5W-04

短縮 URL の安全性判断支援手法の検討

藤根麻羽† 小倉加奈代† ベッドバハドゥールビスタ† 高田豊雄†
岩手県立大学ソフトウェア情報学部†

１．はじめに

近年，Twitter や Facebook を代表とするソーシャルネットワークサービス(SNS)は幅広い年代のユーザに利用されている．SNS の中には冗長性を排除するため，投稿できる文字数に制限が設けられているものがある．文字数制限を解決する方法として，短縮 URL サービスが利用されるようになり，URL の冗長性を排除しつつ長い URL と同じように投稿することができるようになった．短縮 URL サービスの例として，goo.gl[1]や bit.ly[2]がある．URL を短縮するだけでなく，統計や QR コード生成のために利用される．その一方で，短縮 URL サービスを悪用したサイバー犯罪も起こっている[3]．短縮された URL では，リンクが難読化され，ドメイン名で正規サイトかどうかを判断できず，意図しないリダイレクトやフィッシングサイトへの誘導に利用される危険がある．本稿では，短縮 URL に対するユーザのセキュリティ意識向上を目標とした支援手法を検討するために，短縮 URL をクリックする際の安全性を判断するための確認行動やセキュリティ知識，PC やスマートフォンの習熟度レベルとの関連性を調査し，その結果をもとに，短縮 URL に対する安全性判断支援手法を検討する．

２．関連研究

短縮 URL について，AppAppeal による調査[4]では，Goo.gl を利用した短縮 URL サービスで発見された悪意のある URL が，2012 年には 465 万件を超えた．このような悪意のある短縮 URL 対策として，McAfee では macaf.ee ドメインを使用し独自の安全な URL 短縮機能を導入している．短縮 URL に関わらず，Web ブラウザでは怪しい Web サイトへのアクセスをブロックする Google セーフブラウジング[5]などの対策が行われている[4]．

上松ら[6]は，Gumblar と呼ばれる Drive-by-Download 攻撃の一種である攻撃手法に対して，2 つの探査方式により Web サイトの改ざんを検知する方式を提案した．複数の Web サイトからマルウェア配信サイトへのリダイレクトが集中することに着目し，グローバル検査と個々の Web サイトのリダイレクト変更頻度をカウントし，任意の時間間隔で決められた回数以上の変更があれば検知するローカル探査の 2 種類の探索方式を利用する．この研究ではリダイレクトを用いマルウェア配布サイトへ誘導する攻撃手法を対象とした不正 Web サイト検知方式が述べられている．しかし，Web サイト閲覧者自身のクリックによってマルウェア配布サイトに誘導するタイプの攻撃手法が存在する可能性を指摘しており，閲覧者側の対策が議論されている．

３．調査

短縮 URL をクリックする際の安全性を判断するための確認行動とセキュリティ知識，PC やスマートフォン利用の習熟度レベルとの関連性を調べるためにアンケート調査を実施する．

回答者は，著者の所属する学部学生 107 名を対象とし，「URL に対する意識調査」と題したアンケートに回答する．質問項目概要を表 1 に示す．セキュリティの常識を問う設問は，トレンドマイクロ社が提供するクイズ問題[7][8]を利用し，PC 及びスマートフォンの習熟度レベルに関する設問は情報推進機構の情報セキュリティの脅威に対する意識調査の設問を使用した．URL をクリックする際の意識と SNS 上の短縮 URL への注意状況に関する設問は著者らが作成した．URL をクリックする際の意識は，頻度（選択式）とその理由を回答してもらい，SNS 上の短縮 URL への注意状況は，短縮 URL を含む Twitter の投稿を模した例を示し，投稿内容のどのような点に注目するか，短縮 URL をクリックする際に気にすることはあるか，一般的な短縮 URL をクリックする際にためらうことがあるかを回答してもらう．

A study on Methods to Support Safety Management for Short URLs
†Mau Fuzine, Kanayo Ogura, Bhed Bahadur Bista, Toyoo Takata
†Iwate Prefectural University, Faculty of Software and Information Science

