医療情報システムの安全管理を評価するための チェックシートの活用

1）各チェックシートの内容、利用方法および評価の概要

喜多紘一　（一社）保健医療福祉情報安全管理適合性評価協会

2）チェックシートの利用と評価の経験

AmiVoiceを中心にクラウドシステムへの利用と評価

金子　隆　（株）アドバンスト・メディア　医療事業部

地域連携への利用と評価を中心に

石黒満久　（株）NTTデータ中国　法人事業部ヘルスケア＆クラウドサービス部

3）医療等サイドからチェックシートおよび評価結果の利用と期待

野口貴史　（国研）国立成育医療研究センター　情報管理部

第39回医療情報学連合大会
（第20回医療情報学会学術大会） COI開示

演題名：　医療情報システムの安全管理を評価するための
　　チェックシートの活用

オーガナイザー名：　　喜多紘一

今回のチュートリアルの演題について
開示すべきCOIはありません。

各チェックシートの内容、利用方法および評価の概要

(一社)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)　理事長
喜多　紘一　k.kita@gakushikai.jp

2019年11月21日

情報セキュリティ10 大脅威 2018

独立行政法人情報処理推進機構冊子より

「個人」向け脅威	順位	「組織」向け脅威
インターネットバンキングや クレジットカード情報等の不正利用	1	標的型攻撃による被害
ランサムウェアによる被害	2	ランサムウェアによる被害
ネット上の誹謗・中傷	3	ビジネスメール詐欺による被害
スマートフォンやスマートフォンアプリを 狙った攻撃	4	脆弱性対策情報の公開に伴う 悪用増加
ウェブサービスへの不正ログイン	5	脅威に対応するための セキュリティ人材の不足
ウェブサービスからの個人情報の窃取	6	ウェブサービスからの個人情報の窃取
情報モラル欠如に伴う犯罪の低年齢化	7	IoT 機器の脆弱性の顕在化
ワンクリック請求等の不当請求	8	内部不正による情報漏えい
IoT 機器の不適切な管理	9	サービス妨害攻撃によるサービスの停止
偽警告による インターネット詐欺	10	犯罪のビジネス化 （アンダーグラウンドサービス）

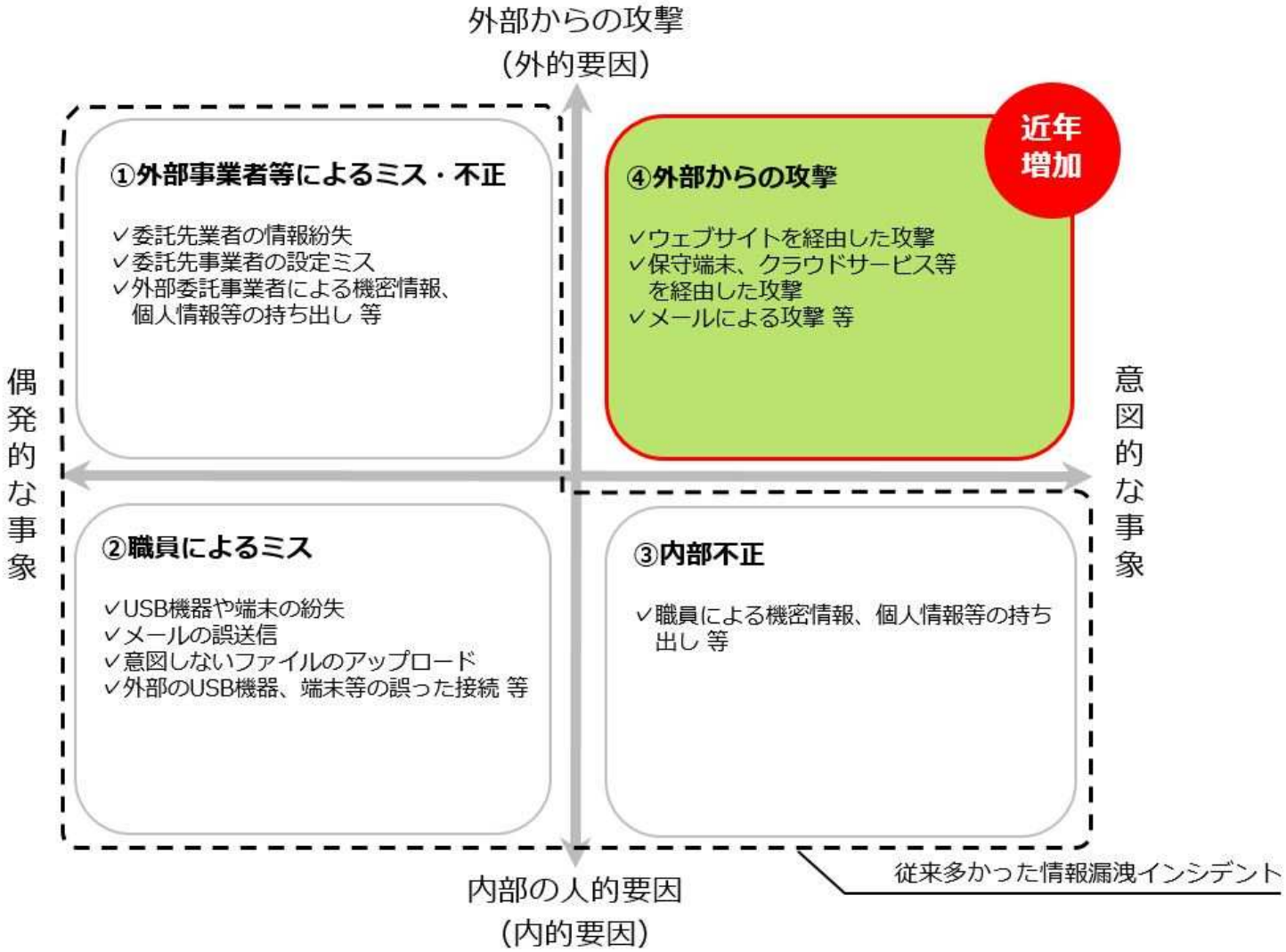
被害事例集

サイバーセキュリティ経営ガイドライン解説書（IPA）2016添付資料+α

メディア掲載日・発生日	発生場所	概要
2014/3/28	福祉事務所	システム管理会社によるサイト変更の際の誤操作により、本人以外でも会員情報が外部から閲覧可能な状態に
2014/12/24	病院	検診受診者の個人情報9千人分を記録したUSBメモリが所在不明
2016/2/5	病院	ランサムウェア感染で電子カルテ等のデータが閲覧不可能となり、攻撃者にビットコインを支払ってデータの復号を依頼
2019/3/8	会社	医療機関から提供を受けた患者情報・アンケート調査情報を元従業員がUSBメモリにコピーし不正に持ち出し
2019/5/20	病院	医師のPCに不正アクセスが発生。メールアカウントが乗っ取られ、官公庁等へマルウェアが添付されたメールを送信
2019/5/31	病院	院内の複数のパソコンがコンピューターウイルスに感染し、新規患者と救急患者の受け入れができない等、診察に支障
2019/8/5	病院	所属する医師が研究のために20の医療機関から集められた「がんの患者情報」をメールに添付し、正規相手外に誤送付された

