GUEST SPEAKER

株式会社　肥後銀行
執行役員
デジタルソリューション部長
藤田 忠士 氏（写真中央）
Tadashi Fujita

デジタルソリューション部
デジタル企画・管理グループ長
古庄 伸一 氏（写真左）
Shinichi Furusho

デジタルソリューション部
デジタル基盤開発グループ長
竹下 潤昌 氏（写真右）
Hiromasa Takeshita

（取材日：2025年11月）

「自分たちのシステムは自分たちで守る」——約140人の現場社員が一丸となった総力戦のサイバー防衛。

2025年に創立100周年を迎えた、熊本県を地盤とする肥後銀行。地域におけるDX戦略の支えとなる、サイバーセキュリティの強化を経営の重要課題に掲げている。

同社は、昨今のサイバー攻撃が激化する社会情勢を踏まえ、「防御」から「検知・対応」にも領域を拡げた次世代型対策への転換に踏み切った。その意思決定の背景と、日々報告される脆弱性を速やかに排除するための独自のチーム運用体制についてお話を伺った。

ASHISUTO CUSTOMER

株式会社　肥後銀行

うるおいある未来のために。
肥後銀行
HigoBank

地域を活性化する銀行DXに求められる“安全・安心”

創業以来の地域との関わりをお聞かせください。

肥後銀行は、大正時代の創業以来、昭和、平成、令和と時代の移り変わりの中で、熊本最大の地域金融機関としてお客様と共に成長してきました。

当行はDXを重要な経営課題と位置付け、業務プロセスの効率化や生産性向上に取り組むとともに、バンキングアプリの提供やキャッシュレス決済の普及を通じて新たなお客様体験を創出しています。また、地元企業に寄り添い、DX推進を支援する独自の取り組みを通じて、地域経済の発展

にも貢献しています。

地元企業のDX支援とは、どういうものですか?

地域の企業や個人事業主のお客様によっては、ITリテラシーの差が大きく、「DXの必要性は理解しているが、何から始めればよいか分からない」「セキュリティ対策はどうすればいいのか」といった悩みを抱える方が少なくありません。特に中小企業では、情報システム部門や専任担当者を配置するのが難しいケースが多く見受けられます。さらに、熊本では首都圏に比べ、支援を提供するコンサルティング会社やシステムインテグレーターの数が限られており、いわゆる"駆け込み寺"的な存在が少ないのが現状です。

そこで、当行は「一番身近な相談相手」として地方銀行がその役割を担うべきだと考えました。具体的には、営業店の行員が「DXアドバイザー」の資格を取得するなどしてスキルを磨き、デジタルやセキュリティに関する知識をお客様に提供していくという取り組みです。こうした活動を通じて、地域全体の競争力向上を目指しています。

DXとセキュリティの関係をどうお考えですか?

ランサムウェアやフィッシング詐欺など攻撃手法が巧妙化する中、金融機関は犯罪者にとって格好の標的と言えます。もしも当行が被害に遭い、システムやバンキングアプリが停止する事態になれば、地域の決済インフラとしての機能やお客様の事業停止にもつながりかねません。

DX推進とセキュリティ対策は、いわば車の両輪です。「攻め」のDXを進めるには、盤石な「守り」が不可欠です。両者を切り離して考えることはできないものとして、セキュリティを当行の最重要課題と位置付けています。

境界防御から"侵入は防げない"前提のセキュリティ対策へ転換

従来は、どのような方法でセキュリティ対策をされていましたか?

かつては多くの企業と同様、外部と社内ネットワークの接点を強化する「境界防御」の考えに基づいて対策していました。具体的には、インターネット接続系と内部システムのネットワークを論理的に分離し、ファイアウォールで不正アクセスや攻撃トラフィックを遮断する、あるいはメールの添付ファイルをサンドボックス環境で無害化するといった方法で、「侵入させない」ことに重点を置いていました。

当時は業界を問わず、この方法が一般的に"最低限やらなければいけないこと"とされる対策であり、何とか一定のセキュリティレベルは担保できている状況でした。

境界防御だけでは不十分と考えるようになったきっかけは?

