

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

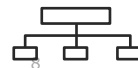
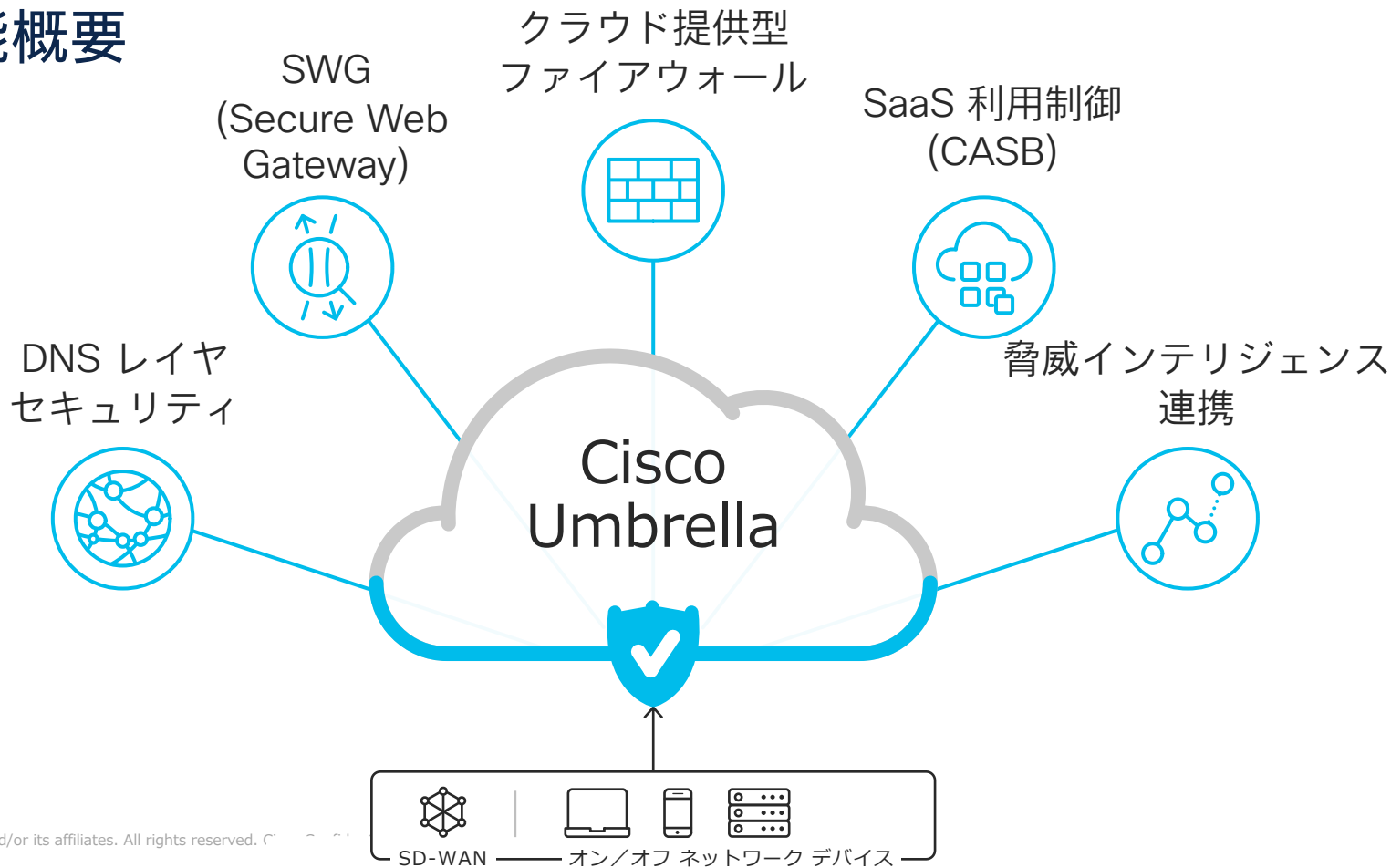


Umbrella 機能紹介

1. Umbrella とは？

1. Umbrella とは？

機能概要



1. Umbrella とは？

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

1. Umbrella とは？

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 (セレクトティブ プロキシ)	—	○	○	○
ファイル インスペクション - アンチウイルス、AMP	—	○ (Proxy 利用時)	○	○
マリシャスな URL のフィルタリング	—	○ (Proxy 利用時)	○	○
SSL 復号	—	○ (Proxy 利用時)	○	○
セキュア ウェブ ゲートウェイ (SWG、フル プロキシ)	—	—	○	○
L3-L4 クラウド型ファイアウォール	—	—	○	○
L7 クラウド型ファイアウォール および IDPS	—	—	オプション	○
サンドボックスによるファイル解析(Threat Grid)	—	—	○ (500 サンプル / 日)	○ (制限無し)
クラウド マルウェア検知	—	—	○ (2 つまで)	○ (制限無し)
CASB (App Discovery & Blockingではない機能)	—	—	○	○
DLP	—	—	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))	—	—	オプション	オプション

※1 Domain Filtering, Security Blocking, App Discovery & Blocking, Network and Branch Protection

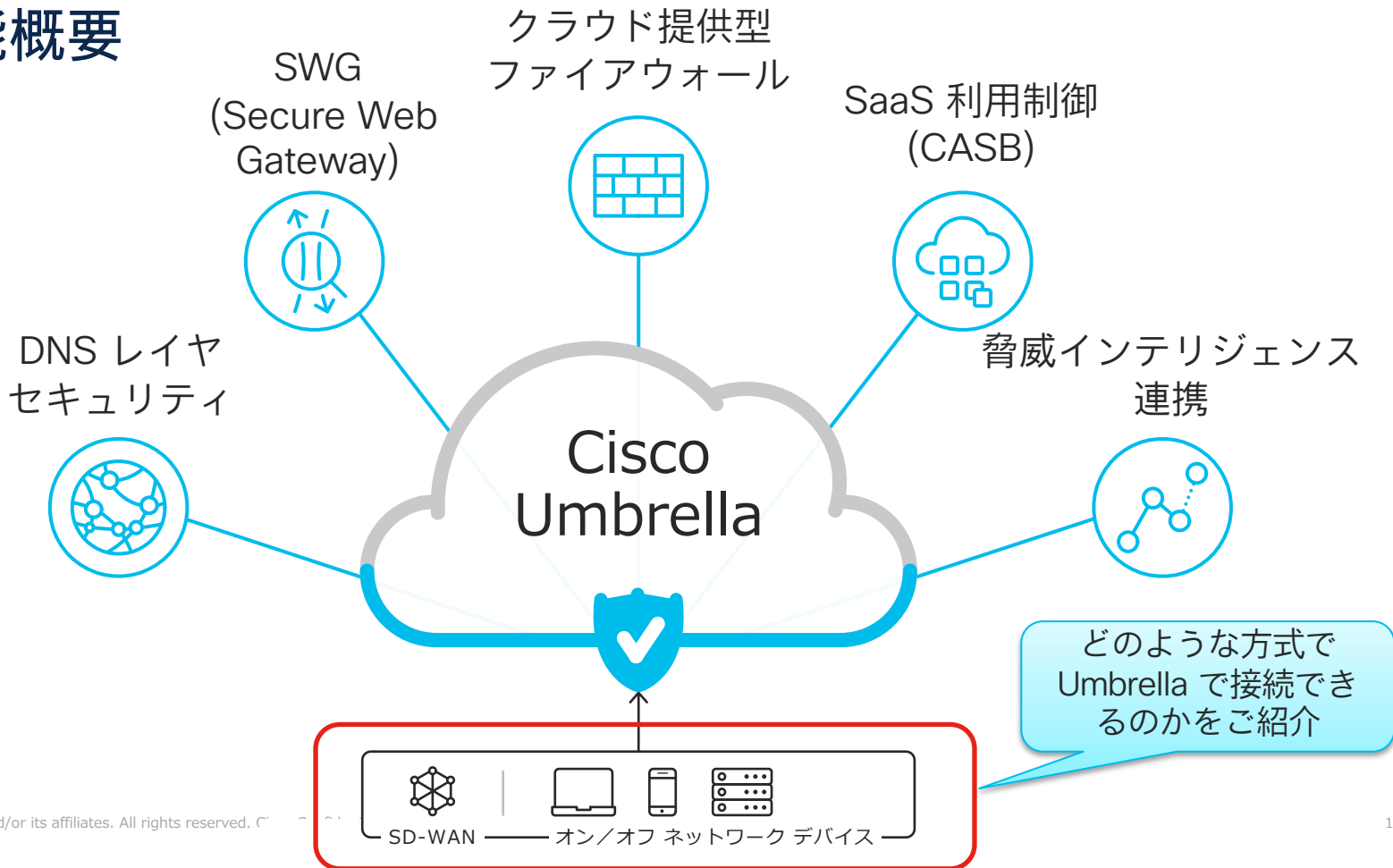
※2 Roaming Client の EoL が発表されており、[サポート終了日が 2025年 4月 2日](#)となっています 10



Umbrella機能紹介

2. 接続方式

機能概要



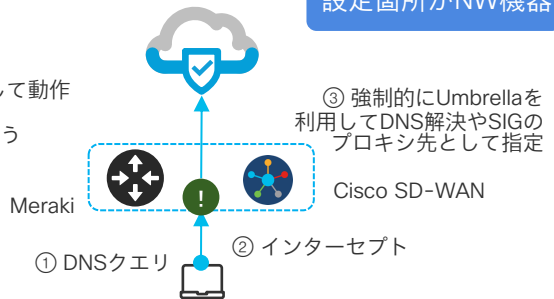
2. 接続方式

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 :

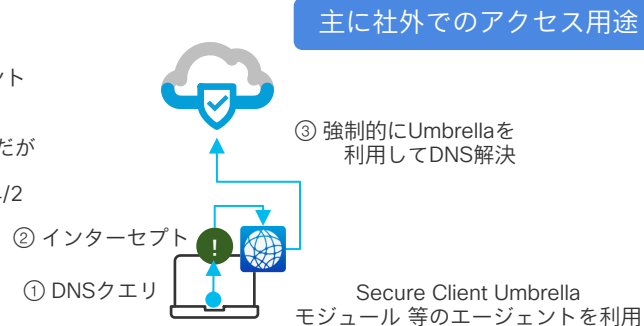
Cisco のWANルータ
Meraki, SD-WAN
から Umbrella と連携して動作
ネットワーク機器から
Umbrella への接続を行う



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



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



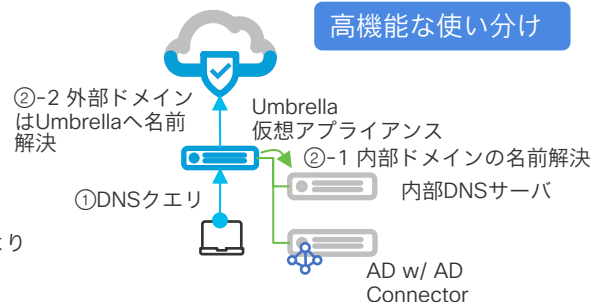
パターン 4 :

