「電子カルテシステム等のセキュリティ対策状況について」報告

20230202

日本病院会会員病院に対して標記調査を実施した集計結果を下記のとおり報告いたします。

日本病院会　ICT 推進委員会　委員長　大道道大

●調査目的：会員病院のセキュリティ対策の状況を把握し、今後のセキュリティ対策に役立てる

●調査方法：Google フォーム〔会員病院（2,453 病院）あてに E メールまたは FAX にて URL を連絡〕

●調査期間：2022 年 11 月 24 日～12 月 13 日

●回 答 数：382 病院（回答率 15.6%）

●そ の 他：回答病院の中で脆弱性があるとされる機器を使用している病院へは個別に注意喚起を行った。

「調査のまとめ」

・今回の回答病院のうち、97.6%は院内システムへのベンダによるリモートメンテナンスを行わせているものの、そのうち 25.0%はメンテナンス用の機器・製品・バージョン情報を把握していない状況。

・2022 年 10 月に深刻な脆弱性が報告された Fortinet 社のリモートメンテナンス製品・機器の利用率は 7.0%と少なく、かつ、該当病院において脆弱性対応が既に完了していると回答した病院は全体の 89.4%に及んでおり、Fortinet 社製品の脆弱性へのリスク認識が高く、それゆえ適切な対応が図られている状況が見受けられる。

・一方で、Fortinet 社製品以外のリモートメンテナンス機器・製品については、種別・バージョン情報等を把握しているものの 22.6%の病院が特段脆弱性対応を実施していない状況である。そのため、Fortinet 社以外の機器の脆弱性を悪用したサイバー攻撃が発生するリスクはまだ根強く残存していることが把握できる。

・ベンダとの間で医療機関としてセキュリティ上の役割・責任分担を定め、契約等で合意形成している病院は全体の 20.0%にしか満たず、さらにセキュリティ等の情報提供も含めた報告を定期的に行わせている病院は 45.0%にしか満たない。

・さらにベンダの報告内容が医療機関の職員にとって理解しやすい水準で整理され、提供されていると回答した組織は 58.5%だが、4 割程度はその内容は理解しづらく、満足していない状況であった。

・病床規模別でみると、基本的にリモートメンテナンス導入率、及びリモートメンテナンス製品情報の把握率ともに、病床規模が大きいほど高くなる傾向がある。

・Fortinet 社製品の利用率は今回の調査結果からは、いずれの病床規模区分においても利用率は低く、さらに利用している病院においてほぼ 2022 年 10 月の深刻な脆弱性対応は完了している状況である。

・一方、Fortinet 社以外のリモートメンテナンス機器の種別・バージョン情報等を把握しているにもかかわらず、脆弱性の対応を最新情報に基づき実施していない病院は病床規模が小さいほど多くみられる傾向であり、病床の小さい病院に Fortinet 社以外の製品を用いたリモートメンテナンス機器の脆弱性が悪用される危険性があると言える。

・電カルベンダとの間でセキュリティに係る契約締結は全体の 2 割程度しか行われていない。電カルベンダからの運用報告の確認は医療機関の半数程度が行っているが、その内容の分かりやすさ・セキュリティ上の有用性にはベンダごとに差があることがわかる。

■記入者の部署、役職の内訳

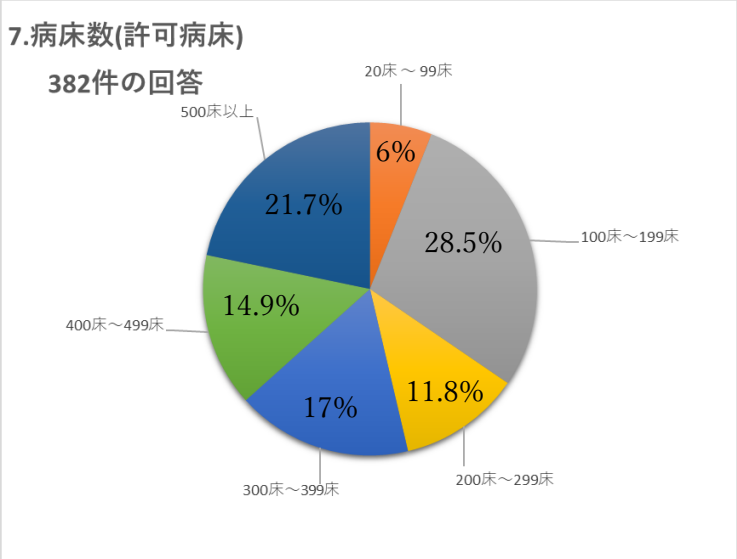
記入者の部署／役職	
情報、システム	289
総務、庶務	51
その他	42
合計	382

■都道府県、開設主体、病床数

都道府県									
北海道	11	埼玉県	10	岐阜県	8	鳥取県	2	佐賀県	3
青森県	6	千葉県	17	静岡県	25	島根県	3	長崎県	6
岩手県	7	東京都	26	愛知県	23	岡山県	7	熊本県	4
宮城県	7	神奈川県	14	三重県	10	広島県	8	大分県	1
秋田県	9	新潟県	8	滋賀県	5	山口県	5	宮崎県	0
山形県	3	富山県	3	京都府	9	徳島県	0	鹿児島県	0
福島県	3	石川県	3	大阪府	40	香川県	6	沖縄県	1
茨城県	15	福井県	3	兵庫県	15	愛媛県	3	合計	382
栃木県	3	山梨県	2	奈良県	8	高知県	2		
群馬県	3	長野県	16	和歌山県	3	福岡県	16		

