Computer Security Symposium 2022
24 - 27 October 2022

悪性サイトにおける常時HTTPS化の普及に関する一考察

大森 幹之[1,a)]

概要：フィッシングやマルウェア感染を招く悪性サイトでも AOSSL (Always-On SSL，常時 HTTPS 化) が普及しつつある．そして，常時 HTTPS 化において，ホスト名といった CN (Common Name) をも平文で送信せず，暗号化する TLS 1.3 も広まりつつある．これにより，未知の悪性サイトを TLS のハンドシェイク時に検知することがより困難になると考えられる．そこで，本稿では，実ネットワークにおいて，TLS 1.3 を採用していると推察される悪性サイトの一部の数を示し，悪性サイトにおける常時 HTTPS 化の普及について考察する．

キーワード：SSL/TLS，常時 HTTPS 化，DV 証明書，TLS1.3，ウェブ

Consideration on Always-On SSL Deployment in Malicious Sites

Motoyuki Ohmori[1,a)]

Abstract: AOSSL (Always-On SSL, HTTPS) is becoming popular even for malicious sites that cause phishing and malware infection. In addition, TLS 1.3, which encrypts CN (Common Name) such as host names without sending them in plain text, is becoming popular. TLS 1.3 may make it more difficult to detect unknown malicious sites during the TLS handshake. Therefore, in this paper, we present some numbers of malicious sites that are presumed to adopt TLS 1.3 in real networks, and discuss the spread of AOSSL in malicious sites.

Keywords: SSL/TLS, AOSSL, DV certificate, TLS1.3, Web

1. はじめに

ウェブページのコンテンツの通信に常時 SSL/TLS を適用する，いわゆる常時 HTTPS 化が普及しつつある．例えば，Google のウェブブラウザである Chrome の通信の内，米国では 95%以上，日本では 89%以上，その他の主要な国でも 90%以上が HTTPS 化された暗号化通信であると報告されている [1]．それに伴い，フィッシングやマルウェア感染を招く悪性サイトの HTTPS 化も進んでいる [2]．以前と比較すると HTTPS 化されたサイトの増加は鈍化しているものの，2021 年上四半期には 83%のフィッシングの悪性サイトが HTTPS 化していると報告されている [3]．また，それらの HTTPS 化されたフィッシングサイトの内，94.5%が DV (Domain Validation) 証明書を採用していたとも報告されている [3]．HTTPS 化により通信が暗号化されていると，ファイアウォールやサンドボックスが，フィッシングサイトなどのコンテンツの平文を検査できず，未知の悪性サイトを検知することが難しくなる．ファイアウォールといったネットワーク機器で復号し，コンテンツの平文を検査する手法も従来から存在するが，復号によるネットワーク機器の負荷の増大や復号に必要なルート CA 証明書の配布が困難であるといった課題がある．

そのため，HTTPS 化された通信においても，SSL/TLS の通信開始時の暗号化されていない電子証明書の特徴量などに基づいた悪性サイトの検知が試みられている [2], [4], [5], [6], [7]．しかし，HTTPS 化で用いられる最新のプロトコルである TLS 1.3 [8] では，ウェブサイ

[1] 鳥取大学情報基盤機構
Organization for Information and Communication Technology, Tottori University
[a)] ohmori@tottori-u.ac.jp

トの FQDN (Fully Qualified Domain Name) である CN (Common Name) や電子証明書といった特徴量が暗号化されてしまう．そのため，TLS 1.3 の通信に対しては，暗号化されていない特徴量のみから悪性サイトを検知することが難しくなることが予想される．

そこで，本稿では，実際の鳥取大学のキャンパスネットワークにおいて，TLS 1.3 の普及とその悪性サイトでの利用を明らかにし，考察する．TLS 1.3 の普及の確認あたっては，TLS 1.2 以前では暗号化されることのなかった電子証明書やそれに含まれる CN といった特徴量の抽出の可否を指標とする．また，悪性サイトでは最新のプロトコルが適用されることが少ないと推察し，最新の TLS 1.3 ではない，つまり，TLS 1.2 以前を用いて HTTPS 化された通信を検知する．特に，悪性サイトの HTTPS 化で採用されることの多い DV 証明書に着目し，DV 証明書を利用したサイト（以下 DV 証明書サイトという）の検知を試みることで，TLS 1.2 以前を用いた悪性サイトを明らかにする．

