IIJ. news

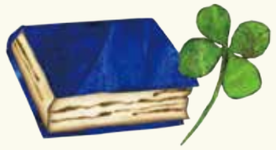
IIJ was founded in 1992 as a pioneer in the commercial Internet market in Japan.
Since that time, the company has continued to take the initiative in the network technology field, playing a leading role in Japan's Internet industry.
The history of IIJ is indeed the history of the Internet in Japan.

April 2015
VOL. 127

特集

備えあれば憂いなし

～新しいセキュリティ対策に向けて



ぷろろーぐ

入社式

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

艶やかなさくら色で、街を包み込んだ束の間の饗宴も終わってしまった。道楽と揶揄されながら十一年目を迎えた「東京・春・音楽祭」も、フィナーレとなった。沈丁花が香る早春から葉桜に至るこの季節は、新しい会計年度が始まる時期であり、事業計画の策定、決算と、仕事に追われているはずなのだが、桜を眺めると胸が騒ぐ。ともすれば、季節の移ろいすら忘れてしまうほど日々に追われ、あっという間に時が過ぎ去ってしまうことに慣れているのだが、この季節だけは、時が消えていく切なさを身体中で実感する。年を経るごとに、時間や空間に対する感受性がますます鈍化していくのは、インターネットにも一因があるのだと、日頃から身に染みているのだが、グローバル化の流れはそれを加速させるばかりである。

四月一日は入社式。わが社の誇るアセットはなにかと言えば、ＩＩＪで仕事をし、能力を伸ばし、自己実現をする「ひと」である。その意味で、入社式は一年でもっとも大切な行事なのだが、一〇〇人を超える新入社員が入社してくれるようになると、まさにスケジュールと形が優先する行事になってしまうようだ。型どおりに進行する行事が悪いわけではないが、ＩＩＪという企業のカルチャーを表現し、それを少しでも共有してもらおうという意思が感じられないのである。形が内容を決めるというのも一理あって、昔は、新入社員が好き勝手に質問をし、それに経営陣が正直に答えていた時代があり、行事の進行としてはいい加減だったのだが、少なくとも、形式にまったくとらわれないＩＩＪらしい行事だった。それが今では、整然と進行する入社式になってしまった。私も挨拶をするのだが、なにかと失言が多く、日頃は講演などもできる限りお断りしていることを忘れて、なんとなく型にはまったような話をして終わってしまった。

入社してくれた若者の能力をできる限り伸ばすことで、給与の支払いもままならなかったほどの厳しい時代を乗り越えて、ＩＩＪはここまで成長できたのである。まさに一緒に働く「ひと」こそ、ＩＩＪの最大のアセットなのである。「神田の町工場」と言われていたのも、若い「ひと」を育てること以外に将来がないという考えを、誰もが共有していたからである。入社式が型どおりの行事になってしまったからといって、その理念が変わったわけではない。行事ということで、とりあえずは、型どおりに進めておくだけの話に過ぎないのかもしれないが、古臭い私には気になるのである。

高校生になって、まさに「落ちこぼれ」という形容がいちばん相応しかった私は、高校の入学式を最後に、それ以降は、高校の卒業式、大学の入学式・卒業式、社会人の第一歩である入社式といった行事に一度も出ていないわけで、型にはまった行事に出ると、いまだに、なんだかなあという気分になってしまうのは、そもそもの私の経歴が「落ちこぼれ」に終始していたことからくる歪みなのかもしれない。今年の新入社員の表情を眺めていて、私のような「落ちこぼれ」がいなかったので、ほっとしたことも事実である。●

イラスト／末房志野

表紙の言葉「クローバー」

四つ葉のクローバーは三つ葉のクローバーの変異体で、偶然見つけると幸せになれるといわれています。クローバーの葉は、それぞれ希望、誠実、愛情、幸運を表すという説があります。どんなにテクノロジーが発展して便利になっても、永遠に変わらない人間にとってプリミティブなものなのでしょう。4月は新年度。初心を忘れず新しいことにチャレンジしたくなります。

末房志野

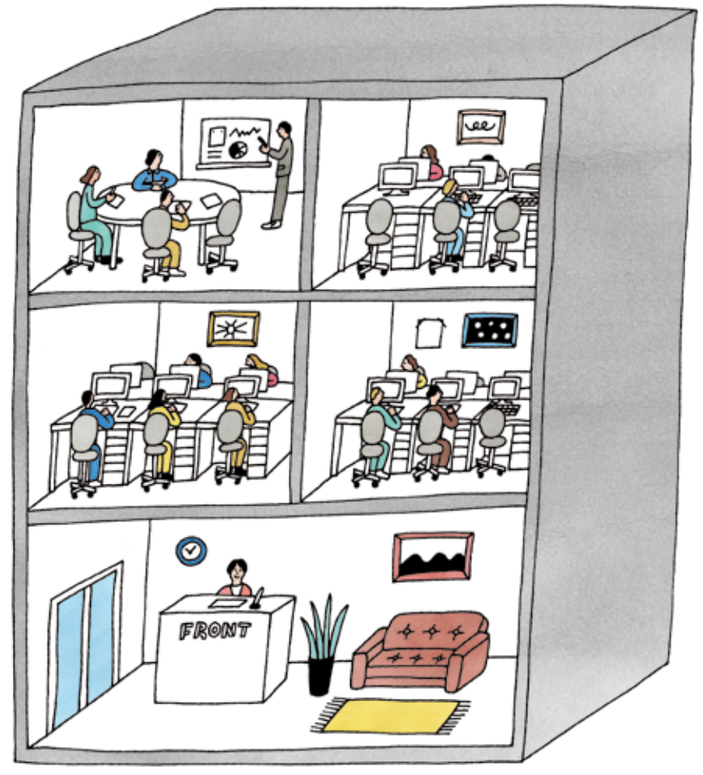
IIJ. news
April 2015
VOL. 127

Topics

備えあれば憂いなし

～新しいセキュリティ対策に向けて

セキュリティ対策が変わりつつある。
かつてのように、対策ソフトやソリューションを導入するだけでなく、
人材教育や啓蒙活動、適切かつ丁寧な情報共有、インシデント発生への備えなど、
平時における多角的な対応が求められるようになった。
本特集では、情報セキュリティをめぐる最新動向を紹介する。



特集イラスト／STOMACHACHE.

IIJにおける セキュリティ対策への取り組み

～情報セキュリティ管理から危機管理へ

社会情報基盤として不可欠な通信サービスを提供するISPに相応しい
安全性・信頼性を確保するにはどうすればいいか？
ここではまず、IIJのセキュリティ対策の大枠を俯瞰する。

IIJ 常務取締役
情報セキュリティ担当役員
三膳 孝通

本稿では、IIJにおけるセキュリティ対策の取り組みや方針について、その概要を紹介します。内容としては具体的な取り組みではなく、基本的な考え方やその方針に至った経緯、関連する課題などが中心になりますが、同時に、情報セキュリティをはじめとするリスクの様相は刻々と変化しており、現在行なっている対策も常に見直しを求められています。よって、今回紹介する方針や取り組みは、執筆時点（二〇一五年二月）のものであることをご了承ください。

情報セキュリティの変化

情報セキュリティを取り巻く環境は、インターネットに代表されるICTの普及とともに大きく変化してきました。情報システムの時代は、大切な情報は閉じたシステムのなかで提供された手段によってのみアクセスできる、というかたちで守られてきました。そのため、システム側で十分な対策を講じることができ、それが効果的に機能してきました。

ところが今や、誰もが情報を発信できます。センサーなど人間以外が発信する情報も増えてきました。情報は、種類・内容ともに爆発的に増え、あらゆる機器で取り扱えるようになっています。それにともない、情報システムで扱う情報を管理・制限したり、つながっている機器を管理・把握できたりする時代ではなくなりつつあり、新たなセキュリティ確保の方法が求められています。

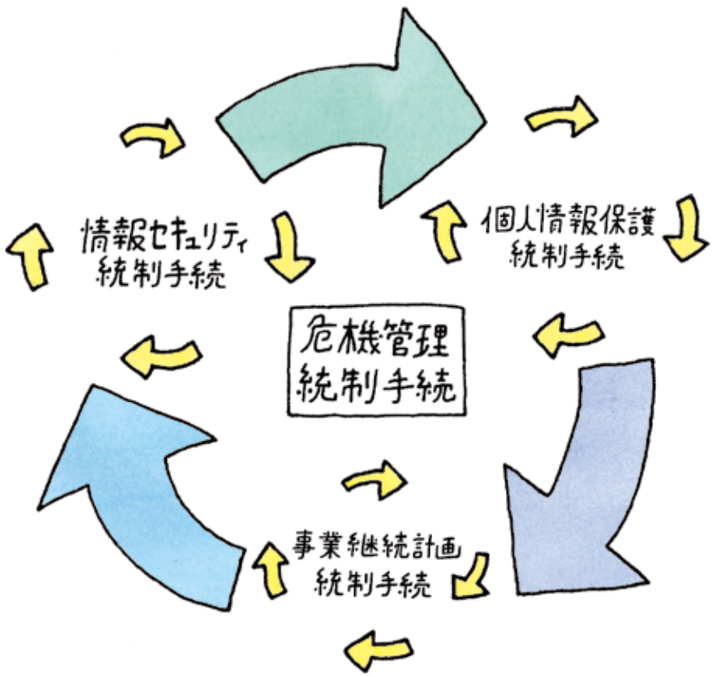
以前は、社内の情報システムを管理・運用している情報システム部門が責任を持って対応していました。それが今日では、多少の差はあるものの、情報システムとほぼ同等の情報処理・発信能力を一人一人あるいは一つ一つが持ち得る時代になったのです。さらにIoT（Internet of Things）など、あらゆるものが相互につながり、いろいろな機能を提供することが期待されています。

