IIJ.news

June 2013
vol.116

【特集】

情報セキュリティとSNS

会議レス

株式会社インターネットイニシアティブ
代表取締役社長 **鈴木幸一**

エレベーターに乗るたびに、パソコンを脇に挟んだ社員と一緒になる。「会議ばかり増えて、仕事する時間あるの」と揶揄する。管理部門は、著の上げ下げまで規定づくりに執心し、技術部門は、部署間の調整に長い時間を費やす……会議の多さを見ていると、そんな悪夢のような状況が、わが社にも広がっているのではないかと、疑心暗鬼になる。規定など少ないほうがいいに決まっているし、部門間の〝小田原評定〟を繰り返さなければ、サービスのかたちにまで持っていけないという状況を受け入れる時は、IIJがカルチャーそのものを失う時だという思いが強いだけに、ちょっとした兆候にも、過敏に反応してしまうようだ。

「ペーパーレス」より「会議レス」にしたほうがいい。会議など必要ないとまでは言えないけれど、いつも会議室に空きがないという状況を見ていると、そんな憎まれ口をたたきたくなる。会議のテーマといえば、大方は部門間の調整のようだ。調整を続けるということは、部門間で収まるべきところに収まるようなかたちにするわけで、破綻はないけれど、尖ったアイデアは削られてしまうことが多い。破綻や欠陥と斬新は隣り合わせで、尖って斬新なアイデアを生かしながら、部門間の調整で収まるようにするのは、ことのほか難しい。結局は、従来のサービスの改善版が溢れるだけである。それはそれで悪いことではないのだが、それだけでは企業を成長させるエンジンにはならない。

おおよそ開発段階から各部門の人間が寄り集まって、各部門が納得するような開発は、遅れ遅れになるか、驚きを与えるような要素は、会議の過程で消えてしまうことが多い。だからと言って、関係部門の調整なしにプロジェクトを進めれば、「誰が運用するのか」という話になってしまう。組織は、大きくなる過程で、自ずと爆発するような思いとエネルギーを削ぐことになる。官僚組織とは、役人の組織を指す言葉ではなく、組織が大きくなることだと言われるが、会議中毒症はその典型的な現象に違いない。

組織が拡大・成長を続けていく限り、それは避けることのできない問題なのだが、なんとかIIJのカルチャーを持続しながら、IIJを飛躍させるような新たなエンジンを次々と生み出していけるダイナミックな組織にしたいと、ぶつくさ自分に言い聞かせている。

連休中、香港に出張に行く。超高層ビルが果てしなく建設され続ける香港のエネルギーには、行くたびに刺激を受けるのだが、それはいつも「あやうさが同居する感動」である。香港の大実業家で大富豪の方々の事業基盤は、不動産に出発し、金融業からインフラ業へと事業を展開している。不動産ビジネスによって、インフラ事業に乗り出すほどの巨額の富を蓄積できるのだから、土地の狭い香港にあって不動産業は、あらゆる産業に優先する事業なのである。

産業と言えば「ものづくり」という時代に育った私は、不動産と金融の都市・香港がつくりあげるエネルギーに、別の刺激を受ける。IT産業の先端を行くサンフランシスコでは、高い賃金を得られる人間に雇用が殺到する一方で、低賃金の労働者には雇用の機会がなくなっているという。それを「格差」というのか難しいけれど、ものづくりでないIT産業というのは、雇用のかたちもずいぶんと違ったものになるのは致し方のないことかもしれない。それは、日本のIT産業の在り方とも、大きく異なるけれど。

イラスト／山本加奈子

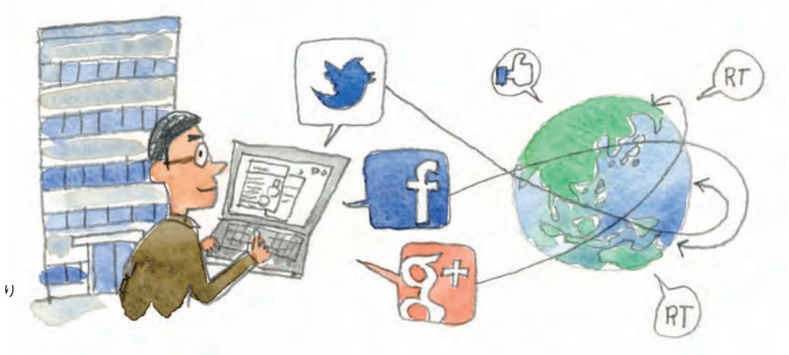
IIJ.news
June 2013
vol.116

Contents

表紙のコトバ　すげさわ かよ
ぽつぽつと雨音が静かに響く、雨の日の池。水辺では、白や青などすがすがしい色合いの花菖蒲が咲き誇り、見頃を迎えています。グレーの水面に映える色彩が、鬱蒼とした梅雨空までも晴れやかに見せてくれるようです。

情報セキュリティとSNS

**昨年に引き続き、「セキュリティ」特集をお届けします。
ハード、ソフトの両面でITが進化・成熟するなか、
パブリック／プライベートを問わず、情報セキュリティの確保は、
現代社会の死活問題となっています。
今回は、SNSやスマートフォンなど、我々にも身近な話題を集めてみました。**



特集イラスト／なかだえり

【座談会】

SNSのセキュリティ

（出席者）
日本マイクロソフト株式会社 チーフセキュリティアドバイザー
高橋正和
日本アイ・ビー・エム株式会社 シニア セキュリティ アナリスト
守屋英一
名古屋大学 教授
高倉弘喜

（司会・進行）
IIJ サービスオペレーション本部 セキュリティ情報統括室長
齋藤 衛

齋藤　今回は、私とSNSでつながっている三名の方に集まっていただきました。最初に、皆さんのSNSの使い方からお聞きしたいと思います。

高橋　SNSを意識し始めたのは三年ほど前です。ブログがテーマのある座談会に呼ばれたのですが、そのときは「セキュリティの仕事をしていて、SNSをやるなんて危なすぎる」という見解で一致しました（笑）。つまり、自分の日常を発信することで、誘拐につながったり、うっかり家族や知人に迷惑をかけてしまう可能性がある、ということです。

しかし、しばらくすると、いろんなところから「SNSは安全なのでしょうか？」という質問が寄せられるようになった。当初は、差し障りのないことを言っていましたが、だんだん矛盾というか詰めの甘さを感じるようになり、「これは自分の身を削ってやるしかない」と思い、匿名を用いないSNSを始めることにしました。

私の使い方はプライベートが中心ですが、他者を巻き込まないように気をつけています。例えば、「今、齋藤さんと食事をしています」とチェックインすると、齋藤さんが、いつ・どこで・誰（私）と、いたことが記録されます。しかし、もしかすると齋藤さんは、別の約束を断って私に会ってくれているのかもしれませんし、大事なミーティングをすっぽかして飲んでいるのかもしれません（笑）。ですから、私が発信するのは自宅で作った料理の写真が多く、これなら、誰も巻き込む心配がなく、安心して載せられるからです。

仕事関係では、イベントを行なう際などにSNSで告知・集客を図るといったことに使っています。そういった用途には、お金のかからない広報媒体として有益だな、という印象を持っています。

齋藤　守屋さんはSNSをどのように使っていますか？

守屋　私はプライベートな使い方からスタートしました。Facebookを始めて面白かったのは、それまで交流のなかった人たちとつながれることです。仕事ではエンタープライズ向けのセキュリティをやっていたので、コンシューマ向けにもセキュリティの勉強会をやりたいと思い、Facebookで参加者を募ったところ、一〇名くらいの一般の方が集まってくれました。フレッシュなメンバーと行なう勉強会はとても新鮮でしたし、自分では「これくらいのセキュリティは当たり前」と思っていたレベルが、一般的な認識とは乖離していることも実感でき、とても有意義でした。

私が『フェイスブックが危ない』を出版できたのもFacebookのおかげでして、勉強会の打ち上げで「セキュリティのことをもっと広く伝えたい」という話をしたら、メンバーの一人がたまたま文藝春秋の取締役の方と知り合いで、それがきっかけとなって本を書くことになったのです。このようにSNSは、全く新しい人脈形成を可能にしてくれるところがす

ごいな、と感じています。

齋藤　高倉先生はいかがでしょうか？

高倉　このなかでは、大学に勤めている私が一番若い人たちと接していると思うのですが、そういう環境だと、プライベートなことをやっているのか、オフィシャルなことをやっているのか、双方の境界がはっきりしないのが私のSNSの使い方です。私は、ポイント・ポイントで位置情報をSNSでアナウンスしています。自分の居場所を公にしておくと、たまたま近くにいた人が声をかけてくれることがあります。そして「じゃあ、一緒に御飯でも食べながら話をしよう」といったことが簡単にできる。そんなとき、SNSはメールより敷居が低く便利、というのが私の実感です。

仕事の面でも、SNSなら自分の考えていることを気軽に話せます。研究内容を論文に落とし込んでいくにはエネルギーが要るし、時間もかかる。その過程で、軽い話題をSNSで話していると、思わぬ進展が得られることもあります。

最近は、学会などの模様がUstreamでよく中継されていますが、それを見ながらSNS上で議論するといったふうに、リアルタイムで流れているものに対して簡単にコメントを出し合えるのもSNSの強みではないでしょうか。

