セッションに関するご質問

アンケートフォームにご記入ください。

担当営業やシスココンタクトセンターまでにお問い合わせください。

今後のシスコセキュリティウェビナー

https://www.cisco.com/c/ja_jp/training-events/events-webinars/webinars.html

毎週木曜日開催を予定。当面の予定は以下となります。

2020/6/4	木	14:00-14:30	30分でわかる最新の多要素認証 (Duo Security)
2020/6/4	木	14:30-15:00	30分でわかるマイクロセグメンテーション
2020/6/11	木	14:00-14:30	30分でわかるVPN（AnyConnect）
2020/6/11	木	14:30-15:00	30分でわかるクラウドセキュリティ（Umbrella）
2020/6/18	木	14:00-14:30	30分でわかるメールセキュリティ
2020/6/18	木	14:30-15:00	30分でわかるエンドポイントセキュリティ（AMP）
2020/6/25	木	14:00-14:30	30分でわかる認証基盤（ISE）
2020/6/25	木	14:30-15:00	30分でわかる可視化と脅威検出（StealthWatch）

30分でわかるクラウドセキュリティ
Cisco Umbrella

シスコシステムズ合同会社　セキュリティ事業
テクニカル ソリューションズ アーキテクト
稲澤　敏

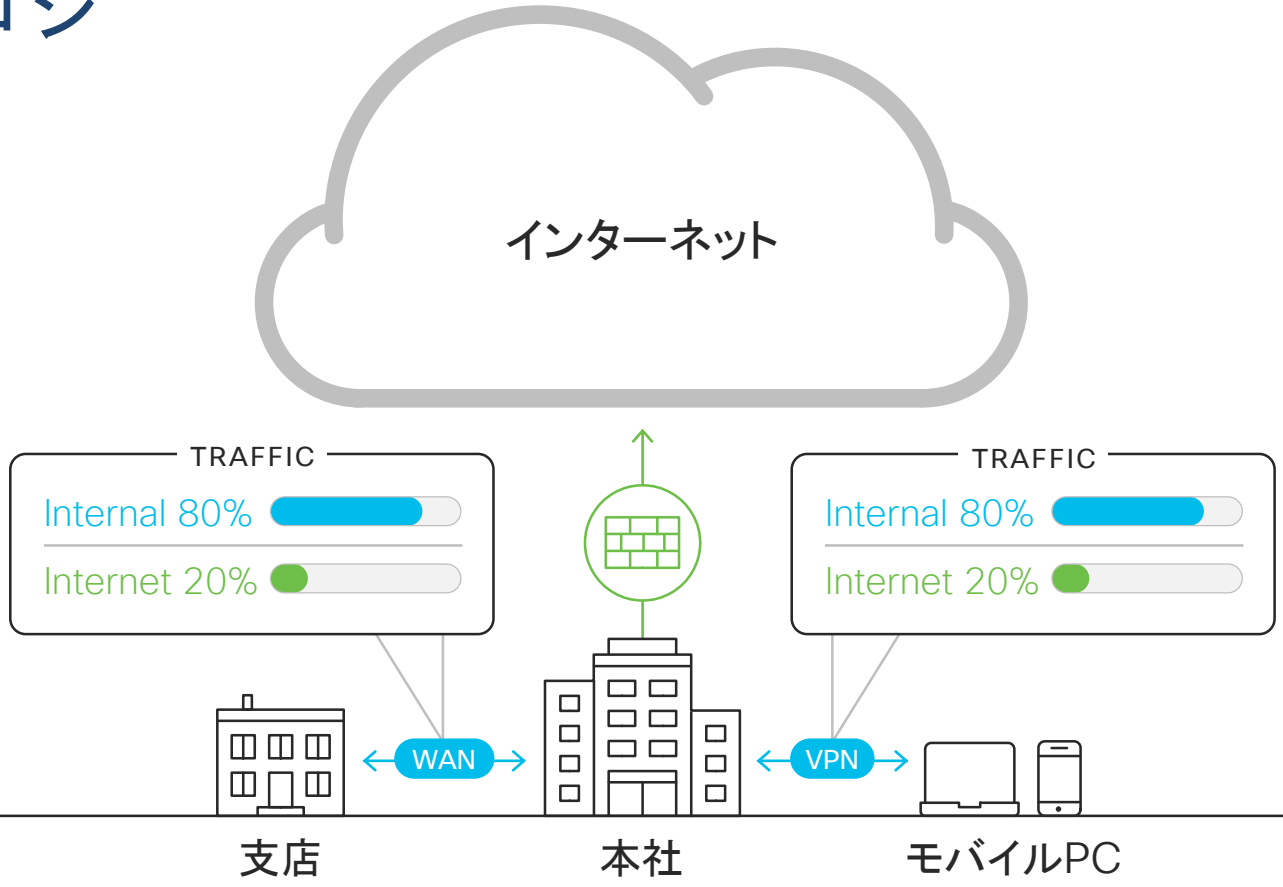
2020/06/11

アジェンダ

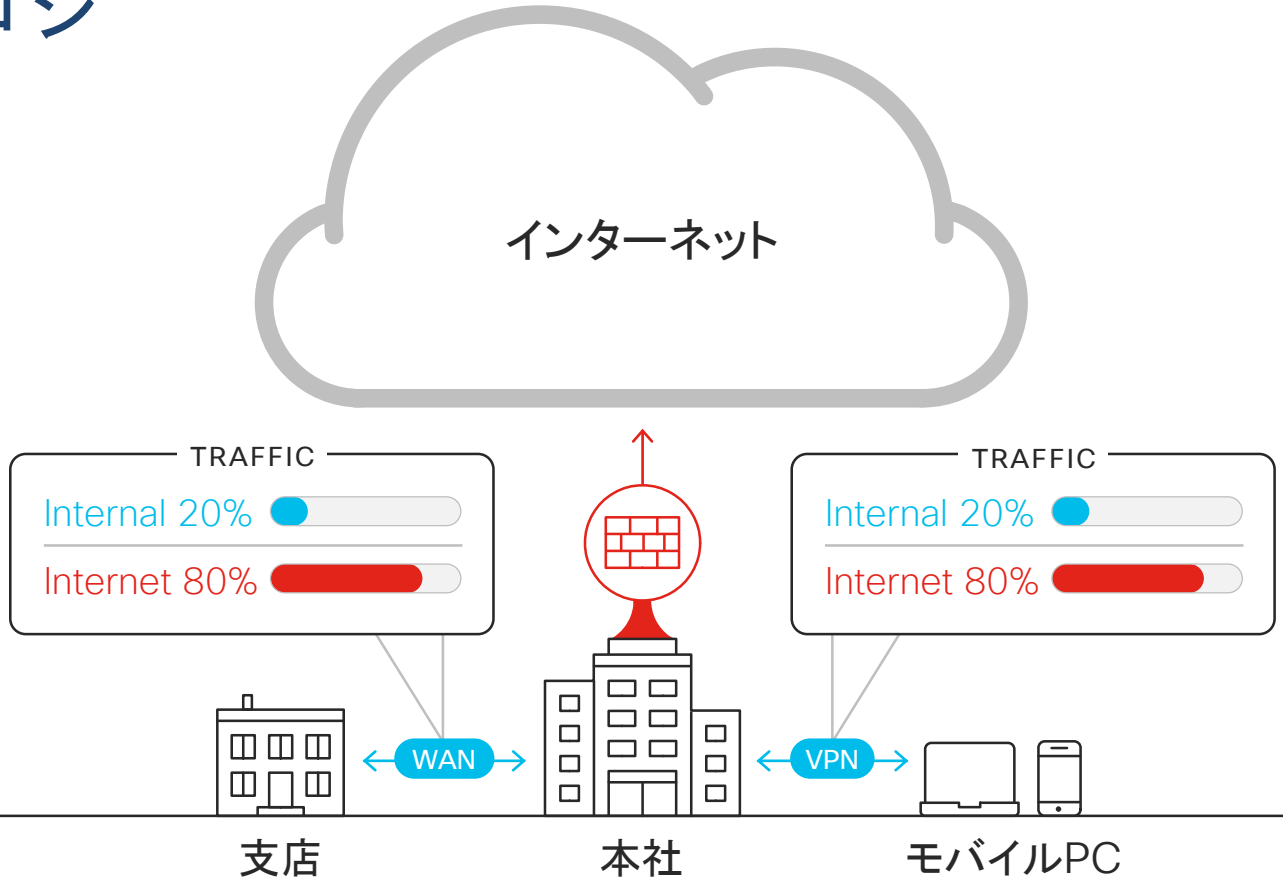
- IT環境の変化に伴う新たな課題
- Cisco Umbrellaが提供するSecure Internet Gateway (SIG)
  - ✓ DNS レイヤセキュリティ
  - ✓ セキュア Web ゲートウェイ
  - ✓ クラウドファイアウォール
  - ✓ SaaS制御機能 (CASB)
- ライセンス
- 導入/展開/連携　その他

