別紙4

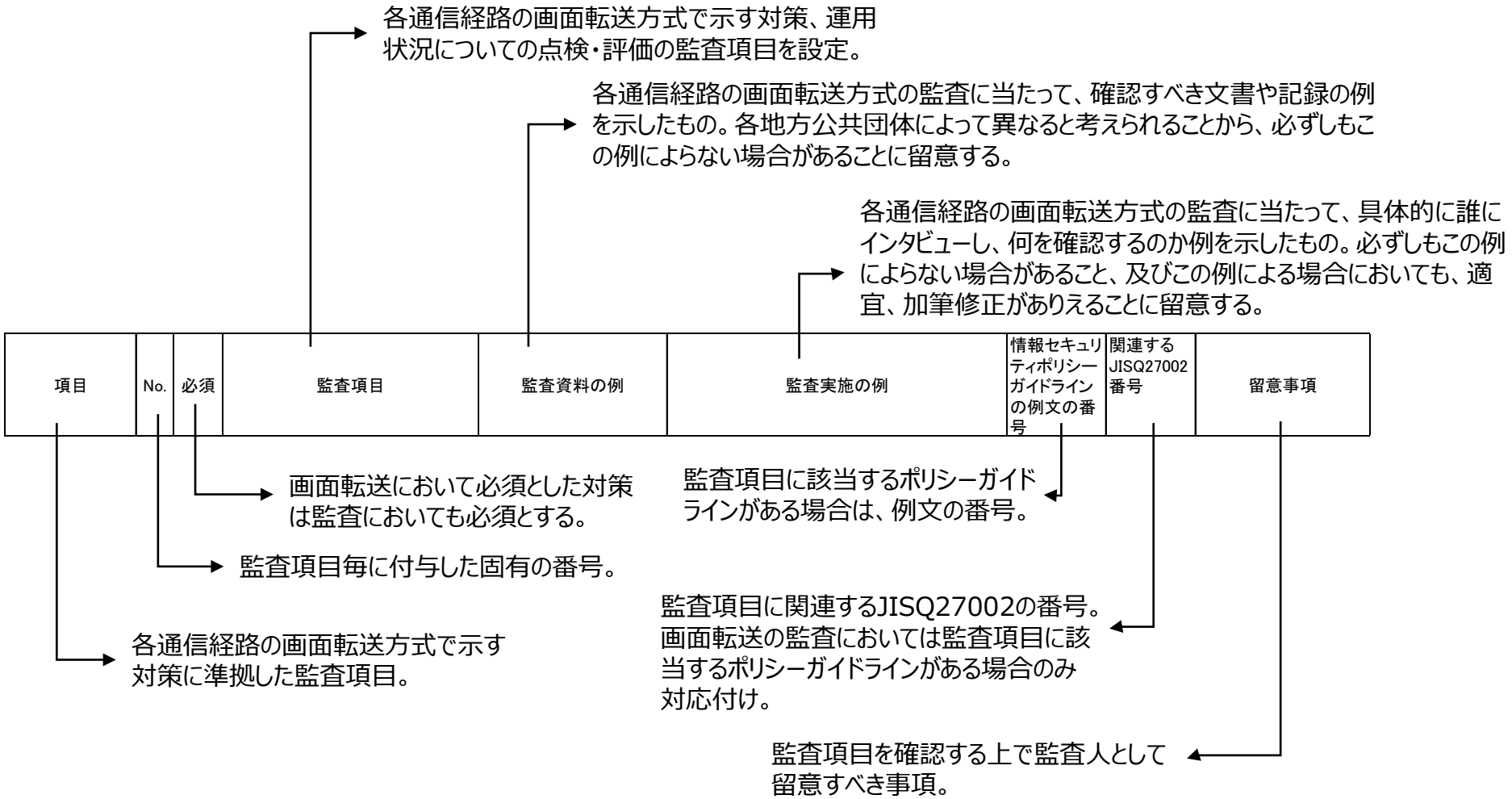
参考資料 「マイナンバー利用事務系に係る画面転送の方式」監査項目（案）

総 務 省

令和７年3月●日

目 次

はじめに



監査項目の趣旨や運用上の留意点を理解するため、総務省の令和７年3月の「地方公共団体における情報セキュリティポリシーに関するガイドライン」別紙「マイナンバー利用事務系に係る画面転送の方式について」を併せて確認されたい。

監査項目

全パターン共通の監査項目

共通対策の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
全パターン共通の対策	組織的・人的対策 手続・規定	1	○	**ⅰ）手続・規定** 統括情報セキュリティ責任者及び情報システム管理者により、クラウドサービス(DaaS)を利用開始する場合の申請、承認等に係る規定を整備するとともに、運用を徹底していることを確認する。	□情報セキュリティポリシー □職員等への周知記録	監査資料のレビューと職員等へのインタビューにより、情報セキュリティポリシーが遵守されているか確かめる。	ー	ー	
	組織的・人的対策 組織・人的な対応	2	○	**ⅰ）情報セキュリティ研修・訓練の実施** CISOによって、職員等が毎年度最低1回は情報セキュリティ研修を受講可能となる研修計画の策定している。	□研修・訓練実施基準 □研修実施報告書 □訓練実施報告書	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、定期的に情報セキュリティに関する研修・訓練が実施されているか確かめる。	5.2.(1)	6.3	
		3	○	**ⅰ）情報セキュリティ研修・訓練の実施** CISOによって、職員等が毎年度最低1回は情報セキュリティ研修を受講可能となる研修計画の策定している。			ー	ー	
		4	○	**ⅱ）緊急時対応訓練の実施** CISOによって、演習等を通じたサイバー攻撃情報やインシデント等への対策情報を共有している。	□研修・訓練実施基準 □訓練実施報告書	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、緊急時対応を想定した訓練計画が定期的かつ効果的に実施されているか確かめる。	5.2.(3)	6.3	
		5	○	**ⅲ）情報セキュリティポリシーの見直し** 情報セキュリティの監査及び自己点検の結果並びに内部及び外部の環境の変化から、定期的又は必要に応じて情報セキュリティポリシーを見直す。	□情報セキュリティ委員会議事録 □情報セキュリティポリシー	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、監査結果が情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直しに活用されているか確かめる。	9.1.(8)	5.1	

共通対策の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
全パターン共通の対策	組織的・人的対策 事務取扱担当者の明確化	6	○	**ⅰ）正規利用者の管理・不正アクセスの防止** 統括情報セキュリティ責任者によって、事務取扱担当者のリスト化を行う。	□事務取扱担当者一覧	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、特定個人情報等を取り扱う職員（以下「事務取扱担当者」という。）をリスト化し、マイナンバー利用事務系への画面転送システムの利用を許可する者を明確化しているか確かめる。	ー	ー	
	物理的対策 特定個人情報等を取り扱う区域の管理	7	○	**ⅰ）事務取扱担当者の端末の保護** 統括情報セキュリティ責任者及び情報システム管理者によって、以下を行う。 ・事務取扱担当者の端末は執務エリア（特定個人情報を取り扱う事務を行う区域であり、支所を含む）から原則持ち出しをしない運用ルールの徹底 ・事務取扱担当者の端末にはのぞき見防止フィルターを装着する運用ルールの徹底	□運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、事務取扱担当者の端末は執務エリア（特定個人情報を取り扱う事務を行う区域であり、支所を含む）から原則持ち出しをしない運用ルール化を行っているか確かめる。	ー	ー	
		8	○	**ⅱ）入退室管理** 統括情報セキュリティ責任者及び情報システム管理者によって、事務取扱担当者（特定個人情報等を取り扱う職員）の庁内の執務エリア（部署単位）をまとめ、執務室を分ける、パーティションの設置等、特定個人情報が他部門に見えないよう分離する。	□フロアレイアウト	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、事務取扱担当者の庁内の執務エリア（部署単位）をまとめ、執務室を分ける、パーティションの設置等、特定個人情報が他部門に見えないよう分離を行っているか確かめる。	6.1.(13)		

共通対策の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
全パターン共通の対策	物理的対策 特定個人情報等を取り扱う区域の管理	9	○	**ⅲ）情報システム室等の管理** 統括情報セキュリティ責任者及び情報システム管理者によって、以下を行う。 ・画面転送システム及び画面転送システムや無線LANにアクセス時の認証システム等を施錠やクラウドサービスなどの管理区域に設置し、第3者からの物理的アクセスからの保護 ・無線LAN APを手が届かない場所に設置し、第3者からの物理的アクセスからの保護	□フロアレイアウト	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、無線LANアクセス時の認証システムや、無線LANのアクセスポイントは、第3者の手が届かない場所に設置していることを確かめる。	6.1.(13)		
		10	○	**ⅳ）特権IDの管理** 統括情報セキュリティ責任者及び情報システム管理者によって、画面転送システムの特権IDを適正に管理する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、画面転送システムの特権IDを適正に監理していることを確かめかる。	6.1.(13)		
		11	○	**ⅴ）電子媒体等の取扱いにおける漏えい等の防止** 統括情報セキュリティ責任者及び情報システム管理者によって、原則、USBメモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定する。	□情報セキュリティポリシー □利用状況調査基準	監査資料のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、USBメモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しているか確かめる。	7.2.(2)	8.15	

