サイバーセキュリティセミナー2026

ランサムウェア攻撃と企業法務

～被害シナリオ別の実務対応～

八雲法律事務所
YAKUMO LAW OFFICE

弁護士　町田　力

自己紹介

経歴

- 2012年　弁護士登録（東京弁護士会）
- 2021年　八雲法律事務所に入所
- 2022～2023年　税務大学校 非常勤講師（商法演習）
- 2024年　情報処理安全確保支援士に登録

八雲法律事務所
YAKUMO LAW OFFICE

サイバーセキュリティ法務に特化した法律事務所

- 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（有事）
  - 個人情報保護法対応
  - 当局対応
  - ステークホルダー対応
- 企業のサイバーセキュリティ体制構築支援（平時）

執筆

（ECサイトからのクレジットカード情報漏えい）
- 「ECサイトからのクレジットカード情報漏えい事案における法的留意点（上）」ビジネス法務2023年１月号
- 「ECサイトからのクレジットカード情報漏えい事案における法的留意点（下）」ビジネス法務2023年２月号
- 「クレジットカード情報漏えい時にECサイト運営企業がとるべき初動対応」UNITIS2023年８月公開

（ランサムウェア攻撃）
- 「サイバー攻撃と企業対応 クラウドサービスのサイバーリスクと個人情報保護法上の留意点」会社法務AtoZ 2023年12月号
- 「ランサムウェア被害を受けた場合の法務対応上の留意点」商事法務ポータル2024年８月
- 「ランサム攻撃事案における責任の範囲と損害の公平な分担」NBL2024年12月15日号

（内部不正による情報漏えい）
- 「サイバーセキュリティ対策を目的としたログ管理の法的留意点」ビジネス法務2023年11月
- 「内部者による企業情報の持出しに関する最新実務対応」ビジネス法務2024年４月号

（サイバー保険）
- 「サイバー保険の概要と加入に際しての検討事項」旬刊経理情報2022年６月10日号

（BEC）
- 「ビジネスメール詐欺に関する法的論点と実務対応上の留意点」NBL2025年5月15日号

著書

- 『実務解説 サイバーセキュリティ法〈第2版〉』中央経済社2025年10月
- 『法律事務所のサイバーセキュリティQ&A』中央経済社2024年６月

本日お伝えしたいテーマ

- 企業はどのようにしてランサムウェア攻撃に巻き込まれるのか？
- その際に発生し得る損害とは何か？
- そして、求められる法的対応とは何か？

目次

I.　企業がランサムウェア攻撃に直面するシナリオ

①自社がランサムウェア攻撃を受ける場合

②利用しているクラウドサービスがランサムウェア攻撃を受ける場合

③取引先がランサムウェア攻撃を受ける場合

この3つのシナリオごとに、企業が直面する典型的な法的課題として、

- ◆ 想定される損害
- ◆ 法的請求の可能性（請求される可能性、請求できる可能性）
- ◆ 必要な法的対応

を整理する

Ⅱ. 自社がランサムウェア攻撃を受ける場合
1. 想定される損害

JNSAの「インシデント損害額調査レポート 別紙 2025年版」に掲載されている一例

従業員20～999名の製造業者

〔事案の概要〕
- 脆弱性のあるVPN機器からの侵入により、サーバー複数台がランサムウェアに感染。
- 被害を受けた社内システムの復旧には2か月を要した。

〔被害額〕

事故原因・被害範囲調査費用	800万円
法律相談費用、コンサルティング費用、ダークウェブ調査費用	1,600万円
詫び状送付、見舞品等購入費用	4,500万円
コールセンター費用	600万円
システム復旧費用	4,000万円
再発防止費用	900万円
合計：1億2,400万円	

＋　対応に要した内部工数：不明
（残業代等超過人件費として1,000万円強を計上）

＋　利益喪失：不明

参照元：
https://www.jnsa.org/result/incidentdamage/data/incidentdamage_20250723.pdf

Ⅱ. 自社がランサムウェア攻撃を受ける場合
2. 法的請求の可能性

■ 自社が顧客（個人情報の本人）から損害賠償を請求される可能性

- 不法行為（プライバシー侵害）に基づく損害賠償請求
- 氏名、住所、生年月日、性別等、漏えいした情報が既に公となっていることが多く、本人自らそれを公表する機会も多いような内容の場合には、プライバシー侵害の程度としては比較的低いと判断され、損害額も低くなる傾向。
- ベネッセ事件の東京高判令和2年3月25日では、上記氏名等のほか出産予定日が漏えいした事案で、**１人あたり3,300円**（慰謝料3,000円、弁護士費用300円）が損害として認定された。
- 他方、通常第三者が知りえない情報まで漏えいした場合には、プライバシー侵害の程度は高いと判断され、損害額も高くなる傾向。
- エステを受けようとしていることやエステの施術コースといった情報が漏えいした事案（東京高判平成19年8月28日判タ1264号299頁〔TBC事件〕）では、損害額として１人あたり最大3万5,000円（慰謝料3万円、弁護士費用5,000円）が認定された。

Ⅱ. 自社がランサムウェア攻撃を受ける場合
2. 法的請求の可能性

■ 自社が取引先から損害賠償を請求される可能性

- 取引先の機密情報が攻撃者により窃取
  - 機密保持義務違反を理由とした債務不履行責任
- 納品の遅れ・サービスの一時中断
  - 履行遅滞・履行不能といった債務不履行責任
- 不可抗力・免責条項の有無
  - 例

