

サイバー攻撃についての新常態(ニュー・ノーマル)

– 政府による調査への対応と保険金の回収 –

ジョセフ・D・ジーン、キャロリーナ・A・フォルノス、ブライアン・E・フィンチ

- サイバー攻撃による被害を受けた企業は、同情を受けることはなく、規制当局による調査の対象となることに留意する。
- 会社役員賠償責任(D&O)保険により、訴訟費用だけでなく、調査費用もカバーすることができ得ることに留意する。
- 会社役員賠償責任(D&O)保険及びエラーズ・アンド・オMISSION(E&O)保険の契約条項如何により、想定されるリスクを軽減することができる。

著名な企業が数千万の顧客に関する記録を失うというようなデータ漏洩の被害を受け、そればかりか州司法長官が企業や役員に対して早々に調査を開始し、訴訟を提起することで問題が一層深刻になるというような目を覆いたくなるような事態が現在頻発しています。貴社の保険は、上記のような州司法長官の請求に対する防御に関連する費用をカバーしているでしょうか？

今日、米国においては、州司法長官がデータプライバシー及び不正・虚偽広告関連法に基づく請求権限を積極的に行使して、サイバー攻撃の責任を追及していることが背景事情として厳存しています。

過去 10 年間に、全米で制定・改正されたデータプライバシー保護法の数は爆発的に増加しています。現在、ほぼすべての州において、あらゆる形式・規模の企業に対して、「個人を特定し得る情報」(personally identifiable information, “PII”) (州によって異なりますが、典型的には氏名と社会保障番号、クレジットカードその他の支払用銀行口座番号、又は運転免許証番号等の固有番号との組み合わせを意味します。)が、いつ許可なしにアクセスされ、又は漏洩されたのかを開示することを要求する法律が制定されています。

これらの法律に基づき、企業は、影響を受ける個人に通知するだけでなく、それらの者に対し、典型的には与信監視サービスへの無料アクセスなど、何らかの形式による請求を認めることに対応することを求められます。さらに、データプライバシー保護法は、通常、州司法長官に対して、データベースの漏洩があった企業に対する訴訟を提起する権限を与えています。このような措置は、当

初は最も重大なデータ侵害(極端に大規模な場合、又はセキュリティの不備が企業側の重大な過失によるものである可能性がある場合)に対して講じられていました。しかし、現在は、データ侵害が発生したというニュースがあったという事実だけでも、司法長官が訴訟を提起するケースが増えています。企業にとって最も厄介なのは、違反がどのように発生したのか、又は誰がそれを行ったのかを把握する前に、訴訟を提起される可能性があるということです。

そのような調査は、費用が嵩み、長引き、企業の日常業務を阻害することになります。役員らは、多くの場合、自らが司法長官や民事訴訟の原告らによる証言録取手続への対応に迫られると同時に、不正行為又は顧客のデータ保護に対する関心の欠如について、報道機関の激しい非難を浴びることにもなります。サイバー攻撃に対する責任を最終的に誰が負うかを判断するために数ヶ月から数年を要するとしても(連邦法執行機関や国家安全保障機関が確定的な結論を下すためのリソースも必要となるでしょう)、内部調査、和解交渉、又は訴訟のコストは、企業の日々の業務を著しく阻害する可能性があります。

民事調査請求・召喚状に対するマネジメント及び対応戦略

サイバー攻撃が発生した場合、民事調査請求(CIDs)又は召喚状(subpoenas)が届く可能性があります。どのように対応するかが重要になります。企業は、政府から要求された情報の範囲、使用された用語、及び影響を受ける期間を把握するために、召喚状、民事調査請求その他の調査請求を慎重に検討する必要があります。そのために、政府による調査への対応経験のある弁護士に相談することが非常に望ましいといえます。弁護士は、政府担当官と対話して、政府から要求されている情報に適切に対応することができます。また、(i)政府が求めている関連情報の対象を効果的に限定し、(ii)政府の要求に効率的に対応し、そのような情報の収集に伴う混乱を最小限に抑えるために、要求の範囲を狭めることができるかどうかの検討を支援することができます。さらに、サイバー攻撃の犯人を特定するために政府に協力する可能性についても助言することができます。これらの初動は、政府の状況認識と調査全体を通じた政府による企業の扱いに多大な影響を与えます。加えて、企業は、政府の要求から生じ得る潜在的なリスクや責任に対処するために、たいいていの場合社内調査を実施するでしょう。

データ侵害・サイバーセキュリティ調査についての保険の適用範囲

データ侵害に対する政府による調査への対応を余儀なくされた場合、サイバー関連攻撃の標的となった企業には多大な費用負担が生じることが予想されます。そのような調査によって生じる、侵害自体の損害額以外の費用としては、以下のものが含まれます。

