ページ	項目	原記述	ご意見等	考え方
14	2．3．1 (1)②	… ASP・SaaS事業者は以下の責任を負わなくてはならない。 ・提供サービスの仕様及び運用、セキュリティ対策に関する文書化 ・提供するサービスの仕様及び提供する品質に関する説明及び必要な情報提供 ・サービス提供に関する監査等情報提供	【意見】 以下の責任に 『・適切な情報提供義務・説明義務を委託契約に含めること』 を追加して下さい。 【理由】 本件は厚労省ガイドラインで病院側に受託者との契約に含むあるいは明記するとされている項目です。本ガイドラインにおける両者合意の場合明記する項目に含まれると事業者と争いになった場合病院側は厚労省ガイドラインを遵守することが不可能になることが想定されます。 【個人】	ご指摘の内容は、第2章及び第3章の各記述の内容に包含されていると考えております。
15	2．3．1 (3)②	… ASP・SaaS事業者は以下の責任を負わなくてはならない。 ・医療機関等の管理者に対する最終的な管理責任者の明確化 ・個人情報保護管理を含むサービス提供体制の明確化 ・サービス提供に関する運用等の定期的な報告 ・医療機関等の管理者からの問合せ等に対して、一元的に対応できる体制の構築	【意見】 以下の責任に 『・医療機関等の管理者が、委託先事業者の管理の実態を理解するため、その監督を適切に行うための仕組みを作ることを契約事項に含める』 を追加して下さい。 【理由】 本件は厚労省ガイドラインで病院側に受託者との契約に含むあるいは明記するとされている項目です。本ガイドラインにおける両者合意の場合明記する項目に含まれると事業者と争いになった場合病院側は厚労省ガイドラインを遵守することが不可能になることが想定されます。 【個人】	ご指摘の内容は、第2章及び第3章の各記述の内容に包含されていると考えております。
16	2．3．1 (2)②	… ASP・SaaS事業者は以下の責任を負わなければならない。 ・サービス提供改善及びセキュリティ向上の必要性についての定期的なレビュー結果の報告	【意見】 以下の責任に 『・当該システムの運用管理の状況を定期的に監査し、問題点を洗い出し、改善すべき点があれば改善していく責任の分担、また、情報保護に関する技術進展に配慮した定期的な再評価・再検討について委託先事業者との契約事項に含める』 を追加して下さい。 【理由】 本件は厚労省ガイドラインで病院側に受託者との契約に含むあるいは明記するとされている項目です。本ガイドラインにおける両者合意の場合明記する項目に含まれると事業者と争いになった場合病院側は厚労省ガイドラインを遵守することが不可能になることが想定されます。 【個人】	ご指摘の内容は、第2章及び第3章の各記述の内容に包含されていると考えております。
17	2．3．2 (1)②	… ASP・SaaS事業者は以下の責任を負わなければならない。 ・緊急時における医療機関の管理者に対して提供する情報内容、役割分担等の明確化 ・サービス提供状況に関する記録を収集、緊急時の報告体制の構築 ・媒体管理及び機器の管理等に関する手順の明確化及び緊急時の報告体制の構築 ・緊急時に備えたアクセス制御等の手順等の明確化	【意見】 以下の責任に 『・説明責任についての分担を契約事項に含める』 を追加して下さい。 【理由】 本件は厚労省ガイドラインで病院側に受託者との契約に含むあるいは明記するとされている項目です。本ガイドラインにおける両者合意の場合明記する項目に含まれると事業者と争いになった場合病院側は厚労省ガイドラインを遵守することが不可能になることが想定されます。 【個人】	ご指摘の内容は、第2章及び第3章の各記述の内容に包含されていると考えております。

ページ	項目	原記述	ご意見等	考え方
19	2．3．2 (2)②	… ASP・SaaS事業者は以下の責任を負わなければならない。 ・情報事故等が発生した場合の原因追及に必要な情報の提供の範囲、条件等の合意、及びその実施 ・善後策として講じる対応策等の提案 ・情報事故が発生した場合の損害賠償責任に関する合意	【意見】 以下の責任に 『・委託契約に、医療機関等と受託する事業者が協力して原因を追及し明らかにすること、そして再発防止策を講ずることの措置を優先させることを明記する ・委託契約に損害填補責任の分担を明記する』 を追加して下さい。 【理由】 本件は厚労省ガイドラインで病院側に受託者との契約に含むあるいは明記するとされている項目です。本ガイドラインにおける両者合意の場合明記する項目に含まれると事業者と争いになった場合病院側は厚労省ガイドラインを遵守することが不可能になることが想定されます。 【個人】	ご指摘の内容を踏まえて、下記のように修正いたします(P19)。 「・情報事故が発生した場合の損害賠償責任に関する合意」 →「情報事故が発生した場合の損害填補責任に関する合意」
