IIJ.news
June 2012
vol.110

【特集】

セキュリティ2012
―最新情報と人材育成―

ぷろろーぐ

ダービーの熱気

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**

初夏の光を浴びて、鍛えられた姿の競走馬が、緑のターフに躍動する。その光景は、淀んで弛緩した日常を忘れさせる。一年ぶりに競馬場を訪れる。張りつめた空気は、磨き抜かれた競走馬のしなやかな筋肉の動きがもたらすのだろうか。四コーナーを回り、長い直線、騎手の激しい鞭が飛ぶ。蹄の音が近くなって、目の前を疾走する。競馬場に来ると、時間が経つのを忘れる。

友人に誘われ、日本ダービーに行く。競馬から遠ざかり、馬の名前もわからなくなったのだが、競馬場に来ると、不思議な昂ぶりを感じる。眺めているだけでなく、何レースも馬券を買って楽しむわけで、賭けのひとつには違いないけれど、そこには日常で失われた緊張感の漂う美しさがある。それは、速く、強く走るためだけに調教を施された、競走馬に特有の緊張を強いる姿があるからだろうか。

さまざまな儀式があって、ダービーに出走する選り抜きの競走馬が馬場に散る。一〇万人を超える観衆の熱気と興奮が競走馬に伝わるのか、馬場に踏み入れた途端、その肢体を伸ばし、走る。それはウォーミングアップというより、走ることで緊張を解き放つかのようだ。レースとは逆方向に、観衆のどよめきが遠くなる四コーナーまで走り、今度はゆったりと騎手と会話をするように歩む。

レースが始まる。ダービーに酔う観衆の興奮が、大きなどよめきとなって、競馬場を覆う。レースは二分半ほどで終わる。四コーナーから直線に向き、ゴールまでの数百メートル、大観衆の熱狂は頂点に達し、歓声に包まれてゴールを駆け抜ける。身体が震えるほどの感動である。購入した馬券を忘れて、その一瞬に酔う。

毎年、ダービーに来るたびに、今では忘れ去った興奮や熱気にひたるのである。馬の名前すらおぼつかない私の馬券が当たることは稀で、当たるときは偶然のたまものである。今回のダービーで二着になったフェノーメノという馬がターフに現れたときの圧倒的な輝きに魅せられたのだが、結果はハナ差の二着だった。もしかして、私にも競馬を見る目があるのかも知れないと、嬉しかったのだが、馬券は当たりを避けるような買い方で、当然のことながら、お小遣いにはならなかった。それでも、久しく忘れていた肌が震えるような感動をしたことで、充たされた一日となった。来年もまた、来ようと。

私が社会人になった頃は、まさに高度成長期の渦中だった。長く続いた自堕落な学生時代が終わり、就職をしても、遠い傍観者として社会人を過ごすはずだったのが、ワーカホリックと言われるほど働き詰めの生活になって、折節、そんな自分の姿を不思議な思いで眺めていた。

現在の新入社員とは較べようもないほど貧しく、半ドンの土曜日の過ごし方にしても、雀荘で昼食をとり、夜まで麻雀を続け、居酒屋で飲んで帰るといった侘しい暮らしだったけれど、何だか憑かれたように働いた。体力があったせいで、週に二、三日は徹夜で働いていた。急げ者の典型だった私のような人間まで、高度成長期の興奮と熱気に巻き込まれていたに違いない。一〇数パーセントも経済が拡大する時期というのは、そんなものだったのかも知れない。それが愚かな時代だったのか、いい時代だったのか、わからないけれど、たしかにそんな時代があって、挙げ句の果てにバブルに浮かれ、崩壊してから二〇年も経った。失われた一〇年とか二〇年とか言われるけれど、社会から何が消えたかと言えば、時代を動かす熱気であり、人々の欲望の大きさだろうか。

淀んで、沈み込んだ空気が蔓延する日本に、あの熱に浮かれたような、豊かさへの欲求や将来への思いが膨らむ時代が蘇るようなことはないと、競馬場の熱気をあとにした帰り道、ふと、そんな思いにとらわれたのである。

イラスト／山本加奈子

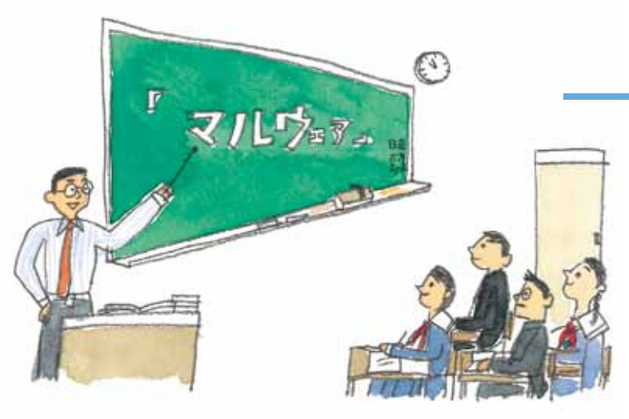
IIJ.news
June 2012
vol.110

Contents

表紙のコトバ　すげさわ かよ

雨空の下、傘を広げて歩いていると、満開の紫陽花が目に入り、その鮮やかな薄藤色にぱっと気持ちが明るくなることがあります。どんより曇った梅雨の季節だからこそ、一段と色の美しさが心に染みるようです。

セキュリティ2012
―最新情 報と人材育成―



特集イラスト／なかだえり

今回は、情報通信分野における“セキュリティ”を特集する。
インターネット上で発生するインシデントは、
年々増加すると同時にその手法も複雑化・巧妙化の一途をたどっている。
それにともない、セキュリティの専門家のみならず、
多くの一般ユーザにも正確な知識と対応能力が求められている。

セキュリティ対策の人材の育成

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

昨年来のサイバー攻撃の頻発を受けて、情報通信環境におけるセキュリティ対策に注目が集まっています。特に、国家規模の諜報活動や産業スパイ活動の一環とも考えられる特定組織に対する標的型攻撃、Ｈａｃｋｔｉｖｉｓｍによる国家や企業のシステムに対するＤＤｏＳ攻撃や情報漏洩などが、一般の企業に対する現実の脅威として考えられるようになってきました。このため、攻撃を受ける組織の業務や防御状況などを踏まえたうえで、個別に情報把握、攻撃予測、対策などを実施する必要が出てきました。

一方で、一般の企業などで日常的に利用する情報通信環境において、決して従来の脅威を忘れてしまっていいという状況ではありません。例えば、二〇〇八年に発生したＣｏｎｆｉｃｋｅｒは、現時点でも世界中で数百万台の端末が感染したままになっていますし、情報通信に利用するシステムやソフトウェアには日々脆弱性が発見され、ネットワークやメモリデバイス、Ｗｅｂなどからのマルウェア感染の危険はなくならず、内部犯行など人的要因による事件も発生し続けています。このため、インターネットから組織内ネットワークまで、情報通信環境のうえでは、依然として従来のセキュリティ対策も適切に実施することが求められています。

さらに、一般の組織においても、コストや利用者からの要望などにより、クラウドコンピューティングやスマートフォンといった新しい情報通信技術への対応も迫られており、これらの要素を考慮したセキュリティ対策について、導入時に検討し実現する必要が生じています。

特に、昨年度後半に立て続けに明らかになった一連の標的型サイバー攻撃に対応するために、自組織の情報通信環境を確認するための監査や、新しい対策手法の導入などを急ピッチで進める必要がありました。また、攻撃を受けた組織では、攻撃端末の特定、マルウェアの解析、組織内のサーバや端末への調査、通信ログの調査、フォレンジックによる情報漏洩の有無の確認などの影響調査や、再発防止策の策定と適用を実施する必要があり

ました。これらの作業のうちいくつかは、専門技能を有する人によってなされる必要があり、セキュリティベンダのサービスを利用して実現します。

しかし、こうした要望の急激な増加に対して、国内ではセキュリティ技能を有する人材が不足して適切に対応できない状況が発生し、大きな問題となっています。内閣官房長官を議長とする情報セキュリティ政策会議でも、本年一月に開催された第28回会合において、緊急対応を行なうＣＳＩＲＴ組織の整備、情報交換の緊密化などとともに、情報セキュリティ人材の育成が重要であるとされています。

