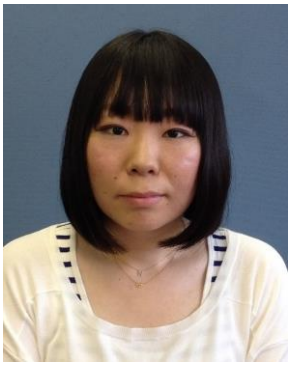
セキュリティソリューションの提供における多角的視点（攻撃者・開発者・お客様）の重要性について

富士通エフ・アイ・ピー株式会社

■ 執筆者Ｐｒｏｆｉｌｅ ■



渡邉　奈津美

2013 年　富士通エフ・アイ・ピー（株）入社
スマートサービス事業部 SaaS システム部所属
セキュリティソリューションの提供を担当

■ 論文要旨 ■

筆者は、Web アプリケーション脆弱性診断、ネットワーク脆弱性診断、Web アプリケーションファイアウォール導入支援サービスなどのセキュリティソリューションをお客様へ提供している。日々の業務の中で、セキュリティソリューションを提供する上では、一システムエンジニアとしてではなく、多角的な視点で物事を捉えることが重要であると気づいた。
本稿では、Web アプリケーション脆弱性診断サービスの提供を通じて、筆者が直面した課題と課題解決への取り組み、その中で養われた複数の視点について述べる。更に、これまで養ってきた視点を、他のサービス提供時にどのように適用可能かを述べる。

■ 論文目次 ■

１．はじめに ……《 3》

２．Webアプリケーション脆弱性診断サービス……《 3》

３．課題と改善策 ……《 4》

３．１　診断実施

３．１．１　課題

３．１．２　改善策

３．２　結果報告

３．２．１　課題

３．２．２　改善策

４．まとめ……《 6》

■ 図表一覧 ■

図１　Webアプリケーション脆弱性診断サービス提供の流れ……《 3》

１．はじめに

当社は国内最高水準の安全性を誇るデータセンターを全国 16 箇所に展開し、これらのデータセンターを基盤に、「アウトソーシング」、「クラウド」、「ソリューション」の 3 つを柱とした事業を展開している。「アウトソーシング」では、システムの企画からインフラ構築、運用、保守までライフサイクル全般を支援している。「クラウド」では、お客様の求める幅広いニーズに応えた SaaS（Software as a Service）サービスや PaaS（Platform as a Service）サービスの提供を通じて、お客様の戦略的な ICT 活用を支援している。「ソリューション」では、豊富なノウハウと最新の開発技術を組み合わせ、お客様と一体となって最適なものづくりを行っている。

筆者は 2013 年 4 月に入社し、学生時代、暗号理論やプライバシ保護の研究に取り組んできたことから、セキュリティに関係する業務に携わりたいという思いを持っていた。2013 年 7 月末、セキュリティソリューションを提供する部署へ配属となり、Web アプリケーション脆弱性診断、ネットワーク脆弱性診断、Web アプリケーションファイアウォール[1]（以下、WAF）導入支援サービスなどをこれまで 22 社に提供してきた。これらのサービス提供を通じ、先に紹介した 3 つの事業をセキュリティ面から支えている。サービスを提供する中で、一システムエンジニアとしてではなく、多角的な視点で物事を捉えることの重要性に気づき、これまでに複数の視点を養ってきた。

本稿では Web アプリケーション脆弱性診断を例に、筆者がどのような取り組みを通じて多角的な視点を養ってきたか、更に他のサービスを提供する際にどのような適用が可能かを述べる。

２．Web アプリケーション脆弱性診断サービス

Web アプリケーション脆弱性診断とは、お客様の Web サイトに潜む脆弱性を調査し、検出された問題点と、その対策方法のアドバイスを提供するサービスである。Web サイトの改ざんや不正アクセス、個人情報の漏えいが問題となっている昨今、需要が高まっている。特に、個人情報やクレジットカード情報を取り扱う通販サイトや、チケットの予約サイトを運営しているお客様からの需要が高い。サービス提供の流れを図 1 に示す。

