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 2017
VOL. 140

特集 wizSafe
安全をあたりまえに

IIJ. news
June 2017
VOL.140

表紙の言葉「紫陽花」

紫陽花は、小さな花（実際は萼）が集まってこんもりとした花になっています。絵にするのは意外とむずかしく、小さな花を一途に追っても玉のような花にはならないし、全体像だけだと、小さな花をどこまで描くか悩みます。大きなイメージを捉えながらも簡略化して的確に表現することはむずかしい…。絵だけではなく、SNSなどで記事を書く際も同じ悩みがある気がします。

末房志野

ぷろろーぐ

仕事と私生活

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

「過重労働は絶対にさせない。私生活を犠牲にするような働き方は強要しない」。今年は、こんな言葉を前面に出した企業の人気が高かったと、就職・採用の専門家の話である。

私が就職したのは、高度成長の只中、ワーカホリックが当たり前の時代である。学生時代からアルバイトに精を出して、飲み代を捻出していたのだが、当時はアルバイトもワーカホリック並みの働き方だった。せめて就職くらいすべきだという批判に圧されて、卒業して時間を経た秋口になって、新聞の求人広告欄から採用試験を受けて、サラリーマンになった。その時の私の選定基準が、アルバイトを続けられる程度には時間に余裕のある組織がいいということで、友人に相談したら、社団法人ならギリギリまで働かせられたりしないだろうと勧められて、働き始めた。しかし当時は「社団法人なら」という時代ではなく、帰宅も終電車ということが多かった。

勤め始めて二年ほどは、アルバイト収入に頼っていた時のほうが実入りも多かった。勤め人になっても、残業の請求が面倒であまりしなかった。なにより、仕事をこなすことに精いっぱいで、仕事面で組織に貢献している気がしなかった。給与を貰いながら勉強しているようなものだと自嘲していたのである。アルバイト時代に借りていた部屋の家賃が、就職後の給与と釣り合わず、家賃を払うと、給与の半分が消えてしまうといった無茶な生活だった。

勤め人になっても、アルバイトによる生活費の補給を心がけていたのだが、昼で終わる土曜日から日曜日にかけての自分の時間も、土曜日の午後は先輩に麻雀などに誘われ、帰宅時間も深夜になることが多かった。その分、日曜日は早朝から夜中まで翻訳の下請け等々のバイトに追われ、徹夜に近い過ごし方をした。週明けの月曜日から、寝不足と疲労でぐったりしながらオフィスに出る羽目になる。そんな生活がずいぶん長く続いた。しかも野球をやっていたことが知られ、日曜日には野球の試合に駆り出されることも多かった。私生活を云々する以前の日々だった。それが苦痛だったかと言えば、そうでもなかった。

仕事に没頭せざるを得ないうちに、仕事にはどんな遊びよりも惹きつけられるものがあって、自ら進んでワーカホリックの仲間入りをしてしまったようだ。集団生活が苦手で、高校から大学と、徹底して授業をさぼり続けたのだが、なぜか社会人になったあとは、人が変わったようになったのだから不思議なものである。与えられた仕事の内容が必ずしも面白かったからではなく、鍛えられているうちに小さなことでも面白くなってしまったのである。

IIJという会社も二五年になる。創業期は給与も払えないような状況が続いたのだが、当時からガランとしたオフィスに泊まり込んでは仕事を続ける社員が多かった。商用のインターネット接続サービスが認可され、堰を切ったように会社は成長をするのだが、その頃は、終電前に帰宅する社員はほとんどいなかった。飲みながらの長い夜飯を食べたあと、オフィスには戻らないで家に帰ったほうがいいと言うのだが、四六時中、エンジニア同士、議論をしていないと気が休まらなかったのだろう。私生活と労働の境がまったくなかったようだ。

IIJが残業制度を導入したのは、創業してからずいぶんと時を経てからである。導入に際しては、ほとんどのエンジニアが反対したようだ。家の環境よりもオフィスの環境がいいのに、残業制度が導入されると、残業代がついてくるから、オフィスにいられなくなるというのが反対の理由だったらしい。残業をしていることが、管理されているようで嫌だというのもあったのだろう。仕事と私生活というのも、そうそう明確な仕切りがあるわけでもないと思うのだが、そんな風に境界をつくってしまうのが、今風なのかも知れない。●

イラスト／末房志野

Topics

wizSafe
安全をあたりまえに

IIJでは、セキュリティ事業の拡充・刷新を目指し、新ブランドを立ち上げた。
今回の特集では、厳しさを増すサイバーセキュリティの現状を見ながら
セキュリティ対策を統括する組織や人材育成のあり方など
幅広い視点から安全で安心なICT環境について考えてみたい。

特集イラスト／STOMACHACHE.

セキュリティ事業 wizSafe 始動

IIJが立ち上げた、新しいセキュリティブランド「wizSafe（ウィズセーフ）」。
ここではその概要を解説する。

IIJ セキュリティ本部長
齋藤 衛

wizSafe
安全をあたりまえに

IIJは老舗の商用インターネットサービスプロバイダであるだけでなく、セキュリティの事業領域においても一九九四年からファイアウォール事業などを展開してきた、国内最古参のひとつです。また、その事業が二〇年以上にわたり順調に拡大していることから、お客さまに認められ続けてきたセキュリティ事業者であったと考えています。

しかしながら、昨今のサイバーセキュリティの領域では、標的型攻撃、ランサムウェア、IoTボットの台頭など、より高度で大規模な事案が発生していることに加え、ICT技術の適用分野も広がっています。こうした状況のもと、IIJにおいてもインシデントに組織横断的な対応が求められたり、大量の情報を網羅的に分析する必要のある状況が増えてきており、従来の事業のやり方では力不足と言わざるを得ない場面が見られるようになってきました。

そこでIIJでは、二〇一六年度からセキュリティ事業のさまざまな点での増強を実施し、いくつかの成果をあげてきました。ここではこの新しいセキュリティ事業について説明します。

ひとつのセキュリティ組織と新しい事業ブランド

まずセキュリティ本部をつくり、セキュリティ機能を提供する部門を全てこの本部一ヵ所に集めました。これまではセキュリティ機能が、SI、サービス、研究開発など複数の部署にまたがって存在していたため、組織的に風通しが良くなかったという反省がありました。そこで、新しい事業の推進と、お客さまのために緊密に連携していくうえで、組織的な基盤となる本部をつくり、お客さま対応の速度や品質の向上を目指しました。

そして、従来はサービス毎にバラバラに行なわれていたブランディングをこの本部のもとに集約し、新しい事業ブランド「wizSafe」を立ち上げました。wizSafeとは、Wizard（熟練した職人）、Wisdom（その英知）、With（お客さまとともに）と、Safe（安全）を組み合わせた造語で、IIJのセキュリティエンジニアがその知識と経験を駆使することで、お客さまとともに安全なICT環境を構築していく状態を表現しています。

セキュリティの〝S〟を基調としたブランドロゴには「安全をあたりまえに」という文言を添え、IIJのセキュリティ事業が目指す将来像を示しています。今後、全てのセキュリティ事業はこのブランドのもとに展開していきます。

wizSafeの立ち上げに際して、お客さまにより良いセキュリティ機能を提供するための三つの柱として「人材、システム、設備」について、それぞれ拡充を行ない

ました。

人材面では、今後、セキュリティ事業に携わるうえで必要な専門性の高い技能を有する人材を育成する仕組みを、システム面では、セキュリティ専門家が分析に要する情報を扱い易くするためのシステムである情報分析基盤を、設備面では、より高度な分析をより安全な環境で行なえるようにすると同時に、プレゼンスの向上も目的としたオペレーションセンター設備を、それぞれ構築しました。以下では、これら三つの柱について詳細をご紹介します。

セキュリティ人材の育成

IIJでは、特にセキュリティ分野において、FIRST（Forum of Incident Response and Security Teams）など外部で教育プログラムや演習を提供するようなエンジニアが多数いる一方、社内では「背中を見せて育てる」といった先輩が多く、若手に系統だった知見を与えるような人材育成にはあまり力を注いできませんでした。

また今日、東京オリンピックのようにサイバー攻撃の対象となり得る大きなイベントを控え、セキュリティを専門とする人材の不足が叫ばれるなか、IIJのセキュリティ事業に適切な技能を有する人材を外部から見つけることが困難な状況となっています。そこで、社内のエンジニアにより高度なセキュリティ専門技能を習得してもらうことを目的とした人材育成コースを設定し、この人材育成を中心にセキュリティ事業の量的・質的な拡充に対応することにしました。

人材育成コースでは、まずセキュリティ事業に関わるうえで必要となるスキルセットを定義し、それぞれについて習得レベルを設定して、一人ひとりが現在どのような技能を習得済みで、どのような位置にいるのかを一目でわかるようにしています。また、実際のマルウェア検体などを教材とした演習を通し、覚えた知識を技能として定着させます。加えて、技能を持った先輩から一方的に教えてもらうだけでなく、輪講形式などで学習をリードする立場を経験することで、他人に教える練習も一緒に行なっています。

情報分析基盤

IIJでは従来からセキュリティインシデントの全容を把握したり、反対に、個別インシデントの詳細を突きとめる分析を行なうためのプラットフォームを保有していました。しかし、インシデントの大規模化・複雑化が進むにつれ、ひとつのインシデントの大局的な情報を検討するために複数のシステムを扱わなければならなかったり、単純に情報量が増えたことで複雑な分析に多くの時間を要するケースが出てくるなど、徐々に使い勝手が悪くなっていました。