19	2．4	ASP・SaaSにより医療情報を処理する場合に、第三者認証等を取得して、マネジメントシステムの上で運用することは、医療機関等の管理者が管理責任や説明責任を果たす際、システムや運用状況を客観的に把握できるようにするため、非常に有効な手段であると考えられる。	【意見】 当面ASP・SaaSが必要な病院は医療・情報両分野に精通したスタッフが居ない中小規模病院・診療所です。彼らに詳細な合意事項の有効性を検証させるのは無理があると考えます。第三者認証を取得している場合の合意については簡便化する方向があっても良いと思います。差別化をお願いします。 【個人】	ご指摘の内容は、今後の見直しの際の参考とさせていただきたいと存じます。
20～117	第3章(全体)	―	【要旨】 厚労省のガイドラインでは“B.考え方”を参照した上で、“C.最低限のガイドライン”、“D.推奨されるガイドライン”に対応することになっているため、本ガイドラインの利用者が、厚労省のガイドラインと本ガイドラインの対応付けについて判りやすくするために、本ガイドラインが厚労省のガイドラインの“B.考え方”で関係する箇所について取り込んだ内容と趣旨を概要部分へ記載し、“ASP・SaaS事業者への要求事項”に “B.考え方”が判るように反映するべきではないか。 【意見】 全体的に厚労省のガイドラインにおける“C.最低限のガイドライン”、“D.推奨されるガイドライン”しか参照しておらず、“B.考え方”を理解した上で要求事項に反映する必要がある。 【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】	ご指摘の内容は、今後の見直しの際の参考とさせていただきたいと存じます。
20	第3章(タイトル)	第3章 安全管理に関してASP・SaaS事業者への要求事項	【案】 第3章 安全管理に関してASP・SaaS事業者への要求事項 【意見】 章のタイトルは“安全管理に関するASP・SaaS事業者への要求事項”ではないか。 【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】	ご指摘の内容を踏まえて、下記のように修正いたします(P20)。 「第3章 安全管理に関してASP・SaaS事業者への要求事項」 →「第3章 安全管理に関するASP・SaaS事業者への要求事項」

ページ	項目	原記述	ご意見等	考え方
25	3．2．1 （2） 表 3-1 最低限4	・自社で定める個人情報保護指針等に基づいて、委託業務を実施する旨を、契約内容に含めること。 ・自社で定める個人情報保護指針等が、医療機関等が求める内容を含むものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	【意見】 厚労省ガイドライン第4章において委託契約に含める、あるいは明記することが必要である。となっている項目について本ガイドライン第3章以降で両者合意の場合明記となっていないか。なっていた場合「両者合意の場合」を除き「必ず明記」と変更して下さい。「両者合意の場合」は随所に見られます。厚労省ガイドライン第4章は本ガイドライン第2章に責任として記載され第3章に記載される対応すべき内容と対比するのは困難です。間違った解釈がなされる危険が有ると考えます。 【個人】	ご指摘の内容については、「合意」をしたうえで、その内容を委託契約等で明記することを前提としておりますので、包含しているものと考えております。
34	3．2．3 （2） 表 3-3 最低限4	・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。	【改定案】 ・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信等から保護するため、通信の暗号化を行うこと 【理由】 「・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと」 と記述されているが、通信の暗号化を行っても破壊は保護できないため、〃、破壊〃は不要と思われる。以下、同様に、106頁も同文章が記述されている 【個人】	本記述は「情報セキュリティ対策ガイドライン」の記述との整合性をとっての記述となっております。ご指摘の事項については、今後、ASP・SaaS業界内における「情報セキュリティ対策ガイドライン」の見直しの際に考慮されるよう、業界と連携しつつ取り組んでまいります。
36	3．2．3 （2） 表3－3 最低限7	・運用管理者とログのレビュー者のアクセス権を分離する等の、アクセスログの改ざん等に対する措置を講じること。	【意見】 「・・・アクセスログの改ざん等に対する措置を講じること」とありますが、医療情報の重要度とASP・SaaSという、運用面から脆弱性に繋がる恐れのある形態であることを鑑みると、「ログへのアクセス権の分離」だけでは不十分と思われます。 「・・・アクセス権を分離したり、ログ情報に対して時刻認証（タイムスタンプ）を適用する等の、アクセスログの改ざん等に対する措置を講じること」としてはいかがでしょうか。 【アマノタイムビジネス株式会社】	ご指摘の内容については、「アクセスログの改ざん等」に包含されているものと考えております。
