Vol.2020-SPT-36 No.43
2020/3/2

Brand Validation 証明書の提案および評価 ～Webサイトのアイデンティティ表示の改善～

奥田 哲矢[1]　千葉 直子[1]　秋山 満昭[1]　福永 利徳[1]　鈴木 亮平[1]　神田 雅透[2]

概要：Extended Validation (EV) 証明書を利用する Web サイトでは，Web サイトのアイデンティティに関する情報をユーザに提示することが出来る．EV 証明書によるアイデンティティ表示は，Web サイトが悪性サイトであるか（例えば，フィッシングサイトであるか）を判別するための情報源となる．しかしながら，いまだ多くのユーザが EV 証明書の仕組みや EV 証明書によるアイデンティティ表示の意味を十分に理解できていない．本研究では，まず，フィッシング攻撃を含めたインターネット上のリスクへのエンドユーザの対策と，Web サイトのアイデンティティ表示の理解について，現状分析および改善提案を行うため，インタビュー調査を行った．その結果，ユーザのセキュリティ行動のベースとなる，ユーザの認知プロセスに関するキーファクターとして，注目度，理解度，信頼度と，それらの関係性を抽出した．言い換えると，Web サイトのアイデンティティ表示は，ユーザの注目を集め，表示の意味を明確に説明し，Web サイトを使うことへの安心感を醸成する必要があることが分かった．次に，上記のユーザの認知プロセスに沿った新しいアイデンティティ表示（Brand Validation 表示）を設計し，ユーザ実験による評価を行った．その結果，筆者らの提案するアイデンティティ表示は，従来のアイデンティティ表示に比べて，注目度，理解度，信頼度の観点で有効であることが示された．最後に，上記インタビューを通じて得られた、EV 証明書や認証局に対する提言を述べる．

1. はじめに

HTTPS に対応したフィッシングサイトが年々増加しており [7]，従来エンドユーザが行ってきた “鍵マークの有無によって安全かどうかを判断する行動” は事実上有効でなくなってきている．HTTPS に対応することで，Web サイトは認証局により認証されたアイデンティティ情報を X.509 証明書を用いて表示することが出来る [5]．認証には 3 段階があり，Domain Validation (DV)，Organization Validation (OV)，Extended Validation (EV) がある．このうち，EV 認証が最も厳しい認証基準であり，Web サイト管理者の法的な実在性の確認を行い，Web サイトのユーザにより多くのアイデンティティ情報を提供可能となる [9]．しかしながら，一般的なユーザは，EV 認証の仕組みや認証の 3 段階について十分に理解していない [21]．こうした弊害が，しばしば Web サイトの信頼性の判断誤りにつながっている．我々の研究の目標は，差し迫るフィッシングサイトの脅威に対して，ユーザの認識を改善・サポートするために，より有効な Web サイトのアイデンティティ情報の表示方法をデザインすることである．本稿では，以降に示すインタビュー調査を通じて，EV 証明書を利用する Web サイトの新しいアイデンティティ表示方法として Brand Validation（BV）証明書および BV 表示を提案し，評価を行った．まず，インターネット上のリスクへの対策に関するインタビューを行った．さらに，フィッシング対策，特にブラウザにおける対策についてインタビューを行った．さらに，対策としての EV 証明書によるアイデンティティ表示の理解度や問題点についてインタビューを行った．これらインタビューを通じて，我々はユーザのセキュリティ行動のベースとなる，ユーザの認知プロセスのキーファクターとして，注目度，理解度，信頼度とそれらの関係性を抽出した．言い換えると，Web サイトのアイデンティティ表示は，ユーザの注目を集めて，表示の意味を明瞭に説明して理解を促進し，ユーザが Web サイトを使うことに安心感を感じるように促す必要があることが分かった（図 1）．次に，上記の認知プロセスに沿った新しい Web サイトのアイデンティティ表示をデザインし，参加者に提示して，注目度，理解度，信頼度の観点で評価を行った．我々のアイデンティティ表示の特徴は，ブランド／サービス名を URL バーに表示し，認証局の認証プロセスを詳細ダイアログに表示することである．参加者による評価の結果，提案する

[1] NTT セキュアプラットフォーム研究所
3-9-11 Midori-cho, Musashino-shi, Tokyo, Japan
[2] 情報処理推進機構
2-28-8 Hon-Komagome, Bunkyo-ku, Tokyo, Japan

