【報道発表資料】

株式会社 KDDI 総合研究所
株式会社セキュアブレイン
国立大学法人横浜国立大学
国立大学法人神戸大学
株式会社構造計画研究所
国立大学法人金沢大学
国立大学法人岡山大学
国立研究開発法人情報通信研究機構

2020 年 3 月 16 日

Web 媒介型サイバー攻撃対策プロジェクト「WarpDrive」スマートフォン向け実証実験を開始

～「攻殻機動隊 S.A.C.」タチコマからの問いに答えながらセキュリティ機能を強化～

株式会社 KDDI 総合研究所、株式会社セキュアブレイン、国立大学法人横浜国立大学、国立大学法人神戸大学、株式会社構造計画研究所、国立大学法人金沢大学、国立大学法人岡山大学、国立研究開発法人情報通信研究機構（NICT）は、NICT の委託研究「Web 媒介型攻撃対策技術の実用化に向けた研究開発」（略称、WarpDrive（注 1））において、スマートフォンを狙った Web 媒介型攻撃の実態把握と対策技術向上のために、アニメ作品「攻殻機動隊 S.A.C.」シリーズのキャラクター「タチコマ」をモチーフにした Android のスマートフォン向けアプリ「タチコマ・セキュリティ・エージェント・モバイル（以下、タチコマ・モバイル）」を開発しました。2020 年 3 月 16 日からタチコマ・モバイルを配布し、ユーザ参加型の実証実験を開始します。

【背景】

サイバー攻撃は多様化・巧妙化を続け、Web サイトを媒介としてマルウェアに感染する Web 媒介型攻撃による被害も後を絶ちません。WarpDrive では、これまで Web 媒介型攻撃の観測と対策のために、PC ユーザ向けの実証実験を行ってきました（注 2）。その一方で、スマートフォンを狙った攻撃も増加しており深刻な問題となっています。スマートフォンへの攻撃は、Web ブラウザだけでなくショートメッセージなど、さまざまなアプリを媒介しユーザごとに異なる経路から行われるために、これまでの攻撃観測網で攻撃の実態把握や迅速な対策展開が困難でした。

【実証実験概要】

WarpDrive において開発した Android のスマートフォン向けアプリ「タチコマ・モバイル」を使ったユーザ参加型の実証実験を 2020 年 3 月 16 日から開始します。また、同日から WarpDrive ポータルサイト（図 1）でアプリを一般ユーザ向けに無償配布します。