一番の理由は、何社もの大手企業がサイバーセキュリティ被害を受けていることへ

「セキュリティを当行の最重要課題と位置付けています」(藤田氏)

の危機感です。ここ数年、名だたる大企業がランサムウェア等により、事業が長期間停止するほどの深刻な事態に陥っていることに衝撃を受けました。

当行よりはるかに事業規模が大きく、優秀なＩＴ人材を豊富に抱えていても侵入されてしまうという事実は、考え方を根底から覆す出来事でした。正直に申し上げると、これまで当行が大きな被害を受けなかったのは、〝単に運が良かっただけ〟なのだと痛感しました。そこで、ゼロトラスト（全ての通信を信頼せず、常に検証する考え方）に基づき、内部への侵入を前提に、被害の最小化を重視した対策へ舵を切りました。

〝侵入前提〟という方針への転換に、経営層から不安の声は出ませんでしたか？

反対する声も出るのではと思っていましたが、幸い当行の役員はＩＴやセキュリティに関してある程度の下地があり、意図をすぐに理解してもらえました。実は現在の頭取は、かつてＩＴ部門長を務めた経験があります。また、他の役員も全員がサイバーセキュリティ研修を受けています。そのため〝完全無欠なセキュリティ対策はない〟という共通認識を持つことができていました。このことは、全社的なセキュリティ方針を定める上で、非常に大きなアドバンテージです。こうして、「侵入されたときに、どうやって被害を最小限にして事業を継続させるか」に価値を置く対策に転換する、迅速な意思決定につながりました。

内部に潜む脆弱性に危険度ランクを付けて可視化

侵入されたと仮定すると、内側の守りを固めることが最重要になりますね。

そのとおりです。以前からサーバーやネットワーク機器にセキュリティパッチを適用してセキュリティホールを塞ぐという運用は行っていました。

しかし当時は、Excelを使った手作業による情報管理が頼みの綱でした。端末ごとのＯＳのバージョン、そして最新のセキュリティパッチが適用済みかどうかを担当者が一台ずつ確認し、Excelに入力していく。このアナログな手法には限界がありました。一つの業務システムは複数台のサーバーで構成されているケースも多く、それぞれＯＳのバージョンが異なるなど構成が複雑です。全てのＩＴ資産の情報を手作業で正確に網羅することは非常に困難でした。

セキュリティパッチを当てる対象は、どのような基準で選んでいたのですか？

ＩＰＡ（独立行政法人 情報処理推進機構）等が公開する脆弱性情報を参考に、当行環境に該当するものを抽出するという方法で対象を選択していました。しかし、この方法では収集できる情報が限られており、世界中で日々発見される脆弱性を網羅的に把握することは困難でした。そのため、「より重大なリスクを見落としているのではないか」という不安を常に感じていました。

そこでツールの力を借りることにしたわけですね。

はい。まず求めたのは、全てのサーバーやネットワーク機器のＯＳやソフトウェアの情報を、手動ではなく自動で収集・一元管理できること。その上で、そこにどんな脆弱性があるかリスクアセスメントができることを要件としました。複数製品を検討した結果、アシストが提案した「Tenable」を選択しました。他の地方銀行でも採用実績があることの他、将来的に対策を検討していたＷｅｂサイト診断、ＣＳＰＭ、ＡＤ保護の機能もあり、一つのプラットフォームで運用できる点が決め手になりました。

Tenable導入の利点は、まずネットワークスキャンによって「自分たちが持っている資産」が自動的に洗い出されること。

Tenableの画面イメージ

そして何より、〝今まさに狙われやすい脆弱性〟が、Tenable独自のスコアリング指標であるVPR（Vulnerability Priority Rating）により、数値として可視化される点です。単なる脆弱性の深刻度だけでなく、「今現在、世界中で攻撃が増加しているか」「実際に深刻な被害が出ているか」といった情報を加味してランク付けしてくれる。これにより、優先的に対応すべき脆弱性はどれかというリスクベースでの判断が可能になるわけです。

実際の診断結果を見てどのような印象でしたか?

