医療情報システムに関するガイドライン5.2版について
サイバーセキュリティの観点から

一般財団法人医療情報システム開発センター・自治医科大学
山本隆一

Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022

COI 宣言

- 本講演に関して開示すべきCOIはありません。

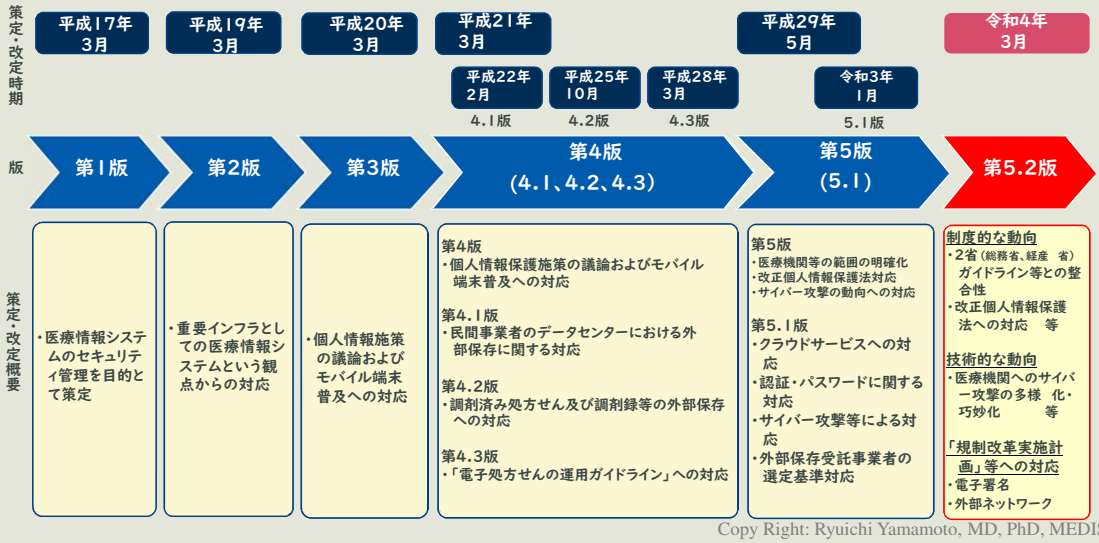
Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022

医療情報システムの安全管理に関するガイドライン改定の経緯

第8回健康・医療・介護情報利活用検討会（2022/03/04）資料より

● 医療情報システムの安全管理に関するガイドラインは、e-文書法、個人情報保護等への対応を行うための情報セキュリティ管理のガイドラインとして、平成17年3月に第1版が策定。以降、各種制度の動向や情報システム技術の進展等に対応して改定。

● 今般、第5.2版に改定し、令和4年3月末に公表。



3

Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022

医療情報システムに安全管理のためのガイドライン5.1版（厚生労働省）

ガイドライン本体　156p

別紙

- 付表1　一般管理における運用管理の実施項目例
- 付表2　電子保存における運用管理の実施項目例
- 付表3　外部保存における運用管理の例

付録　（参考）外部機関と医療情報等を連携する場合に取り決めるべき内容

医療情報システムの安全管理に関するガイドライン 別冊用語集

医療情報システムを安全に管理するために（第2.1 版） ー 医療機関管理者向け読本

「医療情報システムの安全管理に関するガイドライン 第5.1 版」に関するQ&A

4

Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022

医療情報システムに安全管理のためのガイドライン5.2版（厚生労働省）

ガイドライン本編　100p

ガイドライン別冊　85p

別紙

- 付表1　一般管理における運用管理の実施項目例
- 付表2　電子保存における運用管理の実施項目例
- 付表3　外部保存における運用管理の例

付録　（参考）外部機関と医療情報等を連携する場合に取り決めるべき内容

医療情報システムの安全管理に関するガイドライン 別冊用語集

医療情報システムを安全に管理するために（第2.1 版） ー 医療機関管理者向け読本

「医療情報システムの安全管理に関するガイドライン 第5.1 版」に関するQ&A

医療機関のサイバーセキュリティ対策チェックリスト

医療情報システム等の障害発生時の対応フローチャート

Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022

医療情報システムの安全管理のためのガイドライン5．2版（厚生労働省）

Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022

外部ネットワークが活用可能であることをわかりやすく周知

6.11章

7

医療情報システムに安全管理のためのガイドライン5.1版 6.11章

B 考え方

本章では、組織の外部と情報交換を行う場合に、個人情報保護及びネットワークのセキュリティに関して特に留意すべき項目について述べる。・・・・

B-1 医療機関等における留意事項
ここでは4.2 章で述べた責任のうち、ネットワークを通じて診療情報等を含む医療情報を伝送する場合の医療機関等における留意事項を整理する。・・・