では実際には、どのような人材が求められているのでしょうか。セキュリティの専門の技能を有する人材育成は、たしかに大きな課題です。情報通信環境のセキュリティは、システムの脆弱性に関する知識、マルウェアの発見から解析手法に関する知識、情報通信システム内部での影響評価など、攻撃手法と防御手法の双方に精通しなければならない高度な専門技能を要します。くわえて、進歩や変化についていくためには、常に新しい技術を吸収し続ける必要があります。このような専門家の育成の場として、ＣＴＦ（Capture The Falg）形式の国際セキュリティイベントへの国内代表の参加や、学生向けのセキュリティ教育イベントなどが報道で大きく取り上げられるようになりました。

一方で、一般的な企業においても、セキュリティ人材が必要となってきています。例えば、標的型攻撃の対応では、攻撃を受けた組織における適切な対処により、攻撃の影響を少なくできます。これはつまり、日常的な業務もセキュリティを意識して実施するのが重要であることを示しています。また、専門家によるセキュリティのサービスを受けるときも、自組織の業務や情報通信環境に精通していながら、ある程度のセキュリティの知識を有する人が必要であることを意味しています。先の情報セキュリティ政策会議でも、「経営幹部から一般の従業員をふくめたマネジメントスキルの涵養が重要である」とされています。

このように一般の仕事をする人にセキュリティの知識を持ってもらうためには、まず、多くの企業で行なわれている社内の情報教育やセミナーなどの活用が考えられます。また、さまざまな事業分野で実施されている既存の人材育成の活動をこの目的で活用することもできます。例えば、ＩＩＪの属する通信分野では、セミナー形式の勉強会、研究ワークショップ、実務者による演習などが行なわれており、これらは広い意味でセキュリティの人材育成のための活動と言えます。

今必要なセキュリティ人材の素養と規模を想定したうえで、これらの活動をその人材の育成に向けて調整していくことが、人材不足の状況を改善するためのもっとも効果的な方法だと考えることができます。

［座談会］

情報セキュリティの人材育成
～MWSの試みを通して

**標的型攻撃やDDoS攻撃など、インターネット上の脅威が後を絶たない。
その一方で、情報セキュリティに関して正確な知識を持ち、
適切に対処できる人材の不足が懸念されている。
ここでは、セキュリティに携わる人材育成の現状や課題について
専門家の見解をうかがった。**

（出席者）
株式会社日立製作所 情報・通信システム社
寺田真敏

NTTコミュニケーションズ株式会社
畑田充弘

（司会・進行）
株式会社インターネットイニシアティブ
齋藤 衛

齋藤 衛（さいとう・まもる）
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。マルウェア対策研究人材育成ワークショップ2012実行委員、テレコムアイザックジャパン運営委員、他。

畑田充弘（はただ・みつひろ）
NTTコミュニケーションズ株式会社 先端IPアーキテクチャセンタ 主査、セキュリティ技術ユニットリーダー。早稲田大学大学院理工学研究科情報・ネットワーク専攻修了。マルウェア対策研究人材育成ワークショップ2012実行委員長兼プログラム委員長、他。

寺田真敏（てらだ・まさと）
株式会社日立製作所 日立インシデントレスポンスチーム チーフコーディネーションデザイナ。博士（工学）。情報処理学会教育担当理事、マルウェア対策研究人材育成ワークショップ組織委員、テレコムアイザックジャパン運営委員、JPCERTコーディネーションセンター専門委員、情報処理推進機構セキュリティセンター研究員、他。

セキュリティを担う人材とは？

齋藤　今回は、「マルウェア対策研究人材育成ワークショップ」（以下、ＭＷＳ）の委員のお二人にお越しいただき、情報セキュリティを担う人材育成の話題を中心にお話をうかがいたいと思います。

二〇一一年の九月以来、「標的型攻撃」が連続して発生しており、情報セキュリティ業界は対応に追われています。そうしたなか、「情報セキュリティに関わる人材が不足しているのではないか」という声をよく耳にします。寺田さん、畑田さんは、情報セキュリティの人材育成について、どのようなご意見をお持ちでしょうか？

寺田　情報セキュリティの人材育成で大切なのは、まず学生の頃から現実に起こっている問題の解決に取り組んでもらうことでして、それがそのまま人材育成につながると考えています。というのは、情報産業の世界は大変なスピードで変化しており、ひと昔前のように大学を卒業したあと実社会に出て、それから情報セキュリティを学んでいたのでは、なかなか実社会とのギャップを埋めることができないからです。

畑田　たしかに大学でコンピュータやネットワークの基礎を学んで会社に入り、セキュリティ関連の仕事に就いたとき、学生時代に学んだことと現実問題とのギャップはかなり大きいと思います。

一般には、ウイルス対策をするとか、セキュリティパッチをあてるなど、個々の対策があります。しかし、現実には一部にそれを実施できない環境もあり、そのギャップをどうバランスをとって埋めるのかに苦労することが多いのではないでしょうか。なぜなら、技術面だけではなく、セキュリティポリシーやコストを考慮しないといけないからです。そういった実態を把握したうえで、対策を講じられる人材を育てることは急務だと思います。

齋藤　そもそもセキュリティとは、何かが正常に動いている状態を指す言葉ですから、ＩＩＪのようなＩＳＰにとってのセキュリティは、通信がきちんと機能している状態のことです。そうだとすると、通信に携わる専門家が「健全な状態」、つまり「セキュリティ」を意識しながら仕事をするのが、一番のセキュリティ確保につながるのではないでしょうか。

人材育成に関しても、理想を言えば、セキュリティの専門家を育てるというより、セキュリティを意識しながら各現場で働くことのできる人材を育てる必要があると思います。

寺田　齋藤さんのおっしゃる通りで、各業務にセキュリティ項目が含まれているべきですね。

先進的なＭＷＳの取り組み

齋藤　では、ＭＷＳの話題に移りたいと思います。情報セキュリティの人材育成の面で、ＭＷＳの試みは他とは一線を画した独自のものだと思うのですが、最初に活動の概要や実績などを紹介していただけますか。

畑田　ＭＷＳは、サイバークリーンセンターで収集していたボットの観測データを「研究用データセット」として活用することを目的に、二〇〇八年に発足しました。

研究者、企業のセキュリティ技術者、学生などが、同じ研究用データセットを使って解析技術の評価に利用し、その結果をＭＷＳで発表することで、研究成果を共有するという活動を行なっています。

研究の主なテーマは、「検体解析技術の研究」「感染手法の検知ならびに解析技術の研究」「ボットの活動傾向把握技術の研究」という三点です。

また、二〇〇九年からは、「ＭＷＳ Ｃｕｐ」というマルウェア解析のコンテストも実施しています。これは、一時間半という制限時間内に各チームが解析して、その技術を競う催しです。

寺田　ＭＷＳの発足当初は、マルウェアを研究する人たちに、必要な素材が行き渡っていない状況を何とか改善したいという想いがありました。さらに、同じテーマの研究成果を検討する際、同じデータを用いていないと結果を横並びで比較できません。そこで、共通の素材を研究用データセットとして提供し、各自の成果を検討できる場を設けようというのが二つ目の狙いでした。三つ目には、研究というものは、その分野が成長し続けていかないと、関心を持つ人が減って人材確保がむずかしくなる。すると、「マルウェア対策は市販のソフトやセキュリティベンダに任せればいい」ということになり、最後は、「この分野の研究はやらなくてもいい」という結論になってしまいます。我々はそれではいけないと考え、人材育成と研究を兼ねたワークショップを通して、みなで一緒に少しでも良い研究環境を整えていこうと考えました。

畑田　寺田さんのお話に付け加えますと、当時、サイバークリーンセンターで対策活動を行なうなかで、膨大なデータが蓄積されていました。しかし、それらをフルに活用できていたかというと、決して

そうではありませんでした。当然、そのデータを活用できれば、もっと良い成果を出せるはずだと思っていたので、サイバークリーンセンターのデータを研究者に提供して、成果を共有する場を設けると同時に、研究素材として継続的に使用できるデータセットを作るためのスキームを築いていこうということで、ＭＷＳを立ち上げました。

齋藤　スタートが二〇〇八年ということは、今年で五年目になりますね。

畑田　そうです。コンピュータセキュリティシンポジウムと同時に開催していて、三日間で二〇～三〇件の研究発表が行なわれます。ＭＷＳのセッションは非常に注目度が高く、一〇〇人弱が集まって活発な議論を行なっています。

