ネットワークセキュリティチェックシート結果表

（小規模機関用）

機関名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

作成者名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

作成日：＿＿＿＿＿＿＿＿＿＿＿＿

	不適合数	総合診断結果（計）
管理者チェックシート		
ベンダチェックシート		

管理者チェックシート

目的対象	項 目	機能要素	判定基準	判定条件	チェック結果	ガイドライン該当項目	備考
1. 通信形態							
1-1 接続相手の確認	1-1-1 他の接続先拠点におけるセキュリティ基準の確認	-	異なる法人の大規模機関型拠点と接続する場合、接続する大規模機関型拠点は「大規模機関チェックシート」の項目をチェックし、条件を満たしていること。	異なる法人と接続を行う際は、接続相手のセキュリティポリシーを明確にし、責任を明確にする必要がある。	□	6.10 B-1 6.10 B-3	
		-	異なる法人の小規模機関型拠点と接続する場合、接続する小規模機関型拠点は「小規模機関型 チェックシート」の項目をチェックし、条件を満たしていること。		□		
		-	サービスプロバイダと接続する場合、接続するサービスプロバイダは「サービスプロバイダ チェックシート」の項目をチェックし、条件を満たしていること。		□		
2. 通信ポリシー							
2-2 オープンネットワークの利用した拠点間の接続	2-2-1 同一法人以外の複数拠点と接続する場合の不正中継。異なる法人間で複数接続を行う際は、責任主体は各拠点にあり、不正な中継を禁止する必要がある。	VPN機能	ネットワークを利用して拠点間の接続をする場合、自拠点と接続された二つ以上の拠点を結んで不正な中継が禁止されているかチェックする。				
			ネットワークを利用して拠点間の接続をする場合、拠点と接続された２つ以上の拠点を結んで不正な中継が禁止されているかチェックする。	左記の不正な中継を禁止する対策が行われている。	□	6.10 C 4	
2-3 他拠点との接続処理	2-3-1 接続先拠点との通信に関する合意	VPN機能	下記の項目について拠点間で確認を行う。				
			文書によるサービス内容・運用形態の確認と合意がされている	左記の不正な中継を禁止する対策が行われている。	□	6.5 B (5)	
			VPN通信における合意がされている				
3. 拠点内の技術的セキュリティ							
3-3 High Secure Zone のセキュリティ	3-3-3 小規模機関のHigh Secure Zoneを起点とした、サービスプロバイダが提供するプロバイダサービス・中継サービス・ASPサービスの利用	プロキシ機能 ／VPN機能 ／ファイアウォール機能	SPが提供するプロバイダサービス・中継サービス・ASPサービスを利用において、SPのHigh Secure Zoneにある重要データや機器を改ざんや侵入から守るため、次のセキュリティ機能を整備する必要がある。				
			サービス妨害（DoS攻撃など）対策している。	左記の対策を実施しない場合は、High Secure Zoneが起点の各サービスの利用を禁止する。	□	6.5 B (1) 6.5 B (2) 6.5 B (3) 6.5 B (4) 6.5 B (5)	
			データの改ざん、不正侵入などに対する検知・防御･遮断対策している。				
			安全なインターネット接続の担保をしている。				
			ウィルス感染対策を行っている。				
			サービス利用におけるユーザ認証を行うをしている。				
			通信経路の安全対策をしている。				
			アクセス監視をしている。				
	3-3-5 小規模機関のHigh Secure Zoneを起点とした他拠点への接続	プロキシ機能 ／VPN機能 ／ファイアウォール機能	他拠点への接続において、小規模機関のHigh Secure Zoneにある重要データや機器を改ざんや侵入から守るため、次のセキュリティ機能を整備する必要がある。				
			サービス妨害（DoS攻撃など）対策している。	左記の対策を実施しない場合は、High Secure Zoneが起点の各サービスの利用を禁止する。	□	6.5 B (1) 6.5 B (2) 6.5 B (3) 6.5 B (4) 6.5 B (5)	
			データの改ざん、不正侵入などに対する検知・防御･遮断対策している。				
			安全なインターネット接続の担保をしている。				
