後期高齢者医療に関する事務に係る特定個人情報保護評価書（全項目評価書）の変更箇所一覧

該当ページ	番号	項目	変更前の記載	変更後の記載
P6	1	Ⅰ　基本情報 ２．特定個人情報ファイルを取り扱う事務において使用するシステム	記載なし	システム５　統合宛名システム システム６　中間サーバ
P7	2	Ⅰ　基本情報 ４．特定個人情報ファイルを取り扱う理由 ①事務実施上の必要性	・被保険者資格や給付の情報等を個人番号により正確かつ効率的に検索・照会するためには、被保険者資格や給付の情報、住民基本台帳関連情報、福岡市で使用している宛名番号及び後期高齢者医療広域連合で付番する被保険者番号等を、個人番号と紐付けして管理する必要があることから、特定個人情報ファイルとして後期高齢者医療関連情報ファイルを保有する。	・被保険者資格や給付の情報等を個人番号により正確かつ効率的に検索・照会するためには、被保険者資格や給付の情報、住民基本台帳関連情報、福岡市で使用している宛名番号及び後期高齢者医療広域連合で付番する被保険者番号等を、個人番号と紐付けして管理する必要があることから、特定個人情報ファイルとして後期高齢者医療関連情報ファイルを保有する。 ・個人番号を用いることで申請・届出の手間や行政手続きを省略化し、市民の利便性の向上を図る必要がある。
P7	3	Ⅰ　基本情報 ４．特定個人情報ファイルを取り扱う理由 ①実現が期待されるメリット	・個人番号を利用することにより被保険者資格や給付の情報等をより正確かつ効率的に検索・照会することが可能となり、誤った相手に対して保険料の賦課・徴収や給付等を行うリスクを軽減できる。また、現状で情報の連携のために使用されている宛名番号等は市区町村ごとに設定されているものであるが、個人番号は全国の市区町村で共通の番号であるため、同一広域連合内において他の市区町村に転居した場合でも、個人番号を利用することで同一人の正確な名寄せが可能となり、誤支給や誤賦課の防止がより確実なものとなる。	・個人番号を利用することにより被保険者資格や給付の情報等をより正確かつ効率的に検索・照会することが可能となり、誤った相手に対して保険料の賦課・徴収や給付等を行うリスクを軽減できる。また、現状で情報の連携のために使用されている宛名番号等は市区町村ごとに設定されているものであるが、個人番号は全国の市区町村で共通の番号であるため、同一広域連合内において他の市区町村に転居した場合でも、個人番号を利用することで同一人の正確な名寄せが可能となり、誤支給や誤賦課の防止がより確実なものとなる。 ・個人番号を用いることで申請・届出の手間や行政手続きを省略化し、市民の利便性の向上につながる。
P7	4	Ⅰ　基本情報 ６．情報提供ネットワークシステムによる情報連携 ①実施の有無	実施しない	実施する
P7	5	Ⅰ　基本情報 ６．情報提供ネットワークシステムによる情報連携 ②法令上の根拠	記載なし	・番号法第19条第８号及び別表第二の第82の項 ・番号法別表第二の主務省令で定める事務を定める命令第43条の2の2
P8	6	Ⅰ　基本情報 （別添１）事務内容 業務全体図	記載なし	情報提供ネットワークシステム接続について図示
P11	7	Ⅰ　基本情報 （別添１）事務内容 （２）保険料収納管理	記載なし	5-⑥から5-⑧について図示 （備考） 5-⑥被保険者より公金受取口座を活用した還付金の請求を受ける。 5-⑦還付申請書をもとに情報連携（マイナンバー照会→公金受取口座情報取得）を行う。 5-⑧公金受取口座情報を業務システムに入力する。

