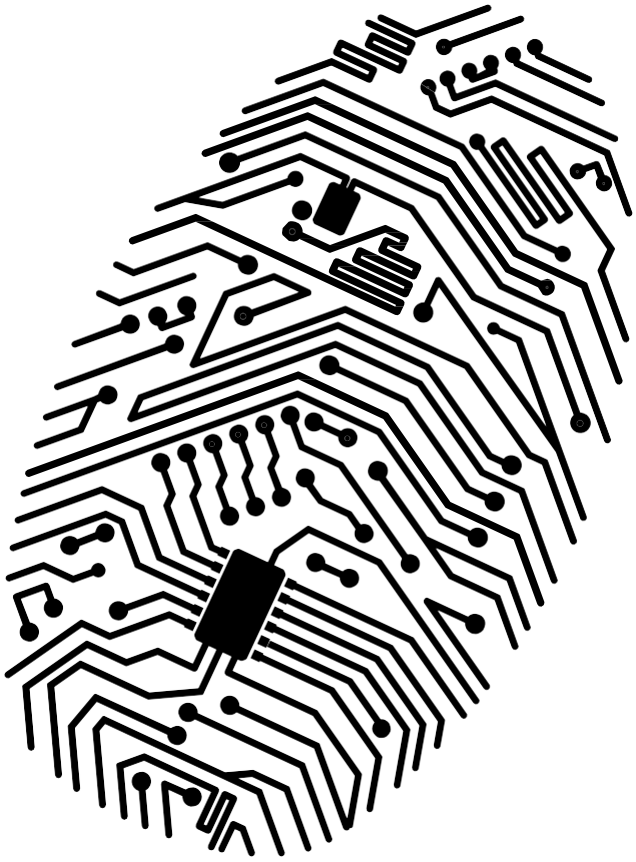
Deloitte.

サイバーセキュリティの変革
進化する脅威の状況に対する新しいアプローチ



Deloitte Center
for Financial Services

目次

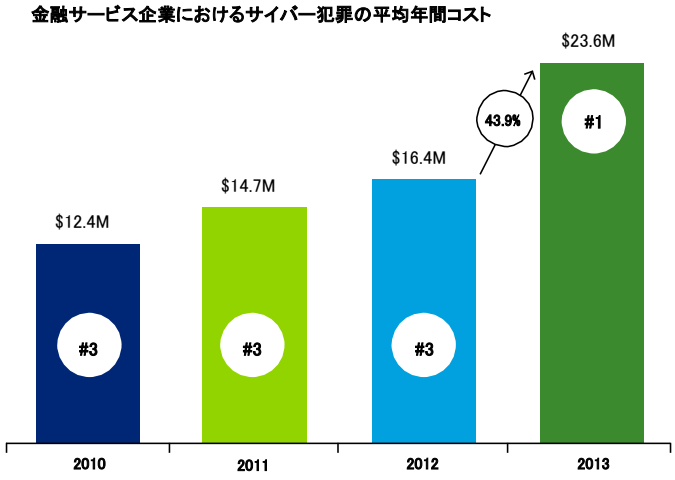
「2013 年は今までで最も問題の多い年となりました。攻撃は量的にも数的にも指数関数的に増加しています。このトレンドは今も続いています・・・」

– アンソニー・ベルフィオーレ、J.P.モルガン、グローバル・サイバーセキュリティ、ヘッド [6]

変わり続けるサイバーセキュリティ

最近の公開されたSF映画「*インセプション*」で、主人公ドミニク・コブは標的の夢に潜入して企業秘密や機密データにアクセスします。その後、コブはその知識を利用して、自分（またはクライアント）に有利になるように影響を与えようとします。コブは、人間の弱さを深く理解しており標的を操る能力があるから成功したのです。サイバー犯罪者は、まさにこのコブのように、その標的の脆弱性を特定し、標的のシステムを侵害するためのインテリジェンスを収集することから始めます。サイバー犯罪者は、このインテリジェンスを武器に、標的の複雑なシステムをうまくすり抜け、長期にわたって発見されることなくシステム内に潜伏します。

図表 1：サイバー犯罪のコストは増加している



（#）– 当該業種内での組織に対するサイバー犯罪による平均年間コストによる業種のランクを示しています

出所：Ponemon Institute[1,2] およびデロイト金融サービスセンターの分析

金融サービス業界におけるサイバー犯罪は、加速的に増加しているとはいえないかもしれませんが、増加基調にあることは明らかです（図表1）。2013年において米国の金融機関はサイバーセキュリティの侵害によって平均で2360万ドルの損失を被っており[3]、これは全業種の中でも最大です。2012年からの1年間に43.9%も増加しており、サイバー上の脅威は急激に増加しているといえるでしょう。2012年には、金融サービス業界の平均損失額は防衛、公益／エネルギーに次いで全業界で3位でした[4]。この傾向は無視できません。実際の損失額は、企業の損益計算書上では重要なものではないかもしれませんが、サイバー犯罪による潜在的な影響は顧客と投資家の信頼感、風評リスク、規制リスクなどであり、これらが相俟って金融サービス企業に対する重大なリスクとなっています。企業のCレベルの幹部や取締役に対する最近の世界的な調査によると、企業の全般的なリスクのうちサイバーリスクが2013年における第3位の優先事項となっています[5]。興味深いことに、2011年の同じ調査ではサイバーセキュリティ優先順位は12位に過ぎません。この急速な上昇の一因は、おそらくサイバーリスク自体の質的な進化によるものでしょう。

映画「*インセプション*」では、コブはほとんどの標的を操ることに成功しますが、フィッシャー氏の手強い抵抗に直面します。フィッシャー氏の強力な自動防御メカニズムによって攻撃者の計画は何度も頓挫に直面します。しかし、コブのチームは障害に直面するたびに、それに耐え、手直しをし、新たな攻撃を開始します。現実のサイバー攻撃はもちろん、コブとフィッシャー氏の間の攻撃と対応よりもはるかに複雑なものです。とは言え、この映画では、金融サービス企業がサイバー犯罪に対処する際に直面する問題を解決するための興味深いヒントが多く示されています。

攻撃者と標的の間の攻撃と防御は「いたちごっこ」であり、それぞれが絶えず学習と適応を繰り返し、創造性を発揮し、また相手側の動機に対する知識を利用して新たな攻撃戦術や防衛体制を作り上げています。多くの金融サービス企業では、セキュリティに対するコンプライアンスやポリシー中心の決まりきった対策をするというアプローチが見られますが、このようなアプローチはずっと以前からすでに時代遅れのものとなっているかもしれません。重要なことは、今日の金融業界がダイナミックで、インテリジェンス主導のアプローチ、つまり攻撃を阻止するだけではなく、検知、対応し、攻撃による潜在的な打撃から回復するためのアプローチをつくり出すことができるかどうかということです。このように、サイバー空間におけるリスクを効果的に管理し、革新を起こしていくためには、安全（セキュア）で、警戒し、回復力の高いモデルへの転換を考える必要があります。

「サイバー分野における敵には、秘密や知的財産を狙う国家からのスパイ、アイデンティティと金銭の窃盗を望む組織的犯罪者、電力網、水道、またはその他のインフラの攻撃を目標とするテロリスト、政治的あるいは社会的な声明を行うことを試みるハクティビストが含まれています」

— リチャード·A. マクフィーリー、エグゼクティブアシスタントディレクター、クリミナル、サイバー、レスポンス、およびサービスブランチ、米連邦捜査局（FBI）[7]

