# ネットワークセキュリティチェックシート結果表

（サービスプロバイダ用）

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 | | |
| SP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 | - | 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。 | 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<br>6.10 B-3 | |
| | | - | 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。 | | □ | | |
| 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 | 2-2-2 SPは、SPを中継した不正な中継を禁止する必要がある。 | VPN機能 | 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の不正な中継が禁止されているかチェックする。 | | | | |
| | | | SPと小規模機関との間の許可していない不正な通信 | 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 | |
| | | | SPと大規模機関との間の許可していない不正な通信 | | | | |
| | | | 通信合意のない拠点間のSPを経由した不正な通信 | | | | |
| 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 | 3-3-1 SPのHigh Secure Zoneを起点とした大規模機関/小規模機関への接続 | プロキシ機能<br>／VPN機能<br>／ファイアウォール機能 | 大規模機関/小規模機関への接続において、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）対策をしている。 | 左記の対策を実施しない場合は、High Secure Zoneからの大規模機関への接続を行わない。 | □ | 6.5 B (1)<br>6.5 B (2)<br>6.5 B (3)<br>6.5 B (4)<br>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･遮断対策をしている。 | | | | |
| | | | ウィルス感染対策を行っている。 | | | | |
| | | | 接続における認証を行っている。 | | | | |
| | | | 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。 | | | | |
| | 3-3-2 SPのHigh Secure Zoneを起点としたインターネットへの接続 | プロキシ機能<br>／VPN機能<br>／ファイアウォール機能 | インターネットへの接続において、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からのインターネット接続を行わない。 | □ | 6.5 B (1)<br>6.5 B (2)<br>6.5 B (3)<br>6.5 B (4)<br>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。 | | | | |
| | | | 接続における認証を行っている。 | | | | |
| | | | 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。 | | | | |
| 3-5 DMZ のセキュリティ | 3-5-1 各ホストに対するウィルスチェック | 各ホスト | ウィルスチェックが正常に機能しているかチェックする。 | | | | |
| | | | ウィルス定義ファイルは常に最新のものを使用している。 | 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・拡散を防ぐために最新の定義ファイルによるチェックを行うこと。 | □ | 6.5 B (4) | |
| 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<br>／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)<br>6.5 B (5)<br>6.10 B-3 I | |
| 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<br><br>【提供サービス項目例】<br>（※資料2　P.4参照）<br>・情報提供サービス<br>・メールサービス<br>・地域連携サービス<br>・検査データ配信サービス<br>・外部保存サービス<br>・タイムスタンプサービス<br>・VAサービス | 4-1-1 医療機関向けの情報提供または公開 | ファイアウォール機能 | 不正利用防止のため次のセキュリティ対策が行われているかチェックする。 | | | | |
| | | | アクセス制限により不正利用を防止する。 | ファイアウォールなどによるセキュリティ対策を行い、接続先拠点と通信に関して合意がなされている接続先・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自拠点から他拠点への不正なアクセスと、その逆を防ぐ。 | □ | 6.10 B2 | |
| | 4-1-2 サービス提供ユーザの認証 | サーバ機能 | ASPサービスの提供においてユーザを識別するための認証しているかチェックする。 | | | | |
| | | | 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)<br>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。 | | □ | | |

| 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 |
|---|---|---|---|---|---|---|---|
| | 4-1-3 外部ASPからのサービス機能の提供を受ける場合にオープンネットワークを利用する場合のセキュリティ対策 | プロキシ機能<br>／VPN機能<br>／ファイアウォール機能 | 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。 | 医療機関向けに情報を公開・提供する場合、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機能を実装する。 | □ | 6.5 B (1)<br>6.5 B (4)<br>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<br>6.10 B 3<br>6.10 C 1 | |
| | 4-1-4 データまたは機器のHigh Secure Zoneへの配置・格納 | ゾーン | 医療機関向けに情報提供を行う場合、重要データや機器を改ざんや侵入から守るために次のセキュリティ対策を整備する。 | | | | |
| | | | 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<br>7.4 C | |
| 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<br><br>【提供サービス項目例】<br>（※資料2 P.4参照）<br>・アウトソーシング | 4-3-1 外部保存型ASPサービスを利用するホスト・機器の配置。 | ゾーン | 利用するホスト・機器がHigh Secure Zoneに配置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。 | 不正なアクセスによる改ざん・情報漏えいを防ぐため、外部保存サービスを提供する機器へのアクセスはHigh Secure Zoneに配置されたホスト端末のみ許可する。 | □ | 6.4 B③ | |
| 4-4 医療機関以外への重要情報提供ASPサービスの展開<br><br>【提供サービス項目例】<br>（※資料2 P.4参照）<br>・情報提供サービス<br>・メールサービス<br>・地域連携サービス<br>・外部保存サービス<br>・タイムスタンプサービス<br>・VAサービス | 4-4-1 情報の提供または公開 | ファイアウォール機能 | 不正利用防止のため次のセキュリティ対策が行われているかチェックする。 | | | | |
