【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

2018 年 6 月 1 日

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
～ 電脳空間にリアライズしたタチコマで Web の安全性向上へ ～

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、攻殻機動隊 REALIZE PROJECT と連携して、Web を媒介とするサイバー攻撃の実態把握と対策技術の向上のため、ユーザ参加型の実証実験を 2018 年 6 月 1 日より開始します。

図 1 WarpDrive ポータルサイト

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

【背景】

サイバー攻撃は多様化・巧妙化を続け、Web サイトを閲覧するだけで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。Web 媒介型攻撃は、特定の Web サイトを閲覧したユーザに対してのみ攻撃が行われるため、受動的なサイバー攻撃観測網では Web 媒介型攻撃の実態把握や迅速な対策展開が困難でした。

【今回の取り組み】

Web 媒介型攻撃の実態把握と対策技術の向上のため、KDDI 総合研究所、セキュアブレイン、横浜国立大学、神戸大学、構造計画研究所、金沢大学、岡山大学は、これまで「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]）に取り組んできました。

WarpDrive ではアニメ「攻殻機動隊 S.A.C.」シリーズに登場するキャラクター「タチコマ」をモチーフに、Web 媒介型攻撃対策ソフトウェア「タチコマ・セキュリティ・エージェント （以下、タチコマ SA）」を開発しました。タチコマ SA は、(1)ユーザの Web ブラウザの中で Web 媒介型攻撃の観測・分析を行い、(2)攻撃検知時には悪性 Web サイトの閲覧をブロックし、(3)ユーザに警告やアドバイスを行います。さらに、インターネット上に分散したタチコマ SA たちが、(4)並列化（情報集約・横断分析・新機能展開等）を繰り返し、最新の Web 媒介型攻撃に対応します。

今回、WarpDrive はユーザ参加型の実証実験を 2018 年 6 月 1 日（金）より開始します。同日より WarpDrive ポータルサイト（図 1）において、Windows 版および macOS 版のタチコマ SA を、一般ユーザ向けに無償配布します。タチコマ SA をインストールすると、上記のセキュリティ機能に加え、攻殻機動隊のコンテンツや同作をモチーフにした Web 空間の可視化等も体験できます（図 2、図 3）。WarpDrive は、本実証実験を通して「電脳空間におけるタチコマ・リアライズ」を進め、Web の安全性向上を目指します。

タチコマ SA のダウンロードはこちらから⇒ https://warpdrive-project.jp/

図 2 Web 閲覧履歴の可視化

図 3 Web コンテンツの可視化

【用語解説】

・攻殻機動隊

1989 年に士郎正宗によって生み出された SF 漫画作品で、21 世紀の科学技術が飛躍的に高度化した日本を舞台に、電脳化した人間、サイボーグ、アンドロイド、バイオロイドが混在する社会で起こるテロや暗殺、汚職事件に立ち向かう内務省の公安警察組織「公安 9 課」通称「攻殻機動隊」の活動を描いた物語です。

・タチコマ

士郎正宗による SF 漫画「攻殻機動隊」を原作とし制作されたアニメ「攻殻機動隊 S.A.C.」シリーズに登場する自律走行可能な思考戦車です。高度な人工知能（AI） を搭載しており、操縦者なしでも独自に任務を遂行することができ、電脳空間においては、情報収集や危険な状況の察知など、公安 9 課のメンバーを強力にサポートします。

・攻殻機動隊 REALIZE PROJECT

日本を代表する企業、大学の研究開発者、公共機関、そして製作委員会が一体となり、「攻殻機動隊」シリーズに描かれている数々の近未来テクノロジーの実現を追究するプロジェクトです。

URL: http://www.realize-project.jp/

・Web 媒介型攻撃

典型的な Web 媒介型攻撃（図 4）では、攻撃の起点となる入口サイトにユーザがアクセスすると、中継サイトを経由して攻撃サイトに転送（リダイレクト）され、最終的にマルウェア（不正プログラム）がユーザのコンピュータに感染します。Web 媒介型攻撃ではユーザの Web アクセスを発端に攻撃が発生するため、ダークネット観測など従来の受動的な攻撃観測手法ではその脅威を捉えられません。また、広大な Web 空間から悪性サイトを見つけ出すためには多くの課題があり、効果的かつ効率的に悪性サイトを検出する技術の研究開発が求められています。

