リスクセンサーご紹介

2026年5月
日本RA株式会社
営業本部

ドメイン1つで！ IT資産管理をサポート
リスクセンサー™

NRA

経済産業省　ASM(Attack Surface Management)導入ガイダンス

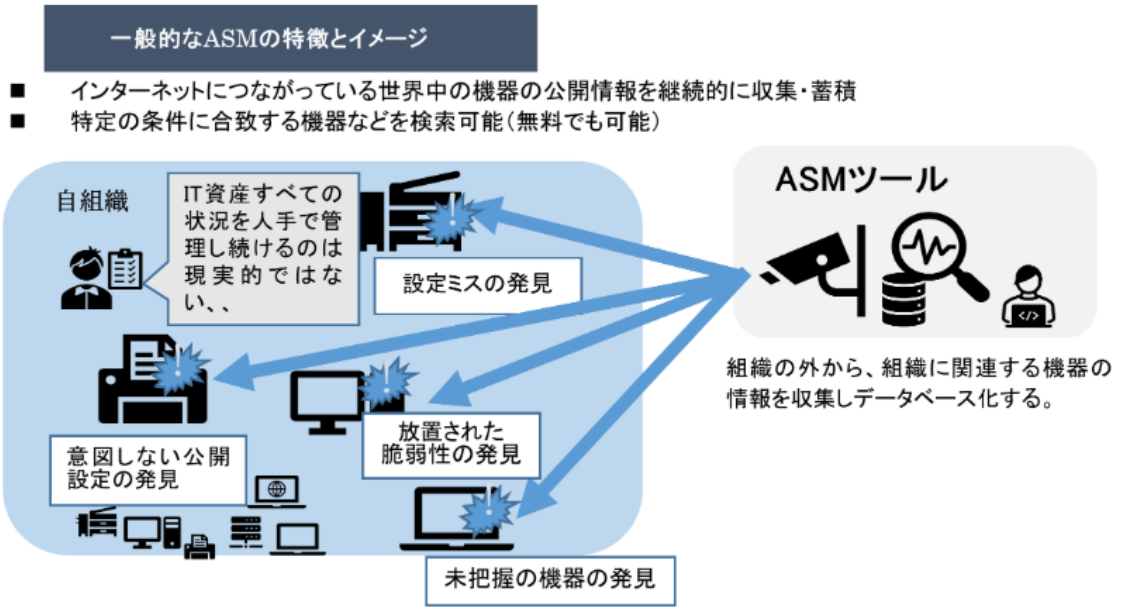
経済産業省が、サイバー攻撃から自社のIT資産を守るための手法として注目されている「ASM（Attack Surface Management）導入ガイダンスを発表

【ガイダンスの背景と趣旨（抜粋）】

デジタルトランスフォーメーション（DX：Digital Transformation）が進展する中、クラウド利用の拡大に加え、民間事業者が所有するIT資産が増加、点在するとともに、コロナ禍によるテレワークの拡大等を通じて、社会全体でリモート化が進められましたが、これらにより、サイバー攻撃の起点が増加している。

サイバー脅威に対して、自社が保有するIT資産を適切に管理しリスクを洗い出すことが求められますが、人手を介した管理の下では、システム管理部門の把握しきれないシステムが生じやすく、機器の実際の設定も見えづらいことなどから、自社の全てのIT資産を管理するのは容易ではない。

外部（インターネット）から把握できる情報を用いてIT資産の適切な管理を可能とするツールやサービスを活用して、外部（インターネット）に公開されているサーバやネットワーク機器、IoT機器の情報を収集・分析することにより、**不正侵入経路となりうるポイントを把握することが望まれる**



出典：経済産業省
https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

ASMとは

- アタックサーフェスとは、組織外の攻撃者が容易に発見できるものでサイバー攻撃に悪用されかねない領域＝すべての経路やポイントなど標的になる攻撃対象領域
- Attack Surface Managementは、組織の外部（インターネット）からアクセス可能なデジタルIT 資産の情報を調査し、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

