別紙9

ネットワーク想定構成

平成26年11月

厚生労働省年金局事業管理課システム室

別紙9-1　ネットワーク想定構成（一覧）

No.	ハードウェア機器		機器分類	本番環境			検証環境			備考
	設置場所	機器名		台数	性能	インタフェース数	台数	性能	インタフェース数	
1	接続認証	ファイアウォール（IPS）	ファイアウォール	2	スループット：40Gbps以上 同時セッション数：10,000,000以上	10Gbase-SR：8ポート以上 1000Base-T：6ポート以上	2	スループット：.40Gbps以上 同時セッション数：10,000,000以上	10Gbase-SR：8ポート以上 1000Base-T：6ポート以上	IPS/IDS機能を含む
2		接続認証用L2スイッチ	L2スイッチ	2	スイッチング容量：160Gbps以上 フレーム処理容量：222Mpps以上	10Gbase-SR：40ポート以上	2	スイッチング容量：160Gbps以上 フレーム処理容量：222Mpps以上	10Gbase-SR：40ポート以上	
3		接続認証用L3スイッチ	L3スイッチ	4	スイッチング容量：1.44Tbps以上 フレーム処理容量：1.07Tpps以上	40Gbase-SR4：6ポート以上 10Gbase-SR：48ポート以上 1000Base-T：1ポート以上	4	スイッチング容量：1.44Tbps以上 フレーム処理容量：1.07Tpps以上	40Gbase-SR4：6ポート以上 10Gbase-SR：48ポート以上 1000Base-T：1ポート以上	
4		負荷分散装置	負荷分散装置	2	負荷分散スループット：10Gbps以上 SSLスループット：8Gbps以上 SSLTPS：9,000tps以上	10Gbase-SR：2ポート以上 1000Base-T：8ポート以上	2	負荷分散スループット：10Gbps以上 SSLスループット：8Gbps以上 SSLTPS：9,000tps以上	10Gbase-SR：2ポート以上 1000Base-T：8ポート以上	
5	L4業務処理	業務処理用L2スイッチ	L2スイッチ	4	スイッチング容量：160Gbps以上 フレーム処理容量：222Mpps以上	10Gbase-SR：40ポート以上	4	スイッチング容量：160Gbps以上 フレーム処理容量：222Mpps以上	10Gbase-SR：40ポート以上	
6		業務処理用L3スイッチ	L3スイッチ	2	スイッチング容量：1.44Tbps以上 フレーム処理容量：1.07Tpps以上	40Gbase-SR4：6ポート以上 10Gbase-SR：48ポート以上 1000Base-T：1ポート以上	2	スイッチング容量：1.44Tbps以上 フレーム処理容量：1.07Tpps以上	40Gbase-SR4：6ポート以上 10Gbase-SR：48ポート以上 1000Base-T：1ポート以上	
7		負荷分散装置	負荷分散装置	2	負荷分散スループット：10Gbps以上 SSLスループット：8Gbps以上 SSLTPS：9,000tps以上	10Gbase-SR：2ポート以上 1000Base-T：8ポート以上	2	負荷分散スループット：10Gbps以上 SSLスループット：8Gbps以上 SSLTPS：9,000tps以上	10Gbase-SR：2ポート以上 1000Base-T：8ポート以上	
8	L5情報格納	情報格納用L2スイッチ	L2スイッチ	2	スイッチング容量：80Gbps以上 フレーム処理容量：111Mpps以上	10Gbase-SR：4ポート以上 1000Base-T：48ポート以上	2	スイッチング容量：80Gbps以上 フレーム処理容量：111Mpps以上	10Gbase-SR：4ポート以上 1000Base-T：48ポート以上	
9	L10管理・監視	管理・監視用L2スイッチ	L2スイッチ	2	スイッチング容量：160Gbps以上 フレーム処理容量：222Mpps以上	10Gbase-SR：40ポート以上	2	スイッチング容量：160Gbps以上 フレーム処理容量：222Mpps以上	10Gbase-SR：40ポート以上	
10		IPS管理装置	侵入検知/防止装置	2	最大管理IPS数：35以上 最大IPSイベント数：6000以上	1000Base-T：1ポート以上	2	最大管理IPS数：35以上 最大IPSイベント数：6000以上	1000Base-T：1ポート以上	
11	L11管理操作	ファイアウォール	ファイアウォール	2	スループット：2Gbps以上 同時セッション数：500,000以上	1000Base-T：8ポート以上	2	スループット：2Gbps以上 同時セッション数：500,000以上	1000Base-T：8ポート以上	
12		管理操作用L2スイッチ	L2スイッチ	2	スイッチング容量：108Gbps以上 フレーム処理容量：107.1Mpps以上	10Gbase-SR：4ポート以上 1000Base-T：48ポート以上	2	スイッチング容量：108Gbps以上 フレーム処理容量：107.1Mpps以上	10Gbase-SR：4ポート以上 1000Base-T：48ポート以上	