			ウィルス感染対策を行っている。				
			サービス利用におけるユーザ認証を行うをしている。				
			通信経路の安全対策をしている。				
			アクセス監視をしている。				
3-4 Secure Zone のセキュリティ	3-4-1 小規模機関が自らの責任においてインターネット接続を行うケースについて	プロキシ機能 ／各サーバ機能	小規模機関がSPの提供するサービス以外の通信経路を用いてインターネットを利用する場合は、次の対策を行う。				
			High Secure ZoneとSecure Zone間のプロキシ機能による代理接続を行っている。	左記の対策を実施しない場合は、High Secure Zoneからインターネットへの接続を行わない。	□	6.5 B (1) 6.5 B (2) 6.5 B (3) 6.5 B (4) 6.5 B (5)	
			データの改ざん、不正侵入などに対する検知・防御･遮断対策している。				
			Secure Zoneからの安全なインターネット接続の担保をしている。				
			Secure Zoneでのウィルス感染対策を行っている。				
			通信経路の安全対策をしている。				
			ユーザ認証を行う。				
			アクセス監視をしている。				
3-6 内部セキュリティサービス	3-6-1 拠点内におけるセキュリティパッチなどの更新機能の実装	ゲートウェイ機能 ／プロキシ機能	セキュリティパッチの状態をチェックする。				
			パッチファイルは常に最新の状態である。	セキュリティパッチなどをインターネット経由で行う際、インターネット通信を許可されていないホスト・ゾーンに対して、パッチのダウンロードを行い必要なホストに配布することでセキュリティホールに対する攻撃の対策を行う。	□	6.5 B (4) 6.5 B (5) 6.10 B-3 I	

目的対象	項 目	機能要素	判定基準	判定条件	チェック結果	ガイドライン該当項目	備考
4. サービス種別							
4-2 医療機関向けの情報提供ASPサービスの利用 【提供サービス項目例】 （※資料2　P.4参照） ・情報提供サービス ・メールサービス ・地域連携サービス ・検査データ配信サービス ・外部保存サービス ・タイムスタンプサービス ・VAサービス	4-2-1 ASPサービスを利用する利用者の認証	サーバ機能	ASPサービス利用時のユーザ認証を行うの方法についてチェックする。				
			認証方法				
			ID/パスワードによるアカウント管理をしている。	サービスを提供しているユーザを左記のいずれかの方法で認証し、不正ユーザによる侵入・情報漏えいを防止しなければならない。（どれか一つをチェックできればよい）	□	6.5 B (1) 6.5 C (7)	
			ICカード/スマートカードでの認証を行っている。		□		
			バイオメトリック認証を行う。		□		
	4-2-2 情報提供ASPサービスの利用におけるセキュリティ対策	プロキシ機能 ／VPN機能 ／ファイアウォール機能	小規模機関にて実施されているセキュリティ対策をチェックする。				
			セキュリティ対策				
			ウィルス、DoS攻撃等に対する防御対策を行う。	ASPサービスにおいては、High Secure Zoneにある医療情報等の重要データや機器を改ざんや侵入から守るため、左記のセキュリティ要件を整え、接続を行う。	□	6.5 B (1) 6.5 B (4) 6.5 B (5)	
			改ざんや侵入に対する不正パケットの検知・遮断対策をしている。				
			アクセス監視をしている。				
			なりすまし防止のための通信経路の暗号化対策を行う。			6.10　B-1 6.10　B 3 6.10　C 1	
	4-2-3 ASPサービスを利用する際の中継サービス、プロバイダサービスとの同時利用の禁止	-	他サービスとの同時利用を禁止しているかチェックする。				
			プロバイダサービスとの同時利用の禁止を行う。	中継サービス、プロバイダサービス、リモート保守サービスとの同時利用の禁止することで、何らかのインシデントが発生した場合の脅威の拡散を防ぐことができる。	□	6.10 B-3	
			中継サービスとの同時利用の禁止を行う。				
	4-2-4 ホストのHigh Secure Zoneへの配置・格納	ゾーン	ASPサービスにより取得した医療情報がHigh Secure Zoneに格納されているかチェックする。				
			ゾーン種別				