開設主体					
厚生労働省	0	地方独立行政法人	25	特定医療法人	8
独立行政法人国立病院機構	6	日赤	31	社会医療法人	43
国立大学法人	2	済生会	11	私立学校法人	14
独立行政法人労働者健康安全機構	5	北海道社会事業協会	0	社会福祉法人	18
国立研究開発法人	0	厚生連	24	医療生協	3
独立行政法人地域医療推進機構	11	健康保険組合及びその連合会	2	会社	5
国(その他)	0	国民健康保険組合	0	その他の法人	19
都道府県	20	公益法人	13	個人	1
市町村	56	医療法人	65	合計	382

回答病院の病床数は、100 床～199 床が最も多く（28.5%）、次いで 500 床以上の病院が（21.7%）、300 床～399 床（17.0%）、400～499 床（14.9%）、200～299 床（11.8%）、20～99 床（6.0%）の順となる。



■Q8、Q9.利用している電子カルテシステムベンダ、医事会計システムベンダについて

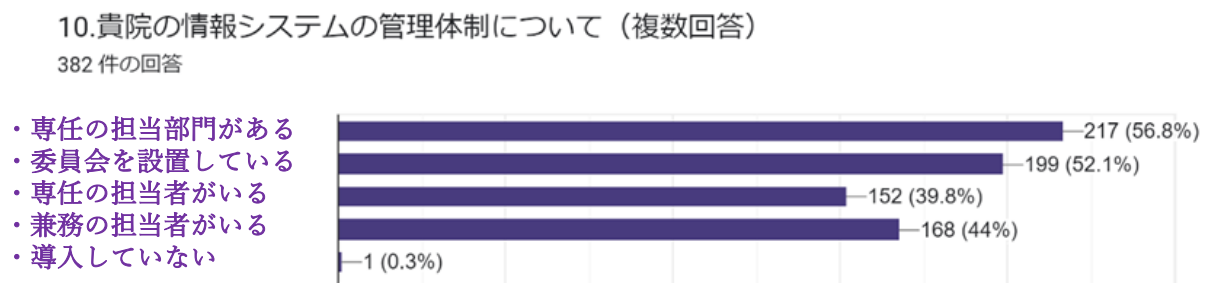
電子カルテシステム、医事会計システムともに富士通が最も多く、次いで電子カルテは、ソフトウェアサービス、医事ベンダは、NEC を使用している病院が多くみられた。なお回答の中で 13 病院が電子カルテシステム未導入、1 病院が医事会計システム未導入であった。（詳細は下記表のとおり）

電カルベンダ	
富士通	141
ソフトウェア・サービス	64
NEC	60
シーエスアイ	22
日本IBM	7
日本事務器	7
キヤノンメディカルシステムズ	7
亀田医療情報	5
ソフトマックス	4
ナイス	4
両備システムズ	3
医療情報システム	3
WorkVision	3
SBS情報システム	3
ワイズマン	2
日立システムズ	2
レスコ	2
大新技研	2
ＮＴＴデータ	2
アイシーエス	2
シグマソリューションズ	1
タック	1
その他のベンダ	19
富士通との共同開発	1
自院開発	1
非公開	1
未導入	13
合計	382

医事ベンダ	
富士通	146
ソフトウェア・サービス	64
NEC	74
シーエスアイ	2
日本IBM	0
日本事務器	13
キヤノンメディカルシステムズ	10
亀田医療情報	0
ソフトマックス	5
ナイス	15
両備システムズ	3
医療情報システム	4
WorkVision	5
SBS情報システム	3
ワイズマン	2
日立システムズ	3
レスコ	0
大新技研	0
NTTデータ	0
アイシーエス	1
シグマソリューションズ	3
タック	2
その他のベンダ	25
富士通との共同開発	0
自院開発	0
非公開	1
未導入	1
合計	382

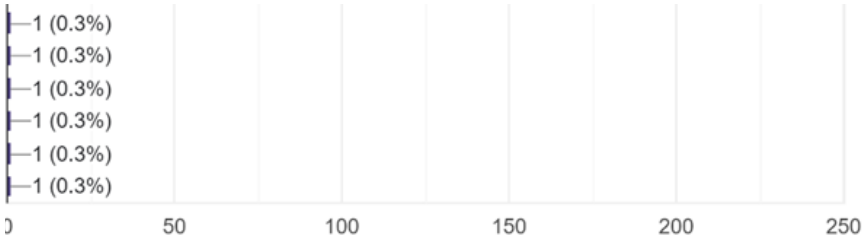
■Q10.情報システムの管理体制

「専任の担当部門がある」と回答したのは 217 病院、「委員会等を設置している」と回答したのは 199 病院、「専任の担当者がいる」と回答したのは、152 病院、「兼務の担当者がいる」と回答したのは 168 病院であった。情報システムの管理体制について、「導入していない」と回答したのは電子カルテ、医事会計システム未導入の１施設であり、「その他の管理体制」と回答したのは 6 病院であった。