BV 表示は，注目度，理解度，信頼度，全ての観点で従来表示を上回ることが分かった．さらに，提案表示をより良いと参加者が判断した理由を収集することが出来た．

2. 背景と関連研究

2.1 フィッシング攻撃とユーザ認知

フィッシング攻撃による被害は年々拡大しており，2018 年には 4,820 万米ドルに上るという報告がある [3]．フィッシング攻撃には被害者となる人間の介在が不可欠であることから，フィッシング攻撃への対策として，技術的な対策と人的な対策が研究されている．技術的な対策としては，フィッシングサイトの URL に基づく検知手法を始め，多くの研究がなされている [1]．人的な対策としては，[6] に始まり，人間の認知と行動にフォーカスした多くの研究がなされてきた．2006 年の実験で，ヒューマンファクターに基づいた最初のフィッシング対策の研究として，Dhamija らは，多くの参加者が Web サイトの URL やブラウザの表示に注目せず，Web サイトの見た目（“look and feel”）でフィッシングサイトであるかどうか判断していることを報告した [6]．2007 年の実験では，参加者が HTTPS に関するブラウザの表示を無視し，HTTPS の表示が無い Web サイトに不注意に個人情報や決済情報を送信する傾向があったと報告した [19]．2016 年の実験では，Felt らは Google Chrome の HTTPS 接続の安全性に対する理解度を改善するためにアイコンおよび文字列の再デザインとユーザスタディを行っている [8]．

2.2 セキュリティインジケータ

セキュリティインジケータは，Web サイト等のセキュリティに関する状態を表示するために使用され，主要な Web ブラウザが HTTPS 接続時には鍵アイコン等をセキュリティインジケータとして表示している [8]．ユーザは Web ブラウザのインジケータの存在を確認することで，Web サイトのセキュリティに関する状態を確認することが出来る．W3C は，ユーザに Web セキュリティに関する情報提供をするためのユーザインタフェース（UI）ガイドラインを発行している [17]．本ガイドラインの中で，以下の UI に関する定義がなされている．

(i) プライマリ UI: Web サイト訪問時の初期表示であり，ユーザの注目度の改善に重要である．

(ii) セカンダリ UI: Web サイトの詳細情報を得るために，ユーザがプライマリ UI をクリックした時の表示であり，ユーザの理解度の改善に重要である．

これらの定義に従って，HTTPS に対応した Web サイトでは，プライマリ UI に鍵アイコンが表示され，セカンダリ UI に証明書の情報が表示される．

2.3 Web サイトのアイデンティティと X.509 証明書

URL と X.509 証明書は，ユーザに Web サイトのアイデンティティに関する情報を提示することが出来る [9], [12]．URL は最も一般的な Web サイトのアイデンティティ表示であるが、homograph attack や combo-squatting attack のような視覚的な錯誤を悪用した攻撃への対策が難しいことが示されており [16]，URL のみでは Web サイトのアイデンティティを正しく判断できないことが知られている [15]．X.509 証明書は，HTTPS を利用する Web サイトのアイデンティティ表示に利用される．X.509 証明書は，一般的に認証局により発行されているが，認証の基準には段階があり，Domain Validation (DV), Organization Validation(OV), Extended Validation (EV) の 3 種が存在し，ユーザは HTTPS に対応しているという理由のみで Web サイトを無条件に信頼すべきではない．DV 証明書では，ドメインの管理権限のみを確認することで証明書を発行する．OV 証明書では，CA/ブラウザフォーラムが発行する Baseline Requirement というガイドラインに従って，ドメイン管理者を確認して証明書を発行する [10]．

EV 証明書は，3 種の証明書の中で最も厳格な基準で発行される証明書であり，CA/ブラウザフォーラムが発行する EV 証明書発行ガイドラインに従って，ドメイン管理者の法的な実在性を確認して証明書を発行する [9]．その厳格な認証プロセスが寄与して，EV 証明書を使用するフィッシングサイトの数は，DV 証明書等を使用するフィッシングサイトの数に比べて，劇的に少ない [7]．さらに，EV 証明書は，ユーザの注目を集めるための視覚的な利点が存在する．EV 証明書を使用するサイトでは，Web サイト運営者の組織名が URL バーに緑色で表示され，ユーザが Web サイトのアイデンティティをより正しく判断することが出来る．EV 証明書の表示について，picture-in-picture attack [13] や cross-jurisdiction collision attack [21] の可能性が報告されているが，より現実的な問題は，EV 表示の注目度の低さ（気付きにくさ）や理解度の低さ（分かりにくさ）である．これまでに，2008 年に FireFox3.0 で EV 表示の注目度を改善する研究 [20] や，2009 年に IE7 で connection のセキュリティと Web サイトのアイデンティティの区別に関する理解度を改善する研究 [2] が行われてきた．さらに、2019 年の Google Chrome の実験で、EV 表示の注目度や理解度の低さが，最新のブラウザでいまだ改善されていないことが報告された [21]．

我々は，ユーザの認知プロセスに関する理解を進めることで，有効なフィッシング対策としての EV 表示に改善の余地があると考え，ユーザインタビューにより認知プロセスに合った評価指標を設定し，本評価指標に沿った EV 表示の改善方式を提案し，評価を実施する．

3. 調査手順

本研究の調査手順を下記に示す．大別して，事前インタビュー，既存表示の解説資料説明，改善表示の提案と評価，といった手順で構成される．
(Step-1) 事前インタビューにより評価指標を抽出
(Step-2) EV 証明書と認証プロセスについて解説
(Step-3) 事前インタビューにより既存 EV 表示の問題点と改善方針を抽出
(Step-4) Web サイトのアイデンティティ表示改善案を作成
(Step-5) インタビューにより提案表示を評価