共通対策の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
全パターン共通の対策	保守端末の対策	12	○	**ⅰ)接続先制限** 統括情報セキュリティ責任者及び情報システム管理者によって、保守端末の管理先以外へのインターネット接続を制限する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、保守端末は管理先以外へのインターネット接続を制限するしていることを確かめかる。	ー	ー	
		13	○	**ⅱ)マルウェア対策ソフト** 統括情報セキュリティ責任者及び情報システム管理者によって、パターンマッチング方式やヒューリスティック方式（不審な動作を行うコードが含まれていることを検出する振る舞い検知方式）などによる不正プログラム対策を行う。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、保守端末はマルウェア対策ソフトにより不正プログラム対策を行うことを確かめかる。	ー	ー	
		14	○	**ⅲ）パッチ適用** 統括情報セキュリティ責任者及び情報システム管理者によって、脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、保守端末は脆弱性を修正するパッチを速やかに適用し、脆弱性を解消を行うことを確かめかる。	ー	ー	
		15	○	**ⅳ）管理者権限管理** 統括情報セキュリティ責任者及び情報システム管理者によって、不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切な管理を行っていることを確かめかる。	ー	ー	

共通対策の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
全パターン共通の対策	保守端末の対策	16	○	**v)権限に基づくアクセス制御** 統括情報セキュリティ責任者及び情報システム管理者によって、権限に応じたアクセス制御を行う。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、保守者の権限に応じたアクセス制御を行っていることを確かめかる。	ー	ー	
		17	○	**vi)多要素によるユーザ認証** 統括情報セキュリティ責任者及び情報システム管理者によって、保守担当者について多要素認証を行う(「知識」「所持情報」「生体情報」のうち、2つ以上の異なる要素を使って認証)。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、保守担当者について多要素認証を行うことを確かめかる。	ー	ー	
		18	○	**vii)アクセスログ** 統括情報セキュリティ責任者及び情報システム管理者によって、管理先へのアクセスに係るログを記録する。	□システム運用基準 □ログ	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、管理先へのアクセスに係るログを記録していることを確かめる。	ー	ー	
		19	○	**viii)操作ログ** 統括情報セキュリティ責任者及び情報システム管理者によって、保守作業の操作ログを記録する。	□システム運用基準 □ログ	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、保守作業の操作ログを記録していることを確かめる。	ー	ー	
		20	○	**ix)保守端末の管理** 統括情報セキュリティ責任者及び情報システム管理者によって、保守は、業務端末とは分けた専用の保守端末で実施する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、保守は、業務端末とは分けた専用の保守端末で実施することが文書化され、正式に承認されているか確かめかる。	ー	ー	

共通対策の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
全パターン共通の対策	技術的対策	21	○	**ⅰ)通信経路に係る対策** 統括情報セキュリティ責任者及び情報システム管理者によって、画面転送に係る全ての通信経路で暗号化を行う。	□ネットワーク管理基準 □ネットワーク設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、画面転送に係る全ての通信経路で暗号化を行うことを確かめかる。	ー	ー	
		22	○	**ⅱ)仮想環境の運用に関する対策** クリップボード、プリンター、ディスクドライブ等の仮想端末と画面転送で接続する手元の端末のデバイス、リソースを双方向共に利用を禁止する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末と画面転送で接続する手元の端末のデバイス、リソースを双方向共に利用を禁止することを確かめかる。	ー	ー	
		23	○	**ⅲ)仮想機能のログオフ** 画面転送システムの仮想機能は、利用後に仮想機能を第3者に悪用されることを防ぐため、手元の端末で仮想画面を閉じた際は、仮想機能もログオフする。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、手元の端末で仮想画面を閉じた際は、仮想機能もログオフすることを確かめかる。	ー	ー	

各パターンにおける監査項目

通信経路パターン

✓ 下記の通り10パターンの通信経路についての監査項目を示す。

	接続元 (業務端末の設置場所)	画面転送の方式	ページ
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合	P13
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合	P19
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合	P26
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する	P32
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合	P38
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する	P45
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC）	P51
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）	P57
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ	P63
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ	P69

通信経路 (1) LGWAN接続系端末に１台化　DaaS利用
監査項目

通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

通信経路 (1)LGWAN接続系端末に１台化　DaaS利用(異なるCSP) の監査項目

✓LGWAN接続系端末からDaaS利用時の監査項目を示す。
✓本画面転送はα'モデルの対策を実施することが前提であるため、α'モデルの監査も実施すること。

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(1)の対策	クラウドサービス(DaaS)上での対策	1	○	**ⅰ）画面転送機能** 仮想端末と画面転送の分離対策にて、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えないDaaSを選定する。 DaaSはISMAPに登録するサービスを選定する。	□クラウドサービス事業者選定基準 □クラウドサービスの仕様書/基本契約書及び利用規約	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、ISMAPに登録するDaaSサービスを選定し、DaaSサービスは仮想端末を画面転送するという分離対策にて、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えないか確かめる。	ー	ー	
		2	○	**ⅱ）多要素によるユーザ認証** 統括情報セキュリティ責任者及び情報システム管理者によって、DaaSのユーザや特権管理者について多要素認証を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザや特権管理者について多要素認証を行うことを確かめかる。	ー	ー	
		3	○	**ⅲ）管理者権限管理** 統括情報セキュリティ責任者及び情報システム管理者によって、不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切な管理を行っていることを確かめかる。	ー	ー	
		4	○	**ⅳ）権限に基づくアクセス制御** 統括情報セキュリティ責任者及び情報システム管理者によって、権限に応じたアクセス制御を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、保守者の権限に応じたアクセス制御を行っていることを確かめかる。	ー	ー	
		5	○	**ⅴ）仮想端末でのパッチ適用** 統括情報セキュリティ責任者及び情報システム管理者によって、仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消することを確かめかる。	ー	ー	

通信経路 (1)LGWAN接続系端末に１台化　DaaS利用(異なるCSP) の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(1)の対策	クラウドサービス(DaaS)上での対策	6	○	**vi）仮想端末でのマルウェア対策ソフト** 統括情報セキュリティ責任者及び情報システム管理者によって、仮想端末でパターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末でマルウェア対策ソフトにより不正プログラム対策を行っていることを確かめかる。	ー	ー	
		7	○	**vii）接続先制限** 統括情報セキュリティ責任者及び情報システム管理者によってLGWAN接続系端末のIPアドレス、画面転送で使用する通信ポートのみにアクセスを制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末とLGWAN接続系端末間にIPアドレス、画面転送で使用する通信ポートでアクセスを制限を行っていることを確かめかる。	ー	ー	
		8	○	**viii)DaaS基盤の脆弱性対応** DaaS基盤の脆弱性へのパッチの適用は、DaaS事業者にて実施するDaaSを選定する。	□クラウドサービスの仕様書/基本契約書及び利用規約	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、DaaS基盤の脆弱性へのパッチの適用は、DaaS事業者にて実施するDaaSを選定していることを確かめる。	ー	ー	
		9	○	**ix)アクセスログ** 統括情報セキュリティ責任者及び情報システム管理者によって、DaaSのアクセスログを取得し、確認する。	□システム運用基準 □ログ	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、DaaSのアクセスログを取得し、確認していることを確かめる。	ー	ー	

通信経路 (1)LGWAN接続系端末に１台化　DaaS利用(異なるCSP) の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(1)の対策	LGWAN接続系での対策（α‘モデルの対策以外のもの）	10	○	**ⅰ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		11	○	**ⅱ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、接続元（インターネット接続系DaaS）と接続先（インターネット、インターネット接続系のメールサーバ）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、接続元（インターネット接続系DaaS）と接続先（インターネット、インターネット接続系のメールサーバ）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		12	○	**ⅲ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、インターネット接続系からマイナンバー利用事務系への通信を遮断する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、インターネット接続系からマイナンバー利用事務系への通信を遮断していることを確かめかる。	ー	ー	

通信経路 (1)LGWAN接続系端末に１台化　DaaS利用(異なるCSP) の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(1)の対策	LGWAN接続系での対策（α'モデルの対策以外のもの）	13		**ⅳ）アプリケーションの制限** 統括情報セキュリティ責任者及び情報システム管理者によって、LGWAN接続系端末でのスクリーンショット機能を停止する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、LGWAN接続系端末でのスクリーンショット機能を停止していることを確かめかる。	ー	ー	
		14	○	**ⅴ）未知の不正プログラム対策（エンドポイント対策）** 統括情報セキュリティ責任者及び情報システム管理者により、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、以下の対応が全て実施されている。 ・端末等のエンドポイントにおけるソフトウェア等の動作を監視し、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）を示す異常な挙動を監視・検出・特定する。 ・異常な挙動を検出した際にプロセスを停止、ネットワークからの論理的な隔離を行う。 ・インシデント発生時に発生要因の詳細な調査を実施する。	□システム設計書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、端末等のエンドポイントにおけるソフトウェア等の動作の監視がされていること、未知及び既知のマルウェア等の異常な挙動を監視・検知・特定ができるようになっていること並びに異常な挙動を検出した際のプロセスの停止、異常な挙動が検知された端末等に対してネットワークからの隔離ができるようになっていること及びインシデント発生要因の詳細な調査が実施できるようになっていることを確かめる。	ー	ー	

