| 中医協　材－２ |
| --- |
| 元．８．７ |

# 中央社会保険医療協議会
# 保険医療材料専門部会
# 意見陳述資料
# 医療機器・医療技術

2019年8月7日

（一社）日本医療機器産業連合会（JFMDA）

（一社）米国医療機器・IVD工業会（AMDD）

欧州ビジネス協会（EBC）医療機器・IVD委員会

# 本日の提案内容

1. 医療機器（医療技術）イノベーション評価について
   使用実績を踏まえた評価：C2チャレンジ申請
   ･･･ 3 ～ 4頁

2. 安全確保を推進するために
   オンライン診療におけるサイバーセキュリティーへの対応について
   ･･･ 5 ～ 9頁

3. ICTを用いた医療技術の基盤整備のために
   医療画像情報のクラウド化の促進に向けて
   ･･･ 10頁

# 1．医療機器（医療技術）イノベーション評価について
## 使用実績を踏まえた評価：C2チャレンジ申請

**【背景・現状】**

① 特定保険医療材料においては2018年度改定でチャレンジ申請が認められ、制度整備に向けた議論が行われている。

② 一方企業が新規医療技術の導入に取り組む場合も、患者へイノベーションを一早く届ける観点から、その時点の限られたエビデンスで一旦市場導入するケースがある。
その後、市場で新たな有用性がエビデンスをもって示された場合、医療技術の見直しは学会からの医療技術評価提案書をもとに行われているところ。

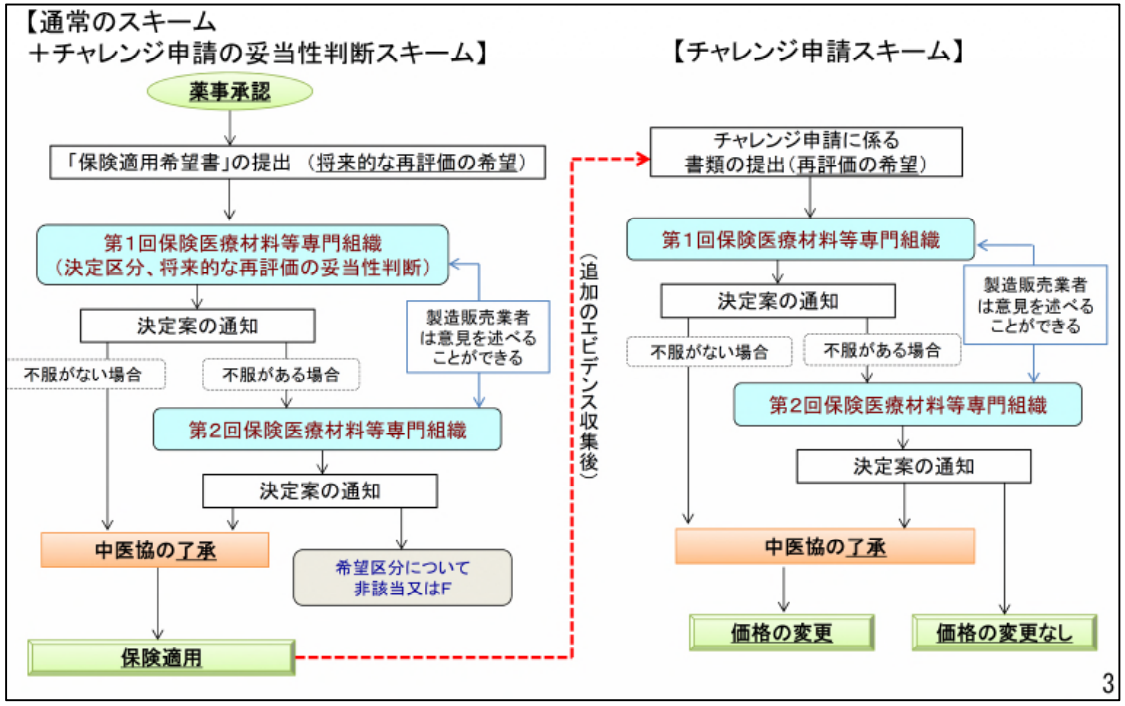
③ 医療技術評価において、医療機器の安定供給、革新性評価等について、一層対応が可能な新たな評価制度を導入することで、患者へのさらなるイノベーション還元が図れることが期待できる。

