

保健医療福祉情報安全管理

適合性評価協会

Health Information Security Performance Rating Organization

HISPROの役割

—安全な情報基盤構築の実現に向けて—

保健医療福祉情報安全管理適合性評価協会

理事長 喜多 紘一

東京工業大学・総合研究院・特任教授

2009年9月30日

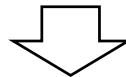
(医療情報システム安全管理評価制度一説明会)

Copyright©2009 KITA All rights reserved

1

設立の経緯

- 厚生労働省の医療情報ネットワーク基盤検討会において「医療情報システムの安全管理に関するガイドライン」が策定され公開されている。
- ガイドラインによって医療情報システムの安全管理に関して、一定の指針は示されたが、ガイドラインの「実効性の担保」については不安が残る状況であった。



「実効性」を確保しつつユーザ視点で「安全性を客観的に評価する」ことを目的に、利用者である、日本医師会、日本薬剤師会、また、医療ITの専門集団である日本医療情報学会を設立時社員とする法人（一般社団）として設立。

Copyright©2009 HISPRO All rights reserved

2

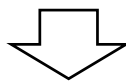
体制

- 社員
 - 一般社団法人日本医療情報学会
 - 社団法人日本医師会
 - 社団法人日本薬剤師会
- 理事・理事長・監事
 - 理事長 喜多 紘一
 - 理事 安部 好弘
 - 理事 中川 俊男
 - 理事 野津 勤
 - 理事 山本 隆一
 - 監事 篠田 英範

Copyright©2009 KITA All rights reserved

当面の業務

- オンライン請求のIPsec+IKEを用いた回線について、医療情報システムの安全管理に関するガイドラインに沿った評価を実施。
- IPsec+IKE以外の方式についても、順次評価手法を確立して実施する予定。



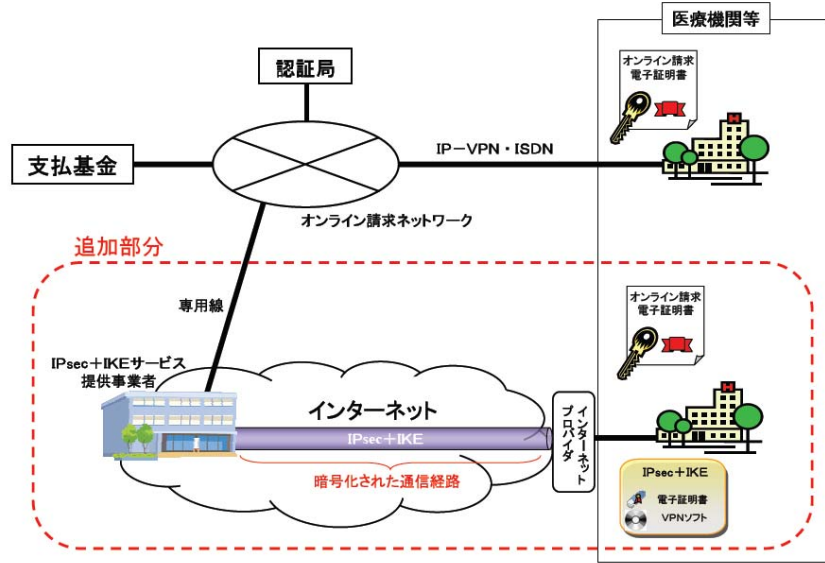
これまでHEASNETが行っていた適合性評価を引き取り、利用者視点から再評価し、HISPROとして評価結果を公開。
HEASNETで評価した4社に加え、順次、評価業者を増やして行く予定。
また、業者だけではなく地域イントラ網を提供している地域医師会等の評価にも対応予定。

