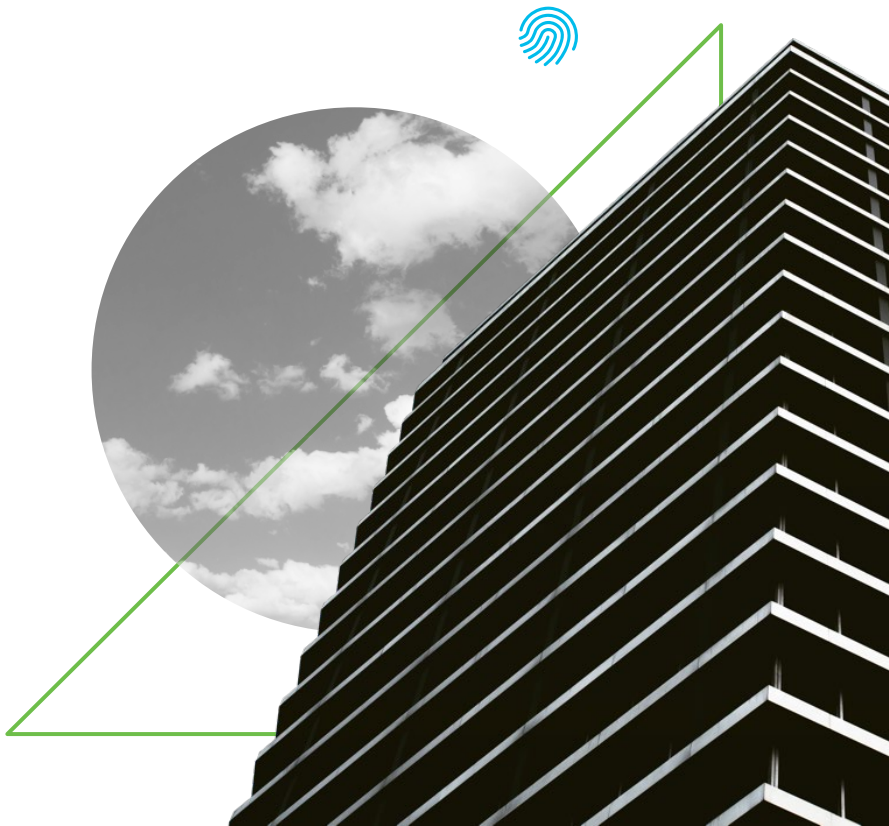
CISCO
SECUREざっくりシリーズ

The bridge to possible

ざっくりUmbrella DNS

Agenda

- ターゲットとゴール
- 前提知識
- Umbrella DNSが必要となる背景と課題
- Umbrella DNSの機能と課題の対応付け
- Umbrella DNSの強み
- 一般的なネットワーク構成図における
  Umbrella DNSの位置付け
- 代表的な機能
- 第三者評価、競合比較
- 事例
- まとめ



ターゲットとゴール

- 営業・SEの皆様がUmbrella DNSをお客様にご紹介頂くため、これを読めばUmbrella DNS が“ざっくり”分かる資料となります。
- Umbrella DNSを知るきっかけとしてご利用頂けますと幸いです。

前提知識

- 本資料で使用する用語の説明は以下の通りである

用語	概要
マルウェア	malicious（悪意のある）にsoftwareが組み合わさった言葉。昔からよく聞くコンピュータウイルスもマルウェアの1種である。PCやスマートフォンがマルウェアに感染すると重要なデータが破壊されたり、盗まれたりする恐れがある。
DNS	Domain Name Systemの略。ネットワーク上で通信を行っている機器にはそれぞれIPアドレスが割り当てられているが、その対応を覚えるのは困難である。したがって、cisco.comのように文字を用いてドメイン名を付ける。IPアドレスとドメイン名を対応させる仕組みがDNSである。
名前解決	本資料ではPCやスマートフォンを用いて、ある機器にドメイン名を指定して通信を行った際に、DNSサーバが対応するIPアドレスを返答することを指している。
Talos	セキュリティの脅威を研究したり、最新情報を発信したりするCiscoの中にあるチーム。Ciscoのセキュリティ製品はTalosの持つ情報と連携することで、保護性能を高める。
AnyConnect	PCやスマートフォン1台でVPN接続やUmbrellaとの接続を行うためのソフトウェア。

