Cisco
Customer Experience

これから導入する方も運用中の方も必見！ Umbrella で実現するセキュリティとその仕組み

2024 年 4 月 25 日

Disclaimer

This document is Cisco Confidential information provided for your internal business use in connection with the Cisco Services purchased by you or your authorized reseller on your behalf. This document contains guidance based on Cisco's recommended practices.

You remain responsible for determining whether to employ this guidance, whether it fits your network design, business needs, and whether the guidance complies with laws, including any regulatory, security, or privacy requirements applicable to your business.

免責

この文書は、お客様またはお客様の代理人である認定リセラーが購入したシスコサービスに関連して、お客様が社内業務において使用することを目的としてシスコが提供するシスコの機密情報です。この文書にはシスコが推奨するプラクティスに基づく手引きが記載されています。

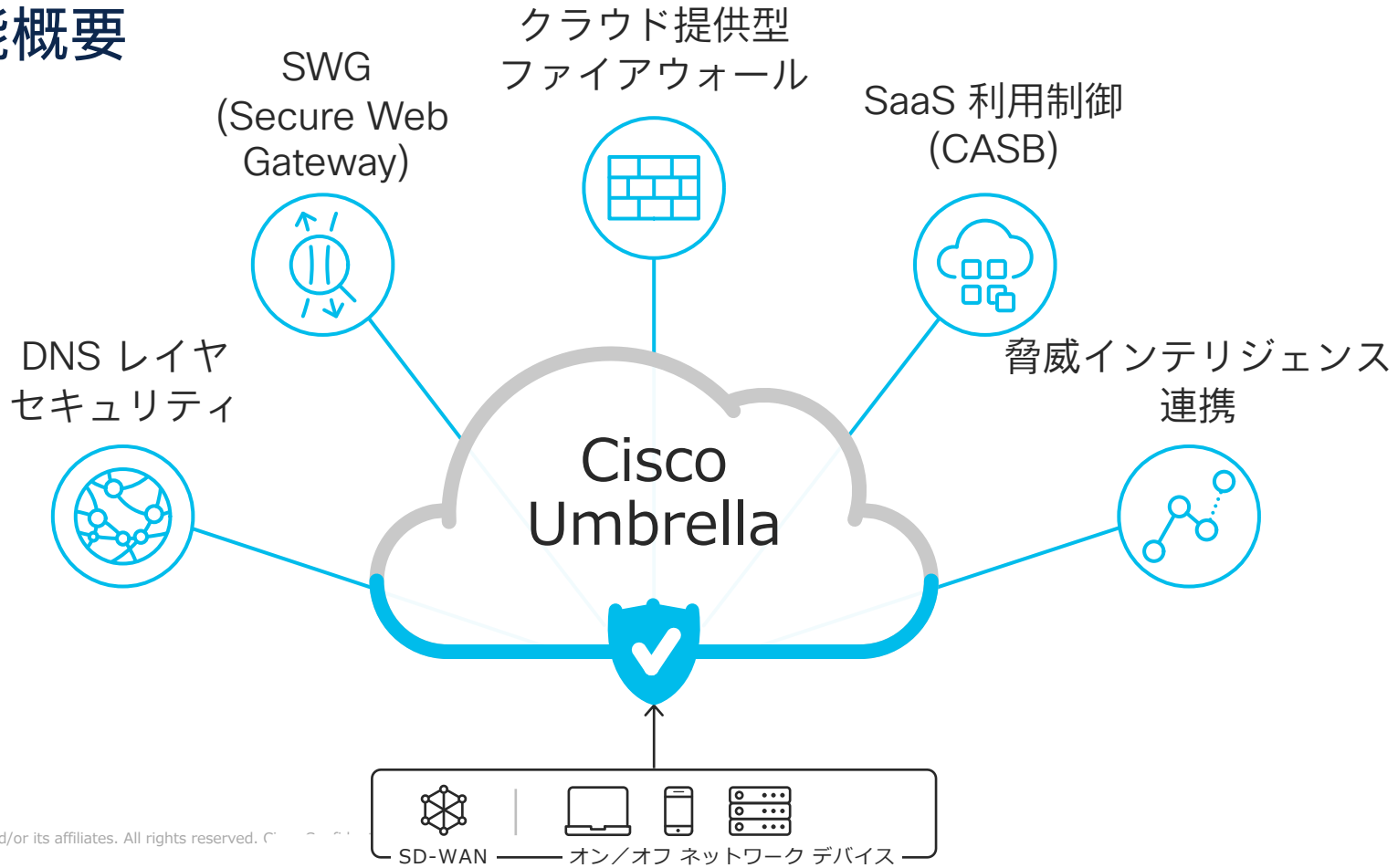
お客様は、この手引きを使用するか否かやお客様のネットワーク設計および業務上のニーズにこの手引きが適合しているか否か、さらにはこの手引きが法律（お客様の業務に適用される規制上の要件、セキュリティ上の要件およびプライバシーに関する要件を含みます）に準拠しているか否かを判断する責任を引き続き負います。

アジェンダ

- Umbrella 機能紹介
  1. Umbrella とは
  2. Umbrella の接続方式
  3. DNS / Webポリシー
  4. セキュリティ設定
  5. デモ ①
- Umbrella の運用について
  6. アプリケーション可視化
  7. Activity Search
  8. レポート
  9. デモ ②

Umbrella 機能紹介
1. Umbrella とは？

機能概要



Umbrella の主な機能について

DNS	CDFW	SWG	CASB
セキュリティカテゴリによる制御	宛先リストによる制御	L3／L4 ファイアウォール	セキュリティカテゴリによる制御	ファイルの分析	高度なアプリケーション制御
コンテンツカテゴリによる制御	ファイルの検査	L7 ファイアウォール	コンテンツカテゴリによる制御	ファイルタイプの制御	アプリケーションの可視化と制御
アプリケーションの制御	選択的なプロキシ	IPS	アプリケーションの制御	選択的なSSL復号化	テナントコントロール
			宛先リストによる制御	RBI	DLP

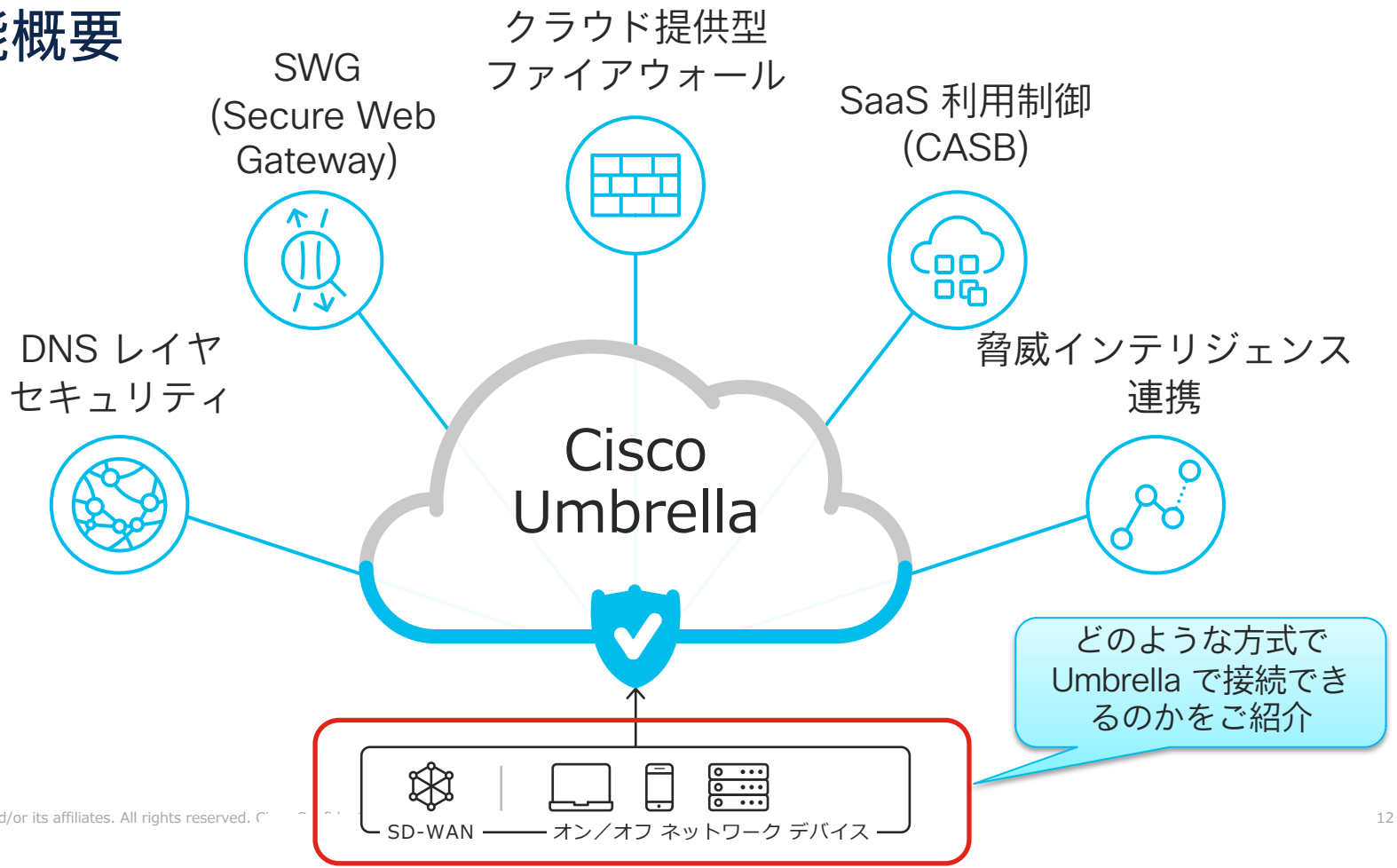
Cisco Umbrella パッケージ比較表

	DNS Security Essentials	DNS Security Advantage	SIG Essentials	SIG Advantage
セキュリティ インテリジェンス (Talos)	○	○	○	○
DC 冗長 & 自動フェイル オーバー	○	○	○	○
S3 ログ管理	○	○	○	○
Multi-Org コンソール	○	○	○	○
Umbrella DNS セキュリティ ※1	○	○	○	○
Umbrella DNS セキュリティ (モバイル端末むけ) ※1	○	○	○	○
Roaming Client & AnyConnect Roaming Security Module	○	○	○	○
インテリジェント プロキシ (セレクティブ プロキシ)	ー	○	○	○
ファイル インスペクション - アンチウイルス、AMP	ー	○ (Proxy 利用時)	○	○
マリシャスな URL のフィルタリング	ー	○ (Proxy 利用時)	○	○
SSL 復号	ー	○ (Proxy 利用時)	○	○
セキュア ウェブ ゲートウェイ (SWG 、フル プロキシ)	ー	ー	○	○
L3-L4 クラウド型ファイアウォール	ー	ー	○	○
L7 クラウド型ファイアウォール および IDPS	ー	ー	オプション	○
サンドボックスによるファイル解析(Threat Grid)	ー	ー	○ (500 サンプル / 日)	○ (制限無し)
クラウド マルウェア検知	ー	ー	○ (2 つまで)	○ (制限無し)
CASB（App Discovery & Blockingではない機能）	ー	ー	○	○
DLP	ー	ー	オプション	○
リモート ブラウザ アイソレーション (Web 分離 (RBI))	ー	ー	オプション	オプション

※1 Domain Filtering, Security Blocking, App Discovery & Blocking, Network and Branch Protection
※2 Roaming Client の EoL が発表されており、サポート終了日が 2025年 4月 2日となっています

Umbrella機能紹介
2. 接続方式

機能概要

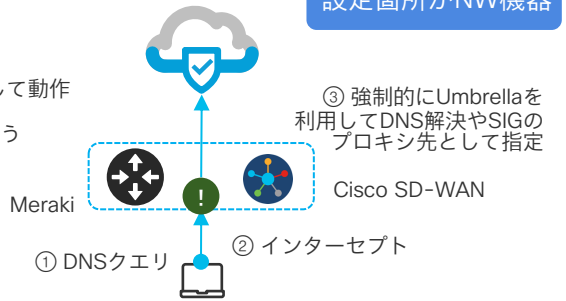


Umbrella との接続方法 ~ 4つのパターン ~

4つの展開パターンが存在

パターン１：
Cisco のWANルータ
Meraki, SD-WAN
から Umbrella と連携して動作
ネットワーク機器から
Umbrella への接続を行う