> 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。

  - ただし、相当の注意をすれば防止できるサイバー攻撃に起因する損害については、免責が認められない可能性が高い。
- 賠償制限条項の有無
  - 例

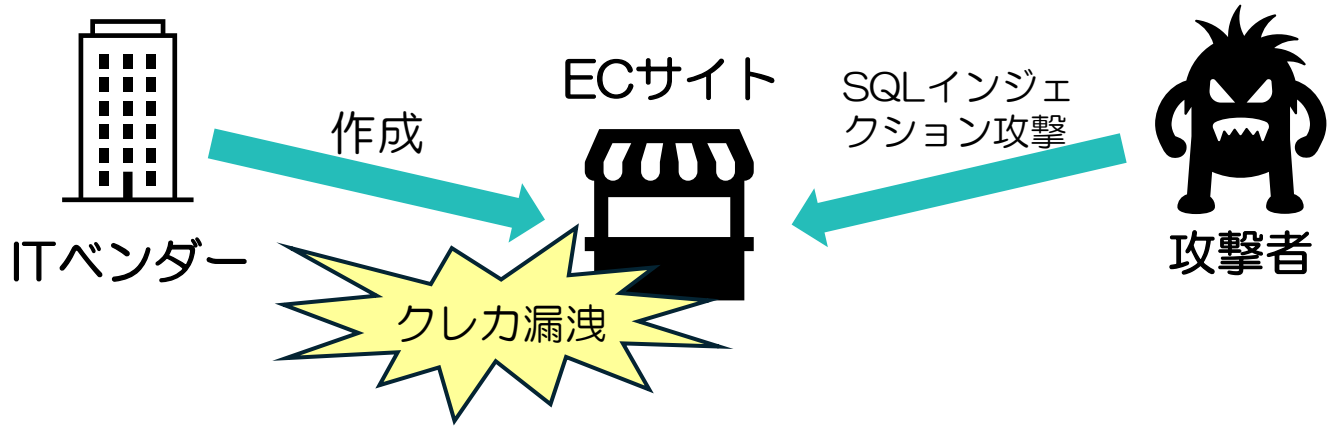
> 当社が利用者に対して負う損害賠償額は、当該利用者が過去6か月間に当社に対して支払ったサービス利用料の合計金額を上限額とする。

  - ただし、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、賠償制限条項は無効、または適用されないと解されている。

Ⅱ. 自社がランサムウェア攻撃を受ける場合
2. 法的請求の可能性

■ 開発・保守ベンダーに対する損害賠償請求

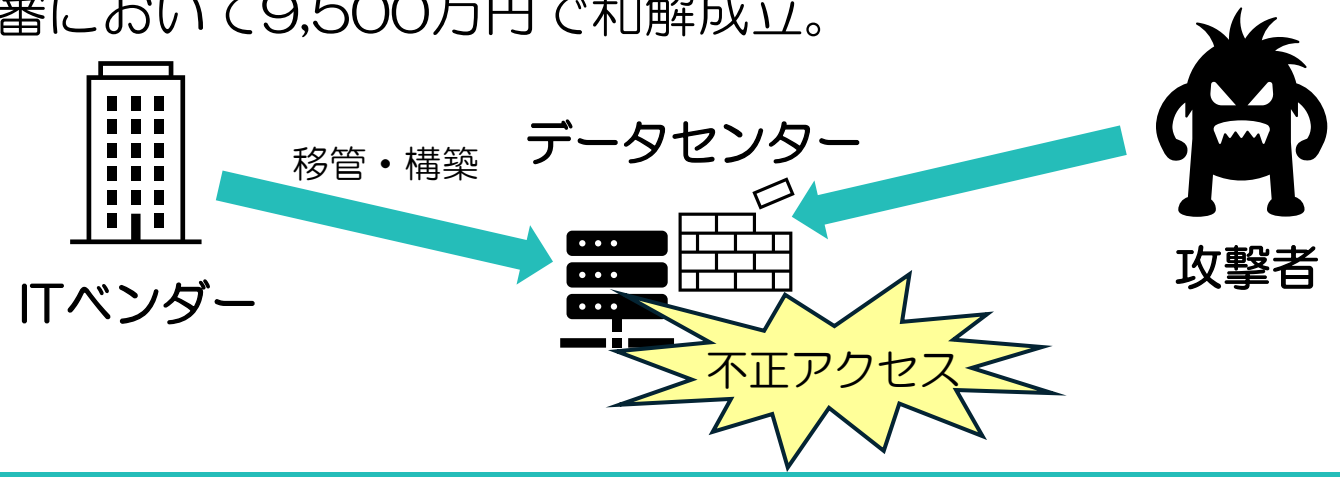
- **SQLインジェクション事件**
  - 東京地判平成26年1月23日（判時2221号71頁）
  - 原告（ECサイト運営事業者）の意向の結果、被告（外部ITベンダー）が作成したECサイト上で同サイトの利用者のクレジットカード情報を保持する設定となっていたところ、SQLインジェクション対策が施されていなかったためにSQLインジェクション攻撃を受け、クレジットカード情報漏えいが生じたことから、原告が被告に対し損害賠償請求をした事案。
  - 被告の債務不履行に基づく損害賠償責任を認めつつ、原告の過失も3割認め（過失相殺）、請求額約1億1,000万円のうち約2,300万円の支払いを認める一部認容判決。



