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.

October 2016
VOL. 136

特集

企業の資産を守る情報セキュリティ

IIJ. news
October 2016
VOL. 136

表紙の言葉「コスモス」

コスモスは、もともとメキシコに咲いていた花で、19世紀にある芸術家が日本に持ち込んだという説があるそうです。人が移動することで新しいものやことが伝わるって、なんだか素敵だなあと思います。SNSなどで海外にいる友人ともコンタクトがとりやすくなりましたが、実際に会うことができれば、より感激します。今度会うときは、ずっと大切にしてもらえるプレゼントを持っていきたいと思います。

末房志野

野蛮なままで

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

秋の長雨とはいっても、秋の気配がたってから、今年は青空を見る機会がないほど、雨雲に覆われた日が続く。偶に晴れた日があると、十月なのに、三〇度を超す暑さ。次々と台風に襲われる。「異常気象」という言葉も、今さらの感がして、季節の移ろいを消してしまう気候にも驚かなくなり、海水温度が上昇してサンマやイカの不漁が続くといったニュースにも反応しなくなってしまった。

空調の効いたオフィスビルで働いていると、季節感が失われていく。暮らしそのものから四季の移り変わりの行事もほとんど消えてしまった。人間が生きていることが生きてきた記憶にあるとするなら、日本人は季節との関わりのなかで記憶を積み重ねてきたのだが、四季の移ろいが変わってしまうと、記憶と季節の関わりが希薄になってくる。過ぎ去った時の経過は、季節が移り変わる体感によって鮮烈な記憶となる。私にとって小学校に入学した時の記憶は、入学式ではなく、校庭の土に落ちた桜の花びらの光景である。

十月の初め、来年入社予定の社員の内定式があった。男子は地味なスーツに白いワイシャツ、ストライプのネクタイ、女性は黒のスーツ。内定式は公式の会ということで、礼儀を重んじて、同じような服装になったようだ。二〇年以上も前になるが、初めて新卒を採用した頃は、内定式もなく、入社式だけがあって、新入社員に「なんでも質問していいよ」と言い、私が長々と答えていた。一応は入社式なのだから、少しはマトモな格好をしてきたらと、そんな時代だった。IIJという会社は、そういうカルチャーだと思っていた若者が、自分のやりたいことが好きにできる場として、研究室の延長といった気分で入社してきたのである。当時のIIJは、マトモに給料が払えるようになったばかりの時代で、オフィスにネクタイを締めて来るような社員はいなかった。そんな企業に礼を弁えた人間が入社することもなかったのかも知れない。ところで、そもそも当時は入社式そのものがなかった気もする。記憶というのもいい加減なものだ。

会社もそれなりの規模になって、毎年、百人以上の新卒が入社してくれるようになると、礼を知る若者が集まるのも当然で、創業当初の若者と違ってくるのは当たり前である。同じような服装だから没個性と感じるほうがおかしいのである。余計なこだわりを持たず、最低限、時と場を弁える程度の常識をもった若者が、将来を担う時代なのである。懇親会のパーティで話をすると、素直で元気のいい内定者ばかりで、ほっとする。

企業における日本のIT化の進展は、欧米と比較すると、極めて慎重である。クラウド、IoT、ビッグデータ、AI……等々、将来のITの方向を決める言葉はすぐに流布するのだが、これらの言葉が変えようとする本質については、できる限り考えようとしていないというか、後退りしながら対処する、というのが一般的な対処法である。企業経営の基盤からその仕組みを変えようとすることこうした流れに対しては、仕組みごと変える時に生じるさまざまな〈痛み〉に正面から取り組まないと難しいのだが、〈痛み〉についてはできる限り避けながら、といった体質が企業に染みついてしまっているようだ。

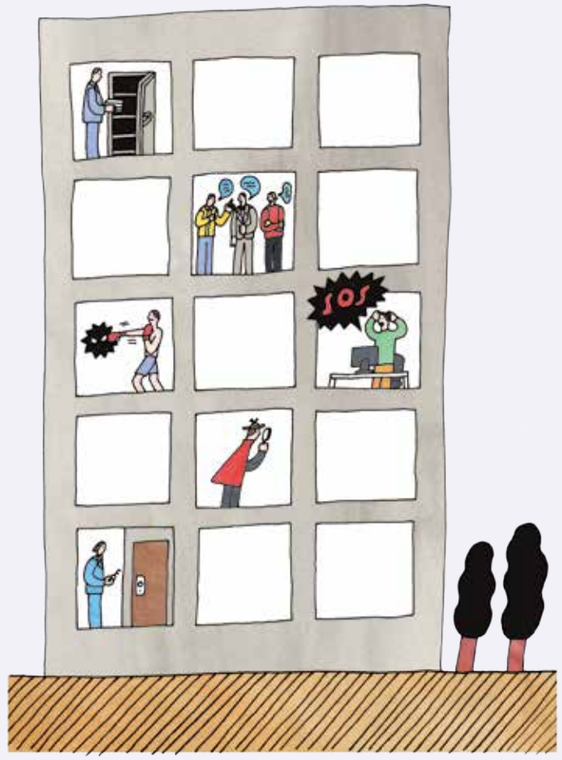
ゼロからスタートして二五年、礼を弁えない若者が集まって成長してきたIIJは、いまだ多くの日本企業が投資に慎重になっているのとは別に、ひたすら将来に向かっての開発投資だけが、IIJの成長を約束するのだという野蛮な精神を持ち続けている。素直で明るい内定者にも、そんなIIJのカルチャーを引き継いでほしいと思うのだが。●

イラスト／末房志野

Topics

企業の資産を守る情報セキュリティ

サイバー攻撃が企業に脅威を与え続けるなか、
本特集では、さまざまな手口から
自社の情報資産を守るための基本事項を紹介する。
セキュリティは「イタチごっこ」と自嘲気味に語られ、
ユーザは攻撃者の後手にまわりがちだが、
やはり最善の対処法は、最新の知識と対策を知ること以外にないと言える。



特集イラスト／STOMACHACHE.

ICT社会のサイバーセキュリティ

本格的な ICT 社会の到来を目前にし、
サイバー攻撃の脅威は、企業活動や社会生活に深刻な影響を及ぼしている。
ここでは、そうした脅威の現状と対策の最前線について聞いてみた。

IIJ セキュリティ本部長
齋藤 衛

サイバーセキュリティの現在

――今回の特集は「企業の情報資産をどのように守るのか?」というテーマです。基本事項として、攻撃者はどんな目的を持ってサイバー攻撃を行なうのでしょうか?

齋藤　攻撃者の目的自体は、あまり変わっていません。もっとも多いのは、直接的に金銭を狙うものです。もちろん、間接的に金銭につながる、企業の知財なども攻撃の対象になりやすいです。

――流行しているサイバー攻撃や、新しく発生した攻撃などはありますか? また、狙われやすい業種・業態などはありますか?

齋藤　最近では、法人・個人双方に対し、データを勝手に暗号化して「復号してほしければ、身代金を出せ」というランサムウェアが流行しました。

　狙われやすさという点では、ICTを使って活動している企業ならどこでも、攻撃の対象になる可能性があります。

――特に注意が必要な情報資産は何ですか?

齋藤　一概には言えません。この十数年来、多くの企業では、自分たちが所持する情報資産を洗い出して、それをきちんと管理するといったことを徹底してきました。ただ、情報の価値は常に変動しています。

　例えば、一昨年末から約一年間、大企業の健康保険組合が相次いで標的型攻撃に狙われるというキャンペーンが発生しました。これは、一企業の情報資産が個別に狙われたわけではなく、日本国内の大企業の社員の「健康」情報に絞った攻撃が試みられ、攻撃者は日本人の健康に関するビッグデータを集めようとしていたことがうかがえます。このような攻撃が起こると、一企業の問題にとどまらず、社会全体に波及するリスクを考えながら対策にあたらなければなりません。そして、そうした大きな動きのなかで自社の情報資産がどれくらいの価値を持っていて、どのくらい狙われる可能性があるのかといったことを常に検討し続ける必要があると思います。

――広くアンテナを張っておくということでしょうか?

齋藤　そうですね。その役割を、企業が個別に担うのか、業界全体か、セキュリティ団体か、もしくは我々のようなセキュリティベンダなのか――そのあたりの社会的なルールは、今後、整備していく必要があります。

――企業の情報資産を守るために、まずは何をすべきですか? 資産の種類・内容によって対策も異なるのでしょうか?

