

CISCO

SECURE ざっくりリシリーズ

ざっくり Umbrella

SIG

(Secure Internet Gateway)

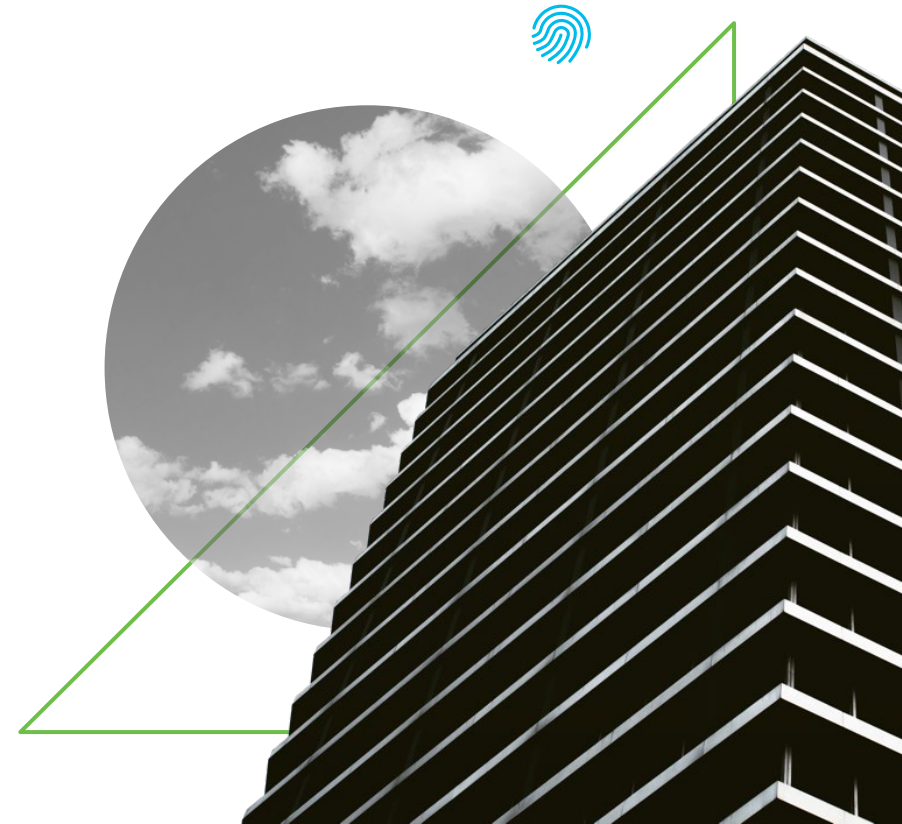


The bridge to possible



# Agenda

- はじめに
- 用語集
- Umbrella SIGとは
- Umbrella SIGが必要となる背景と課題
- Umbrella SIGで解決できること
- Umbrella全体像
- Umbrella SIG主要機能紹介
  - DNS
  - Firewall/IPS
  - SWG
  - CASB/DLP
  - Remote Access as a Service
- 展開パターン
- ライセンス情報
- 第三者機関評価
- 事例
- 参考リンク集



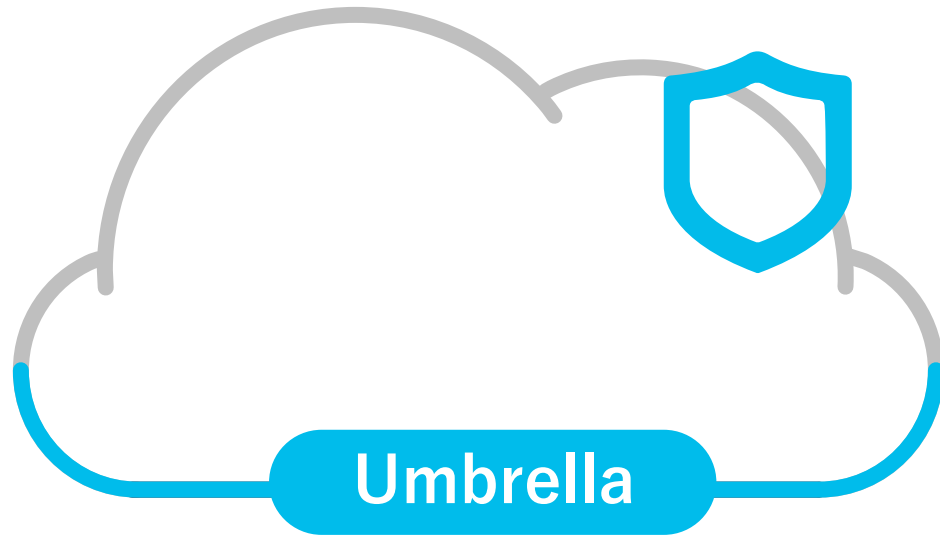
# はじめに

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

# 用語集

用語	概要
SASE (Secure Access Service Edge)	ガートナーが定義した、リモートワークの普及とIaaS/SaaS利用の加速でインターネットやクラウドが中心となるアーキテクチャ対応するセキュリティとネットワークのフレームワーク。企業内境界セキュリティだと各所ボトルネックになり業務に影響が出るため、クラウドサービスとしてセキュリティを統合、シンプルな運用が求められる。
Umbrella	Cisco Umbrella はDNS の名前解決を利用してインターネット上の脅威からユーザを最前線で防御するDNSセキュリティを始め、ウェブアクセスを守るセキュアウェブゲートウェイ、クラウドFirewall、CASB等の機能を統合してクラウドで提供するセキュリティ製品。
Umbrella DNS	Umbrellaの成り立ちであるDNS機能の利用のみを指す場合Umbrella DNSと明記されることがある。ライセンスもDNSとSIGで分かれている。
Umbrella SIG	Umbrella DNSに対してUmbrellaのDNS以外の全機能を含む導入の場合Umbrella SIG(Secure Internet Gateway)と明記されることがある。ライセンスもDNSとSIGで分かれている。
Cisco Plus Secure Connect	UmbrellaをベースにしたRemote Access as a Serviceを指す。
CASB	ガートナーが定義した情報セキュリティコンセプトの一つでCloud Access Security Brokerの略。複数のクラウドサービスに対し一貫性のある可視化、制御を行う。

