別紙５

庁内クラウドの設備情報及び利用時調整項目

30.10.

１　定義

（１）庁内ＬＡＮシステム

全庁共通機能を提供するサーバ、業務アプリケーション、ネットワーク機器、配線、端末機、プリンタ等から構成される全庁に渡るシステム全体をいう。

（２）ネットワーク分離

庁内ＬＡＮを、マイナンバー利用事務ネットワーク、一般業務ネットワーク及びインターネット接続ネットワークの３つに分離しているネットワーク構成をいう。

（３）庁内クラウド

県情報政策課が、個別にサーバシステムを構築・運用する必要のある庁内各課に対して、当該サーバの統合基盤としてのサーバプラットフォームを庁内ＬＡＮシステムにより PaaS 方式で提供するものをいう。

なお、ネットワーク分離に対応し、公開系クラウド、庁内系クラウド、マイナンバー利用事務系クラウドに分離している。

（４）基本サーバ

庁内ＬＡＮシステムのうち、全庁共通機能を提供するためのサーバをいう。

（５）個別システムサーバ

庁内ＬＡＮ上で各種の業務機能を個別に提供するためのサーバであり、基本サーバ以外のすべてのサーバをいう。

（６）個別設置サーバ

庁内各課が物理的に分離して設置する個別システムサーバのことであり、庁内クラウド上で稼動する庁内各課の仮想サーバ以外の個別システムサーバをいう。

（７）公開系クラウド

庁内クラウドのうち、インターネット上に公開される（インターネット接続ネットワークからのみアクセス可能な）仮想サーバを格納するものをいう。

（８）庁内系クラウド

庁内クラウドのうち、一般業務ネットワークからのみアクセス可能な仮想サーバを格納するものをいう。

（９）マイナンバー利用事務系クラウド

庁内クラウドのうち､マイナンバー利用事務ネットワークからのみアクセス可能な仮想サーバを格納するものをいう。

(10) Oracle 共用データベースサーバ

仮想サーバのうち Oracle によるデータベース利用が必要なものについて、共用で利用することができるデータベースサーバをいい、ネットワーク分離に対応し、マイナンバー利用事務データベースサーバと一般業務データベースサーバに分離している。

(11) 仮想 FW

庁内クラウド上に設置される、仮想化技術を用いてアクセス制御を実現するファイアウォールのことをいい、各仮想サーバごとに設定される分散ファイアウォールと、各クラウドごとの境界に設置される境界ファイアウォールで構成する。

2　庁内クラウドの設備情報

表 1　設備情報

項目	公開系クラウド	庁内系クラウド マイナンバー利用事務系クラウド
サーバ仮想化技術	VMWare(ESXi)	
リソース割り当て	CPU コア数、メモリ容量、ディスク容量のリソースは庁内各課からの要望に基づき県情報政策課が決定する。 なお、庁内クラウドを構成するサーバはインテル® Xeon® Gold 6152 プロセッサーを搭載する。	
ドライブ構成	各仮想サーバの仮想ハードディスクは１ドライブ構成とし、システム領域と業務データ領域のドライブを分離しない。	
仮想サーバ OS （選択可能 OS）	・WindowsServer2012(64 ビット)　※1 ・WindowsServer2012R2(64 ビット)　※1 ・WindowsServer2016(64 ビット) ・Red Hat Enterprise Linux Server 7	
ネットワーク	IP アドレス、ホスト名共に１つを割り当てる。　※2	
セキュリティ（FW）	仮想サーバごとに仮想 FW を設定	
ウイルス対策	OS にかかわらず新規構築システムは、庁内各課での調達・導入が必要	・Windows 版は県情報政策課が組み込み提供 ・Linux 版は庁内各課での調達・導入が必要
バックアップ処理	県情報政策課が実施 （各仮想サーバの停止は不要）	
運用管理	死活監視（ICMP） リソース監視（vRealize Operations Manager）	
基本設定	IP 設定、ホスト名設定、DNS 登録	

※1 サポート期限の令和５年（2023 年）10 月 10 日までに 2016 以降のバージョンに変更する見通しが立つことを条件に選択可能とする。

※2 複数の IP アドレスが必要な場合は別途県情報政策課と協議の上決定する。

3　庁内クラウド共通項目

ここに示す項目は、公開系クラウド、庁内系クラウド及びマイナンバー利用事務系クラウドいずれも共通で適用する。

（1）提供範囲

提供範囲はハードウェア（故障時のハードウェア保守を含む)、必要とするメモリやディスク量等の資源割当、OS プレインストール及び表 1 記載の「基本設定」までとし、OS から上位層（上記以外の OS 設定、ミドルウェア、業務アプリケーション等）は庁内各課にて調査、構築・開発、維持管理を行うものとする。