齋藤　貴重品を金庫に入れるように、重要な情報資産も厳重に管理しなければなりません。

　昨今では、そうした金庫にアクセスするためのパソコンなどが狙われることが

齋藤　そうですね。ＩＣＴを使うビジネススタイルは二〇年ほど前から本格化し、徐々に浸透してきました。かつて「人は腕に抱えられる書類のぶんだけしか仕事ができない」と言われたりしましたが、ＩＣＴを使うことで、従業員一人ひとりのパフォーマンスは飛躍的に向上しました。つまり、ＩＣＴに投資することで、プラスの利益を得たわけです。ですから、私個人の見解としては、ＩＣＴで得た利益に相応しい投資をセキュリティにもするべきだと考えています。それは裏を返せば、ＩＣＴがもたらす恩恵が増えたぶんだけ、リスクも増えているということなのです。

　セキュリティは、懸念されるリスクを取り除くためのものであって、通常は利益を生んだりしません。もちろん、セキュリティに十分なコストをかけなかったために、結果的に（サイバー攻撃を受けて）利益が減ったということはあり得るので、経営上の投資と考えられるのかもしれません。ただ、繰り返しになりますが、ＩＣＴ活用が生み出した利益とＩＣＴ環境を守るためのセキュリティコストはセットで考えるのが望ましく、双方のバランスが大事だということです。

　経営に携わっている人は「投資と利益」という観点から物事を考えますので、「セキュリティ＝コスト」と整理してしまうと、無駄なお金と判断されてしまいがちです。このような事情もあって、先のＮＩＳＣの「投資」という言葉を使った指針が出てきたのではないでしょうか。

　――仮に「セキュリティコストは必要経費」という認識を持っていない上層部がいたとしたら、情報システム部門はどのように折衝すればいいでしょうか？

齋藤　むずかしい面もあると思います。想定されるリスクを挙げていき、底が見えない危険性だけを強調しても経営者は引いてしまうので、できるだけ「経営用語」で説明し、経営者が納得できる言葉に翻訳したほうがいいでしょう。

　――現場の知見と経営者の視点は違うということですか？

齋藤　乱暴な喩えですが、セキュリティを守る役務は、人間の体で言うと「白血球」のような働きをしています。外からバイ菌が入ってくると、それを捕らえようとする。でも、人体の経営層である頭脳が理解する病気とは、患部に痛みを感じたり、高熱が出たりすることですよね。この症状を認識して、頭脳が「今日はおとなしく寝ていよう」とか「医者に行こう」と判断するわけです。つまり、セキュリティ対策の活動も技術的な表現だけではなく、こうした症状と同じように、経営者がわかるような、さらに言えば、組織の行動に決断を促すような「サイン」に変換していく必要があるのかもしれません。

　――社内的なコミュニケーションの問題もありますか？

齋藤　先ほど話したように、経営者に響く言葉は何か？　ということ――一例としては、リスクを具体的な金額に置き換えるなど――を考えないといけないでしょう。

　最近は、ＣＳＩＲＴに役員が入ったりして、そうした橋渡しのミッションを担えるようにしている企業もあるようです。

ＩｏＴ社会におけるセキュリティ

　――ＩｏＴ社会では、企業および情報システム部門は、セキュリティに対してどのような考えを持つべきでしょうか？

齋藤　ＩｏＴ社会では、ありとあらゆるモノがネットワークに接続され、その情報が常時やり取りされます。

　最新の「エコビル」では、電力・空調などの使用状況、人の在／不在や入退室などの人流データが、ビル管理会社に送られて活用されています。万が一、こうしたデータが漏えいしたら、どんなことが起こり得るか？　ひょっとすると、他のデータと紐づくことで、入居している企業に関する言外の情報が読み取られてしまうのではないか？　といったことも考えておかなければなりません。また、それが個人宅になると、プライバシーの問題になるでしょう。

　他方、公園や駅といった公共の場にある装置に関する危惧もあります。例えば、自動販売機のなかにはオンライン化しているものもあり、有事の際に災害情報が掲示されたりします。しかし、こうした自販機が侵入された場合、パニックを誘発するような偽のメッセージが掲示されたりするといったこともないとは限りません。日本の自然災害に不慣れな外国の方が増えるオリンピックのときなどは、この種の攻撃に警戒すべきでしょう。

　――個人は、もっと自身の情報管理に注意を払ったほうがいい？

齋藤　実際には「このサービス・機能を提供するために、あなたの情報も集めています」といったことは、何らかのかたちで告知されているはずですので、それに留意・合意しているのか、といったことに気をつける必要があります。

　――安心・安全なＩｏＴ社会に向けて、通信事業者には、どのような取り組み・役割が求められるでしょうか？

齋藤　プラットフォームなどＩｏＴ環境を管理・運用している事業者が自発的にレギュレーションをつくって品質向上を心がけたり、業界団体とも協調してガイドラインを整備しながら、「国内品質」を築いていくことだと思います。

ＩＩＪが目指す情報セキュリティ

　――ＩＩＪは今年四月、セキュリティ本部を立ち上げました。立ち上げの背景や今後の活動予定を教えてください。

齋藤　これまでＩＩＪでは、セキュリティを提供する機能は、基本的に事業毎に分散していました。それらを統合して、よりスピーディなセキュリティの機能提供につなげていきたいという狙いがありました。それに加えて、データアナリストにも参加してもらって、セキュリティに関連する大規模なデータ分析も行なっていく予定です。

　ひとつ補足しておきますと、「セキュリティ」というのは、本来、各サービスに組み込まれていて、そのサービスの健全な品質を維持するためのものです。そういう主旨にもとづき、セキュリティ本部では、企業の皆さまがセキュリティシステムを構築・運用していく際のサポートを行なっていきたいと考えています。それと同時に、ＩＩＪが提供するクラウド、モバイル、ＩｏＴ事業など、すべてのサービスに適宜、セキュリティ機能を提供し、サービス全体の品質向上に寄与したいとも考えています。

　こうしたことを実現するには、膨大かつ最新の知識、正確なネットワーク状況の観測・把握、具体的な策を施すための情報収集・分析が不可欠です。セキュリティ本部は、そうしたインテリジェンスを、二四時間三六五日体制で提供できるプラットフォームになっていきたいと思います。●

CSIRTの本質

企業においてセキュリティインシデントに対応する専門組織CSIRTは、
どのような考えにもとづいて設立し、運営すればいいのか？
ここではその要項をまとめてみたい。

IIJ セキュリティ本部
セキュリティビジネス推進部 インテグレーション課
片桐 卓

セキュリティ分野におけるこの一年は、政府による基準や指針が施行され、頭を悩ますことも多かったかと思います。我々にとっては、さまざまなお客さまにお目にかかり、いろいろな意見をうかがうことができた有意義な年でした。

本稿では、どうすれば、どんな企業でもCSIRT（Computer Security Incident Response Team）の本質を理解し、間違えることなく立ち上げられるのかという点について、ひとつの見解を述べさせていただきます。

CSIRTとは

CSIRTという言葉を聞いて連想するイメージとしては――企業をセキュリティインシデントから守る組織、ITやセキュリティに精通したエンジニア集団、困ったときの連絡先といったイメージから、マルウェアと日々格闘し解析を行なっている、ログを四六時中分析している、寝る間も惜しんで働いている、やや近寄りがたい存在……等々、連想する人の立場によって多種多様だと思います。

では、本質的にCSIRTはどのような機能を提供するのでしょうか？ 先に挙げたイメージの通り、かなり高度な技術を持った人材が在籍する組織であると認知されているかもしれません。しかし、CSIRTのもっとも大きな役目は、現場で発生している事象を迅速かつ正確に把握し、社員を正常な業務状態に復旧させ、経営層へわかりやすく伝える。そして、状況の判断材料を揃え、現場としての見解を添えて、経営層へレポートし、最終的な判断を下してもらうこと、と言えます。

ただ、事象を判断すること自体が非常にむずかしくなっており、従来のような（PCが）ウイルス感染したとか、貸与物を紛失したなど、白黒を明確につけられるものは少なく、専門家が調査・分析しながら濃淡をつけていく必要があります。

そのためCSIRTは、本来、経営リスクを統括する部門に立ち上げるべきですが、実際には情報システム部門で組織されることが多いようです。これは「弊害」とまでは言い切れませんが、情報システム部門の考えるリスクと経営層の考えるリスクの認識に違いが生じるなど、相互の意思疎通が十分でないケースも見受けられます。こうしたズレが生じたとき、いかにコミュニケートして対処していくかが、企業における組織内CSIRTが縦横無尽に活動できるか否かのカギになります。

CSIRTが動かない

昨年度、筆者が見聞きした限りでは、CSIRT組織の構築を試みたものの企画

倒れになってしまった、組織化の素案はできているが実施直前で停滞している、組織を発足し人員をアサインしたが成果を出せていない、といった話がいくつかありました。

今やITインフラは、企業に飛躍的な生産性向上をもたらす、業務に不可欠なものとなり、企業活動全体をカバーしています。そこで、CSIRTの守備範囲も企業全体を網羅できるよう対処しようとすれば、全般的な施策を練る必要が出てきます。その際、最初からすべてを実施しようとすると、検討に費やす期間だけでも長期に及んでしまいますが、CSIRTの本質を踏まえれば、（企業の内外からの）連絡先とメールアドレスがあればCSIRTは開始できます。ポイントを押さえた最小のスコープから始めて、人員や組織の成長とともにCSIRTも成熟させていくのが現実的ではないでしょうか。

CSIRTは作ったら終わりではありません。日本ではこれまでの経緯から、セキュリティと言えば、ISMS（情報セキュリティマネージメントシステム）、PMS（個人情報保護マネージメントシステム）などを導入すれば、対処がほぼ完了するといった事例が大半でした。CSIRTも同じと言えば同じですが、大きな違いがあります。それは、ISMSやPMSのようなマネージメントシステムでは、企業の規則（ルール）を設定していきます。その内容はすべて白黒判別することが可能な状態になっていますが、CSIRTの場合、対処するインシデントが白なのか黒なのか、判別するのが困難なことがほとんどです。判断が明確なものは、そもそも対処手順が決まっているので、CSIRTの中心業務ではありません。一方、受け取り手がない、こぼれた事象に対処するのがCSIRTの重要な業務となります。可能な限り情報を収集し、これまでの知見を組み合わせながら濃淡をつけ、最終的に〝人による決断を下す〟という作業が求められます。これらを積み重ねながら、初期に作った組織や規約・手順などを徐々に最適化し、企業にCSIRTを根付かせていくのです。

CSIRTに必要なもの

何よりもまず、さまざまな人と会話ができるコミュニケーション能力が大切です。社内のあらゆる部門に加え、外部ベンダや公的機関もコミュニケーションの対象になり得ます。繰り返しますが、CSIRTの本質は、確実な情報を迅速に発信して、経営層とともに判断していくことです。よって、日頃からいろいろな部門とコミュニケートしている人材がCSIRTの初期メンバーには最適かもしれません。

