IIJ. news

IIJ was founded in 1992 as a pioneer in the commercial Internet market in Japan.
Since that time, the company has continued to take the initiative in the network technology field, playing a leading role in Japan's Internet industry.
The history of IIJ is indeed the history of the Internet in Japan.

June 2019
VOL. 152

特集 進化する
メッセージング・テクノロジー

IIJ. news
June 2019
VOL.152

ぷろろーぐ　梅雨時の憂鬱 ／ 鈴木 幸一　3

Topics　進化する メッセージング・テクノロジー　4

メッセージング・テクノロジーを取り巻く環境 ／ 櫻庭 秀次　5

今さら聞けない！ メールの基礎知識 その1
メール配送の仕組みとそれを悪用したサイバー攻撃
／東京農工大学大学院工学研究院 北川 直哉 氏　8

今さら聞けない！ メールの基礎知識 その2
あなたのメールが迷惑メールとして扱われる前に
／東京農工大学大学院工学研究院 北川 直哉 氏　10

迷惑メール対策活動の広がりとJPAAWG設立の意義
／迷惑メール対策委員会 北崎 恵凡 氏、迷惑メール対策推進協議会 加瀬 正樹 氏、櫻庭 秀次　12

大規模メールシステムの構築
／コミュニティネットワークセンター ニコライ・ボヤジエフ 氏　16

業務アプリケーションに進化する ビジネスチャットツール ／ 金子 健　18

人と空気とインターネット　新たなブルーオーシャンを目指して ／ 浅羽 登志也　20

Technical Now　白井（しろい）データセンターキャンパス 稼働開始　22

インターネット・トリビア　プロトコルの安全性／ 堂前 清隆　24

グローバル・トレンド　ジャカルタのMRT ／ PT. IIJ Global Solutions Indonesia 西川 善高　25

ライフ・ウィズセーフ　10年にわたる負け戦（いくさ） ／ 齋藤 衛　26

ぷろろーぐ

梅雨時の憂鬱

株式会社インターネットイニシアティブ
代表取締役会長
鈴木 幸一

私にとって梅雨と言えば、紫陽花、蝸牛が思い浮かぶのだが、最近、蝸牛を目にすることがない。庭のない空中の集合住宅の住まいが長いからだろうか。

生活の話はさて置き、株主総会の時期である。IIJがニューヨーク・ナスダック市場に上場したのは、一九九九年の夏だった。その年は、梅雨から夏にかけて、公開の準備、ロードショウ、上場と、ほとんどの時間を米国、欧州で過ごし、梅雨の湿気とは無縁だった。あれから二〇年も経ったのかと、過ぎ去った時の感覚は魔法のようである。

「二、三年もすると、三〇周年ですね」。知人に、ふと、そんな言葉を掛けられる。「ええっ」と、驚くほかない。季節の移り変わりには敏感なのだが、会社の時間の経過については、忘れたままである。言われてみれば、IIJは創業から二七年を経ているわけで、「そろそろ三〇年ですね」という言葉が、的外れというわけでもない。時の経過を忘れさせるほど、インターネットの発展の速度、広がりは、技術からサービス、利用形態に至るまで、歴史を変えてきた過去の巨大な技術革新と同じである。巨大な技術革新が変えてきた世界が、良かったのかどうかは、その時代に生きた人間にしか実感できない。

三〇年前にはほとんど知られていなかったインターネットという通信だが、今や子供から老人まで、日々の生活に欠かすことのできない通信手段となっている。電話と違い、その通信は情報と一体となった手段であり、世界のあらゆる仕組みを変えてしまう技術なのだが、一般の利用者は、そこまで考えることはない。巨大な技術革新が進行する世界で、その技術を利用する人々の意識はそんなものである。

インターネットの発展をリードしてきたと自負する企業の人間にとって、インターネットの世界は、いつときも留まることがない過酷な世界でもある。「昨年と同じ」という言葉で済まされる事業計画も技術もない。クラウド、IoT、5Gといった大きなテーマについては、言葉が流布する前から取り組みを始め、言葉が流布し始めた頃には、開発も進み、自らのサービスとして、いかに市場に投入し、収益を上げていくのかという見通しを立てられるくらいでないと、マーケットから取り残されてしまう。年度単位の数字に捉われれば、将来を失うことになりかねず、長期的な視野を重視し過ぎると、足元の利益を犠牲にすることになる。創業以来、会社の規模にかかわらず、技術帝国主義とか技術至上といった言葉で評されることが多かったIIJにとって、中長期的な視点と短期的な視点をどう噛み合わせ、バランスをとっていくのかは、いまだにもっとも難しい経営判断のテーマである。

五月の長い連休中に、幹部とされる肩書の付いた社員と、合宿と称して泊りがけで議論の場を持ったのだが、将来に向けての明晰な意見交換とはならなかった。仕方なく、酒を飲んで温泉に浸かっていたのだが、酒と温泉によって明確な未来が描けるわけがないのは当たり前である。ぼんやりと思い悩むうちに、それなりの未来の形が見えてくるに違いないのだが、その間にも否応なく時間が過ぎ去っていくのは恨めしいばかりである。六月と言えば、すでに一年の半ばが過ぎ去っている。

イラスト／末房志野

TOPICS

進化する メッセージング・テクノロジー

あの人とはLINE、この人とはチャット、ここでは電子メール、
あそこでは Facebook、さらには、電話や手紙……等々、
私たちはさまざまなコミュニケーションツールをTPOに応じて使い分けている。
今回は、信頼性・利便性・汎用性などの面で
ワン＆オンリーな存在であり続けている電子メールを中心に
メッセージング・テクノロジーの最前線を紹介する。

特集イラスト／高橋 庸平

メッセージング・テクノロジーを取り巻く環境

ビジネス、プライベートの双方において不可欠で、
もっとも汎用性が高いメッセージングツールが“電子メール”である。
ここではその基本的な仕組みをおさらいしたうえで、
今後、末永くメールを活用していく際の課題を見てみたい。

IIJ ネットワーククラウド本部
アプリケーションサービス部 担当部長
櫻庭 秀次

インターネットは、その名前の通りネットワークをつなげていったものです。何のためにつなげるのかと言うと、その先に情報を伝えるため、届けるためです。現在でも情報伝達手段の具体例として「手紙」や「信号」などでメッセージを届けることをイメージする人が多いと思いますが、インターネット上の手紙と言えば、やはり「電子メール」（以下、メール）ではないでしょうか。

筆者が初めてメールを利用したのは一九八〇年代後半で、宛先によってはまだ配送経路の一部がバケツリレー方式になっているような時代でした。それでも郵便に比べれば格段に到達するのが早かったので、（電子）メールのことを単に「メール」と呼び、郵便は「スネールメール（かたつむり）メール」と呼ぶことにしよう、と言われ始めていた時代でした。

その後、携帯電話でメールが利用できるようになったり、ブロードバンドの普及などにより、ISPの利用者が増え、ISPがメールアドレスとWEBページをセットで提供するようになると、メールの利用者が急増していきました。さらに、広告などを表示することで収益を得る、いわゆるフリーメールの台頭により、誰でもメールを利用できる環境が整っていきました。

メールシステムの概要

メールに関する最初の規格は、一九八二年八月に公開されたメール配送のプロトコル（通信手順）を定めたRFC821と、メールのデータ形式を示したRFC822です。両方の規格とも、二度の大きな変更が行なわれ、現在はRFC5321、RFC5322という番号になっていますが、基本的な部分は三七年前に作られた仕様のまま利用できます。

メールが配送される仕組みは、手紙など郵便のシステムとは大きく異なります。メール送信者は、メールソフトなどを利用して、送信メールサーバに接続し、メールを送信（投稿）します。送信メールサーバは、メールの宛先ドメイン名からDNSを参照することで受信サーバを見つけ出し、直接受信サーバにネットワーク接続して、定められた配送プロトコルによってメールを送信します。

メール配送の流れは、郵便のような階層的な集配構造とも違いますし、中央集権的な――例えばSNS内でのメッセージ送信とも異なる、インターネット上の大規模分散システムとして実現されているのです。

こうした構造による利点もあります。新規でメールを利用したいと考えたとき、場所（IPアドレス）とそれを利用するメールサーバ）を用意し、名前（ドメイン名）を（DNS上に）登録するだけで、原則としてメールを使うことができます。こうした参入の容易さが、メールが広がった要因の一つであると言えます。

メールの仕様としては、基本的にテキスト文字し

か扱えないことになっています。しかしながら、メールの送り手と受け手のあいだで配送上はテキスト文字となるような変換規則を共通化できれば、バイナリデータを含めたさまざまなデータをメールとして送受信できます。この規格がＭＩＭＥ（Multipurpose Internet Mail Extensions）です。ＭＩＭＥの登場により、画像やアプリケーションデータなどのバイナリデータや、それらをテキストと混在させることのできる（いわゆる「添付ファイル」）メール仕様が作られ、メールが単なるメッセージのやり取りだけでなく、多様なデータの配送手段として用いられるようになりました。メールの利用形態の広がりです。

手紙とは異なるメールの特徴として、デジタルデータとしての利点を挙げることができます。デジタルデータは複製が簡単なので、受信したメールを再利用して送信したり、同じ文面を同時に複数（あるいは大量に）送ることが容易です。こうした特徴を生かして、受信したメールをあらかじめ登録しておいた複数の宛先に自動送信する「メーリングリスト機能」が開発され、一対一だけでなく、複数人によるグループ間のコミュニケーションツールとしても広く利用されるようになりました。また、購読者を募ってメールマガジンを定期的に提供するサービスにもメールが活用されています。

SNSとメールの違い

今日、インターネット上のコミュニケーションツールはメールだけではありません。Facebookや、それと関連したMessenger、さらにはTwitterやＬＩＮＥといったＳＮＳが、コミュニケーションツールとして広く使われています。こうしたサービスは、いわゆるスマートフォン上のアプリケーションとして利用されることで携帯性・即時性が向上し、非常に便利なツールとして利用者を増やしています。メールで利用できる多くの機能、データファイルの共有やグループチャット機能なども実現されています。筆者も最近、ＳＮＳを利用する機会が多くなりました。

ＳＮＳの普及にともない、「メールが使われなくなるのでは？」とか、「すでに若い人のあいだではメールは使われていない」といった声を時々耳にします。私もメールに長いあいだ関わっていますが、メールは絶対に残すべきシステムだと考えているわけではありませんし、基盤としてより堅牢かつ便利なシステムがあれば、そちらを使っていくべきだと思います。

