Vol.2022-SPT-46 No.13
2022/3/7

多要素認証における共通評価手法の検討とその妥当性の評価

伊藤　優[1]　金岡　晃[1]　藤田　真浩[2]　柴田　陽一[2]　山中　忠和[2]　松田　規[2]

概要：相手に自分が何者であるかを主張し本人性を確認してもらう認証（Authentication）は、インターネットにおいて重要な技術になっている。その中で、セキュリティの強度を高められることから、多要素認証が注目を集めている。これまで多要素認証の研究は数多く行われてきたが、研究によって評価手法が異なり、共通の評価手法が存在していないことが明らかになった。そこで本研究では、多要素認証の共通評価手法を検討し、検討した評価手法の妥当性を検証することを目的とする。

1. はじめに

認証（Authentication）技術の 3 つの要素である「知識による認証」「所有による認証」「生体による認証」のうち複数の要素を用いた認証方式である多要素認証（Multi-Factor Authentiation、MFA）は、情報通信の発達に伴うリモート接続における本人認証の必要性の高まりに伴い、広範なサービスで採用が進んでいる。

MFA を実現するための具体的な認証手段は、たとえば「知識による認証」ではパスワード、「所有による認証」では IC カードやスマートフォンに代表されるデバイス、「生体による認証」では指紋認証や顔認証など、多岐にわたっており、MFA は多様な認証技術の組み合わせにより実現される。近年では代表的な OS により多くの認証技術が標準的に対応がされており、一般ユーザが利用する PC やスマートフォンにおいても MFA が容易に採用可能な状況となっている。

サービスやシステムにおいて MFA を採用するにあたり様々な技術が選択しうるため、どういった方式や手段の組み合わせにより MFA を実現すればセキュリティ等の向上に効果があるか、といった点が重要になるが、MFA のセキュリティやユーザビリティ等の評価において共通する評価手法は我々の知る限り存在していない。共通評価手法の欠如は、効果の低い MFA が誤って実施されるなど本来 MFA により期待されるセキュリティのレベルに達していないままの利用につながりかねず、適切な認証に対するリスクになりうる。

そこで本研究では、MFA における共通評価手法を検討し、提案する。本提案では、これまでの単要素の認証（Single Factor Authencitation、SFA）技術の評価基準をもとに MFA を構成する個々の認証技術を評価し、それら評価を併せて評価することで MFA の評価とするアプローチを採った。そして、提案した MFA 共通評価手法の実現性や妥当性を議論するために、実際の MFA 採用システムに対して評価手法をもとにしたヒューリスティックウォークスルーにより評価を行う。

提案手法により、MFA 採用にあたって様々な認証技術の組み合わせを同一評価基準により評価可能になり、さらに応用として SFA 環境から MFA 環境に移行するにあたりどの 2 要素目が効果的かの測定などにも利用可能など、適切な MFA 利用の実現が期待できる。

2. 関連研究

多要素認証を含む認証技術全般に関する評価に関しては、NIST が発行する SP 800-63-3 が広く参照されている [1]。NIST SP 800-63-3 においても MFA についての言及があり、AAL（Authenticator Assurance Level）の要件にはそれぞれのレベルにおいて MFA を利用した認証技術が記載されている。しかし SP 800-63-3 は認証技術や利用環境の全般に関する評価のフレームワークであり、具体的な MFA 技術のどの組み合わせが SP 800-63-3 における AAL のどのレベルにあたるかの実施基準は示されないため、MFA 自体の評価を可能なものではない。

MFA の評価に関しては、学術論文においていくつかの研究で行われている [2], [3], [4], [5], [6], [7] が、それらのい

[1] 東邦大学
Toho Uniersity
[2] 三菱電機株式会社
Mitsubishi Electric Corporation

ずれも共通する指標は存在せず、それぞれの研究においてMFA として評価すべき点を挙げ、評価がされている。また多くの研究においては、MFA に採用された SFA 技術単体についてのセキュリティに関する議論が明確には行われていなかった [2], [3], [4], [5], [6]。

たとえば Raynolds らの調査 [6] では、2 要素認証のユーザビリティを運用ログを分析することで評価していたが、そこでの評価はログイン頻度や認証に費やした時間の推定、キャッシュによる認証の省略効果、エラー率が評価されていた。また Ciolino らの調査 [5] では SUS（System Usability Scale）の質問子を用いたユーザビリティ評価や、エラーの種類と回数、セットアップ完了までの時間、ログインに要した時間が評価されていた。Das らの調査 [3] では、技術の受容性（Acceptabiliity）とユーザビリティを think-aloud プロトコルにより自由度の高い評価がされていた。項目がそれぞれの研究で共通化されていないことがわかる。