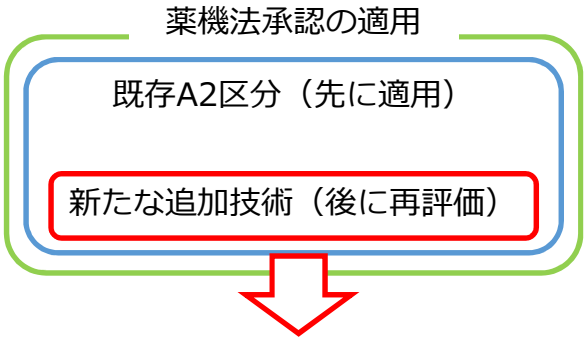
**【提案】**

① 特定保険医療材料と同様に、医療技術に関してチャレンジ申請を制度化。

② 早期導入を可能としながらも、安定供給や新たな評価への期待を反映することが可能な制度を構築。

# 1．医療機器（医療技術）イノベーション評価について
## 使用実績を踏まえた評価：C2チャレンジ申請




《出典：中央社会保険医療協議会保険医療材料専門部会（第100回）資料より抜粋 》

例えば、薬機法承認を得た新たなアプリケーション技術等を含む場合において、当該新技術部分について、後にC2区分保険適用希望の可能性があることを申告した上で、一旦A2区分で上市後、使用実績を踏まえて再評価が出来るスキームを設けてはどうか。

# 2. 安全確保を推進するために
# オンライン診療におけるサイバーセキュリティーへの対応について

【背景・現状】

① レセプトのＩＴ化等の**医療ＩＴ化の集中的推進**のため、2006年度改定で**「電子化加算」**が時限的に設定され、**2010年度改定で廃止**された。

② **サイバーセキュリティへの対応**として策定・公表された「医療情報システムの安全管理に関するガイドライン第１版」は、**2010年度以降も改版**が続いている。

③ **産業界**も、ガイドラインの改定にあわせて「製造業者による医療情報セキュリティ開示書」を策定・更新するなど、**医療機関のサイバーセキュリティ管理を支援**している。

④ 近年のサイバー攻撃による重大な問題発生等から、2017年5月の**ガイドライン第5版**では**極めて幅広い対応**が求められる改定がなされ、**医療機関は規模の大小に関わらず**医療サービスとは**専門性の異なる高い技術**が要求されている。

⑤ 2018年度改定で**オンライン診療**やオンライン医学管理料が保険収載され、**外部の情報通信機器との接続機会の増加**など、さらにサイバーセキュリティ管理の重要性が増している。

【提案】

① **外部の情報通信機器が接続されるオンライン診療を安全に普及させるため**に、患者の要配慮個人情報の漏洩防止、および医療機器や医療情報システム内の情報の保護など**継続的に必要なサイバーセキュリティ管理**を行うのに必要不可欠な専用スタッフや外部委託その他の費用を手当てするための**診療報酬上の評価**

【参考データ】

① サイバー攻撃によって患者の要配慮個人情報の漏洩、診療継続不能などが発生した事例（各種Webサイト情報等）

② オンライン診療への要求事項とセキュリティ対策の現状（「オンライン診療の適切な実施に関する指針の見直しに関する検討会」第4回 資料3 等）

③ 産業界の対応状況（セキュリティ開示書の策定・更新と啓発活動)

# サイバーセキュリティの脅威に関する事例

● **医療サービス提供不能（医療機器や医療情報システムの使用不能）、患者の要配慮個人情報の漏洩などが発生している。**

## ■ 諸外国における事例（一例）

| 事象 | 概要 |
|---|---|
| **米国の430床以上の病院で院内のネットワークがランサムウェアに感染したケース** | ・2016年2月5日、ロサンゼルスのハリウッド長老教会派医療センターのNWに不正アクセスがあり、ランサムウェアが院内中のPCに感染してPCを使用する全業務が遂行不能に。<br>・12日間、電話やFAXでの連絡、メモによるカルテ記載、患者への検査結果の手渡しなどで対応しその間解決を図ったが解決不能、ハッカーの要求通り身代金を(約192万円)を支払いシステムを復旧した。 |
| **米国で院内システムがハッキングを受け、患者情報や医療情報が漏洩したケース** | ・ハッカーがリモートデスクトッププロトコル(RDP)の脆弱性を利用して入手した655,000件以上の医療記録をダークウェブ上で販売。<br>・ミズーリ州の医療施設より48,000件、米国中央～中西部の施設より21万件、ジョージア州の施設より397,000件を取得、10万ドル分のデータを売却。 |
| **米国で医療機器がランサムウェアに感染したケース** | ・WannaCryランサムウェアの感染が世界中に広がった際、米国のとある病院でバイエル社の医療機器が感染した画像がヘルスケア業界筋より提示された。<br>・バイエル社は、２件の顧客から報告を受けたこと、双方とも24時間以内に復旧したことを明らかにし、Windowsベースの機器に対してまもなくMicrosoftのパッチを送り病院のITセキュリティチームと連携して同社のパワーインジェクタのサポートを継続すると発表した。 |

