CITY OF YOKOHAMA

立入検査における
院内サイバーセキュリティについて

横浜市医療局健康安全部医療安全課

令和６年２月９日　　横浜市病院安全管理者会議

明日をひらく都市
OPEN × PIONEER

1. 医療安全課の立入検査の概要・主な指導項目

2. サイバーセキュリティに関する
   立入検査項目について

1. 医療安全課の立入検査の概要・主な指導項目

2. サイバーセキュリティに関する
立入検査項目について

医療安全課の立入検査の概要

明日をひらく都市
OPEN × PIONEER
YOKOHAMA

■定期立入検査

医療法第25条第１項及び厚生労働省の実施要綱に基づき、原則年に１回実施

目的：

医療法及び関連法令により規定された人員及び構造設備を有し、
かつ、適正な管理を行っているか否かについて検査することにより、
病院を科学的で、かつ、適正な医療を行う場にふさわしいものとする

（厚生労働省医政局「医療法第２５条第１項の規定に基づく立入検査要綱」より）

■臨時立入検査

医療安全の確保に必要な場合、随時

医療安全課の立入検査の概要

明日をひらく都市
OPEN × PIONEER
YOKOHAMA

■確認項目

・医療従事者数の充足状況、職員の健康管理体制
・医療の安全管理のための体制の確保
・院内感染予防の体制の確保
・放射線機器や医療機器の管理状況、安全管理体制
・医薬品の管理状況や検体検査の業務の適正な実施
・診療録などの記録・保存状況
・病室や診察室などの構造設備
・防火防災体制　　等

医療安全課の立入検査の概要
■特に注意いただきたい指導事項（例）

・**医療ガス設備に係る点検が不十分**
→定期点検（３か月、６か月、12か月）は年４回、適切な内容で実施する
日常点検は休日も含めて毎日実施する

「医療ガスの安全管理について」（通知）、「医療ガス設備の保守点検指針」を確認してください。

医療安全課の立入検査の概要

■特に注意いただきたい指導事項（例）

・医薬品の管理が不十分
→処方量と在庫数の照合を定期的に実施する
返却薬や廃棄薬の数量も適正に管理する
鍵の保管場所、暗証番号を定期的に変更する。
保管庫に防犯カメラの設置も有効。

医療安全課の立入検査の概要

■特に注意いただきたい指導事項（例）

・看護記録への記載が不十分
院内感染事例に係る患者・家族への説明内容が記載されていない

※診療録や看護記録に記載のない事実は存在しないものと判断される可能性

→院内感染マニュアルに患者・家族への説明や対応に関する規定を追記し、職員に周知する

1. 医療安全課の立入検査の概要・主な指導項目

2. サイバーセキュリティに関する
立入検査項目について

サイバーセキュリティに係る取組

令和５年

４月１日　医療法施行規則の一部を改正
・病院等の管理者が遵守すべき事項に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

５月31日　「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」の策定・公開（厚生労働省）

６月９日　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等の作成及び立入検査の実施（厚生労働省 医政参発0609第1号）

６月19日　医療法第25条第１項の規定に基づく立入検査要綱の一部改正
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

■サイバーセキュリティ関連の事故事例

・大阪急性期・総合医療センター　（2022年10月）

委託先業者のシステムから侵入したランサムウェアにより電子カルテシステムが閲覧不能となった。通常の診療体制の復旧まで約２か月を要した。

【主な原因・課題】

・外部接続機器の脆弱性を放置していた

・ユーザー全てに管理者権限を与えていたため、攻撃者に管理者権限を利用され、ウイルス対策ソフトをアンインストールされた。

・パスワードが共通であり、一つのパスワードが窃取されると他の全てのサーバーも乗っ取り可能だった。

・電子カルテシステムにウイルス対策ソフトが未設定だった。

■サイバーセキュリティ関連の事故事例

・宇陀市立病院　（2018年10月）

　私物の機器を持込接続したことで侵入したと推測されるランサムウェアにより電子カルテシステムが閲覧不能となった。全データの復元まで５か月以上を要した。

【主な原因・課題】

・「私物の機器を接続しない」という基本的ルールが守られていなかった。

・内部聞き取り調査で上記ルール違反の報告がされていない。←ガバナンスが機能していない。

・システムログの保全を行わないままシステムを再セットアップしたことで正確な原因究明ができなかった。また、個人情報の漏洩の有無も判断がつかない状況となった。

サイバーセキュリティに関する立入検査項目

明日をひらく都市
OPEN×PIONEER
YOKOHAMA

■令和５年度立入検査における主な確認項目（サイバーセキュリティ関連）

・システム管理規程の整備状況

・事故発生時の連絡体制、対応フローの整備状況

・USBメモリの使用状況
（病院管理の物のみ使用可能か、貸出管理簿の整備状況　等）

・個人情報保護・サイバーセキュリティ研修の実施状況

サイバーセキュリティに関する立入検査項目

明日をひらく都市
OPEN×PIONEER
YOKOHAMA

■令和５年度立入検査における主な確認項目（サイバーセキュリティ関連）

・情報機器の盗難予防策、画面の覗き見防止策

・システムの技術的安全対策
（適切なID管理、アクセスログの保存、不正アクセス対策　等）

・情報機器・保存媒体の廃棄方法

・サイバーセキュリティ対策チェックリスト（厚労省）への対応状況

サイバーセキュリティに関する立入検査項目

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

医療機関確認用

	チェック項目	確認結果（日付）	備考
医療情報システムの有無	医療情報システムを導入、運用している。 （「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ （　/　）	

○　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）			備考
		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 （　/　）	
	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	はい・いいえ		はい・いいえ	

サイバーセキュリティに関する立入検査項目

明日をひらく都市
OPEN×PIONEER
YOKOHAMA

【参考】

・医療分野のサイバーセキュリティ対策について
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html

・医療情報システムの安全管理に関するガイドライン
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

・医療機関等におけるサイバーセキュリティ対策チェックリスト
上記ガイドラインと同一ページの下部に掲載

・医療機関向け　セキュリティ教育支援ポータルサイト
https://mhlw-training.saj.or.jp/

国の「個人情報保護委員会」に情報漏えい等報告が必要な場合

明日をひらく都市
OPEN × PIONEER
YOKOHAMA

民間事業者等	事例
要配慮個人情報（病歴・診療内容など）が含まれる個人データの漏えい等（又はおそれ）	・個人データを記録したUSBメモリーの紛失 ・従業員の健康診断等の結果を含む個人情報
不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等（又はおそれ）	・ECサイトからクレジットカード番号を含む個人データが漏えいした場合　等
不正目的をもって行われたおそれがある個人データの漏えい等（又はそのおそれ）	・ランサムウェア等により個人データが暗号化され、復元できなくなった場合　等
個人データに係る本人の数が1,000人を超える漏えい等（又はそのおそれ）	・BCC欄に入力して送信すべきところをCC欄に入力して一括送信した場合　等

情報漏えい等の対応

■報告期限

まずは**速報**（新規）
発覚日から、概ね**３～５日**以内

次に**確報**（続報）
発覚日から、**30日**以内

不正な目的で行われたおそれがある場合は、発覚日から60日以内

個人情報保護委員会ＵＲＬ：https://www.ppc.go.jp/personalinfo/legal/leakAction/

ご清聴ありがとうございました

「医師の働き方改革」への対応もお願いします！

２０２７年国際園芸博覧会
『GREEN×EXPO 2027』 略称ロゴ