資料13

第16回
健康・医療戦略参与会合

2019年5月22日

一般社団法人 日本医療機器産業連合会
(JFMDA)
会長　渡部眞也

データヘルスの進展によるサイバーセキュリティ対策の重要性

- ✓ 住み慣れた地域で安心して質の高い医療サービスを受けることができる社会の実現に向け、医療情報の電子化及び地域の医療機関等の間で情報連携が進んでいる。
- ✓ 近年のIT環境や技術の進歩に伴い医療分野におけるモバイルデバイスやIoT機器の普及が進んでいる。
- ✓ このような情報化・ネットワーク化の進展に伴い、サイバー攻撃による情報漏えいのリスク等、サイバーセキュリティ上のリスクが高まっている。

医療分野における情報化・ネットワーク化の進展		サイバーセキュリティリスクの増加
① 医療情報の電子化の進展	→	✓ 従来紙で取り扱われていた医療情報が電子化されることによる、サイバー攻撃の対象の増加
② 地域医療連携の普及	→	✓ 医療機関のネットワークの外部との接続の増加による、標的型メール等のサイバー攻撃による情報漏えいリスクの増加
③ モバイルデバイスの普及	→	✓ モバイルデバイスで医療情報を外部に持ち出す機会が増えることによる情報漏えいリスクの増加
④ IoT機器の普及	→	✓ 脆弱性のあるIoT機器の悪用など、サイバーセキュリティの観点でこれまで想定されなかったリスクの顕在化

データヘルスの進展によるサイバーセキュリティ対策の重要性

地域連携参加施設数の推移

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
合計	264	280	714	884	1,274	1,310	1,308	1,757	2,660	3,112	4,357	7,835	10,589	15,291	19,394	21,475	22,264	22,412	30,589
その他施設(n=215)	0	1	48	48	63	63	65	101	177	180	363	427	741	1,005	1,293	1,343	1,382	1,424	1,580
介護施設(n=213)	39	40	49	58	68	68	70	90	90	92	144	483	734	1,767	2,477	2,690	2,843	2,882	4,590
薬局(n=213)	27	31	62	62	130	130	137	166	773	812	952	1,079	1,290	2,111	2,436	2,972	3,051	3,074	3,357
歯科診療所(n=215)	11	11	27	28	28	28	28	49	85	85	104	509	688	793	946	1,002	1,066	1,072	1,364
医科診療所(n=238)	163	172	422	529	767	767	783	1,084	1,233	1,523	2,189	4,176	5,626	7,601	9,573	10,517	10,845	10,870	13,918
病院(n=237)	24	25	106	159	218	218	225	267	302	411	605	1,071	1,510	2,014	2,669	2,951	3,077	3,090	5,780

