令和４年９月１５日　１４時から
東京区政会館　１５階会議室

令和４年度第１回情報公開・個人情報保護審議会　案件表

【個人情報業務案件】

（諮問）

第１号　　外部委託の可否について
（高額療養費支給事前申請（配慮措置施行対応）等業務支援委託について（追加））

4 東 広 総 総 第 336 号
令 和 4 年 9 月 8 日

東京都後期高齢者医療広域連合
情報公開・個人情報保護審議会会長　様

東京都後期高齢者医療広域連合長
山﨑　孝明

令和４年度諮問第１号

東京都後期高齢者医療広域連合情報公開・個人情報保護審議会条例第２条に基づき下記の事項について諮問します。

記

１　外部委託の可否について（個人情報保護条例第６条）

高額療養費支給事前申請（配慮措置施行対応）等業務支援委託について（追加）

4 東 広 審 第 2 号
令和 4 年 9 月 15 日

東京都後期高齢者医療広域連合長
山﨑　孝明　様

東京都後期高齢者医療広域連合
情報公開・個人情報保護審議会会長
茶谷 達雄

令和４年度答申第１号

東京都後期高齢者医療広域連合情報公開・個人情報保護審議会条例第２条に基づき下記の事項について答申します。

記

１　外部委託の可否について（個人情報保護条例第６条）

高額療養費支給事前申請（配慮措置施行対応）等業務支援委託について（追加）

可とする。

データ送受信方法の変更について

作成日：2022年9月2日

01 背景

対象業務

・高額療養費支給事前申請等業務における、個人情報を含むデータのやり取り

現状

仕様書上では、個人情報を含むデータのやり取りは、**「郵送（特定記録郵送）」**又は**「媒体手渡し」**に限定されている。
しかしながら、以下の課題があるため、**電子ファイル送信への手段変更が必要**となっている。
9月20日以降から実業務が発生するため、早急に変更する必要がある。

課題

郵送や媒体手渡しでのやり取りは、**セキュリティ面と業務効率の両方でデメリットが大きく**、業務に支障がでると想定される。

セキュリティ面	移送中の**紛失・盗難・破損リスク**が、電子ファイル送信と比較して高い
	受領した現物や媒体の**管理・保管のリスク**が発生する
	受領した**現物の物理的廃棄、媒体のデータ消去（又は物理的破壊）**が必要となる
運用面	届くまで数日の郵送期間がかかる ・被保険者へのレスポンスが遅れる事によるクレーム増加 ・タイムリーな状況確認・判断が出来ない
	業務の手間が増える ・郵送の封入作業、封入物チェック、郵便局への持参などの業務量増 ・送付都度、郵便料金やセキュリティー便等の配送費用の支払が発生する ・媒体受渡時の立会いが必要になる

