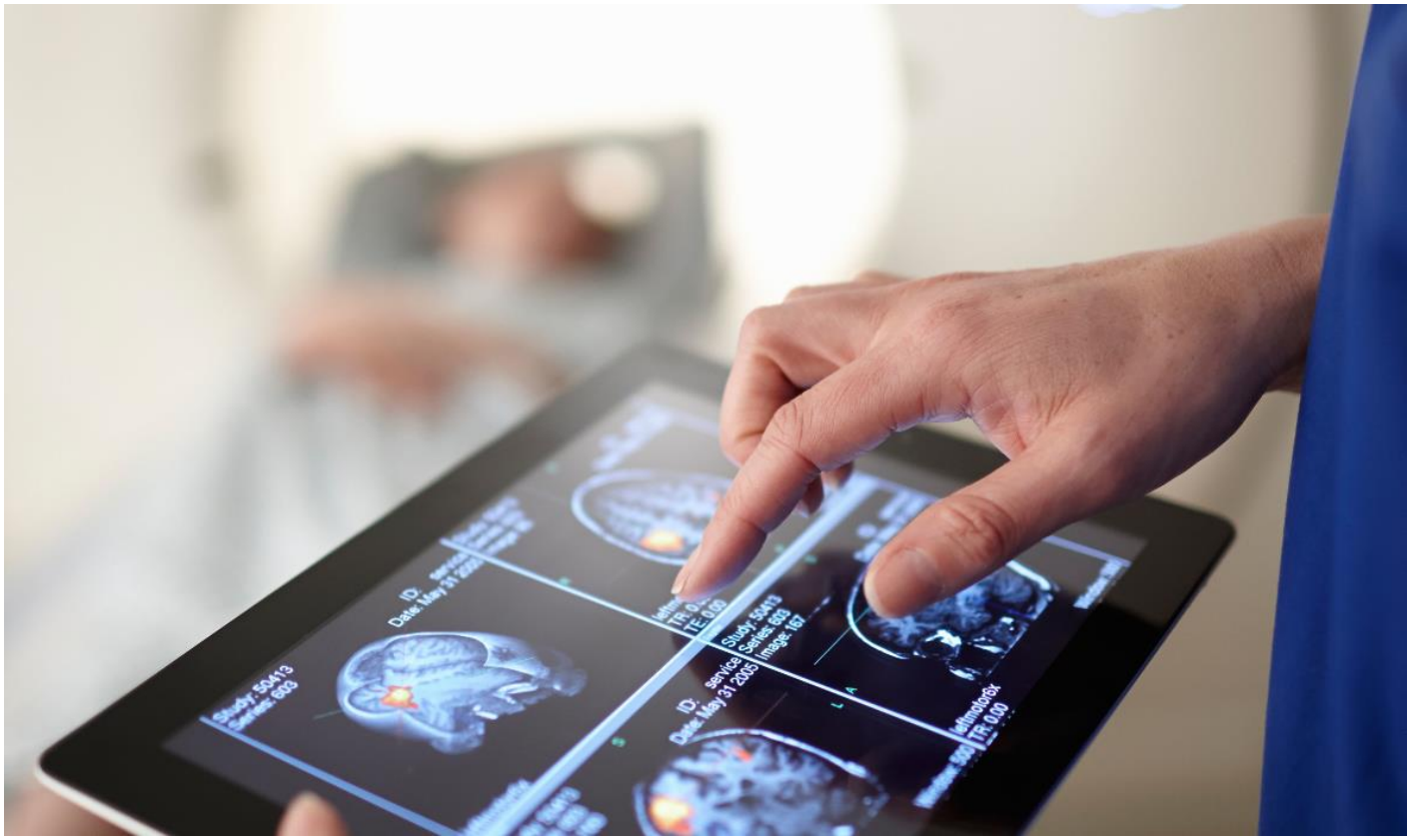
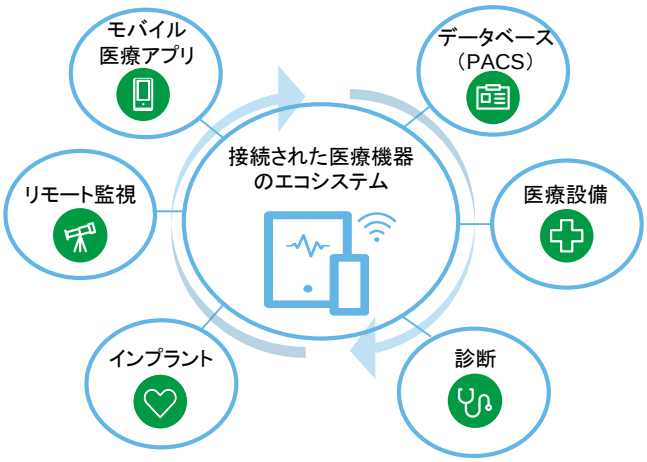
Deloitte.
デロイト トーマツ



