施設、組織体制

別添資料 3.

都道府県	施設数	都道府県	施設数	都道府県	施設数	都道府県	施設数
北海道	26	東京都	34	滋賀県	9	香川県	7
青森県	6	神奈川県	25	京都府	7	愛媛県	9
岩手県	6	新潟県	11	大阪府	45	高知県	5
宮城県	6	富山県	9	兵庫県	16	福岡県	26
秋田県	6	石川県	6	奈良県	9	佐賀県	2
山形県	5	福井県	5	和歌山県	10	長崎県	11
福島県	6	山梨県	7	鳥取県	3	熊本県	24
茨城県	12	長野県	11	島根県	5	大分県	6
栃木県	9	岐阜県	11	岡山県	10	宮崎県	5
群馬県	9	静岡県	15	広島県	13	鹿児島県	8
埼玉県	17	愛知県	29	山口県	9	沖縄県	7
千葉県	21	三重県	11	徳島県	1	合計	550

	施設数	割合
国公立大学病院	25	4.5%
公的な医療機関（大学病院を除く）	216	39.3%
私立大学病院	13	2.4%
私立の医療機関	296	53.8%

	施設数	割合
特定機能病院	35	6.4%
地域医療支援病院	154	28.0%
災害拠点病院（基幹）	41	7.5%
災害拠点病院（地域）	132	24.0%
第三次救急医療機関	87	15.8%
第二次救急医療機関	259	47.1%
総合周産期母子医療センター	30	5.5%
地域周産期母子医療センター	57	10.4%
小児中核病院	17	3.1%
小児地域医療センター	13	2.4%
小児地域支援病院	6	1.1%
上記の認定、指定は受けていない	185	33.6%

病床数	施設数	割合
1000床以上	6	1.1%
800床以上1000床未満	20	3.6%
600床以上800床未満	39	7.1%
400床以上600床未満	84	15.3%
300床以上400床未満	67	12.2%
200床以上300床未満	87	15.8%
100床以上200床未満	170	30.9%
100床未満	77	14.0%

診療録管理体制加算	施設数	割合
加算1	185	33.6%
加算2	127	23.1%
加算3	199	36.2%
算定していない	39	7.1%

医療情報部門の設置	施設数	割合
はい	440	80.0%
いいえ	110	20.0%

専門知識を有する情報セキュリティ人材	施設数	割合
高度な専門知識（IPA ITスキル標準レベル4以上相当）を有する情報セキュリティ人材を配置している	29	5.3%
専門知識を有する情報セキュリティ人材を配置している	209	38.0%
配置していない	312	56.7%

診療録の電子的保管	施設数	割合
はい	502	91.3%
いいえ	48	8.7%

【医療情報システム安全管理責任者を設置している。(1-(1))】

情報セキュリティ責任者（CISO: Chief Information Security Officer）、医療情報システム安全管理責任者の配置	施設数	割合
① 情報セキュリティ責任者（CISO）と医療情報システム安全管理責任者を配置（別の人物）	190	34.5%
② 情報セキュリティ責任者（CISO）のみ配置（医療情報システム安全管理責任者は配置せず）	11	2.0%
③ 情報セキュリティ責任者（CISO）・医療情報システム安全管理責任者（同一人物）を配置	212	38.5%
④ 医療情報システム安全管理責任者を配置（情報セキュリティ責任者（CISO）は配置せず）	102	18.5%
⑤ 配置していない	35	6.4%

知識	①CISO		①管理責任者		②CISO		③管理責任者		④管理責任者	
高度な専門知識（IPA ITスキル標準レベル4以上相当）を有しており、単独でも対策を進めることができる	4	2.1%	8	4.2%	0		6	2.8%	0	
一定の専門知識を有しており、単独でも対策を進めることができる	21	11.1%	35	18.4%	0		32	15.1%	4	3.9%
一定の専門知識を有しているが、対策には情報セキュリティ人材のサポートが必要である	77	40.5%	90	47.4%	6	54.5%	129	60.8%	57	55.9%
ほとんど知識を有していない	76	40.0%	53	27.9%	5	45.5%	40	18.9%	31	30.4%
全く知識を有していない	12	6.3%	4	2.1%	0		5	2.4%	10	9.8%

職位	①CISO		①管理責任者		②CISO		③管理責任者		④管理責任者	
上部組織の理事など	12	6.3%	0		0		0		0	
医療機関の責任者（院長など）	83	43.7%	29	15.3%	4	36.4%	55	25.9%	27	26.5%
院長を補佐する立場（副院長、院長補佐など）	17	8.9%	25	13.2%	1	9.1%	20	9.4%	11	10.8%
医療情報システム管理部門の長	18	9.5%	60	31.6%	2	18.2%	60	28.3%	25	24.5%
医療情報システム管理部門（部門長以外）	3	1.6%	17	8.9%	0		8	3.8%	7	6.9%
事務部門の長	41	21.6%	32	16.8%	2	18.2%	39	18.4%	14	13.7%
事務部門（部門長以外）	6	3.2%	16	8.4%	1	9.1%	17	8.0%	7	6.9%
上記以外の部門の長	7	3.7%	7	3.7%	0		6	2.8%	7	6.9%
上記以外の部門（部門長以外）	3	1.6%	4	2.1%	1	9.1%	7	3.3%	4	3.9%

医療系資格	①CISO		①管理責任者		②CISO		③管理責任者		④管理責任者	
医師・歯科医師	105	55.3%	75	39.5%	5	45.5%	80	37.7%	46	45.1%
看護師・助産師・保健師	0		1	0.5%	0		0		1	1.0%
薬剤師	0		0		0		2	0.9%	2	2.0%
診療放射線技師	2	1.1%	7	3.7%	1	9.1%	8	3.8%	1	1.0%
臨床検査技師	0		3	1.6%	0		2	0.9%	0	
臨床工学技士	0		2	1.1%	0		1	0.5%	0	
医学物理士	0		0		0		0		0	
医療情報技師（上級医療情報技師を含む）	9	4.7%	29	15.3%	1	9.1%	35	16.5%	10	9.8%
診療情報管理士	10	5.3%	16	8.4%	2	18.2%	14	6.6%	9	8.8%
リストされる医療系資格を保持していない	69	36.3%	76	40.0%	3	27.3%	80	37.7%	37	36.3%

IPA資格	①CISO		①管理責任者		②CISO		③管理責任者		④管理責任者	
情報処理安全確保支援士（登録情報セキスペ）	0		2	1.1%	0		0		0	
情報処理安全確保支援士（資格試験合格のみ）	0		1	0.5%	0		1	0.5%	0	
応用技術者試験	3	1.6%	3	1.6%	0		3	1.4%	2	2.0%
基本情報技術者試験	7	3.7%	13	6.8%	0		22	10.4%	7	6.9%
情報セキュリティマネジメント試験	1	0.5%	9	4.7%	0		8	3.8%	0	
ITパスポート試験	9	4.7%	9	4.7%	0		9	4.2%	3	2.9%
リストされる資格・試験は保持していない	178	93.7%	162	85.3%	11	100.0%	178	84.0%	92	90.2%

CISO、安全管理責任者を配置しない理由	施設数	割合
許可病床数が200床以上であるが、医療情報システム安全管理責任者に適任な人材がいないから	7	20.0%
許可病床数が200床未満で、医療情報システム安全管理責任者に適任な人材がいないから	21	60.0%
許可病床数が200床未満で、医療情報システム安全管理責任者の設置の必要性を感じないから	3	8.6%
電子カルテが未導入（現状診療録が紙カルテ）	2	5.7%
その他	2	5.7%

サイバーセキュリティ対策の方針を決定する際に関わる情報セキュリティ人材	施設数	割合
情報セキュリティ責任者（CISO）	248	45.1%
医療情報システム安全管理責任者	404	73.5%
院内に配置する高度な専門知識（IPA ITスキル標準レベル4以上相当）を有する情報セキュリティ人材	23	4.2%
院内に配置する専門知識を有する情報セキュリティ人材	151	27.5%
同一法人等の中央組織に配置する高度な専門知識（ITスキル標準レベル4以上相当）を有する情報セキュリティ人材	27	4.9%
同一法人等の中央組織に配置する専門知識を有する情報セキュリティ人材	79	14.4%
同一法人等の他医療機関に配置する高度な専門知識（ ITスキル標準レベル4以上相当）を有する情報セキュリティ人材	9	1.6%
同一法人等の他医療機関に配置する専門知識を有する情報セキュリティ人材	17	3.1%
保守契約を結ぶ医療情報システムベンダー（情報セキュリティの知識を有することを確認している）	186	33.8%
保守契約を結ぶ医療情報システムベンダー（情報セキュリティの知識を有することを確認できていない）	94	17.1%
情報セキュリティ対策を専門とする企業等（医療情報システムベンダー以外）の情報セキュリティ人材	56	10.2%
その他	59	10.7%

【サーバ、端末PC、ネットワーク機器の台帳管理を行っている。(2- (1))

サーバーの台帳管理	施設数	割合
全ての機器を把握している	389	70.7%
全ての機器を把握していると思うが、漏れがあるかもしれない	136	24.7%
全ての機器を把握できていない	10	1.8%
ほとんどの機器を把握できていない	0	0.0%
台帳管理を行っていない	15	2.7%

サーバーの台帳管理者	施設数	割合
自施設の職員	414	77.4%
機器を導入した事業者（保守契約など）	101	18.9%
導入事業者以外の事業者	15	2.8%
その他	5	0.9%
合計	535	

サーバの台帳管理方法	施設数	割合
用紙運用	22	4.1%
エクセル等の汎用ソフトを使用	448	83.7%
専用のソフトを使用	51	9.5%
その他	14	2.6%
合計	535	

端末PCの台帳管理	施設数	割合
全ての機器を把握している	341	62.0%
全ての機器を把握していると思うが、漏れがあるかもしれない	181	32.9%
全ての機器を把握できていない	17	3.1%
ほとんどの機器を把握できていない	0	
台帳管理を行っていない	11	2.0%

端末PCの台帳管理者	施設数	割合
自施設の職員	469	87.0%
機器を導入した事業者（保守契約など）	47	8.7%
導入事業者以外の事業者	20	3.7%
その他	3	0.6%
合計	539	

端末PCの台帳管理方法	施設数	割合
用紙運用	18	3.3%
エクセル等の汎用ソフトを使用	427	79.2%
専用のソフトを使用	85	15.8%
その他	9	1.7%
合計	539	

ネットワーク機器の台帳管理	施設数	割合
全ての機器を把握している	265	48.2%
全ての機器を把握していると思うが、漏れがあるかもしれない	214	38.9%
全ての機器を把握できていない	41	7.5%
ほとんどの機器を把握できていない	4	0.7%
台帳管理を行っていない	26	4.7%

ネットワーク機器の台帳管理者	施設数	割合
自施設の職員	369	70.4%
機器を導入した事業者（保守契約など）	138	26.3%
導入事業者以外の事業者	14	2.7%
その他	3	0.6%
合計	524	

ネットワーク機器の台帳管理方法	施設数	割合
用紙運用	36	6.9%
エクセル等の汎用ソフトを使用	427	81.5%
専用のソフトを使用	45	8.6%
その他	16	3.1%
合計	524	

外部から医療情報システムに接続している回線

外部から医療情報システムネットワークに接続している回線の把握

	施設数	割合
全て把握している	388	70.5%
一部のみ把握している	134	24.4%
把握していない	28	5.1%

外部から医療情報システムネットワークに接続している回線数

回線数	全て把握	一部のみ把握	合計	回線数	全て把握	一部のみ把握	合計	回線数	全て把握	一部のみ把握	合計
0	11		11								
1	33	10	43	16	7	1	8	31		1	1
2	35	13	48	17	6	2	8	32		2	2
3	43	15	58	18	5		5	33	2		2
4	30	14	44	19	1	1	2	34		1	1
5	36	14	50	20	7	5	12	35		2	2
6	23	6	29	21	1	2	3	36	1		1
7	27	3	30	22	2	1	3	38		1	1
8	10	5	15	23	2		2	40	1		1
9	13	4	17	24	1		1	43	1		1
10	19	10	29	25	2	1	3	45	2		2
11	9	2	11	26	2	2	4	48	1		1
12	12	3	15	27	2	1	3	51	1		1
13	9	2	11	28	1	1	2	80	1		1
14	7	4	11	29	4		4	89	1		1
15	8	2	10	30	6	1	7	無回答	3	2	5
						回線数の平均			8.9	9.4	9.1
						11回線以上の割合			27.3%	28.8%	27.7%

