サイバーリスクとサイバー保険

－米国の動向を中心として－

グループリーダー 主席研究員　牛窪　賢一

目　　次

要旨

近年、世界的にサイバーリスクに対する関心が高まっている。様々なモノがインターネットでつながれるIoT（Internet of Things）時代が到来しつつある中で、企業にとってもサイバーリスクの管理が重要になっており、このリスク管理のうちのリスク移転の役割を担うのがサイバー保険である。

米国では、わが国よりも早い段階から、官民挙げてサイバーリスク対策が推進されてきた。サイバー保険の利用も進んでおり、全世界のサイバー保険市場のおよそ90%（収入保険料ベース）を米国1国で占めているとの推計もある。

本稿では、サイバーリスクおよびサイバー保険の動向について、米国の最近のデータを中心に説明し、保険規制の整備を図る全米保険庁長官会議（NAIC）の取組等についても紹介する。

サイバー保険市場は、将来的にわが国でも大きく拡大する可能性がある。保険会社にとっては、保険の引受やリスク管理に関するアドバイスの提供等、今後大きなビジネスチャンスにつながる可能性のある領域である。一方、リスク管理が十分でないまま、引受を拡大してしまうと、将来的に保険会社の経営に重大な影響を及ぼす可能性も考えられる。

保険会社は、自社のサイバーセキュリティを高度化するとともに、サイバー保険の引受によるデータの蓄積と分析や、業界内外および政府との情報共有等を通じて、より企業のニーズに合った商品の開発、企業が抱えるリスクの評価やモニタリング、引受リスクの管理等の分野において競争力を高める必要がある。

そのためには、サイバーセキュリティに関し高度の専門性を有する人材およびセキュリティ施策をマネジメントできる人材の採用や育成を含む態勢の整備が欠かせないと考えられる。

１．はじめに

近年、世界的にサイバーリスク[1]に対する関心が高まっている。様々なモノがインターネットでつながれるIoT（Internet of Things）時代が到来しつつある中で、サイバーリスクへの対応の重要性が、政府、企業、保険会社それぞれのレベルで高まっている。

実際、サイバー攻撃による被害は世界的に拡大傾向にある。わが国では、2015年6月に日本年金機構において、サイバー攻撃（標的型メールによる不正アクセス）により年金情報125万件が流出したと公表された。また、2016年6月には、大手旅行会社JTBも、同様のサイバー攻撃により最大793万人分[2]の個人情報が流出した可能性があると公表した。

サイバー被害の拡大を背景として、わが国でも規制や態勢の整備が急速に進められている。例えば、サイバーセキュリティの強化を図るための基本理念等を定めたサイバーセキュリティ基本法が2015年1月から完全施行となった。この法律に基づき、2015年9月には、今後3年程度のサイバーセキュリティ政策の基本的な方向性を示す新たな国家戦略として「サイバーセキュリティ戦略」が閣議決定された。

企業にとってもサイバーリスクの管理が重要になっている。このリスク管理のうちのリスク移転の役割を担うのがサイバー保険[3]であり、2015年には国内大手損害保険会社が相次いでサイバー保険の販売を開始した。

米国では、わが国よりも早い段階から、官民挙げてサイバーリスク対策が推進されてきた。サイバー保険の利用も進んでおり、全世界のサイバー保険市場のおよそ90%（収入保険料ベース）を米国1国で占めているとの推計もある[4]。

本稿では、サイバーリスクおよびサイバー保険の動向について、米国の最近のデータを中心に説明し、保険規制の整備を図る全米保険庁長官会議（NAIC）[5]の取組等についても紹介する。当研究所では、サイバーリスクとサイバー保険について、2015年1月発行の損保総研レポート[6]で取り上げているため、本稿では、それ以降の動きを中心に取り上げる。

なお、本稿における意見・考察は筆者の個人的見解であり、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。

---

[1] サイバーリスクについて定型化された定義はないが、本稿では、「インターネットやテレコミュニケーション・ネットワーク等のテクノロジー・ツールを含む電子データの保管、利用およびその伝達によって生じるリスク」の意味で使用する。サイバーリスクには、外部からのサイバー攻撃やシステム上の不具合、従業員等の業務上のミス（ヒューマンエラー）等から生じる、企業が保有する情報の漏えいやサプライチェーンへの悪影響（相手先システムの損壊や営業停止等）による損害賠償責任の発生や信用の失墜、またそれらを要因とする売上の減少等の様々なリスクが含まれる。

[2] その後、データの重複を除いた結果、約679万人分に修正された。

[3] サイバーリスクを補償する保険である。詳細は後記4.(1)a.を参照願う。

[4] Allianz Global Corporate & Specialty, “A Guide to Cyber Risk” (2015.9)

[5] NAICについては後記5.(1)を参照願う。

[6] 山下潤「米国のサイバー・インシュアランスの動向」損保総研レポート第110号（損害保険事業総合研究所、2015.1）

２．サイバーリスクを巡る国内外の動向

本項では、ここ 1～2 年のサイバーリスクを巡る国内外の動向につき概観する。

（1）わが国におけるサイバーリスクを巡る動向

わが国でもサイバー被害は拡大しており、官民挙げてサイバーセキュリティ対策の取組が行われている。国内損害保険会社の多くがサイバー保険の販売を開始し、また、保険を含む金融業界において官民連携による情報共有が図られている。

a. サイバー被害の傾向（2015 年度）

わが国では、2015 年度の上半期には、日本年金機構を含め政府機関等への標的型攻撃[7]が多く確認された。下半期には、政府機関、重要インフラ事業者等への DDoS 攻撃[8]が多数みられ、Web サイトの閲覧障害が相次いだほか、インターネットバンキングに係る不正送金も被害額が拡大している。また、2016 年 2 月以降、ランサムウェア[9]の被害報告も増加傾向にある[10]。

b. サイバーセキュリティ対策の取組

わが国におけるサイバーセキュリティ強化のための主な動きは、図表 1 のとおりである。

図表 1　わが国におけるサイバーセキュリティ強化のための主な動き

時　期	内　容
2014 年 11 月	サイバーセキュリティ基本法が成立、一部施行
2015 年 1 月	サイバーセキュリティ基本法が完全施行
2015 年 2 月	経団連が「サイバーセキュリティ対策の強化に向けた提言」を公表
2015 年 7 月	金融庁が「金融分野におけるサイバーセキュリティ強化に向けた取り組み方針について」を公表
2015 年 9 月	政府がサイバーセキュリティ戦略を閣議決定
2015 年 12 月	経済産業省と情報処理推進機構（IPA）が「サイバーセキュリティ経営ガイドライン」を公表
2016 年 1 月	経団連が「サイバーセキュリティ対策の強化に向けた第二次提言」を公表
2016 年 4 月	サイバーセキュリティ基本法の一部を改正

（出典：各種資料をもとに作成）

---

[7] 特定の組織や情報を狙って、機密情報、知的財産および個人情報等を搾取またはシステムを破壊・妨害しようとする攻撃。電子メールを送りつけ、その添付ファイルやリンクを開かせ、マルウェア等を利用して攻撃する手口が多い。

[8] 分散型サービス不能攻撃（Distributed Denial of Service）の略称。大量のコンピュータが一斉に特定のサーバにデータを送信し、通信路やサーバの処理能力をあふれさせて機能を停止させるサイバー攻撃。

[9] 感染した PC をロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに金銭の支払いを要求する不正プログラム。身代金要求型不正プログラムとも呼ばれる。

[10] サイバーセキュリティ戦略本部「サイバーセキュリティ政策に係る年次報告（2015 年度）」（2016.6.13）

c. 国内大手損害保険会社によるサイバー保険の発売

2015 年は、国内大手損害保険会社によるサイバー保険の発売も広がった。2015 年 2 月には、東京海上日動火災保険社が、事業活動を取り巻くサイバーリスクを 1 契約で包括的に補償する総合保険[11]を発売した。三井住友海上火災保険社[12]およびあいおいニッセイ同和損害保険社[13]も、サイバー攻撃によるリスクを総合的に補償する保険を共同開発し、2015 年 9 月に販売を開始した。さらに、2015 年 10 月には、損害保険ジャパン日本興亜社が、サイバー攻撃に関するリスクを包括的に補償する新商品[14]の販売を開始した。

d. 金融 ISAC（アイザック）の活動

2014 年 8 月、高度化するサイバー攻撃への対策として、金融機関間でサイバーセキュリティに関する情報を共有するための組織として一般社団法人「金融 ISAC（アイザック）」が設立された。わが国の金融 ISAC は、米国の金融サービス ISAC（Financial Services Information Sharing and Analysis Center）[15]と呼ばれる組織をモデルとして創設された。

わが国の金融 ISAC の会員は、国内に事業拠点を持つ銀行、証券、生保、損保、クレジットカード事業者等である。2016 年 6 月 1 日時点での会員数は 237 社（準会員の 13 社を含む）であり、多くの保険会社がこの組織の会員となっている。

金融 ISAC は、会員間のメーリングリスト等を通じて、日々の被害や脆弱性情報等をリアルタイムに共有している。具体的には、公表することが難しい、標的型攻撃やフィッシング詐欺[16]、不正送金、DDoS 攻撃、ゼロデイ攻撃[17]等の手口や被害に関する情報を共有している。また、特定の重要課題について、テーマごとのワーキンググループを設け、会員共同で対策の検討等を行いながら、知見と対応力の向上を図っている。これらの成果はワークショップや年次総会等の場で共有している。

わが国の金融 ISAC は、国内の様々な組織と連携するとともに、米国の金融サービス ISAC とも連携し、情報共有を図っている。

（2）世界におけるサイバー被害と保険業界の懸念

サイバー被害は、世界的にも拡大、多様化する傾向にあり、サイバーリスクは、損

---

11 商品名は「サイバーリスク保険」である。
12 商品名は「サイバーセキュリティ総合補償プラン」である。
13 商品名は「サイバーセキュリティ保険（IT 業務賠償責任保険［拡張補償プラン］）」である。
14 商品名は「サイバー保険」である。
15 米国の金融サービス ISAC については後記 3.(2)a.(b)ｱ.を参照願う。
16 実在の金融機関やショッピングサイト等を装った電子メールを送信し、これらのホームページとそっくりの偽りのサイトに誘導し、銀行口座番号やクレジットカード番号、パスワード、暗証番号等の重要な情報を入力させて搾取する行為。
17 ソフトウェア等にセキュリティ上の脆弱性が発見されたときに、修正プログラムの提供等の対策が取られる前にその脆弱性を悪用して行われる攻撃。

