令和５年7月7日	第100回社会保障審議会医療部会	資料３

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

医療機関におけるサイバーセキュリティ対策チェックリストと立入検査の実施について（報告）

厚生労働省 医政局

Ministry of Health, Labour and Welfare of Japan

医療機関の管理者が遵守するべき事項への位置づけ

第16回 健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ（令和５年３月23日）資料２－２改

健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループでの議論を踏まえ、下記のとおり、サイバーセキュリティの確保を医療機関の管理者が遵守するべき事項に位置づけた。

改正概要・対応の方向性

○　医療法施行規則第14条第２項を新設し、病院、診療所又は助産所の管理者が遵守すべき事項として、サイバーセキュリティの確保について必要な措置を講じることを追加する。

○　令和５年３月10日公布、４月１日施行

○　「必要な措置」としては、最新の「医療情報システムの安全管理に関するガイドライン」（以下「安全管理ガイドライン」という。）を参照の上、サイバー攻撃に対する対策を含めセキュリティ対策全般について適切な対応を行うこととする。

○　安全管理ガイドラインに記載されている内容のうち、優先的に取り組むべき事項については、厚生労働省においてチェックリストを作成し、各医療機関で確認できる仕組みとする。

○　また、医療法第25条第１項に規定に基づく立入検査要綱の項目に、サイバーセキュリティ確保のための取組状況を位置づける。

◎医療法施行規則（昭和二十三年厚生省令第五十号）

第十四条　（略）
２　病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないように、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）を確保するために必要な措置を講じなければならない。

※　下線部を新設。

令和５年度立入検査要綱

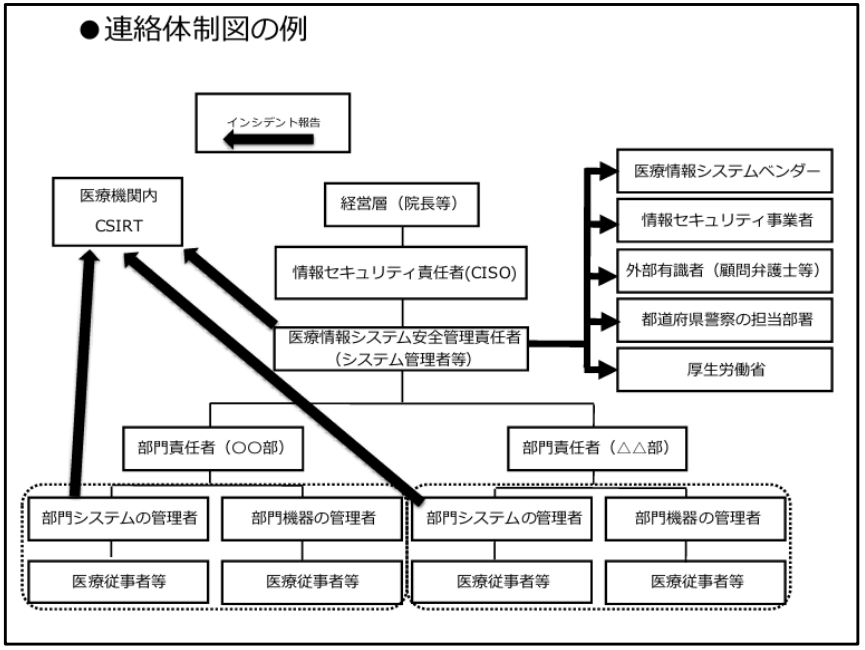
医療法第25条第１項の規定に基づく立入検査要綱の項目に、サイバーセキュリティ確保のための取組状況を位置づけた（令和５年６月）。

（改正内容）

●新規項目を設け（2-19）、備考欄に以下の内容を記載。

2-19 サイバーセキュリティを確保するために必要な措置を講じているか

- 必要な措置については、「医療情報システムの安全管理に関するガイドライン第6.0版」を参照。
- 医療機関において優先的に取り組むべき事項として、「医療機関におけるサイバーセキュリティ対策チェックリスト」及び「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」におけるチェックリストに必要な事項が記入されているかを確認。
- 上記チェックリストにおいて医療機関に求める項目のうち、インシデント発生時の連絡体制図については、連絡体制図の提示を求めることにより、その有無を確認。



