Mitokude

サービス紹介

GRANDSECUNOLOGY

自己紹介

GRANDSECUNOLOGY

渡邉　萌音
わたなべ　もね

配属	営業部
出身地	静岡県富士宮市
出身校	Buckswood School
	国際基督教大学教養学部アーツサイエンス学科 歴史学メジャー
部活動	女子バスケットボール部
趣味	スノーボード、ピアノ、バスケ、お酒、料理
マイブーム	カラオケで全年代ヒッツを歌うこと 赤ちゃんと動物の癒し動画を見ること 読書に再熱中 （最近のおすすめは三島由紀夫のレター教室）

アジェンダ

GRANDSECUNOLOGY

1. 会社概要
2. サイバーセキュリティの潮流
   - なぜサイバー攻撃が起きるのか
   - サイバー攻撃による被害
   - 近年のサイバー攻撃の特徴
   - リスクと解決策
3. Mitokudeサービス概要
4. グランセキュノロジー事業概要まとめ

GRANDSECUNOLOGY

Company 会社概要

グランセキュノロジー会社概要

GRANDSECUNOLOGY

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的な知識を駆使し、企業・教育機関・政府機関向けに包括的なセキュリティソリューションを提供する会社です。

GRANDSECUNOLOGY

Philosophy 企業理念

すべての人に、すべての企業に、セキュアな未来を。

Vision ビジョン

サイバーセキュリティが空気のように存在する社会を創る

Mission ミッション

誰もが安心してテクノロジーを使える世界を実現するために、革新的かつ持続可能なセキュリティソリューションを提供する

会社名	グランセキュノロジー株式会社 Grand Secunology Inc.	資 本 金	5,750万円	事業概要	サイバーセキュリティ対策 コンサルティング
設 立	2024年7月	代表取締役	横濱 友一	住 所	〒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

グランセキュノロジー会社概要

GRANDSECUNOLOGY

グランセキュノロジーは、「サイバーセキュリティを“特別”ではなく“日常”へ」
をスローガンに、サイバーセキュリティで社会に貢献していきます。

例えば……

自動車保険には強制保険と任意保険がありますが、皆様どちらに加入してますか？

恐らく大半の方が両方とも加入していると思います
同様にサイバーセキュリティ対策も強制ではないですが、社会全体が
当たり前に対策を行う環境の実現を目指しております

GRANDSECUNOLOGY

Landscape サイバーセキュリティの潮流

そもそも“なぜ”サイバー攻撃が起きるのか

GRANDSECUNOLOGY

近年のサイバー攻撃を行う者の動機には様々なものが存在。そのため
規模や業種にかかわらずあらゆる企業・組織が標的にされるリスクを孕んでいます。

Reason　サイバー攻撃を行う理由

金銭的利益

金銭を直接得ることが目的

- ランサムウェアによる身代金要求
- ビジネスメール詐欺(BEC)
- カード情報の盗難

機密情報の搾取

情報を盗み、売買や悪用を行う

- 顧客データの流出
- 知的財産(設計図、研究データなど)の盗難
- 契約情報の取得

政治的・社会的目的

抗議や政治的圧力、混乱の誘発

- ハクティビズム(社会運動)
- 国家によるサイバー攻撃
- 選挙妨害

実験・スキル誇示

ハッカーの技術力誇示や脆弱性の調査

- ゼロデイ脆弱性の発見
- 闇市場での脆弱性売買
- 個人の挑戦としての進入

サプライチェーン攻撃

間接的に本命の企業を攻撃するための手段

- 取引先や関連会社を経由して侵入
- ソフトウェア更新にマルウェアを仕込む

サイバー攻撃の被害

GRANDSECUNOLOGY

実際にサイバー攻撃に遭ってしまうと、事故発生から収束に向けた様々な対応が発生。

人件費・外注費・賠償・利益損失等で時には億単位の損害と甚大なレピュテーション毀損にも。

インシデント発生時において生じる損害

JNSA

各種事故対応についてアウトソーシング先への支払が発生

1．費用損害（事故対応損害）	被害発生から収束に向けた**各種事故対応**に関してアウトソーシング先への支払を含め、自組織で直接費用を負担することにより被る損害（下記２～６に該当しないもの）

