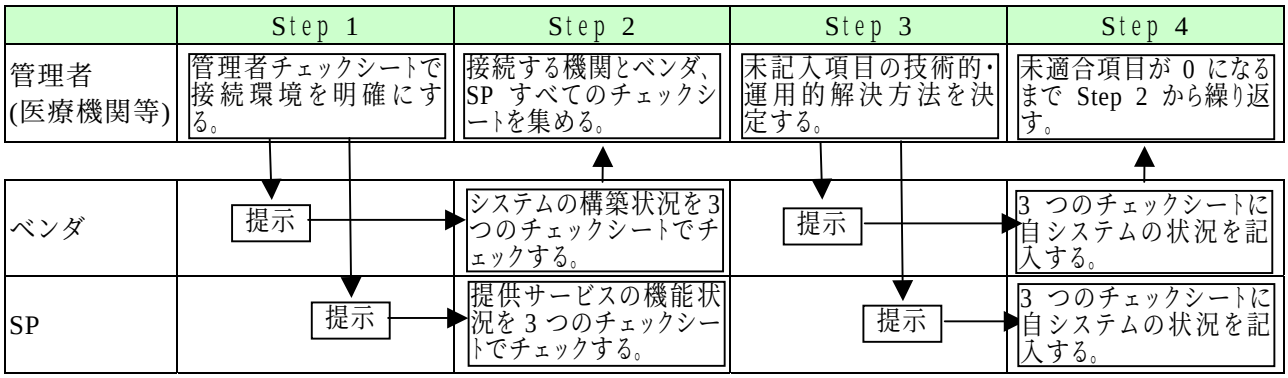
「医療情報システムの安全管理に関するガイドライン 第2版」 NWセキュリティチェックシート

本チェックシートは、対象となる機関や施設のNWセキュリティの「医療情報システムの安全管理に関するガイドライン第 2 版」への準拠度を診断するためのツールとしてご活用いただくものです。医療機関等の管理者は、本チェックシートでシステム・ベンダ並びにサービス・プロバイダ(SP)の提供するサービス内容や機能について確認した上で未対応項目について対策や責任の分担を明確にしてから契約してください(第 6.10 章 C6、C8)。

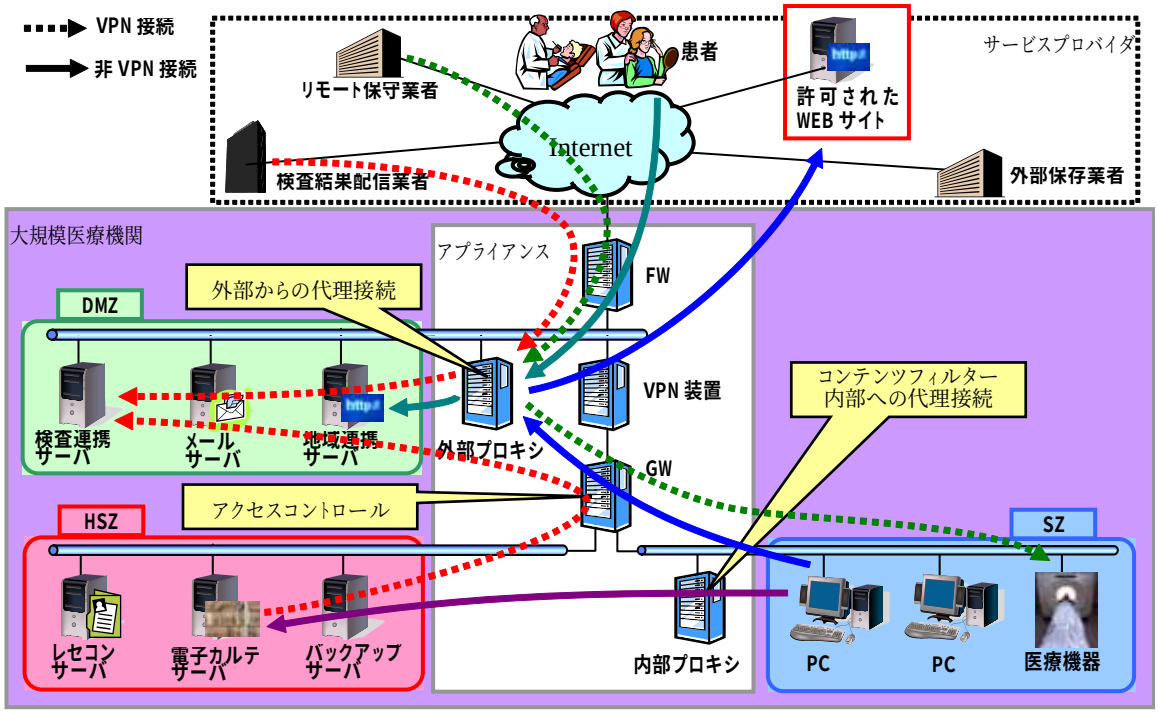
診断は、医療機関においてNWに関する責任を負っている「管理者」が責任を持ち、NW全体の設計や構築を行った「ベンダ」や第 6.10 章 C8 の回線事業者やオンラインサービス提供事業者にあたる「SP」と協同でチェックシートによって各自の提供できる機能を明確にして3者間の責任の分界点や所在を明確にします。このため、以下に示すステップで問題点の発見と対策を行うことを推奨します。