IT環境の変化に伴う新たな課題

従来のトポロジー昔前



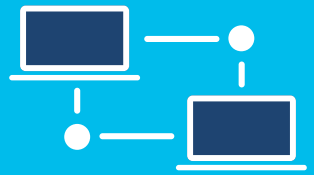
従来のトポロジ
今現在



Why?　変化をもたらす様々な要素

働き方変革
リモートワークの推奨

ハイブリッド化



いままでの境界線

従来のネットワーク:
エンドポイント,
オンサイトのユーザー,
サーバー, 業務アプリ

クラウドシフト
IoT化

BYOD化

モバイル機器の
多様化

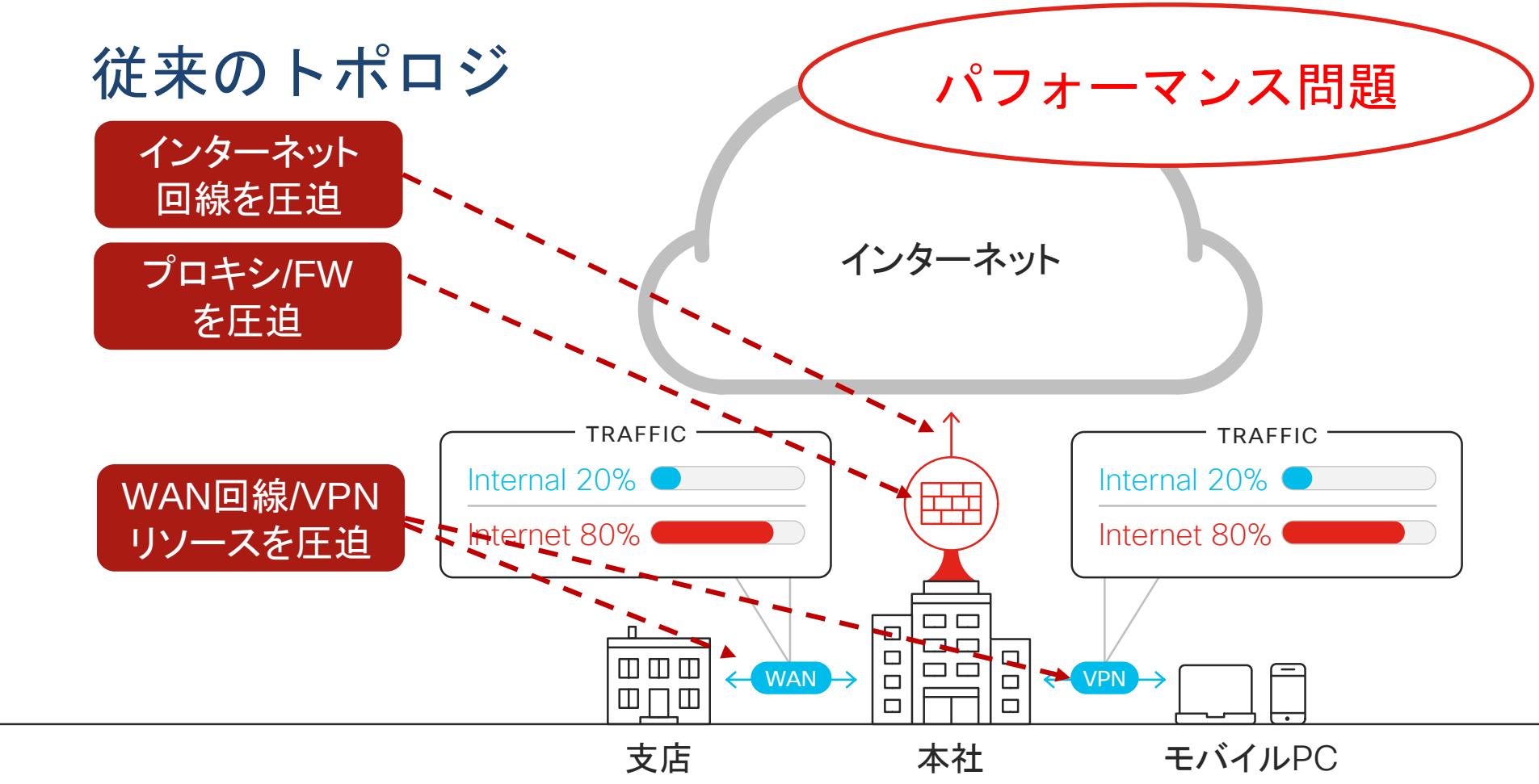
パートナー
協力会社

従来のトポロジ

インターネット
回線を圧迫

プロキシ/FW
を圧迫

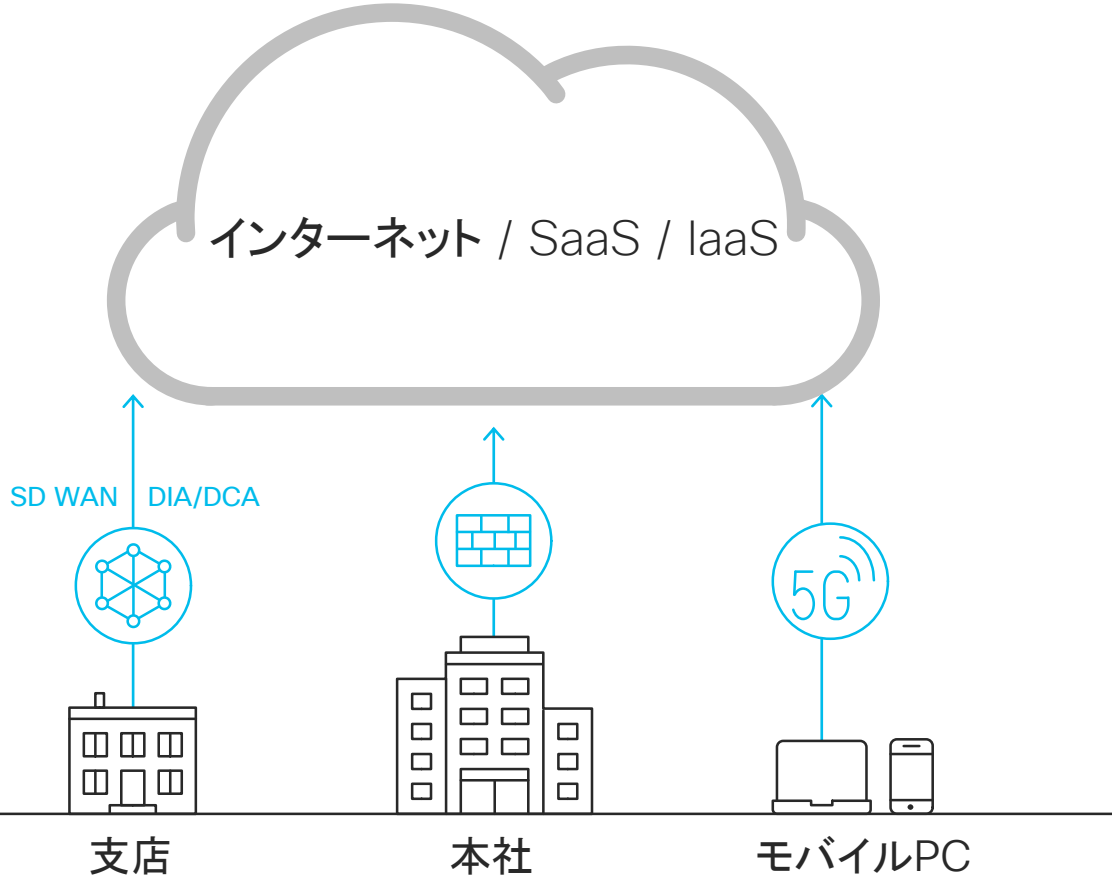
WAN回線/VPN
リソースを圧迫

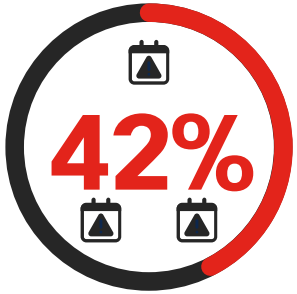


新しいモデル

ネットワーク:
分散型

セキュリティ:
データセンタ、クラウド、
ブランチの出口で防御





セキュリティの展開に一ヶ月以上かかるブランチの割合

ブランチ オフィスは脆弱な状態

最近の脅威により感染したユーザがブランチまたは
ローミングユーザであった割合

Source: ESG Research Survey, Cisco Secure Internet Gateway Survey, January 2019

新しいモデル

新たなセキュリティの課題

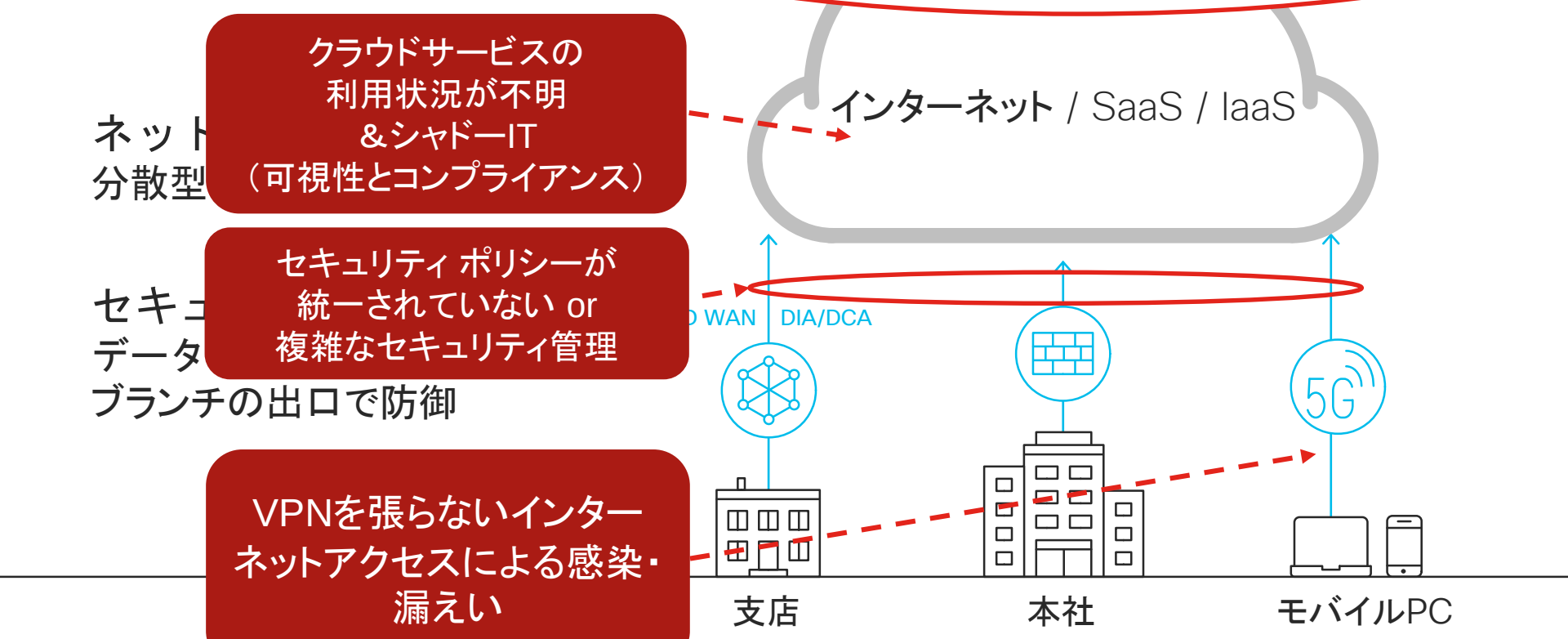
ネット
分散型

セキュ
