NRI SECURE

認証認可の調査研究

最終報告書

別添資料4 OpenID Connect とFIDO を活用した認証認可構成の一部実証環境仕様

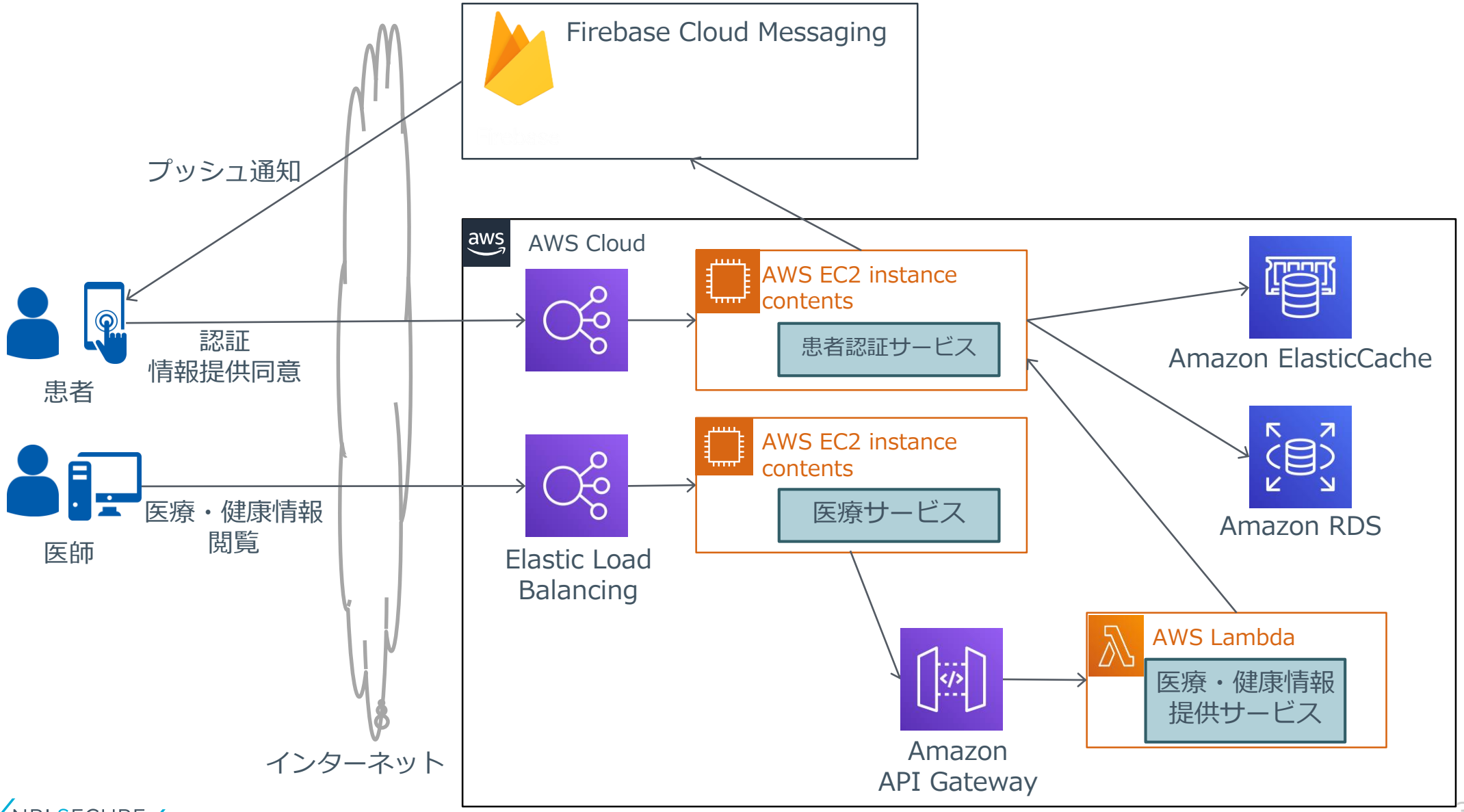
2020年09月25日

NRIセキュアテクノロジーズ株式会社

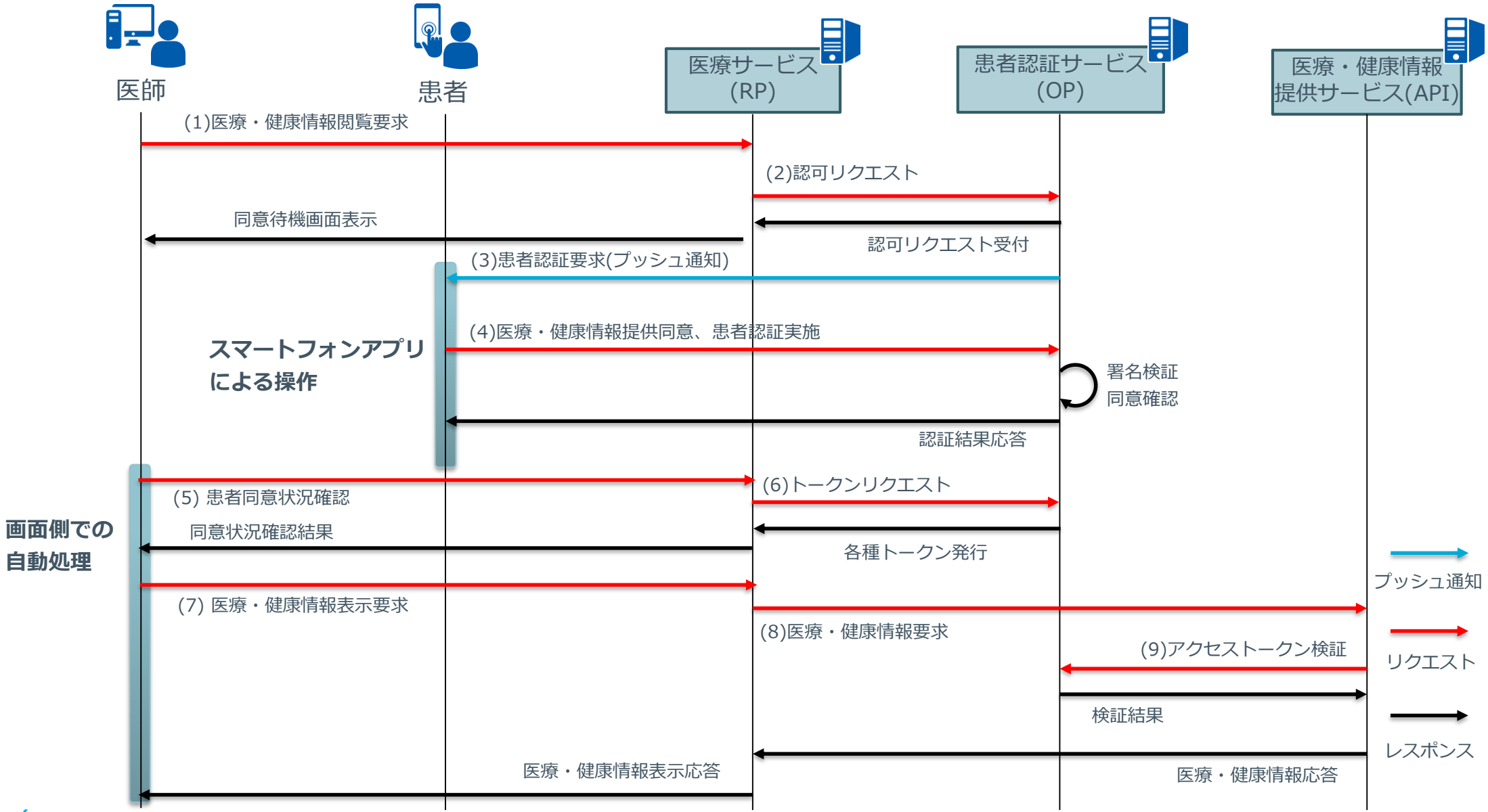
目次

1. システム構成図・処理シーケンス

患者認証サービス、医療サービス、医療・健康情報提供サービスのクラウド環境上の基盤構成は、以下のとおりである。



前項で示した構成における認証認可の処理シーケンスは以下の通りである。



認証認可の処理シーケンスにおけるリクエストの詳細な説明は下記の通り。

No.	リクエスト元	リクエスト先	概要	説明
1	医師端末 (Webブラウザ)	医療サービス	医療・健康情報閲覧要求	医師端末上に表示されている患者の、医療・健康情報閲覧のリクエストを医療サービスに行う。
2	医療サービス	患者認証サービス	認可リクエスト	医療サービスで、医師が医療・健康情報の閲覧を求めている患者の特定を行い、患者認証サービスに対して認可リクエストを行う。
3	患者認証サービス	患者端末 (スマートフォン)	患者認証要求 (プッシュ通知)	医療サービスからの認可リクエストを受け取った患者認証サービスは、患者の特定を行い、患者のスマートフォンに対して医療・健康情報の提供を求めるプッシュ通知を行う。
4	患者端末 (スマートフォン)	患者認証サービス	医療・健康情報提供同意、患者認証実施	患者認証サービスから届いた医療・健康情報提供を求めるプッシュ通知に同意すると、スマートフォン上でFIDO認証を行い、認証結果を患者認証サービスに送る。
