調 査 報 告 書

平成 28 年 9 月 30 日

株式会社エフエム愛知　不正アクセス特別調査委員会

1. 特別調査委員会設置について

株式会社エフエム愛知は、不正アクセスによる個人情報流出に関し、原因究明と再発防止のため、平成28年7月26日、社内調査・対策委員会を設置し、今回の事故に対する調査及び対策を行ってまいりましたが、更なる客観的、専門的な見地からの再発防止策の検討のために、外部の専門家を主たる構成員とした特別調査委員会を同年8月8日に設置し、調査を進めてきました。

(1) 当委員会の構成

委員長　　安田孝美（名古屋大学　大学院情報科学研究所　研究科長・教授）
副委員長　　小泉友　（弁護士法人アーヴェル　弁護士）
委員　　加藤義智（㈱エフエム愛知　常務取締役）
委員　　冨田隆広（㈱エフエム愛知　業務推進・事業部長）

2.本件事故の概要及び経緯について

(1)概要

平成 28 年 7 月 24 日（日）にインターネットを経由した不正アクセスにより、個人情報が漏えいしました。個人情報は、＠ＦＭ(FM AICHI)メール会員の方に関する情報、計 114,581 件の情報です。調査の結果、現時点で本件以外に個人情報の漏えいは確認されておりません。

個人情報のデータは、パスワード、email アドレス、電話番号、住所、氏名、生年月日の 6 項目で構成されていますが、6 項目がまとまって流出したものは 1 件のみで、その他は、パスワード、email アドレス、電話番号、住所の組み合わせ、又はパスワード、email アドレス、電話番号、生年月日の組み合わせで、1 項目から最大 4 項目が流出致しました。

(2)経緯

攻撃発生から不正アクセスの事実の把握、それに対し講じた対策、対応についての経緯は下記の通りです。

日　時		当事者	イベント
7 月 24 日（日）	00:11	攻撃者	SQL インジェクションによる攻撃を開始
	00:13	システム会社	システム会社担当者にサーバー負荷増大異常の通知メールが送付
	17:24	エフエム愛知	個人情報漏えい発生
7 月 25 日（月）	09:00	システム会社	システム会社担当者がメールを確認 サーバー調査、ログ解析実施
	09:30	エフエム愛知	システム会社担当者から不正アクセスの可能性があるとの一報
	15:00	システム会社	システム会社が不正アクセスを把握
	17:00	システム会社	海外からのホームページへのアクセスを遮断
	17:15	システム会社	不正アクセスによる個人情報流出の原因がSQLインジェクションであったこと、また、対象となったプログラムを特定
	18:30	システム会社	対象のプログラムを改修
	20:30	システム会社	ホームページ内の該当するデータ（メール会員データ）を外部からアクセスできない安全な場所に保管 不正アクセスの標的となったホームページのプ

			ログラムの無効化を実施
	21:30	システム会社	会員に関する機能を停止
	22:30	システム会社	流出した可能性のあるデータ件数を確認
	22:55	エフエム愛知	ホームページで個人情報流出の可能性の旨、掲載
	22:58	エフエム愛知	放送内で個人情報流出の可能性の旨、告知
7 月 26 日（火）	00:30	システム会社	ホームページの応募フォーム内ログイン機能を停止
	05:00	エフエム愛知	ホームページ内に特設ページを掲載
	09:30	エフエム愛知	不正アクセス社内調査・対策委員会を設置
	10:00	エフエム愛知	愛知県警に相談
	11:50	エフエム愛知	ホームページで再発防止策、不審なメールに対する注意喚起を実施
	12:00	エフエム愛知	情報漏えいの可能性のある会員へお詫びと注意喚起メールを送付
	12:40	エフエム愛知	放送内で新たな流出がない旨、不審なメールへの注意喚起を実施
	13:30	エフエム愛知	報道発表 ホームページで社内調査・対策委員会設置を掲載
	14:45	エフエム愛知	放送内で新たな流出がない旨、不審なメールへの注意喚起を実施
	16:33	エフエム愛知	放送内で新たな流出がない旨、不審なメールへの注意喚起を実施
7 月 28 日（木）	20:42	エフエム愛知	電子メールアドレス及びパスワード流出の可能性のあるメール会員（54,148 件）へ注意喚起メールを再送付
8 月 8 日（月）	11:00	エフエム愛知	特別調査委員会を開催
8 月 10 日（水）	09:30	エフエム愛知	不正アクセス防御システムを導入
8 月 12 日（金）	14:00	エフエム愛知	愛知県警に被害届の書類を提出、受理
8 月 18 日（木）	09:30	エフエム愛知	ホームページで特別調査委員会の設置を告知
8 月 25 日（木）	17:00	システム会社 エフエム愛知	サーバー内の該当する旧プログラムを使用したホームページについて削除し、脆弱性の調査、対応を完了

