ASM無償キャンペーンのご案内

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

不正アクセス・情報漏えいを招く背景

つなごう。驚きを。幸せを。
docomo Business

公開資産の「把握漏れ」は、不正侵入を招く要因の一つです。
把握済みの資産にも、脆弱性や設定不備が残っている場合があります。

不正侵入から情報漏えいへ

Webサイトや VPN機器などへの不正侵入は、情報漏えいや業務停止につながるおそれがあります。

公開資産の増加・分散

クラウドやリモート接続の利用拡大で、外部からアクセスできる機器・サービスが増加。
管理台帳と実態に、ずれが生じやすくなります。

脆弱性・設定不備の見落とし

把握済みの機器・システムでも、脆弱性や設定不備が残っていれば、
不正侵入の入口になるおそれがあります。

**公開資産を把握し、外部から見えるリスクを継続的に確認することが、
セキュリティ対策において欠かせない取組みとなっています。**

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

ASM調査の概要と実施する意義

つなごう。驚きを。幸せを。
docomo Business

ASM（Attack Surface Management）は、インターネットからアクセスできるIT資産を発見し、
外部から見える脆弱性などのリスクを継続的に把握・評価する取組みです。

公開資産の把握

お申し込みのドメインを起点に、サブドメインやIPアドレス等を可視化。
お客さまの管理台帳との照合により、把握漏れの確認に役立てます。

リスク候補の可視化

外部から取得できる情報をもとに、脆弱性や設定不備の可能性を確認。
把握済みの資産も含め、見落としていたリスクに気づくきっかけになります。

対策検討の判断材料

検出したリスクとそのレベルをダッシュボードで確認。
お客さまによる対処の優先順位づけや、追加調査の検討に役立てます。

まずは公開資産とリスクを確認し、継続的な対策の検討にお役立てください

調査結果には確認が必要です。すべての脆弱性の検出や安全性を保証するものではありません。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

ASM無償キャンペーンのご案内

つなごう。驚きを。幸せを。
docomo Business

この機会に、インターネットから見える自社のIT資産を無償で確認してみませんか？

まずは、現状を知ることから

公開資産とリスクをダッシュボードで確認。対策検討の第一歩に。

無償でのご利用期間

2026年11月1日（予定）～12月31日。
期間途中の利用開始も、12月31日まで利用可能です。

対象・ご利用内容

WideAngle ASMと同様のサービスをご利用可能です。
1独自ドメイン、最大99サブドメインを調査します。
アタックサーフェイス調査（公開資産調査）と情報漏えい調査をご利用いただけます。

お申し込み・ご相談は、担当営業までお気軽にご連絡ください。

申込書のご案内から利用開始まで担当営業がご案内します。利用条件は「WideAngle ASM　機能一覧」「通常契約時の利用料金」をご覧ください。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

