Vol.2021-IOT-52 No.17
2021/3/1

SSL/TLSハンドシェイク時に取得可能な情報によるベイジアンフィルタを用いたWebサーバ信用度判定

大室 高帆[1]　新城 靖[2]　中井 央[3,4]　三宮 秀次[2,4]　星野 厚[5]　佐藤 聡[2,4]

概要：インターネットが世界中で利用されている現代において, 未知のサーバの信頼性を見極める有効な手段は確立されていない. 本研究では HTTPS による未知の通信相手の信用度をコネクション確立前に判定できることを目的とした. 手法としては, 任意のサーバに対し TLS ネゴシエーションを行い, 終了時点までに得られる証明書及びその周辺情報 (以下, ネゴシエーション情報とする）をベルヌーイイベントモデルに適用することでベイジアンフィルタを作成し当該サーバの信用度を判定することを提案した. 学習に先立ち現状調査として, 良性サイトと悪性サイトを定義しネゴシエーション情報の要素を収集し, 証明書チェーン・有効期間・TLS 拡張について分析・学習することと決定した. 分析の結果定めたベクトル化手法を使用しベルヌーイイベントモデルへと適用し, ベイジアンフィルタで学習した結果, 本研究で実装したベイジアンフィルタは7割程度の正答率であり, 良性サイト群・悪性サイト群を分ける何らかの特徴を検出していることが明らかになった.

キーワード：SSL/TLS, 証明書, ベイジアンフィルタ

Decision Method of Web Server's Credibility by Using Information of SSL/TLS Handshake.

Takaho Omuro[1]　Yasushi Shinjo[2]　Hisashi Nakai[3,4]　Shuji Sannomiya[2,4]　Atsushi Hoshino[5]
Akira Sato[2,4]

1. 序論

インターネットが世界中で利用されている現代において, 情報の機密性を確保することは必須である. Web コンテンツの送受信においては従来の HTTP に SSL/TLS による暗号機能を付与した HTTPS がほとんどの場合用いられている. HTTPS 通信は比較的安全だが, 機密情報を送信する前に通信相手の信頼性の見極めを行うことは重要である. 既知のドメインの安全性を確認するサービスが存在する一方, 未知のサーバの信頼性を見極める有効な手段は確立されていない.

本研究は HTTPS による未知の通信相手の信用度を機密情報を送信する前に判定することを目的とする. なお, 本研究における信用度とは相手が良性か, 悪性かということを表すものとする. 手法としては, 任意のサーバに対し TLS ネゴシエーションを行い, 終了時点までに得られる情報の

1 筑波大学大学院博士前期課程システム情報工学研究科コンピュータサイエンス専攻
Master's Program in Computer Science, Graduate School of Systems and Information Engineering, University of Tsukuba
2 筑波大学システム情報系
Faculty of Engineering, Information and Systems, University of Tsukuba
3 筑波大学図書館情報メディア系
Faculty of Library, Information and Media Science, University of Tsukuba
4 筑波大学学術情報メディアセンター
Academic Computing & Communications Center, University of Tsukuba
5 株式会社チノウ

みを用いて当該サーバの信用度を判定することを提案する. 具体的には, 各サーバとの TLS ネゴシエーション終了時点までに得られる証明書及びその周辺情報 (以下, ネゴシエーション情報とする）に着目する. 着目する理由は三つある.

第一の理由として, 通信相手の性質を推定する手掛かりが現れることが挙げられる. 例えばネゴシーション情報から得られる証明書チェーンを用いると, 証明書の有効性を保証し, 提供している認証局を調べることができる. 認証局が証明書を提供する団体・サービスが判明すれば, 証明書がどのような用途で使用されているのか推測する一助となる.

第二の理由として, ネゴシエーション情報の収集が機密情報の送信前に可能であることが挙げられる. ネゴシエーション情報は SSL/TLS ハンドシェイクが終了する時点までにサーバとクライアント間でやりとりされる情報である. したがって, ネゴシエーション情報を用いれば機密情報の送信前に通信相手の信頼性の見極めを行うことができる.

第三の理由として, HTTPS が広く普及しておりネゴシエーション情報が容易に集められることが挙げられる.

ネゴシエーション情報の学習に際しては, 特定の要素を保持しているかどうかで学習する. 要素の有無を学習し, 複数のグループに識別する手法としては, McCallum らの研究 [10] が挙げられる. この研究では文書中の単語をベルヌーイイベントモデル, 多項分布モデルで表現し, ナイーブベイズによる学習でベイジアンフィルタを作成し, 文書を複数のカテゴリに分類した. 本研究では要素の有無の学習という共通点に着目し, ネゴシエーション情報に含まれる各要素をベルヌーイイベントモデルで表し, 学習により作成したベイジアンフィルタで未知の Web サーバのネゴシエーション情報の分類を行う. 具体的には, ネゴシエーション情報から抽出した要素について, 既に収集済みのデータの中で取りうる要素を全て列挙し, 各ネゴシエーション情報内で出現したかどうかを 0, 1 で表現することでベルヌーイイベントモデルを適用する. ベイジアンフィルタは機械学習のアルゴリズムであるナイーブベイズを用いたフィルタであり, メールのフィルタリングに使用されることがある [12].

