

外部からの侵入を未然に防ぐ
WideAngle ASMのご紹介



2025年12月5日

NTTドコモビジネス株式会社

「WideAngle」はNTTドコモビジネスが提供する
グローバル統一の総合セキュリティサービスブランドです



WideAngleという名称には、標的型攻撃など未知の脅威に世界がさらされる中、
広い視野でリスクを見通し、より安心・安全な社会を志す開拓者でありたいという思いを込めています。
NTTドコモビジネスは、WideAngleブランドのもと総合リスク マネジメント サービスを積極的に展開し、
マネージド セキュリティ サービス プロバイダー（以下MSSP）のグローバル トップ プレイヤーを目指します。

Attack Surface Management (ASM) とは



ASM = Attack Surface Management

インターネット(攻撃者)側から見える**IT資産を可視化**
さらに、OSINT情報等から、野良サーバー、設定ミス、**脆弱性を検出**するツール

2023年に経済産業省がガイダンスを発行するなど、最近注目を集めている
サプライチェーン、グループ会社のガバナンス強化にも活用できる



経済産業省
Ministry of Economy, Trade and Industry

申請・お問合せ English サイトマップ 本文へ 文字サイズ変更 小 中 大 アクセシビリティ 閲覧支援ツール

ニュースリリース 会見・談話 審議会・研究会 統計 政策について 経済産業省について

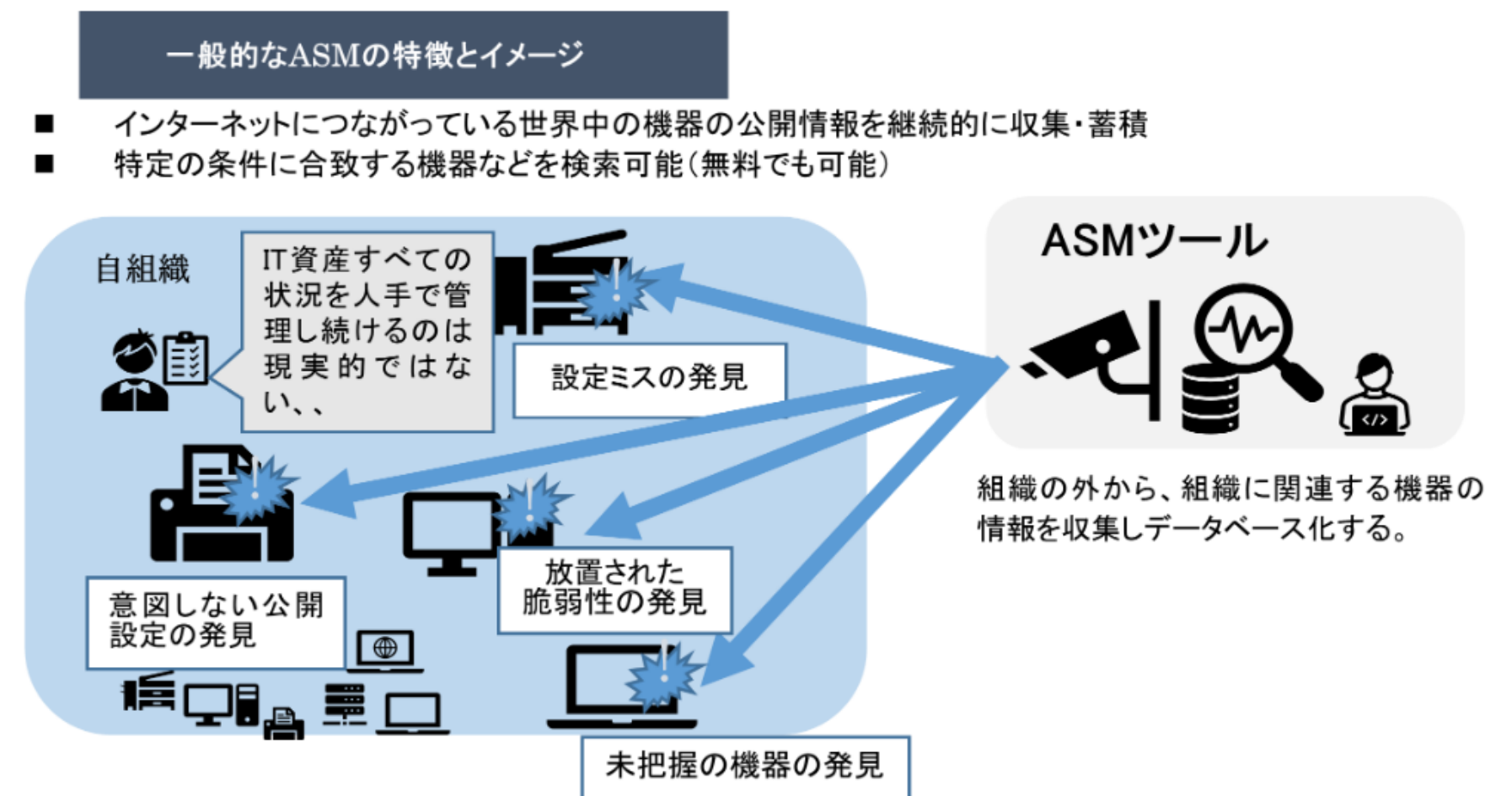
ホーム ▶ ニュースリリース ▶ ニュースリリースアーカイブ ▶ 2023年度5月一覧 ▶ 「ASM (Attack Surface Management) 導入ガイダンス～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」を取りまとめました

「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年5月29日

▶ 安全・安心

経済産業省は、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)」について、自社のセキュリティ戦略に組み込んで適切に活用してもらえよう、ASMの基本的な考え方や特徴、留意点などの基本情報とともに取組事例などを紹介した、「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～」を作成しました。



出展) 経済産業省

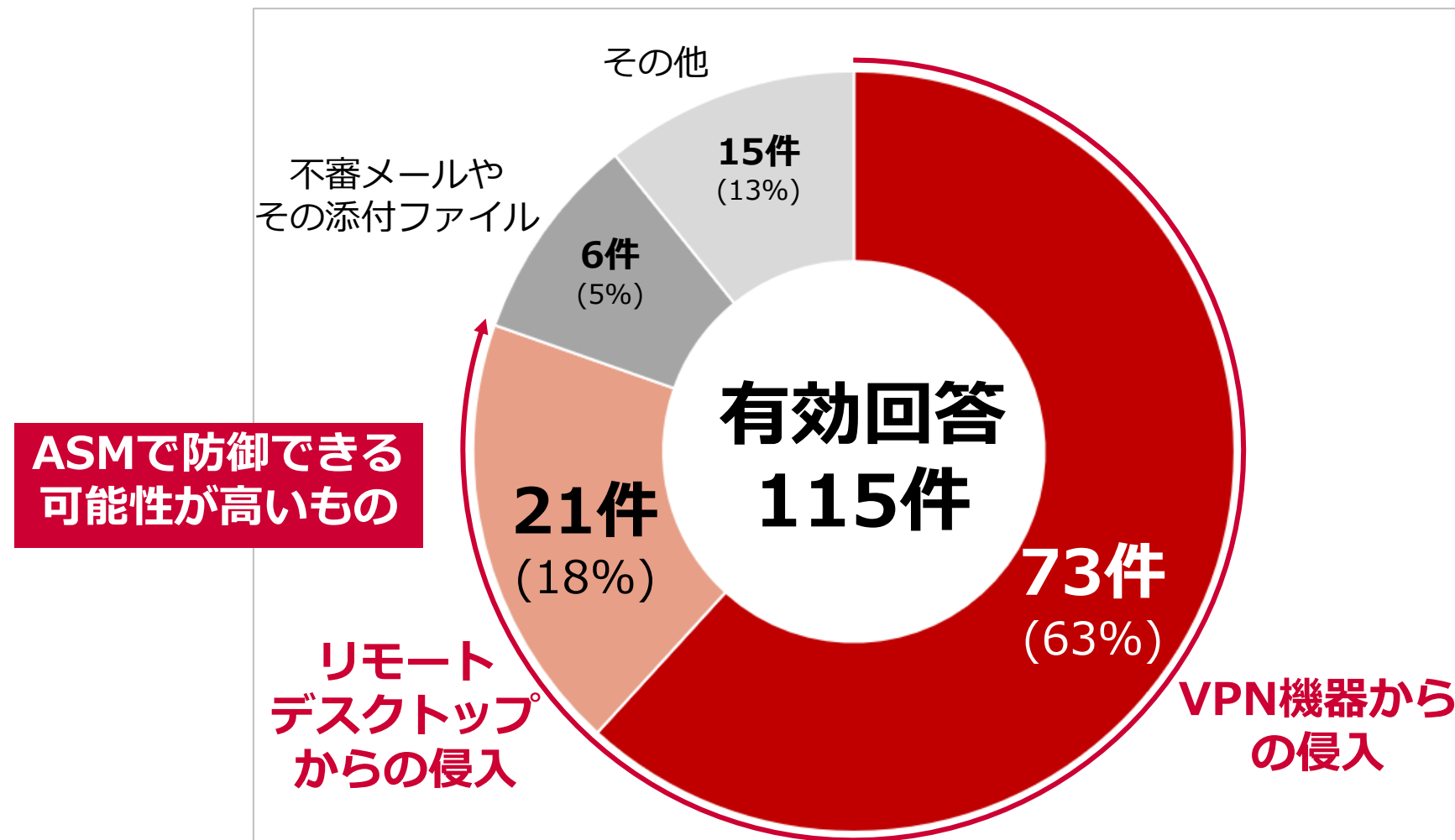
<https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html>