データ
ブランチの出口で防御

クラウドサービスの
利用状況が不明
＆シャドーIT
（可視性とコンプライアンス）

セキュリティ ポリシーが
統一されていない or
複雑なセキュリティ管理

VPNを張らないインター
ネットアクセスによる感染・
漏えい

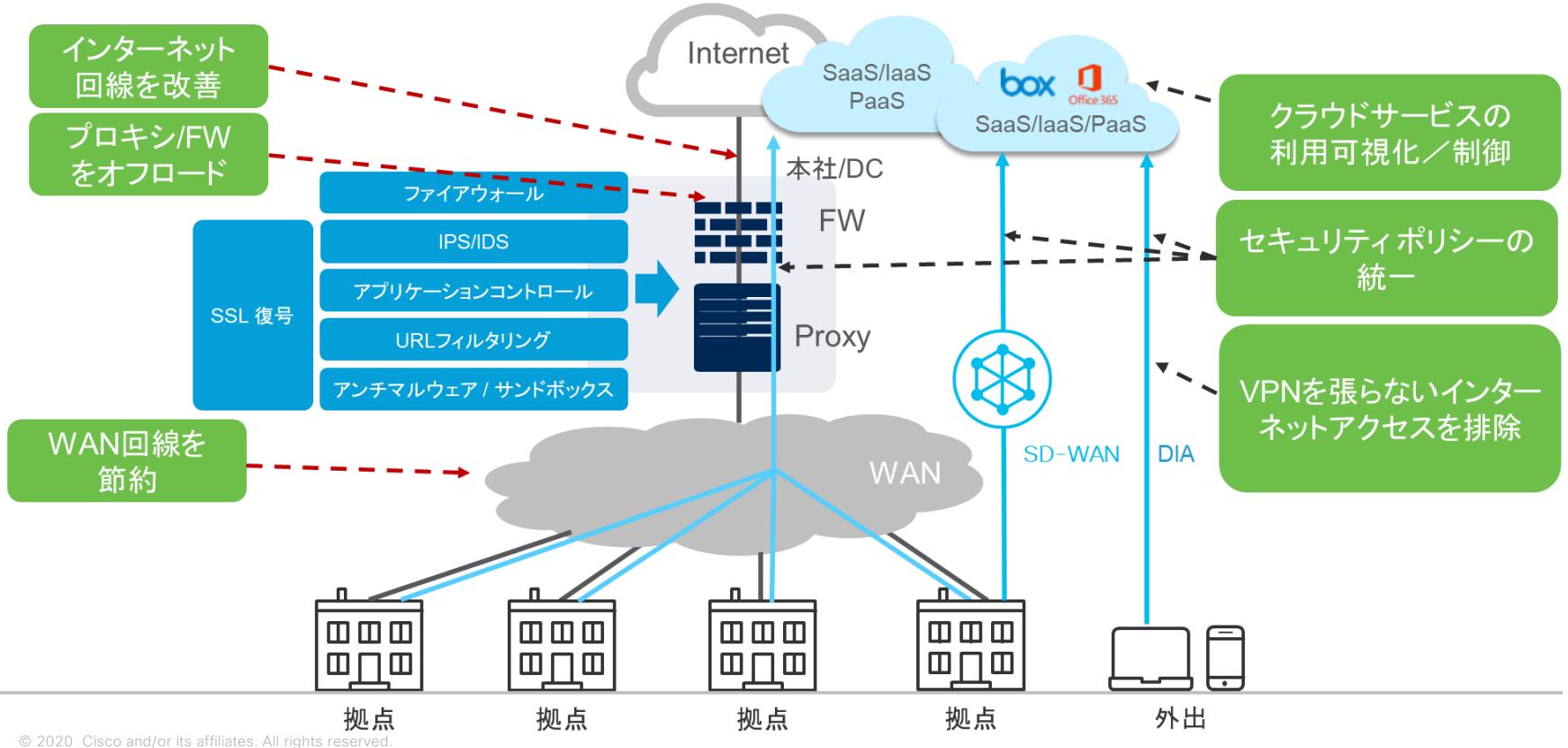


新たな問題・課題の解決策
統合型クラウドセキュリティサービスへのシフト

- DNSレイヤセキュリティ
- Webゲートウェイ
- ファイアウォール
- CASB
- 脅威インテリジェンス

セキュリティの境界をオンプレからクラウドへ
→より効果的で柔軟な保護を実現！！

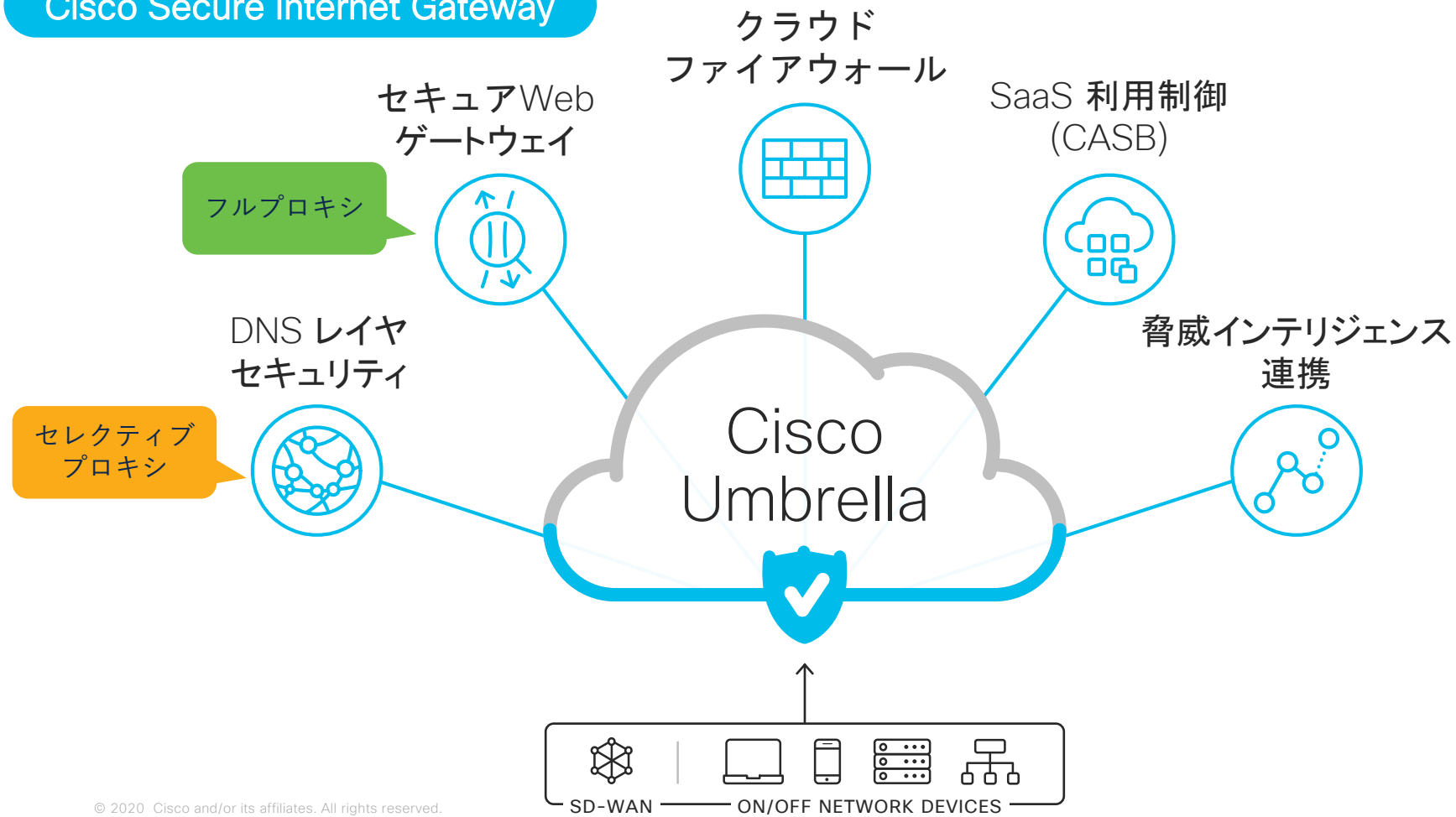
いままでの境界線における課題を解決



Cisco Umbrellaが提供する Secure Internet Gateway(SIG)

Umbrella ≠ DNS Layer Security

Cisco Secure Internet Gateway



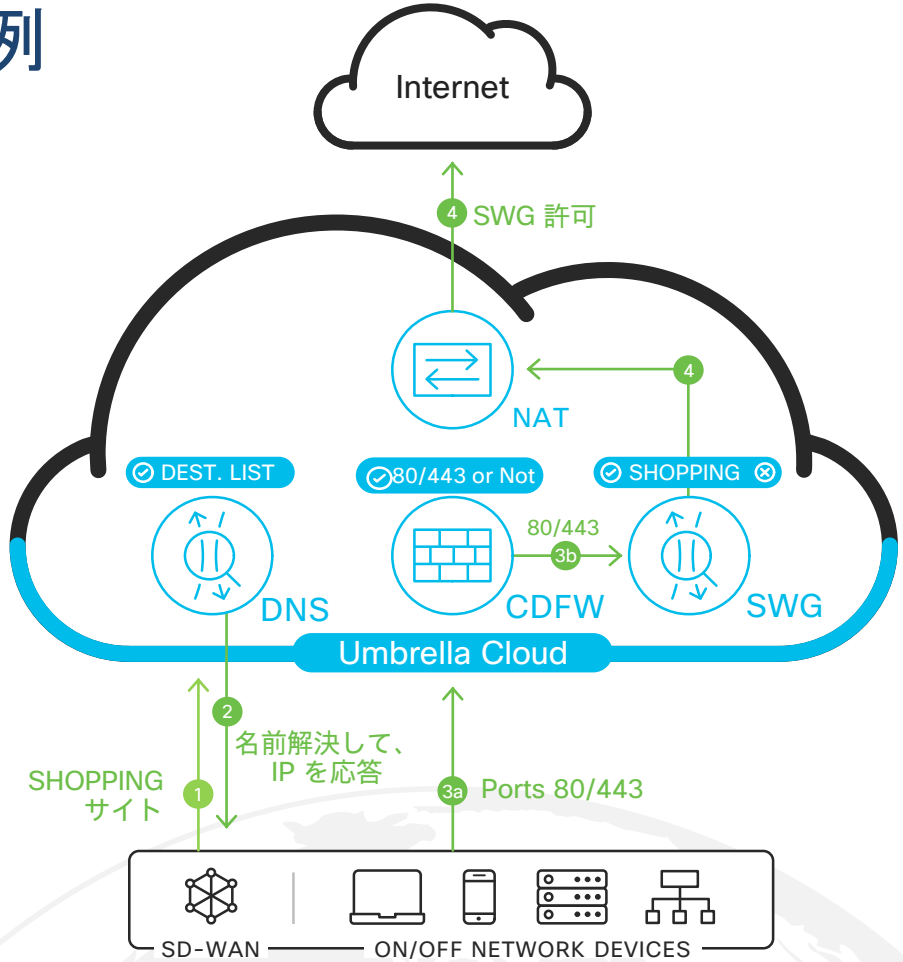
通信ポリシー制御フロー例

本図の想定ポリシー判定

DNSポリシー　⇒許可
CDFWポリシー　⇒許可
SWGポリシー　⇒許可

判定フロー例

1) DNSリクエスト
2) 宛先IPをリターン
3a) ポート80/443/21のリクエストを CDFW で判定
3b) ウェブリクエストを SWG で判定
4) SWGで許可された通信はプロキシされインターネットへアクセス