サイバーセキュリティチェックリストについて　①医療機関確認用

○　令和5年度中

*以下項目は令和5年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*２（２）及び２（３）については、事業者と契約していない場合には、記入不要です。
*1回目の確認で「いいえ」の場合、令和5年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付） 1回目	目標日	2回目
1 体制構築	（1）医療情報システム安全管理責任者を設置している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**			
	（１）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。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（２）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。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	(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）を提出してもらう。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	サーバについて、以下を実施している。			
	(4)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。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	（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している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	(6)アクセスログを管理している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	ネットワーク機器について、以下を実施している。			
	(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。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	(8)接続元制限を実施している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
3 インシデント発生に備えた対応	(1)インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。	はい・いいえ（ / ）		

○参考項目（令和６年度中）

*以下項目について、令和６年度中にすべての項目で「はい」にマルが付くよう取り組んでください。

	チェック項目	確認結果（日付） 1回目	目標日	2回目
2 医療情報システムの管理・運用	**サーバについて、以下を実施している。**			
	(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。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	(9)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。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	端末PCについて、以下を実施している。			
	(4)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。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	(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している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	(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。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	(9)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。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
3 インシデント発生に備えた対応	(2)インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	(3)サイバー攻撃を想定した事業継続計画（BCP）を策定、又は令和６年度中に策定予定である。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）

サイバーセキュリティチェックリストについて　②事業者確認用

○　令和５年度中

*以下項目は令和5年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*1回目の確認で「いいえ」の場合、令和5年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付）		
		1回目	目標日	2回目
1 体制構築	(1)事業者内に、医療情報システム等の提供に係る管理責任者を設置している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**			
	(2)リモートメンテナンス（保守）している機器の有無を確認した。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	(3)医療機関に製造業者/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）を提出した。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	サーバについて、以下を実施している。			
	(4)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。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	(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している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	(6)アクセスログを管理している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	ネットワーク機器について、以下を実施している。			
	(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。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	(8)接続元制限を実施している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）

○　参考項目（令和６年度中）

*以下項目について、令和６年度中にすべての項目で「はい」にマルが付くよう取り組んでください。

	チェック項目	確認結果（日付）		
		1回目	目標日	2回目
2 医療情報システムの管理・運用	**サーバについて、以下を実施している。**			
	(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。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	(9)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。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	端末PCについて、以下を実施している。			
	(4)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。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	(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している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	(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。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）
	(9)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。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）

薬局の管理者が遵守するべき事項への位置づけ

健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループでの議論を踏まえ、下記のとおり、サイバーセキュリティの確保を薬局の管理者が遵守するべき事項に位置づけた。

改正概要・対応の方向性

○　薬機法施行規則第11条第２項を改正し、薬局の管理者が遵守すべき事項として、サイバーセキュリティの確保について必要な措置を講じることを追加する。

○　令和５年３月31日公布、４月１日施行

○　「必要な措置」としては、最新の安全管理ガイドラインを参照の上、サイバー攻撃に対する対策を含めセキュリティ対策全般について適切な対応を行うこととする。

◎医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律施行規則（昭和三十六年厚生省令第一号）

第十一条　（略）
２　法第八条第三項の薬局の管理者が遵守すべき事項は、次のとおりとする。
一　保健衛生上支障を生ずるおそれがないように、その薬局に勤務する薬剤師その他の従業者を監督し、その薬局の構造設備及び医薬品その他の物品を管理し、その薬局の業務に係るサイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）の確保のために必要な措置を講じ、その他その薬局の業務につき、必要な注意をすること。

※　下線部を新設。

厚生労働省 ひと、くらし、みらいのために
Ministry of Health, Labour and Welfare

参考資料

厚生労働省 医政局

Ministry of Health, Labour and Welfare of Japan

（参考）医療機関におけるサイバーセキュリティ対策チェックリストマニュアル ～医療機関・事業者向け～

マニュアルの例①（P1.）

医療機関におけるサイバーセキュリティ対策チェックリストマニュアル
～医療機関・事業者向け～

本マニュアルは、「医療機関におけるサイバーセキュリティ対策チェックリスト（以下「チェックリスト」という。）」をわかりやすく解説するものです。チェックリストを活用する際に、ご覧ください。

