別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名	分類	機能概要	設置場所							対応区分※
					WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
						利用拠点環境	センタ的拠点環境		#1	#2		
1	基本サービス	1 ドメインネームシステム（DNS）機能	共通	1-1 次期統合ネットワーク内に構築するサーバ及びインターネット上のサーバ等において、以下の名前解決機能を提供すること。 ・インターネット上のサーバの名前解決要求 ・サーバ（内部）の名前解決要求 ・サーバ（外部）の名前解決要求 ・インターネット側からの公開サーバの名前解決要求					○	○	○	維持
2				1-2 内部DNSサーバと外部DNSサーバを別々に設置すること。また、障害対策として、各DNSサーバは冗長構成（プライマリ/セカンダリ）とし、内部DNSサーバのプライマリDNSサーバは中央センタ#1に設置し、セカンダリDNSサーバは中央センタ#1及び中央センタ#2に設置すること。外部DNSサーバは、中央センタ#1にプライマリDNSサーバを設置し、セカンダリDNSサーバは中央センタ#1及び中央センタ#2に設置すること。また、インターネット上（ISP）にもセカンダリの外部DNSサーバを配置して障害に備える構成とすること。					○	○	○	維持
3				1-3 中央センタ#1及び中央センタ#2に設置するDNSサーバは、厚生労働省占有とし、DNSサーバが稼動する物理サーバ上に次期統合ネットワークで提供する機能以外のサーバを稼動させることは不可とする。					○	○	○	維持
4				1-4 DNS機能の構成例は「別紙9　補足資料 機能要件一覧」を参照すること。					○	○	○	維持
5			内部DNS	1-5 内部DNSサーバは、mhlw.go.jpゾーンのセカンダリDNSサーバとして、拠点のパソコン、サーバ等からの問合せに対して名前解決が行えること。また、mhlw.go.jpゾーンからサブドメインの権限委譲を受け、サーバ等機器名の管理及び名前解決が行えること。個別システム独自ドメインの名前解決については、個別システム側DNSサーバに転送が行えること。					○	○		維持
6				1-6 個別システムからのドメインネームの参照に対して、応答すること。					○	○		維持
7				1-7 中央センタに導入する機器については、冗長化構成とすること。					○	○		維持
8				1-8 ホスト名から IP アドレスの参照に対し、応答すること。					○	○		維持
9				1-9 IPアドレスからホスト名の参照に対し、応答すること。					○	○		維持
10				1-10 IPv4及びIPv6 のアドレスを応答すること。					○	○		維持
11				1-11 TTLを一時的に短く設定できる機能を有していること。					○	○		維持
12				1-12 担当職員が指定するドメインの管理を行うこと。					○	○		維持
13				1-13 DNSキャッシュポイズニング対策がなされていること。					○	○		維持
14			外部DNS	1-14 外部DNSサーバは、mhlw.go.jpゾーンの権威サーバとしてサーバ等機器名の管理及び名前解決機能を提供すること。							○	維持
15				1-15 厚生労働省が保有するドメイン名を使用したインターネット接続環境とすること。							○	維持
16				1-16 インターネットからのドメインネームの参照に対して、応答すること。							○	維持
17				1-17 中央センタに導入する機器については、冗長化構成とすること。							○	維持
18				1-18 ホスト名から IP アドレスの参照に対し、応答すること。							○	維持
19				1-19 IPアドレスからホスト名の参照に対し、応答すること。							○	維持
20				1-20 IPv4及びIPv6 のアドレスを応答すること。							○	維持

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名	分類	機能概要	設置場所							対応区分※
					WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
						利用拠点環境	センタ的拠点環境		#1	#2		
21				1-21 TTLを一時的に短く設定できる機能を有していること。							○	維持
22				1-22 担当職員が指定するドメインの管理を行うこと。							○	維持
23				1-23 DNSキャッシュポイズニング対策がなされていること。							○	維持
24				1-24 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。							○	維持
25				1-25 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。							○	維持
26		2 時刻同期（NTP）機能		2-1 時刻同期の基準として、政府共通ネットワークから時刻を取得すること。なお、障害発生時に備え、GPS、テレホンJJYサービス等を利用したNTPサーバの機能を有すること。時刻同期サービスを提供する先は、個別システムが設置するNTPサーバ、あるいは時刻同期サービスを必要とする拠点のクライアント端末等である。現行の統合ネットワークで提供しているサーバ等は除く。					○	○		維持
27		3 監視機能	共通	3-1 次期統合ネットワークを構成する回線及びネットワーク機器の稼働状況を監視･管理できること。ネットワーク機器の稼働状況取得間隔時間は、5分以内で監視し、障害検知（アラート通知間隔）は担当職員と協議の上、決定する。					○	○		維持
28				3-2 本調達で導入するファイアウォール、IDS/IPS機器、検疫システムから通知されるセキュリティインシデントの監視ができること。					○	○		維持
29				3-3 次期統合ネットワークを構成するサーバ機器の監視・管理が可能であること。					○	○		維持
30				3-4 各アクセス回線について、帯域使用率の情報が取得できること。					○	○		維持
31				3-5 ネットワーク機器のシステムログの情報を収集、解析できること。					○	○		維持
32				3-6 SNMPv2相当以上の管理機能を有すること。					○	○		維持
33				3-7 ファイアウォールのイベントログ（遮断又はブロックした宛先/送信元IPアドレスやTCP/UDPのポート番号、発生日時等）、システムログ情報を収集、解析できること。					○	○		維持
34				3-8 IDS/IPSのイベントログ（検知した宛先/送信元IPアドレスやTCP/UDPのポート番号、発生日時等）、システムログ情報を収集、解析できること。					○	○		維持
35				3-9 検疫機能のイベントログ（遮断したMACアドレス、発生日時等）を収集、解析できること。					○	○		維持
36				3-10 サーバイベントログを収集、解析できること。各種機器から収集したログの相関分析を行い、異常検出が行えるようにすること。					○	○		維持
37				3-11 インターネット閲覧に関するアクセスログを収集、解析できること。					○	○		維持
38				3-12 ネットワークトラフィックのモニタリング機能を実現できること。					○	○		維持
39				3-13 ファイアウォール、IDS/IPS等セキュリティポリシーの設定を一元的に管理実行し、ネットワーク管理の最適化ができること。					○	○		維持
40				3-14 監視対象スイッチはポート毎にトラフィック、コリジョン、ブロードキャスト、エラーを自動収集できること。					○	○		維持
41				3-15 運用センタからリモートにて、ネットワーク１系、ネットワーク2系の2系統のネットワーク回線への切替え、切り戻しの操作ができること。					○	○		維持
42				3-16 ネットワーク機器に関して、設置場所や設置機種、設置台数を管理し、障害発生時における迅速な復旧やバージョンアップに備えるため、バージョンの管理ができること。					○	○		維持

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名	分類	機能概要	設置場所							対応区分※
					WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
						利用拠点環境	センタ的拠点環境		#1	#2		
43				3-17 機器の設定変更やバージョンアップに迅速に対応するため、ネットワーク機器のアカウント、コンフィグレーション、アドレス、命名規則等の管理ができること。					○	○		維持
44				3-18 ネットワーク機器構成を自動検出し、マップの自動生成ができること。					○	○		維持
45				3-19 複数の管理者に対してそれぞれに応じたレベルのアクセス権を定義できること。					○	○		維持
46				3-20 次期統合ネットワークのトラフィック状況、新規接続に関する工事予定等に関する情報が表示されたWebサイトを個別システム管理責任者が閲覧できること。また、運用状況を公開し、センタ的拠点には、リアルタイムで情報が提供できること。					○	○		維持
47				3-21 拠点に対する障害情報のメール、電話等による連絡ができること。					○	○		維持
48				3-22 バックアップデータの世代管理ができること。					○	○		維持
49				3-23 システム、監視、管理に関する情報を安全かつ完全に保存できる機器構成であること。					○	○		維持
50				3-24 設置運用される主要な機器については、冗長構成に対応していること。					○	○		維持
51				3-25 ハードウェアの追加に対する拡張性があること。					○	○		維持
52				3-26 システムログ、監視ログなどの運用管理に関する情報を安全かつ完全に保存できる機器構成であること。					○	○		維持
53			パケットキャプチャ	3-27 定常的に重要通信のパケットキャプチャ（ヘッダ）を取得できる機能を提供すること。対象とする重要通信は「別紙11 重要通信一覧」を参照すること。			○		○	○		新規
54				3-28 定常的な取得とは別に障害調査、分析等の際に任意で対象通信のパケットキャプチャ（ヘッダ、データ）を取得できる機能を提供すること。			○		○	○		新規
55				3-29 パケットキャプチャを取得することにより、マイクロ遅延の検知（ミリ秒単位）が可能であること。			○		○	○		新規
56				3-30 レスポンスタイムの悪化、エラーコードやマイクロバーストの発生等、対象通信に異常があった際の検知が可能であること。			○		○	○		新規
57				3-31 少なくとも下記情報で絞り込んでパケットキャプチャの取得が可能であること。 ・送信元IPアドレス ・宛先IPアドレス ・ポート番号 ・プロトコル			○		○	○		新規
58			ダッシュボード	3-32 取得したパケットキャプチャを一元的に可視化するためのダッシュボードを提供すること。			○		○	○		新規
59				3-33 「10 ポータル機能」にダッシュボードに関するリンクを掲載し、そのリンクからダッシュボードに接続できること。			○		○	○		新規
60				3-34 ダッシュボードは次期統合ネットワークに接続されている拠点から接続できること。			○		○	○		新規
61				3-35 ダッシュボードは、個別システム管理責任者、担当職員及び受注者等がその管理範囲に応じて必要な情報を参照し障害調査等が実施できるよう、「3 監視機能（ダッシュボード）」への認証機能を有し、各機能及びデータに対する認証・認可の仕組みを有すること。			○		○	○		新規

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類		機能概要	設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
62					3-36	ダッシュボードから少なくとも下記項目により対象データを絞り込み、パケットキャプチャの取得（ダウンロードや参照）が可能であること。 ・送信元IPアドレス ・宛先IPアドレス ・ポート番号 ・プロトコル ・時間帯			○		○	○		新規
63					3-37	パケットドロップ、パケットロス、リンクダウン等の状況がダッシュボードに表示されること。			○		○	○		新規
64					3-38	パケットキャプチャから抽出される統計情報について、ダッシュボードからグラフによる確認、分析が可能であること。			○		○	○		新規
65					3-39	ダッシュボードからドリルダウンにより特定の通信の詳細な確認、分析が可能であること。			○		○	○		新規
66					3-40	パケットドロップ、パケットロス、リンクダウン等の状況についてアラート通知が可能であること。			○		○	○		新規
67					3-41	パケットドロップ、パケットロス、リンクダウン等の状況について定期的にレポートを生成しメール送信が可能であること。			○		○	○		新規
68					3-42	レポートの細やかなカスタマイズが可能なこと。			○		○	○		新規
69					3-43	パケットキャプチャ機能を実現する際に発生するWAN経由の通信（キャプチャデータの管理サーバへの転送、キャプチャデータのダウンロード等）において、業務通信への影響を最小限にするために、優先制御や帯域制御等による対処を行うこと。			○		○	○		新規
70					3-44	定常的に取得するパケットキャプチャの保管期間は1週間とする。ただし、長期休暇時は保管期間を1週間程度延長できるようにログ保管容量を確保すること。			○		○	○		新規
71					3-45	GUI及びマニュアルが日本語であること。			○		○	○		新規
72		4	ルーティング機能		4-1	「別紙9 機能要件一覧」の 14-1～14-6 を実現する機能を有すること。		○	○		○	○	○	維持
73					4-2	通信経路を限定し、アクセス制御を行える機能を有すること。		○	○		○	○	○	維持
74					4-3	優先度に応じて通信の取り扱いを区別し、重要な通信を輻輳や遅延から守るための帯域予約機能を有すること。		○	○		○	○	○	維持
75					4-4	宛先/送信元IPアドレス、TCP/UDPポート番号などにより指定したIPパケットのフィルタリング機能を有すること。		○	○		○	○	○	維持
76					4-5	ポリシーベースルーティング機能を有すること。		○	○		○	○	○	維持
77					4-6	SNMPv2相当以上の管理機能を有すること。		○	○		○	○	○	維持
78					4-7	ソフトウェア及び設定情報をサーバにバックアップを取得し、障害時等にリストアが可能であること。		○	○		○	○	○	維持
79					4-8	SSHv2相当以上のリモートコンソール機能を有すること。		○	○		○	○	○	維持
80					4-9	CPU使用率等の機器の状態や設定情報を表示することが可能であること。		○	○		○	○	○	維持
81					4-10	機器の障害が発生した場合、発生原因を解析するための機器情報を収集することが可能であること。		○	○		○	○	○	維持
82					4-11	機器の起動時において、自己診断を行える機能を有し、障害の影響が広範囲にわたる前に障害部分を検知できること。		○	○		○	○	○	維持
83					4-12	時刻同期機能を有すること。		○	○		○	○	○	維持

