情報共有基盤　機能概要説明書

初版(1.0)　2010 年 10 月 29 日

改訂版(4.0)　2021 年 01 月 13 日

横浜市総務局　住民情報システム課

目次

1 はじめに

(1) 本書の目的

本書の目的は、情報共有基盤の利用者に対して情報共有基盤の利用方法の概要を示すことである。

(2) 対象読者

本書は、情報共有基盤を利用する業務システムの担当者、開発事業者、運用事業者及び保守事業者を対象読者とする。

2 情報共有基盤の概要

(1) 情報共有基盤構築の経緯

本市ではこれまでに様々な業務のシステムが構築されてきたが、業務部門ごとに多種多様な規格や機能をもつシステムが導入されたため、各システム間のデータ連携や機器の共有等が困難であるという課題が生じていた。

こうした状況を改善するため、複数のシステムで共通で利用・連携できるプラットフォームである情報共有基盤を平成 23 年度に整備し、ハードウェア、ソフトウェア、データの共有による全体最適化を進めている。

また、平成 28 年度には仮想化技術を活用した仮想化サーバ基盤である仮想基盤を整備し、翌年度には基盤システムを利用している各業務システムの機器更新において仮想基盤への受け入れを実施した。

平成 30 年 6 月現在、情報共有基盤を利用する主な業務システムは以下の通りである。

- 福祉保健システム（平成 24 年 1 月　稼働）
- 障害福祉システム（平成 24 年 1 月　稼働）
- 母子保健システム（平成 25 年 3 月　稼働）
- 生活保護システム（平成 26 年 1 月　稼働）
- 統合番号連携システム（平成 28 年 1 月　稼働）
- 国民健康保険料収納対策支援システム（平成 29 年 5 月　稼働）
- 顔認証システム（平成 29 月 6 月　稼働）

(2) 情報共有基盤の目的

情報共有基盤の目的は、行政運営の効率化である。具体的には、下記に示す 4 つを掲げている。

ア　　業務の効率化の実現

複数の業務システムが共通して利用できるデータ連携の仕組みを整備することで、システム間の情報伝達を円滑にし、業務を効率化する。

イ　　情報化関連経費の縮減

複数の業務システムがハードウェアなどのシステムインフラを共用することにより、システムの

機器調達・構築・運用に要する経費の縮減を図る。

ウ　　業務所管部門部署の管理負担の軽減

業務システムが利用するシステムインフラの管理を基盤システム所管部門が一括して引き受けることで、業務システム所管部門の管理負担の軽減を図る。

エ　　ベンダロックインの排除

特定の事業者に依存しない基礎技術を採用することで、情報共有基盤を利用する業務システムの構築に複数の事業者が参画できるようにする。

(3) AIST 包括フレームワーク

前述のベンダロックインの排除を達成するためには、特定の事業者に依存しない基礎技術を使用して情報共有基盤を構築する必要がある。この基礎技術として情報共有基盤では国立研究開発法人　産業技術総合研究所が開発した AIST 包括フレームワークを用いている。

AIST 包括フレームワークにおけるフレームワークとは、プロセスや成果物作成ルールを中心とし、Java での Web アプリケーション開発のソフトウェア基盤と開発手法の指針を示すガイドラインなどを含む、開発活動を進める上での包括的な環境全体を提供するものである。AIST 包括フレームワークは、一般的なソフトウェア開発工程のうち、要件分析から受入テストまでを対象とし、各工程の手順を定めるプロセス、開発の共通ルールである開発標準、開発を支援するツールを提供する基盤フレームワークから構成されている。

この AIST 包括フレームワークを本市向けにカスタマイズしたものが情報共有基盤に適用されている。

(4) 情報共有基盤が提供するサービス

情報共有基盤は、以下に示すサービスを提供する。

ア　基盤ネットワーク

情報共有基盤端末や業務システムサーバで利用できる全庁的なネットワークである。また、各種ネットワークサービスを提供している。

本書の 4 情報共有基盤ネットワークで説明している。

イ　　端末統制基盤（情報共有基盤ドメイン）

情報共有基盤端末やサーバの運用・管理のため、資産管理、セキュリティ対策、ドメインサービ

ス、資源配布等の機能を提供している。

本章の 5 基盤端末で説明している。

ウ　　仮想基盤

業務システム用の仮想サーバ及び仮想ネットワークを提供する仮想化サーバ基盤である。また、仮想基盤上の業務システム向けの運用・監視、パフォーマンス管理、バックアップ機能を提供している。

