Deloitte.
Private

ファミリーオフィスに対するサイバー脅威

ファミリーオフィスにおける現代のサイバー脅威を
レジリエントアプローチによって阻止するために

機密データや投資からコネクテッドデバイスまで、サイバー脅威は守るべき家族の様々な側面に影響を及ぼしかねません。サイバー攻撃者とその手口を理解することは、家族とファミリーオフィスを守るための重要な鍵となります。本レポートでは、サイバーセキュリティの10項目のアプローチにより、ファミリーオフィスが広範囲にわたるサイバー攻撃に対抗できることを示しています。

エグゼクティブサマリー

ファミリーオフィスに対するサイバー脅威は数多く、現実のものとなっています[1]。恐喝、詐欺、サイバー攻撃によって引き起こされる物理的な脅威は、ファミリーオフィスの財政や評判、そして家族自身の安全に大きな影響を与える可能性があります。

キャンプデン・リサーチの最新のレポートでは、2017年にファミリーオフィスの32%がサイバー攻撃による損失を被り、あるケースでは1,000万ドル以上もの損失があったことを示しています[2]。それにもかかわらず、回答者の48%はサイバーセキュリティ計画を策定していませんでした。

サイバー犯罪者は通常、サイバーセキュリティが不十分だと認識されている、大金を扱う事業を標的にしています。そのため、ファミリーオフィスはサイバー犯罪者にとって格好の標的となっています。

さらに、ファミリーオフィスはより規模の大きい組織と同様に、機密データを保有しています。しかし、ファミリーオフィスのセキュリティ管理要件は、大半の大規模な組織と比較するとはるかに緩いものです。一般的にファミリーオフィスは、少数のスタッフに依存しているため、大規模な組織と比較するとデータの分離が不十分で、データが無防備な状態にあることが多い点が一因と考えられています[3]。しかし、基本的なセキュリティ対策は、サイバー攻撃を防ぐのに多大なる効果をもたらします。例えば、単に厳格なパスワードポリシーを導入し、アンチウイルスソフトウェアを最新の状態に保つだけでも大きな効果を得ることができるのです。

本レポートでは、デロイトがサイバーインシデントの予防、検出、対応のためにファミリーオフィスが実施を検討すべき10項目の重要なアクションを挙げています。レポートの後半では、ファミリーオフィスがサイバー脅威にさらされる度合いを効果的に軽減するために、相互に依存し、かつ組み合わせることで基本的なサイバー防衛をもたらす上位10項目の戦略的統制に焦点を当てています。

また、家族に対する脅威についても言及します。例えば、ファミリーオフィスは、電話、タブレット、自動車、スマートスピーカーなどのコネクテッドデバイスの使用が増加することで、ファミリーオフィスが代表する家族、自動車、自宅へのサイバー攻撃によるネットワークへの侵入の危険性が高まることを考慮する必要があります。それぞれの脅威の評価については、実際の事例とともに本レポートの前半で説明します。

ファミリーオフィスは財政面以外の分野でも様々なサービスを提供していますが、サイバーセキュリティに関しては、依然としてアウトソーシングが中心となっています。本レポートは、ご自身が直面する脅威を十分にご理解いただき、サイバーセキュリティプロバイダーに適切な質問ができるよう役立てていただくものです。

1. citywire.co.uk/wealth-manager/news/why-family-offices-need-to-up-their-game-on-cyber-security/a1071874
2. ubs.com/global/en/wealth-management/uhnw/global-family-office/global-family-office-report-2018.html
3. europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

脅威の概要

以下の表は、ファミリーオフィスおよびファミリーが職場、自宅および移動中に直面する可能性が最も高い脅威を示したものです。この表では、脅威アクターが使用する最も一般的な攻撃の方向性と、その標的となるシステムに基づいて、それぞれの脅威が最も表れやすい場所を示しています。実際の事例を含むそれぞれの脅威に関する詳細な評価については、本レポートの次のセクションで説明します。

脅威	職場	自宅	移動中
恐喝 • ランサムウェア • 機密データ公開に関する脅迫	◎	◎	
詐欺 • ビジネスメールのハッキング • SNS アカウントの乗っ取り	◎	◎	
スパイ行為	◎		◎
サイバー攻撃によって引き起こされる物理的な脅威 • 情報収集および不要な注目 • 乗り物への不正アクセス（例：スーパーヨットや自動車） • 高級住宅や不動産への侵入		◎	◎

恐喝

ランサムウェア

ランサムウェアは、コンピューターやオフィスのネットワークにアクセスし、ファイルに攻撃者のみが解除可能な暗号をかけるタイプの悪意あるソフトウェア（マルウェア）です。サイバー犯罪者は、個人および組織に対してランサムウェアを広く悪用しており、2017年には世界経済に50億ドルの損失を与えたと推定されています[4]。