SFA に関する評価としては、Bonneau らによる調査が充実している [8]。Bonneau らの調査では、Usability、Deployability、Security の 3 つの評価軸に計 25 の評価項目が提案され（表 1）、35 の認証手法に対して評価が行われた。一方で、Bonneau らは MFA について言及はしているものの、より具体的な評価までは行われておらず、また、「評価として得られた値は同じ重みではない」と言及し、より細かいスコアリングを行うことで評価者によって判断の相違が生まれてしまうとし、実際に重みを付けた評価は行わていなかった。

3. 提案する共通評価手法

3.1 共通評価のアプローチ

MFA の評価は、利用される認証方式の組み合わせによって変化する。本研究の提案手法では、各認証方式単体を評価し、その後それぞれの評価を併せて MFA の評価を導くこととした。

各認証方式単体の評価と併せた評価にあたって、Bonneau らの調査 [8] で用いられた Usability、Deployability、Security の 3 つの評価軸における、25 の評価項目（表 1）を用いる。これらの評価軸と評価項目は細分化が適切に行われており、認証技術を組み合わせて MFA を実現した場合の各 SFA 技術からの差分がさまざまな視点から確認可能になると考えられる。

各評価項目は、まず認証方式の単体での評価に使用し、MFA の評価はそれぞれの項目ごとに併せて評価を行う。また、それぞれの評価項目をその項目の条件に「該当する」、「ほぼ該当する」、「該当しない」の 3 つの段階に分けて評価を行う。

3.2 MFA の評価導出方法

MFA の評価導出では、まず MFA を構成するそれぞれの認証方式を SFA として Bonneau らの評価項目を用いて評価を行い、その結果を数値化する。数値化の方法は、それぞれの評価項目において、「該当する」には 1、「ほぼ該当する」には 0.5、「該当しない」には 0 のスコアを付与するとした。

続いて、各 SFA 認証方式の評価結果の数値から MFA の評価値を求める。この時に、各 SFA 認証方式の数値の扱いを評価軸によって変える。Usability と Deployability の評価軸に含まれる評価項目群に関しては、各 SFA 認証方式の各項目ごとの評価での最も低い値を採用する。各 SFA 認証方式における当該項目の評価結果が「該当する」つまり項目の要件を満たさない場合、MFA としては評価項目を要件を満たすとは考えない、とした。例えば、方式 A と方式 B の 2 つにより MFA を構成する場合において、方式 A では項目 1 の値が 1、方式 B では項目 1 の値が 0.5 となった場合、組み合わせた方式では項目 1 の値は 0.5 となる。

Security の評価軸に含まれる評価項目群に関しては、各 SFA 認証方式の各項目ごとの評価での最も高い値を採用する。各 SFA 認証方式における当該項目のどちらかの評価結果が「該当する」と評価された場合、MFA としては評価項目を要件を満たすと考える、とした。例えば、方式 A と方式 B の 2 つにより MFA を構成する場合において、方式 A では項目 2 の値が 1、方式 B では項目 2 の値が 0.5 となった場合、組み合わせた方式では項目 2 の値は 1 となる。

さらに、Usability と Deployability の評価軸に含まれる評価項目群に関しては、複数の方式で「該当しない」と評価された場合に MFA としての評価はより低い評価にし、Security の評価軸に含まれる評価項目群に関しては、複数の方式で「該当する」の場合により高い評価にすることで、重み付けを行う。

3.3 提案共通評価手法の応用

提案する共通評価手法は、各 SFA 方式に個別に評価を行い、それぞれがスコア化されていることとなる。それを踏まえると、実利用の応用として、以下の 3 つが考えられる。

