サイバー攻撃による業務停止リスクを想定した契約書改定のポイント

近年、ランサムウェアを中心としたサイバー攻撃が急増しています。被害により事業が停止することになれば、取引の納期を守れない等の債務不履行に陥ることとなり、賠償責任の問題が生じることもあります。そこで、こうしたリスクに備えるための契約書改定のポイントを解説します。

八雲法律事務所
弁護士・情報処理安全確保支援士
山岡裕明／千葉哲也／柏原陽平

急増するランサムウェアによる被害

ランサムウェアとは、「ランサム」（身代金）と「ソフトウェア」から成る造語です。ランサムウェアに感染すると、端末内のデータが暗号化され利用できなくなり、復号（復旧）の対価として身代金の支払いを要求されます。

昨今では、データの暗号化に加えて、データを窃取したうえで、そのデータを公開しないことの対価として身代金の支払いを要求されるケースもあります。

データの復旧および窃取したデータの非公開と引換えに身代金の支払いを要求される点で、「二重の脅迫」とも呼ばれています。

昨今頻発しているランサムウェア攻撃は、事業基盤たる情報システムを暗号化して停止に追い込む点で、事業の中断を引き起こすほどのリスクに、その深刻度が増しています。

たとえば、工場制御システムを構成する電子ファイルが暗号化されて同システムが停止すると、企業の製造・販売業務は中断を余儀なくされます。

また、送金システムを構成する電子ファイルが暗号化された場合、金融サービスは中断に追い込まれることになりかねません。

TrendMicro 社・CIO Lounge「サイバー攻撃による法人組織の被害状況調査（2023年6月調査）」によると、ランサムウェア攻撃による業務停止期間は、国内拠点で平均13日、ランサムウェア被害経験組織の累計被害額の平均は1億7689万円となっており、事業に対して深刻な被害が引き起こされていることがわかります（**図表1・2**）。

このように深刻な事業中断を引き起こすという意味において、サイバー攻撃のなかでもランサムウェア攻撃は、サイバーリスクのゲームチェンジャーといえます。ランサムウェア攻撃は、企業として看過できない重大かつ緊急性の高いリスクになりつつあることがわかります。

契約によるコントロールの必要性

サイバー攻撃により企業から情報が窃取される場合、窃取の対象となる情報は、個人情報に限りま

せん。

近時のランサムウェア攻撃においては、企業内のネットワークに侵入してファイルサーバから大量のデータが窃取されます。

通常、このファイルサーバには、個人情報だけではなく、自社で作成した機密性の高い企業情報に関する電子ファイルや、取引先から受領した電子ファイルも多数含まれます。

取引先との秘密保持契約上、秘密情報として扱われる電子ファイルが攻撃者により窃取された場合、企業は、当該取引先から秘密保持義務違反を理由とした債務不履行責任を問われかねません。

また、同じくランサムウェア攻撃において、前述のとおりネットワーク内の重要なファイルやデータが暗号化されてしまい、事業用システムに障害が発生するケースもあります。

これにより、納品の遅れやサービスの一時中断が生じた場合、履行遅滞、不完全履行や履行不能といった債務不履行責任が発生し得ます。

サイバー攻撃を受け、企業と契約関係にない個人（たとえば被害企業の顧客や、取引先担当者）の個人情報が漏えいすると、企業は個人からプライバシー権の侵害を理由とした不法行為に基づく損害賠償請求を受けることになります。不法行為責任については、事前に契約書でリスクをコントロールすることは困難です。

他方で、取引先との関係では秘密保持義務違反の場合であれ、履行遅滞、不完全履行や履行不能の場合であれ、一般的には債務不履行という契約責任の問題が生じます。契約責任である以上は、契約によるリスクコントロールが可能となります。

契約によるリスクコントロールを考えるうえでは、自社がサイバー攻撃を受けた場合と、取引先がサイバー攻撃を受けた場合のそれぞれのリスクを想定して、契約条項を考える必要があります。

