未知の不正 Web サイト判別のための IP アドレスクラスの特徴分析

金澤 しほり[†1]　中村 嘉隆[†2]　稲村 浩[†2]　高橋 修[†2]

概要：近年，Drive-by download 攻撃やフィッシングなど Web サイトを介したサイバー攻撃が急増しており，ユーザの個人情報等が不正に取得され，経済的被害を受ける事件が増加している．このような被害を防ぐために，ユーザが不正 Web サイトを閲覧する前に，Web ブラウザやセキュリティソフト側で警告を促す対策を講じている．本稿では，未知の不正 Web サイトの判別を行うために，IP アドレスクラスのネットワークアドレス部の特徴を分析し，交差検定によって評価した．IP アドレスクラス A と B では，高精度の結果が得られたことから，ネットワークアドレス部を用いた判別は，有効であることが確認できた．

キーワード：サイバー攻撃，不正 Web サイト，ネットワークアドレス， IP アドレスクラス

A feature analysis of the IP address classes for detection of unknown malicious Web sites

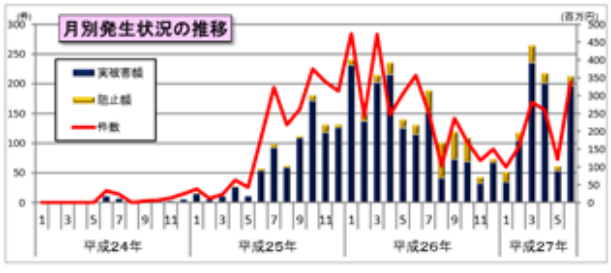
Shihori Kanazawa[†1]　Yoshitaka Nakamura[†2]
Hiroshi Inamura[†2]　Osamu Takahashi[†2]

Abstract: In recent years, cyber attacks through web sites such as Drive-by download attacks or phishing attacks increase rapidly. The attackers acquire personal information of users illegally by these attacks and inflicts economical damage. It is necessary to prompt warning messages in Web browser or security software before users browse malicious web sites to prevent these damages. In this paper, We analyzed features of the network address part of the IP address class to distinguish unknown malicious Web sites. In addition, we evaluate by cross-validation. As a result of evaluation, high distinction precision was provided in IP address class A and B. From this result, we confirm the effectiveness of the proposed distinction method.

Keywords: cyber attack, malicious web site, network address, IP address class

1. 背景

近年，Web サイトを利用した攻撃が急増している．攻撃例として，ユーザが Web サイトを閲覧した際に，ウイルスやマルウェアなどの不正プログラムをパソコンにダウンロードさせる Drive-by download 攻撃や，金融機関を装った偽のサイトへ誘導するフィッシング詐欺が挙げられる．これらの攻撃法により，閲覧者のパソコンでマルウェアが活動し，保管されたデータやプログラムが破壊されることや，暗証番号やクレジットカード番号などの個人情報を不正に取得され，経済的な被害を受ける事件が増加している．2011 年から 2015 年までの警察庁広報資料「インターネットバンキングに係る不正送金事犯発生状況」によると，個人情報が不正に取得されて被害に遭った 2012 年までの発生件数が 50 件程であったのに対し，2015 年には 1400 件近くまで急増しており，現在も増加傾向にある[1]．このような被害を防ぐために，ユーザが危険な不正 Web サイトを閲覧して被害に遭う前の Web アクセス時に注意を促すような対策が用いられている．例えば，Web アクセス先が不正 Web サイトである場合，ユーザに警告を促し，ユーザ自身でアクセスを止めさせる方法などが利用されている．しかし，このような警告を行うことができるのは既知の不正 Web サイトに対してのみあり，未知の不正 Web サイトに関しては対策が難しい．そのため，今後は未知の不正 Web サイトを含めた対策が重要となる．



出典：警察庁広報資料

図 1 インターネットバンキングに係る不正送金事犯の発生件数

これまでに，不正Webサイトへのアクセスを遮断するため，Webレピュテーション，Intrusion Prevention System（IPS，侵入防止システム）といった技術が開発され，対策手法と

†1 公立はこだて未来大学大学院　システム情報科学研究科
Graduate School of Systems Information Science, Future University Hakodate
†2 公立はこだて未来大学　システム情報科学部
School of Systems Information Science, Future University Hakodate