## ■ 本邦における事例（一例）

| 事象 | 概要 |
|---|---|
| **病院のサーバが外部から不正侵入され、IDが不正取得されたケース** | ・2016年9月7日、香川県と茨城県の高校生各１名が滋賀県の病院のサーバに侵入、不正アクセス禁止法違反の疑いで逮捕された。<br>・ハッキングの手口の１つ「SQLインジェクション」で侵入。<br>・動機は「個人情報を盗み、お金にしようとした」。 |
| **国立大学附属病院で医療用端末がウィルスに感染、個人情報漏洩が疑われるケース** | ・2017年3月15日、ログ解析用ソフトで医療用端末を解析したところ、医療用端末がウィルスに感染し、外部と不正な通信を行っていたことが判明。<br>・感染した端末には患者１名分ずつの個人情報が含まれており漏洩した可能性がある。 |

# 外部と接続するオンライン診療への要求事項

● 外部と医療情報システムを接続するオンライン診療を行う場合は、医療情報安全管理関連ガイドラインに従い、情報セキュリティマネジメントシステム(ISMS)の導入・運用管理が求められている。

## ■ オンライン診療の適切な実施に関する指針の要求事項

「医療情報システムと接続するケース」

医療機関が**オンライン診療システムと電子カルテシステム等を接続**し、医師がシステム内の医療情報を確認しながら診療を実施する場合や、患者側に検査結果等を表示しながら診療を行う場合は、**医療情報安全管理関連ガイドラインに沿った対策を行うことが必要**である。

出典：オンライン診療の適切な実施に関する指針 P.22

## ■ 医療情報安全管理関連ガイドラインの要求事項

「**最低限のガイドライン(抜粋)**」

5.　運用管理規程等において次の内容を定めること。
(a) 理念（基本方針と管理目的の表明）
(b) 医療機関等の体制
(c) 契約書・マニュアル等の文書の管理
(d) リスクに対する予防、発生時の対応の方法
(e) 機器を用いる場合は機器の管理
(f) 個人情報の記録媒体の管理（保管・授受等）の方法
(g) 患者等への説明と同意を得る方法
(h) 監査
(i) 苦情・質問の受付窓口

(中略)

**常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとる**こと。また、その**対策の有効性・安全性の確認・維持**（例えばパターンファイルの更新の確認・維持）を行うこと。

出典：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
P.45～46、P.56

# 外部と接続するオンライン診療のセキュリティの現状

- 全体の９８%(165/169)で、外部と医療情報システムを接続してオンライン診療が行われているとの報告がある。
- 外部と接続するオンライン診療を行う場合に要求される、「最低限のガイドライン」が守れないリスクを示唆する報告がある。

## ■ サイバーセキュリティ対策の現状

### 概要　オンライン診療に関するアンケート（医師向け）

**背景**

第一回の検討会において、オンライン診療の実態について調査する必要があるという意見があった。今回、厚生労働省は、急遽、オンライン診療研究会に実態把握のためのアンケート調査を、日本オンライン診療研究会に依頼をしとりまとめを行った。

