SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

脆弱性のテスト環境を併用利用した攻撃検知・防御支援システム
Web Attack Detection and Prevention System in Conjunction with Vulnerable Testing Environment

張 邯尹 * Hanyin Zhang
中川 佑人 * Yuto Nakagawa
花田 真樹 † Masaki Hanada
村上 洋一 † Yoichi Murakami
早稲田 篤志 † Atsushi Waseda
石田 裕貴 ‡ Yuki Ishida
三村 隆夫 ‡ Takao Mimura
布広 永示 † Eiji Nunohiro

キーワード WAF,

1 あらまし

スマートフォンやタブレット端末などの普及に伴い，EC や SNS などの様々な分野で多くの Web サービスが利用されている．Web サービスの利用者が増える一方で，Web サイトの脆弱性を狙った攻撃も増え続けており，その対策が急務となっている．Web サイトの脆弱性を狙った攻撃の対策として，WAF（Web Application Firewall）が開発され，運用されている．WAF は Web サイトへの HTTP/HTTPS 通信を検査し，あらかじめ定義された検知ルールによるマッチングにより攻撃を識別し，遮断する．しかしながら，WAF による誤検知が発生した場合，サービスに大きな影響を及ぼす可能性があるため，攻撃防止のための対応と攻撃によるサービスへの影響の把握が必要となる．

そこで本研究では，本番の Web サイトとは別に設置した脆弱性を含むテスト環境において攻撃を検知した場合，予想されるサービスへの影響を Web サイト管理者に通知するとともに，WAF の検知ルールを更新することにより攻撃を防止するシステムを提案する．

提案システムでは，まず利用者と本番の Web サイトの間に WAF を導入する．また，本番の Web サイトとは別に，脆弱性を含むテスト環境を併用して設置し，本番の Web サイトへの HTTP/HTTPS 通信をテスト環境にも転送する．テスト環境において通信やシステムへの影響を定期的に分析し，その分析結果から攻撃と判断した場合は，予想されるサービスへの影響を Web サイト管理者に通知するとともに，WAF の検知ルールを自動生成し，（Web サイト管理者の判断を基に）WAF を更新することにより攻撃を防止する．

WAF の検知ルールのチューニングに関する研究として，WAF のログを機械学習を用いて分析し，検知ルールの修正案を Web サイト管理者に提示するものがある [1]．先行研究 [1] では，WAF の運用中の検知ルールの更新を想定していない．また，誤検知の通信ログを機械学習を用いて分析しているために，本番の Web サイトにおけるサービスへの影響を予測することができない．

上述の課題に対し，本研究では，併用して設置した脆弱性を含むテスト環境を用いることにより，本番の Web サイトにもどのような影響が考えられるかを予想することが可能となる．加えて，その予想されるサービスへの影響とそれに関連付けられる自動生成した WAF の検知ルールを用いて，（Web サイト管理者の判断を基に）WAF を更新することにより攻撃を防止する可能となる．

参考文献

[1] 工藤千寛 他，”機械学習によるログ解析を利用した WAF Mod Security 用チューニングツールの開発,” 情報処理学会 火の国情報シンポジウム 2021，A4-4，2021 年 3 月．

* 東京情報大学大学院 総合情報学研究科 Tokyo University of Information Sciences, Graduate School of Infomatics 4-1 Onaridai, Wakaba-ku, Chiba-shi, Chiba 265-8501, Japan.
† 東京情報大学大学院 総合情報学部．Tokyo University of Information Sciences, Department of Infomatics 4-1 Onaridai, Wakaba-ku, Chiba-shi, Chiba 265-8501, Japan.
‡ 株式会社セキュアブレイン SecureBrain Corporation 3-12 Kioicho, Chiyoda-ku, Tokyo, 102-0094, Japan.