［その他の管理体制］

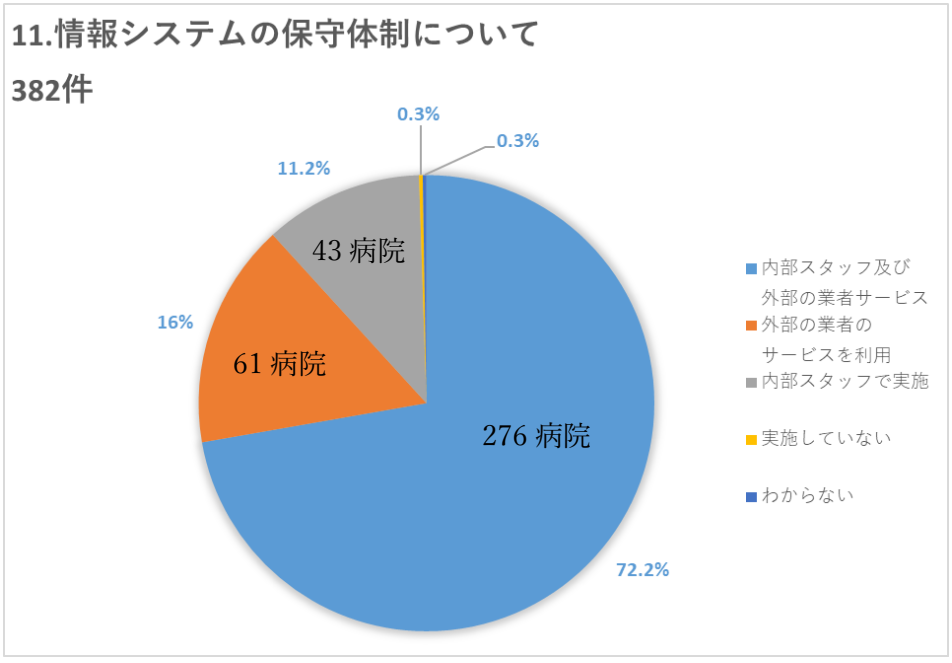
・事務部長が担当している
・外部の専門業者
・法人本部に専任担当者がいる
・兼務の課長がいる
・兼務の担当部署がある
・担当者ではないが
多少わかる人がいる



システム管理体制							
（複数回答）	病院数	20床～99床	100床～199床	200床～299床	300床～399床	400床～499床	500床以上
専任の担当部門がある	217	5	41	21	41	41	68
委員会等を設置している	199	3	55	23	36	32	50
専任の担当者がいる	152	3	38	15	22	28	46
兼務の担当者がいる	168	16	53	26	20	25	28

■Q11. 情報システムの保守体制について

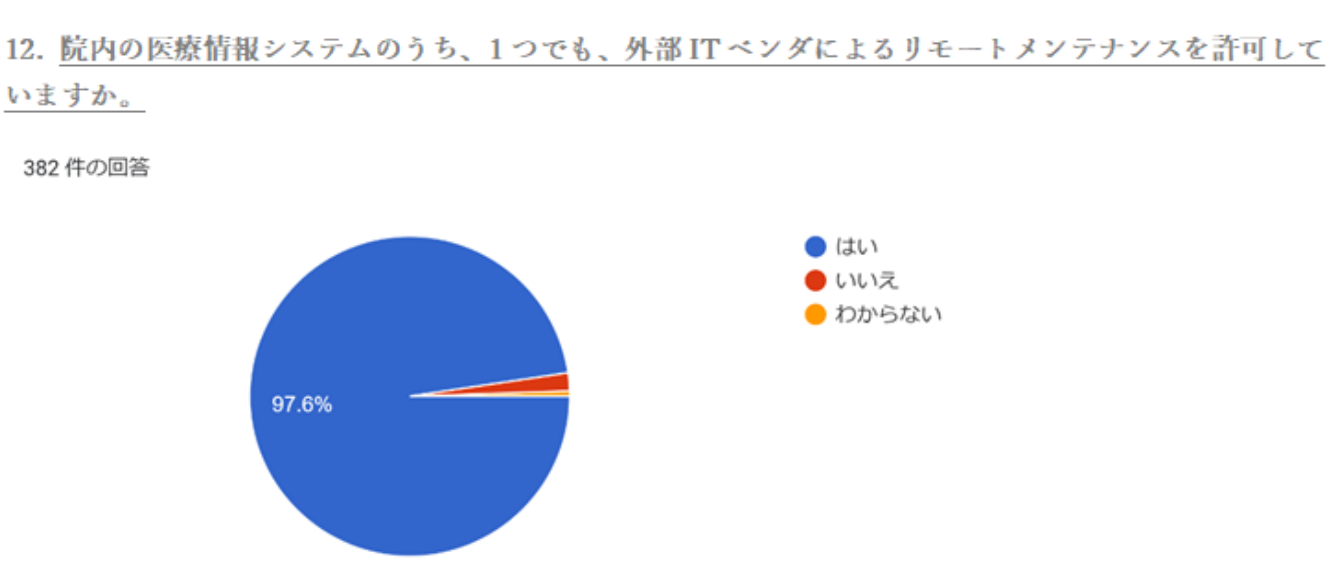
「内部スタッフ及び外部の業者サービスを利用している」と回答したのは 276 病院（72.2%）、「外部の業者のサービスを利用している」と回答したのは 61 病院（16.0%）、「内部スタッフで実施」と回答したのは、43 病院（11.2%）、「実施していない」は 1 病院、「わからない」は 1 病院であった。