後期高齢者医療に関する事務に係る特定個人情報保護評価書（全項目評価書）の変更箇所一覧

該当ページ	番号	項目	変更前の記載	変更後の記載
P12	8	Ⅱ　特定個人情報ファイルの概要 2．基本情報 ④記録される項目	記載なし	・主な記録項目 その他（公金受取口座登録・連携ファイル関係情報） ・その妥当性 ○公金受取口座情報（口座登録・連携ファイル関係情報）：後期高齢者医療保険料の還付金に係る還付口座を把握するもの。
P13	9	Ⅱ　特定個人情報ファイルの概要 3．特定個人情報の入手・使用 ①入手元	行政機関・独立行政法人等（年金保険者）	行政機関・独立行政法人等（年金保険者、デジタル庁）
P13	10	Ⅱ　特定個人情報ファイルの概要 3．特定個人情報の入手・使用 ②入手方法	記載なし	情報提供ネットワークシステムを追加
P14	11	Ⅱ　特定個人情報ファイルの概要 3．特定個人情報の入手・使用 ③入手の時期・頻度	記載なし	4 情報提供ネットワークシステムからの入手 ○後期高齢者医療保険料の還付を受ける者に係る公的給付支給等口座登録簿関係情報について，必要に応じて随時連携する。
P15	12	Ⅱ　特定個人情報ファイルの概要 3．特定個人情報の入手・使用 ④入手に係る妥当性	記載なし	4 情報提供ネットワークシステムからの入手 (1)入手に係る根拠 ○番号法別表第二の82の項及び番号法別表第二の主務省令で定める事務及び情報を定める命令第43条の２の２において、内閣総理大臣に対し公的給付支給等口座登録簿関係情報の提供を求めることができる旨の規定がある。 (2)入手の時期・頻度の妥当性 ○保険料還付の公的給付等登録口座情報の入手に必要な範囲内で、情報提供ネットワークシステムを介し情報収集を適宜行う必要がある。 (3)入手方法の妥当性 ○情報は行政機関専用回線（LGWAN）を介して安全に連携することが期待できる。
P16	13	Ⅱ　特定個人情報ファイルの概要 3．特定個人情報の入手・使用 ⑧使用方法	(2)保険料収納 記載なし	(2)保険料収納 ・保険料の還付が発生した場合において、被保険者の申請がある場合に限り、情報提供ネットワークシステムを介して公的給付支給等口座登録簿関係情報を連携し、福岡市の後期高齢者医療システム内に登録し、還付の支給を行う。

後期高齢者医療に関する事務に係る特定個人情報保護評価書（全項目評価書）の変更箇所一覧

該当ページ	番号	項目	変更前の記載	変更後の記載
P21	14	Ⅱ　特定個人情報ファイルの概要 6．特定個人情報の保管・消去 ①保管場所	記載なし	＜統合宛名システムにおける措置＞ ①統合宛名システムのサーバはデータセンターに設置しており、データセンターへの入館及びサーバー室への入室を厳重に管理する。 ②特定個人情報は、当該サーバのデータベース内に保存されている。 ③サーバへのアクセスは、ユーザアカウントおよびパスワードによる認証が必要である。 ＜中間サーバ・プラットフォームにおける措置＞ ①中間サーバ･プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバー室への入室を厳重に管理する。 ②特定個人情報は、サーバー室に設置された中間サーバのデータベース内に保存され、バックアップもデータベース上に保存される。
P21	15	Ⅱ　特定個人情報ファイルの概要 6．特定個人情報の保管・消去 ①消去方法	記載なし	＜統合宛名システムにおける措置＞ ①統合宛名システムに格納する特定個人情報は、各業務システムの副本データであるため、消去のタイミングは各業務システムの運用に準ずる。 ②ディスク交換やハード更改等の際は、統合宛名システムの保守・運用を行う事業者において、保存された情報が読み出しできできないよう、物理的破壊もしくは、専用ソフトを利用して完全に消去する。 ＜中間サーバ・プラットフォームにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバ・プラットフォームの保守・運用を行う事業者が特定個人情報を消去することはない。 ②ディスク交換やハード更改等の際は、中間サーバ・プラットフォームの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊により完全に消去する。
P25	16	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3．特定個人情報の使用	―	統合宛名システムを利用するには、職員証及びＵＳＢトークンを利用した、二要素による認証機能を設けており、権限を保持しない者は接続できないようになっている。 権限は、番号法に定められた利用事務の所管課の業務担当職員のみに付与され、また、情報を利用する事務と事務に必要な情報項目の対応付けをあらかじめ統合宛名システム上で設定することで、事務に必要のない情報 への接続もできないよう制限している。