出典：日医総研「IT を利用した全国地域医療連携の概況（2017年度版）」

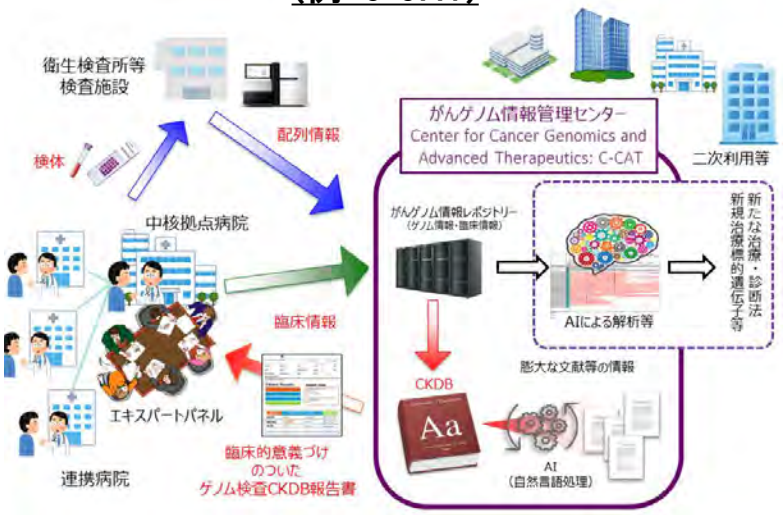
IoT関連機器・システムの増加

出典：日経デジタルヘルス「医療分野でのIoT・AI関連市場、2025年の規模は…」

インターネットに露出した医療関係のIPアドレス：国別Top10

出典：トレンドマイクロ「医療業界が直面するサイバー犯罪とその他の脅威」

大規模データ共有システムの構築（例：C-CAT）



出典：国立がん研究センター「がんゲノム情報管理センター（C-CAT）開設」

医療機関において想定されるサイバーセキュリティの脅威/リスク

脅威/リスク

分類	脅威
悪意のある行為	ウィルス
	ランサムウェア
	乗っ取り(医療機器)
	乗っ取り(セッション)
	機器の窃取
	データの窃取
	医療機器の改竄
	スキミング
	サービス妨害(DoS)
	ソフトウェア障害
	不十分なファームウェア
	機器障害
	ネットワークコンポーネント障害
	メンテナンス不足
	過負荷
	IoT、非IoT通信障害

分類	脅威
ヒューマンエラー	医療システムのconfエラー
	監査ログの未保存
	不正アクセス制御(権限の悪用)
	セキュリティポリシーの未準拠
	医師/患者(ユーザー)ヒューマンエラー
サプライチェーン障害	クラウドベンダー障害
	ネットワークベンダー障害
	電力供給業者障害
	医療機器ベンダー障害
自然災害	火事、洪水、地震

影響のある資産

ソフトウェア・データ

- 相互接続された医療情報システム
- 遠隔医療システム
- IDシステム
- データ

ハードウェア

- ネットワークに接続された医療機器
- ネットワーク機器
- モバイル端末
- 建物・設備

出典:Smart Hospitals - Security and Resilience for Smart Health Service and Infrastructures(ENISA)

インシデント事例(1)　国内医療機関

✓ 医療系ネットワークは他のネットワークと論理的に切り離されているはずだが、外部から電子カルテにランサムウェアに感染する事例や、内部でUSBメモリからマルウェアに感染する事例などがある。

ケース1：外部からの感染

電子カルテシステムの ウィルス（ランサムウェア）感染事例 宇陀市立病院（2018年10月）

【状況】
　職員が電子カルテシステムを使用出来ない状況に気付き、システム会社担当者が、サーバ画面にウイルス感染（ランサムウェア）のメッセージを確認し、システム全面停止、ネットワークからの物理的遮断（コンピュータのLAN ケーブルを抜く）を実施
紙のカルテでの対応を要し、二日後に復旧しても一部データは復元できず。
【原因】
　感染経路は特定できていないが、システム会社の不備により最新のウイルスソフトがインストールされていなかった。
　また、システム会社の不備によりバックアップに必要な磁気テープが装填されていなかったため、データが一部復元出来なかった。

ケース2：内部からの感染

医療機器のウイルス感染事例 金沢大学附属病院

【状況】
各部門で個別に導入したシステムから、他の部門の機器にウイルス感染が広がり、診療業務への影響が発生した。ウイルス検索・駆除ツール導入後のウイルスチェックでは1000件近くの不正プログラムが検出された機器もあった。
【原因】
USBメモリ経由での侵入

インシデント事例(2)　海外医療機関

✓　海外では医療機関のIT化が進む一方で、サイバー攻撃の深刻な脅威にさらされており、個人情報が大量に流出したり、身代金の支払いを応じざるを得なかったケースがある。

