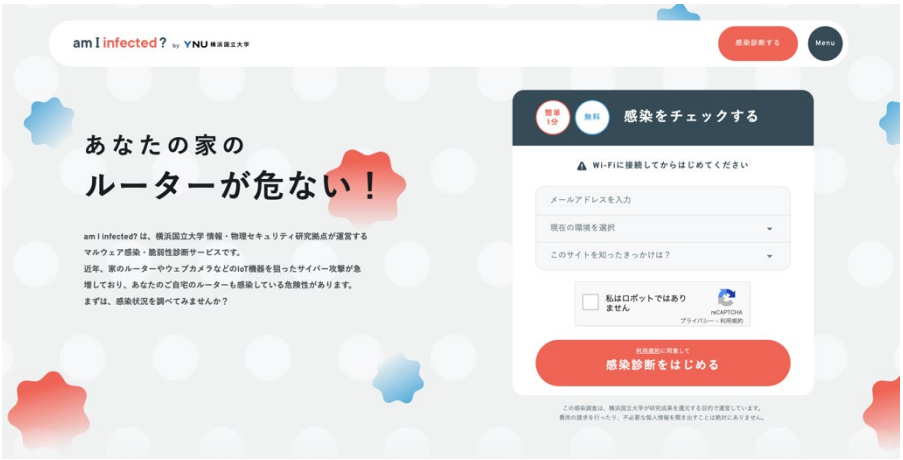
Press Release
2022 年 2 月 24 日

横浜国立大学
株式会社ゼロゼロワン

家庭用ルーターなど IoT 機器のマルウェア検査サービス「am I infected?」の無料提供を開始

～5 分以内に検査結果をメールでお知らせ。マルウェアに感染していた場合の対処法までサポート～

国立大学法人 横浜国立大学（所在地：神奈川県横浜市、学長：梅原出、以下「横浜国立大学」）と株式会社ゼロゼロワン（本社：東京都渋谷区、代表取締役 CEO：萩原雄一、以下「ゼロゼロワン」）は、家庭用ルーターやスマート家電を始めとした IoT 機器のマルウェア※1 検査サービス「am I infected?（アム・アイ・インフェクテッド）」（https://amii.ynu.codes/）の提供を開始します。



本サービスは、家庭用ルーターやスマート家電などの IoT 機器がマルウェアに感染していないか、脆弱な状態で利用していないかを利用者自身で検査・対策できる無料のサービスです。検査結果は、利用者が入力したメールアドレス宛てに 5 分以内に届き、万が一マルウェア感染が疑われる場合や、IoT 機器が脆弱な状態であった場合の推奨対策についてご案内します。

※1 マルウェア（malware）とは、「malicious software」（悪意あるソフトウェア）の略であり、感染した機器に不正かつ有害な動作をさせるプログラムの総称です。

【サービス提供の背景】

横浜国立大学　情報・物理セキュリティ研究拠点では、IoT 機器におけるセキュリティ対策についての研究を 2015 年から取り組んできました。IoT 機器を狙うサイバー攻撃は増加を続けており※2、特に新型コロナウイルスの感染拡大をきっかけに、ニューノーマルな働き方としてテレワークが広く普及したことから、家庭用のルーターやウェブカメラなどの IoT 機器のセキュリティ確保の重要性がさらに高まっています。マルウェア感染した IoT 機器は感染後も変化なく動作し続けるため、感染していたとしても利用者側が気付きにくい特徴があります。そこで、自宅の IoT 機器を安心して利用し続けられることを目的としてマルウェア感染や脆弱性の有無を検査するサービスを開始しました。

※2 総務省：「サイバー攻撃に関する最近の動向、NICT（NICTER）によるサイバー攻撃観測」URL: https://www.soumu.go.jp/main_content/000771974.pdf

【本サービスの概要】

本サービスは、家庭用ルーターやスマート家電などの IoT 機器がマルウェアに感染していないか、脆弱なまま利用していないかを利用者自身で簡単に検査できる無料のサービスです。専用サイトから、検査結果を送信するメールアドレスの入力と、検査を実施する環境に関するアンケートに回答することで Web サイトにアクセスした際に利用している IP アドレスに対して検査を実施します。検査結果は、入力したメールアドレス宛てに検査結果ページへのリンクが送付されます。万が一、マルウェアへの感染が疑われる場合は同ページの推奨対策を参考に利用者自身で対策を行います。

