Radical Transparency

Forbes JAPAN BRANDVOICE

サイバー脅威から企業をどう守るか

「攻めの透明性」という新戦略

The New Strategic Standard for Cyber Defense

一貫した誠実さこそ
企業を守り抜く
「最強の武器」として機能する。

デジタル社会において

真の信頼は「事実を歪みなく開示し続ける姿勢」によって築かれる。

ブラックボックスを排し、常にオープンであり続けることで

社会に確かな安心を提示する。

この一貫した「攻めの透明性」が

顧客との絆をより強固なものにし

積み上げた信頼を未来へとつなぐ生存戦略となる。

INDEX

辻

The Power of Transparency

「隠蔽は最大のリスクだ」
セキュリティをIT対策から「経営思想」の体現へ

経営学者の入山章栄教授は、サイバーセキュリティを「ITの問題」と切り離す風潮に警鐘を鳴らす。企業の有事における信頼を守る盾であり、逆境を好機に変える武器ともなる「透明性」の本質を説く。

illustration by Shapre | text by Motoki Honma | edited by Aya Ohtou (CRAING)

数年前、私が取締役を務める企業がランサムウェア攻撃者集団によるサイバー攻撃を受け、データが人質に取られるという事態に陥りました。当然ながら身代金の要求などは一切無視しましたが、当事者のひとりとして痛感したのは、セキュリティとは技術的な問題ではなく、経営そのものであるという事実です。

多くの経営者はセキュリティと聞くとハード面、つまり強固な防壁を築くことを考えがちです。しかしどれほど高い壁をつくったとしても実際に運用し、有事の際に判断を下すのはソフト面である人間の心、「経営思想」にほかなりません。

そもそも企業ブランドの価値とはステークホルダーに対して「どのような価値を提供し、どう社会と向き合うか」という約束を積み重ねてきた結果です。一貫した誠実な行動の集積が信頼というブランドをかたちづくっているのです。昨今、社会問題化しているフィッシング詐欺などはその価値を揺さぶる最たる例といえます。自社のサービス名を騙った偽メールや偽サイトがつくられ、それを信じた顧客やステークホルダー、さらには潜在顧客までが被害に遭ってしまう。このような状況下で「自分たちも名前を悪用された被害者だ」と言い続けるのは、それまで積み上げてきた社会的な約束を自ら破り捨てるに等しい。セキュリティはもはやITの範疇を超え、経営者の思想を問う防衛戦略そのものなのです。

オーセンティシティが信頼の基盤に

なぜ今、これほどまでに誠実さが求められるのか。それは、現代が隠すことで権威を保てた時代の終焉を迎えたからです。かつてのリーダーは情報を遮断し、自分を特別な存在としてパッケージングすることで地位を維持できました。しかし、現代において隠蔽は最大のリスクであり、誠実さの欠如は即座にブランドの終わりを意味します。インターネットやSNSによって、すべてが可視化されることが前提の社会なのです。

これからの時代、企業に求められるのは「Radical Transparency（抜本的な透明性）」であると考えています。これは、台湾で政治のデジタル化を推進してきたオードリー・タン氏も強調されている概念ですが、単なる道徳論ではなく、隠し事がいずれ露呈してしまう現代における現実的な生存戦略といえます。自社の弱さや失敗も含めて曝け出すこと。この徹底した透明性こそが、信頼を勝ち取る道筋となります。

ブランド価値を守り抜けるかどうかの決定打は不都合な真実が露呈したとき、トップがいかに透明性をもって語るかにかかっています。

お手本となるのは22年7月に行われた大規模な通信障害におけるKDDIの記者会見です。高橋誠社長は技術的な詳細から経営責任に至るまで、記者の鋭い質問に対して一切逃げることなく、ご自身の言葉で答え続けられました。その真摯な姿勢を見て当初は厳しかった世論も「これほど詳細に状況を把握し、誠実に説明できるリーダーがいるならば再起を信じられる」という好意的なものへと変わっていったのです。これは、透明性が信頼を生んだ極めて今日的な事例といえます。自分を飾らず、ありのままを曝け出す「オーセンティック・リーダーシップ」が発揮されたのです。

全可視化時代のサバイバル・プラン

では、リーダーの真摯な姿勢をいかにして持続的な競争力へと転換し、企業文化として定着させていくのか。立派な理念を掲げたとしても、それが仕組みや行動として根付かなければ空虚なスローガンに終わってしまいます。組織の隅々にまで理念を浸透させ、共通の判断軸として醸成していくことが不可欠です。なぜなら、文化とは社員一人ひとりの無意識の判断基準そのものだからです。

世界的化学メーカーであるデュポンでは、「安全」という思想が社員のDNAレベルで共有されています。今のように義務化される以前から、タクシーで後部座席に座れば必ずシートベルトを締め、駅構内の階段でも必ず手すりをもって歩くといった行動が徹底されています。これは、入社初日の研修からタクシーの乗り方に至るまで、具体的な行動様式を徹底してたたき込まれている証しです。

文化を醸成するうえで経営者が陥りがちな間違いはルールや規律を増やしすぎてしまうことです。経営学的な知見から申し上げれば、人間が真に理解し、無意識レベルで実行できる行動規範の数は10個が限界といわれています。重要なのは自社にとって死守すべき価値観を言葉に凝縮し、それを何があっても守り抜くという姿勢をトップが示し続けること。そして、その思想の浸透が最も力を発揮するのは有事の際です。

ここで参照すべきは山崎製パンの事例です。2011年の東日本大震災の際、同社は農林水産省、自治体からの要請に対し、製造・配送のリソースを災害支援に振り向ける決断を下し、未曾有の混乱のなかで被災地にパンを届け続けました。さらに、こうした企業文化が現場にまで徹底されていたことを示すのが、14年の記録的な関東大雪での対応です。配送トラックが各地で立ち往生した際、現場のドライバーが会社に相談し、即座に承認を得ることで、周囲の人々にパンを無償提供した事実は広く知られています。

サイバーセキュリティにおいてもこれと同様で、現場の社員がいざというときにどう動くかという判断基準をもっていなければなりません。それが体に染み込んで初めて、真の意味で企業文化と呼べるものになるのです。