そこで今回、大局的な判断を瞬時に下せるように、全ての情報を一手に取り扱うことができるシステムとして情報分析基盤を構築しました。ファイアウォールやIPS、アンチウイルスやサンドボックス、多くの装置から発生するログやアラートに加え、メールやWEBのセキュリティサービスの情報、DDoS攻撃対策サービスの情報などを、ひとつの基盤で扱えるようになっています。

さらに、この情報分析基盤はセキュリティ事業のログやアラートだけでなく、通信に関わる情報を扱うことを想定した容量と処理能力を備えた設計になっています。このシステムは、いわゆるビッグデータ分析を行なうプラットフォームとしてはもちろんのこと、さまざまな数理モデルや機械学習モデルによる判断にも対応しています。

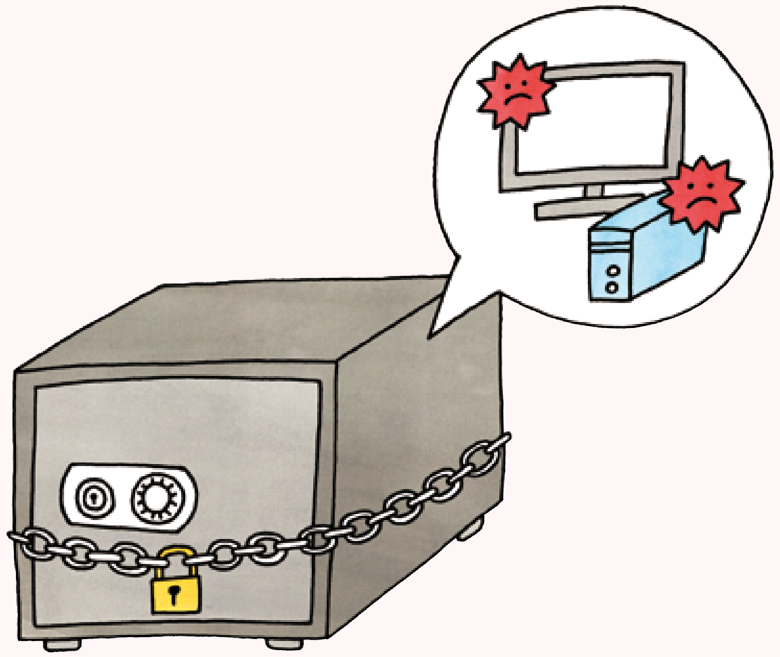
情報分析基盤は、一義的には攻撃に関連する情報を集約し、IPアドレスやURLに関するレピュテーションのかたちで取りまとめます。そして、このレピュテーションを各種セキュリティ事業に還元することで、セキュリティ事業全体として協調的に動作できるようになります。また、レピュテーション情報をインシデント毎に整理したり、時系列で分析したりすることで、傾向を把握し、将来の対応指針に役立てる情報を生み出すことも可能です。さらに、お客さま毎のSIEM（Security Information and Event Management）などとの連携や、セキュリティ・オペレーションセンター内で掲示される大局情報をまとめたり、個別事案に関する人の判断を補助するための情報を提示したりする機能も有しています。

セキュリティ・オペレーションセンター

セキュリティ事業に関する情報は、これまでもオフィスネットワークから分離された環境で慎重に取り扱っていました。また、マルウェア解析やデジタルフォレンジックなど、より危険だったり機密性が高かったりする情報を扱うときには、個別に施錠管理できる場を用意してきました。

しかし、セキュリティ・オペレーション事業の拡大や、解析作業に対する需要の増加などから、これらの仕事に当たるためには、通常のオフィス環境とはネットワーク的にも物理的にも分離された、専用の部屋を用意する必要が生じました。

今回新設したオペレーションルームは、通常の居室から生体情報とICカードによる認証を経たうえでないと入室できず、その様子はカメラで常時監視されています。机椅子などを含む什器は、オペレーションに関わる一人ひとりが集中して技能を発揮できるよう、周りと目線が絡まない高さの仕切りを設置する一方、大規模インシデント対応のときなどは、少し顔をあげたり立ちあがったりすれば、周りの人と協調して対応に当たることができるようになっています。また、セキュリティ・オペレーションを行なう場と、解析作業を行なう場のあいだにもセキュリティの物理的境界を設け、証拠保管用の金庫を常設するなど、より安全に情報を扱える設備を配備しています。



さらに、従来はお客さまからの見学のご要望は全てお断りしていたのですが、実際のオペレーションの様子をご覧いただき、納得のうえご利用いただくことも必要であるとの判断から、この新しいセキュリティ・オペレーションセンターには、見学用の部屋も併設してあります。

セキュリティ事業の展開

これらの人材と設備を駆使して、二〇一六年度には、従来は個別に実現していたSIEMの構築をサービス化したC-SOCサービス、1Tbps規模のDDoS攻撃にも対応可能なDDoSプロテクションサービスの広帯域品目、仮想化によりWEBの分離環境を提供するIIJセキュアWebゲートウェイサービス セキュアブラウジングオプションなどをリリースしました。

今回のセキュリティ事業の強化によって、より精度の高い状況把握、対応時間の向上などを実現しましたので、今後はさらに複雑な事案にも効果的に対応できる高度なセキュリティ機能をお客さまにお届けしたいと考えています。

さらには、インターネット接続、クラウド、モバイルといった事業分野においても、セキュリティの維持機能を、それぞれの基本的な機能として展開する準備を進めています。

「安全をあたりまえに」という言葉には、ICT環境にセキュリティ機能が適切に追加される状況だけでなく、ICTの基本機能としてセキュリティ機能が自ずと含まれている状況を目指すという意味もあるのです。●

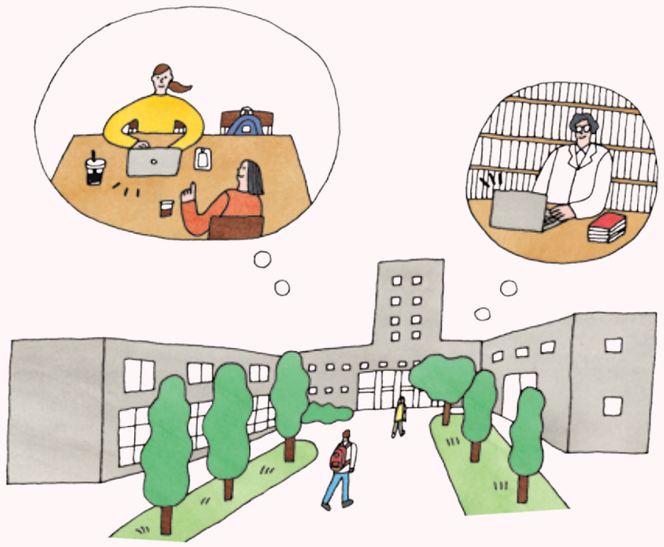
特別対談

セキュリティを支える組織と人材

円滑なセキュリティ・オペレーションを実践するには、何が必要なのか？
本対談では、これからの時代に沿ったサイバーセキュリティのあり方について、
ふたつのセキュリティ・オペレーション組織の比較などをもとに検討してみたい。

国立情報学研究所
サイバーセキュリティ研究開発センター センター長
アーキテクチャ科学研究系 教授
高倉 弘喜氏

IIJセキュリティ本部長
齋藤 衛



NII-SOCSの役割

齋藤 IIJはセキュリティ・オペレーション事業を長年行なってきました。そしてこのたび、SOC、人材、システムを拡充し、新しいSOCが昨年度末に開所しました。

今回は、国立情報学研究所の高倉弘喜先生にセキュリティに関わる組織や人材育成のお話をうかがいたいと思います。まず、国立情報学研究所の概要をご紹介ください。

高倉 国立情報学研究所（以下、NII）は「情報」をめぐるさまざまなことを研究する組織です。もともとは活字や書籍を対象としていましたが、それらを電子化する過程でネットワークの研究を開始し、その後、各大学にあるスーパーコンピュータをつなぐためのネットワークを構築しました。それが国立大学や研究機関を結ぶ学術情報ネットワーク「SINET」に発展したわけですが、SINETをクラウドとつなぐ構想が立ち上がった際、問題になったのがセキュリティ対策でした。当初は、重要なデータが集まるクラウドとの接続部分のみを守るということだったのですが、徐々に守備範囲が広がり、ネットワーク全般を見るようになりました。

そして現在、セキュリティ対策の強化や人材育成を推進する「NII-SOCS」の正式運用に向けた準備を進めています。「SOCS」とはSecurity Operation Collaboration Servicesの略です。

齋藤 セキュリティ・オペレーション・センター（Center）ではないのですね。

高倉 大学と連携（Collaboration）してセキュリティ・オペレーションのサポート・サービス（Service）を提供するという主旨です。

齋藤 各大学のセキュリティ・オペレーションに関するアクティビティは、どのような状況ですか？

高倉 大学によってまちまちです。そこで、CSIRTのような組織を各大学で運用してもらうためのトレーニングを行なう組織としてNII-SOCSが発足しました。

これまでは大学でセキュリティ・オペレーションをやろうとしても人材が不足していたり、センサを購入する資金や使いこなすノウハウもなかったりするなど問題が山積していたので、機器の購入や一次監視はNIIがやることにしました。そして何か異常を発見したら、NIIが大学に連絡を入れ、そのあとの解析や原因究明は共同で行なうことになっています。

