サイバー攻撃によるリスク対応

「サイバー事故あんしん保険」 資料

アジェンダ

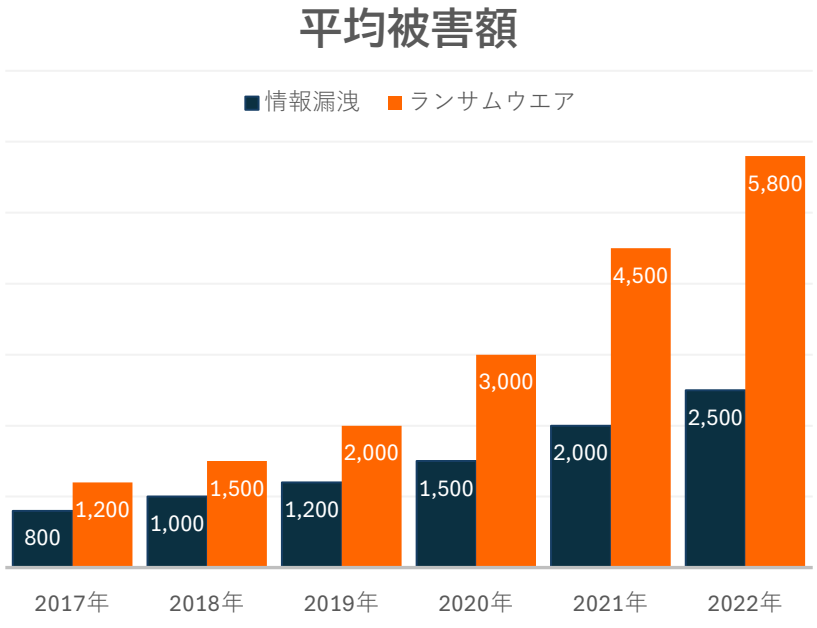
1. 社会動向
2. サイバー攻撃の具体的な事例（宿泊業界）
3. サイバーセキュリティ関連

2025年8月28日

JTB旅連事業株式会社

1. 社会動向：サイバー犯罪の発生件数と被害額の推移（警察庁統計）

サイバー犯罪の検挙件数と被害額は右肩上がりに増加傾向



1. 社会動向：企業対象のサイバー攻撃手口の推移（令和元年～令和5年）

手口分類	令和元年	令和2年	令和3年	令和4年	令和5年	傾向と補足情報
ランサムウエア	120件	150件	180件	217件	222件	中小企業が6割以上を占める
ノーウェアランサム	―	―	―	30件	41件	データ窃取型。BCP未策定企業が多い
不正アクセス（企業対象）	約1,000件	約1,200件	約1,300件	約1,400件	約1,500件	業務システム・クラウドへの侵入が主
ビジネスメール詐欺（BEC）	約300件	約400件	約500件	約600件	約700件	海外送金指示の偽装が中心
サプライチェーン攻撃	―	―	50件	80件	120件	委託先経由の侵入が増加
インターネット詐欺	約800件	約900件	約1,000件	約1,200件	約1,300件	法人名義の偽装・契約詐欺が増加

出典：警察庁「令和6年度におけるサイバー空間をめぐる脅威の情勢等」、帝国データバンク「2025年サイバー攻撃実態調査」、トレンドマイクロ「2024年度サイバー犯罪レポート」

1. 社会動向：規模別サイバー攻撃被害率（全国平均）

「過去にサイバー攻撃を受けたことがある」と回答した企業は全体の32.1%

企業規模	被害経験あり（%）	備考
大企業	41.9%	攻撃対象として目立つ。対策は進んでいるが狙われやすい。
中小企業	30.3%	対策が手薄な企業が多く、被害が急増中。
小規模企業	28.1%	直近の攻撃経験率は高水準。

傾向と実務的インプリケーション（含意）

- **中小企業の脆弱性が顕著**
  →リソース不足や専門人材の不在により、ランサムウェアなどの被害が増加傾向。
- **BCP（事業継続計画）未整備が課題**
  →特に小規模企業では「企業体力がない」「効果が実感できない」といった声も。
- **業種による偏りは少ない**
  →製造業、サービス業、情報通信業など、ほぼ全ての業種で30%前後の被害経験が報告されている。

