LLOYD'S

エマージングリスクレポート2017

テクノロジーシリーズ

コストの算定
（サイバー・エクスポージャーの解明）

CYENCE

免責事項 ― ロイズ・オブ・ロンドン

本レポートは一般的な情報提供のみを目的としてロイズとサイエンス社が共同で制作したものです。データ収集と報告書の作成は慎重に行っていますが、ロイズはこれらの正確性、または完全性についていかなる表明、または保証も行うものでなく、また黙示的表明または保証についても法律上最大限に許容される範囲内で明示的に除外します。

ロイズは本レポートに記載されたステートメント、事実、数字、意見または信念の表明に起因して、または依拠して行動した、もしくは行動しなかったことにより特定の個人・法人に発生した損失、または損害については、その性質を問わず、一切の責任、ならびに賠償責任を負いません。本レポートはいかなる種類の助言の性質を持ちません。

ロイズについて

ロイズは世界的な元受・再保険専門市場です。私達は世界的に信頼されている高い知名度の下で保険市場の管理・監督者として活動しています。ロイズは多様なグローバル資本と優良な財務格付けの裏付けにより、ビジネスと地域社会の回復力を構築し、世界経済の成長を支援するグローバルネットワークを有しています。

数世紀にわたる専門知識の蓄積を備えたロイズは、保険業界とその将来の基盤を担います。ロイズは200を超す国・地域をカバーする専門的なアンダーライターとブローカーによって主導されており、人類の進歩を保険で支えるために必要な本質的、かつ複雑で決定的に重要な保険を開発しています。

サイエンス社について

サイエンス社は、保険業界が損失コストと発生確率の両面におけるサイバーリスクの影響を把握できるよう支援しています。サイエンス社では経済/リスクモデル、サイバーセキュリティ、およびビッグデータ分析を組み合わせて、経済的サイバーリスクモデリングのプラットフォームを創設するユニークなアプローチを採用しています。サイエンス社のプラットフォームと解析は保険業界を代表するトップ企業において、サイバーリスクの理解と管理、および革新的な保険商品の導入に向けて活用されています

Key Contacts

Trevor Maynard
Head of Innovation
trevor.maynard@lloyds.com

For general enquiries about this report and Lloyd's work on innovation, please contact
innovation@lloyds.com

About the authors

Trevor Maynard PhD, MSc, FIA has degrees in pure maths and statistics and is a Fellow of the Institute of Actuaries. He is Head of Innovation at Lloyd's including responsibility for horizon scanning and emerging risks. Subjects covered in recent years include: the economic and social implications of a food system shock; the effects of cyber-attacks on the US energy grid and an exploration of aggregation modelling methods for liability risks.

He is co-chairman of OASIS, an open modelling platform for catastrophe models and sits on the Board of the Lighthill Risk Network.

George Ng, a founder and Chief Technology Officer, leads major research projects and initiatives at Cyence. Previously, he was the Chief Data Scientist at YarcData. George has also worked as a Research Scientist at DARPA and US-CERT and as faculty at American University. He received his PhD from UC Irvine and B.A. from UC Berkeley, both in Economics.

Acknowledgements

The following people were interviewed, took part in workshops or roundtables, or commented on earlier drafts of the report; we would like to thank them all for their contributions:

Insurance industry workshops and consultation

- Tom Allen, Channel 2015
- Scott Bailey, Markel
- David Baxter, Barbican
- Marcus Breese, Hiscox
- Stephanie Bristow, Hiscox
- Robert Brown, Neon
- Wesley Butcher, Atrium
- Danny Clack, Pembroke
- Jason Clark, Faraday
- Nils Diekmann, MunichRe
- Daniel Fletcher, QBE
- Matt Harrison, Hiscox
- Matthew Hogg, Liberty
- Adam Holdgate, AM Trust
- Jerry Hyne, Aegis
- Laila Khudairi, Tokio Marine Kiln
- Nick Leighton, Aegis
- Alessandro Lezzi, Beazley
- Ben Maidment, Brit
- Kelly Malynn, Beazley
- Phil Mayes, Talbot
- Alastair Nappin, MunichRe
- Raheila Nazir, Aspen
- Matt Northedge, AM Trust
- Andrew Pearson, Barbican
- Scott Sayce, CNA Hardy
- David Singh, MS Amlin
- Dan Trueman, Novae
- Stephen Wares, MS Amlin

Cyence project team and area of expertise

- Dr George Ng, CTO and co-founder
- Dr Yoshifumi Yamamoto, Principal Modeler
- Matthew Honea, Cyber Manager
- Misti Lusher, Director of Marketing
- Scott Hammesfahr, Product Marketing Manager
- Phil Rosace, Senior Solutions Manager

