デジタルプラクティス　Vol.11 No.3(July 2020)

推薦論文

DNSシンクホールを用いた悪意あるFQDNに対する通信観測システムの運用

佐保 航輝[1]　池部　実[2]　吉崎 弘一[3]　吉田 和幸[3]

[1]大分大学大学院　[2]大分大学　[3]大分大学学術情報拠点情報基盤センター

インターネットにおいてドメイン名を悪用した詐欺や攻撃が多く発生している．ユーザは攻撃者が用意したFQDN（以降，悪意あるFQDNと呼ぶ）をもつWebサーバへ接続することで，フィッシング詐欺やドライブ・バイ・ダウンロード攻撃などの被害を受ける可能性がある．悪意あるFQDNへの接続を阻止する手法の1つとしてDNSシンクホールがある．DNSシンクホールは，クライアントからのフィッシングサイトのFQDNやマルウェア配布サイトのFQDNなどの悪意あるFQDNの名前解決要求に対して，本来とは異なるIPアドレスを応答し，悪意あるサイトへの接続を防ぐ．本研究ではクライアントが悪意あるFQDNへ接続することを防ぎながら，接続時におけるクライアントの挙動を分析することを目的とする．本稿では，DNSシンクホールと観測サーバを用いてクライアントからの悪意あるFQDNに対する通信を観測するシステムの構築について述べる．現在運用しているDNSシンクホールは，問い合わせられた悪意あるFQDNに対してループバックアドレスを応答する．しかし，管理者はブロックした接続において，たとえばWebサーバからどのようなファイルがダウンロードされようとしていたのか，どのような情報を外部へ送信しようとしていたのかまでは把握できない．また，ユーザ側の視点でもなぜ接続がブロックされたのか把握できない．そこで，我々はDNSシンクホールから観測サーバのIPアドレスを応答することにより，当該通信を観測サーバへ誘導し，クライアントからの悪意あるFQDN宛の通信を分析する仕組みを構築した．本観測システムでは観測サーバで収集したHTTPリクエストを分析することで，ブラックリストに記載されたFQDNのみでは分析できない接続後の挙動や攻撃手法を分析する．本稿では，これまで筆者らが運用してきたDNSシンクホールの現状について述べ，改良したDNSシンクホールについて説明する．さらに，小規模な検証環境において改良したDNSシンクホールを稼働させた結果を報告する．

1. はじめに

オンラインバンキング，Eコマースなどインターネットを介してさまざまなサービスが提供されている．インターネット上のさまざまなサービスを利用する上でDNS（Domain Name System）は欠かせない仕組みである．DNSはドメイン名とIPアドレスを対応付けるインターネットを支える重要な仕組みの1つである．DNSサーバは機能によりコンテンツサーバとフルリゾルバサーバの2種類に分類される．コンテンツサーバは各ドメイン空間を管理し，フルリゾルバサーバはクライアントのリゾルバ（以下，クライアント）からの名前解決要求を受信して，クライアントに代わりコンテンツサーバへ問合せる．クライアントは名前解決によって得られたIPアドレスを用いて，サービスを提供するサーバと通信できる．

しかしながら，正規のサービスに類似したドメイン名を悪用した詐欺や攻撃などが発生している．たとえば，メールに記載されたフィッシングサイトのURLや，マルウェア配布サイトのFQDN（Fully Qualified Domain Name）に接続することで，フィッシング被害やマルウェア感染などの被害が発生している[1],[2]．これらの被害を抑えるために，攻撃者が用意したFQDN（以降，悪意あるFQDNと呼ぶ）やサーバへの接続を阻止する必要がある．

筆者らが管理するネットワークシステムの一部に，悪意あるFQDNへの接続を阻止するためにDNSシンクホールを設置し，運用している．現在のシステムは悪意あるFQDNへの接続を阻止できるが，クライアントがどのようなマルウェアをダウンロードしようとしていたのか，どのような情報をアップロードしようとしていたのかまでは分からない．そこで本稿では，現在運用中のシステムを拡張し，悪意あるサーバに接続後の通信を観測するシステムを構築した結果を報告する．

2. 不正通信の阻止手法

2.1 不正通信の阻止手法

インターネット上には，マルウェアを配布するサーバやフィッシング目的のサーバなど悪意あるサーバが存在している．これらのサーバとの通信を以後不正通信と呼ぶ．不正通信を阻止する手法として，ファイアウォールやDNSシンクホールなどがある．ファイアウォールはネットワークの通信において，送信元IPアドレスや宛先IPアドレス，ポート番号など，パケットのヘッダ情報をもとにその通信を許可するかなどを決める[3]．このようにパケットの情報をもとに処理を行う方式をパケットフィルタ型という．パケットフィルタ型ではIPアドレスやポート番号などを識別して処理を行うが，アプリケーションまでは識別できない．アプリケーションを識別し，アプリケーションやユーザごとに処理を設定するファイアウォールは次世代型ファイアウォールと呼ばれ，主に大規模なネットワークで利用されている．ファイアウォールは主に，クライアントごとに設置するものと，企業や大学など組織内のLANとインターネットの間に設置するものがある．

DNSシンクホールとは，マルウェア配布サイトやフィッシングサイトなど既知の悪意あるFQDNへの接続を阻止するシステムである[4]．DNSシンクホールはフルリゾルバサーバに設置する．DNSシンクホールを設置したフルリゾルバサーバは悪意あるFQDNの一覧をブラックリストとして保持する．ブラックリストに記載されたFQDNの名前解決問合せに対して，本来のIPアドレスとは異なるIPアドレスを応答する．異なるIPアドレスを返すことで悪意あるFQDNへの接続を阻止する．

2.2 関連研究

ファイアウォールを用いた不正通信の阻止に関する研究がある．パケットフィルタ型のファイアウォールでは，通信制御に用いられるルールを設定するアクセスコントロールリスト（以下，ACL）が実装されている．ACLのルールリストの並び替えによってより効率的なルールを探索する研究[5],[6]や，非効率なルールや冗長なルールを減らすことで効率化を図る研究[7]などがある．その他に，ファイアウォールに記録されたログを用いてマルウェア感染を検知する研究[8]などもある．

DNSシンクホールを用いた研究として，瀬川ら[9]は，フルリゾルバサーバに変更は加えず，クライアントとフルリゾルバサーバを中継するシステムを構築している．システム内で複数の機能が実装されているが，その中の1つとしてDNSシンクホールと同様に本来の回答とは異なる回答をクライアントに返す機能が実装されている．また，文献[10]では，攻撃者が以前利用していたドメインを契約し，そのドメインを監視することで攻撃を観測している．2.1節で述べたDNSシンクホールとは異なり，接続阻止という観点からは外れているが，こちらもDNSシンクホールと呼ばれているため紹介しておく．