出典：帝国データバンク「2025年サイバー攻撃実態調査」

1. 社会動向：サプライチェーンと経済安全保障

● 政府主導の評価制度

経済産業省は2026年度開始を目指し、「サプライチェーン強化に向けたセキュリティ対策評価制度」を構築中。企業のセキュリティ水準を★3～★5で可視化し、取引先選定の基準とする動きが加速。

● 中小企業への支援策

IPA（情報処理推進機構：経済産業省のIT政策実施期間）による「セキュリティアクション」や「サイバーセキュリティお助け隊」など、宿泊業を含む中小企業向けの支援制度が拡充。

● 取引見直しの現実化

脆弱な企業が攻撃を受けた場合、サプライチェーン全体が停止するリスクがあるため、発注側がセキュリティ対策を条件に取り引きを見直す事例が増加。

2. サイバー攻撃の具体的な事例：被害事例1

被害事例１：国内宿泊施設の予約サーバーへのサイバー攻撃（2020年）

	内容
概要	宿泊施設の予約システムへの不正アクセス
手口	①宿泊施設の予約システムが外部からの不正アクセスによるサーバー侵入を受ける。 ②詳細な手口は非公表、侵入経路は不明
影響・被害リスク	・宿泊予約の利用情報（最大46,630件）の流出 ・個人情報（最大43,213名分）の流出 ・パスワードや個人情報が暗号化されずに保存されていたため、流出時に直接的な被害に ・情報漏えいに伴う信用毀損および法的リスク（*）改正個人情報保護法により、対象者が1,000人を超える場合、要配慮個人情報が含まれる場合、財産的被害のおそれのある場合、不正な目的による漏会の場合に、個人情報保護委員会への報告義務（最大1億円の罰金）。
復旧対応 再発防止策	①専門業者によるフォレンジック調査：不正アクセスの経路や漏えい範囲を特定 ②該当サーバー辺の通信遮断 ③相談窓口の設置

※過去に外部からの不正アクセスで12万件以上の個人情報を流出した事例もあります。

2. サイバー攻撃の具体的な事例：被害事例2

被害事例２：国内宿泊施設の予約サーバーへのサイバー攻撃（2020年）

	内容
概要	宿泊施設の予約システムへのランサムウエア攻撃
手口	①攻撃者はフィッシングで従業員のアカウント・認証情報を窃取。 ②内部ネットワークに侵入後、予約管理システムのデータを暗号化。
影響・被害リスク	・一部データは破壊され、復旧不能な領域も発生。 ・顧客情報がアクセス不能に（復旧に数週間要した）。
復旧対応再発防止策	①専門業者によるフォレンジック調査：不正アクセスの経路や漏えい範囲を特定 ②該当サーバー辺の通信遮断 ③相談窓口の設置

2. サイバー攻撃の具体的な事例：被害事例3

被害事例３：国内宿泊施設の予約サーバーへのサイバー攻撃（2020年）

	内容
概要	PMSのゼロデイ脆弱性を突いたサイバー攻撃
手口	①大学内の宿泊施設の予約システムが外部からの不正アクセスによるサーバー侵入を受ける。 ②詳細な手口は非公表、侵入経路は不明
影響・被害リスク	①攻撃者がPMSのAPI連携部分の認証回避ゼロデイを悪用。 ②館内のIoT連携（スマートロック、空調制御など）システムが停止。 ③顧客情報が暗号化され、ランサム要求も発生。 ④未修正のブラウザ脆弱性を突かれ、個人情報が流出した。 ⑤情報漏えいに伴う信用毀損および法的リスク
復旧対応 再発防止策	①専門業者によるフォレンジック調査：不正アクセスの経路や漏えい範囲を特定 ②該当サーバー辺の通信遮断 ③相談窓口の設置

※API連携部分の認証回避ゼロデイとは・・・開発元が対策パッチを公開するまでの間に、攻撃者がAPI連携部分の脆弱性を突いて、本来必要な認証プロセスを不正に回避し、サイバー攻撃すること。