本書の 6 仮想基盤で説明している。

エ　　基盤システム

シングルサインオン（SSO)、ポータル、データ連携等、業務システムが共通して必要とする機能を提供している。

本書の 7SSO システム　～　11 データ連携基盤で説明している。

(5) 情報共有基盤の機器構成

情報共有基盤の機器構成の概要を図 2-1　情報共有基盤機器構成図に示す。

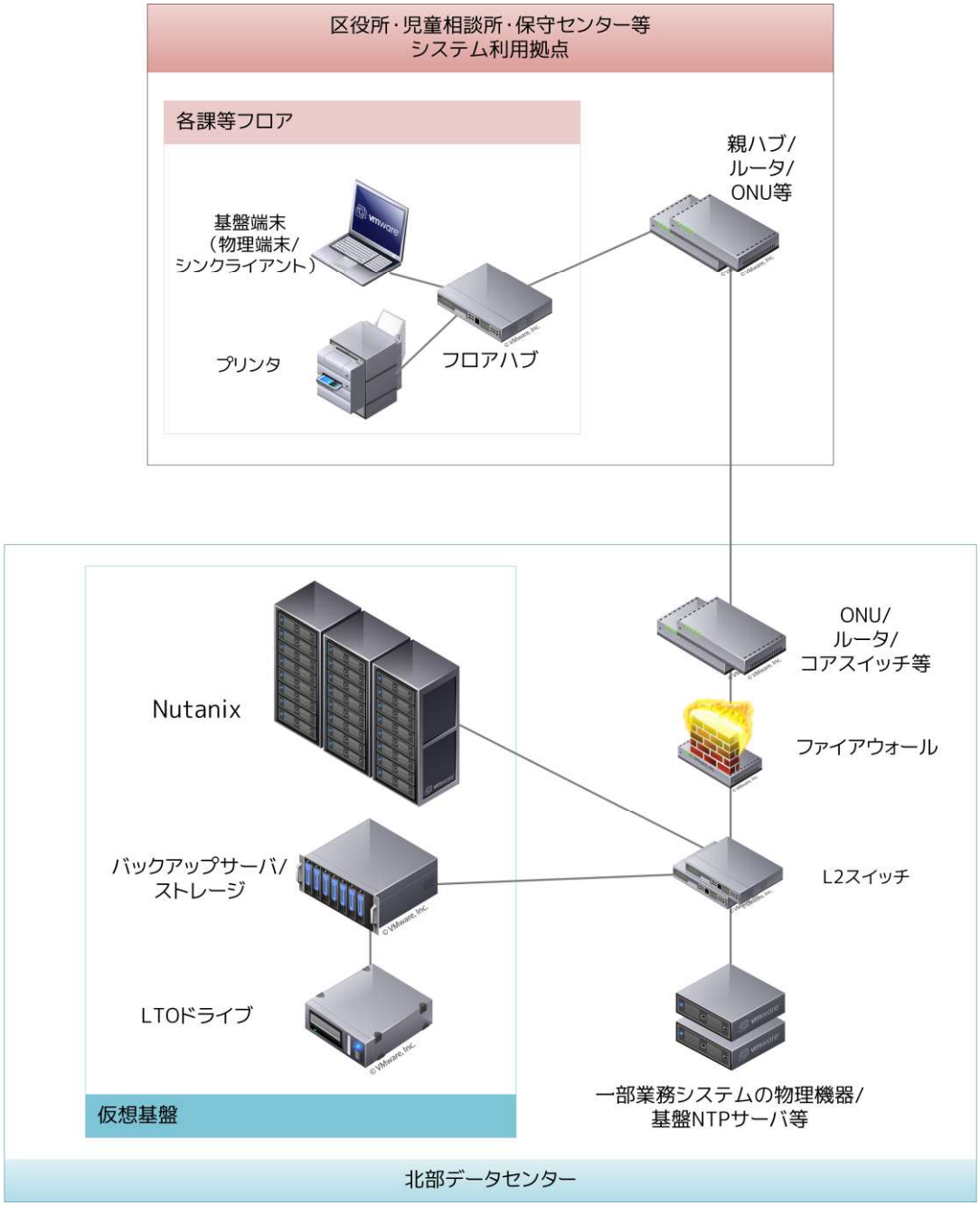

図 2-1　情報共有基盤機器構成図

3 業務システムによる情報共有基盤の利用

業務システムは、その用途に応じて情報共有基盤が提供するシステムインフラや機能の一部、又は全部を利用することができる。

4 情報共有基盤ネットワーク

(1) 情報共有基盤ネットワークの概要

情報共有基盤ネットワーク（以下、「基盤ネットワーク」という。）は、市庁舎や区役所等のシステム利用拠点と北部データセンター（以下、「北部 DC」という。）を結ぶ、全庁的なネットワークである。実態は、住民記録システム等の基幹システム用ネットワークの一部である。

基盤ネットワークは広域イーサネットを利用したプライベートな TCP/IP ネットワークであり、インターネットには接続していない。また、地方公共団体間を接続する総合行政ネットワーク（LGWAN）との通信が可能である。

基盤ネットワークの責任分界点は、システム利用拠点の執務室内に設置された管理・監視機能付きのスイッチングハブ（以下、「フロアハブ」という。）であり、業務システムのサーバからフロアハブまでの通信は基盤システム所管部門が管理する。フロアハブから以降の小規模なハブ、端末・プリンタまでの接続については、業務システムの所管部門や拠点の利用者が管理する。

また、各業務システムや基盤端末がネットワークを利用するために必要な各種サービスも情報共有基盤から提供される。

基盤ネットワークの拠点を表 4-1　基盤ネットワークの拠点に示す。

表 4-1　基盤ネットワークの拠点

拠点名	主な役割
北部データセンター	サーバ設置拠点
保守センター	システム開発・運用拠点
市庁舎	利用者拠点
市庁舎周辺ビル	利用者拠点
１８区役所	利用者拠点
４児童相談所	利用者拠点
障害者更生相談所	利用者拠点

基盤ネットワークの構成の概要を図 4-1　情報共有基盤ネットワーク概要図に示す。

なお、各機器は基本的に冗長構成になっているが、図上の表記は省略している。また、システム利用拠点や業務システムの要件に合わせた構成になっているため、一部機器構成が異なる部分がある。

