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

大森 幹之[1,a)]

概要：ウェブページなどのサイトで AOSSL (Always-On SSL，常時 HTTPS 化) が普及し，フィッシングやマルウェア感染を招く悪性サイトの通信の暗号化も増加している．そこで，我々は，常時 HTTPS 化された悪性サイトが DV (Domain Validation) 証明書をしばしば採用する点に着目し，TLS/SSL ハンドシェイクにおける未知の悪性サイトへのアクセス防止を実ネットワークの次世代ファイアウォール上で実装した．悪性サイトの判定にあたっては，DV 証明書を利用している良性サイトも存在するため，DV 証明書だけでなく，DDNS (Dynamic DNS) や悪性の可能性が高い TLD (Top-Level Domain) の利用を元に悪性サイトを判定した．一方，誤判定でも可用性の劣化を最小限に抑えるため，悪性サイトと判定されても，警告ページへリダイレクトし利用者が閲覧継続ボタンを押下することで閲覧可能とした．そして，これらを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の設定変更のみで実装し，運用性も保ちつつ，未知の悪性サイトへのアクセス防止を試みた．その結果，49.1% の精度で TLD によって悪性サイトへのアクセスを防止できた一方，DDNS による悪性判定は誤判定のみであったことが明かになった．

キーワード：AOSSL，常時 HTTPS 化，常時 SSL 化，フィッシング被害防止，マルウェア感染防止，SSL，TLS，DV 証明書

A Challenge on-the-Fly Preventing an Access to a Malicious Site Considering a DV Certificate in a SSL/TLS Communication

Motoyuki Ohmori[1,a)]

Abstract: Not only many benign sites but also malicious sites for phishing or malware are now implementing *Always-On SSL* (AOSSL). We have, therefore, implemented an on-the-fly access prevention to a unknwon malicious site on a next-generation firewall running in the wild, considering that many AOSSLed malicious sites adopt Domain-Validated (DV) certificates. We judged a malicious site by not only DV certificate but also dynamic DNS (DDNS) and malicious Top-Level Domain (TLD). In order to reduce usability regressions as much as possible, a user was redirected to a warning page, and could access to the site user confirmed by cliking the continue button. We tried to implement these by configuration chages only on the next-generation firewall developved by Palo Alto Networks, Inc., and keep operability and an access prevention. TLD based detection could detect malicious sites by 49.1% accuracy while no malicious sites was detected by DDNS.

Keywords: AOSSL, phishing prevention, malware infection prevention, SSL, TLS, DV certificate

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 SSL/TLS を用い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

[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

前と比較すると HTTPS 化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．

この様な状況でも，次世代ファイアウォールなどでは，悪性サイトの URL や IP アドレスなどのデータベースを参照することで，既知の悪性サイトへのアクセスは遮断できる．しかし，やはり未知の悪性サイトは検知できない．そのため，未知の悪性サイトへのアクセスを防止する手法が必要である．

そこで，我々は，常時 HTTPS 化された悪性サイトが DV 証明書をしばしば採用する点に着目し，未知の悪性サイトへのアクセス防止を実ネットワークの次世代ファイアウォール上で実現する．SSL/TLS のハンドシェイク時に DV 証明書を検知するため，次世代ファイアウォールのカスタムシグネチャを検討する．そして，DV 証明書を利用している良性サイトも存在するため，DV 証明書だけでなく，DDNS (Dynamic DNS) を利用しているサイトを悪性サイトと判定する．また，DDNS を利用していない場合でも，悪性サイトで頻繁に利用される TLD (Top-Level Domain) に属するサイトも悪性と判定する．一方，誤判定でも利便性の劣化を最小限に抑えるため，悪性サイトと判定された場合には，警告ページへリダイレクトし利用者が閲覧ボタンを押下することで閲覧可能とする．そして，これらを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) の設定変更のみで実装することで，運用性も保ちつつ，未知の悪性サイトへのアクセス防止を実現する．