			High Secure Zoneに配置している。	ホストはデータのセキュリティレベル・提供するサービス・利用形態を考慮してHigh Secure Zoneに配置をする。	□	7.3 B 7.4 C	
4-5 医療機関以外での重要情報提供ASPサービスの利用 【提供サービス項目例】 （※資料2　P.4参照） ・情報提供サービス ・メールサービス ・地域連携サービス ・外部保存サービス ・タイムスタンプサービス ・VAサービス	4-5-1 ASPサービスを利用する利用者の認証	サーバ機能	ASPサービス利用時のユーザ認証を行うの方法についてチェックする。				
			認証方法				
			ID/パスワードによるアカウント管理をしている。	サービスを提供しているユーザを左記のいずれかの方法で認証し、不正ユーザによる侵入・情報漏えいを防止しなければならない。（どれか一つをチェックできればよい）	□	6.5 B (1) 6.5 C (7)	
			ICカード/スマートカードでの認証を行っている。		□		
			バイオメトリック認証を行う。		□		
	4-5-2 情報提供ASPサービスの利用におけるセキュリティ対策	プロキシ機能 ／VPN機能 ／ファイアウォール機能	小規模機関にて実施されているセキュリティ対策をチェックする。				
			セキュリティ対策				
			ウィルス、DoS攻撃等に対する防御対策を行う。	ASPサービスにおいては、High Secure Zoneにある重要データや機器を改ざんや侵入から守るため、左記のセキュリティ要件を整え、接続を行う。	□	6.5 B (1) 6.5 B (4) 6.5 B (5)	
			改ざんや侵入に対する不正パケットの検知・遮断対策をしている。				
			アクセス監視をしている。				
			なりすまし防止のための通信経路の暗号化対策を行う。			6.10　B-1 6.10　B 3 6.10　C 1	
	4-5-3 ASPサービスを利用する際の中継サービス、プロバイダサービスとの同時利用の禁止	-	他サービスとの同時利用を禁止しているかチェックする。				
			プロバイダサービスとの同時利用の禁止を行う。	中継サービス、プロバイダサービス、リモート保守サービスとの同時利用の禁止することで、何らかのインシデントが発生した場合の脅威の拡散を防ぐことができる。	□	6.10 B-3	
			中継サービスとの同時利用の禁止を行う。				
	4-5-4 ホストのHigh Secure Zoneへの配置・格納	ゾーン	ASPサービスにより取得した重要な情報がHigh Secure Zoneに格納されているかチェックする。				
			ゾーン種別				
			High Secure Zoneに配置している。	ホストはデータのセキュリティレベル・提供するサービス・利用形態を考慮してHigh Secure Zoneに配置をする。	□	7.3 B 7.4 C	
4-7 メールサービス（プロバイダサービス） 【提供サービス項目例】 （※資料2　P.4参照） ・メールサービス	4-7-4 ユーザによる他ISPメールサーバ（Webメール）の利用	ゲートウェイ機能 ／プロキシ機能	ユーザの希望によりWebメールを利用する場合、利用上のリスクについて説明と合意が行われたかチェックする				
			SPが提供するインターネット接続サービスを利用したWebメールを利用している。	インターネット接続サービスにおけるWebメールの利用にあたっては、利用上のリスク等についてユーザへ説明し、合意を行った上で利用を許可する。	□	8.1.3 C (1)②	
	4-7-5 メールサービス（プロバイダサービス）を利用する際の中継サービス、ASPサービスとの同時利用を禁止	-	他サービスとの同時利用を禁止しているかチェックする。				
			ASPサービスとの同時利用を禁止しているしている。	中継サービス、ASPサービス、リモート保守サービスとの同時利用の禁止することで、何らかのインシデントが発生した場合の脅威の拡散を防ぐことができる。	□	6.10 B-3	
			中継サービスとの同時利用の禁止を行う。				
4-8 インターネット接続サービス（プロバイダサービス） 【提供サービス項目例】 （※資料2　P.4参照） ・インターネット接続サービス	4-8-3 インターネットのサイト閲覧に際して、外部サービス提供機関への中継サービス、ASPサービスとの同時利用の禁止	-	他サービスとの同時利用を禁止しているかチェックする。				
			ASPサービスとの同時利用を禁止しているしている。	中継サービス、ASPサービスとの同時利用を禁止しているしている。することで、何らかのインシデントが発生した場合の脅威の拡散を防ぐことができる。	□	6.10 B-3	