より早く、安全な手段でデータ送受信を実現する必要である。

02　取り扱う個人情報について

対象業務で、取扱う想定の個人情報は以下の通りとなります。

①宛名データ（申請書の印刷・発送のためのデータ）

被保険者情報：　被保険者番号、被保険者氏名、住所、生年月日　等

②申請書のスキャンデータ

被保険者情報：　被保険者番号、被保険者氏名、住所、生年月日、電話番号、登録口座情報

成年後見人情報：　氏名、住所、電話番号

受任者情報：　氏名、住所

③コールセンターへのお問い合わせで取得した情報

お問合せ元の情報：　氏名、電話番号、住所

被保険者情報：　被保険者番号、被保険者氏名、住所、生年月日

④エスカレーション（審査・コールでの要確認事項）

※上記②③と同様

03　郵送と電子ファイル送信サービスとの比較

比較表

サービス名	安全性	到着までの早さ	自治体での実績	その他条件
郵送（特定記録郵便）	× 郵送や社内移送中の紛失リスク	× 数日の郵送期間	△ 類似用途での利用実績は無し	× 都度切手代が発生する＆追跡番号管理も必要
LGーWAN	○ 地方公共団体間専用の高セキュリティ環境	○ 即時送付可能	○ 地方公共団体間専用の高セキュリティ環境	× 業者間でのやり取りでの利用不可
クリプト便	○ 第三者機関からの高いセキュリティ評価	○ 即時送付可能	× 自治体での利用実績は確認できなかった	× 自治体での利用実績無し
個人情報マスキングメール送信	× マスキング漏れのリスク 誤送信リスク	○ 即時送付可能	△ 類似用途での利用実績は無し	× 漏洩リスクの観点から業者側の規定でもNG

結果

※郵送に比べて、LG-WANとクリプト便の方が、安全かつ迅速に取り扱うことが出来る。

※郵送は被保険者へのレスポンスが遅すぎる。やり取りに数日かかるため、
被保険者からのクレームに繋がる可能性が高く、本業務に適さない。

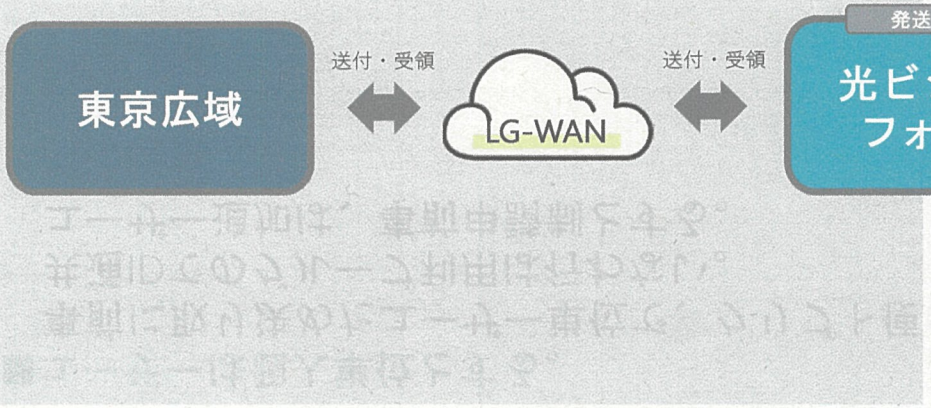
※個人情報マスキングメール送信は、漏洩リスクを完全になくすことが出来ないため、採用は難しいと判断