～はじめに～

○　医療機関等に対するサイバー攻撃は近年増加傾向にあり、その脅威は日増しに高まっています。医療機関が適切な対策をとることで、こうしたサイバー攻撃等の情報セキュリティインシデントによる患者の医療情報の流出や、不正な利用を事前に防ぐことが重要です。医療情報システムは、効率的かつ正確に医療行為を行う上で重要な役割を果たしています。医療の継続性を支える観点からも、適切な管理の下、医療情報システムを利用することが求められています。

○　医療機関等におけるサイバーセキュリティ対策については、厚生労働省が作成している「医療情報システムの安全管理に関するガイドライン（以下「ガイドライン」という。）」を参照の上、適切な対応を行うこととしているところ、このうち、まずは医療機関が優先的に取り組むべき事項をチェックリストにまとめました。

本マニュアルは、医療機関におけるチェックリストを用いた確認の実行性を高めるために、サイバーセキュリティ対策に馴染みがない方にもご理解いただけるよう、チェック項目の考え方や確認方法、用語等についてなるべく平易な言葉で解説することを目指しました。

○　医療機関および医療情報システム・サービス事業者（以下「事業者」という。）は、本マニュアルを参照しつつチェックリストを活用して、日頃から実のあるサイバーセキュリティ対策を行って下さい。

マニュアルの例②（P6.）

2　医療情報システムの管理・運用　【医療機関確認用・事業者確認用】

（用語の解説）
医療情報システム全般：サーバ、端末PC、ネットワーク機器を指します。
サーバ：電子カルテサーバやレセコンサーバ等、ネットワーク上で情報やサービスを提供するコンピュータを指します。
ネットワーク機器：無線LANやルータ等を指します。

（1）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。
（医療情報システム全般）

医療情報システムで用いる情報機器等の安全性を確保するために、情報機器等の所在と、それらの使用可否の状態を適切に管理する必要があります。そのため、企画管理者は医療機関で所有する医療情報システムで用いる情報機器等について機器台帳を作成して管理を行い、情報機器等が利用に適した状況にあることを確認できるようにしてください。また、医療機関の経営層は定期的に管理状況に関する報告を受け、管理実態や責任の所在が明確になるよう、監督してください。台帳で管理する内容としては情報機器等の所在や利用者、ソフトウェアやサービスのバージョンなどが想定されます。

▶経営管理編 1.2.1 ＜管理責任＞ ②
▶企画管理編 9.1

（用語の解説）
情報機器等の所在：実際の設置場所やネットワーク識別情報等を指します。
（補足）
サーバ、端末PC、ネットワーク機器のうち、自身の医療機関で保有する医療情報システムについて台帳管理を行っていれば、「医療機関確認用」2（1）の「はい」にマルをつけてください。

●機器台帳の例

管理番号	メーカー	OS	ソフトウェア	ソフトウェアバージョン	IPアドレス	コンピュータ名	設置場所	利用者	登録日	状態	説明
001	A社	Win11	○○電子カルテ	2.0	192.168.0.0	Room1のPC1	Room1	a医師（○○科）	2020/12/1	稼働	
002	A社	Win11	○○電子カルテ	1.2	192.168.0.0	Room1のPC2	Room1	b医師（○○科）	2020/12/1	停止	メンテナンス
003	A社	Win8	○○電子カルテ	2.0	192.168.0.0	Room2のPC1	Room2	c医師（△△科）	2014/10/1	稼働	
004	B社	Win11	○○管理システム	5.0.1	192.168.0.0	Room3のPC1	Room3	a医師（○○科）、b医師（○○科）、c医師（△△科）	2021/8/1	稼働	

（参考）医療機関におけるサイバーセキュリティ確保に係る立入検査の手引き ～立入検査担当者向け～

【令和５年度版】　医療機関におけるサイバーセキュリティ確保に係る立入検査の手引き ～立入検査担当者向け～

＜　医療機関におけるサイバーセキュリティ対策に係る立入検査について　＞

○　病院、診療所および助産所の立入検査の際は、サイバーセキュリティ確保のために必要な措置が行われているかを確認することとしています。
○　立入検査担当者は、「医療機関におけるサイバーセキュリティ対策チェックリスト」に必要な事項が記入されているかを、下記のとおり確認してください。
○　なお、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」ではチェックリストの項目の考え方や確認方法、用語等について分かりやすく解説しています。立入検査担当者におかれても、立入検査に先んじてご一読ください。