OSSの脆弱性を突いた攻撃により、450万人の患者情報が流出

- 病院経営を手掛けるCommunity Health Systemsは、2014年4月から6月にかけて、中国を発信地とするサイバー攻撃を受けた（病院側は、この事実を同年7月に確認）。
- ハッカーは、OpenSSLフレームワークが抱えるセキュリティ脆弱性を悪用し、仮想プライベートネットワーク（VPN）にログインし、データベース上の患者情報にアクセスしたと考えられる。
- これにより、同院系列の内科医の診察・治療を受けた約450万人の個人データ（過去5年分）が流出。流出したデータには、患者の氏名・住所・誕生日・電話番号・社会保障番号が含まれていた。

ランサムウェア攻撃により医療情報にアクセスできなくなる

- 南カリフォルニアの病院Hollywood Presbyterian Medical Centerは、2016年2月12日に、ランサムウェアによる攻撃を受けていることを公表した。
- 患者データベース（個人情報、レントゲン写真やCTスキャンのデータ、検査結果等）にアクセスできなくなり、数多くの患者が治療を受けられず、一部は他の病院に移送されることとなった。電子メールも停止され、医療従事者らはファックスや電話に頼らざるを得ない状況であった。
- 最終的に、医療機関側は攻撃者に対し、身代金として17,000ドルを支払った。

英医療機関、ランサムウェアの被害

- 英国国民健康保険サービスNHS（2017年5月）
  - ランサムウェア「WannaCry」の感染により、イングランドでは47、スコットランドでは13の病院で被害
  - 一部の病院では手術や診療予約をキャンセル、救急車の受入を拒否
  - 特に深刻な影響が出たのは、磁気共鳴画像装置（MRI）やコンピューター断層撮影装置（CT）、レントゲンなどの画像データをコンピューターでやりとりする病理診断部門
  - 保守党政権によるNHSのIT予算削減によるセキュリティ対策の不備が背景

出典：2017年5月15日BBCニュース「英医療機関、ランサムウェアの被害拡大を懸念」

インシデント事例(3)医療機器

インターネットからアクセス可能な医療機器の脆弱性

- ICS-CERT Monthly Monitor（2012年8月号）で報告された医療機器のリモート監視についての警告。実際に、インターネットからアクセス可能な医療機器が大学で見つかり、システム管理者に連絡を取り、是正がなされた。

インスリンポンプへのハッキング（Black Hat ）

- 2011年Black Hat にてJerome Radcliffe氏が発表。糖尿病患者のインスリンポンプに無線機能の脆弱性を利用して侵入し、投与するインスリンの量を外部から操作するなど「致死的な攻撃」を仕掛けることができることを発表

ペースメーカーへのハッキング

- Barnaby Jack氏が、BreakPoint security conference 2012では、ペースメーカーへのハッキングについて発表し、デモ映像を流した。Black Hat 2013でもペースメーカーへのハッキングについて発表予定であったが、発表前に死去し、詳細不明となっている。