2.3 DNSシンクホールの動作

筆者らが管理するネットワーク内ではファイアウォール，フルリゾルバサーバともに運用している．フルリゾルバサーバのソフトウェアにはBIND9を用いており，このフルリゾルバサーバにDNSシンクホールを導入することは容易である．導入後の運用，管理についても容易に行えることからDNSシンクホールを導入した．

現在，筆者らが管理するネットワークの一部において，クライアントが利用するフルリゾルバサーバ2台にDNSシンクホールを設置し，悪意あるFQDNへの接続を阻止している．接続を阻止するためのブラックリストには，DNS-BH[11]が公開しているブラックリストを使用した．ブラックリストには，悪意あるFQDNに加え，各FQDNに**表1**に示した分類が登録されている．**図1**に，クライアントがフルリゾルバサーバに対して悪意あるFQDNを問合せた際の挙動を示す．

表1　悪意あるFQDNの分類

分類	FQDNの種類
malicious	マルウェア配布サイト， アップローダなどの悪性サイト
phishing	フィッシングサイト
malware	マルウェア配布サイト
suspicious	マルウェア配布サイト， アップローダなどの疑わしいサイト
ransomware	ランサムウェア配布サイト

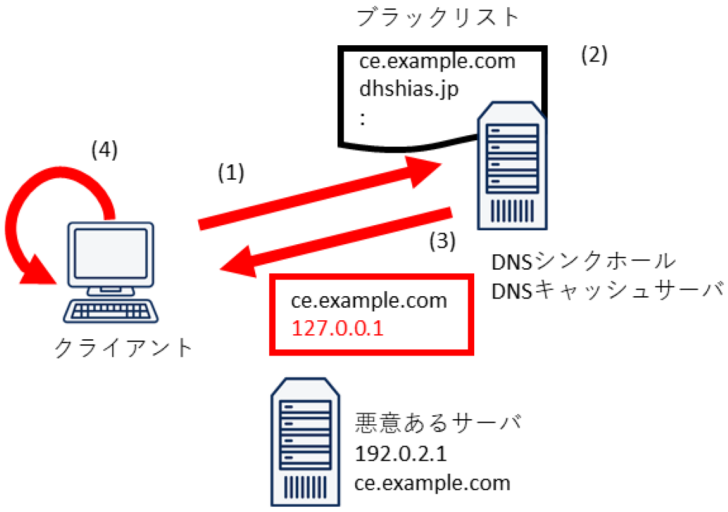

図1　接続阻止の流れ

（1）クライアントが悪意あるFQDN（例: ce.example.com）の名前解決要求をフルリゾルバサーバに問合せる．
（2）フルリゾルバサーバは要求されたFQDN（ce.example.com）がブラックリストに記載されていないか確認する．
（3）ブラックリストに記載されていた場合，本来の応答とは異なるループバックアドレス（127.0.0.1）を応答する．記載されていない場合は通常とおり，フルリゾルバサーバでキャッシュしていればキャッシュから応答し，キャッシュに存在しなければ当該FQDNを管理するコンテンツサーバへ問合せる．ここでは，ce.example.comがブラックリストに記載されているので，127.0.0.1を応答する．
（4）クライアントは応答内に含まれるIPアドレスである127.0.0.1へ接続を試みるため，悪意あるサーバへの接続は阻止される．

運用中のDNSシンクホール2台における問合せ状況を調査した．運用中のDNSシンクホールはサブネットマスク長21のネットワークで約1,000台のクライアントへフルリゾルバサービスを提供している．調査期間は2019年1月1日から2019年10月31日までである．**表2**に調査結果を示す．調査期間中の問合せ件数は全体で約1.4億件あり，このうち，ブラックリストに記載されている悪意あるFQDNの問合せ件数は234件であった．悪意あるFQDNの問合せ率としては，0.00017%とかなり低い割合である．現在設置しているネットワークシステムのユーザが情報系学科の教職員・学生でありセキュリティ面には気をつけていると考えられる．また，クライアントにはウィルス対策ソフトウェアの導入が義務つけられていることも低い問合せ率である要因の1つであると推測している．問合せのあった234件のうち，悪意あるFQDNは6種類のFQDNであった．検出された悪意あるFQDNとその分類の一部を**表3**に示す．検出された悪意あるFQDNは現時点ではブラックリストからコメントアウトされているFQDNをふくんでいる．

表2　調査結果

期間	2019年1月1日～10月31日
全体の問合せ件数	141,607,727件
ユニークなIPアドレス数	1,064個
悪意あるFQDNへの問合せ件数	234件
悪意あるFQDNを問合せたIPアドレス	22個
検出した悪意あるFQDN	6種類

表3　検出された悪意あるFQDN

	悪意あるFQDN	分類	件数
A	bleachkon.net	malicious	2件
B	mobile.audible.com	phishing	10件
C	rebrand.ly	phishing	1件
D	zen.yandex.ru	phishing	11件

検出した悪意あるFQDNのうち，特徴的な問合せのあったbleachkon.netについて詳しく調査した．調査にはVirus Total[12]，IPAddress.com[13]，Sucuri SiteCheck[14]，aguseGATEWAY[15]など，URLやIPアドレスのレピュテーションサイトを利用した．

bleachkon.netは調査期間内において問合せが2件であった．2018年にも複数回の問合せがあったFQDNである．当該FQDNの問合せを**図2**に示す．クライアントからAとAAAAレコードの問合せが同じタイミングで記録されていた．この問合せが図2以外にも1回確認された．2018年にも短時間でAとAAAAレコードを1回ずつ，もしくはA，A，AAAAレコードの順で問合せられていた．このFQDNを問合せていたクライアントはすべて同じIPアドレスである．bleachkon.netを調査すると，米国に設置されているWebサーバで，悪意あるソフトウェアを配布する恐れがあるとしてブラックリストに登録されていた．またDNS-BH以外の複数のブラックリストにも登録されていた．

