NRI グループ　新型コロナウイルス対策緊急提言　第 27 回

2020 年 5 月 28 日

新型コロナウイルス感染拡大に伴う医療のサイバーセキュリティ
～オンライン診療のリスクと求められるセキュリティ対策～

NRI セキュアテクノロジーズ株式会社
ストラテジーコンサルティング部
セキュリティコンサルタント　松本　直毅、木村　匠、内橋　七海

■ **要旨**

- 新型コロナウイルスの感染拡大をきっかけに我が国でも、従来は様々な制約があったオンライン診療について、初診での利用が時限的・特例的に可能になる等、医療のデジタル化に追い風が吹いている。
- 一方で、オンライン診療を含むデジタル化の急速な進展には、サイバー攻撃等のセキュリティリスクが付きまとうため、状況に応じて必要な対策を実施する必要がある。
- さらに、新型コロナウイルス収束後においても医療のデジタル化の恩恵を多くの人々が安心して享受できるよう、政府は利便性・医療安全・セキュリティのバランスが取れた政策立案を行うべきである。

■ **新型コロナウイルス対応で逼迫する医療機関に対するサイバー攻撃が活発化**

新型コロナウイルスをきっかけに、医療機関を取り巻く環境が急激かつ急速に変化している。

海外においては、コロナウイルスの対応で逼迫している医療機関に対して、追い打ちをかけるようなサイバー攻撃が活発化している。「ランサムウェア（「身代金」と「ソフトウェア」を組み合わせた造語）」と呼ばれる、医療機関のコンピュータを不正に暗号化し、解除するための身代金を要求する手口による被害が確認されている。被害を受けたチェコの病院においては、この攻撃により患者データを保有するコンピュータが利用できずにコロナウイルスの急患を受け入れられなくなる、等の医療業務への影響が実際に起きている※1。特に、今回のような緊急事態においては、医療機関が業務の復旧を優先し身代金の要求に応じる可能性が高い、という犯人側の目論見であると考えられる。

また、業務妨害だけではなく、医療機関が保有するコロナウイルスの感染者データを狙ったサイバー攻撃も考えられる。パンデミック封じ込めのためのワクチン開発の重要度が増すと共に、感染者データの価値が高まり、サイバー攻撃の標的対象となっている。米国では FBI と CISA（Cybersecurity and Infrastructure Security Agency）が連名で声明を出し、悪意のある組織による米国の医療研究機関の新型コロナウイルスに関する研究データを狙ったサイバー攻撃について警告を出している。感染者データは感染者自身のプライバシーに関わる個人情報であるという観点からも、不正なアクセスが行われないよう、適切なセキュリティ対策を実施することが求められる。

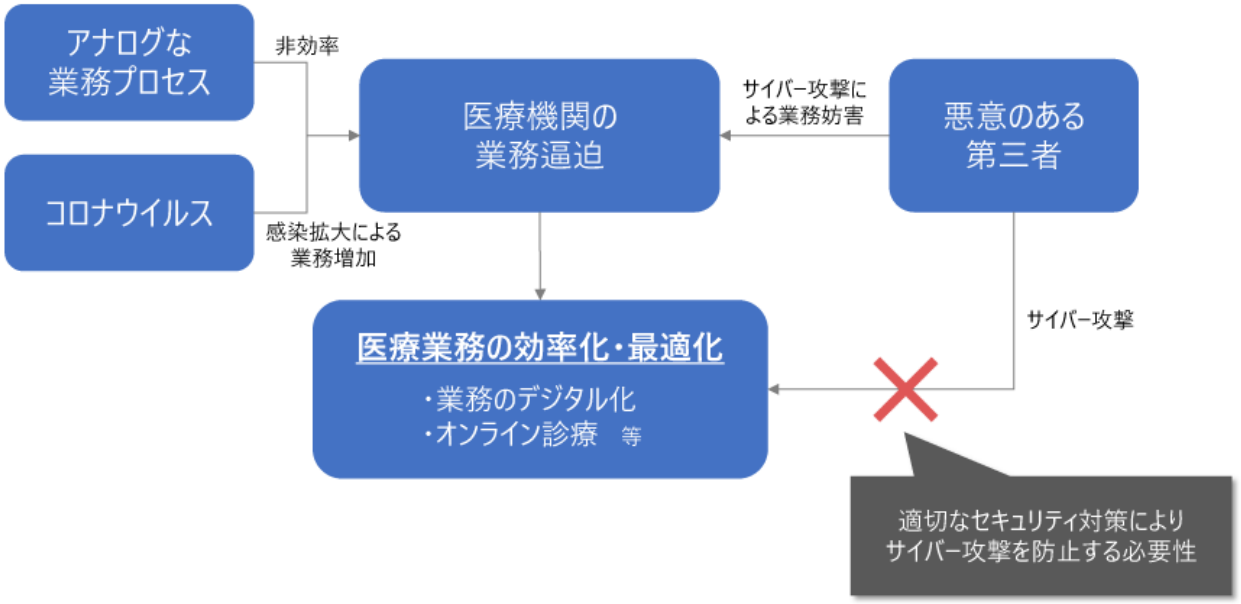
このようなサイバー攻撃の傾向を受けて、英国の NCSC（National Cyber Security Centre）と米国の CISA は連名で医療機関に対し声明を出し、医療機関に対するサイバー攻撃キャンペーンの存在と、攻撃に対して必要な対策のアド

