米国医療機関における情報セキュリティ強化の動向

Survey Says: Healthcare Leaders Ready to Focus on Information Security

DSWRXJP 201404

要旨

米国では「経済的及び臨床的健全性のための医療情報技術に関する法律（Health Information Technology for Economic and Clinical Health Act：HITECH 法）」の制定や「電子健康記録（Electronic Health Record：EHR）」の推進が急速に進み、かつてない量の医療記録が電子化され始めています。EHR の普及は患者と医療従事者の両方に大きなメリットをもたらす一方、大量データのリスク管理をより効率的に行うことが求められることになりました。また医療現場からは蓄積されたデータへの常時接続やスマートフォン・タブレットの利用を求められるようになっていますが、この対応を誤った結果とおもわれる医療情報の漏洩は昨今増加しています。医療情報の漏洩は、一度の事故で多くの人に影響を与えます。最近制定された法律に照らせば、医療漏洩による各種対応は漏洩者やそのデータの管理者に多大な経済的負担を強いるものとなっています。

最近行われた医療組織のエグゼクティブ 500 名以上を対象にした調査では、このような環境の変化に対応し、セキュリティに関する新たな対応の準備が始まっているのが垣間見えます。最高情報セキュリティ責任者(CISO)を設置し、情報セキュリティに関する責任とガバナンスを明確にすると同時に、以前にも増して情報セキュリティに予算を割いているという傾向が顕著に見受けられます。

このような状況の中で包括的なリスク評価や継続的な監視戦略を始めとした適切な管理手法を導入することにより、医療情報に関わる特有のリスクを軽減し、直面する問題を自分たちの力で緩和することが可能となります。

はじめに：情報セキュリティに対する要求の増大

デンマークでは、病院のほぼ半数と一次医療医師の殆どが電子カルテ（またはEHR）を利用しています[1]。米国における電子記録の普及率は未だ 10%程度ですが、既にデンマークで渡される処方箋は既に紙ではなく、電子的な処理で入力されたものとなっています。

デンマークでは場合によっては、遠隔医療により患者は自宅または外出先で治療を受けられるようになりました。患者の自宅にある PC やノート PC に接続された Web カメラやモニター装置を用いて診察が可能となり、医師等が患者を離れた場所から診ることができます。10 年以上の歳月を掛けこの技術レベルへ到達しているデンマークに比べ、米国は最初の一歩を踏み出したという状態です。デンマークが立証したように、EHR 導入のメリットは明らかです：数百万ドルのコスト削減と膨大な時間が費やされている管理業務からの解放です。

このようなIT利用の流れの中において、データの利用過程におけるセキュリティが十分に管理されない可能性がある点が医療情報電子化の阻害要因として指摘されているにもかかわらず、米国ではEHRを急速に普及させるためのインセンティブが設けられるなどしています。実際に 2009 年米国復興・再投資法（ARRA）は先例のない方法で医療情報電子化の推進を行っています。ARRAの一環として、EHRへの移行を支援するためのインセンティブファンドに最大推定 270 億ドルが投じられておりEHRの有効利用を推進しようとしています[2]。この

[1] The New York Times, “Denmark Leads the Way in Digital Care,” 2010 年 1 月 12 日
[2] http://www.hhs.gov/news/press/2011pres/01/20110113a.htm