もうひとつ、思想を文化として醸成するうえで見落とされている視点があります。それは実戦的な訓練の積み重ねです。日本企業は地震の避難訓練には極めて熱心です。しかし、日常的な脅威であるサイバー攻撃に対し、同様の全社的な訓練が行われているケースは驚くほど少ないのが現状です。いざ攻撃を受けた際、現場の社員や広報、そして経営陣がどのように動くかという実践の場がなければ組織は機能しません。必要なのはサイバー攻撃に対しても全社を挙げたシミュレーションを行うことです。例えば情報流出を想定し、コールセンターの対応から経営陣の情報開示に至るまでの意思決定プロセスを徹底的に検証する。こうした訓練を通じて「有事の際、我々は誠実に行動する」という共通体験をもつことが強力な組織文化の醸成につながります。これを経営の優先事項としてスケジュールに組み込み、社員に対応の型を染み込ませること。それが、いざという時にブランドを守る強靭な防壁となるのです。

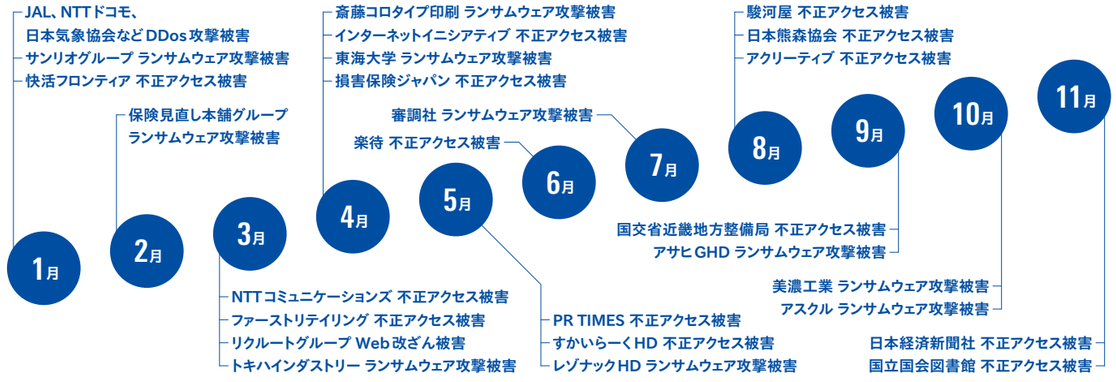
セキュリティは決してIT部門だけの問題ではありません。それは経営者の思想を問い、企業が本当に誠実であるかどうかという真価を映し出す鏡のようなものです。徹底した透明性を支える強固な企業文化。それがデジタル時代においてステークホルダーとの約束を守り、企業価値を永続させるための唯一の道であると私は考えています。Ⓕ

Akie Iriyama 入山章栄

いりやま・あきえ◎早稲田大学大学院 早稲田大学ビジネススクール教授。慶應義塾大学大学院修士課程修了後、三菱総合研究所入社。2008年米ピッツバーグ大学経営大学院でPh.D.取得。米ニューヨーク州立大学バッファロー校助教授を経て、2013年早稲田大学ビジネススクール准教授に就任。2019年4月より現職。

2025年に国内で発生した主要なセキュリティインシデント

※2025年1月〜11月　出典：トレンドマイクロ



Threat Landscape

生成AIによるサイバー攻撃が増加
最新の脅威ランドスケープと経営リスク

生成AIにより巧妙化・自動化する攻撃の実態把握は、経営の最優先事項である。
脅威を直視し、迅速な経営判断を下すことが、デジタル社会における責任ある防衛線を築く第一歩となる。

illustration by nao1008 | text & edited by Aya Ohtou (CRAING)

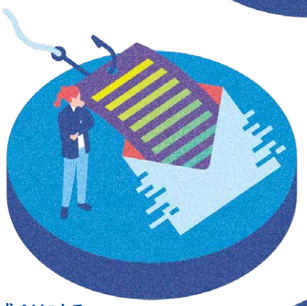
情報セキュリティ10大脅威2025

出典：独立行政法人 情報処理推進機構

1位 ランサム攻撃による被害
2位 サプライチェーンや委託先を狙った攻撃
3位 AIの利用をめぐるサイバーリスク
4位 システムの脆弱性を悪用した攻撃
5位 機密情報を狙った標的型攻撃
6位 地政学的リスクに起因するサイバー攻撃（情報戦を含む）
7位 内部不正による情報漏えい等
8位 リモートワーク等の環境や仕組みを狙った攻撃
9位 DDoS攻撃（分散型サービス妨害攻撃）
10位 ビジネスメール詐欺

進化する脅威の源泉

国家支援・高度犯罪組織（APT/Raas/PhaaS等）
国家背景をもつ組織やビジネスとして身代金要求（ランサムウェア）を行うプロの犯罪集団による攻撃



生成AIによる武装化・自動化
- AIフィッシング
- ディープフェイク（偽動画・音声）詐欺
- 攻撃コード自動作成

DDoS
国際情勢の緊張や政治的な主張を目的とした攻撃

複雑化する事業環境と脆弱性

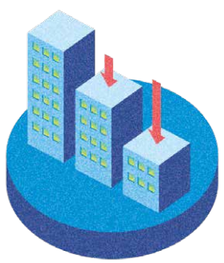
攻撃の巧妙化 規模の拡大

連鎖する多層的なビジネスインパクト

財務・業務的損失
- 業務停止
- 身代金支払い
- 収入機会損失

法的・規制リスク
- 情報漏えいによる賠償
- 巨大な制裁金
- 訴訟対応

企業価値の毀損・経営危機
- 株価暴落
- 経営陣の責任問題
- 事業継続の危機



レピュテーション・信頼の失墜
- 顧客離れ
- ブランドイメージ毀損
- 社会的信用低下

サプライチェーン・海外拠点への二次被害

社会インフラへの波及

入れ替わってしまっているので逆にしてください

サイバー攻撃が引き起こす多層的リスク

サイバー攻撃は生成AIによる武装化で新たな局面を迎えている。攻撃コードの自動生成や巧妙なディープフェイクは従来の防御策を無効化し、攻撃の規模と精度を劇的に向上。さらに、国家背景をもつ組織や高度な犯罪集団の関与、地政学的緊張による攻撃の激化がビジネスのエコシステム全体を脅かしている。

曖昧化する境界線と個社防衛の限界

デジタルシフトの加速はリモートワークやサプライチェーンの拡大をもたらしたが、同時に守るべき境界線を曖昧にした。自社防衛が堅牢でも、海外拠点や委託先を突く攻撃が常態化している。DX推進で広がるシステム全域を統合的に管理・防衛することが、現代経営において不可欠な戦略である。

