

旅行業界情報流出事案検討会 中間とりまとめ
～旅行業情報セキュリティ向上のため早急に講ずべき対策～

平成 28 年 7 月 28 日

「旅行業界情報流出事案検討会」

委員名簿

(委員長)

- 浅野 正一郎 交通政策審議会会長
情報・システム研究機構国立情報学研究所名誉教授
- 小野 睦 KNT-CTホールディングス(株)
経営戦略統括部(IT戦略) IT戦略担当部長
- 梶浦 敏範 一般社団法人日本経済団体連合会情報通信委員会
サイバーセキュリティに関する懇談会 座長
インターネット・エコノミー民間作業部会 主査
- 小松 信行 一般社団法人全国旅行業協会東京都支部運営委員
- 坂 明 一般財団法人日本サイバー犯罪対策センター 理事
- 西見 俊彦 国土交通省最高情報セキュリティアドバイザー
富士通(株) サイバーディフェンスセンター
シニアエキスパート

【目次】

1. はじめに.....	1
2. 事案の検証.....	2
(1)株式会社ジェイティービー事案.....	2
(2)札幌通運株式会社事案.....	8
3. 観光庁の対応について.....	14
4. 再発防止策に向けての提言.....	16
(1)旅行業者が早急にとるべき対応.....	16
(2)中堅・小規模旅行業者がとるべき対策.....	18
(3)観光庁が早急にとるべき対応.....	19
(4)今後検討すべき事項.....	19
5. おわりに.....	21
用語集.....	22

1. はじめに

平成 28 年 6 月 14 日、(株)ジェイティービーより個人情報漏洩の可能性があると
の記者会見が行われた。同社に対する標的型メール攻撃により 6,788,433 名分の情
報が漏えいした可能性があった。翌々日 16 日には札幌通運(株)からも個人情報漏
洩事案が発生したとの記者会見が行われた。同社のホームページに対する攻撃であ
り、2,519 件の個人情報が漏洩し、クレジットカードの不正使用も認められた。相次ぐ
旅行業者の個人情報漏洩については報道でも大きく取り扱われ、旅行業者の情報セ
キュリティ対策が社会的に大きな注目を受けることとなった。

IT化の進展に伴い旅行業をとりまく環境は大きく変化している。これまで旅行業は
店頭型の旅行商品販売が多かったが、IT化の進展に伴い、インターネットを通じた電
子旅行取引が多くなっている。これら電子商取引を通じた情報の中には顧客の購入
履歴等の重要な営業ノウハウが蓄積されており、これらが流出した場合には、我が国
の重要産業である観光に携わる旅行業者の安定したビジネス継続に大きな影響を与
えかねない。

また、ロンドンオリンピックではその期間中に約 2 億回のサイバー攻撃を受けたと
いわれており、2020 年の東京オリンピックを控え、訪日外国人客数が 2,000 万
人を超え訪日外国人客数 4,000 万人を目標とする我が国としては旅行業界の情報
セキュリティ対策は喫緊に取り組むべき課題である。

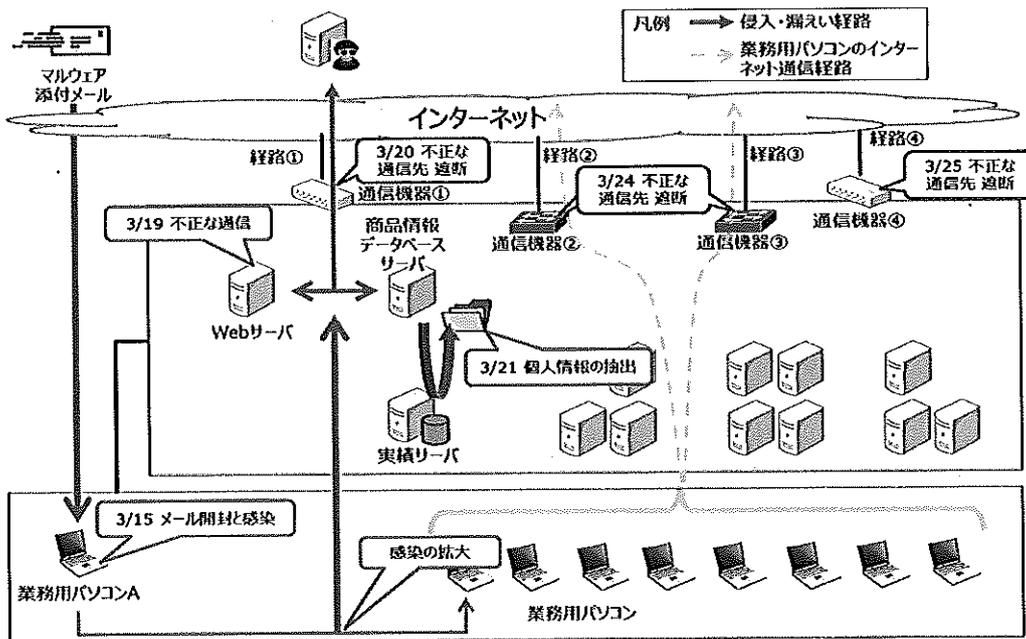
本検討会は、観光庁長官の指示を受け、両社の事案を検証するとともに旅行業界
として情報セキュリティ向上のために取り組むべき対策について提案するため設立さ
れ、2 回の検討会が行われた。情報セキュリティ対策に終わりはないが、今般の事案
に対し両社が講じた当面の対策に対する評価と旅行業界として再発防止に向けた提
言についてとりまとめたものである。