Umbrella DNSが必要となる背景と課題

マルウェア被害の拡大

危険なサイトにアクセスしてしまい
マルウェアに感染

社外にある端末の
セキュリティが無防備

リモートワークの増加

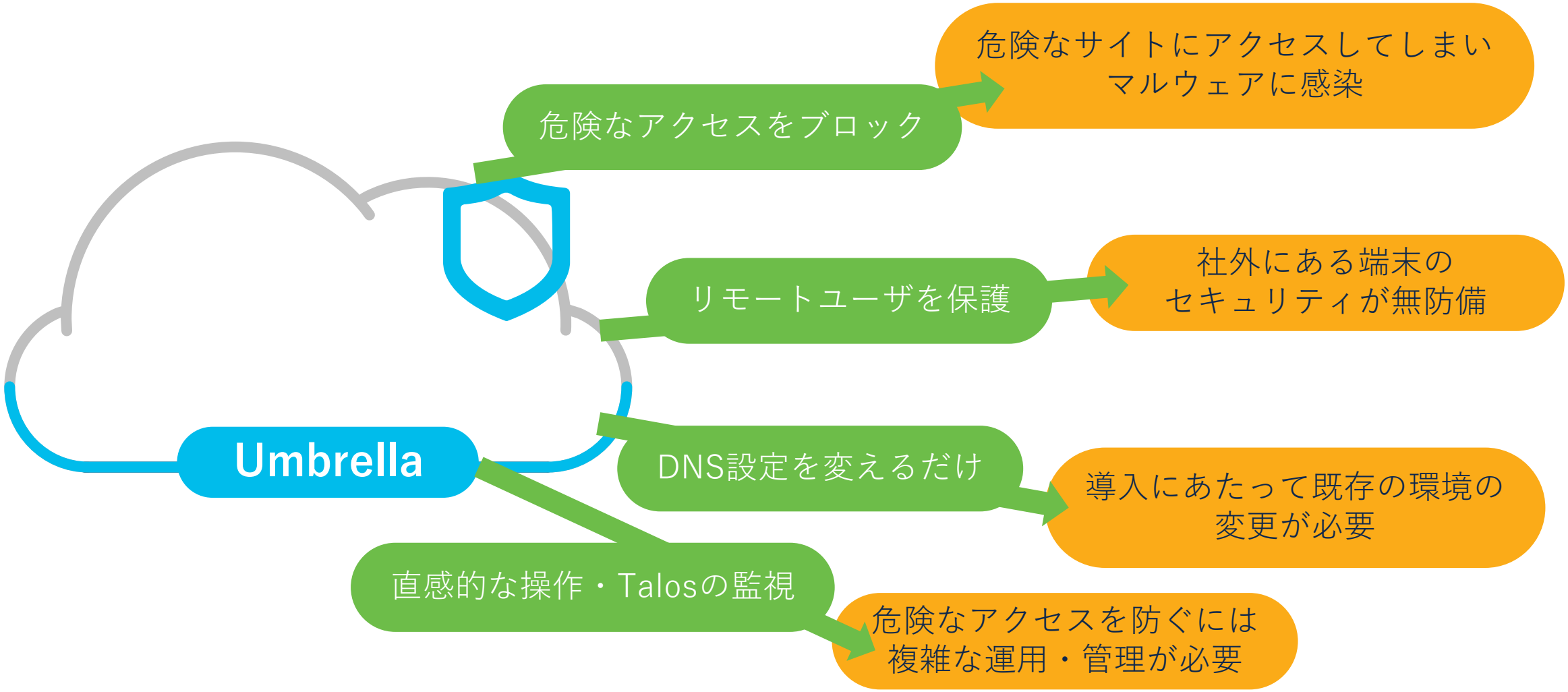
導入にあたって既存の環境の
変更が必要

暗号化されたweb通信の増加

危険なアクセスを防ぐには
複雑な運用・管理が必要

https://www.cisco.com/c/ja_jp/products/security/umbrella/index.html

Umbrella DNSの機能と課題の対応付け



https://www.cisco.com/c/ja_jp/products/security/umbrella/index.html