			中継サービスとの同時利用の禁止を行う。				
4-10 外部サービス提供機関/大規模医療サービス機関への接続（中継サービス） 【提供サービス項目例】 （※資料2　P.4参照） ・VPNサービス ・IXサービス ・ASPサービス	4-10-4 外部サービス提供機関との中継サービスにおいて、プロバイダサービス、ASPサービスの同時利用の禁止	-	他サービスとの同時利用を禁止しているかチェックする。				
			ASPサービスとの同時利用を禁止しているしている。	プロバイダサービス、ASPサービスの同時利用を禁止し、何らかのインシデントが発生した場合の他サービスへの脅威の拡散を防ぐ。	□	6.10 B-3	
			プロバイダサービスとの同時利用の禁止を行う。				

ベンダチェックシート

目的対象	項 目	機能要素	判定基準	判定条件	チェック結果	ガイドライン該当項目	備考
2．通信ポリシー							
2-1 中継の確認	2-1-1 アクセス回線または中継回線に導入されるWAN回線	WAN機能	共有型ネットワークを経由している場合、事業者が検知できないデータの盗聴、改ざんなどのハッキング手法が知られており、セキュリティに関する脆弱性があるため、通信に関するセキュリティを担保する必要がある。下記のWAN技術でどの技術を利用しているかチェックする。				
			共有型			6.10 B-3	
			インターネット	オープンネットワークを使用する場合はIKE/IPSECによる暗号化技術とPKI技術を利用し、設問2-2からチェックする。	□		
			専有型				
			IP-VPN	インターネット以外の専有型ネットワークを使用する場合は設問2-1-2でIKE/IPSecまたはSSL/TLSからチェックする。	□		
			広域イーサネット		□		
			専用線		□		
			ISDN		□		
	2-1-2 アクセス回線または中継回線の認証・暗号化通信方式	VPN機能 ／サーバ機能	アクセス回線または中継回線の認証・暗号化通信方式に、リスクアセスメントされた安全な方式を採用しているかチェックする。				
			IKE/IPSec	2-2-1のIKE/IPSecの要件を満していること。(※IPv6についても同様とする)	□	6.10 B-3	
			SSL/TLS	IP層以下が通信事業者によって担保されている（2-1-1にある専有型サービスを利用している）場合にこの通信方式での接続を許可する。	□		
			その他の方式	「医療情報の安全管理に関するガイドライン第２版」で参照されている、『「医療情報の安全管理に関するガイドライン」の実装事例に関する報告書』に挙げられたリスクに対してリスクアセスメントが行われて安全性が立証されていること。	□		
2-2 オープンネットワークを利用した拠点間の接続	2-2-1 オープンネットワークにおける脅威（盗聴・侵入・なりすましなど）からパケットを守るための、IKE/IPSECの設定	VPN機能	IKE/IPSECのパラメータとして、下記の最適な設定がされているかチェックする。				
			IKEパラメータ			6.5 B (1) 6.5 B (2) 6.5 B (3) 6.10 B-1 6.10 B-2 6.10 B-3 6.10 B-3Ⅱ 6.10 C-1 6.10 C-2 8.1.3 D (1)①	
			モード	メインモード	プロバイダ：どちらでも可 IX：メインモードに限定	□	
				アグレッシブモード			
			認証方式	RSAデジタル証明書認証方式	プロバイダ：どちらでも可 IX：RSAデジタル証明書認証方式	□	
				共通鍵認証方式			
			暗号化アルゴリズム	3DES-CBC	設定条件：左記のいずれか IX：AES128-CBCに限定	■	
				AES128-CBC			
				AES256-CBC			
			認証アルゴリズム	HMAC-MD5	プロバイダ：HMAC-SHA1以上 IX：HMAC-SHA1	□	
				HMAC-SHA1 またはSHA256以上			
			DHグループ	Group2 （離散対数1024ビット）	プロバイダ：どちらでも可 IX：Group2	□	
				Group14 （離散対数2048ビット）			
			Life Type	time（時間）	プロバイダ：どちらも可 IX：timeに設定	□	
				byte（バイト）			