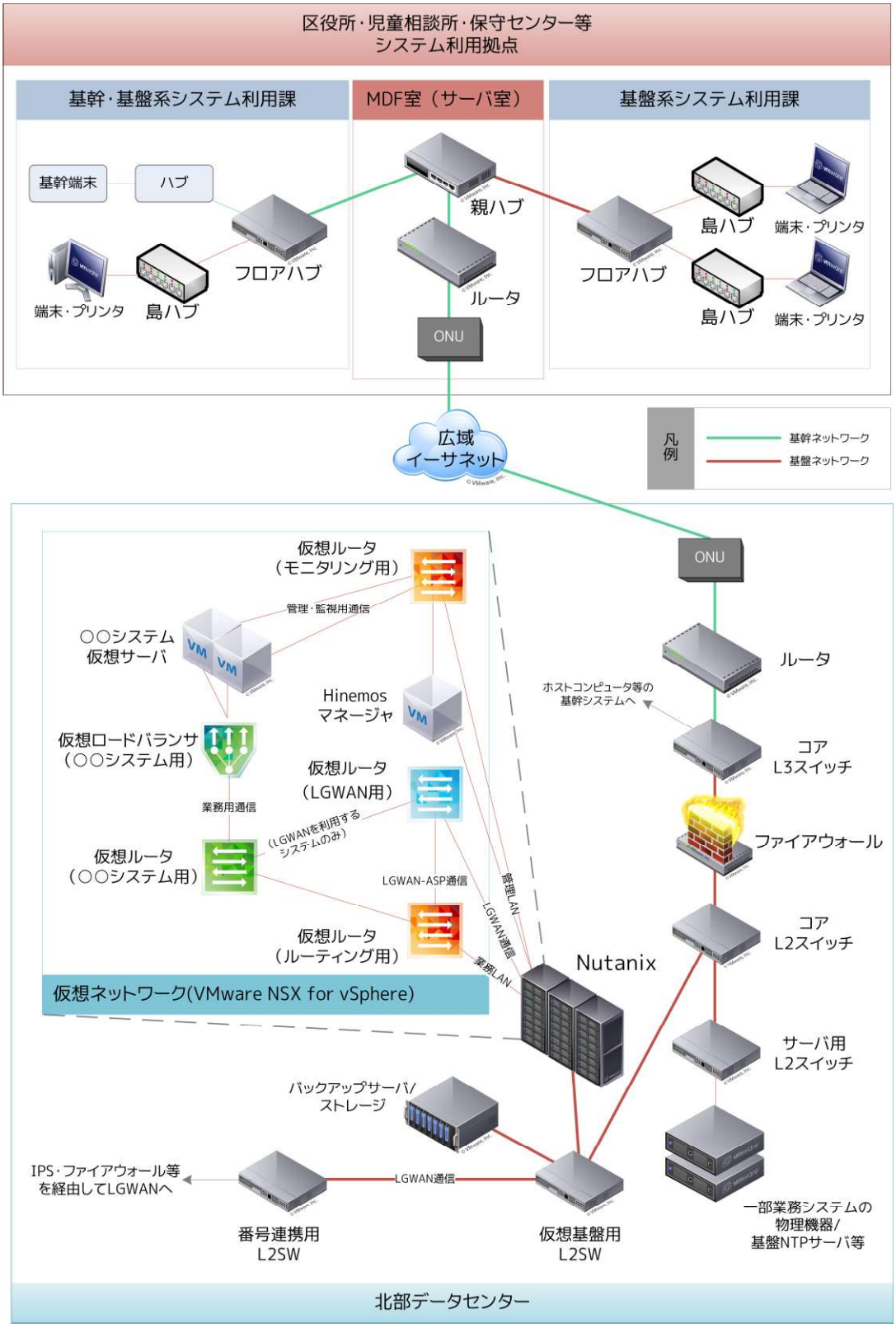

図 4-1　情報共有基盤ネットワーク概要図

(2) ネットワークサービスの概要

情報共有基盤は、基盤ネットワークを利用する各業務システム及び端末向けに、以下のサービスを提供する。

ア　情報共有基盤ドメイン

情報共有基盤では、Active Directory ドメインサービスによって icbs.kiban ドメインを運用している。icbs.kiban ドメインは単一のドメインであり、フォレスト内に他のドメインは存在しない。基盤端末は icbs.kiban ドメインに参加するため、端末の FQDN には icbs.kiban のドメイン名が使用される。

Active Directory で使用する機能については 5(2)ア　Active Directory で説明する。

イ　DHCP

端末・プリンタ等の機器に設定される IP アドレス、サブネットマスク、デフォルトゲートウェイ、機器が利用する DNS サーバの IP アドレス情報は、情報共有基盤の DHCP サーバから配布される。

DHCP サーバには、基盤システム所管部門に対して事前に利用申請をした機器の MAC アドレスと IP アドレスの組があらかじめ登録されている。機器側で DHCP を利用する設定にすることで、常にあらかじめ決まった IP アドレスが設定されるようになる。そのため、機器の故障により基板を交換し、MAC アドレスが変更になった場合は、基盤システム所管部門に登録変更の申請が必要である。なお、DHCP サーバは、登録されていない MAC アドレスを持つ機器に対しては IP アドレスを払い出さない。

また、機器を別の区役所に移設するなど、ネットワークセグメントを越えて機器を移設する場合は、機器の IP アドレスが変更になるため、基盤システム所管部門に登録変更の申請が必要である。

DHCP サーバは、北部 DC の Active Directory サーバ（正/副）と同居し、Active-Active 構成で冗長化されている。端末・プリンタ等の機器は、DHCP サーバ（正/副）に IP アドレス払い出しの要求を送信し、先に応答したサーバから IP アドレスの払い出しを受ける。

ウ　DNS

基盤 DNS サーバは、情報共有基盤ドメイン（icbs.kiban）の FQDN の名前解決を行う。

DNS サーバには、業務システムからの依頼により、サーバの正引き/逆引き/CNAME 等のレコー

ドが登録可能である。基盤ドメインに参加した端末・サーバのレコードには、DNS サーバの動的更新設定により、コンピューター名のFQDNと設定されたIPアドレスの対応が自動的に設定される。

DNS サーバは、北部 DC の Active Directory サーバ（正/副）と同居し、Active-Active 構成で冗長化されている。

エ　NTP

情報共有基盤では、基盤ネットワーク上の機器の時刻同期を行うために NTP サービスを運用している。

NTP サービスは、南部情報システムセンタの NTP サーバ（GPS タイプ）、北部 DC の NTP サーバ（セカンダリサーバタイプ）、Active Directory サーバ（正/副）によって提供されている。基盤 NTP サービスの階層構造を表 4-2　基盤 NTP サービスの階層構造に示す。どの機器のサービスを利用するかは、機器の設置場所と階層を勘案して選択する。

表 4-2　基盤 NTP サービスの階層構造

階層	サービス提供機器
Stratum 0	（米国国防総省 GPS 衛星）
Stratum 1	保守センター　NTP サーバ
Stratum 2	北部データセンター　NTP サーバ
Stratum 3	Active Directory サーバ（正/副）

(3) ネットワークセキュリティ

外部から持ち込まれた PC 等が勝手に接続され、データを窃取されるようなことがないように、許可のない端末は基盤ネットワークに接続できないような構成にしている。新たな端末を使用する場合には、基盤システム所管部門に対し申請を行い、許可を得る必要がある。

ア　機器接続制御

(2)イ　DHCP に記載のとおり、基盤 DHCP サーバは未登録の MAC アドレスの機器に IP アドレスを払い出さないため、未登録の機器には適切な IP アドレスが設定されず、ネットワークに接続できない。しかし、機器に IP アドレスを手動設定することで管理外の機器が基盤ネットワークに接続できてしまう可能性がある。そこで、IP アドレスが手動設定された機器の接続を防止するため、拠点側のスイッチングハブには DHCP スヌーピングに対応しているものを導入している。

