NRI SECURE

認証認可の調査研究

最終報告書

別添資料2 FIDO Alliance の策定規格 詳細

2020年09月25日

NRIセキュアテクノロジーズ株式会社

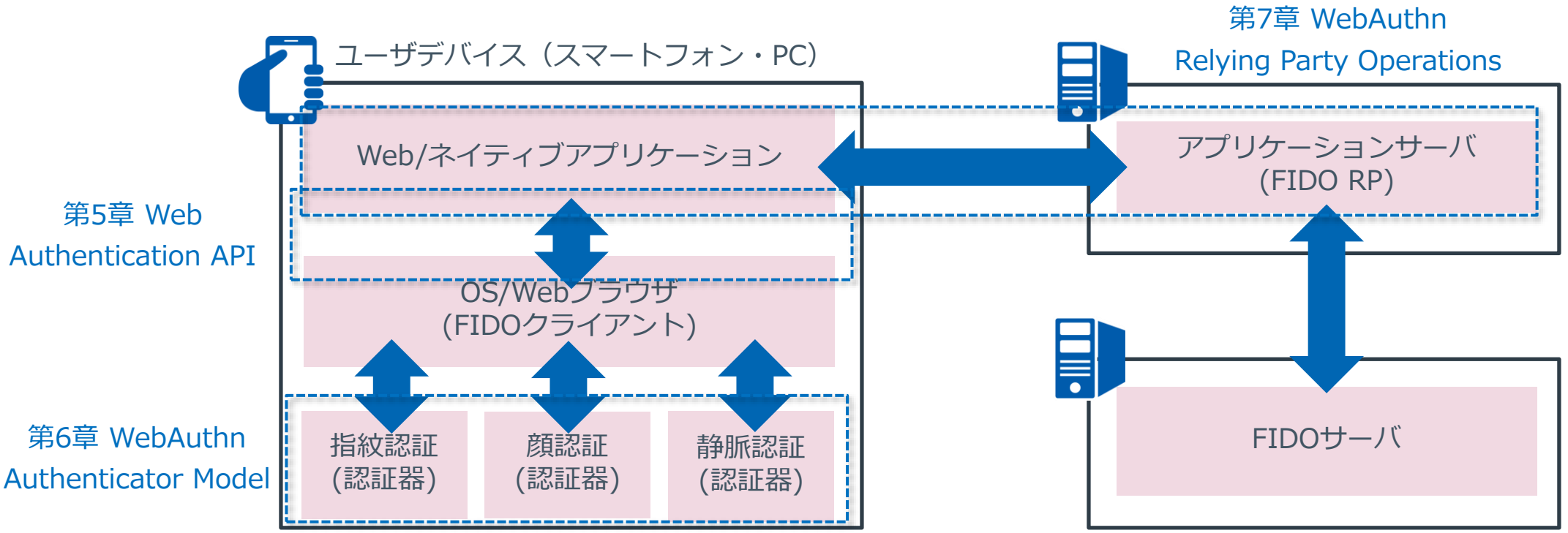
目次

1. Web Authentication API (WebAuthn)

WebAuthnではFIDOクライアントであるWebブラウザがサポートすべきAPI仕様を中心に記載されている。

WebAuthn概要

- WebAuthnは2019年3月にWorld Wide Web Consortium(W3C)にて勧告された。
- WebAuthn仕様のうち主要項目として、FIDOクライアントがサポートすべきAPI(第5章)、認証器モデル(第6章)、RP(Relying Party、アプリケーション)側の操作(第7章)、Attestationのフォーマット仕様(第8章)が定められている。



WebAuthnの各仕様のうち、API定義等の主要項目および本調査研究における実証と関連するセキュリティ・プライバシーに関する記載を中心に確認を行う。

目次

- 青字で記載している章については以降で説明する。

章	タイトル	概要
1	Introduction	WebAuthnの仕様の概略についての記載と、この仕様の位置づけ、想定されるユースケースについて記載
2	Conformance	WebAuthnにおける構成体である適合クラスに関して記載
3	Dependencies	WebAuthnと依存関係になるHTMLやECMAScript等の仕様について記載
4	**Terminology**	WebAuthnの仕様書で使われている用語定義
5	**Web Authentication API**	公開鍵クレデンシャルを作成・利用して認証を行うためのAPIについて定義
6	**WebAuthn Authenticator Model**	認証器の抽象モデル（データ、機能等）について定義
7	**WebAuthn Relying Party Operations**	RP(Relying Party、アプリケーション)側で想定する操作を定義
8	Defined Attestation Statement Formats	Attestationのフォーマットを定義