情報セキュリティインシデントとは何か

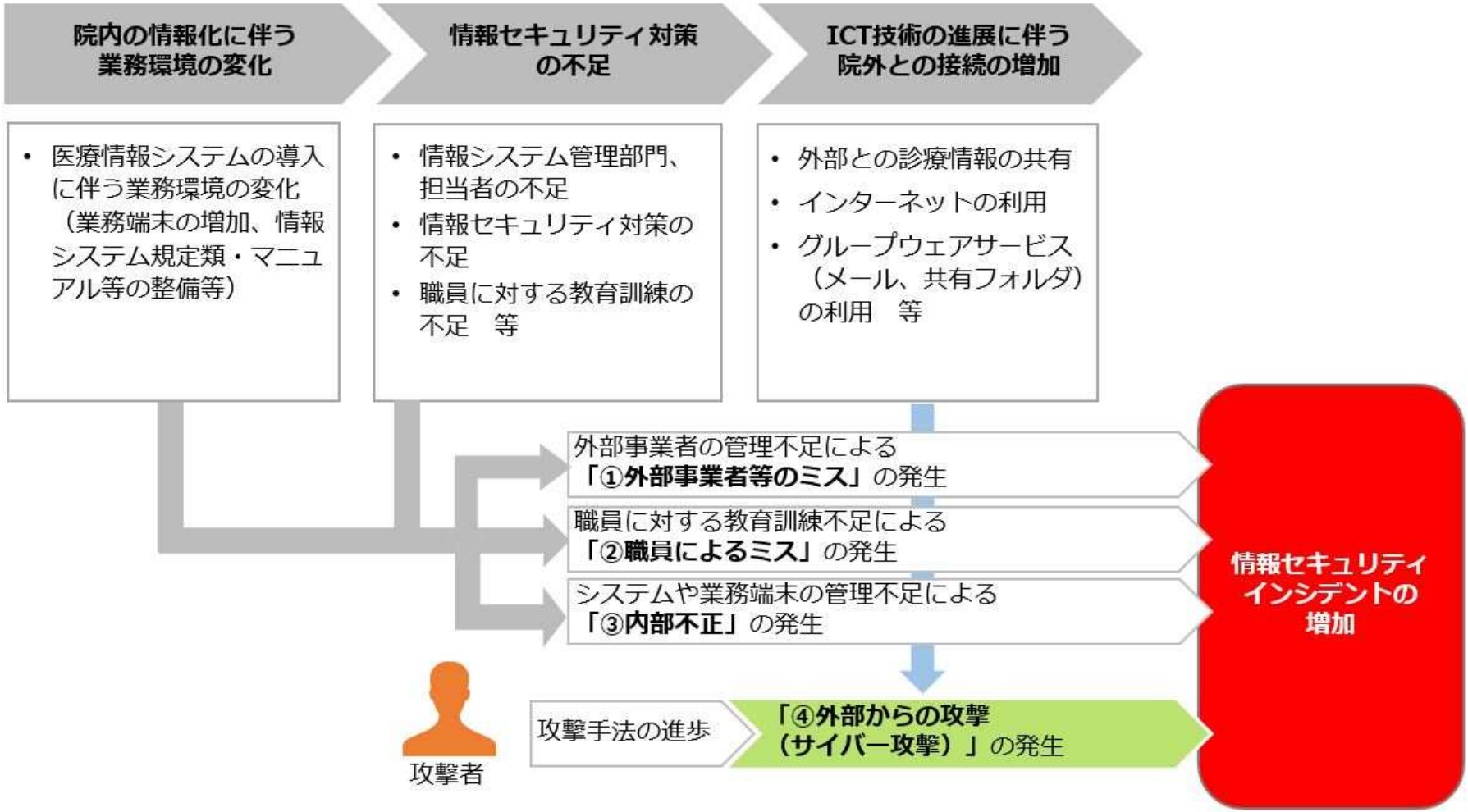
医療情報連携ネットワーク支援Navi　厚生労働省



情報セキュリティインシデントの増加理由

医療情報連携ネットワーク支援Navi　厚生労働省

医療機関における情報化の動向



各種ガイドライン

- 医療情報システムの安全管理に関するガイドライン　第5 版
- クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン　第1版
- 医療情報を受託管理する情報処理事業者向けガイドライン　第2版
- レセプトのオンライン請求に係るセキュリティに関するガイドライン　平成１８年４月
- オンライン診療の適切な実施に関する指針
  令和 元年 ７月一部改訂

適合性評価チェックシートの種類

HISPRO作成

1）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

2）民間事業者による医療情報の外部保存及び
　クラウドサービス

3）地域医療介護連携サービスの安全管理

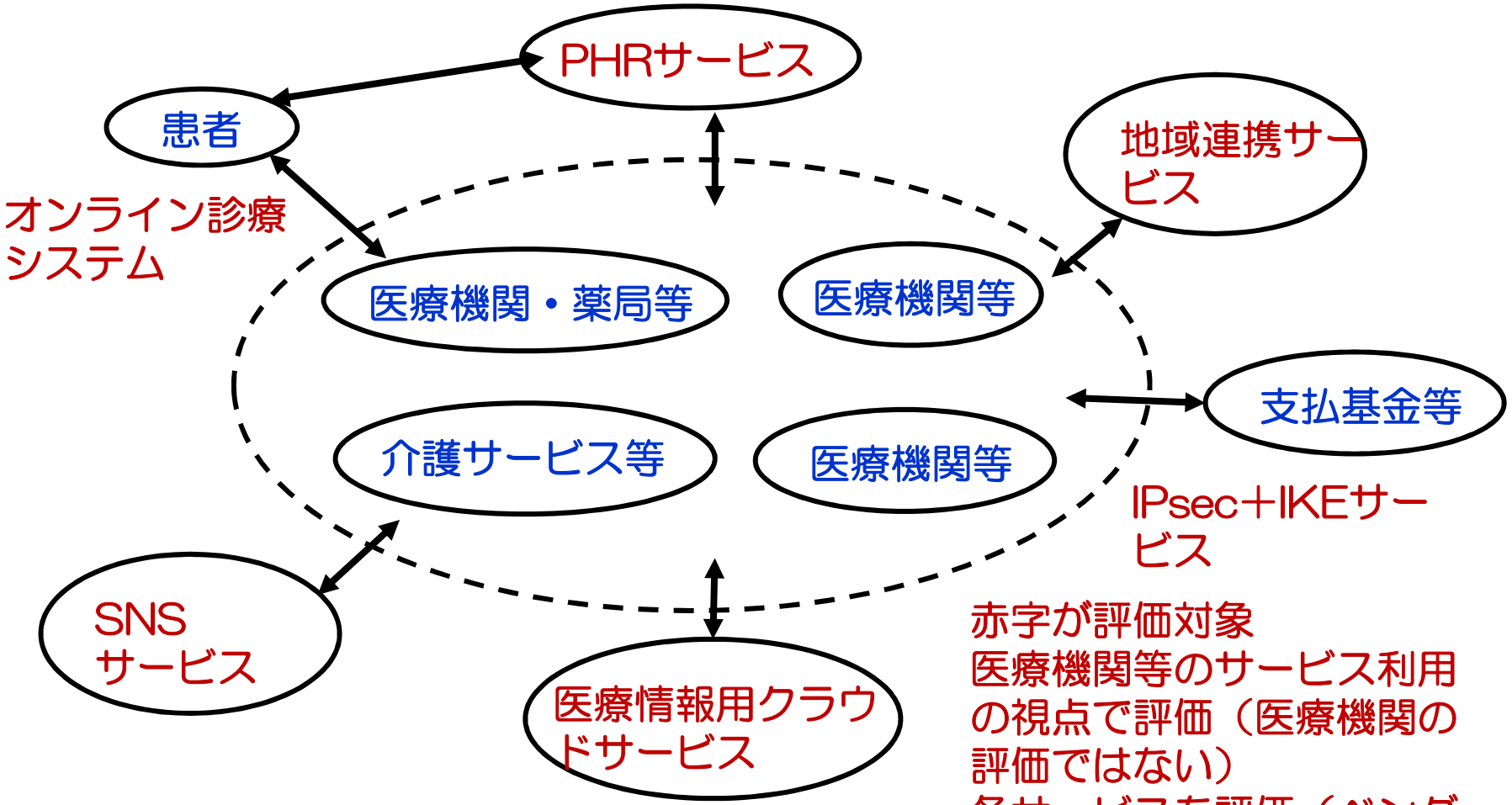
4）SNSサービス利用の安全管理

5）オンライン診療システムの安全管理

6）PHRサービス事業者における安全管理（作成中）

適合性評価対象の連関図

医療機関等向けサービスの評価



赤字が評価対象
医療機関等のサービス利用の視点で評価（医療機関の評価ではない）
各サービスを評価（ベンダーの体制評価ではない）

HISPROチェックシートの引用

- 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
  - セッション間の回り込みリスクへの対策についてHISPROのチェックシートが参考になる（安全管理ガイドライン）
  - 支払基金ホームページ→オンライン支払請求→その他→(HISPRO)事業者の適合性評価結果

