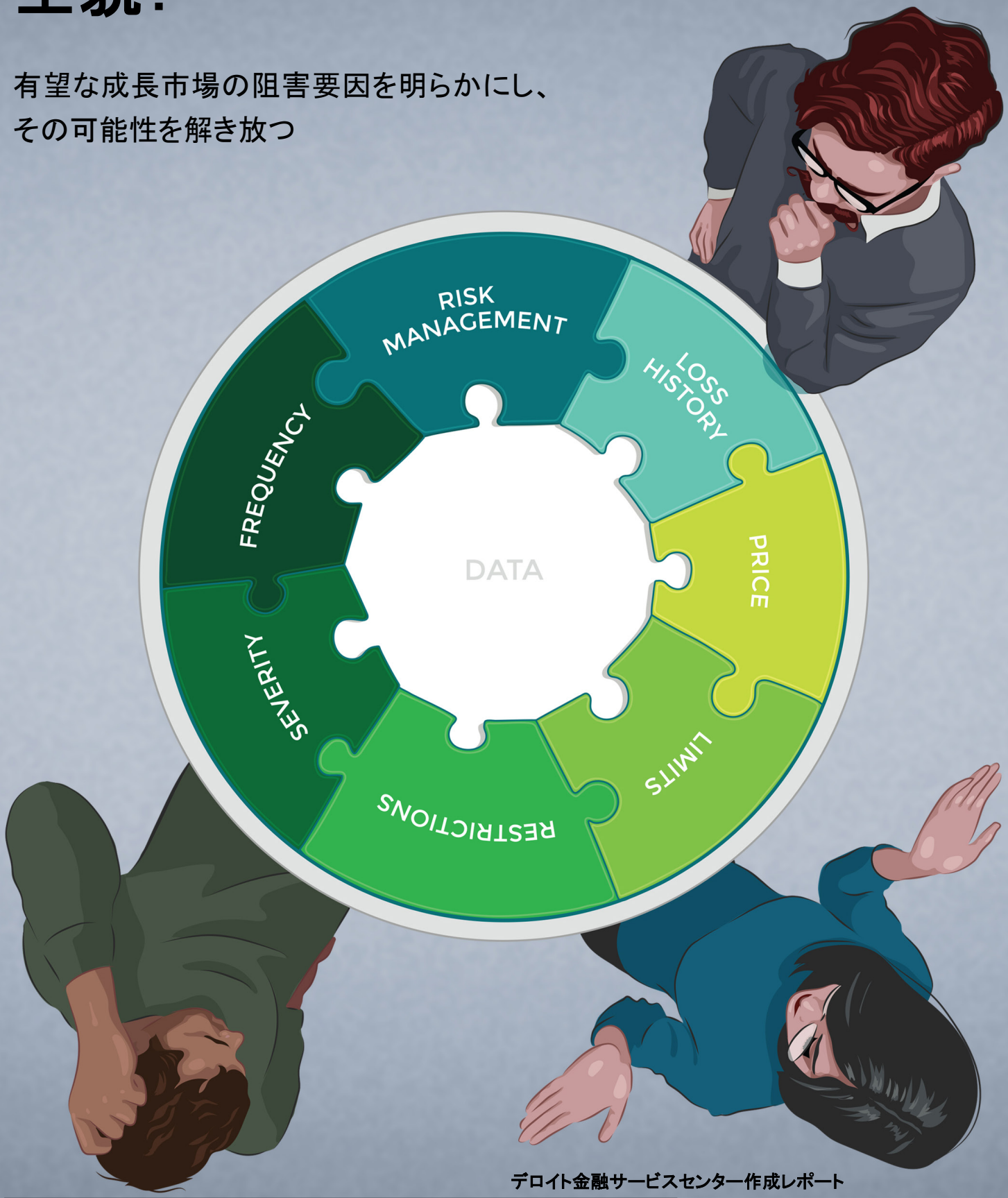
サイバー保険の全貌：

Deloitte. University Press

有望な成長市場の阻害要因を明らかにし、
その可能性を解き放つ



デロイト金融サービスセンター作成レポート

デロイト金融サービスセンターについて

デロイト金融サービスセンターは、米国におけるデロイトの金融サービス関連事業の一部であり、銀行、資本市場の金融機関、投資信託会社、投資運用会社、保険会社、不動産会社などの経営陣が意思決定に際して直面する最も重要な問題に関して最新の見識を提供しています。

当センターは、調査、業界のイベント、討論会などさまざまな場を通じて金融サービスの問題に関する総合的な見解や、刺激的なソート・リーダーシップを、特定の組織上の役割や機能のニーズに合う形で提供しています。

目次

サイバー保険普及に向けての解決策

米国のほとんどの損害保険会社が緩やかに回復する経済や資金余剰の市場、歴史的な低金利環境で成長に苦しむ中、サイバーリスクが上昇しているにも関わらず、サイバー保険の販売がそれほど急速に勢いを増していないのはなぜでしょうか。

規制当局や格付会社が損害保険業界について行った様々な推定によれば、サイバー保険は今のところ米国で年間15億ドルから30億ドルの保険料収入に留まり、2015年の米国内保険会社が計上した保険料総額5,058億ドル[1]に占める割合は極めてわずかです。

しかし、このかなり控えめなスタートにもかかわらず、多くの損害保険業界リーダーらはサイバー保険の将来を強気に見ています。米国保険情報協会（Insurance Information Institute）によれば、今後数年間で米国での売上高が2倍、あるいは3倍に増加するという予測が一部でなされています[2]。アリアンツ・グローバル・コーポレート・アンド・スペシャルティは2025年までに世界全体の市場規模が200億ドル以上になると予測しています[3]。

サイバー保険業界がそうした高い予測水準に到達するには相当の道のりを経なければなりません。多くの事業会社は未だサイバー保険を購入しておらず、購入している場合でも、補償範囲が十分でない傾向があります。米国保険エージェント・ブローカー協会（以下、CIAB）の調査によれば、2016年10月時点でサイバー保険を購入している米国企業は29%に留まります[4]。大企業ほどサイバー保険を購入する公算が大きいものの、大規模な組織の大半が依然として無防備でサイバーリスクのエクスポージャーに晒されています。実際、2015年9月のCIABの調査によれば、その時点では、フォーチュン500企業の40%しかサイバー保険を購入していない上、そのほとんどの企業は、エクスポージャー全体をカバーしていない保険を購入しています[5]。

サイバーリスクに対するエクスポージャーについて消費者意識が高まっているように見えることから、サイバー保険の売上が伸びる条件は熟していると思われています。この消費者意識の高まりの一因には、民間、公共部門へのサイバー被害が大きく報道されることが増え、ID盗難の被害を受ける個人が増加していることにあります[6]。では、業界が埋めるべきエクスポージャーのギャップが大きいにも関わらず、なぜ保険会社は、高額のサイバー保険の引き受けに対して依然として慎重なのでしょうか。また、なぜ多くの潜在的な顧客らは、保険ポートフォリオにサイバー補償を追加するのをためらっているのでしょうか。

保険会社が、拡大しつつあるサイバーリスクに対して慎重に取り組んでいる状況から、積極的になれるものがあるとすれば、それはどのようなものでしょうか。そして損害保険業界は、大小様々な潜在的な顧客が自身のサイバーリスクについて、防御という視点で保険が果たし得る役割についてより深く理解させるために、どのような措置を講じることができるのでしょうか。これら二つの問題に対する取り組みを検討するため、デロイト金融サービスセンターは、様々な損害保険業界関係者にインタビューし、二次調査を実施しました。このインタビューの対象者には、サイバー保険を引き受ける主要保険会社2社（1つは米国、もう一つは欧州の保険会社）のほか、世界市場で企業保険やスペシャリティ保険、再保険のサイバーリスク補償を購入しているブローカー3社が含まれています。我々はまた、保険引受や価格設定に関連する多くの支援業務を行っているデロイトのサイバーリスクサービス部門と協働し、当該業務から得られた教訓をも活用しました。

この調査では、保険会社がサイバー保険を販売しようとするときに直面する様々な重大な阻害要因だけではなく、多くの潜在的な

図1. サイバー保険の需要に対する阻害要因

保険会社の観点から

- **データ不足**
- **進化し続けるサイバー攻撃**
- **破滅的リスクが集積する可能性**
- **提供する補償範囲の狭さ**

消費者の観点から

- **購入者のサイバーリスクや保険のオプションに関する理解不足**
- **サイバーリスクが広範囲に広がる**
- **標準化されていないサイバー保険**
- **法的環境の不安定さ**

出所：デロイト金融サービスセンター

顧客がリスクの一部を第三者に移転しようと考えたときに躊躇する原因が明らかにされました（図1参照）。

保険会社にとって、課題はあるものの有望なサイバー保険市場の可能性を確実なものにするためには、そうした阻害要因を取り去る必要があると思われます。現在のところ、サイバー保険は、保険会社が直面するリスクの評価という点では、分かりやすく包括的で、高い価値の商品やサービスを提供してバイヤーを惹きつけることは依然として未熟な段階にあります。しかしながら、保険会社にとっては、自社の戦略や業務を調整することにより、様々な業界評論家が予測する成長率を達成し、場合によってはそれを超えた成長を遂げ、最も重要なことである利益を生む機会が存在すると思われます。

