Innovation for Wellbeing
SOMPOリスクマネジメント

損保ジャパン日本興亜ＲＭレポート | 188

IT システムにおける損害賠償請求

対応と備えについて

佐々木 亮 Ryo Sasaki
リスクマネジメント事業本部 リスク調査部
上級コンサルタント

はじめに

近年、IT システムからの情報漏えいに関する報道が後を絶たず、IT システムの開発や保守・運用におけるトラブルも多く発生している。訴訟まで発展せずに当事者間の示談で解決するケースも多いが、経験の少ない不慣れな当事者間で行われる場合もあり、過大な請求または支払いとなるだけでなく、完了までに時間がかかっているのが実状である。近年、CSIRT[1]を設置する企業も増えてきたが、情報セキュリティ上のインシデント（事故）対応が目的であり、損害賠償請求への対策の検討は進んでいないようである。

本稿では、IT システムに関る損害賠償請求への備えや対応方法を述べる。特に断りの無い限りベンダー側およびユーザー側双方の立場としている。なお、損害賠償の対応に主眼を置くため、初動対応や訴訟については本稿では多く言及しない（図 1）。損害賠償請求の適正かつ早期解決の一助になれば幸いである。

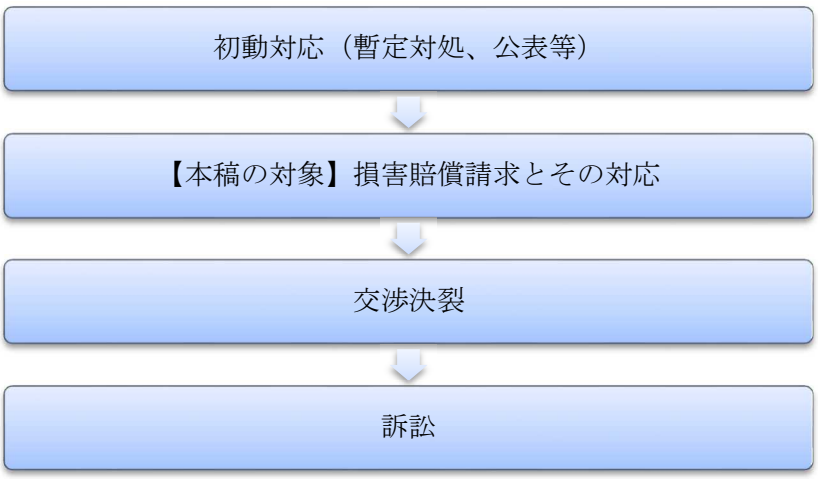

図 1　初動対応から訴訟までの大まかな流れ[2]

[1] Computer Security Incident Response Team の略。セキュリティ上の問題が発生した際に、被害の拡大防止や関連情報の収集・告知、再発防止策の策定などの活動を行うチームのこと。
[2] 当社作成。

なお、本稿では簡単のため、用語を次のように定義する。

- ベンダー：IT システムの販売側。IT システムの開発や保守・運用を行う事業者。
- ユーザー：IT システムの購入側。エンドユーザーと同一の場合もある。
- エンドユーザー：IT システムの利用者。ユーザーと同一の場合もある。
- 事故：IT システム開発・運用におけるトラブルや情報セキュリティ上のインシデント等、損害賠償請求の原因となる事象。

1. 対応の記録、対応チームの組成

1.1. 対応の記録

事故が発生した場合、まずは対応内容を記録するべきである。この記録は、損害賠償請求の対応の際、重要な資料となる。緊急のために電話でやりとりが行われた場合でも、メモやメール（対応の報告等）で記録しておき、後から対応の流れを確認可能とすることをお勧めしたい。記録は、損害賠償請求の対応がクローズするまで続ける必要がある。システム開発に関連した損害賠償請求の場合には、成果物[3]や関連ドキュメント[4]もきちんと管理しておきたい。管理や記録に当たっては、プロジェクト管理ツール[5]等の活用も手段の 1 つである。

1.2. 対応チームの組成

損害賠償請求が生じる可能性がある場合、対応チームを構築する。

対応チームに含むべきメンバーと役割の例を表 1 に示す。なお、同表はあくまで例であり、必要に応じて兼務にしたり、担当者を複数名にしたり等、臨機応変な体制作りをお勧めしたい。

表 1　損害賠償対応チームのメンバーと役割の例

メンバー	主な役割
責任者	チームの取りまとめた方向性について承認する。管理職や役員等が担当する。
リーダー	チーム全体の取りまとめを行う。
営業担当者	関係者の整理や相手方との交渉を行う。
技術担当者	技術的な事象を整理し、関係者にわかりやすく伝える。情報セキュリティに関連する場合には CSIRT が技術担当者と連携しても良い。
法務担当者や顧問弁護士	法的な観点から損害賠償の範囲、金額等の妥当性を検討する。

[3] 要件定義書、設計書、テスト仕様書、テスト成績書等。開発手法や開発フェーズによって異なる。
[4] やりとりのメールや打合せ議事録等。
[5] スケジュールやタスクの管理等をするツール。