外部から医療情報システムネットワークに接続している回線を減らす努力

	全て把握		一部のみ把握		把握していない		合計	
努力をしている	199	51.3%	49	36.6%	10	35.7%	258	46.9%
回線数を減らす必要性は感じているが、努力はできていない	114	29.4%	53	39.6%	13	46.4%	180	32.7%
回線数を減らす必要性は感じていない	75	19.3%	32	23.9%	5	17.9%	112	20.4%

適切に管理できる回線数

	回線数の把握			
回線数	全て把握	一部のみ把握	把握していない	総計
0	42	18	3	63
1	41	10	1	52
2	13	4		17
3	37	7	1	45
4	5	3		8
5	31	18		49
6	4	1		5
7	2			2
8	4			4
9	1			1
10	39	18	1	58
20	8	2		10
24	1			1
25	2			2
30	3	5		8
43	1			1
合計	234	86	6	326
回線数の平均	5.1	6.0	2.3	5.3

適切に管理できる回線数

	回線数を減らす努力			
回線数	努力をしている	努力できていない	必要性を感じない	総計
0	25	25	13	63
1	36	9	7	52
2	6	5	6	17
3	21	17	7	45
4	4	4		8
5	23	18	8	49
6	2	3		5
7	1		1	2
8	3	1		4
9	1			1
10	33	16	9	58
20	6	4		10
24		1		1
25		1	1	2
30	5		3	8
43		1		1
合計	166	105	55	326
回線数の平均	5.4	5.1	5.3	5.3

【リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。(2-(2))】

リモートメンテナンス（保守）の病院情報システムネットワークへの接続方法	施設数	割合	施設数	割合
自施設が設置するリモート接続の仕組みを持っている			346	62.9%
自施設が設置するリモート接続の仕組みを使った接続のみ許可している	100	18.2%		
自施設が設置するリモート接続の仕組みを使った接続を原則とするが、ベンダー側の理由で例外を認めている（接続する全てのリモートメンテナンス回線を把握している）	196	35.6%		
自施設が設置するリモート接続の仕組みを使った接続を原則とするが、ベンダー側の理由で例外を認めている（接続する全てのリモートメンテナンス回線を把握できていない）	50	9.1%		
自施設でリモート接続の仕組みを有さず、ベンダー個々の接続方法で接続を許可している			152	27.6%
（接続する全てのリモートメンテナンス回線を把握している）	114	20.7%		
（接続する全てのリモートメンテナンス回線を把握できていない）	38	6.9%		
リモート接続はベンダーに任せており、リモート接続の許可を行っていない			46	8.4%
（接続する全てのリモートメンテナンス回線の把握はできている）	35	6.4%		
（接続する全てのリモートメンテナンス回線の把握ができていない）	11	2.0%		
リモートメンテナンス（保守）は行っていない	6	1.1%	6	1.1%

【事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。(2-(3))】

事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）の提出を受けている				
	施設数	割合	施設数	割合
提出を受けている			514	93.5%
提出を受け、内容を確認し、必要があれば具体的な対応を行っている	140	25.5%		
提出を受け、内容を確認しているが、具体的な対応までは行っていない	261	47.5%		
提出を受けているが、内容は十分に確認していない	113	20.5%		
提出を受けていない			26	4.7%
提出を受けていない（必要性を感じていない）	19	3.5%		
提出を受けていない（事業者が対応してくれない）	7	1.3%		
事業者と契約していない	10	1.8%	10	1.8%

医療情報セキュリティ開示書（MDS/SDS）への具体的な対応事例

無回答項目への内容確認、記載依頼	3
2要素認証対応について	3
事業者が利用しているルータやファイアウォールのファームウェアバージョンアップの指示やできない場合の対応についての確認	2
同一パスワードの変更依頼、管理台帳などへの反映	1
WindowsUpdateに代表される更新プログラムの適用状況を確認し、適用が可能な内容であれば適切に対応いただいている。	1
システムのリモート対応の手段・仕組みを確認、パスワードの変更可否の確認、デバイス制御をした際のシステムの影響確認	1
セキュリティパッチの確認をし、ネットワークの切断が関係する場合は適用するスケジュールの調整など	1
ネットワーク機器のセキュリティパッチ適用	1
ベンダーで利用するリモート接続保守作業用端末を1台に限定していただき、病院側に提示していただく	1
ベンダーに対し改善依頼を行い、改善状況に応じ報告を求める。	1
扱う情報のリストの提示依頼を行った。	1
医療情報セキリティ開示書の内容確認して、設定に必要な事項があれば、申請書の提出を依頼し、規定に基づき運用を行っている。	1
管理用アカウントのパスワードが簡易なものだったため、複雑なものへの変更を指示した。	1
業者が用意したリモート接続ソフトウェアではなく、自施設が用意したリモート接続ソフトウェアの利用を依頼している	1
更新等があれば提出するように常に依頼している。	1
接続許可は、本部情報システム課が行っている。	1
対応できていない箇所について、理由及び対応可能になる時期の説明を要求している。	1
対応不十分な項目に対する対応見積の要請及び対応実施	1
単純な記入漏れがないか、「いいえ」や「対象外」、「非該当」を選択の場合、備考に理由や説明が記載してあるかを確認しています。また、記載内容に疑問があれば、問い合わせをしています。	1
部門システム更新時に、次のような対応を実施。病院での対応を依頼する表現や「指示があれば対応可能（院内タイムサーバーへの接続、資産管理ソフト導入など）」「必要に応じて病院と取り決める」「運用でカバーしてください」といった、対応が不十分な事項については、仕様書への記載や部署を交えた運用決定などの対応を実施した。	1
未対応項目についてはベンダーと交渉している	1

【利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。(2-(4))】

アクセス権限の付与方法	サーバ		ネットワーク機器	
	施設数	割合	施設数	割合
administrator権限のみ設定し、全ての機器群で同じパスワードを設定している	104	18.9%	127	23.1%
administrator権限のみ設定し、機器群ごとに異なるパスワードを設定している	192	34.9%	188	34.2%
組織ごと(病院やベンダー)にユーザIDと利用権限を設定し、ユーザパスワードは全ての機器群で同じである	46	8.4%	45	8.2%
組織ごと(病院やベンダー)にユーザIDと利用権限を設定し、ユーザパスワードは機器群ごとに異なっている	116	21.1%	96	17.5%
ユーザごとにIDと利用権限を設定し、ユーザパスワードは全ての機器群で同じである	30	5.5%	38	6.9%
ユーザごとにIDと利用権限を設定し、ユーザパスワードは機器群ごとに異なっている	62	11.3%	56	10.2%

端末PCのエンドユーザに対するユーザ認証について	施設数	割合
OSのユーザ認証を活用したユーザ認証を行っている	98	17.8%
OSのユーザ認証とソフトウェアでユーザ認証を組み合わせたユーザ認証を行っている	78	14.2%
OSはadministrator権限で自動ログインを行い、ソフトウェアでユーザ認証を行っている	96	17.5%
OSはadministrator以外の同一ユーザで自動ログインを行い、ソフトウェアでユーザ認証を行っている	252	45.8%
その他	26	4.7%

- ActiverDirectory認証
- OSはadministrator以外の個別ユーザで自動ログインを行い、ソフトウェアでユーザ認証を行っている
- OSはadministrator以外の端末固有ユーザで自動ログインを行い、ソフトウェアでユーザ認証を行っている
- OSはadministrator以外の同一ユーザでパスワードなし手動ログインを行い、ソフトウェアでユーザ認証を行っている
- OSはadministrator以外の同一ユーザでパスワードによるログインを行い、ソフトウェアでユーザ認証を行っている。
- OSはadministrator以外の同一ユーザでログインを行い、ソフトウェアでユーザ認証を行っている
- OSはadministrator権限で自動ログイン、ユーザ認証は行っていない。
- OSはadministrator権限で手動ログインを行い、ソフトウェアでユーザ認証を行っている
- OSは自動ログイン(admin権限なし)、ソフトウェアでユーザー認証
- OSは端末個別ユーザーとPWでログインし、ソフトウェア(電子カルテ)でユーザー認証を行っている
- OSは端末毎のユーザー(端末名)でログインし、ソフトウェアでユーザー認証を行っている。
- OSユーザー認証はしていない、ソフトウエアでの認証もしていない
- OSユーザ認証とエンドユーザの静脈認証
- SQLサーバ使用
- 各システム、各ベンダーで異なる
- ドメインユーザー認証
- ローカル端末はadministrator以外の同一ユーザで自動ログインを行い、ソフトウェアでユーザ認証を実施、VDI側はシングルサインオンにてOSのユーザ認証を行う
- 個人用の端末には個人のIDを設定し、部署用の端末には部署のIDを設定している

端末PCのエンドユーザに対するアクセス利用権限	施設数	割合
すべてのユーザに対して個別のユーザIDを発行し、アクセス利用権限を設定している (複数のユーザで使いまわしをしているユーザIDはない)	274	49.8%
すべてのユーザに対して個別のユーザIDを発行し、アクセス利用権限を設定することを原則とするが、一部、運用等の理由で、複数のユーザで使いまわしをしているユーザIDがある		
(管理者権限のID使いまわしはない)	138	25.1%
(管理者権限のID使いまわしがある)	44	8.0%
(管理者権限のID使いまわしがあるか否かは把握できていない)	8	1.5%
必要に応じて、ユーザごとのID付与と、組織、グループごと(外部委託業者など)のID付与を使い分けている	56	10.2%
その他	30	5.5%

- O/Sレベルではローカルadmin権限を有するが、UI上で機能制限をかけている。また、アプリレベルではすべてのユーザに対して個別のユーザIDを発行しているが、一部のアプリで使いまわしをしている。
- OSでは全てのユーザに対してIDは共通である。ソフトウェアのIDはユーザごとに個別に発行し、アクセス利用権限を設定している。
- OSのユーザは端末毎に個別のユーザIDを発行し複数のユーザで使い回しをしている場合がある
- OSは基本同一ユーザでログインし、ソフトウェアは全てのユーザに対して個別のIDを発行している
- OSは自動ログイン(admin権限なし)、ソフトウェアでユーザー認証及び利用権限を設定
- OSユーザー認証はしていない、ソフトウエアでの認証もしていない
- OSレベルのログインは非特権の単一のIDパスワードを使用している。このOSIDに対しては、端末上でアプリケーションを使用するために最小の権限を設定している。アプリケーションレベルは個別のユーザIDにより　、アプリケーション内のアクセス利用権限を設定している。
- WindowsLogInは全て共用、ソフトウェアログイン時に個別ユーザー、パスワードを入力
- すべてadministratorを利用しアクセス利用権限は設定されていない
- すべてのユーザーに対して個別のIDを発行し、アクセス権限を設定している。電子カルテメンテナンス業者については、専用IDを発行し、ID利用者を台帳管理している
- すべての端末は固定IDで運用されている。利用者権限のみで利用されている。
- すべて共通ユーザで使用している。各アプリケーションはユーザ個別にIDを発行しアクセス権を管理。富士通のパッケージはそうなっていると聞いています。
- ユーザではなく端末ごとにIDを生成
- 運用等の理由で、共通ユーザIDを使用
- 各システム、各ベンダーで異なる
- 管理者権限と、同一ユーザIDで使い分けている
- 機器ごとのIDI・パスワードを使用
- 制限なし
- 全てのユーザーに対して個別のIDを発行し、アクセス権限を設定している。電子カルテメンテナンス業者については、専用IDを発行しID利用者を台帳管理している。
- 端末IDは1つだが、システムは個別IDで対応
- 端末PCのエンドユーザーは端末毎のユーザー(端末名)で、標準ユーザーである。端末PCの管理者ユーザーは、システム管理者のみ利用可能。(管理者ユーザーは全端末で共通)　ソフトウェアのユーザーIDでアクセス利用権限を設定している。
- 端末ごとにユーザIDを作成し、複数ユーザで使いまわしている。このIDにはローカル管理者権限を付与している
- 端末は共有IDを使用しているが、電子カルテへのアクセスは個別IDにてアクセスしている
- 端末レベルでは自動ログイン、アプリケーションレベルで個別ユーザID発行
- 同一ID
- 同一ユーザで自動ログイン
- 部門毎の設定で複数のユーザで使いまわしをしている