システム保守体制							
	病床数	20床～99床	100床～199床	200床～299床	300床～399床	400床～499床	500床以上
内部スタッフおよび外部の業者サービス利用の両方で実施	276	15	68	31	49	40	73
外部の業者サービス利用のみで実施	61	6	25	7	8	9	6
内部スタッフのみで実施	43	2	14	7	8	8	4

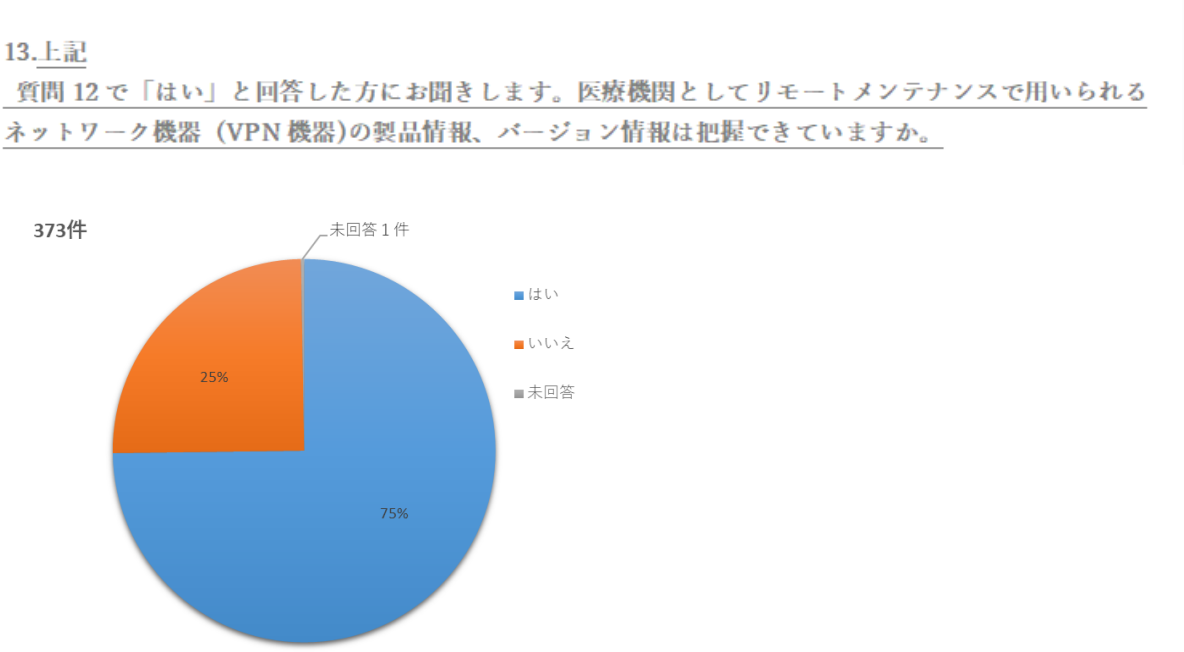
■Q12. 院内医療情報システムのリモートメンテナンスの許可、医療情報システムのバージョン情報の把握について

院内の医療情報システムのリモートメンテナンス許可の有無について373病院(97.6%)が許可をしていた。



■Q13. ネットワーク機器(VPN機器)の情報把握について

リモートメンテナンスを許可していると回答した373病院のうち、バージョン情報の把握が出来ていると回答したのは279病院（75.0%）でありバージョン情報の把握はできていなかったのは93病院（25.0%）だった。1病院は未回答だった。



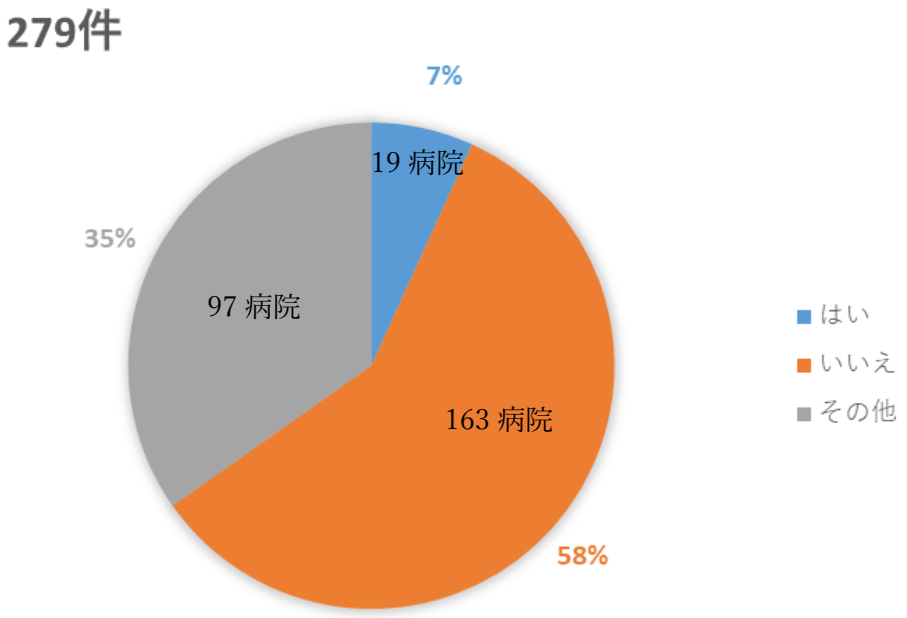
ネットワーク機器の情報把握について							
	病床数	100床以下	100床～199床	200床～299床	300床～399床	400床～499床	500床以上
把握できている	279	12	83	35	44	47	58
把握できていない	93	8	23	9	20	9	24