医療機器サイバーセキュリティ対策サービス
IoT時代特有の変化する脅威からの保護

日本の医療機器メーカーが米国で事業を行う際、米国水準のサイバーセキュリティ規制への対応が遅れ、医療機器の販売停止や回収といった処分を受ける状況に直面しています。
デロイト トーマツは、IoT時代のサイバーリスクや規制の変化に対し、グローバル水準の医療機器サイバーセキュリティ対策を実現する総合的なサービスを提供することで、医療機器メーカー・医療提供団体・患者自身が安全に利用できる、理想的な医療環境の実現を支援します。

サイバーセキュリティの対応はネットワーク接続された医療機器が主な対象



医療機器のリスク

医療機器メーカーや医療機関にとっては、患者へのケアの改善、競争優位の維持、遠隔地への医療拡大などが重要な課題となっています。昨今の医療現場では、医療機関のネットワークや病院内のシステムだけでなく、IoTの機能を備えた医療機器の導入が、多くの臨床的なメリットをもたらしています。しかし、その利益を享受するには、これらのデバイスがもたらす新しいサイバーセキュリティ対策や患者のプライバシー保護および機器の制御による生命維持に対処する必要があります。

米国では2013年のセイバーセキュリティ強化に向けた大統領令により、医療を含む16重要インフラセクターにおいてサイバーセキュリティ強化を推進しています。この動きに伴い、米国で流通する医療機器については、日本とは異なる水準のサイバーセキュリティ規制対応が必要となっています。

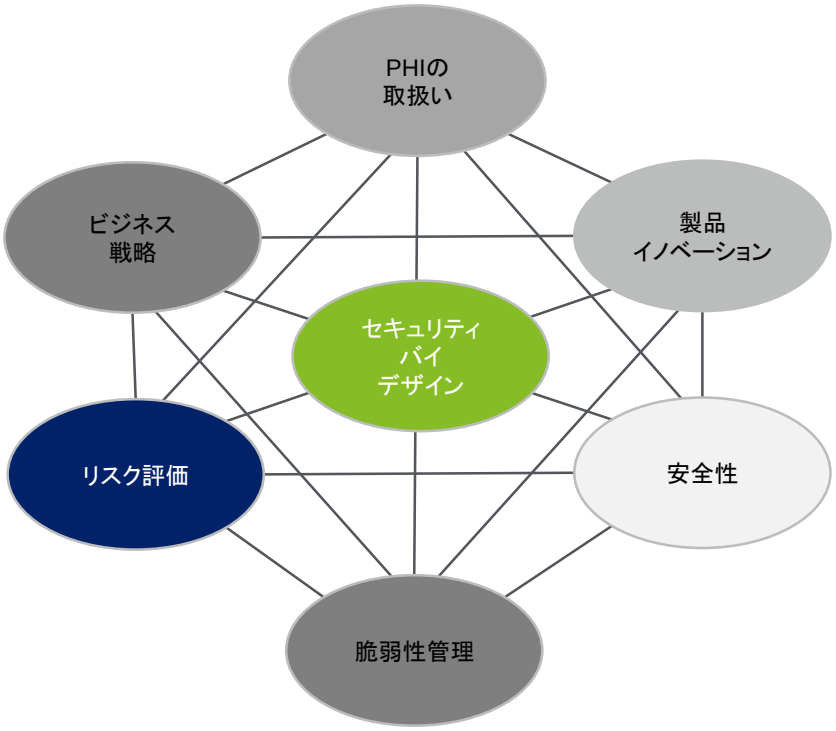
現在までの医療業界における取り組み:

- 医療機関
  HIPAA法に基づいた監査プログラムの第2フェーズが開始し、医療機関から医療機器のサイバーセキュリティ対応について厳しく問われ始めています
- 医療機器
  FDAから2014年10月に医療機器申請時におけるサイバーセキュリティ規制、2016年12月27日に市販後サイバーセキュリティ規制が施行され、販売し既に病院で稼働している医療機器についてもサイバーセキュリティ対応が必要となっています