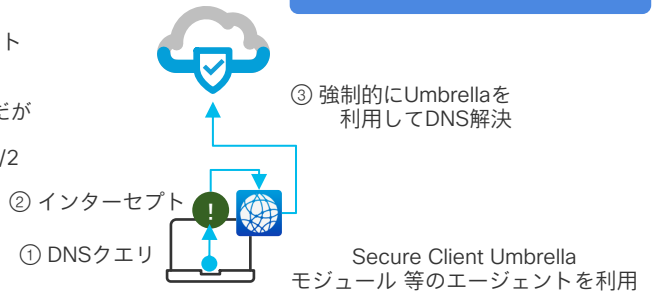
設定箇所がNW機器



パターン２：
Secure Client 等のエージェント
をPCにインストール

※Roaming Clientも利用可能だが
DNSポリシーしか利用不可
EoL もアナウンスされ2025/4/2
最終サポート

主に社外でのアクセス用途

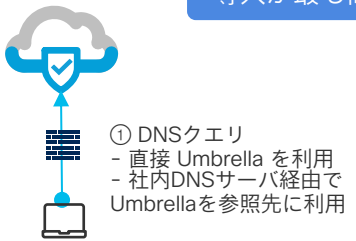


パターン３：
端末のDNSサーバが
Umbrellaになるように設定
- 社内 DNS の参照先に指定
- DHCP サーバでの設定
- 端末のOSに手動設定

など

DNSポリシーの利用のみとなる。
導入は簡単だがユーザ識別が困難

導入が最も簡単



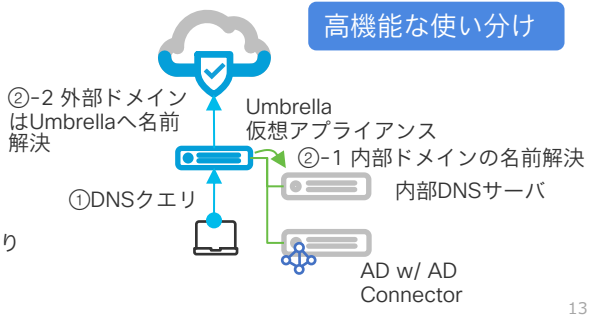
パターン４：
Umbrella 提供の
仮想アプライアンスを設置
連携することで

・サブネット
・内部IPアドレス

をIdentityとして利用可能

追加でADと連携することにより
ユーザ名も利用可

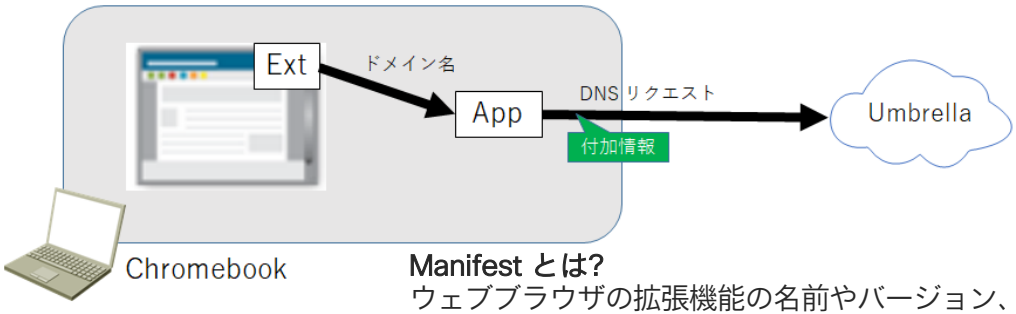
高機能な使い分け



【注意】Chromebook Client で Umbrella をご利用の方

Google 社より「Google Chrome」拡張機能のマニフェスト仕様「Manifest V2」のサポート終了と無効化が 2024 年 6月に行われるとアナウンスされました。
Google Chromebook での Umbrella 利用に必要なエージェントである Chromebook Client は下記の図のように ブラウザの拡張機能を利用して動作しています。そのため、継続利用をするための方法の一つとして Google 管理コンソール より ExtensionManifestV2Availability ポリシーの有効化をお勧めいたします。

【Chromebook Client の動作】

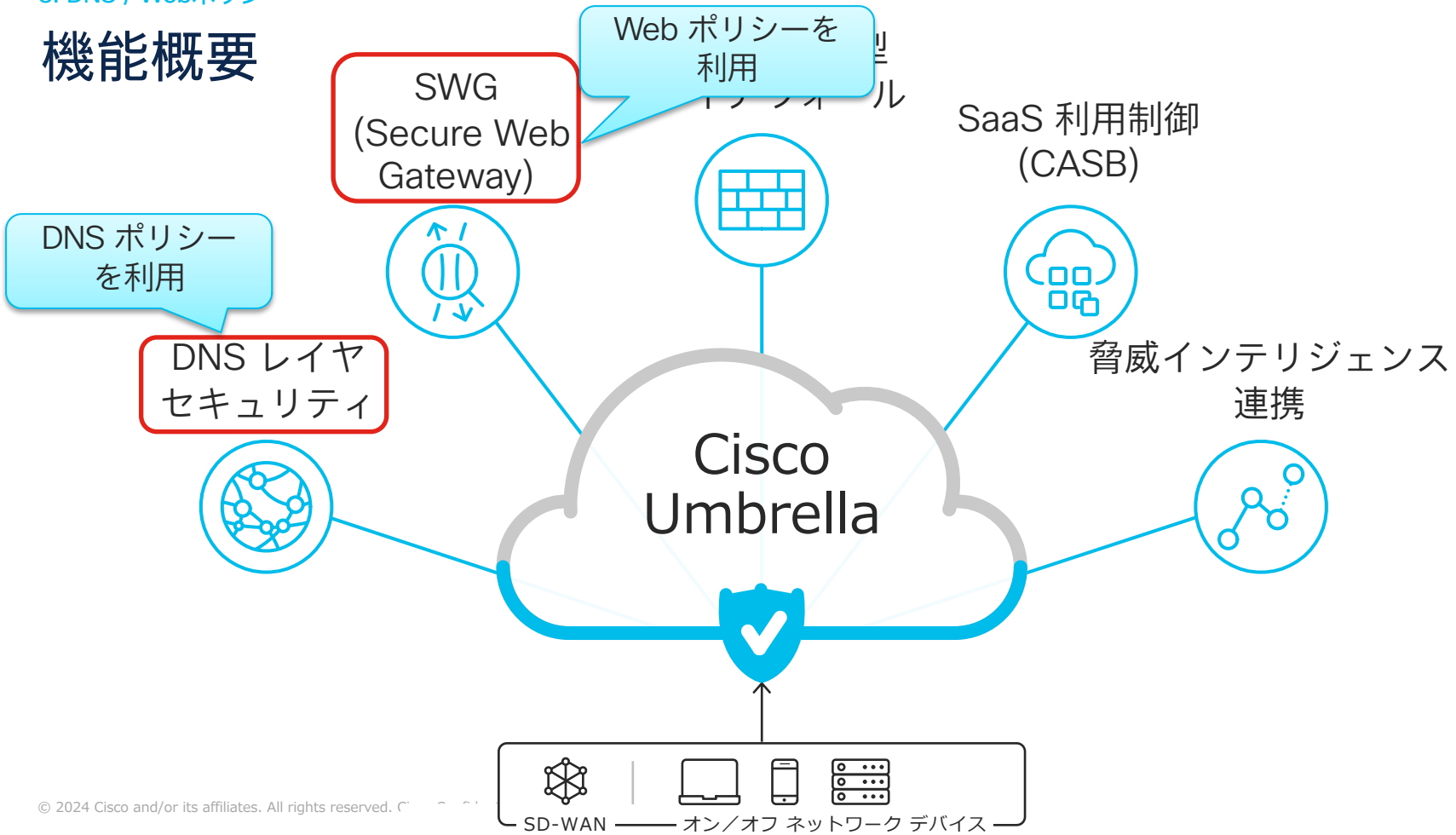


Manifest とは?
ウェブブラウザの拡張機能の名前やバージョン、必要とするパーミッション（権限）などの情報を記しておくファイルのことです。ブラウザ拡張機能にはかならず含まれているものです。

ExtensionManifestV2Availability Policy の変更による延命方法（2025年6月まで機能継続）
https://support.umbrella.com/hc/en-us/articles/21106444957332-Take-Action-Now-Enable-the-ExtensionManifestV2Availability-Policy-for-Both-Umbrella-Chromebook-Client-SWG-Umbrella-Chromebook-Client

Umbrella機能紹介
3. DNS / Webポリシー

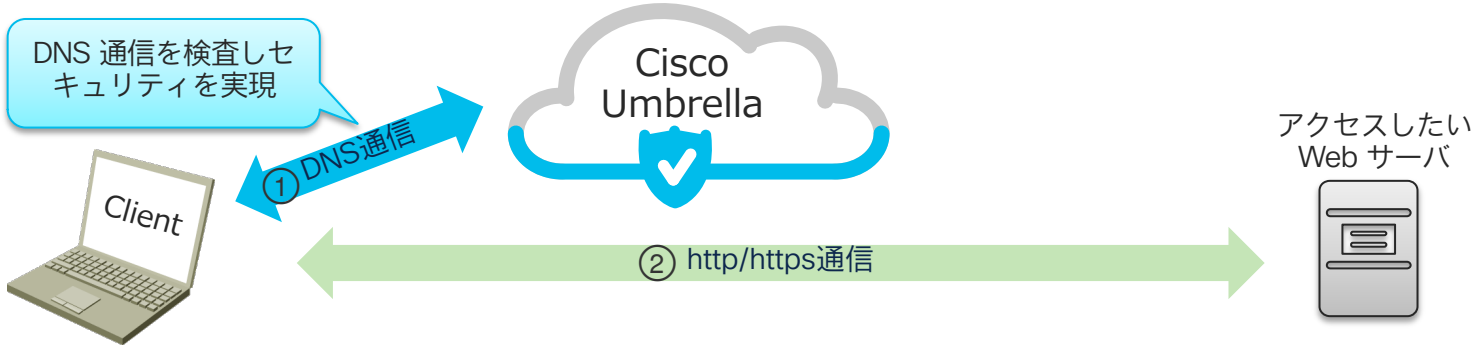
機能概要



DNS レイヤセキュリティと SWG の違い

■DNS セキュリティ

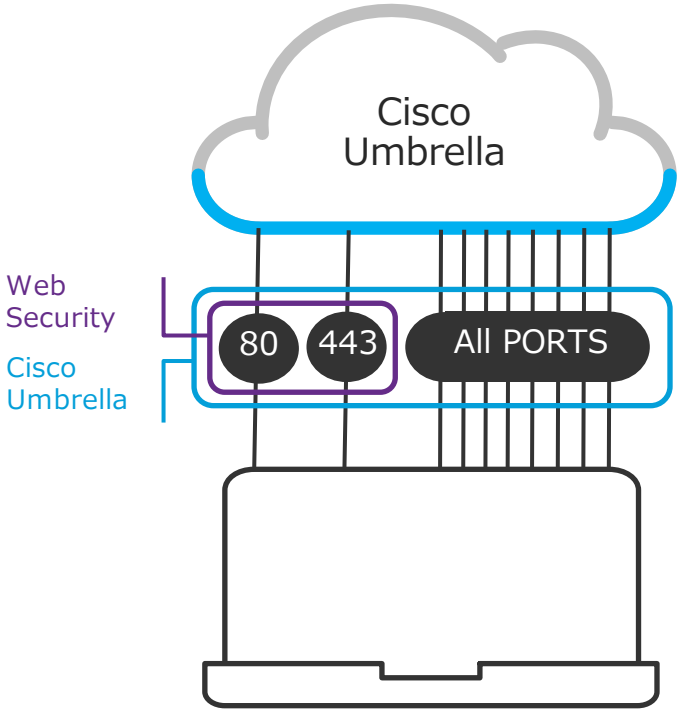
DNS Security ライセンスで可能



■SWG (Secure Web Gateway)

SIG ライセンスで可能

DNS ポリシーと Web ポリシーを両立するべき理由



Web セキュリティでは、Port 80/443の通信のみが検査・保護の対象
(標準ポートを使うHTTP/HTTPSが対象)

DNS セキュリティではプロトコルに関わらず全ての DNS 通信へ保護を行うため、クライアントが HTTP/HTTPS 以外でも**利用するアプリケーションからの通信に対しても有効**
(ポートやプロトコルに依存せず全てが対象)