バイスを公開している。

■ 日本の医療機関における IT 利活用の急速な拡大

日本でもコロナウイルスの急速な感染拡大に伴い、患者数や検査数が増加し、病院や検査所における業務負荷が増加している。特に、日本の感染者の集計業務の多くはいまだ手書きとファクスによる報告というアナログな手段で実施されており、非効率なプロセスが保健所の負荷につながっている等、従来から指摘されていた課題がコロナウイルスをきっかけに改めて明らかになった。

このような状況を改善するために、医療機関における IT 技術の利活用が短期間で急速に拡大している。例えば、保健所や連携する行政機関におけるコロナウイルス関連業務の効率化を目的としたサービスが事業者側で整備され、従来と比べると異例のスピードで業務のデジタル化が医療の現場に浸透し始めている※2、※3。



（出所）NRIセキュアテクノロジーズ

■ 注目を集めるオンライン診療

医療機関の逼迫した状況やコロナ禍での外出自粛の状況を踏まえ、医者⇔患者間の感染や院内感染のリスクがある対面診療に代わり、オンライン診療が注目を集めている。

海外では、例えば米国におけるメディケア（高齢者及び障害者向けの公的医療保険制度）では今年 3 月に保険適用範囲を拡大し、過疎地のみとしていた従来の条件が撤廃され全米でオンライン診療が可能となった※4。また英国でも 3 月に新型コロナウイルスの感染の疑いのある患者をオンライン診療でトリアージを行う方針が NHS（公的医療保障制度）から医療従事者に通知されている※5。このように、様々な国で新型コロナウイルス感染拡大をきっかけとしたオンライン診療の特例的取り扱いが見られる。

我が国においては、2018 年 3 月に厚生労働省によって「オンライン診療の適切な実施に関する指針（以下、「指針」とする）」※6 が取りまとめられ、同年 4 月から診療報酬が設定され保険診療適用となっていたものの、その時点では初

診の原則対面実施やオンライン診療をする際は概ね 30 分以内に対面診察可能な体制を有すること等の制約があった（その後 2019 年 7 月に一部改正）。しかし今回の新型コロナウイルス感染拡大の状況を受け、4 月 10 日、同省が「新型コロナウイルス感染症の拡大に際しての電話や情報通信機器を用いた診療等の時限的・特例的な取扱いについて」※7という事務連絡を公表し、4 月 13 日から平常時よりも比較的自由度が高いかたちでのオンライン診療が実施され始めている。なお、今回の時限的・特例的な取り扱いにより電話による診察や薬剤師によるオンライン服薬指導も可能となっているが、本提言では医師による情報通信機器を用いたオンライン診療のみ取り扱うこととする。