攻撃対象領域

デジタル・アタッサーフェス

攻撃者がインターネットを通じて悪用できるもの

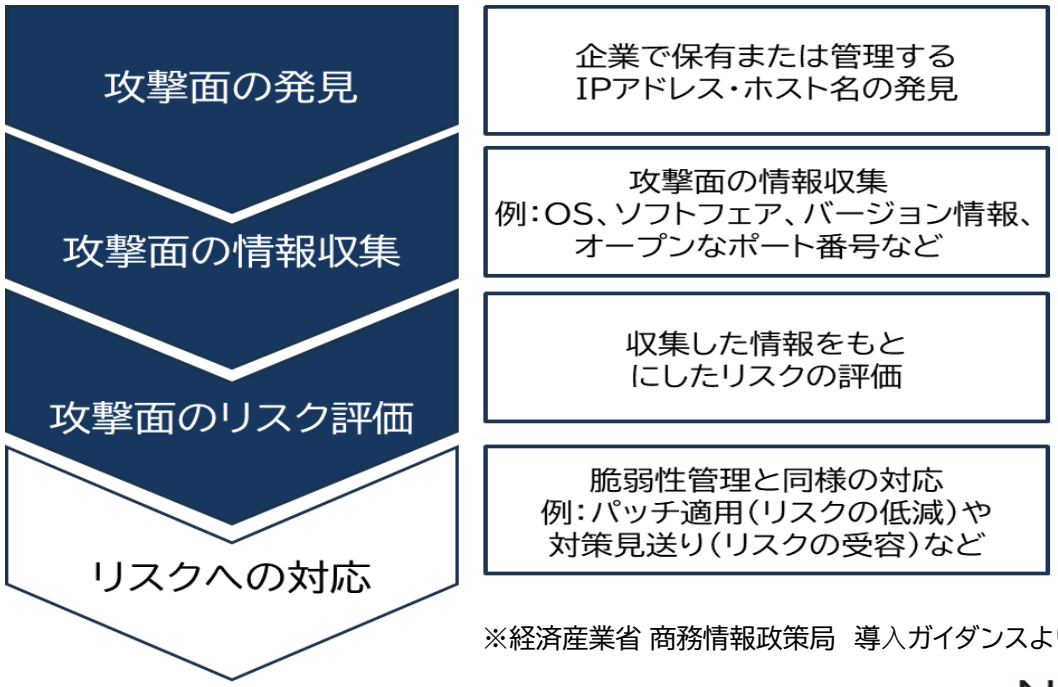
- ネットワークポート、ワイヤレスアクセスポイント、ファイアウォール、プロトコルなどの設定ミス
- 誤って公開されたクラウドサービス、データベース
- ソフトウェア、OS、ファームウェアの脆弱性
- Webサイトの脆弱性
- 閉鎖されず放置されたテスト用のサイト、退職済み職員が利用していたクラウドのアカウントなどの古い資産
- 従業員が許可なく使用しているサービスやアプリケーションなどの不正な資産

フィジカル・アタックサーフェス

物理的な手段で悪用できるもの

- 従業員や業務委託先を装ってオフィスに侵入されてしまう
- 内部からの情報漏洩
- 不適切な管理によるデバイスの紛失や盗難
- 悪意のある者がマルウェアを仕込んだUSBなどを内部者に使用させる
- 重要な書類の不適切な管理
- パスワードメモなど低いITリテラシー