① 「盗聴」の危険性に対する対応
・・・・

② 「改ざん」の危険性への対応
・・・・

③ 「なりすまし」の危険性への対応
・・・・

④ 暗号化を行うための適切な鍵管理
・・・・

B-2. 選択すべきネットワークのセキュリティの考え方
・・・ここでは通信経路上での脅威への対応であるチャネル・セキュリティについて解説する。・・・

電気通信事業者とクラウドサービス事業者がネットワーク経路上のセキュリティを担保する場合
・・・

電気通信事業者とクラウドサービス事業者がネットワーク経路上のセキュリティを担保しない場合
・・・

Ⅰ. クローズドなネットワークで接続する場合
・・・

①専用線で接続されている場合・・・・

②公衆網で接続されている場合・・・・

③閉域IP 通信網で接続されている場合・・・・

Ⅱ. オープンなネットワークで接続する場合
・・・

Ipsec+IKE・・・

TLS 1.2以降・・・

Ⅲ. モバイル端末等を使って医療機関等の外部から接続する場合
・・・

1) 公衆網（電話網）を経由して直接ダイアルアップする場合・・・

2) インターネットを経由して接続する場合・・・

3) 閉域ネットワークを経由して接続する場合・・・

B-3 従業者による外部からのアクセスに関する考え方
・・・・

B-4. 患者等に診療情報等を提供する場合のネットワークに関する考え方
・・・・

8

Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022

医療情報システムに安全管理のためのガイドライン5.2版 6.11章

B 考え方

本章では、組織の外部と情報交換を行う場合に、個人情報保護及びネットワークのセキュリティに関して特に留意すべき項目について述べる。・・・・

（1）医療機関等における留意事項
医療機関等において、ネットワークを利用して医療情報を外部と交換する際の留意事項としては、

「盗聴」の危険性に対する対応

「改ざん」の危険性への対応

「なりすまし」の危険性への対応

暗号化を行うための適切な鍵管理
などが挙げられる。

（2）選択すべきネットワークのセキュリティの考え方

・クローズドなネットワークで接続する場合

・オープンなネットワークで接続する場合

・モバイル端末等を使って医療機関等の外部から接続する場合

の3 つの場合について、それぞれ接続先の医療機関等のネットワーク構成や経路設計によって、意図しない情報漏えいが起こる可能性について留意し、確認する責務がある。

①専用線で接続されている場合・・・・

②公衆網で接続されている場合・・・・

③閉域IP 通信網で接続されている場合・・・・

①クローズドなネットワークで接続する場合
・・・

①専用線、②公衆網、③閉域IP 通信網の3つがある。

②オープンなネットワークで接続する場合
・・・

Ipsec+IKE・・・

TLS 1.2以降・・・

③モバイル端末等を使って医療機関等の外部から接続する場合
・・・

1）公衆網（電話網）を経由して直接ダイアルアップする場合・・・

2）インターネットを経由して接続する場合・・・

3）閉域ネットワークを経由して接続する場合・・・

（3） 従業者による外部からのアクセスに関する考え方
・・・・

（4）患者等に診療情報等を提供する場合のネットワークに関する考え方
・・・・

9

Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022

CyberSecurity

6.10章

10

医療情報システムに安全管理のためのガイドライン5.2版 6.10章
サイバーセキュリティ対策 - 1

B 考え方

(3)サイバー攻撃を受けた際の対応

医療情報システムに不正ソフトウェアが混入した場合、以下の対応等を行う必要が生じる場合がある。これらに備え、関係先への連絡手段や紙での運用等の代替手段を準備する必要がある。サイバー攻撃への対策については、PC やVPN 機器等の脆弱性対策をはじめとする6.5章及び6.6章に記載されている内容や、NISCから示されている「政府機関等のサイバーセキュリティ対策のための統一基準群（令和3年度版）」、2021年4月30日の「ランサムウェアによるサイバー攻撃に関する注意喚起について」も参照すること。また、非常時に備えたバックアップの実施と管理については、7.2章及び7.3章も参照すること。

攻撃を受けたサーバ等の遮断や他の医療機関等への影響の波及の防止のための外部ネットワークの一時切断

他の機器への混入拡大の防止や情報漏えいの抑止のための当該混入機器の隔離

他の機器への波及の調査等被害の確認のための業務システムの停止

不正ソフトウェアが混入した場合、**バックアップ**からの重要なファイルの復元

（重要なファイルは数世代バックアップを複数の方式（追記可能な設定がなされた媒体と追記不能設定がなされた媒体の組み合わせ、端末及びサーバ装置やネットワークから切り離したバックアップデータの保管等）取得することが重要である）

Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022

医療情報システムに安全管理のためのガイドライン5.2版 6.10章
サイバーセキュリティ対策 - 2

B 考え方

バックアップ

医療情報システムは一般に複雑で、医療機関の規模等によって運用やバックアップの方法も様々である。一様に指針を示すことは困難であるが、医療機関においては、重大な障害により医療提供体制に支障が生じた場合であっても、診療の継続や早期に業務を再開することが求められる。バックアップに関しては、全ての情報をバックアップから復元するのではなく、ある程度のリスクを許容することで運用が容易になり、確実に対応することが可能になることも多い。**診療のために直に必要な情報をあらかじめ十分に検討し、確実に運用できるバックアップを確保しておくことが必要である。**特に、一定規模以上の病院や、地域で重要な機能を果たしている医療機関等においては、ランサムウェア等のようにデータ自体を利用不能にするようなものについてバックアップデータまで被害が拡大することのないよう、バックアップを保存する電磁的記録媒体等の種類、バックアップの周期、世代管理の方法、バックアップデータを保存した媒体を端末及びサーバ装置やネットワークから切り離して保管すること等を考慮して対策を講じることが強く求められる。例えば、日次でバックアップを行う場合、数世代（少なくとも3世代）確保し、遅くとも3世代目以降はネットワーク的あるいは論理的に書き込み不可の状態にする等の対策が必要となる。

また、サイバー攻撃によるセキュリティインシデントが発生した際、数世代前までのバックアップデータは既に不正ソフトウェアが混入している可能性が高く、不用意にバックアップデータから復旧することで被害を繰り返し、場合によっては被害を拡大することになりかねない。不正ソフトウェア対策を講じつつ復旧するための手順をあらかじめ検討し、BCP として定めておくとともに、サイバー攻撃を想定した対処手順が適切に機能することを訓練等により確認することなども重要である。

C-4-(5)重要なファイルは数世代バックアップを複数の方式で取得し、その一部は混入が波及しない手段で管理するとともに、バックアップからの重要なファイルの復元手順を整備すること。

Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022

システム管理者向け　サイバーセキュリティ対策チェックリスト

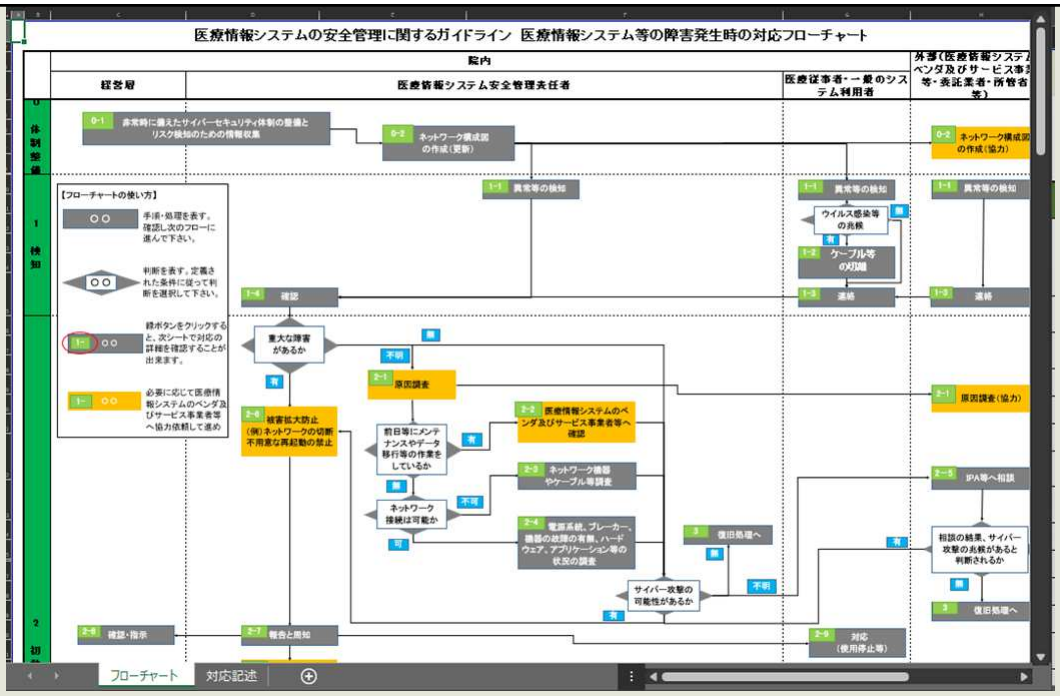
記入者	日付

NO	視点	チェック項目	チェック欄（○or×）
1	予防	医療情報システムで扱う情報を全てリストアップし、リストアップした情報資産に対してリスク分析を実施しているか（医療情報システムの安全管理に関するガイドラインの他、適宜、中小企業の情報セキュリティ対策ガイドライン第3版「(6) 詳細リスク分析の実施方法」、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（5．安全管理のためのリスクマネジメントプロセス）等を参考にすること）	
2	予防	医療情報システムベンダ及びサービス事業者から、役割分担や医療情報システムの安全管理に関する評価、リスクアセスメントの結果、リスクに応じた技術的対策、運用管理規定等の情報を収集しているか	
3	予防	リスク分析の結果に対して、医療情報システムの安全管理に関するガイドライン第5.1 版 6.3章～6.12章に示す対策等を実施しているか	
4	予防	個人情報が参照可能な場所においては、来訪者の記録・識別、入退制限等の入退管理を定めているか	
5	予防	医療情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成しているか	
6	予防	個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めているか	
7	予防	サイバーセキュリティにかかる最新動向（インシデント情報やセキュリティ専門知識を持つ者等からの情報発信等）の収集を実施しているか	
8	予防	アップデート（ソフトウェアを最新の状態に更新すること）の通知が届いたときは、医療機関の他の情報システムへの影響を確認した上で、従業員に対応方法について指示をしているか	
9	予防	セキュリティに関する脅威や対策等について、収集した情報を他の医療機関等と共有しているか	
10	予防	セキュリティ専門知識を持つ者等と協力して脆弱性検査を実施し、既知の脆弱性の有無を点検しているか	
11	予防	情報機器の設置場所や記録媒体の保存場所について、施錠管理、入室権限、盗難・紛失防止対策を行っているか	
12	予防	医療情報システムへのアクセスにおける利用者の識別・認証を行っているか	
13	予防	利用者の識別・認証にユーザID とパスワードの組み合わせを用いる場合、それらの情報を、本人しか知り得ない状態に保つよう対策を実施しているか	
	予防	利用者の識別・認証にIC カード等のセキュリティ・デバイスを用いる場合、IC カードの破損等、セキュリティ・デバイスが利用でき	

チェックリストの使い方　1）経営層向けチェックリスト　2）システム管理者向けチェックリスト　3）医療従事者・一般のシ …

13

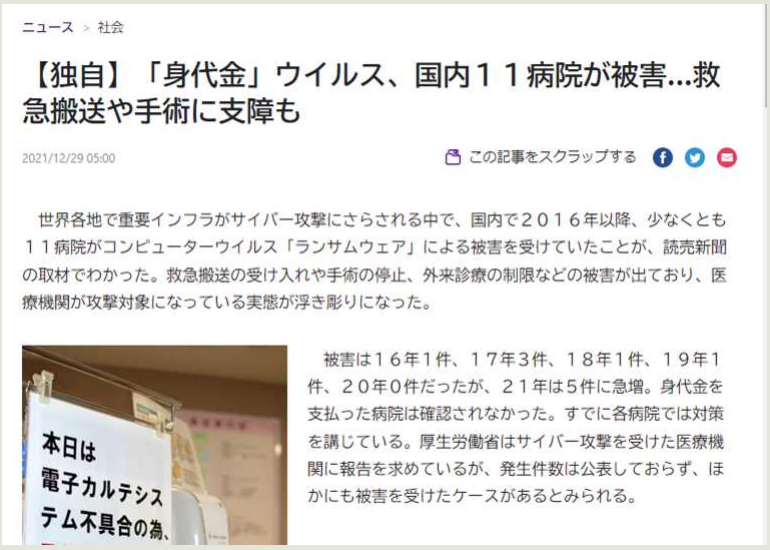
Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022