ベルヌーイイベントモデルを適用する際, ベクトル化の手法が複数考えられる場合は全種類について学習を試行し, 最も本研究に適していると判断した手法を採用する. 具体的には, 証明書チェーンを性質の推定に組み込む場合, ルート認証局, ルート認証局の一つ下, またはそれ以降の認証局を確認するという様々な手法が考えられる. 本研究ではこれら全てについて検証し, 採用した手法を組み合わせて学習手法を決定する.

学習では, 現状調査で判明した事実をもとに, python の機械学習ライブラリの一つである scikit-learn を用い学習器を作成する. 作成した学習器はクロスバリデーションでテストを行い, 正答率・再現率・適合率・真陰性率の値を見ることで未知のサイトの性質を予測することができるか, 検討を行う.

表 1 抽出するネゴシエーション情報

属性名	内容
有効期間	当該証明書がどのくらいの期間有効であるか
TLS 拡張	X509v3 拡張など様々な拡張によるパラメータ群
証明書チェーン	当該証明書が認証に用いる認証局の情報
鍵長	共通鍵暗号において使用される鍵の長さ
証明書の発行者	当該証明書を直接認証している認証局
シリアルナンバー	証明書に一意に割り振られた番号

2. 研究手法

本研究は, HTTPS による未知の通信相手の信用度を機密情報を送信する前に判定できることを目的とする. 手法としては, 任意のサーバに対し TLS ネゴシエーションを行い, 終了時点までに得られるネゴシエーション情報を用いてベイジアンフィルタを作成し, 未知の Web サーバに適用することで信用度を判定する. 本章では本研究において提案する手法の概略を示し, 提案手法をどのように検証するのか示す.

2.1 提案手法の概要

提案手法の概要を**図 1** に示す. 提案手法は，以下に示す 4 つのプロセスから構成される.

(1) 信用度が既知の Web サーバからネゴシエーション情報を収集
あらかじめ良性サイト群・悪性サイト群を定義し, ネゴシエーション情報を収集する. 良性サイトは, アクセス数が多いサイト, 社会的信用度の高い優良企業のサイトとする. 悪性サイト群は, マルウェアサイト, フィッシングサイトなどとする. C 言語で作成した OpenSSL のクライアントとして動作するように作成した抽出ツールを用いて，ネゴシエーション情報から**表 1** に示す情報を抽出する. これらの情報は Web サーバの管理者の意思により選択される情報であるものを選択した.

(2) ネゴシエーション情報のモデル化を検討
提案手法で利用するベルヌーイイベントモデルの概要を**図 2** に示す. 一般的には，ベルヌーイイベントモデルは 文書の学習において単語の出現の有無を 0, 1 で表現しバイナリ列で取り扱う. 提案手法では，ネゴシエーション情報から単語に相当するものを抽出することによりベクトル化を行う. 複数あるベクトル化の手法からから最適な手法を決定するために，良性サイト群と悪性サイト群それぞれから抽出することにより

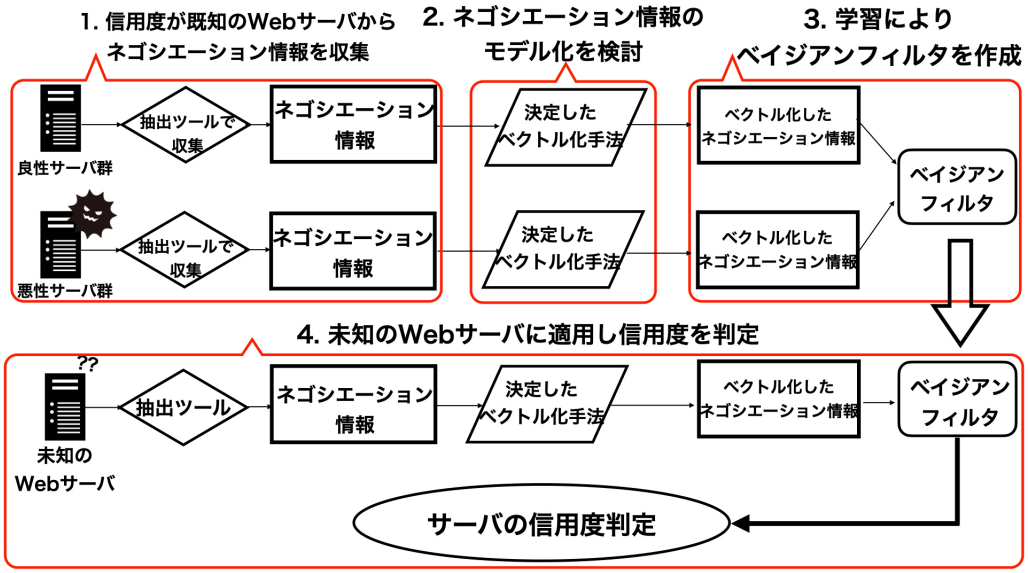

図 1 提案手法の概要

収集したデータを分析し，学習実験を行う．

(3) 学習によりベイジアンフィルタを作成
ベルヌーイイベントモデルを適用したネゴシエーション情報をベクトル列で表現し，ベルヌーイナイーブベイズで学習し，ベイジアンフィルタを作成する．

