プレスリリース
2009 年 6 月 8 日
独立行政法人情報処理推進機構

「ウェブサイト構築事業者のための脆弱性対応ガイド」などを公開

～「情報システム等の脆弱性情報の取扱いに関する研究会」2008 年度報告書を公開～

IPA（独立行政法人情報処理推進機構、理事長：西垣 浩司）は、ウェブサイトのセキュリティ対策を推進するため、「情報システムを安全にお使いいただくために」及び「ウェブサイト構築事業者のための脆弱性対応ガイド」を含む報告書をとりまとめ、2009 年 6 月 8 日から、IPA のウェブサイトで公開しました。

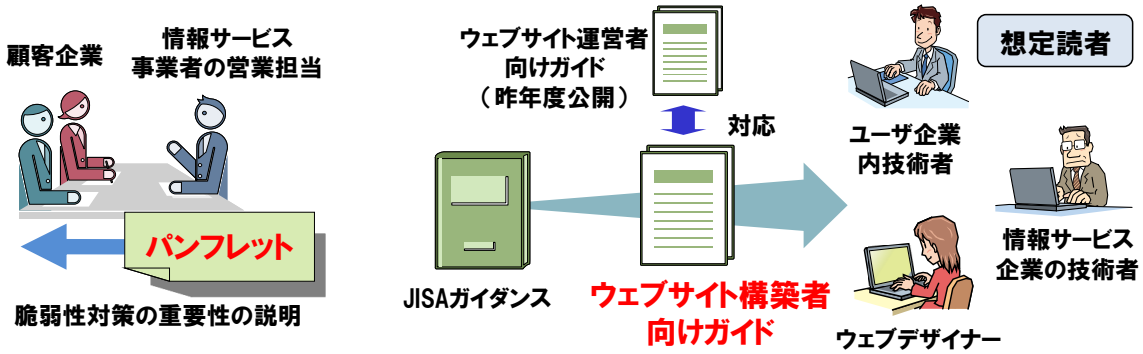
URL： http://www.ipa.go.jp/security/fy20/reports/vuln_handling/index.html

本報告書は、「情報システム等の脆弱性情報の取扱いに関する研究会」（座長：土居 範久　中央大学教授）において、昨年 10 月から行われた検討の成果です。

IPA では、情報サービス事業者、セキュリティベンダー、セキュリティに関する有識者など約 20 組織に対して、昨年 10 月から本年 3 月までにヒアリングを行い、ウェブサイトの脆弱性対策を促進する上での課題を抽出しました。

このヒアリングにおいて、ウェブサイトを公開している企業の中には、システム導入・運営上の意思決定を担う層の脆弱性に関する知識が乏しく、運用・保守の予算が十分に確保されていないケースが少なくないことが判明しました。また、「情報セキュリティ早期警戒パートナーシップ[1]」への届出の半数を占めるクロスサイト・スクリプティングや SQL インジェクション脆弱性に関しては、ウェブサイト構築時の原因も多く、ウェブサイト構築者が脆弱性対策への意識をいっそう高める必要がある、などの課題が浮き彫りとなりました。

このような問題に対応するため、「情報システム等の脆弱性情報の取扱いに関する研究会」では、ウェブサイトの責任者向けに、脆弱性対策の重要性を簡潔に記したパンフレット「情報システムを安全にお使いいただくために」を作成しました。また、情報サービス企業の技術者やウェブデザイナー、企業内でウェブサイト構築・運用を担当する技術者向けに、JISA ガイダンス[2]を補足する資料として、システムの納入前や納入後に考慮すべきことをまとめた「ウェブサイト構築事業者のための脆弱性対応ガイド」を作成しました。



本資料が、ウェブサイト構築関係者にとって、セキュリティ対策推進の参考となることを期待しています。なお、本ガイドは、脆弱性関連情報の適切な流通により、コンピュータ不正アクセス、コンピュータウイルスなどによる被害発生を抑制するために、関係者に推奨する行為をとりまとめたガイドライン「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」の一部とする予定です。