⇒タチコマ・モバイルのダウンロード（https://warpdrive-project.jp/mobile-app/）

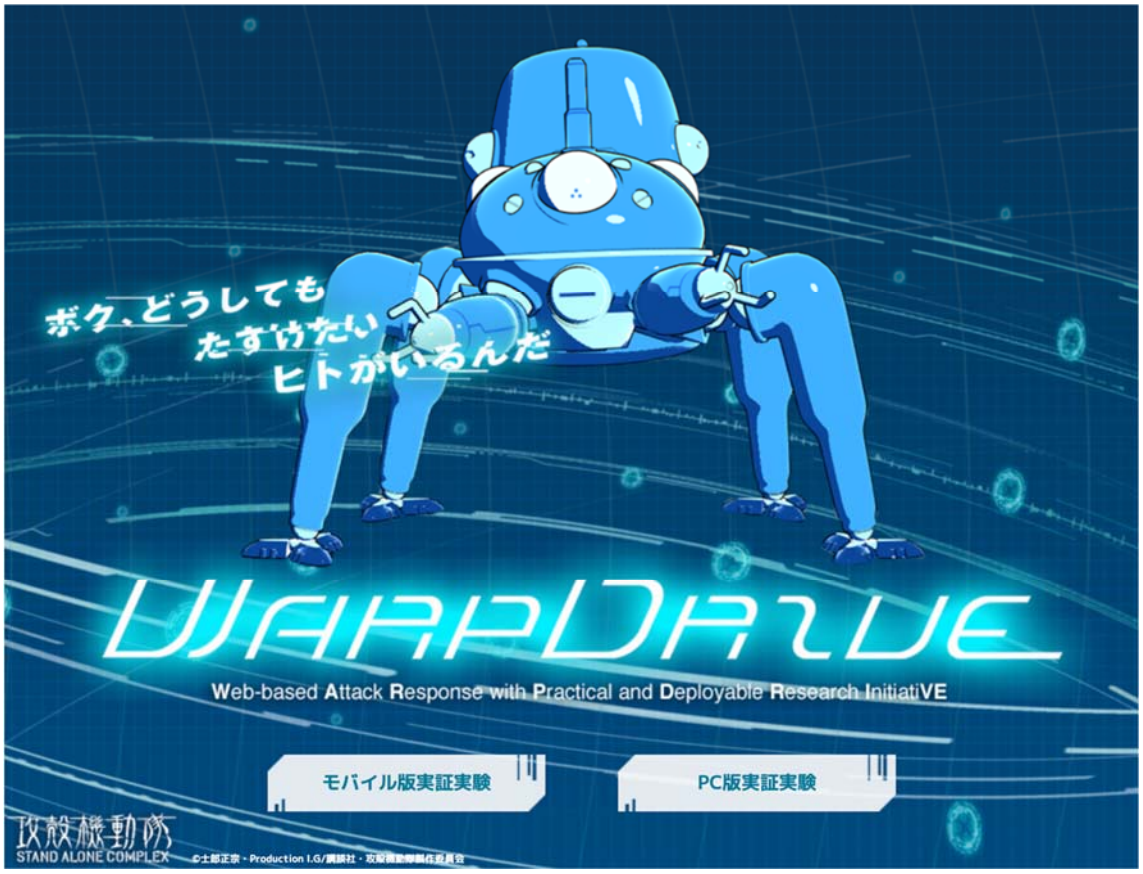


図 1 WarpDrive ポータルサイト（https://warpdrive-project.jp）

「タチコマ・モバイル」には、ユーザが遭遇した怪しいサイトを報告する「タチコマへ報告」機能やスマートフォンの利用状況を可視化する「プロファイル」機能が搭載されています（図 2）。また、ユーザから提供される Web 媒介型攻撃に関するデータを収集・分析し、セキュリティ機能の強化や未知の攻撃の観測を行います。さらに、定期的に出される簡単な質問「タチコマの問い」に回答してもらうことによって、セキュリティをはじめとするさまざまな情報通信技術についてユーザと一緒に考えていきます。