本稿の構成は以下のとおりである．2 節では，SSL/TLS での DV 証明書の正規表現を用いた検知パターンを検討する．3 節では，パロアルトでの悪性サイトへのアクセス防止の実現方法について述べる．4 節では，提案手法を実ネットワーク上で実装した結果を示す．5 節では，提案手法などについて考察する．6 節では，関連研究に言及する．最後に，7 節で本論文をまとめる．

2. SSL/TLS での DV 証明書の検知パターン

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 [4]．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 証明書にマッチするパターンを正規表現で表現できれば，DV 証明書を検知できると考えられる．ここでは，DV 証明書の検知パターンを以下の点も考慮し検討する．

- 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 [5]．
- 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）の正規表現は入力可能ではあるものの，正式にサポートされていない可能性がある．

2.1 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 にはサイトの FQDN (Fully Qualified Domain Name) である CN (Common Name) 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．そして，「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 **1** に SSL/TLS での電子証明書に含まれる O を示す．図 **1** が O にマッチする正規表現である．図 1 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 **1**　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 OU (**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 **1**　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 では動作しないと予想される．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．

2.2 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し，C を含まないパターンを考える．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 **2** 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 **2** 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．

表 **2** 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 **2** C にマッチする正規表現 (PrintableStirng の場合)

2.3 CN のみを含む Subject の検知パターン

2.1 節や 2.2 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 証明書を検知する手法を考える．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 **3** 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 [6] 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 [7].

表 **3** 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 3 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 **3** に示す．

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

図 **3** 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と予想される．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．しかし，パフォーマンスの劣化も懸念されたため，ここでは採用しない．

2.4 発行者の **Subject** を用いた検知パターン

本手法では DV 証明書に必ず含まれる発行者の 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．この手法は当該発行者が DV 証明書のみを発行している場合に限られる．ここでは，`Let's\sEncrypt` の様に発行者の Subject のみを指定する正規表現を考える．ASN.1 の seuqnce や set なども含めて指定することで，より厳密な正規表現にもできるが，PanOS でバイナリ値を含む正規表現が動作するか不明だったため，ここでは，文字列のみに留めることとする．

2.5 **DV** オブジェクトの検知パターン

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 [8]．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 **4** 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と予想される．図 **4** に DV オブジェクトを検知する正規表現を示す．

なお，4.2.5 節で後述のとおり，PanOS 8.1.16 では設定は可能であったが，動作しなかったことに注意されたい．

表 **4** 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 **4** DV オブジェクトにマッチする正規表現

3. 悪性サイトへのアクセス防止

3.1 悪性サイトへのアクセス防止の概要

悪性サイトへのアクセスを防止するため，DV 証明書で常時 HTTPS 化されたサイトへのアクセスを次世代ファイアウォールで以下の様に制御する．

(1) 利用者が DV 証明書のサイトへアクセス
(2) SSL/TLS のハンドシェイク時に DV 証明書を検知
(3) DV 証明書かつ後述の悪性サイトの条件を満たす場合，悪性と判定し，警告ページを表示 (もしくは，ブロック)
(4) 警告ページで閲覧継続ボタンを利用者が押下するとサイトへのアクセスを許可

3.2 パロアルトでの設定の概要

3.1 節で示したアクセス制御をパロアルトでは 1 つの機能のみでは実現できない．脆弱性防御機能，URL フィルタリング機能，タグ機能，ログ転送機能，IP アドレスのアドレスグループ機能などを組み合わせることにより実現できる．具体的には以下の様な設定で実現できる．

(1) 脆弱性防御機能のカスタムシグネチャの作成
2 節で示した検知パターンを用いて DV 証明書を検知し脅威ログを生成させる．
(2) タグの追加
DV 証明書サイトの IP アドレスに付与するタグを事前に定義しておく．
(3) アドレスグループの追加
タグが付与された IP アドレスが属するアドレスグループを事前に定義しておく．
(4) ログ転送プロファイルの設定
脅威ログをトリガーにタグを付与することで，IP アドレスをアドレスグループに登録する．
(5) URL フィルタリングプロファイル追加
全通信に対して block-continue アクションを指定し，警告ページへのリダイレクトを実現する．
(6) セキュリティポリシルールの追加
block-continue アクション用のルールを作成する．
(7) 警告ページを表示するためのルート CA 証明書の生成
(8) 警告ページへリダイレクトする SSL プロキシの設定

