弊社運営の看護師および看護学生向けコミュニティサイト「看護 roo!」への“なりすまし”による不正アクセスについて【第 2 報】

2022 年 5 月 19 日に第 1 報を行いました弊社が運営する看護師および看護学生向けコミュニティサイト「看護 roo!」（以下当該サイト）における“なりすまし”による不正アクセスが確認されました件について、新たな事実が判明いたしました。改めて現時点で把握できている状況について第 1 報に赤字で追記する形で下記の通りご報告を申し上げます。

お客様に対しご心配おかけいたしますことを、深くお詫び申し上げます。

記

1．事故発生に関する状況

［事実経緯］

・5 月 16 日（月）

AM9:36

ご登録いただいているお客様から当該サイトポイント（以下ポイント）使用に関する複数の問い合わせがあったため、不正ログインを疑い社内調査を開始。

AM9:49

調査の結果、登録ユーザー以外の第三者による不正ログイン試行と、ログインが成立した一部のケースにおいて第三者によるポイントの詐取が発生したことを確認。当該 IP からのアクセスを遮断。

PM12:00

上記の調査結果をふまえ、被害拡大の防止と被害範囲の特定、原因調査のために当該サイトの公開を一時的に停止。

・5 月 17 日（火）

セキュリティ専門の第三者機関を交えて詳細な事実関係の調査確認と安全対策に関する協議を開始。

・5 月 19 日（木）（新たに判明した事実）

当該サイトにおいて、ポイント詐取が発生する以前にも不正ログインを試みる攻撃（パスワードリスト攻撃※）が行われ、複数のアカウントについてログインがなされていることを確認。

※外部より不正に入手した他者の ID とパスワードの組み合わせのリストを用いてサイトにログインを試みることで、個人情報の閲覧等を行うサイバー攻撃

・5 月 20 日（金）
ご登録いただいているすべてのお客様のパスワードをリセットし、既に不正利用されたメールアドレス・パスワードの組み合わせでのログインを今後遮断する対応を実施。

・5 月 23 日（月）
パスワードポリシー変更等アカウントの安全性を強化した上で、当該サイトを再度公開。

現在も調査を継続しており、今後新たな情報が判明しましたら、改めてご報告いたします。

2．現時点で分かっている被害状況

①パスワードリスト攻撃による被害　（新たに判明した事実）

［パスワードリスト攻撃が行われた期間］

2022 年 4 月 10 日（日）AM 00：12～2022 年 5 月 16 日（月） PM 12：00

［パスワードリスト攻撃］

のべ 138,338,195 件のログインの試行が行われ、うち 60,518 件（0.04%）がログインされた

※弊社が導入する WAF ではリスト攻撃を検知するための機能を有効化、メーカーの提案値よりも検知率が高くなるよう閾値を設定して運用していましたが、閾値を下回る速度（頻度）でパスワードリスト攻撃が行われたため、検知・遮断ができていませんでした。

②第三者による不正なポイント交換による被害

［不正アクセスによるポイント交換が行われた期間］

2022 年 5 月 13 日（金）PM 6:00 ～ 2022 年 5 月 16 日（月）AM 10:30

［ポイントの不正使用による被害件数およびポイント数］

ポイントが不正使用されたアカウント　：　1,877 件

不正使用されたポイント数　：　651,904 ポイント

3．第三者に閲覧された恐れのある情報

［調査の結果、現時点で第三者によるアクセスが確認できたページで表示される情報］

・氏名

・住所

現時点での調査では、上記情報以外への第三者のアクセスは確認されておりませんが、引き続き調査を継続しております。

なお、銀行口座、クレジットカード情報等、決済関連の情報はもとより保有しておりません。

４．第１報時点で実施済みの対応

・不正アクセスが行われたと思われる特定の送信元 IP アドレスからのアクセスを遮断。

・被害拡大の防止と被害範囲の特定、原因調査のために当該サイトの公開を一時的に停止。

・第三者による不正なポイント交換による被害が確認できた 1,877 件のアカウントで登録されているお客様に対して本件状況を個別にご連絡。

５．新たに実施した対応【追記】

弊社は、「２．現時点で分かっている被害状況」に記載の調査結果を踏まえて、パスワードリスト攻撃に用いられたリストは外部で入手されたリストである蓋然性が高い、と考えております。

そこで、弊社は以下の対策を行い、2022 年 5 月 23 日 18：00 より当該サービスを再開しました。

＜実施済の対策＞

・当該サービスのパスワードポリシーの強化

・認証画面における reCAPTCHA（リキャプチャ）の導入

・ご登録いただいているすべてのお客様のパスワードをリセット

（再ログイン時に、お客様にて新たなパスワードをご設定いただくこととなります。
パスワードの使い回しを避け、従来ご利用されていたパスワード以外を設定いただくようお願いしております）

・再攻撃に備えた重点的な監視策を強化

・不正にポイントを利用されたお客様に対しての損失補填

パスワードリスト攻撃が行われた期間においてログインされたアカウントについては、ご登録いただいているお客様による正規のログインか、攻撃者による不正なログインかの詳細調査を行い、より正確な被害状況の把握を進めてまいります。

また、今後の再発防止策については、改めてご報告を申し上げます。

６．その他

本件については、警察に届け出を行い、必要な対処を要請中です。

７．問い合わせ窓口

弊社では“なりすまし”による不正アクセスの発生について厳粛に受け止め、さらなるセキュリティレベルの向上策を検討するなど、信頼性向上に引き続き努めてまいります。

すでに不正アクセスが確認されているお客様には個別にご連絡差し上げておりますので、ご確認をお願いいたします。

■お問い合わせ先

kango-inc-pr@kango-roo.com

・3営業日を目途としてご回答申し上げます。
・問い合わせによって取得した個人情報は、本件の調査にのみ使用いたします。
・個人情報につきましては、プライバシーポリシーに則って取り扱います。

以　上