DMZ は、必要に応じて、複数設置し、それぞれの機能を明確にすること。

イ．DMZ は、少なくとも二重構成とし、インターネット接続用とインターネットサービス提供用とで、別々の DMZ を構成すること。

ウ．以下に示す個別サービスは、国民向けサービスとしてインターネットに公開すること。また、インターネットサービス提供 DMZ に設置し、セキュリティ上の対策を確実に行うこと。

A. 厚生労働省ホームページサービス
B. アクセシビリティ改善ソフトウェアサービス
C. 厚生労働省総合統計データベースサービス
D. ホームページ検索サービス
E. 厚生労働省法令等データベースサービス
F. 厚生労働省白書等データベースサービス
G. 厚生労働省図書館サービス
H. 都道府県・市区町村のすがたサービス
I. マルチキャリア対応携帯Ｗｅｂサービス
J. 動画配信サービス
K. メール配信サービス
L. 地方厚生局ホームページサーバ
M. 労働経済動向調査オンラインシステム

エ．上記 H～K のサービスについては、アプリケーション・サービス・プロバイダーの利用も可能とする。

オ．上記 L 及び M のシステムは、連携するシステムが 5 号館内に設置されているため、同様に 5 号館内に設置すること。

カ．インターネットでの電子メールの利用は、利用者数が最大約 4 万 3 千人となるため、インターネット転送用のメールサーバは、十分な性能、インターネット接続回線は十分な帯域を確保すること。

キ．インターネットに公開する外部ＤＮＳサーバを設置し、名前解決を行うこと。

ク．メンテナンスの容易性を考慮し、DMZ を複数設置した場合においても、インターネットの接続口は、複数とせず、1 箇所に集約すること。

ケ．耐障害性を考慮し、インターネット接続環境では、機器及び回線の冗長化を図り、一方の機器、または、一方の回線の障害が発生した場合でも、不通とならない通信経路を確保すること。また、調達する回線の負荷分散を図ること。

コ．セキュリティの観点より、国民へのサービスの提供に当たっては、リバースプロキシ／キャッシュ装置を経由したアクセスのみとし、Ｗｅｂサーバ等の直接公開を行わないこと。

(3) IPv6 要件

「3.3.1IPv6 対応」に示すとおり、次期ＮＷシステムでは、国民が利用する個別サービスを主として、IPv6 によるサービスが提供できる状態とする。

サービスの提供に当たっては、以下に示す要求仕様を満たすこと。

ア．基本要件

A. IPv6 の環境を構築する個別サービス、ネットワーク機器、及びサーバに関しては、IPv4・IPv6 デュアルスタックによる通信サービスが可能な機器を提供すること。ただし、アプリケーションの構造上の理由等で IPv4・IPv6 デュアルスタック方式を採用できないものについては、トランスレータ等での代替方式の使用を認めるが、その場合、IPv4・IPv6 デュアルスタック方式を採用できない理由を明確にし、事前に担当職員の承認を得ること。

B. 以下に示すインターネットサービス提供 DMZ 内の個別サービスについては、IPv4・IPv6 によるサービスの提供ができる状態とすること。

① 厚生労働省ホームページサービス
② アクセシビリティ改善ソフトウェアサービス
③ 厚生労働省総合統計データベースサービス
④ ホームページ検索サービス
⑤ 厚生労働省法令等データベースサービス
⑥ 厚生労働省白書等データベースサービス
⑦ 厚生労働省図書館サービス
⑧ 都道府県・市町村のすがたサービス
⑨ マルチキャリア対応携帯Ｗｅｂサービス
⑩ 動画配信サービス
⑪ メール配信サービス