進化するサイバー脅威の現状

サイバー攻撃者は挑戦的であり、自らの目標をなんとかして達成しようとしていますが、金融サービス企業も単に被害者に甘んじているわけではありません。金融サービス企業が、成長、イノベーション、およびコストの最適化のために採用している事業変革や技術革新は、同時に高い水準のサイバーリスクとなっています。これらの技術革新によって、金融サービス技術のエコシステムには新たな脆弱性や複雑性が生じている可能性があります。たとえば、Web、モバイル、クラウド、ソーシャルメディア技術を継続的に利用することによって、攻撃者の攻撃機会を増やしている可能性があります。同様に、コスト削減を目標として推進されているアウトソーシング、オフショアリング、外部人材の活用によって、ITシステムやアクセスポイントに対する組織的な統制がさらに弱まっている可能性があります。この結果として、金融サービス企業が事業を行うエコシステムはますます境界のないものとなっており、脅威者が利用できる「攻撃表面」、つまり攻撃の対象が大幅に広がっています。

サイバーリスクは、もはや金融犯罪に限定されない

さらに問題を複雑にしているのが、サイバー脅威は基本的に非対称的なリスクであるということです。たとえば、多様な動機と目的を持つ高度に熟練した個人らによるほんの小さな集団が、その規模に似つかわしくないような大きな打撃を与える可能性を秘めているのです。過去のサイバーリスク管理において、金融犯罪に重点をおくことは当然でした。それは依然として変わっていません。しかし、私たちのクライアントと議論をしていると、かれらは今や金融犯罪者や熟練したハッカーだけではなく、政治的／社会的な目的を持った政治的ハッカーグループや国家などの、市場におけるシステミックな混乱を引き起こす、大規模で組織的な攻撃者の標的になる傾向がますます強まっています。銀行セクターにおけるサイバー脅威の状況を例示した図（図表 2）からは、金融サービス企業がサイバーリスク戦略の設計に当たって、広範な脅威者および動機を考慮する必要があるということが示唆されています。このためには、サイバーリスクアピタイトとそれに対応したリスク統制環境への根本的に新しいアプローチが必要です。

「投資を行う余裕のある経済的動機を持った組織的犯罪グループから、社会的目標はあるが金銭の窃盗が目的ではないハクティビストに移行しています」

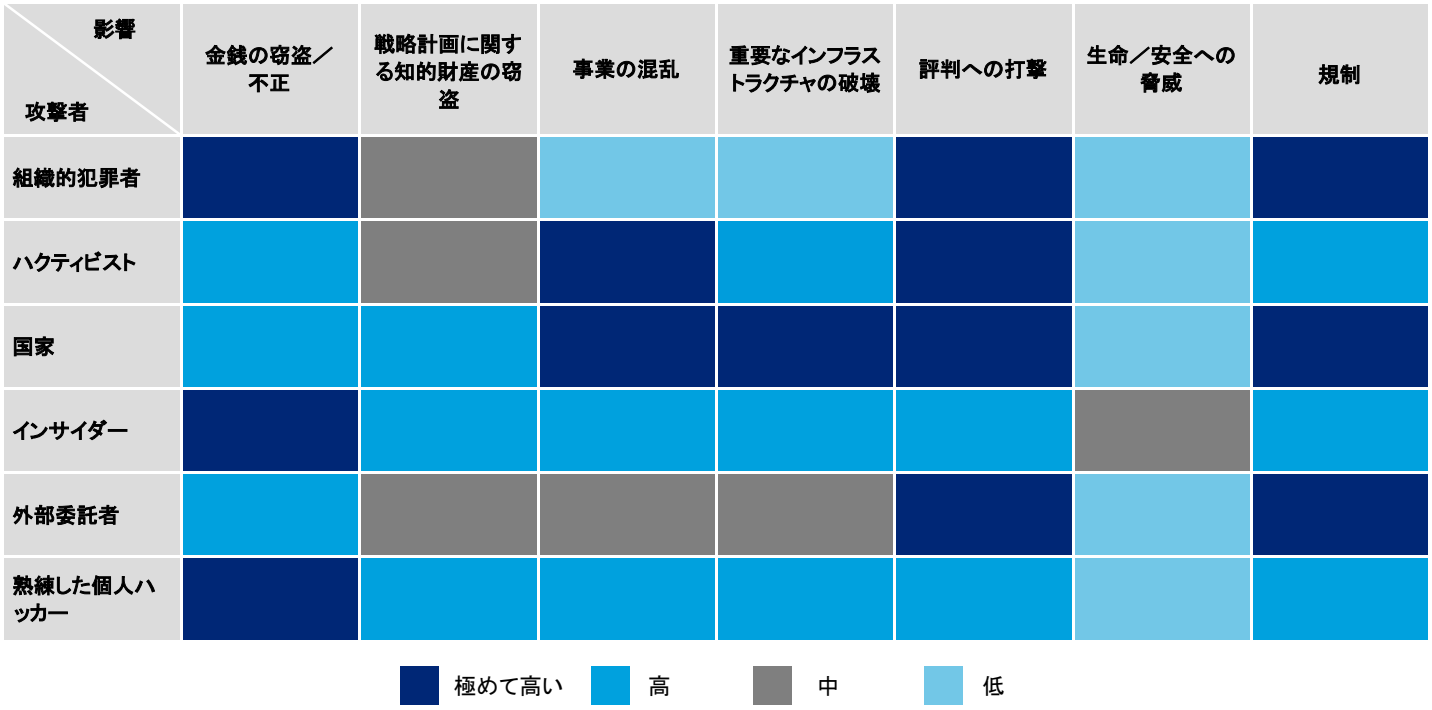
― ルー・スタインバーグ、最高技術責任者（CTO）、TD アメリトレード[10]

ご存知でしたか？
金融サービス企業はサイバー攻撃に対して最も脆弱です

- 金融サービス業界は、サイバー犯罪者が最も標的とする26業種のリストの最上位にあります。[8]
- 消費者は、他の業種の企業ブランドの偽装メールの場合と比較して、銀行ブランドの偽装メールによる攻撃の犠牲者になる確率が7倍となっており、金融サービス業界は依然として悪意のある電子メール偽装者に対して最も脆弱な業種となっています。[9]