害保険業界にとって最も重要な懸念事項の 1 つとして認識されるようになってきた。

a. 世界におけるサイバー被害の傾向（2015 年度）

2015 年度のサイバー被害の傾向について世界全体でみると、2015 年 4 月にフランスの国際放送局に対するサイバー攻撃によって番組の視聴障害が発生し、2015 年 12 月には、ウクライナでサイバー攻撃に起因する大規模停電が発生したように、各国の重要インフラに対するサイバー攻撃が注目を集めるようになった。また、下半期には、ランサムウェアの被害が多数発生しており、例えば、米国では病院等でランサムウェアに感染したことから、重要インフラサービスの提供に支障が生じた事例がみられたとされている[18]。

b. サイバーリスクに対する保険業界の懸念

プライスウォーターハウスクーパース（PricewaterhouseCoopers：以下「PwC」）による 2015 年のアンケート調査[19]において、サイバーリスクは、世界における損害保険業界が直面しているリスクの中で、自然災害リスク（第 2 位）や規制の変化（第 3 位）を抑えて、重要な懸念事項の第 1 位となった。サイバーリスクは、特にサイバー保険市場の成長への期待が大きい米国およびイギリスの損害保険業界において最も重要なリスクと捉えられている。なお、生命保険も含む世界の保険業界全体では、サイバーリスクは第 4 位となっている。

損害保険業界においてサイバーリスクが特に重要視されている背景には、同業界は、保険会社自身がサイバー被害を受けるリスクを抱えていることに加え、他の企業等のサイバーリスクを損害保険商品で引き受けていることの 2 つの側面[20]が挙げられている。

３．米国におけるサイバー被害とサイバーリスクに対する取組

本項では、米国におけるサイバー被害の現状と、サイバーリスクに対する政府および企業の取組等について概観する。

（1）サイバー被害の状況

米国におけるサイバー被害は近年急増しており、サイバーセキュリティ専門の調査会社である Ponemon Institute 社によれば、米国のほぼすべての企業がウィルスやマ

[18] サイバーセキュリティ戦略本部「サイバーセキュリティ政策に係る年次報告（2015 年度）」（2016.6.13）
[19] PwC が 2007 年から 2 年ごとに実施しているアンケート調査。PwC, “Insurance Banana Skins 2015, The CSFI survey of the risks facing insurers” (2015.7)
[20] 格付会社も損害保険会社の格付評価においてこの 2 つの側面を重視している（後記 5.(2)b.参照）。

ルウェア[21]によるサイバー攻撃を受けている。

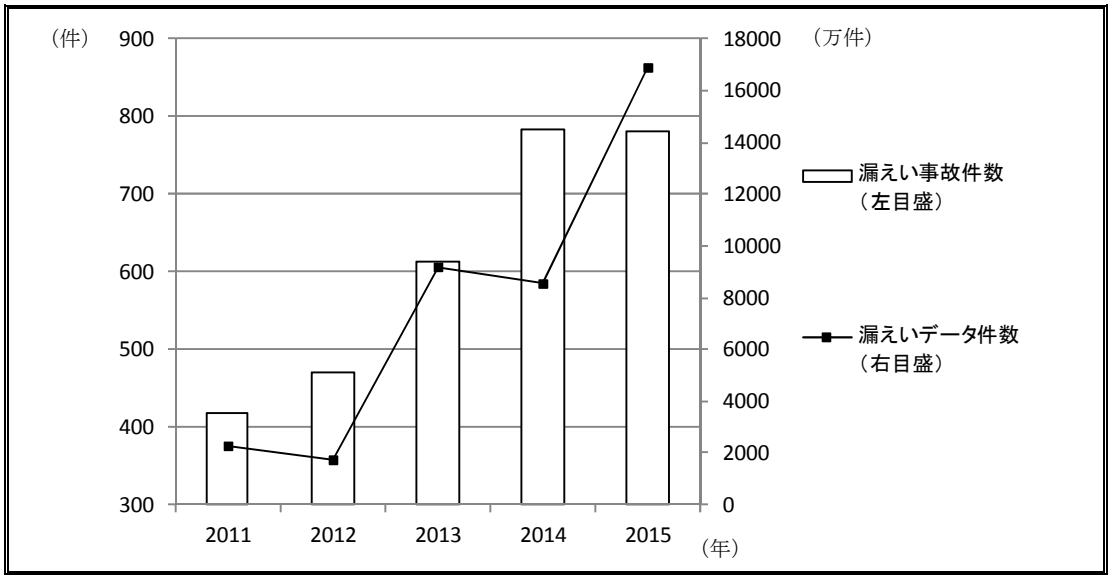
被害のタイプや原因等は多岐にわたるが、本項では、サイバーリスクの中でも米国で最も重要視されている個人情報漏えい被害の動向について説明する[22]。

a. 情報漏えい事故件数・漏えいデータ件数の推移

個人情報盗難リソースセンター（Identity Theft Resource Center：ITRC）[23]の統計[24]によれば、2015 年に公表された個人情報漏えい事故件数は 781 件となり、783 件で過去最多を記録した 2014 年とほぼ同水準であった。他方、2015 年に漏えいしたデータ件数は 1 億 6,907 万件となり、2014 年の 8,560 万件に比べほぼ 2 倍となった（図表 2 参照）。

ただし、この統計数値は氷山の一角に過ぎず、報告されていない被害や、被害を受けたことに気づいていないものも多数にのぼると考えられている。

図表 2　米国における個人情報漏えい事故件数および漏えいデータ件数の推移



（注）ITRC では、個人情報漏えいを氏名のほか、社会保障番号、免許証番号、医療記録、金融取引記録（クレジットカード・デビットカードを含む）のいずれかが流出したと公表された場合と定義している。例えば、2014 年 8 月に、7,600 万人分の個人の連絡先が流出したとされる JP モルガン・チェースは、金融取引情報等は流出していないと公表しているため、本統計には含まれていない。

（出典：ITRC, “Data Breach Reports” (2015.12.31)をもとに作成）

[21] 不正かつ有害な動作を行うソフトウェアの総称。

[22] 情報漏えいは、不正アクセス等のサイバー犯罪を原因とするものだけでなく、ヒューマンエラー等によるものも含んでいる。

[23] 個人の情報漏えい被害者を支援する非営利団体であり、2005 年からデータ侵害について調査を行っている。

[24] ITRC, “Data Breach Reports” (2015.12.31)

b. 業種別の特徴および主な事故の状況

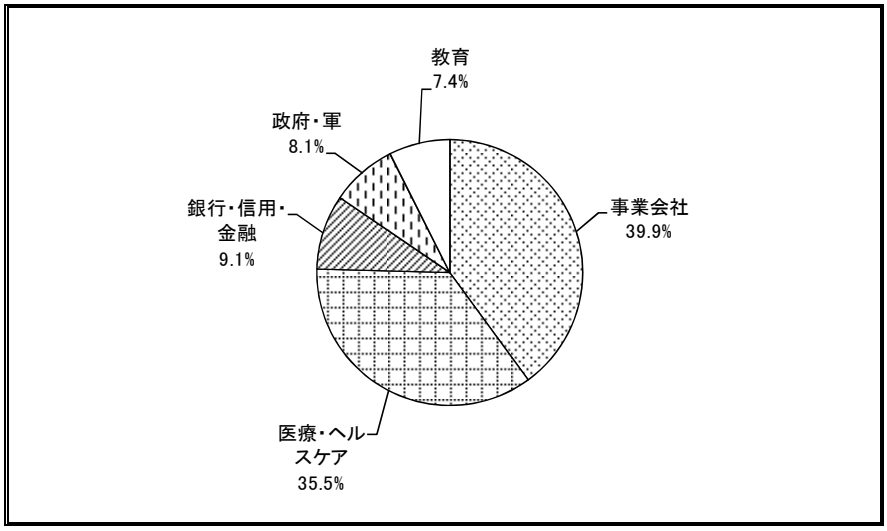
2015 年の事故件数 781 件の内訳を業種別にみると、事業会社（39.9%）、医療・ヘルスケア（35.5%）等で特に多い[25]ことがわかる（図表 3 参照）。

しかし、漏えいデータ件数が多いのは、医療・ヘルスケア、政府・軍等の結果となった。図表 4 は、2015 年の事故のうち、漏えいデータ件数が 100 万件以上となったものを示している。

2015 年 2 月には、医療保険のアンセム社（Anthem）[26]に対するサイバー攻撃により、過去の契約者の情報も含めて米国人口の 4 分の 1 に相当する 7,880 万人分の個人情報等が漏えいした。具体的には、氏名、生年月日、契約者 ID、社会保障番号、住所、電話番号、電子メールアドレス、勤務先情報等が漏えいしたとされている。同様に医療保険のプリメーラ・ブルー・クロス社（Premera Blue Cross）でも、顧客 1,100 万人分のデータが漏えいした。

2015 年 5 月には、米国連邦政府人事管理局（Office of Personnel Management : OPM）が 2 度にわたり別々のサイバー攻撃を受け、現職員や元職員を含む 2,570 万人分の記録が漏えいしている。

図表 3　個人情報漏えい事故の業種別構成（事故件数ベース）（2015 年）



（注）事故件数 781 件の構成割合

（出典：ITRC, “Data Breach Reports” (2015.12.31)をもとに作成）

[25] 総合的な医療保険情報を含む個人情報には、闇市場で 1 件あたり数百ﾄﾞﾙから 1000ﾄﾞﾙの価値がある。このため、攻撃者は医療関連のデータに狙いを定めているとされている（PwC「相互につながった世界におけるサイバーリスクマネジメント：グローバルセキュリティ調査 2015」）。

[26] アンセム社はインディアナ州を本拠地とし、3,700 万人の保険契約者を有する。

図表 4　100 万件以上のデータ漏えい事故（2015 年）

業種等	被害にあった企業等	漏えいデータ件数
医療・ヘルスケア	Anthem, Inc.	7,880 万
	Premera Blue Cross	1,100 万
	Excellus Blue Cross Blue Shield / Lifetime Healthcare	1,000 万
	UCLA Health	450 万
	Medical Informatics Engineering (MIE) / NoMoreClipbo	390 万
	Systema Software	150 万
	CareFirst BlueCross BlueShield	110 万
政府・軍	Office of Personnel Management（2 度にわたるサイバー攻撃による合計）	2,570 万
	Georgia Secretary of State	600 万
事業会社	T-Mobile / Experian	1,500 万
銀行・信用・金融	Scottrade	460 万

（出典：ITRC, “Data Breach Reports” (2015.12.31)をもとに作成）

c. 原因別の状況

2015 年の漏えい事故につき原因別にみると、ハッキングが 37.9%で調査開始以来の 9 年間のうち最も高い割合となった（2014 年は 29.5%）。次いで、従業員のミス・不注意 14.9%、電子メール・インターネットによる事故 13.7%などとなっている。

この調査結果からは、医療・ヘルスケア、政府・軍等の個人情報を狙ったハッキングが、データ漏えいの大きな被害を引き起こす傾向が強まっていることがうかがえる。

（2）サイバーリスクに対する取組の状況

米国では、わが国よりも早い時期から、政府および企業のサイバーリスクに対する取組が進められてきた。

a. 政府のサイバーリスク対策

米国では、サイバーリスク対策は、国家が直面する最も深刻な経済および安全保障上の課題の 1 つとされてきた。オバマ大統領は、2009 年の就任以降、サイバーセキュリティへの取組を積極的に推進し、直近では、サイバー脅威に関する情報共有等を進めるサイバーセキュリティ法案が 2015 年 12 月に成立した。それまでにも、何度かサイバーセキュリティ関連の法案が提案されてきたが、情報共有に伴うプライバシー侵害を懸念するプライバシー保護団体の反対等、様々な事情により廃案となることが多かった。このため、近年は通常の立法の制度を経ずに行政権を行使できる「大統領令（Executive Order）」を中心にサイバーセキュリティの強化が図られてきた[27]。