こうした時代には、一つの部門や視点からだけのセキュリティ対策では不十分で、データ・システム・ネットワーク・端末・アプリ・使い方……等々、多層的・多角的な対策が必須となります。

言い換えると、情報セキュリティをはじめとするリスク統制の手続きは、トップダウンによる全社的な対応だけでなく、各部門・各人が日常業務のなかで考慮すべきものになりつつあるということです。これについては、後半で再び触れたいと思います。

IIJの危機管理室

二〇一一年一〇月、IIJでは従来の情



報セキュリティ管理体制を見直す必要があるとの判断から、体制および役割を大幅に変更しました。

変更理由としては、大きく二つありました。一つは、情報セキュリティ対策や個人情報保護対策、環境対策といった複数のPDCA(Plan-Do-Check-Action)サイクルの検討がほぼ独立して実施されていたこと。もう一つは、同年三月に発生した東日本大震災を受けて、事業継続という大きな危機管理体制への取り組みが急務となったためでした。

当初、社内ではおもに次の三つの対応が、連携しつつも独立に進められていました。

①全社的・具体的な情報セキュリティ対策。

②サービス部門および設備を対象にしたISMS(Information Security Management System)制度への対応。

③個人情報保護とプライバシーマークへの対応。

これらは、情報資産の管理や取り扱いなどに際して重なる部分も多いのですが、同じ対策をそれぞれで検討することがありました。また、同じ情報資産に対する対策についても、個々の対応のあいだに齟齬が生じる可能性が懸念されていました。

ここで、単に認証の取得・維持だけにとどめる、という方法もあったでしょうが、そもそもISMSなどの導入の検討は、ますます重要となる社会情報基盤を提供するISPに相応しい、安全性・信頼性を保持できる手段を確立する、という目的から始まりました。つまり、認証取得はそのための手段であり、様々なマネージメントシステムを、整合性を維持しながら運用していくことが要件だったのです。

もちろん東日本大震災以前も、システムを冗長化するなど、災害時に事業を継続するための対策はとっていましたが、あの未曾有の災害を経験し、改めて検証を行なった結果、取り組みとして不十分な部分があったことが明らかになりました。さらに、情報セキュリティや個人情報保護、事業継続なども危機管理という枠組から捉え直す必要があるとの認識に達しました。

そこで、各マネージメントシステムの基本となる「危機管理統制手続」を中心に据え、情報セキュリティや個人情報保護、事業継続計画などのマネージメントシステムは、危機管理統制手続から実装できるモデルを構築し、それを担う組織として、それまでおもに情報セキュリティを取り扱っていた「情報セキュリティ管理室」を「危機管理室」として、情報セキュリティ管理だけでなく、個人情報保護や事業継続といった様々な取り組みにおいて、その中心を担う組織へと変更しました。(右頁「統制手続相互連携イメージ図」参照)

現場での検討・実装を中心とした体制

危機管理室は大きな組織に見えるかもしれませんが、実際は小さな組織です。そして実質的な対策の検討・実装は、現場毎に行ない、各部門の担当者とは定期的に会合を持っています。

全社的に取り組むべきものについては、社内の情報インフラを担当する部門が対策を行ないますが、サービス関連のシステムなど、現場固有のシステムについては、現場での対策を原則としています。

そのようにした大きな理由の一つに、各部門がシステムや業務の設計・実装段階から情報セキュリティや事業継続の対策を施すことができるため、方法・コストの妥当性が増し、非常時の対策もより迅速になると考えられたからです。

システムや業務、特に個々のシステムについては、その目的によって個別の対策が必要になる可能性があり、全社的な対応がむずかしいものも多々あります。当然、設計段階では考慮されていなかったゆえに、導入が困難なものもあるでしょうが、特に事業継続などでは、設計・実装に関わった経験が非常時の対応にも役立つことが期待されます。サービス提供や業務のコストに関しても、全社で情報セキュリティコストや事業継続コストとしてまとめてしまうよりは、個別のコストとしてそれぞれに還元できるほうがより適正なものになるでしょう。

もう一つの大きな理由は、多層的・多角的に対応することへの備えです。全社としても対策し、部門としても対策し、個人としても対策する――昨今の状況を鑑みるに、一つの対策で十分ということはなく、対策可能なあらゆるフェーズで、実行可能な対策を講じるべきだと考えられます。「全社的にやっているから」「提供されたサービスでやっているから」ではなく、部門単位でできる対策を行なうことが重要なのです。そうすることで、啓蒙や教育としての効果も発揮されます。

もちろんこのような体制は、どこでもとれるものではないかもしれません。ただ、一括的・集中的な対策が困難であることはたしかで、現場の力を活かしていくのが、今後望まれる方向性だと言えるでしょう。

特別なものから日々の習慣へ

情報セキュリティ対策は、以前であれば、ある特定の場面を想定して、その場面において有効な対策を行なえば良かったかもしれません。しかし近年では、膨大な情報が、意識／無意識あるいは意図的／偶発的にかかわらず、コミュニケーション・ビジネス・生活を支えるために、あらゆるところに流れています。つまり、我々は〝四六時中〟情報セキュリティの問題に直面しているのです。

こうした環境下では、「これは情報セキュリティ対策」「これは個人情報保護」「これは事業継続計画」といった区分けはもはや不可能であることは言うまでもありません。

むしろ、セキュリティ的な習慣がシステムや業務のなかに浸透しているような状態が望ましく、喩えるなら、健康維持のために外から帰ったら手洗いとうがいをする、といった日常的な習慣のように、情報セキュリティにも気を配ることが大切なのです。

健康な人や体力がある人は、風邪をひきにくく、風邪をひいても軽くてすみ、早く治ります。それと同じことが組織にも当てはまるのではないでしょうか。つまり「基礎情報セキュリティ体力」のようなものがあって、それが高い組織はインシデントを起こしにくかったり、起こしてもすぐ対応できるということです。今後の危機管理対策は、そういう考え方に変化していくと思われます。●

対談 これからのセキュリティ対策

ここでは、企業が抱えるインターネットセキュリティの課題や、IIJが提供しているセキュリティサービスの概要をわかりやすく述べてみたい。

IIJ 常務執行役員
サービスオペレーション本部長
山井 美和

IIJ ソリューション本部副本部長
兼 セキュリティソリューション部長
神田 恭治

――まず、ＩＩＪのセキュリティサービスの体制を簡単に説明してください。

山井　ＩＩＪはインターネット接続サービスを提供し始めた当初から、「インターネットセキュリティはどうあるべきか」という問題意識を持ちながら、ファイアウォール、ＩＰＳ（Intrusion Prevention System：侵入防止システム）、ＩＤＳ（Intrusion Detection System：侵入検知システム）、DDoS対策ほか、新たな脅威・リスクが現れるたびにそれに対するセキュリティサービスを提供してきました。サービスオペレーション本部は、そうしたサービスの企画・開発・運用など一連のプロセスを担当しています。

神田　中堅・大手企業のセキュリティ対策では、全体最適な環境を構築しなければなりませんが、ＩＩＪが提供する標準的なサービスやその組み合わせだけでは対応できないものも出てきます。そこに関しては、他社のソリューションなども組み込んで、個々のお客さまに最適なセキュリティシステムを構築するインテグレーションビジネスが必要となります。その役割を担うのが、セキュリティソリューション部です。

山井　この二つの部署に加え、ＩＩＪにはセキュリティ情報統括室（以下、ＥＲＣＳＩ）があり、日々インターネット上で発生する問題や事件を早期に発見し、ＩＩＪのサービスにおいて早急に対策を行なうことを目的に活動しています。

ＥＲＣＳＩは、マルウェア観測活動のＭＩＴＦ（Malware Investigation Task Force）や緊急対応チームＩＩＪ-ＳＥＣＴの母体として活動するとともに、一般ニュースなどのパブリックモニタリング、脆弱性情報収集、マルウェア解析、実際に発生した事件のインシデント・ハンドリングなどを行なっています。その活動内容は、ＩＩＪが定期発行している技術レポート「Internet Infrastructure Review」＊のインフラストラクチャ・セキュリティとして公開しています。

さらには、各種関連団体や学会などの運営や活動にも積極的に参画することで、インターネット全体のセキュリティ向上に尽力しています。ＩＩＪのインターネットにおけるセキュリティ対策は、この三極が連動しながら展開しています。

