国が推奨する
次世代のセキュリティソリューション
「ASM」とは

はじめに

Securify

本ホワイトペーパーは、

経済産業省 商務情報政策局 サイバーセキュリティ課による

「ASM(Attack Surface Management)導入ガイダンス
外部から把握出来る情報を用いて次組織の IT資産を発見し管理する」

の初版発表を受け、我々はセキュリティ診断ソリューション Securifyの開発事業者として、
より広いセキュリティ担当者へ分かりやすく情報を拡散するために作成いたしました。

本ホワイトペーパーが ASM取り組みのきっかけとなり、ご覧いただいた方の所属組織における
セキュリティ強化の一助となりますことを願っております。

目次

Securify

1. サイバーセキュリティの現状と課題
2. 経済産業省「ASM導入ガイダンス」ポイント解説
3. ASMツールの料金形態、導入メリットについて
4. まとめ

サイバーセキュリティの現状と課題

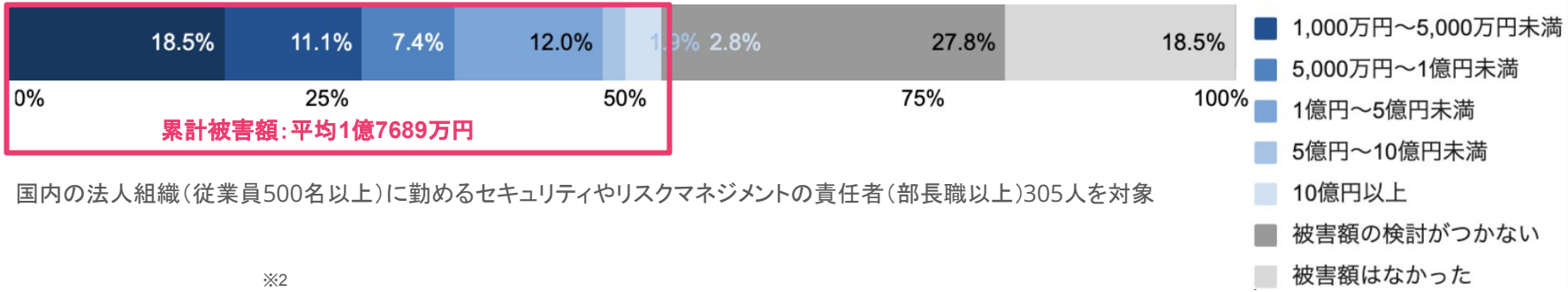
増加するサイバー攻撃

Securify

※1
トレンドマイクロ社の調査レポートによると、
過去3年間で56.8%がサイバー攻撃の被害を経験しており、
被害コストが最も大きかったのは **ランサムウェア** です。

ランサムウェア被害を経験した法人組織の累計被害額は **平均1億7689万円** となっています。

ランサムウェア被害経験組織の累計被害額の割合



国内の法人組織（従業員500名以上）に勤めるセキュリティやリスクマネジメントの責任者（部長職以上）305人を対象

※2
さらに警察庁の報告によると、日系企業におけるランサムウェアによる
セキュリティインシデントの数は、直近 3年間で300件以上発生しており、
特に2022年にはVPNやリモートデスクトップといった
外部公開資産が感染経路として 81% を占めています。

注1）トレンドマイクロ株式会社　サイバー攻撃による法人組織の被害状況調査　https://www.trendmicro.com/ja_jp/about/press-release/2023/pr-20231101-01.html
注2）警察庁　令和4年におけるサイバー空間をめぐる脅威の情勢等について　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

脅威は国民の生活にも

Securify

ランサムウェアによるサイバー攻撃は、組織における経済的な損失のみならず、**国民の生活にも影響**を及ぼしています。2021年には徳島県の公立病院がサイバー攻撃を受け、**一般診療が約2か月間停止**するという事件が発生しました。他に国内外でも生活に影響しうる事件が多数報告されています。

※3

徳島・鳴門の病院にサイバー攻撃　電子カルテにアクセスできず

杉田基 吉田博行　2022年6月20日 20時30分

サイバー攻撃を受けた鳴門山上病院=2022年6月20日午後5時23分、徳島県鳴門市鳴門町土佐泊浦、吉田博行撮影

徳島県 は20日、 鳴門市 の医療法人久仁会「鳴門山上病院」が19日午後、ランサムウェア（身代金ウイルス）による サイバー攻撃 を受けたと発表した。電子カルテにアクセスできない状態だという。