**○調査対象**

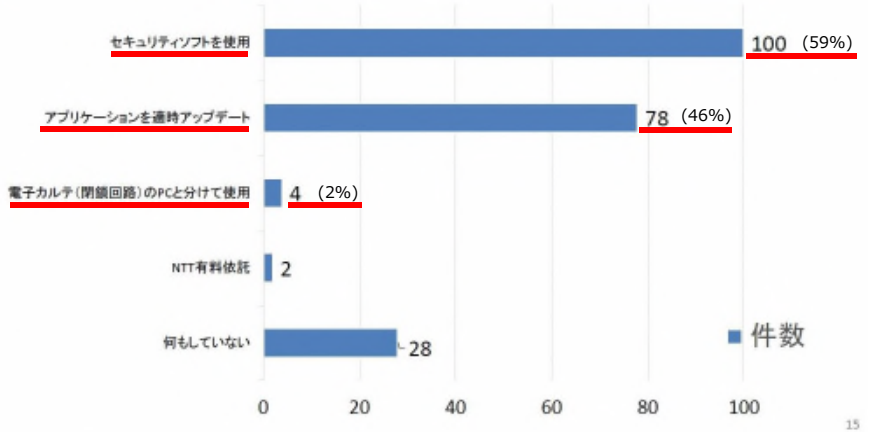
- 実際にオンライン診療を実施している医師
- 回答者数１６９人

**○調査期間**

- ２０１９年1月２８日（月）～2月１８日（月）

### セキュリティ対策として実施していることは何ですか。（複数回答）

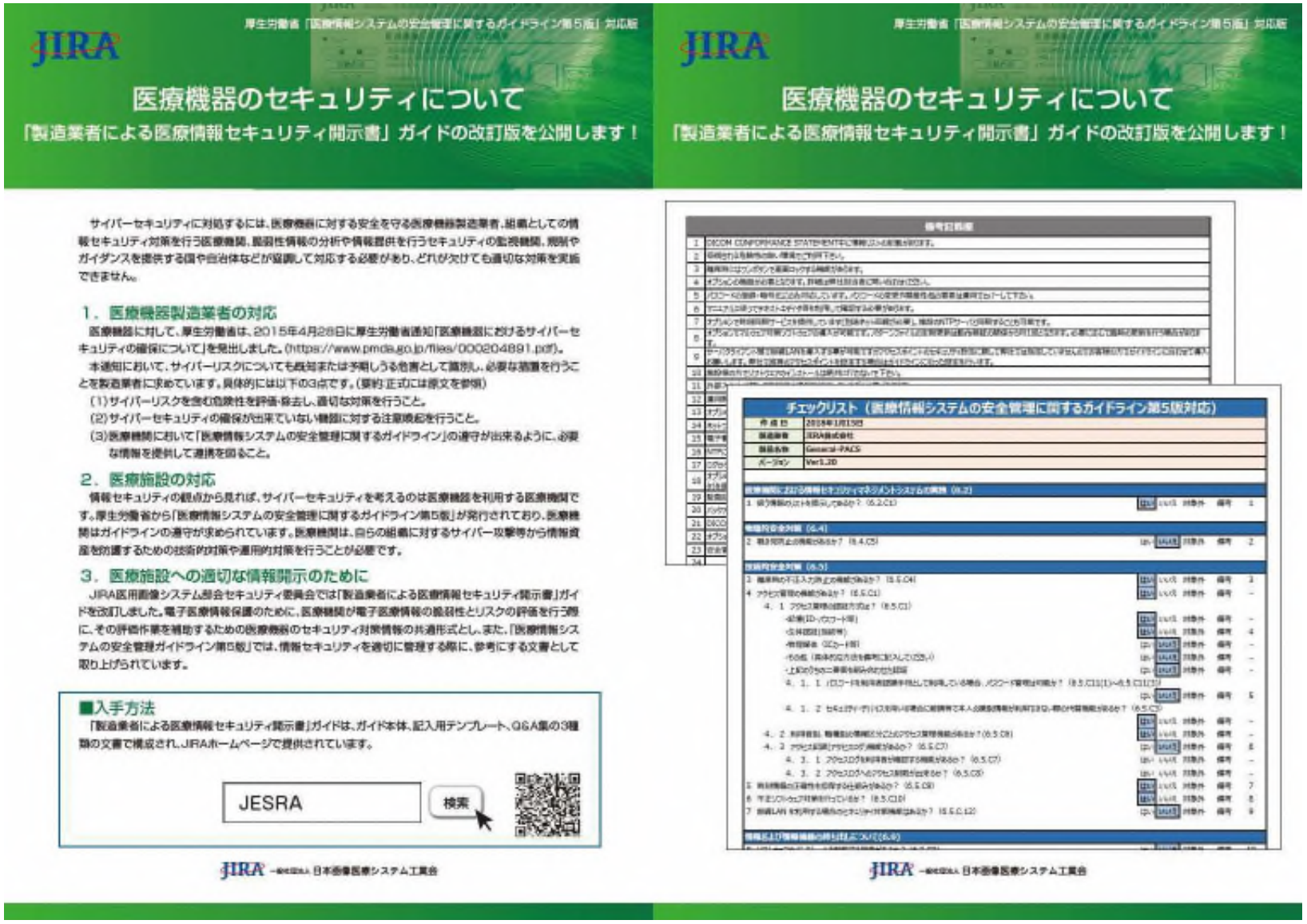
「セキュリティソフトを使用」が100件で最も多く、次いで、「アプリケーションを適時アップデート」が78件となっている。