オンライン診療システムの安全管理←

第三者機関の認証としては以下のいずれかが望ましい（指針）

- SNSサービス利用の安全管理
  - SNSを利用する場合は、これに基づいてチェックを行い、対策を講じることを薦める。（日医IT化宣言2016 実現に向けた方策）
  - （同様に安全管理ガイドライン Q&A5）

チェックシートの体裁

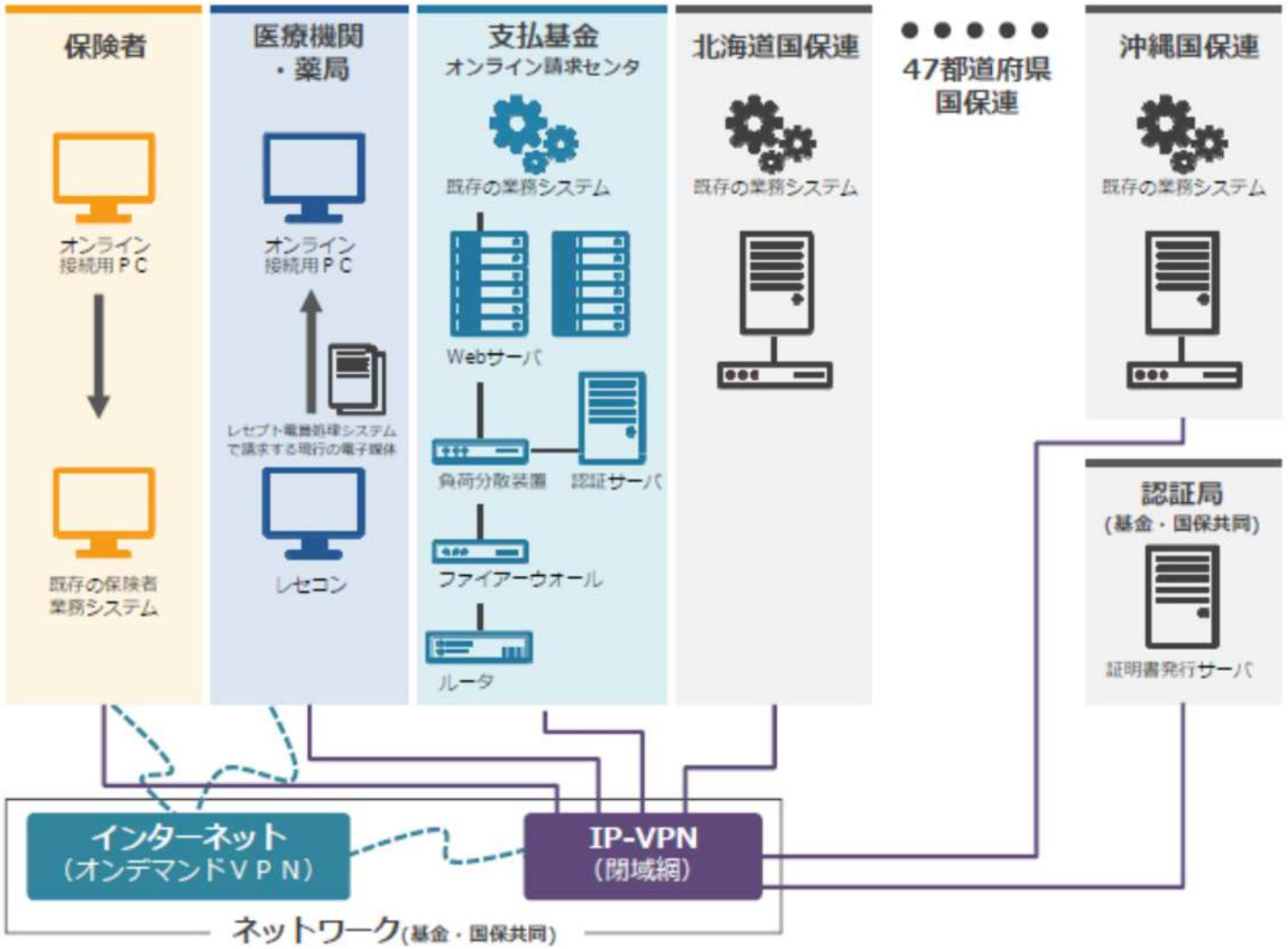
チェック事項			確認者記入欄		評価者記入欄	
項目 分類	確認内容	エビデンス例	対応策	エビデンス	評価 結果	コメント

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 チェックシート

オンライン請求システムの概要

（社会保険診療報酬支払基金ホームページより）

オンデマンド
VPN
→
ＩＰｓｅｃ＋
ＩＫＥサービス



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（1/3）

	大分類	中分類	項目	要件
1.1	サービス全体	サービス内容	5	サービス内容の確認/ 法令順守/第三者の明確化/権限の管理の実施/ サービス内容変更時の対応
1.2		サービス仕様	2	医療機関とサービス提供機関との責任分界点の明確化/サービス連携先との責任分界点の明確化
1.3		情報の管理	1	顧客情報の管理
1.4		事業継続性	3	障害時の体制の明確化/障害時の対策方針の明確化/障害時の対策の明確化
1.5		運用	4	サービスの状態を監視/システム障害防止(守るべき設備要件/バックアップ/バックアップ等の管理
2.1	サービス拠点	サービス拠点の物理セキュリティ	3	入館に対する制限/領域に対する入室管理/システムの設置場所
2.2		サービス拠点の技術セキュリティ（拠点内部）	4	ネットワークの構成/提供サービス毎の通信経路の分離/High Secure Areaを接続起点としたアクセス/ High SecureAreaを起点とした外部への接続

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（2/3）

	大分類	中分類	項目	要件
2.3	サービス拠点	サービス拠点の技術セキュリティ（外部から侵入）	4	他拠点との接続合意がされていない通信/るユーザの認証/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/ 外部からの攻撃の検知
2.4		技術セキュリティ（監視）	1	ファイアウォールやプロキシなどの外部と直接接続している装置のアクセス監視の実施
2.5		技術セキュリティ（端末、サーバ）	1	サービス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
3.1	接続サービス	サービス内容	5	接続先拠点との通信に関する合意/ 責任分界点の明確化/ 禁止事項の明確化/セキュリティ対策の必要性の説明責任/アクセスを監視
3.2		終端装置のセキュリティ	6	終端機器の設定変更/改ざんへの対策/ 導入環境に対する要求事項の確認/ 不正中継に対する対策/ 終端装置のスルーモードの禁止/接続サービスを利用するユーザの認証機能/ 通信合意に対するアクセスコントロール