2. サイバー攻撃の具体的な事例：被害事例4

被害事例４：ホテル予約サイトへの疑似DDoS攻撃（2023年）

	内容
概要	ホテル予約サイトへの海外からの大量アクセスによるサーバーダウン
手口	①海外IPアドレスからホテル予約サイトへ異常なトラフィックが集中 ②サーバーが過負荷状態に陥り一時的にダウン
影響・被害リスク	・サーバー停止による業務妨害（予約受付・管理業務の停止） ・顧客対応の遅延による信頼瀬の低下 ・予約管理システムへの侵入 ・顧客情報の窃取やフィッシング詐欺への布石
復旧対応 再発防止策	①専門業者によるフォレンジック調査：不正アクセスの経路やマルウエア感染の有無を確認 ②技術的措置：サーバー復旧費用、セキュリティ対策費用 ③顧客補償対応（返金・再予約） ④組織的措置：個人情報取り扱いルールの強化 ⑤人的措置：従業員教育とルール徹底

2. サイバー攻撃の具体的な事例：被害事例5

被害事例５：海外OTA宿泊予約管理システムをめぐる不正利用（2024年）

	内容
概要	大手海外OTA宿泊予約管理システムのメッセージ機能を悪用したフィッシング詐欺
手口	①攻撃者が宿泊施設に偽予約メールを送信。 ②マルウエア感染によりID・パスワードを窃取。 ③海外OTA管理システム（メッセンジャー機能）に不正ログイン。 ④宿泊施設になりすまし、予約客に偽メッセージを送信。 ⑤フィッシングサイトに誘導し、個人情報等を搾取。
影響・被害リスク	・個人情報・予約情報の閲覧・流出 ・個人情報漏えいに伴う信用毀損および法的リスク
復旧対応 再発防止策	①専門業者によるフォレンジック調査：不正アクセスの経路やマルウエア感染の有無を確認 ②技術的措置：メールシステムのセキュリティ強化 ③組織的措置：個人情報取り扱いルールの強化 ④人的措置：従業員教育とルール徹底

2. サイバー攻撃の具体的な事例：被害事例6

被害事例６：海外OTAの宿泊施設管理システムを経由したフィッシング詐欺（2023～2024年）

	内容
概要	大手海外OTA宿泊施設管理システムを標的にした多段階型フィッシング詐欺（100施設以上）
手口	①攻撃者が宿泊施設に「アレルギー対応」「バリアフリー確認」等のマルウエア付きメールを送信。 ②宿泊施設の端末が感染し、海外OTAの認証情報を窃取。 ③攻撃者が施設の海外OTAの正規アカウントに不正ログイン（アカウント乗っ取り）。 ④宿泊施設になりすまし、予約客に「支払いエラー／予約キャンセルの恐れ」等の偽メッセージを送信。 ⑤フィッシングサイトに誘導し、個人情報・クレジットカード情報等を搾取。
影響・被害リスク	・個人情報・クレジットカード情報の流出および信用毀損、問い合わせ対応など業務負荷の増大 ・管理画面が乗っ取られ、予約客との通信が改ざん（予約管理が不能） ・偽サイトでのカード情報の入力による予約客の不正決済被害
復旧対応 再発防止策	①専門業者によるフォレンジック調査：不正アクセスの経路や漏えい範囲を特定 ②端末の隔離・再構築 ③技術的措置：CDN、EDR、SOC、二要素認証の導入やアクセス権限の厳格化 ④組織的措置：セキュリティポリシーの見直しと従業員教育

2. サイバー攻撃の具体的な事例：被害事例7

被害事例７：委託業者システムの脆弱性を突いたサイバー攻撃（2022年）

	内容
概要	給食業者のシステムの脆弱性を悪用した総合医療センターへのランサムウエア攻撃
手口	【概要】①総合医療センターが身代金要求型ランサムウエアによるサイバー攻撃を受ける。 ②基幹システムサーバが暗号化され、電子カルテが使用不能に。 ③外来診療や救急患者の受け入れを停止するなど、診療体制が大幅に制限された。 【原因】①給食業者のVPN機器の脆弱性が放置されていた。 ②全ユーザーに管理者権限が付与されていた。 ③サーバーやPCに共通のID・パスワードを使用していた。 ④電子カルテサーバにウイルス対策ソフトが未設定だった。
影響・被害リスク	・被害額約20億円（①調査復旧費：数億円、②復旧まで約2カ月半期間の診療制限（初診患者数約18%減、新規入院患者数約33%減）による逸失利益：十数億円規模 ・民間事業者3社（給食業者、システム開発業者など）が総合医療センターを管轄する地方行政独立法人病院機構へ10億円の解決金を支払う内容で和解が成立。
復旧対応 再発防止策	①医療機関における委託業者のセキュリティ管理責任の明確化 ②システム設計の基本的な安全性の確保