# Cisco Umbrella SIGとは



Cisco Umbrella はDNS の名前解決を利用してインターネット上の脅威からユーザを最前線で防御するDNSセキュリティを始め、ウェブアクセスを守るセキュアウェブゲートウェイ・Firewall・CASB等の機能を統合した[クラウド提供型のSecure Internet Gateway\(SIG\)](#)です。

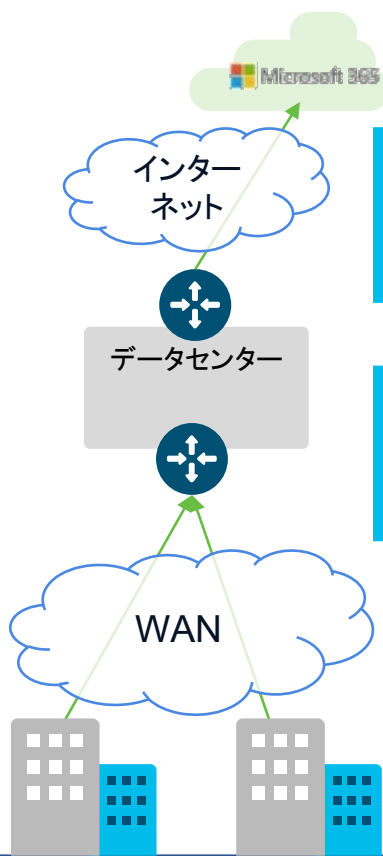
本社、拠点、外出先などの場所、VPN の ON/OFF を問わず、あらゆるユーザとデバイスを保護し、導入も迅速かつ簡単です。

- ✓ Cisco Umbrella はCiscoのSASEソリューションの中核を担う製品です。
- ✓ Umbrellaの成り立ちであり広く実績のあるDNSセキュリティとその他の機能を分けてUmbrella DNS(DNS機能のみ)、Umbrella SIG(すべての機能含む)と記載されることもあります。ライセンスもDNSとSIGで分かれています。

