IIJ. news

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

October 2014
VOL. 124

特集

事業継続を支えるITサービス

IIJ. news
October 2014
VOL. 124

表紙の言葉　末房志野

銀杏は約2億5千万年前から地球に存在し、生きた化石とも呼ばれています。先日、PCの調子が悪く、保存していたデータがあっけなく消えてしまいました。データも大切に保存しなければ、なくなるのだということを実感しました。銀杏のように2億年も生き続けられるデータの保存の仕方があったら…。銀杏並木を歩きながら、自然の生命力の強さに改めて魅了されました。

卓球台

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

「卓球台が出てきましたが、どうしましょう」

引っ越しの折、倉庫の奥からバラバラにして立て掛けられていた卓球台が出てきて、その存在を知った社員は、「なぜ、卓球台があるのか」と、誰もが訝しく思ったらしい。不要物はすぐに廃棄して、無駄なスペースを切り詰めていたIIJの倉庫の片隅で、長いあいだ利用もされず、眠り続けていた卓球台に、社員が訝しい目を向けたのは当然である。

「卓球でもしますか」

月末、給与を払う時期が来ると、元卓球部だったという経理担当者といつも逃げ込んだ場所が、卓球台が置かれた空き部屋だった。一年半後には解体される予定だったビルの一画を、破格の賃料で借りて始まったのがIIJで、一九九二年のことである。解体のスケジュールにあわせ、日を経るにしたがい、入居していた企業が次々と移転し、最後まで居残ったのはIIJだけといった頃である。

一階のショウルームだったスペースがIIJのオフィスで、地下鉄の国会議事堂前駅に近い角地ということもあって、人通りが途切れることのない舗道に面していた。ブラインドを買うお金もなく、西日を避けるために、パソコンやサーバのうえには、日除け代わりの黒い雨傘が不気味な花を咲かせていて、そんなオフィスに視線を走らせては、「この会社、まだ夜逃げをしてないのね」と、OLの言葉が聞こえてきたりした。社員の服装も、一年中、洗い古したTシャツとジーンズ、貧しさを絵に描いたような光景だった。

「鈴木さん、どこでも空き部屋があるから、使っていいですよ。なんか気晴らしができるような空間をつくりましょうか」

ある時、見るに見かねたビルの所有者が、そんな言葉をかけてくれた。

「卓球ができる空間があるといいな。どうしようもない時は、体を動かすほか、逃げる道はないですよ」

翌日の夕方、「できましたよ」と、結構、広い空き部屋に卓球台が設置されて、社員には内緒にした私の卓球場が仕上がっていた。以来、月末ばかりか、なにかと卓球場に逃げ込んでは、汗を流すのが日課のようになってしまったのである。給与を払う資金の当てもない月末など、筋肉痛になるほど卓球に打ち込むようになった。そんな時期が一年半ほど続いた記憶がある。

資金繰り、役所との不毛な長い折衝……不安になっていた社員に、見通しもつかないまま、「なんとかなるはず」という言葉を語り続けるしかなかった日々を救ってくれたのは、長いこと眠っていたこの卓球台であり、憂さ晴らしに付き合ってくれた元卓球部だったという経理の社員である。毎月、茶封筒にささやかな給与を入れて、「今月はこれだけ」と、社員に渡す役まわりはストレスばかりが増すわけで、運動で発散する以外に、やり場がなかったのだろう。

「廃棄していいですか」

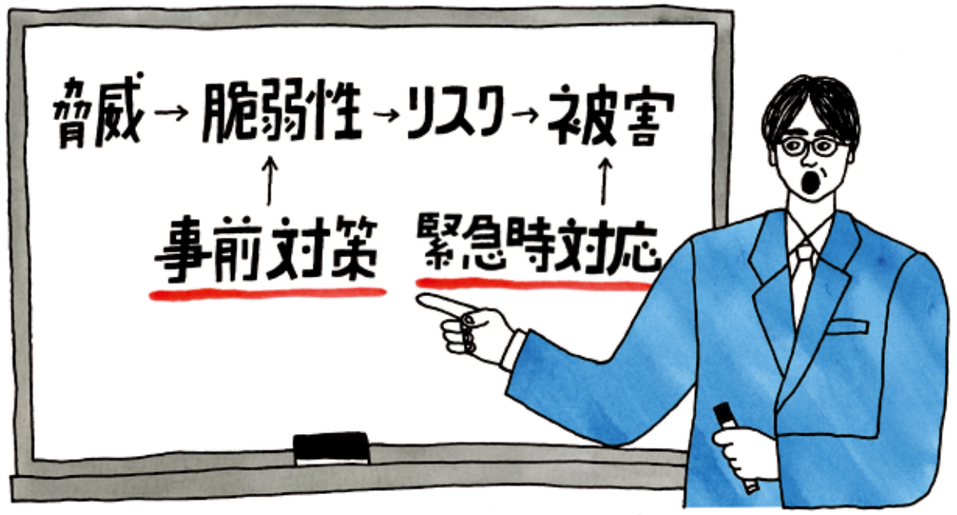
新しいオフィスには、まったく馴染まない卓球台である。今後、利用することもない不用なモノとわかっていながら、「ま、いままで生き延びてきたのだから、倉庫に入れておいてよ」と、なにげなく答える。私にとっては、忘れることができない卓球台なのだが、いずれ、立ち上げの時期のIIJを知る社員がいなくなるように、卓球台も消えていくに違いない。過去は振り返ると、社史の編纂すら拒んでいる私だが、この卓球台は忘れられない思い出の遺物である。いつか、若い社員が使ってくれると、本当に嬉しいのだが。●

イラスト／末房志野

Topics

事業継続を支える ITサービス

東日本大震災を機に“事業継続”を再考する動きが広まったが、
思うように進捗していないケースも多いのではないだろうか？
本特集では、ITサービスの面から事業継続のあり方を整理・提案してみたい。



特集イラスト／STOMACHACHE.

企業活動を継続する際のリスクに対し、インターネットとITは何をすべきか？

IIJ 執行役員
サービスオペレーション本部長
山井 美和

地震や水害などの自然災害からセキュリティ事故などの人的災害まで、IT環境に障害をもたらし、企業の事業継続を妨げるような事象は日々発生しています。IT環境は、企業の事業継続に必要不可欠な道具であり、その整備にとどまらず、日々の運用・管理や統制、そして監査といった幅広い活動に支えられています。

IT環境を様々な事象から守り、事業を継続していくことは、事象が複雑になればなるほど、企業のIT担当者を悩ませていることと思います。一方、我々のようなITサービスを提供する側は、様々な事象から設備やお客さまを守り、サービスを安定的に維持・継続することが、お客さまの事業継続にとって必須であるとの認識を持って、日々の業務にあたっています。

今回の特集では、お客さまが「どのような点を意識してITサービスを選択すべきか」「どのような組み合わせが最適か」「何を重点的に対応すべきか」といったことを考える際のヒントになるよう、実際の事例や普段、我々が注意している事項のなかから、リスクに備えるという視点に即した内容や最新トレンドをまとめてみました。

最初に、企業の事業継続の考え方から計画の策定までを簡単に説明します。流れとしては、事業継続の基本方針を定め、それをもとに事業継続マネージメントシステムを構築し、事業継続計画書を策定して実行することになります。

事業継続の考え方

緊急時に事業継続に最低限必要なリソースを確保できるよう、想定され得るリスクに対して必要な処置を講じるために、被害想定とリスク評価から、脆弱性への事前対策の実施と被害発生時の緊急時対応までを定めておくことが事業継続を考える柱になります（右頁イラスト参照）。

被害を想定し脆弱性の存在を認知したうえで、事前に必要なリソースを割り当て、対応計画として策定していきます。

ネットワークやシステムの設計時点から二重化・冗長化を図り、それに適応可能なサービスを選択します。そして、自社の事業のコアコンピタンスを意識しつつ、「事業継続に必須なリソースは何なのか？」という点から脆弱性と被害想定を常に見直すようにして、事業継続計画を最新の状態に維持（変更）する――これが事業継続計画の基本になります。

リスクの分類

リスクを考えるとき、その分類方法を検討する必要があります。一例として、

被害パターン	被害対象	想定される脅威
物的被害	業務実施場所	天災、事件、事故
	通信サービス設備	損壊、障害
	利用している他社サービス	障害
	ライフライン	テロ、事故
人的被害	社員	病気
	業務委託	経営不安
	社会環境	政変、テロ

IIJにとっての事業継続は、弊社が提供するサービスを考えると、お客さまの事業継続に必要なサービスの運用、お客さまからアウトソースされたシステムを請け負うえでの運用、弊社の経営や管理機能の維持、弊社のサービス提供と業務遂行を支える重要な社内インフラ、以上の四つを事業継続活動の範囲として捉えています。

これらについて想定事象毎に自社の脆弱性を認知し、想定されるリスクへの対応を事前に検討して定めていきます。ただ、リスクに対する考え方は、それぞれの企業の特性に応じて定義されなければならないので、自社の事業活動に与えるリスクを最初に分類する必要があります。その方法論はいくつかあると思いますが、ここでは、上表のような被害パターンの分類を用いて、リスクを想定します。