セキュリティインシデントが発生している現場の社員とのコミュニケーションも良好な状態を保つ必要があります。不測の事態が発生すると、継続すべき業務が停止してしまうことで現場は不安だらけになりますので、安心をもたらすような関係を築けるよう心がけましょう。

また、発生しているセキュリティインシデントを、経営リスク（経営層にわかる内容）に翻訳する力も欠かせません。ぜひ積極的に普段から経営層との意思疎通を図り、互いに認識の齟齬が生じないようにしていただきたいと思います。

昨今では新聞やニュースでセキュリティインシデントに関する記事を多く見かけます。こうした内容を題材として、①どのような事象なのか。②その事象は企業にとってどのようなリスクになり得るのか。③自社にも該当する部分はあるのか。以上の三点について経営層と意見交換を行なっておくといいでしょう。

経営層とCSIRTが判断を下すために必要な情報が企業内部だけでは揃わないことも考えられます。そうした事態に備える意味で、積極的に外部ベンダとのつながりを持つことも重要です。外部とのつながりには、システム導入、セキュリティ機材の導入やアウトソーシング、解析、アドバイザリーなどいろいろありますが、できるだけ高度な知見・技術力を持ったベンダと交流しておくことをお勧めします。日本国内で高度な技術者を内製化できる企業はほんのひと握りです。ですので、各分野の技術者と情報を共有しておくこともCSIRTに求められる活動と言えます。

二〇二〇年に向けて

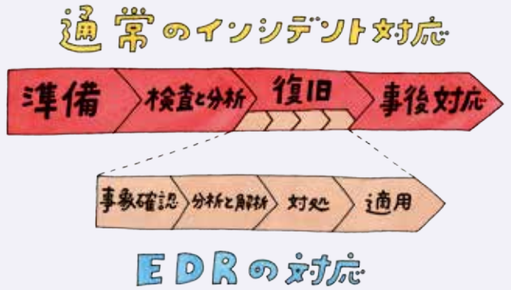
最近、時世に乗じて多くの（CSIRTの本質から外れた？）セキュリティ製品が出ており、製品カテゴリも増え続けています。先ほども申しました通り、セキュリティインシデントへの最終判断は人によって下されるべきです。判断基準が明確でセキュリティ製品により代替可能であればいいのですが、判断材料を提供する製品には、余計な情報まで集まり判断を鈍らせてしまう危険性があります。もっとも重要なのは、企業にとってのリスクをコントロールすることです。この点を常に忘れないようお願いいたします。

二〇二〇年の東京オリンピック・パラリンピックに向けて、今後一層、サイバー攻撃が熾烈になることも予測されます。サイバーセキュリティに対する理解と実践を踏まえて、万全の準備を整えておきたいものです。●

事件は「エンドポイント」で起こっている

サイバー攻撃の手法は日に日に巧妙になっており、
個人ユーザの端末（エンドポイント）をその攻撃から守ることはますます困難になりつつある。

IIJ セキュリティ本部 セキュリティビジネス推進部
インテグレーション課 シニアテクニカルマネジャー
加賀 康之



二〇一六年八月の初旬、IT企業A社でシステムエンジニアとして働くN氏。気温は朝から二五度を超え、汗だくになりながらも普段と同じように出勤した。

朝の日課はメール処理である。夜間に発生した障害アラートメールと、その一時対応履歴のメールがずらりと並んでおり、朝から憂鬱な気分になる。メールボックスをひとつずつ見ていくと、いつもとは違う雰囲気のメールが一通あることに気づいた。差出人は三ヵ月前に参加したセキュリティセミナーの主催会社で、内容は新たなセミナーの案内だった。しかし何か変である。文面は普通だが、旧字体というか繁体字の漢字が用いられている。不信に感じたが、差出人は信頼のおけるセミナー会社であり、またセキュリティ技術にも興味があったので、面白そうなセミナーなら参加してみたいと思い、添付されていた「案内状PDF」を開いてみた。

すると画面が一瞬暗くなり、「実行しますか？」というダイアログが出た。ウィンドウズ標準のユーザアカウント制御（UAC）*1である。「ん？　PDFファイルを開くのに、なぜUACが出るのだろう？」と思いながらも、反射的にOKボタンを押してしまう。PDFは正常に開き、セミナーの案内も表示された。セミナーの内容は前回とほぼ同じらしく、「参加の必要はない」と判断し、PDFを閉じて通常業務に戻った。

内部偵察、そして……

同月の中旬、A社の情報システム部門でシステム管理者として働くL氏に一本の電話がかかってきた。発信元はセキュリティ監視サービスを委託しているI社。普段はほとんど電話連絡のない会社であったため、嫌な予感がした。

電話に出ると、こう告げられた。「貴社のIPアドレスがブラックリストに登録されているC&Cサーバ*2と通信しており、そのIPアドレスから大量のデータが送信された形跡がある。すぐに当該IPアドレスのPCもしくはサーバをネットワークから切り離し、マルウェアなどに感染していないか調査することを推奨する。当該IPアドレスはxxx.xxx.xxx.xxx」。

L氏は電話を切ったあと、当該のIPアドレスを使用している部門・管理者を確認するよう部下に指示を出すと同時に、危機管理部門へ報告を行なうことにした。当該IPアドレスの使用部門とコンピュータはすぐに特定できた。当該IPアドレスを使用していたのは検証用のサーバだった。

しかし、ここで問題が発生した。その検証用サーバは特定の人物が一人で使用しており、ログイン用のIDとパスワードはその本人しかわからないという。さらに、その人物は夏季休暇中で次に出社するのは三日後だった。至急、上司から本人へ連絡を試みるが、休暇中ということもあり連絡がつかず、サーバの状況もわからない。そこで緊急対応としてサーバをネットワークから切り離すことにした。ここまでの対応に丸一日を要した。

三日後――

検証用サーバの担当者が出社し、さっそくサーバ内を調査したところ、作った覚えのないzipファイルがテンポラリフォルダにあった。ファイルを開いてみると、クレジットカード番号を含むA社の顧客リストと契約内容が一覧になったエクセルファイルが複数入っていた。

担当者から報告を受けた情報システム部門の管理者L氏はすぐに危機管理部門に知らせ、危機管理部門からセキュリティ担当役員へ報告が行なわれた。

その後の調査で、情報の漏えいに至ったそもそものキッカケは、N氏に送られてきたあの不信メールであることがわかった。結局、感染からセキュリティ担当役員に報告がなされるまでに約二週間もかかったことになる。（以上の物語はフィクションであり、実在の企業、事案とは関係ありません）

本事象の考察と情報システム部門にできること

本事象は「ばらまき型攻撃」の一種です。ただ、N氏がメールを開かなければ、防ぐことができたでしょうか？　最近のばらまき型メールは巧妙です。標的型攻撃となるとさらに巧妙になるため、人の感覚・訓練だけで不信メールを判別するのは、ひじょうに困難です。

次にセキュリティ監視サービス会社から連絡を受けた情報システム部門の対応はどうだったでしょうか？　C&Cサーバとの通信を検知している以上、何からの攻撃または感染があることは確実です。すぐに当該IPアドレスの所有者に確認するまでは良かったのですが、当該サーバが検証用サーバであり「重要なデータはないだろう」と思い込んでしまい、担当者の出社まで待つことにしたのは、適切ではありませんでした。攻撃者は検証用サーバを攻撃したわけではなく、踏み台サーバとして利用したのです。担当者が夏季休暇中というのも、ただの偶然ではなく攻撃者は事前に把握していたかもしれません。

最後の砦〝エンドポイント〟

こうした事象を防ぐには、いろいろなアプローチがあると思います。アンチウイルスの多層化、サンドボックス製品の導入、社員のセキュリティ教育などです。しかし、報道されているような実際の事件もそうですが、事象の起点はエンドポイントにおけるマルウェア感染というケースが圧倒的に多いのです。

重要サーバまでの経路やインターネットの出入口を複数のセキュリティセンサで監視することはもちろん必要ですが、エンドポイントのセキュリティ強化が、脅威の排除に大きな効果を発揮することがわかっています。

今、エンドポイントセキュリティが新たな世代に移り変わろうとしています。二〇一四年、ガートナー社がEDR(Endpoint Detection and Response)*3という考え方を提唱しました。

これまでのエンドポイントのセキュリティ対策は、ウイルスから〝保護する〟ことに主眼が置かれていましたが、EDRは、万が一、ウイルスに感染しても正しい〝事象確認と証跡保存〟を行ない、被害を最小限に抑えるとともに適切な事後対処方法の確認のための機能を重視した製品を導入すべきだという考えにもとづいています。既存の定義ファイルをベースとしたアンチウイルスによるエンドポイントセキュリティは検知の限界にきており、EDRは〝次の一手〟となり得る対策と言えるでしょう。（右頁イラスト参照）

IIJではエンドポイントソリューションとして、機械学習を用いた新たなアンチウイルス製品の取り扱いを開始しました。また今後は、感染後の適切な事象の把握と対処方法の提言ができるよう、EDR製品の取り扱いも予定しています。

過信は禁物

新たなエンドポイントソリューションを提案すると、お客さまから次のような質問を受けることがあります。「エンドポイントセキュリティが完璧であれば、その他のセキュリティセンサは要らないですか？」。

なかなか鋭い質問です（笑）。たしかに脅威の起点がエンドポイントであることは多々あります。しかし、これはセキュリティ全般に言えますが、〝一〇〇パーセント防ぐ〟ことは、どのような製品でも不可能です。サンドボックス製品が世に出ると、すぐにそれをすり抜けるマルウェアが現れたように、セキュリティ対策は常にイタチごっこです。ですから、驚異的な検知率を誇るエンドポイント製品が開発されても、やがてそれを回避する技術が出てくるでしょう。ひとつの製品を過信せず、多層防御をとることが引き続き重要だと考えています。●