病院は20日の新規患者の受け入れを停止し、再開のめどはたっていない。すでに通っている患者の診察や、入院患者の治療に支障はないという。

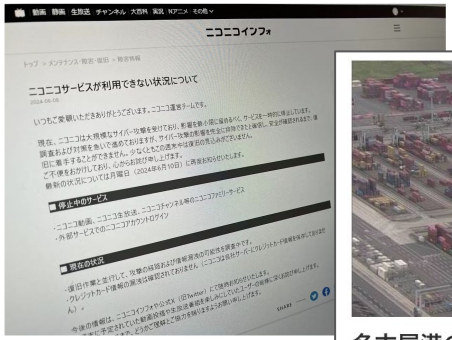
※4

ニコニコ動画、サイバー攻撃で停止　「週末は復旧困難」

情報通信・ネット　＋フォローする

2024年6月9日 11:18 (2024年6月9日 11:48更新)

保存



※6

サイバー被害の米パイプライン、身代金4.8億円の支払い認め 米紙報道

※5

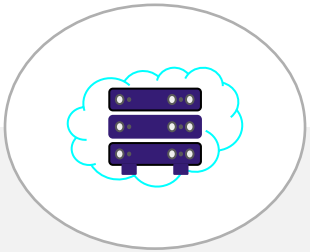
名古屋港のサイバー攻撃問題でセキュリティー対策 国交省

注3）朝日新聞デジタル https://www.asahi.com/articles/ASQ6N6QFPQ6NPTLC01W.html　注4）日本経済新聞 https://www.nikkei.com/article/DGXZQOUC083UD0Y4A600C2000000/
注5）NHK https://www3.nhk.or.jp/news/html/20230929/k10014211351000.html　注6）BBC NEWS JAPAN https://www.bbc.com/japanese/57181463

事業者における課題

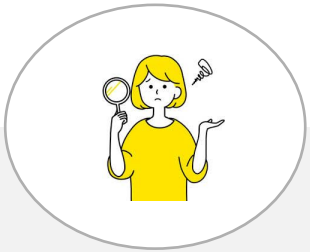
Securify

前項の様なサイバー脅威の危険性や被害数が年々増加しています。
しかし、DXやクラウド化の進む現代社会において、以下の様な課題が多くの事業者を悩ませており、
適切なサイバーセキュリティ対策を行うことは非常に難しい状況です。



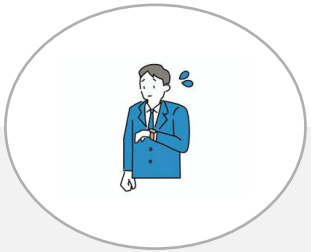
外部に公開されたIT資産の棚卸しが出来ていない

クラウドの活用によってインターネット上からアクセスできるサーバーやネットワーク機器の把握が難しい。



セキュリティリスクがどこにあるのか分からない

自社内で提供しているサービスやIT資産に対するセキュリティリスクが把握できていない。



セキュリティ対策に割ける工数が少ない

セキュリティ人材が不足しており、対応工数が間に合わず、結果的に対策が疎かになっている。

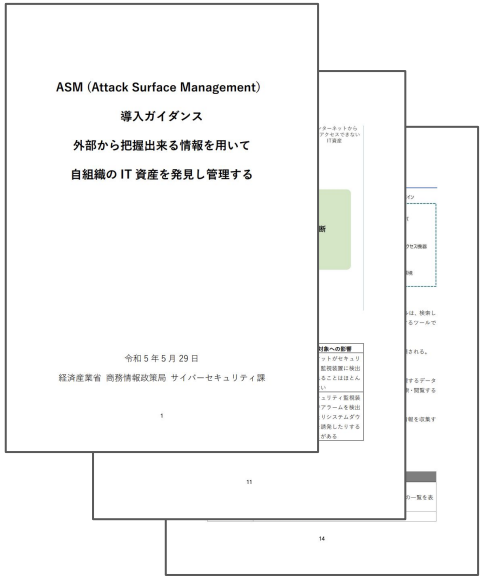
経済産業省「ASM導入ガイダンス」ポイント解説

経済産業省：ASM導入ガイダンス

Securify

前項のように厳しいサイバーセキュリティ情勢を受け、
2023年5月、経済産業省より「ASM（Attack Surface Management）導入ガイダンス」
が発行されました。以降は本ガイダンスの内容について解説します。
まず、2章では定義やプロセス、特徴、脆弱性管理との違いについて述べられています。