これは一例に過ぎず、事故・不祥事・訴訟などによる企業の信用に関わる被害といったものも想定されますが、本特集では、ネットワークやシステムを扱うIT部門を対象としているので、事業継続のための物的被害と人的被害に分類したリスクにフォーカスして考えます。

想定される脅威が現実のものとなり、それによって脆弱な部分に物的被害が発生した場合のリスクを挙げますと――

①サービス機能を維持できなくなる。
②回復までに時間を要する（日単位、週単位）。
③サービスを代替できる機能がない。
④業務に就く人員の移動が困難になる。

次に、人的被害が発生した場合のリスクとしては――

①人員が不足して業務が実施できなくなる。
②外部に委託している業務が実施できなくなる。

ここで例示したリスクはほんの一部であり、挙げていけばまだまだ出てくると思いますが、次の段階の作業としては、これらのリスクを複数の切り口から分類していきます。

通信サービスの提供者としては、お客さまへの影響の度合いを判断し、それをもとにリスクを分類します。

Ⓐお客さまの事業継続に直接関わり、重大な影響を与える。
Ⓑお客さまの事業継続において、お客さま側で代替手段の確保が可能。
Ⓒお客さまの事業継続に与える影響が軽微、もしくはない。

弊社の場合、このような分類で考えています。

また、想定脅威への対策を考える際は、リスク要因の存在場所から見た分類も必要となります。

●IIJ社内。
●業務委託先、派遣会社。
●他社のサービスに依存。

このように想定脅威に対する被害箇所を考え、その被害がお客さまに与える影響の度合いを数値化し、脆弱性につながるリスク要因の存在場所をあぶり出して、対策を事前に検討する、という作業を行なっています。

こうした分類作業を通して、発生の可能性が高そうなリスクについて、事前対策と緊急時対応を実施します。弊社の場合は、通信サービスの提供者という立場でしたが、実際の分類では、お客さまの事業形態や事業継続に対する優先度に応じて検討していきます。

対策の立案と実施

通信サービスの提供者としては、お客さまの事業継続に直接的かつ重大な影響を与えるリスク要因の存在場所の一つに、弊社内のリソースが考えられます。ここからは、そうしたリソースについての事前対策と緊急時対応を見ていきます。

まず、お客さまの事業継続に重大な影響を与えるサービスを抽出し、そのサービス提供を維持することによって、お客さまの事業継続が可能となるようにリソース確保のための対策を定めます。

インターネットを利用するには、ルーティング、DNS、メールといった基本サービスが不可欠です。これらが正常に提供できないと、お客さまの事業に重大な影響が及びますので、これらのサービス提供を途切れさせない体制が必要となります。

上表は対策の一例ですが、こうした対策をとることで、弊社内に存在する、お客さまの事業継続を困難にするようなリスクを軽減し、事業継続を支える体制が強化されます。

これらの項目のなかにはその企業の脆弱性に該当するものもあり、そうした部分を少なくすることは、通常の業務でも求められます。場合によっては、その企業本来の事業活動と直接関わっていないリソースもあり、企業によってリソースの重要度が異なってきますが、直接関わっていないからといって、それに対する考慮を怠ってはならないものも少なくありません。

IT部門では、弊社のような事業者が提供する通信サービスをご利用いただいていると思いますので、事業継続に必要な対策がとられたサービス、複数のサービスを利用することによる冗長化、緊急時にすぐ使えるサービスの契約などが必要だと考えられます。

また、これらの対策は一度実施すれば完了するものではなく、継続的に評価して、常に最新の状態を維持するようにしなければなりません。そうした対応をとるために、それを支える体制がしっかりしていることを確認するのも重要です。

具体的な体制とは

事業継続を考える場合、会社単位で危機管理体制を敷くことが計画にも定められていると思います。弊社では、会社全体の危機管理を指揮する部署を頂点として、「リスク分類」の冒頭で述べた四つの活動領域毎に対策本部を組織して、対応にあたるようにしています。

対策本部は、既存の組織をもとに横断的に設置します。対策本部長に任命された役職員は、通常組織のなかでは事前対策を中心にとりまとめ、平時から準備を行ない、いざ緊急事態となった場合は、迅速に対策本部を立ち上げて、行動に移せるよう定期的に訓練しています。

企業では常に組織変更や人事異動がありますので、日頃からこうした組織横断の活動を行ないやすい環境を整えておくことも重要だと思います。

対策本部は、複雑な階層を設けないで、フラットな体制で役割を決めておき、召集がかかるとその役割に徹してもらうよう定めています。こうした体制は、大きな物的被害をもたらした自然災害への対応として、二〇一一年三月一一日の東日本大震災の際にも活かされました。

もちろん、それ以降も事業継続計画を見直しながら、リスクの再評価・対策の変更などを地道に行ない、「お客さまの事業継続を支えることが弊社の事業継続である」という考えにもとづいて、体制を運営しています。

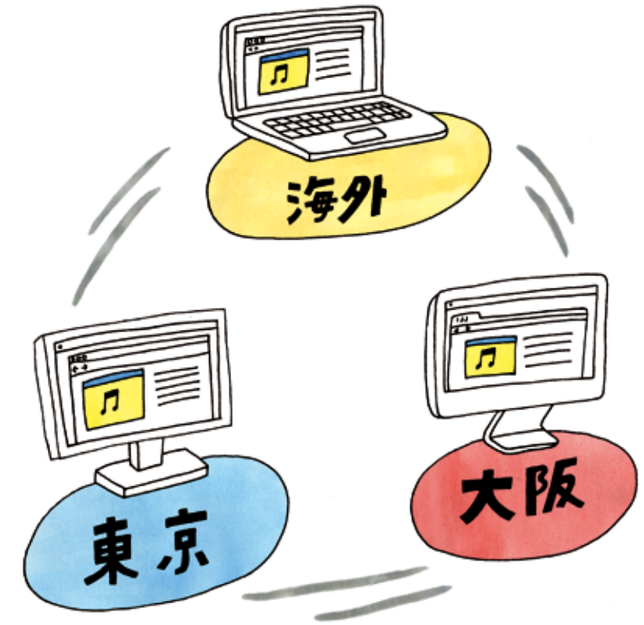
事業継続については、考えれば考えるほど次から次へと様々な案が出てくるものです。今回は、一般論的なところから始めて、リスクに備えるには事業継続をどのように考えればいいか、という点を中心に述べてきましたが、IIJは通信サービスの提供者として、お客さまの事業継続を第一にサービス提供を行なわなければならないのは当然のことです。同時に、お客さまの事業継続を支えるには自分たちの事業継続ができていなければならず、自分たちの事業継続を担保するためにも、日頃から準備・対策を行なっています。

本特集で紹介するいくつかの事柄――設備や体制の事例、情報セキュリティに対する脅威や漏えいリスクの低減などが、自然災害だけではないリスクに備えるという観点からも、お客さまの事業継続を考える一助になれば幸いです。●

WEBサイトのBCP対策

WEBサイトの災害対策は後回しにされがちだが、
クラウドサービスを用いることで、低コストかつ簡便に対策を講じることができる。

IIJ ソリューション本部 エンタープライズソリューション部
基盤ソリューション開発課長
鈴木 透



ITシステムのBCP対策では、一般に業務に直結する基幹システムや業務系システムの対策が優先され、WEBサイトの対策は優先度が低いのが現状です。しかしながら、企業のコーポレートWEBサイトや自治体の公式WEBサイトは、事故や災害発生時に事業への影響や対応状況を迅速に伝え、顧客や関係者とコミュニケーションをとるための重要なツールとなります。

特に大規模な災害や事故では、社会的な混乱や不安から風評などが広まりやすくなるため、公式情報を常に発信し続けることは、企業や組織の社会的信頼を維持するうえで非常に重要です。そこで本稿では、WEBサイトの災害対策について紹介したいと思います。

WEBサイトの災害対策

WEBサイトの災害対策で考慮すべきポイントは左記の四点です。

①地理的に離れた場所にWEBサイトを分散配置する。
②バックアップサイトに切り替える仕組みを備える。
③災害後のアクセス集中により、閲覧不能にならないように備える。
④WEBサイトの情報を更新できる環境を整える。

以上のポイントを押さえた対策は、クラウドサービスを活用することで比較的簡単に、短期間で実現できます。ここからは、IIJのクラウドサービス「IIJ GIO」を利用した対策をポイント毎に解説していきます。

①地理的に離れた場所にWEBサイトを分散配置する。

火災や事故によりサーバルームやデータセンターに損傷が生じると、長時間にわたりシステムを復旧できない状況が起こり得ます。また、大規模な地震や自然災害では、広い地域で電力の供給が止まることが想定されます。

そうした災害時のWEBサイト停止に関する対策では、地理的に離れた場所にバックアップサイトを配置することが効果的です。

IIJ GIOは、東日本、西日本、海外に複数の設備を有しており、利用者はどの地域の設備を利用するか選択できます。一例を挙げると、東日本の自社サーバルーム内に設置されたメインサイトのバックアップに、IIJ GIOの西日本設備を利用するといった使い方です。もちろん、メインとバックアップの両方をIIJ GIOの東西設備に分けて配置することも可能です。