2. 情報の整理

事故がある程度収束すると、損害賠償検討のフェーズに移行する。この際、対応の記録を基に、損害賠償請求の妥当性について整理する。

2.1. 事故内容の整理

技術担当者が主に担当する。事故がいつ、誰の責任で、どのようにして起きたのか等、5W1H の観点で整理する。内容は相手方や対応チームの専門性のない者にも理解できるよう、図解をお勧めしたい。また、IT に疎い関係者のために専門用語についても平易な言葉で一覧を作成しておくことが望ましい。事故の内容によっては、複数の利害関係者から損害賠償請求を受ける可能性があるため、早い段階で影響範囲を把握することをお勧めしたい。

2.2. 利害関係者・商流、仕様・契約の整理

営業担当者が主に担当する。利害関係者はユーザー、ベンダーだけにとどまらない場合もあり、各関係者の間で契約内容を確認しておく必要がある。利害関係者が複数になると混乱を招く場合もあるため、事故内容と同様に、図解しておくことが望ましい。この際、事故内容を基に、簡単で良いので取引内容（開発・運用等）や契約形態（準委任、請負等）についても図中に記載しておくとわかりやすい。

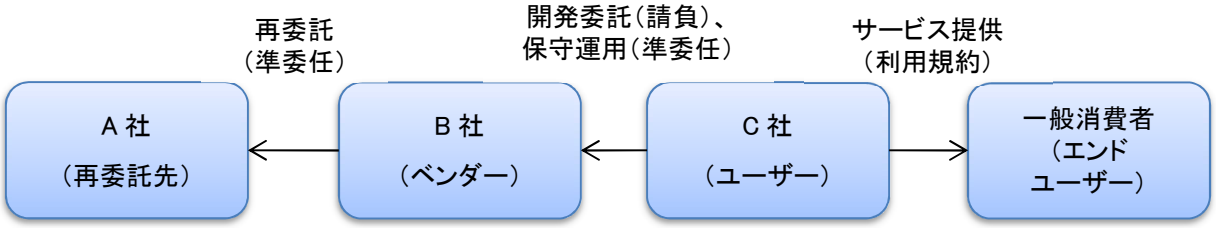

図 2　利害関係者・商流、契約の図解例[6]

仕様・契約については、各社間の取引について、以下のような観点で整理をしておく。基本的にはまず契約に則った対応が必要となる。

- 取引内容（開発・運用等）および仕事の範囲
- 契約形態（請負・準委任、主な項目は表 2 のような整理となる）

表 2　契約形態[7]

契約	請負契約	準委任契約
目的	仕事の完成	事務の処理
義務・責任	瑕疵担保責任	善管注意義務

- 契約の構成（基本契約、個別契約、覚書等）
- 責任限定条項[8]（損害の範囲[9]や上限額等）

[6] 当社作成。
[7] 当社作成。
[8] 責任制限条項とも呼ばれる。
[9] 直接損害に限定するかどうか等。

2.3. 損害賠償項目と妥当性評価

損害賠償の項目について妥当性の評価を行う。妥当性評価は、責任の所在、事故との因果関係、証憑（単価、数量含む)、契約との関連性等を確認する。過大な請求または支払いとならないよう、請求側・被請求側が双方とも妥当性の評価を行うことをお勧めしたい。

3. 日頃の備え

3.1. 事故の未然防止

言うまでもなく、損害賠償請求の基となる事故自体が発生しなければ問題はない。事故の未然防止に当たって、注意すべき項目を挙げる。

- IT システム全般に関する知見の蓄積

経験の浅い担当者の場合、そもそも内容を理解できない場合がある。また、問題や事故に気付かないといったことも多くある。特に中小企業の場合、情報システムの専任者がいなかったり、メンバーが少数だったりするとチェックが足りないまま運用が続くことになる。こうした状態を放置すると、やがて大きな事故・損害につながる可能性がある。ベンダー側は言うまでもないが、ユーザー側のシステム担当者も知見を蓄積しておく必要がある。

- 担当する IT システムの理解、引継ぎ

担当する IT システムを理解していれば、問題や不審点に早期に気が付く可能性が高まる。担当者の異動等で業務を引き継ぐ場合があるが、担当者の理解が不十分の場合には、事故が生じやすい傾向にある。

- 適切なパッチ[10]適用

ソフトウェアのリリース後に発見された脆弱性に対応するため、ソフトウェアベンダーからパッチが提供される。OS[11]やミドルウェア[12]については比較的パッチ適用の問題は無いようだが、フレームワーク[13]、CMS[14]、プラグイン[15]等では見落とされがちであるため、注意が必要である。パッチリリース後、適用が遅いとシステムの安全性が懸念されるため、導入しているソフトウェアの脆弱性情報およびパッチリリース状況の定期的な確認も必要である。

[10] 修正点を更新するデータ。
[11] Operating System：システム全体を管理するソフトウェア、システム。
[12] OS とアプリケーションの中間に位置し、共通して利用される機能を提供するソフトウェア
[13] システム開発の際に土台となる機能を提供するソフトウェア。
[14] Contents Management System（コンテンツマネジメントシステム)：Web サイト等の構築や編集を行うシステム。
[15] 機能を追加・拡張するソフトウェア。

