サイレント・サイバーリスクを巡る動向

－米国・イギリスを中心に－

主任研究員　金　奈穂

目　　次

要旨

年々増大するサイバーリスクの脅威は、同リスクを補償する保険の需要を拡大させている。損害保険会社においては、サイバー保険の市場拡大が見込まれる一方で、サイバー被害に起因する損害が、サイバー保険以外の従来から存在する財物保険や新種保険においても補償対象になるのではないかという「サイレント・サイバーリスク問題」も深刻化している。今後 IoT などのテクノロジーが発展・普及するにつれ、保険会社が損害保険に潜在するサイレント・サイバーリスクを特定し、適切な対応を講ずることの重要性はますます高まるだろう。

本稿では、米国およびイギリスで確認されたサイレント・サイバーリスクや、保険会社等によるサイレント・サイバーリスクへの対応事例などを紹介している。海外の事例をわが国の状況にそのまま適用できるわけではないが、保険業界の着眼点や損害保険の補償範囲を明確化する取組などは、サイレント・サイバーリスクへの対応を進める際のひとつの参考になると思われる。

１．はじめに

サイバー被害の増加・多様化や個人情報保護法規制の強化に伴い、サイバー保険の需要が世界的に拡大している。しかし、サイバーリスクは新興リスク[1]の１つであり、保険会社が引き受けるにあたっては多くの課題が存在する。その１つがサイレント・サイバーリスク問題である。

サイレント・サイバーリスクとは、従来から存在する損害保険（以下「従来型保険」）の約款において明示的に補償されておらず、免責の対象ともされていないサイバーリスクを指す。サイバー被害は財物保険や新種保険で伝統的に補償されてきた物的損害や賠償責任をもたらす可能性があるため、こうした損害は、サイバーリスクを補償するために設計されたサイバー保険だけでなく、サイバーリスクを考慮していない従来型保険においても補償しているとみなされる可能性がある。

従来型保険に潜在するサイレント・サイバーリスクは、実際に損害が発生した後の補償の可否を巡る裁判で表面化する場合が多く、そのエクスポージャーをあらかじめ見積もることは難しい。しかし、サイバー被害の増加・多様化に伴って、サイレント・サイバーリスクのエクスポージャーは今後増大する可能性がある。

サイバー保険の引受の中心地であるイギリスでは、保険監督当局の PRA（健全性監督機構）がサイバー保険の引受リスクの１つとしてサイレント・サイバーリスク問題に取り組んでおり、保険会社に対応を講ずるよう求めている。サイバー保険市場が拡大傾向にあるわが国においても、金融庁がサイレント・サイバーを含むサイバーリスクの引受の考え方等について保険会社と対話を行っていく姿勢を示している。

こうした動向を踏まえ、本稿では、わが国の保険会社がサイレント・サイバーリスクへの対応を進めるうえで参考となるように、米国・イギリスで確認されたサイレント・サイバーリスクの例や保険業界の対応を中心に紹介する。

なお、国・地域や保険会社の別によって法規制、判例の取扱、保険約款の内容などが異なるため、本稿で紹介する事例は、米国・イギリスで一般的に使用されているモデル約款・条項をベースに、基本的な考え方を説明するに留めている。また、本稿における意見・考察は筆者の個人的見解であって、所属する組織を代表するものではないことをお断りしておく。

２．サイバーリスクを補償する保険の概況

サイバーリスクを補償する保険は３つの形態に大別される（図表１参照）。

①サイバーリスク専用の「専用型サイバー保険」および②従来型保険にサイバーリスク補償を付帯した「付帯型サイバー保険」は、一般的に「サイバー保険」と呼ばれてい

[1] 新興リスク（emerging risks）とは、新技術などによって新たに発生するリスクや、以前から存在していたが状況が変化したことで増大したり、新たに認識されたりするリスクをいう。

るものであり、保険約款にサイバーリスクを補償する文言が明示的に含まれる。③サイレント・サイバーリスクが潜在する可能性のある従来型保険（以下「サイレント・サイバーリスクが潜在する従来型保険」）は、約款上、サイバーリスクを補償するとも免責するとも記載されていないため、サイバーリスクが補償されている可能性がある。

本項では、これらサイバーリスクを補償する保険の沿革および市場規模を説明する。また、サイバーリスクを補償する保険の課題の１つとして、サイレント・サイバーリスク問題を説明する[2]。

図表１　サイバーリスクを補償する保険の形態

①専用型サイバー保険	・サイバーリスクを補償するために設計された保険 ・保険約款上サイバーリスクを明示的に補償する
②付帯型サイバー保険	・従来から存在する損害保険にサイバーリスク補償を付帯した保険 ・保険約款上サイバーリスクを明示的に補償する
③サイレント・サイバーリスクが潜在する可能性のある従来型保険	・従来から存在する損害保険 ・保険約款上サイバーリスクを補償するとも免責するともしていない

（出典：各種資料をもとに作成）

（1）沿革

サイバーリスクは新興リスクであり、それを補償するサイバー保険は 1990 年代後半に米国で販売が開始されて以降、20 年余りで米国を中心に急速に発展してきた[3]。

サイバー保険の補償範囲は当初、第三者に対する賠償責任に限定されていたが、個人情報保護に関する法規制強化（特に、個人情報漏えい時の本人への通知義務導入[4]）やサイバー被害の増加・多様化を背景に、サイバーリスクは保険会社が想定していなかった範囲にまで広がった。図表 2 は、主なサイバー被害とそれに起因する損害（以下「サイバー関連の損害」）の例である。また図表 3 は、サイバー関連の損害を分類別に示している。サイバー被害は、多様な種類の賠償責任や被保険者が被る自社損害をもたらす可能性がある。

保険業界は当初、これらサイバー関連の損害が従来型保険の補償範囲外であるとの見解を示していた。しかし補償の可否を巡る裁判でこうした見解が否定され、従来型保険で補償されるサイレント・サイバーリスクが表面化した事例があった。このため米国やイギリスでは、保険契約者のニーズに応え、補償範囲を明確化し円滑な支払を可能とするために、サイバー保険を発展させる一方で、従来型保険の約款にサイバー関連の免

[2] 本稿ではサイレント・サイバーリスクに重点を置いて説明している。その他の課題に関しては、牛窪賢一「米国におけるサイバー保険の動向」損保総研レポート第 120 号（損害保険事業総合研究所、2017.7）を参照願う。

[3] John Loveland, “Cyber insurance – I don’t think it means what you think it means”（RSA Conference 2017, 2017.2）、OECD, “Enhancing the role of insurance in cyber risk management”（2017.12）など。

[4] 個人情報漏えい時の公表義務と本人への通知義務を明文化した全米初の法律として、2002 年にカリフォルニア州で「データセキュリティ侵害通知法」が策定された。その後、同様の法律が他の州でも策定・施行されている。

責を追加してきた（後記 3 参照）。

図表 4 は、主要な保険会社等が販売している専用型サイバー保険において、各種サイバー関連の損害が補償対象になる割合を示している。サイバー保険は主要な顧客である企業のニーズに合わせてカスタマイズされることが多く、商品によって補償内容が異なるものの、多くの専用型サイバー保険が「サイバー被害対応費用」・「訴訟に対する防御費用」・「プライバシー侵害に関する賠償」・「事業中断」などを補償しており、これらは付帯型サイバー保険においても提供されるケースが多い[5]。なお「罰科金」については、サイバー保険の補償範囲外とするケースや、法令で認められる場合に限り補償が提供されるケースがある[6]。また補償が提供される場合でも、個人情報漏えい等に対して高額な罰金を課す GDPR[7]の施行により、サイバー保険の補償限度額をはるかに上回る損害が発生する可能性が指摘されている。

また、サイバー被害の脅威は企業だけでなく個人においても高まっており[8]、サイバーゆすりやネットいじめ、スマートホーム・デバイスを通じた個人情報漏えい等を補償する個人顧客向けサイバー保険の提供も開始されている[9]。

図表 2　サイバー被害とサイバー関連の損害の例

サイバー被害		サイバー関連の損害の例
種類	例	
第三者データの機密性侵害	個人情報の漏えい（不正開示）	サイバー被害対応費用 (注)、評判・ブランド等の失墜、罰科金、プライバシー侵害に対する賠償、訴訟に対する防御費用、会社役員賠償責任
自身のデータの機密性侵害	企業機密の盗難	知的財産の窃盗、会社役員賠償責任
操作技術の障害	制御システムの改ざん	事業中断、罰科金、資産の物的損害、身体障害・死亡、会社役員賠償責任
ネットワーク通信障害	サーバーへの攻撃により会社のウェブサイトが閲覧不能化	サイバー被害対応費用、事業中断、評判・ブランド等の失墜、会社役員賠償責任
第三者システムの非意図的な破壊	第三者のシステムにマルウェアを伝染	訴訟に対する防御費用、ネットワークセキュリティ欠陥の賠償責任

