2020 年 6 月 5 日

Syndrome Finder
ユーザー各位

国立成育医療研究センター
ゲノム医療研究部

# システム不具合によるユーザー登録情報閲覧可能となる可能性に関するお詫びとご報告

2020 年 5 月 15 日に発覚した「システム不具合によるユーザー登録情報が一部閲覧可能となる状態」に関して、Syndrome Finder のユーザーの皆様に深くお詫びするとともに、その原因や対策について下記のようにご報告します。

本件は 2020 年 5 月 15 日と 19 日の 2 回にわたり、それぞれ別の新規登録申請者の通報により発覚したものです。調査の結果、当センターへの移管以前からの潜在的なシステム不具合が原因で、特定条件下で既存ユーザーの登録情報が一部閲覧可能となることが判明しました。

本件は不正アクセス等によるものではなく、またその原因から登録情報の一斉流出の可能性はほぼないと考えていますが、前述のように少なくとも 2 件、新規登録申請者が意図せずして既存ユーザーの情報を一部閲覧できたことが確認されています。一方で、本件では管理者情報の漏洩はなく、管理者権限が必要な当該既存ユーザーの登録情報の書き換えや検索履歴の閲覧等は確認されていません。

本件の対策として、原因となったシステム不具合の解消を行うとともに、新規登録申請における機能の改善と、新たにユーザー情報変更の機能の追加を行いました。

本日 2020 年 6 月 5 日より Syndrome Finder を再開しますが、

1. ユーザーの皆様は、ログイン後に画面右上の「ユーザー情報変更」よりパスワードの再設定をお願いします。
2. また、当センターへの移管以前からのユーザーの皆様は、メールアドレスの設定をお願いします。（現在ダミーのアドレスが設定されています。）
3. 必要に応じて、各自の登録情報の更新をお願いします。

このたびは、Syndrome Finder 停止に伴い、ユーザーの皆様にはご不便・ご心配をおかけいたしました。安定して活用できるよう、システムの改良・改善を今後も続けて参りたいと思います。

記

【経緯】

| | |
|---|---|
| 2020 年 5 月 15 日（金）14:35 | 新規登録申請者より、登録受付完了画面において本人と別の既存登録ユーザーの情報が表示されたとの報告を受ける。 |
| 2020 年 5 月 19 日（火）18:45 | 別の新規登録申請者より、同様の報告を受ける。 |
| 2020 年 5 月 19 日（火）20:12 | サービス関連の全サーバーを緊急停止する。 |
| 2020 年 5 月 20 日（水）10:42 | 全サーバーを再起動した後、外部への公開を一時停止する。 |
| 2020 年 6 月　5 日（金）12:00 | 不具合の解消後、サービスを再開する。 |

【原因】

当時のユーザー登録機能では、登録申請を行った後の遷移先のページに、申請内容の情報を表示していた。この登録申請完了画面では、ユーザーID をもとに情報をデータベースから取得しており、セキュリティ上の問題があった。

【対策】

本脆弱性の対策を以下の方針にて行った。

A) ユーザー登録申請完了のページは、ユーザー登録申請が正常に完了した場合にのみ閲覧可能なようにした。

B) ユーザー登録申請完了のページは、パラメータを許容せず、外部から与えられることのない内部に保持した情報により作成されるようにした。

C) ユーザー登録申請完了のページには、たとえ自身が入力したパスワードであっても表示しないようにした。

さらに、ユーザーの登録情報を本人が即座に変更できるようにするため、新たにユーザー情報変更機能を追加した。

【お問い合わせ】

国立成育医療研究センターゲノム医療研究部 UR-DBMS 担当：urdbms@ncchd.go.jp

以上