セキュリティ対策は〝イタチごっこ〟か？

――現在、企業が抱えるインターネットセキュリティの課題には、どういったものがありますか？

山井　セキュリティに関しては、個々のお客さま毎に課題や要件が異なります。ＩＩＪでは常に〝最大公約数〟を意識しながら、「ファイアウォールで守る。DDoS対策を行なう」など、複数の手段を提供していますが、脅威・リスクへの対策を考えても、すぐにそれをすり抜ける手法が出てきたり、安全だと思っていたソフトウェアに脆弱性が発見されたりするなど、どうしても抜け落ちる部分が出てくる。しかしそこで「イタチごっこだから……」と言って諦めるのではなく、新しい対策を開発していかなければならないし、新しい事象に対してどれだけ速やかに対処できるのかといったあたりが、今、直面している課題です。

さらに言うと、企業の「内部犯行」などは、我々のサービスでは防ぎきれない領域になります。しかし、そういったこともセキュリティに対する新たな脅威・リスクであり、具体的な対策をお客さまと一緒に考えていかなければならないと思っています。

従来は、悪者がいてそれに対する防御を考えれば済んだのですが、昨今では、自分たちの側やまったく想像していなかったところに危険が潜んでいたりします。

――インターネットセキュリティとひと言でいっても、非常に広範なテーマになります。対策を行なう際、どういう枠組で考えるべきでしょうか？

神田　企業の情報システム・ネットワークでは、二つの大きな脅威が考えられます。外部からの脅威と内部の脅威です。典型的な外部脅威は標的型攻撃で、内部脅威は社内の不正行為による情報漏えいなどです。あと、最近話題になることが多いのが、インターネットバンキングやＥＣサイトといった「公開ＷＥＢサイト」における脅威・リスクです。

――対策のリクエストが多いのは、どの分野ですか？

神田　やはり、外部からの脅威に対する対策です。企業内と外部との境界を守る〝ゲートウェイ・セキュリティ〟に関するご要望が一番多い。またＩＩＪはクラウドサービスも提供しているので、公開ＷＥＢサイトのセキュリティ対策も得意としています。

――ＩＩＪならではの強みは何ですか？

山井　ＩＩＪはインターネットのバックボーンを運用しており、第一に自分たちのネットワークを自分たちで守らなければならないのですが、その際、バックボーン側でセキュリティ対策を講じたうえで、それをベースにサービス展開しているので、お客さまが直接リスクにさらされる危険性を減らすことができます。

神田　もう一つ挙げるなら、ＩＩＪはセキュリティベンダやキャリアに対して中立的な立場にあるので、ＩＩＪならではの〝ベスト・オブ・ブリード〟（最善の組み合わせ）による対策・運用を提供できます。

山井　マネージド・セキュリティ・サービスプロバイダということですね。

新たな脅威に対して

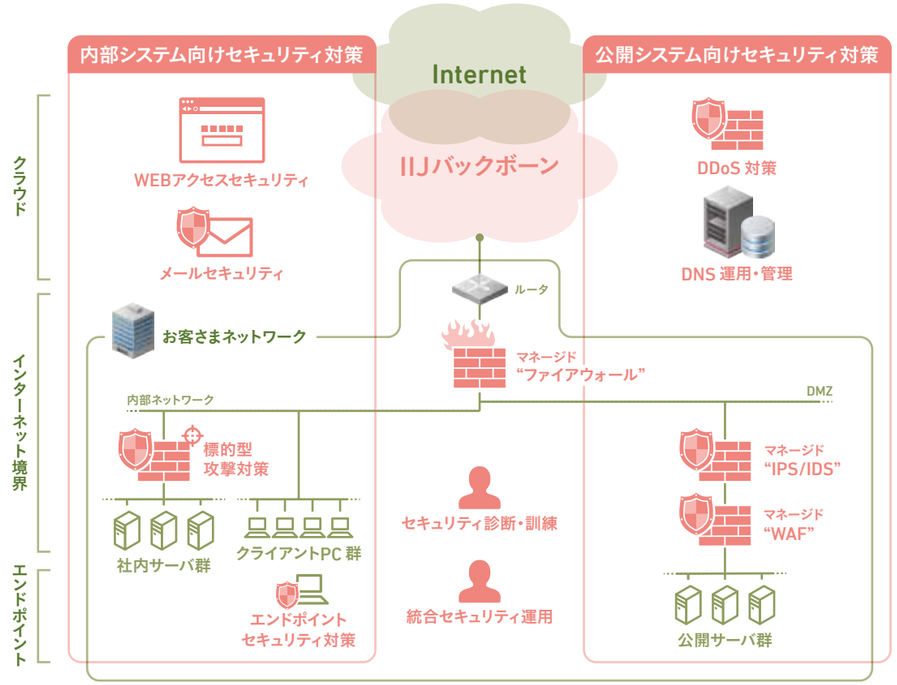
――企業に対する最新の脅威には、どのようなものがありますか？

山井　インターネット上では、詐欺、窃盗、えん罪など、社会と同じ問題が起こると考えて間違いなく、ＩＩＪのバックボーンを守ることでお客さまも守れていた時代から、それだけでは不十分な時代に変わってきています。そうしたなか、ＩＩＪが警察やガードマンになれるわけではないのですが、インターネットを支える一員として、それらを防ぐための啓発・教育や、時にお客さまに迷惑をかけることになっても、一定の強制力を持った対応を行なうこともあります。

――今後、どのような脅威が予想されるでしょうか？

神田　IoT時代になると、これまでと比較にならないくらい膨大なデバイスがネットワークにつながり、脅威・リスクが及ぶ領域も拡大します。新しいデバイスはスピードの問題です。もう一つは、人が処理する何倍ものスピードでデータを処理できるので、何かに感染したら、拡散するスピードも格段に速くなり、リ

＊ http://www.iij.ad.jp/development/iir/



IIJのマルチポイントセキュリティ

スクが急速に広がっていきます。極端な話をしますと、ボタンを押せば、そこにつながっている全デバイスが暴走し始める、といったことが起こり得るのです。

山井　通信事業者には通信サービスを提供する義務がありますが、そうした脅威・リスクの起こる危険性が生じると、通信を止めざるを得なくなる。しかし、本当は止めなくても良かったのに……といった判断ミスや、人為的な原因ではない、機器が勝手にもしくは間違って動作した……といったことも考えられる。今後は、そういう状況にどう対処するのかといった問題も、セキュリティの範疇に入ってくるのではないでしょうか。

神田　様々な問題が想定されるなか、安全・安心なインターネット環境を提供しなければなりませんが、その際、世の中に対する便益と負荷のバランスにも配慮が必要だと思います。

完璧な対策はないが……

――脅威・リスクから企業をどうやって守るのか。対策方法を教えてください。

山井　「こうすれば大丈夫」という完璧な〝解〟があるわけではありません。しかし、具体的な対策は常に考え続けなければなりません。我々はそういう使命感を持って仕事をしているし、それがセキュリティ対策の基本姿勢です。

解決策が進化すれば、脅威も進化します。よって、我々の技術的手段を改善していくと同時に、「これで大丈夫です」と言えなくなっている現状をお客さまにもご理解いただき、セキュリティに関する意識・知識のレベルをあげていく取り組みが必要だと感じています。サービスを提供したらそれで終わりではなく、お客さまに多少のご迷惑をおかけすることがあっても、セキュリティ対策を向上させるために一緒に考えていきたいです。

神田　最近のセキュリティ対策のトレンドは、「多層防御」と「侵入を前提とした対策」です。これは、単独で完全に防御できる仕組みはないため、複数を組み合わせて予防措置を講じつつ、外部から侵入され得ることを前提として、侵入されても短時間で対処し、被害を最小限に食い止めるための仕組みを構築しておこうというものです。（上図参照）

日々の企業活動を通して、多種多様な〝ログ〟が集積されていきますが、一つ一つのログの関連付けをして、そこに意味を見出すことにより、具体的にどんな問題が起きているのか、短時間で判断できるようにするのです。昨今、こうした相関分析を可能にする基盤の構築案件も非常に増えています。

IIJでは昨年より、インシデントの検知から、相関分析の実施、その対処まで、お客さまに代わってセキュリティ運

用を行なう、統合セキュリティ運用というソリューションを提供しています。

「IoT」の時代には、デバイスの数に比例してログの量も膨大になります。すると、それを分析する人が大勢必要になる。つまり、セキュリティに携わる人材が大幅に不足するという次の課題も克服していかなければなりません。ちなみに、数字のうえで八万人、質的には一六万人のエンジニアが不足しているとの調査も出ています（IPA試算）。

セキュリティ情報の取り扱い

――セキュリティ関連の情報はどのように収集・活用していますか？

山井　メーカやセキュリティベンダ、ERCSIが社外から得る情報、業界団体や政府系組織など、様々なところから入ってくる情報に敏感に反応しています。脆弱性情報が出れば、その日のうちに社内に展開し、サービスに影響があるか否かを調べて、対処が必要であれば即日実施しています。

当然、そうした情報はお客さまにもお知らせしますが、お客さま毎に温度差があり、なかには「これは大丈夫だろう」と受けとる方もいらっしゃいます。しかし、そうした対応が続くと、脆弱性や脅威が広がってしまうので、IIJが社内的にやっているような対応を社外にも広めていきたいと考えています。

神田　多くの情報が溢れており、それらを誰かが適切に判断しなければならないということで、IIJでは専門家の視点から定期的にアドバイスするといったことも行なっています。