生成AIがもたらすサイバー攻撃の高度化

サイバー攻撃による被害はITシステムの停止だけでなく、企業の存立基盤を揺るがす多層的な損失へと連鎖する。初期段階では、復旧費用の発生や事業停止による直接的な財務損失を招くが、真の脅威はその後に続く二次被害にある。機密情報や顧客データの流出は法的責任や巨額の賠償問題に発展するだけでなく、長年築き上げたブランド価値や社会的な信頼を一瞬にして失墜させる。さらに、サプライチェーンの寸断によって取引先や顧客へ被害が波及すれば、業界全体での競争力を喪失する恐れもある。ひとつのインシデントが経営リスクとして増幅し、中長期的に企業価値を毀損し続けることを前提としたレジリエンスの構築が急務となっている。

以下反映もれ
8Pの下段の見出し「役割分担が生み出す〜」とQ数ソロエル

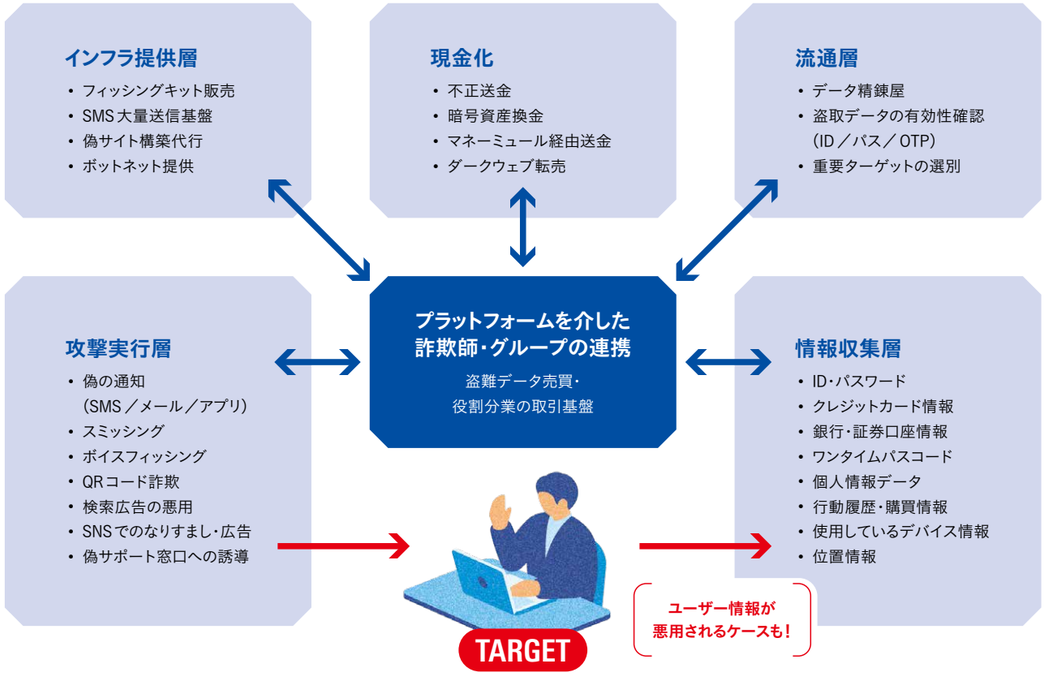
Assault on Authenticity

ブランド価値を失墜させる
フィッシング詐欺・ディープフェイク詐欺の実態

システム化されたフィッシング詐欺は、ブランドの信頼を直接的に毀損する収益モデルへと進化している。終わりのない物量戦に対し、企業はどう対峙すべきか。戦略的な防衛アプローチを探る。

illustration by nao1008 | text & edited by Aya Ohtou (CRAING)

フィッシング詐欺の分業化エコシステム

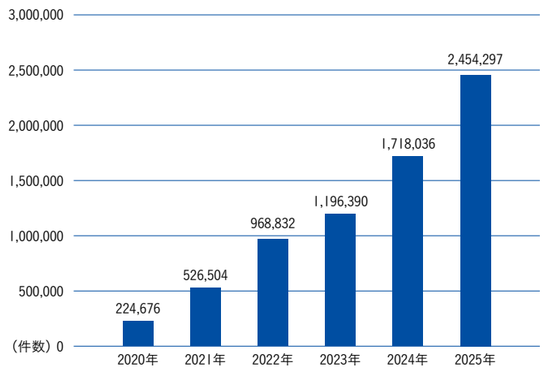


役割分担が生み出す「フィッシング経済圏」

分業化エコシステムの起点となるのが「インフラ提供層」だ。ここでは偽サイト構築代行やフィッシングキットの販売、SMS 大量送信基盤、追跡を逃れるボットネットなど攻撃に必要な道具を供給。これを悪用して実働するのが「攻撃実行層」と「情報収集層」である。攻撃実行層は偽広告、SNS でのなりすましなどから、ターゲットの ID・パスワード、カード情報、さらには使用デバイスの種類や行動履歴をも吸い上げ、情報収集層を介して「プラットフォーム」へと渡る。このプラットフォームが盗難データの売買や役割分担を指示する取引基盤となり、犯罪規模を爆発的に拡大。「流通層」でデータ精錬屋による有効性確認や重要ターゲットの選別が実施され、「現金化」となる。具体的には不正送金や暗号資産への換金、マネーミュール経由の送金、ダークウェブでの転売など追跡を逃れる巧妙な手段で利益が確定する。このように道具の供給から換金に至るまでが強固に連鎖しており、企業にはこのサイクルを断ち切る統合的な防衛戦略が求められている。

フィッシング詐欺の現状とクレジットカードの被害総額

フィッシング報告件数の推移（2020〜2025年）

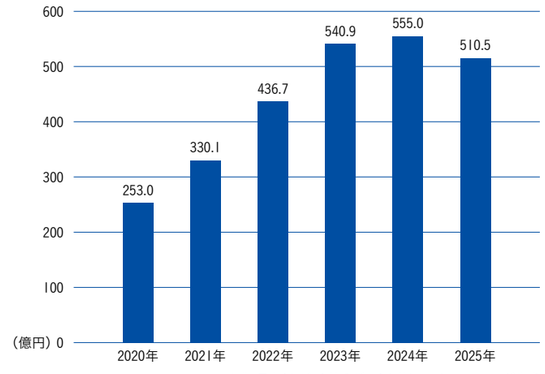


出典：フィッシング対策協議会データを基にForbes JAPANが作成

2020年以降におけるフィッシングの現状

2020 年以降、フィッシング詐欺の報告件数は増加の一途をたどっている。20 年に約 22 万件だった報告数は、わずか 5 年で約 245 万件と約 10 倍に膨れ上がった。これは攻撃プロセスがマニュアル化され、スミッシングや偽広告、SNS を介した誘導が組織的なワークフローとして確立された結果といえる。攻撃は特定のブランドを標的とした集中的なトラフィック投下へと変貌しており、従来の注意喚起だけで制御することは難しい。企業は自社ブランドを騙る不正ドメインや通信をリアルタイムで検知し、被害が発生する前に無効化する防御体制を築くことが急務といえる。防御の解像度を抜本的に高める戦略的投資が、今後の信頼維持における鍵となるだろう。