WebAuthnの各仕様のうち、API定義等の主要項目および本調査研究における実証と関連するセキュリティ・プライバシーに関する記載を中心に確認を行う。

目次（続き）

- 青字で記載している章については以降で説明する。

章	タイトル	概要
9	WebAuthn Extensions	第5章で定義されたAPIを特定のユースケースのために拡張する際の拡張方法を定義
10	Defined Extensions	IANAの“WebAuthn Extension Identifier”で定義済みの拡張仕様について記載
11	IANA Considerations	IANA(Internet Assigned Numbers Authority)が管理する名前空間への登録を行う際に考慮すべき事項を記載
12	Sample Scenarios	WebAuthn利用のユースケースシナリオを記載
13	**Security Considerations**	WebAuthnの使用においてセキュリティ面で考慮すべき点について記載
14	**Privacy Considerations**	WebAuthnの使用においてプライバシー面で考慮すべき点について記載
15	Acknowledgements	謝辞

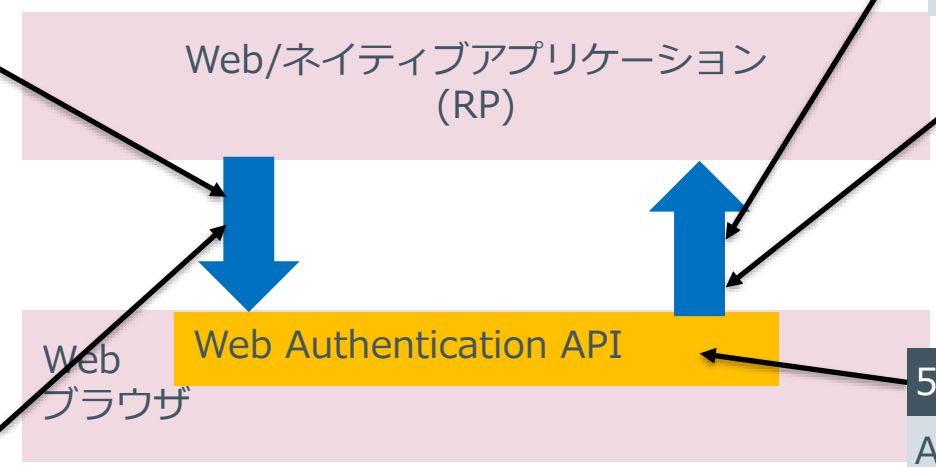
4章では、WebAuthnの仕様内で使用されている主な用語の定義を記載している。

用語定義

用語（一部抜粋）	概要
AAGUID	認証器はAAGUIDを有し、AAGUIDは、認証器のタイプを示す128ビット識別子。
Assertion	認証器から返される、暗号化された AuthenticatorAssertionResponse オブジェクト。
Attestation	一般的に、attestationとは、証明、確認、または認証を行うためのステートメントである。WebAuthnコンテキストでは、attestationは、認証器の製造場所と、認証器が出力するデータを証明するために使用される。たとえば、クレデンシャルID、クレデンシャルキーペア、署名カウンタなど。
Attestation Certificate	認証器がその製造と能力を証明するために使用する、attestationキーペアのX .509証明書。
認証器	公開鍵クレデンシャルを生成してRPに登録し、ユーザを検証して認証し、暗号的に署名して、WebAuthn RPから提示された認証アサーション、チャレンジ、およびその他のデータを返すためにWebAuthn クライアントによって使用される暗号化エンティティ。
クレデンシャル ID	公開鍵クレデンシャルソースとその認証アサーションを識別する一意なバイト列。
クレデンシャル公開鍵 ユーザ公開鍵	RP固有のクレデンシャルキーペアの公開鍵部分で、認証器によって生成され、登録時にRP返される。
WebAuthn Relying Party（RP）	WebアプリケーションがWeb認証APIを利用してユーザーの登録と認証を行うエンティティ。
公開鍵クレデンシャル	一般に、クレデンシャルは、あるエンティティが別のエンティティに提示するデータであり、後者に対して前者を認証する。公開鍵クレデンシャルという用語は、公開鍵クレデンシャル・ソース、公開鍵クレデンシャル・ソース に対応する証明済みの可能性のあるクレデンシャル公開鍵、または認証Assertionのいずれかを指す。公開鍵クレデンシャルソースに対応する、証明された可能性のある信任状公開鍵、または認証アサーションのいずれかを指す。
クライアント Webauthnクライアント	WebAuthnクライアントは一般的にユーザーエージェントに実装されている仲介者エンティティ。 概念的には、Web認証APIの基礎となる部分で、認証器の操作の入力を受け取り側の仕様に合うようにデータ変換することや、操作の結果をWeb認証APIの呼び出し側に返すことの両方を担当する。

