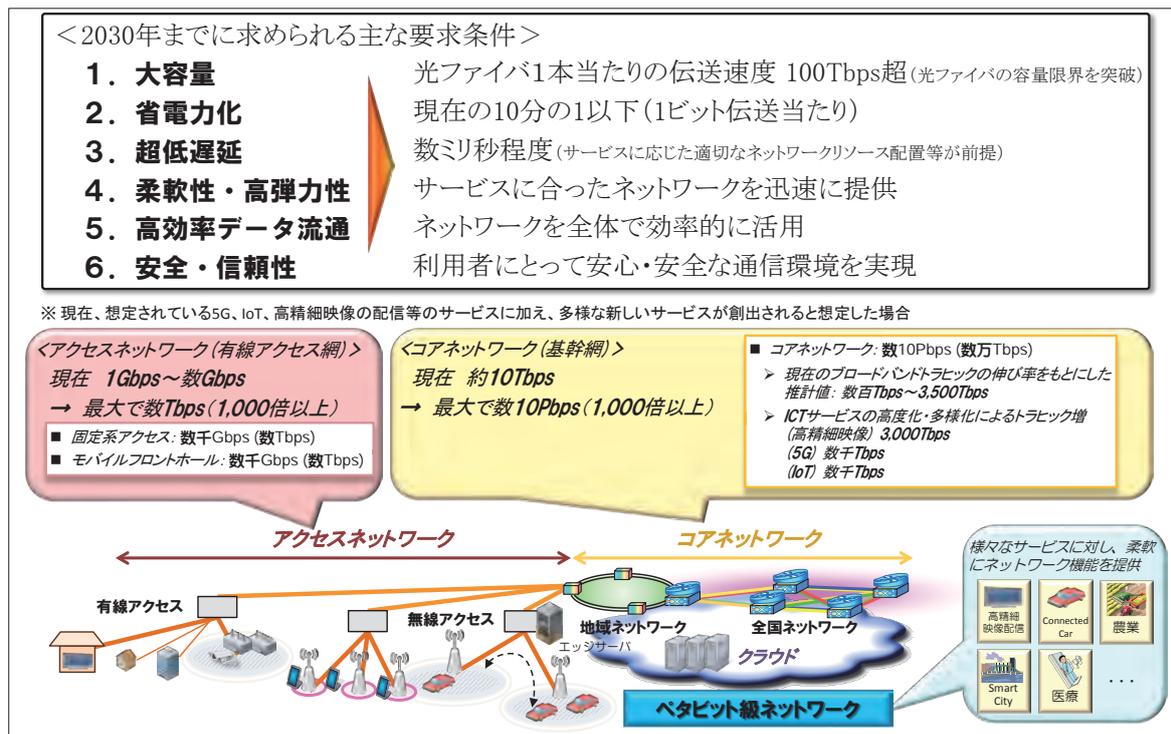
AIの活用、そのために必要なデータ仕様の標準化、IoTの普及に対応した技術基準の整備、サイバーセキュリティの確保、インフラ全体として効率的な整備・活用等に取り組んでいかなければならない。

IoTに対応した技術基準関連制度の検討

近年、国内外においてDDoS攻撃によってインターネットに障害が発生するケースが発生しており、とくにIoT機器を狙った攻撃の増加が情報通信研究機構（NICT）のNICTERプロジェクトなどで顕著に観測されている。サイバー攻撃以外でも、昨年8月に海外の大手事業者がインターネットの通信経路設定を誤ったことが原因で、国内インターネット事業者のサービスに障害が起るなどの事例も発生している。

こうした状況を受け、総務省では、「円滑なインターネット利用環境の確保に関する検討会」を立ち上げ、こうした障害の防止のために何ができるかについて、IoT機器を含む脆弱な端末設備のセキュリティ対策や大規模なインターネット障害発生時の対策などについて検討を行った。これらの項目については、情報通信審議会IPネットワーク設備委員会において引き続き技術的検討を行い、今年の7月までに一次報告を取りまとめる予定である。

図1：将来のネットワークインフラに対する要求条件と主要技術



出所：総務省

講演2：「総務省におけるデータ通信政策の動向」



総務省 総合通信基盤局 電気通信事業部 データ通信課
課長 内藤 茂雄 氏

伸張する無線LAN

電気通信分野のトレンドを2つ上げるとすると、1つは電波（＝移動体通信）、2つめが大容量化（＝ブロードバンドサービス）である。この2つが今後の世の中を作っていると言えるが、この流れを端的に表しているのがWi-Fiである。

スマートフォンの契約者数が平成23年度末から平成28年度末の5年間で約3.3倍増加し、トラフィックも1年で約1.4倍のペースで伸びているが、Wi-Fiはこのスマートフォンの伸びにつれて普及が進んでいる。

海外でも同じような状況にあり、携帯電話のトラフィックと、それをバイパスするWi-Fiによるデータオフロードを比べると、2015年の時点で世界ではオフロードのトラフィックが携帯電話のトラフィックを上回っている。日本ではインターネットトラフィックの約6割がWi-Fiである。

これによってインターネット接続事業者（ISP）が回線設備の増強に追われ、重い投資負担を強いられている。インターネットに繋ぐための回線容量が前年比3割増というペースで伸びているが、このペースは無線LAN技術の進化によって、当面鈍化はしないと考えている。

現在ほぼすべてのスマホやタブレット端末に無線LAN規格の第3世代である「IEEE 802.11n」以上が用いられているが、第4世代である「IEEE 802.11ac」が急速に普及しつつある。来年登場する第5世代の「IEEE 802.11ax」では、MU-MIMOやOFDMAといった技術を用いて1台のルータで8台の端末と同時に通信ができるようになり、実効のスループットは現在の約4倍にもなると言われている。各家庭のトラフィックが向こう数年で数倍になってもおかしくはない状況でありISP業界に影響が出てくることも想定される。

Wi-Fiの課題

今後、Wi-Fiは社会インフラとして定着していくと考えられるが、そうなるためには「セキュリティ」、「電波

の輻輳（混雑）」、「ユースケースの見極め」という3つの課題を克服していかなければならない。

Wi-Fiのセキュリティ対策が十分に行われていない状況を、東京オリンピックまでに如何に改善していくかは大きな課題である。電波の輻輳については、Wi-Fiは通信手順や干渉面で課題が多く解決は容易ではない。第3の課題はユースケースの見極めで、将来、第5世代移动通信システム（5G）が導入されると、Wi-Fi事業は5Gとすみ分けを図る必要が生じると考えている。加えて、地方自治体などを含め、アクセスポイントオーナーの維持管理負担を如何に軽減するかがユーザサイドの課題となってくる。

5Gが変える未来

今後の主要な政策課題はデータ流通の拡大である。そのためIoTと5Gの社会実現を見すえた取組みが大事である。

5Gには「超高速」に加えて、「超低遅延」と「多数同時接続」という二つの新しい性能が加わってくる。「超低遅延」を理解して頂くには、高速道路で自動運転をする際の車線変更を思い描いて頂きたい。そこで0.1秒でもデータ伝送にタイムラグが発生した場合を想像すると、遅延の重要性が分かって頂けるのではないかとと思う。

「多数同時接続」はIoTへの利用普及に不可欠な技術である。電力自由化に伴ってスマートメーターが普及しており、定期的の使用電力量の情報をセンター側に送信して電力利用の効率化を図っている。

