年末年始における情報セキュリティに関する注意喚起について

独立行政法人 情報処理推進機構（IPA）は「年末年始における情報セキュリティに関する注意喚起」として、
年末年始の長期休暇期間における情報セキュリティ対策を発表しています。
重要インフラ事業者各位においても、年末年始における対策を実施して頂きたく、IPAの注意喚起について
対策を抜粋して情報提供いたします。

年末年始における情報セキュリティに関する注意喚起 - IPA セキュリティセンター
https://www.ipa.go.jp/security/topics/alert20201217.html

長期休暇の時期は、「システム管理者が長期間不在になる」等、いつもとは違う状況になりやすく、ウイルス感染
や不正アクセス等の被害が発生した場合に対処が遅れてしまうなど、場合によっては関係者に対して被害が及ぶ
可能性があります。このような事態とならないよう、以下の対策を実施してください。

～ 長期休暇前の対策 ～
○ 緊急連絡体制の確認
不測の事態が発生した場合に備えて、委託先企業を含めた緊急連絡体制や対応手順等が明確になっているか
確認してください。
・連絡体制の確認（連絡フローが現在の組織体制に沿っているか、休暇中のシステム業者の対応の確認等）
・連絡先の確認（各担当者の電話番号が変わっていないか、等）

○ 院内ネットワークへの機器接続ルールの確認と遵守
ウイルス感染したパソコンや外部媒体等を院内ネットワークに接続することで、ウイルスをネットワーク内に
拡散してしまうおそれがあります。長期休暇中にメンテナンス作業などで院内ネットワークへ機器を接続
する予定がある場合は、院内の機器接続ルールを事前に確認し遵守してください。

～ 長期休暇明けの対策 ～
○ 不審なメールに注意
実在の企業などを騙った不審なメールに関する相談が多く寄せられています。こういったメールの添付ファイル
を開いたり、本文中のURLにアクセスしたりすることで、ウイルスに感染したり、フィッシングサイトに誘導され
たりしてしまう可能性があります。長期休暇明けはメールが溜まっていることが想定されますので、誤って不審な
メールの添付ファイルを開いたり、本文中のURLにアクセスしたりしないように注意してください。不審なメール
を受信していた場合は各医療機関のシステム管理者・システム業者に報告し、指示に従ってください。

～ サイバー攻撃を受けた疑いがある場合 ～
○ 保守会社等へ直ちに連絡
保守会社等へ直ちに連絡し、指示に従って必要な対策を講じてください。
○ 厚生労働省へ連絡
サイバー攻撃においては、攻撃者は不正アクセスを行った組織から別の組織へ、又は同種の攻撃を別の組織に行い、
感染を拡大させていきます。こうした被害の拡大を防ぐための情報共有はサイバーセキュリティ対策では重要です。
こうした情報共有の医療としての取組を厚生労働省・医療セプターにて構築しております。
サイバー攻撃を受けた疑いがある場合には、下記の厚生労働省の連絡先に御連絡く

ださい。
　　なお、いたずら防止のため、184発信、公衆電話発信は受信不可としますので、医療機関の電話で御連絡願います。
　　【連絡先】厚生労働省医政局研究開発振興課　サイバーセキュリティ受付
　０８０－２０７３－０７６８

（参考）医療機関等におけるサイバーセキュリティ対策の強化について
過去の通知ファイルを添付します。以下のURLでも公表しています。
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/index.html#h2_free7

（参考）テレワークを行う際のセキュリティ上の注意事項
https://www.ipa.go.jp/security/announce/telework.html

（参考）Web会議サービスを使用する際のセキュリティ上の注意事項
https://www.ipa.go.jp/security/announce/webmeeting.html

厚生労働省　医政局 研究開発振興課
医療情報技術推進室
標準化推進係　荒木　潤
TEL：03-5253-1111（内線4156）
03-3595-2430（直通）
FAX：03-3503-0595
Mail：araki-junaa@mhlw.go.jp

