リモート接続型の運用管理環境の調査へのご協力のお願い

**【調査の背景】**

２０２２年１０月末に大阪急性期・総合医療センター（以下、大阪総合医療C）の医療情報システムがランサムウェア被害を受け、通常診療や手術、救急対応等、患者診療の継続性に著しい影響を及ぼしており、現在も復旧に向けた対応が進められている状況です。

各種メディアの報道からは、今回の感染事案は、昨年度の半田町立病院におけるランサムウェア被害のように院内にリモートメンテナンス目的で設置されていたVPN機器の脆弱性に起因するものではなく、外部企業に委託していた業務とは直接的に関係のない企業内部ネットワークにおけるVPN機器の脆弱性が悪用され、当該ネットワークに侵入が行われたことが推測されます。

企業内部の業務ネットワークと外部委託業務向けのネットワークが分離されていなかったため、後者のネットワークにまで攻撃者が侵入し、そこから拠点間接続していた大阪医療Cの環境への攻撃が行われており、いわゆる、「サプライチェーン攻撃」と呼ばれるものに該当するものです。

大阪総合医療Cでランサムウェアによる感染被害を受けた医療情報システムにはリモートメンテナンス用のVPN機器が設置されていましたが、当該機器は既に脆弱性の対応が完了していたと報道されています。しかしながら、外部委託先の企業内部のネットワーク環境における脆弱性を起点として、委託元である大阪総合医療Cへの二次被害が発生してしまったケースと考えられます。

*＜イメージ図：半田病院等の事例～院内設置した機器の脆弱性が悪用されるケース）＞*



*＜イメージ図：大阪総合医療Cの事例～外部委託先企業のネットワーク機器の脆弱性が起点となり、外部委託元への感染を発生させたケース＞*



上記の背景に基づき、当院に貴社が提供頂いているシステム・サービスに対するリモートメンテナンス環境、あるいは拠点間接続や外部サービス等、貴社内部のネットワーク環境と当院の院内ネットワークが接続している環境（以下、「リモート接続型の運用管理環境」と記載）を対象としたセキュリティ管理状況を確認させて頂きたいと考えています。

お忙しいなかお手数をおかけしますが、ご協力お願いいたします。

**＜調査項目＞**

**No１：**

**リモート接続型の運用管理環境は、貴社内部の業務ネットワークから独立していますか？**

（回答）

□はい　□いいえ

*→回答が「はい」の場合はNo.２、「いいえ」の場合はNo.３に進んでください。*

**No２：**

**社内の業務ネットワークから独立したリモート接続型の運用環境は、（１）：当院のみを接続先としたものか、（２）：当院以外（他の病院群）とも接続しているものか、いずれに該当しますか？**

（回答）

* （１）に該当する　□　（２）に該当する

*→回答が「（１）に該当する」の場合はNo.5に進んでください。「（２）に該当する」の場合はNo.4に進んでください。*

**No.3：**

**貴社内部の業務ネットワークにおけるインターネット等、外部ネットワークとの接続点に設置されているネットワーク機器（VPN機器だけでなく、ルータ、スイッチ、ファイアーウォール等も含む）への新たなファームウェアやセキュリティパッチの適用（脆弱性対応）が実施されていますか？**

* 全ての機器のファームウェア/セキュリティパッチ適用について、メーカが公表した時点から５営業日以内に都度実施している
* 一部の機器（重要度の高い機器）については、ファームウェア/セキュリティパッチ適用を、メーカが公表した時点から５営業日以内に都度実施している
* ファームウェア/セキュリティパッチの適用は、メーカ公表に応じた都度の頻度ではなく、一定の頻度（※）で情報収集し、実施している

*(※：頻度を記入ください：　　　　　　　　　　　　　　)*

* 特に実施していない

*→回答内容にかかわらず、No5に進んでください。*

**No.4：**

**貴社におけるリモート接続型の運用管理環境と接続する、他の病院で仮にマルウェア感染等が発生した場合、貴社の運用管理環境を介して、当院へ感染が拡大しないように、必要なセキュリティ対策（※）は実施していますか？**

（回答）

* 実施している

*（※：具体的なセキュリティ対策を記入ください：　　　　　　　　　　　　　　　　　　　　　　　　）*

* 実施していない

*→回答内容にかかわらず、No5に進んでください。*

**No.5 ：**

**貴社と当院設置の医療情報システム間のリモート接続についてどのような方式（製品）を採用していますか？**

（回答）

* WindowsOS 標準搭載のリモートデスクトップ接続方式（Remote Desktop）
* 上記以外（Remote Desktop）以外の接続方式（※）

*（※：具体的なリモート接続ツールを記入ください：　　　　　　　　　　　　　　　　　　　　　　　　）*

*→回答内容にかかわらず、No6へ進んでください。*

**No.6 ：**

**当院の医療情報システムへリモート接続する場合、リモート接続に用いるVPN等のネットワーク機器のパスワード、及び医療情報システムにリモートログインする際のパスワードを定期的に変更していますか？**

* リモート接続用の機器のパスワード、及びシステムへのリモートログインパスワードともに定期的に変更（※）している

*(※：変更の頻度を記入ください：　　　　　　　　　　　　　　)*

* リモート接続用の機器のパスワードは変更していないが、システムへのリモートログインパスワードは定期的に変更（※）している

*(※：変更の頻度を記入ください：　　　　　　　　　　　　　　)*

* リモート接続用の機器のパスワードは定期的に変更（※）してるが、システムへのリモートログインパスワードは変更していない

*(※：変更の頻度を記入ください：　　　　　　　　　　　　　　)*

* リモート接続用の機器/システムへのリモートログインパスワードともに変更していない

以上