朝日新聞 DIGITAL

ワクチン予約サイト、プロが示す「最悪シナリオ」対処法

有料会員記事　新型コロナウイルス

小宮山亮磨　2021年5月22日 21時00分

東京会場の大規模接種予約サイトで接種券番号などを入力する画面

政府が東京と大阪に設置する新型コロナウイルスワクチンの大規模接種センターで、予約システムの不備が問題になっている。ITセキュリティーに詳しい情報法制研究所の高木浩光理事は、このシステムがサイバー攻撃の標的にされ、多くの人が接種の予約をできない事態になる恐れもあると指摘する。原因は何か、どうすればいいのか。話を聞いた。

――大規模接種センターの予約システムでは、架空の接種券番号などを使っても予約がとれるようになっていることがわかりました。どんな問題が起き得るでしょうか。

予約サイトでは、住んでいる自治体を選んだり、自治体ごとに割り当てられた6桁の番号を入力したりした上で、自治体から届いた接種券に書かれている10桁の番号と生年月日を入力します。ただ、その生年月日が実際のものと合っているかはチェックされません。

初めてアクセスした時に、自己申告にもとづいてその生年月日が「登録」され、アカウントが作られて予約の手続きに入れるようになります。2回目以降にページに入ろうとすると、入力した生年月日が1回目で登録されたものと一致しているか、チェックされます。それによって、本人からのアクセスかどうかを「確認」する仕組みになっているのです。

そのため、もし自分と同じ接種券番号を、ほかの誰かが別の生年月日と組み合わせて入力し、先にアカウントを作られてしまうと、後から作ろうとしても「接種券番号と生年月日が一致しない→別人だ」とシステムに判断されて、入れなくなってしまいます。

他人に接種券番号を使われてしまった場合、どうしたらいいのでしょうか。運営者に求められる対応と、サイバー防衛の「基本中の基本」とは。システムの不備を伝えた報道に、意義はあったのでしょうか。

最悪のシナリオでは、サイバー攻撃によって大量にアカウントの「先取り」が行われ、自分の接種券番号で入れず、予約を取れない人が続出するという事態が考えられます。そこまでいかなくても、接種券番号を間違えて入力した人に先に取られてしまい、入れないということも少なからず起きるでしょう。また、本人が1回目で自分の生年月日の入力を間違えた場合、2回目以降はその間違えた生年月日でないと入れなくなります。

――正しい組み合わせの接種券番号と生年月日が入力されたときにだけ、アカウントを作れるシステムになっていればよかったのでしょうか。

そうでもありません。いまの接種対象者は高齢者ですから、対象者の年齢の幅が30歳あるとして、生年月日は30×365でだいたい1万通り。ひとつの接種券番号について1万通りの生年月日を試せば当たってしまうわけです。

生年月日でのログイン方式「もっての外」

5回間違ったらロックする、といった仕組みにしたとしても、接種券番号の方を変えながら攻撃されるとロックできず、数千個に1個程度の番号で、当たってしまいます。つまり、この方法では結局、完全には防げないわけです。ネット上のログイン機能を設計するときの常識として、生年月日でのログイン方式は「もっての外」なのです。

――マイナンバーを使えば対策になりますか。

マイナンバーでは解決しません。12桁しかありませんので、いまの接種券番号が10桁なのとほとんど変わらず、同じ原理で当てられてしまいます。

――どうすべきだったのでしょうか。

そもそも接種券番号が10桁しかない、しかも各自治体が住民に連続番号を割り振っているとも聞きますが、それはDX（デジタル変革）に対応できていない、20世紀のアナログな発想です。

接種券番号と生年月日で登録する方式でいくなら、接種券番号をランダムな23桁ほどの数字にすることで完全に解決できます。そうすれば、数字の組み合わせは膨大になります。そのなかに本物の番号がごくまれに入っているようにして、システム側で本物の番号かチェックするわけです。

これなら悪意を持った人がランダムに接種券番号を入力しても、本物の番号と一致する確率は無視できるほどに小さくなります。こういう仕組みは、ネットで使えるギフト券のギフト券番号でも使われています。