②バックアップサイトに切り替える仕組みを備える。

メインサイトが停止したら、迅速にバックアップサイトに切り替えなければなりません。WEBサイトの切り替えには、DNSによる名前解決の仕組みを利用します。WEBサイトへアクセスするURLに紐づくグローバルIPアドレスを、メインサイトからバックアップサイトに向けるようDNSの設定を変更します。しかし有事の際は、このようなオペレーションを行なうことがむずかしいと予想されます。そこで、自動的にバックアップサイトに切り替わる仕組みを整えておくのが理想です。

自動的な切り替えを行なうには、IIJ広域負荷分散サービスが効果的です。このサービスは、地理的に離れたWEBサイトの稼働状況を常に監視し、状況に応じて自動的にアクセスを分散させます。メインサイトが停止したら、アクセスを自動的にバックアップサイトに誘導するので、WEBサイトの利用者は、バックアップサイトへの切り替わりを意識することなく、メインサイトと同じURLでアクセスできます。

③災害後のアクセス集中により、閲覧不能にならないように備える。

東日本大震災では、情報伝達の手段としてツイッターなどのソーシャルメディアが大きな役割を果たしました。ソーシャルメディアの普及により、情報が拡散・共有される速度が飛躍的に高まりましたが、その情報源となる企業・自治体・公共インフラなどのWEBサイトには、正確な情報を求める人々のアクセスが殺到し、WEBサイトがダウンしてしまう事態が多発しました。

こうした急激なアクセス負荷に備えるには、迅速にWEBサーバを追加・アップグレードできるクラウドサービスが有効です。IIJ GIOホスティングパッケージサービスでは、管理者画面からオンラインでサーバの追加やリソースの増強が可能です。サーバの追加はクローニング機能を利用することで、契約済みのサーバの設定を引き継いだコピーを作ることができます。追加したサーバのセットアップの時間を短縮し、迅速にWEBサイトを増強できるのです。

しかし有事の際は、サーバの増強オペレーションを行なうことがむずかしい事態も想定されます。そうした場合、IIJ GIOコンテンツアクセラレーションサービスが効果的です。このサービスは、IIJバックボーン上の配信設備にWEBコンテンツをキャッシュし、高速配信します。WEBサイト閲覧者からのアクセスはWEBサーバの手前にあるクラウドの配信設備で処理されるため、急激なアクセス増に対してWEBサーバの負荷を軽減し、WEBサイトのダウンを防ぐことができます。

IIJ GIOコンテンツアクセラレーションサービスは初期費用が0円で、転送量に応じて課金されるため、必要なときに必要な分だけ利用できます。災害に備えた上手な利用方法としては、バックアップサイトにのみIIJ GIOコンテンツアクセラレーションサービスを利用し、先の広域負荷分散サービスと組み合わせます。平常時はメインサイトでアクセスを処理し、災害時に広域負荷分散サービスによりバックアップサイトに切り替わったときのみコンテンツアクセラレーションサービスを使うようにすれば、平常時はコストを抑え、災害時にはアクセス急増に耐えることができます。

④WEBサイトの情報を更新できる環境を整える。

①から③のポイントを押さえて、落ちない・止まらないWEBサイトを構築できたとしても、災害時にWEBサイトをタイムリーに更新できなければ意味がありません。しかし、平常時にWEBサイトの更新に使用している環境が災害時にも使用できるとは限りません。万が一に備えて、リモートからWEBサイトを更新できる環境を用意しておきましょう。

そうした環境を用意する場合、気をつけておきたいのがセキュリティです。IIJ GIOリモートアクセスサービスを利用すると、クライアント端末からの通信は、L2TP/IPsecやSSTPなどで暗号化されます。また、接続元IPアドレスやMACアドレスでの接続元制限、ワンタイムパスワードを利用した安全なリモートアクセスを実現できます。

WEBサイトの災害対策はシンプルで、基幹系や業務系のシステムに比べると低コストで実現できます。さらにクラウドを利用すれば、資産を持つことなく、短期間で実現可能です。ぜひ、WEBサイトのBCP対策の参考にしていただけましたら幸いです。●

情報漏えいを防ぐためにソリューションにできること

悪意あるものからうっかり事故まで、情報漏えいは、企業の信頼を失墜させるリスクを孕んでいる。
情報漏えいを防ぐために、企業はどのように守りを固めるべきなのか？

IIJソリューション本部
ネットワーク・セキュリティソリューション部
セキュリティインテグレーション課
筒井 達大

情報漏えいが発生すると、企業は信頼の失墜や賠償金の支払いなど多大なリスクを負うことになります。情報漏えいに対する危機意識は、世界中で国家レベルにまで高まっており、政府や企業にとってその対策は、もはや先延ばしできない状況にあります。

情報漏えい対策は、外部からの攻撃に備えるだけでなく、内部からの持ち出しも考慮する必要があり、当事者は「どこから手をつけていいのか分からない」というのが実情です。本稿では、組織がとるべき方針、情報漏えいの危機、対策などを紹介します。

組織が行なうべき対策

昨年二月一三日、米国ではオバマ大統領により情報漏えい対策に関連する大統領令（Executive Order 13636）が発令され、米国立標準技術研究所[*1]が作成したCybersecurity Framework[*2]において、対策目標基盤として組織が行なうべき五つの管理活動が示されました。

一つ目は、情報資産を〝特定（IDENTIFY）〟することです。組織が保護すべき対象を明確にして、管理に向けた棚卸しを行ない、組織が定めているガバナンス要件や法令が定めるコンプライアンス要件に沿った、リスクの評価と対応方針を決める活動となります。

二つ目は、〝特定〟された対象を〝保護（PROTECT）〟することです。サイバー攻撃などの脅威に対して、セキュリティ製品の導入、担当者のトレーニング、アクセス制御などの対策を実践することが〝保護〟の活動にあたります。日本の上場企業が内部統制監査制度に対応する場合、以上の二つの管理活動はその対象に入っていると思われます。

三つ目は、保護した対象の異常を〝検知（DETECT）〟することです。異常な活動を速やかに検知し、影響度を把握すること、〝保護〟対策による効果の継続的なモニタリング、検知プロセスとプロシージャの確立と維持が主な活動にあたります。

四つ目は、検知した事象に〝対応（RESPOND）〟することです。異常な活動を検知した際に対応計画を作成しているか、〝対応〟にあたる当事者が十分な責任を理解しているか、〝回復〟活動を支援するための分析やインシデントの除去に努めているか、過去の教訓を生かして改善活動を進めているかなど、実際のインシデント・レスポンスを行なう活動にあたります。

五つ目は、もっとも重要な活動である〝回復（RECOVER）〟です。攻撃により影響を受けたシステムを復旧するために〝回復〟計画を作成しているか、内部はもちろん外部ともリレーションを持って、評判の修復や情報共有の状態を確認する活動にあたります。

これらの管理活動のうち、〝特定〟〝保護〟は、多くの組織ですでに行なわれているかもしれませんが、〝検知〟〝対応〟〝回復〟まで含めた対策を実施している組織は少ないのではないでしょうか。日本でもこのフレームワークをベースに、組織のセキュリティ施策や情報セキュリティポリシーを再考すべきではないかと考えています。

攻撃に狙われている組織

情報漏えいの原因の一つに、外部からの攻撃が挙げられます。IT技術の普及や知的財産価値の高騰を背景に、情報システムの脆弱性を突いて情報漏えいを引き起こす事件が増えています。外部から攻撃を受ける原因は、組織でセキュリティに関する適切な対策がとられていない場合が多く、〝検知〟までの対策を行なっていなかったため、情報が漏えいしたことにすら気づかず、知らないうちに情報が搾取され、気づいたときには対処不能な状況に陥っていた……という話をよく耳にします。

攻撃への対策として、ファイアウォールやIDS／IPSによる境界型防御は大半の組織が行なっており、標的型攻撃対策、WAF、ネットワークフォレンジックといったより高度なセキュリティ対策システムを導入している組織も増えています。

セキュリティ対策に必要なのは、まず自分たちが保護すべき対象を〝特定〟することです。例えば、外部に公開しているサーバにセキュリティホールはないか？ユーザが無意識のうちに攻撃者に利用されることのないよう、組織全体が十分なセキュリティ意識を持っているか？　など、セキュリティ対策システムを導入していない組織は、危機意識を持って現況を正確に把握する必要があります。また、セキュリティ対策システムを導入している組織も、導入するだけでは十分でなく、日々更新されるセキュリティ事情に追随して、適切な管理を行なうことが大切です。最近では攻撃が高度化し、単体のセキュリティ対策システムでは一部しか検知できないといったこともあり、複数のセキュリティ対策システムを導入し、それらを統合的に管理しながら、〝保護〟〝検知〟〝対応〟〝回復〟を適切に行なう必要性が高まっています。

外からだけではない漏えい経路

次に内部からの情報漏えいについてお話しします。JNSAの調査報告[*3]によると、漏えいの原因は、管理ミス59パーセント、誤操作20・1パーセント、紛失・置き忘れ8パーセント、不正な情報持ち出し・内部犯罪3・8パーセント、盗難3・7パーセント、不正アクセス・設定不備の大半を占めるのは、内部からの漏えいであり、その対策としては、関係者に向けた情報セキュリティに関する啓蒙活動以外にも、システム面で対応できる部分も多くあります。