Cisco Umbrella – セキュアインターネットゲートウェイ

インターネットへの入口をすべてセキュアに

可視性

企業ネットワークへの
オン/オフ問わず

全てのインターネットおよび
Webトラフィック

全てのアプリケーション

全てのデバイス

SSLの復号

防御

DNS レイヤセキュリティ

Web インスペクション

ファイル インスペクション

サンドボックス

脅威インテリジェンスへの
アクセス

制御

URL ブロック/許可リスト

ポート & プロトコル ルール

コンテンツ フィルタリング

簡単なアプリ制御

きめ細やかなアプリ制御

Cisco Talos 脅威インテリジェンス

Cisco Umbrellaの
利用実績

200B
リクエスト数/日

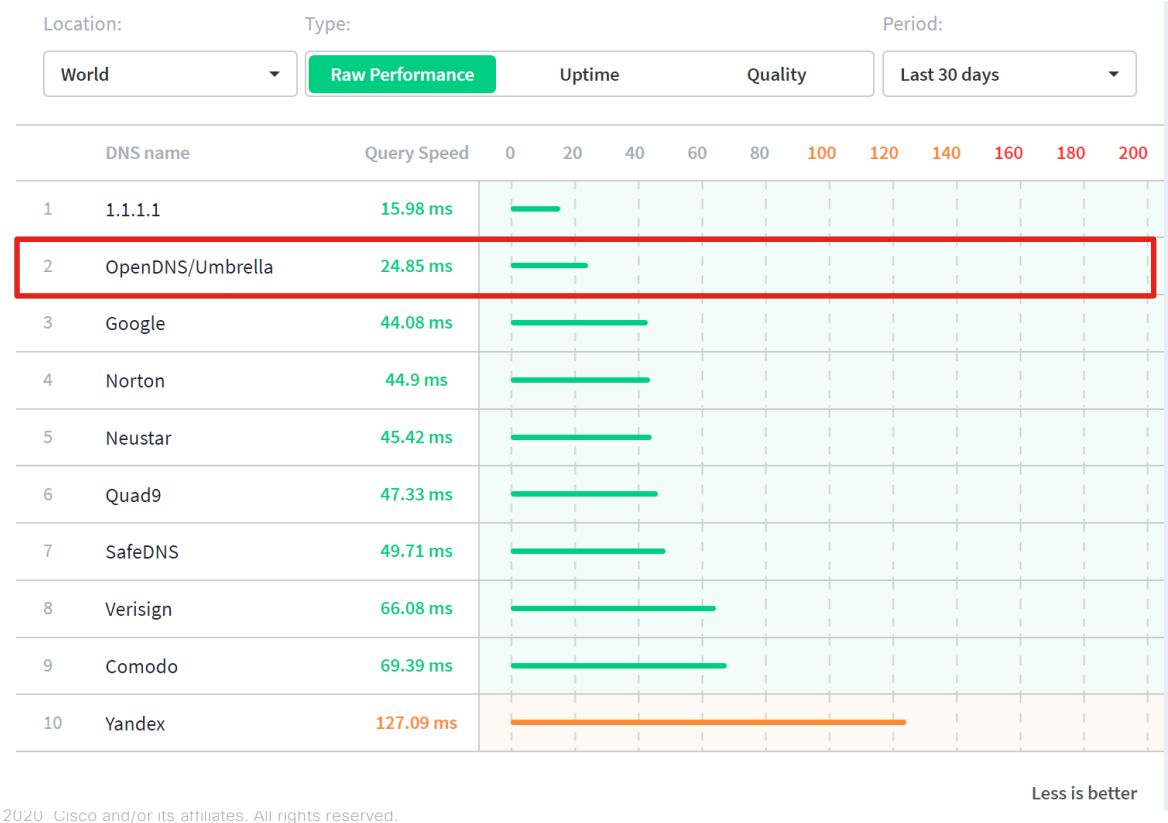
100M
アクティブユーザ数/日

22.5K
顧客数

190+
利用されている国

DNS レイヤセキュリティ

Umbrellaは早くて堅牢なリカーシブDNSサービス



Umbrella DNS
208.67.222.222
208.67.220.220

サービス開始以降100%のアップタイム！

出典:DNSPerf
https://www.dnsperf.com/#!dns-resolvers

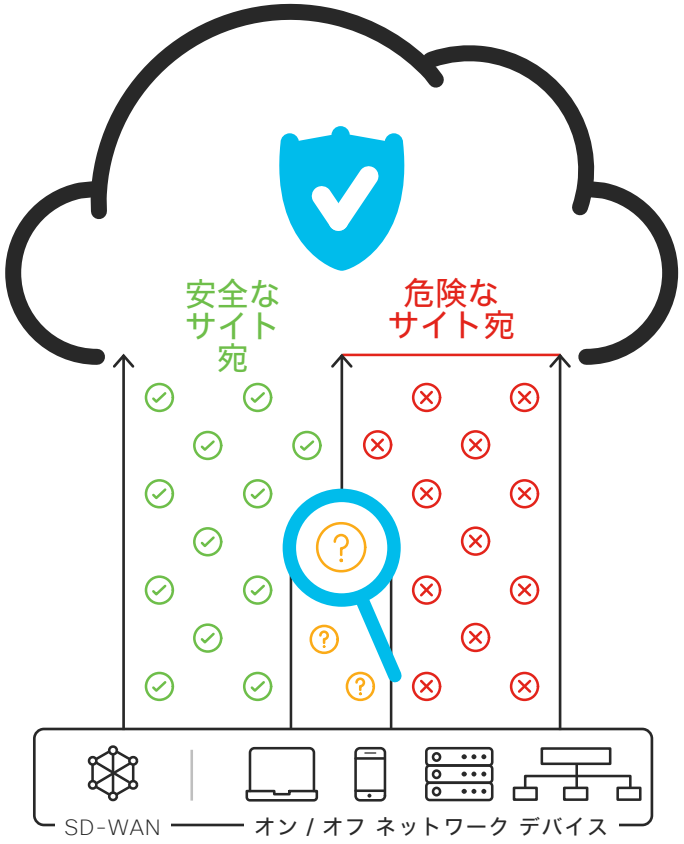
DNS レイヤ セキュリティ
第一線での防御

わずか数分で適用

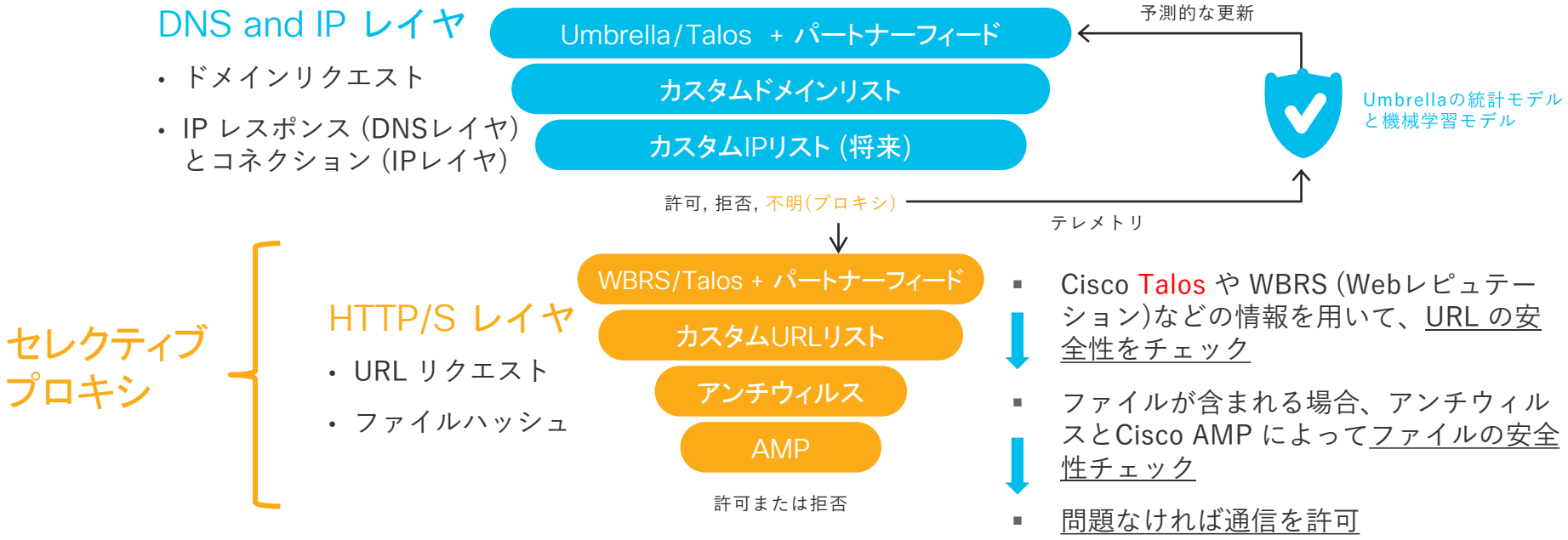
マルウェア、フィッシング、コマンド＆コントロール、DNS トンネリング等に関連づいたドメインをブロック