Umbrella機能紹介
3.1. DNS ポリシー

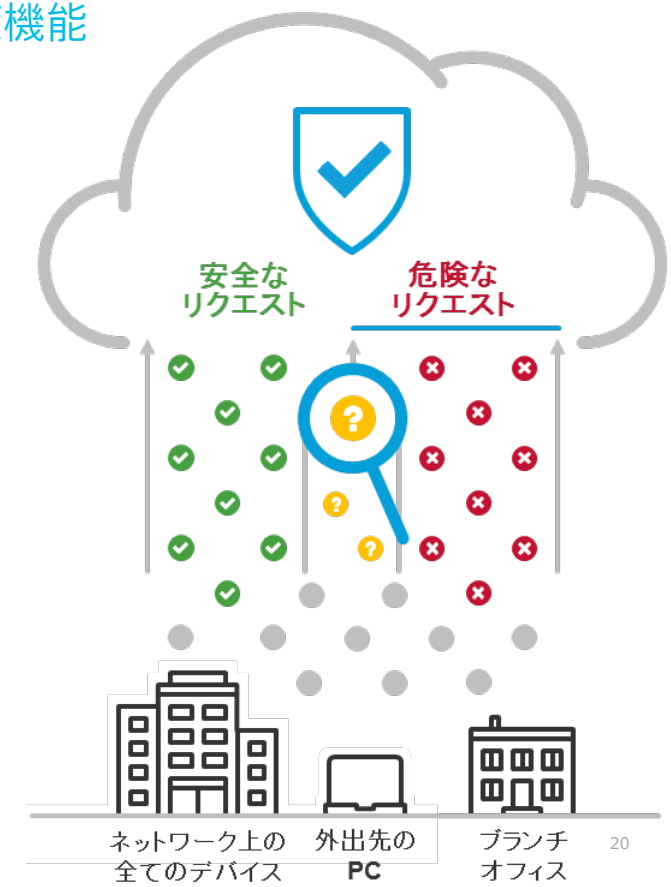
DNSセキュリティ

Cisco Umbrella とは

DNSの名前解決を利用した全く新しいセキュリティ対策機能

Cisco Umbrella の仕組み

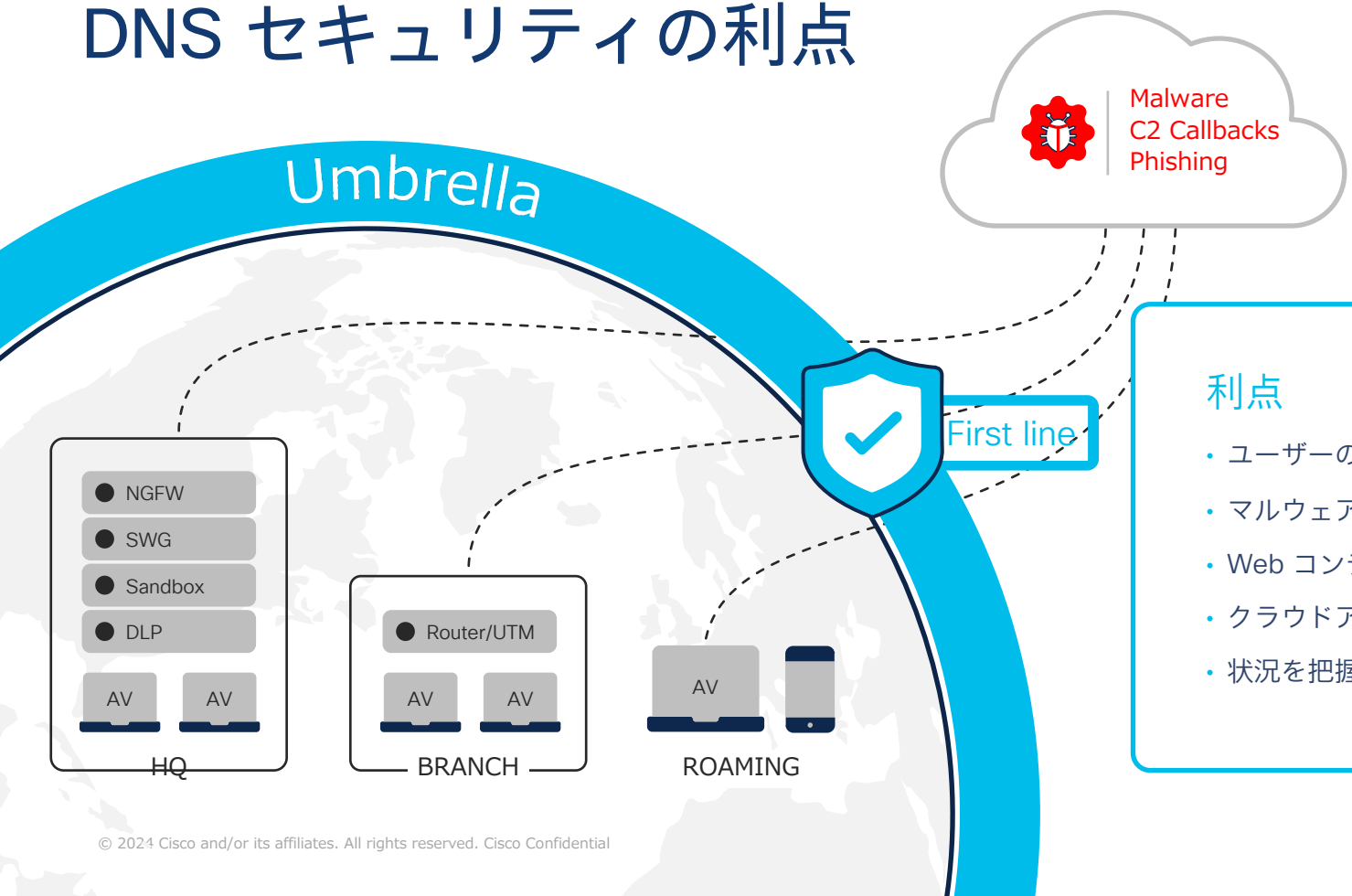
- 安全なサイトへの DNS リクエストは許可
- 危険なサイトへの DNS リクエストは拒否
- 断定できないWebサイトへの DNS リクエストは中身をチェック (インテリジェント プロキシ機能)
  - ➢URL/ファイルの安全性を詳細に評価
    - SSL Decryption(復号)
    - アンチウイルス、アンチマルウェア(AMP)



Cisco Umbrellaは高度で豊富なセキュリティ機能を持つ**DNSサービス**。
世界最大級の解析力と情報提供体制を誇る
シスコのセキュリティ インテリジェンス＆リサーチ グループ（Cisco Talos）と連携し、**常に最新のセキュリティ**を提供

DNSセキュリティ

DNS セキュリティの利点



利点

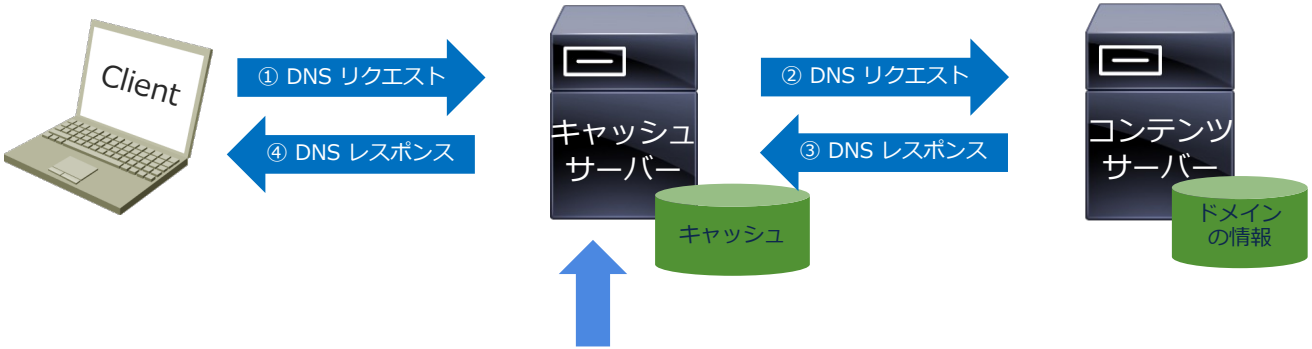
- ユーザーのインターネット接続の可視化
- マルウェアの封じ込め
- Web コンテンツフィルタを容易に
- クラウドアプリの管理・保護
- 状況を把握し素早く調査

DNSセキュリティ

DNS サーバーの役割

DNS サーバーには大きく分けて 2 種類ある

- 自身が管理しているドメインの情報を返す
  DNS コンテンツ サーバー (別名: 権威 DNS サーバー)
- クライアントからの DNS リクエストの代理を行う
  DNS キャッシュ サーバー (別名: フル サービス リゾルバ)