しかしながら、メールと多くのＳＮＳとでは、仕組みや構造に決定的な違いがあります。最初に述べた通り、メールはインターネットとその基盤技術を利用した大規模分散システムです。インターネットの基盤が正しく運用されている限り、メールシステム全体が使えなくなるということはありません。どこかの特定の組織によって管理・運営されている、閉じたシステムではないのです。こうしたことから、新しい技術や仕様の普及に時間がかかったり、なかなか利用が進まないこともありますが、仕様策定の過程も含めてメールはオープンであり、誰でも検証できるようになっています。

メールが簡単にはなくならないと考えられる理由の一つに、ＩＤ（識別情報）としてメールアドレスが広く使われている現状があります。例えば、二〇二〇年の東京オリンピックに向けて、チケット販売が始まりましたが、チケット購入の申し込みには、事前にＴＯＫＹＯ２０２０ＩＤを登録する必要があり、この登録にメールアドレスが必要なのです。登録後のＷＥＢサイトへのログインにも、メールアドレスをＩＤとして入力する必要があります。東京オリンピックのチケット販売に限らず、多くのＳＮＳでも利用者を識別するための情報としてメールアドレスが利用されています。つまり、ＳＮＳもシステム基盤の一つとしてメールを利用しているということです。

メールをＩＤとして使う理由は、メールアドレスが@（アットマーク）の右側のドメイン名と左側のローカルパートによって〝一意的〟になっていることや、パスワードを忘れてログインできない際などの連絡手段としてＩＤの情報が利用できること、通常の情報伝達手段として利用できること……といった多くの利点があるためです。こうした依存関係が続くあいだは、なかなかメールはなくならないように思えます。

メールを使い続けるうえでの課題

メール利用が一般的になるにつれて、迷惑メールなど、さまざまな問題も発生するようになりました。最近では、直接的に金銭を搾取したり、機密情報を得るためのトリガーとしてメールが悪用されています。メールが利用され続けるためには、こうした課題を解決しなければなりません。

メール事業者である我々のアプローチは、送信者を明確に特定できるようにして、本来受け取るべきメールだけを確実に受信者に届けよう、というものです。そのための技術的な仕組みが、ＤＭＡＲＣ（Domain-based Message Authentication, Reporting and Conformance）などの送信ドメイン認証で、正しい送信者を特定する情報がドメインレピュテーションです。また、正しい送信側のシステムに問題があったり、送信者を認証する情報が脆弱だったり漏えいしているケースもあります。こうした場合、送信者が正しくても不明なメールが届いてしまうことになりますし、送信側も不正利用を検知するのがなかなかむずかしい現実もあります。これらの課題に対しても、受信側から送信側への何らかの連絡手段があれば、改善できる可能性があります。これが、ＤＭＡＲＣレポートであり、フィードバックループであると考えています。

メールが幅広い用途で利用されるようになると、送られる情報が途中で見られないように守りたいという要望も出てきました。日本では法律で「通信の秘密」が守られていると考えられているためか、こうしたメール情報を守る仕組みがあまり普及していません。しかし、メールはインターネットというさまざまな経路を通り得る基盤を介して配送されるわけですから、情報を守るためにはあらかじめ送る情報を保護しておく必要があります。

メールの配送経路を暗号化する仕組みとしては、古くからＴＬＳ（Transport Layer Security）（ＳＴＡＲＴＴＬＳ）が用意されていますが、特に日本では欧米に比べてまだあまり利用されていません。通常のメール配送の仕組みでは、ＴＬＳがうまく利用できなかった場合には平文で送ることになっているため、メールサーバがＴＬＳに対応しているから必ず暗号化されていることにはなりません。また、受け取ったメールからはＴＬＳを利用して配送されたものか否かがすぐにはわかりづらく、送信者にとっては確認する手段もありません（最近、一部のサービスで受信メールが暗号化された経路であったかどうかをアイコンなどで表示する機能を提供しています）。

この問題を解決するために、ＭＴＡ-ＳＴＳ（SMTP MTA Strict Transport Security）やＳＭＴＰ ＴＬＳレポーティングといった仕様が作られました。さらに、ＴＬＳを簡単に利用できるようにするために、ＤＡＮＥ（DNS-Based Authentication of Named Entities）も作られました。

メールの仕様が策定されて三七年が経過しましたが、現在でも新しい機能が組み込まれ、進化しています。メールが使われていく過程で、今後も進化は続いていくでしょうし、有益な機能はどんどん追加・普及していくべきです。ＩＩＪはこれからも最新技術のキャッチアップや普及に貢献していきます。

今さら聞けない！ メールの基礎知識 その1

メール配送の仕組みとそれを悪用したサイバー攻撃

ここでは、メール配送の基本的な仕組みをおさらいしたうえで、
メールを悪用したおもなサイバー攻撃の手法をまとめる。

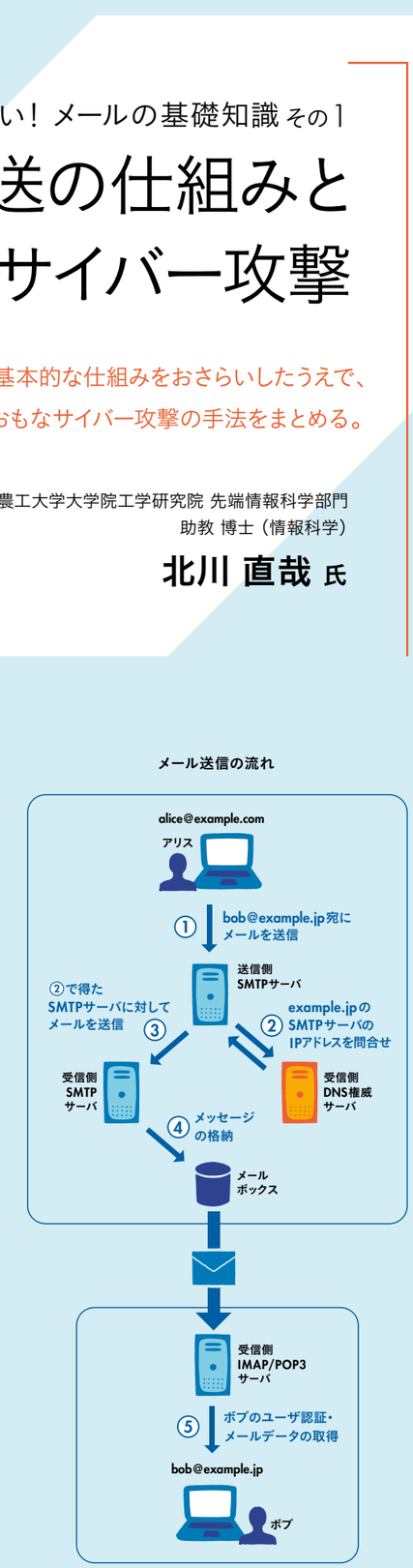
東京農工大学大学院工学研究院 先端情報科学部門
助教 博士（情報科学）
北川 直哉 氏

インターネットサービスのなかで、電子メールはWWW（World Wide Web）と並んで世界中でもっとも広く利用されています。昨今では、LINE、Twitter、Facebook Messenger、Slackといった多くのコミュニケーションツールが利用されていますが、現在でも、とりわけビジネスの世界では、電子メールがもっとも広く利用されている情報伝達ツールです。

本稿では、私たちが普段、何気なく使っている電子メールがどのように配送されているのかを解説するとともに、電子メールを悪用したサイバー攻撃がどのように行なわれるのかを紹介します。

メール配送の流れ

メール配送にメールサーバが使われることは簡単にイメージできると思いますが、さまざまな機能を持つサーバが互いに連携することでメールの送受信が行なわれています。具体例として、送信者のアリスが受信者のボブにメールを送信するケースを見てみましょう。**（右図参照）**



SMTPによるメールの配送

まずアリスが、メールソフトやウェブメール（これらをMUA：Mail User Agentと呼びます）を使ってボブに送るメールを作成し、送信します（図①）。これを受け取った送信側のSMTP（Simple Mail Transfer Protocol）サーバは、宛先であるボブのメールアドレスのドメイン（右図ではexample.jp）のメールサーバを調べるために、DNS（Domain Name System）による名前解決（MXレコード参照）を行ないます（図②）。これによって得られた宛先ドメインのSMTPサーバの25番ポートに対してSMTPセッションを確立させてメールを送信します（図③）。その後、メールを受信したexample.jpのメールサーバは、メールの宛先のユーザであるボブのメールボックスにこのメールを格納します（図④）。以上の手順により、SMTPによるメールの送受信は完了しますが、受信者であるボブがこのメールを閲覧する際は、別のプロトコルを使用します。

POP3／IMAPによるメールの受信

メールの受信側が使用するプロトコルとしては、POP3（Post Office Protocol Version 3）とIMAP（Internet Message Access Protocol）の二つが広く利用されています。

POP3サーバには、メールアカウント毎にメールボックスが存在し、配送されたメールは各メールボックスに保管されます。受信者のボブがPOP3を用いて自分宛のメールを受信するには、メールソフトなどからPOP3サーバの110番ポート（暗号化方式であるPOP over SSLの場合は995番ポート）にアクセスして、アリスからのメールを受信します（図⑤）。このようにPOP3サーバは、メールサーバに保管されたメールを受信者のパソコンにダウンロードする役割を持っています。

POP3は一台のパソコンのみでメールを閲覧する環境において利用されていましたが、個人でもパソコン、スマートフォン、タブレットなど、複数台のデバイスを使用する今日では、IMAPというプロトコルが広く用いられています。IMAPでメールを閲覧する際、受信者のボブはメールソフトなどからIMAPサーバの143番ポート（暗号化方式であるIMAP over SSLの場合は993番ポート）にアクセスして、サーバ上に保管されたメールを閲覧します（図⑤）。

IMAPはPOP3とは異なり、ローカルにあるパソコンなどにダウンロードするのではなく、IMAPサーバ上に保管されているメールのメッセージを閲覧する仕組みであるため、複数の端末から同じメールを閲覧できます。

メールを悪用したサイバー攻撃

「メールを悪用したサイバー攻撃」と言えば、「迷惑メール」と呼ばれるスパムメールによる被害を思い浮かべる方が多いのではないでしょうか。スパムメールに対しては、内容の不審さや不自然な日本語表記から簡単に見破れるというイメージを抱いている方が多いのも事実ですが、近年、スパムメールよりも問題視され、注目されているのが「なりすましメール」です。メディアでも標的型攻撃による大規模な被害の発生が頻繁に報じられていますが、電子メールは標的型攻撃と深く関係しています。

独立行政法人情報処理推進機構（IPA）に報告された、コンピュータウイルスおよび不正プログラムの検出件数と、感染経路がメール経由であるものの件数および割合を左表に示します。