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（3/3）

	大分類	中分類	項目	要件
3.3	接 続 サ ー ビス	通信変換拠点内での管理	1	通信変換拠点内での通信(終端装置から終端装置までHighSecureArea内で通信)
3.4		接続の方式	17	IKEでの通信モード/IKEでの暗号化アルゴリズム/IKEでの認証/IKEでの鍵長/IKEの認証方式/セッション毎の共通鍵の自動決定/ IPSecによる暗号化/IPSecでのメッセージ認証/通信に用いる秘密鍵の管理/提供事業者の確認/要求に応じたVPN接続の運用(通信の必要がないときはVPN接続を行わない機能/接続制御装置が設置してあるサービス拠点について、本チェックリストの2.サービス拠点の基準を満たしていること)
4.1	その他	サービスの共有	2	サービスの分離（サービス拠点で施設・資産の共有/提供先の中で、施設・資産の共有がある場合)
		項目数合計	59	

民間事業者による
医療情報の外部保存及び
クラウドサービスチェックシート

クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン第1版（総務省）

第１章 本ガイドラインの前提条件及び読み方

第２章 クラウドサービス事業者が医療情報を取り扱う際の責任等

第３章 クラウドサービス事業者に対する安全管理に関する要求事項

第４章 安全管理の実施における医療機関等との合意形成の考え方

（別添）ガイドラインに基づくサービス仕様適合開示書及びサービス・レベル合意書（SLA）

第3章 クラウドサービス事業者に対する安全管理に関する要求事項

３．１ クラウドサービス事業者に対する要求事項の考え方

３．２ 医療情報サービスに求められる安全管理に関する要求事項

３．３ 外部保存に 関する 要求事項

３．４ クラウドサービスの利用終了に関する要求事項

３．５ オンライン診療システム提供事業者における安全管理対策

３．６ PHRサービス事業者における安全管理対策

3．2 医療情報サービスに求められる安全管理に関する要求事項

3.2.1 組織的安全管理対策
3.2.2 物理的安全管理対策
3.2.3 技術的安全管理対策
3.2.4 人的安全管理対策
3.2.5 情報の破棄 に関する安全管理対策
3.2.6 情報システムの改造と保守 に関する安全管理対策
3.2.7 情報 及び 情報機器の持ち出しについて の安全管理対策
3.2.8 災害等の非常時対応 についての安全管理対策
3.2.9 個人情報を含む医療外部と 交換する 場合の安全管理対策
3.2.10 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の安全管理対策

医療情報を受託管理する情報処理事業者向けガイドライン 第2 版（経済産業省）

4 電子的な医療情報を扱う際の責任のあり方

5 医療情報の取扱に関する知識

6 電子保存の要求事項について

7 医療情報を受託管理する情報処理事業者における安全管理上の要求事項

- 7.1 医療情報に係る情報処理事業を受託する上で推奨される認証及び認定
- 7.2 情報資産管理
- 7.3 組織的安全管理策（体制、運用管理規程）
- 7.4 医療情報の伝達経路におけるリスク評価
- 7.5 物理的安全対策
- 7.6 技術的安全対策
- 7.7 人的安全対策
- 7.8 情報の破棄.
- 7.9 医療情報システムの改造と保守
- 7.10 医療情報処理に関する事業継続計画

8 診療録及び診療諸記録を外部に保存する際の基準

民間事業者による医療情報の外部保存及びクラウドサービス

	大分類	中分類	項目	対策項目
1～5	ユーザとの契約	サービス提供者の責任	5	医療機関等ガイドライン等を満たすことを「患者等に説明する責任」を果たすための責任/医療機関等が「医療情報システムの運用管理責任」を果たすための責任/医療機関等が「情報保護体制を適宜見直して改善する責任」を果たすため、定期的なレビュー結果の報告等の責任/医療機関等がk緊急時「個々の患者に対する説明責任」「行政機関や社会への説明責任」を果たすための責任
6～9		サービスの利用終了	4	サービス変更の場合、影響を最小とし、十分な期間をもって告知。内容、条件等を明確に提示/サービス仕様適合開示書等の内容を変更する場合も同様/クラウドサービス利用の終了やクラウドサービス変更に対する運用管理規程等を策定・提示/クラウドサービス提供の停止又は医療機関等におけるクラウドサービス利用停止が生じた場合は、速やかに、記録の削除、媒体及び機器の廃棄等を行う

民間事業者による医療情報の外部保存及びクラウドサービス

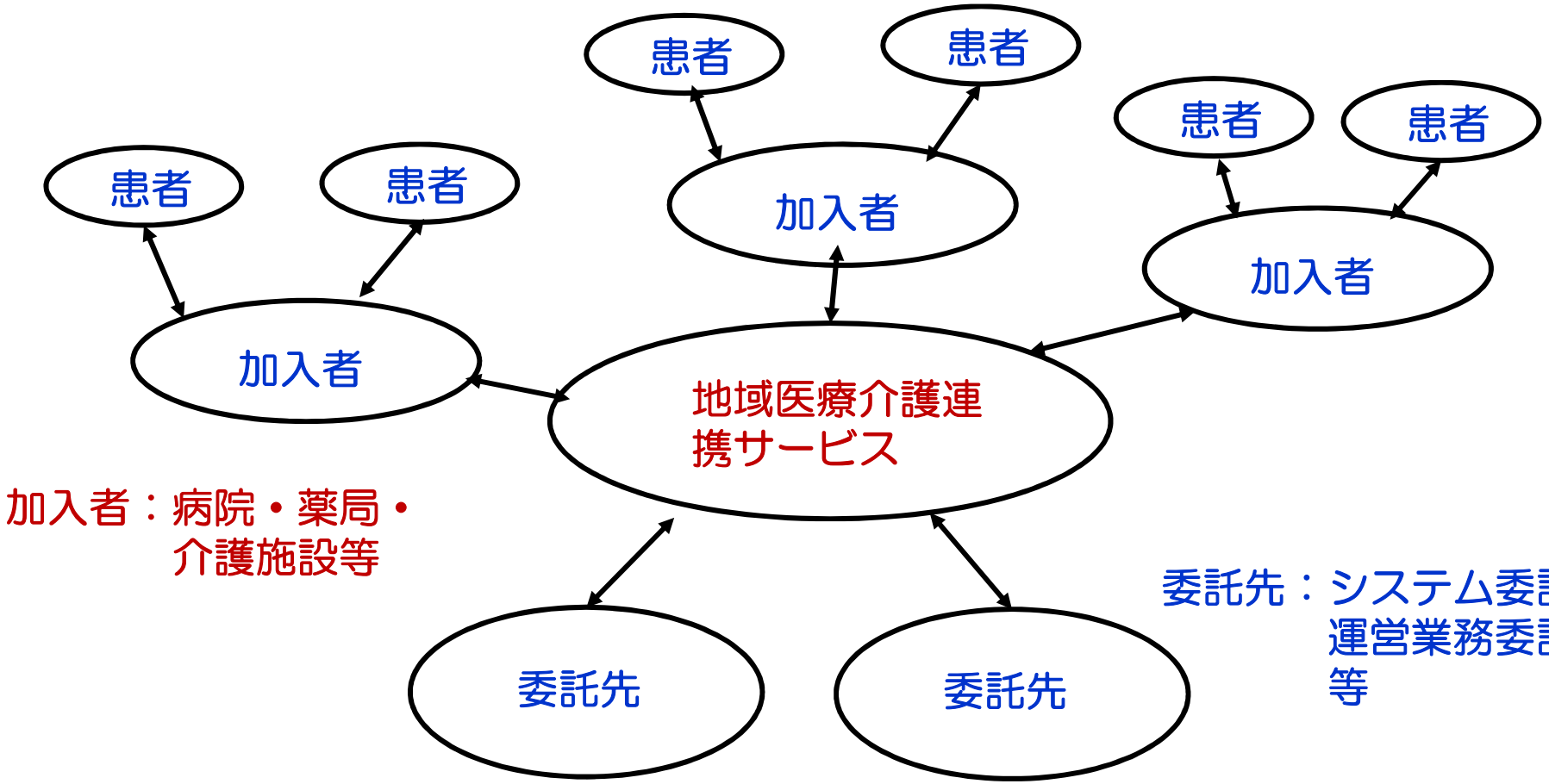
	大分類	項目	中分類
	ユーザとの契約	9	サービス提供者の責任/サービスの利用終了/
	組織	41	実績・第三者評価/情報セキュリティ/体制/リスク管理/資産管理/職員管理/委託管理/事業継続(BCP)/監査
	サービス仕様	150	サービスの構成/外部サービス利用/識別・認証・認可(アクセス制御)/記録(ログ)/情報漏洩対策/データ管理/物理(設備・機器)/ネットワーク/ブラウザ/e-文書法/電子署名/留意する機器等
	運用	53	運用/情報管理/保守・品質管理/非常時
		253	合計項目数