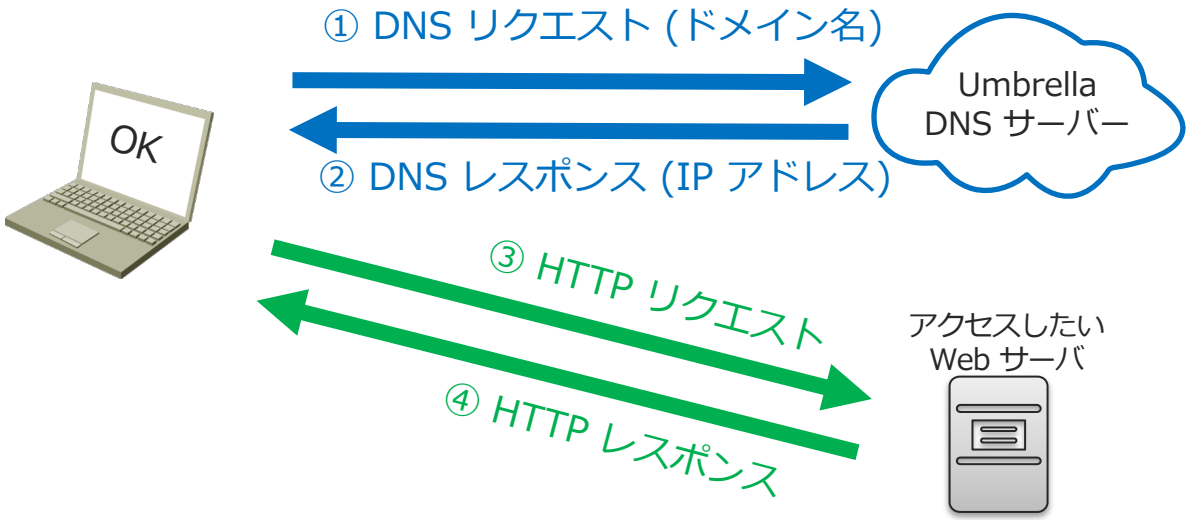


Umbrella はクラウド に設置された
セキュリティキャッシュサーバに該当する

DNSセキュリティ

Web アクセス時の Umbrella の DNS サーバー

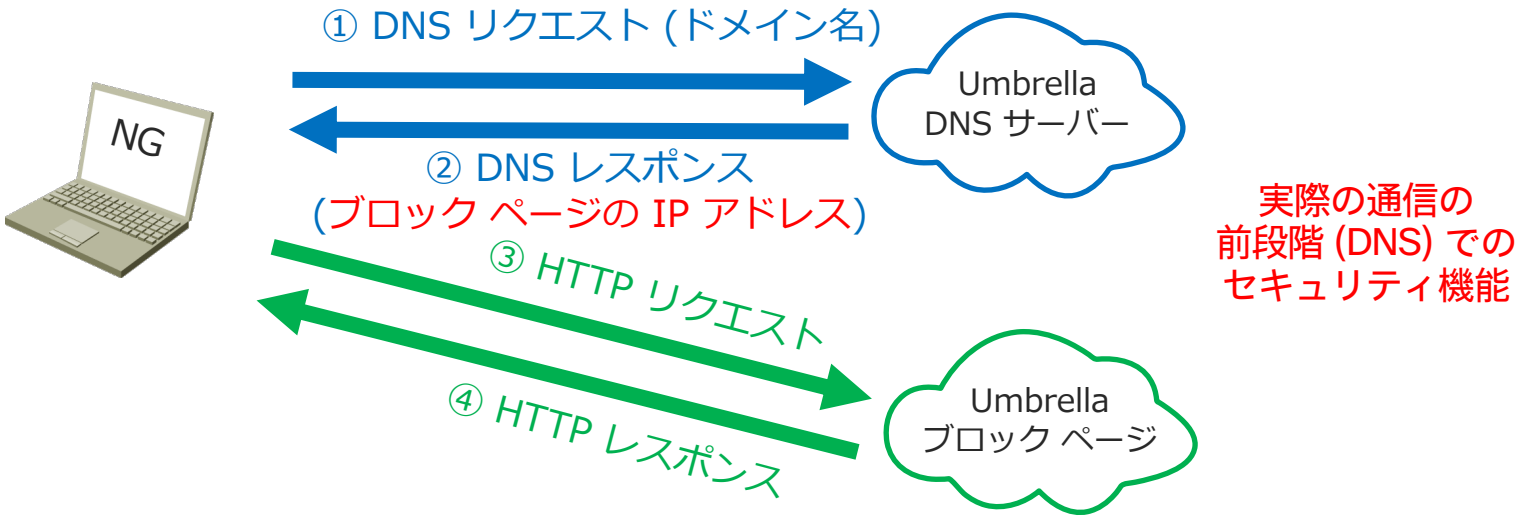
DNS の通信は Web アクセス (HTTP) の通信に先立つ



DNSセキュリティ

Web アクセス時の Umbrella の DNS サーバー

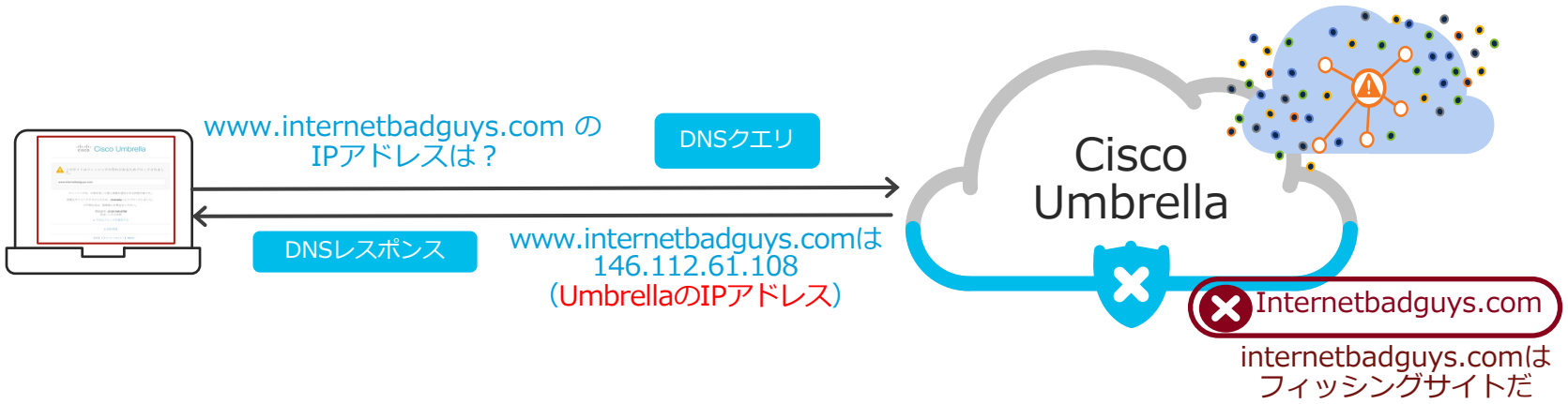
Umbrella の DNS サーバーは、問い合わせのドメイン名に危険性がある場合、ブロック ページの IP アドレスを返す



DNSセキュリティ

Secure DNS によるブロックの例

1. ブラウザがフィッシング メールにあるURLの解決を要求
2. DNSクエリがUmbrellaに向かう
3. 問い合わされたドメイン/URLの安全性をUmbrellaがチェック
4. ドメインがフィッシングに分類されていることが判明
5. ブロック ページ（フィッシング サイト用）のIPアドレスを回答
6. ブラウザがUmbrellaのブロック ページを表示



DNSセキュリティ

ブロック ページの例

リスクのあるページに
アクセスした際の
ブロックページ例

診断情報をクリックすること
でブロックされた理由の
詳細を確認できる

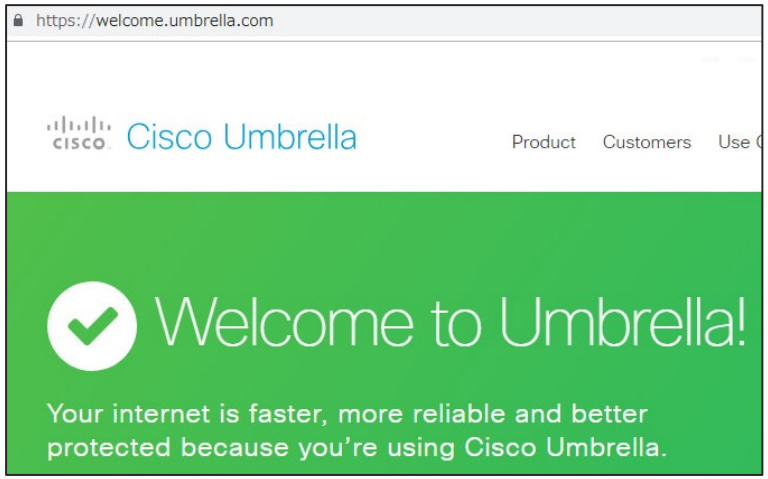
DNSセキュリティ

Web ブラウザによる到達性の確認

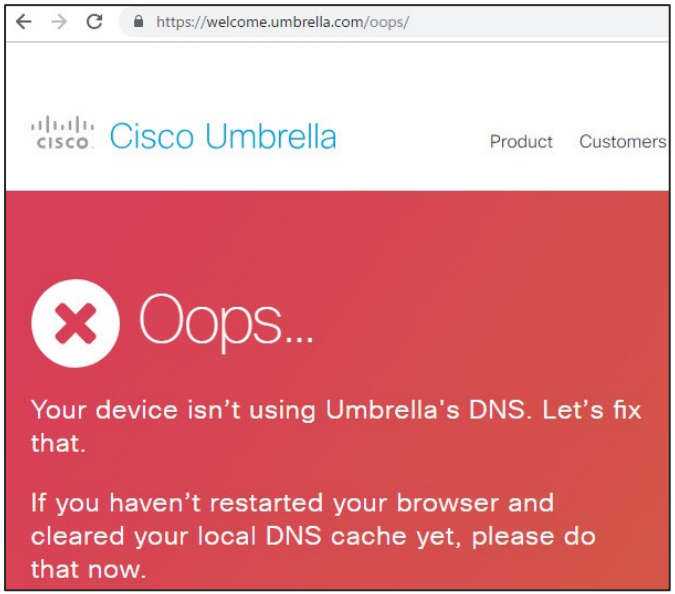
Web ブラウザで welcome.umbrella.com にアクセスすると、

DNS リクエストが Umbrella の DNS サーバーに到達するかが分かる

Umbrella 経由になっている場合



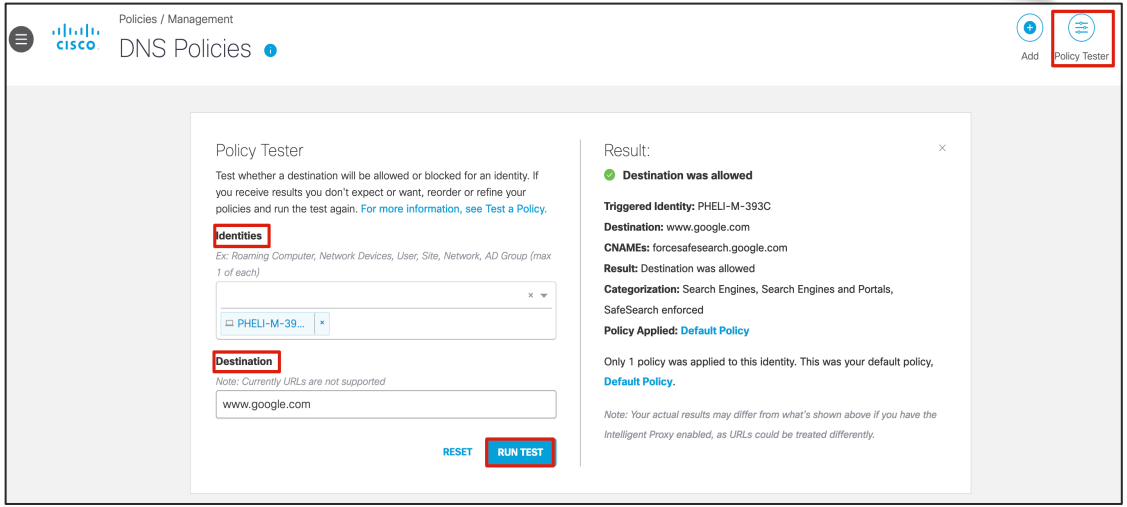
経由に到達できていない場合



DNSセキュリティ

DNS Policy Tester

DNS Policies のページで
Policy Tester をクリック



特定の 宛先のトラフィックに対して、どのポリシーが適用されるかを理解するのに非常に便利

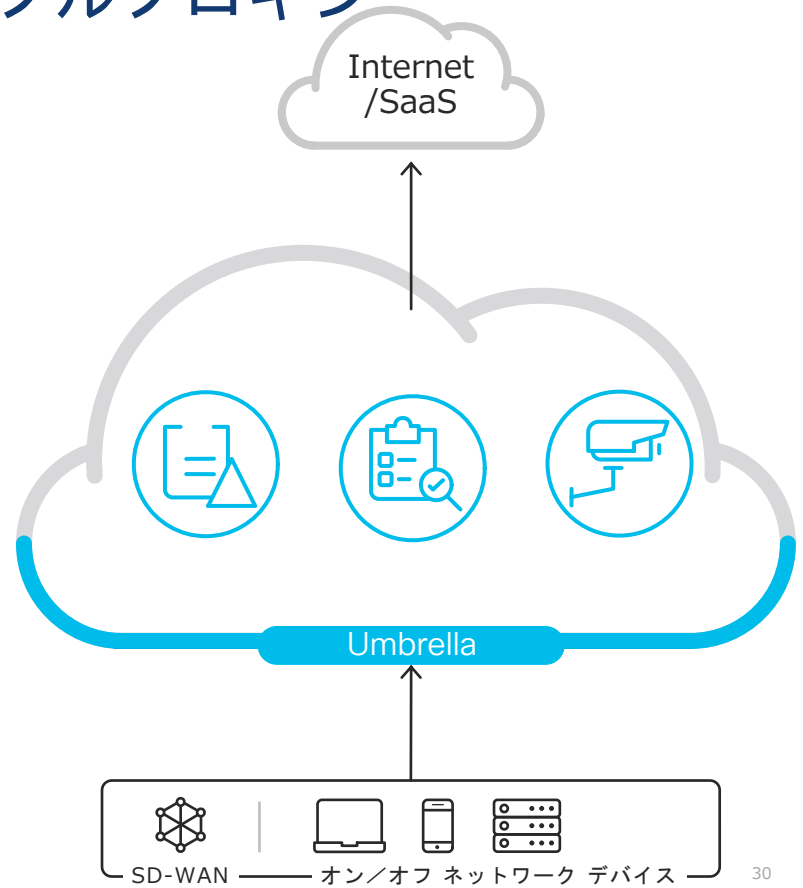
トラブルシュート や どの DNS ポリシー を構築する際に使用できる

Umbrella機能紹介
3.2. Web ポリシー

SIG

SWG (Secure Web Gateway)：フルプロキシ

- 全ての WEB トラフィックをキャプチャし、URL ロギングとブロッキング
- コンテンツ フィルタおよび URL ブロックにもとづく制御も可能
- SSL 復号により、暗号化トラフィックに対して、さらに多くのマルウェアをブロック
- Secure Malware Analytics (Threat Grid) サンドボックスによる解析も可能
- ファイルタイプ制御（特定タイプのファイルをブロックなどの制御）
- アプリケーション可視化と詳細な制御



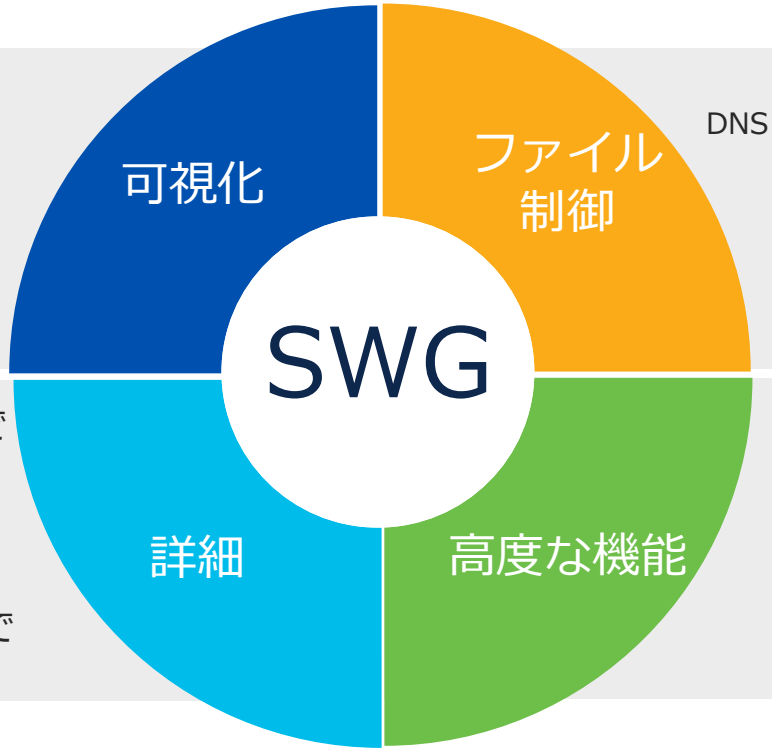
SIG

なぜ SWG を利用した Web Proxy が必要?