(4) 未知の Web サーバに適用し信用度を判定
(3) にて作成したベイジアンフィルタに，未知の Web サーバから得られるネゴシエーション情報を表すバイナリ列を適用することにより，通信相手のサーバの信用度を判定する．このとき，未知のサーバのネゴシエーション情報は (1) にて良性サイト群，悪性サイト群からネゴシエーション情報を抽出したツールを用い，(2) で決定したベクトル化手法を用いてバイナリ列にする．

3. 現状調査

2 章で説明したベクトル化手法を決定するために，実際にネゴシエーション情報を収集し分析を行う現状調査を実施した．

3.1 抽出ツール

提案手法で用いる抽出ツールが満たすべき要求要件を以下に示す．

- 調査対象サーバの FQDN (Fully Qualified Domain Name) が指し示す全て の IP アドレスを，調査しなければならない．
- 調査対象サーバの IP アドレスに複数 FQDN が割り振られている場合でも，対象の FQDN を適切に調査しなければならない．
- 証明書情報に加え，証明書チェーンを収集できなければならない．

これらの要求要件を満たす抽出ツールの動作を以下に示す．

(1) getaddrinfo を使用して入力されたドメインのアドレス解決を行う．

(2) ソケットを作成し connect したのち，SSL_ctx 構造体を作成し SSL 通信の準備を行う．SNI のセッティングはこの段階で行う．

(3) SSL_connect によりサーバとのハンドシェイクを開始し，実際に接続を行う．

(4) 接続が成立したのち，証明書情報の保存，証明書チェーンの取得及び保存を行う．

(5) SSL をシャットダウンして終了する．

3.2 収集したネゴシエーション情報

現状調査では，良性サイトの定義としてアクセス数が多いサイト，優良企業のサイトという二種類を採用した．アクセス数が多いサイトは Cisco 社が提供する Cisco Umbrella Top 1 Million[2] (以下，Cisco Umbrella と記す) に記載されているサイトとして定義した．Cisco Umbrella は対象ドメインを呼び出す一意のクライアント数について独自のスコアを設定し，ランキングを提供している．また，優良企業のサイトとしては Value.Today[13] に記載されていている企業リストのうち，市場価値に基づき世界中の企業をランク付けした企業リストに記載されている各企業の Web サイトの情報を用いた．

悪性サイトは StevenBlack/hosts から提供されているマルウェア・アドウェアリスト [11] に記載されているサイト，加えて PhishTank から提供されているフィッシュングサイトのリスト [9] を合わせたものとして定義した．StevenBlack/hosts は 15 の異なるホストファイルを結合し，マルウェア ・アドウェアをはじめとする 5 つのグループに分類した上で提供している．各サイトのデータについて，Cisco

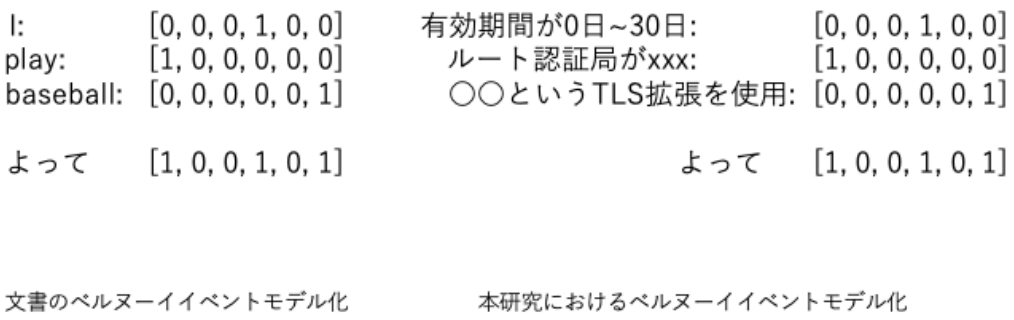

図 2 ベルヌーイイベントモデルの概要

表 2 収集の実行環境

OS	CentOS Linux release 7.9.2009 (Core)
CPU	Intel Core Processor (Broadwell)
メモリ量	990MB

表 3 本研究で用いたデータセット

属性	サイト名	データ数	提供
良性	Cisco Umbrella Top 1 Million	100 万	Cisco
	Value.Today	6,356	Value.Today
悪性	Steven Black	58,550	StevenBlack/hosts
	PhishTank	13,253	PhishTank

Umrella については 2020 年 12 月 11 日時点, Value.Today については 2021 年 1 月 18 日時点, StevenBlack/hosts・PhishTank については 2020 年 12 月 15 日時点のデータを使用した．これらのデータの詳細については**表 3** に示す．悪性サイト群のデータは StevenBlack/hosts・PhishTank の双方を合わせたデータを用いた．