さらに、次のような損害の発生も起こりうる

2．賠償損害	情報漏えいなどにより、第三者から損害賠償請求がなされた場合の**損害賠償金**や弁護士報酬等を負担することにより被る損害
3．利益損害	ネットワークの停止などにより、事業が中断した場合の**利益喪失**や、事業中断時における人件費などの固定費支出による損害
4．金銭損害	ランサムウェア、ビジネスメール詐欺等による**直接的な金銭（自組織の資金）の支払い**による損害
5．行政損害	個人情報保護法における**罰金**、GDPRにおいて課される**課徴金**などの損害
6．無形損害	風評被害、ブランドイメージの低下、株価下落など、無形資産等の価値の下落による損害、**金銭の換算が困難な**損害

アンケート調査まとめ

JNSA

被害種別	平均被害金額
ランサムウェア感染被害	2,386万円
エモテット感染被害	1,030万円
ウェブサイトからの情報漏えい（クレジットカードおよび個人情報）	3,843万円

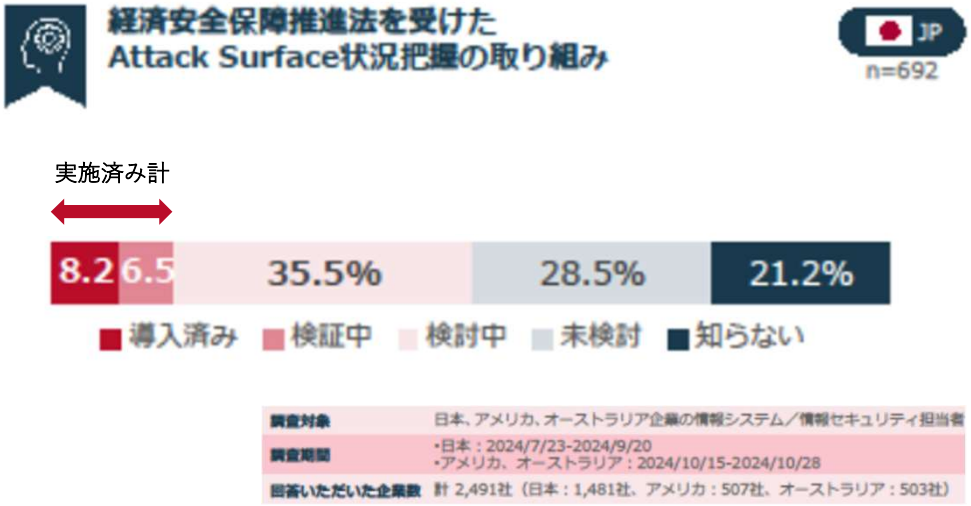
アンケート調査の回答が少ないこと、
人件費、逸失利益は含まれていないことを勘案するに、
実際の損失はもっと高額と考えられる

近年のサイバー攻撃の特徴

GRANDSECUNOLOGY

昨今のサイバー攻撃は攻撃対象領域(Attack Surface) が拡大し件数と範囲が急速に拡大しています。
一方その対策済み組織はわずか15%と大きなセキュリティリスクになっています。

Attack Surfaceの拡大と対策の遅れ



※EXECUTIVESUMMARY（出典：NRI Secure Insight 2024）

ASへ「対策を実施済み」と回答した企業はわずか15%だが、「検討中」とする企業は35%に上り、企業の関心が高まっています。広域にわたるリスクに対し今後は、一次請け企業だけでなく、サプライチェーン全体に対する継続可能なリスクマネジメント体制の整備が急務です。

NICTERにおけるサイバー攻撃関連の通信数の推移

近年、サイバー攻撃は年々増加の一途をたどっており、2023年のサイバー攻撃関連通信は約5,927万件に達し、過去最高を記録しました。

「把握しきれない公開資産」というリスク

GRANDSECUNOLOGY

広範な攻撃対象になりうるインターネット上の「公開資産」。
自社でも把握していないうちに攻撃者に見つかり、標的になってしまっている可能性があります！

“気づかない”5大リスク

01 攻撃対象となっていることに気づかない

クラウドサービスやSaaSの導入、リモートワークの普及により、IT資産が社外に分散し管理されていないサーバやドメイン、APIなどが放置され、攻撃者にとって格好の標的に。