DNS はドメインのみ表示

SWG はフルURLを表示

DNSと異なり以下のファイル制御が可能
ファイルを分析し制御
サンドボックス解析
※1



DNS はビル(Domain) まで

SWG はビルの
どこ/誰であるか(URL) まで

テナントコントロール
ファイルの種別による制御

※1 DNSポリシーもインテリジェントプロキシを実施すれば一部通信で可能

DNSセキュリティ

DNS ポリシーも一部通信のみプロキシ可能

Secure DNS

名前解決の問い合わせに対し、IPアドレスを返答する前にそのドメインが安全かどうか確認

Intelligent Proxy

安全度がグレーなドメインへのアクセスを仲介して悪意のあるコンテンツをブロック

- File Inspection：ファイルがダウンロードされる前にスキャン、悪意のあるコンテンツが含まれていないか確認
- SSL復号：暗号化されたweb通信を復号して精査し、安全性を確認

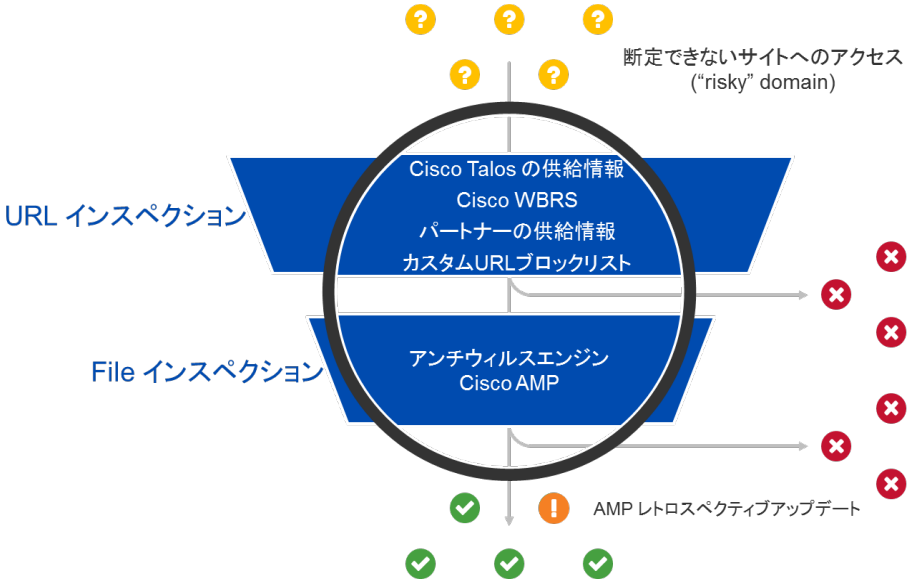
インテリジェント-プロキシとは

DNSセキュリティ

Intelligent Proxy とは？

グレー判定のドメインはURL/ファイルの安全性を精査

別名: Selective Proxy



複数のセキュリティ機能をもった Proxy で
Web のトラフィックを検査

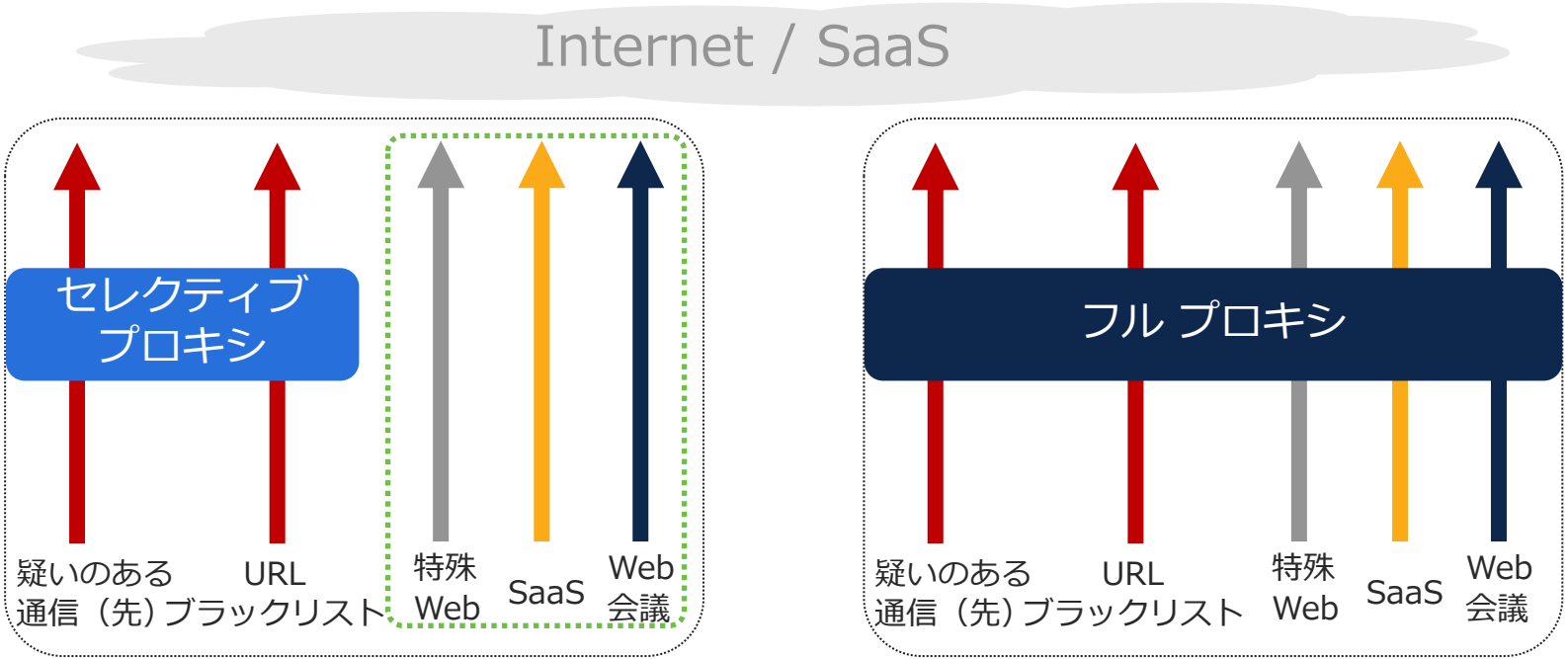
- Cisco Talos や WBRS (Webレピュテーション)などの情報を用いて、URL の安全性をチェック
- ファイルが含まれる場合、アンチウィルスとCisco AMP によってファイルの安全性をチェック
- 問題なければ通信を許可

事後対策として
Cisco AMPのレトロスペクティブ機能にも対応
(通過した未知のマルウェアが既知になった際に、
その存在を通知)

インテリジェントプロキシとフルプロキシ

	インテリジェント プロキシ	フル プロキシ
目的	DNS レイヤの展開の容易性を維持しながら保護を強化する	標準の完全な Web トラフィック プロキシ機能(可視性、制御、脅威)を提供し完全な SIG を実現
機能	選択した Web トラフィックを詳細に検査 (「グレー」ドメインのみ)	すべての Web トラフィックを詳細に検査し、きめ細かい制御とレポート作成を可能にします

セレクティブプロキシとフルプロキシ



安全なサイト宛の通信には関与しない

インテリジェント プロキシとフル プロキシ まとめ

セレクティブ プロキシのメリット

- DNS ポリシーで動作
- クラウド利用パフォーマンス
- IoT 機器に対するセキュリティ
- SaaS との相性
- コラボレーション ツールとの相性

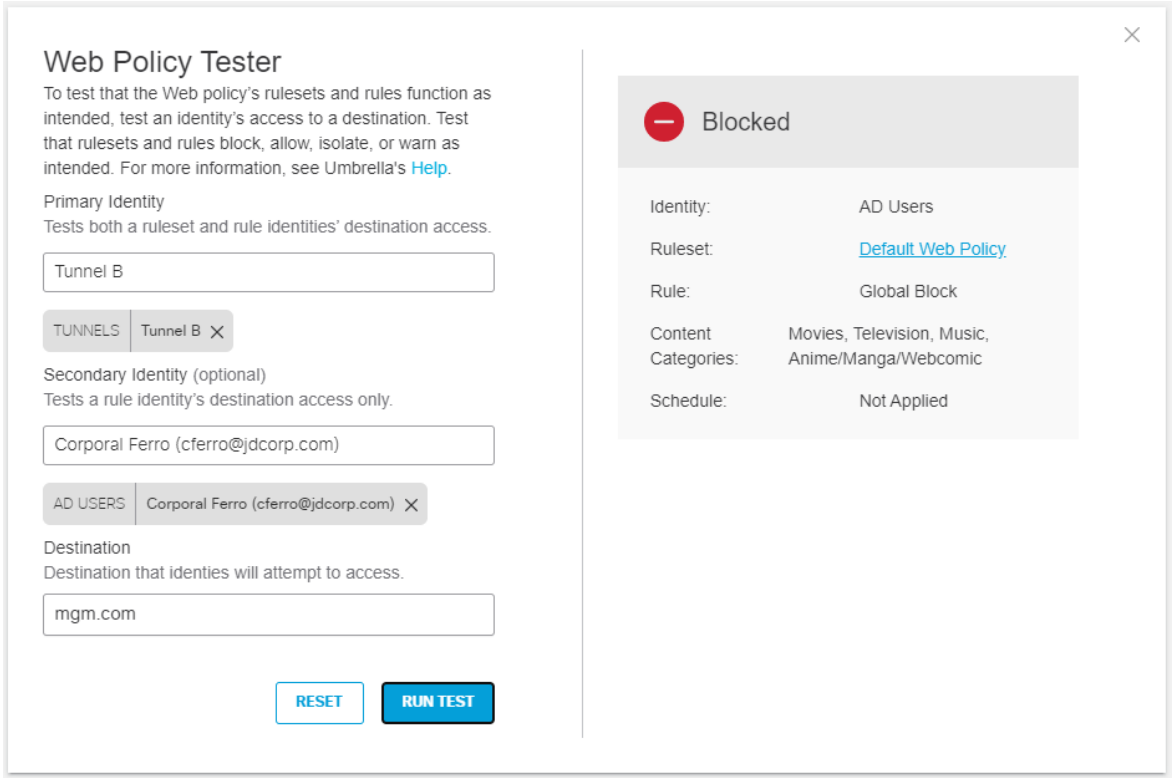
フル プロキシのメリット

- Web ポリシーで動作
- フル URL ログ
- 全ウェブ コンテンツのチェック (AV, Sandbox 等)
- 全ての通信ログ
- SaaS テナント制御
- Data Loss Prevention (DLP)