次に，表 3 に示したデータセットの各々の Web サイトから前述の収集ツールを用いてネゴシエーション情報の抽出を行い，データを収集した．ネゴシエーション情報が抽出できたドメインと抽出でないドメインとに分かれた．ここでは抽出ツールによりネゴシエーション情報が抽出できた場合を収集成功とよび, 取得できなかった場合を失敗とよぶことにする．収集に失敗した原因としては, すでにドメインが削除されている場合や, HTTPS に対応していない場合が考えられる．収集の結果については**表 4** に示す．なお、良性サイト群の Cisco Unbrella，および，悪性サイト群のデータ収集は 2020 年 12 月 18 日から 2020 年 12 月 20 日までに行い，良性サイトの Value.Today のデータ収集は 2021 年 1 月 18 日に行なった．

なお，これ以後の収集データの分析においては，良性サイト群のデータとしては，Cisco Unbrella のデータを用いている．

3.2.1 証明書チェーン

各証明書から派生する証明書チェーンについて, Distinguished Name (以下, DN とする) の種類ごとに分析を行なった．

表 4 証明書情報の収集の試行数及び結果

属性名	収集試行数	収集成功数	成功割合
良性 (Cisco Umbrella)	70,000	52,832	0.754
良性 (Value.Today)	6,356	5,424	0.853
悪性	71,803	34,779	0.484

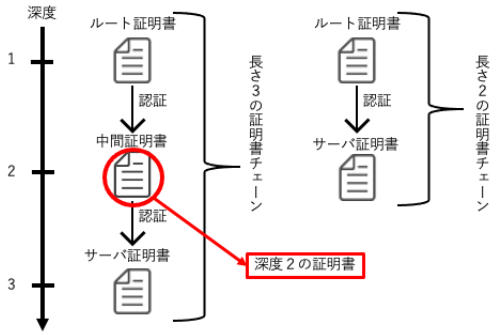

図 3 本研究における証明書チェーンの長さ及び深度の説明

証明書チェーンの DN を調査するにあたり, 証明書チェーンのパスの長さ及び深度について調べた．本研究における長さ及び深度の定義について**図 3** に示す．

本研究における証明書チェーンの長さは, 末端の証明書を含めた認証に関わるエンティティの総数と定義する．また, 深度はある認証局がルート認証局から経ている認証局の数と定義する．すなわち, 深度 n の認証局とはルート認証局から数えて n 番目の認証局のことである．また, 本研究では便宜上ルート認証局以降の認証局を一括で中間認証局と称する．パスの長さは OpenSSL ライブラリが提供する sk_X509_num() を使用してクライアントで取得した．

証明書チェーンの長さの種類別割合について, **図 4** に示す．

証明書チェーンの長さについて, 良性サイト群においては 14, 悪性サイト群においては 10 が最大だった．最も種類数が多かったのは, 良性サイト群・悪性サイト群ともに長さ 3 の証明書チェーンであった．具体的には, 良性サイト群では 64.7%, 悪性サイト群では 49.7%が長さ 3 の証明書

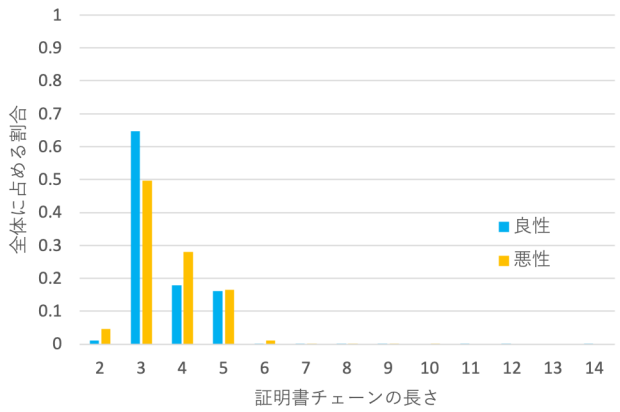

図 4 証明書チェーンの長さの種類についての割合

チェーンであった．証明書チェーンの５割近くは深度３であり，認証局の大半は深度２までに分布していることがわかる．よって，分析の対象を深度２までの認証局とする．

個別の深度の認証局について調査を行う．ルート認証局の DN は，良性サイト群で 269 種類，悪性サイト群で 327 種類が確認された．良性サイト群・悪性サイト群を合わせると 505 種類の DN が存在した．各サイトで使用するルート認証局について，特徴的なものを調査した．良性サイト群・悪性サイト群のルート認証局のうち，どちらかで上位 15 件に入った認証局が各サイト群において占める割合をグラフにして**図 5** に示す．