※8



※9

注8）経済産業省 https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html
注9）経済産業省 商務情報政策局 サイバーセキュリティ課 「ASM（Attack Surface Management）導入ガイダンス 外部から把握出来る情報を用いて自組織の IT 資産を発見し管理する」
https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf

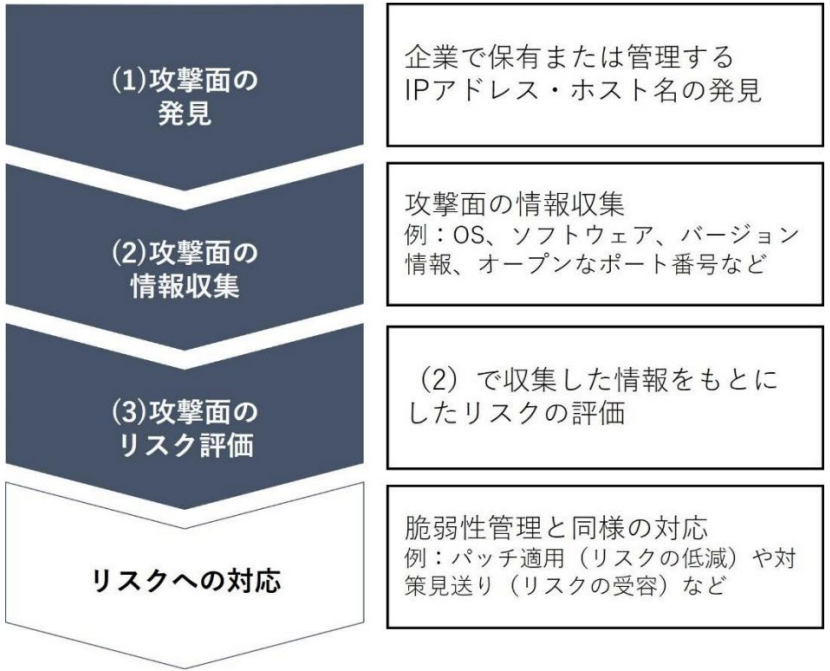
そもそもASM（Attack Surface Manegement）とは

経済産業省の「ASM導入ガイダンス」内では、ASMは以下のように定義されています。
「組織の外部(インターネット)からアクセス可能な IT 資産を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセス」
プロセスの構成は右図を参考。

※攻撃面 =
「組織の外部（インターネット）からアクセス可能な　IT 資産」
インターネットとの境界点にあるネットワーク機器や　PC、
サーバから各種システム、ソフトウェア、　OSなど。

※ガイダンス内ではリスクへの対応については
ASM のプロセスには含めていないが、
自社のセキュリティリスクを減らすという目的においては、
リスクへの対応を実施すべきであると補足があります。

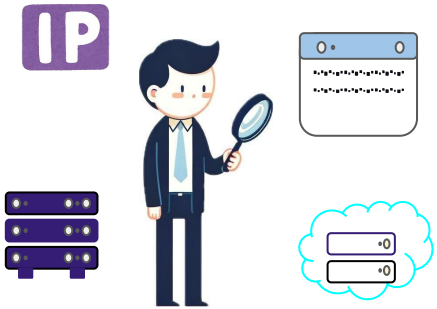
※10



注10）経済産業省　ASM 導入ガイダンス内　図2-1 ASMのプロセス　https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf

Securify

ASMの活用シーン



キャンペーン活動に
利用するWebサイトなど
情報システム管理部門以外
が構築・運用している
IT 資産を発見する。

設定ミスにより、
外部からアクセス可能な
状態となっている社内システム
などを発見する。

グループ企業における
統制上の課題や
地理的な要因によって、**本社で**
一元的に管理できていない
IT 資産を発見する。

ASMと脆弱性管理の関係性

Securify

ASM は未把握の IT資産を発見するという形で 脆弱性管理や IT 資産管理を補完する取り組み

※11

脆弱性管理のライフサイクル	ASMプロセス
対象ソフトウェアの把握	攻撃面の発見
脆弱性関連情報の収集	攻撃面の情報収集
適用の判断	攻撃面のリスク評価
計画	リスクへの対応
検証	
適用	