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

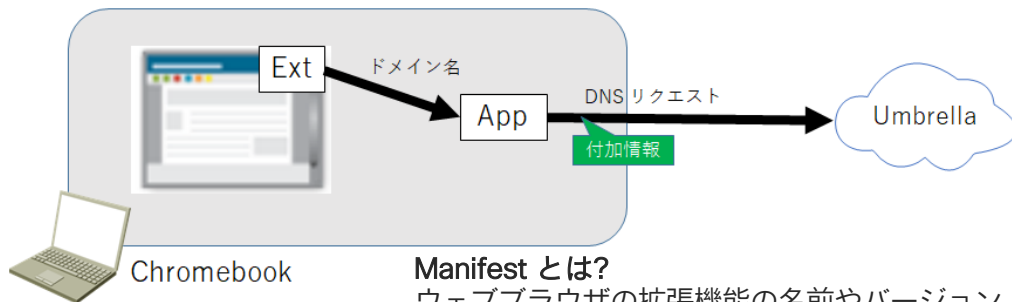


【注意】 Chromebook Client で Umbrella をご利用の方

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-](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)

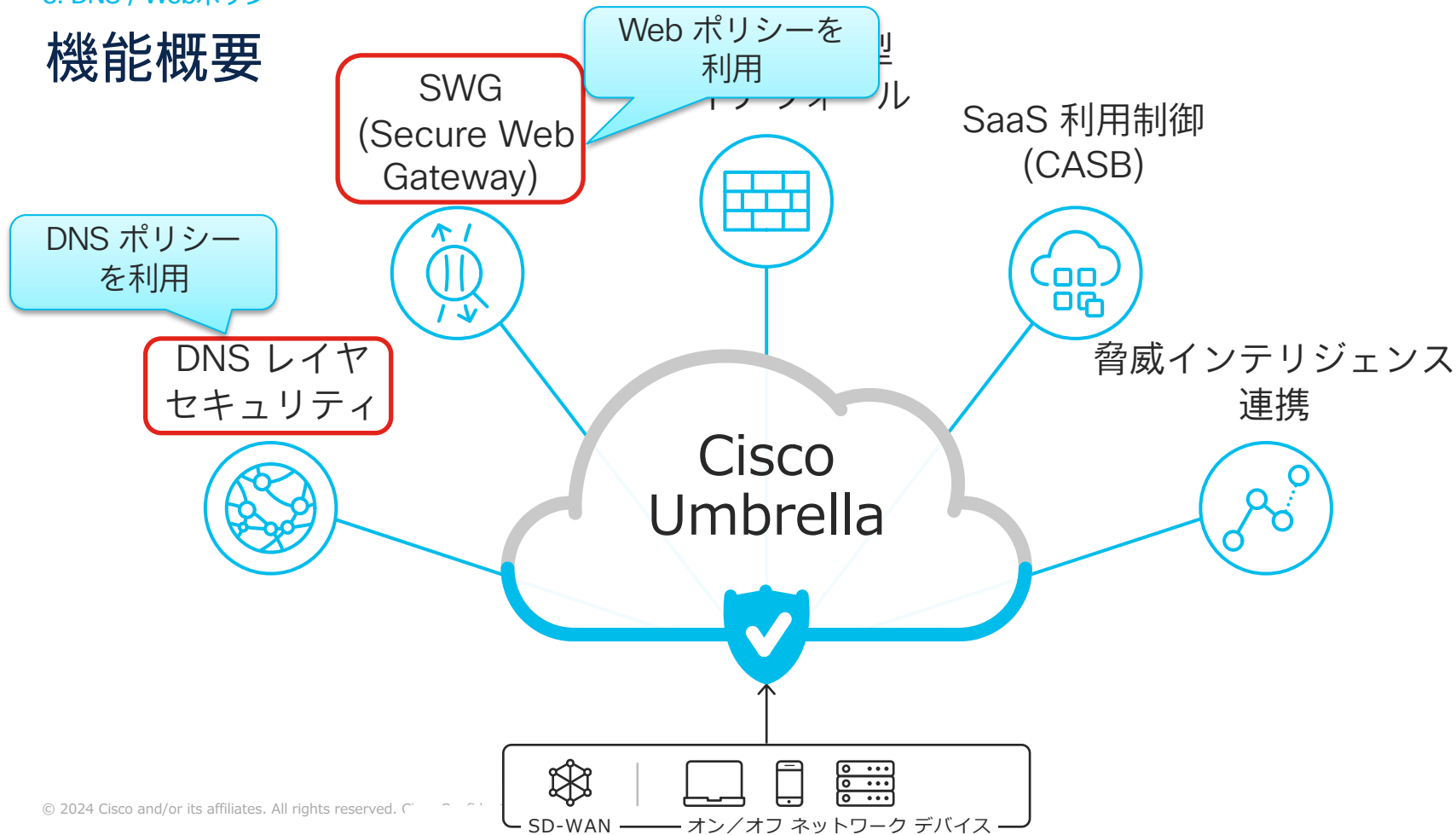
[ExtensionManifestV2Availability-Policy-for-Both-Umbrella-Chromebook-Client-SWG-Umbrella-Chromebook-Client](https://support.umbrella.com/hc/en-us/articles/21106444957332-Take-Action-Now-Enable-the-ExtensionManifestV2Availability-Policy-for-Both-Umbrella-Chromebook-Client-SWG-Umbrella-Chromebook-Client)