5章では、登録処理と認証処理のそれぞれで利用されるWeb Authentication APIのインターフェースおよびデータ仕様について定められている。

- 5章の各節で定義されている仕様が対応する箇所は以下の通りとなる。



5.3 Parameters for Credential Generation
5.4 Options for Credential Creation

登録処理の際にAPIに渡すパラメタ仕様を定義

5.5 Options for Assertion Generation

認証処理の際にAPIに渡すパラメタ仕様を定義

5.2 Authenticator Responses

API応答結果のデータ仕様を定義

5.6 Abort Operations with AbortSignal

認証器側で処理が中断された時に返されるシグナルの仕様を定義

5.1 PublicKeyCredential Interface

APIのインターフェース仕様を定義

5.7 Authentication Extensions Client Inputs
5.8 Authentication Extensions Client Outputs
5.9 Authentication Extensions Authenticator Inputs

独自拡張を加える際に使用されるデータ仕様を定義

5.10 Supporting Data Structures

5章の各節で使用されるデータ仕様を定義

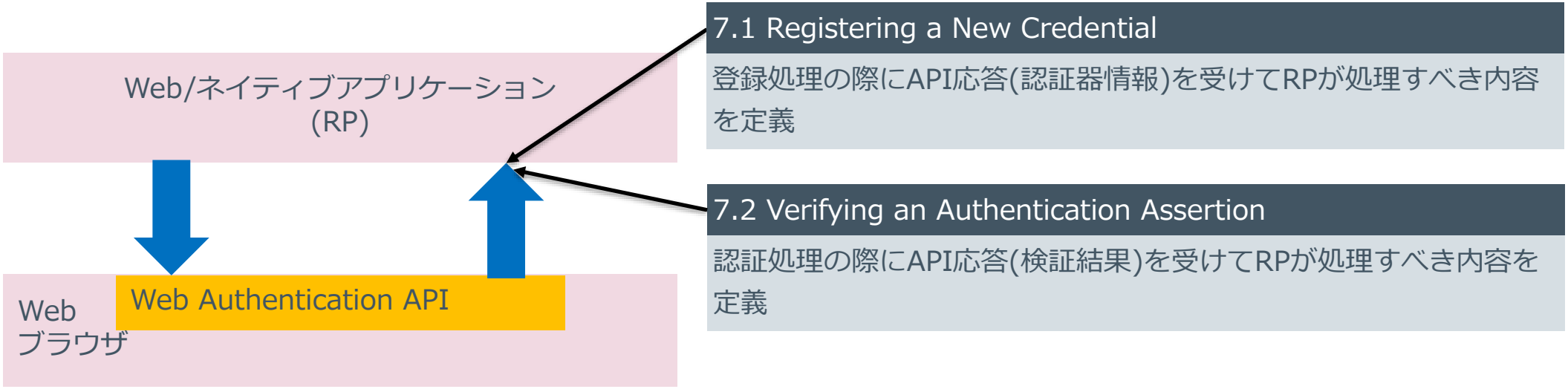
6章では、認証器の抽象モデルとして、認証器の分類や操作、データ仕様が定められている。