*1「ユーザアカウント制御（User Account Control：UAC）」は、Windows Vista 以降の OS に実装されている機能で、ウイルスや不正な操作、操作ミスなどによって、管理者権限が必要となる操作（システム設定の変更やプログラムのインストールなど）が自動的に実行されてしまうのを防ぐことを目的としている。

*2 C＆C サーバとは「コマンド＆コントロールサーバ」の略。マルウェアに感染したコンピュータを制御したり、命令を出したりする役割を持つサーバを指す。

*3「Endpoint Detection and Response：EDR」は、ガートナー社が 2014 年に提唱した考え方。これまでのエンドポイントセキュリティ製品は定義ファイルによる検知と保護が主な機能であったが、EDR ツールはエンドポイントでの脅威を検知し、その後の対応を支援する。
https://www.gartner.com/doc/2926318/competitive-landscape-endpoint-detection-response

見過ごせない!? WEBアクセスのセキュリティ

メールやWEBを無防備に使っていると、サイバー攻撃の被害に遭う危険性がある。
本稿では特にWEBアクセスに関するセキュリティの話題を
有効な対策方法と合わせて紹介する。

IIJ サービスプロダクト事業部
第二営業部長 兼 セキュリティ営業課長
三木 庸彰

プロキシサーバの導入

二〇一五年に起きた年金機構の情報漏えい事故以来、セキュリティ対策の見直しについてさまざまなお客さまにご提案させていただく機会が増えたのですが、このとき意外だったのが、中・小規模の企業を中心にプロキシサーバを未導入のお客さまが多かったことです。

プロキシサーバはキャッシュ機能を利用するためのものという前提であれば、たしかに今のブロードバンド回線の時代には必要性ありません。ただ、もし標的型攻撃によってマルウェアに感染し何らかの被害が想定されるときは、攻撃者が感染したユーザ端末を乗っ取ってどのような通信を行なったのかといったログを調査するうえで、プロキシサーバは重要な対象になります。そして攻撃による被害が発覚した際には、プロキシサーバを導入していなければ、不正な通信を把握できず、被害の特定もむずかしくなり、対策不十分ということで問題を大きくしてしまう懸念もあります。よって、プロキシサーバの導入は、最初に確認・検討すべき対策だと言えます。

HTTPS通信に潜む危険

WEBサイトの改ざんや盗聴が大きな問題となり、個人のプライバシー保護のために通信を暗号化するHTTPS対応が注目されています。そうしたなか「Let's Encrypt」と呼ばれるプロジェクトのもと、HTTPS対応に必要なSSL／TLS証明書を無料で提供するサービスが二〇一六年四月にスタートしました。証明書発行のコストをかけずに通信の暗号化が可能になったことで、今後、普及が加速すると考えられます。

ところが、もし攻撃者がHTTPSを悪用し、暗号化された通信を通じてマルウェアを配布したら、インターネットゲートウェイでのウイルス対策ソフトはもちろん、サンドボックスでも検査できず、ユーザの端末まで到達してしまいます。サーバ証明書が無料になったということもあり、これまで以上に攻撃者に悪用される懸念があるため、HTTPS通信をデコード（復号化）して、ウイルス対策ソフトやサンドボックスでスキャンできるようにしたいという相談が増加しています。

ただ、デコードを実現しようとすると、そのために新たにハードウェアを追加・導入しないといけなかったり、導入済みの製品にデコード機能が付いていたとしても、それを利用すると高負荷で通信が異常に遅くなってしまう、といった課題も出てきます。そこで「IIJセキュアWebゲートウェイサービス」では、HTTPSのデコード機能をオプション（有償）で提供しています。自社に設備を置くことなく、クラウド型サービスとして利用できるので、新しい製品や高性能な製品を購入する前に、ご検討いただければ幸いです。

"見ただけ"で感染する静かな脅威

「マルバタイジング」という造語をご存じでしょうか？　悪意あるオンライン広告を意味するセキュリティ用語ですが、このマルバタイジングが問題になっています。これは、ニュースサイトなどのWEBサイトに表示されるオンライン広告に悪意あるコードを埋め込み、ユーザがアクセスして広告が表示された（またはクリックした）際に、マルウェアを配布するサイトなどに誘導する攻撃です。

この攻撃は、当該するWEBサイトが不正アクセスを受けたことにではなく、掲載している広告ネットワークに対して攻撃者が悪意ある広告を配信したことに起因するため、WEBサイトの運営者は被害を受けた側とも言えます。ユーザも、怪しいWEBサイトを見たわけでなく、一般的なWEBサイトで広告を表示しただけでマルウェアをダウンロードしてしまうため、インターネットの利用者なら誰でも気付かずに感染する危険があります。実際、国内の一般的なWEBサイトがこの攻撃の被害に遭い、閲覧したユーザがマルウェア感染したという事例もあります。

最近「ばらまき型攻撃」と呼ばれるメールによるランサムウェアの拡散が問題になっていますが、このマルバタイジングもさまざまなマルウェアを拡散する手法として攻撃者に利用される可能性が高いと思われます。

インターネットは原則禁止!?

このところ、従業員のインターネットアクセスをホワイトリスト方式にする、という措置が現実味を帯びてきているように感じています。これまでは業務用の端末で自由にインターネットを利用できましたが、業務に関係のないWEBサイトについては原則禁止とし、業務上見る必要があるWEBサイトは申請して許可リスト（ホワイトリスト）に登録するという方法です。

スマートフォンやタブレットの普及を背景に、ニュースサイトや個人のWEBメールなどを見たいときは、ユーザ個人の端末で見てもらうということでしょうが、全面的に導入するのはむずかしいかもしれません。ただ、WEBアクセスセキュリティにかかるトータルコストを考えると、あながち非現実的なこととは言えないのではないでしょうか。

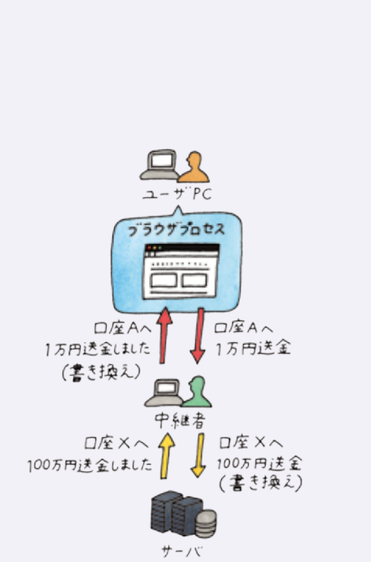
もう一つの方策に「ネットワーク分離」があります。先行事例として全国の自治体において、マイナンバー制度の導入に向けたセキュリティ強化の目的で、ネットワークを分離する取り組みが進んでいます。業務に使うネットワークとインターネットにアクセスするネットワークを分離し、セキュリティを向上させようという狙いです。万が一、マルバタイジングなどの被害に遭っても、マルウェアに感染するのは（業務用ネットワークの環境ではなく）インターネット用の環境だけなので、情報漏えいなどの心配を最小化できます。

企業においても、仮想デスクトップを活用して同様の機能を実現しているところがありますが、導入・運用コストが高い点が課題でした。最近、コストの問題を解決する新しい製品やサービスが登場しており、二〇一七年以降、徐々に普及が進むと見られています。IIJでもサービス開発に取り組んでおり、自治体向けの「IIJセキュアブラウジングサービス」を先行して発表いたしました。今後は、一般企業でもご利用いただけるサービス品目をリリースいたしますので、どうぞご期待ください。●

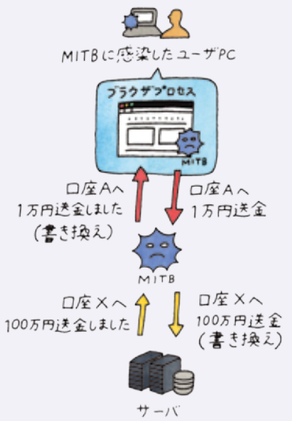
“認証”強化の具体例

WEBサイトで金銭のやり取りを行なう機会が増えているが、
そうした場は、特にサイバー攻撃の標的になりやすい。
そこで今回は、より強固な「認証」システムの指針となる技術を紹介する。

IIJ ネットワーク本部
プロダクト推進部 企画業務課
渡辺 尚徳



Man-In-The-Middle attack



Man-In-The-Browser

インターネットバンキングやオンラインショッピングサイトといった、利用者の金銭に直結するWEBサイトが、自宅・職場・移動中など、まさに至る所で気軽に利用できるようになりました。

その一方で、こうしたWEBサイトが次々にサイバー攻撃を受け、不正ログインが発生する被害も起きています。これらは、利用者のセキュリティの甘さやシステムの脆弱性につけ込んだ不正ログインによるもので、その手口は年々巧妙化しています。ここ数年間でも、ふたつの新たな脅威が現われました。

MITBとMITM

MITB(Man-In-The-Browser)は、利用端末に「トロイの木馬」などのマルウェアを侵入させ、インターネットバンキングなどのWEBサイトにおいて、利用者が意図しないかたちで多額の不正送金を行なわせる手法です。攻撃は、利用者とブラウザのセキュリティの仕組みのあいだで行なわれます。よく似た手口のフィッシング攻撃とは異なり、利用者は本物のサービスに正しくログインして利用するため、何も違いが見あたらず、まったく気づかれないのが特徴です。この攻撃の脅威は、対象となるWEBサービスで認証後のセッションが確立されてから介入してくるため、ワンタイムパスワード(OTP)やPKIといった既存の多要素認証技術が意味をなさない点です。