■Q14. 該当する Fortinet 社の製品を使用状況について

該当する製品・バージョンを使用していないと回答したのは 163 病院（58.0%）、該当の製品・バージョンを院内で使用している病院は 19 病院（7.0%）。
該当以外の Fortinet 社製製品を使用している病院は、97 病院（35.0%）であった。

14.上記
質問13で「はい」と回答した方にお聞きします。その製品はFortinet社による以下に該当する製品を一つでも含んでいますか。

・FortiOS バージョン7.2.0から7.2.1まで・FortiOS バージョン7.0.0から7.0.6まで
・FortiProxy バージョン7.2.0・FortiProxy バージョン7.0.0から7.0.6まで
・FortiSwitchManager バージョン7.2.0・FortiSwitchManager バージョン7.0.0



	病床数	20床 ～ 99床	100床～199床	200床～299床	300床～399床	400床～499床	500床以上
該当するForinet社製製品を使用している	19	1	3	1	4	3	7
Fortinet社製製品を使用していない	163	8	55	24	23	23	30
該当する製品ではないが、Fortinet社製製品を使用している	97	3	25	10	17	21	21

■Q15. 2022 年 10 月に告知された脆弱性について、外部 IT ベンダに対応指示を行う、あるいは外部 IT ベンダから報告への対応

外部 IT ベンダからの報告に従い対応を行っていると回答したのは 17 病院(89%)、対応を行っていない病院は 2 病院(11%)であった。

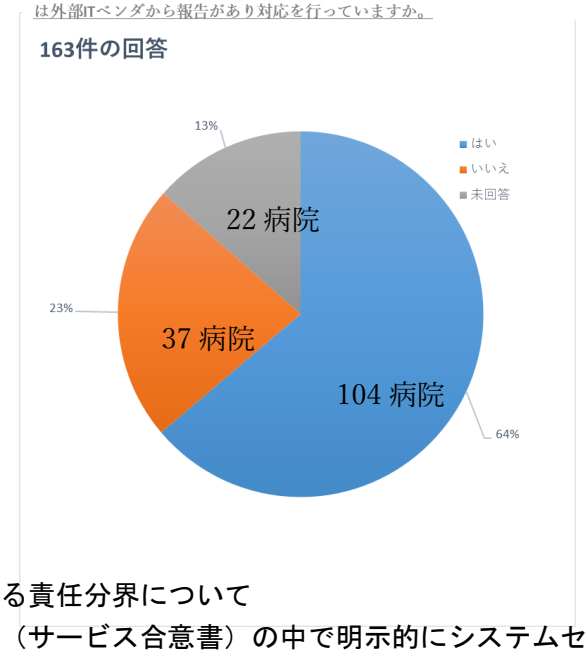
外部ITベンダからの報告に従い対応を行っているか	病床数	100床以下	100床～199床	200床～299床	300床～399床	400床～499床	500床以上
対応を行っている	17	1	3	1	3	3	6
対応を行っていない	2	0	0	1	1	0	0

■Q16. 該当する機器への脆弱性パッチ適用の対応について

該当する機器の脆弱性パッチ適用の対応を行っているのは 104 病院(64%)、対応を行っていない病院は 37 病院(23%)。22 病院(13%)が未回答。

16.上記
質問14で「いいえ」と回答した方にお聞きします。Fortinet社以外のリモートメンテナンス用のVPN機器を利用している場合、該当する機器の脆弱性パッチ適用を最新情報に基づき、自院として外部ITベンダに対応指示を行う、あるいは外部ITベンダから報告があり対応を行っていますか。

163件の回答

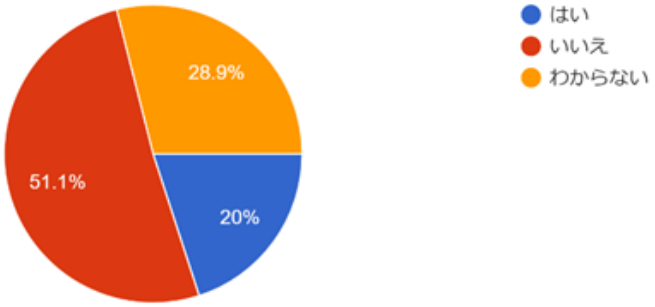


■Q17. システムセキュリティに関する責任分界について

外部 IT ベンダとの契約書・SLA（サービス合意書）の中で明示的にシステムセキュリティに関する責任分界を取り交わしていると回答したのは 76 病院(20%)、取り交していない病院は 194 病院(51.1%)であった。