最近の セキュリティインシデント傾向と その原因



セキュリティインシデントの傾向

- 現在、サイバー攻撃の起点として最も多いのは、**VPN機器からの侵入**である。自社のVPN機器を確実に把握し、脆弱性に対するパッチを確実に当てることが重要。最新の脆弱性情報を継続的に入手し、評価できる体制が必要。
- また、海外の**管理できていないWeb/DNSサーバー**や、適切に管理されず**脆弱性が内在するサーバー**が意図せず、攻撃の入り口になるケースが多発している。



出展) 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
をもとにNTTドコモビジネスで一部編集し作成

日本経済新聞

お申し込み 未登録

朝刊・夕刊 LIVE Myニュース 日経会社情報 人事ウォッチ NIKKEI Prime

トップ 速報 ビジネス マーケット 経済 国際 オピニオン もっと見る

国内企業、海外拠点サーバーに「穴」 古いOS放置

サイバー防衛 +フォローする

2022年7月28日 2:00 [会員限定記事]

保存

企業が所有するサーバーにサポート期限切れの古いソフトウェアが使われ、サイバー攻撃に脆弱な状態となっている。日本経済新聞が売上高1000億円以上の国内企業から50社を無作為に抽出してセキュリティー会社と調べたところ、7割超（37社）がメーカーのサポート期限が終わった古い基本ソフト（OS）を搭載したサーバーを使い続けていた。特に海外拠点のサーバーの管理を怠る例が目立った。

出展) 日経新聞

セキュリティインシデント事例

つながろう。驚きを。幸せを。

 NTT docomo Business



情報セキュリティインシデント調査委員会報告書について

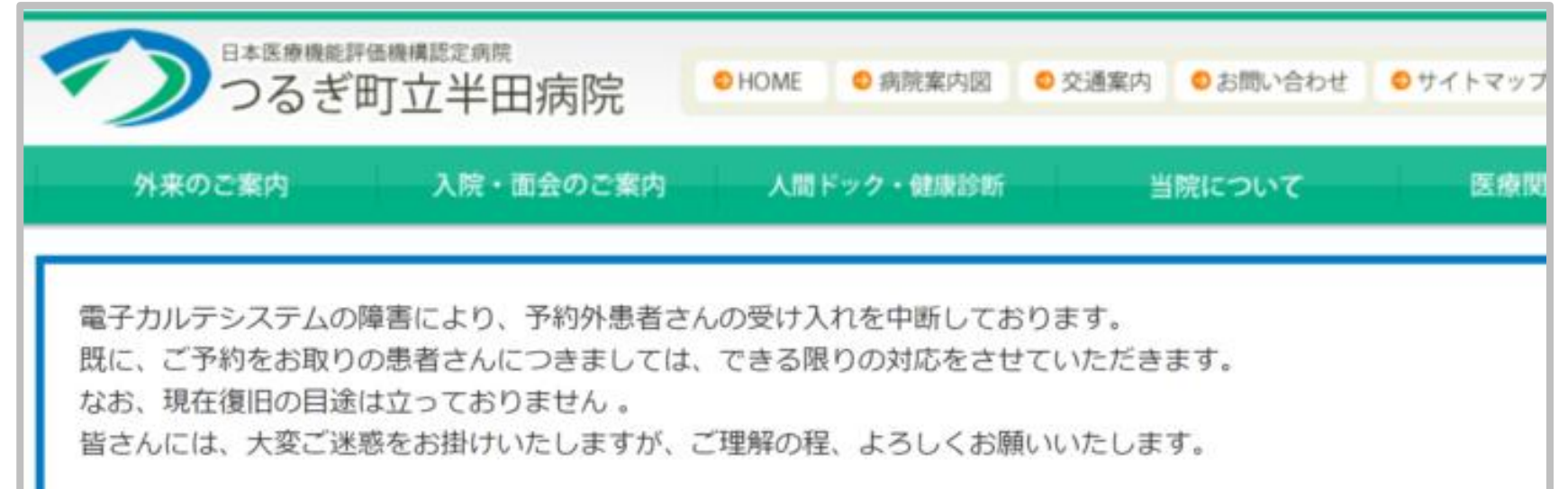
名古屋港コンテナターミナル システム障害



小島プレス工業からのお知らせ

2022.03.31

ウィルス感染被害によるシステム停止事案発生のお知らせ（第2報）



日本医療機能評価機構認定病院
つるぎ町立半田病院

HOME 病院案内 交通案内 お問い合わせ サイトマップ

外来のご案内 入院・面会のご案内 人間ドック・健康診断 当院について 医療関係

電子カルテシステムの障害により、予約外患者さんの受け入れを中断しております。
既に、ご予約をお取りの患者さんにつきましては、できる限りの対応をさせていただきます。
なお、現在復旧の目途は立っておりません。
皆さんには、大変ご迷惑をお掛けいたしますが、ご理解の程、よろしくお願いいたします。