ウイルス・不正プログラムの感染件数とメール経由での感染の割合

期　間	ウイルス検出件数合計	メールからの感染件数（%）
17年 10−12月	825,567	820,029（約99.3%）
18年　1−3月	155,209	138,417（約89.2%）
18年　4−6月	350,234	334,732（約95.6%）
18年　7−9月	58,261	54,608（約93.7%）
18年 10−12月	68,671	61,180（約89.1%）

この結果が示すように、近年のコンピュータウイルスの感染は、ほとんどがメールを経由しています。標的型攻撃と電子メールは深く関係していると先述しましたが、これらのメールの多くは、送信者を詐称した「なりすましメール」であると考えられています。「なりすましメール」は、会社の取引先の担当者や自社の上司・同僚などになりすまして、業務関連のメールを送信し、悪意のある添付ファイルを送ったり、攻撃サイトへ誘導するリンクなどによって、標的となった人物の端末をウイルス感染させ、機密情報を巧妙に盗み取る攻撃の「入口」として悪用します。

また、ビジネス利用以外でも、攻撃者は金融機関、自治体、ショッピングサイトなどを詐称したメールを送信し、ユーザからログインID、パスワード、クレジットカード情報といった個人情報を窃取する攻撃（フィッシング詐欺）が多発しています。

このように、電子メールに起因するサイバー攻撃では、大規模な経済的被害に直結する事例が多発しており、電子メールのセキュリティ対策はサイバー攻撃全体への対策にもつながるため、非常に重要な課題となっています。

北川 直哉（きたがわ なおや）
2014年3月、名古屋大学大学院情報科学研究科博士課程後期課程修了。同年4月より同大学情報基盤センター研究員を経て、同年10月より現職。メッセージングをはじめとするネットワークサービスのセキュリティ対策、情報ネットワーク、ワインの研究に従事。

（参考文献）
独立行政法人情報処理推進機構「コンピュータウイルス・不正アクセスの届出状況［2018年10〜12月］」
https://www.ipa.go.jp/files/000071288.pdf

今さら聞けない！ メールの基礎知識 その2

あなたのメールが迷惑メールとして扱われる前に

自分が送信したメールが「迷惑メール」に振り分けられていた……
そんな経験をしたことがある人もいるのではないだろうか？
ここでは、そうした誤審が起こる理由と対策を見てみたい。

東京農工大学大学院工学研究院 先端情報科学部門
助教 博士（情報科学）
北川 直哉 氏

とある会社との商談を順調に進めていた営業マンのAさんは、打ち合わせを調整する際、日頃からメールを利用していましたが、ある日、相手からの返信が突然、途絶えてしまいました。手応えのあった商談が破談することを心配したAさんが相手に電話で確認すると、「メール？　届いていませんよ」との回答が……。実は、Aさんが送ったメールは「迷惑メール」として扱われてしまっていたのです。

迷惑メール対策の現状

電子メールの世界では、さまざまなサイバー攻撃を防ぐために、受信側での迷惑メール対策が必須であることは言うまでもありません。一方、送信側でAさんのようなトラブルを生じさせないために、「自ドメインから送出する正当なメールが迷惑メールとして扱われないための対策」が重要になってきます。

受信側で受信したメールの信頼性を判定する方法として、メールの内容によって判断する（例えば、ドラッグ、ポルノ、偽ブランド品などに関するメールを制限する）「コンテンツフィルタリング」が広く利用されていますが、全てのメールに対してその内容から悪性度を判定するために、処理速度やスループットの低下、それをカバーするための設備投資コストの増加などが課題になっています。また、こうした問題の解決に加えて、判定の精度を向上させるために、送信ドメインの信頼性スコアによって判定する「ドメインレピュテーション」や、メール配送時の送信・転送サーバの正当性を検証する「送信ドメイン認証」などと組み合わせて多段的に判定するのが一般的かつ理想的な対策と考えられています。

本稿では、送信側ドメインから送出する正当なメールが迷惑メール判定されないための対策について解説しますが、これは受信側で対策する送信ドメイン認証技術と深く関わっています。そこでまずは、世界中で広く利用されている送信ドメイン認証技術から見ていきましょう。

送信ドメイン認証技術「SPF」と「DKIM」

現在、おもな送信ドメイン認証技術には、SPF（Sender Policy Framework）とDKIM（DomainKeys Identified Mail）があります。

SPFによる検証を行なうには、まず送信側ドメインの管理者が、SPFレコードと呼ばれる自ドメイン名を名乗って送信する可能性のあるSMTPサーバのリストを、DNS権威サーバであらかじめ宣言しておきます。受信側では、メール受信時に当該ドメインのDNS権威サーバにSPFレコードを問い合わせて送出する可能性のあるSMTPサーバリスト情報を取得し、実際にメールを送ってきたSMTPサーバのIPアドレスと比較・検証します。そして、送信してきたサーバのIPアドレスがこのリストに含まれていれば検証に合格となり、含まれていなければ不合格となります。

しかしSPFは、メールが転送された場合や、メーリングリストからの配送時に「なりすましメール」ではないものも誤って不合格と判定してしまう問題を抱えています。こうしたことが起こる理由は、受信側のSMTPサーバから見たとき、直接メールを送信してくるサーバがもともとの送信ドメイン下のものではなくなり、送信ドメインのSPFレコードで宣言されたサーバリストに含まれないためです。

次に、DKIMによる検証を行なうには、あらかじめ送信側で秘密鍵と公開鍵のペアを生成し、SPFと同様にDNS権威サーバで公開鍵を公開します。この状態で、送信側はメール送信時にそのメッセージのヘッダと、本文および生成した秘密鍵から電子署名を生成してメールヘッダに付加します。受信側では、受信したメールのヘッダ情報に従って送信側の公開鍵の公開場所を特定し、その公開鍵を用いて電子署名を照合することでDKIM検証を行ないます。ただし、公開鍵の公開場所は、メール送信ドメインとは無関係の署名用ドメインを用いても問題ありません（これを「第三者署名」と呼びます）。

重要なメールが迷惑メールとして扱われないためには、これらの認証技術に正しく対応して設定をし、自分の（正規の）ドメイン名から送出したメールなのか、あるいは「なりすましメール」なのかを、受信側が判断できるように手助けする必要があります。

ドメイン名のブランドを守る「DMARC」

SPFやDKIMを利用したメールの送信ドメイン認証をさらに補強する技術として、DMARC（Domain-based Message Authentication, Reporting and Conformance）があります。SPFやDKIMを用いた認証では、認証に失敗したメールをどのように取り扱うかは受信側の運用方針に委ねられており、認証の失敗状況やそのメールがどのように取り扱われたかについては、送信側は指示することも把握することもできません。

従来の迷惑メール対策や送信ドメイン認証がいずれも受信側で受信の可否を判断する仕組みであったのに対し、DMARCは送信ドメイン認証失敗時にそのメールをどのように処理すればいいのかという方針を、送信側が宣言できる仕組みになっています。

具体的には、送信側ドメインのDNS権威サーバにDMARCレコードとして認証失敗メールの受信側での取り扱い方を、reject（受信拒否）、quarantine（隔離）、none（何もしない）の三種類のいずれかで指定します。DMARCでは、自ドメイン名をなりすました悪意あるメールに対する受信側での取り扱い方を、本物のドメイン名の所有者が表明し、受信拒否を依頼できます。こうして自ドメイン名のブランドを保つことで、ドメイン名そのものの信頼性を高めることが大切になっています。

信頼できるメールを視覚的に表す「BIMI」

BIMI（Brand Indicators for Message Identification）は、現在、標準化に向けてIETFやM[3]AAWGなどの国際会議で議論されている新しい仕組みです。BIMIは、DMARCなどの送信ドメイン認証によって認証成功したドメインからのメールについて、受信者のメールソフトなどのMUA上にロゴマークを表示して、信頼性の高いメールであることを受信者にわかりやすく表示をするフレームワークです。

ここで紹介したように、近年議論されているメールのセキュリティ技術であるDMARCやBIMIは、従来の「迷惑メールを排除する」という目的に加えて、「重要なメールを受信側に正当であると評価させる」という新たな目的を持っています。あなたのメールが迷惑メールとして扱われないために、送信ドメイン認証を正しく導入し、配送の信頼性を高めることが大切になっています。

迷惑メール対策活動の広がりと JPAAWG 設立の意義

昨年11月、JPAAWGが発足した。JPAAWGは、迷惑メール対策などを行なう国際的なワーキンググループM³AAWGの日本リージョンという位置づけのもと、メールやモバイルのセキュリティ、マルウェア対策などを検討・実施する組織である。ここでは、同様の活動を行なっている日本の組織を紹介しながら、国内における連携や対策の強化について考えてみたい。

一般財団法人インターネット協会 迷惑メール対策委員会 副委員長
ソフトバンク株式会社
北崎 恵凡 氏

迷惑メール対策推進協議会 技術ワーキンググループ副主査
株式会社 TwoFive
加瀬 正樹 氏

迷惑メール対策推進協議会 技術ワーキンググループ主査
迷惑メール対策委員会 委員長
IIJネットワーククラウド本部 アプリケーションサービス部
櫻庭 秀次

迷惑メール対策に取り組む組織

迷惑メールがもたらす問題は、時代とともに深刻度が大きく変化しています。例えば、携帯電話やブロードバンド回線の利用が急増した二〇〇〇年前後から、広告宣伝を目的とした迷惑メールが増え、メール利用者にとって文字通り「迷惑」であったことが大きな社会問題となりました。その後、PCをマルウェアに感染させボット化させる手段としてメールが悪用され、そのボットが迷惑メールを送信することで、さらにボットを増やすという悪循環が続きました。メールによって運ばれるマルウェアはさらに進化し、PC内部やネットワーク上にある重要な情報を搾取するものや、勝手に暗号化することで身代金を要求するランサムウェアなど、悪質化していきました。

こうしたメールの不正利用、そして悪用者に対しては、メール運用事業者やセキュリティベンダが協力し、さまざまな対策を講じてきました。その最初の大きな動きは、二〇〇四年に創設されたMAAWG(Messaging Anti-Abuse Working Group)です。設立時は二〇社程度だったメンバーが、今ではグローバルで約二〇〇社にまで増えました。そして年に三回開催されるGeneral Meeting(以下、M³AAWG会合)には、基本的にはメンバーだけの会合にもかかわらず、五〇〇名前後が参加し、幅広いテーマについて議論や情報共有がなされています。二〇一二年からは二つのM(マルウェア、モバイル)を主要検討テーマに加えて、M³AAWG(Messaging, Malware and Mobile Anti-Abuse Working Group)と改称し、インターネット上のセキュリティ脅威全般を取り扱うようになりました。