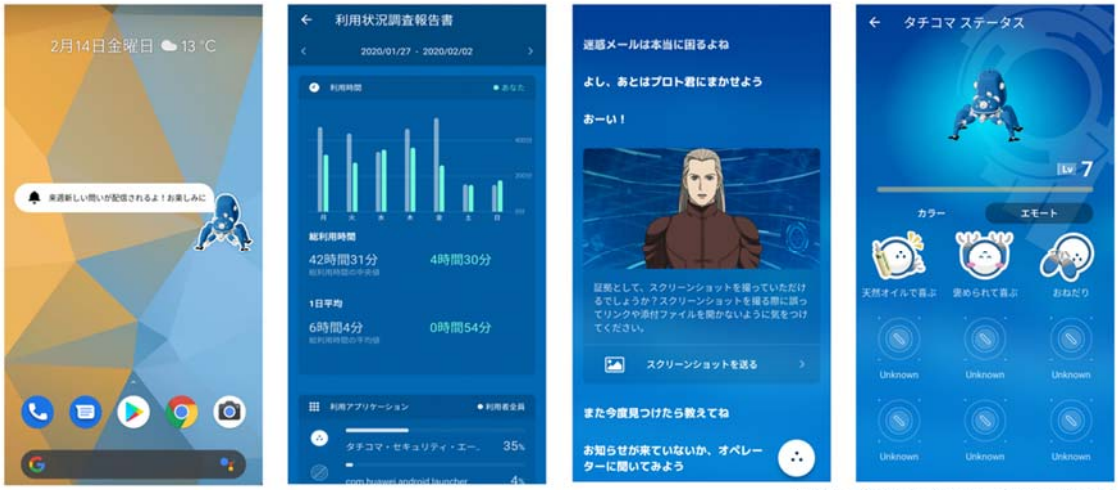


図２　アプリ画面

【今後】

WarpDrive では、PC 版と Mobile 版の実証実験の結果を基に、複雑化している Web 媒介型攻撃の実態を解明して、攻撃サイトの迅速な検知や、テイクダウン（撤去）に向けた情報提供、攻撃対策技術の実用化を目指していきます。

別紙

参考資料

【実証実験体制】

組織名	主な担務
株式会社 KDDI 総合研究所 （代表取締役所長：中島康之）	全体統括、分析基盤の開発、タチコマ・モバイル開発
株式会社セキュアブレイン （代表取締役社長兼 CEO：青山健一）	タチコマ・モバイルのエンジン開発、リパッケージによる不正アプリ検知
国立大学法人横浜国立大学 （学長：長谷部勇一）	危険検索ワードによる攻撃被害の事前予測、IoT 機器に関するセキュリティ通知
国立大学法人神戸大学 （学長：武田 廣）	機械学習による収集データの分析
株式会社構造計画研究所 （代表執行役社長：服部正太）	分析基盤における攻撃事例分析
国立大学法人金沢大学 （学長：山崎光悦）	プライバシー設計・プライバシーリスク評価
国立大学法人岡山大学 （学長：槇野博史）	リダイレクトによる攻撃検知
国立研究開発法人情報通信研究機構 （理事長：徳田英幸）	実証実験の監修、可視化およびデザイン

【プライバシーへの配慮】

実証実験にさきがけて、ユーザのプライバシー保護の観点から、NICT 内の「パーソナルデータ取扱研究開発業務審議委員会」で審議し、収集データの内容、管理方法、利用について確認しています。また、実証実験の参加規約、収集するデータの取り扱いに関して定めた文書を整備し、安心して実証実験にご参加いただけるよう情報を開示しています。詳しくは以下のリンクをご覧ください。

WarpDrive スマートフォン向け実証実験のプライバシーポリシー（https://warpdrive-project.jp/mobile-app/privacypolicy/）

【攻撃観測のための収集データ一覧】

セキュリティの研究開発を目的として、スマートフォンから以下のデータを収集します。このデータは、本研究開発の目的にのみ利用して、その他の目的に利用しません。また、参加者は、いつでも実証実験をやめることができ、提供したデータの削除を求めることができます。データ取扱いについては、実証実験のプライバシーポリシーをご覧ください。

データ種別	説明
Web アクセス履歴	Google Chrome アプリおよび Chrome のコンポーネントを使用したアプリにおいて Web ページを表示した際の URL およびアンカータグのテキストなど
アプリ表示履歴	ユーザがフォアグランドとして実行したアプリおよびアプリにおける Activity の履歴
インストールアプリ一覧	端末にインストールされているアプリのパッケージ名およびアプリ構成や証明書などの関連情報
SMS メッセージのハッシュ値	メッセージに URL もしくはブラックリストの文字列が含まれている場合のメッセージのファジーハッシュ、送信者、URL
通信ネットワーク	端末がインターネットにアクセスする際に付与されるパブリック IP アドレスとその接続種別など
端末情報	端末名、OS のバージョン、パッチレベルなどの端末情報
提供元不明アプリのインストール許可操作	公式アプリ配布サイト以外からアプリをインストールすることをユーザが許可する操作

【強化される新しいセキュリティ機能について】

・リダイレクトによる攻撃検知

Web サイトを表示するときに、ユーザを異なる Web サイトへ自動的に転送するリダイレクトという技術が使われることがあります。Web を媒介とする攻撃における悪性サイトは、頻繁にこのリダイレクトが悪用しており、リダイレクトに特徴があることが知られています。岡山大学では、このリダイレクトのタイミングから悪性サイトへの誘導を検知する方式を研究開発しました（注 3）。