02 勝手に導入されたITに気づかない

現場主導で導入されたツールやサービスが、セキュリティ部門の管理外におかれ、「シャドーIT」という状態に。脆弱性の把握やパッチ適用が遅れるリスクが高まる。

03 従来の脆弱性スキャンでは気づかない

従来の脆弱性スキャンは既知の資産に対してのみ有効。攻撃者視点での「外から見える資産」を把握できていないと本当のリスクが見逃される。

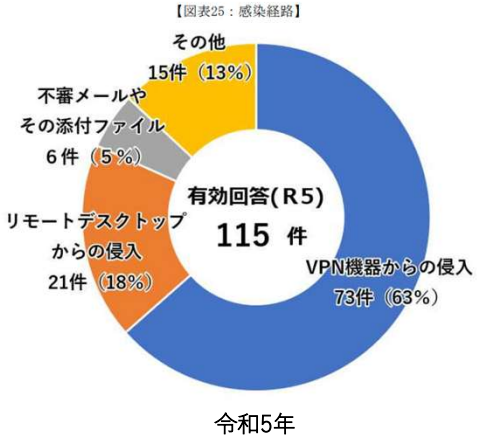
04 人の手だけでは気づかない

攻撃対象領域の監視や分析を人手で行うのは非現実的。
自動化されたASMツールがなければ、対応が後手に回る。

05 インシデントが起きても気づかない

攻撃を受けた際に、どの資産が影響を受けたか即座に把握できない。結果として、初動対応が遅れ、被害が拡大する。

攻撃者の手法が変化し自社の公開資産を管理できていない可能性



令和5年

昨今、攻撃手法は急激に変化し、企業セキュリティの弱点を極めて効果的に突いています。Web経由やメール経由に代わり、対策が進んでいない外部公開サーバへの侵害へ変化。
そのため自社が意図せずインターネット上に晒している“公開情報資産”がハッカーの攻撃対象となるケースが急増。特に「クラウドの利用拡大」「子会社・委託先との連携」「担当者がバラバラで自由に公開」等、企業自身が把握しきれていない公開資産が重大なリスクになっています。

ASMという解決策

GRANDSECUNOLOGY

攻撃の対象となる広範にわたる自社資産を適切に把握・管理して守る Attack Surface Management（ASM）が必要です。

Attack Surface Management（ASM）とはサイバーセキュリティ攻撃の脅威となりうる（Attack Surface）を、把握・管理（Management）する取り組みです。インターネット上に公開された企業の資産を可視化する事で、より効率的な管理が行え、より効率的なセキュリティ対策が行えます。

ASMを実施する際に重要となるポイントは現状だけではなく、変化する将来にも対応可能な網羅的な資産「把握」と把握した資産のリスクに対する緊急性と重要度を加味した対策の「優先順位付け」です。

ASMができること

攻撃対象の可視化	シャドーITの検出	リスクの優先順位付け	継続的な監視	レポートとアラート
インターネット上の資産を自動で発見・分類	管理外のドメインやクラウド資産を特定	脆弱性や設定ミスをリスクレベルで評価	攻撃対象領域の変化をリアルタイムで追跡	経営層にも伝わる可視化されたレポートを提供

ご提案するソリューション

GRANDSECUNOLOGY

リスクまで管理するサイバーセキュリティ対策の新サービス

ASRM（Attack Surface +Risk Management）

Mitokude

- Web上に公開された資産の可視化
- 可視化された資産の脆弱性調査
- 脆弱性の優先度判定
- 脆弱性対策を専門家が指南
- リスクを可視化し経営指標としても活用