＜利用方法＞

・費用：無料（オプション等による追加料金は発生しません）

・サービス URL：https://amii.ynu.codes/

・お問い合わせ：ynugr-cyberpcr@ynu.ac.jp

【本サービスにおけるそれぞれの役割】

本サービスは、横浜国立大学　情報・物理セキュリティ研究拠点が運用しているハニーポット※3 のほか、ゼロゼロワンが開発・提供する IoT 検索エンジン「Karma※4」のデータ、国立研究開発法人情報通信研究機構（NICT：エヌアイシーティー）が開発・運用するサイバー攻撃観測・分析システム「NICTER※5」のデータを利用しています。横浜国立大学　情報・物理セキュリティ研究拠点とゼロゼロワンは、2021 年 6 月より横浜国立大学内外のセキュリティスキャンに関する共同研究を行っており、今回のサービスは学外の IP アドレスに対するセキュリティスキャンの成果を活用しています。また、横浜国立大学は、NICT が昨年 4 月に創設した産学官連携拠点 CYNEX(Cybersecurity Nexus) ※6 に参画しており、CYNEX のサブプロジェクトである Co-Nexus S(Security Operation & Sharing)より NICTER の観測データの提供を受けています。

※3 横浜国立大学　情報・物理セキュリティ研究拠点では、脆弱な IoT 機器を模倣して攻撃を観測するハニーポットと呼ばれる囮システムを運用しています。具体的には、IoT 機器の Web インターフェースを模倣したハニーポットと、Telnet と呼ばれる脆弱なサービスを動作させたハニーポットを運用しており、IoT 機器の脆弱性を利用した攻撃や、IoT 機器に感染するマルウェアの収集を行っています。URL：https://sec.ynu.codes/iot

※4 Karma（カルマ）は、インターネットに接続された国内の IoT 機器を検索するサービスです。独自開発した判別手法と、機器に紐づくポート番号や IP アドレス等の情報、バナーに含まれる日本語検索を組み合わせることで、詳細な機器情報の判別が可能です。また、既存の脆弱性情報や機器のバージョンからセキュリティリスクの可視化も可能です。URL：https://www.00one.jp/karma/

※5 NICTER（Network Incident analysis Center for Tactical Emergency Response：ニクター）は、無差別型サイバー攻撃の大局的な動向を把握することを目的としたサイバー攻撃観測・分析システムであり、ダークネットと呼ばれる未使用の IP アドレスを大規模に観測しています。URL：https://www.nicter.jp/

※6 CYNEX（Cybersecurity Nexus：サイネックス）は、NICT に設けられたサイバーセキュリティに関するデータや人材育成の結節点となる組織であり、サイバーセキュリティ情報の収集・分析・蓄積・共有を行っています。URL：https://www.nict.go.jp/cynex/

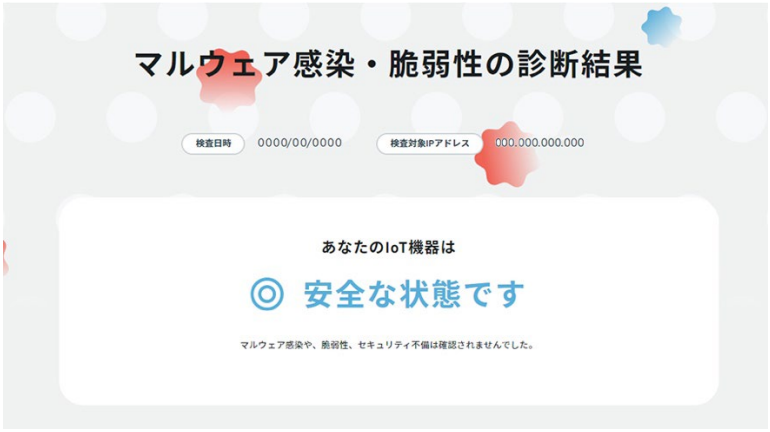
【今後の展開】

本サービスの提供により、脆弱な IoT 機器の根本原因の解決や効果的な注意喚起手法などに向けて、更なる研究開発に活かします。今後もサイバーセキュリティの研究を通じて、安全・安心な社会の実現に貢献します。

