株式会社　J-WAVE
代表取締役社長　斎藤　日出夫　様

OS コマンドインジェクション攻撃に起因する個人情報漏えい事案の調査結果報告書

2016 年 6 月 2 日
特別調査委員会　委員長　　牧野　二郎
副委員長　城所　岩生
委　員　　渡邉　恵美子

株式会社 J-WAVE（以下、「当会社」という）では 2016 年 4 月 21 日未明に発生した個人情報漏えい事案に関して、本件事案の発生原因の徹底した解明と、再発防止対策を検討する必要から、社内調査を基本とし社外の専門的意見を徴収することとし特別調査委員会（以下、「調査委員会」という）を 5 月 2 日に設置した。

まず、今回の不正アクセス行為により、大量の情報にアクセスされた記録があり、その漏えいの可能性が指摘されており、なぜこの不正アクセス攻撃を防御できなかったのか、被害を発生させないための対策はなかったのか、被害を最小限に食い止める対策は十分であったのか、を解明すべきであるとした。次に個人情報を含む情報が大量となったのはなぜか、最小限にすることができなかったのか、を解明することとした。

この2つの点を解明した上で、それぞれに対応した対策を提言することとした。

事案分析

第1　不正アクセス対応

本件は、OS コマンドインジェクション攻撃により「ケータイキット for Movable Type」の脆弱性が狙われ、当会社の Web サーバが遠隔操作され、情報にアクセスされたものであるが、このアプリケーションの脆弱性の指摘は 2016 年 4 月 22 日に IPA（独立行政法人情報処理推進機構）により確認、発表されたものであり、当会社が事前に知ることはできなかったものであり、ユーザーである当会社として、当該攻撃の未然防止は困難であったといえる。しかし、当アプリの導入時において Web アプリケーションの脆弱性を悪用した攻撃から Web サイトを保護する対策を行うべきであったこと、及び攻撃に対する危機管理を徹底し、攻撃を阻止すべきであったこと、が指摘できる。

第2　個人情報を含む大量情報であった点

本来は、全ての個人情報は保管期限を定め、期限到来となった情報ごとに消去されているはずであった。当会社が取り扱う電子メールなどについては、十分な管理と定期的な消去がなされていたが、当該 Web サーバに保管されるログファイルについては、ログデータの保管期間を定め

る手続、消去する制度が未確立であったことから、自動的に各種のログが累積してしまった。その事態をサーバ管理者、担当業務の管理者が認識せず、その危険性にも気づかなかった。

このため、管理者において、消去作業の指示を出せず、結果として、大量の個人情報の累積を放置する結果となった。この点では、個人情報を扱うシステムにおける個人情報の記録、消去にかかるシステム仕様の厳密な指示が必要であった。

求められる対策

調査委員会は、今回の情報漏えい事案について、不正アクセスによる情報の漏えい事案としての側面と、個人情報の大量漏えいという側面があるととらえて、分析を進め、上記の通りの結論に至った。

すなわち、不正アクセスの事案では、巧妙な不正アクセス攻撃であったものの、十分なセキュリティ対策、特に危機対応の体制がとられていれば、事案を未然に防止できた可能性があり、結論としてはセキュリティ対応、セキュリティを確保する体制整備が大きく欠けていた点が指摘されざるを得ない。不正アクセスを想定した緊急事態に対応する体制整備がなされるべきであり、今後はそうした体制を整備することで信頼される情報管理が確立すると考える。

また、個人情報の大量漏えいの可能性がある点では、Web サーバ内に個人情報が消去されないまま順次累積し、その累積自体を認識できない仕組みであったという問題があり、そうした実態を正確に認識できる体制整備がなされるべきである。

以上のように、不正アクセス対策に不十分さがあり、また、情報管理体制が十分でなかったことを指摘して、多岐にわたり、体制の整備、改善を求めた。

当会社の事案に直面した際の緊急対応（危機管理体制）には重大な問題があり、徹底した改善を求めたが、事案発覚後の原因究明や再発防止のための機敏、かつ真剣な努力は高く評価した。

事案を隠すことなく、迅速に対応した結果、早期に当事案の真相が解明され、さらに、事案の概要を開発会社に通知し、その日のうちに対応するパッチが開発、公表され、IPA からも警告が出され、広く注意喚起がなされた。当会社の、機敏な事後対応が行われたことで、広く事業者の同種事案の防止に貢献したこと、さらにリスナーへの周知徹底も誠実に行われ、十分な注意喚起を行った結果、リスナーの二次被害の発生防止に効果的であったことは評価されるべきである。

当会社の誠実な対応を前提にすれば、情報管理の弱さが、管理者にはっきり認識できる体制を確保することで、経営陣及び関係責任者が事態を正確に理解することができれば、的確に対応することが可能になると考えられる。

以上をふまえて、今後の対策としてセキュリティ対策を実施すること、そうした対策が日々更新され、最新化されていることを確認できる体制の整備、さらに、これらに加えて個人情報を含む情報の管理が行われる体制の整備、当会社に存在する個人情報の全容を常に正確に把握でき、適切な情報管理を進めることのできる体制の確保を求めた。経済産業省の「サイバーセキュリティ経営ガイドライン」を参考にした、綿密なセキュリティ対策が必要であることを指摘した。

これらの対策にあわせて、そうした体制が機能しているか、適正に運用されているかを確認点検し、監査する監査体制を確立し、監査報告により、経営陣及び関係責任者に周知徹底される体制が必要である点を指摘し、徹底した監査体制の改善を求めた。

以上