[5] OECD, “Enhancing the role of insurance in cyber risk management”（2017.12）

[6] 被保険者が自身の不法行為や過失行為について保険金により恩恵を受けることは認められないという考え方により、罰科金を保険で補償することを違法とする国がある。また、法令で認められるか否かにかかわらず、罰科金の補償を控える保険会社もある。

[7] GDPR（General Data Protection Regulation：一般データ保護規則）は、EU で 2018 年 5 月より施行されている、わが国の個人情報保護法に相当する法律である。世界で最も厳しい個人情報保護法規制と言われており、違反した場合には「当該企業の年間売上の 4%以上」または「2,000 万ﾕｰﾛ（約 25 億円。2018 年 12 月末時点の為替レートである 1 ﾕｰﾛ＝127 円で換算した。）」のいずれか高い金額を上限とする高額な罰金が課される可能性がある。

[8] 例えば、富裕層に対するサイバーゆすり、SNS やメールの“なりすまし”によるソーシャル・エンジニアリング攻撃、ネットいじめや誹謗・中傷、IoT 家電に対するサイバー攻撃が挙げられる。ソーシャル・エンジニアリング攻撃については脚注 29 を参照願う。

[9] 例えば、ミュンヘン再保険グループ傘下の HSB が提供する「HSB Home Cyber Protection」は、HSB と提携する保険会社の個人向け住宅保険（ホームオーナーズ保険・借家人保険）に付帯され、サイバーゆすりや詐欺のほか、スマートフォンやコンピュータ、コネクテッド・ホーム・デバイスからの個人情報漏えいを補償する。そのほか AIG の富裕層向けサイバー保険「Family CyberEdge」などがある。

サイバー被害		サイバー関連の損害の例
種類	例	
外部のサービス提供会社の断絶	クラウド上のアプリケーションソフトの断絶	事業中断
電子データの消失・使用不能等	インターネットに接続したコンピュータ上のデータをマルウェアが消去	サイバー被害対応費用、データ・ソフトウェアの消失・使用不能等、訴訟に対する防御費用、製造物責任、会社役員賠償責任
電子データの暗号化	ランサムウェア（身代金要求型のマルウェア）がデータへのアクセスを妨害	サイバー被害対応費用、サイバー恐喝・ゆすり、会社役員賠償責任
サイバー犯罪・サイバー盗難	ネットワークに不正侵入され、資金が不正送金された	金融資産の盗難・詐欺、会社役員賠償責任

（注）「サイバー被害対応費用」には、情報漏えいした可能性のある個人についての信用モニタリング費用、通知費用、フォレンジック費用（被害内容や被害の復旧方法、再発防止策等を明らかにするための調査費用）が含まれる。

（出典：OECD, “Enhancing the role of insurance in cyber risk management”（2017.12）をもとに作成）

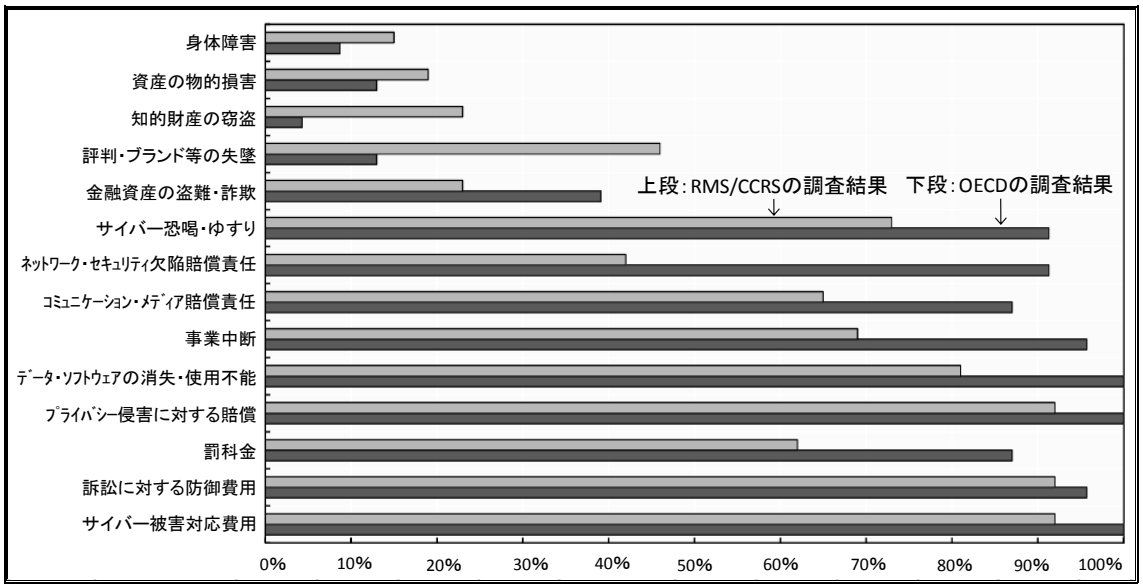
図表 3　サイバー関連の損害の分類（自社損害・第三者賠償責任・その他）(注)

分類	サイバー関連の損害
自社損害	○ネットワーク中断 ・サイバー被害による利益の逸失 ・事業中断 ・無形／有形資産の損傷 ・外部プロバイダーのセキュリティまたはシステムの欠陥に起因する損害 ・システムの欠陥や人為的ミスに起因する損害 ○サイバー恐喝・ゆすり ・身代金費用 ・サイバー専門家の人件費 ○電子データの被害（コンピュータシステムの偶発的な損傷に起因する損害） ○サイバー盗難（不正に資金を電子的に移転することによる経済的損失） ○データの復元 ○通常外特別費用 ○システムのクリーンアップ費用 ○公的機関による調査対応費用・課徴金
第三者に対する賠償責任	○データ保護およびサイバーに係る賠償責任 ・賠償責任請求 ・罰科金 ○コミュニケーション・メディア賠償責任（中傷を目的としたシステムの悪用に起因する賠償責任） ○情報の不正収集 ○メディア上での著作権等の侵害、中傷的なコンテンツ ○通知義務への違反
その他（費用・サービス）	○初期対応 ・危機管理および IT 専門家 ・機密性侵害に関連する法的アドバイス ・フォレンジック調査費用 ・コールセンターおよびホットライン ○事案管理 ・法的／広報活動 ・技術的フォレンジック ・サイバー被害に関する通知 ○コミュニケーション費用（評判・ブランドの失墜のフォロー） ○クレジットモニタリング ○犯罪に対する報奨金の積立金

（注）図表 2 と出典が異なるため、取り上げられているサイバー関連の損害の種類や名称が異なる。

（出典：EIOPA, “Understanding cyber insurance – A structured dialogue with insurance companies”（2018.8）をもとに作成）

図表 4　専用型サイバー保険による補償の割合（損害別）(注)



（注）このデータは、OECD の調査結果（対象：23 社）と RMS/CCRS の調査結果（対象：26 社）に基づくものであり、対象となった専用型サイバー保険の大半はグローバルに利用可能である。

（出典：OECD, “Enhancing the role of insurance in cyber risk management”（2017.12）をもとに作成）

（2）市場規模

サイバーリスクを補償する保険の全体的な市場規模を示すデータは存在しない。様々な機関が公表しているデータの大半は専用型サイバー保険のみを対象としており、現状データや将来予測にも幅がある。

専用型サイバー保険に関しては、2016 年における世界全体の総収入保険料は 25 億～35 億ﾄﾞﾙであり、米国が約 80～90%（25 億～30 億ﾄﾞﾙ）、欧州が 5～9%（1.5 億～4 億ﾄﾞﾙ）を占めるという推計がある[10]。また別の推計では、世界全体の市場規模が 2016 年：30 億ﾄﾞﾙから 2017 年：45.2 億ﾄﾞﾙに拡大し、2023 年には 175.5 億ﾄﾞﾙに達すると予測されるなど[11]、専用型サイバー保険の市場は世界的な拡大が見込まれている。特に欧州市場は、GDPR 施行の影響でサイバー保険に対する需要が高まり、将来的には米国と同等規模にまで成長するとの見方がある[12]。

また、サイバー保険に対する需要の高まりは、専用型サイバー保険だけでなく、付帯

[10] OECD, “Enhancing the role of insurance in cyber risk management”（2017.12）による。なお、アジアにおける総収入保険料は約 5,000 万ﾄﾞﾙと推計される。

[11] ResearchAndMarkets.com, “Global cyber security insurance market - segmented by size of organization, by end-user industry, and region - growth, trends & forecast (2018-2023)”（2018.4）

[12] OECD, “Enhancing the role of insurance in cyber risk management”（2017.12）

型サイバー保険とサイレント・サイバーリスクが潜在する従来型保険の市場拡大にもつながると考えられている[13]。

米国では、NAIC（全米保険庁長官会議）が専用型サイバー保険に加え、付帯型サイバー保険に関するデータも収集している[14]（図表 5 参照）。専用型サイバー保険・付帯型サイバー保険ともに成長しており、2017 年の元受収入保険料は 31 億ﾄﾞﾙに達する。ただし付帯型サイバー保険に関しては、元受収入保険料をゼロと回答した保険会社が複数あった。NAIC はこの理由について、複数のリスクを担保する従来型保険からサイバーリスクだけを抜き出すことが困難だったためだと考え、付帯型サイバー保険の元受収入保険料の一部を「サイバーリスクを補償する保険料」とみなして推計している。また、米国の損害保険市場（5,550 億ﾄﾞﾙ）においてサイバー保険（31 億ﾄﾞﾙ）が占める割合は非常に小さいが、このデータにはサイレント・サイバーリスクが潜在する従来型保険が含まれていないことに留意が必要である。