3.従前の対策について

WEBページより各種の応募を受け付け、また情報発信のためのメールマガジンを発行するため、情報セキュリティについて、システム構築時にシステム会社、ホームページ制作会社と十分な対策を講じることとして、

(1)WEB関連サーバーの必要に応じた最新パッチ対応の実施
(2)新たに作成したプログラムについては最新のセキュリティチェックを実施
(3)プレゼント応募等の受付期間の終了した必要のない応募者データの定期的削除を実施
(4)サーバーやデータベースへのアクセス制限の実施
を行ってきました。

4.原因について

前記の従前の対策を行っていたものの、情報が漏えいしたことは事実であり、結果として対策が不十分であり、技術面、管理面での体制に不備があったと考えます。

(1)技術的側面

WEB のログを解析すると、攻撃者は当社のサーバーに繰り返し様々な手法により不正侵入を試みており、情報を積極的故意的に不正侵入の方法を探り、不正取得を行う意図をもって行われた痕跡が見つかりました。従前の対策の効果でデータへの直接アクセスが不可能であると見て、サーバー上で使用しているプログラムに対して攻撃を行い、今回漏えいの原因となった過去のイベント内容を確認するために利用していた旧プログラムで、SQL インジェクションによりデータ取り出しが可能であると解析され、結果として、メール会員情報の漏えいが発生する事態となりました。

(2)管理的側面

今回、情報漏えいの原因となったプログラムは、以前一般リスナー向けに利用していたものでしたが、システム更新により新しいプログラムに置き換えられており、現在では一般に公開するものではなくなっていました。もっとも、社内業務において過去のイベント内容を確認するために残置してあったものでした。

①新たにプログラムを作成する際、最新のセキュリティ対策を執っていましたが、旧プログラムの脆弱性を検証するといった認識がなく、一定期間経過後に削除する或いは脆弱性を排除したプログラムへ切り替えるなど、明確なセキュリティ対策が取り決められておらず、実施もされていませんでした。

②会員情報は、会員自身が登録や変更を行うことなどから、WEB 関連サーバー上に保持する必要があり、そのセキュリティを確保するため、ID・パスワード方式を採用していましたが、万一の情報漏えいに備えた対策が執られていませんでした。

③「サーバー停止時」はエフエム愛知担当者を含む関係者へ異常検知メールが送信されますが、今回のような「サーバー異常」については、システム会社担当者にしか送信されず、また、異常検知の際に即時通報する仕組み、運用が存在しなかった為、結果として不正アクセス発生時にその防御の即応ができませんでした。

5.再発防止対策について

(1)技術的側面

サーバー内の該当する旧プログラムを使用したホームページについて削除を行い、他のページも脆弱性の調査・対応を完了しました。

①現在使用しているプログラムについて、また、今後、新しいプログラムを導入する場合は、一般的に講じられている SQL インジェクション対策（IPA 発行による「安全なウェブサイトの作り方」、「安全な SQL の呼び出し方」、「セキュリティ実装チェックリスト」）が行われているかの検証を行い、必要な対策を実施します。

