Securify

～情報システム部の担当者様へ～

「セキュリティ大丈夫？」
もう聞かれても怖くない！
🌐ASMでリスクの見える化を実現

はじめに

Securify

～ 未知なる脅威から企業を守る、攻めのセキュリティ対策　～

情報システム部門は、今や企業の生命線です。

サーバーやデバイスだけでなく重要な情報資産を守る情報システム部門には、
従来の運用・管理に加え、サイバー攻撃から企業を守る重大な責任が課せられています。

近年、リモートワークやクラウドの普及により、企業のAttack Surface (攻撃対象領域)は
拡大しセキュリティリスクは増大しています。従来の境界防御中心の対策では不十分です。

そこで、今まさに**『ASM(Attack Surface Management)』**が注目されています。
ASMは、外部から見える自社のシステムやデバイスを網羅的に把握し、
脆弱性を早期に発見、修復することで、被害を最小限に抑える取り組みのことです。

本ホワイトペーパーでは、情報システム部門がASMを理解し、
自社システムのセキュリティ強化に役立てるためのポイントを解説します。

目次

Securify

セキュリティ課題

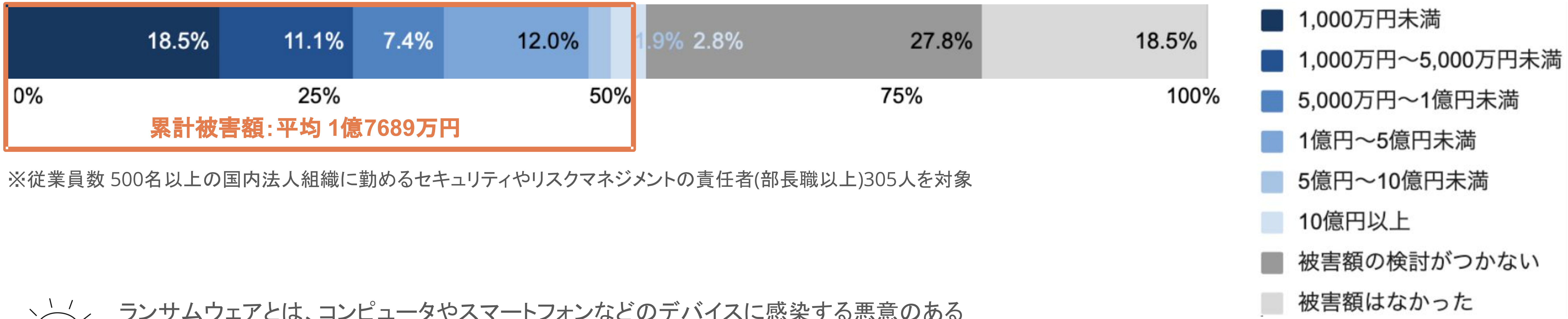
増加するサイバー攻撃

Securify

トレンドマイクロ社が、法人組織のセキュリティ責任者305人を対象とした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**。

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**でした。

ランサムウェア被害経験組織の累計被害額の割合



※従業員数 500名以上の国内法人組織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

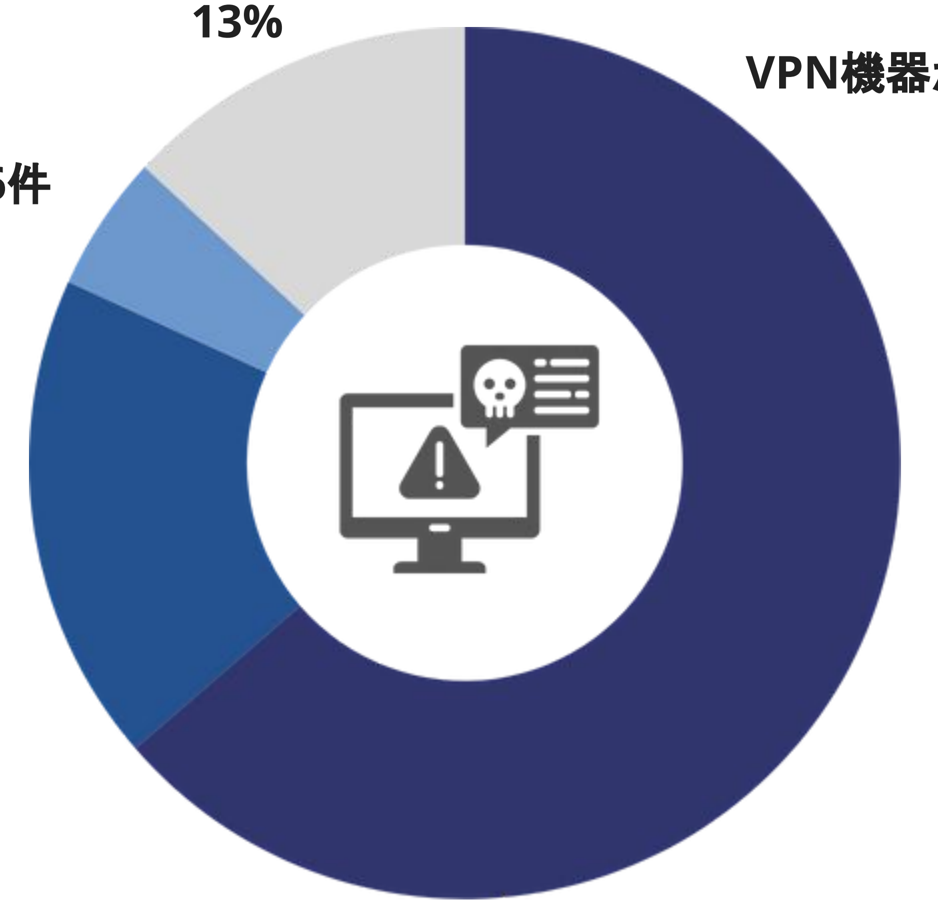
ランサムウェアとは、コンピュータやスマートフォンなどのデバイスに感染する悪意のある
ソフトウェア(マルウェア)の一種です。このソフトウェアは、デバイス上のデータやファイルを
暗号化して使えなくし、その解除のために金銭を要求する　という手口で攻撃します。

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. 2023, https://www.trendmicro.com/ja_jp/about/press-release/2023/pr-20231101-01.html

増加するサイバー攻撃

Securify

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、
依然として高水準で推移するとともに、特に2024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約 82%を占めています。



※ランサムウェア被害のあった企業・団体など197件にアンケート調査を実施・有効回答115件
(図の割合は小数点第1位以下を四捨五入しているため、統計が必ずしも100にならない)