SNSを使う際のルール

齋藤　皆さんはSNSを使うとき、どんな点に注意していますか？

高橋　技術面と心がけの面の二つがあって、まず技術でできることは「設定」です。アプリケーションに対してどこまで情報を出すのか、どの範囲まで情報を公開するのか、といったことは設定で決められるので、そこは必ず確認しています。また、設定を定期的に見直す習慣はあまりないかもしれませんが、変更されていることもあるので、時々見直すようにしています。

「心がけ」の面で一番大切なのは、できるだけ、どこから突っ込まれても大丈夫な文章を書くことです。誰かに反論したくても、「そんな考えがあるとは知りませんでした。とても勉強になりました」と書くとかね（笑）。そういう心がけで、助けられることも多いと思いますよ。

守屋　私が気をつけているのは、「仕事の話題は書かない」ということです。会社は当然、「機密情報は書くな」と言いますが、機密の度合いは受け取る人によって異なります。自分では「これは機密情報じゃない」と思っていても、ある人にとっては有益な情報だったりする。位置情報も同じで「××に出張しています」と書くと、競合他社には「あそこに案件があるな」と分かってしまう。つまり、機密情報の漏れ方は自分ではコントロールできないので、それに関わるようなことは書かないということです。

あと、機能面ではプレビューを使って、一般の人にどう見えているのか、見えす

守屋英一
2007年日本IBMに入社。社外活動として、不正アクセス防止対策に関する官民意見集約委員会、NPO日本ネットワークセキュリティ協会などの構成員や、シーサート協議会運営委員を務める。2012年度JNSA表彰個人の部を受賞。著書に『フェイスブックが危ない』(文春新書)。今年7月『フェイスブック情報セキュリティと使用ルール』(あさ出版)を発売予定。

高橋正和
セキュリティベンチャーでのコンサル事業の立ち上げ、SOC構築支援、社内システム管理(CIO)を経て現職。マイクロソフト製品やサービスのセキュリティに対する取り組みを日本に紹介し、ユーザの要望を反映させ、安全なICT環境の実現を目指して取り組んでいる。

ぎていないか、チェックしています。

高倉　人と人とのつながりは、友達の友達……と六段階ほどたどっていくと、ほぼ世界中が友達になる「六次の隔たり」という話がありますが、それを考えると、自分の友達やフォロワーが何百人かいて、その輪が三段階くらい広がれば、ほぼ日本国民全員が友達になってしまう。要するに、SNSだからと言って、友達にだけ話しているわけじゃないという感覚は、常に持っておかなくてはいけないでしょうね。

齋藤　私は家族で二つだけルールを設けていて、「自宅から半径五〇キロ以内の話題はつぶやかない」、そして位置情報を公開するときは「時制を変える」ということをやっています。

高橋　「過去形にする」ことは、私もやっています。できるだけ当日には出さずに数日おいて公開するみたいに。

齋藤　気をつけないと、意図せず日常生活を公開することになりますからね。

SNSのリスク

齋藤　SNSの利用に際して、利用者はどういったことを想定しておいたほうがいいでしょうか?

高倉　今の若者は、プライベート――我々なら絶対に言わないようなことまで平気でしゃべってしまいます。彼女とデート中だとか、喧嘩したとか……。その程度の話題ならまだいいのですが、プライベートにオフィシャルな話が混ざってきたときに、SNSの敷居の低さが弊害になることがあります。例えば、会社の面接の内容を不用意に書いてしまい、内定を取り消されたなど、使い方を間違うと〝バカ発見器〟になってしまう。

守屋　正しい使い方を知らない人が意外に多いですね。Facebookは、公開、非公開、友達だけに公開など、アクセス制限をかけられるのですが、多くの人がそれを知らないまま使っていたりする。高倉先生がお話しされた内定云々の話も、ちょっと制限をかけておけば問題ないのに、パブリックにしているから誰にでも見られてしまうのです。

齋藤　それは、デフォルトが公開寄りに設定されているので、どこまで情報を公開するのか、利用者が考える必要があるということですね。

守屋　そうです。発言には適切なボリュームがあると思うので、身内だけに話したいのなら、それをアクセス制限というかたちで実行するべきでしょうね。

高倉　怖いなと思うのは、制限をかけていても、誰かが発言をコピペして、「こんなことを言っているよ」とやられた瞬間、情報が劣化しないまま流れてしまうことです。しかも、そこにいろいろなコメントが付いたりすると、書かれようによっては、全く反対のメッセージになってしまうことだってある。

齋藤　文脈みたいなものがある発言の一部かもしれないのに……。

高倉　特にTwitterのように文字数制限があると、一つの文脈を五回くらいに分けてつぶやいているのに、その一つだけがポッと転送されてしまい、本人には特別な意図がないにもかかわらず、読んだ人には「え!　こんなこと言ってる」という誤解になったりするのです。

齋藤　Twitterの場合、自分のつぶやきを消そうとしても、自動的にいろいろなところに拡散していて、なかなか消すことができない。自分の発信が、どこでどのくらいのあいだ生かされているのか意識しておかないと、発言の影響を読み誤る危険性があるでしょうね。

高橋　あと、公開に関して危険なのは、アプリを経由して自分の情報が飛び石的にリンクされているケースがあります。試しに、ある旅行情報のサイトを開くと、「ロンドンに行ったことがあるのはこの人です」と、「友達」の情報が出ている。「アプリに情報を出さない」という設定にしていなければ、知らないうちに、明示的に許可したつもりはないのに、情報が公開されている可能性があります。これはビッグデータの利用形態の一つかもしれませんが、本人には想像もつかないような情報の流れ方をしているのです。

SNSの〝安全〟のために

齋藤　SNSのセキュリティは、どう守ればいいのか?　それに関してコメントをいただけますか。

高倉弘喜
平成2年、九州大学卒業。平成4年、九州大学修士課程修了。平成7年、京都大学博士課程修了。奈良先端科学技術大学院大学助手、京都大学講師、同助教授を経て、現在、名古屋大学教授。

SNSを安全に歩くための10項目(JNSA SNSセキュリティWG)

1. 常に公開・引用・記録されることを意識して利用する
2. 複雑なパスワードを利用し、セキュリティを高める設定を利用する
3. 公開範囲を設定し、不必要な露出を避ける
4. 知らない人とむやみに〝友達〟にならない、知っている人でも真正の確認をする
5. 〝友達〟に迷惑をかけない設定を行う
6. 〝友達〟から削除は慎重に、制限リストなどの利用も考慮する
7. 写真の位置情報やチェックインなど、技術的なリスクを理解し正しく利用する
8. むやみに〝友達〟のタグ付けや投稿を行わない
9. 対策ソフトを利用し、危険なサイトを利用するリスクを低減する
10. 企業などの組織においては、SNSガイドラインを策定し遵守する

●http://www.jnsa.org/result/2012/SNS-WG_ver0.7.pdf

高橋　まずは「パスワードをきちんと管理すること」ですね。

守屋　Facebookやgoogle＋では、だいたい二段階認証になっています。アカウントやパスワードは漏れている恐れもあるので、新しい機器からアクセスする場合は、スマートフォンなどに六桁のワンタイムパスワードを飛ばしてそれを入力しないとログインできない、といった認証方法が一般化しつつあります。

高倉　ユーザ系のアプリは、IDがメールアドレスだったりするので、IDは変えられない。そうなるとパスワードや認証の部分で守るしかないですね。

　パスワードの管理以外では、〝やられている人〟からくる情報を見分ける、といったことが必要です。現状は、Facebookにしても Twitter にしても、怪しいリンク先は英語で示してくるので騙されませんが、これが日本語になったら、本当に踏まないかどうか……。

齋藤　何も手掛かりのない状態で判断するのはむずかしいですね。

高橋　技術面から言うと、アンチウイルスやセキュリティ対策ソフトは、やはり効果が高いようで、弊社が出した「セキュリティインテリジェンスレポート Ver.14」(http://www.microsoft.com/ja-jp/security/resources/sir.aspx)にも、対策ソフトを活用することで、感染率が平均で五・五分の一くらいに減る、というデータが出ています。スマートフォンに対策ソフトを使うケースはまだ少ないかもしれませんが、効果は大きいと思います。

齋藤　最後に、SNSの安全性を確保して不正利用をさせないためには、何をすればいいでしょうか?

高橋　表現がむずかしいのですが、リーチできる〝量〟によって情報の質とエネルギー値が変わると思うのです。情報の届く範囲が広がることで、質が変わる。同じように、より多くの人に届くことで、情報のエネルギー値も高くなる。だから大勢にリーチできる情報は、それがネガティブに転じたとき、同じ大きさのエネルギー値でもって跳ね返ってくる――この〝量的な考え方〟をいつも頭に入れておくことでしょうね。

守屋　二つあって、個人的にはSNSの大きなポテンシャルをポジティブに捉えているのですが、ここで話したようなリスクを知らないままだと、事故につながるかもしれない。その点はぜひ気をつけていただきたいですね。

　もう一つは、若い人、特に未成年の子供がSNSを始めるとき、親がリスクを知らないために、正確なジャッジを下すことができない。子供が無料通話アプリを使いたいと言っても、危なそうなイメージはあるけど、具体的に何が危ないのかよく分かっていない。ですから、まずは親がどんなリスクがあるのか知ったうえで、子供に伝えるようにしていかないと、過ちは続いていくのかな、と……。

齋藤　リスクは知っておいて損はないし、それを伝えるのは親の役割かもしれませんが、リスクがあるなら、サービス提供者が軽減していくのが、道義的には正しいのではないでしょうか?