米国政府によるサイバーリスク対策は多岐に及ぶが、企業におけるサイバーリスク管理に関する特に重要な動きとして、本項では、企業がサイバーセキュリティ対策に

[27] PwC「諸外国の金融分野のサイバーセキュリティ対策に関する調査研究報告書」（2015.3.31）

活用できるNISTフレームワークの策定と、情報共有の拠点となる組織を巡る動きについて説明する。

(a) NISTフレームワークの策定

米国では、2013年2月に、重要インフラのサイバーセキュリティ強化を図るための大統領令（13636号）が発布され、これに基づき、2014年2月に、国立標準技術研究所（National Institute of Standards and Technology：NIST）[28]が、「重要インフラのサイバーセキュリティを強化するフレームワーク」（以下「NISTフレームワーク」）を策定した[29]。このフレームワークは、民間の重要インフラ企業に対し、サイバーリスクの管理に関するガイドラインを提供するものであり、企業による適用は任意とされた。

このフレームワークは、①サイバーリスク対策のベストプラクティス、参考情報等の提供、②企業がサイバーリスクを管理するために実施するプロセスの提示、③企業にとって期待される成果の提示、等の要素で構成されている。企業がこのフレームワークに沿ったリスク管理を実践することで、サイバーリスクの低減を図ることができるとされている。

現在、重要インフラ企業にとどまらず、多くの企業が、NISTフレームワークに基づき、サイバーセキュリティの向上を図っている。

(b) 情報共有の拠点となる組織を巡る動き

官民の情報共有の拠点としては、以前から情報共有分析センター（ISAC）が設置されており、2015年からは、さらに情報共有分析機関（ISAO）が加わることとなった。

ア．情報共有分析センター（ISAC）の活動

米国においてサイバーリスクに関する情報共有のための組織としては、1998年の大統領令（63号）の中で設置が推奨された、情報共有分析センター（Information Sharing and Analysis Center：ISAC）[30]が存在する。

ISACは、金融、エネルギー、ITといった業界ごとに分かれ、基本的に業界固有のサイバーセキュリティ情報を共有する仕組である。金融業界には、金融機関や保険会社等がメンバーとなっている金融サービスISACが設置されている[31]。金融サ

---

[28] 国立標準技術研究所（NIST）は、商務省傘下の機関であり、サイバーセキュリティに関する様々な規格、標準およびガイドラインの策定、ならびに研究開発、人材育成等を行っている。

[29] NISTが中心となり、産業界も協力して既存の国際標準等に依拠しながら開発した。

[30] ISACは、重要インフラ分野を攻撃から守るために情報共有・分析を行う組織であり、サイバーリスクだけでなく、物理的な脅威も活動の対象としている。

[31] 金融業界において重要インフラの保護を目的として活動する団体としては、金融サービスISACのほか、2002年に設立された金融サービス・セクター調整評議会（Financial Services Sector Coordinating

ービス ISAC は、1999 年に創設され、現在は約 7,000 社の金融機関や保険会社等が会員となっており、会員や国土安全保障省（DHS）[32]から提供される情報のほか、様々な情報源から独自に情報を収集し、分析したうえで会員に対し情報発信を行っている[33]。

イ．情報共有分析機関（ISAO）の創設

さらに、2015 年 2 月の大統領令（13691 号）により、産官学の幅広い分野にわたりサイバーセキュリティに関する情報共有と連携を促す観点から、情報共有分析機関（Information Sharing and Analysis Organization：ISAO）の創設が求められることとなった。ISAO は、金融、エネルギー等の各部門や地域ごとに組織を作り、政府と民間の情報共有の接点としての役割を担うもので、民間の事業会社や NPO など様々な組織形態が想定されている。

ISAO は、ISAC 以上に業種、地域、企業規模等の枠を越えて、相互の横断的な情報共有をより活発に行う仕組である。これにより、政府や民間企業から、より広範囲な情報が集まり、サイバーセキュリティに対する精度の高い多面的な情報解析が可能になるとされている[34]。

ISAO は、国土安全保障省（DHS）傘下の国家サイバーセキュリティ通信統合センター（National Cybersecurity and Communications Integration Center：NCCIC）[35]と連携して活動する。今後 ISAO において、情報共有の仕組の標準化も進めていく予定である。

ただし、ISAO については、他業界の企業から有益な情報を得られることに期待する企業がある一方、ISAO を通じて得られるメリットを実感できず様子見の企業もある。また、金融業界では、既に業界内で情報共有を進めている金融サービス ISAC があれば十分であり、複数の情報共有組織への参加は非効率になるとの見方もある[36]。

b. 企業のサイバーリスク対策

米国の企業は、データ漏えい等による被害の報道が増える中で、サイバーリスクに対する認識を高めるようになってきた[37, 38]。このため、企業は次のとおり様々なサイ

Council：FSSCC）等がある。FSSCC も、様々な政府機関や業界団体等と協力して活動している。

[32] 国土安全保障省は、連邦政府のネットワークや重要インフラのサイバーセキュリティに対する責任を有する機関である。

[33] 三菱総合研究所「米国のセキュリティ情報共有組織（ISAC）の状況と運用実態に関する調査」（2010.3）

[34] PwC「諸外国の金融分野のサイバーセキュリティ対策に関する調査研究報告書」（2015.3.31）

[35] 米国内のサイバーセキュリティに関する情報を集約するための組織として 2009 年 10 月に設立された。

[36] PwC「サイバーセキュリティの転換と変容：グローバル情報セキュリティ調査 2016」

[37] National Underwriter, “Eating it up” (2016.5)

[38] PwC「相互につながった世界におけるサイバーリスクマネジメント：グローバル情報セキュリティ調査 2015」

バーリスク対策を実行している。

○ 企業は先進的なサイバーセキュリティ技術を導入する等、情報セキュリティ支出を増やしている[39]。
○ 多くの企業が、NIST フレームワーク等のセキュリティ・フレームワーク[40]を採用するようになってきた。
○ 多くの企業が、同業他社や業界に関する情報共有分析センター（ISAC）と情報を共有するようになってきた。
○ 最高情報セキュリティ責任者（CISO）[41]や最高セキュリティ責任者（CSO）[42]等を任命し、これらの責任者が部門を越えた重大なリスク管理の問題としてサイバーセキュリティに取組み、企業全体で態勢を構築しようとする企業が増えている。
○ 取締役会がサイバーセキュリティ戦略に関与する企業が増えている。
○ 従業員に対するサイバーセキュリティ教育・研修の必要性につき認識する企業が増えている。

ただし、企業が上記のような様々な対策を効果的に行ったとしても、攻撃側も技術力を向上させ常に進化しているため、サイバー攻撃を完全に防ぐことはできない。そのため、多くの企業が、サイバー被害を受けた際の対応計画の策定等と合わせて、サイバー保険への加入または加入の検討を行っている[43]。

証券取引委員会（SEC）のコンプライアンス検査局（OCIE）のガイダンスでも、効果的なサイバーセキュリティ戦略の一環として、サイバー保険への加入が推奨されている。

４．米国におけるサイバー保険の動向

本項では、米国におけるサイバー保険について、サイバー保険の概要、市場の動向、保険金支払の動向の順に説明する。

---

[39] PwC「サイバーセキュリティの転換と変容：グローバル情報セキュリティ調査 2016」
[40] サイバーセキュリティのためのフレームワークには複数の種類があり、NIST フレームワークのほか、国際標準化機構（ISO）の情報セキュリティ管理システムの規格である ISO27001 等が主要なものとなっている。
[41] Chief Information Security Officer の略であり、組織における情報システムやネットワークのセキュリティ、機密情報や個人情報の管理等を統括する責任者。
[42] Chief Security Officer の略であり、組織におけるセキュリティを統括する責任者。
[43] Marsh & McLennan Companies, “The Role of Cyber Insurance in Risk Management” (2016.3.22)

（1）サイバー保険の概要

本項では、サイバー保険の商品の概要、引受時の評価、保険関連サービスについて説明する。

a. 商品の概要

従来型の企業向け保険では、基本的にはサイバーリスクは補償されない[44]。サイバーリスクの引受は、①サイバーリスク専用のサイバー保険、②E&O 保険[45]等の従来型の保険商品にサイバーリスクを補償する特約を付帯するもの、の 2 種類が主流となっている[46]。

サイバー保険[47]は、コンピュータ・ウィルスや不正アクセス、ヒューマンエラー等に起因して生じる損害を補償する保険であり、大別すると、第三者への損害賠償と、各種対応に要する自社の費用の 2 種類の損害に対する補償により構成される。

サイバー保険は、各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も異なる。主な補償内容としては次のものが挙げられる。

○　データ漏えい等に関する賠償費用

　データ漏えい等に伴い第三者に対して与えた損害に関し、これを賠償するための費用

○　データ修復費用

　データが損壊されたことに関する修復のための費用

○　顧客への通知、モニタリング等の費用

　データが漏えいした場合に、顧客等への通知を義務付けている州が多い。こうした通知の費用や、情報が漏えいした可能性のある顧客等のクレジット・モニタリング等にかかる費用

○　フォレンジック調査費用

　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フォレンジック（forensics）調査のための費用

---

44 A.M.ベスト社によれば、サイバーリスクに伴う賠償責任による保険金支払を想定していなかった企業総合賠償責任保険、事業中断保険および D&O 保険等の従来型の保険では、サイバー攻撃やデータ漏えいに伴う損害の一部が支払対象になる場合もあるが、保険金支払の対象になるかどうか明確でない部分もあり、長期間の訴訟に発展するケースもあった。保険会社は、保険契約者のニーズに応え、支払対象を明確化し、円滑な支払いを可能とするためにも、これら従来型の保険とは別の、サイバーリスクに明確に対処するサイバー保険を開発し発展させてきた。また近年では、保険会社は、従来型の保険には、サイバーリスクに関する損害を免責とする条項を加えるようになっている。

45 Errors and Omissions Insurance の略であり、過失怠慢賠償責任保険等と訳される。

46 National Underwriter, “Eating it up” (2016.5)

47 サイバーリスクを補償する保険商品の多くは、Cyber Insurance、Cyber and Privacy Insurance、Cyber Liability & Data Breach Insurance 等の名称で呼ばれているが、本稿では、これらを総称してサイバー保険と呼んでいる。

○　訴訟、罰金、恐喝

機密情報や知的財産の流出にかかわる訴訟費用、法律上の罰金、ランサムウェアによる恐喝に伴う費用等

○　事業中断に伴う損失

ネットワークやシステムの停止、事業中断等に伴う損失

上記のほか、企業の評判や信頼、ブランド等の失墜による損失等のレピュテーショナル・リスクまで補償の対象とする保険会社もあるが、このような保険会社はまだ少ない[48]。