3.3 **SSL/TLS** ハンドシェイクでの **DV** 証明書の検知

SSL/TLS のハンドシェイク時に送信される Server Certificate メッセージを 2 節で検討した検知パターンで走査し，DV 証明書を検知する．これは，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．

なお，パロアルトの脆弱性防御機能では，パケット内のデータを走査してカスタムシグネチャで定義された正規表現にマッチする TCP や UDP などのセッションを検知できる．脆弱性防御機能以外では．パケット内のデータを走査するカスタムシグネチャは実現できない．また，脆検知したセッションの通信遮断自体は脆弱性防御機能のみで実現できるが，本稿で考えている警告ページへのリダイレクトを実現するには URL フィルタリング機能を併用しなければならない．

3.4 悪性サイトの条件

後述の様に，提案手法では，警告ページへリダイレクトするため，DV 証明書の全てのサイトを悪性と見做すことも考えられる．しかし，なるべく可用性の低下を避けるため，DV 証明書に加え，以下の 2 つのいずれかを満たすサイトを悪性と判定することとした．

(1) DDNS で登録された FQDN
鳥取大学において複数回以上インシデントとして検知され，通常のページで利用頻度が多くない DDNS を条件とした．

(2) 悪性サイトで頻繁に利用される TLD
過去鳥取大学において，2 回以上インシデントやそれに繋がるイベントが検知された 9 個の gTLD を登録した．

3.5 警告ページへのリダイレクト

本手法により悪性サイトと判定されたサイトへの通信を全て遮断すると誤判定された良性サイトへのアクセスする術を利用者から奪うことになる．そこで，突然通信遮断するのではなく，警告ページへのリダイレクトを考える．前述のとおり，パロアルトの脆弱性防御機能では実現できないため，URL フィルタリング機能で，block-continue のアクションを設定することで実現できる．また，

```
set deviceconfig setting ssl-decrypt url-proxy
```

コマンドにより，HTTPS 通信のリダイレクトを有効化する．

4. 評価

4.1 評価環境

鳥取大学 (以降本学という) のパロアルト PA-5220 で実装した．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．

また，本学の PanOS が古い PA-5220 では受け入れられない検知パターンなどについては，別途バージョン 10 の PanOS が導入された機器 (以降検証機という) で検証した．

4.2 DV 証明書の検知結果

4.2.1 O と OU の有無による DV 証明書の検知結果

2.1 節で示した手法で検知を試みた．検証の結果，本学の PA-5220，検証機いずれでも，O と OU を含ないことを検知するパターンでは DV 証明書を検出できないことが明らかとなった．これは，一般的に SSL/TLS のハンドシェイクの Server Certificate メッセージが DV 証明書内の発行元の中間 CA 証明書も含むことに起因していた．一般に中間 CA 証明書には O や OU が含まれる．そのため，O と OU を含まない検知パターンは中間 CA 証明書に対してマッチしない．なお，O と OU を含まない中間 CA 証明書を試験的に作成した場合には検知できた．しかし，O と OU を含まない中間 CA 証明書は一般的ではなく，本検知パターンは有効ではない．

4.2.2 C の有無による DV 証明書の検知結果

2.2 節で示した手法で検知を試みた．検証の結果，本学の PA-5220，検証機いずれでも，C が存在しないことを検知するパターンでは DV 証明書を検出できないことが明らかとなった．これは，DV 証明書に含まれる発行者に C が含まれることに依る．また，4.2.1 節と同様に，一般に中間 CA 証明書の Subject でも C は含まれる．これらのことから，本検知パターンは有効ではないと言える．

4.2.3 CN のみを含む Subject の検知結果

2.3 節で示した手法を検証した．本学の PA-5220 では PanOS が古く，正規表現が設定できなかったため，検証機で検証した．検証の結果，DV 証明書を検知できることが明らかとなった．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 **5**)．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．

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

図 **5** パフォーマンスが悪いと判定された正規表現

4.2.4 発行者の Subject による検知結果

2.4 節で示した手法を検証した．ここでは，2.4 節で例示したとおりの正規表現で，Let's Encrypt のみの DV 証明証の検知を検証した．検証の結果，Let's Encrypt の DV 証明書を検知できることが確認できた．

4.2.5 DV オブジェクトによる検知結果

2.5 節で示した手法を検証した．その結果，PA-5220 では DV 証明書を検知できなかった．Server Certificate メッセージに含まれていることが明らかな値のバイナリ表現

の正規表現でもマッチさせることができなかった．古い PanOS ではバイナリマッチできない可能性がある [5].