Umbrella DNSの強み

レスポンスの速いDNS

＋強固で柔軟なセキュリティ

いつでも

100%稼働

どこでも

社内/社外

どのアプリケーションでも

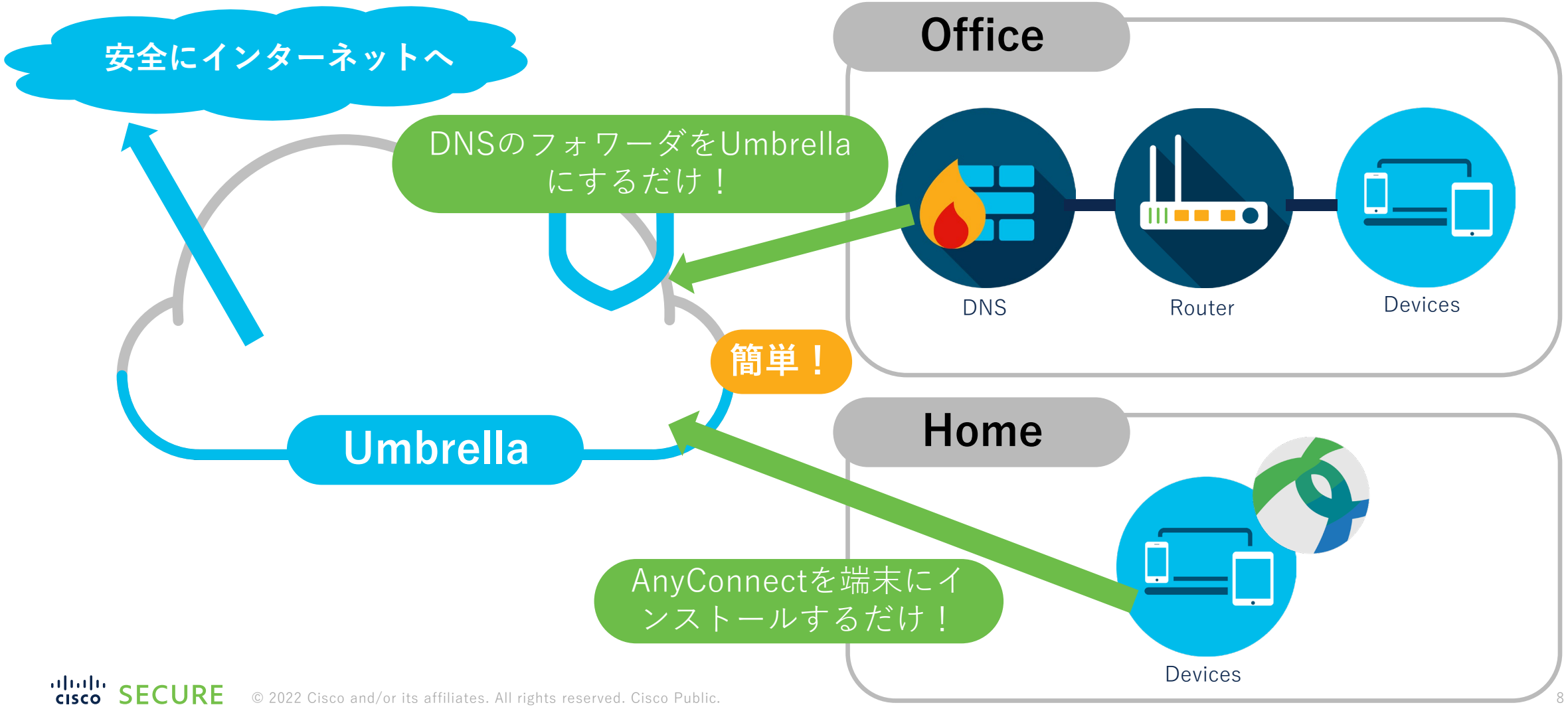
名前解決を行うなら

未知の脅威に対しても

Talosと連携して自動で

容易な
導入・運用

一般的なネットワーク構成図におけるUmbrella DNSの位置付け



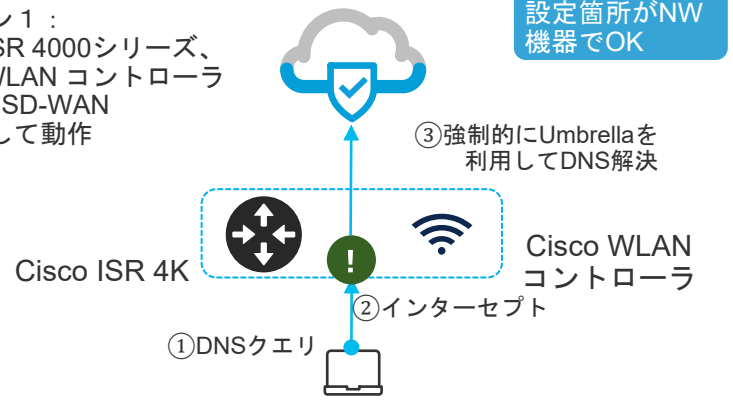
https://www.cisco.com/c/ja_jp/products/security/umbrella/index.html