2. 事案の検証

(1) 株式会社ジェイティービー事案

① 本事案の概要

本事案は、株式会社ジェイティービー（以下、「JTB」）のインターネットを活用して旅行商品の販売を行っている株式会社 i. JTB（以下、「i. JTB」）のオペレータ端末において、取引になりすました不正な添付ファイルを開いたことによる標的型攻撃により、クライアントパソコンがマルウェアに感染した。その後、外部からの遠隔操作により感染が拡大し、個人情報のあるサーバへ攻撃者が侵入した事案が発生した。株式会社 JTB 情報システム（以下、「JSS」）では、外部に委託しているセキュリティ監視会社より内部から外部に向けた不正な通信を検知した旨の連絡を受け事案の対処を行ったが、個人情報のあるサーバへ攻撃者が侵入していることから、情報が流出した可能性がある。



② システムの運用及び体制

本事案にて関係する主なシステム運用体制は、JTB、i. JTB、JSS 及びセキュリティ監視会社となる。

本事案の対象となるシステムは、BtoC 向けシステム（JTB ホームページシステム、るるぶトラベルシステム、JAPANiCAN システム）であり、システムの目的は、JTB ホームページ、るるぶトラベル、JAPANiCAN 及び JTB グループ内

外のオンライン販売提携サイトにおける旅行商品の検索からログイン、オンライン販売（予約と決済）機能を提供し、旅行販売を行うことである。

③被害状況

個人情報流出の可能性があり、対象となるサイトと期間は以下の通り。

対象 Web サイト：JTB ホームページ、るるぶトラベル、JAPANIcAN、JTB グループ内外のオンライン販売提携サイト

データ対象期間：2008 年 9 月 28 日～2016 年 3 月 21 日午前 1 時 32 分までのオンライン予約分

流出の可能性のある個人情報項目は以下の通り。

氏名（漢字、カタカナ、ローマ字）、性別、メールアドレス、住所、郵便番号、電話番号、パスポート番号、パスポート取得日、

流出の可能性のある個人情報の人数：6,788,443 名

流出の可能性のあるパスポート番号の件数：約 4,300 件（現在有効なもの）

④従前の情報セキュリティ対策

従前の情報セキュリティ対策は、一般的な対応であると言える。

外部のセキュリティ会社と連携をし、かつ BtoC 向けシステムの不正アクセス監視を行っている。

また、ウイルス対策ソフトの導入と運用、資産管理ソフトウェアを用いた不正なソフトウェア導入の抑止、ログ管理ソフトウェアを用いた業務用パソコンにおけるファイル操作の記録を行っており、平均以上の対策を講じていると言える。

さらには、教育として勉強会に加え、i. JTB、JSS において月 2 回の標的型攻撃の模擬訓練の実施は一般的な回数以上（通常は年 1 回程度の実施）と言える。

検知後の対応としては、外部への通信ログの定期チェック及び不審なログを確認した場合、都度調査及び通信停止措置（通信経路の遮断）、復旧対策として問題発生時の業務用パソコン、サーバの初期化・再構築手順の作成を実施しており、一般的な対応と言える。

しかし、今回の事案が発生したことは、情報セキュリティ対策の困難さを示すものであり、どこまで事案を想定することができていたかによることが大きい。

⑤本事案での対応及び検討点

標的型攻撃に対して実施してきた対応を振り返ると、いくつかの分岐点がある。標的型攻撃事案を過去経験してきている、または、具体的な対処方針を理解しているかどうかで、これらの分岐点で被害が拡大しない方向へ向かうことができるため、事案発生後の対応を振り返ることは有意義であり、その観点で以降は分岐点を見極めていく。

i) 検知

(今回の経緯)

2016年3月19日にセキュリティ監視会社より、「i. JTBのWebサーバから外部に向けた不正な通信を検知した」との連絡があった。通知を受けたJSSは、i. JTBへ連絡を行うとともに当該サーバをネットワークから切り離し、ウイルスチェックを実施した。

(考察)

セキュリティ監視会社は、単なるブラックリストによる検知ではなく、パケットの内容を確認し、その内容から標的型攻撃によく見られる特徴の情報が得られている。検知連絡を受けた側に、このような攻撃に対する対応経験又は知識があれば、より徹底した調査が必要と判断できたものと推測する。この時点において、セキュリティ監視会社がJSSのどちらかが適切な初動対応を実施することができていた場合、被害は縮小化できていた可能性がある。

ii) 対処

(今回の経緯)

2016年3月20日に行ったウイルスチェックの結果、異常は検出されなかったとJSSからi. JTBへ報告し、経路①上にて不正な通信先と思われるIPアドレスを遮断した。

2016年3月24日～同年3月25日に経路①以外のインターネット接続通信経路を確認し、それぞれで不正な通信先を遮断した。

(考察)

標的型攻撃で使用されるマルウェアや不審なファイルは、ウイルスチェックではほとんど検出されることがないことを理解していることで、違った対応が取れた可能性がある。

また、3月20日に一つの経路を遮断後、3月25日まで通信経路を確認し遮断しているが、標的型攻撃の場合、外部への通信経路は複数使用してC&Cサーバとのやり取りを行うことが一般的である。3月21日に業務上不要なGSVファイルが作成されたとあるが、この時点で外部との通信経路を全て把握し、3月20日の時点において全て遮断していれば、GSVファイルを作成されなかった可能性がある。

これらは、本検証の目的でもある事案を理解することで、今後の再発防止策を検討する上での重要なポイントとなる。

iii) 調査・報告

(今回の経緯)

2016年3月26日～同年4月1日にかけて業務用パソコン及びサーバを調査した後、同年4月13日にGSVファイルが実績サーバにあるデータである可能性が高いことを確認した。

(考察)