事例紹介 — ドライデックス（Dridex）、オーダーメイド型のランサムウェアを標的に送付

2018年9月に、マルウェア「ドライデックス」の背後にいるサイバー犯罪グループが、標的型ランサムウェア攻撃を行うようになりました。同グループは、被害者のセキュリティ対策を特定するための評価を行い、使用されている特定のアンチウイルスを回避するために攻撃方法をカスタマイズしています。同犯罪グループは少なくとも200件の攻撃を成功させ、それぞれの被害者に15,000から300,000ポンドの身代金を要求しました[5]。

機密データ公開に関する脅迫

サイバー犯罪者は、組織のネットワークに侵入し、盗み取ったデータを公開すると被害者を脅迫しています。2017年には、30,000以上の人がデータ侵害を訴えており、米国だけでも7,700万ドルの損失があったと推定されています[6]。機密データの公開は、著名人の評判や財政に与える影響が大きいと考えられているため、恐喝者にとって著名人は格好の標的となります。

事例紹介 — 恐喝グループ「DarkOverLord」

「DarkOverlord」は、身代金を支払わない限り、盗んだ個人情報やビジネス上の機密情報を公開すると被害者を脅迫するグループです。同グループは、ダークウェブ上で自身のハッキングを宣伝し、メディアの注目を集めようとするだけではなく、データ漏洩で被害を受けた有名人を公表して、標的にさらなるプレッシャーを与えます。

2017年10月に、同グループは、London Bridge Plastic Surgery clinicから私的な写真を含む顧客の機密データを盗み、複数の著名な顧客の画像を公表すると脅迫しました。同グループは、恐喝によって275,000ドル以上を受領したとされています[7]。

サイバー攻撃による不正行為対策として推奨される主なアクション

恐喝の脅威を軽減するための主なアクションは以下の通りです。

- 適切なバックアップとリカバリー戦略
- トレーニングおよび意識の向上
- エンドポイント保護

これらの対策は、一般的な不正行為の防止には役立ちますが、成熟したレジリエンスのあるサイバーセキュリティ態勢には、包括的なサイバーセキュリティ戦略を含める必要があります。この点は、これ以降のセクションにも当てはまります。

4. europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018
5. forbes.com/sites/geoffwhite/2018/09/26/how-the-dridex-gang-makes-millions-from-bespoke-ransomware/#6d3a764440d3
6. fbi.gov/news/stories/2017-internet-crime-report-released-050718
7. cyberscoop.com/dark-overlord-arrest-serbia/

詐欺

ビジネスメールのハッキング

詐欺師はデジタル時代のはるか前から、企業になりすまして金融詐欺を試みてきました。しかし、コンピューターと電子メールの普及により、コンピューターを利用したビジネスメール詐欺（BEC）と呼ばれる詐欺が、その手軽さから特に広まっています。BECでは、詐欺師が、被害者の信頼できる同僚やクライアントの電子メールアドレスを模倣したり、電子メールアカウントをハッキングして彼らになりすまし、被害者から多額の金銭（多くは数百万ドル）をだまし取ります。

特に多額の取引を承認することの多い組織が狙われます。2013年10月から2018年5月にかけて、BEC詐欺によって、全世界で125億ドルもの損失が発生したと推定されています[8]。

事例紹介 — 富裕層を狙った国際的なBEC詐欺集団
2018年6月に、法執行機関は米国、ナイジェリア、カナダ、モーリシャス、ポーランドで74人を逮捕し、BEC詐欺で盗まれた約1,640万ドルを回収しました。同詐欺グループの詐欺事件には、富裕層や業務上定期的に多額の送金や機密記録の送信を行っている人たちを標的にしているものもありました[9]。

SNSアカウントの乗っ取り

株式公開されているファミリービジネスにとって、著名人や組織がSNSに投稿した内容は、その株式価値に大きな影響を与える可能性があります。投資家は、特定の銘柄の売買の判断のため、組織の最上位層の人物のSNSプロフィールをモニターすることがよくあります。

著名人のSNSアカウントを一時的にコントロールする脅威アクターは、被害者と関係のある上場企業の株価を変動させるために、偽の情報を投稿する可能性があります。また、プライベートなメッセージの内容を公開し、中傷的な情報で評判を落とそうとする可能性もあります。

事例紹介 — AP通信のツイッター、乗っ取りにより1,360億ドルの市場損失発生
2013年4月に、AP通信のツイッターアカウントがハッカーに乗っ取られ、当時の米国大統領バラク・オバマ氏が爆発によって負傷したという偽のメッセージが投稿されました。このハッキングはすぐに発覚し、不正アクセスされたアカウントは停止されました。しかし、この偽ツイートの投稿から3分後には市場でパニックが起き、株式市場価値で1,360億ドルが消失したとワシントン・ポストが伝えています[10]。この事件は報道機関に影響を及ぼしたものですが、SNSアカウントの乗っ取りによってネット上に投稿されたフェイクニュースに、市場がいかに早く反応するかを示しています。