復旧に要した期間について質問したところ、136件の有効な回答があり、このうち、復旧までに1ヶ月以上を要したものが2ヶ月以上を含め28件ありました。

サイバーセキュリティサーベイ2023によると、過去1年間に発生したサイバー攻撃では、**子会社や委託先のシステムを経由した攻撃が41.5%**を占めていました。

警察庁. 令和5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. 2024, https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf
KPMG. サイバーセキュリティサーベイ. 2023, https://assets.kpmg.com/content/dam/kpmg/jp/pdf/2024/jp-cyber-security-survey2023.pdf

企業の情報システム部における課題

Securify

情報システム部における課題

他部署が各々で作った環境まで管理できていない

忙しい！

全員の動きを監視することは不可能。さらに、監査対応時におけるIT資産の棚卸しは膨大な数のライセンスが存在し、正確な情報把握と管理が難しいとされています。

上司や経営層から「セキュリティ大丈夫？」って聞かれるけど …正直

わからない！

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

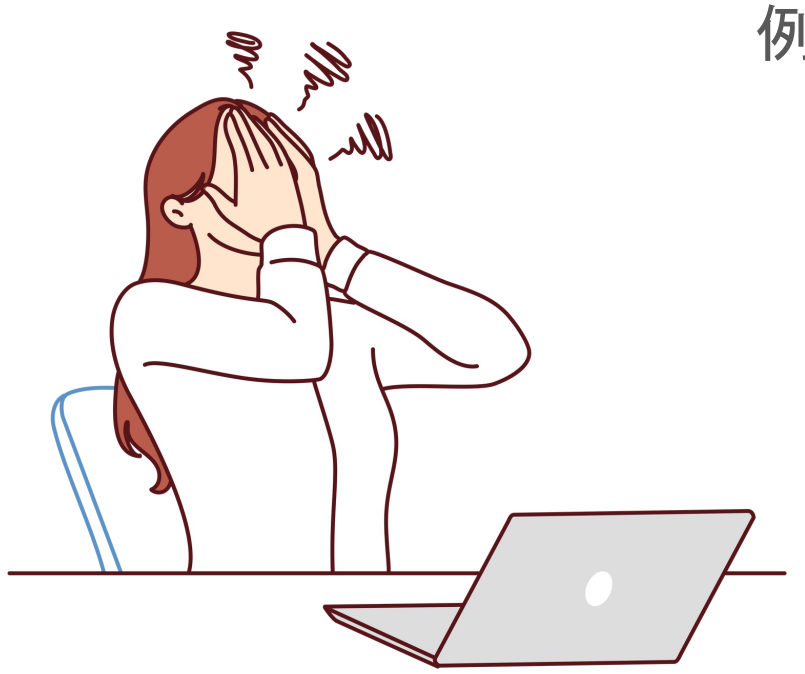
セキュリティの専門知識を持っていない

難しい！

情シス担当は他にも多く業務を抱える中、セキュリティに割ける人も時間も知識も十分ではない。
外部委託を検討するも、責任範囲や要件定義など結局は担当者の負荷に。

企業の情報システム部における課題

Securify

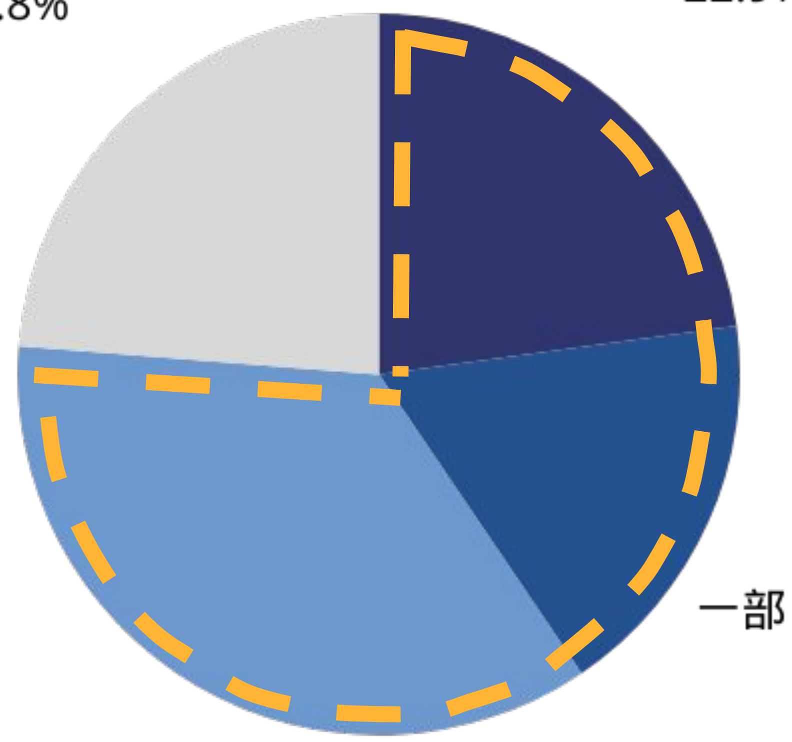


未把握のIT資産

例えば

- メンテナンス用のVPN装置
- 開発メンバーがたてたテストサーバー
- 国外拠点のコーポレートページ
- 大学のゼミ生や講師が作ったWebサイト

etc...



76.2%の企業がシャドー ITを検知できていない と回答しています。

シャドーITを検知できていなかったために、ランサムウェア被害にあった事例もあります。
ある企業はテレワークによりネットワークの負荷が高まったことから、緊急対応で現地法人が所有する旧型のVPN装置を設置したところ、当該機器を狙われました。
攻撃者は北米のVPN装置を経由して社内ネットワークに侵入し、米国や日本のサーバーから情報を盗み、流出の可能性がある個人情報は最大約39万人分に上りました。