# 複雑化するWAN全体管理の煩雑化

過去

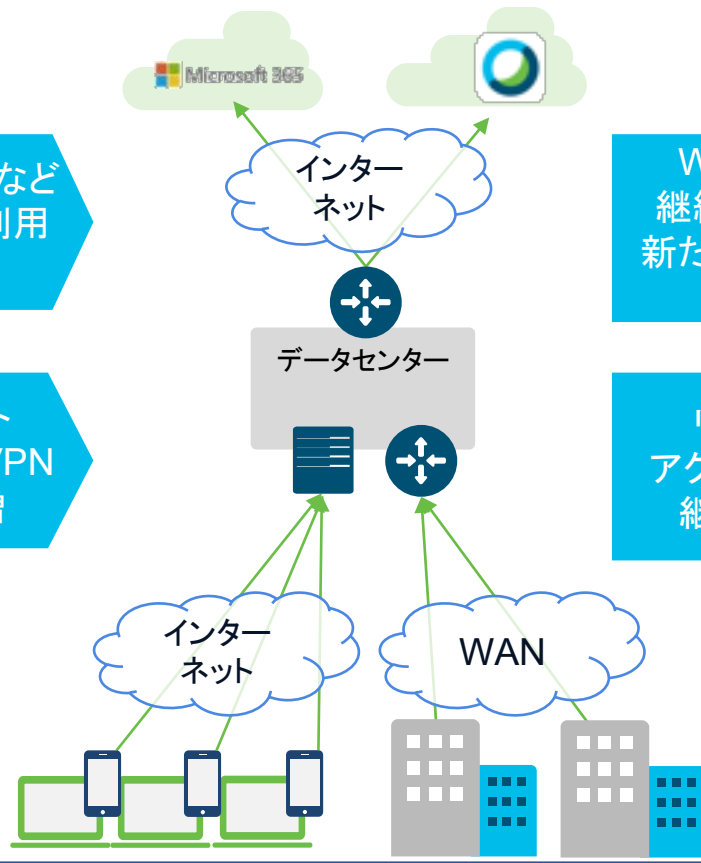
データセンターに集約  
一部をインターネットへ



オフィス

現在

リモートワークの急増  
クラウド利用の拡大

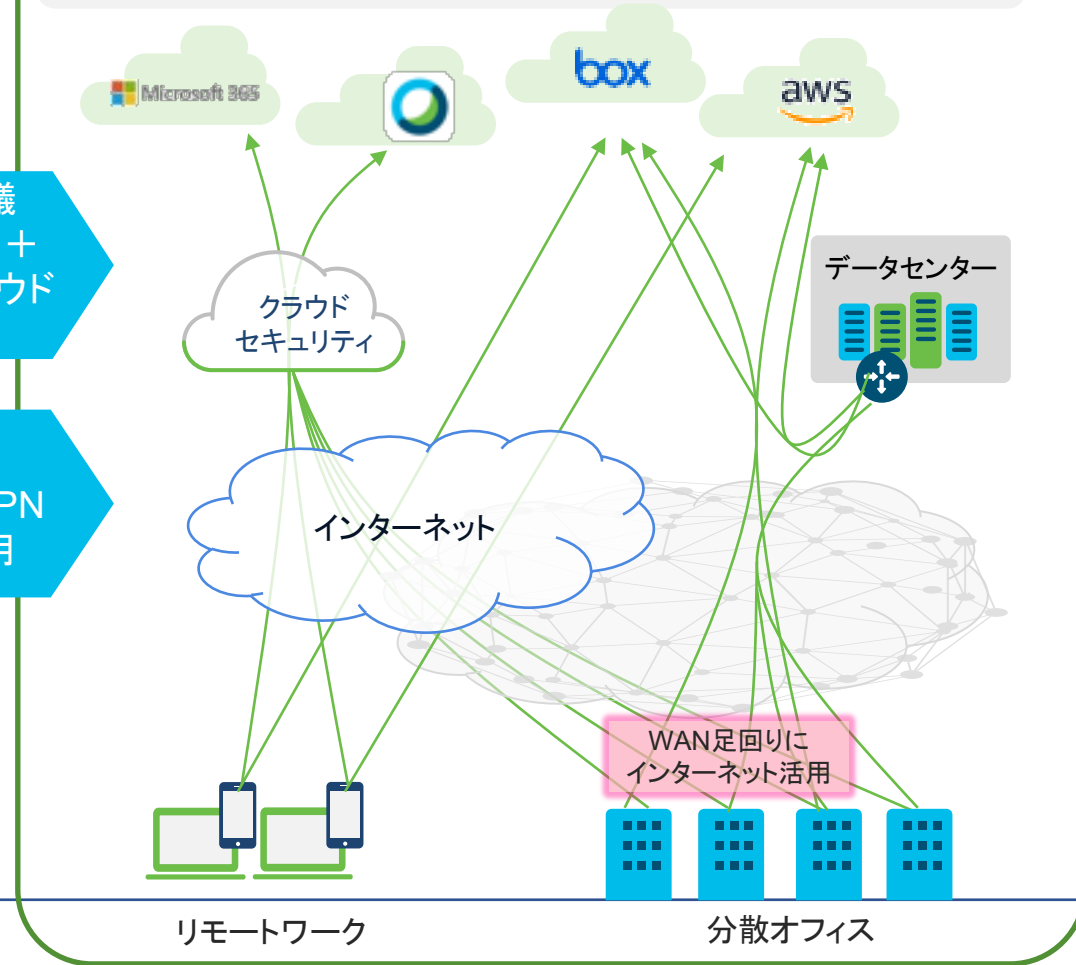


リモートワーク

オフィス

今後

ハイブリッドワークスタイルへの進化  
さらなるクラウド利用、インターネット回線活用



リモートワーク

分散オフィス

Web会議など  
クラウド利用  
急増

リモート  
アクセスVPN  
の急増

Web会議  
継続利用 +  
新たなクラウド  
増加

リモート  
アクセスVPN  
継続利用

オンプレ、IaaS、SaaSのリソースを柔軟に使うためには従来のWANと異なる考え方が必要

# (参考) SASE

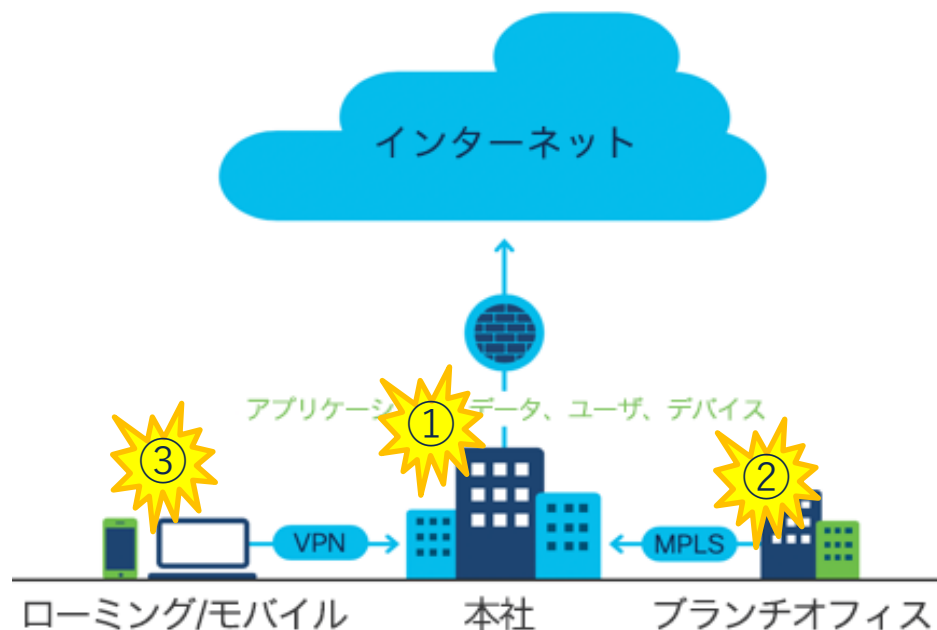
## Secure Access Secure Edge

- Gartner が発表した新しいネットワークとセキュリティのフレームワーク
- インターネット中心となる新しいアーキテクチャに対応してネットワークとセキュリティの機能を包括的にクラウドから提供するモデル
- ネットワークとセキュリティの管理負荷の低減、エンドユーザーの利便性の向上を目指す
- セキュリティ：ハイブリッドクラウド時代に最適なセキュリティをクラウドで実装
- ネットワーク：社内外どこからのアクセスも最適化

CiscoのSASEは  
セキュリティをUmbrella SIGが、  
ネットワークをCisco SD-WANが担っています



# Umbrella SIGが必要となる背景と課題



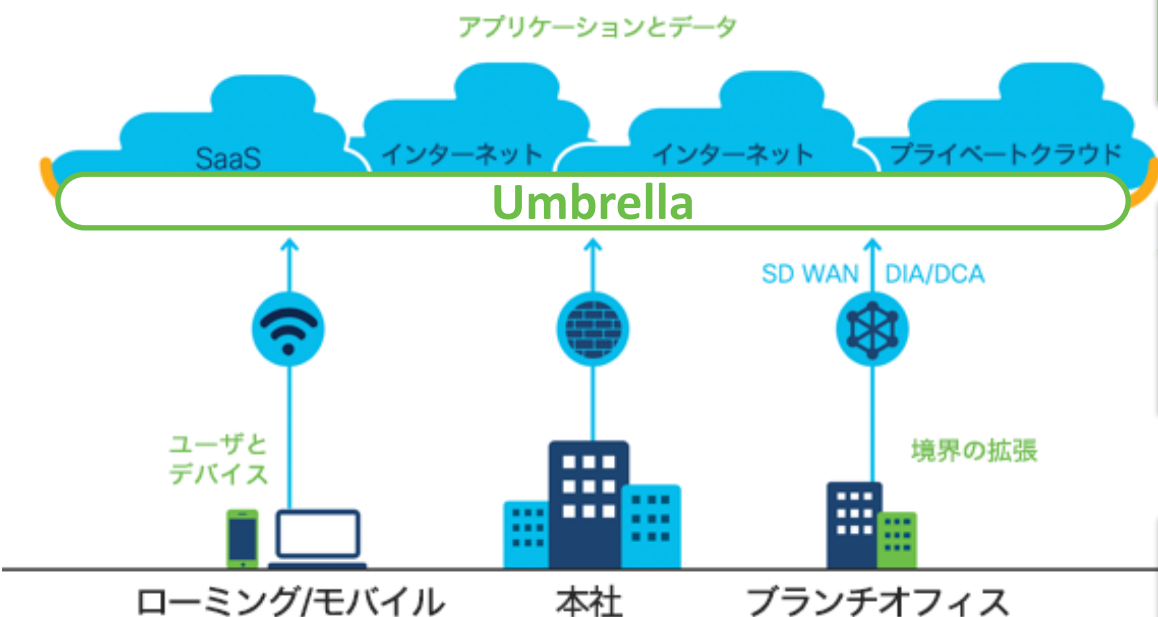
①. データセンターに集約されたインターネットアクセスの際に通るFirewall・IPSやProxyがボトルネックに必要なクラウドアプリケーションの活用が行えず従業員の業務効率低下を招く恐れ