管理不備や誤操作による漏えいをゼロにすることは不可能ですが、情報資産を〝特定〟し、アクセス権限などを見直すことで危険性は減らせます。また、不正な情報持ち出しなども含めて、「やろうとすれば、できてしまう環境」を除いていくことも大切だと思います。ユーザを信頼し、業務に支障が出るからといって、内部制限を厳しく課していない組織もありますが、情報の価値・重要性が高まっている今日、対策を施さないまま、情報が漏えいしてしまうと、組織の存続自体が危うくなることも考えられます。

情報漏えい対策の一つに「証跡取得」があります。ユーザのデータの移動、特に多くの情報が拡散する恐れのあるインターネットへのアップロードや可搬型記録媒体へのコピーの証跡を残すことは、情報持ち出しへの抑止力になりますし、漏えいが発生した際の検知・対応・回復にも有効です。こうした対策を行なっているか否かは、対外的な評判にもつながりますので、どのような組織でも証跡取得の検討・実施を推奨します。昨今では各セキュリティメーカが、Data Loss Prevention製品[*4]を展開しており、国内でも導入事例が出ているようです。

情報漏えいへの取り組み

IIJでは、先に述べた管理活動に取り組むためのコンサルティングやアセスメントを行なっています。また、IIJが得意とするネットワークの領域から、必要かつ効果的なセキュリティ対策のご提案も行なっています。

情報漏えい対策は、ネットワークの領域で実施可能なものも多く、弊社のサービスやソリューションを利用したファイアウォールでの制御、IDS／IPS、WAF、標的型対策による挙動制御、ウェブプロキシやメールリレーサーバでの証跡取得やアップロード制限などは、すぐにご利用いただけます。さらに、インテグレーションによるネットワークフォレンジック製品を利用した通信記録の取得やユーザの操作ログ取得など、情報資産の性質に合わせた包括的なご提案も可能です。

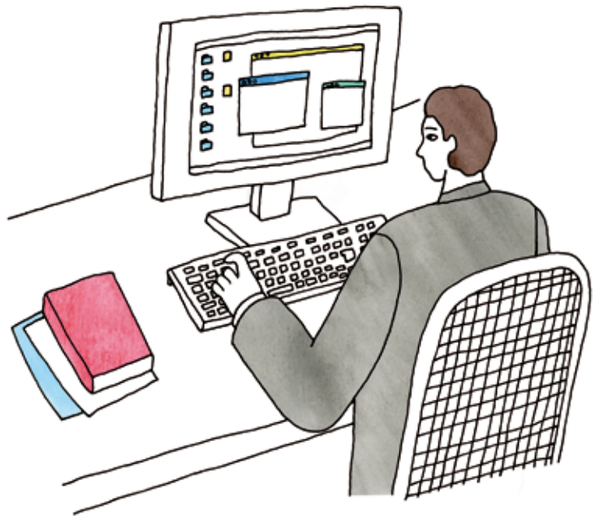
今回紹介したフレームワークは米国での事例ではありますが、日本でも近い将来、同じ状況になると思われます。これをきっかけに「情報セキュリティ対策は緊急の課題になりつつある」という認識を持っていただければ幸いです。●

*1 National Institute of Standards and Technology, NIST
*2 NIST SP 800-53 連邦政府情報システムにおける推奨セキュリティ管理策
*3 JNSA「2012 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」
*4 一般に、機密情報へのアクション（開く、コピー、移動など）をプロファイル（ユーザ）毎に制限、もしくはロギングできる製品。

情報通信環境とともに変貌するセキュリティ事情

企業などへの攻撃に関して、その影響が及ぶ範囲を把握しづらいものが増えている。
これは、昨今の情報通信環境の変化に起因する部分もあるため、
企業は最新のセキュリティ情報を知ることに加え、
自身のシステム環境の詳細も認識しておく必要に迫られている。

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
齋藤 衛



最近、企業などの組織に対して行なわれている攻撃において、例えば、DDoS攻撃では、リフレクション攻撃の流行により、国際的には100Gbpsを超えるような規模の攻撃も珍しくなくなってきました。また、WEBを改ざんしてマルウェアに感染させる試みや、標的型メール攻撃に代表されるメール添付型のウイルスについても、その発生回数が増えるとともに、水飲み場攻撃や、やり取り型攻撃などと呼ばれる攻撃が行なわれるようになってきました。

しかしこれらの攻撃は、規模こそ大きくなり、より複雑化していますが、対策を検討するうえで本質的な違いはなく、対策装置の処理能力の増強や、従来手法の組み合わせの強化によって対応することができます。一方、昨今では、従来とまったく同じような問題や事件が、より幅広い影響を与えたり、これまでとは異なる意味を持ったりする状況が発生しています。ここで、いくつかの例を紹介します。

思わぬところに影響が及ぶ最近の攻撃

まず、OpenSSLに関わる二つの脆弱性が挙げられます。このソフトウェアは通常、WEBサーバの暗号化通信に利用されるものですが、サーバだけでなく、組み込み機器やセキュリティ対策装置などアプライアンス機器の管理インタフェースへの通信の暗号化に利用されていたり、暗号化通信を行なうクライアントでも利用されていたため、脆弱性の発見当初考えられていたよりも多くの装置がその影響を受けました。

また、本稿執筆時点において、世界中で対策が講じられているGNU bashの脆弱性も、Linuxをベースにしたほぼ全ての環境に組み込まれているソフトウェアの脆弱性であるため、サーバからNAS専用機などの組み込み系機器にまで影響が及んでいます。

さらに本年は、ソフトウェアの更新手法を悪用したマルウェア感染事件が複数発生しています。これらはいずれも当該ソフトウェアそのものの問題ではなく、更新に用いるネットワーク側のサーバ環境への侵入や、当該ソフトウェアとともに配布されているアップデート専用のソフトウェアに起因する問題により引き起こされています。

こうしたケースでは、ユーザがその利用を意識していないために意外な場所で影響が出たり、問題の対象であることを認識できなかったために対策が遅れて、問題が発生しているのです。

一方、昨年末から本年初頭にかけて、ネットワーク型のサービスを利用する日本語入力システムにおいて、企業がこのシステムを利用した際に、情報漏えいにつながる可能性があることが指摘され、大きな話題となりました。このシステムは、新規に購入したPCやタブレットなどの端末にプリインストールされていたために、ネットワーク上のサーバに情報が送られることに関する説明が不足していたり、ユーザに同意を得る過程を経ないまま利用される場合があったりして、ユーザが把握していないにもかかわらず、外部に情報が送信されてしまうという問題が発生しました。

さらに、個人ユーザに関連したものと思われがちな事件でも、企業などに影響を与えることがあります。例えば、個人向けオンラインサービスの認証情報の漏えいや、リスト型攻撃などのように漏えいした情報を悪用する事件も、個人ユーザだけが気をつければいいというものではありません。

昨年発生したある文書処理ソフトウェアの登録者情報の漏えいでは、世界中の数千万人の登録情報が漏えいしたとされていますが、ソフトウェアの性質上、会社で使うメールアドレスやパスワードなど、個人を特定するための個人情報ではあるものの、会社で使うメールアドレスなどのように企業に関連する情報が登録される可能性が高い状況にありました。

そして、国内での金融取引を狙ったマルウェアにより取得した情報をもとに不正送金を促すといった手口は、法人口座のオンライン取引においても同様の手口が発生しています。

自身の通信環境を把握することも大切

以上のように、それぞれは従来から発生していた問題や事件ではありますが、その影響範囲が企業などに設置された数多くのシステムや、その組織の活動そのものに影響するような事例が増えています。これらは、情報通信機器の実装の変化、利用するアプリケーションの構成の変化、企業などで利用するサービスの変化にともなって発生しています。

一〇年前の企業などの情報通信環境を考えれば、情報はPCのなかにインストールしたソフトウェアによって取り扱われ、専用のサーバに保存または処理を依頼するような単純な環境でした。しかし現在では、企業などのネットワークには多様な情報通信機器が接続されており、個人が仕事をする環境においても、PCやタブレットにインストールしたソフトウェアの多くが、ネットワーク上のサーバと協調して動作することで、従来よりも高度な機能を提供するようになっています。さらに、企業などにおいても、個人の私的な活動と同様に、ネットワーク上のサービスを活用する機会が増えています。

こうした変化の背景には、コスト面や機能面の利点に加え、セキュリティ対策面での利点もあります。例えば、共通のプラットフォームを利用していることで、特定の脆弱性に対して同じ対策を適用できるようになります。また、ネットワーク上のサービスの利用では、データの保管や処理と、表示、操作など、人間とのあいだの処理を分離することにより、それぞれ別のセキュリティ施策を実施して、仮に人間に表示するためのタブレットがウイルスに感染した場合でも、他への影響を限定できます。

しかしこのような利点は、構成要素を明らかにし、その要素に関する知識を事前に持ち、それぞれの場所でのセキュリティ侵犯の影響を評価することにより、はじめて実現できるものです。

利用する機器の内部でどのようなソフトウェアが動作しているか、PCやタブレットで利用するアプリケーションの内部にどのような構成要素があるのか、どのような外部のサーバとどのように通信を行なうのか、外部のサービスに預ける情報は何かなど、様々な条件を明らかにしたうえで情報通信環境を利用する必要があります。