出典：厚生労働省Webサイト「オンライン診療の適切な実施に関する指針の見直しに関する検討会」第４回　資料３
https://www.mhlw.go.jp/content/10803000/000504416.pdf

# セキュリティ開示書の策定・更新と啓発活動

● 産業界は、ガイドラインの改定にあわせて「製造業者による医療情報セキュリティ開示書」を策定・更新するなど、医療機関のサイバーセキュリティ管理を支援し、情報開示の啓発を図っている。

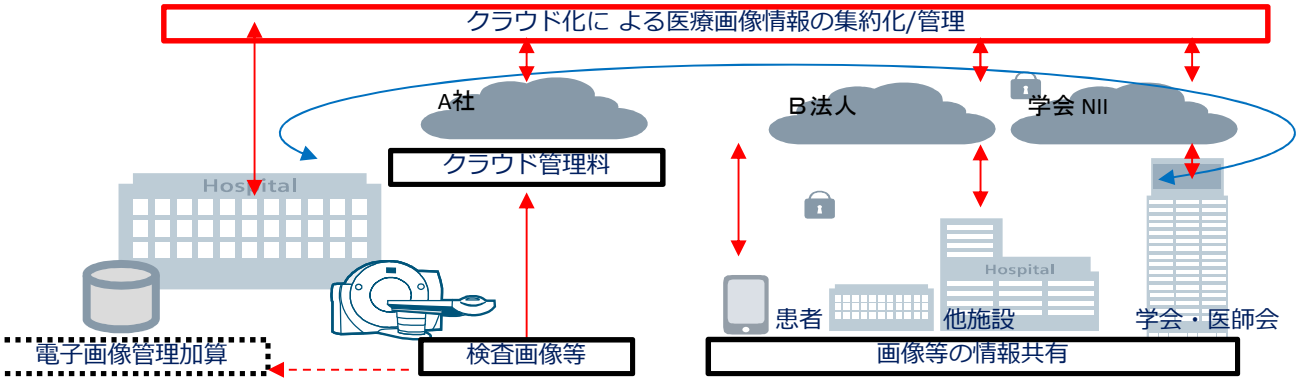


# 3. ICTを用いた医療技術の基盤整備
## 医療画像情報のクラウド化の促進に向けて

【現状】
① 2008年フィルムによるアナログ保存管理から電子保存による電子画像管理加算は、診療報酬上でも評価がおこなわれている。（保医発第0305003号 平成20年３月５日）
② 震災時等に診療画像情報の院内保存のデータは消失し、クラウド化の必要性の認識が広がっている。(1)
③ 診療画像情報の活用モデルがクラウド化技術により拡大している。(2)
④ 2011年より米国ではクラウド化したデータをACR(米国放射線医学会)による線量管理が実施されている。(3)
⑤ 本邦でも、日本医学放射線学会が、AI診断を目的とした診断用画像の精度管理や被ばく線量管理のデータベース（J-MID）化が行われている。(4)
⑥ 本邦はクラウド化が大幅に遅れている。(5)

【提案】
① 外部保存が制度化(6)されたが、診療報酬上の電子画像管理加算を請求するうえで医療機関の多くは、院内保存を前提としている。クラウド化（接続）を促進し、維持管理する為には、新たな評価が必要。例えば「クラウド画像安全管理加算」等。

【効果】
① 医療画像データのヘッダー情報をレジストリデータとしてアップロードし、「被ばく情報」を管理することで、医療機関毎の被ばく量が透明化され、標準化が進み、患者へ安全で質高い検査が促進される。
② 患者の医療機関間の画像情報授受、災害・緊急時のバックアップが期待される。




(1)災害時と震災後の医療IT体制そのグランドデザイン
(2)内閣府官民データ活用推進基本計画実行委員会 データ流通・活用ワーキンググループ医療・健診・ヘルスケアデータの 流通・活用の事例について2018年11月13日
(3)Joint Position Statement on the IAEA Patient Radiation Exposure Tracking
(4)AMEDによる診療画像データベース構築：
(5)日本企業のクラウド移行、世界より遅れているが前進中 2018/9/12 日経新聞
(6)医政発0201 第2 号保 発0201 第1 号平成２２年２月１日