Deloitte.
Private

ファミリービジネスのサイバーセキュリティ（2026年）

ファミリービジネス インサイト シリーズ

インタラクティブナビゲーション

本レポートはインタラクティブな体験を提供するように設計されています。レポートをAdobe Acrobatで開き、お使いのコンピューターにダウンロードすることで機能をご利用いただけます。Adobe Acrobatをお持ちでない場合は、無料でダウンロードできます。Adobe Acrobatを利用しない場合、またレポートをコンピューターにダウンロードしない場合、インタラクティブ機能の一部または全てが利用できない場合があり、ファミリーオフィスについての調査結果を細部にわたって閲覧できないことがありますのでご注意ください。

Adobe Acrobatをダウンロードするには、ここをクリックしてください。

目次

序文

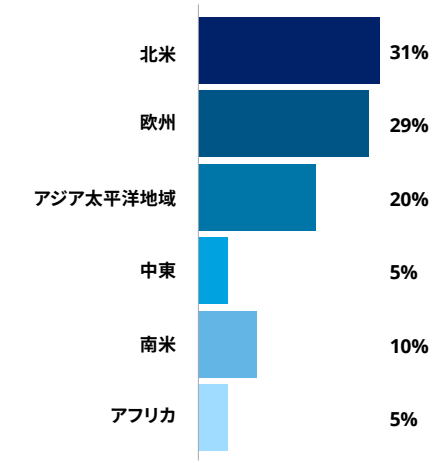
Deloitte Private 発行「ファミリービジネス インサイト シリーズ」の「ファミリービジネスのサイバーセキュリティ」レポートへようこそ。本シリーズを構成する5つのレポートでは、「ファミリービジネス業界の世界的な進化と特徴」、「サイバーセキュリティ」、「デジタルトランスフォーメーション」、「承継計画と次世代」、「ファミリービジネスのトップエグゼクティブからのアドバイス」について掘り下げていきます。

本号では、ファミリービジネスにおけるサイバー攻撃の発生状況、現在の防御手段、今後のサイバー攻撃に備えて講じ得る防御策を考察します。

インサイトを得るために、2025年3月～6月に、収益が1億米ドル以上、かつ、ファミリーが株式の過半数（51%以上）を保有する世界中のファミリービジネス1,587社のシニアエグゼクティブを対象とした調査を実施しました。2024年、対象のファミリービジネスの収益は平均で28億米ドル、合計すると4兆4000億米ドルとなりました。また、調査に加えて、ファミリービジネスのシニアエグゼクティブ30人に詳細なインタビューを行いました。対象者の多くは、数十億米ドル規模の資産を持つファミリーの当主や、100年以上の歴史を有するファミリービジネスの経営トップです。これらのインタビューにより、ファミリービジネスが競争環境で勝ち抜き、長期的な成功を目指すうえで役立つ貴重な示唆とアドバイスを得ました。

これらのインサイトが、ファミリービジネスのサイバーセキュリティ施策を策定するうえで役立つことを願っています。また、惜しみなく時間と意見を共有してくださった調査参加者の方々に心より感謝申し上げます。

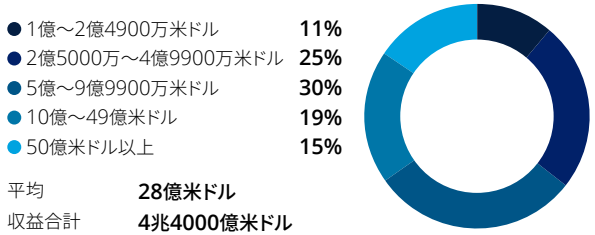
調査に回答したファミリービジネスの地域統括会社の所在地域



ファミリービジネスの年間収益（2024年）

各ボタンをクリックすると、データが表示されます。

グローバル | 北米 | 欧州 | アジア太平洋地域 | 中東 | 南米 | アフリカ



平均 **28億米ドル**

収益合計 **4兆4000億米ドル**

重要なポイント

サイバー攻撃が蔓延する現状

世界のファミリービジネスの約4分の3（74%）は、過去2年間に少なくとも1回のサイバー攻撃を受けており、3分の1（33%）は2回以上の攻撃を受けています。つまり、世界のほぼ全域がサイバー攻撃の脅威にさらされているのです。アジア太平洋地域が最も攻撃の頻度が高く、90%のファミリービジネスが少なくとも1回の攻撃を受けています。さらに、南米（61%）から北米（77%）に至るまで、いずれの地域でも過半数をかなり上回る割合のファミリービジネスが少なくとも1回の攻撃を受けています。

多様なサイバー攻撃

サイバー攻撃には、マルウェア（被害に遭ったことがある回答者の割合：49%）、フィッシングやビジネスメール詐欺（48%）、ソーシャルエンジニアリング（43%）、サードパーティリスク（40%）、インサイダー脅威（27%）など、さまざまな形態があります。

より堅牢なサイバーセキュリティ防御策の必要性

このような脅威が蔓延しているにもかかわらず、期待どおりに機能する「強固な」サイバーセキュリティ戦略を有していると回答したファミリービジネスは、世界全体でわずか43%にとどまっています。これを上回る割合（57%）のファミリービジネスがそうした戦略を策定しておらず、現在の戦略には不十分な点があるという認識を示す回答が49%、戦略は一切ないという回答は8%となっています。結果として、サイバー攻撃に対する準備状況は中程度であると考えるファミリービジネスは39%、全く準備できていないとするファミリービジネスは9%で、全体では半数近く（48%）に及んでいます。

基本的な防御策は普及している一方、先進的な対策には遅れも

現在、ほとんどのファミリービジネスは、ソフトウェアの更新（59%）、ネットワークセキュリティ（57%）、多要素認証（MFA）やパスワード管理（57%）、データのバックアップ（48%）などの基本的な第一線のセキュリティ対策に依存しています。しかし、インシデント対応プレイブック（40%）、サイバー成熟度評価（36%）、ベンダーガバナンス（32%）、アイデンティティ管理（31%）などの高度な機能の活用はそれほど普及していません。基本的なサイバーハイジーンの実施は無差別攻撃に対する防御には有効ですが、巧妙な攻撃への防御には高度化した対策の方が優れている場合が多いのです。

広く見られるようになった負の結果

限定的な防御策しか講じていないため、多くのファミリービジネスがサイバー攻撃によって損失や損害を被ることは一般的になっています。実際、攻撃対象となったファミリービジネスのほとんどが、財務上（54%）、業務上（51%）、評判上（51%）の損害を受けています。損失や損害を被っていないという回答は世界全体でわずか4%であり、サイバーレジリエンスの実現に向けて対策の強化が必要であることを明確に示す結果となっています。

1　サイバー攻撃の発生状況

サイバー脅威は通常、事前に通知されることはありません。本物のように見える電子メール、脆弱なサプライヤー、システムアップデートの見落としなどを通じて、気づかないうちに侵入してきます。攻撃を受けると、その影響は金銭面だけでなく、個人的な面にも影響が及ぶと感じられることがあります。ファミリービジネスの場合、侵害は、単にビジネスを混乱させるだけではありません。それまで慎重に築いてきた評判とファミリーレガシーが損なわれる危険があるのです。