- パフォーマンスと脅威対策を両立するのはセレクティブ プロキシ
- コンプライアンスを実現するのはフルプロキシ

SWG Policy Tester

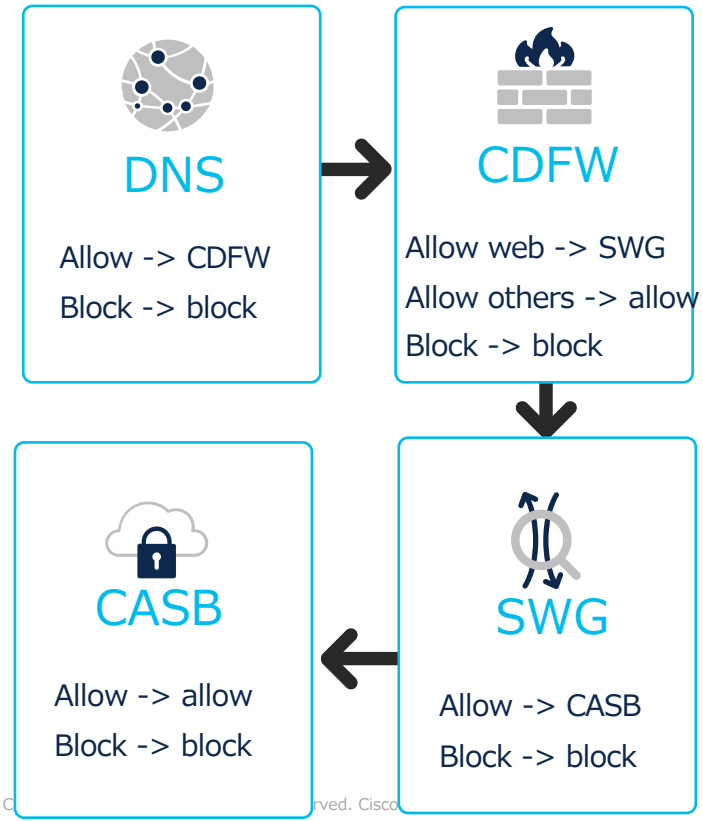
SIG

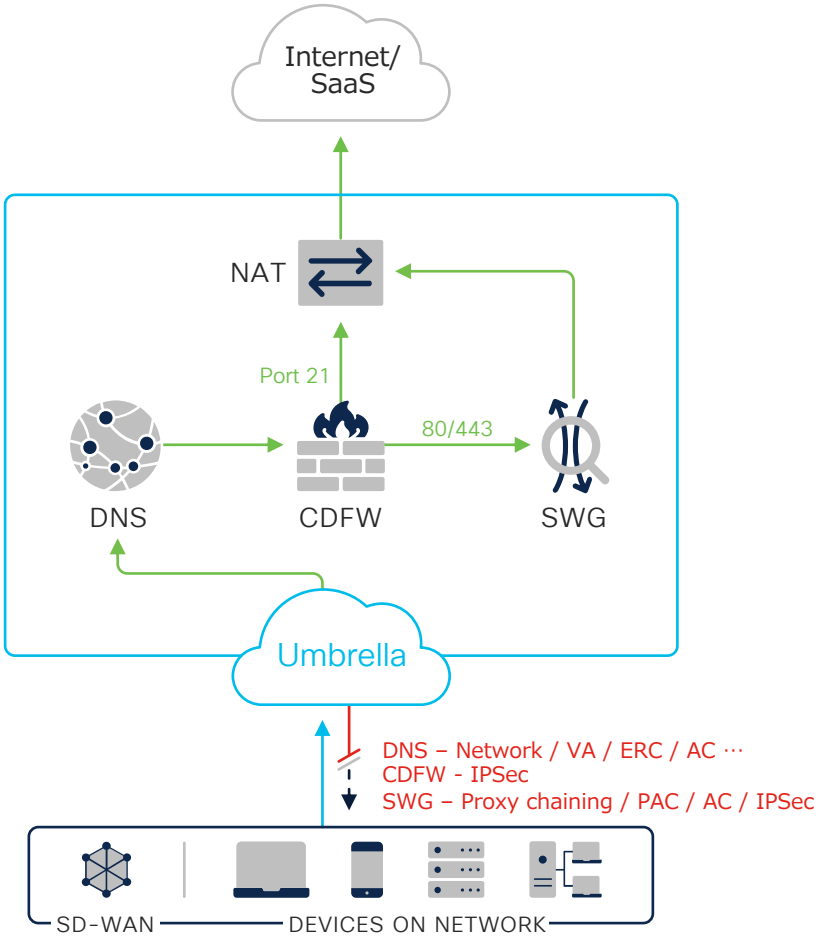


特定の IP や宛先のトラフィックに対して、どのルールセットやルールが適用されるかを理解するのに役たつ

トラブルシュッティングやWEBポリシーを構築する際に使用できる

ポリシーの適用の順序





ポリシーの適用ステップの詳細

DNS

DNS ポリシーが最初に評価され、許可されたトラフィックはその次に評価されます

CDFW

- CDFWは、DNSでブロックされていないものを評価します
- IPS はすべてのトラフィックを検査します
- ブロックされていない 80/443 のトラフィックは SWG に送ります

SWG

SWG は、DNS または CDFW によってブロックされていない 80/443 トラフィックを評価します

CASB

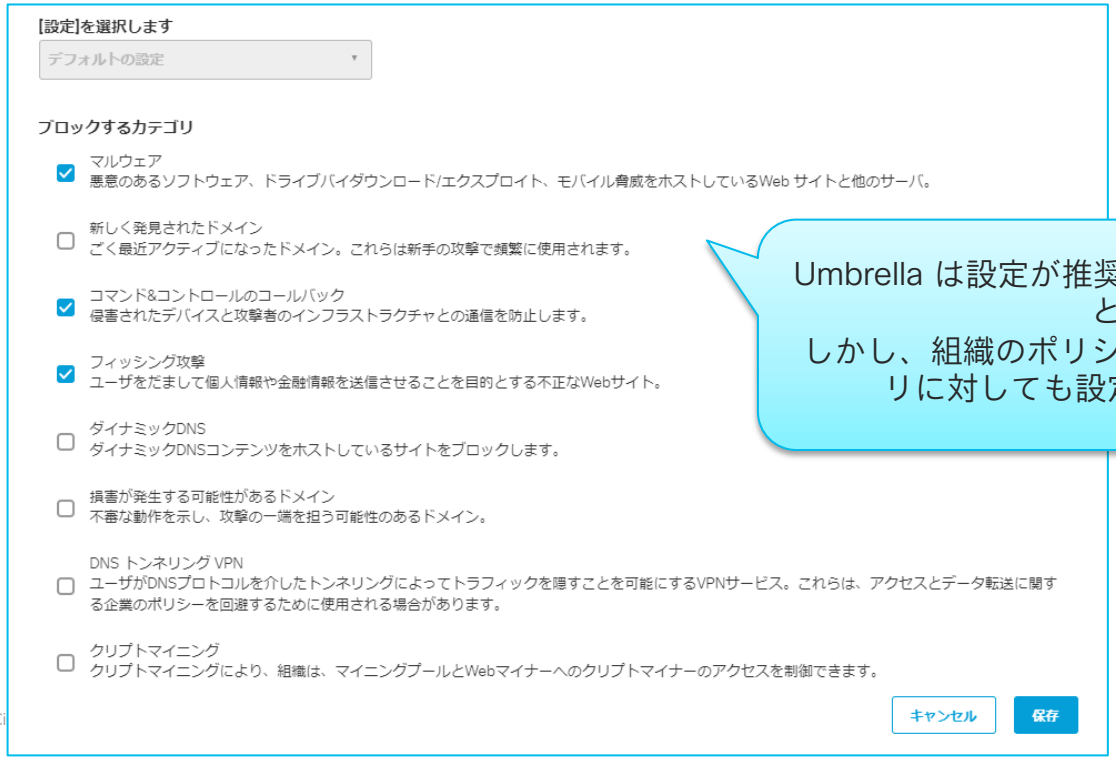
- アプリの挙動を検査し、企業コンプライアンスを確認します。
- 企業のコンプライアンスに対応したDLPでの検査を行います

Umbrella機能紹介
4. セキュリティ設定

DNS ポリシー内のセキュリティ設定

セキュリティ設定とは？

各ポリシーごとにセキュリティ設定を適用することができます。以下のキャプチャはデフォルトで有効となっている
セキュリティ設定のブロックカテゴリになります。



Umbrella は設定が推奨とされる 3 項目がデフォルトで有効となっています。
しかし、組織のポリシーや扱う情報によっては他のカテゴリに対しても設定することをご検討ください。

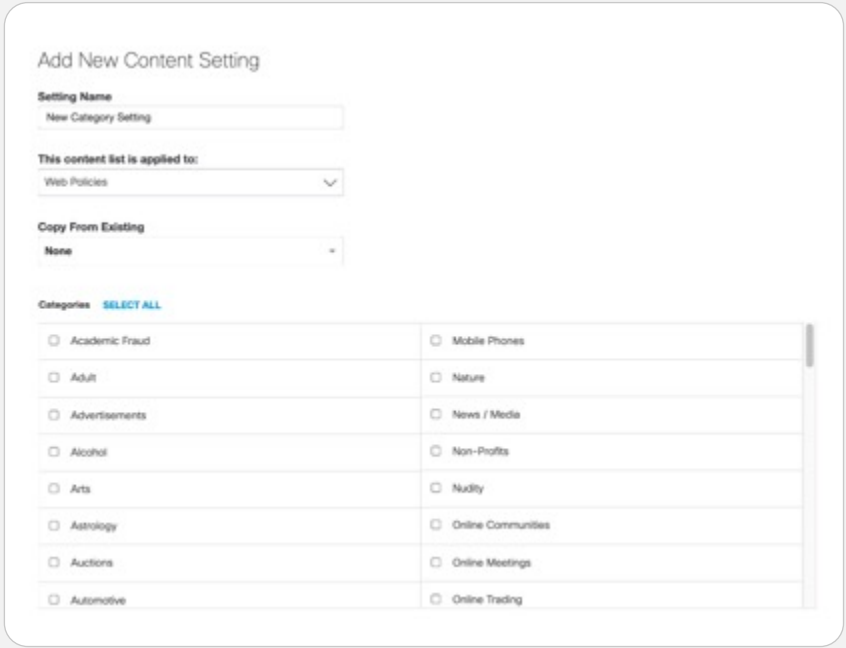
DNS ポリシー内のセキュリティ設定

デフォルト有効となっていないセキュリティカテゴリの詳細

新たに確認されたドメイン	初めて Cisco Umbrella を介してクエリされ、Cisco Umbrella がまだClient Lookup を確認していないドメインへのアクセスをブロックします。そのため、条件により正常な新規ドメインをブロックする可能性もあります。 決まった宛先にしか通信しないような部署のポリシーには適用してもよいかもしれません。
ダイナミックDNS	ダイナミック DNS コンテンツをホストするサイトへのアクセスをブロックします。ダイナミック DNS を利用したコンテンツを組織で利用していない場合には設定を検討ください。
損害が発生する可能性があるドメイン	不審な動作を示し、攻撃の一部である可能性があるドメインへのアクセスをブロックします。Talos によって、疑わしいスコアであるが、悪意があるとまだ断定されていないドメインです。 こちらは組織のリスクに対する許容度と可用性によって判断が必要です。 安全性がより高い水準で求められる環境の場合、設定が推奨です。
DNSトンネリングVPN	ユーザーがDNSプロトコルを介したトンネリングによってトラフィックを隠すことを可能にするVPNサービスをブロックします。これらのサービスは、アクセスとデータ転送に関する企業ポリシーをバイパスするためによく使用されます。
クリプトマイニング	仮想通貨マイニングプールへのアクセスをブロックします。また、既知の Web 仮想通貨マイニング ソース コード リポジトリをブロックします。

コンテンツカテゴリ設定

- 多くのサイトにポリシーを適用
  - コンテンツカテゴリは「Webポリシー」「DNSポリシー」に適用可能
  - 「DNSポリシー」ではプリセットされたカテゴリ（高・中・低でプリセットレベル分け）で簡単に適用可能
- コンテンツとセキュリティの両方にTalos® カテゴリを使用
- 100 以上のカテゴリ
- 動的なクラウド更新（フルデータセット）



Umbrella機能紹介
5. デモ ①
ポリシーによる動作

Umbrella の運用について

Umbrella を活用した可視化に関する運用３選

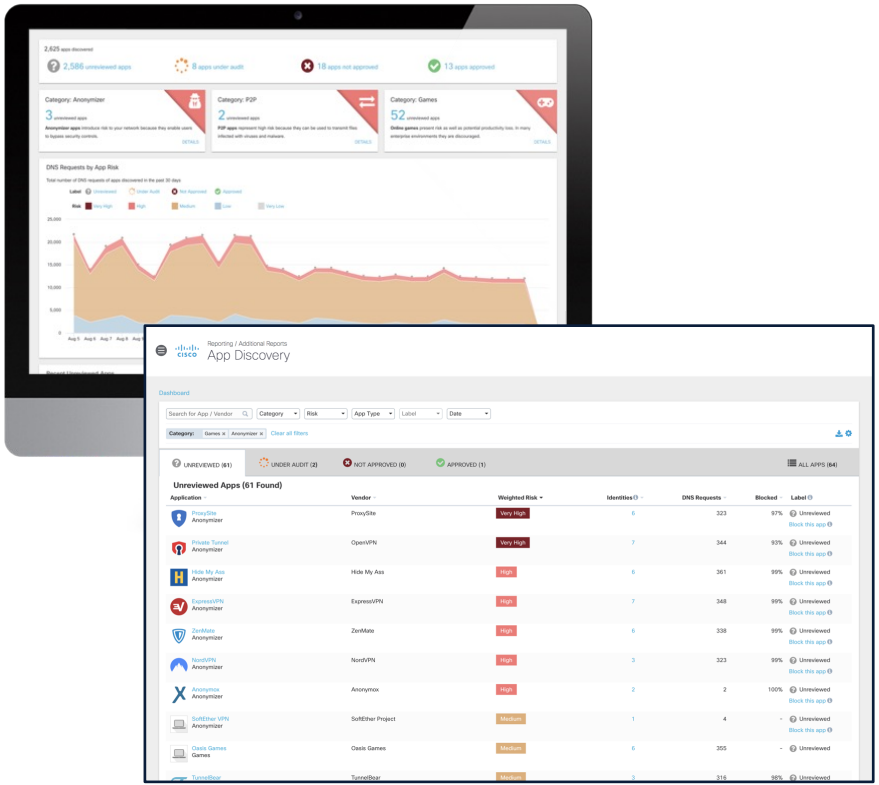
ここではUmbrellaの可視化を最大限に利用可能な運用３選を紹介します。

アプリケーション可視化によるシャドーIT対策	✓ 組織で許可のないクラウドサービスを利用していないか確認したい
インシデント発生時における通信ログ調査	✓ 脅威の侵害や情報流出のインシデント対応で通信ログを調査したい
インターネット宛トラフィックトレンドの把握	✓ 設備投資への判断材料としてトラフィックの傾向を把握したい