DHCP スヌーピングとは、スイッチングハブが、機器（DHCP クライアント）と DHCP サーバの通信内容をのぞき見（snooping）し、DHCP サーバから IP アドレスの払い出しを受けていないにもかかわらず通信しようとする機器（IP アドレスが固定設定になっている等）のネットワーク接続を遮断する機能である。

上記の基盤 DHCP サーバの設定と DHCP スヌーピング機能の組み合わせにより、基盤ネットワークにはあらかじめ申請を受けてサーバ側に登録された MAC アドレスを持つ機器しか接続できない。

イ　基盤ファイアウォール

サーバ設置拠点である北部 DC には、端末側のネットワークとサーバの境界にファイアウォールを設置している。基盤ファイアウォールは、ファイアウォールを通過しようとするパケットの内容を確認し、アプリケーションレベルで通信を制御することが可能である。

基盤ファイアウォールは、全ての通信を禁止し、必要な通信のみを通過させるホワイトリスト方式を採用している。業務システムが北部 DC 内の基盤ネットワーク以外のセグメント（区役所の端末等）と通信を行う場合は、事前に業務システムの通信要件を整理し、基盤システム所管部門へ提出することで通信の許可を申請する必要がある。

ウ　認証局

基盤端末が業務システムと HTTPS 通信を行うために、ルート証明書及びサーバ証明書（自己証明書）を発行する OpenSSL による認証局を構成管理サーバ上で運用している。

ルート証明書は情報共有基盤ドメインのグループポリシーにより配布され、基盤の認証局は信頼されたルート証明機関として全基盤端末に登録される。各業務システムは、基盤の認証局にサーバ証明書の発行を依頼することができる。発行を依頼する際は、業務システムの FQDN のみを提示すればよい。発行に必要な秘密鍵・公開鍵、証明書署名要求（CSR）は認証局側で用意する。作成されたサーバ証明書は、証明書本体と秘密鍵のペアで各業務システムに受け渡す。このペアは原則として仮想基盤の仮想ロードバランサ上のみで用いるため、利用方法については 6(4)ア　仮想ロードバランサを参照すること。

(4) LGWAN 接続

基盤ネットワークは総合行政ネットワーク（LGWAN）に接続しているため、拠点の端末や仮想基盤内の仮想マシンから LGWAN-ASP サービスや自治体中間サーバー・プラットフォームにアクセス

可能である。

LGWAN への途中経路には、北部 DC の基盤ルータ及びファイアウォール、仮想基盤の仮想ルータ、侵入防止システム（IPS）、番号連携用ファイアウォール、LGWAN 用ファイアウォールが存在するため、新たに LGWAN と通信する際は各機器の管理部門との調整が必要である。

5 基盤端末

(1) 情報共有基盤端末の概要

基盤ネットワークに接続し、情報共有基盤や業務システムを利用する端末を情報共有基盤端末（以下、「基盤端末」という。）という。

情報共有基盤では、基盤端末に対して統一した端末統制（ポリシー配信）、セキュリティ対策、資産管理、資源配布の機能を提供するサービスを運用している。基盤端末の管理責任者は各業務システムの所管部門及び外部サービス（中間サーバー、LGWAN-ASP 等）を利用する事業の所管部門（以下、「各所管部門」という。）である。各所管部門は、情報共有基盤が提供する統一した設定と競合しない範囲で自由に端末の設定変更や、ソフトウェアのインストールを実施できる。

基盤端末を利用する各所管部門は、端末台数に応じた情報共有基盤利用料を負担する必要がある。

本章では、情報共有基盤が提供する基盤端末の管理機能について説明する。これらの一部のサービスはサーバでも利用可能である。

(2) 端末・ユーザー管理

ア　Active Directory の運用

情報共有基盤では独自のドメイン（icbs.kiban）を構築し、その運用に Active Directory を用いている。原則として全ての端末がこの独自ドメインに参加している。サーバのドメインへの参加は任意である。

ドメインに参加すると、ドメインユーザー及びグループが利用可能になる。基盤端末には、利用課ごとに割り当てたドメインユーザーを利用してログオンする。このドメインユーザーは Domain Users グループに属する標準ユーザーである。各所管部門が端末の設定変更等、管理者権限を必要とする作業を行う場合は、端末のセットアップ時に設定した、各所管部門で決めたパスワードを持つローカル管理者ユーザーを利用する。

Domain Users グループとは別に、業務システムごとに少なくとも 1 つのドメイングループを払い出す。後述する共有フォルダの利用権限は、原則としてこのグループに対して設定し、ユーザーには設定しない。これは、機構改革等による権限設定変更作業を必要最小限にするためである。

共有フォルダのアクセス権限を細かく制御したいなどの理由でドメイングループを追加したい場合は、基盤システム所管部門に依頼する。

ドメインユーザーで端末にログオンした場合、端末には情報共有基盤のグループポリシーが適用される。グループポリシーにより、全基盤端末には基盤認証局のルート証明書、OS や Internet Explorer の設定等、一元的に管理された設定が適用される。また、依頼により、任意のドメインユーザーに対して、業務システム側が作成した任意のログオンスクリプトを実行させることが可能である。

イ　資産管理

各所管部門は、IT 資産管理ソフトウェアである PalletControl（(株) JAL インフォテック）による資産管理機能を利用できる。

全基盤端末には PalletControl のクライアントソフトウェアがインストールされている。このクライアントソフトウェアは、Windows のログオン時に毎回 PalletControl サーバに対して資産情報を送信する。取得する主な資産情報を以下に示す。

- コンピューター名、ログオンユーザー名
- CPU 機種名・動作周波数（GHz)、メモリーサイズ（GB）
- IP アドレス、MAC アドレス
- Windows、Internet Explorer バージョン
- セキュリティパッチ適用状況
- インストール済みソフトウェア情報
- 登録済みプリンタ情報

ウ　ライセンス認証（KMS）

Windows クライアント OS 及び Microsoft Office 製品のライセンス認証作業の負担軽減のため、キー管理サービスの認証サーバ（KMS ホスト）を運用している。ボリュームライセンスの Windows 及び Office 製品は、DNS から KMS ホストを解決し、自動的にライセンス認証を行う仕組みになっている。