4.3 検知できた DV 証明書の FQDN の数とセッション数

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 8/31 まで)

		DV 証明書		FQDN 数	
月	SSL/TLS	総数	学内	総数	学内
4 月	136510310	508464	44364	21039	26
5 月	473039730	1985794	193730	43666	29
6 月	589203465	2410876	190387	53294	37
7 月	639196346	2505153	196997	48282	26
8 月	447540390	1870734	205234	38877	32
総数	2285490241	9281021	830712	110753*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.

発行者の Subject により検知できた DV 証明書の数と警告ページへのリダイレクト数を確認した．2021/4/21 に発行者の Subject と DV オブジェクトによる DV 証明書の検知を PA-5220 上に設定した．そして，2021/4/21 から 8/31 現在までの実トラフィックで評価した．

表 **5** に示す様に，全体で SSL/TLS は約 23 億セッションあった．一方，DV 証明書として検知された SSL/TLS セッション (以降 DV 証明書セッションという) は約 100 万セッションであり，全 SSL/TLS セッションの約 0.41% であった．DV 証明書セッションの内，9.0%は本学内サイト関連であることが明らかとなった． また，DV 証明書セッションの内，一意な FQDN は 110753 あり，内 38 件は本学内サイトであった． 13905 セッションは FQDN を検出できなかった．これらは，SSL/TLS のネゴシエーション前にコネクションが切断されたり，既知の悪性サイトで未然に通信遮断されていたなどと考えられる．

4.4 アクセスを防止したセッション数と悪性判定の正誤

提案手法でアクセス防止した FQDN の悪性度を，2021/9/14 から 10/16 現在にかけて，Google Safe Browsing [9] 及び VirusTotal [10] で確認した．VirusTotal では過去の判定も残るが，Google Safe Browsing では，1 つの FQDN に対する判定の有効期限は 5 分であり，頻繁に更新される傾向が見られ，悪性の判定も比較的短時間で削除されることに留意されたい．なお，Google Safe Browsing と VirusTotal のどちらにおいても，時間の都合上，IP アドレスによる判定は実施しなかった．

DDNS によりアクセスを防止したセッション数と一意な FQDN の数，悪性と判定された数を表 **6** に示す．DV 証明書セッションの内，DDNS であった FQDN で悪性と検知されたものは無かった．このことから，DDNS を悪性判定の指標にするには疑義があり，より詳細な検証が必要である．また，DDNS を利用したサイト自体の数が少なかった．これは，今回検知できた DV 証明書は Let's Encrypt のものだけであり，DV 証明書発行に DDNS は適さないことも推察される．

*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 6 DDNS によるアクセス防止数 (2021/4/21 から 8/31 まで)

月	総数	FQDN 数	悪性
4 月	45	5	0
5 月	220	9	0
6 月	182	11	0
7 月	159	8	0
8 月	372	4	0
総数	978	22*1	0

同様に，TLD によるアクセス防止数などを表 **7** に示す．アクセス防止したセッション数は，全 DV 証明書セッションの 6.1% (全 SSL/TLS セッションの 0.024%) で 568276 であった．その内，49.1%の 279043 のセッションが悪性と判定された．また，2861 個の一意の FQDN の内，18.7%の 543 個の FQDN が悪性と検知されていた．なお，評価期間において，通信障害に関して利用者からの問い合わせは全く無かった．また，表 7 では，過去に検知された FQDN の方が Google Safe Browsing が悪性判定した件数が少ないが，これは，検証したのが 9/14 以降であり，過去の判定が既に削除済みであったと考えられる．