・危険検索ワードによる攻撃被害の事前予測

特定のキーワードにより検索した結果は、悪性サイトが多く含まれることが報告されています。横浜国立大学の調べでは、ユーザが検索エンジンにおいて特定のワードを検索した後に、悪性サイトへ遷移する確率は、当該ワードを使わない場合に比べて最大で 11 倍とな

ることが確認されています。そこで、危険な検索ワードを検索した際に、悪性サイトへ遭遇する確率が高いことを事前に通知する方式を研究開発しました（注 4）。

・リパッケージ（改造版）アプリ検知

Android では、配布されているアプリに第三者が無断で機能を追加・変更するリパッケージという手法が知られています。人気のあるアプリに対して改造が行われ、悪質な動作が付与されたマルウェアの存在も報告されています。セキュアブレインでは、改造版アプリがインターネット上で多数配布され、ソーシャル・ネットワーキング・サービスの一つである Twitter で情報共有されている実態を明らかにしました。タチコマ・モバイルでは、改造版アプリのインストールに対して通知する実験を行います（注 5）。

・IoT 機器に関するセキュリティ通知

現在、無線 Wi-Fi ルーターなど家庭内の IoT 機器がマルウェアに感染する事例が多く報告されています。IoT 機器がマルウェアに感染すると不特定多数のホストへ探索活動を行ったり、大量の通信を発生させてサービスができないようにしたりする DDoS 攻撃に加担する場合があります。横浜国立大学では、このようにマルウェアに感染してしまう恐れのある IoT 機器を効率的に発見する技術を開発しました。タチコマ・モバイルでは、ユーザの端末の IP アドレスでこのような脆弱な IoT 機器を発見した場合に、ユーザに通知する実験を行います（注 6）。

注 1：Web-based Attack Response with Practical and Deployable Research InitiatiVE

注 2：Web 媒介型サイバー攻撃対策プロジェクト「WarpDrive」の実証実験開始について（2018 年 6 月 1 日）
https://www.kddi-research.jp/newsrelease/2018/060101.html