また、大手企業や金融機関では、自社で人材を確保して、SOC（セキュリティ・オペレーション・センター）やCSIRT（コンピュータ・セキュリティ・インシデント対応チーム）を立ち上げるといった動きも増えていますが、これらを側面から支援することにも対応しています。

表に出てこない情報

神田　注意が必要なのは、セキュリティ関連の情報は全てが表に出ているわけではない、ということです。つまり、公表できない事故・事件がかなりある。

IIJでは、ERCSIが各方面との接点を活かしてそうした生の情報を仕入れて、活用の方法を検討しています。大手企業のセキュリティ担当者なら、同業者同士の横のつながりから情報を得ている方もいるでしょう。

山井　例えば、ある企業で「こんなトラブルは恥ずかしくて表には出せない」といったことが起こったとしても、もしかしたら他の企業でも同じことが起こるかもしれない。言い換えると、貴重な情報・経験が闇に葬られてしまうと、本当の意味でのインターネット上の脅威が再び起こるかもしれないのです。

情報を得る側も、「あそこのサービスはダメだ」と言うのではなく、「こういうことをやるとこうなるのか」と、情報を真摯に受けとめて、一緒に考えることが大切だと思います。共有すべきものは共有し、外に漏らしてはいけないことは他言しない――セキュリティに関わる人には、そういう姿勢を堅持してほしいです。そうした横のつながりは、モラルが少しでも崩れると、「もう二度と情報を出さない」ということになってしまうので、責任感とリテラシーが必須です。

今後、セキュリティを守っていくためには、情報を共有できるコミュニティを大切にして、出せる（出すべき）情報／公表・公言できない情報を精査しながら、貴重な知見をお互いのセキュリティ対策に役立てていく――そういう方向性が求められると思います。

そうしたコミュニティに対しては、IIJでも側面支援を行なって、情報交換の場をつくるなど、サポートしていきたいと考えています。

今後のセキュリティ戦略

神田　これまでIIJは、セキュリティ対策の実装から運用までを、もっとも得意とする事業領域としてきましたが、昨今は、各企業が対策を計画・立案する段階から参画し、現状の分析・可視化を通して、それぞれの要件に合った具体策をコンサルティングする機会も大変増えています。

特に近年、対処すべき領域が急速に広がって、お客さまのほうでも「何から手をつけていいのかわからない」といった状況になりつつある。そこを一つ一つひも解きながら、具体的かつ個別のテーマに選り分けて、優先順位をつけていく。セキュリティ対策の内容はお客さまそれぞれですから、計画段階から個々のケースに即していくことがますます重要になっています。

山井　これからのIoT時代、ネットワークの規模が飛躍的に拡大し、リアルタイムの対応が必要となるなか、人材不足という大きな課題に対処していくためには、パラダイムシフトが必要だと考えています。IIJでは、それに対する一つの有望な選択肢としてAI（人工知能）にも注目をしています。

――セキュリティを守っていくためには、業界業種の垣根を越えた情報共有と、対策技術の不断の改善が不可欠だということですね。本日はありがとうございました。●

企業を守る手法とは？

～CSIRTを立ち上げよう

セキュリティを脅かすインシデントの発生を予防し、
万が一、インシデントが発生した際は、その対応にあたる組織“CSIRT”。
本稿では、その活動内容を紹介する。

IIJソリューション本部 セキュリティソリューション部
セキュリティソリューション課 セキュリティコンサルタント
片桐 卓

セキュリティの世界では、最近出てきたバズワードらしき言葉（キーワード）が飛び交っています。

例えば「SIEM」、これは複数のセキュリティセンサー（ファイアウォールやWEBプロキシなど）から出力されたログを集積し相関分析することで、セキュリティインシデントの発生を検出するという代物です。これまで「シーム」と呼んでいましたが、昨年末に渡米する機会があり、その際に出会った北米のセキュリティベンダの方からは「エス・アイ・イー・エム」と言われたりしました。国内の外資系企業のお客さまにも同じように言われたことがあります。「CISO」は、何と読むと思いますか？日本ではおそらく普通に「シー・アイ・エス・オー」でしょうが、これも違いました。「シー・ソー」と読みます。「CSIRT」は普通に「シーサート」です。

CSIRTとは？

CSIRTは「Computer Security Incident Response Team」の頭文字をつなぎ合わせた言葉で、組織内の情報セキュリティ問題を専門に扱うインシデント対応チームを指します。

おもな役割として、①脆弱性対応（パッチ適用など）、②緊急対応（インシデントハンドリング）、③事象分析、④普及啓発、⑤注意喚起、⑥その他のインシデント関連業務（予行演習など）があります。①～④については、部署内やプロジェクト内でよく行なっていることだと思いますが、CSIRTはこれらを企業レベルにまで発展させ、組織として成立させたうえで活動していこうというものです。

CSIRTが担う役割は、情報の集約および伝播をよりシームレスに行ない、最終判断を行なうことである、とお考えください。もう少し具体的な言葉で表すと、CSIRTは、①適切な対応と有効な対策を実施することにより、インシデントの被害を最小限にする。②インシデントの発生・再発を予防するための活動を行なう。この二つに集約されます。そしてこの活動を行なう理由は、企業の重要資産または利益を保護するために他なりません。ですので、CSIRTを組織する際は、企業として守るべきものは何か？ という点を明確にしておく必要があります。企業活動のなかで取り扱うのは、個人情報、新商品の開発データ、臨床試験結果、設計情報（CAD）など様々ですので、ぜひ、この機会に原点へ立ち返って、企業として守るべきものをご確認いただくことをお勧めします。

CSIRTは、企業それぞれに適切な構造が必要となります。というのは、従来の組織構造、例えば、システムオーナーの所在、情報システム子会社の有無、企業体系といった要因により、一定の組織構造ではなかなか定着しづらいためです。一般的な構造としては、専任制／兼任制／非常時制／集中型／調整型／分散型などがあり、現在の組織構造を鑑みながら適切な構造を選定するといいでしょう。

CSIRTとSOC

CSIRTに関して、一点気を付けていただきたいことがあります。CSIRTとSOC（Security Operation Center）を一つの組織に包含しないことです。SOCはCSIRTと同様の言葉もしくは機能と思われがちですが、それは誤りです。SOCはCSIRTが取り扱うインシデントに対して、高度な解析や迅速な対応に必要な技術領域を持った機能組織です。また、内製化できればそれに越したことはありませんが、内外製分析を行なえば、必ず外製化の検討が必要になりますので、CSIRTとSOCとは混ぜずに、組織化の検討を行なっていただきたいと思います。社内では「まぜるな危険」とよく言っています。

少し話がそれますが、SOCについておきます。IIJにはSOCと類似した組織としてNOC（Network Operation Center）があります。NOCは、ネットワーク設備に関する障害アラートをトリガーとして保守交換作業や設定変更などを行ない、二四時間三六五日稼働し続ける組織です。一方、SOCは、セキュリティに関するインシデントをトリガーとして定められた手順対応を行ないます。また高度なものになると、一次調査や分析、シグネチャーチューニング、マルウェア解析などを行ない、二四時間三六五日稼働する組織になります。

NOCやSOCは、対応についての判断は行ないません。判断する組織はCSIRTになります。よって、SOCなどを外製化したとしても、最終判断など社内組織として持っておかなくてはならない機能があることを覚えておいてください。

もう一つ、よく出てくる言葉「相関分析」を説明します。相関分析とは複数のセンサー（ファイアウォールやWEBプロキシなど）から出力されるログを時系列に並べ、二つ以上のログの相関関係から、クライアント端末やサーバの振る舞いを検知するものです。

CSIRTを立ち上げるにあたって

CSIRTのはじめの一歩を踏み出そうとしている、または踏み出したいと考えている皆さまのなかには、何から手を付けていいのかわからない方も多いかもしれません。ここでアドバイスしますと、最初の一歩は、電話番号でもメールアドレスでも構いませんので、「社外および社内からのインシデントに対して、受付窓口を開設する」ことです。窓口を開設してインシデントを扱うことで、自社CSIRTにとって、①必要な活動内容、②組織体制、③インシデント対応プロセス、④エスカレーションフローが見えてくるはずです。またIT資源的には、①スキルセットを持った人材、②インシデントハンドリング用の管理設備、③インシデントを未然に防ぐための防御設備、④インシデントをいち早く検知するためのセンサー設備など、様々なものが必要であると思えてくるでしょう。

全てを最初から用意しようとすると、CSIRTを作り上げるうえで技術的な要素だけでなく、組織やマネージメントの形成も必要となり、かなりの労力を要するので、最初は必要最小限による立ち上げを行ない、徐々に肉づけして、拡充していくことをお勧めします。

二〇一五年四月一日現在、日本シーサート協議会に加盟している企業は、八三チームになりました。これまでは、IIJのようなインターネットサービスを提供する側の企業が多かったのですが、最近、エンドユーザの活発な参入があり、金融機関、生損保、情報サービス、監査法人、製造業など、幅広い業種業態から加盟があり、今後も増えると見ています。