して用いられている．

Web レピュテーション技術[2]は，不正 Web サイトブロック機能を持つソフトウェアで実現されている．ユーザによる Web アクセス通信が発生する際に，接続先のドメインや Web サイトが不正な場合にはアクセス自体をブロックすることに Web サイトが不正であると判断される場合には，そのアクセス自体をブロックすることによって，不正プログラムによる感染，およびフィッシングによる被害を防止している．しかし，不正 Web サイトとして判断される条件は，ウイルス配信，フィッシング詐欺など，不正行為を行ったことが確認された Web サイトのみである．

Intrusion Prevention System(IPS) [3]は，ファイアウォールやアンチウイルスだけでは防御が困難とされていた DoS 攻撃やボットなど巧妙かつ高度なセキュリティの脅威に対応しており，通信パケットの内容や振る舞いを検査し，不正な通信を検出した後，遮断を行う．このとき，Web サイトへアクセスが行なわれた際に，通信パケットに含まれる不正な通信を検出して，遮断する仕組みになっている．しかし，IPS は，Web アクセス通信に含まれる既知の不審パケットのみ検出している．

前述した 2 つの既存技術は，既知の不正 Web サイトや不正 Web サイトに含まれる既知の不審パケットなどの既知の情報を用いているため，既知の不正 Web サイトの検出率が高いという利点がある．しかし，欠点として，未知の不正 Web サイトに対応した検出ができず，仮に検出出来た場合であっても，十分な精度が得られるか不明である．

このような問題点を解決するために，未知の不正 Web サイトを含めた検出ができる検出条件を考慮し，検出された Web サイトを既知の Web サイトか未知の Web サイトのどちらかに分類した上で，未知の Web サイトに対して正規 Web サイトか不正 Web サイトを判別する手法を提案する．

2. 関連研究

既存技術では，既知の不正 Web サイトと Web アクセス先の Web サイトを照合して，一致した Web サイトを検出する仕組みになっており，既知の不正 Web サイトの検出率は高いが，一方で未知の不正 Web サイトに関しては考慮されていない問題点がある．この問題点に対して，既知の不正 Web サイトの特徴を用いて未知の不正 Web サイトを検出する手法[4,6]や，判別する手法が提案されている[8]. Web アクセス時の通信パケットやドメイン名，TTL(Time to Live)値などから不正 Web サイトの特徴を抽出して，不正の疑惑がある Web サイトと照合することで，類似した特徴を持った未知の不正 Web サイトを検出している．また，上記の情報(ドメイン名や IP アドレスなど)は，Domain Name System(DNS)から得られる．DNS は，あらゆる Web サイトのアクセス元とアクセス先を把握しており，ドメイン名や IP アドレスといった各 Web サイトの情報を一元管理しているため，未知の不正 Web サイトに対しても有効な情報を保持していると考えられる．そこで，DNS から得られる情報(DNS 情報)に着目する．

2.1 検出手法

劉ら[4]は，DNSから得られる情報のうち，不正Webサイトに見られる特徴を条件に用いて検出を行っている．不正Webサイトのドメイン名は，英数字と数字が混在するものが多い傾向があるため，英数字が混在するドメイン名を利用しているかどうかを1つ目の検出条件としている．不正Webサイトのドメイン名は，ボットに感染したパソコン群(ボットネット)を利用してフィッシングやウイルス配布などを行うFast-Flux[5]などの攻撃手法を用いて自動生成されることが多いため，人間にとって扱いにくい10文字以上の長い文字列で構成されるものが多い．このため，10文字以上で構成されるドメイン名であることを2つ目の検出条件としている．また，DNSキャッシュに設定されているパケットの有効期間を表す生存時間(TTL値)として設定された時間を超えた場合に，該当するDNSキャッシュのデータを保持しているネームサーバはDNSキャッシュを破棄することで，データベースの整合性を維持している．生存時間を短くすると，キャッシュが即座に無効になり，最新のデータを頻繁に問い合わせることになるが，不正Webサイトでは，TTL値を小さく設定することで，ドメイン名を捕捉されにくくしている傾向があるため，TTL値が300秒以下のドメインであるかどうかを3つ目の検出条件としている．これら3つの検出条件のいずれかに該当するWebサイトを不正Webサイトとして検出している．

田中ら[6]は，マルウェアが通信を行う際の特徴を利用して，DNS 通信の観測によって未知の不正 Web サイトの検出を行っている．通信を行うマルウェアに感染しているクライアントは複数の不正 Web サイトにアクセスを行う傾向にあるため，不正 Web サイトにアクセスを行ったクライアントは，他の不正 Web サイトにもアクセスを行っている可能性が高い．そのため，DNS 通信において既知の悪性ドメインにアクセスを行っていたクライアントから名前解決要求のあるドメインは，マルウェアとの関連が深いドメインであると考えられるため，未知の不正 Web サイトとして検出している．

