C-15

組織内ネットワークにおける 組織外 DNS との通信監視システムの構築

大地　真司† 　　川橋　裕‡
Ochi Shinji　 Kawahashi Yutaka

1 はじめに

近年，標的型メールをはじめとしたサイバー攻撃により，多くのインターネットユーザが悪質なサイトへ誘導され，マルウェアへの感染や個人情報流出などの被害を受けている．また攻撃手法は日々巧妙化しており，ユーザ個人での対策のみならず，組織レベルでの包括的なセキュリティ対策が求められている．

和歌山大学ではセキュリティ対策の一環として，Cisco Umbrella(以下「Umbrella」という)を学内ネットワークに導入している．Umbrella は Cisco 社が提供する，DNS(Domain Name System)の名前解決のしくみを利用したクラウド型セキュリティサービスで，悪質なサイトへの接続を DNS の名前解決の段階でブロックし，通信の安全性を確保することができる．
しかし欠点として，DNS の設定を Umbrella 以外に変更した端末にはサービスを適用することができない．

本研究では，和歌山大学においてUmbrellaの適用対象外となる，学内ネットワークから学外のDNSに対して，ドメインからIPアドレスへの問い合わせをおこなう通信パケットの情報を記録し、不正なサイトにアクセスした
ユーザの特定を支援するためのシステム構築をおこなった．

2 先行研究

和歌山大学では先行研究として、障害発生時に
原因の特定を支援するためのシステムであるTRAF
Lがある．

TRAFL はネットワークサイド，サーバサイド，ユーザサイドの3 つの構成から成り立っている．
サーバサイドでは，パケットキャプチャにより取得したデータをフロー形式でデータベースに保存する．データベースに保存された情報を基に，グラフやランキング形式に加工し，Web ブラウザで表示させることで，管理者は時間毎のトラフィックの詳細な記録を表示でき，ネットワークの状況を確認するのが容易になる

しかし、TRAFLはパケットのデータ部の情報を記録しないため，HTTP(Hypertext Transfer Protocol)通信の場合，アクセスしたURLを具体的に知ることはできない．

† 和歌山大学大学院システム工学研究科
‡ 和歌山大学学術情報センター

3 研究目的

本研究では，学外DNSに正引きをおこなった通信記録を保存しておくことで，障害発生時に，過去の問い合わせ記録を参照し，不正なサイトへアクセスし，被害を受けたユーザの特定を支援するシステムの構築を目的とする．そうすることで，HTTPS 通信のように暗号化された通信に対しても，ユーザがアクセスしたドメインまでを特定することができる．また，記録したドメインを学内DNSに問い合わせ，問い合わせ結果から，不正なサイトであるかを記録する．これにより，管理者が調査をおこなうにあたって，Umbrellaの判断基準を考慮に入れることができる．

4 提案手法・システム

本研究では，特定のサイトにアクセスしたユーザを調査するため，以下の項目をデータベースに記録し、検索をおこなえるようにした．

_ 送信元IPアドレス
_ 宛先IPアドレス
_ 問い合わせか返答か
_ DNSへの問い合わせ内容
_ DNSからの返答
_ データの取得時間
_ Umbrellaへの問い合わせ結果

提案システムの構成を図1に示す．

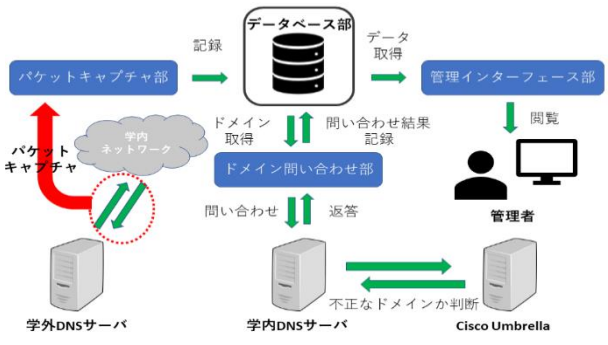

図1：提案システム

はじめに，学内以外のDNSと通信をおこなうパケットのうち，データ部にAレコードが記録されているパケットのキャプチャを行う．そして，キャプチャしたパケットから，必要なデータを抽出する．まずヘッダより送信元IPアドレス，宛先IPアドレスを，次にデータ部より，DNSへ問い合わせたドメイン名，DNSから返答されたIPアドレスを取得する．またDNSヘッダより，パケットが問い合わせと応答のどちらをおこなっているか判断する．これらの情報をデータベースに記録し，ブラウザ上での参照を可能とした．またデータベースに保存されたドメイン情報を学内DNSに問い合わせ，返答された結果から不正なドメインであるかを判断し，データベースに記録する．