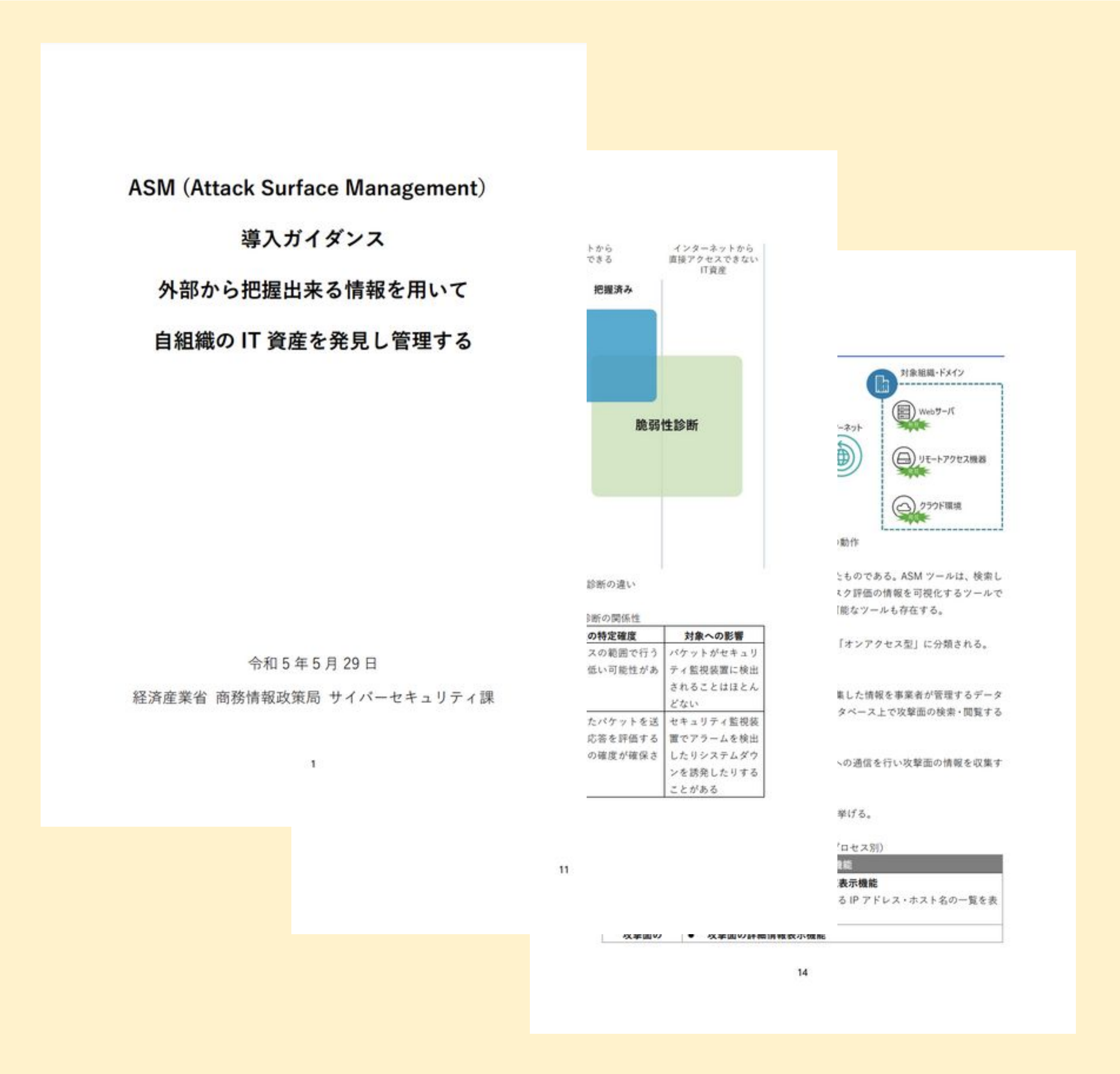
ジョーシス株式会社. 新しい働き方に合わせたセキュリティ対策 ～リモートワークやシャドーITから企業を守る～. 2024, https://jp.josys.com/learning/blog/seminar20230302
日経クロステック. カプコンの不正アクセス被害はVPN装置が原因、20年11月のサイバー攻撃. 2021, https://xtech.nikkei.com/atcl/nxt/news/18/10098/

ASMとは

経済産業省の ASM導入ガイダンス

Securify

厳しいサイバーセキュリティ情勢を受け、
2023年5月に**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を用いてASMの定義やプロセス、特徴、
脆弱性管理や他のセキュリティ製品との違いについてに解説していきます。



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」. 2023, https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf
経済産業省. 「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～」を取りまとめました. 2023, https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