経済産業省推奨ASMプロセス



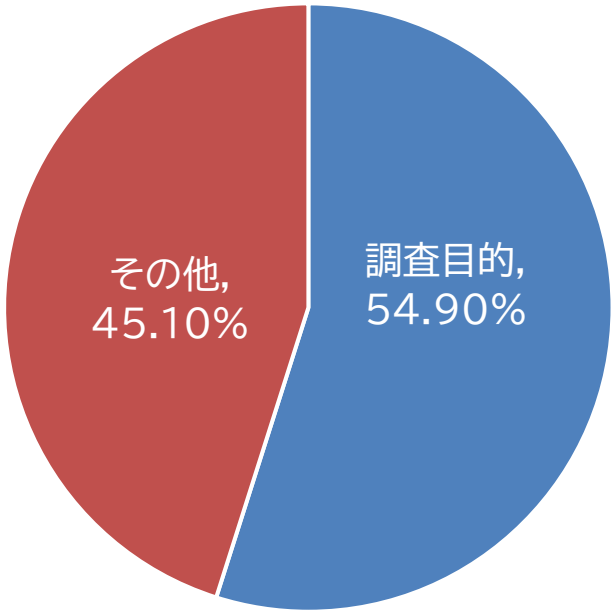
※経済産業省 商務情報政策局　導入ガイダンスより

NRA

公開情報や外部からアクセス可能なIT資産偵察の実態と攻撃事例

2022年偵察行為の実態

全パケットの約55%が偵察目的



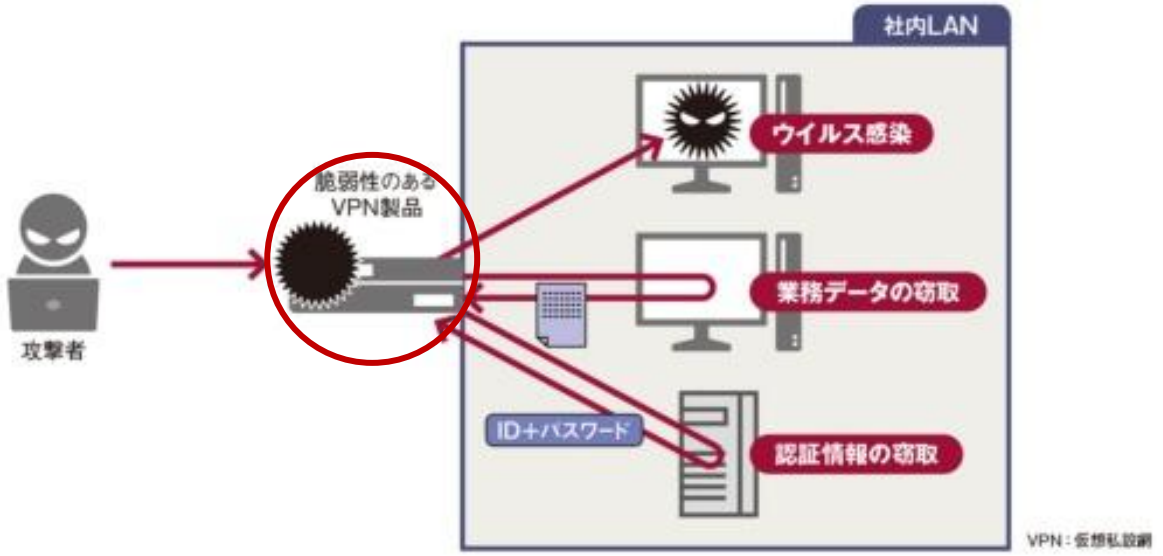
国立研究開発法人情報通信研究機構（NICT）のダークネット観測※1※2において、2022年は12,757のIP アドレスからの約2,871億パケットが調査目的のスキャンとして判定され、2022年に観測された全パケットの約54.9%を占め、悪意の有無に関わらず実際に相当数の偵察行為が行われている

※1:国立研究開発法人情報通信研究機構「NICTER 観測レポート 2022」
※2:インターネット上で到達可能かつ未使用の IP アドレス宛に届くパケットを観測する手法