なお、米国ではほとんどの州において、個人情報を含むデータ漏えいが生じた場合、その企業等に、データ漏えいにより影響を受ける可能性がある顧客等への通知を義務付ける「データ漏えい通知法」が制定されている。このような規制や、実際にデータ漏えいの被害が多く発生していることなどを背景として、データ漏えいに伴う損害への企業の関心は高く、米国のサイバー保険では、データ漏えい時の損害に対する補償に重点が置かれている。

b. サイバー保険引受時の評価

保険会社は、サイバー保険の引受に際し、その企業のサイバーリスクについて評価する。通常は、業種、事業内容、企業規模ごとにリスクを分析し評価している。情報が漏えいした場合の被害の大きさも重視しており、被害発生時に影響が大きい、病院やヘルスケア業界の医療関連の個人情報や小売業界のクレジットカード情報等には特に大きな注意を払っている。

保険ブローカー大手のマーシュ[49]によれば、保険会社は、サイバー保険の引受プロセスにおいて、その企業の技術的な防御力、被害発生の際の対応計画、ソフトウェアの修正の手続き、データやシステムへのアクセス制限の方針等を保険会社が精査する。さらに、高度なカスタマイズ商品を提供する場合は、その企業においてセンシティブ情報の暗号化が確実かどうか、プライバシーに関する文化が構築されているか、従業員は自身の責任について理解しているか等の要素も確認する。

多くの保険会社は、各企業のサイバーリスクを評価するための指標として、NISTフレームワーク（前記3.(2)a.(a)参照）を活用している。これは、国土安全保障省（DHS）の支援もあり、企業がNISTフレームワークを積極的に導入しているためである。

保険会社は、その企業のサイバーリスクに応じた保険料を提示しており、こうした保険会社のプライシングは、保険料を節約したい企業にとって、サイバーリスクに対する管理の高度化やリスクの低減を図るための重要なインセンティブとなる。また企

[48] PwC「サイバーセキュリティの転換と変容：グローバル情報セキュリティ調査2016」
[49] Marsh & McLennan Companies, “The Role of Cyber Insurance in Risk Management” (2016.3.22)

業は、サイバー保険に加入することで損失の補償に加え、保険会社による引受時の評価を通じて、自社の態勢を把握し、サイバー犯罪が発生した場合の法的リスク、対応コスト、ブランドが受けるダメージ等の予測が可能になるとされている。

c. 保険関連サービス

保険会社は、サイバー保険の引受のほか、企業に対しサイバーリスク管理のアドバイス等のサービスも提供している。例えば、保険会社は、政府やベンダー等からセキュリティ関連の最新情報を入手し、企業に情報提供やアドバイス等を行っている。

また、保険会社はサイバー保険に加入している企業に対し、被害を受けた際の対応をサポートしている。例えば、データ侵害に関しては、ほとんどのサイバー保険で、どんな顧客情報が危険にさらされている可能性があるかなどを調べるためのフォレンジック調査、企業の責任に関する法的な分析、各個人への通知、信用モニタリング、データ回復措置等を含め、企業が対応するための支援サービスを提供している。

企業は、被害を受けた際に適切な対応を取ることができれば、データ漏えいから生じる総コストを削減できるだけでなく、訴訟や規制監督当局による調査等から生じる可能性のある問題の多くを回避することができる。保険会社によるこれらのサービスは、自社のリソースが不足している中小企業にとって特に役立つものである[50]。

（2）サイバー保険市場の動向

本項では、サイバー保険市場の規模、引受を行っている保険会社、企業の加入状況等について説明する。

a. サイバー保険市場の規模

サイバー保険市場の規模については、正確な統計データがなく、また関係組織等による将来予測にも幅がある。PwC のレポート[51]では、世界全体でのサイバー保険の収入保険料は、2015 年は 25 億ﾄﾞﾙと推計しており、2020 年には 75 億ﾄﾞﾙになると予測されている。

これらの数値とは異なるが、米国におけるサイバー保険の保険料規模は、2014 年 20 億ﾄﾞﾙ、2015 年 27 億ﾄﾞﾙ[52]との推計があり、現時点では、米国の企業向け損害保険全体の 1%程度[53]であると考えられる。米国のサイバー保険市場はここ数年、年 25%～50%増のペースで急拡大しており、2020 年には 80 億ﾄﾞﾙになるとの予測もある[54]。

---

[50] Marsh & McLennan Companies, “The Role of Cyber Insurance in Risk Management” (2016.3.22)
[51] PwC, “Insurance 2020 & beyond: Reaping the dividends of cyber resilience” (2015.9)
[52] Betterley Risk Consultants, “Cyber/Privacy Insurance Market Survey 2016” (2016.6)
[53] 2014 年の企業向け損害保険の正味収入保険料は 2,413 億ﾄﾞﾙである（Insurance Information Institute, “The Insurance Fact Book 2016”）。
[54] Munich Re, “Cyber Risks in Italian market” (2014)

b. 引受を行っている保険会社

米国でサイバー保険の引受を行っている保険会社は 60 社以上あるが、特に AIG、ACE[55]、Chubb、Zurich Insurance、Beazley Group 等が中心となって市場を先導している[56]。サイバー保険は、サイバーリスクの変化が早く、損害の予測が難しい。また、データが少なく、確率モデルの構築や適正な保険料の算出も難しいなどの特徴がある。このため、保険会社の引受スタンスは、契約者ごとの支払限度額を低めに設定したり、免責事項を多く設定するなど、保守的になる場合が多い。

c. 企業の加入状況

リスク保険マネジメント協会（Risk and Insurance Management Society : RIMS）[57]が会員企業のうちの 284 社を対象として行ったアンケート調査[58]によれば、専用のサイバー保険に加入している企業は、回答した企業全体の 51%であった[59]。また、専用のサイバー保険に加入していないと回答した企業のうちの 34%が、他の保険によりサイバーリスクが補償対象となっていると回答した。サイバーリスクの補償を含む他の保険としては、E&O 保険、企業総合賠償責任保険、財産保険等が回答として挙げられている。サイバーリスクを補償する保険に加入していないと回答した企業については、この 74%が今後 1～2 年以内に保険加入を検討すると回答している。

サイバー保険の支払限度額は、500 万ﾄﾞﾙ未満が 23%、500 万ﾄﾞﾙから 2,000 万ﾄﾞﾙ未満が 35%であり、全体の 58%が 2,000 万ﾄﾞﾙ未満となっている[60]（図表 5 参照）。

また、年間の保険料は、5 万ﾄﾞﾙ未満が 27%を占めた一方、10 万ﾄﾞﾙ以上が 55%となっている（図表 6 参照）。

---

[55] ACE は 2016 年 1 月に Chubb の買収を完了し、世界すべてのグループ会社の社名を、買収された側の Chubb に統一することとした。

[56] National Underwriter, “Eating it up” (2016.5)

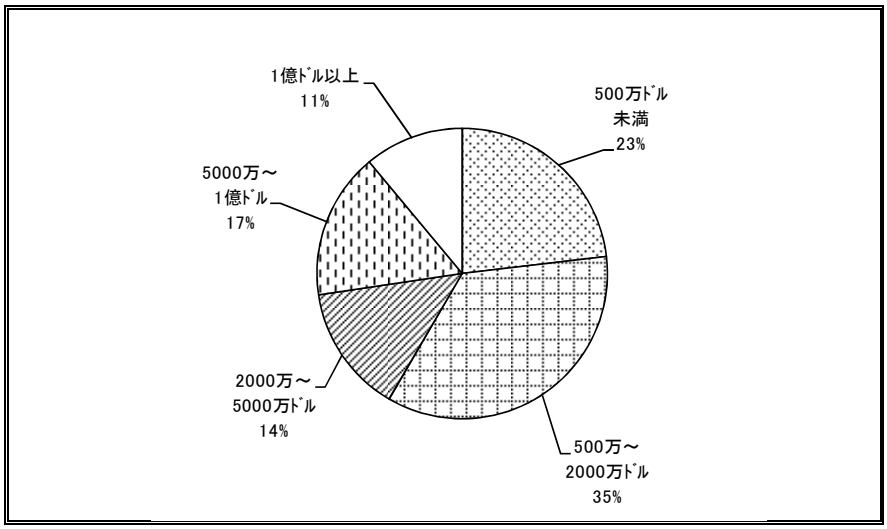
[57] RIMS は、本部をニューヨークに置き、米国およびカナダを中心に、全世界に 9,000 人以上のリスクマネジメントのプロフェッショナルを会員として擁する、世界最大のリスクマネジメント団体である。

[58] RIMS, “Cyber Survey” (2015.5)

[59] サイバー保険への企業の加入割合は、調査によって幅がある。例えば、米国の保険代理店・ブローカー協議会の調査によれば、保険代理店やブローカーの顧客企業のうち、何らかのサイバーリスクの補償を有している企業の割合は 25%程度とされている（The Council of Insurance Agents & Brokers, “Cyber Insurance Market Watch Survey” (2016.4)）。

[60] 上記の保険代理店・ブローカー協議会の調査によれば、サイバー保険の支払限度額は 300 万ﾄﾞﾙ程度に設定されることが多いとされている。

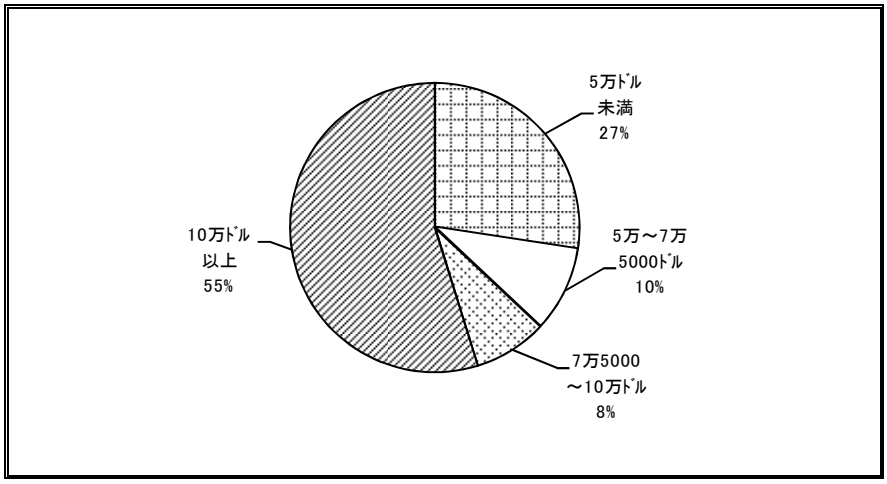
図表 5　サイバー保険の支払限度額



（注）回答した 148 社の構成割合

（出典：RIMS, “Cyber Survey” (2015.5)をもとに作成）

図表 6　サイバー保険の保険料（年間）



（注）回答した 135 社の構成割合

（出典：RIMS, “Cyber Survey” (2015.5)をもとに作成）

d. サイバー保険に対する企業ニーズの変化

企業は、総じて規模や業種にかかわらず、自社のサイバーリスクへの関心を高めている[61]。

ここ 1～2 年の主な変化としては次の傾向が挙げられる。

[61] National Underwriter, “Eating it up” (2016.5)

