学習院大学
GAKUSHUIN UNIVERSITY

RELEASE

2026 年　11 月　16 日

「このドメインは本当に“身内”か？」DNS の名前解決の段階で、組織とドメインの関係を確かめる枠組みを提案

―DoT 対応の権威 DNS サーバと DANE を用いたドメイン間関連性検証―

研究の概要

インターネットでは、通信の中身を守る技術や、データが改ざんされていないことを確かめる技術が普及してきました。しかし、「いま接続しようとしているドメイン（ネット上の住所）が、信頼できる組織と本当に関係があるのか」までは、これらの技術では確かめられません。

学習院大学計算機センターの村上登志男助教が所属する研究グループは、ドメイン名から IP アドレスを調べる仕組み（DNS）の中で、あるドメインが別のドメインから「うちの関連ドメインです」と正式に認められているかどうかを確かめる方法を提案しました。成果は、Clarivate 社の Web of Science Core Collection（SCIE）※1 にインデックスされている国際学術誌『Electronics』に 2026 年 9 月 5 日に掲載されました。

試作システムで実験したところ、実用的な速さで動くこと、いちど確かめた結果を覚えておく（キャッシュ）ことで、2 回目以降の確認が大幅に速くなることがわかりました。

研究の背景

「本物そっくり」のドメインと、「全然似ていない」本物のドメイン

フィッシング詐欺では、本物の組織のドメイン名によく似た偽のドメイン（打ち間違いを狙ったものや、見た目の似た文字を使ったもの）が使われます。一方で、本物の組織が、普段のドメインとはまったく違う名前のドメインを、サービスの裏側で使うことも珍しくありません。たとえば Google は、自社のサーバーに「1e100.net」というドメインを使っています。

つまり、ドメイン名の見た目だけでは、「似ているから偽物」とも「違うから無関係」とも決められません。登録者情報や第三者による分類も、ドメイン同士の関係を直接証明するものではありません。

そこで本研究では、「ある組織が、別の名前のドメインを自分の関連ドメインとして正式に認めたもの」を「関連ドメイン」と定め、その認定が確かにあったかどうかを、暗号の技術で確かめる方法を考えました。

研究の内容

しくみは、会社どうしの「紹介状」に例えるとわかりやすくなります。

- **まず、通常の身分確認をする：**確認したいドメインの DNS サーバー（権威 DNS サーバ※2）と、暗号化した通信（DoT※3）でつながり、サーバーが示す電子証明書※4 を、一般に公開されている認証局の仕組みで確かめます。
- **次に、「紹介状」を確かめる：**元になるドメイン（例：ある組織の主なドメイン）が、自前の認証局から、関連ドメインのサーバーに「追加の証明書」を発行します。これが紹介状にあたります。元のドメインは、その署名の見本（認証局の情報）を、改ざんを防ぐ署名付きで DNS 上に公開しておきます（DNSSEC※5、DANE※6）。確認する側は、この見本と照らし合わせて、紹介状が本物かを確かめます。
- **「関連あり」と判定する条件：**元のドメインが認めた追加証明書の確認に成功したときだけです。有効な証明書を持っているだけでは、関連ドメインとは認められません。
- **たくさんのドメインを預かるサーバーにも対応：**1 台のサーバーが複数のドメインを預かる場合は、接続時に伝えられるドメイン名（SNI※7）を見て、ドメインごとの証明書を使い分けます。
- **確認結果を覚えておく：**確認は、利用者に代わって名前解決を行うサーバー（フルサービスリゾルバ※8）が行い、証明書と結果をキャッシュします。結果は DNS の応答に添えて返すため、利用者側の機器やソフトを作り替える必要はありません。

実験と結果

ルート、TLD、2LD、3LD の 4 階層の DNS を仮想環境に構築し、元になるドメイン 1 万個と、確認の対象となるドメイン 1 万個を使って評価しました。

- **応答時間：**ネットワークの遅延が大きい条件（片道 0.1 秒の遅延を加えた場合）でも、確認を伴う最初の 1 回の応答時間は平均で約 3.7 秒でした。1 万回のうちほぼすべて（99.9%以上）が 5 秒以内に終わっています。確認結果をキャッシュした 2 回目以降は、約 0.5 秒に短縮されました。遅延を加えない条件では、最初の 1 回が約 0.1 秒、2 回目以降が約 0.07 秒でした。
- **処理能力：**同時に多くの問い合わせがあっても、1 秒あたり約 450 件程度を処理でき、確認をしない場合とほぼ同じ水準でした。