IIJは、MAAWGの創設時から参画しており、二〇一九年二月に四五回目をむかえたM³AAWG会合まで継続して参加している数少ないメンバーです。

国内では、MAAWGの立ち上げに関わったIIJや携帯電話事業者などを中心に、JEAG(Japan Email Anti-Abuse Group)が二〇〇五年に創設されました。最初は、メールサービスのエンジニアなどを中心としたボランティア的な活動でしたが、OP25B[*1]や送信ドメイン認証技術の普及に向けて、国内で課題となるような法的な取り扱いについて総務省と協議したり、三つの提言書(リコメンデーション)を発表したりするなど、大きな貢献をもたらしました。こうした活動が評価され、平成二〇年の情報通信月間では、団体として総務大臣表彰を受賞しました。

現在、国内で迷惑メール対策に関する活動を継続している組織には、一般財団法人インターネット協会の「迷惑メール対策推進協議会」と、産学官による「迷惑メール対策委員会」があります。以下では、それぞれの主要メンバーに活動概要を紹介してもらいます。

迷惑メール対策委員会

一般財団法人インターネット協会では、二〇〇四年からメールサービスに関わる運用者・学識経験者を交えた「迷惑メール対策委員会」を構成し、さまざまな活動を行なっています。一定の成果が得られたことから二〇一一年度に活動をいったん休止しましたが、二〇一三年度に新たな迷惑メール対策技術の普及が必要との判断から活動を再開しました。月に一回程度の定例会合を開いて、最新動向を情報発信しています。

定例会合を通じた情報共有

迷惑メール対策に有効な送信ドメイン認証技術の一つであるDMARC[*2]の普及・促進に向けた検討や、送信ドメイン認証技術の普及状況の定期的な調査などを行なっています。

特に国内ではDMARCの普及が遅れており、迷惑メール対策推進協議会などの関係組織や企業とも協力しながら、普及に力を入れています。また、M³AAWGや、DMARCを推進するDMARC.org[*3]といった組織ともグローバルに連携していきたいと考えています。

迷惑メール対策カンファレンスの開催

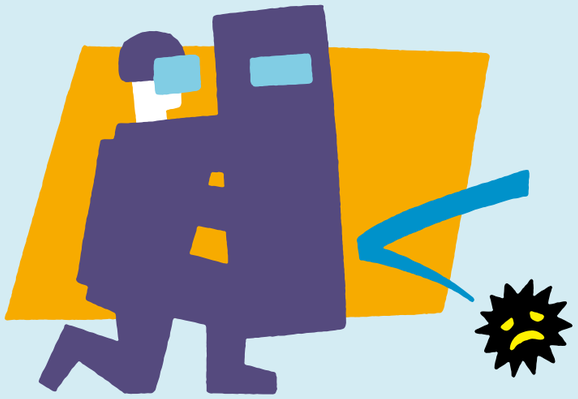
継続して取り組んでいる代表的なイベントとして「迷惑メール対策カンファレンス」[*4]があり、二〇一八年度で第一八回となりました。カンファレンスにはさまざまな立場の方が参加し、情報共有や活発な議論が行なわれています。

二〇一三年にはInternet Week 2013のなかで迷惑メール対策BoFを開催し、二〇一四年は迷惑メール対策を行なう各国の執行機関などによる会合であるLAP(現UCENet)の第一〇回会合(LAP10 TOKYO)と併催し、二〇一五年からは複数のセキュリティ関連イベントを集中的に開催するSecurity WeekにおいてEmail Security Conferenceを東京と大阪で合同開催し、二〇一八年にはM³AAWGの日本の地域ワーキンググループJPAAWG(Japan Anti-Abuse Working Group)[*5]の立ち上げイベントと併催することで、参加者の層を拡大し、迷惑メール対策の周知・啓発活動に寄与してきました。

有害情報対策ポータルサイト 迷惑メール対策編

「有害情報対策ポータルサイト 迷惑メール対策編」[*6]では、一般利用者向けの迷惑メール対策の基礎知識や、メール管理者向けに技術情報・運用情報・法令情報などを掲載しています。

技術情報としては、送信ドメイン認証技術(SPF、DKIM、DMARC)の三技術規格であるRFCやM³AAWGの技術文書ベストプラクティスの翻訳(英日対訳)、法令情報としては、迷惑メール対策実装における法的制約事項や迷惑メールを規制する法律の解説、海外の参考情報としては、ドイツのインターネット産業団体であるecoが公表しているドイツ法におけるDMARC準拠に関する報告の翻訳(英日対訳)などを掲載しています。ポータルサイトに掲載するコンテンツは、今後、充実を図っていく考えです。



迷惑メール対策推進協議会

「迷惑メール対策協議会」（以下、協議会）は、多くの関係者に迷惑メールの問題に取り組んでもらうために設置され、さまざまな情報提供・周知啓発活動に取り組んでいます。

迷惑メール白書

協議会では、迷惑メールの傾向・対策についての概説や事業者の取り組みを紹介しています。また、協議会の設立から現在に至る統計情報・参考資料をまとめて「迷惑メール白書」[*7]として公開しています。特に、協議会に参加している電気通信事業者から提供される統計情報は非常に貴重で、日本国内の迷惑メール動向を把握するうえで重要な指標になっています。

セキュリティセミナーでの講演

国内で開催されるセキュリティ関連カンファレンスやシンポジウムに協議会から講師を派遣して、電子メールに関するセキュリティや迷惑メール対策の技術を紹介しています。

例えば、二〇一七年度は「情報セキュリティワークショップ in 湯沢２０１７」と「サイバーセキュリティシンポジウム道後２０１８」において構成員が解説を行ないました。翌二〇一八年度は、自治体CSIRT協議会の技術セミナーで送信ドメイン認証（DMARCなど）について解説しました。

さらに協議会では、技術的な対策や有効性を議論する場として、技術ワーキンググループ（以下、技術WG）を設置し、参加企業のエンジニアらが技術面に特化した議論を行なっています。そこでは、迷惑メールに関する統計情報の定点観測や、なりすましメール対策の有効性・法的整理などを検討し、いくつかの活動成果はドキュメントとして公開しています。

送信ドメイン認証技術導入マニュアル

迷惑メールの一部は、正規のドメインになりすまして送信されます。「送信ドメイン認証技術導入マニュアル」[*8]では、業界全体への普及を目指して、なりすましメール対策（送信ドメイン認証技術への適応）の具体的な導入方法を紹介しています（現在、公開されているマニュアルは、DMARCの仕様作成以前に記述されたもので、DMARCに関する記述がないため、DMARCの内容を含んだマニュアルとして改訂作業中）。

迷惑メールの踏み台送信対策

近年、ISPが会員向けに提供するメールアカウントが不正利用されるケースが頻発しており、ISPから発信される迷惑メール（以下、踏み台送信）が大きな問題になっています[*9]。技術WGでは、各ISPが実施している対策を整理・共有して、協議会に参加していないISPにも、踏み台送信の対策を実施しやすいように対応方法を公開しています。

送信ドメイン認証技術などの導入に関する法的解釈

ISPが迷惑メール対策を実施する際には、電気通信事業法で規定されている、通信の秘密の保護と役務提供における差別的取扱いの禁止に抵触する恐れがないか確認する必要があります。技術WGでは、各迷惑メール対策技術が法的にどう解釈されているのかを整理し、その結果を総務省のウェブサイトで公開しています[*10]。

迷惑メール対策推進協議会は、こうしたドキュメントの発行や国際会議への貢献などにより、平成三〇年度の情報化促進貢献（企業等部門）で総務大臣賞を受賞しました。

JPAAWGの発足

こうした国内における活動は、M³AAWGやLAP（UCENet）といったグローバルな場で日本の状況を説明する際に有益で、M³AAWGのメンバーらが中心となってIETFなどで規格化してきた技術標準を日本で普及させるうえでも効果的に機能してきました。本来なら、日本からM³AAWG会合への参加者がもっと増えて直接議論できれば……と思ってきましたが、北米・欧州で開催されるM³AAWG会合への参加は、それほど簡単ではないとの声もあります。

今年で一五年目となるM³AAWGは、最近、より多くの地域との連携を掲げ、各地域におけるM³AAWG的な活動を支援しています。二〇一七年には、中南米カリブ地域でLAC-AAWGが立ち上がり、今はアフリカ地域でAFR-AAWGへの働きかけに力を入れています。

そうしたなか、二〇一六年頃からM³AAWG運営側と日本からの参加者のあいだで、日本との連携について定期的に検討を行なうようになりました。こうした話し合いを通して、JPAAWGという組織のイメージが参加者のなかで形成されていきました。その結果、二〇一八年三月にM³AAWGの活動を日本の関係者に紹介するイベントが東京で開催され、同年一一月にインターネット協会の第一八回迷惑メール対策カンファレンスと併催するかたちで、JPAAWG General Meeting（以下、JPAAWG会合）が開催されました。

このときのJPAAWG会合は、当初から以前の迷惑メール対策カンファレンスの規模を大きく上回る、三〇〇名程度の参加者を見込んでいたのですが、当日は予想をはるかに超える五〇〇名以上の参加者があり、私たちが考えている課題に対する関心の高さや、こうした組織の必要性を再認識できた好機となりました。

現在、JPAAWGが継続性を持った正式な組織として活動していけるように、種々の整備を進めている段階です。今後もJPAAWGは、関連組織と連携しながら、インターネットおよびメッセージング業界がより健全に機能するよう活動していく考えです。皆さまも、JPAAWGの活動に関心を持っていただければ幸いです。

*1 Outbound Port 25 Blocking
自ネットワークから外部ネットワークへのTCP25番ポートの通信を遮断することにより、スパムメールやウィルスメールの送信を抑制しようとする技術。
*2 DMARCについては、11ページ参照。
*3 https://dmarc.org/
*4 迷惑メール対策委員会 ライブラリ
https://www.iajapan.org/anti_spam/library.html
*5 https://meetings.jpaawg.org/
*6 有害情報対策ポータルサイト 迷惑メール対策編
http://salt.iajapan.org/wpmu/anti_spam/
*7 迷惑メール白書
https://www.dekyo.or.jp/soudan/aspc/wp.html
*8 送信ドメイン認証技術導入マニュアル
https://www.dekyo.or.jp/soudan/aspc/report.html#dam
*9 迷惑メールの踏み台送信対策の状況
https://www.dekyo.or.jp/soudan/aspc/report.html#dai
*10 送信ドメイン認証技術などの導入に関する法的解釈
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail/legal.html

北崎 恵凡（きたざき あやちか）
ISPと携帯事業でメッセージングサービス、システムの設計・開発・運用に19年以上にわたり携わる。迷惑メール対策推進協議会構成員、日本データ通信協会客員研究員、Email Security Conference プログラム委員などを務める。