17.
医療機関として、電子カルテシステムや医事会計システム等、患者診療/医療経営の継続性に影響を及ぼす医療情報システムの保守管理について、外部 IT ベンダとの契約書・SLA（サービス合意書）の中で明示的にシステムセキュリティに関する責任分界（リモートメンテナンス機器のセキュリティパッチ適用は外部 IT ベンダの責任である旨の明記等）を取り交わしていますか。

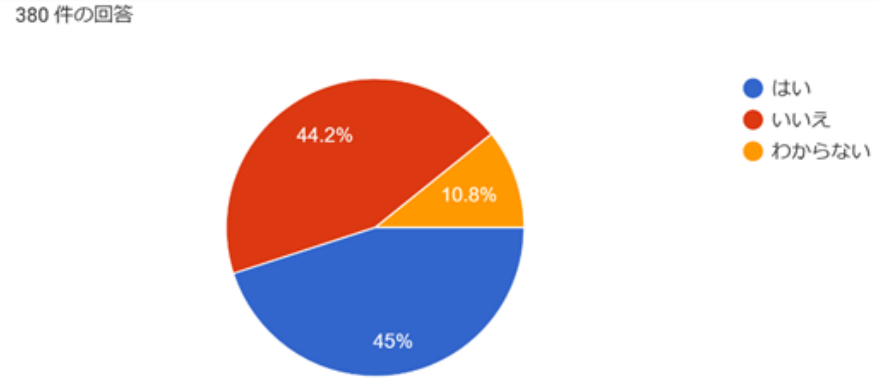
380 件の回答



■Q18. 厚生労働省「医療情報システムの安全管理に関するガイドライン」に基づく外部 IT ベンダからの報告への対応について

厚生労働省「医療情報システムの安全管理に関するガイドライン」に基づき、外部 IT ベンダから報告を受け、内容の確認を行っている病院は、171 病院（45.0%）、行っていない病院は、168 病院（44.2%）、わからないと回答した病院は、41 病院（10.8%）であった。

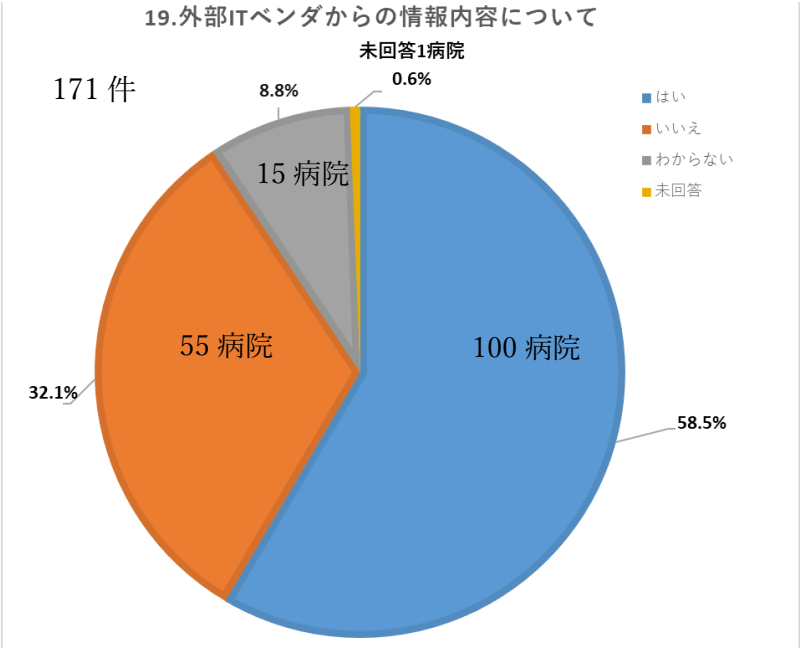
18.
厚生労働省「医療情報システムの安全管理に関するガイドライン」に基づき、医療情報システムを提供する外部 IT ベンダから、システムの開発・保守、運用状況を含めて、システム・機器の脆弱性対応も含めて、一定の頻度（定期的）に基づき、医療機関として報告を受け、内容の確認を行っていますか。



■Q19. 外部 IT ベンダからの情報内容について

外部 IT ベンダからの情報が分かりやすいと回答した病院は、100 病院（58.5%）であった。

19.上記
質問 18 で「はい」と回答した方にお聞きします。 外部 IT ベンダからの情報は、院内の医療情報システムのセキュリティを向上・改善するに資する、分かりやすく役に立つ報告内容の水準となっていますか。（ベンダ目線で運用状況をテクニカルに報告した内容のみで、医療機関の IT 担当者やマネジメント層にとっては理解に悩む、一方通行的で、読解が困難な内容になっていませんか）



担当事務局：日本病院会　情報統計課

2022 年 11 月 24 日

日本病院会 会員病院 各位

一般社団法人 日本病院会
ICT 推進委員会
委員長 大 道 道 大

ネットワーク(VPN)装置のソフトウェア更新とセキュリティ調査について

先般、大阪府内の病院において、ランサムウェアによるサイバー攻撃を受けて診療に支障をきたす事案が発生しました。この事案については、昨年 10 月にサイバー攻撃を受けた徳島県の「つるぎ町立半田病院」と同一で、Fortinet 社製のネットワーク(VPN)装置のソフトウェアの更新が行われておらず、脆弱性の高い状態であったと報道されています。