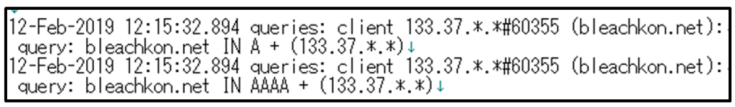

図2　bleachkon.netの問合せログ

3. 設計と実装

運用してきたDNSシンクホールでは接続を阻止できる．しかし，クライアントの接続をローカルホスト宛にするため，管理者側で被害状況を調査するために必要な情報を得ることはできない．被害状況を調査するためには，ダウンロードするファイル名，アップロードしようとしていた情報などが必要となる．これらの情報は宛先に対するURLやリクエスト内容を観測することで得ることができる．また，宛先FQDNのブラックリストにおける分類別に応答を変更することで，ユーザ側でも被害状況を把握できる．そこで，DNSシンクホールに加え，観測サーバを新たに用意し，クライアントからの悪意あるFQDNへの接続を観測サーバへと誘導するシステムを提案している[16]．**図3**に実装する観測システムでの通信誘導の流れを示す．新たに構築した観測サーバへ誘導することでクライアントからの悪意あるFQDN宛の通信を観測できる．ユーザが状況を把握できるよう，観測結果をフィードバックするための機能などを実装する．

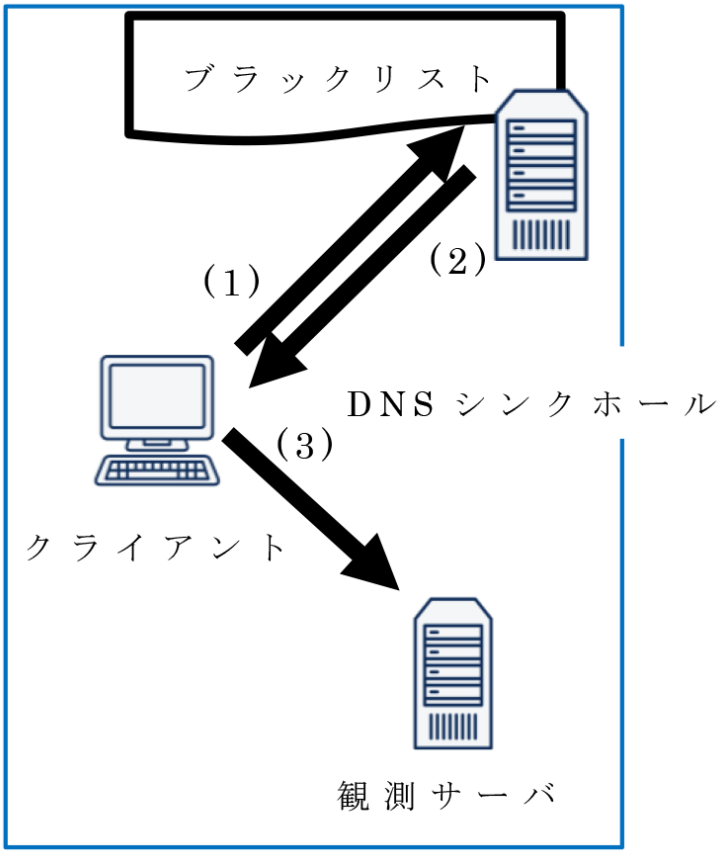

図3　DNSシンクホールによる通信誘導の流れ

(1) クライアントはフルリゾルバサーバのブラックリストに記載されている悪意あるFQDNを問合せる．
(2) DNSシンクホールであるフルリゾルバサーバは，問合せ要求に含まれるFQDNが自身の保持するブラックリスト内に存在するかを確認する．存在した場合，コンテンツサーバに反復問合せするのではなく，DNSシンクホールで設定している観測サーバのIPアドレスを応答する．
(3) クライアントはフルリゾルバサーバからの応答をもとに通信する．フルリゾルバサーバからの応答は観測サーバのIPアドレスであるため通信は観測サーバへ誘導される．

すでに稼働しているDNSシンクホールと同様にDNS-BHが公開しているブラックリストを使用した．DNS-BHの公開しているブラックリストはゾーンファイル形式（**図4**）とFQDN，分類，登録日などが記載されたテキストファイル形式（**図5**）がある．従来は1日1回ゾーンファイルをダウンロードし，フルリゾルバサーバへ組み込んでいた．図4に示したゾーンファイルに記載されているblockeddomain.hostsには，当該FQDNのAレコードとして127.0.0.1を記述している．

```
zone "yhiltd.co.uk" {type master; file "/etc/namedb/blockeddomain.hosts";};
zone "dicrophani.com" {type master; file "/etc/namedb/blockeddomain.hosts";};
zone "airtyrant.com" {type master; file "/etc/namedb/blockeddomain.hosts";};
zone "dionneg.com" {type master; file "/etc/namedb/blockeddomain.hosts";};
zone "vipprojects.cn" {type master; file "/etc/namedb/blockeddomain.hosts";};
zone "hhj3.cn" {type master; file "/etc/namedb/blockeddomain.hosts";};
zone "hryspap.cn" {type master; file "/etc/namedb/blockeddomain.hosts";};
zone "iebar.t2t2.com" {type master; file "/etc/namedb/blockeddomain.hosts";};
zone "bakuzbuq.ru" {type master; file "/etc/namedb/blockeddomain.hosts";};
zone "ksdiy.com" {type master; file "/etc/namedb/blockeddomain.hosts";};
```

図4　DNS-BHで公開されているゾーンファイルの一部

```
yhiltd.co.uk    phishing        openphish.com   20171117        20160527
dicrophani.com  pony    virustotal.com  20171117        20160527
airtyrant.com   malicious       cybercrime-tracker.net  20171117
dionneg.com     attackpage      safebrowsing.clients.google.com 20171117
vipprojects.cn  attackpage      safebrowsing.google.com 20171117
hhj3.cn attackpage      safebrowsing.clients.google.com 20171117
hryspap.cn      attackpage      safebrowsing.clients.google.com 20171117
iebar.t2t2.com  attackpage      google.com/safebrowsing 20171117
bakuzbuq.ru     malspam blog.dynamoo.com        20171117        20160527
ksdiy.com       attackpage      safebrowsing.clients.google.com 20171117
```