本調査はすべて 2019 年 1-3 月の期間に実施した．本インタビュー調査の参加者の募集方法としては，調査会社を使って，より深い洞察を得るために，日本人の IT リテラシーが高く情報セキュリティリスクへの意識の高い参加者を募集した．(N=35, 20–60 歳, 男/女比=1.05)．参加者への報酬としては，2 時間のインタビューに対して 7700 円を支給した．

4. 事前インタビュー（指標抽出）

調査手順 (Step-1) に従い，既存 EV 表示の参加者の理解度の把握と，表示の評価指標の抽出のために，半構造化インタビューを実施した．コーディング方法としては，1 名のコードマスターがコードブックを作成し，1 名のサブコーダーがコードブックを検証した．以降，既存 EV 表示の参加者の理解度に関する結果および考察について述べる．

4.1 事前インタビュー結果（既存 EV 理解度）

Grounded-Theory [14] に基づいたインタビュー分析の結果，下記の代表的な意見に整理できた．
(i) 注目度：プライマリ UI の表示への注目に関する意見
(ii) 理解度：プライマリ UI およびセカンダリ UI の表示の意味の理解に関する意見
(iii) 信頼度：Web サイトの利用時の安心感・信頼感に関する意見

4.1.1 注目度（Attention）

注目度に関して，正しい注目と正しくない注目に関する意見が得られた．正しい注目に関して，EV 表示が採用されている業界に関する意見が多数挙げられた．具体的には「銀行にあった」「金融機関はほとんど」「銀行系は緑だな」「銀行と証券会社のサイトで見た」「クレジットカードのサイトで見た」といった意見が得られた．正しくない注目に関して，EV 表示の正しい見方が不足している状況を示唆する意見が得られた．具体的には「鍵マークは見ていた」「鍵が付いていれば安心」「https の”s”は見ていた」や「色は注意して見ない，色は重要と見ていない」という意見が挙がった．参加者全体としては，何らかの注目が，必ずしも正しい理解に繋がっていない状況が示唆された．

4.1.2 理解度（Comprehension）

理解度に関して，EV 認証の意味に関する正しい理解と正しくない理解に関する意見が挙がった．正しい理解に関して，「鍵マークは暗号化を意味するのみ，サイトの信頼は別で，アドレスバーが緑色であればしかるべき機関が調べたということらしい」「個人情報をやりとりする時は鍵マークと思うが，それはあくまでも途中で盗聴されないという安心感でしかない．相手先が信用できるかは，また別の話」という意見が挙げられた．正しくない理解に関して，認証局の存在や認証プロセスについて疑問を示す意見が多数挙げられた．具体的には「認証局とは国の行政機関なのか，公的な機関なのか，分からない」「認証局が誰なのか分からない．第三者的なものなのか．誰が認証しているのか疑問.」「認証の手続きの中身は漠然としている，特許・商標登録の商品と同じ感覚」「認証局が実際にどんな審査を行っているか分からないため信用する他ない」等の意見が挙げられた．参加者全体としては，認証局の保証の範囲や内容に関する理解の多寡が，各意見に反映されていた．

4.1.3 信頼度（Trust）

EV 認証の信頼度・安心感に関する意見が得られた．具体的には「より重要なサイトで色が変わったから，セキュリティが強化されたと想像した」「銀行などの信用のあるサイトは共通して表示される」「銀行や証券に限ってこうしたマークが出るから，安心だろうなと思っていた」といった意見が得られた。一方，EV 認証の信頼度・安心感に疑問を呈す意見が得られた．具体的には「表示される認証局自体が全然知らない名前だと「大丈夫かな？」と思いそう」「認証局自体が信用できなかったら全てダメになる，認証局を信じて良いのか疑った方が良いのか分からない」「膨大な数のサイトがあるので，どこまで管轄して認証しているのか，少し不安に思う」「認証局がどこまでちゃんと見ているのかなという疑問はある．認証する作業量が結構ある気がするので，認証局の人が機械的にさばいていないのか心配だなと思う」といった意見が挙げられた．参加者全体として，理解の不足が，ひいては信頼の度合に繋がっていることが示唆された．

4.2 事前インタビュー結果考察（既存 EV 理解度）

一般に，セキュリティインジケータは，表示に対してより注目を集めて，表示の意味をより明瞭に説明する必要があり，その結果として，Web サイトの使用時にユーザに信頼感・安心感を与えることが出来る（図 1）．