（1） 多段階認証の評価への応用

（2） 現在利用されている MFA が十分な効果を出せているかの調査

（3） SFA から MFA 化する際、現状の SFA にどの技術を追加すれば最も効果的な MFA になるかの評価

（4） 各認証技術ごとの組み合わせにおける MFA としての有効性（相性）評価

（5） リスクベース認証（Risk Based Authentication、RBA）

表 1　Bonneau らの調査 [8] で示された認証技術の評価軸と評価項目

評価軸	各評価項目	
Usability	U1: Memorywise-Effortless	U5: Easy-to-Learn
	U2: Scalable-for-Users	U6: Efficient-to-Use
	U3: Nothing-to-Carry	U7: Infrequent-Erros
	U4: Physically-Effortless	U8: Easy-Recovery-from-Loss
Deployability	D1: Accessible	D4: Browser-Compatible
	D2: Negligible-Cost-per-User	D5: Mature
	D3: Server-Compatible	D6: Non-Proprietary
Security	S1: Resilient-to-Physical-Observation	S6: Resilient-to-Leaks-from-Other-Verifiers
	S2: Resilient-to-Targeted-Impersonation	S7: Resilient-to-Phishing
	S3: Resilient-to-Throttled-Guessing	S8: Resilient-to-Theft
	S4: Resilient-to-Unthrottled-Guessing	S9: No-Trusted-Third-Party
	S5: Resilient-to-Internal-Observation	S10: Requiring-Explicit-Consent
		S11: Unlinkable

や適応型認証における 2 段階目以降の認証動作発生のタイミング評価

4. Azure AD に対する共通評価手法による MFA 評価

本章では、提案した共通評価手法による MFA 評価を実際に行う。評価では、共通評価手法部分をヒューリスティック評価として用いたヒューリスティック・ウォークスルーを実施した。ヒューリスティック・ウォークスルー実施に際して、静的解析ソフトウェアのユーザビリティ調査を行った Smith らの論文 [9] を参考にし、実験の具体的な実施計画を立てた。評価は著者のうち 2 名がそれぞれ独立して行い、その後それぞれの結果の一致度の計算やそれぞれの判断に関する議論を行い、評価結果の更新をした。

評価対象に、パスワード認証とスマートフォンアプリによる認証の 2 要素での認証設定がされた Azure AD 環境を選択した。ウォークスルーに際しては「新たにソフトウェア会社に勤める際に、勤務開始にあたって Azure AD の初期設定をしなければならない」ことを想定して各機能の実施項目を決定し実施した。実施した項目を表 2 に示す。

4.1 Azure AD で用いられる認証方式

本研究の評価で用いる Azure AD 環境の MFA は、1 つ目の認証方式にパスワードが設定され、2 つ目の認証方式にスマートフォンによる認証が設定されている。スマートフォンによる認証では、スマートフォンに Microsoft Authenticator アプリケーションをインストールした環境を用いた。なお Azure AD におけるスマートフォンによる認証では Microsoft Authenticator 以外にも、生体認証や PIN によって認証を行う方法や、SMS による認証などがあり、これらは選択できるようになっている（図 1）。

表 2　AzureAD に対するヒューリスティックウォークスルーで実施した作業

作業
1. Azure AD のトップ画面（ https://portal.azure.com/ ）にアクセスし、自分用に与えられたメールアドレスと初期パスワードを用いて、サインインを行う
2. 貸与されたスマートフォンにテスト用のアカウントでログインし、Microsoft Authenticator のアプリをインストールする
3. アカウントのセキュリティ保護のセットアップを、Microsoft Authenticator を用いて実施する
4. アカウントのセキュリティ保護設定後、再度 Azure AD にログインする
5. パスワードの変更を試みる。その時に、弱いパスワード等を試す（長さが短い（4 文字〜8 文字）、数値のみ、アルファベットのみ、辞書に含まれる単語）
6. パスワードを忘れたとして、回復作業を試みる
7. スマートフォンを紛失したとして、回復作業を試みる
8. パスワードを忘れたとして、思いつくパスワード（正しいパスワードではない。10 回）を複数試す