これらの事例は、攻撃者の**VPN機器経由からの侵入**を許し**ランサムウェアに感染**、重要システムが暗号化され、**業務が停止**に追い込まれています。

セキュリティインシデント事例

つながろう。驚きを。幸せを。



これらの事例は、攻撃者の**VPN機器経由からの侵入**を許し**ランサムウェアに感染**、重要システムが暗号化され、**業務が停止**に追い込まれています。

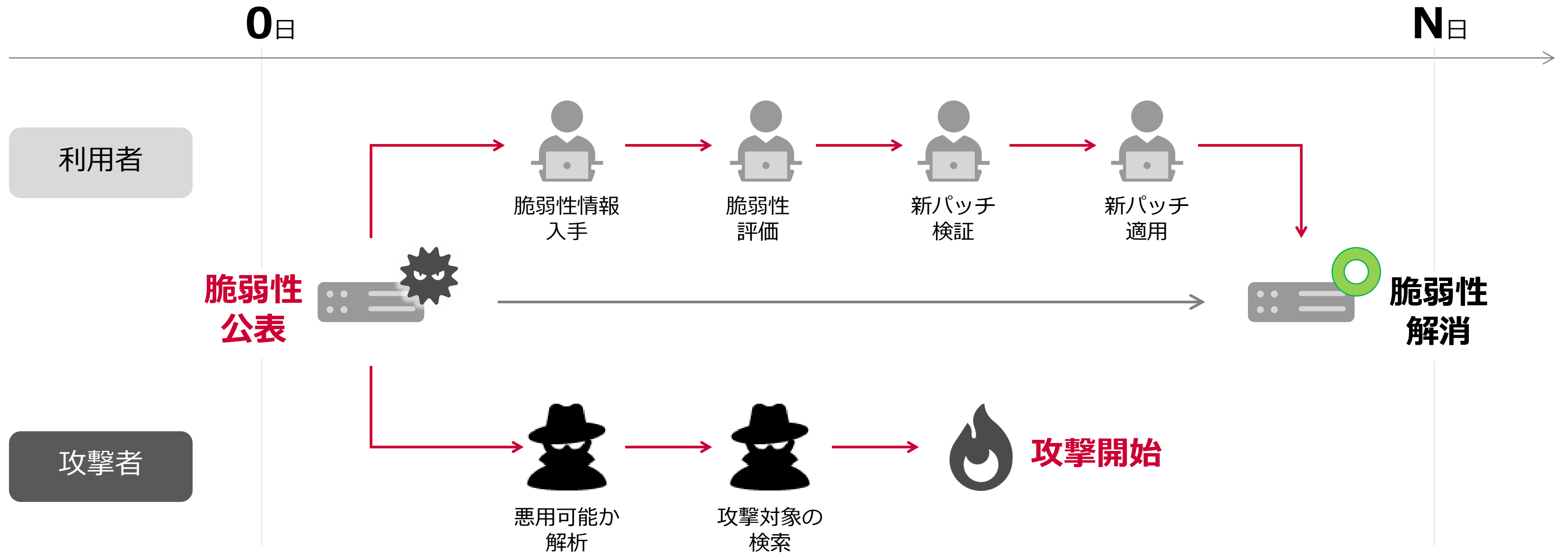
企業名	時期	原因 (VPN機器の脆弱性)	ランサムウェア 感染	サプライチェーンへの 影響
徳島県つるぎ町立 半田病院	2021年10月	Fortigate(保守用VPN 機器)の 脆弱性	感染	2か月 医療機関の停止
小島プレス工業	2022年3月	子会社VPN 機器の 脆弱性	感染	トヨタ工場停止 1日
大阪急性期・ 総合医療センター	2022年10月	給食事業者 のFortigate (VPN機器)の脆弱性	感染	2か月 医療機関の停止
名古屋港 コンテナターミナル	2023年7月	保守用VPN 装置の 脆弱性	感染	物流インフラの遅延 3日

攻撃者の視点と攻撃手法



攻撃者の視点

- 攻撃者は、脆弱性を悪用し、**パッチが適用される前の機器**を狙います。（Nデイ攻撃）
- **定期的なモニタリング**を行い、VPN機器に限らず（サーバーやWindowsのOSも含め）脆弱性が公表されたら、特にCriticalなものは、迅速にパッチを当てて脆弱性を解消しておくことが重要です。



攻撃者は**様々な公開情報を収集**し、お客様の資産を攻撃できないかと狙っています。
攻撃者と同じ目線で自社の弱点を把握し、予め対策することが必要です。

⇒Attack Surface（攻撃される可能性がある場所）を**継続的に管理**し、対策することが重要

攻撃者のアプローチ

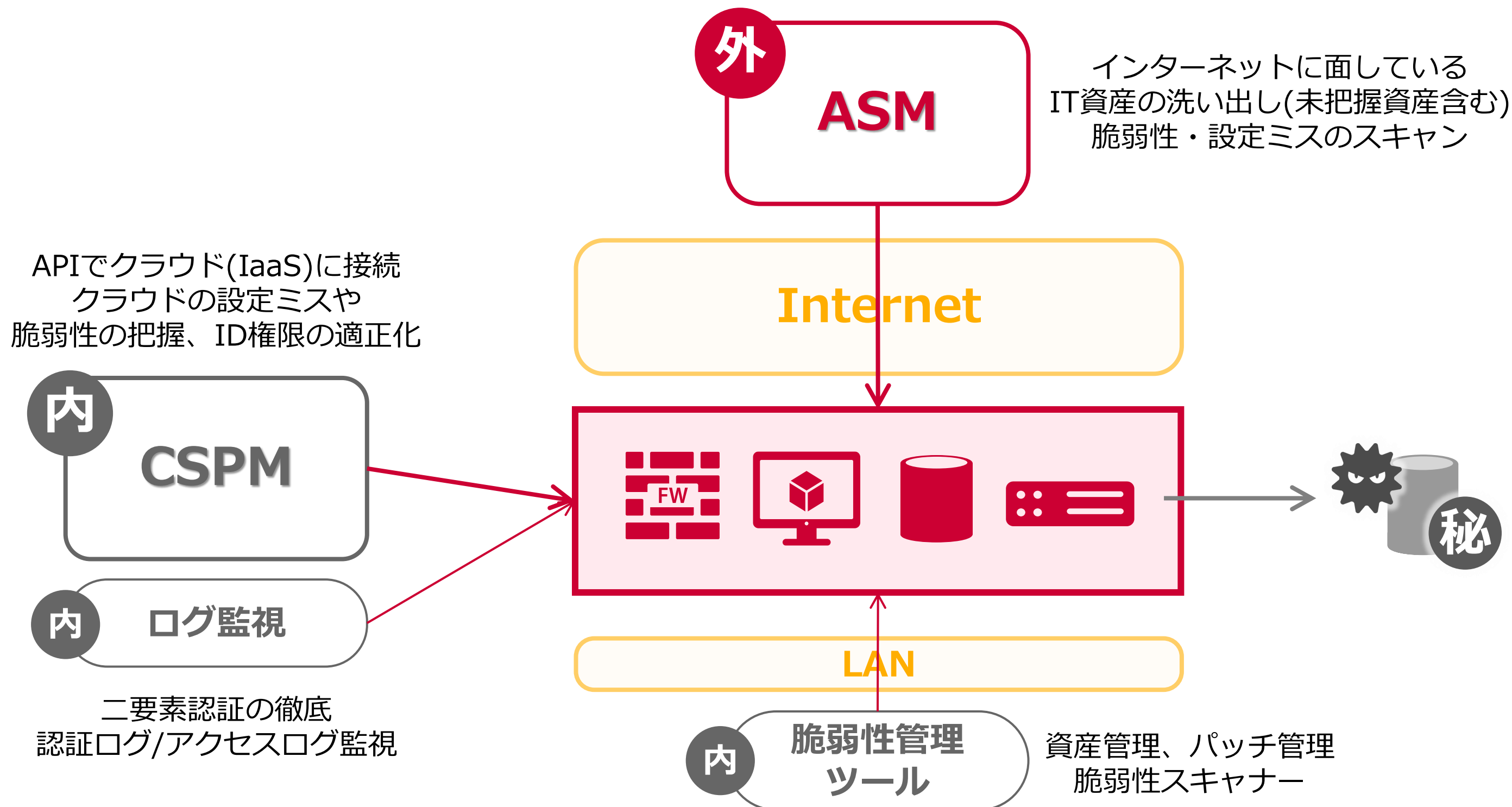
- 1 脆弱性が悪用できるか調査する
 - 2 漏洩しているパスワードを入手
 - 3 開いているポート(入り口)を探す
 - 4 脆弱性が放置されたサーバー/VPN機器を探す
- 攻撃手法を確立する
- 攻撃対象を探す

Attack Surfaceを守るには
- **ASM**とは -



Attack Surfaceを守るために。

- 設定ミスや脆弱性を確実に解消し、攻撃されにくい環境を実現する(入り口をふさぐ)には、**外側(攻撃者)視点のASM**を組み合わせて活用することが効果的です。



ASMの位置づけ

- ASMは**攻撃者と同じ視点**で、お客さまのIT資産を偵察し、攻撃可能な糸口を探します。攻撃可能なIT資産の**脆弱性を事前につぶす**ことで、攻撃の可能性を極力減らすことにつながります。
- サイバー攻撃から自社を守るためには、**外部に公開されているIT資産を特定し、弱点/リスクがないか継続的に監視**する仕組みが必要です。