守屋　確かにそうです。ここで私が言っているのは短期的なリスク低減策です。長期的な対策としては、サービス提供者が問題点を改善すべきだと思います。

高倉　SNSのリスクは、案外、子供のほうがよく分かっていて、実は知らないのは親だったりします(笑)。もちろんリスクを知らない子供もいるわけで、その子を今後どう教育していくのかということは、考えなければならない。例えば、教育の場で教えていったり、我々がこうした活動を通じて啓発していかなければならないでしょうね。

齋藤　若い世代に「こういうインフラがあって、こんな面白いことができるけど、危ない面もあるんだよ」ということを伝えていかなければならないですね。

高橋　JNSAのSNSセキュリティワーキンググループが「SNSを安全に歩くための10項目」(上記)を公開しているので、参考にしてみてください。

齋藤　皆さん、本日はありがとうございました。■

増加する ドライブ・バイ・ダウンロード攻撃

IIJ 管理本部 危機管理室
横須賀憲一

このところ多くの被害をもたらしているドライブ・バイ・ダウンロード攻撃に対しては、ブラウザプラグインの脆弱性対策が重要である。

近年、サイバー攻撃の脅威が増していますが、情報システムの重要性が高まるにつれて、攻撃の目的や対象も著しく変化しています。

今年三月に公開されたＩＰＡの「二〇一三年版 一〇大脅威」によると、昨年、社会的影響が大きかったセキュリティ上の脅威は、第一位の「クライアントソフトの脆弱性を突いた攻撃」を始めとして、一〇件中八件が外部からの攻撃によるものでした。こうした攻撃は、金銭や情報資産の窃取を目的として、日常的に行なわれています。攻撃対象は、不特定多数のインターネット利用者であり、企業活動においても個人利用においても、インターネットからの攻撃への備えが急務です。

サイバー攻撃によるリスクを効率よく低減するには、脅威と脆弱性を正しく認識し、優先度の高い対策から実行していくことが求められます。ここでは「クライアントソフトの脆弱性を突いた攻撃」を具体例として、インターネット利用時のリスク低減に役立つ対策を考えてみたいと思います。

ドライブ・バイ・ダウンロード攻撃とは？

「クライアントソフトの脆弱性を突いた攻撃」は、利用者のＰＣに導入されているクライアントソフトの脆弱性を悪用してマルウェアに感染させる攻撃です。なかでもJava（JRE）、Adobe Reader、Adobe Flash Player などのブラウザプラグインの脆弱性を突いた攻撃が増加しており、「ドライブ・バイ・ダウンロード攻撃」とも呼ばれます。これは攻撃者があらかじめＷｅｂサイトを改ざんしておき、利用者がアクセスして来るのを待ち構える攻撃手法です。利用者が悪意あるＷｅｂサイトにアクセスすると、攻撃者はブラウザプラグインの脆弱性を悪用してマルウェア配布サイトに誘導し、マルウェアをダウンロードさせ、利用者のＰＣに感染させようと試みます。

ブラウザプラグインが狙われる理由

クライアントソフトのなかでも、ブラウザプラグインには三つの特徴があります。第一に、利用者が多いことです。Oracleによると、Javaは一一億台のＰＣで実行され、Java Runtime Environment（JRE）は年間九億三千万回のダウンロードが行なわれています。Adobe Reader や Adobe Flash Player の利用者数は不明ですが、周囲を見渡すとこれらが導入されていないＰＣを探すのがむずかしいほどですから、相当数の利用者がいると考えられます。

第二に、頻繁に脆弱性が発見されるものの、対策されず放置されるケースが多いことです。左頁の表は、ＩＰＡのＷｅｂサイトを参考に、公表されたブラウザプラグインの脆弱性を数えた結果です。感染者が脆弱性対応を怠った理由としては、「重要だと思わなかった」「普段使わないブラウザだったので気づかなかった」「業務が忙しく後回しにした」などが挙げられ、現状、無視できない数の脆弱性が対策されないまま放置されています。

第三に、攻撃の成功率が高いことです。ＩＢＭの「二〇一二年 下半期ＴｏｋｙｏＳＯＣ情報分析レポート」によると、ＴｏｋｙｏＳＯＣにおいて検知されたドライブ・バイ・ダウンロード攻撃で悪用された脆弱性は、Adobe Reader の脆弱性が六四・九パーセント、Java（JRE）の脆弱性が三二・二パーセントでした。一方、マルウェアのダウンロードが成功した割合は、ドライブ・バイ・ダウンロード攻撃全体で二六パーセント、Java（JRE）の脆弱性を悪用するものに限定すると五一・九パーセント、と非常に危険度が高い攻撃手法であることが分かります。

また、Java（JRE）はプラットフォームに依存しない開発技術であるため、これをマルウェア開発に用いることで、Windows 以外の環境へも攻撃可能となります。この点は、攻撃者のメリットであり、今後も Java（JRE）に対する攻撃は増加すると予想されます。

ブラウザプラグインの脆弱性

	2010年度	2011年度	2012年度	2013年度（2013年5月16日現在）
Java（JRE）の脆弱性	1件	1件	6件	1件
Adobe Readerの脆弱性	3件	1件	2件	1件
Adobe Flash Playerの脆弱性	4件	3件	11件	2件

ワクチンソフトを導入すれば大丈夫？

ワクチンソフトを導入してパターンファイルを最新にすることは、ＰＣのセキュリティ対策として重要ですが、それだけでは十分ではありません。今年二月に公開された米国ＣＳＩＳの報告書「Raising the Bar for Cybersecurity」に興味深い数字が紹介されています。

●七五パーセントの攻撃は、ソフトウェアの既知の脆弱性を利用するもので、日常的なパッチ適用で防ぎ得た。

●マルウェア発生後の最初の数日間は、九五パーセントのワクチンソフトがマルウェアを検出できない。

●現在の技術では、二五パーセントのマルウェアが検出されない。

このようにワクチンソフトは万能ではないため、過度に依存することなく、確実なパッチ適用と組み合わせて攻撃に備えることが大切です。

怪しいＷｅｂサイトにアクセスしなければ大丈夫？

「マルウェアに感染しそうな怪しいＷｅｂサイト」と言うと、一般には、違法な薬物販売サイトやアダルトコンテンツなどを連想しがちですが、現実は異なります。

シスコの「シスコ二〇一三年次セキュリティレポート」によると、マルウェアに遭遇するＷｅｂサイトの大部分は、メジャーなＷｅｂサイトを合法的に参照しており、利用者がもっとも頻繁に訪問し、安全だと考えられているような場所です。そして、悪意あるＷｅｂサイトに遭遇しても問題が起こらないようにするには、日頃からブラウザプラグインを始めとするクライアントソフトを最新の状態に保つことが大切です。

ドライブ・バイ・ダウンロード攻撃への対策

ドライブ・バイ・ダウンロード攻撃の多くは、クライアントソフトの既知の脆弱性を悪用するので、利用者がクライアントソフトを更新し、脆弱性を解消することが望まれます。

クライアントソフトにおいて実施すべきおもな対策としては、第一に、不要なソフトウェアを導入しないことです。導入したソフトウェアは、実際に使用するか否かにかかわらず、脆弱性が発見されるたびに更新しなければなりません。不要なソフトウェアが存在すると、更新の手間が増えると同時に見落とす危険性も出てきます。第二に、ソフトウェアを常に最新に保つことです。ＯＳやワクチンソフトだけでなく、ブラウザプラグインも含めたクライアントソフトを確実に更新することが重要です。第三に、脆弱性の有無を客観的にチェックする必要があります。例えば、ＩＰＡのＭｙＪＶＮバージョンチェッカを利用すると、クライアントソフトの脆弱性を簡単に確認できます。[*1]

また、Java（JRE）と Adobe Reader では、ソフトウェアの一部機能を無効化することで、セキュリティを強化できます。

●ブラウザプラグインとしての Java を無効化する。[*2]

●Adobe Reader で、ＰＤＦファイルの JavaScript を無効化する。[*3]

●Adobe Reader で、ＰＤＦ添付ファイルの機能を無効化する。[*4]

これらは、ゼロデイ攻撃などの緊急時にパッチ提供までのワークアラウンド（応急措置）として利用されることもあります。注意点としては、業務上必要な機能もありますので、設定の際は事前にご確認ください。

今回ご紹介した対策はほんの一例であり、これだけやっておけば大丈夫というものではありません。サイバー攻撃への備えは、特定の対策だけに依存することなく、様々な対策を組み合わせてバランスのとれた防御を行なうことが大切です。それらを検討するなかで、本稿が一助となれば幸いです。

＊1 http://jvndb.jvn.jp/apis/myjvn/
＊2 http://www.atmarkit.co.jp/ait/articles/1301/18/news092.html
＊3 http://www.ipa.go.jp/files/000014188.pdf（P.17～18）
＊4 http://blogs.adobe.com/adobereader/2010/04/didier_stevens_launch_function.html

スマートフォン・セキュリティ

IIJ サービスオペレーション本部 セキュリティ情報統括室 シニアエンジニア
加藤雅彦

スマートフォンの利用が急速に進むなか、セキュリティの問題も大きくなっている。ここでは、スマートフォンを安全に活用するための注意事項をまとめてみた。

皆さんの携帯電話はフィーチャーフォンですか？　それともスマートフォンですか？　端末画面を指で触る光景がもはや普通に見られるように、ここ最近、スマートフォンへの移行が急速に進みました。シーズン毎に発表される携帯電話の新機種も、今やほとんどがスマートフォンという状況になり、特にこだわりがない限り、買い替えなどのタイミングでスマートフォンを選択される方も多いのではないでしょうか。スマートフォンの技術革新のスピードは速く、フィーチャーフォンよりも自由度の高い、便利でリッチなアプリケーションやデータ量の多いコンテンツを気軽に利用できるなど、日々便利になっていることを実感します。