②. インターネットをデータセンタ集約から拠点での直接利用に移行の際、拠点ごとにセキュリティ機器設置でバラバラなセキュリティポリシー、管理負荷の大幅な増大も

③. VPN未接続での業務、VPNレス化でリモートワーク端末でのセキュリティ対策漏れが懸念となる



# Umbrella SIGで解決できる課題



①. Firewall・IPSやProxyをUmbrellaでクラウド実装、既設回線の有効活用やダイレクトインターネットアクセスと合わせて\*、共通のセキュリティポリシーを実装しつつボトルネックを解消。クラウドアプリケーションを活用した従業員の効率的な働き方を実現

②. Umbrellaで各拠点に統一したセキュリティポリシーを実装、統合管理で負荷低減

③. ネットワークにつながると自動的に有効に。VPN無効時も端末のインターネットアクセスをUmbrellaで保護

# Umbrella SIGの主要機能



# Umbrella SIG

## 主要機能

- ✓ DNS
- ✓ Firewall
- ✓ IPS
- ✓ セキュアウェブゲートウェイ
- ✓ CASB
- ✓ Remote Access as a Service  
(Cisco Plus Secure Connect)

# DNSセキュリティ

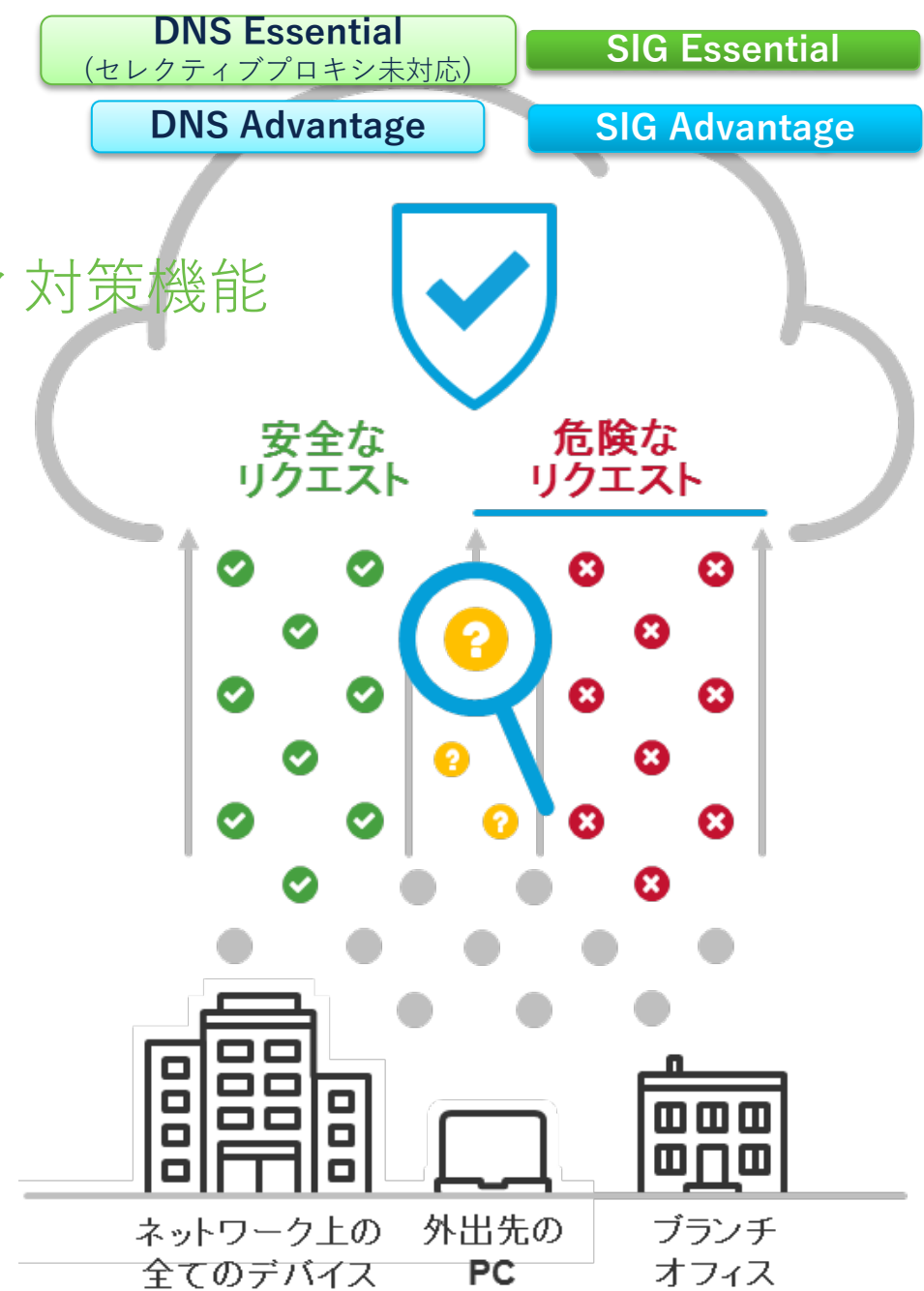
DNSの名前解決を利用した全く新しいセキュリティ対策機能

## Cisco Umbrella DNS Security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 (セレクトティブプロキシ機能)
  - 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