現状、NOC（Network Operations Center）に相当する組織はどこの大学にもあり、NOCを監督できる人材もいるので、そういう人にセキュリティ・オペレーションについて学んでもらっている段階です。

ただ、大学の場合、対応する部署、学部や教職員などさまざまな内情に精通していないと事が進まない。国立大学には附属病院を持つところもありますが、それらと話ができ、なおかつセキュリティもわかっていないと務まりません。よって、学生や外部の事業者に任せるわけにもいかず、まずはその人材を育成しているのです。

齋藤 各大学にいるITエンジニアにセキュリティに関する技能を習得してもらうということなら、きちんとした人材が育つでしょうね。

高倉 最低でもトラフィックを見ることができ、不審な挙動に気がつく人間を各大学に一、二名は置きたい。これを五年以内に達成したいと考えています。さらには、データから読み取った情報を咀嚼して、大学の上層部や監督官庁に報告できる管理者の育成を目指しています。

齋藤 NII-SOCSの規模はどれくらいですか？

高倉 オペレーションをやっているのは一〇名程度で、夜間は二名体制です。それで約八〇の国立大学を見ています。

一般的なSOCと異なる点は、拡散したボットがゾンビ化してノイズのようなアラートを発していますが、そのように常態化したものは相手にしません。NII-SOCSは、新たな攻撃手法で対応が間に合っていない恐れのあるものや、アラートが出たあとのセッションをチェックして大量通信を確認したものについて、OSのバージョン情報などとも照合しながら被害状況を想定して、ある程度の確証を得たうえで大学に通知します。単にアラートが出たから通知するのではなく、根拠をともなった報告を出すことで、大学側に速やかな対応を促すようにしています。

大学では、学外でマルウェアに感染したPCが学内に持ち込まれるケースが多い。そういうときは、感染フェーズから確認されているマシンの挙動と照合して、「このマルウェアを踏んだ可能性があるから調べてほしい」と伝えます。因果関係込みで通知すればアクションも起こしやすいのです。

全国の国立大学を見ていると、共通して起こっている事象が掴める一方、特定の大学・学部・部門の知財を狙ったマルウェアが見つかることもあります。

ただし、メールの「from」や「to」といった個人情報は暗号をかけて、原則として見られないようにしています。

齋藤 暗号を解くプロセスはどうなっているのですか？

高倉 共通鍵で暗号化して、その共通鍵を大学の公開鍵で閉じています。暗号を解く際は、大学がアップロードしてくれた鍵でデータを戻します。もちろん、データや鍵はDRAM上でしか展開しません。NIIのような組織が（学生など）〝民〟のトラフィックを見るのは通信の傍受と受け取られる恐れがあるので、そこは慎重にやっていまして、担当理事や学長の承諾を得るようにしています。

齋藤 どの情報を解こうとしているのかは、大学に伝わっているのですか？

高倉 WEBUIが共通なので、我々が見ている情報は大学も把握しています。

セキュリティ・エンジニアの育成

齋藤 人材育成で苦労している点はありますか？

高倉 NOCの人はネットワークに関する知識があるので、飲み込みは早いですよ。一度、東京に来て講習を受けてもらい、その後は必要に応じてオンラインでやり取りしています。我々がアイデアを出せば、彼らは過去のインシデント対応の経験などをもとに、自分なりのやり方を見つけてくれるので〝オン・ザ・ジョブ〟で学んでもらっています。

今回、もうひとつ取り組んでいるのは、NIIが学術研究機関であることを活かして、トレーニング用のデータをつくることです。一番わかりやすいのはマル

齋藤 衛（さいとう まもる）

写真／渡邊 茂樹

高倉 弘喜（たかくら ひろき）
平成２年、九州大学卒業。平成４年、同大学大学院修士課程修了。平成７年、京都大学大学院博士後期課程修了。博士（工学）。奈良先端科学技術大学院大学助手、京都大学講師・准教授、名古屋大学教授を経て、平成27年、国立情報学研究所教授。平成28年、同サイバーセキュリティ研究開発センター センター長。大規模ネットワークや制御ネットワークにおけるセキュリティ対策などの研究に従事。

ウェアで、監視で得られたデータのなかから公開可能なものを匿名化して、無償で配布します。セキュリティ研究では、当然、鮮度の高いデータを用いたほうが効果的ですが、現状なかなかむずかしい。それなら我々がデータを提供したらどうかということで準備を進めています。

齋藤　人材育成の完成形は、どのあたりを目指しているのでしょうか？

高倉　一〇年二〇年後、このトレーニングを受けた人が役職者になって、大学のマネージメントに関わってほしい。そして、セキュリティがわかる理事や役員として「セキュリティにはこのくらいの予算が必要です」と言えるようなコスト感を身に付けてもらいたいです。

齋藤　コスト感は大切ですね。

　我々が提供しているセキュリティ・サービスは、ともすればお客さまに合わせることを優先しがちで、「教育」と言うとおこがましいですが、互いに学び・育っていくという考え方は希薄だったので、今のお話はとても参考になりました。

高倉　我々もSOC事業者さんの声をいろいろ聞いて、「これは（教育を）やらないとダメだな」ということで始めましたからね。大学としては「今日も安全です」と言ってもらえるのが理想ですが、そうでない事態が発生したとき、適切な対処を決断できる人材が少ないことが最大の課題です。また、話ができるエンジニアも不足しているので、何かあったときに上層部への報告がきちんとなされないと、連鎖的なパニックを引き起こす危険性があります。

　さらに、緊急時は「この案件にどのくらいのリソースを割くべきか」という判断が求められ、今起きている事象と今後起こり得る事象を想定して、適材適所にリソースを配分する、つまり戦略を立てられる人材が必要です。そうでないと、インシデントが起こるたびに関係者が疲弊してしまう。今のままでは、セキュリティを学んだ学生が「セキュリティの仕事は大変だから……」と言って、他の分野に流れて行ってしまう（笑）。

齋藤　セキュリティに携わる人材を育てなければならないという話はよく出てきますが、個人的には「二万人のセキュリティ・エンジニアを育てるより、一〇〇万人のITエンジニアがセキュリティに関するアウェアネスを持つ」ほうが、総体的な底上げにつながるのではないか、と考えています。

高倉　そういう人が各分野に散っているのが理想型ですね。

IoT／AI時代のセキュリティ

齋藤　IoTデバイスが増えていますが、何か対応はされていますか？

高倉　大学間や国際的な共同研究が頻繁に行なわれており、実験機器など多くのIoTデバイスがネットワークにつながっています。我々からすると、ネットワークはVPNを組んでいるのが当然ですが、そうでないところも多く、たいていはポート80が空いているので、そこを叩かれてしまう。

　また、検索エンジンShodanのスキャナ情報をもとにセッションを抽出すると、どのポートが狙われているのかわかる。例えば、あるデバイスの特定のポートめがけてスキャンがかけられる。ポートスキャンがかかると攻撃の前兆だと言われたりしますが、実際に攻撃してくるときは、もう一度ピン・ポイントのレーダー照射が始まり、「いよいよ撃ってくるぞ」となります。

齋藤　特定の実装・インタフェースを狙ってくるわけですね。

高倉　こうしたケースは年に数回ですが、兆候が現れると、大学に「このポートにスキャンがかかっているけど、把握していますか？」と連絡を入れます。

齋藤　そこまでケアしないと、IoTデバイスのセキュリティは守れないのでしょうか？

高倉　とにかくIoTデバイスの直付けは避けるべきです。アップデートも頻繁ではないし、サポート期間も限られているので、できる限り閉じたネットワークを組んでほしい。

齋藤　将来的には、AIの活用なども視野に入っていますか？

高倉　大きな攻撃が来たときの状況分析や被害予測はAIの得意とするところです。また、対応のサジェスチョンなどもAIが示してくれるようになるでしょう。つまり、人間をサポートする役割をAIが担い、最終的な決断は人間が下すという使い方が、これからしばらく続くと思います。イメージとしては『スター・ウォーズ』のR2-D2ですね（笑）。

　ひとつ悩ましいのは、本当にかしこいAIが出てきたら、有利になるのは攻撃者のほうだということです。実際、攻撃者はすでにAIを使っています。

齋藤　マシン・ラーニングを活用すれば、人間が一度やったことは反復できるようになるので、人材不足を補ってくれるツールにはなってくれるでしょうね。

高倉　今、SOCの一番下のレイヤでやっているような作業は、いずれAIに取って代わられるし、休日や夜間に何か起きたときの〝仮止め〟みたいな措置はAIでもできるようになるでしょう。

　インシデントが起こると人間はパニックに陥って、一分一秒の判断を迫られたら、しばしば間違ってしまう。そんな状況でAIが暫定的に食い止めておいてくれたら、人間が正確な対応を考えるための時間を捻出できます。

SOC間連携の可能性

齋藤　SOC間連携などは検討されていますか？

高倉　複数のセキュリティ団体がありますが、情報のシェアリングはあまり進んでいません。「自分たちの情報は出したくないが、相手の情報は知りたい」というのが本心かもしれません。

齋藤　失敗談をシェアすることは重要ですよね。関係者が集まると、共通の敵に対する話題では盛り上がるのですが、「自分のところだけかもしれない」と思った瞬間、口を噤んでしまう……。

高倉　我々は、まず各大学が持っている情報を集めて、それを他の大学とシェアするようにしています。もちろん大学名は伏せますし、事前に承諾もとります。自主的に情報をあげるとなるとまだハードルが高いのですが、匿名化した情報を共有するぶんには、たいていの大学は許可してくれます。

