米国のサイバー・インシュアランスの動向

主席研究員　山下　潤

目　　次

１．　はじめに

２．　サイバー・リスクの概要

(1)　サイバー・リスクの定義

(2)　米国におけるサイバー・リスクの位置付け

(3)　米国におけるサイバー犯罪の動向

(4)　顧客情報漏えい対応に要する費用

３．　サイバー・インシュアランスについて

(1)　サイバー・インシュアランスの概要

(2)　市場動向

(3)　業態別の付保金額（支払限度額）

(4)　サイバー・インシュアランスの保険金支払いの状況

４．　サイバー・インシュアランスの商品内容と関連サービス

(1)　商品の構成

(2)　関連サービス

(3)　保険料率の推移

５．　米国以外の動向（情報漏えい事故、データ保護法、保険等）

(1)　欧州

(2)　アジア・太平洋

６．　サイバー・インシュアランスの今後の展望・課題

(1)　サイバー・リスクの D&O 保険への波及

(2)　リスクの集積等に対する対応

(3)　適正な保険料率の算出、アンダーライティング

７．おわりに

要旨

ハッキング等のサイバー犯罪が世界経済に与える被害額は年間5,800億ﾄﾞﾙとも報じられており、とりわけ米国は世界で最も被害額が多い国である。サイバー犯罪等に起因する顧客情報の漏えいも大きな問題であり、当該企業にとっては、信用（ブランド）の失墜だけでなく、事故対応のために巨額の費用が必要となる。2013 年末にハッキングによって顧客情報の漏えいが発覚した米ディスカウント大手のターゲット社は、既に1億5,000万ﾄﾞﾙを超える対策費を計上している。また、同社ではCEOの辞任にとどまらず、株主から役員に対しての代表訴訟も提起されている。ターゲット社は、これまでに要した顧客情報漏えいの対応に関する費用のうち、既に 9,000 万ﾄﾞﾙは保険で補償されると公表しており、これに加え 6,500 万ﾄﾞﾙの D&O 保険も付保しているとも報道されている。

近年、米国では有名企業による相次ぐ顧客情報漏えい事故等を契機に、サイバー・インシュアランス市場が拡大している。一方、同保険は比較的新しい分野のリスクをカバーする保険であることから、アンダーライティングやキャパシティ等の問題も内包していると考えられる。

わが国においても、2014 年 11 月にサイバーセキュリティ基本法が成立するなど、サイバー・リスクに関する懸念や対応の必要性は高まって来ている。日本企業もグローバル化が進展しており、わが国の保険業界としても、同分野の保険商品の提供や関連サービスを一層充実したものにする必要がある。

本稿では、米国企業におけるサイバー・リスクの位置付けやサイバー・インシュアランスの市場や商品等の動向について取り上げている。サイバー・リスクや同保険に関して米国の保険業界が抱えている課題等については、わが国にも共通するものがあると考えることから、先進的な米国の動向は参考になるものと思われる。

1. はじめに

2014 年夏、わが国では大手通信教育・出版社の委託先元社員による約 3,500 万件の顧客情報漏えい事件が世間を騒がせた。同時期に、米国でも大手銀行の JP モルガン・チェース（JPMorgan Chase& Co.）においてハッキングにより約 7,600 万人の顧客情報等が流出、全米およびカナダ等に 2,000 を超える店舗を有するホームセンター大手のホーム・デポ（The Home Depot,Inc）でも 9 月に支払システムがハッキングされ、5,600 万枚のクレジットカード情報等が漏えいするなど、多くの事故・被害が報告されている。顧客情報の漏えいは、企業の信用（ブランド）失墜を招くことは勿論のこと、損害賠償や原因調査などに巨額の費用が必要となる。

米国においては、1990 年代後半からそれらのリスクをカバーする保険商品（サイバー・インシュアランス）が登場したが、保険の購入先は金融機関やクレジットカード等の顧客情報を多く取り扱う小売業等の一部の業種や、大手企業が中心であった。しかし、著名企業における相次ぐ顧客情報漏えい事故の発生などから、現在は、大企業のみならず、中小企業へと広がっており、サイバー・インシュアランス市場の成長が拡大している。また、近年では、顧客情報漏えい等に起因する損害賠償や各種費用の発生・負担にとどまらず、株主から役員の責任が追及され訴訟を受ける動きもでてきており、会社役員賠償責任保険（D&O 保険）への波及も見せている。

現代はビジネスがグローバル化しており、かつ、近い将来にテクノロジーの粋を尽くした自動運転車の実用化も想定されている。あらゆるものがインターネットを通じて接続されモニタリングやコントロールを可能にする IoT（Internet of Things）[1]の時代を迎えている。同時に、外部からの不正アクセス等のサイバー・リスクは一層増大・複雑化しており、これに伴いサイバー・インシュアランス市場も拡大しつつ、社会の状況に合わせて大きく変化していくものと考えられる。

わが国においても、サイバー犯罪は増加の傾向にあり、2014 年 11 月に「サイバーセキュリティ基本法」[2]が衆議院を通過するなどサイバー・リスクへの対応が強化されてきている。本稿では、世界中で最もサイバー犯罪による被害額が多く、また、サイバー・インシュアランスの世界最大の市場である米国におけるサイバー・リスクとサイバー・インシュアランスの現状を概観しており、わが国の保険業界の今後の参考になれば幸いである。

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] IoT（Internet of Things）とは、一般的に「モノのインターネット」と訳されている。身の回りのあらゆるものにインターネットが組み込まれ、モニタリングやコントロールを可能にするという概念のこと。家電等の物理的な物にコンピュータが組み込まれ人がそれを利用するだけでなく、衣服やメガネ（ウェアラブルデバイス）や家屋（スマートハウス）がスマート化され、必ずしも人を介さずモノ同士の自律連携も可能であるというコンセプトである。

[2] わが国の「サイバーセキュリティ基本法」については、後記 5（2）を参照願う。

2. サイバー・リスクの概要

本項では、サイバー・リスクの定義、米国におけるサイバー・リスクの位置付け、サイバー犯罪の動向等につき説明する。

（1）サイバー・リスクの定義

インターネットの急速な発展により、ありとあらゆるものがコンピューターで接続されている。そのような情報化社会においては、サイバー攻撃[3]（インターネット等を利用して標的とするコンピューターやネットワークに不正に侵入し、データの搾取や破壊、改ざんを行ったり、標的のシステムを機能不全に陥らせる行為）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追及や信用の失墜、またそれらを要因とする売り上げの減少など様々なリスクが存在する。本稿では、それらのリスクを総称して、サイバー・リスクと呼ぶこととする。

（2）米国におけるサイバー・リスクの位置付け

アリアンツ・グローバル・コーポレート&スペシャリティ社は、世界の 30 カ国以上の同社グループ関係者（保険会社引受担当者・査定担当者、リスクコンサルタント等）に対して実施した、「最も懸念するビジネス上のリスク」に関するアンケート結果の 2014 年版を公表した（図表 1 参照）[4]。同調査において、米国におけるサイバー攻撃・システム上の不具合等のサイバー・リスクへの懸念は上昇しており、8 位となった[5]。本調査は世界の他の地域に関しても実施されており、サイバー・リスクは、EMEA 地域（ヨーロッパ、中東、アフリカ）[6]で 9 位、アジア・太平洋地域でも 6 位となった。

また、大手保険グループのチャブ（Chubb）が行った調査[7]においても、海外展開する米国企業のトップが懸念するリスクとして、1 位（19%）のサプライチェーン・リスクに続いて、2 位（15%）にサイバー・リスク（データ漏えい・サイバー犯罪等）がランクされている。近年では、出張の際に、従業員にノートパソコンやスマートフォンの業務上の使用を許可している企業も多く、モバイルデバイスの紛失等により顧客情報等が漏えいするリスクを懸念しているとの声も多く、これらの調査結果からも、サイバー・リスクに関する企業経営者の懸念は大きくなっていることがわかる。