（出所）厚生労働省HP※8

今回の時限的・特例的な取り扱いによる主な変更点は以下の通りである。

	平時の取り扱い	今回のコロナ禍による 時限的・特例的な取り扱い
初診での実施	原則不可	初診から情報通信機器や電話を用いた診療により診断や処方が可能 ※一部処方に制限有り
対面診療実施歴	3か月以上の対面診療実施歴が必要 ※例外有り	不要
疾患の限定	有り（主に慢性疾患）	無し
医師の研修受講の有無	オンライン診療に関する研修受講義務有り	オンライン診療の研修受講を猶予

（出所）厚生労働省「オンライン診療の適切な実施に関する指針」、「新型コロナウイルス感染症の拡大に際しての電話や情報通信機器を用いた診療等の時限的・特例的な取扱いについて」、「新型コロナウイルス感染症の拡大に際しての電話や情報通信機器を用いた診療等の時限的・特例的な取扱いに関するＱ＆Ａについて」※9「令和２年度診療報酬改定の概要 （外来医療・かかりつけ機能）」※10 をもとにNRIセキュアテクノロジーズ作成。

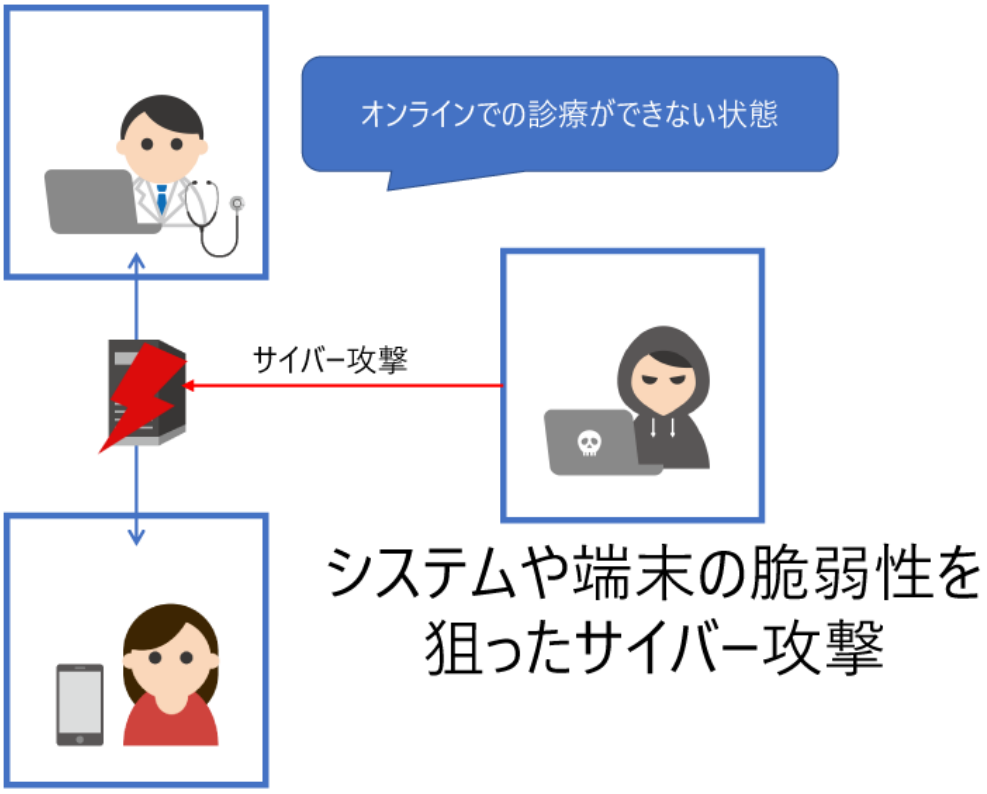
オンライン診療に関する規制の変化に伴い、医療機関のオンライン診療実施を支援するための新たなサービスが提供され始めている。オンライン診療アプリ CLINICS は、従来から提供しているオンライン診療サービスに加え、医療機関と薬局を繋ぐことで、患者が診察から薬剤の受け取りまでの一連の流れを全てオンラインで行うことができる機能を提供している※11。また、ヤフーがオンライン診療に対応している医療機関の検索機能を拡充、LINE とエムスリーが出資する LINE ヘルスケアが参入を表明する等、これからさらにオンライン診療に係る周辺のサービスが増加・拡充すると考えられる※12。ただし、オンライン診療サービスの導入には準備を含め一定の時間を要することから、現在の緊急事態下の医療機関の現場においては、オンライン診療の専用サービスばかりでなく既存のビデオ通話アプリ等の一般的なサービスも利用されていると考えられる。前述の指針においても、汎用サービスが「オンライン診療に限らず広く用いられるサービスであって、視覚及び聴覚を用いる情報通信機器のシステムを使用するもの」として定義され、考慮の対象に含まれている。

