情報処理学会論文誌　コンピューティングシステム　Vol. 2　No. 1　23–32 (Mar. 2009)

アドレスの動的変更による自律防御基盤の設計と実装

黒田大陽[†1]　廣津登志夫[†1]　福田健介[†2]
栗原聡[†3]　明石修[†4]　菅原俊治[†5]

現在，インターネットでは様々な情報やサービスが提供され，社会基盤の一部となりつつある．そのため，悪意のあるユーザやウイルスの攻撃によるサービスの停止は，企業や組織における業務作業の効率やイメージの低下など大きな影響を与える．これらの攻撃への対処には，ファイアウォールや IDS で攻撃を遮断することが一般的である．そのポリシを決定するには攻撃の傾向を知ることが重要となり，その解析の基となる攻撃情報の収集が必須である．本研究では，サーバの防御と攻撃傾向解析の双方の要求を連携させ，サーバのアドレスを動的に変更することにより，サービスの保護と効率的な攻撃情報の収集を同時に行う自律防御基盤を提案する．本稿では，実際の DNS の挙動解析の結果を基にしたサーバアドレスの動的変更ポリシの設計と，アドレスの動的変更を実現する制御基盤の実装について述べる．

Design and Implementation of Network Defense System Using Address Migration

Hiroaki Kuroda,[†1] Toshio Hirotsu,[†1]
Kensuke Fukuda,[†2] Satoshi Kurihara,[†3]
Osamu Akashi[†4] and Toshiharu Sugawara[†5]

The Internet has been used for providing various information and many services, and has been becoming one of infrastructures. As a result, out-of-service by malicious users and viruses inflicts the serious damage on the company. Firewall and IDS have been ordinarily used to protect the service from the attacks. In order to decide the policy, it is important to know the attacks, and is imperative to collect data on the Internet and to analyze attack trend. We propose a network defense system using address migration protection service and attack trend analysis. In this paper, we describe the design of address migration policy by analyzing the cache state on DNS and the implementation of network defense system using address migration.

1. はじめに

現在，インターネットでは様々な情報やサービスが提供され，重要な社会基盤の一部となりつつある．インターネットが一部の研究者のためだけのネットワークから，初心者を含む一般の人々に広く使われるネットワークに変わるにつれ，悪意のあるユーザやウイルスの攻撃による機密情報や個人情報の意図しない流出の問題が深刻になっている．このような問題への対処として，主にファイアウォールによるトラフィック遮断や IDS による異常トラフィックの排除による防御が行われているが，それらの防御ポリシを適切なものにするためには，実際にインターネット上に流れている攻撃を収集・解析することが重要である．これまでの研究では，大規模なアドレス空間を用意して攻撃性パケットを収集し全体的な傾向を把握するか，特定のアドレスにおいて定点観測として状況の推移を追跡することが行われていた．しかし，すべてのサービス提供者が大規模なアドレス空間で攻撃性パケットの収集・解析を行うことは，IP アドレスの枯渇や運用コストを考えると困難であり，また特定の少数のアドレスにおける観測だけでは，効果的な攻撃の観測は難しい．さらに，観測を固定のアドレスで行っていると，攻撃者から観測空間を推定されてしまうという問題がある．

本研究では，各組織が所有するネットワークアドレスの一部を用いて観測を行い，複数の組織が協調することで，全体として広いアドレス空間に対する監視の実現を目指している．この手法は，各組織内で余っている断片アドレスや，DHCP のアドレスプールの使用していない部分を活用してアドレス空間を有効に活用するだけでなく，サーバなどで使用しているアドレス空間の隙間に観測アドレスが配置されることで，より利用環境に近い情報が得られることが期待される．著者らのこれまでの研究[1),2)] での知見として，/24 でアドレス空間を区切った場合に，15 程度離れていても発信元アドレスに対してある程度の相関が得られることが分かっている．また，特定のアドレスにアクセスが集中することも確認されてい

†1 豊橋技術科学大学
Toyohashi University of Technology
†2 国立情報学研究所
National Institute of Informatics
†3 大阪大学/JST CREST
Osaka University/JST CREST
†4 NTT 未来ねっと研究所
NTT Network Innovation Laboratories
†5 早稲田大学
Waseda University

る．そこで，アクセスが集中するアドレスでは収集を行うことでより多くの情報を得られ，また，実際にサービスを提供するアドレスの近くで攻撃性パケットを収集することでより自身のサービスに対する攻撃の特徴を示す情報が得られることが期待される．本研究では，このサービスを提供するアドレス近傍でのデータ収集を実現する手法としてアドレスの動的変更を用いる方法について述べる．ここでは，ある一定幅のアドレス空間の一部をサーバのアドレスとして利用し，これを動的に切り替えることにより，サーバ自体の受ける攻撃を減らし，利用アドレスと観測アドレスを区別しにくくする．本稿では，このアドレスの動的変更を用いてサービスの保護を行う防御基盤の設計と実装について述べる．

2. 背　　景

インターネットにおける攻撃性パケットの収集方法は，大別して能動的方法と受動的方法の2つに分けられる．能動的方法は，Honeypot[3]/Honeynet[4]がこれに相当し，到着したパケットに対して，対応するソフトウェアの挙動を模倣して応答を返す．これにより，攻撃の詳細な挙動を収集したり，ウイルスなどを捕獲したりすることができる．しかし，backscatterといった攻撃に対する余波が外部のネットワークに影響を与える，処理負荷により監視ネットワークを広げられないといった問題がある．受動的方法は，WCLSCAN[5]，ISDAS[6]，警視庁によるインターネット定点観測[7]，Darknetなどの例があり，到着したパケットを収集するだけで応答を返さない．そのため，その他のネットワークに影響を与えず，比較的小さな処理負荷で収集を行うことができる．