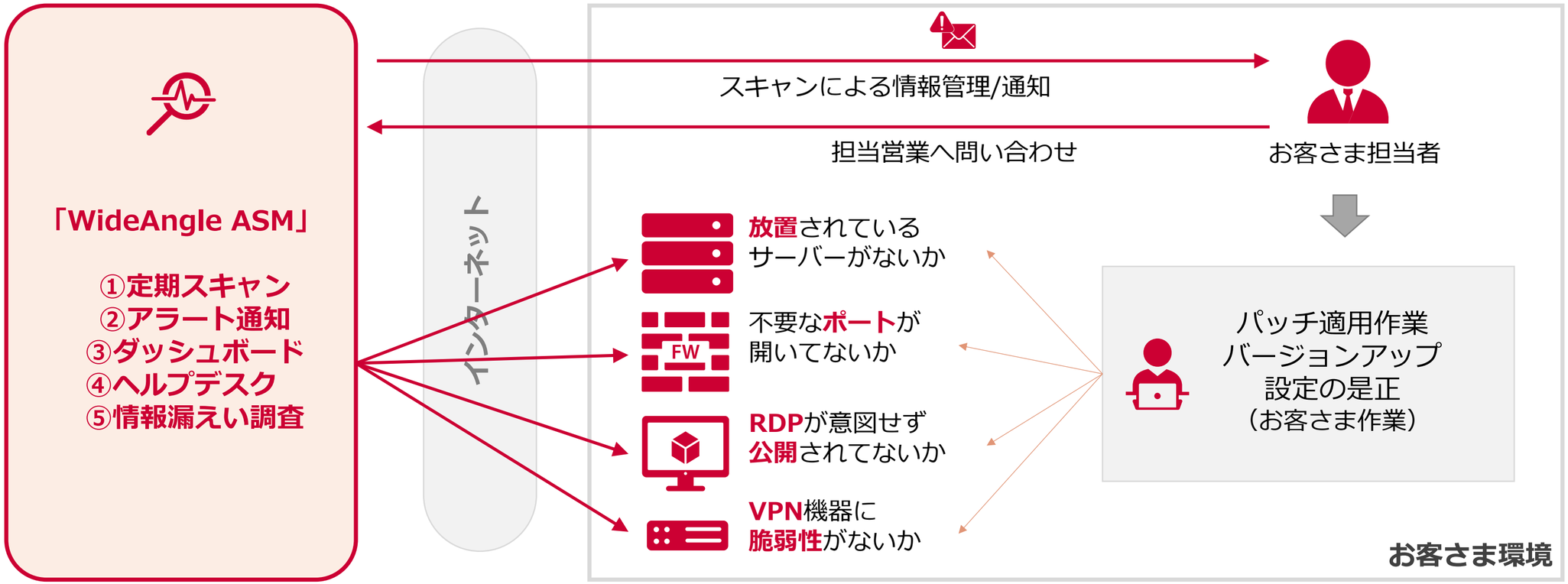
WideAngle ASMご紹介資料

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

WideAngle ASM　サービス概要

WideAngle ASMは、公開資産とリスクを日本語ダッシュボードで確認できるサービスです。

ツールによる定期的な調査で、発見した資産や脆弱性情報を管理します。
ダークウェブなどで検出した情報漏えいの兆候も確認できます。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

WideAngle ASM　機能一覧

- 公開資産の脆弱性・設定不備の候補と、情報漏えいの兆候を調査します。
- 日本語ダッシュボードで結果を確認し、レポートをPDFで出力できます。

つなごう。驚きを。幸せを。
docomo Business

カテゴリ	機能	機能説明	備考
アタックサーフェイス	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	外部から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、社員情報や対象サービスを管理することが可能です。 また、タグ、ステータスの設定も行えます。
	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	
	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で構築したWebサイトの管理者アカウントの外部公開状況	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	調査結果をPDFで出力し、社内関係者への共有に活用できます。
	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。

無償キャンペーンにおいても、上記全ての機能が利用可能です

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

通常契約時の利用料金

つなごう。驚きを。幸せを。
docomo Business

- 以下は通常契約の料金・条件です。
- キャンペーン終了後の継続利用には、別途お申し込み・契約が必要です。

赤枠：今回の無償キャンペーンでの提供範囲

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	• 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	• 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	• 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	• 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 ✓ 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

※独自ドメイン（例：ntt.com）をお申し込みください。

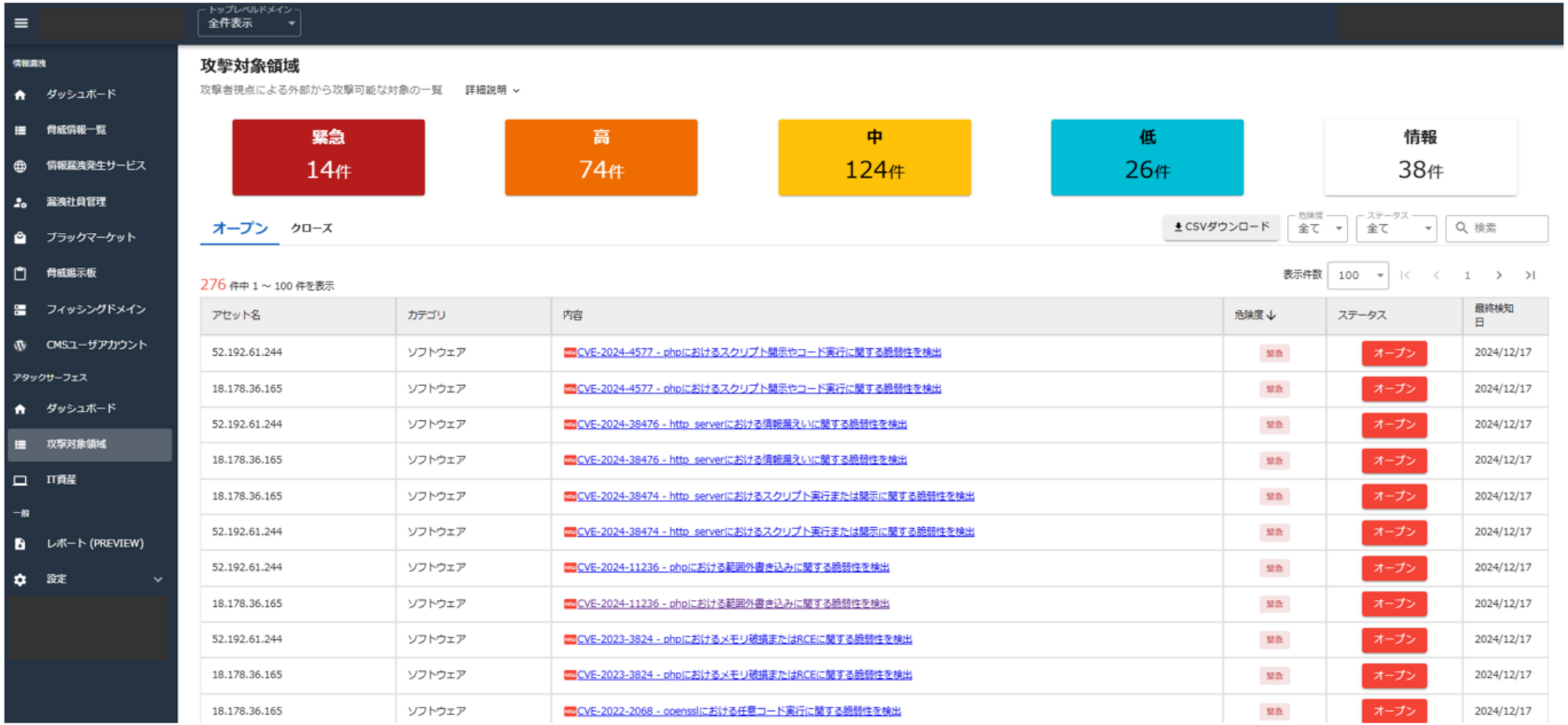
© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

