Press Release
報道関係者各位

2026年9月7日
グランセキュノロジー株式会社

サイバー攻撃の侵入口となる「シャドーIT」を自動検出
社内・工場に潜む“見えないIT資産”とリスクを可視化する
「Mitokude.local」提供開始
-侵入後の攻撃経路も可視化、社内外のIT資産を一元管理するCAASM領域へ展開-

サイバーリスクの可視化・管理を支援するグランセキュノロジー株式会社（東京都新宿区、代表取締役 横濱友一）は、この度、企業のIT資産とサイバーリスクを可視化する「Mitokude（ミトクデ）」の新サービスとして、社内や工場などの内部ネットワークに接続されているIT資産を自動的に検出し、セキュリティリスクを可視化する「Mitokude.local（ミトクデ ドットローカル）」を提供開始します。
【Mitokude.localサイト：https://mitokude.com/local/ 】

企業のIT環境では、PCやサーバーに加え、スマートフォン、ネットワーク機器、IoT機器、工場設備など、ネットワークにつながる機器が多様化しています。その一方で、従業員が持ち込んだ端末や、管理部門が把握しないまま使用されている機器など、企業が存在を把握できていない「シャドーIT」が生じています。こうした未管理のIT資産は、適切なセキュリティ対策が行われないことで、サイバー攻撃の侵入口や、侵入後の被害拡大につながるリスクがあります。

「Mitokude.local」は、内部ネットワーク上の機器を自動的に検出し、管理部門が把握していないIT資産を洗い出します。さらに、検出した機器と脆弱性情報や構成情報を紐づけることで、攻撃者に内部ネットワークへ侵入された場合に悪用される可能性のある機器や攻撃経路まで可視化します。

当社はこれまで、インターネット上に公開されたIT資産とそのリスクを可視化する「Mitokude.pub（ミトクデ ドットパブ）」を提供してきました。今回、内部ネットワークを対象とする「Mitokude.local」を加えることで可視化範囲を社内へ拡大。今後はクラウド環境などにも対象を広げ、社内外に点在するIT資産とサイバーリスクをまとめて把握・管理できるCAASM（Cyber Asset Attack Surface Management）領域へ展開していきます。

なお、現在「Mitokude」は約300の公開資産を対象に提供しており、「Mitokude.local」についても、大手複数社を中心に導入・検証が進んでいます。今後、2027年9月までに「Mitokude」は10,000の公開資産に、「Mitokude.local」で 30社への導入を目指します。

（2026年9月7日開催 記者説明会の様子：左より当社代表 横濱 友一、当社CISO 守井 浩司）

◆背景｜「守るべきIT資産が分からない」シャドーITが新たなサイバーリスクに

近年、サイバー攻撃は高度化・巧妙化しており、企業のネットワークに侵入した後、内部を探索し、管理者権限の奪取などを経て被害を拡大させるケースも発生しています。こうした攻撃に対しては、外部からの侵入を防ぐだけでなく、侵入される可能性を前提に、社内にどのようなIT資産が存在し、どこにリスクがあるのかを平時から把握しておくことが重要になっています。

企業のデジタル化が進み、社内ネットワークにつながる機器は増加・多様化しています。一般的なPCやサーバーだけでなく、スマートフォン、ネットワーク機器、IoT機器、さらには工場の生産設備などもネットワークに接続されています。

一方、こうした環境では、
・管理部門が把握していない端末
・従業員などが持ち込んだ機器
・導入経緯や管理者が不明な機器
などがネットワーク上に存在し、「自社のネットワークに、何が、どれだけつながっているのか」を正確に把握することが難しくなっています。ネットワーク環境が複雑化する中、人間による管理だけで、すべてのIT資産を正確かつ継続的に管理し続けることは容易ではありません。

