「マルチメディア，分散，協調とモバイル
(DICOMO2016)シンポジウム」 平成28年7月

Web 翻訳サービスを利用した 不正通信のフィルタリング回避手法と対策

鈴木 亮太† 佐々木 良一†

概要：近年，標的型攻撃の被害が増加しており，その攻撃手法も多様化してきている．標的型攻撃とは，特定の組織を標的として行われるサイバー攻撃であり，攻撃を受ける件数が少なく，攻撃に気付きにくいため，被害が拡大しやすいという特徴がある．このため標的型攻撃対策では，感染の防止だけではなく，感染時の早期発見や被害の軽減などといった，感染を想定した対策が重要である．本研究では，この感染を想定した対策の際に用いられるフィルタリングに関して，Web 翻訳サービスを利用することでフィルタリングを回避可能な攻撃手法を提案し，調査，対策手法の検討を行う．また，短縮 URL サービスや Web アーカイブサービスなどの他のサービスを併用した攻撃手法についても調査を行い，対策手法を検討する．この結果，両方の攻撃に対応可能な技術面，運用面の対策を明確にすることができたので報告する．

Countermeasures against filtering avoidance using Web translation service

RYOTA SUZUKI† RYOICHI SASAKI†

1. はじめに

近年，標的型攻撃の被害が増加しており，その攻撃手法も多様化してきている．標的型攻撃とは，特定の組織を標的として行われるサイバー攻撃であり，攻撃を受ける件数が少なく，攻撃に気付きにくいため，被害が拡大しやすいという特徴がある．

また，標的型攻撃への対策においては，組織の規模が大きければ大きいほど，感染の防止が難しくなり，完全に感染を防ぐことは困難である． [1] 標的型攻撃では，図 1 の通り，マルウェア感染後に攻撃者が指令サーバ(以下 C&C サーバとする)から，組織内のマルウェアを操作することで，感染の拡大や内部情報の窃取を行う．

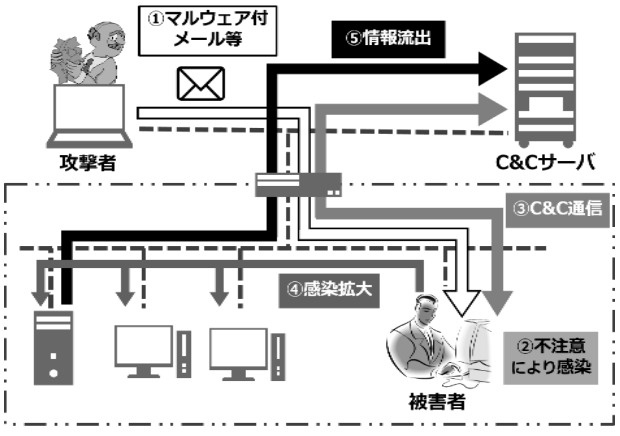

図 1 標的型攻撃

そのため，感染の防止だけではなく，感染時の早期発見や被害の軽減などといった，感染を想定した対策が重要である． [2]

本研究では，この感染を想定した対策の際に用いられるフィルタリングに関して，Web 翻訳サービスを利用することでフィルタリングを回避可能な攻撃手法があることを指摘するとともに種々の翻訳サービス等への実験によって実際に攻撃が可能であることを示す．そして，その攻撃方法に対する対策手法の提案と評価を行う．

Google 翻訳やエキサイト翻訳などの Web 翻訳サービスでは，Web ページの URL を入力することで，入力された Web ページの内容を他言語に翻訳し，Web 翻訳サービス上で対象 Web ページの表示を行う，Web ページ翻訳の機能を提供しているものが多数存在する．

この Web ページ翻訳の機能を利用することで，クライアントから対象 Web ページへ直接通信を行うことなく，Web 翻訳サービスを通じて対象 Web ページの内容を取得することが可能である．

この性質を利用し，図 2 で示す通り，マルウェアから C&C サーバへの通信に Web 翻訳サービスを経由し通信を行うことで，通信先をその翻訳サービスに偽装可能である．これにより，プロキシサーバなどのフィルタリングにより，接続が禁止されている C&C サーバと通信を行うことや，不審な通信の発見を困難にすることが可能である．