Umbrella機能紹介

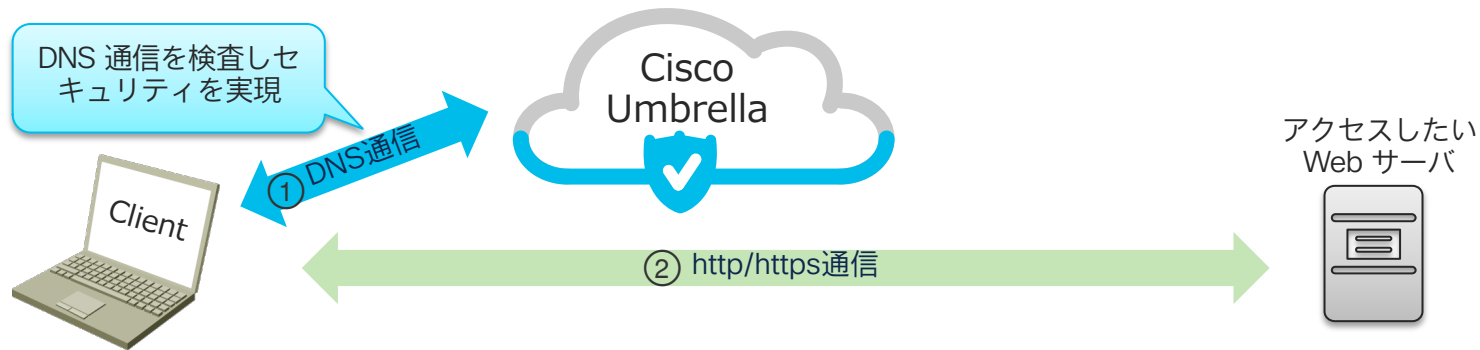
3. DNS / Webポリシー

機能概要

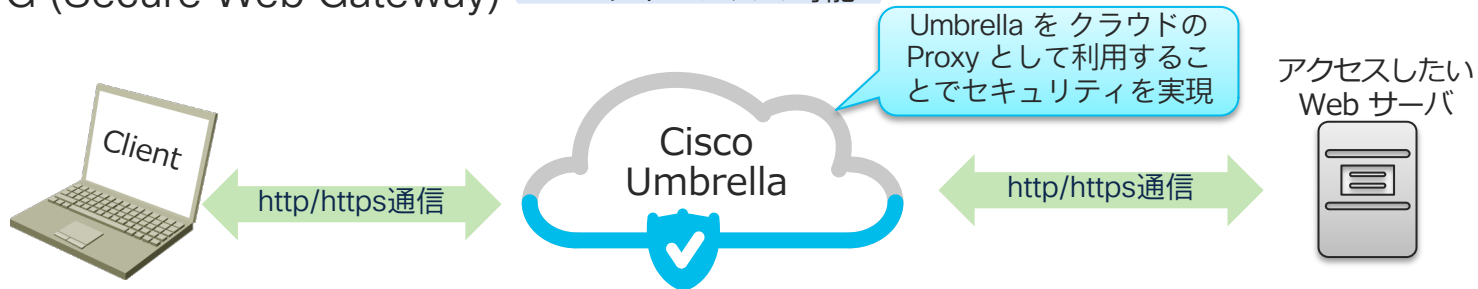


DNS レイヤセキュリティと SWG の違い

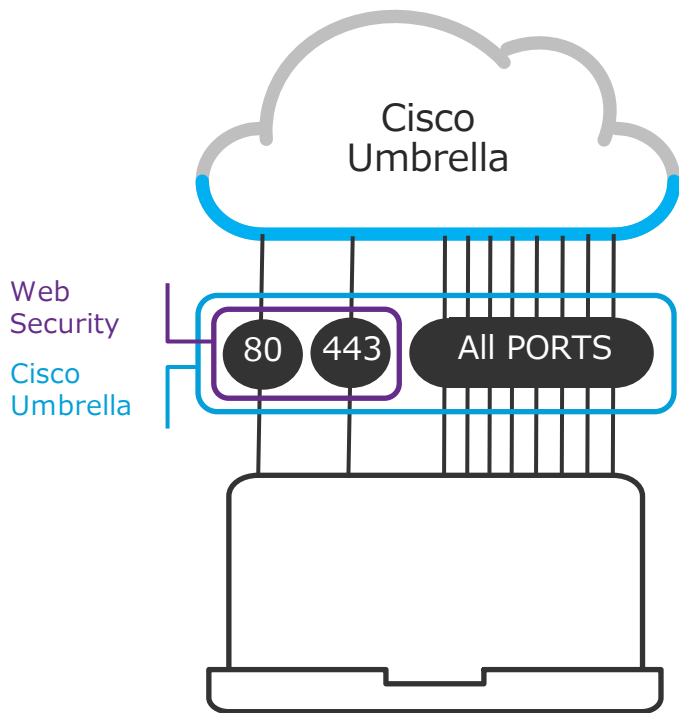
■ DNS セキュリティ DNS Security ライセンスで可能



■ 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

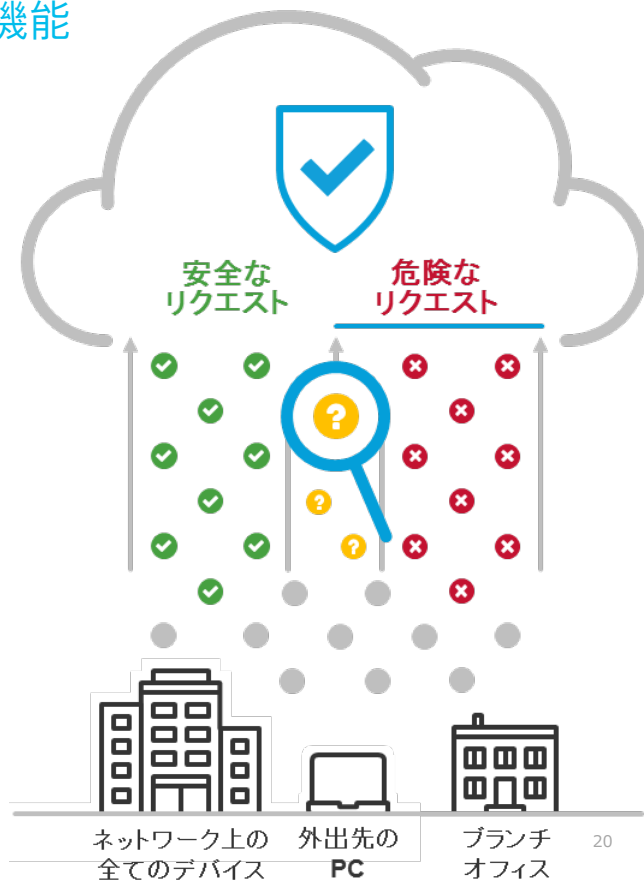
Cisco Umbrella とは

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

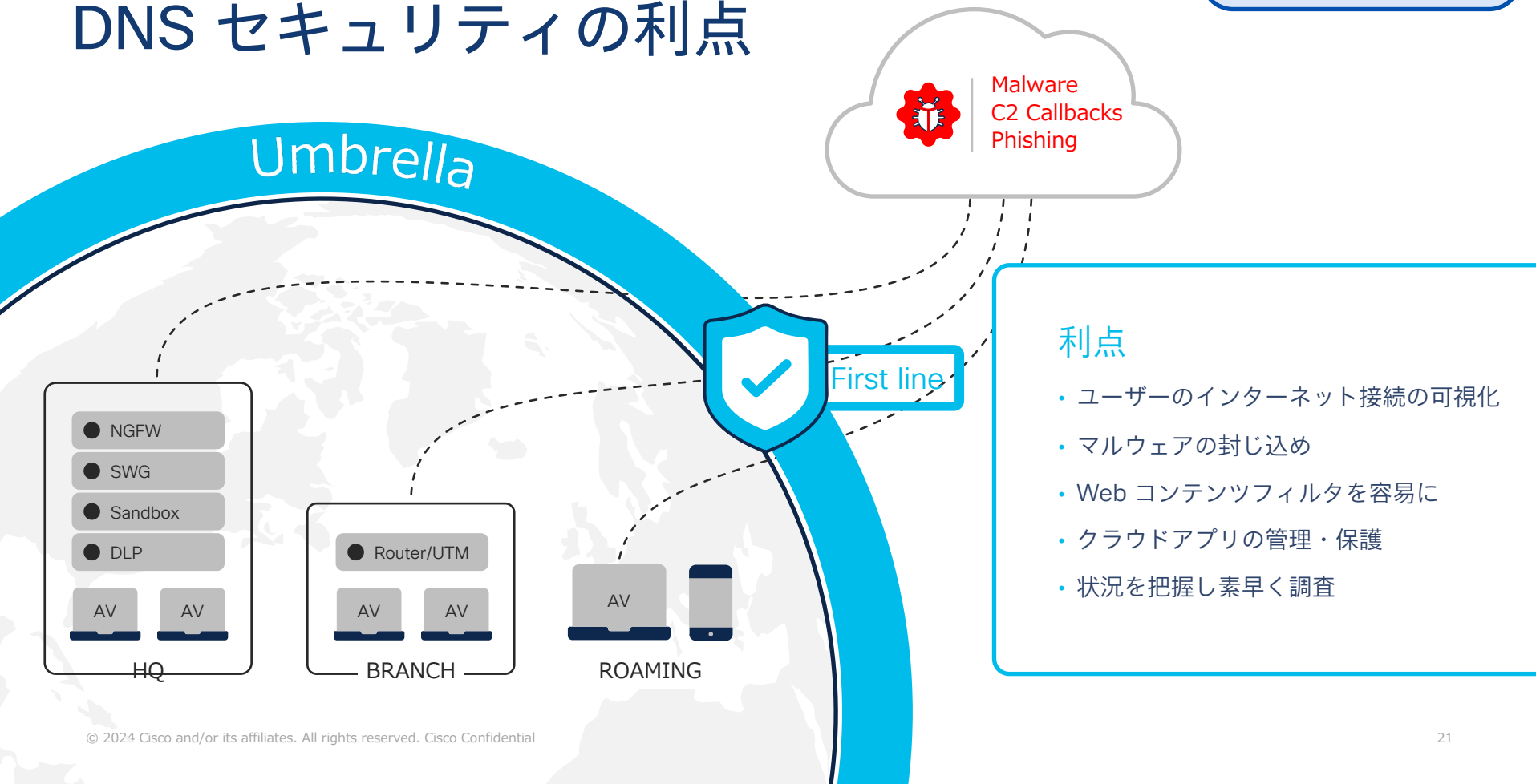
Cisco Umbrella の仕組み

- ✔ 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



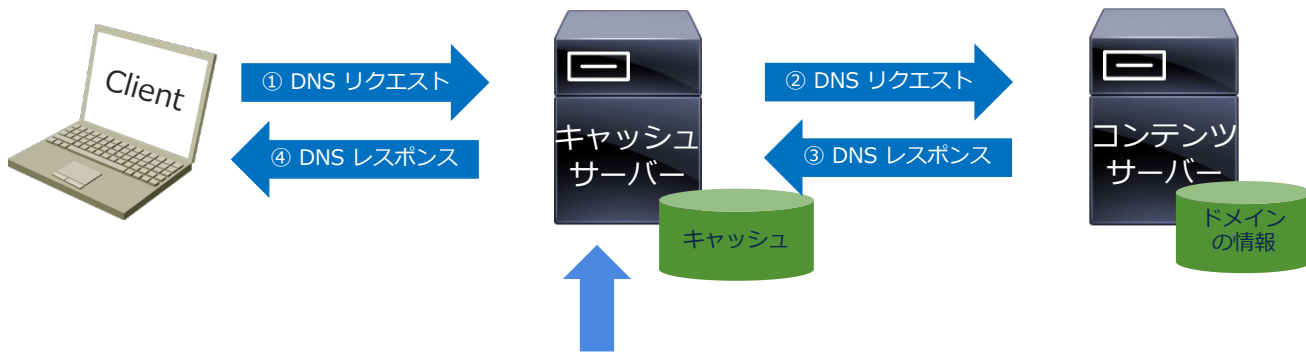
DNS セキュリティの利点



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

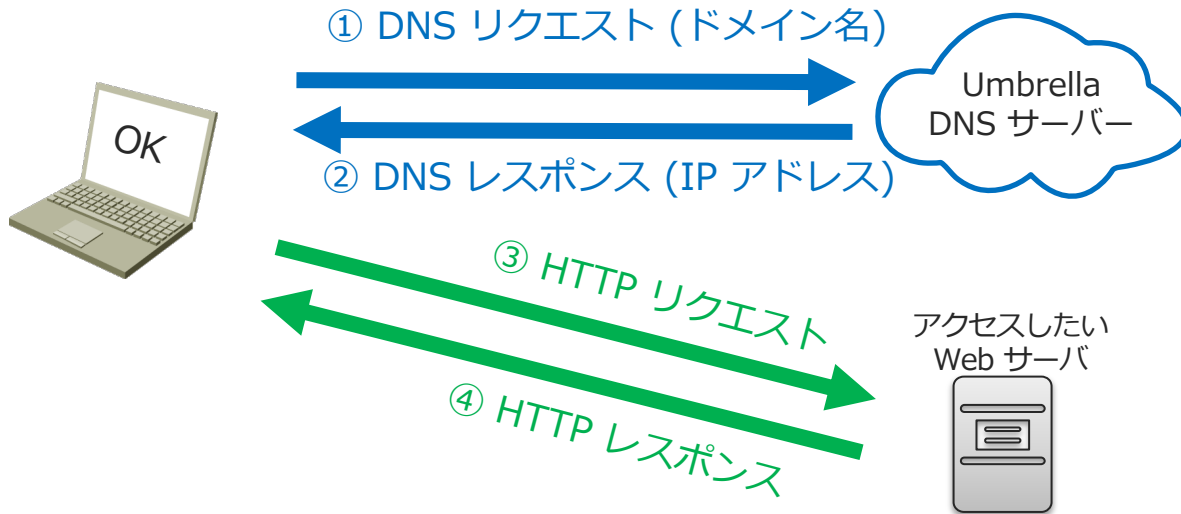
- 自身が管理しているドメインの情報を返す
DNS コンテンツ サーバー (別名: 権威 DNS サーバー)
- クライアントからの DNS リクエストの代理を行う
DNS キャッシュ サーバー (別名: フル サービス リゾルバ)