しかし，これらの検出手法は，ユーザが Web サイトにアクセスする際に，各特徴を利用した検出条件を満たす Web サイトのみを検出しているため，検出できる不正 Web サイトが限定される．

2.2 判別手法

千葉ら[7]は，IPアドレス，FQDN(Fully qualified domain name)文字列，ドメイン名の登録日の3つの情報から特徴を抽出し，分類器によって不正Webサイトを判別する手法を提案している．まず，悪質な活動に利用されるIPアドレスが一部のネットワークに密集する傾向にあることから，IPアドレスの構造的な特徴を利用している．FQDN文字列とは，ホスト名とドメイン名を省略せず繋げて記述した文字列のことであり，このFQDN文字列が，文字をランダムに組み合わせて構成されている場合は不正Webサイトである傾向が強いことから，FQDN文字列構成も抽出する特徴として利用している．また，新しいドメイン登録日を持つWebサイトの方が，悪性度が高い傾向があることから，ドメインの鮮度も抽出する特徴としている．これらの特徴のうち，IPアドレスを用いた判別が，FQDN文字列やドメイン名の登録日よりも有効であることが判明している．このことから，千葉ら[8]は，大学で用いているネットワークから実際にアクセスが行なわれたWebサイトへの通信を収集し，IPアドレスを用いた判別手法を適用して評価実験を行っている．収集したWebサイトのIPアドレスから先頭8~32ビットごとに特徴を抽出し，分類器に適用して判別を行っている．しかし，既知の不正Webサイトと正規Webサイトも判別対象としており，また，IPアドレスの全てのビットを用いて判別を行っているため，判別の効率が低い．

3. 提案手法

3.1 アプローチ

未知の不正 Web サイトに対応するために，疑惑のある Web サイト(疑惑 Web サイト)を発見する「検出」と疑惑 Web サイトに対して正規と不正に分類する「判別」の二段階で行う手法を提案する．まず「検出」処理では，各関連研究のドメイン名を用いた検出条件を組み合わせることで，既知の不正 Web サイトの集合であるブラックリストに存在しない不正 Web サイトに対しても検出範囲の拡張を可能にする．また，「判別」処理では，判別対象を，「検出」で用いた検出条件に該当する Web サイトの IP アドレスのみに限定する．また，検出条件悪質な活動に利用される IP アドレスは一部のネットワークアドレスに密集する傾向にあることを利用して，各 IP アドレスのネットワークアドレス部のみを用いた判別を行う．そのため，検出手法より不正の可能性が高い Web サイトの IP アドレスに判別対象を限定することで，効率性の向上を図る．

3.2 システム構成

提案システムの構成図を図 2 に示す．本研究ではクライアントが Web アクセスを行う際に通信する DNS サーバを用いる．DNS サーバの内部には不正 Web サイトに関するブラックリストと，未知の不正 Web サイトに対応する検出部と判別部を用意する．クライアントが Web アクセスを行った際に，ブラックリストを用いて不正 Web サイトの疑惑 Web サイトを DNS サーバ内の検出部で求め，その情報を判別部で利用する．判別部は，分類器を用いて疑惑 Web サイトを判別してクライアントに通知する．提案システムではアクセス先が不正 Web サイトであることを通知し，警告を促すことによって不正 Web サイトのアクセスを防止する．