図表 2:広範に及ぶサイバー攻撃者と影響

銀行セクターの典型的なサイバーリスクのヒートマップ



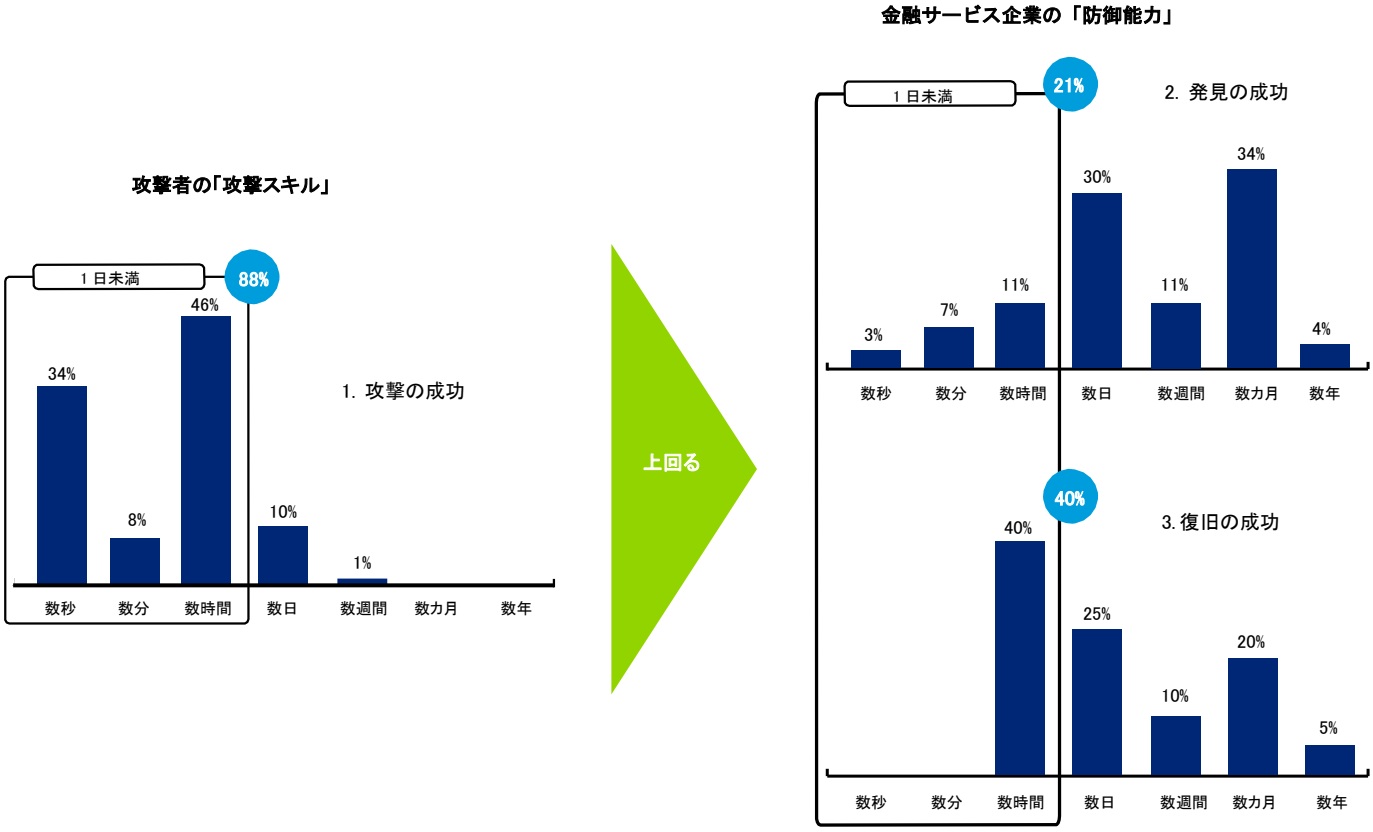
出所:デロイト金融サービスセンターの分析

攻撃の速度は増しているが対応は遅れている

攻撃者はさまざまな新しい攻撃方法を利用しており、金融サービス企業の一歩先をいっています。たとえば、犯罪組織は、彼らの作戦のなかで複合的な侵入手法を使っており、悪意のある内部関係者を利用するようになっています。世界の金融サービスのエグゼクティブに対するデロイトトウシュトーマツリミテッド(DTTL)の調査[11]で報告されているように、金融サービス企業の多くは、脅威の進化に対抗するために必要とされるサイバーリスクの成熟度に達しようとして苦しんでいます。

グローバルな金融サービス企業の75%が自社の情報セキュリティプログラムの成熟度レベルを3以上であると考えていますが[12]、自社組織の情報資産が外部の攻撃から守られているという強い自信を持っている金融サービス企業はわずか40%に過ぎません。かつ、これらの企業は大規模で、比較的高度な技術を持つ金融サービス企業です。中堅企業や小規模な企業の場合は、一般的にリソースが限られており、また攻撃者が容易な標的であると見る可能性があるため、状況ははるかに悪いでしょう。また、同様に、スノーデン事件によって、内部者の脅威に関しても注意が高まっていると見られます。

図表 3:グローバル金融サービス企業の攻撃への対応時間は準備態勢における重大なギャップを示している



1. 攻撃の成功(侵害までの時間):標的に対して最初の悪意のある行動が取られてから、情報資産に悪影響が及ぶ時点までの時間を測定。
2. 発見の成功(侵害から発見までの時間):最初の侵害から、標的が最初にインシデントを関知するまでの時間を測定。
3. 復旧の成功(発見から封じ込めまでの時間):侵害の発見から、その封じ込めの成功までの時間を測定。

丸め誤差により、合計値が100にならない場合があります。

出所:Verizon Risk[13]、デロイト金融サービスセンターの分析

これらの課題はデータを見るとより明らかになります。デロイト金融サービスセンターでは、図表3に示すように、データセキュリティに関するVerizonによる年次調査報告書からのデータを分析し、2013年においては金融サービス企業に対して仕掛けられた攻撃の88%が1日未満で成功していることを確認しています。

しかし、これらの攻撃で1日内に発見されたのはわずか21%に過ぎず、さらに悪いことには、発見以降においてその1日内の期間で回復されたのはわずか40%に過ぎません[14]。攻撃の速度、発見率の大幅なギャップ、復旧に要する期間の長さが、検知と対応の両面の能力において金融サービス企業が直面している課題を示しています。

多面的アプローチによって、今や不十分な伝統的技術の補完が可能

攻撃の 88%が 1 日未満で成功するという結果に対して、「攻撃の成功を阻止するためのツールや技術への投資を増やすことが解決策である」と考えたくなるかもしれません。しかし、脅威に対する認識と対応が不十分であることに対して、予防的対策技術を充実させただけでは、不十分である可能性が高いことを示唆しています。むしろ、金融サービス企業では、広範なサイバー脅威とリスクに対処するための、より包括的なサイバー防御と対応策のプログラムを組み込んだ多面的なアプローチを検討するべきでしょう。

安全、警戒、回復力が絶対的命題

金融サービス企業は、伝統的に安全性を高めることに投資を集中させてきました。しかし、このアプローチは、急速に変化する脅威の状況を考えると、もはや十分ではありません。簡単に言えば、安全、警戒、回復力、という 3 つの不可欠な能力を実現するためのサイバーリスク管理プログラムの構築を金融サービス企業は検討する必要があります（図表 4）。

「多層防御」戦略によるセキュリティの強化

金融サービス企業が予防的でリスクインテリジェントなコントロールの設計と実施によってシステムの安全を確保する上で、既知の脅威とコントロール、業界標準、規制の十分な理解により指針が提供されることがあります。金融サービス企業では、先進的なプラクティスに基づいて、既知および新たな脅威に対処するための「多層防御」アプローチを構築することができます。これは、相互に補強し合う多数のセキュリティ層からなり、これによって冗長性が提供されるとともに、攻撃を阻止できないまでも、進行中の攻撃の進捗を遅らせることができます。

ご存知でしたか？
もし金融サービス企業が、サイバー攻撃を回避しようとするのであれば、最もセキュリティ支出を増加させなければならないのです

金融サービス企業が理想的な防御の状態に達しようとすれば、最も急激な支出の増加に直面することになるでしょう。サイバー攻撃の95%を撃退するには、今の約13倍増の1社当たり2億9240万ドルが必要となるだろう[15]。

「今日の環境では、防御によってすべてのセキュリティインシデントを防止できると期待することは非現実的です。金融業界は、セキュリティインシデントが発生した時点でそれらを検知する能力を向上させて、ビジネスや重要なインフラへの影響を最小限に抑え、包括的なフレームワークの中でこれらの能力を組み合わせる必要があります。Quantum Dawn 2[16]によって、参加者はサイバー脅威を前にして、安全であるだけではなく、警戒と回復力も必要であるということが理解できます」