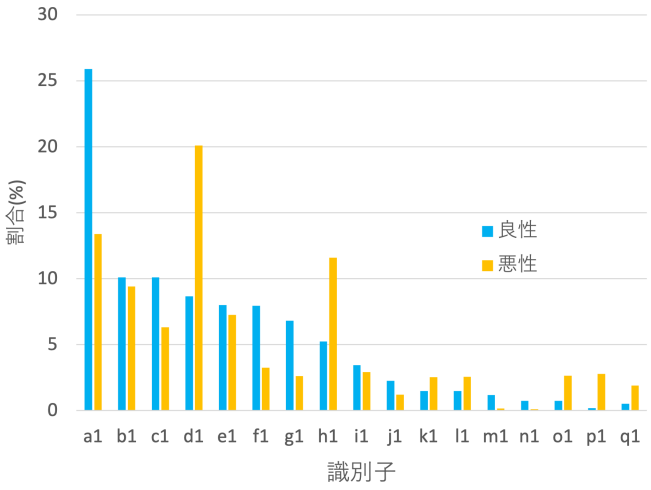

図 5 ルート認証局の DN の良性サイト群と悪性サイト群における度数の割合

良性サイト群について，1 位の DN における CN は DigiCert Global Root CA であった．この CN は DigiCert 社が提供する CA につけられている．DigiCert 社は 2021 年 1 月 5 日時点で 13 種のルート証明書を提供している [4]．良性サイト群で度数が上位にあるルート認証局の DN では，CN が Baltimore CyberTrust Root・DigiCert High Assurance EV Root CA である３つの証明書が DigiCert 社から提供されている．一方，DigiCert 社の証明書は悪性サイト群で

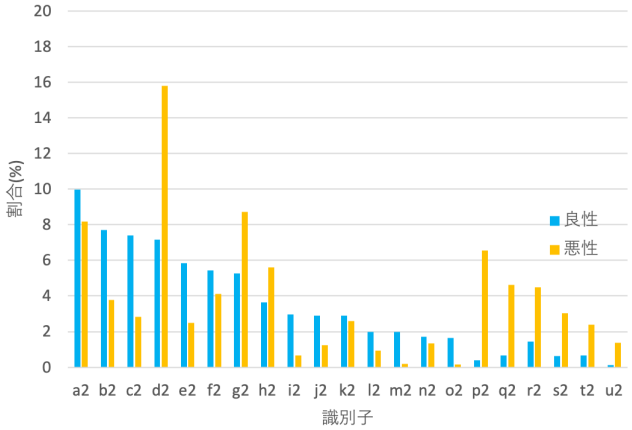

図 6 深度２の中間認証局の DN の良性サイト群と悪性サイト群における度数の割合

も使用されている．悪性サイト群において DigiCert Global Root CA が 2 位に，Baltimore CyberTrust Root が 4 位に，DigiCert High Assurance EV Root が 6 位になっている．

悪性サイト群について，1 位の DN における CN は DST Root CA X3 であった．これは Let's Encrypt で使用されているルート認証局である．Let's Encrypt は、非営利団体の Internet Security Research Group (ISRG) が提供する自動化された無料の認証局である [6]．同一のルート認証局は良性サイト群でも 4 位に存在し全体の 8.67%である一方，悪性サイト群では全体の 20.1%を占めている．この結果から，Let's Encrypt の提供する証明書がより悪性サイト群で使われていることがわかる．

つづいて，深度が 2 の認証局について調査を行う．深度が 2 の DN について，良性サイト群では 400 種類，悪性サイト群では 416 種類が確認された．良性サイト群・悪性サイト群で重複を取り除くと 655 種類の DN が確認できる．各サイトで使用する深度２の中間認証局について，特徴的なものを調査した．良性サイト群・悪性サイト群の深度２の中間認証局のうち，どちらかで上位 15 件に入った認証局が各サイト群において占める割合をグラフにして**図 6** に示す．

深度２の認証局について，良性サイト群でもっとも多い DN の CN は Starfield Services Root Certificate Authority - G2 であった．一方で，悪性サイト群でもっとも多い DN の CN は Let's Encrypt Authority X3 であった．Let's Encrypt Authority X3 の悪性サイト群における割合は良性サイト群における割合の二倍近くであり，深度 2 の認証局において悪性サイト群を特徴付けていると言える．また，p2 に該当する DN の CN は COMODO RSA Certification Authority であったが，この DN は悪性サイト群における割合が良性サイト群と比較して高い．これらの DN は，良性サイト群と悪性サイト群を識別する上で有用だと考えられる．

3.2.2 有効期間

証明書中の"Not Before"および"Not After"のフィール

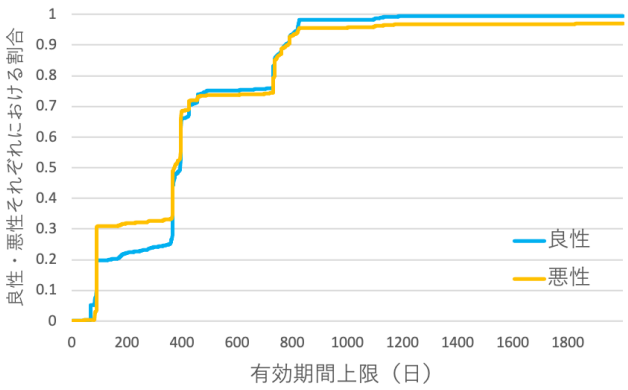

図 7 証明書の有効期間についての累積相対度数分布

表 5 調査対象の TLS 拡張フィールド

番号	拡張名
1	X509v3 Key Usage
2	X509v3 Extended Key Usage
3	X509v3 CRL Distribution Points
4	X509v3 Certificate Policies
5	Authority Information Access
6	X509v3 Basic Constraints
7	X509v3 Authority Key Identifier
8	X509v3 Subject Key Identifier
9	X509v3 Subject Alternative Name
10	X509v3 Issuer Alternative Name
11	X509v3 Issuing Distribution Point
12	X509v3 Policy Constraints
13	X509v3 Inhibit Any Policy
14	X509v3 Name Constraints
15	X509v3 OCSP No Check
16	X509v3 Netscape String extensions
17	X509v3 Netscape Certificate Type
18	CT Precertificate SCTs
19	1.3.6.1.4.1.311