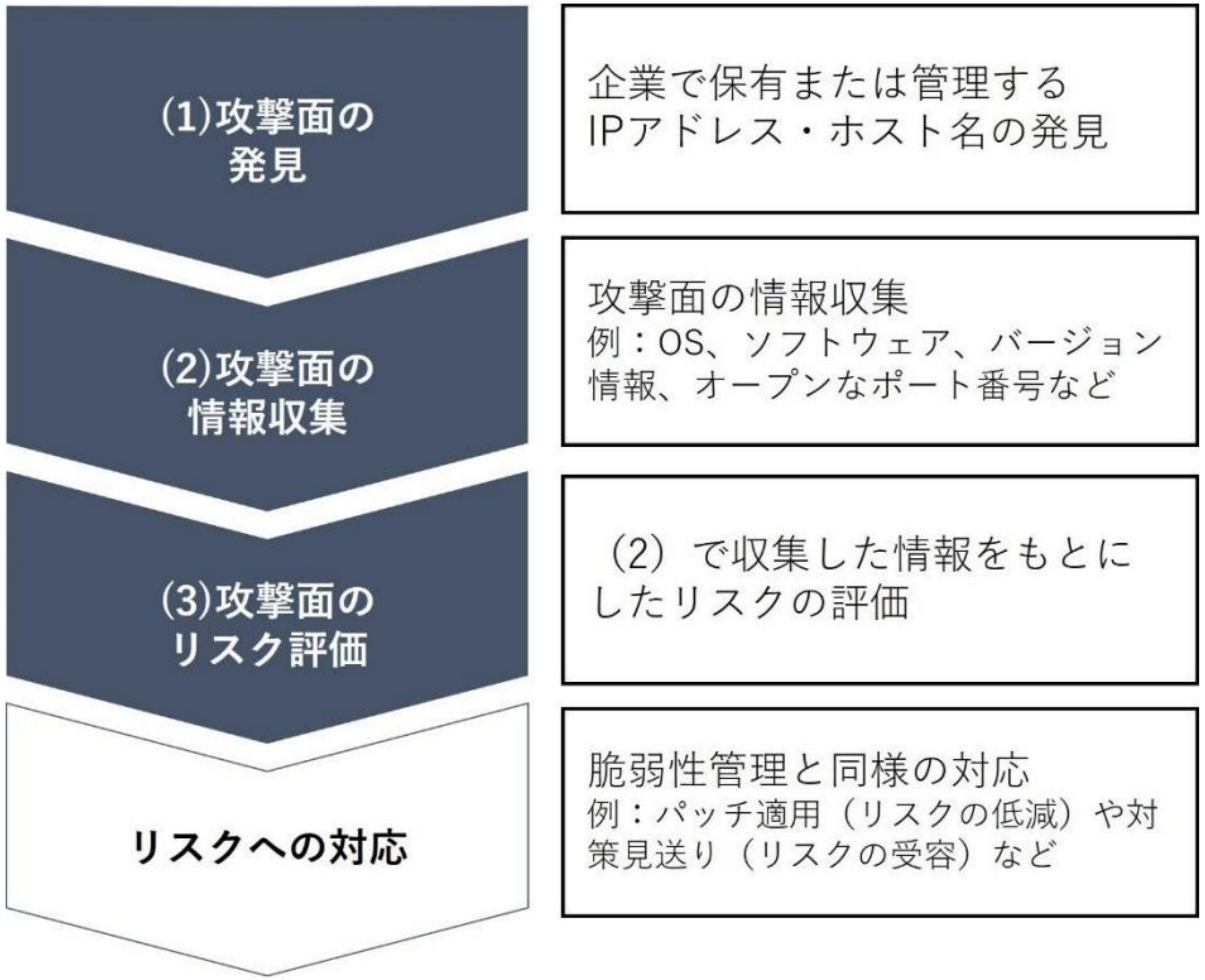
そもそもASM(Attack Surface Manegement)とは

Securify

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ください。)

※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。



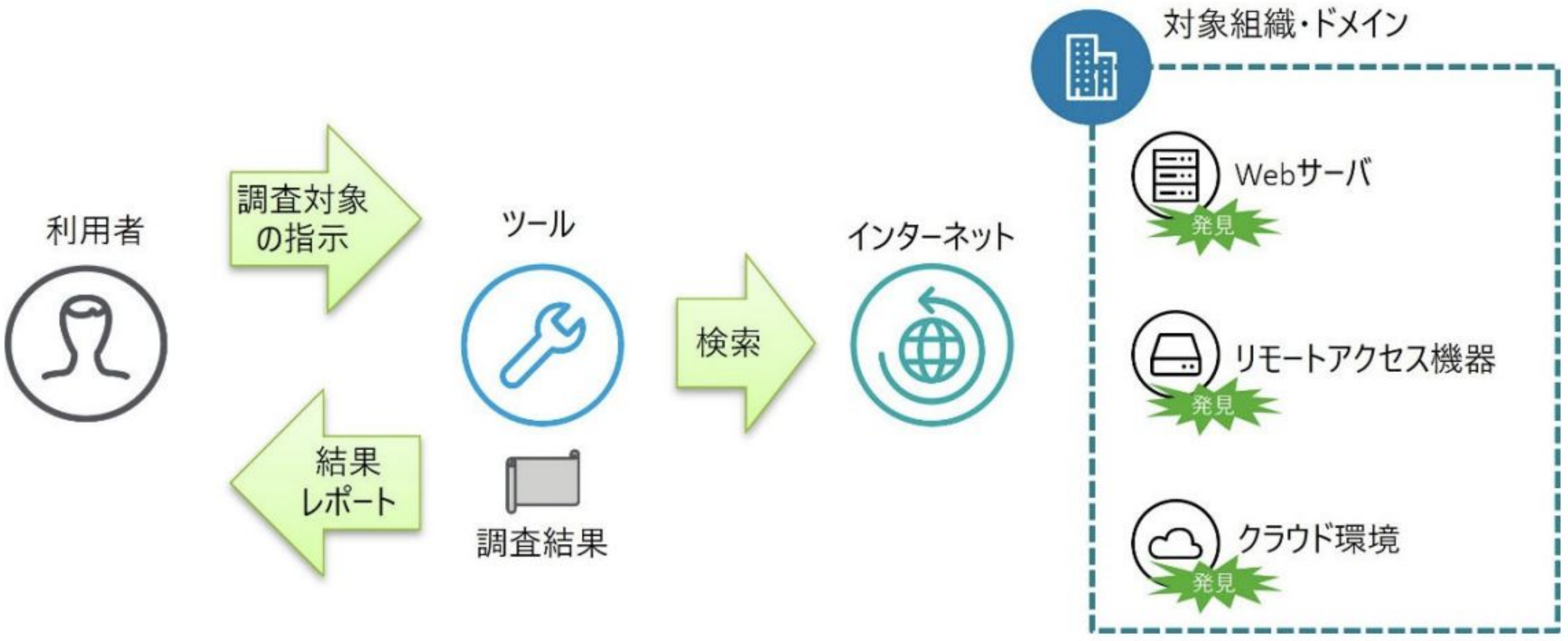
経済産業省. ASM 導入ガイダンス内 図2-1 ASMのプロセス. 2023, https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf

ASMプロセスを自動化する「ASMツール」

Securify

ASMの導入においては、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。

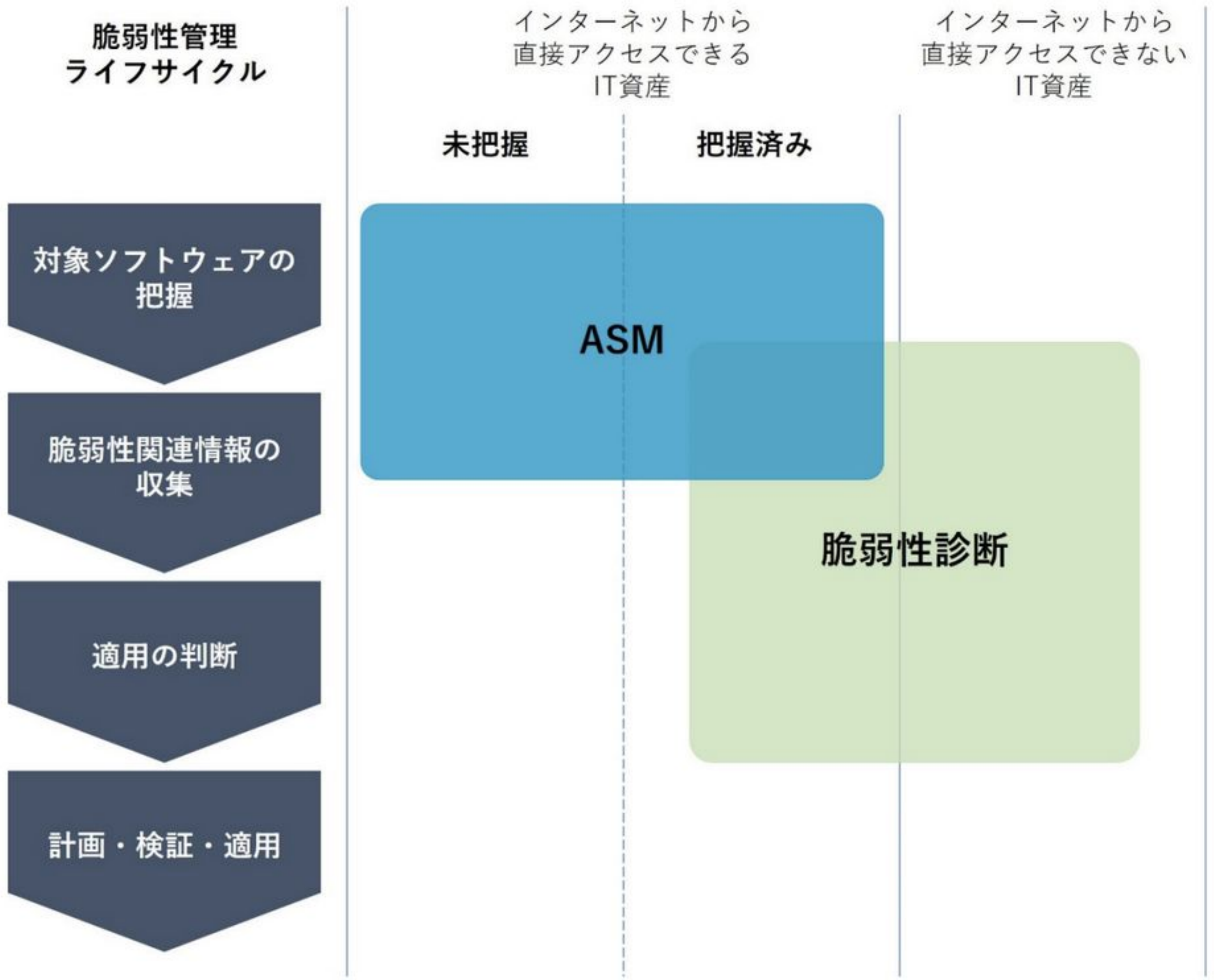
また実際の攻撃面の調査と評価には、**「ASMツール」**の利用が実質的に不可欠です。
以下図はツール利用時の動作イメージです。ASMツールの主要機能は次項に記載しております。