郵送よりも安全で、時間がかからない電子配信サービスを採用したい

04 業務フローと利用用途

「LG-WAN」と「クリプト便」の併用した運用を想定しています。

広域連合と業者間での情報共有



使用用途

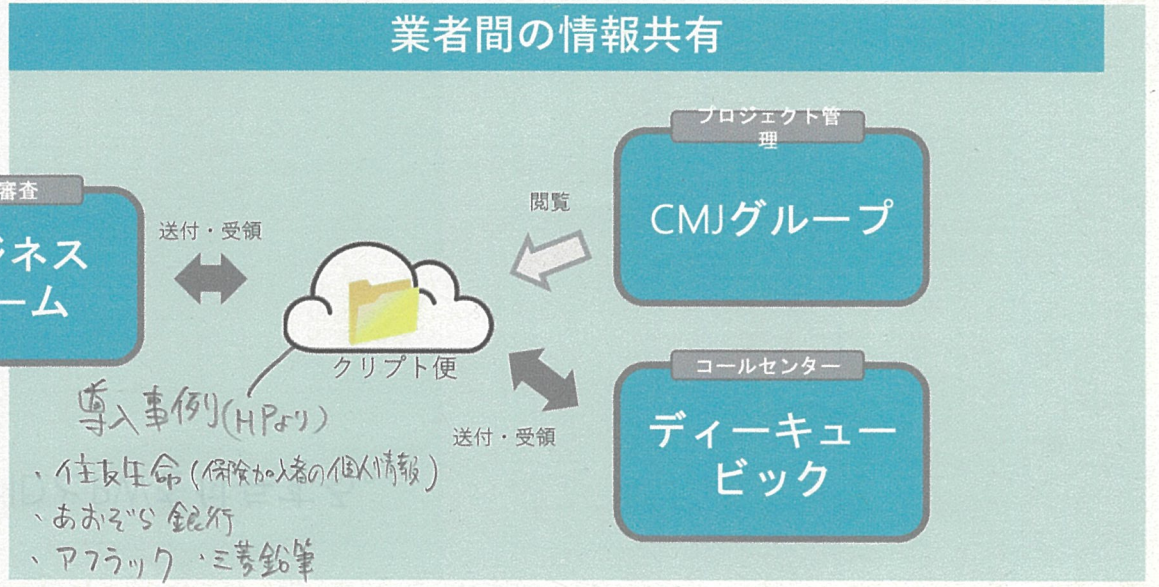
【HBF→東京広域】

1. エスカレーションシートの送付
2. 申請書のスキャンデータ（確認が必要な場合のみ）

【東京広域→HBF】

1. エスカレーションシートの回答

業者間の情報共有



使用用途

【業者間での情報共有】

1. 最新エスカレーションシートの共有 (CMJグループは閲覧のみとなる)
2. エスカレーションシート回答の共有
3. 申請書のスキャン画像データ （緊急時のみ。管理職承認が必要）

※LG−WANは、業者間での使用が出来ないため、クリプト便と併用が必須

05　クリプト便の機能的な対処について

■データの保存期間の設定
データ消去期間は、5日後消去で設定する。

■ユーザーは個人単位とする。
事前に取り決めたユーザー単位で、クリプト便のIDとPWを付与する。
共通IDでのグループ利用は行わない。
ユーザー追加は、事前申請制とする。

06　リスクに対する対応

「クリプト便」利用におけるリスクと対応については以下の通りです。

	想定リスク	評価	対応
1	アカウント不正利用・ユーザー誤送信	○	利用アカウントは、本業務の関係者のみに発行されるので、関係者以外に誤送信されることは無い。 アカウントの新規登録は、管理者権限ユーザーのみしか登録できない仕様で、かつ登録には社内の承認が必要となる。
2	ファイルデータの漏洩・改竄	○	通信はHTTPS通信（TLS.1.2）で暗号化。ファイルはAESで暗号化して保管。最新のパターンファイルで自動的にウイルスチェックを実施。
3	不正アクセス	○	多段にFWを設置し、必要な通信以外は遮断。WAFを設定し、不正な攻撃パターンを検知し、必要に応じた対策を実施
4	物理的侵入	○	Tier4相当のデータセンター内で運用・管理されています。 赤外線監視カメラ、生体認証装置、X線検査装置、３Dホログラフィックボディスキャナを設置し、不正な侵入や機器・媒体の持ち出しを監視しています。
5	システム障害への対策	○	機器、ネットワーク、電源の冗長化。24時間３６５日監視。定期的なセキュリティ診断の適用やセキュリティパッチの適用を実施しています。
6	クラウド事業者内のヒューマンエラー	○	定期的な監査を実施し、ルールの見直し及び改善を実施しています。 研修やＯＪＴで機密情報の取り扱いやセキュリティに関する教育を実施しています。

リスクに対する対応が、実施されている事を確認済み

07 第三者機関によるセキュリティ評価

■クリプト便のセキュリティ対策

ISO/IEC 27001

NRIセキュアテクノロジーズは、ISMS（情報セキュリティマネジメントシステム）の国際規格であるISO/IEC 27001認証を全社で取得しています。

クリプト便においても、規格にのっとった、厳格なセキュリティマネジメントを実施しています。

IS 75215/ISO 27001:IJ 00347
ISO IEC 27001を全社で取得しています。
※国内事業所に限る

ISO/IEC 27017
ISO/IEC 27018

クリプト便は、クラウドサービスプロバイダとしてクラウドサービスの情報セキュリティ管理に関する国際規格「ISO/IEC 27017」、および、クラウドサービスの個人情報管理に関する国際規格「ISO/IEC 27018」の認証※を取得しています。

