「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」技術・運用基準
チェックシート使用説明書

本チェックシートは、「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」に規定された医療機関等が医療情報を扱う際に守るべき事項を網羅的にまとめたものです。本チェックシートには、医療機関等が運用上守るべき事項から、技術的・システム的に守るべき事項まで全て網羅されています。医療機関等が自機関のチェックがし易いように、医療機関等をその機能によって下記のように分類し、チェックができるようにしました。また、医療機関等が「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」を守るためには、医療機関等だけではなく、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がこれを満足している必要があります。このため、チェックシートをサービス機能の提供者とそのチェックすべき事項に沿って、医療機関の管理者、システム・ベンダ、サービス・プロバイダのチェックシートに分けました。

また、ネットワークサービスや ASP サービス等を提供するサービス・プロバイダ（SP）は医療機関等の外にあって医療機関等の一部としてサービス機能を提供することになるため、医療機関等に準じて「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」の遵守をする必要があります。このため、サービス・プロバイダ（SP）についてもチェックシートを設けました。

まず、医療機関等やサービス・プロバイダ（SP）は下の定義に従って使用するチェックシートを選択してください。

- 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。大規模機関の構成を図１に示します。

- 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 の提供サービスを利用する。外部とは下記のような NW 構成で情報交換します。

- サービス・プロバイダ（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。

大規模機関、小規模機関、サービス・プロバイダ（SP）の特徴と、使用するチェックシートを表１にまとめました。

All Rights Reserved Copyright ©2007 保健･医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム

表１　各機関の概要

	医療機関等		ＳＰ
	大規模機関	小規模機関	
機能・設備	外部に情報提供できる設備を有する	外部に情報提供できる設備を有しない	回線事業者・オンラインサービス提供事業者
参照図	図１	図２	図３
必要となるチェックシート	大規模機関チェックシート	小規模機関チェックシート	ＳＰチェックシート

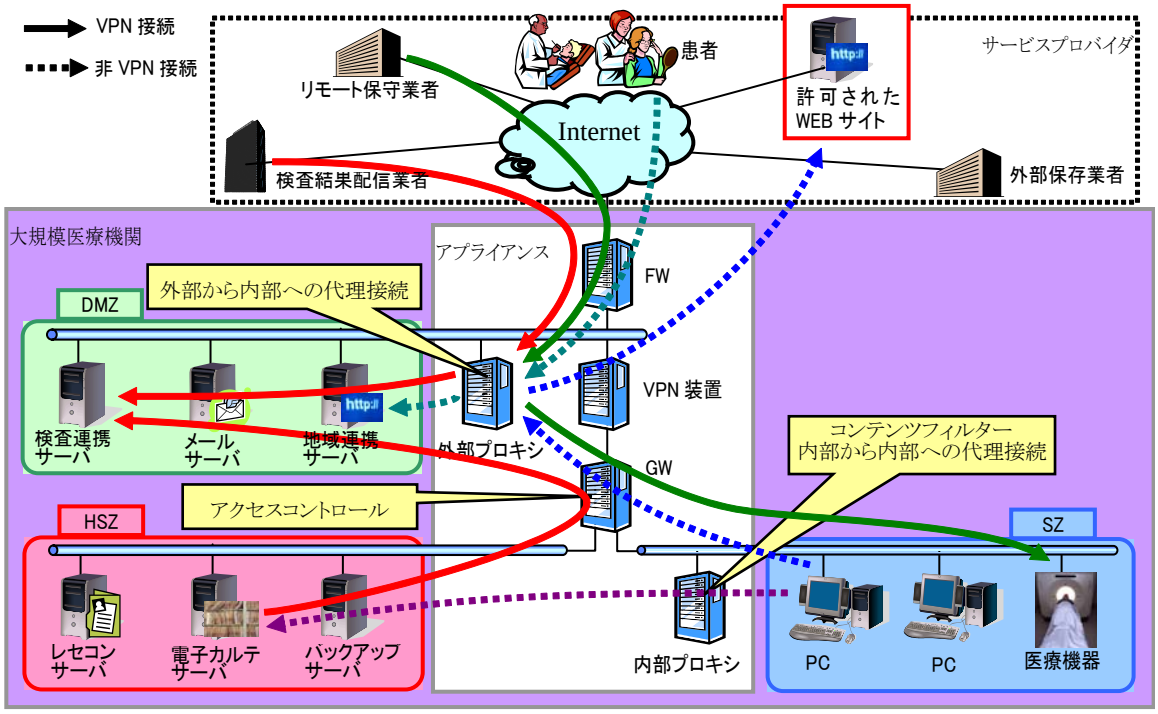


図１　大規模機関

All Rights Reserved Copyright ©2007 保健･医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム

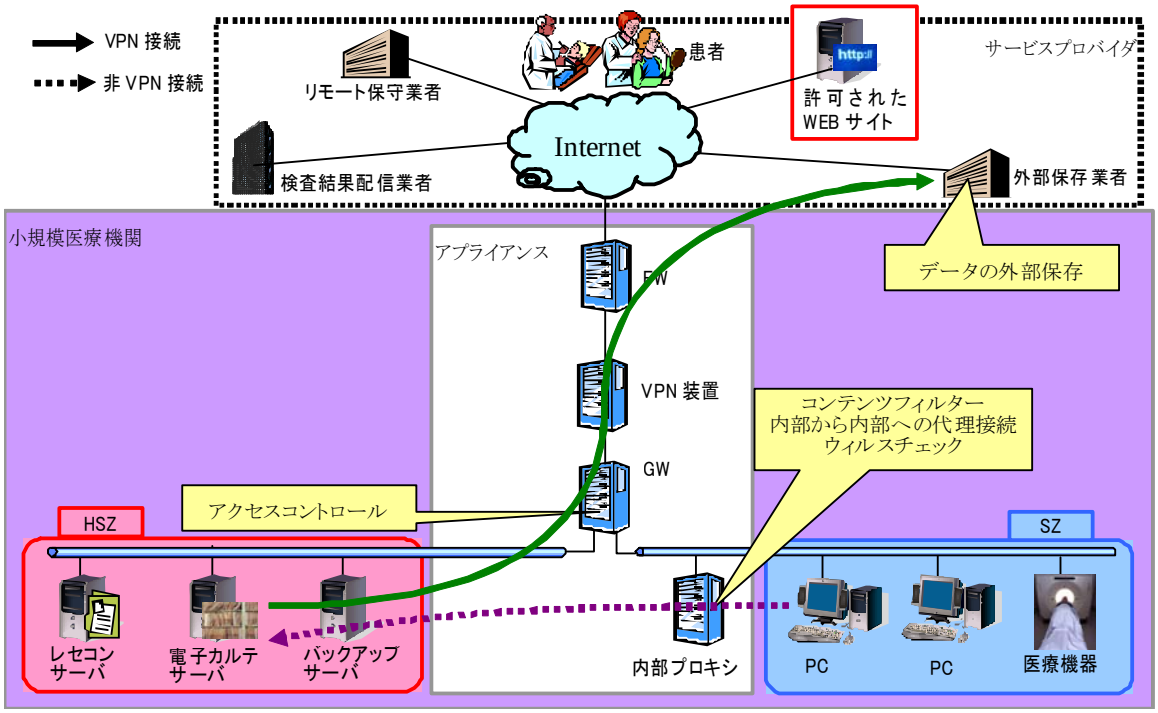


図２　小規模機関

All Rights Reserved Copyright ©2007 保健･医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム

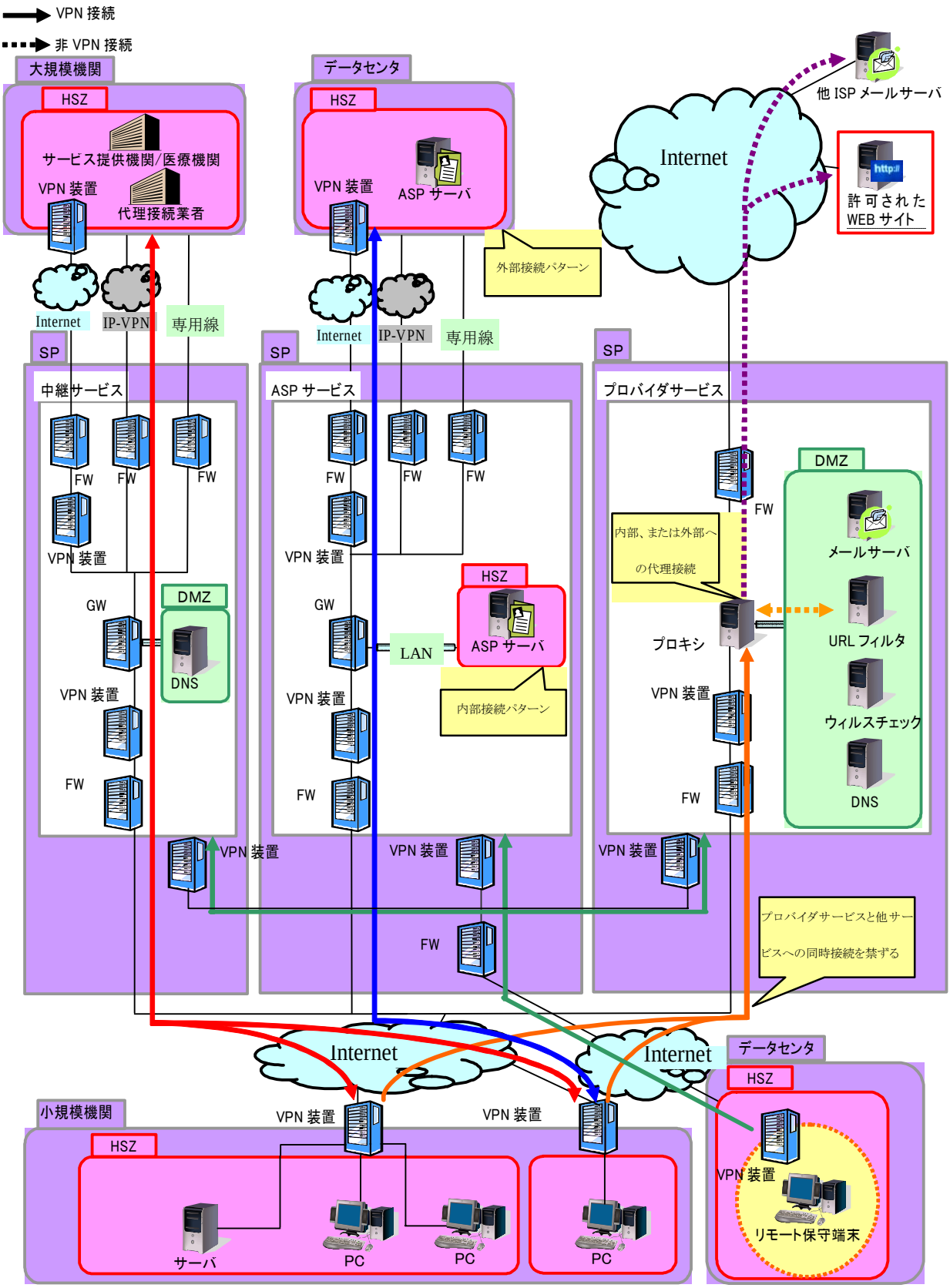


図３　サービス・プロバイダ（SP）

All Rights Reserved Copyright ©2007 保健･医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム

1. 大規模機関用チェックシートの使用方法について

このチェックシートは外部に情報提供できる設備を有する（SP サービスを外部へ提供できる）医療機関等について、チェックを実施するためのものです。外部に情報提供できる設備を有さない（SP サービスを外部へ提供できない）医療機関等については、小規模機関用チェックシートをご利用ください。

【チェックシートの構成について】

大規模機関用チェックシートはチェック実施者の種別に応じて、管理者シート、ベンダシート、SP シートの３枚よりなります。

実施者の種別	定義	大規模機関			備考
		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	各機関を運営する組織、またはその管理責任者を対象としている。	○（※）	－	－	（※）各機関の管理者がチェックが出来ない項目については、ベンダの設計責任者に確認すること。
ベンダ	各機関のネットワークおよびシステムを設計・構築するシステムインテグレータ等を対象としている。	－	○	－	
SP（サービス・プロバイダ）	提供するサービス機能を外部委託（アウトソーシング）する場合に、その委託先の SP の運営する組織、またはその管理責任者を対象としている。	－	－	○（※）	

