MITSUBISHI ELECTRIC
Changes for the Better

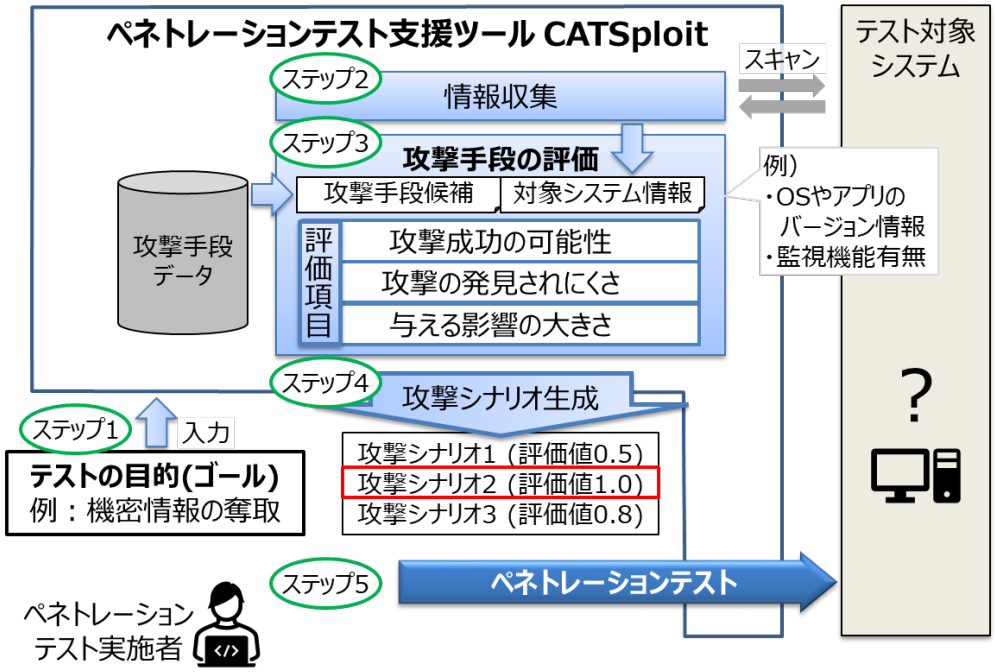
NEWS RELEASE

（開発 No.2316）

2023 年 12 月 5 日
三菱電機株式会社

世界初、ハッカー視点で攻撃シナリオを自動生成するペネトレーションテスト支援ツールを開発

ネットワークに繋がるあらゆる製品のサイバー攻撃耐性向上に貢献



ペネトレーションテスト実施時における支援ツールの活用イメージ

三菱電機株式会社は、ホワイトハッカー※1 視点で、機密情報の奪取可否確認などペネトレーションテスト※2 の目的に応じた攻撃シナリオを自動生成し、その有効性に評価値を付けて提案するペネトレーションテスト支援ツール「CATSploit（キャッツプロイト）」を世界で初めて※3 開発しました。本ツールで生成された攻撃シナリオをペネトレーションテストに活用することで、高度な専門知識を持っていないセキュリティーエンジニアでも容易にテストを実施することが可能となります。

近年、AI やデータ利活用の進展により、社会インフラや工場機器などの制御システムがネットワークに接続されるようになり、制御システムを狙ったサイバー攻撃のリスクが高まっています。サイバー攻撃を受けると、停電や公共交通機関の運行停止など社会インフラの停止に繋がる恐れがあることから、制御システムにおけるセキュリティー対策は急務です。また、ISA/IEC 62443※4 では、システムや機器が受けるサイバー攻撃や実装・設定上のミスに起因する脆弱性への対策として、ファジングテスト※5 やペネトレーションテストなどのセキュリティーテストを実施することを要求しています。しかし、ペネトレーションテストは、ホワイトハッカーが実際にシステムや製品を攻撃することで脆弱性の有無を確認する試験であり、高度な専門知識が必要となることに加えて、ホワイトハッカーが希少な人材であるため、容易に実施できないという課題がありました。

当社は今回、ホワイトハッカーがテスト対象のシステムや製品に対して「攻撃成功の可能性」、「攻撃の発見されにくさ」、「与える影響の大きさ」の視点で手段を選択して攻撃を仕掛けている点に着目しました。この特徴を用いて、攻撃シナリオを選択するために各攻撃手段の有効性を表す評価値が一覧で表示されるペネトレーションテスト支援ツールを開発しました。

本開発成果の詳細は、ロンドンで 12 月 6 日から 7 日まで開催される「Black Hat Europe 2023 Arsenal」で、12 月 6 日（現地時間 11 時）に発表する予定です。

※1　コンピューターなどに関する高度な知識や技術を、善良な目的のために活用するハッカー
※2　システムや装置に対して実際に攻撃を行い、侵入など不正アクセスができるか確認するテスト
※3　2023 年 12 月 5 日時点、当社調べ
※4　産業用制御システム向けのセキュリティーに関する標準規格
※5　ソフトウエアに無効・不正な入力を与えることで、ソフトウエアの欠陥や脆弱性を発見するテスト手法