試験的にスキャンした結果を見た時、「問題ない」と思っていた内部システムにまだまだ多くのリスクが残っていることが分かり、驚きました。さらに本格運用を開始して衝撃を受けたのが、ある企業が重大インシデントで狙われたのとまったく同じ脆弱性が、我々の環境でも報告された時です。しかもそれは、以前のCVSSスコアだけを見る基準では、優先度が低いと判断され見逃されていた可能性が高いものでした。

「もし攻撃のターゲットになっていたら、確実にそこから侵入されていた」、そう思うと冷や汗が出ました。まだ攻撃を受けなくてよかったと胸をなでおろすと同時に、境界防御だけではリスクを防ぎ切れない現実を改めて突きつけられた瞬間でした。

開発・運用担当の約140人を巻き込んでセキュリティ対策体制を構築

可視化した脆弱性は、どのような体制で対処していますか?

まず以前の体制をご説明すると、3名のサイバーセキュリティチームが、脆弱性の特定から対策までを行っていました。しかし、Tenable導入後は報告される脅威の数が格段に増えるため、少人数ではとても対処しきれません。そこで、運用体制を抜本的に強化して、脆弱性を次々とつぶしていこうと考えました。

具体的には、セキュリティパッチの適用作業について、デジタルソリューション部に所属する業務システムの開発・運用担当者、協力会社を含めた約140名に協力を依頼し、分散して行うことにしたのです。

実働部隊を大幅に増やしたわけですね。

そもそもサイバーセキュリティは、攻撃者視点では〝たった一つの穴を見つければいい〟のに対し、防御側は〝一つの穴すら許してはいけない〟という圧倒的に不利な戦いということが前提としてあります。しかも、金融機関に求められるセキュリティ水準は非常に高く、それはメガバンクであっても地方銀行であってもほぼ同等です。とても数人だけで守り切れるものではないため、当行は組織の壁を越え、一丸となって厳しい戦いに臨むことにしました。

「組織の壁を越え、一丸となって厳しい戦いに臨むことにしました」（古庄氏）

現場から反発の声はありませんでしたか？

正直、当初は戸惑いの声もありました。「普段の開発・運用業務で手一杯なのに、セキュリティ対策まで自分たちがやるのか」「それは専門部署の仕事ではないのか」といった反応です。開発現場からすれば、稼働中のシステムにパッチを当てるのはリスクを伴う作業です。「もしパッチを当てて業務に影響が出たらどうするんだ」という恐怖心もありますし、パッチ適用後の検証作業も発生しますから。

そのため、まずサイバー攻撃を受けてしまった場合、当行の資産やお客様の情報がどんな被害を受けるのかというリスクについて、丁寧に説明することから始めました。他社のインシデント事例を共有し、「どこを攻撃され、どんな被害があったのか」「なぜ我々も対策が必要なのか」を説明し続けました。こうして、セキュリティは専門部署だけの課題ではなく、組織全体の最重要テーマであり、〝自分たちのつくったシステムは自分たちで守る〟という意識醸成を図っていきました。

１４０名もの人数が、足並みを揃えて動くのは大変そうですね。

いくら人数が増えても、各自の判断でやみくもに動いていては組織として機能しません。ここで役立ったのが、Tenableで明示されるＶＰＲスコアです。以前は、各システムの担当者に対し「ここが危ないから対策してください」とお願いしても、「本当に今やる必要があるの？」「他にもっと危ないところがあるんじゃないの？」と疑心暗鬼に受け取られることもありました。しかし今は、Tenableという客観的なツールが最も危険なところをエビデンス付きで示してくれる。〝お墨付き〟があるから、現場も納得して動けます。