なお、サイバー保険の主要な販売市場は米国だが、その引受は米国以外の国・地域でも行われている。主要な引受市場はイギリスであり、世界全体のサイバー保険の総収入保険料の約 25%がロイズのシンジケートを通した引受とされている[15]。

図表 5　米国のサイバー保険の市場規模（元受収入保険料）(注)　単位：ﾄﾞﾙ

形態	2017 年	2016 年
専用型サイバー保険	1,759,338,551	1,363,283,406
付帯型サイバー保険	1,327,847,050	1,020,054,169
計	3,087,235,601	2,383,337,575

（注）認可保険会社とサープラスライン保険会社が販売するサイバー保険を対象としている。

（出典：NAIC, “Report on the cybersecurity insurance and identity theft coverage supplement”（2018.8）をもとに作成）

（3）サイレント・サイバーリスク問題

主要な引受市場であるイギリスでは、PRA（健全性監督機構）がサイバー関連の引受リスクの１つとして、サイレント・サイバー問題に取り組んでいる[16]。

---

[13] EU-U.S. Insurance Dialogue Project, “The cyber insurance market”（2018.10）

[14] NAIC は各州の保険庁長官によって構成される会議体である。2016 年より、保険会社に NAIC への年次報告が義務付けられる内容に、サイバー保険の引受状況の記載が追加された。この目的は、保険会社によるサイバー保険の引受が円滑に進むよう、サイバー保険の市場規模・成長性や、保険金支払・収益性の状況をモニターし、万が一巨額な保険金支払が生じた場合に保険会社の支払能力に致命的な影響を及ぼすことがないよう監視することである。なお、EU では現状、こうした情報収集体制は整備されていない（EU-U.S. Insurance Dialogue Project, “The cyber insurance market”（2018.10））。

[15] OECD, “Enhancing the role of insurance in cyber risk management”（2017.12）による。なお OECD によると、ロイズ市場では、2015 年時点で 63 のシンジゲートがサイバー保険を引き受け、総収入保険料は 3 億 2,200 万ﾎﾟﾝﾄﾞ（約 452 億円。2018 年 12 月末時点の為替レートである 1ﾎﾟﾝﾄﾞ＝140.46 円で換算した。）、うち 80%が米国内の企業向けに提供された。またエーオンによると、米国の 2015 年の専用型サイバー保険（15 億ﾄﾞﾙ）の 30%（4 億 5,000 万ﾄﾞﾙ）がロイズによって引き受けられた（Aon, “Global cyber market overview – uncovering the hidden opportunities”（2017.1））。

[16] PRA は、サイバー保険市場が急速に発展するなか、この分野から生じるプルデンシャル・リスクを適切に管理しなければ、保険会社等の存続可能性とイギリス保険業界の評判に重大な影響が及ぶ可能性があ

図表 6 は、PRA が 2015 年から 2016 年にかけて実施した、サイバー関連の引受リスクに関するテーマ・レビュー[17]の結果である。このレビューでは、サイバー保険が補償する「明示的なサイバーリスク」と、サイバーリスクを明示的に除外していないオールリスク型保険その他賠償責任保険に潜在する「サイレント・サイバーリスク」[18]に関して、多くの課題が指摘されている。

サイレント・サイバーリスクに関しては、ほとんどの保険会社が定量化や管理を十分に実施していないことが指摘されている。EIOPA（欧州保険・年金監督当局）が欧州の保険会社 13 社に実施したアンケート調査では、サイレント・サイバーリスクの定量化について 9 社は「とても難しい」、2 社は「不可能に近い」と回答し[19]、保険業界において対応が難しい課題と認識されている。

しかし、専用型サイバー保険に対する需要の高まりは、サイレント・サイバーリスクが潜在する従来型保険の市場拡大にもつながると予想され（前記（2）参照）、こうした市場拡大は、財物保険や新種保険におけるサイレント・サイバーリスクのエクスポージャーを増大させる可能性があると考えられている。

図表 6　明示的なサイバーリスクおよびサイレント・サイバーリスクの引受に関する課題

①	サイレント・サイバーリスクは重大な影響を及ぼす可能性があること サイレント・サイバーが潜在することについてはほぼ例外なく認識されていたが、ほとんどの保険会社はサイレント・サイバーリスクの定量化および管理に関して堅固な手法を実践していない。
②	サイレント損害の発生可能性は時間とともに増大すること サイレント・サイバーリスクを補償する保険の認知度とサイバー攻撃の頻度が高まるにつれ、発生し得るサイレント損害のエクスポージャーも増大する。「サイバーリスクを補償しない」という保険会社の主張が認められなくなる可能性が高まるとの見方がある。
③	新種保険はサイレント・サイバーリスクに大いに晒されている可能性があること 新種保険は、免責が一般的に使用されていないこと（例：専門職業賠償責任保険（PI）、金融機関包括補償保険（FI）、総合賠償責任保険（GL））、および保険の性質上サイバー関連の損害を合理的に除外できない保険約款があること（例：会社役員の広範なリスクを補償する D&O 保険）を理由として、サイレント・サイバーリスクに大いに晒されている可能性がある。

るとの考えに基づき、2015 年以降、サイバー関連の引受リスクについて継続的に取り組んでいる。なお、サイバー関連の引受リスクは「有形物か無形物かにかかわらず、悪意のある行為（サイバー攻撃、IT システムの悪意のあるコードへの感染など）または悪意のない行為（データ消失、偶発的行為、不作為など）に起因するサイバー関連の損害に晒されている保険契約を引き受けることによって生じるプルデンシャル・リスク」と説明されている。

[17] テーマ・レビューは（再）保険会社、（再）保険仲介者、コンサルタント会社、モデリング会社、サイバーセキュリティ企業、規制当局などの利害関係者を対象に、サイバー引受戦略、提供している商品および対象企業、保険料・補償限度額・規模、エクスポージャー管理および再保険、サイレント・サイバーのエクスポージャー、リスク管理、サイバー保険の将来に関して実施された。

[18] PRA は、サイバー保険が補償する明示的なサイバーリスクを「affirmative cyber risk（肯定的サイバーリスク）」、従来型保険に潜在するサイレント・サイバーリスクを「non-affirmative cyber risk（非肯定的サイバーリスク）」と表現している。PRA 以外にも、サイレント・サイバーリスクを「non-affirmative cyber risk」と表現する機関があるが、本稿では「サイレント・サイバーリスク」に統一する。

[19] EIOPA, “Understanding cyber insurance – A structured dialogue with insurance companies”（2018.8）による。このアンケート調査は、イギリス、ドイツ、フランス、スイス、イタリアに所在する 13 の保険会社・再保険会社を対象に実施された。

④	海上・航空・輸送（MAT）および財物保険においてサイレント損害の可能性があること 航空保険や自動車保険では、テクノロジーの発展や自動運転車の開発、サイバーセキュリティ上の課題があるにもかかわらず、黙示的なサイバー補償が提供されている（すなわち免責が一般的に使用されていない）。また財物保険では、企業に対するサイバー攻撃やスマートハウス技術の発展により、サイバーリスクが増大している可能性がある。しかし、これらのリスクを価格付け、管理する方法は十分に開発されていないようである。
⑤	再保険契約におけるエクスポージャーと対応が不確実であること 再保険契約では新種・財物の両方につきサイバーリスクの免責が広く使用されていない。最近、一部のカスタマイズされた再保険契約にはサイバー関連の免責文言が導入されたようだが、免責文言が例外なく使用されているわけではなく、テストもされていないため、サイバー関連の請求が発生した場合に論争の火種となる可能性がある。
⑥	ほとんどの企業が、明示的なサイバーリスクとサイレント・サイバーリスクの両方を管理するための包括的な戦略を所持しておらず、多くの場合、リスク選好ステートメントに基づく明確な戦略も存在しないこと
⑦	サイバー保険が提供され始めてからそれほど時間が経過しておらず、引受について高度な知見を有する専門家が不足しているため、明示的なサイバーリスクとサイレント・サイバーリスクの両方について社内の知見を深めるための投資が不十分であること
⑧	明示的なサイバーリスクが十分に理解されていないこと クラウドの出現とサイバー空間の継続的な発展は、サイバーリスクを明示的に補償するサイバー保険に特有の課題をもたらす。しかしサイバーに関する知見や過去の損害データは限定されており、また、将来的なサイバー損害を見積もるために過去のデータを使用することは適切ではない。
⑨	サイバーリスクは継続的に進化するが、第 2 の防衛線としての機能を担うリスク管理チームがスキルと知見の面で適切に整備されていない場合があること
⑩	モデリング会社によるサイバーの異常災害モデルの開発は初期段階にあり、効果的にサイバーリスクのエクスポージャーを管理できるようになるには数年かかること
⑪	GDPR の施行により、明示的なサイバーリスクが増加すること サイバー保険の販売市場を米国から欧州へ拡大しようとする傾向が見られるが、その結果拡大した収益は、明示的なサイバーリスクが増加することによって相殺される可能性がある。

