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その対策

鈴木 亮太† 佐々木 良一†

†東京電機大学
〒120-8551 東京都足立区千住旭町5
suzuki@isl.im.dendai.ac.jp, sasaki@im.dendai.ac.jp

あらまし 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．標的型攻撃では，感染を防止するだけではなく，感染時の早期発見や被害の軽減などの出口対策が重要であり，感染後の不審な挙動や不正通信の検知を行う必要がある．この不正通信の際，サーバとの通信にHTTPを用い，感染した端末からの接続をGoogle翻訳などのWeb翻訳サービスを経由して行うことで，通信先をそのサービスに偽装し，フィルタリングを回避することが可能である．本研究では,このような翻訳サービスを経由したフィルタリング回避の手法について調査し，その対策手法の検討，提案を行う．

Cfountermeasures about filtering avoidance by Web translation service

RYOTA SUZUKI† RYOICHI SASAKI†

†Tokyo Denki University
5, Senjuasahi-cho, Adachi-ku, Toukyou-to, 120-8551 JAPAN

Abstract In recent years, damage of targeted attacks has increased and the attack technique has also been diversified.In the targeted attacks, exit measures such as quick detection of the attacks and mitigation of the damage as well as protection of the Infection are required. Therefore the detection method to identify susceptive behavior and illegal communication the outside are essential. It is possible to avoid the filtering using WEB translation service such as Google by pretending the service site as the real destination of the communication.This study deals with the survey of the method to avoid the filtering using translation service, and the proposal of the measures to cope with the avoidance.

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．

標的型攻撃対策では，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，完全に感染を防ぎきるということは不可能に近い．そのため，感染を防止するだけではなく，感染時の早期発見や被害の軽減などといった，出口対策が重要であり，感染後の不審な挙動や不正通信の検知などの対策を行う必要がある．

この不正通信の際，サーバとの通信にHTTPを用い，感染した端末からの接続を

Google翻訳やエキサイト翻訳などのWeb翻訳サービスを経由して行うことで，通信先をそのサービスに偽装し，フィルタリングを回避することが可能である．

これらのWeb翻訳サービスでは，よく知られている，文章を入力し，他の言語に翻訳して表示するという通常の翻訳機能の他に，WebページのURLを入力し，入力されたWebページの内容を他の言語に翻訳し，翻訳されたWebページを表示する，Webページ翻訳の機能を提供している翻訳サービスが多数存在する．

このWebページ翻訳の機能を利用し，C&Cサーバと通信を行う際に，これらの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することができる．これを利用することで，プロキシサーバでフィルタリングにより接続を禁止されているC&Cサーバに接続することや，不審な通信の発見を困難にすることが可能である．

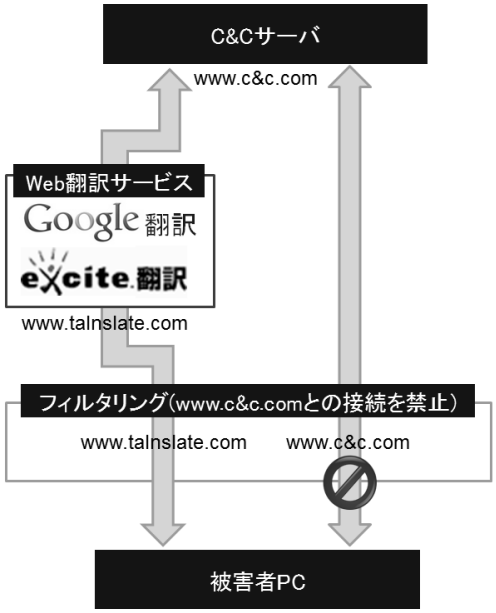

図１． フィルタリング回避手法

本研究では，このWeb翻訳サービスを利用したフィルタリング回避手法について調査し，このフィルタリング回避手法を用いた不正通信の手法について調査し，その対策手法を検討，提案する．

２　関連研究

不正通信の対策手法としてフィルタリングは広く利用されている．しかし，従来のフィルタリング手法では，暗号化通信やブラックリストの不足，更新速度などの多くの問題が存在する．

松木らの研究[1]では，ブラックリストの効率的な集約を行うことで，より高速に多くの脅威をフィルタリング可能にしている．また，榊原らの研究[2]では，プロキシサーバがhttp通信とブラウザの入力を照らし合わせることで，標的型攻撃におけるRATの通信を検知している．