この4月13日の時点で、攻撃者による重要なデータの閲覧又は窃取された可能性があるかと推測できる。その後行われる同年5月13日のJTBのIT部門、i. JTB、JSSでの説明会、同年5月16日のJTB担当役員及び内部統制部門への報告は、4月13日直後に実施されるべきであった。

(今回の経緯)

2016年5月30日～同年6月2日にかけて、警察及び監督官庁(観光庁)に連絡が実施される。

(考察)

JTB担当役員への報告の遅延にも関係するが、事案の重大性を認識してからの行動には改善の余地がある。

出来る限り正しい情報を伝えるということは一定の理解はできるが、何かしらの対策を実施する必要がある中で、各セクションや幹部、関係機関への連絡が遅くなることで少しずつ対応が遅れていくことは、標的型攻撃のこれまでの例からしても致命的となる可能性がある。

⑥事案判明後の対応

(今回の経緯)

本事案判明後、JSS を中心とする CSIRT チーム立ち上げ及びグループ各社緊急対応体制の構築、また、JTB 内に社長を本部長とする事故対策本部を設置し、連絡体制を改善している。

事案後の対処としては、IP アドレス及び URL によりフィルタリングを実施し、不正な通信先（監視で検知された通信先及びマルウェア検体から抽出された通信先）のアクセスを阻止、本件調査で得たマルウェアの検体をウイルス対策ソフトメーカーに提出、パターンアップデートの実施、グループ各社の業務用パソコン及びサーバ類のフルスキャン検査の実施を行った。

(考察)

不正な通信先の遮断やパターンファイルアップデートでの対策だけでは、このような標的型攻撃は、まだマルウェアが潜伏している可能性があるが、ネットワーク上での調査なども実施しているということで対処は概ね問題ないと思われる。

(今回の経緯)

また、外部からのインターネット接続経路箇所（経路①④）の不正アクセス監視の継続、i. JTB の業務用パソコンの管理共有設定の停止とインターネット閲覧の停止、i. JTB のサーバでの遠隔操作を禁止と個人情報を格納しているサーバへのアクセス制御、実績サーバから個人情報の削除を行っている。

顧客対応としてコールセンター設置及びご相談窓口案内のメール通知を実施している。

(考察)

本事案の件については、当面の対策は講じられたと言える。

(今回の経緯)

さらに JTB では当面の再発防止策として、以下の対策を実施するとしている。

- ・システムのセキュリティ強化

(全ての経路でのログ監視。ログ記録保存期間の長期化。個人情報データベースサーバのアクセス制限の強化。)

・体制の整備・強化

(専務取締役を CISO に任命。IT セキュリティ対策専門部署を設置。当該部署には情報セキュリティ・インシデント対応の経験者や情報セキュリティを研究し、社外の様々な個人情報流出事案の収集、分析に詳しい者、グループ企業の IT 推進を担当し、グループ内及び本社との円滑な情報伝達、共有を図る者を配置。)

・運用管理の強化

(CSIRT をシステム専門のグループ会社ではなく、本社内に設置し、グループ会社で事案に対しては本社が経営の危機管理の観点から対応。外部専門家の契約を通信の監視から危機対応含む全般的なコンサルタント契約へ強化。)

・研修・演習の実施

(考察)

今後のサイバー攻撃事案に対して、被害を縮小化または防止する当面の対策を講じていると言える。今後、継続的な運用において実効性を維持・向上していくことが重要である。

⑦本事案の原因

本事案は、オペレータが取引先を装った不正添付ファイル付メールを受信し、その添付ファイルを開いたことを発端とする情報流出事案であるが、添付ファイルを開いたことではなく、その後事案を縮小化できる機会を逃し、かつ重要情報が流失した可能性があるにも関わらず、経営層や監督官庁への報告が遅れた点が課題となる。

以下に、本事案において被害拡大を防げなかった原因と思われるポイントを挙げる。

i) 標的型攻撃に対しての情報不足

本事案を当初発見した IT 担当部署・担当者に、標的型攻撃に対する相応の知識があった場合、今回の事案による被害は拡大しなかった可能性がある。標的型攻撃を受けていない時においても、不断の情報共有のあり方を

検討しておく必要があると言える。

ii) 自社システムの理解不足

不正な通信先との通信遮断を実施するまでの日数に時間を要している。複数のシステムに亘っていることが原因と考えられるが、標的型攻撃の対処としては、インターネット接続口がどこにどれだけあるかを平時から把握しておく必要があったと言える。

iii) ネットワーク構成の問題

不正な添付ファイルを開いてから、CSV ファイルを作成するまで約 6 日間で実行されている。これは、業務端末から重要情報を持つサーバに到達する日数としては通常より早いと考えられる。業務ネットワークと重要情報を持つサーバ群との境界が弱かったのではないかと思われ、各セグメントの境界をより一層厳しくする必要があると言える。

iv) 事案発生時のマネージメント体制不足

個人情報流出などの情報セキュリティ・インシデントは、経営に影響を与える重大な問題と捉え、インシデント把握の端緒となる情報の迅速な共有も含め、状況を見極めて早期に対応できる体制を構築し、業界の見本となることが望まれる。

v) 担当役員及び監督官庁への速やかな報告

本事案では被害拡大の原因とはならなかったが、事案を検知し、情報流出の可能性が認められた時点で、担当役員、監督官庁へ報告及び公表がなされなかった点も指摘しておきたい。二次被害を防ぐ観点からも速やかに報告及び公表がなされるべきであると言える。

(2) 札幌通運株式会社事案

① 本事案の概要

本事案は、外部から札幌通運株式会社(以下、「札幌通運」)の旅行業ブランドである「クラブゲッツ」(以下、「クラブゲッツ」)の Web サイトへサイバー攻撃があり、顧客の個人情報が流出したと判断した事案である。