【退職者や使用していないアカウント等、不要なアカウントを削除している。(2-(5))】

退職者や使用していないアカウント等、不要なアカウントを削除または無効化	サーバ		端末PC	
	施設数	割合	合計	割合
全て、削除または無効化できている	404	73.5%	391	71.1%
一部、削除または無効化できていない	114	20.7%	133	24.2%
全て、削除または無効化できていない	32	5.8%	26	4.7%

不要なアカウントを削除または無効化するタイミング	サーバ		端末PC	
	施設数	割合	合計	割合
退職日を有効期限に設定するなどリアルタイムでアカウントを削除または無効化している	347	63.1%	345	62.7%
年に1回など棚卸作業を行い、不要なアカウントを削除または無効化している （退職後にアカウントが有効な期間が存在する）	157	28.5%	167	30.4%
削除または無効化できていない	46	8.4%	38	6.9%

【アクセスログを管理している。(2-(6))】

アクセスログの残している範囲	サーバ		端末PC	
	施設数	割合	施設数	割合
全ての機器のアクセスログを残している	308	56.0%	285	51.8%
一部の機器のアクセスログを残している	183	33.3%	165	30.0%
アクセスログを残していない	59	10.7%	100	18.2%

アクセスログを確認しているか	サーバ		端末PC	
	施設数	割合	施設数	割合
病院職員がアクセスログを定期的に確認している	57	11.6%	63	14.0%
保守事業者がアクセスログを定期的に確認している	46	9.4%	19	4.2%
アクセスログを定期的に確認していないが、必要があれば病院職員が確認をすることが可能である	177	36.0%	238	52.9%
アクセスログを定期的に確認していないが、必要があれば保守事業者が確認をすることが可能である	179	36.5%	110	24.4%
アクセスログを残しているが、確認方法は把握していない	32	6.5%	20	4.4%

アクセスログの保管期間	サーバ		端末PC	
	施設数	割合	施設数	割合
医療機関がサーバのアクセスログの保管期間を指定している	102	20.8%	115	25.6%
保守事業者が定めたアクセスログの保管期間を医療機関として把握している	164	33.4%	147	32.7%
アクセスログの保管期間を把握していない	225	45.8%	188	41.8%

アクセスログを残さない理由	施設数
医療機関としてアクセスログを残す必要性を感じていない	12
医療機関としてアクセスログを残す必要性を感じているが、コストがかかるため残すことができない	72
医療機関としてアクセスログを残す必要性を感じているが、保守事業者が対応してくれない	18
その他	24

- オーダリングソフトに機能がない
- システムの仕様をベンダーが握っており、全体を統一して管理できないため。
- システム管理が兼務のためログの管理まで手が回らない
- ソフトウェアのログオンにてアクセス確認している。
- ソフトウェアの利用ログはサーバー上にログが残る。クライアントログは取っていない。
- ドメイン管理をしていないため
- ベンダーが管理しているかもしれないが病院で把握できていない
- 一度選択したら外せないのでここに記載
- 各システム、各ベンダーで対応が異なるため
- 残していると回答
- 実施を検討中
- 主要な機器は残しているが、部門機器などよくわからないものがある
- 他の業務が優先されて対応できていない
- 端末PC：アクセスログの管理はないが、NDR、EPPにより保護されている
- 端末PC上に医療情報は保管せず、サーバー上で保管されているため。サーバーへのアクセスログのみ管理している。
- 端末からシステムにログインすることで当該システムのサーバーにアクセスログが残るため端末には残していない。また、端末自体は不特定多数の職員が使用するため自動ログインするため。
- 端末には共通IDでログインしているので、残しても利用できない。
- 端末のアクセスログを残す費用は無い
- 端末自体はほとんど何もできないユーザーでログインしているため。電子カルテログイン後はアプリケーション側のログを取得している
- 電子カルテ等個人情報に係るネットワークが未導入の為
- 電子カルテ用PCは複数が使用するため端末PCにアクセスログは設定していない
- 必要性は感じているが、未対応
- 不明
- 方法が分からない

【セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))】

セキュリティパッチの適用	サーバ		端末PC		ネットワーク	
	施設数	割合	施設数	割合	施設数	割合
全ての機器に対して適用している	138	25.1%	137	24.9%	173	31.5%
一部の機器に対して適用している	149	27.1%	117	21.3%	187	34.0%
適用していない	263	47.8%	296	53.8%	190	34.5%

セキュリティパッチを当てるタイミング	サーバ		端末PC		ネットワーク	
	施設数	割合	施設数	割合	施設数	割合
セキュリティパッチごとにリアルタイムで（システム検証は行わない）	40	13.9%	55	21.7%	42	11.7%
セキュリティパッチごとにできるだけ早いタイミングで（システム検証を行った後）	44	15.3%	39	15.4%	56	15.6%
定期的に（〇ヶ月に1回など時期を決めて）、セキュリティパッチをまとめて適用を行う	26	9.1%	29	11.4%	31	8.6%
適用が必要なセキュリティパッチが出てきた時に、保守事業者と打ち合わせを行った上、適用時期を決める	165	57.5%	115	45.3%	219	60.8%
その他	12	4.2%	16	6.3%	12	3.3%

セキュリティパッチを当てる範囲	サーバ		端末PC		ネットワーク	
	施設数	割合	施設数	割合	施設数	割合
全てのセキュリティパッチを適応している	47	16.4%	61	24.0%	51	14.2%
医療機関が必要と判断したセキュリティパッチと保守事業者が推奨するセキュリティパッチを適用している	73	25.4%	68	26.8%	107	29.7%
医療機関が必要と判断したセキュリティパッチを適用している	15	5.2%	24	9.4%	18	5.0%
保守事業者が推奨するセキュリティパッチを適用している	149	51.9%	95	37.4%	174	48.3%
その他	3	1.0%	6	2.4%	10	2.8%

セキュリティパッチを当てる費用	サーバ		端末PC		ネットワーク	
	施設数	割合	施設数	割合	施設数	割合
保守費用に含まれる	233	81.2%	206	81.1%	269	74.7%
随時、作業費用を支払っている	54	18.8%	48	18.9%	91	25.3%

セキュリティパッチを適用しない理由	施設数	割合
医療機関として必要性を感じていない	18	6.3%
医療機関として必要性を感じているが、事業者が対応をしてくれない	68	23.6%
医療機関として必要性を感じているが、作業費用の捻出が困難である	102	35.4%
その他	100	34.7%

【セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))】

セキュリティパッチを適用しない理由(その他)

- 外部インターネットに接続していないクローズドシステムため
- Closed Netwokで端末は未適用
- HISソフトの動作安定優先
- HIS系ネットワーク（保守ベンダーリモート接続のみ）のため、Windows Updateに対応できていない。一部、ソフトウェアでアップデート対応ができないため時期システム更改時にしか対応できない状況です。
- OSは更新プログラムを適応していないが、ウイルス対策ソフトにて対応している
- VDIとなっていて、すべての部門システムが「相乗り」になっていて、医療機関内で検証ができない
- windows のアップデートは適用していないが、ウイルスソフト「ESET」の更新を実施している
- アプリケーションがセキュリティパッチの更新に対応できない。
- アプリケーションの動作可否の確認と作業時間などの捻出が難しい。
- アプリの関係で適用できない
- インターネットから分離していることと、稼働中のシステムへの影響が懸念されることから、セキュリパッチの適用が難しい環境にある。そのため、インターネットからの分離と、外部記憶媒体の接続制限による代替対応を実施している。代替対応については、医療情報システム安全管理に関するガイドラインQ&Aを参照した。
- インターネットに接続していないため
- インターネットに接続していない前提。又、パッチ適用後の不具合等でシステムに影響させないため
- イントラネットはインターネットに接続していない為
- イントラネットワークをインターネット接続できないようにしているため
- オフアインのため適用が困難
- オフラインの為、適用できない、ウィルス対策ソフトはパッチ適用している
- オフライン運用なので
- オフライン運用の為
- オフライン運用をしている
- オンプレであり、電子カルテ系統はネット接続していない
- オンプレ環境のため、また、テスト環境がないため
- カルテ端末はカルテ以外にもシステムが相乗りしているため、全てのシステムで検証を行わないと動作に不安がある。また、当院ではカルテ端末はネット不可のためWSUSなど更新に必要な仕組みを構築する必要がある。よって端末は外部記憶装置使用の制限やセキュリティソフトで対応している。
- クローズシステムの為
- クローズド運用であること、パッチを当てることによる動作不良等が発生する問題があることと、作業費用の捻出が難しいため適応は難しい。
- クローズド環境のため、セキュリティ更新環境を構築していない。また、システムベンダー側で都度のOSセキュリティ更新におけるシステム動作検証に対応していないため、セキュリティ更新環境を整えてもOSセキュリティ更新を行えないのが実態である
- クローズなので更新が困難
- サーバ、端末PCについては業務システムへの影響を考慮してベンダーへ対応方針を確認中です
- サーバ、端末に関してはクローズドネットワークのため適用していない
- サーバー以外はアップデート済
- システムが稼働しなくなる可能性があるため
- システムが対応していない
- システムによってはセキュリティパッチを適用することで動作に不具合が生じるシステムが存在するため
- システムの仕様をベンダーが握っており、全体を統一して管理できないため。
- システムへの影響が大きい為適用が困難と聞いている
- システム運用上の制限がある
- セキュリティパッチの適用によりシステムの運用障害発生の可能性があるのでクローズネットワーク内のサーバ、PCには適用しない
- セキュリティパッチを適用している
- ソフトウェアの動作保証が確認できない
- ネットに繋げていない
- パッチを適用することによりその影響でシステムが停止（動作不良）の可能性があり、診療継続できない恐れがあるため。
- パッチを適用すると電子カルテが正常動作しない
- パッチ適用による予期せぬ動作不具合のリスクを回避できない可能性があるため
- パッチ適用後の動作検証ができていない
- ベンダーから医療機関の端末PCにおいてセキュリティパッチを適用している機関はほぼないと聞いている
- ベンダーと相談し必要に応じ適用することとしているため
- メーカーの意向
- レセコン単独使用環境
- 医療機関として必要性を感じているが、作業費用の捻出や電子カルテシステムや部門システムの動作検証が困難である。
- 医療情報システムの正常動作への懸念
- 医療情報ネットワークはクローズのため
- 影響が大きいセキュリティパッチのみ保守業者の申告により適用している
- 可能なものは適応している。オフライン環境であり、医療情報システムの運用上未適応のものがある。
- 回線都合
- 外部接続は保守業者のVPNのみであるため。
- 外部接続負荷/クローズの状況で使用しているため
- 各システム、ベンダーで対応が異なる
- 完全な必要性の場合、検討する。
- 機器更新を行って間もないため
- 検証が取れていない
- 検証上適応できないものもあるため
- 原則閉域網であるHIS系機器へのセキュリティパッチを適用が困難。各種システムの動作への影響を懸念
- 古いOSの端末がたくさんあり個々の対応が必要であるが、設定するスタッフがいない
- 作業費用および作業人員の捻出が困難
- 事業者、作業費用の両面で困難である。
- 事業者が拒否している為
- 実施している
- 脆弱性該当機器のみパッチ適用
- 端末PCには不要
- 端末PCのbっ氏hs、パッチ適用による動作不能のリスクがあるため
- 摘要できる環境にない
- 適用させると部門システム含め最新のOSやブラウザに対応していない場合、システムが動作しなくなる可能性があるため。
- 適用することでシステムの稼働が不安定にならないかが心配である
- 電カル関係はパッチ適用による動作保証がない
- 電子カルテシステム・OSに制限がある為
- 電子カルテへ影響する可能性がある場合
- 電子カルテメーカーがインターネッと接続を認めない
- 電子カルテ端末はセキュリティパッチを適用すると動作及び保守対象外となる、または高額な費用を請求されるため適用していない
- 動作の保証がない
- 動作を保証できないため
- 動作確認の保証に関わるから
- 特定の機器・サーバを特定（決済・オン資）FWで接続を制御、リモートメンテもリモート先から外部への接続無し。次期システムでパッチ適用を開始する。
- 費用ももちろんですが、電子カルテ側が最新のパッチに適応されていないため困難
- 費用面から業者が行うのではなく安全管理責任者が行う。またセキュリティパッチの適用自体を禁止にしているベンダーもいる
- 必ずしも最新にはしておらず脆弱性がある場合のみ
- 必要性は感じています
- 必要性は感じているが、各システムが正常に動作することを確認できないため。
- 必要性は感じており、検討中で
- 必要性は理解できるが、オフラインのネットワーク環境でのパッチ適用作業が現実的ではない
- 必要性を感じているが、現在はWSUS等の環境がなく次期更新で検討
- 病院内のみの医療情報システムであり、外部接続は原則ないため。
- 不明
- 負荷
- 部分的に必要に応じて適用しているが、全体としては作業費用の捻出が困難である
- 複数のシステムと連携しているため
- 閉じたLANであり、パッチの適用が難しい
- 閉域網であり、保守事業所の判断
- 保守回線以外ではインターネット接続不可の為
- 保守用の回線のみでダウロードするインターネット接続口がない
- 有償で対応可能だが、他部門システムとの動作確認ができていない為
- 「一律に全台/全パッチ適用」ではなく、リスクに応じた機器選定が現実的になるので、チェックシートでもそのような記載にしてほしい。
- ベンダーが言うようにパッチ適用によることによって出るかもしれない不具合が心配。パッチ適用がある意味リスク。
- パッチ適用を促すのであれば、医療機関へ対応を求めるのではなく、医療情報システムを提供しているベンダーへの義務化をするべき。・利用している医療機関は立場が弱い、できないと言われたり、動作保証できないと言われたり、費用が掛かったりで厳しい。
- その他、パッチ適用に限らず、セキュリティチェックリストで求められていることは、ベンダーへ対応求めるようにしないと解決できない。
- CTやMRI、超音波機器などのモダリティ機器へのセキュリティパッチ適用は、機器の安定稼働の面から適用できないと言われています。ですが、セキュリティ対策チェックリストでは「必要」となっています。現状との解離が生じていますが、この辺りの見解をお聞かせ願います。
- DMZにある機器に対しては、セキュリティパッチを適用している。通常の電子カルテ端末は、多くのシステムが相乗りしており、全パッケージベンダーが対応できないとパッチが当てられない。セキュリティパッチ適用の見積もりを取得すると、高額な見積もりになる（正確にはパッチ適用後に発生する可能性に対する費用は別途になる）医療情報を扱うソフトウェアに対して、セキュリティ順守度を確認する制度ができないか？と考えます。

【セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))】

セキュリティパッチに対する意見 (1)

- HISベンダー側でアプリケーション側のセキュリティパッチ対応の開発が進まない。一般的な汎用システムに比較して医療ベンダーの認識が低く大変困っている。
- OSバージョン固定が大半の医療システム仕様条件となっているため、パッチ適用は補償範囲外となり適用できない。
- PC、サーバは基本的にクローズネットワーク上の配置なのでWindowsUpdateなどの更新は行えない。セキュリティアプリ（シマンテック）は毎日更新しています。
- アプリケーションがセキュリティパッチによる動作保証ができないのであれば、Webアプリケーション化やコンテナ化など、ローカルのカーネルに依存しない作りにする方向で開発して欲しい
- アプリケーションが止まることがあり、この足を踏んでしまう
- あらゆるベンダーの動作検証が必要で、期間は数か月を要し、さらに費用面においても懸念がある。持続的なパッチ更新はほぼ困難。
- いずれのベンダーとの保守契約にもセキュリティパッチの適用は含まれていません。理由は稼働に問題が出た場合に対処ができないとの回答。これは厚労省の規約で記載があっても現状はこのような状況です。
- ウイルスソフト等のパターン更新は可能であるが、OS等の更新プログラム適用は各施設での個別対応は不可能であり、事業者への依頼となると莫大な費用が掛かる。理想ではあるが現実的でない項目であるため解決策が見つからない。
- ウイルス対策ソフトのパターンファイルのみ更新を行うようにしているが、Windows のセキュリティパッチは対応できていないです。また、一部ソフトウェアにおいてWindows Updateで不具合がでるため更新不可との回答があり、費用や運用面において次期リプレイスまでは使い続けるしかない状況です。
- オフライン（インターネット非接続）のサーバーや端末の運用はオンラインの機器とは切り離して考えていただきたい
- オフラインで運用しているとアップデート作業が非常に手間である
- オフライン環境で既存で動いているシステムやプログラムの影響を考慮しながら常にセキュリティーパッチを適用していくのは困難
- オフライン環境下でのパッチ適用作業が現実的ではない。windowsが以前あったSP(サービスパック)方式ではなくなったので、アップデート作業自体非常に手間と時間がかかる。
- オンプレの状況で、セキュリティパッチがどこまで必要か検討しあぐねている
- オンプレミス環境ではサーバーや端末PCへの適用はできてもルーターのファームウェアは実施が難しい
- オンプレ製品を利用している場合、閉鎖空間にあるためパッチ適用が困難であること、また、医療情報システムが正常に動作しなくなる懸念があり適用できない
- カルテ端末はカルテ以外にもシステムが相乗りしているため、全てのシステムで検証を行わないと適用できない。また、当院ではカルテ端末はネット不可のためWSUSなど更新に必要な仕組みを構築する必要がある。よって端末は外部記憶装置使用の制限やセキュリティソフトで対応している。
- クライアントにWindowsを使用している医療機関が多いと思うがマイクロソフトがインターネット接続を実質的に必須としているためオフラインでの運用が非常に困難である。WSUSサーバにおいても廃止予定であり、導入費用もそれなりに高額であるため今更導入は出来ない。そのため安全管理責任者が夜間に手動で当てているが毎月全台数を当てることは難しい。またベンダーもそういう相談には乗ってもらえない。パッチをこちらが当てること自体を禁止しているベンダーもいる。（そういうことを想定していないのではと感じることもある）
- クライアント端末への適用が出来ているが、サーバに関してはベンダー側から許可が下りず対応できていない。また、対応が出来たとしても適用毎に作業費が発生するため、全てのサーバに適用しようとすると多額の費用が掛かる
- クラサバを一定の基準で構築しており、セキュリティパッチの適用により、その関係性を阻害され、サービスの安定的提供ができないおそれがあるため、セキュリティパッチの適用は行いたいという希望はあるが、サービスの安定的提供を優先し、積極的なパッチ適用はベンダーとの了解のもと、行っていない。
- クローズドネットワークでの運用のため、適切なアップデート方法が分からない
- クローズなので更新が困難
- クローン環境を構築しパッチ適用テストを行わないと、実環境への適用は難しいと思います。そうなると、非現実的な環境構築費用を捻出する必要があり、収益の乏しい施設では事実上不可能と判断します。
- サーバ、クライアントのwindowsパッチを適用すると動作保証できず、対応できないと全てのアプリケーションベンダーから言われています。この考えが大多数でないでしょうか。最大手の電子カルテベンダー、最大シェアの各部門システムも同様の姿勢です。
- サーバ・端末PCへのセキュリティパッチの適用はシステム動作の検証等に高額な費用がかかるため困難である。
- サーバーPCや端末PCに最新のファームウェアを適用する際にはインターネット接続が必要と考えています。作業のために接続することが逆にウイルス感染のリスクを高めると思っておりますが如何なものでしょう？
- サーバーや端末PCもOSセキュリティパッチ適用については大病院ほど実質不可能であり、ネットワーク機器と同列にするのは無理がある。（システムが動かなくなる可能性がある。特に部門システム）
- サーバとネットワーク機器につては、VPNでクラウドのサーバと法人内施設にだけ接続しているが、リモート用回線が業者と接続されている。院内ネットワークに入るには、リモート用回線からしか接続できない為、まったく外部からの侵入は考えていない。その為、クライアントはバージョンアップを行っていない。今後はAIの利用を考えるのなら、インターネットに接続できる院内ネットワークが必要になるが、それによりセキュリティが下がる可能性がある。
- サーバと端末PCのパッチ適用には数多ある全システムベンダーによる医療情報システムの動作検証が必要であり、その都度適用する労力と費用を考えると、NDRやEDR等セキュリティ対策用のシステムで画一的に対策する方が現実的であると考える。
- システムの安定動作が担保されるか疑問
- システムの仕様上対応が難しいと言われるケースもある
- システムベンダーから自己責任で適用するように言われているため、医療機関として対応する時間が取れない
- システムベンダー側がオフラインだからという姿勢を崩さないため、実現ができない。適用したいと伝えても、対応したことがないとの回答になる。適用後の動作検証もベンダーでは行わないため、万が一不具合が出た場合に対応してもらえないので、医療機関側の判断だけで行うこともできない。セキュリティパッチだけではなく、バージョンアップも同じ理由で断られる。地方の病院では各々の部門で選択できるシステムベンダーが少ないため、対応ができないのであればシステムを導入しないといった強気の姿勢をとるのは難しい。医療機関にベンダーと協議するようにとの指導ではなく、ベンダーに直接指導を行っていただきたい。
- システムベンダー側で、構築時のOSの状態以外は動作保証しないという姿勢を改めてほしい
- システム停止を伴う作業のため、対応が難しい。
- システム導入契約時のパッチに合わせてベンダが設計構築を行っているため、稼働後のパッチ適用によって生じる不具合・障害が発生するリスクが高い。このような影響を受けない製品の販売開始が待たれるところ。
- セキュリティパッチの重要性や必要性は感じているが、適用後にシステム障害が発生する可能性を考えると適用に躊躇する。また、システムベンダーも適用前後の検証に前向きではなく、病院単独では実施できない。
- セキュリティパッチの対象（OS、アプリケーション、ファームウェア等）や、アプリケーションの動作に必要なソフトウェア（ミドルウェア等）の脆弱性を把握したうえで適切な対応ができていない。優先度が高いもの（例えばファイアウォール）については対応しているものの、それ以外の対応ができていない。SBOMも今後意識しなければならいと理解していますが、当院では今後、対象の洗い出しと、それにおけるリスク、さらに優先順位をまず整理する必要があると認識しています。限られた人的リソースで円滑にパッチ適用が運用できている医療機関を参考にできればと思います。
- セキュリティパッチの適用については、ベンダーに過去20年実施を求めているが、サーバについては検討するとの回答をベンダーが繰り返され適切な実施が遅延されている。
- セキュリティパッチの適用については、作業費用の負担を含め、機器の設置、システムを構築した事業者側の義務としてほしい。特に、PC端末については、複数の事業者のシステムが相乗りした状態で運用しているため、パッチ適用による動作保証ができないと回答する事業者が1つでもあるといつまでも適用できない状態が続くことになる
- セキュリティパッチの適用は必須であると考えるが、システム体制はパッチ適用を前提としていないため、不具合が発生した場合業務停止のリスクがある。ベンダー体制もこれまで閉鎖環境で、稼働率重視で環境を変えない事を前提として設計されているため、設計思想から変更する必要があるため、容易にセキュリティパッチ適用を行う事が難しい。また医療システムは高額である為、容易にシステム更新が出来ないため、EOLを迎えたシステムで稼働していたとしても更新が困難である為、これらの医療施設固有の問題を踏まえ、現実的なセキュリティ対策のガイドラインを示していただく（ネットワーク振る舞い検知型の対策）、セキュリティシステムを継続利用出来るための補助金などの制度を検討していただきたい
- セキュリティパッチの適用後、システムへの影響がどこまであるのか不明なため、テストや状況判断に多くの時間がかかる。
- セキュリティパッチの適用前の確認に時間を要するので、即時適用ができない。
- セキュリティパッチの必要性は感じているが、医療情報システムへの影響がわからないということで医療情報システムベンダーが対応していません。
- セキュリティパッチをあてていても侵入される可能性もあり、可用性の関係や費用を考慮すると非現実的な対策と考える
- セキュリティパッチをサーバや端末に適応させると、部門システムが動かなくなる。ただ、セキュリティ上不安がある
- セキュリティパッチを適用してもこれまでどおり正常に稼働するかの事前検証が難しい
- セキュリティパッチを適用の課題について、システムベンダー側がどう対応を進め取り組んでいるか見えません。状況を定期的に周知してもらえると良いです。
- セキュリティパッチを当てる事で不具合が起こった事もあり、判断が難しい。
- セキュリティパッチ適用はシステムベンダーの検証が済まないと対応できないと考えています。一部システムについては、最新パッチを当てて良いとしているベンダーがありできる範囲での対応を行っている。検証結果を得られないベンダーやベンダーに依頼する必要がある場合、高額になることから対応できていない部分がある。

【セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))】

セキュリティパッチに対する意見 (2)

- セキュリティパッチ適用義務を医療ベンダに国として義務化してほしい
- セキュリティパンチの適用意識がベンダーに欠けている。もっと指導して欲しい。
- セキュリティ上重大な問題がある場合のみ検証済みパッチのみ適用、普段のWindows Updateなどは当たっていない
- ゼロデイリスクは認識していうが、ネットワークなどをセキュリティアップにともなう不具合による、医療情報システムのエラー、不具合対応に不安がある。アップデートタイミングが難しい
- ソフトウェアとの親和性を確認してからの適用なので手間である。
- ソフト等の影響により更新が難しい場合が多々ある
- そもそもの設計に根本の問題がある限り、かけるコストに無駄が多すぎる。セキュリティbyデザインに移行することに、補助金を出し、旧式のデザイン哲学を変えるべき。
- どこまでのことを指すのかが不明。端末PCにファームウェアやWindowsUpdateは適用不可。セキュリティ対策ソフトは該当？
- なし
- パッケージ製品の動作保証（検証）をユーザー側では行えないため、本項を求められる場合は商法上の取扱いについて解決策を提示して欲しい。
- パッチの適用は医療機関側では対応できることではない。電子カルテ業者が不具合の可能性と言うことで対応してくれないため、事業者にパッチの適用を求めるべきである。
- パッチの動作確認には相当な時間と労力もしくは費用が必要となるが、それだけの人材の確保すること若しくは費用に対して理解は得られない。
- パッチの内容にもよる　重大なセキュリティホール等のケースは優先的に実施するが、軽微なもの、利用サービス対象外の機能であれば様子をみる場合もあるが、例えば電子カルテ端末等はメーカがアップデートは対応できないなど、その場合ハードウェア事更新が必要であったりするケースもあるが、一概にパッチを適応していないという文言だけの判断は危険と考えます
- パッチを当てただけで電子カルテがストップする可能性もあり実質適応不可能
- パッチを当てると電子カルテシステムが正常に動作しなくなる
- パッチ適用できるものは適用するようにしているが、ほとんどのシステムがパッチ適用での動作保証をしていないのでは？特にクローズド環境の電子カルテや部門システムについてはほぼ非対応と思われる。実環境と指針があっていないと感じる。
- パッチ適用によるシステムトラブル。ベンダーの保証が得られないため適用できない。
- パッチ適用による不具合リスクがある為、動作優先となる。
- パッチ適用の重要性は十分に理解しているが、1つの端末PCに多くのシステムが稼働しており、セキュリティパッチを適用するたびに各システムベンダーを招集し評価を実施するためには、かなりの費用や時間が必要となる点が一番の課題であると感じている。
- パッチ適用後に障害が発生した場合、問題の切り分け（復旧）対応に関する保証内容が明確になっていない
- パッチ等は安定稼働の問題上、適用が難しく当てていない。
- ベンダーから、セキュリティパッチを適用すると、業務システムの動作保証できないと言われている。
- ベンダーが指定したOSバージョンとは異なる環境下でのアプリケーションの不具合を懸念する
- ベンダーの保守料金内にセキュリティパッチの適用を含めて欲しい
- ベンダーやソフトウェアメーカーの対応が遅い。
- ベンダ側の動作検証がとられていないため、最新に上げることができない。また、作業費用が保守費用以外に発生し病院経営を圧迫してしまう。
- メーカーが動作保証を行えない以上、病院の独断でセキュリティパッチを適用させて、別のリスクを発生させる訳にはいかない。
- リスクや作業量を考慮すると中小病院では外注せざるを得ないが、費用がない。
- 医療機関としては適用していきたいが、電子カルテなどの基幹システムの挙動に影響があると業務に支障をきたすので、医療機関の判断だけでは適用ができない。ベンダー側は動作保証ができないと適用に難色を示すことがある。さらに端末に部門ベンダーのシステムが相乗りしていると全てのベンダーのシステムで動作保証ができない。
- 医療機関は、診療機能を維持し、恒常的に提供できる体制を保つことが主目的であり、セキュリティを向上することはそのための手段に過ぎない。一方、電子カルテベンダは医療機関が診療機能を維持し、恒常的に診療を提供できる体制を保てるように補助することがベンダが果たすべき役割であり、本来であれば、ベンダ側の責任の下、セキュリティパッチ適用後の電子カルテシステム等の動作検証の実施と、セキュリティパッチの適用を担うべきである。特にサーバに関しては、セキュリティパッチ適用によるアプリケーションへの影響を推し量ることは病院の担当者では不可能であり、開発元が責任を以て検証をし、医療機関へ対応すべきである。
- 医療機器は　医療機関の判断で　セキュリティパッチを当てることができない。メーカーマターとなる。
- 医療系のシステムはオフラインの運用が主流であるため、オフラインセキュリティパッチに対応しているシステム業者がそもそも少ない。
- 医療情報システムは、保守用回線以外の外部ネットワークに接続していないクローズドな環境であることが多く、また、稼働中のシステムへの影響も懸念されるため、セキュリティパッチの適用は難しい。そのため、インターネットからの分離と外部記憶媒体の接続制限による代替対応が現実的だと考える。その場合、保守用回線のVPN装置等のファームウェアアップデートが重要になるが、現状、医療機関側からベンダーに確認しないと対応が進まない。保守用回線を導入する場合、医療機関とベンダーの双方が互いに確認し合うような仕組み作りが必要と考える。
- 医療情報システム事業者への義務化が必要です。パッチを適用する場合、適用に要する費用及びシステム不具合が出た場合の費用は医療機関負担となるうえ、不具合の責任は負いませんがそれでも実施しますか？と言われるケースが大多数であり、実質的にセキュリティパッチが適用できません。
- 一部システムや保守事業者では、セキュリティパッチの適応自体が不可能との回答を行う場合があり、実際セキュリティパッチの適用によりシステム障害となることもあるため、セキュリティホールをそのままにして利用を継続しなければならない事態となることがあり、悩ましい。
- 一部はできているが、基幹システムに関しては、パッチ適用後の不具合リスクが大きいため、セキュリティ対策ソフトでカバーしているものもある
- 院内の電子カルテネットワークは完全にイントラネットとなっており、クライアントにはセキュリティパッチを適用していない。
- 開発環境がない施設は、テストが出来ないためアプリケーション動作リスクが伴う可能性がある
- 外部との接続は専用回線で行っており、その他は外部接続は物理的に不可能である
- 各システムの動作検証および、適用するにあたり病院業務の停止が発生する
- 各システムベンダーは、ソフトウェアの動作保証を持ち出してセキュリティパッチの適用に消極的だが、それはベンダーの技術力不足・怠慢だと考えます。
- 各システムメーカーが前提としていないので、大変難しいです。
- 基幹の電子カルテシステムに関わらず、システムにより何かしら業務停止を伴うため、以前より現場の拒否感が強い。
- 規模の小さいベンダーのソフトウェアの製品において、セキュリティパッチの適応に対応していない、または対応に時間がかかることがあり、別途費用が発生する。随時セキュリティパッチが適用できない大きな要因となっている。
- 業務システムにおいては動作検証が必要で難しい部分がある
- 原則閉域網であるHIS系機器へセキュリティパッチやOS等の更新の必要性と仮に行った場合の各種システム正常動作とのリスクが計れない。
- 現実的にすべての機器を対象にパッチ適用することは不可だと考えております。レガシーOSで動かす必要がある端末がぞんざい下り、多々ある種類の機器類の知識を得て判断することは厳しいと思います。
- 古い部門サーバーは移行もできていないため、OSのサポートが切れている。データ移行の費用もねん出できない。
- 互換性の問題で常時最新にはできない。セキュリティパッチを最新にすることを病院に強要するより、ベンダーにセキュリティパッチが最新にできない医療情報システム製品を販売することを禁じてほしい。最低でも追加費用なしで8年間の最新のセキュリティパッチ更新、OSの更新への対応ができることを前提とした厚労省の認定制で販売してほしい。
- 国側で各ベンダーに適用像できるように指示が必要
- 最低限の備えとしてセキュリティパッチは重要と認識しているが、これまでの無事故を理由に対応をしないという方針が事業者から示されています。対象システムはオンプレミスで、約6年間パッチ更新が行われていないレガシーシステムであり、事業者からは技術的、または人員的な理由で現在の状態からのセキュリティパッチ対応は不可能との回答を得ています。事業者から代替案としてセキュリティソフトの配布サーバ新設が提案されました。しかし、この提案はOSの脆弱性を突く攻撃に対する根本的な対策ではなく、単なるアンチウイルス対策に留まるため、根本的な回避策になっていないと回答しました。この対応不可能な状態は、サイバー攻撃に対する重大な脆弱性を継続的に放置していることであり、事業継続性に関わる深刻なリスクとして認識しています。
- 作業費用およびリスクがおおきいため、サーバ、端末など全ての機器に適用するのは困難最低限対応すべきパッチの内容、および対象などの指針を出してほしい
- 事業者からは、「影響が不明であるため適用できない」「適用には高額な検証費用が必要となる」といった回答があります。さらに、いまだに「外部と接続していないため不要と考える」という事業者も存在します。このような状況から、医療機関が単独で対応を進めることは困難。国として事業者対応の実施を働きかけるとともに、必要となる費用の支援をご検討いただきたい。
- 次期システム2029年1月予定で対応
- 次期システム更新時に要件としてパッチ適応を要求していく
- 次年にはベンダー主導にてパッチ適応が行える環境に移行予定
- 手動アップデートは可能であるため、検討中
- 重要性は理解しているが費用が高額であり、連携システムとの兼ね合いで全てに適用するのは難しい。
- 重要度の高い、緊急度が高い項目については、セキュリティパッチの適用を行うよう対応している。しかし、システム停止が伴うため、救外など確認を行い、夜間に対応することになる。
- 助成金が欲しい（適応範囲の拡充、増額）

【セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。(2-(7))】

セキュリティパッチに対する意見 (3)

