



ホーム > プレスリリース

プレスリリース

プレスリリース一覧

2018年

11月07日

プレスリリース

「Black Duck」の販売、及び「脆弱性検証サービス」を提供開始

09月18日

プレスリリース

成長する組み込み用のAI基盤「Sensing Network Cognitive SDK」を販売開始

05月28日

プレスリリース

GUI自動化・RPAツールの決定版 QualityPartner GENEST
RPA機能を強化した「QualityPartner GENEST V2.0」を販売開始

01月22日

プレスリリース

MQTTプロトコルに対応した「ソフトウェア脆弱性検証サービス」を提供開始

[利用条件](#)

[個人情報保護ポリシー](#)

[お問い合わせ](#)

[サイトマップ](#)

[富士通ホームへ](#)

Copyright 1994 - 2021 FUJITSU

プレスリリース

> 2018年

> 2017年

> 2016年

> 2015年

プレスリリース

2018年11月7日

株式会社富士通コンピュータテクノロジー

お問い合わせ

- [当社へのお問い合わせ](#)

カタログ一覧



このコンテンツについて

- [利用条件](#)
- [個人情報保護ポリシー](#)

セキュアな組み込みシステム開発を支援 「Black Duck」の販売、及び「脆弱性検証サービス」の提供を開始

株式会社富士通コンピュータテクノロジー（代表取締役社長：福元 芳朗、本社：川崎市中原区上小田中4-1-1）は、2018年11月よりSynopsys, Inc.（以下、シノプシス社）「Black Duck」の販売を開始します。

昨年、当社は日本シノプシス合同会社（社長 職務執行者：藤井 公雄、本社：東京都世田谷区）とシノプシス社製品における販売店契約を締結し、Coverity、Defensicsを販売しています。今回、新たにBlack Duckの販売を開始することで、セキュアな組み込みシステム開発支援を更に強化することが可能となります。

併せて、セキュアな組み込みシステム開発を支援する「脆弱性検証サービス」の提供を開始します。「脆弱性検証サービス」は、シノプシス社製品を活用することで検証工程における静的・動的検証、また既知・未知の脆弱性対策を網羅的にカバーすることが可能となります。

また、今後は更に要件・設計工程におけるセキュリティバイデザインの適用や、運用・保守工程におけるP-SIRT構築など、セキュアな組み込みシステム開発における全ての工程を対象とした脆弱性対策を提供していく予定です。富士通コンピュータテクノロジーの「脆弱性検証サービス」は、お客様に最も適したサービスとツールの提供で、セキュアな組み込みシステム開発を支援します。

背景

IoTに代表されるインターネットへ接続するIoTデバイス（以下、組み込みシステム）が急激に増加し、それに伴い組み込みシステムに対するサイバー攻撃の脅威も増大しています。この対策として近年、「IoTセキュリティガイドライン」等の指針公開や、標準化・規約化へ向けた整備も進んでいますが、組み込みシステムに対応したセキュリティとして具体的な手段を検討していくには課題があります。

富士通コンピュータテクノロジーでは、セキュアな組み込みシステム開発を実現するために、既に提供している「ソースコード検証サービス」と「ファジング適用サービス（旧名称：ソフトウェア脆弱性検証サービス）」をベースとし、「OSS脆弱性チェックサービス」と「脆弱性スキャン適用サービス」を加えることで、検証工程における静的・動的な検証、また既知・未知への脆弱性対策を網羅的にカバーする「脆弱性検証サービス」の提供を開始します。

「Black Duck」は、その中で「OSS脆弱性チェックサービス」に必要なツールとしてお客様に活用して頂くことを前提に販売を開始します。

そして、当社が長年、組み込みシステム開発会社として培ってきた開発技術と検証技術を活かし、お客様に合うサービスやツールを提供することで、セキュアな組み込みシステム開発を支援します。

脆弱性検証サービス概要

組み込みシステムにおける脆弱性対策の取り組みは、品質の考え方に同様に各工程で適切な対策を施すことが必要とされており、実装工程ではソースコードに対する脆弱性診断などの静的検証、検証工程では既知の脆弱性に対する「脆弱性スキャン」、未知の脆弱性に対する「ファジング」などの動的検証を実施することが効果的です。富士通コンピュータテクノロジーは、これらの検証を「脆弱性検証サービス」の各サービスメニューとして提供しています。

サービスメニュー

サービス	サービス概要
ソースコード検証サービス	ソースコードを解析してソースコード上の脆弱性の有無を確認できる静的解析ツールの導入～運用を支援します。お客様のご

	<p>要望によって静的解析をサービスとして提供、またCERT Cなどのセキュアコーディングガイドライン等への準拠状況確認や、解析で検出された指摘に対する修正要・不要を分析するなど付加価値の高いサービスを提供します。</p> <p>※組込みシステム（IoTデバイス）の開発に関わらず、アプリケーション開発～エンタープライズ向け開発まで幅広い分野、用途での適用実績があります。</p>
脆弱性スキャン適用サービス	<p>既知の脆弱性のパターンを使用し解析対象を攻撃することで、脆弱性の有無を確認するテスト（脆弱性スキャンテスト）をサービスとして提供します。</p>
ファジング適用サービス	<p>未知の脆弱性を検出させるために、ファズデータ等を活用して解析対象をテストするファジングツールの導入～運用、また必要に応じてファジングテストをサービスとして提供します。</p>
OSS脆弱性チェックサービス	<p>ソフトウェア開発に使用するOSS（オープンソースソフトウェア）や外部モジュールや、そこに含まれるソースコードまたはバイナリーから既知の脆弱性の有無を確認できるコンポジション解析ツールの導入～運用を支援します。</p> <p>※ソフトウェア開発全般に適用可能です。</p>

また、セキュアな組込みシステム開発は、上流工程から取り組むこと（セキュリティバイデザイン）が必要です。富士通グループ全体では、「脆弱性検証サービス」以外にも脆弱性対策に関連する様々なサービス等をご用意しています。当社のサービスのメニューに合致しないご要望であっても、可能な限りご対応させていただきます。