サイバー攻撃の種類としては、現時点においては「SQL インジェクション」と思われる。

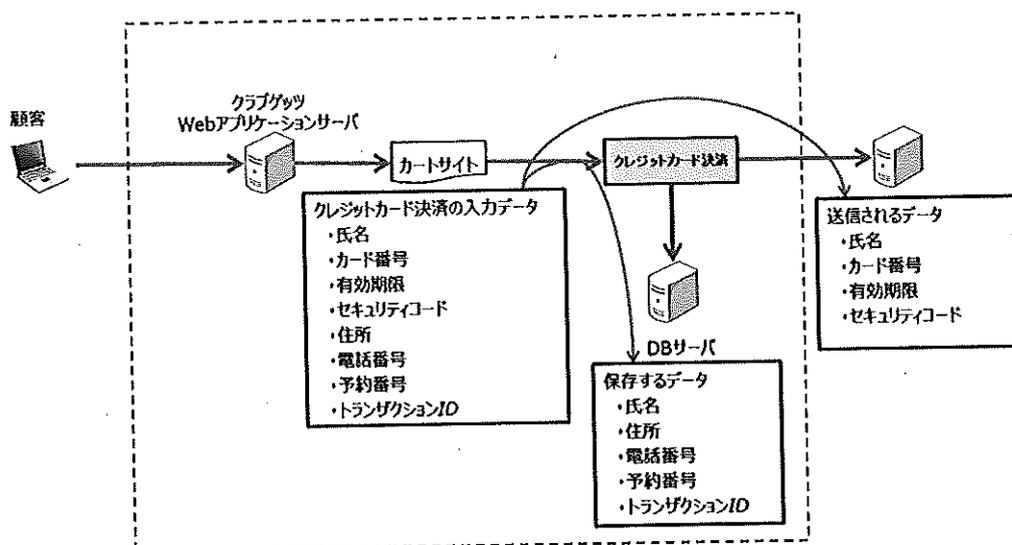
「SQL インジェクション」は、公開している Web サイト上で動作する Web アプリ

リケーションの脆弱性を狙って、その脆弱性を利用し Web サイトと連動しているデータベースを不正に操作し、データを窃取等する攻撃である。

ただし、現状は根本原因の調査中であるため、個人情報が流出した原因が「SQL インジェクション」であるかどうかは確定していない。

②システムの運用及び体制

札幌通運は、クラブゲッツを運用するにあたり、旅行業システムを開発、運用しているシステムベンダー兼サービスプロバイダー(以下、「システムベンダー」)へシステムの開発及び運用を委託している。なお、Web サイトのシステムは、システムベンダーが契約している電力系データセンターに設置されている。Web サイトにおける旅行代金の代金収納は、決済代行会社に委託している。



③被害状況

今回のサイバー攻撃にて発生した被害は、個人情報 2,519 件と想定されている。件数の根拠としては、本事案後にセキュリティ調査会社が調査した結果として、2016 年 1 月 3 日～同年 1 月 31 日の期間にてクラブゲッツの Web サイトへ大量の SQL インジェクションの形跡があったことからそれ以前から発生していたであろうこと、また、カード会社からの情報提供にて被害発生時期が 2015 年 11 月 5 日からであるが、そのカードのクラブゲッツ利用時期が 2015 年 10 月以降に集中していることから、2015 年 10 月 1 日～2016 年 3 月 4 日(クラブゲッツの Web サイトカード決済停止日)の間、クラブゲッツにてカ

ード決済を行った件数を個人情報流出の被害件数と判断している。

④従前の情報セキュリティ対策

上記システムの運用及び体制にて記述している通り、システムはシステムベンダーが運営・管理しているが、このシステムの情報セキュリティ対策は、契約上、札幌通運とシステムベンダーの責任範囲が明記されておらず、責任が不明確で、委託会社に対する管理監督責任が果たされていなかった。

また、実施していた情報セキュリティ対策は以下の通りである。

- ・ファイアウォールの設置
- ・ファイアウォールによる不正アクセス検知
- ・グループにて個人情報保護方針、情報セキュリティ規定を定め、従業員の個人情報を含む情報の取り扱いについての啓発活動実施

(考察)

システム全体をシステムベンダーに委託していたが、契約において情報セキュリティの実施内容を盛り込んでいなかったことから、情報セキュリティ対策はシステムベンダーとの関係で不明確であり、本事案発生の原因となっている。ファイアウォールは設置されているが、ファイアウォールのポリシー(ルール)はアクセス制限が十分でなく、Webサーバを公開しWebアプリケーションが動作しているにも関わらず脆弱性診断を実施せず、開発におけるセキュアコーディングも十分ではなかった。ファイアウォールでは、「SQLインジェクション」のようなWebアプリケーションの脆弱性を狙った攻撃は防げないことを、サービス委託を行う業者として理解しておく必要がある。

今後、ますますシステムの外部委託やクラウドサービスが増えていくことが想定されるが、業者の選定時に情報セキュリティ対策を確認すること及び対策の実施責任について契約に盛り込むことが推奨される。

⑤本事案での対応及び検討点

i) 初動及び調査依頼

(今回の経緯)

2016年3月2日にクレジットカード会社より、カード不正利用の可能性に伴いフォレンジック調査を依頼されるが、その時点では、システムベンダーからは他者との共有であることを理由として、データベースのログの提供や

サーバへのアクセスの協力が得られなかった。

(考察)