なお、セキュリティパッチ等の適用は庁内各課にて対応すること。

（2）アクセス制御

別紙１のとおり、公開系クラウド、庁内系クラウド及びマイナンバー利用事務系クラウドは､ネットワーク分離に対応したそれぞれのネットワーク専用のクラウド環境であり、仮想 FW により分離し、アクセス制御を行う。

また、それぞれのネットワークの専用端末機（インターネット接続端末機、一般業務端末機又はマイナンバー利用事務専用端末機）からのみアクセス可能とする。

なお、マイナンバー利用事務専用端末機について、端末機側のファイアウォールやルータにおいてもアクセス制御を行っていることから､必要な設定について県情報政策課と協議すること。

（3）仮想サーバの操作手段

各仮想サーバの操作は、IP アドレスにより限定された端末機から以下の表に示す方法により行うものとする。

なお、接続に係る ID 及びパスワード並びに端末機ソフトウェア導入方法は、県情報政策課が別途手順書を作成し庁内各課に提供するものとする。

○サーバ操作が可能な端末機の限定

いずれも固定 IP アドレスを付与する。

・庁内各課担当者の庁内ＬＡＮ端末機（県情報政策課が別途許可する。ただし、操作対象のクラウドと同じネットワークに属する端末機に限る。）

・県情報政策課が NOC 室内に設置する共用のコンソール PC３台

表 2　仮想サーバの操作方法

接続先サーバ OS 種別	リモート操作方法	ファイル転送方法	端末機上のソフトウェア
Windows 系 OS	リモートデスクトップ	FTP	Windows 標準機能/FFFTP
Linux 系 OS	SSH	FTP	TeraTerm/FFFTP

（4）メール配信

仮想サーバにメール配信等の機能を実装し、庁内ＬＡＮシステムのメールルータ又はメールサーバを介してメール配送する必要がある場合は、庁内各課は県情報政策課と協議すること。

（5）データベース

ア　仮想サーバにデータベース機能を実装する場合は､費用面で有利な PostgreSQL、MySQL 等オープンソースソフトウェアを積極的に活用すること。

イ　Oracle の利用は、Oracle を利用している既存の個別システムで県情報政策課と協議済みのものに限る。なお、今後、新規に開発・導入する個別システムにおいては、Oracle 共用データベースサーバの利用は認めない。

（6）バックアップ・リストア

ア　バックアップの注意事項

各仮想サーバのデータバックアップ処理は、県情報政策課が庁内クラウドの基本機能として提供し実施する。

なお、各仮想サーバは、スナップショットを利用したエージェントレス方式によりバックアップ処理を行うため、当該処理のために仮想サーバ OS のシャットダウンや仮想サーバ上の一部サービス停止措置等の対応は必要ない。

ただし、仮想サーバで稼働させるデータベース機能においては、データベースのエクスポート機能によりデータベース構造（テーブル情報等）を含むデータバックアップファイルを仮想サーバ内に１日１回以上定期出力・保存する設定を行うこと。

イ　バックアップスケジュール

バックアップ処理の頻度は次のとおりとし、取得したバックアップは 21 日間保持する。

表 3バックアップ対象とスケジュール

	対象領域	フルバックアップ
公開系クラウド	仮想ハードディスク全体	毎日１回（深夜帯）
庁内系クラウド	仮想ハードディスク全体	毎日１回（深夜帯）
マイナンバー利用事務系クラウド	仮想ハードディスク全体	毎日１回（深夜帯）

ウ　リストアの注意事項

バックアップデータからのリストア作業は県情報政策課が行うので、必要とする場合には庁内各課が県情報政策課に依頼すること。

なお、リストアは、スナップショットによる仮想サーバ全体のリストアのほか、ファイル単位でのリストアが可能である。

ただし、ファイル単位でのリストアは、システム全体の動作を保証するものではなく、局所的なリストアとなることに留意すること。

（7）バックアップデータの遠隔地複製保管

県外の遠隔地データセンターに、毎日１回オンラインでバックアップデータの複製保管を行う。(21 日間保管)

（8）仮想サーバの運用管理

ア　仮想サーバ上の運用管理は、庁内各課が主体的に行うものとする。

○庁内各課が行う必要がある運用管理項目の例

・OS の調整・セキュリティパッチ適用

・ミドルウェアの導入・調整・セキュリティパッチ適用

・業務アプリケーションの開発・導入・改修・保守
・仮想サーバの詳細な動作監視
・利用状況の把握
・利用者からの問い合わせ対応

イ　県情報政策課は、各仮想サーバに対する ICMP ポーリング（ping）による応答確認及び vRealize Operations Manager による割当リソースの消費状況の定期監視を行うが、各仮想サーバ内部の詳細な動作監視は行わない。