通信経路（２） LGWAN接続系端末に１台化　DaaS利用
監査項目

通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

通信経路 (2)LGWAN接続系端末に１台化 DaaS利用 ガバメントクラウド/DaaS(同一CSP)の監査項目

✓LGWAN接続系端末からDaaS利用時の監査項目を示す。
✓本画面転送はα'モデルの対策を実施することが前提であるため、α'モデルの監査も実施すること。

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(2)の対策	クラウドサービス(DaaS)上での対策	1	○	**ⅰ)画面転送機能** 仮想端末と画面転送の分離対策にて、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えないDaaSを選定する。 DaaSはISMAPに登録するサービスを選定する。	□クラウドサービス事業者選定基準 □クラウドサービスの仕様書/基本契約書及び利用規約	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、ISMAPに登録するDaaSサービスを選定し、DaaSサービスは仮想端末を画面転送するという分離対策にて、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えないか確かめる。	ー	ー	
		2	○	**ⅱ)多要素によるユーザ認証** 統括情報セキュリティ責任者及び情報システム管理者によって、DaaSのユーザや特権管理者について多要素認証を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザや特権管理者について多要素認証を行うことを確かめかる。	ー	ー	
		3	○	**ⅲ)管理者権限管理** 統括情報セキュリティ責任者及び情報システム管理者によって、不正行為(例:無許可の重要コマンド発行や重要データ読み書き)を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切な管理を行っていることを確かめかる。	ー	ー	
		4	○	**ⅳ)権限に基づくアクセス制御** 統括情報セキュリティ責任者及び情報システム管理者によって、権限に応じたアクセス制御を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、保守者の権限に応じたアクセス制御を行っていることを確かめかる。	ー	ー	
		5	○	**ⅴ)仮想端末でのパッチ適用** 統括情報セキュリティ責任者及び情報システム管理者によって、仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消することを確かめかる。	ー	ー	

通信経路 (2)LGWAN接続系端末に１台化 DaaS利用 ガバメントクラウド/DaaS(同一CSP)の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(2)の対策	クラウドサービス(DaaS)上での対策	6	○	**vi）仮想端末でのマルウェア対策ソフト** 統括情報セキュリティ責任者及び情報システム管理者によって、仮想端末でパターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末でマルウェア対策ソフトにより不正プログラム対策を行っていることを確かめかる。	ー	ー	
		7	○	**vii）接続先制限** 統括情報セキュリティ責任者及び情報システム管理者によってLGWAN接続系端末のIPアドレス、画面転送で使用する通信ポートのみにアクセスを制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末とLGWAN接続系端末間にIPアドレス、画面転送で使用する通信ポートでアクセスを制限を行っていることを確かめかる。	ー	ー	
		8	○	**viii)DaaS基盤の脆弱性対応** DaaS基盤の脆弱性へのパッチの適用は、DaaS事業者にて実施するDaaSを選定する。	□クラウドサービスの仕様書/基本契約書及び利用規約	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、DaaS基盤の脆弱性へのパッチの適用は、DaaS事業者にて実施するDaaSを選定していることを確かめる。	ー	ー	
		9	○	**ix)アクセスログ** 統括情報セキュリティ責任者及び情報システム管理者によって、DaaSのアクセスログを取得し、確認する。	□システム運用基準 □ログ	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、DaaSのアクセスログを取得し、確認していることを確かめる。	ー	ー	

通信経路 (2)LGWAN接続系端末に１台化 DaaS利用 ガバメントクラウド/DaaS(同一CSP)の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(2)の対策	クラウドサービスでの対策	10	○	**ⅰ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		11	○	**ⅱ）管理者権限管理** 統括情報セキュリティ責任者及び情報システム管理者によって、不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、CSPファイアウォールのユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、CSPファイアウォールのユーザ・特権管理者といった権限や管理の役割範囲に応じて適切な管理を行っていることを確かめかる。	ー	ー	
		12	○	**ⅲ）CSPファイアウォールでのパッチ適用** 統括情報セキュリティ責任者及び情報システム管理者によって、CSPファイアウォールの脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、CSPファイアウォールの脆弱性を修正するパッチを速やかに適用し、脆弱性を解消することを確かめかる。	ー	ー	

通信経路 (2)LGWAN接続系端末に1台化 DaaS利用 ガバメントクラウド/DaaS(同一CSP)の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(2)の対策	LGWAN接続系での対策	13	○	**ⅰ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、接続元(マイナンバー利用事務系DaaS)と接続先(庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム)の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより接続元(マイナンバー利用事務系DaaS)と接続先(庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム)の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		14	○	**ⅱ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、接続元(インターネット接続系DaaS)と接続先(インターネット、インターネット接続系のメールサーバ)の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、接続元(インターネット接続系DaaS)と接続先(インターネット、インターネット接続系のメールサーバ)の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		15	○	**ⅲ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、インターネット接続系からマイナンバー利用事務系への通信を遮断する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、インターネット接続系からマイナンバー利用事務系への通信を遮断していることを確かめかる。	ー	ー	

通信経路 (2)LGWAN接続系端末に1台化 DaaS利用 ガバメントクラウド/DaaS(同一CSP)の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(2)の対策	LGWAN接続系での対策	16		**ⅳ)アプリケーションの制限** 統括情報セキュリティ責任者及び情報システム管理者によって、LGWAN接続系端末でのスクリーンショット機能を停止する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、LGWAN接続系端末でのスクリーンショット機能を停止していることを確かめかる。	ー	ー	
		17	○	**ⅴ)未知の不正プログラム対策(エンドポイント対策)** 統括情報セキュリティ責任者及び情報システム管理者により、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、以下の対応が全て実施されている。 ・端末等のエンドポイントにおけるソフトウェア等の動作を監視し、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動(データの持ち出しや外部との通信等)を示す異常な挙動を監視・検出・特定する。 ・異常な挙動を検出した際にプロセスを停止、ネットワークからの論理的な隔離を行う。 ・インシデント発生時に発生要因の詳細な調査を実施する。	□システム設計書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、端末等のエンドポイントにおけるソフトウェア等の動作の監視がされていること、未知及び既知のマルウェア等の異常な挙動を監視・検知・特定ができるようになっていること並びに異常な挙動を検出した際のプロセスの停止、異常な挙動が検知された端末等に対してネットワークからの隔離ができるようになっていること及びインシデント発生要因の詳細な調査が実施できるようになっていることを確かめる。	ー	ー	

通信経路（３)インターネット接続系端末に１台化　DaaS利用（異なるCSP)
監査項目

通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

通信経路 (3)インターネット接続系端末に１台化　DaaS利用(異なるCSP)　の監査項目

✓ インターネット接続系端末からDaaS利用時の監査項目を示す。
✓ 本画面転送はβモデルの対策を実施することが前提であるため、βモデルの監査も実施すること。

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(3)の対策	クラウドサービス(DaaS)上での対策	1	○	**ⅰ)画面転送機能** 仮想端末と画面転送の分離対策にて、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えないDaaSを選定する。 DaaSはISMAPに登録するサービスを選定する。	□クラウドサービス事業者選定基準 □クラウドサービスの仕様書/基本契約書及び利用規約	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、ISMAPに登録するDaaSサービスを選定し、DaaSサービスは仮想端末を画面転送するという分離対策にて、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えないか確かめる。	ー	ー	
		2	○	**ⅱ)多要素によるユーザ認証** 統括情報セキュリティ責任者及び情報システム管理者によって、DaaSのユーザや特権管理者について多要素認証を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザや特権管理者について多要素認証を行うことを確かめかる。	ー	ー	
		3	○	**ⅲ)管理者権限管理** 統括情報セキュリティ責任者及び情報システム管理者によって、不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切な管理を行っていることを確かめかる。	ー	ー	
		4	○	**ⅳ)権限に基づくアクセス制御** 統括情報セキュリティ責任者及び情報システム管理者によって、権限に応じたアクセス制御を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、保守者の権限に応じたアクセス制御を行っていることを確かめかる。	ー	ー	
		5	○	**ⅴ)仮想端末でのパッチ適用** 統括情報セキュリティ責任者及び情報システム管理者によって、仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消することを確かめかる。	ー	ー	