MITM(Man-In-The-Middle attack)は、中間者攻撃といったほうが聞き覚えがあるかもしれません。不正WEBサイトが通信経路に割り込み、利用者が認証情報を漏らすことを狙った手法です。攻撃者は、利用者と正しいWEBサイトのあいだで交わされるすべてのメッセージを横取りし、別のメッセージを差し込みます。利用者には直接対話しているように思わせるため、気づかれにくいのが特徴です。仮に利用者がOTPを使っていたとしても、生成されたOTPの有効時間が切れる前であれば、何度でも認証が成功してしまうため、有効時間内に不正WEBサイト経由でログインされてしまいます。

以上のように、ランダムパスワードを毎回生成するOTPやPKIといった既存の多要素認証だけではMITBやMITMの対策にはなりません。では、これらの攻撃に対して、どのような対策が有効かと言いますと、「マルウェア対策」と「認証」の二点が重要になります。

まず「マルウェア対策」ですが、MITBの場合、利用端末のマルウェア感染がトリガーとなりますので、マルウェア対策ツールを導入して、感染を防ぐことが有効です。ただし、それだけでは攻撃を完全に防ぐことはむずかしく、「認証」に関する対策も必要となります。

「認証」については、サイバー攻撃の対象になりやすい金融機関を監督する金融庁も、「二要素認証」「トランザクション署名認証」「二経路認証」といった対策が有効である、との見解を示しています。

二要素認証

あらゆるWEBサービスでは、利用者の識別にユーザIDが用いられます。そして、ユーザIDを使用してサービスにアクセスした利用者が本人であることを確認するために「認証」が必要となります。その際、一般的に利用されるのが、本人だけが知っている「パスワード」で、これに「本人だけが持っているもの」または「本人の生体情報」を組み合わせて、ふたつの要素による認証を行なうのが「二要素認証」です。

多要素認証を利用すれば、ID・パスワードが盗まれただけでは不正が行なわれないよう保護できるため、こうした対策は最低限の対応だと考えられています。しかし、既存のOTPやPKIなどの二要素認証を用いても、MITBやMITMを防げないことは先に述べた通りで、二要素認証だけでセキュリティが万全になるわけではありません。

トランザクション署名認証

通常のWEBサイトの認証では、ログインできたユーザがログアウトするまでを正しいユーザと判断して処理が行なわれます。しかし、MITBのようにログイン認証後に介入してくる攻撃も存在するため、決済や商取引などトランザクションの前にも再度認証を実施することが考えられます。

トランザクション署名認証を説明する前に、OTPの規格について整理したいと思います。主要な規格は二種類で、RSAセキュリティ社の独自規格である「RSA規格」と各社の相互運用を目的とした「OATH規格」があり、OATH規格には、一定の時刻間隔で自動的にパスワードを生成する「時刻同期方式」、利用時に新しいパスワードを生成する「イベント方式」、さらに、管理者(サーバ)から送付される乱数(チャレンジ)を入力し所定のアルゴリズムで演算した結果(レスポンス)を生成する「チャレンジ&レスポンス方式」の三方式があります。

現在、多くのWEBサイトで採用されているのは「時刻同期方式」ですが、先述した通り、この方式だとOTPの有効期限が切れるまでは、何度でも認証が成功してしまいます。攻撃者は時間内でOTPを不正入手して、悪用しようとするため、「時刻同期方式」はMITMの対策にはなりません。

「イベント方式」は、利用者がOTPを利用しない限り、OTPが更新されない仕様であるため、ID・パスワードが漏えいしていると、(MITMやMITB攻撃以前に)OTPに対して総当り攻撃が成り立ちます。

「チャレンジ&レスポンス方式」では、チャレンジの部分を任意の値に置き換えることが可能です。そのチャレンジの部分をトランザクション内容(送金や商取引)の情報に置き換えて、レスポンスを生成させることを「トランザクション署名認証」と言います。利用者が事前に入力したトランザクション内容をもとにチャレンジを生成させることで、攻撃者にレスポンスが盗まれたとしても、利用者が入力したトランザクション内容以外の処理が行なえず、OTP認証が失敗するため、MITBやMITMの攻撃への対策となり得ます。

二経路認証

二経路認証とは、ログインや取引を実施する際に、その処理を行なっている通信経路とは別経路で処理内容を承認する方式です。MITBやMITMといった攻撃はどちらもアクセスしている経路を汚染し、処理内容を改ざんするため、別の経路を確保して、その別経路上で処理内容の承認を実施します。

以上、MITBやMITMの対策を述べてきましたが、IIJではクラウドサービスとして、認証強化ソリューション「IIJ SmartKey マネージメントサービス」を提供しています。本サービスは「スマートフォンを利用した二要素目の追加認証機能の提供(OTP認証／スライド認証)」「追加認証時のリクエストを独自経路で要求(他経路認証)」「追加認証時のリクエスト内容を通知(ログインや取引内容の通知)」といった機能を備えており、MITBやMITMへの有効な対策です。IIJではこうしたサービスを通して、今後もお客さまの課題解決をサポートしていきたいと考えています。●

人と空気とインターネット

インターネットの「第三の波」

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

ある市場に新たな変革が起こり始めたとき、
既存勢力とのあいだに軋轢が生じ、
それが結果的に、変革のスピードを
遅らせてしまうケースが多々ある。
ICTがそれ以外の世界も巻き込んで
起こそうとしている〝新たな波〟に、
日本はうまく乗ることができるだろうか？

最近、インターネットを用いたさまざまな「シェアリングエコノミーサービス」が欧米を中心に広まり始めています。シェアリングエコノミーでは、Uberならば自家用車、Airbnbなら自宅、といったふうに、自分の所有しているモノが空いていればそれを他者に利用してもらうサービスを、誰でも提供できます。

こうしたサービスの普及は、所有物を他者とシェアするサービスを提供したい人と、それを利用したい人とのマッチングが、インターネットによってリアルタイムに、そして安価かつ簡単に行なえるようになったことが大きいでしょう。

ただし日本の場合は、Uberに対してはタクシー業界が、Airbnbに対しては旅館業界が反対したり、それぞれの業界特有の商習慣や規制があったりして、シェアリングエコノミーサービスが全面的に利用できる状態には至っていません。

現状では、こうした新たなサービスを日本の市場にどう取り入れていくべきか、政府主導の委員会などで規制緩和を検討したり、一部特区を設けて実験的サービスを実施したりしている段階です。

Airbnbとも関連する個人宅の空室を有料で貸し出す「民泊」については、今年六月二日に営業日数の上限を「年間一八〇日以下」とすることを条件に解禁する方針が閣議決定されました。ただ、営業日数に制限を課されては、そもそも民泊事業が成り立たない、という反発の声もあがっているそうです。

当然、旅館やホテルといった既存事業者は自分たちのビジネスを守るために、必死でロビー活動を繰り広げるはずです。調整は一筋縄ではいかないでしょう。

こんな話をしていると何とも懐かしい気分になるから不思議です。日本ではそもそもインターネット自体がその黎明期に、既存通信事業者や通信関連の規制により新規参入を阻まれていた時期があったからです。

特にIIJがベンチャーとして起業した当初は、ベンチャー企業が通信サービスをやった前例がない、という理由だけで、サービスを提供するための事業者登録が認められず、起業後一年以上も事業を開始できなかったのです。

ネットワークサービスとしてのインターネットの導入が遅れたことが、それを前提とするWWWのようなメディアサービスの立ち上がりを遅らせる原因になったはずですし、その後も、著作権法や関連業界との調整の遅れが、検索エンジンのようなネット上での情報収集や加工をともなう情報サービスの立ち上がりを遅らせる要因になったことは間違いありません。

それまでなかった新たなサービスが世界のどこかで始まった時点で、日本でもいくつもの既存企業やベンチャーが参入し国内に新市場を形成して、競争しながらサービスや関連技術の高度化を図っていくような環境は、いつになったら形成されるのでしょうか。

このままだと、既存業界との調整や法規制上の対応が長引いているあいだに、日本企業は新たな動きに乗り遅れ、調整が済んだころには、すでに大きく成長した海外企業が日本市場になだれ込んで来て、一気に市場を奪われる、といったことが繰り返されるばかりではないでしょうか。

IoTからIoEへ

アメリカ・オンライン（AOL）の元CEOで共同創設者であるスティーブ・ケース氏は、UberやAirbnbのようなサービスをインターネットの「第三の波」に位置づけています。これは、未来学者のアルビン・トフラー氏が一九八〇年に出版した『第三の波』という有名な書籍にあやかった命名です。

トフラー氏は、産業発展の歴史を振り返り、農業革命を第一の波、産業革命を第二の波と位置づけ、それに続く第三の波として情報革命が起こる、と予言しました。それが見事的中したことは、改めて指摘するまでもないでしょう。

一方、ケース氏が言うインターネットの第一の波とは、IIJが国内で起業してインターネットのインフラをゼロから築いたインターネットの黎明期を指します。前述のように、第一の波では、インターネットはなかなか理解されず、既存の通信事業者やメディア事業者、そうした業界の監督官庁とのあいだに軋轢が生じ、IIJのような第一の波のプレーヤーはそれらを乗り越えて、インターネットというモノを広めていくところから始めなければなりませんでした。

第二の波では、インターネット自体はすでに世の中に受け入れられ、第一の波の軋轢も解消されていたので、それを土台としてeコマースサービス、検索サービス（日本ではうまくいかなかったことは前述の通りです）、ソーシャルネットワークなどの新たな情報サービスが次々にスタートしました。

