サイバーセキュリティ最前線

「RidgeBot」などのツールを適切に利用しウェブサイトやアプリの脆弱性を克服!!

AI/DXコンサルティング、サイバーセキュリティ対策、CRM&デジタルマーケティングなどを手掛けるアイティーディレクト㈱。同社の佐藤昌弘社長はネット銀行の取締役CIO情報システム統括責任者を務めた経験などを生かし、マクロな視点でハイレベルなセキュリティコンサルティングを実践している。さっそく、昨今のセキュリティに関する課題や同社の取り組みについて語ってもらった。

佐藤昌弘 さとう・まさひろ

アイティーディレクト株式会社 代表取締役

1970年生まれ。94年に大手ゼネコンの㈱竹中工務店に入社し、2000年にネット銀行の設立準備会社に転職。同銀行の取締役CIO情報システム統括責任者などを経て、09年にアイティーディレクト㈱を起業。以来、主に金融機関を中心に、要件定義からシステムの開発、プロジェクトの計画立案と推進管理、品質管理、保守運用、サイバーセキュリティ対策や金融犯罪対策などの幅広い業務をサポートしている。

大手ゼネコン、ネット銀行を経てDXコンサル会社を起業

アイティーディレクト㈱を立ち上げる前に大手ゼネコンやネット銀行に在職していたそうですね。

佐藤昌弘・アイティーディレクト代表取締役　学生時代に「何か大きなものをつくりたい」と思うようになり、まずはゼネコンに就職しました。情報部門はもちろん、現場の管理にも携わらせてもらったおかげで、組織を安全・安心にマネジメントすることの難しさを肌で感じることができましたし、多くの関係者を束ねるノウハウを身につけられたように思います。このノウハウはネット銀行で働いたときにも生かすことができました。ネット銀行には設立準備会社の頃から携わり、建物もシステムも規模が大きくなればなるほど、多くの人手が必要になり、マネジメントが重要になることを学びました。

ネット銀行では取締役CIO情報システム統括責任者を務めていたそうですね。

佐藤　私が勤めていたネット銀行は当時、ネット専業銀行としては世界でも最多の利用者数を誇っていたこともあり、セキュリティにはつねに細心の注意を払っていました。世界中から多数の攻撃を受けていたので、毎日、「大きな被害が出ないようにしなければならない」というプレッシャーを感じていました。

その業務のなかでどのようなことが印象に残っていますか。

佐藤　外部からの攻撃に対する以上に、内部や委託先からの情報漏洩に注意を払っていました。PCをなくしたり、盗難に遭ったり、メールの誤送信があったりと、さまざまなトラブルがあり、その都度、対応と対策に追われていました。

システムというよりも、ヒューマンエラーによるリスクのほうが高かったのですか。

佐藤　多くのセキュリティシステムは外部からの攻撃には万全を期しているのに、内部からのネットワーク通信に係る情報漏洩に関してはほとんど対策がなされていない印象を持っています。そのため、今も多くの組織から情報が漏洩しつづけており、それらが世界中のダークウェブなどで売買されているのです。

ちなみに、金融機関に関してはセキュリティや認証システムが高度化していますし、国内送金であれば、ログをたどることで犯人を突き止めることができます。ただ、ビットコインをはじめとする暗号資産のパスワードなどが流出すると、海外送金が容易なため、いとも簡単に数億円単位の資産を失ってしまう恐れがあります。しかも、ひとたび海外に送金されてしまうと、法律が異なるうえに複雑なマネーロンダリングが行われることが多く、絶望的な状況になってしまうでしょう。

暗号資産が狙われるリスクが高まっているのですか。

佐藤　日本では依然として暗号資産＝投資商品という見方が強いのですが、一部の国では「自国の通貨よりも暗号資産のほうが信頼できる」「海外でも使用できて便利」といった理由から広く普及し、まさに安全資産のように利用されています。そのため、昨今は暗号資産が狙われるリスクも急激に高まっているのです。

