

対談

昨年来、標的型サイバー攻撃が相次いでいる。この脅威に、地域の行政や企業はどのように対処したらいいのか。福岡県の対策と課題を中心に、IT企業出身の神崎聰福岡県議会議員とセキュリティの専門家として活躍するトレンドマイクロの大久保修一福岡営業所長に語つてもらつた。

「地域のセキュリティを強化

福岡県で新雇用の創出へ

地域のBCPは 電力確保が大前提

—神崎議員は地場IT企業の出身として福岡県のICT政策に積極的に取り組んでおられます。

神崎 私は以前、麻生グループの麻生情報システムで金融や流通など民間企業のIT化を進め、その後、筑豊管内の小・中学校の情報教育を行いながら、経済産業省「教育の情報化推進事業」で全国で初めてとなる教師による情報教育の実証実験に取り組みました。また地域の防災や福祉サービスを拡

います。

大久保

昨年9月、弊社などのIT企業

が協力して全国各県のCIO（最高情報責任者）が集う「都道府県CIOフォーラム」が熊本市で開かれたのですが、会場では東日本大震災で実際に被災された自治体の方の発言が注目されました。そこで実際にBCP

が役立つたかといいますと、庁舎や家屋が流されるなど想定外の震災ですから、とてもそんなレベルの対応はできませんでした。まず電話が使えず職員に連絡がつかない。こういった職員の安否確認という初動の段階からつた経験から、BCPを

福岡県議会議員

神崎 聰氏



●こうざき さとし 1962年9月20日生まれ 福岡県出身

日本大商学部卒業後、麻生セメント入社。同社の情報部門が独立して設立された麻生情報システムへ。取締役を経て2003年社長。福岡県情報サービス産業協会理事をはじめ教育や地域づくりにさまざまな公職を務め、11年4月福岡県議会議員に2度目の挑戦で初当選。三井物産戦略研究所傘下のOSACで理事を務めたこともある。

充するための情報ネットワークの導入をお手伝いする一方で、グループの麻生飯塚病院の医療情報システムを全国へ横展開。国や県のIT戦略にも積極的に関わってきました。

このようにさまざまな分野のIT化に携わつてきましたが、実はIT産業というのは、安定した電力供給を大前提として成り立つてゐる産業なんです。電力の供給体制は今まで主に国や電力会社が決めてきましたが、震災以降に電力不足という難しい状況に陥つたことを考えれば、県として電力の地産地消というか分散化、多様化に取り組むべきではないかと思います。これは他の産業も同じでしょう。ライフル線を中心にしてどのような地域のBCP（事業継続計画）を作り、いざといふ事態の発生時に地域で素早く対応できる体制を築くことは、とても大切なことだと思います。

トレンドマイクロ 福岡営業所長 大久保 修一氏



●おおくぼ しゅういち 1972年3月26日生まれ 奈良県出身
大阪国際大経営情報学部卒業後、パソコン関連機器メーカー入社。
システムインテグレータを経て、2001年トレンドマイクロへ転身。大阪
営業所で大手企業向けの営業組織を創設、その後、本社で戦略製品や
SaaS関連のビジネス開発、新卒と中途の人材採用業務などを手掛け
る。09年から九州・沖縄エリアを営業管轄とする福岡営業所へ赴任。

になつたと聞いています。

神崎 5年ほど前だつたか総務省が「地域情報プラットホーム」を提唱しました。当時各自治体には業務ごとのシステムがばらばらに入つていたので、業務の標準化と基盤の共通化を試みましたが、スキル不足とコスト高で、なかなか進みませんでした。

そういう中で災害が発生し、自前でしかシステムやデータが持てず、全て流されてしまつた。これを早く整備して仕組みを作つていけば、電算システムの共同化によるコスト削減や安全性の確保ができるし、セキュリティも担保できるはずです。1つの自治体がICTについて何もかも抱え込むのは、やはり無理がかかります。

巧みな持続的標的型攻撃 セキュリティ対策に課題

— こうしたBCPを通じた危機管理で最も危惧されるのが、昨年来相次いで起きた標的型サイバー攻撃ですね。

事態が深刻なので政府も対策に乗り出しています。

今年2月には九州経済産業局が福岡県で情報セキュリティセミナーを開催しました。100人を超える来場者からのアンケート結果では、「今後必要なセキュリティ対策」の項目で「サイバー攻撃対策」が最優先となつており、来場者の関心の高さが伺えました。弊社としても強く注意喚起や具体的な対策提案を広く進めているところです。