左図は『脆弱性対策の効果的な進め方（ツール活用編）6』(IPA）参考の脆弱性管理のライフサイクルとASMプロセスを対照したものです。

ポイントは2点

①ASM は脆弱性管理のライフサイクルにおいては「対象ソフトウェアの把握」「脆弱性関連情報の収集」「適用の判断」をカバー。
※なお「適用の判断」で発見された脆弱性への対応の要否については、ASM のプロセスに含まれていない。

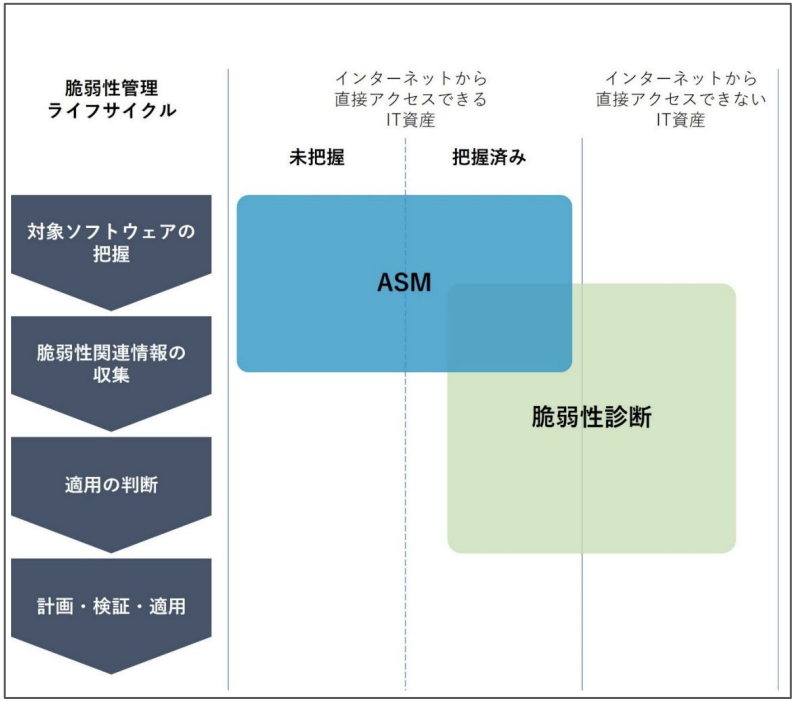
②ASMと脆弱性管理では対象となるIT資産の範囲が異なります。詳しくは次項で解説します。

注11）IPA「脆弱性対策の効果的な進め方（ツール活用編）」https://www.ipa.go.jp/files/000071584.pdf

ASMと脆弱性診断の違い

Securify

「ASM」と「脆弱性診断」は違いがあります。目的に応じて **使い分け、併用** します。



※12

主な違い、関係性は以下となります。

	対象	脆弱性の特定確度	対象への影響
ASM	インターネット上を検索し発見したものを対象とする（未把握のものが含まれる）	通常アクセスの範囲で行うため確度が低い可能性がある	対象のIT資産への影響はほぼ無い
脆弱性診断	予め把握しているドメインやIPなど対象とする	攻撃を模したパケットを送信し、その応答を評価することで一定の確度が期待できる	セキュリティ監視装置によるアラーム検出や、対象の動作に支障をきたす可能性あり

注12）経済産業省　ASM 導入ガイダンス内　図2-2 ASM と脆弱性診断の違い　https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf

ASMプロセスを自動化する「ASMツール」

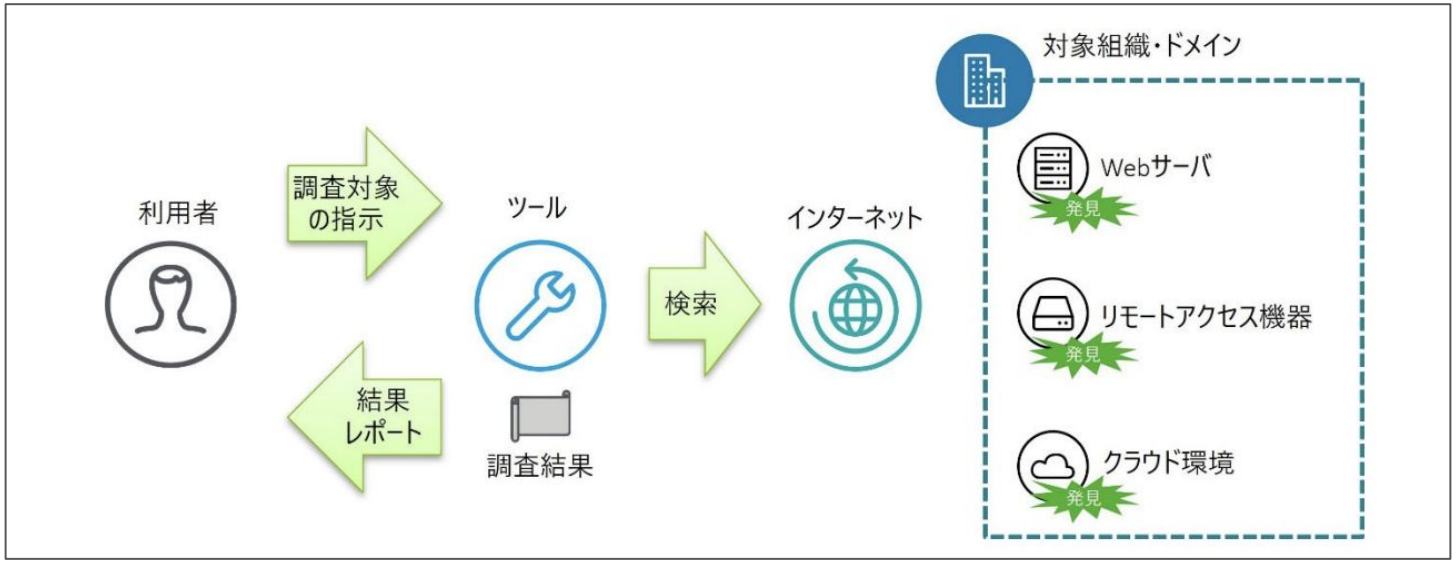
Securify

3章では実際の実施にあたってのポイントが述べられています。

- 導入目的 、調査対象範囲 、運用 をしっかりと整理しておくことが肝要としています。

また実際の攻撃面の調査と評価には、「ASMツール」の利用が実質的に不可欠です。
以下図はツール利用時の動作イメージです。ASMツールの主要機能は次項に記載しております。

※13



注13）経済産業省　ASM 導入ガイダンス内　図3-1 ASMツールの動作　https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf

ASMツールの主要機能

※14

分類	機能
(1) 攻撃面の 発見	• **IP アドレス・ホスト名の一覧表示機能** 一覧は IPアドレス・ホスト名に加え、OS などの情報が表示されている。OS、ミドルウェア、 ポート番号（稼働しているサービス）、CVE、発見された時刻などの情報で 絞り込みが可能な場合が多い。
(2) 攻撃面の 情報収集	• **攻撃面の詳細情報表示機能** 対象ホスト名、IP アドレス、OS、OS のバージョン、ソフトウェア、 ソフトウェアのバージョン、アクセス可能なポート番号、クラウドのベンダー情報、 攻撃面を発見した日付など。
	• **ダッシュボード機能**
(3) 攻撃面の リスク評価	• **リスク評価機能** 検索によって得られた情報をもとにした攻撃面のリスクを表示する機能。 攻撃面の危険度を評価するものが多いが攻撃面全体の成熟度を表示するツールも存在する。 • **レポート機能**
その他	• **リスク対応補助機能** … 対応優先度を付与する • **ファイル出力機能** … 発見した攻撃面や脆弱性情報をCSV などで出力する • **通知機能** … 特定の情報をトリガーとしてユーザーに通知する。 • **ログ機能** … ツール操作のログを収集する。 • **アクセス制御** … ロールを設定し、各ユーザーの操作を制限する • **対応状況管理機能** … 調査中や調査済みなどの対応状況のタグを付与する

注14）経済産業省　ASM 導入ガイダンス内　図3-1 ASMツール機能（プロセス別）　https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf

ASMツール活用上、注意すべき事項とガイダンスまとめ

Securify

ガイダンス内、3章の3.2.3では必要となる知識・スキルについて、
3.2.4ではASMツール活用上の注意点を解説されています。ASMツールを導入する際には、
以下ガイダンス内の注意点と、採用 ASMツールの仕様を併せて確認しましょう。

