2020 年 7 月 28 日

サービス＆セキュリティ株式会社 e-Gate センター

急増する Web サイトの改ざん ～攻撃手法と効果的な対策方法～

1. 概要

私たちが必要とする情報の多くが Web サイトを通じて届けられます。本年 4 月に大手音楽事業会社の Web サイトが攻撃を受け、サイトの一時閉鎖を余儀なくされました。今月には、Web サイトを狙った攻撃により最大 3 万件の個人情報が流失していたにも関わらず 1 か月以上周知しなかったとして人材派遣企業の対応に批判が集まっています。

最近ますます増加する Web サイトへの攻撃にフォーカスして攻撃と対策の全容を紹介します。

Web サイトが悪意ある攻撃者によって改ざんされ、マルウェア（コンピュータウィルスやランサムウェア、スパイウェアなど）感染被害や、大規模な情報漏洩事故になる可能性があり、軽視できません。

セキュリティ事故を引き起こすと会社の信用やイメージの低下は免れることができません。企業として適切なセキュリティ対策を講じることは会社のイメージアップや顧客の満足度にも繋がる重要な要素です。本ニュースを皆様のセキュリティ対策にご活用ください。

2. Web サイトに対する攻撃

2-1.攻撃の実態

昨年発行された Positive Technologies のレポートによると、侵入テストを受けた 92%の企業が外部から侵入が可能な状態で、うち 75%の企業は Web アプリケーションの防御対策が不十分なことによるものでした。

同じく昨年発行された acunetix のレポートによると、35%以上の Web サイトおよび Web アプリケーションに少なくとも 1 つ以上の「重大度の高い脆弱性」があるとされています。

実際に、国内でも 2019 年 1 月 1 日から 2020 年 3 月 31 日までの JPCERT/CC インシデント報告対応レポートによると（表 1 同レポートを加工）、報告された件数だけで 2019 年の 1 年間に 1,000 件を超える Web サイト改ざんによる被害が発生し、2020 年に入ってからの 3 ヶ月の間に 200 件に迫る攻撃が行われていることがわかります。

表 1 Web サイト改ざんインシデント報告件数

日付		件数
2019 年		1,013
	1 月～3 月	229
	4 月～6 月	256
	7 月～9 月	236
	10 月～12 月	292
2020 年		192
	1 月～3 月	192
合計		**1,205**

改ざんの攻撃の対象となった Web サイトは、鉄道会社・バス会社や家電量販店通販サイト、動画配信サービスサイト、県警サイト、大学サイト、観光協会サイトなど、業界を問いません。Web サイトを設置するあらゆる組織・企業が攻撃を受け

る可能性があります。

2-2. 攻撃の手法

Web サイトの主な改ざん手法として以下の 4 点があります。

（１）Web アプリケーションの脆弱性を突く（脆弱性攻撃による改ざん）
組織外部の攻撃者が独自に開発された Web アプリケーションの脆弱性を突きます。
（２）ソフトウェアの脆弱性を突く（脆弱性攻撃による改ざん）
組織外部の攻撃者が Web サイトの使用しているソフトウェアの脆弱性を突きます。
（３）窃取したアカウント情報を悪用した不正ログイン（管理用アカウントの乗っ取りによる改ざん）
組織外部の攻撃者がウェブサイト管理用パソコンから、アカウント情報を窃取し、Web サイトに不正ログインします。
（４）組織内のアクセス制御の不備を突く（管理用アカウントの乗っ取りによる改ざん）
組織内部の管理者権限を持たない攻撃者（内部犯行）がアクセス制御不備を突きます。

3. 対策

今回は 2-2（１）Web アプリケーションの脆弱性を突く手法に対する対策の一例を紹介します。（１）において悪用される Web サイトの脆弱性は以下のとおりです。

・入出力処理に関する脆弱性
・認証に関する脆弱性
・認可に関する脆弱性
・セッション管理に関する脆弱性
・Web サーバ設定に関する脆弱性
・クライアントサイド技術に関する脆弱性
・一般的な脆弱性
・アプリケーション使用や設計に起因する脆弱性

脆弱性への対応については、OS やソフトウェアの場合、各ベンダからの情報を元に、脆弱性修正パッチの適用や安全な設定等、対応を実施することができます。しかし、Web アプリケーションについては、独自に開発される場合が多く、セキュリティ対策は個別に行う必要があり、また早急な対応ができません。開発段階でセキュアな実装を行うことが望まれますが、攻撃の手口はより複雑に、より巧妙になっています。