Ⅱ. 自社がランサムウェア攻撃を受ける場合
2. 法的請求の可能性

■ 開発・保守ベンダーに対する損害賠償請求

- **前橋市対NTT東日本事件**
  - 前橋地判令和5年2月17日（Westlaw2023WLJPCA02176003）
  - ITベンダーである被告が受託したデータセンターの移管・構築業務に関し、セキュリティ上重要な役目を果たす機器（ファイアウォール）の設定に不備があったことにより、原告において不正アクセス被害が生じた事案。
  - 被告の債務不履行に基づく損害賠償責任を認め、請求額約1億7,000万円のうち約1億4,000万円の支払いを認める一部認容判決。
  - ただし、控訴審において9,500万円で和解成立。



Ⅱ. 自社がランサムウェア攻撃を受ける場合
2. 法的請求の可能性

■ 開発・保守ベンダーに対する損害賠償請求

（1）開発・保守ベンダーの債務不履行（特に契約上の義務）の有無

- SQLインジェクション事件でいうと、被告がSQLインジェクション対策を講じる義務
- 前橋市対NTT東日本事件でいうと、被告がファイアウォールを適切に設定する義務

① 契約書に義務が明記されている場合

② 契約書に付随する文書でセキュリティ対策の仕様が特定されている場合

③ セキュリティ対策の仕様が特定されていない場合

Ⅱ. 自社がランサムウェア攻撃を受ける場合
2. 法的請求の可能性

■ 開発・保守ベンダーに対する損害賠償請求

（1）開発・保守ベンダーの債務不履行（特に契約上の義務）の有無

① 契約書に義務が明記されている場合

➢ 義務が認められる。

② 契約書に付随する文書でセキュリティ対策の仕様が特定されている場合

➢ 《前橋市対NTT東日本事件》被告は、原告が主張するところの「本件システムの提供に当たり、その外部ファイアウォール及び内部ファイアウォールを適切に設定して通信制限を行う債務」は「契約書に明示されてい」ない旨を主張したが、裁判所は、契約書の作成前後にやり取りされた提案依頼書、提案書、要件定義書及び基本設計書において、外部ファイアウォール及び内部ファイアウォールにより通信制限を行うものと記載されていることを考慮した上で被告の義務を認定した。

Ⅱ. 自社がランサムウェア攻撃を受ける場合
2. 法的請求の可能性

■ 開発・保守ベンダーに対する損害賠償請求

（1）開発・保守ベンダーの債務不履行（特に契約上の義務）の有無

③ セキュリティ対策の仕様が特定されていない場合

- 《SQLインジェクション事件》契約書上記載がない場合であっても、「（システムの発注を受けた）その当時の技術水準に沿ったセキュリティ対策を施したプログラムを提供することが黙示に合意されていた」として、ベンダーに対して一定のセキュリティ対策を施す義務が認められた。
- そして、具体的にどのような内容のセキュリティ対策を施す義務を負うかの認定にあたっては、システム開発契約締結時点における当該攻撃手法に関する注意喚起・対策の周知状況等が考慮されている。
- 《SQLインジェクション事件》当該システム開発に係る契約締結当時、IPAや経済産業省からSQLインジェクション攻撃についての注意喚起がなされていたこと等を認定した上で、被告はSQLインジェクション対策を施したシステムを提供すべき義務を負っていたと認定した。

Ⅱ. 自社がランサムウェア攻撃を受ける場合
2. 法的請求の可能性

■ 開発・保守ベンダーに対する損害賠償請求

（2）賠償制限条項の適用の有無

- システム開発契約では、主にベンダー側が損害賠償責任を追及されることを避けるため、自らの損害賠償責任を免除あるいは制限する条項を設ける場合がある。
- 《SQLインジェクション事件》

> ベンダーが損害賠償責任を負う場合、個別契約に定める契約金額の範囲内において損害賠償を支払う。

➢ 「被告が権利・法益侵害の結果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って被告の損害賠償義務の範囲が制限されるとすることは、著しく衡平を害するものであって、当事者の通常の意思に合致しないというべきであるから、被告に故意または重過失がある場合には適用されない」と判断した。前橋市対NTT東日本事件も同様。

Ⅱ. 自社がランサムウェア攻撃を受ける場合
2. 法的請求の可能性

■ 開発・保守ベンダーに対する損害賠償請求

（2）賠償制限条項の適用の有無

- 重過失の有無が問題になる。
- 《SQLインジェクション事件》

① 被告に求められる注意義務の程度が比較的高度なものであったこと（専門的知見）
② 経済産業省及びIPAがSQLインジェクション対策をするように注意喚起をしていたこと
③ SQLインジェクション対策を行うことに多大な労力や費用がかかるわけではない

- ➢ 被告に重過失があると認められた。

- 《前橋市対NTT東日本事件》

① 被告に単純かつ明白なミスがあったこと
② 被告が情報セキュリティについて高度な専門的知見を有していること

- ➢ 被告に重過失があると認められた。

Ⅱ. 自社がランサムウェア攻撃を受ける場合
2. 法的請求の可能性

■ 開発・保守ベンダーに対する損害賠償請求

（3）過失相殺

- 《SQLインジェクション事件》ECサイト運営事業者のシステム担当者が、ベンダーの説明からセキュリティ上はクレジットカード情報を保持しない方がよいことを認識し、ベンダーからそのためのシステム改修の提案を受けていながら、何ら対策を講じずにこれを放置したことがクレジットカード情報漏えいの一因になったとして、ECサイト運営事業者の過失を考慮し、3割の過失相殺を認めた。