Copyright©2009 HISPRO All rights reserved

HISPROの業務イメージ



インターネット接続のイメージ



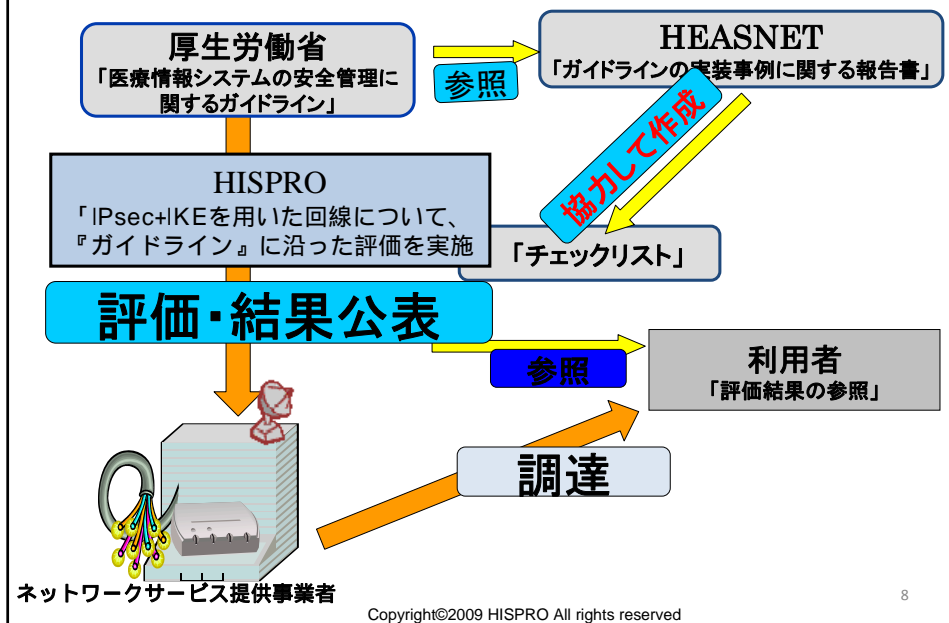
(社会保険診療請求支払基金ホームページより抜粋)

インターネットオンライン請求について

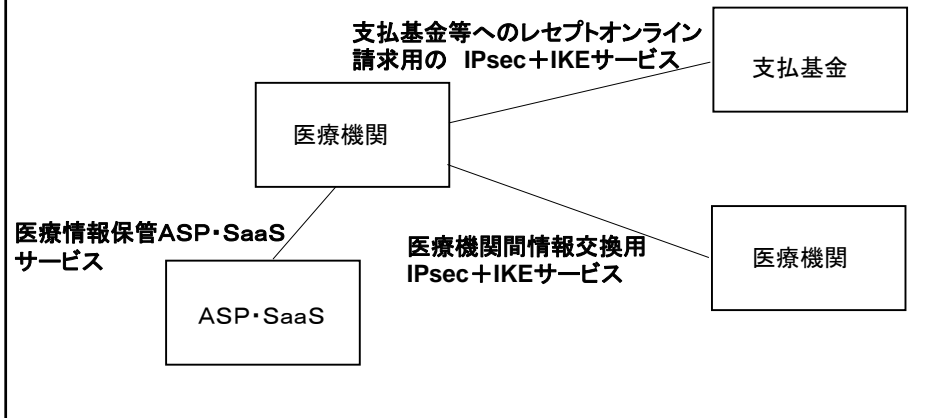
- このオンデマンドVPN接続を実施する場合、インターネットに接続するためのプロバイダ(ISP)の他に、「IPsec+IKEサービス提供事業者」への申し込みが必要となります。
- オンライン請求に接続可能な「IPsec+IKEサービス提供事業者」については、保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム(HEASNET)のホームページで「医療情報システムの安全管理に関するガイドライン第2版」(PDF:1.1MB)に適合したサービスを提供していると評価された事業者が紹介されています。
- 詳しくは、下記のHEASNETホームページ等をご覧ください。

(社会保険診療請求支払基金ホームページより抜粋)

IKE+IPsecの評価の位置付け



サービス区分ごとのチェックリスト による評価 (利用者がサービス導入時に参考にする)



セキュリティ評価制度

- プライバシーマーク制度 (JIS Q 15001)
 - JIS Q15001に適合して電子計算機処理に係る個人情報の適切な保護のための体制を整備している事業者に対し、その申請に基づきその旨の認定及びその旨を示す特別の表示であるプライバシーマークの付与を行う制度。
- 情報セキュリティマネジメントシステム (ISMS) 適合性評価制度 (ISO/IEC 27001)
 - 組織が保護すべき情報資産について、技術的なセキュリティ対策だけでなく、人間系の運用・管理面のセキュリティ対策などを含めたセキュリティ管理に対する第三者適合性評価制度
- セキュリティ評価・認証 (ISO/15408)
 - 情報システムやそれを構成する機器・ソフトについて、セキュリティ機能全般および目標とするセキュリティレベルをある評価基準に基づいて評価し、その結果を認証する制度