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名	分類	機能概要	設置場所							対応区分※
					WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
						利用拠点環境	センタ的拠点環境		#1	#2		
84		5 インターネット閲覧機能	共通	5-1 すべての拠点からインターネットを閲覧できる機能を提供すること。							○	維持
85				5-2 すべての拠点から、ウイルス定義ファイルをHTTP及びHTTPSのプロトコルを利用して、取得できること。							○	維持
86				5-3 各拠点からのインターネット接続に対し、厚生労働省の指定する閲覧規制（IPアドレスによる各拠点単位、利用者単位、組織単位等での制御）に対応できること。							○	維持
87				5-4 各拠点からのインターネット接続において、情報セキュリティ対策が講じられていること。							○	維持
88				5-5 各拠点から直接インターネットへの接続や外部から各拠点に直接接続できないよう、内部プロキシサーバ、認証プロキシサーバ、外部プロキシサーバを設け、各プロキシサーバで接続制御を行えること。 なお、個別システム側で独自に準備したプロキシサーバと内部プロキシサーバ及び認証プロキシサーバが多段構成で利用できるように各個別システムと調整の上、必要な設定等を行うこと。							○	維持
89				5-6 認証プロキシサーバは内部プロキシサーバと同一の筐体による提供でもよい。							○	維持
90				5-7 内部プロキシサーバ及び認証プロキシサーバは外部プロキシサーバと連携することで、インターネットへの接続を行うこと。							○	維持
91				5-8 認証プロキシサーバの導入に対する個別システムとの調整及び設定等を行うこと。							○	維持
92				5-9 各拠点からのインターネット接続に関するログを収集・蓄積できること。なお、ログの取得・管理の詳細については、「別紙1 要件定義書」の「4.10.情報セキュリティに関する事項」を参照すること。							○	維持
93				5-10 担当職員からの求めに応じ、アクセスログを追跡・分析して報告が可能なこと。							○	維持
94				5-11 インターネット接続にはファイアウォールを設置し、外部から次期統合ネットワーク内部への直接的な通信を遮断し、内部からの通信も内部向けサービスセグメントまでとし、直接DMZのサーバとの通信をさせないこと。ただし、個別システムの要件により、内部プロキシサーバ及び認証プロキシサーバを経由せずに直接インターネットに接続する必要がある場合は、想定されるリスクを考慮した上で、必要なセキュリティ設定を行い、当該通信が可能となるよう対応すること。							○	維持
95				5-12 次期統合ネットワークでは、中央センタ#1のインターネット回線として800Mbps以上の回線を2回線（合計帯域1600Mbps以上）敷設し、常時800Mbps以上の回線帯域を提供できるように冗長化を行うこと。 なお、本帯域にはテレワーク機能、運用保守リモート機能での利用も含む。また、中央センタ#2のインターネット接続用回線として、400Mbps以上の回線(テレワーク機能での利用含む)を1回線用意すること。							○	維持
96				5-13 インターネット閲覧機能において、インターネット上でIPv6のみで提供されるサービス（通信サービス、インターネット接続サービス、Web閲覧等）との通信に対応すること。							○	維持
97				5-14 特定のグローバルIPアドレスからのみ閲覧可能なWebサイトが存在する。そのため、次期統合ネットワークにおいても当該サイトが閲覧できるようにWebサイト管理者等と調整を行うこと。							○	維持
98				5-15 アクセス回線を収容するインターネット接続回線事業者のバックボーンについては、すべての回線、機器で冗長構成がとられていること。							○	維持
99				5-16 インターネット閲覧機能の構成例は「別紙9　補足資料 機能要件一覧」を参照すること。							○	維持
100			内部プロキシ	5-17 インターネットへの接続が中継可能であること。					○	○		維持
101				5-18 HTTP、HTTPS、FTPリクエストの中継機能を有すること。					○	○		維持
102				5-19 HTTP1.1 に対応したHTTP リクエストの中継機能を有すること。					○	○		維持
103				5-20 個別システムのクライアント端末等からインターネットへの接続は原則プロキシサーバ経由で行うこと。					○	○		維持
104				5-21 HTMLコンテンツや画像データ等のWebコンテンツのキャッシュ機能を有すること。					○	○		維持

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類		機能概要	設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
105					5-22	キャッシュ機能としてHTTPだけでなく、ストリーミング等のUDPに対応していること。					○	○		維持
106					5-23	IPv4、IPv6のデュアルスタックに対応すること。					○	○		維持
107					5-24	利用状況（アクセス元クライアント端末等のIPアドレス、アクセス先URL等について、アクセス制御（許可、拒否）、日時）の記録機能を有すること。					○	○		維持
108					5-25	プロキシサーバの統計情報が閲覧できる機能を有すること。					○	○		維持
109					5-26	指定したURLへのアクセス制御（ブロック、許可、警告等）ができること。					○	○		維持
110					5-27	特定のWebサイトへの書き込みのみを禁止できること。					○	○		維持
111					5-28	コンテンツフィルタリングのデータベース更新を自動及び手動の両方で更新できること。					○	○		維持
112					5-29	ユーザ別又はアクセス元IPアドレス等で閲覧許可ポリシーを制御可能なこと。					○	○		維持
113					5-30	NTLM、LDAP、ActiveDirectoryと連携した認証が可能であること。					○	○		維持
114					5-31	IPアドレス、Cookie、Redirectを使用した認証が可能なこと。					○	○		維持
115					5-32	認証したユーザ情報を保持でき、その保持時間を変更できること。					○	○		維持
116					5-33	IPアドレス及びローカルパスワードによる認証が任意に組み合わせできること。					○	○		維持
117					5-34	CPU使用率等の機器の状態や設定情報を表示することが可能であること。					○	○		維持
118					5-35	機器の障害が発生した場合、発生原因を解析するための機器情報を収集することが可能であること。					○	○		維持
119					5-36	SNMPv2相当以上の管理機能を有すること。					○	○		維持
120					5-37	ソフトウェア及び設定情報をサーバにバックアップを取得し、障害時等にリストアが可能であること。					○	○		維持
121					5-38	WebベースのGUI（HTTPS）で操作が可能であること。					○	○		維持
122					5-39	HTTPS化されたサイトにおいて、特定の操作（コメント投稿等）のみを禁止できるように、通信の復号ができる機能を有すること。					○	○		新規
123				外部プロキシ	5-40	インターネットへの接続が中継可能であること。							○	維持
124					5-41	HTTP、HTTPS、FTPリクエストの中継機能を有すること。							○	維持
125					5-42	HTTP1.1 に対応したHTTP リクエストの中継機能を有すること。							○	維持
126					5-43	内部プロキシサーバ及び認証プロキシサーバからのインターネット接続を中継すること。							○	維持
127					5-44	HTMLコンテンツや画像データ等のWebコンテンツのキャッシュ機能を有すること。							○	維持
128					5-45	キャッシュ機能としてHTTPだけでなく、ストリーミング等のUDPに対応していること。							○	維持
129					5-46	IPv4、IPv6のデュアルスタックに対応すること。							○	維持
130					5-47	利用状況（アクセス元クライアント端末等のIPアドレス、アクセス先URL等について、アクセス制御（許可、拒否）、日時）の記録機能を有すること。							○	維持
131					5-48	外部プロキシサーバの統計情報が閲覧できる機能を有すること。							○	維持
132					5-49	CPU使用率等の機器の状態や設定情報を表示することが可能であること。							○	維持
133					5-50	機器の障害が発生した場合、発生原因を解析するための機器情報を収集することが可能であること。							○	維持

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類		機能概要	設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
134					5-51	SNMPv2相当以上の管理機能を有すること。							○	維持
135					5-52	ソフトウェア及び設定情報をサーバにバックアップを取得し、障害時等にリストアが可能であること。							○	維持
136					5-53	WebベースのGUI（HTTPS）で操作が可能であること。							○	維持
137				Webウイルス対策	5-54	内部プロキシサーバ及び認証プロキシサーバと連携することで、ウイルススキャンが実現可能であること。							○	維持
138					5-55	内部プロキシキャッシュ及び認証プロキシキャッシュと連携し、ウイルススキャンの最適化が可能であること。							○	維持
139					5-56	パターンファイルの公開後、速やかにアップデートを行い、常に最新の脅威を防御できること。							○	維持
140					5-57	ファイルサイズやコンテンツタイプの制限に加え、拡張子による許可、拒否リストが適用可能であること。							○	維持
141					5-58	受信トラフィックと送信トラフィックの両方を分析するように設定できること。							○	維持
142					5-59	ウイルス検出時は、遮断ができること。							○	維持
143					5-60	最新のウイルスのパターンファイルを自動的にダウンロードし、更新できること。							○	維持
144					5-61	ネットワークパフォーマンスを低下させることなく、転送ファイル、Webトラフィックからのウイルスやワーム、スパイウェア等に対して防御できること。							○	維持
145					5-62	CPU使用率等の機器の状態や設定情報を表示することが可能であること。							○	維持
146					5-63	機器の障害が発生した場合、発生原因を解析するための機器情報を収集することが可能であること。							○	維持
147					5-64	SNMPv2相当以上の管理機能を有すること。							○	維持
148					5-65	ソフトウェア及び設定情報をサーバにバックアップを取得し、障害時等にリストアが可能であること。							○	維持
149					5-66	WebベースのGUI（HTTPS）で操作が可能であること。							○	維持
150		6	ファイアウォール機能		6-1	IP通信パケットの宛先や送信元のIPアドレス、TCP及びUDPのポート番号等を検査し、設定した条件によって、IP通信パケットの処理として通過許可(ACCEPT)及び廃棄(DROP)のフィルタリングが可能であり、その処理結果をログとして記録できること。また、拒否(REJECT)処理もサポートしていること。			○		○	○	○	維持
151					6-2	フィルタリング設定の内容については、個別システムごとあるいは拠点ごとに要望があることが想定されるため、必要に応じて調整を行うこと 。			○		○	○	○	変更
152					6-3	アクセスログを収集できる機能を有すること。			○		○	○	○	変更
153					6-4	ファイアウォールを通過するパケットのデータを読み取り、ポートを開放・閉鎖する機能（ダイナミックフィルタリング技術であるステートフルインスペクション）を有すること。			○		○	○	○	変更
154					6-5	脅威への迅速な対応として、運用センタからの新しいポリシーの定義と割当てができること。			○		○	○	○	変更
155					6-6	次期統合ネットワーク機器（センタ的拠点設置用）との接続に使用されるセンタ的拠点内LAN機器（L2スイッチ/L3スイッチ）では、センタ的拠点内の複数セグメントをVLANにて収容し、次期統合ネットワーク機器（センタ的拠点設置用）と接続することが想定されるため、IEEE802.1Q VLAN Tagging機能を有していること。			○					変更
156					6-7	CPU使用率等の機器の状態や設定情報を表示することが可能であること。			○		○	○	○	変更
157					6-8	機器の障害が発生した場合、発生原因を解析するための機器情報を収集することが可能であること。			○		○	○	○	変更
158					6-9	SNMPv2相当以上の管理機能を有すること。			○		○	○	○	変更