C. 省内のインターネットサービス提供 DMZ 内のシステムは、国民向けシステムであるが、本調達外であるため、「厚生労働省 IPv6 移行計画（仮称）」に示される内容を踏まえ、当該システムの運用保守業者と調整の上、対応すること。

D. 以下に示すインターネット接続 DMZ 内のサーバは、IPv6 によるインターネットサービスの提供が可能な機器を提供すること。

① 外部ＤＮＳサーバ
② 外部メールサーバ

E. 以下に示すインターネット接続環境内のすべてのネットワーク機器は、IPv6 によるサービスの提供が可能な機器を提供すること。

① ルータ
② L2・L3 スイッチ
③ ファイアウォール
④ IDS／IPS

⑤ ロードバランサー

⑥ サーバ・ネットワーク監視機器

⑦ その他必要なネットワーク機器

F. インターネット・サービス・プロバイダーは、IPv6 に対応するプロバイダーを利用すること。

G. 上記の A に示す個別サービスについては、フロントエンドに位置する機能は必ず IPv6 に対応する必要があるが、IPv6 でのサービス提供に支障がない限り、フロントエンドと連携するバックエンド側の機能については、必ずしも IPv6 に対応する必要はない。

H. IPv4・IPv6 機器が混在する環境におけるリスク整理と評価（正常系及び異常系の通信、暗号化機能、セキュリティ関連機能、ルーティング機能等）を行うこと。

I. IPv4・IPv6 の環境の差異を明確に整理すること。

J. 当省の指示により、IPv6 によるサービスを提供する際は、IPv6 通信を想定していない通信回線について、IPv6 通信の有無を監視し、IPv6 通信が検知された際に、通信している機器を特定し、IPv6 通信を遮断するための措置を講ずること。

イ．IPv6 セキュリティ要件

当省の指示により、IPv6 によるサービスを提供するに当たり、以下に示すセキュリティ要件を満たすこと。

A. インターネット接続環境からＮＷシステム内の他の環境への IPv6 のパケットは、ファイアウォールにて遮断すること。

B. ICMPv6 では、異常なパラメータ追加による大量のエラーメッセージを誘導したり、ＬＡＮに接続する端末のすべてのＩＰアドレスを調べられてしまったりする恐れがあること及び ICMPv6 で記載されていない問題があることを考慮し、ファイアウォールにて不正なパケットを閉鎖できる仕組みとすること。

C. IPv6 では、原則、ＮＡＴは利用されないため、IPv4 のような副次的なセキュリティの向上は発生しない。このため、ネットワークの保護を目的として適切なパケット管理・制御を行う仕組みとすること。

D. インターネット接続のルーティングについて、外部へダイナミック・ルーティングをする場合、リンクローカルアドレス、または、ULA（一意ローカル IPv6 ユニキャストアドレス）をアナウンスさせない仕組みとすること。

E. インターネット接続のルーティングについて、既存の IPv4 対応ファイアウォールのポリシーと同様のレベルのフィルタリングを IPv6 環境でも設定すること。

F. インターネット接続のルーティングについて、ソースアドレスが不適切な場合は、フォワーディングしないこと。また、マルチホーム（複数 ISP 接続)では、

原則として、上流インターフェースのアドレス設定を適切に行うこと。

G. インターネット接続のルーティングについて、IPv4 射影アドレスのフィルタリングを適切に実施すること。

H. 外部との通信を制限する場合には、フィルタリング機能が有効となるが、IPv6 プロトコルの仕様上、意図的に他の端末を経由して通信を行うことで、フィルタリング設定の逃げ道を使われてしまう恐れ（Routing Header 及び Mobile IPv6）があるため、悪意のあるパケットが侵入しないように十分配慮した仕組みとすること。

I. IPv6 への移行技術として使われるトンネリング技術により、ＮＷシステムで利用されるクライアントＰＣが外部のサーバとの間にトンネルを自動的に生成する可能性及び生成されたトンネル内部をファイアウォールのチェックなしにパケットが通過する可能性があるため、結果的に、セキュリティホールが生じることが想定される。従って、確実にトンネルの機能を停止する仕組み、または、ファイアウォールを用いて、トンネルの設置を阻止する仕組みを確立すること。

J. IPv6 サーバセグメントでの ICMPv6 フラグメント処理は、中間ノードでは行わず、Path MTU Discovery（ICMPv6 type2 メッセージを使用）により、送信元端末が配送可能なサイズに分割するため、途中のルータ及びファイアウォールで ICMPv6 type2 メッセージをフィルタしないこと。