後期高齢者医療に関する事務に係る特定個人情報保護評価書（全項目評価書）の変更箇所一覧

該当ページ	番号	項目	変更前の記載	変更後の記載
P30	17	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ６．情報提供ネットワークシステムとの接続	【○】接続しない（入手） 【○】接続しない（提供）	【　】接続しない（入手） 【○】接続しない（提供）
P30	18	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ６．情報提供ネットワークシステムとの接続 リスク１：目的外の入手が行われるリスク リスクに対する措置の内容	記載なし	＜統合宛名システムにおける措置＞ ①各業務システムから中間サーバあての情報照会要求の中継においては、照会元・照会先・照会内容等の改変は行わないことで、中間サーバにおける目的外入手抑止の措置に従うことを担保している。 ②接続システムの認証及び統合宛名システム接続端末での職員認証等の機能を設けており、あらかじめ承認されたシステム・職員以外の情報入手を抑止している。 ③番号法に定められている事務以外での情報照会ができないようアクセス制限を設けている。 ＜中間サーバ・ソフトウェアにおける措置＞ ①情報照会機能（※１）により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リスト（※２）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ②中間サーバの職員認証・権限管理機能（※３）では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※１）情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。 （※２）番号法別表第２及び第１９条第１４号に基づき、事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。 （※３）中間サーバを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。
P30	19	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ６．情報提供ネットワークシステムとの接続 リスク１：目的外の入手が行われるリスク リスクへの対策は十分か	記載なし	十分である

後期高齢者医療に関する事務に係る特定個人情報保護評価書（全項目評価書）の変更箇所一覧

該当ページ	番号	項目	変更前の記載	変更後の記載
P30	20	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ６．情報提供ネットワークシステムとの接続 リスク２：安全が保たれない方法によって入手が行われるリスク リスクに対する措置の内容	記載なし	＜統合宛名システムにおける措置＞ ①中間サーバと統合宛名システム間の接続は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）が利用され、また、VPN等の技術も利用されている。このように、福岡市の中間サーバと統合宛名システム間の通信回線を他団体の通信と分離するとともに、通信を暗号化することで安全性を確保している。 ②統合宛名システムは、外部インターネットと接続されている情報系ネットワークとは分離されている、業務系ネットワークに設置することで、通信の安全性を確保している。 ＜中間サーバ・ソフトウェアにおける措置＞ ①中間サーバは、個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。 ＜中間サーバ･プラットフォームにおける措置＞ ①中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。
P30	21	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ６．情報提供ネットワークシステムとの接続 リスク２：安全が保たれない方法によって入手が行われるリスク リスクへの対策は十分か	記載なし	十分である

後期高齢者医療に関する事務に係る特定個人情報保護評価書（全項目評価書）の変更箇所一覧

該当ページ	番号	項目	変更前の記載	変更後の記載
P31	22	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク３：入手した特定個人情報が不正確であるリスク リスクに対する措置の内容	記載なし	＜統合宛名システムにおける措置＞ ①統合宛名システムは、照会対象者に付番された正しい個人番号に基づき、団体内統合宛名番号を付番してインタフェースシステムより処理通番等を入手した上で、情報提供用個人識別符号の取得依頼ができるよう設計される。これにより、照会対象者の個人番号に基づき正確に情報提供用個人識別符号の紐付けが行われることから、正確な照会対象者に係る特定個人情報を入手することが担保されている。 ②統合宛名システム上の宛名情報・業務情報は副本であり、また、中間サーバから各業務システムあての情報照会結果の中継においては、照会結果内容の改変は行わない。これにより、各業務システムが入手する照会結果内容が中間サーバから入手した内容と同一であることを担保している。 ＜中間サーバ・ソフトウェアにおける措置＞ ①中間サーバは、個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。
P31	23	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク３：入手した特定個人情報が不正確であるリスク リスクへの対策は十分か	記載なし	十分である