（9）庁内クラウドの活用ができないもの

ここに示す項目に該当する個別設置サーバは、庁内クラウドを活用することができない。

ア　庁内ＬＡＮシステムの内部ネットワーク以外の別ネットワーク上に整備する必要があるもの。
イ　庁内ＬＡＮシステムの内部ネットワークの利用対象機関ではない県以外の機関と専用線接続等による直接接続があるもの。
ウ　負荷分散装置による処理を必要とするなど大規模なもの。
エ　特定機器でのみ稼働可能であるなど機種依存性があるもの。
オ　外部装置を直接制御又は直接接続する必要があるもの。
カ　汎用機（大型電子計算機）業務に関するもの。
キ　国費等で整備したもののうち、機器を明確に分離して設置する必要があるもの。
ク　小規模なもの、ＡＳＰ等他の方法ですでに安価なサービスが実現・提供されているものなど、庁内クラウドを活用した場合に他の方法よりも総コストが上昇することが明らかなもの。

4　公開系クラウドの調整項目

（1）公開系クラウド上の仮想サーバに係るアクセス制御

ア　インターネット側からの通信

インターネット側からの仮想サーバへのアクセスは、http(80)及び https(443)に限るものとする。

イ　リバースプロキシ機能

前ア項の通信において、http(80)は県が設置する統合 Web アクセラレータ上のリバースプロキシ機能を経由した代理接続となるが、https(443)は当該リバースプロキシ機能を経由しない。

なお、リバースプロキシ機能を経由する http(80)についても、仮想サーバが動的な Web ページやリアルタイム情報を提供する等、リバースプロキシ機能のキャッシュ処理を避ける必要がある場合には当該キャッシュを行わない設定が可能である。該当する場合には、庁内各課は県情報政策課に協議すること。

ウ　ＳＳＬ証明書

前ア項の通信において、https(443)を利用する場合には、庁内各課は必要となる証明書の取得・維持を行うとともに仮想サーバへの証明書の組込みを行うこと。

なお、ＳＳＬ処理を統合Webアクセラレータで実施することを希望する場合は、県情報政策課と協議すること。

また、セキュリティクラウドの WAF 機能を利用する場合、証明書登録（変更も含む）について、別途県情報政策課に依頼を行うこと。

エ　ネットワークからの通信

公開系クラウド上の仮想サーバと一般業務ネットワークとは仮想FWにより分離しており、通信できない。コンテンツ更新等の特別な通信が必要な場合、庁内各課は県情報政策課と協議すること。

ただし、マイナンバー利用事務ネットワークとの通信は一切認めない。

（2）公開系クラウド上の仮想サーバのウイルス対策ソフトウェア

公開系クラウド上の仮想サーバを新規構築する場合、仮想サーバの OS の種別にかかわらず庁内各課がサーバ用ウイルス対策ソフトウェアを調達し、必要な設定を行うこと。

5　庁内系クラウドの調整項目

（1）庁内系クラウド上の仮想サーバに係るアクセス制御

ア　すべての一般業務端末機は、庁内系クラウド上の各仮想サーバへ通信可能であり、アクセス制御は行わない。

イ　前ア項の通信を規制し関係職員以外のサーバアクセスを禁止する等のアクセス制御は、各仮想サーバにおいて ID 及びパスワード認証等により行うものとし、庁内各課が仮想サーバ内に認証処理を実装すること。

ウ　前イ項の措置のほか、より厳格なアクセス制限を行う必要がある場合は、特定の IP アドレス又はセグメント上の端末機に限定して、仮想サーバへの通信到達を可能とするネットワーク設定が仮想 FW により可能であるので、本制御を希望する場合には、庁内各課は県情報政策課と協議すること。

（2）庁内系クラウド上の仮想サーバのウイルス対策ソフトウェア

庁内系クラウド上の仮想サーバにおいて、Windows 系 OS の仮想サーバについては県情報政策課がサーバ用ウイルス対策ソフトウェアを組み込み必要な設定を行うが、Linux 系 OS の仮想サーバについては庁内各課がウイルス対策ソフトウェアのライセンス調達を行い、常に最新パターンファイルの自動更新及びウイルス検索がなされるよう仮想サーバに導入すること。

なお、庁内系ウイルス対策サーバからパターンファイルの配付を希望する場合は、トレンドマイクロ社の ServerProtect 又はウイルスバスターコーポレートエディションを導入し、それ以外のセキュリティ対策製品を利用する場合は、庁内各課が導入及びパターンファイル更新等の管理を行うこと。