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類	機能概要		設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
159					6-10	ソフトウェア及び設定情報をサーバにバックアップを取得し、障害時等にリストアが可能であること。			○		○	○	○	変更
160					6-11	SSHv2相当以上のリモートコンソール機能を有すること。			○		○	○	○	変更
161					6-12	導入した機器及び設定情報を管理サーバ等で一元的に監視・管理できること。			○		○	○	○	変更
162					6-13	機器の起動時において、自己診断を行える機能を有し、障害の影響が広範囲にわたる前に障害部分を検知できる機能を有すること。又は、同等の監視サービスを有すること。			○		○	○	○	変更
163		7	IDS／IPS機能	IDS	7-1	拠点から中央センタ及びその他の拠点に対するすべての通信を対象とした不正接続検知機能を有すること。			○		○	○		維持
164					7-2	トラフィックを検査することで、ポリシー違反、脆弱性の悪用及び異常な動作を検知できる機能を有すること。			○		○	○		維持
165					7-3	担当職員からの求めに応じ、アクセスログを追跡・分析して報告が可能な機能を有すること。			○		○	○		維持
166					7-4	パターンファイルの更新を自動的に適用できる機能を有すること。			○		○	○		維持
167					7-5	パターンファイルの更新はオンラインで行うことができ、再起動せずに最新の状態に反映できる機能を有すること。			○		○	○		維持
168					7-6	不正な通信（P2P、悪意のある通信等）の検知、当該通信の監視システムへの通知機能を有すること。			○		○	○		維持
169					7-7	新たに不正な通信（P2P、悪意のある通信等）プログラムが発生した場合には、対応したパターンファイルの更新をリモートで行える機能を有すること。			○		○	○		維持
170					7-8	port scan等によるDoS攻撃及びDDoS攻撃を検知することが可能な機能を有すること。			○		○	○		維持
171					7-9	不審・攻撃トラフィックをリアルタイムに検知、特定し、当該トラフィックに対する適切なアクションを取ることが可能な機能を有すること。			○		○	○		維持
172					7-10	脅威への迅速な対応として、運用センタからの新しいポリシールールと割当ての仕組みに対応できる機能を有すること。			○		○	○		維持
173					7-11	CPU使用率等の機器の状態や設定情報を表示することが可能であること。			○		○	○		維持
174					7-12	機器の障害が発生した場合、発生原因を解析するための機器情報を収集することが可能であること。			○		○	○		維持
175					7-13	セキュリティインシデントを監視システムに通知できる機能を有すること。			○		○	○		維持
176					7-14	イベントログを収集・分析し、セキュリティ監視を行うこと。			○		○	○		維持
177					7-15	SNMPv2相当以上の管理機能を有すること。			○		○	○		維持
178					7-16	サーバにソフトウェア及び設定情報のバックアップを取得し、障害時等にリストアが可能であること。			○		○	○		維持
179					7-17	WebベースのGUI（HTTPS）で操作が可能であること。			○		○	○		維持
180					7-18	導入した機器及び設定情報を管理サーバ等で一元的に監視・管理できること。			○		○	○		維持
181					7-19	機器の起動時において、自己診断を行える機能を有し、障害の影響が広範囲にわたる前に障害部分を検知できる機能を有すること。又は、同等の監視サービスを有すること。			○		○	○		維持
182				IPS	7-20	外部ネットワークやインターネットに対するすべての通信を対象とした不正接続防止機能を有すること。							○	維持
183					7-21	トラフィックを検査することで、ポリシー違反、脆弱性の悪用及び異常な動作を検知できる機能を有すること。							○	維持

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類		機能概要	設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
184					7-22	担当職員が指定した必要なトラフィックにのみIPSによるインスペクションを実施できる設定が可能な機能を有すること。							○	維持
185					7-23	担当職員からの求めに応じ、セキュリティログを追跡・分析して報告が可能な機能を有すること。							○	維持
186					7-24	パターンファイルの更新を自動的に適用できる機能を有すること。							○	維持
187					7-25	パターンファイルの更新はオンラインで行うことができ、再起動せずに最新の状態に反映できる機能を有すること。							○	維持
188					7-26	不正な通信（P2P、悪意のある通信等）の検知、当該通信の監視システムへの通知機能を有すること。							○	維持
189					7-27	新たに不正な通信（P2P、悪意のある通信等）プログラムが発生した場合には、対応したパターンファイルの更新をリモートで行える機能を有すること。							○	維持
190					7-28	port scan等によるDoS攻撃及びDDoS攻撃を検知することが可能な機能を有すること。							○	維持
191					7-29	不審・攻撃トラフィックをリアルタイムに検知、特定し、当該トラフィックに対する適切なアクションを取ることが可能な機能を有すること。							○	維持
192					7-30	脅威への迅速な対応として、運用センタからの新しいポリシールールと割当ての仕組みに対応できる機能を有すること。							○	維持
193					7-31	CPU使用率等の機器の状態や設定情報を表示することが可能であること。							○	維持
194					7-32	機器の障害が発生した場合、発生原因を解析するための機器情報を収集することが可能であること。							○	維持
195					7-33	セキュリティインシデントを監視システムに通知できる機能を有すること。							○	維持
196					7-34	イベントログを収集・分析し、セキュリティ監視を行うこと。							○	維持
197					7-35	SNMPv2相当以上の管理機能を有すること。							○	維持
198					7-36	サーバにソフトウェア及び設定情報のバックアップを取得し、障害時等にリストアが可能であること。							○	維持
199					7-37	WebベースのGUI（HTTPS）で操作が可能であること。							○	維持
200					7-38	導入した機器及び設定情報を管理サーバ等で一元的に監視・管理できること。							○	維持
201					7-39	機器の起動時において、自己診断を行える機能を有し、障害の影響が広範囲にわたる前に障害部分を検知できる機能を有すること。又は、同等の監視サービスを有すること。							○	維持
202		8	ダッシュボード機能	共通	8-1	回線帯域の利用状況及び脅威検知の状況を一元的に可視化するための表示画面を有すること。「9 ネットワーク可視化情報収集・分析機能（ダッシュボード）」を実現する機能を提供すること。					○	○		新規
203					8-2	IT資産情報、脆弱性の有無及び対応状況等を一元的に可視化するための表示画面を有すること。「24 IT資産管理・脆弱性管理機能（ダッシュボード）」を実現する機能を提供すること。					○	○		新規
204				ログ提供	8-3	次期統合ネットワーク内で取得及び保有している各機器に関するログを取得（ダウンロードや参照）するためのログ提供画面を提供すること。					○	○		新規
205					8-4	「10 ポータル機能」にダッシュボードに関するリンクを掲載し、そのリンクからダッシュボードに接続できること。					○	○		新規
206					8-5	次期統合ネットワーク内で取得及び保有している各機器に関するログにおいて、少なくとも、以下のログを収集、保管できること。 ・サーバ/ネットワーク機器等のsyslog ・プロキシサーバ/ファイアウォールのアクセスログ					○	○		新規

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類	機能概要		設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
207					8-6	個別システム管理責任者、サイバーセキュリティ担当参事官室、受注者等がその管理範囲に応じて必要な情報を取得（ダウンロードや参照）し、障害等の調査、分析が実施できるよう、各機能及びデータに対する認証・認可の仕組みを有すること。					○	○		新規
208					8-7	収集したログやローデータの検索、抽出ができ、ログ分析できること。					○	○		新規
209					8-8	収集したログやローデータは、少なくとも、以下の項目により対象データを絞り込んで取得（ダウンロードや参照）が可能なこと。 ・ホスト指定 ・IPアドレス指定 ・ユーザ指定 ・ログ出力時間帯指定					○	○		新規
210					8-9	収集したログやローデータは、ファイルサイズを指定して分割ダウンロードができること。（ログ量が多い場合を想定）					○	○		新規
211					8-10	収集したログやローデータは、少なくとも過去1か月のログをリアルタイムで取得（ダウンロードや参照）が可能なこと。					○	○		新規
212					8-11	ログ提供画面はログ分析内容ををグラフィカルに表示可能であること。					○	○		新規
213					8-12	ログ提供画面は少なくとも過去1か月のログをリアルタイムで表示できること。					○	○		新規
214					8-13	ログ提供画面は次期統合ネットワークに接続されている拠点から接続できること。					○	○		新規
215					8-14	定期的にレポートを生成しメール送信する機能を有すること。					○	○		新規
216					8-15	レポートの細やかなカスタマイズが可能なこと。					○	○		新規
217					8-16	ログ提供機能を実現する際に発生するWAN経由の通信（表示画面へのログ転送、ログのダウンロード等）において、業務通信への影響を最小限にするために、優先制御や帯域制御等による対処を行うこと。					○	○		新規
218					8-17	任意のグループごとにアラート条件のチューニングが可能なこと。					○	○		新規
219					8-18	GUI及びマニュアルが日本語であること。					○	○		新規
220		9	ネットワーク可視化情報収集・分析機能	共通	9-1	センタ的拠点及び中央センタに配備するネットワーク機器で生成したすべてのパケットのトラフィック情報の収集、保管、分析、可視化が可能であること。			○		○	○		新規
221					9-2	トラフィック情報は、少なくとも以下の情報を含むこと。 ・IPアドレス情報（送信元及び宛先） ・アプリケーション情報（HTTP、HTTPS、SSH、NFS 等） ・送信されるトラフィック量			○		○	○		新規
222					9-3	ネットワーク可視化情報収集・分析機能で発生するWAN経由の通信（トラフィック情報の管理サーバへの転送、ダウンロード等）において、業務通信への影響を最小限にするために、優先制御や帯域制御等による対処を行うこと。			○		○	○		新規
223					9-4	トラフィック情報を生成、収集する機器は、次期統合ネットワークで用意するラックに収容できること。			○		○	○		新規
224				ダッシュボード	9-5	回線帯域の利用状況及び脅威検知の状況を一元的に可視化するためのダッシュボードを有すること。			○		○	○		新規
225					9-6	ダッシュボードは回線帯域の利用状況や脅威検知の状況をグラフィカルに表示可能であること。			○		○	○		新規
226					9-7	ダッシュボードからドリルダウンにより特定の通信の詳細な確認、分析が可能であること。			○		○	○		新規
227					9-8	「I0 ポータル機能」にダッシュボードに関するリンクを掲載し、そのリンクからダッシュボードに接続できること。			○		○	○		新規
228					9-9	ダッシュボードは次期統合ネットワークに接続されている拠点から接続できること。			○		○	○		新規