（出典：PRA, “Dear CEO – Cyber underwriting risk”（2016.11）をもとに作成）

３．サイレント・サイバーリスクの例

前記 2 のとおり、新興リスクであるサイバーリスクについて明示的に言及していない従来型保険であっても、サイバー関連の損害をサイレント・サイバーリスクとして補償しているとみなされる可能性がある。このような状況を踏まえ、米国やイギリスではサイバー関連の免責を導入する動きがある。本項ではそれらの具体例として、サイバー保険の主要な販売市場である米国の判例と ISO[20]の免責を説明する。また、主要な引受市場であるイギリスの LMA（ロイズ市場協会）が実施したモデル約款・免責条項の分析結果を説明する。LMA の分析では、サイバー関連の免責が一部のサイバーリスクを復活担保する事例が確認されている。

（1）米国

米国では、サイバー関連の損害が従来型保険によって補償されるか否かについて、数多くの裁判が行われてきた。しかし判決は一様でなく、従来型保険の補償範囲外とする

[20] ISO（Insurance Services Office）は米国においてモデル約款の提供や保険料率の算出、その他各種データ提供などを行う団体である。

保険会社の見解を支持した判決もあれば、従来型保険に潜在する特定のサイレント・サイバーリスクが表面化した事例もあった。

以下ではその一例として、図表 7 に挙げる 3 つのサイバー被害に関して、企業財産保険、CGL（企業総合賠償責任保険）[21]、犯罪保険で補償の可否が検討された判例を紹介する。また、サイレント・サイバーリスクを従来型保険から除外するために ISO が開発したサイバー関連の免責についても併せて説明する。

図表 7　本項で取り上げるサイバー被害・裁判の対象となった従来型保険・ISO 免責

<table>
<tr><th>サイバー被害</th><th>裁判の対象となった従来型保険</th><th>ISO 免責</th></tr>
<tr><td rowspan="2">データ・ソフトウェアの消失・使用不能等</td><td>○企業財産保険
火災、落雷、爆発、電気的・機械的事故等の様々な偶然の事故によって、保険の対象に生じる直接的な物的損害、事業中断による休業損失等を補償する保険。</td><td rowspan="2">電子データ</td></tr>
<tr><td>○CGL－補償条項 A「身体障害・物的損害」
身体障害または物的損害に起因して、被保険者が負担する法律上の賠償責任を補償する保険。また、保険会社はその賠償責任を請求する訴訟から被保険者を防御する権利・義務を有する。</td></tr>
<tr><td>第三者データの機密性侵害</td><td>○CGL－補償条項 B「人格権侵害・宣伝侵害」
人格権侵害または宣伝行為による侵害（侵害行為の結果として生じる身体障害を含む）に起因して、被保険者が負担する法律上の賠償責任を補償する保険。また、保険会社はその賠償責任を請求する訴訟から被保険者を防御する権利・義務を有する。</td><td rowspan="2">機密情報または個人情報のアクセスまたは開示</td></tr>
<tr><td>サイバー盗難（不正送金）</td><td>○犯罪保険「コンピュータ犯罪補償」
従業員や第三者による盗難、強盗、偽造、ゆすり等に起因する損害を補償する保険。コンピュータ犯罪補償では、被保険者の現金・有価証券・その他資産を敷地内や銀行から不正移転することを目的としたコンピュータの使用に直接起因する損害を補償する。</td><td>－</td></tr>
</table>

（出典：The Institutes, “The Institutes’ handbook of insurance policies 11th edition”（2014）ほか各種資料をもとに作成）

a. データ・ソフトウェアの消失・使用不能等

企業財産保険および CGL 補償条項 A は、ともに「有形物」が被った損害について補償を提供する[22]。保険会社は、電子データやソフトウェアは「有形物ではない」ため、これらの消失・使用不能等は企業財産保険や CGL において補償されないという見解を示していた。しかし裁判所は、保険会社の主張を支持した場合もあれば、電子データを「有形物」と認めて補償対象と判断した場合もあった[23]（図表 8 参照）。

---

[21] 企業総合賠償責任保険（CGL）は、企業の事業活動に伴って生じる損害賠償責任を包括的に補償する保険である。米国では ISO のモデル約款が広く利用されており、基本的な補償条項として、補償条項 A および B のほか、特定の事故を原因とする身体障害につき医療費用保険金を支払う補償条項 C がある。

[22] 企業財産保険は、建物や什器・備品などの動産・不動産を保険の対象としている。また ISO の CGL モデル約款は「物的損害」を次のとおり定義している。①「有形物」に対する物理的損傷（その結果「有形物」が使用不能になったことによる損害を含む）②物理的損傷を被っていない「有形物」が使用不能になったことによる損害

[23] 電子データが「有形物ではない」とする保険会社の主張を支持した判例として America Online Inc. v. St. Paul Mercury Ins. Co., 207 F. Supp. 2d 459, 467, 468-69（E.D. Va. 2002）、State Auto Prop. & Cas. Ins. Co. v. Midwest Computers & More, 147 F.Supp.2d 1113, 1116（W.D. Okla. 2001）などがある。

こうした状況に対応すべく、多くの保険会社は「有形物」の定義から電子データを除外している[24]。

またISOは2004年、電子データの免責（Electronic Data Exclusion）を開発し、企業財産保険の「保険の対象外」条項およびCGL補償条項Aの免責条項に追加した[25]。「電子データ」は図表9のとおり定義されており、データ・ソフトウェアの消失・使用不能等は現在、ISOの企業財産保険およびCGLのモデル約款の補償範囲から除外されている。ただしコンピュータのハードウェアは電子データの定義に含まれず、免責の対象とならない[26]。

なお、ISOの企業財産保険のモデル約款では、特約を付帯することでデータ・ソフトウェアの消失・使用不能等を追加補償することができる。一方CGLに関しては、2014年にISOが提供を開始した免責条項（後記b.参照）を使用することで、データ・ソフトウェアの消失・使用不能等に起因する賠償責任と自社損害を明確に免責することが可能である。

図表8　電子データを「有形物」と認めた判例

Insurance America Guarantee & Liability Insurance（保険会社）対 Ingram Micro（被保険者）
○被保険者はコンピュータを使用して注文処理や取引管理を行っていたが、施設内の停電によりすべてのコンピュータが停止し、そのうちの多くはランダムアクセスメモリ（RAM）内のプログラム構成を失ったため約8時間にわたり使用不可となり、その間、被保険者の事業は中断された。復旧後、被保険者はコンピュータの問題を診断し、修復した。 ○保険会社は、プログラム構成は「有形物」でなく、問題が生じたコンピュータは本来の機能を維持しており再プログラム可能なため、物的損害は生じていないとし、企業財産保険による補償を拒否した。 ○2000年、連邦第8巡回区控訴裁判所は以下の点から、「コンピュータが直接的な物的損害を受けた」とする被保険者の主張を認めた。 ・コンピュータ技術が仕事だけでなく個人生活をも支配する今日において、「物的損害」に関し広範な解釈を与えるべきである。 ・裁判所は、「物的損害」はコンピュータ回路の物理的な損傷等に限定されず、アクセス障害、使用不能、機能障害も含まれると解釈する。
Gulf Coast Analytical Labs.（被保険者）対 Landmark American Insurance（保険会社）
○被保険者は、コンピュータウィルスによってハードドライブに格納された電子データが破損したため、企業財産保険による補償を求めたが、保険会社は、損害が電子データの破損のみで機械装置が損害を被っていないため、直接的な物的損害は生じていないとし、保険金の支払を拒否した。 ○2012年、ルイジアナ州裁判所は以下の点から、本件は財産保険の補償範囲に含まれるとした。 ・電子データは物理的に存在しており、テープ、ディスク、ハードドライブに格納され、物理的作用によって監視、変更、または損害を与えられる可能性がある。

（出典：Karins S. Aldama & Tred R. Eyerly, “Cyber policies – the next wave”（ABA insurance coverage litigation committee CLE seminar, 2018.3.1）ほか各種資料をもとに作成）

[24] Steven R. Gilford & Braddley J. Lorden, “Chapter 16: insurance coverage for data breaches and unauthorized privacy disclosures”（Proskauer Rose LLP, 2015）

[25] Donald S. Malecki, “Risk management －Electronic data exclusion”による。なおCGLに関しては、2001年のISOモデル約款改訂において、物的損害の定義に「この保険において電子データは有形物ではない」との文言が追加されたが（Jeff Woodward, “The 2001 ISO CGL Revision”（2002.1））、2004年に電子データの免責が追加されたことでより一層明確化された。