図5　DNS-BHで公開されているテキストファイルの一部

誘導後の通信観測の目的は，フィッシング詐欺におけるWebアクセスや，Webサーバを介したダウンロード，アップロードする内容の解析である．本システムで観測対象とするプロトコルはHTTPとした．HTTP通信を観測するための観測サーバとして，ハニーポットの一種であるGlastopf[17]を採用した．ハニーポットとは，攻撃者の侵入手法や侵入後の振る舞いなどを調査するため，あえて侵入しやすいように設計された機器やシステム環境である．ハニーポットには高対話型と低対話型の2種類がある．高対話型ハニーポットは，実際に脆弱性のあるOSやアプリケーションを利用する．高対話型ハニーポットでは侵入した攻撃者の詳細な挙動を観測できるが，ハニーポット自身が踏み台とされる可能性もあり，運用に注意する必要がある．一方，低対話型ハニーポットは特定のアプリケーションやプロトコルをエミュレートすることにより攻撃者の挙動を観測する．よって，マルウェアの感染や踏み台とされることなく運用できるが，高対話型と比べて攻撃者から得られる情報が少ない．

Glastopfはオープンソースの低対話型ハニーポットであり，Webサーバをエミュレートする．Glastopfにてクライアントからの誘導したHTTPリクエストを収集する．一般に，サーバ上に存在しないコンテンツをHTTPリクエストで指定した場合，HTTPレスポンスとして“404

Not Found”を応答する．Glastopfではサーバ上に存在しないコンテンツをHTTPリクエストで指定した場合においても，“200 OK”を応答し，クライアント上で動作する悪性のプログラムを騙し，その後の動作を観測できることを期待している．

表1で示したようにDNS-BHブラックリストにはFQDNに対して，フィッシングやspam，マルウェアなど分類が記載されている．この分類に応じてAレコードに対応するIPアドレスを変更することで，より細かな観測やユーザの状況把握の補助などが可能と考えられる．本研究では応答するAレコード用IPアドレスを複数準備し，IPアドレスごとにGlastopfを運用する．また，収集したログに含まれるリクエストURL，HTTPヘッダ，HTTPボディを用いて，ダウンロードされるマルウェアやアップロードされる情報を管理者が分析することで，マルウェアの種類や盗まれる情報の詳細といった特徴を抽出する．

3.1　システム設計

システムの構成図を**図6**に示す．観測用IPアドレスを2つ用意し，それぞれでGlastopfを構築した．DNSシンクホールから本来とは異なる観測サーバのIPアドレスを応答することでクライアントからの接続を観測サーバに誘導する．誘導先はDNSシンクホールにて決定する．

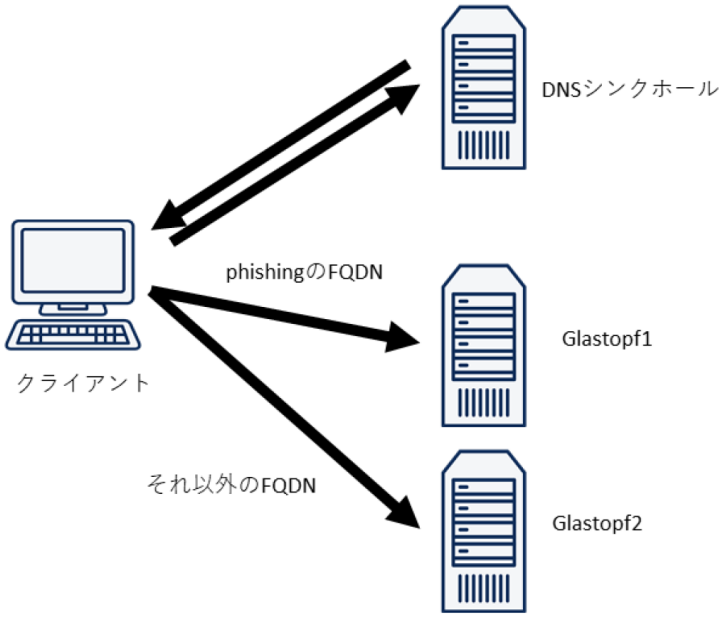

図6　システム構成図

3.2　DNSシンクホール

これまでのDNSシンクホールにおける誘導先は単一（127.0.0.1）であったため，図4に示したゾーンファイルを利用してきた．しかし，本システムでは悪意あるFQDNの分類によって誘導先を変更するため，図5に示したテキストファイル形式のブラックリストから悪意あるFQDNとその分類を抽出し，分類により誘導先を変更したゾーンファイルを作成する．現時点では悪意あるFQDNの分類がphishingであるか，それ以外であるかで誘導先を変更する．誘導先を変更することで，特性にあわせた異なる応答が可能になる．phishingと分類されたFQDNにアクセスを試み

たクライアントは，フィッシングメールに記載されたURLをユーザがクリックしてアクセスを試みた挙動と推測できる．他の分類にはマルウェア配布サイトやC&CサーバのFQDNなどが含まれる．そのようなFQDNへユーザがアクセスすると，マルウェアのダウンロード要求や，ユーザのWeb閲覧履歴やCookieなどのアップロードが考えられる．phishingではユーザのIDとパスワードを盗み出す，そのほかの分類では端末へ悪意のあるファイルをダウンロードさせるなど挙動の違いを考慮した警告をユーザへ提示するため，phishingとそのほかの分類で誘導先を変更した．

現在はすべてのHTTPリクエストに対して，通信を継続させるためのステータスコード"200 OK"とともに危険なサイトへアクセスしていることをユーザに警告するためのページを応答しているが，今後，攻撃の内容を自動的に分析しそれぞれの攻撃に沿って応答することも可能である．たとえば，phishingと分類されたFQDNが示すWebページのスクリーンショットを誘導先サーバが取得し，フィッシングサイトと思われる本来の接続先のスクリーンショットを警告文とともに応答することで，クリックしたURLが示すWebページを安全に確認できるようになる．ほかにも，マルウェア配布サイトからマルウェアをダウンロードするHTTPリクエストと分析した場合，攻撃者に対してダウンロードが成功したように応答し，観測を続けることでダウンロード成功後に攻撃者からどのようなリクエストが送信されるか分析可能となる．また，今後観測を続けることで表1における分類において，ダウンローダであるかアップローダであるかなど異なる挙動を確認できた場合，誘導先サーバを追加することでそれぞれの挙動に沿って応答を変更し，より詳細に分析できるようにすることが考えられる．