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類		機能概要	設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
229					9-10	ダッシュボードは、個別システム管理責任者、サイバーセキュリティ担当参事官室、担当職員及び受注者等がその管理範囲に応じて必要な情報を参照できるよう、各機能及びデータに対する認証・認可の仕組みを有すること。			○		○	○		新規
230					9-11	定期的にレポートを生成しメール送信する機能を有すること。			○		○	○		新規
231					9-12	レポートの細やかなカスタマイズが可能なこと。			○		○	○		新規
232					9-13	任意のグループごとにアラート条件のチューニングが可能なこと。			○		○	○		新規
233					9-14	GUI及びマニュアルが日本語であること。			○		○	○		新規
234				トラフィック情報収集	9-15	トラフィック情報は以下に示す通信を対象として1分間隔で収集すること。なお、拠点内通信（利用拠点内、センタ的拠点内）は収集対象外とする。 ・利用拠点と中央センタ間通信、利用拠点とセンタ的拠点間通信 ・センタ的拠点と中央センタ間通信、センタ的拠点とセンタ的拠点間通信（異なる2つのセンタ的拠点間） ・政府共通ネットワークとの通信 ・中央センタ内の通信			○		○	○		新規
235					9-16	複数のネットワーク機器からのトラフィック情報を収集可能であること。			○		○	○		新規
236					9-17	重複したトラフィック情報を排除できる機能を有すること。			○		○	○		新規
237					9-18	トラフィック情報の収集による業務通信への影響を最小限にするためTAP等による分岐等の対処を行うこと。			○		○	○		新規
238				トラフィック情報生成	9-19	ミラー構成においてすべてのパケットのトラフィック情報の生成が可能であること。			○		○	○		新規
239					9-20	センタ的拠点及び中央センタに配備するネットワーク機器で生成するトラフィック情報を複数の宛先に送信することが可能なこと。			○		○	○		新規
240				トラフィック情報分析	9-21	トラフィック情報から回線帯域の利用状況及び脅威検知の状況の解析が可能であること。			○		○	○		新規
241					9-22	関連する上り／下り（片方向）のトラフィック情報を1つのトラフィック情報として表示することで分析を行いやすくし、かつトラフィック情報の容量が節約可能であること。			○		○	○		新規
242					9-23	ホストやIPサブネットに識別名を付与し、任意のグループ分けを行い、グループごとにトラフィック情報の可視化が可能であること。			○		○	○		新規
243				回線帯域利用の可視化	9-24	拠点単位、個別システム単位で過去1年分のトラフィック情報の参照・取得が可能であること。			○		○	○		新規
244					9-25	トラフィック情報に関するローデータがリアルタイムに参照・取得が可能であること。			○		○	○		新規
245					9-26	回線帯域利用の可視化機能における表示画面は、少なくとも、下記項目により対象データを絞り込み、参照・取得が可能であること。 ・IPアドレス ・時間帯 ・対象拠点 ・ホスト			○		○	○		新規
246					9-27	回線帯域利用の可視化における表示画面は、下記情報を参照・取得が可能であること。 ・個別システム単位の通信状況や帯域利用量 ・個別システム単位の通信ログ情報			○		○	○		新規
247				脅威検知	9-28	トラフィック情報から標的型攻撃の各段階(偵察・攻撃準備、攻撃、感染拡大、実行)の脅威に対し検知可能であること。			○		○	○		新規
248					9-29	トラフィック情報から少なくとも以下の脅威を検知し優先度をつけることが可能であること。 ・偵察行為（ネットワークスキャン） ・C&C通信 ・エクスプロイト（ウイルス・ワームの感染、感染の拡大） ・DDoS攻撃 ・情報漏えい（データ収集、流出） ・ポリシー違反（非承認アプリケーションの利用／ネットワークの不正利用）			○		○	○		新規

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類	機能概要		設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
249					9-30	脅威検知機能における表示画面は、下記情報を参照・取得できること。 ・中央センタ内及び拠点間（中央センタ、センタ的拠点、利用拠点）のトラフィック情報による脅威検知の情報 ・感染源の特定に関する情報 ・感染範囲／影響範囲の特定に関する情報			○		○	○		新規
250					9-31	脅威検知機能における表示画面から脅威検知に関するローデータがリアルタイムに参照・取得できること。			○		○	○		新規
251					9-32	個別システム管理責任者の表示画面から参照・取得できる脅威検知情報は、リアルタイムで表示する情報と受注者で精査後にアラートで提供する情報とを選別する等して、情報の精度に留意し運用に混乱を生じさせないようにすること。			○		○	○		新規
252					9-33	脅威検知に関するローデータのダウンロード等による業務通信への影響を最小限にするために、優先制御や帯域制御等による対処を行うこと。			○		○	○		新規
253		10	ポータル機能	ポータル機能の画面に共通する要件	10-1	ポータル機能の画面に共通する要件を以下に示す。 ＜共通要件＞ ・左メニュー下にサービスデスクの連絡先(TEL、FAX、Mail)を常に（他の画面へ遷移しても）表示すること。 ・URL張り付けができること。 ・PDF、Micrcosoft Word2016、同Excel2016、同PowerPoint2016形式のファイルを文書に添付できること。 ・利用者が添付ファイルをダウンロードできること。 ・下記に示す全利用者向けの画面を除いて、認証による画面アクセス制御ができること。 「ポータルトップ・お知らせ」 「申請書・マニュアル類掲載」 「FAQ掲載」 「スケジュール」 「障害状況表示」 ・アクセス権限を有さない利用者にはメニューが非表示となること。					○	○		維持
254				ポータルトップ・お知らせ	10-2	当画面には、担当職員及び次期統合ネットワークサービスデスクから次期統合ネットワーク利用上の利用者に向けたお知らせを掲載する。 ・権限を有する利用者がお知らせ情報の登録、削除、変更が行えること。 ・お知らせ情報に対して、掲載期間を時刻(hh:mm)単位で指定でき、予約投稿が可能であること。 ・お知らせ情報を一覧にて参照できること。 ・一覧画面から詳細画面に1クリックで遷移できること。					○	○		維持
255				申請書・マニュアル類掲載	10-3	当画面には、担当職員が承認した次期統合ネットワークに関する各種ドキュメント（申請書やマニュアル等）を掲載する。各種（申請書、マニュアル等）は、一覧から参照及びダウンロードを可能とする。各種資料は、担当職員が承認したものを掲載する。 ・各種ドキュメントの登録、削除、変更が行えること。 ・各種ドキュメントを一覧にて参照できること。 ・各種ドキュメントが一覧からダウンロード可能であること。					○	○		維持
256				FAQ掲載	10-4	当画面には、次期統合ネットワークにおいてよくある問合せ（FAQ）を掲載する。掲載するFAQは、次期統合ネットワークサービスデスクにて管理する問合せを受注者が取りまとめ、担当職員が承認したものである。 ・FAQの登録、削除、変更が行えること。 ・FAQを一覧にて参照できること。 ・FAQはカテゴリにより管理が可能であること。 ・FAQはキーワードによる検索が可能であること。					○	○		維持
257				スケジュール	10-5	当画面には、各拠点の計画停電や工事情報等のスケジュールを表示する。 ・スケジュール情報の登録、削除、変更が行えること。 ・スケジュール情報を一覧にて参照できること。 ・スケジュール情報をカレンダ表示できること。 ・スケジュール情報をカテゴリにより管理（登録、表示制御）が可能であること。 ・スケジュール情報を追加する際、工事等の期間を時刻単位で登録できること。 ・スケジュール情報を追加する際、拠点をあいまい検索（都道府県、拠点名の一部等にて検索）できること。					○	○		維持

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類		機能概要	設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
258				障害状況表示	10-6	当画面には、中央センタ＃1、中央センタ＃2、センタ的拠点、利用拠点のネットワーク機器・サーバ機器の障害状況を表示する。 ・障害状況の登録、削除、変更が行えること。 ・障害状況を一覧にて参照できること。 ・障害状況を「拠点所在地の都道府県」「拠点ID」「個別システム」「障害の優先度」「キーワード（拠点名の一部等）」により抽出して表示することが可能であること。 ・「発生日時」等によりソート表示が可能であること。					○	○		維持
259				稼働状況表示	10-7	当画面には、センタ的拠点、利用拠点のネットワーク機器・サーバ機器の稼働状況を表示する。 ・稼働状況を一覧にて参照できること。 ・一覧画面から詳細画面に1クリックで遷移できること。 ・稼働状況を「拠点所在地の都道府県」「拠点ID」「個別システム」「キーワード（拠点名の一部等）」により抽出して表示することが可能であること。					○	○		維持
260				トラフィック状況表示	10-8	当画面には、拠点単位、個別システム単位のトラフィック状況を表示する。 ・トラフィック状況を表示する「ポータル機能」では、「ネットワーク可視化情報収集・分析機能（ダッシュボード）」を閲覧するためのリンクを掲載することが可能であること。					○	○		変更
261				セキュリティ情報表示	10-9	当画面には、個別システムの脅威検知状況を表示する。 ・脅威検知状況を表示する「ネットワーク可視化情報収集・分析機能（ダッシュボード）」を閲覧するためのリンクを掲載することが可能であること。					○	○		新規
262				ログ取得	10-10	当画面では、次期統合ネットワークで取得及び保有している各機器に関するログを提供する。 ・「ポータル機能」では、「ダッシュボード機能（ログ提供）」及び「監視機能（ダッシュボード）」へのリンクを掲載することが可能であること。					○	○		新規
263				脆弱性情報表示	10-11	当画面には、個別システムの脆弱性情報を表示する。 ・「ポータル機能」では、「IT資産管理・脆弱性管理機能能（ダッシュボード）」のダッシュボードを閲覧するためのリンクを掲載することが可能であること。					○	○		新規
264				申請ワークフロー（申請・届出）	10-12	当画面では、申請・届出を行う。 ・「申請ワークフロー機能」へのリンクを掲載することが可能であること。					○	○		新規
265				検疫登録・更新	10-13	当画面では、検疫装置への機器の登録・更新を行う。 ・「検疫機能」へのリンクを掲載することが可能であること。					○	○		新規
266				申請ワークフロー（受領、承認・／否認）	10-14	当画面では、申請・届出の承認・否認を行う。 ・「申請ワークフロー機能」へのリンクを掲載することが可能であること。					○	○		新規
267				運用センタ稼働状況確認	10-15	当画面では、運用センタの稼働状況に関する報告資料（ファイル）の共有を行う。次期統合ネットワーク運営主体のみ閲覧可能とする。 ・ファイル共有のためのオンラインストレージサービスへのリンクを掲載することが可能であること。					○	○		新規
268				ノウハウ共有	10-16	当画面には、障害対応上のノウハウを表示する。 ・ノウハウの登録、削除、変更が行えること。 ・ノウハウを一覧にて参照できること。 ・ノウハウはカテゴリにより管理が可能であること。 ・ノウハウはキーワードによる検索が可能であること。					○	○		新規