齋藤　NII-SOCSは、他のSOCと連携したりしていますか？

高倉　海外のSOCなどと情報のシェアリングを進めています。

齋藤　それは対等な立場で行なっているのですか？

高倉　そうです。

齋藤　我々は個々のお客さまにSOC機能をサービスとして提供していますが、次の段階として各SOCを連携させることで、さらなるアドバンテージが生み出せないか考えています。

　その際、対等な関係で情報交換を行なうだけでなく、ツリーをつくって、例えば「××のトラフィックを止めてほしい」といったオーダも付けるようにできれば、より動きやすくなると思うのですが。

高倉　政府や行政主導でそれを進めて、角度の高い情報をもとに、早急に動ける仕組みをつくるべきかもしれませんね。米国のISACなどは、すでにそうなっています。

齋藤　東京オリンピックのような大きなイベントを成功させるという目標があれば、ビジネスの競合関係を乗り越えて協調できると思うので、そうした機会を活かしたいですね。

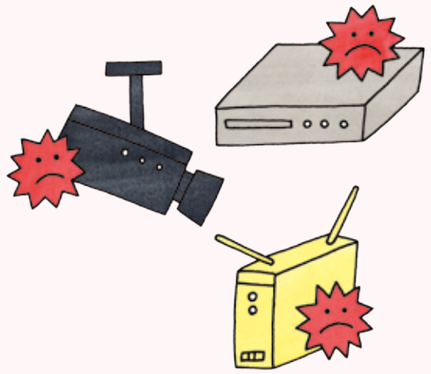
高倉　オリンピックのセキュリティ対策といった喫緊の案件に関しては、時間も人的リソースも限られているので、SOC間連携を進めながら、ワン・ユニット化していくのが現実的な対応策だと思います。

齋藤　おっしゃる通りですね。今日は多くのイメージを共有でき、大変有意義でした。ありがとうございました。●

IoTボットネットからのDDoS攻撃

DDoS攻撃の脅威が続くなか、IoT機器を狙ったボットネットからの攻撃が増加している。本稿では、その現状と対策に関する注意点をまとめる。

IIJ セキュリティ本部
セキュリティ情報統括室
根岸 征史



個人や企業を狙ったサイバー攻撃は日々変化しています。本稿ではDDoS攻撃（分散サービス妨害攻撃）の最近の動向について概観します。

DDoS攻撃とは、インターネット上に分散した多数の機器から同時に攻撃対象のシステムに接続を試みて、他からの正常な接続を妨害することを目的としたサイバー攻撃です。攻撃の動機はさまざまで、サービス停止による営利機会の損失や信用の失墜を狙ったり、個人的な怨恨による攻撃や、政治的な主張を行なうために攻撃することもあります。また、国家間の摩擦や紛争などがきっかけとなり、インターネット上で互いに相手国のシステムを攻撃し合うといった事例も見られます。

リフレクション攻撃

こうした攻撃自体は二〇年以上前から観測されていますが、近年は攻撃の規模や回数が増加する傾向にあり、攻撃手法にも変化が見られます。例えば、二、三年前まではリフレクション攻撃（あるいは「アンプ攻撃」とも言う）という手法が主流でした。これはインターネット上にある不適切な設定の機器を踏み台とした攻撃のひとつで、送信元を攻撃対象に偽装したUDPパケットを踏み台に送信すると、より大きなサイズのパケットが返ってくることを利用して攻撃規模を増幅させ、さらに攻撃の発信元を隠蔽するという狙いもあります。

二〇一三年には非営利のスパム対策組織Spamhausに対してこの攻撃手法が用いられ、当時としては最大規模の300Gbpsを超えるトラフィックが発生し、大きな話題となりました。また、こうしたリフレクション攻撃を安価かつ手軽に実行できるDDoS攻撃の代行サービス（booterやstresserなどと呼ばれる）が大量に生まれたことも、この攻撃が増加した一因に挙げられます。

DNSやNTPなどのプロトコルが狙われやすく、以前から対策は進められているものの、世界中に分散した多数の機器が対象であることや、一般家庭に設置されたホームルータに脆弱性があることなど、そもそも利用者が脆弱性に気付いていないケースも多く、いまだ解決には至っていません。

ボットネットからの攻撃

最近の攻撃傾向としては、相変わらずリフレクション攻撃が多く観測されていることに加え、ボットネットを発信源とする大規模な攻撃が観測されています。ボットネットは、多数の機器を「ボット」と呼ばれるマルウェアに感染させ、それらを遠隔から攻撃者がコントロールするものです。DDoS攻撃だけでなく、スパムメールの送信などにも利用され、感染規模も数千台から数万台を超えるものまでさまざまです。

今、特に多いのはIoT機器であるIPカメラ、デジタルビデオレコーダ、ホームルータなどを感染対象としたボットネットです。これらの機器にはLinux系のOSが組み込まれているものが多く、インターネットに接続されるこうした機器の増加にともない、不適切な設定のために外部からの侵入を容易に許す脆弱性を持つものが増えています。

IoT機器ではtelnet（23／tcp）やhttp（80／tcp）などのポートが管理用に使われており、デフォルトのアカウント（その多くで脆弱なパスワードが設定されている）を利用してログインできるようになっています。そのため、攻撃者にも侵入経路として利用されやすく、格好のターゲットになっています。二〇一四年頃からこうしたIoT機器を狙ったとみられるtelnetポートへのスキャン活動が急増し、インターネット上で広く観測されています。IIJのハニーポットにおける最近の観測でも、telnetポート宛の通信が他を引き離して多数を占めています。

IoTボットネットによる攻撃事例としては、二〇一六年八月、リオ五輪の開催期間中にブラジルで540Gbpsの攻撃トラフィックが観測され、同年九月には米国の著名なブログに対して623Gbpsの攻撃トラフィックが観測されました。他にも同じ時期に1Tbpsを超える攻撃が観測されたとの報告もあり、攻撃トラフィックの規模は著しく増大しています。

九月の攻撃はmiraiと呼ばれるボットネットが発生させたと考えられていますが、同月末にこのボットのソースコードが作者によって公開され、それを改変したと見られる亜種がその後大量に発生しました。感染手法自体はとても簡単なので、mirai以外にもさまざまな種類のIoTボットネットが見つかっており、今後もこの傾向はしばらく続くと見られています。IoT機器ベンダも対策を進めてはいますが、先ほどのリフレクション攻撃と同様に、解決までにはまだ相当の時間がかかりそうです。

攻撃に関する注意点

攻撃規模について注意しておきたいのは、最大規模の攻撃トラフィックはたしかに年々増加しており、1Tbpsに届く勢いですが、その一方で頻繁に発生する回数の多い攻撃はそこまで大規模ではなく、1Gbps未満のものが大半を占めています。そしてこの傾向はそれほど変わっていません。ただ、攻撃規模は小さいものの、httpやhttpsといった特定のプロトコルを利用してサービスを効率よく停止に追い込む、アプリケーション層への攻撃が発生しています。よって、攻撃規模にばかり目を向けるのではなく、攻撃が発生した場合の自サイトへの影響の有無という観点からも攻撃傾向を分析することが大切です。

では、DDoS攻撃を受ける側の対策はどうすればいいのでしょうか？　DDoS攻撃を防ぐ目的は、サイト利用者にサービスを提供し続ける「可用性」を維持することです。そのためには、攻撃トラフィックと正常なトラフィックを判別して、攻撃のみをブロックしなければなりません。それには、こうした処理を専用に行なうアプライアンスを自サイトに設置したり、クラウド上で提供されるDDoS攻撃対策サービスを利用するといった対策が考えられ、通信回線を提供しているキャリア網内でそうした対応が可能な場合もあります。

また、攻撃を防ぐという直接的な対応とは異なりますが、万が一、自サイトが攻撃を受けてユーザが利用できなくなった際は、ユーザにその事態を伝える手段をあらかじめ考慮しておくことをお勧めします。これには、別に用意したサイト上でサービスの状況を伝えたり、公式のSNSアカウントから通知するといった方法が考えられます。いずれにせよ、こうした対応は攻撃が発生してから検討していたのでは間に合わないので、想定される攻撃と自組織の状況を正確に把握し、とり得る対策の選択肢を検討し準備しておくことが肝心です。

今やDDoS攻撃は、いつ・どこで発生してもおかしくない、とても身近な脅威になっています。攻撃が発生しても慌てることなく対応できるように、ぜひ事前の備えに取り組んでいただきたいと思います。●

IIJ SOCリポート

IIJは、セキュリティ事業の中枢を担う「IIJ SOC」を刷新した。
ここではその全貌を紹介する。

IIJ セキュリティ本部 セキュリティビジネス推進部
セキュリティオペレーションセンター長
野間 祐介

「SOC(Security Operation Center)」とは、セキュリティ機器やネットワーク機器から得られるログを二四時間三六五日、監視・分析し、脅威となる事象の発見・特定・通知を行なう組織です。

ひと昔前のサイバー攻撃は、主に企業が管理するサーバを対象としていましたが、最近では社員が利用するPC、タブレット、スマートフォンなどの端末にまで拡大してきました。このように守るべき範囲が拡大する一方、攻撃手法も高度化・複雑化しており、従来のセキュリティ機器による対策だけでは防御しづらくなっています。こうした要因から、SOCの重要性がますます高まっているのです。