これら大変な工程をお客様に代わってワンストップに実施します

GRANDSECUNOLOGY

Overview

Mitokudeサービス概要

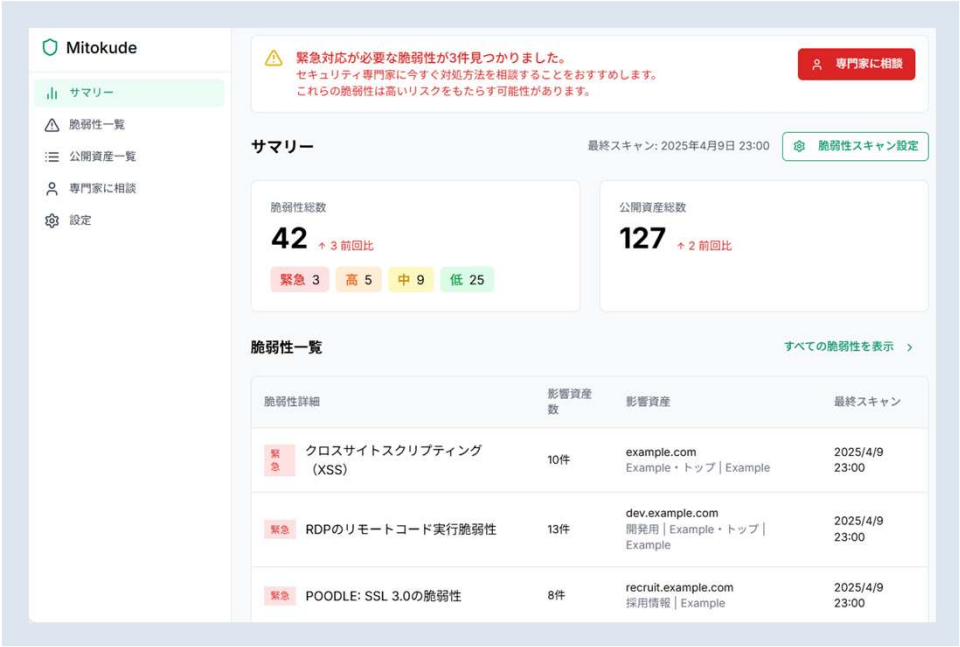
GRANDSECUNOLOGY

Mitokude ASRM

Attack Surface +Risk Management

主要機能

- 攻撃可能領域のスキャン機能（ポートスキャン）
- サブドメイン自動取得機能
- 公開資産の一覧画面表示
- 設定不備評価機能
- 攻撃可能領域の週次可視化レポート
- お問合せ機能
- URL攻撃可能領域のスキャン機能
  - WEBアプリケーション脆弱性スキャン
  - OSミドルウェア脆弱性スキャン
  - SSL証明書チェック
- 資産リスク評価（資産情報のUI拡充）
- 分析機能（サマリー、システム詳細）



＊URLスキャンをリクエストすると、Mitokudeが直接ウェブサイトにアクセスしてドメインの全てのOSINTを収集し、脅威データを分析します。
＊URLのフル・スキャンの結果はレポートで提供され、PDFでダウンロードいただけます。
＊スキャンには平均10分程度がかかり、リアルタイムでウェブサイトやプラットフォームを分析できますが、スキャンの結果脆弱性や関連データがない場合も存在するためご留意ください。
＊スキャンには自組織の資産や委託された資産など管理権限がある資産にのみ実施ください。
一つのアカウントで同時に1回のスキャンしかリクエストできません。

Mitokudeが“守れる理由”

GRANDSECUNOLOGY

Mitokudeは、集約管理・対応履歴・専門家の伴走という
セキュリティ対策に必要な3つのきめ細かなサービスによって貴社資産を守ります。

『Mitokude』ならではのキメ細かなサービス

01

これら大変な工程を皆様に代わってワンストップに実施します

複数の外部情報ソース（OSINT）を自分で横断的に確認する必要はありません。Mitokudeでは、各種OSINTを統合的に集約し、一元化されたダッシュボードで「今、何が晒されているのか」「リスクはどこにあるのか」をスピーディに把握できます。

02

単なる検知で終わらせない——“対応の履歴”まで管理

見つけた公開資産や脆弱性に対して、「誰が」「いつ」「何をしたか」といった対応履歴を記録・管理。これにより、過去の対応方針をチームで共有しやすく、属人化リスクを排除。

03

ツールだけでは分からない“脅威の本質”を専門家がリアルタイムで伴走

Mitokude最大の特長は、「リアルな脅威に、リアルな人が向き合う」支援体制。自社のアタックサーフェスをただ機械的に並べるだけでなく、「どこから攻撃されそうか」「なぜそこが狙われるのか」「今すぐ対応すべきか」をセキュリティの実務経験者が対話を通じてアドバイスします。

Mitokudeがなくても手動でできるのでは？

GRANDSECUNOLOGY

Mitokudeがなければ、攻撃対象領域の管理は“地道な手作業の積み重ね”になります。Mitokudeなら起点ドメインを登録するだけで、外部の公開情報資産を可視化し専門家と共に対策まで進めることができます。

もしMitokudeなしの場合……

公開情報を一つずつ手作業で調査

複数の公開ソースを定期的に確認し、IP・ドメイン・証明書・GitHub等を手作業で拾い集める作業
▶ 見逃しのリスク
▶ 情報の鮮度を保てず、属人化・引き継ぎが困難

資産情報を手動でエクセルで管理更新

検知した資産を自分で表にまとめ、更新も差分を比較。煩雑な記録管理と社内連携が必要に。
▶ 管理が煩雑
▶ ISMSや監査対応に時間と手間がかかる

実際の脅威への対処方針を自力で判断

放置してよいか、優先対処すべきかといった判断も、情報システム部門が孤独に判断し責任を負う
▶ セキュリティ経験が浅いと誤判断リスク
▶ 緊急時、社内合意形成に時間がかかる