- 召喚状、民事調査請求その他の情報請求の検討、並びに、要求された書類の精査及び提出に要する外部の弁護士への相談料
- 企業が委託した内部調査の費用
- 州司法当局その他の執行機関及び担当官との継続的やり取りに関する外部弁護士への相談料
- 調査又は結果として生じる訴訟に関連する和解又は決定に要する費用

さらに、データ侵害に対する政府による調査が公表されることで、株主代表訴訟並びに証券クラスアクション、及び「個人を特定し得る情報」(PII)を漏洩された個人による訴訟等を喚起する可能性があります。

これに対して、企業は、役員及び保険会社にこれらのコストを負担するように求めることができる可能性があります。例えば、会社役員賠償責任保険は、会社の役員、取締役及び従業員、場合によっては会社自体の「不正行為」から生じる「請求」を適用対象としています。各契約の文言によっては、調査関連費用が対象となる場合があります。保険会社またはブローカーが、「社会通念」上、保険契約では召喚状その他の調査対応費用は適用対象と解されない旨異議を述べる可能性があります。これらの請求を断念する必要はありません。第三者のベンダーは、データ侵害の被害を受けた企業に対して補償義務を負う場合があります。場合によっては、賠償保険に追加の被保険者として指定していることもあります。潜在的なあらゆる保険金の支払源を調査することをお勧めします。

召喚状対応費用への会社役員賠償責任保険の適用範囲の把握

召喚状(文書や証言の作成を指示する書面による命令)は、政府による調査で広く用いられ、往々にして、より大きな調査の第一歩となります。保険会社は、会社役員賠償責任保険契約の文言解釈として、召喚状が「請求」に含まれるという点に異議を申し立てることがあります。この問題については、様々な法域で、保険会社の解釈は誤りであるという合意が形成されつつあります。典型的な会社役員賠償責任保険には、以下のような「請求」の定義が含まれています。

- (1) 金銭的又は非金銭的救済の書面による要求
- (2) 金銭的又は非金銭的救済のための民事、刑事、行政、規制又は仲裁の手段であって、以下の行為により開始されるもの
 - (i) 訴えの提起その他これに類する申立て
 - (ii) 起訴、訴追、又はこれに類するもの(刑事訴訟の場合)
 - (iii) 被疑事実の告知の受領又は提出

いくつかの裁判所は、召喚状は「非金銭的救済の要求」に該当すると判断しています。

近年のニューヨークでの重要な裁判例である *Syracuse University v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.* において、ニューヨーク州最高裁判所は、控訴審判決を認容し、契約の「請求」の定義における「非金銭的救済」という文言の一般的意味内容として、性的虐待の調査に関連して米国司法省及び郡司法当局により発せられた召喚状が含まれると判断しました。同裁判所は、第二巡回控訴裁判所が「当裁判所は、召喚状は調査命令に「類似」しない「単なるディスカバリーの手段」であるとする保険会社の特殊な見解は採用しない。ニューヨーク州の判例法は、ニューヨーク州司法長官が権限を有する召喚状は主要な調査手段であることを明確にしている。」と述べて、召喚状の対応費用の範囲を明らかにした *MBIA Inc. v. Federal Ins. Co.* の判断に大きく依拠しました。*Syracuse University* のケースでも、裁判所は、ニューヨーク州法及び連邦法によれば、召喚状に従わないことは罰せられるべき罪とされていると指摘しました。

他の法域の裁判所も、召喚状の対応費用は会社役員賠償責任保険の適用対象となると判断しています。例えば、*Protection Strategies v. Starr Indem. and Liab. Co.* (バージニア州法を適用し、

航空宇宙局の召喚状および捜索差押許可状の対応費用が適用対象となると判断したケース)、*Minuteman International Inc. v. Great American Ins. Co.* (イリノイ州法を適用し、証券取引委員会の召喚状への対応費用が対象となると判断したケース)や *Polychron v. Crum & Forster Ins. Cos.* (アーカンソー州法を適用し、銀行の大陪審の召喚状への対応費用が適用対象となると判断したケース)などの判例があります。

裁判所は、召喚状及び民事調査請求についてのエラーズ・アンド・オMISSION保険契約の適用範囲についても判断しています。例えば、*Ace American Insurance Co. v. Ascend One Corp.* は、メリーランド州司法省から発行された行政召喚状、及び、テキサス州司法省から発行された民事調査請求の対象となった保険契約者に関するケースです。問題となったエラーズ・アンド・オMISSION保険契約にいう「請求」は、「告発、調査命令その他これに類する文書の提出によって開始された民事、行政又は規制上の調査」を含むと定義されていました。メリーランド州地区連邦地方裁判所は、メリーランド州法を適用して、召喚状と民事調査請求は、潜在的な消費者保護法違反の調査の一部であり、従って当該契約にいう「調査」であると判断しました。