「多数同時接続」を実現するために必要な仕組みがIPv6である。使用可能なIPアドレスが約43億個であったIPv4がほぼ枯渇する中、約340潤（＝ 3.4×10^{38} ）個が利用可能なIPv6を用いれば、すべてのセンサーなどにIPアドレスを付与して通信をすることができるようになる。

実はIPv6への対応はデフォルトになりつつあり、現在投入されているスマートフォン端末の大半はIPv4で

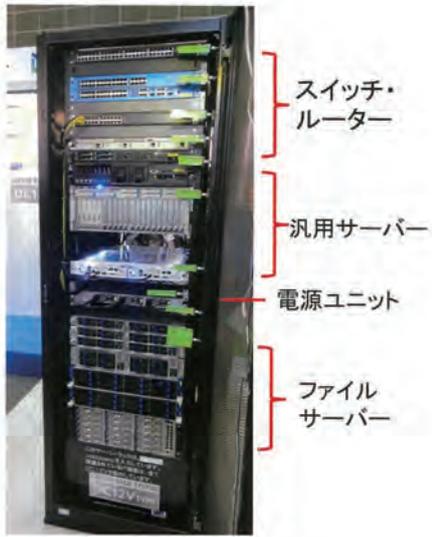
もIPv6でも通信ができるようになってきているほか、ネットワークのIPv6対応はおおむね完了している。

今後、データ流通の拡大に向けて注目すべきは「官民データ活用推進基本法」（2016年12月施行）で、すべての都道府県にデータを活用するための推進計画策定が義務付けられ、市町村にも推進計画策定の努力義務が課された。データ活用の方法を考案し、そのためのシステムを構築することが求められる。この中でWi-Fiのログデータを分析し、観光振興に役立てるなどの取組が進んでいくものと期待される。

この時、データトラフィックの地域分散が重要な課題になる。「超低遅延」のネットワークを構築するためにはネットワークの接続点を地域毎に増やしていかなければならない。現在データセンターの約6割が東京に集中しており、地元の情報を東京のデータセンターに取りに行かなければならないということになれば、せっかくの機能を十分に活用できないことになってしまう。

来年度より地域におけるデータ通信を活性化し、国土強靱化を実現する観点から「地域データセンター整備促進税制」を創設したところ。ぜひ活用頂きたい。

図2：地域データセンター整備促進税制の創設

<p>1 対象者 総務大臣から実施計画の認定を受けた電気通信事業者</p> <p>2 対象設備 実施計画に従って取得した以下の設備 サーバー・ルーター・スイッチ・電源装置</p> <p>3 措置内容 法人税：取得価額の15%の特別償却 ※東京圏以外に整備するもので、設置地域近傍からの利用を主たる目的とする設備に限る。 固定資産税：課税標準3/4の特例（3年間） ※首都直下地震緊急対策区域以外の地域に整備するもので、専ら同区域内のデータセンターのバックアップを目的とする設備に限る。</p> <p>4 適用期間 2018年4月1日から2020年3月31日まで</p>	
--	---

出所：総務省

講演3：「サイバーセキュリティ政策の最新動向」



総務省 情報流通行政局 サイバーセキュリティ課
課長 木村 公彦 氏

サイバーセキュリティ上の脅威の現状

サイバーセキュリティ上の攻撃は、目立つものから次第に目立たないものへと巧妙化し、その目的も悪質化する傾向がある。ICTが社会経済活動の基盤であり、成長力の鍵であると認識される中で被害は深刻化している。

IoTの時代を迎え、脅威はさらに広がりつつある。

IoTが狙われる理由には、「管理が行き届きにくい」、「常に電源が入っていて外部からアクセスできる状態にある」、「ライフサイクルが長く長期間繋がったままで放置されているケースがある」、「セキュリティソフト等の対策が不十分なものがある」といった特徴があるからだ

と考えられる。

政府全体のセキュリティ政策への取り組み

サイバーセキュリティに対し、政府は様々な対策を取ろうとしている。サイバーセキュリティ基本法が平成26年11月に成立し、内閣にサイバーセキュリティ戦略本部が、その事務局的な立場で内閣官房に「内閣サイバーセキュリティセンター（NISC）」が設置され、関係5省庁、重要インフラ所管省庁との間で政策の総合調整を行う体制が整備された。

我が国のサイバーセキュリティ戦略（2015年9月閣議決定）は、産業振興、企業活動の向上等の観点に基づく「経済社会の活力向上及び持続的発展」、脅威への防御能力を高める「国民が安全で安心して暮らせる社会の実現」、国際連携を目指す「国際社会の平和・安定及び我が国の安全保障」の3本の施策を「研究開発の推進」と「人材の育成・確保」の横断的施策で支えるという構造になっている。政府の成長戦略である「未来投資戦略2017」の中でも「サイバーセキュリティの確保」という項目が設けられ、その推進が明確に位置づけられている。

今年（2017年）はサイバーセキュリティの次期戦略が策定される年であり、その過程で現行戦略の中間レビューが2017年7月に行われた。加速・強化すべき施策の中に「ボット撲滅の推進」が挙げられたが、総務省では、これに応じ「IoTセキュリティ総合対策」を検討し、2017年10月に公表した。

総務省のセキュリティ政策への取り組み（IoTセキュリティ総合対策）

総務省の「IoTセキュリティ総合対策」は5本の柱からなる。「脆弱性対策に係る体制の整備」、「研究開発の推進」、「民間企業等におけるセキュリティ対策の促進」、「人材育成の強化」、「国際連携の推進」の5つである。

（1）脆弱性対策に係る体制の整備

脆弱性対策は機器のライフサイクル全体を見直し、それぞれの段階に応じた対策を行うことが必要である。例えば設計・製造の段階では、セキュリティ・バイ・デザインの考え方を踏まえた設計、セキュリティ要件の充足を利用者に分かりやすく伝えるための認証マークの付与などの検討が有用であるし、設置の段階では、個々の機器だけでは十分な対策が困難な場合を想定して、IoT機器とインターネットの境界上にセキュアゲートウェイを設けるなど、ネットワーク上でも安全性を担保できるような取組が重要である。

すでに市場に流通し、利用されている機器についてどのような対策を行うかも大切で、脆弱性調査の実態調査を行い、消費者への注意喚起を実施しつつ関係者間での情報共有を行うといった対策を推進していく。

（2）研究開発の推進

サイバーセキュリティの向上のためには産官学が連携をし、研究開発の成果をできるだけ早期に対策に反映していくことが重要である。情報通信研究機構（NICT）の無差別攻撃対策「NICTER」や標的型攻撃対策「NIRVANA改」などの技術は多くの自治体での導入や民間への技術移転が進んでいる。現在研究開発を進めている一例として、サイバー攻撃の標的型メールを偽装環境で観測・分析するサイバー攻撃誘引基盤「STARDUST」があり、実用化に向けて開発が進んでいる。