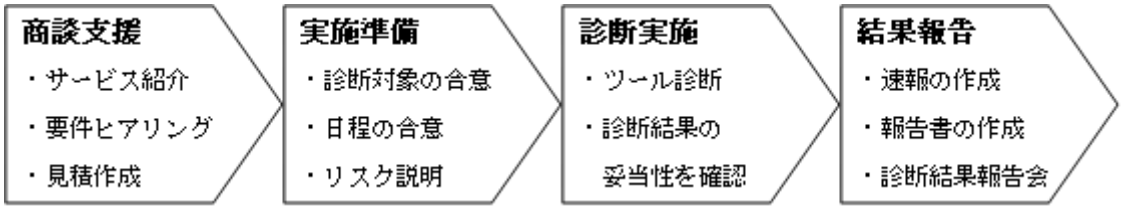


図 1　Web アプリケーション脆弱性診断サービス提供の流れ

[1] Web アプリケーションの脆弱性を悪用した攻撃などから Web アプリケーションを保護するソフトウェア、またはハードウェア。

３．課題と改善策

３．１　診断実施

「診断実施」のフェーズでは、まず、商用の脆弱性診断ツールを用いて診断を実施する。これは、指定した Web サイトに対してツールが数千の攻撃リクエストを自動で送信し、脆弱性の有無を調査するというものである。その後、誤って検出されている脆弱性がないか、診断担当者が手動で攻撃リクエストを送信し、ツールによる診断結果を精査する。更に、お客様から手動で診断して欲しいと依頼いただいた箇所があれば、手動での診断も実施する。

３．１．１　課題

診断を実施するにあたり、当然ながら脆弱性の概要や検出方法、更には Web アプリケーションやデータベースに対する理解など、専門的なスキルが求められる。日々の診断において、何をするにも自分自身で判断できず、他の診断担当者に確認しなければ作業が進まないことから、以下に対する理解が不足していると感じた。

〇攻撃リクエストの目的

- 診断ツールによって送信される攻撃リクエストが、それぞれ何の脆弱性を調査するためのものか
- 手動で診断する際に、どのような攻撃リクエストを送信すべきか

〇妥当性の検証方法

- どのように正しい検知と誤検知を見分けるか
- 脆弱性が見落とされていないか

〇脆弱性の発生ポイント及び原因

- どこで脆弱性が発生するか、また発生しやすい箇所はどこか
- なぜ脆弱性が発生するか

３．１．２　改善策

「攻撃リクエストの目的」及び「妥当性の検証方法」に対する理解を深めるためには、脆弱な Web サイトに対して、実際に攻撃リクエストを送信し、どのようなレスポンスが得られるか、繰り返し試すことが有効であると考えた。筆者が取り組んだ具体的な方法を以下に述べる。

[脆弱な Web サイトの準備]

インターネット上で配布されている、意図的に脆弱性を作りこんだ Web サイトを参考に、当社検証環境の仮想マシン上に脆弱な Web サイトを用意した。インターネット上で一般公開されている Web サイトに対して攻撃リクエストを送信したのでは、法に触れる恐れがあるからである。また、誤って外部へ攻撃リクエストが送信されないよう、外部との接続を遮断することを徹底した。

[擬似攻撃の実施]

筆者の所属部署では 2007 年から Web アプリケーション脆弱性診断サービスを提供してお

り、これまでの診断で溜め込んだ数多くのノウハウがある。中には、診断が原因で発生した障害を例に、なぜ障害が発生したか、どのような注意を払うべきであったかを考察し、再発防止を目的に作られた攻撃リクエストもあり、より実践的な知識を得ることができた。得た知識を定着させるべく、仮想マシン上に用意した脆弱な Web サイトに対して、繰り返し攻撃リクエストの送信を試みた。

結果として、脆弱性診断ツールを利用せずとも、SQL インジェクション[2]やクロスサイトスクリプティング[3]などの危険度の高い脆弱性を自身の手で検出できるようになった。また、攻撃リクエストに対するレスポンスを見ながら、臨機応変に攻撃リクエストを改変するという術も次第に身につけた。実際の診断において、ツールでは検出されなかった脆弱性を手動で検出できるようになったことは大きな成果であるといえる。

よって筆者の取り組みは、「攻撃リクエストの目的」及び「妥当性の検証方法」に対する理解を深めるために有効であったと考える。また、これらの取り組みは、一システムエンジニアとしてではなく「攻撃者視点」で物事を捉えることの重要性に気づくきっかけとなった。日々の診断の中で「攻撃者視点」を常に意識するようになったことは、何よりの収穫である。

「脆弱性の発生ポイント及び原因」に対する理解を深めるためには、実際に Web サイトを作成してみることが有効であると考えた。そこで筆者が実施した取り組みを次項に述べる。

[安全な Web サイトの作成]

IPA（独立行政法人 情報処理推進機構）から発行されている「安全なウェブサイトの作り方」[4]や、社内で開催されているセキュア Web アプリ研修の資料などを参考に、セキュアプログラミングを実践し Web サイトを作成した。

作成した Web サイトが安全か否か、対策は適切であったか確かめるためには、攻撃リクエストを送信して確認する必要があると考えた。そこで、先に紹介した取り組み「擬似攻撃の試行」を通じて習得した攻撃リクエストを送信し、自身の作成した Web サイトの安全性を検証した。脆弱性が検出された場合は、原因を明確にしてから修正し、再度攻撃リクエストを送信することで正しく修正されているか検証を行った。更に、意図的に脆弱性対策を施さない箇所を設けて攻撃リクエストを送信し、対策が施されている場合との差異を確認した。