- 6章で定められている認証器に関する仕様はそれぞれ以下の通り。

節	タイトル	内容
6.1	Authenticator Data	Web Authentication API中で扱われる認証器を表すデータ構造を定義
6.2	Authenticator Taxonomy	認証器の種別について定義
6.3	Authenticator Operations	認証器が行う操作内容について定義
6.4	Attestation	登録処理の際に認証器情報として生成されるAttestationのデータ構造を定義

7章では、RPが実施すべき処理について、登録時と認証時のそれぞれについて記載している。

- 7章の各節で定義されている仕様が対応する箇所は以下の通りとなる。



13章では、WebAuthnのセキュリティ面で考慮すべき点についてまとめられている。

節	項目	対策・考慮事項
13.1	Cryptographic Challenges	登録処理及び認証処理においてRP側で作成されるchallengeの値についての注意事項を記載。具体的には以下の通り。 • サーバ側などの信頼できる環境下でランダムに生成すること。 • challengeの生成はクライアント側の振る舞いに依存しないこと。 • RP側は生成したchallengeを一時的に保存して返ってきた値と一致することを検証をすること。 • 推測不可能とするために十分なエントロピー（情報量）を持つこと。 • 少なくとも16バイト以上とすること。
13.2	Attestation Security Considerations	登録処理において生成されるAttestationの証明書の階層に関する注意事項および証明書が危殆化した場合の注意事項を記載。
13.3	Security Benefits for WebAuthn Relying Parties	WebAuthnを利用することによるRP側の利点についてまとめられている。 • 高い互換性を持ち、容易に多要素認証を利用できることでユーザを保護することが可能。 • WebAuthnという統一規格を利用することで、RPは認証器を独自に用意する必要はなく、ユーザも使いたい認証器を利用できる。また、複数のRPで1つの認証器を共用することも可能。 • 登録処理、認証処理は中間者攻撃から保護されている。 • RPはPINや生体認証のほか、今後出る新しい認証方式にも柔軟に対応可能。また、ユーザも利用する認証器を選択することが可能。 • RPは生体情報などの機密情報を内部で保持する必要がなくなる。

13章では、WebAuthnのセキュリティ面で考慮すべき点についてまとめられている。

節	項目	対策・考慮事項
13.4	Credential ID Unsigned	AttestationやAssertion内に入っているCredential IDは署名されない。しかし、Credential IDが間違って返されるか攻撃者によって改ざんされた場合においても、RP側が対応する公開鍵を参照できず処理はエラーとなるため問題は発生しない。
13.5	Browser Permissions Framework and Extensions	Web Authentication APIはブラウザのパーミッション(許可)フレームワークを活用すべきである。（例：位置情報APIに対するパーミッションフレームワークの利用）
13.6	Credential Loss and Key Mobility	認証器を紛失した場合を考慮し、Web Authentication APIでは1ユーザが複数の認証器に登録することを許可している。RPもユーザに対して複数の認証器に登録することを推奨すべきである。

14章ではWebAuthnのプライバシー面で考慮すべき点がまとめられている。

節	項目	対策・考慮事項
14.1	De-anonymization Prevention Measures	クライアント(OS/Webブラウザ)が扱うデータでユーザ情報の非匿名化につながる可能性のあるデータについて記載。
14.2	Anonymous, Scoped, Non-correlatable Public Key Credentials	クレデンシャル情報(公開鍵）からユーザ情報が特定できないように注意すべき事項について記載。 • クレデンシャル情報からユーザを直接特定できないようにする。 • クレデンシャル情報はRP毎に分けられており、不正なRPが他のRPのクレデンシャル情報を参照できないようにする。 • ユーザの同意なくクレデンシャル情報はRP側に渡さないようにする。 • 複数のクレデンシャル情報が同一ユーザのものであるかどうかの相関関係を見出すことはできないようにする。 • Attestation証明書だけで認証器が特定できないようにする。
14.3	Authenticator-local Biometric Recognition	基本的には認証時に利用される生体情報は認証器内のみで利用されるが、ユーザデバイスに内蔵されている認証器を使う場合、クライアントにも生体情報が参照できる可能性がある。そういった場合でもクライアントはRPに生体情報が渡らないように適切に実装されるべき。
14.4	Attestation Privacy	Attestation Key（認証器情報の識別子）はユーザの追跡につながる可能性があるため、その問題を緩和するために考慮すべきポイントについて記載。