○　すべての業種への広がり

2～3 年前は、金融サービスやヘルスケアのように規制が厳しい業界からの需要が中心だったが、直年では、多くの顧客情報を保有する小売業からの需要が増え、さらに、製造業や不動産業、法律事務所に至るまで、すべての業種において、サイバー保険への加入が進んできている。企業のサイバー保険に対する認識は向上しており、例えば、製造業は、サイバー被害を受けた際の事業中断に伴う損失に対する補償に興味を示している[62]。

○　中小企業への広がり

以前は、収入が 1 億ﾄﾞﾙ未満の中小企業はサイバー攻撃の被害にあうことは少ないと考える傾向があったが、近年は自社のサイバーリスクとサイバー保険の必要性に対する認識が向上し、サイバー保険への加入を検討する中小企業が増えている。

○　支払限度額の引上げ

既にサイバー保険に加入している企業の多くが、更新時に支払限度額の引上げを求めている[63]。

e. サイバー保険の保険料率の動向

サイバー保険全体でみると、2015 年から 2016 年前半における保険料率は、総じて堅調に推移している。しかし、保険料率は、業種や企業規模等によって大きく異なっており、また変化の方向性にも多少の違いがある。

大量の個人情報を保有している大企業やヘルスケア、金融サービス等のリスクが大きい企業では、料率が上昇しているケースが多い。一方、中小企業等の支払限度額が低く比較的単純なリスクの引受については、市場競争が激しくなっているため、料率はわずかながら低下傾向にあるとされている[64]。

f. サイバー保険の課題

サイバー保険の主な課題として、ここでは以下のような点を取り上げる。データの不足によりリスクの定量化が難しいことから、リスクの出し手である企業のニーズと、受け手である保険会社との間にミスマッチが生じやすいことに起因する問題が多い。

○　補償範囲と支払限度額の決定

サイバー保険への加入は、企業規模や業種、扱っているデータの種類、リスク

---

62 電力や製造業のように、保有データ量は少なくても、ネットワークの機能停止により巨大な損害を被るリスクを抱える産業での加入が急増しているとの見方もある（Marsh & McLennan Companies, “The Role of Cyber Insurance in Risk Management” (2016.3.22)）。

63 Aspen Insurance のサイバー保険の責任者によれば、1,000 万ﾄﾞﾙの支払限度額の保険を購入した企業は 3,000 万ﾄﾞﾙの支払限度額の補償を、5,000 万ﾄﾞﾙの補償を購入した企業は 1 億ﾄﾞﾙの補償を求めている。

64 The Council of Insurance Agents & Brokers, “Cyber Insurance Market Watch Survey” (2016.4)

管理の成熟度等によって必要な補償範囲や支払限度額が企業ごとに異なる。企業にとっては、この判断が難しい[65]。

○　支払限度額の引上げへの対応

大企業が自社のリスクに見合うよう支払限度額の引上げを希望しても、保険会社がこれに応じられない場合がある。特に小売業界の大企業は、巨額のリスクに見合う支払限度額の補償を得られていないとの見方が多い。巨大企業のリスクに対応する 10 億ﾄﾞﾙ規模の補償を提供する保険はまだ存在しない。

○　物理的損害や身体的傷害に対する補償

前記 2.(2)a.のとおり、2015 年 12 月の厳冬期に生じたウクライナの発電所に対するサイバー攻撃は、財産損壊や人身傷害による巨額の損害が生じる可能性があることを想起させた。エネルギー、製造、交通業界等の企業にとって、サイバー攻撃が、物理的損害や人身傷害を引き起こすリスクは大きい。これらの補償を含む保険引受を行っている保険会社も一部あるものの、まだ少ない。

○　ソーシャルエンジニアリング攻撃[66]に対する補償

ソーシャルエンジニアリング攻撃も、企業にとって大きな懸念事項となっている。この攻撃による損失に対する補償を提供している保険会社もあるものの、まだ少ない。

○　補償範囲が不明確との懸念

保険会社は、約款の各条項で補償範囲を明確に定める取組を進めているが、サイバーリスクは変化が早いため、すべてを明確に規定することが難しく、実際に被害を受けた際に、個別の費用が補償の対象となるのかどうか不安視している企業も多い。このため、企業がサイバーリスクに伴う損害を確実にカバーできるよう、保険会社はサイバーリスクを現状よりもさらに包括的にパッケージ化したサイバー保険を提供すべきとの声もある。

○　再保険等によるリスク移転

サイバーリスクの引受は、再保険会社にとっても、データの不足からリスクを的確に評価することが難しく、またサイバーリスクの性質上、再保険会社にリスクの集積の問題も生じやすい。このため、今後サイバー保険市場が急成長したときに、元受保険会社が適正な再保険料で再保険を利用してリスクの分散を図ることが難しくなる可能性が考えられる。

なお、調査会社である SANS Institute の調査[67]によれば、リスクの出し手である企

---

[65] PwC「サイバーセキュリティの転換と変容：グローバル情報セキュリティ調査 2016」

[66] ソーシャルエンジニアリングとは、コンピュータやネットワークの管理者や利用者等から、パスワードなどの保安上重要な情報を、情報通信技術を使用せず、人間の心理的な隙や行動のミスにつけ込んで盗み出す方法であり、例えば、巧みな話術による誘導や盗み聞き、盗み見等の手段が該当する。

[67] SANS Institute, “Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey” (2016.6)

業と受け手である保険会社との間には、使われている専門用語の定義が異なり、またリスク対策のフレームワークやモデルに対する評価の考え方も異なるなどのギャップがある。このため、共通言語によるコミュニケーションの土台が構築されていない。例えば、サイバー保険の補償条項や免責条項につき企業側が正しく理解するには、経験を積んだ法律の専門家のサポートが必要となるなど、困難が伴う場合がある。

今後、さらに多くの企業がサイバー保険によるリスク移転を進めるためには、企業のサイバーリスクをできるだけ定量化して一般的な財務用語で把握するなど、企業側および保険会社側のすべての関係者が理解できる共通言語でのコミュニケーションを促進することが必要とされている。

g. サイバー保険の引受を行う保険会社の強み

サイバー保険の引受を行っている保険会社の強みの 1 つは、保険の収支や保険金支払の実績に関するデータを蓄積できることに加え、引受プロセスによって、その加入企業におけるサイバーリスクの脅威、脆弱性、損害の可能性等に関するデータも蓄積できることである。実際、サイバー保険の引受を行っている保険会社は、サイバーリスクの傾向や、損害額に応じたベストプラクティス等に関する分析を主導している。さらに、政府や業界内外の企業等と情報共有することによって、データの分析を深めることができる[68]。

(3) サイバー保険における保険金支払の動向

サイバー保険における保険金支払の全体を示すデータの入手は困難であり、本項では、米国で最も重視されているデータ漏えいに伴う保険金支払に関する調査についてこの概要を紹介する。

ネット・デリジェンス（NetDiligence）社[69]のサンプル調査[70]によれば、2015 年におけるサイバー保険の保険金請求件数は 160 件であった。

160 件のうち保険金支払いが確認された 112 件の支払保険金の総額は 7,550 万ﾄﾞﾙとなった（2014 年の調査では 145 件の保険金請求につき、支払保険金の総額は 8,400 万ﾄﾞﾙであった)。2015 年の 1 件あたりの平均支払額は約 67 万ﾄﾞﾙであった。

---

[68] Marsh & McLennan Companies, “The Role of Cyber Insurance in Risk Management” (2016.3.22)

[69] NetDiligence 社は、サイバーリスクの評価やデータ侵害に関する情報の提供等を行うサービス会社である。

[70] NetDiligence, “2015 Cyber Claims Study”. サイバー保険の引受を行っている多くの保険会社がこの調査に参加している。AIG、ACE、Chubb、Zurich、Beazley を含む主要 19 社において、同期間中に保険金請求がなされた 160 件に関する調査を実施したものである。この調査における支払保険金のデータは、まだ支払総額が確定しておらず、調査時点までの金額を示している。同社によれば、このサンプリング調査は、同時期におけるサイバー被害件数全体の 5%程度に相当すると推計している。なお、本調査における支払保険金は、契約者の免責部分も含めた総額で示されている。

a. 漏えいデータ件数と支払保険金

1 事故あたりの漏えいデータ件数と、漏えいデータ 1 件あたりの保険金支払額については、次の結果となった。

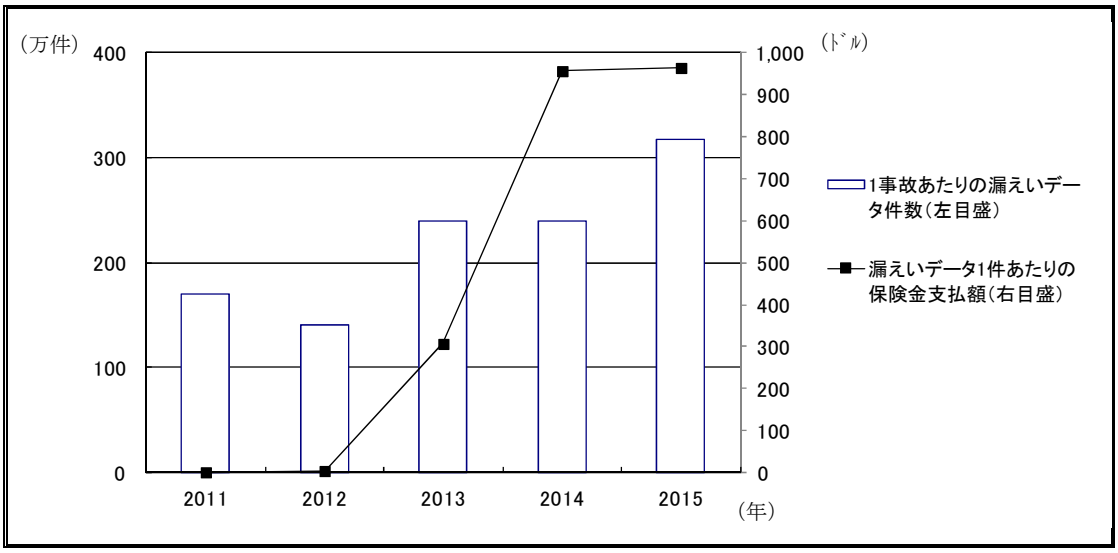
○　1 事故あたりの漏えいデータ件数

2015 年の 1 事故あたりの漏えいデータ件数は約 317 万件であり、2011 年以降で最大となった。図表 7 のとおり、近年増加傾向で推移している。ただし、2015 年の中央値は、平均値に比べて非常に少ない 2,300 件に過ぎず、平均値は、件数の多い事故の影響で統計上引き上げられているが、中央値は、比較的少ない件数のデータ漏えい事故も多数発生していることを示している。