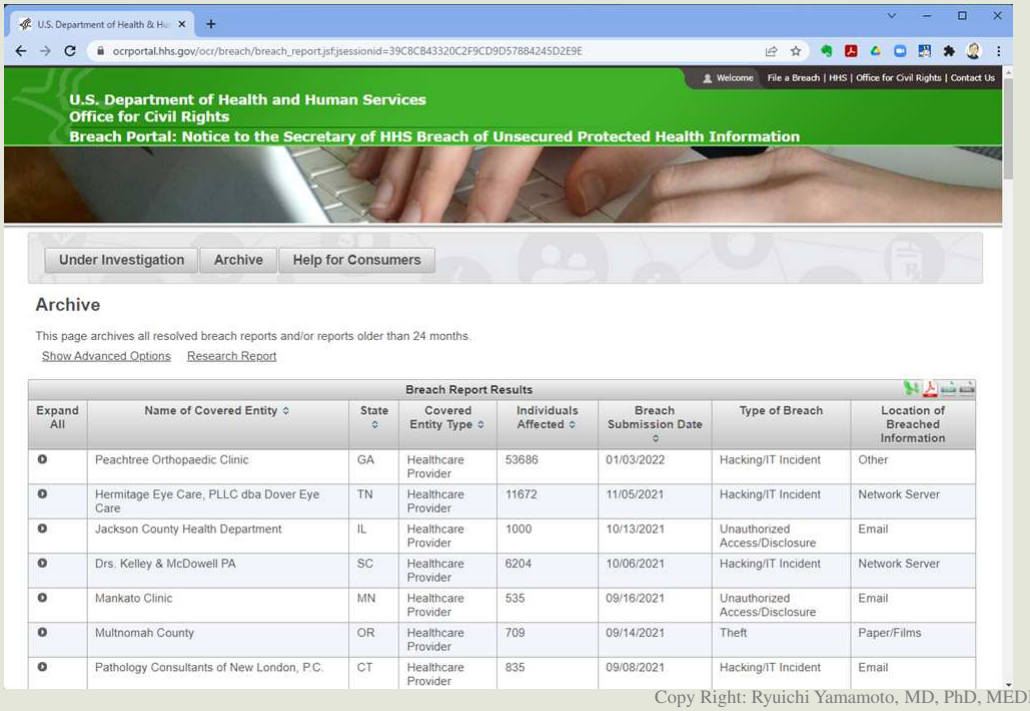
14

Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022

Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022



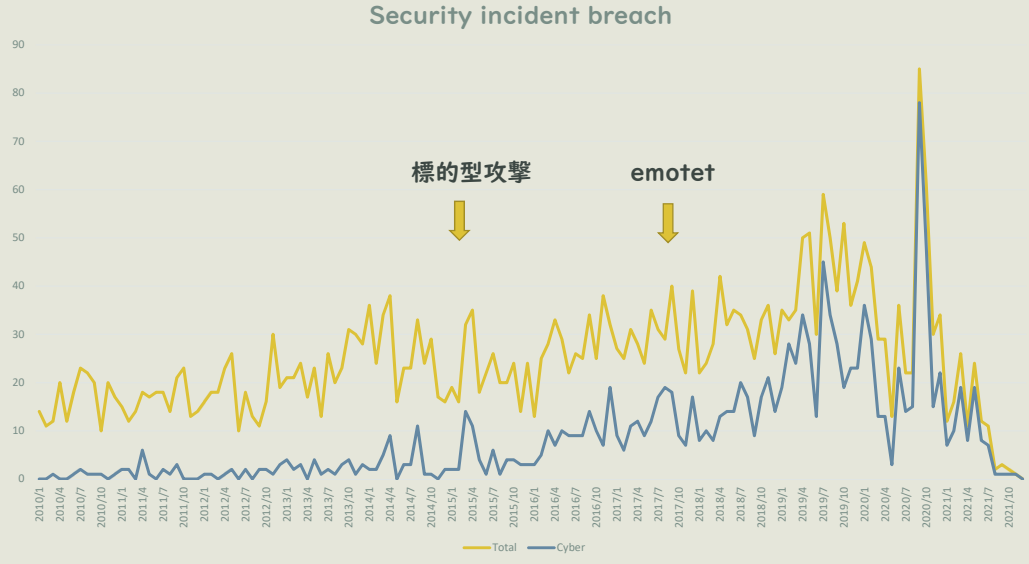
Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022



Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	Peachtree Orthopaedic Clinic	GA	Healthcare Provider	53686	01/03/2022	Hacking/IT Incident	Other
	Hermitage Eye Care, PLLC dba Dover Eye Care	TN	Healthcare Provider	11672	11/05/2021	Hacking/IT Incident	Network Server
	Jackson County Health Department	IL	Healthcare Provider	1000	10/13/2021	Unauthorized Access/Disclosure	Email
	Drs. Kelley & McDowell PA	SC	Healthcare Provider	6204	10/06/2021	Hacking/IT Incident	Network Server
	Mankato Clinic	MN	Healthcare Provider	535	09/16/2021	Unauthorized Access/Disclosure	Email
	Multnomah County	OR	Healthcare Provider	709	09/14/2021	Theft	Paper/Films
	Pathology Consultants of New London, P.C.	CT	Healthcare Provider	835	09/08/2021	Hacking/IT Incident	Email