[26] 企業財産保険では、約款の「保険の対象」条項に「機械装置」が含まれ、これに該当するコンピュータのハードウェアや周辺機器は補償対象となる。CGLに関しては、電子データの免責を付帯したCGLに関する裁判で、ハードウェアは「有形物であり電子データの定義に含まれない」として補償対象になるとの判決が下された事例がある。

図表９　電子データの免責における「電子データ」の定義

電子データとは、コンピュータソフトウェアに蓄積、生成、使用または送受信される情報、事実またはプログラムをいう。コンピュータソフトウェアとは、システムおよびアプリケーションのソフトウェアをいい、ハード、フロッピーディスク、CD-ROM、テープ、ドライブ、セル、データ処理機またはその他の電子的に制御される機器と共に使用されるものを含む。

（出典：各種資料をもとに作成）

b. 第三者データの機密性侵害

CGL の開発当初、第三者データの機密性侵害に起因する賠償責任は約款上考慮されていなかった。しかし、コンピュータシステムを通じた個人情報の漏えいが増加するにつれ、第三者データの機密性侵害が補償条項 B「人格権侵害・宣伝侵害」の対象になるか否かについて裁判で争われるケースが増加した。

こうした裁判では、第三者データの機密性侵害が、CGL 約款上の「人格権侵害・宣伝侵害」の定義[27]のうち「人のプライバシーを侵害する事実の公表」に該当するかどうかが争点となった（図表 10 参照）。「人のプライバシーを侵害する事実」に相当する第三者データが、ハッカーなど外部の者でなく被保険者により「公表」された場合、CGL の補償対象になると判断されている。

このため ISO は新たに免責条項「機密情報または個人情報のアクセスまたは開示」を開発し、2014 年 5 月より米国内のほぼ全ての地域で利用可能とした。当該免責条項は 3 種類あり、免責範囲の広さに応じて保険会社が選択可能となっている[28]。

最も免責範囲が広い免責条項（CG 21 06 05 14）は、CGL の補償条項 A・B の両方において、図表 11 の①～③すべてを補償範囲から除外する。第三者データの機密性侵害およびデータ・ソフトウェアの消失・使用不能等に起因する賠償責任に加え、自社損害であるサイバー被害対応費用についても、CGL の補償範囲から除外することが明確に定められている。

ISO によると、当該免責条項の利用は各保険会社の決定に委ねられているため、利用状況に関して言及できないものの、保険会社から好評を得ているとのことである[29]。

---

[27] ISO の CGL モデル約款は、「人格権侵害・宣伝侵害」について次のいずれかひとつまたは複数の侵害行為に起因する障害（その結果生じる身体障害を含む）と定義している。①誤認による逮捕、留置または拘禁、②悪意による訴追、③所有者や役主、賃貸人等による住宅や施設等からの不当な追い出し、不当な侵入、またはそれらについての個人的占有権の侵害、④人・組織を誹謗・中傷する事実または人・組織の商品やサービスを屈辱する事実の公表、⑤人のプライバシーを侵害する事実の公表、⑥宣伝行為における他者のアイディアの使用、⑦宣伝行為における他者の著作権等の侵害

[28] 機密情報または個人情報のアクセス・開示を、①補償条項 A と B の両方において免責する「CG 21 06 05 14」、② ①から身体障害を除いて免責する「CG 21 07 05 14」、③補償条項 B において免責する「CG 21 08 05 14」の 3 種類である。

[29] Insurance Journal, “ISO comments on CGL endorsements for data breach liability exclusions”（2014.7.18）

図表 10　第三者データの機密性侵害に関する判例

Travelers Indemnity Co.（保険会社）対 Portal Healthcare Decision（被保険者）
○被保険者は、個人の医療記録を 4 ヶ月以上にわたりインターネット上に検索可能な形で掲載していたことに関して、集団訴訟を提起された。保険会社は、当該集団訴訟に関して被保険者を防御する義務を負わないという決定を求め、確認判決訴訟を提起した。 ○2016 年、連邦第 4 巡回区控訴裁判所は以下の点から、保険会社は集団訴訟に関して被保険者を防御する義務を負うと判断した。 ・医療記録がインターネット上に掲載されている間、一般の人々がその情報を閲覧できた可能性がある。集団訴訟は、こうした行為を「患者の私生活に関する情報の不合理な公表または開示」として訴えるものであり、それが証明される場合において、当該行為は CGL の補償対象となる「人のプライバシーを侵害する事実の公表」に該当する。
Zurich Amer. Ins. Co.（保険会社）対 Sony Corporation of America（被保険者）
○被保険者が運営するプレイステーション・ネットワークにハッカーが不正侵入し、ユーザーの個人情報が漏えいした。被保険者は、この情報漏えい事件に関して少なくとも 55 の集団訴訟を提起された。 ○2014 年、ニューヨーク州最高裁判所は以下の点から、保険会社は集団訴訟に関して被保険者を防御する義務を負わないと判断した。 ・プレイステーション・ネットワークからの情報漏えいは、「人のプライバシーを侵害する事実の公表」に該当する。しかし CGL は、被保険者による「公表」を補償するものであり、第三者であるハッカーによる「公表」を補償しない。

（出典：Jana Landon, “Where does Sony settlement leave CGL insurance for data breaches?”（The Legal Intelligence, 2015.3）、Todd Rowe, “Early observations in portal healthcare decision: CGL coverage for cyber claims?”（Privacy Risk Report, 2016.4.12）ほか各種資料をもとに作成）

図表 11　「機密情報または個人情報のアクセスまたは開示」の免責事項

①　特許、企業秘密、処理方法、顧客リスト、財務情報、クレジットカード情報、健康情報、またはいかなる形式の非公開情報を含む、個人または企業の機密情報または個人情報へのアクセスまたは開示に起因する賠償責任 ②　電子データの消失・使用不能、損傷、文字化け、アクセス不能または処理不能に起因する賠償責任 ③　通知費用、信用モニタリング費用、フォレンジック費用、広報費、その他上記①・②に起因して被保険者またはその他の者が被る費用

（出典：各種資料をもとに作成）

c. サイバー盗難（不正送金）

図表 12 は、コンピュータを使用した不正送金に関して、コンピュータ犯罪補償の対象になるか否かが裁判で争われた事例である。

争点は「コンピュータの使用が損害の直接の原因であるか否か」であり、なりすましメールなどのソーシャル・エンジニアリング攻撃[30]は、「コンピュータの使用が損害の直接の原因であるか否か」の判断が異なる一方、ハッキングやコンピュータへの不正アクセスによる不正送金は、特段の免責が定められていない限り[31]、コンピュータ犯罪補償の対象になると考えられている。

[30] ソーシャル・エンジニアリング攻撃は、情報通信技術を使用しない攻撃であり、サイバー攻撃と異なり、人の心理的な隙や行動のミスを突いて情報を盗み出す。主な手法として、ショルダーハッキング（覗き見）、トラッシング（廃棄物から情報を探し出す）、なりすまし電話・メール、敷地内への侵入がある。
[31] 例えば、「従業員による意図的な行為」の免責を定め、従業員による不正送金を補償範囲から除外するケースがある（OECD, “Enhancing the role of insurance in cyber risk management”（2017.12））。

図表 12　サイバー盗難（不正送金）に関する判例

Pestmaster Services（被保険者）対 Travelers Casualty and Surety Company of America（保険会社）
○被保険者は給与関連業務を外部委託しており、小口決済ネットワーク（ACH）のシステム上で、被保険者の口座から外部委託先の口座に自動振替することで、外部委託先が給与・給与税の支払を代行できるよう設定していた。2011 年、外部委託先による給与税の流用（約 37 万ﾄﾞﾙ）が発覚した。 ○2016 年、連邦第 9 巡回区控訴裁判所は以下の点から、本件はコンピュータ犯罪の補償範囲に含まれないとした。 ・コンピュータ犯罪補償は、何者かが不正に資金を移転するためにハッキングやコンピュータへの不正アクセス・侵入を行った場合に適用される。しかし、正規のユーザーがコンピュータを目的に沿って使用した場合には適用されない。 ・外部委託先によるコンピュータの使用は、被保険者の損害に付随するものであって、直接的な原因ではなく、約款の「コンピュータの使用に直接起因する」との要件を満たしていない。
Medidata Solutions（被保険者）対 Federal Insurance（保険会社）
○被保険者は、発信元を同社の社長に偽装したなりすましメールに騙され、海外に送金した。被保険者は、海外に送金した際に被った損害 480 万ﾄﾞﾙにつき保険会社に請求したが、保険会社は、コンピュータ犯罪補償がハッキングによる被保険者の非自発的な送金の場合にのみ適用されるとし、保険金の支払を拒否した。 ○2017 年、ニューヨーク連邦裁判所は以下の点から、本件はコンピュータ犯罪補償の対象になるとした。 ・被保険者のコンピュータは直接的なハッキング攻撃を受けていないとはいえ、犯罪者は詐欺メールを本物に見せるかけるためのコードをメールに埋め込んでいた。 ・保険約款には「不正侵入またはコンピュータ内のデータ改ざんに起因する損害を補償する」と記載されており、本件は、約款上の「不正侵入」に該当する。
Apach（保険会社）対 Great American Insurance（被保険者）
○被保険者は、同社の外部委託先を装った詐欺師から、なりすまし電話となりすましメールで支払口座を変更するよう依頼された。被保険者の従業員は、最小限の調査を行った後、本来の外部委託先の銀行口座から詐欺師の指定する銀行口座に支払先を変更し、送金した。 ○テキサス州地裁は、詐欺行為において人が介在しているにもかかわらず、本件は補償されると判断したが、2016 年、連邦第 5 巡回区控訴裁判所はこの判決を取り消し、以下の点から、本件はコンピュータ犯罪の補償範囲に含まれないとした。 ・保険約款には「不正な移転を目的としたコンピュータの使用に直接起因する損害を補償する」と記載されているが、口座変更を指示するなりすましメールは、不正な移転の直接的な原因ではなく、被保険者の従業員に送金させるための詐欺計画の一部にすぎない。