初期の段階で脅威をブロックしながら、侵入したマルウェアについては活動を阻止

驚くべきユーザ エクスペリエンス –
高速なインターネットアクセスと、リスクのあるサイトへのプロキシ経由アクセス（セレクティブプロキシ）



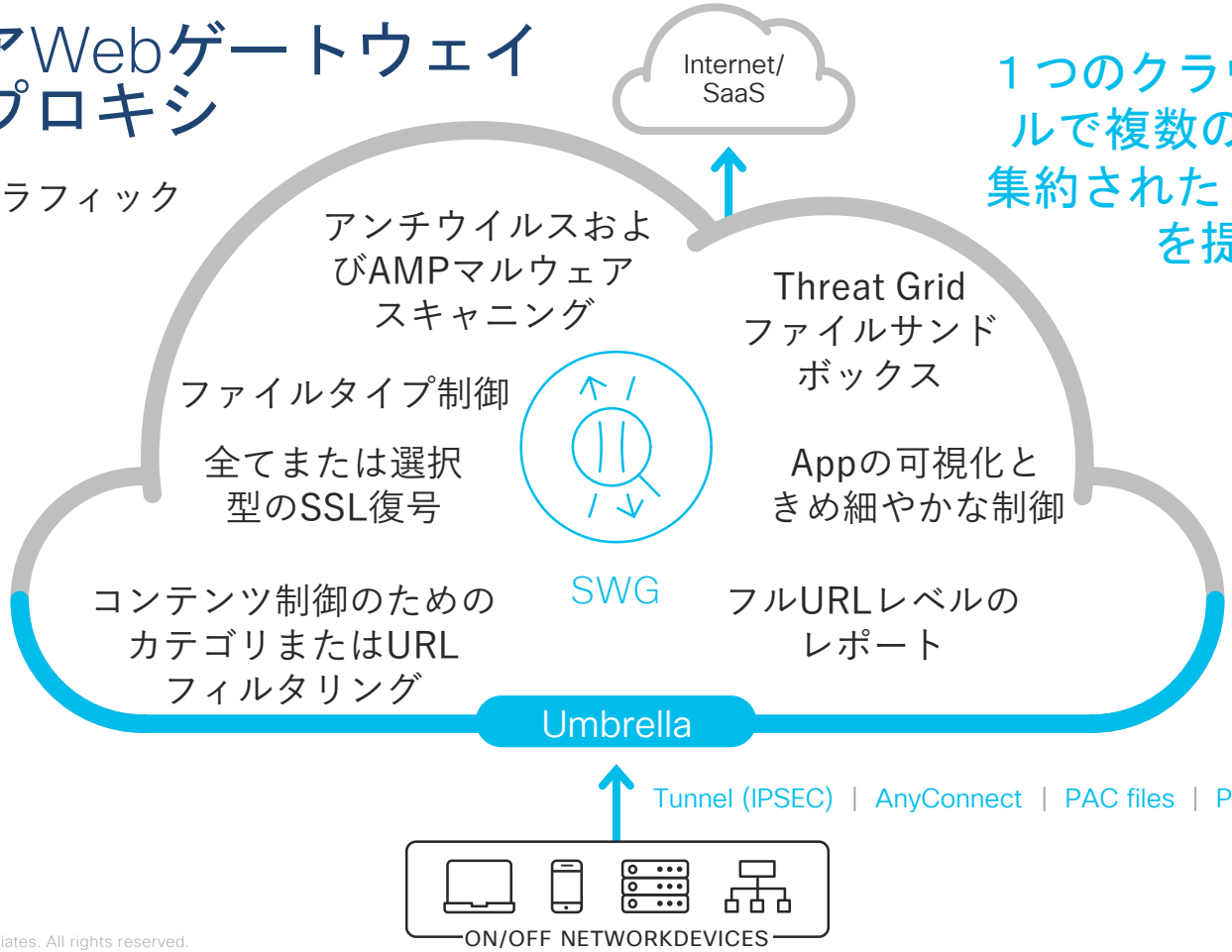
全てのポートをカバーし、危険な（疑わしい）ドメインをより詳細に調査



セキュア Web ゲートウェイ

セキュアWebゲートウェイ＝フルプロキシ

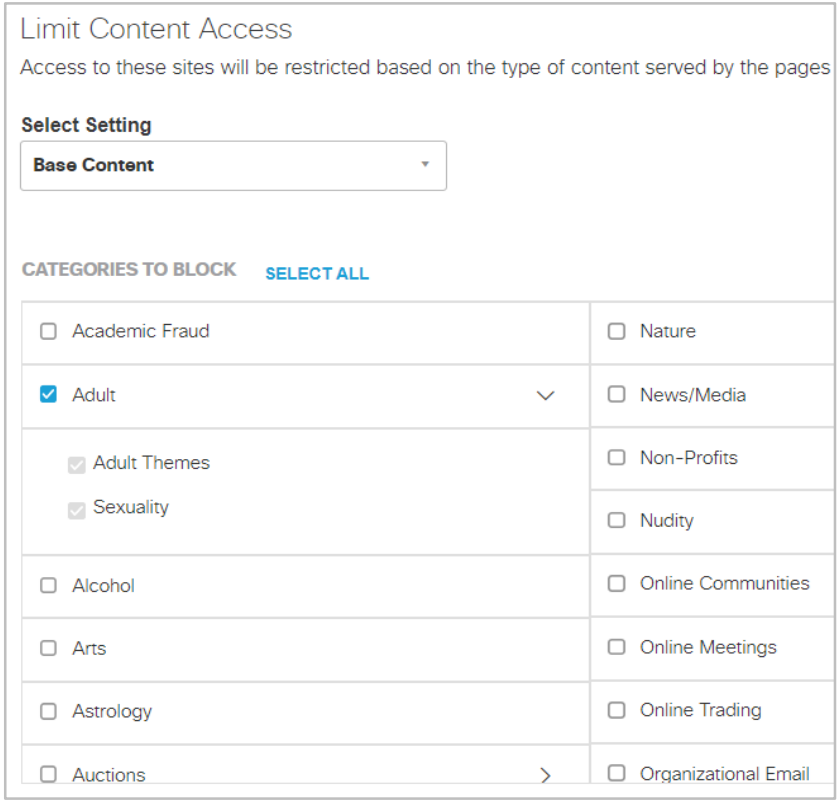
全てのウェブ トラフィックをキャプチャ



1つのクラウドコンソールで複数の機能および集約されたレポート機能を提供！

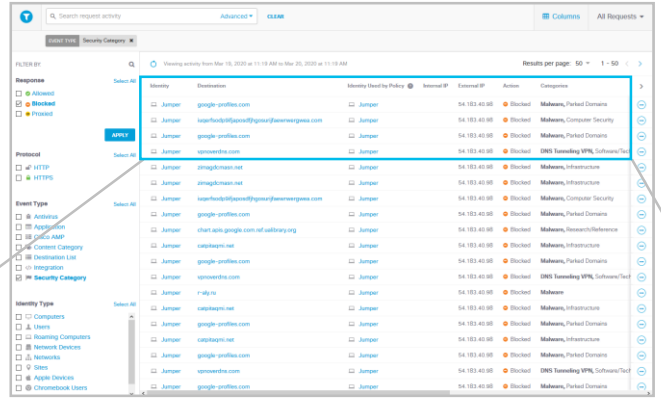
カテゴリベース フィルタリング

- 多数のサイトにポリシーを適用
  - コンテンツカテゴリはコンプライアンス目的での使用
  - セキュリティカテゴリはセキュリティポリシー目的での使用
- Umbrella SWG は双方のカテゴリに Talosカテゴリを使用
- カテゴリ数100+
- 動的なクラウド更新



マルウェアとウィルスからの保護

- 幅広いマルウェアとウイルスをスキャンして検出し、感染を回避して攻撃を阻止
- Advanced Malware Protection (AMP) とサードパーティウィルスプロテクションツールの実装
- アクティビティレポートには、ブロックされたすべてのイベントの詳細が表示



Identity	Destination	Identity Used by Policy	Internal IP	External IP	Action	Categories
Jumper	google-profiles.com	Jumper		54.183.40.98	Blocked	**Malware,** Parked Domains
Jumper	iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	Jumper		54.183.40.98	Blocked	**Malware,** Computer Security
Jumper	google-profiles.com	Jumper		54.183.40.98	Blocked	**Malware,** Parked Domains
Jumper	vpnoverdns.com	Jumper		54.183.40.98	Blocked	**DNS Tunneling VPN,** Software/Tec

Threat Grid ファイル分析（サンドボックス）

サンドボックス検査:

- ウイルススキャンとAMPによるマルウェアスキャンを通過したファイル(50MB以下)
- これまでAMPで未確認でありThreat Gridの検査対象となる属性を持つファイル
- libmagicによるファイルタイプの識別

File Retrospective

Recent Retrospective Events

SHA256	Threat Score	Malware Name	Date Detected
7638f6d4a9cd3ea5fa88f9958da6e6e745b2931b96ecea...	100	W32.7638F6D4A9-100.SBX.TG	Jul 30, 2019 at 3:22 AM
526b2cad716f7dc1e568d5e68b8a251d19e129308806b...	100	W32.526B2CAD71-100.SBX.TG	Jul 27, 2019 at 3:23 AM
1a27fdf68d61964ddc13a62a75b15b7c94978def0b014...	100	W32.1A27FDF68D-100.SBX.TG	Jul 26, 2019 at 3:24 AM
49ade947bb9de7ce36f9735f90758d8425f939c2ce84b6...	100	W32.49ADE947BB-100.SBX.TG	Jul 25, 2019 at 4:31 AM
f9f23288188bc1a959e890084cc685db4ff9c50b95a52a...	100	W32.F9F2328818-100.SBX.TG	Jul 24, 2019 at 3:26 AM

1 - 5 of 32

クラウドファイアウォール

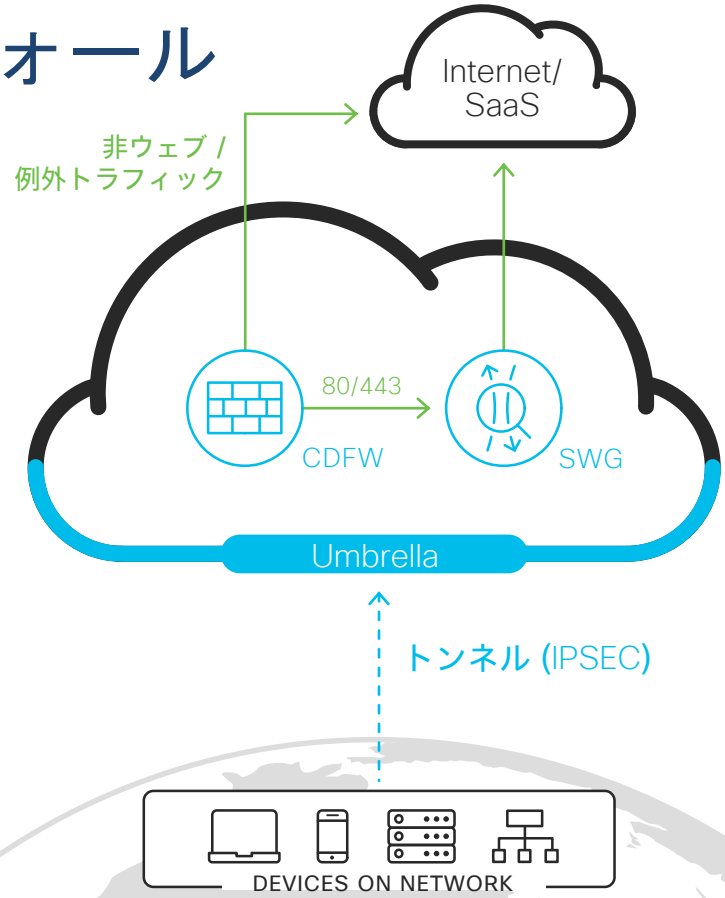
クラウド提供型ファイアウォール

全てのトラフィックを Umbrella にトンネリング

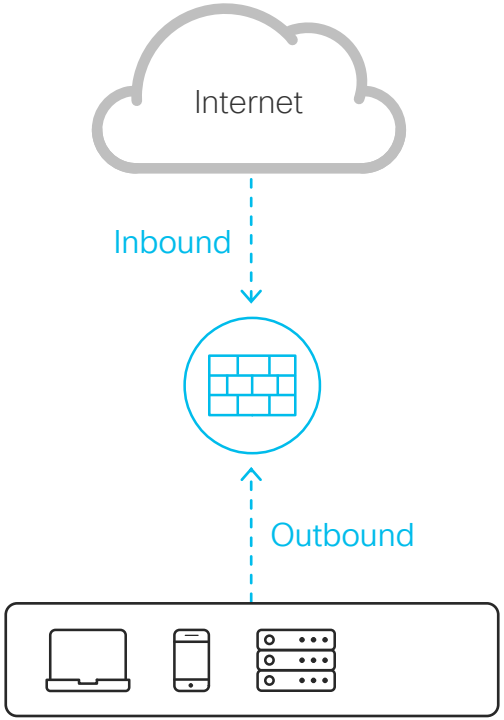
IP アドレス、ポート、プロトコルにもとづくルール設定 (L3/L4)

