www.pwc.com/jp/assurance

医療分野における デジタル・フォレンジックの可能性 ～医療における ＜見えない＊＊＞との闘い

PwCあらた有限責任監査法人
システムプロセスアシュアランス部
マネージャー
江原　悠介

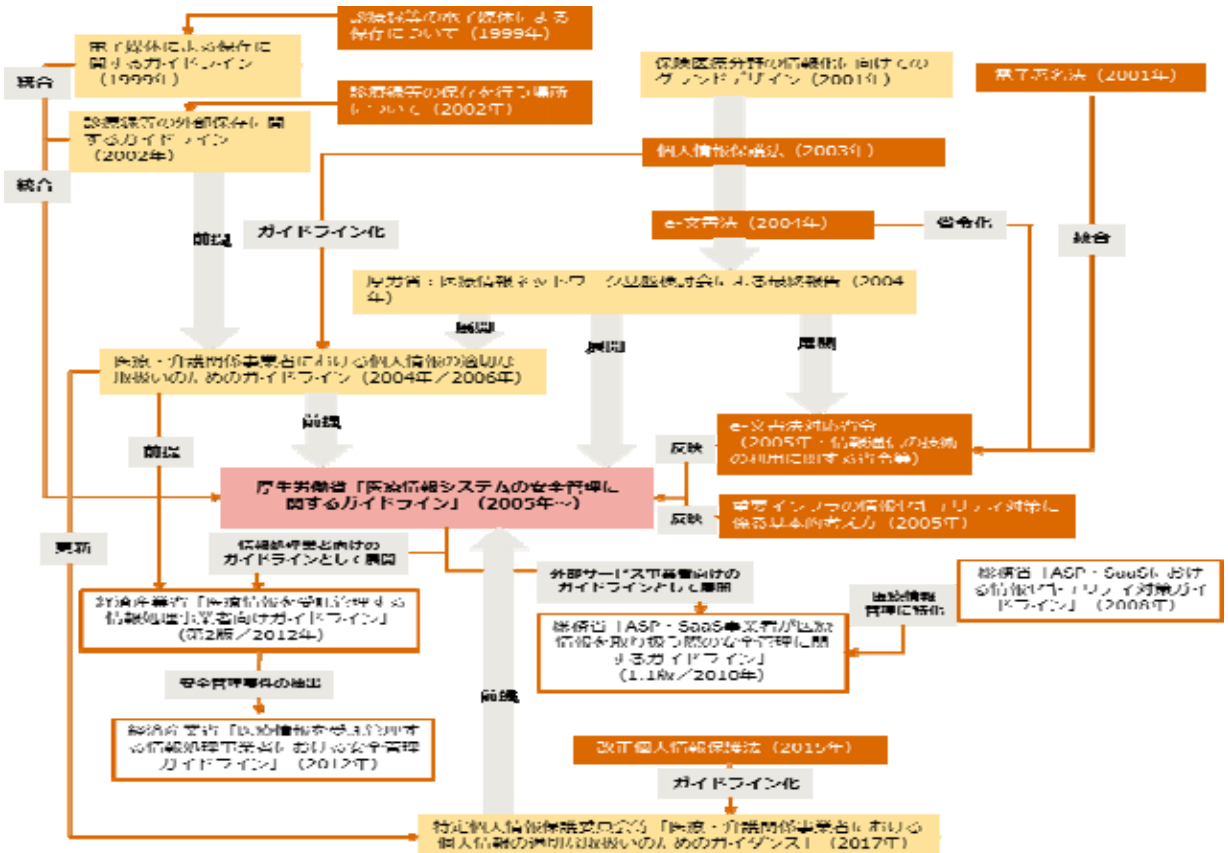
pwc

*医療分野における＜見えない**＞とは？*

- デフォルトのログイン情報を利用しているリモートアクセス
- 既存の攻撃コードを許容するリモートコマンド
- カスタマイズされたマルウェア
- 機器のインターフェースへの悪意のある行為
- 特定ベンダー機器への攻撃キャンペーン

& More・・・

医療情報（患者個人情報）保護に対する国内行政の流れ



医療機関（医療法人/社会福祉法人）への会計監査

社会福祉法人･医療法人の経営組織のガバナンスの強化、事業運営の透明性の向上等を図る目的で、社会福祉法及び医療法が改正され、一定以上の規模の法人への公認会計士による監査の義務化など、**組織運営上のガバナンスの透明化圧力が高まっている**。