医療機関等並びに SP の管理者は、下記の定義と各機関のサービス内容を比較し、大規模機関、小規模機関、SP の中からチェックシートのチェック機関型式を決定してください。機関型式でチェック項目が変わりますので注意してください。

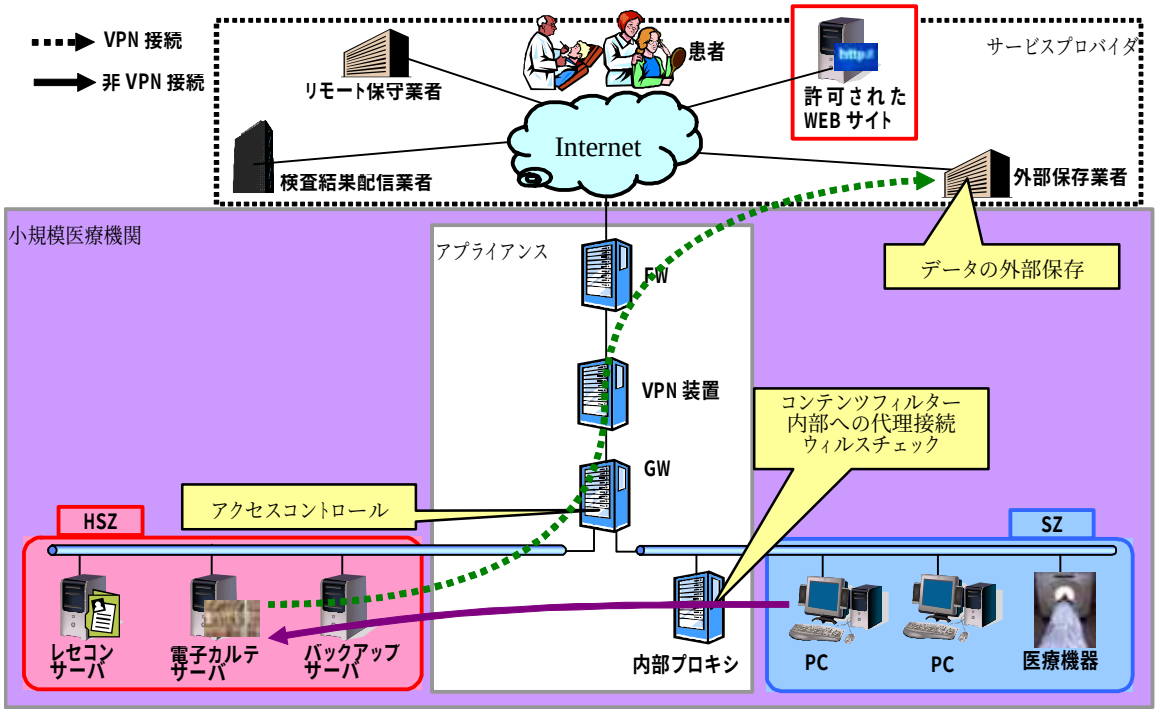
●大規模機関

大規模機関は、機関内の LAN 経由で複数の職員が医療情報や経理情報等の個人情報や機密情報を入出力や共有します。さらに、情報交換または情報提供するための設備を所有し、それらの一部の情報については、外部と下記のような NW 構成で情報交換します。