3-1. ネットワークセキュリティ製品による防御

全体的な攻撃に対して Firewall（ファイアウォール）や IPS/IDS（Intrusion prevention systems:侵入検知システム/Intrusion detection system:侵入防御システム）といったセキュリティ機器を設置することで、攻撃によるセキュリティ事故の発生を低減、セキュリティ事故が起きた際の被害の抑制ができます。

しかし、Web アプリケーションの脆弱性を狙った攻撃に対しては、Web アプリケーションの防御に特化した WAF（Web Application Firewall）の導入が有効な対策の一つです。

標準の Firewall は、特定の通信を通過するようにプログラムできますが、通信内容を解析・検査しないため、80/443 番ポートへの通信など、正常な通信に偽装した攻撃に対処できません。

IPS/IDS は、ネットワークまたはシステムの動きを監視し、悪意のある動きやポリシー違反をシステム管理者に報告しますが、Web アプリケーションに対する攻撃を検知ようには設計されていません。

WAF は、Web アプリケーションとインターネット間の HTTP 通信をフィルタリングおよび監視し、Web アプリケーションを保護するセキュリティ対策製品です。

特に、次のような脅威から Web アプリケーションを保護します。

・クロスサイトリクエストフォージェリ（CSRF）
・クロスサイトスクリプティング（XSS）
・ローカルファイルインクルード（RFI）
・SQL インジェクション
・異常を含めたゼロデイ攻撃防止　など

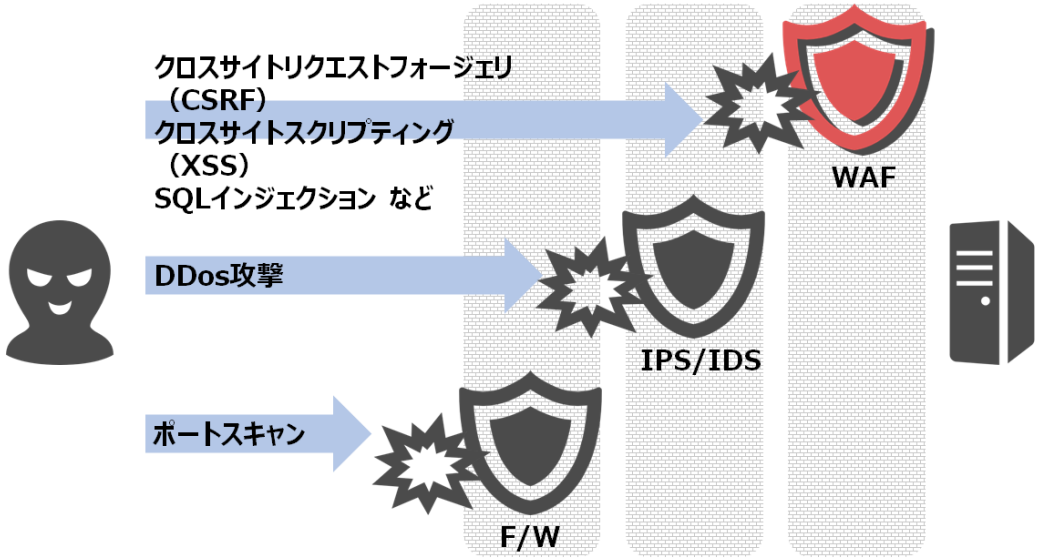

図1　各セキュリティ対策機器の攻撃防御イメージ

弊社で監視している WAF での通信検知数は図 2 のとおり増加傾向にあります（グラフ縦軸は 2019.11 分の検知数を 1 とした比率で表記）。既に WAF による Web アプリケーション保護の必要性は高まっています。