Davisらの研究[3]では国家が行っているフィルタリング手法について示し，それらが暗号化通信を用いることで回避可能であることを示している．このような，暗号化された不正通信の対策として，Laurentの研究[4]では，ソフトウェアの暗号化通信について，ソフトウェアごとの暗号化通信のヘッダ情報の特徴に着目し，機械学習により暗号通信の内容を確認することなく，不正なソフトウェアを検知している．また，暗号化通信の内容を確認し，フィルタリングする手法としては，Hironoらの研究[5]が，プロキシサーバにより暗号化通信を中継する，man in the middle方式で，通信内容のフィルタリングを行っている．

本研究のWeb翻訳サービスを利用したフィルタリング回避手法の新規性として，以下の2点が挙げられる．

1) Web翻訳サービスを利用したフィルタリング回避手法では，見かけ上の通信相手のサーバが，正規のサービスを提供しているWeb翻訳サービスのサーバとなる．しかし，Web翻訳サービスを経由してC&Cサーバへの接続を行うことで，Web翻訳サービスのドメインで不正通信が可能になる．

2) https通信を使用するWeb翻訳サービスを経由することで，通信内容をWeb翻訳サービスによって暗号化し，通信内容から翻訳元サーバのドメインを確認することが困難となる．

３　フィルタリング回避手法

3.1　送信手法

Web翻訳サービスを利用することで，フ

ィルタリングの回避が可能であることを確認するため，実際にフィルタリングを回避する実験を行った．実験では，プロキシサーバのフィルタリング機能を用いて特定のWebサーバへの接続を禁止し，Webブラウザから直接Webページに接続した場合と，Web翻訳サービスを経由して接続した場合について接続し結果を比較した．

使用するOSはUbuntu 11.04，**フィルタリングを行うプロキシサーバをSquid 2.0，接続に使用するWebブラウザはMozilla Fire Fox 35.0とし，東京電機大学公式ホームページのサーバへの接続をブロックし実験を行った．また，キャッシュに保存されたファイルによる表示を防止するため**，Webブラウザやプロキシサーバはキャッシュを保存しないよう設定し，実験を行った．

実験の結果，通常の接続の場合，プロキシサーバによるブロック画面が表示され，接続に失敗した．対して，Web翻訳サービスを経由して接続した場合，Webページ上の画像が表示されず，レイアウトが崩れるなどの問題はあったが，Webページの表示には成功した．

この結果から，Web翻訳サービスを経由したフィルタリング回避は可能であることがわかった．

画像が表示されず，レイアウトが崩れるという点について，Web翻訳サービスでは，翻訳したWebページを表示する際，スタイルシートや画像など，翻訳を行わないファイルに関しては，翻訳元のWebページから直接表示しており，これらのファイルはブラウザから，翻訳元のWebサーバに要求を行っているためプロキシサーバのフィルタリングにより検知，遮断されていることがわかった．

これらの結果から，Web翻訳サービスを経由して送信可能なデータはテキストデータ部分のみであるといえる．

3.2 ファイル送信手法

3.1節で調査した結果から，Web翻訳サービスを経由し，フィルタリングを回避して送信可能なデータは，テキストデータのみであることがわかった．しかし，テキストデータの送信だけでは攻撃には不十分であり，ファイルの送信や応答方法が必要である．

不正プログラムのようなファイルをWeb翻訳サービス経由で送信する場合，テキストデータ部分に埋め込んだ状態で送信し，テキストデータを受信したプログラムが，埋め込まれたデータをファイルとして保存しなおすという処理を行うことでファイルの送信が可能であると考えられる．この手法での，Web翻訳サービスを経由したファイル送信が可能であることを，Web翻訳サービスを経由してファイルの保存を行うプログラムを作成し，確認した．

今回の実験では，送信するファイルを画像ファイルとし，Webページのテキストデータに埋め込まれた画像ファイルを，作成したプログラムにより保存可能であることを確認した．

実験の手順は，送信するファイルのバイナリデータを記述したhtmlファイルを作成し，このhtmlファイルを，Webサーバ上で公開，ブラウザからの閲覧が可能な状態にする．その後，Webサーバのドメインを，プロキシサーバから接続を禁止し，ブラウザからの閲覧が出来ないことを確認する．作成したプログラムにより，Web翻訳サービス経由でWebページに接続し，htmlファイルに記述した文字列からファイルの保存を行う．実験では送信するファイルにjpeg画像用い，最終的に保存された画像が正常に表示できることを確認する．翻訳サービスは攻撃検証実験と同様にGoogle翻訳を使用する．