しかし、SOC構築は想像以上に困難です。運用・監視を行なう設備構築の他に、日々の運用・監視業務で蓄積されるログや、日まぐるしく変化し続ける脅威情報の収集・分析を継続的に行なうには、多額の設備投資に加え、スキルとノウハウを持った人材確保が不可欠です。これら全てを整えるには大変な労力が必要であり、自組織でSOCを構築・維持するのは非常にむずかしいと言えます。

刷新したIIJ SOC

IIJではこのような状況を踏まえ、IIJ SOCの刷新を実施しました。IIJ SOCでは、独自のセキュリティインテリジェンス*1を活用することで、発見が困難とされる脅威にも対応できるようになりました。この独自のセキュリティインテリジェンスは、ISPとして保持するバックボーントラフィックやDNS情報、お客さまに提供しているファイアウォール、IPS、メール、WEBといった各種サービスの膨大なログやイベント情報を、自社で構築した情報分析基盤へ集約し、ビッグデータ解析して、生成しています。

IIJ SOCの設備は、攻撃検知・通知・対処を行なう「オペレーションルーム」と、未知のマルウェア解析やフォレンジック調査*2など、セキュリティリスクの高い情報を扱う「セキュリティラボ」から構成されています（写真参照）。

IIJ SOCの再設計にあたっては、一九九四年に日本で初めてのファイアウォールサービスを開始して以来、二〇数年にわたり培ってきたセキュリティ事業のノウハウをベースとしながら、膨大な情報から迅速かつ正確にリスクを検知し対処するための業務を安定的に行なえるよう随所に工夫を施しました。

例えば、IIJ SOCには、従来のSOCのような（地球防衛軍の作戦司令室

をイメージさせる）一〇〇インチ超の大型モニタは設置していません。大きなモニタは（見学に来たお客さまの目を引くことはできますが）普段は使わないケースが多いので、オペレーション業務に必要でないものは極力排除して、担当者が重要な情報を適切に把握できるレイアウトが望ましいと考えました。

IIJ SOCの取り組み

さまざまな情報分析において重要な役割を果たしているのが、先に挙げた情報分析基盤です。豊富な知識とノウハウを備えたセキュリティエンジニアが情報分析基盤を活用して、ファイアウォールなどのセキュリティ機器単体では発見することが困難なインシデントを早期に発見し、脅威への速やかな対応を実現しています。さらに、独自に収集した脆弱性情報を参照しながら、お客さまへの統計情報の提供やセキュリティ対策の提案なども行なっています。

二〇一七年に入り「Apache Struts 2」の脆弱性を悪用した攻撃が多発していますが、IIJでは情報分析基盤を活用した独自のログ解析を行ない、攻撃手法をパターン化したうえで、インシデントへの対処を実施しました。攻撃のなかには難読化されているものも複数あるため、一般的な防御だけではすり抜けてしまうこともあります。IIJでは攻撃手法を適確にパターン化して対処を施すことで、攻撃がすり抜けるリスクを最小化しています。

またIIJ SOCでは、先に述べた監視やインシデント対処以外にも、独自に取得したマルウェア解析やフォレンジック調査も行なっています。

マルウェア解析では、IIJが運用するハニーポット*3やWEBクローラ*4による巡回で発見したマルウェアに対し、動的解析と静的解析を組み合わせた分析を行なっており、そこで得られた結果をもとに、検知・防御の手法を検討し、お客さまへの対策実施などに活用しています。フォレンジック調査では、実際に感染してしまったお客さまのハードウェアをお預かりし、調査・解析を行ない、感染の原因究明や事後対策の提言などを行なっています。こうしたマルウェアの取り扱いやお客さまの大切な情報を含むリスクの高い作業は、より高いレベルのセキュリティが施された専用スペースであるセキュリティラボで行なっています。

オペレーションルーム

セキュリティラボ

今後の展望

IIJでは、ますます高度化・複雑化する脅威に対抗するために、設備や基盤を拡充すると同時に、情報分析基盤上で得られる独自のセキュリティインテリジェンスの活用をさらに進めていく予定です。今後は、蓄積されたセキュリティインテリジェンスとIIJ SOCの経験やノウハウをIIJが展開する他のサービスと連携させることで、より多くのお客さまに安全なインターネット環境を提供していきたいと考えています。●

*1 さまざまなシステムやデバイスから生まれる大量のデータをリアルタイムに収集・分析することで得られる、セキュリティ上の脅威を未然に防ぐための対策を講じる際に有益な情報。
*2 情報漏えいや不正アクセスなどが起きた際に、機器本体に記録されたデータの証拠保全および調査・分析。
*3 インターネットからの不正侵入の実態を把握するために、わざと侵入しやすいよう設定されたサーバやネットワーク機器。
*4 インターネット上のWEBサイトの情報を取得する自動巡回プログラム。

人と空気とインターネット

AIの進化と人間の未来

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

世界情勢が混迷の度を深めるなか、
AIの進化はとどまるところを知らず、
今や人間の能力を超えるような
成果を出し始めている。
今回は、AIが人間社会に
どのような影響を及ぼすのか、
考えてみたい。

今年四月、シリアが化学兵器「サリン」を使用したと判断したアメリカは、シリアの空軍施設に大規模なミサイル攻撃を行ないました。これは一九九三年に締結された多国間協定「化学兵器禁止条約」に違反したことに対する制裁措置ということでした。

化学兵器と同様に「核兵器禁止条約」制定に向けた交渉も進んでいます。今年三月、ニューヨークの国連本部に一一五ヵ国の非核保有国や市民団体が集まり、核兵器の使用や保有など、条約に盛り込むべき具体的な禁止事項について協議したそうです。この結果をまとめたうえで六月に再び協議を再開し、七月七日までに条約案を完成させる予定だそうです。

四月にシリア空爆が行なわれたとき、アメリカのトランプ大統領は中国の習近平国家主席と、北朝鮮の核実験・ミサイル発射問題への対応について協議中だったと言われています。会談の席上、トランプ大統領は「中国が解決しなければ、我々がやる」と、単独での制裁行動も辞さない強硬姿勢を示したそうです。しかし今のところ、北朝鮮対応がうまくいっているようには見えず、五月になっても弾道ミサイル発射実験が繰り返されています。北朝鮮の最高指導者・金正恩は、自国も核兵器を開発し、核保有国と対等な力を持たなければ国家の自立と安定は望めない、と考えているのでしょうか。

化学であれば難病を治療するための医薬品開発に活用したり、原子力であれば効率のいいエネルギー源として活用するなど、先端科学技術は人類の生活をより豊かにするために積極的に活用すべきだと考えたいものです。

兵器はその威力が大きくなればなるほど、いったん手にしてしまうと、簡単には手放せなくなるものなのかもしれません。

AIの進化

本連載でも時々取り上げている人工知能（AI）の技術は、将棋や囲碁のプロ棋士に勝利したり、グーグルやトヨタなどが自動運転車の実現を目指して応用するなど、特定の分野では人間の能力に近づき、あるいは凌駕する事例も出始めています。しかし、アメリカ、ロシア、中国といった軍事大国は、他の先端技術と同様に、AIの技術を兵器に応用すべく研究を進めているようです。

例えば、AIは自動車の自動運転だけではなく、戦闘機の自動操縦への転用が進められています。昨年、ALPHAという米シンシナティ大学と米空軍が共同で開発した戦闘機操縦AIが、元空軍のベテランパイロットとシミュレータを使った模擬空戦を行なった結果、ALPHAが圧勝し、ベテランパイロットは何度もALPHAに〝撃墜〟されたそうです。

しかも、AIを作動させていたハードウェアは、Raspberry Piというわずか数千円で誰でも購入できるようなパソコンだったということにも驚かされます。もちろん、あくまでもシミュレータでの結果に過ぎないので、本当にAI戦闘機が人間の操縦する戦闘機を撃墜できる性能を持っているのかどうかはわかりません。しかし、そうなるのも時間の問題だとすれば、いずれ人間は機械との戦争に勝てなくなってしまうことになります。

プロ棋士ではない私にとって、将棋や囲碁で負けるくらいなら大したことではないのですが、戦争で勝てなくなると考えると、かなり不安になってきます。

〝ちゃんとした開発されたら……AI〟が

「技術的特異点」と訳される「シンギュラリティ」という言葉は、グーグルでAI開発の総指揮を執るレイ・カーツワイル氏が二〇〇五年に出版された著書で用いたもので、AIが進化して人間の知力を超えることを指しています。同氏は当初、シンギュラリティは二〇四五年ごろ訪れると言っていました。しかし最近では、二〇〇四年当時と比べて技術の進化が加速したため、シンギュラリティは二〇二九年に早まると言っています。二〇四五年であれば、今から二八年もあるので、まだまだ時間があるように感じましたが、二〇二九年となると、猶予が一気に半分以下の一二年になってしまいます。こうなるとシンギュラリティがかなり身近に起こる出来事になり、もうあまり時間が残されていないように感じられます。

ところで、シンギュラリティの議論になると必ず、人間の知能を超えて進化したAIが、ある日、自律的に人類を攻撃し始め、滅ぼしてしまうのではないか、という話になります。しかし私はあまりその心配はしていません。AIにとってわざわざ人類を滅ぼすメリットがない限りは、AIが自発的に人類を攻撃し始めるようなことは起こらないだろうと思うからです。