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

ASMと脆弱性診断の違い

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



▼主な違いや関係性は以下です ▼

	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などを対象とする	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

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. 2023, https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf

ASMと他セキュリティ製品の違い

Securify

	目的	対応する脅威	費用面	実装の柔軟性	導入コスト	学習コスト	運用負荷	適応企業の規模	コンプライアンス対応
ASM	攻撃対象の可視化・管理	IT資産の漏れや影響範囲の見落とし	中 サブスク型が主流	SaaS型が主流	低～中 定額制で迅速な導入が可能	低 ダッシュボード上で簡易に管理	低 Saas 運 用により継続的な定点監視を自動化	中～大規模企業	ISMS FISC NISC　など
CSPM	クラウド環境の設定ミス検出・修正	誤設定、脆弱なアクセス制御	中 サブスク型	SaaS型が主流	中 クラウド環境への統合が必要	中 クラウド環 境 理 解 が必要	中 クラウド環境の管理が必要	クラウドを 積 極活用する企業	ISMS FISC　など
SIEM	セキュリティログの統合と分析	高度な脅威やインシデント	高 運用・ライセンスコスト	オンプレミス型 ハイブリッド型	高 統合インフラが必要	高 分析スキルが必須	高 専 門 運 用チームが必要	大企業 政府機関	ISMS PCI-DSS NISC　など
IPS/IDS	トラフィック監視と攻撃検知	DDoS マルウェア ポートスキャン	中 ハード・ソフトの組み合わせ	オンプレミス型が一般的	中 ネットワーク設置と設定が必要	中 チューニングが必要	中 頻繁なチューニングが必要	中～大規模企業	FISC PCI-DSS　など
EDR	エンドポイントの 監視と攻撃対応	ランサムウェア マルウェア 不正アクセス	高 エージェントと 監視コスト	SaaS型 ハイブリッド型	中 全デバイスへのエージェント導入	高 インシデント対応スキルが必要	高 エージェント監 視の維持が必要	すべての規 模の企業	ISMS PCI-DSS NISC　など

ASMの概要まとめ

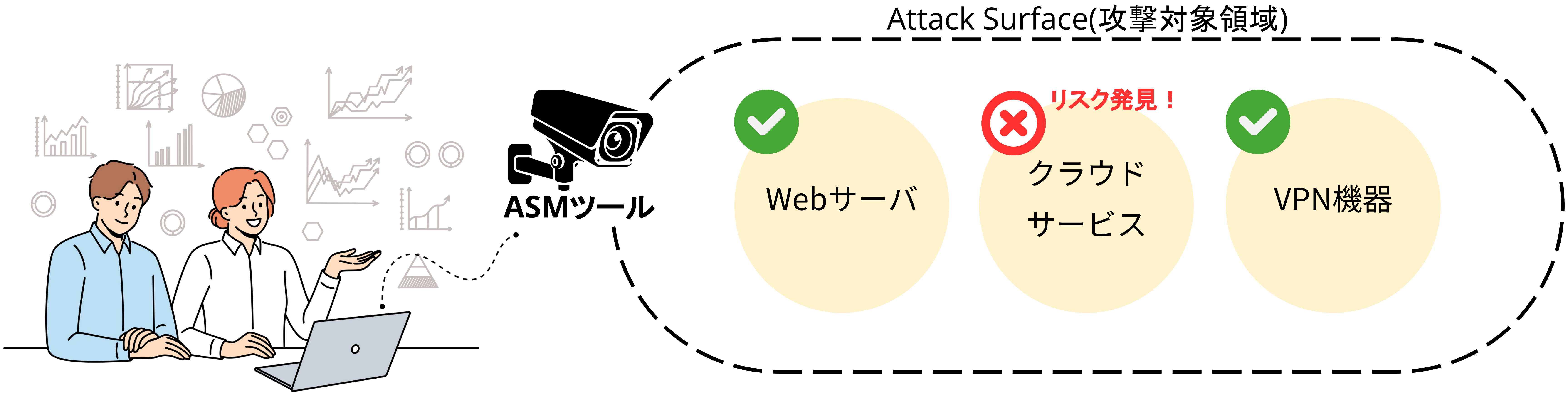
Securify

☑️ASMはサイバー攻撃から **自社の守るべき IT資産のリスクを網羅的に可視化する手法**

☑️インシデント発生時の被害コスト No1の**ランサムウェア対策として有効**

☑️IPAが2023年8月に公開した注意喚起の中でも当該ガイダンスの活用を推奨

☑️**セキュリティ対策を最適化するための初手として ASMで資産の見える化に着手しよう**



IPA(情報処理推進機構). インターネット境界に設置された装置に対するサイバー攻撃について～ネットワーク貫通型攻撃に注意しましょう～2023,
https://www.ipa.go.jp/security/security-alert/2023/alert20230801.html

導入効果

導入効果

Securify

外部公開されている IT資産の棚卸しができることによって ...