表１．アンケート項目内容

分類項目	設問数	解答方法
セキュリティの常識	8	「適切/適切でない」を選択
PC の習熟度レベル	9	「はい/いいえ」を選択
スマートフォンの習熟度レベル	1	4 つの選択肢から１つを選択
URL をクリックする際の意識	2	4 つの選択肢から１つを選択 +その理由
SNS 上の短縮 URL への注意状況	4	選択回答（複数回答可）

４．評価

アンケートの結果，セキュリティの常識を問う設問に対して，107 名のうち全問正解者は約 26.1%(28 名)だった．28 名の回答者は，パソコンやスマートフォンなどの情報端末の違いに関わらず Web サイト閲覧時にクリックする URL を「いつもに気にする」と回答した人が多いことがわかった．また，表 2 のように Web サイト閲覧時に URL を「全く気にしていない（気にせずクリックする）」と回答した人について，PC で Web サイトを閲覧している時については 7 名いたが，スマートフォンを利用時については一人もいなかった．また，「まったく気にしていない」，「どちらかといえば気にしていない」と回答した理由として多かったのは，「普段から URL の安全性について考えたことがなく，危険な URL ではないことを自身で判断している」という回答であった．

表 2：URL を気にするかどうかの回答状況

Webサイトの閲覧時，URLを気にしますか．	PC	スマートフォン
いつも気にしている	22	20
どちらかといえば気にしている	50	47
どちらかといえば気にしていない	28	32
まったく気にしていない(気にせずクリックする)	7	0

５．考察

4 章の結果から，セキュリティ知識レベルが高いと，クリックする URL に対する危険意識も高いことがわかった．また，PC よりもスマートフォンでのクリック操作の方が手軽であるため，スマートフォン利用時の危険意識が低い可能性が考えられる．この点から，安全性を判断する手法として，特にスマートフォン利用時に URL のクリック先の安全性確認支援が必要であるといえる．具体的にはリダイレクト先の URL や投稿者情報を表示することで，安全性判断支援につながると考える．

６．まとめ

本稿では，短縮 URL に対するユーザのセキュリティ意識向上を目標とした支援手法を検討するために，短縮 URL をクリックする際の安全性確認行動やセキュリティ知識，PC やスマートフォンの習熟度との関連性を調査した．その結果，Web 閲覧時の URL クリック行動について，特にスマートフォンについてクリック先の安全性確認に対する支援が必要であることがわかった．以上を踏まえ，今後はスマートフォン上での URL クリック時の注意喚起方法や UI を検討する．

謝辞　本研究は JSPS 科研費 16K01025 の助成をうけたものである．

参考文献

[1] Google:Google URL Shortener,available from<https://goo.gl/>(accessed 2017-01-12)
[2] Bitly:URLShortener and Link Management Platform,available from<https://bitly.com/>(accessed 2017/1/12)
[3] マカフィー株式会社：公式ブログ Twitter で拡散するテロリスト支持者を狙ったスパイウェア，入手先 <http://blogs.mcafee.jp/mcafeeblog/2016/07/twitter-29c3.html>(参照 2017-01-12)
[4] McAfee:Securing Tomorrow.Today.:Short-URL Services May Hide Threats,available from<https://securingtomorrow.mcafee.com/mcafee-labs/short-url-services-may-hide-threats/>(accessed 2017-01-12)
[5] Google：セーフブラウジング-透明性レポート，入手先 <https://www.google.com/transparencyreport/safebrowsing/?hl=ja>(参照 2017-01-12)
[6]上松晴信，名坂康平，酒井崇裕，西垣正勝：相補的な Web 感染型マルウェア検知方式の提案，情報処理学会 CSEC 研究報告，Vol.2011-CSEC-52 No.53，2011.
[7]トレンドマイクロ：セキュリティの常識をクイズでチェック！，入手先 <http://www.is702.jp/special/1902/partner/12_t/>（参照 2016-12-23）
[8]トレンドマイクロ：ネット詐欺の手口と対処法をクイズで確認，入手先 <http://www.is702.jp/special/1725/partner/12_t/>（参照 2016-12-23）
[9]独立行政法人情報処理推進機構：2015 年度情報セキュリティの脅威に対する意識調査，入手先 <https://www.ipa.go.jp/files/000050002.pdf>（参照 2016-12-23）