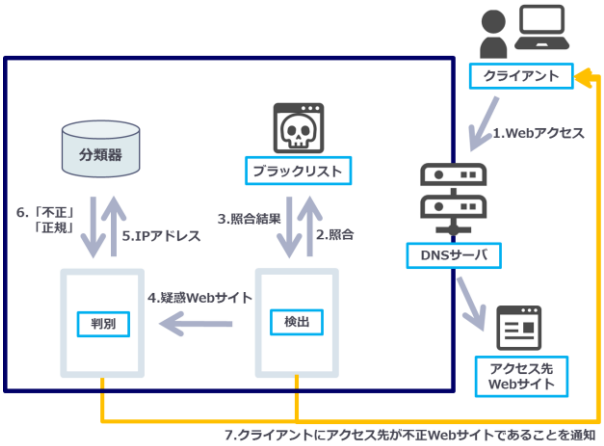


図 2 システム構成

3.3 提案方式の概要

提案方式の概要を図 3 に示す．まず，検出部の処理では，クライアントから Web アクセスが行われた(1)際に，DNS サーバにおいて，ブラックリストを参照してアクセス先の Web サイトと照合する(2)．アクセス先がブラックリストに載っている既知の不正 Web サイトであれば，クライアントにアクセス先が不正 Web サイトであることを通知する(8)．ブラックリストに載っている Web サイトを除外し(3)，不正 Web サイトのドメインの集合であるブラックリストと一致しなかった Web サイトからさらに，ドメイン名に基づいた検出条件と，マルウェアに感染された複数のクライアントからアクセスされている Web サイトのドメイン名を調べ(4)，条件を満たす Web サイトは，未知の不正 Web サイトである可能性が高いとみて検出する(5)．判別部の処理では，(5)で検出されたアクセス先の Web サイトが，正規 Web サイトか不正 Web サイトのどちらであるかを判別する(6)．アクセス先が不正 Web サイトであると判別されたときは(7)，クライアントにアクセス先が不正 Web サイトであることを伝える(8)．検出された新たな不正 Web サイトは，ブラックリストを更新するために提供することで(9)，ブラックリストを常に最新の状態に保つ．

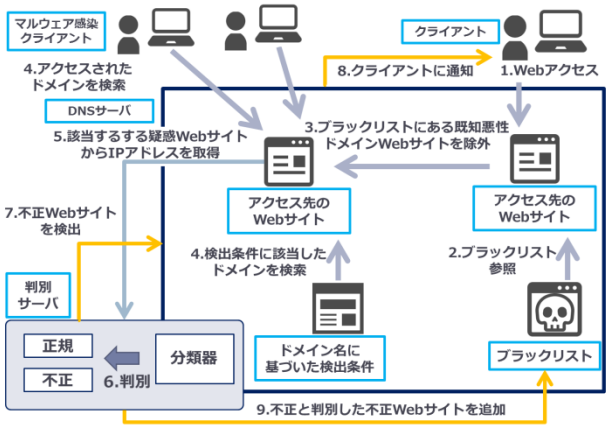


図 3 システムの流れ

3.4 マルウェア感染クライアント

疑惑 Web サイトを選定するために，マルウェアに感染されているクライアント(以下マルウェア感染クライアント)のアクセス先のドメイン名を利用する．マルウェア感染クライアントの検出方法を図 4 に示す．一般にマルウェアは，感染を拡大させるために多数の不正 Web サイトへアクセスを試みる．そのため，不正 Web サイトは，同時に複数のマルウェア感染クライアントからアクセスが行われている可能性が高い．そこで，DNS サーバに Web アクセスしているクライアントの中から(1)，既知の不正 Web サイトのドメイン(悪性ドメイン)にアクセスしているクライアントを探索し(2)，マルウェア感染クライアントとして検出する．

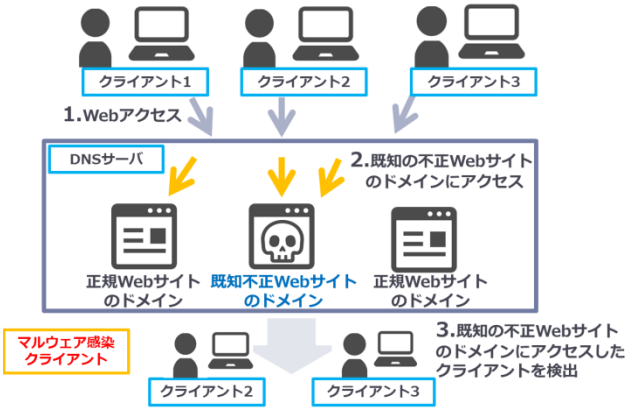


図 4 マルウェア感染クライアントの検出

3.5 未知の不正 Web サイトの検出手法

未知の不正 Web サイトの検出手法を図 5 に示す．クライアントから Web アクセスが行われた際に(1)，アクセスされた Web サイトから URL を抽出する(2)．さらに，抽出した URL から Web サイトのドメイン名を抽出し，不正 Web サイトのドメインの集合であるブラックリストを照合する(3)．(3)でブラックリストと一致した既知のドメイン名をアクセス先のドメインリストから除外する．ブラックリストと一致せず残った Web サイトのドメインの中から，疑惑ドメインの検出条件として，文字数が 10 文字以上，または英数字が混在したドメイン名に該当する Web サイトを抽出する(5)．さらに複数のマルウェア感染クライアントからアクセスがあるドメイン名に該当する Web サイトも抽出する(5)．(5)で該当したドメイン名を疑惑 Web サイトとみなし(6)，これらの疑惑 Web サイトから IP アドレスを取得する．取得した IP アドレスは，正規 Web サイトか不正 Web サイトのどちらであるか判別に利用するため，判別部に IP アドレスを渡す．