3.3　観測サーバ

本システムでは1台の仮想サーバに2つのIPアドレスを割り当て，IPアドレスごとにGlastopfを起動する．2つの観測サーバをGlastopf1，Glastopf2とし，Glastopf1にはフィッシングと思われる悪意あるFQDNへの接続を，Glastopf2にはそれ以外の悪意あるFQDNへの接続を誘導する．ダウンローダ，アップローダと推測される悪意あるFQDNもGlastopf2に誘導する．クライアントがGlastopfに接続した際に表示されるページに，収集したリクエスト内容と警告文を記載することで，ユーザに状況を把握させるよう変更した．誘導後のGlastopf1，Glastopf2でフィッシングの可能性があるサイトへの接続，その他悪意あるサイトへの接続である旨を表示することで，ユーザ自身にて状況を把握できるようになる．Glastopfでは，クライアントからの接続があると，HTTPリクエストの内容をSQLiteのデータベースファイルに保存する．**図7**にデータベースへ保存したリクエスト，**表4**にデータベースの各カラムの説明をそれぞれ示す．

id	time	source	request_url	request_raw
	Filter	Filter	Filter	Filter
338	2020-01-30 18:24:30	133.37.*.*:42670	/favicon.ico	GET /favicon.ico HTTP/1.1Accept: image/web…
339	2020-01-30 18:44:23	202.253.*.*:64479	/l/18358235b03…	GET /l/18358235b03f965b74d5?source=%7Byo…
340	2020-01-30 19:01:19	202.253.*.*:60761	/l/18358235b03…	GET /l/18358235b03f965b74d5?source=%7Byo…
341	2020-01-30 19:24:22	133.37.*.*:43648	/l/18358235b03…	GET /l/18358235b03f965b74d5?source=%7Byo…
342	2020-01-30 19:24:22	133.37.*.*:43648	/favicon.ico	GET /favicon.ico HTTP/1.1Accept: image/web…
343	2020-01-30 19:35:01	133.37.*.*:44080	/l/18358235b03…	GET /l/18358235b03f965b74d5?source=%7Byo…
344	2020-01-30 19:35:01	133.37.*.*:44080	/favicon.ico	GET /favicon.ico HTTP/1.1Accept: image/web…
345	2020-01-30 19:35:30	133.37.*.*:44080	/l/18358235b03…	GET /l/18358235b03f965b74d5?source=%7Byo…

図7　Glastopfが記録するリクエスト内容

表4　データベースの各カラム

カラム名	内容
id	識別子
time	年月日　時刻
source	送信元IPアドレス 送信元ポート番号
request_url	リクエストURL
request_raw	リクエスト行 リクエストヘッダ リクエストボディ

3.3.1　Glastopf1

Glastopf1でクライアント側に表示するページを**図8**に，収集するHTTPリクエストを**図9**にそれぞれ示す．図8では，GET /phishingと実際には存在しないコンテンツを指定したHTTPリクエストを受信して応答している．Glastopf1にはフィッシングの疑いのある悪意あるFQDNへの接続を誘導する．Glastopf1へと接続を試みたクライアントに対して，フィッシングメールなどに記載されたURLへの接続を試みたと考えられるため，接続先のURLとともにフィッシング被害の恐れがある旨の警告文を表示する．図9に図8に示した接続時のHTTPリクエストを示している．

図8　Glastopf1への接続結果

```
GET /phishing HTTP/1.1
～
Connection: keep-alive
Host: mobile.audible.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux
x86_64; rv:65.0) Gecko/20100101 Firefox/65.0
```

図9　Glastop1での収集ログ

本システムではFQDN以降のコンテンツ名からダウンロードされるマルウェアの分析や，リクエストURLやHTTPボディからアップロードされる情報を分析するため，Glastopfを用いた．Glastopf1にてトップページ以下のフィッシングサイトに用いられるページが分析された場合，接続を試みたユーザのみでなく学内全体へ警告を行い，被害を抑制する．

3.3.2　Glastopf2

Glastopf2でクライアント側に表示するページを**図10**に，収集するHTTPリクエストを**図11**にそれぞれ示す．Glastopf2にはマルウェアのダウンロードサーバやクライアントの端末から奪取した情報をアップロードすると推測される悪意あるFQDNへの接続を誘導する．そのため，リクエスト内容をリクエストヘッダのみでなくリクエストボディも含めてユーザのWebブラウザ上に表示する．

図10　Glastopf2への接続結果

```
GET
/malicious/cd+/tmp;cd+/var;wget+http://192.168.0.2/jaw
s+-O+lwodo;sh%25+lwodo;rm+lwodo HTTP/1.1
～
Host: bleachkon.net
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
rv:65.0) Gecko/20100101 Firefox/65.0
```

図11　Glastopf2での収集ログ

3.3.3　観測サーバとしてのハニーポット比較

本システムで観測サーバとして利用するハニーポットとして，GlastopfとSNARE&TANNERを検討した．

本システムでは観測対象をHTTPに限定しているため，現時点においてHTTP以外のプロトコルの情報を収集できる点は考慮していない．HTTPに特化したハニーポットとしては，Glastopfの後継機となるSNARE[18]&TANNER[19]がある．SNAREはWebサーバをエミュレートし，TANNERはレスポンスを作成する．SNAREはインターネット上に公開されているWebページを複製する．実際のWebページと同じ構成になり，リンク先なども複製する．攻撃者がSNAREでエミュレートしたサーバに接続した際に，実在する複製したページを提示するこで攻撃者側からハニーポットであることを推測されにくい工夫がされている．しかし，複製されたページを表示するためユーザが見た際に実際のページが表示されていると勘違いし，誤って複製したページにログインIDやパスワードを入力してしまう可能性がある．また，SNAREでは複製したWebページ構成そのままであるため，SNAREへのリクエストにおいて存在しないコンテンツを指定した場合，“404 Not Found”を応答する．クライアントへ接続の状況を提示するためには，Glastopfのもつ存在しないコンテンツを要求した場合でも設定したコンテンツを返すことができる機能が必要となる．この他にも，Glastopfを採用した理由は，HTTP通信の収集に優れていたためである．GlastopfであればHTTPリクエストのヘッダのみでなくリクエストボディも収集可能であり，本システムで必要な情報を容易に収集できるために採用した．

3.4　実装

本システムを実装し，小規模環境で運用を開始し，動作状況を検証した．従来はサブネット長21のネットワークのクライアントを対象にしていたが，本システムでは同じネットワーク内に新たにフルリゾルバサーバを構築して，サブネット長25のネットワークのクライアントを対象として運用を開始した．検証後，順次対象とするネットワークを拡大する予定である．

新たにフルリゾルバサーバおよび観測サーバを2019年12月2日に設置した．まず，複数のFQDNをフルリゾルバサーバに問合せ，フルリゾルバサーバおよび観測サーバの動作を検証した．検証結果と運用結果を次章で述べる．また，構築したサーバの性能・仕様を**表5**に示す．フルリゾルバサーバ，観測サーバともに仮想計算機で構築した．