（3）民間企業等におけるセキュリティ対策の促進

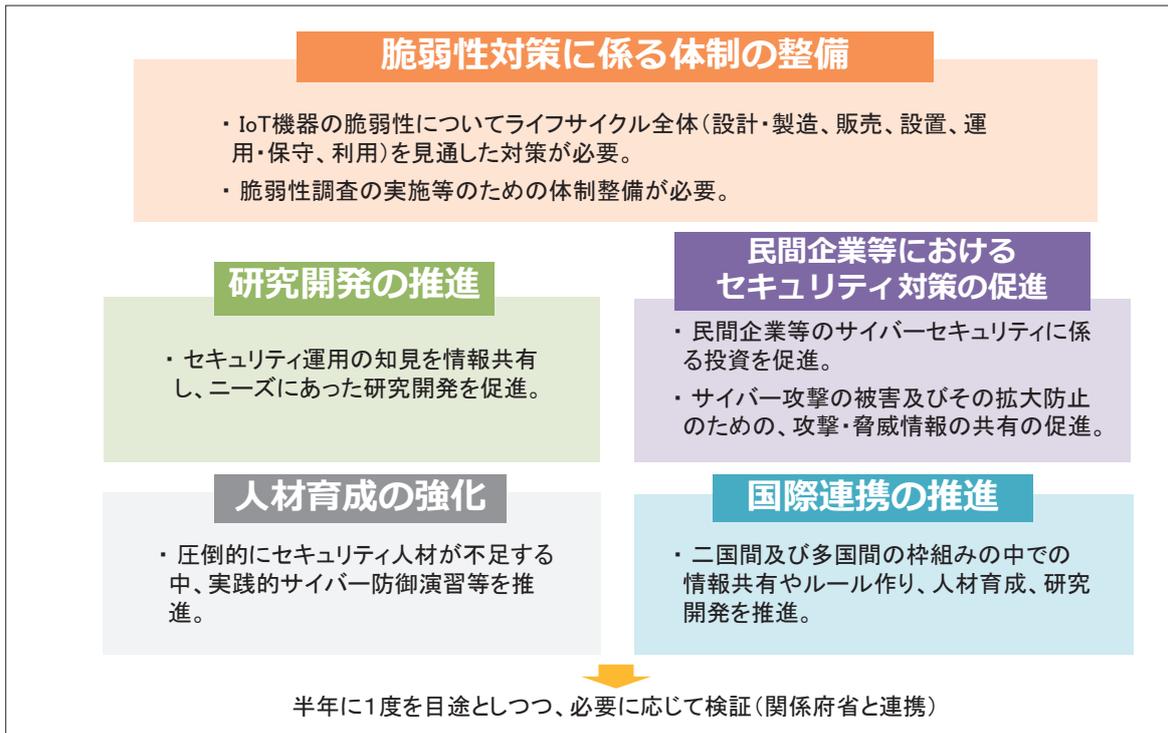
サイバーセキュリティ対策は国だけでできるものではない。民間企業においてセキュリティ対策を経営のための積極的な投資だと認識して対応を頂くことは重要である。今回の総合対策に盛り込んだ税制優遇措置については、経済産業省と共同で要望した結果、一定のサイバーセキュリティ対策が講じられたデータ連携・利活用によって生産性向上につなげる投資に対し、「情報連携投資促進税制」として認められることとなった。

また、サイバーセキュリティタスクフォースの下に「公衆無線LANセキュリティ分科会」を設置し、公衆無線LANにおけるセキュリティ上の課題を検討する作業を進めている。さらに「情報開示分科会」を設け、民間企業のセキュリティ対策の情報開示に関する課題の整理を行っており、両分科会ともに年度末から年度明けを目途に検討結果を取りまとめる予定である。

（4）人材育成の強化

我が国のセキュリティ人材は圧倒的に不足していると言われており、人材育成への積極的な取り組みが不可欠である。昨年4月に情報通信研究機構（NICT）に「ナショナルサイバートレーニングセンター」を設置し、①実践的なサイバー防御演習（CYDER）、②東京オリンピック・パラリンピックの担当者に向けたサイバー演習（サイバーコロッセオ）、③若手セキュリティイノベーターの育成（SecHack365）という3つの大きな取組を進めている。

図3：IoTセキュリティ総合対策（2017年10月）



(5) 国際連携の促進

サイバー攻撃に国境はなく、国際連携は重要である。ここでの柱は、1つは情報共有の促進、2つめが特に途上国向けの能力構築である。

先進国との間の協力は必要不可欠であり、ISAC（情報共有・分析センター）等の民間レベルでの活動とともに、政府関係者においても同様に情報共有を進めていく。能力構築については、サイバー対策のために一定の水準を確保することが重要であるため、ASEAN等を中心としたセキュリティ人材育成支援等に対し積極的に貢献をしていく。

サイバーセキュリティは産学官の連携が非常に重要であり、総務省としても力を入れていくが、ぜひ産業界の皆様とも一緒になって取組を進めていきたいと考えている。

（文責：編集部 中山隆）

05 インタビュー

社内人材を可視化し、モチベーションを高める 富士通の『セキュリティマイスター認定制度』



富士通株式会社
サイバーセキュリティ事業戦略本部
サイバーディフェンスセンター長
奥原 雅之 氏

富士通は2014年に社内セキュリティ人材の認定制度『セキュリティマイスター認定制度』を立ち上げ、それ以来組織的な取り組みを加速している。推進の様子はニュースリリースやホームページで丹念に紹介されており、取り組みは順調に進んでいるように見える。

日本を代表するシステムベンダーの一つである同社がセキュリティノウハウ強化の取り組みをどのような思いで進めているのか。『セキュリティマイスター認定制度』を創設時から推進する同社サイバーセキュリティ事業戦略本部サイバーディフェンスセンター長の奥原雅之氏に話を伺うと、「大企業の育成制度は緻密だが、得てして型にはまっている」という先入観とは相容れない柔軟な取り組みのありようが見えてきた。

異なる役割を担う3つの領域

まずは『セキュリティマイスター認定制度』がどのような制度なのかを概観しておこう。この制度はセキュリティスキルに長けたエンジニアを認定する富士通の社内制度で、現在は本社と直接子会社の社員を対象にしている。奥原氏によると、諸外国の制度を色々と研究した上で『全米サイバーセキュリティ教育イニシアティブ』（NICE）の人材育成プログラムを参考に、人材像を独自に策定したという。約20名で運用する事務局では、人材の認定を行うとともに、育成プログラムを策定し、リアルな仮想環境を使った演習プログラムであるサイバーレンジの開発も自前で行っている。

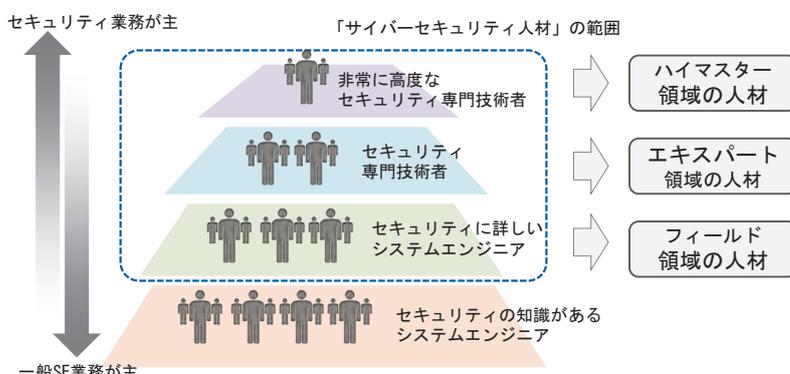
この制度が定義する人材像は、図表1のとおりである。

図の下方に描かれている『フィールド領域』の人材は、“セキュリティに詳しいSE”で、システム開発や運用の現場で業

務を支えるエンジニアを指している。大別すると、設計をする「システムセキュリティエンジニア」と運用に関わる「セキュリティインシデントハンドラー」に別れる。

『エキスパート領域』は、セキュリティソリューショ

図表1：「セキュリティマイスター」の人材像



認定実績（2018年1月現在）

フィールド領域	エキスパート領域	ハイマスター領域	合計
2,554名	216名	8名	2,778名

出所：富士通株式会社

ンの開発など富士通のセキュリティビジネスそれ自体を支える専門家を認定する。

『エキスパート領域』の上に表示されているのが、いわゆるホワイトハッカーと呼ばれている世界的にトップクラスのノウハウを有する人たちで、富士通では『ハイマスター領域』の人材という言葉で冠している。会社の看板・広告塔として機能するのがその役目だ。

