日本航空株式会社　代表取締役社長　植木義晴　殿

# 検証報告書（要約）

2015 年 1 月 14 日

顧客情報漏えい問題に関する独立役員検証委員会

# 第1章　顧客情報漏えい問題に関する独立役員検証委員会設置の経緯および目的

## 第1節　設置の経緯

2014 年 9 月 19 日および同月 22 日、日本航空株式会社（以下、「当社」という。）の顧客情報管理システム（以下、「VIPS」という。）にスローレスポンスが発生したことから、社内で緊急調査を行った。その結果、VIPS にアクセス可能な社内の業務端末（以下、「VIPS 端末」という。）に外部から侵入したマルウェア[1]が VIPS と交信を行い、JAL マイレージバンク（以下、「JMB」という。）会員である顧客の個人情報の一部を抜き出して、香港所在の外部サーバ（以下、「香港サーバ」という。）に送信していた事実（以下、「本事案」という。）が判明した。

当社は、本事案が発覚した 9 月 22 日から 2 日後の同月 24 日に警視庁に相談を開始するとともに、国土交通省に届け出を行い、IT 企画本部およびマイレージ事業部を中心に社内調査体制を立ち上げた。また、IT セキュリティに関する高度な技術を有する社外専門機関等の支援を得て、原因究明、被害範囲の確定および再発防止策の策定等に関する調査（以下、「一次調査」という。）に着手した。併せて、9 月 29 日の定例記者会見において、その時点で把握できている事実関係を公表して顧客にお詫びをし、その後の調査の進捗に応じて必要な情報開示を適時行っていく方針を明らかにした。

また、一次調査の過程で、9 月 19 日以前においても悪意ある第三者が社内の複数の業務端末になんらかの形で侵入し、それらに保存されている個人用ファイルを盗み見た可能性も判明したため、当該業務端末に存在した個人ファイルの検証を進め、通信記録を分析する等して、社外流出の有無や被害範囲を特定する作業（以下、「二次調査」という。）を実施した。

一次・二次にわたる社内調査は、本事案の発覚直後から 11 月中旬にかけて実施され、最終的に、IT 企画本部が 11 月 21 日開催の役員会に報告書を提出した。

一方、当社は、これら社内調査の内容、範囲およびその方法等が適正なものであったかどうか、今後講じられる再発防止策が妥当であるかどうか等について客観的な視点で検証を行う目的から、10 月 29 日に開催された取締役会において社外の独立役員を委員とする「顧客情報漏えい問題に関する独立役員検証委員会（以下、「検証委員会」という。）」の設置を決議し、10 月 31 日、社長から委嘱を受ける形で検証委員会を発足させた。

検証委員会を発足させたのは、本事案が当社の内部統制の信頼性に係る重要な問題であることから、社外の独立役員による委員会によって社内調査の検証を行うことが、社内調査の透明性を確保するとともに、検証行為の公正性と独立性を担保する上で有効であるとの判断によるものであった。併せて、検証委員会の管下に検証作業部会を置き、その検証実務を社外の IT コンサルタントに委任することにより、検証行為の専門性を確保した。

## 第2節　設置の目的

検証委員会は、下記の諸点を目的として設置され、検証結果を社長に答申することとされた。

① 一次調査の内容、範囲、方法等が適切であったかどうかを検証する。

② 二次調査の内容、範囲、方法等が適切であったかどうかを検証する。

③ VIPS からの個人情報漏えい問題に対する改善策を検証し、必要に応じて新たな改善策を提

[1] コンピュータウィルス等の悪意を持った動作をするプログラムの総称。

言する。

④ 上記①および②の検証過程で判明した、当社の顧客情報管理上の問題点一般に関する指摘および改善提言を行う。

## 第2章　検証委員会の構成

検証委員会は当社の独立役員 5 名により構成された。また、補助者として、管下に事務局・検証作業部会を設置した。

### 第1節　検証委員会構成

| | |
|---|---|
| 委員長（委員の互選により決定） | 岩田喜美枝　日本航空株式会社　社外取締役 |
| 委　員 | 甲斐中辰夫　日本航空株式会社　社外取締役 |
| 委　員 | 片山英二　日本航空株式会社　社外監査役 |
| 委　員 | 熊坂博幸　日本航空株式会社　社外監査役 |
| 委　員 | 八田進二　日本航空株式会社　社外監査役 |