※クラウドサービスに関する国際規格であるISO/IEC 27017に基づくISMSクラウドセキュリティ認証(JIP-ISMS517-1.0)、およびISO/IEC 27018に基づくプライバート認証を取得。

CLOUD 712951　PII 712952

情報セキュリティ格付け最高位「AAA_{is}」

クリプト便の運用業務に対して、株式会社アイ・エス・レーティングより、情報セキュリティ格付け最高位※の「AAAis」を付与されました。
※ 2020年9月現在サービス最高レベルの格付け

AAA_{is}で求められる2つの用件

■要件１新たな脅威に迅速に対応し、常時、高水準の管理状態を維持、発展させている。

■要件２常時、リスクをモニタリングし、即時に柔軟な対応ができる。

I.S.Rating
10000080206C2010

PCI DSS

クリプト便は、サービスプロバイダーとして、PCI DSS※に準拠したことを示す認証を取得しています。

従来、電子記録媒体の郵送やFAXなどで社外とやり取りしていたクレジットカード番号を含む重要情報 も、クリプト便で取り扱うことが可能です。

※PCI DSS：Payment Card Industry Data Security Standardsの略称。クレジットカード情報の漏えいを防止するために、策定されたクレジットカード業界における国際的なセキュリティ基準。

GRCS - 2105

第三者機関からのセキュリティ評価も取得しています。

08 その他

■過去に情報漏洩のあった情報共有ツール「ProjectWEB」との安全性の比較

→ ProjectWEBの事案の詳細な原因が公開されていないため、比較が難しい。
検証委員会からの指摘事項は以下①～④が原因として挙げられており、
主に体制や管理体制に問題があったように見受けられる。

① 情報保護の体制が不十分であったこと
② ProjectWEB に対する人員・予算の制約等からセキュリティの強化・管理に手が回らなかったこと
③ 不正アクセスを直ちに検知する体制が整っていなかったこと
④ 各テナントの管理に係る事項の多くがテナント管理者に委ねられていたこと

上記①～④のリスクについては、前頁のリスクに対する対応に記載の内容や、
第三者によるセキュリティ評価で担保されていると思われる。

09 別紙参考資料

■クリプト便セキュリティ対策

クリプト便

NRI SECURE

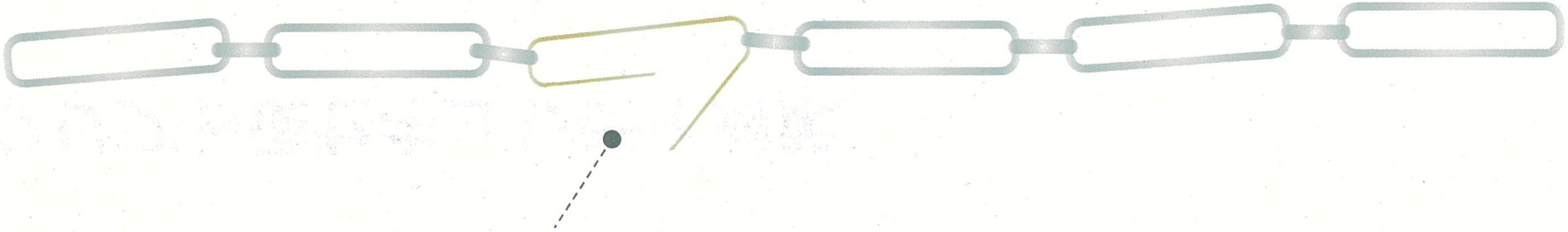
クリプト便セキュリティ対策

2022年4月版

NRIセキュアテクノロジーズ株式会社
ファイルセキュリティ事業部

電子ファイル送付におけるセキュリティ対策の要点

電子ファイルを安全・確実に送受信するためには、
ひとつのものに特化した高水準の対策をするのではなく、
高水準かつ**「抜け」・「漏れ」**のない万全なセキュリティ対策が必要です。