● ウェブアプリケーションのセキュリティ実装

ウェブアプリケーションの場合にはインターネットからの攻撃が想定され、セキュリティに関する事故の発生が懸念される。そのため、ウェブアプリケーションに関しては、対策を可能な限り開発段階で実装しておくことが望ましい。WAF[16]も一定の効果があるが、改修が困難な場合等、あくまで補助的な利用であり、実装で対応することが望ましい。

● 契約の見直し

委託内容の過不足や責任限定条項等、既存の契約に問題がないかどうか確認する。特に、責任限定条項が無い場合には、損害賠償請求が多大となる可能性があるので注意が必要である。

● ウェブサイトの脆弱性診断

ウェブサイトの脆弱性診断が定期的に実施されていない場合が多い。システム開発時や更新時だけでなく、最低でも年 1 回程度の定期的な実施が推奨されている[17]。

脆弱性診断を外部委託した場合には費用がかかるため、自動脆弱性診断ツール等の利用を併せて検討しても良い。

3.2. 対応チームの事前組成と訓練

事故の未然防止策と併せて、IT システムの損害賠償請求対応チームの事前組成と訓練をお勧めしたい。実際に提供または導入している IT システムを訓練で取上げシミュレーションすることで、実際の損害賠償請求時のスムーズな対応に役立つ。

4. おわりに

IT システムは、現代のビジネスにおいて重要な位置を占めている。個人情報や決済情報を取り扱う場合が多い一方で、IT システムの管理や情報セキュリティ向上への投資を躊躇する企業も多い。しかしながら、損害賠償請求となった場合には請求額が数千万円～数億円の規模となる場合も少なくない。さらに訴訟に発展した場合には、数年単位での対応が必要となる。自社の IT システムリスクを把握し、IT 投資や対応のバランスを検討することをお勧めしたい。

[16] Web Application Firewall：Web サーバへの外部からの攻撃をブロックするハードウェアやソフトウェア。
[17] 情報処理推進機構　情報セキュリティ　注意喚起「ウェブサイトへのサイバー攻撃に備えた定期的な点検を」
https://www.ipa.go.jp/security/ciadr/vul/20150714-websiteco.html

参考文献

独立行政法人 情報処理推進機構.
安全なウェブサイトの作り方, https://www.ipa.go.jp/security/vuln/websecurity.html, （アクセス日:2020-01-28）
ウェブサイト運営者のための脆弱性対応ガイド, https://www.ipa.go.jp/files/000044736.pdf （アクセス日:2020-01-28）
ウェブサイト構築事業者のための脆弱性対応ガイド, https://www.ipa.go.jp/files/000044735.pdf （アクセス日:2020-01-28）
セキュリティ担当者のための脆弱性対応ガイド, https://www.ipa.go.jp/files/000058493.pdf （アクセス日:2020-01-28）
脆弱性対策の効果的な進め方（ツール活用編）, https://www.ipa.go.jp/security/technicalwatch/20190221.html （アクセス日:2020-01-28）
委託関係における情報セキュリティ対策ガイドライン, https://www.ipa.go.jp/files/000014018.pdf （アクセス日:2020-01-28）
ITmedia. 「訴えてやる！」の前に読む IT 訴訟 徹底解説, https://www.atmarkit.co.jp/ait/series/1507/ （アクセス日:2020-01-28）
アイティーエス法律事務所. 法とＩＴの話, https://www.its-law.net/category/it-case （アクセス日:2020-01-28）
細川 義洋. なぜ、システム開発は必ずモメるのか?. 日本実業出版社, 2013
上山 浩. トンデモ“IT 契約”に騙されるな. 日経 BP, 2013
伊藤 雅浩, 久礼 美紀子, 高瀬 亜富. IT ビジネスの契約実務. 商事法務, 2017
細川 義洋. システムを「外注」するときに読む本. ダイヤモンド社, 2017
池田 聡. システム開発 受託契約の教科書. 翔泳社, 2018

執筆者紹介

佐々木 亮　Ryo Sasaki

リスクマネジメント事業本部 リスク調査部
上級コンサルタント
情報処理安全確保支援士（登録情報セキュリティスペシャリスト）（登録番号 018034）
専門は IT

ＳＯＭＰＯリスクマネジメントについて

ＳＯＭＰＯリスクマネジメント株式会社は、損害保険ジャパン日本興亜株式会社を中核とするＳＯＭＰＯホールディングスのグループ会社です。「リスクマネジメント事業」「サイバーセキュリティ事業」を展開し、全社的リスクマネジメント（ERM）、事業継続（BCM・BCP）、サイバー攻撃対策などのソリューション・サービスを提供しています。

本レポートに関するお問い合わせ先

ＳＯＭＰＯリスクマネジメント株式会社
総務部　広報担当
〒160-0023 東京都新宿区西新宿 1-24-1 エステック情報ビル
TEL：03-3349-4330（代表）