			Life Duration	time（時間）	時間、バイトどちらのタイプでも特に規定は無い。条件としては、リキーを必ず行うこと。拠点間の機器の設定値にズレがある場合は、Life Durationの低い値にリキーのタイミングを合わせる。	□	
				byte（バイト）			
			IDペイロードタイプ（※RSAデジタル証明書認証方式のみ）	Distingushed Name	プロバイダ：いずれも可 IX：DN	■	
				FQDN			
				USER-FQDN			
				IPv4			
			IPSecパラメータ				
			モード	トンネルモード	プロバイダ：どちらも可 IX：トンネルモード	□	
				トランスポート			
			セキュリティプロトコル	ESP	プロバイダ：どちらでも可 IX：ESPに限定	□	
				AH			
			暗号化アルゴリズム	3DES-CBC	プロバイダ：左記のいずれも可 IX：AES128-CBCに限定	■	
				AES128-CBC			
				AES256-CBC			
			認証アルゴリズム	HMAC-MD5	プロバイダ：HMAC-SHA1以上 IX：HMAC-SHA1に限定	□	
				HMAC-SHA1 またはSHA256以上			
			DHグループ	Group2 （離散対数1024ビット）	プロバイダ：どちらでも可 IX：Group2	□	
				Group14 （離散対数2048ビット）			
			Life Type	time（時間）	プロバイダ：どちらも可 IX：timeに設定	□	
				byte（バイト）			
			Life Duration	time（時間）	時間、バイトどちらのタイプでも特に規定は無い。条件としては、リキーを必ず行うこと。拠点間の機器の設定値にズレがある場合は、Life Durationの低い値にリキーのタイミングを合わせる。	□	
				byte（バイト）			
			PFS（Perfect Forward Secrecy）	有効	通信の安全性を向上させるために有効にすること。	■	
			アプライアンスに設定されたIKE/IPSecの設定が2-2-1項に設定されているかチェックする。				
			アプライアンスに設定された項目が2-2-1項に準じた設定となっていること。		2-2-1項でチェックした設定がネットワーク機器に設定されていること。	■	
	2-2-2 オンデマンドなVPN接続の運用	VPN機能	IKE/IPSecによる安全性をさらに向上させるため、オンデマンドにVPN接続が運用されているかチェックする。				
			オンデマンドなVPN接続が運用されている。		通信の必要がないときはVPN接続を行わないこと。	□	-

目的対象	項 目	機能要素	判定基準	判定条件	チェック結果	ガイドライン該当項目	備考
2-3 他拠点及びインターネットへの接続処理	2-3-1 他拠点またはインターネットからの不正アクセス、不正侵入、情報漏えい等の脅威への防御対策	ファイアウォール機能 ／プロキシ機能 ／サーバ機能	セキュリティ対策に必要なアプライアンスを導入しているかチェックする。				
			アプライアンス種別				
			ファイアウォール／IDS／IPSを導入している。	他拠点またはインターネットへの接続境界に設置し、サービス妨害、不正アクセス等の行為から防御する。また、SPの内部ネットワークに設置し、外部からの不正アクセス、不正侵入等を監視する。	□		
			プロキシサーバまたはその機能を有する機器を導入している。	ユーザからのインターネットアクセスの代理アクセスを行う。			
	2-3-2 ファイアウォールやプロキシなどの外部と直接接続する機器でのロギングによるアクセス監視の実施。「2.2（3）SPC要件より」	ファイアウォール機能 ／サーバ機能	ログによる監査、またはユーザからの提供要請に応じることが常に可能であるかチェックする。また、ログのサービス基準をSPとして規定する。				
			ログ機能要件				
			発信元を特定することが可能である	ログによる監査、またはユーザからの提供要請に応じるための機能を実装している。	□	6.5 B (3) 6.5 C 4 6.5 C 5	
			アクセスポイントを特定することが可能である。				
			アクセス先を特定することができる				
			アクセス先でログを保存している				
	2-3-4 小規模機関間/大規模機関間の通信	ゲートウェイ機能	拠点間の不正侵入などの脅威から守るため、下記のSPによる適切なリスク対策が行われているかチェックする。				