スマートフォンにまつわるセキュリティ事件

スマートフォンの普及が進む一方、様々なセキュリティ上の問題が発生しているのも事実です。例えば二〇一〇年には、Android端末で初めてのウイルスが確認されました。また、二〇一二年に端末の電話番号や電話帳を漏えいさせる「××× The Movie」というアプリケーションが流行したことも記憶に新しいところでしょう。その他にも、公式マーケットから正規のアプリケーションとして提供されているにもかかわらず、電話の発信履歴やGPS情報といったプライバシー情報を外部に送信したり、利用時に高額な料金を請求したりする、セキュリティ上問題のあるアプリケーションも存在しています。

便利ではありますが、残念ながらスマートフォンを狙ったウイルス、情報漏えい、プライバシー侵害、詐欺行為など、数多くの問題が発生し、あとを絶ちません。ここでは、スマートフォンと既存のデバイスとの違いやその仕組みを整理しつつ、安全に利用するにはどうすればいいのかを考えてみます。

従来のデバイスとスマートフォンの違い

スマートフォンは電話であると同時に、GPSやカメラを備えた高性能な携帯端末です。またスマートフォンは、パーソナルデバイスであり、個人に関する多くの情報が保存されています。ただ、これらはスマートフォンに限ったことではなく、フィーチャーフォンも同様の特徴を持っています。では、スマートフォンとフィーチャーフォンの大きな違いは何でしょうか？　それは、スマートフォンはフィーチャーフォンに比べて非常に自由度が高く、様々なアプリケーションをインストールできる点にあります。

電話帳や通信記録といった情報はもちろん、写真、位置情報、動画、文書といった様々な情報を、自由に開発可能なアプリケーションで扱うことができ、そのため、アプリケーションに不要な機能を利用させない仕組みが標準的に備わっています。その一つは「パーミッション」という機能で、アプリケーションがどのような機能や権限を要求しているのかを利用者が確認し、そのアプリケーションをインストールするかどうかを判断できるというものです。しかしながら、パーミッション表示はOSの機能や処理方法をもとに分類されており、直感的とは言い難い場合もあります。また、特定の機能だけを停止できないといった制限もあります。

もう一つは、アプリケーションの様々な動作を制限するための「サンドボックス」という機能が搭載されています。しかし、サンドボックスを回避するアプリケーションなども非公式に提供されており、問題となっています。

加えて、スマートフォン用のアンチウイルスの動作にも制限がある場合があります。PCのアンチウイルスソフトはOSと協調して動作するための特権を与えられていますが、スマートフォンにはそのような特権がなく、一般のアプリケーションとして動作しています。よって、マルウェアがOSの脆弱性などを突いて特権を取得した場合、検知や防御が困難になる可能性があることが指摘されています。機能や性能が大きく進歩したスマートフォンですが、セキュリティ面においては、まだ発展途上にあることは否めません。

スマートフォンの安全な利用方法

では、スマートフォンを安全に利用するにはどうすればいいでしょうか？　それぞれの事業者は安全なシステムやマーケット、アプリケーション、サービスを作ることにかなりの力を入れており、一定の効果をあげています。しかし、現状では事業者の努力のみで安全が維持できるとは言い難い状況です。そこで、スマートフォンのセキュリティ向上に関して、いくつかの提言が出ていますので、少し見てみましょう。

総務省からは「スマートフォンプライバシーイニシアティブ」という包括的な対策が提案されています。プラットフォーム、アプリケーション、利用方法など、幅広くスマートフォンを安全に使うための指針が示されています。その内容は左記のとおりです。

1　アプリケーション提供者や情報収集モジュール提供者を中心に、アプリケーション提供サイト運営事業者、OS提供事業者、移動体通信事業者などのスマートフォンの関係事業者に広く適用可能な「スマートフォン利用者情報取扱指針」を示す

2　第三者によるアプリケーション検証の仕組みなど、指針の実効性を上げるための方策を提案

3　利用者リテラシー向上のための情報提供・周知啓発方策

4　国際連携の推進

同じく総務省のスマートフォン・クラウドセキュリティ研究会では、「スマートフォン情報セキュリティ3カ条」として、左記の項目を挙げています。

1　OS（基本ソフト）を更新

2　ウイルス対策ソフトの利用を確認

3　アプリケーションの入手に注意

こちらはおもに、スマートフォン利用者がどのようなことに気をつければいいのか、重要な点に絞って指摘しています。研究会の報告書も出ていますので、興味のある方は目を通されてはいかがでしょうか。

その他にも、日本スマートフォンセキュリティ協会や日本ネットワークセキュリティ協会などからも、スマートフォンの業務利用に関するガイドラインが出ています。

日常の利用において、スマートフォン本体やアプリケーションの扱いに細心の注意を払いながら、利用者自身で情報の重要性を考え、重要なデータはスマートフォン本体に格納しないといったことが大変重要だと言えるでしょう。まだしばらくのあいだは、スマートフォンを安全に利用するために、利用者も事業者も継続的に努力する必要があるのではないでしょうか。

スマートフォンが持つセキュリティ機能

スマートフォンのセキュリティ機能と環境は携帯電話というよりむしろPCに近いと言えます。では、スマートフォンはPCと同じかというと、そうではありません。ハードウェアの性能、特にストレージ容量などはPCに劣り、OSのアップデートなどは現時点ではPCと比較して遅れる傾向にあります。クラウドを利用してデータのバックアップを行なうことが多い点もPCとは異なると言っていいでしょう。

さらに、ビジネスの提供形態はフィーチャーフォンと大きく異なっています。フィーチャーフォンでは端末からアプリケーションまで、垂直統合型のビジネスが行なわれていますが、スマートフォンでは通信、端末、アプリケーションを別の事業者が提供する水平分業型のビジネスとなっています。このことによりスマートフォンでは、自由度の高いオープンなプラットフォームが提供されていますが、その反面、総合的に安全性を確保するには事業者間の連携などが必要となります。

ビジネスモデル、セキュリティ確保の技術、アプリケーションの配布方法、バージョンアップの方法など複数の点において、スマートフォンは携帯電話ともPCとも異なる特徴を持っていると言えるでしょう。

社員の危機管理教育

IIJ 管理本部 危機管理室長
松原勝美

企業のセキュリティ対策においては、社員への教育の実践が大切であり、その効果を定期的に評価していく必要がある。

セキュリティ対策といえば、アクセス制御・ウイルス対策ソフトなどの技術的な対策や、入退室制限などの物理的な対策に目がいきがちですが、人的対策も同じように重要です。ＩＴシステムを利用・運用し、ルールを守るのは最終的には人だからです。また、システムやルールだけでは、新たな脅威や例外的なケースに対応できないこともあり、そこでも人がカバーする必要があります。

人に行動を起こさせるためには、何らかの教育や訓練が必要です。私はＩＩＪでセキュリティ教育を実施する立場にありますが、今回はその経験をふまえ、教育実施にあたっての全体像を整理したいと思います。読者の皆さんが教育を実施する立場であれば、自社の教育に役立てていただき、教育を受ける立場であれば、なぜ教育が必要なのかという意味や、自社で教育が行なわれている意図を理解し、積極的な教育参加につなげていただければ幸いです。

何を教えるか？

まず思いつくのが「会社のルール」です。会社のルールは、ルールを教えるだけでなく、その背景も併せて教えることで効果が高まります。ルールの意味とその必要性を理解してもらえれば、ルールを守ろうという意識が高まります。

また教育というと、どうしても押し付け感が出てしまいます。ルールを守らずに事故を起こしてしまった場合は個人の責任になるが、ルールを守っていて事故が起きてしまったら、ルールを作った会社の責任であり、個人の責任ではなくなる――つまり、ルールは従業員のためにあり、それを教えているのだ、と訴えるのも、ルールへの理解・順守につながると考えられます。

次に「意識啓発」も重要です。世の中の脅威は技術の進歩にともない常に変化しています。現状の会社のルールやシステムが脅威の進歩に追い付いておらず、既存のルールやシステムでは対応できないという状況が発生するかもしれません。そこで、いかなる事態にも対応できるように、意識面への働きかけが重要になります。そのためには、教育する側も常に世の中の状況にアンテナを張り、それが自社にも起こり得るか否か、気を配っておく必要があります。

人によっては、ルールを守らない、事故につながるような行為がどれくらい危険なのか理解していない、もしくは危険性があると分かっていながら「自分だけは大丈夫」とそれらの行為を正当化してしまう場合もあります。こうしたケースを避けるためには、当事者意識を持ってもらうことが重要です。社内で実際に起きた事例をもとにルールや注意すべき点を伝えるようにすれば、身近な話として理解度が深まるのではないでしょうか。

どのように教えるか？

教育の方法はいくつかありますが、やはり一番効果が高いのは集合研修です。講師が受講者の反応を見ながら伝え方・内容を微調整できますし、身振り手振りといった非言語コミュニケーションも活用できます。ただし、講師・受講者のスケジュールを調整する必要があり、対象者の数が多ければ、実施がむずかしくなることもあるでしょう。