網羅的な資産把握による本質的なセキュリティ対策を実現

ASMは、従来型の棚卸し手法では見落としがちな攻撃対象領域を明確化し、真に必要なセキュリティ対策を実施できます。これにより、監査対象となるIT資産を漏れなく把握することができ、セキュリティ精度向上に繋がります。

リアルタイムなキャッチアップが可能

IT資産の変化を常に監視し、資産情報をリアルタイムに把握することができます。
そのため、最新の情報に基づいた対応が可能となり、従来のように棚卸しのために業務を止める必要もなくなります。

導入効果

Securify

セキュリティリスクがどこにあるのかわかることにより　…

放置された脆弱性の発見

旧環境のシステムや、更新が滞っているソフトウェアの脆弱性など、外部から攻撃されうるリスクの放置を避けることができます。定期的なスキャンにより潜在的な脅威を早期に発見し、必要な対策を講じることが可能です。

対処する優先順位づけが容易に

検出されたリスクの重要度や影響度に応じてスコア化することで、優先順位に基づいた効率的な対応が可能になります。限られたリソースの中で、より重要なリスクへの対策に集中することで、セキュリティ対策の効果を最大化できます。

導入効果

Securify

セキュリティ人材がいなくとも …

スピーディーな診断

ASMで行う攻撃面の発見、情報収集、リスク評価といったプロセスを手作業で行うには
専門知識と工数が必要なため、ツールを使うことが一般的です。
自動化することで、診断時間を大幅に短縮できます。

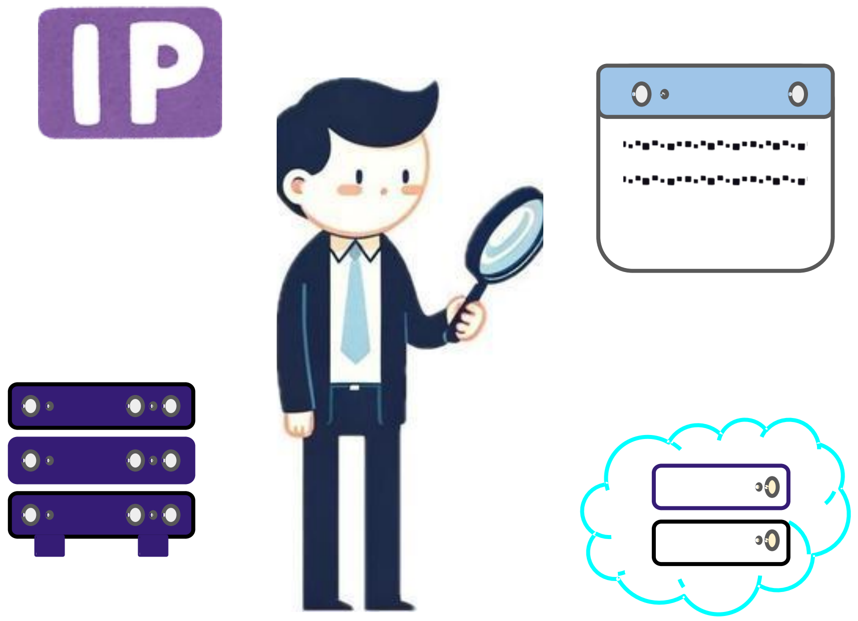
コスト削減

高額なセキュリティ人材の確保や育成に頼らずとも、
ASMツールで高度なセキュリティ対策を実現します。
セキュリティ対策に費やす時間と労力を削減し、他の業務に集中することができます。

情報システム部における ASM導入事例

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。

導入事例：ICT・エンジニアリング事業者の場合

Securify

分かりやすい管理コンソールで一元管理！

課題

- コロナ禍を経て働き方が大きく変化したことに加え、サイバーセキュリティに対する脅威がかつてないほどに高まっている状況を受け、情報システム部門としてグループ全体のセキュリティ体制強化に乗り出した。
- グループ会社ごとに規模や事業内容が異なるため、一律の対策が難しく、セキュリティレベルにばらつきが生じていた。特に、担当者のスキルやITリテラシー、対策意識の差により、全体状況の把握が困難だった。

効果

- 大きな成果は、規模の大小や国内外を問わずあらゆるグループ会社のIT資産を自動的に洗い出し、見やすいダッシュボードで一元管理できるようになったこと。
- また、属人化していたセキュリティ対策を標準化することで、担当者のスキルに依存することなく、一定レベル以上のセキュリティを維持できるようになった。

導入事例：製造業の機器販売事業者の場合

Securify

海外グループ会社の IT資産をASMで把握しセキュリティを強化！

課題

- 製造業を狙ったサイバー攻撃が後を絶たない状況の中、特に海外拠点におけるセキュリティ体制の強化が急務だと感じていた。
- 海外グループ会社が保有するIT資産の全体像をリアルタイムに把握することが難しく、効果的なセキュリティ対策を講じることができていなかった。
- 例えば、VPN機器の脆弱性が世界的なニュースとなった際も、海外グループ会社の状況把握には現地からの報告を待つしかなく、迅速な対応ができなかった
という苦い経験があった。

効果

- リスクの優先度を分類して対応できるようになった。
ASMを導入したことで、最新の情報に基づいた脆弱性診断が可能となり、迅速な対応ができるようになった点を高く評価している。
- また、想定以上の広範囲をカバーしており、資本関係の薄い会社も含めて、グループ全体の脆弱性も検出することができた。
- 限られたメンバーで広範囲にわたるグループ全体のセキュリティ対策を行うには、ASMの活用が不可欠だと感じるようになった。

導入事例：大手広告事業者の場合

Securify

今までの運用に比べ大幅なコストカットを実現！

課題

- セキュリティ専任担当がいない中で、情シス担当者が様々なクラウドリソースやオンプレミス環境を調査し、資産の棚卸しに非常に手間がかかっていた。
- 外部ベンダーへ定期的なグローバルIP診断などを行っていたが、コストが高額になってしまうためコスト削減を図りたいと考えていた。
- 適切な運用までをスムーズに行えるかとコスト最適化が鍵となっていた。

効果

- これまで人手に頼っていた外部公開資産の棚卸しが自動化されたことで、情シス担当者の負担を大幅に減らすことができ、本来の業務に集中できるようになった。
- 診断の自動化により、外部ベンダーへの依頼費用を大幅に削減できた。さらに、潜在的なリスクを早期に発見し、対策を講じることができるため、インシデント発生による損失を抑えることにも繋がっている。
- ASM導入はセキュリティレベルの向上とコスト削減の両立を実現する上で、非常に有効な手段であると実感している。