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public



# 参考：セレクトティブ プロキシとフルプロキシ比較

\* フルプロキシは後述のセキュアウェブゲートウェイを指します

## セレクトティブ 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
- ・運用負担が少ない

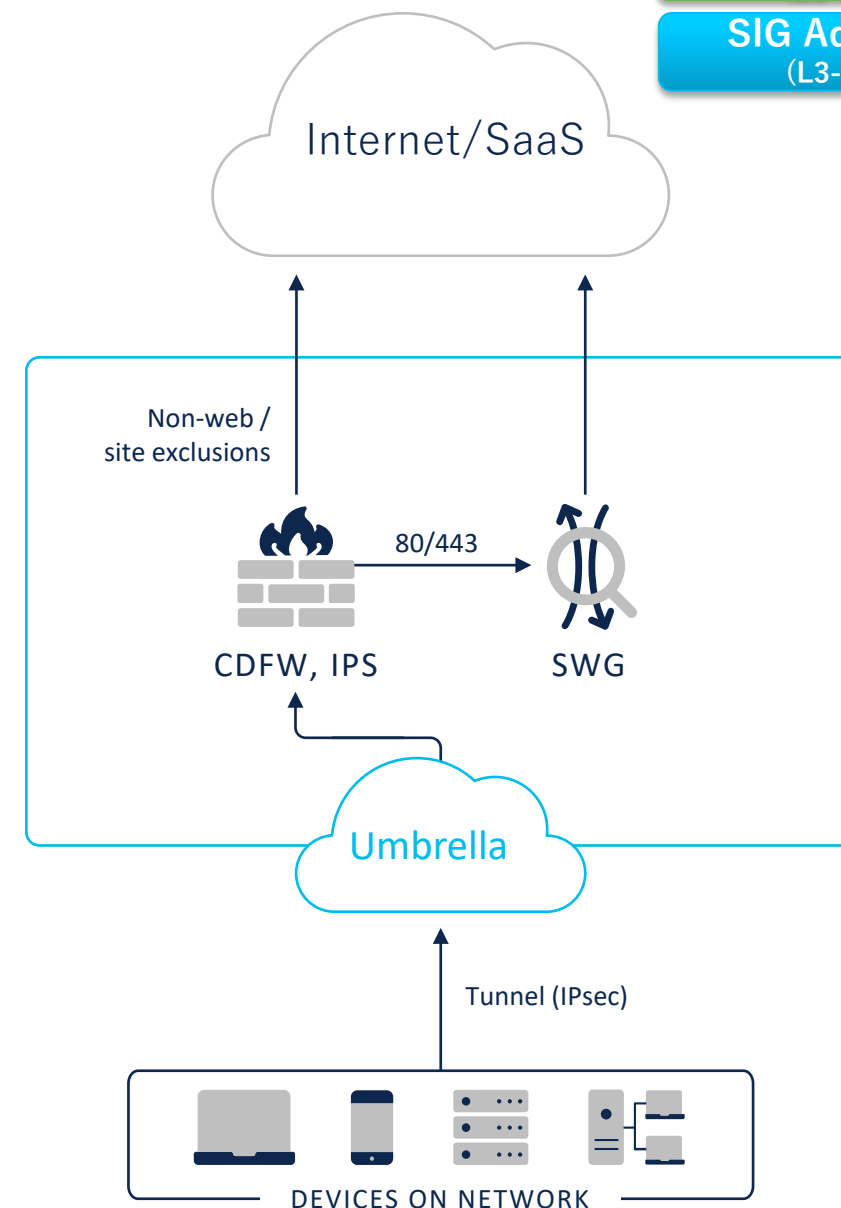
## フルプロキシのメリット

- ・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

# Firewall

- クライアントからのすべてのトラフィックを Umbrella にトンネリング
- IPsecトンネルの終端処理が必要
- リスクの高いアプリケーションやプロトコルをブロック（レイヤー7のアプリケーションの可視化と制御）
- IP、ポート、プロトコル、アプリケーションのルールを一元的に管理（レイヤ3、4、7）
- Webトラフィック（ポート80/443）をセキュアなWebゲートウェイに転送



# IPS

## 機能

- Umbrella のファイアウォールによるクライアントからのトラフィック保護を強化
- シグネチャベースの検知機能（Snort 3）により、ネットワークのトラフィックフローを検証し、脆弱性の悪用を防止
- マルウェア、ボットネット、フィッシングなどの検知/ブロック機能を追加
- Cisco Talos の40,000以上のシグネチャ（現在も増加中）を活用して、脅威をリアルタイムに検出し、相関させることが可能

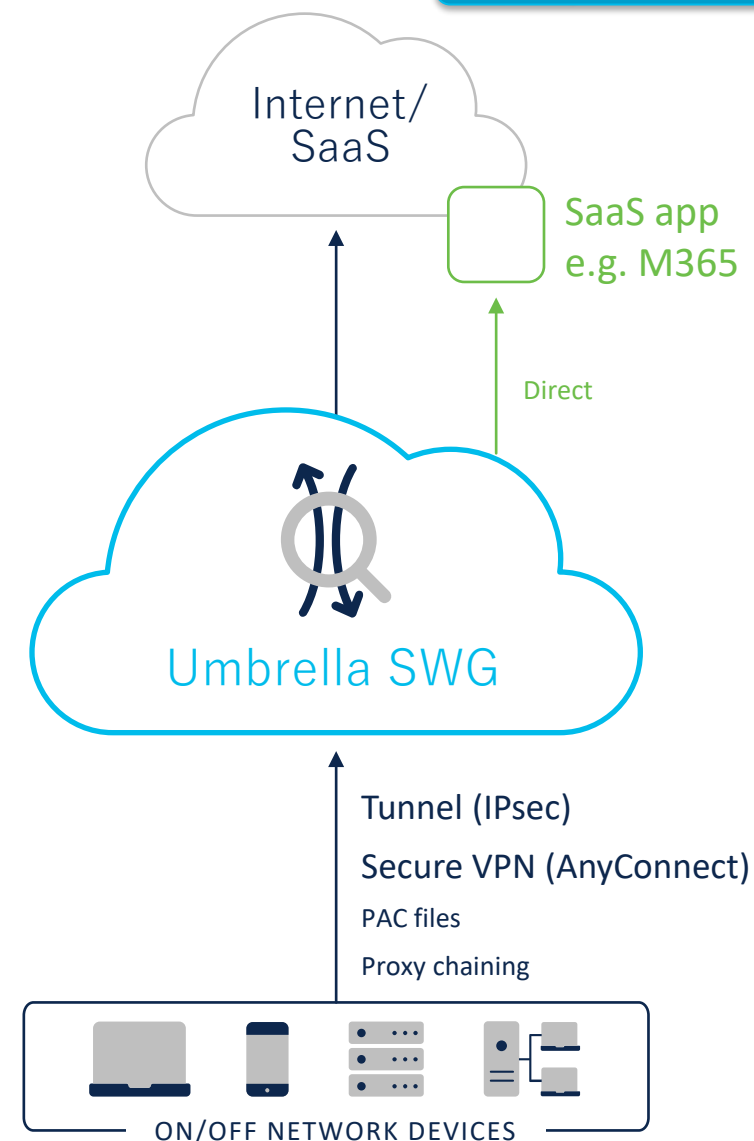
## 効果

- ✓ Umbrellaの統一されたダッシュボードによる管理の簡素化
- ✓ スケーラブルなクラウドコンピュートリソースを使用することで、アプライアンスの容量に関する懸念を払拭
- ✓ 業界で最も効果的な脅威インテリジェンスにより、より多くの脅威を阻止
- ✓ 脆弱性の悪用を検知/ブロック