本稿の構成は以下のとおりである．2 節では，DV 証明書サイトの検知手法を述べる．3 節では，鳥取大学における DV 証明書サイトへの通信の内，TLS 1.2 以前を用いている通信の検知を試みる．4 節では，HTTPS 化された悪性サイトの検知について考察する．5 節では，関連研究に言及する．最後に，6 節で本論文をまとめる．

2. DV 証明書サイトの検知

2.1 SSL/TLS ハンドシェイクと DV 証明書サイト

TLS 1.2 以前において，SSL/TLS のハンドシェイクでは，Server Hello メッセージに続く Server Certificate メッセージにサイトの電子証明書が含まれる [8]．この電子証明書は TLV (Type, Length, Value) 型の ASN.1 (Abstract Syntax Notation One) の BER (Basic Encoding Rules) により文字列以外はバイナリでエンコードされている．そのため，Server Certificate メッセージ内の DV 証明書を検知することで，DV 証明書サイトを検知できる．

実ネットワークでは，DV 証明書にマッチする正規表現を検知パターンとして定義し，次世代ファイアウォール上でのカスタムシグネチャとして追加することにより検知可能となる．本稿では，一例として，パロアルトネットワークス社の次世代ファイアウォール (以降パロアルト) 上での検知パターンを次節以降に示す．そして，パロアルトの設定変更のみで実装することで，運用性も保ちつつ，DV 証明書サイトの検知を可能となる．

パロアルトでは脆弱性防御機能のカスタムシグネチャを作成することで実現できる．この脆弱性防御機能では，Server Certificate メッセージは `ssl-rsp-certificate` という**コンテキスト**として定義されている．`ssl-rsp-certificate` のコンテキストに限定して DV 証明書を検知することによって，誤検知を削減できる．

DV 証明書の検知パターンを導出するにあたり，以下の点を考慮した．

- パロアルトの OS である PanOS 9.1 以前では 7 個以上の連続した固定値を正規表現に含むことが必要である [9]．
- 連続した固定値の長さが短い正規表現はパターンマッチの負荷が高くなる可能性がある．
- パロアルトではテキスト以外（つまり 16 進数でのバイナリデータ）の正規表現も設定可能である．

2.2 発行者の Subject による検知

本検知パターンでは，DV 証明書に必ず含まれる電子証明書の発行者の Subject の文字列を個別に指定することで，DV 証明書を検知する．この検知パターンは当該発行者が DV 証明書のみを発行している場合に限られる．ここでは，図 **1** の様に発行者の Subject のみを指定する正規表現を考える．では，文字列のみに留めることとする．

```
Let's\sEncrypt
```

図 **1** 発行者の Subject にマッチする正規表現例 (Let's Encrypt)

2.3 DV オブジェクトの検知

CA/ブラウザフォーラムは，DV 証明書に特有な DV オブジェクト (OID: 2.23.140.1.2.1) を定めている [10]．そこで，DV オブジェクトにマッチする正規表現を考え，DV 証明書を検知する．表 **1** に DV オブジェクトのバイト列を示す．このバイト列は固定値が 10 個続く．これは，前述の他の正規表現よりも長く，PanOS 9.1 以前でも利用可能である．実際，PanOS 8.1.16 では設定は可能であった．図 **2** に DV オブジェクトを検知する正規表現を示す．

表 **1** DV オブジェクト

off	hex	fix	意味
0	30	o	sequence
1	08	o	length (8 バイト)
2	06	o	object identifier
3	06	o	length (6 バイト)
4	67	o	DV オブジェクト (**2.23.140**.1.2.1)
5	81	o	DV オブジェクト (**2.23.140**.1.2.1)
6	0c	o	DV オブジェクト (**2.23.140**.1.2.1)
7	01	o	DV オブジェクト (2.23.140.**1**.2.1)
8	02	o	DV オブジェクト (2.23.140.1.**2**.1)
9	01	o	DV オブジェクト (2.23.140.1.2.**1**)

```
\x30 08 06 06 67 81 0c 01 02 01\x
```

