am I infected?

report

マルウェア感染・脆弱性事例と
ユーザーの対応状況

「am I infected?」をリリースした2022年2月24日から

2022年10月26日現在までのユーザー数は80,815人となりました。

沢山のご利用ありがとうございます。

本レポートでは、これまでの感染事例や脆弱性事例、

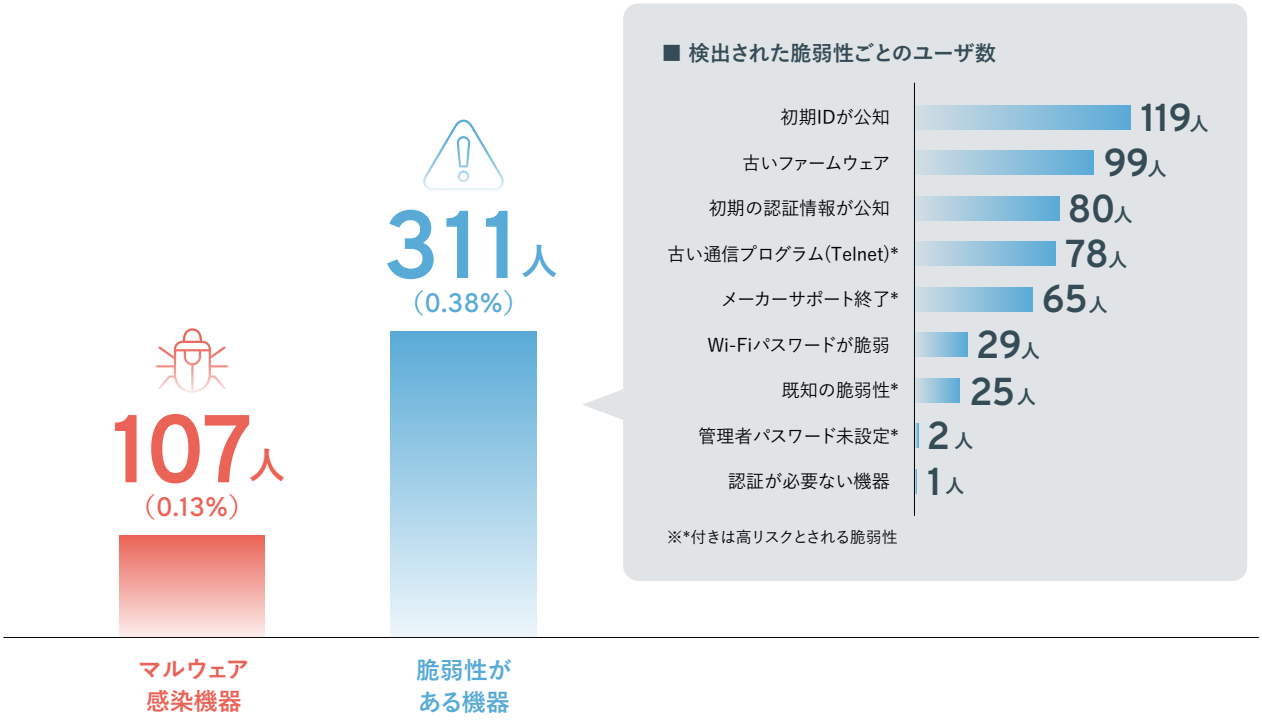
検査で問題が検知された後のユーザーの対応についてご紹介します。

by YNU 横浜国立大学

report 1

これまでの感染事例と脆弱性事例

およそ8万人のユーザーの内、検査でマルウェア感染が検知されたユーザーは107人（0.13%）、脆弱性が検知されたユーザーは311人（0.38%）であり、脆弱性が発見された機器の種類としてルータ、NAS（ネットワークHDD）、Webカメラ、ファイアウォールが確認されています。
検知事例が最も多かった脆弱性は「初期IDが公知」であり、高リスクとされる脆弱性の中では「古い通信プログラム（Telnet）」が最も多く検知されました。



report 2

IoT機器に問題が検知された後のユーザーの対応

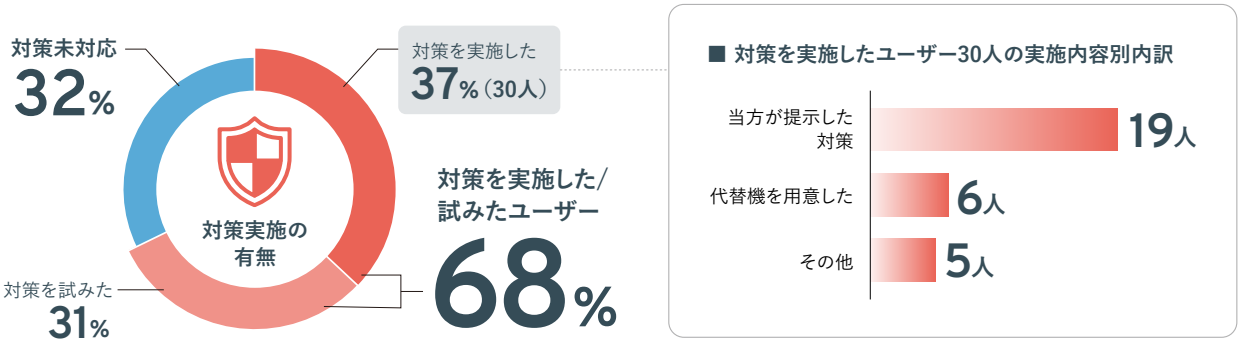
検査でマルウェア感染または脆弱性が検知されたユーザー381人を対象として、その後の対応に関するアンケート調査を実施しましたので、結果の概要をご紹介します。