【チェックシートのチェック項目について】

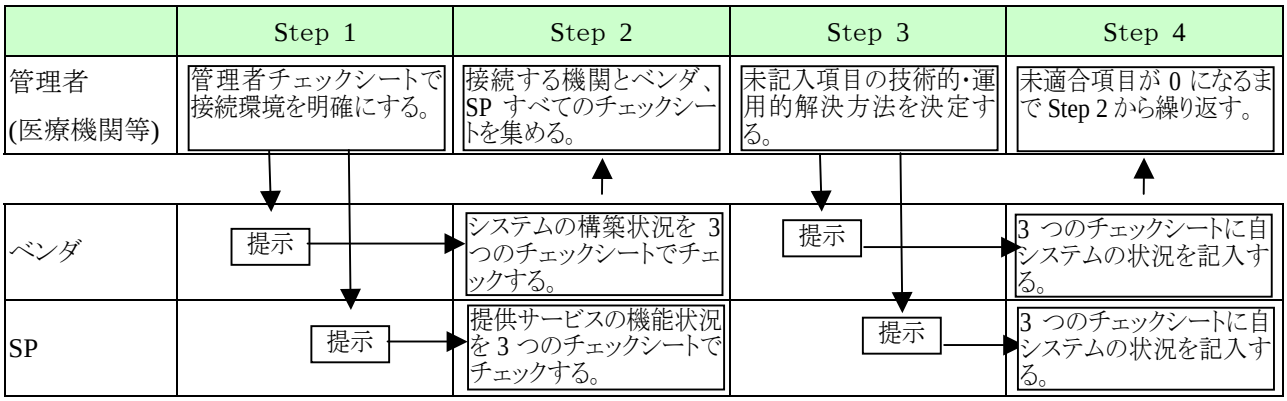
下表に、チェック実施対象者とチェックシートの各入力項目との関係を示します。○部分は全てチェックを実施し、また▲部分については、該当するサービス（提供サービスや利用サービス）に応じてチェックを実施します。

All Rights Reserved Copyright ©2007 保健･医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム

提供サービス項目	「医療情報システムの安全管理に関するガイドライン」 技術・運用基準チェックシート		
	大規模機関		
	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
1. 通信形態	○		
2. 通信ポリシー	○	○	○
3. 拠点内の技術的セキュリティ	○	○	○
4. サービス種別			
4-1 医療機関向けの情報提供ASPサービスの展開	▲	▲	
4-2 医療機関向けの情報提供ASPサービスの利用			
4-3 医療機関向けの情報提供ASPサービス（外部保存型）の利用	▲	▲	▲
4-4 医療機関以外への情報提供ASPサービスの展開	▲	▲	
4-5 医療機関以外への情報提供ASPサービスの利用			
4-6 医療機関以外への情報提供ASPサービス（外部保存型）の利用	▲	▲	▲
4-7 メールサービス（プロバイダサービス）	▲	▲	
4-8 インターネット接続サービス（プロバイダサービス）	▲	▲	
4-9 リモート保守サービスの利用	▲	▲	
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）	▲	▲	▲
5. 拠点内の物理的セキュリティ	○	○	

*1 サービス種別の▲ヶ所は、提供サービス（または利用サービス）に応じてチェックすること。
個別サービスを提供・利用する際は、該当する全ての個別項目をチェックすること。

チェックシートのチェック手順は下図に示すとおりです。下記手順でガイドラインへの適合性チェックを実施する必要があります。



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、未対応項目に対する対策や責任の分担を明確にしてから契約してください。責任の分担については、書面にて取交すことを徹底してください。

All Rights Reserved Copyright ©2007 保健･医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム

2. 小規模機関用チェックシートの使用方法について

このチェックシートは外部に情報提供できる設備を有しない医療機関等について、チェックを実施するためのものです。外部に情報提供できる設備を有する（SP サービスを外部へ提供できる）医療機関等については、大規模機関用チェックシートをご利用ください。

【チェックシートの構成について】

小規模機関用チェックシートはチェック実施者の種別に応じて、管理者シート、ベンダシートの２枚よりなります。

実施者の種別	定義	小規模機関		備考
		管理者チェックシート	ベンダチェックシート	
管理者	各機関を運営する組織、またはその管理責任者を対象としている。	○（※）	-	（※）各機関の管理者がチェックが出来ない項目については、ベンダの設計責任者に確認すること。
ベンダ	各機関のネットワークおよびシステムを設計・構築するシステムインテグレータ等を対象としている。	-	○	