大久保 自治体クラウドの開発にはさまざまな乗り越えるべき壁や初期投資もありました。乗り越えられるのが持続的標的型攻撃といわれるものです。

今回は、国内の防衛産業をはじめ省庁や国会議員などがターゲットになりました。メールを開封した相手のパソコンにOSやアプリケーションの脆弱性があつた場合、添付ファイルに仕込まれたウイルスに感染してキー入力を�いた情報が漏れたり、サーバーを攻撃して管理者権限を乗っ取つたりと、時間をかけながら周到に進められます。ハッカーは攻撃対象で使われているセキュリティソフトも事前検証した上で、それをすり抜けるようウイルスを作つて、関係者に成り済ました上で個別に送信するなど、巧みに攻撃してきます。ですから、攻撃されたという事実や被害に気付きにくい。さらにネットワーク内部に侵入したウイルスは外部の攻撃者と通信を行いながら、攻撃を加え続けるなどの特徴もあります（注1）。いくら注意を喚起しても、上司や同僚などの関係者からのメールであれば、どうしても開いてしまうのが現実ではな

いでしょう。

大久保 標的型サイバー攻撃は、個人情報や技術情報、機密情報を盗むために、特定の企業や組織に対し行われます。対象を入れ念に調査し、目的を達成するまで執拗に

—2月の福岡県の定例議会でもサイバーアクションに対するセキュリティ対策について、神崎議員はさもざまな質問をされました。

監議員はわざわざな質問をされました。

神崎 そこでは、国や企業をターゲットにした最近のサイバー攻撃に対する福岡県の対応を取り上げました。それまで議会でつっこんだ話が出なかつたからです。

てセキュリティ・チェックは行っているものの、全てのファイルへの暗号化や、それが確実に行われている保証があるのかどうかは、はなはだ疑問です。ここでは、外部への感染や情報の流出を防ぐための出口対策も必要との見葉を引き出し、予算に計上する旨の答弁を得ています。

入り口だけでなく
出口も防ぐ

大久保

暗号化についてのお詫びが出来ました

受け、顧客1493人分の個人情報が外部に流出して
います。

福岡県は2002年3月に

「福岡県情報セキュリティ基本方針」を定めており、そのセキュリティ政策として外部に委託して情報システムの異常を監視、外部のネットワークから庁内の情報システムに直接アクセスできないようにするとともに不正なプログラムを除去す

答弁がありました。最新のウイルス対策ソフトの導入を図ると
いった対策を施していると、小川洋知事から



そこで、弊社では、業務システムに影響の出ない隔離された領域で、不正なアプリケーションによる通信を分析し、不審なメールも開いて確認、安全を担保した上で戻すという

そこで、弊社では、業務システムに影響の出ない隔離された領域で、不正なアプリケーションによる通信を分析し、不審なメールも開いて確認、安全を担保した上で戻すというソリューションを持つています。弊社は情報セキュリティの専門会社として「サイバー攻撃

神崎 サイバー攻撃対策が間に合っていないことを、県はもっと認識すべきだと思いま
すね。

私は医療機関についても先の議会で質問しました。医療機関は一般的にはシステムがオフラインなのでサイバー攻撃に対しても大丈夫とかいわれてきましたが、実際は医師などが自宅にデータをUSBメモリーで持ち帰つてそこで感染するケースがあると聞きます。これは教育や研修が必要です。今後、病院連携や福祉・介護関連施設の連携などが増えていきます。この情報システム連携についてもセキュリティ対策が必ず必要です。特に医療機関はたくさんの個人情報を持っていますので、しっかりと安全を担保しないと皆さんが安心して利用できなくなります。

大久保 弊社でも、病院の情報システムに大規模感染があり助けてほしいという依頼が相次いでいます。原因のほとんどがUSBメモリー

「診断サービス」を提供する豊富な解決ノウハウを持つています。

メモリーです。システムを医療業務ごとに導入していくので、セキュリティ対策がばらばら

キュリティを担保していく意識も今後必要になつてきそうです。

うぶ、流一ぶれていませ。感染が明うかこな

らで統一されていなかった。環境が明らかになつたて急にあわてる例が多いようで初めて事態の深刻さが理解されますが、普段情報システムの安全管理が議論されることはありません。どうしても必要な場合、弊社ではウ

イルスを駆除する機能があるUSBメモリーの使用を勧めています。あと、ほかのケースもあります。病院の待合室によくある電子掲示板です。この中ではウインドウズが動いていますので、院内ネットワークを介してウイルスに感染していた例がありました。ですから、オフラインだから大丈夫というのではなく物です。

医療・教育機関でも
不可欠なセキュリティ対策

神崎 参入の是非が政治問題となつていて、TPPについてですが、医療情報、個人情報において懸念されている問題があります。今後とも注視すべきは、日本の医療市場に参入してくる保険会社などに、医療を含めた