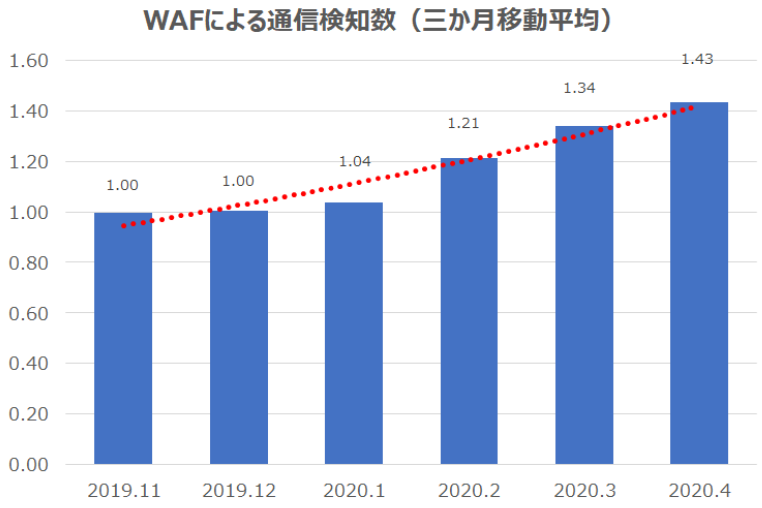

図2　増加傾向にあるWAFの通信検知数

一つ一つの機器は、単体であらゆる攻撃を防御するようには設計されていません。それぞれの製品は多層防御により、セキュリティレベルを高め、攻撃によるセキュリティ事故の発生を低減させます。WAF は Web アプリケーションを攻撃者から守るための要です。

また、様々な機器が生成する大量のログを一元的に集中管理することが、セキュリティ事件の早期検知を可能にし、被害の抑制につながります。専門のアナリストがログを 24 時間 365 日監視・分析するサービス、リモートから手動で多様な攻撃パターンを送信し、WAF によるブロック設定是非を確認するサービスがあります。

3-2. Web アプリケーション診断による予防

脆弱性については、脆弱性診断により Web アプリケーションを対象にセキュリティ診断を実行して、現在のセキュリティレベルを把握し、発見された脆弱性の技術的な対策を実施することで、より信頼性の高い安全なシステムを構築し、サービスの安定性を確保するために行います。

診断は次のような項目で行われます。

- ・SQL インジェクション
- ・クロスサイトスクリプティング（XSS）
- ・クロスサイトリクエストフォージェリ（CSRF）
- ・OS コマンドインジェクション
- ・ディレクトリリスティング
- ・メールヘッダインジェクション
- ・パス名のパラメータの未チェック/ディレクトリトラバーサル
- ・意図しないリダイレクト
- ・HTTP ヘッダインジェクション
- ・認証とセッション管理の不備
- ・認可制御の不備、欠落
- ・クローラへの耐性

診断サービスは図３の流れで行われ、単なる診断だけでなく結果をもとにした脆弱性の修正のアドバイスも行われます。

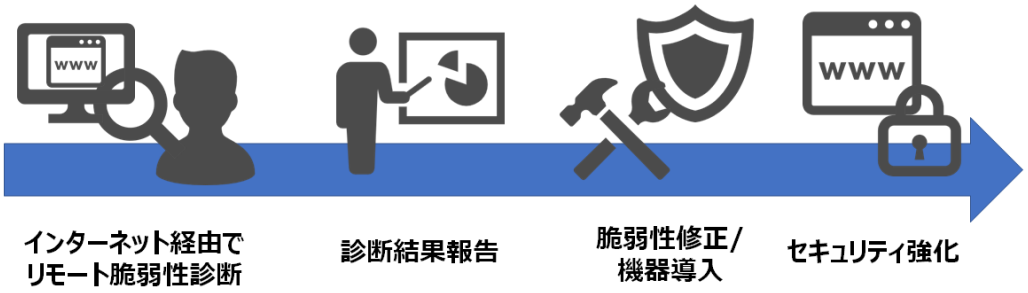

図3　脆弱性診断の流れ

発見された脆弱性が修正されていることを再診断するサービスもあります。攻撃によるセキュリティ事故の発生を低減させることで、被害の抑制につながります。

4. 参考情報

Positive Technologies

・Penetration testing of corporation information systems: statistics and findings 2019

https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Corp-Vulnerabilities-2019-eng.pdf

acunetix

・acunetix Web application vulnerability report 2019

https://cdn2.hubspot.net/hubfs/4595665/Acunetix_web_application_vulnerability_report_2019.pdf

JPCERT

・JPCERT/CC インシデント報告対応レポート

https://www.jpcert.or.jp/ir/report.html

IPA（独立行政法人 情報処理推進機構）

・ウェブサイト改ざんの脅威と対策 ～企業の信頼を守るために求められること～

https://www.ipa.go.jp/files/000041364.pdf

・「安全なウェブサイトの作り方」別冊 ウェブ健康診断仕様

https://www.ipa.go.jp/files/000017319.pdf

5. e-Gate の監視サービスと脆弱性診断について

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。e-Gate のセキュリティ監視サービスをご活用いただきますと、迅速なセキュリティインシデント対応が可能となります。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、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。Web サイトが危険な状態で放置されていないか監視する、Web 改ざん監視サービスも併せてご提案させていただくことができます。

監視サービスや脆弱性診断サービス等をご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を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/

※本資料には弊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。

«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