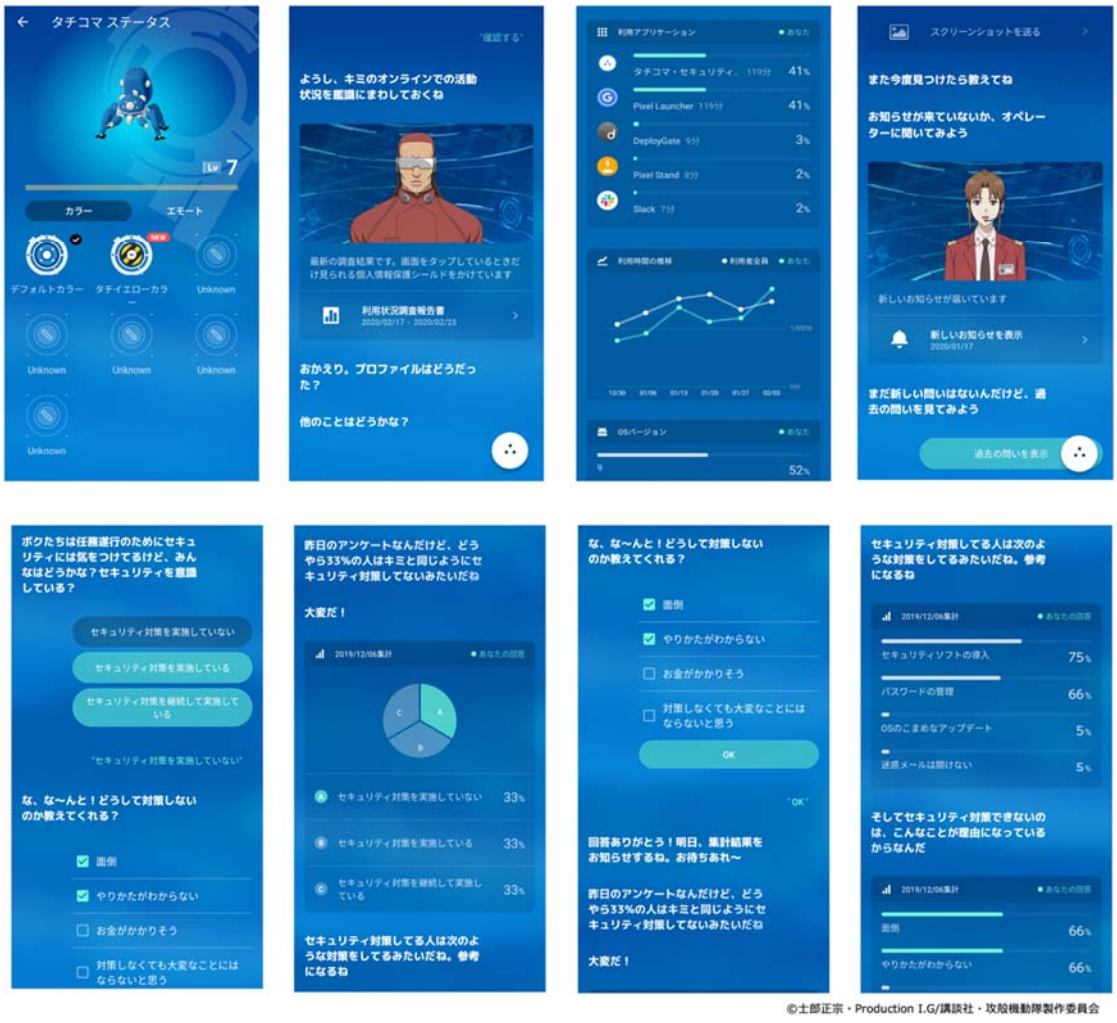
注 3：折戸凜太郎，佐藤将也，山内利宏，"Android における URL バーの切り替わり間隔に着目した利用者の意図しない Web サイトへの遷移の検知手法，" コンピュータセキュリティシンポジウム 2019 論文集

注 4：源平祐太，中川雄太，高田一樹，小出駿，金井文宏，秋山満昭，田辺瑠偉，吉岡克成，松本勉，"悪性 Web サイトに到達しやすい危険検索単語の検知，" コンピュータセキュリティシンポジウム 2019 論文集

注 5：三村隆夫，巻島和雄，岩本一樹，"ソーシャルネットワークで共有される Android アプリケーションの実態調査，" コンピュータセキュリティシンポジウム 2018 論文集

注 6：西田慎，保泉拓哉，内田佳介，藤田彬，吉岡克成，松本勉，"IoT 機器のユーザへの専用クライアントを介したセキュリティ通知実験の検討，" 信学技報，vol. 118，no. 486

【スクリーンショット】



【本件に関する問い合わせ先】

株式会社 KDDI 総合研究所　営業・広報部
TEL：049-278-7464

株式会社セキュアブレイン　広報
TEL：03-3234-3001

国立大学法人横浜国立大学　総務企画部 学長室広報・渉外係
TEL：045-339-3027

国立大学法人神戸大学　数理・データサイエンスセンター
TEL：078-803-5753

株式会社構造計画研究所　広報・IR 室
TEL：03-5342-1040

国立大学法人金沢大学　総務部広報室
TEL：076-264-5024

国立大学法人岡山大学　総務・企画部 広報課
TEL：086-251-7292

国立研究開発法人情報通信研究機構　広報部 報道室
TEL：042-327-6923

＜リリース内容に関する岡山大学へのお問い合わせは、下記の宛先へお願いします。＞
岡山大学大学院自然科学研究科
准教授　山内　利宏
（電話番号）086-251-8188
（ URL ）　https://www.swlab.cs.okayama-u.ac.jp/~yamauchi/index-j.html