- 不正確な情報の検知
- 対象となる企業への影響
- 脆弱性評価の方法
- リスク評価指標の活用方法
- 検索エンジン型の更新頻度

その後、ガイダンスでは 4章では国内企業に対して、
ASMの取組実態と課題についてヒアリングを実施した際の 2つの事例をとりあげて解説されています。
最後に5章にてまとめとなります。(6章に付録あり)

ASMツールの料金形態、導入メリットについて

市場のASMツールの特徴、料金形態

Securify

ここからは、「Securify」がASMツールについて調査した情報を提示しています。

- 既にセキュリティプラットフォームを提供している事業者から機能拡張　or リパッケージした
  統合ソリューションが先行して市場に展開されています。（ Tenable,Mandiant,Cloud Strikeなど）

- プロセス内でツールによる自動化とセキュリティエンジニアによる手動サービスを
  組み合わせたソリューションもあります。

- 具体的な料金情報は公開されていないサービスがほとんどです。提供機能、ライセンス形態、
  検知するドメイン、IP数などの導入規模、連携サービスの種類などによって
  見積り価格が変動する形となります。

- 当社調べによりますと、おおよそ

  中規模の事業者導入料金（想定従業員数　1000名以下）　約 **30** 万円～/月

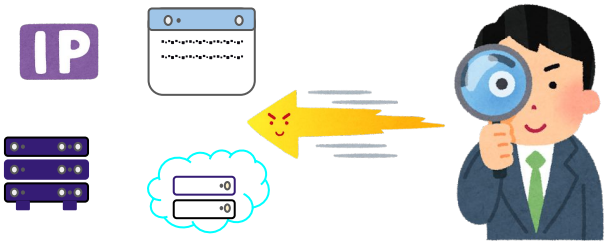
  大規模の事業者導入料金（想定従業員数 1000名以上）　約 **100** 万円～/月

といった料金帯で市場が展開されている様です。

導入のメリット（短期的）

Securify

リアルタイムに
迅速な攻撃面の可視化、評価



企業の外部に公開されている全ての
IT資産を即座に特定、リスクを把握し
必要な対策を実施することが可能です

重大な脆弱性が存在する場合、その
リスクに即座に対応することができます

コスト削減

インシデントを未然に防ぐことでの
対応コスト削減を見込めます

また外部公開資産への棚卸しの自動化
によって、運用保守における人的コストの
省力化を実現します

導入のメリット（長期的）

Securify

- **持続的なセキュリティ強化**
  継続的な攻撃面の監視とリスク評価が可能です。常に最新のセキュリティ状況を把握し、
  対策を講じ続けることができます。

- **ガバナンス統制の強化**
  監査や報告の際に必要なデータを提供できるため、
  各種セキュリティ規制や標準に準拠するための要件を満たすことが容易になります。

- **リスク管理の最適化**
  長期的にわたるデータ収集と分析によって、リスクの傾向やパターンを把握しやすくなります。
  リスク管理戦略を最適化を実現します。

- **資産管理の効率化**
  継続的にIT資産の状況を監視することで、資産管理の効率が向上します。
  不要な資産の削減や新たな資産の導入時に迅速かつ的確な判断が可能になります。

まとめ

まとめ

Securify

クラウド環境やデジタル化が進む現代では、企業の　IT資産管理が複雑化しています。
攻撃者はその複雑化しているが故に、管理が行き届いていない領域をターゲットとして
ランサムウェア攻撃などのサイバー攻撃を仕掛けています。

まずはASMツールを活用し、**攻撃者目線**で自社の外部公開された IT資産を把握して
みましょう。さらに継続的に攻撃面のリスク把握、情報収集、対応を行うことで、
その複雑さを解消し、効率的なリスク管理を実現が見込めるはずです。

このホワイトペーパーが、皆さんの組織における　ASMの導入と活用の一助となり、
事業者にとって、ひいては国民の生活にとって、安全な　IT環境を築くためのきっかけと
なることを願っています。

新たなセキュリティ対策として、ぜひ　ASMの取り組みをご検討ください。

Appendix

スリーシェイクのセキュリティソリューション「Securify」

実績紹介

Securify

Securifyは、**経済産業省が策定した一定の技術要件および品質管理要件の基準を示した「情報セキュリティサービス基準」に適合しているサービス**であり、各SaaS比較サイトにおけるランキングで1位を受賞しています。