17

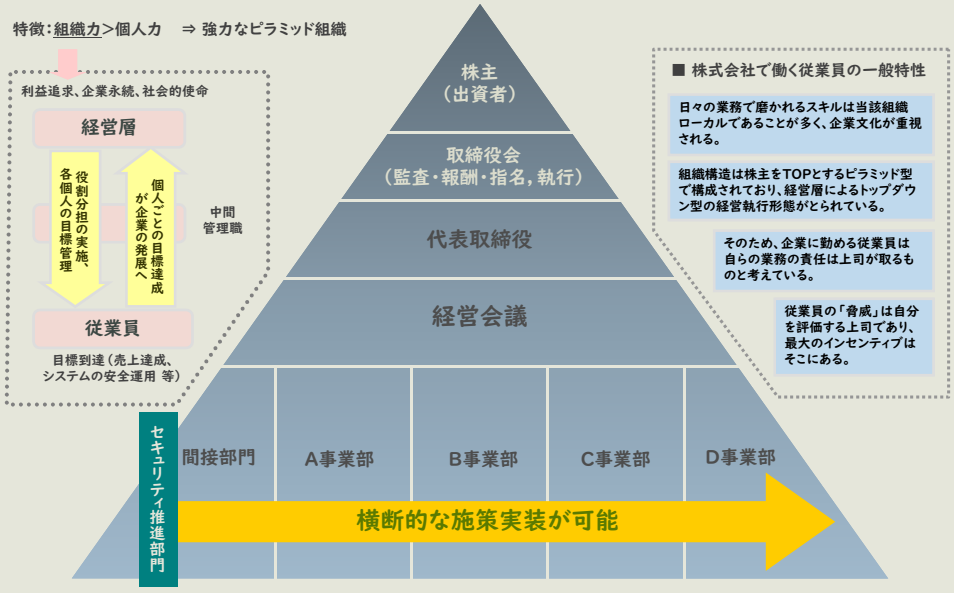
Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022



18

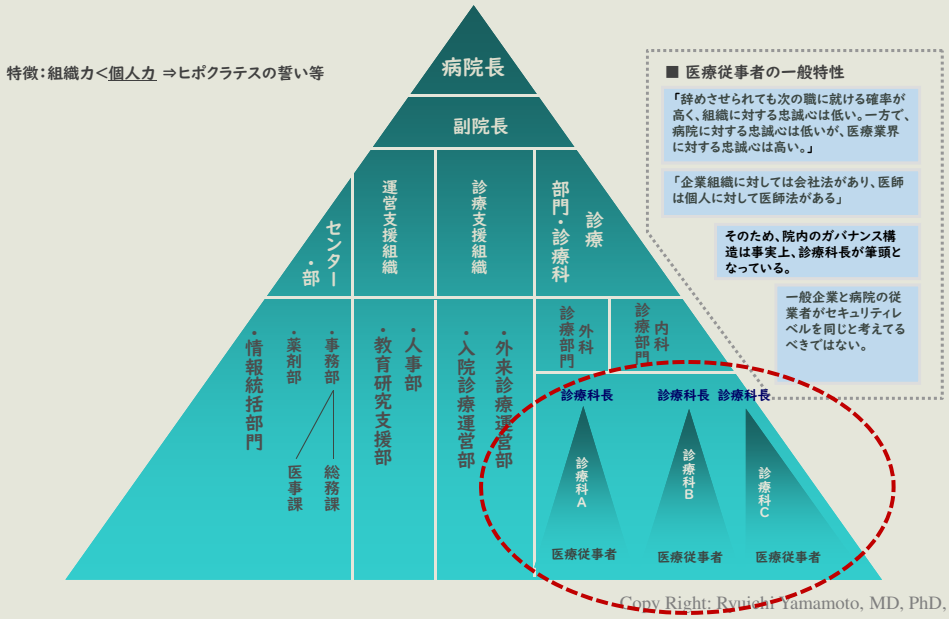
Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022