ウ．IPv6 運用要件

当省の指示により、IPv6 によるサービスを提供するに当たり、以下に示す運用要件を満たすこと。

A. 各 DMZ 内の個別サービスへのコンテンツのアップロード等については、IPv4 とすること。

B. IPv6 アドレスの取得は当省で行うが、ＩＰアドレスに関する申請手続き、管理方法等について、支援を行うこと。

C. ＩＰアドレス使用状況の把握と経路管理等の情報を整理・管理すること。

D. ＩＰアドレス割り当て、再割り当てを行う際、JPNIC で提供されているデータベースへの適切な登録を担当職員と協議の上、実施すること。

E. ＩＰアドレスの追加割り振り申請は当省で行うが、RFC3194 の推奨に従い、Host-Density Ratio（ＩＰアドレスの割り当て効率を表す指標）を 0.8 とした場合の利用率を満たした時点で追加申請を行うことができる。このため、ＩＰアドレスの使用状況を把握し、JPNIC で提供されているデータベースへの適切な登録を担当職員と協議の上、実施すること。

F. 割り振られた IPv6 アドレス空間に対する逆引きルックアップゾーンを適切に管理すること。

G. 当省において、ＩＰアドレスを管理する場合は、ＩＰアドレス取得に伴い、2

年以内に最低でも「200 の／48」の割り当てを行う計画をすること。ただし、政府が共通的に管理しない場合に限る。

(4) セキュリティ要件

ア．インターネット接続環境とインターネット間、インターネット接続環境とＮＷシステム内の他環境間には、ファイアウォールを設置することにより、インターネットからのアクセスを制限することで、セキュリティを確保すること。

イ．それぞれの DMZ では、ネットワーク型 IDS を導入、かつ不正アクセス等の通信を検知し、収集すること。

ウ．インターネットへの電子メールの送受信において、ウィルスの検知と駆除を行うこと。

エ．DMZ 上に設置されるサーバ及びネットワーク機器等のアクセスログは、「11.5 ログ管理」に従い収集、分析ができること。

オ．DMZ 上に設置されるサーバ及びネットワーク機器等のアクセスログは､アクセスログ管理・統計サービスで集中管理を行い、かつ月次でログのバックアップを取得し、担当職員へ提出すること。

カ．特定のクライアントＰＣから､DMZ 上のサーバ群へセキュリティレベルを低下させることなくコンテンツアップロード等が行えること。この場合、サーバへのアクセス制限を設けると同時に、通信の暗号化も実施すること。

キ．その他のセキュリティについては、「11.情報セキュリティ」を参照し、必要な対策を行うこと。

(5) インターネット接続用 DMZ

ア．機能要件

A. インターネットへの電子メール送受信を行えること。

B. インターネットへのメール送信等のための名前解決､国民向けサービスに対する名前解決の問合せに対応できること。

イ．機器構成要件

以下の各システムを設置すること。

A. 外部メールサーバ

① 機能要件

- 電子メールの送受信機能を有すること。

② ソフトウェア要件

- ＮＷシステム標準ＯＳを使用すること。
- SMTP サーバとして最新の「SendMail」及び「qmail」と同等以上の機能を有すること。
- IPv6 に対応していること。

B. 外部ＤＮＳサーバ

① 機能要件

- 名前解決の機能を有すること。

② ソフトウェア要件

- ＮＷシステム標準ＯＳを使用すること。
- ＤＮＳサーバとして最新の「BIND」と同等以上の機能を有すること。
- IPv6 に対応していること。

C. メール対策サーバ

① 機能要件

- 「11.2.1 ウィルス対策」を参照のこと。
- 「11.2.4 メール対策」を参照のこと。

② ソフトウェア要件

- ＮＷシステム標準ＯＳを使用すること。なお、アプライアンスを使用する場合はこの限りではない。

ウ．運用要件

外部メールサーバでは、受信及び送信された電子メールに関する統計情報を日報として提出すること。また、統計情報には、メールの送受信統計・配送先との接続タイムアウト統計を取得すること。