5	医師端末 (Webブラウザ)	医療サービス	患者同意状況確認	医師端末から定期的に患者の医療・健康情報提供の同意状況の確認を行う。本処理は患者同意の待機画面側のJavascriptにより自動的に行われる。
6	医療サービス	患者認証サービス	トークンリクエスト	医療サービスから患者認証サービスへトークンリクエストを行い、患者のスマートフォンでの認証・同意が完了している場合に各種トークンが返却される。
7	医師端末 (Webブラウザ)	医療サービス	医療・健康情報表示要求	患者同意状況確認の結果、同意済みとなっている場合に医師端末から医療サービスへ医療・健康情報表示画面のリクエストを行う。
8	医療サービス	医療・健康情報提供サービス	医療・健康情報の要求	患者認証サービスから受け取ったアクセストークンを使って、医療・健康情報提供サービスに、医療・健康情報提供の要求をする。
9	医療・健康情報提供サービス	患者認証サービス	アクセストークン検証	医療サービスから受け取ったアクセストークンが正しいか検証するため、医療・健康情報提供サービスから患者認証サービスにアクセストークン検証のリクエストをする。

※上記の表でCIBAの仕様に関わるリクエスト（淡紅色の項目）に関しては、詳細を3章に記載。

2. 主要画面一覧

患者認証サービスおよび医療サービスの画面一覧は以下の通りである。

No.	システム・サービス	利用ユーザ	画面名称	説明