この問題は、地域や市場を問わず、広範囲に及んでいます。シンガポールからサンディエゴに至るまで、そして世界中のファミリービジネスが、状況に違いはあっても、同じようなデジタルの脆弱性の問題に苦心しています。一部のファミリービジネスは、クラウドサービスやデジタル決済、AI搭載ツールを驚異的なスピードで導入し、未来に向けて果敢に突き進んでいますが、そのスピードに防御策の進化が追い付いていないケースが見られます。また、慣れ親しんでいるとはいえ、それ自体にさまざまな課題がある古いシステムに固執するファミリービジネスもあります。いずれの場合においても、ファミリービジネスの間では、サイバーセキュリティは現状維持のみを目的とした取り組みではないという認識が広がっています。現在のファミリービジネスがどの程度競争力を維持できるかを決定づけるのみならず、次の世代にどのような事業を引き継ぐかを決定づける戦略的選択がサイバーセキュリティなのです。

ファミリービジネスの４分の３がサイバー攻撃の標的に

本調査のデータでは、世界中のファミリービジネスに対するサイバー攻撃の広がりと地域差という両方の傾向が浮き彫りになっています（図1.1）。過去２年間に少なくとも１回のサイバー攻撃を受けたとする回答が世界全体では74%に達し、その割合はアジア太平洋地域（APAC）を拠点とするファミリービジネスが最も高く（90%）、南米が最も低い（61%）結果となりました。この差は、地域間において、エクスポージャー（サイバー攻撃にさらされるリスク）やデジタル化の程度が異なることに加え、報告事項や規制環境、サイバーレジリエンスの成熟度が異なることを反映しています。

アジア太平洋地域においてエクスポージャーが高いことの背景として、この地域でデジタル化が進んでいることが挙げられます。また、77%がサイバー攻撃を受けたとする北米のデータは、デジタルへの依存度の高さと攻撃者にとって魅力的な地域であることの両方の特性を反映しています。

これとは対照的に、欧州のファミリービジネスはエクスポージャーが比較的低く（67%）、３分の１はサイバーインシデントが発生していないと回答しています。欧州のこうした状況は、データの取り扱いの厳格化や侵害報告、サイバーセキュリティ基準の整備を企業に促してきた一般データ保護規則（GDPR）に関連している可能性があります[1]。

1　サイバー攻撃の発生状況

図1.1：ファミリービジネスにおける過去２年間のサイバー攻撃発生状況
（攻撃成功の有無は問わない）

グローバル | 北米 | 欧州
アジア太平洋地域 | 中東 | 南米
アフリカ

- 攻撃を1回受けた　41%
- 攻撃を2回受けた　26%
- 攻撃を3回以上受けた　7%
- 攻撃されていない　26%

サイバー攻撃の種類：

- **フィッシングやビジネスメール詐欺（BEC）：**広く横行している手口で、一見本物に見える電子メールを使い、サイバー犯罪者が従業員を標的にして、資金の移動、機密情報の開示、マルウェアのダウンロードを行うよう仕向けるものです。フィッシングには、SMS（ショートメッセージサービス）を利用した「スミッシング」、電話や留守番電話による「ビッシング」もあります。
- **マルウェア：**「被害者のデータやアプリケーション、オペレーティングシステムの機密性、完全性、可用性を損なうこと、被害者に損害や混乱、業務障害を引き起こすことを目的として、通常は密かにシステムに侵入するプログラム」です[2]。マルウェアの一般的な例として、ランサムウェア（金銭的要求が満たされるまで被害者のITシステムを人質に取るタイプのマルウェア）があります。
- **ソーシャルエンジニアリング：**個人を標的にして、資金の移動や機密情報の公開などの危険な行為を実行させることです。ソーシャルエンジニアリングの最も一般的な形態は、フィッシングやBEC、プリテキスティング（被害者を信用させ、サイバー犯罪者を信頼できる人物と信じるように仕向けるもの）です。
- **サードパーティリスク：**組織のシステムやファイルにアクセスできるサードパーティ（サプライヤー、請負業者、パートナーなど）がビジネスに損害や悪影響を及ぼすリスクです。意図的なもの（悪意のあるアクターが引き起こす結果）と意図的でないもの（サードパーティへの攻撃の影響が組織に及ぶことによる結果）があります。
- **インサイダー脅威：**従業員が意図的に機密情報にアクセスする場合を指します。データ操作や窃取、漏洩などの形で発生すると考えられます。

1 サイバー攻撃の発生状況

最も一般的なサイバー攻撃はマルウェアとフィッシング

世界中のファミリービジネスは、マルウェアやフィッシングからインサイダー脅威、サードパーティの脆弱性に至るまで、さまざまなサイバー攻撃に直面しています（図1.2）。

世界全体では、マルウェアによる攻撃を受けたと回答したファミリービジネスが半数近く（49%）に上り、フィッシングやビジネスメール詐欺（BEC）（例：横行する偽装電子メール詐欺）が48%、ソーシャルエンジニアリングが43%となっています。こうした数字は、サイバー犯罪者がさまざまな方法で人的・技術的な弱点に付け込み、脅威が増大し続けている状況を表しています。

地域別のデータでは、顕著な差が明らかになっています。世界全体では、マルウェアによる攻撃を受けたとする回答が最も多く、49%に上っています。そして、北米では54%、欧州ではこれをやや下回る45%と、デジタルで相互接続された市場にマルウェアが存在していることは確かでしょう。しかし、デジタル化が進んでいない市場でもマルウェアが横行しており、アフリカでは56%、南米では50%のファミリービジネスが攻撃を受けています。国際刑事警察機構（インターポール）発行の「Africa Cyberthreat Assessments Report 2025」では、アフリカにおける最も一般的な脅威として、ランサムウェアやバンキング型トロイの木馬、マルウェア・アズ・ア・サービス（MaaS）を引き続き挙げており、モバイル端末やデジタル技術が急速に普及する一方、インシデント対応能力にばらつきがあるために、こうした脅威が増大しているとしています[3]。また、北米では、価値の高いデータを持ち、デジタルへの依存度が高い企業が、攻撃者にとって魅力的な標的となっています。Verizon発行の「2025 Data Breach Investigations Report（2025年度データ漏洩／侵害調査報告書（DBIR））」においても、システム侵害の大半がランサムウェアと窃取した認証情報の利用によるものであるとしています[4]。

サイバー脅威が単独で発生することはほとんどありません。例えば、ソーシャルエンジニアリングは、ランサムウェアなど技術的にさらに高度な攻撃手法の経路になる場合が多いことが研究で示されています。こうした意味で、インサイダー（内部関係者）は知らず知らずのうちに、さまざまな形の脅威を増大させる可能性があります。この問題は、報告、規制環境、サイバーレジリエンスの成熟度の違いを考慮すると、真にグローバルなサプライヤーエコシステムではさらに深刻になります。