---

[3] サイバー攻撃の具体的手法としては、コンピュータ・ウィルスを添付した e メールを送信したり、大量のデータを送りつけ相手方がシステムを稼働できない状態にする Dos（Denial of Service attack）／DDos（Distributed Denial of Service attack）等がある。

[4] Allianz Risk Barometer on Business Risks 2014。有効回答数 557。

[5] 2013 年調査では、10 位圏外。

[6] EMEA とは、Europe, the Middle East and Africa の略で、ヨーロッパ、中東、アフリカの総称である。

[7] 2014 Chubb Multinational Risk Survey

図表 1　アリアンツグループ関係者が懸念するビジネス上のリスク上位 10（米国）

順位	懸念するリスク	投票率（%）(注)	2013 調査 括弧内は順位	前年との順位比較
1	事業継続、サプライチェーン・リスク	56%	52%（1）	－
2	自然災害（洪水、地震等）リスク	53%	49%（2）	－
3	火災・爆発リスク	26%	32%（3）	－
4	レピュテーション（評判）リスク・ブランド価値の毀損	16%	10%（4）	－
5	規制・制度変更リスク	15%	23%（8）	↑
6	市場（景気）停滞・減退リスク	12%	－（－）	↑
7	盗難・詐欺・汚職・腐敗リスク	11%	11%（7）	－
8	**サイバー・リスク（サイバー攻撃、システム上の不具合等）**	**11%**	**（－）（－）**	**↑**
9	労働力リスク（労働者不足、高齢化）	9%	（－）（－）	↑
10	競争激化リスク	9%	23%（4）	↓

（注）各社が 3 つの懸念するリスクを選択する方式で行われた。

（出典：Allianz Global Corporate & Specialty,“Allianz Risk Barometer on Business Risks 2014”をもとに作成）

（3）米国におけるサイバー犯罪の動向

本項では、世界経済および米国経済に大きな影響を与えるサイバー犯罪による損害額およびサイバー・リスクの代表例ともいえる企業等による顧客情報漏えい事故の件数、漏えいした情報数の推移等について紹介する。

a. サイバー犯罪による損害額（世界、米国）

米国のシンクタンクである戦略国際問題研究所（CSIS）の報告によると、サイバー犯罪が世界経済に与える損害額は、年間 3,750 億ﾄﾞﾙ（45 兆 6,000 億円）[8]から 5,750 億ﾄﾞﾙ（69 兆 9,000 億円）と推計されている[9]。そのうち、最も被害実額が多い米国は約 1,010 億ﾄﾞﾙ（12 兆 3,000 億円）と突出して大きな数値となっている[10]。

[8] 2014 年 12 月末時点の為替レートである 1ﾄﾞﾙ=121.55 円で換算した。

[9] Center for Strategic and International Studies,“Net Losses:：Estimating the Global Cost of Cybercrime（2014.7）”

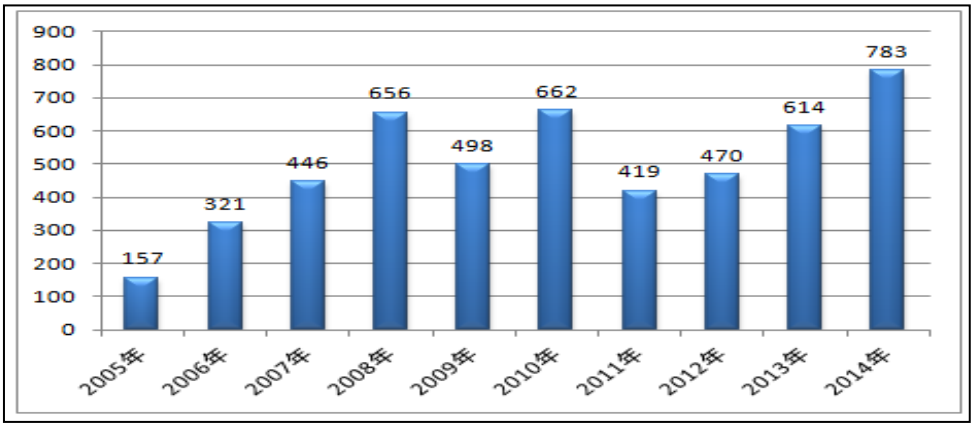
[10] 1,010 億ﾄﾞﾙは米国の GDP の 0.64%に相当する。米国に次いで、中国が約 600 億ﾄﾞﾙ（GDP の 0.63%）、ドイツが 580 億ﾄﾞﾙ同 1.60%）となっており、3 国で約 2,200 億ﾄﾞﾙにのぼっている。日本は GDP の 0.02%、10 億ﾄﾞﾙと報告されている。

b. 情報漏えい事故件数・漏えい情報数の推移

本項では、サイバー・リスクの代表例である顧客情報漏えいに関する米国での動向について説明する[11]。

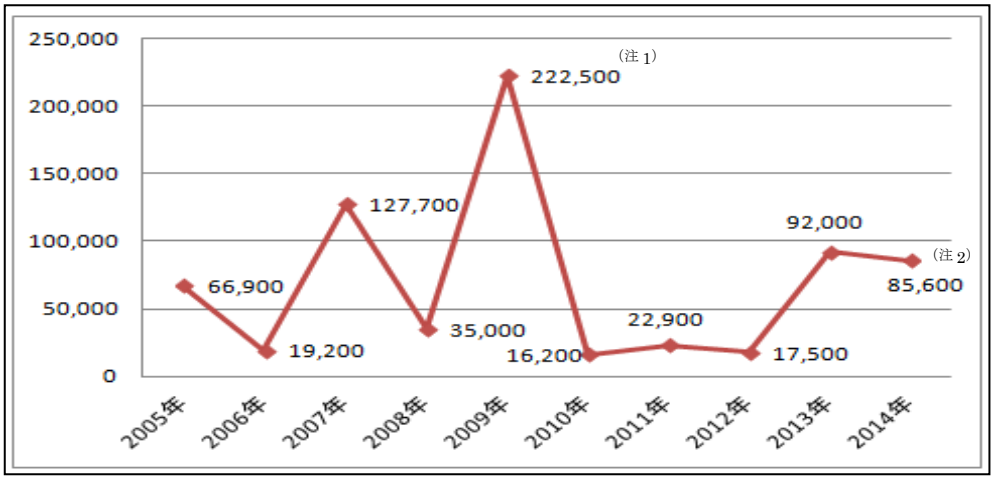
個人の情報漏えい被害者を支援する非営利団体である Identity Theft Resource Center（ITRC）の統計によると、公表された 2014 年の個人情報漏えい事故は 783 件、漏えいした情報数は 8,500 万件を超えている。現在、調査中で公表前のデータがあること等を勘案すると事故数・漏えい情報件数ともに増加傾向にあると考えられる（図表 2、3 参照）。

図表 2　米国における個人情報漏えい事故の推移　（単位：件）



（出典：The Identity Theft Resource Center,“2014 Data Breachs”をもとに作成）

図表 3　米国において漏えいした個人情報数の推移　（単位：千件）



（注 1）2009 年は、クレジットカード決済大手のハートランド・ペイメント・システムズ（1 億 3,000 万件）や退役軍人（7,600 万件）等の大型の個人情報漏えい事故が発生した。

[11] 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。

（注 2）ITRC では、個人情報漏えいを氏名に加え、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数値には含まれていない。

