情報セキュリティセミナー

情報サービス事業者として実施すべきセキュリティ対策

平成 27 年 6 月 29 日、TKP有楽町会議室において、JISA 情報セキュリティセミナー「情報サービス事業者として実施すべきセキュリティ対策」が開催された。出席者は 136 名。本セミナーは情報セキュリティ研究会が平成 26 年度の調査活動の中でとりあげたテーマから、JISA会員企業にも広く知って貰うべき内容を吟味して企画したものである。

まず初めにSQLインジェクションに起因するベンダ敗訴の事例が、(株)日本総合研究所法務部村上佳子氏から報告された。

本件はインテリア商材の販売を行う企業からネット通販システムの受託を受けたベンダが構築したシステムが外部からSQLインジェクション攻撃を受け、WEB サイトから顧客クレジットカード情報が漏えいし、1 億円を超える損害賠償がベンダへ請求された事件である。裁判では債務不履行責任の有無について争われたが、経産省や IPA がSQLインジェクション対策を実施するよう注意喚起していたことから債務不履行に該当すると判断され、判決として 2262 万円の支払が求められた。

今回注目すべき点は、契約書に明記されていなくてもIPAが必要としているセキュリティ対策を講じないと重過失と判断され、たとえ契約書に賠償限度額の定めがあったとしても適用されないということである。

ベンダとして同種の事案を回避するためには、以下のような対策を講じることが有効となる。

①経産省や IPA が必要と公表している措置は対応するべきである。作業工数、コスト等の情報も添えてユーザに採択を働きかけることが望ましい。

②裁判所は経産省が「望ましい」とした措置で、作業量や代金に大きく影響する事項を債務とすることには慎重である。作業工数、コスト等の情報も添えてユーザに採否の打診を行っておくことが望ましい。

③ベンダが説明を尽くしたとの事実があれば裁判所の判断も異なっていたと思われる。説明を行う場合はメール等証跡を残すべきである。採否の結果に関わらず自衛策として証跡を残すこと。

④オープンソースプログラムを利用する場合、当該プログラムを調査し、技術情報、利用条件についてユーザに提示し、その採否につきユーザに判断を求め、ユーザの責任での利用であることを契約に明記する。

続いてNTTデータの西尾秀一氏からは、情報セキュリティ早期警戒パートナーシップガイドライン 2015 年版の概要と注意点について説明が行われた。

この仕組みは平成16年7月7日に経済産業省から告示された 235 号「ソフトウェア等脆弱性関連情報取扱基準」が基となっており、ソフトウェア製品の脆弱性が発見された場合、信頼出来る第三者機関を仲介することで情報の秘匿性を保ちながら関係者に限定して安全に情報を共有し、対処することができる仕組みとして構築されている。これにより、製品開発者やウェブサイト運営者の脆弱性対策を促進するとともに危険な公表を抑制し、重要システムの停止を予防することが効果として期待されている。

2015年版では、「公表等に係る調整が不可能な場合に、公表判定委員会の審議に基づき公表することができる」「ISO に準拠するための留意点を付録として新設する」などの改正が行われている。西尾委員からは2015年版の改正のポイントに加えてSI事業者の位置づけや脆弱性対策への費用負担の調整と契約のあり方等について説明が行われた。

最後にIPAセキュリティセンター主任研究員の渡辺貴仁氏から、ウェブサイトを安全に運用するための勘所について説明が行われた。IPAでは、「安全なウェブサイトの作り方」「ウェブ健康診断仕様」「安全なSQLの呼び出し方」「ウェブサイト攻撃兆候検出ツール」「脆弱性体験学習ツール AppGoat」などの様々な読本やツールを提供している。脆弱性への対応はパッチを適用することが有効であるが、実際の場面ではシステムを止めることが出来ないことも多く、技術的な特性から影響度を分析して取捨選択する必要があり、多層防衛を考慮した総合的な対策と定期的なメンテナンスが重要であることなどが説明された。（佐藤）