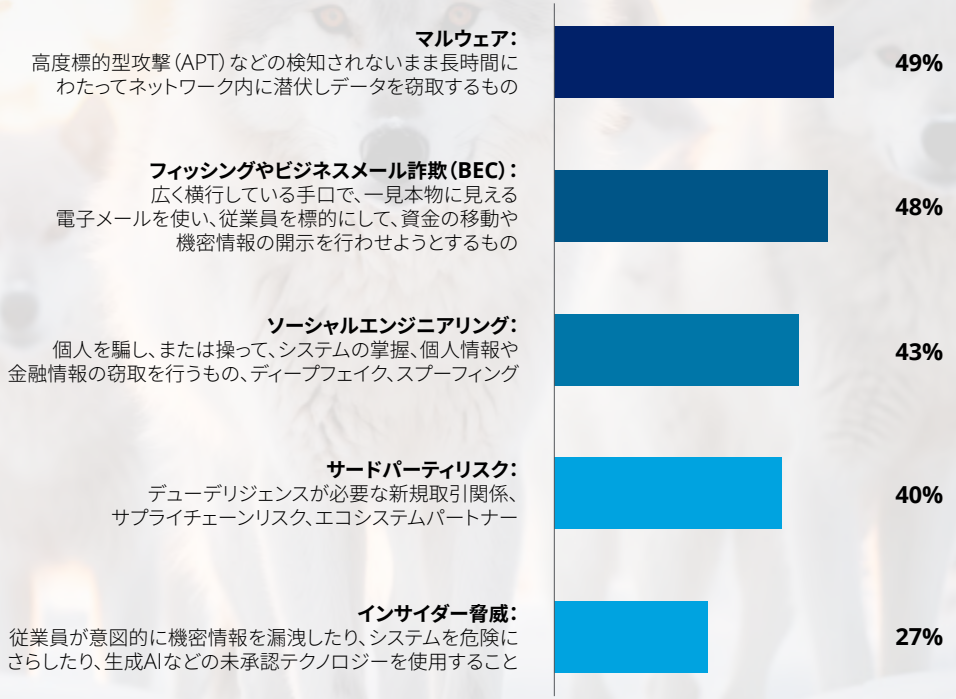
サイバー攻撃による損害や損失の例

- **財務：**財務上の損失はさまざまな形で発生する可能性があります。例えば、システムやファイルへのアクセスを回復するための身代金として攻撃者に金銭を支払うことで、直接的な損失が発生します。また、この種の攻撃は業務のダウンタイムによる追加の金銭的損失を招く可能性があり、ファミリービジネスの事業運営や、ファミリーへのサービス提供能力に直接影響が及ぶことになります。さらに、攻撃を受けた事実が公になれば、評判やブランド価値が低下し、結果として財務リスクが生じる可能性があります。
- **業務：**サイバー攻撃は、機密データの損失、従業員の士気（およびその後の定着率）への悪影響、オフィスでのリーダーシップの交代を生じさせ、結果的に業務の混乱を招くこともあります。例えば、マルウェア攻撃によって組織のITシステムが停止され、業務が中断して収益が失われる結果になる場合があります。
- **評判：**サイバー攻撃は、メディアによる否定的な報道など評判の毀損につながる可能性があり、攻撃を受けたファミリーやファミリービジネスと仕事をすることにサードパーティ（潜在的な貸し手、投資管理会社、その他のファミリーなど）が消極的になる可能性があります。

1　サイバー攻撃の発生状況

図1.2：ファミリービジネスが受けたサイバー攻撃の種類（複数選択可）

グローバル | 北米 | 欧州 | アジア太平洋地域 | 中東 | 南米 | アフリカ



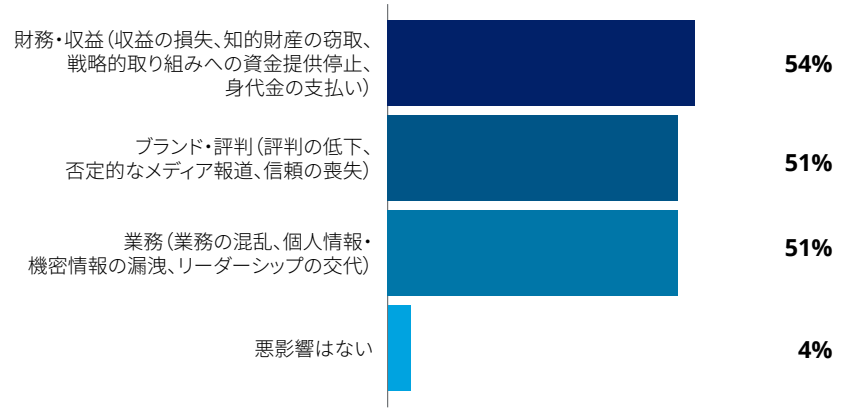
現代のサイバー攻撃が及ぼす甚大な影響

グローバルでは、ファミリービジネスに対するサイバー攻撃の影響は、財務（回答者の54%）、評判（51%）、業務（51%）の各側面に等しく及んでいます（図1.3）。この結果は、一回の侵害が金銭的損失、評判の毀損、業務の混乱を同時に引き起こし得るサイバーリスクの多面的な性質を明確に示しています。ランサムウェアや恐喝といった攻撃は資金流出、業務停止、評判の低下を直ちに生じさせる可能性があるため、これは当然の結果といえるでしょう。サイバー攻撃による被害がないと答えた回答者が相対的に少なかった（4%）ことは、現代のサイバー攻撃で悪影響を受けないことは稀であるという見解と一致しています。

> *従業員がフィッシング被害に遭い、社内システムは45日間にわたり攻撃者による不正アクセスを受けました。請求書の傍受と支払いのリダイレクトにより、50万米ドル超の損失が発生しましたが、取り戻すことはできませんでした。このインシデントにより、組織全体での強固なサイバーセキュリティ対策と警戒の重要性が明確になりました。*
>
> **ファミリー当主、CEO**
> 製造会社（米国）

図1.3：サイバー攻撃による負の結果（複数選択可）

グローバル | 北米 | 欧州 | アジア太平洋地域 | 中東 | 南米 | アフリカ



未来への備え：サイバーセキュリティ強化とデジタル技術導入で優位性を保つ、収益数十億ドル規模の企業の事例

今日の進化するリスク環境において常に機敏に対応し、安全を維持するために、サイバー防御の強化と新たなデジタルツールの導入をファミリービジネスがどのように進めているのかについて、米国を拠点とする大手消費財メーカーにお話を伺いました。

Deloitte Privateによる最近のファミリービジネス調査では、内部リスクとして最も多く挙げられたのはサイバー攻撃への対策の不備です。貴社では、この課題にどのように対処し、ビジネス全体でレジリエンスを構築していますか。

当社はサードパーティのサイバーセキュリティソフトウェアを使用していますが、完全な社内運用にすることで、常時制御と監視を行えるようにしています。最近導入したシステムでは、AIエージェントが信憑性の高い脅威をリアルタイムで検知します。これにより、従来のアプローチから大きく前進しました。以前は、セキュリティ運用センターの担当者がシステムを監視し、不審なアクティビティを通知していました。しかし誤報が多く、従業員はこうした通知への注意や緊張感を失っていました。今では、アラートが鳴ると、それが重要であることを皆が理解しています。

エージェント型AIはサイバー防衛において重要な役割を果たしている一方で、AIの利用拡大によるサイバー脅威はさらに高まっています。インサイトの獲得や意思決定に役立つAIツールを導入する企業が増えていますが、多くの場合、AIのスタートアップ企業と膨大な量の機密データが共有されています。こうしたスタートアップ企業はクラウドで事業を展開しており、セキュリティ・プロトコルの水準にもばらつきがあるため、新たな攻撃経路となり得ます。

このような脆弱性のため、当社ではAI利用において慎重なアプローチを取っています。セキュリティに保証はありません。また、選び抜いた業者であっても、実質的な保護を担保できていないケースが多いのです。AI革命に乗り遅れることを恐れてこの激流に飛び込む企業があるかもしれませんが、当社は堅実な道を歩んでいます。最先端で活動するよりも、迅速なフォロワーでありたいと思っています。