4.2 ヒューリスティック・ウォークスルーの実施

ヒューリスティック・ウォークスルーを実施するにあたって、作業者の実施項目や評価視点などをそろえることを目的に、実施ガイドラインを作成した。

認知的ウォークスルー部分では、指針となる質問として以下の 4 つをガイドラインに記載した。

(1) そもそもユーザは何をするべきかわかっているか？

(2) ユーザはインターフェースを探索してやり方に気付くだろうか？

(3) ユーザは目的と正しい操作方法を関連付けられるだろうか？

(4) システムのフィードバックから、ユーザは操作が順調に進んでいることが分かるだろうか？

また、実際の Azure AD の初期設定を行った際の記録を、

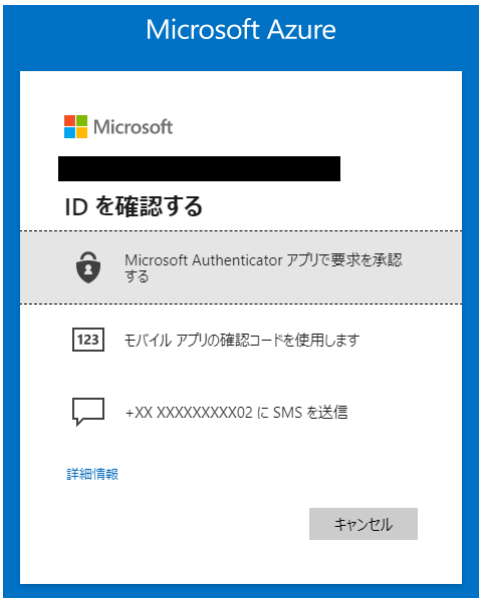

図 1　Azure AD の 2 つ目の認証方式

スクリーンショットを用いて画面保存し、作業におけるメモと共にドキュメントにまとめた。

4.3　ヒューリスティック評価結果

評価者 1 と評価者 2 がそれぞれ実施した共通評価手法における各項目の評価結果を表 3、4 に示す。

4.3.1　Cohen の重み付き κ 係数の導出

実施した評価者 1 と評価者 2 の評価結果をもとに、Cohen の重み付きカッパ係数 $\kappa(w)$ を求めたところ、

$$\kappa(w) = 0.641 \tag{1}$$

となった。

Landis と Koch によれば、κ 係数が 0.81 を超える場合、その一致は「Almost Perfect」であるとされるため、本研究でも $\kappa(w) \geq 0.8$ を目指し、再度の評価を行うこととした。

4.4　ヒューリスティック評価の妥当性の議論と再評価の実施

前述の評価では、$\kappa(w) = 0.641$ であったため、$\kappa(w) \geq 0.8$ を目指すために議論を行い、その議論をもとにそれぞれの評価者が再評価を行った。

4.4.1　評価結果

議論をもとに、再評価を実施した結果を以下の表 5、6 に示す。

4.4.2　Cohen の重み付き κ 係数の導出

実施した評価者 1 と評価者 2 の再評価評価結果をもとに、Cohen の重み付きカッパ係数 $\kappa(w)$ を求めたところ、

$$\kappa(w) = 0.858 \tag{2}$$

となり、$\kappa(w) \geq 0.8$ を実現した。

5.　考察

5.1　共通評価手法の妥当性

5.1.1　認知的ウォークスルー

ヒューリスティックウォークスルーにおける認知的ウォークスルー部分である 4 つの質問に対する回答は評価者 1 と評価者 2 で異なっていた。特に、サインインに関する作業に関して、評価者 1 はユーザビリティがある程度高いと判断したが、評価者 2 は逆にユーザビリティが低いと判断した。作業する環境や評価者の経験値などが異なっているため、評価が一致しなければならないわけではないと考えられる。

MFA の設定をする際に、「アカウントのセキュリティ保護」というメッセージが表示され、「MFA」や「多要素認証」といった表示はされなかった。これは多要素認証という言葉が現時点では世間に普及していないからだと考えられる。

5.1.2　ヒューリスティック評価

1 回目の評価では、$\kappa(w) = 0.641$ と、一致の評価は「Substantial（実質的に一致）」であったが、それぞれの評価について議論を行い再評価を行った結果、0.858 となり、「Almost Perfect（ほぼ完全に一致）」という結果になったためこれで確定とした。

議論後の再評価結果における MFA の評価値について、「D1: Accessible」と「S11: Unlinkable」の項目に関しては両評価者とも判断がつかない理由によって空欄となっている。そのため、この 2 つの評価項目は提案する評価手法としては妥当な評価指標ではないと判断できる。修正した評価項目の一覧を以下の表 7 に示す。

5.2　Azure AD の MFA 評価結果

Azure AD において、MFA 化した際に Usability、Deployability、Security の評価軸における結果がどのように変化したのかを考察する。Usability、Deployability 評価軸に関しては、評価者 1 は「U5: Easy-to-Learn」と「D5: Mature」以外のすべての項目で下がっており、評価者 2 は「U5: Easy-to-Learn」、「U6: Efficient-to-Use」、「U7: Infrequent-Erros」、「D5: Mature」以外のすべての項目で下がっている。つまり、認証方式が増えることによって、ユーザの利便性は低下し、導入のしやすさも低下することが示された。

Security 評価軸に関しては、評価者 1 は「S2: Resilient-to-Targeted-Impersonation」以外のすべての項目で上がっており、評価者 2 はすべての項目で上がっている。このことから、認証方式が増えることによって、セキュリティの強度は上昇することが示された。しかし、Usability、Deployability 評価軸の MFA の評価値に関しては、より低い値（-1）が検出されなかったが、Security に関してはより高い値（2）が評価者 1 の評価では「S8: Resilient-to-Theft」、「S9: No-