実験の結果，翻訳元，翻訳先言語の設定によってはバイナリデータ部分も翻訳されてしまい，保存に失敗する場合があることがわかった．しかし，同一言語への翻訳や，日本語から英語の設定では，画像ファイルの送信に成功し，正常に画像が表示された．

この結果から，Webページへの接続とファイルの書き込みが可能ならば，テキストデータに攻撃用ソフトウェアを埋め込み送信することで，フィルタリングを回避してファイルの送信が可能であると考えられる．

また，今回の実験では，バイナリデータ部分がWeb翻訳サービスにより翻訳され，保存に失敗する場合があった．これは，バイナリデータをhtmlファイルのbody部に埋め込んでいたためであり，翻訳の対象にならないタグなどの形式で埋め込むこ

とで，翻訳元，翻訳先言語の設定を問わず攻撃用ソフトウェアの送信が可能である．

3.3 応答手法

標的型攻撃を行う場合，C&Cサーバからの命令や不正プログラムの受信だけでなく，不正プログラム側も同様にC&Cサーバに対して，攻撃の結果などの情報を応答として返信する必要がある．この不正プログラムによる応答の際，これまでの実験と同様に，翻訳サービスを経由しての通信が可能であることを実験により確認した．

実験では，Webサーバ上にPHPを用いた，ブラウザからの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プロキシサーバによりブロックした．その後，対象のページに翻訳サービスから接続し，ブラウザからの書き込みが可能であるかを調査した．データの送信方法はGETメソッドとPOSTメソッドを使用し，それぞれ，書き込みが可能であるかを調査した．

実験の結果，GETメソッド，POSTメソッドのどちらを使用した場合にも，翻訳元のページに対しての接続となり，プロキシサーバにより検知，遮断された．

実験の結果から，翻訳サービスから他のページに遷移する場合，リンクについては翻訳サービスで翻訳されたページへのリンクに変更されるが，入力フォームなどによる遷移の場合，翻訳元のWebサーバへの接続となることがわかった．このため，プロキシサーバにより検知され，通信が遮断されると考えられる．

今回の実験では，書き込みの際の接続が，翻訳元のページに対しての接続となり，プロキシサーバにより検知され，通信が遮断された．これは，入力フォームの送信先のアドレスが翻訳元のWebページのアドレスであるためであり，この部分を，あらかじめ翻訳サービスを経由したページのアドレスに設定しておくことで，翻訳サービスを経由して情報を送信できると考えられる．

このことを確認するため，同様のページを作成し，入力フォームの送信先のアドレスを，翻訳サービスを経由したアドレスに変更した上で同様の実験を行った．

実験の結果，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．POSTメソッドを使用した場合，画面の遷移は発生したもののデータの書き込みには失敗した．

これは，GETメソッドではデータがURL中に含まれ，翻訳元のサーバに送られるのに対し，POSTメソッドではデータがURL中には存在しないため，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．また，翻訳サービスに対し，GETのリクエストをURL中に含むアドレスを直接入力した場合にも，書き込みに成功した．このことから，GETメソッドで送信可能なデータ量という上限はあるが，Web翻訳サービスを経由した，C&Cサーバへの応答は可能であると考えられる．

4 外部Webページを表示可能なWeb翻訳サービス

これまでの調査の結果から，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，攻撃が可能であることがわかった．攻撃検証実験で使用した，Google翻訳以外のWeb翻訳サービスでも，同様にフィルタリングが回避可能であることを確認するため，他のWeb翻訳サービスについて調査した．

結果，外部Webページを表示可能なサービスは以下の表2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

Google翻訳
Yahoo!翻訳
@nifty翻訳
WorldLingo 無料オンライン翻訳者
So-net翻訳
エキサイト翻訳
Infoseekマルチ翻訳
So-net翻訳
CROSS Languege ホームページ翻訳サービス
SDL FreeTranslation.com

調査の結果，文章の翻訳を行う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．また，そのほかにも，文章の翻訳を行わず，Webサイトの翻訳を専門に行う翻訳サービスも見られた．

さらに，表1のWeb翻訳サービス以外にもInternet Archiveやウェブ魚拓といった，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，不正プログラムからの応答こそ受信不可能であるが，攻撃指令やプログラムの送信などの攻撃には利用可能であると考えられる．

特に，Internet ArchiveではWeb翻訳サービスとは異なりファイルのアーカイブを保存可能であり，アーカイブがアーカイブとして記録されるという欠点はあるが，不正プログラムを送信するという点では，Web翻訳サービスよりも容易に送信が可能である．