通信経路 (3)インターネット接続系端末に１台化　DaaS利用(異なるCSP)　の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(3)の対策	クラウドサービス(DaaS)上での対策	6	○	**ⅵ）仮想端末でのマルウェア対策ソフト** 統括情報セキュリティ責任者及び情報システム管理者によって、仮想端末でパターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末でマルウェア対策ソフトにより不正プログラム対策を行っていることを確かめかる。	ー	ー	
		7	○	**ⅶ）接続先制限** 統括情報セキュリティ責任者及び情報システム管理者によってインターネット接続系端末のIPアドレス、画面転送で使用する通信ポートのみにアクセスを制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末とインターネット接続系端末間にIPアドレス、画面転送で使用する通信ポートでアクセスを制限を行っていることを確かめかる。	ー	ー	
		8	○	**ⅷ)DaaS基盤の脆弱性対応** DaaS基盤の脆弱性へのパッチの適用は、DaaS事業者にて実施するDaaSを選定する。	□クラウドサービスの仕様書/基本契約書及び利用規約	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、DaaS基盤の脆弱性へのパッチの適用は、DaaS事業者にて実施するDaaSを選定していることを確かめる。	ー	ー	
		9	○	**ⅸ)アクセスログ** 統括情報セキュリティ責任者及び情報システム管理者によって、DaaSのアクセスログを取得し、確認する。	□システム運用基準 □ログ	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、DaaSのアクセスログを取得し、確認していることを確かめる。	ー	ー	

通信経路 (3)インターネット接続系端末に１台化　DaaS利用(異なるCSP)　の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(3)の対策	インターネット接続系での対策	10	○	**ⅰ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		11	○	**ⅱ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によってLGWAN接続系DaaSとLGWAN接続系業務サーバの間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、LGWAN接続系DaaSとLGWAN接続系業務サーバの間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		12	○	**ⅲ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、インターネット接続系からマイナンバー利用事務系への通信を遮断する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、インターネット接続系からマイナンバー利用事務系への通信を遮断していることを確かめかる。	ー	ー	

通信経路 (3)インターネット接続系端末に１台化　DaaS利用(異なるCSP)　の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
面転送 通信経路(3)の対策	インターネット接続系での対策	13		**y)アプリケーションの制限** 統括情報セキュリティ責任者及び情報システム管理者によって、インターネット接続系端末でのスクリーンショット機能を停止する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、インターネット接続系端末でのスクリーンショット機能を停止していることを確かめかる。	ー	ー	
		14	○	**ｖ）未知の不正プログラム対策（エンドポイント対策）** 統括情報セキュリティ責任者及び情報システム管理者により、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、以下の対応が全て実施されている。 ・端末等のエンドポイントにおけるソフトウェア等の動作を監視し、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）を示す異常な挙動を監視・検出・特定する。 ・異常な挙動を検出した際にプロセスを停止、ネットワークからの論理的な隔離を行う。 ・インシデント発生時に発生要因の詳細な調査を実施する。	□システム設計書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、端末等のエンドポイントにおけるソフトウェア等の動作の監視がされていること、未知及び既知のマルウェア等の異常な挙動を監視・検知・特定ができるようになっていること並びに異常な挙動を検出した際のプロセスの停止、異常な挙動が検知された端末等に対してネットワークからの隔離ができるようになっていること及びインシデント発生要因の詳細な調査が実施できるようになっていることを確かめる。	ー	ー	

通信経路（３）‘インターネット接続系端末に１台化　DaaS利用（異なるCSP)
LGWAN接続系　α’モデルで接続　監査項目

通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

通信経路 (3)'インターネット接続系端末に１台化　DaaS利用(異なるCSP)
LGWAN接続系　α'モデルで接続の監査項目

✓ インターネット接続系端末からDaaS利用時の監査項目を示す。
✓ 本画面転送はβモデル、α'モデルの対策を実施することが前提であるため、βモデル、α'モデルの監査も実施すること。

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(3)'の対策	クラウドサービス(DaaS)上での対策	1	○	**ⅰ）画面転送機能** 仮想端末と画面転送の分離対策にて、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えないDaaSを選定する。 DaaSはISMAPに登録するサービスを選定する。	□クラウドサービス事業者選定基準 □クラウドサービスの仕様書/基本契約書及び利用規約	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、ISMAPに登録するDaaSサービスを選定し、DaaSサービスは仮想端末を画面転送するという分離対策にて、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えないか確かめる。	ー	ー	
		2	○	**ⅱ）多要素によるユーザ認証** 統括情報セキュリティ責任者及び情報システム管理者によって、DaaSのユーザや特権管理者について多要素認証を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザや特権管理者について多要素認証を行うことを確かめかる。	ー	ー	
		3	○	**ⅲ）管理者権限管理** 統括情報セキュリティ責任者及び情報システム管理者によって、不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切な管理を行っていることを確かめかる。	ー	ー	
		4	○	**ⅳ）権限に基づくアクセス制御** 統括情報セキュリティ責任者及び情報システム管理者によって、権限に応じたアクセス制御を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、保守者の権限に応じたアクセス制御を行っていることを確かめかる。	ー	ー	
		5	○	**ⅴ）仮想端末でのパッチ適用** 統括情報セキュリティ責任者及び情報システム管理者によって、仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消することを確かめかる。	ー	ー	

通信経路 (3)'インターネット接続系端末に１台化　DaaS利用(異なるCSP)
LGWAN接続系　α'モデルで接続の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(3)'の対策	クラウドサービス(DaaS)上での対策	6	○	**ⅵ）仮想端末でのマルウェア対策ソフト** 統括情報セキュリティ責任者及び情報システム管理者によって、仮想端末でパターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末でマルウェア対策ソフトにより不正プログラム対策を行っていることを確かめかる。	ー	ー	
		7	○	**ⅶ）接続先制限** 統括情報セキュリティ責任者及び情報システム管理者によってインターネット接続系端末のIPアドレス、画面転送で使用する通信ポートのみにアクセスを制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末とインターネット接続系端末間にIPアドレス、画面転送で使用する通信ポートでアクセスを制限を行っていることを確かめかる。	ー	ー	
		8	○	**ⅷ)DaaS基盤の脆弱性対応** DaaS基盤の脆弱性へのパッチの適用は、DaaS事業者にて実施するDaaSを選定する。	□クラウドサービスの仕様書/基本契約書及び利用規約	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、DaaS基盤の脆弱性へのパッチの適用は、DaaS事業者にて実施するDaaSを選定していることを確かめる。	ー	ー	
		9	○	**ⅸ)アクセスログ** 統括情報セキュリティ責任者及び情報システム管理者によって、DaaSのアクセスログを取得し、確認する。	□システム運用基準 □ログ	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、DaaSのアクセスログを取得し、確認していることを確かめる。	ー	ー	

通信経路 (3)'インターネット接続系端末に１台化　DaaS利用(異なるCSP)
LGWAN接続系　α'モデルで接続の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(3)'の対策	インターネット接続系での対策	10	○	**ⅰ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		11	○	**ⅱ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によってLGWAN接続系DaaSとLGWAN接続系業務サーバの間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、LGWAN接続系DaaSとLGWAN接続系業務サーバの間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		12	○	**ⅲ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、インターネット接続系からマイナンバー利用事務系への通信を遮断する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、インターネット接続系からマイナンバー利用事務系への通信を遮断していることを確かめかる。	ー	ー	
		13		**ⅳ)アプリケーションの制限** 統括情報セキュリティ責任者及び情報システム管理者によって、インターネット接続系端末でのスクリーンショット機能を停止する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、インターネット接続系端末でのスクリーンショット機能を停止していることを確かめかる。	ー	ー	

通信経路 (3)'インターネット接続系端末に１台化　DaaS利用(異なるCSP)
LGWAN接続系　α'モデルで接続の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送 通信経路(3)' の対策	インターネット接続系での対策	14	○	**ｖ）未知の不正プログラム対策（エンドポイント対策）** 統括情報セキュリティ責任者及び情報システム管理者により、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、以下の対応が全て実施されている。 ・端末等のエンドポイントにおけるソフトウェア等の動作を監視し、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）を示す異常な挙動を監視・検出・特定する。 ・異常な挙動を検出した際にプロセスを停止、ネットワークからの論理的な隔離を行う。 ・インシデント発生時に発生要因の詳細な調査を実施する。	□システム設計書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、端末等のエンドポイントにおけるソフトウェア等の動作の監視がされていること、未知及び既知のマルウェア等の異常な挙動を監視・検知・特定ができるようになっていること並びに異常な挙動を検出した際のプロセスの停止、異常な挙動が検知された端末等に対してネットワークからの隔離ができるようになっていること及びインシデント発生要因の詳細な調査が実施できるようになっていることを確かめる。	ー	ー	

