国立成育医療研究センター関連 Web サイトのサーバーへの

不正アクセスについて

2021 年 10 月 6 日

国立成育医療研究センター　理事長

五十嵐　隆

本年 1 月に国立成育医療研究センター(以下「当センター」という。）に関連した Web サイトのサーバー（以下「Web サーバー」という。）に不正アクセスが行われた件につき、1 月 13 日付けで当センターのホームページ内「お知らせ」に「「小児医療情報収集システム」web サイトへの不正アクセス発生および運用停止について」として掲示いたしましたが、より詳細な事象及び調査経過・今後の対応策等について、以下のとおり取りまとめ公表いたします。

1. 事象及び経緯の概略

2021 年 1 月 4 日、当センターが管理するドメイン内に不正に置かれたと思われるファイルが見つかった旨の連絡が、政府機関より当センター情報管理部にありました。具体的には、検索サイトで「激安」のキーワードで検索した際、pharma-net.ncchd.go.jp 内に多数ヒットするとのことでした。

状況としては、Web サーバー内に無関係なファイルが作成され、また既存のものの一部（ヘッダー部等、Web サイトの外見や動作に影響のない部分）が書き換えられていました。通常の閲覧方法ではたどり着かず、検索結果から辿っても表示されない（エラー画面になる）状態でした。

なお、pharma-net.ncchd.go.jp は「小児と薬事業」を紹介するためのもので、その Web サーバー内には一切患者情報は保存しておりません。

発見日には pharma-net.ncchd.go.jp の名称（ドメイン名）を削除することで応急対応し、翌日より Web サーバーを停止しています。

2. 原因及び問題点

1）今回の事象は、CMS（Web サイトのコンテンツ管理システム）として用いていた WordPress の管理用 ID・パスワードを取得・不正利用されて発生していました。これが取得された原因は、類推しやすいものが用いられていたことであったと推定されました。

また、一連の対応・調査の過程で以下の点も問題と考えられました。

2）発見翌日まで委託先業者に連絡がつかず、当日は緊急対応が指示できなかった。

3）アクセスログの保存期間の設定が比較的短く、アクセスログからの調査に限界があった。

3．再発防止策

上記問題点の改善策・再発防止策として以下を行います。

1）ID・パスワードの運用の適正化

１－１．システムのデフォルト管理者 ID は無効とする。
１－２．パスワードをより適切な、推測等が困難なものとする。（1 月 5 日実施済み）

２）委託先業者の管理・対応の改善
２－１．各業者の責任範囲を明確化する。
２－２．各業者の緊急連絡先をまとめ、セキュリティインシデント時の対応等につき申し入れ、了解を得ている。（1 月 5 日より順次実施、 4 月末までに取りまとめ完了）

３）センター側の管理体制の見直し
３－１．緊急対応が必要となった場合に備え、認証情報の共有方法を見直す。（1 月 5 日実施済み）

４）ログ及びバックアップについての運用の改善
４－１．管理権限を持つ ID のログイン・ログアウト及び操作履歴を、充分な期間記録・保存することとする。（1 月 5 日設定済み）
４－２．Web サーバー内のコンテンツファイルの全てのバックアップを、コンテンツの更新時に加え、定期的にも取得することとする。（1 月 5 日取得済み）

その他 Web サーバー管理上において下記の点に留意することとします。

- 利用している OS・ソフトウェアは適宜アップデートし、セキュリティの確保に努めること。
- 不必要なポートは全てふさぐこと。
- Web サーバーの管理画面・CMS のログイン画面はアクセス可能な IP アドレスを制限するなどの制御をすること。（1 月 13 日実施済み）

４．今後の対応

今回のように事業や研究等で独自に Web サイトを構築しているものについては、これまで当センターとして把握・管理できていないのが実情でした。

これらを一括して管理する体制の構築に向け、まずはこれら独自 Web サイトについての状況を常時把握し、助言・指導・介入等を行える体制の構築を目指すこととしました。

取り急ぎ、利用するプログラムの更新方針や認証情報の管理状況・セキュリティに関するログの設定・個人情報の取り扱い等についてセンター内各部署に調査を行い、現在内容の確認を行っています。

またこれと並行して、Web サイトの構築・管理を委託する際に必要とすべき要件に「３．再発防止策」の各事項の継続的な遵守を追加し、原則として委託時にはこれを仕様等に含めることとします。また既存のサイトについても、原則として同要件を満たす形に移行するものとします。

現在停止している「小児医療情報収集システム」web サイトについては、センター公式ホームページ内に一旦移行し 10 月より再開することといたします。