2020 年 12 月 25 日

サービス＆セキュリティ株式会社 e-Gate センター

Web アプリケーション脆弱性診断での検出傾向と対策について

1. 概要

2020 年 10 月 22 日に JPCERT/CC から報告された 2020 年度第 3 四半期の「ソフトウェア等の脆弱性関連情報に関する届出状況」によると、ウェブサイトに関するものが全体の 7 割となっており、公開されるウェブサイトには脆弱性存否の確認とその対策が必須と言えます。

当社 e-Gate センターでは WEB アプリケーションの脆弱性診断サービスをご提供しており、10 数年（約 1900 プロジェクト以上）の豊富な実績がございます。今回は、JPCERT/CC から報告された脆弱性関連情報に加えて、当社 e-Gate センターの脆弱性診断サービスで検出された脆弱性から、検出傾向とその対策についてご紹介いたします。

2. 状況

2.1 JPCERT/CC から報告された脆弱性関連情報

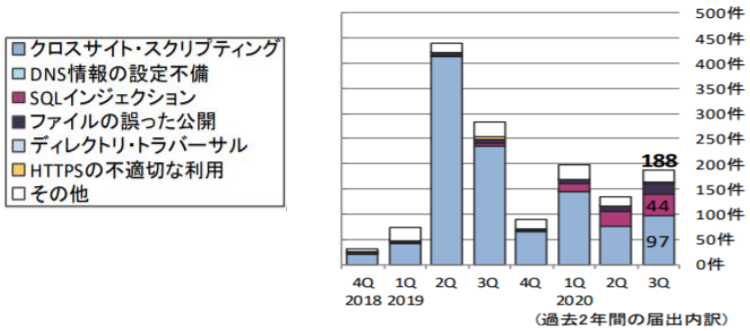
JPCERT/CC の報告書によると、2020 年第 3 四半期に JPCERT/CC に報告された脆弱性関連情報は、ソフトウェア製品が 58 件、ウェブサイトは 189 件となっています。また届け出受付開始(2004 年 7 月 8 日)から本四半期末までの累計では、ソフトウェア製品が 4,627 件、ウェブサイトは 11,296 件となっています。直近四半期から見ても累計数からみても、報告内容の 7 割超がウェブサイトに関する脆弱性で占められています。

表 1 届出件数

分類	2020 年 7 月から 9 月	累計
ソフトウェア製品	58 件	4,627 件
ウェブサイト	189 件	11,296 件
合計	247 件	15,923 件

ウェブサイトに関する脆弱性種類別の届出状況では、2020 年第 3 四半期はクロスサイトスクリプティング（XSS)97 件、SQL インジェクション 44 件となっています。また、クロスサイトスクリプティングが最も報告の多い脆弱性である傾向は 2018 年第 4 四半期から変わりがありません。

図 1 四半期ごとの脆弱性の種類別届出件



出典： JPCERT/CC：ソフトウェア等の脆弱性関連情報に関する届出状況

2-2. e-Gate センターで実施した脆弱性診断サービスでの検出傾向

当社 e-Gate センターの WEB アプリケーション脆弱性診断サービスで検出した脆弱性についても同様の傾向が見て取れます。

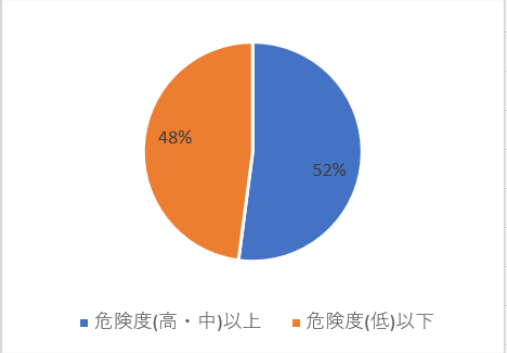
2020 年 1 月から 10 月までの危険度高及び中の検出脆弱性上位 5 種類は、下表の通りです。特にクロスサイトスクリプティングについては、当社で実施した診断案件でも、危険度高・中の検出脆弱性の 34%を占めており、JPCERT/CC から報告された内容と同様に、数多くのウェブサイトで検出されている傾向となっています。

表２　脆弱性、種類別(高・中)の検出割合

脆弱性種類(高・中)	割合
クロスサイトスクリプティング	34%
クロスサイトリクエストフォージェリ	16%
メール本文の改ざん	11%
SQL インジェクション	8%
HTTP リクエストスマグリング	5%
その他	26%

また、同期間の全診断案件で危険度中以上の脆弱性が検出された案件は 52%に上っています。

図２　実施案件ごとの危険度別検出割合



3. クロスサイトスクリプティングの概要と影響

本章では、最多の検出数であるクロスサイトスクリプティング（XSS)の概要と影響についてご説明いたします。

Web アプリケーションが外部からの入力に応じて表示を変化させる箇所で HTML 生成の実装に問題があった場合、任意のスクリプトをサイト利用者に実行させることが可能となる場合があります。この脆弱性がクロスサイトスクリプティング（XSS）と呼ばれるものです。