表5　各サーバの性能・仕様

	観測サーバ	DNSシンクホール
OS	Debian 8.10.0	FreeBSD12.0
ソフトウェア	Glastopf3.1.2	BIND9.11
CPU	AMD Ryzan 5 2400G	Intel Xeon E5-2640 v4 2.40GHz
メモリ	1GB	8GB
仮想化ソフトウェア	VirtualBox	VMware ESXi

4. 運用結果

4.1　提案システムの動作検証

提案システムの動作を確認するため，正規のFQDNへの接続と悪意あるFQDNへの接続時の様子をWiresharkにてパケットデータを収集しながら動作を検証した．

4.1.1　正常な接続

まず正常な問合せとして，筆者らの研究室のWebサーバへ接続を試みた．DNSシンクホールへの名前解決で正規のWebサーバのIP アドレスが応答され，正規のWebサーバへ接続できることを確認した．

4.1.2　hitnrun.com.my

次にブラックリストに登録されている悪意あるFQDN hitnrun.com.myへの接続を試みた．その結果を**図12**と**図13**にそれぞれ示す．図12はWiresharkで確認した名前解決の応答である．名前解決の結果は観測サーバの持つGlatopf1のIPアドレスである．hitnrun.com.myはphishingに分類されているFQDNであり，観測サーバGlastopf1へ誘導される．観測サーバへ接続した結果を図13に示す．ブラウザに，フィッシングの可能性がある旨をユーザに提示している．また，hitnrun.com.myについて，DNSシンクホールを未設置のフルリゾルバサーバで名前解決して，接続を試みたところ，**図14**に示すような結果となった．図14に示した結果はファイアウォールで接続が拒否されている．また，URLの分類がmalwareとなっていた．観測サーバへの接続時のリクエスト内容を観測することによって，分類についても詳細な検証ができると考えられる．

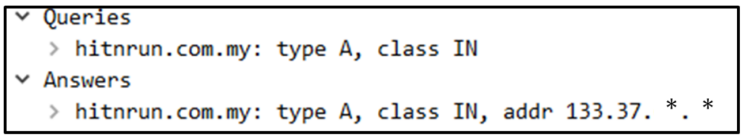

図12　Glastopf1への誘導

図13　hitnrun.com.myへの接続結果

図14　ファイアウォールによるhitnrun.com.myへの接続遮断

4.1.3　izlinix.com，GETリクエスト

他の悪意あるFQDNとしてizlinix.comへの接続を試みた．その結果を**図15**および**図16**にそれぞれ示す．図15に示した名前解決の結果は観測サーバの持つGlastopf2のIPアドレスである．izlinix.comはmaliciousと分類されておりphishing以外の悪意あるFQDNは観測サーバGlastopf2のIPアドレスを応答し誘導する．誘導先に接続した結果を図16に示す．このリクエストはダウンローダがサーバからマルウェアのファイル名を取得する際の通信として報告されたリクエスト[20]を模倣した．このようなリクエスト内容を観測することで，どのような被害があった可能性があるのかなどを分析できる．

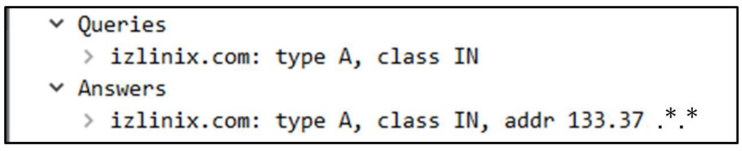

図15　Glastopf2への誘導

図16　izlinix.comへのGETリクエストでの接続結果

4.1.4　izlinix.com，POSTリクエスト

同じ悪意あるFQDNに対してPOSTメソッドでのHTTPリクエストを検証した．その結果を**図17**に示す．この検証ではユーザ名とパスワードを抜き取りアップロードする動作を想定した．観測サーバにてリクエストボディを記録することでユーザ側からどのような情報が奪取されようとしていたのかをユーザに提示する．

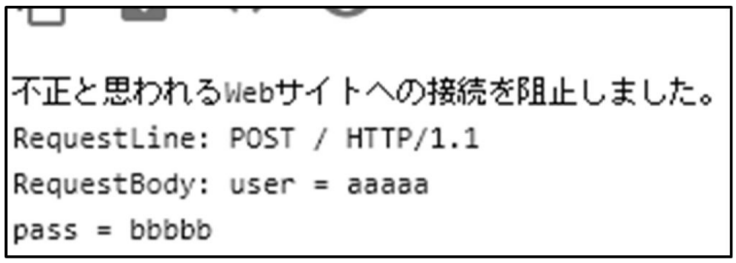

図17　izlinix.comへのPOSTリクエストでの接続結果

4.1.5　意図しないWebブラウザ動作

検証を進めている中で，一部の悪意あるFQDNにおいて意図しない動作を確認したので報告する．例としてupdate-apple.com.betawihosting.netへの接続を試みた結果を**図18**に示す．update-apple.com.betawihosting.netはphishingとしてブラックリストに登録されているFQDNであり，図13と同様のページが表示されると予想し検証を進めていた．今回の検証では，WebブラウザにGoogle Chromeを用いていた．図18では，提案システムからの応答ではなく，偽サイトに接続しようとしていますと警告ページが表示されている．Google safe browsing[21]によって警告が表示され，接続がブロックされていた．Google Chromeにおいては，Google safe browsingによる独自のブラックリストが存在し，ブラウザにてアクセスする前にブラックリストを参照して悪意あるFQDNでないかを判断している．検証結果として，Google safe browsingに登録されているFQDNへ接続を試みた場合，提案システムからの応答ではなく，図18に示した警告ページが表示される．警告ページにおいて，危険性を理解したうえで当該FQDNへの接続することが可能である．警告ページから当該FQDNへ接続を試みた結果，図13と同様に提案システムから応答した内容のページが表示された．