通信経路 (4)インターネット接続系端末に 1 台化 DaaS利用 ガバメントクラウド/DaaS(同一CSP)
監査項目

通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

通信経路 (4)インターネット接続系端末に１台化　DaaS利用 ガバメントクラウド/DaaS(同一CSP) の監査項目

✓ インターネット接続系端末からDaaS利用時の監査項目を示す。
✓ 本画面転送はβモデルの対策を実施することが前提であるため、βモデルの監査も実施すること。

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(4)の対策	クラウドサービス(DaaS)上での対策	1	○	**ⅰ)画面転送機能** 仮想端末と画面転送の分離対策にて、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えないDaaSを選定する。 DaaSはISMAPに登録するサービスを選定する。	□クラウドサービス事業者選定基準 □クラウドサービスの仕様書/基本契約書及び利用規約	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、ISMAPに登録するDaaSサービスを選定し、DaaSサービスは仮想端末を画面転送するという分離対策にて、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えないか確かめる。	ー	ー	
		2	○	**ⅱ)多要素によるユーザ認証** 統括情報セキュリティ責任者及び情報システム管理者によって、DaaSのユーザや特権管理者について多要素認証を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザや特権管理者について多要素認証を行うことを確かめかる。	ー	ー	
		3	○	**ⅲ)管理者権限管理** 統括情報セキュリティ責任者及び情報システム管理者によって、不正行為(例:無許可の重要コマンド発行や重要データ読み書き)を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切な管理を行っていることを確かめかる。	ー	ー	
		4	○	**ⅳ)権限に基づくアクセス制御** 統括情報セキュリティ責任者及び情報システム管理者によって、権限に応じたアクセス制御を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、保守者の権限に応じたアクセス制御を行っていることを確かめかる。	ー	ー	
		5	○	**ⅴ)仮想端末でのパッチ適用** 統括情報セキュリティ責任者及び情報システム管理者によって、仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消することを確かめかる。	ー	ー	

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(4)の対策	クラウドサービス(DaaS)上での対策	6	○	**vi）仮想端末でのマルウェア対策ソフト** 統括情報セキュリティ責任者及び情報システム管理者によって、仮想端末でパターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末でマルウェア対策ソフトにより不正プログラム対策を行っていることを確かめかる。	ー	ー	
		7	○	**vii）接続先制限** 統括情報セキュリティ責任者及び情報システム管理者によってインターネット接続系端末のIPアドレス、画面転送で使用する通信ポートのみにアクセスを制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末とインターネット接続系端末間にIPアドレス、画面転送で使用する通信ポートでアクセスを制限を行っていることを確かめかる。	ー	ー	
		8	○	**viii)DaaS基盤の脆弱性対応** DaaS基盤の脆弱性へのパッチの適用は、DaaS事業者にて実施するDaaSを選定する。	□クラウドサービスの仕様書/基本契約書及び利用規約	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、DaaS基盤の脆弱性へのパッチの適用は、DaaS事業者にて実施するDaaSを選定していることを確かめる。	ー	ー	
		9	○	**ix）アクセスログ** 統括情報セキュリティ責任者及び情報システム管理者によって、DaaSのアクセスログを取得し、確認する。	□システム運用基準 □ログ	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、DaaSのアクセスログを取得し、確認していることを確かめる。	ー	ー	

通信経路 (4)インターネット接続系端末に１台化　DaaS利用 ガバメントクラウド/DaaS(同一CSP)の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(4)の対策	クラウドサービスでの対策	10	○	**ⅰ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、接続元(マイナンバー利用事務系DaaS)と接続先(庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム)の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、接続元(マイナンバー利用事務系DaaS)と接続先(庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム)の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		11	○	**ⅱ)管理者権限管理** 統括情報セキュリティ責任者及び情報システム管理者によって、不正行為(例:無許可の重要コマンド発行や重要データ読み書き)を防止するために、CSPファイアウォールのユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、CSPファイアウォールのユーザ・特権管理者といった権限や管理の役割範囲に応じて適切な管理を行っていることを確かめかる。	ー	ー	
		12	○	**ⅲ)CSPファイアウォールでのパッチ適用** 統括情報セキュリティ責任者及び情報システム管理者によって、CSPファイアウォールの脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、CSPファイアウォールの脆弱性を修正するパッチを速やかに適用し、脆弱性を解消することを確かめかる。	ー	ー	

通信経路 (4)インターネット接続系端末に１台化　DaaS利用 ガバメントクラウド/DaaS(同一CSP)の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(4)の対策	インターネット接続系での対策	13	○	**ⅰ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		14	○	**ⅱ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、LGWAN接続系DaaSとLGWAN接続系業務サーバとの間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューによりLGWAN接続系DaaSとLGWAN接続系業務サーバとの間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		15	○	**ⅲ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、インターネット接続系からマイナンバー利用事務系への通信を遮断する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、インターネット接続系からマイナンバー利用事務系への通信を遮断していることを確かめかる。	ー	ー	

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(4)の対策	インターネット接続系での対策	16		**ⅳ）アプリケーションの制限** 統括情報セキュリティ責任者及び情報システム管理者によってインターネット接続系端末でのスクリーンショット機能を停止する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、LGWAN接続系端末でのスクリーンショット機能を停止していることを確かめかる。	ー	ー	
		17	○	**ⅴ）未知の不正プログラム対策（エンドポイント対策）** 統括情報セキュリティ責任者及び情報システム管理者により、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、以下の対応が全て実施されている。 ・端末等のエンドポイントにおけるソフトウェア等の動作を監視し、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）を示す異常な挙動を監視・検出・特定する。 ・異常な挙動を検出した際にプロセスを停止、ネットワークからの論理的な隔離を行う。 ・インシデント発生時に発生要因の詳細な調査を実施する。	□システム設計書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、端末等のエンドポイントにおけるソフトウェア等の動作の監視がされていること、未知及び既知のマルウェア等の異常な挙動を監視・検知・特定ができるようになっていること並びに異常な挙動を検出した際のプロセスの停止、異常な挙動が検知された端末等に対してネットワークからの隔離ができるようになっていること及びインシデント発生要因の詳細な調査が実施できるようになっていることを確かめる。	ー	ー	

通信経路 (4)’インターネット接続系端末に１台化　DaaS利用
ガバメントクラウド/DaaS(同一CSP) LGWAN接続系　α‘モデル接続
監査項目

通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

通信経路 (4)'インターネット接続系端末に１台化　DaaS利用　ガバメントクラウド/DaaS(同一CSP)
LGWAN接続系　α'モデルで接続の監査項目

✓ インターネット接続系端末からDaaS利用時の監査項目を示す。
✓ 本画面転送はβモデル、α'モデルの対策を実施することが前提であるため、βモデル、α'モデルの監査も実施すること。

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(4)'の対策	クラウドサービス(DaaS)上での対策	1	○	**ⅰ）画面転送機能** 仮想端末と画面転送の分離対策にて、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えないDaaSを選定する。 DaaSはISMAPに登録するサービスを選定する。	□クラウドサービス事業者選定基準 □クラウドサービスの仕様書/基本契約書及び利用規約	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、ISMAPに登録するDaaSサービスを選定し、DaaSサービスは仮想端末を画面転送するという分離対策にて、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えないか確かめる。	ー	ー	
		2	○	**ⅱ）多要素によるユーザ認証** 統括情報セキュリティ責任者及び情報システム管理者によって、DaaSのユーザや特権管理者について多要素認証を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザや特権管理者について多要素認証を行うことを確かめかる。	ー	ー	
		3	○	**ⅲ）管理者権限管理** 統括情報セキュリティ責任者及び情報システム管理者によって、不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切な管理を行っていることを確かめかる。	ー	ー	
		4	○	**ⅳ）権限に基づくアクセス制御** 統括情報セキュリティ責任者及び情報システム管理者によって、権限に応じたアクセス制御を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、保守者の権限に応じたアクセス制御を行っていることを確かめかる。	ー	ー	
		5	○	**ⅴ）仮想端末でのパッチ適用** 統括情報セキュリティ責任者及び情報システム管理者によって、仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消することを確かめかる。	ー	ー	

通信経路 (4)'インターネット接続系端末に１台化　DaaS利用　ガバメントクラウド/DaaS(同一CSP)
LGWAN接続系　α'モデルで接続の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(4)'の対策	クラウドサービス(DaaS)上での対策	6	○	**vi）仮想端末でのマルウェア対策ソフト** 統括情報セキュリティ責任者及び情報システム管理者によって、仮想端末でパターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末でマルウェア対策ソフトにより不正プログラム対策を行っていることを確かめかる。	ー	ー	
		7	○	**vii）接続先制限** 統括情報セキュリティ責任者及び情報システム管理者によってインターネット接続系端末のIPアドレス、画面転送で使用する通信ポートのみにアクセスを制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末とインターネット接続系端末間にIPアドレス、画面転送で使用する通信ポートでアクセスを制限を行っていることを確かめかる。	ー	ー	
		8	○	**viii)DaaS基盤の脆弱性対応** DaaS基盤の脆弱性へのパッチの適用は、DaaS事業者にて実施するDaaSを選定する。	□クラウドサービスの仕様書/基本契約書及び利用規約	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、DaaS基盤の脆弱性へのパッチの適用は、DaaS事業者にて実施するDaaSを選定していることを確かめる。	ー	ー	
		9	○	**ix)アクセスログ** 統括情報セキュリティ責任者及び情報システム管理者によって、DaaSのアクセスログを取得し、確認する。	□システム運用基準 □ログ	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、DaaSのアクセスログを取得し、確認していることを確かめる。	ー	ー	

