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（第１報）

2018 年 1 月 20 日

九州商船株式会社　個人情報不正アクセス調査委員会

目次

1. はじめに

本報告書は、2018 年 1 月 5 日に発見された、九州商船 WEB 予約サービス(以下、当サービス)に対する不正アクセスに対する調査報告書です。

2. 発見の端緒

2018 年 1 月 5 日に、当サービスに接続しにくいとの指摘を受け、調査を行ったところ、外部からの不正アクセスを受け、外部から不正なプログラムを設置され、このプログラムが実行されていたことが判明しました。

3. 当サービスを構成するシステムの概要

当サービスを構成するシステムの概要を、図 1 に示します。

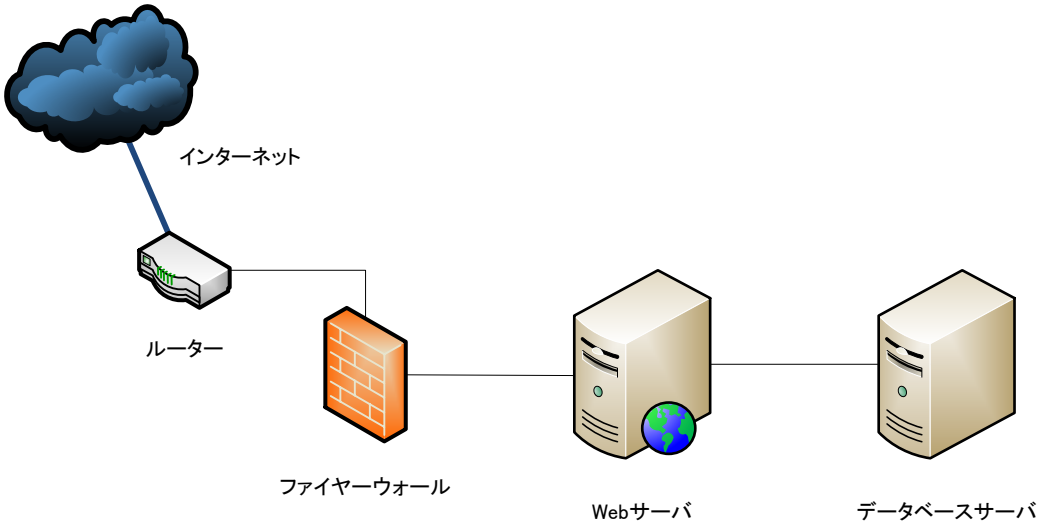

図 1　システムの概要構成図

今回、不正アクセスを受けた Web サーバの構成は以下の通りです。

OS:　　Red Hat Enterprise Linux Server release 7.2 (Maipo)
Apache: Apache/2.2.21 (Unix)
PHP:　　PHP 5.3.29 (cli) (built: Oct 24 2016 11:44:52)

Web サーバについては、2016 年 11 月 21 日にハードウェアのリプレースを目的とした移行を行っております。移行前のサーバの構成は以下の通りです。

OS:　　Red Hat Enterprise Linux Server release 5.7 (Tikanga)

Apache: Apache/2.2.21 (Unix)
PHP:　PHP 5.3.8 (cli) (built: Jan 17 2012 17:43:14)

4. 不正アクセスが行われた時期と想定される手法

不正アクセスを受けた Web サーバについて、保存されていた以下のログを調査しました。

サービス	ログファイル名	保存されていた期間
Apache	access_log	2017/01/08～2018/01/05
	error_log	2017/01/08～2018/01/05
vsftpd	vsftpd.log	2017/10/16～2018/01/05

※保存されていたログの連続性に関しては、引き続き調査、確認し、続報します。

vsftpd のログによれば、2017 年 10 月 20 日から、計 14 回の不正なログインを許し、ファイルアップロードが行われた痕跡が確認されました。

No	日時	アクセス元	ファイル
1	**2017/10/20 10:20:44～10:21:12**	A	/htdocs/config.php
2	**2017/10/25 14:50:14～14:50:44**	A	/htdocs/config.php
3	**2017/11/07 14:08:07～14:08:35**	A	/htdocs/config.php
4	**2017/11/23 21:32:50～21:33:04**	A	/htdocs/cron.php
5	**2017/11/26 15:52:40～15:53:54**	A	/htdocs/cron.php /htdocs/wp-cron.php /htdocs/cron-curl.sh /htdocs/drupal.sh
6	**2017/12/02 08:34:06～08:36:05**	A	/htdocs/cron.php /htdocs/wp-cron.php /htdocs/cron-curl.sh /htdocs/drupal.sh
7	**2017/12/02 19:05:29～19:06:33**	A	/htdocs/config.php
8	**2017/12/17 08:05:26～08:07:07**	A	/htdocs/cron.php /htdocs/wp-cron.php /htdocs/config.php
9	**2017/12/17 14:06:45～14:08:17**	A	/htdocs/wp-session.php
10	**2017/12/18 21:24:15～21:24:33**	B	/htdocs/wp-cron.php
11	**2017/12/20 19:42:03～19:43:42**	A	/htdocs/cron.php /htdocs/wp-cron.php