５　回避可能なフィルタリング形式

6章で調査したサービスについて，それぞれのサービスが，どのようなフィルタリング形式を回避することができるのかを調査する．

プロキシサーバでIPアドレス，ドメイン，キーワード（URLに含まれる任意の文字列）によるフィルタリングを行い，ブラウザからWebページに接続，それぞれのフィルタリング形式ごとに，通常接続の場合とWeb翻訳サービスを経由した場合について，Webページが表示可能かどうかを調査した．

調査の結果は表2の通りである．

表２．　各サービスのフィルタリング結果

フィルタリング形式	IPアドレス	ドメイン	キーワード
通常接続	×	×	×
Google翻訳	○	○	○
エキサイト翻訳	○	○	×
Yahoo!翻訳	○	○	×
Infoseek マルチ翻訳	○	○	×
@nifty翻訳	○	○	×
So-net翻訳	○	○	×
WorldLingo 無料オンライン翻訳者	○	○	×
CROSS Languege ホームページ翻訳サービス	○	○	×
So-net翻訳	○	○	×
SDL Free Translation.com	○	○	×
Internet Archive	○	○	○
ウェブ魚拓	○	○	×

○が接続成功，×が接続失敗を表す．

通常の接続を除いた全ての翻訳サービスで，IPアドレス，ドメインによるフィルタリングを回避し，接続に成功した．これに対して，キーワードによるフィルタリングでは，Google翻訳とInternet Archiveを除いて，検知，遮断に成功した．

IPアドレス，ドメインによるフィルタリングは，通常の接続を除いた全てのサービスで回避に成功している．このことから，IPアドレス，ドメインによるフィルタリングはWeb翻訳サービスを経由した攻撃に対して効果が無いといえる．

対して，キーワードによるフィルタリングでは，Google翻訳とInternet Archiveを除いて，検知，遮断に成功している．

これは，これらの翻訳サービスでは，翻訳するWebページのURLをGETパラメータで送信しており，図2のURLの下線部分のように，URL中に翻訳するWebページのドメインが含まれ，このドメインがキーワードによるフィルタリングで検知，遮断されるためである．

http://www.excite-webtl.jp/world/english/web/?wb_url=http%3A%2F%2Fweb.dendai.ac.jp%2F&wb_lp=JAEN

図２．　エキサイト翻訳 URL

以上のことから，キーワードによるフィルタリングはWeb翻訳サービスを経由した攻撃に対して，有効なフィルタリング形式であると考えられる．

しかし，Google翻訳とInternet Archiveの2つのサービスでは，キーワードによるフィルタリングを行った場合にも接続に成

功した．この2つのサービスの場合も，キーワードによるフィルタリングで検知，遮断に成功した他のサービスと同様，翻訳するWebサイトのURLをGETパラメータで送信しており，URL中に翻訳するWebページのドメインが含まれているが，この2つのサービスは，キーワードによるフィルタリングでは検知，遮断ができなかった．

この2つのサービスと他のサービスを比較した結果，図3，図4のURLからわかるように，Google翻訳とInternet Archiveではhttps通信を使用していることがわかった．

https通信では，URLなどの情報は暗号化されて送信されるため，URLに含まれるGETパラメータも暗号化されて送信される．このため，プロキシサーバから確認できるのはドメイン部分のみになり，GETパラメータに含まれている翻訳元WebサイトのURLを確認し，フィルタリングすることはできない．

よって，この2つのサービスに関してはプロキシサーバからのフィルタリングが機能せず，通信の検知，遮断に失敗したと考えられる．

https://translate.google.com/
translate?sl=ja&tl=en&u=http://www.web.dendai.

図３． Google 翻訳 URL

https://web.archive.org/web/
20140130001059/http://web.dendai.ac.jp/

図４． Internet Archive URL

以上のことから，Google翻訳とInternet Archiveのようなhttps通信を使用するサービスでは，プロキシサーバから通常の方法でのフィルタリングを行うことは出来ないと考えられる．

６　Web翻訳サービスの暗号化対策

回避可能なフィルタリング形式についての調査の結果から，Google翻訳とInternet Archiveではhttps通信を使用しているため，URLが暗号化され，キーワードによるフィルタリングでの検知，遮断が不可能であるということがわかった．