＜　立入検査時に確認する事項　＞

①「医療機関確認用」チェックリストについて

○　「医療情報システムの有無」の「いいえ」欄にマルがつく場合、それ以下すべての項目は確認不要です。
○　「医療情報システムの有無」の「はい」欄にマルがつく場合、チェック項目すべてに、１回目の確認結果（日付と「はい」または「いいえ」）が記入されていることを確認してください。
（※）２（２）及び２（３）は医療機関が事業者と契約していない場合には、確認が不要になります。
○　「いいえ」にマルが付いた項目については、目標日の記入を確認してください。また、令和5年度中に「はい」にマルがつくように、医療機関に取組を促してください。
○　３（１）の連絡体制図については立入検査までに作成することを求めています。立入検査時は、連絡体制図の有無を、現物を見て確認してください。連絡体制図が無い場合は、早急に作成するよう促してください。

②「事業者確認用」チェックリストについて

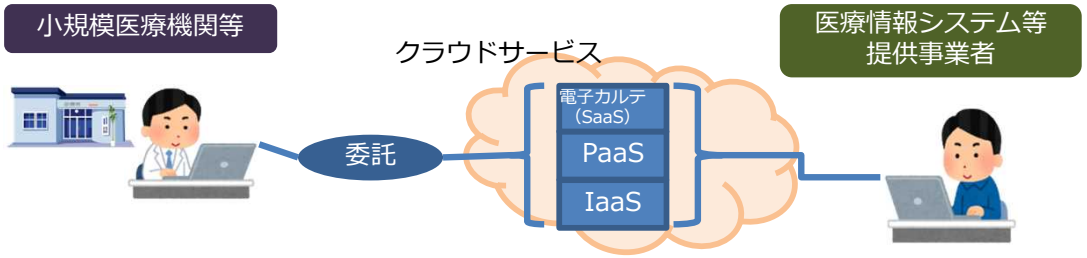
○　医療機関が事業者と契約している場合には、「事業者確認用」も確認してください。
○　「事業者確認用」は、医療機関と契約している事業者ごとに作成するため、複数事業者と契約している場合は、すべてを確認してください。
○　チェック項目について、１回目の確認結果（日付と「はい」または「いいえ」）が記入されていることを確認してください。
○　契約内容によっては、一部の項目の確認が不要になることもあります。その場合、同項目について「医療機関確認用」または別の事業者が作成する「事業者確認用」に記入があれば問題ありません。
（※）例えば、サーバのみを提供している事業者の場合、ネットワークの状況は必ずしも把握できていない等のケースが想定されます。
○　「いいえ」にマルがついた項目については、目標日の記入を確認してください。また、令和5年度中に「はい」にマルがつくように事業者の取組を促すよう、医療機関に伝えてください。

※　令和５年度の立入検査では、①②ともに、参考項目の検査は不要です。

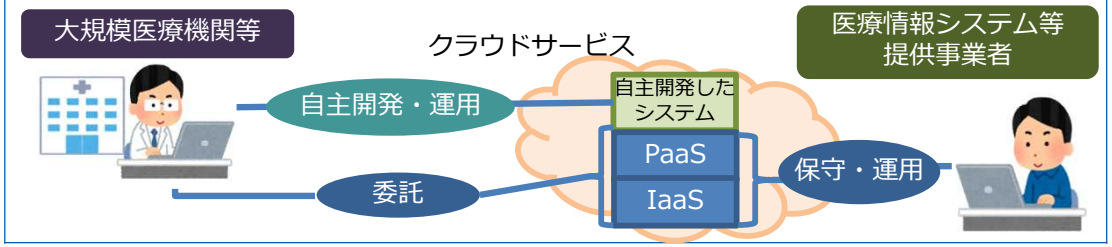
（参考）医療情報システムの安全管理に関するガイドライン 第6.0版主な改定ポイント（概要）

