

2026 年 10 月 26 日

NTT ドコモビジネス株式会社

企業の公開 IT 資産と脆弱性を可視化する「WideAngle ASM」を期間限定で無償提供 ～サイバー攻撃のリスク把握を促進し、Web システムのセキュリティ対策強化を支援～

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)は、企業のサイバーセキュリティ対策の強化を支援するため、インターネットに公開されている IT 資産や、その脆弱性・設定不備などを可視化する「WideAngle^{※1} ASM^{※2}」(以下 本サービス)を、期間限定で無償提供します。

1.背景

国内では、インターネットに公開された Web システムなどへの不正アクセスによる情報漏えいが相次いでいます。こうした状況を踏まえ、企業には、自社がインターネット上に公開している IT 資産を把握し、攻撃の起点となり得る脆弱性や設定不備を早期に発見することが求められています。

企業の Web サイトや Web サービス、クラウドサービス、VPN 機器など、インターネットに公開された IT 資産は、サイバー攻撃の対象となる可能性があります。これらの資産や外部からアクセスできる接点は、「攻撃対象領域(Attack Surface)」と呼ばれます。特に、企業が把握していないサーバーやサブドメイン、不要な公開ポート、更新されていないソフトウェアなどが残されている場合、必要な対策が講じられず、不正アクセスなどにつながるおそれがあります。このため、第三者視点で公開 IT 資産を洗い出し、脆弱性や設定不備の有無を確認することが重要です。

NTT ドコモビジネスは、公開 IT 資産の把握から、脆弱性への対応、アプリケーションの診断、攻撃通信の検知・遮断、脅威監視、インシデント発生時の対応まで、Web システムを保護する多層的なセキュリティ対策を提供しています。

今回の無償提供を通じて、こうした対策の第一歩となる「攻撃対象の把握」に取り組む機会を提供し、お客さまによる自社の公開 IT 資産とリスクの把握、および必要な脆弱性対策への着手を支援します。

2.本サービスの概要

本サービスは、攻撃者と同じインターネット側の視点から企業の IT 資産を調査し、公開 IT 資産とそのリスクを継続的に把握するサービスです。本サービスでは、IP アドレス、ドメイン、公開ポート、VPN 機器・OS・ソフトウェアに関する情報、脆弱性情報などを自動的に検出します。また、週 1 回の定期スキャン、アラート通知、ダッシュボード、ヘルプデスクを提供しています。

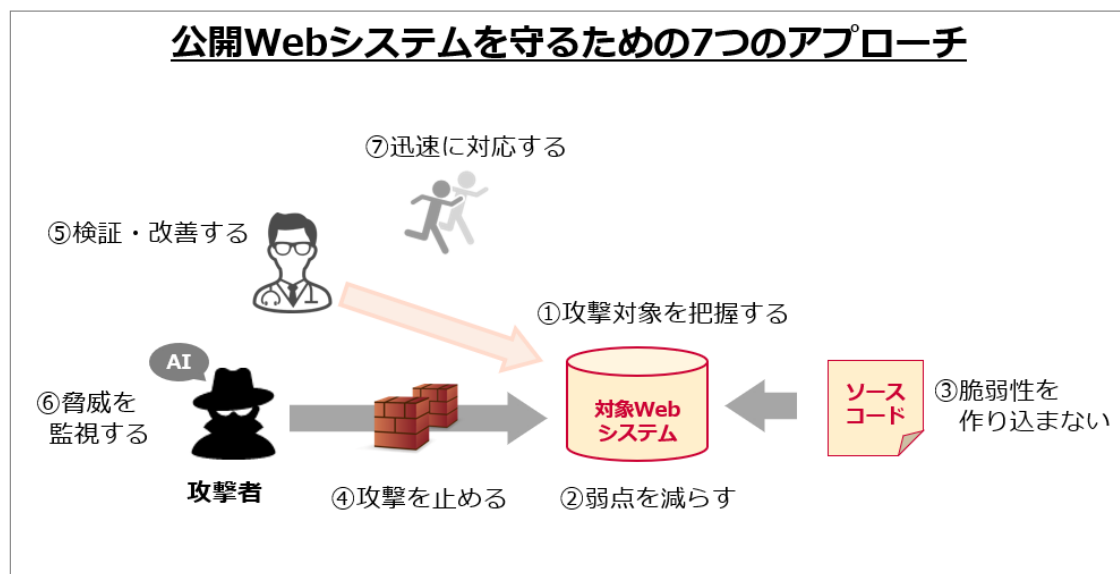
項目	内容
対象サービス	WideAngle ASM
無償利用期間	2026年11月1日～12月31日
対象	1独自ドメイン
サブドメイン	検出したサブドメインを最大99件まで調査対象へ追加
提供社数	先着200社

<本サービスの無償提供条件>

※詳しくは[説明資料](#)もご参照ください。

3.Web システムを守る包括的なセキュリティ対策

NTT ドコモビジネスは、企業の Web システムをサイバー攻撃から保護するため、「攻撃対象を把握する」「弱点を減らす」「脆弱性を作り込まない」「攻撃を止める」「検証・改善する」「脅威を監視する」「迅速に対応する」の7つの観点から、多層的なセキュリティ対策を支援します。公開 IT 資産の可視化に加え、脆弱性への対応やアプリケーションの診断、攻撃通信の検知・遮断、脅威監視、インシデント発生時の対応を組み合わせることで、Web システムのセキュリティ強化を支援します。