最後に、CSIRTをひと言でいうと、企業をセキュリティインシデントから守る最後の砦となります。これまで可視化できていなかったものや、軽視していたものが非常に重要なインシデントとなり、企業に大きな負荷（金銭的にも人的資源的にも）をもたらすことも出てくるでしょう。ですが、どうか諦めずにCSIRTを立ち上げて、企業におけるセキュリティインシデントに立ち向かっていただきたいと思います。●

ISPから始まったセキュリティサービス

IIJはエンジニア集団から始まった会社で、技術に対する探究心が強く、
そのマインドは今日にも受け継がれている。
そうしたエンジニアが開発から導入・運用まで携わっているのが、
IIJのセキュリティサービスの特徴である。

IIJサービスオペレーション本部
セキュリティサービス企画推進室
小前田 佑介

IIJサービスオペレーション本部
サービスサポート部 セキュリティサービス課
木島 章

インターネット接続サービスは、つながる（情報を漏れなく迅速に届ける）ことを提供するのに対し、セキュリティでは時に、通信を遮断する（不要なものを届けない）ことも機能として提供します。

IIJのセキュリティサービスの歴史

これまでIIJは、一九九四年に国内で初めて商用ファイアウォールサービスを提供して以来、インターネットの利用用途の変化に応じて、世の中で必要とされるセキュリティサービスを開発・提供してきました。

また、過去のDDoS攻撃への対応経験などを踏まえて、今後増えるであろう攻撃からお客さまのシステムを守るために開発したのが、二〇〇五年リリースのDDoS対策サービスです。DDoS対策では、不正なトラフィックがお客さまのインターネット回線へ流入する前段で排除することが重要ですが、こうした防御が可能なのは、IIJがISPとしてバックボーンの運営を行なっているからです。

また、セキュリティ対策における大きな変化として、IPv6の利用が徐々に進んでいる点が挙げられます。IIJでは一九九九年からIPv6商用実験サービスを開始しており、早い段階からIPv6の普及に取り組んできました。

IPv6の環境が広がることで、セキュリティ対策も変化します。例えばIPv6のみの環境になれば、ファイアウォール機器でのアドレス変換機能（NAT）は基本的に必要なくなります。その結果、クライアント毎に付与されたIPアドレスをそのまま使ってインターネットの世界と通信することになり、境界防御機器としてのファイアウォール自体の役割が見直されるかもしれません。

IPv6の普及にはまだ時間が必要ですが、IIJではIPv6の普及・促進を見据えて、IIJマネージドファイアウォールサービス、IIJセキュアWEBゲートウェイサービスなど、複数サービスでIPv6対応を進めています。

サービスに必要な機器はレンタルで利用できます。それらの機器は、IIJが各ベンダやメーカとの信頼関係により収集した情報や、メーカ毎の製品の特徴などを考慮し、メーカやベンダと対等に交渉して、不具合の修正や機能の改善などを行なっています。これらは、お客さまに安定したサービスを提供するための重要な構成要素となっています。

こうした製品は、カタログ上のスペックだけに頼らず、実際に通信を流して取得した測定結果をもとに、安定したサービスを提供できる範囲の性能を、検討時に指標としてお客さまに提示しています。

同じ製品を同じ組織（サービス部門）で大量かつ長期間運用するなかで得られたデータは、IIJサービスの貴重な財産であり、お客さまには見えない部分で生かされています。

サービスの開発

新規サービスの開発は各提供機能に対し、IIJとして「こうあるべきだ」という考えを軸に、お客さまが要望する機能とIIJが考える理想をいかに共存させるかを考えながら進めています。費用は、お客さまにとって重要な検討項目となるため、サービスを提供・維持していくコスト面は市場価格などを加味して検討を行なっています。リリース済みの既存サービスについてもお客さまの利便性向上や市場動向を調査しながら、必要な機能の追加や安定性の向上に努めています。

さらに、セキュリティ分野でIIJがイニシアティブをとるために、論文の調査、先進的な技術の評価・研究なども合わせて行なっており、どのようなかたちでサービスに取り込めば、より良いサービスを提供できるのか、日々検討しています。

サービスの導入

一つの案件に対して、セキュリティ設計担当者と、サービス設計・設定・デバイスキッティングの各タスクの担当者を決めて対応しています。各タスクで求められる能力は異なるため、より専門性の高いエンジニアを育成することで、構築時の品質向上を図っています。

例えばIIJマネージドIPS／IDSサービスでは、セキュリティ設計担当者が、導入作業後に誤検知や過検知が発生しないよう期間を決めてインシデント分析を行ない、結果をレポートしています。IIJ DDoSプロテクションサービスでも、お客さまシステムの通信傾向を分析したうえで、各種機能の利用有無や閾値をレポートしています。

お客さまの環境毎に分析結果は様々であり、案件毎に状況を確認し、お客さまから得られた情報や要望に応じてセキュリティの観点から検討した設定値をご提案しています。

サービスの運用・サポート

IIJのセキュリティサービスは非常に多くのバリエーションがあるため、一つのサービスを専任で担当する者もいれば、複数のサービスを横断的に担当する者もいます。担当するサービスにより必要なスキルセットは異なりますが、セキュリティサービスのサポート担当者同士で緊密な連携をとり、複数サービスをご利用いただいているお客さまには、各サービスの情報をもとにトータルでサポートを行なっています。

IIJには各分野の専門家がいるので、「ちょっと電話で聞いてみよう」といったことが日常的に部門を跨いで行なわれており、それぞれの分野から意見をもらいやすい環境は、サービスのサポートにも活かされています。

お客さまに満足いただけるサポートを行なうためには、お客さまとのコミュニケーションはもちろん、社内でのコミュニケーションも重要です。社内にある〝人が持つ情報〟をいかに集約して、お客さまへフィードバックできるかを意識しながら、チームとして対応するように努めています。

サポート品質を向上させるための取り組みとして、開発部門と連携して内製ツールの作成による自動化なども行なっています。人間が得意な部分と機械が得意な部分を見極めつつ、満足度の高いサービスサポートを提供できるよう改善に取り組んでいます。

バックグラウンドにある監視システム、ログ分析システム、レポーティングシステムなども、安定稼働のために日々メンテナンスを行ない、安定性の向上、処理能力の向上、セキュリティへの確実な対応を心がけています。特にログ分析システムで扱うログは膨大なので、数十億レコードを解析・保存するために高速処理技術や大容量ストレージの利用なども進めています。

これらの取り組みでは、お客さまに実際にご覧いただける効果を出すことはむずかしいですが、地道な努力を重ねてサービス品質を向上させています。●

人と空気とインターネット

人間と人工知能

IIJイノベーションインスティテュート
代表取締役社長
浅羽 登志也

近年、人工知能が急速に進化しており、
なかには人間を超える
能力を獲得したものもある。
今後、人工知能は
どのような方向へ進むのか？
人間との共存共栄は可能なのだろうか？

先日グーグルが、ビデオゲームのプレイ方法を自分で学習しながら上達することができる人工知能を開発したと発表しました。

この人工知能ソフトウェアは、グーグルが昨年買収したDeepMind社のディープラーニング（深層学習）技術を活用したものです。この技術を使うと、人間のように学習しながら特定のスキルを身に付けることが可能な人工知能を実現できるそうです。グーグルの開発した人工知能は、Atari 2600というゲーム機の四九種類のゲームのうち二九のゲームで人間のプロのゲームテスターを上回るパフォーマンスを見せ、四三のゲームで既存のゲームをプレイする他の人工知能を上回ったそうです。

最近、このような学習型の人工知能が注目を集めています。人間が行なう様々な知的活動の全てをプログラミングすることは、実質的に不可能だと考えられますので、あらかじめ全てを教えるのではなく、人間と同じように試行錯誤を繰り返しながらコンピュータ自身に学習をさせて、様々な領域の知識や問題解決能力を獲得させようということなのでしょう。

しかし、Atari社のゲーム機は一九八〇年代に流行ったものですので、三〇年前のシンプルなゲームを学習できるようになったに過ぎません。現実の複雑な問題に対応するには、現実社会を構成する多くの概念を理解し、そこから課題を見出して、解決方法を見つけるという、人間が普通にやっていることができなければなりません。今回の発表を聞く限りでは、コンピュータが人間と同等の知的レベルに到達するには、まだまだ長い道のりが必要だと感じました。

昨年末、スティーヴン・ホーキング博士は、あるインタビューで「完全な人工知能を開発できたら、それは人類の終焉を意味するかもしれない」と発言しています。仮にコンピュータが人間の知能に追いつくようなことが起これば、それ以降、コンピュータは人間の意志とは無関係に自分の意志により、しかももの凄いスピードで勝手に進化していくでしょう。すると、ゆっくりとしか進化できない人間は、コンピュータに二度と追いつけなくなる、というのです。つまりその時点で、科学技術の進歩は人間ではなく人工知能が司ることになり、その先何が起こるかは、人間には予測不可能になるのです。これを「シンギュラリティ（技術的特異点）」と呼ぶのですが、シンギュラリティは二〇四五年頃に起こる、という予測もあります。今から三〇年先の未来です。

