

パブリックコメントにおける主な意見と対応

	コメント	回答
1	<p>P16 Figure3-暗号化処理ロジックのイメージ ワークフロー記号内の文字が途中で切れている箇所があります。</p> <p>(提案)下記の通りに修正してはいかがでしょうか。「鍵(key)生成の流れ」上から4個目「PadKey を MD5 でハッシュ」→「PadKey を MD5 でハッシュ化する。」「暗号アルゴリズム呼び出しの流れ」下から2個目「GenKey,GenIV、ファイルデ」→「GenKey,GenIV、ファイルデータを暗号化する」</p>	<p>ご指摘の点を改訂しました。</p>
2	<p>P16 Figure3-暗号化処理ロジックのイメージ ハッシュ関数を MD5 を事例にして説明しています。</p> <p>(提案)MD5 は電子政府推奨暗号リストにありません。MD5 を推奨していると誤解を与えるように思えますが、いかがでしょうか。</p>	<p>CRYPTREC 暗号化リスト最新版に記載の暗号関連技術を利用した規定に改めました。</p>
3	<p>P22 9.2 通信路 1行目 「 Upload Data [cloudPDI-4]、Download Data [cloudPDI-6]では TLS1.2 以上等、・・・」と記載されています。</p> <p>(提案)TLS の要件は、厚生労働省「医療情報システムの安全管理に関するガイドライン」で定義されていますので、あえて TLS のバージョンを記載する必要はないと思われます。さらに、同ガイドラインでは、CRYPTREC/IPS「TLS 暗号設定ガイドライン Ver3.0.1」の「高セキュリティ型」の設定を要求しています。これは TLS のプロトコルバージョンの他に、サーバー証明書及び暗号スイートの要件も指定されています。</p>	<p>ご指摘の点を改訂しました。</p>
4	<p>P22 9.2 通信路 2行目 「・・・、厚生労働省の「医療情報システムの安全管理に関するガイドライン 第 5.2 版」の・・・、」と説明されています。</p> <p>(提案)2023 年 5 月に「医療情報システムの安全管理に関するガイドライン 第 6.0 版」が公開されていますので、最新版を記載してはどうでしょうか。なお、第 6.0 版に変更されるのであれば、対応箇所は「システム運用編 13. ネットワークに関する安全管理措置[I、III]」などとなります。</p>	<p>ご指摘の点を改訂しました。</p>

5	<p>P.4 「FHIR では REST 通信が用いられるが、データが大容量となるため、REST 通信で送ることが可能なデータ量に分割」という記載について。REST は Web API の設計思想であり、以後の説明上も API 設計についての話がないことから REST の語が出てくることに違和感を覚えます。また REST は設計思想であることから「REST 通信」という用語にも違和感を感じるどころです。(日本国内で使われていることは認識しておりますが)</p> <p>また、REST API 及びそれを支える HTTP プロトコルの仕様自体にはデータ量の制限はない認識です。たしかに HTTP リクエストにおいて大容量のデータの送受信は実務上好ましくない(たとえば、本文中にあるように POST 時にサーバ側の設定として上限が定められていることが多いことや、GET 時も途中で通信が切断された場合に再度最初からの通信のやり直しが必要になること等)ことは事実ですが、HTTP や REST 自体に限界があるかのような現状の記載は事実誤認を生じさせる懸念があります。</p> <p>たとえばですが「FHIR では REST API が用いられるが、データが大容量となるため、データ受信側が 1 回の API リクエストで受け取ることが可能なデータ量に分割」といった記載に変更してはいかがでしょうか。</p>	<p>ご指摘の点を改訂しました。</p>
6	<p>全般 各アクターごとにマルチベンダーを意識した仕様</p> <p>1) Exporter/Uploader, 2) Reository, 3) Authorization Server, 4) Importer/Downloader のアクタがそれぞれ他ベンダーが実装することを前提にトランザクションやプロトコルについて明確に記述してほしい。</p> <p>現状、IF に対する仕様が不明確であり、ベンダー間の情報交換が行うことができない。</p>	<p>説明が不親切であったと思われる箇所について、記述や例を追加するなど改善しました。</p>
7	<p>全般 HI-TOKEN 仕様の詳細化</p> <p>HI-TOKEN の利用に際し、今回のケースでの各項目がどのようなデータを入力されるべきか、詳細な説明を記載してほしい。</p> <p>ISO ファイルには一般的な記述しかなく、相手先が施設が決まらない場合に相手先施設の ID は入れるべきか、患者情報に関して記載すべきかどうか、documentId の発番ルールやパスワードの格納の有無</p>	<p>•HI-TOKEN の利用にあたって本技術仕様での必須項目は community.identifier, document.identifier, decryption.password の 3 点で、それぞれについてアサインする情報を記述しています。</p> <p>•必須 3 項目が必須であること(他が任意であることを)記述いたしました(8.2)。</p> <p>•ドキュメント ID の発番ルールについては、OID</p>