しかし，事前インタビューを通じて，多くのユーザが，

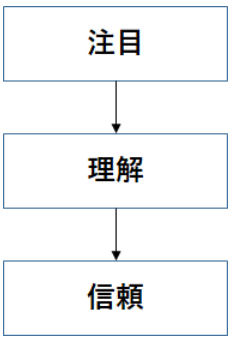

図 1 注目（Attention），理解（Comprehension），信頼（Trust）の関係性

既存の EV 表示への注目・理解が不足しており，Web サイトへの信頼感の形成に支障が生じていることが判明した．

5. 事前インタビュー（問題点抽出）

調査手順 (Step-2) に従って，EV 証明書の仕組みに関する啓蒙的なコンテンツを作成して，EV 証明書と他証明書の違い，認証局の存在，具体的な認証プロセスについて説明を行った．その後，調査手順 (Step-3) に従って，既存 EV 表示の問題点の把握のため，半構造化インタビューを実施した．コーディング方法としては，1 名のコードマスターがコードブックを作成し，1 名のサブコーダーがコードブックを検証した．以降，既存 EV 表示の問題点に関する結果および考察について述べる．

5.1 事前インタビュー結果（既存 EV 問題点）

Grounded-Theory に基づいたインタビュー分析の結果，表示上の問題（注目に関する問題）と，ユーザ教育の不足（理解に関する問題）に整理できた．一部の意見は，次章の提案表示に反映された．

5.1.1 表示上の問題（注目に関する問題）

表示上の問題について参加者から多数指摘が有った．

・URL 表示とのトレードオフ

画面サイズの小さいモバイル端末においては，EV 表示を行う場合に URL を非表示にする端末もあり，「URL が隠れて見えず怪しいと思ったことがある」という意見が挙げられた．一方で，「URL は正体が分からないものが多い」という，アイデンティティ表示としての URL に疑義を示す意見も挙げられた．

・表示の真正性および発信元

表示の真正性に関する意見が挙がった．具体的には「ポップアップで偽装できそう，認証した特別感が無い」「この情報の裏が自分で取れるわけでもない」「表示される情報が本当に真実なのかは直接電話するしかない」という意見が挙げられた．また，表示の発信元に関して「メッセージを誰が言っているのか分からない」という意見が有った．ブラウザの発信する内容と，サイト運営者の発信する内容を，ユーザが明確に区別出来ていないことが示唆された．

・詳細表示の無効性

EV 認証を理解したユーザには，詳細画面の必要性が下がるという意見，具体的には「鍵マークと緑のアドレスバーを見た時点で EV 認証されていることはわかるから，詳細までは見ない気がする」という意見が挙げられた．

・企業名の是非

そもそも企業名を表示する是非について，20 代女性から疑義を挙げる意見，具体的には「企業名が出るとサービス名と混乱することが一定数ありそう．運営会社はペーパー会社である等」という意見が挙がった．本意見は，次章の提案表示（プライマリ UI）に反映されている．

5.1.2 ユーザ教育の不足（理解に関する問題）

ユーザ教育の不足について参加者から多数指摘が有った．

・全体的な教育の不足

EV 啓蒙資料の説明後，一般的な教育の不足が指摘された．具体的には「もっと皆に伝えた方が良い」「どうして知らない人が多いのか」「テレビ・雑誌・CM で知らせれば良い」「報道が無く，知れ渡っていない.」等といった意見が多数挙げられた．

・教育による安心感の醸成の可能性

また，EV 啓蒙資料の説明後、安心感を覚える意見が多数挙げられた．具体的には「ネットだけで認証が完結するのではなく，リアルな世界も認証しているところが，安心感につながる」「認証が表示されたら，その会社は意識が高いところだなと思う．安心感は上がる.」「認証のある企業とない企業だったら，ない企業がマイナスにはならないまでも，ある企業のほうが，信頼性や安心感というところでプラスになると思う」「基本的には安心な仕組み，偽サイトに引っ掛かり難くはなりそう」「私が知らない間にちゃんとした企業が働いていたんだなと感動」「思ったよりもちゃんと，ネットの水面下では，こうしたチェックがされていたんだなと思った．ちょっと見直した．もうちょっと野放しで，自己責任の世界かと思っていた」「認証局が所在地までちゃんと調べているという前提であれば，信頼できると思う」等，啓蒙資料により，EV 認証の理解と安心感の醸成を示唆する意見が多数得られた．これら意見は，次章の提案表示（セカンダリ UI）に反映されている．

・過度の信頼の可能性

少し注意が必要な意見として，過度の信頼を示す意見も得られた．具体的には「実際の会社であれば信頼して取引できる」「EV 認証されているから個人情報を送信しても大丈夫」という意見が挙げられたが，取引上の与信については，EV 認証ガイドラインのスコープの範囲外である [9]．ここ

に，EV 認証が提供出来ている安心感と，実際の取引時に必要な安全性のギャップが存在することも，また浮き彫りになったと言える．

5.2 事前インタビュー結果考察（既存 EV 問題点）

EV 表示の注目度に関して，インターネット上の購買意欲が高いと思われる 20 代女性から，企業名はサービス名と混乱する，運営会社はペーパー会社であり得る，等，企業名表示への疑義が挙げられたことは注目に値する．本意見は次章の提案表示（プライマリ UI）に反映されている．また，EV 表示の理解度に関して，認証局の存在や認証プロセスに関する疑問が多数挙げられたが，これらの啓蒙・教育が，EV 認証を含むサーバ認証をユーザが正しく行うために必要と考えられるため，これら意見は次章の提案表示（セカンダリ UI）に反映されている．