医政総発 1029 第１号
医政地発 1029 第３号
医政研発 1029 第１号
平成 30 年 10 月 29 日

各 都道府県 保健所設置市 特別区 医政主管部（局）長　殿

厚生労働省医政局総務課長
厚生労働省医政局地域医療計画課長
厚生労働省医政局研究開発振興課長
（　公　印　省　略　）

医療機関等におけるサイバーセキュリティ対策の強化について

日頃より医療分野の情報化に関し、格別のご配慮を賜り、厚く御礼申し上げます。

医療分野における情報化につきましては、近年、電子カルテシステムや地域医療情報連携ネットワーク等の普及が進み、情報通信技術は医療現場の多くで活用されています。

一方で、昨年５月に発生した世界的なランサムウェア「WannaCry」による被害をはじめ、我が国の医療機関においても相次いでコンピュータウイルスの感染事案が報告され、医療提供体制に支障が生じる事例も発生するなど、医療機関等におけるサイバーセキュリティ対策の充実は喫緊の課題となっております。

厚生労働省におきましては、内閣サイバーセキュリティセンター（NISC）及び医療関係団体等と連携して、医療機関等（医療法（昭和 23 年法律第 205 号）に規定する医療提供施設のほか、地域医療情報連携ネットワーク等を含む。以下同じ。）におけるサイバーセキュリティ対策に取り組んできたところですが、今後は都道府県、保健所設置市及び特別区とも連携を強化し、対策のさらなる充実を図ってまいりたいと考えておりますので、貴職におかれましては、下記についてご協力方よろしくお願いいたします。

なお、本通知は、地方自治法（昭和 22 年法律第 67 号）第 245 条の４第１項の規定に基づく技術的助言であることを申し添えます。

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」の周知徹底について

医療機関等においてサイバー攻撃を受けた際の非常時の対応については、「医療情報システムの安全管理に関するガイドライン　第 5 版」（平成 29 年５月 30 日政統発 0530 第１号。以下「ガイドライン」という。）に定められているところです。

医療機関等に対するサイバー攻撃の危険性がさらに高まっていることに鑑み、貴職におかれましては、管内の医療機関等に対して、ガイドラインの更なる周知徹底を図るとともに、医療機関等においてコンピュータウイルスの感染などによるサイバー攻撃を受けた疑いがある場合にあっては、別紙を活用して直ちに医療情報システムの保守会社等に連絡の上、当該サイバー攻撃により医療情報システムに障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、速やかに当該医療機関等から厚生労働省医政局研究開発振興課医療技術情報推進室（以下「医療技術情報推進室」という。）に連絡を行うよう、注意喚起をお願いいたします。

２　情報セキュリティインシデント発生時の国への報告について

管内の医療機関等において、コンピュータウイルスの感染などによるサイバー攻撃を受け医療情報システムに障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案を貴自治体が把握した場合（医療機関等からの報告により把握した場合のほか、報道発表又はマスコミ報道等により把握した場合を含む。）にあっては、事実把握後速やかに貴自治体から医療技術情報推進室に報告いただくようお願いいたします。特に自治体立病院につきましては、自治体立病院運営部署（団体）又は都道府県におかれては、自治体立病院を有する市区町村と連携し、国との情報共有に万全を期していただきますようお願いいたします。

３　情報セキュリティインシデントが発生した医療機関等に対する調査及び指導について

貴自治体においては、コンピュータウイルスの感染などによるサイバー攻撃を受けた医療機関等に対し、必要に応じて、被害状況、対応状況、復旧状況、再発防止策等に係る調査及び指導を行い、医療技術情報推進室に報告いただくようお願いいたします。なお、事案発生時には厚生労働省より情報収集・調査・指導等の依頼があり得ることを申し添えます。

また、病院、診療所又は助産所に対する情報セキュリティインシデントに係る調査及び指導につきましては、医療法第 25 条及び第 26 条並びに医療法施行規則（昭和 23 年厚生省令第 50 号）第 42 条に基づく立入検査等を行うことが可能です。当該立入検査等の実施にあたっては、サイバーセキュリティに係る技術的事項等につ