情報セキュリティの世界では、孫子の兵法から「彼を知り己を知れば、百戦殆うからず」という言葉がよく引用されますが、今は己を知ることに努力を払うべきときだと言えるのです。●

有事に負けないサポートセンター運営

いざというとき、サービス提供者とユーザとのあいだをつなぐのが、
サポートセンターの役割である。
特に“有事”の際は、その責務がいっそう重くなるため、
普段からそうした事態に対応できる体制作りを進めている。

IIJ サービスオペレーション本部
サポートセンター 部長
菅原 史

IIJは、冗長化構成などサービスインフラにおける耐障害性の向上を図ることで、有事の際にもサービスを継続的に提供できるよう努めており、お客さまと弊社を結ぶインタフェースであるIIJサポートセンターも、サービスサポートの継続に注力しています。

IIJサポートセンターは、以前は東日本のみで運営していましたが、二〇一一年の東日本大震災をきっかけに、東日本と西日本で分散運営するようになりました。

東日本大震災のような広域災害は、通信網の切断や電力危機など想定を超える広範囲な影響を我々の生活基盤に及ぼします。そして、こうした状況は、サポートセンターの電源設備やサポートネットワークの冗長化を図ることで、機能自体は維持されている状態にあっても、その業務を実際に遂行する運営スタッフの確保に影響を及ぼす場合があります。

東日本大震災では、震災や輪番停電による交通機関の乱れは数日のうちに一定レベルにまで回復し、サポートセンターの運営に大きな支障が出ることはありませんでしたが、このときの経験がもとになって、東日本と西日本にサポートセンターの機能と運営スタッフを分散配置・運営する必要がある、との判断に達しました。

大規模障害対策本部とサポートセンター連携

地震が発生した二〇一一年三月一一日一四時四六分、サポートセンターの運営スタッフは、IIJ本社で大きな揺れを感じ、すぐに大規模障害対策本部の設置にかかりました。このとき、本部設置を知らせる携帯メールが携帯電話網の混雑により各担当者に届きませんでしたが、地震が発生した日が平日の金曜日であったため、大規模障害対策本部の設置は各担当者の判断で地震発生から一三分で完了し、対策本部とサポートセンター間の連携が確立しました。

しかし、JRをはじめとする公共交通機関は、安全確認・復旧作業・停電などの影響により機能が麻痺してしまい、二四時間体制で稼働しているサポートセンターに夜勤の運営スタッフが出勤できない状態となり、残された運営スタッフが交代で業務を継続することになりました。これは、翌日が週末（土曜日）であったから可能になった対処であり、万全な体制とは言えませんでした。

サポートセンターの東日本・西日本分散運営

●統合窓口

IIJサポートセンターは、全国共通の電話番号を用意しており、この統合窓口の代表番号にかけると、東日本の番号と西日本の番号の両方に着信し、被災地から遠隔な地域の番号へ着信するように制御が可能です。通常、災害発生時には救援・復旧や公共の秩序を維持するために、防災関係などの機関に対して固定電話や携帯電話への接続が優先される「災害優先通信」が発動されます。この「災害優先通信」が実施されると、一般電話の被災地への接続が制限され、仮にサポートセンターが被災地域内に存在する場合は、この制限を受けることになります。

IIJサポートセンターへの電話接続は、こうした状況下でも東日本・西日本に分散されて着信し、サポートセンターへの間を接続している自社運営のIP電話網を経由して、お客さまからの着信を平時と同じように受けることができます。

●体制

サポートセンターの機能を西日本にも拡張する作業に着手したのは、二〇一二年の後半です。初期段階では、災害発生にともない東日本のサポートセンターが機能停止した場合、お客さま向けの窓口機能や情報提供を引き継ぐことができる体制を整えました。

広域災害の発生時、IIJでは、単一または複数サービスにおいて多数のお客さまに影響を及ぼしている、または及ぼす可能性があると判断されると、災害対策本部を設置すると同時に大規模障害対策本部を設置します。IIJサポートセンターは、この大規模障害対策本部の対応方針にもとづき、お客さまに提供しているサービスの稼働状況や災害による影響の有無などをご案内します。

二〇一三年以降、西日本のサポートセンターの体制を強化するために、東日本サポートセンターで実施しているサービスサポート機能・業務の移管を進めてきました。そして、二〇一四年上期に体制強化が完了したら、窓口業務、障害対応業務、問題解決支援業務など個々の機能を移管し、冗長化を推進していく予定です。

●災害など非常時におけるリモートアクセスの許容

IIJサポートセンターへの入室時の管理方法は、執務エリアへの入室はオフィスビルが提供する非接触ICカードによる制限、さらにセンターエリアへの入室は独自に用意した生体認証を用いた制限という二重管理を施しています。

同センター内で取り扱うお客さまの契約情報や構成情報などは、センター内にあるサーバ類にはいっさい保管せず、全て弊社が運営する堅牢なデータセンターで保存・管理しています。そして運営スタッフは、業務端末を用いてこれらの情報にアクセスすることでサポート業務を行なっています。

また、公共の交通手段などを利用できず、運営スタッフが出勤できない状態に陥ることも想定して、「非常時専用のリモートアクセス環境」が準備されています。リモートアクセスできる環境は、情報管理の点から見ると賛否両論あると思いますが、当社ではリモートアクセス環境の発動基準を明確に規定しており、想定を超える広域災害や大規模障害などが発生し、運営スタッフの出勤が困難になったときのみ、発動するように取り決めています。

より充実したサポートセンターを目指して

地震や台風など大規模な自然災害発生時に安定したサービスサポートを提供していくには、分散運営によるハード（サポートセンターの機能や環境）の冗長化のみならず、ソフト（運営スタッフ）の確保が不可欠です。

東西に分散されたIIJサポートセンターは、これまでのところ順調に運営されています。今後は、こうした運営面にとどまらず、サポート対応についても業界でイニシアティブをとれるよう、様々な取り組みを続けていきたいと考えています。例えば、ユーザサポートページの改善、情報発信の刷新、問題解決支援の強化……等々、お客さまの期待を上回ることができるようなサポート対応を目指して、システム面の高度化も進めていく予定です。●

人と空気とインターネット

自動化・機械化の行く末

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

自動車の自動運転技術の開発は、
グーグルが口火を切り、その後、
多くの自動車メーカが追随している。
こうした自動化・機械化の流れは、
我々の生活全般にどのような
影響を及ぼすのだろうか？

二号前の小誌で、週末を利用して農業に少し力を入れ始めたと書いたのですが、それに関連して今年の春、軽トラックを購入しました。

昨年はセダンのトランクに長靴、農機具、肥料などを積んで畑に通っていたのですが、トランクはすぐに一杯になって必要なものを積みきれませんし、何よりも車の内も外も泥だらけになっていました。そんなわけで、今年は思い切って軽トラ・オーナーになる決意をしたのです。

その際、AT（オートマ）車はMT（マニュアル）車よりも値段が高くなるので、これまた思い切ってMT車を選びました。MT車を運転するのは実に三〇年ぶりくらいでしたので、最初は何度もエンストを起こして、周りの人の顰蹙を買っていました。それでも、半月くらいでMT車の運転感覚を取り戻し、今ではまったく問題なく運転できるようになりました。若い頃、身につけたスキルはブランクがあってもちゃんと思い出すものだなと、少し自分を褒めてあげたい気分です。しかし、久々に運転してみると、MT車の運転って、クラッチを何度も踏み、何段階もギアを切り替えながら加速しなければならないので、何とも面倒くさいものだったんだなと感じています。改めてAT車のありがたさと、技術の進歩の恩恵を感じた出来事でした。

自動運転車の実用化

グーグルが「自動運転車」の開発に着手したのは二〇一〇年でしたが、二〇一二年には米ネバダ州の公道で試運転を行なえる免許を取得し、実際の路上での試験が始まりました。これに刺激され、国内の自動車メーカもこぞって自動運転車の開発に着手し始めました。二〇二〇年には日本でも高速道路走行などの限定的な環境で、ドライバーが運転操作をしなくても走行できる、いわゆる〝ロボットカー〟が実用化される見込みです。これが実用化されれば、人間はギアチェンジどころか、アクセルを踏んだり、ハンドルを操作する必要もなくなり、非常に楽チンで快適な運転環境が実現します。

このようなことが可能になった背景には、コンピュータの小型化が進み、非常に高性能なコンピュータを車に載せられるようになったことと、ソフトウェアが高度化し、自動運転に欠かせない膨大な情報処理を短時間で行なえるようになったことが、おもな要因として挙げられるでしょう。また、刻々と変わる道路の混雑状況など、様々な判断に必要なデータをネット経由でリアルタイムに入手し、活用可能になったことも大きいと思います。これは自動運転車に限ったことではなく、コンピュータの小型化・高性能化、ソフトウェア技術の進化、インターネットの発達により、今後、多くの分野において、これまで人間が行なっていた、ある程度以上のスキルや知識を要する操作が、自動化・ロボット化されていくでしょう。そして状況によっては、人間以上の「能力」を発揮するケースも増えてくるに違いありません。