対応方針に“相談相手がいない”

対策に迷っても相談できる専門家がいないため、調査・検討・社内説明の全てを自力でこなす
▶ 現場のストレス増大
▶ セキュリティ対応が後手に回る原因に

それでも「攻撃者は24時間、あなたの資産を見ています」

Mitokudeなら

01 まずドメインを登録するだけ！

お客様のドメインをご提供いただくだけで、関連するサブドメインや公開情報資産の洗い出しを自動でスタートします。

02 資産の自動把握と可視化

「攻撃者からどう見えるか」の視点で、企業の“攻撃対象領域”を一覧化します。

03 専門家が伴走して対応方針をアドバイス

可視化だけでは終わりません。セキュリティの専門家が対話・支援し、「今、何をすべきか」を共に考え、サポートします。

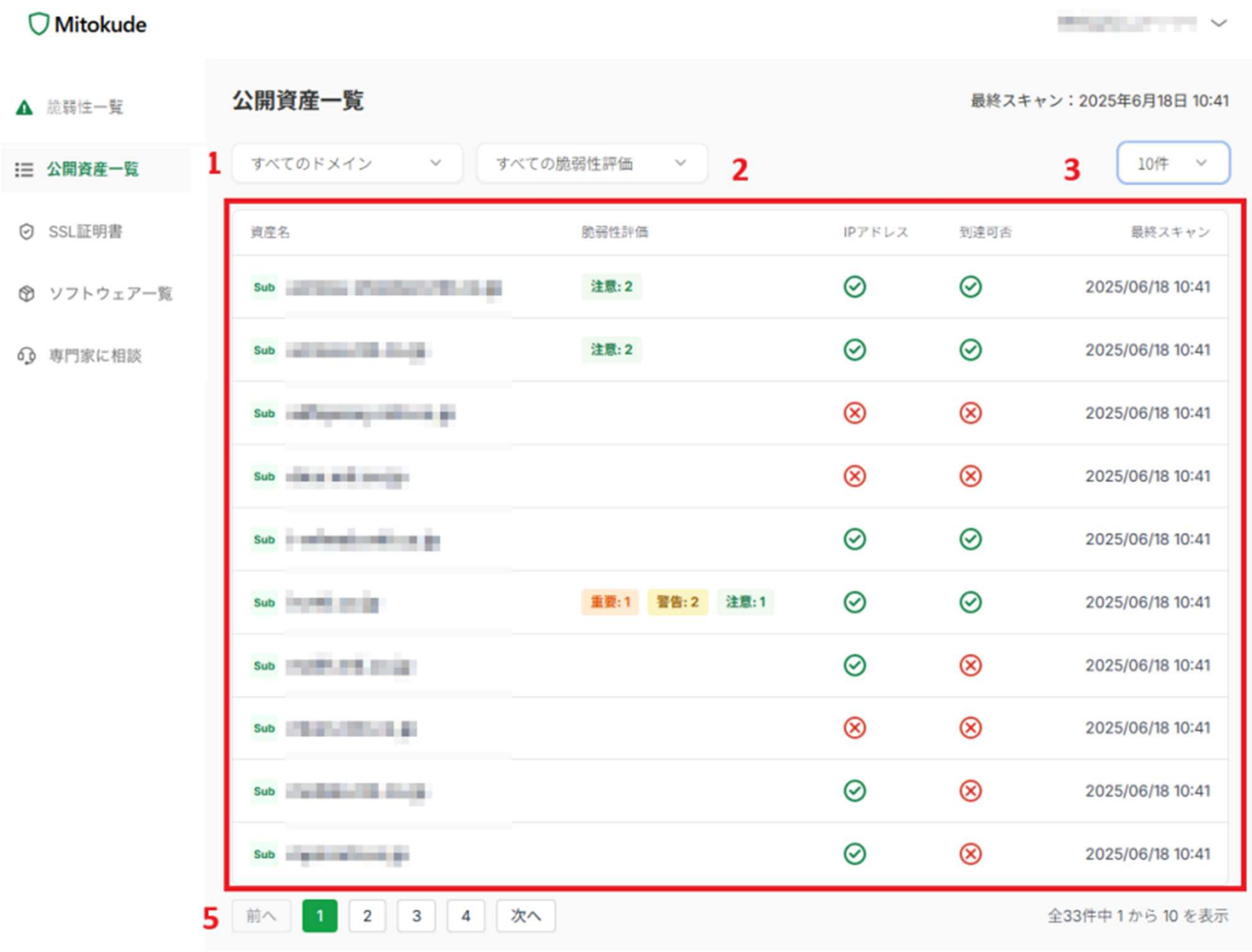
Mitokude　ログイン後画面

GRANDSECUNOLOGY

Mitokude　脆弱性一覧

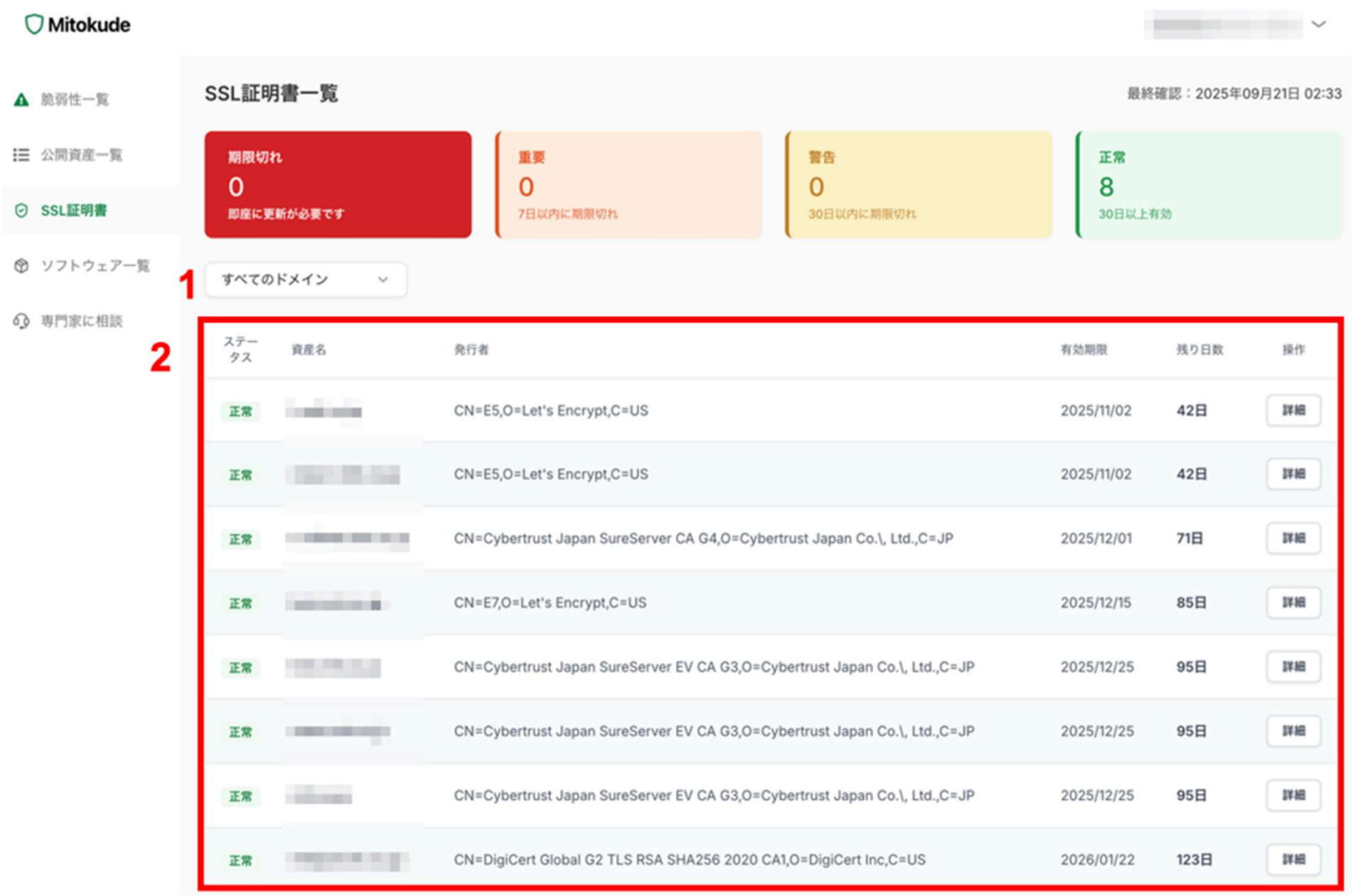
Mitokude　公開資産一覧