■ オンライン診療に潜むリスク

オンライン診療というと「医師はノートパソコン１つあれば、オンライン診療を始められる、患者もスマホがあれば済む」というイメージがあるが、取り扱われる医療情報は、場合によっては人命や健康にも関わるものであり機密性が非常に高い。また、先に述べたような活発化する医療機関へのサイバー攻撃において、オンライン診療も例外ではない。ではオンライン診療には具体的にどのようなリスクが潜んでいるのか。以下に例を述べる。

リスク（1）オンライン診療に使用するシステムや端末の脆弱性を起因としたサイバー攻撃による業務停止

オンライン診療に使用されるシステムや端末に脆弱性※13 があった場合、その脆弱性を突いたサイバー攻撃が起こり、マルウェアに感染することでオンラインでの診療が継続できなくなる可能性がある。

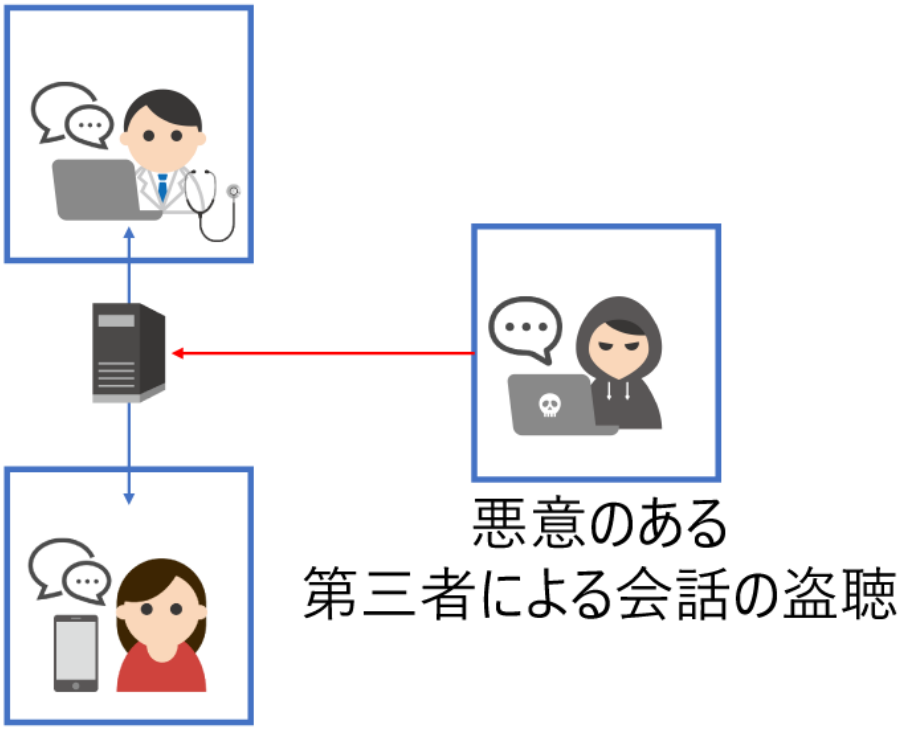


（出所）NRIセキュアテクノロジーズ

リスク（2）悪意のある第三者による医師や患者のなりすましや会話の盗聴

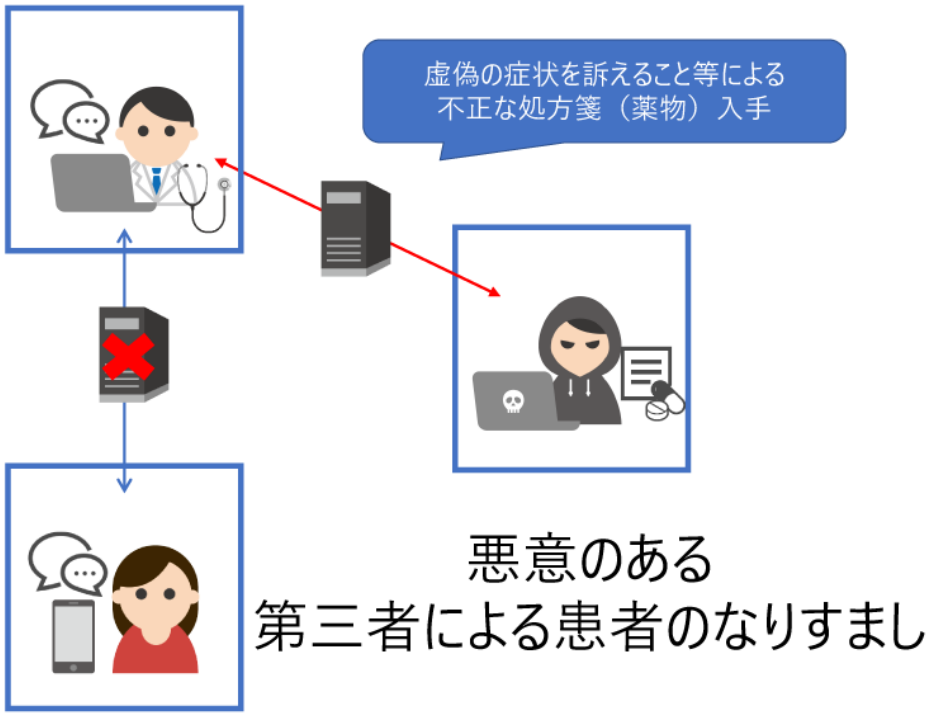
本来、病院で医師の診察を受ける場合は密室であり、基本的には医療従事者と患者のみの空間であるが、オンライン診療では別々の空間にいる医師と患者が通信で繋がれている。オンライン診療に使用されるシステムの通信が暗号化されていない場合、第三者が通信に侵入する可能性がある。

これにより、悪意のある第三者による会話の盗聴や、偽装されたサイトに繋がれることによる医師や患者のなりすまし等が起こり、医療情報の窃取や、違法な薬剤の入手といったリスクがある。



例えば汎用サービスで行われているオンライン診療中に、医師と患者が気づかないうちに悪意ある第三者によって会話が盗聴される、情報が窃取される等の可能性がある。

（出所）NRIセキュアテクノロジーズ