ASMは攻撃者に先回りし、セキュリティ事故を未然に防ぐ、**予防ソリューション**に位置付けられます



ASMで対策していくべき領域

境界防御/SASE/EDR等で対策していくべき領域

経産省のASMガイドンス

つながろう。驚きを。幸せを。



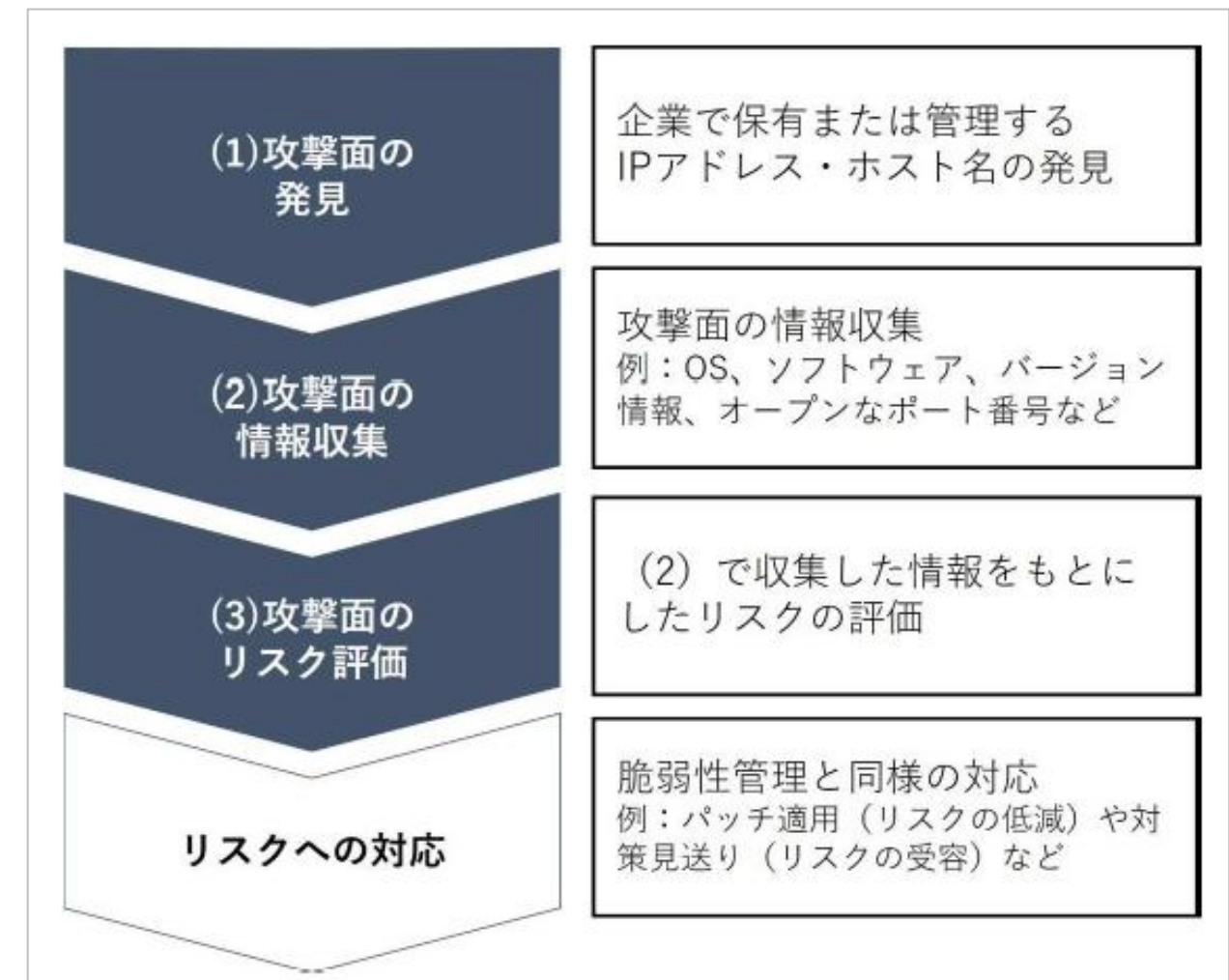
経産省ASMガイドンス(2023年5月)のポイント

- **攻撃面の発見、情報収集、リスク評価**の3STEPがASMのプロセスである。
- 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ているが、**人手を介した管理手法には限界**があり、ASMのような管理ツールを使うのが望ましい。
- 攻撃者視点を持つという特徴があり、**防御側が同じ視点で自社環境をチェック**することが重要である。
- 脆弱性などのリスクを**継続的に検出・評価**することが求められる。
- 確認できる情報を基に、脆弱性診断やさらに細かい確認が必要なこともある。

経産省のウェブサイトスクリーンショット。ナビゲーションメニューには「申請・お問合せ」、「English」、「サイトマップ」、「本文へ」、「文字サイズ変更 小 中 大」、「アクセシビリティ 閲覧支援ツール」があります。メインメニューには「ニュースリリース」、「会見・談話」、「審議会・研究会」、「統計」、「政策について」、「経済産業省について」があります。記事タイトルは「ASM (Attack Surface Management) 導入ガイドンス～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～」です。日付は2023年5月29日です。記事本文には「経済産業省は、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)」について、自社のセキュリティ戦略に組み込んで適切に活用してもらえよう、ASMの基本的な考え方や特徴、留意点などの基本情報とともに取組事例などを紹介した、「ASM (Attack Surface Management) 導入ガイドンス～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～」を作成しました。」と記載されています。