見えないリスクを顕在化し持続可能なセキュリティ体制を構築

こうした多岐にわたるリスクを防ぐため、御社ではどのようなセキュリティコンサルティングを実践しているのですか。

佐藤　セキュリティリスクは目に見えるものではないため、多くの人にとってイメージしづらいものになっています。そこで、当社ではまず「現状のシステムにおいて、PCやサーバーからどのような情報が漏洩する恐れがあるか」といったリスクを顕在化することからはじめます。そして、そのうえですべてを完璧に守り抜こうとするのではなく、守る必要がある情報の優先順位を検討したうえで、最適な対策を提案しています。なかには不安を煽り、さまざまなセキュリティツールの導入を促すコンサルタントもいますが、それではコストが膨らみすぎてしまい、持続可能なセキュリティ体制を構築することはできないでしょう。

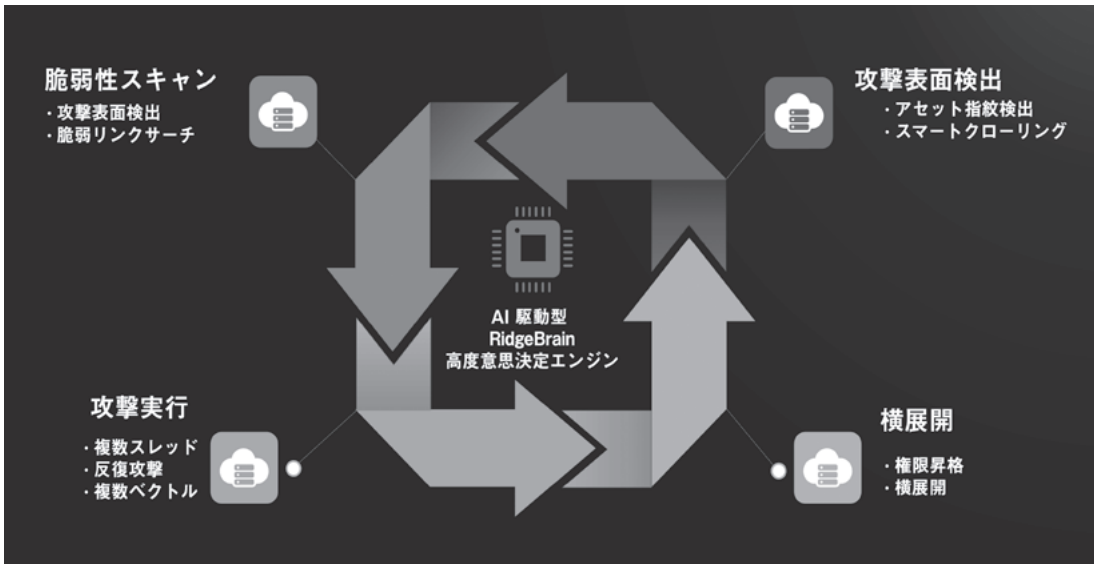
セキュリティのなかでも強みとしている分野はあるのでしょうか。

佐藤　ネット銀行時代のノウハウがあるので、ウェブサイトやアプリの脆弱性診断に強みがあります。たとえば、最近はハッカーがウェブサイトのライブラリ（プログラム部品の集まり）やプラグイン（追加機能）にマルウェアを仕込み、それらの導入・更新時に被害が拡大するケースが増えていますが、当社では最新のセキュリティツールを活用し、そういった不正プログラムを導入前に検知し、被害を未然に防げるような体制づくりを支援しています。

具体的にはどのようなセキュリティツールを推奨しているのでしょうか。

佐藤　自動化ツールとして米国のRidge Security社が開発した「RidgeBot」なども推奨しています。このツールはAIを活用して攻撃者視点で本番環境（実際にシステムが稼働している状態）の脆弱性を自動検証するため、定期的に自動検証を行うことができ、高いレベルのセキュリティを維持することができます。社内システムがマルウェアに汚染されたらどうなるかといったこともシミュレーションもできるため、ランサムウェア（身代金要求型ウイルス）対策にも一役買うでしょう。従来は大手企業や金融機関が専門企業に委託して実施してきたような高度なセキュリティ検査を、中小企業でも自社で手軽に実施できるようになることに期待しています。ちなみに、このツールの販売代理店を務めている㈱ブロード（東京都千代田区）は、先進性と独自性に満ちたソリューションを多数取り扱っている素晴らしいセキュリティ会社なので、今後とも協力しながら、大きな視点で日本のセキュリティレベルの向上に努めていきたいと思います。

RidgeBotで自動化できるセキュリティ検証ステップ



AIがIT資産の検出、脆弱性スキャン、模倣攻撃で侵害可否や経路を検証し、結果の提示までを100％自動化