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類		機能概要	設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
269				ファイル共有	10-17	当画面では、各種資料（ファイル）の共有を行う。 ・ファイル共有のためのオンラインストレージサービスへのリンクを掲載することが可能であること。					○	○		新規
270		11	検疫機能	検疫装置	11-1	ネットワーク上に流れるパケット（MACアドレス）を基に、許可・登録された機器情報と照合して未承認機器の接続を検知する機能を有すること。		○	○					維持
271					11-2	個別システム管理責任者が、検疫装置にて機器の登録・削除・閲覧等を行える機能を有すること。		○	○					変更
272					11-3	「10 ポータル機能」に「11 検疫機能」における機器の登録・更新を行うための画面に関するリンクを掲載し、そのリンクから接続できること。		○	○					変更
273					11-4	個別システム管理責任者が機器登録する前に、個別システム管理責任者の承認を得る等の接続可否の検証ができるワークフロー機能または運用方法が確立できること。更に、内部牽制を目的として、担当職員及び受注者等の第三者により、個別システム管理責任者の不正利用有無の確認を定期的に実施すること。		○	○					変更
274					11-5	検疫装置の設定変更やパターンファイルの更新等をリモートで行える機能を有すること。		○	○					維持
275					11-6	拠点に設置した検疫装置及び検疫装置の設定情報を管理サーバ等で一元的に監視・管理できる機能を有すること。		○	○					維持
276					11-7	1つの拠点で複数の個別システムが利用している場合、個別システム（セグメント）単位で検疫対象/対象外とする設定が可能な機能を有すること。		○	○					維持
277					11-8	不正機器の接続を検知し、監視システムへ通知する機能を有すること。		○	○					維持
278					11-9	不正機器の接続を検知した場合、不正機器の通信を遮断する機能を有すること。		○	○					維持
279					11-10	不正機器の識別に必要な情報（MACアドレス、IPアドレス等）を自動的に収集・登録する機能を有すること。		○	○					維持
280					11-11	SNMPv2による管理機能を有しており、セキュリティインシデントを監視システムへ通知できる機能を有すること。		○	○					維持
281					11-12	ソフトウェア及び設定情報をサーバにバックアップを取得し、障害時等にリストアが可能であること。		○	○					維持
282					11-13	個別システム単位で検疫装置の制御（検疫装置の利用有無の制御、MACアドレス、IPアドレス等の自動収集・登録・検知・遮断の制御など）・管理が可能な機能を有すること。		○	○					維持
283					11-14	個別システム管理責任者が検疫装置で操作（機器の登録・削除・閲覧等）できる対象範囲（担当者の属する個別システムの機器のみ）を限定できること。		○	○					変更
284					11-15	一定期間次期統合ネットワークに接続していない機器は、指定する期間で登録情報を削除する機能または運用方法を確立できること。		○	○					変更
285					11-16	一定期間次期統合ネットワークに接続していない機器の利用者に対して、登録削除前に継続利用要否の確認を通知し、登録削除後に削除通知する機能または運用方法を確立できること。		○	○					変更
286				検疫用L2スイッチ	11-17	ネットワーク構成上の役割に応じて導入し、パケットロスが起こらない十分な処理性能とポート数を有すること。		○	○					維持
287					11-18	レイヤ2のスイッチングを行えること。		○	○					維持

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類	機能概要		設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
288					11-19	IEEE802.1Q VLAN Taggingに準拠していること。		○	○					維持
289					11-20	IEEE802.1D、IEEE802.1s及びIEEE802.1wに準拠したスパニングツリー機能を有すること。		○	○					維持
290					11-21	IEEE802.3ad Link Aggregation機能を有すること。		○	○					維持
291					11-22	リンクフラッピングや、L2ループによるネットワーク全体への影響を抑えるため、ポートにて障害を検知した際、ポートを一時的に使用不可能な状態にし、更に一定時間経過後、自動的に再度利用可能にする機能を有すること。		○	○					維持
292					11-23	ループ障害を防ぐため、Bridge Protocol Data Unit（BPDU）を予期していないポートで受信した場合、そのポートが自動的にダウンすることでルートブリッジが変更されてしまう事態を防止する機能を用いること。		○	○					維持
293					11-24	トラフィック解析のためポートのミラーリング機能を有すること。		○	○					維持
294					11-25	SNMPv2相当以上の管理機能を有すること。		○	○					維持
295					11-26	ソフトウェア及び設定情報をサーバにバックアップを取得し、障害時等にリストアが可能であること。		○	○					維持
296					11-27	SSHv2相当以上のリモートコンソール機能を有すること。		○	○					維持
297					11-28	CPU使用率等の機器の状態や設定情報を表示することが可能であること。		○	○					維持
298					11-29	機器の障害が発生した場合、発生原因を解析するための機器情報を収集することが可能であること。		○	○					維持
299					11-30	機器の起動時において、自己診断を行える機能を有し、障害の影響が広範囲にわたる前に障害部分を検知できること。		○	○					維持
300					11-31	時刻同期機能を有すること。		○	○					維持
301		12	申請ワークフロー機能		12-1	次期統合ネットワークに関する申請・届出書についてワークフロー上での申請を可能とすること。					○	○		新規
302					12-2	申請・届出書は、「別紙10 申請・届出一覧」に示す現行統合ネットワークで利用されている申請・届出様式（Excel）を申請ワークフロー機能の申請フォームに添付して申請することを可能とすること。また、次期統合ネットワークで提供される新規サービスに関する申請・届出の手順についてもワークフローによる申請・届出を可能とすること。					○	○		新規
303					12-3	進行中のワークフローの状態を画面から確認できること。					○	○		新規
304					12-4	ワークフローの状態の変化に対応して自動通知メールが配信されること。					○	○		新規
305					12-5	申請済みの申請フォームから申請・届出書の内容を確認し承認、却下、差戻しが可能であること。					○	○		新規
306					12-6	代理承認が可能であること。					○	○		新規
307					12-7	許可された範囲で後続の承認者のスキップ（事後承認）や変更が可能であること。					○	○		新規
308					12-8	ワークフローは条件により分岐させることが可能であること。					○	○		新規
309					12-9	申請者、承認者について代理者の設定が可能であること。					○	○		新規
310					12-10	申請・届出書は、キーワードによる全文検索、データ項目による検索、ワークフロー属性による検索が可能であること。					○	○		新規
311					12-11	閲覧権限を設定することでワークフローの経路上に含まれない利用者による申請・届出書の確認が可能であること。					○	○		新規
312					12-12	申請フォーム上に添付する届出・申請書、添付ファイルを任意のフォルダへのダウンロードが可能であること。					○	○		新規
313					12-13	申請フォーム上に添付する申請・届出書のデータをCSV形式のファイルで出力が可能であること。					○	○		新規
314					12-14	申請ワークフロー機能上の操作は操作ログとして記録されること。					○	○		新規

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類	機能概要		設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
315					12-15	申請ワークフロー機能上の人事データには有効期間の設定が可能であること。					○	○		新規
316					12-16	「10 ポータル機能」に「12 申請ワークフロー機能」に関するリンクを掲載し、そのリンクから接続できること。					○	○		新規
317					12-17	個別システム管理責任者、サイバーセキュリティ担当参事官室、受注者等がその管理範囲に応じて必要な情報を参照し申請・届出が実施できるよう、各機能及びデータに対する認証・認可の仕組みを有すること。					○	○		新規
318		13	帯域予約（QoS）機能		13-1	ネットワーク1系、ネットワーク2系の両回線に対して、帯域予約ができること。	○		○					維持
319					13-2	各拠点の回線において、指定する通信単位（個別システム、個別システムのサブシステム（Web会議やマイナンバーのトラフィック等）単位）でトラフィック種別による通信の上り下りの双方向に帯域予約ができる機能を有すること。	○		○					維持
320					13-3	回線障害時のバックアップ運用（ネットワーク1系又はネットワーク2系のいずれか一方のみで通信している状態）においても、帯域予約ができること。また、バックアップでの運用中においても、ネットワーク1系又はネットワーク2系の通信トラフィックが、障害が発生していない回線であらかじめ定められている帯域予約及び優先制御の内容にて制御されること。	○		○					維持
321					13-4	中央センタ#2の帯域予約値は、中央センタ#1の帯域予約値の50%以上を割り当てること。	○		○					維持
322					13-5	予約する帯域幅を変更できること。また、1Kbps単位で設定可能であること。	○		○					維持
323					13-6	「SSL/TLS」のようなアプリケーションのデータ部分のみを暗号化する方式ではなく、IPsec(トランスポートモード)のようにTCPヘッダ部分まで暗号化された通信においてもパケットヘッダのCOS値又はTOS値を利用し、ルータ及び回線サービスの制御方式にて帯域予約を可能とすること。	○		○					維持
324					13-7	帯域の利用状況（個別システム、個別システムのサブシステム（Web会議やマイナンバーのトラフィック等）単位のピーク及び平均等）、トラフィック種別ごとの分布、その他傾向等について予約帯域に関する情報を収集し、報告できる機能を有すること。	○		○					維持
325					13-8	契約期間中におけるすべてのトラフィックデータを指定する通信単位で保管し、厚生労働省からの求めに応じ、整理・分析して提示が可能なこと。	○		○					維持
326					13-9	開庁時間帯（開庁日の夜間等を除いた時間帯）のトラフィックデータを抽出し、平均値、ピーク値の分布を月次で作成し報告が可能なこと。ピーク値の取り方については別途指示する。	○		○					維持
327					13-10	各拠点や外部接続環境において、制御及び管理可能なトラフィックを多数（約10個/拠点、約3個/個別システムの運用・保守事業者等）割当てられること。なお、現行統合ネットワークにおける帯域予約のシナリオ数は約75000程度となる。	○		○				○	維持
328					13-11	専用の保守用コンソールポートを有していること。	○		○					維持
329		14	ネットワーク回線	通信プロトコル及びルーティング方式	14-1	インターネットプロトコルに対応していること。	○							維持
330					14-2	拠点間及び中央センタと拠点間のトラフィックは、ネットワーク1系とネットワーク2系で可能な限り均等に負荷分散（フローベース等）させること。負荷分散を実現するにあたり、拠点にL3スイッチ等を設置しても良い。	○							変更
331					14-3	ネットワーク1系又はネットワーク2系の回線障害により、いずれかの通信経路が断たれた場合には、自動的に相互バックアップへ切替えを行うこと。また、バックアップでの運用中においても、ネットワーク1系又はネットワーク2系の通信トラフィックが、障害が発生していない回線であらかじめ定められている帯域予約及び優先制御の内容にて制御されること。	○							維持
332					14-4	ルーティングプロトコル等を利用したトラフィックの負荷分散処理（フローベース等）による通信経路の振分け及び中央センタ#1が被災した場合の中央センタ#2への切替え要件を考慮したアドレス設計を行うこと。	○							維持
333					14-5	検疫システム及び検疫用L2スイッチを除く次期統合ネットワーク機器（拠点設置用）は、ネットワーク1系とネットワーク2系を完全に別系統の機器で構成し、次期統合ネットワーク機器（拠点設置用）の故障によりネットワーク1系・ネットワーク2系の両ネットワークが利用できなくなることがないようにすること。	○							維持
334					14-6	次期統合ネットワークに接続する個別システムのルーティング情報を管理すること。	○							維持

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類	機能概要		設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
335					14-7	正常稼動時のルーティングイメージは「別紙9　補足資料 機能要件一覧」を参照すること。	○							維持
336					14-8	主系回線障害発生時のルーティングイメージは「別紙9　補足資料 機能要件一覧」を参照すること。	○							維持
337					14-9	主系ルータ障害発生時のルーティングイメージは「別紙9　補足資料 機能要件一覧」を参照すること。	○							維持
338					14-10	主系ファイアウォール障害発生時のルーティングイメージ（センタ的拠点のみ）は「別紙9　補足資料 機能要件一覧」を参照すること。	○							維持
339				バックボーン回線	14-11	「バックボーン回線」、「中継区間回線」、「アクセス回線」の位置付けについては「別紙9　補足資料 機能要件一覧」を参照すること。	○							維持
340					14-12	東日本経路、西日本経路等の複数の迂回経路を有して、大規模災害等の広域にわたる災害が発生した場合においても、次期統合ネットワーク全体のサービスを停止させないこと。	○							維持
341					14-13	ネットワークの中枢を担う全国中継用の機器は複数のキャリアビルに分散設置されていること。なお、そのキャリアビルは他のビルと補完関係にあり、１つのビル全体に及ぶ障害が全国中継の運用に支障を来さないこと。	○							維持
342					14-14	交換機等のバックボーン回線に係る機器については、すべて冗長化構成を有していること。	○							維持
343					14-15	バックボーン回線に障害が発生した場合には、自動的に経路切替えを行えること。	○							維持
344					14-16	バックボーンの通信ルートは国内に限定すること。	○							維持
345					14-17	接続可能なアクセス回線として、イーサネット網、DSL回線、高速デジタル回線、専用線、帯域専有型網及び帯域共用型網、モバイル回線等を収容できること。	○							変更
346				中継区間回線及びキャリアビル	14-18	センタ的拠点については、センタ的拠点自体は正常に稼働しているにも関わらず、アクセス回線を収容するネットワーク機器及びネットワーク機器を設置したキャリアビルの災害等でセンタ的拠点の通信の停止が起こらないようにキャリアビルを分散すること。その他の利用拠点については、2本のアクセス回線を可能な限り別のネットワーク機器に収容すること。	○							維持
347					14-19	キャリアビルに収容される機器については、すべて冗長化構成を有していること。ただし、構成上、冗長化させることが技術的に不可能な機器を除く。	○							維持
348					14-20	アクセス回線としてDSL回線を提供する場合は、可能な限り中継区間回線が最低帯域保証型の回線を提供すること。	○							維持
349					14-21	帯域保証型及び最低帯域保証型の回線を提供する場合には、ネットワーク設備を常時監視し、契約帯域における保証速度を保つよう、必要に応じてネットワーク設備の増強を実施すること。	○							維持
350				アクセス回線（ラストワンマイル）及び局舎ビル	14-22	センタ的拠点については、電力系/電話系のマルチキャリア回線を必須とし、モバイル回線は不要とする。利用拠点については、電力系/電話系のマルチキャリアを必須としないが、シングルキャリアの場合はモバイル回線をバックアップとして用意すること。電力系/電話系のマルチキャリアの場合はモバイル回線は不要とする。	○							変更