Cyence external partners

- Sean Kanuck, advisory board member for Cyence and former first United States National Intelligence Officer for Cyber Issues from 2011-2016
- Marc Goodman, New York Times best-selling author of Future Crimes and global strategist and advisory board member for Cyence

Lloyd's project team

- Dr Trevor Maynard, Head of Innovation
- Dr Keith Smith, Innovation team
- Lucy Stanbrough, Innovation team
- Flemmich Webb, Speech and Studies

Further thanks go to the following for their expertise, feedback and assistance with the study:

LMA

- Mel Goddard, Market Liaison Director, Lloyds Market Association
- Tony Ellwood, Senior Technical Executive – Underwriting, Lloyds Market Association

Lloyd's

- Caroline Dunn, Class of Business
- Linda Miller, Marketing and Communication
- Tope Omisore, International Regulatory Affairs
- Paul Sanders, International Regulatory Affairs
- Christian Stanley, Class of Business

エグゼクティブサマリー

本レポートはサイバー保険を引き受ける保険会社に対して、サイバーリスクの集積を定量化するための現実的、かつ説得力のあるシナリオを提供することを目的としています。サイバーリスクに潜む賠償責任とリスクエクスポージャーに対する理解は、他の保険種目と比較して遅れています。

サイバーリスクのエクスポージャーを理解することにより、保険会社は保有するポートフォリオのエクスポージャー管理を強化し、適切な限度額を設定することができ、急速な成長を続けるサイバー保険分野において自信を持ってビジネスを拡大することが可能となります。

本レポートではサイバー攻撃の2つのシナリオを解説しており、本レポートを読んでいただきたいのはこの種のサイバー攻撃に晒されている企業のリスクマネジャーです。即ちハッキングによってクラウドサービスがダウンする場合、およびサイバー攻撃によって自社内、顧客、サプライヤーや取引先において、特定のオペレーティングシステムがダウンする場合です。

掲載されたシナリオはそれぞれ、リスク軽減の可能性やサイバー攻撃への対応など、様々な変数を包含しています。これは、企業が自社事業に対する影響を検討することが可能であることを意味します。

方法論

本レポートはロイズとサイエンス社の共同制作によるもので、双方から投入されたサイバーセキュリティ、経済リスクモデリング、およびサイバー保険の人材による多角的な専門家のチームが制作を担当しました。

サイエンス社は本レポートにおけるシナリオ作成、ならびに推定損失額の算出に際して**以下の**7段階の組織的な調査プロセスを実施しました。

1. 業界全体で広く採用されている技術のレビュー
2. 他の非技術的要素のレビュー
3. リスクエクスポージャー算定のためのデータ収集と処理
4. リスクエクスポージャーの集積経路の解析
5. シナリオ、頻度、損失規模モデルの選択
6. 保険・サイバーセキュリティ専門家との討議とレビュー
7. 損失の算定と最終レビュー

ロイズでは、ロイズ市場協会（Lloyd’s Market Association）と協力の上、ロイズ市場でサイバー保険担当アンダーライターが参加する一連の共同ワークショップを通じて、保険業界に対する影響と考察すべきポイントを検討し、フィードバックを本レポートに盛り込むと同時に、それらを特定しました。

サイバー攻撃 – 増大する脅威

サイバーリスクは世界的に増大しつつある脅威です。デジタル化がビジネスモデルを革命的に変化させ、私たちの日常生活を変貌させる一方で、世界経済のサイバー攻撃に対する脆弱性は高まっています。

その結果、サイバー犯罪が経済・保険事業に及ぼす影響は増大しています。2016年において、サイバー攻撃によって世界中の企業に発生するコストは4,500億ドルに上るものと推定されています（Graham著、2017年）。この種の事象は悪意のある内部関係者やハッカーによる個々のサイバー侵犯から、小売り業におけるPOS（販売時点情報管理）デバイス侵犯のような大規模な損害、さらにビットロッカー（BitLocker）やワナクライ（WannaCry）などのランサムウェア攻撃、ミライ（Mirai）のようなDDoS攻撃に至るまで多岐にわたっており、保険会社は保険契約者がこれらの事象に対処できるよう支援を提供しています。

世界経済において事業、サプライチェーン、ビジネス取引、従業員・顧客サービスのデジタル化が進む中で、サイバー攻撃の脅威は増大しており、この傾向は今後も継続することが予想されます。