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

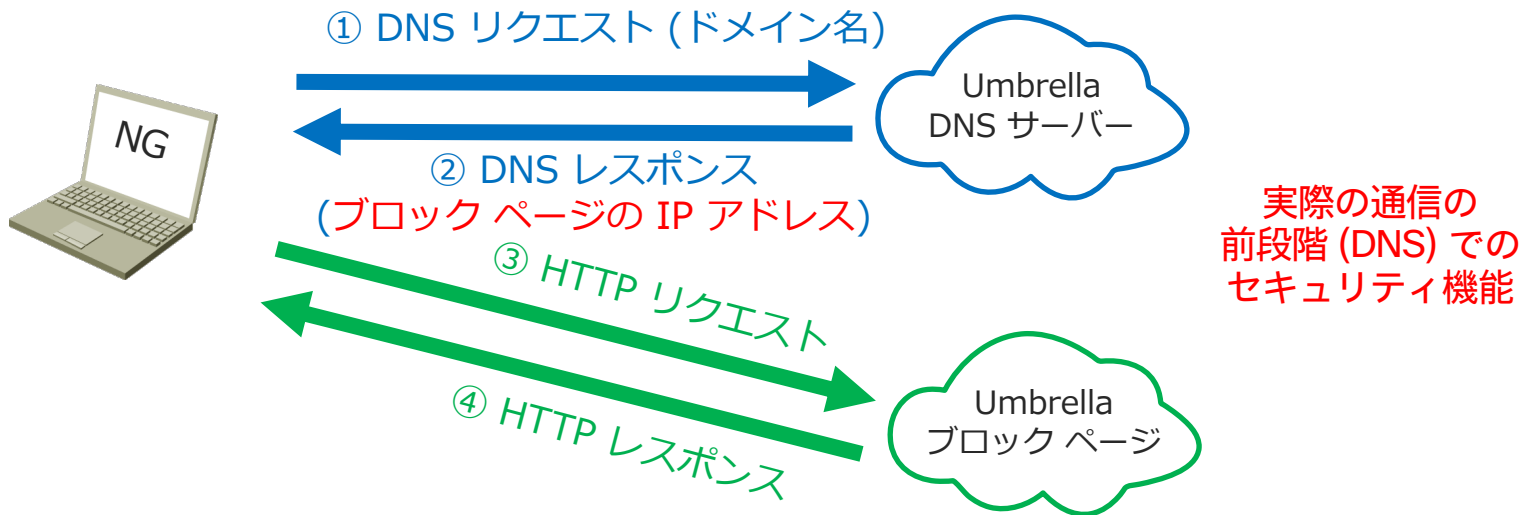
Web アクセス時の Umbrella の DNS サーバー

DNS の通信は Web アクセス (HTTP) の通信に先立つ

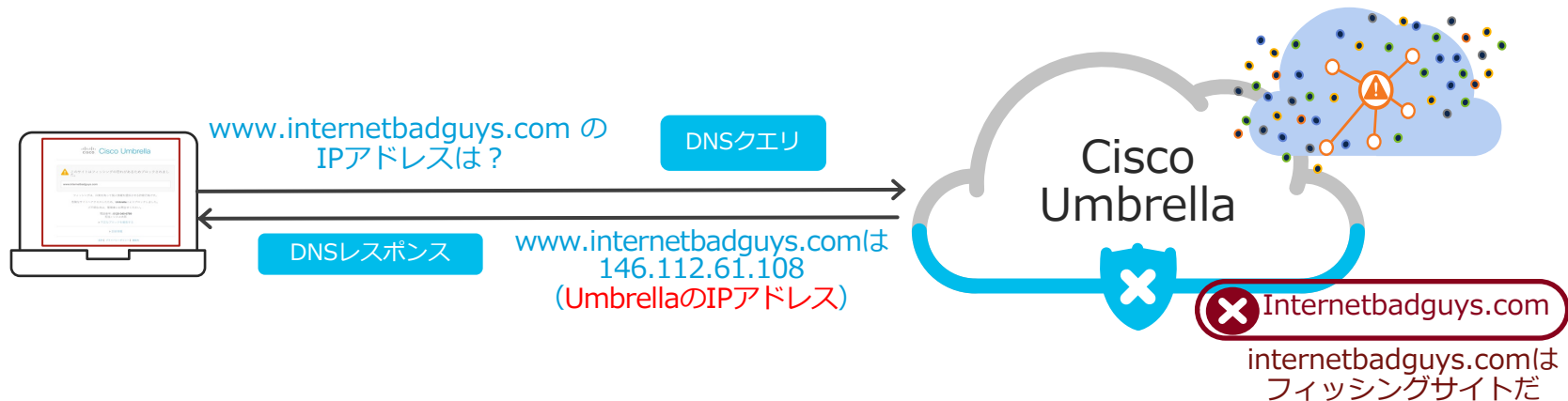
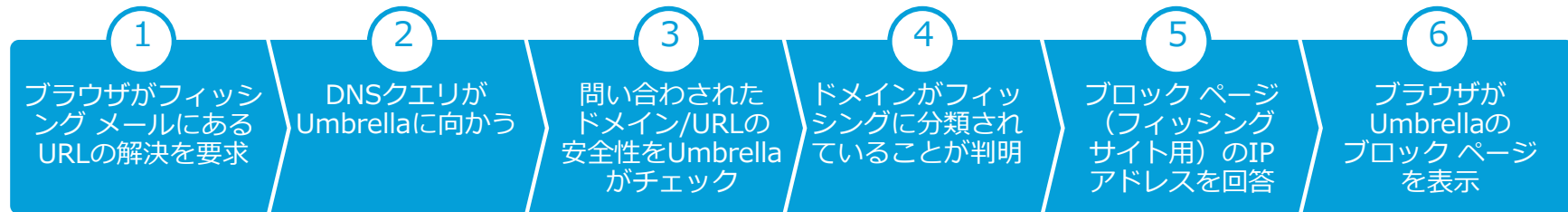


Web アクセス時の Umbrella の DNS サーバー

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



Secure DNS によるブロックの例



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

CISCO Cisco Umbrella

 このサイトはフィッシングの恐れがあるためブロックされました。

www.internetbadguys.com

フィッシングは、口実を偽って個人情報を提供させる詐欺行為です。

www.internetbadguys.com はネットワーク管理者によってブロックされました。

[> 診断情報](#)

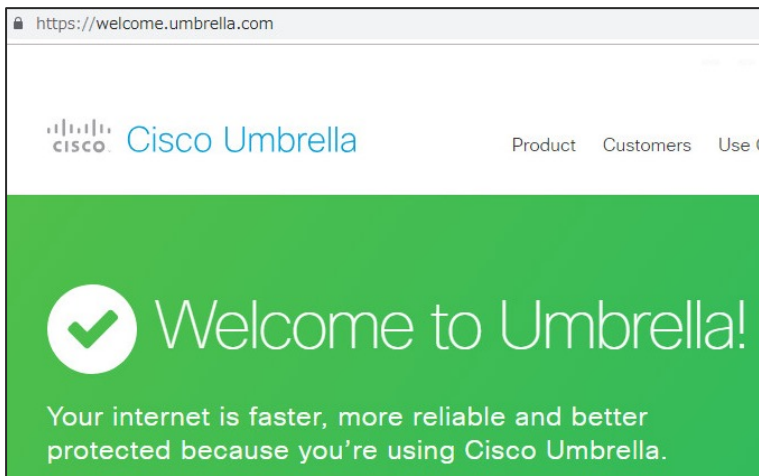
条件 | [プライバシーポリシー](#) | [連絡先](#)

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

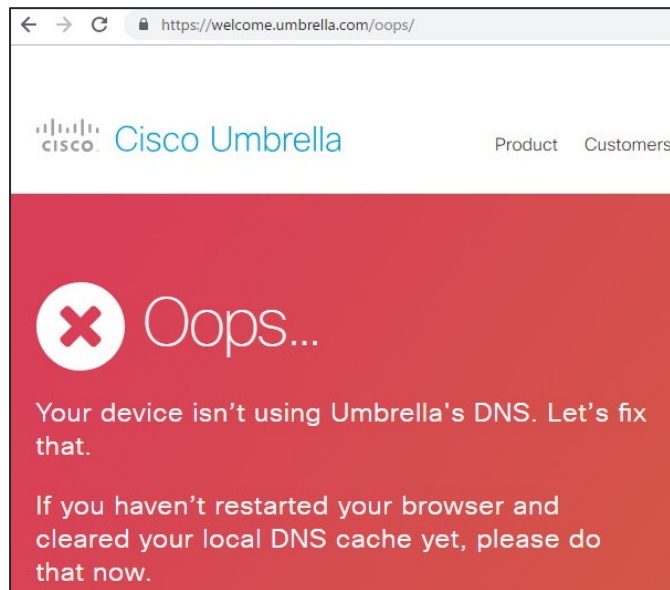
Web ブラウザによる到達性の確認

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 Policy Tester

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

Policies / Management
DNS Policies

Add Policy Tester

Policy Tester

Test whether a destination will be allowed or blocked for an identity. If you receive results you don't expect or want, reorder or refine your policies and run the test again. [For more information, see Test a Policy.](#)

Identities

Ex: Roaming Computer, Network Devices, User, Site, Network, AD Group (max 1 of each)

PHELI-M-39...

Destination

Note: Currently URLs are not supported

www.google.com

RESET RUN TEST

Result:

● Destination was allowed

Triggered Identity: PHELI-M-393C
Destination: www.google.com
CNAMEs: forcesafesearch.google.com
Result: Destination was allowed
Categorization: Search Engines, Search Engines and Portals
SafeSearch enforced
Policy Applied: Default Policy

Only 1 policy was applied to this identity. This was your default policy, Default Policy.

Note: Your actual results may differ from what's shown above if you have the Intelligent Proxy enabled, as URLs could be treated differently.