図18　update-apple.com.betawihosting.netへの接続結果

update-apple.com.betawihosting.netはGoogle safe browsingにも登録されているFQDNであった．ユーザがGoogle Chromeを利用しており，Google safe browsingに登録されているFQDNの場合，本システムでの警告ページより先にChromeの警告ページが表示される．この時の通信の様子をWiresharkで確認すると，update-apple.com.betawihosting.netの名前をDNSシンクホールへ問合わせた後，Google safe browsingのAPIサーバの名前も問合わせていた．その後，Google safe browsingのAPIサーバとの通信でブラックリストに登録されているかを確認して，登録されていた場合警告ページを表示していた．その後にGlastopf1とも通信を開始しており，HTTPリクエストの送信とHTTPレスポンスの受信が確認できた．また，Glastopf側でも観測ログが記録されていた．なお，Wiresharkでパケットを収集している際に，Chromeの警告ページを経由して当該FQDNへの Webアクセスはしていない．

update-apple.com.betawihosting.netへのアクセス時の挙動を確認するため，Mozilla Firefox，Microsoft Edgeで検証した．その結果Mozilla FirefoxではGoogle Chromeと同様に警告ページが表示されたが，Microsoft Edgeでは警告ページが表示されず提案システムから応答した内容のページが表示された．

ユーザの利用するWebブラウザによって本システムが想定していない動作が起きることを確認した．しかし，Google safe browsingによりアクセスがブロックされたとしても，本システムでログを収集できるため，管理者の状況把握の点において問題はないと考えられる．また，Webブラウザの警告ページでもユーザが状況を把握できるため，ユーザの状況把握の点においても問題はないと考えられる．ユーザの利用するWebブラウザが異なる場合でも，提案システムを使用することで，組織内のユーザすべてを脅威から守る仕組みとなると考えられる．

4.2　運用結果

本提案システムは，既存の2台のDNSシンクホールとは別に新しくDNSシンクホールを構築した．その提案システムの動作検証後，2019年12月2日から一部ユーザを対象として運用を開始した．現在は試験運用の段階であり，約30台程度のクライアントを対象として提案システムを運用している．2019年12月2日から2020年1月31日までの観測状況を調査した．また，既存のDNSシンクホールの状況についても同じ期間で調査した．既存のDNSシンクホールはサブネットマスク長21のネットワークで約1,000台のクライアントへフルリゾルバサービスを提供している．それぞれの調査結果を**表6**に示す．調査の結果，観測システムではブラックリストに登録されたFQDNの問合せが2件あり，FQDNの分類はphishingであった．そのため通信はGlastopf1へと誘導され，Glastopf1にて悪意あるFQDN宛の通信が6件観測された．観測されたHTTPリクエ

ストの内容を**図19**に示す．今回Glastopf1で観測した通信は本来の接続先への接続を阻止している．さらに，観測されたFQDNを詳しく調査したところ，正規のサイトが改ざんされたと推測されるFQDNであった．今回の観測ではトップページへのアクセスのみであり，改ざんされたコンテンツは確認できなかった．また，User-AgentはExcel2014となっており，このFQDNに対する他のリクエストについてもExcel2014またはofficeとなっていた．これらはExcelのWebクエリ機能による通信であり，ユーザが悪意あるマクロなどが組み込まれたExcelファイルを開きWebクエリ機能が実行されたと考えられる．

表6　観測システムの調査結果

	観測システム	先行研究
期間	2019年12月2日～2020年1月31日	
問合せ総数	2,408,729件	33,062,096件
送信元IPアドレス	37個	849個
悪意あるFQDNの問合せ	2件	7件
悪意あるFQDN	2種類	3種類
悪意あるFQDNを問合せたIPアドレス	1個	4個

```
HEAD / HTTP/1.1
Accept-Auth: badger,Wlid1.1,Bearer
Authorization: Bearer
Connection: Keep-Alive
Host: ***
User-Agent: Microsoft Office Excel 2014
X-Featureversion: 1
X-Idcrl-Accepted: t
X-Ms-Cookieuri-Requested: t
X-Office-Major-Version: 16
```

図19　観測されたHTTPリクエスト

既存のDNSシンクホールと比較すると，問合せ件数，送信元IPアドレス数はともに20倍程の差があった．今後，既存のフルリゾルバサーバを提案システムに置き換え，対象範囲を拡大することで悪意あるFQDNに対する通信観測の件数も増加すると考えられる．ユーザに提示する情報についても機能の追加が必要であると考えられる．たとえば，フィッシングサイトに接続を試みたユーザに対して，観測サーバがユーザの代理で悪意あるFQDNに接続し，その結果を表示させ

る．近年のフィッシングサイトはより正規のサイトに似せたものを作成しているため，接続結果とFQDNを同時に表示させることによって，ユーザが接続先を確認できる機能を実装する．また，FQDNなどから推測してユーザに注意を喚起する機能も実装する．

また，本システムで観測する対象を拡大させるため，現在使用しているブラックリストDNS-BHのほかにファイアウォールで阻止しているFQDNに対してGlastopf1およびGlastopf2への誘導を試みた．ファイアウォールにて阻止している通信のうち，80番ポート宛の接続を試みていた一部のFQDNを学内で運用する別のフルリゾルバサーバのブラックリストに追加した．その結果，4日間で225件のHTTPリクエストがGlastopfサーバで観測できた．観測されたHTTPリクエストのFQDNは1種類であるが，70個の送信元IPアドレスが記録されていた．リクエスト内容を分析したところ，クライアントのOSはiOSもしくはAndroidであり，スマートフォンやタブレット端末の情報を当該FQDNのサーバに送信するリクエストであったことが判明した．

悪意あるFQDNを持つWebサーバへの通信を阻止し，観測サーバにて通信を観測できた．観測サーバで通信を観測することで，コンテンツ名やHTTPボディといったFQDN以上の情報を収集できる．システム管理者がこれらの情報を分析することでマルウェアの種類を特定する手がかりとなる．また，攻撃の傾向などを分析して組織内のすべてのユーザに注意喚起を行い，被害の抑制につなげることが可能である．

4.3 今後の運用

今後は多くのユーザを守るために，カバーする範囲を拡大する予定である．現在，筆者らがネットワークを運用管理する旦野原キャンパスでは，所属学科で独自に設置したDNSシンクホールの他に，キャンパス全体のクライアントを対象としたフルリゾルバサーバ2台がある．今後は運用体制を整えてキャンパス全体をカバーするフルリゾルバサーバに今回構築したDNSシンクホールの仕組みを導入，キャンパス全体で悪意あるFQDNへの通信を防ぐ仕組みを運用する．また，ファイアウォールで阻止した悪意あるFQDNへの通信を，DNSシンクホールのブラックリストに追加する仕組みも開発する．現在観測サーバではHTTP通信のみを観測しているが，それ以外のプロトコルについても観測できる仕組みを検討する．

