〇変更箇所

全項目評価書の項目	変更前の記載	変更後の記載
Ⅱ．６．③ （連携用符号発行管理ファイル）	ディスクの論理的消去が終了して搬出が許可されるまで、現行システムのデータセンター内にて機器を保持する。電源をオフするまでは運用中と同様のアクセス制限を実施する。データセンターへの入館、マシンルームの入室に関する手続は継続して行う。	ディスクの物理破壊が終了して搬出が許可されるまで、現行システムのデータセンター内にて機器を保持する。電源をオフするまでは運用中と同様のアクセス制限を実施する。データセンターへの入館、マシンルームの入室に関する手続は継続して行う。
Ⅱ．６．③ （情報提供等記録ファイル）	ディスクの論理的消去が終了して搬出が許可されるまで、現行システムのデータセンター内にて機器を保持する。電源をオフするまでは運用中と同様のアクセス制限を実施する。データセンターへの入館、マシンルームの入室に関する手続は継続して行う。	ディスクの物理破壊が終了して搬出が許可されるまで、現行システムのデータセンター内にて機器を保持する。電源をオフするまでは運用中と同様のアクセス制限を実施する。データセンターへの入館、マシンルームの入室に関する手続は継続して行う。
Ⅱ．６．③ （連携用符号発行管理ファイル）	データの破棄に当たっては、データを復元できないよう論理的消去を行うとともに、消去完了の証跡の提示により確実な履行を担保する。	データ消去に当たっては、同値性確認を行って確実に必要なデータ移行を実施した後、データの破棄を行う。また、データの破棄は、データを復元できないよう、記憶装置に対し論理的消去処理を行った上で、当該装置の物理破壊の措置を講じるとともに、消去完了の証跡の提示により確実な履行を担保する。
Ⅱ．６．③ （情報提供等記録ファイル）	データの破棄に当たっては、データを復元できないよう論理的消去を行うとともに、消去完了の証跡の提示により確実な履行を担保する。	データ消去に当たっては、同値性確認を行って確実に必要なデータ移行を実施した後、データの破棄を行う。また、データの破棄は、データを復元できないよう、記憶装置に対し論理的消去処理を行った上で、当該装置の物理破壊の措置を講じるとともに、消去完了の証跡の提示により確実な履行を担保する。
Ⅲ．３．リスク４に対する措置の内容 （連携用符号発行管理ファイル）	データ移行時において、作業者等によるデータの詐取や外部へのデータ漏えいの予防のために、第二期システムにおいてはログ情報等の統合分析・監査を行うシステム（SIEM）、第三期システムにおいてはガバメントクラウド環境のデータ分析・可視化サービス(SIEM)を用いて、作業ログ、ファイル、フォルダ、NWのアクセス状況を監視（モニタリング）・分析し、移行元・移行先双方での不正の兆候や不正アクセスの検知を行う。	データ移行時において、作業者等によるデータの詐取や外部へのデータ漏えいの予防のために、第二期システムにおいてはログ情報等の統合分析・監査を行うシステム（SIEM）、第三期システムにおいてはガバメントクラウド環境のデータ分析・可視化サービス(SIEM)を用いて、各種ログによる監査及びファイル、フォルダ、NWのアクセス状況の監視（モニタリング）・分析を行い、移行元・移行先双方での不正の兆候や不正アクセスの検知を行う。
Ⅲ．３．リスク４に対する措置の内容 （情報提供等記録ファイル）	データ移行時において、作業者等によるデータの詐取や外部へのデータ漏えいの予防のために、第二期システムにおいてはログ情報等の統合分析・監査を行うシステム（SIEM）、第三期システムにおいてはガバメントクラウド環境のデータ分析・可視化サービス(SIEM)を用いて、作業ログ、ファイル、フォルダ、NWのアクセス状況を監視（モニタリング）・分析し、移行元・移行先双方での不正の兆候や不正アクセスの検知を行う。	データ移行時において、作業者等によるデータの詐取や外部へのデータ漏えいの予防のために、第二期システムにおいてはログ情報等の統合分析・監査を行うシステム（SIEM）、第三期システムにおいてはガバメントクラウド環境のデータ分析・可視化サービス(SIEM)を用いて、各種ログによる監査及びファイル、フォルダ、NWのアクセス状況の監視（モニタリング）・分析を行い、移行元・移行先双方での不正の兆候や不正アクセスの検知を行う。
Ⅲ．７．リスク１．⑨ （情報提供等記録ファイル）	―	（「連携用符号発行管理ファイル」の当該項目において記載済みの内容を再度記載）
Ⅳ．１．①	― (右記を追記)	また、セキュリティ対策として不正なアクセスがないこと等、定常又は定期的に監査を実施している。