

SMB Cグループで蓄えた知見を生かし 企業のホームページやPCを守る!!

1972年に設立したさくら情報システム(株)(東京都港区)はSMB Cグループに属し、(株)三井住友銀行やグループ各社の基幹システム構築・運用業務に携わりつづけているシステムインテグレーターだ。現在はグループの枠を越え、より幅広い層の顧客に先進的なシステム・サービスを提供している。その特色や強み、そしてサイバーセキュリティに関する取り組みについて、同社のセキュリティ部に聞いてみた。

金融機関の基幹システムの構築・運用で得た知見を活用

——まずは御社の概要から伺いたいと思います。

さくら情報システム(株)は1972年の設立以降、(株)三井住友銀行をはじめとしたSMB Cグループ各社の基幹システムの構築・運用に携わってきました。おかげで、システムの構築・運用スキルはもちろん、品質管理やプロジェクトマネジメントのレベルにおいても、一日の長があると自負しています。また、SMB Cグループということもあり、金融機関の顧客が多いと思われがちですが、実は銀行からの紹介を通じて、大企業から中小企業まで幅広い層の業種・規模のお客さまにシステムやサービスを提供しています。——昨今はどういったニーズが多いのでしょうか。

やはりDXをいかに推進すればよいか、という相談が増えています。それに大企業ばかりではなく、中小企業からの相談も相ついでにいます。問題は中小企業の場合です。信用取引などの慣行商売が多く、DXの予算を十分に確保するのは難しく、思うようにDXをすすめるられないでいるのが現状です。そこで、さくら情報システムでは中小企業のDXを支援するためにIT企画伴走支援サービス「絆」を立ち上げました。通常、さくら情報システムでDXを支援する場合、SE(システムエンジニア)を1カ月当たり100万〜200万円の予算で派遣するのが一般的なのですが、それでは中小企業にとって敷居が高すぎます。そこで、絆では1時間単位の派遣と伴走型支援を可能にし、できるだけ短時間で顧客の課題を抽出し、アイデアやソリ

ユーザの提案できるようにしたのです。いざサービスを開始してみると思いのほか、人手不足に悩む大企業の情報システム部門からの問い合わせが多くて驚きましたが、引きつづき企業の大小を問わず、柔軟な伴走支援を展開していければと考えています。

——サイバーセキュリティにも強みがあるのでしょうか。

さくら情報システムではサイバーセキュリティに関しても、これまでの知見を生かしたサービスを数多く提供しています。具体的にはAIを活用したホームページ脆弱性診断サービスがそのひとつです。これは最近、力を入れているサービスで、1分間に1000回程度アクセスしてみるなど、100以上の検査項目を経て、ホームページのプログラムやサーバーの設定のなかにあるバグ(欠陥や不具合

など)を発見し、対策などとお知らせするというものです。

——ホームページに脆弱性があると、どのようなリスクがあるのでしょうか。

今や企業の「顔」であるホームページはサイバー攻撃の対象になることが多いうえに、企業のホームページが改ざんされたり、ホームページ経由でウイルスに侵入されたりすると、企業そのものの信頼が大きく損なわれてしまいます。また、ホームページ上でEC(電子商取引)を展開している場合は、信頼が損なわれるだけでなく、顧客情報などが流出してしまう恐れもあります。

——どのようにして侵入される可能性があるのでしょうか。

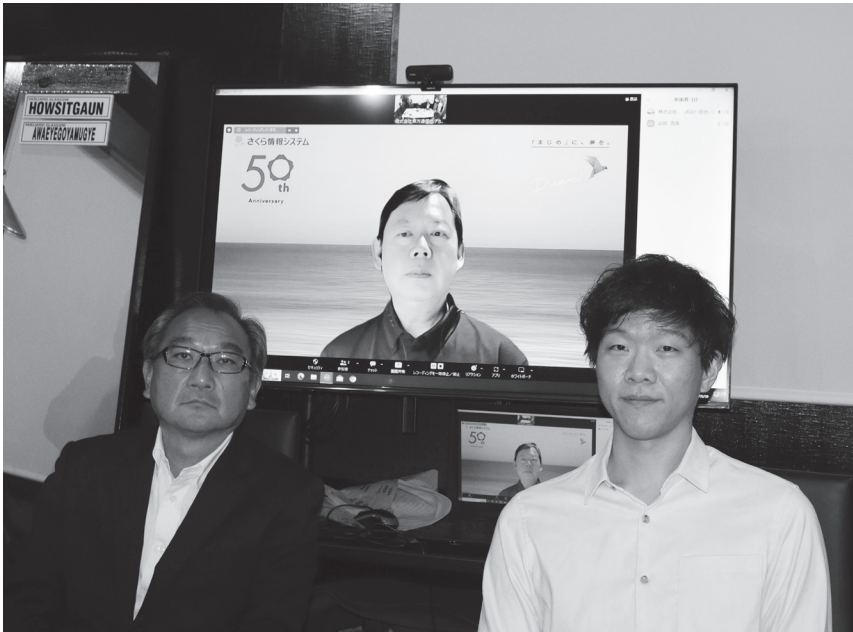
たとえば、管理パスワードを設定し忘れていたり、侵入者みずからパスワードを設定し、