医療関連評価

- 病院機能評価(日本医療評価機構)
 - 病院の現状を客観的に把握する為に、病院機能を体系的な審査により、優れている点や改善すべき問題点を評点と評価所見として具体的に示す。
- 医療情報システム安全管理評価制度(MEDIS-DC)
 - 医療機関等の「医療情報システムの安全管理に関するガイドライン」への準拠レベルを第三者が客観的に評価する
- 保健医療福祉安全管理適合性評価(HISPRO)
 - ユーザ視点で提供されたサービスの「医療情報システムの安全管理に関するガイドライン」への適合性を客観的に評価する

Copyright©2009 KITA All rights reserved

当面の評価対象システムについて

- 「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」に該当する
- 回線事業者とオンラインサービス提供事業者が、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
- 販売形態は売りきりではなく、安全管理の為にユーザが遵守すべき項目を明示した利用規定等を説明し、且つ、ユーザが実施していることをサービス提供事業者が定期的に確認している
- 6.11-C1最低限のガイドラインに対する対策として「IPSec とIKE を利用することによりセキュアな通信路を確保する」を適用している
- 端末装置は接続サービス全体ならびにサービス拠点(中継接続拠点)により管理されている
- 他サービスに接続する場合はユーザの端末装置からVPN接続サービスを利用し、サービス拠点(中継接続拠点)の管理により行っている

Copyright©2009 KITA All rights reserved

6 情報システムの基本的な安全管理

- 6.1 方針の制定と公表
- 6.2 医療機関における情報セキュリティマネジメントシステム(ISMS)の実践
- 6.3 組織的安全管理対策(体制、運用管理規程)
- 6.4 物理的安全対策
- 6.5 技術的安全対策
- 6.6 人的安全対策
- 6.7 情報の破棄
- 6.8 情報システムの改造と保守
- 6.9 情報及び情報機器の持ち出しについて
- 6.10 災害等の非常時の対応
- 6.11 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
- 6.12 法令で定められた記名・押印を電子署名で行うことについて

当面の評価対象システムについて

- 「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」に該当する
- 回線事業者とオンラインサービス提供事業者が、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
- 販売形態は売りきりではなく、安全管理の為にユーザが遵守すべき項目を明示した利用規定等を説明し、且つ、ユーザが実施していることをサービス提供事業者が定期的に確認している
- 6.11-C1最低限のガイドラインに対する対策として「IPSec とIKEを利用することによりセキュアな通信路を確保する」を適用している
- 端末装置は接続サービス全体ならびにサービス拠点(中継接続拠点)により管理されている
- 他サービスに接続する場合はユーザの端末装置からVPN接続サービスを利用し、サービス拠点(中継接続拠点)の管理により行っている

6.11 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」(最低限のガイドライン) 1/2

1. ネットワーク経路でのメッセージ挿入、ウイルス混入などの改ざんを防止する対策をとること。セッション乗っ取り、なりすまし防止、例えばIPSecとIKEを利用すること
2. 相手の確認を行う。PKIによる認証、Kerberosのような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワードなど
3. 施設内における正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策をとること
4. 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…。ルータでの回り込み禁止
5. 送信元と相手先の当事者間で当該情報そのものに対する暗号化などのセキュリティ対策を実施すること。…………

Copyright©2009 KITA All rights reserved

6.11 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」(最低限のガイドライン) 2/2

6. 関連組織の責任分界点、責任の所在を契約書等で明確にすること
7. リモートメンテナンスを実施する場合は不必要なログインを防止すること。
8. 回線事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質に関して問題がないか確認。