クレジットカード不正利用被害額の推移（2020〜2025年）



出典：日本クレジット協会データを基にForbes JAPANが作成

クレジットカードの被害額は3年連続500億円超え

2025 年の不正利用被害額は 510 億 5000 万円と、前年の 555 億円から 8.0%減少したものの、23 年以降 3 年連続で 500 億を超えている。昨年同様、被害の 9 割以上が「番号盗用」による非対面取引で行われており、なかでもフィッシングによる被害が拡大。これは奪取された情報が即座に精査され、決済へとつながっていることを裏付けている。経済産業省は、原則すべての EC 加盟店に対して「EMV 3-D セキュア」等の本人認証の導入を求めるなど制度的な対策を強化。今後は番号だけでは決済を成立させない認証の高度化が最低条件となるだろう。拡大し続ける実害を食い止めるために決済システムの信頼性をどう再構築するか、より包括的な戦略が問われている。

サイバー犯罪にどう立ち向かうべきか
「誠実な防衛」を企業価値に転換するためのアプローチ

STEP 1
ブランド毀損の実態把握

攻撃者が自社のブランドをどのように悪用しているかを分析し、潜在的な顧客流出や信用低下の規模を、経営が対処すべきリスクとして明確に定義する。

STEP 2
能動的な防御への転換

不正サイトの早期無効化など、顧客が攻撃に接触する手前で排除する仕組みをサービスの「品質保証」の一部として位置づけ、先制的な投資判断を行う。

STEP 3
透明性の証明

セキュリティへの取り組みを経営戦略の重要課題として定義。中長期計画や統合報告書を通じて防衛体制を開示し、ガバナンスとしての説明責任を果たす。

STEP 4
信頼資本による持続的成長

一貫した情報公開によりステークホルダーからの信頼をブランドアセット（資産）として蓄積し、長期的な事業成長を支える強固な経営基盤を確立する。

Value through Collaboration

孤立した防御を脱し、知の循環へ
防衛の最前線を担うキーパーソンが語る協働のかたち

高度化・巧妙化が進むサイバー攻撃。人の心理的な弱みに付け込む手法も増え、従来の対策だけでは防ぎきれない状況にある。
今求められているのは、攻撃の実像を正しくとらえ、企業の枠を超えて守る連携である。

text by Motoki Honma | photographs by Daichi Saito | edited by Aya Ohtou (CRAING)

本対談に集ったのは、日本のデジタル社会の安全を構造的に支える主要組織で意思決定を担うキーパーソンたち。JPCERTコーディネーションセンター（JPCERT/CC）は、国内のインシデント対応のハブとして機能する防御の要である。同センターの山本健太郎（写真左。以下、山本）はフィッシング報告の分析やサイトのテイクダウン※を指揮する実務の責任者だ。非営利の立場から数多の攻撃サンプルを見える化し、企業の防波堤を築く視点をもつ。対して日本サイバー犯罪対策センター（JC3）は産官学が情報をもち寄るインテリジェンスの集積地である。警察庁や内閣官房で国際テロ、情報インテリジェンス対策を歴任した櫻澤健一（写真中央。以下、櫻澤）が率いる同組織は、犯罪の構造を可視化し官民をつなぐことで実効性ある対策へと転換する役割を担う。そして実務レベルでの連帯の旗振り役を担うのが日本クレジットカード協会（JCCA）だ。事務局長の辻中伸幸（写真右。以下、辻中）はカード会社での実務経験を背景に業界横断的なテイクダウン活動を主導。競合するカード会社同士が協調領域で手を取り合う新たなビジネススタンダードを提示している。

辻
※以下全て同

――サイバー攻撃の質が劇的に変化しています。最新の潮流をどうとらえていますか。

山本：最大の変化は攻撃の目的が金銭に特化した点にあります。愉快犯的な攻撃は影を潜め、現在は効率的に収益を上げるためのビジネスとして確立しています。なかでも深刻なのがブランドへの愛着や信頼を逆手に取るフィッシング攻撃です。大手ECサイトや配送業者といった知名度の高いブランドをかたり、心理的ハードルを下げて偽サイトへ誘導する手口が横行しています。

※フィッシングサイトを閉鎖する取り組み

攻撃を仕掛ける側はビジネスとして動いている。
犯罪がエコシステム化している以上、防御も構造で考えるべきです。
櫻澤健一

さくらざわ・けんいち◎日本サイバー犯罪対策センター業務執行理事。1988年警察庁入庁。外務省、内閣官房、警察庁警備局長等を歴任後、2023年より現職。国際テロ・情報インテリジェンス対策に携わった経験を生かしサイバー犯罪対策を進める。

後、
し、国際テロ・情報インテリジェンス対策などに携わる。2023年より現職。

櫻澤：背後にはダークウェブや匿名 SNS を介した犯罪エコシステムが存在しています。組織こそもっていませんがフィッシングキットの作成者、偽サイトの構築者、盗んだ情報の販売者、現金化を担う出し子までネットワーク上で匿名かつ国境を越えて分業しています。

辻中：攻撃者は技術的な脆弱性だけでなく、人の心の隙やプロセスの隙を巧妙に突いてきます。そこが現在の攻撃の最も厄介な特徴だと言えますね。

山本：フィッシングはアクセスされて初めて成立する攻撃で一般ユーザーが標的となるため、技術的な対策だけで 100%防ぐことは極めて困難です。特にコロナ禍以降、ネットスーパーや金融サービスの利用が急増したことで、攻撃者にとっての狙いどころは日常のあらゆる場面に広がっています。

競合が手を組むセキュリティ防衛

――攻撃者が分業体制で組織的に攻めてくるのに対し、守る側の企業は個別対応にとどまるケースが見受けられます。この現状をどう打破すべきでしょうか。

辻中：クレジットカード業界では、いままさにその壁を打ち破ろうとしています。現在、カードの不正利用被害は年間で数百億円規模に達しており、主戦場は対面の偽造カードから非対面の番号盗用へと移りました。この被害を食い止めるための効果的な手段のひとつが偽サイトを閉鎖させるテイクダウンです。しかし、これを各社がバラバラに行う個社対応には、構造的な限界がありました。