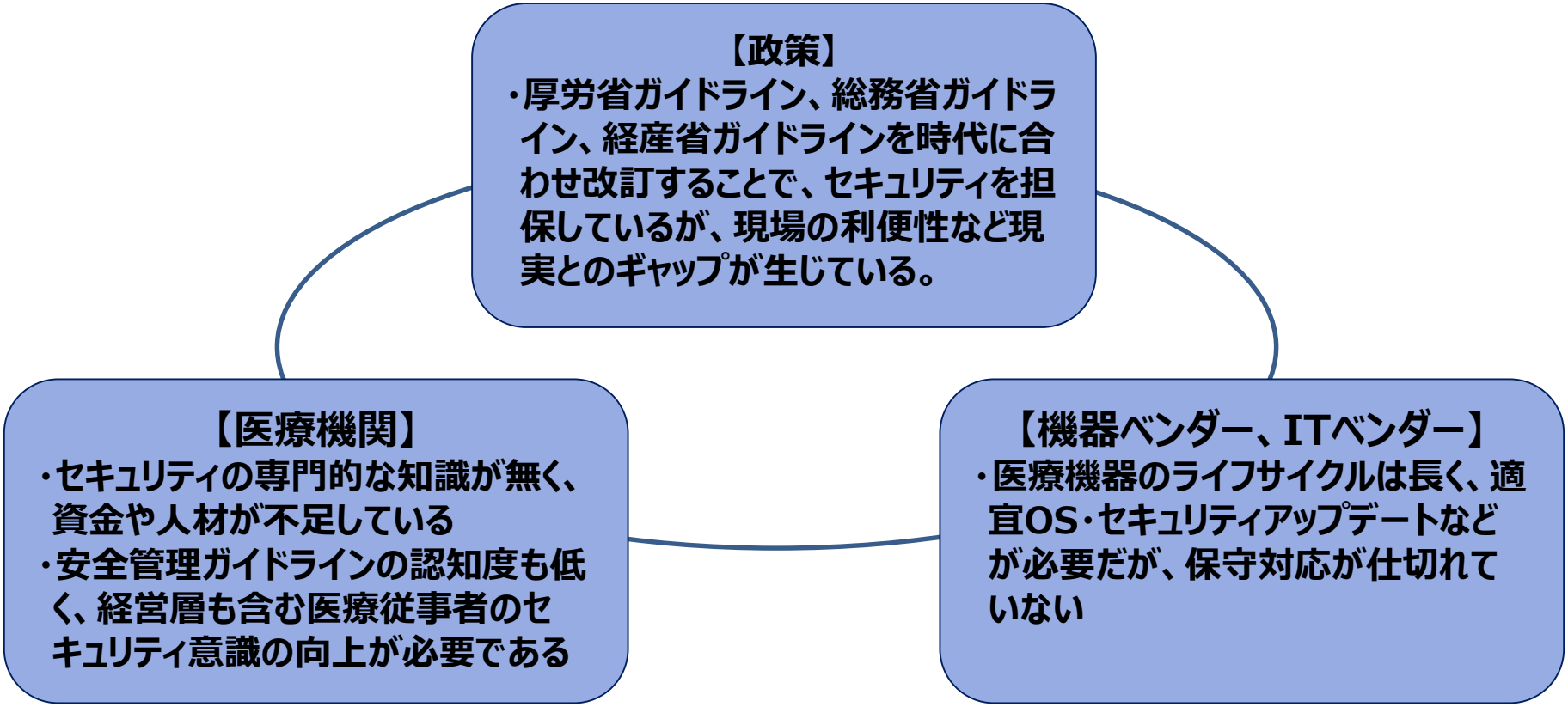
医療機器のハードコードされたパスワード

- 40ベンダ300の医療機器に関連するハードコードされたパスワードについて2013年6月にICS-CERTからAlertが出された。手術用機器や麻酔器、人工呼吸器、薬物注入ポンプ等が関係しており、機器によって遠隔操作が可能とされている。

出典：「医療機器における情報セキュリティに関する調査」(IPA)

現状の課題

- ✓ サイバー攻撃の増加・多様化、医療分野における情報化・ネットワーク化の進展といった環境変化に伴い、医療分野におけるサイバーセキュリティ対策の重要性は増しており、これに呼応する形で安全管理ガイドラインの継続的な改定等、政策的対応がなされているが、現場とのギャップが生じている。
- ✓ また、医療現場でのガイドラインの認知度は低く、セキュリティ意識の向上が必要と思われる。
- ✓ ベンダーは医療機器を継続して守るため、随時セキュリティアップデートが必要だが、対応しきれていない。



「総務省GL」：・ASP・SaaS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
→「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」に改正
・IoTセキュリティガイドライン
「経産省GL」：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

提言

エコシステムの取り組み

1．サイバーセキュリティ感染情報の開示及び対応策を含めた情報共有の仕組み構築

医療機関におけるサイバーインシデントの情報が極めて少ない。そのため、安全対策が後手になっていることが見受けられるため、インシデント事例及び対応策、予防策等を共有するための、H-ISACのような仕組みが必要である。(金融ISAC、ICT-ISAC等他分野では確立されている)