4.5 警告ページへのリダイレクトによる副作用

`ssl-proxy` を有効化することで，SSL/TLS のサイトへのアクセスであっても，警告ページへのリダイレクトが可能にできた．その一方で，パロアルト上のルート CA 証明書をクライアントにインストールしない限り，電子証明書の警告が表示される様になった．悪性サイトと判定したサイトへのアクセスで，リダイレクト時の電子証明書の警告が表示されるのは止むを得ないと考えられる．しかし，Internet Explorer で図 **6** のダイアログが頻繁に表示される現象が利用者から報告された．DV 証明書により常時 HTTPS 化された別のサイトの CSS や JavaScript を参照している場合などに，頻発してダイアログが表示される様であった．利用者のブラウザの設定変更により回避できるが，他にも同様の問い合わせが頻発することが予想された．そこで，警告ページへリダイレクトしない，つまり，DV 証明書を利用していて，DDNS を利用，もしくは，悪性サイトの可能性が高い TLD の場合に，通信を即座に遮断する様にパロアルトの設定を変更した．

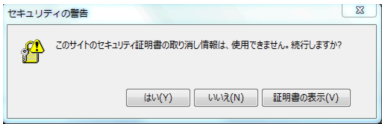

図 6 Internet Explorer の電子証明書の警告ダイアログ

表 7　悪性 TLD によるアクセス防止数 (2021/4/21 から 8/31 まで)

月	総数	悪性	SB	VT	FQDN 数	悪性	SB	VT
4 月	21861	10773	0	10773	336	77	0	77
5 月	132299	83265	0	83265	1056	209	0	209
6 月	158392	73079	74	73071	1256	243	11	241
7 月	156039	56765	286	59461	1168	250	39	237
8 月	99685	55161	428	43669	1010	246	71	213
総数	568276	279043	788	270239	2861[*1]	534[*1]	121[*1]	486[*1]

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.

5. 考察

5.1 最適な DV 証明書の検知手法

2 節に挙げた検知パターンの内最適なものは，DV 証明書を一意に識別できる DV オブジェクトを検知するパターンと考えられる．しかし，PanOS 8.1.16 では設定自体はできるものの検知できなかった．4.2.5 節で述べたとおり，PanOS 8.1.16 ではバイナリ値へマッチできない可能性がある．PanOS 8.1.16 では他にも様々なパターンでバイナリマッチを試行したが，マッチさせることはできなかった．本稿では時間の都合上検証機で挙動を試せなかったため，今後は検証機や PanOS をバージョンアップして再度評価する予定である．

また，PanOS 8.1.16 では DV オブジェクトでは DV 証明書を検知できなかったが，発行者の Subject によって検知できた．このことから，最後の手段として，運用の手間は増加するが，発行者の Subject による検知の実運用への採用も十分に考えらえる．

5.2 DV 証明書の誤検知

提案手法では SSL/TLS のハンドシェイク時の Server Certificate メッセージに含まれるバイト列に対して正規表現でパターンマッチすることで，DV 証明書の検知を試みた．今回検討した正規表現のパターンが, Server Certificate メッセージ内の他の想定していない箇所でマッチしてしまう可能性も排除できていない．今後，考察を深め，より大くの検証を行い，検討した正規表現が必要十分であるかを検証したい．

5.3 DV 証明書サイトへのアクセスの常時警告

DV 証明書により常時 HTTPS 化しているサイトへのアクセスに対して常時警告ページへ誘導することにより，悪性サイトへのアクセスを防止できる確率が高まる．しかし，DV 証明書を利用している良性サイトも存在し，4.3 節で前述のとおり DV 証明書セッションが全 SSL/TLS セッションの 0.41%にしか満たないとは言え，実環境で実装することは難しい．また，常に利用者を警告ページに誘導できれば良いが，CSS や JavaScript などによるバックグラウンドでの HTTPS アクセスなどの場合に警告ページを表示できない可能性もある．その場合は，利用者に見えないところで HTTPS がブロックされてしまい，正常な利用ができなくなる．そのため，全ての DV 証明書による HTTPS 通信に対して警告ページへの誘導を設定するのは難しいと考えられる．