○　漏えいデータ 1 件あたりの保険金支払額

2015 年の漏えいデータ 1 件あたりの保険金支払額は 964ﾄﾞﾙとなっている。前年とほぼ同水準にとどまったものの（2014 年は 956ﾄﾞﾙ）、数年単位でみれば拡大傾向にある（図表 7 参照）。

図表 7　1 事故あたりの漏えいデータ件数と、漏えいデータ 1 件あたりの保険金支払額



（出典：NetDiligence, “2015 Cyber Claims Study” をもとに作成）

b. 保険金支払額の内訳

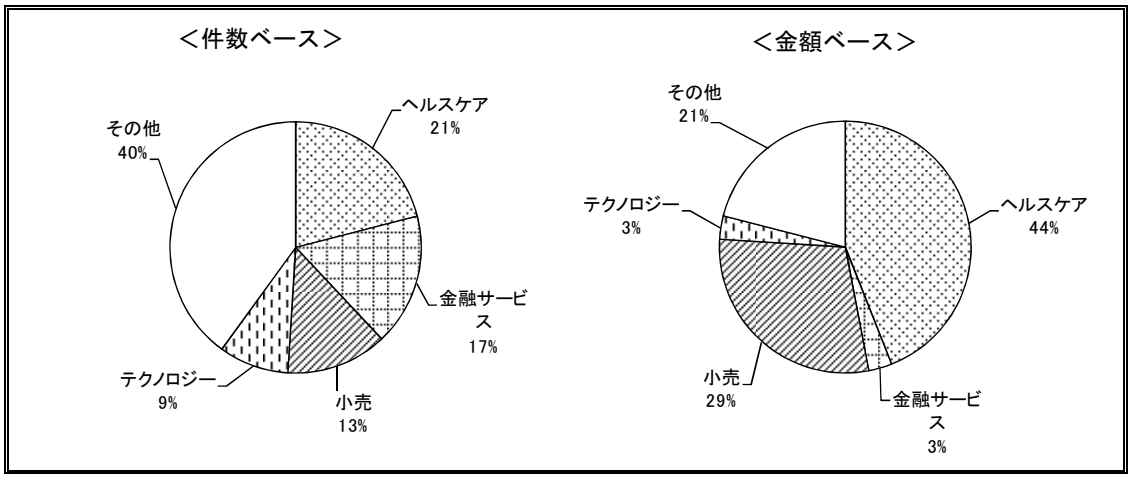
2015 年の支払保険金総額 7,550 万ﾄﾞﾙの内訳は、78%が危機対応サービス（フォレンジック調査、顧客への通知、コールセンター対応、データ保護サービス等の費用）、17%が法的解決または法的防御のための費用等となっている。

本項では、さらに 2015 年の保険金請求および保険金支払につき、業種別、企業の収入規模別、損害の原因別に紹介する。

（a）業種別

保険金請求件数160件の業種別内訳につき件数ベースでみると、ヘルスケア21%、金融サービス 17%、小売 13%等が上位を占めている（図表 8 参照）。一方、保険金の金額ベースでみると、ヘルスケア 44%、小売 29%の割合が高く、金融サービスは3%にとどまった。金額ベースでヘルスケアと小売の割合が高くなったのは、両業界ではハッカーやマルウェア・ウィルスの攻撃により、大きな被害が何件か発生したためである。

図表 8　保険金の内訳（業種別）



（注）件数ベースは保険金請求 160 件に対する割合。金額ベースは、保険金支払 112 件に対する割合。

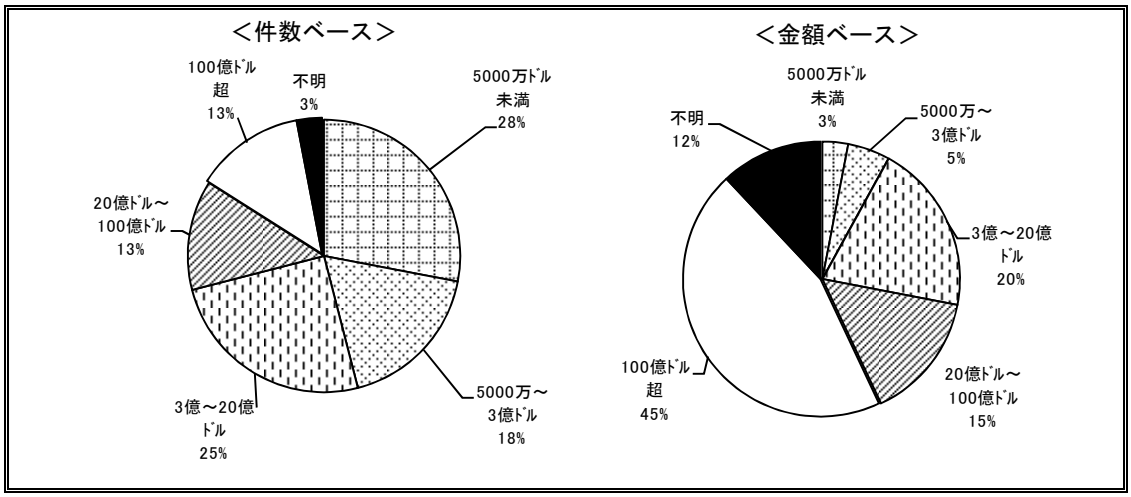
（出典：NetDiligence, “2015 Cyber Claims Study” をもとに作成）

（b）企業の収入規模別

保険金請求につき企業の収入規模別に件数ベースでみると、5,000 万ﾄﾞﾙ未満が28%となり、これを含め全体の 71%が 20 億ﾄﾞﾙ未満となっている（図表 9 参照）。ネット・デリジェンス社は、このように中小企業の割合が高くなった要因として、企業の総数自体において大企業よりも中小企業の方が多いことに加え、中小企業の方がサイバーリスクに対する認識が低く、また適正なデータ保護や従業員に対する研修を実現するためのリソースに乏しいため、大企業に比べサイバーリスク対策が進んでいないことなどが推測されるとしている。

保険金の金額ベースでは、収入規模 100 億ﾄﾞﾙ超の大企業が 45%を占めた。件数ベースで71%を占めた20億ﾄﾞﾙ未満の中小企業は金額ベースでは28%にとどまっている。これには、企業の収入規模が大きくなるにつれ、1 件あたりの保険金支払額も大きくなる傾向が反映されている。

図表 9　保険金の内訳（企業の収入規模別）



（注）件数ベースは保険金請求 160 件に対する割合。金額ベースは、保険金支払 112 件に対する割合。

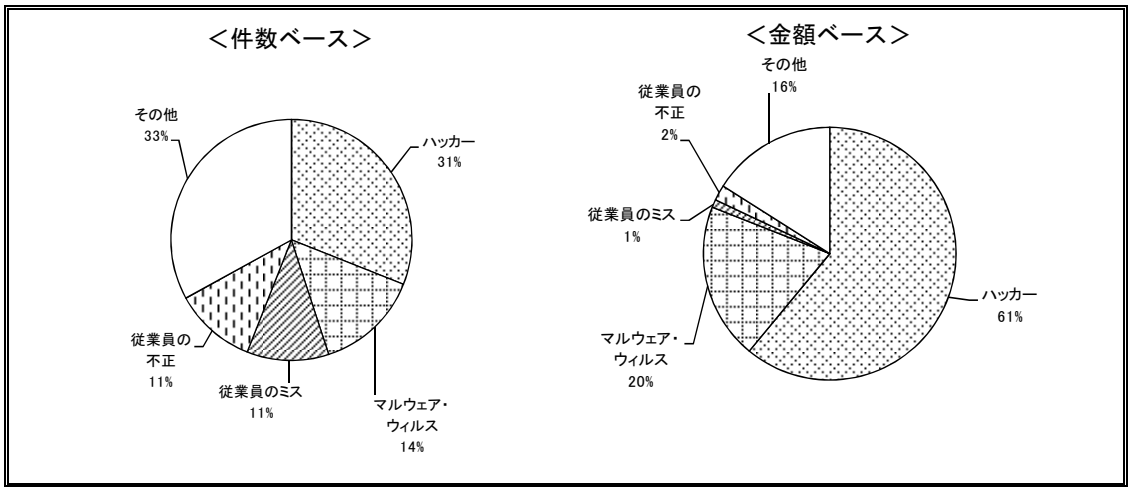
（出典：NetDiligence, “2015 Cyber Claims Study” をもとに作成）

（c）損害の原因別

保険金請求につき損害の原因別に件数ベースでみると、ハッカー31%、マルウェア・ウィルス 14%、従業員のミス 11%、従業員の不正 11%等となっている（図表 10 参照）。

しかし、保険金の金額ベースでみると、ハッカー61%、マルウェア・ウィルス 20%、の両者で全体の 81%を占めている。従業員等によるミスや不正よりも、ハッカー等の悪意をもった外部からの攻撃による被害が大きかったことがわかる。

図表 10　保険金の内訳（損害の原因別）



（注）件数ベースは保険金請求 160 件に対する割合。金額ベースは、保険金支払 112 件に対する割合。

（出典：NetDiligence, “2015 Cyber Claims Study” をもとに作成）

c. その他の特徴

上記のほか、本調査では次のような特徴が、ネット・デリジェンス社によって指摘されている。

○ ほとんどの保険金支払には、被害を受けた企業自身および第三者への賠償責任の両方の損害が含まれている。
○ モバイル機器には脆弱性があるものの、現時点では、サイバー攻撃において優先的に利用される手段とはなっていない。
○ 漏えいデータ件数と保険金支払額との間には明確な関係を見いだせなかった。したがって、漏えいデータ１件あたりの損害を基準として総損害額（＝保険金支払額）を推計する単純なモデルではミスリーディングとなる可能性がある。

さらに、漏えいデータ件数と総損害額との関係に関しては、顧客への通知等のように漏えいデータ件数と直接関連する費用、規制上の罰金等のように間接的に関連する費用のほか、フォレンジック調査のように、漏えいデータ件数と明確な関連性のない費用もある。このため、漏えいデータ件数は、損害を表すモデルの構築に関し、損害の一部を説明できるに過ぎない。今後データが多く集まり、分析が精緻化されることによって、他の変数も解明され、モデルが改善すると見込まれるとしている。

５．NAIC の取組と保険会社の健全性への影響

本項では、全米保険庁長官会議（NAIC）[71]におけるサイバーリスクに関する保険契約者保護のための取組、ならびに保険会社自身のサイバーリスクおよびサイバー保険の引受に伴う保険会社の健全性への影響について説明する。

（1）NAIC の取組

米国各州の保険規制当局は、保険会社や保険仲介者等が保険契約者や保険金請求者等から提供された個人データを保護する役割も担っている。NAIC は各州の保険規制当局がこのような業務を円滑に進めることができるよう、様々な取組を行っている。

a. アンセム社のデータ漏えい後の NAIC と州保険規制当局の対応

NAIC は 2015 年 2 月のアンセム社のデータ漏えい（前記 3.(1)b.参照）後、消費者に対し、個人情報の流出被害につき格別の注意を払うよう呼び掛けた[72]。また、州保険規制当局に対し、アンセム社およびその関連会社の検査を実施するよう求めた。さ