まとめ

まとめ

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 ASM」について

Securify(セキュリファイ)とは

Securify

Securify

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(Attack Surface Management)と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の提供範囲

ASM

組織内のドメインやグローバルIP、Public Cloudのアカウントを設定することで、外部公開資産の棚卸しを行います。

Webアプリ診断

Webアプリケーションの脆弱性を評価し、継続的な脆弱性診断を実現します。

SaaS診断

GoogleドライブやOneDriveといったSaaSドライブ内ファイルの公開設定状況を可視化し、情報漏洩管理の向上を実現します。

WordPress診断

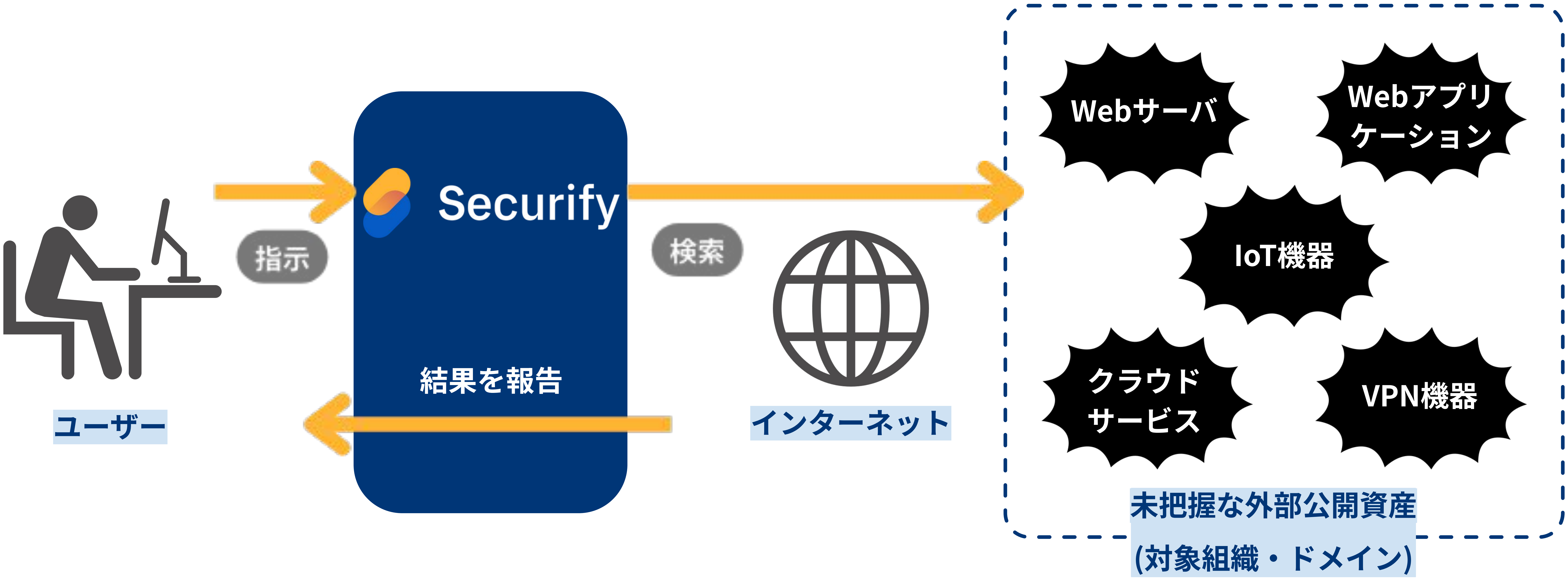
攻撃者に攻撃の糸口を与えるようなWordPressの運用上の設定を評価し、WordPressのセキュリティ向上を実現します。

棚卸しされた資産に対して高度な脆弱性診断を一気通貫で行うことができ、継続的な運用によって新たな脅威への対策を実現します。

Securify ASM(Attack Surface Management)

