JPNIC会員 企業紹介

「会員企業紹介」は、JPNIC会員の、興味深い事業内容・サービス・人物などを紹介するコーナーです。

株式会社ブロードバンドセキュリティ

住所：東京都新宿区西新宿8-5-1 野村不動産西新宿共同ビル4F
設立：2000年11月30日
資本金：346,500,000円
代表取締役社長：持塚 朗
URL：http://www.bbsec.co.jp/
事業内容：1. マネジメントサービス
2. セキュアメールサービス
3. セキュリティサービス
従業員数：103名　（2013年7月1日時点）

今回は株式会社ブロードバンドセキュリティを訪問しました。折りしも訪問した日の新聞一面には、大手企業や官公庁のWebサイトの改ざんと、そこに仕掛けられたウィルスにより、Webサイトを訪れただけで感染してしまうことへの注意喚起がなされていました。2013年はことさら、インターネットセキュリティに関心が集まった年ではないでしょうか。同社はJPNIC会員としては珍しい、セキュリティのサービスに特化して展開する企業です。昨今のインターネットセキュリティについての状況と、その危機に対して、どう立ち向かっていけば良いのか、お話をうかがいました。

起こって欲しくないことこそ起こるのだから、できることからやるしかない ～事故前提社会に生きるということ～

お話しいただいた方
株式会社ブロードバンドセキュリティ
代表取締役社長 持塚 朗氏

1コア、3クラウドで提供するセキュリティ ～セキュリティの普及を目指した事業内容～

貴社はセキュリティを提供されています。まずは、その事業内容について詳しく教えてください。

当社の事業は「1コア、3クラウド」から成り立っています。うち、コア部分は「システムセキュリティコンサルティング」「セキュリティ認証取得・準拠」「デジタルフォレンジック（緊急時の駆けつけサービス）」です。

クラウド部分は大きく三つの分野からなります。

一つ目の「Cloud for Assessment」は、ネットワークとサーバの現状における脆弱性診断サービスです。ツールに加えて目視検査もやっています。ペネトレーションテストなど、外から攻撃を実行してみるテストなどについては、ほぼクラウド化されています。ソースコードを入力すると、Web上で問題点を指摘できるようなものは現在開発中で、クラウド化の達成率は半分ぐらいです。

二つ目の「Cloud for MAIL」は、いわゆるセキュアメールソリューションで、ここにいる安藤が一から作ったものです。メールをクラウドで使うと言うと、みなさん頭に浮かぶのはGmailだと思いますが、Cloud for MAILは企業向けに特化したサービスとして、いろいろな仕掛けがあります。添付ファイルを外部に送る時は暗号化する、アーカイブする、また、上長の承認が無いとメール送信できないなどの機能です。その中で、最近喜ばれているのは、このサービスでアカウントハッキング検知ができることですね。去年2012年7月からこの添付ファイルに関するサービスを開始しましたが、知っている限りで、これができるのは、多分まだ当社だけです。

最後の「Cloud for Secure Management」はいわゆるSOC（Security Operation Center）です。SOCをはじめてまだ4年ということもあり、他社のサービスとの違いは、設備が比較的良く、お客様の利用コストも安いというところでしょうか。

セキュリティ事業を始めた頃、世間から「投資対効果がわからない」「効果も上がらないのに高すぎる」「いくら投資すればいいんだ」などと言われました。これではセキュリティは普及しないと、できるだけ広くサービスを使って欲しくてクラウドという形で提供することにしたのです。

3クラウドとしていますが、特定のものだけしかやらないわけではなく、マルチベンダとしていろいろなものを見ています。セキュリティ対策については、お客様のニーズに応じて、この三つに限らず追加していきます。

それぞれの事業規模の割合はどのようになっていますか。

コンサルティングや認証取得・準拠、駆けつけなどのコアサービスが約2億円の売り上げです。3クラウドの方では、「Cloud for Assessment」の診断サービスが約5億円、「Cloud for MAIL」のメールサービスが約5億円、最後の「Cloud for Secure Management」の運用支援サービスが約8億円で、合計すると約20億円の売り上げです。

SOCやメールのサービスなどについては固定客がいらっしゃると思いますが、お客様の業種はどのような感じでしょうか?