5.4 DV 証明書サイトの IP アドレスデータベース

提案手法での実装では，結局，DV 証明書サイトの IP アドレスをデータベース化している．そして，その IP アドレスへの SSL/TLS 通信の場合に，さらに条件を加えて，悪性サイトと判定し，警告ページへリダイレクトする．そのため，SNI (Server Name Indication) を活用して複数ドメインを 1 つのサーバで利用している場合に，良性サイトであっても警告ページへリダイレクトされてしまう可能性がある．この様な良性サイトへの対応についても，対応の必要性も含め，今後検討する必要がある．

なお，PanOS 8.1.16 などの古い PanOS では DV 証明書サイトの IP アドレスデータベースが自動的に揮発することはないため，手動で定期的にクリアが必要である．PanOS 9.0 以降ではタイムアウトを指定できる．

5.5 HSTS を適用した良性サイト

本提案手法では，SSL/TLS の通信を警告ページへリダイレクトしている．そのため，警告ページへのリダイレクト時に電子証明書の CN である FQDN とアクセス先のサイトの FQDN が不一致となる．HSTS (Hypertext Strict Transport Security) [11] を有効にしたサイトの場合，警告ページへのリダイレクトもできず，当該サイトへのアクセスが不可能になる．パロアルトのルート CA 証明書をクライアントにインストールすることで解消できる可能性があるが，全てのクライアントにルート CA 証明書を配布することは難しく，必ずしも好ましい解決策とは言えない．今後何らかの対応策を検討したい．

5.6 他のスコアリング手法の併用

悪性サイトの判定手法については他にも様々な研究がなされている [12], [13], [14]．他の判定手法を用いることで悪性サイトをより高精度に検出できる可能性もある．今後は，パロアルトの URL もしくは IP アドレスリストの外部参照機能を活用することにより，他の判定手法を組み合わせることも検討したい．

5.7 QUIC への対応

今回の手法では QUIC に対応できていない可能性がある．今後，より精査し，QUIC への対応も検討したい．

5.8 パロアルトへの依存

本稿の提案手法は，パロアルトの機能への依存が高く，他ベンダの次世代ファイアウォールへの応用可能性は確かではない．他ベンダでの応用可能性については今後の課題とする．また，現時点で他ベンダの次世代ファイアウォールで実現できなかったとしても，本稿で 1 つの実装例を示せたのは確かである．本稿で提案した手法を実現可能とするため，必要に応じて他ベンダでの実装の修正を期待したい．

6. 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 [12]．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 [13]．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．しかし，具体的な実装方法は明らかになっていない．

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 [14]．しかし，悪性サイトへのアクセス防止の実装については触れられてはいない．

7. おわりに

本稿では， 常時 HTTPS 化された悪性サイトが DV 証明書をしばしば採用する点に着目し，未知の悪性サイトへのアクセス防止を実ネットワークのパロアルトで実装し，検証した．また，DV 証明書に含まれる固有のオブジェクトがあることを示した．そして，検証の結果，DV 証明書を使用している悪性と判定したサイトへの通信を遮断できた．遮断に際しては，パロアルト上の設定変更のみで実現できることを示し，運用性も保ちつつ，未知の悪性サイトへのアクセス防止を実現できた．

謝辞　機器の設定方法などを懇切丁寧に御教授頂いたパロアルトネットワークス株式会社 早川 浩平氏に深謝する．

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] Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.3, RFC 8446 (2018).
[5] Palo Alto Networks, Inc.: TECHDOCS: Custom Signature Pattern Requirements (2021). Accessed on 2021/4/21.
[6] ITU: X.501 : Information technology - Open Systems Interconnection - The Directory: Models (2019). Accessed on 2021/4/20.
[7] 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.
[8] CA/Browser Forum: Object Registry of the CA/Browser Forum, `https://cabforum.org/object-registry/` (2011). Accessed on 2021/8/1.
[9] Google LLC: Google Safe Browsing. Accessed on 2021/10/1.
[10] VirusTotal: VirusTotal. Accessed on 2021/9/1.
[11] Hodges, J., Jackson, C. and Barth, A.: HTTP Strict Transport Security (HSTS), RFC 6797 (2012).
[12] 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).
[13] 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).
[14] 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).