医療機関の取り組み

2．医療機関によるサイバーセキュリティ対応の推進

多数の医療機関のIPアドレスが外部からアクセスできており、IoT検索エンジンなどを利用した外部からの簡易セキュリティ調査など、現状を把握が必要である。
また、現状を把握した後、適宜、継続的な対策の実装が必要である。

医療機器の取り組み

3．医療機器における柔軟なセキュリティ対策の推進

医療機器のライフサイクルは長い。そのため、OSにセキュリティパッチを適宜更新していく必要があるが、セキュリティを担保するため、柔軟な対応が必要である。

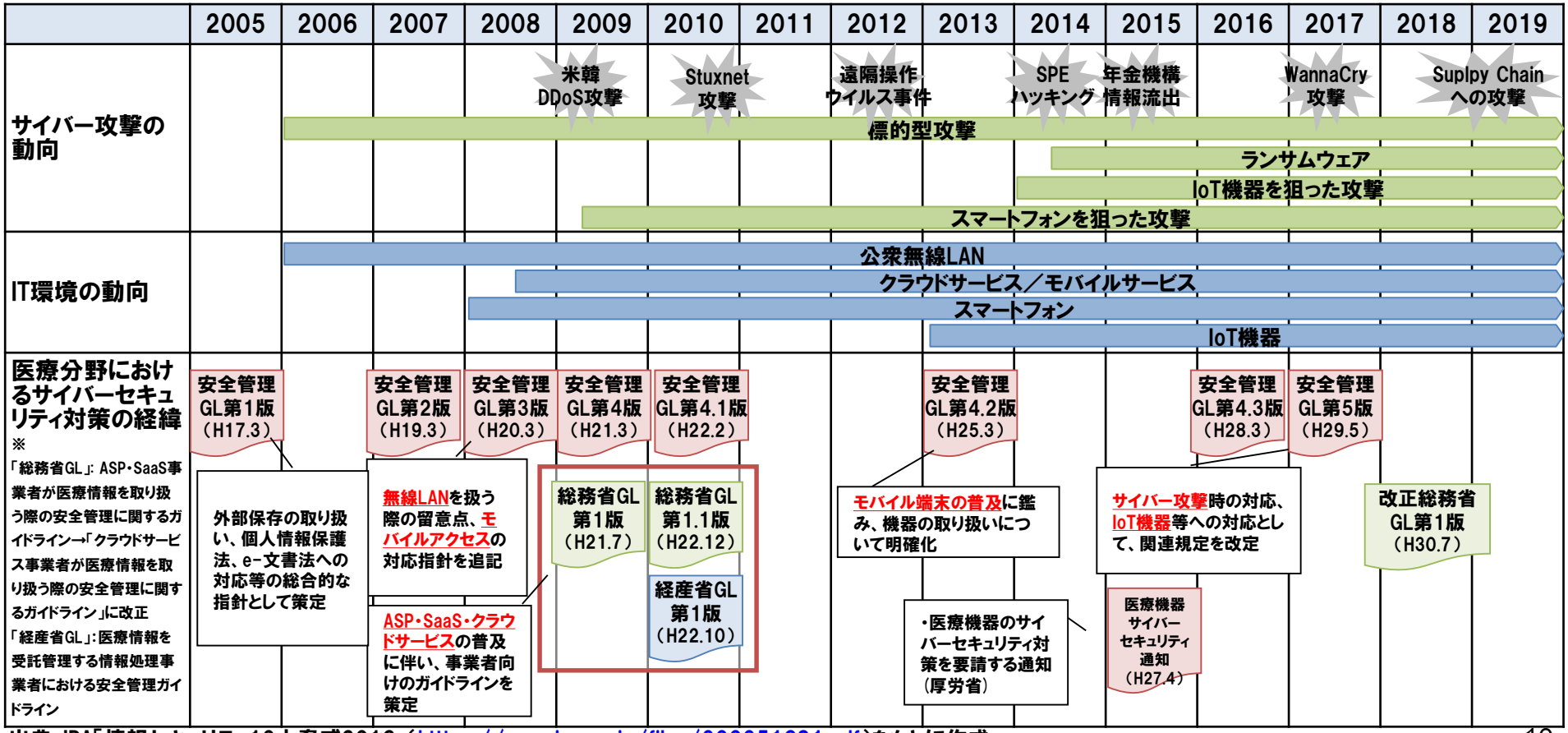
医機連

一般社団法人 日本医療機器産業連合会
JFMDA
The Japan Federation of
Medical Devices Associations

＜参考＞政策の取組み

✓ サイバー攻撃の増加・多様化、医療分野における情報化・ネットワーク化の進展といった環境変化に応じて、医療分野におけるサイバーセキュリティに関しては、厚労省の安全管理ガイドラインの継続的な改定等の対策が実施されることで、守られてきた。

医療分野におけるサイバーセキュリティに関わる経緯



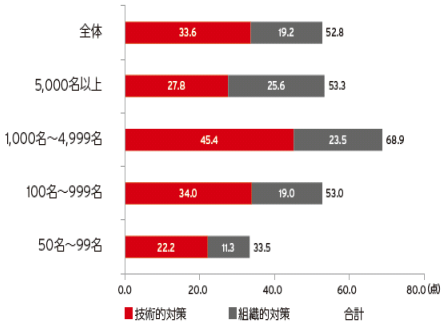