外部から入力・変更できるパラメータを表示する箇所の 1 か所でもクロスサイトスクリプティングの脆弱性があると、サイトの全利用者に甚大な影響を与える場合もあります。

また攻撃が容易な点も特徴になります。脆弱性存否の確認が一般的なスクリプトを入力箇所に入力するだけで試行することができます。

XSS を悪用した攻撃として、次のような例が挙げられます。

・セッションハイジャック－攻撃者による cookie 情報の奪取。奪取する事による正規ユーザへのなりすまし等

・ウィルスの感染－WEB サイト閲覧者へのウィルス感染

・フィッシングサイト－WEB サイト閲覧者の個人情報やクレジットカード情報などの盗聴

今夏だけでも、下記の様な被害事例が発生しています。

・2010 年 7 月に動画共有サイトでの攻撃により、ショッキングなデマが流れたり、不正なポップアップが表示されたり、悪趣味な WEB サイトにリダイレクトされたりした。

・2010 年 9 月に SNS にてクロスサイトスクリプティングの脆弱性を悪用したワーム(ロールオーバーした文章を自動でリツイートしてしまう性質を持つ)が拡散し、爆発的な勢いで混乱が拡大した。

以上のとおり、XSS は、扱う変数全てで処理が必要なために抜け漏れも発生しやすい脆弱性であること、また攻撃も容易で、攻撃が成立した場合の影響が大きいことが分かります。

4. WEB アプリケーションの総合的な脆弱性対策と脆弱性診断サービスの重要性

WEB アプリケーションには様々な脆弱性が潜んでいます。これら脆弱性を可能な限り減らし、ウェブサイトを安全に運用するためには、WEB アプリケーション構築における設計から本番リリース、運用までの各工程で次のような対策が考えられます。

・設計・開発工程－セキュリティを考慮したシステム設計に基づいてプログラムの作成やサーバー設定を実施する。
・テスト工程－ソースコードレビューやテストにより、設計・開発工程で考慮・実装したセキュリティの存否・適否を確認する。
・本番リリース・運用－Web アプリケーションファイヤウォール（WAF）や侵入遮断装置（IPS）などで攻撃を防ぐとともに監視サービスなどを利用し迅速な対応が実施可能な運用サイクルを構築する。

WEB アプリケーションの設計・開発工程で完全な対策ができれば脆弱性の混入を防ぐことができます。しかし現実には、当社で実施している脆弱性診断サービスでも半数以上のお客様で危険度が高・中レベルの脆弱性が検出されているように、構築時時点での脆弱性をゼロにすることは困難と言えます。その主な原因として下記が挙げられます。

・全開発者が脆弱性の知識を持っているわけではないため、知識不足により脆弱性が混入する可能性がある。
・知識を持った開発者や設計者でも短い開発期間で十分な考慮が出来ない場合がある。
・ウェブ技術の進歩により新たな攻撃手法が開発されることがある。

脆弱性の悪用による重大なインシデント発生を防止するためには、脆弱性診断サービスを本番リリース前に利用して脆弱性を検出・除去すると共に、新しく顕在化した脆弱性に対応するために運用後も脆弱性の情報を定期的に取得・確認することが重要と考えます。

5. 参考情報

JPCERT
・ソフトウェア等の脆弱性関連情報に関する届出状況 [2020 年第 3 四半期 (7 月～9 月)]
https://www.jpcert.or.jp/pr/2020/vulnREPORT_2020q3.pdf

ITmedia
・SNS にてクロスサイトスクリプティングに対する脆弱性
https://www.itmedia.co.jp/news/articles/1009/24/news023.html
・動画共有サイトを狙った攻撃
https://www.itmedia.co.jp/enterprise/articles/1007/06/news018.html

6. e-Gate の脆弱性診断サービスについて

e-Gate の脆弱性診断サービスでは、お客様のシステムの脆弱性存否を診断し、検出されたリスクへの対策をご提案させていただいております。

次のような内容を実施することで混入してしまった脆弱性を検出しています。

・WEB アプリケーションで発生するリクエストとレスポンスの静的スキャン

・WEB アプリケーションで発生するリクエストに対して様々なパターンで疑似的な攻撃を行う動的スキャン

・スキャンでは検出できない脆弱性に対する手作業による診断

脆弱性診断サービスをご活用いただくことで、セキュリティインシデントの発生を予防することが可能となり、対策コストや被害を最小限に抑えることができます。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた「IT 運用のノウハウ」と最新のメソッドで構築した「次世代 SOC“e-Gate センター”」。この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”サービスです。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

※本資料には当社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。
リンク先のコンテンツは予告なく、変更、削除される場合があります。

※掲載した会社名、システム名、製品名は一般に各社の登録商標 または商標です。

«お問合せ先»

サービス＆セキュリティ株式会社

〒150-0011

東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F

TEL 03-3499-2077

FAX 03-5464-9977

sales@ssk-kan.co.jp