### 第2節　事務局

日本航空株式会社　総務本部　総務部

### 第3節　検証作業部会

デロイト トーマツ ファイナンシャル アドバイザリー株式会社（以下、「DTFA」という。）

## 第3章　検証方法等

### 第１節 検証のスコープ

検証委員会は、以下のスコープを定め各項目の妥当性を検証した。

① 本事案への対処および社内調査の検証
- 初動対応の妥当性
- 調査方針の妥当性
- 調査体制の妥当性

② 社外専門機関等による調査の検証
- JPCERT コーディネーションセンター（以下、「JPCERT」という。）の調査の妥当性
- NRI セキュアテクノロジーズ（以下、「NRI」という。）の調査の妥当性
- S&J コンサルティング（以下、「S&J」という。）の調査の妥当性
- マカフィーの調査の妥当性

③ 一次調査の検証
- マルウェア感染経路調査の妥当性
- 漏えい調査の妥当性
- 原因究明の妥当性

④ 二次調査の検証

・漏えい問題とは直接は関連しない業務端末に対する影響範囲特定調査方針の妥当性
・影響範囲特定調査の妥当性

⑤ 本事案発生以前のセキュリティ対策についての検証

⑥ 緊急対応および今後の課題整理についての検証

・緊急対応の妥当性
・今後の課題整理の妥当性
・再発防止策・改善策の提言

⑦ 情報漏えいが確認された顧客への対応策についての提言

第２節 検証方法・期間

下記のとおり計 8 回の検証委員会を開催し、検証実務に携わる検証作業部会および事務局からの報告を受け、委員間で協議を行うとともに、委員相互間のメーリングリストを設定して適時必要な情報共有・意見交換を実施し、本報告書をまとめるに至った。

| | 開催日 | 主な協議事項 |
|---|---|---|
| 第 1 回検証委員会 | 2014 年 10 月 31 日 | ・検証の方向性確認<br>・社内調査に関する報告聴取・検証 |
| 第 2 回検証委員会 | 2014 年 11 月 12 日 | ・社内調査に関する報告聴取・検証 |
| 第 3 回検証委員会 | 2014 年 11 月 19 日 | ・社内調査に関する報告聴取・検証 |
| 第 4 回検証委員会 | 2014 年 11 月 26 日 | ・社内調査に関する報告聴取・検証 |
| 第 5 回検証委員会 | 2014 年 12 月 10 日 | ・社内調査に関する報告聴取・検証<br>・課題整理 |
| 第 6 回検証委員会 | 2014 年 12 月 17 日 | ・再発防止策の検討<br>・検証報告書の構成方針確認 |
| 第 7 回検証委員会 | 2014 年 12 月 24 日 | ・検証報告書の検討 |
| 第 8 回検証委員会 | 2015 年 1 月 7 日 | ・検証報告書の確定 |
| 答 申 | 2015 年 1 月 14 日 | |

第３節 検証作業部会の検証実務

検証委員会の検証作業部会として、DTFA を選定し、同社に検証実務の取りまとめを委任した。DTFA は、IT 関連のデータ集計・分析、IT セキュリティ対策、リスクマネジメント全般に関する十分な知識と経験を有していることが選定理由である。

検証作業部会は、検証委員会の意向を受けて、以下の作業を実施した。

① 社内調査を担当した IT 企画本部、マイレージ事業部等に対するヒアリングを実施した。

② 社内調査を支援した社外専門機関等 4 社および初動対応を支援した JAL インフォテック（以下、「JIT」という。）に対するヒアリングを各社毎に複数回行い、必要なデータの提出を受けて検証を実施した。

③ これらの検証結果を集計、取りまとめの上、検証委員会に報告した。

## 第4章　社内調査に関する検証結果

### 第１節 社内調査結果の概要

本項では、検証委員会の検証対象である、IT 運営企画部が作成した社内調査結果報告書の概要を述べる。

① 発生経緯・原因

・9 月 19 日、同 22 日の両日、VIPS にスローレスポンスが発生し、IT 運営企画部による原因調査の過程で、VIPS 端末に侵入したマルウェアによる不正アクセスが原因であることが判明した。

・また、それらの端末のうち一部がインターネットを介して香港サーバと通信した形跡が認められ、かつ、通常の業務では発生しない手法で VIPS から顧客情報をダウンロードし該当端末内に保管されていたことから、IT 運営企画部は該当顧客情報が漏えいした可能性が高いと判断した。