管理部門が把握できていないIT資産は「シャドーIT」と呼ばれます。シャドーITは、企業の資産台帳に登録されず、ソフトウェアの更新や脆弱性への対応などが適切に行われないまま使用される可能性があります。その結果、攻撃者にとって侵入しやすい“見えない入口”となったり、一度侵入された後の攻撃拡大に利用されたりするリスクがあります。

特に、社内ネットワークや工場など、外部から直接確認できない閉域環境では、従来の資産台帳だけでは実際の接続状況を把握しきれないケースがあります。

こうした背景から当社は、これまで外部から見えるIT資産を可視化してきた「Mitokude」の対象を内部ネットワークへ広げ、社内・工場に存在する“見えないIT資産”とそのリスクを可視化する「Mitokude.local」の提供を開始します。

◆「**Mitokude.local**」で早期発見・対策につなげられる被害例

「Mitokude.local」は、ネットワーク上のIT資産や脆弱性、侵入後に想定される攻撃経路を可視化することで、以下のような被害リスクの早期発見・対策につなげます。

＜ケース**1**｜港湾システムでランサムウェア被害、コンテナ作業が停止＞
ある港湾システムでは、社外から社内ネットワークへ安全に接続するために使われるVPN機器などを起点に内部ネットワークへ侵入され、ランサムウェア攻撃によってコンテナの積み下ろしや搬出入作業が停止する被害が発生しました。

こうしたケースでは、単に「VPN機器に脆弱性がある」と把握するだけでなく、その機器を突破された場合に、内部ネットワークを経由して重要な業務サーバーまで到達できる状態にあるかを把握することが重要です。

「Mitokude.local」では、ネットワーク上のIT資産や脆弱性、機器同士の接続関係を継続的に可視化し、侵入口となり得る機器から重要システムまで、どのような経路で到達できる可能性があるのかを把握することで、優先的な対策につなげます。

＜ケース**2**｜小売事業者で**VPN**経由の侵入、複数サーバーに被害、約**49**万人分の個人情報にも影響＞
ある小売事業者では、ネットワーク機器の脆弱性を悪用してVPN経由で社内ネットワークへ侵入され、その後、内部を探索しながら攻撃が拡大しました。最終的に11台のサーバーの大部分のデータがランサムウェアによって暗号化され、約49万人分の個人情報を含むデータにも影響が及びました。

このようなケースでは、「VPN機器に脆弱性がある」という情報だけでなく、VPNを突破された後、内部ネットワークを通じて複数のサーバーへ被害が広がる可能性まで把握しておくことが重要です。

「Mitokude.local」により、侵入後に想定される経路を事前に可視化することで、リスクの高い箇所を把握し、アクセス制限やネットワークの分離など、被害拡大を抑えるためにどこから対策すべきかを判断する材料とすることができます。

◆新サービス「**Mitokude.local**」とは

「Mitokude.local」は、社内や工場などの内部ネットワークに実際に接続されているIT資産を自動的に発見し、その構成やセキュリティリスクを可視化するサービスです。ネットワーク内にSCAN端末を設置し、各機器に専用ソフトウェアをインストールする必要のない「エージェントレス型」でスキャンすることで、PCやサーバー、スマートフォン、ネットワーク機器など、実際にネットワークにつながっている機器を把握します。

管理部門が把握していない端末や持ち込み機器などの「シャドーIT」を洗い出すだけでなく、検出した機器と脆弱性情報や構成情報を紐づけることで、「どの機器にリスクがあるのか」「侵入された場合にどこが悪用される可能性があるのか」まで把握できることが特徴です。