当社は、ISPやCATVのISP部門のアウトソーシング先として設立された過去があるため、元々の顧客はそういう業種が多かったです。しかし現在では、ISPやCATVのお客様もいらっしゃいますが、ほとんどが一般企業で、ありとあらゆる業種の方がいます。ゼロではありませんが、解約が少ないのが自慢の種です。長いお客様ともなると8年も利用していただいているところもあります。

最初の顧客は、ISPやCATVのISP部門が多かったとのことですね。貴社の成り立ちについて教えてください。

当社は、2006年にインターネット総合研究所（IRI）のエンジニア部門としてスタートした時点からセキュリティに着手し、それから7年が経過しました。IRIには、24時間の死活監視などをやっている株式会社インターネットシーアンドオー（ICO）、ネットワークのトランジットを販売している株式会社ブロードバンド・エクスチェンジ（BBX）という子会社がありました。IRIの事業部を含めたこの三つを一つにしたのが当社です。設立が2000年11月となっているのは、母体をBBXとしたためです。しかし現時点では、トランジット事業は2007年に株式会社NTTPCコミュニケーションズに事業を売却してもう行っていません。この売却以降は、セキリティ事業に特化しています。

● 対談の様子

開発は自社内でされているのですか?

例えば、メールサービスだと、コアのメール部分は著名なMTA（Mail Transfer Agent）であるSendmailを使っていますが、それ以外の機能の部分はすべて自社開発しています。Sendmailとはかなり深い付き合いがあります。当社で働いているメンバーには外国人エンジニアもおり、社内もグローバルです。開発会社ではないため、必要があれば外注もし、常駐して開発してもらったりもしますが、その場合も設計はすべて自社で行っています。何にしても、他社とは少し毛色の違う部分があるとは思います。

どんな情報を持ち、何を守るかを考えることが重要 ～最近の攻撃手法について～

本日も大手新聞一面でWebサイトの改ざんの話題が取り上げられていましたね。最近伸びているインシデント、それに対するサービスはどういうものでしょうか?

サービスはどれも伸びていますが、特に駆けつけサービスへのニーズが増えていると感じています。

中でも、Webが書き替えられたことが発端となるインシデントが端的に多いですね。これは発見がしやすいためと想定されます。これらのインシデントをより早く見つけだすために、当社でも非常に安くてお得な改ざん検知のサービスがあります。

また、今年で一番大きかったのは、新年明けましておめでとうメール、いわゆるグリーティングメールで起こった事件だと思います。これは大騒ぎとなりました。

これらのケースをよく見てみると、社内でマルウェアに感染していたり、CMS（Content Management System）がクラックされていたりするケースが圧倒的に多いです。SOCは効果的ではありますが、100%守れることはありません。ただ、攻撃の大半は既知ものが多いため、すべき対策さえ普通にしていれば大半は防げます。でもそれをやっていない企業が多いのが実情です。

一方、どことは言えませんが、お客様の中には、選択的に狙われているのではないかというところもあります。そのお客様が取り扱っている情報からそのように推測しているのですが、その企業に対しては、考え得る限りの攻撃が山ほど来ます。しかも、ほとんどが新規の手口で攻撃されるため、ターゲットにされると本当に大変です。当社のSOCはかなり高いレベルで防御を行っていると自負していますが、それでも攻撃されますね。攻撃側は1,000回攻撃して1回侵入できれば良いですが、守る方は1,000回とも防がなくてはなりません。1回でも入られれば終わりです。明らかに状況は圧倒的に不利ではありますが、その中で高品質のサービスを提供していかなければなりません。

攻撃を見つけたらどうするのでしょうか。しばらく泳がしておいて……ということもあるのでしょうか。

そういう意味では、すぐさま遮断して相手に悟られるような対応は取っていません。また、未知の攻撃が来た場合はわざと泳がせて様子を見ることもあります。特に標的型攻撃の場合、相手の狙いははっきりしているため、狙われるデータは絶対に取られないように切り離した仕組みを作っています。あとは、とにかく侵入をいち早く検知し、動き出したらそれを察知する、仕組みを作る以外に方法はありません。

攻撃元は特定まではできないとしても、国内からとか国外からとか、最近の傾向はあるのでしょうか?