6. Web サイトの新しいアイデンティティ表示の提案

調査手順 (Step-4) に従って，また，前章の事前インタビューの意見を考慮して，我々は Web サイトの新しいアイデンティティ表示として，Brand Validation（BV）証明書および BV 表示を提案する．BV 表示は，ユーザの注目度および理解度を改善することで，ユーザが Web サイトの使用時に安心感・信頼感を得られることを目指して，下記の工夫を実施した．

・注目度の改善

企業名よりブランド名／サービス名の方がユーザ認知度が高い場合に，ユーザの注目度がより高くなると想定して，証明書にブランド名を追加し，URL バーにブランド名を表示した．

・理解度の改善

認証プロセスを可視化するために，認証局が何の情報を根拠として認証／登録したかを，詳細画面に表示した．

W3C の Web セキュリティ UI ガイドラインに従って，初期表示用のプライマリインタフェース（UI）と，詳細表示用のセカンダリインタフェース（UI）を用意した [17]．次章のユーザテストに使用するため，BV 表示のプロトタイプ画面を作成した．具体的な画面デザインについては次節以降に述べる．

6.1 プライマリ UI の注目度の改善（URL バー）

プライマリ UI 上にブランド／サービス名を表示することとした．ブランド／サービス名の方が組織名より認知されやすいため，注目度が改善されると考えた．提案のプライマリ UI は，ユーザの注目度を改善することを目指して，URL バーにサービス／ブランド名を組織名の代わりに表示している（図 2）．サービス／ブランド名は，企業等が認知向上のために広告投資しているため，よりユーザに認知されやすいと考えられる．ユーザがプライマリ UI をクリック時には，詳細画面（すなわちセカンダリ UI）が表示され，証明書情報の詳細が表示される．

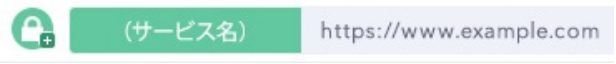

図 2 提案プライマリ UI の例

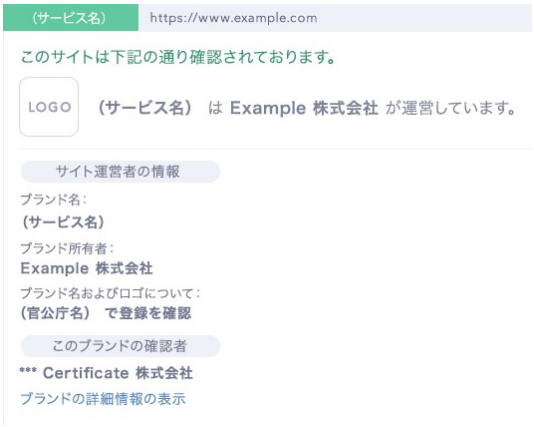

図 3 提案セカンダリ UI の例

6.2 セカンダリ UI の理解度の改善（詳細表示）

セカンダリ UI 上に，ブランド／サービス名を確認したエビデンスを含めて，証明書の認証プロセスを表示することとした．ユーザが認証プロセスを知ることで，ユーザの理解度が改善されると考えた．提案のセカンダリ UI は，ユーザの理解度の改善が, ひいては信頼度の改善に寄与すると考えている．HTTPS に対応した Web サイトが一般的になってきているため，コネクションのセキュリティに関する情報（HTTPS であるか否か）より，Web サイトのアイデンティティに関する情報の方が，今後は重要になってくると考えている．そのため，提案のセカンダリ UI は，Web サイトのアイデンティティに関する情報を充実させることとした．上記の目的で，セカンダリ UI に以下の情報を表示することとした（図 3）．

・Web サイトのアイデンティティ情報の認証プロセスを表示することとした．今回のプロトタイプでは，認証時に利用した情報源，例えば，サイト運営元組織を会社登記簿で確認している，ブランドを特許商標庁 DB で確認している，等の情報を表示することとした．

・視覚的な分かり易さが安心感の醸成に繋がるという考えから，サービス／ブランドロゴを表示することとした．

7. 提案表示の評価

7.1 評価方法

調査手順 (Step-5) に従って，提案 BV 表示の有効性を評価するために半構造化インタビューを実施した．従来 EV 表示と提案 BV 表示を参加者に視覚的に呈示し，より注目度・理解度・信頼度の高い表示はどれかをヒアリングし，提案方式の評価を実施した．提案方式の評価および意見は，インタビューという対面調査においては誘導的／恣意的になりがちであるため，オープンクエスチョンを基本として，提案方式をより改善するモチベーションを持って，批判的／建設的な意見を含めて収集するように留意した．当日はグループインタビューの形式で 5-6 名同時にインタビューを行ったが，前の参加者のコメントの影響を受けない様に，個別で紙ベースのアンケート評価の実施後に，口頭でヒアリングを行う形式とした．