人工知能は人間を超えた？

たった三〇年で人間に追いつくはずはない、と思いたいところですが、すでに追い越されつつある分野もあります。IBMの「ワトソン」というシステムは、二〇一一年に米国のJeopardy!というクイズ番組で、人間のクイズ王と対戦し、勝利しています。また、長い歴史を持つコンピュータ将棋では、二〇一二年に開催された将棋電王戦で、前年のコンピュータ将棋世界選手権で優勝したソフトウェアが、米長邦雄永世棋聖を破っています。その後、二〇一三年の第二回電王戦は人間の一勝三敗一引き分け、二〇一四年の第三回は人間の一勝四敗と人間が負け越し続けています。今後、人間はコンピュータに勝てないのでしょうか？

クイズや将棋以外の多くの分野でも、人間の知力がコンピュータに歯が立たなくなる状況がどんどん積み重なっていけば、ホーキング博士の鳴らす警鐘も、あながち大げさなものとは言えなくなるでしょう。コンピュータが人間の言うことを聞かなくなり、勝手な判断で世の中を動かし始めてしまったら……なんて、子供の頃、SF小説で読んだような世界がすぐそこまで迫っているのかもしれません。

名人、王位、王座、棋聖のタイトルを持つ羽生善治四冠は、コンピュータ将棋に関するインタビューで「昨年の電王戦で出た、人間には違和感があって指せない斬新な手が、その後棋士に流行したり、計算力だけでなく創造性や独創性も発揮し始め、人間が学び始めている」と答えています。これはつまり、人間の思考プロセスには何らかの死角や盲点があり、その道のプロでも気がつかなかったような斬新な解を、人工知能なら見つけられる可能性を示しています。人工知能をうまく使えば、人間の視野や、思考の幅・アイデアを広げるためのツールとして活用できるというわけです。

そういう視点で世の中を見渡すと、地球温暖化、人口や食糧問題、終わりが見えない戦争やテロなど、人間にはもはや解決が不可能に思えるような課題が溢れています。人工知能をうまく活用することで、人間には盲点になっていて解けなかった問題に解決策が見出され、人類の進歩が加速すれば、それは素晴らしいことではないでしょうか。

しかし、テスラモーターズのCEOイーロン・マスク氏は昨年トークショーで、例えば、スパム削除をミッションとするロボットが「スパム削除のためには人間を削除するのが一番だ」などと判断してしまったら、人間を削除する殺人ロボットが生まれる可能性もあるとの見解を述べ、人工知能開発を安易に進めることの危険性を訴えました。そして同氏は今年一月、人工知能を人間にとって有益なものに保つ研究支援に一〇〇〇万ドルを寄付したと発表しました。人工知能は人類に多大な恩恵をもたらす可能性があるからこそ、そのデメリットや危険性をあらかじめ検討し、安全にコントロールするための技術の開発に投資を行なうという考えは、リーズナブルに思えます。

科学技術の進歩により、人間は肉体的な能力の限界を遥かに超えた力を獲得しました。そのおかげで高度で便利な文明社会を築くことができた反面、力の巨大さゆえに、何らかの事故や想定外の出来事が起こり、力に対するコントロールを失ってしまったら、計り知れないほど大きな被害を被ることにもなりかねません。仮にシンギュラリティが起こり得たとして、知的能力の面で人間を超えるものが現れたら、はたして知力で劣る人間は、それをコントロールできるのでしょうか？

しかし、仮にコントロールできないとしても、人間より賢くなった人工知能がわざわざ人類を滅ぼしたりするでしょうか？　相手はコンピュータですから、人間を殺して食べたりはしないですし、人間が人工知能を攻撃するようなことがなければ、うまく共存できるように思います。むしろ、人間がコントロールできる人工知能があったりすると、戦争やテロのための兵器として使われるに決まっていますから、そちらのほうがよほど危険です。そう考えると、人工知能には人間がコントロールできる機能など付けないほうが、世界は平和になるのかもしれません。●

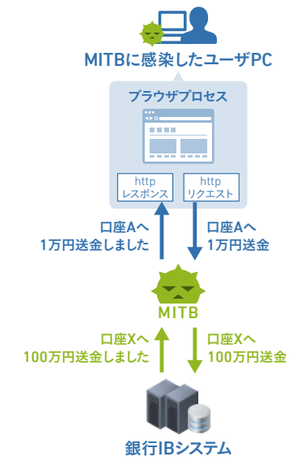
イラスト／末房志野

Technical Now

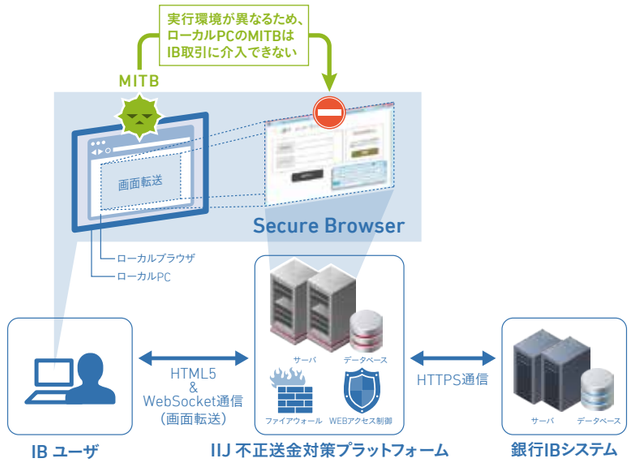
IIJ不正送金対策ソリューション

IIJ 金融システム事業部 プロフェッショナルサービス部長
前川 陽一

インターネットバンキングで不正送金被害が急増するなか、
銀行には早急かつ抜本的な対策が求められている。
本稿では、既存の各種対策を整理したうえで、
IIJ不正送金対策ソリューションの有効性とメリットを解説する。



通信データ改ざん型 “MITB” 攻撃イメージ



IIJ 不正送金対策ソリューションイメージ

インターネットバンキング（以下、IB）利用者の口座から預貯金が不正に別口座に送金される被害が急増しています。警察庁の資料によると、平成 26 年上期の被害総額は前年同期比 8 倍超の 18 億 5200 万円、件数は前年同期比 6 倍超の 1254 件となっています。

昨年 5 月には、ワンタイムパスワードを導入している銀行で、利用者が正規の ID・パスワードでログインしているにもかかわらず、気付かないうちに不正送金される被害が発生し、世間を騒がせました。銀行もいろいろ対策を打っていますが、イタチごっこが続いており、決定打がない状況です。今回は不正送金の攻撃手法とその対策を整理したうえで、IIJ 不正送金対策ソリューションの有効性について説明します。

不正送金の攻撃手法

不正送金の攻撃手法は次の 2 つに大別できます。

①情報盗み取りからのなりすまし型

デザインを似せた銀行の偽サイトへメールなどによりユーザを誘導し、ID・パスワードや乱数表情報などの本人認証情報を入力させるフィッシングと呼ばれる手法や、ユーザパソコンをキーロガーや遠隔操作などのウイルスに感染させて盗み取った情報を用い、本人になりすまして不正送金を行ないます。

②通信データ改ざん型

正規の ID・パスワードでログインしたユーザのパソコン画面情報や入力情報を改ざんし、不正送金先口座にユーザの意図しない大きな金額を送金させる手法です。この手法はマン・イン・ザ・ブラウザ（以下、MITB）攻撃と呼ばれ、ユーザパソコンが特定の通信データをトリガーに発動するウイルスに感染することで起こります。MITB 攻撃の特徴は、正規のユーザが ID・パスワードを使って操作しているにもかかわらず、知らないうちに情報が改ざんされるため、ユーザも銀行側もすぐに不正に気付かない点です。

各種対策と限界

なりすまし型攻撃対策は、本人認証情報の盗み取り防止となりすまし防止で構成されます。盗み取りに対しては、ウイルス対策ソフトウェアや、サイトの真偽を判別しブラウザに表示するフィッシング対策ソフトウェアの導入が有効です。これらソフトウェアを無償提供している銀行も多数あります。しかしながら、セキュリティに対するユーザ意識が様々であることや、セットアップの煩雑さなどにより、必ずしも普及していないのが現状です。

なりすまし防止は、ランダムパスワードを毎回生成するワンタイムパスワードを用いた本人認証が有効な対策となります。近年、ワンタイムパスワード生成カードをユーザに配ったり、携帯メールに通知するといった仕組みの導入が進んでいます。また、銀行システム側でユーザの IP アドレスやキーボードタッチの癖などを記録し、アクセスがあった際に突き合わせて、通常と異なると判断された場合は、取引を停止するリスクベース認証と呼ばれる対策を取り入れている銀行も多数あります。

次に、通信データ改ざん型 MITB 攻撃の対策として日本で多く採用されているのは、MITB 攻撃に特化した対策ソフトウェアの導入です。パソコン内で MITB 攻撃に類似した動作をするプロセスを検知し、停止させるのが基本的な機能です。インストールするタイプやブラウザのアドオンとして提供されるタイプなど複数の製品が存在し、銀行による無償提供も行なわれています。しかし、対応する OS やブラウザが限定的であったり、パソコンに与える負荷が大きいことなどから、広く普及するには至っていません。

