別紙４

# 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について

平 成 ３ ０ 年 ５ 月

情報流通高度化推進室

# 医療情報システムのセキュリティに関するガイドラインの全体像

医療情報システムのセキュリティについては、**厚生労働省、総務省及び経済産業省が連携してガイドラインを整備**。（いわゆる３省４ガイドライン）

## 医療機関向け

・医療情報システムの安全管理に関するガイドライン　【担当：厚生労働省】
（平成17年３月～）

## 事業者向け

① 医療情報の処理等サービスをオンラインで提供する事業者向け【担当：総務省】

・ ASP・SaaSにおける情報セキュリティ対策ガイドライン（平成20年１月～）

・ **ASP・SaaS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（平成21年７月～）**

② 医療情報の外部保存を行う情報処理事業者向け【担当：経済産業省】

・ 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
（平成20年３月～）

# ３省４ガイドラインの位置づけ

**総務省の「ASP・SaaS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」を含む３省４ガイドラインについては、医政局長及び保険局長発、都道府県知事及び地方厚生（支）局長宛通達において、遵守を徹底することとされている。**

厚生労働省医政局長及び保険局長通達　　平成22年2月1日
「診療録等の保存を行う場所について」の一部改正について

外部保存通知第１に掲げる診療録等の電子媒体による外部保存については、外部保存通知第２の１及び第３に掲げる事項を遵守すること。

**特に、今回の外部保存通知の改正は**
**「医療情報システムの安全管理に関するガイドライン」**（厚労省）、
**「ASP・SaaSにおける情報セキュリティ対策ガイドライン」**(総務省)、
**「ASP・SaaS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」（総務省）　及び**
**「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」**（経産省）
**が整備されたことを前提に行うものであることから、これらのガイドラインについての遵守を徹底すること。**

※　厚生労働省医政局長及び保険局長発、都道府県知事及び地方厚生（支）局長宛通達（平成22年２月１日）「「診療録等の保存を行う場所について」の一部改正について」より抜粋

# 厚生労働省ガイドラインと総務省ガイドラインの対応関係



## 医療情報システムの安全管理に関するガイドライン（厚生労働省）

- 第1章　はじめに
- 第2章　本指針の読み方
- 第3章　本ガイドラインの対象システム及び対象情報
- 第4章　電子的な医療情報を扱う際の責任のあり方
- 第5章　情報の相互運用性と標準化について

**第6章　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 | 医療機関等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、サイバー攻撃等の非常時の対応 |
| 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 |

**第7章　電子保存の要求事項について**

| | |
|---|---|
| 7.1 | 真正性の確保について |
| 7.2 | 見読性の確保について |
| 7.3 | 保存性の確保について |

**第8章　診療録及び診療諸記録を外部に保存する際の基準**

| | |
|---|---|
| 8.1 | 電子媒体による外部保存をネットワークを通じて行う場合 |
| 8.1.1 | 電子保存の基準の遵守 |
| 8.1.2 | 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準 |
| 8.1.3 | 個人情報の保護 |
| 8.1.4~8.4.1 | （略） |
| 8.4.2 | 外部保存契約終了時の処理について |
| 8.4.3 | （略） |

- 第9章　診療録等をスキャナ等により電子化して保存する場合について
- 第10章　運用管理について

7.1～7.3は関連箇所に統合

## 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（案）（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の処理を行う際の責任等
- 第3章 安全管理に関するクラウドサービス事業者への要求事項