別紙9-2 ネットワーク想定構成（機能要件）

No.	名称	分類	要件詳細
1	L3スイッチ	A 構成	主系、従系で2台以上の構成とすること。
2		B LAN インタフェース	各サーバとネットワーク機器が接続できること。
3		C LAN ポート数	各サーバとネットワーク機器が接続するために必要なポート数を有すること。
4		D 設定方法	SSH等暗号通信を利用した遠隔設定作業ができること。
5		E 設定方法	コンソールポートを使用できること。
6		F 装置管理	SNMPにより、機器内の内部情報を取得(Get)及び情報を通知(Trap)できること。
7			SYSLOGを使用でき、ログを転送できること。
8		G 時刻同期	NTPサーバと時刻同期できること。
9		H 筐体	19インチラックに設置できること。
10			予期せぬ接続機器の増加に対応するため、モジュール型等の拡張が容易なもの、又は空きポートの余裕があるものであること。
11			モジュール型の場合は、システムを停止することなくモジュールを追加、交換、撤去できること。
12		I 電源	AC100V、又は200V（ 50/60Hz）であること。
13			電源装置を冗長化できること。
14			システムを停止することなく電源装置を交換できること。
15		J 冷却ファン	冷却ファンを冗長構成とすること。
16		K 外型寸法・重量・最大消費電力	設置場所の条件に従うこと。
17		L 機能	外部回線サービスの終端ゲートウェイのほかLAN集線機能を有すること。
18			QoS等の通信優先制御を行えること。
19			ACLを使った通信制御を行えること。
20			LANワイヤレートでの接続を行えること。
21			異なるLANセグメント（サブネット）を超えた通信を経路プロトコルを使って経路制御する機能を有すること。 （LAN等の高帯域でのルーティングが可能）
22			スタティックルーティングが使用できること。
23			VRRPを使用しゲートウェイ機能が冗長化できること。
24			ポートに対してVLANを割当てられること。
25			リンクアグリゲーション機能を有し、伝送路の冗長性を確保するため、スイッチ間の複数の物理リンクを論理的に1本にまとめることができること。
26	L2スイッチ	A 構成	主系、従系で2台以上の構成とすること。
27		B LAN ポート数	各サーバとネットワーク機器が接続するために必要なポート数を有すること。
28		C 設定方法	SSH等暗号通信を利用した遠隔設定作業できること。
29			コンソールポートを使用できること。
30		D 装置管理	SNMPにより、機器内の内部情報を取得(Get)及び情報を通知(Trap)できること。
31			SYSLOGを使用でき、ログを転送できること。
32		E 時刻同期	NTPサーバと時刻同期できること。
33		F 筐体	19インチラックに設置できること。
34			予期せぬ接続機器の増加に対応するため、モジュール型等の拡張が容易なもの、又は空きポートの余裕があるものであること。
35			モジュール型の場合は、システムを停止することなくモジュールを追加、交換、撤去できること。
36		G 電源	AC100V、又は200V（ 50/60Hz）であること。
37			電源装置を冗長化できること。
38			システムを停止することなく電源装置を交換できること。
39		H 冷却ファン	冷却ファンを冗長構成とすること。
40		I 外型寸法・重量・最大消費電力	設置場所の条件に従うこと。