7.2 プライマリ UI の評価結果（URL バー）

注目度の観点では，サービス／ブランド名の方が認知されており気付きやすいという理由で，多くの参加者（82.8%）が提案 BV 表示を支持した（表 1）．ただし，認知されているブランドであることが必要で，認知度が低いブランドではかえって怪しいと認識された．より馴染みのある方が安心感も高まるため．「有名な方を表示するのが良い」という意見も挙がった．そのため，Web サイトに応じて，サービス／ブランド／組織名のうち最も認知度の高い名称を選択して表示することが良いと考えられる．その他の有効性や懸念点に関する意見を下記に述べる．

・ブランド表示の有効性

ブランド表示について，好意的な意見としては，「企業名よりもサービス名の方が認知度は高いと思うので，わかりやすさや目に付きやすさということで選んだ」「複数ブランドを有する会社，会社名では複雑になる」「例えば，清涼飲料の会社で，ブランドや商品ごとにサイトを作るなら，こういう風に商品名を表示した方が良いのかもしれない」「多角的にいろんなことをやっているような会社だと，大きすぎて，会社自体が身近に感じられないかもしれない．でも，個々の商品ブランドなら身近に感じそう．」等の意見が挙がった．これらは提案に好意的な意見であった．

・ブランド表示の懸念点

ブランド表示について，懸念点を示す意見としては，「商品名は変わることがある」「ブランドは売買されることもあるので，会社名とイコールではなく，わかりにくくなりそう．ブランド単位で売買されることを考えると会社のほうがいいかなと思った．」「企業名は実在，サービス名は抽象的で固有でない」「会社名で登記しているので，会社名の方が安心」「正式な会社名，役所に登録している会社名が出ているほうが，安心かなという気がした．ブランド名はコロコロ変わる．それに，1 つの企業が，ブランドをいくつも持っていることもある」「何かあったときの責任の所在は会社だと思う．」「いきなりサービス名が書かれるようになったら，逆にうさん臭く感じるような気がする．」「ブランドを表示できると広告に使われそう」といった意見が挙げられた．これらは提案に懸念を示す意見であった．

また，プライマリ UI の更なる改善点について，参加者が挙げた意見を述べる．

・企業名とブランド名のセットが良い

企業名とブランド名のセットが良いとする意見が複数挙げられた．具体的には「「このサービスは○○という会社が運営しています」という表記があれば，運営している会社もわかるので，サービス名だけを見るよりは安心感が増すと思う．」「ブランド名とは別にブランド所有者が明記されているので，安全だと思った．」「認知度は人による」等の意見が有った．

・企業名とブランド名の表示切替の有効性

企業名とブランド名の表示切替が可能であれば良いとする意見，具体的には「サービスを目的として使うサイトではサービス名を見たいし，純粋に企業のホームページを見ているときは企業名が出て欲しい，使い分け，どっちもできたらよいと思う」「サービス名が出るのが慣れていない，ユーザが自分でサービス名と企業名を切替設定できれば一番便利と思う」という，企業側あるいはユーザ側で表示を切替可能とする提案が，いずれも 20 代女性の参加者の側から挙げられた．サービス名と企業名の表示を切替可能とする提案は，今後の改善の可能性を示唆すると言える．

7.3 セカンダリ UI の評価結果（詳細表示）

理解度・信頼度ともに，全ての参加者が提案 BV 表示を支持した（表 2, 3）．特に，ブランドロゴは視覚的に分かりやすく，ブランドに加えて企業も連想しやすいと評判が良かった．また，認証プロセスの表記は，お墨付き感を増した等の意見が得られたが，改善点に関する意見も多かった．その他の有効性や改善点に関する意見を下記に述べる．

・ブランドロゴの有効性

ブランドロゴ表示について，好意的な意見としては，「商品名と社名が違うときはロゴが出ると安心する」「商品名などは似ているので，ロゴが出ると分かりやすい」「ロゴって意外と認知されていると思うから，ロゴがあると印象に残る」「「このロゴならここだな」と認知されているロゴが出てくると，ビジュアル的にもわかりやすい．」「ロゴが入っているので，形から入るというか，形から認識する人にとってはわかりやすい．わかりやすいことは安全につながるんじゃないか．」「個人の小さい店ならロゴはないだろうし，ロゴを取るぐらい，ちゃんとやろうとしている会社

だと確認が取れる」といった意見が挙げられた．これらは提案に好意的な意見であった．特に，（ブランドロゴの）分かりやすさが安全に繋がるのではないか，という意見は，ユーザブルセキュリティ研究の方向性と軌を一にし，本意見が参加者から得られたことは注目に値する．