そして第三の波では、インターネットによる変革が、いよいよ通信やメディア以外の領域にも組み込まれていく過程が始まるというのです。つまり、インターネットという情報ネットワークが、次第に情報以外のモノの製造・流通・サービスを制御するようになり、既存の枠組みにとらわれることなく、誰もが自由にさまざまな製品やサービスをつくって提供できるようになる、ということが起こり始めているのです。

ケース氏はこの状況を、人間が自分たちの行なうあらゆることにインターネットを統合すること、すなわち〝IoE（Internet of Everything）（あらゆるモノのインターネット）〟と名付け、まさに今、それが起こり始めていると言っています。

彼の主張は、IoT（モノのインターネット）で言われていることと基本的には同じですが、語る視点が大きく違っています。IoTはどちらかというと具体的なモノをどうやってインターネットにつなげるかという個別のモノの視点や技術論から語られることが多いように思いますが、IoEはもっと大きくサービス全体がどう変わるか、さらに産業全体がどう変わるのかというマクロな文明論の視点から語られているように感じます。

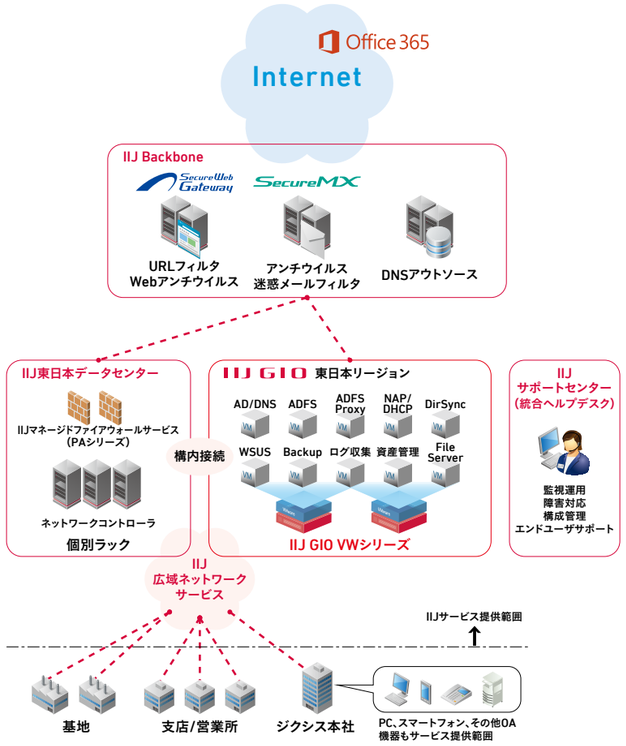
第三の波では、第一の波で起こったような既存の業界や規制とのぶつかり合いが、さまざまな業界で同時多発的に起こるでしょう。われわれの業界が最初に苦労したことを、そうした業界の新規参入者たちが再び経験することになるのです。願わくは、ICT業界がインターネットの立ち上がりの遅れにより海外勢に大きくシェアを明け渡すことになったという苦い教訓を活かして、建設的な調整を速やかに進めてほしいものです。●

イラスト／末房志野

Technical Now

新会社の「オフィスIT」の構築・運用を IIJにフルアウトソース 業務基盤のサービス化により、 初期構築コストを1/3に低減

LPガス元売4社の事業統合により誕生したジクシス。
同社は、ユーザがオフィス業務で必要となる情報系システム「オフィスIT」全般を
IIJにフルアウトソースした。オフィスITをサービス化することで、
約6ヵ月でPCを含めたすべての業務基盤を整備し、迅速な業務の立ち上げが可能になった。
実績豊富なIIJの多様なサービスを活用することで、初期構築コストも1/3に低減できた。



ジクシス株式会社
人事総務本部　情報システム部
次長　吉田 真典 氏

ジクシス株式会社
GYXIS

ジクシス株式会社
本社：東京都港区芝五丁目36番7号
　　三田ベルジュビル12階
設立：2015年4月

[導入前の課題]
新会社の規模感や IT 要件が不確定。自前のインフラはリスクが大きい

コスモ石油、昭和シェル石油、住友商事、東燃ゼネラル石油の 4 社の LP ガス事業の統合により、2015 年 4 月に誕生したジクシス。LP ガス元売トップクラスの実績を誇る 4 社それぞれの強みを発揮し、社会基盤を支える LP ガスの安全・安定供給を強化するとともに、次世代に向けた新たな価値創造を目指している。

シナジー効果を最大化するためには、会社の枠組み構築など 4 社の合意形成が不可欠だ。しかし、文化の異なる 4 社の事業を統合するのは容易ではない。全体の枠組みが決まらなければ、新会社の規模感や業務に必要な IT インフラの要件も見えてこない。「事業統合に向けた話し合いが進むなか、当初は IT に対して、どれだけの人とコストを費やすべきかわからない状態だったのです。その状態で自前のインフラを持つという決断は、大きなリスクになりかねません」と同社の吉田真典氏は語る。

そこでジクシスが選択したのが “持たざる IT” である。「業務に必要な『オフィス IT』をすべてサービスとして利用するかたちにすれば、短期間で IT 環境の整備が可能です。自前でインフラを調達したり、システムを構築する必要がないので、所有リスクも回避できます」と吉田氏は狙いを述べる。

[選定の決め手]
コストと導入スピードを評価。他社クラウドとの連携も可能

新会社に求められる IT インフラの要件が見えてきたのは 2014 年 8 月後半。新会社の設立時期は 2015 年 4 月と決まっていたため、対応を急ぐ必要があった。限られた時間のなか、同社はオフィス IT をサービスとして利用する方針にもとづいて複数ベンダの提案を募り、比較検討を行なった。その結果、選定されたパートナーが IIJ である。

IIJ の提案は同社の要件を十分満たし、なおかつ「コスト」と「導入スピード」で他社の提案を上回るものだったという。「初期構築コストは他社の提案に比べ 1/3 程度。5 年間の運用を含めたトータルコストも、もっとも安価に抑えられるものでした」と吉田氏は評価する。

導入スピードを支えているのが、IIJ の多様なサービス群だ。サーバ、ネットワークはもちろん、Active Directory をはじめとする認証基盤、メールやインターネット接続環境、セキュリティサービスのほか、PC や固定電話、スマートフォン、複合機に至るまで、業務に必要なサービスとインフラのすべてをワンストップで提供できる。こうしたサービスの提供を通じ、多くの企業の IT 環境の変革に貢献してきた実績も豊富にある。

「コミュニケーション基盤にはクラウド型グループウェアの Office 365 を利用する方針が決まっていましたが、IIJ は他社クラウドなどの外部サービスともシームレスに連携が可能です。オフィス IT のサービス化を安心して任せられ、短期間でリスクの少ない導入が可能になると判断しました」（吉田氏）

[導入後の効果]
約 6 ヵ月で業務基盤を構築。要件の変更にも柔軟に対応

現在、ジクシスはグループ会社を含めた 9 つの拠点で PC 約 230 台、スマートフォン約 130 台、固定電話約 200 台を導入し、主要な業務基盤を IIJ GIO に集約して、デバイスも含めたすべてのオフィス IT を「サービス」として利用している。

具体的には、本社および支店は二重化されたネットワークを介して IIJ GIO とつながっており、IIJ GIO の仮想サーバ上に構築した Active Directory、認証を統合する Active Directory フェデレーションサービスなどのサーバ群は Office 365 と連携している。さらに、Office 365 の Exchange Online によるメール通信は IIJ セキュア MX サービスと連携し、セキュアなメールのやり取りを支えている。

また、オフィス IT の実現には、IIJ の豊富なサービスと実績に加え、柔軟な対応力も大きな力になった。

会社が設立される 2015 年 4 月に向けて、極めて短期間で PC などのデバイスを必要台数分調達・設定するとともに WEB やメールの環境、業務を支えるサーバ環境なども迅速に構築する必要があった。「約 6 ヵ月で、すべてのオフィス IT を整備できたのは、IIJ の迅速な対応力のおかげです」と吉田氏は振り返る。

要件の変更に機敏に対応した点も評価している。初期の検討段階ではスマートフォンの利用は考えていなかったが、事業内容が見えてくると、社員のモビリティ向上の必要性が高まった。「IIJ はプロジェクト進行中にもかかわらず、機器の調達・設定からネットワーク環境の見直しまで柔軟に対応してくれました。その結果、計画通りに新会社の業務を立ち上げることができました」と吉田氏は満足感を示す。

導入後のサービスは安定稼働しており、大きなトラブルは一度も発生していない。煩雑な運用管理に人員を割く必要がないので、本来の業務に注力できるのも大きなメリットだ。

今後は BYOD を含めたモバイル環境の強化と、クラウドサービスの活用拡大を考えている。「他の SaaS の利用も視野に入れ、利便性とセキュリティの両立を図るシングルサインオンの仕組みを実現したいですね。より最適な IT 利用を加速するため、今後も IIJ の提案とサポートには大いに期待しています」と吉田氏は抱負を語った。●

Technical Now

進化する Biznet GIO Cloud

PT. IIJ Global Solutions Indonesia
Senior Vice President
田中 三貴

**好調が続くインドネシアの IT 市場において、IIJ が昨年から展開している
クラウドサービス“Biznet GIO Cloud”は順調な滑り出しを見せている。
ここでは、Biznet GIO Cloud に加わった新たなサービスを紹介する。**

インドネシア国内の IT 市場は高い成長率を維持しており、国際調査会社 IDC 社の昨年の報告によると、2019 年には現在の約 3 倍の 1.8 億米ドル規模に達するとされ、引き続き需要が拡大すると見られています。

2015 年 5 月、我々がインドネシアで提供を開始したクラウドサービス「Biznet GIO Cloud」は、2016 年 9 月時点で約 1500 社にご採用いただいています。一年という短期間で、インドネシア市場に受け入れられた要因は、IIJ の高いクラウド技術と、パートナーであるインドネシアの大手通信サービス会社 Biznet Networks の強固なインフラ基盤によるところが大きいと考えています。