- **偽のドメインへの対処：**実在の組織に似せた検証用の偽ドメインで試したところ、通常の証明書の確認は通りましたが、追加証明書がない場合や、攻撃者が自作した追加証明書を使った場合は、いずれも「関連性は未確認」のままとなりました。

本研究の意義

この方法は、ドメイン名が似ているかどうかではなく、元のドメインが正式に認めたかどうかを根拠に関係を判定します。確認が DNS の中で完結し、DNSSEC、DoT、DANE といった既存の標準技術の組み合わせで実現できます。将来は、ユーザーが接続先と正規の組織との関係を確認できる仕組みや、フィッシング対策の判断材料としての活用が期待されます。

なお、この方法はドメインを「フィッシング」「正常」「悪意あり」などに分類するものではありません。「関連性が未確認」であることは、そのドメインが悪意あるものだという意味ではありません。フィッシングを見つける精度や、利用者の被害を減らす効果は、今回の評価の対象外です。

限界と今後の展望

- 評価は仮想環境での試作によるもので、実際のインターネット上の通信や、多数の DNS 事業者にまたがる規模での検証は行っていません。
- 導入には、元のドメイン側の DNSSEC 運用と認証局の管理、関連ドメイン側の DoT 対応と追加証明書の提示、確認するサーバー側の検証とキャッシュ管理が必要です。また、証明書をすぐに失効させる仕組みは備えていません。
- 今後は、実際の運用環境での評価、証明書の失効や鍵の更新の手順の整備、他の TLS 実装との相互接続の確認、確認結果を利用者やアプリにどう見せるかの評価、DoH や DoQ への拡張などに取り組む予定です。

用語解説

※1　Web of Science Core Collection：Clarivate 社が提供する学術文献データベース。独自の基準で審査して選んだ学術誌を収録し、収録誌は継続的に見直される。国際的に広く利用され、研究評価にも使われている。SCIE（Science Citation Index Expanded）はその索引の一つ。

※2　権威 DNS サーバ：ドメインに関する情報（IP アドレスなど）の正本を持ち、問い合わせに答えるサーバー。

※3　DoT（DNS over TLS）：DNS の通信を暗号化して、盗み見られないようにする方式。

※4　電子証明書：サーバーなどの身元を証明するデジタルの証明書。公開されている認証局の階層で確かめる方式を PKIX という。

※5　DNSSEC：DNS の応答にデジタル署名を付け、改ざんされていないことを確かめられるようにする仕組み。

※6　DANE：改ざんを防ぐ署名付きの DNS 上に、証明書やその発行元の情報を公開し、証明書の確認に使う仕組み。

※7　SNI：暗号化通信の開始時に、接続先のドメイン名をサーバーに伝える仕組み。1 台のサーバーが複数のドメインの証明書を使い分けるのに使う。

※8　フルサービスリゾルバ：利用者に代わって、ルートから順に権威 DNS サーバへ問い合わせ、名前解決を行うサーバー。

発表者

村上　登志男（学習院大学計算機センター　助教）
根木　湧人（東京農工大学工学研究院　大学院生＝研究当時）
中川　令（東京農工大学工学研究院　助教）
金　勇（東京科学大学情報基盤センター　マネジメント准教授）
山井　成良（東京農工大学工学研究院　教授）

論文情報

論 文名：A Framework for Verifying Inter-Domain Relationships Using DANE-Based Trust Models on DNS-over-TLS-Enabled Authoritative Servers

雑　誌：Electronics 2026, 15(17), 4020（2026 年 9 月 5 日公開、オープンアクセス。Clarivate 社 Web of Science Core Collection（SCIE）収録誌）

著 者名：Toshio Murakami（村上登志男）、Yuto Motogi（根木湧人）、Rei Nakagawa（中川令）、Yong Jin（金勇）、Nariyoshi Yamai（山井成良）

D O I：https://doi.org/10.3390/electronics15174020

（研究助成）

本研究は、共著者の山井成良教授（東京農工大学）の科学研究費助成事業（課題番号 JP22K12007）の一部、および学習院大学計算機センター特別研究プロジェクト費の一部の支援を受けて実施しました。また、本論文の掲載にあたっては、MDPI による事前審査を経て、論文処理費用（APC）の全額免除を受けました。

研究に関する問い合わせ

学習院大学　計算機センター
助教　村上　登志男（むらかみ　としお）
E-mail : toshio.murakami@gakushuin.ac.jp

報道に関する問い合わせ

学習院大学学長室広報センター
Tel：03-5992-1008
E-mail：koho-off@gakushuin.ac.jp