ITトレンド
「セキュリティ診断」カテゴリ
1位

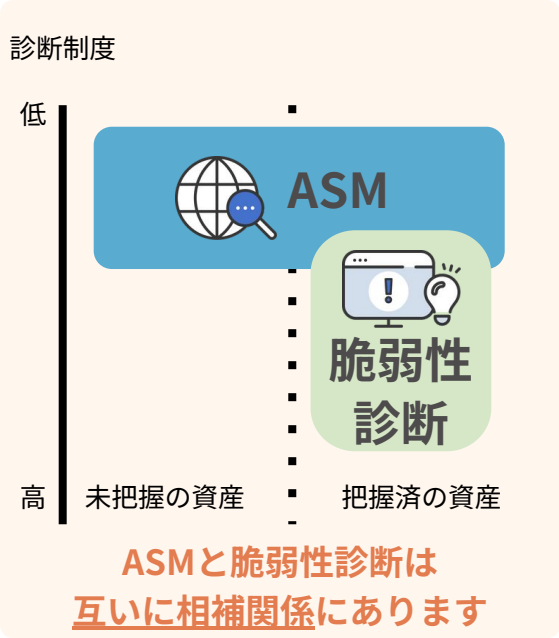
スマートキャンプ株式会社主催
「BOXIL SaaS AWARD Autumn 2024」
「BOXIL SaaS AWARD Winter 2024」
セキュリティ診断サービス部門で受賞

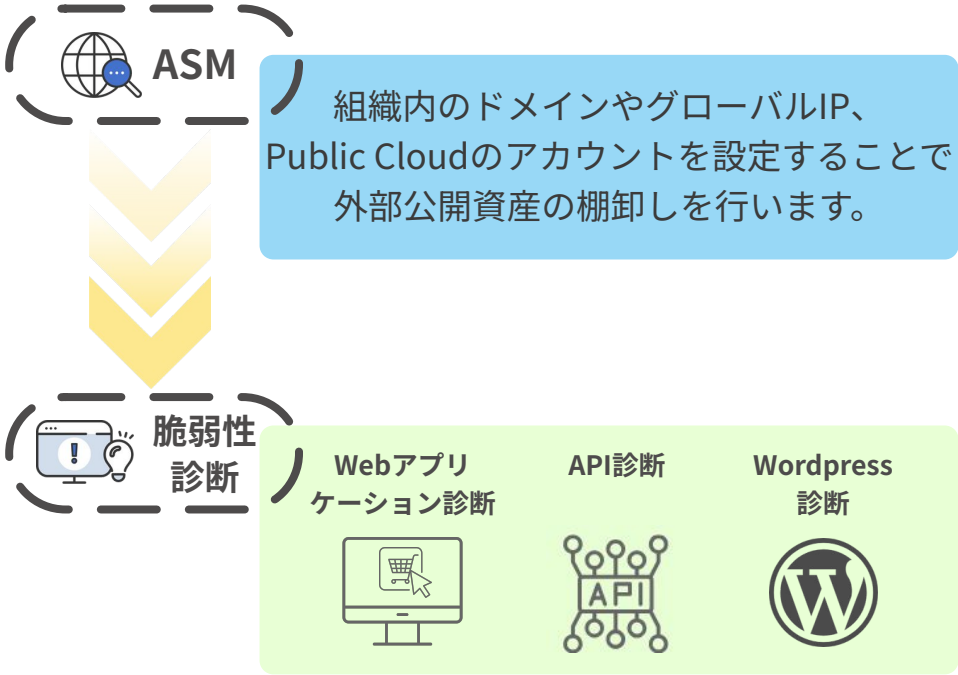
ASPICクラウドアワード2024
支援業務系ASP・SaaS部門
社会貢献賞 受賞

Securify(セキュリファイ)とは

Securify

Securifyは、情報漏洩の起点から逆算で対策を行うことができる画期的なセキュリティプラットフォームです。
強力なASM(外部公開されているIT資産の棚卸し)と高度な脆弱性診断の組み合わせにより
攻撃者視点で診断を行い、企業内のセキュリティリスクをあぶり出します。





Securify ASMの3つの特徴

Securify

1.パブリッククラウドからリソース検出可能

AWS / Google Cloud / Azure
などのパブリッククラウドを連携することで、Public Cloud 上のリソースの変動性にも対応した定常的な棚卸しを自動的に行います。