[71] NAIC は、各州の保険庁長官によって構成される組織であり、直接的な監督権限は持たないが、各州の保険規制・監督の均質化・調和化を図るための取組を行っている。
[72] NAIC のニュースリリース（2015.2.6）による。

らに、州保険規制当局は消費者に対し、クレジット・ビューロー[73]が提供する消費者報告[74]を注意深く確認することも奨励している。

b. サイバー保険の引受に関するモニタリング

2016 年より、保険会社が NAIC に提出する年次報告書に、サイバー保険の引受状況も記載することが義務付けられた。具体的には、サイバー保険引受による元受計上保険料、元受既経過保険料、損害調査費用を含む保険金支払額に関する情報、残存契約件数、保険金支払件数等の情報を記載することが求められている。

この情報収集の狙いは、保険会社によるサイバー保険の引受が円滑に進むように、保険規制当局が、サイバー保険市場の規模や成長性、保険金支払や収益性の状況をモニターするのに役立てることにある。また、この情報収集は、保険会社がサイバー保険の引受に伴い、万が一、巨額な保険金支払が生じ、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、保険規制当局が監視するためのものでもある。

c. サイバーセキュリティ作業部会の設置とガイダンス等の策定

NAIC は、2014 年 11 月にサイバーセキュリティ作業部会（Cybersecurity Task Force）を設置し、保険会社自身のサイバーセキュリティ対策等について本格的に検討を開始した。検討の結果、2015 年 4 月に「効果的なサイバーセキュリティのための原則：保険規制ガイダンス」が、2015 年 12 月に「サイバーセキュリティ消費者保護のためのロードマップ」が採択された。本項では、これらの概要について説明する。

（a）効果的なサイバーセキュリティのための原則：保険規制ガイダンス

このガイダンスは、保険会社や保険仲介者が保有する消費者の個人情報を保護するために必要な原則を示すものであり、また、保険規制当局のためのガイダンスでもある。保険業界や保険規制当局が、リスクの特定、実務的な解決策、必要な情報へのアクセス等につきどのように取り組むべきかを示している。

例えば、サイバーセキュリティを保険会社の ERM の中に取り込み、取締役会でも監視することが取り上げられている（原則 9 および 10）。また、情報共有分析機関（ISAO）[75]に参加することの重要性（原則 11）や従業員研修の重要性（原則 12）も示されている（図表 11 参照）。

---

[73] クレジット・ビューローとは、消費者信用情報を直接収集しているエキファックス、エクスペリアン、トランスユニオンの 3 社を意味する。クレジット・ビューローは、収集した消費者信用情報（「消費者報告」と呼ばれる）を金融機関や企業等に広く販売しており、この消費者報告は、金融機関の与信判断のほか、保険の引受、企業の雇用判断等の用途で利用されている。

[74] 消費者報告は、個人信用情報の利用等について規定する公正信用報告法により、「消費者の信用度、一般的評判、個人の特性等に関する情報であり、与信、保険の引受または雇用の妥当性等を判断するために収集・利用される情報」と定義されている。消費者報告については、後掲図表 12 も参照願う。

[75] ISAO については、前記 3.(2)a.(b)ｲ.を参照願う。

図表 11　効果的なサイバーセキュリティのための原則：保険規制ガイダンス

原　則	概　要
原則 1	・州保険規制当局は、保険会社、保険仲介者および他の規制対象組織が保有する個人を特定できる消費者情報をサイバーリスクから保護する責任を有する。 ・州保険規制当局は、データ漏えい等の被害が生じたときに最適なタイミングで消費者に警告を発するシステムを、保険会社、保険仲介者および他の規制対象組織が維持するように働きかける必要がある。 ・州保険規制当局は、保険会社、保険仲介者、連邦政府等と、一貫した整合的なアプローチの確立に協力する必要がある。
原則 2	・保険会社、保険仲介者および他の規制対象組織のネットワークの内外で収集、蓄積、移転される機密情報や、個人が特定できる消費者情報は、適正に保護されるべきである。
原則 3	・州保険規制当局は、州保険規制当局や NAIC の内外で収集、蓄積、移転される情報を保護する責任を有する。 ・この情報には、個人を特定できる消費者情報のほか、保険会社や保険仲介者の機密情報も含まれる。
原則 4	・保険会社や保険仲介者のためのガイダンスは、柔軟かつ実務的で、NIST フレームワーク等の国家的に進められている取組と整合的でなければならない。
原則 5	・ガイダンスは、リスクベースで、保険会社や保険仲介者のリソースを考慮したものでなければならない。 ・ガイダンスは、インターネットや他の公的ネットワークと接続しているすべての保険会社や保険仲介者にとって最低限必要なサイバーセキュリティ基準を備える必要があることを示すものでなければならない。
原則 6	・州保険規制当局は、適正な監督を行う必要があり、この監督には、サイバーセキュリティに関するリスクベースの財務検査や市場行為検査も含まれる。
原則 7	・保険会社、保険仲介者および他の規制対象組織、ならびに州保険規制当局における危機対応計画の策定は、効果的なサイバーセキュリティ・プログラムの重要な構成要素の１つである。
原則 8	・保険会社、保険仲介者および他の規制対象組織、ならびに州保険規制当局は、第三者やサービス・プロバイダーが個人を特定できる情報の保護を実現できるよう、適正な対策を取る必要がある。
原則 9	・サイバーリスクは、保険会社や保険仲介者の ERM プロセスの一部として組み込まれ、取り扱われる必要がある。 ・サイバーセキュリティは、IT 部門だけでなく、その組織の全体を包含するものでなければならない。
原則 10	・その保険会社にとって重大なリスクを提示する IT 内部監査で明らかになった事項は、取締役会またはその傘下の適切な委員会で審議する必要がある。
原則 11	・保険会社や保険仲介者にとって、情報を共有し、既存の脅威だけでなく、新たに生じる脅威や脆弱性について知識を維持するために ISAO の利用が必要である。
原則 12	・保険会社、保険仲介者、他の規制対象組織および第三者の従業員のために、サイバーセキュリティに関する定期的でタイムリーな研修および相互評価が必要である。

（出典：NAIC 保険規制ガイダンスをもとに作成）

（b）サイバーセキュリティ消費者保護のためのロードマップ

このロードマップは、個人情報を収集し使用する保険会社や代理店等に対し、消費者が自身の個人情報に関して有する権利の保護を目的としている。ロードマップは、今後策定される NAIC モデル法および関連規制等に取り込まれる予定である。

ロードマップには、保険契約者等の権利として、図表 12 に示す 6 点が取り上げられている。この中には、保険会社からのデータ漏えい時に、保険契約者等が通知を受ける権利を持つことも記載されている。保険会社側にとっては、データ漏えい

時に通知を行う義務があり、その通知に記載しなければならない内容も読み取れる（図表 12 の 4）。

図表 12　NAIC のロードマップ（保険契約者等の権利）

	権利の内容
1	保険会社や保険仲介者およびそれらが契約している企業等（マーケティング会社やデータ管理会社等）によって収集され、蓄積されている個人情報のタイプを知ること
2	保険会社や保険仲介者等がプライバシーポリシーをウェブサイトに掲載し、またあなたが依頼すればコピーを入手できることを期待すること。プライバシーポリシーは次のことを説明するものでなければならない。 ・保険会社や保険仲介者等は、どんな個人情報を収集しているか ・消費者は、それらのデータについてどんな選択肢を有するか ・消費者は必要なときにそれらのデータをどのように確認し、修正できるか ・データはどのように蓄積され、保護されているか ・保険会社や保険仲介者等がプライバシーポリシーに従わない場合、消費者は何ができるか
3	保険会社や保険仲介者およびそれらが契約している企業等が、権限のない者があなたの個人情報を見る、盗むまたは使用することを防ぐ合理的な対策を取っていることを期待すること
4	権限のない者があなたの個人情報を見た、盗んだまたは使用した（またはそのように疑われる）場合、保険会社や保険仲介者およびそれらが契約している企業等から通知を受けること。これをデータ漏えいと呼び、この通知は次の要件を満たす必要がある。 ・第 1 種郵便（first-class mail）またはあなたが合意している場合、電子メールにより文書形式で送付される ・データ漏えい後すぐに、漏えい発覚後 60 日を超えないうちに送付される ・漏えいした情報のタイプおよび、ID 盗難または詐欺から自分を保護するためにあなたが取れる対策につき記載する ・保険会社や保険仲介者およびそれらが契約している企業等が、あなたの個人情報の安全を確保するために取った行動につき記載する ・全米ベースの 3 つのクレジット・ビューロー（注1）の連絡先を含む ・データ漏えいに関係する保険会社や保険仲介者の連絡先を含む
5	データ漏えいがあった保険会社や保険仲介者から、少なくとも 1 年の ID 盗難の補償を受ける。
6	誰かがあなたの ID を盗んだ場合、あなたには次の権利がある。 ・あなたの消費者報告（注2）に、当初 90 日間の ID 盗難警告を設定できる。 ・この ID 盗難警告は 7 年間延長できる。 ・あなたの消費者報告に、信用凍結（credit freeze）を設定できる。 ・各信用報告機関から、あなたの消費者報告を無料で入手できる。 ・あなたの消費者報告から取り除かれた（またはブロックされた）漏えいデータに関連する詐欺情報を入手できる。 ・あなたの消費者報告における詐欺または誤った情報を指摘できる。 ・貸し手や債務取立人が、漏えいデータに関連する詐欺の報告を行うことを止めさせる。 ・ID 盗難に関する文書のコピーを入手できる。 ・債務取立人があなたに連絡するのを止めさせることができる。

（注１）クレジット・ビューローについては、前掲脚注 73 を参照願う。

（注２）消費者報告については、前掲脚注 74 を参照願う。

（出典：NAIC ロードマップをもとに作成）

（2）保険会社の健全性への影響

本項では、サイバーリスクによる保険会社の健全性への影響について、保険監督者国際機構（IAIS）の文書で示された保険業界の脆弱性と、米国の格付会社による格付評価の見方について紹介する。

a. IAIS の文書で示された保険業界の脆弱性

2016 年 4 月、保険監督者国際機構（IAIS）は、保険部門のサイバーリスクに関する市中協議文書を策定・公表した[76]。この文書の目的は、保険部門におけるサイバーリスクの脅威に関し、保険会社および保険監督当局が対処すべき課題につき意識を高めることにある。

この文書では、保険会社が保険会社自身のサイバーリスクに対し脆弱であることが強調されている。保険会社のシステムは業務上、資金調達や資産運用等のため、複数のルートを通じて他の金融機関と接続されており、サイバー攻撃に伴うこれら機能の停止は、保険会社の事業運営に重大な影響を及ぼす。また、保険会社のシステムへの悪質なサイバー攻撃による保険契約者等の個人情報の流出は、保険契約者等に多大な被害をもたらすだけでなく、保険会社の風評被害にもつながる可能性がある。