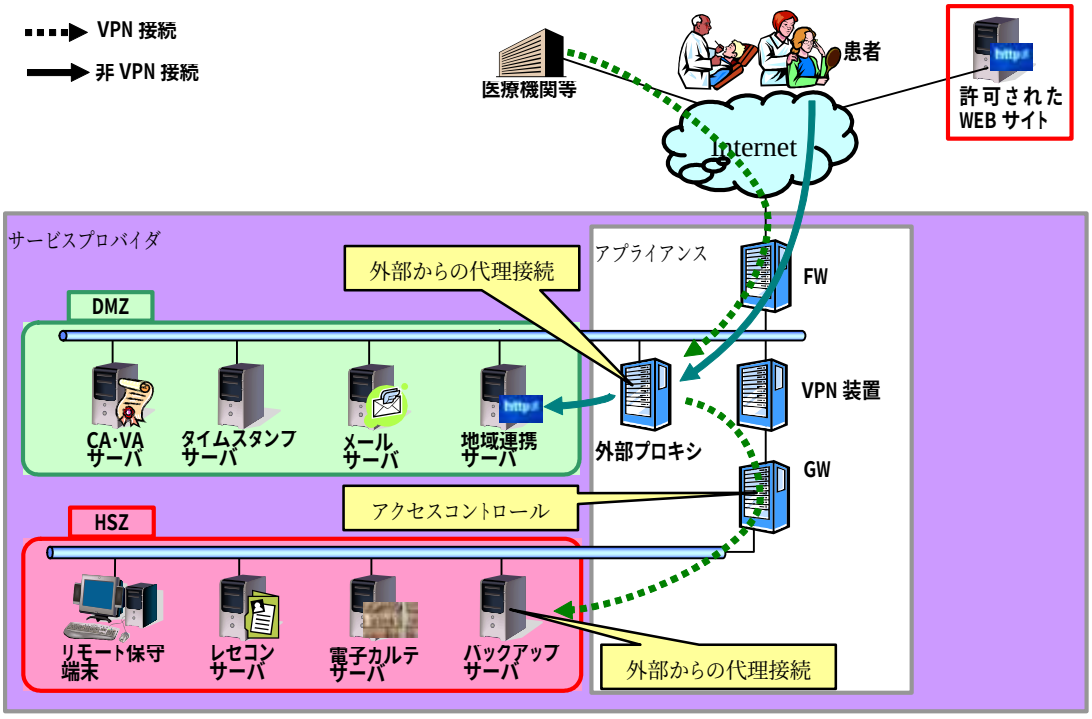
●小規模機関

小規模機関は、機関内の LAN 経由で複数の職員が医療情報や経理情報等の個人情報や機密情報を入出力や共有します。インターネット接続、メール等の情報交換、情報提供や外部保存等のサービスは SP の提供ービスを利用する。外部とは下記のような NW 構成で情報交換します。



●SP

SP は、医療機関等で発生した個人情報や機密情報を外部保存、またはその一部の情報を他の機関と情報交換または情報提供するための設備を所有し、それらの情報を下記のような NW 構成で情報交換します。また、タイムスタンプ、インターネット接続、コンテンツ・スクリーニング等の共通的なサービスも提供します。



【各ゾーンの説明】

HSZ (High Secure Zone)

ガイドラインの「第 6.3 章 組織的安全管理対策（体制、運用管理規程）」、「第 6.4 章 物理的安全対策」、「第 6.5 章 技術的安全対策」、「第 6.6 章 人的安全対策」が対処されおり、一部のリモート保守を除いて外部と直接データ交換しないエリア