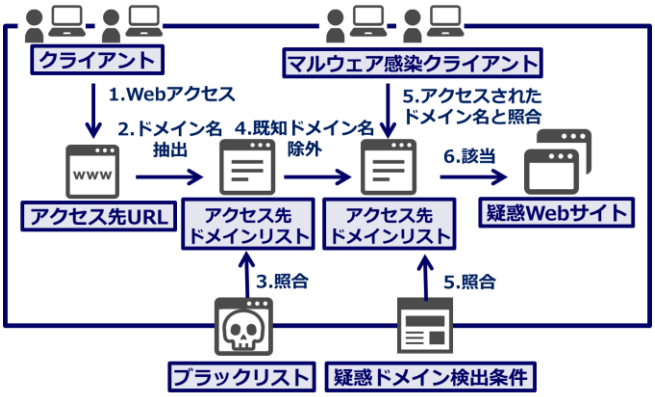


図 5 未知の不正 Web サイトの検出

3.6 IP アドレスを用いた Web サイトの判別手法

疑惑 Web サイトに対する判別手法を図 6 に示す．不正 Web サイトの疑惑 Web サイトを正規 Web サイトと不正 Web サイトに判別するために，疑惑 Web サイトから IP アドレスを取得し，IP アドレスクラスごとに分けて，それぞれの IP アドレスクラス専用の分類器に適用して判別を行う．ここで，正規 Web サイトの IP アドレスを良性アドレス，不正 Web サイトの IP アドレスを悪性アドレスと呼ぶ．このとき，それぞれの分類器には，各 IP アドレスクラスにおける良性 IP アドレス群と悪性 IP アドレス群を教師データとして用いて分類器を構築する．悪質な活動に利用される IP アドレスは一部のネットワークアドレスに密集する傾向にあることが知られている[8]．文献[8]の手法ではネットワークアドレス部とホストアドレス部を合わせた IP アドレス全体を用いて Web サイトの判別を行っているが，一部のネットワークアドレスに悪質な活動に利用される IP アドレスが密集するため，ホストアドレス部を含めて判別に用いるより，各 IP アドレスクラスのネットワークアドレス部を用いて判別する手法の方が，より悪性 IP アドレスを正確に判別できる可能性が高い．判別には，教師あり機械学習法の一つである Support Vector Machine(SVM)を用いる．悪性 IP アドレスが一部のネットワークアドレスに密集する特徴を元に，既知の不正 Web サイトが密集しているネットワークアドレスを教師データとして用いることで，悪性 IP アドレスの近傍に存在する Web サイト，つまり，悪性

IP アドレスの特徴に類似した特徴をもつ Web サイトを，未知の不正 Web サイトとみなして判別する．

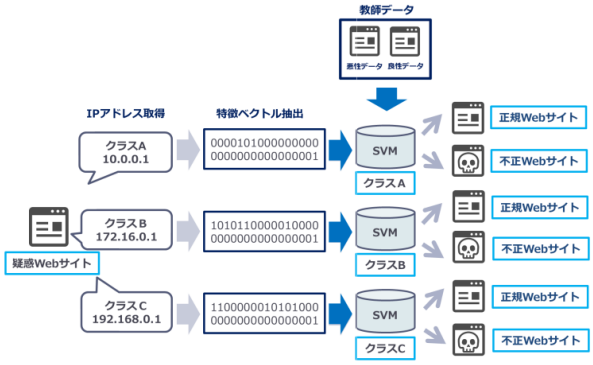
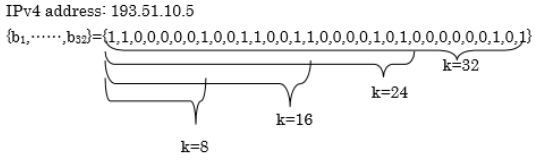


図 6 判別手法

3.7 特徴ベクトルの生成

SVM は，分類器の一種であり，教師データを用いて，入力された未知のデータ（テストデータ）を分類することができる．そのため，本手法では，予め良性・悪性が判明している IP アドレス(教師データ)を用いて，未知の IP アドレス（テストデータ）を良性 IP アドレスのクラス（良性クラス）と悪性 IP アドレスのクラス（悪性クラス）に分類する．SVM では，教師データの様々な特徴を元にクラスを構築し，良性クラスと悪性クラスの決定境界を決める．このとき，クラスを構築するために用いる特徴を特徴ベクトルと呼ばれる．特徴ベクトルの個数を次元数と呼ぶ．本手法では，文献[8]における特徴ベクトル生成手法を参考にし，図 7 のような形で IP アドレスから特徴ベクトルを生成する．IP アドレスをバイナリビット列に変換する．まず，IP アドレスの各ビットを{ b_1,……,b_k}で表す．IP アドレスクラス A にあたる k=1~8 の 8 次元，IP アドレスクラス B にあたる k =1~16 の 16 次元，IP アドレスクラス C にあたる k =1~24 の 24 次元，最後にホストアドレスまで含めた k =1~32 の 32 次元で特徴ベクトルを生成し，クラスの決定境界を構成する．



k	特徴ベクトル
8	b_k=1(k=1,2,8) b_k=0(その他)
16	b_k=1(k=1,2,8,11,12,15,16) b_k=0(その他)
24	b_k=1(k=1,2,8,11,12,15,16,21,23) b_k=0(その他)
32	b_k=1(k=1,2,8,11,12,15,16,21,23,30,32) b_k=0(その他)

図 7 特徴ベクトル生成

教師データとして用いる IP アドレスには，クラスごとに悪性を 1，良性を 0 と設定し，データセットを作成する．

表 1 教師データセットの例

IP アドレス	特徴ベクトル	ラベル
193.51.10.5	1,1,0,0,0,0,0,1,0,0,1,1,0,0,1,1	1
10.10.10.10	0,0,0,0,1,0,1,0,0,0,0,0,0,1,0,1	1
203.4.12.89	1,1,0,0,1,0,1,1,0,0,0,0,0,1,0,0	0
…	…	…

悪性の教師データ，良性の教師データを用いて表 1 のように SVM を構築して，疑惑 Web サイトの IP アドレスをテストデータとして，3.6 節で述べた判別手法を用いて，正規 Web サイト・不正 Web サイトに分類し，判別を行う．

4. 評価実験

本章では，IP アドレスのネットワークアドレス部を用いた Web サイトの判別の有効性を示す実験について述べる．

4.1 実験データ

本実験では，良性 IP アドレスデータと悪性 IP アドレスデータの 2 種類のデータを標本として使用する．良性 IP アドレスデータは Alexa の公表する Alexa Top Global Sites[10]を用いて，アクセス数のランキング上位の Web サイトから良性 IP アドレスとして取り出す．悪性 IP アドレスデータは，CCC DATAset[11]に含まれる 2008 年から 2011 年の 4 年分の通信データから，悪性 IP アドレスデータを抽出してリストを構成する．CCC DATAset は，マルウェア検体を収録したボット観測データ群であり，CCC 運営連絡会が運用するサイバークリーンセンターハニーポットで収集したマルウェア検体とウイルス対策ソフト 6 製品での検知名をリスト化したデータである．CCC DATAset には，マルウェア検体，攻撃通信データ，攻撃元データの 3 つから構成されたボット観測データ群が含まれている．

4.2 実験概要

ネットワークアドレスは，IP アドレスを構成するビット列のうち，個々の組織が管理するネットワークを識別するために使用される．このネットワークアドレスを用いて分類することで，より正確な判別ができるか SVM を用いて基礎評価実験を行った． IP アドレスは，ネットワーク部とホスト部から成り立っており，ネットワーク部は，その IP アドレスが属しているネットワークを識別するための部分を指す．ホスト部は，ネットワーク内のコンピュータを識別するための部分を指す． IP アドレスクラスは，IP アドレスの値によって，IP アドレスをいくつかのカテゴリに分類したものであり，クラス A からクラス E の 5 つの IP

アドレスクラスにわけられている. IP アドレスクラス A は，上位 8bit がネットワークアドレス部となり，残り 24bit がホストアドレス部となる. IP アドレスクラス B は上位 16bit がネットワークアドレス部となり，残り 16bit がホストアドレス部となる．IP アドレスクラス C は上位 24bit がネットワークアドレス部となり，残り 8bit がホストアドレス部となる．須藤ら[12]による CCC DATAset の解析によると，CCC DATAset は IP アドレスクラス A~C の IP アドレスが頻繁に悪質な活動に利用されている部分と利用されていない部分が存在している．本実験では，各 IP アドレスクラスのネットワークアドレスを用いる. IP アドレスクラス A は，良性データ数 9251 個，悪性データ数 46258 個を，また，IP アドレスクラス B は，良性データ数 647 個，悪性データ数 3238 個を，IP アドレスクラス C は，良性データ数 14271 個，悪性データ数 75000 個をそれぞれ用いて評価実験を行った．