37	3．2．3 （2） 表 3-3 最低限9	… 技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。（Ⅲ．1．1．6【基本】）	【意見】 107ページに「情報セキュリティ対策ガイドラインを遵守すること。」の記載があるが情報セキュリティ対策ガイドラインは実施必須事項を示すものではなく指標であるのでⅢ．1．1．6【基本】に示されている評価項目パターン1を最低限達成すべき間隔とする。との表現を追記して下さい。 【個人】	本記述の前提として、医療に関する情報の取扱いについては、「情報セキュリティガイドライン」のパターン1が該当することが前提となっておりますので、ご指摘の内容は包含されているものと考えております。
40	3．2．3 （2） 表3－3 推奨3	・データベースに格納されたデータの暗号化を行うこと。 （Ⅲ．2．2．2【推奨】）	【改定案】 ・データベースに格納されたデータの暗号化を行うこと。 なお、暗号化については、電子政府推奨暗号リストに記載されている暗号アルゴリズム及び鍵長を用いること 【意見】 「・データベースに格納されたデータの暗号化を行うこと。」 と記述されているが、P71の意見と同様の理由から、〃暗号化については、電子政府推奨暗号リストに記載されている暗号アルゴリズム及び鍵長を用いること〃と追加した方がよい。 【個人】	ご指摘の内容は、今後の見直しの際の参考とさせていただきたいと存じます。

ページ	項目	原記述	ご意見等	考え方
45	3．2．4 (2) 表 3-4 (2) 最低限1①	・従業員に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。	【意見】 厚労省ガイドラインでは「受託する事業者に対する包括的な罰則を定めた就業規則等で裏づけられた守秘契約を締結すること。」となっている為Ⅱ．5．2．2【基本】の表現「従業員が、情報セキュリティポリシーもしくはASP・SaaS サービス提供上の契約に違反した場合の対応手続を備えること。」をここにも記載して下さい。 【個人】	従業員に対する契約に関する文書化を含む内容は、「情報セキュリティ対策ガイドライン」のⅡ．5．1．1【基本】に記述しており、ご指摘の内容は包含していると考えております。
47	3．2．4 (2) 表 3-4 (2) 最低限1④	・連携ASP・SaaS 事業者が提供するASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．3．1．2【基本】）	【意見】 定期的の指標を例示してください。 【個人】	本記述は「情報セキュリティ対策ガイドライン」の記述との整合性をとっての記述となっております。ご指摘の事項については、今後、ASP・SaaS業界内における「情報セキュリティ対策ガイドライン」の見直しの際に考慮されるよう、業界と連携しつつ取り組んでまいります。
51	3．2．5 (2) 表 3-5 最低限3	・情報の破棄を実施した場合に、その内容を医療機関等に対して報告し、破棄記録等を提出すること。	【意見】 「・情報の破棄を実施した場合に、その内容を医療機関等に対して報告し、破棄記録等を提出すること。」 と記述されているが、ハードディスクの情報削除を考慮する場合、復元可能な削除方式や擬似乱数や固定値を複数回上書きする削除方式など、様々な削除方式が存在する。そのため、想定する情報破棄の方式を明確にし、情報の破棄についても医療機関と合意しておく必要があると考える。 【個人】	ご指摘の内容は、情報破棄の趣旨から包含されていると考えておりますが、明確化の観点から、下記のように修正いたします(P51)。 「情報の破棄を実施した場合に、その内容を医療機関等に対して報告し、破棄記録等を提出すること。」 →「情報の破棄を実施した場合に、電磁記録媒体の消磁、物理的破壊等、情報の削除方法を含む実施内容を医療機関等に対して報告し、破棄記録等を提出すること。」
57	3．2．6 (2) 表 3-6 最低限9	・連携ASP・SaaS 事業者が提供するASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．3．1．2【基本】）	【意見】 定期的の指標を例示してください。 【個人】	本記述は「情報セキュリティ対策ガイドライン」の記述との整合性をとっての記述となっております。ご指摘の事項については、今後、ASP・SaaS業界内における「情報セキュリティ対策ガイドライン」の見直しの際に考慮されるよう、業界と連携しつつ取り組んでまいります。
63	3．2．7 (2) 表 3-7 最低限8 及び 最低限9	技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、随時パッチによる更新を行うこと。（Ⅲ．5．2．1【基本】）	【意見】 107ページに「情報セキュリティ対策ガイドラインを遵守すること。」の記載があるが情報セキュリティ対策ガイドラインは実施必須事項を示すものではなく指標であるのでⅢ．5．2．1【基本】に示されている評価項目パターン1を最低限達成すべき間隔とする。との表現を追記して下さい。 【個人】	本記述の前提として、医療に関する情報の取扱いについては、「情報セキュリティガイドライン」のパターン1が該当することが前提となっておりますので、ご指摘の内容は包含されているものと考えております。