（出典：The Identity Theft Resource Center“2014 Data Breachs”をもとに作成）

（4）顧客情報漏えい対応に要する費用

企業の持つ顧客情報が漏えいした場合、原因の調査、復旧、対策を講じるにあたり多額のコストおよび売上・利益の減少等が生じる。

米国の調査会社ポネモン・インスティチュート[12]によると、顧客情報漏えい事故の発生により企業が被る損失は、平均して漏えい情報 1 件あたり 201ﾄﾞﾙ（24,000 円）、1 事故あたり平均で 585 万ﾄﾞﾙ（約 7 億 1,000 万円）となっており、それぞれ前年と比較して 13ﾄﾞﾙ（対前年 106.9%）、45 万ﾄﾞﾙ（対前年 108.3%）上昇している。585 万ﾄﾞﾙの内訳は、以下のとおりである。

○原因を調査するためのフォレンジックス費用[13]：42 万ﾄﾞﾙ（約 5,100 万円）
○顧客への通知費用[14]：51 万ﾄﾞﾙ（約 6,200 万円）
○事後対応費用：160 万ﾄﾞﾙ（約 1 億 9,000 万円）
（コールセンターの設置費用、クレジットカード等の不正使用のモニタリングに係る費用等）
○売上減少等：332 万ﾄﾞﾙ（約 4 億円）

2014 年 9 月に 5,600 万件のクレジットカード情報等の漏えいが発覚したホームセンター大手のホーム・デポ社の対策費用は、9 月から 11 月の 3 か月で既に 6,200 万ﾄﾞﾙ（75 億 4,000 万円）に達している[15]と言われている。また、2013 年末に 4,000 万件のクレジット･デビットカード等の情報漏えいがあったディスカウント大手のターゲット（Target Corporation）社は、2014 年の第 3 四半期（9 月末）までに 1 億 5,800 万ﾄﾞﾙ（約 192 億円）の対策費を計上している[16]。

---

[12] Ponemon Institute LLC,IBM,“2014 Cost of Data Breach Study：United States”（2014.5）。情報漏えいを経験した 16 業種、61 社に対する調査。ただし、10 万件以上の情報漏えいは除いている。
[13] フォレンジックス（forensics）とは、証拠保全や侵入経路特定のために適切なデータを収集・解析する等に要する費用のこと。
[14] 米国ではデータ保護に関しての関心が高く、National Conference of State Legislatures（全米州議院協議会）のデータベースによると、全米 47 州および特別区であるワシントン DC や準州であるグアム等において、個人情報漏えい事案等が発生した場合に、住民への通知を義務付けるセキュリティ侵害通知法（Security （Data）Breach Notification Laws）が制定されている。
[15] Chain Store Age（2014.9.19）
[16] Target Corporation,“Target Reports Third Quarter 2014 Earnings（2014.11）”

3. サイバー・インシュアランスについて

本項では、米国のサイバー・インシュアランスの概要および市場動向、保険金支払いの状況、保険商品および関連サービス等について説明する。

（1）サイバー・インシュアランスの概要

サイバー・インシュアランスは、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への補償の 2 つの条項により構成される保険商品である。

米国においては、1990 年代後半に販売が開始された。保険約款の作成・料率算出支援団体である ISO（Insurance Services Office）では、2005 年からサイバー・リスクに関する保険商品やリスクマネジメントのサービスを提供している[17]。

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、本項では、Cyber Insurance（以下、「サイバー・インシュアランス」）という呼称を用いて説明する。

（2）市場動向

保険会社やコンサルタント会社等によるアンケート調査に基づき、米国におけるサイバー・インシュアランスの収入保険料の規模・成長率、同保険の販売・付保状況について説明する。

各種調査結果において、現時点ではサイバー・インシュアランスは急速な成長の途上にあり、米国における同保険市場の規模拡大の動きは、当面加速していくものと予測できる。

a. 収入保険料規模・成長率

サイバー・インシュアランスのみに関する正式な統計はないが、保険会社やコンサルタント会社等によるアンケート調査では、以下のような結果が公表されており、現在の米国における市場規模は約 10 億ﾄﾞﾙ（約 1,200 億円）から 20 億ﾄﾞﾙ（約 2,400 億円）の範囲内と捉えられ、企業保険分野全体の 1%程度[18]であると考えられる。

○ 大手保険ブローカー・エーオン（Aon）

2013 年のサイバー・インシュアランスの業界全体の保険料収入は、合計約 10 億

[17] ISO ウェブサイト“Cyber Insurance Program”

[18] 損保ジャパン日本興亜総合研究所“アメリカ損害保険事情ファクトブック 2014”によると、2012 年の企業保険分野の正味収入保険料は 2,211 億ﾄﾞﾙ（26 兆 4,000 億円）である。

ﾄﾞﾙ（1,200 億円）に達したと推定している[19]。

○ スイス・リー（Swiss Re）

2013 年のサイバー･インシュアランスの保険料収入規模は 13 億ﾄﾞﾙ(1,600 億円）に達したと推定している[20]。

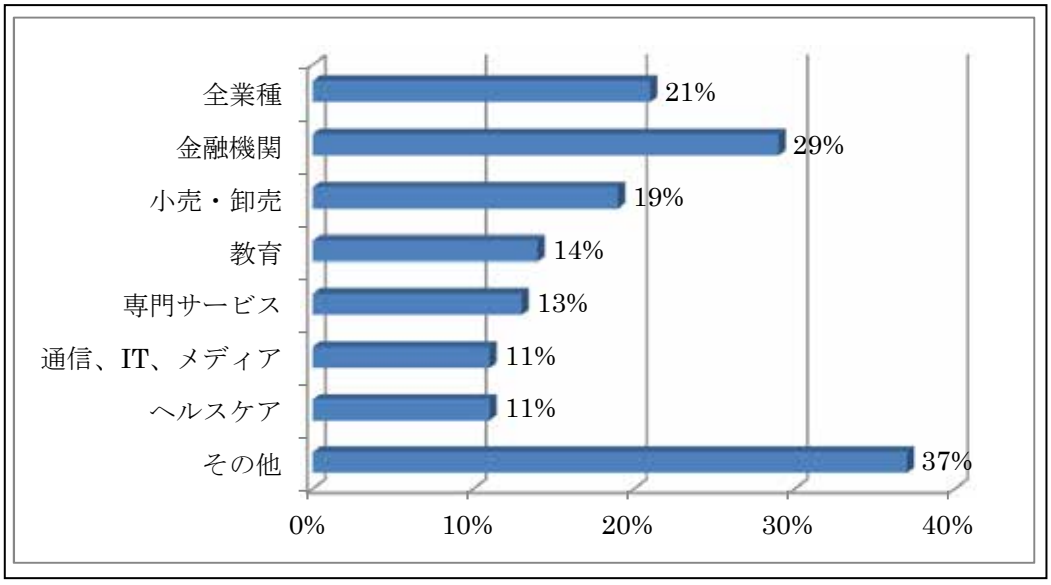
○ リスクコンサルティング会社（Batterley Risk Consultants, Inc）の調査[21]

米国のサイバー保険の保険料収入規模は約 20 億ﾄﾞﾙ（2,400 億円）であり、2013 年には、多くの保険会社が、対前年比 10%から 25%の増加、一部の保険会社においては 25%から 50%を超える伸びを見せている。

○ 大手保険ブローカー・マーシュ（Marsh）の調査[22]

2013 年に、同社を介してサイバー・インシュアランスを契約した企業の数は、前年と比べて 20%超増加し、支払限度額 1 億ﾄﾞﾙ（120 億円）を超えるカバーが購入された。また、同保険を購入する動きは従前からの契約の主体であった金融機関や小売業等だけでなく幅広い業種に拡がっている（図表 4 参照）。