AIによるサイバー脅威であると認識して対応できるように、従業員にどのような準備をさせていますか。

AIの脅威は増大しています。企業がこの脅威を検知するのはますます困難になり、特により精緻で巧妙化した攻撃手法は厄介です。例えば、わずか数年前まで、フィッシングメールの多くはスペルミスやお粗末な文法から偽物だと容易に判別できました。しかし、今日ではAI生成により、攻撃者は従業員を容易にだましてクリックさせることが可能です。悪意のある攻撃者は、従業員の文体や口調をプロファイルし、信頼性の高いメールを生成することもできるのです。

サイバーセキュリティソフトウェアの活用に加えて、従業員への研修と情報提供を優先して行っており、サイバー攻撃のリスクとその防止のために果たすべき重要な役割について伝えています。組織の全ての従業員を対象にウェブキャストとライブセッションを定期的に行っています。最近のウェブキャストでは、最高情報セキュリティ責任者（CISO）が、財務担当シニアエグゼクティブのディープフェイク動画を冒頭で流しました。その人物が本物ではないと明かされると、皆が愕然としていました。このことがきっかけとなり、従業員がサイバー詐欺やサイバー脅威に目を向けるようになったのです。

CISOは、侵害された可能性があるときは隠さず、すぐに報告することの重要性を強調しています。脅威の封じ込めは一刻を争う事態ですし、ミスや騙されたことを理由に従業員を叱責すべきではないと考えています。これは重要なメッセージです。誰しも誤った判断で不利益を被るかもしれないと考えがちで、その結果、侵害の報告をためらう可能性があるからです。

サイバー攻撃で目立った被害を受けたことはありますか。

ツールの厳密な精度と社内の警戒心のおかげで、これまで防御に成功してきましたが、常に攻撃を受ける可能性があると認識しています。幸いなことに、当社が過去に直面した最も重大なインシデントによる被害額は、2万米ドル足らずでした。当社事業所の1つで業務を行う小規模なサードパーティのベンダーが攻撃され、ハッカーがシステムにアクセスして数カ月にわたってベンダーの活動を監視していたのです。ベンダーのオーナーは当社の買掛金チームと定期的に連絡を取り合っていたので、オーナーから新規の銀行口座に関するメールを受け取ってもチームは不審に思いませんでした。実際には、ハッカーがオーナーのシステムに侵入していたため、本人のメールアカウントから直接メッセージを送信できたというわけです。買掛金チームは侵害されたことに気づかず、要求通りに送金してしまいました。

問題が表面化したのは、後日、オーナーが未払いについて照会してきたときでした。残念ながら、FBIに通報してもオーナーは代金を回収できませんでした。そのハッカーを追跡できなかったのです。

このインシデントの後、当社は厳格な検証ポリシーを導入しました。支払いや口座変更は、電子メールのやり取りではなく、当社システム内の信頼できる連絡先によって個別に確認できた場合にのみ行います。最初のステップとして、全ての要求を検証する厳密なプロセスであるチェック・アンド・バランスが重要です。

ファミリービジネスに関するデロイトのレポートでは、「テクノロジー変革プラットフォームの構築」が今年の最優先事項となっています。この点での取り組みはいかがですか。

大手ソフトウェアプロバイダーとのパートナーシップを開始し、統合ツールプラットフォームを導入して、AIを搭載したチャットボットやアナリティクス、高度なアプリケーションを活用しています。これにより、当社のセキュリティプロトコルへの信頼を強化しながら、重要な分野で飛躍することができます。

また、コア業務システムの統合にも取り組んでいます。例えば、時間管理アプリケーションから作業現場のソフトウェアにデータを提供し、それをエンタープライズリソースプランニング（ERP）プラットフォームと人的資本プラットフォームに結び付けます。さらに、ビジネスの理解を深めるために、大規模な言語モデルとデータモデルの使用を開始しました。生産性レベルの測定に加えて、一部のチームがどのようにして常にスクラップ率を低く抑えているのかなど、ベストプラクティスを明らかにすることを目指しています。このようなチームを特定してスポットライトを当て、その成功を祝うことができれば、他のチームの改善にも役立ちます。

さまざまなシステムがあるため、対応の成果を今得ることはできませんが、こうした取り組みによって、詳細なインサイトを掘り起こし、より多くの情報に基づいた行動を取るために必要な可視性を高めています。

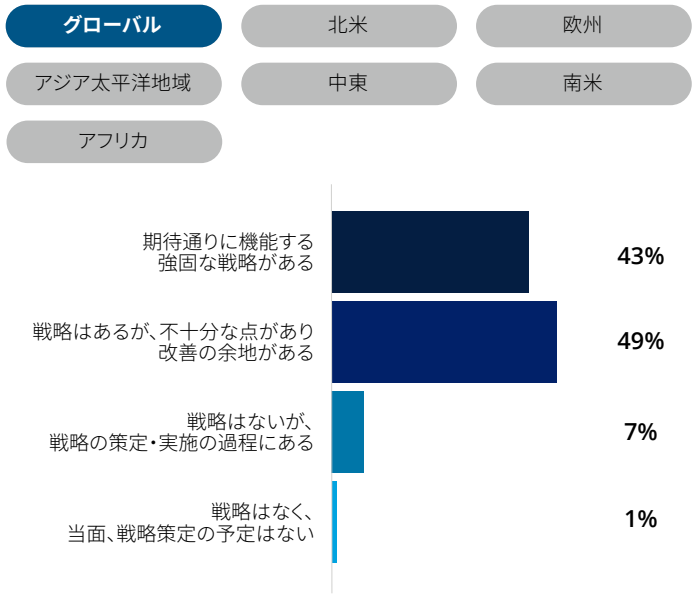
こうしたテクノロジーを展開すると同時に、従業員をより戦略的な役割に再配置しています。統合化の進んだデータにアクセスすることで、従業員はもはやタスクを完了するだけでなく、より賢明な意思決定を行い、ビジネスリーダーのように考えることを学んでいます。この進化は、当社の長年にわたる機敏性を重視した文化を反映したもので、ビジネスの変革に合わせて従業員が適応し、学習し、リーダーシップを発揮することができるようにしています。

2 サイバーセキュリティ戦略

ファミリービジネスの大半はサイバーレジリエンスが不十分な状態

ファミリービジネスの43%が「期待通りに機能する強固なサイバーセキュリティ戦略」を有していると回答したのに対し、過半数（57%）がそうした戦略を策定しておらず、49%が現在のサイバー戦略には不十分な点があり「改善の余地がある」という認識を示し、8%が戦略はないと回答しました（図2.1）。不十分な点に気づくことは最初の一歩であり、ファミリービジネスがサイバーセキュリティの重要性を認識していることを示す一方、この結果は、回答者の大半ではないにしてもその多くが、十分なレジリエンスや自社の戦略への自信を見せることができない現状も反映しています。こうした不十分な点を補うことが戦略上の必須事項となります。