そういった場合には e-Learning として動画を視聴してもらったり、テキストを読んでもらうといった形式が主流になります。ここで気をつけなければならないのは、業務の片手間に動画やテキストを見る人がいることです。これでは十分に受講者へ内容を伝えることができません。そこで、テストを実施して理解度を確認することが大切になります。テストの際には、教育内容を発展させた応用問題を出題したり、テスト問題を多めに用意してランダムに出題することで、受講者に真剣に動画やテキストを学んでもらうようにしましょう。

いつ教えるか？

当然、入社したときには、会社のルールを伝える必要がありますが、それだけでは日々の業務に追われてついつい忘れがちになってしまうため、定期的な教育も不可欠です。会社のルールなどは同じ事柄でも毎回伝えることになりますが、興味をもって受講してもらうには、関心を惹きやすい最新技術動向や世の中の事件の解説など、コンテンツを追加するのもいいでしょう。コンテンツが重要なのはもちろんですが、定期的なイベントとして実施すれば、それが開催されるというだけで、従業員への意識啓発になります。

また、イベントとしての教育だけでなく、日常において上司・先輩が後輩にルールを守ることを教える必要もあります。そのためには、上司・先輩が率先してルールを順守する姿を部下に見せなければなりません。部下は上司・先輩を見て仕事をしていますので、上の人がやらないことは下の人もやりません。

教育の有効性

教育を実施してコンテンツを伝えることはもちろん重要ですが、それは最終目的ではなく、教育を行なったことで受講者の行動に働きかけることこそ真の目的です。教育の有効性を確認し、教育した内容が本当に伝わっているのか、その理解度を知るためには、穴埋めや○×問題を出題し、正答率を確認することになるでしょう。

その際、こうした教育が受講者の行動をどの程度変化させているのかといったことを、実際に測りたいところです。定性的な内容ですので、その後の事故や〝ヒヤリ・ハット〟の発生時に、教育したことが活かされているかどうかを見ていくのがいいと思います。

また、受講後にアンケートを実施するのも効果的です。普段はセキュリティをあまり意識していない人でも、受講直後は意識が向いているので、会社のルールについて考え、疑問や改善点をコメントしてもらいやすく、以後の教育やルールの改善につなげることができます。「考える時間を持ってもらう」ことも教育の一環なのです。

私は毎年教育を開催しながら、どうすれば受講者に積極的に受講してもらえるかを検討して、企画を立てています。内容も重要ですが、運営する側が教育を押し付けるのではなく、受講者のためにやっているということを伝えていくのも大切です。

教育を含め、セキュリティ対策に終わりはありません。会社から人がいなくなることはないので、会社で働く皆さんにセキュリティの重要性を日々伝えていく姿勢が何よりも大事であり、それが受講者に伝われば、危機管理教育のベースになると考えています。

U.S. ARMYのSNSポリシー

IIJ 管理本部 コンプライアンス部長
墨矢 亮

SNSの公的な活用が増えるなか、多くの組織では、利用ポリシーを文書化する必要に迫られている。本稿では、アメリカ陸軍がSNSの利用についてまとめた“Social Media Handbook”を紹介する。

SNS（ソーシャル・ネットワーキング・サービス）についての文書を組織が定めようとする動機は、各種ステークホルダーとのリレーション強化に向けてのコミュニケーション戦略・戦術の記述を目的とする場合と、リスクマネージメントを目的とする場合とがあると言えます。両方をまとめてトータルなポリシーを作ることができれば美しいですが、よほど見識と力量のある責任者がいる場合を除き、やめたほうが無難に思えます。後者のリスクマネージメントとは、所詮、従業員に対して、「余計なことを言ってはならない。言えばあなたに不利益をもたらす」と通達することであり、愉快なものにはなりません。

当社にも、「余計なことを言ってはならない」を主旨とするSNS利用ポリシーは存在します。筆者は、そのポリシー策定に携わりましたが、編集しただけであり、実際にはSNSに造詣の深い多くの社員を集めて議論してもらった結果、できあがりました。ユーザレベルで世界中のSNSを使っている社員がたくさんいることは当社の強みであり、うかつなものは作れないというプレッシャーもありました。

もっともSNSポリシーも文書には違いないので、最初にやったことは、著名な企業の類型文書の収集です。それらを並べ、最小公倍数と最大公約数の項目を作り、コピー・ペーストを存分に行なって配置してから、会社独自の要素を考える……このアプローチ自体がそう悪いとは思いませんが、どうにも腑に落ちるものができあがってきません。

社内にどう提示すればいいのやら、と悩んでいるときに、アドバイザーの社員に教えてもらったのが、U.S.Army（米国陸軍）が開示している Social Media Handbookでした（現在、二〇一三年版が出ています。以下「ハンドブック」）。考えてみれば、軍事における情報の取り扱いは、最重要事項の一つであるはずです。きっと役に立つことが書いてあるだろうという筆者の期待は、裏切られることはありませんでした。

「ハンドブック」の内容

実は「ハンドブック」では、前述したリレーション強化やブランディングのためのポリシーとリスクマネージメントのポリシーが一体となっています。Army Brandingという項があり、危機管理にソーシャルメディアを活用した Case Study があり、部隊単位で Facebook のファンページを持つためのマニュアルがあり、Soldier の心得の項があります。このような一体性は、リスクマネージメントそのものが組織の仕事である軍隊だからこそできることで、素人が真似をするべきではありませんが、ともかく説得力があります。

「余計なことを言ってはならない」と通達するからには、なぜ余計なことを言ってはいけないのか、余計なおしゃべりが組織や個人にどのような影響をもたらすのか、ということに関して納得してもらう必要があります。

例えば、Social Media for Soldiers and Army Personnel という項の一節では、**「取るに足らないと思われる情報であっても、オンライン上で共有することで、愛する人達や仲間が危険にさらされ、殺されることもある」「米国の敵は、ブログやフォーラムやチャットルームや個人のWebサイトをあさりまわり、米国と我が軍に害をなす情報を集めている。敵すなわちアルカイダや国内のテロリストがそれを明かしている」**と迫力十分です。〝The ENEMY is listening〟と大書したステッカーロゴもあります。従業員にSNS利用の危険性を教えるなら、自社のポリシーを配るよりも、「ハンドブック」を全訳して渡したほうが効果的ではないか、と思えるほどです。

ただし本稿の目的は、「ハンドブック」から自社のリスクマネージメントの教訓を引き出すことではなく、「ハンドブック」の内容がいかに興味深いものであるかを紹介することです。実際、とても面白いのです。以下にご紹介するのは拙訳ですので、原文の味わいが伝わりにくいと思われる箇所は原文のままにしてあります。興味ある方は、全てを原文で読まれることを強く推奨します。

ハンドブックのFAQより

Q：自分の部隊にはソーシャルメディアを管理する金も人もいません。
A：Facebook、Twitter、YouTube、Flickr ほか、様々なSNSは無料である。したがって、予算なしでもソーシャルメディアチームを保有することは可能である。（以下略）
Q：自分の部隊のページのフォロワーをどうやって増やせばいいのでしょうか。
A：Be creative.（中略）Don't be afraid to experiment and have fun.
Q：自分は Facebook（Twitter、YouTube）をやったことがありません。どう始めれば?
A：First, know that you're not alone.（以下略）

また、Facebook や Twitter には個別の Quick Reference があります。

●質問に対してはタイムリーに返答すること。
●週末や夜にも投稿してみて、いつの投稿が効果的か評価すること。
●投稿の前に必ずスペルチェックを。Army の評判にかかわる。
●フォロワーに感謝し、時に称賛すること。
●一日に何度も投稿するな。フォロワーを失う。
●推奨しているように見えるから、Pepsi とか Coke とかをフォローするな。

こうした簡潔かつ丁寧な助言があり、もちろん危機回避のための項目もあります。

●位置情報が表示されるプログラムを使うな。
●Remember：You do not control what happens to a message once it is posted. ●Ask yourself "Would I want to retweet this?" before Tweeting. ●Once a Tweet is out there, it is out there.

このように、どこを切っても「ハンドブック」は有益なテキストでありましたが、その内容を当社のポリシーに多く反映したかと言うと、そうでもありません。懇切丁寧なアドバイスは、強い関与の裏返しでもあり、軍隊には軍隊の、当社には当社の、組織と構成員間との適切な距離感があるべきだからです。

一方で「ハンドブック」から読み取れる編集方針、例えば、ルールの意味についてのリアリティある説明、具体的な事例をなるべく挙げる、重要なことについては冗長になることを恐れないといった点については、大いに参考にしました。Quick Reference のような簡潔でリズムのある表現もぜひ真似したかったのですが、こちらはうまくいきませんでした。そして、何より素晴らしいと思うのは、毎年、中身が更改されているところです。「ハンドブック」が本格的にできあがったのは二〇一一年版ですが、二〇一二年版、二〇一三年版と内容が増補されています。作りっぱなしにするのではなく、PDCA（plan - do - check - act）サイクルをきちんと回して、適切なものへとアップデートしていく姿勢こそ、見習うべきでありましょう。■

「ハンドブック」ほか U.S.Army のソーシャルメディア関係文書は http://www.slideshare.net/USArmySocialMedia/documents から参照できます。