Copyright©2009 KITA All rights reserved

評価区分: HISPRO 支払基金等へのレセプトオンライン請求用の
IPsec+IKEサービス提供事業者に対するチェックシート

要件			確認項目	対応策	確認エビデンス
大分類	中分類	小分類			
サービス全体	サービス内容、サービス仕様(責任分界点)、情報の管理、事業継続、運用				
サービス拠点	物理的セキュリティ 技術的セキュリティ(拠点内部・外部侵入・監視・端末&サーバ)				
接続サービス	サービス内容 端末装置のセキュリティ 通信変換拠点内での管理 接続の方式				
その他	サービスの共有				

Copyright©2009 KITA All rights reserved

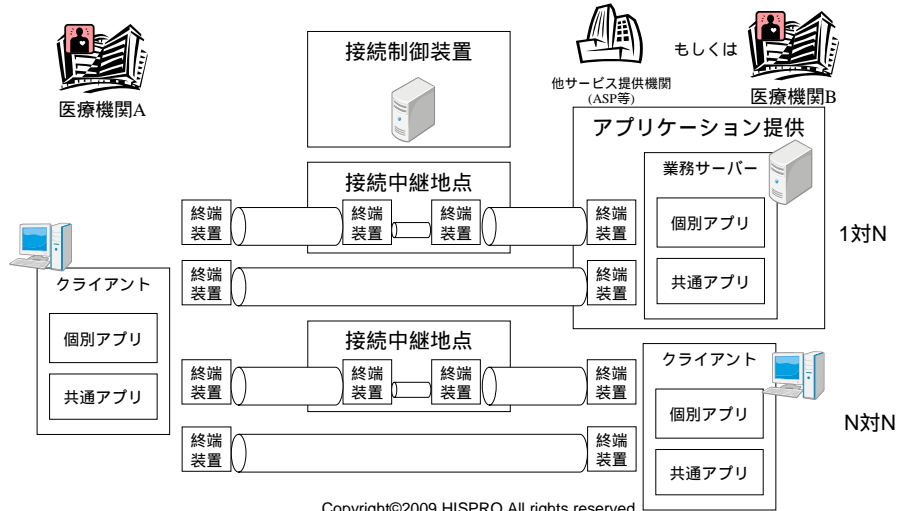
評価システムの申請単位

- 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。

Copyright©2009 HISPRO All rights reserved

VPNサービスの提供範囲

- 以下の図サービスの提供範囲(責任範囲)について、青で塗りつぶしてください
- サービス拠点(区画)がある場合は、拠点(区画)単位で赤枠で囲ってください
 - サービス拠点(区画)ごとに基準を満たしているか評価致します



評価指針

- 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端末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端末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

適合性評価結果

評価区分:「支払基金等へのレセプトオンライン請求用
IPsec+IKEサービス」

厚生労働省「医療情報システムの安全管理に関するガイドライン」……チェックリスト」に基づいて適合性を評価した結果、下記のサービスについて適合していることを評価しました。適合性評価有効期間は2年です。サービス利用に当たっては評価コメントの内容に留意してください。

評価サービス名	
サービス提供事業者	
評価番号	HSP-C-C1XXX
評価証発行日	
評価コメント	

Copyright©2009 KITA All rights reserved

評価済サービス

セキュアネットワークサービス PC接続型<レセプト>
セキュアネットワークサービス ルータ型<レセプト>
FENICS メディカル・グループネットサービス ルータタイプ
FENICS メディカル・グループネットサービス USBタイプ
レセプトオンライン接続サービス
IP-Members SCタイプ(レセプト接続のみ)
IP-Members STタイプ(レセプト接続のみ)

Copyright©2009 KITA All rights reserved

まとめ(HISPROの役割)

- 目的
 - 当協会は、保健医療福祉の各分野において、国の提唱する「医療情報システムの安全管理に関するガイドライン」に基づいた安全な情報基盤を効率よく実現することを目的とします。
- 事業内容
 - 保健医療福祉情報安全管理に関わる評価基準立案
 - 保健医療福祉情報安全管理に関わるシステムおよびサービスの適合性評価
 - 保健医療福祉情報安全管理に関するリスク管理ならびに対策に対する助言
 - 保健医療福祉情報安全管理および適合性評価に関する普及活動
 - その他、上記の目的を達成するのに付帯する一切の活動