ドを確認し差を算出することで有効期間を求めた．これをもとに作成した累積相対度数分布を**図 7** に示す．

3.2.3 TLS 拡張

収集した証明書に含まれる TLS 拡張について調査した．調査対象について，収集に用いた OpenSSL で定義されている拡張のうち”STANDARD EXTENSIONS” および ”DEPRECATED EXTENSIONS” に含まれる 17 種類を調査対象とした [8] ．また，証明書の性質に関連があると推測できる追加の拡張として，Certificate Transparency（以下 CT）プロジェクトの形式に従った CT フィールド，Microsoft 社の管理情報を含むフィールドが挙げられる．これら二つの拡張は証明書の TLS 拡張フィールドにおいて個別の OID を書き込むことで反映される．今回の調査では前述の 17 種に加え，CT を示す”CT Precertificate SCTs”，Microsoft 社の管理情報の OID である”1.3.6.1.4.1.311” の 2 つを対象とした 19 種の TLS 拡張について，番号を割り振った上で調査を行った．一覧を**表 5** に示す．

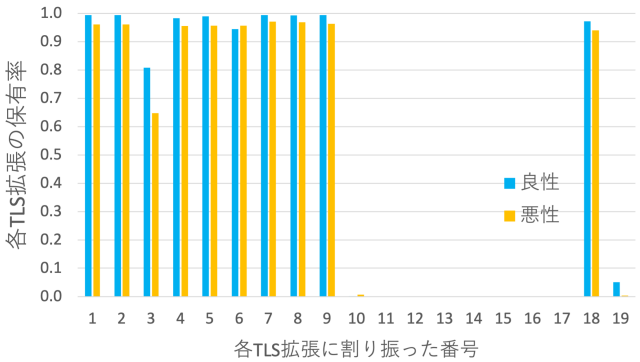

図 8 TLS 拡張 19 種の保有率

表 6 決定したベクトル化手法

要素	ベクトル化手法
証明書チェーン	深度 2 の中間認証局を使用
有効期間	89 日で分割
TLS 拡張	今回発見できなかった 7 種類の拡張を除いた 12 種類の TLS 拡張を使用

良性サイト群・悪性サイト群それぞれ全てのネゴシエーション情報において，表 5 の 19 種の TLS 拡張が証明書内に存在する割合（以下，保有率とする）を調査した．結果を**図 8** に示す．

全てのネゴシエーション情報において，11 から 17 の 7 つの TLS 拡張については，良性・悪性ともに保有率が 0 であった．理由としては，調査対象が CA 証明書ではなかったこと，すでにほとんどの証明書で使われていないことが挙げられる．例えば，12 と 13 はルート CA のみで使用される拡張である．また，16 と 17 は OpenSSL において非推奨であり，使用されることが少ないと考えられる．良性サイト群と悪性サイト群の保有率において最も差が大きかったのは，表 5 で 3 にあたる X509v3 CRL Distribution Points であった．良性サイト群における保有率が 80.8% である一方，悪性サイト群における保有率は 64.8%であった．CRL Distribution Points は 自らが掲載される可能性がある CRL の配布 URL を提示することで，失効を確認することができる TLS 拡張である．6 の X509v3 Basic Constraints においてのみ，悪性サイト群の保有率が良性サイト群の保有率より高かった．それ以外の TLS 拡張では，良性サイト群の保有率が悪性サイト群の保有率より高かった．

3.3 ベクトル化方法の決定

ネゴシエーション情報をベクトル化する最適な手法を決定するため，各要素のみで考えうる学習を試行し，本研究で採用するベクトル化手法を決定した．決定したベクトル化手法を**表 6** に示す

表 7　学習の実行環境

OS	Ubuntu 18.04LTS
CPU	Intel(R) Core(TM) i7-7700K CPU @ 4.20GHz
GPU	GeForce GTX 1080
メモリ	62GB

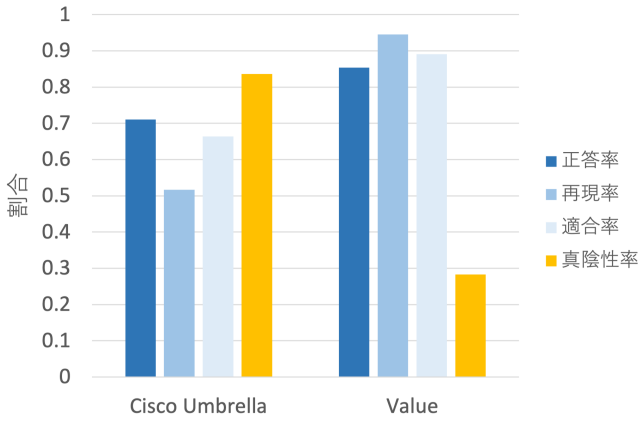

図 9　異なるデータを用いた学習の結果比較

4. 評価実験

ベルヌーイナイーブベイズによる学習は, python の機械学習用ライブラリである scikit-learn に実装されている BernoulliNB を用いる．学習の実行環境を**表 7** に示す．