対策	対策の意義	主な対策例
① 攻撃対象を把握	公開資産と攻撃対象領域を把握	ASM
② 弱点を減らす	設定ミス・脆弱性・過剰権限を是正	CNAPP ^{※3} 、CSPM ^{※4} 、脆弱性管理
③ 脆弱性を作り込まない	開発工程で脆弱性を早期に検出・是正	Webアプリ診断、SAST ^{※5} 、DAST ^{※6} 、SCA ^{※7}
④ 攻撃を止める	攻撃通信を検知・遮断	WAF ^{※8} 、WAAP ^{※9} 、IPS ^{※10} 、DDoS対策、SOC ^{※11}
⑤ 検証・改善する	対策の有効性を検証し継続改善	ペネトレーションテスト ^{※12} 、Red Team、CTEM ^{※13}
⑥ 脅威を監視する	漏えい情報・なりすましサイト・脅威情報を早期発見	OSINT ^{※14} 、ダークウェブ監視
⑦ 迅速に対応する	有事の際の初動対応・原因調査・被害拡大防止を実現	IR、デジタルフォレンジック

<7つのアプローチの意義と対策例>

4.お申し込み方法

NTT ドコモビジネスグループの営業担当までお問い合わせください。

5.今後の展開

NTT ドコモビジネスは、今回の「WideAngle ASM」の無償提供を通じて、お客さまによる公開 IT 資産とサイバーリスクの把握を促進し、脆弱性対策への着手を支援します。また、ASM による公開 IT 資産の可視化に加え、クラウド環境の保護・設定管理(CNAPP/CSPM)、Web アプリケーション脆弱性診断、Web アプリケーションや API への攻撃対策(WAF/WAAP)、セキュリティ監視(SOC)、公開情報を活用した脅威情報の収集・分析(OSINT モニタリング)、インシデントレスポンスなどを組み合わせ、お客さまの Web システムに対する継続的かつ多層的なセキュリティ対策を支援していきます。

6.ウェビナーのご案内

本サービスを紹介するウェビナーを、以下のとおり開催します。

- ・タイトル：昨今急増するサイバー攻撃の背景を解説！
～AI 時代に求められるリスクベースの脆弱性管理と多層防御～
- ・開催日時：①2026 年 10 月 29 日(木) 16:00～17:00
②2026 年 11 月 5 日(木) 12:00～13:00
- ・対象者：企業のセキュリティ担当者
- ・参加費：無料
- ・開催形式：オンライン
- ・お申し込み方法：ウェビナー事務局(wideangle-pr@ntt.com)までお問い合わせください。

「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

フォーマー」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。

つながる。驚きを。幸せを。



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

- ※1：「WideAngle」とは、NTT ドコモビジネスが提供する総合リスクマネジメントサービスで、オンプレミス、クラウド、ハイブリッドなど、さまざまな ICT 環境に対しマネージドセキュリティサービスを提供します。
- ※2：ASM(Attack Surface Management)とは、外部から攻撃を受ける可能性のある資産の脆弱性対応などを管理する営みのことです。
- ※3：CNAPP(Cloud Native Application Protection Platform)は、クラウドネイティブアプリケーション保護プラットフォームという、クラウドセキュリティの考え方であり、クラウドの設定ミス、脆弱性の発見、権限の過多、マルウェアの検出を可能とします。
- ※4：CSPM(Cloud Security Posture Management)とは、クラウド環境の設定状況を継続的に確認し、設定不備やセキュリティリスクを可視化・管理するための仕組みです。
- ※5：SAST(Static Application Security Testing)とは、ソースコードなどを静的に解析し、脆弱性を検出する手法です。
- ※6：DAST(Dynamic Application Security Testing)とは、動作中のアプリケーションを外部から検査し、脆弱性を検出する手法です。
- ※7：SCA(Software Composition Analysis)とは、利用するライブラリなどの構成要素を分析し、既知の脆弱性などを確認する手法です。
- ※8：WAF(Web Application Firewall)とは、Web アプリケーションへの通信を監視し、サイバー攻撃などの不正な通信を検知・遮断する仕組みです。
- ※9：WAAP(Web Application and API Protection)とは、Web アプリケーションと API を対象とする保護機能の総称です。
- ※10：IPS(Intrusion Prevention System)とは、ネットワークへの不正な通信を検知し、遮断する侵入防御システムのことです。
- ※11：SOC(Security Operation Center)とは、サイバー攻撃の検知や分析を行い、対策を講じる専門組織のことで、各種セキュリティ装置やネットワーク機器、サーバーの監視や、それらから出力されるログの分析、サイバー攻撃を受けた場合の影響範囲の特定、サイバー攻撃を阻止するためのセキュリティ対策の立案などを担います。
- ※12：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。
- ※13：CTEM(Continuous Threat Exposure Management)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。
- ※14：OSINT(Open Source Intelligence)とは、公開情報を収集・分析する活動のことを指します。本資料では、脅威や情報漏えいの兆候の把握に活用しています。