インターネット上の攻撃防御方法としては，ファイアウォールやIDSを用いる方法があげられる．前者は攻撃の傾向や提供しているサービスによって，インターネットとの境界部分で特定の通信だけ通過させるようにするものである．後者は，実際のトラフィックのコンテンツを解析し，特徴的なパターン（シグネチャ）などにより攻撃を検知し，攻撃性トラフィックを遮断する．また，DDoS攻撃のような攻撃集中に対しては，上位のネットワーク管理者と協調してより攻撃元に近い箇所でフィルタリングを行うといった対処も行われている．

サーバに複数のアドレスを割り当てたり，アドレスを変更したりする技術は，サーバの負荷分散においては広く使われている．Round-robin DNS[8]は，DNSの問合せに対して複数のAレコードをラウンドロビンに基づいて応答するもので，クライアントのトラフィックを複数のサーバに誘導することができる．これは，負荷の分散を目的としたものであり，途中でアドレスを変更することは考慮されていない．また，Webサーバの性能に応じてクライアントのアクセス負荷を調整する目的で，DNSのTTL値を制御する研究[9),10)]はあるが，異なるアドレスに変更させるためのものではない．CISCO Distributed Director[11]のような負荷分散装置においては，クライアントの位置やネットワークの状況に応じてトラフィックを誘導するサーバを動的に変更するが，通常，DNSキャッシュのTTLを0にしてクライアント側に情報を残さないことで一貫性を実現しようとしている．しかし，TTLを0にするとDNSサーバの負荷が増大するという問題があり，また，実際にはブラウザなどのクライアントが保持するキャッシュにより，サーバの誘導に遅延が生じてしまう．

3. アドレス変更によるサーバの保護

本研究では，IPアドレスの動的な変更によるサービスの保護と，それと並行した攻撃情報の収集を行う．サービスを提供しているIPアドレスを変更することで，特定のアドレスに集中するような攻撃からサービスを保護することができるようになる．しかし，単純にIPアドレスの変更を行うと，通常のユーザもサービスへアクセスできなくなってしまう．これを避けるために，通常のユーザについては特別な操作を行うことなく，変更先のサービスにアクセスできるようにする必要がある．

ここで，一般的なユーザがWebサービスやSSHサービスにアクセスすることを考えると，IPアドレスを用いてアクセスすることはあまりなく，URLやホスト名を利用してアクセスすることが一般的である．一方，悪意のあるユーザのアクセス方法について考えると，URLやホスト名を使わずにIPアドレスを直接利用していると思われる．著者らが行っている受動的方法による収集[1)]に用いたIPアドレスは，インターネット上においてDNSで対応するエントリが公開されているIPアドレスではない．さらに，サービスが提供されていないにもかかわらず，パケットが観測されている．観測されるパケットには，DNSエントリやルーティングの設定ミス，発信元アドレスが詐称されたパケットに対する応答も考えられるが，アクセス頻度やトラフィックの対象アドレス空間の広さを考えると単純なミスが主要因であるとは考えにくい．これにより，悪意のあるユーザがIPアドレスを指定したアクセスを行っていると考えられる．

以上のことから，本研究ではURLやホスト名とIPアドレスを対応付けているDNSエントリを制御することにより，通常のユーザのみを変更先のIPアドレスに誘導する．これに対して，悪意のあるユーザはサービスが提供されているIPアドレスが変更されたかどうかを知ろうとしないため，変更前のアドレスに攻撃し続けると考えられる．さらに，通常のユーザのみを変更先のIPアドレスに誘導してしまえば，攻撃されている変更前のIPアド

レスのアクセスはすべて攻撃と見なすことができ，より効果的な攻撃性パケット収集を行うことができると考えられる．

4. アドレス変更による防御機構の設計

本研究で提案する防御基盤では，あるアドレスの集合に対して，対象アドレスに到着した攻撃性パケットの収集，収集したパケットからの攻撃傾向の解析，アドレス集合から適切なアドレスのサービスサーバへの設定といった処理が必要となる．最初にそれぞれの処理について説明する．

攻撃性パケット収集は，対象アドレス集合に到着するパケットを収集し，保存する．保存されたデータを解析することで，攻撃の原因や今後の対策を立てることができるため，汎用的な形式で保存することが望ましい．また，攻撃傾向を解析し，サーバアドレス変更の判断をする必要があるため，リアルタイムでパケットを処理できる必要がある．

攻撃傾向の解析では，実際に到着しているパケットを解析し，サービスを稼働させているアドレス（以下運用アドレスと呼ぶ）とそれ以外の監視対象アドレスへの攻撃傾向を調べる．運用アドレスに対する攻撃が，他の監視対象アドレスに対する攻撃と比べてある程度より大きくなったときにアドレス制御部にアドレス変更制御の依頼を発行する．

アドレス制御部は，攻撃傾向の解析に従って運用アドレスを危険度の低いアドレスに変更するとともに，対応する DNS エントリを変更する．ここで，攻撃傾向の解析によるアドレス変更の必要性の有無と DNS・アドレス制御の状況から，アドレス変更の手順は以下の 5 つのフェーズからなる．

