ケーススタディ

「WEB アプリケーション」を常に安全に保つ秘訣

新型コロナウイルスによりインターネットそしてウェブサイトを経由して行うサービスは一段と加速した。教育現場においても、教職員や学生が授業や学務、学校生活でWeb アプリケーションを利用することは加速した。その反面、Webアプリケーションを介した攻撃や情報漏洩の報道は列挙にいとまがない。

オンラインがもたらす利便性や新型コロナウイルスへの対策をしっかり享受しつつ、個人情報や資産の保護を両立させるために行うべきことをエヌ・ティ・ティ・データ九州の取り組みと実際に起こったセキュリティのイベントにスポットライトを当ててみる。

株式会社 NTTデータ九州

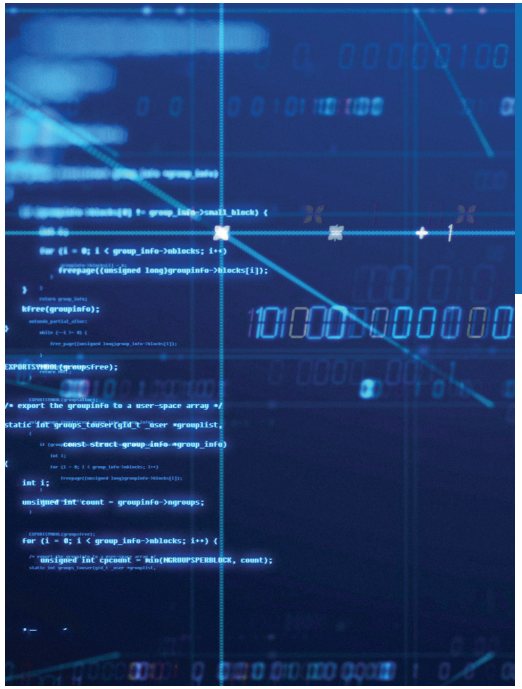
https://www.nttdata-kyushu.co.jp

業種：情報技術

課題：利便性向上とセキュリティ

導入サービス：DigiCert クラウド型WAF

NTTデータ九州は、情報技術で、新しい「しくみ」や「価値」を創造し、より豊かで調和のとれた社会の実現に貢献します。



Web アプリケーションにより実現する世界

公共の利益を追求する大学や公立図書館は、基本的にオープン性が強く求められる組織だ。その点、インターネット経由で情報を発信したりサービスを提供したりできるWeb アプリケーションを充実させることは、こうした組織の特性にも合っているといえる。NTT データ九州では、大学向け教務システム「LiveCampus」や大学・公立図書館向け図書館情報システム「NALIS」といった実績あるパッケージシステムを提供している。そして、大学向けNALIS は、クラウドサービスとして利用できるSaaS（Software as a Service）として提供されており、WAFの同時利用は過去5年間で21%から51%増加しており、全国各地の大学や公立図書館から高い評価を得ている。

さらにコロナの感染拡大により、外出制限を伴った対策が求められたためインターネット経由でのサービスの提供は加速したことが、大学での実装増加の背景にあった。

セキュリティの重要性

一方で大学や公立図書館は、学生の成績や図書館利用者の閲覧履歴など極めて慎重に扱うべき個人情報がやりとりされる。オンライン化での利点は生かしつつ、必要な情報は公開し、機密情報をしっかり守るためにはセキュリティ対策はしっかりと検討する必要がある。「大学や公立図書館は外部から攻撃を受けやすい組織です。しかしながら、他業種と同様セキュリティ人材は不足しており、セキュリティに十分なリソースを割けないのが現状です。」NTT データ九州 公共システム事業部　文教ビジネス統括部　営業担当部長の後藤裕治氏は、説明する。「セキュリティを正しく理解し、適切な対応をすることが重要です」と後藤氏は述べる。セキュリティインシデント対処基準は、公的なインシデント報告があったときなどに、同社の業務システムやサービスでどのような対策を実施すべきかを明確にし、ユーザー組織へ余計な不安を与えないようにする取り組みだ。

特に大学や図書館でWebサービスの管理を行うメンバーは、ITの専門家ではなく業務担当者であることがほとんどであり、外部の業者の協力を得ながらサービスを導入し運用していくことになる。しかしここでセキュリティの落とし穴が顕在化することがある。全てのシステムを一つの業者が担当していれば、Webサービスを構成する全ての構成を理解し新たに発見された脆弱性への対策を早くに判断・導入できる。しかし、複数

