適合性評価申請手順と適合性評価方針

一般社団法人保健医療福祉情報適合性評価協会

1. 適合性評価申請の手順

適合性評価申請に当たっては下記の手順で進めます。

1）先ず、当協会のメールアドレスに、評価希望機器，サービスの概要をお知らせ頂き、当協会とコンタクトを取って頂きます。

2）お知らせいただいた内容が当協会の評価業務範囲に含まれると判断した場合には、直接申請希望者から内容を説明をお聴きし、協会からも評価手順等のご説明を致します。

3）当協会による内容の検討後にお示しする「費用見積もり等の条件」に同意頂いた場合に、申請者にご記入頂くチェックリスト、添付資料のご提出を頂き、評価を開始いたします。

2. 評価対象システム

厚生労働省から発行されている「医療情報システムの安全管理に関するガイドライン（最新は第 4 版　2009.3）」（以下、ガイドライン））「6.11-B-2-Ⅱオープンなネットワークで接続されている場合」に該当している VPN 接続サービスのシステムを当面の評価対象とし、以下の条件を満たしているものとします。

1）回線事業者とオンラインサービス提供事業者が、「盗聴」「侵入」「改ざん」「妨害」等の様々な脅威の対策のためネットワーク経路上のセキュリティを担保した形態でサービス提供している。

2）販売形態が売切りではなく、自システムの安全管理を確認する為の項目を明示した利用規定等を説明し、ユーザにその規定を基にユーザとしての安全管理等の規程を作成して頂き、ユーザが実施するようにサービス提供事業者が喚起している。

3）終端装置は接続サービス全体およびサービス拠点（中継接続拠点）により管理されている。

4）他サービスに接続する場合はユーザの終端装置から VPN 接続サービスを利用し、サービス拠点（中継接続拠点）に管理された接続点を経由して行っている　。

（他サービスへ接続する機能を提供する際の接続点と他サービスシステムとの接続評価は本評価の対象外とします）

3. 評価システムの申請単位

1）評価申請はユーザに対してユーザの安全管理の実施を確認しているサービス提供事業者ごとに 申請するものとします。申請単位は商品販売名あるいは型式名ごとに行ってください。

（従ってOEM製品でも商品名が異なる場合は別途申請を行ってください。
また商品名が同じでもユーザの安全管理を確認している最終サービス提供者が異なる場合も申請を行ってください）

2）サービス提供の形態が、直接ユーザに販売するのではなく OEM として提供するサービス提供事業者の場合、あるいは評価済みの OEM 製品をユーザに販売しているサービス提供者の場合は、その旨を明記して申請してください。

4. 評価指針

評価は、以下の観点に基づき実施するものとします。

①接続中継地点がある場合は電気通信事業法に従い、事業の届出を行っている事業者であること
②評価対象となるサービスの契約書およびサービス仕様書が提示されていること
③サービスの提供範囲、責任範囲が明確になっていること
④顧客情報を適切に管理することが明文化されていること
⑤サービス拠点の物理セキュリティや災害に対する対応が明確になっていること
⑥サービス設備のセキュリティが確保されていること
⑦サービス設備のシステム障害などを考慮した BCP（business continuity plan）が確立していること
⑧システム監視や障害発生時の連絡方法、故障復旧体制について記述されていること
⑨合意された内容に沿った通信設定がされていること（通信の合意をしていない拠点との通信やアクセスができないようになっていること）が明確になっていること
⑩暗号化通信において適正な技術を適用していること
⑪サービスに使用する医療機関の終端装置の製品情報および仕様が明確になっていること
⑫医療機関のセキュリティを守るために終端装置の設置個所から医療機関外までのセキュリティ対策実施を喚起していること

<注意事項>

VPN 接続サービスに対して適合性が評価されても、これは VPN 接続サービスの提供範囲内でガイドラインに適合していることが提出資料により評価されただけであり、当協会は VPN 接続サービスを利用して接続する他サービスに対する接続可否を、保証するものではありません。

5. 必要添付書類

申請書に以下の書類 ①～⑨を添付してください。

評価申請内容によっては、省略あるいは追加がありえます。

①評価チェックリスト(内容は当協会より提示します)

②サービス契約内容を示すドキュメント

③サービス仕様を示すドキュメント

以下の情報が記載された医療機関に提示する資料

a)サービス提供機能、責任範囲

b)サポート情報(監視、障害に関する体制など)

c)提供価格、サービス費用についての説明

d)終端装置情報

e)ユーザ利用規定等および実施喚起

(医療機関自身での利用規定作成および安全管理実施喚起について記載されていること)

④電気通信事業者の場合は、そのことを示すドキュメント

⑤参考として電気通信事業者としてサービス提供実績を示すドキュメント

⑥サービス拠点の物理セキュリティや災害に関するドキュメント

⑦サービス設備のシステム構成を示すドキュメント

以下の情報が記載されていること

a)システム障害対策

b)ネットワークセキュリティ

c)装置監視

d)システム最適化(パッチ適用、ファームウェア更新)

e)サービス拠点、終端装置、終端装置と接続システムの関係

f)終端装置とそれに接続するシステムの関係

g)他サービスとの接続

⑧終端装置に関するドキュメント

暗号化通信仕様および最低限のガイドライン 6.11-C4「ルータ等のネットワーク機器は、安全性が確認できる機器を利用」への対策として、終端装置がガイドラインに適合していることを確認できる情報が記載されていること

⑨プロダクトの提供範囲，提供主体に関するドキュメント

以 上