(6) インターネットサービス提供用 DMZ

ア．機器構成要件

以下のネットワーク機器及び個別サービスの環境を設置すること。

A. リバースプロキシ／キャッシュ装置

① 機能要件

- インターネットからのリクエストの中継機能を有すること。
- その他機能は、「12.8.2（7）リバースプロキシ／キャッシュ装置」を参照のこと。

② ハードウェア要件

- アプライアンス製品を導入すること。

B. 厚生労働省ホームページサービス

「18.1 厚生労働省ホームページサービス」を参照のこと。

C. アクセシビリティ改善ソフトウェアサービス

「19.4 アクセシビリティ改善ソフトウェアサービス」を参照のこと。

D. 厚生労働省総合統計データベースサービス

「18.4 厚生労働省総合統計データベースサービス」を参照のこと。

E. ホームページ検索サービス

「19.5 ホームページ検索サービス」を参照のこと。

F. 厚生労働省法令等データベースサービス

「18.7 厚生労働省法令等データベースサービス」を参照のこと。

G. 厚生労働省白書等データベースサービス

「18.5 厚生労働省白書等データベースサービス」を参照のこと。

H. 厚生労働省図書館サービス

「18.8 厚生労働省図書館サービス」を参照のこと。

I. 都道府県・市区町村のすがたサービス

「18.3 都道府県・市区町村のすがたサービス」を参照のこと。

J. マルチキャリア対応携帯Ｗｅｂサービス

「19.2 マルチキャリア対応携帯Ｗｅｂサービス」を参照のこと。

K. 動画配信サービス

「19.3 動画配信サービス」を参照のこと。

L. メール配信サービス

「19.1 メール配信サービス」を参照のこと。

イ．運用要件

A. 各サーバで出力される syslog・アプリケーションログ等については、アクセスログ管理・統計サービスへ、指定日時に自動転送できること。

B. ホームページメンテナンス用 VPN ルータを設置すること。

(7) 5 号館内インターネットサービス提供用 DMZ

ア．機器構成要件

以下の各システムを設置すること。

A. 地方厚生局ホームページサーバ

B. 労働経済動向調査オンラインシステム

イ．運用要件

A. 上記「ア」の各システムは調達対象外のため、各サーバを接続するポートを準備し、必要なファイアウォールの設定を行うこと。

B. 省内各課室が、独自にインターネットに公開している国民向けサービスのシステムを、5 号館内インターネットサービス提供用 DMZ に移設する予定であるため、必要に応じ、ポートの準備、ファイアウォールの設定変更を行うこと。

14.2.2 外部接続環境

(1) システムの概要

共通サービスを 5 号館以外の利用機関に提供する窓口であり、また、他省庁、省外組織との接続点となるため、接続先別に DMZ を設け、セキュリティの強化を図る。DMZ は図 14-4 に示すとおり、共通サービス DMZ、霞が関 DMZ、及び WISH DMZ に分割す