その他の調査関連費用についての適用範囲

司法長官による調査に直面している企業は、召喚状への対応に加えて、多くのコストのかかる他の作業を行う可能性があります。例えば、場合によっては、当局から召喚状より先に非公式の接触がある可能性があり、そのような要請に応じるかどうか、どのように対処するかについて(多くの場合、外部の弁護士の助言を得て)決定する必要があります。上記 *MBIA* のケースで、第二巡回控訴裁判所は、証券取引委員会及びニューヨーク州司法長官による非公式の口頭による文書請求に自発的に従うことにより被保険者が負担する費用は、保険の適用対象となると判断しました。第二巡回控訴裁判所は、かかる非公式の行為は、正式な召喚状及び追加のパブリック・リレーション上の損害を免れる目的でなされたものであり、これに伴う費用は保険の適用対象となると判断しています。

調査中の企業は、政府による調査が公表されたことによる悪影響を管理するために、パブリック・リレーション会社、セキュリティサービス、及び他のベンダーと交渉することもあり得ます。これらの「間接的」な対応費用は、調査対応費用となり得ますが、保険の適用対象となるかどうかについての判例の蓄積は十分ではありません。しかし、「危機対応」カバレッジを含む保険では、ある程度の救済が認められる可能性があります。結果的に提起される株主訴訟も、会社役員賠償責任保険及びエラーズ・アンド・オMISSION保険契約における「請求」の定義に一般的に該当するため、適用対象となる可能性があります。

保険契約者のための実務上の留意点

政府の調査に対する保険適用の対象範囲を最大化するために、企業は以下の点に留意する必要があります。

- 能動的に行動すること。召喚状や「ターゲットレター」をジェネラル・カウンセルや法務部が受領する前であっても、会社役員賠償責任保険及びエラーズ・アンド・オMISSION保険契約における、比較的広い「請求」の定義について交渉するために、ブローカーと協力することをお勧めします。いくつかの新しい契約文言は、政府当局からの特定の「事前請求」の要求、具体的には執行当局との面談や会議に関連する費用(弁護士費用)を含む召喚状への対応費用の補償が保険の適用範囲に含まれます。適用除外条項についても精査する

必要があります。保険契約の文言を精査するために、専門の弁護士に相談することをお勧めします。

- 通知義務を理解し、遵守すること。政府の調査は正式な召喚状で開始することもあれば、事前に非公式に開始することもあります。貴社の会社役員賠償責任保険及びエラーズ・アンド・オMISSION保険契約の下で、請求の通知、又は請求を生じさせる状況の通知がいつ行われなければならないかを理解することが不可欠です。同様に、調査に対応するために、保険会社に対してどのような情報を提供し、協力する義務について理解することが重要です。最善の対応は、早急に専門の弁護士に相談することです（弁護士依頼者秘匿特権によって弁護士による助言の内容が保護されますが、ブローカーとの会話はそうではない可能性があるためです。）。

政府の調査に直面した場合、保険契約者は、潜在的に利用可能なすべての保険を慎重に検討する必要があります。多くの州によってルールは異なり、一部の法域ではこの問題に対処していません。保険契約者は、調査の対象となる前に、保険契約、法律、及びリスクを慎重に理解する必要があります。

サイバー、ホワイト・カラー、保険償還の各分野に精通する弁護士は、民事調査請求及び召喚状への対応に日々関与し、依頼者の対応戦略を立案するだけでなく、保険会社がその対応に伴う費用について保険金を支払う可能性を最大限に高めるための支援を行っています。我々は、多くの場合、比較的低コスト又は固定報酬で、状況を検討・分析することができます。それにより、我々は、積極的に依頼者の地位を向上させ、リスクを最小限に抑えることを支援します。

本稿の原文(英文)につきましては、[Cyberattacks Are the New Norm](#) をご参照ください。

本稿の内容に関する連絡先

木本泰介 (日本語版監修)
725 South Figueroa Street, Suite 2800
Los Angeles, CA 90017-5406
213.488.7113
taisuke.kimoto@pillsburylaw.com

Joseph D. Jean
1540 Broadway
New York, NY 10036-4039
212.858.1038
joseph.jean@pillsburylaw.com

Carolina A. Fornos
1540 Broadway
New York, NY 10036-4039
212.858.1558
carolina.fornos@pillsburylaw.com

Brian E. Finch
1200 Seventeenth Street, NW
Washington, DC 20036
202.663.8062
brian.finch@pillsburylaw.com

早瀬孝広 (日本語版作成協力)

Legal Wire 配信に関するお問い合わせ

Yoko Nagami-Rosasco
yoko.nagamirosasco@pillsburylaw.com

This publication is issued periodically to keep Pillsbury Winthrop Shaw Pittman LLP clients and other interested parties informed of current legal developments that may affect or otherwise be of interest to them. The comments contained herein do not constitute legal opinion and should not be regarded as a substitute for legal advice.
© 2017 Pillsbury Winthrop Shaw Pittman LLP. All Rights Reserved.