組込みシステム（IoT機器）の各工程と対応サービスの例



拡大イメージ

シノプシス社製品概要

- Black Duck®**
 ソースコードまたはバイナリーから、ソフトウェアで使用しているOSS（オープンソースソフトウェア）の一覧や、これらに含まれる既知の脆弱性やライセンス条件などを可視化するコンポジション解析ツールです。Black Duckは、専任のセキュリティチームの情報提供により、いち早く脆弱性の解析に結び付けることが可能です。
- Coverity®**
 ソースコードを解析し、信頼性やセキュリティ上の欠陥を検出する静的解析ツールです。Coverityは、ソースコードの網羅的な解析（プロシージャ間解析、パス解析）を特徴とし、人手のレビューでは見逃す可能性の高い欠陥を検出できます。また、自動車業界標準となっているMISRA、セキュアコーディングのCERT Cなど、コーディングルールの準拠状況を確認することも可能です。
- Defensics®**
 システムに対してファズデータ（予測不可能なデータ）を送信し、その応答を確認することで未知の脆弱性を確認するファジング（動的検証ツール）です。Defensicsは、OpenSSLの脆弱性であるHeartbleed（CVE-2014-0160）を発見したツールで、HTTP・Bluetooth・CANをはじめとするネットワークや外部インターフェース、またXML・オーディオファイルなどの外部ファイル入力など、組込み開発に必要な様々なプロトコルやファイルフォーマットをカバーしていることが特徴です。



Synopsys, Inc.は、半導体設計からソフトウェア開発に至るコンピュータの設計・製造・検証に関わる幅広い領域をカバーするソリューションを提供しています。特にEDA (Electric Design Automation) や半導体IP (Intellectual Property) の分野では、グローバル・リーディング・カンパニーとして長年の実績を持ち、近年ではセキュリティソリューション、ソフトウェア品質の分野でも業界をリードしています。ガードナー社のマジック・クアドラント評価では、アプリケーション・セキュリティ・テストの分野で2017年、2018年と2年連続でリーダーに指名されています。

関連ホームページ

 [脆弱性検証サービスのご紹介 \(パンフレット\)](#) (610 KB)

本件に関するお問い合わせ

以下のページよりお問い合わせください。

[ツール・サービスに関するお問い合わせ](#)

商標

- Coverity, Defensics, Black Duck, Synopsys, またはその他のシノプシス社製品の名称および製品名は、米国Synopsys社の、米国およびその他の国における登録商標または商標です。
- その他、記載されている製品名などの固有名詞は、各社の商標または登録商標です。

プレスリリースに記載されたサービスの内容、お問い合わせ先などは、発表日現在のものです。その後予告なしに変更されることがあります。あらかじめご了承ください。

[ページの先頭へ](#) 

プレスリリース

> 2018年

> 2017年

> 2016年

> 2015年

プレスリリース

2018年9月18日

株式会社富士通コンピュータテクノロジー

お問い合わせ

- [当社へのお問い合わせ](#)

カタログ一覧



このコンテンツについて

- [利用条件](#)
- [個人情報保護ポリシー](#)

～クラウドとエッジの連携で成長する組み込み専用のAI基盤～ Sensing Network Cognitive SDK Powered by Zinrai

株式会社富士通コンピュータテクノロジー（代表取締役社長：福元 芳朗、本社：川崎市中原区上小田中4-1-1）は、組み込み向けAI関連製品の開発者向けに、組み込み専用AI基盤「Sensing Network Cognitive SDK」を10月18日より販売開始します。

「Sensing Network Cognitive SDK」は、FUJITSU Human Centric AI Zinraiによる学習とエッジ端末での推論を連携させ、学習→推論→再学習を繰り返すことで、機器を変更することなく成長可能なAI基盤を提供します。

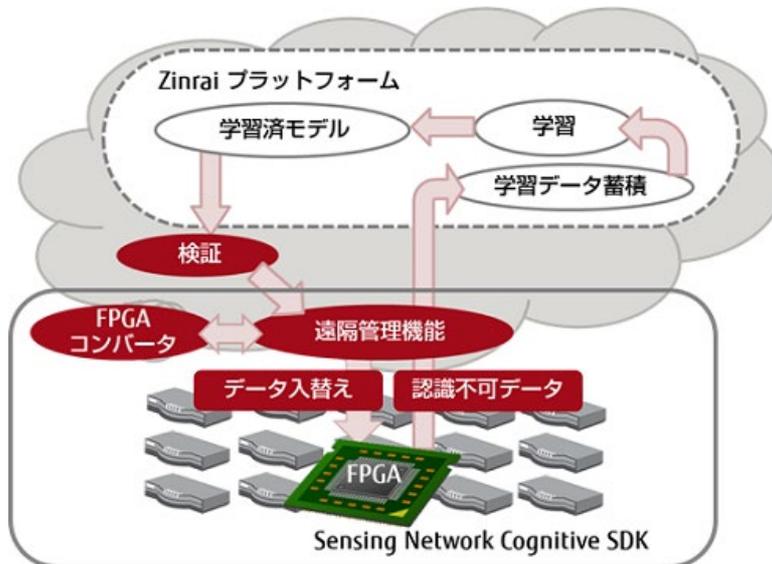
また、複数の異なる種類のエッジ端末に対応可能な「遠隔管理機能」により、学習済データの配信から適用までを管理し、AI基盤の運用・保守を飛躍的に効率化できます。

「Sensing Network Cognitive SDK」は、従来クラウドAIでの課題（オフライン時動作やリアルタイム性等）とエッジAIでの課題（安定した推論性能や省電力化など）を解決します。