自社がサイバー攻撃を受けた場合に備える条項

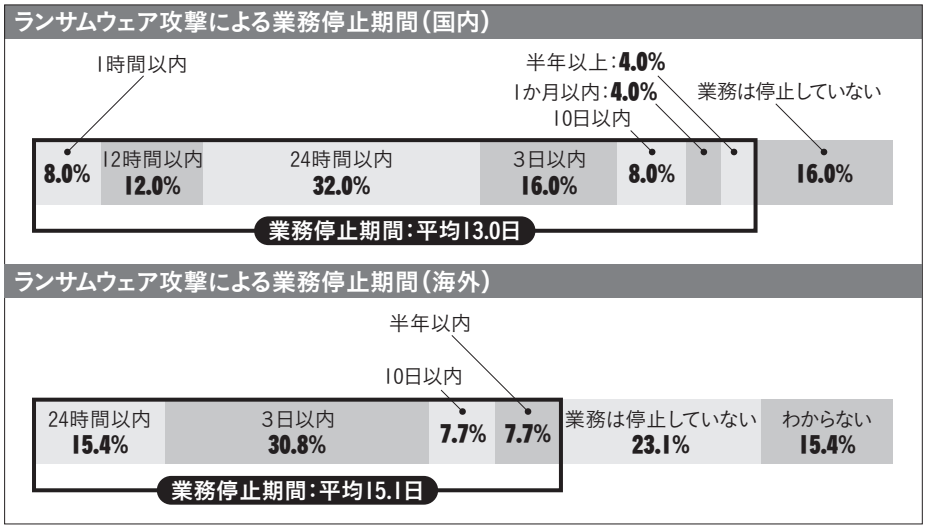
(1) 不可抗力条項

契約実務においては、天災や戦争等の不可抗力が原因で発生した債務不履行について債務者が債務不履行責任を負わないことを規定します（いわゆる不可抗力条項）。

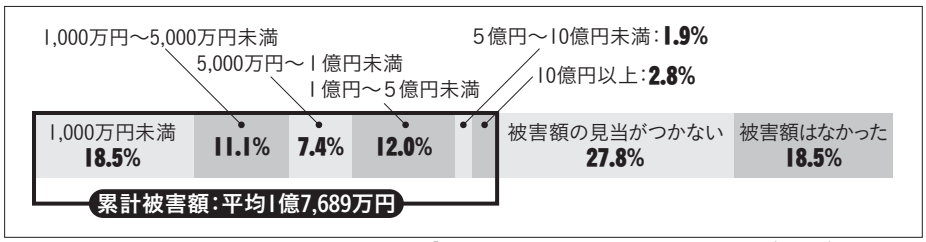
実際にサイバー攻撃により債務不履行が生じた場合、仮に「戦争、テロ行為……その他の不可抗力により」といったいくつかの事由が例示列挙された不可抗力条項が存在したとしても、「サイバー攻撃」が不可抗力事由として具体的に規定されていないと、不可抗力事由に該当するか否かが当事者間で争点となる可能性が高く、最悪の場合には、サイバー攻撃が不可抗力事由に該当しないという判断が下される可能性があります。

そのため、自社がサイバー攻撃を受けた場合のことを想定し、債

図表1　ランサムウェア攻撃による業務停止期間



図表2　ランサムウェア被害経験組織の累計被害額



図表1・2出典：トレンドマイクロ株式会社とCIO Loungeによる「サイバー攻撃による法人組織の被害状況調査」（2023年）

務不履行責任を免れるべく不可抗力事由としてサイバー攻撃を明記しておくことが契約実務上有用といえます（**条項例1**）。

ただし、不可抗力条項は万能ではありません。不可抗力事由としてサイバー攻撃を明記した場合であっても、常に責任を免れることができるわけではなく、相当の注意をすれば防止できるサイバー攻撃については、免責が認められない可能性が高い点に留意が必要となります。

(2) 賠償制限条項

民法上、債務不履行に基づく損害賠償は、通常生ずべき損害（通常損害）、および当事者が予見すべきであったときは、特別の事情によって生じた損害（特別損害）について認められています（民法416条1項、2項）。

そのため、契約実務においては、多額の損害賠償責任を免れるために、損害賠償の範囲を通常損害に限定したり、賠償すべき損害額に一定の上限を設けたりすること（このような条項を以下「賠償制限条項」といいます）が一般的に行なわれています。

この点、企業がサイバー攻撃により事業の中断に追い込まれ、取引先に対して債務不履行を起こした場合、同時に多数の取引先との関係で債務不履行責任を問われる可能性があります。そのため、民法が直接適用されると、企業にとっては、全体として多額の損害賠償責任を負わなければならない事態が想定されます。

そこで、不可抗力条項と同様に、自社がサイバー攻撃を受けた場合のことを想定すると、責任を負う場合および賠償の範囲を限定する賠償制限条項を定めておくことが望ましいといえます。

ただし、賠償制限条項を定めたとしても、債務者の故意または重過失による債務不履行の場合には、賠償制限条項が無効、または適用されないと解されることが可能である点に注意が必要です（東京地判平成26年1月23日判時2221号71頁は、開発を委託したウェブサイトにおける商品の受注システムの脆弱性により、顧客情報が漏えいした事案において、裁判所は、賠償制限条項について、損害賠償額を一定の範囲内に制限することにより、契約金額を低額に設定することができる機能に一定の合理性があるとして、その有効性を認めつつ、権利・法益の侵害について故意または重過失がある場合にまで、当該条項により損害賠償が制限されるとすることは、著しく衡平を害し、当事者の通常の意思に合致しないとして、受注者に故意または重過失がある場合には、賠償制限条項が適用されないと判示しています）。