図2.1：ファミリービジネスにおけるサイバーセキュリティ戦略の整備状況

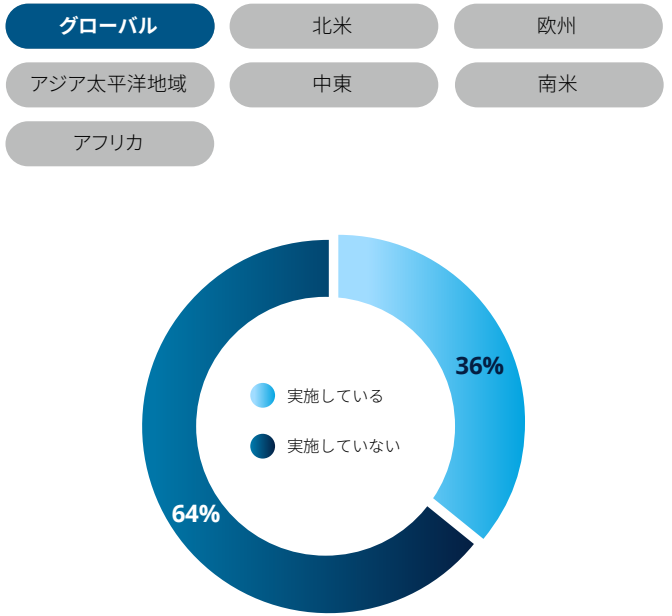


戦術的なサイバーセキュリティアプローチがファミリービジネスに人気

前述の憂慮すべき調査結果と整合するように、サイバー成熟度評価（業界最高水準に照らして、サイバー脅威の予防・検知・対応能力を評価すること）を実施しているファミリービジネスは3分の1強（36%）にすぎず、大半（64%）が実施していないことが明らかになりました（図2.2）。このことから、ファミリービジネスの多くが、国際標準化機構（ISO）が定めるような正式な成熟度プログラムや系統立った評価を利用するのではなく、戦術的にサイバーセキュリティ（パッチ適用、ウイルス対策、データバックアップ）を扱っていると考えられます[5]。

> *サイバー攻撃による重大な脅威を考慮して、当社は持株会社レベルでサイバーセキュリティを一元化し、全ての事業体に基準の整備と投資を義務付けています。このプロアクティブな全社的アプローチにより、脅威を早期に検知して軽減することが可能になり、ビジネスを保護し、夜もぐっすり眠ることができます。*
>
> **パートナー**
> 大手持株会社（米国）

図2.2：サイバー成熟度評価を実施しているファミリービジネスの割合



2　サイバーセキュリティ戦略

基本的な防御策は普及する一方、先進的対策の導入は遅れが見られる

現在、ほとんどのファミリービジネスは基本的なサイバーハイジーンを実施しており、最も根本的な対策を広範に導入しています（図2.3）。ソフトウェアの更新（59%）、ネットワークセキュリティ（57%）、多要素認証（MFA）やパスワード管理（57%）、データのバックアップ（48%）が世界的に広く実施されている代表的な対策です。ここに挙げたものは、主要なサイバーハイジーンのフレームワークによって承認されている、不可欠な「第一線の」防御策です[6]。その一方で、サイバー成熟度評価、ベンダーガバナンス、脅威インテリジェンス、インシデント対応プレイブック、アイデンティティ管理など、高度な対策の導入には依然としてばらつきがあり、明らかに普及が進んでいません。

基本的な対策と高度な対策の間のギャップは、地域間でも見られます。北米や欧州では、基本的な対策がしっかりと行われており、高度な対策も導入率がやや高い状況です（例えば、北米でのインシデント対応計画の導入率は46%）。GDPRなどの規制・コンプライアンス要件や過去の侵害に伴うコストの影響を受け、レジリエンスの強化やインシデント対応、ベンダーガバナンスへの投資が進んでいます[7]。アジア太平洋地域を拠点とする組織は基本的な対策を導入していますが、ガバナンス整備のスピードを上回ってデジタル変革が急速に進む中、これに応じたエクスポージャーに対処するための正式な成熟度評価やベンダーガバナンスが遅れています[8]。

全体として、このような不十分な点がファミリービジネスの戦略的課題となっています。基本的な対策を講じていれば多くの無差別攻撃を減らすことができるかもしれませんが、巧妙な攻撃やサプライチェーンの侵害など、財務や業務に重大な悪影響を及ぼし、ブランドの信頼低下も招きかねない事象による被害は、高度な対策（サードパーティリスク管理、アイデンティティガバナンス、時宜を得た脅威フィード、実践的なインシデント対応）によって抑えられる場合が多いのです。

> *サイバーセキュリティは主な重点事項であり、専任チームと外部パートナーが継続的にシステムを監視し、テストしています。取締役会は定期的に進捗状況を確認しており、防御を強化するために包括的な従業員研修とフィッシングのシミュレーション演習を実施しました。*
>
> **CFO**
> 製造会社（メキシコ）

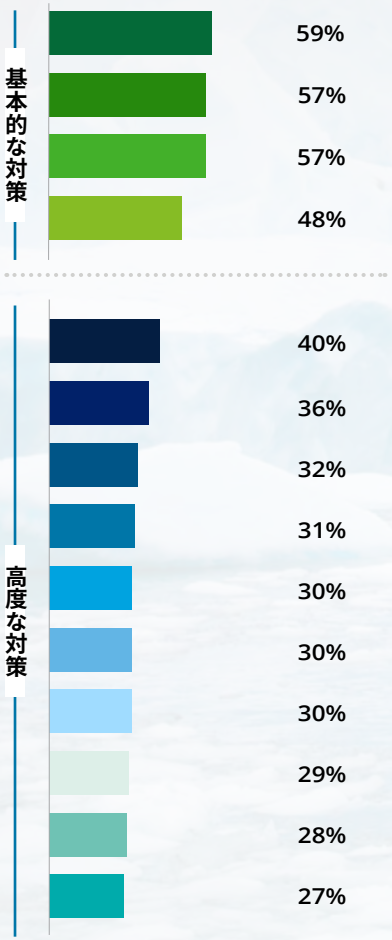
> *当社はリスク委員会を維持し、外部コンサルタントを起用してサイバーセキュリティを評価しており、二要素認証やオーストラリア標準の認定など、政府契約や防衛契約で求められる厳しい基準を満たしています。*
>
> **MD、ファミリーメンバー**
> 建設会社（オーストラリア）

> *サイバーセキュリティは、現代のあらゆる企業にとって常に変化し続ける課題です。当社もフィッシング攻撃やサイバー脅威に直面してきましたが、真の防御になるのは、徹底した従業員研修、手厚い保険、全てのインシデントを教訓にする姿勢です。*
>
> **President兼CEO**
> 小売業（米国）

