

2026 年 10 月 2 日

NTT ドコモビジネス株式会社

Powder Keg Technologies 株式会社

NTT ドコモビジネスと Powder Keg Technologies、 AI を活用し OT 環境の資産可視化から攻撃リスクの検証までを自動化するシステムを 開発

～継続的脅威エクスポーチャー管理(CTEM)により OT セキュリティ運用を高度化～

NTT ドコモビジネス株式会社(旧 NTT コミュニケーションズ株式会社、以下 NTT ドコモビジネス)と Powder Keg Technologies 株式会社(以下 PKT)は、NTT ドコモビジネスの OT システム向け IDS^{※1}「OsecT(オーセクト)^{※2}」と PKT の自律型ペネトレーションテストツール^{※3}「MUSHIKAGO^{※4}」を統合し、AI 技術を取り入れて OT 環境の資産可視化から攻撃リスクの検証までを自動化するシステム(以下本システム)を開発しました。これにより、工場やプラントなどの設備を制御・運用する OT 環境において、継続的脅威エクスポーチャー管理(CTEM)^{※5}を実現し、サイバーリスクを継続的に可視化・評価し、優先度に応じた対策を支援します。

1. 背景

近年、工場のスマート化や社会インフラにおける IoT やフィジカル AI の活用が進む一方で、OT 環境を標的としたランサムウェアなどの高度なサイバー攻撃が急増しており、継続的なリスク管理が急務となっています。しかし、OT 環境では管理対象機器の増加による資産管理の複雑化に加え、システムの安定稼働を優先する必要があるため、高負荷なアクティブスキャン^{※6}を使った脆弱性検査が難しいといった課題が存在します。そのため、パッシブスキャン^{※7}による脆弱性の検知漏れや、実環境における攻撃リスクの検証を踏まえたリスク評価や優先度付けが困難となっています。さらに、セキュリティ人材の不足により、継続的なセキュリティ運用の負担も増大しています。

2. 本システムの概要

本システムは、OT 環境において、AI の高度な推論・自律処理能力を活用することで、資産可視化、脆弱性検知、攻撃の検証、リスク評価までを一気通貫で自動化できるものです。

両社は共同開発により、OsecT の OT 環境内における資産や脆弱性の「可視化・検知」と MUSHIKAGO の攻撃経路やリスクに対する「安全な自律検証」を融合させ、近年サイバーリスク管理で重要性が高まる継続的脅威エクスポーチャー管理(CTEM)を OT 環境で実現しました。本システムの特長は、以下のとおりです。

(1) 大規模な OT 資産の自動可視化

工場やプラントなどに配置された機器をネットワークに接続するだけで、大規模な OT ネットワーク内に存在する機器を漏れなく自動検出します。管理者が把握しきれていない機器を含む OT 資産を毎日自動で可視化し、管理の抜け漏れを防ぎます。

(2) 可用性に配慮したアクティブスキャンによる脆弱性の特定

正規の読み取り専用コマンドを用いてアクティブスキャンを行うことで、OT 環境の可用性を低下させることなく、機種やファームウェアを特定します。機種やファームウェアの情報から機器に含まれる脆弱性を検知することが可能となります。推定ではなく確実な情報収集により、脆弱性の検知漏れを改善します。

(3) ペネトレーションテストまでの完全自動化

AI 技術を活用し、「資産の可視化 → 脆弱性の検出・管理 → ペネトレーションテスト」のプロセスを一気通貫で自動実行します。高度な専門知識を持つセキュリティ人材が現場に不足している場合でも、実用的なセキュリティ検証が運用可能です。

(4) 実環境に基づくリスクの優先度付け

単に脆弱性を網羅的に羅列するのではなく、詳細なセキュリティテストを通じて設定不備や実際の攻撃成立の可能性を検証し、現場で優先的に対応・修正すべきセキュリティリスクを明確に提示します。

3. 今後の展開

NTT ドコモビジネスと PKT は、2026 年度中を目途に、本システムを製造業や社会インフラを担う事業者向けの法人向けソリューションとして提供を開始します。将来的には、NTT ドコモビジネスが提供するネットワークサービスへのセキュリティ機能としての組み込みを視野に入れ、安全な産業の DX 実現に貢献します。

4. NTT docomo Business Forum'26 出展情報

2026 年 10 月 8 日(木)～9 日(金)に開催する「NTT docomo Business Forum'26」にて、本システムに関するデモ展示を行う予定です。詳細は、公式 Web サイトの展示情報よりご確認ください。

公式 Web サイト : <https://www.ntt.com/business/go-event.html?ir=nr>

■展示名：海外拠点の OT セキュリティー元監視

■展示番号：GD-04

*会場：[ザ・プリンス パークタワー東京 B2 フロア](#)

* 日時 : 2026 年 10 月 8 日(木)~9 日(金) 9:30~17:30

* 参加方法 : 完全招待制

* 参加費用 : 無料

「NTT コミュニケーションズ株式会社」は 2025 年 7 月 1 日に社名を「NTT ドコモビジネス株式会社」に変更しました。私たちは、企業と地域が持続的に成長できる自律・分散・協調型社会を支える「産業・地域 AX のプラットフォーム」として、新たな価値を生み出し、豊かな社会の実現をめざします。

つながろう。驚きを。幸せを。



<https://www.ntt.com/about-us/strategy.html>

- ※1 : IDS とは、Intrusion Detection System(侵入検知システム)の略で、ネットワークやシステムへの不正アクセスや攻撃をリアルタイムで検知し、警告を発するセキュリティ技術です。
- ※2 : OsecT(オーセクト)とは、工場の生産ラインなどを支える制御システムのセキュリティリスクを可視化・検知する NTT ドコモビジネスが提供するサービスです。
- ※3 : ペネトレーションテストとは、実際の攻撃者と同じ手法を用いてシステムやネットワークへの侵入を試し、セキュリティ対策の有効性を検証するテスト手法です。
- ※4 : MUSHIKAGO とは、閉域・OT 環境を含むネットワーク上のあらゆる資産(PC、IoT 機器、プリンターなど)を AI で可視化し、ペネトレーションテストまで一気通貫で実施する Powder Keg Technologies 株式会社の国産セキュリティ製品です。
- ※5 : 継続的脅威エクスポージャー管理(CTEM)とは、企業や組織に存在するサイバー攻撃の対象領域とリスク(エクスポージャー)を攻撃者視点で継続的に発見・評価・検証・改善するためのセキュリティ対策管理手法です。
- ※6 : アクティブスキャンとは、ネットワーク上のシステムや機器に対して、診断ツールから直接パケットやコマンドを送信し、その応答内容を分析することで、機器の状態や脆弱性を調査する手法です。
- ※7 : パッシブスキャンとは、通信の受動的な監視のことで、ネットワーク機器においてミラーリングと呼ばれる機能により転送パケットをコピーし、外付けの監視機器で監視する方式です。