	<p>など、解釈の違いをなるべく起こらないように記載を加えるべきと考える。また具体的なサンプルデータと合わせて提示をしてほしい。</p>	<p>であることから、形式やポリシーは一般的な OID のルールに従います。この仕様で OID のルールを記述する必要はないと考えております。</p> <ul style="list-style-type: none"> ・パスワードは必須ですが、このことは技術仕様全体を通じて(以前の記述でも)自明であるとと考えております。 ・ドキュメントIDについての説明を追加いたしました(7.2.3.1)。 ・パスワードの定義を変更し、また表現が明確になるように説明を追加いたしました(7.2.3.2)。
8	<p>P23 PDI データセットに対する FHIR の明示化 出力される FHIR がどの仕様に基づき出力されるべきなのか記述がない。</p> <p>受け取る側のビューアやインポーターにとり、どの実装ガイドを元に FHIR 形式のファイルが出力されるのかがわからないと受け取り解釈をすることもできない。受け取り側で解釈できずに、重要データの見落としなどのインシデントにもつながりかねない。</p> <p>JP Core 実装ガイド、3文書6情報実装ガイド等の形式に限定するもしくは、PDI データセットに関する FHIR 実装ガイドを作成し、仕様を明確化するなどの対策をとってほしい。FHIR のライブラリを利用してバリデーション等を行う際には、定義を参考にしているかの記載がないと検証を行うこともできない。</p> <p>定義しないのであれば、FHIR を解析する代替手段として PDF 等の情報を出力する等も検討してほしい。</p>	<p>7.3.6.3-7.3.6.4 が説明不足と思われるため、以下のとおり追記しました。</p> <ul style="list-style-type: none"> ・トランザクションの説明に例(Appendix E)への参照を追加いたしました(7.3.6.3)。 ・トランザクションの説明に FHIR リソースの定義への参照を追加いたしました(7.3.6.3)。 ・トランザクションの説明にデータ利用(再構成)の方法への参照を追加いたしました(7.3.6.4)。
9	<p>全般 アウトラインデータ形式について</p> <p>独自形式ではなく、FHIR 準拠した形式に記述すべきである。</p> <p>現在扱っている情報は、多くは JP Core 実装ガイドに定義済みであり、足りない部分は拡張定義を利用することで FHIR にて記述可能と考える。(アウトラインは Bundle と Composition を組み合わせた文書リソースとして定義すると収まりがよいと思います)</p> <p>独自形式と FHIR 形式が混在することで、別々のライブラリを用意してアクセスしなければならず開発の負荷が高くなったり、JP Core 実装ガイド等で記載してい</p>	<p>データ本体に画像を含むため、一般にデータサイズが大きく、ダウンロードには時間がかかります。アウトラインは、ダウンローダーがデータをダウンロード中に概要を一時的に表示するための情報であって、ダウンロード完了後は使用いたしません。アウトラインを FHIR Resource として定義できないか検討を重ねましたが、適切な FHIR Resource がありません。施設情報、患者情報以外の情報はメタレベルが異なっていて、混在させると混乱を招きかねないので敢えて使わないことにしております。</p>