GRANDSECUNOLOGY



Mitokude　SSL証明書一覧画面

GRANDSECUNOLOGY



Mitokude　SSL証明書一覧画面

GRANDSECUNOLOGY

スキャン概要	
IPアドレス	[redacted]
ポート番号	443
逆引きDNS	--
サービス	HTTP
コモンネーム	-
信頼ステータス	trust is via wildcard
EV証明書	いいえ
サブジェクト	CN=[redacted]
発行者	CN=E5,O=Let's Encrypt,C=US
シリアル番号	[redacted]
残り日数	42日
サブジェクト代替名	[redacted]
検証ステータス	有効: はい 期限切れ: いいえ 自己署名: いいえ ホスト名一致: はい 証明書チェーン有効: はい
有効期間の開始	2025年8月4日 11:58:22
有効期間の終了	2025年11月2日 11:58:21
最終確認日時	2025年9月21日 02:33:22

Mitokude　SSL証明書一覧画面

GRANDSECUNOLOGY

検出された問題

問題の種類	重要度	説明	推奨事項 / CVE / CWE
expiring_soon	低	証明書が42日以内に期限切れになります	証明書の更新を計画してください
BREACH	中	potentially VULNERABLE, br gzip HTTP compression detected - only supplied '/' tested	CVE-2013-3587 / CWE-310

推奨事項

- TLS 1.3のサポートを有効化してください
- HSTSヘッダーを設定してください
- OCSP Staplingを有効化してください

プロトコルサポート

SSL v2	無効
SSL v3	無効
TLS 1.0	無効
TLS 1.1	無効
TLS 1.2	無効
TLS 1.3	無効

Mitokude　SSL証明書一覧画面

GRANDSECUNOLOGY

セキュリティ機能

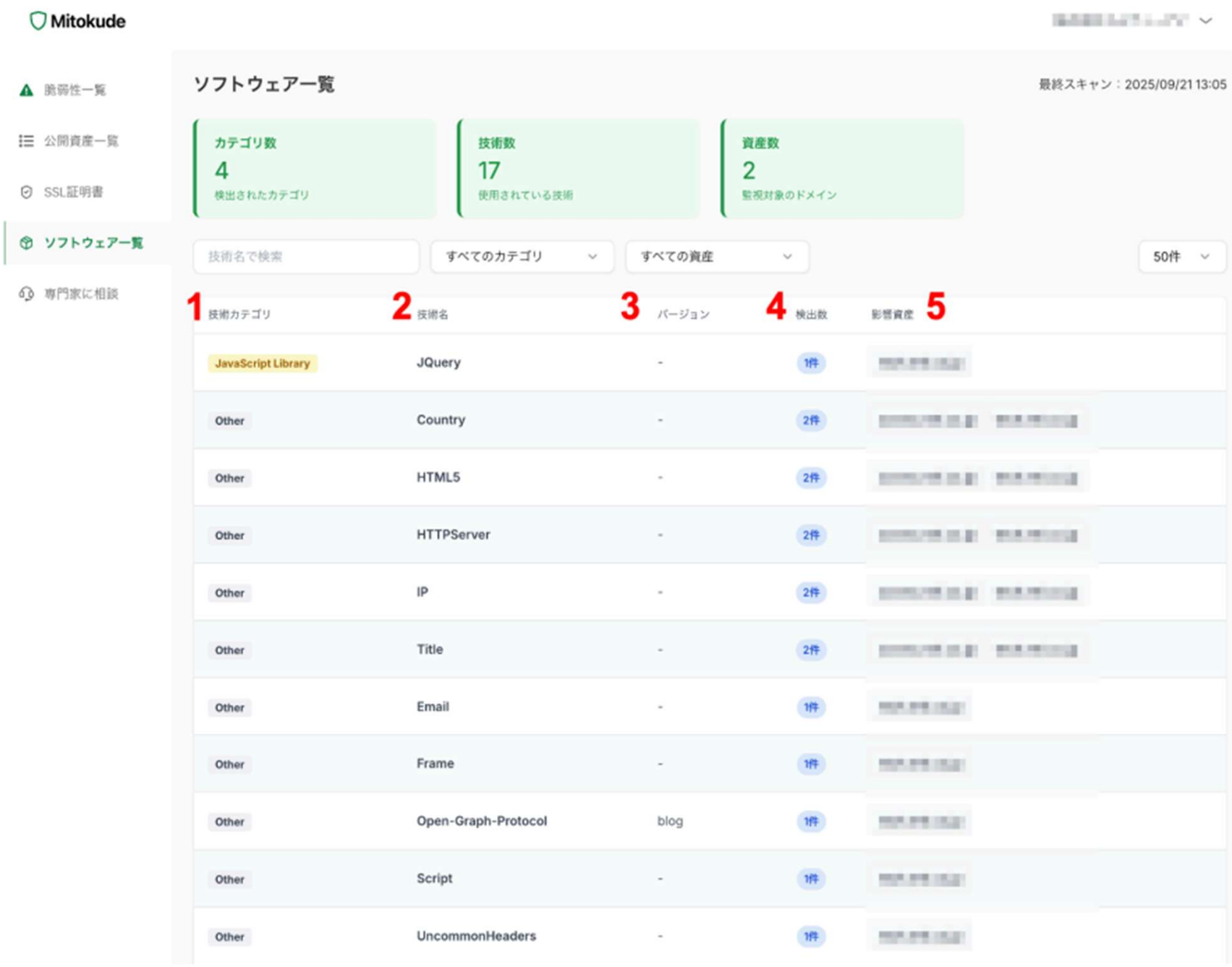
Forward Secrecy	有効
HSTS	無効
HPKP	未設定
OCSP Stapling	未設定
証明書の透明性	未設定
DNS CAA	未設定