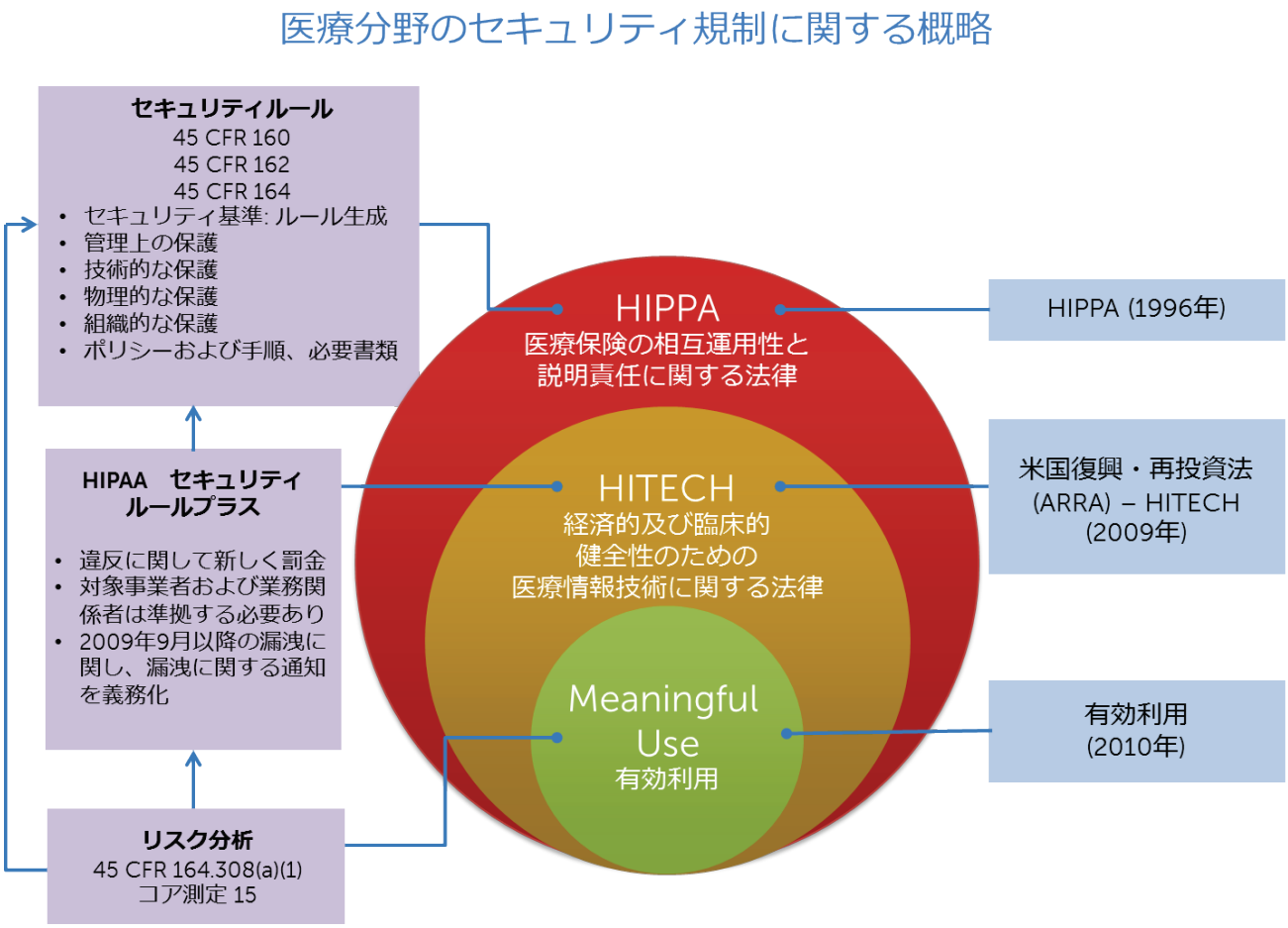


図 1：医療保険の相互運用性と説明責任に関する法律（HIPAA）における EHR の有効利用

一方で医療機関等がEHRの有効利用率を 2015 年までに達成できない場合、メディケア（米国における高齢者向け医療保険制度）の補助金が削減されることになっています（図 1）。夢の話と思われて数年、EHRは急激に業界の標準となることが期待されています。米国の病院は 2014 年までに 68 億ドルを情報技術に支出すると見込まれています[3]。

この法律は電子データの使用を促進するだけではなく、病院やクリニック、研究所や政府機関などさまざまな医療従業者において情報の電子的な交換を進めることを意図しています。全米各地で医療情報交換組織（HIEs）が設立され始め、既に 67 の公立HIEsおよび 161 の私立HIEsが存在しており、更に拡大することが予想されています[4]。また「責任あるケア機関（ACOs）」のような新しい活動からも、医療における電子データの有効利用と関係者のシームレスな接続に対する需要はますます増えることが見込まれています。

医療業務に利用できる EHR プラットフォームを構築するためには、セキュリティに対する精密な検討と調査が必要になります。電子化にむけて急速に動きはじめている業界の状況を考えれば、情報セキュリティが重要な関心事となっていることは意外なことではありません。今後、さらに大量のデー

[3] Hospital I.T. Spending SurgePredicted」、Health Data Management magazine、2009 年 6 月