後期高齢者医療に関する事務に係る特定個人情報保護評価書（全項目評価書）の変更箇所一覧

該当ページ	番号	項目	変更前の記載	変更後の記載
P31	24	情報提供ネットワークシステムとの接続リスク４：入手の際に	記載なし	＜統合宛名システムにおける措置＞ ①接続システムの認証及び統合宛名システム接続端末での職員証及びＵＳＢトークンを利用した、二要素による認証機能を設けており、あらかじめ承認されたシステム・職員以外の情報入手を防止している。 ②番号法に定められている事務以外での情報照会ができないようアクセス制限を設けている。 ③中間サーバと統合宛名システム間の接続は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）が利用され、また、VPN等の技術も利用されている。このように、福岡市の中間サーバと統合宛名システム間の通信回線を他団体の通信と分離するとともに、通信を暗号化することで安全性を確保している。 ④統合宛名システムは、外部インターネットと接続されている情報系ネットワークとは分離されている、業務系ネットワークに設置することで、通信の安全性を担保している。 ⑤操作内容の追跡調査機能が設けられており、不適切な端末操作や情報照会などを抑止する仕組みになっている。 ＜中間サーバ・ソフトウェアにおける措置＞ ①中間サーバは、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ②既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ③情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において自動で削除することにより、特定個人

後期高齢者医療に関する事務に係る特定個人情報保護評価書（全項目評価書）の変更箇所一覧

該当ページ	番号	項目	変更前の記載	変更後の記載
				情報が漏えい・紛失するリスクを軽減している。 ④中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）中間サーバは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ＜中間サーバ･プラットフォームにおける措置＞ ①中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、漏えい･紛失のリスクに対応している。 ②中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい･紛失のリスクに対応している。 ③中間サーバ･プラットフォーム事業者の業務は、中間サーバ・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはできない。
P31	25	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク４：入手の際に特定個人情報が漏えい・紛失するリスク リスクへの対策は十分か	記載なし	十分である

後期高齢者医療に関する事務に係る特定個人情報保護評価書（全項目評価書）の変更箇所一覧

該当ページ	番号	項目	変更前の記載	変更後の記載
P32	26	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	記載なし	＜本市における措置＞ 情報提供ネットワークシステムとの全ての連携（接続）は、中間サーバが行う構成となっており、情報提供ネットワークシステムは、統合宛名システムや業務システムは直接接続はできない。 ＜中間サーバ・ソフトウェアにおける措置＞ ①中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバ･プラットフォームにおける措置＞ ①中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバ・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバ・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバ・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。
P32	27	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7．特定個人情報の保管・消去 ⑤物理的対策 　具体的な対策の内容	記載なし	＜中間サーバ･プラットフォームにおける措置＞ ①中間サーバ･プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。