図表 4　マーシュ社のサイバー・インシュアランス契約の対前年増加率（2013 年）



（出典：Marsh,“Bench Marking Trend: Interest in Cyber Insurance Continues to Climb”をもとに作成）

b. サイバー・インシュアランスの販売・付保状況

サイバー・インシュアランスを販売する保険会社、購入する企業もまだ様子見の感は見られる。しかし、2013 年から 2014 年にイーベイ（eBay）や JP モルガン・チェース

[19] Dow Jones（2014.3.27）
[20] Sigma,“Liability claims trends: emerging risks and rebounding economic drivers（2014.4）”
[21] Batterley Risk Consultants,Inc,“The Batterley Report”（2014.6）。
[22] Marsh,“Bench Marking Trend: Interest in Cyber Insurance Continues to Climb”（2014.4）

やホーム・デポ等の米国を代表する企業の情報漏えい事故が多発しており、下記の調査結果等から見ても同保険に関する企業の関心度の高まりがみられること、米国におけるサイバー・リスクに対する消費者保護に関する法律や規制の整備が進んでいること[23]等を考慮すると、保険会社の同保険分野への参入や保険を付保することの必要性の認識が大企業だけでなく中小企業へも拡がっていき、市場規模が拡大していくことが考えられる。

○ ISO とハノーバー・リサーチ（Hanover Research）の調査[24]

アンケート対象の 271 社の保険会社のうち、約半数の 125 社がサイバー・インシュアランスを販売しており、さらに 1 年以内には 85 社が新たに販売するであろうと回答した[25]。また、2015 年は、前年と比較して、半数以上が 25%以内、4 分の 1 以上が 25%超の成長を記録するであろうと回答している。

○ ポネモン・インスティチュート[26]の調査

調査対象の 31%の企業がサイバー・インシュアランスを既に付保しており、26%の企業に保険の購入計画があることから、近い将来には 60%近い企業がサイバー・インシュアランスを付保することになるであろうと回答している。一方、約 4 割の企業が保険購入に否定的であるが、その理由として「保険料が高い」、「免責等が多い」等を挙げている。

（3）業態別の付保金額（支払限度額）

マーシュの調査によると、売上高が 10 億ﾄﾞﾙ（1,200 億円）超の大企業が購入するサイバー・インシュアランスの平均付保金額（支払限度額）は 2,820 万ﾄﾞﾙ（約 34 億 3,000 万円）と前年と比べ 10%程度上昇している。この売上高規模の企業の場合、金融機関が平均 5,320 万ﾄﾞﾙ（約 64 億 7,000 万円）と最も大きいカバーを購入している（図表 5 参照）。

一方、図表 6 のとおり、売上高を勘案しない場合の、保険カバーの平均付保金額（支払限度額）は、全業種平均で 1,150 万ﾄﾞﾙ（約 14 億円）である。また、最も付保金額（支払限度額）の大きい業態は通信・IT・メディアの 2,390 万ﾄﾞﾙ（約 29 億 1,000 万円）であり、前年度と比較して多くの業態で増加している。

2013 年、2014 年にハッキングによる大型の顧客情報漏えいが起きたターゲット社と

---

[23] 前掲脚注 14 を参照願う。

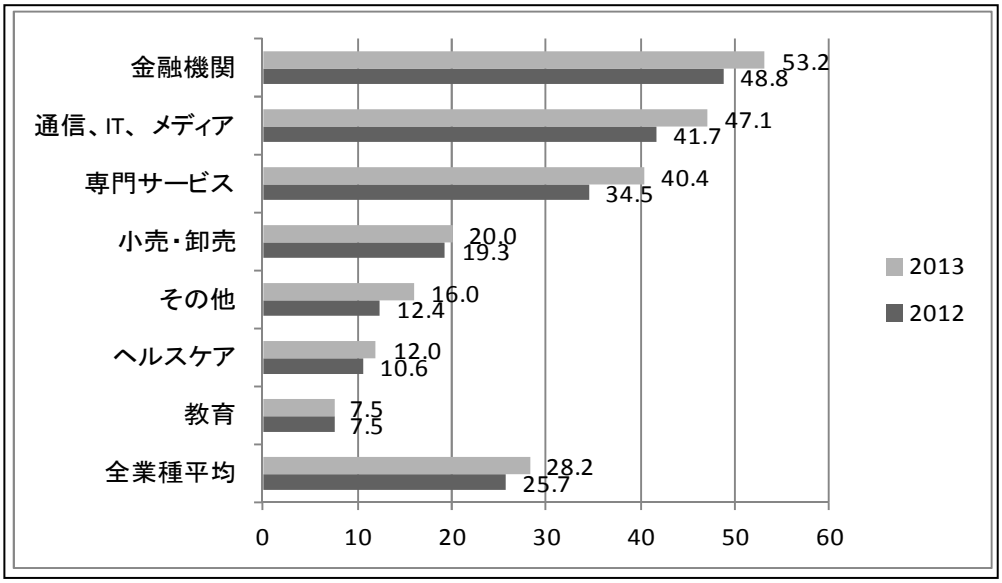
[24] ISO, Hanover Research“Cyber Insurance Survey”（2014.11）。ISO が委託し、マーケットリサーチ会社のハノーバー・リサーチが実施した 271 の保険会社の従業員名に対するオンライン調査。

[25] Swiss Re の SigmaNo.4（2014）「賠償責任保険の保険金請求トレンド：顕在化するリスクと景気回復の要因」によると、従来は「サイバー・リスクには風評損害、知的財産権侵害やデータの価値そのもの等が含まれており、多くの保険会社はこうしたリスクのカバーに消極的であった」と報告されている。

[26] Ponemon Institute, Exoerian “Managing Cyber Security as a Business Risk：Cyber Insurance in the Digital Age”（2013.8）。各種業種のリスクマネージャーに対するアンケート調査で、有効回答数は 638。

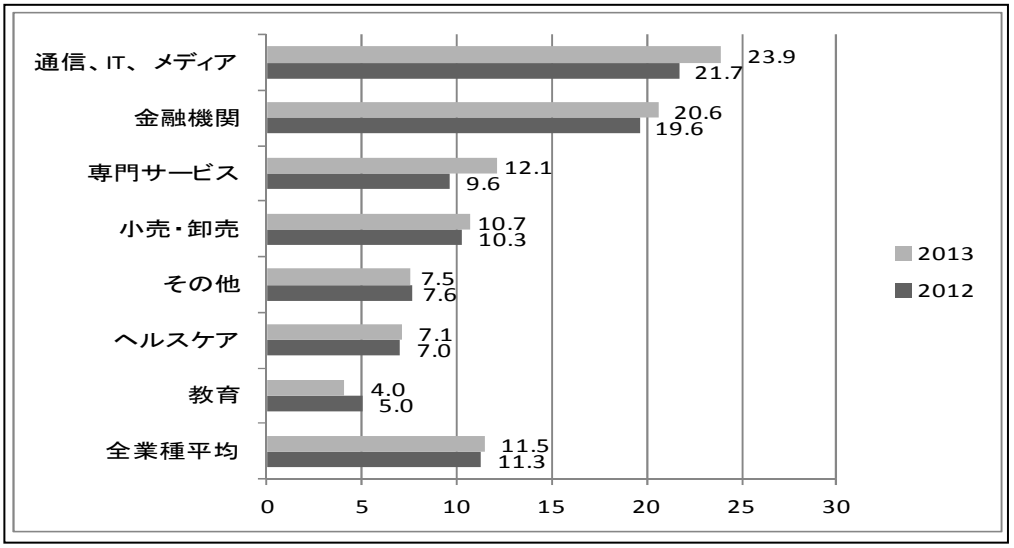
ホーム・デポ社は、それぞれ支払限度額1億ﾄﾞﾙ（約120億円）[27]と1億500万ﾄﾞﾙ（約127億6,000万円）[28]のサイバー・インシュアランスを付保していると報道されている。

