岩田合同法律事務所 ニュースレター
2025 年 5 月

情報・テクノロジー

サイバーインシデントに備える契約条項

弁護士　齋藤弘樹
弁護士　岩本圭矢

企業活動がインターネット空間と切り離せない状況となっている現在において、技術的のみならず法的にもサイバーセキュリティ対策を講じることの重要性はますます高まっています。本稿では、サイバーセキュリティやサイバーインシデントに関連する契約条項について整理し、その効果や必要性についてご説明いたします。

1　はじめに

企業活動を行うに当たっては、個人情報や企業秘密を第三者に委託又は提供しなければならないという場面も少なくないため、個人情報や企業秘密を委託又は提供した第三者においてサイバーインシデントが発生するというリスクに備える必要があります。

これに対し、個人情報や企業秘密の委託又は提供を受ける企業からすると、完全なサイバーセキュリティ対策を講じることは不可能であることから、損害賠償義務が免責される場合等を明確に規定しておく必要性があります。

以上の観点から、本稿では、委託元、委託先の双方の観点からサイバーセキュリティやサイバーインシデントに関連する契約条項の効果や必要性について整理し、ご説明いたします。なお、以下では、個人情報や企業秘密を併せて「個人情報等」と、個人情報等を第三者に委託又は提供する企業を「委託元」と、個人情報等の委託又は提供を受ける企業を「委託先」といいます。

2　平時のセキュリティに関する条項

平時のサイバーセキュリティへの取組として契約条項に盛り込むことが考えられる規定としては、以下のようなものが考えられます。

①	委託先のシステム構成などの情報開示を求めることができる旨の規定
②	委託先において、JVN[1]、IPA 又はメーカー等が公表する脆弱性に関する情報を収集し、対策を講じることを義務付ける規定
③	委託先における不要な情報の複製や保持を制限する（不要な情報の削除義務を課すことを含む）旨の規定
④	委託先において、従業員に対するセキュリティ研修の実施を義務付ける規定

このうち、上記①の規定は、委託先のノウハウや企業秘密が委託元に明らかとなってしまうのみならず、委託元の情報管理次第ではかえって委託先を含むセキュリティリスクが増加する等の問題があるため、一般的に採用される契約条項ではありません。

次に、上記②の規定については、公表されている脆弱性、すなわち、「既知の脆弱性」については委託先に対策義務を課して後述の免責条項の対象外とし、「ゼロデイ攻撃」[2]や「未知の脆弱性」については免責条項の対象とするという形で設けることが考えられます。

上記③の規定は、サイバーインシデントの回避というよりも、インシデントが発生した際の被害を軽減するための措置を定めるものであり、例えば、個人情報等の従業員 PC へのダウンロードを禁止する、委託先における個人情報等の削除対応の期間を 1 か月など明確に定める（「速やかに」・「遅滞なく」といったあいまいな期間設定としない）ことが考えられます。

また、委託先において、定期的に従業員に対する研修等が可能であれば、上記④の規定を設けることも考えられます。

3　インシデント発生時に関する条項

(1)　通知義務条項

通知義務条項とは、インシデント発生時に相手方へ速やかに通知する義務を定める条項です。契約上、通知義務条項を設けなかった場合、委託先は必ずしも委託元に対してサイバー攻撃を受けたことの通知を行う義務を負うわけではありません。そのため、委託先を管理するという観点から、委託元としては、契約において通知義務条項を設け、通知の期限、手段、対象範囲等を明確にしておくことが重要となります。

通知義務の発生原因については、大別すると、

ⅰ）（個人情報等に限らず）委託先に対する不正アクセスのおそれがある場合
ⅱ）委託元から預かっている個人情報等に対する不正アクセスのおそれがある場合
ⅲ）委託元から預かっている個人情報等の漏洩のおそれがある場合
ⅳ）委託元から預かっている個人情報等の漏洩があった場合

の 4 パターンが考えられます。

---

1 Japan Vulnerability Notes という脆弱性対策情報ポータルサイト。JPCERT/CC と IPA（情報処理推進機構）が共同で運営している。
2 脆弱性が発見された後、対策方法が確立・公表される前になされるサイバー攻撃を指す。

このうちⅰやⅱのパターンでは、委託元は委託先から具体的な被害又は被害発生のおそれの有無にかかわらず広く報告を受けることが可能となりますが、委託先としては広範に通知義務を負うことになります。他方で、ⅳのパターンの場合、委託元は、具体的に個人情報等の漏洩が発生しないと委託先から通知を受けられず、デジタルフォレンジック調査等によっても漏洩があったことを確定させることは難しいことに照らすと、委託先から「実際に漏洩があったとまでは言い切れない」として通知を受けられないリスクが大きくなります。また、中間的なⅲのパターンとする場合には、どの程度の可能性があれば「漏洩のおそれがある」といえるのかについて、委託元と委託先の認識の齟齬が発生する可能性がある点に留意が必要です。

また、通知の期限については、「速やかに」といった幅を持たせた規定ではなく、「●時間以内」など具体的に定めることが望ましいといえます。さらに、認識の齟齬をさけるため、どの時点から起算するのか（現場の担当者が認識したときか、責任者や役員が認識したときか）についても、契約上明示しておくことが重要です。

なお、実際にサイバーインシデントが発生した際には、各契約書を確認して委託元への通知義務の有無、通知の時期・範囲等を１つ１つ確認する時間的余裕がないことが想定されます。そのため、委託先においては、平時から通知義務条項の有無や内容を取引先ごとに把握・データベース化しておくことが望ましいと考えられます。