➢ ベンダーとしては、自らの法的責任を軽減するためにも、セキュリティ対策について十分な説明や提案をすべきであり、他方でECサイト運営事業者としては、ベンダーからECサイトのセキュリティ対策に関する提案を受けた場合、これを真摯に傾聴することが肝要である。

Ⅱ. 自社がランサムウェア攻撃を受ける場合
3. 必要な法的対応

■ 個人情報保護法対応

サイバー攻撃により個人データが漏えい（おそれを含む）した場合の法律上の義務（2.5個）

① 個人情報保護委員会への報告
（速報：発覚から概ね5日以内、確報：発覚から60日以内）

② 本人への個別通知

②´公表（本人への通知が困難である場合の代替措置）

Ⅱ. 自社がランサムウェア攻撃を受ける場合
3. 必要な法的対応

■ 個人情報保護法対応

個人情報保護委員会への報告義務

	報告期限	報告内容
速報	漏えい等の発覚後、速やかに報告 ※概ね3～5日以内	その時点で把握している事項
確報	30日以内 （サイバー攻撃による場合は60日以内）	⑴概要 ⑵漏えい等が発生し、または発生したおそれがある個人データの項目 ⑶漏えい等が発生し、または発生したおそれがある個人データに係る本人の数 ⑷原因 ⑸二次被害またはそのおそれの有無およびその内容 ⑹本人への対応の実施状況 ⑺公表の実施状況 ⑻再発防止のための措置 ⑼その他参考となる事項

Ⅱ. 自社がランサムウェア攻撃を受ける場合
3. 必要な法的対応

■ 個人情報保護法対応

本人への通知義務

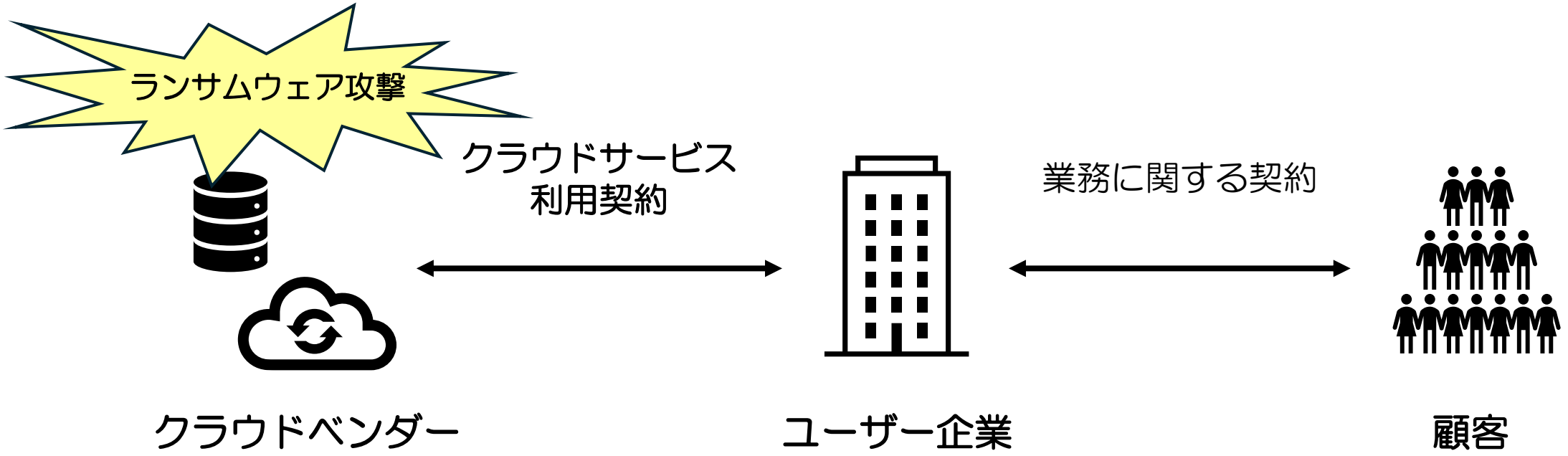
通知期限	通知内容
当該事態の状況に応じて速やかに通知 ※通知が困難な場合には、公表等の代替措置	⑴概要 ⑵漏えい等が発生し、または発生したおそれがある個人データの項目 ⑶原因 ⑷二次被害またはそのおそれの有無およびその内容 ⑸その他参考となる事項

Ⅱ. 自社がランサムウェア攻撃を受ける場合
3. 必要な法的対応

■ 取引先対応

- **機密保持契約上の報告義務**の有無を確認
  - 報告義務がある場合は速やかに報告
- 取扱いの委託を受けた個人データが漏えいした場合
  - 委託元に通知
  - 個人情報保護委員会への報告義務・本人への通知義務を免除される（詳細は後述）