2　サイバーセキュリティ戦略

図2.3：ファミリービジネスが現在取り組んでいるサイバーセキュリティ対策（複数選択可）

グローバル | 北米 | 欧州 | アジア太平洋地域 | 中東 | 南米 | アフリカ



- **ソフトウェアの更新（ウイルス対策ソフトウェアなど）：**ウイルス対策やファイアウォールの最新ソフトウェアに対応したコンピューターや電話などのデバイスのリスト、最新版ソフトウェアのインストールなど。
- **仮想プライベートネットワーク、安全なEメールツールなどの基本的なネットワークセキュリティ：**組織のネットワークへのアクセスにおける仮想プライベートネットワーク（VPN）の使用、パブリックWi-Fiとホームルーターの使用に関する接続デバイスポリシーの策定・運用。
- **強力なパスワードの使用と多要素認証：**重要なウェブサイトやアプリケーションなどにアクセスするには、2つ以上の情報が必要。
- **データのバックアップ（3-2-1ルール）：**データのコピーを3つ作成し、2つをそれぞれ異なる種類のメディアに、残り1つをオフサイトに保存。
- **強力なセキュリティポリシー（インシデント対応計画など）：**ソーシャルメディア、支払いなど日常業務のセキュリティに関連するポリシーと手順、および潜在的な脅威の監視・対応に関する明確なアプローチの積極的導入・実施。
- **サイバー成熟度評価：**組織環境における現在のサイバー成熟度、リスクの状態・レベルを、人材、プロセス、テクノロジーの観点から検証するための評価の実施。
- **サードパーティの管理サービスプロバイダー：**責任の共有を通じた、サイバーセキュリティプロセス／コントロール／ベンダー／運用モデルの管理と運用をサポートするサービスプロバイダーとの契約締結。
- **アイデンティティとアクセスの管理機能の整備：**シングルサインオン、多要素認証、特権アクセス管理の整備。
- **保険による補償：**最悪のシナリオが現実になった場合に経済的な補償を提供する保険の導入。
- **主要資産と最重要資産の特定：**主要資産、知的財産や企業秘密、機密性の高い顧客情報など組織にとって最も重要で保護すべき情報の特定。
- **人材関連のリスクと教育の重視：**従業員と請負業者の身元調査、及び、サイバーセキュリティリスク、注意すべきこと、サイバーインシデントへの備え方に関する従業員教育の実施。
- **脅威データの適時取得：**潜在的な脅威の早期警告を特定するためのオープンソースとクローズドソースをオンラインで監視する社内機能を保有、または専門的プロバイダーへ委託。
- **災害復旧プレイブック：**サイバー攻撃による業務中断後の事業再開方針を策定。
- **ベンダーに関する理解：**契約締結前のセキュリティ監査レポート要求など、ベンダーのセキュリティ体制を確認。

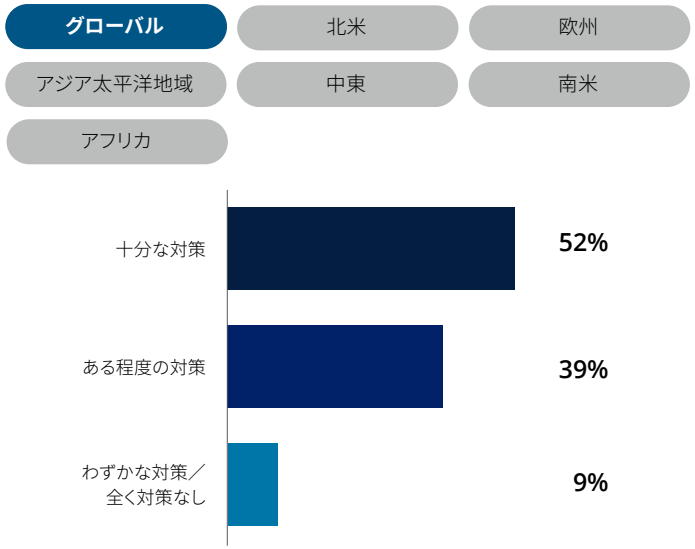
3 サイバー攻撃に対する防御策の強化

ファミリービジネス全体では防御策がかなり整っているが、依然として深刻な課題も

世界的に見ると、ファミリービジネスの52%はサイバー攻撃に対する「十分な」防御策を講じていると考えていますが、残りの48%は全く対策がない、わずかな対策もしくはある程度の対策しか講じていないと感じています。(図3.1) この結果は一般的な傾向を反映しており、多くの組織が対策は部分的に講じているものの、高度な備えは十分ではないと認識していることを示しています。多くの企業が基本的な対策を取り入れているものの、インシデント対応、ベンダーリスク管理、高度な脅威の監視に苦慮していることがさまざまな研究で示されており、今回の調査データでも裏付けられています[9]。

地域別で見ると、十分な対策を講じていると回答した割合が最も多いのはアジア太平洋地域（58%）です。考えられる要因として、デジタル化の加速と政府主導の取り組み（シンガポールのサイバーセキュリティ法やオーストラリアのサイバーセキュリティ戦略など）を挙げることができます。一方、図1.1を見ると、過去2年間に少なくとも一度はサイバー攻撃を受けたとする回答がアジア太平洋地域では約90%と、他の地域に比べて突出した割合となっており、対策についての「見解」と「実際の状態」の間にはギャップがあることが浮き彫りになっています。北米と欧州のいずれも、十分な対策を講じているという見解を示した回答は50%強でした。どちらも成熟したサイバーセキュリティ市場であり、比較的強固な規制の枠組みが整備されています（GDPR、証券取引委員会（SEC）のサイバー開示規制、州のプライバシー法など）。

図3.1： サイバー攻撃に対する防御策の程度に関するファミリービジネスの見解



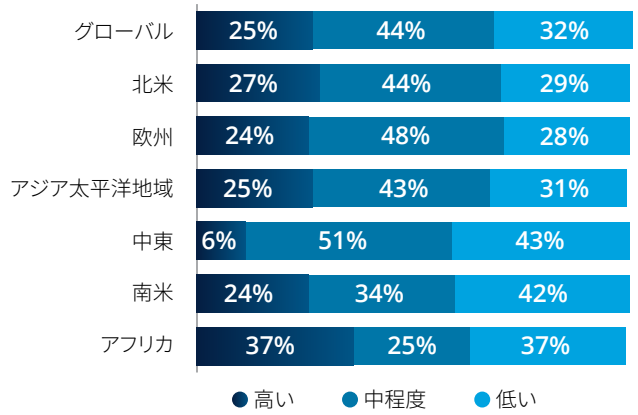
サイバー脅威のリスクは中程度または高いとする見方が大勢を占める

回答者の70%近くは、サイバー脅威のリスクを中程度（44%）または高い（25%）と考えており、リスクが低いと回答したのは32%でした（図3.2）。この結果は、多くの企業がサイバーリスクの深刻さを多少なりとも認識していることを示唆しています。

他の地域に比べて、北米と欧州の回答者はサイバー脅威のリスクをやや高く捉えています。この背景には、両地域における成熟したデジタルトランスフォーメーション、高度な脅威（ランサムウェア、サプライチェーン攻撃など）へのエクスポージャー、サイバーリスクが取締役会の懸念事項になるほど世間の注目を集めた侵害インシデントなどがあると考えられます[10]。サイバー脅威に関するアジア太平洋地域の回答結果は、グローバルの見解をそのまま映し出したものとなりました。しかし、この地域の一部、特に東南アジアでは、AIを悪用したフィッシングやディープフェイクなどの詐欺が急速に広がっており、この状況をファミリービジネスはまだ十分に把握していない可能性があります。事実、国連薬物犯罪事務所は、「サイバー詐欺の拡大は、今日東南アジア地域が直面している最も差し迫った法執行上の課題の1つとなっている」と述べています[11]。

> *資金移動を伴う高度化した詐欺への対策として、検証プロセスを大幅に強化しました。これまでに大きな金銭的損失は発生していませんが、不正な証書によって少額の損失が発生した事案が数件ありました。取引量や売上高の規模を考慮し、このようなインシデントを未然に防ぐことに全力を尽くしています。*
>
> **Chairman**
> 建設、不動産サービス、開発の企業グループ（英国）

図3.2： 今後1～2年におけるビジネスに対するサイバー脅威のリスクレベルに関するファミリービジネスの見解



レジリエンスの教訓：CEOが語る遠隔医療におけるサイバーセキュリティの課題

北米を拠点とする遠隔医療サービス企業のCEOにインタビューを行い、重大なサイバーセキュリティ侵害をどのように乗り越えたのか、率直に語っていただきました。社内の脆弱性、危機対応、そしてクライアントの信頼への影響に関する振り返りを通じて、サイバー脅威による現実世界への影響と、ヘルスケアテクノロジー分野における包括的なセキュリティ戦略、及び保険による支援の重要性について、実践的なインサイトを提示していただきました。