（出典：Jeff Sistrunk, “The state of computer fraud coverage law: 5 key rulings”（Law360, 2017.10.30）
ほか各種資料をもとに作成）

（2）イギリス（ロイズ市場）

LMA は、ロイズ市場で利用されている従来型保険のモデル約款・条項について、サイバー関連の損害を免責または補償する文言が含まれるか否かを分析した。図表 13 では、その一部として 10 のモデル約款・条項を示している。

図表中、LMA3127・LMA3150・NMA2912・NMA2918 の 4 つには、サイバー関連の損害を免責する文言が定められている一方、補償する文言は定められていないため、サイレント・サイバーリスクが認められない。

残り 6 つのモデル約款・条項には、以下のいずれかの形態でサイレント・サイバーリスクが潜在している可能性がある。

① サイバー関連の免責を付帯しない
② 一部のリスクを復活担保する

①に該当するのはLMA3141である。これは、コンピュータを使用する金融機関が悪意のある行為によって被った経済的損失を補償する「電子犯罪およびコンピュータ犯罪保険（Electronic and Computer Crime policy）」のモデル約款であり、サイバー関連の損害を免責する文言がない。当該モデル約款では、ハッキングやコンピュータへの不正アクセスによる不正送金が、米国の犯罪保険（コンピュータ犯罪補償）と同様に補償されると考えられる[32]。

②に該当するのは、NMA2914・NMA2915・LMA3030A・LMA3092A・CL380の5つであり、サイバー関連の損害を免責する文言に加え、免責された損害の一部を復活担保する文言が定められている。図表14は、このうち多くの種目で利用されている3つのモデル免責条項NMA2914・NMA2915・CL380の概要である。

MMA2914およびNMA2915は、損害の原因が悪意のある行為であるか否かにかかわらず、データ・ソフトウェアの消失・使用不能等を免責したうえで、それらに起因する火災および爆発を復活担保する。例えば、サイバー攻撃により工場の制御システムのコードが改ざんされ火災が発生した場合の物的損害は、これらの免責条項でサイレント・サイバーリスクとして補償される可能性がある[33]。なお米国ISOの電子データの免責と同様に、コンピュータのハードウェア（電子データの処理メディア）は電子データの定義に含まれず、免責の対象とならない[34]。

一方CL380は、損害の原因を悪意のある行為（危害を与える手段としてのコンピュータ等の使用）に限定し、それに起因する直接損害および間接損害を免責する。復活担保の範囲はMMA2914・NMA2915に比べて限定的である。ただし、損害の原因を「危害を与える手段」に限定しているため、悪意のないサイバー被害は免責されないことに留意が必要である。また「危害を与える手段」という文言が特段定義されていないため、事故発生後の保険金支払対応においてその解釈を巡り論争が生じる懸念があるとの指摘がある[35]。

図表13　モデル約款・条項に含まれるサイバー関連の文言（注）

文言		LMA 3030A	LMA 3092A	LMA 3127	LMA 3141	LMA 3150	CL 380	NMA 2912	NMA 2918	NMA 2914	NMA 2915
免責	悪意のある行為	●	●			●	●				
	悪意＋悪意のない行為			●				●	●	●	●
補償（復活担保含む）		●	●		●		●			●	●

（注）免責または補償する文言がある場合は「●」、ない場合は空欄としている。

（出典：LMA, “Cyber risks and exposures, model clauses – Class of business review”（2018.1）をもとに作成）

[32] 前記3.（1）cを参照願う。
[33] IMIA Working Group, “Cyber risks engineering insurers perspective”（2016）
[34] 前記3.（1）aを参照願う。
[35] IMIA “Cyber Risks – PD/BI coverage in industrial property cyber exposure for power, energy and project risks”（2016.11）

図表 14　モデル条項「NMA2914」「NMA2915」「CL380」の概要

免責条項	概要	利用されている保険種目
NMA2914（Electronic Data Endorsement A） および NMA2915（Electronic Data Endorsement B）	1. 電子データの免責（NMA2914・2915 共通） a) この保険は、いかなる原因（コンピュータウィルスを含む）に起因する電子データ（プログラム、ソフトウェア、データ処理や電子的に制御された機器の操縦に関する命令コードを含む）の喪失、損傷、破壊、歪曲、消失、文字化け、改ざん、およびいかなる性質の使用不能、機能の低下、費用を補償しない。 b) ただし、以下の危険が上記 a)のいずれかを原因とする場合、当該危険に直接起因する保険の対象への物的損害を補償する。 ・火災 ・爆発 2. 電子データの処理メディアの査定 この保険で補償される電子データの処理メディアがこの保険で補償される物的損害を被った場合の査定基準は次のとおり。 ○NMA2914 : 当該メディアを損害直前の状態に修復・交換するための費用と、当該メディア内の電子データの再生費用（復元や再設計に係る費用を含む）。修復等を行わない場合は空白メディアの費用。 ○NMA2915 : 空白メディアの費用と、バックアップ等から電子データをコピーする費用（電子データの復元や再設計に係る費用は除外）。	○ノンマリン ・Engineering ・Onshore Energy ・Power Generation ・Property D&F ・Property UK Commercial ・Terrorism
CL380（Institute Cyber Attack Exclusion Clause）	1.1 この保険は、危害を与える手段としてのコンピュータ等（コンピュータ、コンピュータシステム、コンピュータソフトウェアプログラム、悪意のあるコード、コンピュータウィルス、コンピュータ処理、その他電子システム）の使用または運用に直接または間接的に起因する損害賠償責任または費用を補償しない。 1.2 この免責条項が戦争、反乱、暴動、テロ、政治的動機に基づく行為等のリスクを担保する保険に付帯される場合、上記 1.1 は、いかなる武器・ミサイルの発射・誘導システムや点火装置内のコンピュータ等の使用に起因する損害に適用しない。	○航空 ○マリン ○ノンマリン ・GL ・Livestock ・Onshore Energy, ・Political Risks ・Power Generation ・Property UK Commercial

（出典：IMIA Working Group, “Cyber risks engineering insurers perspective”（2016）および LMA, “Cyber risks and exposures, model clauses – Class of business review”（2018.1）をもとに作成）

4．サイレント・サイバーリスクへの対応

本項では、イギリスの LMA（ロイズ市場協会）による従来型保険の引受時の留意点、PRA（健全性監督機構）が保険業界に期待する対応、および欧米の保険業界の取組事例を説明する。

（1）イギリス LMA（ロイズ市場協会）による従来型保険の引受時の留意点

LMA は、アンダーライターが従来型保険におけるサイレント・サイバーリスクの潜在的な影響を考慮するにあたって重視すべき点を「頻度」・「規模」・「システミックリスク」の観点で整理している（図表 15 参照）。

これによると、データの機密性侵害の増加は、当該サイバー被害に起因する賠償責任を補償するノンマリン種目において、「頻度」と「規模」の両方に影響を及ぼしている可能性がある。例えば、CGL（企業総合賠償責任保険）の約款に第三者データの機密性侵害の免責が導入されていない場合、当該保険におけるサイレント・サイバーリスクの

エクスポージャーは増大している可能性があると考えられる。

一方、物的損害に関しては、例えばサイバー攻撃を原因とする火災に起因する物的損害はモデル条項 NMA2914・NMA2915 においてサイレント・サイバーリスクとして補償される可能性があるが（前記 3.（2）参照）、従来型保険において補償される「頻度」は現在のところ低く、「規模」についても従来型保険が伝統的に補償している火災に比べて小さいと考えられている。

なお、サイバー被害がシステミックリスクを引き起こす可能性も指摘されているが、その影響は、サイレント・サイバーリスクが潜在する従来型保険よりも、サイバーリスクを明示的に補償するサイバー保険に大きく及ぶとされている。