――どのような限界があったのでしょうか。

辻中：フィッシングの狡猾な点は受益者と負担者が一致しないことにあります。例えばあるカード会社の利用者が EC サイトなどの偽サイトで情報を盗まれたとします。このとき、ブランドを悪用された側の企業には直接の金銭被害が出ないケースが多く、対策コストを投じる動機が生まれにくい。一方で実害を被るカード会社側は他社の偽サイトに直接対応するスキームがなく、対応が後手に回らざるをえなかったのです。

山本：攻撃者はその“企業の隙間”を突いてきます。JPCERT/CC には週に 5 万件もの報告が寄せられますが、個別の企業がそれぞれに動いていてはサイト量産のスピードに到底追いつけません。

辻中：この個社の限界を痛感し、JCCA は業界の枠組みを超えた共同運用に踏み切りました。本来、カード業界は激しいシェア争いを繰り広げる競合他社の集まりです。しかし、セキュリティに関しては協調領域であると定義し直しました。

――具体的にはどのような連携体制を構築されたのですか。

辻中：銀行系、流通系、通信系などのクレジットカード会社主要 8 社が足並みをそろえました。我々 JCCA がハブとなり、一括してテイクダウンを依頼するプラットフォームを構築しました。

櫻澤：この取り組みの意義は極めて大きいと思います。セキュリティホールをひとつでも残せば、攻撃者はそこを集中砲火します。逆に日本を代表する 8 社が強固なガードをつくれば、攻撃者にとっての ROI（投資対効果）が悪化する。彼らもビジネスでやっている以上、手間がかかり収益の上がらない市場からは撤退せざるをえなくなります。

辻中：8 社がまとまるまでには各社の運用フローの違いやコスト負担など多くの調整が必要でした。しかし、「顧客を守るために業界全体を守る」という視点で一致できたことが本プロジェクトの原動力となりました。

山本：各 ISAC（業界内での情報共有・連携の取り組み推進を図る組織）では、ビジネスではライバル同士の企業がセキュリティの現場では情報を共有し合っています。ビジネスでは戦い、セキュリティは協力し合うという意識が根付き始めているように見受けられます。

金融犯罪対策を目的にクレジットカードの主要8社が団結しました。
この動きは、他の業界にも必要な取り組みであると考えています。
辻中伸幸

つじなか・のぶゆき◎日本クレジットカード協会事務局長。2008年、三井住友カードに入社。主にアクワイアリング（加盟店業務）に関する管理・営業企画・推進業務、経営企画部で渉外業務に従事。25年度より現職。

攻撃は業種や企業規模を問いません。
だからこそ、産官学が情報を共有することが不可欠です。
山本健太郎

やまもと・けんたろう◎JPCERT コーディネーションセンター 国内コーディネーショングループマネージャー。大手通信事業会社を経て2009年に着任。フィッシング対策の責任者として週5万件超の報告を基に国内外のフィッシングサイト停止調整などを指揮。

トルツメ

「不祥事」から「誠実な開示」へ

――企業が自社の被害情報を開示することには、依然として心理的な抵抗が強いように感じます。

山本：対策の第一歩は現状を正しく把握することしかありません。ある企業の経営理念に「見えないものは管理できない」という言葉がありますが、サイバーセキュリティにおいても同じです。攻撃の実態がブラックボックス化されている限り、有効な資源配分も迅速な意思決定も不可能です。

櫻澤：見える化を阻んでいるのが日本企業に根強く残る「被害＝不祥事」という観念ではないでしょうか。米国では被害を受けたのは対策不足の結果ではなく、攻撃者が執拗に隙を突き続けた結果であるという認識が広がりつつあります。被害事実を伏せればインテリジェンスは共有されず、攻撃者は次の標的へと連鎖を広げていく。情報を隠蔽することは結果として攻撃者に猶予を与え、被害の拡大に手を貸すことになってしまいます。

辻中：日本は対面決済における IC 化が欧米に比べて大幅に遅れたことで、世界中の不正組織から「日本は狙いやすい」と見なされ、攻撃が集中した過去があります。事実を直視し、業界全体で早期に情報を共有できていれば大きな被害は避けられたはずです。この失敗を現在のオンライン不正の現場で繰り返してはなりません。

山本：JPCERT/CC が検討会事務局の一員を務めた「サイバー攻撃被害に係る情報の共有・公表ガイダンス」をご参照いただければと思いますが、重要なのは事前の予行練習です。広報体制まで含めたシミュレーションを経営層が自ら行い、隠さず迅速に事実を説明する準備をする。その姿勢が企業への評価につながることは間違いないでしょう。

辻中：現在、クレジットカードを選ぶ基準として「セキュリティの強固さ」は多くのアンケートで上位に入っており、消費者から支持されています。セキュリティ対策をコストではなく、顧客との信頼を維持するための戦略的な資源配分としてとらえられるかどうかが、企業の存続を左右する時代になっています。

産官学の「知」が犯罪の ROI を破壊する

――犯罪を未然に防ぐための能動的な連携はどうあるべきでしょうか。

櫻澤：実効性のある産官学連携の理想像として、2025 年に結実したインドでのテクニカルサポート詐欺拠点の摘発事例を挙げたいと思います。摘発において決定打となったのは、民間企業のリサーチャーが 5 年という歳月をかけて収集し続けてきた膨大な痕跡のデータでした。民間がもつ情報資源を国家の執行力と結びつける。このふたつの力が面として機能することで、初めて攻撃者の生産性、つまり犯罪の ROI を徹底的に破壊することができた事例ですね。

山本：対策をさらに強くするには学術的な知見も欠かせません。「なぜ人は偽サイトへ誘導されてしまうのか」という行動心理を分析し、技術と啓発の両面から先回りして防ぐ。こうした能動的な連携がアクティブ・サイバー・ディフェンスの土壌となります。

辻中：対策が進んでいる英国やオーストラリアでは、行政が主導してフィッシング情報の一元管理やテイクダウンを一気通貫で行っており、不正利用の抑止に成功しています。日本でも各省庁、業界団体などが有機的に連携し、フィッシング被害を未然に防止するプラットフォームの構築が待ったなしの状況といえますね。

――これからのデジタル社会において経営者はセキュリティとどう向き合うべきか、お考えをお聞かせください。

山本：まずは自社がどのような攻撃にさらされているのかを正しく可視化すること。そして、その情報を ISAC や JCCA のようなプラットフォームを通じて共有する。ISAC において競合同士が手を取り合っているように、安全の領域では共助が最も合理的な戦略となります。また、攻撃を受けた際に経営者が迷わずハンドルを握れるよう、広報体制まで含めたシミュレーションを日常に組み込むこと。こうした地道な取り組みが、企業のレジリエンスを最大化させると考えています。