医療法人		社会福祉法人
改正後医療法　第51条 2　医療法人（その事業活動の規模その他の事情を勘案して厚生労働省令で定める基準に該当する者に限る。）は、厚生労働省令で定めるところにより、前項の貸借対照表及び損益計算書を作成しなければならない。 5　第二項の医療法人は、財産目録、貸借対照表及び損益計算書について、厚生労働省令で定めるところにより、公認会計士又は監査法人の監査を受けなければならない。		**改正後社会福祉法　第37条「会計監査人の設置義務」** 特定社会福祉法人（その事業の規模が政令で定める基準を超える社会福祉法人をいう。第四十六条の五第三項において同じ。）は、会計監査人を置かなければならない。 **第45条の２「会計監査人の資格等」** 会計監査人は、公認会計士（外国公認会計士（公認会計士法（昭和二十三年法律第百三号）第十六条の二第五項に規定する外国公認会計士をいう。）を含む。以下同じ。）又は監査法人でなければならない。
＜厚生労働省令第96号（平成28年４月20日）＞ ・負債50億円又は事業収益70億円の医療法人 ・負債20億円又は事業収益10億円の社会医療法人 ・社会医療法人債発行医療法人	対象法人の規模	政令にて規定予定。
平成29年４月２日以降に開始する事業年度から （多くの医療法人は平成30年４月１日開始事業年度から）	開始年度	平成29年４月１日に開始する事業年度から

日本公認会計士協会
「公認会計士監査（会計監査人の監査）の概要」

会計監査におけるIT内部統制の位置付け

コンプライアンスは誰のため？

患者影響は？

直近の患者のみでなく、今後想定される未来の患者を含む

連携先医療・非医療組織への影響は？

連携先の医療機関、非医療組織への影響は？

違反した組織体が影響を受けるだけではなく、
ステークホルダー全てに影響を及ぼす

米国FDAによる医療機器向けの規制動向

2013年2月
オバマ大統領が社会インフラのサイバーセキュリティの強化を要求

2013年6月
FDAは医療機器の既知の脆弱性について警告を公表

2015年7月
FDAによる機器単体水準での脆弱性に関する警告の公示

2016年1月
FDAによる承認後（販売後）の医療機器に関するサイバーセキュリティモニタリングガイドラインの草案を公表

2013年6月
FDAによる一般的な医療機器向けのサイバーセキュリティ管理に向けた草稿を公表

2014年10月
FDAによる販売前のアプリケーションにおける医療機器のサイバーセキュリティ管理に関する最終ガイダンスの公表

2016年12月
FDAによる承認後（販売後）の医療機器のサイバーセキュリティモニタリングガイドラインの最終草稿の公表

医療機器の脆弱性？

脆弱且つハードコーティングされた管理者権限

- 医療行為の未許可の変更
- 現場では対応できない

既存/新規の医療機器における既知の脆弱性

- Post-marketにおける脆弱性コントロールの課題
- 医療安全を確保するための追加コスト

暗号化や認証機能のないデータ送受信

- プライバシーやデータ一貫性の課題
- Pre-marketにおける信頼性は確保可能か？

医療システム/機器の脆弱性の具体例

Shodanから、医療機関における意図しない外部情報公開状況が確認可能である。
この検索結果からは、医療機関のインターネットに繋がった医療機器のシステムが公開されているケースがあることが分かる。

- 麻酔システム– 21
- 心臓等システム– 488
- 静脈内注入システム– 133
- MRI – 97
- PACS Systems – 323

簡単に攻撃可能？

Shodanの検索結果例

ログインを必要としないシステムの例

System with Lockout Exemption:

```
050580      Echo Vas OR 1 -    _ScreenLock_0_Exception
050581   _ScreenLock_0_Exception
050583        OR 1-    _ScreenLock_0_Exception
050585     Echo Vas OR 2 -    _ScreenLock_0_Exception
```

```
046142 Anestisia OR
046774
046785 Me     A
046798
046799 Da    Fav
047271 Anesthesia Work Room
```

麻酔システム(Pediatric Nuclear Medicine Anesthesia Systems)の発見

電子カルテシステム(Electronic Medical Record Systems)の発見

EMR:

```
EP03 EPIC Cogito Clarity RDBMs Server
EP04 EPIC Clarity Test Console
EP05 EPIC Business Objects test
EP06 EPIC Realy BCA Server 1
EP07 EPIC Hyperspace
EP08 EPIC Hyperspace Web Server 1
EP09 EPIC Hyperspace Web Server 2
EP10 EPIC Hyperspace Web Server 3
EP11 EPIC Web BLOB Server
EP12 EPIC Kuiper Server
EP13 EPIC EPS Server 1
EP14 EPIC EPS Server 2
EP15 EPIC Interconnect
EP16 EPIC Care Everywhere
EP17 EPIC Soap Proxy
EP18 EPIC System Pluse
EP19 EPIC Multipurpose SQL Server
EP20 EPIC - Citrix XenApp 6.5 License/Web
EP21 EPIC - Citrix XenApp 6.5 Application Server
EP22 EPIC - Citrix XenApp 6.5 Application Server/DC
EP23 EPIC My Chart
EP24 EPIC Care Link
EP25 EPIC File Service
```

医療分野（医療機関）におけるＤＦの可能性

事後検証性 → **事前性（事前準備性）**

- イベントドリブン型の監査を前提
- 現場におけるアクセスコントロールの困難さ

- 厳格な安全管理水準（失敗は許されない）
- 同一のリスク認識を共有する共同体
- リスクベースなアクセスコントロール水準

非統一的なリスク認識による統制不備の発生有無をチェックするプロセス

リスク認識の共通度に基づく、透明性の高いトレーサビリティシステムの確立