本レポートでは、市場の成長を妨げる阻害要因およびその解決方法について検討します。そして、教訓的な話として指摘しておきたいのは、サイバー保険の販売に躊躇しているうちになすすべがなくなる可能性があるということです。損害保険業界が早急に解決策を見いだし、適切且つ分かりやすく、手ごろな価格のサイバー保険の提供者としての信頼性を向上させられない場合、キャプティブやリスクリテンショングループ、保険リンク証券といった代替的なリスク移転手段が、最終的に保険会社の進出を制限し、場合によっては保険会社のポジションの大半を取って代わる可能性すらあります。

サイバー保険会社の観点から見た阻害要因

データ不足のために保険会社は予測が困難

保険会社がサイバーリスクを完全に掌中の物とすることが難しい主な理由の一つは、過去のデータが不足しているため、損害発生確率の評価に役立ち得る予測モデルの構築が困難なことです。調査のインタビュー対象者によれば、信頼できるデータの供給が不足している理由には様々なものがあります。その一つは、保険会社が十分な期間、または十分な規模のサイバー保険を販売していないため、必要最低減の社内データが蓄積されていないということです。また、保険会社が利用できる、サイバーセキュリティインシデントに関する総合的で集約された情報源も存在していません。さらに、米国保険情報協会が指摘するように、「大多数と言わないまでも多くの攻撃が報告および発見されないままになっている」[7]ため、サイバー被害のうち大部分が外部に知らされてさえいません。

同時に、多くの州で法律上の通知義務があることにより、報告された被害の大半が個人識別情報（Personally Identifiable Information：PII）を晒してしまうといった違反も絡んできます。しかし、こうした被害報告は、企業やその保険会社が直面するサイバーリスクエクスポージャーのほんの一部にしかすぎないものと見られます。サービス拒否攻撃（DoS攻撃）やランサムウェア、知的財産の盗難といった他のサイバーセキュリティインシデントは、往々にして表沙汰にされません。したがって保険会社は、予測モデルおよび保険引受や価格設定システムを構築する際は、報告に偏りがある可能性を考慮に入れる必要があります。

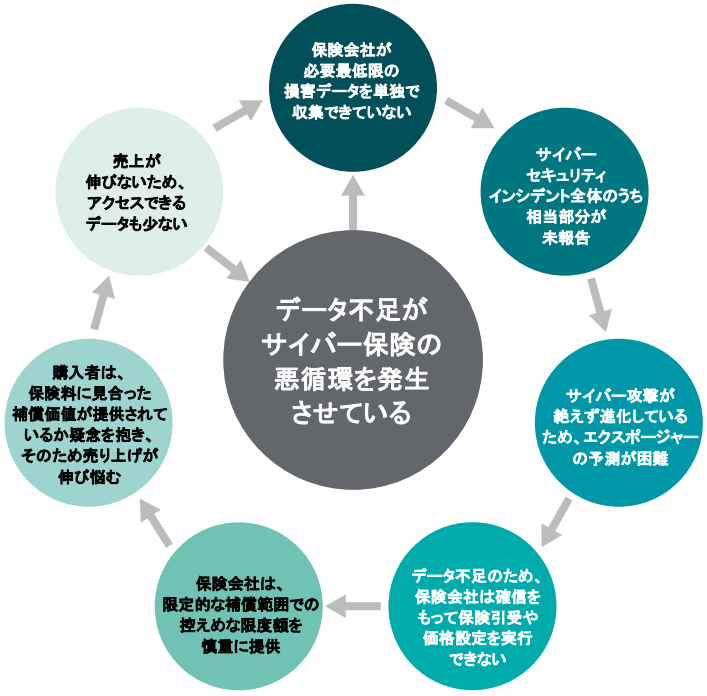
こうしたデータ不足はデータに関連する阻害要因といった「悪循環」を生み出し、ハイエンドマーケットである企業保険市場での独立したサイバー保険の成長を妨げている可能性があると考えられます（図2参照）。第一に、データが不十分なため、保険会社は通常、確信をもって保険引受や保険料設定を行うことができず、その結果、比較的控えめな限度額や厳しく制限された補償範囲を提供することで安全性を保ちます。このことは、請求される保険料に見合った補償価値が提供されているかという購入者の疑念を引き起こし、サイバー保険の売上が伸びず、市場への浸透が進まない状況が生じる可能性があります。これにより、保険会社がエクスポージャーの金額設定を行うために収集できる一次データ量が不足することになります。その結果、保険会社は補償範囲の広い保険を引き受けることが躊躇され売上が伸び悩む、といったサイクルが繰り返されます。

サイバー攻撃が進化し続ける一方、新たなリスクが間断なく出現

あらゆる種類のサイバー保険会社が直面する別の困難は、絶えず進化するリスク固有の変化です。そのために、過去の経験値が限定され、エクスポージャーの予測可能性が低下します。既存のサイバーエクスポージャーの性質が変化し続ける一方、新たなエクスポージャーが間断なく出現しています。デロイト金融サービスセンターが行ったサイバーセキュリティ調査においてインタビューした保険会社や銀行、投資機関の最高情報セキュリティ責任者（Chief Information Security Officer: CISO）は、あるタイプの攻撃に順応している間に、脅威を及ぼす者は絶えず新たな手法やターゲット、侵入地点を考え出して攻撃してくるため、リスク管理は継続的に困難な状況に置かれていると述べています[8]。

本レポートのためにインタビューした相手は、保険会社がより多くのデータを収集し、過去のサイバー脅威に基づき予測モデルを精緻化している間にも、対象となるエクスポージャーが変化し続けていると指摘しました。その結果、ハッカーが次にどのような新しい標的や戦略、手法を考え出すか明確でないため、信頼性の高い予測モデルの作成が困難になります。保険会社は、サイバーリスクに関してまさに何を知らないのか分からない状態に置かれています。

図2. サイバー保険の悪循環



出所：デロイト金融サービスセンター

あるインタビュー対象保険会社は、「我々はサイバーセキュリティ市場に遅れずについていこうと努力していますが、脅威者が何を行い、どんな能力を持つかが常に進化しているため、どのような種類の攻撃や方法が使用されるかを予測するのが非常に困難です」と述べています。

事態を複雑にしているのは、事業の状況も変化していることです。保険会社は既存リスクの計測やモデル化に苦労していますが、一部では、モノのインターネット（IoT）の普及や自動運転車の開発によって生じる新興のサイバーエクスポージャーに業界が遅れずに対応できるかどうかを懸念する動きもあります。こうした技術の進化によって新たなサイバー攻撃の可能性が生じるため、その評価や発見、軽減、保険手配が必要となります。このことは明らかに新たな機会をサイバー保険会社にもたらす反面、検討すべき大量の危険事情（hazard）が付け加わり、たとえあるとしてもさほど多くない過去のデータでそれを捕捉しなければなりません。

保険会社はサイバーエクスポージャーの破滅的リスクが集積する可能性を懸念

多くのサイバー保険会社は、手に負えない量のリスクに対処することに懸念を抱いています。先述したようなデータ不足のためにサイバーエクスポージャーの保険引受や価格設定が相当困難なことに加え、保険会社は、損害が突然集積する事態に対応不可能となることを不安視することがあります。

インタビューしたある保険会社は、「もし明日、ウェブサイトのホストがサービス妨害攻撃、もしくは、ハッキングされたとしたら何が起きるか」と考えました。「ウェブサイトホストがクライアントにサービスを提供できなくなったらどうなるでしょうか。そのプラットフォーム上にウェブサイトを構築した人は全員、第三者のサーバーがオフラインになっている間、オンラインビジネスができなくなる可能性があります。この場合、本当のリスク集積が発生します。サイバー保険の被保険者らが、クラウドやウェブサイトのホスト、電子メールサーバー、共有サービスとしてのソフトウェアなど、一つの籠に入っていないかどうかどうすれば分かるのでしょうか」。

そうした第三者のファシリティやベンダーが、自身のサイバー保険でカバーしている可能性は十分あるでしょうが、それが個々のクライアントの被った損害を十分補償しているかどうかは不明であり、したがって、当該クライアントは、システミックイベントの影響に対処するために自前の保険による補償が必要になる可能性が高いと思われます。

市場で保険を仲介しているブローカーは、特に再保険会社が、複数の会社や国、業界全体にわたる広範な保険金支払いを引き起こす「連鎖的」インシデントの可能性を警戒していると述べました。一部のブローカーは、再保険の相当の支えがない場合、成長の足かせとなり、サイバー保険市場がいつまでも軌道に乗れない状態となることを懸念しています。