昔は特定の国からの攻撃が多かったですが、最近は踏み台が至るところにあり、国内、国外など区別はあまりないですね。先ほどのグリーティングメールの事件では、取引先のアカウントが乗っ取られたそうですが、その盗んだデータを利用したメールの送信元はタイのサーバでした。

やはり標的型攻撃で狙われるのは個人情報を扱っている会社が多いのでしょうか?

そうとも言い切れません。例えば、とある防衛関連企業は十分な対策を採ってはいますが、とにかくしつこく攻撃されます。この場合、攻撃側も社員の名簿が欲しくてやっているわけではないですよね。

もちろん個人情報である、特にクレジットカードの情報は昔から常に狙われています。特に日本人のカードは与信額が高いので標的にされやすい傾向にあります。

怖いですね。一般のユーザーや企業はどう対策すれば良いのでしょうか?

まずはアセスメントを実施し、今、何をどこまで扱っているのかを把握することが重要です。企業レベルや情報の重要度によっても当然取り扱いは違ってきます。中には情報を取られても、Webが書き替えられても別に構わないという企業もいらっしゃるにはいらっしゃいます。しかし、個人情報、クレジット、国の機密、未発売の製品情報、そういう情報はしかるべき方法で何としても守る必要がありますよね。

人のやることや、最近のリスト攻撃など、潜在的なリスクにどう対応するか

企業におけるスマートフォンやタブレットの利用も増えていますが、最近何か動きはあるでしょうか?

スマートフォン向けの相談は増えてきており、案件が多いですね。社内で使わせるために、セキュリティをどうしたらいいかというような相談が多いでしょうか。ただ、こうした分野は、既に世の中にいくつかのソリューション、例えば紛失がわかったら電話を止める、データを消去する等がすでに提供されています。そのため、紹介や相談にはもちろん応じますが、当社として積極的に手を付けていこうという考えはあまりありません。

スマートフォンやタブレットに限りませんが、そもそも人間のやることは制御不能な部分があります。その点が一番難しいところです。

例えば、PCを紛失されたお客様がいらっしゃいました。社のポリシーでは絶対に持って帰ってはいけないことになっているとのことですが、実際には持ち帰らないと仕事が終わらないため、いけないと思いながら持って帰ってしまう。そういう意味で、人がやることは、いくら徹底しようとしてもどうしても難しい部分がある、ということです。

そういったトータルな、ソーシャルな部分まで含めたセキュリティに対する助言などはサービスとして提供していらっしゃいますか?

コンサルティングという形で、もちろんセキュリティポリシーの作成から、具体的なソリューションの提供までやっています。

当社では、PCI DSS（Payment Card Industry Data Security Standard）というクレジットカード業界の基準への準拠を評価する資格（QSAs）を会社として持っています。

このPCI DSSはカード業界における基準で、これを持たなければ、クレジットカードのデータは取り扱えないものですが、この基準への準拠が、情報セキュリティに対する具体的な実装を定量的に要求しているために、他業界からも注目されています。当社はQSAsとして基準に精通している為、お客様のご相談に、幅広く対応することが可能です。

最近の傾向として、「パスワードを90日ごとに変える」など機密性の保持ばかりに重点を置いているなど、PCI DSS自体にも不具合が出てきており、PCI DSSに沿っていれば100%ということはもちろんありませんが、ただそこも押さえておくことには十分意味があります。

ソーシャルなセキュリティ対策、ではどういうことを重点的に見られていますか?