Ⅲ. 利用しているクラウドサービスがランサムウェア攻撃を受ける場合
1. 想定される損害



Ⅲ. 利用しているクラウドサービスがランサムウェア攻撃を受ける場合
1. 想定される損害

- 業務に組み込んだクラウドサービスの利用停止
- これに伴う自社の顧客に対する納品の遅れ・サービスの一時中断

→
- **事業の中断による逸失利益**
- **顧客離れによる逸失利益**
- **追加コスト（別のクラウドサービスへの移行費用等）**
- **顧客からの損害賠償請求**

ユーザー企業がクラウドベンダーのサーバー内に保存した電子ファイルが窃取

- 顧客から機密保持義務（守秘義務）を負った上で受領した電子ファイルが漏えい

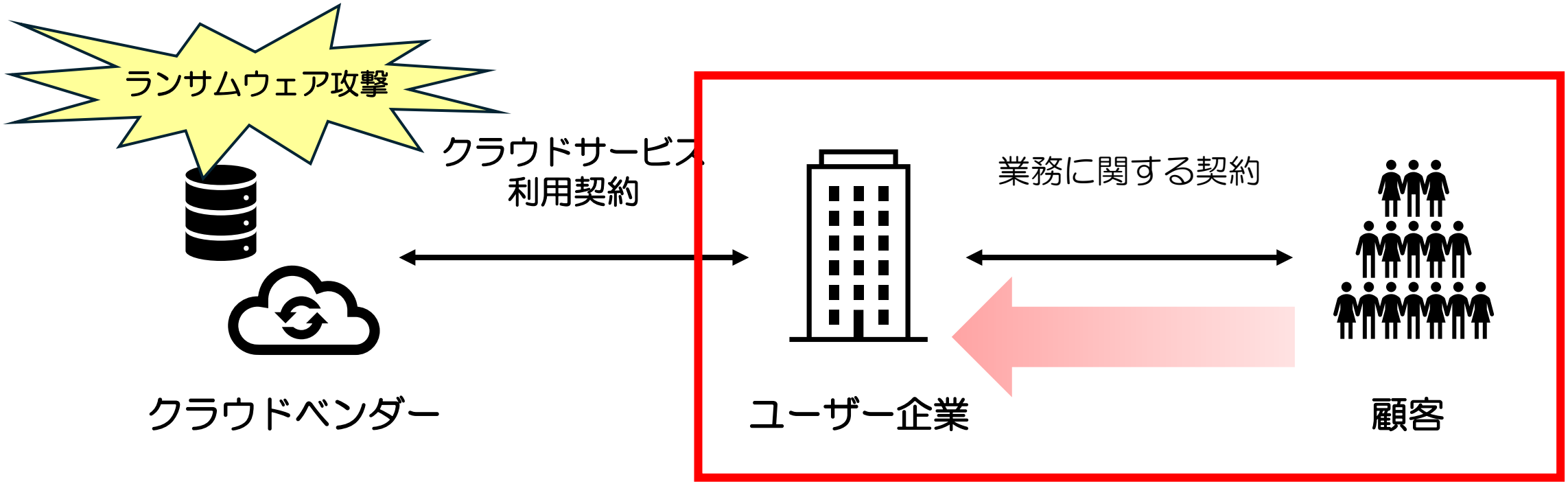
→
- **顧客からの損害賠償請求**

- 従業員や顧客の個人データが漏えい

→
- **個人情報漏えい対応費用**

Ⅲ. 利用しているクラウドサービスがランサムウェア攻撃を受ける場合
2. 法的請求の可能性

■ 自社が顧客から損害賠償を請求される可能性



Ⅲ. 利用しているクラウドサービスがランサムウェア攻撃を受ける場合
2. 法的請求の可能性

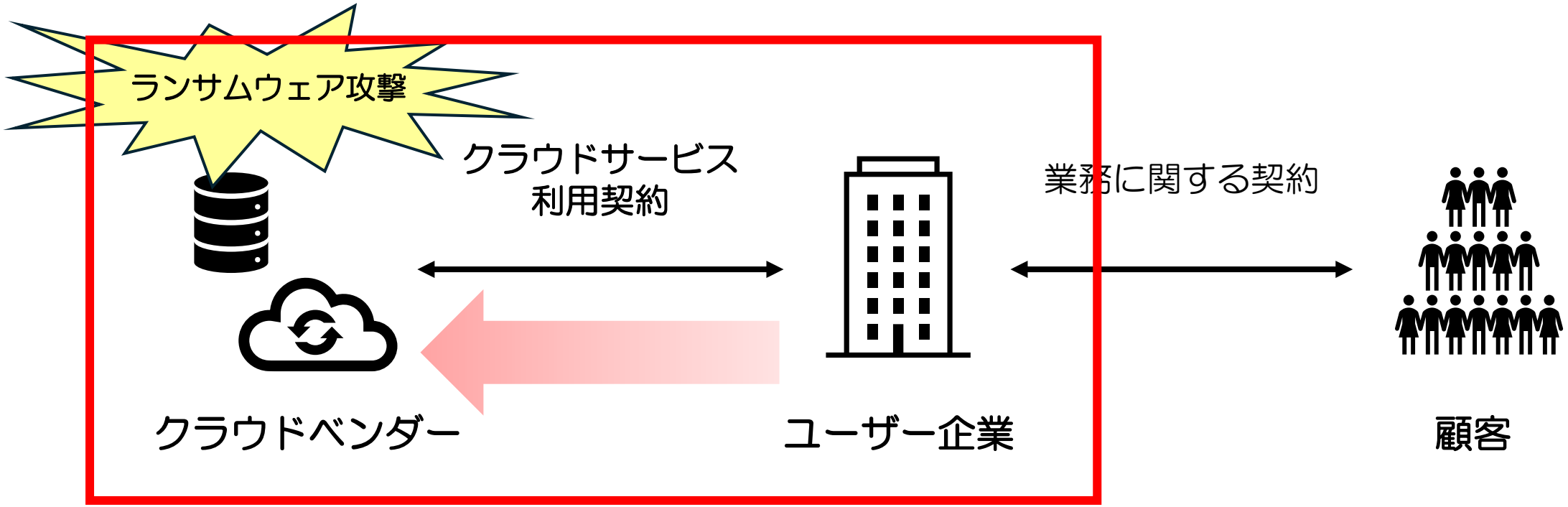
■ 自社が顧客から損害賠償を請求される可能性

- 以下を理由とした債務不履行に基づく損害賠償請求
  - ユーザー企業による業務の履行が遅滞したこと
  - 顧客から受領した機密情報・個人情報を漏えいしたこと（守秘義務違反）