齋藤　共通の研究用データセットを用いて相互に検討するという試みは、過去にもあったのでしょうか？

畑田　ネットワークの侵入検知の分野で「ＫＤＤＣｕｐ１９９９Ｄａｔａ*」という研究用データセットがありました。

寺田　ただ、このデータセットは、ＭＷＳのように継続的に提供されているものではありませんね。

齋藤　ということは、ＭＷＳの活動がこれだけ長いあいだ続いているのは、十分評価に値しますね。

畑田　ＭＷＳは、世界的に見ても先進的な取り組みだと思います。

　ＭＷＳがここまで継続できたことで、学生時代にワークショップに参加したり、ＭＷＳＣｕｐで優秀な成績を収めた人が、各企業のセキュリティ担当として活躍し始めています。そういう意味で今後は、ＭＷＳの人材育成が具体的な成果として現れてくるだろうと期待しています。

産学の貴重な交流の場

齋藤　企業にとって、ＭＷＳに参加するメリットは、どこにあるのでしょうか？

寺田　技術者、研究者の〝横のつながり〟ができる点ではないでしょうか。以前なら、研究機関と産業界の接点はそれほど多くありませんでしたが、ＭＷＳをきっかけに交流の場、コミュニティが生まれました。

齋藤　ＩＩＪは産業界の立場で参加していますが、ＭＷＳでさまざまな発表を聞くと、「目から鱗が落ちる」ことがあります。そんなときは、何かインシデントが発生したら、協調して対応できるのではないかという可能性も感じられます。

寺田　複数の視点での解が提示されますから、対応の選択肢が広がる効果は確実にあると思います。

畑田　普段会社にいると、研究開発などの業務でなければ学術論文に接する機会はあまりないですし、反対に学術界は、市販の製品に使われているような技術やサービスプロバイダでの運用をきちんと押さえているわけではない。研究機関に長くいると、産業界では当たり前になっているような動きにも疎かったりしますし……。

齋藤　産業界は、研究成果を企業秘密として抱え込んでしまう場合もあり、実はその技術をシェアすれば大勢の人の役に立つのに……といったことにもなりかねない。

寺田　そうした両者が一緒に集まって、共通のデータを見ていく試みは、やはり貴重だと思いますね。

　学術機関には豊富な研究成果がありますから、それを産業界がいかに活用して社会に還元していくかという点は、今後のＭＷＳを通して、より望ましい方向性を探っていきたいですね。

齋藤　「この研究によって、このマルウェアをやっつけました」と言えることが重要ですから、そういった事例を積み重ねていける場に育って欲しいですね。

　さて、今年のＭＷＳはどういった内容になるのでしょうか？

畑田　昨年まではサイバークリーンセンターから主要な研究用データセットの提供を受けていましたが、サイバークリーンセンターのプロジェクトが終了したことで、今年からはＩＩＪさんを始めとする企業・研究機関・大学から、それぞれの観測データを提供していただいて研究用データセットとし、参加者に配布する方式に移行します。

寺田　研究用データセットの選定は、ＭＷＳの組織委員会が中心となって行ないます。

畑田　昨年のＭＷＳＣｕｐでは、ＩＩＪ

＊1999年に米カリフォルニア大学によって提供された、
侵入検知のためのデータマイニングに利用する研究用データセット。

写真／宮脇 進

チームが優勝しているので、そういうところが出してくれる観測データなら、そのデータを使ってみたいとか、ＩＩＪさんの話をもっと聞いてみたい、といった注目が多く寄せられるはずです。そうした交流を通して、分析技術のレベルがさらに向上していくといいですね。

マルウェアのない社会を目指して

齋藤　マルウェア対策というものは、マルウェアのない社会が実現されて、ＭＷＳのような集まりが必要なくなることが、究極の目標ですよね。（笑）

畑田　まさにその通りです。問題となっている特定のマルウェアを根絶するためにどうすればいいか、といった具体的なテーマを議論して実行に移す取り組みなどが、ＭＷＳを通じてできるといいですね。

寺田　現状、攻撃側は常に進化しているので、我々も研究をやめるわけにはいかないですから、これからもＭＷＳで培った技術を活かして、「こんなマルウェアが出てきたということは、攻撃者はこんなことを考えているのだろう」といった予測を観測データから読み取って、先手、先手で対策を打っていきたいですね。

齋藤　研究者も技術者も、マルウェアを根絶するというイメージを持ちながら仕事をしていただきたい。企業の担当者は、セキュリティベンダに対策を一任するだけではなく、自分の管理しているネットワークのセキュリティを向上させるうえでも、マルウェアに関する知識を吸収してもらいたいです。

畑田　対策に関する知識は、セキュリティベンダだけが知っていればいいというものではなく、そのサービスや製品を利用する側にも当然必要です。特に緊急時は、まず自分たちで何かしなければならない状況に出くわすので、そこできちんと対処できる人材は不可欠です。

　先ほども言いましたが、ＭＷＳで実践的な経験を積んだ〝卒業生〟と呼べるような人たちが、各企業において〝一人称〟で仕事をできるようになれば、彼らはマルウェア対策にあたって最低限何をすればいいか理解しているので、自社に合ったセキュリティ対策を推進できるようになるのではないでしょうか。

齋藤　とにかく我々は、マルウェア対策で実効力のある結果を出して、社会のみなさんから感謝してもらえるような方向に持っていきたい。そういうところでＭＷＳも貢献できるといいですね。

　本日はありがとうございました。■

標的型攻撃の現状

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
加藤雅彦

このところ多くの被害をもたらしている“標的型攻撃”であるが、本稿では、その実態と攻撃手法を見たうえで、具体的な対策の一例を紹介する。

二〇一一年九月に発生した、大手企業や官公庁への攻撃をきっかけに、「標的型攻撃」というキーワードがクローズアップされています。標的型攻撃という言葉は、複数の解釈がなされていますが、ここでは、「特定の企業や組織の内部にある秘密情報を窃取し、悪用することを目的として行なわれる攻撃」とします。

従来の対策では防御がむずかしいとされるこうした攻撃に対して、各社から新たな対策製品やサービスが続々と発表されていますが、標的型攻撃は、今までの攻撃と何が異なるのでしょうか？

標的型攻撃の実態

標的型攻撃の全体像や実体の把握は簡単なことではありません。実際の攻撃者が明らかになっていないばかりでなく、攻撃がかなり狭い範囲で行なわれている、関係者を装ったメールなどが使われるため攻撃に気付きにくい、HTTPなどよく利用される通信を使いセキュリティ対策をすり抜ける、といったことがその要因として挙げられます。攻撃行為そのものが発覚することが少ないために、攻撃者や攻撃の全体像がプロファイリングしづらくなっているのです。

しかし、今までに「標的型攻撃を受けた」と公表された内容から、標的型攻撃と従来型の攻撃の大きな違いは、攻撃の「目的」にあるのではないかと言われています。従来の攻撃も、いたずらであったり、何らかの主義主張を表す行為であったりと、目的は存在していました。しかし標的型攻撃には、特定組織の情報を窃取するというよりはっきりした目的があり、その達成のために手段を選ばない攻撃が行なわれていると考えられます。不正な侵入行為はあくまでも手段の一つでしかありません。まして、ウイルス感染させるといったことも行為者の本来の目的ではないと言えるでしょう。

このような状況を鑑み、総務省、経済産業省、警察庁、重要インフラの集うセプター・カウンシル、日本セキュリティオペレーション事業者協議会（ISOG-J）などで、標的型攻撃の実態把握に向けた取り組みが始まっています。IIJは、ISOG-Jの標的型攻撃対策検討WGに参加しています。WGに参加している各組織から情報を集約し、攻撃情報を分析することで、標的型攻撃の拡散状況や全体像の解明、攻撃検出や対策手法の検討などを進めています。

標的型攻撃の手法

標的型攻撃には、いくつかの段階があると考えられています。ここでは、その流れを簡単に解説します。

まず、標的に関する事前の情報収集が行なわれます。一般的な公開情報を始め、SNSなどの流行により、個人に関する情報がネット上で容易に入手可能になっています。さらなる情報入手のために、標的の関連組織が攻撃されることもあります。その後、入手した標的に関する情報をもとに、密かに組織内ネットワークへの侵入が企てられます。ここで用いられる侵入・攻撃手法は一つとは限りません。多くの場合、複数の攻撃手段を組み合わせて行なわれます。