商品の特長

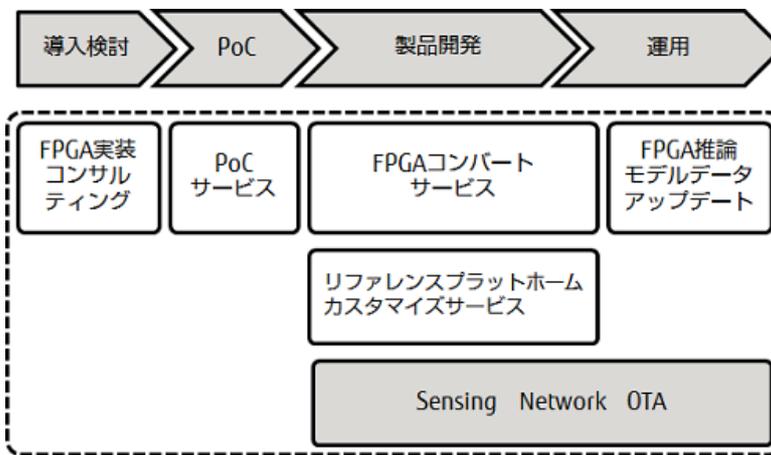
- 学習環境、エッジ端末遠隔管理、FPGAの推論回路および、これらの導入から運用までの支援を含めたソリューションサービスを提供します。
- 学習→推論→再学習を繰り返すことにより、より精度の高い学習済モデルに成長させることができます。



Sensing Network Cognitive SDKとその運用イメージ

お客様工程とサービス

お客様工程



「Sensing Network Cognitive SDK」は、図中にある5つのサービスと、Sensing Network OTA（別商品）で構成されています。

サービス

お客様に合わせて、それぞれのサービス内容を最適化して提供します。

サービス	説明
FPGA実装コンサルティング	推論回路の規模や速度見積り、FPGA選定を支援します。
PoCサービス	お客様に代わり、リファレンス環境で性能や回路規模の数値データを採取し、取得した数値データを提供します。
FPGAコンバートサービス	学習済ニューラルネットワークモデルから、ターゲットデバイスに対するFPGA回路データと推論ニューラルネットワークモデルデータを作成します。
FPGA推論モデルデータアップデート	お客様の「運用テスト～運用」フェーズをターゲットに、推論ニューラルネットワークモデルデータのアップデートを支援します。
リファレンスプラットフォームカスタマイズサービス	リファレンスプラットフォームをお客様のターゲットデバイス用にカスタマイズをします。

利用シーン例「画像認識エンジンや監視アプリケーションのFPGA化」

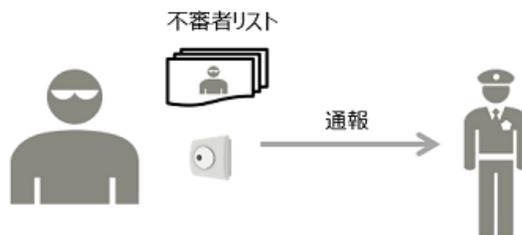
画像認識エンジンのFPGA化



カメラからの入力映像と学習済モデルの照合をFPGA化することで、オブジェクト認識を行う画像認識エンジンとして使用できます。

例えばデジタルサイネージに紐込み、年齢や性別を画像認識エンジンで識別し、その層にあった広告を表示するアプリケーションを作成することができます。画像エンジンの認識精度は、デジタルサイネージを見るごとに向上し、よりの確な広告を表示できるようになります。

監視アプリケーション



カメラに不審者を識別する画像エンジンをFPGA化して搭載することでリアルタイムに監視し、通報可能な防犯システムを作成することができます。また、不審者として通報しなくても良いものは、再学習することで精度が向上します。

関連ホームページ

- [「FUJITSU Emdedded System Sensing Network Cognitive SDK」紹介サイト](#)
- [「FUJITSU Human Centric AI Zinrai」紹介サイト](#)

製品・サービスに関するお問い合わせ

商品の詳細や価格については以下のページよりお問い合わせください。

[製品・サービスに関するお問い合わせ](#)

プレスリリースに記載された商品の内容、お問い合わせ先などは、発表日現在のものです。その後予告なしに変更されることがあります。あらかじめご了承ください。

[富士通ホームへ >>](#)

プレスリリース

> 2018年

> 2017年

> 2016年

> 2015年

プレスリリース

2018年5月28日

株式会社富士通コンピュータテクノロジー

お問い合わせ

- [当社へのお問い合わせ](#)

カタログ一覧



このコンテンツについて

- [利用条件](#)
- [個人情報保護ポリシー](#)

- GUI自動化・RPAツールの決定版 - RPAの導入をさらに簡単に運用を効果的に 「QualityPartner GENEST」のRPA機能強化版V2.0の販売を開始

株式会社富士通コンピュータテクノロジー（代表取締役社長：福元 芳朗、本社：川崎市中原区上小田中4-1-1）は、自社開発製品GUI自動化・RPAツールQualityPartner「GENEST（ジェネスト）」のRPA機能強化版V2.0を5月28日より販売開始します。

「GENEST」は直感的なキャプチャー&リプレイ機能を持ったGUI自動化・RPAツールです。文字認識技術や画像認識技術を使用しているため、人が目で見て操作するように画面を認識してマウスやキーボード操作を自動化します。初心者でも容易に操作手順をシナリオ化でき、ソフトウェアのテスト、キッティング、システム運用や事務作業まであらゆるシーンで活用できます。

V2.0ではフローチャート形式のシナリオ編集機能に対応しました。GUI画面から簡単な操作で繰り返し操作や分岐操作などのシナリオを作成し自動化することができます。また、RPAとして利用頻度の高いExcel操作やメール送信、スケジュール実行機能を追加しました。RPAの導入をさらに簡単に運用を効果的にします。