る。

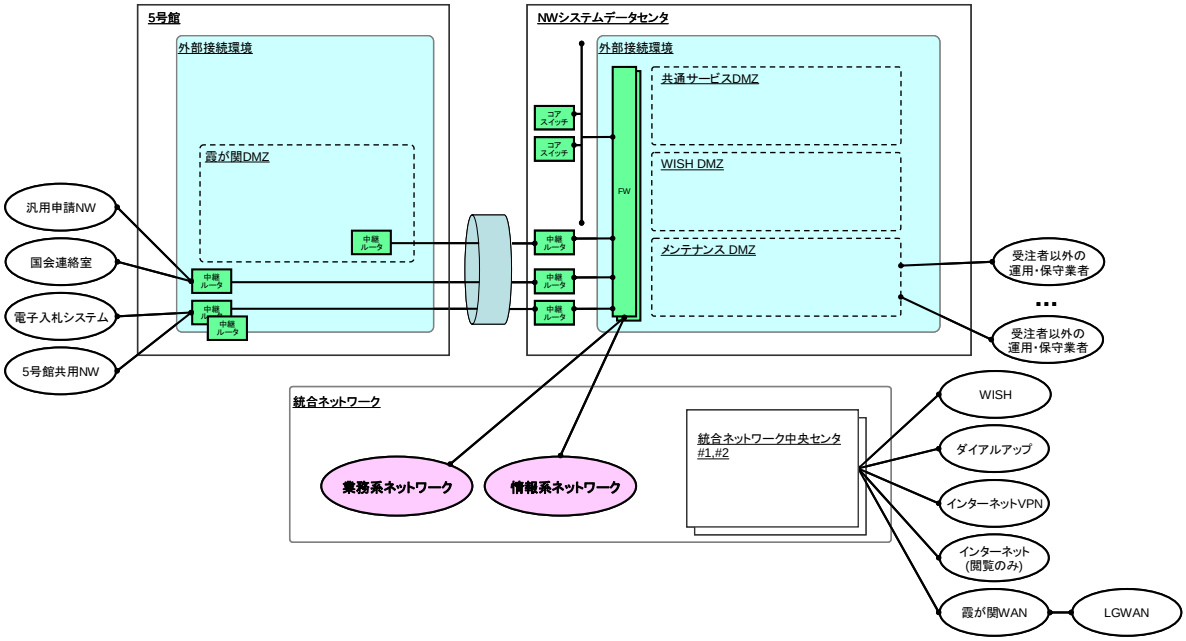

図 14-4　外部接続環境構成イメージ

(2) 基本要件

ア．外部接続環境では、設置する個別サービスの接続別に DMZ を構成し、各接続先とＮＷシステム間のすべての通信は、原則、DMZ 経由で行うこと。

イ．以下の外部ネットワークと接続すること。

A. 統合ネットワーク（ＷＩＳＨ接続、霞が関ＷＡＮを含む）

B. ５号館内を接続する共用のネットワーク

C. 国会連絡室のネットワーク

D. 電子入札システムのネットワーク

ウ．上記 B～D の各外部ネットワークは、現状で、5 号館にて回線を接続している。原則として、この回線の接続先の変更は行わないため、外部接続環境をＮＷシステムデータセンタに設置する場合は、別途ＮＷシステムデータセンタと５号館を接続する回線を敷設すること。

(3) セキュリティ要件

ア．外部接続環境と本省外組織及び外部接続環境とＮＷシステム内の他環境間には、ファイアウォールを設置し、本省外組織からのアクセスを制限することで、セキュリティを確保すること。

イ．すべての DMZ において、ネットワーク型 IDS を導入、かつ不正アクセス等の

通信を検知し、収集すること。

ウ．DMZ 上に設置されるサーバ及びネットワーク機器等のアクセスログは、「11.5 ログ管理」に従い収集、分析ができること。

エ．DMZ 上に設置されるサーバ及びネットワーク機器等のアクセスログは､アクセスログ管理・統計サービスで集中管理を行い、かつ月次でログのバックアップを取得し、担当職員へ提出すること。

オ．その他セキュリティについては、「11.情報セキュリティ」を参照し、必要な対策を行うこと。

(4) 移行・導入要件

外部接続環境に設置される個別サービスは、特別な機能変更を行うことなく、現行ＮＷシステムの機能及び必要なデータをすべて継承させ、正常に動作させること。

(5) 運用要件

ア．セキュリティ対策のため、ファイアウォール等の設定変更が生じた場合、担当職員の指示により、必要な作業を行うこと。

イ．担当職員の要求により、外部接続環境に外部連携システムが追加される場合、ファイアウォール等の必要な調整及び設定作業を行うこと。

(6) 共通サービス DMZ

統合ネットワーク経由でメール､ポータル等の基本サービスに接続するための中継機能を提供すること。また、図 3-1 に示す、統合ネットワークで提供される、名前解決、時刻同期、インターネット閲覧機能を中継し、ＮＷシステム内のメールサーバ、ＤＮＳサーバ、ＮＴＰサーバ、及びプロキシーサーバと連携すること。

(7) WISH DMZ

ＷＩＳＨは、2008 年（平成 20 年）1 月にＷＩＳＨサービス用のデータセンタへ移行し、現行ＮＷシステムで外部接続環境に接続していた回線は、統合ネットワークの外部接続環境への移行を予定している。従って、ＷＩＳＨは引き続き次期ＮＷシステムにおいても、統合ネットワーク経由で接続されることとなる。当該システムの機能、移行・導入要件等については、「18.2　厚生労働行政総合情報サービス（ＷＩＳＨ）」を参照すること。