図 **2** DV オブジェクトにマッチする正規表現

2.4 その他の検知パターン

本節では，前述の 2 つの検知パターン以外の検討したものの，動作しなかった検知パターンを参考までに示す．

2.4.1 O と OU が存在しないことを検知するパターン

DV 証明書も含めてサイト用の電子証明書では，Subject には CN が含まれる．また，OV (Organization Validation) 証明書や EV (Organization Validation) 証明書では O (Organization)，OU (Organization Unit) が含まれる．一方で，DV 証明書では O や OU は含まれない．そのため，O と OU を含まないことを検知することで DV 証明書を検知できると考えられる．なお，実際には，SSL/TLS のハンドエシェイク時には，サイトの証明書だけでなく，その発行者である中間 CA 証明書も同時に送信される．中間 CA 証明書には，O が含まれるため，ここで検討した検知パターンでは，DV 証明書サイトを検知できない．ここでは，参考までに，検討した検知パターンを示す．

さて，「O と OU を含まない」ことは「O を含み，かつ，OU を含む」の否定である．そこで，「O を含む」と「OU を含む」の正規表現を考え，それらの論理積の否定を検知パターンとする．表 **2** に SSL/TLS での電子証明書に含まれる O を示す．図 **3** が O にマッチする正規表現である．図 3 はパロアルトにおける正規表現であり，\x で挟まれる箇所は 16 進数で表現されたバイト列である．ドット (.) は一般的な正規表現と同様任意の 1 文字を表す．OID (Object ID) が 2.5.4.11 である OU に関しても同様に正規表現を定義できる．

表 **2** 電子証明書に含まれる O

off	hex	fix	意味
0	30	o	type: sequence
1	??		length: ?バイト
2	06	o	type: object identifier
3	03	o	length: 3 バイト
4	55	o	X.500 O (**2.5**.4.10)
5	04	o	(2.5.**4**.10)
6	0a	o	(2.5.4.**10**)
7	13	o	type: PrintableString (0x0c UTF-8 も取り得る)
8	??		length: ?バイト
9	??		O の文字列

```
\x30\x.\x06 03 55 04 0a 13\x
```

図 **3** O にマッチする正規表現 (PrintableStirng の場合)

なお，O と OU の正規表現は連続した固定値が 6 バイトしか続かず，7 バイト未満のため，古い PanOS では動作しなかった．また，CA/ブラウザフォーラムでは，2022/9/1 より OU を含んだ電子証明書の発行を禁止することが可決されている．

2.4.2 C が存在しないことを検知するパターン

正式に定められた文書を発見できていないが，DV 証明書には C (Country) も含まれないと仮定すると，C を含まない検知パターンにより，DV 証明書を検知できると考えられる．C は ISO 3166 で定められた 2 文字の国コードを値として持ち，電子証明書内では表 **3** に示される様な構成を取る．そのため，C にマッチする正規表現としては図 **4** が考えられる．この正規表現は連続した固定値が 9 バイト以上続くため，古い PanOS でも動作する可能性を期待できる．そして，「C を含まない」ことを「C を含む」の否定と考え，この正規表現にマッチしない，という検知パターンとする．

なお，検知パターンは，2.4.1 節と同様に，DV 証明書サイトを正しく検知できない．SSL/TLS ハンドシェイク時に含まれる中間 CA 証明書などに C が含まれるからである．

表 **3** 電子証明書に含まれる C (日本)

off	hex	fix	意味
0	30	o	type: sequence
1	09	o	length: 9 バイト
2	06	o	type: object identifier
3	03	o	length: 3 バイト
4	55	o	X.500 Country (**2.5**.4.6)
5	04	o	X.500 Country (2.5.**4**.6)
6	06	o	X.500 Country (2.5.4.**6**)
7	13	o	type: PrintableString (0x0c UTF-8 も取り得る)
8	02	o	length: 2 バイト
9	4a		J
10	50		P

```
\x30 09 06 03 55 04 06 13 02\x
```

図 **4** C にマッチする正規表現 (PrintableStirng の場合)

2.4.3 CN のみを含む Subject の検知パターン

2.4.1 節や 2.4.2 節よりも正確に直接的に Subject 内に O と OU が含まれていない DV 証明書を検知する検知パターンである．電子証明書の Subject そのものを一意に表す OID は定義されていない．有効期限の後に置かれるオブジェクトの列 (sequence) と集合 (set) が Subject である．表 **4** に実際の DV 証明書の CN とその前後のバイト列を示す．