ビジネスに対する現在のサイバーセキュリティの脅威をどのように考えていますか。

当社のポートフォリオ企業の1つに、患者様の遠隔モニタリングを提供する仮想医療サービス企業があるのですが、そこでサイバーセキュリティ侵害が発生しました。それは、かつてないほどの厳しい状況でした。医療の提供において、信頼が最も重要です。データ侵害には、医療サービス企業が患者様やさらに広範な医療コミュニティに対して築いてきた信頼を損ない、企業全体の評判を傷つけるリスクがあります。当社の場合は、攻撃による金銭的損害と業務上の問題には対応できましたが、レピュテーションリスクのコントロールは最も重要な要素でした。法律、コミュニケーション、サイバーの各分野の優れた専門家チームがサイバーセキュリティ保険会社によって結成され、彼らから指導を受けることで、当社の信頼性を維持することができました。発生当初から、お客様に対して十分に透明性を保ち、お客様の懸念に対処して信頼を回復するために、継続的でオープンなチャネルを維持しました。

侵害はどのように発生したのですか。

多くのサイバーインシデントと同様に、人為的なミスが原因でした。プログラマーが、セキュリティ保護されていない検査サイトに患者様の実データを移してしまったのです。サイバー犯罪者はこの脆弱性を悪用し、1万5,000～2万人の患者様のデータ記録にアクセスしました。

ビジネスに対する財務上および評判上の影響はどのようなものでしたか。

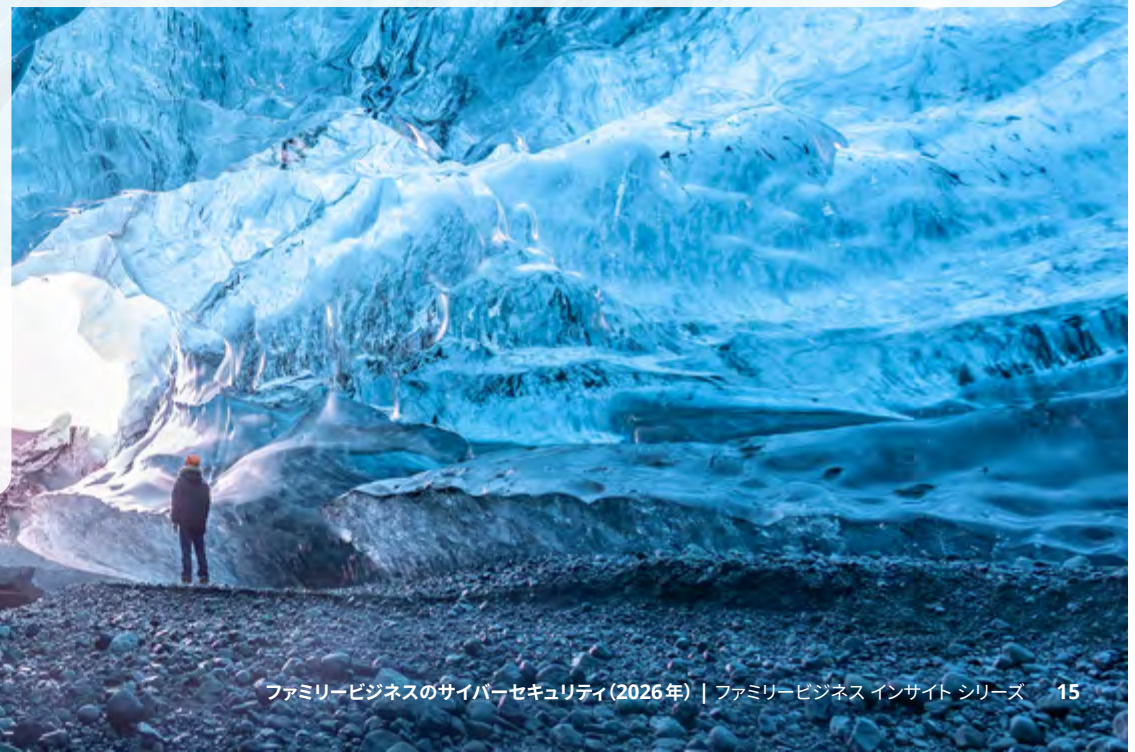
訴訟や危機コミュニケーション、新たなサイバーセキュリティ対策などにかかる直接的な費用は200万米ドル弱でしたが、ほとんどを保険でカバーできました。しかし、レピュテーションリスクは半年にわたる集中的な対応の中で、ステークホルダーである病院や保健当局、影響を受けた患者様に対して、週次報告や個別連絡を通じた率直な情報共有を行うことで、私たちは信用を維持しました。財務的な問題よりもはるかに大きな問題でした。その結果、失った顧客は2件にとどまり、迅速で透明性の高い対応と専門家による指導が有効であることが示されました。

サイバーセキュリティを強化するために、どのように取り組んできましたか。

この侵害の発生後は、システム全体に保護レベルを追加し、従業員のサイバーセキュリティ研修を強化したほか、社内スタッフと外部パートナーを組み合わせた専門のセキュリティチームを作りました。現在では、定期的に攻撃のシミュレーションを実施するとともに、フィッシング演習を頻繁に行い、皆が将来の脅威に備えられるようにしています。

ファミリービジネスのオーナーに対して、サイバーセキュリティ対策についてどのようなアドバイスをしますか。

サイバーセキュリティ保険は、補償を受けるためだけではなく、専門家のサポートを迅速に受けるためにも不可欠です。当社の場合、対応チームが数時間で編成されたため、調査や調達、面談にかかる時間が数週間短縮されました。同様に重要なのは、透明性へのコミットメント、ステークホルダーとの迅速なコミュニケーション、強力な内部統制と研修を維持するための継続的な取り組みです。こうした手順を踏むことで、最も重要なときに、当社の評判と業務の両方を守ることができました。



4 結論：サイバーセキュリティの必須事項への対応

今回の調査は、ファミリービジネスが直面する世界的なサイバーセキュリティの状況を鮮明に表す結果となりました。例えば、広範なエクスポージャー、地域間の差、基本的な対策と高度な対策の間にある継続的なギャップです。回答者のおよそ4分の3（74%）が過去2年間に少なくとも1回のサイバー攻撃を受けたというデータから、サイバー脅威が稀な出来事でも、特別な出来事でもないことは明らかです。それどころか、地域や業種、企業規模に関係なく、拡大する脅威となっています。

ファミリービジネスはサイバー攻撃の嵐にさらされています。それぞれの地域が危険にさらされていることはデータから明らかです。マルウェアやフィッシングのような従来型の攻撃から、内部的な脅威やサプライヤー関連の脆弱性まで、脅威の範囲は広く、弱点を悪用すべく進化し続けています。

また、サイバー攻撃の影響は多面的です。財務上、業務上、評判上の被害が同時に発生することが多く、ファミリービジネスのリスクを増大させています。負の結果を伴わないサイバーインシデントは稀であることが調査結果で裏付けられています。わずか1件の侵害でも、組織全体に影響を及ぼし得ます。