「GENEST」はICT業務のコスト・品質・納期の改善、生産性向上により「働き方改革」に貢献します。

*RPA (Robotic Process Automation)：ソフトウェアロボットによるパソコン定型業務の自動化

無料トライアルをご用意してありますので、まずはお試ください。

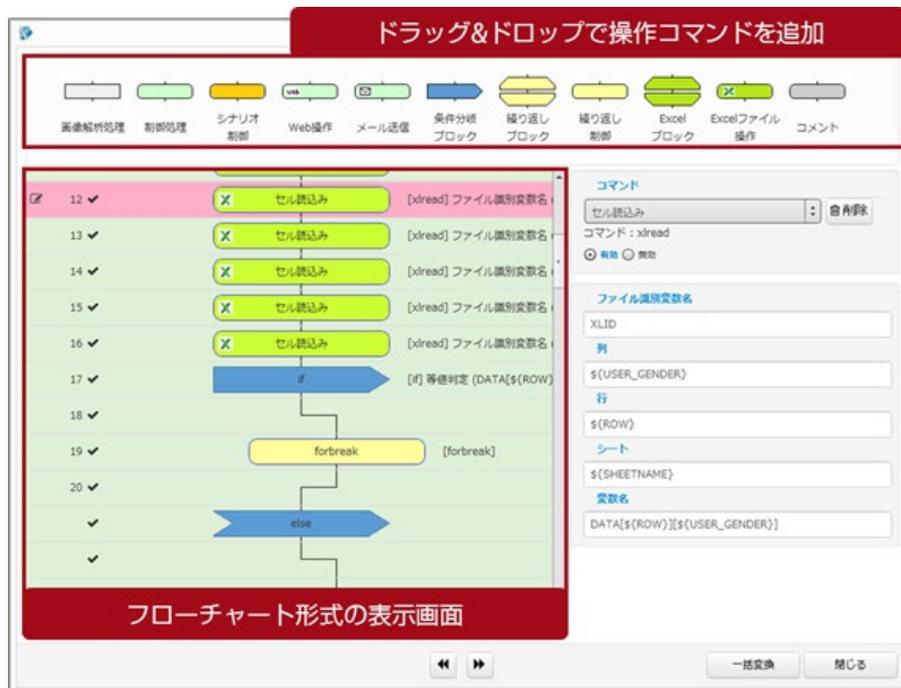
GUI自動化・RPAツール「GENEST」をお試ください！

製品・サービスに関するお問い合わせ

GENEST V2.0で追加・強化されたポイント

フローチャート形式のシナリオ編集画面でシナリオ作成がさらに簡単に

フローチャート形式のシナリオ編集機能に対応しました。
ドラッグ&ドロップ操作で簡単に操作コマンドの編集ができ、フローチャート形式のシナリオ編集画面により、繰り返し操作や分岐操作もわかりやすく表示されシナリオの構造が一目で把握できます。

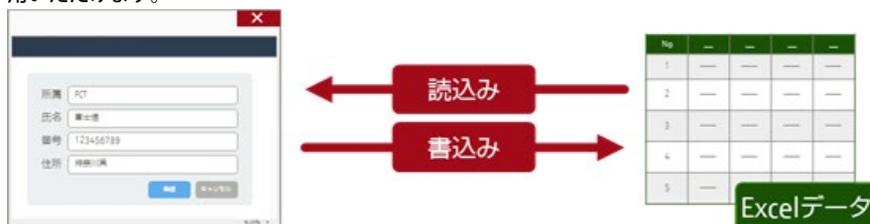


RPAで利用頻度の高い機能を追加

RPAで利用頻度の高いExcel操作やメール送信機能、スケジュール実行機能を強化しました。シナリオ編集機能で簡単な操作でシナリオに組み込むことができます。

- Excel操作

Excelファイルの指定されたセルの値をWeb画面の入力項目に入力するなど、Excelファイルの読み書きが自動化できます。進捗状況の出力や人事データの入力、帳簿の作成など様々な業務で活用いただけます。



- メール送信機能

送信に必要な設定をするだけでテンプレートを使ったメールやデータを添付したメールの送信が可能です。

実行中に出力されたデータを添付して通知するなど様々な用途で活用いただけます。



- スケジュール実行機能

「毎日9:00実行」、「毎週金曜日18:00実行」といった定期的な実行や、日時を指定した実行が可能なスケジュール実行機能を追加しました。

毎日繰り返す、売上げ実績データのダウンロードや伝票の登録など、定期作業で活用いただけます。

[関連ホームページ](#)

GUI自動化・RPAツールの決定版
ICT業務のコスト・品質・納期、生産性を大幅改善!!



[製品・サービスに関するお問い合わせ](#)

以下のページよりお問い合わせください。

製品・サービスに関するお問い合わせ

商標

- Microsoft、Windowsまたはその他のマイクロソフト製品の名称および製品名は、米国Microsoft Corporationの、米国およびその他の国における登録商標または商標です。
- その他、記載されている製品名などの固有名詞は、各社の商標または登録商標です。

プレスリリースに記載されたサービスの内容、お問い合わせ先などは、発表日現在のものです。その後予告なしに変更されることがあります。あらかじめご了承ください。

[ページの先頭へ](#) 

プレスリリース

> 2018年

> 2017年

> 2016年

> 2015年

プレスリリース

2018年1月22日

株式会社富士通コンピュータテクノロジー

MQTTプロトコルに対応した 「ソフトウェア脆弱性検証サービス」を提供開始

株式会社富士通コンピュータテクノロジー（代表取締役社長：福元 芳朗、本社：川崎市中原区上小田中4-1-1）は、2018年1月22日よりファジングツール(※)活用した未知の脆弱性を検出する「ソフトウェア脆弱性検証サービス」に、新たにIoT機器のプロトコルとして注目されているMQTT (Message Queue Telemetry Transport) への対応を追加したサービスの提供を開始いたします。

(※)株式会社富士通研究所の技術を活用しています。

お問い合わせ

- [当社へのお問い合わせ](#)

カタログ一覧



このコンテンツについて

- [利用条件](#)
- [個人情報保護ポリシー](#)

背景

IoT機器およびサービスでは、よりリソース制約の厳しいハードウェアやネットワーク環境で使用するための軽量のプロトコルとしてMQTTが注目されています。このような環境におけるセキュリティの担保（脆弱性の検証）を目的として、この度MQTTプロトコルに対応した「ソフトウェア脆弱性検証サービス」を提供します。