このWeb翻訳サービスによる暗号化への対策として，まず考えられるのは，https通信を使用するWeb翻訳サービスに対するhttps通信を禁止し，http通信に変更するという対策である．実際に調査を行い，Google翻訳とInternet Archiveへのhttps形式での通信を禁止し，http形式での接続を強制することで，キーワードによるフィルタリングによる検知，遮断が可能であることを確認した．このことから，Google翻訳，Internet Archiveなどのhttps通信を行う外部ページを表示可能なサービスの場合，これらのサービスに対するhttps形式での通信を禁止し，http形式での通信を行うことで，他のWeb翻訳サービスと同様に，キーワードによるフィルタリングで対策することが可能である．

ただし，この対策手法では，https通信を禁止しhttp通信を使用することにより，本来は暗号化によって保護されている通信を暗号化せずに送信するため，これらのWeb翻訳サービスとの通信が盗聴，改ざんされる危険性が高まるという問題点がある．

暗号化を維持した状態での対策手法として，プロキシサーバが，Webサーバに対してはクライアント，クライアントPCに対してWebサーバとして振舞い，暗号化通信を中継するという，man in the middle方式を用いることで，暗号化を禁止することなく，通信のフィルタリングが可能である．しかし，この対策手法では，プロキシサーバの証明書を発行し，クライアントPCにルート証明書としてインストールする必要があり，この証明書を用いることで，Web翻訳サービス以外の全ての暗号化通信の内容が確認できてしまうため，証明書の管理やプライバシーなどの新たな問題が発生する．

このように，Web翻訳サービスに対してhttps通信を禁止する場合は通信内容の盗聴，改ざんの問題が，man in the middle方式を用いる場合は証明書の管理やプライバシーといった問題が発生する．

７　対策手法

Web 翻訳サービスにより回避可能なフィルタリング形式の調査結果から，Web翻訳サービスでは，翻訳元ページのアドレスの送信にGETメソッドが使用されていることがわかった．このため，翻訳サービスを経由して接続した場合も，通常の

Web ページへの接続と同様に，URL 中に翻訳元ページの URL が含まれる．このことから，URL 中に含まれる単語によりフィルタリングを行う，キーワードによるフィルタリングを使用することで，翻訳サービスを経由したフィルタリング回避を防ぐことが可能である．

しかし，Google 翻訳や Internet Archive などの https 通信を使用するサービスがフィルタリングの回避に利用されている場合，通信内容は Web 翻訳サービスのサーバとクライアント PC 間で暗号化されており，通常ではプロキシサーバから通信内容を確認できず，URL やリクエストの内容などの情報を参照するフィルタリングを行うことが出来ない．

この暗号化の対策として，Web 翻訳サービスに対しては https 通信での接続を禁止し, http 通信での接続を強制するという対策と，man in the middle 方式により，プロキシサーバから通信内容をフィルタリング可能にするという対策の 2 種類が考えられる. どちらの対策も, それぞれ, Web 翻訳サービスに対して https 通信を禁止する場合は通信内容の盗聴，改ざんの危険性が，man in the middle 方式を用いる場合は証明書の管理やプライバシー保護の問題が発生する．

後者のman in the middle方式を用いた対策の場合，暗号化通信のフィルタリングを行う製品も存在するため，既にこれらの製品を使用している場合は，新たな問題は発生しないため，こちらの対策手法を使用するべきだと考えられる．

それらの製品を使用しておらず, Web翻訳サービスとの通信を暗号化する必要が無い場合は，Web翻訳サービスに対して，https通信での接続を禁止し，通常の通信と同様にフィルタリングする対策手法を使用するべきであると考えられる．

ただし，この対策手法を用いる場合，Google翻訳やInternet Archiveなどのサービスへブラウザから接続した際，通常ではhttps通信での接続となり，プロキシサーバにより接続を検知，遮断されてしまうため，同サービスのhttp通信用のページにリダイレクトさせるよう設定する必要がある．

この対策では，特定のアドレスに対する https 通信での接続の禁止や，リダイレクトなどの機能は，フィルタリング機能を持つ多くのプロキシサーバで設定可能であり，新たなシステムを用意することなく，Web 翻訳サービスを利用したフィルタリング回避の対策が可能であるという利点がある．

8　おわりに

本研究は, Web翻訳サービスを経由してC&Cサーバと通信することで，プロキシサーバによるフィルタリングを回避し，ブラックリストに登録されているC&Cサーバから攻撃ソフトウェアの送信やC&Cサーバに対する応答を行う手法について調査し，その対策手法を提案した．