人と空気とインターネット

情報端末とのつき合い方

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

**昨今の日常生活には“情報端末”があふれている。
しかし、その恩恵に浴しきってしまうのは、
ある意味、我々に備わっている本来的な判断能力を
損なうことにつながらないだろうか?**

イラスト／山本加奈子

先日、車を定期点検に出したら、一箇所不具合が見つかってしまい、部品を交換しましょう、ということになりました。交換部品はメーカから取り寄せなければならないため、その日は車を預けて、代車を借りて帰ることにしました。お借りした車は初めて乗る車種だったので多少緊張しましたが、整備工場から自宅まではいつも走っている慣れた道でしたので、特に問題なく帰宅できました。ただ、途中に一箇所だけ狭い路地に入らなければならないところがあり、そこはどこを曲がればいいのか分かりにくく、いつもカーナビの地図で確認しながら曲がるのが習慣になっていました。ところが、この日の代車にはカーナビがついていなかったので、その近くに差しかかったとき、私は「あれ、どこを曲がるんだっけ?」と一瞬慌ててしまいました。しかし、いつも曲がる路地ですから落ち着いて見ていれば分かるわけで、しっかりと目で確認しながら、曲がるべきところでちゃんと曲がることができました。

カーナビのようなIT情報端末は、我々が日常生活を営むうえでの様々な判断に必要な、便利な情報をタイムリーに示してくれます。そのおかげで生活がとても簡便になっているのは確かです。しかし、過度に頼り過ぎてしまうと、人間が本来持っていた情報収集能力や分析力、そして判断力を鈍らせることになってしまうのかもしれない……そんなことを考えさせられる出来事でした。

もし情報端末がなければ、自分の目や耳を使って情報を集めて、判断を下し、行動できるはずなのに、おせっかいな情報端末が必要な情報を集めて、使いやすいかたちに加工して、判断に必要な分析もあるていどまで提示してくれることに慣れてしまうと、いざそれが得られなくなった瞬間、判断を誤ったり、取るべき行動が取れなくなってしまうことがあるのではないでしょうか。

科学技術の進歩は、人間の生身の力では不可能だったことを次々と可能にしてきました。例えば、車や電車などの交通手段の発達は、人間が自分の足で移動するのに比べて桁違いに速く、遠くまで移動する力をもたらしてくれました。反面、それに頼っていると、いつしか人間がもともと持っていた身体能力を弱めてしまうものでもあります。現代人は昔の人に比べて、格段に足腰が弱くなっているでしょう。昔の人のように長距離を自分の足で走ったり歩いたりする行為は、今ではスポーツ競技か、二四時間テレビのなかでしか行なわれなくなってしまいました。上記のカーナビの例は、運動能力に関してだけでなく、情報収集・処理能力に関しても同様な劣化が起こっていることを意味しているように思えます。

「いやいや、それは考え過ぎだ」という人もいるでしょう。もちろんカーナビなどなくても、あらかじめ地図で道順を調べて、頭に入れておけば問題ないですし、そもそもカーナビができる前はみんなそうしていたわけですから、できないはずはありません。実際、そういう手間さえ惜しまなければ、情報端末なんてなくても大丈夫なことも多いはずです。

しかし、新しい技術が導入された当初はそう思っていても、いったん便利さに慣れてしまうと、もうわざわざ手間をかけて自分で情報を集めたり、分析しようとは思わなくなるでしょう。そして、カーナビが道順を教えてくれることが常識になってしまえば、それを使うことに何ら疑問を持たなくなるはずです。そうなってしまうと、いざ自分で地図を開いて道順を調べなければならなくなったとき、思うようにそれができなかったり、最近では、そもそも地図で道順を調べたことなどない人も、少なくないのではないでしょうか?

カーナビに限ったことではありません。特に首都圏では電車の乗り換え案内や、最寄り駅から目的地までの道順など、様々な情報をスマホやその他の情報端末に頼っている人が増えています。これは日々の生活のなかで自分自身の行動を決めるために、情報端末から得られる情報に頼るケースが増えている、ということを意味しています。そういう生活に慣れ切ってしまうと、いざというとき、そのような情報サービスにアクセスできないと、何も判断できなくなってしまう危険性さえあるように思います。結果的にそのほうが効率があがるのかもしれませんが、情報を発するシステム側に何か致命的な誤りがあったら、取り返しのつかない事故につながりかねません。

世界を救った男の判断

旧ソビエト連邦、モスクワ近郊のセルプホフ-15というミサイルサイトの将校だったスタニスラフ・ペトロフ中佐は、冷戦のさなかの一九八三年九月二六日の当直中、真夜中に突然鳴り響いた警報に世界の運命を左右する決断を迫られました。それは、監視衛星の警報システムが発した、アメリカから五発の大陸間弾道ミサイル（ICBM）がソビエトに接近しつつあるという警報でした。当時、そのような攻撃を受けた場合のソ連の対応は、米国への即時の報復核攻撃とされていました。しかしペトロフ氏は、米国の先制核攻撃だとすれば、たった五発のミサイルであるはずがなく、何百発ものミサイルが同時発射される総攻撃のはずだと考え、冷静にこの警報をコンピュータの誤報であると結論づけ、上層部へのエスカレーションも行ないませんでした。結果的に、この警報は本当に誤報であったことが分かりました。ペトロフ氏が冷静な判断を下さないで、システムの警報をそのまま信じ、それを上層部に上げていたら、報復攻撃の判断が下されて、核戦争が勃発していたかもしれません。この件は冷戦が終わる頃まで公にされませんでしたが、今ではペトロフ氏は、核戦争を未然に防ぎ「世界を救った男」と言われることもあります。

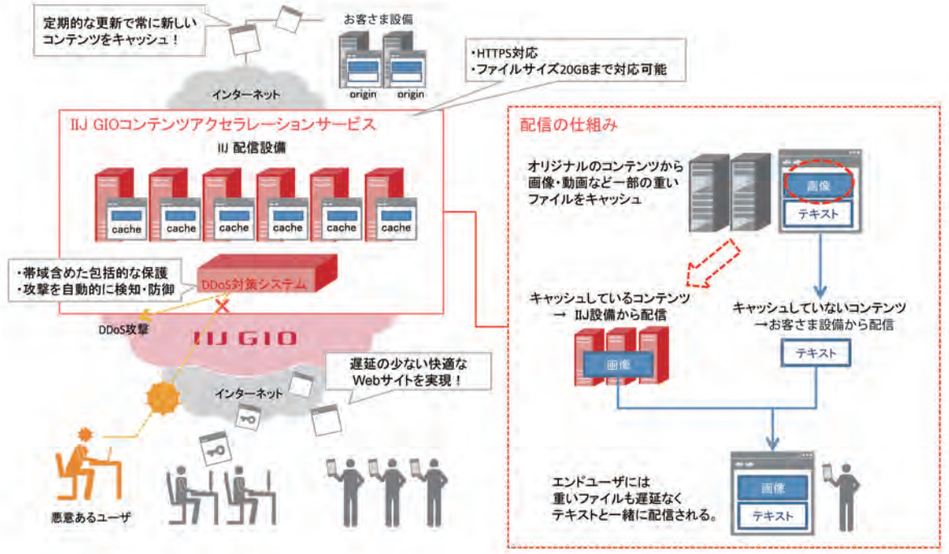
さすがにこの例は大げさに聞こえるかもしれませんが、作り話ではなく本当にあったことです。ペトロフ氏のように、システムや端末からまことしやかに提供される情報を鵜呑みにするのではなく、たまにはそれが本当かどうかを疑って検証してみたり、「何となく怪しい」と勘を働かせてみることも、今後の高度な情報化社会において、ますますおせっかいになる情報端末をうまく使いこなしながら生き延びていくには必須ではないでしょうか。

現代社会では、何もしないと運動能力がどんどん劣化してしまうので、それを防ぐためにわざわざジョギングをしたりトレーニングジムに通ったりすることが普通になっていますが、近い将来、生身の人間としての情報処理能力を劣化させないために、情報端末をいっさい信じないで、身の回りのことを自分の感覚と頭だけで対処するようなトレーニングが大流行するかもしれません。

手軽に利用できる クラウド型Webコンテンツキャッシュサービス
IIJ GIOコンテンツ アクセラレーションサービス

IIJ プロダクト本部 プロダクト開発部 アプリケーションサービス課長
田口景介

IIJ GIO コンテンツアクセラレーションサービスは、ピークトラフィックのサイジングがむずかしいWebサイトに最適なContents Delivery Networkサービスである。



IIJ GIOのラインナップに、新たにCDN（Contents Delivery Network）サービスであるIIJ GIOコンテンツアクセラレーションサービス（Contents Acceleration Service。以下「CAS」）が加わりました。必要なときに必要なだけ、すぐさま配信に必要なリソースを手配し、システムを柔軟に構成できる、まさに“クラウド”と呼べるサービスです。

クラウドファースト時代のCDN

一般的にCDNサービスは、Web サイトの配信性能、安定性、信頼性の向上をもたらします。CASはそれに加えて、即時利用が可能なうえに、利用量に応じた従量課金のみで、初期費用や基本料金は不要というクラウドスペックでサービスが提供されるため、急激なアクセス集中が予想されるサイト、普段からトラフィックの緩急が激しいサイト、イベント期間中だけ一時的に用意されるサイトなど、必要とされる配信性能が大幅に変動し、一時的なピークトラフィックのサイジングがむずかしい場合に最適です。

コンテンツに注目が集まり、アクセスが急増することは喜ぶべき事態ですが、それが行き過ぎて想定されたサイジングを超えるのは、悪夢のような状況です。そんなときCAS を導入しておけば、アクセス数が増加するにしたがって、ネットワークやサーバリソースが適切に割り当てられ、オリジンサーバに代わってキャッシュされたコンテンツの配信が行なわれます。これにより、コンテンツがキャッシュされる限りは、オリジンサーバには平常時のアクセスをさばけるだけの能力があれば十分となり、変動するトラフィックは、CASの能力によってまかなわれます。