私が心配なのはむしろ人間のほうです。化学兵器も核兵器も、これまで人間の判断によって実際に使われてきましたから、AI兵器も開発が進み実用化段階に達した時点で、誰かが必ず他者を攻撃するために利用するでしょう。過去の教訓を生かすことができるのなら、AI技術を兵器として活用すること自体を阻止したいところです。

実際、AI兵器の開発を禁止しようという動きも起こっています。二〇一六年一二月、国連の「特定通常兵器使用禁止制限条約」の締約国一二三ヵ国は、人間が介在しない完全自律型兵器の禁止に向けた公式な取り組みを進めることで合意しました。他方、本稿冒頭で紹介した「核兵器禁止条約」に向けた協議には、アメリカなどすでに核を保有している国は参加していません。そうした現状を見ると、AI兵器の開発で先行しているアメリカなどの軍事大国は、AI兵器の開発を放棄しないのではないでしょうか。

核兵器に関しては、核の抑止力があるから世界の平和が維持されており、安易な核廃絶は世界平和を乱す、という考え方があります。それが真実か詭弁かはともかく、現状としては、アメリカ、ロシア、中国などの軍事大国が、次の支配的な兵力となり得るAI兵器をいち早く完成させることで、主導権を握ろうと争っていることはたしかなようです。

私見になりますが、シンギュラリティが起こり、AIが人間よりも高い知力を持つようになった時点で、兵器のコントロールを含めたクリティカルな判断は、全てAIに委ねてしまってはどうかと考えています。〝ちゃんとしたAI〟が開発されたら、それは人類の知性を超えた存在になるわけですから、せっかく結んだ平和条約を破るようなことはしないはずですし、人類は彼らの判断に従って生きる方がきっと安全で幸せになるに違いありません。

むしろ、そうなるまでの期間が危険です。人間が誤った判断で不完全なAI兵器を作動させるようなことが起こったら、そのときこそ人類が滅びるときかもしれません。昨今のAIの進展ぶりを見ていると、ふとそんなSFっぽい妄想も浮かんでしまいます。●

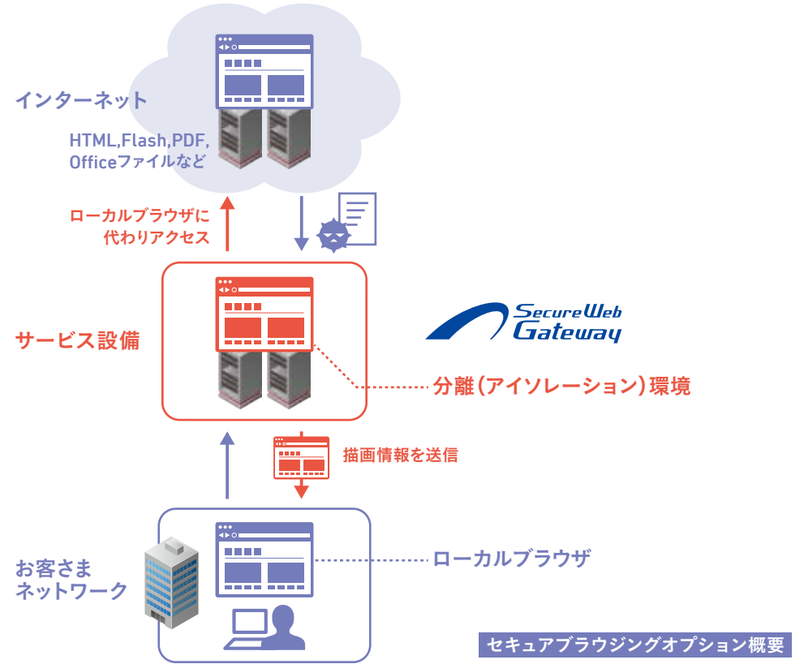
イラスト／末房志野

Technical Now

IIJセキュアWebゲートウェイサービス
セキュアブラウジングオプション

IIJ セキュリティ本部 セキュリティビジネス開発部
一條 敦

業務上欠かすことのできない WEB を安全に閲覧するには、
どのような対策が必要か?
このたび IIJ は、WEB コンテンツの実行環境を分離する技術に着目した
新たなサービスをリリースした。



セキュアブラウジングオプション概要

昨今、特定の企業や組織を狙ったサイバー攻撃が多発しています。いわゆる「標的型攻撃」と言われるもので、ファイアウォールや IDS／IPS、アンチウイルスなど、既存のセキュリティ対策をすり抜けて、マルウェアに感染させる攻撃です。

手口としては、巧妙に細工したメールの添付ファイルを開かせたり、本文に貼り付けた URL をクリックさせてマルウェアに感染させ、PC やサーバなどにある情報を盗み取るといった手法が一般的です。現在もこのメールによる攻撃が多いのですが、WEB サイトを利用した攻撃も増加しています。企業や組織の従業員がよく閲覧する WEB サイトを改ざんして、マルウェアに感染させたり、気づかないあいだに悪意のあるソフトウェアをダウンロードさせる「ドライブバイダウンロード」や、「マルバタイジング」と言われるオンラインの広告のバナーをクリックさせて、マルウェアに感染させるといった手法があります。

メールを利用した攻撃に対する対策としては、不要な添付ファイルは開かない、クリックしないなどの注意が喚起されており、対策も徐々に進んでいますが、明らかに怪しいサイトを除いて、普段閲覧している WEB サイトを媒介としてマルウェアが配布されるようなケースでは、対策もなかなかむずかしいようです。例えば、サンドボックスはそういった攻撃に有効ですが、サンドボックスを回避するマルウェアも確認されており、そのようなマルウェアに対する有効な対策は見出されていません。また、マルウェアが利用する脆弱性はブラウザのプラグインに潜んでいるケースが多く、脆弱性を修正した最新版を利用する対策を徹底したとしても、未知の脆弱性を突いた攻撃を受けたり、業務上どうしても必要なため、プラグインを利用せざるを得ないなど、抜本的な対策がとりにくいと言えます。

有効な対策は?

そうしたなか、現時点で有効な対策と考えられているのが WEB の分離です。WEB の分離とは、WEB サイトを閲覧する際に、コンテンツを読み込む環境を、利用している手元の PC（ローカル PC）から切り離して用意し、万が一、マルウェアが仕込まれた WEB サイトを閲覧した場合でも、ローカル PC がマルウェアに感染するのを防ぐという方法です。主要な方法としては、ブラウザの仮想化技術や WEB コンテンツの実行環境を分離する技術を利用して、WEB の分離を行ないます。

ブラウザの仮想化技術を利用する際は、ブラウザをふたつ用意し、ローカル PC 上にインストールしているブラウザを社内イントラネット用として利用して、インターネット上の WEB サイト閲覧用に仮想化したブラウザ（仮想ブラウザ）を新たに用意します。この方法なら、インターネット上の悪意のあるサイトやマルウェアに感染した WEB サイトを閲覧したとしても、仮想ブラウザで WEB サイトの閲覧が行なわれ、画面だけがローカル PC に転送されるため、マルウェア感染のリスクを排除できます。ただし、エージェントをインストールする必要があったり、ふたつのブラウザを使い分け、インターネットからファイルをダウンロードするには別の仕組みを用意するなど、使い勝手の面で慣れる必要があります。

一方、WEB コンテンツの実行環境を分離する技術では、ブラウザから WEB サイトを閲覧する際、分離された環境で WEB コンテンツを構成する JavaScript などのスクリプトを実行し、その結果である文字や画像などのレンダリング（描画）情報をローカル PC で読み込んで表示します。この方法は、高いセキュリティを保持しながら、普段使っているブラウザをそのまま使用でき、ファイルもダウンロード可能ですので、利便性を損なうこともありません。

セキュアブラウジングオプションとは?

IIJ では、後者の WEB コンテンツの実行環境を分離する技術に着目し、今年 1 月、「IIJ セキュア Web ゲートウェイサービス」において「セキュアブラウジングオプション」をリリースしました。こちらを利用すれば、IIJ が提供する基盤上に用意された分離環境で WEB コンテンツの実行処理が行なわれ、レンダリング情報の文字や画像がローカル PC に転送されます。

前述した通り、他の WEB の分離を行なう技術と違って、基本的にはローカル PC でのブラウザをそのまま使用できますので、面倒なエージェントのインストールなども不要です。ファイルに関しても、HTML5 で変換表示を行なうので、安全な状態で確認でき、確認後もオリジナルファイルもしくはスクリプトが除去された状態で PDF としてダウンロードが可能です。

このサービスは、IIJ セキュア Web ゲートウェイのオプションとして提供されるため、大規模な設備構築や多額の初期費用が発生せず、クラウドサービスとして費用の平準化が可能です。他の WEB の分離を行なう製品・ソリューションのように Windows のライセンス費用なども発生しません。現在、IIJ セキュア Web ゲートウェイサービスをご利用いただいているお客さまなら、このオプションをお申し込みいただくだけで、高いセキュリティと利便性の共存を実現できます。

セキュアブラウジングオプションは、米国 Menlo Security の協力により提供され、同社の特許技術である ACR（Adaptive Clientless Rendering）を利用して、ユーザの WEB サイトへのアクセス時に分離環境で全てのアクティブコンテンツ（JavaScript や Flash など）を実行・分離し、ACR を使ってレンダリング（描画）情報のみをクライアントのブラウザに表示します。