※パターンファイルの配信であっても庁内系クラウドからインターネットへの通信は許可しない。

（3）庁内系クラウドの WSUS サーバ利用

庁内系 WSUS サーバをセキュリティパッチのダウンロード先として利用することが可能であるため、希望する場合は県情報政策課と協議すること。

6　マイナンバー利用事務系クラウドの調整項目

（1）マイナンバー利用事務系クラウド上の仮想サーバに係るアクセス制御

ア　マイナンバー利用事務専用端末機は、指定した仮想サーバ等特定のシステムにのみ通信可能とするアクセス制御を行う。そのため、特定の IP アドレス又はセグメント上のマイナンバー利用事務専用端末機等に限定して、仮想サーバへの通信到達を可能とするネットワーク設定を仮想 FW により実施するので、庁内各課は必要な設定について県情報政策課と協議すること。

イ　前ア項のほか関係職員以外のサーバアクセスを禁止する等のアクセス制御として、各仮想サーバにおいて ID 及びパスワード認証等により行うものとし、庁内各課が仮想サーバ内に認証処理を実装すること。

（2）マイナンバー利用事務系クラウド上の仮想サーバのウイルス対策ソフトウェア

マイナンバー利用事務系クラウド上の仮想サーバにおいて、Windows 系 OS の仮想サーバについては県情報政策課がサーバ用ウイルス対策ソフトウェアを組み込み必要な設定を行うが、Linux 系 OS の仮想サーバについては庁内各課がウイルス対策ソフトウェアのライセンス調達を行い、常に最新パターンファイルの自動更新及びウイルス検索がなされるよう仮想サーバに導入すること。

なお、マイナンバー利用事務系ウイルス対策サーバからパターンファイルの配付を希望する場合は、トレンドマイクロ社の ServerProtect 又はウイルスバスターコーポレートエディションを導入し、それ以外のセキュリティ対策製品を利用する場合は、庁内各課が導入及びパターンファイル更新等の管理を行うこと。

※パターンファイルの配信であってもマイナンバー利用事務系クラウドから一般業務ネットワークやインターネットへの通信は許可しない。

（3）マイナンバー利用事務系クラウドの WSUS サーバ利用

マイナンバー利用事務系 WSUS サーバをセキュリティパッチのダウンロード先として利用することが可能であるため、希望する場合は県情報政策課と協議すること。

7　Oracle 共用データベースサーバ利用の調整項目

（1）Oracle 共用データベースサーバ上のデータベース構築

ア　構築方法

データベースの構築方法は、県情報政策課が庁内各課に別途提供するパラメータシートに庁内各課が必要事項を記載し県情報政策課に提出することで、県情報政策課が当該サーバ上に庁内各課が必要とする Oracle のデータベースファイル及びインスタンスを作成し、ID 及びパスワードを庁内各課に発行するものとする。

提供バージョンは Oracle Database 12c Release2 Standard Edition 2(Ver.12.2.0.1)とする。

イ　利用方法

データベースの利用方法は、庁内各課が、庁内系クラウド又はマイナンバー利用事務系クラウド上の仮想サーバに当該インスタンスに接続して処理をするサーバアプリケーションを搭載し実行してアクセスするものとする。なお、庁内ＬＡＮ端末機から当該データベースサーバに直接アクセスする利用方法は禁止する。

ウ　データベースアクセスツール

仮想サーバ上の業務アプリケーションにおいて必要とする JDBC ドライバ等データベースアクセスツールは県情報政策課から庁内各課に別途提供する。

（2）利用対象サーバ

Oracle 共用データベースサーバを利用するシステムは、既存の個別システムで、県情報政策課と協議済みのものに限る。

（3）Oracle 共用データベースサーバのデータバックアップ

ア　Oracle 共用データベースサーバは、県情報政策課が無停止でバックアップ処理を行う。

なお、バックアップ処理中にデータベースへのアクセスは可能であるが、バックアップデータについて、アプリケーション等との整合性を確実に求める場合は、バックアップ処理中はデータベースの更新処理を行わない、又はサーバアプリケーション等該当サービスの停止など、静止点を設けるために必要な対応を行うこと。

イ　バックアップ処理の頻度は次のとおりとする。

区分	対象領域	フルバックアップ	差分バックアップ
マイナンバー利用事務データベースサーバ	システム領域	構築時又はシステム改変時のみ	―
	業務データ領域（データベース関連ファイル）	週１回（深夜帯）	毎日１回（深夜帯）
	業務データ領域（データベース表ファイル）	毎日１回（深夜帯）	―
一般業務データベースサーバ	システム領域	構築時又はシステム改変時のみ	―
	業務データ領域（データベース関連ファイル）	毎日１回（深夜帯）	―
	業務データ領域（データベース表ファイル）	毎日１回（深夜帯）	―

（4）Oracle 共用データベースサーバのウイルス対策ソフトウェア

県情報政策課がサーバ用ウイルス対策ソフトウェアを組み込み必要な設定を行う。