サプライチェーン攻撃の脅威

日本における48%がサードパーティ経由の攻撃

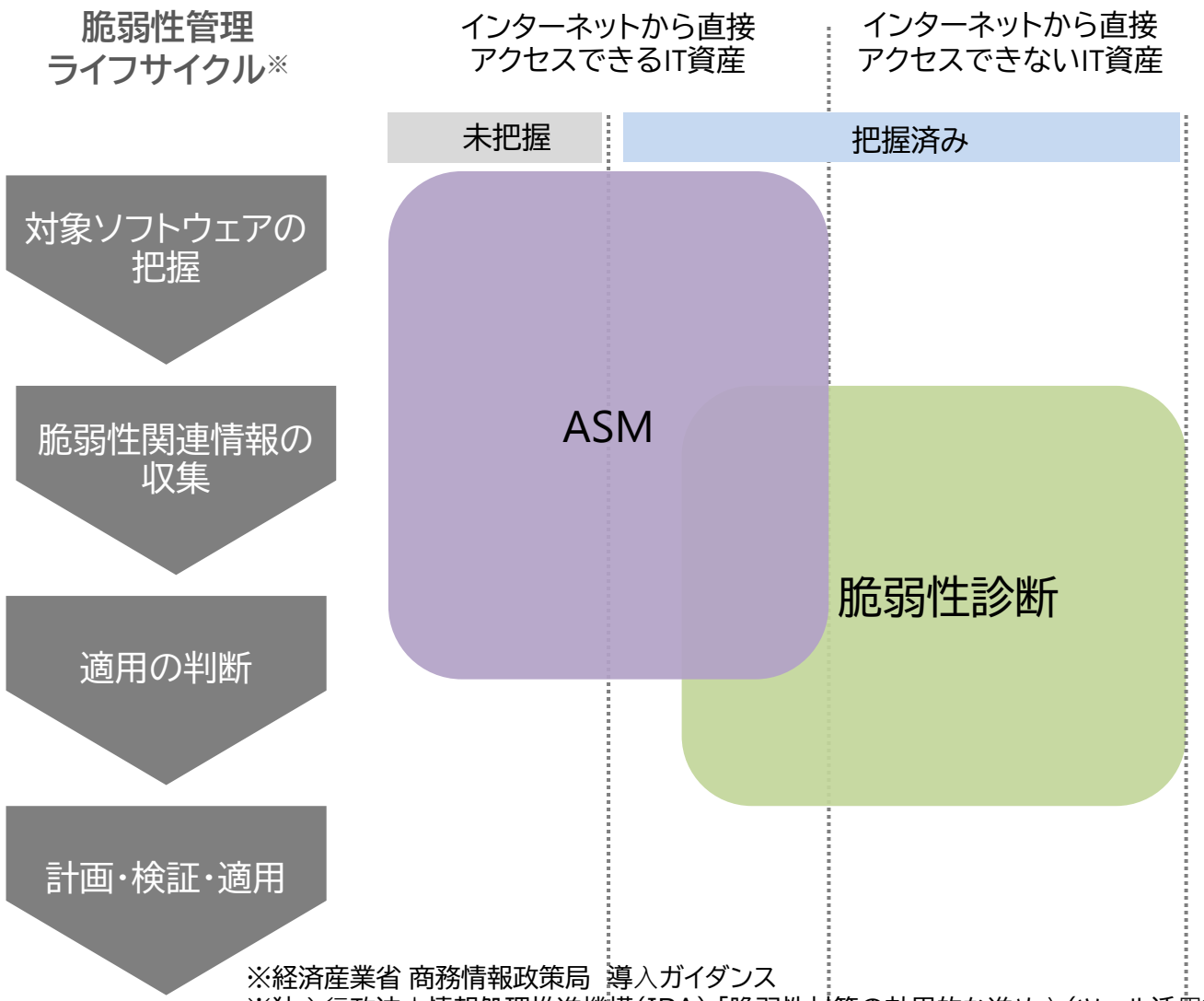
トヨタ自動車のサプライチェーン（供給網）に連なる小島プレス工業マルウエア被害



トヨタ自動車の主要取引先小島プレス工業マルウェア被害：
サプライチェーン（供給網）を支える1社のシステム障害により、14カ所の工場の28ラインが止まり、約1万3000台の生産を見送った。トヨタ自動車に加えグループの日野自動車、ダイハツ工業が被害同日の一部生産を見合せるなど広範囲に影響。
原因はVPN装置の脆弱性。従業員向けの装置と別に保守用の装置が盲点になりやすい。

※出典・引用：日経クロステック、経済産業省 ASMガイダンス、情報処理学会・象徴的な事件としては，学会誌「情報処理」
※4「サプライチェーンに起因する情報漏えいが全体の約50%を占める」（KPMG Japan調査より）

ASMと脆弱性診断の違い



※経済産業省 商務情報政策局　導入ガイダンス
※独立行政法人情報処理推進機構（IPA）「脆弱性対策の効果的な進め方（ツール活用編）6」より

ASMと脆弱性診断の違い

- **対象とするIT 資産：**
  ASM は外部（インターネット）からアクセス可能な未把握を含むIT 資産
  脆弱性診断は、既に把握済みのIT資産
- **脆弱性特定：**
  ASM は、未把握資産を含む外部公開資産を発見し、外部から特定できるリスクを検出し、IT資産に含まれている可能性のある脆弱性情報を提示するもの
  脆弱性診断は、模擬攻撃などで対象となる既に把握しているサーバに潜在するリスク調査して脆弱性を特定するもの
- **対象に及ぼす影響：**
  脆弱性診断は、調査のためのパケットがセキュリティ監視装置に検出されアラートを発報するなど、対象とするIT資産の動作に影響を与える場合があるが、ASM は対象のIT資産への影響はほとんどない

ASM と脆弱性診断では対象が異なるため
目的に応じて使い分けや併用の検討を

NRA

参考：ASMと脆弱性診断の違い

	ASM	脆弱性診断
目的	自社およびサプライチェーンの攻撃リスクの網羅的な把握と調査作業の軽減	特定のシステムにおける脆弱性の詳細な調査と特定
範囲	自社およびサプライチェーンの既知・未知を問わず、外部からのアクセスが可能な IT資産すべて	特定のシステムやサーバー
調査に必要な情報	対象企業のドメイン名、IPアドレス	対象サーバーのIPアドレスやURL
対象範囲	既知・未知を問わず、外部からのアクセスが可能な IT資産すべて	外部からのアクセス可否に関わらず、既知のIT資産のうち、任意の対象
役割	自社がサイバー攻撃者からどのように見えるかリスクを把握する	システム開発やアップデート後に詳細な脆弱性を把握し具体的な対処に役立てる
利用頻度	定期的	任意のタイミング

ASMツールとスキル

ASMを実現するには、攻撃者目線に立ち、自社で未把握のIT資産を含め、自社が公開しているIT環境のアタックサーフェスを網羅的に把握することが重要

ASM の活用に必要となる知識とスキル

■ 情報セキュリティの知識

情報セキュリティ、情報セキュリティ管理、情報セキュリティ対策、セキュリティ実装技術、セキュリティ関連法規、ネットワーク方式、データ通信と制御、通信プロトコル、情報資産管理の計画、情報セキュリティリスクアセスメント及びリスク対応、情報資産の管理、部門の情報システム利用時の情報セキュリティの確保、情報セキュリティに関する動向・事例情報の収集と評価

■ ヒューマンスキル

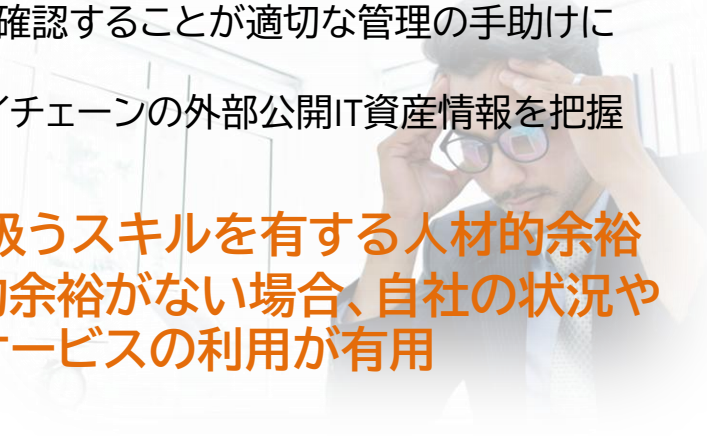
ASMの管理者は発見した脆弱性を関係者に報告する役割を担うことが想定されるため、コミュニケーションスキルやレポーティングスキルが求められ、公開される最新の脆弱性情報は一次情報が英語であることが多く英語情報を読み解くスキルを持つことが望ましい