HTTP情報

HTTPステータスコード	-
リダイレクトURL	-
サーバーバナー	cloudflare
アプリケーションバナー	--
Cookieセキュリティの問題	なし

Mitokude　ソフトウェアー覧画面

GRANDSECUNOLOGY



Mitokude　専門家に相談画面

GRANDSECUNOLOGY

GRANDSECUNOLOGY

Mitokude Ver1.0_ASM

料金プラン

月額 5,000円 / FQDN（+消費税）

脆弱性診断 + 警告 + 対策提案 + 相談込み！
ボリュームディスカウントあり（1000FQDN以上）
専用環境・エンタープライズ対応（個別ご相談）

※2025年9月末リリース予定

✓攻撃対象資産の可視化

精度の高い独自OSINT技術で
「野良資産」も逃さない

✓サブドメイン/ドメイン取得

ホワイトハッカー視点で
設計された検出ロジック

政治的・社会的目的

攻撃者目線のリアルな
リスク評価と提案

✓設定ミスの洗い出し

「なぜ危険なのか」を解説

✓セキュリティ対策提案

利用者の声を即反映し
進化し続けるASM

✓アラート通知・相談窓口

月10件までホワイトハッカーに
直接相談無料！

GRANDSECUNOLOGY

進化する ASRM Mitokude

Attack Surface +Risk Management

Mitokudeは進化し続けます

お客様の声に耳を傾け進化し続けます
攻撃手法の進化に追随し進化し続けます
ITの高度化とともにより便利に進化し続けます

社会の変化とともに進化し続けます

拡張予定機能

GRANDSECUNOLOGY

ＡＩ機能： スキャン結果に対しAIが評価、分析を行い脆弱性の原因特定や推奨対応策を提示します

ローカル資産管理機能： 社内ネットワーク上の“見えないIT資産”の検出・管理機能

ＩｏＴ資産管理機能： ネットワークに接続されたIoT機器を対象にした資産管理機能

脆弱性自動対応機能： 検出された脆弱性に対する自動的な対応を行う機能

その他続々機能拡張予定

お客様のご意見、ご要望を是非お聞かせ下さい

グランセキュノロジーの事業全体

GRANDSECUNOLOGY

グランセキュノロジーは、Mitokudeによる見える化＋耐える力の基礎体制構築から
実際の様々なセキュリティ対策・コンサルティングまでトータルでサポート可能です

セキュリティコンサル事業

セキュリティ診断

- 脆弱性診断
  Webアプリケーション診断、
  ネットワーク診断、ソースコード診断等
- ペネトレーションテスト
  内部・外部ペネトレーションテスト、
  クローリングサービス
- セキュリティレビュー
  GitHub設定レビュー、クラウド設定レビュー、
  OS設定レビュー

マネジメント監査／システム監査

- セキュリティガバナンス、内部統制、
  リスクマネジメントの評価
- システムの設計・運用・監査の実施

セキュリティコンサルティング

- 企業のセキュリティポリシー策定支援
- サイバー攻撃対策の強化とインシデント
  対応計画の策定
- セキュリティ教育・啓発プログラムの提供
- インシデント対応体制の構築
  （CSIRT・SOC支援）

Contact US!　sales@grandsecunology.co.jp

GRANDSECUNOLOGY