簡単に侵入されてしまいます。こうしたリスクを軽減するには脆弱性やバグなどをできるだけ早く発見し、プログラムや設定を改善しなければなりません。

——プロが制作したものであっても、そういった脆弱性やバグは発生してしまうのでしょうか。制作側でもダブルチェックなどさまざまな対策を講じていると思いますが、やはり人の手によるものにはどうしてもミスがつきものです。また、プログラムや設定の複雑な組み合わせによって思いがけない脆弱性やバグが発生してしまうこともあり、もともととは万全なシステムや設定であってもサイバー攻撃の手の進化によって脆弱性やバグが見出されてしまうこともあります。だからこそ、定期的に最新の脆弱性診断を実施し、今の時代に即したプログラムや設定になっているかをチェックする必要があります。

——この脆弱性診断では、AIを活用しているそうですが、どのような特徴がありますか。

従来の脆弱性診断だと、かなりの人手と工数が必要になるため、費用が数百万円ほどかかっていました。しかし、それでは中小企業が気軽に、定期的に診断を受けることができません。そこで、AIを活用して工程の



左からさくら情報システム(株)プラットフォーム事業本部営業部シニアアドバイザーの塚田 筒逸氏、同本部セキュリティソリューション部セキュリティサービスグループの山田 克英氏、同グループ4チームリーダーの榎垣 貴良氏の3人が編集部のインタビューに答えてくれた

一部を自動化することによって、費用を40万円程度に抑えることにしたのです。ちなみに、診断可能な画面数は一律で5000画面以内となっていますが、通常のホームページは10000、2000画面程度で収まり、多い場合でも20000、3000画面程度なので、十分に範囲内に収まると思います。また、この脆弱性診断では報告書とあわせて、ホームページの

構成を示した画面遷移図も提供するようにしているのですが、案外と自社のホームページの全体像を把握されている方が少ないようで、多くのお客さまに喜んでいただいています。

——どういった業種からの問い合わせが増えていきますか。

中小企業はもちろん、4年ほど前に金融庁が「信用金庫のホームページ脆弱性診断が遅れている」と指摘したこともあり、

全国の信用金庫から多くの問い合わせを頂戴しています。とはいえ、まだまだ認知度が不足しており、さくら情報システムの全体の売り上げが年間約202億円であるのに対し、ホームページ脆弱性診断サービスの売り上げは1割程度にとどまっています。引きつづき脆弱性診断の重要性を訴求しながら、顧客拡大に努めていきたいと思っています。

——スマートフォン向けの脆弱性診断サービスなども実施されているのですか。

スマートフォンに関しては、スマホアプリがウイルスなどの侵入経路になるケースが多いため、アプリに特化した脆弱性診断サービスを展開しています。安全性に配慮しているアプリ制作会社などからの問い合わせが着実に増えてきている段階です。

「HP SCE」も導入し 万全の体制で DXに臨んでほしい

——そうしたなかで、HP社の「HP Sure Click Enterprise (HP SCE)」の販売にも力を入れているそうですね。

5、6年前にセミナーでこのツールを知って感銘を受け、ほどなくして総代理店の(株)ブロード(東京都千代田区)の

もとに足を運び、一緒に販路拡大に取り組みことにしました。

——HP SCEのどのような点に感銘を受けたのですか。

すでにレガシーともいえる仮想化技術に着目し、「マイクロVM(仮想パソコン)を介してメールやインターネットなど外部から受け取るファイルのすべてを安全に開けるようにする」という発想は非常に画期的でしたし、ツール自体も実用性が高く、唯一無二のものと感じました。

——今後の方針についてお聞かせください。

脆弱性診断サービスについても、HP SCEについても、正直、まだまだ知名度が足りていないと感じています。ただ、今や中小企業にとっても「情報はとても重要な資産であり、セキュリティ対策は待たなしの状況です。「会社の顔」であるホームページを守りつつ、社員の必需品であるPCを守る」というスタンスが多くの企業で定着するよう、情報発信などに注力していきたいと思っています。

——全国各地の中小企業が健全にDXをすすめるられるよう、これから素晴らしいサービスやツールを提供しつづけてください。

もう無駄な時間と費用は「0」にしましょう

hp HP Sure Click Enterprise

おかげさまで Bromium は HP Sure Click Enterprise に進化しました

POWERED BY **Br Bromium**

エンドポイントのサイバー対策に関する費用や専門家は、もう必要ありません。
100%* 防御し、レポートします。是非ブロードにお問い合わせください。

*2013年以降、Bromiumは推計20億以上のMicroVMが実行されましたが、侵害報告件数はゼロです。(Bromium社調べ)

詳細は [BROAD Security Square] で … <https://bs-square.jp/columbus>

株式会社ブロード

〒100-0014 東京都千代田区永田町1-11-30 サウスビル永田町7F
TEL: 03-6205-7463 (代表)