辻中：クレジットカードについては利便性やポイントのみで選ばれる時代は終わり、セキュリティへの姿勢そのものが差別化要因になりました。自社に直接被害がないからと静観するのではなく、社会全体の信頼を守るために情報を分かち合う。この姿勢がお客様に安心を提供し、最終的に選ばれるブランドにつながっていくと考えています。

櫻澤：攻撃者は ROI を最大化させるために連帯しています。これに対抗するには守る側も有機的につながらなければなりません。経営者に求められるのはセキュリティを担当者任せの技術論にせず、経営戦略の中心に据える覚悟です。有事の際に自らの言葉で説明し、迅速にリソースを配分する。そのリーダーシップが犯罪者のエコシステムを打破し、日本のデジタル社会の健全性を守る最後の砦となると確信しています。F

Engineering Financial Confidence

提携金融機関600超の巨大インフラを守り抜く コンビニATMを祖業とするセブン銀行の矜持

堅牢なシステムで利用者と提携金融機関の安全を担保するセブン銀行。
セキュリティを熟知するエンジニアの代表取締役社長 松橋正明が考える「守りの鉄則」とは。

text by Motoki Honma | photographs by Daichi Saito | edited by Aya Ohtou (CRAING)

まつはし・まさあき◎セブン銀行代表取締役社長。釧路工業高等専門学校卒業後、日本電気エンジニアリング（現NECプラットフォームズ）入社。2003年アイワイバンク銀行（現セブン銀行）入行。15年常務執行役員、18年専務執行役員を経て、22年より現職。

ネット銀行を中心とした16機関が参加する金融犯罪対策検討会で、幹事を務めるセブン銀行。2019年には電通総研とともにサイバーセキュリティ企業を設立し、自社の防御ノウハウを他の企業も利用できるサービスとして提供するなど、業界横断のセキュリティ強化の一翼を担っている。

今や誰もがコンビニのATMを利用しているが、このサービスを日常の“当たり前”にしたのがセブン銀行だ。01年、セブン銀行（当時・アイワイバンク銀行）はコンビニ内に設置したATMを起点に、預金の入出金や振り込みなどを行う銀行としてスタートした。現在、ATMは全国に約2万8000台、提携金融機関は600を超え、年間の利用件数は約10億件にも上る。

この巨大な決済インフラを支える安全の礎を築いてきたのが、代表取締役社長 松橋正明（写真。以下、松橋）だ。松橋は、前職の日本電気（NEC）で図書館の蔵書検索システムの構築や、銀行窓口の伝票をデータ化するワークフローの設計など、アナログをデジタルに置き換えるプロジェクトを数多く手がけてきた人物である。

転機となったのはセブン銀行の設立。松橋はメーカー側のエンジニアとして同行初代となるATMの開発・提案を主導した“生みの親”のひとりである。03年、セブン銀行のサービスが本格始動するタイミングで同行への入行を決意。「自ら設計し開発したシステムだからこそ、誰よりもその中身を熟知している」と、現場に飛び込んだ。当時のATM設置目標は全国6,000台。しかし、セブン－イレブンの店舗増とともにATMの需要は爆発的に拡大する。松橋は急激に膨らむネットワークの安定性を担保しながら、同時にコンビニという場所特有のセキュリティ課題に直面することとなる。この現場での実体験が、のちの「利便性と安全性の高度な両立」という経営思想の原点となった。

提供側がお客さまを先回りして守らなければ
金融機関としての信頼は維持できない
松橋正明

※読点

利便性と安全性を技術の視点で両立する

巧妙化するフィッシング詐欺やサイバー攻撃に対し、松橋の経営判断は明快だ。松橋は「利用者の注意義務だけに頼る“利用者責任”の時代ではなくなった」と話す。

「サービスを提供する側がいかに先回りをしてお客さまを守り切るか。そのための工夫を怠れば、金融機関として選んでいただけなくなるという危機感をもっています」

この思いを具現化したのが業界に先駆けて導入してきた一連のメールセキュリティ対策である。11年には電子メールの暗号化・署名規格「S/MIME（エスマイム）」を導入。受信者の手元に届く前に不正メールを隔離する「DMARC（ディーマーク）」や、認証済みメールに企業ロゴを表示させる「BIMI（ビミ）」もいち早く採用し、利用者がメールを開く前の段階で視覚的に本物であることを確信できる仕組みを構築している。

こうした決断を迅速に下せるのは、松橋自身がシステム構造を知り尽くすエンジニアであることが大きい。16年ごろからAIや画像処理技術の変化を注視してきた松橋は、精巧な偽サイトが容易につくれる時代の到来を予見していたという。

現在、同行では口座の動きをリアルタイムで分析し、不正な取引を停止する技術を実装している。新たな手口を組み込み自動でブロックする仕組みには、AIも活用。SNSなどで募った送金バイトによる資金移動のパターンを見破る技術もそのひとつだ。松橋が先制防御を徹底する背景には、セブン銀行というブランドだけでなく、ATMを通じて接続する数百の金融機関を含む決済ネットワーク全体を守るという前提がある。

「信頼は一度でも失うと取り返しがつきません。ATMそのものに問題がなくてもインターネットバンキングの安全性が揺らげば、お客さまはATMを含めたすべてのサービスに不信感を抱くでしょう。全方位で安全性を高め続けなければ、私たちが提供する価値を維持することはできないと考えています」

全方位の追求は創業時のATM開発から一貫している。例えば、画面ののぞき見を防ぐフィルターや手元を隠すバイザーの設置、そしてテンキーで入力した瞬間に情報を暗号化する。これらは今でこそ業界の標準だが、当時は利便性とのバランスを突き詰めた独自の工夫であった。また店舗に店員がいないATM専用店において、異常を瞬時に検知しリモートで対応するコントロールセンターの仕組みも構築。通信速度の制約もあったが、圧縮技術を駆使して現場の画像を送り、ワンクリックで警備員が駆けつける体制を整えた。

「リモートで把握し対処できるようにしたことは結果として少人数での運用を可能にし、大幅な省力化につながりました。当時の金融業界においてはネットワークを通じたリモート処理にIT投資を集中させるのは、いわば“逆張り”の戦略でした。安全性のための投資をいかに運用の効率化という価値に転換するか。このせめぎ合いのなかに我々が提供すべき本質的な役割があると考えています」

知見を社会へ還元し、社会に安全を届ける

セブン銀行はATM運営や口座事業で蓄積した知見と最新の攻撃手口に関する情報を、金融犯罪対策検討会などを通じて継続的に共有している。また、社内のCSIRT（シーサート／セキュリティインシデント発生時に緊急対応を担うチーム）が各金融機関と直接連携し、未知のアタックにも横断的に対処する体制を構築してきた。