外部委託、外部サービスの利用に関する整理

クラウドサービスに医療情報システムの運用管理を、すべてを外部に任せる場合

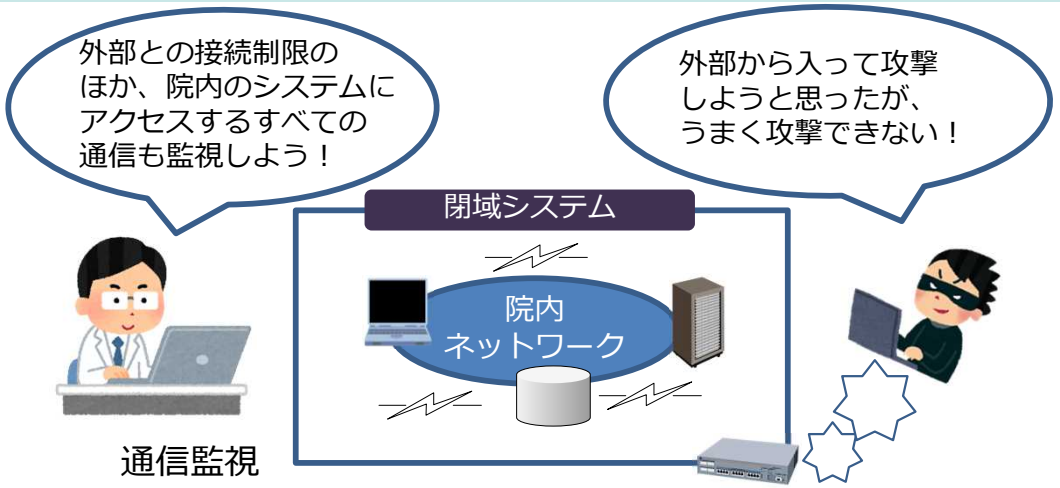


クラウドサービスに医療情報システムの一部を運用管理を外部に任せる場合



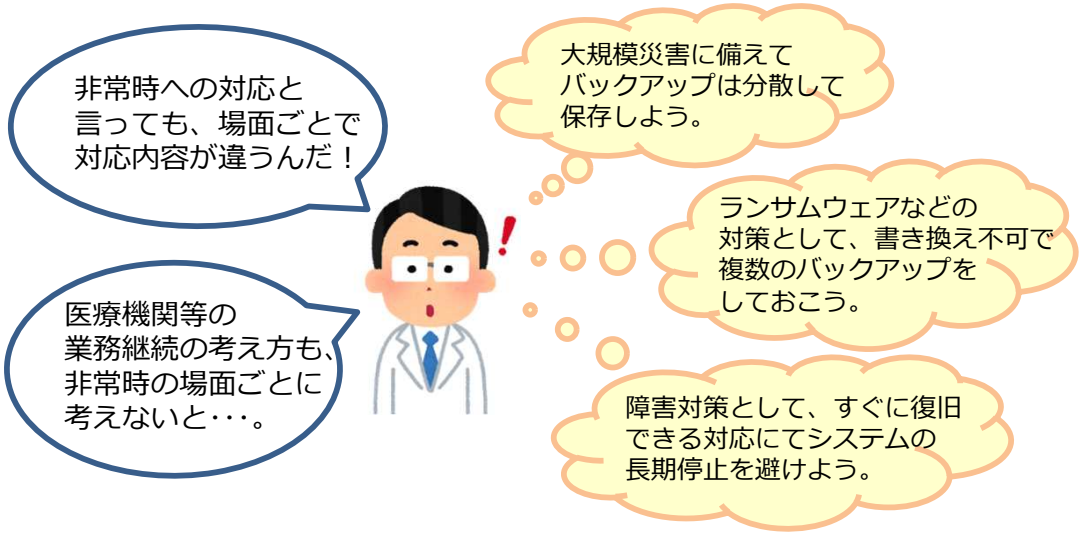
ネットワーク境界防御型思考／ゼロトラストネットワーク型思考

ゼロトラストの思考を取り入れることで、個々の外部からの侵入にも適切な対応が可能となります。



災害、サイバー攻撃、システム障害等の非常時に対する対応や対策

非常時場面ごとのバックアップの考え方の違い（例）



本人確認を要する場面での運用（eKYCの活用）の検討