			/htdocs/wp-session.php
12	**2017/12/21 16:02:54～16:05:23**	A	/htdocs/wp-contacts.php /htdocs/wp-session.php
13	**2017/12/28 17:42:43～17:44:18**	A	/htdocs/cron.php /htdocs/wp-cron.php /htdocs/wp-trans.php
14	**2018/01/03 21:38:38～21:40:13**	A	/htdocs/cron.php /htdocs/wp-cron.php /htdocs/wp-trans.php

※アクセス元については、IP アドレスで分類し、記号を付しています。

なお、vsftpd への不正ログインによるダウンロードは、確認されませんでした。

一方、Apache のログから、不正にアップロードされたと思われるファイルへのアクセスを検索したところ、2017 年 7 月 15 日 08:58:21 以降、1,391 件のアクセスが確認されました（不正にアップロードされた可能性があるファイルとそのファイルに対するアクセスについては、引き続き調査を行います）。

一方、この様なファイルの探索については、2017 年 4 月以降、約 1,000 件のアクセス失敗が記録されています。これは、これらのファイルに対しての、インターネット全体のサーバに対する機械的な探索が行われているためだと考えられます。

これらの事から、

1) 不正なファイルを設置することを可能とする脆弱性を探査し
2) 不正なファイルを設置することができれば、このファイルにアクセスすることによって、Web サーバ実行ユーザの権限でこのファイルを実行する

といった、機械的な不正アクセスによって、今回の一連の攻撃が行われたものと推定されます。ログに記録が残されている期間においては、2017 年 7 月 15 日に不正なプログラムの設置が行われ、以降、不正なプログラムの実行が行われたものと判断されます。

5. 不正アクセスに使用された脆弱性

当該のメンテナンス用 FTP アカウントにおいては、ユーザ名とパスワードが、ドメイン名から比較的容易に推測できるものだったため、今回の不正アクセスにおいては、FTP アカウントに設定されたパスワードの不備が悪用されたものと考えられます。

このことから、今後の対策として、

1) FTP を使用しない（メンテナンスについては、他の手段によりアクセスを行う）
2) メンテナンスに使用するサービスについては、IP アドレスによる制限を行う
3) メンテナンスに使用するアカウントのパスワードは、ランダム生成するなど、十分に

推測しにくいものとし、メンテナンスに関わるメンバーの変更などの必要に応じて変更する。

を実施すべきだと考えます。

6. 個人情報の漏えいについて

当サービスにおいては、Web サーバには、お客様データを置かず、データベースサーバに保存するため、FTP サービスによるお客様データの持ち出しは生じない構成となっております。

しかしながら、今回の不正アクセスにおいては、Web サーバ実行ユーザ権限(nobody/nobody)で、攻撃者が任意のプログラムを実行することができる状況にあったため、

1) メンテナンス用アカウントでの不正アクセスによって、当システムの構成ファイルを取得し
2) 構成ファイルあるいは、攻撃者が設置したプログラムを通じた操作によって、データベースパスワードを入手し
3) 入手したデータベースパスワードによって、Web サーバからデータベースサーバにアクセスする

といった手法を用いることによって、お客様情報を持ち出した可能性を想定する必要があります。

データベースサーバについては、2017 年 12 月 3 日以降のログが残されているため、上記の様な手法による、データ取得の痕跡を探しましたが、データベースファイルサーバのログが存在する 2017 年 12 月 3 日以降には、その様な痕跡は発見されませんでした。

しかしながら、2017 年 12 月 3 日より前においても、不正なプログラムの実行が行われた痕跡があることから、現段階で、個人情報の持ち出しの可能を否定することはできません。

今後の調査では、バックアップやアーカイブからのログの抽出を行い、入手できたログから個人情報取得の可能性を判断し、取得された可能性の限定を進めます。さらに、データベースログと Web サーバのログの照合を行い、Web サーバを経由しないアクセスが確認されないかどうかの調査を行います。また SQL インジェクション等の他の攻撃によるデータ持ち出しの可能性について引き続き調査を行います。

7. 今後の調査

ここまでの調査で、今回の一連の不正アクセスには、FTP アカウントの不適切な設定が使用されたことが判明しましたが、他の手法による不正アクセスの可能性について引き続き調査を実施します。

また、ログに欠落した期間がないかについての連続性の確認。ソースコードや設定についてレビューを行います。

あわせて、システム構築や運用、保守に関する記録と情報を収集し、見直すべき点を調査

します。

8. 今後の対策

これまでの調査から、以下の対策を行うべきだと考えます。

容易に推測可能なパスワードによって、FTP アカウントへの不正アクセスを許し、外部から実行可能なプログラムの設置を許したことについては、

1) 不要あるいはより安全な代替方法があるサービスの停止、ポート、アクセス元の制限
2) メンテナンスアカウントのセキュリティ強化

を行うべきだと考えます。

また、不正アクセスを許していたにも関わらず、長期にわたって、これを発見できなかったことから、

3) ログの定期的な監視を行う体制の整備

を行うべきであり、さらに、サービスを構成する OS やミドルウェアについては、

4) 継続的にシステムをアップデートする体制の整備

も行うべきだと考えます。

情報漏えいが発生した場合の緩和策として、

5) パスワードのハッシュ化等による保存

をあわせて行うべきです。

（以上）