「金融は経済の血液。だからこそ、このインフラは社会全体で守る責任があります。私たちは異業種から参入した身であることから新しいテクノロジーを柔軟に取り入れてきました。ここで得た知見を共有することで、より安全な社会をつくっていきたいと考えています。また、EC事業者や運送業といった金融業以外の業種も同様です。サイバー攻撃は我々のような企業に限ったことではありません。IDやパスワードを管理する企業はすべて守るべき対象です。危険な状況にある事業者がいれば即座に情報を提供する。こうした取り組みが安心で安全な社会をつくるうえで重要だととらえています」

加えて、金融庁主導によるサイバーセキュリティ訓練のほか、自主的な演習も実施。これらは全社的な取り組みとしてセキュリティ意識の底上げを図ることを目的としている。松橋は「セキュリティ対策に終わりはない」と断言する。

「今後、AIエージェントが旅行の予約から決済までを完結させるような時代になれば『人間による本人認証』を前提としたセキュリティの考え方そのものが揺らぐ可能性があります。ゼロトラストを含むあらゆる仕組みは“完成形”として固定するのではなく、一度つくったものを自ら壊すビルド・アンド・スクラップを繰り返し、アジャイルに進化させていく必要があると考えています」

技術の進化を読み解き、先手を打って実装し続ける。その絶え間ないアップデートの積み重ねが、決済インフラを担う側が果たすべき責任のかたちといえるだろう。F

Strategic Security Investment

意思決定を遅らせる“分断”をどう乗り越えるか
横浜銀行が専門人材と兼務体制で築いた防衛の実効性

犯人の収益性を削り、早期撤退へ追い込む。横浜銀行が実践するサイバー防衛は、極めて戦略的だ。
複数部門が密に連携し、有事の意思決定を加速させる独自の運営モデル。創業100年余の信頼を次世代へつなぐ、攻めの守りとは。

text by Motoki Honma | photographs by Daichi Saito | edited by Aya Ohtou (CRAING)

かたやま・あきら◎横浜銀行ITソリューション部セキュリティ統括室リーダー兼リスク管理部マネロン等金融犯罪対策室リーダー。都市銀行系のシステム子会社に入社後、非対面チャネルのシステム開発に従事。2019年より警察機関に出向し、サイバー犯罪捜査官として活躍。22年横浜銀行入行。

たけなか・ゆきこ◎横浜銀行デジタル戦略部マーケティング戦略室ダイレクトチャネル企画グループプロフェッショナル兼リスク管理部マネロン等金融犯罪対策室リーダー。大学卒業後、関西の金融機関にて窓口業務やシステム開発に従事。2009年横浜銀行入行。20年より現職。

横浜銀行はサイバーセキュリティを、経営基盤そのものを支えるための不可欠な投資と定義している。2022 年 4 月に策定した「サイバーセキュリティ経営宣言」について、ITソリューション部セキュリティ統括室でサイバーセキュリティ対策の実務を担う片山晃（写真左。以下、片山）は、次のように述べる。

「サイバーセキュリティを経営課題として正面から議論する土壌ができたことで、短期的な対症療法にとどまらず、将来的なサイバー攻撃の脅威を見据えた準備を計画的に進めやすくなりました」（片山）

22 年にはセキュリティ統括室を新設。それまでシステム部門が開発ルールの延長線上で管理していた体制を改め、専任組織として独立させた。警察機関でサイバー犯罪捜査官を務めた経験をもつ片山を含むサイバーセキュリティの専門人材を中核に据え、パートナー企業を含めた約 25 人体制の専任組織へと拡張。経営課題としてのガバナンスと、現場における実効性の高い実行力を両立させる構造を構築している。

組織の壁を越える兼務体制が強固な防衛ラインを築く

同行のサイバー犯罪対策における最大の特徴は、リスク管理部門である金融犯罪対策室に、デジタル戦略部とセキュリティ統括室の担当者が兼務で加わる体制を構築している点だ。デジタル戦略部で商品企画を担う竹中由起子（写真右。以下、竹中）は、過去に勘定系システムの内製化におけるシステム開発や共同利用システムへの移行プロジェクトに従事したエンジニアとしての背景をもつ。

「非対面チャネルのサービスにおいて、私が商品企画の目線から、片山がサイバーセキュリティの目線から金融犯罪対策の助言を行います。これにより、犯罪手口や脅威情報に対し、商品特性を踏まえたビジネス判断を現場レベルで直結させることが可能です。金融犯罪対策では、犯罪手口や脅威情報に基づいたモニタリングルールの検討と現場への迅速な反映が不可欠です。当体制では、技術的エビデンスに基づいた実効性の高い対策を構築できる仕組みを整えています」（竹中）

この緊密な連携は、有事における迅速な意思決定の基盤としても機能する。フィッシング攻撃や不正送金の予兆を検知した際、セキュリティ統括室がフィッシングサイトや不正アクセスの状況を即座に分析して攻撃手法を特定し、金融犯罪対策室が攻撃手法から有効な取引制限の方法を検討、デジタル戦略部およびコールセンター部門が顧客影響を判断するという、4つの部署が一体となったスクラム体制を構築しているのだ。また、コールセンター部門と緊密に情報を連携することで、顧客対応への迅速な初動を可能としている。

「攻撃を確認してからアプリ上の注意喚起や取引制限を完了させるまで、短時間で対応することができます。また、コールセンターを自前で運用しているので、システム上の変更内容を即座に共有し、お客さまからの問い合わせに対して一貫した回答を用意できる体制となっています」（竹中）

サービスの取引制限による技術的防御と、アプリなどの注意喚起、そしてコールセンターによる顧客への説明責任を同時並行で完結させる。この実効性が横浜銀行の強みとなっている。片山はサイバー犯罪の本質を次のように分析している。

「攻撃コストが犯罪により獲得する収益を上回れば、犯人は利益を得られないため攻撃を断念する。いかに犯人側の収益性を削り、早期撤退に追い込むかが防御の要となります。23 年にフィッシング攻撃を受けた経験を糧に、現在は対応スピードを飛躍的に向上させ、検知から 1 日以内、あるいは当日中に犯人を撤退させることが可能となっています」（片山）

またフィッシング対策をリスクに応じて多層化している点も独自の取り組みといえる。

「第三者の不正利用が明らかな場合は即座に遮断しますが、判定が難しい場合は追加認証を求め、お客さま自身での解決を促します。普段お取引されないお客さまの急な高額振込など、還付金詐欺やロマンス詐欺が疑われるケースではシステム制限に加えて直接の架電確認を行う。このように、リスクの性質に合わせた柔軟な対応を徹底しています」（竹中）