■ 組織・体制の知識

組織体制の知識、システム構成やアーキテクチャの知識、自社で定めたセキュリティポリシーやルールに関する知識

ASMツールによって

- 申告ベースでIT資産を管理している場合、申告漏れや誤認などが発生するリスクがあり、攻撃者視点で実態ベースでIT資産を探索・発見し、従来のIT資産管理と併用することで精度向上やリスク管理の高度化を実現可能
- 把握しているつもりの自社IT資産情報には、部門が独自に導入したクラウドサービスや管理不十分で放置されているサーバなど未把握の資産が見つかるケースもあり重大なインシデント発生に及ぶことがあります。そのため定期的に脆弱性診断を実施している企業でも外部からどのような情報が見られているかを確認することが適切な管理の手助けに
- 委託先・提携先を含むサプライチェーンの外部公開IT資産情報を把握



自社内にASM ツールを扱うスキルを有する人材的余裕や導入を検討する時間的余裕がない場合、自社の状況や目的に合わせて、ASM サービスの利用が有用

NRA

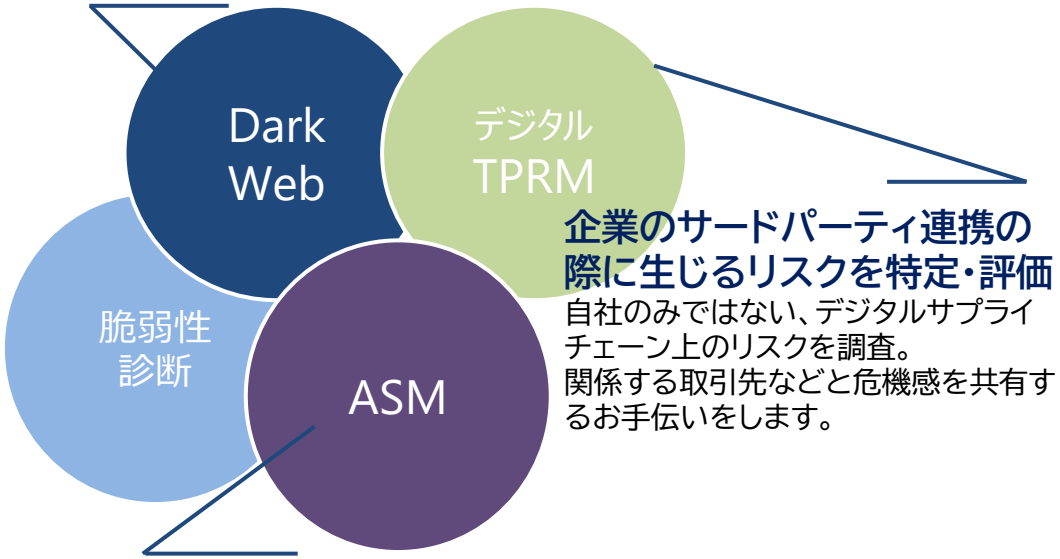
リスクセンサー

ASM＋デジタルTPRM＋脆弱性診断に関するスキャンからDarkWeb調査まで、専門家による詳細調査を経て、把握できていなかった危険性や脅威を可視化したレポートを行うサービス

- PIPELINE株式会社のリスクセンサーは、脆弱性や緊急性を**社名と企業ドメインなどの基本情報だけで診断できる日本国内の企業向けに開発された純国産製品**
- 導入企業実績100社超、プライム上場企業の採用増加中
- **ハッカー目線**で、対象が外からどう見えているか、脆弱性や攻撃リスク、漏洩した情報の検出など**見えない不調を可視化**
- 診断後に提出されるレポートは、経営層など情報システムの細部までご理解されていないステークホルダーへ、サイバー攻撃リスクと対策の重要性を社内共有することを考慮し、スコア形式のわかりやすさを重視した構成
- サイバー攻撃対策としてどこから着手してよいかわからないなど、ITセキュリティ担当者がいない組織でも**現状を分析を実施して必要な対策について把握する支援**

サイバーセキュリティインシデントを特定し軽減するための専門的な調査

PIPELINE社は、世界中の業界をリードする脅威インテリジェンスに関連する企業とパートナーシップを結んでおり、国内企業に合わせた脅威インテリジェンスデータから調査します。



企業のサードパーティ連携の際に生じるリスクを特定・評価

自社のみではない、デジタルサプライチェーン上のリスクを調査。
関係する取引先などと危機感を共有するお手伝いをします。

脅威ハンティングと攻撃対象領域スキャン

経験豊富なサイバーセキュリティ専門家チームが、高度な脅威ハンティング手法を採用して、隠れた脆弱性や悪意のある活動を特定します。
サイバー犯罪者の一歩先を行くことで、お客様のビジネスに不可欠な資産を保護するお手伝いをします。