一般企業の構造とセキュリティマネージメント

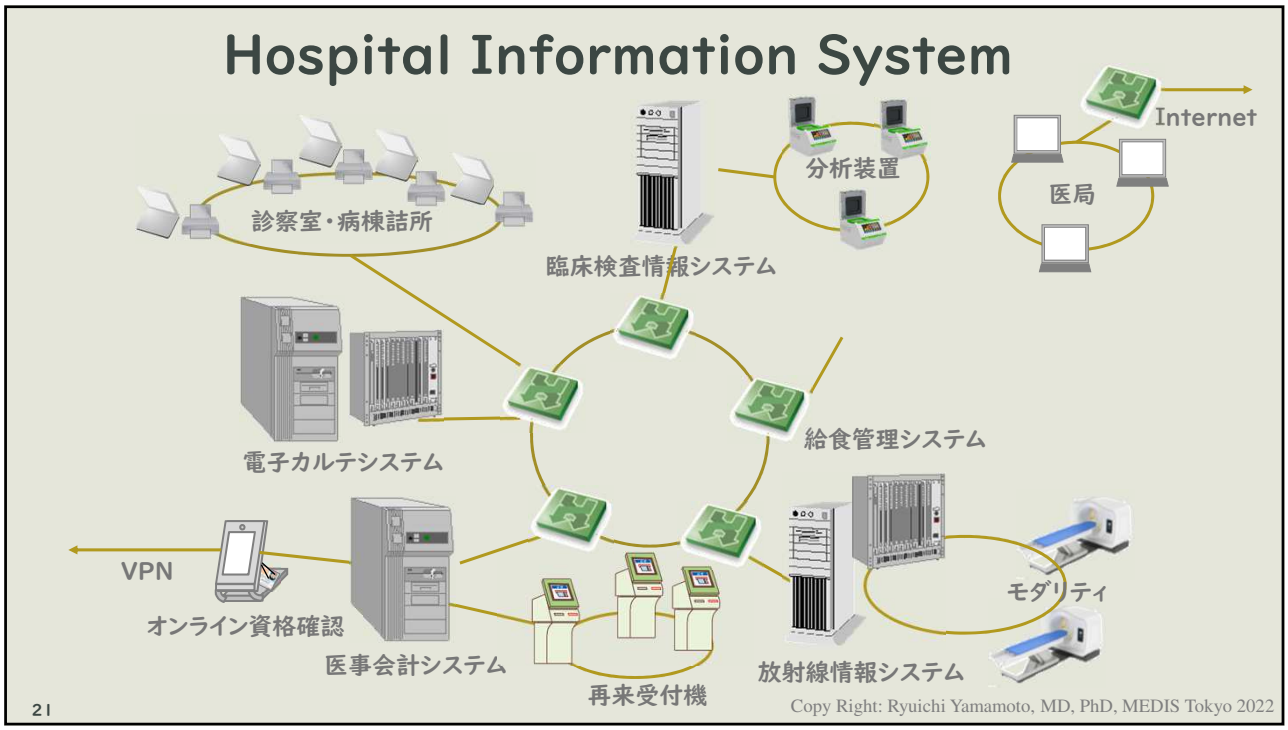


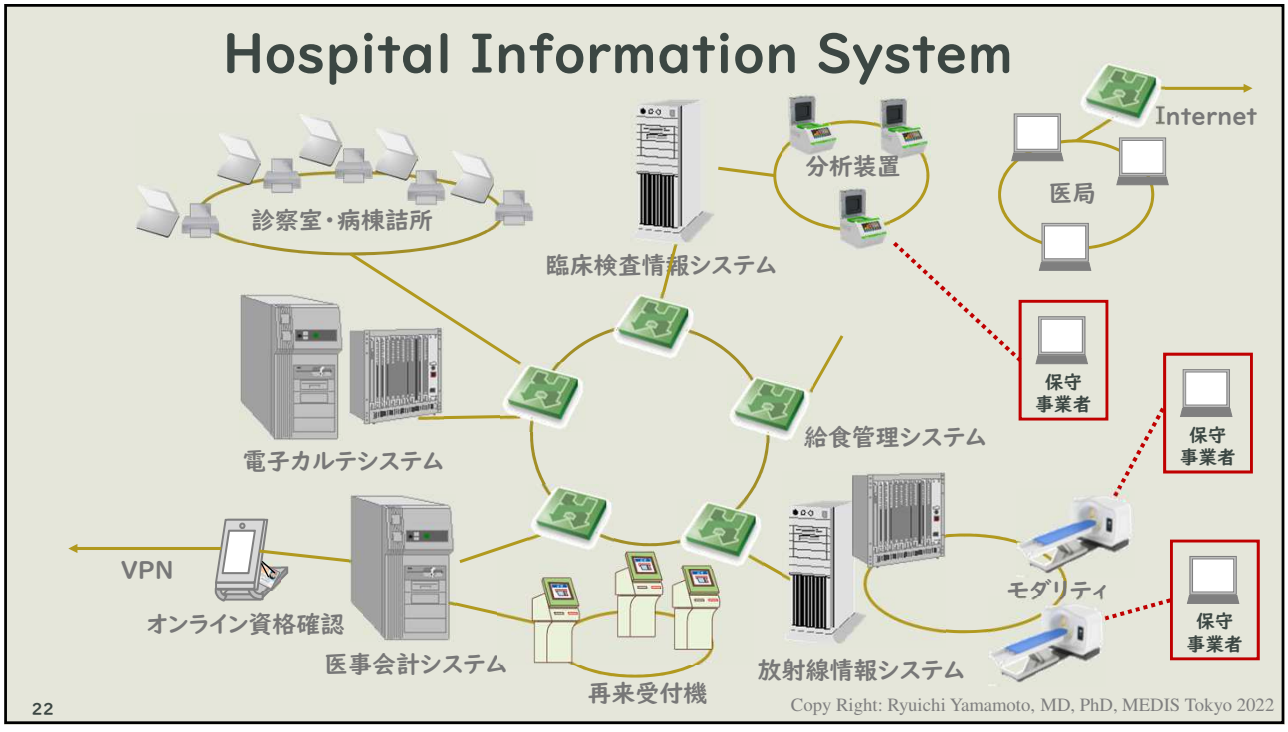
Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022