ページ	項目	原記述	ご意見等	考え方
67	3．2．8 表 3-8 最低限4	所管官庁に対して法令に基づく資料を円滑に提出できるよう、ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等は国内法の適用が及ぶ場所に設置すること。	【改定案】（②） 所管官庁に対して法令に基づく資料を円滑に提出できるよう、ASP・SaaS事業者は国内法の適用を受ける法人であり、かつASP・SaaSサービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージ等を設置する場所について適用ある国外法、契約等によって、当該資料の提出が制限を受けていないこと。 【意見】（②） 法令に基づく資料を所轄官庁に円滑に提出できるための前提条件として、SaaSの事業者が日本の法令の適用を受けるか、または医療サービス事業者と適切な契約を締結していれば、サーバ、アプリケーション等の場所に「国内法の適用が及ぶ」かどうかは、直接の関連がないと思われます。逆に日本のセンターにシステム機器を設置しながら日本に法人を持たない事業者がサービスを提供する方が問題であると思われます。 国際化の中で外資系企業にとって日本市場の割合が5%を切りはじめており、魅力的ではない市場となりつつある現状において、排他的な施策は、結果として日本市場への投資の低下、日本企業への新技術導入の遅延、さらには日本企業の海外販売の低下にもつながるのではないのでしょうか。 【株式会社セールスフォース・ドットコム】 【指摘】（③） 独立医療法人などの公共医療機関に関しては、調達の内外無差別性が求められている。入札時にデータセンターの制約を求めることにより、海外取引の障壁とならないよう配慮する必要がある。 【追記理由】（③） 所管省庁に対して法令に基づく資料提出のため、機器等の設置場所を制限するため。 【個人】	医療情報の保存は、医療法等の国内法で規定されていることから、その保存場所は法の執行の及ぶ範囲であることが求められます。
69	3．2．9 （2） 表 3-9 最低限1	―	【意見】 厚生省ガイドラインの記述から欠落している箇所があるため、記述に対して修正を行い、対応する要求事項を作成するべきである。 医療機関等の管理者への要求事項（厚生労働省ガイドラインの記述）に、 『 セッション乗っ取り、IP アドレス詐称等のなりすましを防止する対策をとること。上記を満たす対策として、例えば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ことがあげられる。 チャネル・セキュリティの確保を閉域ネットワークの採用に期待してネットワークを構成する場合には、選択するサービスの閉域性の範囲を事業者に確認すること。』 を追加記述し、ASP・SaaS事業者への要求事項に対しても、転記するべきでないか。 【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】	ご指摘の内容通り、厚生労働省ガイドラインからの引用が漏れておりましたので、追記します(P69)。要求事項の内容については、ご指摘の内容は包含されていると考えております。

ページ	項目	原記述	ご意見等	考え方
70	3．2．9 （2） 表 3-9 最低限2	・厚生労働省ガイドラインに基づいて医療機関等が採用する通信方式認証手段が妥当なものであることを確認することにつき、事業者の役割と範囲を、医療機関等と合意すること。	【改定案】 ・厚生労働省ガイドラインに基づいて医療機関等が採用する通信方式認証手段が妥当なものであることを確認することにつき、事業者の役割と範囲を、医療機関等と合意すること。 なお、通信方式認証手段の妥当性確認については、第三者の確認を優先(または推奨)する。 【意見】 医療機関を含む当事者による妥当性確認では客観的な確認でないため、客観的な妥当性確認を優先するか推奨すべきである。また、同様に、P106にも「・自社で講じるネットワークの安全対策が、医療機関等が定めるネットワーク回線の安全性に関する基準を満たしていることを確認し」とあるが、上記と同様の文章を追加した方がよい。 【個人】	ご指摘の内容は、事業者と医療機関が合意する役割の内容に包含されていると考えております。
71	3．2．9 （2） 表 3-9 最低限5	・ASP・SaaSにおいて送受信されるデータに対して、電子政府推奨の暗号鍵を用いた暗号化等によるセキュリティ対策を講じること。 ・暗号化によるセキュリティ対策が、医療機関等が求める水準を満たすものであることを確認し、不足があれば事業者でとるべき対応について、医療機関等と合意すること。	【改定案】 ・ASP・SaaSにおいて送受信されるデータに対して、電子政府推奨暗号リストに記載されている暗号アルゴリズム及び鍵長を用いた暗号化等によるセキュリティ対策を講じること。 また、暗号アルゴリズム実装の確実性を確認するために、暗号アルゴリズム実装試験及び暗号モジュール試験及び認証制度を推奨する。 