今後の展望

IIJ セキュア Web ゲートウェイサービスは、約 116 万アカウントのお客さまにご利用いただいており、豊富な実績があります。WEB セキュリティに必要なフィルタリング、アンチウイルス、サンドボックスなどに加え、今回追加したセキュアブラウジングを提供しており、WEB セキュリティ対策に必要とされる技術を網羅し、高いセキュリティ対策と WEB サイトの閲覧・利用状況の把握が可能です。また、昨今増加している、抜け道として利用されやすい暗号化された WEB サイトとの HTTPS 通信にも対応しています。

セキュアブラウジングオプションは、金融業界を中心に多くの引き合いをいただいており、実際にご利用いただいているお客さまもいらっしゃいます。今後は、より多くの方にご活用いただけるようアピールを続けながら、より進化した WEB のセキュリティサービスを提供していきたいと考えています。●

Technical Now

セキュアな入退場管理システムにIIJサービスを活用
伊勢志摩サミットの成功に貢献

先進的な IT ソリューションでお客さまの課題解決に貢献する電通国際情報サービス（以下、ISID）。
同社は伊勢志摩サミットの入退場管理システムを支えるインフラ、ネットワークに IIJ サービスを採用した。
「IIJ GIO コンポーネントサービス 仮想化プラットフォーム VW シリーズ（以下、IIJ GIO VW シリーズ）」、
「IIJ Omnibus サービス」などを活用することで、3.5 ヵ月という短期間でシステムを構築。
厳しいセキュリティ要件をクリアし、安全な入退場を実現することでサミットの成功に大きな役割を果たした。

[導入前の課題]
万全のセキュリティを施し、短期間でシステムを構築

広告代理店最大手である電通のグループ会社としての強みを活かし、多様なお客さまに最適な IT ソリューションを提供する ISID。同社は、ビジネス課題の解決だけでなく、大規模なイベントやキャンペーンの運営などもサポートする。その一環として取り組んだのが、2016 年 5 月に三重県で開催された伊勢志摩サミットにおける入退場管理システムの構築だ。

求められたのは、関係者が事前登録を行なう WEB サイトの構築と、会場の入退場管理。正規の ID パスを持つ人だけがセキュリティゲートを通れるようにするシステムだ。

しかし、その構築は容易ではない。「受注が決まってから会議の開催までの期間は約 4.5 ヵ月でした。受付サイトの立ち上げまでは 2 ヵ月ほどしかなかったのです」と同社の松島宏明氏は振り返る。同社は WEB プロモーションに関わる一連の機能を提供する ASP サービス「DMAP（Digital Marketing Platform）」、クラウド型の開発運用基盤「iPLAss」を保有する。このふたつを組み合わせれば、システムのアプリケーション部分は短期間で構築できるが、サービスの提供基盤やネットワークの整備には時間がかかってしまう。

セキュリティの確保も重要な要件だ。「入退場を認証するため、システムでは登録者に関連する機密情報を管理します。お客さまからは DDoS 攻撃をはじめとするサイバー攻撃に対し、万全の備えが求められていました」（松島氏）。さらに、「攻撃に備えるだけでなく、万が一、システムに問題が起きても運営に支障が出ない仕組みが求められていました」と同社の榎本高広氏も語る。

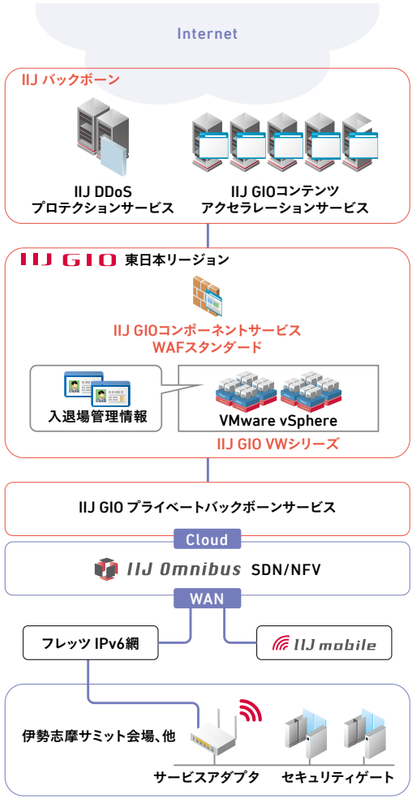
[選定の決め手]
多様なニーズを網羅するサービスの総合力を評価

この課題解決のパートナーに選定されたのが IIJ である。決め手になったのが総合力だ。「インフラやセキュリティ関連の豊富なサービスがあり、必要なサービスを短期間で調達できます」と古城晃氏は語る。

これまでの実績も大きな選定ポイントになった。DMAP の基盤のひとつには IIJ GIO VW シリーズを採用している。その信頼性を評価し、今回の入退場管理システムのサービス基盤にも IIJ GIO VW シリーズを採用することに決めた。「すでに実績のある環境にセキュリティオプション、ネットワークオプションを追加することにより、課題をクリアできると考えました」と古城氏は述べる。

IIJ GIO VW シリーズ上の入退場管理システムは IIJ のインターネット接続サービスを介して、インターネットにつながる仕組みだ。さらに IIJ DDoS プロテクションサービス、IIJ GIO コンポーネントサービス WAF スタンダード、IIJ GIO コンテンツアクセラレーションサービスを活用し、セキュリティレベルを高めた。また、入退場管理システムと会場のセキュリティゲートをつなぐ WAN 回線には IIJ GIO プライベートバックボーンサービスと IIJ Omnibus サービスを組み合わせ、クローズドなネットワークを短期間で構築。特に IIJ Omnibus サービスに対する評価は高い。

IIJ Omnibus サービスはネットワークに必要な機能を、クラウドを介して提供するサービス。ルータ、VPN などのネットワーク機器やファイアウォールなどの専用機器を所有することなく、各拠点に配布されるサービスアダプタに接続するだけでさまざまな機能を利用できる。「すぐに WAN を構築できるうえに、サービスアダプタにはコンフィグなどの情報が残らない。今回のように期間限定で利用したい場合には最適なサービスです」と同社の岸田正輝氏は述べる。



さらに WAN のアクセス回線は有線のフレッツ IPv6 網を主回線にするとともに、バックアップとして無線の IIJ モバイルサービスで冗長化を図った。そして、急きょ発生したセキュリティゲートの検証作業の際には、有線回線の敷設が間に合わなかったが、モバイルを活用することで動作検証をスムーズに行なうことができた。「モバイル回線を利用することで、どこでも WAN 拠点を開設できるため、現地に行かず東京のオフィスから検証環境に接続できました。モバイルを活用できた点は、開発の効率化という面でもメリットが大きい」と古城氏は評価する。

[導入後の効果]
3.5 ヵ月で構築を完了。
実績を糧に提案の幅を広げる

IIJ のサービスを活用することで、同社は計画どおりに入退場管理システムをカットオーバーした。そして、伊勢志摩サミットは事故やトラブルもなく成功裡に終幕した。

「自社で開発したアプリケーションとカード発行システムやゲートとの連携の検証を含め、システム全体を 3.5 ヵ月で構築できました。IIJ のサービス活用の効果は大きかったです」と松島氏は満足感を示す。

IIJ のサポート対応も短期構築に大きく貢献した。プロジェクトの立ち上げにともない、IIJ は専門のサポートチームを発足させ、対応にあたった。「現地から急なテスト依頼があり、IIJ Omnibus サービスの設定を変更しなければならないときも、サポートチームのおかげで現地の要請に迅速に対応できました」と岸田氏は話す。

同社にとってもメリットが大きい。「高度なセキュリティ要件の入退場管理システムを短期間で構築し、無事稼働できた実績は、今後のイベントサポート事業に活かせます」と古城氏は期待を寄せる。

IIJ サービスを活用し、伊勢志摩サミットの成功に貢献した ISID。「これからも IIJ のサービスを適材適所で活用し、お客さまの多様なニーズに応えていきたい」と話す松島氏。革新を続ける IT の可能性を追求し、お客さまの課題解決と新たな価値創出を目指す ISID を IIJ は強力に支援していく。●

株式会社電通国際情報サービス
コミュニケーションIT事業部
ソーシャルテクノロジー開発部
プロジェクトディレクター
松島 宏明 氏

株式会社電通国際情報サービス
コミュニケーションIT事業部
ITソリューション部
プロジェクトマネージャー
古城 晃 氏

株式会社電通国際情報サービス
コミュニケーションIT事業部
公共ビジネス部
プロジェクトディレクター
榎本 高広 氏

株式会社電通国際情報サービス
コミュニケーションIT事業部
公共ビジネス部
プロジェクトマネージャー
岸田 正輝 氏

iSiD IT Solution Innovator

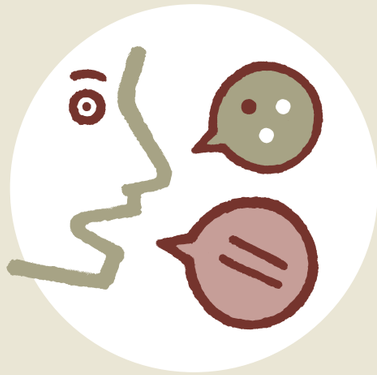
株式会社電通国際情報サービス
本社：東京都港区港南2-17-1
設立：1975年12月11日
URL：http://www.isid.co.jp/