DNSクエリをUmbrellaに向ける方法

4つの展開パターンが存在

パターン１：
Cisco ISR 4000シリーズ、
Cisco WLAN コントローラ
Meraki, SD-WAN
と連携して動作

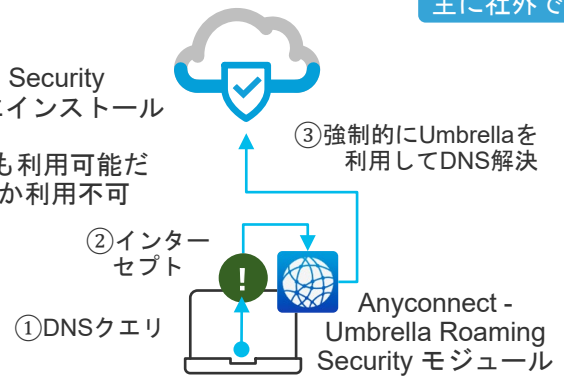
設定箇所がNW機器でOK



主に社外でのアクセス用途

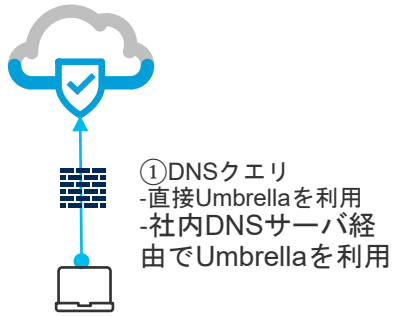
パターン２：
AnyConnect –
Umbrella Roaming Security
モジュールをPCにインストール

※Roaming Clientも利用可能だがDNSポリシーしか利用不可



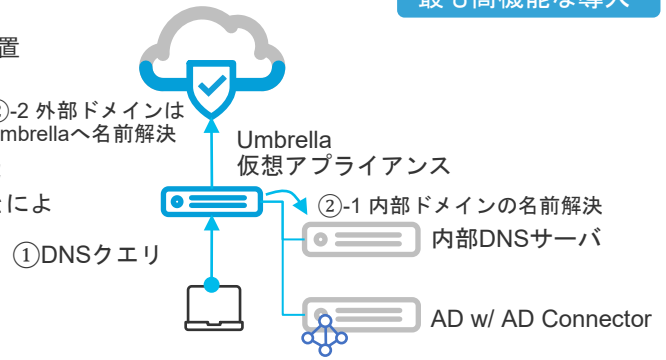
導入が最も簡単で一般的

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



最も高機能な導入

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



代表的な機能

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

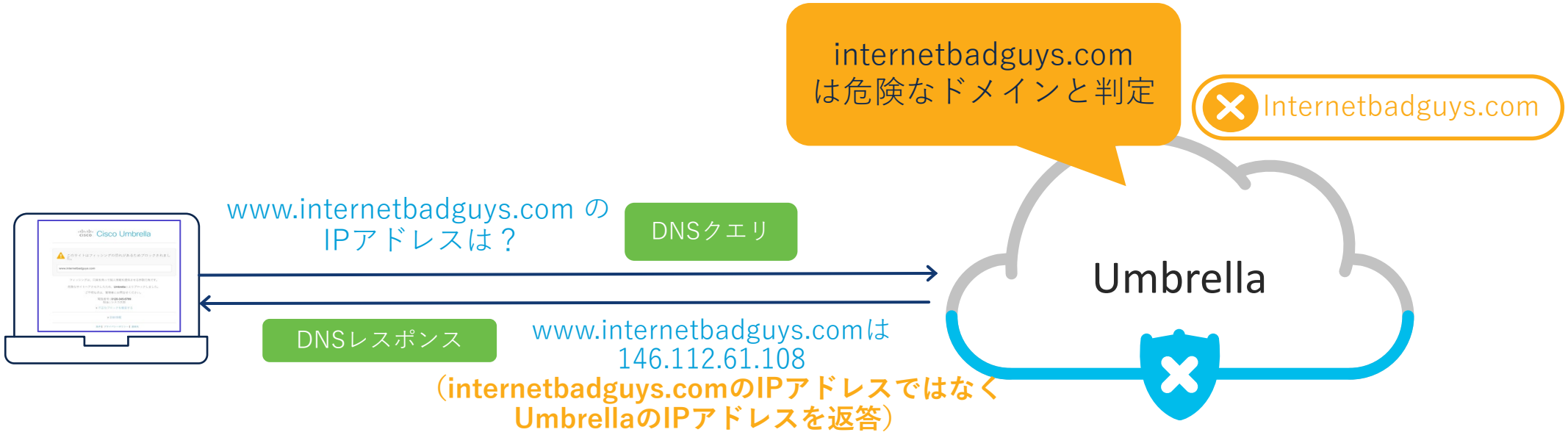
- File Inspection：ファイルがダウンロードされる前にスキャン、悪意のあるコンテンツが含まれていないか確認
- SSL復号：暗号化されたweb通信を復号して精査し、安全性を確認