そこで，ここでは，以下のいずれも満たされる場合，O や OU を含まない電子証明書，すなわち，DV 証明書とみなすこととする．

(1) 有効期限の直後に Subject が続く．

(2) Subject の先頭が CN である．

後者に関しては，Subject である DN (Distinguished Name) に現れるオブジェクトの順番は，C，O，OU，L

(Locality)，CN であることが多いという仮定に基づいている．この仮定が真であれば，Subject の先頭が CN であれば O や OU が含まれないことは保証される．この仮定の真偽については，X.500 や X.501，RFC5280，RFC4514 などを精査する必要がある．X.501 [11] では Subject である DN (Distinguished Name) に現れるオブジェクトの順番を定めていない様である．慣例的には，X.509 の証明書では上記の仮定の通りの順であり，LDAP などでは逆順にして表示する様である．

なお，国立情報学研究所 (NII: National Institute of Informatics) が運用している電子証明書発行サービスである UPKI で発行される証明書は，上記のオブジェクト順である．

一方，UPKI への申請で提出する TSV (Tab Separated Values) ファイルでは，Subject である DN は逆順となっており，CN が先頭で O が後に続いている [12].

表 **4**　Let's Encrypt の DV 証明書の一部 (CN とその前後)

off	hex	fix	意味
-2	5a	o	Validity の最後の Z
-1	30	o	type: sequence: Subject の先頭
0	14		length: 20 バイト
1	31	o	type: set
2	12		length: 18 バイト
3	30	o	type: sequence
4	10		length: 16 バイト
5	06	o	type: object identifier
6	03	o	length: 3 バイト
7	55	o	X.500 CommonName (**2.5**.4.3)
8	04	o	X.500 CommonName (2.5.**4**.3)
9	03	o	X.500 CommonName (2.5.4.**3**)
10	13	o	type: PrintableString (0x0c UTF-8 も取り得る)
11	09		length: 9 バイト
12	6c		l
13	65		e
14	6e		n
15	63		c
16	72		r
17	2e		.
18	6f		o
19	72		r
20	67		g
21	30	o	type: sequence: Subject public key info の先頭
22	22		length: 34 バイト

表 4 から分かる様に，電子証明書の有効期限の直後に続く sequence が Subject である．そして，有効期限の末尾は一般に「Z」である．これは，有効期限はテキスト文字で電子証明書に含まれており，協定世界時 (UTC) が ISO 8601 で表現され必ず「Z」になるからである．そのため，有効期限の末尾の「Z」に続く，sequence，set の先頭にある CN は，Subject 内の CN であるはずである．以上を踏まえ，O と OU を含まず CN のみを含む Subject にマッチする正規表現を図 **5** に示す．

```
\x5a30\x.\x31\x.\x30\x.\x060355040313\x
```

図 **5**　CN のみを含む Subject にマッチする正規表現

なお，前述のとおり，ここで示した正規表現は，連続した固定値が最長でも 6 文字であり，PanOS 9.1 以前では利用できない．また，Subject の直後が Subject public key info であることを保証する様な正規表現でより厳密に CN 内に O と OU が含まれないことも考えられる．

本検知パターンでは，DV 証明書を検知できた．しかし，パロアルトの CLI で `show bad-custom-signature` コマンドにより確認したところ，パフォーマンスが悪い正規表現である旨が表示された (図 **6**)．そのため，本検知パターンは実運用には適さないと考えられる．

```
admin@PA-VM> show bad-custom-signature

bad performance custom signature list:
TID: 41102, Vsys 1, Context: ssl-rsp-certificate,
Pattern \x5a30\x.\x31\x.\x30\x.\x060355040313\x
```

図 **6**　パフォーマンスが悪いと判定された正規表現

3. DV 証明書サイトの検知結果

3.1 検証環境

鳥取大学のパロアルト PA-5220 で 2.2 節および 2.3 節で示した検知パターンを設定し，TLS 1.2 以前を採用した DV 証明書サイトを検知した．2.2 節における DV 証明書の発行者としては，広く利用されていると考えられる Let's Encrypt だけを設定した．PanOS は 8.1.16 であり，脅威防御，URL フィルタリング，WildFire，DNS セキュリティのライセンスが有効であった．

3.2 DV 証明書セッション数

表 **5** に，鳥取大学における検知された 月毎の SSL/TLS のセッション数と検知できた DV 証明書のセッション数を示す．表 5 から，全ての SSL/TLS セションの内，0.40% のみが，検知できた DV 証明書サイトであった．つまり，99.6%のセッションが，TLS 1.3 を採用していたと考えられる．このことから，TLS 1.2 以前を用いているサイトは少数であると推測される．また，学内でも DV 証明書サイトが確認できたが，セッション数，FQDN 数いずれも 1% 未満と少数であった