SZ (Secure Zone)

ガイドラインの「第 6.4 章 物理的安全対策」が困難なため、これを「第 6.3 章 組織的安全管理対策（体制、運用管理規程）」、「第 6.5 章 技術的安全対策」、「第 6.6 章 人的安全対策」で対処しており、機関内で情報の入出力を行う、外部とのやり取りが制限される エリア

DMZ (De Militarized Zone)

ガイドラインの「第 6.4 章 物理的安全対策」が困難なため、これを「第 6.3 章 組織的安全管理対策（体制、運用管理規程）」、「第 6.5 章 技術的安全対策」、「第 6.6 章 人的安全対策」で対処しており、外部とデータ交換するエリア

機関名:＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

作成者:＿＿＿＿＿＿＿＿＿＿＿＿＿＿

作成日:＿＿＿＿年＿＿＿＿月＿＿＿＿日

機関型式:　大規模 ・ 小規模 ・ SP

	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		
SP チェックシート		

○管理者チェックシート

目的対象	項　　目	大規模機関型	小規模機関型	SP 型	備　考	ガイドライン該当項目
通信形態						
接続相手の確認	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チェックシートの各項目を満たしていますか？			■	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
	SP と接続する場合、接続する SP はチェックシートの各項目を満たしていますか？			■		
	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チェックシートの各項目を満たしていますか？			■		
	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チェックシートの各項目を満たしていますか？	■	■			
	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チェックシートの各項目を満たしていますか？	■	■			
通信ポリシー						
オープンネットワークを利用した拠点間の接続	同一法人以外の複数拠点と接続する場合, 不正な中継を禁止していますか？			■	オープンネットワークを利用した拠点間の接続をした場合、同時に複数の拠点と接続が可能になる。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。	6.10 C 4
	不正な中継を禁止していますか？	■	■			6.10 C 4
他拠点との接続	接続先拠点と通信に関して合意がなされていますか？				接続先拠点を文書･口頭などで合意を行い、サービス内容･運用形態等を確認し不正利用を防ぐ	6.5 B (5)
拠点内のセキュリティ						
HSZ のセキュリティ	インターネット接続を禁止していますか？				重要データが格納されているゾーンからの、インターネット接続を防ぐ。	6.5 B (5)
	各ホストでウィルスチェックを行っていますか？				格納したデータにウィルスが混在されていた場合の、発病･拡散を防ぐ。	6.5 B (4)
SZ のセキュリティ	インターネットへの HTTP 接続のサイト制限をしていますか？			■	業務上で必要なサイトのみを許可し、不正サイトによるウィルスの混入･情報漏えいを防ぐ。	
	各ホストでウィルスチェックを行っていますか？			■	格納したデータにウィルスが混在されていた場合の、発病･拡散を防ぐ。	6.5 B (4)
DMZ のセキュリティ	各ホストでウィルスチェックを行っていますか？		■		格納したデータにウィルスが混在されていた場合の、発病･拡散を防ぐ。	6.5 B (4)
内部セキュリティサービス	セキュリティパッチなどの更新機能を拠点内に装備していますか？				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対策を行う。	6.5 B (4) 6.5 B (5) 6.10 B-3 I
サービス運用例						
情報提供サービスの展開	医療機関向けに情報（診療記録、検査データ、診療サマリ、健診データ等）を公開･提供する場合、接続先･接続元の制限を行っていますか？		■		接続先拠点と通信に関して合意した接続先･元 IP アドレスのみ接続を許可し、自拠点と合意のない他拠点間の不正なアクセスを防ぐ。提供しているサービスポートのみを許可し、サービス不正利用･侵入を防ぐ。	6.10 B2
	医療機関向けに情報を公開･提供する場合、通信路を暗号化していますか？		■		オープンネットワークにおける脅威（盗聴･侵入など）からパケットを守るために、それらに対応可能な技術対策を講じる必要がある。	6.10 B-1 6.10 B 3 6.10 C 1
	医療機関向けに情報を公開･提供する場合、ログの収集を行う仕組みにし、実際に監視を行っていますか。		■		ログは、発信元･アクセスポイント･アクセスされた場所の 3 箇所で取る必要がある。本項目は発信元･アクセスポイントのログの収集を行う仕組みの確認になる。	6.5 B (3) 6.5 C 4 6.5 C 5