・本記事は 2016 年 11 月に取材した内容をもとに構成しています。記事内のデータや組織名、役職などは取材時のものです。

Internet Trivia

インターネット・トリビア

コンピュータと日本語表示



IIJ MVNO事業部
事業統括室　シニアエンジニア
堂前 清隆

スマートフォンのアプリやWEBを見ていて、「日本語の文章なのに、文字の形に違和感を感じた」経験はないでしょうか？　今回は、そんな話にも通じる「コンピュータと日本語」について紹介したいと思います。

日本語には、ひらがな・カタカナ・漢字など多くの文字があります。特に漢字には、文字の一部が微妙に違う「異体字」もあり、日常的に使われている漢字だけでもかなりの数にのぼります。コンピュータで日本語を扱うためには、まず、扱うべき文字の種類を定める必要があります。これを「文字集合」と言い、日本ではJIS（日本工業規格）により「JIS第1水準」「JIS第2水準」などの文字集合が定義されています。また、文字をコンピュータで取り扱うためには「文字コード」という番号を使います。文字コードの割り当て方を「符号化方式」といい「Shift_JIS」「EUC-JP」「ISO-2022-JP」などいくつか種類がありますが、いずれもJISの文字集合を基本にしており、含まれる文字に違いはありません。

コンピュータに記録された文字を画面やプリンタで表示するために必要なのがフォントです。日本語には「明朝体」や「POP体」と呼ばれる「書体（タイプフェイス）」があり、一定の様式に沿ってデザインされた文字を集めたものがフォントです。フォントに含まれる個々の文字を「字体（グリフ）」といい、日本語の場合JISの定義をもとにひとつのフォントあたり数千のグリフが収録されています。

コンピュータの文字表示は、フォントのなかから文字コードによって指定されたグリフを取り出し、順番に画面に表示することによって実現しています。

ここまでは日本語を前提として文字集合や符号化方式について言及してきましたが、世界に目を向けると英語や中国語、ヒンディー語など多種多様な言語があり、コンピュータでこれらの言語を扱うために、言語毎に文字集合や符号化方式が定義されています。しかし、取り扱う言語に合わせて処理を切り替える必要があり、複数の言語を混在させて使用するのは困難でした。

この不便を解消するため、多様な言語を統一的に扱うことを目的とした新しい規格がつくられました。それが「Unicode（ユニコード）」です。Unicodeでは言語毎に文字集合を定義するのではなく、世界中の言語で使われる文字を集めた文字集合を定義しています。また、多くの文字を取り扱うために「UTF-8」などいくつかの符号化方式を定義しました。Unicode文字集合と符号化方式により、処理を切り替えることなく、複数の言語を混在させることが可能になったのです。

しかし、その一方で新たな問題も発生しました。文字数が多い中国語・日本語・韓国語は、Unicode文字集合を定義する際、字体の似た文字に同じ文字コードを割り当てるという判断がなされたのです。文字コードが同じである以上、表示されるグリフも同一になります。しかし、これらの文字はもともと異なる文字ですので、書体によってはかなり見た目が違います。結局、Unicodeを使っていても、それを表示する際には中国語用・日本語用・韓国語用と、それぞれのフォントを使って表示しなければ、期待する文字として表示されないという事態になってしまいました。

冒頭で紹介した「違和感のある文字」は、まさにこれによって引き起こされた現象です。Unicodeで保存された日本語の文章を表示する際に、何らかの原因で中国語や韓国語用のフォントが適用された結果、日本語風ではない字形で表示されてしまったのです。

今回紹介したエピソードだけを見ると、Unicodeは大変乱暴な規格だと感じるかもしれません。たしかにそのような側面もありますが、Unicodeという規格が定められたことで、特に日本にフォーカスされたわけではない機器やソフトウェアでも、ある程度日本語が扱えるというメリットも生まれています。日本語を扱う人間としては複雑な気持ちです。●

イラスト／末房志野（P22,23）

Global Trends

グローバル・トレンド

レバラン休暇明けの転職と人事の力量

PT. IIJ Global Solutions Indonesia
President Director　**延廣 得雄**

イスラム教の「ラマダン（断食）」という言葉をご存じの方も多いでしょう。ひと月ほど続くこの禁欲生活のあとには「レバラン（断食月明け大祭）」があり、日本でいうと、盆と正月とGWを合わせたような休暇になります。ここインドネシアでは、公式に二日間の祝日が設定されていますが、政府の指導により、前後含めて最低でも一週間、最大で三週間程度の休暇をとるケースもあります。

特にジャカルタは地方出身者が多く、日本と違って交通事情も不便なため、飛行機の運賃などはこの時期高騰し、多くの人が出費を強いられるのですが、企業はTHR（宗教手当）という一種のボーナスを社員に支給します。これは法律で決められています。つまり、多くのムスリムが六月末の給与と一緒にボーナスを確実にもらえることになりますから、数週間のレバラン休暇を挟んで、新しい会社へ転職しようとする人が多くなる時期でもあります（有給休暇を消化しなくていいというメリットも生じます）。

標準的な雇用契約ですと、退職する場合は一ヵ月前に会社へ通知する義務があるので、六月末付けで退職しようとした場合は、五月末には会社に通知しなければなりません。従って転職活動は最低でも四月頃には始めています。企業にもよりますが、昇給や昇進の時期がこの辺りですと、自分の希望にそぐわない待遇が分かった瞬間に転職活動を開始するということになります。

とはいえ、ジャカルタの転職市場はそんなに甘くないので、早々に転職先を見つけたいがために、自分の経歴を拡大解釈して宣伝する人も多くいます。技術者や専門職の場合は、応募の過程である程度の課題を与えることで一〇〇の応募を数パーセントに絞ることができるのですが、営業職となるとその判断もむずかしくなります。

よって、この時期の採用は人事担当者の力量がもっとも試され、ここで成果が出せる（＝良い人材を採用できる）優秀な人事を育てられれば、事業の成長に必要なピースを獲得できることになります。インドネシアで持続的な成長を目指すなら、この点はトッププライオリティにすべき施策だと考えています。●

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

今年に入って熱帯魚のグッピーを飼いはじめました。先日、メスの1匹が出産し、8匹の赤ちゃんグッピーが仲間入りしました。大人と一緒にしておくと食べられてしまうので、小さな穴を空けたペットボトルを水槽に入れて避難させています。この赤ちゃんグッピー、成長がとてもはやく、毎日少しずつ大きくなっているのが見てわかり、最近はその変化を観察するのが日課となっています。私もペットボトルのなかの赤ちゃんグッピーのように成長していきたい！ と思う今日この頃です。（M）

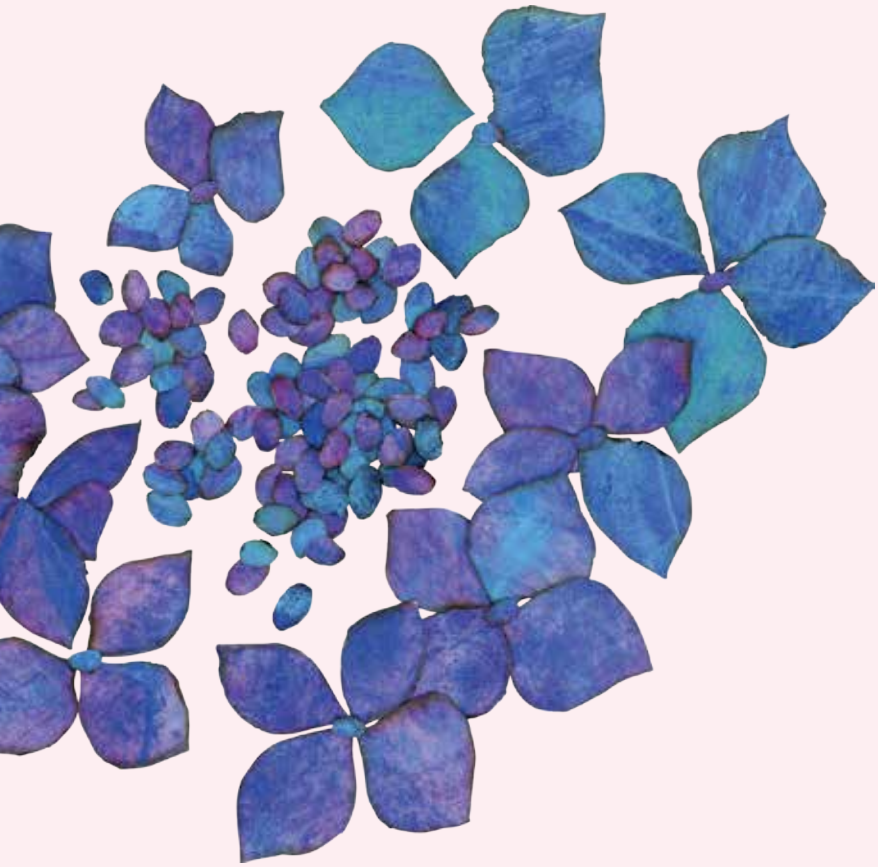
Information

個人向けモバイルサービス「IIJmio」Amazonギフト券プレゼントキャンペーン

IIJmioのWEBサイトで音声通話機能付きSIMと同時にIIJmioサプライサービスの対象端末をお申し込みいただいたお客さま、およびIIJmioモバイルプラスサービス（エコプラン）で対象端末をお申し込みいただいたお客さまに、Amazonギフト券をプレゼントいたします。

キャンペーン期間　2017年7月31日（月）まで

詳細は、以下のページをご覧ください。
https://www.iijmio.jp/campaign/device/2017summer.jsp



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四条西 4-1 伊藤・加藤ビル 5F
〒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

◎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