例えば、送信元を詐称したウイルス付き電子メールが標的となった受信者に送られ、そのメールを開くことで端末がウイルスに感染します。さらにウイルスは感染端末から攻撃者に向けてバックドアを開き、境界防御内の端末を攻撃者から操作できるようにします。次の段階では、侵入に成功した端末を踏み台として組織内部の他の端末に侵入するなどして、攻撃者が必要とする組織内部の情報を窃取する、といった行為が行なわれます。このように標的型攻撃では、段階を踏んで連鎖的に攻撃が実行されるのが特徴と言えます。

標的型攻撃への対策

標的型攻撃を防ぐことはできないのでしょうか？「一〇〇パーセントのセキュリティ対策はない」とよく言われますが、完璧に防ぐことは困難だとしても、リスクを軽減することは可能です。

先に述べたように、標的型攻撃では複数の攻撃手段が使われますが、境界防御を突破する攻撃手法には既知の対策を適用できるものも数多くあります。OSだけでなく、アプリケーションも含めた迅速なセキュリティアップデートの実施や、不要なサービスやユーザを削除するといったサーバのハードニングなど、今まで行なってきたセキュリティ対策をしっかり継続していくことが重要となります。

標的型攻撃を早期に検出する、時間を遡って原因や影響範囲を調査しやすくする、といったことを行なうためには、通信記録を詳細化する、記録の保存期間を長くする、インシデント調査を迅速に行なえる体制を整える、といったことも有効でしょう。電子メールが攻撃手段として多用される点を考慮すれば、署名付きメールやドメイン認証といった手法の導入も効果があると考えられます。

さらに、対策へのアプローチとして、IPAから発行されている『「新しいタイプの攻撃」の対策に向けた設計・運用ガイド』などを参考にするのもよいでしょう。

このガイドでは、従来の対策を入口対策とする一方、出口対策として、侵入を許した場合でも重要な情報を流出させないためにはどうすればいいのか、といったことが提案されています。既存の環境でも比較的対策が行ないやすい、ファイアウォールのルールの見直しや、プロキシサーバの利用といった手法が述べられています。さらに、境界防御により攻撃を「入れない」ことで、システムを安全にするという従来型の設計方針の見直しや、出ていく通信を制御するには設計時にどのような出口対策を行なえばいいのか、といった点に関しても重点的な説明がなされています。

なお、本稿で紹介した対策はほんの一例であり、他にもさまざまな対策の試みがあります。また今後、さらに有効な対策が出てくることも期待されます。

日々の運用管理が重要

情報システムの安全性は、セキュリティ装置を導入すれば、その後は何もしなくても、安全であり続けるというものではありません。また、境界防御設備の導入で対策は終了するのではなく、少しでも早く攻撃の兆候に気付き、先手を打って対策を行なっていくことが重要です。

とりわけ、「境界内でシステムがどのような通信を行なっているか」「どのように構成が変更されているか」「システムリソースがどのような状態になっているか」など、日常における運用管理の必要性が従来以上に高まっていると言えるでしょう。要件定義からシステム設計、開発、構築、運用に至るまで、そのライフサイクル全てにおいて、安全性を考慮しながら実装することがいっそう重要になっているのです。(山)

DDoS攻撃――その実態と対策

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
根岸征史

近年増え続けるDDoS攻撃に対しては、最新のセキュリティ情報を入手しつつ、万が一の場合にも正確かつ迅速に対応できる体制作りが不可欠である。

インターネット上に公開されているサーバへのDDoS攻撃は日常的に発生しており、その数は年々増加する傾向にあります。IIJのDDoS攻撃対策サービスにおいても、二〇一二年一月から三月の三ヵ月間に、四〇四件のDDoS攻撃を観測しており、毎日数件の攻撃が休みなく発生しています。

ここでは、DDoS攻撃の主な攻撃手法と発生要因、対策方法を紹介します。

攻撃手法

DDoS攻撃には、さまざまな攻撃手法が存在しますが、「回線容量に対する攻撃」と「サーバに対する攻撃」に大別できます。

回線容量に対する攻撃は、サイズの大きなIPパケットを大量に攻撃対象に送信することで、接続回線の容量を圧迫する攻撃です。他方、サーバに対する攻撃は、TCP SYN Flood、TCP Connection Flood、HTTP GET Floodなど、攻撃対象サーバの処理能力やメモリを無駄に消費させ、正常なサービスを妨害する攻撃です。

近年では、回線容量への攻撃は少なくなり、サーバに対する攻撃が主流となっています。特に最近では、HTTPプロトコルを利用した攻撃が多く観測されるようになりました。

コンピュータの性能向上や高速ネットワーク回線の普及により、大量の攻撃トラフィックを発生させることが、誰でも比較的簡単にできるようになりました。専用の攻撃ツールの入手も容易で、特別な知識や技術がなくても攻撃を実行できます。また、ボットネットを利用することで、攻撃者はインターネット上の多数のコンピュータから一度に集中して攻撃することも可能です。そのため、観測されるDDoS攻撃の規模は年々大きくなっており、数百Mbpsから大きいものでは数Gbpsクラスの攻撃が発生することも珍しくありません。

また、単に大量のパケットを送付するだけでなく、WebサーバやWebアプリケーションの脆弱性などを利用した攻撃も増加しています。二〇〇九年にはSlowlorisや、一一年にはApache KillerやHashDosなど、この種の攻撃手法が相次いで見つかっており、脆弱性のあるサーバに対しては、効率的な攻撃が可能です。

特にApache Killerの場合、メモリを無駄に消費させてApacheのプロセス肥大化を誘発する脆弱性が狙われ、該当プロセスだけでなく、サーバ全体のメモリが枯渇してしまうので、その影響は甚大です。また、脆弱性公開時に攻撃ツールも同時に現れ、その時点では対策方法が明確になっていないうえに、全てのバージョンのApacheが対象となるなど、影響範囲が極めて大きかったと言えます。

攻撃の要因

DDoS攻撃が発生する要因には、政治的な主張にもとづくものや、金銭目的の脅迫をともなうものなどさまざまですが、二〇一〇年から一二年にかけて特に増加したのが、いわゆるHacktivismによるものです。

LulzSecやAnonymousに代表されるこれらの攻撃活動は、特定の企業、組織、政府機関に対して、何らかの主義主張をもとに行なわれています。多くの場合、これら組織の活動への不満や反対表明がきっかけとなり、DDoS攻撃によってその評判を落とすことが目的となっています。彼らはLOICやHOICなどの専用攻撃ツールを使い、賛同する人を募って攻撃を行ないます。賛同者を得られない場合は、小規模な攻撃で失敗に終わることもありますが、逆に大規模な攻撃に発展することもあります。

最近では二〇一二年一月末に、ファイル共有サイトMegauploadがFBIにより閉鎖されたことへの報復攻撃が発生しましたが、このときは数千人もの参加者がいたと言われています。攻撃対象も、米国政府機関、著作権保護団体、音楽関連企業など広範囲に渡りました。このように単一の組織だけでなく、関連する組織にまで攻撃が波及するのも彼らの攻撃活動の特徴の一つです。国際的に知名度の高い日本企業は攻撃対象になることが想定されるため、今後の動向に注意が必要です。

DDoS攻撃への対策

DDoS攻撃を受けると、インターネットへの接続回線の容量が圧迫されたり、サーバが過負荷状態になったりして、正常なサービス提供ができなくなります。そして、何も備えがない状態では、攻撃が止むまでじっと待つしかありません。では、DDoS攻撃に備えるには、どうすればいいのでしょうか？

対策としては、①攻撃に耐えてサービスを継続できるようにサーバの防御力を強化する、②攻撃が発生したことを検知して攻撃による影響を軽減する、という二つの方針が考えられます。もちろん、両方を実施したほうが望ましいことは言うまでもありません。

サーバの防御力強化には、回線容量やメモリなどのリソースに余裕を持たせることができればいいのですが、攻撃側のトラフィックが増大している現状では、攻撃に合わせてリソースを準備するのは得策とは言えません。ただ、クラウド環境の普及により、比較的短時間でサーバ台数を増やすなどスケールアウトさせることもできるので、攻撃を受けた場合には、速やかにこうした対応がとれるよう検討しておくべきでしょう。