当社だけではないですが、顧客向けにメール訓練のサービスを行っており、お客様から好評を得ています。具体的にはテスト用の偽装ウィルスメールを送っての開封率調査です。この調査では、開封率がゼロの会社はどこにもなく、当社のデータだと2割ぐらいが開封してしまっているでしょうか。これも何回か訓練をしていると下がってはきますが、決してゼロにはならないんですね。中には「うちは開封率が低かったから合格点だ」と考えられるお客様もいらっしゃるのですが、「防御」という意味だと、1人でも開封する人がいたらダメなんですね。

具体的に、訓練はどういう風に実施しているのでしょうか?

基本的に2回で1セットで、1回目は抜き打ちで実施、その結果を基にレクチャーして1ヶ月後に2回目を実施しています。基本的には2回目の開封率は下がるところが大半ですが、中には開封率が上がったところがありました。開封率を上げるように、2回目は巧妙なものにしたのですが、ただ、上がったのは初めてのケースだったので驚いた覚えがあります。

最近では、2回で終わらず定期的にやって欲しいと言われることも増えてきています。四半期ごとにやってくれなど、避難訓練と同じ扱いになってきていますね。訓練の予算の出所も、必ずしもIT部門ではなく、総務、監査、内部統制等が行うケースも増えてきています。

メールのサブジェクトはどんなものにしているのでしょう?

そこにはいろいろノウハウがありますね。普通ならこれ、レベルを上げた場合はこれ、というように。

某TV局の「ほこ×たて」ではありませんが、成りすましは、メールサービスの大きな課題です。すり抜けようとするメールをどうやって見分けるか、という話で、ある意味、セキュリティの両輪と言ってもいいのかもしれません。

クラウドを使うとそういう部分を可視化できるというところがありますね。常にチェックしているので、判断がつかなくとも「怪しい」ということがわかります。いつもと何かが違うメールの場合は、警告を出してあげることもできます。例えば、Facebookなどで見かけるソーシャルグラフがありますが、実はメールでも同じようにグラフを書けます。いきなり変なところからメールがきたら、同じ仕組みで警告が出せます。

現在、正規のIDとパスワードのリストを盗んで攻撃を行う、いわゆる「リスト攻撃」についてもよく取りざたされていますが、こちらはどのような状況でしょうか?

ご相談は多数いただいているのですが、本当の意味で有効な対策は無いですね。アカウントとパスワードのリストが流通していて、複数のサービスで同じ組み合わせを利用していることから攻撃に使われるわけですが、システム的には、正規のIDとパスワードでアクセスしてくるのですから、いくら守ろうとしていても防ぎようがないのです。今のところ有効な手立ては「パスワードを変える」方法しかありません。強い認証の仕組みを前段階に入れることも可能ですが、膨大な投資が必要になります。この攻撃のやっかいなところは、侵入されてしまっている、つまりリストが漏れている状態でも、悪者がアクセスしてくるまではそれがわからないというところです。

まだ被害が出ていなくても、リストが存在し、本人以外からアクセスされる可能性があることに潜在的なリスクがあります。当人が被害を被らないためにはどうすればいいのかを考える必要があります。

どの程度の被害がありますか?

2013年7月からやっているメールサービスでのストップ対策では、1ヶ月あたりアカウント総数の0.5%ずつぐらいが被害にあっている感じでしょうか。

アカウント自体が盗まれているのかどうかはわかりませんが、悪用されている数がその数であるため、盗まれているのはもっと多いのかもしれません。目的があって盗んだアカウントを使っているわけですから、必要以上に使ったりはしないはずです。ですから、潜在的なリスクはもっと大きいと言えますね。そういう状況が毎月続いています。放置すればどんどん増えていきます。本当に怖いですよ。

新サービス「モダンマルウェア検知サービス（MARS）」の提供開始 ～サブタイトル～

こうした時期に、新規サービスとしてはどういうものを考えていますか?