出展) 経済産業省

<https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html>



出展) 経産省ASMガイドンスより抜粋 ASMのプロセス

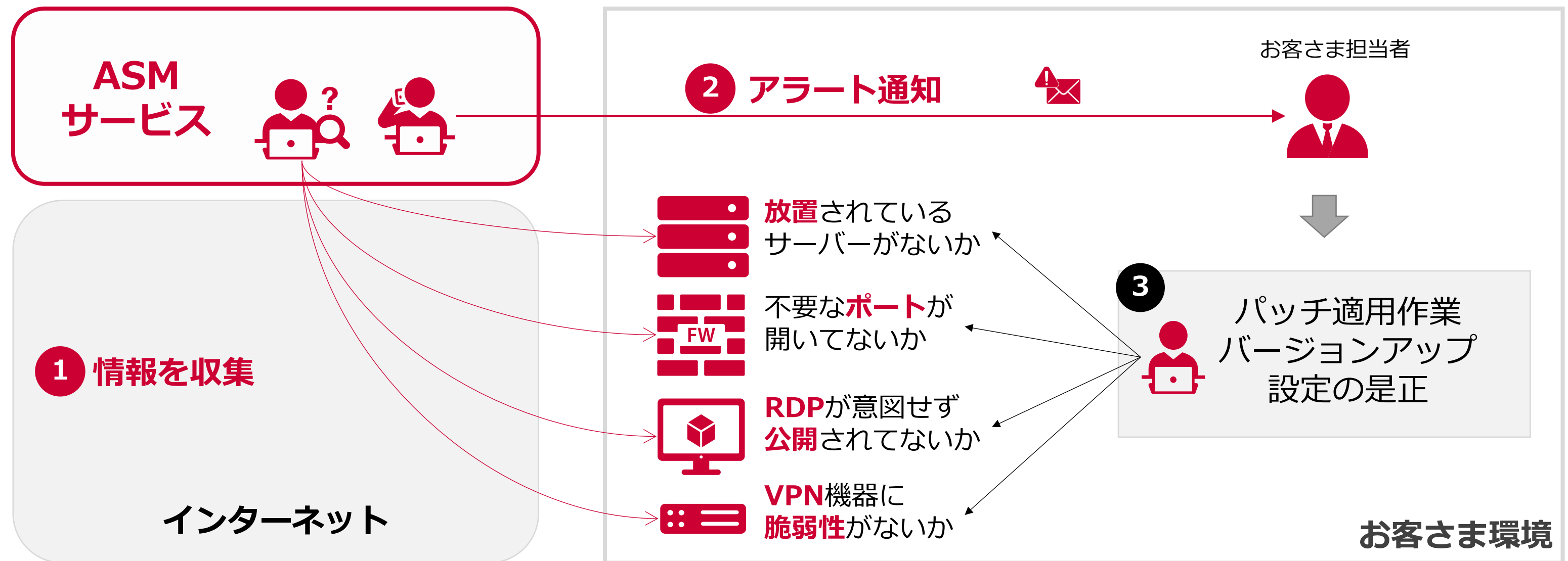
Attack Surface Management (ASM) とは

つながり。驚きを。幸せを。

NTT docomo Business

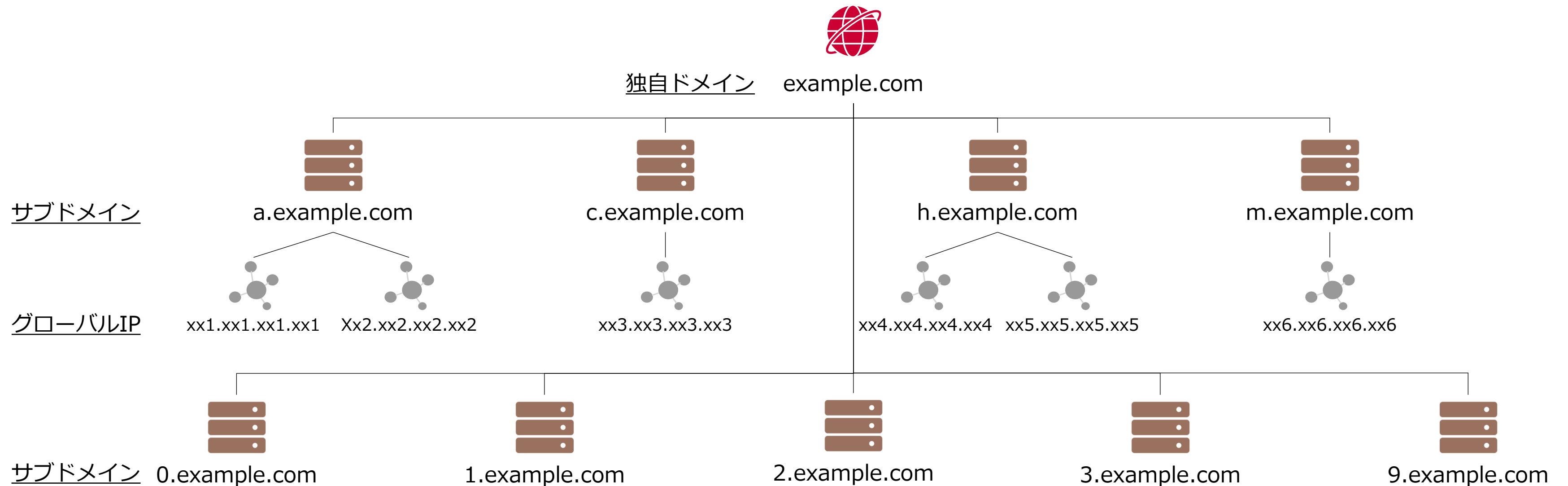
- ASMとは、**Attack Surface Management**の略であり**外部に公開されているIT資産を特定し**、**弱点がないか**、**攻撃の起点になりうるリスクがないか**、**定期的に監視する仕組み**です。

※ASMツール・サービスのイメージ



ASMの仕組み

- ①ドメイン情報から、**Whois、DNSなどのOSINT情報**からIT資産の洗い出し
- ②芋づる式にIT資産をたどって、関連するIT資産をリストアップ
- ③発見したIT資産の、**ポートスキャン結果や、バナー情報より、機器やバージョンを特定**
- ④リスクを洗い出す



ASMと脆弱性診断の違い

WideAngleサービス	特長	頻度
脆弱性診断	把握済みの特定資産を詳細に診断	年1~2回
ASM	未把握資産含め守るべき対象を定期診断し、 対応管理	常時（スキャンは週1回）
リスクスコアリング	調査対象を広く診断	月1回 or 1回(取引先)

ASMで、よく発見されるインシデント例

- ① Apacheの古いバージョンの利用
- ② サポート切れのOSが稼働
- ③ 管理されていない野良端末発見
- ④ RDPやSQLなどのサービスが公開
- ⑤ VPN機器の脆弱性がある
- ⑥ FWで不要なポートが空いている



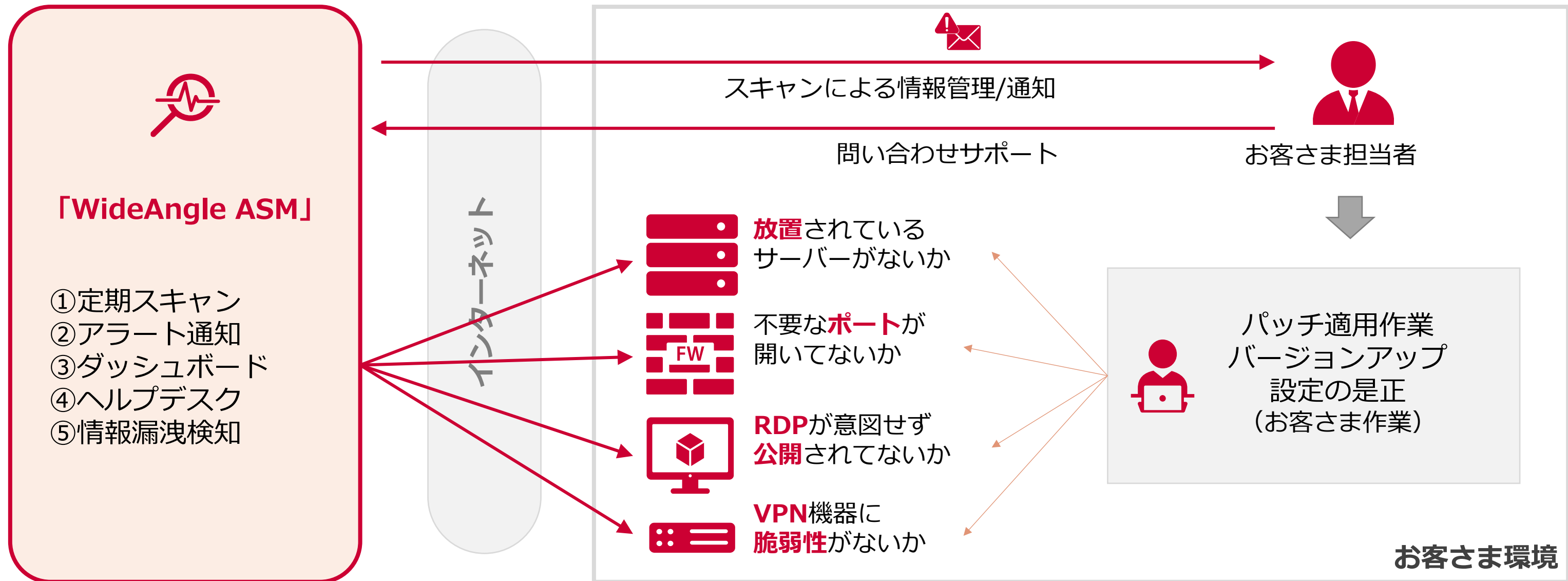
WideAngle ASMのご紹介



WideAngle ASM 概要

WideAngle ASMの特長は、**コストを抑えた、シンプルな日本語ダッシュボード**のサービスです。

- ・ ツールを中心に調査を行うことで、より導入コストを抑えられます。
- ・ お客さまにて発見された、資産や脆弱性情報を管理できるWebポータルをご提供いたします。
- ・ ASMのみならず、ダークウェブへの**情報漏えい検知**も可能です。



WideAngle ASM 機能一覧

つなごう。驚きを。幸せを。



- WideAngle ASMの機能は、**アタックサーフェス**と**情報漏えい**。
- 特徴として、アタックサーフェスのみならず、**ダークウェブまでスキャン**し、脆弱性等を検出。
- シンプルな日本語**ダッシュボード**で、検出結果の確認やレポート生成の管理を実現。

