実務解説

インシデント発生前の予防を
サイバー保険導入・活用のポイント

オリックス株式会社 投融資管理本部 ポートフォリオ管理部
担当部長 山越誠司

共立インシュアランス・ブローカーズ株式会社 企業営業本部
営業第二部長 瀧山康宏

サイバー保険は企業にとってどのような効用があるのか理解が難しい保険である。そもそも，サイバーリスクの実態把握も困難な状況なので当然である。本稿においては，先行して普及しているアメリカの状況などにも触れながら，日本企業にとってのサイバー保険の活用法について検討してみたい。特に大企業と中小企業では，同列に論じることができないが，どちらもサイバーリスクへの対策は重要な経営課題である。

I はじめに

近年，サイバーリスクに対する脅威が高まっている。たとえば技術的リスクとして，自動車の車載システムが遠隔で不正操作され，偽メッセージが送信されたり，メーターが操作されたりする危険性が指摘される[1]。また，ビジネス的リスクとしては，一旦，消費者からのセキュリティに対する信頼を失うと，消費者が自社に戻り収益が改善するまでの逸失利益が膨大になることが懸念される。このように，一度，サイバーセキュリティに問題が生じると，企業経営に甚大な被害をもたらすため，リスクへの予防や対応は慎重を期する必要がある。特に初期対応を確実にするためにもサイバー保険の検討は大企業でも中小企業でも必要になってこよう。

II 中小企業にこそ有益なサイバー保険

アメリカにおけるサイバー保険の市場は，2014年の総保険料で約2,000億円の規模と言われている[2]。そして，サイバー保険を提供する保険会社も60社程度存在している。また，世界のサイバー保険市場では，アメリカが90％を占めると言われており，10年後には全世界において保険料で２兆円規模の保険市場に成長すると予想されている[3]。

日本に比べて，アメリカでサイバー保険が普及している理由のひとつに法規制がある。

[1] 岩井博樹「自動車セキュリティで懸念されるサイバーリスクと現状の脅威」安全工学54巻６号425～427頁（2015年）。
[2] Financial Services Sector Coordinating Council, *2016 Cyber Insurance Buying Guide*, American Bankers Association 2 (2016).
[3] Allianz Global Corporate & Specialty, *A Guide to Cyber Risk*, Publication 5 (2015).

アメリカの各州では，データ侵害通知法が制定されており，その法規制が各企業にサイバー保険の購入を促した経緯がある。法の目的は，個人情報が盗取された，あるいは侵害された可能性がある場合は，消費者に確実に通知することを要請し，消費者を保護することにある。さらに，もう一点，サイバー保険の普及を後押しする事象として，犯罪組織が，支払詐欺や窃取した個人情報を利用した犯罪等が，組織として旨味のあるビジネスであるということに注目し始めたこともある[4]。皮肉にもサイバー犯罪の増加が，サイバー保険の必要性を認識させるきっかけになっているわけである。

このように犯罪組織の暗躍が注目されるわけであるが，一般的にひとつの誤解があると言われる。すなわち，犯罪組織は世界的な多国籍企業をターゲットにしているということである。しかし，むしろサイバー攻撃に対する脆弱性からすると，セキュリティ方針や手続に不備がありがちな中小企業がサイバー犯罪組織から狙われるということを認識しておく必要がある。

このような状況で，特に財務基盤が脆弱な中小企業にとってサイバー保険が，リスク管理の道具として有用であると言える。なぜなら，一旦データ侵害が発生すると，被害の甚大さのために危機対応費用や弁護士費用，あるいは損害賠償金が負担しきれないほど高額になる可能性があるためである。さらに，中小企業は危機発生時のサイバーセキュリティの専門家，フォレンジック調査会社，サイバーリスク専門弁護士などとのネットワークも不足しているため，保険会社を通じて専門家を紹介してもらい，適切な初動をとることもひとつの実用的な活用方法である。

Ⅲ 大企業における サイバー保険の課題

サイバー保険は，大別すると２種類の補償で構成されている。①自社損害の補償（First Party Coverage），②第三者損害賠償責任の補償（Third Party Liability Coverage）である[5]。自社損害の補償の具体的な例としては，データ侵害の通知費用，弁護士費用，フォレンジック調査費用，危機管理費用，事業中断に伴う損失，恐喝に伴う支払などがある。第三者損害賠償責任の補償は，情報漏えいやネットワークセキュリティへの侵害，人格権侵害，知的財産の侵害などが原因で，第三者から損害賠償請求された場合の補償である。次頁**【図表】**は，サイバー保険と既存の損害保険商品との比較であるが，その他の保険では対応できないリスクがあることが理解できよう。

このように，サイバー保険がサイバーリスクに対して有効な保険であることは理解できるが，特に大企業にとっては，活用しようと思うと実務的な問題が発生する。すなわち，どの保険会社も自社のリスク管理の観点から，10億円以上の支払限度額は提供しない傾向がある。結果的に，保険ブローカーを通して複数の保険会社を積み上げ，高額な支払限度額を設定する必要が出てくる。実際，海外では400億円から500億円程度の支払限度額を確保した事例[6]はあるようであるが，非常に複雑な手続が必要になってくるであろう。そもそもサイバーリスク自体も新しいリスクで，リスクの見極めが難しいので，保険料が高額になりがちである。よって，合理的な保険料で適切な支払限度額を確保するためには，大企業として高額の免責金額（自己負担

[4] Robert Jones「サイバー保険に関してすべてのCISOが知っておくべきこと」シマンテック・ホワイトペーパー8頁（2015年）。
[5] 牛窪賢一「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」損保総研レポート116号13～14頁（2016年）。
[6] Willis Re, *Market Realities 2017 : Spring update*, 14 (2017).