インタビュー対象者のうち何人かはテロ保険市場との類似性を挙げました。テロリスクとサイバーエクスポージャーは、どちらも意図的に被保険者に危害を加えようとする行為者が絡んでおり、そうした攻撃がどの時点でも、どのような場所でも、ほとんどすべての人に対して行われる可能性があるという点で似ています（これと異なり自然災害は、特定の地理的地域に発生する可能性が他より高い傾向があるため、予測可能性がより高いと言えます）。2001年9月11日以後、単一インシデントや一連の攻撃によって発生する巨額の損害に対する懸念から、多くの保険会社や再保険会社がテロ保険市場から遠ざかっています。米国全土あるいは世界全体にさえ影響が及ぶ大規模損害が発生した場合、サイバー保険市場が同じように冷え込む可能性があります。

ある保険会社は、「結局のところ、我々は実際にどれほどのエクスポージャーを引き受けたのかよく分からないのです。リスクの源泉がどこにあるのかを十分に知らないためそれを軽減することができません。引き受け側に有用なデータが十分にないため、各々のセグメントについてどの水準が本当に妥当なのか分からない」と述べています。

これとは別の、しかし恐らく同様に厄介な集積したダイナミクスが中小企業市場で展開されているようにみえます。競争が激しい中小企業市場では、多くの保険会社が被保険者を惹きつけて関係を維持するために、標準的な財産・賠償責任保険にほとんどあるいは全く追加保険料を請求せずに、サイバーリスクに関する裏書（endorsement）を追加した商品を提供しています。

そのため、一部の格付け機関では、被保険者である中小企業で、一斉に広範な影響を与えるシステミックリスクが発生した場合、保険会社の帳簿に多額の積立不足のエクスポージャーが集積するのではないかと警戒しています。

サイバー保険商品の魅力を制限するのは視野の狭さ

別の懸念事項としては、サイバーリスクの捉え方の視野が比較的狭いために、多くの保険会社の販売が主に個人識別情報盗難に集中する可能性があるということです。しかしながら、インタビュー対象者によれば、そうした保険は急速にコモディティ化され消費者は価格に敏感になっていきます。その結果、保険会社の長期的な成長や潜在的な利益は限定されてしまいます。

より重要なことは、個人識別情報以外にも、サイバー保険が有効に役立つ多くの複雑なリスクがあるという点です。実際、消費者の機密的な記録を保有していない企業にとって、個人識別情報を対象とするサイバー保険にどのような意味があるでしょうか。

IoT技術を利用して産業用制御システムを運用する製造企業の例を考えてみたいと思います。悪意をもってそれを停止させたり、当該企業が生産する製品に対する妨害工作を行ったりする者によって制御システムが危険に晒された場合、どうなるでしょうか。つまり、自動運転乗用車の製造会社には、理論上、その製品がハッカーによって遠隔的に操作され、盗まれたり、事故へ誘導されたりする独自のリスクが存在しているのです[9]。また、自動運転の商用トラックがサイバー攻撃によって遠隔的にハイジャックされる可能性も考えられます。新たに出現しつつあるこれらのエクスポージャーは標準的な損害賠償保険によって補償されるのでしょうか。それとも、サイバーリスクに関する特定の補償条項や単独のサイバー保険が、より確実なリスク移転の代替手段と成り得るでしょうか。

これらが、ますます複雑化するサイバーリスクの市場へ参入、またはサイバー保険市場でのプレゼンスを拡大しようとする保険会社にとって、立ち向かわなければならない根本的な問題となります。

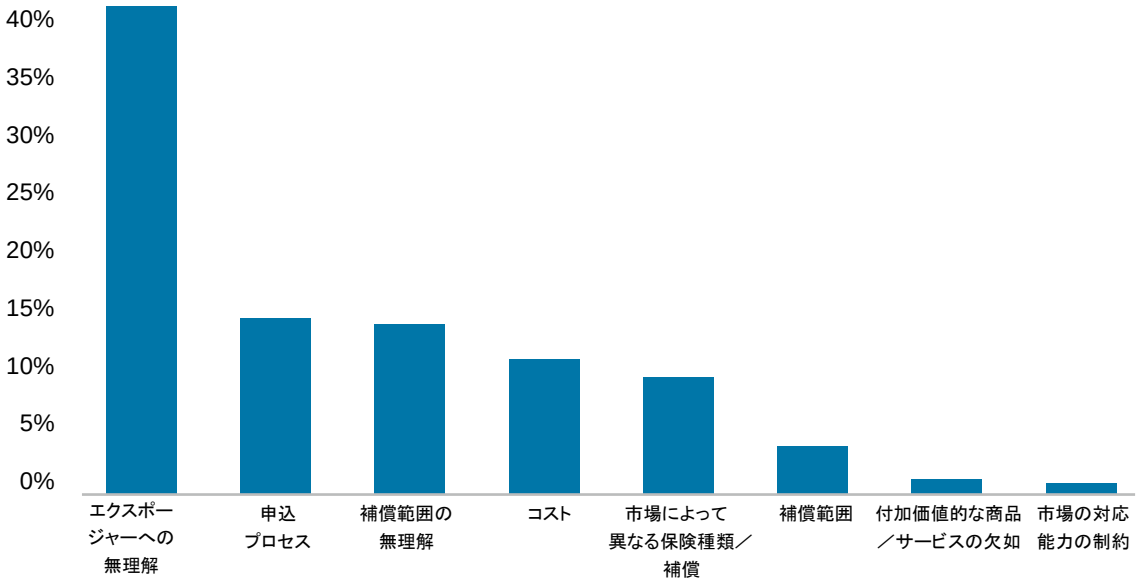
サイバー保険の購入者の観点から見た阻害要因

購入者は往々にしてサイバーリスクや保険のオプションを理解していない

サイバー保険の価値や有用性の判断という点で、データ不足や信頼できる予測モデルの欠如による困難に直面しているのは保険会社だけではないようです。インタビューを行ったブローカーは、購入者は事業の大小に関わらず、直面しているリスクの大きさを正確に定量化するのに苦労することがあると述べています。その結果、自身がどのような種類の補償やどれほどの補償金額を必要としているのか、また、この急拡大するエクスポージャーの少なくとも一部を保険会社に移転することに伴う費用対効果について、確信が持てない状態が生じています。

実際、経験の浅い小規模事業者だけでなく消費者の多くは、直面するサイバーリスク自体すら認識していない状況にあり、利用可能な保険オプションに関しては言うまでもありません。パートナー・リーおよびアドバイゼンが行った調査によれば、ブローカーの42%が、サイバー保険を販売することを妨げる要因として、クライアントの「エクスポージャーへの無理解」を挙げており、これが抜きんでてトップになっています（図3参照）[10]。さらに、CIABによる2016年10月の調査によると、調査対象となったブローカーの内55%が、サイバー保険の補償内容は明瞭ではない、と述べています。

図3. ブローカーが上位に挙げるサイバー保険販売の阻害要因



出所：パートナー・リー（アドバイゼンと共同）、「サイバー賠償責任保険の動向：調査」、2015年8月

これは、1年前のCIABの調査では71%がそのように回答していたことに比べれば改善していると言えるものの、大企業へサイバー保険を仲介するブローカーの過半数は、依然としてこの問題を感じていることを示しています[11]。

別の懸念事項はサイバー保険の価値です。インタビューを行ったブローカーによれば、多くの大企業は、保険会社が提供する補償が、自社の直面するリスクや保険料に十分見合ったものかどうか疑問に思っています。現在のところ、サイバー保険はたいていの場合、補償対象リスクについて比較的低い限度額が設けられていますが、ブローカーによれば、このことが、購入の決断をためらう購入者が多くなる状況を作り出している可能性があるといいます。SANSインスティテュートおよびアドバイゼン・リミテッドの調査によれば、対象となった最高情報セキュリティ責任者(CISO)およびその他セキュリティ専門家のうち、サイバー保険はサイバー攻撃の結果に対応するという点で少なくとも「十分」であると答えたのは48%にとどまっています[12]。

さらに、多くの潜在的な顧客にとっては、新たに出現しているリスクに対する補償がまだ広く知らされていないか、価格が手ごろではありません。先述のように、IoTに依拠して運用を行う企業は、個人識別情報の流出を懸念する企業とは全く異なる一連のエクスポージャーに直面している可能性があります。しかし、メディアや保険市場では、顧客データに関連する被害がはるかに多くの注目を集めています。保険会社がサイバー保険市場の将来について示された楽観的な成長予測を実現しようとするなら、こうした狭いアプローチを拡大する必要があるでしょう。

サイバーリスクが広範囲の補償に広がる可能性

インタビュー対象ブローカーによれば、サイバー保険の販売が抱える問題の1つは、サイバーリスクが、一般賠償責任保険、財産保険、専門業務賠償責任保険、事業中断（business interruption）保険、犯罪保険、その他の標準的な保険を含む様々な商品の一部として組み込まれることがあるという点です。その結果、補償の必要性を評価したり、エクスポージャーに対応した保険を選んだり、複数の選択肢を比較したりする作業が複雑になります。また、フォレンジックや通知、クレジットモニタリング、広報活動、レピュテーションリスク、弁護士費用と和解費用、危機管理、回復費用、規制の違反金などのサイバー関連費用に関する補償について、購入者やその保険仲立人が最善な補償範囲を判断するのは難しい問題といえます。