加瀬 正樹（かせ まさき）
2000年４月、株式会社ニフティ入社。おもに会員向けメールサービスならびに企業向けメールサービスの開発・運用に従事。17年５月、電子メールセキュリティベンダである株式会社 TwoFive に入社。

インタビュー

大規模メールシステムの構築

IIJでは、メールに関する多くのサービスを提供すると同時に、
事業者向けのメールシステムを数多く構築してきた。
ここではIIJが手がけた大規模メールシステムの
構築事例を紹介する。

株式会社コミュニティネットワークセンター（CNCI）技術本部
サーバグループ長
ニコライ・ボヤジエフ 氏

数年単位で行なわれるメールシステムのリプレース

――最初に御社の業務概要を教えていただけますか。

ボヤジエフ　コミュニティネットワークセンター（以下、CNCI）は統括運営会社（MSO）として、東海地区でケーブルテレビ局の事業者を対象とした放送や通信サービスを手がけています。国内第二位のMSOとして、数十万ユーザ向けにインターネット接続サービスを提供しています。

私は技術本部のサーバグループに所属しており、各種サーバシステムの企画・設計・構築・運用に携わっています。

――構築・運用の両方をご担当されているのですね。

ボヤジエフ　広く深くやっています（笑）。ですから、システムを選定する際、自分たちがそのシステムを熟知していることが大事になります。というのは、障害が発生したとき、自分たちでトラブルシュートできるようにするためです。ベンダに依存していると、復旧までに時間がかかってしまいますからね。

――御社では、メールサービスをずっと提供されてきたのですか？

ボヤジエフ　そうです。メールシステムは数年おきに世代更新（リプレース）していて、IIJさんに構築してもらったのは、CNCIの第二世代のシステムです。それ以前は、二〇一〇年に構築したシステムを長く運営してきましたが、モバイルデバイスへの対応や大容量メールボックスの導入など、時代にマッチしたものにするためにリプレースすることになりました。

――第一世代のシステムは、御社で構築されたものですか？

ボヤジエフ　いいえ。メールシステムの構築は非常にむずかしいので、（IIJとは別の）ベンダに作ってもらいました。

――リプレースの狙いは、どういったものでしたか？

ボヤジエフ　第一に、ユーザにとって利便性の高いシステムにしようと考えました。もともとメールサービスとしてはPOPのみを提供していたのですが、リプレースを機に10Gバイトの大容量メールボックス（旧システムのメールボックスは100M）と、IMAP対応を始めました。

運用サイドから言いますと、第一世代のシステムは、障害対応や不正アクセス対応などでいろいろ苦労していたので、そういった点を改善したいという狙いがありました。

選定の決め手は「チャレンジ精神」

――メールシステムの移行は、どのようなスケジュールで進めたのですか？

ボヤジエフ　企画フェーズは、二〇一六年からスタートしました。その後、ベンダ選定に一ヵ月ほどかけて、二〇一六年六月から要件定義、そして構築を開始し、二〇一七年三月に新しいメールシステムが完成しました。ただ、三月の時点では1テナントのみの切り替えで、その後、約半年をかけて移行を完了させました。

――ベンダ選定では、どのような点を重視されましたか？

ボヤジエフ　リプレースの要件を取りまとめて、何社かに相談に行き、最終的にIIJさんにお願いすることにしたのですが、その決め手になったのは、IIJさんが「二つの顔」を持っているということでした。

まず、メールシステムの運用を実際に行なっているメールサービスプロバイダの顔を持っていること。次に、事業者向けに大規模メールシステムを構築するSIerの顔を持っていることです。そうした二つの顔を持っているベンダは珍しく、豊富な知見と情報に対する期待がありました。

もう一つの決め手と言いますか、印象的だったのが、IIJさんは、技術を恐れないSIerだと感じた点です。SIerのなかには、自分たちが慣れていない技術には挑戦したがらないところもありますが、IIJさんはそういったことが全くなかった。しかも「ストレージはどれがいいですか？」とか「ソフトウェアは何にしますか？」といったふうに、細かいコンポーネントの選択にまで、我々の意向を取り入れてくれました。そういう発言ができるのは、「何でもできますよ」という自信とそれを裏付ける技術力、そしてチャレンジ精神があるからだと思います。

綿密なドキュメントに驚き

――プロジェクトの過程で印象に残った出来事などはありましたか？

ボヤジエフ　とにかく会議が多かった（笑）。もちろん、その会議がとても重要なのですが。

IIJさんの特徴は、ドキュメントが詳細かつしっかりしているところです。要件定義、基本設計、詳細設計と、各フェーズのドキュメントの数も非常に多い。個人的には、ここまで作る必要があるのか？　と思うくらい細かい内容でした。そして会議において、ドキュメントをもとにレビューを繰り返しながら、曖昧なところをなくしていき、品質を上げるという取り組みがなされました。結果的には、そうすることで曖昧な点が払拭され、プロジェクトの成功につながったと思います。

要件定義のフェーズがスタートすると、打ち合わせの時間が足りなくなってきたので、「（IIJのオフィスがある）飯田橋まで来てくれませんか？　そのほうが集中的に作業できますから」と言われて、二日ほど朝から晩まで缶詰状態で打ち合わせを行なって詳細を詰めました。

切り替えフェーズでは、リハーサルを行ないました。以前ならリハーサルは一回だけでしたが、大規模メールシステムの切り替えを何度も実施してきたIIJさんから「二回は必須で、この案件は、できれば三回やったほうがいい」というアドバイスがあったので、三回行ないました。実際、三回目で数多くの問題をつぶしたおかげで、本番作業が非常にスムーズにいきました。

とは言うものの、本番の切り替え作業は、午後三時から始めて、翌朝九時にリリースという〝マラソン状態〟のハードワークになりました。このときはIIJさんの営業の方が差し入れてくれたインスタントラーメンを食べながらがんばりました（笑）。

――最後は体力勝負だったのですね（笑）。

業界全体でベスト・プラクティスを目指す

――リプレースから二年が経過して、運用状況などはいかがですか？

ボヤジエフ　この二年間、大きなトラブルはいっさいありません。過去の経験に照らし合わせても、大規模なシステムを切り替えたときは、必ず何か起こるものですが、今回は（ごく小さなトラブルを除いて）本当に何もないので、驚いています。IIJさんが蓄積してきた経験や対策が十分に活かされているのだと思います。

また、メールシステムでは、不正アクセスや迷惑メールなどに対して、普段から小さな対策を継続的に施していくのですが、新しいシステムには、本番環境と全く同じ構成の維持環境があるので、設定を変更したり確認したりするときも、維持環境のほうでテストすることができ、とても便利で助かっています。

――今後に向けた課題などはありますか？

ボヤジエフ　これはCNCIに限ったことではないと思いますが、メールのソフトウェアはどんどん進化・更新されるので、バージョンアップを行なう必要があります。しかしその際、何の問題もなく機能しているシステムを、小さなバージョンアップのたびにテスト・調整し直さなければならない。こうした点は改善の余地があるかもしれませんね。あとは、フィッシング対策などの強化は不可欠だと感じています。

――既存の対策では止められない手口を遮断するための対策は、進めなければなりませんね。

ボヤジエフ　最近、私自身、一般財団法人インターネット協会（迷惑メール対策カンファレンス）やJPAAWGなどで、メールシステムをリプレースした際に取り入れたDMARCなどの新しい技術について、導入事例を発表させてもらいました。そうした活動を通して、最新の問題に関する情報を共有しながら、業界全体でベスト・プラクティスを追求していけるといいですね。

――おっしゃる通りですね。本日は、お忙しいなか、貴重なお話をありがとうございました。

ニコライ・ボヤジエフ
Nickolay Boyadjiev
ブルガリア生まれ。2002年に来日。05年に担当就任後、4世代のISPメールシステムの構築・運用に携わる。16年より、迷惑メール対策カンファレンス登壇を経て、JPAAWG立ち上げに関わる。

業務アプリケーションに進化する

ビジネスチャットツール

「チャット」と聞くと、パソコン通信など楽しげな昔話を想起する方が多いかもしれないが、
本稿では、日々進化している“ビジネスチャットツール”の動向を紹介する。

IIJプロダクト本部
副本部長
金子 健

チャットツールの現状

みなさんは、ビジネスチャットツールを使っていますか？　スタートアップ企業やベンチャー企業では「Slackを使っているよ！」でしょうし、大手企業ではOffice 365と合わせて、Teamsの導入が進んでいるのではないでしょうか。

新しいツールを導入するには新たな費用がかかるので、大手企業では小規模な試験導入で効果を検証し、セキュリティ面の対応を考えて、全社導入計画を作成して、決裁にかけることになります。さすがに今では「チャット？　無料のやつ？　メールじゃだめなの？」と「チャット？　無料のやつ？」といった話はほぼなくなりました。「電子メール？　電話とFAXで十分でしょ？」という時代を乗り越えてきた我々からすると、そんなやり取りに懐かしささえ覚えます。

二〇一九年四月現在、チャットツールはざっと数えただけでも三〇くらいあり、利用者はこれらのなかから、導入事例を見たり、スペックを比べたりして、複数のツールを選抜・試用し、どれを導入するのか決めることになります。

一方、ツールのほうは、価格勝負、販促勝負、無手の営業勝負で、このままでは〝レッドオーシャン〟待ったなし！　という状態から、機能勝負、業界・業務特化で勝負という新しいフェーズに挑むツールも現れ、業務や目的に応じて使い分けるという考え方も必要になっています。

例えばIIJでは、IRC、Teams、direct、Slackの四つのツールを適材適所で使い分けています。IRCはおもにシステム運用のためのコミュニケーション、Teamsは社内のコミュニケーションと遠隔会議や社内セミナー、directは社外メンバーを含むプロジェクトのコミュニケーションやチャットボットの企画開発、Slackは一部の技術系部門で試験的に利用されています。

ビジネスチャットツール〝direct〟

directは、ビジネスチャットツールの黎明期である二〇一三年に始まったサービスで、その当時から新しいフェーズに挑み、ユーザを拡大しているチャットツールです。IIJはdirectを開発・運営する株式会社Lis B（エルイズビー）と二〇一五年に資本業務提携しています。

directは「現場のチカラを最大化するビジネスチャット」として、大林組、竹中工務店、西日本旅客鉄道、ANAエアポートサービス、テレビ朝日、ロイヤルホテルなど、土木・建設、電設、運輸、流通小売、不動産といった、さまざまな現場を持つ企業に採用されています。

