# URL 情報分析に基づくフィッシング対策方式の検討

A proposal of phishing countermeasures based on URL information analysis

松ヶ谷新吾

Shingo Matsugaya

概 要

フィッシングは既に多方面からの対策が実施されているが，国内外で未だに多くの被害が発生している．原因を調査するため，フィッシング URL 情報を分析したところ，McGrath らが 2008 年に行った先行研究の結果と比較してフィッシング URL は以前より正規 URL と判別しにくくユーザが誤認識しやすい傾向にあることが分かった．また，調査の結果，フィッシングページの 65%は正規の Web サイトが改ざんされたものであり，安価なレンタルサーバを利用するライトユーザの Web サイトを悪用している可能性が高いことが分かった．そこで悪用を防ぐためのサーバサイドの対策として，Web サイト運営者が自ら導入できるホワイトリストフィルタ方式を提案した．これは，アクセスを許可する URL を事前にホワイトリストに登録しておき，フィッシング URL および標的ブランド名のブラックリストと組み合わせることで，フィッシングに対する被害を防ぐとともにユーザに対して危険を通知する対策である．実装実験を行って有効性の範囲と導入の容易さを確認した．

## Abstract

Although phishing has been prevented by various countermeasures, there are still many victims both at home and abroad. We analyzed the phishing URL information in order to investigate the cause, and found that the phishing URL becomes difficult to distinguish and tends to be mistaken for legitimate URL, comparing with the previous study results by McGrath et al. in 2008. We also found that 65% of the phishing pages are on falsified websites, and that in many cases phishers exploit the websites of the light users with inexpensive rental servers. So we proposed a server-side countermeasure using whitelist filtering, which can be easily introduced by website operator. By keeping the whitelist in advance to permit URL access and combining with the black list of the brand name of phishing target, the proposed countermeasure informs the risk to the user while preventing damage to the phishing. We experimented the countermeasure and verified its effectiveness and ease of deployment.