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

トラブルシューティングやどのDNSポリシーを構築する際に使用できる

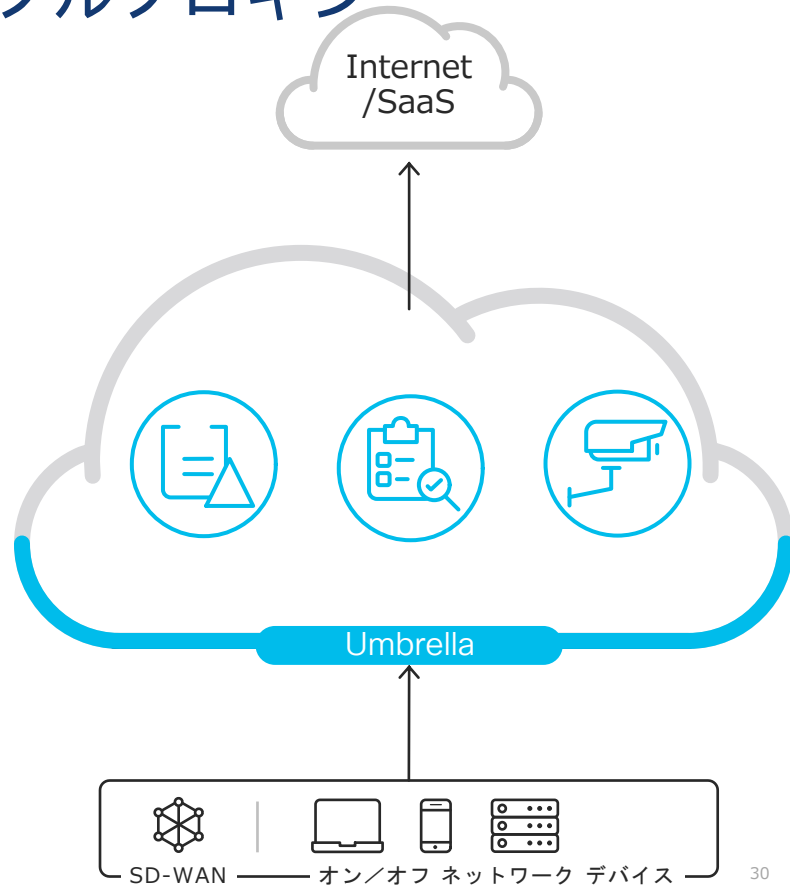


Umbrella機能紹介

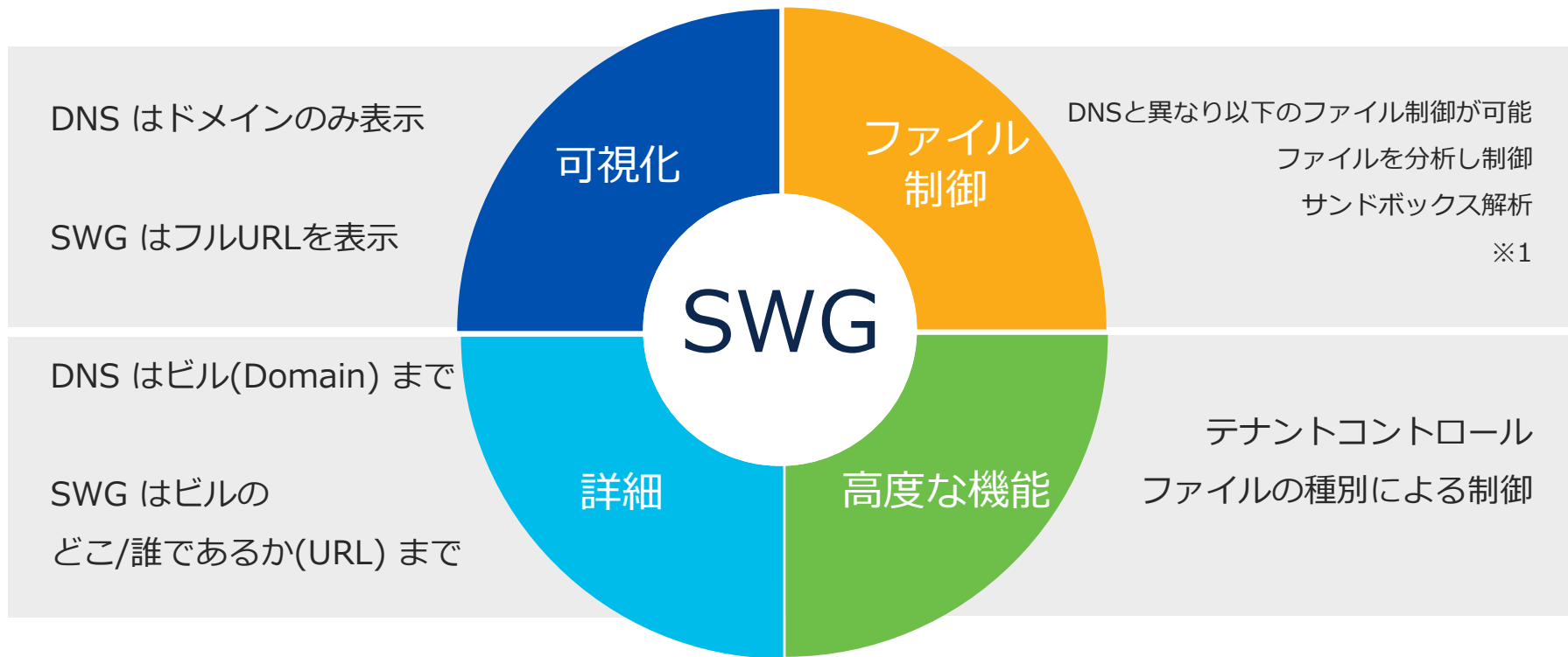
3.2. Web ポリシー

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



なぜ SWG を利用した Web Proxy が必要?



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

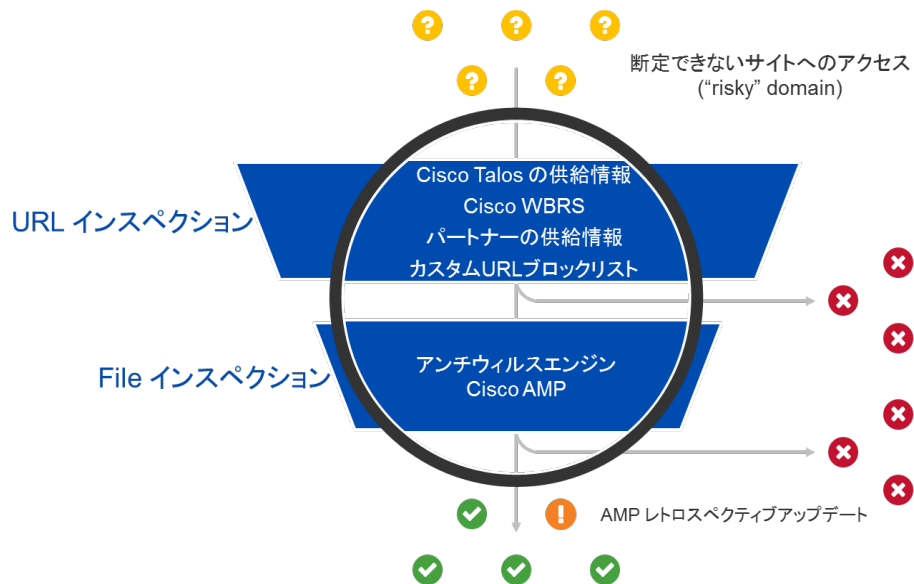
File Inspection ファイルがダウンロードされる前にスキャン、悪意のあるコンテンツが含まれていないか確認

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

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、アンチウイルスと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

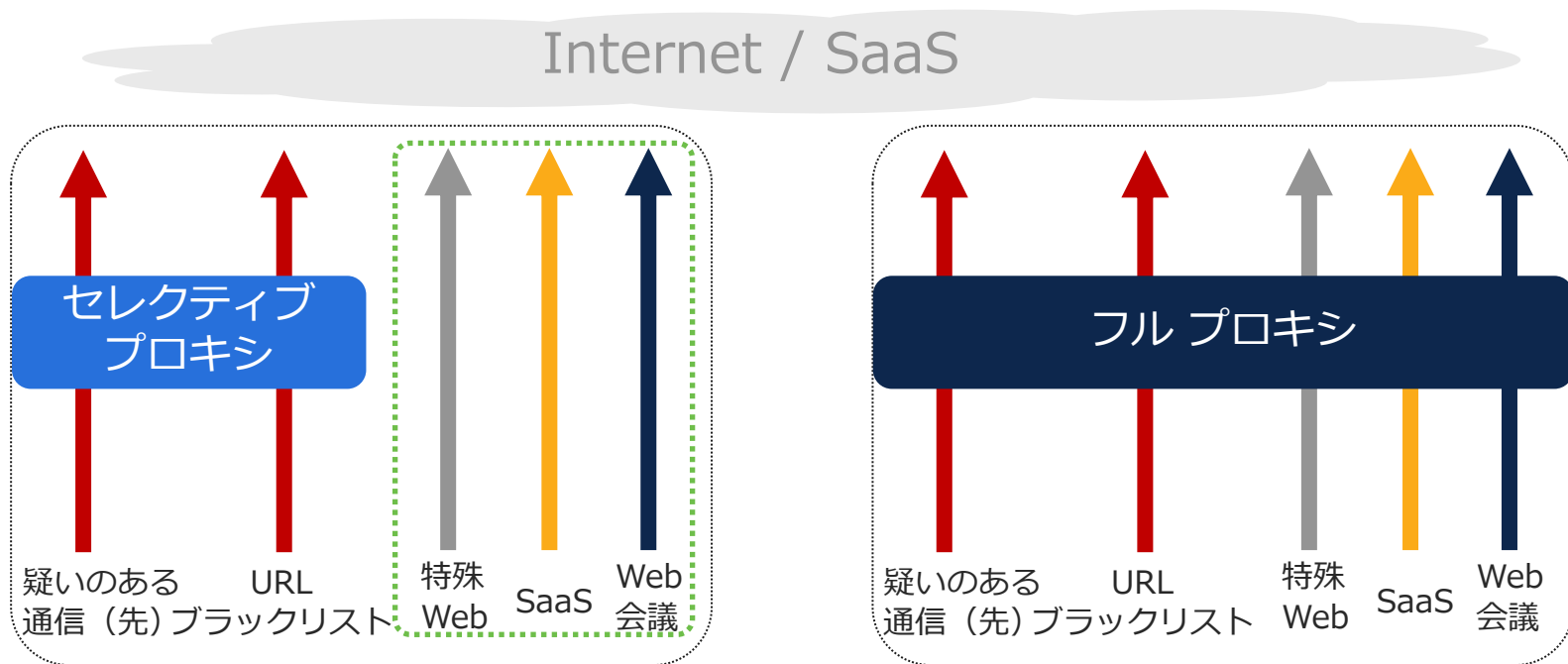
事後対策として

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

セレクト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

セレクトティブ プロキシのメリット

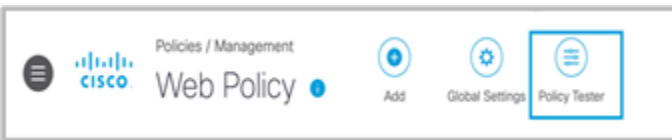
- ・ DNS ポリシーで動作
- ・ クラウド利用パフォーマンス
- ・ IoT 機器に対するセキュリティ
- ・ SaaS との相性
- ・ コラボレーション ツールとの相性

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トティブ 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



Web Policy Tester

To test that the Web policy's rulesets and rules function as intended, test an identity's access to a destination. Test that rulesets and rules block, allow, isolate, or warn as intended. For more information, see Umbrella's [Help](#).

Primary Identity
Tests both a ruleset and rule identities' destination access.

TUNNELS | Tunnel B X

Secondary Identity (optional)
Tests a rule identity's destination access only.

AD USERS | Corporal Ferro (cferro@jdcorp.com) X

Destination
Destination that identities will attempt to access.