No.	名称	分類	要件詳細
41		J 機能	主にLANを構築する際に各種サーバ、接続する端末を集線し、上位の機器へスイッチングさせる機能を有すること。
42			ブロードキャスティングによる通信の輻輳を避けるためハードウェアレベルでのスイッチで通信を行えること。
43			ポートに対してVLANを割当てられること。
44			リンクアグリゲーション機能を有し、伝送路の冗長性を確保するため、スイッチ間の複数の物理リンクを論理的に1本にまとめることができること。
45			各サーバとネットワーク機器が接続できること。
46	ファイアウォール	A 構成	主系、従系で2台以上の構成とすること。
47		B LAN インタフェース	各サーバとネットワーク機器が接続できること。
48		C LAN ポート数	各サーバとネットワーク機器が接続するために必要なポート数を有すること。
49		D 設定方法	SSH等暗号通信を利用した遠隔設定作業ができること。
50			コンソールポートを使用できること。
51		E 装置管理	SNMPにより、機器内の内部情報を取得(Get)及び情報を通知(Trap)できること。
52			SYSLOGを使用でき、ログを転送できること。
53		F 時刻同期	NTPサーバと時刻同期できること。
54		G 筐体	19インチラックに設置できること。
55			予期せぬ接続機器の増加に対応することため、モジュール型等の拡張が容易なもの、又は空きポートの余裕があるものであること。
56			モジュール型の場合は、システムを停止することなくモジュールを追加、交換、撤去できること。
57		H 電源	AC100V、又は200V（50/60Hz）であること。
58			電源装置を冗長化できること。
59			システムを停止することなく電源装置を交換できること。
60		I 冷却ファン	冷却ファンを冗長構成とすること。
61		J 外型寸法・重量・最大消費電力	設置場所の条件に従うこと。
62		K 評価保証レベル	EAL4以上であること。 ※調達時に最新の「ITセキュリティ評価及び認証制度等に基づく認証取得製品リスト」を確認し求められるセキュリティレベルが変更されている場合は、最新の情報を取り込むこと。
63		L 機能	設定変更や状態を確認するインターフェースを提供する機能を有すること。
64			通過・拒否したパケットの記録を出力・保存する機能を有すること。
65			スタティックルーティングが使用できること。
66			VRRPを使用しゲートウェイ機能が冗長化できること。
67			パケットフィルタリング機能を有すること。
68			ステートフルインスペクション機能を有すること。
69	負荷分散装置	A 構成	主系、従系で2台以上の構成とすること。
70		B LAN インタフェース	各サーバとネットワーク機器が接続できること。
71		C LAN ポート数	各サーバとネットワーク機器が接続するために必要なポート数を有すること。
72		D 設定方法	SSH等暗号通信を利用した遠隔設定作業ができること。
73			コンソールポートを使用できること。
74		E 装置管理	SNMPにより、機器内の内部情報を取得(Get)及び情報を通知(Trap)できること。
75			SYSLOGを使用でき、ログを転送できること。
76		F 時刻同期	NTPサーバと時刻同期できること。
77		G 筐体	19インチラックに設置できること。
78			予期せぬ接続機器の増加に対応するため、モジュール型等の拡張が容易なもの、又は空きポートの余裕があるものであること。
79			モジュール型の場合は、システムを停止することなくモジュールを追加、交換、撤去できること。
80		H 電源	AC100V、又は200V（50/60Hz）であること。
81			電源装置を冗長化できること。
82			システムを停止することなく電源装置を交換できること。