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類	機能概要		設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
351					14-23	128Kbpsを越える帯域を求める拠点に対しては、光回線でのサービスを提供すること。ただし、光回線を敷設するために必要な基盤設備が局舎ビルに準備することができないために光回線での提供が困難な場合であって、担当職員が認めた時に限り帯域占有型（メタル回線）での提供とする。メタル回線の場合、通信速度が低速となるため、モバイル回線等の代替手段を用意すること。 なお、帯域共用型（メタル回線又は光回線）網による接続を利用する場合にはこの限りではない。	○							変更
352					14-24	帯域共用型（メタル回線又は光回線）網による接続を利用する場合には、各々適切な回線を選定すること。ただし、帯域共用型（メタル回線又は光回線）が物理的に敷設できない等、帯域共用型（メタル回線又は光回線）での提供が困難な場合であって、担当職員が認めた時に限り帯域占有型（メタル回線）での提供とする。 なお、帯域共用型（メタル回線又は光回線）を敷設した拠点において、契約期間中に当該サービスが著しく不安定となる事象が認められた場合は、受注者の負担により帯域共用型の利用料で帯域占有型（メタル回線）を提供すること。	○							維持
353					14-25	日本全国に点在する拠点との接続において、イーサネット回線、DSL回線、高速デジタル回線、専用線等を活用し、回線サービス全体として厚生労働省が求める帯域占有型（帯域保証あり）又は帯域共用型（メタル回線又は光回線）のサービスを提供すること。	○							維持
354		15	データセンタ設備	共通	15-1	大規模災害等への対策として、中央センタを2箇所以上設置し、中央センタ#1が提供する機能を３時間以内に中央センタ#2で提供すること。中央センタ#1が被災した場合には中央センタ#2に切替えサービスを継続して提供するが、原則として、3ヶ月以内に中央センタ#1で提供するすべてのサービスを復旧させること。大規模災害等の被害状況によっては、担当職員の承認を得た上で、大規模災害時発生前の中央センタ#1とは別の場所で中央センタ#1のサービスを提供することも可とする。					○	○		維持
355					15-2	すべての中央センタは、国内に設置すること。					○	○		維持
356					15-3	中央センタを接続するアクセス回線については、各拠点側の帯域に応じて、必要十分な帯域を提供すること。ただし、中央センタ#2に接続するアクセス回線は中央センタ#1と同じ帯域を提供すること。					○	○		維持
357					15-4	中央センタ#1と中央センタ#2とのデータセンタ間通信回線を有効活用し、中央センタ#1の局所的な障害においても、中央センタ#2のネットワーク資源やサーバ資源を活用して中央センタ機能を提供できること。					○	○		変更
358					15-5	民間クラウド接続機能について、個別システムがルータ等を設置するラック及び電源を提供するとともに、接続するスイッチの運用保守についても実施すること。							○	維持
359				L2スイッチ	15-6	ネットワーク構成上の役割に応じて導入し、パケットロスが起こらない十分な処理性能とポート数を有すること。					○	○	○	維持
360					15-7	レイヤ2のスイッチングを行えること。					○	○	○	維持
361					15-8	IEEE802.1Q VLAN Taggingに準拠していること。					○	○	○	維持
362					15-9	IEEE802.1D、IEEE802.1s及びIEEE802.1wに準拠したスパニングツリー機能を有すること。					○	○	○	維持
363					15-10	IEEE802.3ad Link Aggregation機能を有すること。					○	○	○	維持
364					15-11	IEEE802.1p の優先制御機能を有すること。					○	○	○	維持
365					15-12	通信経路を限定し、アクセス制御を行える機能を有すること。					○	○	○	維持
366					15-13	宛先/送信元 IP アドレス、TCP/UDP ポート番号などにより指定した IP パケットのフィルタリング機能を有すること。					○	○	○	維持
367					15-14	リンクフラッピングや、L2ループによるネットワーク全体への影響を抑えるため、ポートにて障害を検知した際、ポートを一時的に使用不可能な状態にし、更に一定時間経過後、自動的に再度利用可能にする機能を有すること。					○	○	○	維持
368					15-15	ループ障害を防ぐため、Bridge Protocol Data Unit (BPDU) を予期していないポートで受信した場合、そのポートが自動的にダウンすることでルートブリッジが変更されてしまう事態を防止する機能を用いること。					○	○	○	維持
369					15-16	ポートごとに通信可能なMACアドレス、又はMACアドレス数を制限できること。					○	○	○	維持
370					15-17	トラフィック解析のためポートのミラーリング機能を有すること。					○	○	○	維持
371					15-18	SNMPv2相当以上の管理機能を有すること。					○	○	○	維持

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類		機能概要	設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
372					15-19	ソフトウェア及び設定情報をサーバにバックアップを取得し、障害時等にリストアが可能であること。					○	○	○	維持
373					15-20	SSHv2相当以上のリモートコンソール機能を有すること。					○	○	○	維持
374					15-21	CPU使用率等の機器の状態や設定情報を表示することが可能であること。					○	○	○	維持
375					15-22	機器の障害が発生した場合、発生原因を解析するための機器情報を収集することが可能であること。					○	○	○	維持
376					15-23	機器の起動時において、自己診断を行える機能を有し、障害の影響が広範囲にわたる前に障害部分を検知できること。					○	○	○	維持
377					15-24	時刻同期機能を有すること。					○	○	○	維持
378				L3スイッチ	15-25	ネットワーク構成上の役割に応じて導入し、パケットロスが起こらない十分な処理性能とポート数を有すること。					○	○	○	維持
379					15-26	レイヤ2及びレイヤ3のスイッチングを行えること。					○	○	○	維持
380					15-27	ハードウェアによるIPv4及びIPv6のルーティングに対応すること。					○	○	○	維持
381					15-28	IEEE802.1Q VLAN Taggingに準拠していること。					○	○	○	維持
382					15-29	IEEE802.1D、IEEE802.1s及びIEEE802.1wに準拠したスパニングツリー機能を有すること。					○	○	○	維持
383					15-30	IEEE802.3ad Link Aggregation機能を有すること。					○	○	○	維持
384					15-31	IEEE802.1pの優先制御機能を有すること。					○	○	○	維持
385					15-32	通信経路を限定し、アクセス制御を行える機能を有すること。					○	○	○	維持
386					15-33	宛先/送信元IPアドレス、TCP/UDPポート番号などにより指定したIPパケットのフィルタリング機能を有すること。					○	○	○	維持
387					15-34	リンクフラッピングや、L2ループによるネットワーク全体への影響を抑えるため、ポートにて障害を検知した際、ポートを一時的に使用不可能な状態にし、更に一定時間経過後、自動的に再度利用可能にする機能を有すること。					○	○	○	維持
388					15-35	ループ障害を防ぐため、Bridge Protocol Data Unit (BPDU) を予期していないポートで受信した場合、そのポートが自動的にダウンすることでルートブリッジが変更されてしまう事態を防止する機能を用いること。					○	○	○	維持
389					15-36	ポートごとに通信可能なMACアドレス、又はMACアドレス数を制限できること。					○	○	○	維持
390					15-37	トラフィック解析のためポートのミラーリング機能を有すること。					○	○	○	維持
391					15-38	SNMPv2相当以上の管理機能を有すること。					○	○	○	維持
392					15-39	ソフトウェア及び設定情報をサーバにバックアップを取得し、障害時等にリストアが可能であること。					○	○	○	維持
393					15-40	SSHv2相当以上のリモートコンソール機能を有すること。					○	○	○	維持
394					15-41	CPU使用率等の機器の状態や設定情報を表示することが可能であること。					○	○	○	維持
395					15-42	機器の障害が発生した場合、発生原因を解析するための機器情報を収集することが可能であること。					○	○	○	維持
396					15-43	機器の起動時において、自己診断を行える機能を有し、障害の影響が広範囲にわたる前に障害部分を検知できること。					○	○	○	維持
397					15-44	時刻同期機能を有すること。					○	○	○	維持

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名	分類	機能概要	設置場所							対応区分※
					WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
						利用拠点環境	センタ的拠点環境		#1	#2		
398		16 外部ネットワーク接続機能		16-1 外部ネットワークを接続するための専用の接続セグメントを中央センタ内に設置し、次期統合ネットワークと接続するための外部ネットワーク接続機能を提供すること。また、外部ネットワークと次期統合ネットワークとの接続仕様を策定し、本内容を調達仕様書「4.2.1.成果物」に示す、「接続仕様書」に含めること。							○	維持
399				16-2 中央センタ内に、外部ネットワークを接続する専用のセグメントを有すること。							○	維持
400				16-3 外部ネットワークの接続セグメントと内部ネットワークとのアクセス制御を行うファイアウォール機能を有すること。							○	維持
401				16-4 外部ネットワークの接続セグメントと内部ネットワークとの情報セキュリティ対策として、IDS/IPS機能を有すること。							○	維持
402				16-5 不正な通信（P2P、悪意のある通信等）を検知し、監視システムへ通知する機能を有すること。							○	維持
403				16-6 外部ネットワーク接続機能の構成例は「別紙9　補足資料 機能要件一覧」を参照すること。							○	維持
404	端末サービス	17 統合ログ分析機能		17-1 統合ログ分析機能を有すること。					○	○		変更
405				17-2 解析対象のログは日本国内に保管すること。					○	○		変更
406				17-3 セキュリティの観点から、次期統合ネットワークの外部へログを転送する通信は、ログ転送用の専用回線を準備した上で、暗号化又は仮想閉域網を利用する等の措置を講じること。					○	○		変更
407				17-4 ログ解析処理に特化した専用のDBを利用し、高速な処理が可能であること。					○	○		変更
408				17-5 GUIインタフェースは、可能な限り日本語対応であること。					○	○		変更
409				17-6 ログ解析には、傾向分析だけではなく、自動分析エンジン（SIEM）を使った相関分析が可能であること。					○	○		変更
410				17-7 セキュリティベンダが提供する最新の脅威情報等に関する情報を取り込み、提案者にて独自に相関分析ロジックの見直しやルールを加え常時最新化することが可能であること。また、自動分析エンジン（SIEM）基盤を用いた分析をグローバルで展開することにより得られる検知ロジックやルールのノウハウを自動分析エンジン（SIEM）にフィードバックすることで、検知精度を常に高度化すること。					○	○		変更
411				17-8 1つのログでは確認できないセキュリティインシデントに対して、イベントの種類・時間・発生頻度等の情報を基にして正常ではないふるまいを検出可能であること。					○	○		変更
412				17-9 新しい攻撃のシナリオを想定して対応する相関分析ルールを作成した場合、過去のログに遡って当該シナリオの発生有無を確認することが可能であること。					○	○		変更
413				17-10 ログの相関分析だけではなく、ログの変化量の相関分析や攻撃プロセスのロジック化など、複数の独自検知ルールに基づいた分析が可能であること。					○	○		変更
414				17-11 IPアドレスを有するすべてのログに関してIP Reputationリストとマッチングし、不正な通信を検出できること。					○	○		変更
415				17-12 統合ログ分析機能については、日本国内に設置されたセキュリティオペレーションセンターが運用するサービスとして導入すること。セキュリティオペレーションセンターでは、セキュリティアナリストが受信したログを元に24時間365日体制で分析・報告可能なこと。厚生労働省の求めに応じて、該当する個別システムや拠点の特定を行ったうえで報告すること。セキュリティ機器が出力する重要度（セベリティ）だけに依存するのではなく、実際の通信内容を確認のうえで攻撃の進行度合いを評価し、その評価結果を報告対象に含めること。また、確認された脅威に対する推奨対策を報告対象に含めること。報告された分析結果に対する問い合わせ回答についても、24時間365日体制で実施すること。中央センタに設置する場合は、同箇所にセキュリティアナリストが配置されていること。					○	○		変更
416				17-13 セキュリティオペレーションセンターが独自に取得した悪性URLリストを、（厚生労働省からの設定変更申請に拠らず）セキュリティ機器やネットワーク機器に自動適用・更新することが可能なこと。					○	○		変更
417				17-14 収集対象となるセキュリティログやアクセスログについては、導入するセキュリティ機器を原則対象とし、導入時に担当職員と協議すること。					○	○		変更