最後には人間は邪魔になる？

例えば、タクシーの運転などは、全ての道を記憶し、目的地までの最短ルートを素早く頭のなかで組み立て、しかも安全に安定した運転を行なわなければなりませんので、特殊な能力や訓練が要求される業務です。実際に、非常に厳しい試験をパスしないと免許がもらえないことで知られるロンドンのタクシー運転手は、記憶をつかさどる〝海馬〟と呼ばれる脳の部位の大きさが、平均的な人よりも大きく発達している、との研究成果もあります。しかし、記憶や計算はコンピュータの得意分野ですから、ロボットカーに人間の運転手が敵わなくなる日もそう遠くないでしょう。あとは、自動運転車の量産が可能になり、生産コストが人間を雇うより安くなれば、タクシー運転手という職業は姿を消すのかもしれません。

一般社団法人日本ハイヤー・タクシー連合会のホームページを見ると、平成二二年の登録運転者数は三七万人となっています。これに同年の個人タクシー事業者数の四万三千人を足すと、およそ四一万人のタクシー運転手が近い将来、職を失う可能性があるということになります。万が一、そうなってしまうと、平成二二年末の完全失業者数は三二一万人でしたので、失業者数が一〇パーセント以上も増える計算になります。タクシー以外にもバスや郵便や宅配便など、多くの運転業務はありますので、運転手という職業がなくなるインパクトは計り知れません。

ただ、グーグルカーも、実際の道路を安全に走行するには、周りの状況を認知する機能にまだまだ課題があるようです。現状のグーグルカーは、大雨や降雪時には走行できない、とする分析レポートがMITの科学雑誌に掲載されたそうです。つまり、周りの状況を把握するためのセンサの精度が低く、大粒の雨や雪を障害物と判断してしまい、動けなくなることがあるというのです。また、路上に落ちている石と、丸められた紙の区別がつかなかったり、日差しが強い日は信号を見落としたり、まだまだ人間の運転手でなければ対応できない状況がたくさんあるようです。それらが全て解決され、一〇〇パーセント安全に自動運転が可能になるまでには、もう少し時間がかかりそうです。

しかし、人間の運転手と完全に同じ環境で自動走行を行なおうとするからむずかしいのであって、問題を少し単純化すれば解決できるのではないでしょうか？

例えば、自動運転車専用道路を作って、そこを走行する全ての自動運転車をネット経由で集中管理・制御するようにし、人間が運転する車や歩行者はいっさい侵入禁止にしてしまえば、別に人間用の信号なんて認識する必要はなくなります。そうすることで、個々の車の速度や振る舞いを決めて、全体の車の流量を最適化でき、非常に効率的な交通システムが実現されるでしょう。すると、近い将来、人間が公道で運転することは禁止され、道路上にはコンピュータ制御された自動運転車のみが静かに整然と行き交うようになる、なんてことは考えられないでしょうか？　そして、人間が〝趣味〟で運転を楽しむためのアミューズメントパーク（かなり大がかりなものになるでしょうが）が作られて、どうしても自分で運転したい人は、お金を払ってそこで遊ぶ、という新ビジネスも生み出せるので一石二鳥です。（笑）

システムの完全性や経済合理性を突き詰めていくと、結局、最後には人間は邪魔になるのかもしれません。もし植物工場で野菜が安価に大量生産できるようになったら、人間が手作業で行なう畑仕事なんて、もはや贅沢な趣味に過ぎなくなるのかもしれません。ですが、食糧生産という、生きるために直接必要な仕事まで機械に奪われてしまったら、人間は何を喜びとして生きていくのかなぁ……などと呟きながら、軽トラのマニュアルギアチェンジも軽やかに、通勤前の農作業を楽しんでいます。●

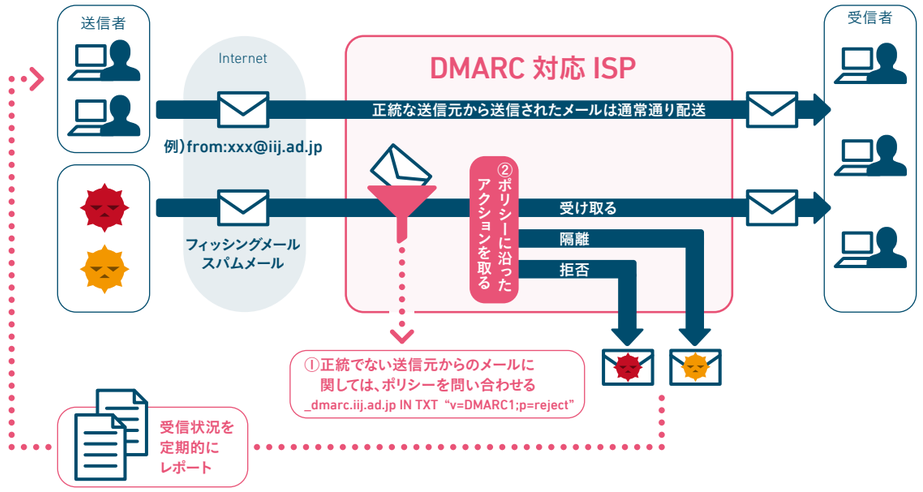
イラスト／末房志野

Technical Now

“DMARC”によるフィッシングメール対策

IIJプロダクト本部 アプリケーション開発部 サービス開発課
鈴木 高彦

フィッシング詐欺が横行するなか、
その対策として DMARC の導入が進んでいる。
ここでは「DMARC がどのような考え方で利用者を守るか」について、
考察を加えてみたい。



金融機関からのメールを装い、受信者の口座情報や ID などを不正に搾取するフィッシング詐欺が蔓延しています。フィッシングメールでは、受信者に違和感を与えないよう、送信元アドレス（From アドレス）を金融機関などフィッシングターゲットのアドレスに詐称するケースが大半です。送信元アドレスが詐称されると、ユーザはフィッシングメールであることに気づきにくくなり、フィッシングに巻き込まれる危険性が高まるだけでなく、送信元アドレスが詐称された企業やブランドの本物のメールまで疑わしく見えてしまうなど、企業やブランドのイメージにも悪影響を及ぼします。

DMARCとは？

DMARC は、送信元アドレスを詐称したメールに対して、ドメインの本来の所有者がポリシーの宣言というかたちで配送拒否を要求できる仕組みです。この仕組みにより、著名ドメインで数千万通から数億通のメールを配送拒否した、という成果が DMARC.org*より報告されています。また、ユーザから申告されたフィッシングメールの件数も著しく減少するなど、絶大な効果を上げています。

DMARC の目的は、フィッシングメールのような悪意あるメールから、ユーザとブランドの両方を守ることです。DMARC.org の立ち上げメンバーには Google、Yahoo!、AOL といった米大手 ISP や、PayPal、Bank of America といった米大手金融機関など、自社のドメインを不正に利用される被害に頭を悩ませていた企業が名を連ねています。

DMARC が提供する機能は大きく分けて二つあると言えます。一つは、送信元アドレスの正当性を確認できなかったメールに対するポリシーの宣言であり、もう一つは、主に ISP などのメール受信者からドメイン所有者への受信状況のレポートです。今回は、著しい成果を上げているポリシー部分について詳しく紹介します。

解決の方向性

DMARC のポリシーは、送信元アドレスの正当性を確認できなかったメールに対して「どう扱って欲しいか」を、ドメインの所有者が意思表示するものです。送信元アドレスの正当性の確認には、SPF や DKIM といった既存の送信ドメイン認証技術を使用します。

送信元アドレスを送信ドメイン認証技術で認証できないメールは、「正規のユーザが設定や使い方を誤って送ってしまったメール」か、「第三者が送信元を偽って送信しているメール」のいずれかです。ドメインの所有者は、「正規のユーザが誤った方法で送っているメール」「第三者が送信元を偽って送っているメール」に対して、「受け取って欲しい」「隔離して欲しい」「拒否して欲しい」のいずれかを選択し、ポリシーとして宣言します。ただし、原則的にこのポリシーはドメイン所有者の希望であって、実際にその通りのアクションをとるかどうかは、受信者の判断に委ねられています。

ポリシーのなかでも特に注目すべきは、「拒否」ポリシーです。DMARC.org を立ち上げた Google、Yahoo!、AOL などは、DMARC ポリシーを尊重したアクションをとりますので、「拒否」ポリシーを選択することで、「第三者が送信元を偽って送っているメール」を遮断できます。

ただし、「正規のユーザが誤った方法で送っているメール」も同様に遮断してしまいますので、「拒否」ポリシーを導入する前に、メールを想定外のサーバから送信しているユーザがいないかを洗い出したり、「受け取る」「隔離」といったよりインパクトの少ないポリシーから徐々に導入したりするなど、適切な準備が必要です。また、そのドメインが不正に利用された場合のインパクトと、正規のユーザが誤った方法で送っているメールが届かなくなることのインパクトのどちらを重視するかは、ドメインにより異なります。常に「拒否」が最良のポリシーというわけではなく、ドメインの用途に応じた適切なポリシーの選択が重要なのです。（コミュニケーションメール、マーケティングメール、トランザクションメールなど）メールの用途に応じてドメインを分割し、ドメイン毎に異なるポリシーを導入することが有効な場合もあるでしょう。

DMARC.org の立ち上げメンバーに金融機関が含まれていることからもわかるように、DMARC は不正利用された場合の影響が大きいドメインのオーナーを強く意識した設計になっています。つまり、ドメインの正規ユーザが多少の制約を受けても、ドメインを悪者による不正利用から守ろう、という考え方が支配的なのです。