提案手法の評価実験の目的は，提案手法により作成したベイジアンフィルタがサイトが悪性であるかを信用度判定できるかということにした．

この目的を実現するために，既存の研究にてナイーブベイズによる学習を用いたスパムフィルタリングにおける評価実験にて求めている，正答率，再現率・適合率，真陰性率を用いて比較する．これら， 正答率・再現率・適合率の計測方法は， Ion Androutsopoulos らの研究 [3] と参考にして, 交差検定の結果の平均をとる手法を用いた，具体的には，収集したネゴシエーション情報を 5 分割した五倍交差検定を行なった．

3.3 節にて述べた手法により，ネゴシエーション情報から取り出した三つの要素からバイナリ列を生成し， ベイジアンフィルタによる学習を行なった．この時, 良性サイト群として Cisco Umbrella を採用した場合と, Value.Today を採用した場合の二種類について学習を実行し結果を比較した．実行の結果を**図 9** に示す．

図 9 より, 正答率・再現率・適合率については Cisco Umbrella を用いた場合が優れていたが, 真陰性率については Value.Today を用いた場合が優れていた． これは, Cisco Umbrella を用いた場合は良性を誤認する可能性は比較的低い一方で悪性を取りこぼす可能性が高いことを示している．一方で, Value.Today を用いた場合は悪性はより良い精度で検出するが良性サイト群を誤認する可能性が Cisco Umbrella の場合より高いということも示している．

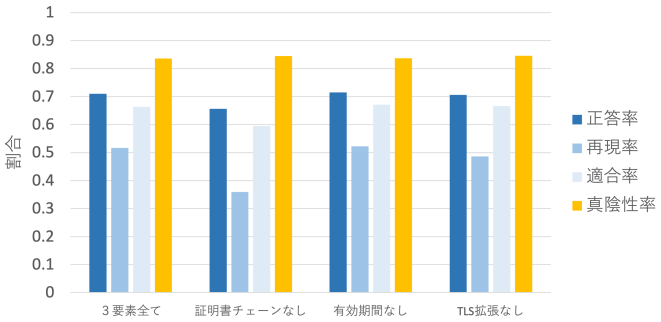

図 10　異なるデータを用いた学習の結果比較

また, ネゴシエーション情報の三つの要素のいずれの要素がベイジアンフィルタの精度に対してもっと影響を与えているかを明らかにするための評価実験も行なった．具体的には, 本研究で学習を行った証明書チェーン・有効期間・TLS 拡張の三つの要素のうちいずれか一つを用わずに作成したバイナリ列を用いて学習を行った．この評価実験の結果を**図 10** に示す．

図 10 より， 正答率・再現率・適合率いずれについても証明書チェーンの情報を削除した場合が最も低い値となった．これにより，提案手法で学習データを作成した場合, 証明書チェーンの情報がベイジアンフィルタの精度の向上に最も貢献していると推測できる．また有効期間を削除したデータを学習した正答率・再現率・適合率は，3 要素全てを学習した場合の正答率・再現率・適合率との差が最も小さかった．本研究で採用したネゴシエーション情報の三つのうち, 有効期間が最も精度の向上に寄与していないと推測できる．

5. 考察

4 章での実験結果から, 本研究で着目するネゴシエーション情報の要素を用いた判定により, 正答率 71.0%, 再現率 51.7%, 適合率 66.3%という結果を得た．この結果と最も近い学習結果は, ネゴシエーション情報から取り出した個別の要素について学習した際に深度が 2 の認証局で行った学習結果であった．具体的には, 正答率が 71.6%, 再現率が 56.6%, 適合率が 65.5%である．さらに, 本研究で注目した証明書チェーン・有効期間・TLS 拡張というネゴシエーション情報における三つの要素について二つずつの組み合わせで学習を行ったところ, 証明書チェーンを除いた場合の精度が最も低かった．よって, 本研究で調査したネゴシエーション情報の要素のうち最も判定の精度に影響を与えるのは証明書チェーンだと判断できる．証明書チェーンに含まれる個別の認証局情報は, 発行する証明書の性質に影響を与えるといえる．

本研究で注目したネゴシエーション情報の要素を用いたフィルタは, Cisco Umbrella を用いた場合正答率が 7 割程

度となった．その理由としては, ネゴシエーション情報に関する環境が非常に短期間で変化している状況が挙げられる．SSL/TLS 証明書を取り巻く環境が近年急速に変化しているため 良性サイト群・悪性サイト群に固定した特徴が現れづらく, 判定を困難にしている可能性がある．例えば，証明書の有効期間において, 主要なブラウザを提供するベンダのうち数社が相次いで, 2020 年より証明書の有効期間を最長 398 日に制限すると発表した．Mozilla が提供する firefox では 2020 年 8 月 31 日以降に発行された有効期間が 398 日より大きい証明書を信用しないと発表している [7]. 同様に Apple が提供する Safari, Google が提供する Chrome についても 2020 年 9 月 1 日以降に発行された有効期間が 398 日より大きい証明書を信用しないという発表がなされた [1][5]. 信用する有効期間の長さが 398 日以下に制限されたことで, 良性サイト群で用いられる証明書の有効期間が変化したことが予測できる．