Fortinet 社製の VPN 装置については、別添のとおり「管理インターフェースへのアクセスにおける認証バイパスの脆弱性が見つかり、対策済み OS へのバージョンアップを行うよう」通知がされているところです。

つきましては、Fortinet 社製のネットワーク機器(VPN)の使用の有無をご確認いただき適切にご対応くださいますようご連絡申しあげます。

なお、今後のセキュリティ対策に役立てるため、各病院の電子カルテシステム等のセキュリティ対策状況について下記のとおり調査を行うことといたしましたので、ご協力の程よろしくお願い申しあげます。

記

1. 調 査 名　　電子カルテシステム等のセキュリティ対策状況について

2. 調査方法　　日本病院会の調査 URL により回答(記入・送信)をお願いします。

https://forms.gle/LPX6zSn6FoaYDk5u7

3. 締 切 日　　2022 年 12 月 9 日(金)

4. 問合せ先　　一般社団法人 日本病院会 情報統計課
TEL:03-3265-0077
e-mail:joho@hospital.or.jp

《添付資料》

【脆弱性】FortiOS における認証バイパスの脆弱性(CVE-2022-40684)について
株式会社日立ソリューションズ Fortnet 製品ユーザーサポート

2022 年 10 月 12 日

お客様各位

株式会社日立ソリューションズ
Fortinet 製品ユーザサポート

【脆弱性】FortiOS における認証バイパスの脆弱性(CVE-2022-40684)について

拝啓、平素は Fortinet 製品サポートをご利用下さいまして誠にありがとうございます。

この度 Fortinet 社より、深刻度の高い脆弱性として、FortiOS の管理インターフェースへのアクセスにおける認証バイパスの脆弱性(CVE-2022-40684)がアナウンスされています。本脆弱性の影響を受けるバージョンをご利用のお客様は、対策済み OS へのバージョンアップ、若しくは回避策・緩和策の適用について、ご検討をお願いいたします。

敬具

記

1. 事象の概要

FortiOS において、管理インターフェースへのアクセス時の認証がバイパス可能となる脆弱性が見つかりました。これにより、攻撃者が細工した HTTP/HTTPS リクエストを FortiGate の管理インターフェースに送信することにより、管理インターフェースアクセス時の認証が行われなくなる可能性があります。

Fortinet 社からは、既にこの脆弱性を悪用した攻撃が確認されていること、および緊急での対処が必要である旨が、アナウンスされています。

詳細、最新の情報については Fortinet 社から発表されています以下セキュリティアドバイザリ(PSIRT Advisories)をご覧ください。

FortiOS / FortiProxy / FortiSwitchManager - Authentication bypass on administrative interface
<https://www.fortiguard.com/psirt/FG-IR-22-377>

2. 該当製品と対策バージョン

脆弱性の影響を受けるバージョン、及び対策バージョンは以下の通りです。
影響を受けるバージョンをご利用中の場合は、対策済み OS へのバージョンアップをお願いいたします。

項	メジャーバージョン	影響を受けるバージョン	対策バージョン	備考
1	FortiOS 7.2 系	7.2.0 ～ 7.2.1	7.2.2 以降	弊社からは未リリースのバージョンです。
2	FortiOS 7.0 系	7.0.0 ～ 7.0.6	7.0.7(※)以降	7.0.0 および 7.0.1 は弊社から未リリースのバージョンです。
3	FortiOS(6000 シリーズ) 7.0 系	7.0.5	－	弊社からは未リリースのバージョンです。

※ 2022 年 10 月 11 日に弊社からリリース済です。

3. 回避策および緩和策

脆弱性の回避策と緩和策は以下の通りです。なお、緩和策により IP アドレスを制限した後も、該当 IP アドレスからのアクセスには脆弱性が残るため、早急に対策バージョンへのアップグレードの検討をお願いいたします。

回避策

FortiGate の管理インターフェースにおいて、HTTP/HTTPS によるアクセスを無効化することにより、本脆弱性の回避可能です。なお、本回避策を適用すると、WebUI を使用した管理アクセスが出来なくなります。

緩和策

FortiGate の管理インターフェースへのアクセス元の IP アドレスを制限することにより、本脆弱性の影響の緩和が可能です。

FortiGate の管理インターフェースへのアクセス元の IP アドレスの制限方法については、セキュリティアドバイザリ掲載の Workaround をご覧ください。

4. OS ファイルの入手方法

バージョンアップは、対象機器がインターネットに接続している場合は、GUI で OS のダウンロード、及びバージョンアップを行うことができます。

OS ファイルがご入用の場合は、弊社サポートからご提供しております。対象機器のシリアル番号（S/N）と共に、現在のバージョン、バージョンアップ先のバージョンをご連絡ください。

5. Fortinet 社セキュリティアドバイザリ

Fortinet 社では、脆弱性情報を以下、FortiGuard Labs PSIRT Advisories で公開しています。最新の脆弱性情報は以下サイトをご覧頂き、適時ご利用環境の対策をいただきますようお願いします。