カテゴリ	機能	機能説明	備考
アタックサーフェス	ダッシュボード	脅威状況のグラフィカルなサマリ	
	攻撃対象領域	アプリケーション・ソフトウェア・ネットワークなどに関する 脆弱性等の一覧	危険度ごとに脆弱性等を管理可能です。
	IT資産	ハッカー目線でドメイン名から探索可能な IPアドレス、ドメイン、ASネーム、国、ポート、NW機器・OS情報、ソフトウェア、SSL証明書、公開文書の一覧	外部公開資産を一元的に管理し、ダッシュボードで閲覧できます。
情報漏洩	ダッシュボード	脅威状況のグラフィカルなサマリ	
	脅威情報一覧	ダークウェブ・ディープウェブ上で検出可能な対象の 脅威一覧	危険度ごとに脅威を一覧表示します。
	情報漏洩発生サービス	情報漏洩が発覚した サービスの一覧	ダークウェブ上に漏洩している、社印情報や対象サービスを管理することが可能です。
	漏洩社員管理	情報漏洩した社員のメールアドレスとそれに紐づく 漏洩した個人情報の一覧	また、タグ、ステータスの設定も行えます。
	ブラックマーケット	ブラックマーケット上で 漏洩しているユーザ名・パスワード等 を確認	ダークウェブ上のマーケットで売買されている情報を表示します。
	脅威掲示板	外部から閲覧可能な 掲示板の一覧	メールアドレスやパスワード等の情報が記載されていないか確認可能です。
	フィッシングドメイン	自社保有のドメインに 似ているドメイン名 を検出	監視ドメインに酷似した類似ドメインがないか確認可能です
	CMSユーザーアカウント	CMSで構築されているWebサイトの 管理者アカウントの漏洩状況 の一覧	CMSの管理者アカウントがAPIで確認できるかどうかを表示します。
一般	レポート	検知された情報漏洩とASMに関する情報を PDFで出力	検索結果に基づいた考察・対策方法を纏めている為社内関係各所へ報告資料として活用可能です。
	設定	プロジェクト管理、チーム管理、ユーザ管理、 ドメイン管理 が可能	ポータルにログインするユーザの追加削除、監視対象のドメインが確認できます。
	個人設定	通知管理 、ユーザ名やパスワード変更、マニュアルのダウンロードが可能	ユーザ毎に、新しい脅威や資産を検知時の通知設定が可能です。

WideAngle ASM 提供メニュー

つながろう。驚きを。幸せを。








- ASMは**2つの基本プラン**をご用意しています。
- ASM機能に加えて**情報漏えい機能**もご提供するプランがあります。
- 1ドメインからスモールスタートをすることが可能です。

No	カテゴリ	メニュー名	提供単位	料金	提供内容
1	基本プラン	ASM	ドメイン単位	4.5万円/月	<ul style="list-style-type: none"> • ASM機能を提供します • ポータル機能を提供します • 問い合わせサポートを提供します • 最低利用期間12カ月 • 週一回スキャン • 100サブドメイン未満までスキャンします
2	基本プラン	ASM+情報漏洩	ドメイン単位	7.5万円/月	<ul style="list-style-type: none"> • ASMと情報漏えい機能を提供します • ポータル機能を提供します • 問い合わせサポートを提供します • 最低利用期間12カ月 • 週一回スキャン • 100サブドメイン未満までスキャンします • 情報漏えい機能はサブドメイン数制限ありません
3	オプション	サブドメイン100以上	ドメイン単位	2万円/月	<ul style="list-style-type: none"> • 100以上1000サブドメインまでスキャンします
4	オプション	レポート解説	契約単位	8万円/チケット	<ul style="list-style-type: none"> • レポート結果の内容について解説、専門的アドバイスを行います 以下のチケットメニュー以外は個別相談です <ul style="list-style-type: none"> ✓ 2チケット：解説+実施報告書 ✓ 3チケット：解説+実施報告書+専門的アドバイス

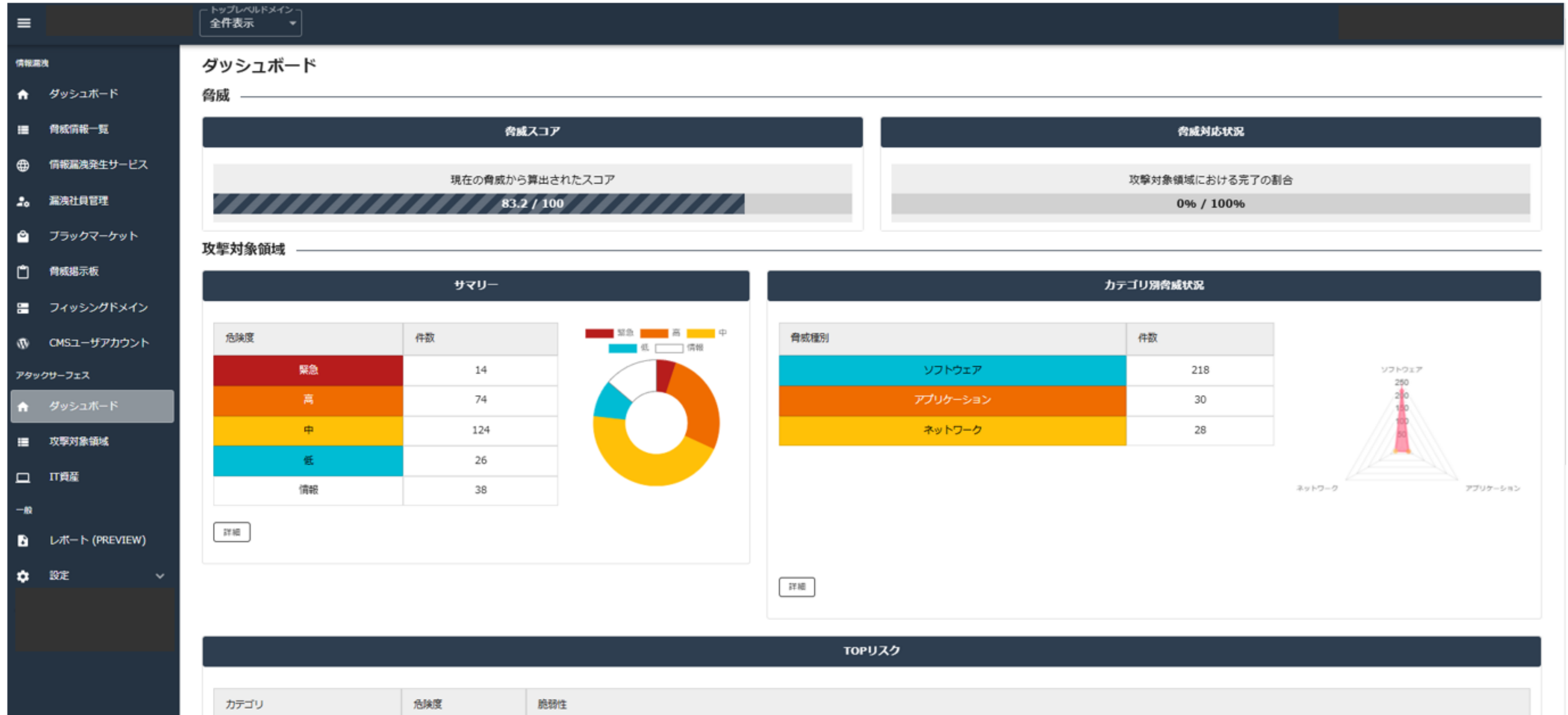
※お申し込みいただくドメインは、独自ドメインです。
ex. ntt.com

WideAngle ASM 特徴

カテゴリ	アピールポイント	説明
機能面	①見やすいUI 	日本語GUIで直感的に使えます
	②対応状況管理できるUI 	脆弱性や情報漏洩の対策実施状況をポータル画面で管理できます
	③ドメイン単位の料金設定 	課金単位がIT資産数でなく独自ドメイン数のため、お申し込みが簡単です
運用面	①ヘルプデスク 	セキュリティに特化したヘルプデスク。Cyber Exposure Managementとしてお客さまの総合的な運用をサポートします
	②レポート解説 	ポータルが提供するレポート情報について、セキュリティ専門家がリモート会議にて解説やアドバイスを行います（オプション）

提供機能① (ASM)

- ASMのダッシュボード (サマリ情報の閲覧) 画面です。
- 危険度の数、種類など**概要を把握**することが可能です。



提供機能① (ASM)

- ASMの脆弱性情報の管理画面です。
- 危険度ごとに上位から表示し、具体的なCVEと共に脆弱性の管理を行うことが可能です。

The screenshot displays the ASM interface for managing vulnerabilities. The top navigation bar includes a hamburger menu, a dropdown for 'トップレベルドメイン 全件表示', and a search bar. The left sidebar contains various navigation options like 'ダッシュボード', '脅威情報一覧', and '攻撃対象領域'. The main content area is titled '攻撃対象領域' and shows a summary of vulnerabilities by severity: 緊急 (14件), 高 (74件), 中 (124件), and 低 (26件). Below this, there are filters for 'オープン' and 'クローズ', a 'CSVダウンロード' button, and dropdown menus for '危険度 全て' and 'ステータス 全て'. A table lists 276 items, with the first 100 displayed. The table columns are 'アセット名', 'カテゴリ', '内容', '危険度', 'ステータス', and '最終検知日'. The '内容' column contains links to specific CVE details.