一方、エクスポージャーが進化し続けるなか、新たなサイバーリスクが定期的に出現しています。その結果、それをどのように保険でカバーするのが最善なのかという問題が生じています。例えば、最近の米国大統領選挙中には、ハッキングによって選挙運動に関する機密的な電子メールが公開されるといったケースがありました。民間部門も同様のリスクに直面しています。企業幹部の機密的な電子メールや内部報告書がハッキングされ、主要な報道機関やソーシャルメディアを通じてその資料が公開され、打撃を受ける可能性があるのです。この場合、内部情報が取引されることによる損失や企業ブランドへのダメージ、あるいは株価の下落といった多様な損害が発生する恐れがあります。

こうした論点が整理されていない不明瞭な市場では、購入者は、既存の保険契約で補償されているものに対し追加でどのような補償が必要になるかを理解できず、サイバー保険の販売が妨げられる可能性があります。

標準化されていないサイバー保険

さらに事態を複雑にしている要因は、サイバー保険では一般的に、保険の諸条件や免責事項が標準化されていないということです。SANSインスティテュートおよびアドバイゼン・リミテッドが今年行った調査によれば、サイバーリスクに関して共通の文言があると答えたのは、ブローカーの19%、保険会社の30%にすぎませんでした[13]。さらに、CIABの2016年10月に行ったサイバー保険に関する調査によると、多くの回答者が、たいていの場合、カスタマイズされた保険契約を通じて補償の引き受けを行っているため、保険会社ごとに異なる専門用語が使用されていると述べています[14]。

保険金を請求するまで何が補償されていないかわからないとし、購入者の多くは依然としてサイバー保険の購入に慎重深い

実際、異なる保険会社から提供される類似したサイバー保険商品では、度々別の特徴を含んでいるため、価値や価格の点で購入者が保険契約を比較するのを困難にしています。インタビューを行ったある大手ブローカーは、市場にはいわゆる「サイバー保険」があるものの、その補償がどのような内容なのか、またエクスポージャーに十分対応できるほど包括的なものかが購入者に明瞭ではないという点で、「損害保険業界は重大なブランド戦略の問題を抱え込んでいる」と言います。

どの保険がどのサイバーリスクを補償しているのか、および保険契約間で異なる文言が、インシデントの発生時に実際に何を意味するのかといった潜在的な曖昧さがあることから、インタビューを行ったブローカーは、多くの購入者が依然として保険の購入に用心深くなっており、また保険金を請求した後になっても補償内容を理解できていない事態を恐れている、と述べました。

実際、サイバーリスクを謳う一つの保険契約、または複数の保険契約間の潜在的な補償内容のギャップが、差しあたり、多くの企業が付保を見送る主な理由になっていると思われます。インタビューを行ったブローカーによれば、企業は、これらの懸念について明瞭化がさらに進み、もう少し市場が淘汰されることを待っており、完全に理解はできず、その文言が依然として解釈の対象となるかもしれない保険の購入は避けたいと考えているのです。

依然として流動的な法的背景

インタビューを行ったブローカーは、たとえ最良の環境下でも、異なる保険会社による複数の保険契約で一つのインシデントが補償されている場合に、保険契約の文言が完全に明確でないか、最低限の標準化がなされていないときは、そうした相違が原因で合意に対する議論が発生し、十分な保険金請求の管理が妨げられる可能性があると述べました。

インタビューを行ったブローカーによれば、一部の購入者は、最悪のシナリオとして、どの保険契約が適用されるか、または保険契約の文言が補償を意味しているかどうかについて、この相違が原因で保険金請求に関する紛争として提訴せざるを得なくなり、最終的に多額の損害について無保険になる事態を懸念しています。

ある保険会社は「サイバー保険を巡る紛争はまだ裁判で取り扱われたことがありません。したがって、判例法が明確でないため、保険契約の条件は今後の訴訟の中で検証されることになる」と述べ、「互いに重複や、時として矛盾があったりする州規制の不統一性が、エクスポージャーと補償のギャップを生み出す可能性がある」と指摘しました。

なかなか解消されないこうした不確実性のために、保険会社は、サイバー保険を引き受ける際に生じるエクスポージャーを定量化することが一層困難になり、また購入者にとっては、現在販売されている保険によって実際にどの程度のエクスポージャーが移転されているのかを評価することが一段と難しくなると思われます。

次に講じるべき措置

以上述べた阻害要因で、多くの保険会社は、データを集め、直接的な経験を積み重ねるために、サイバー保険市場で単に「実験」を行っているにすぎない、とブローカーは言います。他方、あるブローカーは、多くの購入者は、この新興的な市場の不確実な状況を踏まえ、自身が直面する脅威やリスク管理、利用可能な保険のオプションについて深く精通するまでは、サイバー保険の購入を先延ばししていると指摘します。

次のセクションでは、こうした懸念を緩和するために講じられる可能性のある措置を取り上げます。また、保険会社がこの有望な成長市場により深く関与し、サイバー保険の購入を一つの手段として、エクスポージャーの管理を改善できることをより多くの潜在的な顧客に納得させるために、何がなされ得るかについても検討します。

サイバー保険の成長の阻害要因を克服する戦略

データ不足のサイバー保険会社は代替的なアプローチにより時間を稼ぐことが可能

大半の保険会社にとって、サイバー保険の畑に種を蒔いて現在よりはるかに豊かな収穫を得るためには、厄介な仕事を抱え込む可能性があると思われます。先述した多くの成長の阻害要因を克服し、あるいは少なくともそれを埋め合わせる必要があるのです。サイバーリスクに関するデータの相対的な不足と、潜在的な集積損害を定量化しそれに対処することへの懸念、これら2つが最大の課題となります。

過去のデータが十分にない上、進化する脅威を絶えず評価する必要があることから、サイバー保険の価格設定は今後、相当長期間、いわば未完成の状態が続き、大半の保険会社にとって試行錯誤が事実上の運用戦略になると見込まれることをインタビュー対象者は認めています。多くの保険会社は今後数年、より急速な成長の妨げとなっている「悪循環」を打ち破るために必要最低量のデータや経験を取得するためだけに、より多くのサイバー保険を引き受けざるを得なくなる可能性があります。サイバー保険の引受会社は、短期的には拡大のペースが鈍化する可能性があるとしても、急速に発展し依然として不確実なこの市場においては一歩一歩着実に取り組む必要があると思われます。

一方、保険会社は、脅威が絶えず変化する状況下で限定的な予測モデルが陳腐化することを避けるため、その予測を修正したいと思うかもしれません。むしろ、保険引受や価格設定の評価にあたっては、申込者がサイバー関連の業務において安全性を保ち（防止）、警戒を怠らず（発見）、回復力に富む（損害管理と回復）ために講じることのできる具体的なリスク管理策に重点を置く「リスク情報に基づくモデル（risk-informed model）」の構築に集中的に取り組むことが考えられます。

こうしたアプローチを取った場合、多くの保険会社は恐らく、対外的な事業の成長を促進するために内部のサイバーセキュリティの専門知識を活用できるはずです。保険会社は多くの場合、サイバー攻撃から自社を防御するために、自身のリスク管理の必要性に応じてデータを収集・分析する脅威インテリジェンス・ユニットを設置しています。こうしたリソースを対外的に活用して、より賢明なサイバー保険の引き受けや価格設定の情報源とすることができるものと思われます。

インタビューを行った保険会社は、潜在的な顧客の損害管理プログラムの成熟度を評価する一助として、自社の直接的なサイバーセキュリティの経験を直接活用するには至っていませんでした。そして、インタビューを行ったブローカーは、これがほぼ業界全体の実状であると述べました。保険引受部門だけでなく、社内のリスク管理部門にも恩恵をもたらすようにするために、このような部門間の垣根は取り払うべきです。こうすることによって、労働災害補償や大規模災害のエクスポージャーにおける損害管理の経験の共有から恩恵が得られたのと同様、保険会社が、自社の多様な保険契約者グループの経験やアプローチから新たな事柄を学ぶのに役立つと思われます。

また保険会社は、保険引受をセグメント化することにより、データ不足の不利を幾らか補うことも考えられます。これは、保険対象の中の特定の業種またはニッチにターゲットを絞ることによって、保険会社に要求されるサイバーの専門知識の範囲を限定しようとするものです。別の方法として、保険会社は、全種類のリスクを対象とする総合的なサイバー保険を引き受けるのではなく、特定の種類のエクスポージャー（例えば、サービス妨害攻撃ではなくデータ漏洩のみ）または特定の技術分野（例えば、IoTまたはドメインネームサーバー）に特化することにより、評価対象となるエクスポージャーの管理を改善することが可能です。