No.	名称	分類	要件詳細
83		I 冷却ファン	冷却ファンを冗長構成とすること。
84		J 外型寸法・重量・最大消費電力	設置場所の条件に従うこと。
85		K 機能	ネットワークにおいて、各リソースへの通信アクセスや要求を一元的に管理し、同等の機能を持つ複数のサーバに要求を分散転送する機能（各サーバ資源を最適化し、通信応答速度を保つ機能）を有すること。
86			スタティックルーティングが使用できること。
87			負荷分散対象サーバのTCPコネクション数を計測し、もっともコネクション数の少ないサーバにリクエストを割り当てることで負荷分散できること。
88			Cookieパーシステンスを使用し、継続的に同一のサーバへセッションを転送できること。
89			コンテンツチェックにより、故障が発生しているサーバにはリクエストを転送しないよう負荷分散対象から切り離すことができること。
90			接続制限値(最大同時コネクション数)を設定し、この制限を超える分のリクエストは状況伝達サーバへ転送できること。
91		L ダミーリクエスト	ダミーリクエストを負荷分散製品から定期的に送信し、ダミーリクエストに対する処理結果のチェックができること。
92			負荷分散装置側でチェック結果により、サービス提供が不可能であると判断された場合、負荷分散装置上のルーティングテーブルを変更し、以後のユーザリクエストに対してすべてサービス停止である旨を返すことができること。
93		M 負荷分散方式	ラウンドロビン方式及び最小コネクション方式による振り分けできること。
94		N セッション維持機能	Active-Active構成において、サーバ障害時にクラスタリンググループからサーバが切り離された際にセッションが断絶し、業務処理を初めから行なうことを避けるため、同じサーバからのリクエストは、リクエスト先のサーバに固定的に割り振り、セッションを維持できること。
95		O クラスタリング再構成機能	障害を発生したサーバを除き、現行稼働可能なサーバ間でクラスタリングを再構成できること。
96		P セッション・リカバリー	異常を検出するとクラスタリング対象から除外し、別の正常なサーバに再送信することができること。
97		Q セキュリティ機能	セキュリティホールが発見された時に、迅速に修正モジュールを入手が可能な開発ベンダからソフトウェアを調達できること。
98			ソフトウェアデフォルトで配置された使わないコマンドを削除できること。
99			ソフトウェアデフォルトで配置された使わないプログラムを削除できること。
100			使わないポートを閉じられること。
101			ソフトウェアのデフォルト設定でソフトウェアバージョン、ソフトウェアを稼動させるサーバOS等、プラットフォーム情報を外部から取得し、外部から情報参照できないように修正できること。
102		R 拡張性	スケールアウトができること。
103		S 信頼性	冗長構成として、Active-Active方式を採用できること。
104	侵入検知/防止装置	A 構成	主系、従系で2台以上の構成とする。
105		B LAN インタフェース	各サーバとネットワーク機器が接続できること。
106		C LAN ポート数	各サーバとネットワーク機器が接続するために必要なポート数を有すること。
107		D 設定方法	SSH等暗号通信を利用した遠隔設定作業ができること。
108			コンソールポートを使用できること。
109		E 装置管理	SNMPにより、機器内の内部情報を取得(Get)及び情報を通知(Trap)できること。
110			SYSLOGを使用でき、ログを転送できること。
111		F 時刻同期	NTPサーバと時刻同期できること。
112		G 筐体	19インチラックに設置できること。
113			予期せぬ接続機器の増加に対応するため、モジュール型等の拡張が容易なもの、又は空きポートの余裕があるものであること。
114			モジュール型の場合は、システムを停止することなくモジュールを追加、交換、撤去できること。
115		H 電源	AC100V、又は200V（50/60Hz）であること。
116			電源装置を冗長化できること。
117			システムを停止することなく電源装置を交換できること。
118		I 冷却ファン	冷却ファンを冗長構成とすること。
119		J 外型寸法・重量・最大消費電力	設置場所の条件に従うこと。
120		K 評価保証レベル	EAL3以上であること。 ※調達時に最新の「ITセキュリティ評価及び認証制度等に基づく認証取得製品リスト」を確認し求められるセキュリティレベルが変更されている場合は、最新の情報を取り込むこと。
121		L 機能	不正と考えるパターンを設定するシグネチャを作成、更新できること。
122			不正を検知したことを通知できること。
123			証跡管理によりログ解析を行うため、検知情報を記録できること。
124			シグネチャアップデートができること。

No.	名称	分類	要件詳細
125		M ネットワーク侵入検知機能	不正アクセスを検知できること。
126			内部から外部への不正な通信についても検知できること。
127			ネットワーク上の通信を監視できること。
128			パケット内のデータ部分に含まれる特定のキーワードと、シグネチャ内の文字列パターンをマッチングさせ、不正な通信を検知できること。
129			個々のパケットに対する処理を最小限に抑えるため、後述するシグネチャ・データベースとのマッチングを行い、そのパターンと一致するか否かの比較処理を行い、効率的に処理できること。
130			通信に対してRFC(IETF:InternetEngineeringTaskForceの策定した技術仕様)のプロトコル仕様と比較し、仕様から逸脱している不正な通信を検知できること。
131			日常通信で想定される以上の過剰な通信量がネットワーク上に流れたことを検知できること。
132		N ネットワーク侵入防止機能	不正アクセスを検知、遮断する機能できること。
133			内部から外部への不正な通信についても検知、遮断できること。
134			ネットワーク侵入検知機能より、ネットワークを介した不正と考えられる通信を検知したことを伝達できること。
135			TCPプロトコルを使用した不正な通信を検知した場合、発信元/発信先に向けて接続を切断するためのパケット(リセットパケット)を送信し、不正な通信により確立された接続を切断できること。
136			UDP及びICMPプロトコルを使用した不正な通信を検知した場合、発信元に対して発信先ホストが存在しないことを示すレスポンスを返すことで攻撃を回避できること。
137			ファイアウォール機能と連動し、下記の通信を遮断できること。 ・特定のIPアドレスからの通信を遮断 ・特定のIPアドレスへの通信を遮断 ・特定の発信元IPアドレスの特定のポートとプロトコルからの通信を遮断 ・特定の発信元IPアドレスの特定のポートとプロトコルへの通信を遮断
138		O 検知パターン更新機能	不正アクセスと考えられる通信パターンを設定するシグネチャを作成、更新できること。
139		P アラート機能	不正を検知したことを通知できること。マネジャに通知するアラートの内容には以下の内容が含まれるものとすること、 ・検知元(検知したセンサが設置されている箇所を示す情報) ・検知時刻 ・シグネチャと比較して不正と検知した内容
140		Q ログ出力機能	ログ解析を行うため、検知情報を記録できること。
141			シグネチャアップデートができること。