また、主に災害復旧を目的としたバックアップサイトの構築や、CDNによるコンテンツの負荷分散なども、本来の目的だけでなくDDoS攻撃への対策としても有効です。さらに、サーバのOSやソフトウェアの機能を利用して同時接続数を制限したり、あらかじめ脆弱性を利用した攻撃を防ぐための対策をしておくなど、サーバ毎の対策も実施すべきです。

攻撃の検知については、サーバおよびネットワークの状態を監視して、異常を検知する仕組みの整備が必要です。ログの取得、分析を行なうシステムの構築や、DDoS攻撃対策専用のアプライアンスの導入、あるいはIIJなどの事業者が提供するDDoS攻撃対策専用のサービスも利用できます。

DDoS攻撃の場合、大量のトラフィックが発生することがあるため、比較的リソースに余裕のある、上流のネットワークで対策を実施するのが望ましいでしょう。その際、自組織だけで対応するのではなく、日頃からISPなどと連携して対応策を検討しておく必要もあります。

Hacktivismによる攻撃は、事前に予告されることもあるため、自組織に対する攻撃が発生する可能性について、インターネット上の情報をモニタリングするなど情報収集に努めることも求められます。もし、突然攻撃が発生した場合は、慌てずに対処できるように、緊急対応の体制を整備しておくことも重要です。攻撃の検知、被害状況の把握、攻撃の軽減対策、顧客対応、外部組織との連携、適切な情報開示など、緊急時に求められる要件はさまざまです。これらについて、あらかじめ十分な検討を行ない、攻撃に備える体制を築いておくことが不可欠なのです。

マルチポイントでのセキュリティ対策

IIJ マーケティング本部 プロダクトマーケティング部 プロダクトマーケティング2課 課長
久保田範夫

**標的型攻撃にはマルチポイントでのセキュリティ強化が必要である。
本稿では、標的型攻撃対策の考え方や、具体的なセキュリティ対策案を解説する。**

昨年から「標的型攻撃」が話題になっていますが、「これさえ対策すればいい」という解決策はあるのでしょうか？　この問いに答えるまえに、まずは代表的な標的型攻撃の事例を紹介します。

巧妙に成りすました偽装メールを使ってマルウェアに感染させ、感染後には感染端末に限らず内部ネットワークからさまざまな情報を収集し、外部に対してメール、ＦＴＰ、ＲＡＴといった手段を用いてその情報を持ち出す――これは標的型攻撃の一例に過ぎず、「特定ターゲットに標的を合わせた攻撃」という広義の解釈ができるものが標的型攻撃です。

ここでいったん「標的型攻撃」を「窃盗」に置き換えてみましょう。窃盗被害に遭わないためには、どんな対策が必要でしょうか？　ドアに鍵をかける、鍵を二重にする、警備員を雇う、大切なものは金庫に保管する、最新型の金庫に買い替える、現金は銀行に預ける、訪問者を玄関に入れない、家を留守にしない……等々、多くの対策が考えられ、個々の対策を併用すれば被害に遭わない確率を上げることもできます。しかし、対策方法が複数あるということは、一つの対策では窃盗被害を防ぐのはむずかしいということでもあります。また、対策を行なっても次々に新しい手口が出てきますので、これで完璧というものは存在しないことも理解しておく必要があります。

標的型攻撃への対策としては、メール対策やＷｅｂアクセス対策がクローズアップされていますが、対策はこれだけではありません。ファイアウォールの設定、不正侵入対策、外部または内部ネットワークにつながれた端末やサーバの脆弱性対策、内部端末から重要な情報が置かれているサーバへのアクセス管理など、対策可能なポイントや手法は多数存在します。

セキュリティ対策の実例

インターネットの境界にファイアウォールを設ける対策は、どこの組織でも導入されていますが、ポリシー設定が適切でないケースがしばしば見受けられます。特に内部から外部への通信に対するポリシーでｓｃｒ／ＡＮＹを多用しているケースが多く、まずここを見直す必要があります。かつて内部ネットワークは信頼できる対象として考えられていましたが、昨今では一度マルウェアに端末が感染すると、その感染端末からＬＡＮ側に接続された端末やサーバ、さらには外部に対しても攻撃が行なわれたり、収集された内部情報を外部に送信されるといった被害につながります。こうした〝万が一〟に備え、必要最小限の通信を許可するポリシーへの見直しが不可欠です。

また一般的なファイアウォールは、必要な通信プロトコル、ポートを必要なＩＰアドレスに対して許可あるいは拒否することを目的としており、ポリシーで許可された通信に対しては、ログをとるだけであることを再認識しなければなりません。

標的型攻撃の多くは、ファイアウォールで許可された通信である場合が多いのです。このため、不正な通信の有無を検知・遮断するための侵入検知・防御システム（ＩＰＳ／ＩＤＳ）の利用も検討すべきです。

ＩＰＳ／ＩＤＳでは、通信そのものを監視し、ファイアウォールで許可された通信であっても、攻撃行為や管理者が意図しない不正な通信が行われていないかを検知・防御できます。さらに、ＩＰＳ／ＩＤＳを外部からの通信だけでなく、内部から内部、内部から外部への通信にも適用することで、標的型攻撃などで感染した端末からの不正な通信を検知・防御するのに役立ちます。

次に標的型攻撃の入口対策としてクローズアップされているメールのセキュリティについて考えてみます。アンチウイルスと迷惑メールフィルタによる対策は浸透してきましたが、成りすまし対策に有効な「送信ドメイン認証技術」は、まだ普及し始めたばかりです。これは、受信するメールに対してＳＰＦ、ＤＫＩＭといった送信ドメイン認証を行ない、その結果をもとにメールをブロックして成りすましメールを防ぎます。

また、ウイルスメールでよく利用される「.pif」「.scr」といった添付ファイルの拡張子をあらかじめブロック対象に設定しておくことで、未知のウイルスへの防御力を高めることができます。

ユーザのＷｅｂアクセス対策も重要な対策の一つです。Ｗｅｂアクセス時のアンチウイルスはもちろんのこと、アクセス可能なサイトを業務に応じてフィルタリングするのも、感染リスクの低減に役立ちます。また、マルウェアに感染した端末から外部への危険な通信を専用のデータベースを参照してブロックできるサービスや製品が出ていますので、併せて導入すれば防御力を高めることができます。さらに、アンチウイルスやフィルタリングなどの対策を一元適用したり、アクセスログを一元的に管理するために、プロキシを必ず経由させ、端末から外部への直接接続をファイアウォールで禁止することも、マルウェア感染時に有効な出口対策となります。

こうした対策以外にも、端末への最新パッチの適用、メール対策やＷｅｂアクセス対策で利用するベンダとは異なるベンダのエンジンを搭載したアンチウイルス対策、振る舞い検知の導入、公開サーバ群および社内サーバの脆弱性対策、アクセス制御、ネットワーク分離、定期的なセキュリティスキャン、仮想デスクトップの利用など、取り得る対策は多岐に渡ります。また、機器の導入・設定・構成変更だけでなく、最新の情報収集、ユーザ教育といった側面的な対策も欠かせません。このようにマルチポイントでセキュリティ対策を強化し、標的型攻撃を含むセキュリティリスク全般への防御力を総合的に高めていくことが大切なのです。

マルチポイントでのセキュリティ対策を強化するにあたり、それぞれのログ解析、インシデント分析、相関関係分析などの運用も考える必要があります。セキュリティ対策では、機器の構築や導入に目が行きがちですが、導入後の運用が実は一番大切なのです。流行りの攻撃手法に応じて、適切なポリシーの見直しと運用を行なわないと、せっかく導入時に一時的に向上した防御力も徐々に低下してしまいます。日々の運用には専門的な知識と経験が必要で、進化する攻撃手法や対策の情報を収集するとともに、ポリシー・構成・設定などを適切に変更・対応させ、防御力を保ち続けなければなりません。

安心で安全なインターネットのために

ＩＩＪでは、セキュリティ対策の専門部隊がネットワークからアプリケーションレイヤまでの幅広いマネージドサービスを提供・運用しており、サービス間のインシデント共有やログの突き合わせなど、専門的な運用が行なわれています。また社内にはマルウェア解析部隊を持ち、最新のマルウェアの分析を行なったり、さまざまな脆弱性やインシデントに対する情報の収集・対応を行なうＩＩＪ-ＳＥＣＴ（IIJ group Security Coordination Team）が、ＩＩＪのセキュリティを支えています。