企画設計段階からセキュリティを考慮したリスクベースの包括的アプローチ

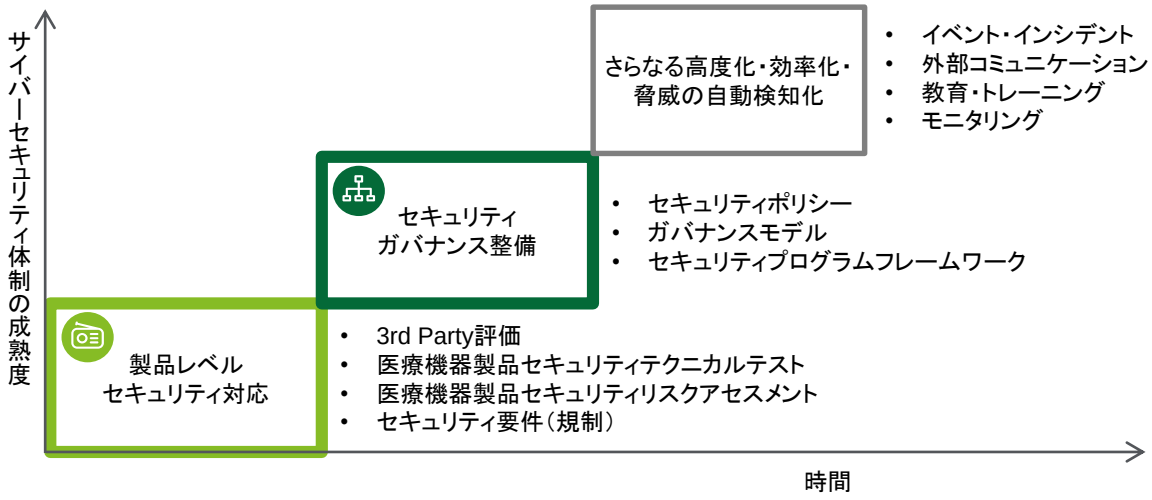
脅威がめまぐるしく変化する高度に動的な環境で、接続された医療機器を保護することは容易ではありません。製造メーカーは、製品開発ライフサイクル（PDLC）に「セキュリティ・バイ・デザイン」プロセスを実装することを検討する必要があります。デバイスを調達する者は、調達プロセスにセキュリティ要件を組み込み、一度取得したデバイスを確実に実装および保守するための措置を取る必要があります。

セキュリティ・バイ・デザインは、デバイスが市場に出された後にセキュリティ機能を追加するのではなく、デバイスを根本から安全に設計する方法論です。このアプローチでは、新しい規制とガイドライン、現在の脅威環境、技術的なテスト結果など、デバイスが設計、構築、およびテストされているときに、多くの要素が考慮されます。しかし、セキュリティによる設計だけでは十分ではありません。進化し続けている医療機器の展望において、敵対者を前にしてリスクの継続的な特定、評価、修復を必要とします。



私たちは、医療エコシステム全体にわたり支援します

医療機器の安全性を継続的に改善するためには、継続的な努力が必要です。デロイトトーマツの医療機器サイバーセキュリティチームは、標準と業界指針の継続的な開発を支援するために、プロジェクトの取りまとめを通じて得た洞察を提供することで、メーカー、医療提供団体、患者自身が接続され、IoTのメリットを享受することが出来る医療機器の可能性の拡大と理想的な医療環境の実現を支援いたします。
また本サービス提供に際しデロイトUSと連携します。デロイトUSは医療サイバーセキュリティの専門部隊MeDSS（Medical Device Security and Safety）を擁し、医療機関と医療機器メーカー双方への広範なコンサルティングサービスの提供、業界団体との連携、ベンダーとの協業等の活動実績を有し、特に直近の課題である米国における規制への対応について強みを持っています。



「総合的な医療機器サイバーセキュリティ対策サービス」主なサービスメニュー

	サービス名	サービス内容
1	医療機器製品セキュリティプログラムの成熟度評価	組織で開発、販売、保守されたコネクテッド医療機器製品のセキュリティ確保のための医療機器メーカーにおけるエンタープライズレベルのフレームワークと関連プロセスの評価
2	医療機器製品セキュリティリスクアセスメント	コネクテッド医療機器製品の設計と実装における弱点を特定するための論理ベースの製品セキュリティリスクアセスメント
3	セキュリティガバナンスモデルの確立支援	ガバナンス体制の確立、コネクテッド医療機器製品セキュリティプログラムおよび関連する業務プロセスを監督する役割と責任
4	医療機器製品テクニカルセキュリティテスト	ハードウェア、ソフトウェア、ファームウェアのレベルで潜在的な脆弱性を特定するための自動ツールと同時に、手動によるレビューと悪用の組み合わせを含む、堅牢な技術セキュリティテスト
5	医療機器製品認可取得支援	医療機器製品のセキュリティに関する規制についての問い合わせに対応するとともに、コネクテッド医療機器の承認のための提出パッケージ開発
6	医療機製品セキュリティプログラムの設計、開発、実装	組織が開発、販売、およびフィールド接続された医療機器製品のサイバーリスクを管理することを可能にするエンタープライズレベルの製品セキュリティプログラムの設計、開発、および実装

デロイト トーマツ リスクサービス株式会社
本　社　〒100-0005 東京都千代田区丸ノ内3-3-1 新東京ビル　TEL：03-6213-1300

IS 669126 / ISO 27001