サイバー詐欺対策として推奨される主なアクション

詐欺の脅威を軽減するための主なアクションは以下の通りです。

- トレーニングおよび意識の向上
- 認証
- サイバー脅威インテリジェンス

8. ic3.gov/media/2018/180712.aspx
9. justice.gov/opa/pr/74-arrested-coordinated-international-enforcement-operation-targeting-hundreds-individuals; fbi.gov/news/stories international-bec-takedown-061118.
10. washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/?noredirect=on&utm_term=.86e3b75b5da3

スパイ行為

サイバースパイ行為とは、高度な技術を持った集団が、政治的・商業的な動機からデータを盗み出すものです。例えば、犯罪者はインサイダー取引のため、または競合他社に雇われたハッカーとしてこのような行為をします[11]。ファミリーオフィスは第三者企業の株式を大量に保有することがあり、また、そのオーナーはしばしば政治的な関わりを持っていることがあります。つまり、個人とそのファミリーオフィスは、サイバースパイ行為の動機が商業的であれ、政治的であれ、標的となりやすいのです。盗まれた機密データは、敵意を持つ政府が監視のために使用したり、都合が悪いと思われる情報を公表される可能性もあります。

事例紹介 — 北朝鮮、ロシアがホテルのWi-Fiを狙う
スパイ組織はホテルのWi-Fiに不正にアクセスし、著名な出張者を標的にします。北朝鮮の「DarkHotel」グループは少なくとも2007年以降、アジアや米国のホテルのネットワークに不正侵入しており、ロシアのAPT28グループは、ヨーロッパや中東で同様の行為をしています。ファミリーオフィスは、富裕層の出張先に関する情報を保護し、標的型攻撃を防ぐ必要があります。

推奨される主なアクション

スパイ行為の脅威を軽減するための主なアクションは以下の通りです。

- エンドポイント保護
- セキュアバイデザイン
- ファイアウォールとコンテンツセキュリティ

しかし、洗練された脅威アクターは、包括的なサイバーセキュリティ戦略を含む、成熟したレジリエンスのあるサイバーセキュリティ態勢がなければ対抗できません。

11. fireeye.com/current-threats/threat-intelligence-reports/rpt-fin4.html

サイバー攻撃によって引き起こされる物理的な脅威

情報収集および不要な注目

オンラインまたはSNSで公開されている情報は、大量の個人情報を明らかにし、個人への嫌がらせや安全を脅かすために利用される可能性があります。パパラッチは、公開された投稿を利用して、著名人に嫌がらせをすることが可能です。脅威アクターは、友人、家族、連絡先、旅行の予定や現在の行動に関する情報へのアクセスを利用し、個人の安全に対する物理的な攻撃を計画することができます。海外滞在中に家族が正確な滞在場所をSNSで共有してしまうなど、SNSの軽率な利用によって、富裕層への脅威は実際に起きています[12]。

乗り物への不正アクセス

プライベートジェット、スーパーヨット、自動車はコネクテッドデバイスへの依存度が高まっているため、標的にされています。特に最近のヨットは脆弱です[13]。不正アクセスに成功した場合、脅威アクターはエンジンやナビゲーションシステムを制御することが可能になります。少なくとも1つの事例では、サイバー攻撃による不正アクセスでスーパーヨットが完全に危険にさらされ、GPS偽装もますます広まっています[14]。また、高級自動車も潜在的な標的ですが、現実に起きている悪用例としては、今のところキーレス車の盗難にとどまっています[15]。

高級住宅や不動産への侵入

高級住宅では、ますますIoTデバイスが使用されるようになっています。2015年に行われた調査では、調査対象の全てのインターネット接続型セキュリティ機器において、機器の遠隔操作が可能であるという重大なセキュリティの脆弱性が判明しました。この影響が深刻になる可能性があります。インターネットに接続された脆弱なセキュリティシステムがすり抜けられ、物理的な侵入が可能になったり、セキュリティカメラの映像がハッキングされ、ネット上に公開されるような可能性があります。

推奨される主なアクション

サイバー攻撃によって引き起こされる物理的な脅威を軽減するための主なアクションは以下の通りです。

- セキュアバイデザイン
- 脅威の監視および侵入テスト
- 認証

12. campdenfb.com/article/market-insight-critical-risk-extortion-blackmail-and-kidnap-ransom
13. kaspersky.com/blog/yachts-vulnerabilities/21576/
14. boatinternational.com/yachts/luxury-yacht-advice/why-cyber-crime-is-the-biggest-threat-to-superyacht-security—33945 ; newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/
15. express.co.uk/life-style/cars/1048780/car-theft-keyless-entry-hack-stolen-seconds-UK-epidemic
16. hp.com/us/en/hp-news/press-release.html?id=1909050