ＩＩＪは、グループ内やマネージドサービスだけでなく、広く一般に向けてセキュリティ情報を発信し、安心で安全なインターネットの実現を目指しています。

セキュリティ2012 キーワード集

IIJ マーケティング本部 プロダクトマーケティング部　プロダクトマーケティング2課
大野慎吾

1 TCP SYN Flood攻撃

インターネットにおけるDoS攻撃（Denial of Service attack＝サービス不能攻撃）の一つ。TCP接続における3ウェイ・ハンドシェイクの仕組みを利用した攻撃手法です。TCPのコネクション開始要求にあたるSYNパケットだけを大量に送り、ACKパケットを送信しないことで、接続応答待ち状態を発生させます。この行為を短時間に繰り返し行なうことで、サーバのメモリ領域を飽和させ、対象となるWebサイトを一時的に利用不能に陥れます。

2 Connection Flood攻撃

インターネットにおけるDoS攻撃の一つ。長時間オープン状態を続ける大量のTCPコネクションを確立させることにより、ソケットを占拠する攻撃手法です。コネクション数の上限を設けていない場合には、サーバリソースを食いつぶされ、システムがクラッシュする可能性があります。

3 HTTP GET Flood攻撃

インターネットにおけるDoS攻撃の一つ。HTTPプロトコルのGETメソッドを悪用した攻撃手法です。TCPセッションのみを大量に確立させるだけでなく、セッション確立後に大量のHTTP GET要求を送信し、サーバに対して高負荷をかけることでサーバを一時的に利用不能に陥れます。この攻撃は特別な攻撃ツールを必要とせず、ブラウザのリロードボタン（F5キー）を繰り返し押すことで簡単に実行できるのが特徴です。また、ボットネットにこの攻撃手法が実装されることも多く、大きな脅威になっています。

4 Slowloris

Webサーバの脆弱性を利用したDoS攻撃ツール。Webサーバに不完全なリクエストを送ると、プロセスが待機状態になることを悪用します。Webサーバが最後のヘッダが送られてくるのを待つあいだ、偽のヘッダを送ることで接続をオープンにし続け、Webサーバのプロセスを上限まで一杯にさせます。Apacheなどの複数のWebサーバの実装が影響を受けます。

5 Apache Killer

Apacheの脆弱性を利用したDoS攻撃ツール。Rangeヘッダに多くのパラメータを指定した多数のリクエストをApacheに送ることで、ターゲットとなるシステムのCPUとメモリ使用量を増大させ、過負荷状態を発生させます。

6 HashDos攻撃

PHPやRubyなど、幅広く用いられているWebアプリケーション開発プラットフォームに対し、CPUリソースを枯渇させるDoS攻撃手法です。HTTPリクエストのパラメータ名に対するハッシュ値を故意に同じ値（ハッシュ衝突）にしたものを短時間に多数送信することにより、Webサーバを過負荷な状態にします。

7 Hacktivism

「ハクティビズム」とは、高い情報技術の知識を活用し物事を改良するという意味の「hacking」と、政治的な目的を達成するという意味の「activism」を合わせた造語です。ハクティビズムを行なう代表的な集団としては、LulzSecやAnonymousが挙げられ、社会的・政治的な主張のもと、自分たちが敵と見なしている企業や政府機関のWebサイトを攻撃してダウンさせたり、Webページを改ざんして自分たちの声明を掲載するといった行為を行ないます。

8 Anonymous、LulzSec

「アノニマス」「ラルズセック」は、インターネット上の匿名掲示板のようなオンラインコミュニティの利用者を中心に構成されています。抗議行動、DDoS攻撃、SQLインジェクションを利用したクラッキングといった行為を行なう集団です。

9 LOIC / HOIC

LOIC（Low Orbit Ion Cannon）、HOIC（High Orbt Ion Cannon）は、オープンソースのネットワーク負荷テストツール。ターゲットとするサーバにTCPパケットまたはUDPパケットを大量に送るDoS攻撃を行なうことで、サーバをダウンさせることができます。

10 CDN

CDN（Contents Delivery Network）の略で、ファイルサイズの大きなデジタルコンテンツをインターネット経由で配信するために最適化されたネットワークを指します。大量アクセスによるWebサイトの表示速度低下、サーバダウンなどを防ぐことができます。

11 送信ドメイン認証

送信ドメイン認証とは、そのメールが正当なメールサーバから送信されたメールか否か（差出人のメールアドレスが詐称されていないか）を識別する技術です。受信するメールに対して、送信元メールアドレスのドメイン名の管理者が宣言している内容にもとづき、送信に使用されたメールサーバの正当性をチェックします。ドメイン名をチェックした結果は、「スコア」としてメールヘッダに記述されます。なお、送信ドメイン認証には、SPF（Sender Policy Framework）やDKIM（DomainKeys Identified Mail）といった手法があります。

12 IIJ-SECT

IIJ-SECT（IIJ group Security Coordination Team）は、インターネット上のインシデント、特にIIJの設備や顧客が巻き込まれた事件に対応するために、2001年に結成されました。IIJの設備で発生した事件の発見、解析、関連各組織との連携を主なミッションとしています。このTeamはセキュリティ情報統括室を中心として、IIJ内部の設備運用からインテグレーションまで複数の組織のメンバーによって構成されています。

ネットワークの仮想化がもたらすもの

**“ネットワークの仮想化”が話題になっているが、
いったいどこがそれほど凄いのだろうか?
今回は一歩踏み込んで、この新しい技術の全貌を描いてみたい。**

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

イラスト／山本加奈子

前回、ネットワークの仮想化がこれからのクラウドの発展に不可欠な技術となる、と書きました。今回も引き続きこのテーマで〝妄想〟を膨らませてみたいと思います。

今はまだ、ネットワーク仮想化の何が凄いのか、よく分からないとおっしゃる方が多いと思います。ネットワークが仮想化された状況を実際に体験した人はほとんどいませんし、仮に使ってみたとしても、非常に限定的な使い方やデモ環境での評価利用程度でしょうから、無理もないことです。

たしかにネットワークを仮想化して、ソフトウェアで全てを制御できるようにするのは、技術として面白いのは分かりますが、それで今までできなかった何か新しいことができるようになるわけでもないので、「いったい何の役に立つの?」と思うのが普通でしょう。そもそも「お金が儲かる話なの?」と思っている人も多いのではないでしょうか。

それでも、東京と大阪で論理的なネットワーク構成を変えることなく、仮想マシンをマイグレーションして動かし続けられれば、災害時でも情報システムを動かし続けることができますし、前回も書いたように、物理的なネットワークの制約を越えて、同一VLANを複数拠点に伸ばしていくことも可能です。とはいえ、そういうニーズがあるなら、最初から物理的なネットワークシステムをそのように設計して組み上げておけば、決してできないことではないはずです。冷静に考えて、ネットワーク仮想化の何がそんなに凄いのでしょうか?

情報システム自体がコンテンツになる

前回お話ししたように、ネットワーク仮想化とは、情報システムの仮想化を実現するための最後のミッシングピースを作る、ということです。そして、これが実現すれば、情報システム自体がコンテンツになります。では、情報システムがコンテンツになるとは、どういうことでしょうか?

情報システムとは単純に言うと、複数のコンピュータやストレージのような周辺機器を、あるトポロジのもとネットワークで相互に接続して構成したものです。それらのコンピュータ上では、特定のタスクを実行するアプリケーションソフトウェアが動いていて、互いに協調しながら一連の情報処理を行なっています。しかし現状では、その情報システム自体を情報として扱うことはできません。すなわち、システムを構成するコンピュータやクライアントのコンピュータ、もしくはその情報システムを監視しているコンピュータからでさえも、情報システムの全体像を一連の情報として把握することができていないのです。

情報システムを構成するいずれかのマシンで動いているアプリケーションは、担当している業務ロジック、扱うデータの形式や値などを把握しているはずですが、例えば、その前段にあるサブシステムがどういう構成になっていて、どのようなネットワークトポロジで接続されているのか、といったシステムの他の部分も含めた全体像に関する情報は持っていません。そういう情報は、そもそもシステム上には存在しないか、あったにせよプログラムから直接アクセスしやすい形式になっていないかで、仮にきちんとモデル化され整理されていたとしても、あちらこちらに分散していて、ひとまとまりの情報として扱える状態になっていないケースがほとんどではないでしょうか。