非ウェブアプリケーションとプロトコルに対するルール設定（L7, AVC） 近日公開予定

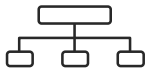
お客様のアドレスを匿名化してインターネットへのアクセスを提供（ソース アドレスにもとづく格付けの影響を低減）



Umbrella はアウトバウンドファイアウォール



アウトバウンドファイアウォールは
インターネットへのアクセスを保護
し、クラウドアプリへの制御を行うた
めに不可欠



SaaS制御機能（CASB）

App Discovery & Control – Breaking it Down

App可視化
16K+ Apps

- DNS
- SWG

App制御
+1000 Apps

- DNS Block
- DNS Allow
- SWG Block
- SWG Allow

詳細なApp制御
21 Apps

- SWG
- 21 Apps
- DNS or Selective Proxyでは非サポート

テナント制御可能なApp
3 Apps

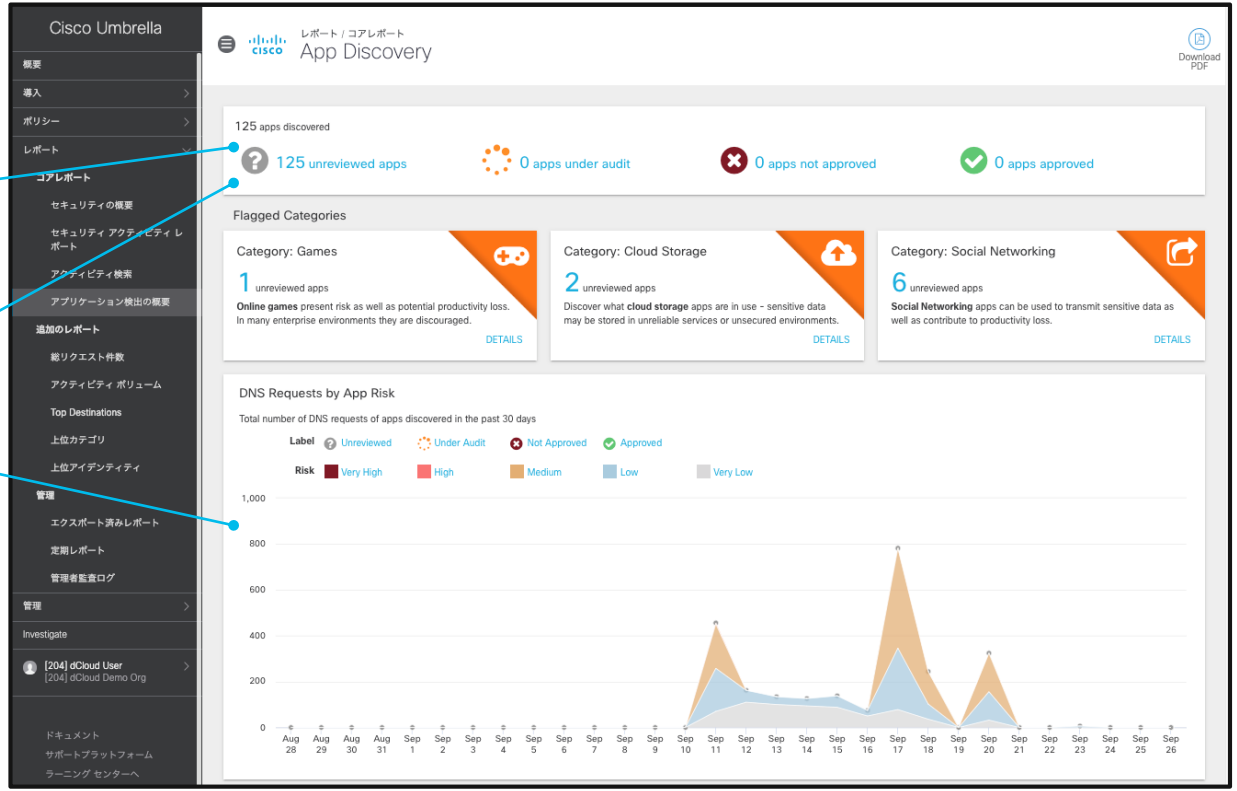
- SWG - (ベータ)
- O365, Slack and G Suite が最初
- 順次追加を予定

シャドーIT可視化と制御

検知した SaaS の状況

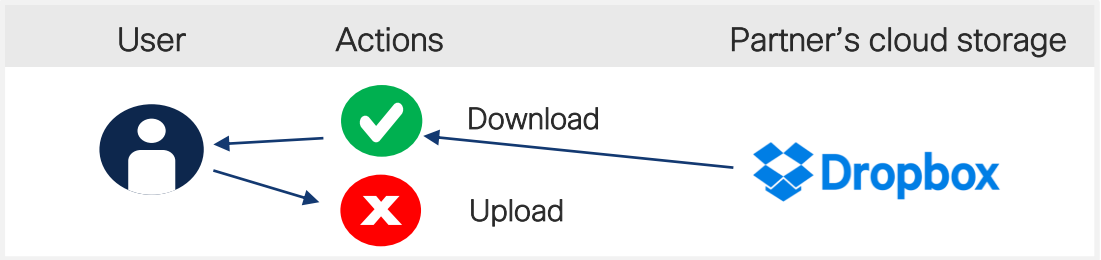
認められていない SaaS
を簡単にブロック

クラウド アプリの利用状況を
リスクごとに可視化し、詳細に説明



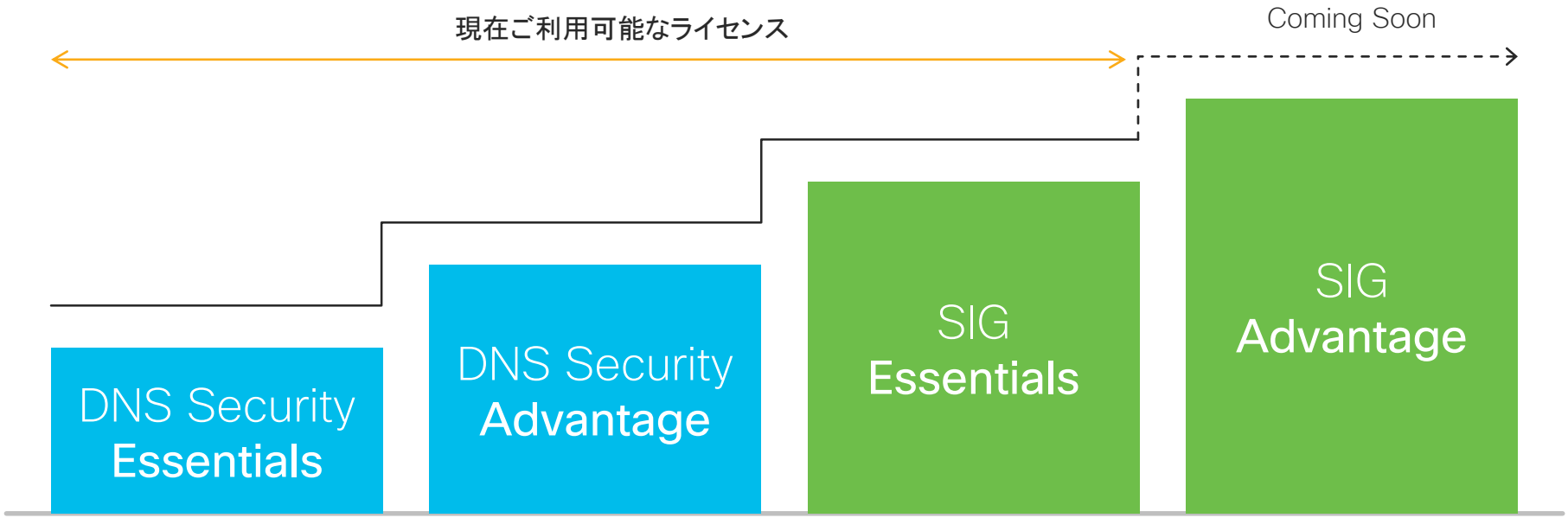
人気のSaaSアプリのきめ細やかな制御

- ソーシャルメディアアプリへの投稿/共有をブロック
- ウェブメールアプリへの添付ファイルをブロック
- クラウドストレージ、コラボレーション、業務系、コンテンツ管理、メディアアプリへのアップロードをブロック
- 要SIG Essential License