「これら三つの領域はそれぞれ作った動機が違います。『フィールド領域』の人材は、お客様に提供するソリューションがセキュリティ事故を起こさないようにするという、品質に関わる領域を期待されています。私どもが納めるシステムは必ずセキュアでなければならないということは、従来から弊社がこだわっている部分ですので、それを実現するための人たちということでスタートしています。

『エキスパート領域』の人材は、まさに富士通のセキュリティ系ビジネスを担う人間をどうやって育てるかという問いから出てきています。

『ハイマスター領域』はセキュリティに関わる技術の一部に極めて特化した人材で、その領域では右に出る者はいないほどの人材と規定しています」（奥原氏）

当初は700人の認定を目標として設定したが、その数字はあっという間にクリアしてしまい、2018年1月時点の認定者数は約2,800名に上る。会社は2019年度末（2020年3月）までに1万人の認定を目指すと言っている。

認定実績を見ると約2,800人のマイスターのうち約2,700名は『フィールド領域』の人材である。人数の規模もさることながら、セキュリティが分かるSEの増大を目指す『フィールド領域』は、この制度の中でもっとも目立つ部分かもしれない。奥原氏によれば、「ちょっ

としたプロジェクトチームには必ず一人はセキュリティが分かるエンジニアがいる」という形を作りたいのだそうだ。「組織ごとに置かれている防火責任者のようなイメージ」という表現もしてくれた。

まず目指したのは人材の可視化

“マイスター”という人目を惹くネーミングがなされていることや、1万人という大きい目標が報道などで目立つこともあって、ともすると、会社が総力を挙げて技術系社員のお尻を叩いているような印象を抱いてしまいがちだが、当初の目論見は強権的な知識詰め込み教育などとはまるで様子が異なっている。奥原氏は言う。

「高い技能を持つ社内人材の可視化と発掘に焦点を当てています。もちろん育成は必要なのですが、今回の制度では、それに先んじて、もしそういう技術を持っている人がいるのであれば、そういう人を認定しようという考えです」（奥原氏）

人材を育てる以前に、まず「見つける」から始めているということなのだ。

「世の中で、セキュリティ人材が足りないという話かなされていますが、私が思ったのは“本当はいるのではないか”ということです。本当はいるのに、ちゃんとそれを見つけていることができていない。もしかしたら、本人も分かっていないかもしれないし、会社もそうした技術を持っている人が誰かをちゃんと分かっていないのではないか、という仮説を立ててみました」（奥原氏）

こうした“仮説”が閃いたのは、自ら永くセキュリティの業務に携わり、また社内インシデントに対応するCSIRTチームのリーダーとして社内を見渡していた奥原氏の経歴と実感のなせる技と言ってよいだろう。

「可視化の必要を感じた理由の一つには、現場で「セキュリティができます」と本人が言ったとしても、その価値を必ずしも十分に理解してもらえていない現実がありました。だから、会社として「そういう人は大事な人だ」と認めてあげる、そういう制度を作ったかったということがあります」と奥原氏は述べる。

実際、奥原氏は社内人材が見えていないことを痛感していたという。

「可視化できていない人は多かったですね。とくに分らなかったのは、主要業務がセキュリティではない人たちです。全社の人材認定システムや教育システムは、基本的にはその人の業務分野を先に決めて、その分野の育成のために運用しています

図表2：「セキュリティマイスター」の人材モデル類型

	セキュリティ戦略/統括	企画/設計	開発/構築	運用/管理	監査/検査	コンサルティング/教育
ハイマスター領域	グローバルホワイトハッカー					
	コンピュータウィザード					
	コードウィザード			シニアセキュリティコーディネーター		
エキスパート領域	サイバースクアセッサ	セキュアネットワークコーディネーター		フォレンジックエンジニア		
	セキュリティプロダクトエキスパート		サイバースリサーチャー	ペネトレーションテスター		
	レジスタードセキュリティスペシャリスト			セキュリティアナリスト		
フィールド領域	システムセキュリティエンジニア			シニアセキュリティインシデントハンドラー		
				セキュリティインシデントハンドラー		
	業種特化マイスター（官公庁など）					
一般	一般SE向け人材育成（セキュリティ認定制度の対象外）					

出所：富士通株式会社

ので、「主要業務としてセキュリティを目指しているわけではないけれどもセキュリティの知識を有しているという人」は把握できていませんでした」

こうした人々に対し、あなたのスキルはこういう風に定義できて、それはこうしたレベルにありますよと教えてあげる。それが社内のセキュリティレベルを上げるための大切な第一歩だったのである。その点で、この制度は正しい解だったようだ。

「社内のどこに、どんな人がいるのか、フラグを立てて回るといふことができる程度できてきました。もっとも、それが成功していると言えるかどうかは、今後それらの人材をどう生かすか次第だとは思いますが」（奥原氏）

あくまで現場ありきで運用される人材モデル

この制度のもう一つの大きな特徴として「現場ありき」の発想がある。

「まず、現場のニーズを大事にして、それらに基づくセキュリティ技術者人材像を定義しました。アメリカなどの制度を勉強し人材像を独自に定義したとお話ししましたが、当社のグループ内にある仕事をベースにモデルを作ることにこだわりました。机上で考えたり、外部の規格で定められたりしたものをそのまま取り入れようということではなく、実際にやっている人たちの仕事を切り出してそれを人材像にしたということです。ですから、この認定を受けた人は、必ずその仕事が弊社グループの中にあることとなります。取ったけれど役に立たないということはありません」（奥原氏）

得てして企業の人材開発では、会社が定義した型に人をはめることを余儀なくされる部分が生じるものだが、全社のキャリアパスとは関わりのないところで、まずは人材の可視化を行うことを目的に作られた『セキュリティマイスター認定制度』は、実業務の中で必要とされている能力を最大限に尊重する仕組みになっており、それが社員と会社のベクトルをうまく合わせるのに役立つように見える。

実際の業務に基づいて人材像を組み立てる合理性は明らかだ。例えば、『フィールド領域』の中に『業種特化マイスター』というモデルがあるが、現在は官公庁を顧客にしている部門に特化したモデルとなっており、認定されると官公庁や自治体向けの政府統一基準の知識があ



『CYBERIUM (サイベリウム)』の様子

るといふお墨付きを社内で得られる。業種独自のノウハウを現場の意向を反映させて盛り込むことによって担当部門からの支持を得ることができ、現場主義を中心に据えることによって、実ビジネスと直接につながり、実ビジネスに合わせた柔軟な制度の展開を可能としているのである。