*1　期間全体を通じて一意の FQDN の総数．各月の合計ではない．

表 5　SSL/TLS セッション数と DV 証明書セッション数 (2021/4/21 から 12/31 まで)

		DV 証明書		FQDN 数	
月	SSL/TLS	総数	学内	総数	学内
4	136510310	508464	44364	21039	26
5	473039730	1985794	193730	43666	29
6	589203465	2410876	190387	53294	37
7	639196346	2505153	196997	48282	26
8	447540390	1870734	205234	38877	32
9	503926358	2341165	183087	43189	32
10	619292518	2606252	49813	49245	26
11	603683472	2165780	22477	46300	26
12	640696503	2287530	20615	41313	22
総数	4653089092	18681748	1106704	168337*1	38*1

SSL/TLS: 443 番ポートのセッション数．QUIC なども含む．また，TCP コネクションなどが確立できなかったものも含む．

3.3 TLS 1.2 以前を採用した悪性サイト

3.2 節で検知された DV 証明書サイトの内，鳥取大学において過去に検知された悪性サイトと同様の TLD の一部に属するサイトについて，その悪性度について，VirusTotal と Google Safe Browsing を用いて検証した (表 **6**)．表 6 から，検知された DV 証明書サイトで TLD を限定すれば，60%以上が悪性であり得ることが分かる．

4. 考察

4.1 NII-SOCS 通知の悪性サイトでの HTTPS 化

NII が実施している大学間連携に基づく情報セキュリティ体制の基盤構築 (NII-SOCS: NII Security Operation Collaboration Services) では，各参加大学のファイアウォール以降のインターネットとの通信，つまり，SINET (Science Information NETwork) を経由する通信からインシデントを検知する．ここでは，NII-SOCS から通知されたインシデントに関連した悪性サイトでの HTTPS 化について考察する．

2021/4/21 から 8/31 までの間，鳥取大学で NII-SOCS から通知を受けたインシデントについて確認した．当該期間の内，インシデントは 21 件あり，その内 16 件が HTTP であり，残りの 5 件が HTTPS 化されていた．このことから，NII-SOCS が検知した悪性サイトの内，23.8%で HTTPS 化が普及していたと言える．また，HTTPS 化されていた 5 件全てで 2 節で述べた手法では検知できなかった．そのため，この 5 件の内，少なくとも 3 件は TLS 1.3 を用いていたと考えられる．残りの 2 件は，パロアルトの脆弱性防御機能によって通信が遮断されていたため，TLS 1.3 の採用の事実については不明である．

4.2 悪性サイトでの HTTPS 化の普及

3.2 節で示した様に，鳥取大学においては，全 SSL/TLS セッションの内，99$\dot{6}$ また，4.1 節で前述のとおり，NII-SOCS から通知された悪性サイトの内少なくとも 60%以上は，TLS 1.3 を採用していると考えられ，悪性サイトでの HTTPS 化の普及も進みつつあると考えられる．その一方で，TLS 1.2 以前を採用しているサイトの内，過去に検知された悪性サイトと同様の TLD を持つサイトは，TLD を限定すれば，60%以上の確率で悪性と判定され得ることが明らかとなった．このことから，TLS 1.2 を採用している悪性サイトは一定数存在すると考えられる．そのため，現状では，SSL/TLS ハンドシェイク時に得られる暗号化されていない電子証明書の特徴量を用いて悪性サイトを判定することには，一定の意義があると考えられる．しかし，今後，ウェブブラウザが TLS 1.2 以前を採用しない様になる将来においては，SSL/TLS ハンドシェイク時に得られる特徴量は限定的になると予想される．

5. 関連研究

Dong らは電子証明書の特徴を機械学習により分類しフィッシングサイトの実時間での検知手法を提案した [4]．しかし，2015 年当時よりも DV 証明書がより普及している現在での有効性は明らかではない．特に，電子証明書の特徴の 1 つとして電子証明書の発行元により信頼度を定義しているものの，DV 証明書の発行元については考慮してない．

Drury らは HTTPS 化されたフィッシングサイトにおける電子証明書などの特徴を調査し，フィッシングサイトとそれ以外で一般的な明確な差はないと報告している [2]．その一方で，正規のサイトとそれを模倣したフィッシングサイトそれぞれの電子証明書の特徴には差が見られているとしている．