# セキュアウェブゲートウェイ

## フルプロキシ機能

- マルウェアスキャンには2つのアンチウイルスエンジンとセキュアエンドポイント (AMP) ルックアップを搭載
- ファイルタイプコントロール
- 完全または選択的な SSL 復号化
- コンテンツ カテゴリまたは URL ベースのフィルタリング
- セキュア・マルウェア・アナリティクス (Threat Grid) によるファイルのサンドボックス解析
- アプリの可視化ときめ細かなコントロール\*
- 完全なURLレベルのレポート





**SIG Essential**  
(クラウドマルウェア検知  
(アプリ数2))

**SIG Advantage**  
(クラウドマルウェア検知  
(サポート済みの全アプリ)、  
インラインDLP)

# CASB(Cloud Access Security Broker)

## アウトオブバンド (API) 型

### Umbrella

- 契約クラウド内のマルウェア検知

### Cloudlock \*CASB専用製品

- ユーザーの行動監視/アラート
- クラウドストレージポリシーの適用
- **DLP** の検疫および失効アクション  
(アウトオブバンド)
- **OAuth** アプリ：可視化と制御

## インライン/プロキシ型

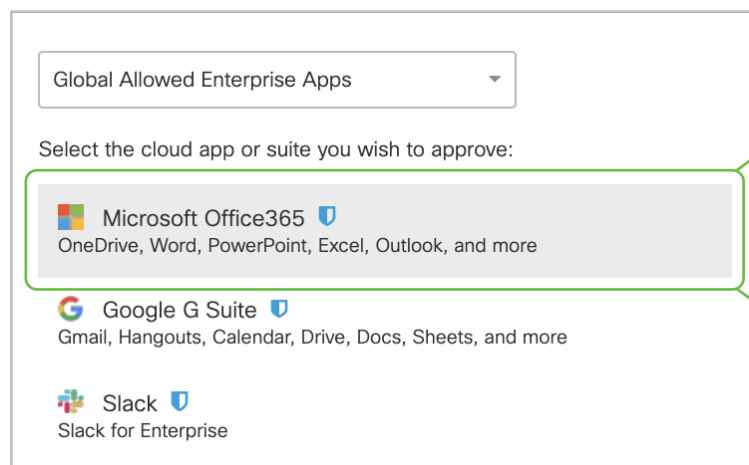
### Umbrella

- アプリの可視化とブロック
- 高度なアプリ制御
  - アップロードのブロック  
(Dropbox/Boxなど)
  - 添付ファイルのブロック  
(ウェブメール等)
- テナントコントロール
- インライン **DLP**

# CASB

## テナント制御

特定のSaaSアプリケーションに対して利用できるテナントを制限



✓ cisco.com (会社契約)

✗ Deb Smith (個人契約)

✗ Bob Jones (個人契約)

### 主なユースケース

セキュリティ  
機密データが承認されたクラウド・アプリケーションのインスタンスで作成・保存されることを担保

生産性  
コアな SaaS アプリケーションの企業インスタンスへのアクセスのみを提供

# CASB

## インライン型 DLP(Data Loss Prevention)

接続性、ルーティング、SSL 復号化に SWG を活用

堅牢な DLP 分類

- 80 以上の内蔵データ分類
- カスタムキーワード

柔軟な DLP ポリシー

- 定義されたデータ分類を利用し、特定のアイデンティティと宛先に対して適用

レポートニング

- ID、ファイル名、宛先、分類、パターンマッチ、抜粋、トリガールールなどわかりやすく表示
- Umbrella に統合されたユーザ インタフェース

The screenshot displays the Cisco Umbrella DLP Data Classification interface. It shows a table with columns for Detected, Identity, Name, Destination, Classification, and Action. The table lists several detected events, all classified as Confidential Classification and blocked.

Detected	Identity	Name	Destination	Classification	Action
Aug 13, 2020 at 3:31 PM	ProxyChain	Content	app-tester-workspace.slac...	1 Match Confidential Classification	Block
Aug 13, 2020 at 3:22 PM	ProxyChain	Content	app-tester-workspace.slac...	1 Match Confidential Classification	Block
Aug 13, 2020 at 3:22 PM	ProxyChain	Content	app-tester-workspace.slac...	1 Match Confidential Classification	Block
Aug 13, 2020 at 3:08 PM	ProxyChain	Content	app-tester-workspace.slac...	1 Match Confidential Classification	Block
Aug 13, 2020 at 3:08 PM	ProxyChain	Content	app-tester-workspace.slac...	1 Match Confidential Classification	Block
Aug 13, 2020 at 3:08 PM	ProxyChain	test.pdf	files.slack.com	1 Match Confidential Classification	Block
Aug 13, 2020 at 3:08 PM	ProxyChain	test.pdf	files.slack.com	1 Match Confidential Classification	Block

2021年7月リリース予定

# ☀️(参考) アプリケーション可視化と制御

エンフォースメントポイントを超えた広がり

## DNS レイヤ セキュリティ

- 組織内で使用されているクラウドアプリケーションを可視化
- 潜在的なリスクを特定し、特定のアプリをブロック (16Kアプリを識別可能)

## クラウド提供型ファイアウォール

レイヤ7アプリケーション可視化と制御

- 可視化と制御を拡張:
  - 非ウェブ (非HTTP/S) トラフィック
  - ハードコードされたIPアドレスを使用し、DNSルックアップを行わないアプリ
  - シグネチャベースの検出 (IP、ドメイン、URLに基づかない) が検出およびブロックに必要なアプリ