1	医療サービス	医師	患者一覧画面	医療・健康情報の参照を要求できる患者の一覧が表示されていて、患者に対して医療・健康情報の閲覧を要求をすることができる画面。
2	医療サービス	医師	患者同意の待機画面	医療・健康情報閲覧要求に対する患者の同意が得られるまで表示される画面。医療・健康情報閲覧要求の情報を確認することができる。
3	医療サービス	医師	医療・健康情報閲覧画面	患者の医療に関する情報を確認できる画面。
4	患者認証サービス（スマートフォンアプリケーション）	患者	医療・健康情報提供同意画面	患者へ医療・健康情報の提供に関する同意を取得する画面。
5	患者認証サービス（スマートフォンアプリケーション）	患者	FIDO認証画面	医療・健康情報の提供に関する同意が本人によってされていること確認するため、FIDO認証が行われる画面。

3. 主要インターフェース一覧・リクエスト仕様

主なインターフェースの一覧は下記の通り。

No.	システム・サービス	インターフェース名	説明
1	患者認証サービス	バックチャネル認証エンドポイント	CIBAのフローの認可要求を受けるエンドポイントで、CIBAの一連のフローを開始する際の最初のエンドポイント。
2	患者認証サービス	トークンエンドポイント	トークンを払い出す際に使われるエンドポイントで、医療サービスからリクエストが届く。
3	患者認証サービス	トークンインストロスペクションエンドポイント	アクセストークンの検証に使われるエンドポイントで、医療・健康情報提供サービスからリクエストが届く。
4	医療・健康情報提供サービス	医療・健康情報エンドポイント	医療・健康情報を払い出す際に使われるエンドポイントで、医療サービスからリクエストが届く。