アセット名	カテゴリ	内容	危険度	ステータス	最終検知日
52.192.61.244	ソフトウェア	CVE-2024-4577 - phpにおけるスクリプト関数やコード実行に関する脆弱性を検出	緊急	オープン	2024/12/17
18.178.36.165	ソフトウェア	CVE-2024-4577 - phpにおけるスクリプト関数やコード実行に関する脆弱性を検出	緊急	オープン	2024/12/17
52.192.61.244	ソフトウェア	CVE-2024-38476 - http_serverにおける情報漏えいに関する脆弱性を検出	緊急	オープン	2024/12/17
18.178.36.165	ソフトウェア	CVE-2024-38476 - http_serverにおける情報漏えいに関する脆弱性を検出	緊急	オープン	2024/12/17
18.178.36.165	ソフトウェア	CVE-2024-38474 - http_serverにおけるスクリプト実行または関数に関する脆弱性を検出	緊急	オープン	2024/12/17
52.192.61.244	ソフトウェア	CVE-2024-38474 - http_serverにおけるスクリプト実行または関数に関する脆弱性を検出	緊急	オープン	2024/12/17
52.192.61.244	ソフトウェア	CVE-2024-11236 - phpにおける範囲外書き込みに関する脆弱性を検出	緊急	オープン	2024/12/17
18.178.36.165	ソフトウェア	CVE-2024-11236 - phpにおける範囲外書き込みに関する脆弱性を検出	緊急	オープン	2024/12/17
52.192.61.244	ソフトウェア	CVE-2023-3824 - phpにおけるメモリ破壊またはRCEに関する脆弱性を検出	緊急	オープン	2024/12/17
18.178.36.165	ソフトウェア	CVE-2023-3824 - phpにおけるメモリ破壊またはRCEに関する脆弱性を検出	緊急	オープン	2024/12/17
18.178.36.165	ソフトウェア	CVE-2022-2068 - opensslにおける任意コード実行に関する脆弱性を検出	緊急	オープン	2024/12/17

提供機能① (ASM)

つながろう。驚きを。幸せを。



- ASMの外部公開資産の一覧画面です。
- IPアドレス、ドメイン、空きポート、推測されるNW機器・OS、ソフトウェアなどを確認できます。

The screenshot shows the ASM interface with a sidebar on the left and a main content area. The main content area displays a table of IP addresses and their associated information.

IPアドレス	ドメイン名	ASネーム	国	ポート	タグ	自社タグ	脆弱性	最終検知日
93.184.215.14	• example.com	Edgecast Inc	United States	80 443 1119 1935		<input type="text"/>		2024/12/16
54.65.19.9	• vuln-ruhuna.net	Amazon Inc	Japan	- (接続不可)	Datacenter IP	<input type="text"/>		2024/12/16
18.178.36.165	• www.vuln-ruhuna.net • blog.vuln-ruhuna.net	Amazon Inc	Japan	80 443		<input type="text"/>	緊急	2024/12/16
52.192.61.244	• www.vuln-ruhuna.net • blog.vuln-ruhuna.net	Amazon Inc	Japan	80 443	Datacenter IP	<input type="text"/>	緊急	2024/12/16
13.230.189.4	• vulnhub.test.vuln-ruhuna.net • wp.vulnhub.test.vuln-ruhuna.net • zabbix.vulnhub.test.vuln-ruhuna.net • webmin.vulnhub.test.vuln-ruhuna.net	Amazon Inc	Japan	- (接続不可)	Datacenter IP	<input type="text"/>		2024/12/16
54.92.43.183	• vulnhub.test.vuln-ruhuna.net • wp.vulnhub.test.vuln-ruhuna.net • zabbix.vulnhub.test.vuln-ruhuna.net • webmin.vulnhub.test.vuln-ruhuna.net	Amazon Inc	Japan	- (接続不可)	Datacenter IP	<input type="text"/>		2024/12/16

提供機能② (情報漏えい)

- 情報漏えいの**脅威管理**の画面です。
- 危険度ごとに優先順位をつけており、**情報漏えいリスクを一覧管理**することが可能です。

The screenshot displays the 'Threat Information Overview' (脅威情報一覧) page. At the top, there are four colored boxes representing risk levels: Emergency (12 items), High (34 items), Medium (9 items), and Low (2 items). Below these is a table of 79 items, with the first 10 rows visible. The table columns are Asset Name, Category, Content, Severity, Status, and Last Detection Date. All items shown have a severity of 'High' and a status of 'Open'.

アセット名	カテゴリ	内容	危険度 ↓	ステータス	最終検知日
blog.vuln-ruhuna.net	CMSユーザアカウント	管理画面のユーザアカウント情報の漏洩を検出	高	オープン	2024/12/16
r.example.com	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Collection5	高	オープン	2024/12/16
1.example.com	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Collection4	高	オープン	2024/12/16
r.example.com	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Collection4	高	オープン	2024/12/16
r.example.com	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Collection2	高	オープン	2024/12/16
1.example.com	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Collection2	高	オープン	2024/12/16
r.example.com	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - AntiPublic	高	オープン	2024/12/16
1.example.com	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - AntiPublic	高	オープン	2024/12/16
example.com	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - AntiPublic	高	オープン	2024/12/16
example.com	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - 2844Breaches	高	オープン	2024/12/16