また、コンテンツも目指すべき人材像を基にオリジナルの教材を作成し、『CYBERIUM (サイベリウム)』と名付けられたサイバーレンジでリアルな環境を再現して、受講者に実践的な演習を体験させることができる。ここでも実務ありきの基本姿勢は貫かれている。

業務ニーズに基づくモデルもあれば、社外の公的資格との連動を全面に立てたモデルもある。最近作ったという『エキスパート領域』の『レジスタードセキュリティスペシャリスト』は、国家資格である『情報処理安全確保支援士』を取得すると自動的になることができる。

現在の『セキュリティマイスター認定制度』は人事評価とは連動しておらず、その点について今後どうしていくかは社内で調整中とのことだが、会社の人材育成や人事制度から自由なフィールドで、様々なニーズと向き合いながら発展させているところにこの制度の特色と魅力があると言って差し支えなさそうだ。

自発的な教育を誘発する制度

話を聞いていて感心するのは制度を受け止める社員の側の積極的な反応である。それは700人の予定だった認定者があつという間にその4倍の約2,800人に達したという事実で端的に表れているが、そうしたやる気を引き出したのは、制度を設計した奥原氏の次のような明確な意図だと思われる。

「もちろん彼らのスキルセットもノウハウも大事な

ですが、そういう人材が自分自身をモチベートできることを大事にしたいなと思っています。そうした認定を受けると、自分はセキュリティが分かるエンジニアだとフラグが立ちますから、ちゃんとやらなければいけないと思ってもらえたり、情報収集をして周囲に提供するといった活動してもらえたりするといいなというのが基本的な発想です」(奥原氏)

事務局が用意している「コミュニティ」ではSNSやメーリングリストを用いてマイスターたちが情報をやり取りし、『フィールド領域』のマイスターが『エキスパート領域』や『ハイマスター領域』のマイスターから知恵を借りるといった活動が自然とできあがっており、何よりも社員本人からは「社内で活動しやすくなった」という声が聴こえてくるという。

「『フィールド領域』はもちろんですが、『エキスパート領域』でも認定の意義はあったと思っています。例えば“ペネトレーションができる人”といったドメインはなかったの、それを作ることによって本人も活動がしやすくなっていると思います。我々から見ても、「あのサービスは、あのペネレーターがやっているので安心だ」といったことが見えるようになってるのは利点です。それをビジネスにどう活かしていくかが次の課題になります。」(奥原氏)

人事制度とは連動しておらず、処遇上のメリットとは直接関係ないし、認定のための受講費用は現場持ち。それでも社員が率先して取得してくれる『セキュリティマイスター認定制度』の成功の裏に制度設計と運用にあたった奥原氏の慧眼があったことは疑いがない。

インタビューの最後に、セキュリティ人材育成の意義についてIT業界リーダーである富士通の立場を踏まえて奥原氏の思いを訊いた。

「『セキュリティマイスター認定制度』は弊社の制度ではあるのですが、そのベースには日本全体でセキュリティ技術者が足りないという国の課題があり、それに対する一つのソリューション足りえるといいなと考えています。その意味で、他社様と連携できるようなことがあれば前向きに対応をしていきたいですし、富士通の人材を育てるだけでなく、日本のセキュリティ人材を底上げすることに貢献できればいいなと考えています。サイバーレンジも公開できるところは公開し、公共的な目的でも使っていただけるといいなと思っています」(奥原氏)

(文責：編集部 中山隆)

プロフィール

奥原 雅之 (おくはら まさゆき) 氏

1990年富士通入社。フィールドSEを経て1998年より情報セキュリティ業務を担当。2010年より社内CSIRTチームである「富士通クラウドCERT」のチームリーダー。2011年より現職の前身組織である情報セキュリティセンターのセンター長に就任。2015年より現職。

平成 29 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
人材研修部 部長代行 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、平成29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）を東京で実施した。

第1期である平成27～29年度までの3年間の講習を振り返り、取りまとめた。

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14回（平成28・29年は東京で各2回）実施した。



講習風景



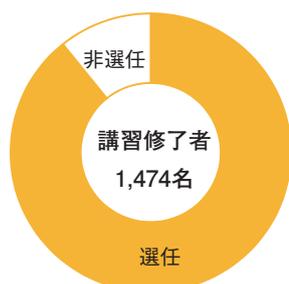
講習テキスト・追補版

1 受講者

第1期講習修了者は1,474名で、内11%ほどが受講時点で非選任の受講者であった。年齢は、平均年齢が50歳で、60歳以上の割合は15%であった（平成29年度講習修了者：188名、内約6%非選任。平均年齢48歳、60歳以上7%）。

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る。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る。選任後は講習の有効期限内において受講の必要はない。

図表1：受講者内訳（27+28+29年度）



図表2：受講者の年齢（27+28+29年度）

	平均	最年少	最年長
選任	50.0歳	25歳	83歳
非選任	48.0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る。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る。登録事業者は316事業者（2月末現在）であり受講済み事業者は第1期合計（以下「累計」と言う）で約80%だった。非選任で受講された方が選任となったかは不明であるが約69登録事業者が全く受講していない形となっている。この他、受講期限の切れている方は平成28+29年度で35名存在した。

また、選任受講者中の累計52名が1社ではなく複数の事業者から選任されており（52人で延べ147社から選任）、県間をまたがる選任も累計27名ほどいた。

これらについては法制度改正後の1期目でもあることなどから、「都合が悪く講習期限を超えますがよろしいですか」と、協会に問い合わせる方があるなど十分に周知・理解されていない状況にあることから、総務省関係部署にて十分に管理・指導して頂く必要があると言える。

なお、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29%と約3分の1であった。

3 修了考査

第1期修了考査合格率は97%で、不合格者は41名であった（平成29年度合格率98%、不合格者4名）。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の確に把握できるものであること」とある。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る。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る。また、合格基準は講義に集中できるよう、70%以上としている。

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慮して、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る。

図表3：実施年度別正解率

平成	27年度	28年度	29年度	全体
伝送交換	88.1%	88.5%	89.9%	88.3%
線路	85.9%	89.2%	87.3%	88.2%



修了考査風景

4 講習修了者・修了証の発行

第1期の平成30年2月末の講習修了者は累計で1,474名（内平成29年度188名）であった。

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、選任されている事業者名を含め総務省への報告を行っている。

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、例えば平成27年7月の講習修了者は平成30年7月31日までに受講することとなります。

5 平成30年度を迎えて

平成30年度は27年度受講修了の方1,095人が3年の有効期限ともなっており、第2期のスタートでもあります。昨年10月に登録講習機関の更新申請を行い、2月に公示し案内を送付させていただきました。27年度講習修了の方はその受講同月までに受講しなければならないことから4月より優先して受付を開始し、一般の受付を5月からとしました。30年度は東京・大阪・福岡で7月から12月まで伝送交換技術・線路技術の各8回（計16回）定員1,220名を計画している。

また、テキストを告示に合わせ一新するとともに、事前配布や事前課題などにより短期間ではあるがより充実した講習となるように準備を進めている。あわせて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するなど修了証をお持ちの方にご提供する等のアフターフォローを実施していきたい。