外部委託のシステムやクラウドサービスなど、自社独自のオンプレミスシステムでない場合、このような情報セキュリティ・インシデントの調査の実施や協力を得る際に、困難を極めることが多い。

したがって、上記従前の情報セキュリティ対策と同様、外部委託やクラウドサービスを利用する場合には、このようなリスクがあることを認識したうえで、インシデント発生時のデータ保全、原因調査、犯罪捜査等の観点も含めて契約内容を確認等することが望ましい。

ii) 調査

(今回の経緯)

2016年3月11日以降、クレジットカード会社、札幌通運、システムベンダー及び弁護士等とのやり取りを経て、同年4月5日にフォレンジック調査をセキュリティ調査会社へ依頼した。

(考察)

そもそも、「クレジットカード会社との加盟契約からフォレンジック調査等を行う義務がある」という契約でありながら、システムベンダー等とそのような契約及び情報セキュリティ・インシデント対応フローがないことは、情報セキュリティ・インシデントに関する考慮が不足していたと考えられる。しかしながら、ビジネスを行いつつ、システムやニーズを日々更新していく必要があり、過去の契約のまま引き続いて運用しているケースは非常に多いと考えられ、今回の件を教訓に情報セキュリティ・インシデント対応についてよく検討する必要がある。

また、CISO や CSIRT のような情報セキュリティの事案が発生した場合の体制にも問題があったと言える。このような事案を例として、旅行業界内にて CISO や CSIRT などの情報セキュリティ・インシデントが発生した際の体制を整えておくことの重要性を共有していくことが望ましい。

iii) 調査結果

(今回の経緯)

2016年5月30日にセキュリティ調査会社より、「特定の URL のみを狙った SQL インジェクション攻撃が多量に行なわれていること、お客様との渉外対応の際に業務オペレータが記録したカード番号がデータ内に記録されたままになっていた(203件)ことから、SQL インジェクション攻撃により、DB サーバからカード会員データを不正に取得されていたものと考えられる。」との報告がある。また、同年5月23日時点で直接的な原因とされた SQL インジェクションの脆弱性は、被害のあった Web サイトでは解消されたとの報告であった。

なお、2016年1月2日以前のログは、保管されておらず調査はできていなかった。

(考察)

この調査結果には様々な矛盾点があり、きちんと精査する必要がある。

報告書の「特定の URL のみを狙った SQL インジェクション攻撃が大量に行われていた」という内容と、「お客様との渉外対応の際に業務オペレータが記録したカード番号がデータ内に記録されたままになっていた(203件)こと」の関連性について記述がない。特定の URL を狙った大量(2,900件)の攻撃のログ(2016年1月)が存在していたのであれば、情報漏えいしたと思われる2015年10月から12月のログが保存されていなかったとしても、データベース内に記録されていた203件のデータを窃取できる攻撃であったかどうか判明できたと考えられるが、調査では明らかにされていない。また、203件のデータには漏えいの形跡は無く、攻撃との関連が不明である。加えて、被害のあった Web サイトの SQL インジェクションに対する脆弱性は、2016年5月23日に調査した時点で解消していたとのことであるが、同年1月の時点でその脆弱性が存在し攻撃を受けたのであれば、この期間におけるシステムベンダーによる改修の有無などの調査をする必要がある。

調査において前述のとおりデータベースのログやサーバへのアクセスができず、システムベンダーから提供を受けたログやデータベース内容のリストのみを確認したとのことであるが、この報告書の内容では、攻撃のログが大量にあったことから攻撃を受けていたと述べているに過ぎず、どのような攻撃であったのか判断できる具体的な根拠も示されていない。この時点において、きちんとした調査が成されていれば、再度調査を実施する必要もなく、

時間や経費を浪費する必要もなかったと考えられるため、今後、調査を依頼する際の方法等を含めて検証が必要である。

さらに、ログの保管や事案判明時のデータ保全についても問題があったと考えられる。まず、ログが適切な箇所、期間にて保管されていなかったため、十分な調査ができていない。また、事案の調査の際にサーバの保全等が行われておらず、現在2回目の調査が行われているが、適切にサーバの保全等がされていなかったことで調査に影響が出る可能性がある。

⑥事案判明後の対応

(今回の経緯)

今後のクレジットカード決済については、システムベンダーに委託しているシステムを経由せず、直接決済代行会社のWebサイトにて決済を行う仕組みに仕様を変更することで旅行業システムでは、クレジットカード情報の入力はしないようにすることとしている。

本事案の根本原因の調査などを確認することと組織面でのセキュリティ体制の構築を行うべく対応をしているところである。

(考察)

上記本事案での対応及び検討点に記載の要因により、根本原因が判明していないことが問題であるが、2回目の調査が行われているということで、調査結果を待ちたい。

⑦本事案の原因

本事案の根本原因については、現段階において調査中であるため、本年6月24日の報告書及びヒアリングの内容を基に記述するが、これまでの情報からすると外部へWebサーバを公開しているにも関わらず、情報セキュリティ対策を怠っていたことが原因と考えられる。

i) システム導入時の契約の問題

システムを委託するにあたり、情報セキュリティ対策についての契約が不十分であった。

契約が10年前に交わされたものであったため、その後の情報セキュリティの高まりなどから契約内容の見直しなども実施すべきであったと言える。

ii) 運用時における情報セキュリティ対策の不足

Web アプリケーションを開発し外部に公開しているが、脆弱性の診断を行っておらず、適切なログの保管も実施していなかったため、サイバー攻撃に対して無防備に近い状態であった。普段の適切な情報セキュリティ対策が重要になると言える。

iii) 情報セキュリティの事案に対する知識不足

Web サイトを公開することにより、どのようなセキュリティリスクが存在するか理解しておくことで、対処方針について検討が可能となる。しかし、セキュリティリスクに係る知識不足は簡単に補えるものではないため、業界全体での共有などが重要になると言える。

iv) 事案発生時のマネジメント体制不足

個人情報流出などの情報セキュリティ・インシデントは、経営に影響を与える重大な問題と捉え、各事業者において、状況を見極めて早期に対応できる体制を整えることが望まれる。