†東京電機大学
Tokyo Denki University

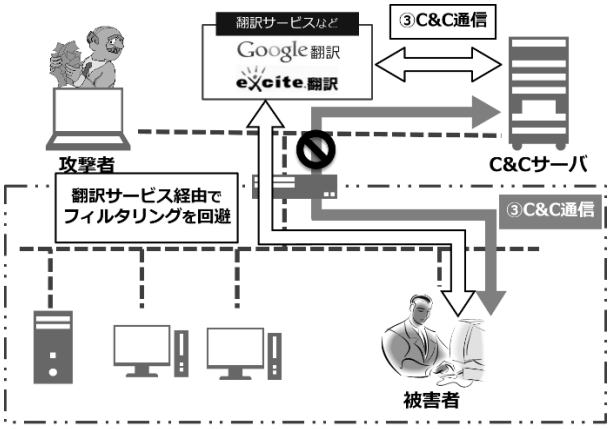

図 2　フィルタリング回避手法

Web 翻訳サービスを経由したフィルタリング回避手法については一部専門家の間では知られていたが実際に可能であるかどうかの検証は行われてはいなかった. そこで, 種々の実験によって実際に可能であることを確認する．また，短縮 URL サービスや Web アーカイブサービスなどの他のサービスを併用した攻撃手法についても実験を行い，攻撃の成功可能性を検証する．併せて，それらの攻撃方法に関する対策手法を検討し，両方の攻撃に対処可能な対策を明確化する．

2. 関連研究

Web 翻訳サービスを攻撃に利用する手法としては，Hoffman らの研究 [3]の Jikto が挙げられる．Jikto では JavaScript による Web スキャンを行う目的で，Google 翻訳が用いられている． Google 翻訳を経由して，スキャン対象のサーバに接続することで，複数のサーバを全て Google 翻訳内のコンテンツとして扱うことで，Web スキャンを実現している．

また，BarracudaLab [4]は，スパムメールの送信者が，スパムフィルタリングに対抗する手法として，Google 翻訳と URL 短縮サービスを組み合わせた手法を編み出したと伝えている．この手法では，メール中の URL フィルタリングが，リンク先のドメインの評価によって行われることを利用している．具体的な処理としては，まず，スパムへのリダイレクトページへの URL を，URL 短縮サービスによって短縮する．この短縮された URL を Google 翻訳の Web ページ翻訳機能で表示し, 生成されたページの URL をメールで送信する．これにより，メールの受信者からは，Google ドメインのリンクが見えることになり，フィルタリングが困難となる．

これらはいずれも Google 翻訳を用いる攻撃に関するものであるが，本研究で扱うような，C&C 通信のフィルタリング回避への対策ではない．

3. 調査

Web 翻訳サービスについて，提案攻撃手法に利用可能であると考えられる，Web ページ翻訳の機能を持ち外部 Web ページが表示可能な翻訳サービスについて調査を行った．

結果, 外部 Web ページを表示可能なサービスは表 1 の通りであることがわかった．

表 1　外部 Web ページを表示可能なサービス

	サービス名
①	Google 翻訳 [5]
②	エキサイト翻訳 [6]
③	Yahoo!翻訳 [7]
④	Infoseek マルチ翻訳 [8]
⑤	So-net 翻訳 [9]
⑥	WorldLingo 無料オンライン翻訳者 [10]
⑦	SDL　FreeTranslation.com [11]

調査の結果，文章の翻訳が可能な Web サービスの多くは，通常の翻訳の機能に加え，外部 Web ページを翻訳し，表示する機能を提供していることがわかった．

さらに, 表 1 の Web 翻訳サービス以外にも Internet Archive Wayback Machine [12]やウェブ魚拓 [13]といった，任意のタイミングで Web ページを保存し, 表示する機能を持ったサービスも存在することがわかった. これらのサービスも，Web 翻訳サービスと同様に攻撃に利用可能であると考えられる．

4. 実験目的

本研究では，提案攻撃手法が標的型攻撃に利用可能であると判断する条件として，3 つの条件を設定し，フィルタリングにより対象サーバへの通信が禁止されている状態で，提案攻撃手法が以下の機能を実現可能であることを確認した．

1. C&C サーバからマルウェアへの命令の送信
2. C&C サーバからマルウェアへのファイルの送信
3. マルウェアから C&C サーバへの応答の送信

実験環境は以下の通りである．

・OS　Windows 10 Education
・プロキシサーバ Squid 3.5
・Web ブラウザ Mozilla Fire Fox
・実験用プログラム Java