通信経路 (4)'インターネット接続系端末に１台化　DaaS利用　ガバメントクラウド/DaaS(同一CSP)
LGWAN接続系　α'モデルで接続の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送 通信経路(4)'の対策	クラウドサービスでの対策	10	○	**ⅰ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		11	○	**ⅱ）管理者権限管理** 統括情報セキュリティ責任者及び情報システム管理者によって、不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、CSPファイアウォールのユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、CSPファイアウォールのユーザ・特権管理者といった権限や管理の役割範囲に応じて適切な管理を行っていることを確かめかる。	ー	ー	
		12	○	**ⅲ）CSPファイアウォールでのパッチ適用** 統括情報セキュリティ責任者及び情報システム管理者によって、CSPファイアウォールの脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、CSPファイアウォールの脆弱性を修正するパッチを速やかに適用し、脆弱性を解消することを確かめかる。	ー	ー	

通信経路 (4)'インターネット接続系端末に１台化　DaaS利用　ガバメントクラウド/DaaS(同一CSP)
LGWAN接続系　α'モデルで接続の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(4)'の対策	インターネット接続系での対策	13	○	**ⅰ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより接続元（マイナンバー利用事務系DaaS）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		14	○	**ⅱ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、LGWAN接続系DaaSとLGWAN接続系業務サーバとの間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューによりLGWAN接続系DaaSとLGWAN接続系業務サーバとの間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		15	○	**ⅲ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、インターネット接続系からマイナンバー利用事務系への通信を遮断する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、インターネット接続系からマイナンバー利用事務系への通信を遮断していることを確かめかる。	ー	ー	

通信経路 (4)'インターネット接続系端末に１台化　DaaS利用　ガバメントクラウド/DaaS(同一CSP)
LGWAN接続系　α'モデルで接続の監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(4)'の対策	インターネット接続系での対策	16		**ⅳ）アプリケーションの制限** 統括情報セキュリティ責任者及び情報システム管理者によって、インターネット接続系端末でのスクリーンショット機能を停止する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、インターネット接続系端末でのスクリーンショット機能を停止していることを確かめかる。	ー	ー	
		17	○	**ⅴ）未知の不正プログラム対策（エンドポイント対策）** 統括情報セキュリティ責任者及び情報システム管理者により、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、以下の対応が全て実施されている。 ・端末等のエンドポイントにおけるソフトウェア等の動作を監視し、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）を示す異常な挙動を監視・検出・特定する。 ・異常な挙動を検出した際にプロセスを停止、ネットワークからの論理的な隔離を行う。 ・インシデント発生時に発生要因の詳細な調査を実施する。	□システム設計書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、端末等のエンドポイントにおけるソフトウェア等の動作の監視がされていること、未知及び既知のマルウェア等の異常な挙動を監視・検知・特定ができるようになっていること並びに異常な挙動を検出した際のプロセスの停止、異常な挙動が検知された端末等に対してネットワークからの隔離ができるようになっていること及びインシデント発生要因の詳細な調査が実施できるようになっていることを確かめる。	ー	ー	

通信経路 (5)　LGWAN接続系端末に１台化　オンプレミス　画面転送システム
監査項目

通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

通信経路 (5) LGWAN接続系端末に１台化　オンプレミス　画面転送システムの監査項目

✓LGWAN接続系端末からVDI利用利用時の監査項目を示す。

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(5)の対策	VDIでの対策	1	○	**ⅰ）画面転送機能** 統括情報セキュリティ責任者及び情報システム管理者によって、仮想端末と画面転送の分離対策にて、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えない。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、仮想端末を画面転送するという分離対策にて、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えないか確かめる。	ー	ー	
		2	○	**ⅱ）多要素によるユーザ認証** 統括情報セキュリティ責任者及び情報システム管理者によって、VDIのユーザや特権管理者について多要素認証を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザや特権管理者について多要素認証を行うことを確かめかる。	ー	ー	
		3	○	**ⅲ）管理者権限管理** 統括情報セキュリティ責任者及び情報システム管理者によって、不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切な管理を行っていることを確かめかる。	ー	ー	
		4	○	**ⅳ）権限に基づくアクセス制御** 統括情報セキュリティ責任者及び情報システム管理者によって、権限に応じたアクセス制御を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、保守者の権限に応じたアクセス制御を行っていることを確かめかる。	ー	ー	
		5	○	**ⅴ）仮想端末でのパッチ適用** 統括情報セキュリティ責任者及び情報システム管理者によって、仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消することを確かめかる。	ー	ー	

通信経路 (5) LGWAN接続系端末に１台化　オンプレミス　画面転送システムの監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(5)の対策	VDIでの対策	6	○	**ⅵ）仮想端末でのマルウェア対策ソフト** 統括情報セキュリティ責任者及び情報システム管理者によって、仮想端末でパターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末でマルウェア対策ソフトにより不正プログラム対策を行っていることを確かめかる。	ー	ー	
		7	○	**ⅶ）接続先制限** 統括情報セキュリティ責任者及び情報システム管理者によって、LGWAN接続系端末のIPアドレス、画面転送で使用する通信ポートのみにアクセスを制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末とLGWAN接続系端末間にIPアドレス、画面転送で使用する通信ポートでアクセスを制限を行っていることを確かめかる。	ー	ー	
		8	○	**ⅷ)VDI基盤の脆弱性対応** 統括情報セキュリティ責任者及び情報システム管理者によって、VDI基盤の脆弱性へのパッチの適用を行う。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、VDI基盤の脆弱性へのパッチの適用を行うことを確かめる。	ー	ー	
		9	○	**ⅸ)アクセスログ** 統括情報セキュリティ責任者及び情報システム管理者によって、VDIのアクセスログを取得し、確認する。	□システム運用基準 □ログ	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、VDIのアクセスログを取得し、確認していることを確かめる。	ー	ー	

通信経路 (5) LGWAN接続系端末に１台化　オンプレミス　画面転送システムの監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(5)の対策	LGWAN接続系での対策	10	○	**ⅰ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、接続元（マイナンバー利用事務系VDI）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、接続元（マイナンバー利用事務系VDI）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		11	○	**ⅱ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、接続元（インターネット接続系VDI）と接続先（インターネット、インターネット接続系のメールサーバ）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、接続元（インターネット接続系VDI）と接続先（インターネット、インターネット接続系のメールサーバ）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		12	○	**ⅲ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、インターネット接続系からマイナンバー利用事務系への通信を遮断する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、インターネット接続系からマイナンバー利用事務系への通信を遮断していることを確かめかる。	ー	ー	

通信経路 (5) LGWAN接続系端末に１台化　オンプレミス　画面転送システムの監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(5)の対策	LGWAN接続系での対策	13		**ⅳ）アプリケーションの制限** 統括情報セキュリティ責任者及び情報システム管理者によって、LGWAN接続系端末でのスクリーンショット機能を停止する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、LGWAN接続系端末でのスクリーンショット機能を停止していることを確かめかる。	ー	ー	
		14	○	**ⅴ）未知の不正プログラム対策（エンドポイント対策）** 統括情報セキュリティ責任者及び情報システム管理者により、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、以下の対応が全て実施されている。 ・端末等のエンドポイントにおけるソフトウェア等の動作を監視し、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）を示す異常な挙動を監視・検出・特定する。 ・異常な挙動を検出した際にプロセスを停止、ネットワークからの論理的な隔離を行う。 ・インシデント発生時に発生要因の詳細な調査を実施する。	□システム設計書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、端末等のエンドポイントにおけるソフトウェア等の動作の監視がされていること、未知及び既知のマルウェア等の異常な挙動を監視・検知・特定ができるようになっていること並びに異常な挙動を検出した際のプロセスの停止、異常な挙動が検知された端末等に対してネットワークからの隔離ができるようになっていること及びインシデント発生要因の詳細な調査が実施できるようになっていることを確かめる。	ー	ー	

通信経路経路 (6) インターネット接続系端末に 1 台化　オンプレミス　画面転送システム
監査項目

通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

通信経路 (6) インターネット接続系端末に１台化　オンプレミス　画面転送システムの監査項目

✓インターネット接続系端末からVDI利用時の監査項目を示す。
✓本画面転送はβモデルの対策を実施することが前提であるため、βモデルの監査も実施すること。

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(6)の対策	VDIでの対策	1	○	**ⅰ）画面転送機能** 統括情報セキュリティ責任者及び情報システム管理者によって、仮想端末と画面転送の分離対策にて、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えない。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、仮想端末を画面転送するという分離対策にて、仮想端末上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えないか確かめる。	－	－	
		2	○	**ⅱ）多要素によるユーザ認証** 統括情報セキュリティ責任者及び情報システム管理者によって、VDIのユーザや特権管理者について多要素認証を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザや特権管理者について多要素認証を行うことを確かめかる。	－	－	
		3	○	**ⅲ）管理者権限管理** 統括情報セキュリティ責任者及び情報システム管理者によって、不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切な管理を行っていることを確かめかる。	－	－	
		4	○	**ⅳ）権限に基づくアクセス制御** 統括情報セキュリティ責任者及び情報システム管理者によって、権限に応じたアクセス制御を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、保守者の権限に応じたアクセス制御を行っていることを確かめかる。	－	－	
		5	○	**ⅴ）仮想端末でのパッチ適用** 統括情報セキュリティ責任者及び情報システム管理者によって、仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消することを確かめかる。	－	－	