主な提案事項

本セクションでは、上述したサイバー脅威を最も効果的に軽減するために、ファミリーオフィスとその関係者が優先的に取り組むべき主要な対策の上位10項目を簡潔にまとめています。社内で実施可能なものもあれば、効果や費用効率の面からファミリーオフィスが専門業者にアウトソーシングすることが多いものもあります。

準備

1. **資産管理** ー 家族とその財産を支える最も重要なデジタル資産を把握します。分類することによって、優先順位付けがされた適切な保護、監視、対応戦略が可能になります。
2. **サイバー脅威インテリジェンス** ー オンラインのオープンソースとクローズドソースを監視するサービスを委託してください。これにより、潜在的な脅威の前兆を早期に特定すること、また、攻撃が既に起きている可能性を示す指標を特定することができます。
3. **適切なバックアップとリカバリー戦略** ー データのバックアップを保存し、その完全性を保護するための技術的ソリューションを導入する必要があります。このソリューションはテストおよびリカバリーのリハーサルを実施し、確実に機能するようにしなければなりません。
4. **トレーニングおよび意識向上** ー 積極的なトレーニングと信頼できる資料を用い、スタッフがサイバー脅威、予防・検出方法およびその重要性を認識していることを確実にします。getsafeonline.org（イギリスのウェブサイト）には社内トレーニング用の優れた資料があります。

保護のためのシステムおよびネットワークセキュリティ

5. **エンドポイント保護** ー 健康診断で体の潜在的な健康問題を検出するように、アンチウイルスソフトウェアは、ITシステム内の悪意ある活動を防止し、検出することができます。常に最新の状態を維持するようにしてください。
6. **認証** ー 家には頑丈な錠と固有の鍵があります。デジタルな生活でも同じであるべきです。常に強力なパスワードを使用し、ネットワークでの管理者権限の使用を制限し、多要素認証で重要なアカウントを保護しましょう。
7. **セキュアバイデザイン** ー 建物は安全性に考慮して設計されるべきであり、ITネットワークも同様です。ご自身のITプロバイダーが、設定のハードニング、ネットワークのセグメンテーション、脆弱性管理、自動パッチ適用をしているか確認してください。これらは攻撃者が悪用する可能性のあるものを最小限に抑えるために役立ちます。
8. **ファイアウォールとコンテンツセキュリティ** ー 建物を囲む柵のように、ファイアウォールはデジタルシステムを保護します。ファイアウォールとWebプロキシ技術に投資することで、ITシステムに侵入する可能性のある、悪意を持ったネットワークトラフィックを検出・防止することができます。

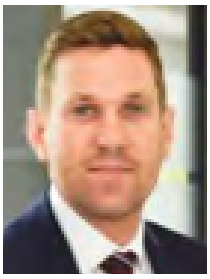
検出・対応管理

9. **脅威の監視および侵入テスト** ー IT環境において攻撃者が悪用できてしまう弱点がないかを検証し、監視技術を利用してコンピューターとネットワークの動作の異常を検出します。これにより、攻撃の兆候を把握し、早期対応を図るとともに、家族、資産および財産に及ぼしうる影響を最小限に抑えることができます。
10. **インシデント対応計画** ー 蓄積された専門知識を利用し、予測または実際のサイバーインシデントや攻撃に対する計画、リハーサルおよび対応に役立てます。

レジリエントな態勢を構築するために、多くのセキュリティ管理、技術および慣行を利用することができます。上記の上位10項目の戦略的統制は重要であり、正しく組み合わせて実施することで、強固なサイバー防衛能力をもたらします。これにより、ファミリーオフィスは既知の脅威を積極的に予測し、防御することが可能になるとともに、警戒態勢を保ちながら新たな脅威を検出し、それに対応するための十分な用意が可能になります。

担当者

Phill Everson
Partner, Cyber Risk Services Risk Advisory
+44 (0)20 7303 0012
peverson@deloitte.co.uk



Tim Erridge
Director, Cyber Risk Services Risk Advisory
+44 (0)20 7303 3872
terridge@deloitte.co.uk

注意事項：本誌はDeloitte Privateが発刊した原稿をデロイト トーマツ グループが翻訳し2023年2月に発行したものです。和訳版と原文である“Cyber Threats to Family Office（英語）”に差異がある場合には英文を優先いたします。

Deloitte. Private

お問い合わせ
Deloitte Private Japan
email : dpj@tohmatsu.co.jp