地域医療介護連携サービスの安全管理チェックシート

HISPROオリジナル

想定する地域医療介護連携サービス

患者：住民・健常者・患者・被介護者・家族等



加入者：病院・薬局・介護施設等

委託先：システム委託
運営業務委託
等

地域医療介護連携サービスの安全管理

（体制・規定有無に対する適合性評価）HISPROオリジナル

	分類	項目	評価内容
A	方針公表	4	サービス全体を把握し、提示できる資料/個人情報保護方針/患者データに対して、加入者が同意を取る仕組み/同意なくデータの第三者提供をしていないこと
B	責任分界の明確化	6	システム仕様と責任分界点/情報・データの所在場所把握/端末の取り扱い/リスクの分析/免責事項の明確化
C	組織・運用管理規程	10	運用管理規程/組織体制図/アクセスポリシー/教育/委託管理契約/秘密保持契約/データの適切な管理/加入者の退会/運用状況の開示/加入者へSLAの開示
D	システム	1	システムの各省ガイドライン準拠の確認
E	モニタリング・監査	2	アクセスログの取得と監査/監査規約と定期的見直し
F	事業継続性	3	BCP規定/相互運用性/契約終了時のデータ移行
G	加入者の実施義務の明確化	6	責務およびリスク/整備すべきシステム機能＆環境/職種別アクセス管理/作成すべき運用管理規程/従業員へ教育内容の提供/患者への同意の取り方
	項目数合計	32	

SNSサービス利用の安全管理
チェックシート

HISPROオリジナル

SNSサービス利用の安全管理

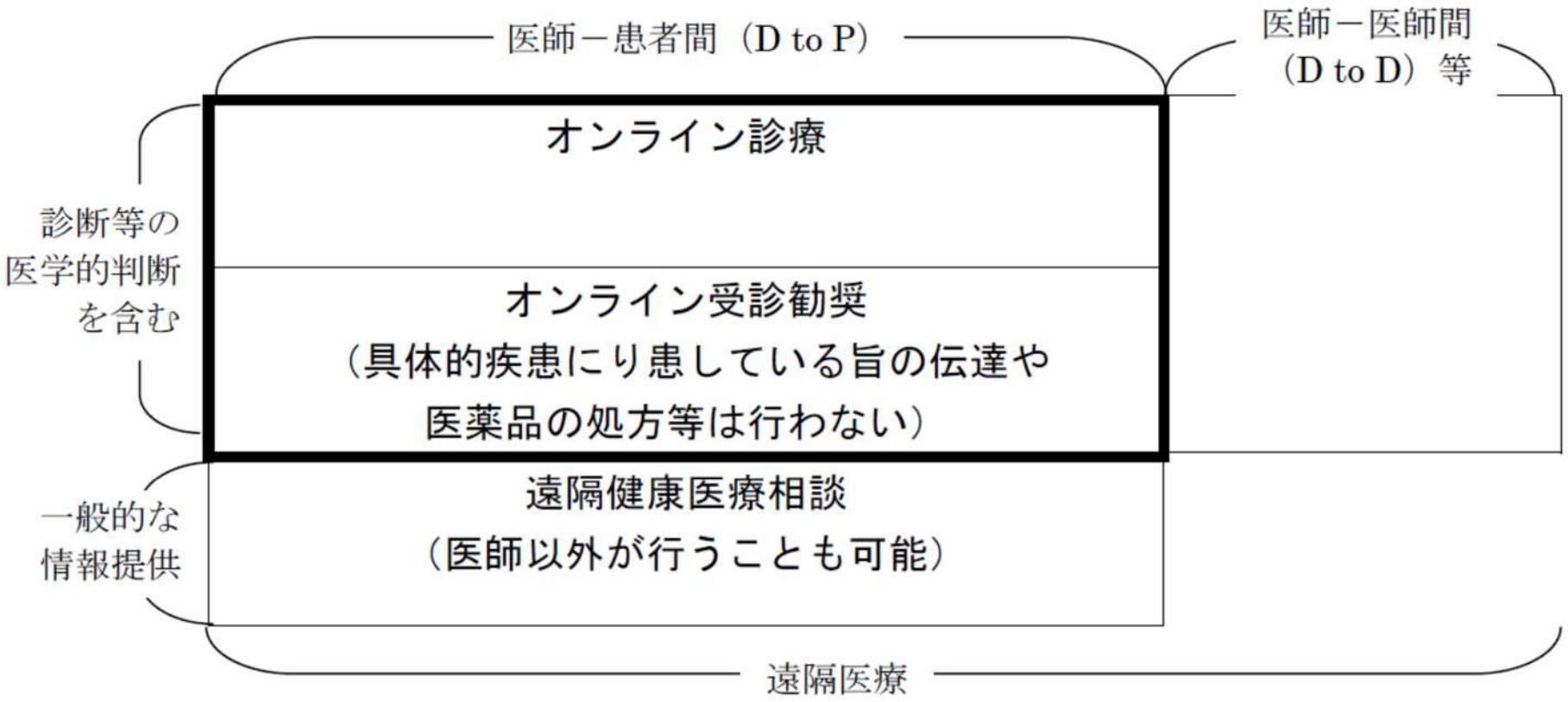
	大分類	中分類	項目	対策項目
	A:契約事項	個人情報保護方針の策定	2	SNSサービス利用主体として策定/運営ホームページ等、もしくは説明事項として公開
		苦情のための窓口体制の構築	3	SNSサービス利用主体として、利用者に対する問い合わせ体制の構築/連絡先、手段/運営ホームページ等もしくは説明事項として公開
		サービス内容や利用目的の説明	2	患者・利用者へ説明できる資料の作成/運営ホームページ等もしくは説明事項として公開、もしくは個別同意
		サーバ蓄積情報の目的外利用	3	利用者間の情報連携のためのみに利用/サービスの正常な動作のための確認に限定した利用/利用目的の明記・運営ホームページ等もしくは利用する際の説明事項として公開
		ユーザの実施すべき対策や運用の明確化	3	利用する端末に対する技術的セキュリティ対策/実施すべき運用/運営ホームページ等もしくは説明事項として公開、もしくは個別説明