			SPの中継サービスの経由による接続または、適切なリスク対策がされたSPによる通信管理がされている通信経路を利用している。	小規模機関や大規模機関間の通信はSPによる適切なリスク対策が行われている接続のみ許可していること。	□	6.10 I③	
3. 拠点内の技術的セキュリティ							
3-1 ホストの配置と役割	3-1-1 業務用端末、インターネット接続用端末、電子カルテ検査データ等の重要なデータを保持する端末または機器の配置	ゾーン	重要データを保持する端末がHigh Secure Zoneに配置されていることをチェックする。				
			ゾーン種別				
			High Secure Zoneに配置している。	業務において重要なデータを処理蓄積する機能を持つ端末または機器はHigh Secure Zoneに配置すること。	□	6.3 ～ 6.6 7.3 C (2) 1 7.3 C (2) 3	
3-2 外部からの脅威	3-2-1 インターネットなどの外部からHigh Secure Zone, Secure Zone への接続	VPN機能 ／サーバ	外部を起点とした次のゾーンへの接続を禁止しているかチェックする。				
			外部を起点とした、High Secure Zoneへの接続を禁止している。	外部を起点にした接続を禁止して、改ざんや侵入に対して資産を守る。	□	8.1.3 C (1)②	
			外部を起点とした、Secure Zoneへの接続を禁止している。				
	3-2-2 インターネットなどの外部からの攻撃（DoS的攻撃・不正形式パケットなど）の検知	ファイアウォール	ファイアウォール等のセキュリティ機器のポリシー設定をチェックする。				
			FW設定パラメータ				
			DoS攻撃/DDoS攻撃に対する防御設定	DoS攻撃/DDoS攻撃対する防御設定が有効になっていること。	□	6.5 B (5)	
			ポートスキャンに対する防御設定	ポートスキャン対する防御設定が有効になっていること。			
			不正パケットに対する防御設定	不正パケットに対する防御設定が有効になっていること。			
			不正アクセスに対する検知	不正アクセスに対する防御設定が有効になっていること。			
			不正侵入に対する検知・防御設定	不正侵入に対する検知・防御設定が有効になっていること。			
			ポートフィルタ機能の設定	ポートフィルタ機能が有効になっていること。			
			IPアドレスフィルタ機能の設定	IPアドレスフィルタ機能が有効になっていること。			
			コンテンツフィルタ機能の設定	コンテンツフィルタ機能が有効になっていること。			
			IPスプーフィング（なりすまし）に対する検知・	IPスプーフィング（なりすまし）に対する防御設定が有効になっていること。			
			ログ収集／解析機能の設定	ログ収集／解析機能が有効になっていること。			
	3-2-3 インターネットなどの外部からのウィルスによる脅威への対策		適切なウィルス感染対策が行われているかチェックする。				
			アンチウィルスサーバを導入している。	外部からのウィルスによる脅威を未然に防止する。	□		
	3-2-4 他拠点との接続合意がされていない通信	VPN機能	接続合意がされていない通信を禁止しているかチェックする。				
			合意の無い不正なアクセスを禁止している	他拠点と接続の合意がとれている通信のみを許可して、不正なアクセスを禁止する。	□	6.10 C 3 6.5 B (5)	
3-3 High Secure Zone のセキュリティ	3-3-1 接続の起点をHigh Secure Zoneとした Secure Zone、DMZ への直接アクセスの禁止	ゲートウェイ機能 ／プロキシ機能	接続の起点をHigh Secure Zone としたSecure Zone、DMZ への代理接続についてチェックする。				
			接続の起点をHigh Secure Zone としたSecure Zone、DMZ へのアクセスは内部プロキシ機能による代理接続を行っている。	High Secure Zone に格納されている電子カルテ・レセプトなどの重要データの漏えいを防ぐため、内部プロキシ機能により代理接続を行う。	□	8.1.3 C (1)②	
3-6 High Secure Zone間の通信	3-6-1 High Secure Zoneを起点とした通信におけるプロキシ機能の経由	ゲートウェイ機能 ／プロキシ機能	次の機能項目の導入についてチェックする。				
			セキュリティ要件（プロキシ機能）				