例えば、今回の時限的・特例的な取り扱いによって可能となった初診の利用で、医師が患者とオンラインで繋いでいるつもりが、実際には患者になりすました悪意のある第三者に繋がれていた場合、虚偽の症状を訴える等して違法に薬物を入手、転売等が行われる可能性がある。

（出所）NRIセキュアテクノロジーズ

■ **オンライン診療におけるセキュリティリスクを低減するための対策**

それでは、このようなオンライン診療を取り巻くセキュリティリスクをどのように低減していくことができるだろうか。厚生労働省では前述の指針において、個人情報やプライバシーを保護するために「医師」、「オンライン診療システム事業者」、「患者」がそれぞれ実施するべきセキュリティ対策を、組織的・人的観点（例：セキュリティポリシーの確認）及び技術的観点（例：適切な認証手段の実装）から幅広く整理している。また、今回の時限的・特例的取り扱い下においても、当該指針を参照してセキュリティ・プライバシーに配慮したオンライン診療を提供することが求められている。

もちろん、本来であれば、上記指針に記載されている全ての対策が、速やかに実施されるのが望ましい。しかし、医療を取り巻く状況に日々変化が見られるような現状においては、セキュリティリスクについては特に重要な事項にのみ焦点をあててスピーディーな対応を実施し、新型コロナウイルス感染拡大や慢性疾病の進行等の他のリスクを同時に低減することが肝要である。そこで以下では、上記指針に記載されている対策や追加で必要と考えられる対策を、「速やかに実施すべき対策（時限的・特例的取り扱い下においても実施すべきと考えられる対策）」と「中長期的に実施すべき対策」に分類して記載する。オンライン診療の利用/提供にあたっては、医療全体に関する様々なリスクも勘案しつつ、セキュリティリスクの低減については下記を参考にしていただきたい。

