

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すべき対策～

概要

1. 事案の検証

(1) 株式会社ジェイティービー(以下「JTB」)の事案

- ・ JTBの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。
- ・ 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。
- ・ 被害の拡大を防げなかった原因としては、標的型攻撃に対しての情報不足、自社システム構成の理解不足、事案発生時のマネジメント体制不足、担当役員及び監督官庁への報告の遅れ等を指摘。

(2) 札幌通運株式会社の事案

- ・ 本事案の原因是、現段階において調査中であるが、これまでの情報からすると外部へ Web サーバー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。
- ・ 具体的には、システム委託契約時にセキュリティ対策について事項が不十分であったこと、情報セキュリティの事案に対する知識不足、事案発生時のマネジメント体制不足等を指摘。

2. 観光庁の対応について

- ・ 観光庁では、旅行業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できていなかった。
- ・ 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旅行業界に関しては制定されていなかったことも一因。
- ・ 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、すでに当該規定に基づいた対応を開始。

3. 再発防止策の提言

(1) 旅行業者が早急にとるべき対応

- ・ 情報セキュリティ最高責任者(CISO)の任命、サイバーセキュリティ対策部署(CSIRT)の設置、個人情報サーバーとインターネットを使用するシステムを物理的に分離する等、体制とシステムの面で今回の事案を踏まえた措置を講じること。
- ・ 事業者団体の事務局内に情報セキュリティ担当者を任命、業者間の情報交換を図ること。

(2) 中堅・小規模旅行業者がとるべき対応

- ・ 中小旅行業者も大手旅行業者と同様の対応が望ましいが、まずはアンチウイルスソフトの更新等基本的な対策を講じること。
- ・ 個々の企業での対応が困難であれば事業者団体に相談窓口やCSIRTを設置する等、業界団体として対応すべく検討を始めること。
- ・ クラウドサービスの活用やサイバー保険に付帯する緊急時サポートサービスの活用も考えられること。

(3) 観光庁が早急にとるべき対応

- ・ 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こと。
- ・ 情報共有会議を開催し、今回の提言を事業者に周知すること。

(4) 今後検討すべき事項

- ・ 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こと(例:金融ISAC)。
- ・ 航空等重要インフラではすでに整備されている旅行業のシステムに対応したサイバーセキュリティガイドラインを策定すること。
- ・ 業界団体として旅行業界で発生した情報セキュリティ事案を共有するため、会員向けのHPや会員に情報発信を行うためのメーリングリストを整備すること。