	<p>る知見が活かされず、バリデーション機構等も独自で実装しなければならなくなり、メリットが少ない。FHIR 準拠形式にすることを強く望みます。</p>	<p>4.5 用語及び定義を修正して明確にしました。 ・アウトラインは転送データの一部ではなく、一時的な表示のための情報であることを記述いたしました(4.5)。</p>
10	<p>P4 引用規格 IHE-ITI Technical Framework Volume 1 Revision 18.0 IHE-ITI Technical Framework Volume 2 Revision 18.0 IHE-ITI Technical Framework Volume 3 Revision 18.0 ⇒現在は Revision20.0 と思われます。</p>	<p>ご指摘の点を改訂しました。</p>
11	<p>P8 Repository 1) FHIR サーバであり、WebAPI の仕様も FHIR に準拠することを明示してほしい。現状そのインタフェースについての記述が不明瞭であり、本当に実装しても通信ができるか不安である。 2)各アクタ Uploader, Repository, Downloader が実装すべき機能をトランザクション1つにつき明確に記述してほしい。 特に upload 時の新規、download 時の period 指定等はサンプルを交えて説明を追記すべきと考える。 3)上記の明確にするためにも、FHIR 実装ガイドを作成するとともに、各アクターごとの CapabilityStatement を記述すること。 これがないと、FHIR をメリットのひとつである機械可読な仕様を実現できずないため、必須の項目と考える。 4)ISO の HI-TOKEN の仕様にも記載されているように、今回の仕様は IHE MHD プロファイルの一部の機能に相当すると考える。実装ガイド作成の際には、IHE MHD 実装ガイド (https://profiles.ihe.net/ITI/MHD/index.html)との関連性についても記述があるとよい。</p>	<p>1) 2) コメント#7 への回答のとおり対応しました。 3) 4) 実装ガイドは別途作成し、公開する予定です。</p>
12	<p>P21 8.1.6.2 cloudPDI FHIR Bundle Bundle リソース定義、bundle リソースの説明 identifier の説明が bundle 項目表に記述がない。サンプルに記載があるが、表には記載がない、キーとなる項目であるため記載が必要。</p>	<p>ご指摘の点を改訂しました。</p>
13	<p>P21 8.1.6.2 cloudPDI FHIR Bundle Bundle リソース定義、Identifier に関連 HI-TOKEN の document.identifier に対する bundle リソースの格納先は、Identifier のみとし、id は指定し内</p>	<p>アップロード側では事前に発行されたドキュメント ID を id として update as create で登録し、ダウンロード側では検索を利用せずトークンによって伝達された同ドキュメント ID を id として直</p>

	<p>容がよいと考える。今後、修正に対応し履歴データを持つ場合に、同一の Identifier に対して id の異なる複数レコードを持つ場合に混乱が生じると考える(一般的には Id の割り振りはサーバ側で行われるユースケースが多いと考えられる)。</p> <p>それに合わせて検索方法は、Identifier を SearchParameter に指定して検索し、id を指定して read で取り出すフローに修正が必要になる。(IHE PDQm の Identifier に関する動作が参考になります。)有効期間(period)チェックは、検索の際に行うのか、取得した後チェックするのかも明記が必要と思います。</p>	<p>接 read で取得するというくみで、履歴は使用いたしません。period も利用いたしません。この構造がわかりやすくなるように表現を変更いたしました。</p> <ul style="list-style-type: none"> •各トランザクションについて利用する FHIR のインタラクションを明記しています。 •履歴データを利用しないことを明示するために、登録済みのドキュメント ID (id) に対する update をおこなわないことを記述いたしました(7.3.4.5)。 •search インタラクションを利用しないことを記述いたしました(7.3.6.2)
14	<p>P21 8.1.6.2 cloudPDI FHIR Bundle</p> <p>Composition リソース定義、subject の扱い</p> <p>患者情報の格納エリアである、Composition.subject をどのように扱うのか指針について説明を記載してほしい。現状の定義であれば、本仕様で定義されていないため FHIR Base を引継ぎ、入力してもよいと解釈してよいのでしょうか。アウトライン情報を暗号化していることもあり、もし隠したいのであれば仕様上明確に不可である旨を記述したほうがよいのでは。</p>	<ul style="list-style-type: none"> •subject を含む Bundle 全般について暗号化しない患者情報等を記載しないことを記述いたしました(8.1.6.2)。
15	<p>P21 8.1.6.2 cloudPDI FHIR Bundle</p> <p>Composition リソース定義、Composition.author</p> <p>author には複数プロファイルが指定可能であるが、今回それが指定されていない。指定されている文字列を見ると、device 型だと推測されるが明示的に仕様として提示をしたほうがよいと思われる。</p>	<p>device 型であることを仕様に記述しました。</p>
16	<p>P21 8.1.6.2 cloudPDI FHIR Bundle</p> <p>Composition リソース定義、Composition.author</p> <p>uploader の施設情報の格納するエリアに利用したい。現在の仕様では、施設情報は composition.entry の配下に暗号化されたうえで格納されており、簡単に取り出せない位置にいる。document.identifier では、Identifier が重複してしまう可能性を否定できないため、書類取り出しの際に施設情報を比較するために Composition リソースに格納場所を用意したい。</p>	<p>検索を利用しないことを仕様に記述しました。</p> <ul style="list-style-type: none"> •FHIR の read インタラクションで使用する id は検索の結果ではなく、ドキュメント ID そのものであることを記述いたしました(7.3.6.2)。 •履歴データを利用しないことを明示するために、登録済みのドキュメント ID (id) に対する update を行わないことを記述いたしました(7.3.4.5)。 •search インタラクションを利用しないことを記述いたしました(7.3.6.2)。
17	<p>P21 8.1.6.2 cloudPDI FHIR Bundle</p> <p>Composition リソース定義、Composition.author に対</p>	<p>コメント#15 への回答のとおり、device 型であることを記述したため、構造上 1..1 となります。</p>