【図表】サイバー保険と既存の損害保険商品の比較

	損害の種類	犯罪保険	CGL保険	誘拐保険	業務過誤保険	D&O保険	財物保険	サイバー保険
自社損害	事業中断損失							✓
	第三者によるコンピューター犯罪	✓						✓
	従業員による妨害行為	✓						✓
	レピュテーション・リスクに対する広報活動費							✓
	侵害発生の消費者への通知費用							✓
	恐喝による支払			✓				✓
	災害によるデータ損壊						✓	
第三者賠償責任	データ侵害による顧客情報の漏えい				✓	✓		✓
	取引先へのネットワーク・セキュリティの損害							✓
	人格権侵害		✓		✓	✓		✓
	規制当局の調査費用				✓	✓		✓
	防御費用				✓	✓		✓

出典：American Bar Association, *Protecting Against Cyber Threats—A Lawyer's Guide to Choosing a Cyber-Liability Insurance Policy*（2016）を元に筆者作成

額）を採用するなど工夫が必要である。

それでも，サイバー保険の購入を検討する価値はある。実際に，アメリカの小売業ターゲット社は，データ侵害によって4,000万人の顧客情報が盗取された後，速やかに規制当局へ通知していないこと，および顧客への正確な通知を怠ったことで，株主から役員に対して代表訴訟を提起され，さらには，会社としての危機管理対応費用や弁護士費用に300億円も負担したということである。そして，サイバー保険は自家保険部分の約10億円を含めて，合計100億円程度の支払限度額が手配されていたが[7]，合計の損害額をカバーするには不十分であった。そして，この事件を単なる情報セキュリティの管理ミスと捉えるのは誤りで，どんなに高度な対策を施していても，それを上回るサイバー攻撃が実行されることがあるということを認識しておく必要がある[8]。

Ⅳ 日本企業におけるサイバーリスク対策

経済産業省と独立行政法人情報処理推進機構は2015年に「サイバーセキュリティ経営ガイドラインVer1.0」を策定しており，昨年11月には改訂版も発行され[9]，CISO（Chief Information Security Officer）に指示すべき「重要10項目」がまとめられている。また，独立行政法人情報処理推進機構からは，対策に経営資源を割けない中小企業向けに「中小企業の情報セキュリティ対策ガイドライン」[10]が

[7] Business Insurance, Target has $100 million of cyber insurance and $65 million of D&O coverage, 19th January, 2014.

[8] 長尾慎一郎「米国の実例とセキュリティ政策からみたサイバーリスクへの備えと情報開示の考え方」旬刊経理情報1406号58頁（2015年）。

[9] 経済産業省＝独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドラインVer2.0」（2017年）。

示され，行政サイドからもサイバーリスク対策を後押ししている。他にもさまざまな対策ガイドが出ているが，一貫して主張されているのは「サイバーリスクは経営者が関与すべきリスク」としている点である。日々巧妙化するサイバー攻撃に対応するには，現場任せの対応では対処しきれず，各企業では自社のサイバーリスクに見合った対策を経営者主導で検討する必要があろう。

日本企業のサイバー対策について，大企業ではCISOを任命し，SIRT（Security Incident Response Team）の設置を行いサイバー攻撃に負けない経営を目指すところが増えてきている。経営者もサイバーリスクについては積極的に関与し，インシデントの発生報告もすぐに経営層まで上がる態勢構築も行い始めている。もちろんIT技術については専門チームが対応している訳だが，経営層とのコミュニケーションをうまく取りながら対策費を確保しセキュリティ投資を行っているようである。

一方，近年発生している個人情報漏えい事故を見ると，たとえば2016年に発生した大手旅行会社の個人情報えい事故の際は，経営層へのインシデント報告がすぐには上がらずに被害を拡大させてしまい，社内態勢の問題が露呈されてしまった。また，2018年５月に施行されるEU一般データ保護規則（General Data Protection Regulation/GDPR）については，新聞記事にも多く掲載されていることから認識している企業は増えてきたものの，まだまだ十分なサイバーリスク対策ができていない企業のほうが多いと推察される。日本国内だけの現状からするとリスクの大きさを実感できないこともあるのかと思うが，サイバー空間の恐ろしさを知ると対策の必要性が理解できると思われる。