- クラウドベンダーの過失によりランサムウェア攻撃を受けた場合、ユーザー企業の過失（帰責事由）の有無をどのように考えるか？
- **履行補助者の理論**
  - 手足として使用している者の過失を債務者の過失と同視する。

    ⇒ クラウドベンダーの過失をユーザー企業の過失と同視する。

Ⅲ. 利用しているクラウドサービスがランサムウェア攻撃を受ける場合
2. 法的請求の可能性

■ クラウドベンダーに対する損害賠償請求



Ⅲ. 利用しているクラウドサービスがランサムウェア攻撃を受ける場合
2. 法的請求の可能性

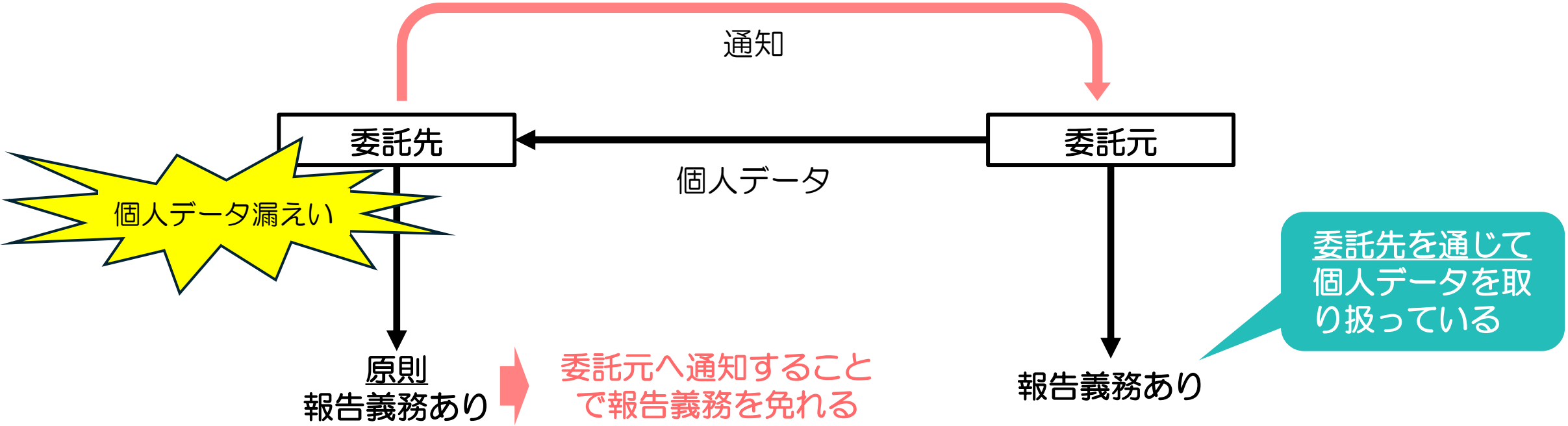
■ クラウドベンダーに対する損害賠償請求

- 以下を理由とした債務不履行に基づく損害賠償請求
  - データが漏えいしたこと（守秘義務違反）
  - クラウドサービスが一定期間提供されなかったこと（役務提供義務違反）
- ただし、ユーザー企業とクラウドベンダーとの間の契約（利用規約）において、**賠償制限条項**が存在する場合がある。
  - クラウドベンダーに重過失がないと、ユーザー企業はクラウドベンダーに対して損害賠償請求できない。

Ⅲ. 利用しているクラウドサービスがランサムウェア攻撃を受ける場合
3. 必要な法的対応

■ 個人情報保護法の適用関係：個人情報の取扱いの委託（個情法27条5項1号）

【個人情報保護法26条1項】
個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより、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らない。