インドネシア市場の特徴

今年 5 月まで提供していたクラウドサービスはいわゆる IaaS でしたが、同国のクラウド市場は PaaS や SaaS のほうがエンドユーザにとって導入しやすく、需要も大きいという特徴がありました。

そこで、既存インフラのうえに PaaS を開発することにし、今年 5 月 26 日、Biznet GIO Cloud 開始 1 周年を機に、4 つの PaaS「GIO Storage」「GIO Backup」「GIO Box」「GIO Bricks」をリリースしました。以下では、これらサービスについて紹介します。

オブジェクトストレージサービス GIO Storage

増え続けるデータの保管コストを抑えたいという要望を受けて開発された GIO Storage は、豊富な REST API（Amazon S3 互換）を提供し、大容量のデータ保存に最適な高い拡張性を備えたクラウド型ストレージサービスです。

従量課金制を採用し、データ保存料は 1GB あたり月額 700 ルピア（5 円程度）で、導入費用も不要です。保存容量は無制限なので、大容量のデータを保存できます。ストレージは 99.999999999 パーセント（通称「イレブン・ナイン」）の耐久性を誇り、保存データが失われる確率が極めて低い構造となっています。

このように最新の技術を採用し、柔軟でコスト効率の高いデータストレージサービスの需要に応えられるよう設計された GIO Storage は、データの収集・蓄積、ビッグデータの分析、既存のストレージ基盤のクラウド化など、多様な要件に適したソリューションと言えます。GIO Storage はオンラインでご利用いただけますので、サインアップからデリバリまでお客さまが自由に行なえます。

クラウド型のバックアップサービス GIO Backup

データのバックアップ機能はどんな企業にも必須だと思いますが、バックアップの仕組みを自社で用意するには、バックアップツールやストレージなどを購入する必要があります。また、データが増えると、ストレージの拡張なども考えなければなりません。GIO Backup は、お客さまがオンプレミスや複数のクラウドサービスで保管していたり、パソコンやモバイルなどに保存しているデータを Biznet GIO Cloud にバックアップするサービスです。

GIO Backup では、自動バックアップの規模と条件を個別に設定できます。ひとつのフォルダから VM レベルのバックアップまで、定期的な自動バックアップ以外にも、お客さまにご指定いただいたタイミングでのバックアップも設定可能です。また GIO Backup に保存されたすべてのデータは一元的に管理でき、データの復元も 1 ステップで行なえます。さらに、バックアップ時にすべてのデータが自動的に圧縮されるため、ネットワークの負荷を抑えられます。データの暗号化も選択可能で、機密性の高いデータを安全に保護できます。

GIO Backup はこうした多くの利点を備えているので、サービスリリース前からたくさんの引合いをいただき、現在は日系／現地企業を問わず、幅広くご利用いただいております。

GIO Bricks の UI

オンラインファイル共有サービス GIO Box

GIO Box は、Biznet GIO Cloud のラインナップのなかで唯一のコンシューマ向けサービスです。インドネシア人は、スマートフォンで写真を撮ったり、音楽をダウンロードして聞いたりするのが好きなため、写真や音楽データを保存できるオンラインストレージの需要が大きいとの判断のもと、GIO Box の開発が決まりました。

オンラインストレージサービスには、Dropbox、Google Drive、One Drive など手軽に始められるサービスがたくさんありますが、これらのサービス基盤はインドネシア国外に置かれています。インドネシアと海外との国際回線は不安定なことが多く、アクセスしにくかったり、レスポンスが遅いといった話をよく聞きます。

GIO Box は、モバイル端末やパソコンなどさまざまな端末から、ファイルを安全に保存・同期、そして SNS で共有できるシンプルなオンラインストレージサービスです。ファイルは、暗号化された安全な通信経路で送受信され、冗長化された GIO Storage に保存されます。お客さまは、安価な大容量ストレージを利用して、いつでも・どこからでも、ファイルを複数のユーザ間で共有できます。

これまで GIO Box は主にコンシューマ向けサービスでしたが、今年 10 月 1 日より、セキュリティが強化された、エンタープライズ向けのプレミアム版「GIO Box Enterprise」をリリースしました。GIO Box との違いは、GIO Box が共有環境の使用を前提としているのに対し、GIO Box Enterprise は専有環境を提供します。また GIO Box Enterprise には多くの商用機能が備わっています。

お客さまの SSL 証明書やドメインが使えるほか、インターネット VPN やクローズドネットワークでの使用にも対応しています。それだけでなく、ウイルス・スキャンやファイルの暗号化など、セキュリティ面も強化しています。また、企業単位でひとつ契約していただければ、ユーザアカウントを無制限に設けることができます。それぞれのアカウントの容量と権限は設定が可能で、グループ化などの管理機能を管理ツールからお客さま自身で操作できます。

企業内のユーザ（社員）が利用できる機能としては、App Store や Google Play から GIO Box Enterprise のアプリをダウンロードするだけで、モバイルデバイスからもサービスをご利用いただけます。カレンダーとアドレス帳のデータをアップロードすると、モバイルなどで、どこからでもそのデータにアクセスすることが可能になります。さらに GIO Box Enterprise には、ファイルの変更履歴を自動的に残す仕組みがあり、ボタンをクリックするだけで、簡単に前のバージョンに復元できます。

WEB アプリ開発プラットフォーム GIO Bricks

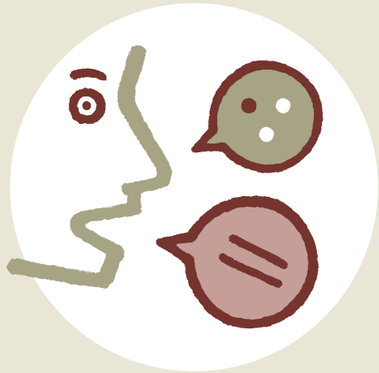
GIO Bricks は WEB アプリケーション開発者向けに、開発支援環境と実行環境をクラウド上で提供するサービスです。GIO Bricks をご利用いただくことで、サーバ構築やリソース管理の苦労から解放され、プログラミングに集中できます。

GIO Bricks は Java、PHP、Ruby、Node.js、Python など多彩なアプリケーションに対応しています。お客さまはパッケージ化されたアプリケーションサーバやデータベースを選択して、簡単にセットアップできるため、数分でシステム環境を導入できます。また WordPress などオープンソースのソフトウェアを数クリックするだけでデプロイでき、すぐにご使用いただけます。実行環境は、実際のトラフィックに応じて単一および複数のサーバで自動的にスケールアップ／スケールダウンを行なえます。一般のクラウドサービスなら監視が必要で、リソースの変更にはある程度時間がかかりますが、GIO Bricks はサーバにかかる負荷に合わせて、リソースを自動変更してくれます。その CPU や RAM の変更は数秒で完了し、再起動や再デプロイなども不要です。現在、GIO Bricks は β 版を提供しています。

以上、Biznet GIO Cloud に加わった 4 つの PaaS を紹介してきましたが、インドネシアを含め、世の中にはクラウドサービスの安全性に懸念を抱いている方がまだいらっしゃいます。そこで、今後も Biznet GIO Cloud 基盤の信頼性強化を目指して、PCIDSS（2016 年内）と ISO27001（2017 年内）を取得する予定です。そのほかにも、セキュリティ系のクラウドサービスを開発するなど、引き続きサービスラインナップの拡充に努めてまいります。●

インターネット・トリビア

スマートフォンと位置情報



IIJ MVNO事業部
MVNO事業統括室 シニアエンジニア
堂前 清隆

道に迷ったとき、目的の店が見つからないとき、スマートフォンをさっと取り出して地図アプリを開けば、「現在位置」を中心とした地図を見ることができます。今ではすっかり当たり前になったこの技術ですが、スマートフォンは現在位置をどのように調べているのでしょうか？ これには大きく分けて三つの技術が使われています。

一番よく知られているのは、GPS（Global Positioning System）です。GPSは上空2万メートルの位置を周回している複数の人工衛星から発信される電波を用いて自分の位置を調べるシステムです。GPS衛星にはとても精度の高い時計が搭載されていて、スマートフォンが受信した複数の衛星の時刻のズレを比較することで自分の位置を割り出します。

GPSは比較的精度が高く、条件が整えば数メートルの範囲で現在位置を特定できます。また、現在30機以上のGPS衛星が地球上にまんべんなく配置されており、世界中で利用できます。その反面、GPSには弱点もあります。ひとつは位置を特定するのに時間がかかること、もうひとつは人工衛星の電波を受信できない屋内や地下では利用できないことです。前者については、スマートフォンの場合、携帯電話網を使ってGPSの補助情報を取り込むことで、位置の特定に要する時間を数秒程度にまで短縮できます。しかし、後者については良い解決方法がありません。GPS衛星の電波はそれほど強くないため、コンクリートのビルなどでは窓際を離れると電波を受信できなくなってしまいます。

現在位置を特定するためのふたつ目の方法は、携帯電話の基地局の情報を使うことです。携帯電話の基地局が設置されている位置はある程度わかっているため、スマートフォンがどの基地局から電波を受けているのかによって、自分の大まかな位置を調べることができます。この方法であれば、衛星の電波を受信できない屋内でも大丈夫です。しかし、精度の問題があります。基地局が細かい間隔で設置されている都市部であれば、ほぼ精確な情報を得られますが、山間部など基地局間の距離が広がると、大まかな情報しか得ることができません。場合によっては、数キロメートル単位で誤差が出ることもあります。