また、事前に想定できなかった突発的なアクセス集中に対しても、CASなら対応可能です。具体的には、IIJのカスタマーサポートサイトからCASを申し込み、DNSの設定を変更するだけで（サイトのホスト名に対してCNAMEレコードを設定）、基本的な構成ならば即座に利用が可能です（DNSが切り替わり、キャッシュが行き渡るまでにある程度の時間を要するかもしれませんが、機材増強に必要な時間を考えれば、「即座」と表現しても差し支えないでしょう）。

高性能と機能性を両立させるハイブリッドキャッシュシステム

そんなCASの実体はと言うと、もっとも簡単に表現すれば、IIJの広帯域・高品質なネットワーク回線に接続され、複数の異なるキャッシュシステムを備えたリバースプロキシサーバ群です。ここでのポイントの一つは、IIJ のネットワークであるということですが、もう一つは、特性の異なるキャッシュサーバを組み合わせたハイブリッドシステムであるということです。

一方のキャッシュサーバは、比較的小さなファイルを短期間だけキャッシュし、大量のコネクションを高速にさばけるようにチューニングされています。もう一方のキャッシュサーバは、より大きなファイルのキャッシュが可能です（最大20GBまで）。それだけでなく、パスに応じて「キャッシュする／しない」を設定したり、特定のクエリストリングが付けられたURLについては、オリジンサーバのレスポンスにかかわらず、キャッシュを強制したり、IIJのカスタマーサポートサイトから、管理者が指定したポリシーに応じて、システムの動作をカスタマイズする機能を備えています。さらには、いったんキャッシュされたコンテンツをCASから取り除くことにより、キャッシュの有効期限切れを待つことなく、新しいコンテンツを配信する機能も備えています。

つまり、非常にシンプルでありながら、極めて高速に処理を行なうシステムと、柔軟性に優れた高機能なシステムが連携して、一つのCASというサービスを実現しているのです。なぜこのようなハイブリッドシステムとして構成されているかと言うと、ひとえにサイズの異なる様々なコンテンツを効率よくキャッシュし、広大なネットワーク帯域とキャッシュシステムの能力を使い切るためです。

なにしろ、一口にWebサイトのコンテンツと言っても、ごく小さなインライン画像を大量に含む 1 ページのコンテンツもあれば、数GBのアプリケーションファイルもあるといったふうに、HTTPという転送路に乗せられるコンテンツは本当にバラエティに富んでいます。それはつまり、シンプルなコンテンツながら毎秒数万コネクションの接続数を要求するサイトもあれば、同時接続数は数百ながら数GBの大きなデータを淀みなく流し続けたいサイトもあるということです。

こうした性格の異なるサイトを、巨大な一つの配信システムでまかなうために導き出されたのが、CAS のシステムというわけです。

組み合わせて実現する様々な価値

ここまではCASのエッセンスとなる能力について述べてきましたが、その他にも悪意あるアクセスから守るDDoSプロテクション連携オプションやSSLオプションなどが用意されています。

このDDoSプロテクション連携オプションを提供したことで、クラウド環境とインターネットを結ぶセキュリティゲートウェイとしての役割を期待されるなど、当初は想定していなかったニーズも出てきました。

通常、ファイアウォールや WAF（Web Application Firewall）、DDoSプロテクションなどを導入するには、ある程度ネットワークの構成変更を必要としますが、多くのクラウドでは、今のところそこまで自由にネットワークを構成できないか、手間がかかるためクラウドサービスの一環として提供される機能を利用するのが一般的です（もちろん、そうした機能が提供されていなければ、利用できないということになります）。一方 CASは、言ってみればリバースプロキシですから、導入の敷居が低く、DDoSプロテクションのような機能をクラウド環境にアドオンできます。

今後は、IIJが提供するサービスと連携して、様々な付加価値を生み出していけるような機能を追加していく予定です。例えば、DNSサービスや監視サービスをCASと組み合わせることで、より高度な広域負荷分散を実現できるようになります。また、大規模災害対策を目的として導入しやすい仕組みを提供したり、IIJ GIOホスティングパッケージサービスと連携して、オリジンサーバに IIJサービスを利用した場合に、より能動的にキャッシュ管理を行なえる仕組みを提供する、といったことも考えています。このようにCASは、引き続きサービスの魅力を高めていきます。

プジョー・シトロエン・ジャポン株式会社
本　社　東京都渋谷区東3-16-3
　　エフ・ニッセイ恵比寿ビル
資本金　4億円（2012年3月1日現在）
URL　http://www.peugeot.co.jp/
URL　http://www.citroen.jp/

仮想化プラットフォーム「VWシリーズ」を基盤にコスト効果の高いディーラー向けシステムを実現

フランスの自動車メーカ、プジョー・シトロエンの日本法人、
プジョー・シトロエン・ジャポン株式会社では、
新たに提供する国内ディーラー向け会計システムの基盤に、
「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」を採用。
VMware vSphereをインストール済みのサーバリソースやストレージリソースを活用し、
システムの早期稼働とアセットレスによるコスト効果の高いプライベートクラウドを実現している。

プジョー・シトロエン・
ジャポン株式会社
総務部
システム グループマネジャー
室 雅雄 氏

プジョー・シトロエン・
ジャポン株式会社
総務部
IT担当
府川岳洋 氏

株式会社QES
営業本部 金融・法人営業部 次長
舛岡敏幸 氏

フランスの自動車メーカ、プジョー・シトロエンはヨーロッパトップクラスの売り上げを誇り、さらなる国際化とラインナップの拡充を進めている。また、環境に対する取り組みを積極的に推進し、ハイブリッド技術を採用したモデルの開発にも力を入れている。

プジョー・シトロエン・ジャポン（以下、PCJ）では、全国に正規販売店網を展開し、ディーラーは国内で約80社、150拠点を数える。「ディーラーに対し、推奨するDMS（Dealer Management System）と呼ばれる業務系のシステムを用意し、車両や部品のカタログ・出荷情報、その他マスター情報などを提供していますが、ディーラーからはシステムに関する様々な要望が寄せられていました」と、PCJのシステム グループマネジャーを務める室雅雄氏は述べる。

サーバなどのITリソースを利用しプライベートクラウドを実現

ディーラーではDMSから提供されるデータを、自社の会計システムに仕訳入力する。入力作業の手間がかかるだけでなく、入力ミスによるシステム間のデータ不整合が発生するリスクも皆無ではない。そうしたなか、会計システムのリプレースを控えたディーラーから、DMSと連携できる会計システムを提供してほしいという要望があったという。

「専任のIT担当者を配置することがむずかしいディーラーもあります。インターネットを介してセキュアかつ手軽にDMSと会計系システムの連携やデータバックアップが行なえる仕組みを提供したいと考えていました」と室氏は述べる。そして、PCJが導入している会計システムのパッケージをベースに、仮想化環境による会計システムの検討を開始した。

ディーラー向け会計システムを検討開始後、「ITソリューション会社のQESから、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、VWシリーズ）を紹介されたのです。vSphere環境の管理が自由で、ITリソース自体もサービス提供されていたので、リソースの増減を調整でき、コストを抑えられると判断しました」とPCJのITを担当する府川岳洋氏は振り返る。そして、IIJのパートナー企業であるQESの舛岡敏幸氏は「IIJ GIOサービスは高い信頼性が要求される金融機関などにも導入されており、自信を持って推奨させていただきました」と付言する。

VWシリーズは、VMware vSphereをインストール済みのESXiサーバを始め、メニューが多彩なデータストアと呼ばれるストレージ、ネットワークの各リソースプールからシステム用途に合わせて、必要な分だけリソースを選び、仮想化基盤として利用可能。サーバやストレージを購入することなくプライベートクラウドの構築もできる。また、VWシリーズでは、vSphereだけでなく、vCenterをプリセットしたサーバも標準利用が可能で、ユーザ自身で仮想基盤を自由に構築できる利点がある。

ミッションクリティカルなシステムを「VW シリーズ」上に構築

ディーラー向け会計システムの構築は、PCJのシステムを担当するインテグレータが実施。具体的には、VWシリーズを仮想化基盤として、会計システムのフロントサーバを始め、ADサーバやファイルサーバ、DBサーバ、仮想デスクトップのXenAppサーバ、仮想ファイアウォールなどの仮想サーバを載せ、ミッションクリティカルなシステムを構成した。

会計システムはクライアント／サーバ型のアプリケーションのため、XenAppのブラウザ経由で画面転送を行なっている。「これにより、ディーラーはアプリケーションの違いを意識することなく、インターネットを介して安全にクラウド上の会計システムを利用できます」と府川氏は仮想デスクトップの狙いを説明する。

そして、室氏は「多数のディーラーがいっせいにクラウド上の会計システムを利用する場合にも、安定稼働できる高い信頼性が重要です」と強調する。そこで、サーバを冗長化するなど高可用性のシステムを構成。障害時のサーバ切り替えなどの検証を経て、2013年1月からディーラー向け会計システムの本格稼働を開始した。