○お問い合わせ

協会 電気通信主任技術者講習担当
03-5907-7575（平日10時～16時）
HP <https://www.dekyo.or.jp/jinzai/>

工事担任者試験、合格に向けた ゼロからの出発

山梨県立富士北稜高等学校
電気情報系列 教諭 楠 秀樹 氏



学校紹介

本校は平成16年に北富士工業高等学校と吉田商業高等学校が統合され創立された山梨県では二校目となる総合学科高校である。総合学科では現在、教養、福祉健康、総合ビジネス、電気情報、機械テクノロジー、建築デザイン、6つの系列があり、それぞれ専門的な教科を学ぶことができる。「明日を拓き、未来を創る」という校訓のもと、生徒達は部活動や資格取得に熱心に取り組んでいる。各年次の定員が260名であり、例年90名前後が工業系の系列を選択する。電気情報系列の選択者は平均すると各年次30名ほどである。

工事担任者試験への取り組み

本校の電気情報系列は平成26年度入学生まで系列内に情報エレクトロニクスコースと電気エネルギーコースの2コース制であった。情報エレクトロニクスコースは電気通信の工事担任者試験の認定校（AI3種とDD3種）であったにもかかわらず、DD3種の合格者がほとんどいない状況であった。そのため工事担任者試験の合格を目指すことはまさしくゼロからの出発であった。平成27年度入学生よりコースを統合し、新教育課程で学ぶこととなったのを期に、電気情報系列の生徒にDD3種の資格取得を積極的に行っていくこととした。なお、平成27年度以降の入学生の学ぶ新教育課程においても、工事担任者試験の認定をいただいている。

本校の1年次生は前期の期間、各系列の体験授業を受けたのち、系列を決定する。本校では本人の希望を優先するため、各系列の定員を設けていない。そのため各年次で電気情報系列の生徒数は年次ごとに異なるが平均す

ると30名程度である。1年次後期から選択した系列の専門的な教科の学習が開始する。ただ、1年次の専門教科の単位は2単位であり、本格的に専門的な学習が開始するのは、実質的には2年次になってからである。そのため工事担任者試験の受験についても、2年次の秋の試験からの受験になる。本校では2年次により電気基礎、電子回路、電子情報技術を学び始める。それまで学んだ専門的な知識が身につけているかを確認する意味でも2年次の秋の工事担任者試験DD3種を生徒達に受験することを勧めている。

各分野の対策について具体的に述べる。DD3種の「基礎」分野については上記の専門教科で学んだ内容が多く含まれるので、夏休みの宿題として過去問を数回分与え、休業明けに確認試験を行っている。「法規」の分野は、基本的に法律で決まっていることなので必然的に暗記的な要素が多い。DD3種の申込みを終えた時点で、早々に法規の学習に取りかかるように生徒達に指示している。過去問を分析すると出題される条文の箇所は限定されている。そのため課外では資格試験用のテキストを購入するように指示をしている。テキストにはリックテレコム社の『工事担任者DD3種標準テキスト』を用いている。上記テキストでは良く出題される部分が強調されていて非常に使いやすく、生徒にも教えやすい。「理論」分野については、生徒達が情報機器に触れる機会をなるべく多くするなどの工夫をしている。課外に使用する部屋がコンピュータ室であるので、コンピュータ室の備品をもとに説明を行ったりしている。具体的な例を示すことで、生徒の知識の定着を図っている。問題演習は過去問を使用し、課外時に前出のテキストを用いて該当箇所を説明している。

最後に本年度の受験結果について報告する。昨年度の合格者が8名であったのに対し、今年度の合格者は5名にとどまった。生徒達に本格的にDD3種試験の指導を行うようになって、生徒達の得意、苦手としているところの分析を進め、更により資格試験対策が出来たらと考えている。今後も系列の職員が協力して継続して工事担任者試験の合格者を輩出できるように努めていきたい。



校庭から仰ぎ見る巨大な富士山

合格者の声



電気情報系列 2年
佐野 開穂

この度私は工事担任者DD3種を取得しました。この資格を取得した理由は、今後の大学進学や就職に有利になると思ったからです。また、インターネットやネットワークの知識をさらに深めようと思ったからです。

この資格は三つの科目があり、私は全ての科目を一発で合格しなかったため過去問を何度もやったり専門の教材を見たり先生や友人に相談したりと、何度も試行錯誤していました。基礎の科目が少し苦手な前日になっても合格点にとどかなかったので不安な気持ちで当日をむかえました。

試験を受けた後の自己採点では、心配だった基礎も合格点にとどいていて未だに嬉しかったのを覚えています。ですがどこか気がかりだったので家に合格通知が届いたときは肩の荷が降り軽くなった気がしました。

今回の試験でどんなに不安でもどんなに心配でも結果を信じて努力を続ければ実を結ぶのだなと思いました。人生の糧になったし、社会人になったら活かしていきたいです。



電気情報系列 3年
大森 匠

私が工事担任者DD3種の資格試験を受験したのは、インターネットや情報ネットワークはこれからの社会で必要不可欠なものになってくると思うとともに、インターネットの知識にも興味があり、この資格取得を通して今よりも知識を深めたいと思ったからです。

工事担任者DD3種の資格は国家資格ということもあり、初めて問題集を見た時には、難しい問題ばかりでとても不安でしたが、休み時間や家庭でも過去の問題を解きながらわからない部分は問題集を用いて何度も繰り返し勉強しました。

その結果、工事担任者DD3種を無事に取得することができました。努力して勉強した結果が資格の取得に繋がったので、とても嬉しく思っています今回の資格取得を通して、目標に向けて少しずつ努力をする大切さを学ぶことができました。

これからは社会人になりますが、社会人になってからも勉強していくことは大切だと思いますので、自分の知識を深めるだけでなく、仕事の幅も広げられるように様々な資格取得に挑戦していきたいと思っています。

国税関係帳簿書類のスキャナ保存で拡大する タイムスタンプ利用



アンテナハウス株式会社
取締役e-ドキュメントソリューショングループ
グループリーダー 益田 康氏

書類の効率的な処理は組織にとって普遍的な課題である。書類の作成と保管は事業を遂行するに当たり常に付いて回る作業であり、仕事をする上では息をするのと同じぐらい当たり前の行為だが、その上手下手は組織全体の効率に大きな影響を及ぼす。さらにe-文書法で書類の電子化が認められ、電子帳簿保存法で国税関係の書類の電子化への対応が具体的に定められた現在、帳簿書類を含む文書の電子保存への対応は多くの企業にとって真摯に取り組むべきテーマとなってきている。今回は、書類電子化のソリューションを提供するアンテナハウス(株)の益田康夫取締役にお話を伺った。

多言語組版ソフトとPDFフォーマットでグローバル市場を開拓

アンテナハウスは代表取締役の小林徳滋氏が「世界で売れるソフトを作る」を標榜するソフトウェアベンダーである。ISOの電子組版国際規格であるXSL-FOに準拠し、Unicodeで扱える50以上の文字をトランスペアレントに変換できる自動組版ソフト『AH Formatter』が世界規模でトップシェアを誇り、マニュアル類を取り扱うグローバル企業にはなくてはならない製品となっている。