サービス内容

特長

- 実績豊富な独自のファジング技術で脆弱性をチェック
- 製品やソフトウェアを限定せずに実施
- 検出された問題をわかりやすくレポート
- 検出した「問題」の再現を支援

サービスメニュー

サービスメニュー	サービス概要
ファジング基本サービス	「テスト計画立案」、「ファジング実施」、「再現確認」、「結果報告」を実施する基本的なサービスです。ファジングの実施期間やファジングを実施するポート数によって価格が異なります。
ファジング再現支援／修正確認サービス	「ファジング基本サービス」で検出された問題の再現支援と修正を確認するサービスです。

※サービスの詳細、価格についてはお問い合わせください。

※サービス内容は改善などのため予告なく変更する場合があります。

※ファジングの実施はご都合にあわせてお客様先、または当社で実施いたします。

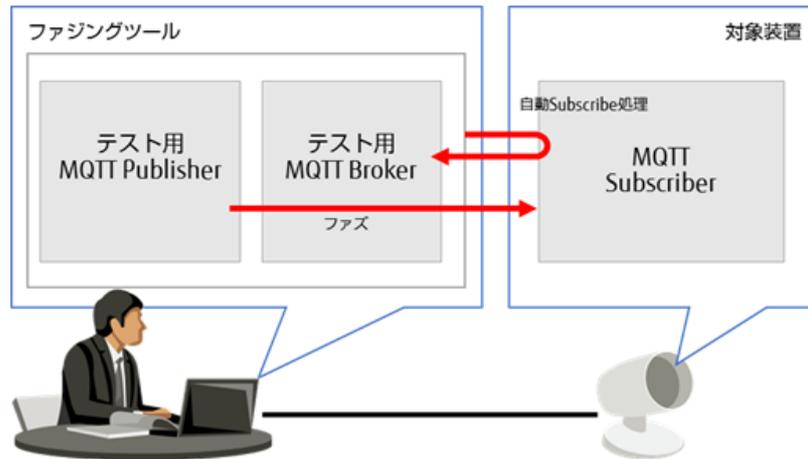
MQTTプロトコルに対応

特長

- TCP、UDP、SSL/TLSなどの代表的プロトコルに加え、新たにIoT機器等で広く利用されているMQTTプロトコルのファジングに対応
- MQTTクライアントに対するファジングを実現
- 独自の死活確認効率化技術によりファジングの高速実行を実現

検出事例

- IoT機器（MQTTクライアント）の脆弱性を検出



- 主な脆弱性の検出実績（IPA報告済み）
 - JVNDB-2017-000252
[MQTT.js における PUBLISH パケットの扱いに関する問題](#)

関連ホームページ

 [ソフトウェア脆弱性検証サービスのご紹介（パンフレット）](#) (204 KB)

本件に関するお問い合わせ

株式会社富士通コンピュータテクノロジーズ
「製品・サービスに関するお問い合わせフォーム」からお問い合わせください。

 [お問い合わせフォーム](#)

プレスリリースに記載されたサービスの内容、お問い合わせ先などは、発表日現在のものです。その後予告なしに変更されることがあります。あらかじめご了承ください。

[ページの先頭へ](#) 

プレスリリース

[> 2018年](#)[> 2017年](#)[> 2016年](#)[> 2015年](#)

プレスリリース

2017年

3月1日

- GUI自動化ツールの決定版 QualityPartner GENEST
[シナリオ作成・実行・確認機能を強化した「QualityPartner GENEST」を販売開始](#)

お問い合わせ

- [当社へのお問い合わせ](#)

カタログ一覧

[ページの先頭へ](#)

このコンテンツについて

- [利用条件](#)
- [個人情報保護ポリシー](#)

プレスリリース

> 2018年

> 2017年

> 2016年

> 2015年

プレスリリース

2017年3月1日

株式会社富士通コンピュータテクノロジー

- GUI自動化ツールの決定版 - シナリオ作成・実行・確認機能を強化した 「QualityPartner GENEST」を販売開始

株式会社富士通コンピュータテクノロジー（代表取締役社長：福元 芳朗、本社：川崎市中原区上小田中4-1-1）は、OCR解析技術やアイコン認識技術を使用したGUI自動化ツール「QualityPartner GENEST（ジェネスト）」のシナリオ作成・実行・確認機能を強化した製品を3月1日より販売開始します。

「GENEST」は直感的なキャプチャー&リプレイ機能を持ったGUI自動化ツールです。初心者でも容易に操作手順をシナリオ化できる上、マルチプラットフォームで「シナリオの再利用」が可能。定型作業やテストの効率化に貢献します。今回の改版ではサポートOSの追加に加え、コンバータ機能の強化やCLIによる自動化実行機能といったシナリオ作成・実行・確認機能の強化をしました。また、製品構成としてシナリオの実行と結果確認機能のみ利用できる低価格なランタイムライセンスをご用意いたしました。

従来の機能に加えて様々な新機能が利用いただけます。
無料トライアルをご用意しておりますのでまずはお試しください。

GUI自動化・RPAツール「GENEST」をお試しください！**製品・サービスに関するお問い合わせ**

お問い合わせ

- [当社へのお問い合わせ](#)

カタログ一覧



このコンテンツについて

- [利用条件](#)
- [個人情報保護ポリシー](#)

GUI自動化ツール「GENEST」の新機能

サポートOSの追加

サポートOSを追加しました。

- Microsoft® Windows® 8.1 (32/64bit)
- Microsoft® Windows® 10 (32/64bit)
- Microsoft® Windows Server® 2012R2

※詳細については「動作条件」を参照してください。

シナリオ編集機能（コンバータ）の強化

GENESTではアイコンやボタンなどを特定するために「ラベル」と呼ばれる文字列や画像を指定します。従来はクリックなど操作をさせたい文字列や画像の周囲を手動で囲んでラベルを指定する必要がありました。