セキュリティの水準が低い部分ほど攻撃者から狙われやすく、
情報の漏えいの可能性が高まります

クラウドのファイル転送/共有サービスを選定する際の確認ポイント

サービス選定時にはセキュリティ面で様々な確認ポイントがあります。
セキュリティホールになりかねないため**包括的な対策が必要**です。

No.	リスク	確認すべき点
1	ユーザアカウントの不正利用、ユーザの誤送信	ユーザに提供されるセキュリティ機能
2	ファイルデータの漏洩、改ざん	通信・保管データに対する保護
3	不正アクセス	内部・外部からの不正アクセス対策内容
4	物理的な侵入行為	サーバ(データセンター)の設備基準
5	システム障害	システム障害への対策と復旧までのプログラム
6	クラウド事業者内でのヒューマンエラー、内部犯行	クラウド事業者内の管理体制や人材教育

電子ファイル送付におけるセキュリティ対策の要点

クリプト便は**複数のセキュリティ対策**を合わせたサービスを運用することで、
「**安全かつ確実**」な電子ファイルの送受信サービスを提供します。

1.多彩なセキュリティ機能の実装

自社に合わせたセキュリティポリシーの設定、**誤送信防止**機能、**不正利用防止**機能など

2.通信・保存データに対する保護

クリプト便サーバへ転送されるファイルについては、通信経路およびサーバ保管時に暗号化を行い、**漏洩・改ざん対策**

3.外部・内部からの不正アクセス防止

入口対策に多段階の防御網を実装、**出口対策**として　データサーバ接続時に承認を必須とするゲートウェイサーバを設置し**不正アクセスを防止**

4.サーバの物理的な保護

Tier4相当の日本国内データセンターにて**厳重なセキュリティ管理**を実施

5.システム障害への対策

可用性を維持するため様々な**冗長化**や、継続的な**障害検知**からの迅速**復旧体制**、定期的な**セキュリティ診断**、効果的・迅速的な**パッチ適応**

6.組織および人材面での対策

セキュリティ対策の見直しを定期的に実施

セキュリティ対策 ❶

多彩なセキュリティ機能の実装

クリプト便の仕組みによるセキュリティ対策を標準機能として提供します。

クリプト便の送受信時（ユーザ）	
✓	端末のIPアドレス制御 ユーザごとに、接続許可するグローバルIPアドレスを設定可能
✓	ワンタイムパスワード認証 通常のログインパスワード認証に加えて、ワンタイムパスワードによる認証が可能
✓	送受信画面のセッションタイムアウト 不正利用防止のため30分経過すると、自動的にログアウト
✓	送信可能な宛先・拡張子の制限 特定の送信先、ファイル拡張子のみを許可/拒否することが可能
✓	ファイル取得用パスワードの設定 万一誤送信してもパスワードが分からなければファイル取得不可
✓	送信結果の通知 送信結果通知メールにより、なりすましの検知が可能
✓	送信キャンセル ファイル送信後でも随時送信キャンセルが可能

クリプト便の管理時（管理者）	
✓	端末のIPアドレス制御 管理者ごとに、接続許可するグローバルIPアドレスを設定可能
✓	ワンタイムパスワード認証 通常のログインパスワード認証に加えて、ワンタイムパスワードによる認証が可能
✓	管理者画面のセッションタイムアウト 不正利用防止のため30分経過すると、自動的にログアウト
✓	管理者権限の細分化 管理者ごとに、ユーザ設定やログ閲覧等の権限を分けて付与可能
✓	送受信ログの取得 いつ、どのユーザが、どこへ、何を送受信したのか、送受信ログを取得
✓	不正送信の停止 ファイル送信後でも管理者が随時送信を停止可能