尚、同サイト記載内容以上の情報は開示されていません。記載内容の解釈また内容等については、弊社サポートではお答えいたしかねます。予めご了承ください。

PSIRT Advisories は RSS 配信も行われていますので、合わせてご活用ください。

FortiGuard Labs PSIRT Advisories
<https://www.fortiguard.com/psirt>

FortiGuard Labs RSS Feeds
<https://www.fortiguard.com/rss-feeds>

以上

電子カルテシステム等のセキュリティ対策状況について

この度は、当調査へのご協力をいただきましてありがとうございます。

【期間】2022 年 12 月 9 日(金)まで

●重複して回答されますと調査結果の正確性が損なわれるため回答は 1 回のみでお願いいたします。

●設問は全 19 問あります。

※ご回答いただいた内容は、本調査の集計目的に利用し個別の病院名および個人が特定されるような処理・取り扱いは一切いたしません。注意喚起、問い合わせなど必要な場合は連絡をさせていただきますことご承知のほどお願いいたします。

■メールアドレス ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

■貴院についてお伺いいたします。

1. 医療機関名 ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

2. 都道府県名（選択） ＿＿＿＿＿＿＿＿

3. 電話番号(ハイフンなしの記入をお願いいたします) ＿＿＿＿＿＿＿＿＿＿＿＿

4. 記入者の部署/役職 ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

5. 記入者名 ＿＿＿＿＿＿＿＿＿＿＿＿

6. 開設主体（選択） ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

7. 病床数(許可病床数) ＿＿＿＿＿＿＿＿

8. ご利用の「電子カルテシステムベンダ」をご記入ください。

9. ご利用の「医事会計システムベンダ」をご記入ください。

■貴院でのセキュリティ対策についてお伺いいたします。

10. 貴院の情報システムの管理体制について（複数回答）

□専任の担当部門がある　□委員会等を設置している　□専任の担当者がいる
□兼務の担当者がいる　　□その他

11. 貴院の情報システムの保守体制を選択してください。

□内部スタッフで実施　□外部の業者のサービスを利用
□内部スタッフ及び外部の業者サービス　□実施していない　□わからない

12. 院内の医療情報システムのうち、1 つでも、外部 IT ベンダによるリモートメンテナンスを許可していますか。

□はい　□いいえ　□わからない

13. 上記 質問 12 で「はい」と回答した方にお聞きします。医療機関としてリモートメンテナンスで用いられるネットワーク機器(VPN 機器)の製品情報、バージョン情報は把握できていますか。

□はい　□いいえ

14. 上記 質問 13 で「はい」と回答した方にお聞きします。その製品は Fortinet 社による以下に該当する製品を一つでも含んでいますか。

FortiOS バージョン 7.2.0 から 7.2.1 まで／FortiOS バージョン 7.0.0 から 7.0.6 まで
FortiProxy バージョン 7.2.0／FortiProxy バージョン 7.0.0 から 7.0.6 まで
FortiSwitchManager バージョン 7.2.0／FortiSwitchManager バージョン 7.0.0

□はい
□その他（上記以外の、Fortinet 社製製品をご使用の場合は、製品名・バージョンを下記にご記入ください）
□いいえ

上記以外の、ご使用の Fortinet 社製製品

15. 上記 質問 14 で「はい」と回答した方にお聞きします。 2022 年 10 月に告知された脆弱性について、自院として外部 IT ベンダに対応指示を行う、あるいは外部 IT ベンダから報告があり対応を行っていますか。

□はい　□いいえ

いいえ理由

16. 上記 質問 14 で「いいえ」と回答した方にお聞きします。 Fortinet 社以外のリモートメンテナンス用の VPN 機器を利用している場合、該当する機器の脆弱性パッチ適用を最新情報に基づき、自院として外部 IT ベンダに対応指示を行う、あるいは外部 IT ベンダから報告があり対応を行っていますか。

□はい □いいえ

17. 医療機関として、電子カルテシステムや医事会計システム等、患者診療/医療経営の継続性に影響を及ぼす医療情報システムの保守管理について、外部 IT ベンダとの契約書・SLA（サービス合意書）の中で明示的にシステムセキュリティに関する責任分界（リモートメンテナンス機器のセキュリティパッチ適用は外部 IT ベンダの責任である旨の明記等）を取り交わしていますか。

□はい □いいえ □わからない

18. 厚生労働省「医療情報システムの安全管理に関するガイドライン」に基づき、医療情報システムを提供する外部 IT ベンダから、システムの開発・保守、運用状況を含めて、システム・機器の脆弱性対応も含めて、一定の頻度（定期的）に基づき、医療機関として報告を受け、内容の確認を行っていますか。

□はい □いいえ □わからない

19. 上記 質問 18 で「はい」と回答した方にお聞きします。 外部 IT ベンダからの情報は、院内の医療情報システムのセキュリティを向上・改善するに資する、分かりやすく役に立つ報告内容の水準となっていますか。（ベンダ目線で運用状況をテクニカルに報告した内容のみで、医療機関の IT 担当者やマネジメント層にとっては理解に悩む、一方通行的で、読解が困難な内容になっていませんか）

□はい □いいえ □わからない

その他、ご意見等ございましたら記入をお願いいたします。

回答が終わりましたら、左下の「送信」ボタンを押してください。