この制約とは、具体的には、送信する際は必ず正規の送信サーバから送信することと、メーリングリスト（ML）にメールを送信してはならない、という二点です。これらの制約は、金融機関に限らず自社ブランドの保護に関心がある多くの企業にとって、十分に受け入れ可能だと考えられています。一方、ISP のサービスドメインのように、極めて多様な利用のされ方をするドメインにとっては、受け入れがたいものであり、「拒否」ポリシーを採用することはむずかしいと思われていました。

配送拒否という“劇薬”

そうしたなか、「状況は思ったより切迫している」と感じさせる事件が起こりました。2014 年 4 月、米国の Yahoo! と AOL が、相次いでそれぞれのメールサービスで提供しているドメインの DMARC ポリシーを「受け取る」から「拒否」に変更したのです。どちらも膨大な数のユーザを抱えるサービスだけに、ポリシーの変更によるインパクトは小さくなく、大きな物議を醸しました。

Yahoo! や AOL の正規のサーバではなく、他 ISP や送信事業者経由でメールを送信していたユーザ、ML を利用していたユーザは、突然、相手にメールが届かなくなりました。同時に、ML の管理者は、大量のエラーメールを受け取ることになりました。業界内でもこのポリシーの変更については、賛否両論が巻き起こりました。

Yahoo! も AOL も DMARC.org の立ち上げメンバーであり、何が起こるかを把握したうえで、ポリシーの変更を行なっています。では、なぜ両社は顧客の不利益を承知で、「拒否」ポリシーの選択に踏み切ったのでしょうか？

その理由ですが、金融機関などがドメインによる「拒否」ポリシーを採用し、フィッシング詐欺に対して極めて有効であることが明らかになってきました。一方で、Yahoo! や AOL のドメインを詐称したフィッシングメールによる被害は後を絶たず、拒否ポリシーの採用による副作用にこだわっている場合ではない、との判断が勝ったと考えられます。「拒否」ポリシーは劇薬ではありますが、これに頼らざるを得なかったのです。

さて、ドメインが「拒否」ポリシーを宣言すると、攻撃者はそのドメインを詐称したフィッシングメールを送れなくなりますが、残念ながらそのドメインを使わなくなるだけで、フィッシングを止めるわけではありません。おそらく彼らは、別の魅力的な、「拒否」ポリシーを宣言していないドメインにターゲットを変更するでしょう。実際に、有名ドメインが「拒否」ポリシーを宣言したのち、同業他社のドメインを使った詐称メールの増加が観測された、という報告もありました。

米国を中心に、送信元アドレスを詐称したフィッシングメールの被害の大きかったドメインにおいて、DMARC の「拒否」ポリシーを導入するケースが増えているため、今後、攻撃者は規模が大きくなくても「拒否」ポリシーを宣言していないドメインにターゲットを移していくと予想されます。ドメインのオーナーは、フィッシングのターゲットにされる前に、DMARC の仕組みや制約を適切に理解し、インパクトのない「受け取る」ポリシーの導入は、すぐにでも始めるべきではないでしょうか。●

＊DMARCについて主体的にとりくむ有志団体。http://www.dmarc.org

Technical Now

クラウド型アウトソーシングサービス “GLASIAOUS”

IIJ グローバルソリューションズ サービス推進本部 サービス企画推進部
嶋田 大祐

**日系企業の海外進出が加速するにつれ、
現地法人の業務面での過重が課題となっている。
ここでは、現地法人の経理業務を全面的にサポートするソリューションを紹介する。**

近年、多くの日系企業が新たな市場を求めて海外進出を計画したり、実際に進出を果たしています。そして、競争に勝ち抜くために、海外拠点の状況を本社が常に把握する必要性が高まっています。

しかし、新たに進出した国・地域において、現地の制度（法律・税制など）は、日々改定され複雑化しており、事業を展開する先々でそれらを遵守し、自社のリソースのみでコンプライアンスリスクの低減や現地業務の可視化を実行することは大変むずかしく、大きな負担になっています。

そこで本稿では、クラウドを活用した経営情報の可視化と効果的な現地経営管理の実現方法についてご紹介します。

日系企業の直面する課題

海外に進出する日系企業は、様々な経営課題に直面しています。

① ガバナンス強化

グローバル市場への展開は、地域・業務（機能）・文化・言語など、多様な環境に対応しなければなりません。昨今では、ビジネスプロセスの透明化や経営のスピード化が求められていますが、現実には多様性への対応に追われて、業務の標準化が徹底されておらず、属人的な仕事が多かったり、日本本社から会計情報を参照できず、現地の状況をタイムリーに把握することがむずかしい、といった問題が生じています。

また、可視化や業務標準化を目指してシステム化を進めても、現地の事業規模に対して「膨大なワークロード」「甚大なコスト」がかかるわりに、業務の仕組みとしての満足度が十分に得られないケースもあるようです。

② 要員強化

海外駐在員は数年で異動することが多く、現地の人材流動性は日本国内に比べ高い傾向にあります。また、駐在員は経理やITの専門家ではなく、多くは営業の専門家です。そのため、法規制・税制など国毎のリスク管理を海外拠点に任せたり、日本国内でさえ要員が不足しているなか、要員を確保し、全進出国に派遣するには限界があります。

さらに、現地の要員育成は、有能な人材を確保するために、人材マネージメントを効果的に実施しなければなりませんが、海外現地法人では日本本社に比べてリソースが不足しがちで、十分なマネージメントが行なえず、優秀な人材が他へ流れてしまうリスクも考えられます。

解決の方向性

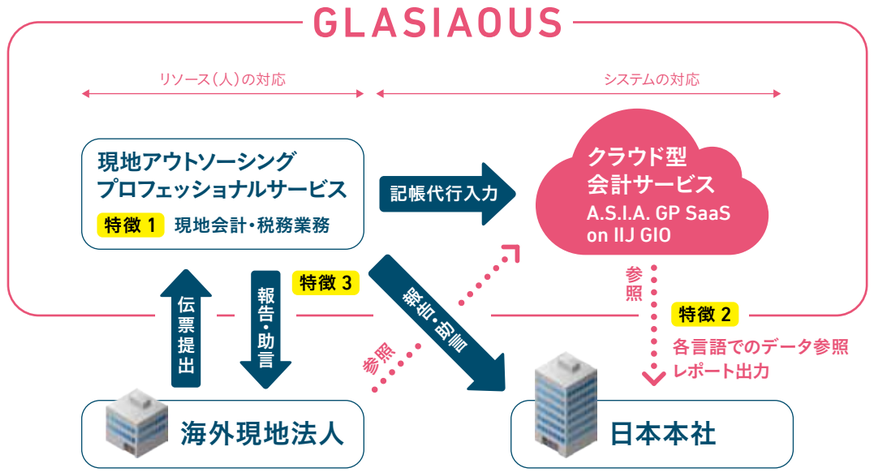
こうした課題があるなか、可視化を実現するには、次の 2 点での対応が必要です。

① システムリソース面

可視化に向けた業務システムを導入することにより、日本本社と海外拠点との情報共有が実現し、ガバナンス強化につながります。

しかし、拠点の事業規模が小さく、導入・運用に多額の IT 予算を確保できないケースや、各拠点の諸制度・言語・文化・商習慣の違いを考慮しつつシステム化していく際の困難、そして、システムを入れてもその管理要員・利用要員を確保・育成するむずかしさなど、事業規模と IT リソースのバランスをどのようにとっていくかが課題になります。同時に、海外進出時には、時間もコストも限られていることが多いため、全ての業務プロセスをシステム化するのではなく、現地の運営に欠かすことができない機能を定めて、順次拡張していくといった方法も検討する必要があるでしょう。

近年、IT のコモディティ化が進んでおり、外部調達が完全に不可能なものは限定されています。どんなに高価で高機能なシステムを導入しても、成果に直結しない「ノンコア業務」は、海外拠点においては、社外へアウトソースしたり、クラウドコンピューティングなどを活用して、コスト面と提供スピードを向上させ、可視化を実現することが重要です。



② 人的リソース面

会計税務を含む管理業務を円滑に遂行するには、有能な人材が不可欠です。会計業務には、多くの経験や知識が求められます。海外では有能な経理担当者の確保がむずかしいうえに、現地の法規制が変更・刷新されたとき、いかにその情報を適時・適切に把握・対応するかが大きな課題となります。

これらは、システム導入だけでは解決できないため、経理業務はアウトソースして、自社のリソースは本業に集中させる企業が増えています。しかし、会計業務のアウトソーシングサービスは、情報を把握できるタイミングが四半期決算時や次月末に限られるものが多く、日本本社や現地駐在員からすると、情報の可視化を行ないにくい面があります。そのため、業務要員を外部へアウトソースしながら可視化を実現でき、進出支援・リスク管理アドバイス・労務管理など進出国で発生する課題にも対応できるアウトソーシングサービスが求められています。