三つ目の方法として、Wi-Fiのアクセスポイント情報から現在位置を特定する方法があります。携帯電話の基地局と同じように、アクセスポイントの設置場所がわかっていれば、周辺にある基地局の情報から位置を特定することは可能です。しかし、Wi-Fiのアクセスポイントは会社や個人が自由に設置できるため、どの基地局がどこに設置されているのか、一元的な管理は行なわれていません。そこで、事前にアクセスポイントの位置データベースをつくるという準備が必要になります。実は、Androidスマホやiphoneには、このような情報収集の仕組みが備わっています。GPSでスマホの現在位置を特定できたとき、周囲にあるアクセスポイントの情報を収集し、それらをGoogleやAppleのサーバに送信してデータベース化しているのです。

このような方法でデータベースをつくっているため、Wi-Fiアクセスポイント情報を使って現在位置を調べると、思わぬ結果になることがあります。例えば、アクセスポイントを移動させたのに、以前の設置場所がデータベースに登録されたままになっている場合があり、それを使って位置を調べた結果、現在地とまったく異なる場所が表示されてしまう、といったことが起こっています。

それぞれの仕組みには一長一短があります。スマートフォンで位置情報を取得する際には、場所の特性に応じて適切な方法が自動的に選択され、その結果が地図アプリなどで表示されるようになっているのです。●

イラスト／末房志野（P22,23）

グローバル・トレンド
クラウドセキュリティ規格「MTCS」

認証取得までの道のり

IIJ Global Solutions Singapore Pte. Ltd.
Managing Director **大野 修**

今年六月にプレスリリースで発表しました通り、IIJ Global Solutions Singaporeは、日系のクラウドベンダとして初めて、シンガポールのクラウドセキュリティ規格である「Multi-Tier Cloud Security（MTCS）Singapore Standard」の認証を取得しました。

MTCSは、シンガポールの情報通信開発庁の外郭団体が管理するクラウドセキュリティに関する公的な管理規格で、二〇一四年に世界に先駆けて認定制度が始まりました。本認定を取得することで、クラウド基盤上のデータの安全性・機密性や、クラウド基盤の運用面における透明性などが担保され、三年に一度の更新はあるものの、毎年一回は監査を受けることが義務付けられています。

ご存じの通り、シンガポールのクラウド市場は競争が加速しており、政府もクラウドの利用を積極的に推進しています。二〇一四年からクラウドサービスを開始しているIIJ Global Solutions Singaporeにとっては、他社との差別化を図り、日系のクラウドベンダとして現地企業を含む、より多くのお客さまにご利用いただくために、本規格の取得が不可欠であると考え、認証取得に向けた検討を開始しました。

しかし、検討を始めてすぐに、申請に必要なドキュメントの整備や、認証を取得するための運用体制を整えるリソースが不足していることが明らかになりました。さらに、ちょうど同じ時期にさまざまな案件が佳境を迎えていたこともあり、検討が一時中断することになりました。しかし、専任の担当者を新たに採用し、全社でMTCSの認証取得の必要性を再認識することで、マネージメント層、エンジニア、人事を含むバックオフィスなど、全部門を横断する体制を再構築し、二〇一五年三月に認証取得に向けたプロジェクトを再スタートさせました。

取得に際しては、合計二〇〇ページ・計六一種類におよぶ資料を準備し、社内一丸となって取り組みました。プロジェクトを開始した当初の目的は「ビジネスチャンスの拡大」でしたが、最終的にはMTCS取得に向けたさまざまな業務が「社内の情報セキュリティに関する大幅な意識の向上」につながり、それが結果的に「対外的な信用の向上」をもたらしてくれたと実感しています。●

IIJ Technical WEEK 2016のご案内

IIJグループでは11月9日～11日の3日間、技術者の方々を対象に「IIJ Technical WEEK 2016」を開催します。今年は、1日目「クラウド」、2日目「ネットワーク」、3日目「セキュリティ」をテーマに掲げ、全部で12のセッションを予定しております。皆さまのご参加を心よりお待ちしております。

開催概要
日　時　：2016年11月9日（水）～11日（金）　13:45～17:30（開場13:15）
会　場　：IIJグループ本社（東京都千代田区）
参 加 費：無料（事前登録制）
定　員　：160名（先着順）
締め切り：2016年11月8日（火）17:00

詳細・申し込みはこちらから　**http://www.iij.ad.jp/techweek/**

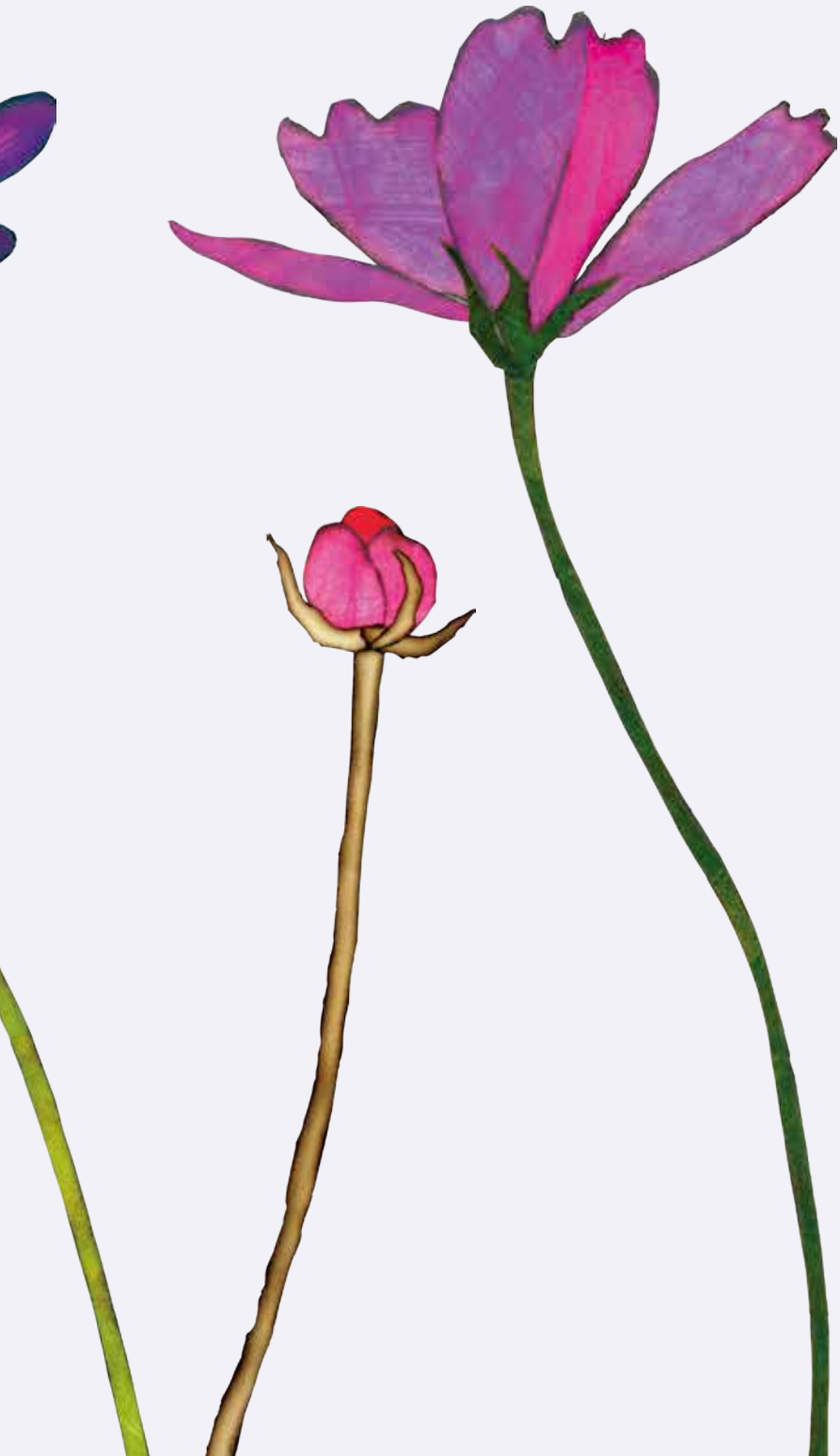
発行／株式会社インターネットイニシアティブ 広報部
お問い合わせ／株式会社インターネットイニシアティブ
広報部内「IIJ.news」編集室
〒102-0071 東京都千代田区富士見2-10-2
飯田橋グラン・ブルーム
TEL：03-5205-6310　E-mail：iijnews-info@iij.ad.jp

編集／増田倫子、村田茉莉
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

編集後記

巷で話題のスマホゲーム「ポケモンGO」、皆さんもやっていますか？　もう飽きてしまってやってないという人もいるようですが、私は毎日コツコツ続けています。最近は、コイキングというポケモンのアメを400個集め、ギャラドスに進化させました。ジム戦（ジムバトル）で大活躍しています。おかげで、やっと少し勝てるようになってきました。

さて今号は、読者アンケートの「過去一年間で印象に残ったテーマ」で1位になった「セキュリティ」を特集します。皆さまの期待に応えられる内容になっているか少し心配ですが、ぜひご一読いただき、感想などをお寄せください。（M）



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ニ号館 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 3F
〒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一条西 3-3 札幌 MN ビル 9F
〒060-0001　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

株式会社ハイホー
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：0120-858140

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

この冊子の内容はサービス形態・価格など予告なしに変更することがあります。（2016 年 10 月作成）

※ 表示価格には、消費税は含まれておりません。

※ 記載されている企業名あるいは製品名は、一般に各社の登録商標または商標です。

◎IIJ.newsのバックナンバーをご覧いただけます。URL: http://www.iij.ad.jp/iijnews/

◎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: http://www.iij.ad.jp/news/iijnews/wp/

IIJ
Internet Initiative Japan