5. おわりに

本稿ではDNSシンクホールと観測サーバを用いた，悪意あるFQDNに対する通信を観測するシステムを実装した．また，観測システムを検証し，悪意あるFQDN宛の通信誘導と誘導した通信を観測できていることを確認した．現在，小規模な検証環境で運用しており，実際のユーザから悪意あるFQDNへの通信を数件観測できた．誘導後の通信を観測することで，接続を試みたクライアントの挙動などが分析可能になる．実際にどのような情報がアップロードされようとしていたか，どのようなファイルがダウンロードされようとしていたかを実際にマルウェアに感染することなく分析できる．フィッシングメールに記載されたURLをクリックしたユーザに対しては，自身がフィッシング詐欺の被害に遭おうとしていたことを把握させるとともに，観測したホスト名からどのような企業を装っていたかを分析できる．

今後，本システムの適用範囲を拡大するにあたり，大学内のネットワークシステムを運用管理する情報基盤センタと協力していく必要がある．ユーザに何らかのトラブルが発生した場合，連絡先が情報基盤センタとなっているためである．さらに，運用性を高めるため，観測システムに接続したクライアントを定期的に管理者に通知する機能などを実装する．

ユーザへの応答についても機能を追加する．たとえばFQDNの調査で用いたaguse GATEWAYでは，調査するFQDNへの接続結果をスクリーンショットで表示し，接続先の正当性などを確認できる．本システムでもphishingのFQDNへ接続を試みたユーザに対して，本来の接続先のスクリーンショットを取得し，FQDNと同時に表示させる．スクリーンショットを表示することでより容易にユーザが状況を把握できるようにシステムを開発する．

参考文献

1）フィッシング対策協議会：フィッシングレポート2019，https://www.antiphishing.jp/report/pdf/phishing_report_2019.pdf
2）マルウェア情報局：マルウェアレポート，https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1910.html (Oct. 2019)
3）総務省：国民のための情報セキュリティサイト，http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/structure/01.html
4）Guy Bruneau : DNS Sinkhole，https://www.sans.org/reading-room/whitepapers/dns/dns-sinkhole-33523
5）Tapdiya, A. and Fulp, E. W. : Towards Optimal Firewall Rule Ordering Utilizing Directed Acyclical Graphs, icccn, pp.1-6, 2009. Proceedings of 18th International Conference on Computer Communications and Networks (2009).
6）Tanaka, K., Mikawa, K. and Takeyama, k. : Optimization of Packet Filter with Maintenance of Rule Dependencies, IEICE Communications EX-press, Vol.2013, pp.80-85.
7）若林　慶，小林大祐，岡部寿男：トラフィック傾向に基づいたパケットフィルタ型ファイアウォールルール群の再構築，情報処理学会，第81回全国大会，No.3, pp.463-464 (2019年3月16日).
8）神谷和憲，青木一史，中田健介，佐藤　徹，倉上　弘，谷川真樹：Firewallログを用いたマルウェア感染端末の検知手法，第77回全国大会論文集，Vol.2015, No.1, pp.433-434.
9）瀬川　駿，桝田秀夫，森　真幸，永井孝幸：柔軟な応答制御機構を持つDNSサーバファイアウォールの提案と試作，IOT第40回研究会，Vol.2018-IOT-40, No.3, pp.1-6 (2018年3月5日).
10）日経XTECH：DNSシンクホールが明かす，日本を狙う標的型攻撃の実態，https://tech.nikkeibp.co.jp/it/atcl/column/15/101400241/101400002/
11）DNS-BH Malware Domain Blocklist by RiskAnalytics : BH DNS Files, http://www.malwaredomains.com/
12）Virus Total，https://www.virustotal.com/ja/
13）Find Your IP Address and More Free Tools - IPAddress.com, https://www.ipaddress.com/
14）Sucuri SiteCheck - Free Website Malware Scanner, https://sitecheck.sucuri.net/
15）aguse GATEWAY, https://gw.aguse.jp/
16）佐保航輝，池部　実，吉田和幸：DNSシンクホールとハニーポットを用いた不正FQDNに対する通信観測システムの開発，IOT第41回研究会，Vol.2018-IOT-41, pp.1-7 (2018年5月10日).
17）Know Your Tools : Glastopf - A dynamic, lowinteraction Web , application honeypot, http://index-of.co.uk/Various/KYT-Glastopf-Final_v1.pdf
18）Welcome to SNARE's documentation!, https://snare.readthedocs.io/en/latest/index.html
19）Welcome to TANNER's documentation!, https://tanner.readthedocs.io/en/latest/index.html#welcome-to-tanner-s-documentation
20）JPCERT：マルウェアが含まれたショートカットファイルをダウンロードさせる攻撃, https://blogs.jpcert.or.jp/ja/2019/05/darkhotel_lnk.html

21）セーフブラウジング—Google Transparency Report,
https://transparencyreport.google.com/safe-browsing/search?hl=ja

佐保航輝（正会員）hewak.bykoki@gmail.com
2018年大分大学工学部知能情報システム工学科卒業．2020年同大学大学院工学研究科工学専攻知能情報システム工学コース博士前期課程修了．現在は企業にて携帯通信のインフラを活用した移動体通信網およびGPSを活用した移動体管理システムの開発に従事．

池部　実（正会員）minoru@oita-u.ac.jp
2006年奈良先端科学技術大学院大学情報科学研究科博士前期課程修了．2011年同大学情報科学研究科博士後期課程修了．現在，大分大学理工学部共創理工学科知能情報システムコース講師．博士（工学）．ネットワーク運用技術，ネットワークセキュリティ，広域分散処理システムの研究に従事．電子情報通信学会，ACM，IEEE各会員．

吉崎弘一（正会員）kyoshi@oita-u.ac.jp
2001年東北大学大学院理学研究科博士課程修了．現在，大分大学学術情報拠点情報基盤センター准教授．博士（理学）．学習支援システムの開発，情報基盤構築などに従事．教育システム情報学会，CIEC,IMS Global Learning Consortium, IEEE各会員．

吉田和幸（正会員）yoshida@oita-u.ac.jp
1979年九州大学工学部情報工学科卒業．1984年同大学院工学研究科情報工学専攻博士後期課程修了．同年大分大学工学部講師．1986年同助教授，2002年同総合情報処理センター助教授を経て，2008年同学術情報拠点教授．工学博士，ネットワークの運用技術，情報セキュリティに関する研究に従事．電子情報通信学会，日本ソフトウェア科学会，ACM，IEEE各会員．

投稿受付：2019年6月18日
採録決定：2020年4月24日
編集担当：宮下健輔（京都女子大学）