【チェックシートのチェック項目について】

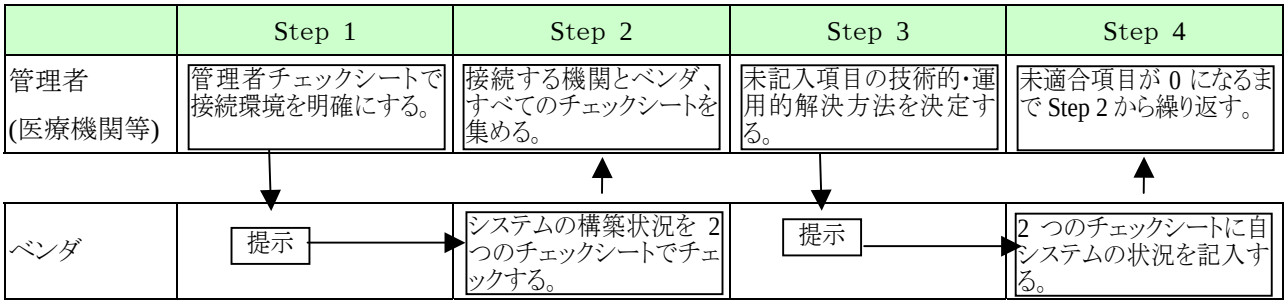
チェックシートは実施対象者ごとに管理者・ベンダシートからなります。下表は、チェック実施対象者とチェックシートの各入力項目との関係を示します。○部分は全てチェックを実施し、また▲部分については、該当するサービス（利用サービス）に応じてチェックを実施します。

All Rights Reserved Copyright ©2007 保健･医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム

提供サービス項目	「医療情報システムの安全管理に関するガイドライン」 技術・運用基準チェックシート	
	小規模機関	
	管理者チェックシート	ベンダチェックシート
1. 通信形態	○	
2. 通信ポリシー	○	○
3. 拠点内の技術的セキュリティ	○	○
4. サービス種別		
4-1 医療機関向けの情報提供ASPサービスの展開		
4-2 医療機関向けの情報提供ASPサービスの利用	▲	
4-3 医療機関向けの情報提供ASPサービス（外部保存型）の利用		
4-4 医療機関以外への情報提供ASPサービスの展開		
4-5 医療機関以外への情報提供ASPサービスの利用	▲	
4-6 医療機関以外への情報提供ASPサービス（外部保存型）の利用		
4-7 メールサービス（プロバイダサービス）	▲	
4-8 インターネット接続サービス（プロバイダサービス）	▲	▲
4-9 リモート保守サービスの利用		
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）	▲	
5. 拠点内の物理的セキュリティ		○

*1 サービス種別の▲ヶ所は、利用サービスに応じてチェックすること。
個別サービスを利用する際は、該当する全ての個別項目をチェックすること。

チェックシートは管理者・ベンダシートからなります。下図に示す手順でガイドラインへの適合性チェックを実施する必要があります。



医療機関等の管理者は、本チェックシートで確認した上で、未対応項目に対する対策や責任の分担を明確にしてから契約してください。責任の分担については、書面にて取交すことを徹底してください。

All Rights Reserved Copyright ©2007 保健･医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム

3. サービス・プロバイダ（SP）チェックシートの使用方法について

【チェックシートの構成について】

サービス・プロバイダ（SP）チェックシートはチェック実施者の種別に応じて、管理者シート、ベンダシート、SP シートの３枚からなります。

実施者の種別	定義	SP（サービス・プロバイダ）			備考
		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	各機関を運営する組織、またはその管理責任者を対象としている。	○（※）	－	－	（※）管理者がチェックが出来ない項目については、ベンダの設計責任者に確認すること。
ベンダ	各機関のネットワークおよびシステムを設計･構築するシステムインテグレータ等を対象としている。	－	○	－	
SP（サービス・プロバイダ）	提供するサービス機能を外部委託（アウトソーシング）する場合に、その委託先の SP の運営する組織、またはその管理責任者を対象としている。	－	－	○（※）	

サービス･プロバイダ(SP)は、上記管理者チェックシート、ベンダチェックシート、SP チェックシートの、全てのシートのチェックを実施する必要があります。

【チェックシートのチェック項目について】

チェックシートは管理者、ベンダ、SP の３つのシートからなりますが、各シートのチェック個目については、サービス・プロバイダ（SP）が医療機関等に提供するサービスの種類により異なります。