| | | | アクセス制限により不正利用を防止する。 | ファイアウォールなどによるセキュリティ対策を行い、接続先拠点と通信に関して合意がなされている接続先・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自拠点から他拠点への不正なアクセスと、その逆を防ぐ。 | □ | 6.10 B2 | |
| | 4-4-2 サービス提供ユーザの認証 | サーバ機能 | ASPサービスの提供においてユーザを識別するための認証しているかチェックする。 | | | | |
| | | | 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)<br>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。 | | □ | | |
| | 4-4-3 外部ASPからのサービス機能の提供を受ける場合にオープンネットワークを利用する場合のセキュリティ対策 | プロキシ機能<br>／VPN機能<br>／ファイアウォール機能 | 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。 | 重要な情報を公開・提供する場合、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機能を実装する。 | □ | 6.5 B (1)<br>6.5 B (4)<br>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<br>6.10 B 3<br>6.10 C 1 | |
| | 4-4-4 重要なデータまたは機器のHigh Secure Zoneへの配置・格納 | ゾーン | 医療機関向けに情報提供を行う場合、重要データや機器を改ざんや侵入から守るために次のセキュリティ対策を整備する。 | | | | |
| | | | 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<br>7.4 C | |
| 4-6 医療機関以外での重要情報提供ASPサービス（外部保存型）の利用<br><br>【提供サービス項目例】<br>（※資料2 P.4参照）<br>・アウトソーシング | 4-6-1 外部保存型ASPサービスを利用するホスト・機器の配置。 | ゾーン | 利用するホスト・機器がHigh Secure Zoneに配置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。 | 不正なアクセスによる改ざん・情報漏えいを防ぐため、外部保存サービスを提供する機器へのアクセスはHigh Secure Zoneに配置されたホスト端末のみ許可する。 | □ | 6.4 B③ | |
| 4-7 メールサービス（プロバイダサービス）<br><br>【提供サービス項目例】<br>（※資料2 P.4参照）<br>・メールサービス | 4-7-1 メールのスクリーニングの実施 | ゲートウェイ機能 | スパムメール・ウィルス添付メール等から内部が守られているかチェックする。 | | | | |
| | | | メールの送受信を行う相手が制限されている。 | 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対策を行わなければならない。対策を実施しない場合は、サービスの利用を禁止する。 | □ | 6.5 B (4)<br>6.5 B (5) | |
| | | | スパムメールを防止している。 | | | | |
| | | | 送受信時にウィルスチェックが行われ、不審なメールは削除もしくは隔離されている。 | | | | |
| | 4-7-2 不正なメール転送の禁止 | メール機能 | メール転送が適切に行われているかチェックする。 | | | | |
| | | | 適切なメール転送処理を行っている。 | 不正メール転送の踏み台になることを防止しなければならない。 | □ | 6.5 B (4)<br>6.5 B (5) | |
| | 4-7-3 メールサービスを提供するユーザの認証 | ゲートウェイ機能／サーバ機能 | メールサービスの提供において認証にどのような方法を用いているかチェックする。 | | | | |
| | | | 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)<br>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。 | | □ | | |

| 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 |
|---|---|---|---|---|---|---|---|
| 4-8 インターネット接続サービス（プロバイダサービス）<br><br>【提供サービス項目例】<br>（※資料2　P.4参照）<br>・インターネット接続サービス | 4-8-1 サイト閲覧の制限 | ゲートウェイ機能 | 業務・サービスで必要なサイトのみ閲覧を許可しているかチェックする。 | | | | |
| | | | URLホワイトリスト機能によるスクリーニングが行われている。 | 左記の機能により、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・情報漏えいなどを防止しなければならない。 | □ | 6.5 B (4)<br>6.5 B (5) | |
| | | | スクリーニングにより不適切なサイトが閲覧できないようになっている。 | | | | |
| | | | コンテンツフィルタにより、必要のない実行プログラムが動作しないようになっている。 | | | | |
| | 4-8-2 インターネット接続サービスを利用するユーザの認証 | ゲートウェイ機能／サーバ機能 | インターネット接続サービスの提供においてユーザを認証する機能にどの技術を用いているかチェックする。 | | | | |
| | | | 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認証することで、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） | □ | 6.10 B-1<br>6.10 C-7<br>8.1.1 C③ | |
| | | | ICカード/スマートカードでの認証を行っている。 | | □ | | |
| | | | バイオメトリックによる認証を行っている。 | | □ | | |
| 4-9 リモート保守サービスの利用<br><br>【提供サービス項目例】<br>（※資料2　P.4参照）<br>・リモート保守サービス | 4-9-1 リモート保守端末の配置 | ゾーン | 利用するホスト・機器がHigh Secure Zoneに配置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。 | リモート保守作業およびリモート監視において、システムの機器または情報を守るため、High Secure Zoneへ配置しなければならない。 | □ | 8.1 | |
| | 4-9-2 リモート保守作業者の認証 | ゲートウェイ機能／サーバ機能 | リモート保守作業者の利用者認証にどのような方法を用いているかチェックする。 | | | | |
| | | | 導入される認証技術 | | | | |
| | | | 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） | □ | 6.10 B-1<br>6.10 C-7<br>8.1.1 C③ | |
| | | | ICカード/スマートカードでの認証を行っている。 | | □ | | |
| | | | バイオメトリックによる認証を行っている。 | | □ | | |
| | 4-9-3 リモート保守作業者による不正作業・操作を防ぐための対策 | - | リモート保守において導入されている規定をチェックする。 | | | | |
| | | | 規定すべき要件 | | | | |
| | | | リモート保守作業者の管理規定を設けている。 | 個人情報の保護やシステムの安全な運用を行うために、左記の運用規定等を設けている。 | □ | 8.1.1 C③ | |
| | | | リモート端末、ネットワークに関する管理規定を設けている。 | | | | |
| | | | リモート端末を許可された要員以外による不正操作を防ぐ対策規定を設けている。 | | | | |
| | | | リモート保守作業を行う際の記録、授受データの処理に関する規定を設けている。 | | | | |
| | | | リモート端末が増設・移動される場合の規定を設けている。 | | | | |
| 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）<br><br>【提供サービス項目例】<br>（※資料2　P.4参照）<br>・VPNサービス<br>・IXサービス<br>・ASPサービス | 4-10-1 外部のサービス提供機関に接続する機器またはデータの配置 | ゾーン | 外部のサービス提供機関に接続する機器がHigh Secure Zoneに配置されているかチェックする。 | | | | |
| | | | 外部のサービス提供機関に接続する機器が設置されたゾーン | | | | |
| | | | High Secure Zoneに配置している。 | システムの機器または情報を守るため、High Secure Zoneへ配置する。 | □ | 6.5 B (5) | |
| | 4-10-2 外部サービス提供機関のサービス提供を受けるユーザの認証 | ゲートウェイ機能／サーバ機能 | 外部サービス提供機関のサービスの利用者認証にどのような方法を用いているかチェックする。 | | | | |
| | | | 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） | □ | 6.10 B-1<br>6.10 C-7<br>8.1.1 C③ | |
| | | | ICカード/スマートカードでの認証を行っている。 | | □ | | |
| | | | バイオメトリックによる認証を行っている。 | | □ | | |
| | 4-10-3 外部サービス提供機関との接続におけるセキュリティ対策 | - | 実施されているセキュリティ対策をチェックする。 | | | | |
| | | | ウィルス、DoS攻撃等に対する防御対策を行う。 | 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、守るべきセキュリティ要件を整え、接続を行う。 | □ | 6.5 B (1)<br>6.5 B (4)<br>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。 | | | | |
| | | | 利用者認証を行う。 | | | | |
| | | | アクセス監視をしている。 | | | | |
| | 4-10-5 外部サービス提供機関との接続に関する文書等による合意と接続認可 | - | 外部サービス提供機関との接続に際してチェックする。 | | | | |
| | | | 文書によるサービス内容・運用形態の確認を行う。 | 外部サービス提供機関との接続を行うにあたっては、文書等による合意と接続認可を受ける。 | □ | 6.5 B (5) | |
| | | | サービス提供機関との合意と接続認可を行う。 | | | | |

## 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)<br>6.5 B (2)<br>6.5 B (3)<br><br>6.10 B-1<br>6.10 B-2<br>6.10 B-3<br><br>6.10 B-3Ⅱ<br>6.10 C-1<br>6.10 C-2<br><br>8.1.3 D (1)① | |
| | | | モード | メインモード<br>アグレッシブモード | プロバイダ：どちらでも可<br>IX：メインモードに限定 | □ | |
| | | | 認証方式 | RSAデジタル証明書認証方式<br>共通鍵認証方式 | プロバイダ：どちらでも可<br>IX：RSAデジタル証明書認証方式 | □ | |
| | | | 暗号化アルゴリズム | 3DES-CBC<br>AES128-CBC<br>AES256-CBC | 設定条件：左記のいずれか<br>IX：AES128-CBCに限定 | ■ | |
| | | | 認証アルゴリズム | HMAC-MD5<br>HMAC-SHA1<br>またはSHA256以上 | プロバイダ：HMAC-SHA1以上<br>IX：HMAC-SHA1 | □ | |
| | | | DHグループ | Group2<br>（離散対数1024ビット）<br>Group14<br>（離散対数2048ビット） | プロバイダ：どちらでも可<br>IX：Group2 | □ | |
| | | | Life Type | time（時間）<br>byte（バイト） | プロバイダ：どちらも可<br>IX：timeに設定 | □ | |
| | | | Life Duration | time（時間）<br>byte（バイト） | 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。 | □ | |
| | | | 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<br>FQDN<br>USER-FQDN<br>IPv4 | プロバイダ：いずれも可<br>IX：DN | ■ | |
| | | | IPSecパラメータ | | | | |
| | | | モード | トンネルモード<br>トランスポート | プロバイダ：どちらも可<br>IX：トンネルモード | □ | |
| | | | セキュリティプロトコル | ESP<br>AH | プロバイダ：どちらでも可<br>IX：ESPに限定 | □ | |
| | | | 暗号化アルゴリズム | 3DES-CBC<br>AES128-CBC<br>AES256-CBC | プロバイダ：左記のいずれも可<br>IX：AES128-CBCに限定 | ■ | |
| | | | 認証アルゴリズム | HMAC-MD5<br>HMAC-SHA1<br>またはSHA256以上 | プロバイダ：HMAC-SHA1以上<br>IX：HMAC-SHA1に限定 | □ | |
| | | | DHグループ | Group2<br>（離散対数1024ビット）<br>Group14<br>（離散対数2048ビット） | プロバイダ：どちらでも可<br>IX：Group2 | □ | |
| | | | Life Type | time（時間）<br>byte（バイト） | プロバイダ：どちらも可<br>IX：timeに設定 | □ | |
| | | | Life Duration | time（時間）<br>byte（バイト） | 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。 | □ | |
| | | | 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<br>／プロキシ機能<br>／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<br>／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)<br>6.5 C 4<br>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 | | | | |
| | 2-3-3 SPの提供サービス毎の脅威拡散防止のための通信経路の分離 | - | サービス毎に通信経路を分離しているかチェックする。 | | | | |
| | | | 分離項目 | | | | |
| | | | プロバイダサービスと中継サービスの分離がされている。 | SPの提供サービス毎の脅威拡散防止のための通信経路の分離されていること | □ | 6.10 B-3 | |
| | | | プロバイダサービスとASPサービスの通信経路の分離がされている。 | | | | |
| | | | ASPサービスと中継サービスの通信経路の分離がされている。 | | | | |
| 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<br>7.3 C (2) 1<br>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<br>／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<br>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<br>／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 | |
| 3-5 DMZ のセキュリティ | 3-5-1 High Secure Zone, Secure Zone への直接アクセスの禁止 | ゲートウェイ機能<br>／プロキシ機能 | 接続の起点をDMZとしたHigh Secure Zone、Secure Zoneへの代理接続についてチェックする。 | | | | |
| | | | 接続の起点をDMZとしたHigh Secure Zone、Secure Zone 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。 | DMZ の公開サーバが外部からの不正アクセスにより侵入等が行われた場合、High Secure Zone, Secure Zone への被害拡散を防止する。 | □ | 6.5 B (5) | |
| | 3-5-2 各ホストでのウィルスチェックの実施 | 各ホスト | 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。 | ウィルスチェックには最新のウィルス定義ファイルを使用している。 | □ | 6.5 B (4) | |
| 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<br>／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<br>／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)<br>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 | | | |
| | | | 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)<br>6.5 C 4<br>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<br>／VPN機能<br>／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)<br>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。 | | | | |
| 3-8 High Secure Zone とDMZ間の通信 | 3-8-1 DMZ 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<br>／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。 | | | | |
| | 3-8-2 ロギングを行いアクセスを監視する。<br>「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)<br>6.5 C 4<br>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。 | | | | |
| | 3-8-3 High Secure Zone からの接続制限 | プロキシ機能<br>／VPN機能<br>／ファイアウォール機能 | IPアドレス・ポート・コンテンツの利用を制限する機能が正常に機能し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、情報漏えい・改ざんなどへの防止対策が行われていること。 | □ | 6.5 B (5)<br>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 | | | | | | | |
| 4-1 医療機関向けの情報提供ASPサービスの展開<br><br>【提供サービス項目例】<br>（※資料2　P.4参照）<br>・情報提供サービス<br>・メールサービス<br>・地域連携サービス<br>・検査データ配信サービス<br>・外部保存サービス<br>・タイムスタンプサービス<br>・VAサービス | 4-1-1 医療情報等の提供またはデータの格納を行っている機器へのアクセスにおけるプロキシ機能による外部ユーザからの遮蔽 | プロキシ機能<br>／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 | □ | 8.1 | |
| | | | 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 | | | |
| | | | 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 | | | |
| | 4-1-2　医療情報等の提供またはデータの格納を行っているサーバ等の機器へのウィルスチェック | サーバ機能 | ウィルスチェックが正常に機能しているかチェックする。 | | | | |
| | | | 最新のウィルス定義ファイルを使用している | 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・拡散を防ぐために最新の定義ファイルによるチェックを行うこと。 | □ | 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 |
|---|---|---|---|---|---|---|---|
| | 4-1-3　ユーザへの医療情報等の提供にあたってのインターネットからの攻撃（DoS攻撃・不正形式パケットなど）に対する検知機能 | ファイアウォール／侵入検知・防御 | 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。 | | | |
| | 4-1-4 医療機関向けに情報を公開・提供する場合のロギングによるアクセス監視。「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)<br>6.5 C 4<br>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 | | | | |
| | 4-1-5 プロバイダサービス・中継サービス・リモート保守サービスとの通信経路の分離 | - | サービス毎に通信経路が分離されている。 | | | | |
| | | | 分離項目 | | | | |
| | | | プロバイダサービスとの分離がされている。 | SPの提供サービス毎の脅威拡散防止のための通信経路の分離を行っていること | □ | 6.10 B-3 | |
| | | | 中継サービスとの分離がされている。 | | | | |
| | | | リモート保守サービスとの分離がされている。 | | | | |
| | 4-1-6　情報提供サービスを利用するユーザの認証機能 | ゲートウェイ機能／サーバ機能 | 情報提供サービスを利用するユーザの認証でどの技術を用いているかチェックする。 | | | | |
| | | | 認証技術 | | | | |
| | | | ID/パスワードによるアカウント認証 | サービスを提供しているユーザを認証することで、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。（いずれか一つをチェック出来ること） | □ | 6.5 B (1) | |
| | | | 認証サーバによる認証（RADIUS/LDAP） | | □ | | |
| | | | 認証サーバ＋ワンタイムパスワードによる認証 | | □ | | |
| | | | ICカード/スマートカードによる認証 | | □ | | |
| | | | バイオメトリックによる認証 | | □ | | |
| 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<br><br>【提供サービス項目例】<br>（※資料2　P.4参照）<br>・アウトソーシング | 4-3-1 外部のASPサイトが起点の接続の禁止 | ゲートウェイ機能<br>プロキシ機能 | 起点となる接続が禁止されているかチェックする。 | | | | |
| | | | 外部ASPからの接続を禁止している | SPからのアップロードのみの接続を行うため、外部ASPからの接続は禁止し不正アクセスを防ぐ。 | □ | 6.5 C (3) | |
| | 4-3-2 外部のASPサイトへの接続 | ゾーン | 外部ASPに接続される機器がHigh Secure Zoneから接続されているかチェックする。 | | | | |
| | | | 外部ASPに接続される機器はHigh Secure Zoneに設置されている。 | High Secure Zone からの外部ASPへの不正なアクセスを防ぐ。 | □ | 6.5 C (3) | |
| | 4-3-3 プロバイダサービス・中継サービスとの通信経路の分離。 | - | サービス毎に通信経路が分離されている。 | | | | |
| | | | 分離項目 | | | | |
| | | | プロバイダサービスとの分離がされている。 | SPの提供サービス毎の脅威拡散防止のための通信経路の分離されていること | □ | 6.10 B-3 | |
| | | | 中継サービスとの分離がされている。 | | | | |
| | | | リモート保守サービスとの分離がされている。 | | | | |
| | 4-3-4　サービスの利用においてロギングに際するアクセスの監視。「2.2 (3) SPC要件より」 | サーバ機能 | 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)<br>6.5 C 4<br>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 | | | | |
| | 4-3-5　外部保存サービスを利用するユーザの認証機能 | ゲートウェイ機能／サーバ機能 | 外部保存サービスを利用するユーザの認証でどの技術を用いているかチェックする。 | | | | |
| | | | 認証技術 | | | | |
| | | | ID/パスワードによるアカウント認証 | サービスを提供しているユーザを認証することで、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。（いずれか一つをチェック出来ること） | □ | 6.5 B (1) | |
| | | | 認証サーバによる認証（RADIUS/LDAP） | | □ | | |
| | | | 認証サーバ＋ワンタイムパスワードによる認証 | | □ | | |
| | | | ICカード/スマートカードによる認証 | | □ | | |
| | | | バイオメトリックによる認証 | | □ | | |
| | 4-3-6　外部保存型ASPサイトとの接続におけるオープンネットワークの利用 | VPN機能 | オープンネットワークの利用した外部保存型ASPサイトとの接続についてチェックする。 | | | | |
| | | | 「2-2 オープンネットワークを利用した拠点間の接続」のチェック項目がすべて条件をクリアしている。 | オープンネットワークを利用する際は、「2-2 オープンネットワークを利用した拠点間の接続」のチェック項目を満たした通信技術を用いている。 | □ | 8.1.3 C (1)② | |

| 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 |
|---|---|---|---|---|---|---|---|
| | 4-3-7　オープンネットワークからの脅威（DoS攻撃・不正形式パケットなど）に対する検知機能 | ファイアウォール／侵入検知・防御 | 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。 | | | |
| | 4-3-8　外部保存サービス提供のサイトに接続される機器においてウィルスチェックを行う | サーバ機能 | ウィルスチェックが正常に機能しているかチェックする。 | | | | |
| | | | 最新のウィルス定義ファイルを使用している | 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・拡散を防ぐために最新の定義ファイルによるチェックを行うこと。 | □ | 6.5 B (4) | |
| 4-4 医療機関以外への情報提供ASPサービスの展開<br><br>【提供サービス項目例】<br>（※資料2　P.4参照）<br>・情報提供サービス<br>・メールサービス<br>・地域連携サービス<br>・外部保存サービス<br>・タイムスタンプサービス<br>・VAサービス | 4-4-1 医療機関以外への重要情報の提供またはデータの格納を行っている機器へのアクセスにおけるプロキシ機能による外部ユーザからの遮蔽 | 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 | □ | 8.1 | |
| | | | 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 | | | |
| | | | 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 | | | |
| | 4-4-2　医療機関以外への重要情報の提供またはデータの格納を行っているサーバ等の機器へのウィルスチェック | サーバ機能 | ウィルスチェックが正常に機能しているかチェックする。 | | | | |
| | | | 最新のウィルス定義ファイルを使用している | 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・拡散を防ぐために最新の定義ファイルによるチェックを行うこと。 | □ | 6.5 B (4) | |
| | 4-4-3　医療機関以外のユーザへの重要情報の提供にあたってのインターネットからの攻撃（DoS攻撃・不正形式パケットなど）に対する検知機能 | ファイアウォール／侵入検知・防御 | 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。 | | | |
| | 4-4-4 医療機関以外への重要情報を公開・提供する場合のロギングによるアクセス監視。「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)<br>6.5 C 4<br>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 | | | | |
| | 4-4-5 プロバイダサービス・中継サービス・リモート保守サービスとの通信経路の分離 | - | サービス毎に通信経路が分離されている。 | | | | |
| | | | 分離項目 | | | | |
| | | | プロバイダサービスとの分離がされている。 | SPの提供サービス毎の脅威拡散防止のための通信経路の分離を行っていること | □ | 6.10 B-3 | |
| | | | 中継サービスとの分離がされている。 | | | | |
| | | | リモート保守サービスとの分離がされている。 | | | | |

| 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 |
|---|---|---|---|---|---|---|---|
| | 4-4-6 情報提供サービスを利用するユーザの認証機能 | ゲートウェイ機能／サーバ機能 | 情報提供サービスを利用するユーザの認証でどの技術を用いているかチェックする。 | | | | |
| | | | 認証技術 | | | | |
| | | | ID/パスワードによるアカウント認証 | サービスを提供しているユーザを認証することで、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。（いずれか一つをチェック出来ること） | □ | 6.5 B (1) | |
| | | | 認証サーバによる認証（RADIUS/LDAP） | | □ | | |
| | | | 認証サーバ＋ワンタイムパスワードによる認証 | | □ | | |
| | | | ICカード/スマートカードによる認証 | | □ | | |
| | | | バイオメトリックによる認証 | | □ | | |
| 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<br><br>【提供サービス項目例】<br>（※資料2 P.4参照）<br>・アウトソーシング | 4-6-1 外部のASPサイトが起点の接続の禁止 | ゲートウェイ機能プロキシ機能 | 起点となる接続が禁止されているかチェックする。 | | | | |
| | | | 外部ASPからの接続を禁止している | SPからのアップロードのみの接続を行うため、外部ASPからの接続は禁止し不正アクセスを防ぐ。 | □ | 6.5 C (3) | |
| | 4-6-2 外部のASPサイトへの接続 | ゾーン | 外部ASPに接続される機器がHigh Secure Zoneから接続されているかチェックする。 | | | | |
| | | | 外部ASPに接続される機器はHigh Secure Zoneに設置されている。 | High Secure Zone からの外部ASPへの不正なアクセスを防ぐ。 | □ | 6.5 C (3) | |
| | 4-6-3 プロバイダサービス・中継サービスとの通信経路の分離。 | - | サービス毎に通信経路が分離されている。 | | | | |
| | | | 分離項目 | | | | |
| | | | プロバイダサービスとの分離がされている。 | SPの提供サービス毎の脅威拡散防止のための通信経路の分離されていること | □ | 6.10 B-3 | |
| | | | 中継サービスとの分離がされている。 | | | | |
| | | | リモート保守サービスとの分離がされている。 | | | | |
| | 4-6-4 サービスの利用においてロギングに際するアクセスの監視。「2.2（3）SPC要件より」 | サーバ機能 | 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)<br>6.5 C 4<br>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 | | | | |
| | 4-6-5 外部保存サービスを利用するユーザの認証機能 | ゲートウェイ機能／サーバ機能 | 外部保存サービスを利用するユーザの認証でどの技術を用いているかチェックする。 | | | | |
| | | | 認証技術 | | | | |
| | | | ID/パスワードによるアカウント認証 | サービスを提供しているユーザを認証することで、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。（いずれか一つをチェック出来ること） | □ | 6.5 B (1) | |
| | | | 認証サーバによる認証（RADIUS/LDAP） | | □ | | |
| | | | 認証サーバ＋ワンタイムパスワードによる認証 | | □ | | |
| | | | ICカード/スマートカードによる認証 | | □ | | |
| | | | バイオメトリックによる認証 | | □ | | |
| | 4-6-6 外部保存型ASPサイトとの接続におけるオープンネットワークの利用 | VPN機能 | オープンネットワークの利用した外部保存型ASPサイトとの接続についてチェックする。 | | | | |
| | | | 「2-2 オープンネットワークを利用した拠点間の接続」のチェック項目がすべて条件をクリアしている。 | オープンネットワークを利用する際は、「2-2 オープンネットワークを利用した拠点間の接続」のチェック項目を満たした通信技術を用いている。 | □ | 8.1.3 C (1)② | |
| | 4-6-7 オープンネットワークからの脅威（DoS攻撃・不正形式パケットなど）に対する検知機能 | ファイアウォール／侵入検知・防御 | 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。 | | | |
| | 4-6-8 外部保存サービス提供のサイトに接続される機器においてウィルスチェックを行う | サーバ機能 | ウィルスチェックが正常に機能しているかチェックする。 | | | | |
| | | | 最新のウィルス定義ファイルを使用している | 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・拡散を防ぐために最新の定義ファイルによるチェックを行うこと。 | □ | 6.5 B (4) | |
| 4-7 メールサービス<br><br>【提供サービス項目例】<br>（※資料2 P.4参照）<br>・メールサービス | 4-7-1 サービスの提供または利用においてロギングに際するアクセスの監視。「2.2（3）SPC要件より」 | サーバ機能 | 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)<br>6.5 C 4<br>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 | | | | |

| 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 |
|---|---|---|---|---|---|---|---|
| | 4-7-2 中継サービス・ASPサービス・リモート保守サービスとの通信経路の分離 | | 他サービスの通信経路との分離されているかチェックする。 | | | | |
| | | | 分離項目 | | | | |
| | | | 中継サービスとの分離がされている。 | SPの提供サービス毎の脅威拡散防止のための通信経路の分離されていること。 | □ | 6.10 B-3 | |
| | | | ASPサービスとの分離がされている。 | | | | |
| | | | リモート保守サービスとの分離がされている。 | | | | |
| | 4-7-3 メールサービス利用制限の利用者とSP間での合意 | - | メールサービスにおける下記の制限事項について合意・遵守されているかチェックする。 | | | | |
| | | | サービスプロバイダが提供するメールサービス以外のPOP3、SMTPのメールサービスを利用を禁止する。 | High Secure Zoneにあるホストによるメール利用では、左記の条件についてユーザとSP間で合意を行い、ユーザに対する説明と指導を行うこと。 | □ | 6.5 B (2) | |
| | | | 利用者の希望によりWebメールを利用する場合は、インターネット接続サービスによる利用のみに制限されている。 | | | | |
| | 4-7-4 メールサービスの提供または利用する機器へのウィルスチェック | サーバ機能 | ウィルスチェックが正常に機能しているかチェックする。 | | | | |
| | | | 最新のウィルス定義ファイルを使用している。 | 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・拡散を防ぐために最新の定義ファイルによるチェックを行うこと。 | □ | 6.5 B (4) | |
| | 4-7-5 他ISPのメールサーバを利用する際におけるセキュリティ対策 | - | 実施されているセキュリティ対策をチェックする。 | | | | |
| | | | 対策項目 | | | | |
| | | | DoS攻撃等に対する防御対策が行われている。 | 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対策を行わなければならない。対策を実施しない場合は他ISPのメールサーバの利用を禁止する。 | □ | 6.10 B-3Ⅱ | |
| | | | 改ざんや侵入に対する不正パケットの検知・遮断対策が行われている。 | | | | |
| | | | ウィルス、スパムメール等に対する防御対策が行われている。 | | | | |
| | | | 利用者の認証が行われている。 | | | | |
| | | | アクセス監視が行われている。 | | | | |
| | 4-7-6 メールサービスを利用するユーザの認証機能 | ゲートウェイ機能／サーバ機能 | メールサービスを利用するユーザの認証でどの技術を用いているかチェックする。 | | | | |
| | | | 認証技術 | | | | |
| | | | ID/パスワードによるアカウント認証 | サービスを提供しているユーザを認証することで、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。（いずれか一つをチェック出来ること） | □ | 6.5 B (1) | |
| | | | 認証サーバによる認証（RADIUS/LDAP） | | □ | | |
| | | | 認証サーバ＋ワンタイムパスワードによる認証 | | □ | | |
| | | | ICカード/スマートカードによる認証 | | □ | | |
| | | | バイオメトリックによる認証 | | □ | | |
| 4-8 インターネット接続サービス<br><br>【提供サービス項目例】<br>（※資料2 P.4参照）<br>・インターネット接続サービス | 4-8-1 ロギングを行いアクセスを監視する。「2.2（3）SPC要件より」 | ゲートウェイ機能／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)<br>6.5 C 4<br>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 | | | | |
| | 4-8-2 インターネットからの攻撃（DoS攻撃・不正形式パケットなど）に対する検知・防御機能 | ファイアウォール／侵入検知・防御 | 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。 | | | |
| | 4-8-3 インターネットからの攻撃（DoS攻撃・不正形式パケットなど）に対するアクセスコントロール機能 | ゲートウェイ機能 | アクセスコントロール機能を実装しているかチェックする。 | | | | |
| | | | アクセスコントロール機能が実装されている。 | インターネット上からのあらゆるリスクの発生により、システム全体に重大な損害を与えることが見込まれる場合はサービスにおける通信の遮断するなどの制御を行うこと。 | □ | 6.5.D.5 | |
| | 4-8-4 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。 | | | | |
| | | | プロキシ機能 | | | | |
| | | | 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)<br>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 | | | |
| | | | 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 | | | |
| | 4-8-5 中継サービス・ASPサービス・リモート保守サービスとの通信経路の分離 | | 他サービスの通信経路との分離されているかチェックする。 | | | | |
| | | | 分離項目 | | | | |
| | | | 中継サービスとの分離がされている。 | SPの提供サービス毎の脅威拡散防止のための通信経路の分離されていること | □ | 6.5 B (5) | |
| | | | ASPサービスとの分離がされている。 | | | | |
| | | | リモート保守サービスとの分離がされている。 | | | | |

| 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 |
|---|---|---|---|---|---|---|---|
| | 4-8-6 インターネット接続を提供する機器におけるウィルス感染対策 | サーバ機能 | ウィルスチェックが正常に機能しているかチェックする。 | | | | |
| | | | 最新のウィルス定義ファイルを使用している | 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・拡散を防ぐために最新の定義ファイルによるチェックを行うこと。 | □ | 6.5 B (4) | |
| | 4-8-7 インターネット上のサイト閲覧に際しての名前解決 | サーバ機能 | サイト閲覧に関して名前解決の方法をチェックする。 | | | | |
| | | | 外部プロキシによる名前解決を行っている | 利用者によるインターネット上の不正サイトへの接続による情報漏えいなどを防ぐ。 | □ | 6.5 B (4) | |
| | 4-8-8 インターネット接続サービスを利用するユーザの認証機能 | ゲートウェイ機能／サーバ機能 | インターネット接続サービスを利用するユーザの認証でどの技術を用いているかチェックする。 | | | | |
| | | | 認証技術 | | | | |
| | | | ID/パスワードによるアカウント認証 | サービスを提供しているユーザを認証することで、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。（いずれか一つをチェック出来ること） | □ | 6.5 B (5) | |
| | | | 認証サーバによる認証（RADIUS/LDAP） | | □ | | |
| | | | 認証サーバ＋ワンタイムパスワードによる認証 | | □ | | |
| | | | ICカード/スマートカードによる認証 | | □ | | |
| | | | バイオメトリックによる認証 | | □ | | |
| | 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) | |
| 4-9 リモート保守サービスの利用<br><br>【提供サービス項目例】<br>（※資料2 P.4参照）<br>・リモート保守サービス | 4-9-1 ロギングを行いアクセスを監視する。「2.2（3）SPC要件より」 | ゲートウェイ機能／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)<br>6.5 C 4<br>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 | | | | |
| | 4-9-2 リモート保守作業者の認証 | ゲートウェイ機能／サーバ機能 | 外部保存サービスを利用するユーザの認証でどの技術を用いているかチェックする。 | | | | |
| | | | 認証技術 | | | | |
| | | | ID/パスワードによるアカウント認証 | サービスを提供しているユーザを認証することで、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。（いずれか一つをチェック出来ること） | □ | 6.5 B (5) | |
| | | | 認証サーバによる認証（RADIUS/LDAP） | | □ | | |
| | | | 認証サーバ＋ワンタイムパスワードによる認証 | | □ | | |
| | | | ICカード/スマートカードによる認証 | | □ | | |
| | | | バイオメトリックによる認証 | | □ | | |
| 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）<br><br>【提供サービス項目例】<br>（※資料2 P.4参照）<br>・VPNサービス<br>・IXサービス<br>・ASPサービス | 4-10-1 ロギングを行いアクセスを監視する。「2.2（3）SPC要件より」 | ゲートウェイ機能／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、ユーザと合意しておくこと。 | □ | 6.5 B (1) | |
| | | | 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 | | | | |
| | 4-10-2 プロバイダサービス、ASPサービス・リモート保守サービスとの通信経路の分離 | - | 他サービスの通信経路との分離されているかチェックする。 | | | | |
| | | | 分離項目 | | | | |
| | | | プロバイダサービスとの分離がされている。 | SPの提供サービス毎の脅威拡散防止のための通信経路の分離されていること | □ | 6.10 B-3 | |
| | | | ASPサービスとの分離がされている。 | | | | |
| | | | リモート保守サービスとの分離がされている。 | | | | |
| | 4-10-3 サービスプロバイダが外部のサービス提供機関から機能の提供を受ける場合の、外部のシステム機器との接続 | ゲートウェイ機能／サーバ機能 | 利用する回線種別をチェックする。 | | | | |
| | | | 専用線による接続を行い、サービス提供機関より接続認可を受けている。 | サービスプロバイダがサービス機能の提供を外部から受ける場合は、相互にHigh Secure Zone間の通信によって外部のサイトと接続する。そのためサービスプロバイダが外部サービス提供機関に接続するためには、次に記載にする通信方式のいずれかで通信を行い、サービス提供機関より接続認可を受ける必要がある。 | □ | 6.5 B (5) | |
| | | | IP-VPN・広域イーサネットによる接続を行い、サービス提供機関より接続認可を受けている。 | | □ | | |
| | | | IKE/IPSecによる暗号化とオンデマンド接続を条件としたオープンネットワークによる接続を行い、サービス提供機関より接続認可を受けている。 | | □ | | |
| | 4-10-4 外部のネットワークからの攻撃（DoS攻撃・不正形式パケットなど）に対する検知機能 | ファイアウォール／侵入検知・防御 | 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・防御の設定 | 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。 | | | |

| 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 |
|---|---|---|---|---|---|---|---|
| | 4-10-5 中継サービスの提供または利用においてのウィルスチェック | ゲートウェイ機能 | ウィルスチェックが正常に機能しているかチェックする。 | | | | |