保険会社の課題

サイバー攻撃の脅威が増大するにつれて、サイバー保険の需要も増加しています。現時点でロイズの保険種目別業績管理部門では、サイバー保険のグローバル市場規模を30億～35億ドルと推定しており（Stanley著、2017年）、一部のアナリストは2020年までに同市場規模は75億ドル（PwC著、2015年）に達するものと予測しています。フィッチ・レーティングスとA.M. Bestの報告によると、2016年の損害保険会社によるサイバー保険の元受収入保険料は13億5000万ドルに達し、2015年と比べて35%も増加しています。

このようにサイバー保険の市場規模が拡大している一方で、保険会社のサイバー賠償責任とリスク集積に関する理解は、サイバー攻撃に対する経験と知識の蓄積をなす、発展途上にあります。

被保険者のインターネット利用形態も変化しており、サイバーリスクの集積は他の危険には見られない程急速なペースで変化しています。

伝統的な保険リスクモデリングは、国や業界のデータなど権威のある情報源に依拠していますが、サイバーリスクについてはこれらに匹敵する情報源はなく、リスク集積モデリングのためのデータについては、大規模なデータ量の収集が必要となります。この関係でデータの収集と定期的更新は、進化過程にあるリスクについて理解を深める上で重要な要素となっています。

本レポートを活用してどのようにサイバーリスクの集積に対する理解を深めるか

本レポートは保険会社およびリスクマネジャーが、サイバーリスクに潜む賠償責任およびリスク集積をより深く理解できるようお手伝いすることを狙いとしています。ここではデジタルリスク関連の脆弱性に寄与する6つのトレンドに基づく視点からリスク集積を分析しています。これらのトレンドを理解することは、サイバーリスクの集積を理解するうえで不可欠です。

これらの傾向は**以下**のとおりです。

1. 貢献者の数：ソフトウェア開発者数は過去30年間で大幅に増加しました。貢献者が増える毎に人為的ミスに起因するシステムの脆弱性は増大する可能性があります。
2. ソフトウェアの大きさ：コードの修正を行う人の数が増えていることに加えて、存在するコードの数も増えています。コードが増えればエラーの可能性、ひいては脆弱性も増加します。
3. オープンソースソフトウェア：オープンソース拡大の動きは、多くの革新的なイニシアチブをもたらしました。一方で、オンライン上にアップロードされている多数のオープンソースライブラリが、機能・セキュリティの面からレビューされているという一般的な想定は、必ずしも実態に沿ったものではありません。プライマリコード内のエラーはその後知らず知らずのうちに無意識に反復コピーされる可能性があります。
4. 古いソフトウェア：ソフトウェアが市場に流通する期間が長くなればなるほど、悪意のある人物が脆弱性を発見し、つけ込む時間的な余裕が発生します。より安全な代替があるにも拘わらず、陳腐化したソフトウェアを使用し続けている個人や企業は少なくありません。
5. 複層ソフトウェア：最新のソフトウェアは多くの場合、既存ソフトウェアコードを基にしてその上に構築されています。このためソフトウェアの検証と修正が非常に困難になり、膨大なリソース投入が必要となります。
6. 「生成」ソフトウェア：コードは自動化されたプロセスを通じて生成することができますが、これは悪意のある目的のために変更することが可能です。

本レポートではさらに、2つの異なるサイバー事象に起因して発生しうる様々な損害を、シナリオを用いて定量化しています。

シナリオ1：クラウドサービスプロバイダに対するハッキング

高度な技術を持った「ハクティビスト（hacktivists）」の集団が、企業や現代の経済が及ぼす環境への影響に注目を集める目的で、クラウドサービスプロバイダとその顧客を混乱させるための攻撃を実行する。ハクティビスト集団はクラウドインフラストラクチャを制御する「ハイパーバイザ（hypervisor）」に悪意のある変更を加える。これによって多数のクラウドベースのカスタマーサーバーがダウンし、広範なサービスおよびビジネスの中断がもたらされる。

シナリオ2：大規模脆弱性攻撃

あるサイバーアナリストが、誤ってバグを列車に置き忘れた。このバグには、世界市場の45%で稼動しているオペレーティングシステムの全バージョンに影響を及ぼす脆弱性レポートのハードコピーが入っていた。このレポートはダークウェブ（dark web）上で取引され、その結果、これを入手した不特定多数の犯罪者がシステム・エクスプロイト（exploit）[a]を開発し、金銭的利益のために脆弱性の高い企業に対する攻撃を開始する。

[a] エクスプロイトとは何らかの悪質な意図を実行するために、特定のコンピュータシステムまたはプログラムの弱点につけ込むことを目的としたソフトウェア、データまたはコマンドの使用を指します。