まずは、自社運用の会計システムのリプレースが間近なディーラー2社からスタート。「スモールスタートし、ディーラーの増加など必要に応じてシステムを拡張できることもクラウドサービスの利点です。余裕のあるシステム構成により、当面はサーバ台数を増やさずに拡張できます」と室氏は述べる。また、府川氏は「タイトなスケジュールのなかで、IIJはVWシリーズの基盤をスピーディーに提供してくれました。その後のシステム構築もスムーズに行なえ、本番稼働を迎えられました」とIIJの対応を評価する。

ディーラーは、DMSとの自動仕訳連携により、会計システムへの入力作業が不要になるなど、業務の効率化やリアルタイム処理による売り上げデータの早期把握が可能になると期待している。PCJではIT分野の支援を含め、各ディーラーへのバックアップを通じて日本市場の拡大を推進していく。そして、IIJはパートナー企業とともに、企業ニーズにマッチしたクラウドソリューションを提供していく考えだ。

メールの気持ち

IIJ 執行役員 サービスオペレーション本部長
山井美和

『ミクロの決死圏』という古いSF映画をご存じでしょうか。人間が乗った潜航艇ごと縮小して、脳内出血で倒れた亡命科学者の血管から体内に入り、疑心暗鬼な人間関係のもと、1時間というタイムリミットのなかでオペレーション（手術）を成し遂げて、涙腺から涙と一緒に体外に出て生還するという映画です。

生身の肉体ではないですが、これと似たようなことをインターネットに置き換えてみるとどうなるのか、想像してみました。私がメールに添付されてインターネットのなかを旅してみようかと……。

まず、送信者の PC のなかにファイルとなって、送信を待ちます。送信者がメーラの送信ボタンをクリックすると、ソフトウェアによって私がメールのエンベロープのなかに、暗号化された文字記号の羅列として組み替えられます。意識はありませんね、きっと。

送信者の PC からルータに入ります。自分はどこに送られるのかさっぱり分かりませんから、夢でも見ながらデータストリームに身を任せて、あちこちに送られて行きます。

何個かのルータを経由したのち、とあるサーバのスプールのなかに保存されている状態で目を覚ましました。さて、これからどうなるのかなと待っていると、誰かから呼び出されて、また同じようにデータストリームに乗って、宛先の人の PC に社内のネットワークを経由して送られて行きました。そこで初めて相手の人の目に留まり、長い旅は終わったはずでした。

ところが、もう一人の自分がいるのです。最初に目覚めたときに見た人とは別の人がもう一人の自分を見ているのです。私は眠っているあいだに、なんとコピーされていました。To とか Cc とか、場合によっては存在を知られたくない Bcc とか。何人もの私ができあがっているではありませんか……。

かなり簡単に書きましたが、メールが相手に届くまでには、たくさんのネットワーク機器やサーバを仲介して行きます。そのメールの気持ちになってサービスを考えてみようと思ったわけです。

メールは今や大切なビジネスツールであり、ネットワーク社会の大切な基盤でもあります。SMTP によるメールの仕組みは、ある意味ではよくできていて、今ではメールを確実に届けることもでき、迷惑メールがないかしっかり目を光らせたり、ウイルスを取り除いたりできるようになりました。

また、事業者側でメールをお預かりし、ネットワークにつながれば、Web ブラウザを使ってどこからでも閲覧できるなど、様々な改良が加えられご利用いただいていると思います。

ただ、メール自身に成り代わってみると、読んでもらいたいのに読んでもらえないメール、捨てられると分かっているメール、間違って送られて迷惑がられるメール、読み終わったらさっさと削除されるメール……等々、「さみしい思いをしているメールも結構あるな」と思うようになりました。

メールの立場になれば、「どうせ日の目を見ないのだからさっさと消してくれぃ！」という威勢のいいメールもいるはずで、「断捨離」なんてものを始めて身軽になってみるのも、一つのライフスタイルかもしれません。

我々の使命は、こうした日の目を見ないメールも含めて、24時間365日、メールをしっかりとお届けできるよう、日夜、努めることです。メールの“声なき声”を自分たちがメールの気持ちになって、社会インフラとなったインターネットの主要な通信手段の一つとして運用し、お客さまをサポートしています。山

イラスト／山本加奈子

●インターネット・トリビア

インターネットと広告

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

Ｗｅｂサイトを見ていると、企業の運営するポータルサイトでも個人のブログでも、何かしらの「広告」が掲載されていることが大変多くなっています。こうした広告が増えているのは、インターネットの一般化によりＷｅｂサイトの媒体価値が高まったことはもちろんですが、インターネット広告ならではの「アドネットワーク」という出稿方法が普及したことも大きな要因と言えます。

新聞や雑誌では、広告主はどの媒体のどの場所に広告が掲載されるかを指定して広告を出稿します。ところが、アドネットワークでは、広告主は広告が掲載されるＷｅｂサイトを指定しません。

アドネットワークとは、その名の通り、広告を掲載したいＷｅｂサイトの「ネットワーク」です。広告主がアドネットワークに対して条件を指定し広告を登録しておくと、そのネットワークに参加しているＷｅｂサイトに自動的に広告が配信されます。このような仕組みを利用することで、広告主は多数のＷｅｂサイトに一度に広告を配信でき、Ｗｅｂサイトは個別の営業を行なうことなく広告収入を得ることができるのです。

ただし、アドネットワークは良い面ばかりではありません。ネットワークへ広告を登録する際にある程度の条件を設定できますが、どれだけ狙い通りに広告が掲載されるかは未知数です。

反対に、広告を掲載するＷｅｂサイトにとっても、どのような広告が配信されるか事前に分からないという不安があります。Ｗｅｂサイトのイメージにそぐわない広告が掲載され、閲覧者に不快な思いをさせてしまうというケースも考えられます。

アドネットワークによっては、広告主・Ｗｅｂサイトの双方に基準を設けて審査を行なうことで、このようなミスマッチをできるだけなくすように努めているところもあります。アドネットワークを利用するときは、そのネットワークがどのような基準で運営されているかを確認することが重要です。山

※関連する話題をIIJ公式技術ブログ「てくろぐ」に掲載しています。http://techlog.iij.ad.jp/archives/iijnews116

Information

IIJmio 高速モバイル／D サービス「増量先取り！ご愛顧感謝キャンペーン」

NTTドコモのLTE 網を利用した個人向けデータ通信サービス「IIJmio 高速モバイル／D サービス」では、2013年9月1日の仕様変更に先立ち、「増量先取り！ご愛顧感謝キャンペーン」を実施しております。

・実施期間：2013年6月1日～8月31日
・実施内容：LTE／3G による高速通信が可能なデータ量（バンドル クーポン）を増量します。
▼ファミリーシェアプラン：月間 1GB → 2GB
▼ライトスタートプラン：月間 1GB → 2GB
▼ミニマムスタートプラン：設定なし→月間 500MB

詳細：https://www.iijmio.jp/info/iij/20130426-2.html

IIJ 公式 Facebook アカウントのご紹介

▼IIJ 公式ファンページ
プレスリリースやお知らせ、技術・開発情報、イベント・セミナー情報など、IIJ に関する様々な情報をお届けします。
https://www.facebook.com/IIJPR

▼IIJ GIO 公式ファンページ
IIJ GIO の最新情報をお届けするとともに、ファン限定のコンテンツやイベントも予定しています。
https://www.facebook.com/IIJGIO

▼SEIL 公式ファンページ
SEILに関連する最新情報や活用方法、便利な設定方法、開発秘話などをお届けします。
https://www.facebook.com/SEIL.jp

▼MOGOK 公式ファンページ
MOGOKの最新情報をお届けするとともに、ファン限定のコンテンツやイベントも予定しています。
https://www.facebook.com/IIJMOGOK

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」編集部
〒101-0051 東京都千代田区神田神保町1-105
神保町三井ビルディング
TEL：03-5259-6310
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／すげさわ かよ
デザイン／B.C.
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
Internet Initiative Japan

株式会社インターネットイニシアティブ

本社　東京都千代田区神田神保町 1-105 神保町三井ビルディング
〒101-0051　TEL：03-5205-4466

関西支社　大阪府大阪市中央区北浜 4-7-28 住友ビルディング第二号館 5F
〒541-0041　TEL：06-4707-5400

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1条西3丁目3番地 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

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　広島県広島市南区稲荷町 2-16 広島稲荷町第一生命ビル 11F
〒732-0827　TEL：082-506-0700

横浜営業所　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

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（IIJ Global）
東京都千代田区神田神保町 1-105 神保町三井ビルディング
〒101-0051　TEL：03-5217-5700

株式会社ネットケア（Net Care）
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
〒101-0041　TEL：03-5205-4000

ネットチャート株式会社（NCJ）
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（hi-ho）
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（IIJ-II）
東京都千代田区神田錦町 3-13 竹橋安田ビル 3F
〒101-0054　TEL：03-5205-6501

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

株式会社 IIJ エクスレイヤ（IIJ-EX）
東京都千代田区神田神保町 1-105 神保町三井ビルディング
〒101-0051　TEL：03-5205-6580

IIJ Europe Limited（IIJ-EU）
15-25 Artillery Lane London E1 7LP, U.K.
TEL：+44-0-20 7650 5966

株式会社トラストネットワークス（TN）
東京都千代田区神田神保町 1-105 神保町三井ビルディング
〒101-0051　TEL：03-5282-3358

Ongoing
Innovation

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。(2013年6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。
＊ 本書は著作権法上の保護を受けています。本書の一部あるいは全部について、著作権者からの許諾を得ずに、いかなる方法においても無断で複製、翻案、公衆送信等することは禁じられています。

IIJ-MKTG001AA-1306BK-10300PR