SNSサービス利用の安全管理

	大分類	項目	中分類
A	契約事項	21	個人情報保護方針の策定/苦情窓口/患者・利用者にサービス内容や利用目的の説明/目的外利用/実施すべき対策や運用に関する提示/責任分界点の明確化/SLA/SLAの見直し/継続性
B	運用事項	27	プライベートSNS/リスク分析/個人情報や医療情報が含まれている場合のルール/通常の業務範囲を超える事項/アクセス権/ 誰が扱っているか明確化/職種に応じた情報が閲覧/職種が特定できないことを前提とする場合、機微な情報を流さないことを定めてあるか/SNSサービス上、保存される情報が明確になっているか/端末に関する管理ルール/端末紛失時等の対応/何をしてはいけないか、何があったら知らせないといけないかについて定義され周知されているか/教育
C	技術事項	22	ネットワークの特定/ウイルス混入等の改ざんを防止する対策/パスワード盗聴、本文の盗聴/セッション乗っ取り、IP アドレス詐称等のなりすまし/ID・PWが設定さ/暗号化/アクセス権の設定/ログを取得/アクセスログの不当な削除／改ざん／追加等防止情報を保管する場所/暗号化通信/ファイヤーウォール/利用者以外に無線LANの利用を特定できない
		70	合計項目数

オンライン診療システムの
安全管理
チェックシート

オンライン診療の適切な実施に関する指針の対象



オンライン診療の適切な実施に関する指針（厚労省）より

3.5.2 オンライ診療 システム 提供 事業者における 要求事項(クラウドガイドライン)

① 医療情報システムとの接続がある場合には、本ガイドラインの「３．２」～「３．４」の要求事項を適用する(安全管理/外部保存/利用終了)

② 患者側端末は、医療情報システムと接続する機能等を含まないこと、サービス仕様適合開示書に基づき、医療機関等と合意する。

③ オンライン診療システムを提供するクラウドサービス事業者と患者との間の責任分界について、サービス仕様適合開示書に基づき、医療機関等と合意する。

オンライン診療システム事業者が行なうべき対策（オンライン診療の適切な実施に関する指針）

２－１）共通事項

２－２）医療情報システムに影響を及ぼす可能性があるシステムの場合

- 法的保存義務のある医療情報を保存するサーバーを国内法の執行が及ぶ場所に設置すること。
- 医師（医療機関の医療情報管理責任者）に対してそれぞれの追加的リスクに関して十分な説明を行うこと。
- 医療情報を保存するシステムへの不正侵入防止対策等を講ずること。

第三者機関の認証としては以下のいずれかが望ましい。

第三者機関の認証としては以下のいずれかが望ましい

- 一般社団法人保健医療福祉情報安全管理適合性評価協会(HISPRO)、
- プライバシーマーク（JIS Q15001）、
- ISMS（JIS Q 27001 等）、ITSMS（JIS Q 20000-1 等）の認証、
- 情報セキュリティ監査報告書の取得、
- クラウドセキュリティ推進協議会のCS マークやISMS クラウドセキュリティ認証（ISO27017）の取得

オンライン診療システムの安全管理(1)

	中分類	項目
	オンライン診療システム事業者の説明責任	13
	オンライン診療システムとして備えるべき事項	7
	オンライン診療システムの利用環境に対する確認	4
	オンライン診療システム事業者における組織的対策	7
	オンライン診療システム事業者における人的対策	7
	オンライン診療システム事業者における物理的対策	3
	オンライン診療システム事業者における通信回線での対策	10
	オンライン診療システム事業者における外部からの攻撃への対策	11
	オンライン診療システム事業者におけるアクセス制御	20
	オンライン診療システム事業者におけるログに関する事項	7
	オンライン診療システム事業者におけるシステム構築・提供時の対策	4

オンライン診療システムの安全管理(2)

	中分類	項目
	オンライン診療システム事業者における運用・保守時の対策	23
	オンライン診療システム事業者が医師の代わりに患者への説明を行う場合	4
	医療情報システムと接続する場合	5
	診療計画（訪問看護指示書）を電磁的記録として保存する機能を有する場合	4
	録音・録画・撮影機能を有する場合	2
	ファイル送信、チャット機能を有する場合	5
	Personal Health Record(以下、PHR)と接続する場合	1
	例外初診が行われるシステムの場合	1
	項目数合計	138

PHRサービス事業者における
安全管理チェックシート
（作成中）

PHRサービス事業者における安全管理

- 本ガイドラインで対象とするPHRサービスは、患者が管理する医療情報（主に医療機関等が作成し、患者に提供したもの）を扱うクラウドサービス等を対象とする。
- したがって、患者自らが計測した体温、脈拍数等の情報で、医療従事者の取扱いがない情報を扱うクラウドサービス等は、本ガイドラインの対象とはしない。