・さらに、本事案とは別に、マルウェアに感染した業務端末に保存されていた個人情報が、悪意のある第三者に閲覧されていた可能性もあるとも判断した。

② 情報漏えいの被害概要

【一次調査結果】

調査の結果、VIPS からデータを抜き出し、香港サーバに対して送信された個人情報は 4,131 件と判定された。なお、検証委員会はクレジットカード情報の流出は確認されなかったとの報告を得た。

【二次調査結果】

調査対象となった業務端末に保存されていた個人情報が外部に流出した証跡は認められなかった。

③ 緊急対応

IT 運営企画部は、社外専門機関等の支援を得て、緊急対応として下記施策を実施した。

・危険サイトの接続制限によるマルウェア感染拡大防止

・社内の全業務端末から外部にアクセスする際の認証要求の追加

・新たなマルウェア検知機能による漏えいの防止　等

④ 再発防止策・課題

IT 運営企画部は、緊急対応に加え、今後、下記の施策を講じてセキュリティ強化に努める必要があると判断している。

・当社ホームページのセキュリティ認証の強化

・社内の全業務端末からのマルウェア駆除

・メールに添付されたマルウェアを検知する仕組みの導入

・当社および関連会社社員への IT セキュリティ教育の強化、等

### 第２節 検証結果の概要

本項では、社内調査結果に関して検証委員会が行った検証の結果の概要について述べる。

① 本事案への基本的対処の検証

本事案については、以下の 2 種類の異なる情報漏えい経路を想定して調査が実施された。

・一次調査 ： VIPS 端末から不正なプログラムにより顧客データを抽出し外部へ送信した可能性

・二次調査 ： マルウェアに感染した業務端末上のファイルを閲覧もしくは外部へ送信した可能性

一次調査については、過去の通信記録から通常業務では発生し得ない通信を行っていた業務端末を特定し、通信記録に記録された通信容量および通信日時から送信可能であったデータ容量を算出して調査が行われている。この手法は、当社内の情報がネットワークを通じて外部に送信される経路を論理的に網羅している点、通信した情報の証跡を全て確認している点からも合理的な調査であったと判断する。

二次調査については、調査対象を以下の基準に従って特定し、調査が実施された。

・香港サーバと通信したことが確認された業務端末

・当社社内ネットワークの管理者権限で不正にアクセスされたことが確認された業務端末

・既知のマルウェアないし不正なタイマー設定等の痕跡が確認された業務端末

本事案の調査を進めるにあたり、専門性が高く高度な知識やオペレーションが必要と判断された工程については、社外専門機関等に業務を委託している。こうした社外専門機関等への、調査依頼は、当時の緊急を要する状況下においてやむを得ないものであり、これを受けて行われた各社の調査は、当社の依頼内容を順守して実施され、本事案を収束に導く重要な情報が提供されていることから、調査方法および結果はいずれも妥当であると判断する。

② 社内調査の妥当性

【一次調査】

マルウェアにより香港サーバに通信を行った可能性のある業務端末 20 台に対して、詳細な調査が行われた。その結果、顧客情報を外部に送信した対象は 3 台に限定された。また、今回感染していたマルウェアは、圧縮ソフト「RAR」を用いてファイルを「.rar」形式に圧縮し、外部に送信するものであることが確認されている。そのため、限定された 3 台の対象に対しては「.rar」形式で圧縮されたファイルのサイズと通信記録に残る送信ファイルサイズが一致した場合、その情報は漏えいが確定したと判断するものとし、調査が実施された。

その結果、マルウェアが作成したと考えられる「.rar」ファイルのファイルサイズと一致する通信記録の履歴が確認された。該当ファイルに保存されている顧客情報は 4,131 件であったことから、香港サーバに送信された件数を 4,131 件と判定している。

上記調査結果は、ファイルサイズと通信記録の内容が一致していること、「.rar」ファイル作成直後に情報の送信が行われていることから、妥当な判断である。

【二次調査】

マルウェアに感染した可能性のある業務端末の内、個人情報を扱う可能性のある業務端末については拡張子[2] で対象ファイルを絞り込んだ後、全て目視にてファイル内容の精査

[2] ファイルの種類を識別するために ファイル名の末尾につけられた文字列。

が実施された。顧客情報を扱う可能性がない業務端末については拡張子で対象ファイルを絞り込んだ後、チェックツールで顧客情報の有無が確認され、画像データおよび顧客情報が１件でも検出されたファイルはさらに精査が行われた。これら全業務端末の通信記録を調査した結果、保存されていた情報が外部に流出した形跡は、認められなかったとしている。