Securify

未把握の情報資産がインターネットに外部公開されていないかを自動で見つけます

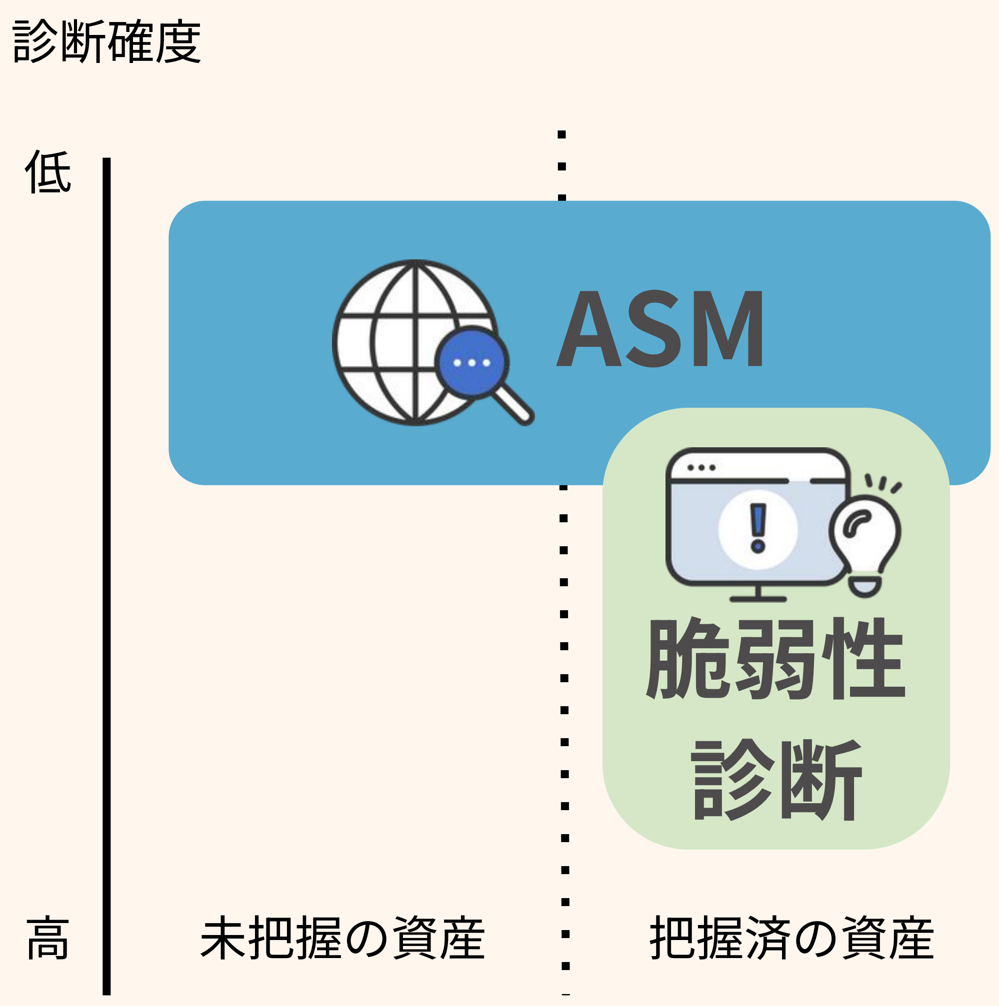


Securify Webアプリケーション(脆弱性)診断

Securify

攻撃者視点での疑似的な攻撃を行うことで

Webアプリケーションに脆弱性が潜んでいないかを診断します



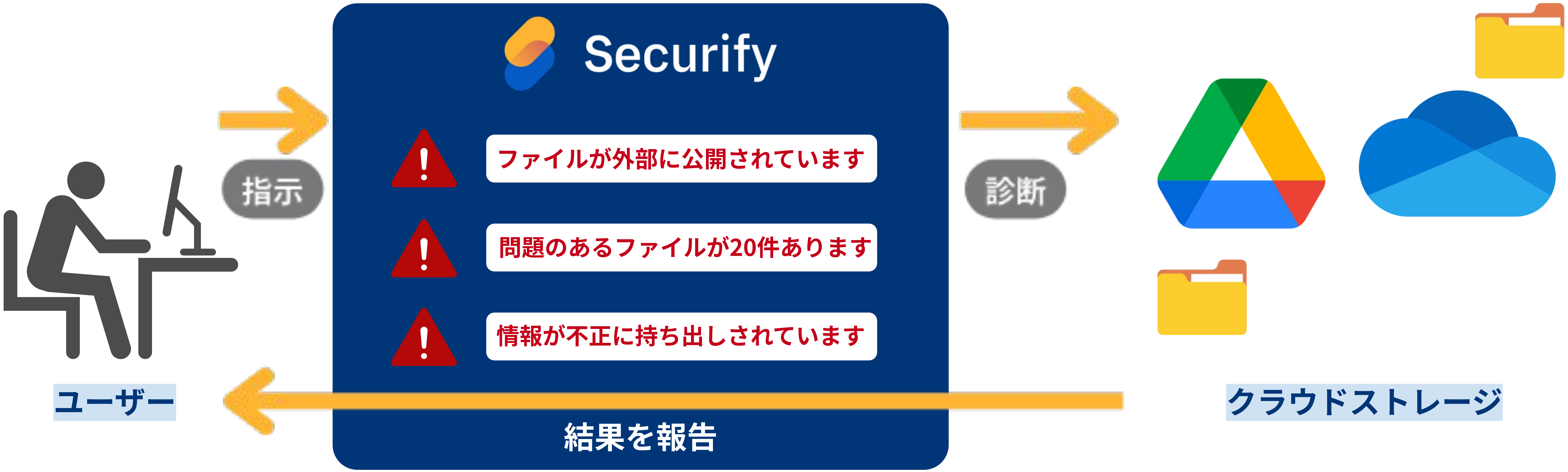
ASMと脆弱性診断は
相補関係にあります

Securify Saas診断

Securify

ドライブ上にあるファイルの公開状態を可視化し

機密情報が社外に公開されていないかを知らせます

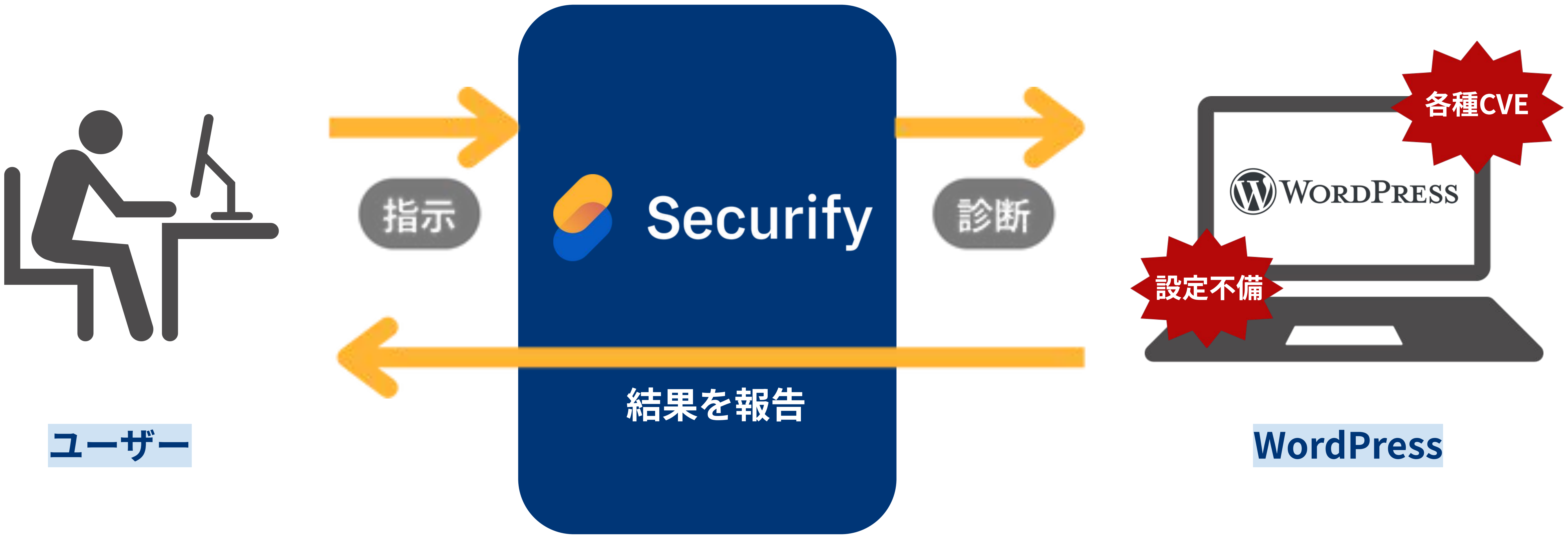


Securify WordPress診断

Securify

WordPressの設定において

攻撃者に有利な情報が公開されていないかを検知します



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位を受賞しております。

ITトレンド
「セキュリティ診断」カテゴリ 1位

経済産業相
情報セキュリティサービス基準適合

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

Securify

Securifyについて、こちらより
お問い合わせをお待ちしております！

お問い合わせはこちら CLICK