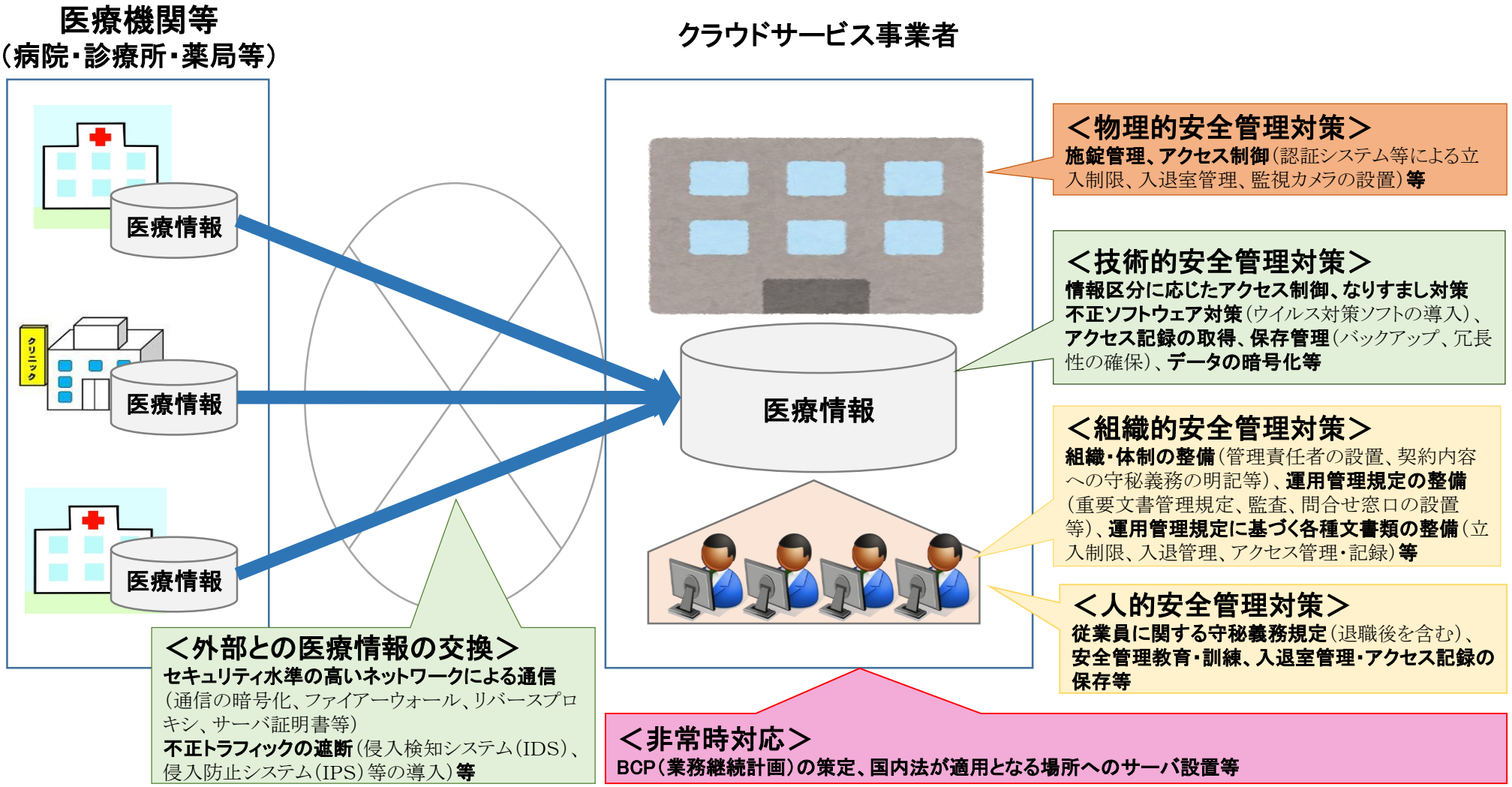
| | |
|---|---|
| 3.1 | 本章の読み方 |
| 3.2 | 医療情報サービスに求められる安全管理に関するクラウドサービス事業者への要求事項 |
| 3.2.1 | 組織的安全管理対策 |
| 3.2.2 | 物理的安全管理策 |
| 3.2.3 | 技術的安全管理策 |
| 3.2.4 | 人的安全管理対策 |
| 3.2.5 | 情報の破棄 |
| 3.2.6 | 情報システムの改造と保守 |
| 3.2.7 | 情報および情報機器の持ち出しについて |
| 3.2.8 | 災害等の非常時の対応 |
| 3.2.9 | 外部と個人情報を含む医療情報を交換する場合の安全管理 |
| 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 |
| 3.3 | 外部保存におけるクラウドサービス事業者への要求事項 |
| 3.3.1～3.3.4 | ・真正性の確保におけるクラウドサービス事業者への要求事項<br>・見読性の確保におけるクラウドサービス事業者への要求事項<br>・保存性の確保におけるクラウドサービス事業者への要求事項<br>→　厚生労働省ガイドラインに関する解説のみ |
| 3.3.5 | 外部保存におけるクラウドサービス事業者への要求事項 |
| 3.4 | クラウドサービスの提供終了におけるクラウドサービス事業者への要求事項 |
| 3.5 | 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 |

新設

- 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SLA参考例及びサービス仕様適合開示書

# 総務省ガイドラインが求めるセキュリティ対策（全体像）

総務省ガイドラインでは、厚労省ガイドラインにおける医療機関側への要求事項を踏まえ、**クラウドサービス事業者が実施すべき総合的な対策**（組織的安全管理対策、物理的安全管理対策、技術的安全管理対策、人的安全管理対策、外部との医療情報の交換、非常時対応等）**を規定**。



# 総務省ガイドラインの改定について



**クラウドやスマートフォンの普及などの技術的進展、地域医療連携やPHR、オンライン診療などの医療情報の利用シーン拡大等を踏まえ、医療情報を取り扱うクラウドサービス事業者向けのセキュリティ対策にかかるガイドラインを改定。**

※ 名称を「ASP・SaaS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」から「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」に変更予定。