	<p>する多重度</p> <p>多重度を派生元である 1..*のままにしてほしい。現在の定義である 1..1 の制約により、送信元施設情報や送信者などの付加情報を格納できないため。</p>	
18	<p>P21 8.1.6.2 cloudPDI FHIR Bundle</p> <p>Compsitoion.type</p> <p>compision.type をテキストで記載しているが、あらかじめ決まっている項目であれば、CodeSystem,ValueSet を定義しコードとしてほしい。</p>	<p>コードとして定義しました。</p>
19	<p>P21 8.1.6.2 cloudPDI FHIR Bundle</p> <p>Compsitoion.category</p> <p>他用途で利用している Bundle リソースと区別をするために、Category を定義してほしい。今回の用途以外の Bundle リソースを格納する可能性もあることからあらかじめ定義を決めておくべきと考える。</p>	<p>コードとして定義しました。</p>
20	<p>P22 9.4 監査</p> <p>監査の書式、記録方法、対象イベント等どこまでをサポートすべきかを記載してほしい。できれば IHE ATNA 等の標準的な仕様で定めてほしい。</p>	<ul style="list-style-type: none"> ・記録する内容や記録の方法については規定しないことを記述いたしました(9.4) ・参考資料への参照を追加いたしました(9.4)
21	<p>その他 改ざんチェック</p> <p>施設間のデータ連携であるため、データ改ざんのチェックを行いたい場合にどのような実施すべきかの方法の記述が見当たらない。改ざんのチェックの必要性や方法についての指針を記述してほしい(例えば bundle.signature を利用し、受け入れ時にチェックをするなど)</p>	<p>コメント#8 に対する回答のとおりです。</p>
22	<p>その他 FHIR リソースに関するバリデーション</p> <p>他ベンダーとの間でやり取りを前提とすると、Repository 受信時にデータの Validation が必要と考える。</p> <p>Validation のフローを追加し、また不正データだった時の対応を記述してほしい。(IHE MHD(ITI-65)のトランザクションが参考になります)</p>	<ul style="list-style-type: none"> ・データ内容に不正があった場合、Repository はリクエストに応じないことを記述いたしました(7.3.4.5)
23	<p>その他 削除・修正について</p> <p>削除・修正をオプション扱いとすることができないか。</p> <p>紙を患者に渡した後、間違いに気づいた場合に、これを止めるべきがないため。</p>	<ul style="list-style-type: none"> ・登録済みデータの削除は本仕様では規定しないことを記述いたしました(6)。 ・登録済みデータに対する変更ができないことは仕様として維持いたしました。