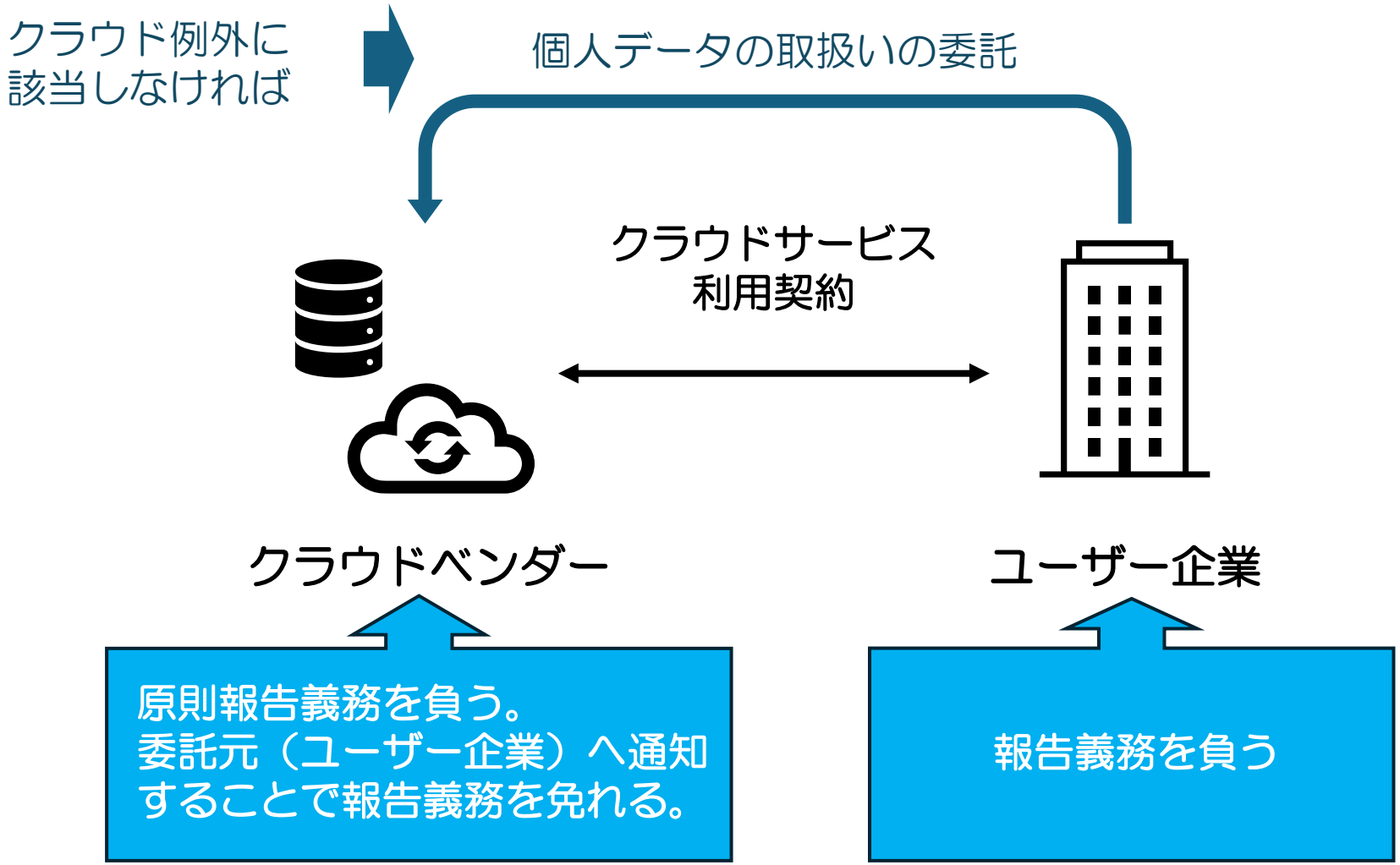
Ⅲ. 利用しているクラウドサービスがランサムウェア攻撃を受ける場合
3. 必要な法的対応

■ クラウド例外

- 委託に該当するかどうかは、クラウドサービス提供事業者において、個人データを取り扱うこととなっているのか又は取り扱わないこととなっているのかのいずれであるかが判断の基準となる（ガイドラインQ&A 7-53）。
- 「個人データを取り扱わないこととなっている場合」とは、契約条項によってクラウドサービス提供事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等が考えられる。
- エムケイシステムは、以下の事情から、「個人データを取り扱わないこととなっている場合」に該当しない（＝委託を受けて個人データを取り扱っている）と判断された。
  - 利用規約において、特定の場合にクラウドサービス利用者の個人データを使用等できることとなっていた。
  - クラウドサービス提供事業者が保守用 ID を保有し、クラウドサービス利用者の個人データにアクセス可能な状態であり、取扱いを防止するための技術的なアクセス制御等の措置が講じられていなかった。
  - クラウドサービス利用者と確認書を取り交わした上で、実際にクラウドサービス利用者の個人データを取り扱っていた。

出典：個人情報保護委員会「クラウドサービス提供事業者が個人情報保護法上の個人情報取扱事業者に該当する場合の留意点について（注意喚起）」（令和6年3月25日）https://www.ppc.go.jp/files/pdf/240325_houdou.pdf