[4] http://www.informationweek.com/news/healthcare/interoperability/231700227

タが電子データとして転送され、保存されるようになるでしょう。さらに多くのユーザがモバイルデバイスを使用して、データにアクセスするようになるでしょう。その一方で政府が医療組織にデータ漏洩の報告を義務付けたことから、データセキュリティに関して要求される透明性はますます高くなっています。

医療現場におけるモバイルデバイスの急激な増加は、業界のリーダーたちが情報セキュリティに関し慎重に考慮を求めるきっかけとなりました。2001 年にはわずか 30%でしたが、現在、米国の医師の 72%がスマートフォンを利用しています [5]。医療機関の最高医学責任者（CMO）のうち 39%はモバイルコンピュータやスマートフォンを自身が管理する施設に導入しています [6]。医師の 86%は、モバイル技術を最も利用するのは、電子カルテへのアクセスと回答しています [7]。

さらに医師や臨床医は、患者の情報にいつでも・どこからでもアクセスできるようにするため、個人所有のデバイス（iPad や iPhone）の利用を求めています（いわゆる Bring Your Own Device: BYOD）。モバイルデバイスの利用により、臨床医は患者のために素早く決断をできるようになり、業務全体の流れや患者の治療効果を高めることができるでしょう。しかしこの技術にリスクがないわけではありません。この技術の導入により確かに素早く情報にアクセスできるようになるでしょうが、その一方で情報を危険にさらす新たな手段となる可能性があります。

現実には電子データの増加やモバイル利用の増大により、医療組織で扱われるセキュリティに関する懸念事項のリストは長くなる一方です。

- 安全対策を行う必要のある OS の増加（多くのスタッフが個人所有デバイスの使用を希望していることによる）
- ラップトップ PC、USB ドライブ、他のリムーバブルメディア等の紛失または盗難に起因するデータ損失
- 正当なユーザによる情報の悪用（連番の患者記録の閲覧、平均を上回るアクセス回数、有名人の患者記録の閲覧等、業務に不必要・不適切なデータの閲覧・収集）
- 内部犯行者による、データベース等データが集約される場所への不正・不適切なアクセス
- 権限のない者によるネットワークやセキュリティ機器対する侵入の試み
- 日常業務の中での複数の認証メカニズム（例: ログイン）や認証ポイント
- モバイル機器におけるアプリケーションやインターネットアクセスの管理を目的とした、ポリシー強制

いらだたしいことではありますが、米国では医療組織が電子健康情報（ePHI）を 500 件以上漏洩した場合、次の措置を取る必要があります。

a) 60 日以内に HHS(米国保健福祉省)へ通知
b) 情報を漏洩された患者が住む地域の有名な報道メディアに事故を通知

[5] “Taking the Pulse” Manhattan Research 2011
[6] http://mobihealthnews.com/7985/cmios-39-percent-have-installed-mobile-devices/
[7] PricewaterhouseCoopers Health Research Institute report: “Healthcare Unwired” 2010 年 9 月

通知を受けると、HHSは漏洩組織、漏洩情報、漏洩数の一覧をWEBサイトに掲載します[8]。

2009 年から 2011 年 4 月までの間に、この規定に従い 260 を超える情報漏洩事故が報告され、1,000 万人以上の患者の情報が漏洩したことが明らかになりました[9]。マスコミは（医薬の業界誌ばかりでなく全国紙といわれる新聞まであらゆるメディアで）この種の事故に関する記事をこぞって取り上げました。

最近注目を浴びた医療組織における情報漏洩事故のいくつかを以下に示します。

- 個人情報の盗難を行う犯罪組織がメリーランド州のホーリークロス病院で緊急救急室のファイルを奪い、患者 1,500 名の社会保障番号等の個人情報が盗まれた[10]。
- 2010 年にSunBridge Healthcare社において 1 台のBlackBerryの紛失が発覚。データ領域は暗号化されておらず、ここには約 1,000 名の個人情報（名前、生年月日、診察記録番号、診察を受けた日や臨床データ）が含まれていた。全ての影響を確認・回復するまでに 6 カ月を要した[11]。
- マネージドケアとよばれる医療保険サービスを提供するWellPoint社はインディアナ州に 100,000 ドルの制裁金を支払った。支払の理由は、32,000 名を超える人々の記録に影響を与えた消費者データの漏洩がありながら、通知が遅れたため。制裁の一部として、WellPoint社はこの漏洩の対象となったインディアナ州に住むすべての顧客に対しクレジットモニターサービスに対する料金を最長 2 年間提供し、また個人情報を窃盗されたことにより損害が発生した場合、最大 5 万ドルを支払うことで合意した[12]。