## セキュアウェブゲートウェイ

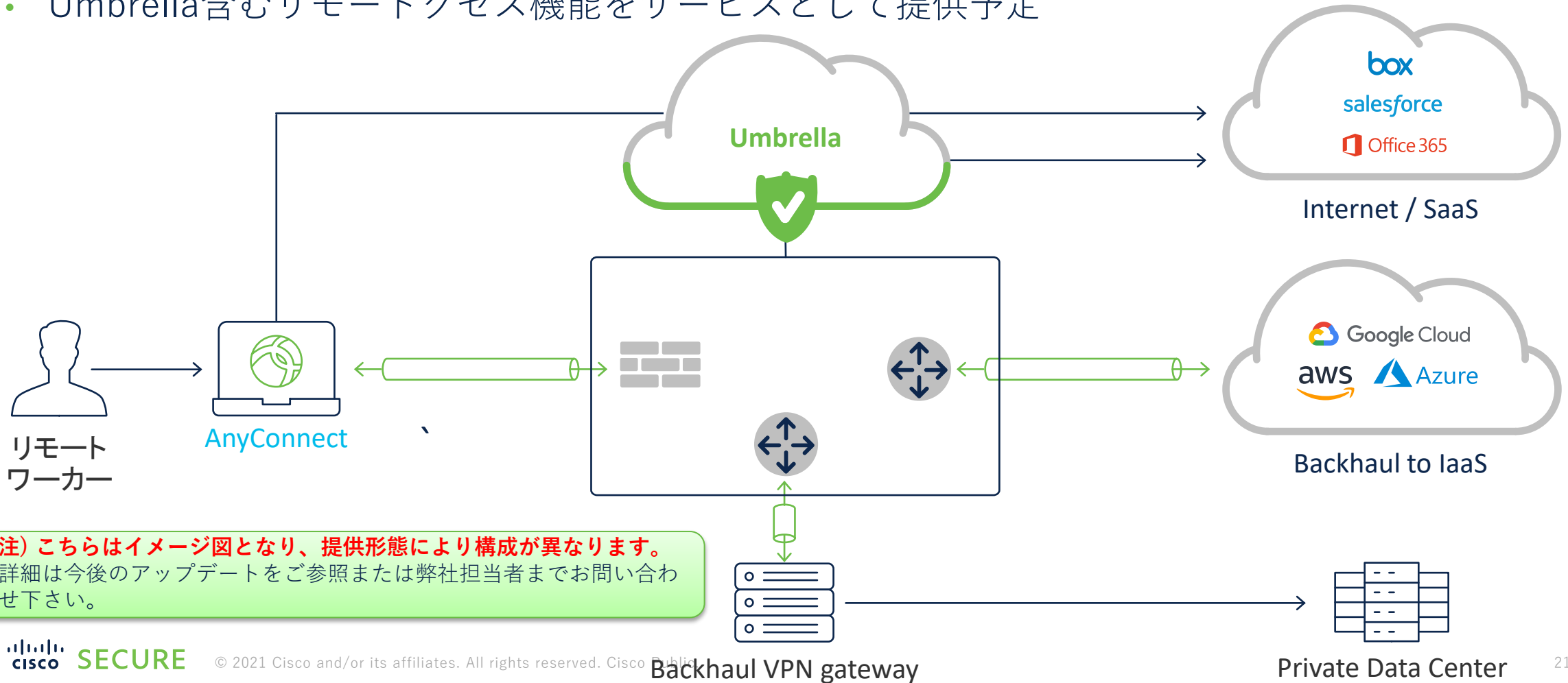
HTTP/S (ポート80/443) を介したウェブアプリのきめ細かな制御:

- クラウドストレージアプリへのアップロードをブロック
- ソーシャルメディアアプリへの投稿/共有のブロック
- ウェブメールアプリへの添付ファイルのブロック
- テナント制限