IIJ グローバルでは、こうした要望に応えるために、経験豊富なプロフェッショナルが迅速かつ正確に会計処理を行ない、海外現地法人の経理業務を全面的にサポートするソリューション「GLASIAOUS（グラシアス）」を提供しています。単に経理要員を提供するだけでなく、現地情報の可視化に向けたシステムもクラウドで提供しています。クラウド上に構築された会計情報基盤（システムリソース）を軸に、会計・税務業務を代行する（人的リソース）クラウド型アウトソーシングサービスです。

GLASIAOUSの3つの特徴

特徴 1：海外現地法人での記帳業務は不要。会計業務だけでなく、税務申告業務も提供

海外進出に際して、十分な準備期間がなく設立までにシステム導入が間に合わない、海外現地法人で十分な経理リソースを確保できないといったケースが増えています。そこで本サービスでは、経験豊富な会計のプロフェッショナルが海外現地法人の経理業務を全面的にサポートし、会計から税務までの全業務をワンストップで提供します。これにより、本来のコア業務へリソースを集中できます。

特徴 2：本社・本部がクラウド上の会計データを参照、多言語でレポート出力可能

処理されたデータはクラウド上の会計基盤上にセキュアに保存され、本社・本部がいつでも WEB ブラウザで参照・出力できます。多言語対応のレポーティング機能により、様々な言語で閲覧でき、財務諸表・総勘定元帳などの経理帳票や管理会計用のレポートも提供されます。これらを活用することで、連結決算の迅速化や省力化が可能となり、システム構築費や運用費を削減できます。

特徴 3：お客さまのニーズや将来の成長に対応する豊富なオプションサービス

労務管理、給与計算代行、現地支払の代行、海外現地法人と本社との会計基準の組み替え、セグメント別の会計情報管理、海外現地法人に対する会計監査や経営コンサルティングなど、お客さまのニーズに応じて様々なオプションサービスを提供しており、現地事業の変化やニーズに応じた豊富なオプションも用意しています。

今後の展開

今回は、クラウドを活用した現地経営情報の可視化と効果的な経営管理を実現するソリューション「GLASIAOUS」を紹介しました。海外事業は常に変化にさらされており、市場の変化とスピードに柔軟に対応できる経営管理を行なうことが必須です。本サービスは、2014 年 5 月から中国とタイで提供を開始し、2014 年中にシンガポール、香港、インドネシア、ベトナム、インド、ブラジル、メキシコへのエリア拡充を予定しています。IIJ グローバルでは、クラウドサービスを中心として海外現地法人のグローバル事業を強力に支援していきます。●

Internet Trivia

インターネット・トリビア

JavaScript

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

インターネット上で使われるプログラミング言語には様々なものがあります。今、WEBサイト構築において、もっとも重視されているのが、JavaScript（ジャバスクリプト）です。JavaScriptが開発されたのは1995年頃で、すでに20年近くの歴史がありますが、その間、数奇な運命を辿ってきました。今回のインターネット・トリビアでは、JavaScriptの足跡を振り返ってみたいと思います。

もともとJavaScriptは、JavaScriptという名前ではなく、このプログラミング言語を開発したNetscape Communications社では当初、LiveScriptと呼んでいました。ところが、当時Netscape社が提携していたSun Microsystems社が別のプログラミング言語、Java（ジャバ）を開発しており、LiveScriptはJavaとの親和性を打ち出すために、JavaScriptという名前に変更されたのです。

残念ながら、これが大きな禍根を残します。今でも混乱されている方が少なくないのですが、JavaとJavaScriptは全く異なるプログラミング言語です。JavaScriptは当初、ブラウザ内で動作するWEBページ用のプログラミング言語として出発しましたが、Javaは基幹業務を含めた汎用的なプログラミング言語として開発されました。両者は文法も異なり、互換性はありません。商業上の都合から似たような名前がつけられただけなのです。

出だしから波乱含みだったJavaScriptですが、世間に知られるようになってからも、あまり有効に活用されませんでした。JavaScriptはブラウザのなかで動作する簡易的なプログラミング言語のため、当初はブラウザに表示された文字や絵を多少操作する程度の機能しかありませんでした。また、その頃登場したMicrosoft社のInternet Explorerは、JavaScriptと互換性を持った JScript（ジェイスクリプト）を搭載しましたが、両者には微妙な違いがあり、それに起因する動作の不具合にプログラマは悩まされました。

そのようにJavaScriptの有効な活用が進まないなか、「ブラウザの表示を書き換える」という機能を悪用して画面表示をごまかし、誤操作を誘発させる悪質なWEBサイトが出現するようになりました。結果、「JavaScriptはメリットよりデメリットのほうが大きい」という評判が定着してしまいます。なかには「JavaScriptは無効に設定するのが当たり前」といった極端な意見すらありました。

ところが、この評価を覆すサービスが登場しました。2005年頃に公開された「Googleサジェスト」と「Googleマップ」です。

それまでのWEBサイトは「マウスでクリックすると、次のページが開く」という動作が一般的で、クリックしてから次の画面が開くまでに一瞬の間が空き、利用者にもたつきを感じさせました。しかしGoogleが作ったこれらのWEBサイトでは、いちいちページを切り替えることなくスムーズに次の情報が表示されました。この革命的な手法にJavaScriptが使われていたことが知られ、世間のJavaScriptに対する印象が一変したのです。

のちにこの手法は「Ajax（エイジャックス）」と名づけられ、Google以外のWEBサイトにも広く活用されました。その過程でJavaScriptの仕様や周辺ツールが整備され、プログラマにとって利用しやすい環境が整っていきました。

そしてJavaScriptは「ブラウザ内で使う簡易プログラミング言語」という枠を越え、サーバ上で動作するプログラムを書くために使われたり、スマートフォンのアプリ開発に使われたりするようになりました。今ではJavaScriptは、人気と実力を兼ね備えた立派なプログラミング言語として認知されています。

ここまで評価が一変したプログラミング言語というのも、珍しいのではないでしょうか。●

イラスト／山本加奈子（P22,23）

Global Trends

グローバル・トレンド

ロンドンのオフィス引っ越し事情

IIJ Europe Limited
Project Manager
田中 泰孝

ヨーロッパの人気の観光地としてロンドンを外すことはできないでしょう。また、ヨーロッパ金融市場の中心地であるロンドンでは、新たにオフィスを構える企業が後を絶ちません。今回は、ロンドンに拠点を持つ日系企業の「オフィスの引っ越し事情」についてお伝えします。

日系企業が初めてロンドンに進出する際、三ヵ月程度から契約できるレンタルオフィスを借りて小さくビジネスをスタートさせ、その後、会社の成長にあわせて、本命のオフィスに引っ越すというのがよくあるパターンのようです。この背景には、ロンドンのオフィス賃料が世界一高いという事情があり、いきなり自社でオフィスを構えるのは、よほどの大手企業でない限りむずかしいのでしょう。

ロンドンには景気動向に敏感な日系企業が多く進出しているので、景気が良くなるといっせいにオフィスを新規開設し、景気が悪化すればいっせいに撤退していきます。通常のオフィスビルは契約期間が一〇年から一五年と日本並みに長く、普段、企業の引っ越しはさほど多くありませんが、景気が変動すると日系企業の引っ越し件数が急増します。

これはロンドンに限ったことではないでしょうが、ヨーロッパで日系企業がオフィスを引っ越す際にもっとも気を配らなければならないのが、回線業者など現地ベンダとの調整です。

ベンダの対応は国によって様々で、ドイツやポーランドのように対応品質が非常に高い国もありますが、アフリカ・中東・ロシアなどでは、オーダーしても違うものが出てきたり、問い合わせに返事がないなど、一筋縄ではいきません。イギリスのベンダは、特に対応が酷いわけではありませんが、やはり日本のようにはいきません。

弊社で引っ越しをお手伝いする場合は、プロジェクトマネージャが可能な限り日本と同じピード感と正確性に近づけるように最大限努力しますが、もしもの場合に備えて、常に代替案を検討しながら引っ越しを進めることが重要です。

最後に〝こぼれ話〟を一つ。フランスやベルギーなどフランス語圏のベンダに問い合わせるときは、グーグル翻訳で「英語を話せる人がいますか?」というフランス語をあらかじめ調べてから電話をかけると、比較的取り次いでくれることが多いようです。英語がわからない担当者もいるので、取っかかりだけでもその国の言葉で話せば、「頑張っているな」と評価してくれるかもしれません。●

Information

IIJ Technical WEEK 2014のご案内

IIJグループでは11月26日～28日の3日間、技術者の方々を対象に「IIJ Technical WEEK 2014」を開催します。クラウド基盤を構成する技術のご紹介、ネットワークやセキュリティの最新事情など、幅広いセッションを予定しています。

開催概要

日　時　：2014年11月26日（水）～28日（金）　13:45～17:30（開場13:00）
会　場　：IIJグループ本社（東京都千代田区）
参 加 費：無料（予約制）
定　員　：160名（定員超過の場合は抽選となります）
締め切り：2014年11月12日（水）17:00

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

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

編集／増田倫子、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/

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（IIJ Global）
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（IIJ-EG）
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（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）
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　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

IIJ Europe Limited（IIJ-EU）
1st Floor 80 Cheapside London EC2V 6EE, U.K.
TEL：+44-0-20 7022 2700

株式会社トラストネットワークス（TN）
東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム
〒102-0071　TEL：03-5205-6490

IIJ

Internet Initiative Japan