(2)　調査義務条項

サイバーインシデントが発生した場合の調査について、委託先に対し、一定の調査会社を起用させることや、一定の調査方法を義務付けることも考えられます。もっとも、サイバーインシデントに関する調査費用は、規模によっては数千万円に上る可能性があり、委託先としても、契約においてあらかじめ調査の具体的なルールまで規定するような契約条項に応じることは難しいと考えられます。

他方で、契約上、明示的に調査義務が課されていない場合においても、サイバーインシデントが生じた後、委託元が委託先に対して一定の調査を行う要請することは十分にあり得るところです。委託先としては、インシデントの内容・規模、取引を維持することの重要性、保険金で調査費用が賄われるか否か等を考慮し、調査要請に応じるかどうかを判断することになります。

(3)　不可抗力条項

不可抗力条項は、契約の相手方（取引先）の責に帰すことができない事由により債務の履行が不能となった場合に、取引先の債務不履行責任を免除するという条項です。

従来の契約では、戦争・天災・ストライキ等が挙げられており、サイバーインシデントは挙げられていませんでしたが、近年ではサイバーインシデントを不可抗力[3]事由として明示的に

[3] 学説上、不可抗力とは「外部からくる事実であって，取引上要求できる注意や予防方法を講じても防止できないもの」と考えられている（我妻榮ほか『我妻・有泉コンメンタール民法　総則・物権・債権（第８版）』（日本

定める契約が増えています。

しかしながら、サイバーインシデントを不可抗力事由として定めたとしても、それにより当然に免責が認められるわけではありません。そもそもサイバーインシデントは、災害や戦争と異なり、個人情報等の委託先の社内体制が適切に整備されていればサイバーインシデントによる個人情報等の漏洩が回避可能であったという場合も想定されます。したがって、不可抗力事由として単に「サイバーインシデント（サイバー攻撃）」とのみ定められていたとしても、裁判になった場合には、この「サイバーインシデント（サイバー攻撃）」は、予見不可能であって、予防措置を尽くしても回避することができないインシデントに限られると限定的に解釈される可能性も相応に高いと考えられます。

上記の点を踏まえ、不可抗力として免責されるサイバーインシデントの範囲を具体的に規定するという手法をとることも考えられます。例えば、「ゼロデイ攻撃」や「未知の脆弱性」（JVN、IPA 又はメーカー等が公表する脆弱性に関する情報に含まれないもの）を利用した攻撃については不可抗力であるとして、免責の対象にするといった内容の契約条項が採用されることがあります。

(4)　損害賠償責任の範囲の制限条項

サイバーインシデントによる損害は甚大になる可能性があるため、個人情報等の委託先としては、契約において、損害賠償の範囲を限定したり、金額の上限を定めることが考えられます。

このような損害賠償責任の範囲の制限条項として、消費者契約法の適用がない B to B ビジネスにおいては、重過失があった場合でも損害賠償責任が限定されるという内容の契約条項が設けられることがあります。しかし、B to B ビジネスにおいても、委託先の重過失が認定されるような事情がある場合にまで、損害賠償責任の制限条項が有効であるかは議論の余地があり、裁判になった際には、そのような責任制限条項が無効と判断されるリスクもあることに留意する必要があります。

なお、当該リスクを踏まえた上で、交渉上のけん制材料として、重過失がある場合にも損害賠償責任を制限する旨の条項が導入されることもあります。

４　まとめ

サイバーインシデントは、技術部門だけでなく法務部門にとっても重大なリスクであるため、契約において平時の予防措置から有事の対応までの体制を包括的に設計し、リスクマネジメントを行うことが重要です。また、委託先としては、有事の場合、個人情報保護法上の義務（個人情報保護委員会への報告義務、本人通知義務等）の有無の判断・履行方法の検討のみならず、委託元への対応方針についても検討することが重要です。

評論社、2022）・826～827 頁）。

【執筆者】

齋藤 弘樹（弁護士）
E-mail: hiroki.saito@iwatagodo.com

2013 年　弁護士登録、潮見坂綜合法律事務所入所
2017 年　岩田合同法律事務所入所

企業法務の中でも、IT 関連業務対応（サイバーセキュリティ、システムの開発・保守・障害、ソフトウェアライセンス等）及び危機管理業務を中心に手がける。
サイバーインシデントの平時の予防措置・有事対応（調査方針の立案から開示・広報対応まで）に関するアドバイスを数多くの企業に提供している。

岩本 圭矢（弁護士）
E-mail: yoshiya.iwamoto@iwatagodo.com

2018 年　裁判官任官
2023 年　弁護士登録、岩田合同法律事務所入所

裁判官として民事訴訟、破産、執行、保全事件等を担当した経験を活かし、金融機関、電力会社、メーカー、保険会社、不動産会社等における企業間取引に関する訴訟や株主代表訴訟などを多数取り扱う。また、個人情報保護を含む IT 関連の案件にも注力しており、裁判官としての視点・経験を積極的に取り入れて、IT 関連案件における紛争の予防・解決に向けたアドバイスを提供している。そのほか、株主総会対応、危機管理業務（調査委員会対応）などの企業法務全般に取り組む。

岩田合同法律事務所

1902 年（明治 35 年）、司法大臣や日本弁護士連合会会長を歴任した故・岩田宙造弁護士が「岩田宙造法律事務所」を創立したことに始まる、我が国において最も歴史のある法律事務所の一つです。
創立当初より、我が国を代表する企業等の法律顧問として広範な分野で多数の企業法務案件に関与しております。弁護士 110 余名のほか、日本語対応可能な外国法事務弁護士（中国法、フランス法、米国法）も所属し、特別顧問として元金融庁長官中島淳一氏、特別招聘顧問として元最高裁長官大谷直人氏が在籍しております。

〒100-6315 千代田区丸の内二丁目 4 番 1 号　丸の内ビルディング 15 階
岩田合同法律事務所　広報：　newsmail@iwatagodo.com