いて厚生労働省より助言を行うことが可能ですので、必要に応じてご相談をいただきますようお願いいたします。

４　医療分野におけるサイバーセキュリティの取り組み（医療セプター）との連携について

セプターにおいては、IT 障害の未然防止、発生時の被害拡大防止・迅速な復旧及び再発防止のため、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係者間で共有することにより、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資することを目指しています。

このうち、医療セプターについては、平成 30 年３月より事務局を公益社団法人日本医師会に設置するとともに、公益社団法人日本歯科医師会、公益社団法人日本薬剤師会、公益社団法人日本看護協会、一般社団法人日本病院会、公益社団法人全日本病院協会、一般社団法人日本医療法人協会、公益社団法人日本精神科病院協会等を構成員として、NISC や厚生労働省と連携し、サイバーセキュリティに関する情報共有や演習参加等の活動を行っています。

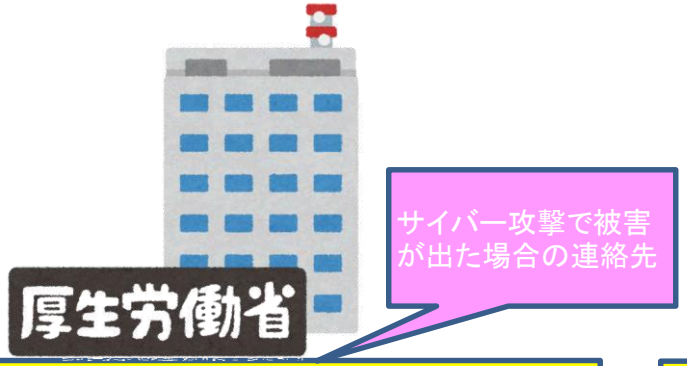
医療セプターの構成員団体は都道府県支部等を通じて会員施設との情報共有を行っている場合もあるため、各都道府県、保健所設置市及び特別区におかれましては、地域の医療関係団体を通じて医療セプターの活動に連携・ご協力をいただきますようお願いいたします。

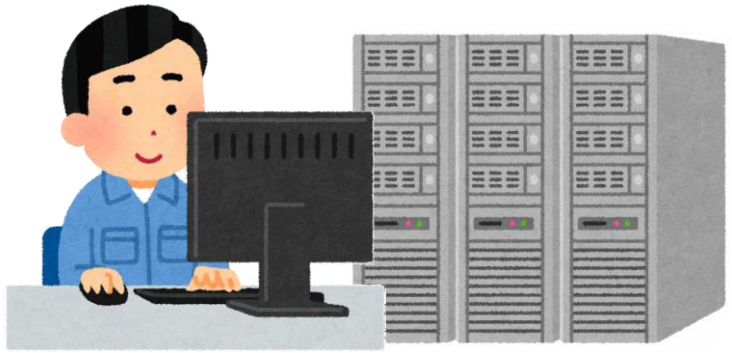
（参　考）

セプター（CEPTOAR（Capability for Engineering of Protection, Technical Operation, Analysis and Response の略称））：重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。平成 30（2018）年 10 月現在、各重要インフラ分野の業界団体等が事務局となって、全 14 分野で、計 19 のセプターが活動中。

サイバー攻撃を受けた場合の対応について（院内掲示用）

サイバー攻撃（コンピュータウイルスの感染等）を受けた疑いがある場合は、被害の拡大を防ぐため、直ちに医療情報システムの保守会社等に連絡し、指示を仰いでください。
また、診療系情報システムの停止や個人情報の流出等の被害等が発生した場合は、厚生労働省へご連絡ください。





医政局 研究開発振興課
医療技術情報推進室
電話：03-3595-2430
平日　午前９時～午後６時

医療情報システムの保守会社 等
緊急連絡先

社　　名：

電話番号：

担当者名：

セキュリティ対策を徹底し、大切な情報を守りましょう！

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