(1)　通常観測

(2)　攻撃傾向によるアドレスの制御
　さらに攻撃が続いたときに運用アドレスの DNS キャッシュを無効化するため，DNS エントリの TTL を減少させる．

(3)　アドレス変更
　DNS キャッシュ伝播遅延を考慮し，ある程度の期間（アクセス遮断マージンと呼ぶ）は新旧両方の運用アドレスに対するアクセスを受け付ける．アクセス遮断マージンは，DNS キャッシュ伝搬遅延に対処するためのものであり，その値は DNS 伝搬遅延とアプリケーションに含まれるキャッシュによって決定される．

(4)　旧運用アドレスに対する通信遮断
　アクセス遮断マージンを待ってから，新規アクセスを遮断する．継続セッションは通過させる．

(5)　新運用アドレスへの完全移行
　旧運用アドレスへのすべての通信を遮断する．

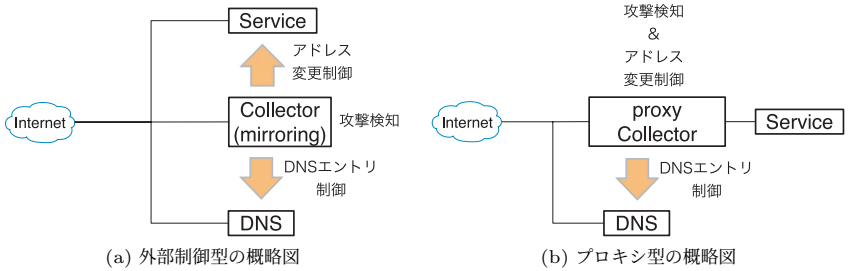


図 1　防御基盤の設計
Fig. 1　Design of the network defense system.

以上の状態の推移を実現するための基盤の構造として，外部制御型（**図 1** (a)）とプロキシ型（図 1 (b)）が考えられる．外部制御型においては，パケット収集は，ルータやネットワーク機器によるポートミラーリングなどの機能を用いて実現する必要がある．運用アドレスの変更における DNS エントリの変更などは，外部からの制御プロトコルを用いることが可能であるが，運用アドレスの変更や通信の制御はサービス運用サーバ上に管理エージェントを導入することが必要となる．この構成はサービスの待ち受けアドレスを任意のローカルアドレスにできるサービスなら任意のものを運用することができるが，サーバ上に特権実行が可能な管理エージェントが必要であったり，ルータやネットワーク機器の支援がなければトラフィックの収集ができなかったりする．

プロキシ型では，収集・アドレス制御サーバがプロキシとしてサービスサーバとインターネットの間に入る．収集・アドレス制御サーバは監視アドレス集合のすべてのアドレスに向かう通信を受け取り，パケットの収集を行う．運用アドレスの変更については，収集・アドレス制御サーバ上の攻撃傾向の解析部の通知で外部の DNS サーバにおける DNS エントリを変更する必要はあるが，インタフェースアドレスの変更，適切なパケットフィルタリングなどの制御はすべて収集・アドレス制御サーバで実現すればよい．この構成ではプロキシ化できるサービスが限られるが，アプライアンス的に収集・アドレス制御サーバを加えるだけでよいという単純さが利点である．

5. DNS キャッシュについての予備評価

DNS を用いてアドレス変更を実現する際，攻撃ではない正当なアクセスに対しては影響を及ぼさないことが望ましい．しかし，Web サーバの負荷分散においては DNS エントリの変更が伝播するのに時間がかかり，DNS エントリの TTL が過ぎても変更前のアドレスに Web アクセスが生じることが知られている[12]．本稿で提案する防御基盤では，この伝播遅延に対応する時間としてアクセス遮断マージンというパラメータを定義しているが，すべての正当なアクセスを阻害しない遮断マージンを設定することは，各アプリケーションごとにアプリケーションの起動・停止を含めた実際のネットワーク環境のすべての動作記録が必要となり，実現は非常に困難である．一方，この遮断マージンは短く設定した方が攻撃回避の効果が大きく出てしまうため，システムの評価のために妥当な遮断マージン値を決める必要がある．そのため，今回は DNS サーバとアプリケーションからなる小規模な実験環境を用いて，DNS キャッシュの予備評価を行った．

DNS キャッシュ伝播遅延は，DNS 参照の中継サーバやリゾルバライブラリにおける DNS キャッシュ破棄までの遅延（DNS レベル遅延と呼ぶ）と，アプリケーションが内部に DNS エントリを保持することによる遅延（アプリケーションレベル遅延と呼ぶ）が考えられる．そこで，まず DNS レベルの遅延が DNS の仕様どおり TTL 未満か確認を行った．実験環境として**図 2** のような構成を用意し，実験に応じたアプリケーションのサーバを 2 つのアドレスで稼働させ，master DNS 上の DNS エントリ（TTL = 60 sec）を変更した際の DNS サーバへの問合せの発生状況とアプリケーションサーバのアクセス状況を調べた．この実験では起動のたびに新しいプロセスが生成され，アプリケーション遅延が発生しないアプリケーションとして telnet を用いた．実験の結果を**図 3** に示す．図では縦軸がアクセスアドレス，横軸が経過時間，矢印線が DNS エントリの変更時刻であり，A，B それぞれのアドレスへのアクセスをプロットし，master DNS サーバに問合せが発生した時刻を縦線で示している．実験の結果，DNS レベル遅延は DNS の仕様どおり TTL 未満であることが確認された．したがって，アプリケーションレベル遅延のないものに対しては DNS の TTL を基準として遮断マージン値を決めればよい．