開発ツールの特長

1. ホワイトハッカー視点で、攻撃シナリオを自動生成

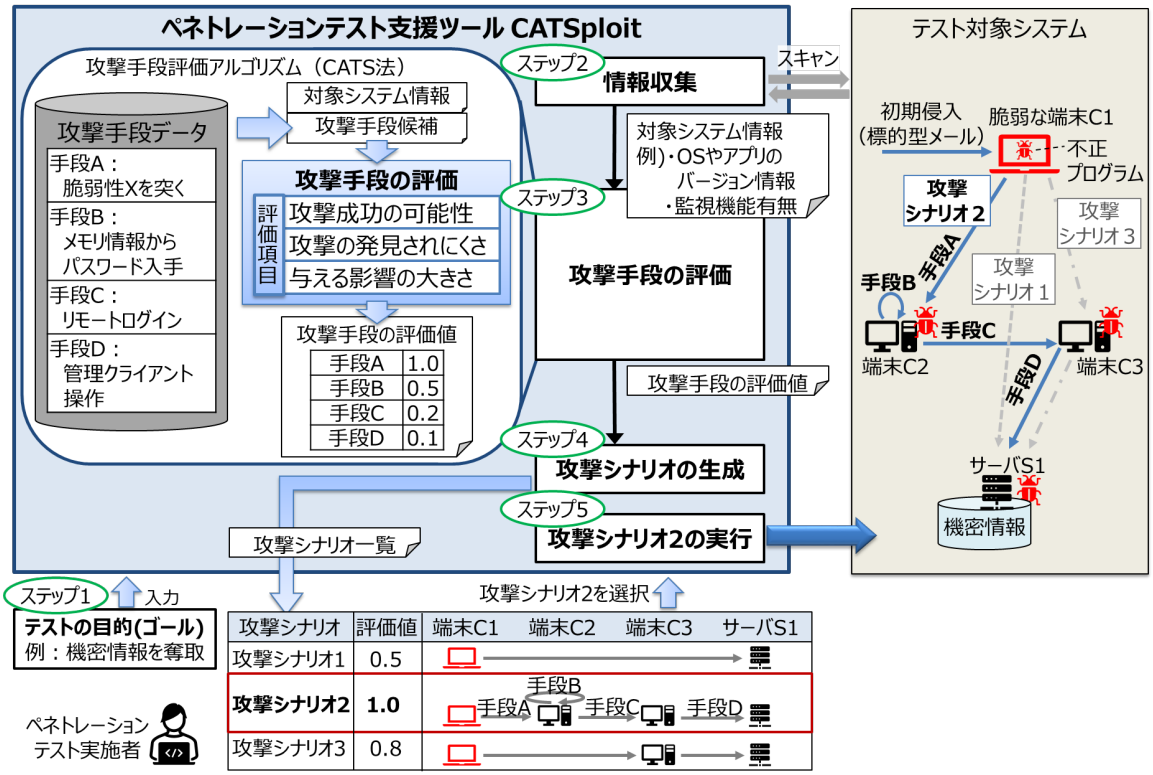
・ホワイトハッカーが攻撃手段を選択する際に「攻撃成功の可能性」、「攻撃の発見されにくさ」、「与える影響の大きさ」を意識することに着目。テストの目的を入力することで、目的達成のために必要な攻撃手段の実施手順を示した攻撃シナリオを自動で生成

2. ホワイトハッカー視点で攻撃シナリオの有効性を評価することで、最適なペネトレーションテストが容易に実施可能

・当社独自の CATS 法※6 の採用により、ホワイトハッカー視点で各攻撃手段の有効性を表す評価値を算出、攻撃シナリオを一覧で提示することで評価値の高い攻撃シナリオの選択が可能

・評価時には OS やアプリケーションのバージョン、セキュリティー監視機器の有無に関するシステム情報だけでなく、不足するシステム情報も考慮して評価値に反映することで攻撃者の視点により近い評価を実現

・自動でホワイトハッカー視点での評価を可能にしたことで、高度な専門知識を持っていないセキュリティーエンジニアでも容易にペネトレーションテストを実施することが可能



ペネトレーションテスト支援ツール「CATSploit」の仕組み概要

今後の予定・将来展望

当社が開発するシステムや機器のサイバー攻撃耐性の向上に向けて、今回開発したツールのさらなる研究開発および有効性評価を進め、2026 年を目標に当社製品のセキュリティー試験への適用を目指します。

お問い合わせ先

＜報道関係からのお問い合わせ先＞
三菱電機株式会社　広報部
〒100-8310 東京都千代田区丸の内二丁目 7 番 3 号
TEL 03-3218-2332　FAX 03-3218-2431

＜お客様からのお問い合わせ先＞
三菱電機株式会社　情報技術総合研究所
〒247-8501 神奈川県鎌倉市大船五丁目 1 番 1 号
https://www.MitsubishiElectric.co.jp/corporate/randd/inquiry/index_it.html

※6　当社が開発した攻撃手段の有効性を評価する手法。Cyber Attack Techniques Scoring の略