今はマルウェア対策としてサンドボックス型が流行っていますが、これはマルウェア侵入時に、箱の中で動かし、挙動を見て通過させるかしないかを判断するものです。この方法は、マルウェアが動作するまでに時間がかかり、リアルタイムに状況が見られないため、エンドユーザーからの評判はそこまでよくありません。

これらに変わる次世代のサンドボックスとして、当社ではマルウェアをクラウドに投げ、そこで調べて止めるか否かを判断するサービスを、米国のLastline社と業務提携し、日本で「モダンマルウェア検知サービス（MARS：Malware Analysis & Research Service）」として提供し始めました。コードインスペクションを行うため、たとえ中で条件分岐していても、変なコードが入っていればきちんと見つけることができます。

従来Lastline社が提供していたサービスは、マルウェアの投げ先が米国となっていました。しかし、これでは電話で詳細を聞きたくても、対応が米国側になり使いづらく、かつ国内の重要な情報を海外に送付することを嫌う日本人の傾向から、本サービスでは、当社の国内クラウドを使って行うことになりました。

設備はどちらが持つのでしょうか?データは日本から出さないということになりますか?

クラウド設備も当社で持ち、エンジンについては同期を取っています。データはLastline社には開示しません。そこがネックになってLastline社のサービスを利用できない企業もいらっしゃいますから。しかし調べ終わったら、検体は全部提出します。

Lastline社は、Christopher Kruegel氏をはじめとした、カリフォルニア大学サンタバーバラ校の先生達が立ち上げた企業で、米国ではセキュリティにおいてかなり有名です。そういうところと業務提携して最新の技術を吸収しようと考えました。

これ以外の新しいビジネスの展開も考えていらっしゃるのでしょうか?

セキュリティ関連のサービスは、我々としては価格以上の価値があると思っていますが、廉価なサービスを望む顧客とそれに答える提供側の存在により、セキュリティ市場全体の相場は比較的安く留まっています。しかしながら、それなりのサービスを提供するためには、ある程度のコストがかかることは避けられず、そういった低価格帯のサービスには言わゆる「安かろう悪かろう」というものも少なくありません。単に低価格にすることのみにとらわれてそういう価格帯で戦ってしまうと、良いサービスは提供できないのです。

その解決方法の一つが、「規模を大きくしてコストを下げる」という方法です。いろいろ仕掛けをして、安く使える環境をさらに提供していこうと考えています。

IPv6への対応状況

話は変わりますが、IPv6の利用にあたって何か気になる点や問題点はありますでしょうか?

今のところ特に問題は感じていませんね。IPv6の方がIPv4より遅いとか、経路が複雑などの意見はありますが、大きな問題は無いと思います。

当社でも、お客様からの要望でIPv6への対応を順次進めていますし、自社のことで言うと、かなり初期から取り組んでいる方だと思います。ネットワークエンジニアが多い会社だったので、機敏に反応して準備を行いました。特に、アプリケーション側で対応しないとどうしようもないものについては当社社内では何も

できませんが、例えばメールのケースでいえば、Sendmailに再三リクエストを行い、IPv6への対応を促進させるなど、IPv6への普及に陰ながら貢献していると自負しています。

IPv6が、サービスに特に影響しているということはありますか?

IPv6は防御が少し弱めといった側面はありますが、顕在化はしていないですね。しかしそれは規格の問題ではなく、IPv6のアドレス空間がIPv4と違って広すぎるために起こることです。これは、あくまでIPv4の時と比較すると弱いということで、それ以外はほぼIPv4に追いついていると思います。

怪しいアドレスを見つけた時、IPv6アドレスだと警告の振る舞いは変わってきたりしますか?

変わってきますね。IPv4と同じ精度での特定は、現状では難しい状況です。「ドメインレピュテーションにしよう」という話もあるのですが、これはこれで多くの課題をかかえています。

IPv6の利用は増えてきている感じを受けますか?JPNICが、例えば教育などの観点で何かできることはありますか?