調査概要

調 査 内 容 ： IoT機器に問題が検知された後のユーザーの対応に関するアンケート調査
調 査 対 象 ： 2022年6月12日までに検査で問題が検知されたユーザー381人
調 査 時 期 ： 2022年6月15日にアンケートをメールで送付
回 答 者 数 ： 95人

対策を実施したユーザーはどの程度いるのか？

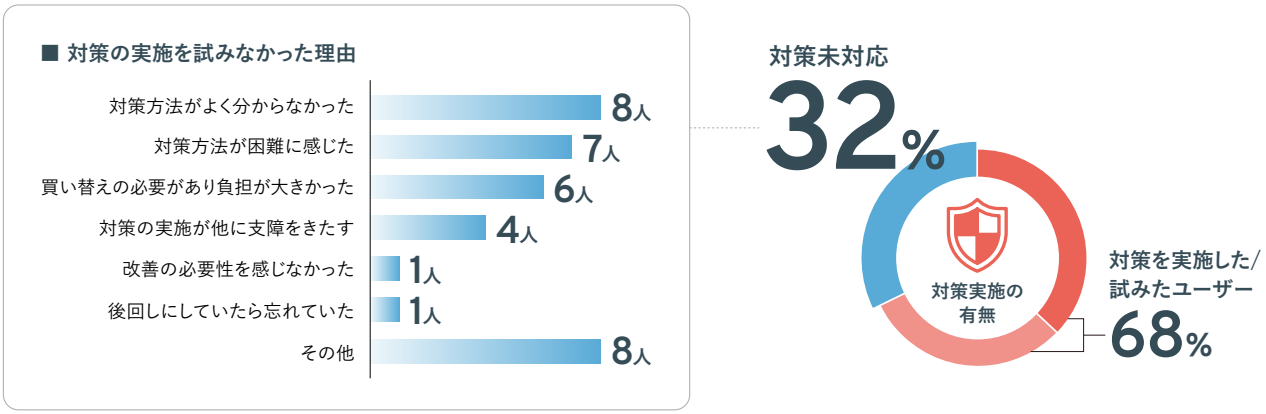
対策実施の有無に関する質問に対し、回答者全体のおよそ68%が「対策を実施した」または「対策の実施を試みた」と回答しました。
「対策を実施した」と回答したユーザーは、概ね提示された方法に従う形で問題を解消したと回答しました。例えば、マルウェア感染が検知された方であれば機器の再起動やファームウェア更新、脆弱性としてTelnet（古い通信プログラム）の動作が検知された方につきましてはその停止が提示内容にあたります。
その他、「代替機を用意した」と回答する方が多い結果となりました。



※「対策を実施した」と回答したユーザは改善確認済み、「対策を試みた」と回答したユーザは改善未確認

対策方法にご不明点がある方やサポートが必要な方はご連絡下さい

「対策の実施を試みなかった」と回答したユーザーの多くは、その理由として「対策方法がよく分からなかった」「対策方法が困難に感じた」と回答しており、問題を解消する必要性を理解していてもそれをどう解消するかに悩んでいる方が多いようでした。
「am I infected?」が提示する対策内容は、多くのユーザーに当てはまるように、どうしても抽象度が高くなってしまいます。対策方法にご不明点がある方やサポートが必要な方は、ぜひynugr-cyberpcr[atmark]ynu.ac.jpまでお問合せください。



対策を実施できたらぜひ再検査を

「対策の実施を完了した」と回答したユーザーの中で、再検査を実施していないユーザーが多数見受けられました。再検査していただかなければ改善有無の確認が取れませんので、対策を実施したらぜひ再検査していただけますと幸いです。
また、マルウェア感染に対して「対策の実施を完了した」と回答したユーザーの中で、感染が検知されてから24時間経たない内に再検査を実施しているユーザーが多数見受けられました。マルウェア感染検査の仕組み上、対策を実施した後24時間以上置いて頂かなければその効果を確認することができません。マルウェア感染が検知された方で対策を実施された方は、24時間以上置いてから再検査していただきますようお願い致します。