■ 本件に関するお問い合わせ先
IPA セキュリティセンター　山岸／渡辺
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／大海
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp

[1] ソフトウェア製品及びウェブアプリケーション（ウェブサイト）に関する脆弱性関連情報を円滑に流通し、対策の普及を図るための、公的ルールに基づく官民の連携体制です。経済産業省告示に基づき、2004 年 7 月より開始しました。

[2] 「SI 事業者における脆弱性関連情報取扱に関する体制と手順整備のためのガイダンス、（社）情報サービス産業協会（JISA）、（社）電子情報技術産業協会（JEITA）」：http://www.jisa.or.jp/report/2004/vulhandling_guide.pdf

別添

「情報システム等の脆弱性情報の取扱いに関する研究会」報告書について

2008 年度を概観すると、内閣官房情報セキュリティセンターが事務局を務める情報セキュリティ政策会議で、2009 年 2 月 3 日の会合で「第 2 次情報セキュリティ基本計画『IT 時代の力強い「個」と「社会」の確立に向けて』」をとりまとめた点が注目される。第 2 次基本計画は、第 1 次基本計画に基づく各種の取組みの進展や社会環境の変化などを踏まえ、引き続き我が国全体として情報セキュリティ問題への取組みを力強く推進するもので、第 1 次基本計画同様、3 年間（2009 年度から 2011 年度まで）を対象としている。

一方、2008 年 7 月に複数の DNS サーバ製品の開発ベンダーから公表された「DNS キャッシュポイズニングの脆弱性」は幅広い機関が該当したため、「情報セキュリティ早期警戒パートナーシップ」に届出が急増し、2008 年 8 月～2009 年 3 月のわずか 8 ヶ月間で届出累計は 1,131 件に達している。また、「SQL インジェクションの脆弱性」についても、2008 年 4 月～2009 年 3 月の届出累計は 318 件に達しており、依然として情報化社会は脆弱な環境であることがうかがえる。

このような状況において、脆弱性対策を促進するための社会制度である「情報セキュリティ早期警戒パートナーシップ」が果たすべき役割は、ますます重要になっている。

そこで、今年度の「情報システム等の脆弱性情報の取扱いに関する研究会」では、そうした先導役としての社会的ニーズを踏まえ、具体的なアプローチや課題、啓発ツール等について議論した。本報告書はその検討を集約したものである。

■ 報告書の構成（目次）

1. 情報セキュリティ早期警戒パートナーシップの現状と課題
    1.1. 背景
    1.2. 運用の状況
    1.3. 普及啓発の状況
    1.4. 本年度研究会における検討
2. 脆弱性対策の普及・啓発に係る検討
    2.1. 対策促進に関する課題
    2.2. 情報サービス事業者等が活用可能な普及・啓発資料の策定
    2.3. 普及・啓発に係る方策の検討
3. 組込みシステムの脆弱性に係る検討
    3.1. 対策促進に関する課題
    3.2. 組込み製品の情報セキュリティ機能に係るユーザ向け普及啓発資料の策定
    3.3. 組込み製品の情報セキュリティ機能のユーザ向け説明記載等のあり方の検討
    3.4. 組込み製品における脆弱性の検討
4. パートナーシップの強化・浸透に係る検討
    4.1. パートナーシップ関係者間の関係強化
    4.2. 脆弱性発見から対策適用までの分析・検証能力の強化
    4.3. 暗号アルゴリズム及びプロトコルの脆弱性の取扱い
5. JVN/パートナーシップの目指すべき方向性と展開に係る検討
    5.1. 海外の関連研究動向を踏まえた JVN 機能の方向性
    5.2. 長期化案件への対応方針の検討
    5.3. 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の修正に関する検討
    5.4. 今後の課題

別紙 1. 情報システム等の脆弱性情報の取扱いに関する研究会 名簿
別紙 2. 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 改訂案

■報告書のダウンロード

http://www.ipa.go.jp/security/fy20/reports/vuln_handling/index.html