■ **速やかに実施すべき対策**

速やかに実施すべき対策としては、主に以下のようなものが考えられる。導入に比較的時間を要する技術的な対策よりもむしろ、今回の時限的・特例的取扱い下でも迅速・円滑に医療を提供するために、それぞれの責任範囲の明確化とコミュニケーションに焦点を当てた対策が重要となる。

対象者	速やかに実施すべき主な対策
医師	• セキュリティリスクの説明・合意 • 顔写真付きの身分証明書等の提示(医師のなりすまし防止) • 同意のない録画・撮影等を行わない(患者のプライバシー保護) • セキュリティインシデント発生時の対応検討
オンライン診療システム事業者	• 高い品質での保守対応 • セキュリティリスクの責任主体を医師に対して事前に説明・合意する • 医師や患者に対する脆弱性情報の共有
患者	• 医師から説明を受け、セキュリティリスクの存在を理解 • 顔写真付きの身分証明書の提示(患者のなりすまし防止) • チャット機能を用いる場合、外部URLへの誘導は行わない • 同意のない録画・撮影等を行わない(医師のプライバシー保護)

（出所）NRIセキュアテクノロジーズ

医師

医師が最優先で行うべき事項としては、どのようなオンライン診療システムを用いるのかを診療前に患者に対して説明し、当該システムの利用に際してのセキュリティリスクを提示した上で、利用に関する合意を得ることが挙げられる。平常時においては、オンライン診療の開始に先駆けた対面での診療計画提示の際、患者に対してセキュリティリスクを説明することとなっている。時限的・特例的取り扱い下で診療計画の策定を行わない場合でも、電話等、何らかのかたちで当該リスクについて説明することが重要である。

また、診療を行っているのが医師本人であることを示すために、顔写真付きの身分証明書等を提示することでなりすましを防止することや、録画・撮影等を同意なしに行わないこと、万が一のセキュリティインシデント発生時に、誰が・どこへ・どのように報告を行うかを明らかにしておくことも重要である。

なお、医師はオンライン診療が適切に実施されることを担保するために、後述の患者側で実施すべき対策についても確認し、これら対策が患者側にて適切に実施されるよう努めるべきであろう。

オンライン診療システム事業者

オンライン診療システム事業者としては、提供しているシステムが安定的に稼働するよう、通常時から実施している保守業務を滞りなく高い品質で実施することが大前提として重要となる。また、セキュリティリスクの責任主体（自社と医師のどちらがどのような責任を負うのか）を医師に対して事前に説明し、合意するべきである。加えて、自社が提供するシステムに対してセキュリティ面での弱点（脆弱性）が発見された場合に、速やかに、かつ分かりやすく、それらの情報を医師や患者に共有することが重要である。

患者

患者としては、まず医師からの説明を受け、オンライン診療システムの利用にセキュリティリスクが存在していることを理解することが重要である。リスクに関しての説明を事前に受け、疑問に思う箇所を解消することで、安心して受診することができるだろう。また、受診しているのが患者本人であることを医師が確認できるよう、顔写真付きの身分証明書を提示することも重要である。さらに、医師側の指示によりチャット機能を使う場合は、医師側の端末のセキュリティに悪影響を与える恐れがあるため、外部 URL への誘導は行わないよう注意が必要である。例えば、患者側が誤ってフィッシングサイト等の偽サイトへ接続される URL をチャットで送付してしまうと、医師がこのような悪意ある Web サイトにアクセスし、個人情報の漏えいが発生する可能性がある。加えて、医師側のプライバシーを考慮し、録画・撮影等を同意なしに行わないよう注意が必要だ。

■ 中長期的に実施すべき対策

この度の時限的・特例的取り扱いを機にオンライン診療のメリットが広く社会に共有されれば、新型コロナウイルス収束後もオンライン診療の利用は拡大していくだろう。そのような将来を見据えた場合、技術的な対策を含めた、より中長期的な視点からの対策が必要となる。中長期的に実施すべき対策としては、主に以下のようなものが考えられる。