NRA

リスクセンサー導入までの流れ

簡単3ステップ

1 注文書と申込書のご提出

申込書と利用規約をお送りしますので、申込書にスキャン対象となるドメイン名またはグローバルIPアドレスを含む必要事項をご記入いただき、ご注文書と合わせてご提出いただきます

2 スキャン実施

申込書記載のスキャン実施ご希望日にスキャンを実施します

※受付後、PIPELINE社稼働日の都合から実施日に関してご調整いただくことがあります

3 評価レポート納品

スキャン完了後1週間程度でレポートを納品します

※レポートは申込書記載のご担当者様へ電子メールでお送りします
※レポート納品完了後、ご請求書を送付します

NRA

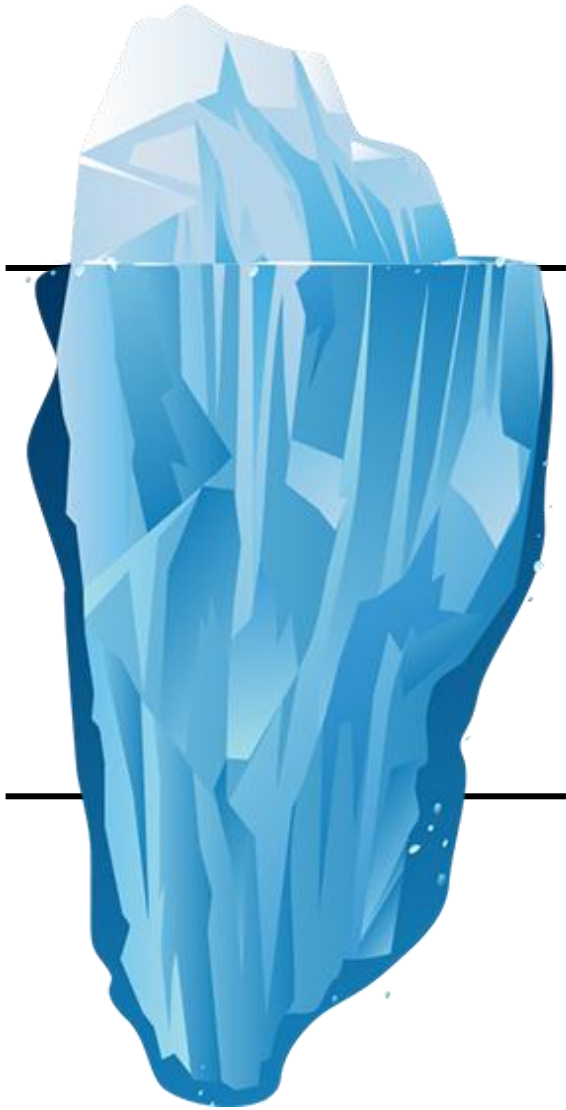
リスクセンサー他社比較

診断項目		A社	B社	C社	リスクセンサー	
リスクスコア		○	○	○	○	報告レポートは課題提示だけでなく セキュリティアップも望めるよう リスク緩和行動も併せてご報告！ 社内チームや弊社にご依頼、 外部連携先へお渡しで対処OK
セキュリティ課題	洗い出し	○	○	△ 項目選択式	○	
	想定リスク	○	△	○	○	
	リスク緩和の推奨事項	○	×	×	○	
脆弱性診断	WEBサーバー	△ オプション	△	△ オプション	○	一部脆弱性診断も兼ねています
被害	ダークウェブ流出可否	△ オプション	？	○	○	細かく難しい設定も必要なく レポート発行時に自動で検出！ フォーラム内メンションもカバーで Darkwebスキャンでもリスク把握
	ダークウェブ漏洩内容	×	？	△	◎	
サイバー保険	追加可否	？	？	△ オプション	△ オプション	ご希望の場合にはご案内可能です
従業員向け訓練		○	×	×	△	レポートで洗い出された実際の被害 リスクを社内フィードバック
開発国	日本か否か	×	×	×	○	純国産は弊社だけ！ 日本に向けて開発しました！
相談窓口	結果に伴う相談	△	×	×	○	課題解決まで伴走できるよう 説明会付きプランもございます
	説明会／定例会	×	×	○	△ オプション	