図表5（売上高10億ﾄﾞﾙ超）業態別平均付保金額（支払限度額）（単位：百万ﾄﾞﾙ）



（出典：Marsh Risk Management Research，“Benchmarking Trends：Interest in Cyber Insurance Continues to climb（2014）”をもとに作成）

図表6（全売上高）業態別平均付保金額（支払限度額）　（単位：百万ﾄﾞﾙ）



（出典：Marsh Risk Management Research，“Benchmarking Trends：Interest in Cyber Insurance Continues to climb（2014）”をもとに作成）

[27] Judy Greenwald,“Target SEC filing details insurance coverage and outlines costs of data breach（Business Insurance）”（2014.3.30）

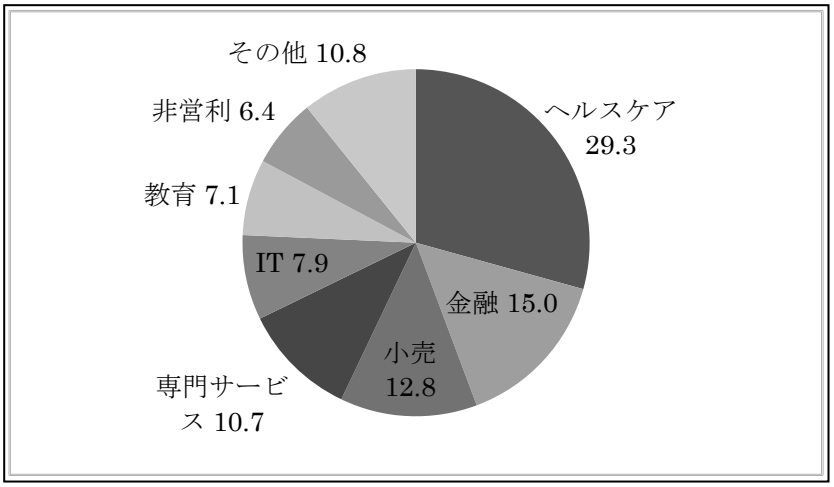
[28] Business Insurance（2014.9.12）。また、ターゲット社は支払限度額6,500万ﾄﾞﾙ（79億円）のD&O保険も付保していると報道されている。

（4）サイバー・インシュアランスの保険金支払いの状況

ネット・デリジェンス（NetDiligence）社の調査[29]によると、AIG や ACE 等の 19 社において、2010 年から 2012 年の間にサイバー・インシュアランスで支払われた保険金の平均額は 95 万 4,000ﾄﾞﾙ（約 1 億 2,000 万円）であり、免責金額などの契約者が自社で保有している部分を含めると、平均 350 万ﾄﾞﾙ（約 4 億 3,000 万円）に達していると推測されている。

業種別の保険金支払い件数の割合では、病院等のヘルスケア業界の 29.3%を筆頭に、金融（15.0%）、小売（12.8%）と続いている（図表 7 参照）。2013 年末に 7,000 万件の顧客情報が流出し CEO の辞任にまで発展したターゲット社は、2014 年の第 3 四半期（9 月末）までに顧客情報漏えいの対策等に要した累計 1 億 5,800 万ﾄﾞﾙ（192 億円）の費用のうち、これまでのところ 9,000 万ﾄﾞﾙ（109 億円）は保険で補償されると発表した[30]。また、ホーム・デポ社もこれまで要している費用 6,200 万ﾄﾞﾙ（75 億 4,000 万円）のうち 2,700 万ﾄﾞﾙ（32 億 8,000 万円）は保険でカバーされる見込みである[31]と報道されている。

図表 7　保険金支払件数の業種毎割合　（単位：%）



（出典：NetDiligence,“2013 Cyber Liability & Data Breach Insurance Claims”をもとに作成 ）

[29] NetDiligence,“2013 Cyber Liability & Data Breach Insurance Claims - A study of Actual Claim Payouts”。AIG、ACE 等の主要 19 社において、同期間中に保険金請求がなされた 145 のクレームに関する調査を実施したもの。同期間中に支払が行われた 88 のクレームに対する支払保険金の総額は約 8,400 万ﾄﾞﾙ（102 億 1,000 万円）であった。

[30] Target Corporation,“Target Reports Third Quarter 2014 Earnings（2014.11）”

[31] Guy Carpenter ,“Emerging Risks Report - Ahead of the curve：Understanding Emerging Risks”（2014.9）

4. サイバー・インシュアランスの商品内容と関連サービス

本項ではサイバー・インシュアランスの構成およびサイバー・リスクに関する保険関連のサービスを紹介する。

（1）商品の構成

サイバー・インシュアランスは、コンピューター・ウィルスや不正アクセス等の外部からの攻撃やシステム上の不具合、ヒューマンエラー等に起因して生じる「第三者への損害賠償」と「自社が被る損害」を補償する条項で構成されている。

○ サード・パーティ・ライアビリティ・カバー（Third‐Party Liability Coverage）
企業の保有する個人や取引先に関する情報が漏えいした場合に生じる、権利侵害等の第三者への損害賠償や訴訟費用をカバーする。

○ ファースト・パーティ・カバー（First‐Party Coverage）
サイバー・リスクによる事故で生じた自社の所有物等に関する損害や事故の発生により必要となった費用をカバーする。

（例）・損壊を受けた機器、コンピュータプログラム、電子データ等の復元費用
・事故の発生の事実やパスワードの変更等を顧客へ通知する費用
・弁護士や広報コンサルタントとの契約等の危機管理費用
・原因を調査するためのフォレンジックス費用
・コールセンターの設置費用
・ネットワークへの侵入による詐欺行為（金銭の搾取、資金の不正移動等）により受けた損害
・事業中断による逸失利益
・クレジットカードのモニタリング（不正使用の監視）等

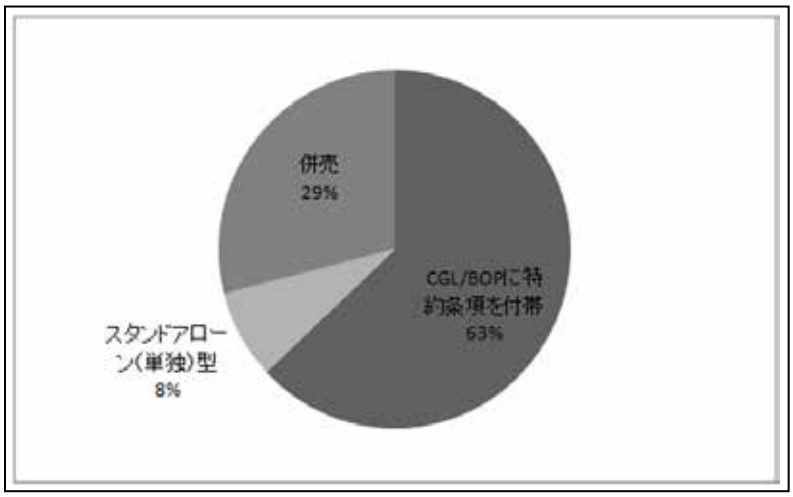
米 ISO の調査[32]によると、サイバー・インシュアランスを販売している保険会社のうち 63%が賠償責任保険である CGL（Comprehensive/Commercial General Liability）や財産保険である BOP（Business Owner's Policy）等にサイバー・リスクに関する特約条項を付帯して販売し、8%が専門職業人賠償責任保険（Errors &Omission）等のスタンドアローン（単独）型の商品として、29%が特約・スタンドアローンの両者の方式を併売している（図表 8 参照）。