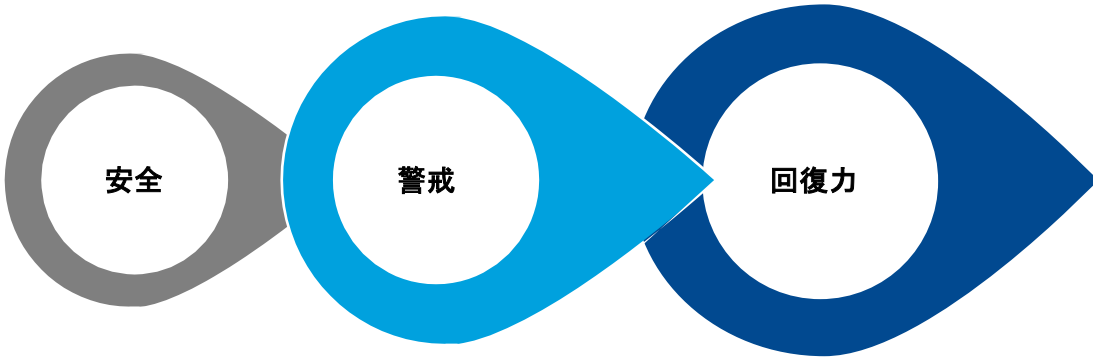
– エド・パワーズ、ナショナル・マネージング・パートナー、サイバーリスク・サービス、デロイト&トウシュ LLP[17]

効果的な早期検知及び警報システムによる警戒の強化

新たな脅威や攻撃者の動きの両方を検出するためのプログラムの強化による早期検知は、損失の抑止と軽減に向けた重要なステップとなります。高度かつ適応的な警報／レポーティングシステムを組み込んだインシデント検知によって、企業全体でITおよびビジネスの大量のデータ、そして様々なインシデントインジケーターの関連付けと分析の自動化が可能になります。金融サービス企業の監視システムは1日24時間、1年365日間動作し、効率的なインシデント処理と修復プロセスに対する十分なサポートを備えている必要があります。

図表 4:「安全、警戒、回復力」戦略によるサイバーセキュリティの改善

伝統的に、安全性に焦点があたっていました。しかし、進化するサイバー脅威の状況によって、よりダイナミックでバランスのとれたサイバーセキュリティ能力へのシフトが必要となるでしょう。



安全: 既知および新たな脅威からの保護のためのリスクによって優先付けされたコントロールの強化、業界のサイバーセキュリティ標準と規制の遵守

警戒: 環境全体を通じた状況認識の改善による違反や異常の検出

回復力: 迅速に通常の業務に復帰し、事業への損傷を修復する能力の確立

出所:デロイト金融サービスセンターの分析

テストと危機管理プロセスのシミュレーションによる回復力の強化

破壊的な攻撃能力が勢いを増す中で回復力の重要性が高まるでしょう。金融サービス企業では、物理的な攻撃や自然災害からの回復に係る計画を従前から行っているので、サイバー脅威に対する回復力に関してもほぼ同様な対処が可能でしょう。金融サービス企業は、複数の次元にわたって全体的なサイバー回復力を考慮する必要があります。第一に、システムおよびプロセスは長期間に及ぶストレスに耐えることができるように設計とテストを行うことが可能です。これには、重要なオンライン・アプリケーションのサイバーエコシステムに対する依存度の査定による脆弱度の判定が含まれる場合があります。第二に、金融サービス企業は、攻撃の優先順位を即座に決定し、迅速に業務を復旧してサービスの混乱を最小限に抑制するための優れた戦略を導入することが可能です。最後に、事業部門、IT、コミュニケーション、広報、および組織内の他の分野を含む様々な部門の参加によって、堅牢な危機管理プロセスを構築することができます。

「安全、警戒、回復力」モデルへの変革

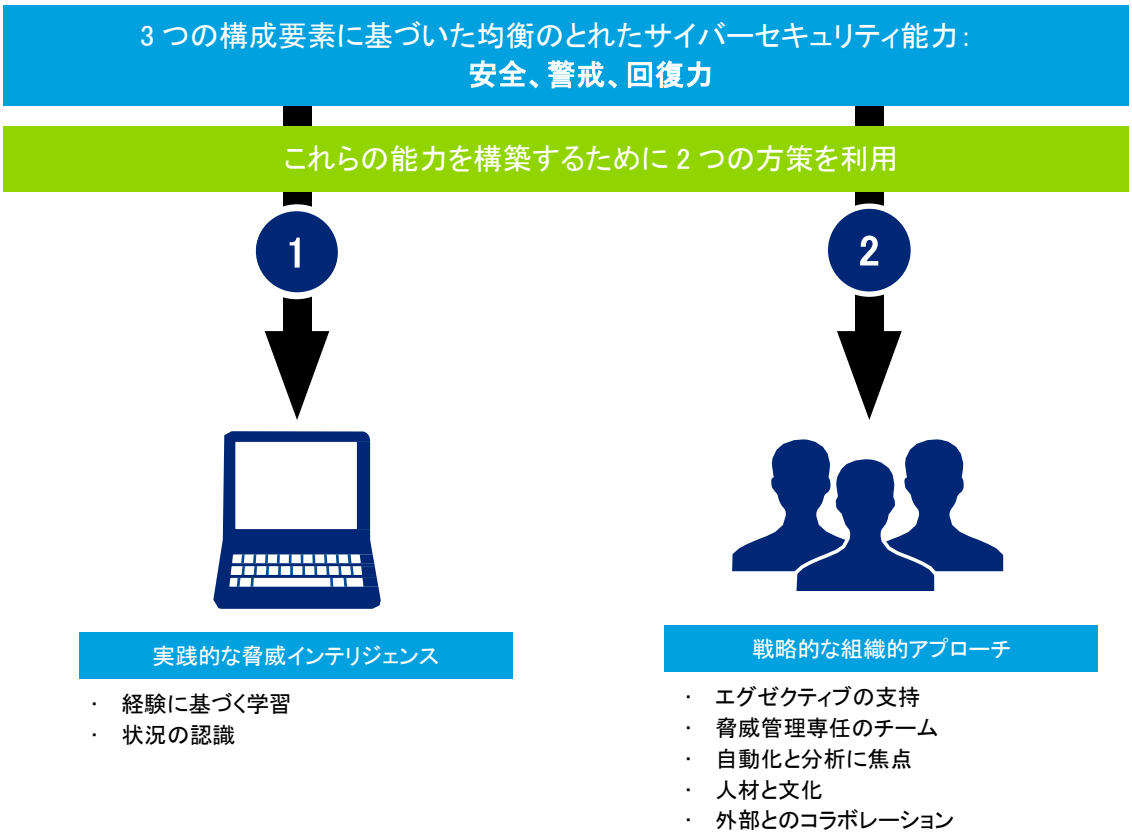
金融サービス企業は、より安全で、警戒と回復力を強化するためのプログラムの確立、つまりサイバーリスク管理プログラムの転換をどのようにすれば実際に始めることができるでしょうか。多くの金融サービス企業では、進化するサイバー脅威の長期的な管理を目標とするに当たって、以下の二つの重要な方策が取られています。
（図表 5）:

1. モデルにある 3 つの構成要素すべてにわたってバランスの取れた能力をサポートする実践的な脅威インテリジェンスの開発
2. サイバーセキュリティを単なる「IT の問題」としてではなく、戦略的な事業の問題として認識する断固たる行動による組織的な課題への対処