14章ではWebAuthnのプライバシー面で考慮すべき点がまとめられている。

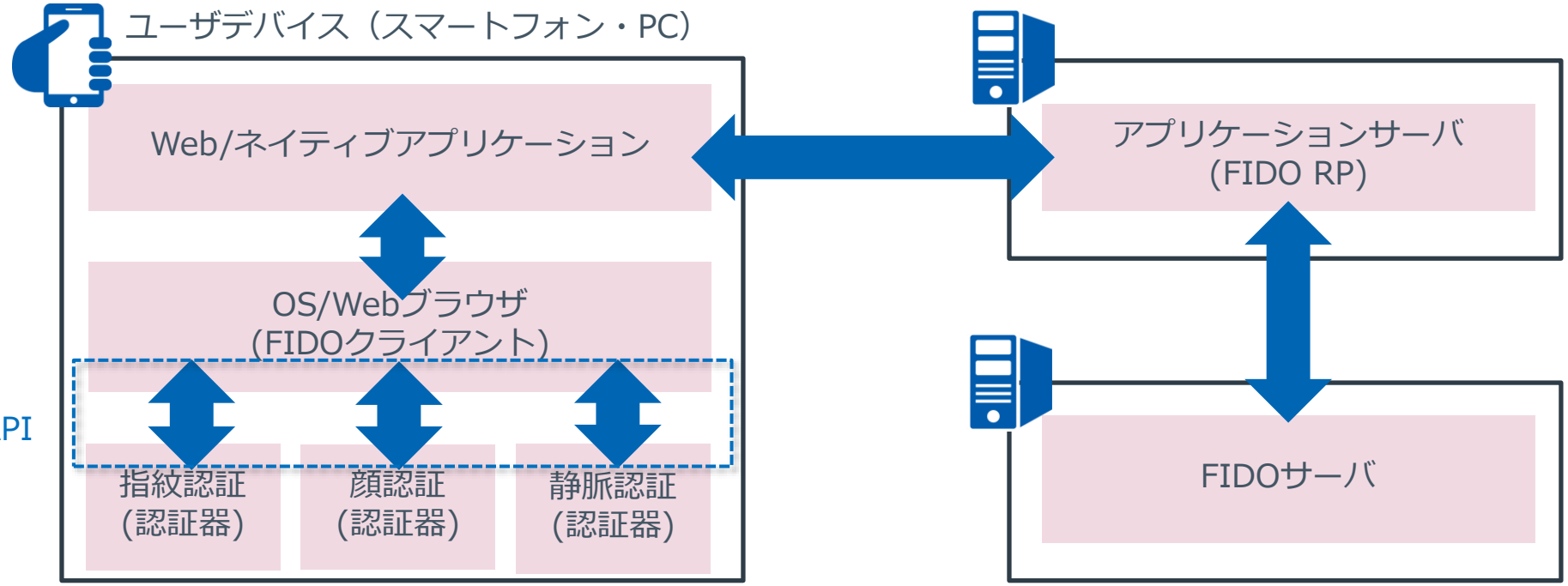
節	項目	対策・考慮事項
14.5	Registration Ceremony Privacy	登録処理においてユーザが同意なしに識別されることが無いようにクライアント側が注意すべきポイントについて記載。
14.6	Authentication Ceremony Privacy	認証処理においてユーザが同意なしに識別されることが無いようにクライアント側が注意すべきポイントについて記載。
14.7	Privacy Between Operating System Accounts	認証器がマルチユーザOSに内蔵されている場合において、クレデンシャル情報がそれを作成したユーザのみに公開されるように認証器とクライアントデバイス側が対応すべきと記載。
14.8	Privacy of personally identifying information Stored in Authenticators	• ユーザ識別機能を持つ認証器がWebAuthnの仕様外の追加情報をクライアント側に渡す場合においても、ユーザ認証が成功した時以外にユーザを識別する情報をさらさないようにすべきと記載。 • ユーザ識別機能を持たない認証器は個人識別情報をもってはいけない。
14.9	User Handle Contents	User HandleはRPがクレデンシャル情報とRP内のユーザを紐づけるために利用される識別子であるが、その識別子にメールアドレスやユーザ名などユーザが特定できる情報を使うべきではないと記載。また、ソルトなしのハッシュも使用すべきでないと記載。User Handleとして64バイトのランダム値の使用を推奨。
14.10	Username Enumeration	認証器を使って登録処理・認証処理を開始する際に、そのユーザが登録されているかどうかが判別できないようにRP側が実装時に考慮すべき点について記載。