一方、サイバー・リスクに関する特約条項が付帯されていない従来からの CGL でも保険対応が可能であるとの議論も存在していた。しかし、不正アクセスにより 1 億を超える個人情報がオンラインゲームから流出した事案に関する保険対応の可否を巡るオンラインゲームの運営会社と保険会社の裁判で、CGL での保険対応を求めるオンラインゲ

[32] 前掲脚注 24 を参照願う。

ーム運営側に不利な判断が下された[33]。これが 1 つの契機となり、保険業界では、一般の CGL にサイバー・リスクに関連する損害を除外する文言を盛り込む動きを加速しており、米 ISO においても CGL に付帯可能な複数のデータ侵害免責条項[34]が 2014 年 5 月に新設されるなど、約款を明確化する動きがある。

図表 8　サイバー・インシュアランスの販売方式



（出典：ISO, Hanover Research“Cyber Insurance Survey”（2014.11）
をもとに作成 ）

（2）関連サービス

サイバー・リスクについては、保険カバーと合わせ、保険会社によるリスクマネジメント・サービスの提供が行われている。

主なサイバー・インシュアランス関連の付帯サービスは図表 9 のとおりである。多くの保険会社が、情報セキュリティや危機管理に関する専門家の紹介や 24 時間アクセス可能なフリーダイヤルでの相談窓口の設置、顧客企業の従業員がサイバー関連知識の習得を目指すための e ラーニングによるトレーニング・プログラムの提供、顧客が抱えるサイバー・リスクや事故発生時のリスク量の測定等のサービスを提供している。

[33] 2011 年にオンラインゲームが不正アクセスされたことにより、1 億人以上の個人情報が流出した事案をめぐり、一般的な賠償責任保険でコストの一部を支払うべきか否かを争った裁判があり、2014 年 2 月にニューヨーク州裁判所は、当該約款はハッカー攻撃に言及しておらず、訴訟で当該企業を守る費用を支払うことを保険会社に義務付けていないとの解釈を示した。

[34] Exclusion - Access Or Disclosure Of Confidential Or Personal Information And Data - Related Liability（ISO - CG21060514）等

図表 9　保険会社が提供する主なサイバー・インシュアランスの関連サービス

サービスの例
○モバイルアプリ等でサイバー・リスクに関する最新の情報の提供
○情報セキュリティに関するトレーニング・プログラムやコンプライアンス・プログラムの提供
○コンピューター会社や情報セキュリティ専門会社と提携したコンサルティングサービス
○弁護士や危機管理専門家の手配
○24 時間・365 日アクセス可能なフリーダイヤル
○漏えい事故発生時の対応ロードマップの作成（チェックリスト作成等）
○情報漏えい事故のリスク量の測定
○ハッキングされた場合のクレジット・モニタリング（不正使用の監視）
○情報セキュリティ・ポリシーの策定支援およびチェック

（出典：各社ウェブサイトをもとに作成）

（3）保険料率の推移

マーシュの調査[35]によると、2012 年から 2013 年のサイバー・インシュアランスの保険料率は安定して推移している。しかし、2013 年末から 2014 年にかけて、前述したターゲット社やホーム・デポ社のように巨額な保険金支払いが必要となる事故が相次いでおり、保険料率も引き上げの方向に向かっていくのではないかと思料する。

5. 米国以外の動向（情報漏えい事故、データ保護法、保険等）

サイバー・リスクによる情報漏えいは米国のみならず、世界の国々でも増加傾向にある。リスク・ベイスド・セキュリティー社の調査[36]によると、2009 年から 2013 年の 5 年間におけるデータ漏えいの世界での年平均事故数は約 1,650 件であり、直近 2 カ年（2012 年、2013 年）はこれを上回っている（図表 10 参照）。さらに、2014 年の 1 月から 9 月には、既に 1,922 件の事故が発生、漏えいしたデータ数は 9 億 400 万件にものぼっており、事故数・漏えいデータ件数とも上昇傾向にある。

また、2013 年のサイバー犯罪による企業の被害額は、1,130 億ﾄﾞﾙ（13 兆 7,000 億円）[37]に達するなど、サイバー・リスクは世界中でますます深刻化している。

本項では、アメリカ以外の主な国・地域のサイバー・リスクおよびサイバー・インシ

---

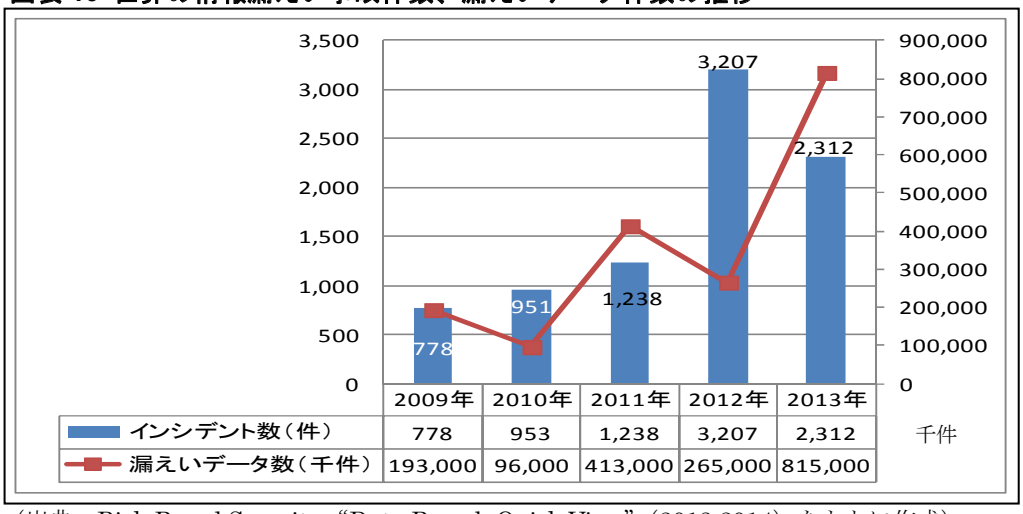
35 Marsh,“Benchmarking Trends:Interest in Cyber Insurance Continues to climb（2014）”,“Benchmarking Trends：More Companies Purchasing Cyber Insurance（2013）”,“United States Insurance Market Report 2014（2014）”

36 Risk Based security ,“Data Breach Trends during the First Nine months of 2014”（2014.10）

37 シマンテック「2013 ノートンレポート（Norton Report）」

ュアランスに関する動向を概観する。

図表 10 世界の情報漏えい事故件数、漏えいデータ件数の推移



（出典：Risk Based Security,“Data Breach Quick View”（2013,2014）をもとに作成）

（1）欧州

現在のサイバー・インシュアランス市場は、約 1 億 5,000 万ﾄﾞﾙ（約 182 億円）と米国の 10%程度であるが、近年では 50%から 100%の成長率で推移しており、2018 年までには 9 億ﾕｰﾛ（約 1,330 億円）[38]に達するとも予測されている[39]。

現在、欧州連合（EU）では、2015 年の施行を目指して顧客情報保護に向けたルール案[40]づくりが進められており、同ルールの成立を契機として、サイバー・インシュアランス市場の拡大が加速していくことが見込まれている。

（2）アジア・太平洋

アジア・太平洋地域の企業は最もサイバー犯罪による被害が多い地域で、年間 1,380 億ﾄﾞﾙ（約 16 兆 8,000 億円）の損害を被っており、2014 年には 2,300 億ﾄﾞﾙ（約 28 兆円）に達するとの調査結果がある[41]。同地域のサイバー・インシュアランスに関する統計データはないものの、アジアの政府や企業においても、サイバー・リスクに関する危機意識が高まっている。アジアの多くの国には既にデータ保護に関する法律[42]があり、インドネシアや台湾、韓国、フィリピン等には米国と同様に個人の情報の漏えいが発生