仮想化を制御するコントローラ

ネットワーク仮想化は、この状況を一変させる可能性を持っています。仮想化を制御する「コントローラ」と呼ばれるソフトウェアでは、ユーザのシステムの論理ネットワークを構成するために、そのユーザに割り当てられている仮想マシン群をつなぐ論理ネットワーク構成に関わる情報を全て把握している必要があります。

しかも、それは単なる論理的な構成情報のみではなく、その仮想マシンが稼働している物理マシンの位置や稼働状況、また、物理マシン同士をつないでいる物理的なネットワークのトポロジ、回線の帯域や利用率など、物理と論理の両方の世界に関わるさまざまな情報を集約管理することになります。つまり、コントローラがユーザのシステムとその環境条件を全て情報として把握しており、それらの情報を用いて、たくさんの仮想情報システムを、一つの物理インフラ上に展開し、管理できるようになっていなければならないはずです。

ネットワーク仮想化のコントローラは、システム全体の構成情報をもとに、ある戦略にもとづいて動的に仮想情報システムを物理インフラ上に展開し、管理するのです。複雑で巨大な情報システムであっても、こんなふうにソフトウェアだけで操作できるようになる、つまり、一つのコンテンツになるということを意味しているのです。そして、これが実現されたら、クラウドを構成するインフラとそのうえで動作する情報システムとを水平分離できるようになるでしょう。

すると、物理インフラの構成が、そのうえに展開される仮想情報システムの構成に依存しなくなるわけですから、ハードウェア構成を標準化することが可能になります。インフラの増設は、そのうえで動いている個別の情報システムの状況とは独立して行なえるようになり、展開されたインフラのどの部分を、どの仮想システムでどのように利用するかは、全てコントローラが全体の状況を見ながら最適化するようになります。

さらに、ハードウェアの生産ラインもソフトウェアで制御し、できあがった機器の物流から設置までのプロセスを標準化し、可能な限り自動化してしまえば、インフラ展開にかかるコストを桁違いに下げることも可能になるでしょう。ほぼ全てをソフトウェアで管理し、勝手に増殖し成長するクラウドインフラができるなんて言うと、まるでSFのようですが、グーグルがネットワーク仮想化に力を注ぐ理由は、この辺にあるように思います。

また、こうした自己組織化インフラ上で動作する仮想情報システムが、仮想化コントローラから自分自身の現在の状況のフィードバックをもらって、コントローラに指示を出すことで、自分自身のインフラ上への展開方法を制御するようなことも可能になるかもしれません。こうなると、自己言及による何らかのパラドックスに陥って抜けられなくなってしまうかもしれませんが……。

妄想がどんどん膨らむのでこの辺でやめますが、ネットワーク仮想化とは、このように楽しくも恐ろしげな技術です。ひょっとすると、ネットワーク仮想化は、破壊的イノベーションにつながる革命的な技術かもしれません。今は何の役に立つのか分からないかもしれませんが、しばらくはその動向から目が離せない技術だと思います。

世界各国で利用可能な基幹業務支援のクラウドサービス「G-BASS〝ERP〞」

IIJグローバルソリューションズ サービス戦略室 担当部長
竹島三千代

IIJグローバルソリューションズでは、グローバルビジネスを支える「ビジネスアプリケーション・サービススイート」の第1弾として、低価格で高機能のERP(Enterprise Resource Planning) をクラウド型で提供開始する。

IIJグローバルソリューションズは、基幹業務に必要なさまざまなソフトウェアをクラウド型で提供する「ビジネスアプリケーション・サービススイート」を新たに展開し、業務アプリケーション分野でのサービスを拡大します。その第1弾として、世界各国で利用可能な基幹業務支援のクラウドサービス「G-BASS[*1] “ERP”[*2]」を、2012年6月より提供します。

多くの企業が海外でのビジネスを積極的に推進するなか、現地法人や関連会社の基幹業務のシステム化が大きな課題となっています。言語・通貨・商習慣・法制度・ICTインフラストラクチャーなどの違いから、日本国内で使用している業務システムがそのまま海外では展開できず、現地の業務プロセスの最適化・効率化や本社とのシステム連携の遅れにより、期待していたビジネス展開ができていない企業も少なくないでしょう。また、グローバル対応のためのシステム構築は、従来のようなSIでは長い時間と大きなコストを必要とするため、スピードが要求される今日のグローバルビジネスには不向きとも言えます。

このような課題を解決し、企業の海外事業展開を促進できるように、IIJグローバルではクラウドサービスとして「G-BASS “ERP”」を発表しました。

G-BASS “ERP”は、IIJのクラウドサービス「IIJ GIO」の基盤上に、20年以上にわたりERPシステムの構築を手がけてきたローリーコンサルティングのグローバル対応ERPパッケージ「ReCent」を展開し、会計・受発注・在庫・固定資産管理などの機能を、モジュール毎に提供するアプリケーションサービスです。

ReCentは、すでに多数の導入実績があり、従来のSIモデルによるシステム構築との比較では「短期間かつ安価」に、また従来のパッケージソフトウェアと比べると「お客さまの業務に柔軟に適合できる本格的ERPシステム」を導入できます。

本サービスをご利用いただくことで、海外現地法人や関連企業の業務プロセスの最適化、グループ連結会計の迅速化、TCO削減などが実現され、グローバルビジネスを加速できます。

G-BASS〝ERP〞の特徴

1　IIJ GIOを基盤とした高信頼・高品質なサービス

G-BASS “ERP”は、IIJがグローバルに展開するクラウドサービスIIJ GIOを基盤とした基幹業務支援サービスです。IIJ GIOは、2009年のサービス開始以来、大手企業を中心にすでに600社以上のお客さまにご利用いただいており、多くの実績に裏付けられた高い信頼性を誇るシステム基盤と高品質の運用サービスにより、重要な基幹業務のアプリケーションサービスを安心してご利用いいただけます。

2　グローバル対応の高機能ERPソフトウェア

ReCentは、世界中で1000社以上が導入しているオープンソースERPソフトウェアをもとに開発された、会計・受発注・在庫・固定資産管理を全てカバーするERPパッケージです。多言語（日本語、英語、中国語など）、多通貨に対応しており、容易に各国の会計基準に合わせることができるため、海外拠点でもすぐにご利用いただけます。また、本社で導入されているERPシステムとの連携も容易なため、グローバルビジネスの可視化、迅速な事業戦略の立案・実施、適正な内部統制などが可能になります。

「G-BASS “ERP”」のサービス概要

参考価格

料金区分		サービス範囲	月額料金	単位	備考
基本料金		ERP全体（全モジュール）	¥280,000	一式	5ID分を含む
		会計	¥240,000	一式	2モジュール以上の場合は全モジュール利用時と同額。
		受発注・在庫管理	¥240,000	一式	
		固定資産	¥220,000	一式	
1IDあたりの追加料金	ID数 6～20	ERP全体（全モジュール）	¥15,000	ID	
		会計	¥7,500	ID	
		受発注・在庫管理	¥7,500	ID	
		固定資産	¥4,500	ID	
	ID数 21～50	ERP全体（全モジュール）	¥10,000	ID	
		会計	¥5,000	ID	
		受発注・在庫管理	¥5,000	ID	
		固定資産	¥3,500	ID	

（注）上記には初期導入費用、追加開発費用は含まれません。

3　短期間でサービス開始できるクラウドモデル

SIモデルでの導入と比較し、アプリケーション、ミドルウェア、ハードウェアなどの各種ベンダとの調整や管理が不要なため、短期間でのサービスリリースが可能です。またReCentは、20年以上のERPシステム構築経験をもとに、必要十分な機能に最適化されているため、最低限の帳票や画面のカスタマイズだけですぐにご利用いただけます。標準的な会計モジュールの場合、要件確定後 1、2ヵ月でサービス開始が可能です。

4　柔軟で確実なアプリケーションサービス

ERPに関して経験豊富なローリーコンサルティングのコンサルタントとグローバルプロジェクトのノウハウを持つIIJグローバルのエンジニアが、お客さまのビジネスプロセスとシステムの最適化を実現し、円滑なサービス導入を支援します。従来のパッケージソフトウェアでは困難であったカスタマイズやアドオン（追加開発）にも柔軟に対応できるため、ビジネスプロセスに合わせた最適なアプリケーションサービスをご利用いただけます。