NRA

ダークウェブ

攻撃対象は見えない場所にある



サーフェイスウェブ　4%

インターネットに接続するだけでアクセスでき、検索エンジンで見つけられるデータ

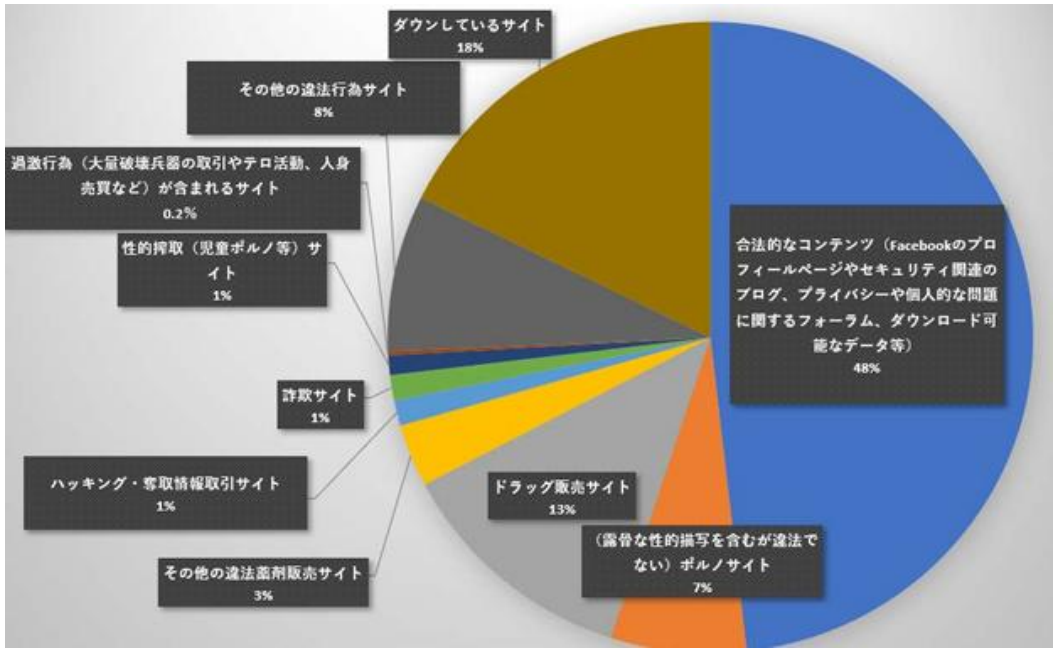
ディープウェブ　90%

一般的な方法でアクセス可能だが、パスワードなどでアクセスが制限されていて、検索エンジンで見つけられないデータ

ダークウェブ　6%

有用なサイトもあるが匿名性が提供されるため、悪意を持った第三者、違法な取引場所

onionサイトに占める違法・合法コンテンツの割合

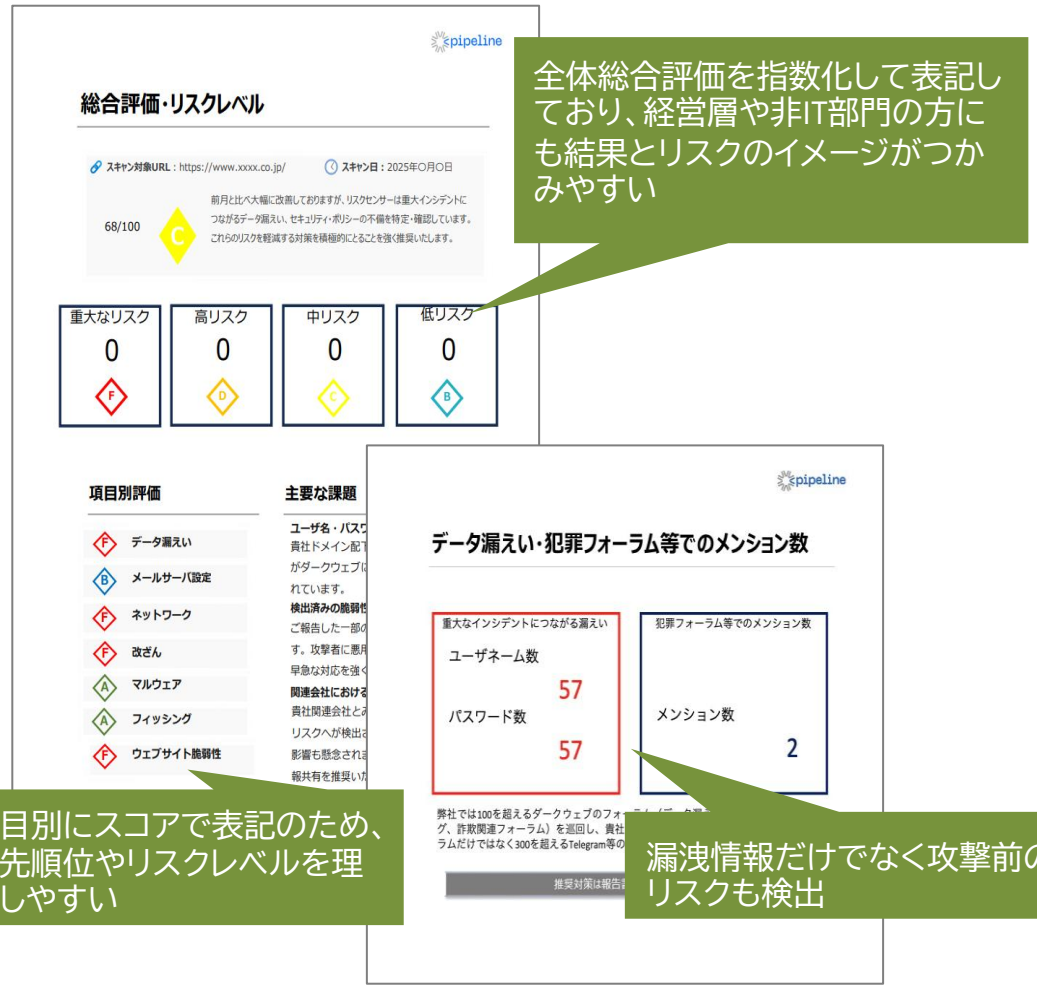


- フィッシング攻撃などに成功したサイバー犯罪者は、盗んだアカウントを自ら利用することはなく、ダークウェブ上で他の犯罪者に転売されている
- 幅広いランサムウェアパッケージが販売されている