現行ＮＷシステムで利用できる機能が､引き続き次期ＮＷシステムにおいても利用できるようにすること。

(8) 霞が関 WAN 用 DMZ

霞が関ＷＡＮは、2009 年（平成 21 年）7 月に、現行ＮＷシステムで接続していた回線を統合ネットワークに移設する予定である。次期ＮＷシステムにおいても引き続き霞が関ＷＡＮを利用するため、霞が関 WAN 用 DMZ を５号館内に設置し、移行する必要がある。霞が関ＷＡＮの詳細については、霞が関ＷＡＮ規程集及び霞が関ＷＡＮ利用ガイドを参照のこと。

現行ＮＷシステムで利用できる機能が、引き続き次期ＮＷシステムにおいても利用できるようにすること。

(9) メンテナンス用 DMZ

コンテンツ掲載業務等、受注者以外の運用・保守業者が、運用・保守作業時にＮＷシステム内のサーバにアクセスする際のセキュリティを確保するため、次期ＮＷシステムにおいては、受注者以外の運用・保守業者からのアクセス経路を一元化する目的でメンテナンス用 DMZ を設置する。当該 DMZ の構築に当たっては、以下に示す要件を満たすこと。

ア．サーバを既存の設置環境からメンテナンス用 DMZ へ移設し、アクセス経路を切り替える際は、関連する個別サービスの利用状況を調査し、担当職員及び受注者以外の運用・保守業者と、テスト項目、役割分担、及びスケジュール調整の上、疎通確認及び接続テストを行うこと。

イ．メンテナンス用 DMZ におけるサーバ及びネットワーク機器等については、「11.2.3 暗号化」に示す暗号化を実施すること。

ウ．作業記録サーバを設置し、HTTPS、SFTP、及び SSH 等のプロトコルを中継することにより、作業日、作業対象サーバ、作業内容、及び作業実施者等の項目を記録できる仕組みとすること。

エ．次期ＮＷシステム外部より、メンテナンス用 DMZ に接続するためのルータ及びネットワーク回線は、受注者以外の運用・保守業者が準備することとするが、ルータを収容するためのスイッチ及びルータとスイッチを接続する回線については、受注者の負担において、準備・接続すること。