表 3 Azure AD に対するヒューリスティックウォークスルー実施結果 1（共通評価手法の Usability、Deployability 評価軸の評価結果）

評価者	認証方式	Usability								Deployability					
		U1: Memorywise-Effortless	U2: Scalable-for-Users	U3: Nothing-to-Carry	U4: Physically-Effortless	U5: Easy-to-Learn	U6: Efficient-to-Use	U7: Infrequent-Erros	U8: Easy-Recovery-from-Loss	D1: Accessible	D2: Negligible-Cost-per-User	D3: Server-Compatible	D4: Browser-Compatible	D5: Mature	D6: Non-Proprietary
評価者 1	パスワード	0	0	1	0	1	0.5	1	1	1	1	1	1	1	1
	スマートフォンのアプリによる認証	1	1	0.5	1	1	1	0	0	x	0	0	x	1	0
	組み合わせた認証方式	0	0	0.5	0	1	0.5	0	0		0	0		1	0
評価者 2	パスワード	0	0	1	0	1	1	1	0.5	1	1	1	1	1	1
	スマートフォンのアプリによる認証	1	1	0.5	0	1	1	1	0	1	0	1	1	1	0
	組み合わせた認証方式	0	0	0.5	-1	1	1	1	0	1	0	1	1	1	0

表 4 Azure AD に対するヒューリスティックウォークスルー実施結果 2（共通評価手法の Security 評価軸の評価結果）

評価者	認証方式	Security										
		S1: Resilient-to-Physical-Observation	S2: Resilient-to-Targeted-Impersonation	S3: Resilient-to-Throttled-Guessing	S4: Resilient-to-Unthrottled-Guessing	S5: Resilient-to-Internal-Observation	S6: Resilient-to-Leaks-from-Other-Verifiers	S7: Resilient-to-Phishing	S8: Resilient-to-Theft	S9: No-Trusted-Third-Party	S10: Requiring-Explicit-Consent	S11: Unlinkable
評価者 1	パスワード	0	0	0	0	0	x	x	1	1	1	x
	スマートフォンのアプリによる認証	1	0	1	1	x	x	x	1	1	1	x
	組み合わせた認証方式	1	0	1	1				2	2	2	
評価者 2	パスワード	0	0.5	1	0	0	0	0	0.5	1	1	1
	スマートフォンのアプリによる認証	1	1	1	1	1	1	0.5	1	1	1	1
	組み合わせた認証方式	1	1	2	1	1	1	0.5	1	2	2	2

Trusted-Third-Party」、「S10: Requiring-Explicit-Consent」の 3 つで検出され、評価者 2 の評価では「S3: Resilient-to-Throttled-Guessing」、「S9: No-Trusted-Third-Party」、「S10: Requiring-Explicit-Consent」の 3 つで検出された。この結果から、Usability、Deployability 評価軸は MFA 化しても大幅に下がることはないが、Security はより強固なものになることが期待できると言える。

これらの考察から、この共通評価手法は、MFA 化することによるメリット・デメリットが明確に議論できる指標となっており、適切に評価できていると判断した。

6. おわりに

本研究では、多要素認証（MFA）における共通評価手法の欠如から考えうるリスクに焦点を当て、MFA の共通評価手法を提案した。共通評価手法は、MFA を構成するそれぞれの認証技術の単体を評価した後にそれぞれの評価結果を併せて評価することで MFA の評価とした。評価項目は Bonnerau らの調査の行ける項目を援用し、妥当性評価実験に基づき修正を行った。また提案した共通評価手法を利用し、Azure AD 環境における MFA を評価し、評価結果として MFA の効果が示されたことを確認し、併せて提