外部知見を組織の知恵へ進化を止めない防衛戦略

外部ソリューションを活用する企業のなかにはツールの導入自体が目的化し、運用が形骸化してしまうケースも少なくない。対して同行は導入後の運用に重きを置いている。

「優れたツールも、どう使いこなすかが大切です。入手した犯罪手口や脅威を基に、システム強化や顧客保護のためにどう動くのか。外部の知見を精度向上のための素材として取り込み、自組織の運用に合わせて昇華させていくプロセスがあって初めて、対策は機能すると考えています」（竹中）

一方、片山は「セキュリティをより強化するには他行との情報共有が欠かせない」と話す。実際、横浜銀行は日本サイバー犯罪対策センターや金融 ISAC を通じて最新の攻撃動向などを収集するほか、地方銀行との連携も深めている。

「セキュリティにおいて他行はライバルではなく、ともにお客さまをお守りするパートナーです。こうした協働は結果として、金融インフラを守ることにつながると考えています」（片山）

共有された情報を即座に現場の防衛力へと反映させるのが竹中の役割のひとつでもある。他行で発生した手口が波及するまでのタイムラグを利用し、コールセンターや金融犯罪対策室への情報共有を済ませておく。こうした先回りの対応が、創業 100 年余を誇る横浜銀行としての信頼を守る盾となっている。

生成 AI の普及によりボイスフィッシングなど攻撃の手口が巧妙化するなか、同行は顧客の資産を預かる銀行として信頼を支える防衛基盤をアップデートし続けている。単一のシステムに依存せず、専門知見と組織の機動力を統合した運営モデルは、進化を止めることができないサイバー犯罪に対する戦略的な防衛策といえるだろう。

優れたツールを導入するだけで終わりではなく
情報を基に、組織に即した対策を講じることが重要です
※読点
竹中由起子

セキュリティにおいて他行はパートナー。
知見を共有し合うことが未然防止に役立ちます
※読点
片山晃

Vision for Sustainable Security

終わりなきデジタル社会を生き抜く経営者がもつべき視座とは

**本誌では、サイバー攻撃の実態とそこから生じるリスク、さらに企業連携による防衛の取り組みを見てきた。
では、未来の安全を経営者はどう築いていくべきなのか。
国内最大規模のサイバーセキュリティネットワークを構築してきたふたりの視点から、そのヒントを探る。**

▲photographs by Daichi Saito▲

illustration by Ryota Okamura | text & edited by Aya Ohtou (CRAING)

独自の検知技術でサイバー攻撃を予知、防御するアクシオン 代表取締役の安田貴紀（以下、安田）と瀧下孝明（以下、瀧下）。瀧下は近い将来、AI を介した意思決定が当たり前になれば、インターネット空間における脅威は、従来とは異なる次元へと変化すると指摘する。

「人が AI エージェントとの対話を通じて知見を深め判断を下すようになるなかで、AI が参照する情報にフェイクが紛れ込んでいたらどうなるのか。あたかも正しい情報として提示されたものを人が鵜呑みにしてしまう。こうした前提自体がフェイクである世界は十分に起こりえると考えられます。自社のサービスが他社のサービスや情報とつながるとき、接続先や参照元は果たして信用できるものなのか。今後はそこまで含めた対策が不可欠になるでしょう」（瀧下）

一方安田は、企業間の情報格差は、結果としてサイバー攻撃に脆弱な企業を生みかねないと指摘する。そのうえで、個社対応だけでは攻撃の実態をとらえきれず、企業間の協働が重要だと説く。

「我々のようなセキュリティ企業は、フィッシング詐欺の発生地や手口を時系列で把握しています。しかし各企業が認識できるのは自社への攻撃に限られ、背後にある流れまでを見通すことは難しい。例えば、神奈川県で発生した攻撃が静岡県へと移り、次に自社エリアが狙われる兆候があったとしても、企業間で情報が共有されていなければ迫り来る危機を察知することはできません」（安田）

こうした情報の格差は対策を後手に回らせるだけでなく、攻撃手口やその進化の把握を困難にする環境を生む。その一例として瀧下は、現在起きている「機械 VS 機械」の攻防の一端を明かす。

「最近ではスマートフォンの加速度センサーを悪用した手口が出てきました。フィッシングを仕掛ける側は、アクセスしてきた端末の微細な手ブレを検知。静止していれば調査用機械からのアクセスだと判断し、接続を遮断する。これは内部構造を見破られないようにするとともに、攻撃対象である人間を確実に狙うための対策と考えられます」（瀧下）

テクノロジーが変容し続ける以上、セキュリティに完成はない。安田は、高度化・巧妙化するサイバー攻撃への対策を戦略的投資ととらえ、企業が透明性をもって手を取り合う必然性を強調する。

「システムを構築したら終わりではなく、サステナブルに変化し続ける対策が重要です。そのためには各社が情報を開示し、協働する姿勢が欠かせません。対岸の火事を自社の予兆として取り込み、未知の脅威に柔軟に動ける体制を整えていく。自社が最初の標的となった際は情報を開示し、他社が対策できる環境をつくる。そうした実践の積み重ねが、デジタル社会の安全性を高め、ひいては企業のブランド価値となるはずです」（安田）F

安田貴紀

やすだ・よしき◎アクシオン代表取締役。2004年セブン銀行入社、14年より金融犯罪対策部にて金融犯罪対策の構築を企画推進。15年に7BK-CSIRTを立ち上げ初代リーダーを務める。18年にアクシオンの立ち上げに参画、19年より現職。20年よりフィッシング対策協議会 運営委員に就任。

瀧下孝明

たきした・たかあき◎アクシオン代表取締役。2001年電通国際情報サービス入社。金融領域におけるコンサルティングおよびマーケティングを統括。著書に『金融マーケティングの考え方とやり方』（金融財政事情研究会）。19年アクシオン創業に取締役として参画、25年より現職。

Radical Transparency
サイバー脅威から企業をどう守るか
「攻めの透明性」という新戦略

2026年3月発行
（内容・役職は26年3月時点のもの）

制作	Forbes JAPAN Brand Studio ソーンマヤ
編集	大藤 文（CRAING）
デザイン	株式会社direction Q
校閲	株式会社聚珍社
企画プロデュース	Forbes JAPAN Business Design 谷口幸平
企画	株式会社ACSiON（アクシオン）
印刷・製本	株式会社美松堂
発行	リンクタイズ株式会社