さらに, 精度を上げるために他の情報と組み合わせる手法も考えられる．例えば, ドメイン情報に着目して同様の推定を行う研究が存在する．米谷の研究 [14] ではサイトのドメイン情報により着目し, データのクラスタリングを試みている．ネゴシエーション情報の定義を拡張し, ドメイン情報を学習の対象に加えれば精度が向上する可能性がある．

6. 結論

本研究では，個人情報等の機密情報を送信する前に通信相手の信用度を判定することを目的とし, 良性サイト群・悪性サイト群それぞれから得られるネゴシエーション情報を収集・分析した．またネゴシエーション情報内の証明書チェーン・有効期間・TLS 拡張というパラメータを ベルヌーイイベントモデルに適用するためにベクトル化手法を決定した. 具体的には，深度 2 の認証局，有効期間の区切りとしては 89 日とした．そしてベルヌーイナイーブベイズを用いてベイジアンフィルタを作成し, 五倍交差検定で正答率・再現率・適合率・真陰性率に関する評価を行った．

学習の結果, 良性サイト群として Cisco Umbrella を使用した場合, 悪性サイトを判定する信用度の正答率が 71.04%, 再現率が 51.70%, 適合率が 66.33%, 真陰性率が 83.61%であった．一方, 良性サイト群として Value.Today を使用した場合，悪性サイトを判定する信用度の正答率が 85.36%, 再現率が 94.56%, 適合率が 89.10%, 真陰性率が 28.26%であった．

今後の課題として, ドメイン情報と組み合わせてた場合に信用度の判定精度がどのように変化するかを調査することや，サーバの TLS の設定，Web サーバの設定などの情報と組み合わせた場合にどのように変化するかを調査することなどが挙げられる．

参考文献

[1] Apple: About upcoming limits on trusted certificates, https://support.apple.com/en-us/HT211025. Accessed : 2020-01-10.
[2] Cisco Umbrella: Cisco Umbrella, https://umbrella.cisco.com/blog/cisco-umbrella-1-million. Accessed:2020-12-22.
[3] Deshpande, V. P., Erbacher, R. F. and Harris, C.: An Evaluation of Naïve Bayesian Anti-Spam Filtering Techniques, *2007 IEEE SMC Information Assurance and Security Workshop*, pp. 333–340 (online), DOI: 10.1109/IAW.2007.381951 (2007).
[4] DigiCert: DigiCert Trusted Root Authority Certificates, hhttps://www.digicert.com/kb/digicert-root-certificates.htm. Accessed:2021-01-05.
[5] Google: Enforce 398-day validity for certificates issued on-or-after 2020-09-01, https://chromium.googlesource.com/chromium/src/+/ae4d6809912f8171b23f6aa43c6a4e8e627de784. Accessed : 2020-01-10.
[6] Internet Security Research Group: Let's Encrypt - Free SSL/TLS Certificates, https://letsencrypt.org/. Accessed:2019-07-04.
[7] Mozilla: Mozilla Security Blog - Reducing TLS Certificate Lifespans to 398 Days, https://blog.mozilla.org/security/2020/07/09/reducing-tls-certificate-lifespans-to-398-days/. Accessed : 2020-01-10.
[8] OpenSSL Software Foundation: x509v3_config., https://www.openssl.org/docs/man1.0.2/man5/x509v3_config.html. Accessed : 2020-10-29.
[9] PhishTank: PhishTank, https://www.phishtank.com/. Accessed:2021-01-01.
[10] Schneider, K.-M.: A Comparison of Event Models for Naive Bayes Anti-Spam e-Mail Filtering, *Proceedings of the Tenth Conference on European Chapter of the Association for Computational Linguistics - Volume 1*, EACL '03, USA, Association for Computational Linguistics, p. 307–314 (online), DOI: 10.3115/1067807.1067848 (2003).
[11] SteveBlack: SteveBlack/hosts, https://github.com/StevenBlack/hosts. Accessed:2020-12-20.
[12] 田端利宏：SPAM メールフィルタリング：ベイジアンフィルタの解説 (¡特集¿情報のフィルタリング)，情報の科学と技術，Vol. 56, No. 10, pp. 464–468（オンライン），入手先 ⟨https://ci.nii.ac.jp/naid/110004811940/⟩ (2006).
[13] Value: Value.Today, https://www.value.today/. Accessed:2020-01-28.
[14] 米谷嘉朗：ドメイン名関連情報を使用したドメイン名悪用兆候の数値化と指標化の提案，インターネットと運用技術シンポジウム論文集，Vol. 2020, pp. 25–32 (2020).