Lis Bはdirectの技術をベースに、「○○をなんとかしたい」といったユーザの要望に応えるソリューションも開発しています。例えば、チャットでコールセンターのオペレーターとつなぐ「お忘れ物チャットサービス」は西日本旅客鉄道が採用しており、時間外労働内容・時間をリアルタイムに可視化する「スマートワーキングソリューション」は竹中工務店他が採用しています。また、建設現場に設置された大型モニターにdirectから安全・衛生管理などに関するコンテンツを配信できるdirectサイネージも導入に向けた試験が始まっています（directおよびdirect関連ソリューションについては、Lis Bのサイト*をご参照ください）。

チャットボットとAIの組み合わせ

準リアルタイムで、スマートデバイス・ネイティブなチャットによるコミュニケーションとUIの相性の良さは、説明するまでもないでしょう。そして二〇一八年あたりから、AIとチャットボットを組み合わせたユーザ窓口系サービスを、スタートアップや大手IT企業が続々とリリースしているのはご存じの通りです。

しかし、今年の四月初旬に開催されたAI・人工知能関連の展示会に行ってみたところ、予想以上に出展者の打ち出している適用分野の方向性が似ており、「百花繚乱」と言えるようなソリューションが出揃うまでには、もう少し時間がかかりそうです。

Lis Bは、この展示会で「AI-FAQボット」というサービスを展示していましたが、この「FAQ」こそ、展示各社の多くが打ち出していた適用分野です。ここでもLis Bは、独自のアプローチをしており、AIを質問と回答に関連する語句の自動学習だけに利用するという割り切りの良さで、現実的かつシンプルで扱いやすいサービスに仕立てていました。

業務システムとの組み合わせ

チャットボットはAIだけでなく、業務システムと組み合わせることで、さまざまな〝コト〟をチャットツール上で実現できるようになります。ここではIIJがPoC（Proof of Concept）として開発したチャットボットをいくつかご紹介します。

ワット君	スマートメーターBルート活用サービスと連携し、日次の電力使用量をプッシュ通知、リアルタイムの電力グラフを取得。
パー子さん	スケジューラ、内線検索と連携。
厠（かわや）君	社内開発した男性トイレ個室モニタリングシステムと連携し、空き状況をリアルタイムで応答。
視（みる）君	ラズベリーパイ+カメラで、指定時刻の映像を取得。
測（はかる）君	ラズベリーパイ+環境センサで、温湿度・照度を取得。

IoT関連のチャットボットが多いのは、実働している業務システムと連携させるよりも、社内手続き的・技術的に簡単だったためです。いずれも技術者一人が、短ければ一日かからず、長くても数日で開発したもので、開発にはLis Bがdirectユーザに無料で公開しているdaab SDKを利用しています。機能やサービスをチャットボットにすると、専用のスマホアプリを開発・運用する必要がありません。開発コストも圧縮できますし、iOSやAndroidのバージョンアップに合わせたアプリの検証・改修がほぼ不要となり、メンテナンスコストも圧縮できます。

ビジネスチャットツールのポテンシャル

チャットボットにより、さまざまな機能やサービスを普段使いの一つのチャットツール上で提供・利用して、これまでコスト的にIT化できなかった細々したたくさんの業務をチャットボットでIT化できるようになり、現場からIT化の企画が出てくるようになる――こうした業務効率化のポテンシャルは極めて大きいと考えられます。もちろん、全ての業務がチャットUIに適しているというわけではありませんが。

directをはじめとする新世代型のビジネスチャットツールは、もはや単なるコミュニケーションツールではありません。現場のさまざまな業務をIT化するためのプラットフォームとして活用され始めており、その事例も続々と増えています。みなさんがお使いのチャットツールは、プラットフォームに進化できるでしょうか？

＊ https://l-is-b.com/ja/service/

人と空気とインターネット

新たなブルーオーシャンを目指して

IIJイノベーションインスティテュート
取締役
浅羽 登志也

米の有機栽培、酒造りに続いて、
米俵作りを行なった筆者が、
機械化・自動化の及ばない、
〝手作業〟の存在意義について考える。

今年も米作りが始まりました。例年通り「お布団農法」での米作りですが、気がつけば今年ではや四年目となりました。令和が始まった直後の五月の連休明けに、種籾を植え込んだ「お布団」を田んぼに敷きつめる作業を完了しました。一ヵ月半ほど経った今では、種籾が無事に発芽して、稲の若芽がすくすくと育ち始めています。

この農法の最大の弱点は、お布団を田んぼに敷くところから稲刈りの直前までの作業が全く機械化できていないことです。お布団を敷くには、水を張った田んぼに入り、中腰でお布団のロールを両手で支えて、転がすように少しずつ敷いていきます。この中腰作業は、かなり足腰への負担を強いられます。作業が終わって一週間くらいは、足から腰・脇腹あたりまで筋肉痛が続くほどです。

機械化できないということは、次の二つを意味します。一つは、スケーラビリティがないこと。つまり、全てを人間が作業するので、耕作規模が作業可能な人の数で決まります。すると、いくら米の有機栽培ができると言っても、米を売って生計を立てているプロの農家はなかなか手を出しにくいわけで、実際、この農法は全く流行っていません。流行らないと、お布団にかかるコストも下がりません。

もう一つは――われわれ人間にとっては朗報ですが、機械化できないと、将来、AIやロボットに仕事を奪われる心配がないことです。人型ロボットが、私の代わりに田んぼに中腰になってロールを敷く作業まで難なくこなせるようになったら、話は別ですが（それはそれで、未来感溢れる相当にシュールな光景ではあります）、高価で優秀なロボットをそんな作業に使ってはもったいないし、コスト面から考えても、人間がこの仕事を奪われることはないと考えていいでしょう。とは言え、この仕事をずっと続けたいかと言われるといささか微妙ではありますが、まぁ、足腰が立つうちは続けられるといいな、と思っています。

「米俵作り」に挑戦

少し別の話になりますが、実は今年の二月、念願だった「米俵」の作り方を教えてもらいました。今や米俵を作れる人は全国にもあまり残っていないそうで、私が手伝っている田んぼのオーナーも、注連縄は作れるけど、米俵は作ったことがないとのこと。でも、せっかく米作りをしているので、米俵の作り方もぜひ知りたいと思い、昨年末、どこかに米俵の作り方を教えてくれる人はいないものかとネットで検索してみました。すると、長野県のとある自治体のふるさと納税の返礼品に「米俵作り」があるではないですか！　さっそくその自治体に納税し、二月には俵作りの実習を受けることになりました。

行ってみて驚いたのは、先生が思ったよりずいぶん若く、四〇代半ばだったことと、米俵作りをビジネスとして行なっていることです。先生はもともと違う職業に就いていたのですが、その土地に根付いていた稲作文化を復興するために、七年ほど前に藁細工職人に転身したのだそうです。さらには、俵作りを活性化するために、小さめの米俵を担いで走る「米俵マラソン」という大会を企画から運営まで手がけ、今では一〇〇〇人もの参加者が集まるイベントに成長させたというから驚きです。

この自治体は古くからの米どころ。しかし近年、農業人口が減少して耕作放棄地が増大するという、どこの地方にもある問題を抱えています。先生の発案した米俵マラソンを通して、地域を訪れる人が増えると同時に、自分自身のビジネスもしっかり伸ばしている、まさに地域の特性を生かしたイノベーションを牽引している人物というわけです。

藁細工や米俵は、贈答品やお祝い事に用いられることが多いので、綺麗な稲藁が必要になります。そこで先生は米農家と契約し、藁細工用の稲藁を買い取るスキームを構築。農家も米作りとは別に、新たな収入源として藁細工専用の綺麗な藁を作るための稲作りを始めたそうです。つまり、農家も見事に巻き込んで、新しいビジネスを立ち上げることに成功したのです。

今では先生の作る贈答用米俵は、中身の米よりも高い値段で売れるとのこと。他に同じように米俵を作れる人はいないので、小規模ではありますが、競争相手のいない完璧なブルーオーシャンです。もちろん機械化されていないので、AIやロボットなど敵ではありません。米俵マラソン大会の直前は人手不足で大わらわになるそうなので、今年の秋は、私もボランティアで手伝いに行って、俵づくりの腕を磨かせてもらおうかと密かに狙っています。

ちなみに、今や先生は、なんと大相撲の土俵作りも請け負っているそうです。こちらも質の良い俵を作れる人がいないらしく、先生のブルーオーシャンは着実に広がっています。

酒造りの続報

今回は、お米ネタをもう一つ。昨年、自作のお米を持ち込んで、お酒を作ってもらった話を書きましたが、自前ブランドを増やすべく、別の酒蔵にも委託することにしました。二つ目の蔵は、長野県塩尻市にある生産量二〇〇石（一升瓶一〇〇本で一石）の小さな蔵です。基本的には杜氏さんが一人でやっているのですが、この杜氏さんも四〇代半ばのかなりマニアックな方で面白かったです。以前は別の蔵で杜氏をやっていたのですが、この塩尻の蔵が杜氏を探していて、小さい蔵なら自分の好きなように酒造りができると考え、移ってきたそうです。ユニークなのは、自分の手であれこれ試したいからと、機械を使うのをほとんどやめて、昔ながらの手作業に戻してしまったそうです。とは言え、この蔵には長い歴史があり、昔からのファンもいるので、これまでの味の酒も作り続けつつ、こっそり新たな挑戦を進めているのです。

日本酒には主にリンゴ酸、乳酸、コハク酸、クエン酸という四種類の有機酸が含まれているのですが、この杜氏さんは、造りを少しずつ変えることで、それぞれが際立つ酒を作り分けています（この酒は蔵に行かないと飲めません）。よく造り分けられるものだなと思い、飲み比べてみたところ、どれもちょっと不思議な味でしたが、それぞれの酸の特徴がよくわかり、興味深かったです。これらをブレンドすれば、四つの酸のバランスを自分好みにできるので、どんな不思議な酒が生まれるのか楽しみです。もしかすると、この分野も新たなブルーオーシャンになるかもしれません。

あらゆるものを機械化・自動化することで生活はどんどん便利になっていきます。その一方で、新たなブルーオーシャンを生み出すのは、ユニークな発想と地道な手作業なのかもしれないなんて思う私は、昭和の遺物でしょうか。でも、機械に仕事を奪われずに、いつまでも楽しく仕事をし続けるためには、経済合理性がなく、ロボットもAIも進出してこない分野で、人間にしかできない、独自のスキルを身につけておくことが大事なのかもしれないと思う今日この頃です。