Umbrellaの可視化機能はDX・リモートワーク・クラウド活用を最大限に支援

Umbrella の運用について
6. アプリケーション可視化

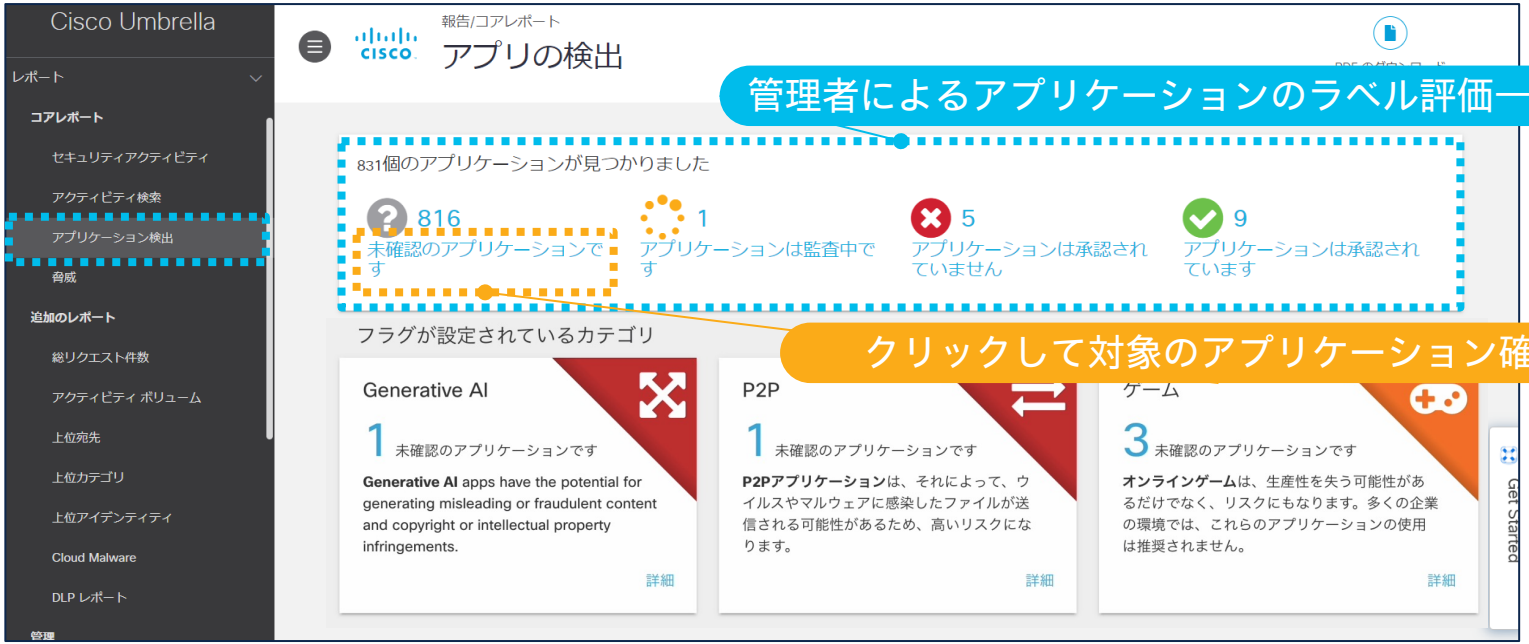
アプリケーション検出 機能概要



- ✓ 組織内のユーザーが生成した通信で Umbrella まで到達したパケットをもとに、クラウドアプリケーションの利用状況を可視化（使用中のアプリケーションをリスト化）
- ✓ クラウドアプリケーションのリスクスコア・ベンダー・アプリケーション・証明書・リスク要因に関する詳細情報を表示
- ✓ ユーザー数と送受信のトラフィック量を表示 (SWG 併用の場合)
- ✓ アプリケーション検出機能から対象のアプリケーションを許可・ブロックすることが可能

アプリケーション検出 トップページ

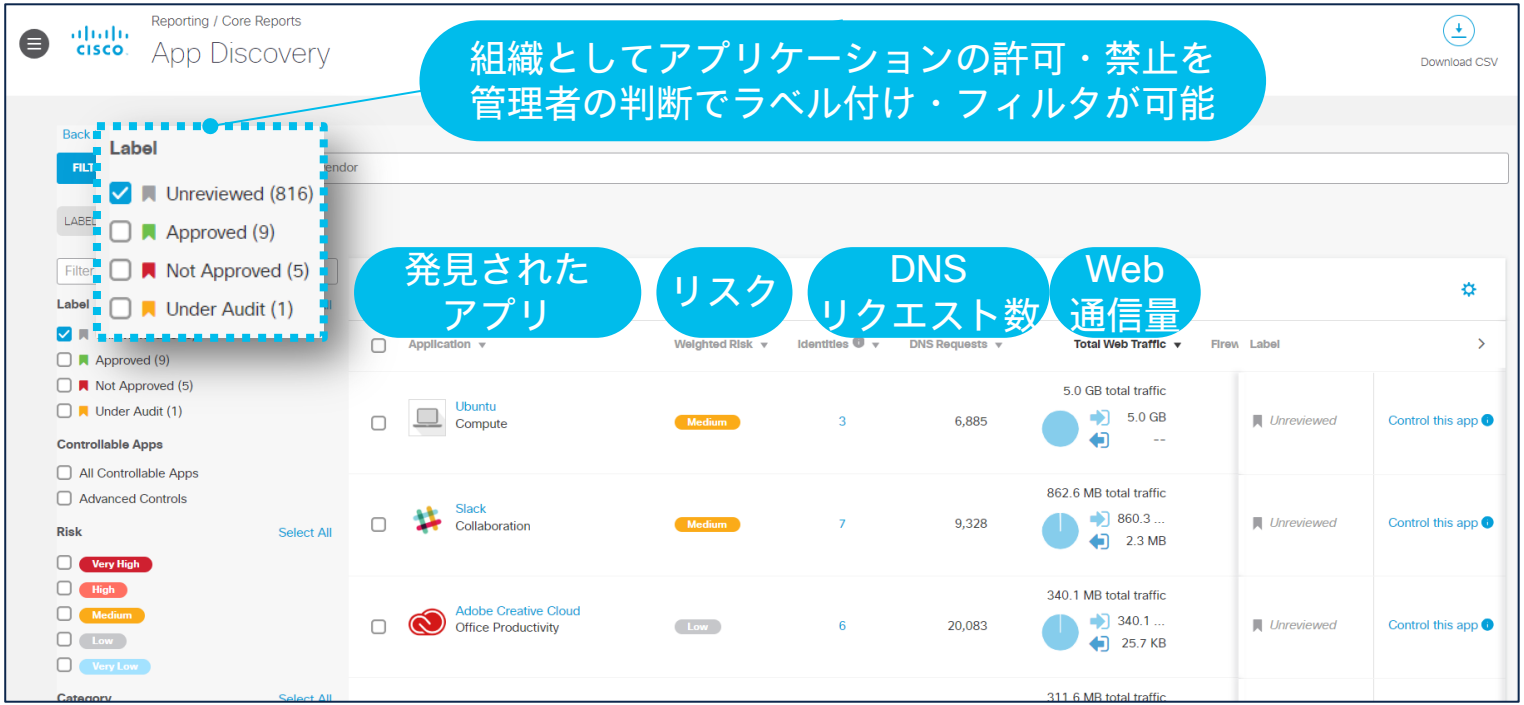
トップページからは発見されたアプリケーションに関するサマリーを確認できます。



組織の管理者によるアプリケーション監査が可能に

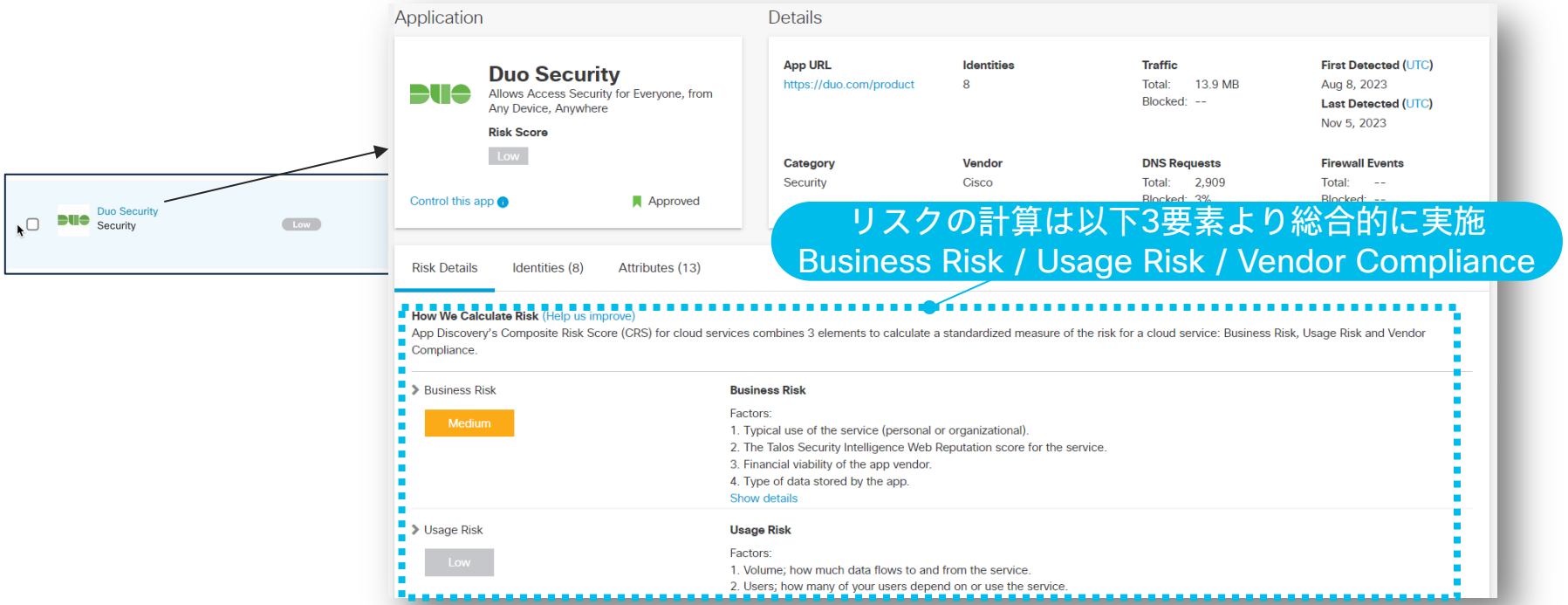
アプリケーション検出 一覧画面

一覧画面からはアプリケーションのリスト、リスクや通信量を確認できます。



アプリケーション検出 詳細画面 (1/2)

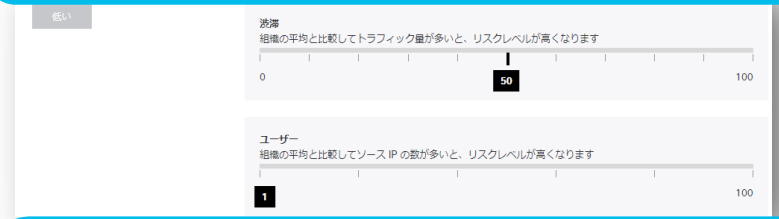
詳細画面からはアプリケーションを評価したリスクの詳細など確認できます。



アプリケーション検出 詳細画面 (2/2)