今回の改版では、新機能の「なぞり&クリック選択」や「直接入力による検索」によって自動的にラベルの範囲が特定されるようになり、コンバータによるシナリオ編集がより簡単になりました。

- なぞり&クリック選択によるラベル指定
ラベルとして指定したい文字列や画像の中心部分をクリックすると自動的にラベルの範囲を特定します。

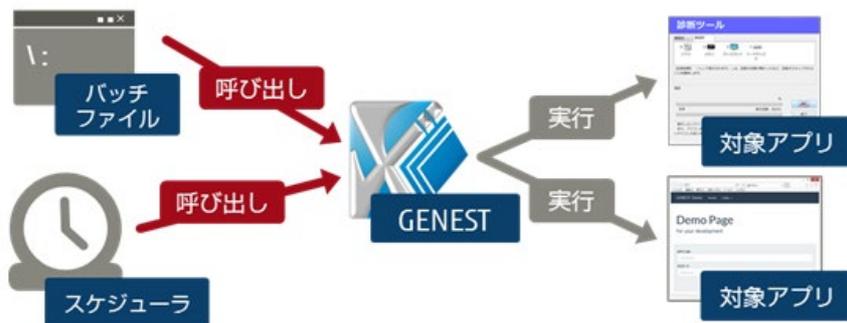


- 直接入力による検索でのラベル指定
ラベルとして指定したい文字列や画像データを入力し実行することで自動的にラベルの範囲を特定します。



CLIによる実行機能の追加

GENESTのGUI画面を表示せずにコマンドプロンプトから実行できるCLIモードを追加しました。従来はGENESTを起動させなければ自動化のシナリオを実行することしかできませんでしたが、今回の改版ではバッチファイルやスケジューラなどからGENESTを呼び出せるようになりました。バッチファイルやスケジューラとの連携により定時でのシナリオの実行やGENESTを実行スクリプトの一部として使用するなど運用の幅が広がりました。



レポート出力機能の追加

実行結果をもとに操作記録時、実行時のクリック位置などを表示したレポート出力機能を追加しました。

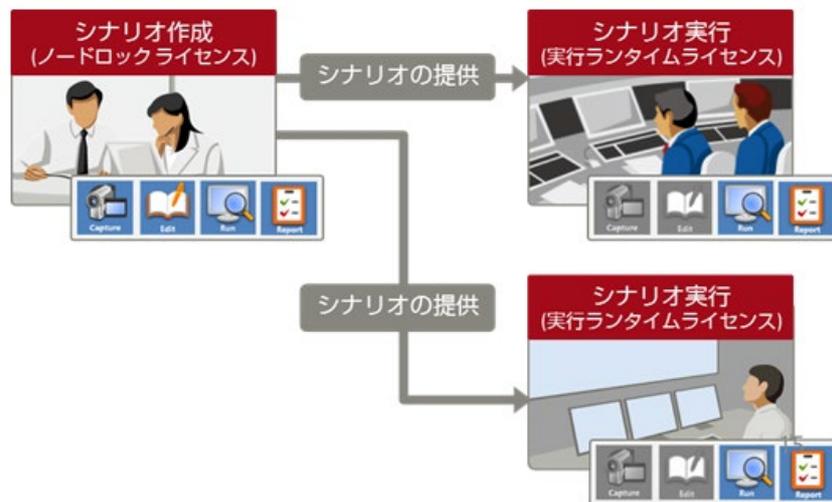
従来の実行結果よりも見やすく・分かりやすくなり、出力形式もExcel形式・HTML形式に対応しています。手順書や報告書などにも活用しやすくなりました。

項目	操作内容				テスト結果	エビデンス		実行時間						
	操作	ターゲット	値	ラベル		画像キャプチャ	実行画像キャプチャ							
1	クリック&文字入力	286,179	user	ユーザID	OK			0:00:03.089						
2	クリック&文字入力					<table border="1"> <thead> <tr> <th colspan="2">エビデンス</th> </tr> <tr> <th>画像キャプチャ</th> <th>実行画像キャプチャ</th> </tr> </thead> <tbody> <tr> <td>ユーザID (*必須)</td> <td>ユーザID (*必須)</td> </tr> </tbody> </table>		エビデンス		画像キャプチャ	実行画像キャプチャ	ユーザID (*必須)	ユーザID (*必須)	
エビデンス														
画像キャプチャ	実行画像キャプチャ													
ユーザID (*必須)	ユーザID (*必須)													
3	クリック													

ノードロック 実行ランタイムライセンスをサポート

実行・結果確認のみに対応した低価格なランタイムライセンスをサポート

従来のノードロック ライセンスに加えて、実行・結果確認のみに対応したランタイム ライセンスをご用意しました。「作成したシナリオを複数の端末で実行させたい」など実行環境が複数ある場合にお得なライセンスです。ランタイムライセンスを利用することでGENESTの利用の幅が広がります。



商品名	型番
ノードロック ライセンス (操作記録、シナリオ編集、実行、結果確認機能)	<ul style="list-style-type: none"> ライセンス期間：年間/半年/3ヶ月間（3ヶ月以上であれば月単位で期間設定可能） ライセンス費用には、プログラムの保守（マイナーアップデート）費用も含まれます
ノードロック 実行ランタイムライセンス (実行、結果確認機能)	

- ライセンスの購入方法、価格については、お問い合わせください。
- 「ノードロック 実行ランタイムライセンス（実行、結果確認機能）」は、シナリオの作成/編集機能をサポートしていません。操作記録、シナリオ編集には「ノードロック ライセンス」が必要になります。
- 詳細については「製品構成」を参照してください。

関連ホームページ

GUI自動化・RPAツールの決定版
ICT業務のコスト・品質・納期、生産性を大幅改善!!