特に大口顧客セグメントにおける破滅的な集積損害の可能性への懸念を緩和するため、ブローカーが示唆したように、保険会社は、複数の保険会社が引き受けるレイヤー方式に基づく補償プログラムを検討する可能性があります。

このオプションでは、個々の保険会社のエクスポージャーが限定されると同時に、全体として十分な補償が保険契約者に提供されます。

さらに、再保険の関与の拡大が、元受保険市場への集積負担を軽減し、より積極的な成長を促進することに役立ちます。インタビューを行ったブローカーは、再保険会社がサイバーエクスポージャーの補償への関与を深めようとしているように見えると示唆しており、同様の事が最近メディアで報道されました。ベスツ・インシュアランス・ニュース誌によれば、「伝統的な損害再保険市場が依然として低調であることから、再保険会社は新たな収益源を求めて次第にニッチ市場に目を向けるようになっており、中でも最大の注目を集める市場の1つがサイバー保険である」。しかしながら、その記事は、「課題は、保険会社が十分な知識を持たないと思われる保険種目で採算の取れる市場シェアを獲得することである」と付け加えています[15]。

保険会社は包括的なサイバーリスク管理プログラムを提供することが可能

より長期的には、サイバー保険商品の設計を根本から見直し、価格や条件、補償限度額以外の点で保険契約を差別化するために、関連するリスク管理サービスの提供を重視すべき時期にきていると思われます。そのためには、伝統的なリスク移転の提供を補完する、購入者のサイバーリスクのライフサイクル全体に及ぶ包括的で総合的なプログラムの作成が必要になるでしょう。

保険会社は、購入者のリスク管理の成熟度に基づいてサイバー保険の引き受けと価格設定を行うという、より厳密なプロセスを実施することを考慮すべきです。

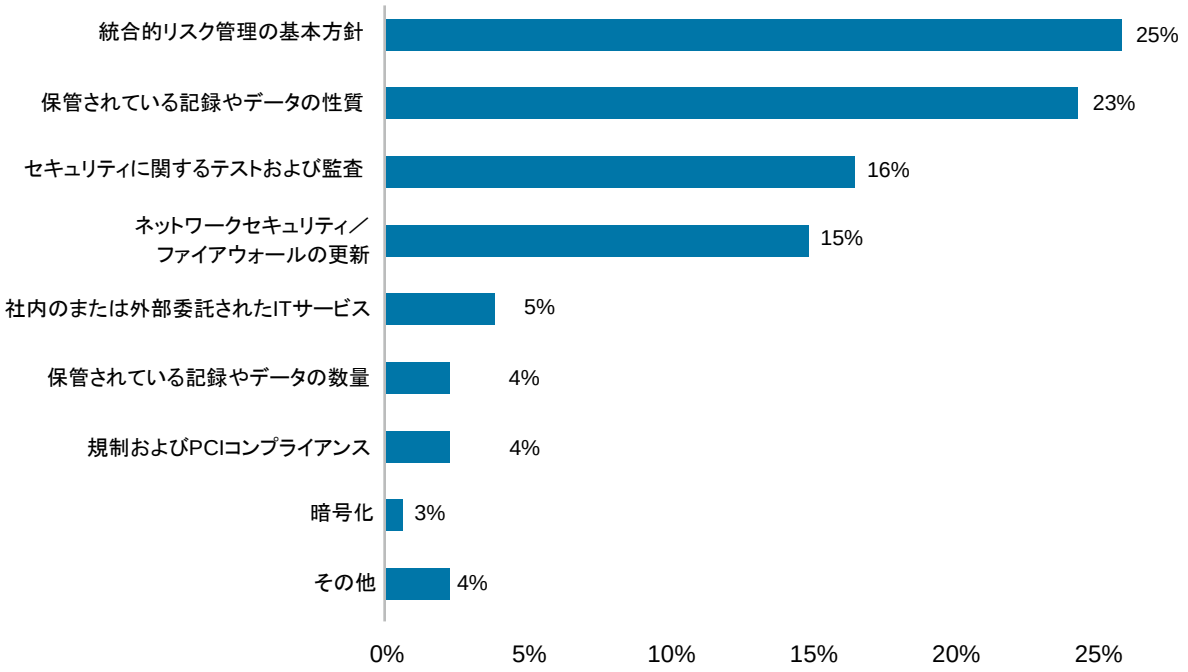
リスク防止サービスならびに損害発生後の対応および回復の支援は、アカウントを維持し、顧客関係を一層活性化しながら、顧客へサイバー保険を購入してもらうために提供されることが考えられます。顧客関係の活性化は、リアルタイムのモニタリングによって、リスク管理の成熟度のベンチマークを充足またはクリアする保険契約者に対するインセンティブとして保険料の引き下げおよび／または限度額の引き上げを提供することによって達成できるでしょう。

クライアントに包括的サービスを提供するサイバーリスクマネジャーおよびクライアントへの補償を充実させ主要なリスク移転手段となることは、購入者にとっても（何よりもまずインシデントの発生防止の支援により）、保険会社にとっても（損害の頻度と重大性の低減および顧客維持の可能性の増大により）恩恵をもたらす可能性があります。この場合も、保険会社内部のリスク管理チームが、努力して取得した知見や経験を、類似したエクスポージャーに直面するクライアントに伝えることにより、事業の発展に貢献することができます。サイバー保険会社は、このことをさらに一歩推し進め、自社の脅威インテリジェンスの能力を対外的に活用し、警告やリスク管理に関する提案を保険契約者に提供することによって、自身を差別化し、価値を付加することが可能になるでしょう。

サイバー保険業界は、より多くのデータを収集・分析するのに時間を要すると見られることから、またこの進化しつつあるリスクに固有の予測不能性や変動性を踏まえると、保険会社は、購入者のリスク管理の成熟度に基づいてサイバー保険の引き受けと価格設定を行うという、より厳密なプロセスを実施することを考慮すべきです。多くの保険会社は、サイバーリスクの評価にあたり、見込み顧客の統合的リスク管理の基本方針を重視するという点で、すでにそうした方向に進んでいるように思われます（図4参照）[16]。

データが不足する状況では、保険会社がサイバー保険の申込者をより厳密に審査することは理に適っていると言えるでしょう。追加条項形式ではなく独立したサイバー保険を求めようとする大規模な組織は恐らく、大口の企業向け損害保険の申込者の資格審査と同じ方法で取り扱う必要があると思われます（小規模な保険契約者の場合、それは恐らく実行困難であり、その補償ニーズやリスク管理の成熟度は、質問表ベースで適切に評価されるでしょう）。このプロセスでは実地検査に加え、当該組織の損害管理能力に対する継続的モニタリングがよく実施されています。ブローカーによれば、現在こうしたプロセスはサイバー保険の申込者について概ね行われておらず、そのため、多くの保険会社は、大口の見込み顧客の売上増加になりそうな、より広範囲の補償やより高い限度額の保険引受をためらっています。

図4. 保険会社はサイバーリスクの評価に際して何を重視するか



出所：ハノーバー・リサーチ／マーケット・インサイト・センター、「サイバー賠償責任保険の動向：調査」、ISO対象、2014年11月

全般的に見て、リスク管理ベースのアプローチを採用することにより、保険会社は、より多くのデータを収集し、長期予測モデルを補強するための一定の猶予期間を手に入れることができます。また、保険会社の競争上の地位を直ちに改善し、当面、これまで以上に積極的にサイバー保険を拡大することも可能になるでしょう。

保険会社、保険仲立人は常にリスク意識を高めることが必要

企業や財団、政府、政党、個人に影響を与えるサイバー関連の出来事がますます頻繁にメディアによって報道されているため、大半の大企業は、重大なサイバーエクスポージャーに直面しているかもしれないと基本的に自覚していると言ってよいでしょう。実際、パートナー・リーが昨年実施した保険会社とブローカーに対する調査によれば、サイバー保険の売上を牽引する要因として、「他社のサイバー関連の損害／経験のニュース」が群を抜いて第1位になっています（調査対象者のほぼ3分の2がリストアップ）（図5参照）[17]。このように社会の注目が集まると、多くの場合、公開企業の取締役会もサイバーリスクへの関心を高めます。金融機関におけるサイバーリスク管理に関するデロイトの過去のレポートでは、そうした取締役会の関心は、企業の経営陣にとって、注目を浴びているサイバーエクスポージャーを抑制し、保険カバーを有していることを明瞭に示すことへの圧力となると、CISOが回答しています[18]。

「不安要因」が拡大するにつれ、すなわち、ますます多くの見込み購入者がメディアの事件報道を読み、同業者から事件について聞き、競争相手が事件に巻き込まれるのを目撃し、あるいは自ら事件を経験するにつれ、リスク意識（そして、願わくは、それに応じたサイバー保険への需要）が徐々に高まり、加速するはずである、とインタビュー対象保険会社は答えました。