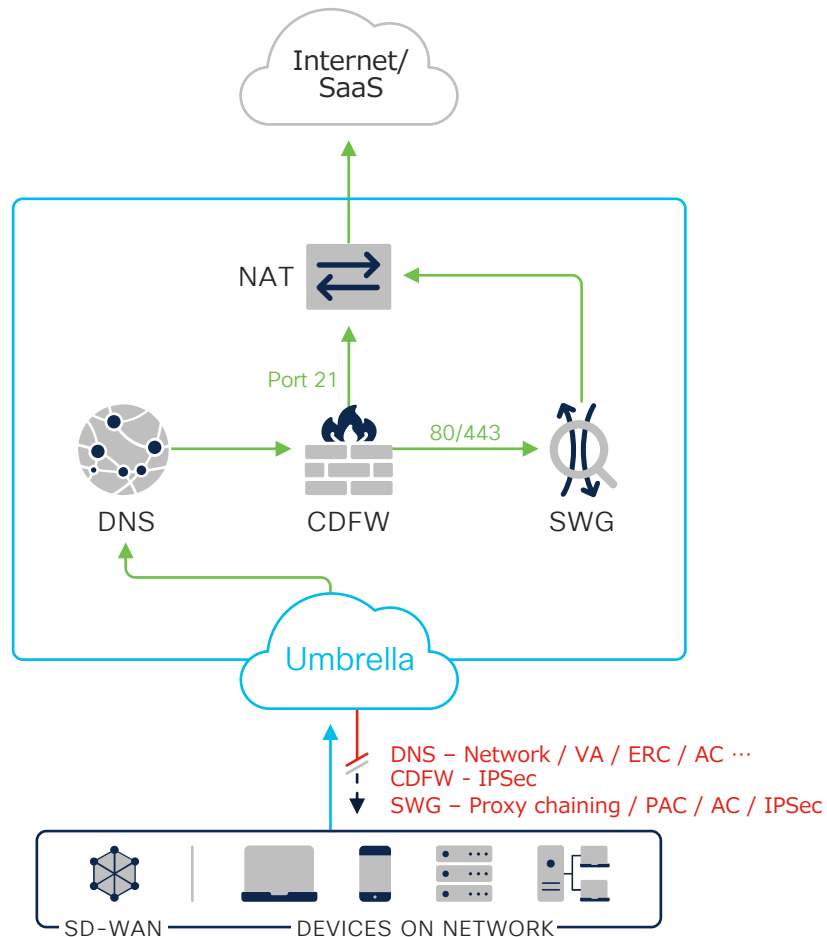
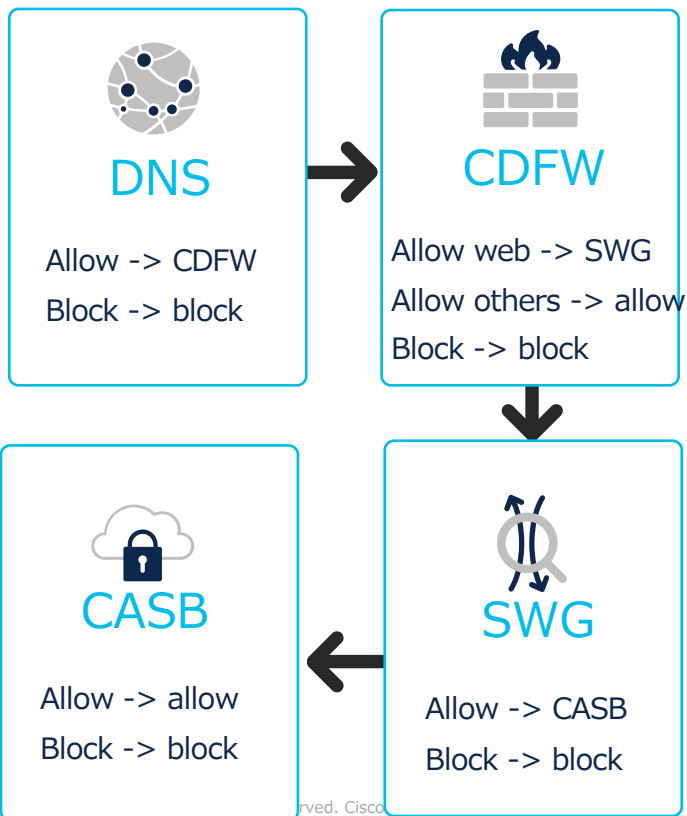
- Blocked

Identity:	AD Users
Ruleset:	Default Web Policy
Rule:	Global Block
Content Categories:	Movies, Television, Music, Anime/Manga/Webcomic
Schedule:	Not Applied

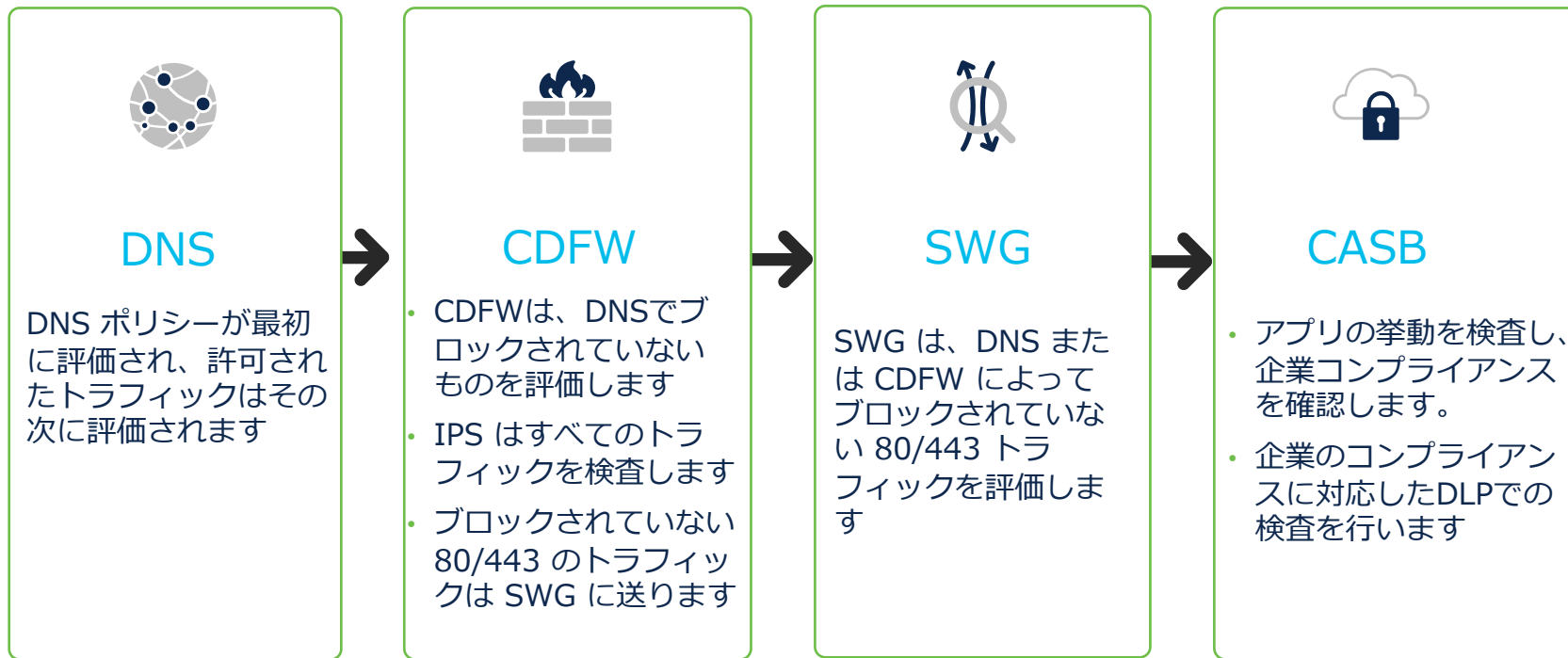
特定の IP や宛先のトラフィックに対して、どのルールセットやルールが適用されるかを理解するのに役立つ

トラブルシューティングや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





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。

【設定】を選択します

デフォルトの設定 ▼

ブロックするカテゴリ

- マルウェア
悪意のあるソフトウェア、ドライブバイダウンロード/エクスプロイト、モバイル脅威をホストしているWeb サイトと他のサーバ。
- 新しく発見されたドメイン
ごく最近アクティブになったドメイン。これらは新手法の攻撃で頻繁に使用されます。
- コマンド&コントロールのコールバック
侵害されたデバイスと攻撃者のインフラストラクチャとの通信を防止します。
- フィッシング攻撃
ユーザをだまして個人情報や金融情報を送信させることを目的とする不正なWebサイト。
- ダイナミックDNS
ダイナミックDNSコンテンツをホストしているサイトをブロックします。
- 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、攻撃の一端を担う可能性のあるドメイン。
- DNS トンネリング VPN
ユーザが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。これらは、アクセスとデータ転送に関する企業のポリシーを回避するために使用される場合があります。
- クリプトマイニング
クリプトマイニングにより、組織は、マイニングプールとWebマイナーへのクリプトマイナーのアクセスを制御できます。

キャンセル 保存

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）

Add New Content Setting

Setting Name
New Category Setting

This content list is applied to:
Web Policies

Copy From Existing
None

Categories [SELECT ALL](#)

<input type="checkbox"/> Academic Fraud	<input type="checkbox"/> Mobile Phones
<input type="checkbox"/> Adult	<input type="checkbox"/> Nature
<input type="checkbox"/> Advertisements	<input type="checkbox"/> News / Media
<input type="checkbox"/> Alcohol	<input type="checkbox"/> Non-Profits
<input type="checkbox"/> Arts	<input type="checkbox"/> Nudity
<input type="checkbox"/> Astrology	<input type="checkbox"/> Online Communities
<input type="checkbox"/> Auctions	<input type="checkbox"/> Online Meetings
<input type="checkbox"/> Automotive	<input type="checkbox"/> Online Trading



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

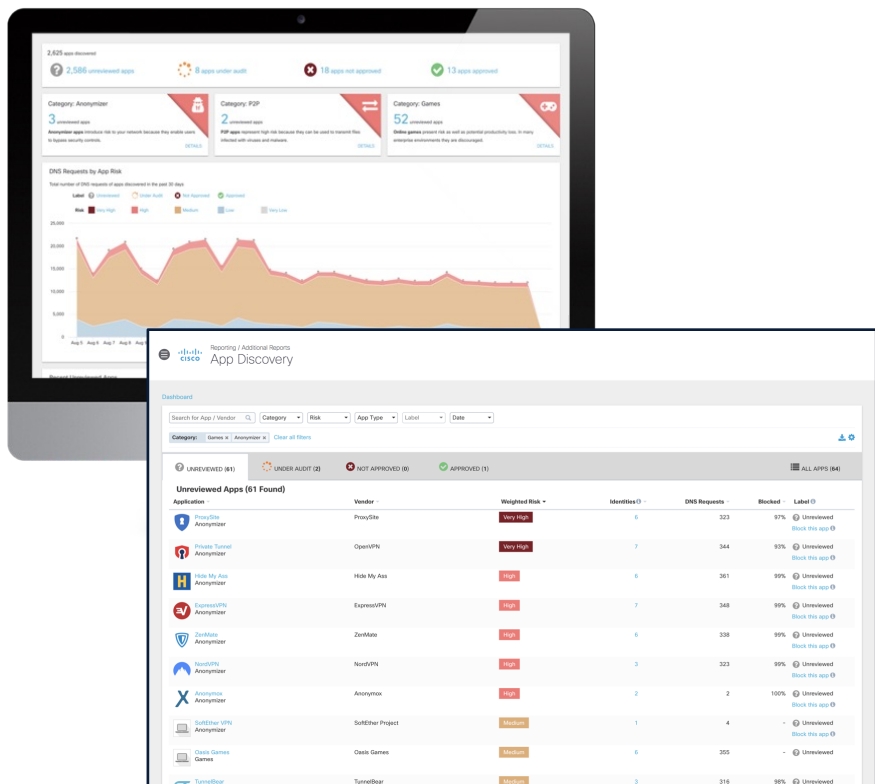


Umbrella の運用について

6. アプリケーション可視化

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

6. アプリケーション可視化

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。

Cisco Umbrella

報告/コアレポート

アプリの検出

管理者によるアプリケーションのラベル評価一覧

831個のアプリケーションが見つかりました

- 816 未確認のアプリケーションです
- 1 アプリケーションは監査中です
- 5 アプリケーションは承認されていません
- 9 アプリケーションは承認されています

フラグが設定されているカテゴリ

Generative AI

1 未確認のアプリケーションです

Generative AI apps have the potential for generating misleading or fraudulent content and copyright or intellectual property infringements.