3. 観光庁の対応について

今般の一連の旅行業者における個人情報流出事案において、旅行業者による関係官署への報告・相談の遅れが指摘されているところであるが、観光庁内においても旅行業者からの報告に基づく対応に遅れがあったことは否めない。

以下に JTB 及び札幌通運の事案について、観光庁の対応について時系列にて整理する。

○JTB の事案(「←」以降が観光庁の対応。)

5月13日 JTBとして、個人情報流出の可能性のある本事案の発生を認識。

5月30日 品川警察署に対して本事案を相談。

5月31日 観光庁に本事案を報告。

←担当班内で共有するも、外部流出したデータの具体的状況が不明だったため、次の報告を待つて庁内展開を図ることとした。

6月10日 流出可能性のある個人情報の概数の確認完了。

6月13日 観光庁に詳細報告。

←この段階で、観光庁内幹部、国土交通省へ情報展開。翌日には内閣サイバーセ

キュリティセンター(NISC)へ情報展開。

6月14日 記者会見の実施。

6月15日 ←個人情報保護法に基づく報告の指示を発出。

○札幌通運の事案(「←」以降が観光庁の対応。)

3月2日 カード会社より、Web上でカード決済を行った顧客のカード不正利用の可能性の連絡。

3月17日 法律事務所に対応を相談。

5月31日 クレジットカード会社、法律事務所に報告書提出。

6月6日 札幌中央警察署、北海道運輸局(観光庁)に事案報告。

←北海道運輸局より観光庁に対し、メールにて事案の報告あり。担当班内での情報共有に止まる。

6月15日 ←札幌通運が記者会見を実施する旨の報告を受け、観光庁内幹部、国土交通省へ情報展開。

6月16日 記者会見の実施。

←個人情報保護法に基づく報告の指示を発出。

(考察)

このように両事案において、旅行者からの個人情報流出の一報を受けた際に、事案の重大性を認識できず、幹部への報告等観光庁として即応していなかったということが問題点として掲げられる。

とりわけ、JTB 事案については、外部流出の可能性があるデータの組み直しを行い、それが出揃ってから庁内展開を図ることと担当者がしたところであるが、それを待たずに情報の外部流出の可能性があるとの報告を受けた際に即時の対応を行うべきであった。

この対応の遅れは、情報セキュリティ・インシデントが発生した場合の対応方針及び体制が、航空、鉄道等の重要インフラについては、内閣サイバーセキュリティセンターにより制定されているものの、旅行業界においては制定されておらず、その対応方針及び体制が定まっていなかったことも一因である。

観光庁として、情報セキュリティ・インシデント発生時の対応についてすみやかに定めるとともに、体制の整備・強化を継続して行う必要がある。

観光庁としては、「旅行・宿泊業者において情報セキュリティ・インシデントが発生した場合の対応について」を6月29日に制定し、情報セキュリティ事案についても、災害等非常時と同等の対応方針を整備し、観光庁、国土交通省、各地方運輸局に周知を行った。

また、情報セキュリティ・インシデントに係る業界への情報共有が図られていないとの反省のもと、6月14日付けで、観光関連団体に対し、「情報流出防止の徹底について」と題した文書を発出し、必要な措置の徹底を要請するとともに、6月28日に「観光庁・旅行業界情報共有会議」を開催し、旅行業界における個人情報流出事案に関する情報の共有を図った。

4. 再発防止策に向けての提言

(1) 旅行業者が早急にとるべき対応

- ・ 本検討会としては、JTBが前述2(1)で記した体制の整備・強化、システムのセキュリティ強化、システム運用管理の強化等今回の事案の発生を受けて当面とるべきシステム上の対策及び体制整備を行っていることを確認した。
- ・ 札幌通運については、現時点において情報セキュリティ会社に改善に向けたコンサルティングを受けている段階であり、その結果は8月末とのことであるが、できる限り早期にその結果を受け、セキュリティ対策の強化を図るべきである。
- ・ 大規模旅行業者はJTBが事案発生後に行ったのと同様の体制整備、システムのセキュリティ強化等が求められる。また、JTBを含めた大規模旅行業者は情報セキュリティに対して一過性の対応を行うのではなく、継続的に資源を確保し、対策を強化することが必要である。
- ・ 旅行業者の事業者団体は、旅行業における情報セキュリティ対策の重要性にかんがみ、その事務局内に情報セキュリティに係る担当者を任命し、旅行業者間の情報共有を図ることが必要である。
- ・ 個々の旅行業者は、今般の事案を踏まえ以下の視点に基づき対策を講ずる必要がある。内閣サイバーセキュリティセンター(NISC)からは「重要インフラの情報セキュリティ対策に係る第3次行動計画」(平成27年5月改訂)が、経済産業省・独立行政法人情報処理推進機構からは「サイバーセキュリティ経営ガイドライン Ver1.0」が出されており、対策の検討を行う際の参考と