DNSをサービスしている立場からみると、IPv6のクエリは確かに増えており、徐々に利用者が拡大していることが想定されます。

最初はIPv6も大騒ぎでしたが、今は落ち着いた感じです。これ以上の普及については、待つしか無いのかな、と感じています。IPv4も在庫が枯渇したとは言え、今はまだ/25ぐらいのブロックでISPからもらうことができます。これがもう少し経つとどう変わってくるのかが今後の関心事ですね。ヨーロッパや中国など、一足先にIPv6に大幅に舵を切ったところもありますが、今後どうなっていくのだろうということもウォッチしています。

事故前提で、そして初動をきちんとする ～今後のインターネットと向き合うには～

これからのインターネットはどうなると思いますか?

インターネットで一番顕著なのは、国の枠が無いことです。ある国から別の国に動かした瞬間に法制度が変わります。日本では意識されていませんが、ヨーロッパでは大問題になっていますし、こういう部分が社会に影響を与えていくのではないでしょうか。

国によってインターネットの捉え方が違うのは、確かに大きな問題ですね。

例えば中国では、Facebook等は普通には使えませんが、VPNを使ったり、スマホでテザリングすれば書き込めます。つまり、簡単にはできませんが、やろうと思えばできる状態にあるわけです。

国家に限りませんが、情報を力で制限して……というのは長続きしないのではないでしょうか。いくら制限しても情報を見たい人には見られます。民族も多民族、そういう中でいつまでも力だけでは抑制できずに、そのうち国家制度も変わるのではないかと思います。

米国のNSA（国家安全保障局）がインターネットを監視して……という話もありましたね。

そういう仕組みが無くなると、国が維持できなくなるのかもしれません。NSAはそもそもの暗号アルゴリズムを制定していますから、あずかり知らないところで我々のメールも解読されている可能性もあるわけですしね。

しかし別の観点で言えば、日本はどっち付かずの対応しかしておらず、一番まずいパターンと言えるのかもしれません。

これから脅威が増す中で、日本は何をどうすべきなのでしょうか?

地道なことにはなりますが、できるところからやっていくしかないと思います。あとは心構えでしょうか。「起こって欲しくないものこそ、むしろ必ず起こる」と考えないといけないのではないでしょうか。これはお客様に必ずお伝えすることです。「事故前提社会ですよ」と。

またセキュリティに限らず、初動が一番重要です。それによって影響を最小限にすることが必要です。初動が遅れると傷が大きくなるし、下手をすれば致命傷にもなります。セキュリティで言えば、感染して悪さをし出すとわかるので、いかに早く見つけて対応するかということです。

英国でバーチャルホストサービスを提供している企業が攻撃され、11万件の顧客の情報が盗まれ、次の日に社長が自殺した事件がありました。日本でも、サイトクローズやサービスを止めたという話は山ほどあります。そういったインシデントの影響を最小限に防ぐためには、見つける仕組み、仕掛けを持っていないとダメなんです。どんなサービスにも言えることですが、ツールを入れてそれで解決ということはありません。そこからが始まりで、毎日いろいろなチェックをし続けることが求められます。ある意味、ヘルスモニタリングです。アカウントハックの検知も自動的ですが、チェックし続けています。「どれだけ準備するか、そしてそれが使えるか」が肝です。

貴社にとってのインターネットとは、何でしょうか?

公的な立場としてはビジネスですね。一方で、インターネットなんて25年前にはなかった。そういう意味では今しかない実験環境なのかなとも思います。まだ手探りでいろいろなところが進んでいる状況であります。

リアル世界で起こるのと同じようなことが、インターネットでも起こるようになってきています。世の中から警察や警備会社が無くならないのと同じで、セキュリティ事業にも同じようなところがあるのかもしれないとは思います。

リスト攻撃にしても、銀行などで問題が起こるたびに2段階の認証にして……と、セキュリティを強化していますが、強化しても強化しても破られているのが現実です。一体どこまでいくんだと思います。指紋認証でさえ、その気になれば指紋の入手は可能なわけで安心はできません。本当にキリがありません。

もちろん、将来的にこうした脅威が解決される可能性もあります。その方が世の中的には良いことでしょう。そうなった時は、当社も社名を変えることになるのでしょうね（笑）。