提供機能②（情報漏えい）

- 情報漏えいの漏洩情報一覧画面です。
- 各ユーザごとに、情報漏えいしたサービスと漏洩情報を可視化します。
- パスワード情報は一部マスクしてお出しします。

漏洩社員管理 **メールアドレス** パスワード 電話番号 ユーザ名 氏名

情報漏洩したメールアドレスとそれに紐づく漏洩した個人情報の一覧 詳細説明

CSVダウンロード 在籍変更 PW変更依頼メール タグ管理

ステータス: 未対応, 処理中, 完了, 対象外 在籍: 全件表示 検索: メールアドレス・漏洩サービス・タグ検索

表示件数: 100 1

No	メールアドレス	漏洩数	在籍	PW変更依頼日	完了率	タグ																																			
1	account@example.com	4	在籍	-	0%																																				
<table border="1"> <thead> <tr> <th>漏洩サービス名</th> <th>パスワード</th> <th>電話番号</th> <th>ユーザ名</th> <th>氏名</th> <th>漏洩検知日</th> <th>ステータス</th> </tr> </thead> <tbody> <tr> <td>al.type</td> <td></td> <td></td> <td></td> <td></td> <td>2017/12/09</td> <td>未対応</td> </tr> <tr> <td>8fit</td> <td>\$2*****y</td> <td></td> <td></td> <td></td> <td>2019/03/22</td> <td>未対応</td> </tr> <tr> <td>Adult FriendFinder (2015)</td> <td></td> <td></td> <td></td> <td></td> <td>2015/05/22</td> <td>未対応</td> </tr> <tr> <td>Animal Jam</td> <td></td> <td></td> <td></td> <td></td> <td>2020/11/12</td> <td>未対応</td> </tr> </tbody> </table>							漏洩サービス名	パスワード	電話番号	ユーザ名	氏名	漏洩検知日	ステータス	al.type					2017/12/09	未対応	8fit	\$2*****y				2019/03/22	未対応	Adult FriendFinder (2015)					2015/05/22	未対応	Animal Jam					2020/11/12	未対応
漏洩サービス名	パスワード	電話番号	ユーザ名	氏名	漏洩検知日	ステータス																																			
al.type					2017/12/09	未対応																																			
8fit	\$2*****y				2019/03/22	未対応																																			
Adult FriendFinder (2015)					2015/05/22	未対応																																			
Animal Jam					2020/11/12	未対応																																			
2	chido_edg@r.example.com	4	在籍	-	100%																																				
<table border="1"> <thead> <tr> <th>漏洩サービス名</th> <th>パスワード</th> <th>電話番号</th> <th>ユーザ名</th> <th>氏名</th> <th>漏洩検知日</th> <th>ステータス</th> </tr> </thead> <tbody> <tr> <td>Collection #2</td> <td>10***e</td> <td></td> <td></td> <td></td> <td>2019/01/01</td> <td>対象外</td> </tr> <tr> <td>Collection #4</td> <td>10***e</td> <td></td> <td></td> <td></td> <td>2019/01/01</td> <td>対象外</td> </tr> <tr> <td>Collection #5</td> <td>10***e</td> <td></td> <td></td> <td></td> <td>2019/01/01</td> <td>対象外</td> </tr> <tr> <td>Anti Public Combo List</td> <td>10***e</td> <td></td> <td></td> <td></td> <td>2017/05/05</td> <td>対象外</td> </tr> </tbody> </table>							漏洩サービス名	パスワード	電話番号	ユーザ名	氏名	漏洩検知日	ステータス	Collection #2	10***e				2019/01/01	対象外	Collection #4	10***e				2019/01/01	対象外	Collection #5	10***e				2019/01/01	対象外	Anti Public Combo List	10***e				2017/05/05	対象外
漏洩サービス名	パスワード	電話番号	ユーザ名	氏名	漏洩検知日	ステータス																																			
Collection #2	10***e				2019/01/01	対象外																																			
Collection #4	10***e				2019/01/01	対象外																																			
Collection #5	10***e				2019/01/01	対象外																																			
Anti Public Combo List	10***e				2017/05/05	対象外																																			



3

考察

考察

初めに

このレポートは、情報セキュリティの重要性を強調し、ダークウェブに漏洩している情報の件数、内容、およびそれらの危険度を詳細に分析します。情報セキュリティは現代社会において切っても切れない関係であり、その問題を速やかに解決するための取り組みを共有することが我々の目的です。このレポートを通じて、情報漏洩の現状を理解し、適切な対策を講じることを促します。

結論

情報収集の結果、危険性が緊急である脆弱性が検知されました。問題を解決するための原因と対策を以下に記載します。即座の認識と対策を推奨します。

原因

- セキュリティ設計の不備
アプリケーションやネットワークが初期段階でセキュリティを考慮せずに設計された場合、深刻なセキュリティの弱点が生じることがあります。
- サードパーティコンポーネントの脆弱性
外部ライブラリやフレームワークが更新されずに古いまま使用されることで、既知のセキュリティ脆弱性を抱えることがあります。
- 不十分なテストと監査
製品のリリース前に十分なセキュリティテストや脆弱性評価が行われない場合、重要な脆弱性が見逃されることがあります。
- 適用されていないセキュリティアップデート
システムやソフトウェアのアップデートが定期的に行われず、既知の脆弱性が放置されることが多いです。

6

攻撃対象領域

ドメイン名	脆弱性	危険度	ステータス
	PHP 7.1.26 にて脆弱性を検出	高	オープン
	Apache HTTP Server 2.4.25 にて脆弱性を検出	高	オープン
	80番ポートにて脆弱性を検出	高	オープン
	コンテンツ・セキュリティ・ポリシー (CSP) ヘッダが設定されていない	中	オープン
	サブリソースの整合性異性が見つからない	中	オープン
	クリックジャッキング防止ヘッダの欠落	中	オープン
	危険なJS関数	低	オープン
	サーバーが "Server" HTTPレスポンス・ヘッダ・フィールド経由でバージョン情報を漏らす	低	オープン
	サーバーが "X-Powered-By" HTTPレスポンス・ヘッダ・フィールドから情報を漏らす	低	オープン
	パーミッションポリシーヘッダが設定されていない	低	オープン
	X-Content-Type-Optionsヘッダが見つからない	低	オープン
	アバッチ検出	情報	オープン
	モダンWebアプリケーション	情報	オープン
	保存可能でキャッシュ可能なコンテンツ	情報	オープン
	情報開示・不要なコメント	情報	オープン
	CAA記録	情報	オープン
	ワッパライザー・テクノロジー検出	情報	オープン
	HTTP セキュリティ・ヘッダの欠落	情報	オープン
	PHP検出	情報	オープン
	許可されたオプション方法	情報	オープン

ご提供条件

つながり。驚き。幸せを。

 NTT docomo Business

- 1契約で1つのプランのみお申し込みとなります。
- ASMと情報漏えいは1 独自ドメインからお申込みいただけますが、情報漏えいのみのご契約はできません。
- Gmail、Hotmail、Yahoo!メールや、通信キャリア・ISP（インターネットサービスプロバイダー）が提供するメールドメインは監視対象外となります。また監視ドメインが別のドメインのサブドメインとなっている場合等、一定の条件に該当する場合には監視対象外とさせていただくことがあります。
- 本サービスに、SLAはございません。
- 基本プランの最低利用期間は12カ月となります。
- スキャン頻度は週1回になります。
- 本プラットフォームは、ポートスキャンなどのアクティブスキャンを実施いたします。
- インターネット上の公開情報やダークウェブの情報などを様々な手法を用いて情報収集致します。
- 本サービスの監視ドメインは申込者が管理している資産である必要があります。
- スキャンする送信元IPアドレスを指定することはできません。
- 1つの独自ドメインに関するサブドメインは最大1000サブドメインまで表示可能です。基本プランはシステム側で選択した99サブドメインのみスキャン実施します。100サブドメイン以上スキャンする場合は、オプションのお申し込みが必要です。
- OSINT技術をベースとしてるため、精度は100%ではなく、誤検知等が混ざる可能性がございます。
- 株式会社エス・エム・エス・データテック（以下、SDT社）のプラットフォームを使用します。
- レポート、GUIの言語は、日本語のみとなります。
- ポータル利用環境は、OS：Windows, Mac、ブラウザ：Chrome, Edgeです。
- 本サービスは日本国内限定での提供となります。

WideAngle ASMの実績一覧表



WideAngle ASM 実績一覧表

顧客名	業種	エリア	ステータス	ドメイン数	プラン
N社	製造業	関西	受注	1	ASM + 情報漏洩
K社	建設業	九州	受注	3	ASM + 情報漏洩
Y社	教育・学習支援業	東北	受注	1	ASM + 100サブドメイン以上
D社	製造業	東海	受注	1	ASM + 情報漏洩 + 解説オプション (3チケット)
M社	金融業・保険業	九州	受注	1	ASM + 情報漏洩
M社	製造業	東海	受注	1	ASM + 情報漏洩
N社	製造業	東海	受注	7	ASM + 情報漏洩 + 解説オプション (3チケット)

WideAngle ASM 導入効果

つながろう。驚きを。幸せを。

 NTT docomo Business

外部公開資産の可視化と脆弱性の早期発見

WideAngle ASMは企業が保有する外部公開IT資産（サブドメイン、IP、NW機器、リモートアクセス機器、Webサーバー、メールサーバーなど）を自動でスキャンし、放置されたサーバーや不要なポート、脆弱性のある設定などを検出します。

これにより、攻撃者に狙われやすいリスクを早期に把握し、対策を講じることが可能になります。

情報漏えいの検知と迅速な対応

WideAngle ASMは、ダークウェブ上で流通しているメールアドレスやパスワード、CMS管理者アカウントの漏えい情報を検知し、アラート通知を行います。

これにより、漏えいが発生した際の迅速な対応が可能となり、被害の拡大を防ぎます。

継続的なセキュリティ監視と運用負荷の軽減

週1回の定期スキャンやアラート通知、ダッシュボードによる可視化により、セキュリティ状態を継続的に監視できます。

WideAngle ASMは、特に専門知識がなくても運用しやすい日本語GUIとレポート機能が評価されています。

つながろう。驚きを。幸せを。

 ^{NTT} docomo **Business**