KMS ホストは、北部 DC の Active Directory サーバ（正/副）と同居し、Active-Active 構成で冗長化されている。端末は、基盤 DNS サーバに KMS ホストとして登録されている上記サーバの

FQDN に対して、定期的に OS と Office 製品のライセンス認証を要求する。Windows Server 用にはサービスを提供していないため、サーバ OS においては電話認証を行う必要がある。

エ　端末の導入

各所管部門が基盤端末を新規に導入する場合は、それぞれの業務システムの要求を満たす仕様及び基盤システム所管部門が用意する「基盤端末仕様書案」の仕様を満たした端末を調達する。また、「基盤端末に必要なソフトウェア等について」のドキュメントに基づいたソフトウェアを調達する必要がある。「基盤端末仕様書案」では、基盤端末に導入必須とされているソフトウェアが適切に動作する最低限の仕様を示している。

各所管部門は、「基盤端末化設定手順書」に従って、コンピューター名、ローカル管理者ユーザー、ドメイン参加及び KMS 認証の設定、利用禁止デバイスの無効化、更新プログラムの適用、基盤端末に導入必須とされているソフトウェアのインストールを実施する。また、マイナンバー利用事務で利用する場合は、二要素認証ソフトウェアを導入する必要がある。なお、二要素認証ソフトウェアとして、基盤を利用する業務システムの１つである顔認証システムを利用することもできる。

新たに端末をネットワークに接続する際には、端末の MAC アドレスと設置場所を提示することで基盤システム所管部門へ申請する必要がある。DHCP により端末に設定される IP アドレス及び端末に設定するコンピューター名はこの申請受付完了時に払い出される。また、プリンタについても同様の運用を行っている。

(3) 資源配布

情報共有基盤では、基盤端末に必要な OS の更新プログラム、外字フォント・外字変換辞書等の、配布して適用する必要がある各種資源を配信する資源配布基盤を運用している。また、資源配布基盤を用いて、各所管部門が、自ら作成した任意のスクリプトの配布・実行、ファイル配信等を基盤システム所管部門に依頼することができる。資源配布基盤には、資産管理機能と同様に PalletControl を用いている。

ア　外字の配信

住民記録や税務等の基幹システムから連携されたデータには Windows 標準のフォントでは表示できない横浜市独自の外字が含まれている。資源配布基盤は、この外字のフォント及び外字変換辞書を端末に配信して適用することで、業務システムやアプリケーション上で基幹システム外字の表示・入力ができるようにしている。

イ　任意のスクリプトの配信

各所管部門は、基盤システム所管部門への依頼により、各所管部門が管理する端末に対して、自ら作成した任意のスクリプトの配布・実行ができる。例として、業務システム端末へのプリンタドライバインストール・プリンタ登録、業務システムのクライアントソフトウェアの更新（ファイル配信）、ソフトウェアの修正プログラムの適用等が依頼により実施されている。

PalletControl では製品の公式ホームページにて資源配布に用いるスクリプトのサンプルを配布している。配布されているスクリプトの例を以下に挙げる。

- Microsoft Office、Acrobat Reader 等のインストール
- 権限がない先へのファイルコピー
- レジストリ書き込み
- 管理者権限でファイル実行
- メッセージを表示

サンプルスクリプトにはバージョン 6.3 用のスクリプトとバージョン 8 用のスクリプトの２種類が存在するが、基盤端末に導入されている PalletControl8 にはバージョン 6.3 用のスクリプトを実行するためのアドオンが付属しているため、両バージョンのスクリプトを利用できる。

(4) セキュリティ対策

基盤端末は個人情報を取り扱う業務で用いられることが多い。そのため、情報共有基盤では各種のセキュリティ対策ソフトウェアが利用できる仕組みを構築し、基盤ネットワーク上のすべての機器で統一したセキュリティ対策を実施している。

ア　ウイルス対策

情報共有基盤は、全基盤端末及びサーバ向けに、ウイルス対策ソフトウェアが利用できる仕組みを提供している。各所管部門が端末にウイルス対策ソフトウェアをインストールした後、最新のウイルスパターンファイル及びウイルス検出エンジンは、基盤システムの検証用端末及び全業務システムの開発用サーバに先行して適用した上で、数日後に全端末・サーバに自動的に配布される。

クライアントソフトウェアを利用する業務システムで、特定のフォルダを常時監視（オンアクセ

ススキャン）の対象外にする必要がある場合は、基盤システム所管部門へ申請が必要である。なお、Linux サーバの Oracle Database 領域についてはデフォルトで監視から除外されている。

ウイルス対策ソフトウェアには、基盤端末及び Windows Server 用に McAfee VirusScan Enterprise、Linux サーバ用に McAfee Endpoint Security for Linux を採用している。

ｲ　データ書き出し制限

個人情報を含むデータが端末の外部に持ち出されることを防ぐため、端末で利用できる USB メモリを制限するデータ保護ソフトウェアを導入している。データ保護ソフトウェアには McAfee DLP Endpoint を採用している。

基盤端末では、基盤システム所管部門に事前に申請してシリアル番号等を登録された USB メモリ（USB 接続の外部記憶媒体）のみが利用できる。未登録の USB メモリは読み込みもできない。USB ポートを経由せず媒体に直接書き出し可能な内蔵カードリーダ等が端末に搭載されている場合は、端末導入時に各所管部門で無効化する必要がある。

内蔵光学ディスクドライブにおいては、グループポリシーで書き込みを制限しており、読み込みのみ可能である。

WPD デバイスについてはグループポリシーにより書き込みを制限している。

(5) 共有フォルダ

情報共有基盤では、業務システムの利用者向けに共有ファイルサーバ（共有フォルダ）を運用している。ファイルサーバ内には各業務システムの単位で共有フォルダが作成されており、業務システム毎に割り当てられた共有フォルダのみ利用可能なようにアクセス制御されている。各システムの共有フォルダへのアクセス権限の付与は、(2)ア　Active Directory の運用に記載したドメイングループに対して行う。