なお、**条項例2**(1)においては、損害賠償の範囲について「直接かつ現実に発生した損害の範囲」というように抽象的に限定するに留めていますが、条項例2(2)のように取引先から契約に基づいて受領した金額を上限としたり、利用料数か月分を上限としたりするといったように、損害賠償の金額を具体的に限定する条項を加えることも一案です。

取引先がサイバー攻撃を受けた場合に備える条項

(1) 期間を明示した報告義務条項

取引先がサイバー攻撃を受けた場合、早期に事態を把握することができれば、自社としても被害の拡大を防止するための措置を講ずることができます。

また、個人情報保護法（以下「個情法」といいます）上、個人情報取扱事業者は、不正の目的をもって行なわれたおそれがある個人データの漏えい等が発生し、または発生したおそれがある事態が生じたときは、当該事態が生じた旨を個人情報保護委員会に報告しなければなりません（個情法26条1項本文、個情法施行規則7条3号）。

この報告義務の主体については、個人データの取扱いを委託している場合、原則として委託元と委託先の双方が報告する義務を負います（個情法ガイドライン［通則編］3－5－3－2。ただし、委託先が、報告義務を負っている委託元に当該事態が発生したことを知った後、速やかに通知したときは、委託先は報告義務を免除される［個情法26条1項ただし書、個情法施行規則9条］）。

報告の時期については、当該事態を知った後、速やかに「速報」をするとともに、60日以内に「確報」をしなければなりません（個情法施行規則8条1項、2項）。

「速やか」の日数の目安については、個別の事案によるものの、個人情報取扱事業者が当該事態を知った時点からおおむね3日～5

日以内とされています（個情法ガイドライン［通則編］3－5－3－3）。

そのため、自社の被害の拡大防止を図るとともに、委託先を適切に管理し、個情法上の義務を全うするという観点からは、取引先がサイバー攻撃を受けた場合、またはそのおそれがある場合には、適時に報告させるとともに、必要な調査や協力（ログ等の証拠保全を含みます）をさせる条項を設けることが望ましいといえます。

この点、実務的には「すみやかに」報告することや「遅滞なく」報告することを定めたり、「ただちに」報告することを定めたりすることが行なわれています。

もっとも、期限が曖昧になることを避けるという観点からは、たとえば、発覚から2日以内等と具体的に期限を明示することが望ましいといえます（**条項例3**）。

(2) 足並みを揃える条項

個人データの取扱いを委託している場合、前述のとおり原則として委託元と委託先の双方が報告する義務を負います。

委託先が委託元に報告することなく、または委託元への報告に先行して、個人情報保護委員会に報告したり、本人通知を実施したりすると、委託元としては準備が十分ではない状態で、個人情報保護委員会や個人から問い合わせを受けることになり、業務に支障が出かねません。

また、個人情報が漏えいした個人としても、委託先から本人通知が届き、後日、ほとんど同じ内容の本人通知が委託元から届くのは煩雑といえます。

そこで、委託元としては、こうした事態を避けるべく、委託元の了解なく個人情報保護委員会への報告や本人通知を行なってはならないという内容を定めることで、委託元と委託先とで足並みを揃えて個情法上の対応を進めるのも実務上有用といえます（**条項例4**）。

条項例

条項例1　サイバー攻撃が不可抗力事由として列挙されている条項

当社は、天災地変、火災、戦争、テロ行為、疫病の蔓延、法令の改廃、悪意の第三者によるサイバー攻撃その他不可抗力により、利用者が本サービスを利用することができなくなった場合であっても、これにより利用者に生じた損害について、一切の責任を負わないものとする。

条項例2　故意・重過失の場合に責任を負い、軽過失の場合を免責する条項

(1) 損害賠償の範囲を抽象的に限定

本サービスの利用に関して利用者に生じた損害については、当社の故意または重過失によるものである場合に限り、直接かつ現実に発生した損害の範囲でのみ賠償するものとする。

(2) 損害賠償の範囲を具体的に限定

① 本サービスの利用に関して利用者に生じた損害については、当社の故意または重過失によるものである場合に限り、受領済み報酬額を上限として賠償するものとする。

② 本サービスの利用に関して利用者に生じた損害については、当社の故意または重過失によるものである場合に限り、利用料3か月分相当額を上限として賠償するものとする。

条項例3　報告義務を定める条項

乙は、サイバー攻撃を受けた場合、またはそのおそれがある場合、発覚から2日以内に甲に報告するとともに、甲の指示に従い、乙の費用負担による必要な調査および協力を行なうものとする。

条項例4　個人情報保護法上の対応の足並みを揃える条項

乙は、事前の甲の承諾なくして、個人情報保護委員会等への報告や本人への通知を行なってはならない。

八雲法律事務所　サイバーセキュリティ法務に特化した法律事務所。八雲Security & Consulting株式会社とともに企業のサイバーセキュリティ体制構築支援やサイバー攻撃を受けた際のインシデントレスポンス支援を専門とする。主な編著に『実務解説 サイバーセキュリティ法』『法律事務所のサイバーセキュリティQ&A』。