次にアプリケーションレベル遅延の予備評価を行った．実験環境は DNS レベル遅延の予備評価と同様で，アプリケーションは代表的な Web ブラウザを用い，同一ページの再読み込みを行った場合の DNS 参照とアクセスアドレスを観測した．アプリケーションレベルの DNS キャッシュを破棄するタイミングは，参照回数，参照間隔，キャッシュエントリ作成か

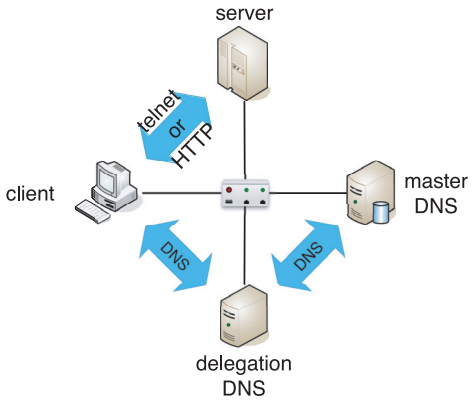


図 2　DNS キャッシュ伝播計測実験環境
Fig. 2　Experimentation environment of DNS cache propagation.

表 1　実験マシン諸元
Table 1　The specification of the evaluation environment.

	master DNS	delegate DNS	server
OS	Ubuntu 8.04		
Software	BIND 9.4.2		apache 2.2.8

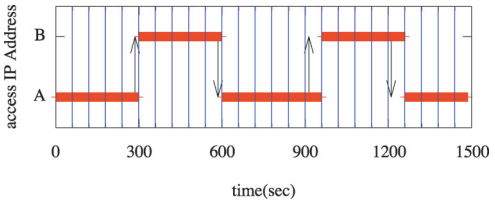
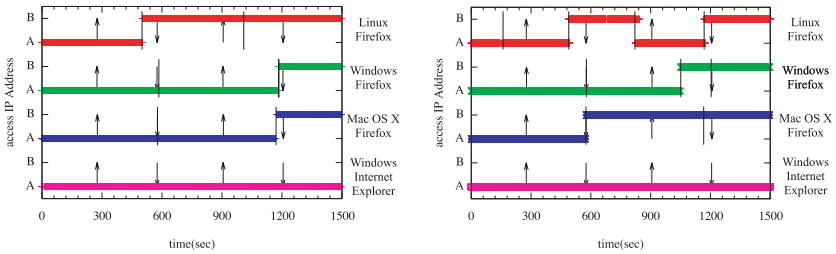
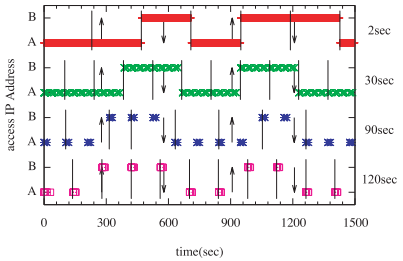


図 3　DNS レベル遅延（Linux，telnet）
Fig. 3　DNS propagation delay on cache servers (Linux, telnet).

らの経過時間など様々な要因があると予想される．そこでまず 5 秒ごとの再読み込みという高頻度のアクセスを調べ，次に再読み込みの間隔を 2 秒，30 秒，90 秒，120 秒というそれぞれのアクセス間隔での状況を調べた．まず 5 秒ごとの再読み込みをブラウザのページキャッシュON と OFF それぞれの設定で，HTML の meta タグを用いた自動再読み込み（meta reload）とブラウザのキャッシュを無視した再読み込み（super reload）の 2 種類について



(a) meta reload 5 sec　(b) super reload 5 sec



(c) meta reload 2, 30, 90, 120 sec (Firefox, Mac OS X)

図 4　アプリケーションレベル遅延
Fig. 4　DNS propagation delay on applications.

調べた．ブラウザは Firefox 3.0 と Internet Explorer 7 で，Linux，Windows XP，Mac OS X の 3 種類の OS を用意した．結果を**図 4** (a) と図 4 (b) に示す．図の見方は基本的には図 3 と同様であるが，縦線が delegation DNS への問合せである点が異なる．上から順に Linux–Firefox，Windows–Firefox，Mac OS X–Firefox，Windows–Internet Explorer の順である．ページキャッシュの設定の違いで挙動が変わらなかったため，ページキャッシュ ON の場合のみを示す．

図 4 (a)，図 4 (b) を見ると，Firefox では DNS 問合せのタイミングは TTL に従っておらず，OS によりタイミングの違いはあるがどの場合もほぼ一定の間隔となっている．また，DNS エントリの更新の間隔とブラウザによるキャッシュ破棄の間隔の関係から，アドレス変更がクライアントに伝わらない事態も見られる．Internet Explorer は，最初のアクセス時を除いて DNS 問合せが発生せず，ブラウザが新しいアドレスにアクセスしないという状態が観測された．再読み込みではなくブラウザを終了して再起動した場合には変更されたアドレスにアクセスに行くことから，標準設定ではブラウザの内部に保持している DNS キャッシュを破棄しないと思われる．これについては，Microsoft が公開している情報[13] によると，ブラウザが保持している DNS キャッシュを破棄するまでのタイムアウトをレジストリに設定することが可能となっており[*1]，対象のレジストリを 60 秒に設定して同様の実験を行ってみた．結果は**図 5** に示すとおりで，Internet Explorer は固定時間で DNS キャッシュを破棄できることが確認された．

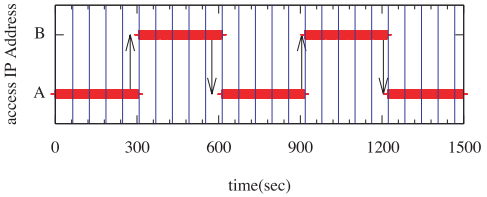


図 5　アプリケーションレベル遅延（Internet Explorer，meta reload，レジストリ操作）
Fig. 5　DNS propagation delay on applications (Internet Explorer, meta reload, registory setting).