6 仮想基盤

(1) 仮想基盤の概要

仮想基盤は、業務システム用の仮想サーバ及び仮想ネットワークを提供する仮想化サーバ基盤である。また、仮想基盤上のシステム向けの運用・監視及びバックアップ機能を提供している。

仮想基盤は、HCI アプライアンス・仮想化プラットフォーム・仮想ネットワークの組み合わせで構成されており、業務システムからの申請に基づき、仮想基盤保守事業者が仮想マシンを払い出すことで仮想サーバが利用可能になる。

仮想サーバの払い出しを受けた各所管部門は、利用リソースに応じた情報共有基盤利用料を負担する必要がある。

詳細については、別紙　「横浜市情報共有基盤システム仮想基盤　利用者ガイドライン」を参照すること。仮想基盤の利用イメージを図 6-1　仮想基盤の利用イメージに示す。

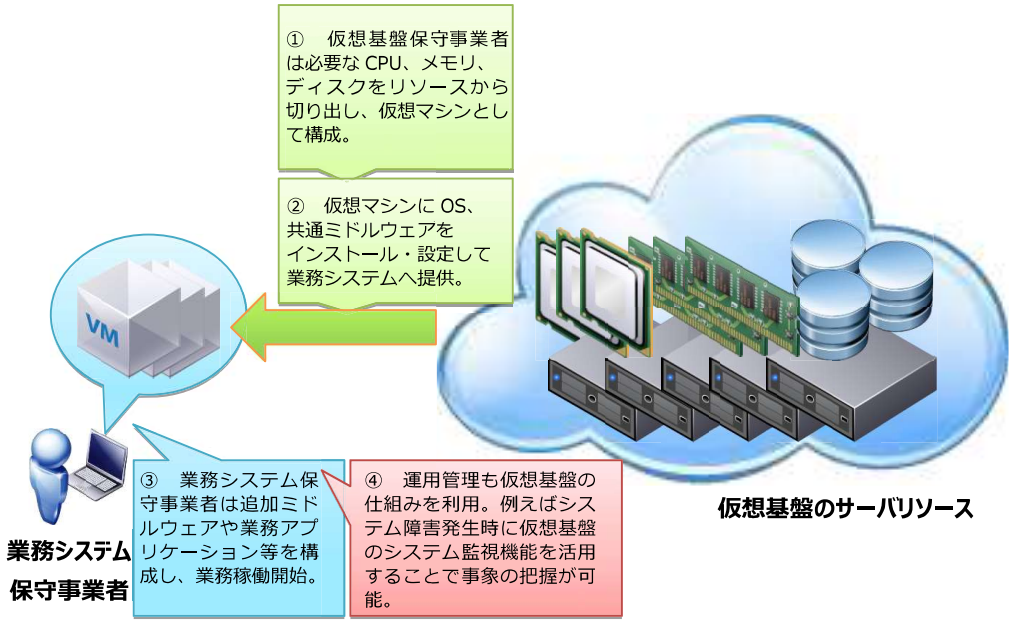

図 6-1　仮想基盤の利用イメージ

(2) HCI アプライアンス（Nutanix）

仮想基盤の機器には、ハイパーコンバージドインフラストラクチャ（HCI）と呼ばれるアプライア

ンスである Nutanix（ニュータニックス）を採用している。Nutanix（HCI）は、機器自体は一般的なサーバと同様であるが、Nutanix 専用のソフトウェア（OS）を搭載して機器の制御を行うことで、本来は別途用意するストレージ機器を必要とせずにサーバ及びストレージの機能を利用可能にしている。また、Nutanix の専用 OS は複数の Nutanix 筐体を横断してまとめて制御可能であり、１つの仮想マシンのデータを複数の筐体に分散して複製するため、仮想基盤においても高可用性を実現している。

注意点として、Nutanix で採用されている分散ファイルシステムの特性により、シングルスレッドかつブロッキング I/O 方式で実装した読み込み処理では、一般的なサーバの HDD に比べてスループットが低下する可能性がある。

(3) 仮想化プラットフォーム（VMware vSphere）

仮想基盤は、仮想化プラットフォームとして VMware vSphere を採用している。仮想マシンの動作環境としては、vSphere のハイパーバイザ製品である ESXi を使用している。ESXi を使用することで、複数の Nutanix 筐体をまとめたサーバ基盤上に、複数の仮想マシンを実行可能にしている。また、vCenter Server を用いて仮想マシンを管理しているため、各業務システムは vSphere Client を用いて仮想マシンの実行管理、スナップショットの取得、パフォーマンス監視等を行える。

仮想基盤では、vSphere が高可用性を保つ機能である vSphere HA（High Availability）を利用している。vSphere HA により、Nutanix または ESXi に障害が発生した際は、自動的に異なる Nutanix 上に仮想マシンを移動して再起動することで、業務システムの停止時間を最小限に抑えることができる。また、Nutanix や vSphere をメンテナンスする際は、手動で仮想マシンを無停止で別の Nutanix に移動することができる vMotion を利用して、基本的に業務システムを停止せずに仮想基盤側のメンテナンスを実行できる。

(4) 仮想ネットワーク（VMware NSX for vSphere）

仮想基盤上の仮想マシン間のネットワークは、ハイパーバイザ上に構築された VMware NSX for vSphere（以下、「NSX」という。）による仮想ネットワークである。仮想ネットワークでは、スイッチ、ルータ、ロードバランサ等のネットワークリソースも仮想化している。仮想基盤のスイッチは、分散スイッチと呼ばれるハイパーバイザの機能の一部として動作し、ルータ及びロードバランサについては、NSX Edge と呼ばれる個々の仮想マシン（仮想アプライアンス）としてハイパーバイザ上に存在する。

仮想ネットワークでは、仮想マシンの役割（Web/AP サーバ、DB サーバ等）や構成（ロードバランサ、LGWAN 等の利用）を考慮して、用途ごとにネットワークセグメントを定義している。