- 上記の理由により当院ではパッチ適用を実施していないが、実際にやっている病院があればどのように実施しているかご教示いただけますと幸いです。
- 常に最新のセキュリティパッチを適用するには、相当高額な費用と適用前のテストなどの準備が必要となり、対応したくても現実的に難しい現状がある。
- 情報管理部門としては必要性を理解しているが、病院管理者が不同意。
- 新たな脆弱性は増加の一途、本来は迅速に適用すべきだが、検証・費用がかかるため、必ずしも迅速に適用できていません。また、ベンダによってはセキュリティ対策に前向きでないケースも散見されます。公的な機関から、実運用が可能なレベルでの必須度や緊急度のガイドライン提示や、ベンダへの対応必須化を指導していただけることを希望します。
- 診療報酬や補助金等による十分な補填がなければ実施困難である。
- 数百のサーバ及び百数十のシステム（オンプレ、Saas含む）に対し、まずパッチの対象かどうか、各ベンダに適用の可否を確認、そして適用作業立会いと適用後の変更・構成管理のサイクルを最低でも月1で行うことは、SBOMを使用しても情報システム部門のマンパワーが足りず難しいと苦慮している。またパッチ当てを行うことを保守契約に追加する、もしくはスポットで依頼すると大幅に費用増となるため、予算計上が難しくなる
- 素人なのでセキュリティパッチを適用して不具合が起こった場合、元に戻す手立てがわからない。
- 多種多様な構成のシステムを運用しており、セキュリティパッチの適応でシステム自体の動作に影響が発生する場合がある。もちろん可能なものは最新のパッチを適応しているが一律に最新のパッチを適応するにはならない。
- 端末・サーバへのセキュリティパッチは動作不良を起こす可能性があるので、全国的な課題であると考えます。
- 端末PCについて、Windowsの最新のセキュリティパッチの適用が場合によって使用している電子カルテ等の互換性の確認がされておらず不具合が発生する場合があり業者に確認を要する。また、イントラ環境下の端末PCについて自動的に最新のパッチ適用ができず現実的に対応はできていない。（現状実施する場合は、1台ずつインターネットに接続して適応を繰り返すことになる）
- 適用するには、メーカーによる影響調査及び作業（有償）が発生するため、金額的に難しい
- 適用による動作保証が取れず、ほぼ適用できない状況です。大きな障害になる事が予想される不具合に対するパッチのみ適用しています。
- 適用による不具合が懸念される
- 電子カルテシステムのクライアント端末などの複数台に対して、適用することは難しいと考えております。
- 電子カルテなどのソフトウェアとの競合を理由になかなか更新を行えない状況
- 電子カルテベンダーがwindowsのパッチに対応するのが遅い（国内ベンダーに検証する要員が少ない）
- 電子カルテベンダーより、最新パッチを適用した場合にソフトウェアが動かなくなるとの連絡があるため。またバンドル版OSなどの場合、オフラインでの最新パッチの適用が非常に手間である。WSUSも検討したが、費用がかかる。各端末に直接インストールは現実的ではない。よい手段があれば開示してほしい。
- 電子カルテベンダより対応不可と言及
- 電子カルテ関連のサーバーや端末について、当院は電子カルテでは富士通製を利用しており、その他の部門システムと連携していますがセキュリティパッチの適用は、現行の電子カルテシステムとの互換性に関わるため、富士通や部門システムベンダーの専任事項になっています。そのため、一般に公開されたタイミングでのセキュリティパッチ適用ができない状況です。電子カルテや部門システムベンダーには一般に公開されたタイミングになるべく合わせてセキュリティパッチの検証を実施し、病院側でパッチ適用ができるように運用していただきたい。
- 電子カルテ端末だけでも、複数のシステムが相乗りしており動作検証などの作業負荷や費用面の負担が大きいと感じる。医療機器等を含めてすべからずと言われると、現実的にはかなり厳しいイメージ。医療機器業者からは薬機法のため適用不可と言われることが多い。
- 電子カルテ端末のパッチ適用は理解できますが、これが医療機器も情報端末の一部と規定された場合、医療機器ということもあり不具合が出る可能性があるので対応が難しいです。
- 当院ではまず電子カルテベンダーが対応しないため、施設内でパッチ適用を試みたが動作不良が発生したりと継続できない状況また、たとえ電子カルテベンダーが対応したとしても相乗りの部門ベンダーが対応しなければ意味がないすべてのベンダーがセキュリティ対策への共通認識を持ってほしい
- 当院としてはWindowsUpdateの最新化は必要性を感じているが、システムベンダーのポリシーとして対応が難しい。最新化後の都度のシステム健全性の確認など
- 当院と契約がある業者は、必要がある場合に業者で自動適用(契約内)してくれるか、必要な場合には有償で対応となる場合が多い。最新版のセキュリティパッチを常に適用するのが望ましいのは理解できるが、ソフトの動作や機器の動作といった面、費用面でとても現実的でない。
- 当院のネットワーク構成と業務への影響を鑑み、一般的な緊急性とコスト（発生時）を統合的に判断が必要。
- 動きがおかしくなることがあり　パッチは当てていない　逆にウイルスが入らないように努力している
- 動作の保証ができないといって、特に部門ベンダが積極的にWindowsUpdateをやりたがらない。チェックリストに記載があるのならば、厚生省からベンダに積極的に働きかけるべきである。
- 動作保証されるもの、ベンダーより情報があったものは適応する。また、FWのパッチは全て当てているが、スイッチ類はメモリーリークなど大きな障害になるもの以外は適応していません。
- 導入されている全システムでの検証が必要であり、費用もかかるが、多くのベンダーが対応してくれない。現時点では、非現実的と感ぜられる。
- 特になし
- 特に端末に関しては電子カルテの動作安定性を優先する関係上、一律でのパッチ適用は困難であり、業者からも推奨はされていないため、中々実施できない。
- 年に1回程度のパッチ適用を行っているが、本来は月1回程度は実施すべき。しかしパッチ適用による運用アプリへの影響を考慮すると現実は年2回程度と考える。運用には専従の院内システム担当者または、保守業者との契約が必要と考えるが、現実的には予算確保が難しい。
- 費用、人的に公的な支援が不可欠である
- 非常にコストがかかり厳しい
- 病院側も最新のセキュリティパッチの内容を把握する努力が必要
- 富士通の電子カルテは、OSのパッチをあてると、動作しなくなり、その都度動作確認と改修が必要になる。時間と費用が必要になる。
- 部門システムでIE11を使用している。実施出来たとしても全サーバ・端末へ対応は台数が多いため、コスト（費用と時間）が確保できるか不明
- 部門システム等の仕様によりパッチ適用ができないケースがある。
- 複数のシステム会社のアプリケーションが混在する医療システムPCにおいて、常にOSの最新セキュリティパッチを適用していくことはシステム動作保証の観点から非現実的であると思われます。つまりは最新のOSバージョンもリリースの度に不具合が発生しており、さらにOSバージョンアップリリースの度にその動作検証を10数社ある相乗りアプリケーションのすべてを動作検証することは現状の保守契約では実現不可であり保守契約費用の高騰が考えられ、費用面から病院システム運用継続も難しくなることが想定されます。 ガイダンスにあるとおり常に最新のOS環境で運用している病院情報システムが存在するでしょうか？存在するのであればモデルケースとして是非公開して頂きたいと思います。
- 閉じているから大丈夫の神話が長引いたため、セキュリティパッチを当てて最新化するという文化がなく、パッチを当てたことによるシステムへの影響が予測・対応する体制がとられていないためベンダーの担当者自体を、医療の世界以外のインターネット接続当たり前の世界を担当していたSEなどに切り替えないと、変わっていけないと思います。
- 閉域で運用中の電子カルテサーバ、端末へのセキュリティパッチ適用は、システム不具合発生リスク、作業コスト等を考慮してあまり現実的ではない。
- 閉域網でのセキュリティパッチを充てる必要があるかどうか。また、それにかかる費用は誰が負担するか？
- 閉域網での運用でセキュリティパッチの適用に関して重要性を低くとらえる文化が医療機関・ベンダー双方にあり、ガイドライン改定後もそれに関する提案などは少なく、機運が盛り上がらないでいる。最低限行うべきラインについて、具体的な製品名と標準的な設定などで示された方が上層部には理解しやすく、導入の判断を促すために、それに対する公的な助成が行われることが望ましい。
- 閉域網の医療情報システム端末について、保守業者にセキュリティパッチを適用したいと提案すると、「動作保証対象外」、「保守対象外」、「保守費とは別に作業費とさらなる保守費の上乗せ」と回答されます。中小規模病院では大規模病院と比較し、①立場が弱く強く出れない（保守業者に撤退されたりするとシステム更新時等に更新希望業者不在となるリスク）のと②経営が厳しいため追加費用の捻出が難しいという現実的な問題があります。セキュリティパッチ適用後の動作保証等は他業界では当たり前に行われており、特に医療関係の業者はセキュリティパッチ適用という現代の常識が無いように感じています。国や都道府県より、医療システム業者やメーカに対し強く、ユーザ側に対し追加費用が生じることなくセキュリティパッチ適用することを業界標準としてできるよう動いてもらいたいです。
- 保守業者が行わず院内システム管理者が適応を行っている。
- 保守契約にパッチ適用が含まれないので、都度予算調整が必要になる。このため、予算面から不可になるケースや速やかな対応が困難であるケースがある。また、業務システムへの影響が不透明であり、業務影響への懸念からパッチ適用が難しい。管理部署が異なる機器への統制が困難である。
- 保守事業者ごとに保守範囲が異なるため、択一式のアンケートでは回答が難しい。
- 本当に必要なパッチは適用する必要があると感じているが、動作保証や作業時間の確保などで対応することは難しい。
- 問39、自院で対応している。
- 問41に回答選択を追加していただきたいです。医療機関側で実施するため費用なし。

【接続元制限を実施している。(2-(8))】

ネットワーク機器の接続元制限の実施		
	施設数	割合
はい	439	79.8%
いいえ	111	20.2%

ネットワーク機器の接続元の管理設定と監視	管理設定		監視	
	施設数	割合	施設数	割合
病院	61	13.9%	81	18.5%
病院とネットワーク事業者が協力して	252	57.4%	182	41.5%
ネットワーク事業者に任せている	114	26.0%	152	34.6%
その他	12	2.7%	24	5.5%

管理設定(その他)
- システムベンダー
- ネットワーク事業者とシステムベンダー
- メーカー
- 機器による。運用委託事業者等。低機能のハブは制限していない。
- 上部組織(機構本部)
- 中央組織の職員
- 同一法人の中央組織および病院
- 保守事業者
- 保守用回線を導入しているシステムベンダー
- 本庁とネットワーク事業者に任せている
- 本部
- 本部中央管理

監視(その他)
- インターネットからのアクセスはすべて認めず、必要なメンテナンス回線は閉域網に限定している。
- システムベンダー
- ネットワーク事業者とシステムベンダー
- メーカー
- 監視していない
- 監視はしていない
- 監視はそれぞれの事業者任せ
- 監視は出来ていない
- 監視までにはいたっていない
- 期限を設けているため監視していない
- 機器による。運用委託事業者等。低機能のハブは制限していない。
- 上部組織(機構本部)
- 常時はネットワーク事業者に任せ、任意タイミングで病院が接続実績のみ確認。
- 常時監視はしていない
- 常時監視は行っていない
- 全てのネットワークの監視を実施できてはいない。
- 中央組織の職員
- 同一法人の中央組織および病院
- 病院でやれと言われたが、方法は提示されなかった。
- 保守事業者
- 保守用回線を導入しているシステムベンダー
- 本部
- 本部中央管理

【バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。(2-(9))】

バックグランドで動作している不要なソフトウェア及びサービスの停止	サーバ		端末PC	
	施設数	割合	施設数	割合
はい(定期的に確認している)	75	13.6%	78	14.2%
はい(システム導入時に確認したのみ)	420	76.4%	411	74.7%
いいえ	55	10.0%	61	11.1%

端末PCにエンドユーザが希望するソフトウェアをインストールすることが可能ですか。	施設数	割合
ソフトウェアを端末PCにインストールすることは、システム設定で禁止している。 エンドユーザの希望による端末インストールは行わない	126	22.9%
ソフトウェアを端末PCにインストールすることは、システム設定で禁止している。 ソフトウェアのインストールを病院に申請し、許可を受けたソフトウェアのみシステム管理者がインストールを行う	243	44.2%
ソフトウェアを端末PCにインストールすることは、運用で禁止している(システム設定で制限はかけていない)。 エンドユーザの希望による端末インストールは行わない	38	6.9%
ソフトウェアを端末PCにインストールすることは、運用で禁止している(システム設定で制限はかけていない)。 ソフトウェアのインストールを病院に申請し、許可を受けたソフトウェアのみシステム管理者がインストールを行う	93	16.9%
ソフトウェアを端末PCにインストールすることは、運用で禁止している(システム設定で制限はかけていない)。 ソフトウェアのインストールを病院に申請し、許可を受けたソフトウェアのみエンドユーザがインストールを行う	31	5.6%
エンドユーザが自由にソフトウェアを端末PCにインストールできる	19	3.5%