表 2　アクセスアドレスが変更されるまでの時間（meta reload）
Table 2　Delay time of changing access address (meta reload).

マージン値（秒）	第 1 変更 誤差(秒)	第 2 変更 誤差(秒)	第 3 変更 誤差(秒)	第 4 変更 誤差(秒)
2 秒	194	133	41	220
30 秒	110	91	42	23
90 秒	*39*	*15*	145	*56*
120 秒	*3*	*124*	*75*	*56*

一方，Firefox の挙動については，何が要因なのかが判然としない．そこでアクセス間隔を変えて同様の実験を行った．OS は 5 秒間隔でのアクセスの際に DNS サーバへの問合せの間隔が大きかった Mac OS X を用いた．結果は図 4 (c) に示したとおりで，上から 2 秒，30 秒，90 秒，120 秒の間隔におけるアクセス状況である．**表 2** はアドレス変更を行ってからアクセスされるアドレスが変更されるまでの誤差を表しており，斜体字はアドレス変更を行ってから最初のアクセスが変更先のアドレスにアクセスしている場合を示している．これを見ると，アクセス頻度が高いときは約 240 秒間隔で DNS キャッシュを更新していると考えられる．アクセス頻度が下がってくると，90 秒間隔ではタイミングによって DNS キャッシュを使っていると思われるが，120 秒間隔では毎回 DNS の問合せを行っており，90 秒か

⋆1 この文書で Internet Explorer 7 は対象に含まれていない．

ら 120 秒の間の時間でキャッシュを破棄しているものと考えられる．以上の予備評価の結果から，システム評価の遮断マージン値には DNS の TTL，120 秒，240 秒の 3 種類を用いることにする．

6. システム実装

4 章の設計に基づき，アドレス変更による防御基盤を実装した．今回は分散システムとしての機能のモジュール性や既存サーバとの親和性を考慮してプロキシ型で実装した．proxy 機能は pound [14] を利用し，パケット収集部や攻撃傾向の解析部，アドレス変更制御部は Ruby を用いて実装した．ここでパケット収集・解析機能として Ruby の拡張ライブラリである Ruby/Pcap を用いた．これにより，収集したパケットを tcpdump 形式で書き出すことが可能であるため，後に解析を行う際に汎用性が高い．システムの概略図は**図 6** に示すとおりで，今回 Ruby により実装した部分は破線の枠内である．

攻撃検知には，トラフィック変動やコンテンツ解析など多様な手法がある．ここでは，一定時間に到達したパケット数がある閾値を超えた場合に，攻撃と見なすポリシを用いた．具体的には各アドレスごとにある一定時間（たとえば 10 分）に到着するパケット数をカウントし，直前のカウントと現在のカウントの多い方のカウントを危険値として記録する．危険

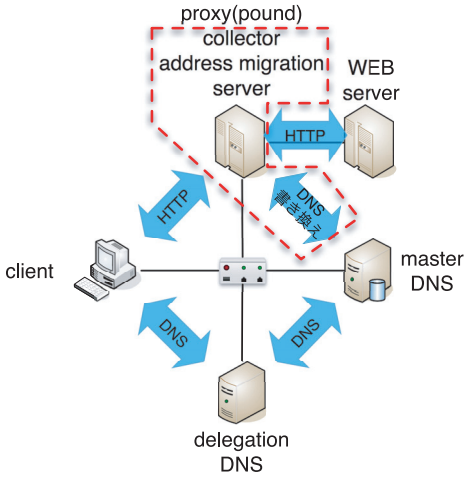


図 6　実装システム概略図
Fig. 6　Overview of the system.

値が warning として設定された閾値を超えると，対応する DNS エントリの TTL の値を半分にするように通知する．さらに攻撃が継続され，危険値が alert として設定された値を超えたら，アドレスの変更を通知する．その際における変更先アドレスは，その時点で最も危険値の低いアドレスとした．

DNS エントリの書き換えは，攻撃検知から warning もしくは alert の通知が来た場合に実行される．warning の場合には，対象の DNS エントリを持つ DNS サーバに対して “nsupdate” を実行し，対象の DNS エントリの TTL を減少させる．alert の場合には，warning と同じく対象の DNS エントリを持つ DNS サーバに対して “nsupdate” を実行し，変更前のアドレスを持つエントリを削除し，新たに変更先のアドレスを持つエントリを作成する．

アドレス変更については，監視アドレス集合すべてのアドレスをインタフェースに付与しておく．そして，pound の対象を監視アドレス集合すべてにすることで，運用アドレスへの接続をすべてサービスサーバに転送できる．したがって，特定の運用アドレスを決めることはそれ以外のアドレスをファイアウォールで遮断することに相当し，遮断するアドレスを変更することでアドレス変更が実現される．攻撃傾向の解析部から，alert が通知されると，変更先のアドレスに対するアクセスを許可するようにファイアウォールポリシを変更する．そして，アクセス遮断マージン値に合わせて，変更前のアドレスに対する新しいセッションを発生させないために，変更前のアドレスに対する SYN パケットを破棄するようにファイアウォールポリシを変更する．そして，変更前のアドレスに対するセッションがすべてなくなったことを確認した後に，変更前アドレスに対するすべてのパケットを破棄するようにファイアウォールポリシを変更する．