通信経路 (6) インターネット接続系端末に１台化　オンプレミス　画面転送システムの監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(6)の対策	VDIでの対策	6	○	**ⅵ）仮想端末でのマルウェア対策ソフト** 統括情報セキュリティ責任者及び情報システム管理者によって、仮想端末でパターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末でマルウェア対策ソフトにより不正プログラム対策を行っていることを確かめかる。	ー	ー	
		7	○	**ⅶ）接続先制限** 統括情報セキュリティ責任者及び情報システム管理者によって、インターネット接続系端末のIPアドレス、画面転送で使用する通信ポートのみにアクセスを制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、仮想端末とインターネット接続系端末間にIPアドレス、画面転送で使用する通信ポートでアクセスを制限を行っていることを確かめかる。	ー	ー	
		8	○	**ⅷ)VDI基盤の脆弱性対応** 統括情報セキュリティ責任者及び情報システム管理者によって、VDI基盤の脆弱性へのパッチの適用を行う。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、VDI基盤の脆弱性へのパッチの適用を行うことを確かめる。	ー	ー	
		9	○	**ⅸ)アクセスログ** 統括情報セキュリティ責任者及び情報システム管理者によって、VDIのアクセスログを取得し、確認する。	□システム運用基準 □ログ	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、VDIのアクセスログを取得し、確認していることを確かめる。	ー	ー	

通信経路 (6) インターネット接続系端末に１台化　オンプレミス　画面転送システムの監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(6)の対策	インターネット接続系、LGWAN接続系での対策	10	○	**ⅰ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、接続元（マイナンバー利用事務系VDI）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、接続元（マイナンバー利用事務系VDI）と接続先（庁内のマイナンバー利用事務系のシステム、ガバメントクラウド上のマイナンバー利用事務系のシステム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		11	○	**ⅱ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって接続元（LGWAN接続系VDI）と接続先（LGWAN接続系システム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、接続元（LGWAN接続系VDI）と接続先（LGWAN接続系システム）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		12	○	**ⅲ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、インターネット接続系からマイナンバー利用事務系への通信を遮断する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、インターネット接続系からマイナンバー利用事務系への通信を遮断していることを確かめかる。	ー	ー	
		13		**ⅳ)アプリケーションの制限** 統括情報セキュリティ責任者及び情報システム管理者によって、インターネット接続系端末でのスクリーンショット機能を停止する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、LGWAN接続系端末でのスクリーンショット機能を停止していることを確かめかる。	ー	ー	

通信経路 (6) インターネット接続系端末に１台化　オンプレミス　画面転送システムの監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(6)の対策	インターネット接続系、LGWAN接続系での対策	14	○	**ｖ）未知の不正プログラム対策（エンドポイント対策）** 統括情報セキュリティ責任者及び情報システム管理者により、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、以下の対応が全て実施されている。 ・端末等のエンドポイントにおけるソフトウェア等の動作を監視し、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）を示す異常な挙動を監視・検出・特定する。 ・異常な挙動を検出した際にプロセスを停止、ネットワークからの論理的な隔離を行う。 ・インシデント発生時に発生要因の詳細な調査を実施する。	□システム設計書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、端末等のエンドポイントにおけるソフトウェア等の動作の監視がされていること、未知及び既知のマルウェア等の異常な挙動を監視・検知・特定ができるようになっていること並びに異常な挙動を検出した際のプロセスの停止、異常な挙動が検知された端末等に対してネットワークからの隔離ができるようになっていること及びインシデント発生要因の詳細な調査が実施できるようになっていることを確かめる。	ー	ー	

通信経路 (7)　LGWAN接続系端末に１台化　オンプレミス　セキュアブラウザ
監査項目

通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

通信経路 (7) LGWAN接続系端末に１台化　オンプレミス　セキュアブラウザの監査項目

✓ LGWAN接続系端末からオンプレミス　セキュアブラウザ利用時の監査項目を示す。

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(7)の対策	LGWAN接続系端末セキュアブラウザの対策	1	○	**ⅰ）画面転送機能** 統括情報セキュリティ責任者及び情報システム管理者によって、端末とブラウザ実行環境の分離対策によりブラウザ実行環境上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えない。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、端末とブラウザ実行環境の分離対策により、ブラウザ実行環境上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えないか確かめる。	―	―	
		2	○	**ⅱ）セキュアブラウザの選定** ディスク領域（ファイル・レジストリ）の分離、メモリ領域の分離（プロセス分離）、ローカルと分離環境間の通信の禁止、仮想ブラウザ自身の正常性の維持、仮想ブラウザ自身の脆弱性の対応、任意のプログラム実行禁止が可能なセキュアブラウザを選定する。	□サービスの仕様書	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、ディスク領域（ファイル・レジストリ）の分離、メモリ領域の分離（プロセス分離）、ローカルと分離環境間の通信の禁止、仮想ブラウザ自身の正常性の維持、仮想ブラウザ自身の脆弱性の対応、任意のプログラム実行禁止が可能なセキュアブラウザを選定していることを確かめる。			
		3	○	**ⅲ）セキュアブラウザ基盤の脆弱性対応** 統括情報セキュリティ責任者及び情報システム管理者によって、セキュアブラウザ基盤の脆弱性にパッチを適用する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、セキュアブラウザ基盤の脆弱性にパッチを適用することを確かめかる。	―	―	
		4	○	**ⅳ）セキュアブラウザ　での不正プログラム対策** 統括情報セキュリティ責任者及び情報システム管理者によって、ブラウザ実行環境上で認可プログラムのみ実行を許可するなどにより、不正プログラム対策を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ブラウザ実行環境上で認可プログラムのみ実行を許可するなどにより、不正プログラム対策を行うことを確かめかる。	―	―	
		5	○	**ⅴ）アクセスログ** 統括情報セキュリティ責任者及び情報システム管理者によって、セキュアブラウザのアクセスログを取得し、確認する。	□システム運用基準 □ログ	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、セキュアブラウザのアクセスログを取得し、確認していることを確かめる。	―	―	

通信経路 (7) LGWAN接続系端末に１台化　オンプレミス　セキュアブラウザの監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(7)の対策	VPN終端での対策	6	○	**ⅰ)多要素によるユーザ認証** セキュリティ責任者及び情報システム管理者によって、VPNのユーザや特権管理者について多要素認証を行う(「知識」「所持情報」「生体情報」のうち、2つ以上の異なる要素を使って認証)。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、VPNのユーザや特権管理者について多要素認証を行っていることを確かめかる。	ー	ー	
		7	○	**ⅱ)管理者権限管理** 統括情報セキュリティ責任者及び情報システム管理者によって、不正行為(例:無許可の重要コマンド発行や重要データ読み書き)を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切な管理を行っていることを確かめかる。	ー	ー	
		8	○	**ⅲ)権限に基づくアクセス制御** 統括情報セキュリティ責任者及び情報システム管理者によって、権限に応じたアクセス制御を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、保守者の権限に応じたアクセス制御を行っていることを確かめかる。	ー	ー	
		9	○	**ⅳ)ファームウェア最新化** 統括情報セキュリティ責任者及び情報システム管理者によって、VPN終端の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、VPN終端の脆弱性を修正するパッチを速やかに適用を行うことを確かめる。	ー	ー	
		10	○	**ⅴ)アクセスログ** 統括情報セキュリティ責任者及び情報システム管理者によって、VPN終端のアクセスログを取得し、確認する。	□システム運用基準 □ログ	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、VPN終端のアクセスログを取得し、確認していることを確かめる。	ー	ー	

通信経路 (7) LGWAN接続系端末に１台化　オンプレミス　セキュアブラウザの監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(7)の対策	LGWAN接続系での対策	11	○	**ⅰ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、接続元（LGWAN接続系端末）と接続先（マイナンバー利用事務系VPN終端）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、接続元（LGWAN接続系端末）と接続先（マイナンバー利用事務系VPN終端）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		12	○	**ⅱ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、接続元（LGWAN接続系端末）と接続先（インターネット接続系VPN終端）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、接続元（LGWAN接続系端末）と接続先（インターネット接続系VPN終端）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		13	○	**ⅲ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、インターネット接続系からマイナンバー利用事務系への通信を遮断する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、インターネット接続系からマイナンバー利用事務系への通信を遮断していることを確かめかる。	ー	ー	
		14		**ⅳ)アプリケーションの制限** 統括情報セキュリティ責任者及び情報システム管理者によって、LGWAN接続系端末でのスクリーンショット機能を停止する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、LGWAN接続系端末でのスクリーンショット機能を停止していることを確かめかる。	ー	ー	