14.2.3 内部システム環境

(1) システムの概要

内部システム環境は、ＮＷシステムの基盤となるネットワークである。概要を図 14-5 に示す。

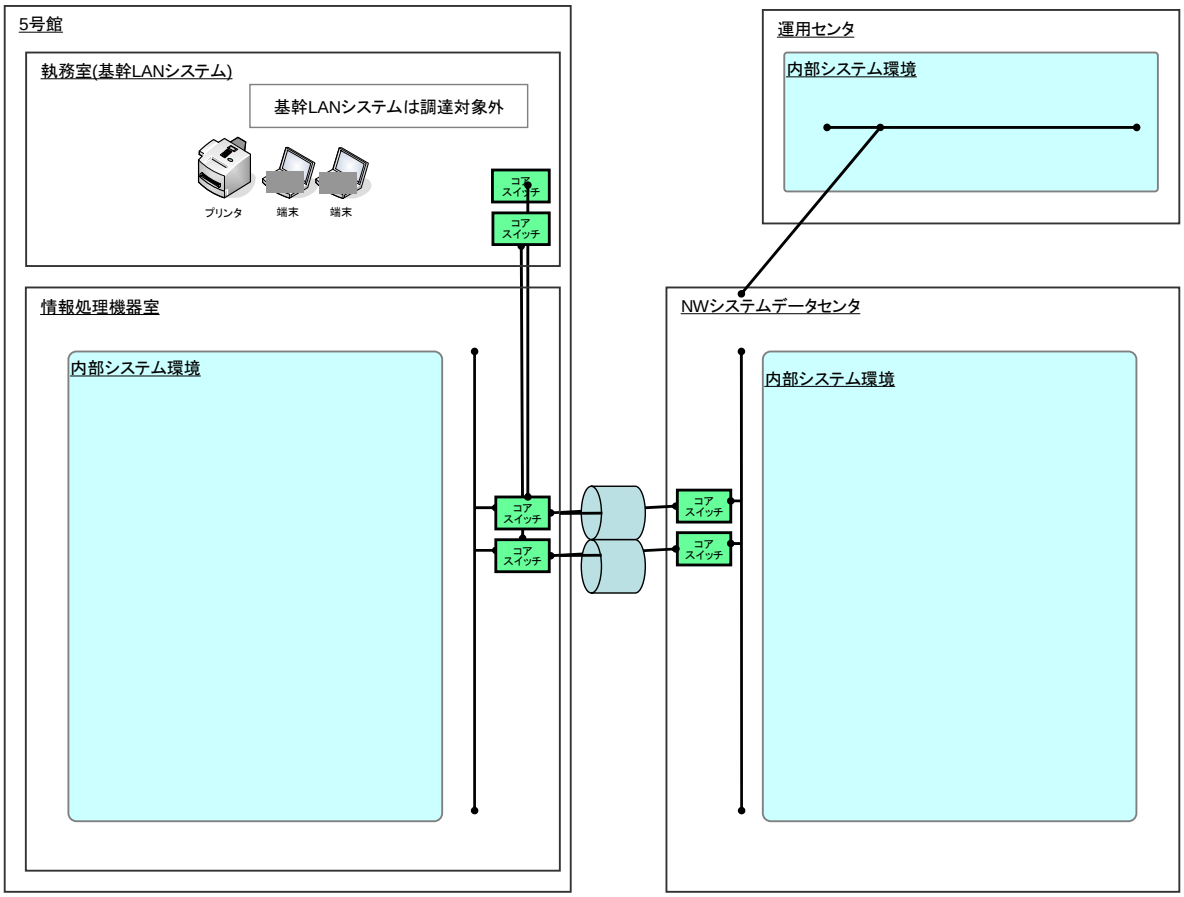

図 14-5　内部システム環境構成イメージ

(2) 基本要件

以下の個別サービスは、個別サービスを利用する業務の特性を考慮し、５号館内に設置すること。

ア．会計予算事務処理サービスサーバ群

イ．分散型統計処理サービスサーバ群

(3) セキュリティ要件

ア．内部システム環境内に設置されるサーバ及びネットワーク機器等のアクセスログは、「11.5 ログ管理」に従い収集、分析ができること。

イ．内部システム環境内に設置されるサーバ、ネットワーク機器等のアクセスログは、月次でログのバックアップを取得し、担当職員へ提出すること。

ウ．上記「ア」及び「イ」以外のセキュリティ要件については、「11.情報セキュリティ」を参照し、必要な対策を行うこと。

(4) ネットワークサービス

ア．機能要件

A. 外部 SMTP サーバ、霞が関ＷＡＮ用 SMTP サーバ、ＷＩＳＨ用 SMTP サーバ、及びその他外部接続先 SMTP サーバ等からのメールを中継し、グループウェアのメール機能にメールを受配信する機能を有すること。

B. ＮＷシステム内名前解決、インターネット、霞が関ＷＡＮ、ＷＩＳＨ、及びその他外部接続ネットワーク等を利用するための名前解決の機能を有すること。

C. ＮＷシステム内に対し、時刻を同期するための標準時刻を提供する機能を有すること。

D. ５号館内からインターネット閲覧、ＮＷシステム内ウィルス管理サーバからウィルス定義ファイル取得等のリクエストを統合ネットワークインターネット閲覧機能へ中継する機能を有すること。

イ．機器構成要件

A. 内部メールサーバ

① 機能要件

- 電子メールの送受信機能を有すること。

② ソフトウェア要件

- ＮＷシステム標準ＯＳを使用すること。
- SMTP サーバとして、最新の「SendMail」及び「qmail」と同等以上の機能を有すること。

B. 内部ＤＮＳサーバ

① 機能要件

- 名前解決の機能を有すること。

② ソフトウェア要件

- ＮＷシステム標準ＯＳを使用すること。
- ＤＮＳサーバとして、最新の「BIND」と同等以上の機能を有すること。名前解決の機能を有すること。

C. メール対策サーバ

① 機能要件

- 宛先や添付ファイルの拡張子の種類、本文中や添付ファイルに含まれるキーワード等をチェックし、送受信の可否を判断できる機能を有すること。
- 「11.2.1 ウィルス対策」を参照のこと。
- 「11.2.4 メール対策」を参照のこと。