出典：IPA「情報セキュリティ10大脅威2016」（htttps://www.ipa.go.jp/files/000051691.pdf）をもとに作成

＜参考＞サイバーセキュリティの現状に関する仮説

✓ 医療現場におけるサイバーセキュリティの現状の仮説と根拠について、以下に示すような調査結果がある。

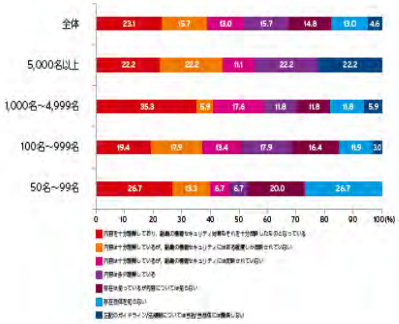
サイバーセキュリティの現状に関する仮説

医療業界のセキュリティ対策レベル*1



➢ 全業界平均（62.0点）と比べて、52.8点と低い

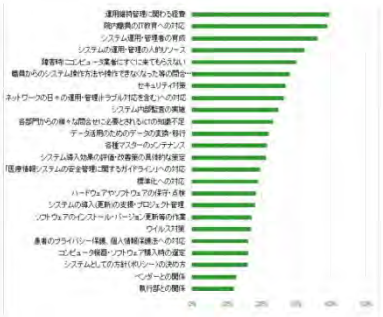
安全管理ガイドラインの認知度*1



➢ 内容を理解し、組織の情報セキュリティに反映している医療機関は約38%と低い

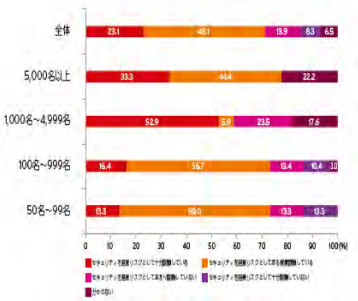
根拠

情報システムの運用管理で困っている点*2



➢ 主に、資金・人材不足に困っている

情報セキュリティに関する経営層のリスク認識*1



➢ セキュリティを経営リスクと十分認識しているのは、約23%と低い

出典：*1 トレンドマイクロ「組織におけるセキュリティ対策実態調査2016年版　～医療業界編～」
*2 日本医療情報学会「医療機関における情報システムの運用・管理に携わる人材に関する実態調査報告書」