個人情報が集まることになり、万が一ここにサイバー攻撃があるとどうなるでしょう。例えばサイバー攻撃を受けたのが米国企業の場合、パトリオット法によつて大統領が直接情報の開示を求めることができるのです。

大久保 国内だけでなく国外を経て個人情報や機密情報が漏れていかないように、セ

神崎 ところで警察庁では、今回の攻撃を国際的な「サイバーテロ」と位置づけており、米国国土安全保障省による国際的なサイバー攻撃対処演習「サイバーストームIII」にも参加しています。

福岡県の教育機関では昨年1年間で情報漏えいが9件ありました。教職員に対してセキュリティ意識をさらに身につける研修が必要だと思います。福岡県はそのためのルール作りや意識向上のための研修を行い、デジタル情報の校外への持ち出し規制も行つているようですが、教職員が学校の中で公務をすべて終えることがなかなか難しいという現実もあり、どうしても自

宅にデータを持ち帰ることになる。ですから、学校でも自宅でもクラウドサーバーの中で公務がすべて完結できるような教育現場のクラウド化を提



た質問は出なかつたと思ひます。提言をしていくことが、予算もいい啓発になると思ひます。デフコンと言われる世界一祭典を毎年ラスベガスで開催。リバーアクセスで開催が人材として採用していまるや民族性には馴染めないハッスを防ぐ知識や技術を競う月に国内で初めて不正アクセスを防ぐ知識や技術を競う大会「Capture The Flag」(CTF) が九州工業大学情報工学部の飯塚キャンパスで開催されました。また、CTFの全国大会も2年内に開催される予定だと聞いています。

大久保 今年2月に佐賀県教育委員会では、36の県立高校の全生徒にタブレット端末を配布する方針を固めました。こういったタブレット化への取り組みは全国的にも九州が進んでいるようを感じます。IT環境が変わることでセキュリティのアプローチも変わります。

なります。福岡県は先端技術や情報産業の育成に取り組んできただけに、その強みをもつと生かして人材を開発していくば、他の産業にも波及していくのではないかと考えます。この新産業の創出が非常に大事で、これはつまり雇用なんです。産業が空洞化しないためには地域の差別化戦略が必要になつてくるので、私は福岡県はクラウドや情報セキュリティ

に特化した先進県を目指すべきだと考えています。

もう一つは人材の活用という課題もあります。これが実はなかなかうまく行つていらないようで、官民により人材育成はできるのですが、その後に実際どう活用していくのかが、定まっています。

先ほどお話しした福岡県の差別化という意味でも、企業でもどんどんスキルを高めた人材を受け入れていただきたいと願っています。

大久保

警察や学校のお話が出ましたが、弊社も

そちらの教育や研修に実際携わっております

し、国や政府とも深く連携を取っています。

私たちがいるソフトウェア業界は知的労働産業ですから、やはり人ですね。資源があるないも関係なく、住んでいる場所も関係ない。

神崎

ナレッジワーカーを増やして九州を活性化していくことで人や情報を集積していくば、国内どころか世界からもビジネスが集まつくる可能性だつてあります。

データセンターの誘致については、

九州の中⼩企業はセキュリティへの認

識が不十分という指摘があります。特に経営者が優先的に投資しないというのが現実

にはあるようです。



データセンターは 過疎地域が適地

福岡市や北九州市といった目立った大都市ではなく地方、特に私の地元の田川のような中山間地域もいいのではないか。

攻撃されて初めてことの重大さに気づくようです。前にいくつか例が出たように、被害の拡大は顧客や取引先にまで及びます。それこそ「想定外でした」では済ませませんから、当然経営責任が問われます。確かにセキュリティにある程度の投資がかかりますが、それを怠ると経営者としての姿勢が疑われかねません。関係先に対する安全性、信頼性、事業継続性を高めるためにも、むしろ商売の強みにするくらいであつて、いいのではないでしょ

うか。これから企業は、徹底したセキュリティ対策が備わっているかどうか、そういう厳しい目で周囲からも見られると思います。マスコミの論調も、情報漏えいに厳しい目で周囲からも見られると思います。

大久保

関しては非常に風当たりが厳しいです。事業継続性やコスト削減の追求を背景に、サーバやデータの保管を外部に委託したとしても、

情報のオーナーシップは自らにあることを自覚し、自らデータの安全性を確保するための対策を打つことが大切です。まずは、現状の可視化から始めましょう。

— 本日はありがとうございました。

トレンドマイクロのサイバー攻撃対応サイト

■サイバー攻撃対策の無料診断

<http://satool.trendmicro.co.jp/>

■サイバー攻撃緊急相談窓口

jp-fukuoka@trendmicro.co.jp