詳細

P2P

1 未確認のアプリケーションです

P2Pアプリケーションは、それによって、ウイルスやマルウェアに感染したファイルが送信される可能性があるため、高いリスクになります。

詳細

ゲーム

3 未確認のアプリケーションです

オンラインゲームは、生産性を失う可能性があるだけでなく、リスクにもなります。多くの企業の環境では、これらのアプリケーションの使用は推奨されません。

詳細

Get Started

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。

Reporting / Core Reports
App Discovery

Download CSV

Back Label

Filter

- Unreviewed (816)
- Approved (9)
- Not Approved (5)
- Under Audit (1)

Filter

Label

- Unreviewed (816)
- Approved (9)
- Not Approved (5)
- Under Audit (1)

Controllable Apps

- All Controllable Apps
- Advanced Controls

Risk

- Very High
- High
- Medium
- Low
- Very Low

Select All

Select All

Select All

発見されたアプリ

リスク

DNS リクエスト数

Web 通信量

Application	Weighted Risk	Identities	DNS Requests	Total Web Traffic	Firew	Label	
Ubuntu Compute	Medium	3	6,885	5.0 GB total traffic 5.0 GB	--	Unreviewed	Control this app
Slack Collaboration	Medium	7	9,328	862.6 MB total traffic 860.3 ... 2.3 MB		Unreviewed	Control this app
Adobe Creative Cloud Office Productivity	Low	6	20,083	340.1 MB total traffic 340.1 ... 25.7 KB		Unreviewed	Control this app
				311.6 MB total traffic			

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。

Application

Duo Security
Allows Access Security for Everyone, from Any Device, Anywhere

Risk Score
Low

Control this app Approved

Details

App URL https://duo.com/product	Identities 8	Traffic Total: 13.9 MB Blocked: --	First Detected (UTC) Aug 8, 2023
Category Security	Vendor Cisco	DNS Requests Total: 2,909 Blocked: 3%	Last Detected (UTC) Nov 5, 2023
		Firewall Events Total: -- Blocked: --	

Risk Details | Identities (8) | Attributes (13)

How We Calculate Risk (Help us improve)
App Discovery's Composite Risk Score (CRS) for cloud services combines 3 elements to calculate a standardized measure of the risk for a cloud service: Business Risk, Usage Risk and Vendor Compliance.

Business Risk
Medium

Usage Risk
Low

Risk Calculation Factors:
Business Risk: Typical use of the service (personal or organizational), The Talos Security Intelligence Web Reputation score for the service, Financial viability of the app vendor, Type of data stored by the app.
Usage Risk: Volume; how much data flows to and from the service, Users; how many of your users depend on or use the service.

リスクの計算は以下3要素より総合的に実施
Business Risk / Usage Risk / Vendor Compliance

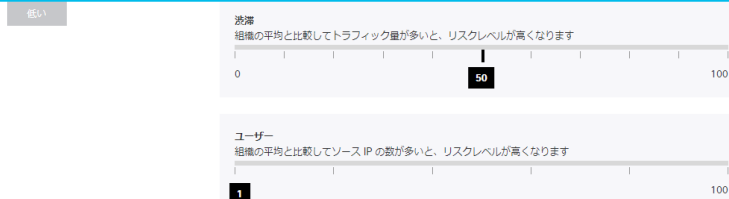
6. アプリケーション可視化

アプリケーション検出 詳細画面 (2/2)

トラフィック量や送信元IPの数を基に評価

ウェブプレデケーションや財務状況等を基に評価

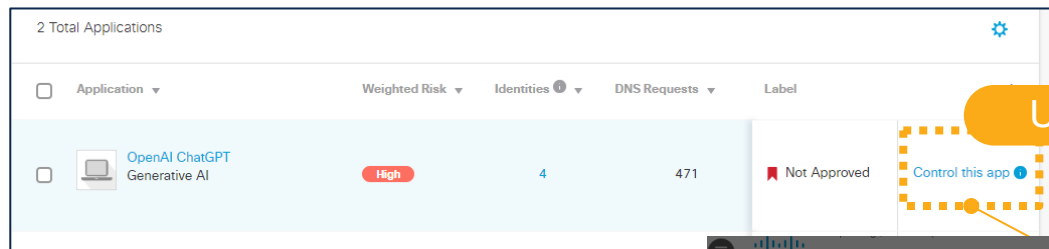
App Discovery のクラウド サービスの複合リスクスコア (CRS) は、ビジネス リスク、使用リスク、ベンダー コンプライアンスの 3 つの要素を組み合わせて、クラウド サービスのリスクの標準化された尺度を計算します。



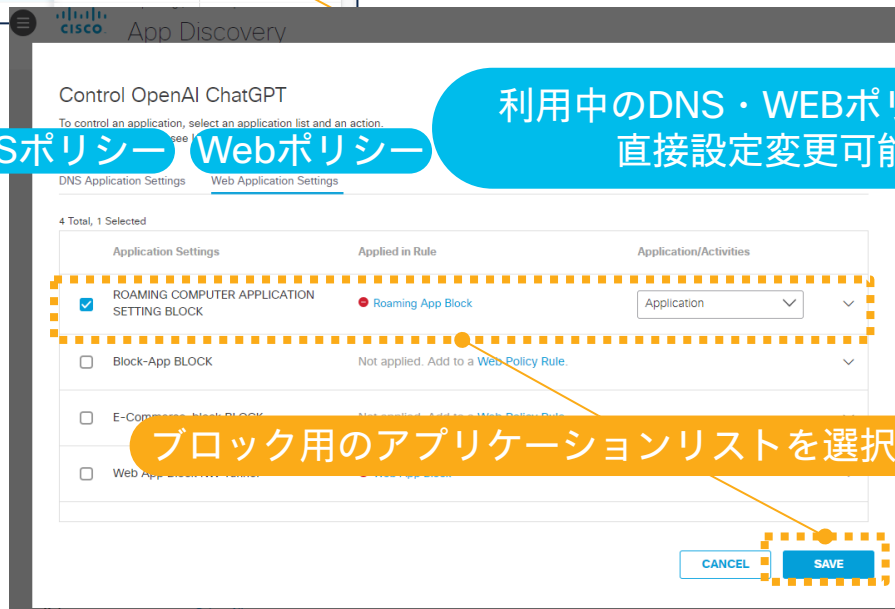
クラウドアプリケーションベンダーの
各種業界標準コンプライアンス対応を基に評価

準拠していない、または見つからない	ビット	NIST Special Publication 800-53 は Special Publication 800 シリーズの一部であり、情報技術研究所 (ITL) の情報システム セキュリティにおける研究、ガイドライン、実証活動、および産業界、政府機関、学術団体との ITL の活動について報告しています。
準拠していない、または見つからない	コビット	COBIT は、情報および関連技術の制御目標の略です。これは、ISACA (Information Systems Audit and Control Association) によって作成された IT ガバナンスと管理のフレームワークです。
✓ 認証済み	フェドランプ	連邦リスクおよび認可管理プログラム (FedRAMP) は、クラウド製品とサービスのセキュリティ評価、認可、継続的監視に対する標準化されたアプローチを提供する政府全体のプログラムです。
準拠していない、または見つからない	ギャップ	一般に認められたプライバシー原則 (GAPP) は、公認会計士および公認会計士がプライバシー リスクを管理および防止するための効果的なプライバシープログラムを作成することを支援することを目的としたフレームワークです。
✓ 認証済み	ヒバア	HIPAA (1996 年医療保険の相互運用性と責任に関する法律) は、医療情報を保護するためのデータ プライバシーとセキュリティ規定を規定する米国の法律です。
✓ 認証済み	ISO27001/27002	ISO 27001 は、情報セキュリティ管理システム (ISMS) の仕様です。ISMS は、組織の情報リスク管理プロセスに關わるすべての法的、物理的、技術的管理を含むポリシーと手順のフレームワークです。
✓ 認証済み	PCI_DSS	Payment Card Industry Data Security Standard (PCI DSS) は、クレジットカード、デビット、キャッシュ カード取引のセキュリティを最適化し、個人情報の悪用からカード所有者を保護することを目的とした、広く受け入れられている一連のポリシーと手順です。
✓ 認証済み	SOC2	SOC2
✓ 認証済み	SP800_53	連邦情報システムおよび組織のセキュリティとプライバシーの管理、米国立標準技術研究所 (NIST)

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



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

The screenshot shows the Cisco Umbrella management interface. On the left is a navigation menu with 'Web ポリシー' highlighted. The main area is titled 'ルールセットルール' and contains a table of rules. A rule named 'Roaming App Bl...' is selected, showing an action of 'ブロック' (Block). A callout box points to the 'Web ポリシー' menu item, and another callout points to the rule's configuration area.