医療データは犯罪者にとってますます魅力的になっていることから、昨今この種の犯罪が増加しており、今後もセキュリティ侵害は急増することが予想されています。マサチューセッツ州に本拠を構えるリスク＆コンプライアンスソリューション社（RSA）からの新しいレポートによれば、紙に記された医療情報が電子化されることにより、医療組織はサイバー犯罪者にとってますます魅力的に映っています。実際に診療記録を入手すれば犯罪者が不正請求に利用できることから、この価値は高く、末端価格は 50 ドルと言われています（社会保障番号単体の場合、価格は 1 ドルです）[13]。

情報セキュリティのトレンド

Dell SecureWorks は、医療組織においてもセキュリティは重要な懸念事項であると認識しています。Dell が米国で様々な医療組織の役員 593 名を対象に実施した調査によると、最も重要な懸念事項は増大するセキュリティ面からの要求に対する必要な予算の確保、セキュリティ対策に必要なスタッフの

[8] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html
[9] http://www.eweek.com/c/a/Health-Care-IT/Health-Care-Data-Breaches-Affect-10-Million-Patients-Since-Fall-2009-809191/
[10] www.phiprivacy.net: “Holy Cross Hospital Notifies Emergency Room Patients of Possible Data Breach,” 2010 年 11 月
[11] http://www.phiprivacy.net/?s=sunbridge&x=16&y=3
[12] http://www.informationweek.com/news/healthcare/security-privacy/231001204
[13] RSA whitepaper: 「Cybercrime and the Healthcare Industry」2011 年

確保、そしてモバイル機器の盗難であることがわかりました。

この調査の回答のうち約 44%が、情報セキュリティの予算は今後 3 年で増加すると思うと回答し、減少すると思うと回答した人は 2%に留まりました。また 1/3 強の回答は、予算が増加するか減少するか不明だとしています。残る 21%は横ばいであろうと回答しています。医療関係のエクゼクティブが今後の情報セキュリティの方向性や対応の優先順位を必要としていること、そしてその多くの方々はセキュリティに関する取り組みの改善や維持のため、投資を増やす必要があると認識しているということを示しています。

モバイルへの潮流

データの電子化やモバイル機器の進歩とともに、モバイルデータの保護が現在最大の懸念事項になっていることに疑いはありません。前項の調査回答の 55%は、暗号化されていない患者のデータがラップトップPC、スマートフォン、タブレットや他のいわゆるモバイル機器に保存されていることが、セキュリティ上最も緊急を要する脆弱性と考えています。確かに 2009 年 8 月から 2010 年 12 月にHHSに報告された医療関係の情報漏洩のうちの 65%は、紛失または盗難されたモバイルデバイスやラップトップPCによるものでした [14]。

[14]http://www.redspin.com/docs/WP_Redspin_2010_Protected_Health_Information_Breach_Report.pdf

情報セキュリティ実践における矛盾

調査結果から医療組織においては、情報セキュリティに関する事項を基本的に以下の枠組みの下で決定しているということが浮かび上がってきます。

コンプライアンス主導による情報セキュリティの決定
情報セキュリティに関する購買行動調査において実に 70%以上の人々が政府の規制に準拠することがその主たる目的であると回答しています。おそらくこのシナリオに基づき、医療組織内部では様々な規制の特定の要件を満たすためにセキュリティ技術やプログラムに投資をするようトップを説得することでしょう。しかし幅広くセキュリティプログラムを揃えれば揃えるほど重要なポイントが不明瞭になり、またプログラムとプログラムの強固な連携を構築できず、成功を収めることが著しく難しい結果に陥りがちです。

保守的な意思決定 テクノロジーは絶えず変化しています。そしてメディアは大げさにデータ漏洩事故を取り上げます。このため医療組織は瞬間的な「恐怖」へ反応しがちです。例えば、大規模なデータ漏洩事故の原因がラップトップ PC の特定の使用方法にあると報告された場合、データを安全に保つために設計された専用のセキュリティソリューションに目を向けます。このシナリオに沿う場合、医療組織は反射的行動をとりがちで「直近の問題」に対応したセキュリティ技術や対策プログラムへ投資することになるでしょう。このような危機を回避するための投資 ー 近視眼的な投資が長期的な視点から組織の目標に合致して効果を発揮するセキュリティ対策プログラムに引き継がれる可能性は低く、投資対効果にも問題を残すものとなりがちです。