目的対象	項　　目	大規模機関型	小規模機関型	SP 型	備　考	ガイドライン該当項目
	患者向けに情報を公開･提供する場合、ユーザ認証を行っていますか？				不正なユーザによるデータの閲覧を防ぐ。	6.5 B (1) 6.5 C (7)
情報提供サービス（医療機関向け）の利用	医療機関向けの情報（診療記録、検査データ、診療サマリ、健診データ等）の提供サービスを利用する場合、アクセスするホストを限定していますか？				接続先拠点と通信に関して合意がなされている接続先･元 IP アドレスのみ接続を許可し、合意のなされていない自拠点から他拠点への不正なアクセスと、その逆を防ぐ。提供しているサービスポートのみを許可し、サービス不正利用･侵入を防ぐ。	6.10 B-3Ⅱ
	医療機関向けの情報（診療記録、検査データ、診療サマリ、健診データ等）の提供サービスを利用する場合、取得したデータは HSZ に格納していますか？				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適切なゾーンに配置をする。	7.3 B 7.3 C
インターネット接続サービス	業務･サービス上必要なサイトのみ接続の許可をしているか？				業務上で必要なサイトのみを許可し、不正サイトによるウィルスの混入･情報漏えいを防ぐ。	6.5 B (4) 6.5 B (5)
	インターネット接続サービスを提供するユーザの認証をしていますか？				サービスを提供しているユーザを認証することで、不正なユーザによる侵入･情報漏えいなどを防ぐ。	6.5 B (4) 6.5 B (5)
メールサービス	メールのスクリーニングを行っていますか？				スパムメール･ウィルス添付メール等から内部を守る。	6.5 B (4) 6.5 B (5)
	不正なメール転送を禁止していますか？				メール転送の踏み台になることを防ぐ。	6.5 B (4) 6.5 B (5)
	外部からの医療機器への接続をリモート保守サービスのみに制限していますか？				リモート保守を行うSPによる、不正アクセスを防ぐ。	6.10 B-1 8.1.1B
	リモート保守端末を HSZ に配置し、作業者の認証を行っていますか？				医療機器へアクセスの際は専門の技術者が接続し、不正なユーザによるアクセスを防止する。	6.10 B-1 6.10 C-7 8.1.1 C③