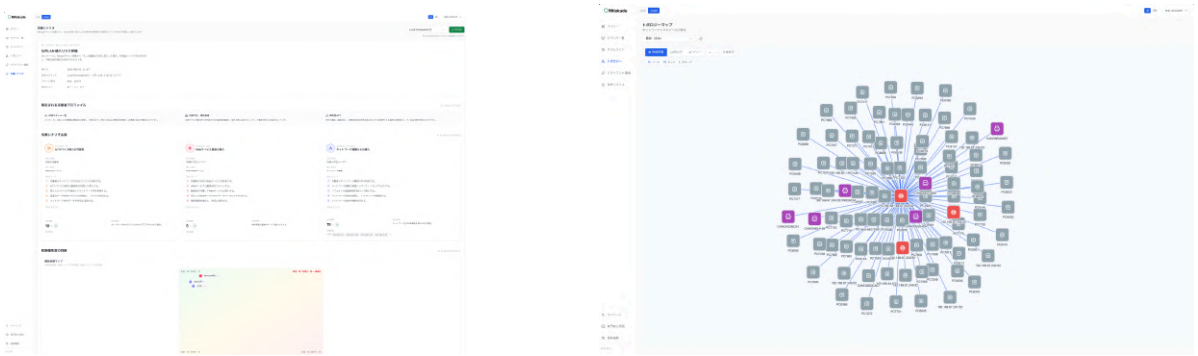
＜**3**つの特徴＞
1. 管理部門が知らない「シャドー**IT**」を自動検出
社内ネットワーク上に実際に接続されている機器を自動的に検出します。
管理部門が把握していない端末や持ち込み機器などを可視化するほか、定期的なスキャンを行い、監視設定によって新たな機器が接続された際に通知することも可能です。

2. 侵入後に悪用される機器や「攻撃経路」まで可視化
検出した機器に脆弱性情報や構成情報を紐づけることで、内部ネットワークへ侵入された場合に、攻撃者に悪用される可能性のある機器や攻撃経路を可視化します。
「侵入させない」ための対策だけでなく、万が一侵入された場合に、どこにリスクがあり、どのように被害が広がる可能性があるのかを把握し、対策につなげることができます。

3. **IT**資産とセキュリティリスクを一元管理
発見したIT資産を一元管理し、それぞれの資産にセキュリティリスクを紐づけて表示します。
従来の資産台帳だけでは把握しきれなかった「実際にネットワークにつながっているIT資産」を反映し、リスク情報と紐づいた最新の資産台帳として継続的な管理に活用することができます。

◆**PC**・サーバーだけでなく、工場設備など幅広い**IT**資産に対応

「Mitokude.local」の対象は、一般的なPCやサーバーだけではありません。Windows、Linux、macOSを搭載した端末のほか、スマートフォンやネットワーク機器などにも対応します。さらに工場環境では、PLC（プログラマブルロジックコントローラ）／SCADA・HMI／産業用PC／製造実行システム（MES）など、製造現場で使用される機器も想定しています。また、導入企業の環境や要望に応じたカスタム対応も可能です。



（画像左：内部侵入時の悪用リスク把握機能として攻撃シナリオを提供、右：シャドーIT可視化機能 として社内ネットワークの機器を可視化）

◆社内＋社外の**IT**資産を可視化、「**Mitokude**」を**CAASM**領域へ

当社はこれまで、インターネット上に公開されているドメインやIPアドレス、サーバーなど、企業の外部からアクセス可能なIT資産を継続的に発見・可視化する「Mitokude.pub」を提供してきました。（URL：https://mitokude.com/pub/ ）

今回、内部ネットワークを対象とする「Mitokude.local」をラインアップに追加することで、
・外から見える**IT**資産 → **Mitokude.pub**
・社内・工場など内部の**IT**資産 → **Mitokude.local**
と、可視化できる範囲を拡大します。

今後はクラウド環境などにも対象を広げ、社内外に点在するIT資産を横断的に把握し、セキュリティリスクとあわせて一元管理できるCAASM（Cyber Asset Attack Surface Management）サービスとして「Mitokude」を展開していきます。

＜**CAASM**とは＞
CAASM（Cyber Asset Attack Surface Management：サイバー資産攻撃対象領域管理）とは、ガートナーにより定義されたセキュリティ技術コンセプトです。組織内外に点在するIT資産を横断的に把握し、攻撃者に悪用される可能性のある資産や脆弱性を可視化することで、管理漏れの防止やセキュリティ対策の優先順位付けにつなげます。
PCやサーバーに加え、クラウド、SaaS、モバイル端末など、企業を取り巻くIT環境が複雑化する中で、「何を保有しているのか」「どこにリスクがあるのか」を継続的に把握するための考え方として注目されています。