4.3 評価方法

精度，適合率，再現率の 3 項目によって評価を行う．評価は，図 7 で定義した *k*=8，*k*=16，*k*=24，*k*=32 の 4 つで行う．悪性 IP アドレスを正しく悪性 IP アドレスと判定した数を真陽性(TP)，良性 IP アドレスを誤って悪性 IP アドレスと判定した数を偽陽性(FP)，良性 IP アドレスを正しく良性 IP アドレスと判定した数を真陰性(TN)，悪性 IP アドレスを誤って良性 IP アドレスと判定した数を偽陰性(FN)としたとき，精度，適合率，再現率をそれぞれ下記の計算式で評価する．

精度は，テストデータを良性・悪性 2 つのクラスにそれぞれ正確に判別できた割合である．

$$\text{精度} = \frac{TP + TN}{TP + TN + FP + FN} \qquad (1)$$

適合率は，悪性と判定した IP アドレスのうち，実際に悪性 IP アドレスであった割合である．

$$\text{適合率} = \frac{TP}{TP + FP} \qquad (2)$$

再現率は，全ての悪性 IP アドレスのうち，悪性と判定した IP アドレスの割合である．

$$\text{再現率} = \frac{TP}{TP + FN} \qquad (3)$$

4.4 実験結果

IP アドレスクラス A のデータについては，*k*=8，*k*=16，*k*=24，*k*=32 の 4 つの場合の結果を表 2 に示す．ちょうど IP アドレスクラス A でのネットワークアドレスを指している *k*=8 で再現率が一番高い数値を示した．しかし，精度と適合率は *k*=32 で一番高い数値を示した．

表 2　IP アドレスクラス A の精度評価

	精度	適合率	再現率
k=8	89.83949	93.13721	94.79225
k=16	89.81787	93.1318	94.77063
k=24	89.81787	93.1318	94.77063
k=32	90.19618	93.54914	94.77063

IP アドレスクラス B のデータについては，*k*=8，*k*=16，*k*=24，*k*=32 の 4 つの場合の結果を表 3 に示す．IP アドレスクラス B のネットワークアドレスである *k*=16 で精度，再現率が一番高い数値を示した．

表 3　IP アドレスクラス B の精度評価

	精度	適合率	再現率
k=8	79.41328	87.57707	87.73935
k=16	84.01956	89.11809	92.063
k=24	83.45342	89.04604	91.38357
k=32	83.94236	89.22569	91.81594

IP アドレスクラス C のデータについては，*k*=8，*k*=16，*k*=24，*k*=32 の 4 つの場合の結果を表 4 に示す．精度，適合率は *k*=16 で一番高い数値を示し，再現率はすべて一定の数値を示した．

表 4　IP アドレスクラス C の精度評価

	精度	適合率	再現率
k=8	67.36454	91.05442	67.81733
k=16	67.43287	91.15396	67.81733
k=24	67.40711	91.11641	67.81733
k=32	67.42839	91.14743	67.81733

5. 考察

IP アドレスクラス A のネットワークアドレスである *k*=8 で再現率が最も高い数値を示したことから，IP アドレスクラス A では，ネットワークアドレスを用いて悪性 IP アドレスを正確に判別することに適していると考えられる．一方，*k*=32 のとき精度と適合率が最高値を示したことから，一見 k=32 とした判別が適していると思われるが，*k*=16，*k*=24，*k*=32 の TP(真陽性)は一定値となっており，悪性 IP アドレスを正確に判別した数が最も多いのは *k*=8 のときである. *k*=32 のときは TN(真陰性)が増加した影響で FN が減少したため，適合率の数値が高くなり，全体の精度も向上

していると考えられる．従って，悪性 IP アドレスとして多く利用されている IP アドレスクラス A では，ネットワークアドレスを用いた悪性 IP アドレスの判別が有効であると考えられる．

IP アドレスクラス B のネットワークアドレスである *k*=16 のときに再現率が最も高い数値を示している．IP アドレスクラス B では，悪性 IP アドレスと良性 IP アドレスを正しく判別できた数が共に多く，また，*k*=16 のとき精度も最高値を示していることから，ネットワークアドレスを用いて悪性 IP アドレスを正確に判別することに適していると考えられる．

IP アドレスクラス C では，精度，適合率は *k*=16 のときに最高値を示し，再現率はすべて一定値を示している．また，他の IP アドレスクラスの精度は 8 割を超えているのに対し，IP アドレスクラス C の精度は 6 割程で低い数値であった．これらの結果が得られた原因として，IP アドレスクラス C は他の IP アドレスクラスより IP アドレスの範囲が狭く，かつ，全体的に悪質な活動に多く利用されているため，悪性 IP アドレスの特徴が表れにくかったと考えられる．また，*k*=8 で判定を誤っている IP アドレスは，*k*=16，*k*=24，*k*=32 のすべてにおいて判別を誤っていた．判別を誤ったこれらの IP アドレス群が精度を下げている可能性があると考えられる．