日本より早い時期に MITB 攻撃による被害が発生していた欧米では、振込先口座番号などの情報をもとに生成したワンタイムパスワードにより取引を完了させる取引認証と呼ばれる対策を導入している銀行もあります。しかし日本では、導入コストやユーザ利便性の低下といったデメリットのために、本稿執筆時点で導入している銀行はありません。*

IIJ不正送金対策ソリューション

MITB 攻撃の登場により IB に対する信頼が揺らぐなか、IIJ はブラウザ実行環境分離と呼ぶ新しい方式で MITB 対策ソリューションを開発しました。

これは、「ユーザのセキュリティ意識や IT リテラシーは様々であり、全ての IB ユーザのパソコンを安全な状態に保つことは不可能である」という考えにもとづき、「ユーザパソコンがウイルスに感染しても影響を受けないよう、IB アクセスのためのブラウザを別な環境で動作させる」ソリューションです。その特徴をいくつか紹介します。

特徴 1：MITB の脅威を根絶

ユーザパソコンは、画面表示およびキーボードマウスの入力装置としてのみ動作する（シンクライアントをイメージしていただくとわかりやすいでしょう）ため、ウイルスの影響を受けません。また、受信するデータは画像データのため、文字改ざんの脅威がありません。

特徴 2：多角的なセキュリティ対策

クラウド環境は、仮想アプリケーション技術により、マイクロソフトの Internet Explorer（以下、IE）のみが動作するよう構成されています。IE は使用するたびに初期化され、アクセス履歴などを含めたユーザ情報はいっさい残りません。IE は特定サイト以外到達できないよう制限するなど、DDoS 攻撃の踏み台として利用されるリスクも排除しています。またこの環境は、ファイアウォールや WEB アクセス制御など、IIJ の堅牢なセキュリティ対策で守られています。

特徴 3：普及障壁の低さ

ご利用に際して専用クライアントソフトウェアを必要としません。最新の WEB アプリケーション記述の枠組みである HTML5 を採用することで、IE、Firefox、Google Chrome、Safari などの汎用ブラウザから利用できます。インストール不要・登録不要で、ソリューション導入前と同等のユーザビリティを実現します。

IB システム側も、ソリューション導入にあたり改修の必要がありません（導線のためクラウド環境へのリンクボタンをサイト内にご用意いただく必要があります）。

もうひとつ、IIJ 不正送金対策ソリューションには副次的なメリットもあります。自行 IB アクセスを IIJ 不正送金対策ソリューション経由に限定することで、IB システムがサポートするブラウザをひとつに統一できます。これにより、複数のブラウザやバージョンで実施していたリグレッションテストなどの IB システム維持管理工数を大幅に削減できます。

今後の展開

今後のソリューション拡張における最優先の課題は、スマートフォンやタブレットといったキーボードレス端末への対応です。具体的には、ユーザビリティを損なうことなく、ソフトウェアキーボードを使えるように改良する必要があります。今後は、スマートフォンを狙ったウイルス攻撃が増加すると予想され、ユーザから早急な対応を求める声が多数届いています。将来的には、IB アクセスチャネルを統合するようなセキュリティサービスに育てていきたいと考えています。●

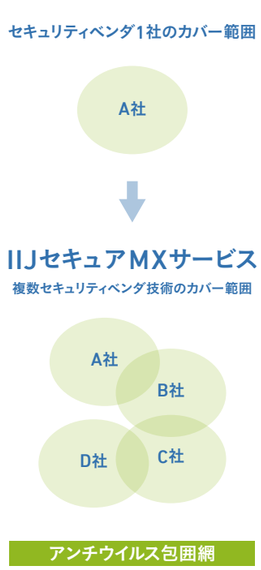
＊みずほ銀行が2015年3月下旬より取引認証を導入する旨を発表しています。

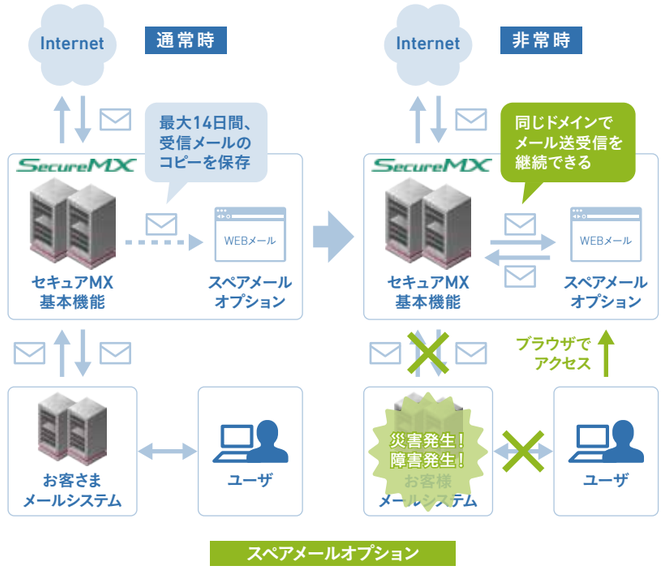
Technical Now

パワーアップした IIJセキュアMXサービス

IIJ プロダクト本部 プロダクト推進部 企画業務課長
久保田 範夫

日本の企業でもっとも多く採用されている
SaaS型の統合メールセキュリティ対策「IIJセキュアMXサービス」が、
セキュリティやBCP対策の面で一段とパワーアップした。
ここではその概要を紹介する。





インターネットが普及し、電子メールがビジネスで担う役割は年々高まっています。それにともない、標的型攻撃メール、ウイルス、フィッシング、スキャムなど、様々なメールを用いた攻撃も増加しており、メールシステムのセキュリティ対策強化や、災害・障害といった万が一の事態に備えたBCP対応が急務となっています。今回は、この3月にパワーアップした「IIJセキュアMXサービス」を通して、これらの課題へのアプローチについて述べます。

アンチウイルスの強化

脅威メールへのセキュリティ対策強化として、このたび、IIJセキュアMXサービスに標準搭載されているアンチウイルス（以下AV）のエンジンをクワッド（4）エンジンに強化しました。

一般に単一セキュリティベンダのAV技術だけでは、流行中の新たなウイルスに対する検知率が低下してきている、と言われています。昨年、あるセキュリティベンダの幹部が「単一のAV技術の検知率は45パーセント程度である」という衝撃の事実を公表しました。セキュリティベンダ1社が収集できるウイルスの情報網やソースは限られており、これはどんなに著名なセキュリティベンダでも同じです。セキュリティベンダ同士でウイルス情報を共有できれば、カバー可能な範囲も広がるのですが、各社のビジネスの都合上、実現性は低いと考えられます。

IIJでは、従来から提供している複数セキュリティベンダのAV技術をさらに増強し、ウイルス包囲網を劇的に広げました。IIJセキュアMXサービスの基本機能として備わっている2種類の商用AVエンジンに、市販されていないクラウド専用AVエンジンを2種類加え、合計4種類のAVエンジンを搭載することで、クワッド（4）エンジンによるウイルス検査が可能になりました。また、オプションであるアドバンストアンチウイルスオプションを追加することで、合計5種類のAVエンジンによる多段検査にも対応します。

アンチスパムの強化

近年、メールによる脅威も進化しており、アンチスパム（以下AS）に求められる機能は年々増加し、従来の「迷惑メールを検知する」だけでなく、標的型攻撃メールに代表される様々な脅威メールをAVとは別のアプローチでブロックする必要性が生じてきました。

IIJセキュアMXサービスでは、従来から単一セキュリティベンダの技術に頼らず、適材適所に複数ベンダのASエンジンを採用すると同時に、IIJ独自のASエンジンを追加したマルチレイヤードフレームワーク構造で多層検知から導き出された総合判定結果によってのみ得られる、「高い検知率」と「低い誤検知率」の共存を実現してきました。市販されているアプライアンス製品とは異なり、スパム技術の流行り廃りに応じて判定エンジンの組み換えを行なったり、有効な新技術を追加して継続的に進化させることで、常に最新の対策技術を提供しています。

このたび、脅威メールへの防御力向上を目指して、新ASエンジンを基本機能として追加しました。この新エンジンは長らくIIJでテスト、検証を重ねてきたもので、様々なチューニングを施したうえでようやく高い精度基準を満たし、既存のASエンジン群に追加されることになりました。これにより、新しいメール脅威に対して、さらなる効果が発揮されると期待しています。

メールシステムの災害、障害のインパクト

東日本大震災から4年が経過しました。震災後、多くの企業がビジネスにおけるメールの重要性を再認識し、DR対策、BCP対応の検討を進めましたが、実際にメールシステムをもう1セット構築・運用するには、その対策に約2～3倍のコストがかかるとされ、万が一の保険と考えても、コスト負担があまりに大きく、検討段階で計画自体が頓挫してしまうケースも多かったようです。

大規模災害だけでなく、障害対策にも備える必要があります。ハードウェアはいつか必ず故障します。実際に機器が故障したら、復旧までの時間はいったいどのくらいかかるでしょうか？　ハードウェア故障が起きてから、保守ベンダが駆けつける時間、パーツや機器の交換作業にかかる時間、設定の再投入、稼働テスト、データをバックアップから戻す時間など、最短で数時間、長ければ数日間、メールシステムを利用できない事態が想定されます。