https://docs.umbrella.com/deployment-umbrella/docs/%E3%82%A4%E3%83%B3%E3%83%86%E3%83%AA%E3%82%B8%E3%82%A7%E3%83%B3%E3%83%88-%E3%83%97%E3%83%AD%E3%82%AD%E3%82%B7%E3%81%A8%E3%81%AF

Secure DNS機能の動作

- ドメインの安全性を確認してから名前解決を行い、IPアドレスを返す

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



第三者評価、競合比較

- 2020年9～10月に AV-TEST にて実施
- 各製品は最も高い防御となるようそれぞれ設定
- リモート エージェントへの保護を検証
- Cisco のエージェントは AnyConnect 4.9MR1

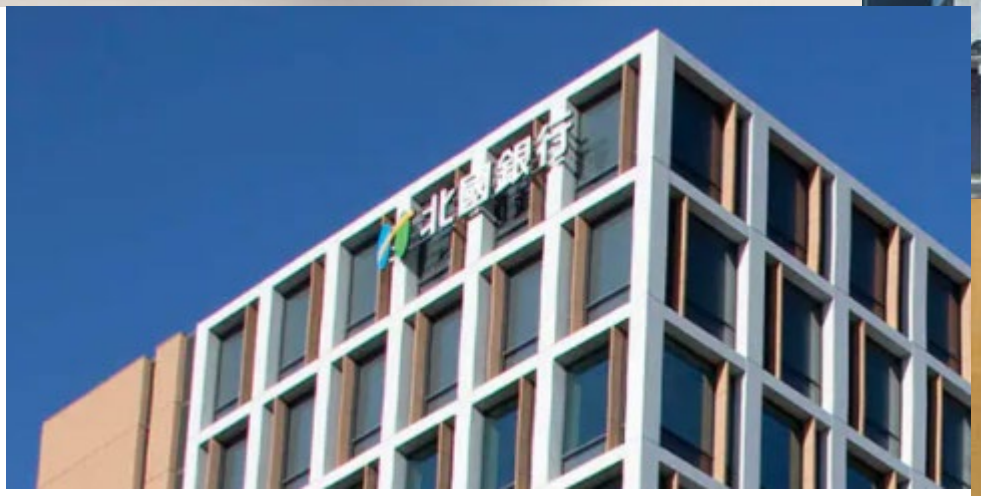
Product	製品パッケージ	検知率	誤検知率
サンプル数		3,572	2,165
Cisco Umbrella	DNS Security Advantage	70.69%	0.28%
Akamai Enterprise Threat Protector	Intelligence	53.58%	1.34%
Infoblox BloxOne	Advanced	36.28%	11.78%