新しい情報セキュリティ管理の枠組みの必要性

この情報化時代において情報セキュリティをさらに効果的に実現するため、医療組織は戦略を錬る必要があります。単なるコンプライアンス対応、狭い意味での情報漏洩防止あるいは同業組織でのデータ流出事故への横対応からではなくより全体的なアプローチを採用する必要があると言えます。

次の例について考えてみましょう。病院のトップがサービス品目の拡大を決定し、さらに高い医療報酬で収益を得るため、随意外科手術メニューの提供を検討しています。そのためには物理的なスペース、新しい設備の購入、そして新しい情報技術・セキュリティ技術の導入計画を新しいビジネス戦略の中で合わせて検討する必要があります。

このビジネスプランが検討される場合、全体的な投資規模を確定し新規投資への最終判断をするため、あらゆるリスクを特定しその対策に必要なコストを測定する必要があります。セキュリティの面からは、あらゆるセキュリティの脆弱性を特定するため詳細なリスク評価を実施する必要があります。このリスク評価は実は継続的なプロセスでもあり、問題を発見、修正、回避するための最も有効な手段です。リスク評価には以下の 3 フェーズがあり、これらは相互に関係しています。

- **システムドキュメンテーションフェーズ**　事業運営に必須なシステムをすべて特定する。
- **リスク特定フェーズ**　事故発生の可能性や、保護すべき対象の価値に基づき、リスク量を計算して相対的なリスクを正確に測定する。
- **対応決定フェーズ**　測定されたリスクを限られた予算の中で緩和するためにどのような措置を取ることができるか検討する。

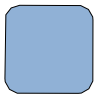
実際のところ、このリスク評価とその分析は、特に米国の医療機関が直面している 2 つの課題、すなわち「モバイル機器の導入とそのセキュリティポリシー」「米国 EHR の有効利用に関わるステージ 1 要求事項」への対応においてまず最初に行うべきことであり、プロジェクトとしての出発点です。

医療組織は包括的なセキュリティ管理の枠組みを構築し、リスク分析能力や患者の健康情報（ePHI）に対する脅威やデータ漏洩といった事故が業務に影響を及ぼす前にそれを監視・対応するために必要な人材、プロセス、技術（危機管理能力を含む）を保有する必要があります。これにより医療組織は多大な時間の節約を可能とするばかりでなく、組織のレピュテーションや最終的な収益に対するダメージを最小限に抑えることができるのです。

セキュリティリスク評価を全体的 IT 戦略の基礎に位置づけて実施するという推進力は、単に HIPPA や EHR の有効利用に関するコンプライアンスを満たすための強力な助けになるというだけでなく、例えば医療情報の増加やモバイル機器の利用シーンの拡大に伴い確実に増加する情報漏洩リスクに対応し、ここから発生するダメージを緩和することを可能とする戦略策定に対する価値ある第一歩となります。患者情報を起点として、このデータがどこに存在し、どのように使用されており、また誰がアクセス可能なのか、またアクセスしているのかなど、情報の利用に関する包括的な状況を描きだすことができれば、患者情報の完全性を結果的に安価に維

持することが可能になり、ビジネスに影響を与えかねないマスコミ報道を事前に防ぐことができ、さらにコンプライアンス違反に関わる制裁を防ぐことが可能となります。連邦会計監査、EHR の有効利用に関する罰則、そして漏洩が発生した場合の当事者への通知義務（データ保護違反通知制度）など、組織にからすればさまざまに政府を始めとする公的機関から監査をうける可能性があり、この中で医療組織が直面しているセキュリティリスクに対する理解が不足しており、対応計画も立てられていないと判断された場合、さまざまなペナルティを課せられ、レピュテーションにも傷がつく「最悪の事態」となりうる可能性があります。

結局のところ、医療情報セキュリティにおいては「1 オンスの予防薬は 1 ポンドの治療薬に値する（転ばぬ先の杖）」という古いことわざが、かつてないほど真実味があると言えるのかもしれません。



Dell SecureWorks の詳細については
次のサイトを参照してください。
www.secureworks.jp