米谷はドメイン名や電子証明書の特徴からドメイン名をスコア化する手法を提案している [5]．また，CT (Certificate Transparency) ログを利用し，フィッシングされる以前の電子証明書が発行される段階でのフィッシング被害の防止を目指している．そして，クライアントのウェブブラウザなどでの悪性サイトへのアクセス防止を目指している．

大屋らは，SSL/TLS ハンドシェイク時に取得可能な情報にベイジアンフィルタを適用し，悪性サイトを検出する手法を提案している [6]．

6. おわりに

本稿では，鳥取大学における通信において，全体の 99.6%以上のセッションで TLS 1.3 が採用されていることを明らかにした．また，NII-SOCS から通知されるインシデントで明らかになった悪性サイトの内，少なくとも 60% は TLS 1.3 を用いていることが明らかとなった．その一方で，DV 証明書を採用している悪性サイトの内，TLD を限定

表 **6** 悪性 TLD による検知数 (2021/4/21 から 2022/2/28 まで)

月	総数	悪性	SB	VT	FQDN 数	悪性	SB	VT
4	21861	10773	0	10773	336	77	0	77
5	132299	83265	0	83265	1056	209	0	209
6	158392	73079	74	73071	1256	243	11	241
7	156039	56765	286	59461	1168	250	39	237
8	99685	55161	428	43669	1010	246	71	213
9	136647	56646	626	56020	1185	185	-	185
10	159966	53439	736	52703	1340	223	-	223
11	1025	325	0	325	31	12	-	12
12	191641	53300	212	53088	1244	209	-	209
1	120279	36543	160	36383	976	139	-	139
2	144552	27026	158	26868	935	129	-	129

悪性: 以下の SB もしくは VT が悪性と判定した一意な FQDN の数.
SB: Google Safe Browsing (脅威種別は URL) が悪性と判定した数.
VT: VirusTotal のドメイン解析または URL 解析により，1 回もしくは 1 つの解析が悪性もしくはその疑いがあると判定した数.

して考えると，60%以上が TLS 1.2 を採用していることが明らかになった．そのため，現時点では，TLS 1.2 以前では暗号化されない電子証明書の特徴量を SSL/TLS ハンドシェイク時に検知することによって，悪性サイトを検知する手法には一定の意義があると考えられる．

謝辞　本研究の一部は JSPS 科研費 22K11992 の助成を受けたものである．

参考文献

[1] Google LLC: HTTPS encryption on the web, `https://transparencyreport.google.com/https/overview` (2021). Accessed on 2021/8/1.

[2] Meyer, U. and Drury, V.: Certified Phishing: Taking a Look at Public Key Certificates of Phishing Websites, *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, Santa Clara, CA, USENIX Association, pp. 211–223 (online), available from ⟨`https://www.usenix.org/conference/soups2019/presentation/drury`⟩ (2019).

[3] Anti-Phishing Working Group: Phishing Activity Trends Report 1st Quarter 2021, `https://apwg.org/trendsreports/` (2021). Accessed on 2021/8/28.

[4] Dong, Z., Kapadia, A., Blythe, J. and Camp, L. J.: Beyond the lock icon: real-time detection of phishing websites using public key certificates, *2015 APWG Symposium on Electronic Crime Research (eCrime)*, pp. 1–12 (online), DOI: 10.1109/ECRIME.2015.7120795 (2015).

[5] 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).

[6] 大室高帆，新城　靖，中井　央，三宮秀次，星野　厚，佐藤　聡：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，No. 17 (2021).

[7] 大森幹之：SSL/TLS での DV 証明書の利用に着目した未知の悪性サイトへのアクセス防止，情報処理学会インターネットと運用技術シンポジウム論文集，Vol. 2021, pp. 1–8 (2021).

[8] Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.3, RFC 8446 (2018).

[9] Palo Alto Networks, Inc.: TECHDOCS: Custom Signature Pattern Requirements (2021). Accessed on 2021/4/21.

[10] CA/Browser Forum: Object Registry of the CA/Browser Forum, `https://cabforum.org/object-registry/` (2011). Accessed on 2021/8/1.

[11] ITU: X.501 : Information technology - Open Systems Interconnection - The Directory: Models (2019). Accessed on 2021/4/20.

[12] 国立情報学研究所：サーバ証明書発行申請 TSV フォーマット, `https://certs.nii.ac.jp/manual/TSV_File_Format/issue/02`. Accessed on 2021/4/21.