5　初期投資を抑えた安価なクラウドサービス

多くのお客さまの要件を満たすことができるよう最適化されたソフトウェア、システム基盤、運用サービスをセットにしたクラウドサービスを提供することで、従来のERPシステム構築のような大きな初期投資を必要としません（詳細は上記の参考価格参照）。また、ユーザ数に応じた月額の従量課金体系のため、お客さまの事業拡大に合わせた段階的な拡張が可能です。

IIJグローバルでは、企業の海外事業展開を支援するために、従来からグローバルネットワークを中心としたIT基盤サービスを提供してきました。このたび、新たに開始するERPのクラウドサービスにより、IT基盤からビジネスアプリケーションまで一貫したサービス提供が可能となり、お客さまのグローバルビジネスをいっそう加速できるようになります。

今後は、営業支援ツール（SFA）など、ビジネスアプリケーション・サービススイートとしてサービスを拡充してまいります。

*1 G-BASS（ジーバス）：Global Business Application Service Suite。
*2 ERP：Enterprise Resource Planning（企業資源計画）。部門毎ではなく、企業全体の経営資源を統合的に管理する手法・概念。

日々のサービス運用の現場から

技術的出発点の違い

IIJ サービスオペレーション本部長
山井美和

IIJは創業20周年を迎えています。筆者は30年前すでに社会人でしたが、技術の進歩は当時と比べると、すさまじい勢いで進んでいることを実感します。

無線関係の仕事に従事していた頃、海と陸を結ぶ無線電話機は肩からぶら下げて、重たいハンドセットを使うのが当たり前でしたが、今では手のひらに乗る携帯電話です。しかも、Bluetoothヘッドセットを耳に差し込み、本体はポケットのなかにあって、両手を使って作業もできます。

日本でインターネットが本格的に商用利用され始めた1990年代、通信がうまくいかないときは、プロトコルアナライザで通信内容をダンプしたり、ヘッダを解析したりしたものです。コアダンプを解析するにしても、プリントアウトした紙を定規と蛍光ペンでマーキングしながらやっていました。

ラジオと言えば組み立てることもできましたが、今やデジタル化されサイマル放送されているので、インターネットさえあれば（もちろんPCなどは必要ですが）、ラジオを買う必要もない時代になっています。

そんな環境下で、どのようにして運用の技術を継承すべきか。自分たちが数十年に渡って経験してきたことを教えるために昔にさかのぼることは可能ですが、その理解を前提に始めたのでは、これからの技術革新には追いつけないと思うのです。

筆者が若かった頃の上司は、細かいことまで教えてくれないこともあり、逆に細かい質問をして怒られた経験もありますが、そのとき上司には、そういうもどかしさがあったんだなと、最近理解できるようになりました。

「技術知識の出発点が違う」のです。技術は進歩していくものなので、新しい技術には新しい使い方や運用方法を考えていかなければなりません。しかし、サービス提供は継続性が重要で、今まで考えもしなかった事象が障害となり、お客さまにご迷惑をおかけすることになってもいけません。

この20年のあいだに蓄積してきた運用技術は、時代に合わせて適用方法を変えながら継承していかなければなりません。古いやり方をそのまま新しいものに適用すれば無理が生じるでしょうが、その伝承方法には共通するものがあると思っています。

「温故知新」――新しい技術だけを追求するのではなく、先人たちの思想や考え方の基本は、使う技術が進歩しても変わらないものなので、その思想をもとに新しい技術に適用していくことが大切だと思うのです。すなわち、新しい技術と古い運用経験のベストミックスをどのようにして作り上げるかということです。

日々の業務のなかで、ミスや障害には厳しいことも言わなければなりませんし、技術論では本筋を忘れたシステムやテクノロジーの話にすり替わってしまうことも多々あるので、そういうときは「技術的出発点が違う」ということを意識しながら話すように心がけています。

当然のことながら、お客さまからはレスポンスの早さも求められています。安定したサービス提供と早いレスポンスを両立するためには、技術的出発点の違いを意識しながら、相互理解を深めていく必要があります。その過程でお客さまにご迷惑をおかけすることがないとは言い切れませんが、将来の品質を向上させることで、それ以上のメリットを還元できると確信して、運用現場のメンバーは日々努力を続けています。IIJ

イラスト／山本加奈子

●インターネット・トリビア

動画配信の裏側

IIJ プロダクト本部 アプリケーション開発部 戦略的開発室
堂前清隆

インターネットで動画が見られるサービスが大流行しています。従来のようにパソコンの画面で見るだけでなく、インターネットに対応した家庭用のテレビで動画を見るサービスも一般的になってきました。

視聴できる番組はさまざまですが、なかには地上波テレビの番組と同じクオリティで制作されているものもあり、見た目ではテレビ放送と全く区別がつかないようになってきました。

しかし、地上波テレビに代表される「放送」とインターネットによる「配信」は、見た目は同じでもその方式が大きく異なります。放送では、各放送局から送り出される番組はあくまで一種類で、全ての視聴者が同じ番組を見ています。そして、視聴者が一人であっても一万人であっても、番組を送り出す側の負担は基本的に同じです。また、チャンネルを変えればもちろん別の番組を見ることができますが、設定できるチャンネル数はそれほど多くありません。

一方、インターネット配信は、配信サーバから視聴者一人一人に個別に番組が送信されます。たくさんの視聴者が同じ番組を見ている場合でも、配信サーバが全ての視聴者に同じ番組を送っているのです。よって、放送と違って、視聴者が増えれば増えた分だけ、番組を送り出す側の負担が大きくなります。ですから、非常に多くの視聴者が見込まれる番組は、インターネットサービスプロバイダなどが運営しているCDN（コンテンツデリバリネットワーク）と呼ばれる専用の設備に配信を依頼するのが一般的です。

さて、このように一見非効率なインターネット配信ですが、配信サーバから視聴者に個別に番組が送られるということは、裏を返せば、それぞれの視聴者に異なる番組を配信できるということでもあります。

放送では、チャンネル数に制限があるため視聴者が少ない番組を放送することは困難ですが、インターネットなら極端な話、視聴者が数人の番組であっても配信できるのです。実際、このような特徴を生かして、多数の番組を配信しているインターネットならではの配信サービスもあります。IIJ

※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/iijnews110

Information

IIJ技術研究所のランディ・ブッシュがインターネットの殿堂入り

IIJ技術研究所の特別研究員ランディ・ブッシュ（Randy Bush）が、Internet Society（ISOC）の「The Internet Hall of Fame（インターネットの殿堂）」入りを果たしました。
The Internet Hall of Fameは、ISOCがインターネットの発展に多大な貢献をした人物を称える初めての賞で、4月23日にスイスのジュネーブで開催された ISOCのカンファレンスで発表されました。本賞は、「Pioneers Circle」「Innovators」「Global Connectors」の3つのカテゴリ別に世界で33名が受賞し、ランディ・ブッシュは、世界的なインターネット利用の発展に貢献した人々に贈られる「Global Connectors」に選ばれました。

詳細はこちら http://www.iij.ad.jp/news/pressrelease/2012/0502.html

LTE対応 IIJmio高速モバイル/Dサービス『LTE高速モバイル通信をはじめよう!』キャンペーン

IIJの個人向けサービス「IIJmio」では、LTEに対応したデータ通信サービス「IIJmio高速モバイル/Dサービス」を提供しています。
「IIJmio高速モバイル/Dサービス」は、NTTドコモのLTE網を使用したデータ通信用のSIMカードを提供するサービスで、月額945円からはじめられる「ミニマムスタート128プラン」または、複数のSIMカードでデータをシェアできる「ファミリーシェア1GBプラン」から、プランを選択できます。
あわせて、同サービスで利用できる、LTE対応のモバイルWi-Fiルータ「LTEモバイルルータ（NI-760S）」を販売しています。
今なら、「ファミリーシェア1GBプラン」の契約と「LTEモバイルルータ」の購入で5,000円がキャッシュバックされる『 LTE高速モバイル通信をはじめよう！』キャンペーンを実施中です。

詳細はこちら https://www.iijmio.jp/campaign/lte/

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
表紙イラスト／すげさわ かよ
デザイン／B.C.
印刷／株式会社興陽社

◎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
20th Anniversary

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3-3 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

北陸支店　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神保町 1-105 神保町三井ビルディング
〒101-0051　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）
東京都中央区新富 2-4-4 アクアビル
〒104-0041　TEL：03-6280-4981

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

IIJ-MKTG001AA-1206BK-09800PR