後期高齢者医療に関する事務に係る特定個人情報保護評価書（全項目評価書）の変更箇所一覧

該当ページ	番号	項目	変更前の記載	変更後の記載
P33	28	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7．特定個人情報の保管・消去 ⑥技術的対策 　具体的な対策の内容	＜中間サーバ･プラットフォームにおける措置＞ ①中間サーバ・プラットフォームをデータセンターに構築し、設置場所への入退室管理、友人監視および施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。	＜統合宛名システムにおける措置＞ ・サーバにはウイルス対策ソフトを導入し、ウイルスチェックを実施する。ウイルスパターンファイルは定期的に更新し、最新のものを使用する。 ・導入しているＯＳ及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ・外部インターネットと接続する情報系ネットワークと分離された業務系ネットワークに設置しており、外部ネットワークからの不正アクセスを防止する。 ・内部者によるデータへの不正アクセスを防止するため、サーバ上のデータ保管フォルダに対してアクセス制限を行う。 ＜中間サーバ･プラットフォームにおける措置＞ ①中間サーバ・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ②中間サーバ・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ③導入しているＯＳ及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。
P35	29	Ⅳその他のリスク対策 1．監査 ①自己点検 　具体的なチェック方法	記載なし	＜中間サーバ･プラットフォームにおける措置＞ ・運用規則等に基づき、中間サーバ･プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。
P35	30	Ⅳその他のリスク対策 1．監査 ①監査 　具体的な内容	記載なし	＜中間サーバ･プラットフォームにおける措置＞ ・運用規則等に基づき、中間サーバ・プラットフォームについて、定期的に監査を行うこととしている。

後期高齢者医療に関する事務に係る特定個人情報保護評価書（全項目評価書）の変更箇所一覧

該当ページ	番号	項目	変更前の記載	変更後の記載
P35	31	Ⅳその他のリスク対策 ２．従業者に対する教育・啓発	＜本市における措置＞ (1)研修について ・全職員を対象とした情報セキュリティ研修を毎年度実施し、個人情報の取扱いを含めた情報セキュリティに関する基礎的な知識の習得及び情報セキュリティに対する意識の向上を図っている。 ・情報セキュリティ及び個人情報の取扱いについて、新規採用職員を対象とした研修、情報セキュリティ責任者及び担当課個人情報保護責任者（課長）を対象とした研修等、それぞれの役割に応じた特別研修を毎年度実施している。 ・Ｊ-LISのｅラーニングやCYDER等の外部の研修受講を広く募集し、毎年度活用している。 (2)情報セキュリティに係る各種周知について ・情報セキュリティポータルや情報セキュリティニュース、注意喚起等により、情報セキュリティポリシー等各規程の内容や情報セキュリティに関する様々な情報を積極的に周知し、情報セキュリティについての職員の意識向上を図っている。 ・個人情報の適切な取り扱いや情報セキュリティポリシー等に基づき遵守すべき事項について関係課と連携して通知する等、情報セキュリティ及び個人情報の取扱いに関して継続的に周知を行っている。	＜本市における措置＞ (1)情報セキュリティ研修について ・全職員を対象として情報セキュリティ研修を毎年度実施し、個人情報の取扱いを含めた情報セキュリティに関する基礎的な知識の習得及び情報セキュリティに対する意識の向上を図っている。 ・新規採用職員を対象とした研修、情報セキュリティ責任者（課長）を対象とした研修等、それぞれの役割に応じた特別研修を毎年度実施している。 ・J-LISのeラーニングやCYDER等の外部の研修受講を広く募集し、毎年度活用している。 (2)情報セキュリティに係る各種周知について ・情報セキュリティポータルや情報セキュリティニュース、注意喚起等により、情報セキュリティポリシー等各規程の内容や情報セキュリティに関する様々な情報を積極的に周知し、職員の意識向上を図っている。 ・個人情報の適切な取り扱いや情報セキュリティポリシー等に基づき遵守すべき事項について情報公開室等と連携して通知する等、情報セキュリティに関して継続的に周知を行っている。 ＜中間サーバ･プラットフォームにおける措置＞ ・中間サーバ･プラットフォームの運用に携わる職員及び事業者に対し、セキュリティ研修等を実施することとしている。 ・中間サーバ･プラットフォームの業務に就く場合は、運用規則等について研修を行うこととしている。
P35	32	Ⅳその他のリスク対策 ３．その他のリスク対策	―	＜中間サーバ･プラットフォームにおける措置＞ ・中間サーバ・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。