このため、保険会社はサイバー攻撃に対する対応力を高めることが重要であるとされている。

b. 米国の格付会社の見方

S&P 社、Moody's 社、Fitch 社、A.M.ベスト社等の米国の格付会社は、損害保険会社の格付評価において、サイバーリスクをこれまで以上に重視しており、抱えているサイバーリスクが大きく、その管理が不十分な保険会社は、格付けに影響を及ぼす可能性があるとしている。以下は、A.M.ベスト社の格付評価における基本的な考え方であり、他の格付会社とも共通する部分が多い。

A.M.ベスト社では、損害保険会社の格付評価に関するサイバーリスクの影響について、保険会社自身がサイバーリスクの脅威に対しどの程度の防御策を取っているか、また、サイバー保険の引受を行っている場合、潜在的な損失の可能性はどの程度かの 2 点を中心に評価している。

1 点目の保険会社自身の防御策に関しては、膨大な個人データを保有している保険業界は、大規模なデータ漏えいやそれに伴う風評被害により、財務的に大きな影響を受けるリスクがあるとされている。

2 点目のサイバー保険の引受による格付けへの影響については、どのようなタイプのリスクを引き受けているか、どの程度の支払限度額の補償を提供しているか等の状況が、その保険会社の資本水準に比べどの程度の影響力を持つかによって決まる。

保険会社は、サイバーリスクの相互関連性を考慮すると、個々の契約者の支払限度額を保守的な水準に設定せざるを得ない。また、保険金支払実績のデータや数量的分析のための情報が乏しい現状では、サイバーリスクに対する準備金の積立方法は、慎重なリスク管理に基づくものでなければならない。保険会社が、このように保守的な

[76] IAIS, "Issues Paper on Cyber Risk to the Insurance Sector" (2016.4.14)

運営を行っている場合、格付においては好意的に評価される。

保険会社にとって、サイバー保険の引受ポートフォリオにおけるリスクの集積や潜在的な巨大被害シナリオをテストする手法が極めて重要になっている。1 つの攻撃が非常に多くの数の被保険者の損害につながる可能性があり、このリスクの集積に保険会社は大きな注意を払う必要がある。また、巨額の損失につながるシナリオを分析し、信頼できる方法で、潜在的な損失の大きさを把握しておく必要があると A.M.ベスト社は考えている。

６．おわりに

IoT の進展は、世界的に避けられない流れであり、企業や保険会社にとって、サイバーリスクの脅威は益々大きくなり、複雑化していくと考えられる。わが国では、官民挙げてサイバーリスク対策の取組が進められつつあるが、サイバー保険の利用は、まだ始まったばかりである。

サイバー保険市場は、米国では急速に拡大しており、わが国でも企業の需要が大きく拡大する可能性がある。保険会社にとっては、保険の引受やリスク管理に関するアドバイスの提供等、今後大きなビジネスチャンスにつながる可能性のある領域である。一方、リスク管理が十分でないまま、引受を拡大してしまうと、将来的に保険会社の経営に重大な影響を及ぼす可能性も考えられる。

保険会社は、自社のサイバーセキュリティを高度化するとともに、サイバー保険の引受によるデータの蓄積と分析や、金融 ISAC との連携を含む業界内外および政府との情報共有等を通じて、より企業のニーズに合った商品の開発、企業が抱えるリスクの評価やモニタリング、および引受リスクの管理等の分野において競争力を高める必要がある。

そのためには、サイバーセキュリティに関し高度の専門性を有する人材およびセキュリティ施策をマネジメントできる人材の採用や育成を含む態勢の整備が欠かせないと考えられる。

サイバー保険市場は、米国でもまだ成長途上にあり、様々な変化が生じる可能性がある。その動向はわが国のサイバー保険市場の今後について考える上でも参考になるため、引き続き注視することとしたい。

＜参考資料＞

・金融庁「金融分野におけるサイバーセキュリティ強化に向けた取組方針について」（2015.7）
・経済産業省、情報処理推進機構「サイバーセキュリティ経営ガイドライン」（2015.12）
・サイバーセキュリティ戦略本部「サイバーセキュリティ政策に係る年次報告（2015 年度）」（2016.6）
・情報処理推進機構「企業におけるサイバーリスク管理の実態調査 2015～サイバー保険の認知やニーズの現状～」（2015.6）
・総務省「平成 27 年版情報通信白書」
・日本経済団体連合会「サイバーセキュリティ対策の強化に向けた第二次提言」（2016.1）
・日本経済団体連合会「サイバーセキュリティ対策の強化に向けた提言」（2015.2）
・PwC「サイバーセキュリティのための情報共有分析機関（米国 ISAO）に関する調査分析結果および提言」（2015.7.14）
・PwC「サイバーセキュリティの転換と変容：グローバル情報セキュリティ調査 2016」
・PwC「諸外国の金融分野のサイバーセキュリティ対策に関する調査研究報告書」（2015.3.31）
・PwC「相互につながった世界におけるサイバーリスクマネジメント:グローバルセキュリティ調査 2015」
・福留竜太郎「米国 NAIC のソルベンシー近代化構想の進展」損保総研レポート第 102 号（損害保険事業総合研究所、2013.1）
・三菱総合研究所「米国のセキュリティ情報共有組織（ISAC）の状況と運用実態に関する調査」（2010.3）
・山下潤「米国のサイバー・インシュアランスの動向」損保総研レポート第 110 号（損害保険事業総合研究所、2015.1）
・Accenture, “Accenture’s 2016 Compliance Risk Study: Compliance at a Crossroads: One Step Forward, Two Steps Back?”
・Allianz Global Corporate & Specialty, “A Guide to Cyber Risk”（2015.9）
・A.M. Best, “A.M. Best’s View on Cyber-Security Issues and Insurance Companies”（2015.11.24）
・Aon Risk Solutions, “Cyber Risk for Technology Industry”（2016.2）
・Aon Risk Solutions, “Cyber Survey 2016”
・Asia Insurance Review, “Cyber and emerging risks take centre stage”（2016.6）
・Betterley Risk Consultants, “Cyber/Privacy Insurance Market Survey 2016”（2016.6）
・Business Insurance, “Careful negotiations reduce risk of being held to cyber ransom”（2016.5.23）
・Business Insurance, “Cyber insurance rates moderate”（2016.6.6）
・EY, “Global Forensic Data Analytics Survey 2016”
・Financial Services Sector Coordinating Council, “2016 Cyber Insurance Buying Guide”（2016）
・Financial Services Sector Coordinating Council, “Purchaser’s Guide to Cyber Insurance Products”（2016）
・Fitch Ratings, “Global Cyber Insurance Update: Expanding Threats Amplify Underwriting Opportunity, Loss Potential”（2016.3）
・Hanover Research, “Cyber Insurance Survey Prepared for ISO”（2014.10）

・Higher Education Information Security Council, “Cyber Liability Insurance FAQ”（2015.9）
・IAIS, “Issues Paper on Cyber Risk to the Insurance Sector”（2016.4.14）
・Insurance Information Institute, “Cyber Risks: The Growing Threat”（2014.6）
・Insurance Information Institute, “The Insurance Fact Book 2016”
・Insurance Post, “Digital Cyber Insurance”（2016.6）
・ITRC, “Data Breach Reports”（2015.12.31）
・ITRC, “Data Breach Reports”（2016.7.5）
・ITRC, “2015 Data Breach Stats”
・Marsh & McLennan Companies, “The Role of Cyber Insurance in Risk Management”（2016.3.22）
・Moody’s Investor’s Service, “Threat of cyber risk is of growing importance to credit analysis”（2015.11.23）
・Munich Re, “Cyber Risks in Italian market”（2014）
・National Underwriter, “Eating it up”（2016.5）
・NAIC, “CIPR Newsletter”（2015.12）
・NAIC, “CIPR Newsletter”（2015.5）
・NAIC, “CIPR Newsletter”（2014.7）
・NetDiligence, “2015 Cyber Claims Study”
・New York State Department of Financial Services, “Report on Cyber Security in the Insurance Sector”（2015.2）
・Ponemon Institute, “2016 Cost of Data Breach Study: United States”（2016.6）
・Ponemon Institute, “Cost of Data Center Outages”（2016.1）
・PwC, “Insurance Banana Skins 2015, The CSFI survey of the risks facing insurers”（2015.7）
・PwC, “Insurance 2020 & beyond: Reaping the dividends of cyber resilience”（2015.9）
・RIMS, “Cyber Survey”（2015.5）
・SANS Institute, “Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey”（2016.6）
・The Council of Insurance Agents & Brokers, “Cyber Insurance Market Watch Survey”（2016.4）
・Weightmans LLP, “Cyber Risk Survey Report”（2015.11）
・Wells Fargo Insurance Services USA, “2015 Cyber Security and Data Privacy Survey: How prepared are you?”（2015.9）

＜参考ウェブサイト＞

・あいおいニッセイ同和損害保険　http://www.aioinissaydowa.co.jp/
・金融 ISAC　http://www.f-isac.jp/index.html
・金融庁　http://www.fsa.go.jp/
・財務省　http://www.mof.go.jp/
・総務省　http://www.soumu.go.jp/

・損害保険事業総合研究所　https://www.sonposoken.or.jp/
・損害保険ジャパン日本興亜　http://www.sjnk.co.jp/
・損保ジャパン日本興亜総合研究所　http://www.sj-ri.co.jp/
・東京海上日動火災保険　http://www.tokiomarine-nichido.co.jp/
・日本経済団体連合会　http://www.keidanren.or.jp/
・日本損害保険協会　http://www.sonpo.or.jp/
・米国土安全保障省（DHS）　https://www.dhs.gov/
・米財務省　http://www.ustreas.gov/
・米ホワイトハウス　https://www.whitehouse.gov/
・三井住友海上火災保険　http://www.ms-ins.com/
・AIG　http://www.aig.com/home_3171_411330.html
・Allstate　https://www.allstate.com/
・A.M. Best　http://www.ambest.com/
・EY Global　http://www.ey.com/
・Financial Stability Board（FSB）　http://www.financialstabilityboard.org/
・Fitch Ratings　http://www.fitchratings.co.jp/
・FRB　http://www.federalreserve.gov/
・Insurance Information Institute　http://www.iii.org/
・Insurance Services Office（ISO）　http://www.verisk.com/iso.html
・International Association of Insurance Supervisors（IAIS）　http://www.iaisweb.org/
・KPMG　https://home.kpmg.com/
・Moody's Investor's Service　http://www.moodys.co.jp/pages/HomePage.aspx
・National Association of Insurance Commissioners（NAIC）　http://www.naic.org/
・Property Casualty Insurers Association of America（PCI）　http://www.pciaa.net/sitehome.nsf/main
・PwC　http://www.pwc.com/
・S&P　http://www.standardandpoors.com/en_US/web/guest/home
・Travelers　https://www.travelers.com/