図表 15　従来型保険の引受時の留意点

	物的損害	賠償責任
損害の頻度	○データが不足しているため、頻度の影響を確定的に述べることは非常に難しい。 ○物的損害をもたらすサイバー攻撃は、保険が付保されている場合、ノンマリン市場に影響を及ぼしている可能性がある。 ○ただし、保険が付保されていない損害が発生していることや、保険会社による調査やデータへのアクセスが非常に限定的であることから、そのようなサイバー被害の発生は現在のところ非常に稀である。	○ノンマリン市場において、データの機密性侵害やシステム障害を含むサイバー被害の頻度が増加している。ただし、すべての損害につき保険が付保されているわけではなく、頻度は、保険の補償範囲やサイバー被害に起因する経済的損失の性質による。 ○マリン種目で補償される賠償責任は、通常、物的損害が要因であることを必要とするため、マリン種目の賠償責任は、物的損害に比べてサイバー・エクスポージャーに晒されているとは考え難い。
損害の規模	○サイバー被害に起因する火事や爆発は、例えば放火により石油精製所が爆発した場合に比べ、損害の規模が小さいと考えられる。 ○盗難損害に関しても、通常、保険の対象を物理的に持ち去ることが要件となるため、損害の規模は限定される。ただし、このことは、暗号通貨やその他電子証券に関する盗難損害には必ずしも適用されないだろう。	○電子データは、紙よりも大量に持ち去ることが容易なため、ノンマリン市場における損害の規模が大きい可能性がある。 ○航空保険分野における損害（例えば発券システムの障害）は、航空保険以外の損害保険の対象になるだろう。
システミックリスク	○データが不足しているため、システミックリスクが存在するサイバー被害の範囲を正確に述べることは非常に難しい。しかし、2017 年の Petya／NotPetya 攻撃により、サイバー被害が多様な事業に大規模な損害と混乱をもたらす可能性があることが明らかとなり、サイバー被害に対する補償について更なる考慮が必要となった。例えば、クラウドコンピューティングサービスの使用の増加によって、多数の被保険者がサイバー関連の損害を被る可能性がある。 ○ただし、こうしたサイバー被害に起因する各種システミック損害は、サイバー被害を復活担保する従来型保険よりも、サイバー関連の損害を明示的に補償するサイバー保険に影響を及ぼす可能性が高い。	

（出典：LMA, “Cyber risks and exposures, model clauses – Class of business review”（2018.1）をもとに作成）

（2）イギリス PRA（健全性監督機構）等が保険業界に期待する対応

PRA は 2017 年 7 月、前記 2.（3）のテーマ・レビューに対するフィードバックを踏まえ、サイバー関連の引受リスクに関して損害保険会社等の企業[36]に期待される対応を

[36] ソルベンシーⅡ規制の対象企業（保険会社、再保険会社、ロイズ市場など）である。

記した監督ステートメントを発行した。

サイレント・サイバーリスクに関するものは図表 16 のとおりであり、サイレント・サイバーリスクの意図しないエクスポージャーを低減するための措置として、サイレント・サイバーリスクを補償する可能性のあるすべての従来型保険について、サイバーリスクを考慮した保険料や補償限度額の設定、サイバー関連の免責の導入などを検討すべきとしている。また、従来型保険で追加保険料を課さずにサイバー関連の損害を補償する場合でも、補償する旨を約款において明確化すべきとしている。

補償範囲の明確化に関しては、EIOPA によると、一部の保険会社はサイレント・サイバーリスクへの対応としてシナリオ開発やストレステストを実行するとともに、従来型保険の約款文言の改定を進めている（図表 17）。しかし、補償範囲を明確化するために導入されたサイバー関連の免責が、従来型保険の補償範囲からサイバーリスクを効果的に除外せず、反対に、サイバー関連の損害が補償されることを明確化する場合もあることが指摘されている[37]。従来型保険の補償範囲からサイレント・サイバーリスクを除外する場合には、前記 3.（2）の LMA による分析のように、免責条項の中にサイバー関連の損害を復活担保する文言が含まれていないかを確認する必要があるだろう。

また補償限度額の設定に関しては、OECD によると、従来型保険の補償限度額は一般的に専用型サイバー保険よりも高額に設定されているため、保険契約者は専用型サイバー保険よりも従来型保険を好む可能性がある。しかし、専用型サイバー保険の発展はサイバーリスクの定量化および管理に関するインセンティブを生み出すが、こうしたインセンティブはサイバーリスクを担保危険の 1 つとして取り扱う従来型保険では生み出されない。このため OECD は、サイバーリスクを補償する保険に複数の形態がある状況は、保険契約者を混乱させるとともに、サイバー保険の発展も妨げる可能性があることを指摘している[38]。

図表 16　PRA が保険会社に期待するサイレント・サイバーリスクへの対応

○すべての企業が、サイレント・サイバーリスクを具体的に考慮したうえで、保険商品を評価し積極的に管理することを期待する。これには、物的損害および非物的損害によるサイバーリスクのエクスポージャーを生じさせる可能性のあるすべての損害保険が含まれる。
○また企業が、残存リスクを取締役会が合意したリスク選好および戦略と整合させるために、サイレント・サイバーリスクの意図しないエクスポージャーを減らすための措置を導入することを期待する。これを達成するため、企業は、サイレント・サイバーリスクに対応した資本を十分に確保するとともに、他のリスクと同様に、例えば以下の対応を検討すべきである。
・追加のリスクを反映し明示的な補償を提供するために保険料を調整すること
・確実な免責文言を導入すること
・補償限度額を具体的に定めること

[37] EIOPA, “Understanding cyber insurance – A structured dialogue with insurance companies”（2018.8）
[38] OECD, “Enhancing the role of insurance in cyber risk management”（2017.12）

○企業が特定の保険商品や保険種目で追加保険料を課さずにサイバー補償を提供すると決定する場合、 ・その結果生じ得る損害について包括的な評価が実施されたこと、およびサイレント・サイバーリスクのエクスポージャーがリスク選好に含まれていることが、当該企業の取締役会によって確認されることが期待される。 ・サイバー補償が特定の保険商品や保険種目の一部として提供されることを明確化するために、保険契約の文言を書き換えることが望まれる。
○PRA の短期～中期的目標は、企業がサイレント・サイバーリスクを監視、管理、低減し、保険契約者に提供される補償レベルや補償内容の確実性を高めるための能力を強化することである。PRA は、企業がサイレント・サイバーリスクのエクスポージャーを評価するための適切なアプローチを採用することを期待する。その際、企業の引受部門およびリスク管理部門が主要な役割を担うべきである。

（出典：PRA, “Supervisory statement (SS4/17) －Cyber insurance underwriting risk”（2017.7）をもとに作成）

図表 17　サイレント・サイバーリスクへの主な対応

（出典：EIOPA, “Understanding cyber insurance – A structured dialogue with insurance companies”（2018.8）をもとに作成）

（3）欧米の保険業界の取組事例

前記（2）のとおり、一部の保険会社は従来型保険の約款を改定して補償範囲の明確化を進めている。

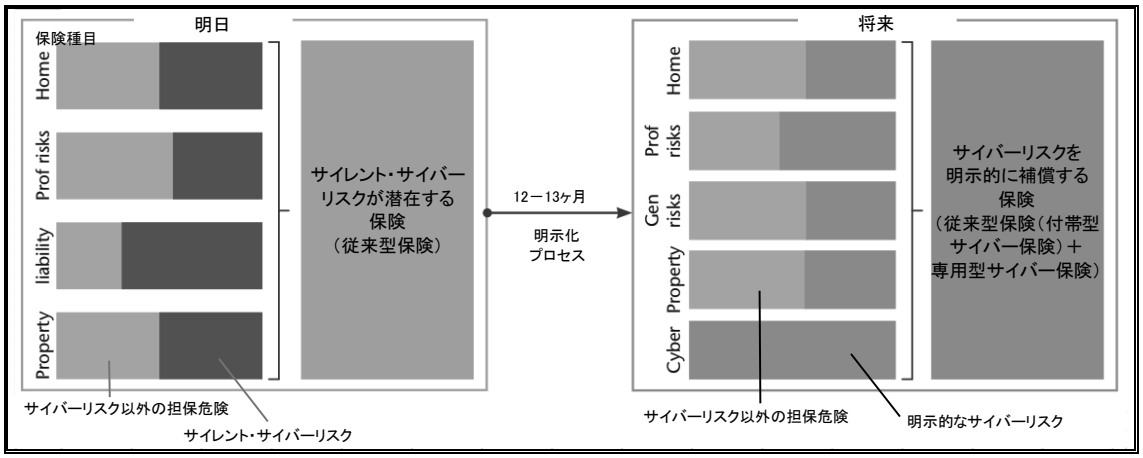
アリアンツ・グループ傘下の AGCS は、企業向け損害保険の約款を改定し、2019 年 1 月 1 日以降始期の新規契約、および 2019 年 4 月 1 日以降始期の更改契約に適用する。改定後の損害保険約款では、サイバー被害に起因する物的損害および身体障害を補償するが、物的損害または身体障害を伴わない経済的損失は補償しないことが明確化される。例えば、ハッキング攻撃によって工場の火災が発生した場合の物的損害は、同社の従来型保険で明示的に補償されることになる。しかし、例えばシステムがマルウェアへ感染し商品・サービスの納期に遅延した場合、それによって企業が被る経済的損失は従来型保険で補償されないため、企業は専用型サイバー保険を手配するか、従来型保険にサイバーリスクの補償を特約付帯する（すなわち付帯型サイバー保険を手配する）ことが必要になる[39]。