② ソフトウェア要件

- ＮＷシステム標準ＯＳを使用すること。なお、アプライアンスを使用する場合はこの限りではない。

D. 時刻サーバ

① 機能要件

- 時刻情報を共通サービス DMZ の時刻サーバから取得し、ＮＷシステムの時刻を同期すること。

② ソフトウェア要件

- ＮＴＰサーバとして最新の「ＮＴＰデーモン」と同等以上の機能を有すること。

③ ハードウェア要件

- アプライアンス製品を導入すること。
- 時刻同期のための時刻情報源を共通サービス DMZ の時刻サーバとすること。

E. インターネット閲覧中継サーバ

① 機能要件

- インターネット閲覧の中継機能を有すること。
- その他機能は、「12.8.2（7）リバースプロキシ／キャッシュ装置」を参照のこと。

② ハードウェア要件

- アプライアンス製品を導入すること。

14.3 ネットワーク構成機器

14.3.1 ファイアウォール設置要件

ア．外部からの不正アクセス（攻撃）を防止するため、以下の接続回線にファイアウォールを設置すること。また、設置に際しては、耐障害性を考慮した冗長構成とすること。

A. ＮＷシステムとインターネット回線間
B. ＮＷシステムと統合ネットワーク接続回線間
C. 霞が関ＷＡＮとの接続回線間
D. ＷＩＳＨとの接続回線間
E. 国会連絡室との接続回線間
F. 電子入札システムとの接続回線間
G. ５号館共用ＮＷとの接続回線間
H. 分散型統計処理サービスセグメントとの接続回線間
I. 人事異動情報サービスセグメントとの接続回線間
J. その他、セキュリティ上必要な箇所間

イ．省内のすべてのサーバ及びクライアントＰＣは、ファイアウォールの内側に設置し、外部からの不正アクセス（攻撃）を防ぐ構成とすること。

ウ．ファイアウォールの機能的制限により、パフォーマンスの著しい低下が発生し

ないよう冗長構成とすること。

14.3.2 ネットワーク型侵入検知システム（IDS／IPS）設置要件

ア．ファイアウォールだけでは防ぎきれない不正アクセスから、ＮＷシステムを防御するため、以下の回線にネットワーク型 IDS を設置すること。

A. ＮＷシステムとインターネット回線間

B. ＮＷシステムと外部接続回線間

C. インターネット接続環境、外部接続環境、及び内部システム環境の各環境間

D. その他、セキュリティ上必要な箇所

イ．ネットワーク型 IDS を複数台設置し、外部から省内ネットワークへの不正アクセス（攻撃）を検知すること。

14.3.3 運用要件

ア．ネットワーク構成機器が動作するために必要なすべてのソフトウェアの状態を定期的に調査し、不適切な状態にあるネットワーク構成機器を検出した場合には、改善を図ること。ただし、ソフトウェアを変更することが困難なネットワーク構成機器の場合は、この限りでない。

イ．通信要件の変更の際、定期的に、アクセス制御の設定の見直しを行うこと。

14.4 テレワーク

ＩＴ新改革戦略（平成 18 年 1 月 19 日 ＩＴ戦略本部決定）において、「2010 年までに適正な就業環境の下でのテレワーカーが就業者人口の 2 割を実現」という目標が置かれたことを受け、当省においても、自宅あるいは、出張先での業務といった、場所と時間を自由に使った柔軟な働き方を実現するためのＩＴ基盤を導入することとする。

当省が提供するテレワーク用のクライアントＰＣ（以下「テレワーク端末」という。）を用いてＮＷシステムに接続しようとする利用者に対しては、統合ネットワークのダイヤルアップ接続環境からの接続（ダイヤルアップ接続あるいは、インターネットＶＰＮ接続）を前提としており、統合ネットワークへの接続時にワンタイムパスワードでの認証を実施する想定である。そのため、ＮＷシステムでは、ワンタイムパスワードでの認証を通過した利用者に対して、ＮＷシステムへの接続に必要な認証と検疫を実施するとともに、①テレワーク端末の整備サービス、②基本サービスの提供、③クライアントＰＣへのリモート接続サービスの 3 サービスを用意し、業務の特性に応じて、利用者がサービスを選択できる基盤を実現する。各サービスの具体的な実現イメージは図 14-6 のとおりである。