しかしながら保険会社は、既存および見込み保険契約者が、直面するリスクやその対処法に関する情報に常に通じているようにするために、単にメディアの報道を待っているべきではありません。業界はむしろ「もっと先回りして消費者の教育を促進することにより、より多くの企業がリスク管理プログラムを導入し、保険を購入するように導くべきです。このことを達成する方法の1つは、マーケティングや広告宣伝による直接的な働きかけの取り組みを強化することです。もっと個人に重点を置いた別の方法として、保険仲立人を使って保険について

説明し、販売促進を図ることがあります。

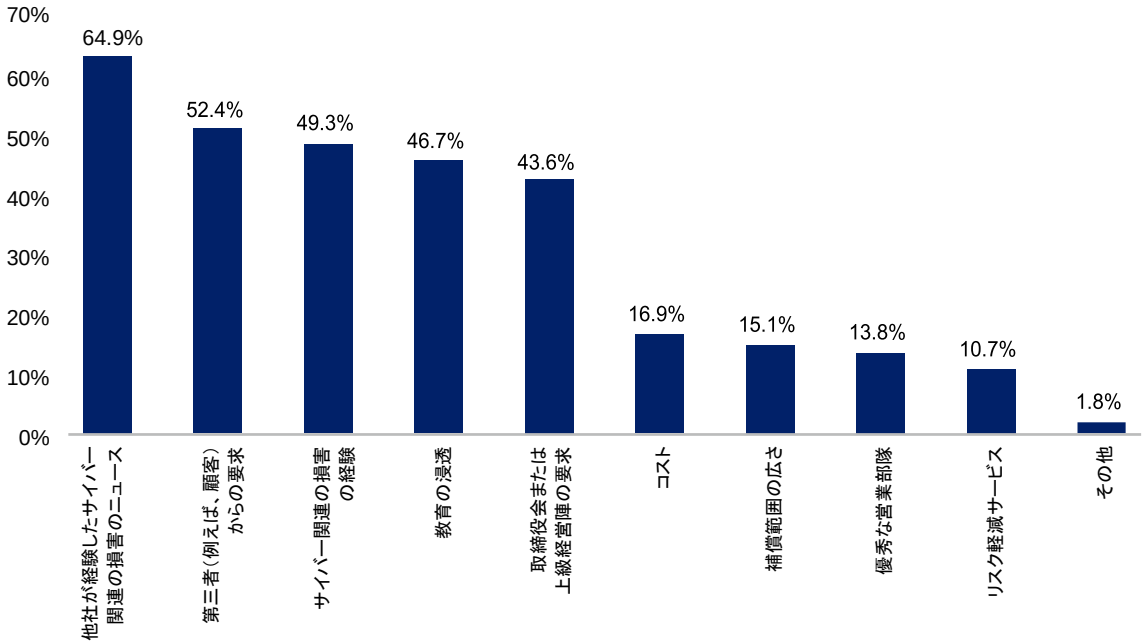
大手ブローカーのほとんどは、そうした情報を保険契約者に提供することにすでに熱心に取り組んでいるようです。実際、直近のCIABの調査では、回答者の88%が、「サイバーリスクに関するクライアントや見込み顧客への教育について、何らかの先を見越した戦略的アプローチ」を有していることが明らかにされました[19]。しかし、クライアントが「事前対策的な情報セキュリティプログラム」を導入していると答えた調査対象者はわずか37%にとどまることから、そうした取り組みの効果はかなり限定的と言えます。CIABによれば、このことは、「企業は、タイトな予算をやり繰りしてサイバー対策を採用しようと努力しているため、進歩が緩やかであることを示す」[20]ものです。

さらに、世界的および地域的規模で展開するブローカーは、こうした教育の任務を担うためのリソースや専門知識を備えているでしょうが、小規模な独立系代理店はその水準についていくのが難しいかもしれません。こうした代理店は、保険料収入や手数料収入が比較的低い中小企業の顧客と取引することが多いため、標準的な保険契約にサイバーの補償条項を追加する程度がせいぜいです。

サイバー保険会社は、リスク意識や損害管理に関する材料を提供することにより、小規模および大規模いずれの保険仲立人も支援することができます。そうした材料としては、情報誌やウェブサイト、ポッドキャストのほか、サイバーセキュリティの専門家（恐らく自己のリスク管理サービス部門や提携しているサイバーセキュリティ企業が含まれます）への紹介などがあります。

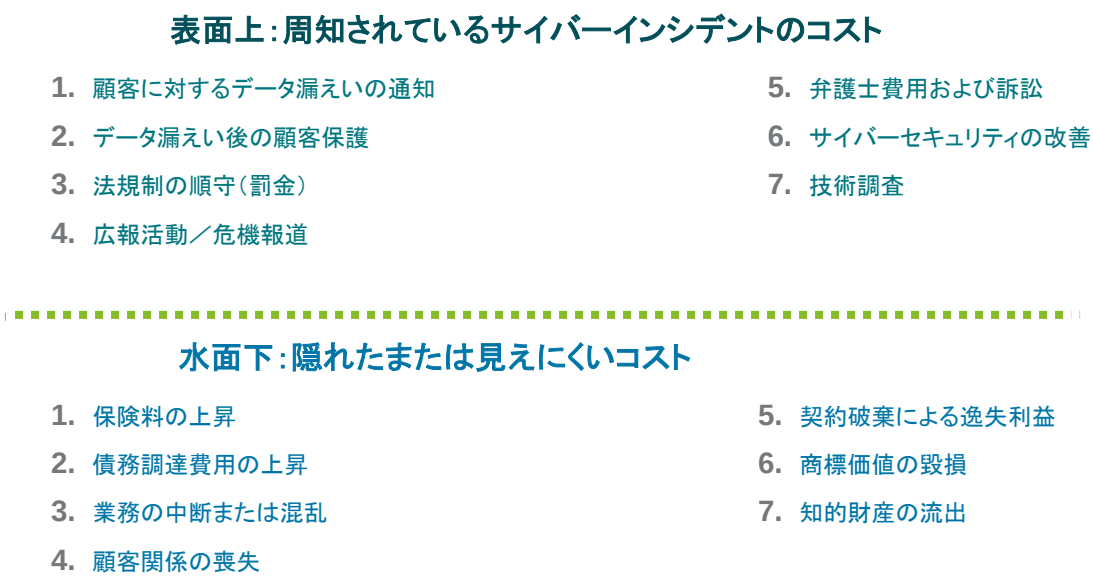
リスク管理サービスを提供することで追加的な手数料収入が生み出されるといったインセンティブをもたらすことで、代理店がより積極的にサイバー教育に関心を持つ可能性があります。二つめのインセンティブとしては、価格に左右される保険の販売業者から脱皮して、少なくとも大規模な企業顧客に対してより付加価値の高いリスクマネジャーへと進化することで、直販の動きを回避できる可能性があることです。三つめのインセンティブとして、サイバー保険を購入するクライアントに助言を怠り、現在の補償範囲に特定のサイバーリスクが含まれていないことをクライアントに説明しなかった場合に生じ得る、過失怠慢責任に係る高額の請求を回避できると思われることです。最後に、代理店やブローカーは、クライアントから収集する貴重なデータに基づいて、自身のサイバーエクスポージャーを自覚し、クライアントの代理人としてサイバー保険を購入することを含め、自発的にその経験や専門知識を顧客に伝えようとする可能性があるということでしょう。

図5. サイバー保険の売上を牽引する有力な要因



出所：パートナー・リー（アドバイゼンと共同）、「サイバー賠償責任保険の動向：調査」、2016年10月

図6. データ漏えいのコスト



出所：「サイバー攻撃の潜在的側面：企業への影響に関する掘り下げた分析」、デロイトサイバーリスクサービス

教育プロセスの重要な部分は、サイバーセキュリティインシデントによって発生する可能性のある表面上と水面下のコストについてクライアントに情報提供することです。一例としてデータ漏えいについて考えてみます（図6参照）。顧客に対する漏えいの通知など、責任を負うことが周知されているサイバーセキュリティインシデントのコストがある一方、契約破棄による逸失利益の価値や知的財産の流出など見えにくいコストもあります。こうしたことが、より多くの情報に基づいた販売提案や購入決定に向けた下準備となります。

保険契約の文言の標準化が消費者の信頼を高める可能性

ブローカー、保険会社とも、どの保険契約が何を補償しているかを巡る混乱を解消するには、契約書の文言の標準化を推し進めることが必要になるだろうと述べました。また、CIABが直近に行ったサイバーセキュリティに関する調査で「我々が何を販売しているかを知るために、そしてクライアントが何を購入しているかを理解するために標準化する必要があります」と回答されていることを指摘した上で、「多くのブローカーは、共通の用語集があればサイバー保険の文言の明確化に大いに役立つと感じています」[21]と述べました。

ISO（国際標準化機構）は、用語の標準化は、補償内容に関する紛争が「大量に」発生する可能性およびそれに伴う長期間かつ高コストの訴訟を回避するのに役立ち得ると指摘しました。その上で、次のような追加的な利点を挙げました。「保険契約書の表現の標準化は、保険会社が独自の商品やソリューションの品揃えを一新できるようになるための跳躍台の役目も果たします。そして、保険会社がより大きな自信、スピード、効率性をもってこの市場に参入するのを加速させます」[22]