PHRサービスを提供する場合における クラウドサービス事業者の責任分界の考え方

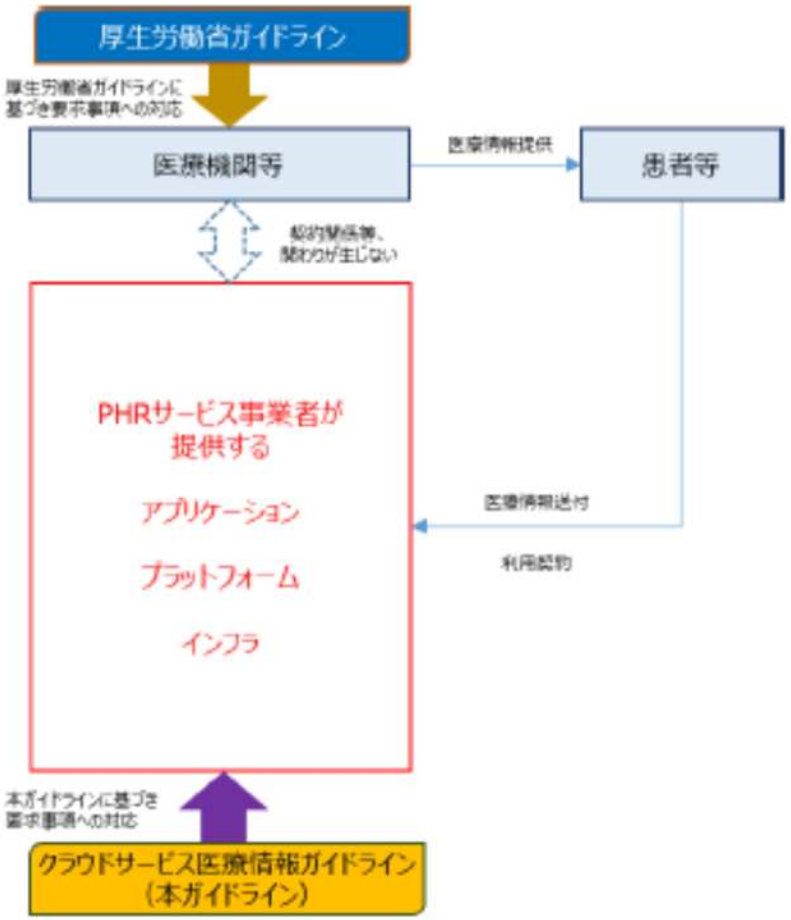


図 14　患者等が PHR サービス事業者に自らデータの送付等を行う場合

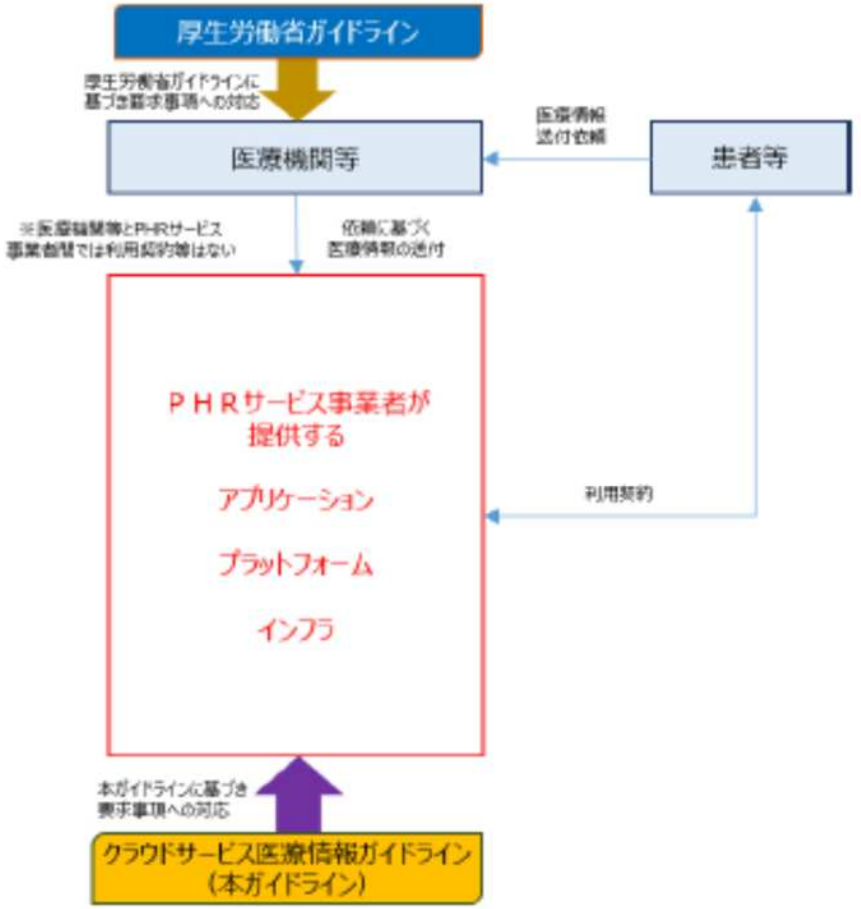


図 15　患者等の依頼で、医療機関等が患者の医療情報を送付する場合

厚生労働省　クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン第1版より

3. 6 PHRサービス事業者における安全管理対策

3.6.1 PHRサービス事業者への要求事項

読替の方針

3.6.2 PHRサービス事業者を適用対象とする要求事項

読替え

3.6.3 PHRサービス事業者を適用対象外とする要求事項

適用対象外とする項番

３．６．１ PHRサービス事業者への要求事項（１）（クラウドサービスガイドライン）

１）読み替え

- 「医療情報」→「PHRで利用する医療情報」
- 「医療機関等」→「患者等」
- 「クラウドサービス事業者」→「PHRサービス事業者」

２）TLSの設定は1.2、サーバ証明書、本人性の確認

３）2要素認証の部分を削除

４）３．３．６　外部保存を受託するPHRサービス事業者の選定基準及び情報の取扱いに関する基準

（ウ）　受託情報の解析及び第三者提供制限

受託した医療情報は、法令による場合又は患者等の指示に基づく場合を除き第三者へ（「患者本人を含め」削除）の提供禁止

３．６．１ PHRサービス事業者への要求事項（２）（クラウドサービスガイドライン）

５）以下要求事項を適用対象外とする。（続く）

３．２．１　組織的安全管理対策

関係ガイドラインの遵守/医療機関が患者の同意を得る方法

３．２．３　技術的安全管理対策

職種による権限管理/真正性の確保/アクセス記録の保存年限/応答時間の合意/保存容量管理/冗長化・毀損・見読性/IoT機器利用

３．２．４　人的安全管理対策

再委託の事前説明

３．２．５　情報の破棄

破棄記録の提出

３．２．６　情報システムの改造と保守

保守業務の実施報告/標準フォーマットの使用/保守体制・再委託の合意形成

３．６．１ PHRサービス事業者への要求事項(３)(クラウドサービスガイドライン)

５)以下要求事項を適用対象外とする。(続き)

３．２．７　機器持ち出し

BYODの禁止

３．２．８　災害時

見読性確保/ブレークグラス/国内法の執行が及ぶ範囲

３．２．９　PHRで利用する医療情報を外部と交換

ネットワーク経路の確認/責任分解の医療機関との合意

３．２．１０　法令で定められた記名押印

電子署名/タイムスタンプ

３．３．６　PHRサービス事業者の選定基準及び情報の取扱い

事業者情報の提供

受託情報の解析・分析の制限

3．6．1 PHRサービス事業者への要求事項(4)

6)PHRサービスの提供時の手順策定と実施確認(追加)

・登録時のID申請者である患者等の本人確認(実在性の確認)

・利用時の患者等の認証(利用者の本人確認)

・新たに受領した医療情報の患者等のIDとの紐づけ(患者本人情報の確認)

7)「サービス仕様適合開示書に基づき、患者等と合意する」は適用対象外とし、それらの要求事項に代えて以下を追加

・PHRサービスで取り扱う個人情報に関して、患者等からの同意の取得方法について運用管理規程を策定する。

・PHRサービスの提供終了時又は契約終了時における患者等に関する医療情報の返却の範囲、方法、条件について、患者等とあらかじめ合意する。

・患者等の指示により、医療機関等が(自ら管理する)医療情報を患者等が契約するPHRサービス事業者へ送付する場合において、PHRサービス事業者と医療機関等との責任分界について、あらかじめ患者等に示す。

・PHRサービスの提供に関する患者等との合意においては、免責事項等を定める

PHRサービス事業者における安全管理チェックシート

「民間事業者による医療情報の外部保存及びクラウドサービス」のチェックシートを基に作成予定

関連する医療機関用チェックリストおよびベンダー用開示シート

- **医療情報システムの安全管理に関するGL適合性チェックリスト（第５版対応） iMISCA発行（医療機関用）**
- **ASP・SaaS（医療情報取扱いサービス）の 安全・信頼性に係る情報開示指針（総務省）（ASPICで認定制度）**
  - サービスに関する情報開示を推進する目的
  - 項目により内容または開示の可否と可の場合はその方法を宣言
- **JAHIS「製造業者による医療情報 セキュリティ開示書」ガイド Ver.3.0a （医療情報システムの提供）**
  - 厚労省ガイドラインへの技術的適合性を示し、医療機関側で必要な運用的対策の理解を容易にする （はい・いいえによる開示）
- **サービス仕様適合開示書（総務省クラウドガイドライン 4.2）**
  - ガイドラインへの適合性、責任分界や、役割の範囲等の表示により、サービスの品質や内容を示すこと（必要な開示文章の列挙）

HISPROとは(一社)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

- システム利用者がサービスを利用する際に「医療情報システムにおける安全管理ガイドライン」に従ってシステムを評価する手助けをすること、またそれにより健全なシステム提供者が発展していただけることを目標に設立された(2018年)
- HISPROは、サービス提供事業者が医療機関等へ提供するサービスの評価をユーザーの代わりに行います
- 各種ガイドラインに適合していることを認定されたサービス名も公表し、これにより医療機関等は安全が確認されたサービスを選択することができ、サービスベンダーも指標に沿った対策案を講じることができます