イラスト／末房志野

Technical Now

白井データセンターキャンパス稼働開始

IIJ 基盤エンジニアリング本部データセンター技術部企画課
堤 優介

**デジタルトランスフォーメーションの本格的な普及に向け、
新たなデータセンター需要に対応するシステムモジュール構造の
「白井データセンターキャンパス」が2019年5月、稼動を開始した。**

今日、ICTは社会インフラとなり、SNS、ネットショッピング、オンラインゲームなど、日常生活のなかで膨大なデジタルデータが使われるようになりました。また、企業のIT環境においても、保有からアセットレス化へ向かう流れが加速してクラウド需要はさらに拡大し、今後も5G、IoT、AIの普及により、データ量が増大していくと見込まれています。

こうしたなか、データの保管や処理を安全に行なう場所として、データセンターの重要性がますます高まっています。IIJでもクラウド、ネットワーク、セキュリティといったサービスが拡大し続けており、デジタルデータの爆発的な増大や中長期的なサービス設備の拡張に対応するために、千葉県白井市に「白井データセンターキャンパス」(以下、白井DCC) を建設しました。

白井DCCは、データセンターの基本である堅牢性や信頼性を持ちながら、市場の変化によって大規模化・多様化する需要に柔軟かつ迅速に対応できるデータセンターです。以下では、白井DCCの特徴を紹介します。

大規模・大容量

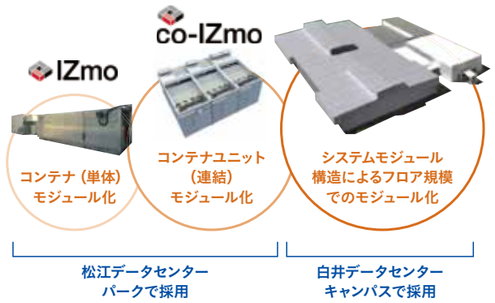
延床最大面積	最大受電容量	設備収容
約80,000㎡	50MW	6,000ラック

※ 実効平均6kVA/ラックで利用した場合

特徴1｜大規模・大容量

敷地面積約4万平方メートル（東京ドームとほぼ同じ大きさ）、延床面積最大約8万平方メートルに、最大50MWの受電容量を備えます。第一期棟は約1000ラック規模ですが、最大で6000ラック規模の設備を収容できます。荷物搬入口には、10トントラックが同時に2台停車可能なスペースがあり、大量のラック・IT機器を搬入できます。さらに、需要や技術動向に応じてスペックを決めて増設していける拡張エリアがあり、キャンパス内（同一敷地内）で、大規模構築およびスケールアップを実現できる環境になっています。

モジュールコンセプトを大規模DCに適用



特徴2｜モジュールコンセプトの採用

IIJのデータセンターは多様なITサービスの基盤として使用されているため、中長期的にはラック需要計画の変更が起こり得ます。こうした際にも、最適な設備投資、スピーディな増設、先端技術の取り込みを可能にするために、構成要素をモジュール化し、設備を容易に増減・更新できるモジュールコンセプトを採用しました。

IIJは2011年、松江データセンターパークを開設し、コンテナ型データセンターでモジュール化を実現しています。ここで培ったノウハウを大規模DCに適用し、白井DCCでは、フロア規模（数百ラック規模）でモジュール化しました。建物の鉄骨や外壁といった部材の形状・配置を標準化したシステム建築方式を採用し、高品質、短工期、低コストでの構築を実現しました。今回完成した第一期棟も、工事着工から8ヵ月という短期間で竣工しました。

特徴3｜省エネの追求

省エネは、電気料金を抑え、運用コストの低減につながります。また、国連で採択された「SDGs」（Sustainable Development Goals＝持続可能な開発目標）における日本政府の「SDGsアクションプラン2019」では、省エネや気候変動対策が、取り組みの優先分野とされています。他方、IT産業の消費電力は、市場の拡大とともに増え続けており、今後はCO_2の排出量削減などがより強く求められると考えられます。

白井DCCでは、松江データセンターパークで高い省エネ性能を実現した「外気冷却空調方式」をはじめ、チラーの出口温度を通常より高くすることで効率を上げる「中温冷水送水システム」、最高効率98パーセントを誇る「高効率UPS」といった省エネ技術を採用し、環境省の「平成30年度次世代省CO_2型データセンター確立・普及促進事業」に採択されています。また、AIによる空調運転の効率化にも取り組んでいます。

空調設備架台
架台上部の「チラー」の出口温度を通常より高く設定することで高効率運転を実現

特徴4｜運用の高度化・効率化

データセンターが大規模化する一方、将来的には労働人口の減少により人材確保が困難になると予測されるため、IIJではデータセンター運用の高度化・効率化は不可避であると考えています。白井DCCでは、ロボット技術を導入し、フィジカルロボットによる来訪者アテンド、屋内外の巡回業務などの無人化（綜合警備保障株式会社と共同実証）、ソフトロボット（RBA/RPA基盤）による入館申請業務、障害発生時の復旧対応などのITオペレーション業務の自動化（株式会社IIJエンジニアリングと共同実証）を進めています。また、スマートデバイス、IoT、モバイル技術などを活用した新たなサービス提供にも取り組んでいます。

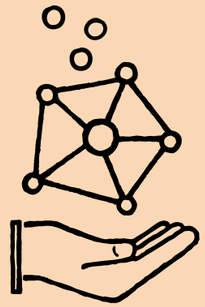
フィジカルロボット（ALSOK製）による来訪者アテンド、屋内外の巡回業務を実証予定

今後の展望

白井DCCは、ファシリティの提供だけでなく、顧客への付加価値を高めるために、各種クラウドサービス、近郊データセンター、IX（インターネット相互接続点）などと接続する「ネットワークHUB構想」のもと、ネットワークを拡充していく予定です。

近年、電力自由化により電力供給元を選べるようになりましたが、電力取引市場の整備、FIT（電力買取制度）の終了、原発再稼働の行方など、電力供給を巡る環境が変化するなか、データセンターに不可欠な電力をどのように調達していくのかという点も、大きな課題になっていくでしょう。新技術が次々と実用化され、目まぐるしく変容していく社会情勢に合わせて、データセンターも柔軟に変わっていく必要があります。白井DCCはそれを実現する“Sustainable”なデータセンターです。進化し続けるこれからの姿を楽しみにしていてください。

Internet Trivia



インターネット・トリビア

プロトコルの安全性

IIJ MVNO事業部
事業統括部 事業統括課 シニアエンジニア
堂前 清隆

インターネット上で通信を行なう際には、それぞれの目的に合わせて、決められた通信手順（プロトコル）を使います。Telnet、SMTP、POP3、HTTPといったプロトコルは、インターネット初期から現在まで広く使われているものです。そのため、これらのプロトコルは、今の常識からすると、ずいぶん〝ゆるい〟設計になっています。

例えば、電子メールの送信・配送に使われるSMTPは、送信の際、送信者の確認がなく、誰でも他人のメールアドレスを「送信者」に設定して送信可能でした。こうした〝ゆるさ〟を突くかたちで送信者を騙ったメールが大量に送られる事態が頻発し、今日の迷惑メール問題へと発展しました。

また、これらのプロトコルは全般的に通信の中身を保護するという考え方に乏しく、インターネット上で通信の内容や、場合によってはパスワードそのものが第三者にも見られかねない構造になっています。

さて、現在ではこのような〝ゆるい〟プロトコルだと、不正利用に対抗することがむずかしくなっているため、安全性強化のための改良が図られています。その主なポイントは、通信の暗号化による盗聴対策、利用者・サーバ双方のなりすましを防止するための認証の強化などです。ただし、プロトコルによってその実現方法はさまざまです。

一つの方法は、プロトコル自体を新規に作り直すことです。ネットワーク経由でコンピュータを操作するためのTelnetプロトコルは、同じ目的を持ったsshというプロトコルで代替されています。sshは、通信自体を暗号化して盗聴対策を行なうとともに、コンピュータや利用者がなりすましていないかを確認するための強固な認証システムを備えています。sshはTelnetと全く異なるプロトコルであり、接続のためのプログラムも全く異なるものが使われています。

別の方法として、既存のプロトコルを生かしたまま、暗号化や接続先の認証機能を強化する方法もあります。例えば、メールの受信に使われるPOP3では、通信中にやり取りされる命令群はそのままにして、その命令をSSL・TLSといった安全な通信を行なうための別のプロトコルで送受信することで暗号化を実現しました。この方式は、新しいプロトコルへの置き換えに比べて、従来使っていたソフトウェアを生かしたまま、小規模な改修で安全性を高めることができます。

ただ、プロトコル自体を置き換えてしまったり、小規模な改修では安全性を向上させることがむずかしい場合もあります。SMTPは利用者からのメールの送信だけでなく、メールサーバ同士の中継にも使われていますが、メールサーバは世界中に存在し、相互に中継を行なっているため、新しいプロトコルに全面的に置き換えることは困難です。そのため、中継用のプロトコルは従来のままとし、メール送信時の通信を分離し、そちらに対して認証機能と暗号化が導入されました。これによってメール送信時の不正にはある程度対抗できるようになりましたが、メールサーバ同士の中継部分は従来のままなので、中継部分に横入するようなかたちの不正には対抗できませんでした。結局、中継部分についてはプロトコルの改善ではなく、一般利用者がサーバに接続できなくなるようなフィルタリングを施すことと、中継されたメールが正当なものかどうかを確認するための別の手法を用意することで、不正対策が図られています。

安全性が十分でない〝ゆるい〟プロトコルは、置き換えや改良が行なわれるべきですが、もともとのプロトコルの設計や利用様態によっては、それが困難なこともあります。そうした制約があっても、互換性を保ちながら安全性を高める試みが続けられています。

イラスト／末房志野（P24,25,26）

Grobal Trends

グローバル・トレンド

ジャカルタのMRT

PT. IIJ Global Solutions Indonesia
VP of Technology
西川 善高

ジャカルタには、自動車、タクシー、さまざまなバス路線、バイク、バイクタクシー、トゥクトゥク（三輪タクシー）など、数多くの交通手段があります。市内では年々、自動車とバイクが増え続けているため、世界ワースト三位内にランクされる酷い渋滞が毎日発生しています。例えば、1キロメートルを自動車で移動するのに一時間以上かかることもよくあります。日本の中古車両を購入し、電車を走らせている地区もありますが、その運行はささやかな規模であり、交通渋滞の緩和には大して貢献していません。

交通渋滞の緩和策として導入されたのが、MRT（Mass Rapid Transit＝大量高速輸送）です。ジャカルタのMRTは二〇一九年三月、インドネシア初の地下鉄として開通しました。第一期はNorth - South Lineと呼ばれる一三駅、全長15・7キロメートルからなる一路線です。渋滞緩和だけでなく、それにともなう経済効果にも、市民の期待が寄せられています。私たちのオフィスはMRTの駅の近くにあります。これまではオフィスから日本人がよく行くエリアまで一時間以上かかりましたが、MRTの開通により、約一五分になりました。MRTを利用した営業活動は生産性の向上につながると、私たちは考えています。