・認証プロセスに関する情報の改善点

事前インタビューにおいても認証プロセスの不透明さが問題視されていたことから，認証プロセスに関する情報の十分な提供を求める意見が挙げられた．具体的には「詳細情報に登録番号が欲しい」「認証時の認証番号，調べることが出来る.」「いつ登記をチェックしたか．最初に登録した年月日，その後，更新したのであれば，更新年月日．1 年後，2 年後にもう 1 度チェックし直したということであれば，何度もチェックしているということがわかる.」「詳細情報に「いつ信頼性を確認したか」を知りたい.」等の意見が挙げられた．これら事項は，既存の認証プロセスにおいて既に確認されている事項であることから，認証局の業務プロセスに大きな変更を加えることなく，表示の理解度・信頼度を改善することができるため，有用な提言と考えられる．

・認証レベルに関する情報の追加

「認証の三段階のレベルの差を知りたい」という意見が挙がった．各ブラウザベンダは認証レベルの差が分かり難くなる方向に表示変更を進めているが [21]，低い認証レベルほどフィッシングサイトが多いという知見を踏まえると [7]，フィッシング対策の観点では，認証レベルの差を明示する方向に方針を戻すべき，という示唆と捉えられる．

・問合せ連絡先の情報の追加

その他に追加すべき情報として，問合せ連絡先が必要という意見が複数挙がった．「カスタマーサポート・問合せ窓口の電話番号・メールアドレス」「電話番号，実体があるか確認するために電話をかけることがある，応対が悪いときはやめる」「電話番号で検索すれば，本当に会社があるかどうか分かる」「パソコンを見ながらタブレットに電話番号を入れて調べることがある」という意見が有った．日本人特有の事象の可能性もあるが，リアルの信頼関係を重視する文化のためか，電話番号が安心・信頼の起点になり得るものと解釈できる．

7.4 評価結果に関する考察

プライマリ UI に関して，インターネット上の購買意欲が高いと思われる 20 代女性から，サービス名と企業名の表示を切替可能とする提案が挙げられたことは，今後の改善の可能性を示唆すると言える．セカンダリ UI に関して，（ブランドロゴの）分かりやすさが安全に繋がるのではないか，という意見は，ユーザブルセキュリティ研究の方向性と軌を一にし，本意見が参加者から得られたことは注目に値する．

表 1 プライマリ UI の注目度に関する結果

	注目度
EV	6
BV	29

表 2 セカンダリ UI の理解度に関する結果

	理解度
EV	0
BV	35

表 3 セカンダリ UI の信頼度に関する結果

	信頼度
EV	0
BV	35

8. 研究倫理

・個人情報

本研究では，自社 PIA（Privacy Information Assessment）委員会の審査を経て，インタビュー調査の設計を行った．インタビュー調査の回答とその他の発言内容を書き起こした発言録を含む，すべてのデータについて，特定の個人を識別することができないように加工した上で保管し，本調査に利用した．自由回答については，固有名詞等が出ないように配慮した．

・研究倫理

特定のブランドの評価に影響を与えないようなインタビュー構成とした．例えば，インタビュー内容および画面素材について，具体的な社名やサービス名は，一切使用しなかった．また，攻撃事例の説明において，具体的なサービスが想起される事例は一切述べず，特定のジャンルが想起される事例も一切述べなかった．ブラウザのデザインについては独自の設計とした．

9. 関連研究とディスカッション

9.1 関連研究

本研究に関連する研究や取組みとして，[18]，[4]，[11] が挙げられる．[18] は，Web サイト毎にブランドロゴを表示することにより，[4] は，Web サイト毎にユーザが通称を付けることにより，ユーザ認知に沿った Web サイトの認証を目指した取組みであるが，ユーザテストに関する内容は公開されておらず，有効性を検証できない課題が有った．[11] は，[18] に類するブランドロゴ表示について，ユーザテストを行った研究であるが，本研究のようなユーザの認知プロセスに関するアプローチは行っていない．本研究は，ユーザインタビューにより，これら取組みに，ユーザの認知プロセスに基づいた指標化と考察を試みた点に新規性があると考えている．

9.2 議論

・ユーザインタビューを通じて，EV 認証はサイト種別により必要度合いが異なるという意見が多く挙げられた．具体的には，EV 表示について「普段の買い物，金額が大きくなければ無くても良い」「金額が大きければ見る」「銀行・証券・旅行会社であれば見る」「取引するなら付いている方が良いが，ただ閲覧するならそうでもない」「知っている店では気にしない．気分的なもの.」「初めてアクセスするサイトなら，こういう認証があれば，信頼できるのかなという感じはする.」等の意見が有った．例えば，金融系サイトと他サイト，大手サイトと中小サイトで，EV/BV 表示の導入必要性が異なることが示唆される．