提案手法では，外部 Web ページを表示可能なサービスは，翻訳時の URL に翻訳元ページのドメインが含まれることに着目し，URL 中に任意の文字列が含まれているか否かでの判定を行うキーワードによりフィルタリングを用い，ブラックリストに登録されているサーバのドメイン, IP アドレスを含んだ URL への接続を禁止することで対策を行った. これにより，ブラックリストに登録されている C&C サーバとの通信を検知，遮断することが可能である．

しかし，Google 翻訳や Internet Archive などの https 通信を使用するサービスとの通信の場合，通信内容が暗号化されるため，プロキシサーバからはドメイン以外を確認することが出来ず，URL 中のキーワードによるフィルタリングを行うことができない．よって，上記の手法では，Google 翻訳や Internet Archive などの https 通信を使用するサービスに対して不正通信の検知，遮断ができない．

これは，man in the middle 方式により暗号化通信のフィルタリングを可能にする製品を使用し，上記の対策手法と同様に URL 中のキーワードによるファイルタリングを行うことで対策することが可能である．

それらの製品の導入が困難である場合, プロキシサーバにより，Google 翻訳や Internet Archive に対する https 通信を禁止し，同サービスの http 通信を行うページにリダイレクトするよう設定することでも対策が可能である． ただし，この対策を使用する場合，これらのサービスへの暗号化を禁止することにより，盗聴や改ざんの危険性が発生する．

同様に，man in the middle 方式を用いた

製品を新たに採用する場合，証明書の管理やプライバシー保護の問題が発生するため，両者の対策を比較し，組織にあった対策を採用するべきである．

参考文献

[1] 松木隆宏; 新井悠. URL ブラックリストの効率的な利用方法の一検討 (高度インシデント分析を支える要素技術，インターネットセキュリティ，一般). 電子情報通信学会技術研究報告. IA，インターネットアーキテクチャ, 2009, 109.85: 19-23.

[2] 榊原裕之; 桜井鐘治. ユーザが意識しない HTTP 通信の識別について. 情報処理学会第 74 回全国大会, 2012, 5: 1.

[3] SHORTER, Davis Gossett1 Jack D. Effectiveness of Internet Content Filtering. 2011.

[4] BERNAILLE, Laurent; TEIXEIRA, Renata. Early recognition of encrypted applications. In: Passive and Active Network Measurement. Springer Berlin Heidelberg, 2007. p. 165-175.

[5] HIRONO, Soshi, et al. Development of a Secure Traffic Analysis System to Trace Malicious Activities on Internal Networks. In: *Computer Software and Applications Conference (COMPSAC), 2014 IEEE 38th Annual*. IEEE, 2014. p. 305-310.

[7] Google ,Google 翻訳,
https://translate.google.co.jp/

[8] Excite，英語翻訳 ウェブページ翻訳 - エキサイト 翻訳 - Excite,
http://www.excite.co.jp/world/english/web/

[9] Weblio，ウェブページ翻訳 - Weblio 翻訳,
http://translate.weblio.jp/web/english

[10] Yahoo! JAPAN，ウェブ翻訳 - Yahoo!翻訳 - Yahoo! JAPAN,
http://honyaku.yahoo.co.jp/url/

[11] Infoseek，Infoseekマルチ翻訳,
http://translation.infoseek.ne.jp/

[12] nifty，英語翻訳・WEB英語翻訳・スピード英語翻訳｜@nifty翻訳,
http://honyaku.nifty.com/

[13] worldlingo，無料オンライン翻訳者 - WorldLingo,
http://www.worldlingo.com/ja/products_services/worldlingo_translator.html

[14] クロスランゲージ，ホームページ翻訳サービス｜自動翻訳／翻訳ソフト｜クロスランゲージ,
http://www.crosslanguage.co.jp/auto-translation/homepage/

[15] So-net，翻訳 | So-net,
http://www.so-net.ne.jp/translation/

[16] SDL，SDL の無料翻訳サービスとプロフェッショナル翻訳サービス,
http://www.freetranslation.com/ja

[17] Internet Archive，Wayback Machine,
https://archive.org/

[18] 株式会社アフィリティー，**ウェブ魚拓**,
http://megalodon.jp/

[19] **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，デジタルアーツ株式会社**,
http://www.daj.jp/bs/i-filter/old/option_relation_ssl_adapter/

[20] **SSL暗号化通信の中身を見る！“Counter SSL Proxy，スワットブレインズ株式会社**,
http://www.swatbrains.co.jp/csp.html