- 世界のサーバ ーにアクセスするログイン情報を販売するサービスが提供されている
- スパム メールの送信やDDoS攻撃の実行のためのコンピューター機能をダークネ ット上で貸し出す例もある

※IPA独立行政法人情報処理推進機構「ダークウェブに関する現状」より引用

リスクセンサー評価レポートイメージ

対象ドメインの評価・漏洩情報・良好項目の詳細

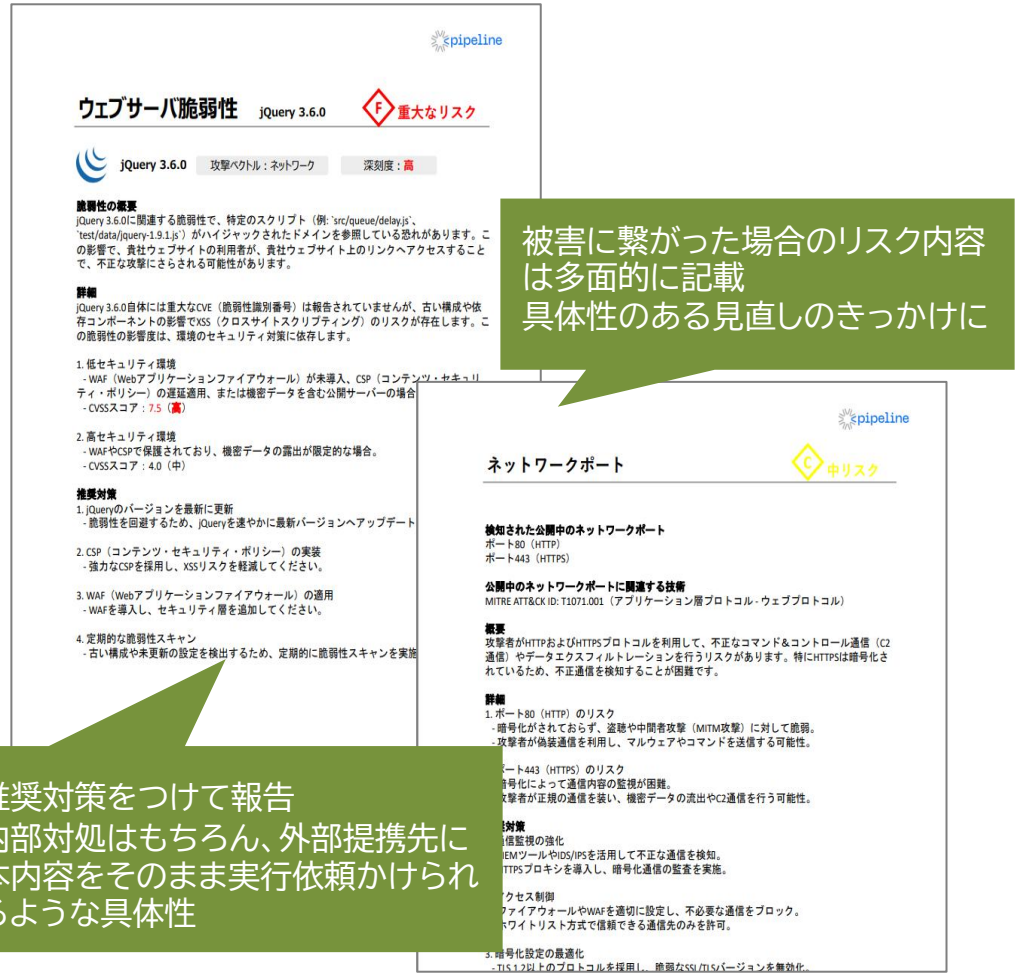


全体総合評価を指数化して表記しており、経営層や非IT部門の方にも結果とリスクのイメージがつかみやすい

項目別にスコアで表記のため、優先順位やリスクレベルを理解しやすい

漏洩情報だけでなく攻撃前の標的リスクも検出

課題や推奨される対策などのご報告



被害に繋がった場合のリスク内容は多面的に記載
具体性のある見直しのきっかけに

推奨対策をつけて報告
内部対処はもちろん、外部提携先に本内容をそのまま実行依頼かけられるような具体性