表 5　Azure AD に対する共通評価手法の Usability、Deployability 評価軸の再評価評価

評価者	認証方式	Usability								Deployability					
		U1: Memorywise-Effortless	U2: Scalable-for-Users	U3: Nothing-to-Carry	U4: Physically-Effortless	U5: Easy-to-Learn	U6: Efficient-to-Use	U7: Infrequent-Erros	U8: Easy-Recovery-from-Loss	D1: Accessible	D2: Negligible-Cost-per-User	D3: Server-Compatible	D4: Browser-Compatible	D5: Mature	D6: Non-Proprietary
評価者 1	パスワード	0	0	1	0	1	0.5	1	1	1	1	1	1	1	1
	スマートフォンのアプリによる認証	1	1	0.5	1	1	1	0	0	x	0	0	0	1	0
	組み合わせた認証方式	0	0	0.5	0	1	0.5	0	0		0	0	0	1	0
評価者 2	パスワード	0	0	1	0	1	1	1	1	1	1	1	1	1	1
	スマートフォンのアプリによる認証	1	1	0.5	1	1	1	1	0	x	0	0	0	1	0
	組み合わせた認証方式	0	0	0.5	0	1	1	1	0		0	0	0	1	0

表 6　Azure AD に対する共通評価手法の Security 評価軸の再評価評価

評価者	認証方式	Security									
		S1: Resilient-to-Physical-Observation	S2: Resilient-to-Targeted-Impersonation	S3: Resilient-to-Throttled-Guessing	S4: Resilient-to-Unthrottled-Guessing	S5: Resilient-to-Internal-Observation	S6: Resilient-to-Leaks-from-Other-Verifiers	S7: Resilient-to-Phishing	S8: Resilient-to-Theft	S9: No-Trusted-Third-Party	S10: Requiring-Explicit-Consent	S11: Unlinkable
評価者 1	パスワード	0	0	x	0	0	0	0	1	1	1	x
	スマートフォンのアプリによる認証	1	0	1	1	1	1	0.5	1	1	1	x
	組み合わせた認証方式	1	0		1	1	1	0.5	2	2	2	
評価者 2	パスワード	0	0.5	1	0	0	0	0	0.5	1	1	x
	スマートフォンのアプリによる認証	1	1	1	1	1	1	0.5	1	1	1	1
	組み合わせた認証方式	1	1	2	1	1	1	0.5	1	2	2	

案手法の妥当性があると判断した。

本提案手法はさまざまなシーンで応用可能であると考えられるため、さらなる広範の技術に評価を行いその妥当性をより明確にしていくことが課題となるだろう。

参考文献

[1] Paul A. Grassi, Michael E. Garcia, James L. Fenton, "NIST Special Publication 800-63 Revision 3", 2017

[2] Reynolds, Joshua, et al. "A tale of two studies: The best and worst of yubikey usability." 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018.

[3] Das, Sanchari, Andrew Dingman, and L. Jean Camp. "Why Johnny doesn't use two factor a two-phase usability study of the FIDO U2F security key." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2018.

[4] Reese, Ken, et al. "A usability study of five two-factor authentication methods." Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019). 2019.

[5] Colnago, Jessica, et al. "“It's not actually that horrible” Exploring Adoption of Two-Factor Authentication at a University." Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. 2018.

[6] Reynolds, Joshua, et al. "Empirical measurement of systemic 2fa usability." 29th USENIX Security Symposium (USENIX Security 20). 2020.

[7] Jacomme, Charlie, and Steve Kremer. "An extensive formal analysis of multi-factor authentication protocols." ACM Transactions on Privacy and Security (TOPS) 24.2 (2021): 1-34.

[8] Joseph Bonneau,Cormac Herley,Paul C. van Oorschot,Frank Stajano, "The Quest to Replace

表 7　修正版の評価項目

評価軸	各評価項目	
Usability	U1: Memorywise-Effortless	U5: Easy-to-Learn
	U2: Scalable-for-Users	U6: Efficient-to-Use
	U3: Nothing-to-Carry	U7: Infrequent-Erros
	U4: Physically-Effortless	U8: Easy-Recovery-from-Loss
Deployability	D2: Negligible-Cost-per-User	D4: Browser-Compatible
	D3: Server-Compatible	D5: Mature
		D6: Non-Proprietary
Security	S1: Resilient-to-Physical-Observation	S6: Resilient-to-Leaks-from-Other-Verifiers
	S2: Resilient-to-Targeted-Impersonation	S7: Resilient-to-Phishing
	S3: Resilient-to-Throttled-Guessing	S8: Resilient-to-Theft
	S4: Resilient-to-Unthrottled-Guessing	S9: No-Trusted-Third-Party
	S5: Resilient-to-Internal-Observation	S10: Requiring-Explicit-Consent

Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes”, 2012 IEEE Symposium on Security and Privacy

[9] Justin Smith, Lafayette College; Lisa Nguyen Quang Do and Emerson Murphy-Hill, Google, ”Why Can’t Johnny Fix Vulnerabilities: A Usability Evaluation of Static Analysis Tools for Security”,soups2020