7. 評　　価

今回実装した防御基盤は，実際の攻撃収集環境内ですでに稼働しているが，収集された攻撃データ量が十分に多くないため，著者らがこれまでに Darknet で収集してきた攻撃データのアクセスパターンを用いて，DNS を用いずにアクセスしてくる攻撃性パケットに対してどの程度削減できるかについて評価を行った．収集データは tcpdump 形式で保存されており，実装した防御基盤は Ruby/Pcap により tcpdump 形式を扱うことができるため，実装したシステムに収集データの時刻情報を用いるように改造し，直接収集データを読み込んで動作のシミュレーションを行った．

ここでは，攻撃を受けた場合の回避効果を調べるのが目的であるので，評価は事前に 3 カ月間のパケットデータを解析し，Web（TCP 80 番）に対して最も多数のパケットを受け

ている 1 日分と 3 カ月すべてのデータについて評価を行った．それぞれのデータセットに対するサーバの初期運用アドレスは，1 日分については対象パケットが最も多かったアドレス，3 カ月分については対象パケットが最も多かったアドレスから上位 4 つを選択し，4 回シミュレーションを行った．評価に用いたデータは，初期アドレスを含むプレフィックス長 24 bit（/24，256 台分）のアドレス範囲とした．また，攻撃検知の際のパケット集計単位は DNS エントリの TTL の値である 60 秒の 10 倍の 600 秒（10 分）とし，攻撃と判定する閾値は対象データを事前に解析して，初期運用アドレスに対して到着する対象パケット数を 10 分間隔でカウントを行い，その中から上位 10%に位置する値を用いた．また，遮断マージン値は 5 章の予備評価の結果から 60 秒，120 秒，240 秒のそれぞれを設定し，シミュレーションを行った．

それぞれの拠点の 1 日分のシミュレーション結果を**表 3** (a) と表 3 (b) に示す．この表は，無変更はアドレス変更を行わなかった場合，すなわち Darknet データで初期運用アドレスが受けた攻撃パケット数を表し，各々のアドレス遮断マージン値に対する結果は，初期運用アドレスと変更先アドレスに到着した対象パケット数の合計と，アドレスを変更しなかった場合と比較した削減率を示している．この結果から，収集地点の違いで削減率に差異が見られるが，どちらにおいても攻撃性パケットの削減を確認できた．

次に 3 カ月分のデータに対するシミュレーション結果を表 3 (c) と表 3 (d) に示す．表の上から，アドレス遮断マージン値，アドレス変更回数の最低値，アドレス変更回数の最高値，アドレス変更回数の平均値，削減率の最低値，削減率の最高値，削減率の平均値を示している．この結果から，1 日分のデータと同様に収集地点により削減率に差異が見られるが，どちらにおいても対象パケットの削減を確認できた．また，1 日分と 3 カ月分のデータでは期間が長い 3 カ月の方が削減率が高くなっている．今回は閾値に初期運用アドレスに対して到着する対象パケット数を 10 分間隔でカウントを行い，その中から上位 10%に位置する値を用いている．そのため，データセットの期間が長くなることで，対象カウント数が増え，全体として閾値が低くなってしまったことが考えられる．しかし，これらの結果から期間が短期，長期にかかわらず運用アドレスを変更することで攻撃を回避できていることが確認できた．また，アドレス変更範囲をプレフィックス長 23 bit（/23，512 台分）と 25 bit（/25，128 台分）とした場合においてもほぼ同様の削減率が得られ，組織の余剰アドレス程度でもアドレスを変更することによる攻撃性パケットの削減効果を得ることができるといえる．

表 3　アドレス変更の効果
Table 3　Effect of address migration.

(a) site A，Darknet，1day

マージン値（秒）	合計対象パケット数	削減率（%）
無変更	7,158	-
60	5,870	18.0
120	5,891	17.7
240	5,923	17.3

(b) site B，Darknet，1day

マージン値（秒）	合計対象パケット数	削減率（%）
無変更	11,649	-
60	3,937	66.2
120	4,174	64.2
240	4,474	61.6

(c) site A，Darknet，3months

マージン値（秒）	60	120	240
最低アドレス変更回数	1	1	1
最高アドレス変更回数	2	2	2
平均アドレス変更回数	1.5	1.5	1.5
最低削減率（%）	72.0	71.9	71.7
最高削減率（%）	96.5	96.5	96.5
平均削減率（%）	84.2	84.1	83.9

(d) site B，Darknet，3months

マージン値（秒）	60	120	240
最低アドレス変更回数	1	1	1
最高アドレス変更回数	1	1	1
平均アドレス変更回数	1	1	1
最低削減率（%）	99.0	99.0	99.0
最高削減率（%）	99.7	99.7	99.7
平均削減率（%）	99.4	99.4	99.4

8. 考　　察

従来，攻撃対策ポリシの設定はセキュリティ情報を提供する機関などから攻撃傾向の情報を得て行っていたが，必ずしも自身が運用するネットワークにおいて有効な情報ではなかったり，より詳細な情報を得るために自身で大規模な観測アドレス空間を運用することは多大なコストが必要であったりした．一方，今回実装したアドレスの動的変更を用いた防御基盤を用いることで，組織内に割り当てられているアドレス空間を利用し，大きなコストを必要とすることなく管理するネットワークに即した情報とサービスの保護を得ることができるといえる．