バックグランドで動作している不要なソフトウェア及びサービスを停止していない理由

- Word、Excel、Acrobat等、業務に必要であるため。
- カルテ端末はカルテ以外にもシステムが相乗りしているため、判断が難しい。
- ゲームソフト以外のソフトウェアに関して、バックグランドでどのように動作しているかわからないため削除後の不具合も考え削除していない。
- コスト
- これまで医療情報システムの管理は主に病院(医事課)が行っており、設問にある不要なものを停止するという知識が無かった。
- サーバーのインストールはシステム業者に一任のため、こちらではインストールされているアプリに関与していない。
- サーバや端末のすべてのソフトウェア、サービスを把握しないと不要なものの判断がつかないと思いますが、一般的なOSが動作している端末のサービスは約200ぐらい項目があり、実行中のサービスは40程度はあると思いますがそのすべてを把握することが困難で、その為不要と判断することができないサービスは停止できないと回答せざるをえないと思うのですが、本件はもっとアバウトに考えてもよいのでしょうか？
- サーバを職員が常に監視しておらず、定期的に確認を行ったとしても不要なソフトウェアかどうかの判断が難しい。
- サービス停止の影響を把握出来ない、また、サービス停止の方法が複雑なため、職員が対応できない。
- システム導入時の役務に含まれていなかった。慣例的に明らかに不要なソフトウェアやサービスの一部を停止している。
- バックグラウンド動作している不要なソフトウェアの判断が病院職員では難しいため。
- バックグランドで動作している不要なソフトウェア及びサービスが何か判断できない
- ベンダーがサーバーについては対応してもらえない
- ベンダーによる動作確認作業が必要な為
- ベンダーに任せているため
- ベンダー自身が不要なサービスを把握できていない。
- メーカー製PCを端末として使っているならば、不必要なソフトウェアとサービスは外しているつもりでも、OSとドライバーだけがインストールされた製品はないので、全てのソフトとサービスを把握ができるわけがなく、バックグランドで動作しているものすべてが止められるわけもなく、不要かどうかがわかるわけがないので。不要なソフトとサービスをすべて止めることができたと思っているのがおかしいと思う。
- 意図していない不要なソフトを検知するためにセキュリティーソフトを導入している。
- 一部完全に不要なサービスは止めているが、全て止めているわけではないため、いいえとしている。
- 何が不要かわからない。
- 何が不要なソフトウェアか判断がつかない為。
- 稼働時よりインターネトに接続している端末はなく、USBも院内で1台のみ接続が可能で、その端末を管理している者の許可が必要で、ウィルスチェック後に接続ができるようになる為。
- 各システム、各ベンダーでの対応が異なるため。
- 管理コスト、工数不足
- 管理端末数が600台強あり、全端末の管理は出来ない
- 基本的に必要なものしかインストールしていない理解であり、バックグラウンドで意図しないソフトウェアおよびサービスは動いていない認識である。さらに、ポート制限を徹底して行っており、意図しないバックグラウンドのソフトウェア、サービスがあってもネットワーク越しの通信自体ができないようにしているから。
- 機器による。特に医療機器は製造販売事業者からの情報開示がほぼ無い。
- 手が回らない。スキル不足。
- 専門知識が無い為、そういう確認作業に困難がある
- 全ての端末で不要なソフトの有無などを確認しきれていないため
- 全ての不要なサービスを停止しているかの確認はできていません。具体的に不要であれば起動していないことが望ましいプロセスを提示して頂けると、それに沿った確認は可能かと思います。
- 対応する知識を有していないから
- 端末においては、複数メーカーソフトが相乗りしており、停止することでの影響を考慮し、ベンダーと必要に応じて調整することとしているため。
- 端末一台一台把握することが難しいため
- 知識、技術不足
- 知識を持つ職員が少なく、体系的な管理ができていない
- 導入当時にシステムベンダにて不要と判断されたサービスは停止しているが、システム導入から7年経過し見直す必要性があると思うが人的リソースが足りず実施できていない。
- 必要な知識を有していない
- 必要性が不明
- 不要なソフトウェア、不要なサービスを調べる手間がかかる。停止した場合の動作トラブルの懸念。
- 不要なソフトウエア・サービスの判断がつかない
- 不要なソフトウェアかどうかの判断がつかない
- 不要なソフトウェアをインストールしていない。また確認できる人数も少ないため確認が出来ない。
- 不要なソフトウェア及びサービスの利用は停止している
- 不要なソフトウェア及びサービスを導入していないため
- 不要なソフトウェア及びサービスを把握していない。
- 不要なソフトの定義が曖昧でベンダーの理解が得られない。ベンダーですらOS標準は全て必要なソフトだと思っている。
- 不要なものがない
- 不要の判断がつかないため
- 複数のベンダがあり、電子カルテのサーバや端末PCは導入初期や定期的に対応できているが、一部のベンダが対応できていない。対応できていない理由は、作業分担面や費用面などの調整ができなかったため。
- 明らかに不要なものは停止しているが、何が不要なものか判断できないものもあるため100%停止しているかどうか判断がつかない

【パスワードは英数字、記号が混在した8文字以上とし、定期的に変更している。※二要素認証、または13文字以上の場合は定期的な変更は不要(令和7年度2-⑦)】【パスワードの使いまわしを禁止している(令和7年度2-⑧)】【二要素認証を実装している。または令和9年度までに実装予定である。(令和7年度2-⑩)】

機器に対するパスワード管理	サーバ		端末PC		ネットワーク	
	施設数	割合	施設数	割合	施設数	割合
パスワードは、英数字、記号が混在した13文字以上としている	135	24.5%	65	11.8%	128	23.3%
パスワードは、英数字、記号が混在した8文字以上とし、定期的に変更している	155	35.3%	257	58.5%	155	35.3%
左記を実現できていない	260	59.2%	228	51.9%	267	60.8%

サーバ室の入退室管理	施設数	割合
用紙記録による入退室者の把握	305	55.5%
防犯カメラのよる監視		
出入口付近	111	20.2%
サーバ室内	66	12.0%
物理鍵による入退室管理		
貸出記録を保管	121	22.0%
貸出記録の保管は行わない	150	27.3%
知識認証(IDとパスワードなど)による入退室管理		
入退室者の記録が残る	16	2.9%
入退室者の記録は残らない	29	5.3%
物理認証(カード認証など)による入退室管理		
入退室者の記録が残る	128	23.3%
入退室者の記録が残らない	16	2.9%
生体認証(指紋認証、静脈認証、顔認証など)による入退室管理		
入退室者の記録が残る	33	6.0%
入退室者の記録が残らない	1	0.2%
サーバ室は設置していない	34	6.2%

サーバに対する二要素認証の有無	施設数	割合	施設数	割合
一要素認証である	465	84.5%	465	84.5%
二要素認証(物理認証あるいは生体認証によるサーバ室への入退室管理とサーバに対する一要素(パスワード)認証)			70	12.7%
リモート接続では一要素認証となっている	55	10.0%		
リモート接続でも二要素認証を実現している	15	2.7%		
サーバに対する二要素認証を実装している			9	1.6%
リモート接続では一要素認証となっている	5	0.9%		
リモート接続でも二要素認証を実現し	3	0.5%		
その他	7	1.3%	7	1.3%

サーバの二要素認証の実現	施設数	割合
必ず実装する	20	4.3%
実装を検討中		
実装の可能性が高い	143	30.8%
実装の可能性が低い	229	49.2%
実装を行わない	73	15.7%

サーバに対する二要素認証の実装を行わない理由

- 今までコストが発生していないものなので事務長等の上司への理解が非常に難しい。
- IT知識不足のため
- オフライン運用なので
- ガイドライン上二要素認証の適用範囲が不明瞭であり、サーバ群まで適用が必要か不明のため
- クラウド型の電子カルテへ更改する予定のため。
- コスト
- コストが高いため
- コストを抽出できない。病院建て替え時にしか検討できない
- サーバOSに対するログインに二要素認証が義務付けられると考えていなかった
- サーバー室内に設置しているため。
- サーバに接続できるIPアドレスを制限することでサーバのセキュリティを強化する方向である。
- サーバ設置場所が施錠された室内であり操作者が限定されるため
- システムが未対応
- システムの更新時に2要素認証を検討する予定
- システムベンダーに現在のところその機能が無い
- システムベンダより推奨提案を受けていない為
- システム更新の予定がない
- システム導入にコストがかかるため
- そもそも金銭コスト・人的コスト上オンプレミスを持つべきではなく、Saasへの積極的移行とオンプレミスの廃止を目標と考えるため
- どのように実施するか実現方法なども特に検討していないため。
- ベンダーからの提案もなく、独自に価格を調べたが、高額であり実現不可能
- ベンダーが対応できない
- ベンダーとは話題になっていない(クライアント側はある)
- ベンダーメンテナンス上の問題。
- まだ検討していない。
- リモート保守時に対応ができないため
- リモート保守時に対応できないため
- 医療システム更新を令和10年度に予定しているため。
- 医療情報システム完治部門のみメンテナンス等で対応する運用のため
- 運用上の問題が懸念される事や、改修費用の負担が大きいため。
- 各種システムサーバーは、原則、保守業者のみの取り扱いのため
- 管理者として導入するメリットがない
- 関連費用の捻出
- 業務の煩雑化にしかならない。医療システム全体が多岐に渡ることに対して、管理をミクロ化しすぎることは望ましくない。
- 経営層からの承認がおりない。費用がない。
- 警備されているサーバー室内で、施錠されているサーバーラックに設置されているため。
- 現在更新の予定がない為。
- 現時点では対応検討の話もでていない
- 現時点では対応検討の話も出ていない
- 現時点で検討していなかったため、メーカーに対しても確認していないため。
- 現実的でない費用
- 後付けで設定するのは費用が高く、院内の理解が得られない。また、サーバごとにベンダーが異なるので実装方法にも違いが出て管理も困難。
- 構築ベンダーとも検討しておりますが、具体的な解決にまで至っておりません。
- 今年サーバーを入れ替えたばかりで早期実装は難しい
- 次期サーバ更新時に対応予定
- 次期システム2029年1月対応
- 設問34のとおり、サーバは管理者権限の使いまわしを行っており、現状では二要素認証の実装が不可能であるため。
- 対応の煩雑さと費用的な理由になります
- 費用がかかる、またシステム更新が近くなるので余分な出費となる
- 費用的な問題と、システムベンダーが対応不可(更新が必要)という理由※稼働済システムは努力義務と言う認識です
- 費用捻出が難しい
- 費用の面から実装を行わない。令和11年度に 医療情報システムの更改を行うときに導入する予定である。
- 必要な知識を有していないから
- 必要性を感じないため
- 病院情報管理システムの次回更新(令和12年1月)に併せ実装予定のため
- 物理的手段(鍵・入室許可)を講じている。論理的には令和7年度中に接続デバイスが実装予定。
- 毎年の予算申請に導入申請をしても通らず、却下される為
- 予算がないため
- 予算が出ない
- 令和10年度に医療情報システムを更新予定であるため
- 令和8年3月末にて閉院のため
- 令和9年度までに対応は事業者が不可能と回答

【パスワードは英数字、記号が混在した8文字以上とし、定期的に変更している。※二要素認証、または13文字以上の場合は定期的な変更は不要(令和7年度2-⑦)】【パスワードの使いまわしを禁止している(令和7年度2-⑧)】【二要素認証を実装している。または令和9年度までに実装予定である。(令和7年度2-⑩)】

端末PCに対する二要素認証の有無	施設数	割合
一要素認証である	449	81.6%
端末PCは二要素認証を導入しているが、医療情報システムネットワークに接続する部門システム端末(ワークステーション等)は一要素認証の端末がある	62	11.3%
医療情報システムに接続する端末は全て二要素認証を導入している	20	3.6%
その他	19	3.5%

端末PCの二要素認証の実現	施設数	割合
必ず実装する	67	14.9%
実装を検討中		
実装の可能性が高い	172	38.3%
実装の可能性が低い	165	36.7%
実装を行わない	45	10.0%

ネットワーク機器に対する二要素認証	施設数	割合	施設数	割合
一要素認証である	483	87.8%	483	87.8%
二要素認証(物理認証あるいは生体認証によるサーバ室等への入退室管理とネットワーク機器に対するパスワード認証)			48	8.7%
リモート接続では一要素認証となっている	37	6.7%		
リモート接続でも二要素認証を実現している	11	2.0%		
ネットワーク機器に対する二要素認証を実装している			8	1.5%
リモート接続では一要素認証となっている	2	0.4%		
リモート接続でも二要素認証を実現している	6	1.1%		
その他	11	2.0%	11	2.0%