標準化は必ずしも簡単には実現されないでしょう。業界内の競合企業間だけでなく、事業者団体や標準化団体などの中立的な第三者との協力と協調が必要になる可能性が高いと思われます。

長期的な視点では、保険会社の保険金請求管理費用を増加させる補償内容に関する議論や補償内容に関する消費者の信頼を損ない売り上げの伸びを妨げる可能性が、標準化することによって低減されると見込まれます。最終的には、サイバー補償の標準化を確立することにより、すでに商品を販売している保険会社が保険引受を拡大することを可能にすると同時に、新たなプレーヤーの市場参入が容易になると思われます。

サイバー保険会社の将来

歴史の長い損害保険市場の成熟度を考慮した場合、最も好調な時期でさえ、損害保険会社が本業での成長を達成するのは困難な可能性があります。その上、今日では多くの元受保険および再保険セクターが供給過剰の状態にあることから、持続可能な成長の達成は通常よりはるかに不確実になっていると思われます。短期的には、熾烈な競争に伴い、全般に価格が低迷し、保険料収入の拡大が限定され、最終利益の収益性が損なわれています。将来に目を向けると、迫り来るマイナス要因として自動運転車やカーシェアリングが、業界最大の保険種目である自動車保険が占める高い比率を押し下げる可能性があります。オートメーションを通じた労働力への打撃は、企業向け保険収入の大部分を占める労災保険に混乱をもたらしかねません。こうした困難な状況にあって、サイバー保険は、長期的な高度成長につながる数少ない機会の1つを提供しているように思われます。

業界の当初段階の実績は良好であり、2015年のサイバー保険の損害率（loss and loss adjustment expense ratio）は42%となりました。ただし、総じてこの数値は、中小企業を対象として引き受ける総合保険に組み込まれている補償（わずか34%）よりも独立したサイバー保険（51%）の方がはるかに高くなっています[23]。ただこの実績は、労災保険（77.4%）、企業向け自動車保険（75.9%）および企業向け包括補償保険（66.8%）などの多くの標準的な保険種目の5年平均[24]よりもかなり良好です。

しかしながら、何らかの形で状況が急速に変化する可能性があります。あるインタビュー対象者は、特に様々な業種に亘り広範な保険金請求を引き起こすシステミックなサイバーセキュリティ事件など、損害の重大度が突然上昇することによる潜在的影響について懸念を表明しました。あるブローカーはこう述べました。「テロリズムに関して、保険会社は実際のところそのエクスポージャーに見合った保険料を課していませんでしたが、同時多発テロが発生しました。保険会社は「サイバー保険でも同時多発テロ・レベルの事件が起きるのだろうか」と心配になるでしょう」。そのブローカーは、同時多発テロを受けて一夜のうちにテロ保険市場の取引がほとんど消えてしまった、と指摘しました。この状況は、保険会社が市場に呼び戻すために連邦政府による再保険の安全装置が導入され、より手ごろな価格で補償の提供するまで続きました（実際、多くのインタビュー対象者が、大規模なサイバー攻撃を受けた場合、一定の状況下でテロリズムとして分類される可能性があるのではないか、そしてサイバーテロに関する特定の補償条項が要求されるのではないかと考えており、その結果、サイバー保険に関する論争に別の種類の不確実性が持ち込まれています）。

他方、一部のインタビュー対象者は、あまりに多くのプレーヤーが新たな「ゴールドラッシュ」の一幕としてサイバー保険の引き受けに殺到し、その結果、あるブローカーの言う「未熟な引受能力（naive capacity）」が市場にあふれ、保険会社が顧客を引き付け、契約関係を維持するために料率を引き下げ、補償範囲を拡大する圧力を受けることへの懸念を表明しました。現状はゴルディロックス(Goldilocks)の童話さながらと言えます。サイバー保険市場が急速に過熱化へと向かい、大事件が起きて突然冷え込むのか、それとも適温の状態が続いて着実に成長する安定したセグメントとして発展するのでしょうか。その答えは、保険会社がどのように事業を始めて、この不安定なリスクをどう取り扱うのかによって決定されるでしょう。

サイバー保険は、長期的な高度成長につながる数少ない機会の一つとして見受けられます

またサイバーリスクの補償に関して言うと、伝統的な保険会社は、保険契約のみが購入者にとって唯一のリスク移転の選択肢ではないことを肝に銘じておくことも重要です。大口の購入者は、かつて保険カバーの供給が乏しくなり価格が高騰した時期に、代替的手段（キャプティブやリスク保有グループ、証券化など）を利用したように、同様の検討を行う公算が大きいと思われます。大規模災害保険市場がキャットボンドやその他の保険リンク証券によってどのような混乱に陥ったか、特に、再保険セクターがどのような影響を受けたかを考えてみてください。結果的に、伝統的な保険市場の価格と収益性が急激に低下したのです[25]。

いずれ近いうちに、大規模な組織が、伝統的な保険会社を利用せずに、自身のエクスポージャーを資本市場の投資家に移転する一助としてサイバーボンドが発行されるのでしょうか。同様の趣旨で、中小企業グループを補償するためにサイバーリスク保有グループが形成されるのでしょうか。あるいは、サイバーキャプティブを国内外で設立して自家保険を促進し、再保険市場への直接的なアクセスを購入者に提供するようになるのでしょうか。

これらはすべて極めて現実的で、確率が高いとさえ言える選択肢になりうる可能性があります。保険補償が不十分で不確実であり、過度に複雑、提供される価値に比べてあまりに高コストかそうではないか、またはその両方と多くの購入者によって引き続き認識された場合、特にそう言えます。

保険会社は、より先見的で伝統的な競争相手のみならず、代替的市場に取って代わられるのを避けるために、この有望だが不確実な市場への参入や拡大を容易にするための選択肢について積極的に検討すべきです。その選択肢には、外部からの支援が必要になるかどうかも含まれます。保険会社が戦略を策定する際に心に留めておくべき根本的問題として下記のものがあります。

- このリスクを自社の既存のリソースによって評価することができるか。それとも、少なくとも短期間は、引受および価格設定システムを補強するために外部データや第三者のモデルを購入すべきであるか。

- 保険契約の文言を標準化する一方、追加的な補償やサービスのオプションを通じて差別化する余地を依然残すために、業界内でどのように活動するのがよいか。

- サイバーリスクを管理する保険組織として自社の直接的経験から何を学ぶことができるか。自社の保険引受や価格設定、クライアント向けリスク管理サービスを補強するために、そうした経験をどのように活用するか。

最後の点は長期的にも短期的にも最重要と考えられます。ハッカーの目を引くターゲットとして、保険業界はサイバーリスクについて直接的な知識を有していることです。保険会社は、補償を求めるクライアントと同一のエクスポージャーやリスク管理の課題を有しており、その多くに取り組んでいます。リスク管理の成熟度は互いに異なるものの、保険会社は総じて、リスクにどれほど予測困難なことがあるか、その発見、防止および抑制がどれほど難しいか、さらには一つのインシデントがどれほど大きな損害を引き起こす可能性があるかを認識しています。したがって、多くの保険会社がサイバー関連事業を拡大することや、そもそも当該市場に参入することさえ慎重に考えてきたことは意外ではありません。

しかし、リスクビジネスに従事している保険業界は、サイバー保険への関心がますます高まると見込まれる状況を活用する最適の位置にあると言うこともできます。ただし、その前提として、保険業界は、購入者がサイバーエクスポージャーを補償する別の方法を発見する前に、解決策を見出す必要があります。

巻末注

1. Robert P. Hartwig and Steven N. Weisbart、「2015 year end results（2015年末時点における実績）」、米国保険情報協会、2016年5月16日、http://www.iii.org/article/2015-year-end-results

2. Robert P. Hartwig and Claire Wilkinson、「Cyber risk: Threat and opportunity（サイバーリスク：脅威と機会）」、米国保険情報協会、2015年10月21日、http://www.iii.org/white-paper/cyber-risks-threat-and-opportunities-100715.

3. Carrier Management（保険会社管理部門）、「Cyber risks poised to become a $20 billion dollar market（サイバーリスクは200億ドル規模の市場になる見込み）」、Wells Media Group（ウェルズ・メディア・グループ）、2015年9月、http://www.carriermanagement.com/news/2015/09/13/145178.htm.