## 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章 本ガイドラインの前提条件及び読み方**

主にガイドラインの対象・目的・読者等を定義

**第２章クラウドサービス事業者が医療情報の処理を行う際の責任等**

クラウドサービス事業者が、医療情報の取り扱いに関して受託する際に生じる責任や、医療機関等との責任分界の考え方を記述

**第３章 安全管理に関するクラウドサービス事業者への要求事項**

厚労省ガイドラインの各要求事項に従って、クラウドサービス事業者における要求事項を、クラウドサービスにおける情報セキュリティ対策ガイドラインの内容を踏まえて記述

**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**

第3章の要求事項のうち医療機関と事業者間で合意すべき事項について、合意形成の進め方などについて記述

**（別添）ガイドラインに基づくSLA参考例及びサービス仕様適合開示書参考例**

ガイドラインに基づくSLA（Service Level Agreement）参考例、サービス仕様適合開示書の雛形を掲載

## 【主な改正点】

● **医療情報連携ネットワーク（EHR）の位置付けの明確化**

○ EHR運営団体が、EHR参加施設の医療情報を管理する責任を有する場合には、クラウドサービス事業者とされることを明確化

● **オンライン診療サービスの位置付けの明確化**

○ オンライン診療の適切な実施に関する指針（平成30年3月厚生労働省）の策定を踏まえ、位置づけを明確化

● **PHRサービス（Personal Health Record：個人の医療情報を自身の健康管理等に活用するサービス）の位置付けの明確化**

○ ガイドラインの対象となるPHRを定義（個人による医療情報の管理）

○ 医療機関・個人間の責任分界点（責任範囲）の明確化

○ PHRサービス事業者が対応すべきセキュリティ対策（利用者認証、ウィルス対策等）を明確化

● **医師等がスマートフォン等のモバイル端末で医療情報を取り扱う際の要求事項を整理**

○ モバイル端末へのアプリケーションインストールの制限やデータ暗号化、公衆無線LANの利用禁止等を規定

● **サービス仕様適合開示書の策定**

○ クラウドサービス事業者が自社の安全管理措置、提供条件等のガイドライン適合状況を自主的に医療機関等に示すひな形を規定

# 【参考】サービス仕様適合開示書参考例（抜粋）

巻末　サービス仕様適合開示書　サンプル例

※（例）と記載して有るものは、記入の例として示したものである。

（１）　組織的対応（3.2.1）

① 組織的取組における基本方針（（２）(ウ)1.⑥）

(a) 当社における情報セキュリティに関する組織体制

| 情報セキュリティに関する役職 | 有無(在る場合には役職または氏名) |
|---|---|
| 情報システム責任者 | |
| 本サービスに関する管理責任者 | |
| 本サービスのシステムに関する運用管理責任者 | |

(b) 当社における個人情報保護指針、プライバシーポリシー等について

| 策定の有無(有の場合には文書名) | 内容の開示の有無及び開示されている場合の開示方法 | プライバシーポリシー等の遵守上、顧客側に求める対応 |
|---|---|---|
| | | |

(c) 当社における個人情報保護法及び個人情報保護委員会が定めるガイドライン等への遵守状況

| サービス提供に際して遵守している個人情報に係る法令、ガイドライン・ガイダンス |
|---|
| *・個人情報保護法及び同施行令、施行規則（例）* |
| *・個人情報の保護に関する法律についてのガイドライン（通則編、外国にある第三者への提供編、第三者提供時の確認・記録義務編）【個人情報保護委員会】（例）* |
| *・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1.0版【総務省】（例）* |
| *・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】（例）* |
| *※　なお、下記のガイドライン、ガイダンスについても、クラウドサービス事業者として対応しております。* |
| *・医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス【厚生労働省】（例）* |
| *・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【厚生労働省】（例）* |

(d) 当社における情報セキュリティポリシー、セキュリティ規程、運用管理規程等の策定状況

| 策定の有無及び策定している文書 | 内容の開示の可否及び開示条件、提供方法 |
|---|---|
| *情報セキュリティポリシー（例）* | |
| ・・・・・・ | |

② サービス提供に係る体制等に関する情報の開示（（２）(ウ)2.②）

再委託先のクラウドサービス事業者の有無・事業者名・再委託先クラウドサービス事業者との契約種別（（２）(ウ)2.②）

保守・運用に関する再委託事業者の有無・管理体制（（２）(ウ)2.②）

(a) 本サービス提供に係るサービス提供体制

| 部門 | 役割 |
|---|---|
| *本サービス提供を行う責任部門（例）* | *電子カルテ事業部（例）* |
| *顧客問い合わせ対応部門（例）* | *コールセンター事業部（例）* |