提供機能①（ASM）

ダッシュボードサンプル

つなごう。驚きを。幸せを。
docomo Business

- ASMの調査で検出したリスクを、危険度ごとに一覧表示します。
- CVE（脆弱性の識別番号）などを確認し、対策や追加調査の検討に役立てます。



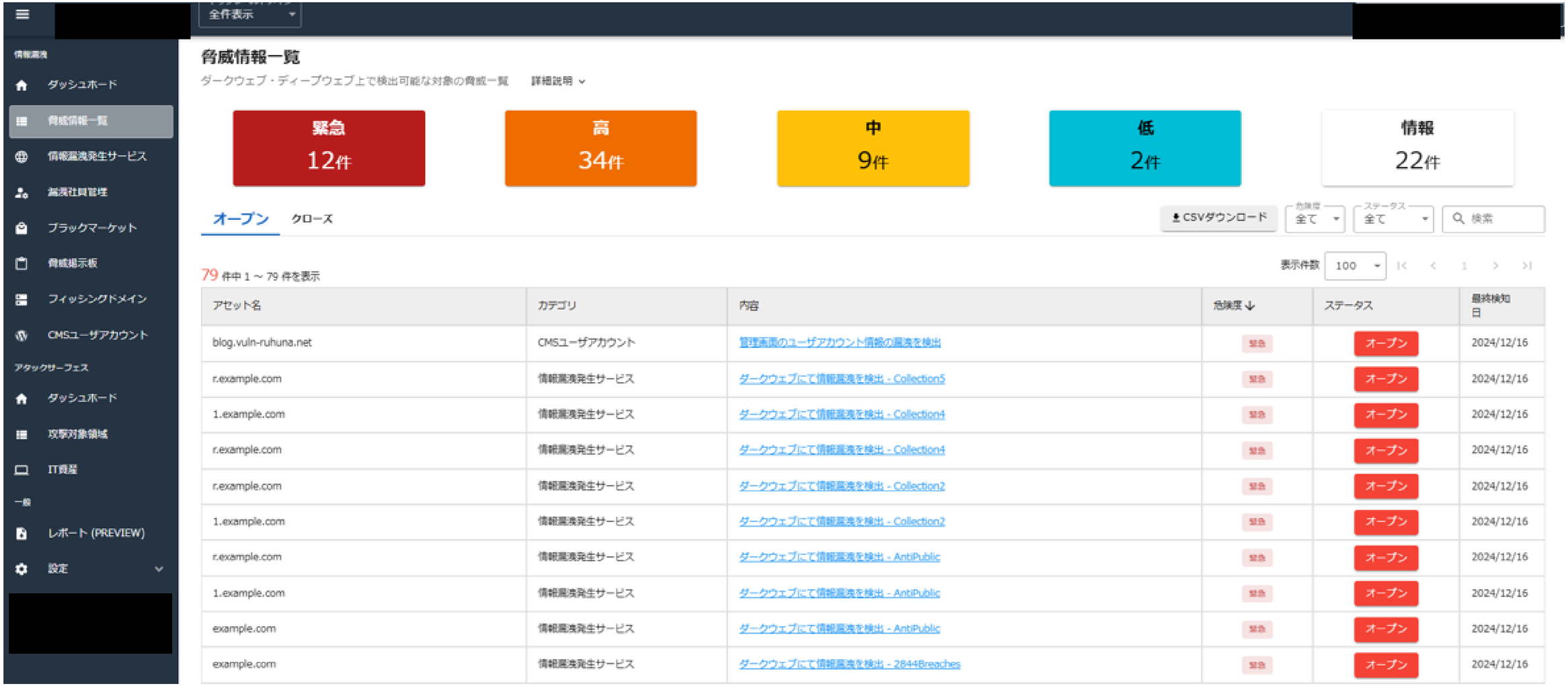
© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

提供機能②（情報漏えい）

ダッシュボードサンプル

つなごう。驚きを。幸せを。
docomo Business

- 情報漏えいの兆候を、危険度ごとに一覧表示します。
- 検出内容がお客さまに関係するかを確認し、追加調査や対策の検討に役立てます。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.