【意見】 ・「ASP・SaaSにおいて送受信されるデータに対して、電子政府推奨の暗号鍵を用いた暗号化等によるセキュリティ対策を講じること。」 と記述されているが、電子政府推奨暗号リストは、暗号アルゴリズムと暗号アルゴリズムに対応した鍵長がリスト化されている。そのため、"電子政府推奨の暗号鍵を用いた暗号化等"という記述は、"電子政府推奨暗号リストに記載されている暗号アルゴリズム及び鍵長を用いた暗号化等"に修正した方がよい。なお、同様に、P125も同文章が記述されている。 また、実際に電子政府推奨暗号リストに記載された暗号アルゴリズムが実装されていることを確認する制度（暗号アルゴリズム実装試験：独立行政法人情報処理推進機構）が存在し、現状では国内外のハードディスクメーカは同制度を導入し第三者による実装検証を取入れている。以上のことから、第三者による客観的な評価・試験制度である暗号アルゴリズム実装試験を推奨することが望ましい。 【個人】	ご指摘の内容を踏まえて、下記のように修正いたします（P71）。 「ASP・SaaSにおいて送受信されるデータに対して、電子政府推奨の暗号鍵を用いた暗号化等によるセキュリティ対策を講じること。」 →「ASP・SaaSにおいて送受信されるデータに対して、電子政府推奨の暗号を用いた暗号化等によるセキュリティ対策を講じること。」
73	3．2．9 （2） 表 3-9 最低限8	・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行うこと。（Ⅲ．2．1．4【推奨】）	【意見】 107ページに「情報セキュリティ対策ガイドラインを遵守すること。」の記載があるが情報セキュリティ対策ガイドラインは実施必須事項を示すものではなく指標であるのでⅢ．2．1．4【推奨】に示されている評価項目パターン1を最低限達成すべき間隔とする。との表現を追記して下さい。 【個人】	本記述の前提として、医療に関する情報の取扱いについては、「情報セキュリティガイドライン」のパターン1が該当することが前提となっておりますので、ご指摘の内容は包含されているものと考えております。

ページ	項目	原記述	ご意見等	考え方
83-84	3．3．2 表3-12 (2)a 最低限3 及び (2)b 最低限1 最低限2	[83P（2）a] ・情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又はASP・SaaS サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。（Ⅱ．2．1．3【基本】） ・連携ASP・SaaS 事業者が提供するASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．3．1．2【基本】） ・利用者の利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。（Ⅲ．2．1．3【基本】） ・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．2．3．1【基本】） [84P（2）b] 1・臨床検査システム、医用画像ファイリングシステム等との連携におけるインターフェースの構築に関し、事業者の役割、範囲について医療機関等と合意すること。 2・同上	【意見】 「表3-12真正性の確保におけるASP・SaaS 事業者への要求事項」の中で、「ASP・SaaS における情報セキュリティ対策ガイドライン」で挙げられている原本性確保の要件を引用する箇所が十分でないと思われます。 よって、まずは、Page83の項目3、Page84の項目1および2 において、Page83の項目1に書かれている「・電子データの原本性確保を行うこと。（Ⅲ．5．1．1【推奨】）」と同じ内容を追記すべきではないでしょうか。 さらに、「ASP・SaaS における情報セキュリティ対策ガイドライン」の原本性の確保の章を参照する方法は、他のガイドラインとの整合性の維持と記述の簡素化に効果的ですが、その反面、読み手にとって具体的なイメージが湧きづらい恐れがありますので、「原本性の確保」などのイメージ困難で且つ重要なものに関しては、「時刻認証（タイムスタンプ）」などの具体的な手段を例示することが望ましいと思われます。 【アマノタイムビジネス株式会社】	ご指摘の内容については、事業者と医療機関等が合意するインターフェースの構築の範囲に包含されていると考えております。
83	3．3．2 表 3-12 (2) a. 最低限3	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．2．3．1【基本】）	【意見】 107ページに「情報セキュリティ対策ガイドラインを遵守すること。」の記載があるが情報セキュリティ対策ガイドラインは実施必須事項を示すものではなく指標であるのでⅢ．2．3．1【基本】に示されている評価項目パターン1を最低限達成すべき間隔とする。との表現を追記して下さい。 【個人】	本記述の前提として、医療に関する情報の取扱いについては、「情報セキュリティガイドライン」のパターン1が該当することが前提となっておりますので、ご指摘の内容は包含されているものと考えております。
83	3．3．2 表 3-12 (1) a. 最低限3	・連携ASP・SaaS 事業者が提供するASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．3．1．2【基本】）	【意見】 定期的の指標を例示してください。 【個人】	本記述は「情報セキュリティ対策ガイドライン」の記述との整合性をとっての記述となっております。ご指摘の事項については、今後、ASP・SaaS業界内における「情報セキュリティ対策ガイドライン」の見直しの際に考慮されるよう、業界と連携しつつ取り組んでまいります。
85	3．3．2 表 3-12 (3) 最低限1	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．2．3．1【基本】）	【意見】 107ページに「情報セキュリティ対策ガイドラインを遵守すること。」の記載があるが情報セキュリティ対策ガイドラインは実施必須事項を示すものではなく指標であるのでⅢ．2．3．1【基本】に示されている評価項目パターン1を最低限達成すべき間隔とする。との表現を追記して下さい。 【個人】	本記述の前提として、医療に関する情報の取扱いについては、「情報セキュリティガイドライン」のパターン1が該当することが前提となっておりますので、ご指摘の内容は包含されているものと考えております。
85	3．3．2 表 3-12 (3) 最低限1	・連携ASP・SaaS 事業者が提供するASP・SaaS サービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。（Ⅱ．3．1．2【基本】）	【意見】 定期的の指標を例示してください。 【個人】	本記述は「情報セキュリティ対策ガイドライン」の記述との整合性をとっての記述となっております。ご指摘の事項については、今後、ASP・SaaS業界内における「情報セキュリティ対策ガイドライン」の見直しの際に考慮されるよう、業界と連携しつつ取り組んでまいります。

ページ	項目	原記述	ご意見等	考え方
92	3．3．3表 3-13	ー	【意見】 厚生省ガイドラインの記述から欠落している箇所があるため、記述に対して修正を行い、対応する要求事項を作成するべきである。 表 3-13 見読性の確保におけるASP・SaaS事業者への要求事項において、厚労省のガイドラインの“7.2 見読性の確保について”の“D. 推奨されるガイドライン”の【医療機関等に保存する場合】が抜け落ちているため、ASP・SaaS事業者への要求事項の【保存する場所について共通する内容】の推奨項目に抜けがでている。 【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】	ご指摘の内容を踏まえて、表3－13を修正いたします。
93	3．3．3 表 3-13 （2） 推奨	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．2．3．1【基本】）	【意見】 107ページに「情報セキュリティ対策ガイドラインを遵守すること。」の記載があるが情報セキュリティ対策ガイドラインは実施必須事項を示すものではなく指標であるのでⅢ．2．3．1【基本】に示されている評価項目パターン1を最低限達成すべき間隔とする。との表現を追記して下さい。 【個人】	本記述の前提として、医療に関する情報の取扱いについては、「情報セキュリティガイドライン」のパターン1が該当することが前提となっておりますので、ご指摘の内容は包含されているものと考えております。
93	3．3．3 表 3-13 （1） 推奨	・緊急時の医療機関等における診療録等の見読性の確保を支援する機能(例えば画面の印刷機能、ファイルダウンロードの機能等)をASP・SaaSにおいて含めることについて、医療機関等の管理者と協議し、合意すること。	【意見】 厚労省ガイドラインは内部に保存するか、内部に同様の内容を保存するように求めています。「自動による定期的なファイルダウンロード機能」として下さい。当面本ガイドラインを必要とする病院・診療所にはぬかりなくマニュアルでダウンロードを担当する職員が不足することが考えられます。「ハードウェアが毀損した場合の復旧時間いわゆるダウンタイムのサービスレベルについて医療機関等と合意すること。」をここ、もしくは3．3．3に追加して下さい。 【個人】	ご指摘の内容は、今後の見直しの際の参考とさせていただきたいと存じます。
96	3．3．4表 3-14	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．2．3．1【基本】）	【意見】 107ページに「情報セキュリティ対策ガイドラインを遵守すること。」の記載があるが情報セキュリティ対策ガイドラインは実施必須事項を示すものではなく指標であるのでⅢ．2．3．1【基本】に示されている評価項目パターン1を最低限達成すべき間隔とする。との表現を追記して下さい。 【個人】	本記述の前提として、医療に関する情報の取扱いについては、「情報セキュリティガイドライン」のパターン1が該当することが前提となっておりますので、ご指摘の内容は包含されているものと考えております。