また、1980年代後半からはワープロ専用ソフトで作られた文書をPDFに変換するコンバータソフトが当たり、PDFの分野でも地歩を築いている。日本の国税庁に当たる米国の内国歳入庁（IRS）では、同社のフォーマットを用いて税務関係のPDF資料が作成されており、パッケージソフト『瞬簡PDF』は同社を代表する商標の一つである。

東日本大震災で売上を落とした後にV字回復を図った2015年には、稲盛経営者賞を受賞するなど、自身の強みを知り、市場の動きに即応できる戦略性を持った企業だ。

コンサルティング力が支えるe-文書ソフト『ScanSave』（スキャンセーブ）

同社が電子組版、PDFに続く3本目の柱として位置づけるのがe-文書ソリューションである。紙の書類をスキャナ保存するためのアプリケーションソフト『ScanSave』が目下の主力製品。スタンドアロンで動く最初のバージョンから始まり、顧客の要望を取り入れて機能を強化し続け、現在ではWeb版、クラウド版まで揃えて大企業から中小企業に至る幅広い企業のニーズに対応している。

「顧客の会計システムやワークフローと組み合わせ、タイムスタンプが使える、スキャナ保存や「電子取引」PDF保管ができ、CSVやWeb連携のインターフェースがしっかりとれるという必要とされるすべての電子文書ニーズに対応します。だから既存の社内システムに組み込んでもらいやすいということがあります」と益田氏は語る。

同社がこの分野で競争力を維持しているのにはいくつかの理由があるが、印象的なのは、いたずらなカスタマイズを排除し、同社の資源を最大限パッケージに取り込むことで、製品のポジションを強固にするとともに、導

入のためのコンサルティング、導入後のコンサルティングを重視し、製品採用のてこにしている点だ。

「お客様からは、「アンテナハウスはワンストップでやってくれるので助かる」と喜んでいただけます。我々の強みは現場を熟知するとともに、現場の意見を機能アップにつなげている点にあると考えています」と益田氏はその重要性を強調する。

社内文書、証憑の取扱い全般を見渡した上でコンサルティングを実施

また、コンサルティング力という点にさらに踏み込むと、そこにも同社の戦略性がくっきりと見えてくる。同社のコンサルティングは、自社の製品を売り込むのではなく、顧客の問題解決を目指すという、マーケティングの教科書を地で行くスタイルを貫いているのだ。益田氏は述べる。

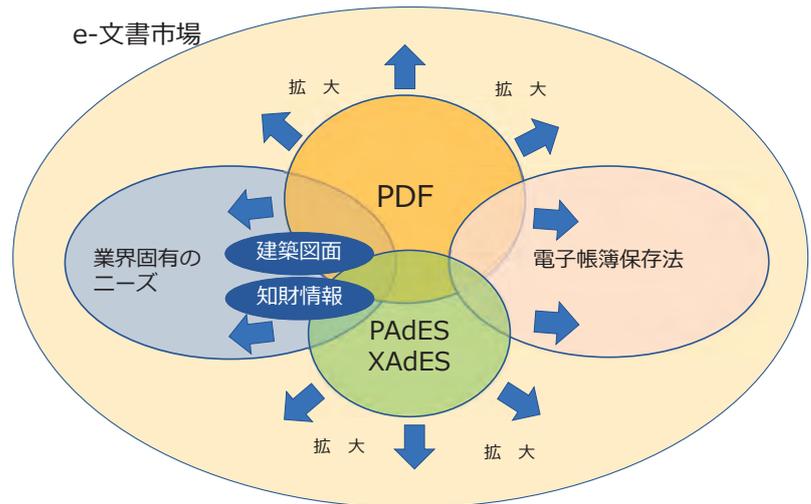
「他社様の営業は、スキャナ保存ソフトを開発し、営業教育をしても、スキャナ保存の範囲にとどまってしまう傾向があります。スキャナ保存のことは分かっても、周辺領域に話を振られると分からない。「電子的な方法でPDFをもらうことがあるが、それはどう処理すればよいのか?」、「EDIはどうすればよいのか?」、「伝票の扱いは?」などといったことを問われたとき、スキャナ保存自体の知識しかないに対応が難しくなってしまいます」

文書情報管理士上級の資格を持つ益田氏は、文書化にまつわるコンサルティング力を高めるために行政書士や簿記の資格まで取得しており、スキャナ保存を導入する際、企業が何を考える必要があるかを的確に伝えることに力を注いでいる。

次の一手として重視するのはタイムスタンプ技術

帳簿書類のスキャナ保存が広まることによってタイムスタンプの利用も伸びていくが、まだ実績は限られており、国税庁の発表（2017年10月）によれば、2015年度のスキャナ保存文書は1,050件に過ぎない。それでも前年が380件だったことを考えると、明らかに伸びを示している。益田氏も「タイムスタンプ利用に力を入れている企業がたくさん出てきていますから、今後の申請数は5千件、1万件程度まではすぐに到達するのではないかと思います」と今後の拡大に期待する。同社への引き合いも確実に伸びていると言う。

図表：アンテナハウスのe-文書事業領域のイメージ



ただ、スキャナ保存の市場拡大がこれからという今、益田氏は「その次」の開拓に視線を向けている。

「いずれにせよ、電子帳簿保存法だけに依存してはビジネスの広がりには限られてしまいます。紙は減ってきていますから、スキャナ保存自体が注目されるのは、あと数年ではないかとも思っています。EDIや電子取引がどんどん広まっており、将来的には電子保存が中心になってきます。ですので、私どもの事業としてはその次を考えていかなければなりません。」

そこで注目しているのがタイムスタンプだ。益田氏は「我々のコア技術にはPAdES、XAdESなど電子署名・タイムスタンプの技術がありますので、そこを広げていく必要があります」とこの分野でのさらなるビジネスの開拓に意欲を示している。

企業プロフィール



会社名：アンテナハウス株式会社
 本社所在地：東京都中央区東日本橋2丁目1番6号
 東日本橋藤和ビル5階
 代表取締役：小林 徳滋
 設立年月日：1984年8月
 ホームページ：<https://www.antenna.co.jp/>

09 Pマーク取得事業者の横顔

株式会社アイ・コミュニケーション



株式会社アイ・コミュニケーション
代表取締役 目次 真司 氏



株式会社アイ・コミュニケーションは島根県松江市を拠点に双方向告知通信システムの開発・販売等を手がける企業である。過疎の問題にITを用いて対応しようとする同社の取り組みが評価を受け、平成29年12月には、経済産業省が選定する「地域未来牽引企業」の1社にも選ばれている。

——会社設立の経緯について教えてください。

私は1990年にケーブルテレビ施設関連の設計事務所として株式会社メディアトークを設立しました。当時のケーブルテレビ業界はメーカー主導で、機器に合わせた設計・施工を行っており、自治体やケーブルテレビ局の立場に立って中立的な機器選定や効率の良い設計が行われていないことに疑問を感じたことが始まりでした。お客様に寄り添って業務を行っていたある日、業務先の自治体の町長から「通信インフラを整備することは良いが、若者がインターネットを使うだけになっている。年寄りにも意味のあるサービスはできないか。」と言われ、末端の利用者である住民、特に過疎化の進む中山間地に住む高齢者でも利用する価値のあるサービス提供が必要だと感じました。そこで2008年に株式会社アイ・コミュニケーションを設立し、双方向告知通信システムの開発・販売を行うようになりました。