◆導入状況と今後の展開

なお、現在「Mitokude」は約300の公開資産を対象に導入・提供しており、「Mitokude.local」についても、大手複数社で導入・検証が進んでいます。今後、2027年9 月までに「Mitokude」は10,000の公開資産に、「Mitokude.local」は30社への導入を目指します。
また、7月には株式会社DTSと「Mitokude」を基軸に協業し、DTSは、セキュリティサービスのさらなる高度化に向け、「Mitokude」の取り扱いを開始しました。

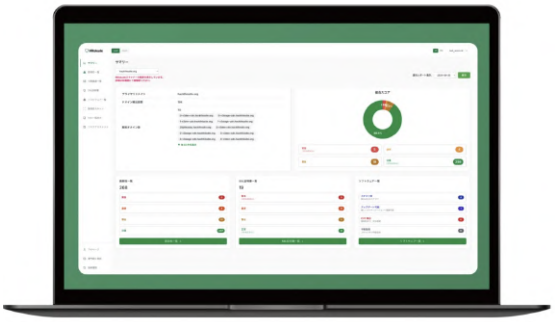
さらに今後は、個々の企業内のIT資産管理にとどまらず、取引先やグループ企業を含めたサプライチェーン全体のIT資産とサイバーリスクを可視化する仕組みへと発展させます。企業単体だけでなく、サプライチェーン全体のセキュリティ強化を支援していきます。

（2026年9月7日開催 記者説明会の様子 左から：DTS セキュリティ担当 担当課長 小川、DTS 上席執行役員 則包、グランセキュノロジー 代表 横濱、グランセキュノロジー CISO　守井）

※関連リリース　2026年07月21日発表
DTSとグランセキュノロジー、ASRMサービス「Mitokude」を基軸に協業　～継続的な脆弱性対策を両社の知見を融合し総合的に支援～
https://prone.jp/press_releases/8421

◆「Mitokude」について

「Mitokude」は、企業の社内外に点在するIT資産とサイバーリスクを横断的に可視化・管理するCAASM（Cyber Asset Attack Surface Management）領域への展開を進めるセキュリティサービスです。



これまで、インターネット上に公開されているドメインやIPアドレス、サーバーなどを継続的に発見し、「自社のIT資産が攻撃者からどのように見えているのか」を把握する「Mitokude.pub」を提供してきました。

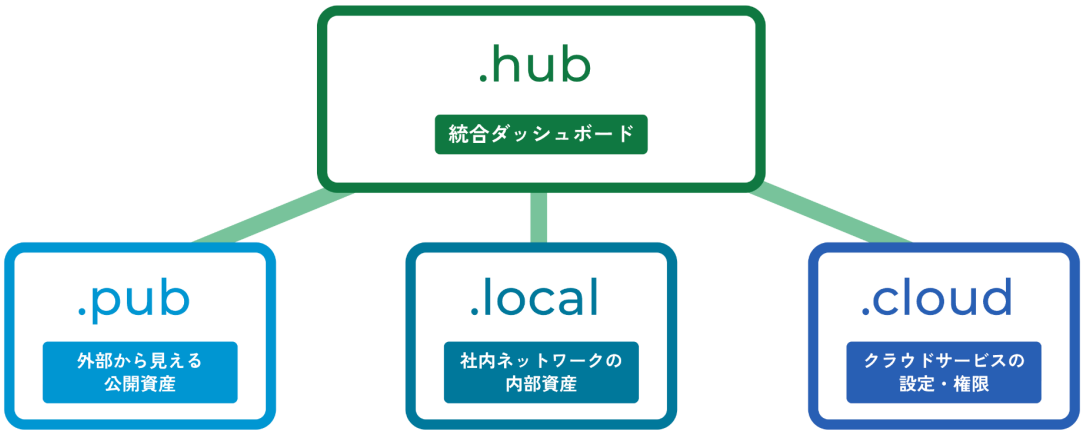
今回、新たに社内や工場などの内部ネットワークに存在するIT資産を可視化する「Mitokude.local」を追加し、外部公開資産から内部ネットワークまで可視化対象を拡大します。今後はクラウド環境などにも対象を広げ、社内外のIT資産とサイバーリスクを一元的に把握・管理するCAASMサービスとして、「Mitokude」を展開していきます。
【「**Mitokude**」サービスサイト：**https://mitokude.com/** 】