HISPRO
評価マーク

HISPROで現状実施している評価

- 現在実施している評価は、下記の分類で実施している

＜サービス事業者向け評価＞

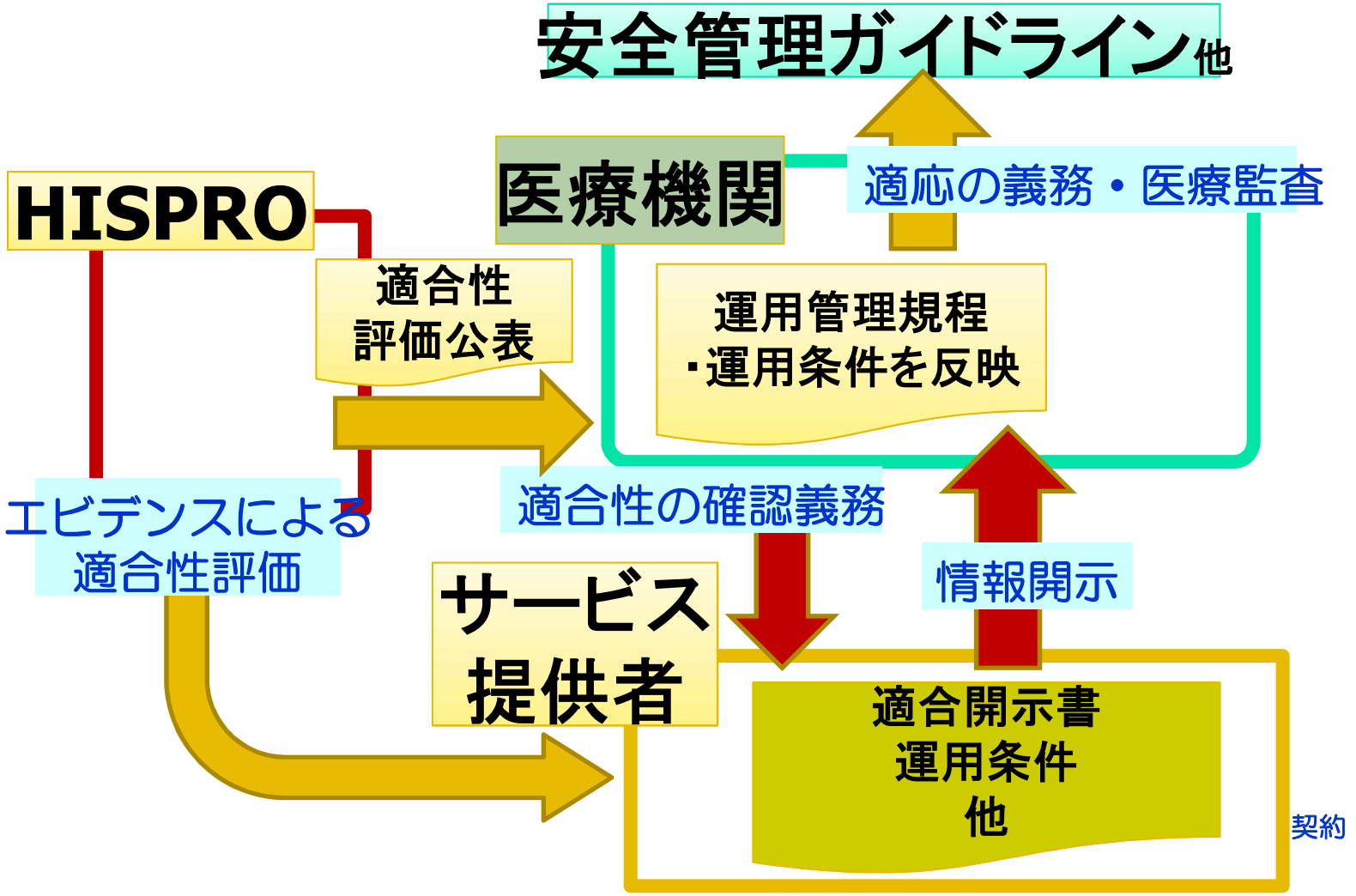
- 支払基金等へのレセプトオンライン請求用IPsec＋IKEサービス
  - サービス事業者が提供するVPN接続サービスの評価（IP-VPNは対象外）
- 民間事業者による医療情報の外部保存及びクラウドサービス
  - サービス事業者の提供するサービスにおける、総務省ガイドライン、経産省ガイドラインへの対応について評価

・オンライン診療システムの厚生労働省指針への適合性の評価

＜運営主体向け評価＞

- 地域医療介護連携サービスの安全管理
  - 地域医療介護連携において、運営主体が適切な管理を行って運営しているかを評価
- SNSサービス利用の安全管理
  - SNSを利用して医療情報連携を行う際の管理体制について評価

HISPROの位置づけ



HISPROの評価作業

- 申請者から下記のような資料の提出を求める
  - 製品の概要説明書
  - 製品の評価に係る責任分界点と申請者の責任範囲の説明資料
  - 提示された内容に基づき記載されたチェックリスト
  - チェックリストに記載されている内容が正しく記載されているかのエビデンス＊
    - 特にユーザの視点で見るため、ユーザでのマニュアル、重要事項説明等資料を重点的に評価する
  - 提出された資料を基に評価を行い、疑問点等やり取りを行う
- 評価された内容について、評価委員会、理事会で審議し、適合性評価結果を公表する

- 利用者にガイドライン適合性を示す資料は、開示資料であることを基本とする。

＊法的要請への適合性を示す文書類は開示が基本

ガイドラインでの“HISPRO”への言及

ソフトウェア型のIPsec若しくはTLS1.2により接続する場合、
セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃のリスクがあるため、適切な対策を実施すべき。
HISPROの「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」チェック項目が参考先に。（安全管理ガイドライン6.11）

SNS（Social Networking Service）利用時の留意点について記載
SNSにおいて患者の医療情報を取り扱う場合、当該サービスは医療情報システムに該当し、ガイドラインの基準を満たす必要がある。
SNSには、セキュリティが十分に確保されていないサービスもあることから、HISPROが公表している「医療情報連携において、SNSを利用する際に気を付けるべき事項」を参考に。
（安全管理ガイドライン Q&A5）

オンライン診療システム事業者が行うべき対策
２．オンライン診療の提供体制に関する事項（5）２）
オンライン診療システムは、第三者機関に認証されるのが望ましい。
第三者機関の認証としては以下のいずれかが望ましい。
HISPRO、プライバシーマーク（JIS Q15001）、ISMS（JISQ 27001 等）、ーーー。
（オンライン診療の適切な実施に関する指針（2019改定））

日本医師会報告書での言及

SNS（Social Networking Service）について

具体的な対策に関しては、HISPRO49の「医療情報連携において、SNS を利用する際に気を付けるべき事項」に、基本的な考え方、契約面・運用面・技術面での対策が記載されている。

また、「『SNS 利用時の注意事項』チェックリスト項目集」も掲載されているので、これに基づいてチェックを行い、対策を講じることを薦める。

（日医IT 化宣言2016 実現に向けた方策―地域医療連携、多職種連携のあるべき姿
平成30 年6 月　日本医師会　医療IT 委員会―）

情報通信事業者の第三者認証について

安全なオンライン診療が行われるためには、事業者が「オンライン診療ガイドライン」を遵守し、適切な運用を行っていることを確認できる仕組みが必要であり、それは国または情報通信に関するセキュリティ評価に実績のある第三者機関（HISPRO1等）において整備されるべきである。

（情報通信機器を用いた診療に関する検討委員会報告書
平成30年6月　日本医師会　情報通信機器を用いた診療に関する検討委員会）

まとめ

- 医療機関等はチェックシートの提出をサービス提供者に依頼してください
- サービス提供者は自己サービス評価にチェックシートをご活用ください
- 第三者評価が必要な場合は
  HISPROへご相談ください

e-mail: info2009vpn[a]hispro.or.jp
（メール送信の際には、[a]を＠として下さい）