多彩なセキュリティ機能の実装課題

○：根本対策　△：部分対策

主な課題と対策になります。オプション毎の機能/仕様は別資料をご参照ください。

リスク観点	項番	対策	ファイル送受信		ファイル共有(オプション)	
			標準	オプション	標準	オプション
許可していない環境への送受信禁止	1-1	許可された環境外からのログインを禁止する（パスワード漏洩対策をする）	○IPアドレス制限 ○ワンタイムパスワード認証	○端末認証 ○認証連携	○IPアドレス制限 ○ワンタイムパスワード認証	○端末認証 ○認証連携
	1-2	許可していない相手先への送受信/共有を禁止する	○クローズドグループ ○送信先制限		○クローズドグループ	
危険な操作の監視/対応	2-1	宛先/添付ファイルの誤設定を監視/防止する	○送信前チェック △追加メールアドレス	○上長承認 △宛先直接入力禁止	△追加メールアドレス	○上長承認
	2-2	不正操作の痕跡を確認できるようにする	△メッセージログ	○管理者操作ログ ○ファイルアーカイブ	△ファイル共有ログ	○管理者操作ログ ○ファイルアーカイブ
危険な操作ができない環境を用意	3-1	ウイルスファイルの送受信/共有がされないようにする	○ウィルスチェック※1 △拡張子制限		○ウィルスチェック※1	
	3-2	ファイルのダウンロード権限を制限する	△ファイル持ち出し抑止※2		○掲示/回収ボックス	○プレビュー(開発予定)
	3-3	ファイルを長期間保管しないようにする	○お預かり期限の設定		○自動ゴミ箱移動/自動削除	
	3-4	ヒューマンエラーによる誤送信リスクを排除する		△オートパイロット※3		△オートパイロット※3
	3-5	当該監査人の対象外グループのログ閲覧を禁止する		○グループ毎 送信ログ監査		○グループ毎 送信ログ監査
不要アカウントの利用禁止	4-1	使わなくなったアカウントを棚卸する	△自動ロック	○ユーザID連携	△自動ロック	○ユーザID連携
	4-2	他社セクション発行のID利用／他社セクションのゲストユーザ利用を禁止する		○専用ドメイン※4 (+端末認証 ※5)		○専用ドメイン※4 (+端末認証 ※5)

※1 ウィルスチェックを実施するファイルサイズの上限はアップロード時100MB、ダウンロード時20MBです。
※2 送信ボックスでのファイルダウンロードを禁止する設定です。
※3 ヒューマンエラーを排除するには貴社側での開発・作り込みが必要となります。
※4 自社セクションを専用ドメイン化し、クリプト便の汎用ドメインをURLフィルタリングで禁止する必要があります。 URLフィルタリングは貴社側でのご用意が必要です。
※5 専用ドメインと端末認証を併用することで、他社セクションのID利用禁止と、特定端末からのアクセスのみに制限できるため、より強固な環境を構築可能です。

セキュリティ対策 ❷

通信・保存データに対する保護

クリプト便で転送・保存するデータは暗号・ウィルスチェック・バックアップ等で保護します。

送受信における通信の暗号化

- ✓ 通信経路はHTTPS通信（TLS1.2）で暗号化を施しています。

TLS

ウィルス対策

- ✓ 送受信の際、最新のパターンファイルで自動的にウィルスチェックを実施します。

※ 20MB以上のファイルは送信時のみ、100MB以上のファイルは対象外となります。

サーバ上のファイルの暗号化

- ✓ ファイルはAESで暗号化して保管します。
- ✓ 弊社運用担当者もファイルの内容を閲覧、取得することはできません。
- ✓ 保存期間が過ぎると自動的に削除します。

ログのバックアップ

- ✓ ログは24時間に1回バックアップされます。

※ 送受信されたファイルは、バックアップを行いませんので、障害等でファイルが消失した場合、再送信をお願いします。