対象者	中長期的に実施すべき主な対策
医師	• 本人認証の強化(例：多要素認証の導入) • 厚生労働省が定めるオンライン診療に関する研修への参加
オンライン診療システム事業者	• 定期的なセキュリティ評価の実施 • IDS/IPS等の導入による、不正アクセスの防止 • システムへのアクセスログ・操作ログ等の取得 • ログ監査・ログ監視の実施
患者	• 「速やかに実施すべき対策」を引き続き確実に実施 • オンライン診療に使用するアプリケーションや使用端末(PC、スマートフォン等)のOSを適宜バージョンアップする

（出所）NRIセキュアテクノロジーズ

医師

医師としては、第三者によるなりすましをより強固に防ぐために、本人認証の強化を行うのが望ましい。例えば、オンライン診療システムを利用する際に多要素認証（パスワード認証、物理認証、生体認証のうち異なる 2 種類以上の方法を用いる認証）を導入することが考えられる。また、オンライン診療に関する研修を受講すべきである。本来、オンライン診療を実施する医師については、厚生労働省が定める研修の受講が必要だが、この度の時限的・特例的な取扱いが継続している間に限り、当該研修の受講が猶予されている（時限的・特例的な取扱い解除後は研修の受講が必須となる）。過去に実施された研修では、オンライン診療で使用されるクラウドサービスに関するセキュリティ対策や、実際の臨床現場におけるオンライン診療実施事例等、多数の専門家から具体例を交えた話題が提供されている[※14]。

医療機関が医療情報に関するセキュリティ対策を実施する際のガイドラインとして、「医療情報システムの安全管理に関するガイドライン」（厚生労働省）が公開されており、オンライン診療におけるセキュリティ対策を検討する際にもこのガイドラインが参考になるだろう。

オンライン診療システム事業者

オンライン診療システム事業者としては、患者の個人情報を保護するために、より強固な対策を実施していくのが望ましい。例えば、定期的なセキュリティ評価によって、オンライン診療システムの提供に関係しないサーバーや端末等において患者の個人情報が蓄積・残存していないかを確認するべきである。更に、IDS/IPS[※15] 等の導入により不正アクセスを防止する措置を講じることや、システムへのアクセスログ・操作ログ等を取得した上でログ監査・ログ監視を行うことも重要となる。

情報処理事業者やクラウドサービス事業者が医療情報を取り扱う場合のセキュリティ対策に関するガイドラインとしては、「医療情報を受託管理する情報処理事業者における安全管理ガイドライン」（経済産業省）、「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」（総務省）がそれぞれ公開されている。上記指針とあわせて、これらのガイドラインを参照するのが望ましいだろう。なお、上記 2 つのガイドラインは「医療情

報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（経済産業省・総務省）として統合・改定されることとなっており、現在改定案が両省から公表されている。

患者

患者としては、「速やかに実施すべき対策」で示した事項を引き続き確実に実施することが重要となる。加えて、中長期的な観点から見ると、医師やオンライン診療事業者から共有される情報をチェックし、オンライン診療の際に使用するアプリケーションや、使用端末（PC、スマートフォン等）の OS を適宜バージョンアップしておくことも重要だ。

■ 提言：「コロナ後」の医療のサイバーセキュリティ

メッセージングアプリの LINE は、東日本大震災発生時に既存の手段（電話、メール）で繋がりにくかったという課題をきっかけに 2011 年 6 月にリリースされ、今では日常生活に欠かせないコミュニケーション手段として広く浸透している。このように、非常時の課題に応える形で一度普及したサービスは人々の生活に浸透し、それ以前の状態に戻ることはない。現在進んでいる医療における IT 利活用についても同様の経緯を辿り、例えばオンライン診療は収束後も一定の形で利用継続・拡大が進むと考えられる。したがって、新しいサービスの利便性を社会全体として享受し続けるために、医療に関わる全ての関係者はセキュリティについて当事者意識を持った対応が今後も継続的に求められる。