ア　仮想ロードバランサ

仮想基盤では、Web/AP サーバ等の負荷分散を実現するために、NSX の仮想ロードバランサ（Edge Load Balancer）を利用できる。

仮想基盤を利用する業務システムは、原則として業務システムのサーバ自体と端末間ではHTTPS通信を行わず、端末から見てサーバの手前側に設置された仮想ロードバランサと端末間で HTTPS 通信を行う。仮想ロードバランサには SSL アクセラレータ機能が存在するため、ロードバランサに基盤認証局が用意したサーバ証明書と秘密鍵を導入することで HTTPS 通信のデコードを行う。ロードバランサとサーバ間の通信は HTTP 通信となるため、ロードバランサを経由する構成ではサーバ側へのサーバ証明書の導入は不要である。

(5) 運用管理（Hinemos）

仮想基盤は、Hinemos（(株) NTT データ）によるジョブ管理・状態監視機能を持つ。各業務システムは、仮想サーバに Hinemos エージェントを導入することで、ブラウザから Hinemos Web クライアントを利用して仮想マシンの運用管理を行うことができる。

Hinemos のジョブ管理機能では、業務システムのジョブネットを定義し、登録することで、業務システムのジョブのスケジュール化及び実行結果の管理ができる。また、後述の業務システムのバックアップポリシーも、１つのジョブとしてスケジュール化ができる。

Hinemos の状態監視機能では、業務システムの仮想マシンの各種状態・情報・ジョブ実行結果の監視が可能である。各業務システムにおける Hinemos への監視項目の追加は、業務システムから基盤システム所管部門への申請に基づいて仮想基盤保守事業者が行う。仮想基盤の Hinemos における主な監視項目を以下に示す。

- PING 監視、サービス・ポート監視
- システムログ、イベントログ、ログファイル監視
- リソース監視
- プロセス監視

- Windows サービス監視
- ジョブ監視

(6) バックアップ機能（NetBackup）

仮想マシンのバックアップ処理には JP1/VERITAS NetBackup ((株)日立製作所) を採用している。各業務システムは、仮想基盤保守事業者が提供する、仮想マシンへのバックアップ設定サービスを利用する形でバックアップポリシーを作成し、バックアップ/リストアを実施できる。また、バックアップポリシーの実行を自動化する場合は、必要なスクリプト等を各業務システム側で作成する必要がある。

バックアップの取得単位は仮想マシン単位であるが、リストアは仮想マシン単位及びファイル単位で実施できる。また、本番環境のバックアップデータのうち、一定容量内のデータについては、申請に基づいて二次バックアップとして LTO テープへ書き込まれ、災害対策として遠隔地に保管することができる。

7 SSO システム

情報共有基盤は、利用者の利便性の向上及び業務システムの実装コストの削減を目的として、認証及びアクセス制御の共通化を実現するエージェント型のシングルサインオン（Single Sign-On, SSO）による認証システムを運用している。SSO システムは、利用者ごとにアカウントを発行し、利用者を認証する機能を提供する。利用者の所属組織ごとに業務システムの URL 単位のアクセス可否を制御することができる。

業務システムに SSO クライアントを組み込むことで業務システム独自の認証機能が不要となるが、業務システム自体へのアクセス可否以外の権限を制御する場合（例えば、更新権限を持つ利用者だけに項目の入力を許可する場合）には、業務システム側での作り込みが別途必要である。この際に使用する情報（職員や所属の情報など）は SSO システムから取得できる。

なお、8 基盤ポータルを利用するためには、SSO システムの利用が必須となる。

SSO システムを利用するにあたっての技術的制約については、添付の別紙『SSO システム_連携方式の概要』を参照すること。

詳細は、業務システム開発事業者へ提供する（システム発注段階においては閲覧に供する）『SSO システムユーザーズガイド』を参照すること。

8 基盤ポータル

基盤ポータルは、SSO ユーザが利用可能な複数の業務システムへのリンクを表示するポータルサイトである。各業務システムにアクセスするための URL へのリンクと、情報共有基盤及び各業務システムから利用者に対してのお知らせ情報が表示されている。業務システムがポータルへのリンク及びお知らせの追加を希望する場合は、基盤システム所管部門に依頼する必要がある。

基盤ポータルの画面イメージを図 8-1　基盤ポータル画面に示す。

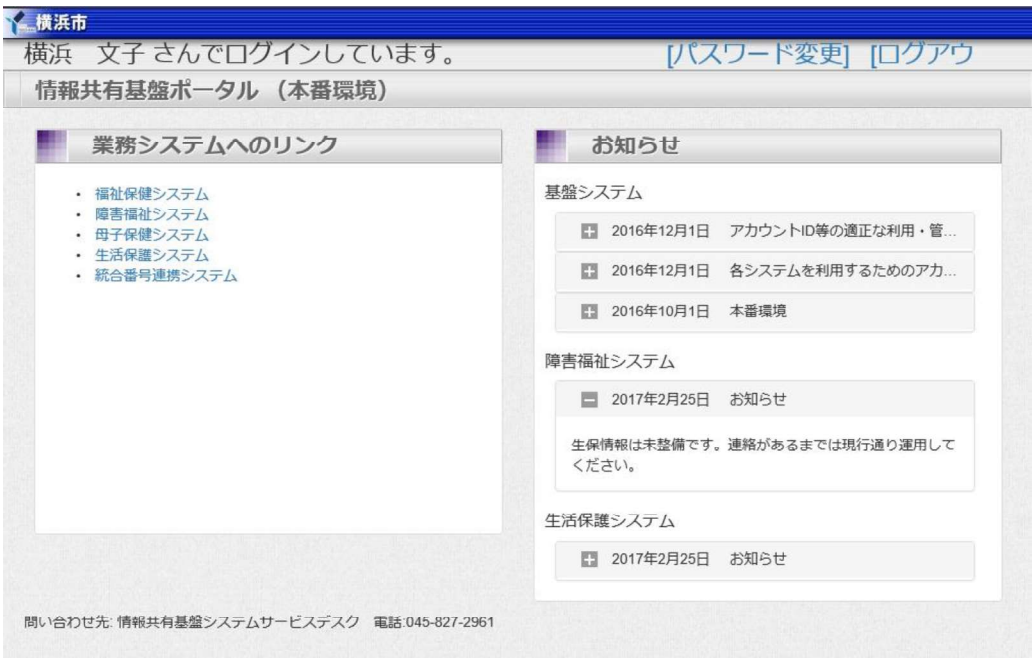

図 8-1　基盤ポータル画面

9 基盤連絡受付データベース

基盤システム所管部門への連絡、問い合わせ及び依頼は、Redmine による基盤連絡受付データベースにチケットを起票する。

基盤連絡受付データベースの画面イメージを図 9-1　基盤連絡受付データベースに示す。

図 9-1　基盤連絡受付データベース

10 帳票基盤

情報共有基盤は各業務システム向けに帳票出力機能を提供するため、共通の帳票基盤を運用している。各業務システムはこの帳票基盤を利用して帳票を作成及び出力することができる。