すべきである。

①マネジメントに関すること

- ・ CISO の任命、本社役員を含む情報セキュリティ対策部署 (CSIRT) の設置等情報セキュリティの対応体制を構築し、また、可能であれば外部専門家の評価を受けること。事案発生時には CISO、CSIRT (必要に応じ、外部専門家も含めて) で早急に対応できる体制とすること。
- ・ グループ企業がある場合には、グループ企業全体を統括するネットワーク構成管理を行うこと。
- ・ PDCA サイクル(リスク評価、課題抽出、対策実施等)を適切に実施すること。
- ・ 情報セキュリティ事案発生時の対処手順及び報告手順を整備すること(IT部門から経営層への速やかな報告、情報漏洩の可能性が認められた時点で監督官庁へ報告、二次被害を防ぐ観点からの速やかな对外公表等をルールとして明確化すること)。
- ・ ISO27000、プライバシーマーク等の取得等既存の認証制度を活用することが望ましい。

②人材育成・社員教育に関すること

- ・ 情報セキュリティに係る人材を育成すること。自社だけでの養成が困難な場合には外部専門家の協力を受けつつ人材育成をすること。各旅行業者だけでなく業界全体で人材育成をすることが望ましい。
- ・ 研修、訓練の実施等経営層を含めた全従業員の個人情報保護意識の向上を図ること。研修、訓練は標的型攻撃の脅威を理解できるものとする等実践的な方法で行うことが望ましい。

③システムに関すること

<設計段階>

- ・ グループ全体のシステムを見渡して、どこに重要な情報があるかを確認する等情報の見える化を行うこと。
- ・ 情報の見える化の結果を踏まえつつ、適切なシステム構成とすること(個人情報にアクセスするシステムが、インターネットを使用する環境と物理的に分離されている等)。
- ・ 個人情報を保有するデータベースサーバへのアクセス権を必要最小限とする等アクセス権を厳格化すること。

- ・ 各種ログを収集・保管すること(事案発生時に集約・分析可能な環境とするこ
と)
- ・ パソコン・サーバのパッチ適用状況を把握すること。
- ・ 通信経路上及びパソコン・サーバ上の防御をすること。
- ・ Web アプリケーションでは、セキュアコーディング等の脆弱性を作り込まない
対策を行うこと。
- ・ 適切に業務を遂行できるとともに、セキュリティが確保されるような仕組みに
配慮すること。(個人情報を保存すべきでない場所にコピーすることなく業務
を進められるような仕組みとするなど。)

<運用管理>

- ・ 設計段階で講じた措置を適切に運用すること。
- ・ 外部から内部に向けた通信及び内部から外部に向けた通信の適切な監視を
行うこと。
- ・ 事案発生の可能性が認められた際に局所的な対応にとどめず、グループ全
体で対応すること。
- ・ システム全体に対するセキュリティ診断等適切な外部監査を「定期的」に実施
すること。
- ・ 特にインターネット公開システムでは脆弱性診断を行うこと。

(2) 中堅・小規模旅行業者がとるべき対策

- ・ 平成 27 年 9 月に個人情報保護法が改正され、平成 27 年 9 月 9 日(公布日)
から 2 年以内の政令で定める日以降は、これまで同法の適用除外とされて
いた取り扱う個人情報が 5,000 人分以下の事業者に対しても適用されること
を踏まえ、中堅・小規模事業者は、まずはウイルス対策ソフト、OS 及びソフト
ウェアを常に最新のものに更新する等セキュリティ上の脆弱性対策に関する
基本的な対策を行うとともに、社外の情報セキュリティ事案に係る最新情報に
留意し、社内のシステムや体制を見直す等情報セキュリティへの意識を高め
ることが必要である。
- ・ 中堅・小規模旅行業者は、大規模旅行業者のようなセキュリティ対策への投
資は困難であるが、将来的には大規模旅行業者と同様の対策を構ることが
望ましい。個々の事業者で対策を構ることが困難であれば事業者団体と
して会員企業を対象として通常の情報セキュリティ対策や事案発生時に助言

を行う相談窓口の設置、緊急支援 CSIRT を設置する等業界団体として検討を始めるべきである。

- ・ 旅行業者の事業者団体は、旅行業における情報セキュリティ対策の重要性にかんがみ、その事務局内に情報セキュリティに係る担当者を任命し、旅行業者間の情報共有を図ることが必要である。
- ・ 前述(1)①～③に掲げた対策を実施可能な信頼できるクラウドサービスを利用し、システムの管理運営を外注することが考えられる。クラウドサービス提供事業者の選定やサービス利用後の通信監視やインシデント発生時の対応等契約時の注意点等について事業者団体として検討することが望ましい。
- ・ 保険会社により、サイバー保険が提供されているが、同保険には専門家の派遣等緊急時サポートサービスが付帯しており、このような保険に加入することで実務的な支援を受けることが考えられる。保険料負担の軽減のため、複数旅行業者での共同の加入や業界団体として加入し、会員企業が支援を受けられるよう保険会社と交渉することも考えられる。

(3) 観光庁が早急にとるべき対応

- ・ 今般の一連の事案に関し、観光庁において旅行業者からの報告に基づく対応に遅れがあったことを踏まえ、6月29日に制定した「旅行・宿泊業者において情報セキュリティ・インシデントが発生した場合の対応について」に基づき、情報セキュリティ事案について災害等非常時と同等の対応を行うとともに、旅行業者に業界内の情報セキュリティ事案の情報共有を行うことはもとより、情報セキュリティ事案に係る政府の取組みや旅行業以外で発生した情報セキュリティ事案の共有を図ること。
- ・ 観光庁は、速やかに旅行業者との情報共有会議を開催し、旅行業者に対し今回の中間とりまとめにおいて示した再発防止に向けての提言を周知徹底すること。
- ・ 情報共有会議は当初は観光庁主体となって開催するが、情報セキュリティに対し、旅行業者が意識を持って自主的に対策に取り組む必要がある。速やかに旅行業者の自主的な情報セキュリティに係る情報交換の場として発展させるよう支援すること。