なお, キャッシュによる Web ページの表示を防止するため，プロキシサーバ，Web ブラウザのキャッシュ機能を使用しない設定を行い実験した．

実験に使用するフィルタリング形式は以下の通りである．

表 2　実験に使用するフィルタリング形式

IP アドレス フィルタリング	特定の IP アドレスのホスト に対する通信を遮断
ドメイン フィルタリング	特定のドメイン名のホスト に対する通信を遮断
URL フィルタリング	URL 中に，検知対象の文字列が 含まれている場合，通信を遮断 (検知対象の文字列は，対象ホストの IP アドレス及びドメイン名を指定)

5. フィルタリング回避の実験結果

5.1 命令送信手法

一つ目の条件である，C&C サーバからマルウェアへの命令の送信が，フィルタリングが行われている環境下で可能であるか否かを確認した．命令の送信手法については，Web サーバ上のページに書き込み，マルウェアが翻訳サービス経由で接続することで受信する形とする．

実験では Web ブラウザから，通常の接続及び翻訳サービスを経由した接続を行い，結果を比較，翻訳サービスを経由することでフィルタリングを回避し，サーバからの情報が取得可能であることを確認した．

表 3　各サービスのフィルタリング回避結果

通信方法	IPアドレス	ドメイン	URL
通常の接続	×	×	×
Google 翻訳	○	○	○
エキサイト翻訳	○	○	×
Yahoo!翻訳	○	○	×
Infoseek マルチ翻訳	○	○	×
So-net 翻訳	○	○	×
WorldLingo	○	○	×
SDL	○	○	○
Internet Archive	○	○	○
Web 魚拓	○	○	×

○が情報の取得成功，×がプロキシサーバによる遮断

実験の結果，通常の接続の場合全てのフィルタリング形式で通信が検知，遮断されており，フィルタリングは正常に機能していると考えられる．

次に，全ての Web 翻訳サービスを利用した場合で，IP アドレス及びドメインによるフィルタリングを回避し，C&C サーバからの情報の送信に成功していることがわかる．しかし，多くの Web 翻訳サービスでは，URL フィルタリングが行われている場合は，プロキシサーバによるフィルタリングが機能し，C&C サーバからの情報の送信が防がれている．

これは，表 4 の下線部の通り，Web 翻訳サービスでは，翻訳対象の Web ページの URL を GET パラメータに格納して送信しており，URL 中に C&C サーバのドメイン名が含まれるためである．他の翻訳サービスについても，翻訳対象の Web ページの URL は GET メソッドにより送信されており，URL フィルタリングは翻訳サービスを利用したフィルタリング回避手法に対する有効な対策手法であると考えられる．

表 4　Web 翻訳サービスと翻訳時の URL

翻訳サービス	翻訳時の URL
エキサイト翻訳	http://www.excite-webtl.jp/world/english/web/?wb_url=http%3A%2F%2Fweb.dendai.ac.jp%2F&wb_lp=JAEN
Google 翻訳	https://translate.google.co.jp/translate?hl=ja&sl=auto&tl=en&u=http%3A%2F%2Fweb.dendai.ac.jp%2F

しかし，Google 翻訳や SDL，Internet Archive を経由した通信の場合，URL フィルタリングが行われている場合にも，フィルタリングを回避し，C&C サーバからの情報の送信に成功していることがわかる．

Google 翻訳や SDL を利用した場合でも，表 4 の通り，翻訳対象の URL は GET メソッドにより送信されており，URL 中に C&C サーバの URL は含まれる．

しかし，Google 翻訳及び SDL はクライアントとの通信の際，https 通信による暗号化通信を行っているため，GET パラメータは暗号化されて送信されており，プロキシサーバからは GET パラメータの内容が確認できず [14]，フィルタリングに失敗したと考えられる．