行政としては、新型コロナウイルス感染拡大をきっかけとして、医療における IT 利活用やデジタル化を通じた医療業務全体の効率化・最適化を更に推進するべきである。その際、制度設計においてセキュリティを「後付け」で考えるのではなく、構想の段階からセキュリティ上のリスク・対応を事前に検討する、セキュリティ・バイ・デザインの考え方を採用することが重要である。もちろん、リスクや必要となる対応の内容は、日々変容することが想定されるので、制度設計の段階ではすべてを網羅的に考慮することが難しい。したがって、医療従事者（医師、看護師、検査技師、薬剤師等）、関連する事業者（電子カルテベンダー、医療機器メーカー、オンライン診療システム事業者等）、患者等、医療に携わる幅広い関係者から定期的に知見を収集し、医療のデジタル化全体におけるリスクを多面的・継続的に検討する必要がある。

特に、オンライン診療に関する時限的・特例的取扱い下の対応については、厚生労働省が各医療機関における対応状況を検証することとなっている。厚生労働省をはじめ、政府はこの検証結果を精緻に分析し、利便性・医療安全・セキュリティのバランスが取れたオンライン診療のあり方を検討すべきである。

※1　新型コロナ対応のなかで病院・研究機関にサイバー攻撃　欧州で続出
https://www.sankeibiz.jp/macro/news/200513/mcb2005130645001-n1.htm

※2　セールスフォース・ドットコム、 新型コロナ保健所業務支援クラウドパッケージを 全国の保健所向けに無償提供
https://www.salesforce.com/jp/company/news-press/press-releases/2020/04/200413/

※3　神奈川県での新型コロナ対策に kintone を活用
https://topics.cybozu.co.jp/news/2020/03/11-8780.html

※4　日本経済新聞 2020 年 5 月 17 日「ネット診療、世界で拡大　米英中は保険適用」
https://www.nikkei.com/article/DGXMZO59218260X10C20A5SHA000/

※5　Yahoo!ニュース 2020 年 4 月 26 日「新型コロナで問われるオンライン診療の価値　海外事例から見る医療環境の変化」
https://news.yahoo.co.jp/articles/92490534cf21113947efa5adade365056c21b0d7?page=3

※6　オンライン診療の適切な実施に関する指針
https://www.mhlw.go.jp/content/000534254.pdf

※7　新型コロナウイルス感染症の拡大に際しての電話や情報通信機器を用いた診療等の時限的・特例的な取り扱いについて
https://www.mhlw.go.jp/content/R20410tuuchi.pdf

※8　オンライン診療に関するホームページ
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/rinsyo/index_00010.html

※9　新型コロナウイルス感染症の拡大に際しての電話や情報通信機器を用いた診療等の時限的・特例的な取扱いに関するＱ＆Ａについて
https://www.mhlw.go.jp/content/000627376.pdf

※10　令和 2 年度診療報酬改定の概要　（外来医療・かかりつけ機能）
https://www.mhlw.go.jp/content/12400000/000605491.pdf

※11　メドレー、調剤薬局向けオンライン服薬指導支援システムの提供を 2020 年 9 月から開始　～9 月までは「CLINICS オンライン診療」を暫定的に提供～
https://www.medley.jp/release/20209-9clinics.html

※12　Yahoo! JAPAN、厚生労働省の公開情報をもとに、オンライン診療に対応している医療機関の検索機能を拡充
https://about.yahoo.co.jp/pr/release/2020/05/13a/

※13　脆弱性とは「コンピュータの OS やソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のこと」
総務省　安心してインターネットを使うために　国民のための情報セキュリティサイト
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/risk/11.html

※14　平成 30 年度　厚生労働省事業　遠隔医療従事者研修
https://enkakuiryo.jp/#about

※15　IDS＝Intrusion Detection System（不正侵入検知システム）、IPS=Intrusion Prevention System（不正侵入防止システム）

以上

【NRI グループ　新型コロナウイルス対策緊急提言】
https://www.nri.com/jp/keyword/proposal

【提言内容に関するお問い合わせ】
株式会社野村総合研究所　未来創発センター
E-mail：miraisouhatsu@nri.co.jp

【報道関係者からのお問い合わせ】

株式会社野村総合研究所　コーポレートコミュニケーション部
E-mail：kouhou@nri.co.jp