Umbrella は 2年連続でDNS、プロキシ共にベストの検証結果と誤検知率*1

*1 誤検知率の検証は、2020年から実施

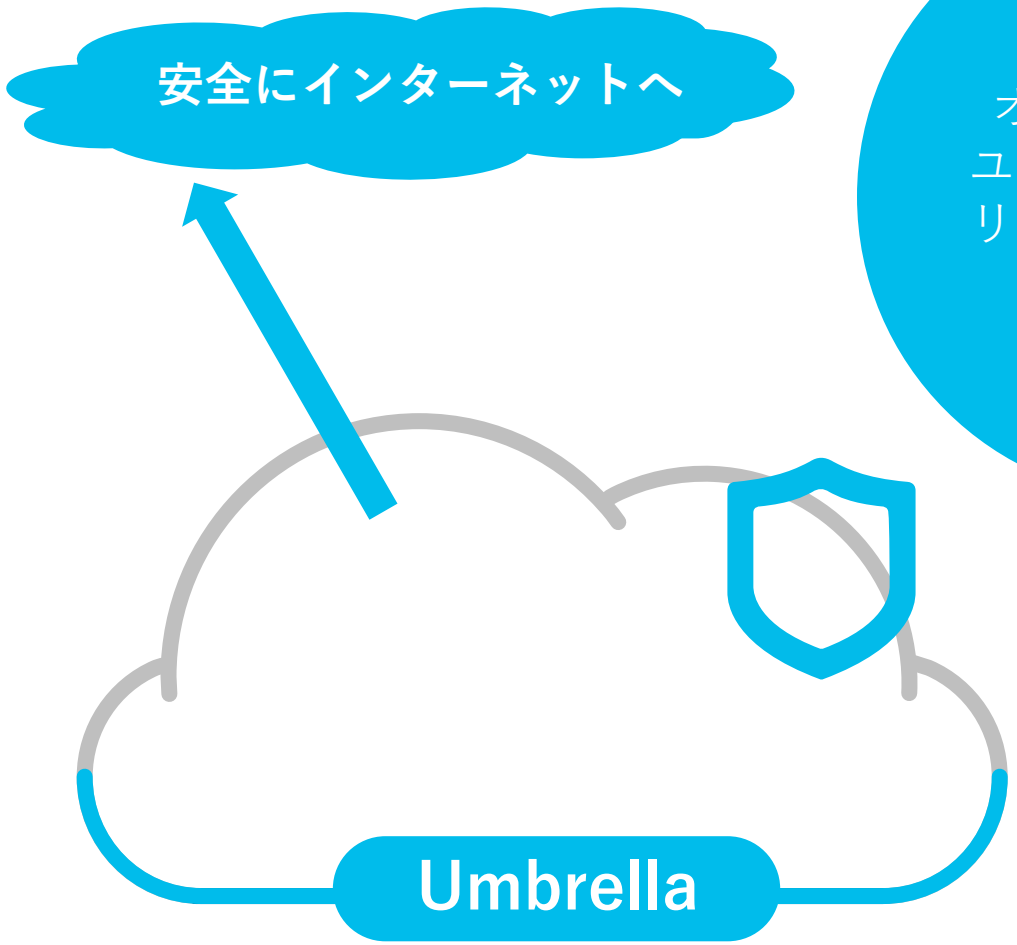
https://gblogs.cisco.com/jp/2020/11/av-test-places-cisco-umbrella-first-in-security-for-secure-web-gateway-and-remote-workers/

多数の業界で導入実績あり



https://www.cisco.com/c/ja_jp/about/case-studies-customer-success-stories/customer-stories-listing.html?flt2_general-table0=umbrella

まとめ



オフィスで働く
ユーザだけでなく
リモートユーザも
保護

名前解決の問い合わせに
対し危険なドメインへの
アクセスをブロック

直感的な操作
Talosの監視

DNS設定を変えるだけ
の簡単導入

参考リンク集

- Sales Connect セキュリティ資料　Umbrella及び他セキュリティ製品に関するコンテンツがまとまっています

製品情報

- PSU-VoD-SEC-Umbrella-01 概要のご紹介-Umbrella-01 Overview
- PSU-VoD-SEC-Umbrella-02 機能のご紹介-Umbrella-02 Feature Introduction -
- PSU-VoD-SEC-Umbrella-03 機能(初期セットアップ）のご紹介-Umbrella-03 Feature（Initial Setup) Introduction -
- PSU-VoD-SEC-Umbrellaライセンス概要-Umbrella license
- パッケージ比較

設定・POV

- Umbrella User Guide
- PSU-VoD-SEC-Umbrella SIG PoVベストプラクティス1 POVパターン抽出-Umbrella SIG PoV Best Practice1 –
- PSU-VoD-SEC-Umbrella SIG PoVベストプラクティス2 テクニカルガイド-Umbrella SIG PoV Best Practice2 -

SECURE