次に提案した防御基盤の評価について考える．今回，評価に用いたデータは 2 カ所のアドレス空間で収集された Darknet のデータを用いた．この収集データに含まれるパケットは，広報していないアドレス空間に対して送信されているものであり，DNS を用いずに直接 IP アドレスを利用した攻撃性パケットであるといえる．この収集データから，アドレスを変更することで攻撃性パケットを削減させることが確認できた．

次にアドレスの動的変更について考える．通信セッションの継続性を保つ技術として Mobile IP [15] があげられる．Mobile IP は，ノードに一意の IP アドレスを割り当てることで，ネットワークを切り替えても通信セッションを継続することが可能になる．Mobile IP を用いることでアドレスの動的変更を行うことが可能であるが正常な通信パケットと攻撃性パケットの両方を転送してしまうため，目的であるサービスの保護を行うことができない．

本稿で提案する機構の基本アイデアは，Darknet や Honeynet には DNS 問合せを行わずに攻撃性パケットだけが到達していることを逆手にとったものである．したがって，DNS を用いることで正規のユーザのパケットのみを転送し，IP アドレスを直接利用した攻撃性パケットは転送しないアドレスの動的変更を達成することが可能になったといえる．

次に観測アドレス空間を探索する攻撃について考える．インターネット上の攻撃傾向を把握するために，攻撃性パケットを収集することは重要である．しかし，いくつかの研究[16),17)]では，攻撃性パケットを収集している観測アドレスを探し出せることを指摘している．観測アドレスが特定されてしまうと，悪意のあるユーザが正しい情報が得られないように虚偽のデータを紛れ込ませるなどの攻撃が行われる可能性がある．今回実装した防御基盤では，観測アドレスとサービスを提供する運用アドレスが混在しており，またそれらのアドレスが不定期に入れ替わっていくため，従来の観測だけを行っている空間を探索するより，探索は困難になると考えられる．また，多地点の断片アドレスを連携してサーバアドレスと観測アドレスを入れ替えたり，協調解析を行うことで，観測環境を探知しようとする攻撃自体の検知も容易になることが期待される．

本研究で提案した防御基盤は，DNS キャッシュの伝播によりユーザのアクセスが阻害されたり，すでに確立している通信を遮断しないような配慮は行っている．一方で，アプリケーションや OS が保存している DNS キャッシュの挙動により，ユーザに影響を与える可能性を完全には排除できない．提案したシステムではアクセス遮断マージンとしてこの影響に対応できるようにしているが，マージン値の設定が実際にどの程度のユーザの処理に影響を及ぼすかを調査するためには，トラフィックだけでなくすべてのアプリケーションの挙動を追跡する必要があり，すべてを解析することは困難である．本提案で用いている DNS を用いたアドレス変更が実際の利用に影響を与えるかどうかは，アプリケーションの実装に大きく依存する問題である．実際，予備評価で調べた主要なブラウザの挙動においても，ある程度の期間，クライアントがアドレス情報を保持していることは確認された．しかし，ブラウザを停止して再起動すれば新しい情報を構築するので，現在の実装でも影響は限定的であると考えられる．また近年，DNS ラウンドロビンを用いた負荷分散や Dynamic DNS などの動的なアドレス変更に対応するために，保持しているアドレス情報を用いての接続に失敗したら，再度アドレス情報を取得し直す実装が増えている．実際，予備評価と同じ実験で，アドレス変更時に変更前のアドレスへのアクセスを遮断すると，クライアントは新たなアドレスにアクセスを行う．したがって，将来的には本手法のような DNS を用いた動的変更により影響を受けるクライアントは少なくなっていくことが期待される．

最後にアドレス移動の判定基準について考察する．本稿では，アドレス変更機能の実現とそれにより攻撃性パケットがどの程度削減されるかに主眼があったために，アドレス移動の判定基準は Darknet のデータセットを事前に解析して設定した．このデータには正規の通信は含まれていないが，実際に本システムを運用する段階では，攻撃性パケットと正当なサービスリクエストの混在したトラフィックの中から，攻撃を受けている危険度の判定を行わなければならない．これに対する 1 つの方法としては，あえてアドレス変更を発生させ正当なサービスリクエストだけを追従させるという方法が考えられる．また，本提案手法ではアドレス変更に対して正当なアクセスは追従してくる仕組みのため，アドレス変更によるフィルタリングと考えることができる．また，本提案手法では特定の攻撃判定手法によらないので，IDS などでの攻撃検知技術を応用することも可能である．仮に攻撃を誤検出してアドレス変更が起こってしまっても正当なアクセスは追従してくる仕組みなので，攻撃判定の閾値などのパラメータ設定については通常の IDS よりも容易であると考えられる．

9. ま と め

本稿では，インターネット上における脅威からサービスを保護するために，大規模な観測アドレス空間を用いることなく，組織内のアドレス空間で情報収集を行い，アドレスの動的変更によってサービスを保護する防御基盤の設計と実装を行った．また，DNS キャッシュの DNS レベル遅延とアプリケーションレベル遅延を確認し，シミュレーションによって本提案手法の効果について確認を行った．これにより，実際の攻撃状況に動的に対応し，サービスの運用を続けるとともにより多くの攻撃性パケットの収集を行うことが可能となった．今後の課題として，複数の観測拠点での運用による効果の確認などがあげられる．