① VPN プロバイダ・サービスを提供
医療機関等に対し、VPN サービスを提供する VPN プロバイダは、チェックシート記載の VPN プロバイダ要件へのチェックをお願いします。

② ASP プロバイダ・サービスを提供
医療機関等に対し、VPN サービスだけではなく、ASP サービスをも提供するプロバイダは、チェックシート記載の ASP プロバイダ要件へのチェックもお願いします。

③ ASP プロバイダ・サービス（個別サービス）を提供
医療機関等に対し、メールや、インターネット接続、情報提供サービス等の個別 ASP サービスを提供するプロバイダは､チェックシート記載の個別 ASP プロバイダ要件へのチェックもお願いします。

下表には、サービス・プロバイダ（SP）チェックシートの各入力項目とサービス・プロバイダの提供サービスによるチェック該当部分との関係を示します。サービス・プロバイダ（SP）は提供サービスに応じて、チェックシートの該当入力項目のチェック（下表○部分のチェック）を実施します。

All Rights Reserved Copyright ©2007 保健･医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム

チェックシート 入力項目	VPN プロバイダ要件		ASP プロバイダ要件	ASPプロバイダ（個別サービス）要件									
	VPNサービス	IXサービス	ASPサービス	地域連携サービス	情報提供サービス	リモート保守サービス	メールサービス	インターネット接続サービス	外部保存サービス	検査データ配信サービス	タイムスタンプサービス	VAサービス	アウトソーシング
1. 通信形態	○	○	○	○	○	○	○	○	○	○	○	○	○
2. 通信ポリシー	○	○	○	○	○	○	○	○	○	○	○	○	○
3. 拠点内の技術的セキュリティ			○	○	○	○	○	○	○	○	○	○	○
4. サービス種別 *1													
4-1 医療機関向けの情報提供ASPサービスの展開				○	○		○		○	○	○	○	
4-2 医療機関向けの情報提供ASPサービスの利用													
4-3 医療機関向けの情報提供ASPサービス（外部保存型）の利用				○	○		○		○	○	○	○	○
4-4 医療機関以外への情報提供ASPサービスの展開				○	○		○		○		○	○	
4-5 医療機関以外への情報提供ASPサービスの利用													
4-6 医療機関以外への情報提供ASPサービス（外部保存型）の利用													○
4-7 メールサービス（プロバイダサービス）							○						
4-8 インターネット接続サービス（プロバイダサービス）								○					
4-9 リモート保守サービスの利用						○							
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）			○										
5. 拠点内の物理的セキュリティ	○	○	○	○	○	○	○	○	○	○	○	○	○

*1　提供するサービス項目が複数存在する場合は、該当する全ての個別項目をチェックすること。また、上記表の個別の ASP サービス要件にないサービスを提供する場合は、「4. サービス種別」の中で、提供サービスが該当する項目を全て選択し、チェックすること。

また、サービス提供をする医療機関等に対し、医療機関等の機能に応じて大規模機関チェックシート、または小規模機関チェックシートの管理者・ベンダ・SP シートのチェックを実施し、ガイドラインに基づいた安全性を担保する必要があります。そのため、サービスプロバイダ(SP)は、医療機関等用のチェックシートの判定基準が確保されるように、大規模機関チェックシートまたは小規模機関チェックシートのチェック内容について、その責任範囲を記載した契約書または覚書を医療機関等と取交し、保管する必要があります。

All Rights Reserved Copyright ©2007 保健･医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム

【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をしないエリア

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、外部とデータ交換をするエリア

中継サービス

ガイドラインの「第 6.10 章 外部と個人情報を含む医療情報を交換する場合の安全管理」における「B-3.I.③閉域 IP 通信網で接続されている場合」にて定義されている「通信事業者が保有する広域ネットワーク網と医療機関等に設置されている通信機器とを接続する通信回線が他のネットワークサービス等と共用されていない接続方式」を用いて大規模拠点と小規模拠点とのデータ交換をするエリア

プロバイダサービス

ガイドラインの「第 6.10 章外部と個人情報を含む医療情報を交換する場合の安全管理」において定義されている回線事業者やオンラインサービス提供事業者とデータ交換をするエリア

All Rights Reserved Copyright ©2007 保健･医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム