News release

2020 年 9 月 9 日
PwC あらた有限責任監査法人

PwC あらた、医療情報を取り扱う情報システム・サービス事業者向けに、新セキュリティガイドラインへの対応支援サービスを提供開始

リスクベースアプローチに基づくセキュリティ管理およびユーザーに対するリスクコミュニケーション態勢の整備を包括的に支援

PwC あらた有限責任監査法人（東京都千代田区、代表執行役：井野 貴章）は、9 月 9 日、医療情報を電子的に管理する情報システム・サービス事業者向けに、新たに策定された「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」への対応を支援するサービスを開始しました。

これまで、医療情報を電子的に取り扱う情報システム・サービス事業者は、経済産業省と総務省が公表するそれぞれのガイドライン※への準拠が求められていましたが、今般、これらのガイドラインが「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」として一つに整理・統合されました。

本ガイドラインでは、標準化された指定のセキュリティ対策の実施を求める従前のルールベースアプローチから、自社が提供する医療情報システム・サービスにおけるデータの流れを明確化した上でセキュリティリスクの特定・分析・評価を行い、合理的なセキュリティ対策の設計とその継続的な運用を求めるリスクベースアプローチへと、大幅な内容の変更が行われています。
また、事業者には、自社の医療情報システム・サービスに係るセキュリティリスク、およびそれに基づく対策の内容などを、医療機関をはじめとするユーザーに対して説明し、セキュリティ管理態勢全体について合意形成を図ることが求められており、従前よりもユーザーに対する能動的なリスクコミュニケーションが重視される内容となっています（図 1 および図 2）。

当法人は、監査や各種アドバイザリー業務で培ったガバナンスやリスク管理、医療業界に関する知見を活かし、医療分野の情報システム・サービス事業者が提供する各種システム・サービスにおける情報の流れを特定し、リスクの洗い出しや評価を行い、必要なセキュリティ対策の策定や現行のリスク管理態勢を改善することを支援します。また、これらのリスク対応の取り組みについて医療機関などのユーザーと十分な共通理解のもとに円滑な合意形成を進めるため、対外開示する情報の整理などもあわせて支援することで、新たなガイドラインへの対応を包括的にサポートします（図 3）。

医療・介護現場のデジタル化に伴い、サイバー攻撃を防ぐためのセキュリティ対策の必要性は急速に高まっています。医療情報を取り扱う情報システム・サービス事業者は、病院や診療所、介護事業者、薬局などのユーザーに対し、自社のセキュリティ対策の対応状況を正確に説明し、対話を通じて信頼構築を図ることが不可欠となっています。団塊世代が後期高齢者となる「2025 年問題」などにより、医療・介護の現場業務の効率性・継続性を支える情報システム・サービスのセキュリティ確保は、極めて重要な課題です。当法人は、全ての個人が安心して IT 技術を活用した、より質の高い医療・介護サービスを受けられるよう、セキュリティが整備された社会環境の構築に貢献することを目指します。

※経済産業省の「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ガイドライン」、および総務省「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」

図 1：医療情報を取り扱うシステム・サービスの提供事業者向けのガイドライン

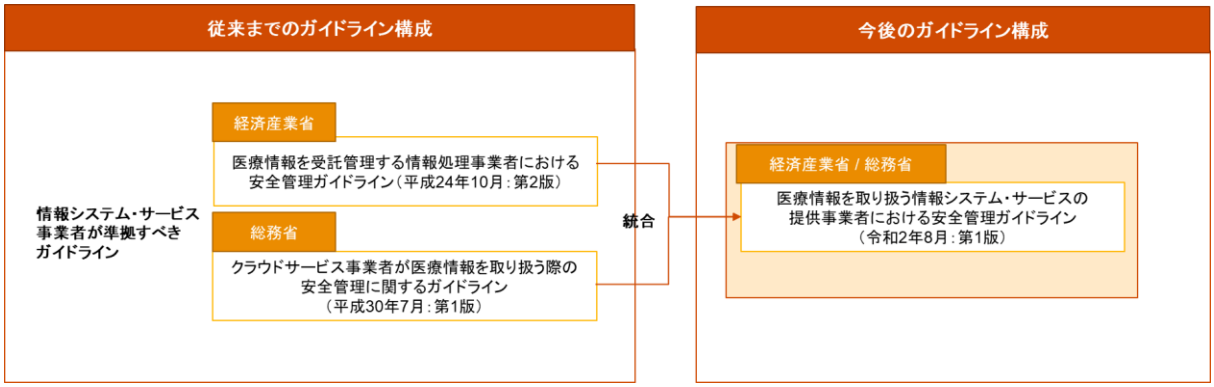
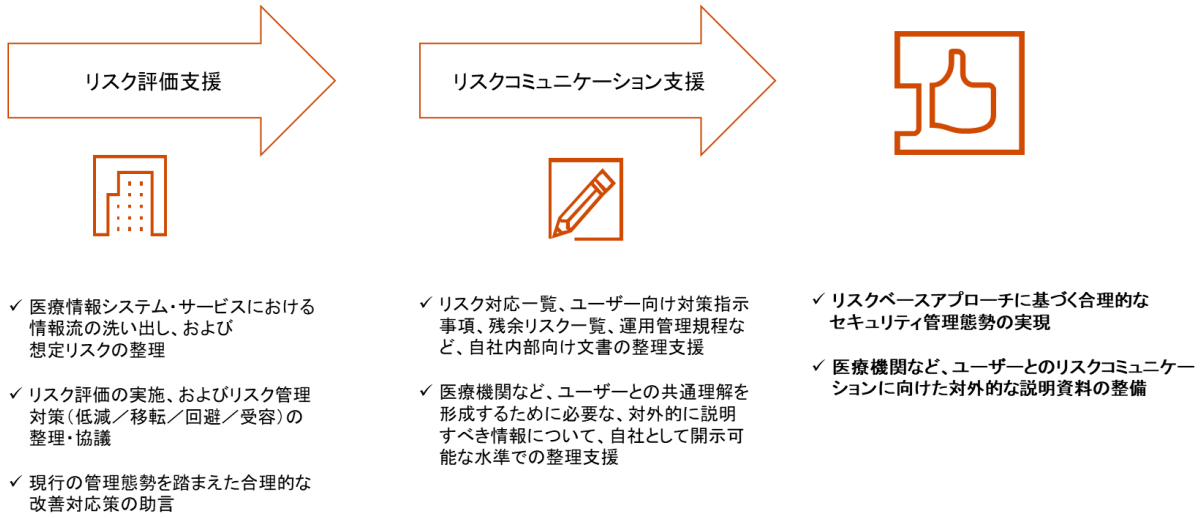


図 2：ガイドラインの新旧要件比較

	改定前のガイドライン	改定後のガイドライン
考え方	ルールベースアプローチ	リスクベースアプローチ
事業者に求められる実施事項の考え方	・最低限／推奨の二段階で実施事項を標準的に策定し、実施を求める ・対策の範囲はサービス提供中（システム運用・保守フェーズ）が中心	・医療情報という保護すべきデータを軸に、ユーザー／情報システム・サービス提供事業者間のデータの流れから想定されるリスクを洗い出し、リスク評価の結果に基づき合理的な対策を講じることを求める ・対策の範囲は、システム開発フェーズ、運用・保守フェーズ、およびサービス利用修了後のフェーズの全域（サービスライフサイクル全体）
事業者に求められる責任	医療機関などとの責任分界を事前に定義し、契約上の主管範囲の管理を徹底	・情報システム・サービス提供事業者のリスク評価結果に基づき、ユーザーが実施すべきリスク管理対策を指示し、能動的に合意形成を図る責任を重視（主体的なリスクコミュニケーションを通した合意形成） ・情報システム・サービス提供事業者／ユーザーが一体となり、役割分担のもとでサービス全体のセキュリティを確保し、セキュリティ水準を維持するための見直しを継続的に行う
主要な参照規格例	ISO27001(ISMS)	・ISO31000(リスクマネジメント) ・IEC62853（Open Systems Dependability）

図 3：本ガイドライン対応支援サービスのスコープ



以上

PwC あらた有限責任監査法人について　　www.pwc.com/jp/assurance

PwC あらた有限責任監査法人は、卓越したプロフェッショナルサービスとしての監査を提供することをミッションとし、世界最大級の会計事務所である PwC の手法と実務を、わが国の市場環境に適した形で提供しています。さらに、国際財務報告基準（IFRS）の導入、財務報告に係る内部統制、また株式公開に関する助言など、幅広い分野でクライアントを支援しています。

＜本件に関するお問い合わせ＞
PwCあらた有限責任監査法人　広報担当　Email：JP_PR@pwc.com
坂本　友紀：070-1574-8791 /只友　真理：　080-7268-7630