[38] 2014 年 12 月末時点の為替レートである 1 ﾕｰﾛ＝148.04 円で換算した。
[39] Guy Carpenter,“Emerging Risks Report - Ahead of the curve：Understanding Emerging Risks”（2014. 9）
[40] EU データ保護規則改正案は、2014 年 3 月に欧州議会を通過、欧州理事会による最終協議に入っている。
[41] IDC (International Data Corporation)/NUS (National University of Singapore) Study,“Cost of Cyber-Security Breaches Highest in Asia Pacific”（2014.3）
[42] 例えば、Personal Data Protection Act of 2012（シンガポール）、Personal Data Protection Act 2010（マレーシア）、Personal Information Protection Act（韓国）、Personal Data（Privacy）Ordinance（香港）がある。

した際に行政や本人へ通知義務を課す国も存在している[43]。

わが国においても、政府のサイバーセキュリティ戦略の基盤となる「サイバーセキュリティ基本法」が 2015 年 1 月 9 日に全面施行された。同法は、国や地方自治体にサイバー攻撃への安全対策を課す法律であり、金融機関や電力会社等の民間の重要インフラ事業者にも政府の対策に協力するよう努力義務を課している。さらに、米 SEC の取組を参考に、上場企業がサイバー攻撃を受けた場合に想定される経営上のリスクを投資家に開示する仕組を導入する検討に入っている。また、グローバルなサイバー空間に対応するため、サイバーセキュリティ政策に関する欧米諸国との協議や、新興国でも急増しているサイバー攻撃に対処するため、情報セキュリティに関する情報交換や技術共有を行うなど海外情報セキュリティ機関との連携を深めていくことを政府は表明している[44]。

6. サイバー・インシュアランスの今後の展望・課題

本項では、サイバー・リスクおよびサイバー・インシュアランスにおける今後の展望や主な課題を整理する。

（1）サイバー・リスクの D&O 保険への波及

サイバー・リスクから生じた損害は、経営に甚大な影響を与える可能性があることから、米証券取引委員会（SEC）は、2011 年 10 月に「サイバー攻撃リスクおよびインシデントに関する企業財務部門開示ガイダンス」[45]を公表し、投資家保護の観点から会社の業績に影響を及ぼすようなサイバー攻撃を受けた場合、投資家がそのリスクについて判断できるだけの情報を開示すべきであるとしている（図表 11 参照）。

そのような環境の中、米国では外部からのサイバー攻撃により保有する膨大な数の顧客情報が漏えいした 2 社に対して 2014 年に株主代表訴訟が提起された。まず、2014 年の 1 月および 2 月に、本社を構えるミネソタ州ミネアポリスの連邦地裁において、ターゲット社の株主が同社役員に対して、株主代表訴訟を提起した[46]。また、同年 5 月には、大手ホテルグループのウィンダム・ワールドワイド社[47]の役員に対し、株主代表訴訟が提起されている[48]。いずれの訴訟においても原告側は、サイバー・リスクに対し経営者として十分な防衛手段を講じておらず、かつ、事故発生後の情報開示等が適切に行われ

---

43 DLA Pipper,“Data protection laws of the world”（2014）
44 情報セキュリティ政策会議資料「サイバーセキュリティ 2014」（2014.7）
45 U.S. Securities and Exchange Commission（Division of Corporate Finance）,“CF Disclosure Guidance: Topic No.2-Cybersecurity”（2011.10.13）
46 Kevin M.LaCroix,“The D&O Diary”（2014.2.3）
47 ウィンダム・ワールドワイドは、米ニュージャジーに州に本拠を置くニューヨーク証券取引所上場のホテルチェーンである。ラマダホテルやデイズインを運営している。同グループが運営するホテルで適切なセキュリティ対策が行われていなかったことから 2008 年から 2010 年の間に 3 件のデータ漏えいが発生し、約 62 万人のクレジットカード情報が漏洩し、不正請求等により 1,000 万ﾄﾞﾙ以上の損害が顧客に生じた。
48 Kevin M.LaCroix,“The D&O Diary”（2014.2.3）

なかったことにより会社・株主が損害を被ったと主張している。

このようにサイバー・リスクは、情報漏えい事故から生じる損害額が拡大するに応じて、サイバー・インシュアランスや CGL 等だけでなく、会社役員賠償責任保険（D&O 保険）にまでそのリスクが及んできており、今後の D&O 保険の市場環境にも大きな影響を与え得る存在になることが予測される。

図表 11　企業財務委員会開示ガイダンス（CF Disclosure Guidance）一部抜粋

項目	内容
リスクファクター	企業のサイバーインシデントに関するリスクが、当該企業への投資を投機的あるいは危険なものにし得るリスクファクターである場合に、その開示をする必要があるとし、その中には付保内容（insurance coverage）も含まれている。
MD&A[49]	サイバーセキュリティ・リスクおよびサイバーインシデントに関わる費用やその他の影響が、企業経営、資産流動性、財務状況等に重大な影響を与えると考えられる場合には、それらについて開示する必要がある。
事業内容	サイバーインシデントが、企業の製品、サービス、顧客や取引先との関係や競合状況に重大な影響を与える場合には、「事業内容」の中で開示する必要がある。
法的手続	企業あるいはその子会社が、サイバーインシデントに関わる法的手続を保留されている場合には、その訴訟に関わる情報を「法的手続に関する情報開示」の中で開示する必要がある。
財務諸表の開示	潜在的あるいは実際のインシデントの性質や大きさにより、サイバー・セキュリティリスクやサイバーインシデントと当該企業の財務諸表に広範な影響を与える可能性があることを開示する必要がある。

（出典：内閣官房情報セキュリティセンター「わが国のサイバーセキュリティ戦略」、U.S. Securities and Exchange Commission, “CF Disclosure Guidance: Topic No.2-Cybersecurity” をもとに作成）

（2）リスクの集積に対する対応等

グローバルにサプライチェーンを構築している企業において、外部からのサイバー攻撃等が発生した場合、サプライチェーンで繋がる取引先企業のシステムへも影響を与え、自社の持つシステムの損壊や保有情報の漏えいから、取引先企業の財物の損壊や事業中断リスク等にリスクが変化・拡大していくことも考えられる。保険者としても、従来では、1 つの企業のリスクに過ぎなかったものが、被保険者である企業がサプライチェーンで繋がる企業群にまでリスクが連鎖・拡大した場合、保険の引受方式によってはリスクが集積し、巨大化することとなる。また、近年、日本企業においても利用が進んでいるクラウド・コンピューティングの分野においても、サイバー攻撃やウィルス等のリス

[49] Management’s Discussion and Analysis of Financial Condition and Results of Operations（経営者による財務状態および経営成績の検討と分析）

クも考えられ、サプライチェーンと同様の集積リスクが存在するのではとも考えられる。

2014 年 9 月、大手保険ブローカーのマーシュは、大企業向けに 3 億ﾄﾞﾙ超（最低自己負担金額 1 億ﾄﾞﾙ）のサイバー・インシュアランスの巨大災害補償（カタストロフィック・プロテクション）のカバーの提供を開始することを公表した[50]。このことからも企業において保険カバーへのニーズが高額化していることが推測でき、急増かつ多様化するサイバー・リスクやサイバー・インシュアランスの急速な普及に伴い、グローバルにサプライチェーンを構築する企業等に対する保険の引受方法や提供可能なキャパシティの確保等に関しては、課題が存在するものと考える。

（3）適正な保険料率の算出、アンダーライティング

サイバー・インシュアランスの保険料率は、業種、売上高規模、企業が保有する情報の種類・量、企業の情報セキュリティ対策の実施状況や市場環境等の様々な要素を反映して決定される。また、同商品は、比較的新しいリスクをカバーする保険であることから、過去の事故データ数や事故の詳細に関するデータの蓄積も少ない。加えて、近年急速に市場が伸長するなど市場環境が大きく変化しており、適正な保険料率の算出やアンダーライティング手法にも改善の余地があると考えられる。あわせて、情報セキュリティに関する知識や技術など特殊なサイバー・リスクを評価し、引受を行う人材の育成も急務であると考えられる。