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名	分類	機能概要	設置場所							対応区分※
					WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
						利用拠点環境	センタ的拠点環境		#1	#2		
418		18 ふるまい検知（HTTP/HTTPS）機能		18-1 導入する機器については、電源装置を冗長化し、電源装置に障害が発生した場合に、冗長化電源から電源供給される構成とすること。					○	○		変更
419				18-2 アプリケーションをポート番号に依存せず識別することが可能であること。					○	○		変更
420				18-3 未知のマルウェア等の脆弱性攻撃に対する防御機能を有すること。					○	○		変更
421				18-4 ワームやボットネット通信の兆候を検知する機能を有すること。					○	○		変更
422				18-5 不正な通信を検知した際に通信を遮断する機能を有すること。					○	○		変更
423				18-6 未知のマルウェアへの感染と悪意のあるサーバへの通信を検知できること。					○	○		変更
424				18-7 未知のマルウェア感染が疑われる実行ファイルを検査し、そのマルウェアのシグネチャを生成、配信し、早期発見と対策が可能な機能を有すること。また、未知のマルウェアを検知した場合、以降において再度そのファイルを受信した際に通信を遮断できること。 なお、これらの機能はクラウド環境やインターネット等外部にファイル情報を送信することなく提供されること。					○	○		変更
425				18-8 パターンファイルの更新はオンラインで行うことができ、再起動せずに最新の状態に反映できること。					○	○		変更
426				18-9 未知のマルウェアを検知した際に、当該マルウェアの外部への不正な通信を内部プロキシサーバと連携して自動的又は手動で遮断する機能を有すること。					○	○		変更
427				18-10 厚生労働省からの求めに応じ、アクセスログを追跡・分析して報告が可能なこと。					○	○		変更
428				18-11 CPU使用率等の機器の状態や設定情報を表示することが可能であること。					○	○		変更
429				18-12 機器の障害が発生した場合、発生原因を解析するための機器情報を収集することが可能であること。					○	○		変更
430				18-13 情報セキュリティインシデントを次期統合ネットワークの監視システムに通知できること。					○	○		変更
431				18-14 ふるまい検知（HTTPS）機能でイベントログを収集・分析し、情報セキュリティ監視を行うこと。					○	○		変更
432				18-15 SNMPv2相当以上の管理機能を有すること。					○	○		変更
433				18-16 ソフトウェア及び設定情報をサーバにバックアップを取得し、障害時等にリストアが可能であること。					○	○		変更
434				18-17 WebベースのGUI（HTTPS）で操作が可能であること。					○	○		変更
435				18-18 導入した機器及び設定情報を次期統合ネットワークの管理サーバ等で一元的に監視・管理できること。					○	○		変更
436				18-19 機器の起動時において、自己診断を行える機能を有し、障害の影響が広範囲にわたる前に障害部分を検知できる機能を有すること。又は、同等の監視サービスを有すること。					○	○		変更
437				18-20 HTTPSを復号する機能を有する又はHTTPSを復号する機器を導入すること。					○	○		変更
438				18-21 HTTPSを復号する機能を実装するため、端末にインストールするSSL証明書を提供すること。ただし、端末へのSSL証明書の配布及び端末の設定変更は個別システムで実施する。					○	○		変更
439				18-22 機能要件及び非機能要件を満たすために必要となる、負荷分散装置、タップ装置及びL2スイッチ等は必要に応じて導入すること。					○	○		変更
440				18-23 ふるまい検知（HTTPS）で収集するイベントログは過去1年分以上を保存すること。ただし、分析結果については、2025年3月31日までは保存すること。また、磁気テープ等の外部媒体に保存することも可とする。なお、ログの取得・管理については、以下のURL情報を参考とすること。 http://www.nisc.go.jp/inquiry/pdf/log_shutoku.pdf 「平成23年度 政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書」（平成24年3月 内閣官房情報セキュリティセンター）					○	○		変更
441				18-24 ふるまい検知（HTTPS）で収集するイベントログは、次期統合ネットワークで稼働中のログ収集サーバへ取り込み、かつ、統合ログ分析の対象とすることができるようにすること。					○	○		変更
442		19 ふるまい検知（メール）機能		19-1 導入する機器については、電源装置を冗長化し、電源装置に障害が発生した場合に、冗長化電源から電源供給される構成とすること。					○	○		変更

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名	分類	機能概要		設置場所							対応区分※
						WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
							利用拠点環境	センタ的拠点環境		#1	#2		
443				19-2	次期統合ネットワークのメール中継サーバ及び厚生労働省LANシステムのメールサーバと連携し、メールの配送を実施すること。					○	○		変更
444				19-3	未知のマルウェア等の脆弱性攻撃に対する防御機能を有すること。					○	○		変更
445				19-4	ワームやボットネット通信の兆候を検知する機能を有すること。					○	○		変更
446				19-5	不正なメールを検知した際に自動的にメールを隔離する機能を有すること。					○	○		変更
447				19-6	未知のマルウェア感染が疑われる実行ファイルを検査し、そのマルウェアのシグネチャを生成、配信し、早期発見と対策が可能な機能を有すること。また、未知のマルウェアを検知した場合、以降において再度そのファイルを受信した際に自動的にメールを遮断できること。なお、これらの機能はクラウド環境やインターネット等外部にファイル情報を送信することなく提供されること。					○	○		変更
448				19-7	メールの本文中のURL及び添付ファイルとして送付されるマルウェアの接続先を解析し、脅威をリアルタイムで検知する機能を有すること。また、検知した不正な接続先情報を、導入済みのふるまい検知（HTTP）装置及びコンテンツフィルタリングサーバと連携し、不正なURLへの通信を自動遮断する機能を有すること。また、必要に応じて連携するために必要となる機器を導入すること。					○	○		変更
449				19-8	パターンファイルの更新はオンラインで行うことができ、再起動せずに最新の状態に反映できること。					○	○		変更
450				19-9	厚生労働省からの求めに応じ、アクセスログを追跡・分析して報告が可能なこと。					○	○		変更
451				19-10	CPU使用率等の機器の状態や設定情報を表示することが可能であること。					○	○		変更
452				19-11	機器の障害が発生した場合、発生原因を解析するための機器情報を収集することが可能であること。					○	○		変更
453				19-12	情報セキュリティインシデントを次期統合ネットワークの監視システムに通知できること。					○	○		変更
454				19-13	ふるまい検知（メール）機能でイベントログを収集・分析し、情報セキュリティ監視を行うこと。					○	○		変更
455				19-14	SNMPv2相当以上の管理機能を有すること。					○	○		変更
456				19-15	ソフトウェア及び設定情報については、サーバにバックアップを取得し、障害時等にリストアが可能であること。					○	○		変更
457				19-16	WebベースのGUI（HTTPS）で操作が可能であること。					○	○		変更
458				19-17	導入した機器及び設定情報を次期統合ネットワークの管理サーバ等で一元的に監視・管理できること。					○	○		変更
459				19-18	機器の起動時において、自己診断を行える機能を有し、障害の影響が広範囲にわたる前に障害部分を検知できる機能を有すること。又は、同等の監視サービスを有すること。					○	○		変更
460				19-19	機能要件及び非機能要件を満たすために必要となる、負荷分散装置、タップ装置及びL2スイッチ等は必要に応じて導入すること。					○	○		変更
461				19-20	ふるまい検知（メール）で収集するイベントログは過去1年分以上を保存すること。ただし、分析結果については、2025年3月31日までは保存すること。また、磁気テープ等の外部媒体に保存することも可とする。 なお、ログの取得・管理については、以下のURL情報を参考とすること。 http://www.nisc.go.jp/inquiry/pdf/log_shutoku.pdf 「平成23年度 政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書」（平成24年3月 内閣官房情報セキュリティセンター）					○	○		変更
462				19-21	ふるまい検知（メール）で収集するイベントログは、統合ログ分析の対象とすることができるようにすること。					○	○		変更
463				19-22	ふるまい検知（メール）の導入にあたってはミラー構成で導入（インライン構成は採用しない）し、性能テストを実施の上、性能テスト結果報告書を提出すること。					○	○		変更
464				19-23	ミラー構成用回線として、メール通信をタップする一部のセンタ的拠点（厚生労働省LANシステムのデータセンタ及びバックアップデータセンタ並びに日本年金機構）と、ふるまい検知（メール）機能を設置する中央センタ＃1との間に、必要となる通信帯域を想定した閉域WAN回線を冗長構成で提供すること。					○	○		変更
465				19-24	構築にあたっては、厚生労働省LANシステム及び日本年金機構と連携し、構築・テストを行うこと。					○	○		変更
466				19-25	前日分の日時レポートを掲載するポータルサイトを構築すること。本ポータルサイトは、担当職員のみアクセス可能とするよう権限管理を設定すること。					○	○		変更