			ゾーン間通信の代理接続機能を導入している。	左記の項目を実施することでHigh Secure Zone間の直接的な接続を禁止し、拠点内のセキュリティの向上を図る。また、逆の接続は禁止する。	□	8.1.3 C (1)②	
			ゾーン間通信でのウィルスチェック機能を導入している。				
			ゾーン間通信のスクリーニング機能を導入している。				
			逆方向からの接続を禁止している。				

目的対象	項 目	機能要素	判定基準	判定条件	チェック結果	ガイドライン該当項目	備考
	3-6-2 インターネットアクセスにおけるウィルス感染、情報漏えい等の脅威へのプロキシ機能による防御対策	プロキシ機能 ／サーバ機能	プロキシ機能の設定をチェックする。				
			プロキシ設定パラメータ				
			内部ネットワークアドレスの遮蔽	内部ネットワークアドレスを遮蔽してい	□	6.5 B (5) 6.5 D 5	
			必要なプロトコル（HTTP、HTTPS、SSLなど）に限定した内部ネットワークからのアクセス	内部ネットワークからの必要なプロトコルのみ許可している。			
			適切な外部ネットワークアドレスの設定	適切な外部ネットワークアドレスの設定を			
			プロキシ経由のアクセスであることの外部への遮蔽	プロキシ経由のアクセスであることを外部に遮蔽している。			
			プロキシの利用認証機能の導入	プロキシの利用で利用者の認証を行ってい			
	3-6-3 ロギングを行いアクセスを監視する	プロキシ機能	ログ収集機能をチェックする。				
			ログ収集の要件				
			必要な期間のログを保存している。	ログによる監査、またはユーザからの提供要請に応じることが常に可能であること。また、ログのサービス基準をSPとして規定しておくこと。	□	6.5 B (3) 6.5 C 4 6.5 C 5	
			日時、ユーザ識別、送信元/送信先アドレス情報の識別など、いつでも監査が可能なメッセージ形式であること。				
			世代管理を行っている。				
			定期的かつ適切なバックアップを行っている。				
	3-6-4 High Secure Zone からの接続制限	プロキシ機能 ／VPN機能 ／ファイアウォール機能	患者データなど重要データのアップデート・閲覧において必要なアドレス・ポート・コンテンツに限定したフィルタによる制限（スクリーニング）が行われているかチェックする。				
			フィルタ機能				
			IPアドレスフィルタによる適切な制限が行われている。	患者データなど重要データのアップデート・閲覧の際、ホストのサービスを制限するための機能が実装されていること。	□	6.5 B (5) 6.5 D 5	
			ポートフィルタによる制限が適切に行われている。				
			コンテンツフィルタによる制限が適切に行われている。				
3-7 High Secure Zone と Secure Zone 間の通信	3-7-1 Secure Zoneを起点とした通信におけるプロキシ機能の経由	ゲートウェイ機能 ／プロキシ機能	次の機能項目の導入についてチェックする。				
			セキュリティ要件（プロキシ機能）				
			ゾーン間通信の代理接続機能を導入している。	左記の項目を実施することでHigh Secure Zone間の直接的な接続を禁止し、拠点内のセキュリティの向上を図る。また、逆の接続は禁止する。	□	8.1.3 C (1)②	
			ゾーン間通信でのウィルスチェック機能を導入している。				
			ゾーン間通信のスクリーニング機能を導入している。				
			逆方向からの接続を禁止している。				
	3-7-2 ロギングを行いアクセスを監視する。「2.2 (3) SPC要件より」	プロキシ機能	ログ収集機能をチェックする。				
			ログ収集の要件				
			必要な期間のログを保存している。	ログによる監査、またはユーザからの提供要請に応じることが常に可能であること。また、ログのサービス基準をSPとして規定しておくこと。	□	6.5 B (3) 6.5 C 4 6.5 C 5	
			日時、ユーザ識別、送信元/送信先アドレス情報の識別など、いつでも監査が可能なメッセージ形式であること。				
			世代管理を行っている。				
			定期的かつ適切なバックアップを行っている。				
	3-7-3 High Secure Zone からの接続制限	プロキシ機能 ／VPN機能 ／ファイアウォール機能	患者データなど重要データのアップデート・閲覧において必要なアドレス・ポート・コンテンツを限定し、フィルタによる制限を行い、情報漏えい・改ざんなどを防止する。				
			フィルタ機能				
