医療機関の情報セキュリティリスク対応に関する研究

The Study of Information Security Risk Treatment on Healthcare Institutions

新水美代子　マネジメント分科会　情報セキュリティ大学院大学

Abstract:While digitalization is ongoing in medical institutions, cyber incidents have been occurring, and information security is strongly required. It seemed risk treatments by healthcare institutions were not enough. Therefore, the research with actual cyber incidents shows that the intrusion to the system was from network or e-mail. The causes and background factors of cyber-attacks were considered for risk treatments using the guidelines. As a result, it is necessary to treat the entire network for reduce vulnerabilities with security knowledge. Recommendations are made for healthcare institutes to obtain the knowledge for configuring a secure network of hospital systems and for Japanese government to support them for it.

背景

- 医療機関や医療はIT化が進んでいる. 法やガイドラインも整備されている
- しかしながら医療機関における情報漏えいだけではない情報セキュリティの事故事件も発生している

医療機関はサイバーセキュリティリスク対応が不足しているのではないか

【医療情報】＊診療の継続に必須　＊患者情報保護　＊公文書保管義務

公開情報からサイバーセキュリティの事件事故を調査

期間：2011/1～2022/3

インターネットの公開調査で医療機関で起こった事件事故のニュース256件を収集

調査結果からICT系（通信上の情報やサーバ等に保存されている情報など, 情報そのものに対して起きた事故）は85件, 物系（PCや可搬型媒体）の事件事故は171件

ICT系事件事故のうち**サイバー攻撃の事件は49件**

種類	媒体	件数	%
ICT	ネットワーク	17	20.0%
	eメール	17	20.0%
	Webサイト	15	17.6%
	システム	13	15.3%
	電子カルテ	9	10.6%
	医療機器	3	3.5%
	FAX	2	2.4%
	PC	2	2.4%
	データ＊	2	2.4%
	電話	2	2.4%
	SNS	2	2.4%
	検査機器	1	1.2%
総計		85	100.0%

46件の事例を医療情報システムの安全管理に関するガイドライン第5.2版 6.5. 技術的安全対策と照合
リスク対策が必要な項目を確認→「不正ソフトウェア対策」「ネットワーク上からの不正アクセス」

14件が診療業務に影響

電子カルテ・検査機器が利用できない
受付・会計システムが利用できない

クローズドネットワークだったはずなのに

・医療システムネットワークが外部とつながっていた（VPN機器に脆弱性）
・セキュリティソフトが最新でなかった

調査のまとめ:

- オープンなWebサイト、eメールだけでなく医療情報システムにも不正アクセスが行われていた
  →クローズドネットワークになっていなかった
- ガイドライン「不正ソフトウェア対策」,「ネットワーク上からの不正アクセス」が優先的に行うリスク対応

本研究のまとめ:

- サイバーセキュリティのリスク対応として着目すべき点が明らかになった
- 患者の医療安全に影響するリスクとして対応すべき
- 技術的な実際の対策は保守業者等のベンダーが行うが, 医療機関はその影響に対して患者に責任を負う　→経営側が技術的リスク対応の実施をリードして進める必要性

国に技術的な知識やリソースを医療機関が持つための公的支援が必要