2.高精度な脆弱性診断とシームレスな連携

実際にハッカーが攻撃をした場合、
どのような危険性があるのかを
棚卸しされたエンドポイント毎に
擬似攻撃的リクエストをし、
レスポンスを分析する脆弱性診断を
同プラットフォーム上で実施可能。

3.ゼロデイ脆弱性への対策をアラート

検出したエンドポイントごとに
利用しているテクノロジー情報を
一元管理します。

また、関連したゼロデイ脆弱性の
発見時、Securifyから
アラートメールが発信されるため、
迅速な対応を行うことが可能です。

特徴1. パブリッククラウドをソースとして検出

Securify

	経産省が紹介するASMツールの主流 （検索エンジン型・オンアクセス型）	NEW Securify ASM
探索手法	• 公開情報の利用 • 自動収集(スクレイピング、スキャン) • ベンダー独自調査	• 自動収集(スキャン) • **クラウド内部からデータ収集**
特徴	• 通常のインターネットアクセスでスキャンを行うため検知確度に懸念がある。 • 独自調査に基づくデータ提供は利用料が高額になりがち。 • 調査手法やアルゴリズムが公開されていない場合、結果を評価しづらい。 • 自社と関係のないドメインを検出してくるケースもあり、運用に工夫が必要な場合も。	• APIによるデータ取得のため、**検知精度は100%！全て自社のクラウド内の公開資産のため、運用しやすい。** • クラウド内の公開資産を網羅的に検知することができるため、DNSが紐づけられていない放置された一時的なテスト用サーバーのIPなども検知可能。

Securify ASMなら管理すべき対象を確実に検知！

特徴1. パブリッククラウドをソースとして検出

Securify

Securify

aws

- Elastic Load Balancing
- Amazon CloudFront
- Amazon Elastic Compute Cloud(EC2)
- AWS Simple Storage Service(S3)
- Amazon Relational Database Service

Google Cloud

- Cloud Load Balancing
- Compute Engine
- Cloud Run
- Cloud Storage
- Cloud SQL

Azure

- Azure Load Balancer
- Azure Content Delivery Network
- Azure Virtual Machines
- Azure Blob Storage
- Azure Database , Azure SQL Database

通常のASMツールでは
確認できない**クラウドリソース情報を一元管理する**ことで、
クラウドの利用状況を可視化し、
セキュリティリスクや
不要なコストの削減を支援します。

特徴2. 高精度な脆弱性診断とシームレスな連携

Securify

通常のASMでは対応しないアプリケーションレベルの脆弱性診断などを、同一サービス内で実施できます。
つまり、診断の外部委託にかかる工数・コストを大幅に減少しつつ、
全工程においてノーコード操作で公開資産の発見から脆弱性診断までをストレスフリーで行えます。

SecurifyASM

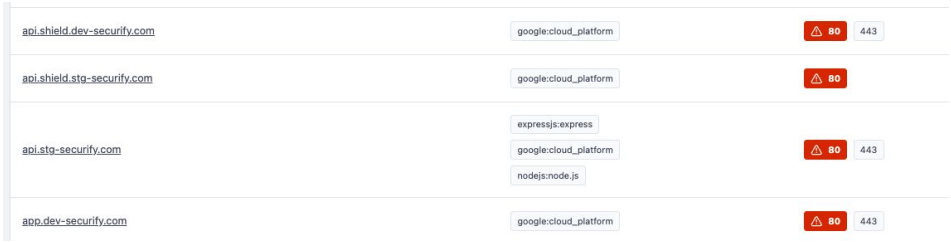
ワンストップ

Securify

外部公開資産
棚卸し

Webアプリ
診断

▼棚卸しイメージ



API診断

Wordpress診断

特徴3. ゼロデイ脆弱性への対策をアラート

Securify

検出されたエンドポイントのテクノロジー情報を
(プログラミング言語 / HTTPサーバー情報など)
一元管理

新たなセキュリティ脅威に対して
一元管理下の情報とCVE情報
(共通脆弱性識別子/Common Vulnerabilities and Exposures)
を元にSecurify が迅速なアラートをお届けします

**これらの機能により、
新たなセキュリティ脅威に
迅速に対応できる体制を実現します！**

お問い合わせはこちらから

Securify

ぜひお気軽にご連絡ください。

お問い合わせはこちらをクリック

Thank you.