製品・サービスに関するお問合せ

以下のページよりお問い合わせください。

商標について

- Microsoft、Windowsまたはその他のマイクロソフト製品の名称および製品名は、米国Microsoft Corporationの、米国およびその他の国における登録商標または商標です。
- その他、記載されている製品名などの固有名詞は、各社の商標または登録商標です。

プレスリリースに記載された商品の内容、お問い合わせ先などは、発表日現在のものです。その後予告なしに変更されることがあります。あらかじめご了承ください。

[ページの先頭へ](#) 

プレスリリース

[> 2018年](#)[> 2017年](#)[> 2016年](#)[> 2015年](#)

プレスリリース

2016年

11月1日

- [未知の脆弱性を検出する「ソフトウェア脆弱性検証サービス」を提供開始](#)

7月29日

- FUJITSU RFID・センサーソリューション EyeExpert
[視線検出システム「EyeExpert」を機能強化し、販売を開始](#)

お問い合わせ

- [当社へのお問い合わせ](#)

カタログ一覧



このコンテンツについて

- [利用条件](#)
- [個人情報保護ポリシー](#)

[ページの先頭へ](#)

プレスリリース

2018年

2017年

2016年

2015年

プレスリリース

2016年11月1日

株式会社富士通コンピュータテクノロジー

未知の脆弱性を検出する
「ソフトウェア脆弱性検証サービス」を提供開始

株式会社富士通コンピュータテクノロジー（代表取締役社長：福元 芳朗、本社：川崎市中原区上小田中4-1-1）は、2016年11月1日より未知の脆弱性を検出する「ソフトウェア脆弱性検証サービス」の提供を開始いたします。

製品開発におけるセキュリティへの対応は今や最重要課題です。サイバー攻撃の多くは製品の脆弱性を狙ったものであり製品開発段階での対応が必要です。本サービスは独自のファジング技術(※)と当社が40年以上に渡って培ってきた検証技術をベースにファジングを実施するサービスです。ファジングの実施により未知の脆弱性を事前に検出・対応することでセキュリティのリスクを低減することができます。(※)本ファジングは株式会社富士通研究所の技術を活用しています。

お問い合わせ

- 当社へのお問い合わせ

カタログ一覧



このコンテンツについて

- 利用条件
- 個人情報保護ポリシー

背景

近年、IoTの普及に伴いサイバー攻撃のリスクは増し続け、お客様へ提供する「課題」としても、経営上の「課題」としてもセキュリティ対策が重要になっています。

ファジングは実際にサイバー攻撃を仕掛ける攻撃者と同じように「ファズ」とよばれるデータを大量に送り応答や挙動を検証する手法です。特に未知の脆弱性を検知する技術として注目が高まっています。ファジングの導入によってソフトウェアの脆弱性を事前に検出・事前に対応することによってセキュリティのリスクを低減することができ、また開発プロセスに組み込むことで継続的な品質確保にもつながります。

セキュリティの「課題」、「品質」の確保について当社が培ってきた検証技術を生かして、「ソフトウェア脆弱性検証サービス」を提供いたします。

サービス内容

特長

- 実績豊富な独自のファジング技術で脆弱性をチェック
- 製品やソフトウェアを限定せずに実施
- 検出された問題をわかりやすくレポート
- 検出した「問題」の再現を支援

サービスメニュー

サービスメニュー	サービス概要
ファジング 基本サービス	「テスト計画立案」、「ファジング実施」、「再現確認」、「結果報告」を実施する基本的なサービスです。 ファジングの実施期間やファジングを実施するポート数によって価格が異なります。
ファジング 再現支援／修正確認 サービス	「ファジング基本サービス」で検出された問題の再現支援と修正を確認するサービスです。

※サービスの詳細、価格についてはお問い合わせください。

※サービス内容は改善などのため予告なく変更する場合があります。

※ファジングの実施はご都合にあわせてお客様先、または当社で実施いたします。

独自のファジング技術

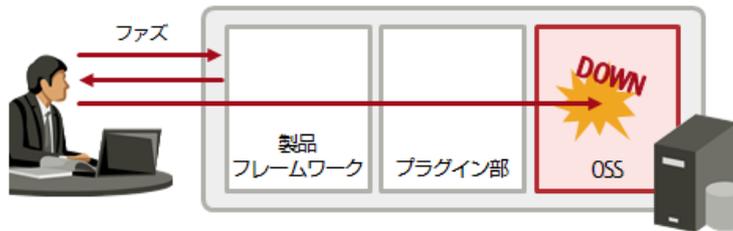
特長

- TCP、UDP、SSL/TLSなどの代表的プロトコルに対応
- 独自の解析技術によって製品固有のプロトコルに対応
- 並列実行によるファジングの高速実行を実現

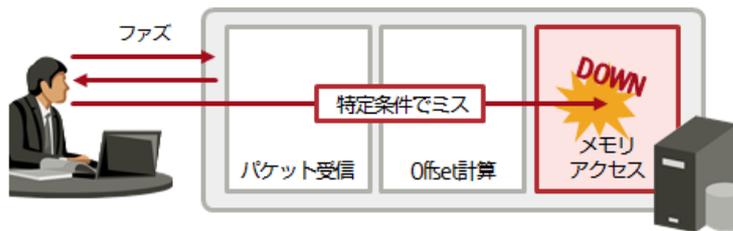
※ファズ：ランダムなデータや正常なパケットを変異させて生成した予測不可能な入力データ

検出事例

- 製品内部で使用していたOSSの脆弱性を検出



- ネットワーク・パケットの扱いに対する脆弱性を検出



- 主な脆弱性の検出実績（IPA報告済）
 - JVNDB-2011-000092：
無線LAN機器におけるバッファオーバーフローの脆弱性を検出
 - JVNDB-2013-000017：
ネットワークSWにおけるサービス運用妨害(DoS)の脆弱性を検出
 - JVNDB-2013-000019：
組込みOSのSSHサーバにおけるサービス運用妨害(DoS)の脆弱性を検出
 - JVNDB-2013-000023：
組込みOSのWebサーバにおけるサービス運用妨害(DoS)の脆弱性を検出