優先	ルール名	ルールアクション	アイデンティティ	送信先	ルール構成
	Roaming App Bl...	ブロック	ルールセット アイデンティティ アイデンティティを追加する	適用されたアプリケーションリスト... 宛先を追加	任意の日、いつでも 変更スケジュール 追加の設定は適用されません 保護されたファイルのバイパスが無効 編集

“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

報告/コアレポート
Cisco アクティビティ検索

フィルタ リクエストアクティビティの検索 詳細 クリア

アイデンティティタイプ ローミングコンピュータ

検索フィルタ 合計1,246 4月9, 2024 6:51 午後から4月10, 2024 6:51 午後後のアクティビティの表示

レスポンス すべてを選択
 許可 [詳細](#)
 ブロック済み
 選択的にブロックされました

ページの動作の警告 すべてを選択
 警告済み
 警告後にアクセス

分離
 Isolated

IPスニグニャ すべてを選択
 ログインのみ
 ブロックする
 ブロック済み

プロトコル すべてを選択
 HTTP
 HTTPS

要求	アイデンティティ	ポリシーまたはルールセットのアイデンティティ	優先
WEB	サクセちゃんのMacBook Pro	サクセちゃんのMacBook Pro	https://ocsp2.apple.com
WEB	サクセちゃんのMacBook Pro	サクセちゃんのMacBook Pro	https://ocsp2.apple.com
WEB	サクセちゃんのMacBook Pro	サクセちゃんのMacBook Pro	https://global.telemetry.insights.video.a2z.com/E
WEB	サクセちゃんのMacBook Pro	サクセちゃんのMacBook Pro	https://global.telemetry.insights.video.a2z.com/E
DNS	サクセちゃんのMacBook Pro	サクセちゃんのMacBook Pro	global.telemetry.insights.video.a2z.com
WEB	サクセちゃんのMacBook Pro	サクセちゃんのMacBook Pro	https://fts-fe.amazon.co.jp/1/batch/1/OE/
DNS	サクセちゃんのMacBook Pro	サクセちゃんのMacBook Pro	40-courier.push.apple.com
DNS	サクセちゃんのMacBook Pro	サクセちゃんのMacBook Pro	1-courier.push.apple.com
DNS	サクセちゃんのMacBook Pro	サクセちゃんのMacBook Pro	www.apple.com
DNS	サクセちゃんのMacBook Pro	サクセちゃんのMacBook Pro	apple.com
DNS	サクセちゃんのMacBook Pro	サクセちゃんのMacBook Pro	gs.apple.com
DNS	サクセちゃんのMacBook Pro	サクセちゃんのMacBook Pro	gateway.fe2.apple-dns.net
DNS	サクセちゃんのMacBook Pro	サクセちゃんのMacBook Pro	1-courier.sandbox.push.apple.com
DNS	サクセちゃんのMacBook Pro	サクセちゃんのMacBook Pro	apl.apple-cloudkit.com

- ✓ 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

7. Activity Search

Activity Search 画面詳細

合計7,233 4月 4, 2024 12:00 午前から4月 10, 2024 7:58 午後のアクティビティの表示 ページ: 1 各ペ

アイデンティティ	ポリシーまたはルールセットのアイデンティティ	宛先	宛先IP	内部IP
VPN-Home	VPN-Home	https://www.youtube.com	172.217.31.142	192.168.1.100
VPN-Home	VPN-Home	https://www.youtube.com	142.250.196.142	192.168.1.100
VPN-Home	VPN-Home	https://www.youtube.com	172.217.31.174	192.168.1.100
VPN-Home	VPN-Home	https://www.youtube.com	142.251.42.206	192.168.1.100
VPN-Home	VPN-Home	https://www.youtube.com	142.250.196.110	192.168.1.100
VPN-Home	VPN-Home	https://www.youtube.com	142.251.222.46	192.168.1.100
サクセスちゃんのMacBook Pro	サクセスちゃんのMacBook Pro	https://www.youtube.com/embed/	172.217.175.46	192.168.1.100
サクセスちゃんのMacBook Pro	サクセスちゃんのMacBook Pro	https://www.youtube.com/iframe_api	完全な詳細を表示	...
サクセスちゃんのMacBook Pro	VPN-Home	https://www.youtube.com	フィルタ基準 www.youtube.com	...
サクセスちゃんのMacBook Pro	VPN-Home	https://www.youtube.com	URLによるフィルタ	...
サクセスちゃんのMacBook Pro	サクセスちゃんのMacBook Pro	https://www.youtube.com/ytubei/v1/	フィルタ基準 サクセスちゃんのMacBook Pro	...

宛先IP

「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

イベントの詳細

アクション

許可

時間

4月 9, 2024 10:53 午前

ルールセットまたはルール

Demo-WP-SecureCl

アイデンティティ

サクセスちゃんのMacBook Pro

ポリシーまたはルールセットのアイデンティティ

サクセスちゃんのMacBook Pro

内部IPアドレス

192.168.1.6

外部IPアドレス

宛先

https://www.youtube.com/iframe_api

ホスト名

www.youtube.com

カテゴリ

映画 (レガシー), エンターテインメント (レガシー), ビデオ共有 (レガシー), ビデオ ストリーミング

分類に同意しない

アプリケーション

YouTube

アプリケーションのカテゴリ

Media

発生時間

端末情報

HTTPヘッダ

コンテンツタイプ

text/javascript

ファイル名

iframe_api

ファイルアクション(リモートブラウザの分離)

-

総サイズ(バイト)

2807

Request Method

GET

Referer ヘッダー

https://www.google.com/

ステータスコード

200

ユーザーエージェント

Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36

SHA256ハッシュ

e4d5c28787419e7eaae569549d12df6ea9b1e7aa76e6f2a08b28ab812bfc1486

Umbrella出力IPアドレス

155.190.52.44

接続先が所属する
コンテンツカテゴリと
アプリケーションカテゴリ



Umbrella の運用について

8. レポート

8. レポート

レポート 機能概要

報告/管理
Cisco 定期レポート

スケジュール

レポート名、タイプ、頻度、または受信者による検索

名前	レポートタイプ	頻度	受信者	次の配信
Umbrella月次レポート				
Umbrella週次レポート				
Umbrella日次レポート				
Youtube監視-サクセスちゃんの				

新しいレポートのスケジュール設定

レポートに進んで、必要なフィルタを適用し、右上の[スケジュール]をクリックすることで、新しいレポートをスケジュールできます。

- セキュリティの概要の (エグゼクティブサマリー)
- セキュリティアクティビティ
- アクティビティ検索
- 総リクエスト件数
- アクティビティ ボリューム
- 上位ドメイン
- 上位カテゴリ
- 上位アイデンティティ

閉じる

- ✓ 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

8. レポート

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

概要

Settings スケジュール 過去24時間

2 Messages

Critical End of Life for Umbrella Roaming Client
6ヶ月 ago
Cisco has announced End of Life of the Umbrella Roaming client on April 2, 2024. Last Date of Support will be April customers begin planning and scheduling their migration to Cisco Secure Client now.
[VIEW DETAILS](#)

Warning The Umbrella SWG SAML certificate used for User Identity is due to expire on 27th of June 2024
16日 ago
This certificate will be renewed and made available from the 27th of May 2024 providing time from then until the 27 you to update your Identity provider (IdP) with the new Umbrella SAML certificate.
[VIEW DETAILS](#)

Malware: 0 requests blocked in the last 24 hours [View Trends](#) / [View Details](#)

Botnet: 0 requests blocked in the last 24 hours [View Trends](#) / [View Details](#)

Cryptomining: 0 requests blocked in the last 24 hours [View Trends](#) / [View Details](#)

レポートのスケジュール設定

次の情報に基づいて、レポートを定期的に電子メールで送信します。定期レポートのリストから、送信されるレポートを管理できます。

フィルタが適用されました

イベント
セキュリティブロック

アイデンティティ
すべてのアイデンティティ

キャンセル

続行

8. レポート

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

配信スケジュールの選択

次の情報に基づいて、レポートを定期的に電子メールで送信します。定期レポートのリストから、送信されるレポートを管理できます。

毎日

配信日時

9:00 午前

Asia/Tokyo (UTC 9: 00)

レポート範囲

直近の暦日

過去24時間

毎週

毎月

キャンセル

戻る

続行

レポートのタイトルと メールアドレスを指定

受信者の選択

次の情報に基づいて、レポートを定期的に電子メールで送信します。定期レポートのリストから、送信されるレポートを管理できます。

レポートのタイトル

新しい概要のスケジュール設定されたレポート

電子メール

複数の電子メールアドレスを、カンマまたはセミコロンで区切る

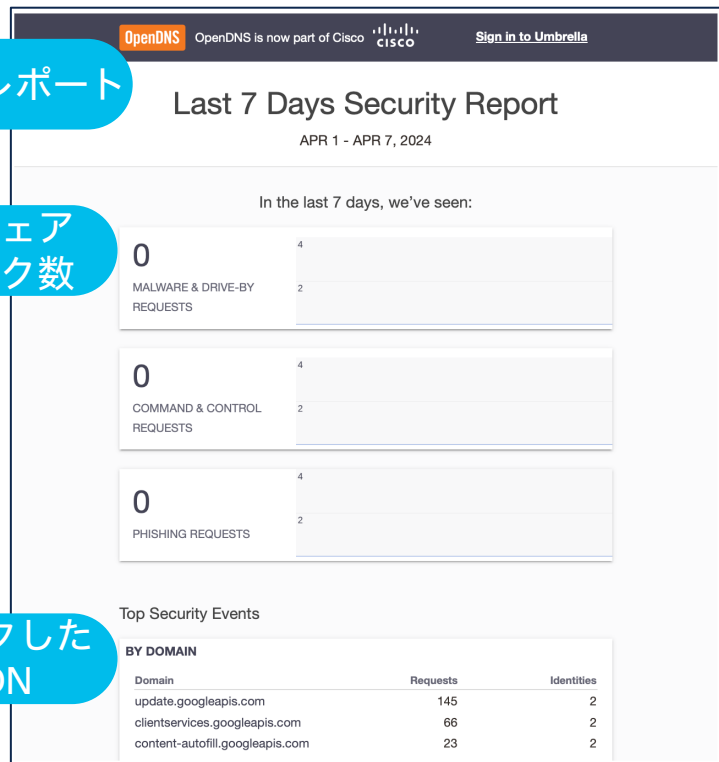
キャンセル

戻る

保存

8. レポート

レポート サンプルメール本文





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

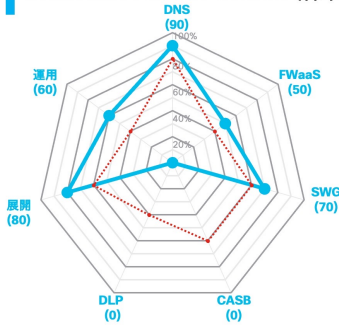
10. Q&A

Cisco Umbrella 健康診断サービス

Umbrella Health Check 結果報告サマリー

サンプル
レポート

左の図はお客様のご利用状況を各機能と展開/運用状況別にスコアを算出したグラフとなります。(水色線)



- DNS** 😊 ・ 今後アプリケーション制御やセーフサーチのご利用を推奨します
- FWaaS** 😊 ・ IPSIDSやアプリケーション制御のご利用を希望される場合、上位ライセンスへの移行やアドオン購入をご検討ください
- SWG** 😊 ・ 今後アプリケーション制御やセーフサーチのご利用を推奨します
- CASB** 😊 ・ シャドードキュメントやアプリケーション利用の適正化を目指して、検出されたアプリケーションに対する評価や制御の実施を推奨します
- DLP** 😊 ・ DLPはご利用のライセンスでは利用不可となっておりますが、ご利用を希望される場合、上位へのライセンス移行をアドオンをご検討ください
- 展開** 😊 ・ ログを保持期間 (30日) よりも長く保持したい、またSIEM製品と連携したい場合は、AWS S3機能をご利用ください
- 運用** 😊 ・ 発行されたレポートをもとにご通知されたマルウェアの検知やアプリケーションの制御を推奨します

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](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