・現状の EV 認証の限界として，会社登記簿上の実在確認と取引上の与信判断には一定の線引きがある，具体的には「実在と信頼は別」「登記簿だけであればペーパーカンパニーも取得可能，それだけで信頼できるとは思えない」「実在した会社でも詐欺をするところもある」「会社の存在有無だけでは，真面目な会社かどうか分からない．それを審査するのが大変だから認証局を使うととってもお金がかかる」「認証を取るのにお金がかかりそう」「悪い人もお金を払えば認証を取れるかもしれない」「信頼できる会社でもお金がないと認証が取れない」といった意見が挙げられた．また，逆に，誤って過度の信頼を示して，「鍵マークがあれば不審なサイトではないと判断する.」「HTTPS や鍵マークがあれば心配ない.」といった意見もあった．EV/BV 認証の有効性を高めるためには，認証プロセスを与信判断にまで拡張することが有効ではないか，という示唆を与えると考えられる．

10. 結論と今後の課題

本研究では，Web サイトのより良いアイデンティティ表示に関する探究を行った．まず，既存の EV 表示に関する事前インタビューを通じて、ユーザの認知プロセスに基づく評価指標の設定を行った．具体的には，安心感・信頼感の醸成と，そのための注目度・理解度の改善が重要と分かった．次に，当該評価指標に基づいて，既存の Web サイトのアイデンティティ表示の改善として，Brand Validation（BV）表示の提案と評価を実施した．ユーザインタビューの結果，提案の BV 表示は，注目度・理解度・信頼度をいずれも改善することが出来た．本研究では，すべて日本人かつ IT リテラシーが高く情報セキュリティ意識が高い参加者へのインタビュー評価であったため，今後は，多国籍かつ IT リテラシーを問わない参加者による大規模評価を実施する予定である．更に，Brand Validation 証明書の運用に必要な，認証局の認証プロセスの変更に関する考察を行い，業界団体である CA/Browser フォーラムや IETF で認証局業界の関係者とディスカッションを行う予定である．

参考文献

[1] K. Althobaiti, G. Rummani, and K. Vaniea. A Review of Human- and Computer-Facing URL Phishing Features *(EuroUSEC '19)*.
[2] R. Biddle, P. C. Oorschot, A. S. Patrick, J. Sobey, and T. Whalen. Browser Interfaces and Extended Validation SSL Certificates: An Empirical Study *(CCSW '09)*.
[3] Internet Crime Complaint Center. 2018. *2018 Internet Crime Report*.
[4] T. Close. 2005. Petname Tool: Enabling web Site recognition using the existing SSL infrastructure. W3C.
[5] S. D. Cooper, S. Santesson, S. Farrell, R. Boeyen, and W. Polk Housley. 2007. *RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.
[6] R. Dhamija, J. D. Tygar, and M. Hearst. Why Phishing Works *(CHI '06)*.
[7] V. Drury and U. Meyer. Certified Phishing: Taking a Look at Public Key Certificates of Phishing Websites *(SOUPS '19)*.
[8] A. P. Felt, R. W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M. E. Acer, E. Morant, and S. Consolvo. Rethinking Connection Security Indicators *(SOUPS '16)*.
[9] CA/Browser Forum. 2007. *Guidelines For The Issuance And Management Of Extended Validation Certificates*.
[10] CA/Browser Forum. 2011. *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*.
[11] A. Herzberg and A. Jbara. Security and Identification Indicators for Browsers against Spoofing and Phishing Attacks *(ACM TOIT '08)*.
[12] C. Jackson, D. R. Simon, D. S. Tan, and A. Barth. An Evaluation of Extended Validation and Picture-in-Picture Attacks *(USEC '07)*.
[13] M. Jakobsson, A. Tsow, A. Shah, E. Blevis, and Y. K. Lim. What Instills Trust? A Qualitative Study of Phishing *(USEC '07)*.
[14] J. Lazar, J. H. Feng, and H. Hochheiser. 2017. *Research Methods in Human-Computer Interaction, Second Edition*. Elsevier Inc.
[15] E. Lin, S. Greenberg, E. Trotter, D. Ma, and J. Aycock. Does Domain Highlighting Help People Identify Phishing Sites *(CHI '11)*.
[16] M. Luo, O. Starov, N. Honarmand, and N. Nikiforakis. Hindsight: Understanding the Evolution of UI Vulnerabilities in Mobile Browsers *(CCS '17)*.
[17] T. Roessler and A. Sladhana. 2010. *Web Security Context: User Interface Guidelines*. W3C Recommendation.
[18] S. Santesson, R. Housley, and T. Freeman. 2004. RFC3709: Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates. IETF.
[19] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer. The Emperor's New Security Indicators *(S&P '07)*.
[20] J. Sobey, R. Biddle, P. C. Oorschot, and A. S. Patrick. Exploring User Reactions to New Browser Cues for Extended Validation Certificates *(ESORICS '08)*.
[21] C. Thompson, M. Shelton, E. Stark, M. Walker, E. Schechter, and A. P. Felt. The Web's Identity Crisis: Understanding the Effectiveness of Website Identity Indicators *(USENIX Security '19)*.