(4) 今後検討すべき事項

- ・ 航空、鉄道等の重要インフラについては、すでにサイバーセキュリティガイドラインが策定されているが、旅行業にはまだ整備されていない。旅行業界のシステムに対応したガイドラインの策定が必要である。また、中堅・小規模旅行業者にIT専門家がないことを踏まえ、わかり易い簡易版のガイドラインも合わせて策定する必要がある。またガイドラインの策定については観光庁が支援を行うことが望まれる。
- ・ 観光業界で発生した情報セキュリティ・インシデントの情報を各社情報セキュリティ担当者間で共有する必要がある。そのためメーリングリストの整備、会員クローズドのポータルサイトを業界団体で設置すべきである。その立ち上げについては観光庁としても協力することが望まれる。
- ・ 旅行業各社の情報セキュリティ担当者の情報共有を深め、情報セキュリティに係る勉強会を定期的に行う等、情報セキュリティの向上のため業界全体として取り組む体制を目指すべきである。業界としての取り組みとしては金融 ISAC や J-CSIP を参考にすることができる。また、業界団体としても各社のセキュリティ対策を評価する仕組みを構築し、一定の基準を満たしている場合には認証を付与する等の仕組みを検討することが望ましい。
- ・ 観光庁は旅行業者における情報セキュリティ対策の重要性にかんがみ、情報セキュリティ事案を担当し、業界団体及び旅行業各社の情報セキュリティ担当者と密接な情報共有が図られるよう体制の整備を行うべきである。

5. おわりに

今般の事案は、旅行会社が連続してサイバー攻撃を受け、かつその当事者が最大手の旅行会社であったことから旅行業界における情報セキュリティ対策に注目を集めることとなった。

当委員会としては、今般の事案に関し JTB が当面とるべきシステム上の対策及び体制整備を行っていることを確認したが、セキュリティ対策に終わりはない。日々セキュリティ上の脆弱性を補正し、ウイルス対策のパターンを更新し、診断・監査をし、情報セキュリティの向上に努め、旅行業界の範たることが期待される。

今般の両社の事案は、JTB 及び札幌通運において発生した事案であるが、個人情報保有する企業全てに共有する問題である。鉄道、航空、物流の重要インフラや今般再発防止策を検討した旅行業だけでなく、国土交通省が所管する分野全体で、情報セキュリティ対策の強化に努めるべきである。

今般の事案を機に各旅行業者が、情報セキュリティ向上に向けて体制整備、システム改善を行い、社員一人一人が情報セキュリティに対する意識を高め、旅行業界全体が情報セキュリティに強い業界と社会から認められるようになるよう、観光庁及び旅行業界に対し、引き続き取り組むことを強く望むものである。

用語集

C&C サーバ

「コマンド&コントロールサーバ」の略称。マルウェアに感染したコンピュータに指令(コマンド)を送り、制御(コントロール)する際を中心となるサーバのこと。

CISO

「Chief Information Security Officer」の略称。企業内で情報セキュリティを統括する担当役員のこと。機密情報や個人情報の管理やコンピュータシステム及びネットワークのセキュリティ対策等について統括する。

CSIRT

「Computer Security Incident Response Team」の略称、(シーサート)。組織において発生した情報セキュリティ・インシデントに対処するため、当該組織に設置された体制のこと。

CSV ファイル

「Comma Separated Values」の略称。データのフィールドの区切りをカンマ(,)のみで表現する形式のファイルのこと。

RAT

「Remote Access Tool」の略称。管理者権限を利用してコンピュータを遠隔操作できるようにするツールの通称である。ほとんどの場合、リモートアクセス型トロイの木馬を指す。

SQL インジェクション

データベースと連携した Web アプリケーションに問い合わせ命令文の組立て方法の問題があるとき、Web アプリケーションへあてた要求に、悪意を持って細工された SQL 文を埋め込まれてしまうと、データベースを不正に操作されてしまう問題。

オンプレミスシステム

自社で保有し、自社の設備において運用する情報システムのこと。

クラウドサービス

狭義には、クラウドコンピューティングによって提供される IT サービスのことである。広義には、外部業者が利用者にインターネットを通じて IT 機能を提供するサービス全般 (ASP サービスと同義) を指すことがある。本報告書でも広義の意味で用いる。

情報セキュリティ・インシデント

情報セキュリティに対して脅威となる事件や事故のこと。特に本報告書においては、主にサイバー攻撃により発生するものに焦点をおく。

脆弱性診断

ネットワーク、Web サーバ、Web アプリケーションに対して、攻撃者の視点で侵入、不正操作等を試みることにより、システムに脆弱性が存在しないか検査し、システムのセキュリティ度合いを診断すること。

セキュアコーディング

プログラムが意図したとおりに動作するよう、脆弱性を含まないソースコード (プログラミング言語によって記述された、プログラムの元になるテキストデータ) を作成すること。

(ネットワーク)セグメント

ネットワークをグループ毎に分離することを意味する。一般的には、機能または組織などの単位で分離し、ルータ (L3 スイッチ)、ファイアウォール等により通信を制御する。

フォレンジック調査

コンピュータ・フォレンジック (デジタル・フォレンジック) を意味する。コンピュータやネットワークシステムに記録された電子データを収集、分析し犯罪などの証拠を見つけ出し事実を解明すること。

マルウェア

ネットワークやコンピュータに何らかの被害をもたらすように設計されたソフトウェアのこと。例えばネットワークを通じてコンピュータに侵入し、情報の外部への流出やデータ破壊などを行うような、害悪をもたらすソフトウェアのこと。