九州商船 WEB 予約サービス
不正アクセスに関する調査報告書
（調査委員会）

2018 年 3 月 28 日

内容

1. はじめに

1.1. 調査委員会設置の経緯

九州商船株式会社では、インターネットを通じた WEB 予約サービス（以下「WEB 予約サービス」という。）を提供している。

2018 年 1 月 5 日に、WEB 予約サービスに接続しにくいという事象が確認され、不正アクセスを受け、不正に設置されたプログラムが実行されていた事実が確認された（以下「本件不正アクセス」という。）。

本件不正アクセス発見後（2018 年 1 月 5 日 19 時 50 分）に、WEB 予約サービスを停止したが、この時点では、WEB 予約サービス上のお客様情報の漏えいがあったかどうかについての判断を即断することはできなかったため、お客様情報の漏えいのおそれがあるとして、本件不正アクセスに対応することとし、お客様へのメールおよびウェブページでの案内を行った（2018 年 1 月 9 日付「不正アクセスによるインターネット予約サービスの停止とお客様情報漏洩の恐れに関するお知らせ」）。

九州商船株式会社では、本件不正アクセスの事実関係の調査、お客様情報の流出の蓋然性の評価、本件不正アクセスの原因究明、再発防止策については、客観的かつ専門的で、より公正性、透明性を有した調査、検討および判断が必要であると判断し、社外の専門家により構成される調査委員会（以下「本調査委員会」という。）を 2018 年 1 月 24 日付で設置した（2018 年 1 月 24 日付「弊社 WEB 予約サービスに対する不正アクセスに関する中間報告」）。

なお、本調査委員会は、九州商船株式会社美根晴幸代表取締役の諮問機関としての調査委員会であり、平成 22 年 7 月 15 日付日本弁護士連合会策定の「企業等不祥事における第三者委員会ガイドライン（平成 22 年 12 月 17 日改訂）」に準拠した第三者委員会ではない。

WEB 予約サービスに対する不正アクセス調査委員会の構成は、以下のとおりである。

役　職	氏名	所属
委員長	大山　健	長崎総合科学大学工学部・大学院工学研究科（教授）
委　員	古賀　正訓	古賀正訓法律事務所　弁護士

1.2. 調査の目的

本報告書は、2018 年 3 月 20 日までの調査に基づき、次項記載の受任事項に関して、本報告書提出時における本調査委員会の見解を報告することを目的とするものである。

（1） 本件不正アクセスの事実関係の調査

（2） 本件不正アクセスの原因究明
（3） お客様情報漏えいの蓋然性の評価
（4） 再発防止策の提言

1.3. 調査期間

2018 年 1 月 24 日から、2018 年 3 月 20 日まで。

1.4. 調査方法

調査委員会は、本報告書を作成するにあたり、以下の方法に基づいて調査を実施し、上記調査期間内に開示された情報の範囲内で、その情報の真実性および正確性を前提として本報告書を作成した。

（1） 各種ログの調査（ディスクイメージ含む）
（2） インタビューによる調査
（3） 契約書などのドキュメントのレビュー

2. 本件不正アクセスの事実関係および原因

事実関係については「不正アクセスに関する調査報告書（解析編）」に詳説する。

本件不正アクセスは、外部からの自動化された攻撃によるものであり、直接的な原因はメンテナンス用 FTP アカウントの不備によるものである。

3. お客様情報漏えいの蓋然性

「不正アクセスに関する調査報告書（解析編）」で検討した通り、

- 本件不正アクセスが、九州商船株式会社を特定して行われてものではなく
- もっぱら機械的な探索と、暗号通貨の発掘を目的としたものであり
- データベースログ上にデータ持ち出しの痕跡が発見されなかった

ことから、本件不正アクセスによって、お客様情報が漏えいした可能性は極めて低いと考えられる。

4. 再発防止策の提言

4.1. 技術的な対策

「不正アクセスに関する調査報告書（解析編）」で指摘した通り、総合的な対応として、

（1） 不要なサービスの停止、ポート、アクセス元の制限
→FTP は使用しない、IP アドレスによる制限等の実施
（2） メンテナンスアカウントのセキュリティ強化

→証明書を使用した ssh 等の利用

（3） 継続的なシステムのアップデート
→アップデート時の動作検証を速やかに行う体制の整備

（4） 不正アクセスを意識した設計とコーディング
→多層防御を意識した設計（パスワードのハッシュ化含む）、外部パラメーターを信用しないコーディング

（5） 開発時のペネトレーションテスト
→コードレビューの一環としての自動化テスト

（6） ログの定期的な監視
→ログにノイズとなる情報が出力されない様なコード整備、ログ監査の自動化

を実施し、継続する体制を整備すべきである。

4.2. 情報セキュリティマネジメント上の対策

4.2.1. 業務委託について

（契約）

本件不正アクセスを受けた WEB 予約サービスは、構築・運用を外部の企業に委託していたものであるが、構築・運用に関する契約においては、不正アクセスへの対応事項が含まれておらず、果たすべき責任とその所在が明確になっていなかった。

（委託者）

少なくとも、お客様情報を預かり、外部に公開されるサービスの委託においては、「４．１技術的な対策」で指摘した様な事項が実施されることを契約において担保し、委託者において監査可能な体制を整備すべきである。

また、情報セキュリティ上の事故が発生した場合には、速やかに報告することを求めるとともに、委託者としての対応方針を決定できる体制を整備すべきである。

（受託者）

加えて、受託者においては、日々新しくなっていく、一定レベルの技術を組織として提供できるように、社内において、セキュリティ等の情報収集及び収集した情報を組織において共有できる体制を整備すべきである。

受託者は、定期的なレベルアップを行ったり、サーバー等の入れ替え等の作業を行う際にセキュリティの設定が適切に完了されたことなどの確認を行う体制を整備すべきである。

受託者においても、情報セキュリティ上の事故が発生した場合に、速やかにかつ適切に対応を行えるように、マニュアル等を作成し、危機管理を行える体制を整備すべきである。

4.2.2. 情報セキュリティマネジメント体制の整備について

本件不正アクセス発生の背景と、初期の対応においての混乱の背景には、基本方針やセキュリティポリシー、ルール類の不備といった、情報セキュリティマネジメント上の課題が指摘される。

WEB 予約サービスに限らず、お客様の情報を預かる企業として、また、事業の様々な局面においても、情報セキュリティマネジメント体制の確立が必要であることは論を待たない。

全社的な課題であり、中長期的な対策となるが、情報セキュリティに関する組織体制の整備、セキュリティポリシーの策定、ルール類の整備を行い、これらを実現する人材の育成および教育、継続的な改善を行う、情報セキュリティマネジメント体制を整備すべきである。

（以上）