さらに当行では、Tenableから出力した情報に一手間加えて、独自のダッシュボードを構築しています。脆弱性ごとに「発見から何日経過したか」「いつまでに対策を完了させるか」といった期日管理を行えるようにしています。

そのダッシュボードの情報が、チーム共通の目標になるわけですね。

優先度は４段階（表参照）に分け、「危険度に応じて限られた期日内に対応する」というルールを設けています。これが全員の〝共通言語〟となり、迷いなく対策を進めることが可能になっています。また、運用ルールとして「脆弱性を見つけた際、深刻なものを除いては経営層へ報告せず現場が対処する」ことにしました。これは、個々にお伺いを立てていては対策のスピードが落ちてしまうからです。

新しい運用体制になって、現場の意識に変化はありましたか？

意識は劇的に変わりました。〝セキュリティは専門家の仕事〟という人ごとから、〝自分たちのシステムは自分たちで守る〟という当事者意識へと変化しています。脆弱性情報を通達すると「すぐに対応します」「パッチ適用の影響調査を始めます」と、前

優先度	対応方針
４（高）	可能な限り速やかに対応
３（中）	速やかに対応
２（低）	定期メンテに合わせて対応
１（参考）	不定期に対応

肥後銀行が独自のダッシュボードで可視化している脆弱性レベル。優先度に応じて、具体的な対応期間（1ヵ月以内に実施など）を設定。

「強固なセキュリティ基盤があってこそ、DXを加速させることができます」（竹下氏）

向きな反応が返ってくるようになりました。

また、彼らの本来業務である、システムやサービスの開発においても、セキュリティ意識の高まりを感じます。今では要件定義や設計の段階から、「この設計では安全性が低いのではないか」といった意見が飛び交うようになり、「セキュリティ・バイ・デザイン」※の考え方が浸透していると感じます。こうした意識変革に加えて、サイバーセキュリティチームも行員5名、協力会社4名の総勢9名に増えました。

DXとセキュリティを両輪として地域を活性化

サイバーセキュリティ専門の行員が5名いらっしゃるのは、地方銀行としてかなり多いのではありませんか？

そうですね。他の地方銀行さんでは専任が1～2名、あるいは完全に外部ベンダーに委託するケースも少なくありません。当行の9名体制というのは、かなりリソースを割いている方だと思います。とはいえ、最初から当行に専門家がいたわけではありません。行員5名も元々インフラエンジニアやIT未経験者からスタートしています。地方ではセキュリティの専門人材を採用しようとしても、そもそも対象となる人材が少なく、募集をかけても集まらないのが現実です。

ですから当行では「今いるメンバーを育成する」という方針を採っています。インフラやネットワークの担当者が、実務を通じてセキュリティのスキルを身に付けていく。足りない知見は外部のエージェントやベンダーに入ってもらい、伴走しながらノウハウを吸収する。そうやって組織能力を高めてきました。

金融ISAC※にも積極的に参加しています。週1回のWeb会議や年2回のカンファレンスで、「今どんな攻撃がはやっているか」「他行はどう対策しているか」といった生きた情報を収集しています。学んだ知見は、同じ九州フィナンシャルグループ内の鹿児島銀行などとも共有し、連携を深めています。

※システムや製品の企画・設計段階から、セキュリティ対策を組み込む考え方。

肥後銀行は、キャッシュレス決済サービス「くまモン!Pay」の導入を推進。地域における資金循環の活性化、住民の利便性向上に貢献している。

セキュリティ基盤の強化は、地域に対する貢献にどう結び付くと思いますか？

強固なセキュリティ基盤があってこそ、お客様に安心してデジタルバンキングサービスをご利用いただけますし、DXを加速させることができると考えています。この安全性を支えとして、営業用のタブレット端末アプリの開発や、生成AIの活用などにさらに力を入れていきたいと思います。今、特に力を入れているのが「AIエージェント」の活用です。