○ベンダ･チェックシート

目的対象	項　　目	大規模機関型	小規模機関型	SP 型	備　考	ガイドライン該当項目
通信ポリシー						
中継の確認	アクセス回線または中継回線に共用型ネットワークが使用されていますか？			[redacted]	はい：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、オープンネットワークとして扱いユーザ側で通信に関するセキュリティを担保する必要がある。 いいえ：オープンネットワークを使用しない。専用線･ISDNなどを利用する。 本チェックシート**「他拠点との接続」に進む**。	6.10　B-3
オープンネットワークを利用した拠点間の接続	IKE でユーザ認証を行っていますか？				オープンネットワークにおける脅威（盗聴･侵入など）からパケットを守るために、それらに対応可能な技術対策を講じる必要がある。	6.5 (1) 6.10 B-3Ⅱ 6.10 C-1
	IKE の認証は公開鍵または自動鍵配送機能を持った共通鍵方式ですか？					6.10 B-3Ⅱ 6.10 C-2
	セッション毎に共通鍵を自動決定していますか？					6.10 B-3Ⅱ 6.10 C-1
	IPSec による暗号化を行っていますか？					6.10 B-1 6.10 B-2 6.10 B-3 6.10 C 1
	IPSec でメッセージ認証を行っていますか？					6.10 B-3 8.1.3 D (1) ①
他拠点との接続	他拠点への接続先をアドレス･ポート等で制限していますか？				接続先拠点と通信に関して合意がなされている接続先 IP アドレスのみ接続を許可し、合意のなされていない自拠点から他拠点への不正なアクセスを防ぐ。他拠点で提供しているサービスポートのみを許可し、サービス不正利用･侵入を防ぐ。	6.5 B (5) 6.5 D 5
	他拠点からの接続元をアドレス･ポート等で制限していますか？				接続先拠点と通信に関して合意がなされている接続元 IP アドレスのみ接続を許可し、合意のなされていない他拠点から自拠点への不正なアクセスを防ぐ。自拠点で提供するサービスポートのみを許可し、サービス不正利用･侵入等を防ぐ。	6.5 B (5) 6.5 D 5
	ログの収集を行う仕組みによりアクセス監視（接続先･接続元）を行っていますか？				ログは、発信元･アクセスポイント･アクセスされた場所の 3 箇所で取る必要がある。本項目は発信元･アクセスポイントのログの収集を行う仕組みの確認になる。	6.5 B (3) 6.5 C 4 6.5 C 5
拠点内のセキュリティ						
アプライアンスのセキュリティ	ルータなどのネットワーク機器は、安全性が確認できる機器を利用していますか。				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などの対策がされた機器を使用する。	6.10 C4
ホストの配置役割	電子カルテ検査データ等の重要なデータを処理蓄積する機能は HSZ に配置していますか？				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適切なゾーンに配置をする。	6.3 ～ 6.6 7.3 C (2) 1 7.3 C (2) 3
	業務用端末インターネット接続用端末は SZ に配置していますか？			[redacted]		6.3　6.5 6.6
	情報公開外部サービス等の機能は DMZ に配置していますか？		[redacted]			6.3　6.5 6.6
外部からの脅威	外部から HSZ, SZ への接続を禁止していますか？			[redacted]	起点が外部から、HSZ, SZ への接続を禁止して、改ざんや侵入に対して資産を守る。	8.1.3 C (1) ②
	外部から HSZ への接続を禁止していますか？	[redacted]	[redacted]		起点が外部から、HSZ への接続を禁止して、改ざんや侵入に対して資産を守る。	8.1.3 C (1) ②