関連ホームページ

 [ソフトウェア脆弱性検証サービスのご紹介（パンフレット）](#) (204 KB)

本件に関するお問い合わせ

株式会社富士通コンピュータテクノロジーズ
「製品・サービスに関するお問い合わせフォーム」からお問い合わせください。

 [お問い合わせフォーム](#)

プレスリリースに記載されたサービスの内容、お問い合わせ先などは、発表日現在のものです。その後予告なしに変更されることがあります。あらかじめご了承ください。

[ページの先頭へ](#) 

プレスリリース

> 2018年

> 2017年

> 2016年

> 2015年

プレスリリース

2016年7月29日

株式会社富士通コンピュータテクノロジー

視線検出システム「EyeExpert」を機能強化し、販売を開始

株式会社富士通コンピュータテクノロジー（代表取締役社長：福元 芳朗、本社：川崎市中原区上小田中4-1-1）は、7月29日、視線検出技術を用いた視線検出システム「Eye Expert」の機能を強化した製品の販売を開始しました。本視線検出システムは、小型視線センサーと制御ソフトウェアからなり、今まで容易には得ることの出来なかった人の視線位置（見ている場所）を非接触で検知しデータとして蓄積することが可能です。例えば、小型視線センサーを店舗に設置し収集したデータを分析することで陳列改善や商品開発などマーケティングに活用することができます。

新機能として、他のアプリケーションとの連携を可能にするAPIのサポート、視線データを見やすく可視化するツール、視線データ精度を高めるキャリブレーション機能（個人を特定できる用途に限る）をサポートし、お客様の多様なニーズに合わせた活用が可能となりました。また、費用を抑えたトライアルでのご利用など、用途に合わせてセンサー数、ライセンス期間を選べる商品をご用意しました。

お問い合わせ

• [当社へのお問い合わせ](#)

カタログ一覧



このコンテンツについて

• [利用条件](#)
• [個人情報保護ポリシー](#)

視線検出システム「EyeExpert」の新機能

従来の機能（視線検出・データ蓄積）に加えて以下の機能がご利用頂けます。

1. 他のアプリケーションとの連携を可能にするAPI (EyeExpert API)

本APIを使用することで、EyeExpertが出力する視線データをリアルタイムに取得することができ、見ている場所に応じてアクションを起こすといったアプリケーションの開発が容易になります。

活用例：

- お客様の興味に応じたプロモーション
- 見落とし時のアラーム通知
- 視線を用いたユーザーインターフェース



2. 視線データを可視化するツール (EyeExpert Utility)

本ツールを使用することで、EyeExpertが出力した視線データを様々な形式で容易に可視化/出力できます。視線データの解析等にご活用いただけます。

- 統計表示
視線のデータ量を時系列でグラフ化します。
- マッピング表示
視線データの分布状況を画像上（※1）に重畳させ可視化します。
【ヒートマップ】
視線データの集中度に応じて7色で表現
【フォーカスマップ】
視線データの集中度に応じて黒の透過度で表現



例：ヒートマップ

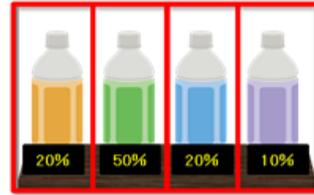
- スキャンパス表示
視線の軌跡を画像上（※1）に重畳させ可視化しま

す。



例：スキャンパス

- 。エリアカウント表示
視線検出エリア内の視線のデータ量の割合を画像上
(※1) に数値で可視化します。



※1 画像とは、視線検出する対象物を撮影した静止画

例：エリアカウント

- 3. 個人ごとの検出誤差を軽減するキャリブレーション機能
視線検出時の個人差を補正し、視線の検出精度をより高める機能です。個人を特定できるシチュエーションでご使用いただくことを想定しています。

商品構成

商品名	型番	内容
製品	EyeExpert視線検出基盤	EE-0001 視線センサー 4個、および制御ソフトウェア
	(新規)	EE-0002 視線センサー 1個、および制御ソフトウェア
ライセンス	EyeExpertデータ出力ライセンス (※2)	EE-L001 視線検出基盤の1年ライセンス
	(新規)	EE-L002 視線検出基盤の3ヶ月ライセンス
	(新規)	EE-L003 視線検出基盤の3年ライセンス
サービス	EyeExpert導入支援サービス	EE-S001 お客様に代わり、EyeExpert製品のインストール、視線センサーの設置、動作確認を実施し、操作説明を行います。 経験豊富な技術者が作業を行いますので視線データの収集をスムーズに開始することができます。
	EyeExpert移設サービス	EE-S003 お客様に代わり、視線センサーの移設、動作確認を実施します。 経験豊富な技術者が作業を行います。
	EyeExpertカスタマイズサービス	個別 製品をお使いいただく上でのお客様固有のご要望に対応します。対応内容は個別に相談させていただきます。 (例：お客様専用ソフトウェアの開発)
保守	EyeExpert保守サポート	EE-M001 EyeExpert視線検出基盤に関するQAサポート (1年契約)

※2 EyeExpertの導入において必ずご利用いただく必要があります。1ライセンスにつき、視線センサーを最大4個までお使い頂けます。

製品・ライセンス・サービス、保守の購入方法、価格についてはお問い合わせください。

販売目標

2017年度末までに300システムの販売を目標としています。

関連ホームページ

以下の当社ホームページにて製品をご紹介します。

<http://www.fujitsu.com/jp/group/fct/products/eyeexpert/index.html>

製品・サービスに関するお問合せ

以下のページよりお問い合わせください。

<http://www.fujitsu.com/jp/group/fct/contact/index.html/>

商標について

- 記載されている製品名などの固有名詞は、各社の商標または登録商標です。

プレスリリースに記載された商品の内容、お問い合わせ先などは、発表日現在のものです。その後予告なしに変更されることがあります。あらかじめご了承ください。

[ページの先頭へ](#) 