②利用しなくなったプログラムは削除を第一として、再利用する可能性があるものは外部からアクセスできない場所に保存し、当該プログラムを再利用する場合は①の検証を必ず実施するものとします。

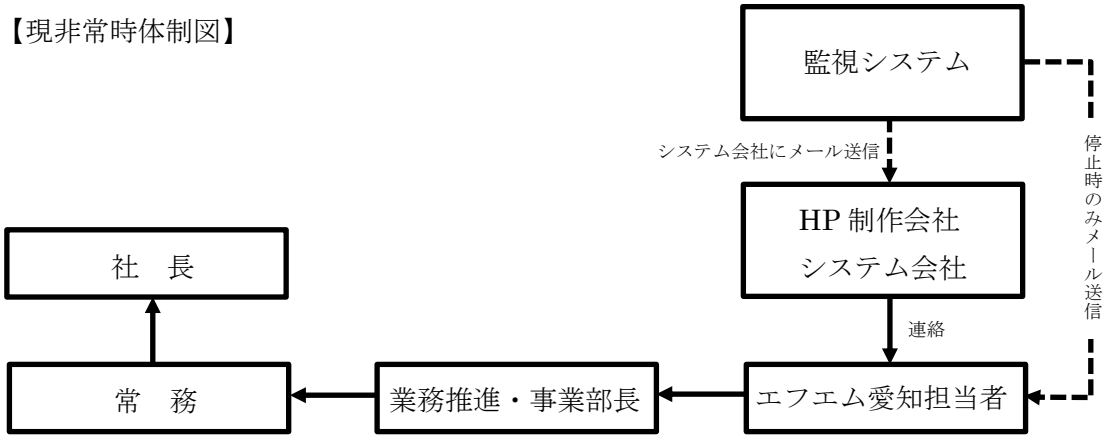
③一般的に取られている SQL インジェクション対策を超える新たな手法による攻撃、又は誤ってプログラムに脆弱性が存在した場合の対策として、不正アクセスを防御するシステムをサーバーに導入しました。

④攻撃は常にあるとの前提でデータの暗号化を実施します。

(2)管理的側面

今回の事故でも同様でしたが、攻撃者の最初のアタックから実際の情報漏えいまでにはある程度の時間がかかっています。そこで、より早い検知とそれに素早く対応することが、情報漏えいを防ぐためには有効であるとの観点から、不正アクセス防御システムの導入に併せ、不正アクセス等が検知された場合、エフエム愛知の責任・指揮の下、システム会社と連携して即応できるように管理体制を確立しました。