帳票ソフトウェアはウイングアーク 1st 社の SVF を導入している。導入している製品パッケージは下記の通り。

- SVF Connect SUITE Standard（旧名「Universal Coonect/X」）
- SVF for PDF
- SVF for Java Print
- SVF for Web/Client

11 データ連携基盤

業務システム同士がファイルを用いたデータ連携を行う際の中継点として、データ連携基盤を利用することができる。データ連携基盤は、ファイル送受信及び文字コード変換の機能を備えている。

業務システムは、データ連携基盤が備えるファイル転送ソフトウェアである HULFT ((株)セゾン情報システムズ）または共有フォルダ（Windows ファイル共有）を利用して、ファイルの送受信をすることができる。データ連携基盤の利用例を図 11-1　データ連携基盤利用の例に示す。

詳細については、別紙　「データ連携基盤概要」を参照すること。

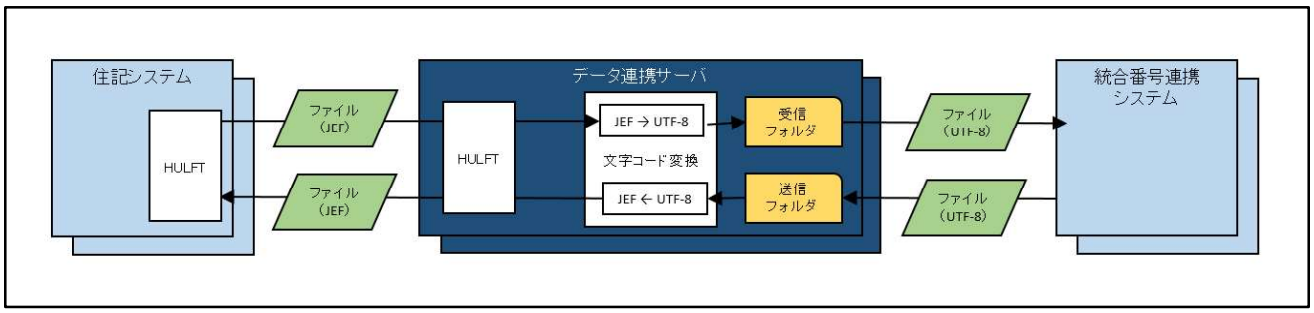

図 11-1　データ連携基盤利用の例

(1) 文字コード変換

業務システムは、データ連携基盤が備える文字コード変換の機能を利用することで、他業務システムに合わせた異なる文字コードのファイルを連携することができる。変換可能な文字コードは表 11-1　変換可能な文字コードのとおりである。なお、JEF 及び Unicode には横浜市独自の外字が登録されており、相互に変換が可能である。

データ連携基盤が行うのは文字コードの変換のみであり、可変長/固定長などのレイアウト変換は行わない。

表 11-1　変換可能な文字コード

	JEF に変換	Unicode（UTF-8/16/32）に変換	Shift-JIS に変換
JEF から		・外字の変換が可能。 ・PACK 形式のバイト列は変換不可。 ・マルチバイト文字列の前後にシフトコードを付加すること。 ・UTF-8 への変換後は、BOM なしとなる。 ・UTF-16/32 への変換後は、BOM 付となる。	・外字の変換は不可。 ・JEF から Unicode に変換したのち、Shift-JIS に変換する。（2 段階）
Unicode（UTF-8/16/32）から	・外字の変換が可能。 ・変換後はマルチバイト ・PACK 形式のバイト列への変換は不可。 ・文字列の前後にシフトコードが付加される。 ・UTF-8 は BOM なしとすること。 ・UTF-16/32 は BOM 付とすること。		・外字の変換は不可。
Shift-JIS から	・外字の変換は不可。 ・Shift-JIS から Unicode に変換したのち、JEF に変換する。（2 段階）	・外字の変換は不可。	

12 用語集

初出ページ	用語	意味
8	シングルサインオン（Single Sign-On）	一度ユーザ認証に成功することで、独立した複数のシステムが利用可能になる特性のこと。
11	LGWAN（総合行政ネットワーク）	地方公共団体を相互に接続する行政専用のネットワーク。このネットワーク上に LGWAN-ASP や自治体中間サーバー・プラットフォームが存在する。
11	基幹（システム・端末・ネットワーク）	ホストコンピュータ上で稼働している業務システム（住民記録、税務、国保等）の総称。また、それらを利用するための端末及びネットワーク。
15	自治体中間サーバー・プラットフォーム	マイナンバー制度における情報連携等を行うために、連携の対象となる個人情報を管理するサーバ。各機関間の連携における中継点となる。
21	WPD デバイス（Windows Portable Device）	Windows における、接続した携帯電話、カメラ等のポータブルデバイスと通信するためのデバイスの認識種別。WPD デバイスとして認識されると、USB メモリと同様に、ポータブルデバイスの記憶域にデータの書き込みができる。
22	アプライアンス	機器と専用のソフトウェアがセットになっているなど、特定の機能に特化した機器の総称。
23	ブロッキング I/O	I/O のスレッド処理において、スレッドがリクエストを処理している間は他のリクエストが割り込まない方式のこと。一方、スレッドがリクエストを処理している間の I/O 待ち時間を活用して他のリクエストを処理することをノンブロッキング I/O という。
30	JEF（JEF 漢字コード）	富士通が策定した文字コード。基幹システムではデータを主に JEF 形式で保持している。Windows 上で文字を読むためには変換が必要になる。
31	BOM（byte order mark）	Unicode で符号化したテキストにおいて先頭に付与される、UTF-8/16/32 のどの形式で符号化しているか判別するためのデータ。