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類		機能概要	設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
467		20	電子メールの中継機能		20-1	インターネットからのメールを厚生労働省LANシステム及び日本年金機構のメール中継サーバに中継する機能を提供すること。また、厚生労働省LANシステム及び日本年金機構のメール中継サーバからのメールをインターネットへ中継する機能を提供すること。							○	維持
468					20-2	厚生労働省LANシステム及び日本年金機構のメール中継サーバで提供しているメールのウイルス対策、スパム対策及びSPF認証等の機能と連携できる構成とすること。							○	維持
469					20-3	電子メールの中継機能は、厚生労働省占有とし、電子メールの中継機能が稼動する機器上に次期統合ネットワークで提供する機能以外の機能を稼動させることは不可とする。							○	維持
470					20-4	次期統合ネットワークのメール中継サーバから外部のメールサーバへのサーバ間通信において、暗号化機能を有すること。							○	変更
471					20-5	電子メールの中継機能の構成例は「別紙9　補足資料 機能要件一覧」を参照すること。							○	維持
472	オプションサービス	21	運用保守リモート機能		21-1	個別システムの運用保守事業者が遠隔地（運用保守事業者の拠点等）から運用保守作業を行うためのリモートアクセスを可能とすること。「22 運用保守リモート機能」を利用する対象システムについては、「別紙4 オプションサービスの利用対象システム」を参照のこと。							○	新規
473					21-2	個別システムの運用保守事業者の端末からL2TP/IPsecを利用してリモートアクセスを可能とするため、中央センタにVPN装置を設置すること。							○	新規
474					21-3	リモートアクセスのための専用のインターネット回線は敷設せず、中央センタに敷設するインターネット回線を利用すること。							○	新規
475					21-4	インターネット回線を利用する業務通信への影響を最小限にするために、優先制御や帯域制御等による対処を行うこと。							○	新規
476					21-5	個別システムの運用保守事業者が、各個別システムにて用意するターミナルサーバを経由して、個別システムへのリモートアクセスを可能とすること。							○	新規
477					21-6	個別システムの運用保守事業者の端末は、厚生労働省から事前に確認を受けた端末のみリモートアクセスを可能とすること。							○	新規
478					21-7	許可された端末のみがリモートアクセス可能とするため、端末の識別又は認証ができること。							○	新規
479					21-8	端末のアクセス制限を行う際に、利用可能な期間等を指定できること。							○	新規
480					21-9	運用保守リモート機能の構成例は「別紙9　補足資料 機能要件一覧」を参照すること。							○	新規
481		22	テレワーク機能	共通	22-1	利用者が出張及び外出の際にモバイル端末からインターネットを経由して次期統合ネットワークにアクセスするためのインターネットVPN接続機能を提供すること。「23 テレワーク機能」を利用する対象システムについては、「別紙4 オプションサービスの利用対象システム」を参照のこと。							○	維持
482					22-2	VPN接続を行うモバイル端末のOSは、Windows、Mac OS、Linux、iOS、Androidに対応していること。							○	維持
483					22-3	インターネットVPN接続ポイントを提供すること。							○	維持
484					22-4	不正な通信（P2P、悪意のある通信等）を検知し、監視システムへ通知する機能を有すること。							○	維持
485					22-5	インターネット経由のVPN通信路は暗号化すること。通信の暗号化については、要件定義書「4.10.4.1.セキュリティ機能の装備」の要件及び機能を実装すること。							○	維持
486					22-6	インターネットVPNを終端するにあたり、「6.ファイアウォール機能」にVPN終端機能を持たせる又は専用のVPN装置を導入すること。							○	維持
487					22-7	「23 テレワーク機能」の構成例は「別紙9　補足資料 機能要件一覧」を参照すること。							○	新規
488				ワンタイムパスワードトークン	22-8	VPN接続を行う際の情報セキュリティ対策として、スマートフォンへ導入が可能なソフトウェアトークン及びハードウェアトークンのワンタイムパスワードによる認証を行えること。トークンの必要数については、「別紙4 オプションサービスの利用対象システム」を参照のこと。							○	変更
489					22-9	個別システムの希望により、運用開始当初ハードウェアトークンを導入していても、翌年度以降からすべて又は一部のハードウェアトークンをソフトウェアトークンに切り替えることも可能とすること。							○	変更

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類		機能概要	設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
490				認証サーバ連携	22-10	VPN装置への認証を個別システム側の資格情報にて実現できるように、個別システムの認証サーバと連携すること。連携においては、VPN装置がRADIUS端末として個別システムの認証サーバに接続可能であること。							○	変更
491					22-11	パスワード有効期限切れのユーザに対して、VPN装置からユーザに通知できる機能または運用方法を確立できること。							○	変更
492		23	IT資産管理・脆弱性管理機能	IT資産情報収集	23-1	エージェントが導入されるネットワークセグメント全体をスキャンしてIT資産（仮想環境及びクラウド上のIT資産を含む）のIT資産情報を収集し、脆弱性によるリスクを自動的に発見し分類できること。「24 IT資産管理・脆弱性管理機能」を利用する対象システムについては、「別紙4 オプションサービスの利用対象システム」を参照のこと。					○	○		新規
493					23-2	OS、データベース、ネットワーク、アプリケーション層の資格情報で認証されたスキャンを用いることにより詳細情報の取得を可能とすること。					○	○		新規
494					23-3	個別システムに導入されるエージェントによりIT資産（仮想環境及びクラウド上のIT資産を含む）の以下の項目を含むIT資産情報を収集し、脆弱性によるリスクを自動的に発見し分類できること。 ＜IT資産情報項目＞ ・拠点名 ・個別システム名 ・ホスト名 ・IPアドレス ・MACアドレス ・OSバージョン ・パッチバージョン ・ソフトウェア名 ・ソフトウェアバージョン ・ベンダー名 ・インストール日					○	○		新規
495					23-4	エージェントの導入による個別システムの性能等への影響は最小限とすること。					○	○		新規
496					23-5	IT資産のIPアドレスが変更されても継続して追跡できること。					○	○		新規
497					23-6	スキャンを実施する定期的なスケジュールや対象範囲の設定が可能なこと。					○	○		新規
498					23-7	定期スキャンの未実施期間にネットワークに接続されたIT資産についてもIT資産情報を収集し、脆弱性によるリスクを自動的に発見し分類できること。					○	○		新規
499				脆弱性評価	23-8	CVSS等の業界標準に基づき、脆弱性対応の優先度を自動的に分類できること。また、脆弱性を悪用するエクスプロイトコードやマルウェアの確認状況等の時間的な指標も考慮した優先度付けも可能であること。					○	○		新規
500					23-9	IT資産の場所、管理部門、役割等の情報に基づく業務特性を踏まえた脆弱性対応の優先度を自動的に分類できること。					○	○		新規
501				改善計画管理	23-10	脆弱性対応に関連するパッチ、対応手順などの改善を計画する際に必要となる情報が提供されること。					○	○		新規
502					23-11	脆弱性対応に関する改善の進捗状況を追跡できること。					○	○		新規
503				脆弱性検査	23-12	IT資産におけるセキュリティの堅牢化（ハードニング）に関する設定標準（厚生労働省内で作成された標準を含む）に準拠していることを評価できること。 ＜設定標準（例）＞ ・Center of Internet Security (CIS) ・International Organization for Standardization(ISO) ・SysAdmin Audit Network Security(SANS) Institute ・National Institute of Standards Technology (NIST)					○	○		新規

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類		機能概要	設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
504				IT資産情報連携	23-13	既にIT資産管理ツールを整備している以下の個別システムからIT資産情報を定期的（週1回程度を想定）に収集し、「24 IT資産管理・脆弱性管理機能」に取り込むことができる機能を有すること又は開発すること。 ・厚生労働省LANシステム、日本年金機構LAN・社会保険オンラインシステム、ハローワークシステム、労働基準行政情報システム・労災行政情報管理システム 、労働保険適用徴収システム、労働局共働支援システム（IBM　Big Fix、Skysea、SystemWalker等のツールを利用している。） ・上記システムが次期統合ネットワークに接続する端末個体数は100,000とすること。（うちシンクライアントOS・ゼロクライアントOSの数が51,350台ある前提とすること）					○	○		新規
505					23-14	緊急にセキュリティ対応確認が必要な際にも情報を収集できるように、任意のタイミングで取り込みが可能であること。					○	○		新規
506					23-15	連携機能で取り込んだIT資産情報であっても「24 IT資産管理・脆弱性管理機能」を用いた脆弱性の評価が可能であること。					○	○		新規
507				ダッシュボード	23-16	「24 IT資産管理・脆弱性管理機能」のスキャンエンジンやエージェントから収集された個別システムのIT資産情報、脆弱性の有無、脆弱性に対する優先度などを一元的に可視化するためのダッシュボードを提供すること。					○	○		新規
508					23-17	「10 ポータル機能」にダッシュボードに関するリンクを掲載し、そのリンクからダッシュボードに接続できること。					○	○		新規
509					23-18	ダッシュボードは細やかなカスタマイズが可能なこと。					○	○		新規
510					23-19	ダッシュボードから個別システムのIT資産情報及び脆弱性情報等のレポート出力が可能であること。					○	○		新規
511					23-20	定期的にレポートを生成しメール送信する機能を有すること。					○	○		新規
512					23-21	レポートの細やかなカスタマイズが可能なこと。					○	○		新規
513					23-22	属性、分類、重要度等によるIT資産情報及び脆弱性情報のフィルタリングが可能なこと。					○	○		新規
514					23-23	複数の属性に基づいて自動的にIT資産情報を分類し、分類されたグループごとのレポート出力が可能なこと。					○	○		新規
515					23-24	個別システム管理責任者、サイバーセキュリティ担当参事官室、受注者等がその管理範囲に応じて必要な情報を参照し脆弱性対応が実施できるよう、各機能及びデータに対する認証・認可の仕組みを有すること。					○	○		新規
516				その他	23-25	「24 IT資産管理・脆弱性管理機能」の拡張機能等に関する定期的なアップデートは、自動更新及び手動更新が可能であること。					○	○		新規
517					23-26	スキャンエンジンを分散構成として収集したデータを集約するなど、業務通信への影響を最小限とすること。					○	○		新規
518					23-27	「24 IT資産管理・脆弱性管理機能」は、仮想環境及びクラウド上（監視対象機器を含む）での動作が可能であること。					○	○		新規
519		24	拠点設備	L3スイッチ	24-1	ネットワーク構成上の役割に応じて導入し、パケットロスが起こらない十分な処理性能とポート数を有すること。		○	○					維持
520					24-2	レイヤ2及びレイヤ3のスイッチングを行えること。		○	○					維持
521					24-3	ハードウェアによるIPv4及びIPv6のルーティングに対応すること。		○	○					維持
522					24-4	IEEE802.1Q VLAN Taggingに準拠していること。		○	○					維持

別紙9　機能要件一覧

※現行統合ネットワーク要件からの維持・変更・新規を区分している。

項番	サービス	機能名		分類	機能概要		設置場所							対応区分※
							WAN環境	拠点環境		運用センタ環境	中央センタ環境		外部接続環境	
								利用拠点環境	センタ的拠点環境		#1	#2		
523					24-5	IEEE802.1D、IEEE802.1s及びIEEE802.1wに準拠したスパニングツリー機能を有すること。		○	○					維持
524					24-6	IEEE802.3ad Link Aggregation機能を有すること。		○	○					維持
525					24-7	IEEE802.1pの優先制御機能を有すること。		○	○					維持
526					24-8	通信経路を限定し、アクセス制御を行える機能を有すること。		○	○					維持
527					24-9	宛先/送信元IPアドレス、TCP/UDPポート番号などにより指定したIPパケットのフィルタリング機能を有すること。		○	○					維持
528					24-10	リンクフラッピングや、L2ループによるネットワーク全体への影響を抑えるため、ポートにて障害を検知した際、ポートを一時的に使用不可能な状態にし、更に一定時間経過後、自動的に再度利用可能にする機能を有すること。		○	○					維持
529					24-11	ループ障害を防ぐため、Bridge Protocol Data Unit (BPDU) を予期していないポートで受信した場合、そのポートが自動的にダウンすることでルートブリッジが変更されてしまう事態を防止する機能を用いること。		○	○					維持
530					24-12	ポートごとに通信可能なMACアドレス、又はMACアドレス数を制限できること。		○	○					維持
531					24-13	トラフィック解析のためポートのミラーリング機能を有すること。		○	○					維持
532					24-14	SNMPv2相当以上の管理機能を有すること。		○	○					維持
533					24-15	ソフトウェア及び設定情報をサーバにバックアップを取得し、障害時等にリストアが可能であること。		○	○					維持
534					24-16	SSHv2相当以上のリモートコンソール機能を有すること。		○	○					維持
535					24-17	CPU使用率等の機器の状態や設定情報を表示することが可能であること。		○	○					維持
536					24-18	機器の障害が発生した場合、発生原因を解析するための機器情報を収集することが可能であること。		○	○					維持
537					24-19	機器の起動時において、自己診断を行える機能を有し、障害の影響が広範囲にわたる前に障害部分を検知できること。		○	○					維持
538					24-20	時刻同期機能を有すること。		○	○					維持