5.2 ファイル送信手法

二つ目の条件である，C&C サーバからのファイルの送信について，フィルタリングが行われている環境下で送信が可能であるか否かを確認した．

マルウェアによる Web 翻訳サービスを経由したファイルの受信手法として，以下の 2 つの手法が考えられる．

1. Web 翻訳サービスに対し，直接ファイルの URL を指定し，ファイルをダウンロード
2. ファイルへのリンクを含んだページを，Web ページ翻訳により取得し，ページ上のリンクからファイルをダウンロード

上記の 2 つの手法により，翻訳サービスを経由すること

で，接続が禁止されているサーバから，ファイルのダウンロードが可能であるかを実験により確認した．

結果，全てのフィルタリング形式に対する，全ての翻訳サービスについて，1，2 どちらの手法を用いた場合でもファイルの保存に失敗した．

1. の手法が失敗した理由としては, 翻訳対象の URL に，html や php といったテキストデータの URL ではない，jpg や exe といった翻訳が不可能なファイル形式の URL を指定した場合はエラーが返されるため，直接のダウンロードは不可能である．

2．の手法が失敗した理由としては，Web 翻訳サービスでは, 翻訳対象のテキストデータである html や php のページは翻訳のため，Web 翻訳サービスから転送されるが，jpg や exe といった翻訳を行わないファイルに関しては，翻訳元のサーバに存在するファイルに直接リンクが貼られており，このリンクを使用した場合，Web 翻訳サービスを経由しない通常の通信となってしまう為である．

1.2.の結果から，Web 翻訳サービスを経由して送信可能なファイルは，図 3 のように，翻訳対象のテキストデータのみであることがわかった．

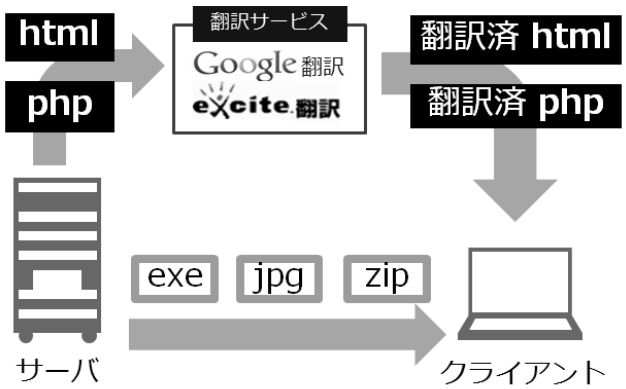

図 3　送信可能なファイル形式

この結果から，ファイルを html などの中に埋め込み，テキストデータとして，Web 翻訳サービスを経由させることで，ファイルの送信が可能であると考えられる．

このような，html 中に他のファイルを埋め込む手法として，画像を Base64 でエンコードし，タグとして html ファイルに埋め込む手法が存在する. この Base64 エンコードで html 内に埋め込んだ画像ファイルが，Web 翻訳サービスを経由することで，フィルタリングを回避し，ダウンロードが可能であることを実験により確認した．

実験では，フィルタリングが行われている状態で，ブラウザ及び作成した保存用プログラムにより，Web 翻訳サービスを経由したダウンロードを行った．

結果，ブラウザでの画像ファイルの表示，プログラムでのダウンロード共に，以下の結果となった．

表 5　各サービスのフィルタリング結果

サービス名	IP アドレス	ドメイン	URL
Google	○	○	○
SDL	○	○	○
その他の翻訳サービス	○	○	×
Internet Archive	○	○	○
Web 魚拓	○	○	×

○が情報の取得成功，×がプロキシサーバによる遮断

暗号化通信を用いていないサービスは，5.1 節の結果から URL フィルタリングにより遮断されることが明らかなため, この結果から, ファイルを html 内に埋め込むことで, Web 翻訳サービスを経由した，フィルタリングを回避してのダウンロードが可能であることがわかった．

同様の手法を用いることで，攻撃用ソフトウェアを html ファイル内に埋め込み, マルウェアにより保存することで, C&C サーバからの攻撃ファイルの送信が可能であると考えられる．

また，Internet Archive はファイルのアーカイブも行っている性質上, ファイルがアーカイブさえされていれば, URL の直接指定, リンクどちらの手法でも保存に成功した. Web 魚拓はファイルのアーカイブは行わないため，Web 翻訳サービスと同様，保存に失敗した．

これは，Internet Archive では，html や php といったファイル形式に囚われず，jpg や exe などのファイルも，アーカイブのサーバ上に記録が可能なためである．このため，攻撃用ソフトウェアの送信の際には，これらの Web アーカイブサービスを利用することで，フィルタリングが行われている環境下でのファイル送信を実現することも可能である．