| | | | 最新のウィルス定義ファイルを使用している | 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・拡散を防ぐために最新の定義ファイルによるチェックを行うこと。 | □ | 6.5 B (4) | |
| 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 | 5-1-1 システム障害防止のための設備管理 | - | 実施されている設備管理をチェックする。 | | | | |
| | | | システムの稼動状態、ハードウェア・ソフトウェアの使用状況の監視。 | 拠点内にある設備をシステム障害からの被害を抑えるため、守るべき設備要件を整え、管理を行う。 | □ | 6.10 C4 | |
| | | | 回線のトラフィック監視と回線使用量の把握。 | | | | |
| | | | 障害対応または防止に備えた、運用マニュアル・障害対応マニュアルの整備。 | | | | |
| | | | 機器および電源の冗長化等による高可用性の確保。 | | | | |
| | 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<br>6.10 C-7<br>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<br>6.10 C-7<br>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 | | | | |

## SP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 SP間の接続処理 | 2-1-1 SP間での通信に関する合意 | VPN機能 | 外部のSPとの間で通信の合意についてチェックを行う。 | | | | |
| | | | 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 | SPがASPプロバイダとしてサービス機能の外部委託を行う場合に、SP間の通信の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 | | | | | | | |
| 3-1 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。 | | | 6.3 ～ 6.6<br>7.3 C (2) 1<br>7.3 C (2) 3 | |
| | | | ゾーン種別 | | | | |
| | | | High Secure Zoneに配置されている。 | 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。 | □ | | |
| | 3-1-2 サービスプロバイダ内のネットワークの構成 | | 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分離している。 | 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分離することで不正アクセスを防止している。 | □ | 6.5B (2)<br>6.10 B-3Ⅱ | |
| 4．サービス種別 | | | | | | | |
| 4-3 医療機関向けの情報提供ASPサービス（外部保存型）の展開<br><br>【提供サービス項目例】<br>（※資料2 P.4参照）<br>・情報提供サービス<br>・メールサービス<br>・地域連携サービス<br>・検査データ配信サービス<br>・外部保存サービス<br>・タイムスタンプサービス<br>・VAサービス | 4-3-1 外部ASPが起点の接続の禁止 | ゲートウェイ機能<br>プロキシ機能 | 起点となる接続が禁止されているかチェックする。 | | | 6.5 C (3) | |
| | | | 外部保存ASPからの接続を禁止している | SPからのアップロードのみの接続を行うため、外部保存ASPからの接続は禁止し不正アクセスを防ぐ。 | □ | | |
| | 4-3-2 外部接続ASPサービスを提供する際の機器のHigh Secure Zoneへの配置 | ゾーン | 外部保存サービスに接続する機器がHigh Secure Zoneに格納されているかチェックする。 | | | 6.4 B③ | |
| | | | ゾーン種別 | | | | |
| | | | High Secure Zoneに配置されている。 | 保存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に配置し、不正なアクセスによる改ざん・情報漏えいを防ぐ。 | □ | | |
| | 4-3-3 外部接続ASPサービスを利用するユーザの認証機能 | ゲートウェイ機能／サーバ機能 | 外部保存サービス提供機関のサービスを利用するユーザの認証でどの技術を用いているかチェ | | | 6.5 B (1) | |
| | | | ID/パスワード | サービスを提供しているユーザを認証することで、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。 | □ | | |
| | | | 認証サーバによる認証（RADIUS/LDAP） | | □ | | |
| | | | 認証サーバ＋ワンタイムパスワードによる認証 | | □ | | |
| | | | ICカード/スマートカードによる認証 | | □ | | |
| | | | バイオメトリックによる認証 | | □ | | |
| 4-6 医療機関以外への情報提供ASPサービス（外部保存型）の展開<br><br>【提供サービス項目例】<br>（※資料2 P.4参照）<br>・情報提供サービス<br>・メールサービス<br>・地域連携サービス<br>・外部保存サービス<br>・タイムスタンプサービス<br>・VAサービス | 4-6-1 外部ASPが起点の接続の禁止 | ゲートウェイ機能<br>プロキシ機能 | 起点となる接続が禁止されているかチェックする。 | | | 6.5 C (3) | |
| | | | 外部保存ASPからの接続を禁止している | SPからのアップロードのみの接続を行うため、外部保存ASPからの接続は禁止し不正アクセスを防ぐ。 | □ | | |
| | 4-6-2 外部接続ASPサービスを提供する際の機器の配置 | ゾーン | 外部保存サービスに接続する機器がHigh Secure Zoneに格納されているかチェックする。 | | | 6.4 B③ | |
| | | | ゾーン種別 | | | | |
| | | | High Secure Zoneに配置されている。 | 保存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に配置し、不正なアクセスによる改ざん・情報漏えいを防ぐ。 | □ | | |
| | 4-6-3 外部接続ASPサービスを利用するユーザの認証機能 | ゲートウェイ機能／サーバ機能 | 外部保存サービス提供機関のサービスを利用するユーザの認証でどの技術を用いているかチェ | | | 6.5 B (1) | |
| | | | ID/パスワード | サービスを提供しているユーザを認証することで、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。 | □ | | |
| | | | 認証サーバによる認証（RADIUS/LDAP） | | □ | | |
| | | | 認証サーバ＋ワンタイムパスワードによる認証 | | □ | | |
| | | | ICカード/スマートカードによる認証 | | □ | | |
| | | | バイオメトリックによる認証 | | □ | | |
| 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）<br><br>【提供サービス項目例】<br>（※資料2 P.4参照）<br>・VPNサービス<br>・IXサービス<br>・ASPサービス | 4-10-1 外部サービス提供機関/大規模医療サービス機関との接続における、接続先の機器の配置 | ゲートウェイ機能／プロキシ機能 | 外部のサービス提供機関/大規模医療サービス機関に接続する機器が設置されたゾーン。 | | | 6.5 B (1) | |
| | | | ゾーン種別 | | | | |
| | | | High Secure Zoneに配置されている。 | 外部サービス提供機関/大規模医療サービス機関へのアクセスはHigh Secure Zoneからのみを許可し、不正なアクセスによる改ざん・情報漏えいを防ぐ。 | □ | | |
| | | | Secure Zoneが配置されている。 | | □ | | |
| | | | DMZが配置されている。 | | □ | | |