Information-technology Promotion Agency, Japan

プレスリリース
2013 年 8 月 8 日
独立行政法人情報処理推進機構

IPA テクニカルウォッチ：「脆弱性検査と脆弱性対策に関するレポート」の公開

～インターネットを介した各種攻撃の主たる原因である“脆弱性”を低減する検査手法の紹介と解説～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、昨今増加する脆弱性を狙った攻撃への対策に有効とされる、ソフトウェアの脆弱性を検出する各種方法とその特徴などをまとめた「脆弱性検査と脆弱性対策に関するレポート」を 2013 年 8 月 8 日から IPA のウェブサイトで公開しました。
URL：http://www.ipa.go.jp/about/technicalwatch/20130808.html

平成 25 年度警察白書(*1)によれば、平成 24 年中に、5 分 20 秒に 1 回の割合で不審なアクセスが確認されたとあります。このようにインターネットを介した攻撃は日常的に行われており、企業の機密情報を狙った標的型攻撃やウェブサイトの改ざんなど、脅威がますます増大していることがわかります。

これらのインターネットを介した攻撃が成立してしまう大きな要因の一つに、ソフトウェアの脆弱性が挙げられます。ソフトウェアの脆弱性とは、攻撃者が意図してソフトウェア本来の仕様とは異なる動作をさせてしまうことができる弱点のことです。

攻撃を成立させないためには、脆弱性を作りこまないこと、新たに発見される脆弱性に適切な対応をすることが重要です。そのためには、①提供するソフトウェアは提供の前に適切に検査しておくこと、②運用中のシステムは定期的に脆弱性の点検をすること、が有効です。

その具体的な策の一つとして、脆弱性検査がありますが、この検査は対象とするソフトウェアや検査を行うフェーズにより、適用するツールや方法が異なります。そこでレポートでは、システムライフサイクル上（図 1）に検査方法を配置し、“いつどのような検査を行うと脆弱性の低減につながるのか”を整理しています。

大きくは、①脆弱性を作りこまないために「開発フェーズ」で実施する脆弱性検査、②新たに発見される脆弱性への対策として「運用フェーズ」で行う検査、に分け検査方法ごとに解説しています。

また、1 種のツールを用いて、実際に脆弱性検査を行い、検査にあたって必要な事前準備や今回の検査で得られた結果等を紹介しています。

本レポートの主たる対象者は開発や運用に携わる方ですが、これにより脆弱性検査への理解が開発企業の経営層にも広がることで、脆弱性検査が一層普及し、その結果脆弱性の少ない安全なシステムやサービスの提供につながることを期待しています。

(*1) 平成 25 年度 警察白書 要約版 6 ページ http://www.npa.go.jp/hakusyo/h25/youyakuban/youyakuban.pdf

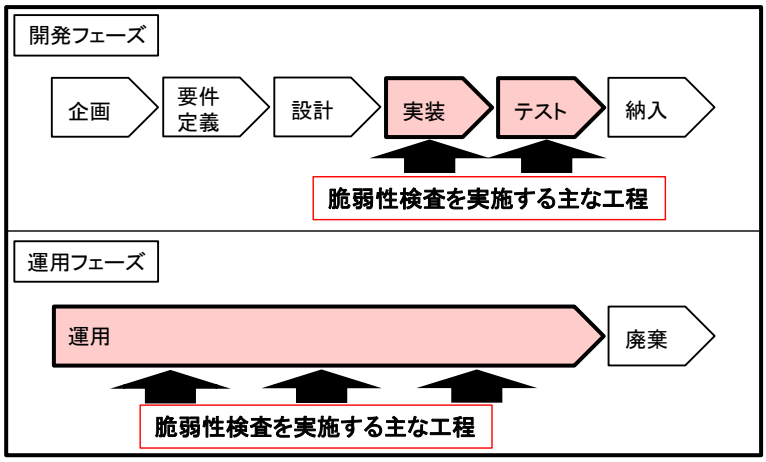

図１　：システムライフサイクルにおける脆弱性検査の実施工程

■ 本件に関するお問い合わせ先
IPA 技術本部 セキュリティセンター 金野／相馬
Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: vuln-inq@ipa.go.jp
■ 報道関係からのお問い合わせ先
IPA 戦略企画部広報グループ 横山／白石
Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: pr-inq@ipa.go.jp