通信経路 (7) LGWAN接続系端末に１台化　オンプレミス　セキュアブラウザの監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(7)の対策	LGWAN接続系での対策	15	○	**ｖ）未知の不正プログラム対策（エンドポイント対策）** 統括情報セキュリティ責任者及び情報システム管理者により、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、以下の対応が全て実施されている。 ・端末等のエンドポイントにおけるソフトウェア等の動作を監視し、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）を示す異常な挙動を監視・検出・特定する。 ・異常な挙動を検出した際にプロセスを停止、ネットワークからの論理的な隔離を行う。 ・インシデント発生時に発生要因の詳細な調査を実施する。	□システム設計書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、端末等のエンドポイントにおけるソフトウェア等の動作の監視がされていること、未知及び既知のマルウェア等の異常な挙動を監視・検知・特定ができるようになっていること並びに異常な挙動を検出した際のプロセスの停止、異常な挙動が検知された端末等に対してネットワークからの隔離ができるようになっていること及びインシデント発生要因の詳細な調査が実施できるようになっていることを確かめる。	―	―	

通信経路 (8)　インターネット接続系端末に 1 台化　オンプレミス　セキュアブラウザ
監査項目

通信経路

	接続元 (業務端末の設置場所)	画面転送の方式
通信経路(1)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合 インターネット接続系に端末が残る場合を(1)'とする
通信経路(2)	LGWAN接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合 インターネット接続系に端末が残る場合を(2)'とする
通信経路(3)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合
通信経路(3)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが異なるCSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(4)	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合
通信経路(4)'	インターネット接続系	DaaS ※ガバメントクラウドと画面転送のDaaSが同一CSPである場合において、 LGWAN接続系からインターネットへブレイクアウト回線が存在する
通信経路(5)	LGWAN接続系	オンプレミス画面転送（VDI/SBC） インターネット接続系に端末が残る場合を(5)'とする
通信経路(6)	インターネット接続系	オンプレミス画面転送（VDI/SBC）
通信経路(7)	LGWAN接続系	オンプレミスセキュアブラウザ インターネット接続系に端末が残る場合を(7)'とする
通信経路(8)	インターネット接続系	オンプレミスセキュアブラウザ

通信経路 (8) インターネット接続系端末に１台化　オンプレミス　セキュアブラウザの監査項目

✓ インターネット接続系端末からオンプレミス　　セキュアブラウザ利用時の監査項目を示す。
✓ 本画面転送はβモデルの対策を実施することが前提であるため、βモデルの監査も実施すること。

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(8)の対策	インターネット接続系端末セキュアブラウザの対策	1	○	**ⅰ)画面転送機能** 統括情報セキュリティ責任者及び情報システム管理者によって、端末とブラウザ実行環境の分離対策により、ブラウザ実行環境上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えない。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、端末とブラウザ実行環境の分離対策により、ブラウザ実行環境上でのマルウェア感染、不正プログラムの動作などが手元の端末には影響を与えないか確かめる。	―	―	
		2	○	**ⅱ)セキュアブラウザの選定** ディスク領域（ファイル・レジストリ）の分離、メモリ領域の分離（プロセス分離）、ローカルと分離環境間の通信の禁止、仮想ブラウザ自身の正常性の維持、仮想ブラウザ自身の脆弱性の対応、任意のプログラム実行禁止が可能なセキュアブラウザを選定する。	□サービスの仕様書	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、ディスク領域（ファイル・レジストリ）の分離、メモリ領域の分離（プロセス分離）、ローカルと分離環境間の通信の禁止、仮想ブラウザ自身の正常性の維持、仮想ブラウザ自身の脆弱性の対応、任意のプログラム実行禁止が可能なセキュアブラウザを選定していることを確かめる。			
		3	○	**ⅲ)セキュアブラウザ基盤の脆弱性対応** 統括情報セキュリティ責任者及び情報システム管理者によって、セキュアブラウザ基盤の脆弱性にパッチを適用する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、セキュアブラウザ基盤の脆弱性にパッチを適用することを確かめかる。	―	―	
		4	○	**ⅳ)セキュアブラウザ　での不正プログラム対策** 統括情報セキュリティ責任者及び情報システム管理者によって、ブラウザ実行環境上で認可プログラムのみ実行を許可するなどにより、不正プログラム対策を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ブラウザ実行環境上で認可プログラムのみ実行を許可するなどにより、不正プログラム対策を行うことを確かめかる。	―	―	
		5	○	**ⅴ)アクセスログ** 統括情報セキュリティ責任者及び情報システム管理者によって、セキュアブラウザのアクセスログを取得し、確認する。	□システム運用基準 □ログ	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、セキュアブラウザのアクセスログを取得し、確認していることを確かめる。	―	―	

通信経路 (8) インターネット接続系端末に１台化　オンプレミス　セキュアブラウザの監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(8)の対策	VPN終端での対策	6	○	**ⅰ)多要素によるユーザ認証** セキュリティ責任者及び情報システム管理者によって、VPNのユーザや特権管理者について多要素認証を行う(「知識」「所持情報」「生体情報」のうち、2つ以上の異なる要素を使って認証)。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、VPNのユーザや特権管理者について多要素認証を行っていることを確かめかる。	―	―	
		7	○	**ⅱ)管理者権限管理** 統括情報セキュリティ責任者及び情報システム管理者によって、不正行為(例:無許可の重要コマンド発行や重要データ読み書き)を防止するために、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切に管理する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、ユーザ・特権管理者といった権限や管理の役割範囲に応じて適切な管理を行っていることを確かめかる。	―	―	
		8	○	**ⅲ)権限に基づくアクセス制御** 統括情報セキュリティ責任者及び情報システム管理者によって、権限に応じたアクセス制御を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、保守者の権限に応じたアクセス制御を行っていることを確かめかる。	―	―	
		9	○	**ⅳ)ファームウェア最新化** 統括情報セキュリティ責任者及び情報システム管理者によって、VPN終端の脆弱性を修正するパッチを速やかに適用し、脆弱性を解消する。	□システム運用基準	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、VPN終端の脆弱性を修正するパッチを速やかに適用を行うことを確かめる。	―	―	
		10	○	**ⅴ)アクセスログ** 統括情報セキュリティ責任者及び情報システム管理者によって、VPN終端のアクセスログを取得し、確認する。	□システム運用基準 □ログ	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、VPN終端のアクセスログを取得し、確認していることを確かめる。	―	―	

通信経路 (8) インターネット接続系端末に１台化　オンプレミス　セキュアブラウザの監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(8)の対策	インターネット接続系端末での対策	11	○	**ⅰ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、接続元（インターネット接続系端末）と接続先（マイナンバー利用事務系VPN終端）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、接続元（インターネット接続系端末）と接続先（マイナンバー利用事務系VPN終端）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		12	○	**ⅱ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、接続元（インターネット接続系端末）と接続先（LGWAN接続系VPN終端）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行う。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、接続元（インターネット接続系端末）と接続先（LGWAN接続系VPN終端）の間でのみ通信できるよう、IPアドレスと通信ポートによるアクセス制限を行っていることを確かめかる。	ー	ー	
		13	○	**ⅲ)アクセス制限** 統括情報セキュリティ責任者及び情報システム管理者によって、インターネット接続系からマイナンバー利用事務系への通信を遮断する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、インターネット接続系からマイナンバー利用事務系への通信を遮断していることを確かめかる。	ー	ー	
		14		**ⅳ)アプリケーションの制限** 統括情報セキュリティ責任者及び情報システム管理者によって、インターネット接続系端末でのスクリーンショット機能を停止する。	□システム管理基準 □システム設計書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、インターネット接続系端末でのスクリーンショット機能を停止していることを確かめかる。	ー	ー	

通信経路 (8) インターネット接続系端末に１台化　オンプレミス　セキュアブラウザの監査項目

項目		No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
画面転送通信経路(8)の対策	インターネット接続系端末での対策	15	○	**ｖ）未知の不正プログラム対策（エンドポイント対策）** 統括情報セキュリティ責任者及び情報システム管理者により、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、以下の対応が全て実施されている。 ・端末等のエンドポイントにおけるソフトウェア等の動作を監視し、外部からの侵入や、未知及び既知のマルウェア等による悪意ある活動（データの持ち出しや外部との通信等）を示す異常な挙動を監視・検出・特定する。 ・異常な挙動を検出した際にプロセスを停止、ネットワークからの論理的な隔離を行う。 ・インシデント発生時に発生要因の詳細な調査を実施する。	□システム設計書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、端末等のエンドポイントにおけるソフトウェア等の動作の監視がされていること、未知及び既知のマルウェア等の異常な挙動を監視・検知・特定ができるようになっていること並びに異常な挙動を検出した際のプロセスの停止、異常な挙動が検知された端末等に対してネットワークからの隔離ができるようになっていること及びインシデント発生要因の詳細な調査が実施できるようになっていることを確かめる。	―	―	