医療機関のガバナンス構造

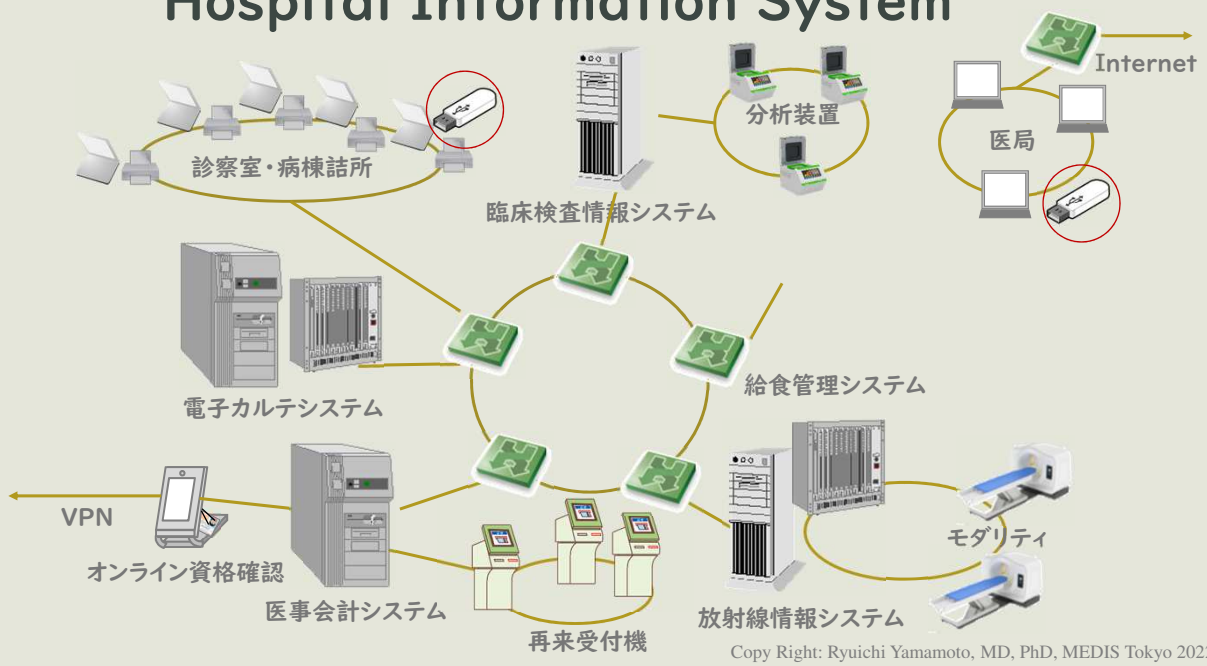


Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022


Hospital Information System
Internet
分析装置
医局
診察室・病棟詰所
臨床検査情報システム
電子カルテシステム
給食管理システム
VPN
オンライン資格確認
医事会計システム
再来受付機
モダリティ
放射線情報システム
21
Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022


Hospital Information System
Internet
分析装置
医局
診察室・病棟詰所
臨床検査情報システム
保守
事業者
保守
事業者
電子カルテシステム
給食管理システム
VPN
オンライン資格確認
医事会計システム
再来受付機
モダリティ
保守
事業者
放射線情報システム
22
Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022

Hospital Information System



Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022

CyberSecurity

組織的対策　ガバナンスの確立を確実にするモデルセキュリティポリシー

人的対策　　教育・訓練（不要な添付ファイル付きやURL埋め込みのメール）

技術的対策

- バックアップをさらに具体的に
- EDR
- 仮想ブラウザ
- クラウドシステム前提の技術対策

APIベースの情報システム連携が増えるので、ゼロトラストセキュリティの考え方の適切な導入などとともに6版の宿題

Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022

電子署名の活用促進

6.12章

25

ご清聴ありがとうございました。

Copy Right: Ryuichi Yamamoto, MD, PhD, MEDIS Tokyo 2022

26