MRT開通プロジェクトで、私たちはAFC（Auto Fare Collection System＝自動料金収受システム）のインフラ構築をおもに担当しました。MRTの各駅にある自動改札機、券売機と、管理センターのメインサーバを接続するネットワークを構築しました。本プロジェクトは、ジャカルタの地図や歴史に残るものです。その一端を担えたことを私たちは誇りに感じており、現地社員は「将来、自分の子供に語れる仕事ができた」と喜んでいます。その一方で苦労もありました。非常に多くの組織・人間が関わるため、突然のスケジュール変更や作業延期が頻発したほか、大雨による機器の水没や粉塵による機器の不具合など、建設現場ならではのトラブルにも見舞われました。

今回開通したMRTは一期目です。二期目の実施は決定済ですが、まだ着工していません。他の路線も含めて計画は進んでいますが、North - South Lineの延伸には時間がかかりそうです。しかしMRTの建設は続いていくでしょうし、ジャカルタが将来、東京にも負けない鉄道網を持つ大都市になることを、私は一市民として願っています。

MRTのホームと自動改札機

株式会社 インターネットイニシアティブ

本社　東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL:03-5205-4466

関西支社　大阪府大阪市中央区北浜 4-7-28 住友ビルディング第二号館 5F
〒541-0041　TEL:06-7638-1400

名古屋支社　愛知県名古屋市中村区名駅南 1-24-30 名古屋三井ビルディング本館 4F
〒450-0003　TEL:052-589-5011

九州支社　福岡県福岡市博多区冷泉町 2-1 博多祇園 M-SQUARE 3F
〒812-0039　TEL:092-263-8080

札幌支店　北海道札幌市中央区北四条西 4-1 伊藤・加藤ビル 5 階
〒060-0004　TEL:011-218-3311

東北支店　宮城県仙台市青葉区花京院 1-1-20 花京院スクエアビル15F
〒980-0013　TEL:022-216-5650

横浜支店　神奈川県横浜市港北区新横浜 2-15-10 YS 新横浜ビル 8F
〒222-0033　TEL:045-470-3461

北信越支店　富山県富山市牛島新町 5-5 タワー 111 10F
〒930-0856　TEL:076-443-2605

中四国支店　広島県広島市中区銀山町 3-1 ひろしまハイビル 21 5F
〒730-0022　TEL:082-543-6581

新潟営業所　新潟県新潟市中央区東大通 1-3-1 帝石ビル 4F
〒950-0087　TEL:025-244-8060

豊田営業所　愛知県豊田市西町 4-25-13 フジカケ鐵鋼ビル 5F
〒471-0025　TEL:0565-36-4985

沖縄営業所　沖縄県那覇市久茂地 1-7-1 琉球リース総合ビル 8F
〒900-0015　TEL:098-941-0033

IIJグループ／連結子会社

株式会社 IIJグローバルソリューションズ
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL:03-6777-5700

株式会社 IIJエンジニアリング
東京都千代田区神田須田町 1-23-1 住友不動産神田ビル2号館 7F
〒101-0041　TEL:03-5205-4000

ネットチャート株式会社
神奈川県横浜市港北区新横浜 2-15-10 YS 新横浜ビル 8F
〒222-0033　TEL:045-476-1411

株式会社 IIJイノベーションインスティテュート
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL:03-5205-6501

株式会社竜巧社ネットウエア
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL:03-5205-6766

IIJ America Inc.
55 East 59th Street, Suite 18C, New York, NY 10022, USA
TEL：+1-212-440-8080

IIJ Europe Limited
1st Floor 80 Cheapside London EC2V 6EE, U.K.
TEL：+44-0-20-7072-2700

株式会社トラストネットワークス
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL:03-5205-6490

発行／株式会社インターネットイニシアティブ 広報部
お問い合わせ／株式会社インターネットイニシアティブ 広報部内「IIJ.news」編集室
〒102-0071 東京都千代田区富士見2-10-2 飯田橋グラン・ブルーム
TEL: 03-5205-6310　E-mail: iijnews-info@iij.ad.jp

編集／村田茉莉、鈴木健二、小河文乃
表紙イラスト／末房志野
デザイン／榊原健祐 (Iroha Design)
印刷／株式会社興陽館 印刷事業部

Information

令和元年度

情報通信月間推進協議会 会長表彰

迷惑メール対策推進協議会の座長代理を務める、IIJネットワークサービス本部アプリケーションサービス部の櫻庭秀次が、「令和元年度 情報通信月間推進協議会会長表彰」で、「情報通信功績賞」を受賞しました。
受賞理由は「迷惑メール対策推進協議会の座長代理および同協議会技術 WGの主査などとして、迷惑メール対策を推進する活動に10年以上にわたり尽力し、多大な貢献をもたらしたこと」です。

詳細
https://www.iij.ad.jp/news/pressrelease/2019/0529.html

情報通信月間とは

情報通信月間は、情報通信の普及・振興を図ることを目的に、電気通信市場が自由化された昭和60年に設けられました。期間は5月15日から6月15日の約1ヵ月間で、全国各地で情報通信に関する行事が実施されます。

表紙の言葉「夏至と夕陽」

季節は梅雨でも、暦のうえでは夏を迎えました。昼の時間が長くなると活動的な気持ちになり、太陽の存在の大きさを実感します。また、今にも沈みそうな太陽を見ていると、過ぎていく時の儚さを感じます。今も昔も変わらない夕陽が作り出す美しさを目の当たりにして、古の人々も同じように感じたのだろうかと思いを馳せると、自然への感謝と敬意の気持ちが溢れてきます。

末房志野

◎IIJ.news表紙のデザインを壁紙としてダウンロードいただけます。ぜひご利用ください。
URL: https://www.iij.ad.jp/news/iijnews/wp/
◎IIJ.newsのバックナンバーをご覧いただけます。URL: https://www.iij.ad.jp/iijnews/

編集後記

昨年の紅白歌合戦、松任谷由実『やさしさに包まれたなら』の、会場全体を巻き込む大合唱はご覧になりましたか？　ユーミンは、自分のメッセージを観客に届けるシンガーを超えた存在になっていました。言うならば、記憶や感情といったインフォメーションを、歌というメッセージツールに乗せて運び、増幅・昇華させて、不特定多数の人々に届ける途轍もないプラットフォームと化していました。あの時間は「平成最後の奇跡」だったと、半年たった今もときどき思い返します。やさしい気持ちで目覚めるためには自助努力が欠かせない大人にも、時にはこのような奇跡が訪れることがあります。もしかしたら静かな木洩れ陽の中に神様は隠れていて、カーテンを開いた人にだけ気まぐれに微笑みかけるのかもしれません。(A)

wizSafe

ライフ・ウィズセーフ

10年にわたる負け戦（いくさ）

IIJ セキュリティ本部長
齋藤 衛

2018年末、マルウェア Conficker が登場して10年をむかえました。しばらく話題になることはなかったので、現在、セキュリティに関わっている人でも、すでにご存じない方もいらっしゃるかもしれません。Confickerは、登場から半年のあいだに5つの亜種が現れ、世界中で Windows PC を500万台以上も感染させたマルウェアで、その大規模な活動から特に企業などの内部ネットワークにおいて大きな影響を与えました*。

IIJの運用するハニーポットでは、2018年12月中に8,597回の感染活動を観測しており、その約1割が国内のIPアドレスからのものでした。感染に利用する脆弱性がおもに10年前のOSを対象としているので、今日における大規模な新規感染はあり得ないとしても、Confickerは10年たっても根絶されなかった歴史に残るマルウェアであると言えます。ここで Conficker はどのようなものであったか振り返ってみたいと思います。

まず、その感染能力の高さが特徴的でした。インターネット上でのおもな感染活動としては、2008年10月に公開された Windows XP の脆弱性 MS08-067を悪用し、ネットワーク経由で直接攻撃を行ないました。また、当時 OS のデフォルト設定で許可されていた、USB メモリからの自動実行の仕組みを悪用したり、マルウェア内部に内包する平易なユーザ名とパスワードの組を用いて組織内の共有サーバを悪用したりすることで、ファイアウォールなどの境界を越えて組織内のネットワークに侵入したり、ネットワーク内で爆発的に感染を広げました。

ひとたび感染したあとも、活動を阻害しにくくするための2つの仕組みが導入されていました。1つは、感染後にアップデートなどの指示を受けるための指令サーバの特定に、プログラムを用いたドメイン生成アルゴリズムが利用されていたことです。このため、指令サーバの動きを停めようとすると、毎日生成される5,000のアルゴリズムの候補のなかから実際に使われる1つを特定して対処するということを、毎日実施しなければなりませんでした。また、いくつかの亜種では、アップデートに P2P の技術が利用され、マルウェアの更新を妨害しにくくしていました。

さらに、このマルウェアは多くの場合、感染活動以外の悪さをしない、ということも特徴として挙げられます。2009年5月に登場した最後の亜種では、Waldac など他のマルウェアをダウンロードして実行する機能が組み込まれましたが、この亜種は大量に感染することはなく、実際の被害は少なくてすみました。

Conficker に対処するために、世界中のセキュリティ関係者が集って対策活動を実施しました。皆が協力することで、大規模感染の抑制や、ドメイン生成アルゴリズムへの対応の定石を確立するといった成果を得ましたが、約2年半の活動ののち、対策を終えています。しかしながら、このマルウェアはその後も活発な活動を続け、IIJセキュリティ関係のレポートにおいても長きにわたり、数の多い Conficker を観測情報から除いて報告しなければならないほどでした。

以上のように、感染能力が高いだけでなく、対応のコストを高くすることで、Conficker は根絶をむずかしくし、長期にわたって存在した事例となりました。時は流れ、状況は変わり、今、このマルウェアそのものは大きな脅威でなくなったと言えます。クライアント PC に対して、ネットワークから攻撃しやすい脆弱性はほぼ根絶されるか、ファイアウォールの利用などで攻撃されにくくなっています。また、対策をむずかしくするための仕組みは、現在のPC用のマルウェアにも利用されていますが、いくつかの対策技術も醸成されました。一方で、利用者が安易なユーザ名とパスワードを選ぶという点と、直接的に深刻な影響のない事案の対策は見過ごされがちという点について、今日の IoT ボットなどにも悪用され続けています。これらは、このマルウェアが残した課題なのです。

＊マルウェア Conficker の世界的流行
https://www.iij.ad.jp/dev/report/iir/pdf/iir_vol04.pdf


IIJ
Internet Initiative Japan