2. Client to Authenticator Protocol Ver.2.0 (CTAP2)

CTAP2では認証器がサポートすべきAPI仕様を中心に記載されている。

CTAP2概要

- CTAP2は国際電気通信連合（ITU）の「ITU T 勧告 X.1278」によって、国際標準として承認されており、すでに認定取得済みの認証器が市場に出回っている。
- CTAP2仕様のうち主要項目として、認証器がサポートすべきAPI(第5章) が定められている。



第5章
Authenticator API

CTAP2の各仕様のうち、API定義等の主要項目を中心に確認を行う。

目次

- 青字で記載している章については以降で説明する。

章	タイトル	概要
1	Introduction	CTAP2の概略および同じく認証器に関する仕様としてCTAP1/U2Fとの関連について記載
2	Conformance	本仕様書に関する注意事項や用語定義について記載
3	Protocol Structure	プロトコルを構成する要素(Authenticator API, Message Encoding, Transport-specific Bindings)について記載
4	Protocol Overview	認証器とプラットフォーム(認証器と接続されるユーザデバイス)とのプロトコル概要を記載
5	**Authenticator API**	認証器がサポートすべきAuthenticator APIの各メソッドの仕様を記載
6	Message Encoding	CTAP2におけるメッセージをバイナリエンコーディング形式であるCBOR形式(RFC7049で定義)に変換する際の規則について記載
7	Interoperating with CTAP1/U2F authenticators	CTAP1/U2F対応の認証器をCTAP2で利用するためのリクエスト・レスポンスメッセージの互換方法について記載
8	Transport-specific Bindings	USB HID(Human Interface Device)、NFC、Bluetoothのそれぞれの通信規格に応じた通信仕様について記載

CTAP2の各仕様のうち、API定義等の主要項目を中心に確認を行う。

目次（続き）

- 青字で記載している章については以降で説明する。

章	タイトル	概要
9	Defined Extensions	認証器を特定のユースケースのために拡張する際の拡張方法を記載
10	IANA Considerations	IANA(Internet Assigned Numbers Authority)が管理する名前空間への登録を行う際に考慮すべき事項を記載
11	Security Considerations	CTAP2の使用においてセキュリティ面で考慮すべき点について記載 本仕様書ではセキュリティ面の考慮事項については別ドキュメントである「FIDO Security Reference」を参照している。

5章では、認証器がサポートすべきAPIのインターフェースおよびデータ仕様について定められている。

- 5章の各節では、APIのインターフェース仕様としてサポートすべきメソッドを以下の通り定めている。

節	メソッド名	説明
5.1	authenticatorMakeCredential	登録処理の際に呼び出され、鍵ペア情報を作成しそれを基にAttestationを作成する。
5.2	authenticatorGetAssertion	認証処理の際に呼び出され、ユーザ認証成功後に検証結果としてAssertionを作成する。
5.3	authenticatorGetNextAssertion	authenticatorGetAssertion(5.2節)の実行結果として複数のAssertionが返される場合、本メソッドを実行して2つ目以降のAssertionを取得する。
5.4	authenticatorGetInfo	認証器の情報を返す。
5.5	authenticatorClientPIN	認証器のPIN情報を操作する。
5.6	authenticatorReset	認証器の状態をリセットする(認証器に登録されている鍵情報などは削除される)。

NRI SECURE