主な調査結果

本レポートには5つの重要な調査結果を記載します。

- サイバー事象の直接的な経済的影響は広範囲の潜在的な経済損失をもたらします。本レポートで取り上げたクラ　ウドサービス障害のシナリオでは、損失は大規模事象の場合で46億ドル、最大規模事象の場合は530億ドルに上ります。一方で、大規模なソフトウェア脆弱性のシナリオにおける損失は、大規模事象の場合で97億、最大規模事象の場合で287億ドルに及びます[b]。

– サイバー損失の集積における不透明性のため、経済的損失はシナリオ上の平均値から大きく上下に乖離する可能性があります。たとえばクラウドサービス障害のシナリオにおける平均損失は、最大規模事象で530億ドルですが、関係する組織の種類や障害の期間といった要因によって、最大で1,210億ドル、最小で150億ドルと推定されます[c]。

– サイバー攻撃は数十億ドルに上る保険金支払いを引き起こす可能性があります。例えば、クラウドサービスのシナリオでは、保険金の支払対象となる損失は、大規模損失の場合で6億2,000万ドル、最大規模損失の場合で81億ドルとなります。大規模ソフトウェア脆弱性シナリオでは、保険金の支払対象となる損失は7億6,200万ドル（大規模損失の場合）から21億ドル（最大規模損失の場合）の範囲となります。

– クラウドサービス障害のシナリオでは、40億ドル（大規模損失の場合）から450億ドル（最大規模損失の場合）の無保険である付保ギャップがあり、保険でカバーされているのはそれぞれ損失の13%から17%となります。一方、大規模脆弱性シナリオにおける付保ギャップは90億ドル（大規模損失の場合）から260億ドル（最大規模損失の場合）の範囲であり、経済的損失のわずか7%しかカバーされてない実態を示しています。

– 本レポートの予測サイバーシナリオによる保険金支払いの推定額と対比して現在のマーケットの概算保険料を評価した場合、単一のサイバー事象による大規模および最大規模の損失事象によって、業界損害率がそれぞれ19%、250%押し上げられうることが明らかとなっており、サイバーリスク保険の持つ巨大損害のポテンシャルを如実に示しています。

[b]これらの数値は大規模・最大規模損失事象においてシミュレーションされた損失規模の平均値を示しており、該当事象に関連するすべての予測される直接費用を考慮に入れていますが、物的損害、身体傷害、そして顧客の喪失や風評被害などの間接損失の影響は考慮していません。

[c]これらの値は95%の信頼区間（既知・未知のパラメータをカバーする有効な推定値の範囲）を前提としています。

結論

サイバー攻撃の脅威の増加に伴ってサイバー保険の需要も拡大しています。

このような市場の成長と裏腹に、保険会社におけるサイバー賠償責任とリスク集積に関する理解は、サイバー攻撃の経験の増大に伴って進化している最中です。それゆえテクニカル保険料の算定と資本モデルを含めて、変化を続けるサイバーリスクの知識ベースに見合った、リスクの把握が重要です。

他の幾つかの保険種目では、賠償責任とリスク集積に関する理解がより進んでいます。たとえば、巨大な自然災害の結果複数の保険契約者から複数の保険金請求が行われ、保険会社の保険金支払いコストを劇的に増加させることが広く認められています。通常巨大自然災害を担保する保険の引受に際してはこの点が考慮されており、リスク集積の影響を軽減するために一般に再保険が用いられます。

本レポートの調査結果は、サイバー事象による経済的損失が、巨大ハリケーンに匹敵する規模に達しうることを示唆しています。保険会社はその旨を念頭に置いた上で、サイバーに関連した大規模被害が集積することを明確に勘案し、サイバー保険を検討するとよいと考えられます。サイバーリスクは絶えず変化していることから、そのためにはデータの収集と品質が重要となります。

成長途上にあるサイバー保険市場に資本投下する保険業界にとって、各保険会社がサイバー保険に内在する潜在的なテールリスクについて深く理解することが有益です。

企業のリスクマネジャーはサイバー攻撃のシナリオを用いて、サイバー攻撃が自社のコアビジネスプロセスに及ぼす影響を把握し、これらのリスクの軽減に向けてどのような施策を取りうるかを計画することができます。

参考文献

Graham, L. 2017. Cybercrime costs the global economy $450 billion [online]. CNBC Cyber Security. Available at: http://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html

PwC. 2015. Insurance 2020 & beyond: Reaping the dividends of cyber resilience [online]. Available at: http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf

Stanley, C. 2017. Cyber market estimate (interview 26 June, Christian Stanley, Casualty Executive, Class of Business Underwriting Performance, Lloyd's).


LLOYD'S
CYENCE