実践的な脅威インテリジェンス

金融サービス企業のエグゼクティブは、インテリジェンスによってアクションが決定される学習する組織の構築が、複数の次元にわたる成功にとってますます重要になる可能性が高いということを認識しています。サイバーセキュリティにおいても、安全、警戒、回復力を可能とする上でリアルタイムの脅威インテリジェンスが重要な役割を果たしており、その例外ではありません。もちろん、ここでいうインテリジェンスというのは、多くのベンダーがインテリジェンスという言葉を使って、脅威インテリジェンスをデータフィードの形態で提供しているような、既知の脅威インジケーターに関する生データの集合だけを意味しているわけではありません。脅威インテリジェンスは、自動的な手段および直接的な人間による、内部および外部の広範なソースからの脅威に関する意味のある洞察の導出も意味しています。

図表 5: サイバーセキュリティ管理への多面的なアプローチ

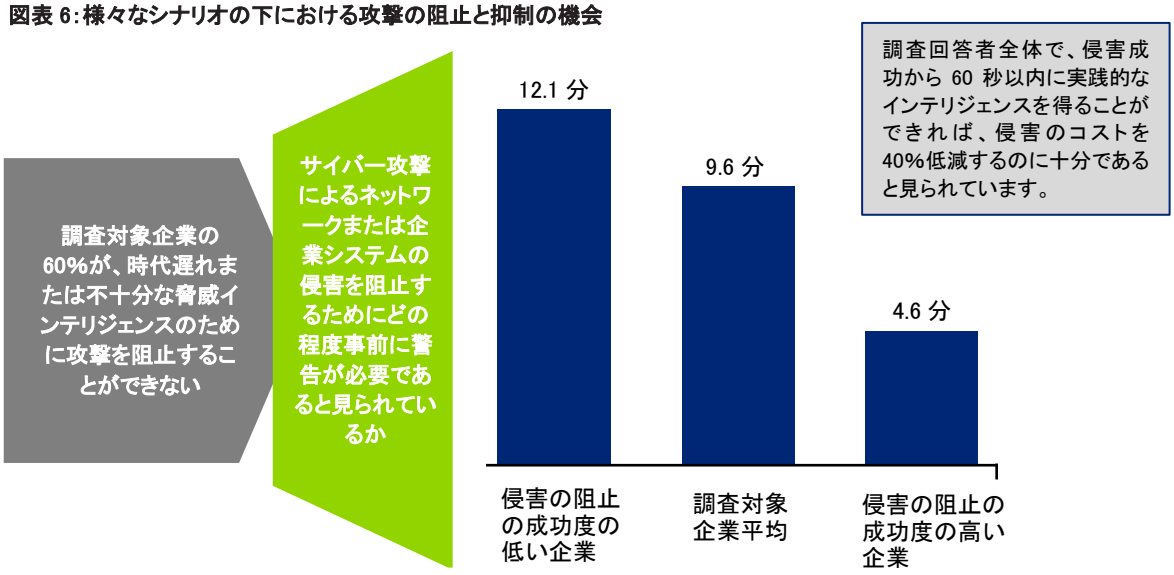


出所: デロイト金融サービスセンターの分析

リアルタイム・インテリジェンスの利用可能性は、組織におけるサイバー攻撃の阻止と影響の抑制に寄与

Ponemon Instituteの最近の研究では、調査対象のIT幹部は、セキュリティ侵害まで10分未満の時点での事前通知であっても、それは脅威を無力化するために十分な時間であると考えていることが明らかにされています[18]。侵害後60秒の通知であっても、セキュリティ侵害のコストは平均で40%低減される可能性があります[19]（図表6）。

図表 6：様々なシナリオの下における攻撃の阻止と抑制の機会



出所：Ponemon Institute[20]、デロイト金融サービスセンターの分析

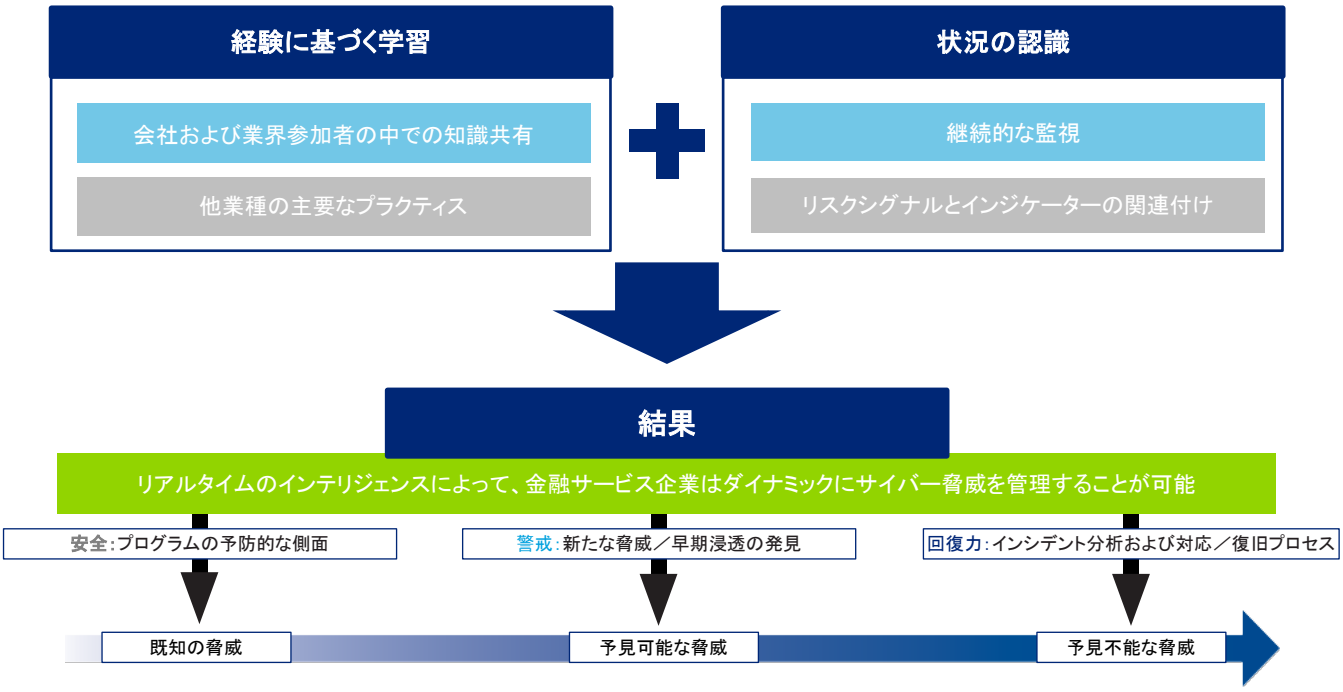
脅威データが実践的なものであるためには、組織にとって意味のある文脈でデータを見る必要があります。金融サービス企業のデータ収集および処理能力の成熟度が高まるのに伴って、自動化を利用して重要なリスク領域に直接的に関連する情報をより的確にフィルタリング／強調することが可能です。このように、脅威インテリジェンスは、安全、警戒、回復力の能力を構築する基盤になります（図表 7）。それでは、金融サービス企業はどのようにすれば、このダイナミズムを生み出して、インテリジェンス主導のサイバーセキュリティモデルに移行できるのでしょうか。

経験に基づく学習：サイバー攻撃者が標的の弱点を利用するように、金融サービス企業は攻撃者を十分に理解し、攻撃者のアキレス腱を特定することが可能です。金融サービス企業は、個別企業および業種のレベルでの過去における侵入から学ぶことが可能です。また、金融サービス企業の多くは、航空宇宙や防衛などの他の業種からの教訓を借りて、新たな手法、作戦、コントロールを導入することも可能です。