——貴社の主な業務内容は何ですか？

「知らせますケン」

弊社は双方向告知通信システム「知らせますケン」の販売を行っています。自治体の情報を住民にお知らせするには広報や回覧板、ホームページへの掲載等が挙げられますが、その中で告知端末を住民宅に設置し放送を行う方法があります。「知らせますケン」は耳の不自由な

高齢者でもお知らせの確認ができるよう、画面と音声で構成されています。「知らせますケン」は中山間地の自治体を中心に85,000世帯の方にご利用頂いています。

「知らせますケンII」

東日本大震災の時、「知らせますケン」を導入する自治体も被災したことを受け、家庭に設置した端末の限界を痛感しました。外出した方、町外に移住した方でも自治体の発する情報を即座に受けることができれば、災害時に情報が遮断されることも無く、かつ、地域との繋がりを保ち続けることができるのではと考え、「知らせますケンII」の開発を始めました。

「知らせますケンII」は各個人の所有するスマートフォン、タブレットに対し告知情報の発信が行えます。個人の所有する端末を利用することで導入する際の費用負担の軽減も見込めます。昨今、スマートフォンの保有率が60%を超えたとされていますが、地域の高齢者にはスマートフォンやタブレットの操作が出来ない方も多くいらっしゃいます。我々は「いつでも・どこでも・だれでも」を合言葉に、スマートフォンやタブレットの操作に慣れていない方でも直感的に操作できるよう工夫し、多くの方にご利用していただけるものづくりに邁進していきたいと思います。



テレビ電話端末を活用する「知らせますケン」(上)と、端末機器を選ばないクラウド型「知らせますケンII」(下)

——Pマークを取得しようと考えたのは何故ですか？

ケーブルテレビ施設の設計のみであれば個人情報の取得について管理することはあまり多くはありませんでした。しかし、「知らせますケン」の販売・保守を行うにあたり、告知端末を導入する自治体の住民の個人情報を多量に取扱う必要が出てきたため、Pマークの取得を考えました。現在、「知らせますケンII」のユーザーの個人情報も取扱うようになり、今後、個人情報の管理は一層強くなる必要となっていくことが考えられる中、Pマークがあることで個人情報を扱うことがどれほど責任重大であることなのかを社内で認識することにつながっています。

——個人情報保護の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？

今回でPマークの更新は4回目になるのですが、前回の3回目の更新時までは、個人情報管理台帳に挙げていた個人情報の項目が多く管理するのが大変でした。個人情報管理台帳は部署毎の個人情報を記載しているのですが、同じような個人情報を重複して記載していたり、氏名だけの書類も個人情報管理台帳に挙げて管理していたりしていたからでした。前回の審査後にまずは個人情報管理台帳の見直しを行い、特に重要な機微な個人情報を重点的に管理していくことにしました。個人情報を整理したうえで、個々の個人情報について、改めてリスク分析等をし、運用を見直すことにしました。その結果、無駄な作業が減り、本当に重要な個人情報に特化して、PMS（個人情報保護マネジメントシステム）を運用することによって、会社全体の個人情報漏洩のリスク低減

につながっているのではないかと考えています。

——審査を通じて感じられたことを教えてください。

更新の審査を通じて、PMSを運用していく上で最も重要なことはPDCAのサイクルを回していくことだと改めて認識しました。特に「D」で実際に実施していくことはもちろんですが、「C」でチェックを行い、不備があれば「A」で対策を打っていき、また運用していくといった運用レベルの質を上げていき、できる限りリスクを減らしていくことが重要だと感じています。

また社内のPMS運用のレベルを上げるために、まずは個人情報保護の知識を高める必要があると考え、2年前に日本データ通信協会に個別の研修を開催していただきました。従来から抱いていたモヤモヤした疑問などにも丁寧に解説してもらいました。おかげさまで今までの運用を改めて見直すことができ、しっかりとした運用が再スタートできたものと感謝しています。

——今後強化していくポイントは何でしょうか？

今まで自治体に納めさせてもらっている告知システムですが、今後はインターネット上に設置している弊社のサーバで告知システムを運用してもらってクラウド型にシフトしていくことを考えています。クラウド型のシステムを利用してもらうことによって、専用の端末だけでなく、スマホなど個人が所有している端末にも告知配信ができ、従来の自治体の住民だけでなく、住民以外の関係する方々にも利用できるようになります。それによって、弊社が扱う個人情報の幅が広がってくる反面、より個人情報漏洩のリスクが高まってくるものと思われます。クラウド型のシステムにおける個人情報保護については、クラウドサーバのセキュリティ強化はもちろんですが、漏洩するリスクが高まることを再認識して、リスク分析をしっかりとっていくことが重要だと考えています。

企業プロフィール



会社名：株式会社アイ・コミュニケーション
 本社所在地：島根県松江市北陵町 46-4
 代表取締役：目次 真司
 設立年月日：平成 20 年 4 月 1 日
 ホームページ：<http://www.i-communication.co.jp/>

編集後記

言わずもがなですが、日本に暮らす私たちの情報空間はインターネットに席卷されています。JR山の手線の車両に乗り込み、目の前の長椅子に座っている8人に目をやると、そのうち7人がスマホの画面に見入っているのがごく当たり前の光景というご時勢です。単行本や文庫本どころか、漫画雑誌を読みふけているサラリーマンを目にただけで、懐かしさに頬が緩んでしまいそうになるかというくらいのものです。

そんな時代に広報誌『日本データ通信』の担当者になりました。いま紙の広報誌を発行するのは、なかなかアナクロニズムの匂いが漂う作業ではあるのですが、作るからにはぜひ紙媒体ならではの気品と読みやすさを備えた毎号になるよう、心をこめて仕事をしていきたいと思っています。

そして、メディア多様化時代の流れに応えるという意味で、『日本データ通信』は、本年1月よりWebでのコンテンツ配信を始めました (<https://www.dekyo.or.jp/info/>)。冊子版で読める記事は漏れなくWebマガジン『日本データ通信』でお読み頂くことができます。さらに、字数の制約から解放される電子媒体の強みを活かして、同じ記事でも冊子版よりも長めで内容豊かな記事を掲載したり、刊行時期にとらわれないメリットを活かして、冊子版には紙面の都合上盛り込めないWebマガジン独自記事をお読み頂いたりするなど、ハイブリッドなメディア活用を目指しています。どうか新しいWebマガジンを含め、引き続き『日本データ通信』に対しご愛顧を賜りますようお願い申し上げます。(中山)

日本データ通信 【通巻218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30年4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>



国家試験

電気通信主任技術者試験

平成30年度 **第1回** 試験実施日

平成30年7月8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4月1日(日)～5月9日(水)	平成30年5月10日(木)まで
郵送申請	実務経歴の申請がない場合	平成30年4月1日(日)～5月9日(水)	
	実務経歴の申請がある場合	平成30年4月1日(日)～4月20日(金)	

合否発表

平成30年

7月30日(月)

平成30年度 **第2回** 試験実施日

平成31年1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10月1日(月)～11月7日(水)	平成30年11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10月1日(月)～11月7日(水)	
	実務経歴の申請がある場合	平成30年10月1日(月)～10月22日(月)	

合否発表

平成31年

2月18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 東京都豊島区巢鴨2-11-1 巢鴨室町ビル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