ライセンス

Cisco Umbrella パッケージ



Simplified view of seat-based packages

Cisco Umbrella パッケージ

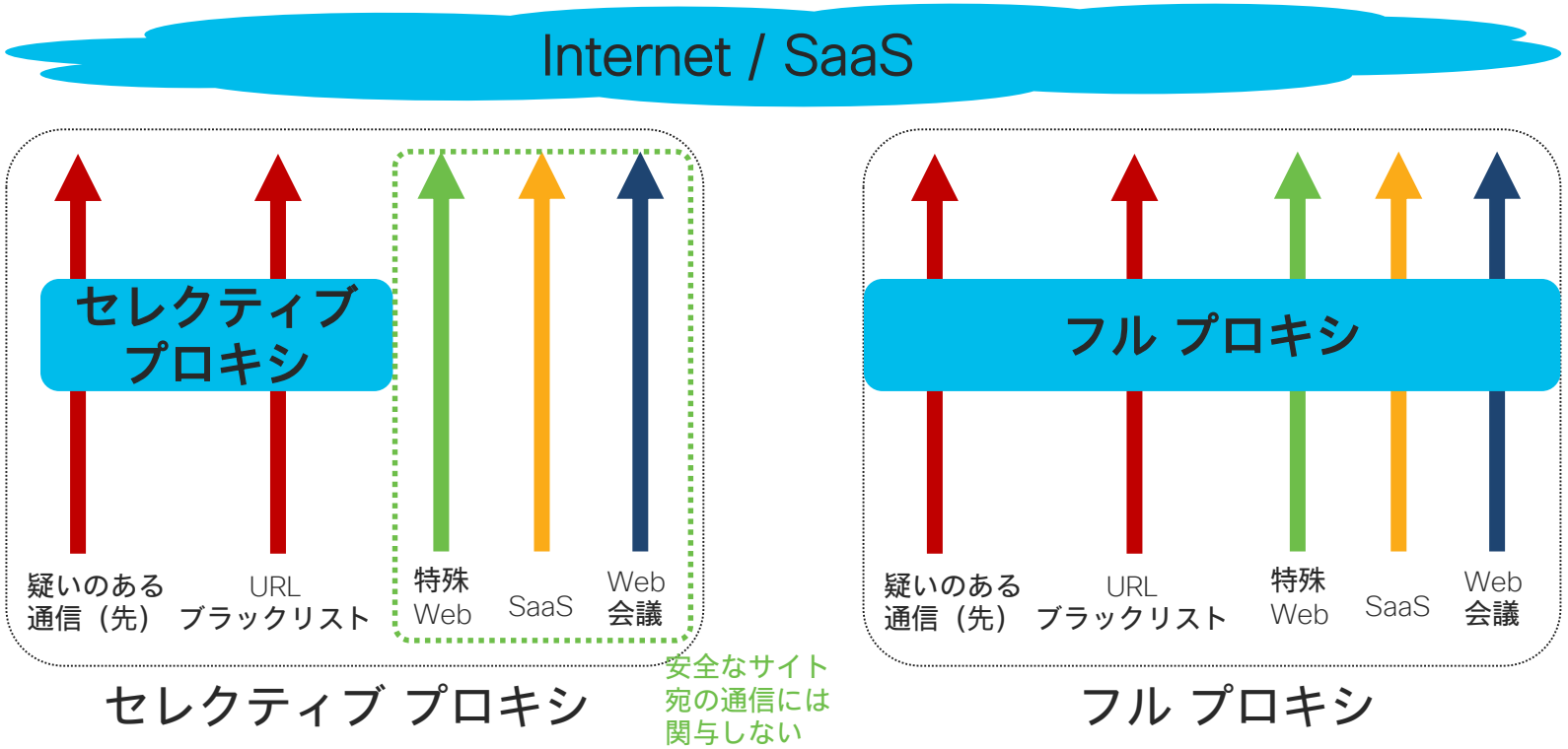
- Cisco Umbrella DNS Security および Secure Internet Gateway のライセンスは、シート数に基づいて提供されます。
- シート数は、インターネットに接続してサービスにアクセスする可能性があるユーザの数として定義されます。ユーザ数は保護対象のデバイスまたはエンドポイントの数とは無関係です。

主要パッケージのセキュリティサービス		DNS セキュリティ Essentials	DNS セキュリティ Advantage	SIG Essentials
DNS レイヤ セキュリティ	フィッシング、マルウェア、ボットネット、および危険なカテゴリ（マイニングや新規ドメインなど）に属するドメインをブロック	●	●	●
	パートナー（Splunk、Anomali など）インテグレーションやエンフォースメント API によるカスタムリストに基づいてドメインをブロック	●	●	●
	DNS をバイパスする C2 コールバック対策として直接 IP トラフィックをブロック	—	●	●
セキュア Web ゲートウェイ（SWG）	Web トラフィック検査用プロキシ	—	危険なドメインのみ	●
	SSL（HTTPS）トラフィックの復号化および検査	—	危険なドメインのみ	●
	Web フィルタリング	カテゴリベース ドメインベース	カテゴリベース ドメインベース	カテゴリベース ドメインベース URL ベース
	カスタマイズ可能なブロック/ 許可リスト	ドメインベース	ドメインベース	IP ベース URL ベース
	Cisco Talos などからのフィードに基づいて URL をブロック、アンチウイルスエンジンと Cisco AMP のデータに基づいてファイルをブロック	—	危険なドメインのみ	●
	Cisco Threat Grid クラウドのサンドボックス環境を使用して疑わしいファイルを分析（200 ファイル～/日）	—	—	●
	無害なファイルが危険なファイルに変化しても特定できる、遡及的セキュリティ	—	—	●
クラウド提供型 ファイアウォール	レイヤ 3 および レイヤ 4 ポリシーで特定の IP/ ポート/ プロトコルをブロック	—	—	●
	IPsec トンネル終端対応	—	—	●
クラウドアプリ セキュリティ制御	シャドー IT を検出およびブロック	ドメインベース	ドメインベース	URL ベース
	アプリケーション別にきめ細やかな制御（アップロード / ファイル添付 / 投稿の禁止など）が可能なポリシー	—	—	●

選べるプロキシ
セレクティブ プロキシとフル プロキシ

	セレクティブ 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	VS	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)	VS	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

比較：セレクティブ プロキシとフル プロキシ



セレクティブ プロキシ

フル プロキシ

比較：セレクティブ 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

- 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
- 既存グローバル IP アドレス活用
- 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

- 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

AV-TEST による検証結果

- 2019年11～12月に AV-TEST にて準備されたデータを利用（シスコは関与せず）
- 各製品は最も高い防御となるようそれぞれ設定
- DNS レイヤにおいては、Umbrella と Akamai でセレクティブ プロキシを有効化（SWG 無し）
- ウェブレイヤにおいては、DNS セキュリティの設定無し

DNS レイヤ テスト

テストの種類	Umbrella DNS + SEL. PROXY	Umbrella DNS	Infoblox	Akamai	paloalto NETWORKS
Malicious PE files (Portable executables)	77.94	57.11	33.70	11.09	4.17
Malicious destinations	55.09	24.55	25.36	38.27	28.18
Phishing links	83.97	74.57	49.57	39.42	13.14
Total detection rate	**72.63**	**51.80**	**35.25**	**26.47**	**13.66**

ウェブ レイヤ テスト

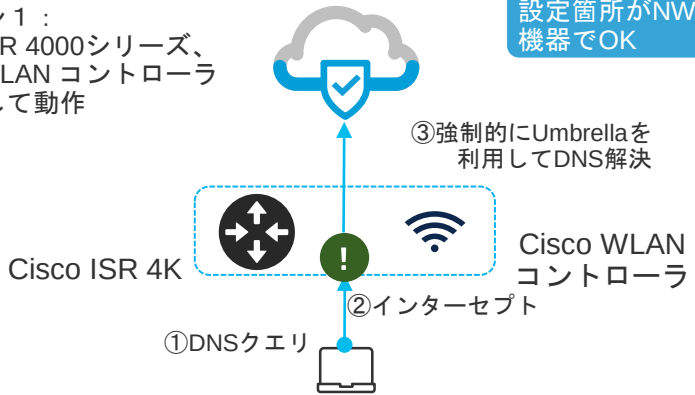
Type of test	Umbrella SWG	Symantec	zscaler	paloalto NETWORKS
Malicious PE files (Portable executables)	92.65	88.66	77.88	65.07
Malicious destinations	93.82	89.82	88.36	77.00
Phishing links	82.80	71.69	88.25	79.70
Total detection rate	**90.49**	**84.68**	**83.67**	**72.38**

導入/展開/連携　その他

Umbrella DNS セキュリティ展開イメージ

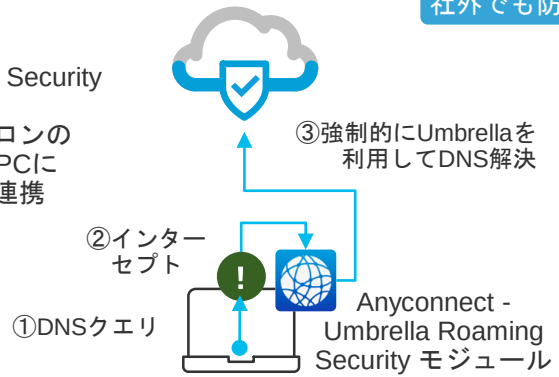
パターン１：
Cisco ISR 4000シリーズ、
Cisco WLAN コントローラ
と連携して動作

設定箇所がNW
機器でOK



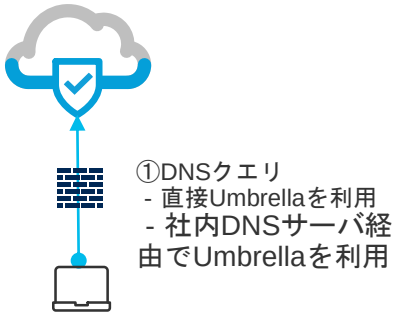
パターン２：
AnyConnect –
Umbrella Roaming Security
モジュール、
またはスタンドアロンの
Roaming Client をPCに
インストールして連携

社外でも防御が有効



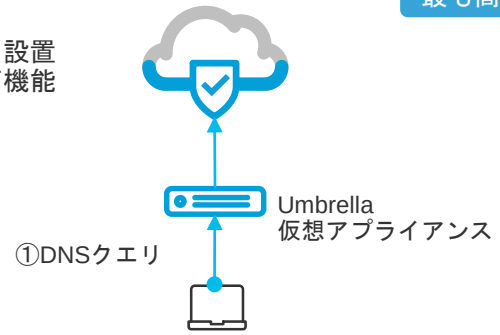
パターン３：
端末のDNSサーバが
Umbrellaになるように設定
- 社内DNSの参照先に指定
- DHCPサーバでの設定
- 端末のOSに手動設定
など