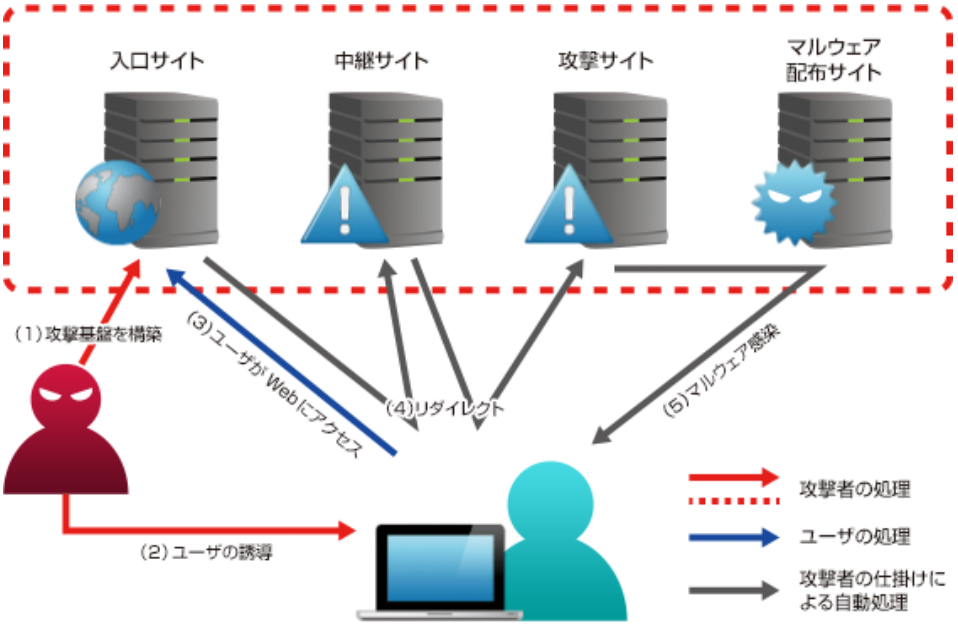

図 4　Web 媒介型攻撃の流れ

【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）	実証実験の全体統括、大規模分析基盤の開発
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 SA 開発
国立大学法人横浜国立大学 （学長：長谷部勇一）	Web に関連する脅威分析
国立大学法人神戸大学 （学長：武田 廣）	機械学習による攻撃検知手法の検討
株式会社構造計画研究所 （代表取締役社長：服部正太）	大規模分析基盤における攻撃検知手法の検討

国立大学法人金沢大学 （学長：山崎光悦）	プライバシに関する検討
国立大学法人岡山大学 （学長：槇野博史）	モバイル環境における攻撃観測方法の検討
国立研究開発法人情報通信研究機構 （理事長：徳田英幸）	実証実験および可視化デザインの監修

【プライバシへの配慮について】

本実証実験の実施に先駆け、実証実験参加ユーザのプライバシ保護の観点から、実証実験におけるデータの収集および利用について、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、収集するデータの内容、管理方法、利用について実証実験参加ユーザのプライバシに配慮した実施内容となっていることを確認しています。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 実証実験の参加規約およびデータの取り扱い
https://warpdrive-project.jp/terms.html

【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
E-mail：inquiry@kddi-research.jp

株式会社セキュアブレイン　広報
TEL：03-3234-3001
E-mail：info@securebrain.co.jp

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
E-mail：press@ynu.ac.jp

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
E-mail：cmds-sec@edu.kobe-u.ac.jp

株式会社構造計画研究所　広報・海外支援室
TEL：03-5342-1040
E-mail：kke-pr@kke.co.jp

国立大学法人金沢大学　総務部広報室
TEL：076-264-5024
E-mail：koho@adm.kanazawa-u.ac.jp

国立大学法人岡山大学　総務・企画部 広報・情報戦略室
TEL：086-251-7292
E-mail：www-adm@adm.okayama-u.ac.jp

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
E-mail：publicity@nict.go.jp