現状踏まえた運用でカバー

――予約システムを作り直すべきでしょうか。

接種券番号を23桁にするというのは、接種券の発行からやり直しなので、今からではできないでしょう。そのほかに、架空の自治体番号ですら通ってしまうといった不具合も指摘されていました。その不具合を改修すれば、入力ミスは多少防げるでしょうから、直すのも良いと思いますが、架空の予約をされてしまう問題は解決しません。

接種券番号と生年月日の正しい組み合わせのデータを自治体から集めて、予約システムでチェックするように改修すれば、架空予約される頻度を下げられますが、改修までに数カ月はかかるでしょう。

――ではどうすれば。

「他人に接種券番号を使われてしまって、入れない場合がある。そういう時は連絡してください」ということを、国民に周知するほかありません。また、正しく予約した人が攻撃者に不正にキャンセルされてしまう可能性もあるということを、接種会場の係員が知っていなければいけない。

万が一、係員がわかっていないようだったら、予約した本人が「勝手にキャンセルされたんじゃないか」と交渉しないといけない。そのためには、そういうシステムだということを、皆さんに知ってもらわないといけないわけです。

予約システムを管理する側では、攻撃者によって作られた架空の予約がおおむねどれだけあるのかを把握して、明らかな架空予約は削除したうえで、架空とみられる分だけ、予約の枠を増やす必要があります。

ともかくワクチン接種を速やかに進めることが社会の利益なのだから、接種会場で受け付けする人は、キャンセル扱いになっている人が来ても、本人からの申し立てがあればそれを信用して通せばいいと思います。接種券番号を間違えて登録した人が来たときも、同様です。

架空予約を運用でカバーできるなら、いっそのこと、予約システムで接種券番号を使うのをやめてしまい、氏名を登録してもらうだけの予約方式にして、接種会場の受付では、接種券の氏名と照合する、というやり方もあり得ますね。これなら、予約枠の転売を防ぎつつ、最初に述べた「先取り」の被害を防げます。

それから、外国からのサイバー攻撃で架空の予約を大量に入れられてしまう事態が起きるかもしれませんが、その際には上記のように粛々と対処して、「何の影響もありませんよ」という態度を示すことが肝心です。そうした妨害型のサイバー攻撃は、相手国の威信をおとしめることが目的ですから、「知らん顔しておく」ことがサイバー防衛の基本中の基本のはずです。

取材手段は合法、事実の周知を

――防衛省は、記者が架空の接種券番号や市区町村コードを入力しても予約できたと指摘する報道をした朝日新聞出版のニュースサイト「アエラドット」や毎日新聞に抗議しました。

報道の目的が何だったのかは知りませんが、システムの脆弱（ぜいじゃく）性を調べる手順としては、合法なステップを踏んでいると思います。今回の場合、このような挙動をするシステムだということを、利用者となる国民や接種の現場の係員まで広く知らせておくことが必要ですから、その事実を周知したことの意義は大きいでしょう。今回の報道がなかったとしても、アカウント「先取り」の被害が出始めれば、いずれ報道されることになったでしょう。それが外国からのサイバー攻撃だったとしたら、今回より増して私たちの国は恥をかかされることになったでしょう。

――報道する前に政府の側に伝えて、改修のための時間を与えるべきだったという意見もあります。

情報漏洩（ろうえい）が発生する事案の場合には、そういうステップを踏むべきですが、今回はそうではありません。特に今回は、システム改修では解決しないことが明らかです。ワクチン接種を止めるわけにいかない中で、このようなトラブルが起きるシステムだということを広く知らせ、それを承知の上で続けることのほうが重要です。

報道の方々には、「こういったシステムだから、勝手にキャンセルされていることがあるかもしれないけども、ちゃんと受け付けてもらえるから、落ち着いて行動しましょう」と呼びかけてもらいたいと思います。（小宮山亮磨）

◇

たかぎ・ひろみつ　1967年生まれ。名古屋工業大学大学院工学研究科博士後期課程修了。同大学助手、旧通産省工業技術院を経て、産業技術総合研究所サイバーフィジカルセキュリティ研究センター主任研究員。2016年から一般財団法人情報法制研究所理事を兼務。