これらの教訓には、攻撃の性質、戦術とパターン、封じ込め戦略に関する理解が含まれており、またそれによって、金融サービス企業がサイバー攻撃から自社を守る上で考慮すべき以下のようないくつかの質問が提起されます：

- 攻撃者は誰で、その動機は何か？
- サイバー攻撃者はいかにして、高い攻撃成功率を上げることができるのか？
- 攻撃者の高い専門性によるものか、被害者の無知が招いた結果なのか？もし、そうであれば、それはどのように対応可能か？
- 金融サービス企業のシステムへ侵入する際に、攻撃者が直面する共通の課題にはどのようなものがあるか？
- 他の金融サービス企業／業界はこのような攻撃をどのように扱っているか？

図表 7:新たなサイバーセキュリティモデルの基礎になるリアルタイムの脅威情報



出所:デロイト金融サービスセンターの分析

状況の認識：金融サービス企業は、外部と内部の両方の脅威に焦点を当てた継続的な監視プログラムによって経験に基づく学習を補完することができます。継続的な監視によって、脅威環境に対する状況認識を向上させるために、エコシステム全体にわたるリスクシグナルとインジケーターを把握することができます。これによって、組織における攻撃パターンの特定と、防衛と対応のメカニズムを受動的なスタンスから能動的なスタンスへの移行が可能となります。また、継続的な監視は、攻撃者が金融サービス業界に対して利用している対応速度の問題への対処の第一歩となります。

多くの企業では、学習する組織への転換は、攻撃者の動機と攻撃手法の理解が十分できていないという弱点に対処するためのアプローチを開発する必要があることを意味しています。経験から学び、組織内外の両方で情報を共有することは、多くの金融サービス企業がかかえる攻撃の発見と攻撃からの回復の能力についての弱点に対処する上で有用であるでしょう。

ご存知でしたか？
研究では、インサイダーの脅威の検出と対応のために IT システムが十分に導入されていないということが明らかにされています

金融サービス企業内での内部者の不正例（サイバーベース）のうち、ソフトウェアとシステムを用いて検出されたのはわずか6%に過ぎません[21]。

「IT の問題」から戦略的な事業の問題への変化

金融サービス企業では、自社だけではなく、市場のシステミックな安定性に対してサイバーリスクが提起している問題の大きさを認めているかもしれませんが、この重要事項は必ずしも企業全体にわたって十分に認識、あるいは把握されているとは言えません。サイバー脅威プログラムの成功と失敗についての詳細な分析から、サイバーリスク管理に対するより包括的なアプローチを策定するために、経営陣が取ることのできる以下の潜在的なアクションが導かれました。

1	サイバーリスク戦略を中核的な企業戦略の不可欠な一部として幹部レベルで推進すること
2	セキュリティへの動的でインテリジェンス主導のアプローチのために専任のサイバー脅威管理チームを確立すること
3	内部および外部のリスクの透明化のために自動化とアナリティクスに注力すること
4	サイバーリスクに対する認識の高い文化の一環として、防衛チェーンにおける「人」のリンクを強化すること
5	共通の敵に対処するため、サイバーセキュリティのコラボレーションを企業の壁を超えて拡張すること

アクション 1: サイバーリスク戦略は幹部主導であり、明確な説明責任を伴う必要がある

私たちが接触している金融サービス企業で行われている議論の多くは、サイバーリスク管理の説明責任のモデルと、事業部門、最高情報責任者（CIO）、最高情報セキュリティ責任者（CISO）、IT リスクオフィサーの役割に関するものです。CISO や IT リスクオフィサーがサイバー上の戦いに果敢に挑んでいる一方で、上級経営陣や広範な IT チームからの支援が限られているということもしばしば見られます。また、CISO が、防衛ラインという文脈の中での自分の役割の定義付けに苦労しているケースもしばしば見られます。CISO は主導者なのでしょうか、運営担当者あるいは監督機能なのでしょうか。最終的な結果として、これらの内部での苦労は有効でないサイバーリスク管理プログラムにつながる可能性があります。

ご存知でしたか？
Financial Services Sector Coordinating Council では、俊敏なリスクベースのアプローチを議論しています

すべてのサイバーセキュリティフレームワークは高度に構造化されつつも、新たな脅威の出現にリアルタイムに適応できる十分な機敏性と柔軟性を備えている必要があります。当初のリスクベースのアプローチを欠いた固定的な「チェックリスト」となる標準または指針は、結果として金融サービス企業が「遵守状態」にあるものの、有効な安全確保がなされていないという状況となる可能性があります [22]。

解決の方向性

サイバーリスクが、成長とイノベーションの課題に密接に関連しているのであれば、なぜサイバーリスク管理の責任が組織内でトップから複数のレベルを下ったポジションに権限委譲されているのでしょうか。CISO や IT リスクオフィサーが極めて重要な役割を果たすことは明確ですが、企業は持続可能な成功のために、最高業務執行責任者（COO）または最高管理責任者（CAO）に相当する者を、部門を横断するチームを率いて、サイバーリスク関連の課題を推進する責任者に任命することを考慮するべきです。上級者の任命と部門横断的な委員会の設置によって、企業の経営陣はサイバーリスクが単なる技術の問題ではなく、企業全体の課題であるという明確なメッセージを送ることができます。この委員会は、リスクアピタイトの決定および企業のリスク管理戦略の策定を主導することができます。この委員会はまた、サイバーリスク管理のための防御ラインモデルを正確に定義し、従業員に説明責任を課すことができます。CIO 及びその直属はインフラストラクチャとアプリケーションの両方に関連するリスク管理のオーナーシップを取ることを考慮しなければならず、人事及び他の部門は特にインサイダーの脅威への対処における、各々の役割を理解する必要があります。最後に、ビジネスリーダーはデータの分類と保護に関する説明責任を負うことができます。

アクション 2:セキュリティへのダイナミックでインテリジェンス主導のアプローチの導入と維持のための専任のサイバー脅威管理ユニットの確立

私たちは、有効ではない管理業務によって脅威につながる可能性のシナリオをいくつか知っています。一部のケースでは(現在ではまれなケースですが)、企業に専任の脅威管理チームがないという場合があります。第二に、チームが存在する場合であっても、チームの使命が明確ではないか、使命を達成するための十分なリソースが配分されていないという場合がしばしばあります。また、チームは正式に確立されているものの、広範な IT と事業部門との運営モデルや情報のフローが定義されていないという場合も見られています。

解決の方向性

検知時間を短縮し、多くの場合においてインシデントを完全に回避するチームの能力にとって、迅速な情報共有、積極的なコラボレーション、集団的な学習が極めて重要です。小さな規模と限定的なミッションで始める場合でも、金融サービス企業は脅威及び強化を要するコントロールに関して広範なチームにアップデートを提供する責任を負う専任のサイバー脅威インテリジェンスユニットの設置を検討すべきです。このユニットでは、インフラストラクチャ、アプリケーション開発、脆弱性管理、セキュリティ運用、インシデント対応とフォレンジック、不正などを含む、組織の他の責任部門との間での運営モデルと情報のフローが定義されている必要があります。該当するプロセスとツールによってサポートされた、この相互関係のモデルはサイバースペースにおいて安全性と警戒度を確保するためのファブリックを構築する上で極めて重要です。

