NTT AT

News Release

2025年10月23日
NTTアドバンステクノロジ株式会社

AI技術によりアタックサーフェスのリスク管理を効率化する「XCockpit EASM」と「XCockpit IASM」を提供開始
～外部と内部のリスクを可視化し管理することでインシデントの予防策を高度化～

NTTアドバンステクノロジ株式会社（以下：NTT-AT、本社：東京都新宿区、代表取締役社長：伊東匡）は、AI技術を活用して攻撃者に利用される可能性のあるリスクを洗い出し、管理する「XCockpit EASM」および「XCockpit IASM」サービス（以下：本サービス）を2025年10月23日から提供開始します。

本サービスは、台湾において先進的なAI技術で高い評価を得ているセキュリティベンダーCyCraft（サイクラフト）の製品を日本向けのサービスとしてパッケージングしたものです。NTT-ATは2024年5月、CyCraftの日本法人である、株式会社CyCraft Japan（所在地：東京都千代田区、代表取締役社長：ベンソン・ウー）との間で協業契約を締結しました。

サイバー攻撃の高度化が進み、防御策をすり抜けて侵入してくる脅威が増えるなか、NTT-ATは、実績あるAI技術を活用した本サービスの提供により、外部に漏洩したIDなどの情報資産やID管理におけるActiveDirectry[*1]に起因するリスクを洗い出してランク付けを実施し、セキュリティ運用の効率化・高度化を支援します。

1. 背景

昨今のセキュリティインシデント規模拡大の要因のひとつに、近年のDX（デジタルトランスフォーメーション）化の進展に伴う攻撃対象の拡大による公開情報や他のサービスからの漏洩情報などをつかみ切れていない企業の状況が挙げられます。

このような状況に対しては、本サービスの「XCockpit EASM」の導入により、情報の把握と対処のサイクルを回すことでセキュリティレベルの向上が期待できます。また、漏洩したID情報を使った侵入が増加しており、このIDを管理しているActiveDirectory設定の不備が感染拡大の一因となっています。これに対しては、「XCockpit IASM」によるリスク管理および可視化と脆弱箇所の特定による効果的な対策が実施可能です。

2. 本サービスの概要・特長

本サービスで活用するCyCraftの技術は、組織外部に漏洩したID情報や内部のIDおよび構成情報に対してAI技術を適用することで、リスクごとに脅威レベルを付加し、ハッカー観点での攻撃のしやすさに基づく優先度付けを行うため、運用者は専門の分析官なしでも効果的なアタックサーフェスマネジメント[*2]が実施可能です。

NTT-ATは、導入の支援（オプションサービス）やセキュリティ対応の実績を活かしたレポート内容の解説、報告会などをCyCraftの技術に加えて、本サービスとしてパッケージングすることで、日本のお

客さまのニーズに対応したサイバーセキュリティ対策を提供します。
本サービスには次のような特長があります。

(1)「XCockpit EASM」の特長

①外部に漏洩したIDや管理できていない資産に関するリスクを洗い出します。
通常の診断サービスは管理・把握している資産を対象に実施するものですが、本サービスは自社が管理上把握できていないインターネット上でアクセス可能な情報(サーバーなどの脆弱性、ドメインに関する付随情報、ダークWeb漏洩情報)を、攻撃者の視点で洗い出します。調査対象を自社だけでなくグループ企業・サプライチェーン対象企業などにも拡大可能です。

②AIがリスクを分析してレベル判定し、対策案まで提示します。
洗い出したリスクは攻撃の容易さや影響の大きさなど、さまざまな角度からAIが分析してレベル判定を実施し、これらのリスクを低減するための対策案を自然言語で提示します。

③検出したリスクをタスク化して管理し、対処までサポートします。
検出して評価されたリスクは「XCockpit EASM」の画面で一元化してタスクとして確認可能であり、対処状況を入力することで対処完了までの進捗管理が可能です。リスク検出から対処までのサイクルがワンストップ管理できるので、リスク残存防止や今後の類似リスクへの対応の迅速化や内容の向上が期待できます。

(2)「XCockpit IASM」の特長

①ActiveDirectoryに関する高度な専門知識を必要とせずにリスクを洗い出します。
ID管理の不備、グループに対する過大な権限設定、設定に関する脆弱性、ActiveDirectory特有の攻撃に対する防御策の不備などを洗い出します。