Ⅲ. 利用しているクラウドサービスがランサムウェア攻撃を受ける場合
3. 必要な法的対応



Ⅳ. 取引先がランサムウェア攻撃を受ける場合
1. 想定される損害

- サプライチェーン（製造ライン、物流、業務委託等）の停止
- これに伴う自社の顧客に対するサービス提供の遅延・停止

- 事業の中断による逸失利益
- 顧客離れによる逸失利益
- 追加コスト（代替サプライヤー確保費用等）
- 顧客からの損害賠償請求

- 委託先が管理していた自社の機密情報が漏えい

- 営業機会の喪失、競争力の低下による逸失利益

- 委託先が管理していた自社の顧客情報が漏えい

- 個人情報漏えい対応費用

Ⅳ. 取引先がランサムウェア攻撃を受ける場合
1. 想定される損害

JNSAの「インシデント損害額調査レポート 別紙 2025年版」に掲載されている一例

従業員1,000名～の小売業者

〔事案の概要〕
- 業務の委託先がランサムウェアに感染
- 委託先が管理していた、自社（委託元）の顧客情報20,000件以上が漏えいしたおそれ

〔被害額〕
- 広告・宣伝活動費用　170万円
- コールセンター費用　310万円
- 交通費等　150万円

合計：630万円

- ✓ 詫び状送付（印刷、封入、郵送代金）90万円
- ✓ 公式サイトへの告知文
- ✓ 個人情報保護委員会への報告内容の支援

参照元：
https://www.jnsa.org/result/incidentdamage/data/incidentdamage_20250723.pdf

Ⅳ. 取引先がランサムウェア攻撃を受ける場合
2. 法的請求の可能性

■ 自社が顧客から損害賠償を請求される可能性

■ 取引先に対する損害賠償請求

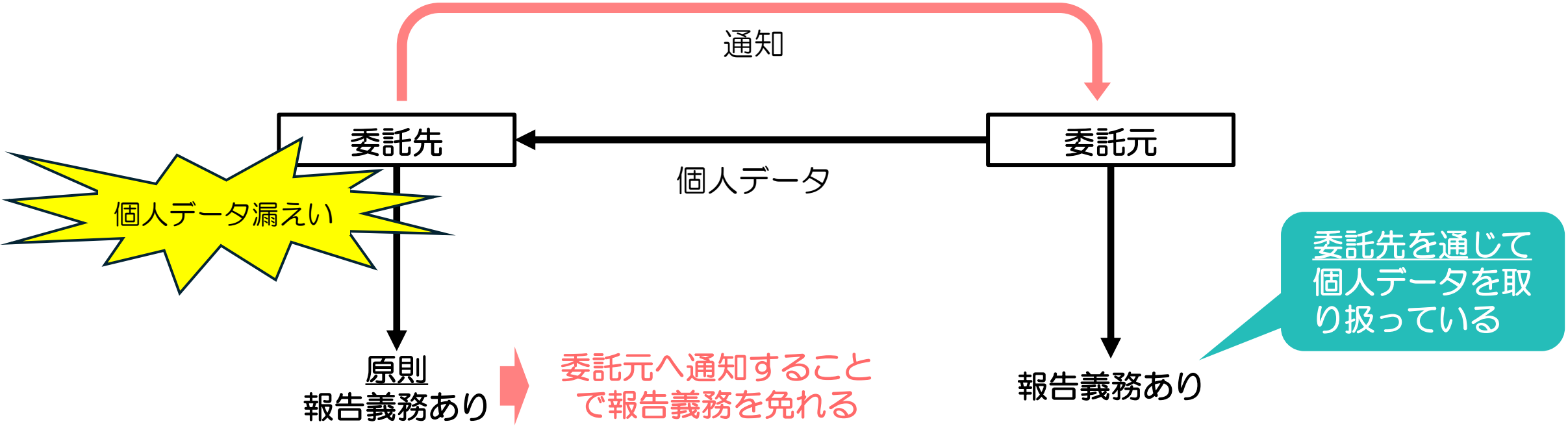
- 自社の機密情報が攻撃者により窃取 ➢ 機密保持義務違反を理由とした債務不履行責任
- 納品の遅れ・サービスの一時中断 ➢ 履行遅滞・履行不能といった債務不履行責任
- 不可抗力・免責条項の有無（前述）
- 賠償制限条項の有無（前述）
- 契約上、取引先に一定のセキュリティ対策を講じることや一定のセキュリティ水準を確保することを義務づける条項がない場合、またはそれが抽象的である場合には、取引先は、セキュリティに関する義務の存在や義務違反の存在を否定して争ってくる可能性が高い。

Ⅳ. 取引先がランサムウェア攻撃を受ける場合
3. 必要な法的対応

再掲

■ 個人情報保護法の適用関係：個人情報の取扱いの委託（個情法27条5項1号）

【個人情報保護法26条1項】
個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより、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らない。



Ⅳ. 取引先がランサムウェア攻撃を受ける場合
3. 必要な法的対応

- 個人データの取扱いの委託の場合における漏えい等報告の方法

  - 委託先と委託元の**連名報告**（個情法ガイドライン（通則編）3-5-3-2）とした上で、委託先が報告書案の作成や提出を行うことができる。

V. まとめ（ポイント）

① 自社が直接攻撃を受けなくとも、クラウドベンダーや委託先の過失は履行補助者の理論等により自社の責任として評価され得ること

② セキュリティ対策の具体的仕様の特定や、重過失時の賠償制限条項の適用排除など、契約設計が責任の帰趨を大きく左右すること

③ 発覚後短期間（速報5日以内等）での報告が求められるため、初動対応の遅れは直ちに法令違反や契約違反に直結し得ること

④ 有事の帰結は平時の備えで決まる。契約確認、インシデント対応体制の整備・訓練、サイバー保険の活用といった事前準備が最重要であること