導入が最も簡単

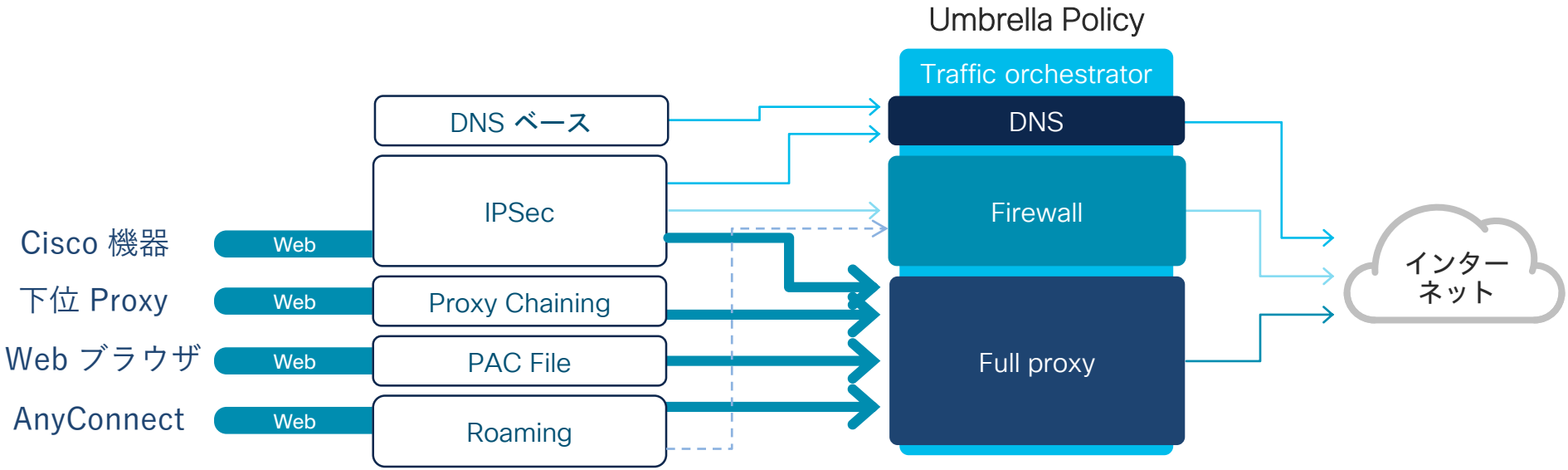


パターン４：
Umbrella 提供の
仮想アプライアンスを設置
連携することでより高機能
な動作が可能

最も高機能な導入



セキュア Web ゲートウェイ（SWG）接続イメージ



※Umbrella Roaming Clientは現状SWG非対応

*サポート予定 - - -

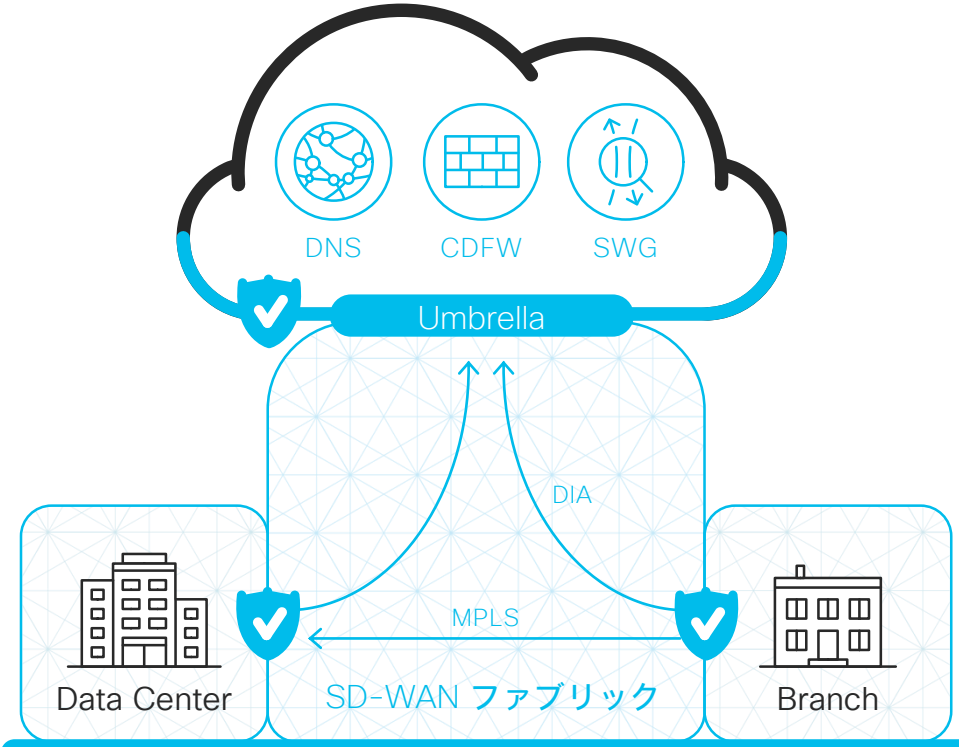
リモートワーク環境を常にセキュアにする AnyConnect 連携

VPN 接続時
(例：社内サーバへアクセス時)

VPN 切断時
(例：カフェで就業時)

Cisco SD-WAN 連携

シンプルかつ SD-WAN 通信に対する効果的な防御



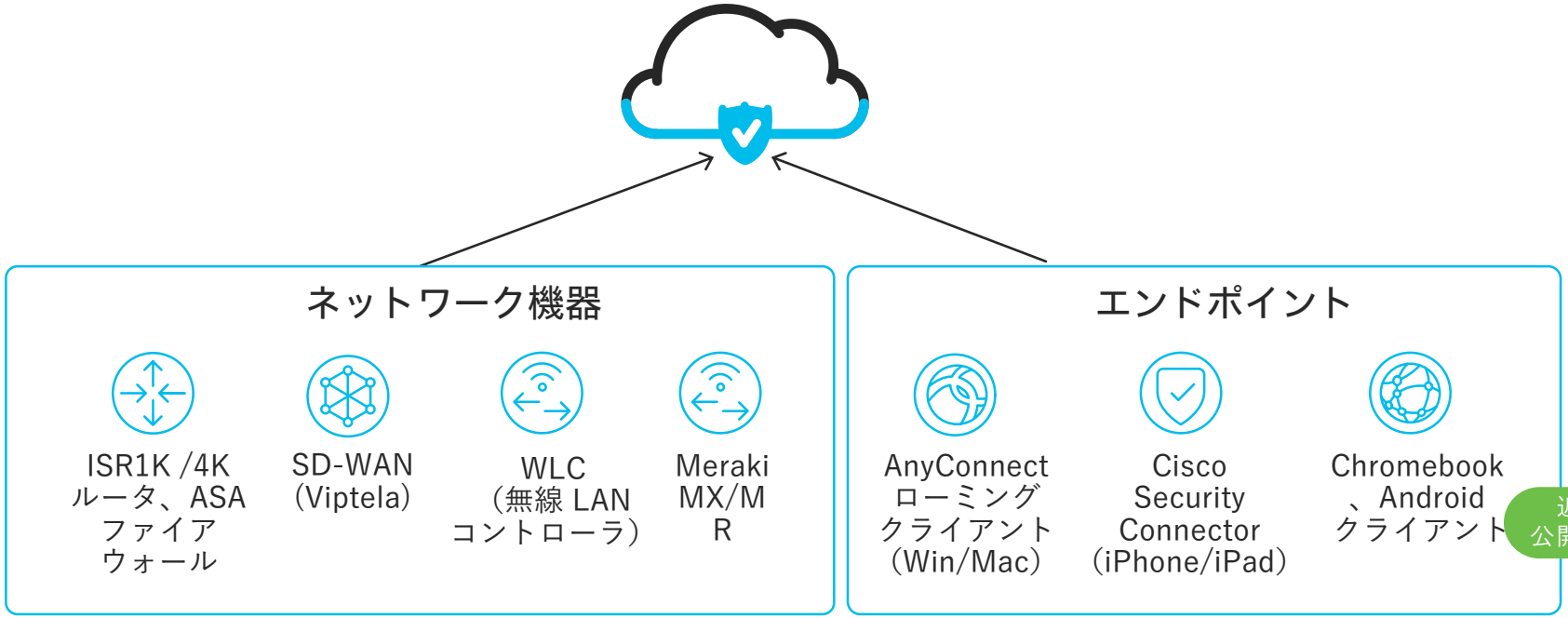
DNS レイヤ セキュリティをクイックに展開

新機能：クラウド提供型ファイアウォール (CDFW) およびフル プロキシ (SWG) による深いレベルの検査と制御

今後増える SaaS および ウェブトラフィックに対する容易な拡張性

製品プラットフォーム・製品間連携・一括サポートまでご提供可能な唯一の製品ベンダー

連携ネットワーク機器、エンドポイント一覧



まとめ

- 社内外全てのユーザを守るには適用漏れのない脅威対策が必要
- Umbrella SIGによりDNSセキュリティ、プロキシ、ファイアウォール、CASBなどの適材適所での設計が可能
- 脅威対策とパフォーマンスを両立するならDNSセキュリティ（セレクティブプロキシ含む）でバランスよく楽に運用
- コンプライアンス対策はフルプロキシ
- 様々な機器と連携（SD-WAN、AnyConnect、スマートフォンetc)、展開の素早さ・柔軟さ
- 業界トップの検知率（DNS、ウェブ共（第三者調査結果））

無料トライアル
ぜひお試し下さい

https://signup.umbrella.com/

お客様自身で評価ライセンスの申請が可能です。

申請後、1時間ほどで評価ライセンスのアクティベーション(有効化)メールが届きます。

評価アカウント用の管理者メールアドレスは、本番導入・運用を想定した管理者メールアドレスをご利用ください。

ご発注後の製品ライセンスの管理者アカウントは、評価時に登録したメールアドレスがそのまま利用されます。

セキュリティオファー：Cisco Umbrella

オファーの詳細：

- **既存のお客様**：オファー期間の終了まで、購入したユーザ数の上限に関係なく利用可能
- **新規のお客様**：Umbrella DNS セキュリティのトライアル期間を 通常の 14 日間から 90 日間に延長可能（オファー期間はアクティベーションから 90 日間）

パートナー様のアクション：

- 新規のお客様については、Umbrella Partner コンソール（UPC）トライアルをご利用のパートナー様が umbrella.partner.extensions@cisco.com へ電子メールを送信することにより、トライアル期間を最大 90 日間延長可能 ※1

サポート：シスコ セキュリティ パートナー セールス スペシャリスト、Umbrella サポートチーム、パートナーヘルプへお問い合わせください

Cisco Umbrella


CISCO

Webinarでのご質問への回答

ご質問内容	回答
DNSレイヤセキュリティでの"ドメインレベルの判別"とセレクティブプロキシで実施される"URLの安全性のチェック"の違いがいまいち理解できておりません。どちらも"https://~"の~以降の信頼性をチェックするものかなと考えており。。	DNSセキュリティではドメインリクエストが、セレクティブプロキシではHTTPまたはHTTPSのリクエストがそれぞれ検査対象となり、参照されるDBや解析方法も異なります。セレクティブプロキシではHTTP/HTTPSのコンテンツのインスペクションを行いますのでより細かな情報を取得可能で詳細な制御も可能となります。
フルプロキシ利用に必要なライセンスはSIG Essentials以上が必要と認識に相違ないでしょうか？	ご認識の通りです。
検討にあたり、ライセンス体系などの料金体系を教えてほしい（定価でOKです）	パートナー様、もしくは担当のCisco営業までご連絡頂きますようお願い致します。
Umblellaの新パッケージの比較をわかりやすく説明した資料がありましたら、共有いただけないでしょか。	本資料もしくは下記をご参照ください。 https://www.cisco.com/c/dam/global/ja_jp/products/collateral/security/umbrella/umbrella-pack-comparison-ds.pdf https://www.cisco.com/c/m/ja_jp/umbrella/packages.html
固有名詞の解説が欲しい	下記Blogにいくつか用語に関する説明が掲載されておりますので是非ご参照ください。 https://gblogs.cisco.com/jp/2020/02/cybersecurity-terms-and-threats-you-need-to-know-in-2020/