97	3．3．4表 3-14	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．2．3．1【基本】）	【意見】 107ページに「情報セキュリティ対策ガイドラインを遵守すること。」の記載があるが情報セキュリティ対策ガイドラインは実施必須事項を示すものではなく指標であるのでⅢ．2．3．1【基本】に示されている評価項目パターン1を最低限達成すべき間隔とする。との表現を追記して下さい。 【個人】	本記述の前提として、医療に関する情報の取扱いについては、「情報セキュリティガイドライン」のパターン1が該当することが前提となっておりますので、ご指摘の内容は包含されているものと考えております。
98	3．3．4 表 3-14 （2） 推奨3	・利用者のサービスデータ、アプリケーションやサーバ・ストレージ等の管理情報及びシステム構成情報の定期的なバックアップを実施すること。（Ⅲ．2．3．1【基本】）	【意見】 107ページに「情報セキュリティ対策ガイドラインを遵守すること。」の記載があるが情報セキュリティ対策ガイドラインは実施必須事項を示すものではなく指標であるのでⅢ．2．3．1【基本】に示されている評価項目パターン1を最低限達成すべき間隔とする。との表現を追記して下さい。 【個人】	本記述の前提として、医療に関する情報の取扱いについては、「情報セキュリティガイドライン」のパターン1が該当することが前提となっておりますので、ご指摘の内容は包含されているものと考えております。

ページ	項目	原記述	ご意見等	考え方
98	3．3．4 表 3-14 (2) 推奨3	・紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。	【意見】 「保管場所の安全性に関して医療機関等と合意すること。」を追加して下さい。距離要件、地盤要件がサービスレベルになります。 【個人】	ご指摘の内容は、「3.2.8　災害等の非常時の対応におけるASP・SaaS事業者への要求事項」における事業者と医療機関等との合意事項に含まれていると考えております。
102	医療機関等以外に保存する際の要求事項 (2) 最低限	・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行うこと。（Ⅲ．2．1．4【推奨】）	【意見】 107ページに「情報セキュリティ対策ガイドラインを遵守すること。」の記載があるが情報セキュリティ対策ガイドラインは実施必須事項を示すものではなく指標であるのでⅢ．2．1．4【推奨】に示されている評価項目パターン1を最低限達成すべき間隔とする。との表現を追記して下さい。 【個人】	本記述の前提として、医療に関する情報の取扱いについては、「情報セキュリティガイドライン」のパターン1が該当することが前提となっておりますので、ご指摘の内容は包含されているものと考えております。
102	医療機関等以外に保存する際の要求事項 (2) 最低限	・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行うこと。	【改定案】 なし 【意見】 「・ASP・SaaS サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージについて定期的にぜい弱性診断を行い、その結果に基づいて対策を行うこと。」 については、ぜい弱性診断については、診断する項目や手法及びについて例示を記載すべきである。 また、アプリケーションについては取り扱う情報の機密性・重要性に応じて、攻撃者のレベルを想定した攻撃耐性に関する検査を推奨すべきである。 【個人】	ご指摘の内容は、今後の見直しの際の参考とさせていただきたいと存じます。
104	3．3．5 (1)	(1) 外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準におけるASP・SaaS事業者への要求事項 厚生労働省ガイドラインでは、外部保存を受託する機関として、3つのケースを想定している。 ① 病院、診療所、医療法人等が適切に管理する場所に保存する場合 ② 行政機関等が開設したデータセンター等に保存する場合 ③ 医療機関等の委託を受けて情報保管する民間等のデータセンターに保存する場合 ASP・SaaSにおいては、③により外部保存を行うことが一般的であることから、以下では③に対応するASP・SaaS事業者への要求事項を表3－15に整理する。	【案】 厚生労働省ガイドラインでは、外部保存を受託する機関として、3つのケースを想定している。 ① 病院、診療所、医療法人等が適切に管理する場所に保存する場合 ② 行政機関等が開設したデータセンター等に保存する場合 ③ 医療機関等の委託を受けて情報保管する民間等のデータセンターに保存する場合 ASP・SaaSにおいては、③により外部保存を行うことが一般的であることから、以下では③に対応するASP・SaaS事業者への要求事項を表3-15に整理する。 