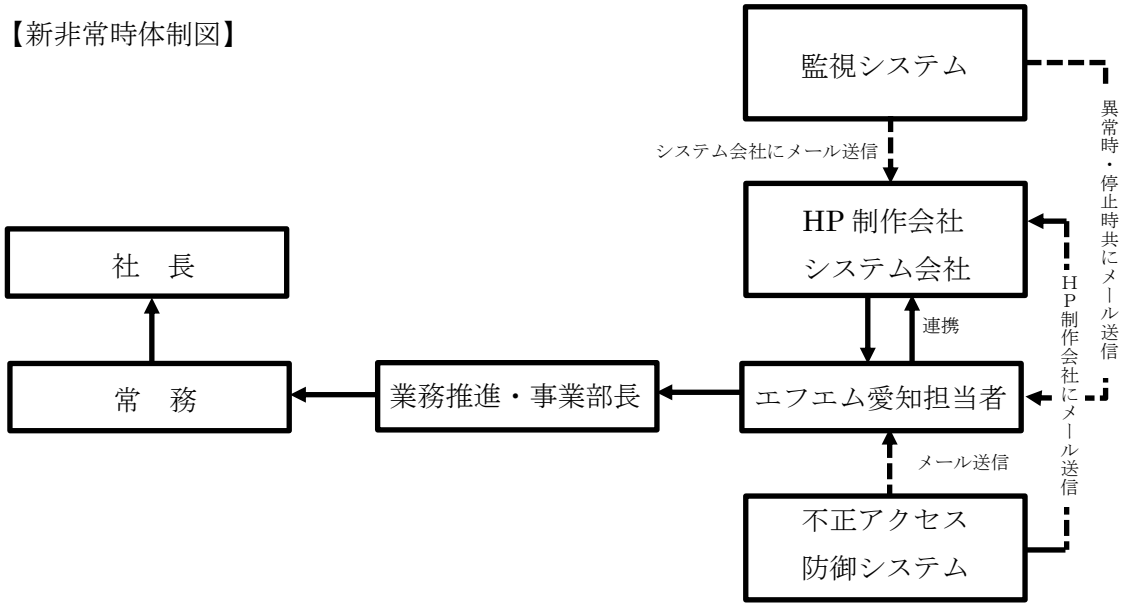
【現非常時体制図】



①サーバー異常時はシステム会社のみメール送信

②サーバー停止時はシステム会社及びエフエム愛知担当者 2 名へメール送信

【新非常時体制図】



＜サーバーが異常、停止と検知した場合＞

①サーバー異常時、サーバー停止時は監視システムよりシステム会社及びエフエム愛知担当者2名へメール送信

②システム会社とエフエム愛知担当者は連携し、ログ解析、ハードウェアチェック、回線チェック等を行い、内容を総合的に分析、判断

③分析の結果として異常であると判断した場合、体制図に沿って速やかに連絡

＜不正アクセス防御システムが異常を検知した場合＞

①不正アクセス防御システムが異常を検知した時はエフエム愛知担当者2名及びホームページ制作会社担当者へメール送信

②ホームページ制作会社とエフエム愛知担当者は連携し、メールの内容を確認、必要であれば、ログ解析、ホームページチェックを行い、内容を総合的に分析、判断

③分析の結果として異常であると判断した場合、体制図に沿って速やかに連絡

6.刑事処分等その他の対応

事故発生後、警察に相談し、8月12日（月）被害届を提出、受理となりました。

7.特別調査委員会の提言

エフエム愛知において、不正アクセス認知後の緊急対応及び発生事実の公表、原因究明のための調査と再発防止策について、適時迅速な対応がされた点については、一定の評価ができるものといえます。

ただし、本件の発生原因からは、日常のセキュリティ対策及び管理報告の徹底、また、異常検知時に即応できる体制が整っていれば、場合によっては事態の発生を未然に防ぎ、または被害の拡大を防ぐことができた可能性もあり、この点で、体制の不備が明らかになった点は否めません。

すでに、報告第5項のとおり、エフエム愛知の自主的な対策として、現時点で一定の再発防止対策はなされていますが、さらに、本委員会として、今後より一層のセキュリティを確立し、安全な管理、運営を行われることを望み、以下の対策を講じられるよう提言します。

(1)攻撃者による不正アクセスに対抗するためには、管理的側面から二重三重のチェック体制が重要であり、システム会社及びホームページ制作会社より日常的な管理報告を受ける体制を構築することで、常時、リスク認識を確立・継続することが重要と考えます。

そのために、具体的に、以下の施策の実施を求めます。
①脆弱性への対応等、年に2回程リスクマネジメントの報告
②WEB関連サーバーへアタックされた場合のシミュレーションの実施と体制の確認
③インシデント発生時の対応等について契約内容の見直し

(2)技術的側面において、最新情報のアップデートと確実な対策を講じるため、IPA発行による「安全なウェブサイトの作り方」、「安全なSQLの呼び出し方」、「セキュリティ実装チェックリスト」等による脆弱性の対応を継続的に且つ確実に実施することを求めます。

(3)今回の事故を契機として、全社的に情報漏洩及びコンプライアンスの意識を醸成するため、情報漏えいには様々な事象があり、個人情報を取り扱うセキュリティ対策が重要であることについて、社員への定期的な教育の実施を求めます。

以上