5.3 応答手法

三つ目の条件である，マルウェアから C&C サーバへの応答について，実験により確認した．標的型攻撃を行う場合, C&C サーバからの命令や攻撃用ソフトウェアの受信だけでなく，マルウェアから C&C サーバに対して，攻撃の結果などの情報を応答する必要がある．この応答が，Web 翻訳サービス経由下で可能であることを確認した．

なお，Web アーカイブサービスは，クライアントからのアクセスによる，アーカイブ元ページへのアクセスは発生しないため，応答への利用は不可能であると判断し，除外する．

実験では, Web サーバ上に GET メソッド及び POST メソッドによる書き込みが可能なページを設置し，この Web サーバのドメインをフィルタリングの対象とした．対象のページに対し, 作成したプログラムから Web 翻訳サービス経由で書き込みのリクエストを送信し，データが書き込まれ

るかを調査した． フィルタリング形式は，5.1 節の結果から, 暗号化通信を用いる翻訳サービスに対しては URL フィルタリング，暗号化通信を用いない翻訳サービスに対してはドメインによるフィルタリングを用いた．

実験の結果，全ての翻訳サービスにおいて，GET メソッドを使用して送信した場合は書き込みに成功した. 対して，POST メソッドを使用した場合，データの書き込みに失敗した．

図 2　応答に利用可能なメソッド

これは，図 4 の通り，GET メソッドではデータが URL 中の http リクエスト部に含まれ, URL として翻訳元のサーバまで到達するのに対し, POST メソッドではデータが http ヘッダやボディ部に含まれ，URL 中には存在せず，翻訳サービスに送られた時点で情報が失われてしまうためだと考えられる．

この結果から，マルウェアから C&C サーバへの応答では，GET メソッドを用いてデータを送信することで，実現可能であるということがわかった．ただし，GET メソッドでは，送信可能なデータ量に制限があり，応答の内容が URL のログとしてプロキシサーバに記録されるといった，攻撃者にとっては不利な要素も見られる．

5.4 結果

5.1 節～5.3 節の実験の結果から，Web 翻訳サービス経由での，命令の受信，ファイルの受信，C&C サーバへの応答の全てが可能であることがわかった．この結果から，Web 翻訳サービスを用いたフィルタリング回避手法を標的型攻撃の際の通信に用いることは可能であると考えられる．

また，全ての Web 翻訳サービスにおいて，翻訳対象の Web ページの URL を GET パラメータにより送信しているため，URL フィルタリングでの検知，遮断が可能である．ただし，Google 翻訳や SDL，Internet Archive などの暗号化通信を用いる Web 翻訳サービスでは, GET パラメータなどの内容が暗号化されて送信されるため，URL フィルタリングに加え，フィルタリング前に暗号化データを復号するなどの対策が必要となる．

6. 短縮 URL サービスを併用した回避手法

6.1 目的

関連研究で述べている通り，Web 翻訳サービスによるフィルタリング回避の際, 短縮 URL サービスを併用する手法が有効である．短縮 URL サービスとは，URL を指定することで, 対応した短い URL を生成するサービスである．短縮された URL にアクセスがあった場合, リダイレクトにより短縮前の URL の Web ページへ移動する．

この短縮 URL サービスにより, C&C サーバの URL を短縮し，短縮された URL に Web 翻訳サービスからアクセスすることで，フィルタリングの回避を行う．この短縮 URL サービスを併用したフィルタリング回避手法について，5 章と同様に標的型攻撃に利用可能であるか，実験を行い調査した．短縮 URL サービスは bit.ly [15]を用いた．

6.2 命令送信手法

URL 短縮サービスを併用した場合での，フィルタリングが行われている環境下での命令の送信が可能であることを確認した．

実験では, フィルタリング対象のページの短縮 URL を作成し, Web ブラウザから Web 翻訳サービス経由で短縮 URL に対してアクセス，フィルタリングの回避が可能であることを確認した．

表 6　各サービスのフィルタリング回避結果

通信方法	IP アドレス	ドメイン	URL
通常の接続	×	×	×
Google 翻訳	○	○	○
エキサイト翻訳	○	○	○
Yahoo!翻訳	○	○	○
Infoseek マルチ翻訳	○	○	○
So-net 翻訳	○	○	○
WorldLingo	○	○	×
SDL	○	○	○

○が情報の取得成功，×がプロキシサーバによる遮断

この結果を, 短縮 URL サービスを併用しない場合の結果と比較すると，暗号化を行わないサービスの場合でも，短縮 URL サービスを利用することで URL フィルタリングを回避可能であることが分かる．