上記調査は、一次調査同様にファイル特定および通信記録を用いた調査が行われており、妥当な結果が得られていると判断する。

## 第5章　本事案発覚以前のセキュリティ対策についての検証

本事案発覚以前より、当社は以下のようなセキュリティ対策を講じていた。

- J-SOX 対応のシステム監査
- 情報セキュリティ規程および JMB 個人情報マニュアル等の各種規程類の整備
- 上記規程類に沿った定期的な業務監査
- インターネット接続部分における Proxy サーバの導入
- 業務端末へのマルウェア対策ソフトの導入
- 当社および当社関連会社社員への情報セキュリティ教育
- 複数のセキュリティ専門業者とのアドバイザリー契約

これらは、システムおよびネットワークに関する対策として大きな過失や欠落は認められず、企業として基本的に必要な対策は事前に講じられていたと判断する。

ただし、当社ネットワーク外からの侵入を防ぐことに主眼が置かれ、悪意のある第三者が当社ネットワークに侵入した以降の対策については不十分であったことに関しては改善の余地があり、今後の防止策としての取り組みの中で解消されるべきものと考える。

なお、この点については、一部緊急対応にて導入したシステムを継続利用することで既に改善されている要素もある。また、顧客情報の取り扱いに関する各種規程類が整備されてはいたものの、社員への周知徹底が十分ではなかった。

## 第6章　緊急対応および今後の課題整理についての検証

システム監査では対象とならないヒューマンリソースに関する課題、日常の業務および情報の運用に関する課題、また、「当社ネットワークおよびそれを構成するシステム」という大枠で捉えた際の周辺システムとネットワークに関する課題等、早期検討を必要とする点が見受けられた。

① 社員への啓発活動および情報管理制度の見直し

- 本事案を当社で実際に発生した事例として教材化し、当社および当社関連会社社員への IT セキュリティ研修のあり方を見直す。
- 業務効率を鑑みながら、個人の業務端末に顧客情報を極力保存しないことを目指し、顧客情報の管理ポリシーを見直す。
- 個人情報だけではなく、当社事業における重要情報に該当する項目の洗い出しと重要度の再定義を実施し、重要度に沿った情報の管理体制および運用の実現を目指す。

② サイバー系インシデントに対する事前の体制整理

・当社内でのセキュリティオペレーションセンター（SOC）機能の立ち上げと、セキュリティ関連情報のシステムによる一元管理・運営機能（SIEM）実装を目指す。
・サイバー系インシデント再発の可能性に鑑み、有事の際に一元的対応が可能な社外専門機関等に関する情報を事前に収集する。

③ 社内のネットワークとシステムの見直し
・接続環境の仮想化[3]や重要情報を収容する機器への接続制御等を行い、当社重要情報への当社ネットワーク内外からの不要なアクセスを制限する。
・アカウントの権限管理システムの再構築を行う。
・社内 IP ネットワークのさらなる細分化および重要情報の作業専用スペースを設ける等、ネットワークの物理構成[4]と論理構成[5]を再検討する。

④ 中立的な検証機能の導入
・システムやソフトウェアの導入に際し、スペック・規模・費用対効果等について導入目的に対する妥当性を中立的に判断できる機能の確立を検討する。

## 第7章　情報漏えいが確認された顧客への対応策について

本事案に関する広報対応、当社ホームページへの掲載等は迅速であり、謝罪および周知に関する対応は妥当であると判断する。

また現時点で実害は報告されていないが、今後顧客になんらかの実害が発生した場合には、誠意をもって対応すべきであるとの提言を行った。

## 第8章　まとめ

本事案における調査については、初期の調査対応、関係機関への連絡と広報対応、マルウェア感染被害の拡大防止、および調査結果を踏まえた本事案解決に向けた行動が迅速に行われており、調査方法と調査結果を踏まえた本事案への対応は、妥当であると判断する。

しかしながら、悪意のある第三者によるサイバー攻撃は手口が極めて巧妙になっており、システムやネットワークに対する機械的な対応だけでは完璧に阻止することはできない。そこで、システムやネットワーク等のハードと、ヒューマンリソースや業務・運用等のソフトを両輪としたバランスの取れたセキュリティ対策が重要であり、今後の取り組みでさらに向上されることを期待する。

以上

---

[3] コンピューターや記憶装置、ネットワークなどのコンピューター資源を、実際の物理的な構成とは異なるもののように見せかけて動作させる技術。

[4] 機器やケーブル類を物理的に接続して形成する構成。

[5] 物理的な構成とは別に、システムやネットワーク内でソフトウェアの機能や接続制限等によって分離された構成。