事　務　連　絡
令和 2 年 8 月 4 日

大臣官房厚生科学課長 殿
医政局経済課長 殿
医政局研究開発振興課医療情報技術推進室長 殿
健康局結核感染症課長 殿
健康局健康課予防接種室長 殿

大 臣 官 房 参 事 官
(ｻｲﾊﾞｰｾｷｭﾘﾃｨ・情報ｼｽﾃﾑ管理担当)

新型コロナウイルスワクチン開発を標的とした医療、製薬分野への
サイバー攻撃に対する対応について(注意喚起)

2020 年 7 月、新型コロナウイルスワクチン開発を行う世界の研究機関等に対して、その開発情報の窃取を目的としたサイバー攻撃が盛んになっていることが、英国、米国等の政府から公表されました。この公表には対応策として、2020 年 5 月 5 日に発出された、米国、英国の 2 国による合同注意喚起が引用されています。これらを踏まえ、内閣サイバーセキュリティセンター(以下「NISC」という。)より、別添のとおり注意喚起が発出されました。

サイバー攻撃は国境を超えた手口であり、我が国においても、世界各国と同様、医療、製薬分野等に対するサイバー攻撃が同様に発生しているリスクが高まっていると思われます。

NISC からの注意喚起文書(別添)と併せ、サイバー攻撃へのより具体的な対策として、下記の対策を実施いただくよう、所管の機関、組織等に必要な注意喚起をお願いします。

記

○ アカウントの保護
- パスワードは他人に推測されにくいもの(大文字、小文字、数字、特殊文字を含む、できる限り文字列の長いものとする等)を使用する。
- 複数の情報システムで、パスワードの使い回しを行わない。
- パスワードの漏えい、解読された場合に備え、多要素認証を使用してアカウントを保護する。

○ 端末や環境の保護
- 端末上のオペレーティングシステム、ブラウザ、ウイルス対策ソフトウェア、その

他のソフトウェアを最新の状態に保ち、定期的に全てのファイルをウイルススキャンする。

- 信頼できる送信元であってもメール上の添付ファイルやリンクを開く場合は、不審な点がないか確認をする。
- VPN(仮想専用回線)を使用する場合はベンダが提供する最新パッチを VPN ゲートウェイ及びクライアントに適用する。
- ネットワークやサーバ等へのインフラへ最新パッチを適用する。
- 端末上で使用するアカウントは必要最低限な権限に制限したものを使用する。
- 重要なファイルは定期的なバックアップを取得する。

○ 侵入の検知と対応

- 定期的に端末上の全てのファイルをウイルススキャンし、スパイウェア等が存在しないか確認する。
- インシデント管理プロセス(インシデント対処手順)を確認し、必要に応じ更新する。
- セキュリティ監視機能やネットワーク監視機能を設定して、侵入を検知する。
- より優れたセキュリティを活用するため、最新の情報システム、ソフトウェアを使用する。
- 社員・職員等へサイバーセキュリティ意識の向上を目的とした訓練・研修等を実施する。

以上

【照会先】
サイバーセキュリティ担当参事官室
サイバーセキュリティ対策第一係・第二係
野口(内 7409)・高橋(内 7421)・杉(内 2258)
TEL:03-3595-2427