ネットワーク機器の二要素認証の実現	施設数	割合
必ず実装する	10	2.1%
実装を検討中		
実装の可能性が高い	110	22.8%
実装の可能性が低い	266	55.1%
実装を行わない	97	20.1%

二要素認証を実装しない理由

端末PC

- アプリケーションで二要素認証を実装しているため
- オフライン運用なので
- コスト
- システムで二要素認証を実装する為。
- システムベンダーに現在のところその機能が無い
- システム更新の予定がない
- システム導入にコストがかかるため
- どのように実施するか実現方法なども特に検討していないため。
- 医療システム更新を令和10年度に予定しているため。
- 運用上の問題が懸念される事や、改修費用の負担が大きいため。
- 運用上の理由から現時点では検討していない。
- 外部への接続が不能であること。パスワードを半年ごとに変更していること
- 看護業務に差し支える
- 関連費用の捻出
- 業務効率の低下とコスト増
- 経営層からの承認がおりない。費用がない。
- 現時点で検討していなかったため
- 現実的でない費用
- 個々に任せているため
- 今までコストが発生していないものなので事務長等の上司への理解が非常に難しい。
- 次期システム2029年1月対応
- 実装を検討したが予算の都合により対象をアプリケーションのログイン時とした。
- 対応の煩雑さと費用的な理由になります
- 端末PCのログインユーザは共通としているため、ソフト側での二要素認証対応を予定している。
- 費用
- 費用がかかる、またシステム更新が近くなるので余分な出費となる
- 費用的な問題と、システムベンダーが対応不可(更新が必要)という理由※稼働済システムは努力義務と言う認識です
- 費用捻出が難しい
- 費用面
- 費用の面から実装を行わない。令和11年度に 医療情報システムの更改を行うときに導入する予定である。
- 必要な知識を有していないから
- 不便
- 不要。
- 本庁担当職員とベンダーとの協議等で必要な場合に取り入れると思われるが、現時点では計画の予定がないため
- 毎年の予算申請に導入申請をしても通らず、却下される為
- 予算がないため
- 予算が出ない
- 令和10年度に医療情報システムを更新予定であるため
- 令和8年3月末にて閉院のため

ネットワーク機器

- DHCPでなく、固定IPを使用。また、WI-FIはステルス型で認証を必要とし、システム管理者以外の接続が難しいと考えるため。
- ID/パスワードの2段階認証を実装できているため
- IT知識不足のため
- ガイドライン上二要素認証の適用範囲が不明瞭であり、NW機器まで適用が必要か不明のため
- コスト
- コスト。
- コストがかかりすぎる
- コストが高くなるため
- コストの関係
- コストの捻出が難しい
- サーバ・端末PCについては前述の通りだが、ネットワーク機器については二要素認証を考えていなかった為
- サーバーと同じ理由です。
- サーバー同様
- システムの複雑化
- システムベンダによる設定情報がないとログイン不可のため
- システム導入にコストがかかるため
- どのように実施するか実現方法なども特に検討していないため。
- ネットワーク機器が二要素認証に対応しておらず、改修費用の負担が大きいため。
- ネットワーク機器が二要素認証未対応
- ネットワーク機器についての二要素認証はガイドラインで定められていないため。
- ネットワーク機器にも二要素認証が必要との情報を知らなかったため
- ネットワーク機器に対して要件がないため
- ネットワーク機器に対する二要素認証の必要性を把握していませんでした。
- ネットワーク機器に二要素認証が義務付けられると考えていなかった
- ネットワーク機器の管理がベンダーの提示したものをそのまま利用している為
- ネットワーク機器の管理を保守業者に委託しているため
- ネットワーク機器は関係者しか扱うことができないため。
- ベンダーからの提案もなく、独自に価格を調べたが、高額であり実現不可能
- ベンダーで対応できない
- ベンダーとは話題になっていない
- ベンダーメンテナンス上の問題。
- ベンダー等保守業者のみの取り扱いのため
- 医療システム更新を令和10年度に予定しているため。
- 医療情報システム管理部門のみメンテナンス等対応する運用のため
- 一般職員が操作できる場所にない為、1要素認証で充分と考えている
- 一般的なネットワーク機器における二要素認証は、Azureなどの外部認証サーバを使用した二要素認証であることが多く、これが医療情報システムの安全管理に関するガイドラインに準拠しているか不明であることと、通常は外部との通信を遮断していることから外部認証事体も使用が困難であることが理由となります。
- 該当機器なし
- 管理機能に接続できるIPアドレスを制限することでセキュリティを強化する方向である。
- 管理者として導入するメリットがない
- 関連費用の捻出
- 機器が機能を実装していない。
- 機器が対応していない
- 機器が対応できない
- 機器更新の予定がない
- 機器仕様上二要素認証に対応できるとは限らず、現在採用している機器では二要素認証が導入不可。機器更新が発生する際は再検討とする。
- 機器上実装が困難
- 業者が対応していない。また出来るようになっても更新時しか検討できない
- 経営層からの承認がおりない。費用がない。
- 現時点では対応検討の話もでていない
- 現時点では対応検討の話も出ていない
- 構築ベンダーとも検討しておりますが、具体的な解決にまで至っておりません。
- 今までコストが発生していないものなので事務長等の上司への理解が非常に難しい。
- 今後検討は行うが、令和9年度までの実装は未定。
- 施錠されているシャフト内で、施錠されているHUB BOXに設置しているため。
- 次期システム2029年1月対応
- 次期ネトワーク更新時に検討する。
- 実装方法を把握できていないため、また各機器において個別に設定することは現実的に不可と思われるため
- 接続する管理コンソールで実施を検討
- 対応していない機器を導入している
- 対応の煩雑さと費用的な理由になります
- 対応機器を導入していない。
- 導入費用が捻出できない
- 二要素認証がないため
- 二要素方法がないため
- 費用
- 費用捻出が難しい・実現自体が難しい
- 費用の面から実装を行わない。令和11年度に 医療情報システムの更改を行うときに導入する予定である。
- 必要な知識を有していないから
- 必要性を感じていないため
- 必要性を感じない
- 必要性を感じないため
- 不要。
- 物理的手段(鍵・入室許可)を講じている。論理的には令和7年度中に接続デバイスが実装予定。
- 無理なので。ネットワーク機器がサーバー室だけにあるわけがないし、設置した箇所全部を2要素認証にするほどの予算が出るわけがない。
- 予算がないため
- 予算が出ない
- 予算都合があわない。サーバー機のため、設置は保守ベンダーとなるため。
- 利便性が低下する
- 利用上の理由
- 令和10年度に医療情報システムを更新予定であるため
- 令和8年3月末にて閉院のため
- 令和9年度までに対応は事業者が不可能と回答

【USBストレージ等の外部記録媒体や情報機器に対して接続を制限している。(令和7年度 2-⑨)】

サーバに対するUSBメモリの使用	施設数	割合
外部記録媒体や情報機器を接続しても、サーバが認識できないシステム設定となっている	94	17.1%
許可された外部記録媒体や情報機器だけが、サーバが認識できるシステム設定なっている	122	22.2%
外部記録媒体や情報機器を認識する		
接続は運用で禁止されている	134	24.4%
許可された外部記録媒体や情報機器のみ、サーバに接続する運用となっている(運用での制限)	100	18.2%
外部記録媒体や情報機器のサーバへの接続を制限していない	92	16.7%
その他	8	1.5%

端末PCに対するUSBメモリの使用	端末PC				部門システム管理者が使用する部門システム端末				エンドユーザが使用する部門システム端末			
	施設数	割合	施設数	割合	施設数	割合	施設数	割合	施設数	割合	施設数	割合
外部記録媒体や情報機器の接続を許可していない												
システム設定による接続制御	149	27.1%	167	30.4%	91	16.5%	152	27.6%	131	23.8%	202	36.7%
システム設定ではなく、運用による接続制御	18	3.3%			61	11.1%			71	12.9%		
外部記録媒体や情報機器の接続は医療情報システム管理部門に依頼を行う												
システム設定による接続制御	103	18.7%	113	20.5%	67	12.2%	101	18.4%	49	8.9%	77	14.0%
システム設定ではなく、運用による接続制御	10	1.8%			34	6.2%			28	5.1%		
病院に申請し許可された外部記録媒体や情報機器のみ端末PCに接続することができる												
システム設定による接続制御	204	37.1%	223	40.5%	138	25.1%	204	37.1%	117	21.3%	185	33.6%
システム設定ではなく、運用による接続制御	29	5.3%			66	12.0%			68	12.4%		
外部記録媒体や情報機器を自由に接続できる	24	4.4%	24	4.4%	63	11.5%	63	11.5%	53	9.6%	53	9.6%
その他	13	2.4%	13	2.4%	30	5.5%	39	7.1%	33	6.0%	33	6.0%

【3. インシデント発生に備えた対応】

インシデント発生時における組織内の連絡体制図の整備	施設数	割合
整備しており定期的な見直しを実施している	370	67.3%
整備しているが定期的な見直しは実施していない	138	25.1%
整備を計画している	33	6.0%
整備する計画はない	9	1.6%

データやシステムのバックアップの対象の検討	施設数	割合
すべての医療情報システムのデータはバックアップが取れている	248	45.1%
診療を継続するために必要な情報を検討している		
必要と判断したデータはバックアップが取れている	181	32.9%
バックアップが取れているのは、必要と判断した情報の一部である	52	9.5%
診療を継続するために必要な情報を検討しておらず、ベンダーが提案したデータのバックアップを取っている	60	10.9%
データのバックアップを取っていない	9	1.6%

データやシステムのオフラインバックアップ	施設数	割合
オフラインバックアップを実施している	394	72.8%
オフラインバックアップを実施できていない	147	27.2%

バックアップの手法				
テープバックアップ	イミュータブルバックアップ	クラウド保存	施設数	割合
●			230	58.4%
	●		57	14.5%
		●	51	12.9%
●	●		15	3.8%
●		●	26	6.6%
	●	●	9	2.3%
●	●	●	6	1.5%

バックアップのタイミング	施設数	割合
日次	476	88.0%
2日に1回	6	1.1%
3日に1回	8	1.5%
4日から7日に1回	33	6.1%
8日から14日に1回	3	0.6%
15日以上	15	2.8%

バックアップは何世代行っているか	施設数	割合
1世代	71	13.1%
2世代	60	11.1%
3世代	172	31.8%
4世代	19	3.5%
5世代	42	7.8%
6世代以上	177	32.7%

データバックアップの復旧手順の確認	施設数	割合
データバックアップの復旧手順を確認し、復旧の実証訓練を行っている	34	6.3%
データバックアップの復旧手順を確認しているが、復旧の実証訓練は実施していない	214	39.6%
データバックアップの復旧は保守事業者に一任しており、医療機関として復旧手順の確認は行っていない	285	52.7%
その他	8	1.5%

サイバー攻撃を想定した事業継続計画(BCP)の策定	施設数	割合	施設数	割合
策定している				
厚生労働省が作成したBCPを参考	326	59.3%	465	84.5%
他院が作成したBCPを参考	75	13.6%		
自施設で独自に策定した	64	11.6%		
策定していない	85	15.5%	85	15.5%

事業継続計画(BCP)の定期的な見直し	施設数	割合
はい	319	68.6%
いいえ	146	31.4%

【4. 規程類の整備（令和7年度）】

体制構築について、具体的な実施方法を運用管理規程等に定めていますか。		
	施設数	割合
はい（定期的に見直している）	285	51.8%
はい（定期的な見直しはできていない）	216	39.3%
いいえ	49	8.9%

医療情報システムの管理・運用について、具体的な実施方法を運用管理規程等に定めていますか。		
	施設数	割合
はい（定期的に見直している）	287	52.2%
はい（定期的な見直しはできていない）	224	40.7%
いいえ	39	7.1%

インシデント発生に備えた対応について、具体的な実施方法（サイバー攻撃を想定した事業継続計画（BCP））を運用管理規程等に定めていますか。		
	施設数	割合
はい	356	64.7%
いいえ	194	35.3%