これは, 短縮 URL の形で Web 翻訳サービスに URL を送信することで検知対象のドメインを隠し，検知を防いだためであると考えられる．ただし，WorldLingo を用いた場合はフィルタリング回避に失敗している．

これらの結果から，Web 翻訳サービスを併用することで暗号化を用いない Web 翻訳サービスを利用した場合にも，URL フィルタリングを回避可能であることがわかった．

6.3 ファイル送信手法

URL 短縮サービスを併用し，フィルタリングが行われている環境下でファイルの送信が可能であることを確認した．

5.2 節の実験と同様，直接ファイルの URL を指定する手法, リンクからのダウンロードを行う手法, ファイルを html に埋め込み送信する手法の三つについて実験した．

結果，Web 翻訳サービスのみでの実験と同様，ファイルを埋め込む手法の場合でのみファイルの送信に成功した．また，6.2 節同様，暗号化を行わない Web 翻訳サービスを利用した場合でもフィルタリング回避に成功した．

6.4 応答手法

URL 短縮サービスを併用し，フィルタリングが行われている環境下での C&C サーバへの応答が可能であることを確認した．

5.3 節の結果から C&C サーバへの応答では，GET パラメータを付加した URL を Web 翻訳サービス経由で送信することが必要となる．このため，短縮 URL サービスを用いて応答を送信する場合, 応答を行う度に GET パラメータを付与した URL を URL 短縮サービスに送信し，短縮を行った後に Web 翻訳サービスへの送信を行う必要がある．

この手法により， 実験を行った結果，WorldLingo を除く全ての翻訳サービスで C&C サーバへの応答に成功した．WorldLingo で失敗した理由については，6.2 節の結果の通り短縮 URL サービスを用いた場合にもフィルタリングが可能であるためだと考えられる．

6.5 結果

6.2 節～6.4 節の実験の結果から，Web 翻訳サービスと短縮 URL サービスを併用した手法での，命令の送信，ファイルの送信, C&C サーバへの応答が可能であることがわかった．この結果から，短縮 URL サービスを併用した手法についても，標的型攻撃の通信に用いることができると考えられる．

短縮 URL サービスを併用したフィルタリング回避手法を用いた場合，Web 翻訳サービスのみを利用した手法の場合は有効な対策であった URL フィルタリングを回避し, 通信を行うことが可能である．ただし，短縮 URL サービスを併用した手法では，C&C サーバへの応答を行う度に URL の短縮が必要となるといった欠点も存在することがわかった．

7. 対策手法

5 章の結果から，暗号化通信を用いない Web 翻訳サービスを利用した回避手法に対しては，URL フィルタリングが有効であることがわかった．Google 翻訳や SDL などの，暗号化通信を用いる翻訳サービスに対しては，プロキシサーバによる復号処理などによる暗号化通信対策を行った上での URL フィルタリングが必要となる．

暗号化通信の対策としては，プロキシサーバの証明書を端末に保存し, この証明書を用いて暗号化通信を複合する，https デコード機能 [16]と呼ばれる機能を持つフィルタリングソフト [17] [18]が必要となる．

Web アーカイブサービスについても，暗号化通信への対策と URL フィルタリングを併用することで対策可能である．

短縮 URL を併用したフィルタリング回避手法に対しては，6 章の結果から URL フィルタリングでは対策できないことがわかっている．ただし，短縮 URL を生成する際の短縮 URL サービスに対する元 URL の送信や, 短縮 URL を生成した際の応答時に, 短縮前 URL が含まれる通信が行われていることから，短縮 URL を利用する手法については，コンテンツフィルタリングを行うことで対策可能である．なおコンテンツフィルタリングを行う場合, 短縮 URL サービスには暗号化通信を行うサービスも多数存在するため，暗号化通信対策は必要である．

また，技術的な対策ではなく，運用面での対策として，翻訳サービスや短縮 URL サービスに対する通信そのものを禁止してしまうという対策も考えられる．これらの対策は，フィルタリングの設定のみで実現可能という利点はあるが，利用者に対する利便性の負担がかかる．