5 実験・評価

提案システムを用いて，Web ユーザインタフェースで管理者が不審なドメインに接続したユーザを特定できるか実験をおこなった．本実験では，Umbrellaで不正なサイトと判断されるURLへの，学外DNSを介したHTTP通信，HTTPS通信をおこなう．そしてDNSへの問い合わせを記録し，ブラウザ上で参照できることを確認する．また，Umbrellaで不正なサイトと判断されるURLを分類できることを確認する．

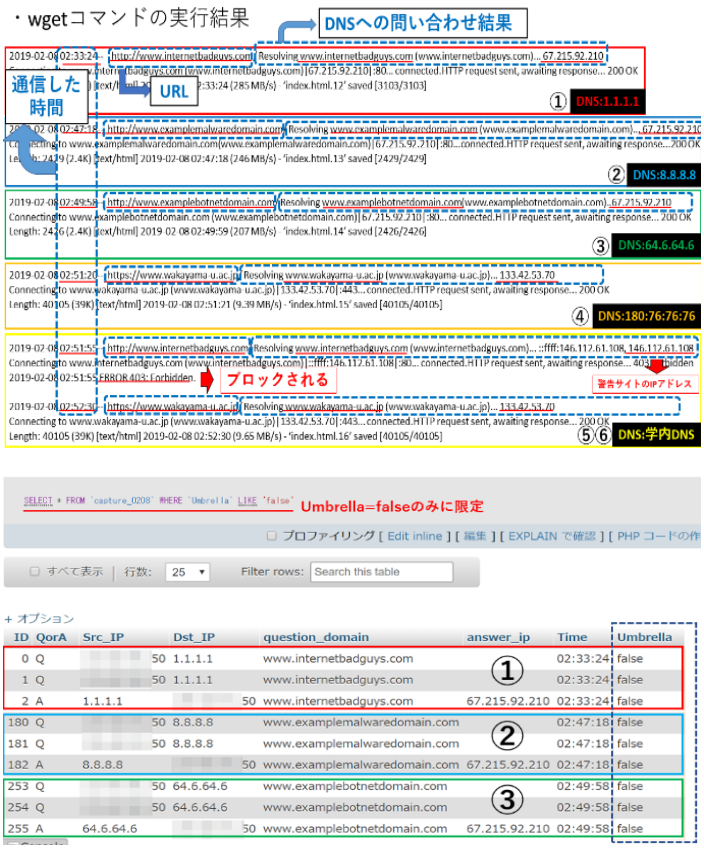

図2：実験結果

実験結果は図２のようになった．図２はwgetコマンドの実行結果，および，提案システムのデータベースか特定のドメインに接続したことを示すレコードを検索した結果である．図２から，HTTP，またHTTPS通信について，学外DNSに正引きをおこなう通信パケットのみをキャプチャし，正しく情報を取得できていることが確認できた．また，指定したドメインに接続したユーザを特定できていることも確認できた．

実験結果より，不正なサイトへアクセスしたユーザを調査する場合について，本システムが有用であると考えられる．

6 今後の課題

本研究では実験環境で本システムの試験運用をおこなった．しかし，学内ネットワークへの導入にあたっては，監視をおこなう通信量は，実験環境よりも膨大なものとなる．そのため，システムの動作のさらなる効率化が求められる．

また，現在はブラウザでのデータ参照にデータベース管理ツールであるphpMyAdminを用いている．

しかし，phpMyAdminは詳細なデータベース操作にはSQL文の入力が必要であるなど，本システムの運用にあたっては，管理者への負担が大きい．そのため，今後本システムの利用用途に沿ったインターフェースの構築をおこなっていきたい．

参考文献

[1] 釼本　倫章　"トラフィックグラフとフローに基づくネットワーク管理支援システムTRAFLの構築と運用"
2015 年度卒業論文　和歌山大学大学院システム工学研究科

[2] 和歌山大学　“クラウド型セキュリティサービスの導入について“(2019)
http://www.wakayama-u.ac.jp/limited/aic/umbrella.html

[3] Cisco　“Cisco Umbrella – クラウドを保護する企業向けセキュリティ“(2019)
https://www.cisco.com/c/m/ja_jp/umbrella/index.html