6. 追加実験

IP アドレスクラス C の精度を下げている原因が，判別を誤っている．IP アドレス群であるかどうかを確かめるため，*k*=8 のときに判別を誤っている IP アドレス群を除外して追加実験を行った．IP アドレスクラス C のデータについては，*k*=8，*k*=16，*k*=24，*k*=32 の 4 つの場合の結果を表 5 に示す．全体の精度が 9 割を超えた結果となった．

表 5 IP アドレスクラス C の精度評価

	精度
k=8	99.98337
k=16	99.98337
k=24	99.98337
k=32	99.98337

この結果より，IP アドレスクラス C で *k*=8 の場合に誤判別される IP アドレス群が判別精度低下の原因となっていたことがわかる．

7. まとめ

本稿では，未知の Web サイトに対して正規・不正 Web サイトの判別を行うために，DNS サーバから得られる情報のうち，ドメイン名，IP アドレス，マルウェア感染クライアントを利用して未知の不正 Web サイトに対応した検出手法を提案した．また，IP アドレスクラスのネットワークアドレスを用いて疑惑 Web サイトの判別精度を評価した．悪質な活動に多く利用されているアドレスクラス A の結果が高精度を示しており，IP アドレスクラス B の結果も高精度を示したことから，ネットワークアドレス部を用いた判別は，有効であることが確認できた．一方，IP アドレスクラス C では，特定の IP アドレス群の影響で高い精度が得られなかった．このため，判別を誤った IP アドレス群を分析し，改善を図る必要がある．また，今回用いたデータセットに限らず，他の種類のデータセットでも判別が可能か評価する必要がある．

参考文献

[1]警察庁広報資料: 平成 26 年中のインターネットバンキングに係る不正送金事犯の発生状況等について, <https://www.npa.go.jp/cyber/pdf/H270212_banking.pdf> (参照 2016-08-11).

[2]TREND MICRO: Web レピュテーション, <http://www.trendmicro.co.jp/why-trendmicro/spn/features/web/index.html> (参照 2016-08-11).

[3]CISCO: テクノロジー解説, <http://www.cisco.com/web/JP/news/cisco_news_letter/tech/index.html> (参照 2016-08-11).

[4]劉亦晨: DNS 情報による悪意のあるサイトの検出法, 2012 年度 早稲田大学大学院 基幹理工学研究科 情報理工学専攻 修士論文 (2012).

[5]日立ソリューションズ: 情報セキュリティブログ, <http://securityblog.jp/words/2898.html> (参照 2016-08-11).

[6]田中晃太郎，長尾篤，森井昌克: DNS ログからの不正 Web サイト抽出についてー解析手法とその匿名化ー，コンピュータセキュリティシンポジウム 2013 論文集, Vol.2013, No.4, pp.132-138 (2013).

[7]千葉大紀,森達哉，後藤滋樹: 悪性 Web サイト探索のための優先巡回順序の選定法， コンピュータセキュリティシンポジウム 2012 論文集, Vol.2012, No.3, pp.805-812 (2012).

[8]Daiki Chiba, Kazuhiro Tobe, Tatsuya Mori, Shigeki Goto: Detecting Malicious Websites by Learning IP Address Features, Proc. 2012 IEEE/IPSJ 12th International Symposium on Applications and the Internet(SAINT2012), pp.29-39 (2012).

[9]平井有三: はじめてのパターン認識，森北出版 (2012).

[10]Alexa: The top 500 sites on the web, <http://www.alexa.com/topsites> (参照 2016-08-11).

[11]秋山満昭，神薗雅紀，松木隆宏，畑田光弘: マルウェア対策のための研究用データセット～MWS Datasets 2014～，情報処理学会研究報告, Vol. 2014-CSEC-66, No. 19, pp. 1-7, (2014).

[12]須藤年章: CCC Dataset 2010 によるマルウェア配布元 IP アドレス評価に関する一考察，情報処理学会シンポジウム論文集, Vol.2010, No.9 pp.19-24 (2010).

[13]金澤しほり，中村嘉隆，稲村浩，高橋修: IP アドレスクラスにおけるネットワークアドレスの特徴を用いた未知の不正 Web サイト判別方法，情報処理学会，第 12 回マルチ メディア，分散，協調とモバイル(DICOMO2016)シンポジウム論文集, pp.806-812, 2016