謝辞　この研究は科学研究費補助金特定領域研究「情報爆発時代に向けた新しい IT 基盤技術の研究」の支援を受けている．

参 考 文 献

1) 廣津登志夫，福田健介，栗原　聡，明石　修，菅原俊治：断片アドレスを用いた分散協調インターネット監視に関する一考察，*SWoPP* (2007).
2) Fukuda, K., Hirotsu, T., Akashi, O. and Sugawara, T.: Correlation among piecewise unwanted traffic timeseries, *Proc. IEEE Globecom* (2008).
3) Honeyd: Developments of the Honeyd Virtual Honeypot. http://www.honeyd.org
4) HoneynetProject: Know your Enemy: Honeynets (2005). http://www.honeynet.org/papers/honeynet

5) Ishiguro, M., Suzuki, H., Murase, I. and Ohno, H.: Internet Threat Detection System Using Bayesian Estimation (2004).
6) JP/CERT: ISDAS：インターネット定点観測システム．http://www.jpcert.or.jp/isdas
7) @police：インターネット定点観測．http://www.cyberpolice.go.jp/detect/observation.html
8) Allbitz, P. and Liu, C.: DNS & BIND 第 4 版，O'REILLY (2002).
9) Colajanni, M., Cardellini, V. and Yu, P.S.: Dynamic Load Balancing in Geographically Distributed Heterogeneous Web Servers, *18th International Conference on Distributed Computing Systems*, pp.295–302 (1998).
10) 小野村哲也，齊藤智也，稲井　寛：DNS ラウンドロビンにおける TTL 値算出法，電学論 C，Vol.124, No.3, pp.827–834 (2004).
11) CISCO: Distributed Director. http://www.cisco.com/
12) Pang, J., Akella, A., Shaikh, A., Krishnamurthy, B. and Seshan, S.: On the Responsiveness of DNS-based Network Control, *Proc. ACM IMC'2004* (2004).
13) Microsoft: Microsoft サポートオンライン．http://support.microsoft.com/kb/263558/ja
14) POUND: REVERSE-PROXY AND LOAD-BALANCER. http://www.apsis.ch/pound/index_html
15) mobileip wg: RFC3344: IP Mobility Support for IPv4. http://tools.ietf.org/html/rfc3344
16) Shinoda, Y., Ikai, K. and Itoh, M.: Vulnerabilities of Passive Internet Threat Monitors, *14th USENIX Security Symposium*, pp.209–224 (2005).
17) Cooke, E., Bailey, M., Jahanian, F. and Morier, R.: The Dark Oracle: Perspective-Aware Unused and Unreachable Address Discovery, *3rd Symposium on Networked Systems Design & Implementation* (2006).

(平成 20 年 7 月 23 日受付)
(平成 20 年 11 月 15 日採録)

黒田　大陽

2007 年豊橋技術科学大学工学部情報工学課程卒業．現在，同大学大学院情報工学専攻在学中．ネットワークに関する研究に従事．

廣津登志夫（正会員）

1995 年慶應義塾大学大学院理工学研究科計算機科学専攻博士課程修了．同年日本電信電話株式会社入社．2004 年より豊橋技術科学大学情報工学系准教授．分散システム，OS，ネットワーク，ユビキタスシステム等の研究に従事．博士（工学）．日本ソフトウェア科学会，ACM，IEEE-CS 各会員．

福田　健介

1999 年慶應義塾大学大学院理工学研究科計算機科学専攻後期博士課程修了（博士（工学））．同年日本電信電話株式会社入社以来，未来ねっと研究所に所属．この間 2002 年ボストン大学訪問研究員．2006 年より国立情報学研究所アーキテクチャ科学研究系准教授．2008 年より科学技術振興機構さきがけ研究員（兼任）．学術情報ネットワーク，インターネットおよびネットワーク科学に関する研究に従事．

栗原　　聡（正会員）

1992 年慶應義塾大学大学院理工学研究科計算機科学専攻修士課程修了．同年日本電信電話株式会社入社．基礎研究所を経て未来ねっと研究所に所属．1998 年から慶應義塾大学大学院政策・メディア研究科専任講師（有期）．現在同大学環境情報学部非常勤講師．2004 年から大阪大学産業科学研究所知能システム科学研究部門准教授（同大学大学院情報科学研究科情報数理学専攻准教授兼務）．マルチエージェント，ネットワーク科学等の研究に従事．著書『社会基盤としての情報通信』（共立出版，共著）．翻訳『スモールワールド』（東京電機大学出版局，共訳）．編集『Emergent Intelligence of Networked Agents』（Springer in Computational Intelligence Series）等．博士（工学）．人工知能学会，日本ソフトウェア科学会，ESHIA 各会員．

明石　　修（正会員）

1987 年東京工業大学理学部情報科学科卒業．1989 年同大学大学院理工学研究科情報科学専攻修士課程修了．同年日本電信電話株式会社入社．以来，分散システム，ネットワークアーキテクチャ，マルチエージェントシステム等の研究に従事．現在，NTT 未来ねっと研究所主幹研究員（特別研究員）．博士（理学）．ACM，日本ソフトウェア科学会各会員．

菅原　俊治（正会員）

1982 年早稲田大学大学院理工学研究科数学専攻修士課程修了．同年日本電信電話公社入社（武蔵野電気通信研究所基礎研究部）．以来，知識表現，学習，分散人工知能，マルチエージェントシステム，インターネット等の研究に従事．1992〜1993 年，マサチューセッツ大学アマースト校客員研究員．現在，早稲田大学基幹理工学部情報理工学科教授．博士（工学）．日本ソフトウェア科学会，電子情報通信学会，人工知能学会，AAAI，ISOC，IEEE，ACM 各会員．