少し古い事例であるが，2009年にイランの核燃料施設に対し，スタックスネットというマルウェアによるサイバー攻撃が行われ多数の遠心分離機が制御不能となった事故が発生している。この施設では安全性確保のためインターネット等の外部ネットワークから隔離されていたにもかかわらず，技術者のパソコンがUSBメモリ経由でマルウェアに感染し，施設の中央制御システムと接続した際に感染が広がった。この事件ではウィンドウズの脆弱性を悪用し，メーカー側もまだ知らないプログラムの欠陥をつく「ゼロデイ攻撃」（ウィンドウズ修正プログラムが提供される前に仕掛ける攻撃）が行われた。その後も国の重要なインフラに対する攻撃や産業スパイを目的としたハッキングは頻繁に行われているが，この脆弱性を利用したサイバー攻撃は頻発しており，「ゼロデイ脆弱性」が商品として闇市場で高値で取引されている状況である[11]。テクノロジーの発達は，人々の生活が便利になる反面，犯罪行為や破壊行為を行う人達に武器を提供している部分もあり，法の秩序が確立されていないサイバー空間は，国家やテロリスト，産業スパイなどが標的を攻撃する格好の舞台にもなっている。これまで仮想空間という認識だったサイバー空間が現実の一部になってきており，企業のリスクマネジメントを考えた場合，経営者はサイバーリスクを単なるIT部門が対応するリスクではなく，自然災害リスクや製造物責任などの賠償責任リスク等と同列に位置づけし，ビジネスリスクのひとつとして捉え対策を講じる必要がある。

[10] 独立行政法人情報処理推進機構「中小企業の情報セキュリティ対策ガイドライン第2.1版」（2017年）。
[11] 山田敏弘『ゼロデイ――米中露サイバー戦争が世界を破壊する』（文藝春秋，2017）46頁。

Ⅴ わが国のサイバー保険市場

最近の新聞にもサイバー保険関連の記事がみられるようになり，この保険の注目度も上がってきたように思われるが，欧米ではすでに加入率がかなり高くなっている現状に比べ，日本ではサイバーリスク担当者と保険購入の担当者が異なっているため検討がされないことや，国内では賠償事故に発展するケースが少ないことから普及が進んでいないと思われる。しかし最近では，保険会社もインシデント発生時の補償以外の付帯サービスを厚くした商品を投入するなど，普及に向けた動きが出てきた。ある大手損害保険会社では，シリコンバレーのIT企業と提携し，保険契約者には企業が晒されているサイバーリスクの要因を分析したレポートやサイバーリスク関連の情報誌を提供するなどのサービスを提供しており，付帯サービスを目的に契約をする企業も出ているようだ。また，他の損害保険会社では事故発生時にどの程度の損害が発生するのか簡易診断サービスを提供しており，予想損害額を想定するうえで，一定程度参考となるデータを提供してくれる。

日系企業の海外拠点ではサイバーリスク保険に対する関心が高まっていることもあり，海外拠点からの声をきっかけに日本本社でも検討を始めるケースも出ている。そもそもサイバー空間に国境はないことから，海外拠点では検討するが日本では検討しないという選択肢はないはずである。したがって今後日本でもこのサイバー保険市場が拡大することは間違いないであろう。

Ⅵ おわりに

繰り返しになるがサイバーリスクはビジネス上のリスクのひとつであり，教科書的ではあるが，リスクシナリオを想定し，どの程度の損害が発生する可能性があるかシミュレーションを行い，その損害に対しリスクの保有，軽減，回避，転嫁を検討し，転嫁するのであればサイバー保険を購入するというプロセスを踏むことが肝要かと思う。また，サイバー保険を検討する場合，損害賠償リスクや自社の利益喪失リスクをヘッジする観点と保険会社が持つ付帯サービス利用の２つの観点から検討するのがよいと思われる。

また，発生確率は少ないリスクかもしれないが，発生した場合のインパクトは非常に大きいため，インシデントが発生する前にしっかり対策を立てておくことは，事業継続の観点から必須の状況にある。そのため，保険を利用したリスク転嫁策について検討することは，結果的に保険を購入しない場合でも，その過程で自社の抱えるリスクが明確化され，自社の財務体力に基づくリスク保有可能額を把握することなどを通じ，リスクマネジメントに対する姿勢がこれまで以上に強化されることとなり，価値ある取組みとなることは間違いないと言える。

山越誠司（やまこし　せいじ）
1993年日産火災海上保険株式会社入社。その後，オリックス株式会社でリスク管理業務やフェデラル・インシュアランス・カンパニーで経営保険の営業・引受業務などを経験し，2016年より現職。東洋大学大学院法学研究科博士前期課程修了。本稿Ⅰ，Ⅱ，Ⅲ執筆担当。

瀧山康宏（たきやま　やすひろ）
1993年日産火災海上保険株式会社入社。その後，AIU保険会社，MSTリスクコンサルティングを経て2010年より現職。グローバルプログラムや経営保険のスキーム構築業務を担当。中央大学経済学部産業経済学科卒業。本稿Ⅳ，Ⅴ，Ⅵ執筆担当。