の業者が関わる場合など、漏れが生じるリスクがあるのだ。また、学生や一般消費者向けで時間帯問わず利用されるシステムである特性上、サービスを止めない時間帯でメンテナンスを行う必要がでるなど制限事項が発生する。

メンテナンスフリーで最新の安全性を確保

特に昨今、Web アプリケーションの脆弱性に関する報告が急増し、サービスベンダーの対応が困難な状況が続いている。NTT データ九州でも「一度セキュリティインシデントが発生した場合、当社製品をご利用いただく全国120以上の管理対象サイトに対して、すべて短時間で即応するというのは技術的にも要員的にも現実的ではない状況です」と、開発担当の堤公孝氏は明かす。堤氏が「Web アプリケーションへのセキュリティ侵害を未然に防ぎ、根本的な解決を図るまでの施策として効果的」だと語るのが、Web アプリケーションファイアウォール（WAF）だ。そこで NTT データ九州では、大学や公立図書館向けの全ての製品／サービスに対して、WAF のバンドルを推奨する。

WAF といえば、ソフトウェアやアプライアンス製品などをオンプレミスシステムとして導入する形態をイメージされるかもしれない。ただ、ソフトウェアやアプライアンス製品のWAFは利用中のWebアプリケーションやシステムに対する脆弱性の情報収集、新たに見つかった脆弱性の自社システムへの影響を判断するのはハードルが高く敬遠されがちである。メンテナンスの煩雑さを懸念して、導入を諦める大学や公立図書館も少なくない。「そもそも IT 人材の確保に苦労されている組織に、まさか“セキュリティ対策に知見のある保守要員を準備してほしい”などとは言えません。とはいえ、アプリケーション開発を主業務とする当社で全てのお客さまの WAFサービスを運用するのも困難です」（後藤氏）

そこでNTT データ九州が選んだのが、デジサート・ジャパン（以下、デジサート）が提供するWAF のクラウドサービス「デジサート クラウド型 WAF」である。クラウドサービスなので、保護対象であるWeb アプリケーションへの影響が小さく、ネットワークの設定変更だけで短期間に導入できる。そしてWAF のメンテナンスは国内集中管理された国内教育機関や公共機関での実績が豊富にある堅牢な WAFセンターで実施する。

WAF システムは年 100 回にわたる更新で常に最新の状態に保っており、緊急性の高い脆弱性情報にも極めて迅速に対処している。何よりユーザー組織の運用負荷の増大がないことが大きなメリットだ。

特に2021年の年末に発見されたLog4j脆弱性は、2022年前半にかけて各企業に激震を走らせた。汎用性が高いプログラミング言語として高い人気を誇るJava。このJavaで書かれたログ出力ライブラリ「Apache Log4j」に、脆弱性が潜んでいたのだ。この脆弱性を突けば、攻撃者は簡単にサーバで任意のプログラムを実行させることができる。この脆弱性を含んだLog4jのバージョンを自社のサービスの一部として利用している事をAWS、Salesforce、VMware、RedHatといった企業が公表したことから、それらのサービスを利用する業務システムや企業ホームページ、ECサイトのほとんどが対象となり得る。

幸いクラウド型WAFは脆弱性の発表から1日とおかず対応を完了していたため、クラウド型WAFを導入していたサイト・サービスでは、何の心配もなく守られている状態になっていた。しかし、導入していなかったサイトは慌てて対応に迫られる事態になった。

Log4j脆弱性のような脆弱性の発見は実は過去にも度々発生している。同じApache財団のStrutsやStruts2脆弱性、OpenSSLに含まれていたHeartBleed脆弱性、Linux/Unixのbashに含まれたShellshock脆弱性と数年に一度の頻度でウェブアプリケーションのセキュリティを揺るがす脆弱性の発見がある。

これらの脆弱性の新たな発見は事前に対処しようがないと思われるかもしれない。しかし、そこで慌てなくて良いように、クラウド型 WAFを入れることで緊急対応は専門家に任せるというのはどうだろう？　クラウド型 WAF を活用した NTT データ九州の取り組みは、効率的かつ効果的なWeb セキュリティ対策を進める上で大いに参考になるはずだ。