3. サイバーセキュリティ関連：サイバー攻撃対策（例）

サイバー攻撃対策		サプライチェーン対応
技術的対策	組織的対策	
● WAF（Webアプリケーションファイアウォール）導入 → 予約サイトや決済ページをSQLインジェクション等から保護 ● VPNの活用 → 館内Wi-Fi利用時の通信暗号化で顧客情報を保護 ● 不正改ざん防御・検知サービス（EPP/EDR） → 予約ページの不正改ざんを未然防御、即時検知・復旧	● 従業員教育 → フィッシングメールの見分け方、パスワード管理、インシデント対応訓練 ● 情報管理体制の整備 → 個人情報の暗号化、不要情報の収集回避、GDPR等の海外法令への対応 ● 多要素認証の導入 → 予約管理システムや社内ネットワークへのアクセス制限強化	● 委託先のセキュリティ確認 → 予約システムや清掃業務などの外部委託先のセキュリティ水準を評価 ● 取引先との契約書へのセキュリティ条項の追加 → 情報漏洩時の責任分担や報告義務を明記

3. サイバーセキュリティ関連：サイバー攻撃等によるインシデント対応費用（例）

主な対応事項例	主な対応内容例	外部委託費用例
原因究明・影響範囲調査 （インターネット出入口1箇所、 調査対象PCは2～3台レベル）	■ 被害状況の確認、証拠・痕跡の保全状況から事故査定（⇒約100万円） ■ ログ解析、フォレンジック調査等の調査・分析、IPSなど不正侵入防御装置の設置等、被害拡大防止をサポート（⇒約1,000万円）	約1,100万円
謝罪、報告、社外公表等の 広報対応	■ 被害者への謝罪、関係機関への報告、社外公表文書、緊急記者会見用の報道発表資料・想定Q＆Aの作成助言・レビュー、緊急記者会見の手順等のコンサルティングなど各種の広報対応のサポート	約300万円
専用コールセンターの設置・運営（被害者数百人規模、機微情報を含む漏えい）	■ コールセンターに専用のコール受発信ブース設置、3週間の照会対応実施（初日と第3週目：5ブース、2～14日目：10ブース） ■ 受付／結果の入力、受付結果の日時報告	約700万円
対外説明や再発防止策の実施に向けた事故の評価	■ 第三者を含む委員会等の設置による調査結果や再発防止策の公表等	約200万円
弁護士等への相談	■ 外部提供文書のレビュー・指導、個人や企業など個別紛争への対応等	約200万円
その他の費用	■ 個人情報漏えいのお詫び近であれば@500×被害者人数、暗号化されたデータを再作成するための費用、その他にも臨時雇用費用、ベンダーへの追加費用（保守契約外の作業費用）等	プラスα
外部委託費用に係る合計費用（イメージ）		約2,500万円 プラスα

＊費用の多寡は、企業規模よりも、サイバー事故の内容と影響規模により大きく変動します。

3. サイバーセキュリティ関連：サイバー事故あんしん保険

- **賠償責任・事故発生時の各種対応費用を包括的に補償**

  サイバーリスクに起因する事故が発生した場における「賠償責任」「事故対応に要する諸費用」を総合的に補償

- **事故初動から再発防止までに要する費用をトータルで補償**

  サイバーリスクに起因する事故が発生した場における「初動対応→原因調査→被害抑制→事態収拾→再発防止」までの対応に要する費用をトータルで補償

- **事故発生の“おそれ”に対応する費用も補償**

  サイバー攻撃のおそれが発生した場合において、これらの発生の有無を調査するために要した費用も補償
  （外部からの通報などによりサイバー攻撃のおそれが発見された場合に限ります）

＜ご加入プラン＞以下4つプランの中からお選びいただけます。　※年間保険料は売上高区分に基づきます。

お薦め

プラン	(A)事故対応費用保険金	(B)賠償保険金
【A】　充実プラン	3,000万円	3億円
【B】　あんしんプラン	1，000万円	1億円
【C】　お手頃プラン	500万円	5,000万円
【D】　ライトプラン	300万円	3，000万円

JTB

感動のそばに、いつも。