4. 米国保険エージェント・ブローカー協会（CIAB）、「Cyber insurance market watch survey（サイバー保険市場観察調査）」、2016年10月26日、https://www.ciab.com/uploadedFiles/Resources/Cyber_Survey/102016CyberSurvey_Final.pdf

5. CIAB Cyber Market Watch（サイバー市場観察）、「Cyber insurance market watch survey（サイバー保険市場観察調査）」、米国保険エージェント・ブローカー協会、2015年9月

6. Celine French and Lisa Hamilton、「Consumer data under attack: The growing threat of cybercrime（攻撃を受ける消費者データ：サイバー犯罪の脅威の増大）」、Deloitte Consumer Review、The Centre for Economics and Business Research（経済ビジネスリサーチセンター）、デロイトLLP、2015年、https://www2.deloitte.com/tr/en/pages/risk/articles/consumer-data-under-attack.html

7. Robert P. Hartwig and Claire Wilkinson、「Cyber risk: Threat and opportunity（サイバーリスク：増大する脅威）」、米国保険情報協会、2014年6月、http://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf

8. Sam Friedman、「Taking cyber risk management to the next level: Lessons learned from the front lines at financial institutions（サイバーリスクマネジメントを次の段階に進める：金融機関の最前線から学んだ教訓）」、デロイトユニバーシティプレス、2016年6月22日、https://dupress.deloitte.com/dup-us-en/topics/cyber-risk/cyber-risk-management-financial-services-industry.html

9. Alexa Liautaud、「Autonomous car era brings risks of hijacking by hackers（自動運転車の時代がもたらすハッカーによるハイジャックのリスク）」、Automotive News（オートモーティブ・ニュース誌）、2014年9月4日

10. ParnerRe and Advisen（パートナー・リーおよびアドバイゼン）、「Cyber liability insurance market trends: Survey（サイバー賠償責任保険市場の動向：調査）」、2015年10月、http://www.partnerre.com/assets/uploads/docs/PartnerRe_Cyber_Liability_Trends_Survey_2015.pdf

11. CIAB、「Cyber insurance market watch survey, 2015（2015年度サイバー保険市場観察調査）」

12. Barbara Filkins、「Bridging the insurance/infosec gap: The SANS 2016 cyber insurance study（保険と情報セクターのギャップを埋める：2016年度SANSサイバー保険調査）」、SANS Institute and Advisen Ltd（SANSインスティテュートおよびアドバイゼン・リミテッド）、2016年6月、http://www.advisenltd.com/2016/06/21/bridging-the-insuranceinfosec-gap-the-sans-2016-cyber-insurance-survey/

13. 前掲資料.

14. CIAB、「Cyber insurance market watch survey, 2016（2016年度サイバー保険市場観察調査）」

15. David Pilla、「Reinsurers look to cyber as key niche expansion market（重要なニッチ拡大市場としてサイバーに目を向ける再保険会社）」、Best’ s Insurance News（ベスツ・インシュアランス・ニュース誌）、2016年11月23日、©AM Best（許可を得て使用）

16. ISO and Hanover Research/Market Insight Center（ISOおよびハノーバー・リサーチ／マーケット・インサイト・センター）、「Cyber insurance survey（サイバー保険調査）」、2014年11月、http://www.verisk.com/downloads/emerging-issues/cyber-survey.pdf

17. 「2016 Survey of Cyber Insurance Market Trends（2016年度サイバー保険市場動向調査）」 、パートナー・リーとアドバイゼンの共同調査、2016年10月

18. Friedman、「Taking cyber risk management to the next level（サイバーリスクマネジメントを次の段階に進める）」

19. CIAB、「Cyber insurance market watch survey, 2016（2016年度サイバー保険市場観察調査）」

20. 前掲資料.

21. 前掲資料.

22. Maroun Mourad and ISO、「How carriers can unlock the multi-billion dollar cyber marketplace（保険会社はどうすれば数十億ドル規模のサイバー保険市場の鍵を開けられるか）」、PropertyCasualty360.com、2016年8月11日

23. S&Pのグローバル・マーケット・インテリジェンス部門のデータ

24. 前掲資料.

25. Andrew Mais、「Securing tomorrow: The ripple effect of insurance-linked securities in the reinsurance market（将来の確保：再保険市場における保険リンク証券の波及効果）」、デロイト金融サービスセンター、デロイト ディベロップメントLLC、2016年1月、https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-securing-tomorrow-insurance.pdf

著者紹介

サム・フリードマン（SAM FRIEDMAN）

サム・フリードマンはデロイト・サービシズLPのシニア・マネジャーで、デロイト金融サービスセンターの保険リサーチ部門のリーダー。最新動向の分析および損害保険・生命保険会社が直面する主な課題の特定に従事。2010年10月にデロイトに入社する前は、29年間*ナショナル・アンダーライターP&C（National Underwriter P&C）*に所属、編集長を務めました。ツイッター（@SamOnInsurance）、LinkedInでフォローしてください。

アダム・トーマス（ADAM THOMAS）

アダム・トーマスはデロイトのサイバーリスクサービス部門のプリンシパル。情報システム分野に15年以上の経験を有しています。過去7年間、デロイトにとって最も重要かつ複雑な、グローバルな金融サービス分野の規制対象クライアントのために情報技術のリスク管理および情報セキュリティプログラムの設計と導入の支援に注力してきました。現在、銀行および保険分野におけるデロイトの最大クライアントのシニア・リーダーや取締役会に様々なサイバーセキュリティ関連事項に関するコンサルティングを提供しています。

現在の職務に就く前は、デロイトの技術リスク管理センター・オブ・エクセレンスに所属、デロイトの情報セキュリティおよび技術リスクに関するクライアントへのアドバイス提供能力の強化に責任を負っていました。

謝辞

当センターは、本レポートの調査および執筆に対する支援と貢献について、以下のデロイトの専門家の皆様に心より感謝の意を表します。

John Lucker, advisory principal, Deloitte & Touche LLP

Michelle Canaan, manager, Deloitte Center for Financial Services, Deloitte Services LP

Nikhil Gokhale, manager, Deloitte Center for Financial Services, Deloitte Support Services India Pvt. Ltd.

当センターは、本レポートの編集、デザイン、製作および配布について、以下のデロイトの専門家の皆様に心より感謝の意を表します。

Lisa DeGreif Lauterbach, financial services industry marketing leader, Deloitte Services LP

Michelle Chodosh, marketing manager, Deloitte Center for Financial Services, Deloitte Services LP

Courtney Scanlin, senior marketing manager, Deloitte Services LP

Junko Kaji, senior manager, US Eminence, Deloitte Services LP

Karen Edelman, manager, US Eminence, Deloitte Services LP

Kevin Weier, art director, Deloitte University Press, Deloitte Services LP

Chris Lyons, illustrator

CONTACTS

Industry leadership

Gary Shaw
Vice chairman
US Insurance Leader
Deloitte LLP
+1 973 602 6659
gashaw@deloitte.com

Deloitte Center for Financial Services

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

Authors

Sam Friedman
Insurance research leader
Deloitte Center for Financial Services
Deloitte Services LP
+1 212 436 5521
samfriedman@deloitte.com

Adam Thomas
Advisory principal
Deloitte & Touche LLP
+1 602 234 5172
adathomas@deloitte.com

日本における問い合わせ先

青木　計憙（Kazunori Aoki）
パートナー
金融保険セクター　リード
デロイト トーマツ コンサルティング合同会社
03 5220 8600
kazaoki@tohmatsu.co.jp

宮崎　茂（Shigeru Miyazaki）
パートナー
金融保険セクター　監査担当
有限責任監査法人トーマツ
03 6213 1160
shigeru.miyazaki@tohmatsu.co.jp

後藤　茂之（Shigeyuki Goto）
ディレクター
金融保険セクター　規制担当
有限責任監査法人トーマツ
03 6213 1162
shigeyuki.goto@tohmatsu.co.jp

編集担当

工藤　美保子（Mihoko Kudo）
マネジャー
有限責任監査法人トーマツ
03 6213 1160
mihoko.kudo@tohmatsu.co.jp

Deloitte.
University Press

Follow @DU_Press
Sign up for Deloitte University Press updates at www.dupress.deloitte.com.

About Deloitte University Press
Deloitte University Press publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.
Deloitte University Press is an imprint of Deloitte Development LLC.

About this publication
This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.
None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Member of Deloitte Touche Tohmatsu Limited

（日本語版について）

デロイト トーマツ グループは日本におけるデロイト トウシュ トーマツ リミテッド（英国の法令に基づく保証有限責任会社）のメンバーファームおよびそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人および DT 弁護士法人を含む）の総称です。デロイト トーマツ グループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査、税務、法務、コンサルティング、ファイナンシャルアドバイザリー等を提供しています。また、国内約 40 都市に約 9,400 名の専門家（公認会計士、税理士、弁護士、コンサルタントなど）を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループ Web サイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）は、監査、コンサルティング、ファイナンシャルアドバイザリーサービス、リスクアドバイザリー、税務およびこれらに関連するサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界 150 を超える国・地域のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスを Fortune Global 500® の 8 割の企業に提供しています。“Making an impact that matters”を自らの使命とするデロイトの約 245,000 名の専門家については、Facebook、LinkedIn、Twitter もご覧ください。

Deloitte（デロイト）とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッド（“DTTL”）ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数を指します。DTTL および各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTTL（または“Deloitte Global”）はクライアントへのサービス提供を行いません。Deloitte のメンバーファームによるグローバルネットワークの詳細は www.deloitte.com/jp/about をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。