アクション 3:内部および外部のリスクの透明化のために自動化とアナリティクスに注力

多くの金融サービス企業では、インフラは複雑で標準化されておらず、サポートモデルはサイロ化されており、これが透明性と迅速な情報フローの望まれる目標に対する主要な障壁となっています。多くの企業においては、優れたアセット/コンフィギュレーション管理実務の基盤的能力が存在していないか、十分に成熟していません。自社環境に出入りするネットワークトラフィックに対する透明性のない企業もあれば、たとえあっても、それが業務運営の目的にのみ利用され、リスク管理目的には活用されていない場合もあります。内部者の脅威が最近注目されていますが、企業においては機密に関連する職務の定義と監視に関する優れたプロセスが存在せず、その結果として危険信号が見逃されるケースもしばしば見受けられます。

解決の方向性

金融サービス企業は、自社の IT セキュリティ投資を再検討し、自社の環境で必要とされる自動化とアナリティクスを構築するための投資の優先順位を上げることを検討する必要があります。残念ながら、多くの場合、少し例を挙げるだけでも、これにはアプリケーションやインフラストラクチャ(ネットワークおよびホスト)、ユーザー、アカウント、取引などの膨大な数の分野が含まれる可能性があります。これは対処できないように見えるかもしれませんが、80/20 ルールが適用可能であり、またインテリジェンス主導のアプローチが重点分野に優先順位を付ける上で役立ちます。また、金融サービス企業は、過去の履歴分析のために、過去 3 カ月から 6 カ月分の重要なデータの保存を検討すべきです。多くの大企業では、これは数百テラバイトのデータになりますが、これは新たな現実であり、サイバー世界で事業を行うコストです。ソーシャルメディアアナリティクスも、多くの企業がインテリジェンス、ブランド保護のため、そしておそらくは最も重要なことに、危機管理において細心の注意を払っている領域の一つです。

ご存知でしたか?
研究では金融サービスにおける IT セキュリティ予算が不十分であることが示されています

グローバルな金融機関の 44%が、有効な IT セキュリティプログラムの実施に対する主要な障壁として十分な予算がないことを挙げています [23]。

アクション4：サイバーリスクに対する認識の高い文化の一環として、防衛チェーンにおける「人」を強化することが可能

「鎖の中の弱いリンク」としての人間に焦点を当てたサイバー攻撃の頻度が増えているにもかかわらず、この弱点に対処するための投資も、あるいはサイバー意識の高い全般的な文化を醸成するための投資も増加していません。たとえば、デロイトのサイバーリスク・サービスが実施したスピアフィッシング[24]テストでは、多くの場合において経営トップ層やそのアシスタントがこのような悪意のある攻撃の一般的な標的となっていることが示されています。一部の金融サービス企業においてはサイバー研修が義務付けられていますが、従業員はこれらを理論的なもので、退屈なものであると考えがちです[25]。私たちの経験でも、サイバー意識の高い組織では、サイバー意識の高い従業員が攻撃と不正の検知に重要な役割を果たし、中長期的に高い投資収益率を示す可能性が高いということが示唆されています。

解決の方向性

金融サービス企業においては、従業員が職能面での専門知識を持っているとしても、疑わしいサイバー活動を発見するスキルを必ずしも持っているとは限らないということを理解することが重要です。サイバー研修および意識向上に関連した戦術の大幅な変更が必要とされる可能性が高く、組織はユーザーの経験を考慮し、また同時に情報が提供される、「人間中心」のアプローチを採用する必要があります。先進的な実務例には、現実的なシミュレーションに組織の各部門を参加させるサイバー戦争ゲーム演習や、洞察に満ちたトレーニングビデオ、あるいは幹部向けのタブレットベースのアプリケーションがあります。

「最新のツールを追いかけることは、サイバーリスク管理の一部ですが、それだけではありません。ユーザーの心を本当に変えなければなりません。技術よりも人を重視することをCIOは検討すべきです。企業のセキュリティポリシーの理解を証明する22ページの法的文書をクリックするようにユーザーに求めるということではありません。むしろ、ユーザーが組織のセキュリティとプライバシーの課題、そしてその課題に応える上での各自の役割を理解できるように、簡潔さでユーモアに富み、その他の集中できる手法を試みる必要があります」

— ラリー・クインラン、CIO、デロイトサービス LP[26]

アクション5：共通の敵に対処するためサイバーセキュリティのコラボレーションを企業の壁を超えて拡張	解決の方向性
サイバーリスクの課題は多くの場合、金融サービス企業の境界内だけで解決することは不可能です。しかし、一部の企業ではサイバーエコシステムの他のメンバーとの関係の構築に時間や資金を費やしていません。情報共有の多くの正式なチャネルがあるにもかかわらず、実際に有意義なインテリジェンスの共有は、多くの場合において依然として信頼できる仲間に限られています。接点の確立はインシデントの予防及び対応の両方に役立ちます。最悪の事態が発生し、金融サービス企業が危機管理活動のために、自社のコントロール外にあるエコシステムからの支援を必要とする場合に特に必要性を強く感じることになります。	金融サービス企業は業界内での関係構築と官民の連携の推進から大きな利益を得ることができます。それには時間と労力を要しますが、長期的には利益となります。金融サービス企業は、サイバー危機に備え、潜在的には支援を受けるため、法執行機関、フォレンジック、インシデントレスポンス専門家、サイバー関連に精通した弁護士事務所、コミュニケーション／広報会社との関係を構築しておくことが推奨されます。また、金融サービス企業は、通信会社および主要なハードウェアとソフトウェアのプロバイダなどの重要なサービスプロバイダーとの関係を構築し、緊急の際に重要なリソースへのアクセスを得ることを考慮すべきです。さらに、金融サービス企業は、業界団体や政府機関（たとえば、多くあるなかでもFinancial Services' Information Sharing and Analysis Centerや米国国土安全保障省など）を活用して自社の目標を推進し、先進的な実務を学ぶことが可能です。

「Quantum Dawn 2は、民間セクターと政府の間の情報共有がサイバー犯罪と闘うための最も有効な方法の一つであるということを証明しました・・・ この情報共有とその他の活動を推進する法制化は、米国が金融システムに対するサイバー脅威をより効果的に軽減することに資するとみられます」

― ジャド・グレッグ、最高経営責任者（CEO）、SIFMA [27]

要約

金融サービス企業に対するサイバー攻撃は、ますます多様化し、予見することができなくなりつつあります。しかしサイバー攻撃は消滅することはありません。サイバー攻撃の多くは、経済的な利得のために行われていることが多いのは、皆さまもご存知のとおりです。しかし、システムの破壊や市場にパニックを起こすことを狙う社会的、政治的な目的を持つグループも加わり、攻撃者層はますます拡大しています。
同時に、現在の経済情勢によって、金融サービス企業は新たな技術とビジネス手法を利用して継続的に競争優位を生み出し、収益性を高めることを求められています。その変更によって新たな脆弱性が生まれる可能性があります。ハッカーは容赦のない機敏さでそれを利用することが可能であり、実際に利用しています。

映画*「インセプション」*では、攻撃者と標的の両方がいかに自らの強みと相手方の弱点を活用するかが強調されています。攻撃が重大なものとなる場合には、不可避のサイバーリスクに対して金融サービス企業の準備態勢を整えることができるのは、回復力が高く柔軟なサイバーセキュリティモデルであるとみられます。このように、金融サービス企業は準備態勢のレベルを引き上げ、以下の3つの基本的な性質の達成を目標とする、新たなサイバーリスク管理のパラダイムに進化することを考慮する必要があります:

- 基盤的／予防的なコントロールとポリシーへのリスク主導の投資による既知の脅威に対する***「安全」***
- 非常に複雑で、データの飽和する環境において、新規の脅威や異常なパターンの検出能力の改善による***「警戒」***
- 組織が可及的速やかに攻撃から回復し、直接および間接の両方の損害を最小化することを可能とする***「回復力」***

広範な情報源から導出される実践的な脅威インテリジェンス、そしてサイバーリスク意識、説明責任、効果的で継続的な適応を浸透させる十分に定義されたガバナンスプロセスが、このパラダイムシフトを推し進める重要な燃料となります。多くの企業にとって現在一般的にITリスク管理プログラムと呼ばれているものは、経営幹部の主導するサイバーリスク管理に進化し、戦略的事業計画の不可欠な一部分となります。この変革は戦略的な事業の課題によって必須のものとなります。すなわち、この新たなアプローチをマスターする金融サービス企業は、より俊敏なサイバーリスク管理アプローチを組み入れることによって現在進行中のデジタル革命を自社に有利なように利用できるため、業界の最前線に立つことができる可能性があります。

巻末脚注

[1] “2013 Cost of Cyber Crime Study: United States,” Ponemon Institute (sponsored by HP Enterprise Security), October 2013; “2012 Cost of Cyber Crime Study: United States,” Ponemon Institute (sponsored by HP Enterprise Security), October 2012.

[2] この調査では、企業がサイバー犯罪インシデントに対応する際に要する合計コストの検討が行われており、それには内部でのセキュリティ関連の活動（検出、調査とエスカレーション、復旧、事後対応、封じ込め）および外部の影響／コスト（情報の損失または盗難、事業の混乱、設備への損害、収益逸失）などが含まれています。

[3] “2013 Cost of Cyber Crime Study: United States,” Ponemon Institute (sponsored by HP Enterprise Security), October 2013.

[4] “2012 Cost of Cyber Crime Study: United States,” Ponemon Institute (sponsored by HP Enterprise Security), October 2012.

[5] “Risk Index 2013,” Lloyd’s, July 2013.

[6] Ivy Schmerken, “Cyber Crime on Wall Street,” Wall Street & Technology, July 16, 2013.

[7] 米国上院歳出委員会での声明、ワシントン D.C.、2013 年 6 月 12 日。

[8] “Not Your Average Cybercriminal: A Look at the Diverse Threats to the Financial Services Industry,” Mandiant, September 23, 2013.

[9] “Agari Email Trust Index:3rd Quarter Edition,” Agari, November 2013.

[10] Ivy Schmerken, “Cyber Crime on Wall Street,” Wall Street & Technology, July 16, 2013.

[11] “2012 DTTL Global Financial Services Industry Security Study,” Deloitte Global Services Limited, September 2012.

[12] 調査では、組織の情報セキュリティプログラムの成熟度を 1～5 のレベルで定義しています。レベル 3 – 定義（一連の定義され、文書化された標準プロセス、時間をかけて一定の改善）、レベル 4 – 管理（プロセス評価指標、効果的な管理統制、品質を損なうことなく適応）、レベル 5 – 最適化（継続的な改善、イノベーションに重点）。

[13] “Threat Landscape: Financial Services (Verizon DBIR 2011–2013),” Verizon, September 2013 で使用されたデータのサブセット。

[14] 前掲書

[15] Eric Engleman and Chris Strohm, “Cybersecurity Disaster Seen in U.S.Survey Citing Spending Gaps,” Bloomberg, January 31, 2012.

[16] Quantum Dawn 2 サイバー演習（QD2）。2013 年 7 月 18 日に SIFMA が主催。金融セクターの 50 機関以上からの 500 人を上回る参加者が、それぞれのサイバー危機対応計画に沿って演習を実施しました。これには、金融セクター全体および政府機関との連携による情報の共有をどのように行うかということも含まれていました。

[17] “SIFMA Announces Key Findings of Quantum Dawn 2,” SIFMA, October 21, 2013.

[18] “Live Threat Intelligence Impact Report 2013,” Ponemon Institute (sponsored by Norse Corporation), July 2013.

[19] 前掲書

[20] 前掲書

[21] Adam Cummings, Todd Lewellen, David McIntire, Andrew P. Moore, and Randall Trzeciak, “Insider Threat Study:Illicit Cyber Activity Involving Fraud in the U.S.Financial Services Sector,” CERT Insider Threat Center of Carnegie Mellon University’s Software Engineering Institute, July 2012.

[22] “Developing a Framework to Improve Infrastructure Cybersecurity,” Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, April 8, 2013.

[23] “2012 DTTL Global Financial Services Industry Security Study,” デロイトグローバルサービスリミテッド、September 2012.

[24] スピアフィッシングには、攻撃者が侵害を望む、組織あるいは専門的グループ内の特定の個人（あるいは関連する個人のグループ）を標的とした攻撃が含まれます。これは、攻撃者が標的と一定の意図された親密度を確立することに依存しています。

[25] “Cyber Training 3.0:New Solutions Addressing Escalating Security Risks,” NASCIO, June 3, 2013.

[26] “An Interview with Deloitte Services LP CIO Larry Quinlan,” The Wall Street Journal’s CIO Journal, February 5, 2013.

[27] “SIFMA Announces Key Findings of Quantum Dawn 2,” SIFMA, October 21, 2013.

連絡先

日本の連絡先

デロイト トーマツ リスクサービス
パートナー
丸山　満彦
サイバーセキュリティ担当
03 – 6213 – 1300
mitsuhiko.maruyama@tohmatsu.co.jp

デロイト トーマツ リスクサービス
パートナー
大沼　靖秀
金融機関向けサイバーセキュリティ担当
03 – 6213 – 1300
yasuhide.onuma@tohmatsu.co.jp

Executive sponsor
Ed Powers
Principal
Deloitte & Touche LLP
+1 212 436 5599
epowers@deloitte.com

Authors
Vikram Bhat
Principal
Deloitte & Touche LLP
+1 973 602 4270
vbhat@deloitte.com

Lincy Francis Therattil
Assistant Manager
Deloitte Center for Financial Services
Deloitte SVCS India Pvt Ltd.

Deloitte Center for Financial Services
Jim Eckenrode
Executive Director
Deloitte Center for Financial Services
Deloitte Services LP
+1 617 585 4877
jeckenrode@deloitte.com

Industry leadership
Bob Contri
Vice Chairman
U.S. Financial Services Leader
Deloitte LLP
+1 212 436 2043
bcontri@deloitte.com

本レポートの制作をサポートし貢献してくれた以下のデロイトのプロフェッショナルに感謝の意を表します。:

Michelle Chodosh, Marketing Manager, Deloitte Services LP
Lauren Fischer, Lead Marketing Specialist, Deloitte Services LP
Mary Galligan, Director, Deloitte & Touche LLP
Lisa DeGreif Lauterbach, Marketing Leader, Deloitte Center for Financial Services, Deloitte Services LP
Jennifer O'Neill, Director, Deloitte Services LP
Ash Raghavan, Principal, Deloitte & Touche LLP
Beth Ruck, Marketing Leader, Vigilant by Deloitte, Deloitte & Touche LLP
Irfan Saif, Principal, Deloitte & Touche LLP
Surabhi Sheth, Executive Manager, Deloitte SVCS India Pvt Ltd
Val Srinivas, Research Leader, Banking & Securities, Deloitte Services LP
Prasad Yadav, Senior Analyst, Deloitte SVCS India Pvt Ltd

Deloitte Center
for Financial Services