Family

Mitokude製品ファミリー全体図

.pub, .local, .cloudはそれぞれ単体でも利用可能です。

.hub があることで複数製品をまたがって簡単に統合管理が可能になります。



（「Mitokude」製品ファミリー全体図。それぞれ単体でも利用可能。
「.hub」「.cloud」は2027年提供開始予定）

＜サービス概要＞

■「**Mitokude.local**」｜内部ネットワークの**IT**資産を可視化
サービス名：Mitokude.local（ミトクデ ドットローカル）
https://mitokude.com/local/
提供開始日：2026年9月
料金：利用規模・環境に応じて個別見積もり
対象環境：社内ネットワーク、工場ネットワークなど
主な機能：内部ネットワーク上のIT資産の自動検出・可視化、シャドーITの検出、脆弱性・リスク情報の把握、内部侵入後の悪用リスク・攻撃経路の可視化、IT資産管理 など

■ **Mitokude.pub**｜インターネット上の外部公開資産を可視化
サービス名：Mitokude.pub（ミトクデ ドットパブ）
https://mitokude.com/pub/
提供開始日：2025年6月
料金：Basic：5,000円／月・1FQDN、Advanced：50,000円／月・1FQDN
　　Chaos engineeringオプション：＋25,000円／月～
対象：インターネット上に公開されている企業のIT資産
主な機能：ドメイン、IPアドレス、公開サーバーなどのIT資産の発見・可視化、脆弱性・セキュリティリスクの把握、外部から見た攻撃対象領域の継続監視 など

※FQDN（Fully Qualified Domain Name／完全修飾ドメイン名）：ホスト名を含む完全なドメイン名。1つのホストを特定する単位。

＜サービスに関するお問い合わせ先＞
グランセキュノロジー株式会社　営業部
Email：sales@grandsecunology.co.jp　　TEL：03-5333-6743

◆会社概要

・グランセキュノロジー株式会社
グランセキュノロジー株式会社は、「すべての人に、すべての企業に、セキュアな未来を。」を理念に掲げ、企業・教育機関・政府機関向けにサイバーセキュリティソリューションを提供する企業です。ホワイトハッカーをCISOに迎え、最新のサイバーセキュリティ技術と専門知見を活かした支援を行っています。

主要サービスの「Mitokude」は、企業のIT資産とサイバーリスクを可視化・管理するセキュリティサービスです。インターネット上に公開されたIT資産を外部から継続的に可視化する「Mitokude.pub」に加え、今回、社内や工場などの内部ネットワーク上のIT資産を可視化する「Mitokude.local」を提供開始。社内外に点在するIT資産とサイバーリスクを一元的に把握・管理するCAASMサービスとして展開していきます。

社名：グランセキュノロジー株式会社
設立：2024年7月
所在地：〒163-1435 東京都新宿区西新宿3-20-2 東京オペラシティタワー
代表者：代表取締役　横濱 友一
事業内容：サイバーセキュリティ対策、コンサルティング
URL：https://www.grandsecunology.co.jp/

◆本件に関するお問い合わせ先

グランセキュノロジー広報事務局（株式会社シプード内）
担当：佐藤・舩木
MAIL：pr@shipood.com