[39] Charlie Wood “Allianz to address silent cyber with updated policy wordings”（2018.11）

またロイズ市場では、サイバーリスクを除外する新たなモデル免責条項の開発が進められているほか、サイバーリスクを明示的に補償する文言の使用も増加している。LMA によると、サイバーリスクを明示的に補償する文言の使用は 2015 年においてゼロであったが、2017 年には、ロイズ市場で引き受けられた保険契約の 2～3%が該当するという[40]。

さらに大手仲介者のエーオンは 2018 年 10 月、サイレント・サイバーリスクのエクスポージャーを定量化するための保険会社向けソリューションを開発したことを公表した。このソリューションでは、サイレント・サイバーリスクが保険会社のポートフォリオ全体に潜在している可能性があるため、保険約款の文言分析・サイレント・サイバーリスクの定量化・保険会社ごとのシナリオ開発・再保険へのリスク移転などを種目横断で行い、補償範囲の透明性、保険料設定、および支払能力を改善させる。こうした対応により、将来的にはサイバーリスクが従来型保険に「サイレント」に存在する状況がなくなり、再保険を含むサイバー保険市場の強化が期待されるとしている（図表 18 参照）。

図表 18　サイレント・サイバーリスクの明示化のイメージ図



（出典：Aon UK Limited trading as Aon Benfield, “Managing silent cyber – A new solution for insurer”（2018）をもとに作成）

５．おわりに

サイバー被害には様々な種類があり、もたらされる損害も多様であるが、その多くは従来型保険によって伝統的に補償されてきた物的損害や賠償責任に該当する可能性がある。また、本稿ではサイレント・サイバーリスクの事例として一部の企業向け損害保険のみを取り上げたが、サイレント・サイバーリスクは様々な保険種目に潜在している可

[40] LMA, “Cyber risks and exposures, model clauses – Class of business review”（2018.1）

能性がある。

今後、自動運転車やIoTなどのテクノロジーはさらに進展し、企業活動や個人生活に必要不可欠なものとなるだろう。その結果、保険会社においてはサイバー保険の市場拡大が見込める一方、従来型保険に潜在するサイレント・サイバーリスクのエクスポージャーも増大する可能性がある。このため、会社がサイレント・サイバーリスクを特定し、適切な対応を講ずることの重要性はますます高まると考えられる。

国・地域や保険会社の別によって法規制、判例の取扱、保険約款の内容などが異なるため、本稿で紹介した米国やイギリスの事例をわが国の状況にそのまま適用できるわけではないが、保険業界の着眼点や損害保険の補償範囲を明確化する取組などは、サイレント・サイバーリスクへの対応を進める際のひとつの参考になるのではないだろうか。

＜参考資料＞

・石原康史「損害保険におけるエマージング・リスクへの取組みの一例－サイバーリスクについて－」保険学雑誌第 642 号（日本保険学会、2018.9）
・牛窪賢一「米国におけるサイバー保険の動向」損保総研レポート第 120 号（損害保険事業総合研究所、2017.7）
・保険毎日新聞「金融庁 業界団体との意見交換会で主な論点公表① 外貨建保険の募集実態検証へ」（2018 年 11 月 1 日）
・三井住友海上火災保険会社「損害保険講座テキスト 新種保険論（賠償責任）2017 年版」（損害保険事業総合研究所、2017.4）
・Amanda T. Dimatteo & Robert A. McCall, “Cyber scams are not computer fraud under commercial crime insurance”（Peadoby & Arnold, 2017.7.6）
・Aon, “Global cyber market overview – Uncovering the hidden opportunities”（2017.1）
・Aon UK Limited trading as Aon Benfield, “Managing silent cyber – A new solution for insurer”（2018）
・Artemis, “Silent cyber has potential to cause ILS fund losses, scenario shows”（2018.10.26）
・Best’s Review, “Special report focuses on cyber insurance - Best's special Report (Excerpt): cyber insurance market: stress testing the future”（2018.10）
・Brian T. Himmel, Cristina M. shea, David E. Weiss & J. Andrew Moss, “Cyber, data-security liability claims: coverage under traditional lines of insurance”（Read Smith Client Alters, 2014.9.8）
・Butcher, Robinson & Staples International Limited, “Electronic crime”
・Cambridge Centre for Risk Studies & Risk Management Solutions, Inc. “Cyber risk outlook”（Cambridge Judge Business School, University of Cambridge, 2018）
・Charlie Wood, “Allianz to address silent cyber with updated policy wordings”（2018.11）
・Daniel M. Hofmann & Steve Wilson, “Advancing accumulation risk management in cyber insurance - Prerequisites for the development of a sustainable cyber risk insurance market”（Geneva Association, 2018.8）
・Darren Lee Pain, Jonathan Anchen, Maya Bundt, Eric Durand & Michael Schmitt, “Cyber: in search of resilience in an interconnected world”（Swiss Re, 2016.10）
・Donald S. Malecki, “Risk management －Electronic data exclusion”
・EIOPA, “Understanding cyber insurance – A structured dialogue with insurance companies”（2018.8）
・EU-U.S. Insurance Dialogue Project, “The cyber insurance market”（2018.10）
・IMIA, “Cyber Risks – PD/BI coverage in industrial property cyber exposure for power, energy and project risks”（2016.11）
・IMIA Working Group, “Cyber risks engineering insurers perspective”（2016）

・Insurance Journal, “ISO comments on CGL endorsements for data breach liability exclusions”（2014.7.18）
・Jana Landon, “Where does Sony settlement leave CGL insurance for data breaches?”（The Legal Intelligence, 2015.3）
・Jeff Sistrunk, “The state of computer fraud coverage law: 5 key rulings”（law360, 2017.10.30）
・Jeff Woodward, “The 2001 ISO CGL revision”（2002.1）
・John Loveland, “Cyber insurance – I don’t think it means what you think it means”（RSA Conference 2017, 2017.2）
・K&L Gates, “Insurance coverage for cyber risks and realities - Presentation to the Association of Corporate Counsel — Western Pennsylvania Chapter”（2013.9.24）
・Karins S. Aldama & Tred R. Eyerly, “Cyber policies – the next wave”（ABA insurance coverage litigation committee CLE seminar, 2018.3.1）
・LMA, “Cyber risks and exposures, model clauses – Class of business review”（2018.1）
・Martin Samson, “American guarantee & Liability insurance Co. v. Ingram Micro, Inc.”（Internet Library of Law and Curt Decisions）
・Michael L. Young, “Do ISO’s new “Access of disclosure of confidential or personal information and data-related liability” exclusions eliminate insurance coverage for cyber liability and data breach claims?”（2014.5.1）
・NAIC, “Report on the cybersecurity insurance and identity theft coverage supplement”（2018.8）
・NAIC, “Report on the cybersecurity insurance coverage supplement”（2017.8.6）
・OECD, “Enhancing the role of insurance in cyber risk management”（2017.12）
・Pascal Millaire, “7 Predictions for how IoT will impact the global insurance industry”（Symantec. Connect, 2016.9.28）
・Paul McNamara, “Modelling silent cyber incidents”（Asia Insurance Review, 2018.11）
・Paul Merry, Matthew Smith, Matthew Martindale & Artures Kokins, “Sizing the cyber insurance opportunity – Rethinking insurers’ strategies and structures in the digital age”（KPMG, 2017.7）
・PCS, “PCS global risk loss report FY2017”（2018.9）
・PRA, “Consultation paper (CP39/16) – Cyber insurance underwriting risk”（2016.11）
・PRA, “Dear CEO – Cyber underwriting risk”（2016.11）
・PRA, “Supervisory statement (SS4/17) – Cyber insurance underwriting risk”（2017.7）
・ResearchAndMarkets.com, “Global cyber security insurance market - segmented by size of organization, by end-user industry, and region - growth, trends & forecast (2018-2023)
・Suzanne Barlyn, “AIG expanding commercial casualty policies to include cyber”（Insurance Journal, 2017.11.6）
・Todd Rowe, “Early observations in portal healthcare decision: CGL coverage for cyber claims?”（Privacy risk report, 2016.4.12）

・Troutman sanders, “Retail Ventures decision is another example of ongoing efforts to determine how insurance applies to cyber attacks”（2012.9.17）

＜参考ウェブサイト＞

・イギリス健全性監督機構（PRA）　https://www.bankofengland.co.uk/prudential-regulation
・欧州保険・年金監督局（EIOPA）　https://eiopa.europa.eu/
・金融庁　http://www.fsa.go.jp/
・経済協力開発機構（OECD）　http://www.oecd.org/
・全米保険庁長官会議（NAIC）　http://www.naic.org/
・ロイズ市場協会（LMA）　https://www.lmalloyds.com/
・Business Insurance　https://www.businessinsurance.com/
・Insurance Journal　https://www.insurancejournal.com/
・Law360　https://www.law360.com/
・Lexology　http://www.lexology.com/
・PwC　http://www.pwc.com/