			IPアドレスフィルタによる適切な制限が行われている。	患者データなど重要データのアップデート・閲覧の際、ホストのサービスを制限するための機能が実装されていること。	□	6.5 B (5) 6.5 D 5	
			ポートフィルタによる制限が適切に行われている。				
			コンテンツフィルタによる制限が適切に行われている。				
4. サービス種別							
4-8 インターネット接続サービス 【提供サービス項目例】 （※資料2　P.4参照） ・インターネット接続サービス	4-8-9 インターネット上のサイト閲覧に対する防御対策	サーバ機能	サイト閲覧に関して閲覧制限を用いているかチェックする。				
			スクリーニングにより安全なインターネット接続を行っている。	URLホワイトリスト機能により、利用者が業務で利用するサイトを限定することで、より安全なインターネット接続を行う。	□	6.5 B (4)	

目的対象	項 目	機能要素	判定基準	判定条件	チェック結果	ガイドライン該当項目	備考
5. 拠点内の物理的セキュリティ							
5-1 アプライアンスのセキュリティ	5-1-2 各ゾーンに配置・格納された機器・データに対する、破壊・盗難・事故・災害などの脅威への対策	-	機器・データに対する、破壊・盗難・事故・災害などの脅威に対する次のセキュリティ対策についてチェックする。				
			セキュリティ対策				
			破壊・盗難・事故・災害に対する安全対策	左記の対策が実施されていること。	□	6.10 C (4)	
			万一の場合の速やかなサービス復旧を目的とした事前対策				
	5-1-3 耐タンパ性のアプライアンスの利用	ゲートウェイ機能／サーバ機能	アプライアンスの耐タンパ性の確認				
			耐タンパ性を備えているアプライアンスを利用している。	項目5-1-4の「耐タンパ認証付メモリに重要情報を保存」のチェックを行う	□	6.5 D-1	
			耐タンパ性を備えていないアプライアンスを利用している。	項目5-1-4の「非耐タンパ認証付メモリに重要情報を保存」のチェックを行う	□		
	5-1-4 システムの設定や盗難、システム設定の変更、ネットワーク機器の改ざんへの対策	ゲートウェイ機能／サーバ機能	破壊・盗難防止のための設置場所における入退室管理および管理者のID/パスワード等による権限管理を下記のいずれかでチェックする。				
			耐タンパ性メモリ利用時の認証方法				
			耐タンパ認証付メモリに重要情報を保存している。	左記の対策が実施されていること。	□	6.10 B-1 6.10 C-7 8.1.1 C③	
			非耐タンパ認証付きメモリ利用時の認証方法				
			作業者の入館管理を行う	左記の対策が実施されていること。	□	6.10 B-1 6.10 C-7 8.1.1 C③	
			ログイン認証を行う				
			認証情報は定期的に変更する				
			改ざんなどを防止、故意、運用上で定期的にチェックする				
	5-1-5 個人情報等の重要なデータが端末に保存される場合において、情報の漏えいを防ぐための対策。	-	個人情報等を保存する端末が複数のサービスを利用する場合、アプライアンスの利用によって下記項目が運用上で規定しているかチェックする。				
			対策項目				
			プロバイダサービスと他サービスとの同時接続の禁止	同時利用の禁止することで、何らかのインシデントが発生した場合の脅威の拡散を防ぐことができる。	□	6.10 B-3	
			中継サービスと他サービスとの同時接続の禁止				
			ASPサービスと他サービスとの同時接続の禁止				
			個人情報等の重要なデータを保存する端末においてアプライアンスを用意しない場合、サービスの利用には下記項目をチェックする。				
			対策項目				
			各サービス毎に専用の端末を用意する	同時利用の禁止することで、何らかのインシデントが発生した場合の脅威の拡散を防ぐことができる。	□	6.10 B-3	
			個人情報等の重要データを保存しない端末について、下記項目をチェックする。				
			対策項目				
			個人情報等の重要なデータが保存しない端末と個人情報等の重要データを保存する端末との接続、情報共有が出来ないように適切な技術または運用上の手段（*）によって対策が講じられている。 （*）手段については備考欄に明記する。	重要データや機器を改ざんや侵入から守るため、守るべきセキュリティ要件を整え、接続を行う。	□	6.5 B (1) 6.5 B (4) 6.5 B (5)	