結果として、脆弱性の発生ポイントや原因に加えて、一般的な対策や修正方法を修得することができた。脆弱性の概要や事象、原因だけでなく、本質や根本的なメカニズムを理解するのに大いに役立った。

よって筆者の取り組みは、「脆弱性の発生ポイント及び原因」に対する理解を深めるた

---

[2] Web アプリケーションと連動したデータベースの不正操作が可能となる脆弱性。
[3] Web アプリケーションに不正なスクリプトの埋め込みが可能となる脆弱性。
[4] IPA（独立行政法人 情報処理推進機構） 安全なウェブサイトの作り方
https://www.ipa.go.jp/security/vuln/websecurity.html

めに有効であったと考える。それだけでなく、「攻撃者視点」に加えて「開発者視点」からも物事を捉えることが重要であるということに気づくよいきっかけとなった。

３．２　結果報告

「結果報告」のフェーズでは、診断結果に基づいて速報及び報告書を作成し、お客様の希望に応じて対面での報告会を実施する。

３．２．１　課題

結果報告書を作成する中で、他の診断担当者や上司から

- 単に事実を記載しているだけではないか
- お客様が知りたいことは何か考慮しているのか

との指摘を度々受けた。これまでに養った「攻撃者視点」でどのようにして脆弱性が検出されたか、「開発者視点」でどのような対策を取ればよいか記載しているのみで、「お客様視点」が欠如していたことが原因と考えられる。

３．２．２　改善策

お客様が知りたい情報は一体何であるか、また、筆者の作成した報告書に不足している点は何かを探るべく、経験豊富な他の診断担当者が作成した報告書と、筆者の報告書とを比較した。結果として、筆者の報告書には「脆弱性」に付随する「脅威」や「リスク」に対する言及が全くないことに気づいた。また、お客様が専門的な知識を持たないケースを想定していないことが明らかとなった。Web アプリケーション脆弱性診断サービスを提供する際、お客様≠開発者というケースがほとんどである。このような場合、お客様が求めているのは、何故脆弱性が検出されたか、どのように修正すればよいかという技術的な話ではないということに気づいていなかったのである。

このような分析から、「脆弱性」が存在する場合、どのような「脅威」と結びつくことによって「リスク」が生じるのか、つまり「脆弱性」を悪用された場合どのような被害が想定されるかということこそ、お客様の知りたいことであると気づくことができた。また、システムリスクだけでなく、情報漏えいによる社会的信用の失墜や Web サイトの一時閉鎖による機会損失などのビジネスリスクにも言及する必要があるということに気づいた。

以降、報告書を作成する際にこれらの観点を取り入れるよう心がけたところ、指摘を受ける機会も徐々に少なくなり、お客様から「報告書がとてもわかりやすかった」との言葉をいただくこともできた。

４．まとめ

日々の業務の中で、セキュリティソリューションを提供する上では、一システムエンジニアとしてではなく多角的な視点で物事を捉えることが重要であると気づいた。筆者はこれまで、Web アプリケーション脆弱性診断サービスの提供において様々な課題に直面し、課題解決のための取り組みを自ら考えて実践してきた。結果として、診断を実施する際は「攻撃者視点」、脆弱性の修正方法や対策を考える際は「開発者視点」、報告書を作成する際は「お客様視点」で物事を捉えることができるようになった。その中でお客様からい

ただいたお褒めの言葉や感謝の言葉は、仕事に対するやりがいを感じさせてくれるだけでなく、更によいサービスを提供しようという原動力となっている。

そして、筆者は現在、複数のお客様に対し WAF 導入支援サービスを提供中である。これまでに筆者が養ってきた 3 つの視点は、WAF の導入支援サービスにおいても適用可能である。WAF を導入するにあたり、正常な通信が誤って遮断される可能性や、ネットワークへの負荷などを考慮する必要がある。また、WAF による検知ログを解析しお客様へ報告する際は、解析結果を表やグラフで示すだけでなく、攻撃通信が正しく遮断されており、Web サイトに与える影響はないということを伝えていく必要がある。導入に際しては「開発者視点」に加え「インフラ視点」で、お客様への報告に際しては「お客様視点」で物事を捉えるよう心がけている。更に、WAF の導入後や設定変更後に、期待どおりに攻撃が遮断されるか検証する必要があり、テストケース作成時には「攻撃者視点」で自ら攻撃リクエストを考えている。

今後は、Web アプリケーション脆弱性診断、WAF 導入支援サービス以外にも様々なサービスをお客様へ提供していくことになる。いかなる場合も、多角的な視点で物事を捉えることを心がけ、お客様へよりよいサービスを提供していきたい。