【意見】 ASP・SaaSについて、今後①の病院、診療所、医療法人等や②の行政機関等が事業者の役割になることが考えられるため、本ガイドラインの読み手に関して限定しないのであれば、③に対応するASP・SaaS事業者への要求事項に絞らずに、全体のASP・SaaS事業者への要求事項として整理すべき。それに伴い表3-15について見直す必要がある。 【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】	ご指摘の内容につき、現時点では③によるケースがASP・SaaS事業者においては一般的であると考えております。①、②についてもご指摘の内容を踏まえて、今後の見直しの際の参考とさせていただきたいと存じます。

ページ	項目	原記述	ご意見等	考え方
106	3．3．5 （1） 表 3-15 最低限（イ）	・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと。	【改定案】 「・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信等から保護するため、通信の暗号化を行うこと」 【意見】 「・外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行うこと」 と記述されているが、通信の暗号化を行っても破壊は保護できないため、″、破壊″は不要と思われる。 【個人】	本記述は「情報セキュリティ対策ガイドライン」の記述との整合性をとっての記述となっております。ご指摘の事項については、今後、ASP・SaaS業界内における「情報セキュリティ対策ガイドライン」の見直しの際に考慮されるよう、業界と連携しつつ取り組んでまいります。
115	3．4．3	ASP・SaaS において使用するデータの形式等についても、将来的な移行を視野に入れた対応をすることが望ましい。	【意見】 表 3-17中「受託データを医療機関に引き渡す際には、厚生労働省ガイドライン「5 情報の相互運用性と標準化について」に従って行うこととし、」と若干整合しないと考える。「使用するデータの形式などについては厚生労働省ガイドライン「5 情報の相互運用性と標準化について」に従って行うことが求められる。」としていただきたい。 【個人】	ご指摘の内容は、「3.4.3ASP・SaaS事業者間のサービス移行における留意点」の記述において包含されていると考えております。
116	3．4．3 表 3-17	・個人情報、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、該当する法令又は契約を特定した上で、その要求に基づき適切な情報セキュリティ対策を実施すること。	【意見】 「事業者に保存されている診療録等をサービス終了時に調べ、終了しなければならない診療録等は速やかに処理を行い、処理が厳正に執り行われたかを監査できる資料を提示すること。」を追記して下さい。 【個人】	ご指摘の内容は、「ASP・SaaSの提供を終了する場合に、受託しているデータ及びこれに関連する資料の内容、範囲、条件等について、医療機関等と合意すること。」の内容に、包含されていると考えております。
118	4．1	ASP・SaaS では契約書、SLA 等の文書において合意内容を明文化し、両当事者において遵守する必要がある。	【意見】 契約条項、SLAを例示して下さい。 今ASP・SaaSを選択する中小規模病院・診療所には契約条項、SLAの指標が必要です。 SLAは数段階のレベルごと、それが困難であればベスト、ベターなレベルの例示をして下さい。 【個人】	ご指摘の内容は、引き続き検討させていただきたいと存じます。
その他	報道資料「医療・福祉情報サービス展開委員会」委員名簿	―	【意見】 主査副主査を除いてベンダー側委員と病院側委員の人数には10名程度の開きがありバランスに問題があると思います。今ASP・SaaSシステムが必要な病院・診療所の運用を理解できる委員を採用しバランス是正の上ぜひバージョンアップをお願いします。 【個人】	ご指摘の内容は、今後の見直しの際の参考とさせていただきたいと存じます。
その他	―	―	【意見】 このような、IT技術を活用し、医療の現場が改善されることを期待する。 【個人】	ご指摘の内容は、本案を支持するご意見として承ります。

ページ	項目	原記述	ご意見等	考え方
その他	ー	ー	【要望】（外部委託元の委託責任について） 「医療機関側が、ASP・SaaS事業者に医療情報を取り扱わせるにあたってのガイドライン」も作成し、これと組み合わせて使うことが重要である。 【理由】 （1）外部委託元の委託責任を果たすためにすべき内容をまとめておくことにより、より、導入と運用を確実にするため。 （2） 外部保存を提供するサービスの場合には、個人情報の扱いについて、情報主体たる患者等に外部委託に起因するさまざまなリスクについて予め告知し承認を受けることが適当である。これは、委託側の医療機関が行うことである。 【個人】	ご指摘の内容は、今後の見直しの際の参考とさせていただきたいと存じます。