目的対象	項　　目	大規模機関型	小規模機関型	SP 型	備　考	ガイドライン該当項目
	外部からの攻撃（Dos 的攻撃・不正形式パケットなど）を検知できますか？		■		DMZ で公開しているサービスに対して、攻撃があった場合、それらのパケットを検知・遮断することで改ざんや侵入などから資産を守る。	6.5 B (5)
	他拠点との接続合意がなされている通信のみを許可していますか？				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)
HSZ のセキュリティ	接続の起点を HSZ とした SZ DMZ への直接アクセスを禁止していますか？			■	HSZ 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洩を防ぐ。	8.1.3 C (1) ②
	接続の起点を HSZ とした DMZ への直接アクセスを禁止していますか？	■	■		HSZ 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洩を防ぐ。	8.1.3 C (1) ②
SZ のセキュリティ	DMZ、HSZ からの直接アクセスを禁止していますか？		■	■	DMZ の公開サーバが外部からの不正アクセスにより侵入された場合、被害拡散を防止する。HSZ からの重要データの内部情報漏えい防ぐ。	6.5 B (5)
DMZ のセキュリティ	HSZ, SZ への直接アクセスを禁止していますか？		■		DMZ の公開サーバが外部からの不正アクセスにより侵入された場合、HSZ, SZ への被害拡散を防止する。	6.5 B (5)
HSZ と SZ 間の通信	接続の起点を SZ から行い、プロキシ機能を経由していますか？			■	HSZ への直接的な接続を禁止し、ウィルスチェックや制限を行うことで、拠点内のセキュリティの向上を図る。逆の接続は禁止する。	8.1.3 C (1) ②
	プロキシ機能でログの収集を行う仕組みにし、実際に監視を行っていますか？			■	「いつ」「だれが」「どこに」接続したかのログを収集することで、不正アクセスが生じた場合の監査を可能にする。	6.5 B (3) 6.5 C 4 6.5 C 5
	SZ からの接続をアドレス・ポートで制限していますか？			■	患者データなど重要データのアップデート・閲覧の際、ホストとサービスを制限し情報漏えいを防ぐ。	6.5 B (5) 6.5 D 5
HSZ と DMZ 間の通信	接続の起点を DMZ から行い、プロキシ機能を経由していますか？		■		HSZ への直接的な接続を禁止し、ウィルスチェックや制限を行うことで、拠点内のセキュリティの向上を図る。逆の接続は禁止する。	8.1.3 C (1) ②
	プロキシ機能でログの収集を行う仕組みにし、実際に監視を行っていますか？		■		「いつ」「だれが」「どこに」接続したかのログを収集することで、不正アクセスが生じた場合の監査を可能にする。	6.5 B (3) 6.5 C 4 6.5 C 5
	DMZ からの接続をアドレス・ポートで制限していますか？		■		患者向け診断情報提供サービスなどで、HSZ の情報の一部を閲覧・取得する場合、ホストとサービスを制限しで情報漏えい・改ざん等を防ぐ。	6.5 B (5) 6.5 D 5
DMZ と SZ 間の通信	接続の起点を SZ から行い、プロキシ機能を経由していますか？		■	■	DMZ への直接的な接続を禁止し、ウィルスチェックや制限を行うことで、拠点内のセキュリティの向上を図る。逆の接続は禁止する。	8.1.3C（1） ②
	プロキシ機能でログの収集を行う仕組みにし、実際に監視を行っていますか？		■	■	「いつ」「だれが」「どこに」接続したかのログを収集することで、不正アクセスが生じた場合の監査を可能にする。	6.5 B (3) 6.5 C 4 6.5 C 5
	SZ からの接続をアドレス・ポートで制限していますか？		■	■	DMZ の公開サーバなどの情報をアップデートする際、ホストとサービスを制限し、情報漏えい・改ざん等を防ぐ。	6.5 B (5) 6.5 D 5
サービス運用例						
情報提供サービスの展開	情報サービスにおいて HSZ の情報を提供する際、プロキシ機能を使用して外部ユーザから遮蔽していますか？		■		外部からの HSZ への直接的な接続を禁止し、ウィルスチェックや制限を行うことで、拠点内のセキュリティの向上を図る。	6.5 B (5)
外部保存サービスの利用	外部保存 SP が起点の接続を禁止していますか？			■	自拠点からのアップロードのみの接続を行うため、SP からの接続は禁止し不正アクセスを防ぐ。	8.1 8.1.3 C（1） ②
	外部保存を利用するホストは HSZ から接続していますか？			■	業務端末などが配置されている SZ からの外部保存 SP への不正なアクセスを防ぐ。	8.1

○SP チェックシート

目的対象	項　　目	大規模機関型	小規模機関型	SP 型	備　　考	ガイドライン該当項目
拠点内のセキュリティ						
ホストの配置役割	SP は、プロバイダ自身の社内ネットワークとサービスを提供するネットワークを切り離していますか？				サービス用ネットワークと自社ネットワークが連携することは想定されないので、物理的に切り離すことで不正アクセスを防止する。	6.5 B (2) 6.10 B-3 II
サービス運用例						
外部保存サービスの利用	外部保存サービスを提供するユーザの認証をしていますか？				サービスを提供しているユーザを認証することで、不正なユーザによる侵入・情報漏えいなどを防ぐ。	8.1 8.1.1 B 8.1.1 C ①
	データの格納時の DMZ から HSZ への通信はプロキシ機能等を経由して行い、外部・ユーザから遮蔽されていますか？				外部からの HSZ への直接的な接続を禁止し、ウィルスチェックや制限を行うことで、拠点内のセキュリティの向上を図る。	8.1 8.2.2 C ①
	ユーザのデータは HSZ に格納していますか？				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適切なゾーンに配置をする。	8.1 8.1.2 B 8.1.2 C