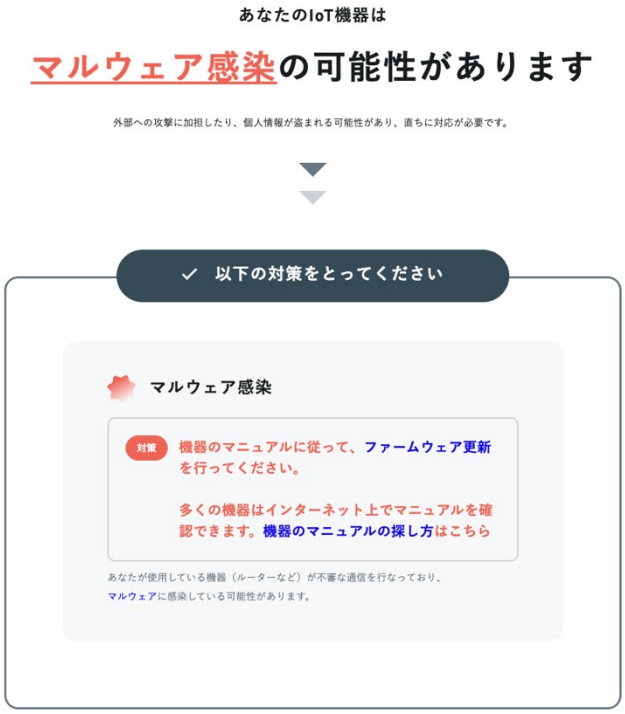
【横浜国立大学　大学院環境情報研究院/先端科学高等研究院　吉岡 克成　准教授のコメント】

我々の周りにある様々なモノがインターネットに接続するようになり、サイバー攻撃やマルウェア感染による脅威が高まっています。また、昨今のテレワークの普及に伴い家庭用ルーター等のセキュリティの重要性が今まで以上に高くなっています。これまでの研究成果と知見を生かして、サイバー攻撃を未然に防ぐことや、万が一、感染してしまっても自分で気づくことができる仕組みをこの度作りました。無償でご利用いただけますので、ぜひ多くの方にこのサービスを使っていただき、安全・安心に IoT 機器を利用いただけたらと思っています。

【サービスの利用イメージ】



安全な状態の表示例



マルウェア感染の可能性がある状態の表示例

横浜国立大学　情報・物理セキュリティ研究拠点　概要

横浜国立大学 情報・物理セキュリティ研究拠点では、サイバー攻撃の実観測、分析に基づき、対策を導出する研究を行っています。おとりのシステムである「ハニーポット」によりサイバー攻撃を惹きつけ、詳細に観測する受動的観測や攻撃の対象となる脆弱なシステムを探索する能動的観測により、これらの状況を把握し、独自の分析により、そのメカニズムを明らかにすることで、効果的な対策を導出します。これまで IoT におけるサイバー攻撃やマルウェア感染の蔓延、超大規模サービス妨害攻撃の観測、分析を行い、その観測・分析結果を多数の公的機関、民間企業、研究コミュニティに提供しています。

株式会社ゼロゼロワン　概要

ゼロゼロワンは、IoT 機器開発事業者向けに設計段階におけるセキュリティ面での不安解消や想定外の脅威を作らないための支援を行うとともに、IoT 機器を安全・安心に利用してもらうための啓蒙活動を行う会社です。IoT 機器の普及に伴いインターネットに繋がることが当たり前になった時代の不安を取り除くために生まれました。OSINT を含む様々な情報を可視化する検索エンジンである Karma と、より安全な製品開発のためのコンサルティングサービスを事業の柱としています。

設　立　　2019 年 8 月 23 日

資本金　　5,000 万円

所在地　　東京都渋谷区本町 4-22-10　パークハビオ渋谷本町レジデンス 219 号

事業内容　IoT 機器のシステム解析・コンサルティングサービス・調査研究・啓蒙活動等

URL　https://www.00one.jp/

【本サービスに関するお問い合わせ先】

横浜国立大学　吉岡克成、佐々木貴之

e-mail： ynugr-cyberpcr@ynu.ac.jp