自社構築に代わって昨今ブームとなっているクラウド型メールサービスなら、障害の心配はないでしょうか？　そうではありません。現状、グローバルのクラウドサービスの安定性に対し、過剰な期待が寄せられています。クラウドサービスに移行後、認証システムの障害からサーバ、ディスクなどクラウドの裏側で起こる数々の障害に遭遇し、日本のビジネスアワーにメールが数時間にわたって利用不能に陥ったという事例も報告されています。

つまり、自社構築、クラウドにかかわらず、災害、障害に備えたメールシステムのバックアッププランの検討は必須なのです。

BCPのためのスペアメールオプション

今回ご紹介するのは、IIJセキュアMXサービスのスペアメールオプションです。お客さまがメインで利用しているメールシステムが災害、障害など、何らかの事由により長時間利用できなくなった際、スペアメールオプションで提供されるWEBメールを通じて、メールの継続利用が可能になります。

スペアメールオプションは、お客さまが構築したメールサーバだけでなく、Office 365、Google Appsといったクラウドメールシステムでも利用できます。平常時は受信メールのセキュリティ対策を担いながらお客さまメールシステムにメールを配送するとともに、契約されたプランに応じて最大14日間分のメールを容量無制限でIIJセキュアMXサービス上で保管します。

災害、障害などによりメールシステムが利用できない非常時は、スペアメールのWEBメールにアクセスすることで、保管されている日数分の受信メールが確認でき、また新規メールを送信・受信できます。

本オプションを利用することで、多額の費用がかかるバックアップ用のメールシステムを自社構築する場合と比べて、設備投資や運用コストを大幅に抑えることができます。

SaaS型で提供している統合メールセキュリティサービス、IIJセキュアMXサービスでは、脅威メールからの防御、誤送信対策、情報漏えい対策、BCP対策といったメールシステムに不可欠な多くの強化を低コストで実現できますので、この機会にぜひご検討ください。●

Internet Trivia

インターネット・トリビア

SNSの迷惑メッセージは友達からやってくる

IIJ プロダクト本部 プロダクト推進部
企画業務課 リードエンジニア
堂前 清隆

電子メールアドレスを持つと、何かしらの「迷惑メール」がやってくるというのが、いつの間にか当たり前のことになってしまいました。スマホのメールアドレスでも、ISPが提供するメールアドレスでも、無料メールアドレスでも、気がつくと迷惑メールがやってきて、メールボックスがあふれてしまいます。迷惑メールフィルタを使えば、ほとんどの迷惑メールは見ずに済みますが、あまり気分のいいものではありません。

同じような行為が、TwitterやFacebookなどのSNSでも発生しています。SNSの多くは無料で利用できることを悪用し、アカウントを大量に登録して、無差別にメッセージを送りつける業者が現れました。SNSサービスではこのような利用は規約で禁じられているため、サービス提供者によりアカウントが順次停止されていますが、次から次へと新規のアカウントを取得して、迷惑メッセージを送信するのです。

こうした状況に対しSNSサービスによっては、「あらかじめ友達登録をしている間柄でないとメッセージを送信できない」「アカウント登録後、一定期間経たないとメッセージ表示の優先順位が低くなる」といった仕組みを取り入れて、できるだけ迷惑メッセージが出回らないようにしたり、迷惑メッセージが届いてしまった場合に備え、「よく知らない人からのメッセージは無視してほしい」と呼びかけているところもあります。

しかし最近、これらの対策をくぐり抜ける手法が広がっています。迷惑メッセージが、自分といつもやり取りしている友達のアカウントから送られてくるのです。それまでのやり取りを無視して、突然「あなたに○○をおすすめします」や「××のホームページを見てください」といったメッセージが送られてきて、いかにも不審ではあるのですが、自分のよく知っている人のアカウントなので、信用してしまうようです。このような迷惑メッセージは、なぜ送信されるのでしょうか？　その原因の一つが、SNSに備わっているアプリケーション連携機能（API）です。

最近のSNSは、SNS自身が提供する公式アプリやWEB画面以外に、第三者が独自のアプリやWEB画面を作るための仕組みを提供しており、これをAPIと呼びます。APIがあることで、公式にはない便利な機能を持ったアプリや、キャンペーン企画と連動したWEBサイトを第三者が作ることができます。

ところが、このAPIが迷惑メッセージの送信に悪用されることがあります。APIを利用すればSNS利用者の名前でメッセージを送信できるため、悪意を持ったアプリがSNS利用者になりすまして、迷惑メッセージを送信するのです。

アプリがAPIを利用する前には、SNSの利用者に「このアプリに操作を許可していいか」と確認が入ります。その段階で不審なアプリを拒否できればいいのですが、なかには「話題の動画を見るためにAPIを許可して」などと、目的を隠してAPI利用の許可を迫るものも存在します。

こうした不正なアプリにAPIの利用をいったん許可してしまうと、送信済みの迷惑メッセージだけを削除しても継続的にメッセージが送信され、SNS上で友達登録をしている相手に迷惑をかけ続けます。メッセージの送信を止めるには、SNSの管理画面を使って、不正なアプリのAPI利用許可を取り消す必要があります。

肝心なのは、不審なアプリにAPIの使用許可を出さないことですが、どのようなアプリが不審なものかを一目で見分けるのはむずかしいのも事実です。被害を予防するためにも、定期的にアプリの一覧を確認し、必要最低限のアプリを除いて許可を取り消すように心がけてください。またAPI以外にも、他のサービスと同じパスワードを使い回さないといった基本的な対策も怠らないようにお気をつけください。●

イラスト（P22,23）／山本加奈子

Global Trends

グローバル・トレンド

IT化を模索するラオス

IIJグローバル事業本部
グローバル事業開発室　**文園 純一郎**

二〇一四年夏、IIJは「コンテナ型データセンターの導入によるJCMプロジェクト実現可能性調査」を経済産業省より受託しました。それをきっかけに、出張でラオスを頻繁に訪れています。

ラオスといえば、タイ、ベトナム、ミャンマー、カンボジア、中国の五ヵ国に囲まれたASEAN諸国のなかで唯一の内陸国で、国土は日本の本州とほぼ同じ大きさですが、そのうち約七〇パーセントが山岳地帯という自然豊かな国です。主力産業は農業で、最近では石炭、鉄鉱石などの豊富な天然資源が注目されており、資源開発が急速に進んでいます。タイに進出している日系の製造業も、次の進出先としてラオスを検討するケースが増えているようです。

しかし、国のIT化の面では、他のASEAN諸国に大きく後れをとっており、政府高官でさえも、メールはGmailやYahoo!メールを利用しているのが現状です。ラオス政府もこの事態を憂慮し、日本などの援助を活用しながら、国立のデータセンター建設に向けた検討や、人材の育成など、様々なIT強化施策に取り組んでいます。

その一環として昨年の一二月、首都ヴィエンチャンでラオス政府が主催する初のテクノロジー系イベント「ラオテックマート2014」が開催されました。IIJもコンテナ型データセンターの紹介を目的に、数少ない日系企業の一社として出展しました。

テクノロジー系イベントというと、日本で開催されるIT系イベントを連想される方も多いと思いますが、蓋をあけてみると、バイオテクノロジー、農業、情報通信、エネルギー、医療、電子・電化製品など、幅広い技術分野を対象としたイベントであり、合計八〇の出展者のうち、情報通信やIT関連は片手で数えられるほどでした。IIJの向かいのブースは有機野菜の栽培技術関連の企業で、野菜で作った綺麗なオブジェが飾られていました（笑）。

それでもIIJのブースにはラオス政府の高官が多数訪れ、コンテナ型データセンターの映像や説明を熱心に見聞きしていました。こうした状況を目の当たりにし、ITに対する関心が非常に高いことが実感されました。ラオスがIT化を進め、メコン地域の中心という好立地を活かして、近い将来、ASEANのITハブとしての役割を果たすようになってほしい、IIJも少しでもその力になりたい――そんな思いで今日もラオスに出発です。●

Information

IIJモバイルサービス／タイプK スタートアップキャンペーン

KDDI LTE網を利用したIIJモバイルサービス／タイプKの販売開始を記念したキャンペーンを実施しています。NTTドコモ網を利用したIIJモバイルサービス／タイプDと組み合わせることで、MVNO事業者であるIIJならではのモバイルサービスをご利用いただけます。

特典内容

1. 「タイプD 定額プランL」「タイプK 定額プランL」を新規申し込みの場合、
   初期費用0円（通常20,000円）、登録手数料0円（通常3,000円）
   月額費用3,500円（通常6,300円～）でご提供
2. IIJ SMFsxサービスと組み合わせて、「タイプD」「タイプK」で冗長構成をとる場合、
   バックアップ側のIIJモバイルサービスの月額費用を6ヵ月間無料でご提供

お申込期間　2015年6月末まで

詳細はこちら：http://www.iij.ad.jp/svcsol/campaign/mobile_201503.html

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、小河文乃、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

◎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/

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：06-4707-5400

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

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
東京都千代田区神田神保町 1-103 東京パークタワー 2F
〒101-0051　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
東京都中央区京橋 1-14-9 依田忠ビル 7F
〒104-0031　TEL：03-5159-0600

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。（2015年4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

Internet Initiative Japan