医政研発 0314 第 1 号
平成 28 年 3 月 14 日

各都道府県衛生主管部（局）長　殿

厚生労働省医政局研究開発振興課長
（公印省略）

伊勢志摩サミット等開催に伴う医療機関におけるサイバーセキュリティ対策等について

医療分野の情報化につきましては、平素より多大な御理解、御尽力を賜り、厚く御礼申し上げます。

今般、伊勢志摩サミットが 5 月 26 日及び 27 日に開催されること等に伴い、別添のとおり、警察庁警備局長から警備協力の要請がありました。

つきましては、伊勢志摩サミット及び関係閣僚会合開催中における医療機関のサイバーセキュリティ対策の強化等について、下記のとおり、管内関係機関に対し周知・徹底を図られますようお願いします。

記

1．「医療情報システムの安全管理に関するガイドライン 第 4.2 版」（平成 25 年 10 月 厚生労働省）※1に基づき、主に以下の点から、サイバー攻撃発生時に遅滞なく対応できるよう情報セキュリティ確保について改めて点検を行うとともに、必要に応じて技術的安全対策等を実施すること。

①利用者の識別及び認証

情報システムへのアクセスを正当な利用者のみに限定するために、情報システムは利用者の識別と認証を行う機能を持つ必要がある。

②情報の区分管理とアクセス制限の管理

情報システムの利用に際しては、情報の種別、重要性と利用形態に応じて情報の区分管理を行い、その情報区分ごと、組織における利用者や利用者グループ（業務単位等）ごとに利用権限を規定する必要がある。

③アクセスの記録

個人情報を含む資源については、全てのアクセスの記録（アクセスログ）を収集し、定期的にその内容をチェックして不正利用がないことを確認す

る必要がある。

④不正ソフトウェア対策

不正ソフトウェアのスキャン用ソフトウェアの導入及びパターンファイルの最新のものへの更新、オペレーティング・システム等でセキュリティ・ホールの報告されているものについての対応版（セキュリティ・パッチと呼ばれるもの）への更新が必要である。

⑤ネットワーク上からの不正アクセス対策

コンピュータウイルスや不正アクセスを目的とするソフトウェア等の攻撃から情報システムを保護等するための対策が必要である。

2．サイバー攻撃への対応として、別添の「サイバー攻撃対応力向上の手引き（第３版）」（平成27年１月20日セプターカウンシルサイバー攻撃対応力向上WG（第３版改訂情報共有WG））※2や独立行政法人情報処理推進機構(IPA)において公表されている対策「標的型攻撃メールの例と見分け方」※3についても参考にされたい。

3．医療機器における対策については、「医療機器におけるサイバーセキュリティの確保について」（平成27年４月28日 薬食機参発0428第１号 薬食安発0428第１号 厚生労働省大臣官房参事官（医療機器・再生医療等製品審査管理担当） 厚生労働省医薬食品局安全対策課長 通知）※4を参考にされたい。

※１：「医療情報システムの安全管理に関するガイドライン」

特に「6.2 医療機関における情報セキュリティマネジメントシステム(ISMS)の実践」「6.5 技術的安全対策」「6.9 情報及び情報端末の持ち出しについて」「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を参照されたい。

http://www.mhlw.go.jp/stf/shingi/0000026088.html

※２：「サイバー攻撃対応力向上の手引き」

セプターカウンシル（電気、金融、医療等の重要インフラ分野の代表で構成される協議会）において、各重要インフラ事業者等におけるサイバー攻撃に係る対応力の向上に資することを目的に作成されたもの。

※３：「標的型攻撃メールの例と見分け方」

http://www.ipa.go.jp/security/technicalwatch/20150109.html

※４：「医療機器におけるサイバーセキュリティの確保について」
http://www.mhlw.go.jp/file/05-Shingikai-11121000-Iyakushokuhinkyoku-Soumuka/0000090664.pdf