ほとんどのファミリービジネスは、ソフトウェアの更新、ネットワークセキュリティ、バックアップなどの基本的なサイバーハイジーンを取り入れていますが、高度な対策の導入に関しては依然として大きなばらつきがあります。サイバー成熟度評価、ベンダーガバナンス、脅威インテリジェンス、インシデント対応計画といった対策は一般的ではなく、そのために多くの組織が非常に高度な攻撃やサプライチェーンの侵害にさらされています。このような差は全地域で顕著に見られます。

今回の調査結果から、1つの戦略的必須事項を導き出すことができます。それはつまり、ファミリービジネスが基本的なサイバーハイジーンを実施するだけではなく、エンドツーエンドの予測的なサイバーセキュリティ手法の導入を検討する必要があるということです。この課題は、技術的な問題に限ったものではありません。事業継続性、ブランド力、長期にわたるビジネスの存続に関わる問題なのです。

4 結論：サイバーセキュリティの必須事項への対応

実行可能な推奨事項：ファミリービジネスにおけるサイバーレジリエンスの構築

調査で明らかになった課題に対処するために、ファミリービジネスは以下のベストプラクティスを検討するとよいでしょう。

1. サイバーセキュリティをビジネスにおける必須事項として位置づける

- サイバーリスクを単なる技術的な問題ではなく、企業全体のリスクの一部として扱う。
- 取締役会と経営陣を戦略の策定に関与させ、適切な投資が行われるようにする。
- デジタル資産の保護は組織全体の相互責任であるという発信を強化する。

2. 継続的なサイバー成熟度レビューの実施

- 強みと弱みを特定するために、一般に認められた基準に照らしてベンチマークを定期的に実施する。
- 評価を継続的なサイクルとし、1回限りまたはその場限りのレビューを行うのではなく、脅威の進化に応じてプラクティスを更新する。

3. 基本的な防御策と高度な防御策の強化

- 迅速なパッチ適用やMFAから、ネットワークのセグメンテーション、テスト済みの安全なバックアップに至るまで、基本となる防御策を一貫して実施する。
- 脅威インテリジェンスの統合、アクセス制御、サードパーティリスクの監視、インシデント対応プレイブックなどの高度な対策でレジリエンスを強化する。

4. 従業員の意識向上とインサイダーリスクの管理

- 従業員に重点的な研修を実施し、フィッシング詐欺や心理的操作の手口、危険な行動を特定できるよう理解を促す。
- 偶発的および意図的な内部者の行動から生じるリスクを検知し、軽減するための監視ツールと明確なポリシーを導入する。

5. 対応手順と復旧手順の作成と検証

- 明確な対応プロセスを確立し、定期的なシミュレーション演習を通じてテストする。
- サイバーインシデント管理を、より広範な事業継続フレームワークと災害復旧フレームワークに組み込む。

6. ピアネットワークの利用

- サイバーセキュリティ企業やプロフェッショナルネットワーク、その他の信頼できるパートナーと協力して、新たな脅威の一歩先を行く。
- ピアツーピアのフォーラムに参加して、業種固有のリスクや共通の防御策についてのインサイトを得る。

7. ベンダーとサプライチェーンのレジリエンス強化

- サプライヤーと請負業者のセキュリティ体制の評価を行い、サイバーセキュリティ基準を調達や契約の合意事項に組み込む。
- 攻撃ベクトルとして、サプライチェーンの侵害が一般的になってきていることを認識し、サードパーティリスクを継続的に監視する。

8. 規制の変化を積極的に把握

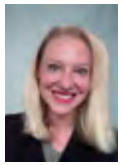
- 要件や規制の変更を常に把握し、最新のコンプライアンス体制を維持する。
- 将来のコンプライアンス要件への適合に役立つ機能に積極的に投資する。

終わりにあたって：気づきをインパクトに変える

調査の結果は、警鐘を鳴らすとともに、改善の機会を示しています。ファミリービジネスは直面するリスクを強く意識するようになっていますが、多くは依然として岐路に立ち、基本的な防御策の徹底と高度なレジリエンスの確立の間で身動きがとれない状況にあります。前進するためには、リーダーシップ、慎重な投資、絶え間ない改善の文化が必要です。

サイバーセキュリティを戦略的な経営の最優先事項として位置づけることで、ファミリービジネスは今日の脅威から身を守るだけでなく、デジタル化が進む世界で持続可能な成長の基盤を築くことができます。今こそ行動を起こす時です。サイバーレジリエンスの弱点を埋めることは、単なる被害の軽減にとどまらず、信頼を築き、レガシーを守り、これからの世代のために未来を守ることにつながるのです。

連絡先



Dr. Rebecca Gooch
Deloitte Private Global Head of Insights
2 New Street Square, London, EC4A 3BZ, United Kingdom
Direct: +44 20 7303 2660 | Mobile: +44 (0) 7407 859053
rgooch@deloitte.co.uk
www.deloitte.co.uk/deloitteprivate

Adrian Batty
Global Family Enterprise Leader | Deloitte Private
Partner | Deloitte Private, Tax & Advisory, Deloitte Australia
477 Collins Street, Melbourne, Victoria 3000, Australia
Direct: +61 3 9671 7858 | Mobile: +61 414 427 692
abatty@deloitte.com.au
www.deloitte.com/au

Yali Yin
Global Deloitte Private Leader
Partner I Deloitte Tax Ltd
No. 23, Zhenzhi Road, Beijing 100026, PRC
yayin@deloitte.com.cn
www.deloitte.com/cn

Wolfe Tone
Vice Chair, US Deloitte Private Leader
Partner | Deloitte LLP
111 S. Wacker Drive, Chicago, IL 60606-4301, United States
Direct: +1 312 486 1909 | Mobile: +1 312 545 9670
wtone@deloitte.com
www.deloitte.com

樋口 亮輔／Ryosuke Higuchi
デロイト トーマツ税理士法人　パートナー
ファミリーコンサルティング 部門長
デロイト トーマツ ファミリーオフィスサービス合同会社
代表職務執行者社長
東京都千代田区丸の内3-2-3　丸の内二重橋ビルディング
Direct: +81 3 6213 3800 | Mobile: +81 80 4170 9347
ryosuke.higuchi@tohmatsu.co.jp
https://www.deloitte.com/jp/ja/services/tax/services/familyoffice.html

巻末注

1 Amoo, O. O., Atadoga, A., Osasona, F., Abrahams, T. O., Ayinla, B. S., & Farayola, O. A., GDPR's impact on cybersecurity: A review focusing on USA and European practices, p. 1338-1347, 2024

2 National Institute of Standards and Technology, Computer Security Resource Center Glossary.

3 INTERPOL, 23 June 2025

4 Verizon, *2025 Data breach investigations report*, p. 26

5 World Economic Forum, Here's how SMEs can turn cybersecurity risk into opportunity | World Economic Forum, 30 July 2024

6 Cybersecurity & Infrastructure Security Agency, *Cybersecurity best practices*

7 TechRadar Pro, *Compliance is evolving — Is your resilience ready?*, 2024

8 Aon, Asia-Pacific's commitment to cyber security pays off, 30 May 2025; CIO World Asia, *Cyber budgets surge as mid-market firms in APAC struggle with AI security gaps*, 30 May 2025.

9 World Economic Forum, 2024

10 Reuters, ESG Watch: Companies 'complacent about cybercrime,' despite rise in risk from AI, 3 February 2025.

11 United Nations Office on Drugs and Crime, *TOC convergence report 2024*. ROSEAP

Deloitte.
Private

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

IS/BCMSそれぞれの認証範囲はこちらをご覧ください
http://www.bsigroup.com/clientDirectory