これらの対策を表 7 に示す．

表 7　対策手法と対策可能範囲

対策	Web 翻訳	暗号化通信	短縮 URL
①URL フィルタ	○	×	×
②暗号化対策＋URL フィルタ	○	○	×
③暗号化対策＋コンテンツフィルタリング	○	○	○
④短縮 URL サービスへの通信禁止	×	×	○
⑤暗号化利用 Web 翻訳サービスへの通信禁止	×	○	×
⑥Web 翻訳サービスへの通信禁止	○	○	○

表中の対策①②③は技術的な対策であり，③を採用すれば問題の解決が図れることがわかる．しかし，下に行くほ

ど高機能なフィルタリングソフトが必要であり，費用や処理速度の負担が増加する．

表中の対策④⑤⑥は運用面での対策であり，下に行くほど利便性面での負担が増大する．

これらの対策を組織の環境に合わせて組み合わせて行うことで，Web 翻訳サービスによるフィルタリングを利用した攻撃手法の対策を行うことが可能である．

8. おわりに

本研究では，標的型攻撃における C&C サーバとの通信の際，Web 翻訳サービスを利用することで，フィルタリングを回避し，攻撃の遂行が可能であることを示した．また，短縮 URL サービスを併用した手法についても同様に攻撃に利用可能であることを示した．

対策としては，暗号化通信を用いない Web 翻訳サービスに対しては URL フィルタリングが有効であること，暗号化通信を用いる Web 翻訳サービスに対しては暗号化通信の対策を行った上でのフィルタリングが必要であることを述べた．短縮 URL サービスを併用した手法の対策としては，コンテンツフィルタリングが有効であることを確認した．さらに，運用面の対策としてこれらのフィルタリング回避に利用可能なサービスそのものへの通信を禁止する対策があることを示した．

今後は，これらの対策の対策費用や処理速度，利便性への負担を考慮し，組織ごとに最適な対策を提案可能な手法を検討していきたいと考えている．

9. 引用文献

[1] 佐々木良一，上原哲太郎，& 松本隆. (2013). 標的型攻撃に対するネットワークフォレンジック対策の現状と今後の展望. コンピュータセキュリティシンポジウム 2013 論文集, 2013(4), 155-162.

[2] 山田正弘，森永正信，海野由紀，鳥居悟，& 武仲正彦. (2013). 組織内ネットワークにおける標的型攻撃の検知方式. 情報処理学会研究報告, 1-6.

[3] Hoffman, B. (2008). JavaScript Malware for a Gray Goo Tomorrow.

[4] “Spammers disguise links using Google translate “, https://barracudalabs.com/2013/03/spammers-disguise-links-using-google-translate/, (参照 2015-11).

[5] “Google 翻訳 “, https://translate.google.co.jp/, (参照 2016-04).

[6] “エキサイト 翻訳 - Excite“, http://www.excite.co.jp/world/, (参照 2016-04).

[7] “Yahoo!翻訳“, http://honyaku.yahoo.co.jp/, (参照 2015-11).

[8] “Infoseek マルチ翻訳“, http://translation.infoseek.ne.jp/web.html, (参照 2015-11).

[9] “翻訳 | So-net“, http://www.so-net.ne.jp/translation/, (参照 2015-11).

[10] “無料オンライン翻訳者 - WorldLingo“, http://www.worldlingo.com/ja/products_services/worldlingo_translator.html, (参照 2015-11).

[11] “SDL FreeTranslation“, https://www.freetranslation.com/ja/, (参照 2015-11).

[12] “Internet Archive: Digital Library of Free Books, Movies, Music & Wayback Machine“, https://archive.org/index.php, (参照 2015-11).

[13] “ウェブ魚拓“,http://megalodon.jp/, (参照 2015-11).

[14] D. G. J. D. Shorter, “Effectiveness of Internet Content Filtering.,” Journal of Information Technology Impact.

[15] “Bitly | URL Shortener and Link Management Platform“,https://bitly.com/, (参照 2015-11).

[16] E. Akbaş, “Next generation filtering: Offline filtering enhanced proxy architecture for web content filtering.,” ICIS 2016, 2008.

[17] “有償オプション製品「i-FILTER SSL Adapter」｜旧バージョンの製品情報｜i-FILTER“, http://www.daj.jp/bs/i-filter/old/option_relation_ssl_adapter, (参照 2015-11).

[18] “SSL 暗号化通信の中身を見る！“Counter SSL Proxy ““,http://www.swatbrains.co.jp/csp.html, (参照 2015-11).