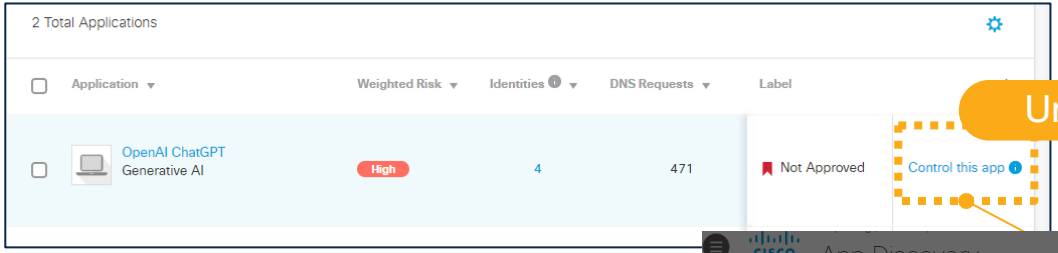
ウェブレピュテーションや財務状況等を基に評価

トラフィック量や送信元IPの数を基に評価



クラウドアプリケーションベンダーの
各種業界標準コンプライアンス対応を基に評価

アプリケーション検出 制御の運用



Umbrellaのポリシー設定リンクをクリック

DNSポリシー

Webポリシー

利用中のDNS・WEBポリシーへ
直接設定変更可能

ブロック用のアプリケーションリストを選択して保存

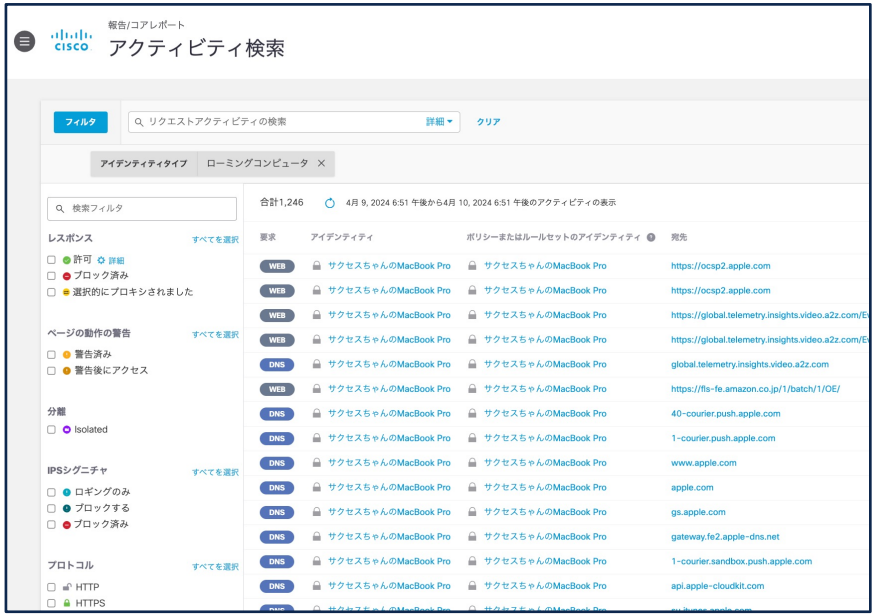
アプリケーション検出 制御の運用

“Control this app” から
直接設定変更した
Webポリシーのルール

設定変更後はポリシーの
ルールに紐づく
端末やネットワークからの
通信をブロック

Umbrella の運用について
7. Activity Search

Activity Search 機能概要



- ✓ Activity Search レポートには Umbrella が処理した全ての通信 (アクティビティ) が一覧で表示
- ✓ 特定の通信のみを抽出するための豊富なフィルタを用意
- ✓ フィルタを1つまたは複数を同時に利用することが可能
- ✓ 通信ログの種類はDNS、Web、Firewall、IPSの4つ

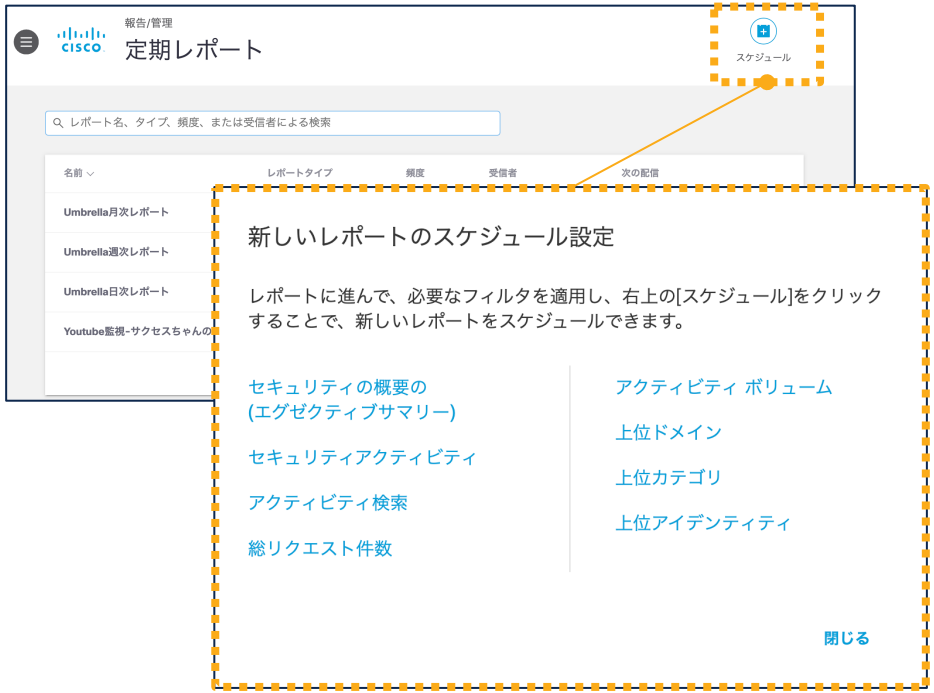
Activity Search 画面詳細

「完全な詳細を表示」をクリックすると
通信ログの詳細が確認可能

* 右スクロールでもいくつかの情報を確認可能

Umbrella の運用について
8. レポート

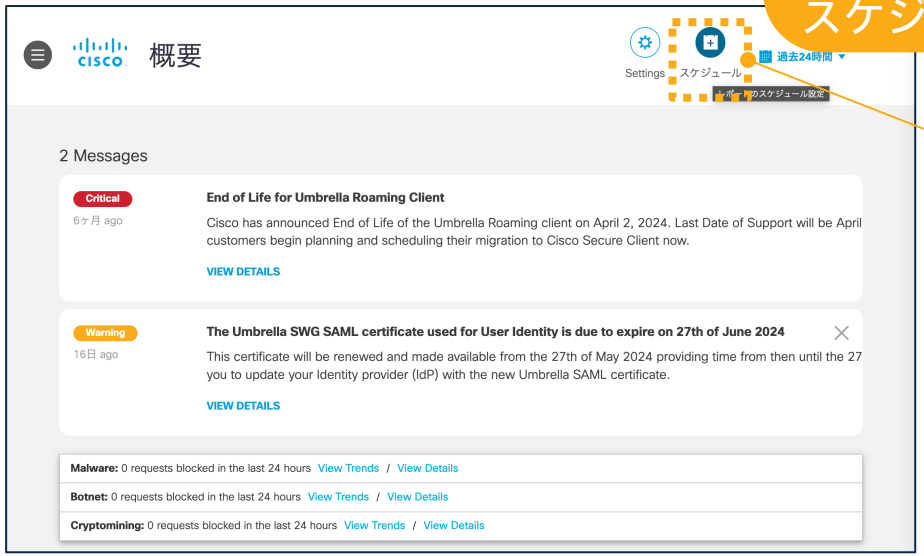
レポート 機能概要

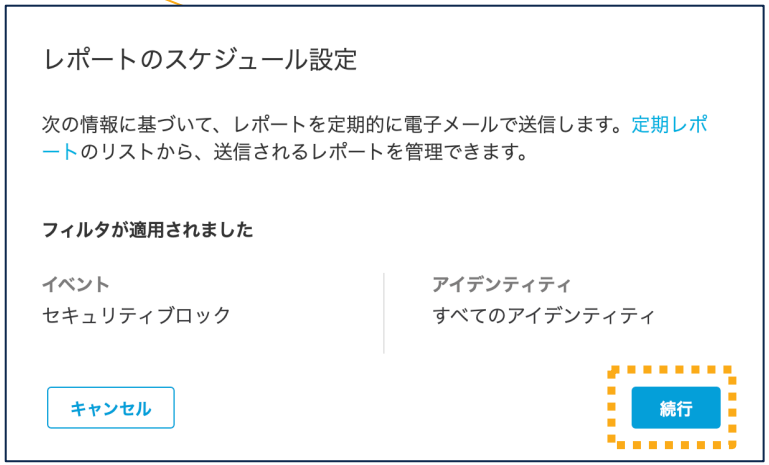


- ✓ Umbrella Dashboard のメニューの一番上にある概要 (Overview) もレポートの一種
- ✓ Umbrella の現在の状況を一目で確認するのに非常に便利
- ✓ ユーザがカスタムで作成する事も可能
- ✓ スケジュール設定を使って日次・週次・月次でレポートをメールに送信可能

レポート 設定方法 (1/2)

概要ページの
スケジュールをクリック



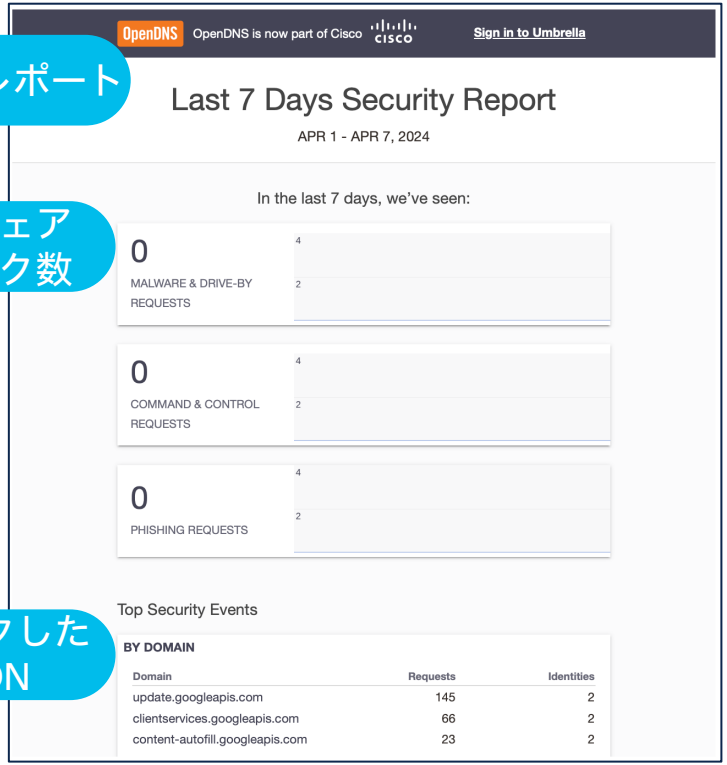


レポート 設定方法 (2/2)

電子メールで送信する期間を指定

レポートのタイトルとメールアドレスを指定

レポート サンプルメール本文



週次のレポート

マルウェア ブロック数

ブロックした FQDN

セキュリティイベントが発生した アイデンティティの数

デプロイ状況

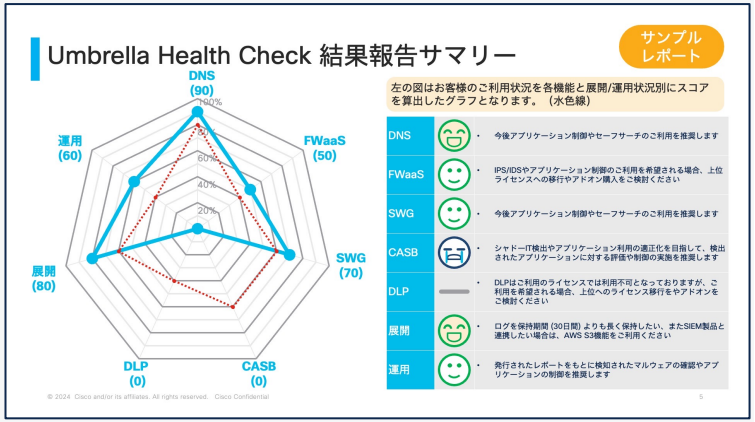
Umbrellaコンソールへ アクセス可能なリンク

詳細はリンク先へ 定例会等で活用

Umbrella機能紹介
9. デモ ②
Umbrella を活用した可視化

Umbrella の運用について
10. Q&A

Cisco Umbrella 健康診断サービス



期間限定トライアル (～ 2024.7)

お問合せ先：
ciscocxseminar@cisco.com

このような課題はありませんか？

- ✓ とりあえず導入したが適切に利用できているか不明
- ✓ 有効に活用できているのかを定量的に知りたい
- ✓ 新しい技術も取り入れたいが学習時間の確保が難しい

Cisco Umbrella 健康診断サービスは
お客様の製品利活用の悩みを解決

STEP①

健康診断

ベストプラクティスを基にご利用状況を確認します

STEP②

レポート報告

現在のご利用状況の良い点・更に良くなる点を評価します

STEP③

技術支援

新規利用や改善のために技術支援を実施、お客様の課題解決を実現します

YouTube チャンネル ご紹介

https://www.youtube.com/@Cisco-Success-Channel

1.49K subscribers

298 videos

シスコ社員が有志で運営する
＼ 非公式のYouTubeチャンネル ／

サクセスちゃんねるで検索！！


Cisco
Customer Experience