7. おわりに

IT への依存度が高く、業務においてもソーシャル・ネットワーキング・サービス（SNS）やスマートフォン等のモバイルデバイスが積極的に活用されている現代社会においては、サイバー・リスクへの対策は企業において重要な課題である。サイバー・リスクが顕在化した場合、被害は瞬く間に全国、そして世界に広がり、対応策にかかるコストは莫大なものとなる。その一方で、企業のハード・ソフトのシステム損壊を狙った外部からの不正な攻撃や、企業が保有する機密情報の窃取を狙った攻撃の技術も高度化・巧妙化している。

米国においては、サイバー・リスクは、エマージング・リスク[51]の位置付けから、すでに一般的に認知されたリスクになっている。サイバー・インシュアランスを購入する企業層も大企業から中小企業へと広がりを見せており、保険業界においても市場の拡大が最も期待される商品の 1 つになっている。

現代は、自動車や家・家電製品の身近な製品から社会インフラに至るまで、あらゆるものがコンピューターで制御されている時代であり、また今後はウェアラブル端末やド

[50] Marsh ウェブサイト（2014.9）
[51] 現在はリスクとしては認識されていないものの、社会や環境の変化などにより、新たに現れたり、認識されるリスクのこと。

ローン（無人飛行機）のビジネスへの活用等の保険業界にとっても未だ見ぬリスクが出現してくることが予測される。また、クラウド・コンピューティングの時代にあっては、サイバー・リスクは、集積しキャタストロフィー損害をもたらす可能性もある。さらに、サイバー・リスクについては、伝統的な賠償責任保険や財産保険にとどまらず、企業の役員に対するD&O保険のリスクへと広がりを見せている。

これらに対し、保険業界としては、顧客企業のニーズにあった保険カバーや保険金額（支払限度額）の提供、適切な保険料率水準の算出はもちろん、引受キャパシティの確保、企業のリスク認識に有用となるようなアンダーライティング手法の実施が必要である。さらに、保険は企業のリスクマネジメント手段の1つに過ぎず、その他のリスクマネジメント・サービス（サイバー・リスクへの対処能力の向上に向けた教育プログラムの提供、原因究明や被害の拡大防止、再発防止のための支援、適切な情報開示のアドバイス等）の提供が重要であると考える。

当然ながら、わが国を含めた米国以外の国にもサイバー・リスクおよび対応する保険も現存しているが、インターネットを通じサイバー空間ではすでに世界は1つとなっており、先進的な米国の動向や保険業界が抱えている課題等は、わが国の損害保険市場にも大きな影響を与えると考えられることから、引き続き米国等の動きを注視していくこととしたい。

本稿が、米国のサイバー・リスクおよびサイバー・インシュアランスに関する動向やその影響をより理解していただく一助になると幸いである。

＜参考資料＞

・株式会社シマンテック“2013 年ノートンレポート”
・谷脇康彦「ミッシングリンクーデジタル大国ニッポン再生」
・谷脇康彦「わが国のサイバーセキュリティ戦略」内閣官房情報セキュリティセンター（2014.7）
・独立行政法人 情報処理推進機構「クラウドコンピューティングの社会インフラとしての特性と緊急時対応における課題に関する調査－概要報告書－」（2012.9）
・内閣官房情報セキュリティセンター「サイバーセキュリティ 2014」（2014.7）
・長尾慎一郎「サイバー攻撃によるインシデントの開示に係る SEC の取り組みとわが国の状況」EY 情報センサーVol.95（2014.7）
・廣岡知「急拡大する米国サイバー保険市場」Global Insurance Topics Vol.13（損保ジャパン日本興亜総合研究所、2013.6.15）
・ベーカー&マッケンジー法律事務所“Client Alert”（2014.4）
・ベライゾン・ジャパン“2014 年度データ漏洩/侵害調査報告書”（2014.4）
・Advisen,“D&O Claims Trends：Q2 2013”（2013.7）
・Allianz Global Corporate & Specialty, “Allianz Risk Barometer on Business Risks 2014（2014.1）”
・Aon “Cyber Exposures and Solutions in Asia”（2014.4）
・Aon“European Union cyber exposure and solutions”（2013.9）
・Center for Strategic and International Studies,“Net Losses: : Estimating the Global Cost of Cybercrime（2014.7）”
・DLA Pipper “Data protection laws of the world”（2014）
・Ernst & Young“2014 Global Insurance Outlook”（2014）
・Guy Carpenter “Emerging Risks Report - Ahead of the curve：Understanding Emerging Risks”（2014．9）
・IDC/NUS“The Link between Pirated Software and Cyber security”（2014.3）
・Identity Theft Resource Center,“2013 Data Breach Stats-A Study of Actual Claim Payout-”
・Insurance Information Institute,“Cyber risks：The Growing Threat”（2013.4）
・Insurance Information Institute,“Cyber risks：The Growing Threat”（2014.7）
・Insurance Services Office, Hanover Research, “Cyber Insurance Survey”（2014.11）
・Jenner & Block“Insurance Litigation and Counseling Practice Advisory”（2011．10）
・Kevin M.LaCroix,“The D&O Diary”（2014.2）
・Kevin M.LaCroix,“The D&O Diary”（2014.5）
・Lewis Brisbois Bisgaard & Smith LLP, Insurance Information Institute, Pwc“Practical Strategies to Address Cyber Risk in Your Business”（2014.11）
・Marsh,“Benchmarking Trends: Interest in Cyber Insurance Continues to Climb”（2014.4）
・Marsh,“Benchmarking Trends: More Companies Purchasing Cyber Insurance ”（2013）
・Marsh,“Cyber Crime In Asia：A Changing Regulatory Environment”（2014）

・Marsh,“United States Insurance Market Report 2014”（2014.2）
・NetDiligence,“Cyber Liability & Data Breach Insurance Claims 2013”
・Ponemon Institute,“Cost of Cyber Crime Study：Unites States2013”（2013.10）
・Ponemon Institute,“Cost of Data Breach Study2013: Global Analysis”（2013.5）
・Ponemon Institute,“Cost of Data Breach Study 2014: United States”（2014.5）
・Ponemon Institute,“Is your Company Ready for a Big Data Breach?”（2014.9）
・Ponemon Institute,“Managing Cyber Security as a Business Risk：Cyber Insurance in the Digital Age”（2013.8）
・PWC Global State of information Security Survey 2014（2014.9）
・Risk Based Security,“Data Breach Quick View-Data Breach Trends during the First Half of 2014”（2014.7）
・Swiss Re, Sigma “Liability claims trends: emerging risks and rebounding economic drivers”（2014）
・The Betterley Report,“Cyber/Privacy Insurance Market Survey”（2014.6）
・Zurich American Insurance Corporation“Data Breach Cost”（2012）

＜参考サイト＞

・サイバーインシデント・レポート・ウェブサイト
・独立行政法人情報処理推進機構ウェブサイト
・内閣官房情報セキュリティセンターウェブサイト
・みずほ情報総研ウェブサイト
・Ace ウェブサイト
・AIG ウェブサイト
・Chubb Group ウェブサイト
・Philadelphia ウェブサイト
・Home Depot ウェブサイト
・Insurance Journal ウェブサイト
・Insurance Services Office ウェブサイト
・IT Media ウェブサイト
・National Conference of State Legislatures ウェブサイト
・Target ウェブサイト
・Travelers ウェブサイト
・U.S. Securities and Exchange Commission ウェブサイト