(b) サービス提供に係る再委託の状況

| 再委託事業者の有無(在る場合には事業者名) | 再委託事業者がある場合には、再委託業務内容 |
|---|---|
| *○×株式会社（例）* | *サービス提供用システム保守（例）* |
| ・・・・・ | |

③ 管理する医療情報の管理状況に関係する資料の提供（（２）(ウ)3.④）

| 資料提供の可否 | 内容の開示の有無及び開示する場合の開示方法・条件・範囲 |
|---|---|
| | |

④ サービス提供に係る運用管理規程の開示等の有無、範囲、条件等

（（２）(ウ)3.③）

| 資料提供の可否 | 内容の開示の有無及び開示する場合の開示方法・条件・範囲 |
|---|---|
| | |

⑤ 受託する医療情報に係るリスク分析の結果と対応措置（（２）(ウ)4.②）

(a) 受託する医療情報に係るリスク分析の概要

| リスク分析の結果、脆弱性に関す | 脆弱性に対する対応の概要 |
|---|---|

# 「ASP・SaaS・クラウド事業者が医療情報を取り扱う際の安全管理に関する検討委員会」構成員名簿（平成29年8月～）

## 委員

| | |
|---|---|
| 山本　隆一【主査】 | （一財）医療情報システム開発センター　理事長 |
| 宮内　宏 | 宮内・水町IT法律事務所　弁護士 |
| 矢野　一博 | （公社）日本医師会総合政策研究機構　主任研究員 |
| 玉川　裕夫 | （公社）日本歯科医師会嘱託（情報管理担当） |
| 河野　行満 | （公社）日本薬剤師会　中央薬事情報センター<br>医薬情報管理部　部長 |
| 茗原　秀幸 | （一社）保健医療福祉情報システム工業会<br>医療システム部会セキュリティ委員会　委員長 |
| 渋谷闘志彦 | 総務省　情報流通行政局　情報流通高度化推進室長 |
| 河合　輝欣 | （特非）ASP・SaaS・IoT クラウドコンソーシアム　会長 |

## オブザーバー

| | |
|---|---|
| 坂野　哲平 | ㈱アルム　代表取締役社長 |
| 園田　勝一 | ㈱NTTデータ　第二公共システム事業本部<br>ヘルスケア事業部長 |
| 山本　拓真 | ㈱カナミックネットワーク　代表取締役社長 |
| 鳥居　幹大 | ㈱セールスフォース・ドットコム　ヘルスケア・ライフサイエンス業界担当　ディレクター |
| 松山　征嗣 | トレンドマイクロ㈱　業種営業推進グループ |
| 石山　敏昭 | 日本電気㈱　医療ソリューション事業部　シニアエキスパート |
| 河合　敏充 | ㈱日立製作所　スマート情報システム統括本部　担当部長 |
| 辻元　洋典 | 富士通㈱　ヘルスケア事業本部　マネージャー |
| 佐山　国央 | ㈱ワイズマン　営業本部　担当部長 |

## オブザーバー（関係省庁）

| | |
|---|---|
| 山路　栄作 | 内閣官房　情報通信技術（IT）総合戦略室　参事官 |
| 笹子宗一郎 | 厚生労働省　政策統括官付情報化担当参事官室　政策企画官 |
| 和泉　憲明 | 経済産業省　商務情報政策局　情報産業課　企画官 |

# 「ASP・SaaS・クラウド事業者が医療情報を取り扱う際の安全管理に関する検討委員会」スケジュール

想定

| 第1回<br>2017<br>8/30 | 第２回<br>2017<br>10/25 | 第3回<br>2017<br>11/29 | 第4回<br>2017<br>12/20 | 第5回<br>2018<br>3/13 | 第6回<br>2018<br>5/15 |
|---|---|---|---|---|---|
| ・ 検討の進め方<br>・ ASP・SaaS事業者医療情報ガイドラインにおける改定対象等<br>・ベンダー各社におけるガイドライン等の活用状況等 | ・ クラウドサービスを利用した新しい論点への対応（PHR，モバイル，地域医療連携等）に関する有識者によるプレゼンテーション<br>・ ASP・SaaS事業者医療情報ガイドラインの改定イメージの提示 | ・ ASP・SaaS事業者医療情報ガイドラインの改定検討結果の報告<br>・ SLA参考例の改定箇所の整理 | ・ ASP・SaaS事業者医療情報ガイドラインの改定案（素案）<br>・ SLA参考例の改定案（素案） | ・ ASP・SaaS事業者医療情報ガイドラインの改定案<br>・ SLA参考例の改定案 | ・ ASP・SaaS事業者医療情報ガイドラインの改定案（オンライン診療指針反映版）<br>・ SLA参考例の改定案 |

5月22日～6月21日：パブコメ実施

※

7月初旬：ガイドライン公表

※必要に応じて公表前に第７回を開催（６月最終週～７月第一週）