「(2)認可リクエスト」のパラメータとして、CIBAのSecurity Considerationの内容を考慮して定めた。

No.	名称	説明
(2)	バックチャネル認証エンドポイント	CIBAによる認証リクエストを受け付けるエンドポイント

ヘッダーパラメータ	設定値／方針	説明／設定根拠
Authorization	“nri_medical:[client_secret※]”に対してbase64URLencodeで変換を行い、”Basic base64URLencodeで変換した文字列”を指定	OpenID Connect CIBA プロファイルの仕様に基づき設定した。
Content-Type	“application/x-www-form-urlencoded”を指定	患者認証サービスの仕様に基づき設定した。

ボディパラメータ	設定値／方針	説明／設定根拠
scope	“openid profile patient/Patient/read”に指定	スコープについてはHEART FHIR OAuth 2.0 Scopesの記載を参考にして、一番近いデータセットのスコープを採用した。
id_token_hint	患者認証サービスから取得した、患者のIDトークンを指定	OpenID Connect CIBA プロファイルの仕様に基づき設定した。
binding_message	患者に提供を求める医療・健康情報の詳細な内容を記載	攻撃者からの意図しない認証リクエストを患者が誤って認証しないように本パラメータを指定した。 値の指定の際はデバイスの制約上長い文字列や特定の文字セットを表示できない可能性を考慮した。
binding_title	“医療・健康情報提供への同意依頼” を設定	攻撃者からの意図しない認証リクエストを患者が誤って認証しないように本パラメータを指定した。 値の指定の際はデバイスの制約上長い文字列や特定の文字セットを表示できない可能性を考慮した。

※client_secretに関しては非開示

「(6)トークンリクエスト」におけるトークンリクエストのパラメータとして、CIBAのSecurity Considerationの内容を考慮して定めた。

No.	エンドポイント名	説明
(6)	トークンエンドポイント	アクセストークン、IDトークン、リフレッシュトークンを取得するエンドポイント

ヘッダーパラメータ	設定値／方針	説明／設定根拠
Content-Type	“application/x-www-form-urlencoded”を指定	患者認証サービスの仕様に基づき設定した。

パラメータ	設定値／方針	説明／設定根拠
auth_req_id	患者認証サービスから発行されたauth_req_idを指定	OpenID Connect CIBA プロファイルの仕様に基づき設定した。
grant_type	“urn:openid:params:grant-type:ciba”を指定	OpenID Connect CIBA プロファイルの仕様に基づき設定した。
client_id	“nri_medical”に指定。	患者認証サービスが払い出す値を設定した。
client_secret	医療・健康情報提供サービスのクライアントシークレットを指定	患者認証サービスが払い出す値を設定した。

「(8)医療・健康情報要求」のパラメータとして、 OAuth 2.0の内容を考慮して定めた。

No.	エンドポイント名	説明
(8)	医療・健康情報エンドポイント	医療・健康情報の提供を行うエンドポイント

ヘッダーパラメータ	設定値／方針	説明／設定根拠
Content-Type	“application/json”を指定	医療・健康情報提供サービスの仕様に基づき設定した。

パラメータ	設定値／方針	説明／設定根拠
access_token	患者認証サービスから発行されたアクセストークンを指定。	API認可の方式として、OAuth 2.0のアクセストークンを利用したアクセス制御を行った。
client_id	“nri_medical”に指定。	医療・健康情報提供サービスが提供するAPIアクセス用に患者認証サービスが医療サービス向けに払い出した値を設定した。
client_secret	医療サービスのクライアントシークレットを指定	医療・健康情報提供サービスが提供するAPIアクセス用に患者認証サービスが医療サービス向けに払い出した値を設定した。

「(9)アクセストークン検証」のパラメータとして、OAuth 2.0の内容を考慮して定めた。

No.	エンドポイント名	説明
(9)	トークンインストロスペクションエンドポイント	アクセストークンの検証を行うエンドポイント

ヘッダーパラメータ	設定値／方針	説明／設定根拠
Content-Type	“application/x-www-form-urlencoded”を指定	患者認証サービスの仕様に基づき設定した。

パラメータ	設定値／方針	説明／設定根拠
access_token	患者認証サービスから発行されたアクセストークンを指定。	OAuth 2.0の仕様に基づいて設定。
client_id	“nri_medicalinfo_provider”に指定。	患者認証サービスが医療・健康情報提供サービス向けに払い出す値を設定した。
client_secret	医療・健康情報提供サービスのクライアントシークレットを指定	患者認証サービスが医療・健康情報提供サービス向けに払い出す値を設定した。

NRI SECURE