AIを具体的にどのように活用していく構想ですか？

システム開発におけるテスト工程やコーディングの一部をAIエージェントに任せ

※ISAC：同じ業界のセキュリティ利用企業とベンダーが情報を共有するための組織。金融、通信、電力など業界別にISACが存在する。Information Sharing and Analysis Center（情報共有分析センター）の略。

る取り組みを進めています。人間は限られた時間しか働けませんが、デジタル労働力であるＡＩなら、24時間３６５日疲れることなく働いてくれます。私たちが休んでいる間にＡＩがコードテストを行い、品質を高めていく。人間は人間にしかできない創造的な業務に集中する。そういった役割分担の開発スタイルを確立しようとしています。将来的にはお客様への融資判断サポートにもＡＩを活用したいと考えています。

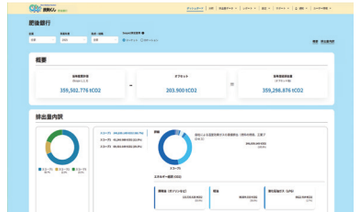
またＡＩはセキュリティ領域でも大きな可能性があります。現在、ＡＩを利用して、サイバー攻撃の兆候をリアルタイムで捕捉するシステムの開発に取り組んでいます。

最後に、今後の新たな挑戦についてお聞かせください。

実は、１００周年事業の一環として、地域のＩＴインフラに関する新たな挑戦を発表しました。地方銀行として初となる、自前のデータセンター建設です。

きっかけは、熊本県内の既存データセンターが老朽化している一方で、次の受け皿となる施設が足りないという地域課題でした。ＴＳＭＣ進出などで熊本経済が活況を呈する中、地元企業のデータの保管場所が県外に出ていってしまっていいのか。「それならば当行が、生成ＡＩのプラットフォームとしても活用できるデジタルインフラを提供しよう」という発想から生まれた計画です。まずは自行利用からスタートし、将来的には地域の企業の皆様にもご活用いただきたいと考えています。

当行がＤＸやサイバーセキュリティ対策を通じて学んだのは、最初から完璧を目指すのではなく「まず一歩を踏み出すこと」の大切さです。小さな成功を積み上げて組織全体をデジタル化に適したかたちにシフトさせていく。そして、これまで得た知見やノウハウで、地域企業の皆様をご支援し、地域の発展に貢献し続けていきたいと思います。



Zero-Carbon-System®
CO2 炭削（たんさく）くん

企業のカーボンニュートラルを支援するサービス「炭削（たんさく）くん」。企業が排出する二酸化炭素量を計測・算出し可視化する、自社開発ソリューション。

会社概要
corporate profile

株式会社　肥後銀行

本　店：熊本市中央区練兵町1番地
創　立：1925年
資本金：181億円
ＵＲＬ：https://www.higobank.co.jp/

事業内容

普通銀行業務（預金、融資、国内・外国為替、証券、信託代理業務、各種保険など）

肥後銀行様の創立100周年、誠におめでとうございます。心よりお祝い申し上げます。この記念すべき年に『お客様の声』の取材にご協力を賜りましたこと、深く感謝申し上げます。

弊社イベント「アシストフォーラム」での事例発表につきましても、快くお引き受けいただきました。とりわけ金融機関である肥後銀行様にセキュリティ関連の事例をご発表いただけることは、非常に大きな意義がございます。セキュリティ対策の取り組みを公の場でお話しいただくことはハードルが高く、金融機関様ご自身からご発信いただける機会は極めてまれであることから、弊社のお客様の間でも関心は非常に高く、強い注目を集めたご講演となりました。重ねて御礼申し上げます。

また、地元企業のDXご支援や地域のITインフラを支える新たな挑戦として自前のデータセンターを建設されるなど、地域貢献に重きを置かれた取り組みの数々には、深い感銘を受けております。

アシストは、肥後銀行様の「攻め」のDXと、その土台を支える盤石な「守り」の両面をお手伝いできるよう、これからも良きパートナーとして伴走してまいります。今後とも末永くお付き合い賜りますよう、何卒よろしくお願い申し上げます。