②AIがリスクを分析してレベル判定し、対策案まで提示します。
Windowsの管理機能で確認可能な設定を分析し、あるアカウントからシステムを侵害可能なAttackPathを生成します。また、これらのリスクを低減するための対策案をAIが自然言語を用いて提示します。

③検出したリスクをタスク化して管理し、対処までサポートします。
検出して評価されたリスクは「XCockpit IASM」の画面で一元化してタスクとして確認可能であり、対処状況を入力することで対処完了までの進捗管理が可能です。リスク検出から対処までのサイクルがワンストップ管理できるので、リスク残存防止や今後の類似リスクへの対応の迅速化や内容の向上が期待できます。

3. 対象のお客さまと主な効果

本サービスは、お客さまの規模やセキュリティ運用のレベルにかかわらずご利用いただけます。

4. 提供開始

2025年10月23日

5. 提供価格

ご利用や価格(お見積り)など詳細は、下記「お問い合わせ先」までご連絡ください。

6. 両社のコメント

このたびNTT-ATさまによる「XCockpit EASM」「XCockpit IASM」サービスの提供開始を心より歓迎いたします。

サイバー攻撃はますます巧妙化し、“見えにくいリスク”への対応が求められています。CyCraftのAIベースの技術を通じて、NTT-ATさまがお客さまに提供するセキュリティサービスの価値をさらに高めることができると確信しています。

今回の取組みを皮切りに、私たちはNTT-ATさまとともに、日本企業のセキュリティ運用を一層強化し、安心してデジタル化を進められる環境づくりに貢献してまいります。

CyCraft Japan
Country Manager
姜 尚郁 SANGWOOK KANG

昨今のサイバー攻撃は、システムの脆弱性を利用して侵入してくるものよりも、公開サーバーの設定不備や漏洩した認証情報を悪用するなど、企業が気づきにくい部分を悪用して侵入してくる傾向が顕著です。

今回提供を開始する2つのアタックサーフェスマネジメントサービスは、これまでお客さまが十分把握できていなかった外部に露出したリスクや、ID権限に関するリスクを継続的に洗い出して、攻撃者の目線で把握し、侵入や攻撃を未然に防ぐことを可能にするものになります。

本サービスをぜひご活用いただきたいと考えております。

NTTアドバンステクノロジ株式会社
取締役 ソーシャルプラットフォーム・ビジネス本部長
岡崎 義勝

■株式会社CyCraft Japanについて【https://cycraft.com/ja/】

CyCraftは、AIによる自動化技術を専門とするサイバーセキュリティ企業。
2017年に設立され、台湾に本社、日本とシンガポールに海外拠点を持つ。アジア太平洋地域の政府機関、警察・防衛機関、銀行、ハイテク製造業にサービスを提供し、日本においては東京都による中小企業情報セキュリティ強化プロジェクトの専属セキュリティプロバイダーとして2年連続で選定され、日本の中小企業数百社に自動化サイバーセキュリティソリューションを提供している。
CyCraftのAI技術と機械学習技術によるソリューションが評価され、CIDグループとテマセク・ホールディングス旗下のパビリオンキャピタルから強力なサポートを獲得し、また、国際的トップ研究機構であるGartner、IDC、Frost & Sullivanなどから複数の項目において評価を受けているほか、国内外の著名な賞をいくつも受賞している。

■NTTアドバンステクノロジ株式会社について【https://www.ntt-at.co.jp/】

NTTアドバンステクノロジ株式会社は、1976年の設立以来、NTTグループの技術的中核企業として、NTT研究所のネットワーク技術・メディア処理技術・日本語処理技術・環境技術・光デバイス・ナノデバイス技術などの多彩な先端技術のみならず、国内国外の先端技術を広く取入れ、それらを融合してお客さまの課題を解決し、お客さまにとっての価値を提供し続けています。

*1 ActiveDirectry：
Windowsサーバーに搭載されたディレクトリサービス機能のこと。企業内のユーザー情報やデバイス・アプリケーションなどのリソースを一元管理することで、効率的な業務運営を可能とする。
*2 アタックサーフェスマネジメント：
サイバー攻撃の対象となりうるIT資産を発見し、継続的にリスクの探索・評価を実施する活動およびサービスのこと。

■本件に関するお問い合わせ先
NTT アドバンステクノロジ株式会社
【商品に関するお問い合わせ先】
ソーシャルプラットフォーム・ビジネス本部
セキュリティビジネス部門 セキュリティ事業開拓担当
担当：上野、吉田

【報道関係のお問い合わせ先】
経営戦略室　経営企画部門
広報担当
担当：後藤・根本