# Remote Access as a Service

## Cisco Plus Secure Connect / Secure Connect Plus

- Umbrella含むリモートアクセス機能をサービスとして提供予定

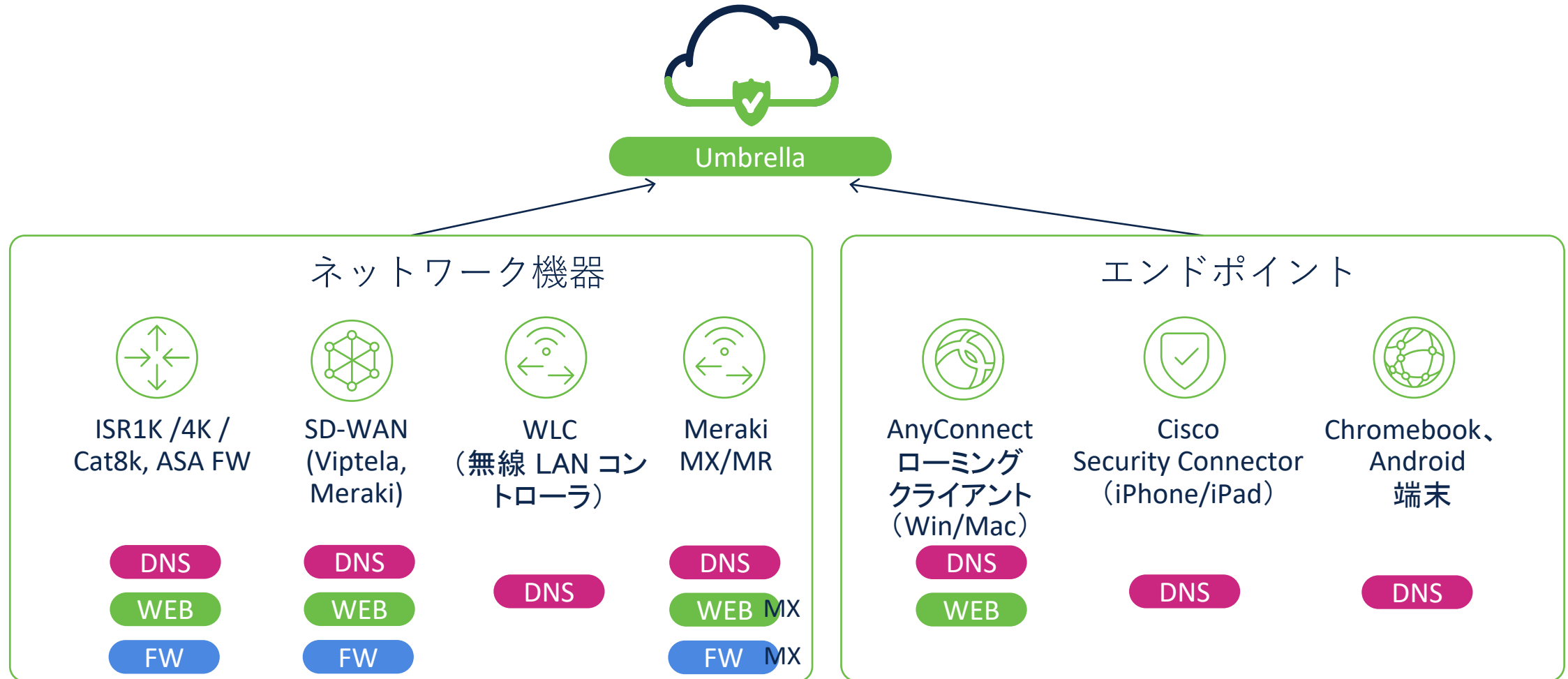


✓ 注) こちらはイメージ図となり、提供形態により構成が異なります。  
 ✓ 詳細は今後のアップデートをご参照または弊社担当者までお問い合わせ下さい。

# 展開パターン

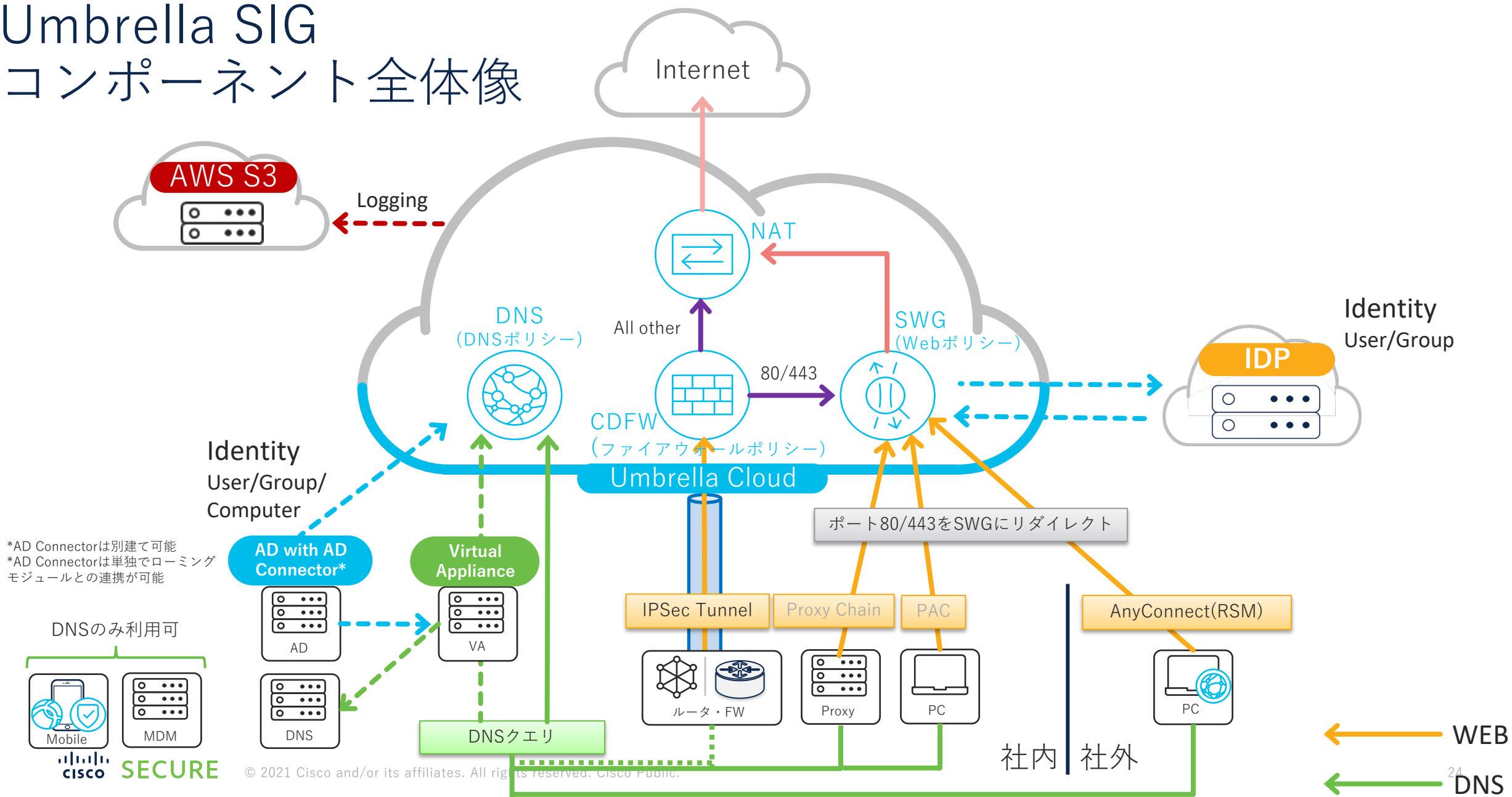


# Cisco Umbrella は様々な接続形態に一つで対応



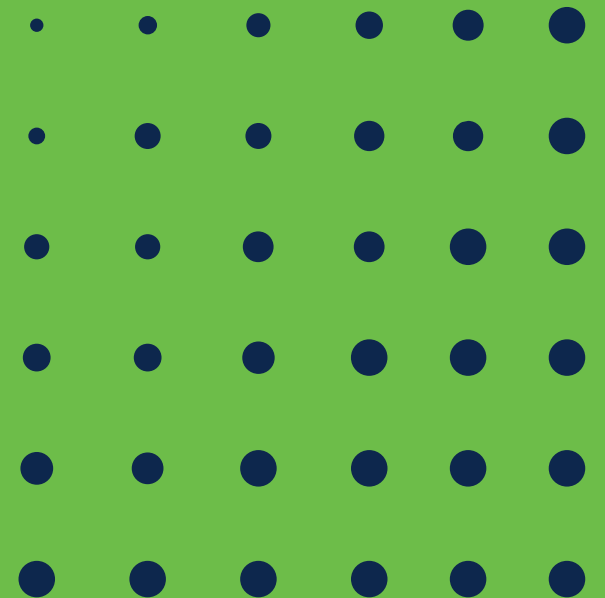
このネットワーク内のユーザは Umbrella の防御が適用される 企業ネットワークの外においても Umbrella の防御を適用

# Umbrella SIG コンポーネント全体像





# ライセンス情報

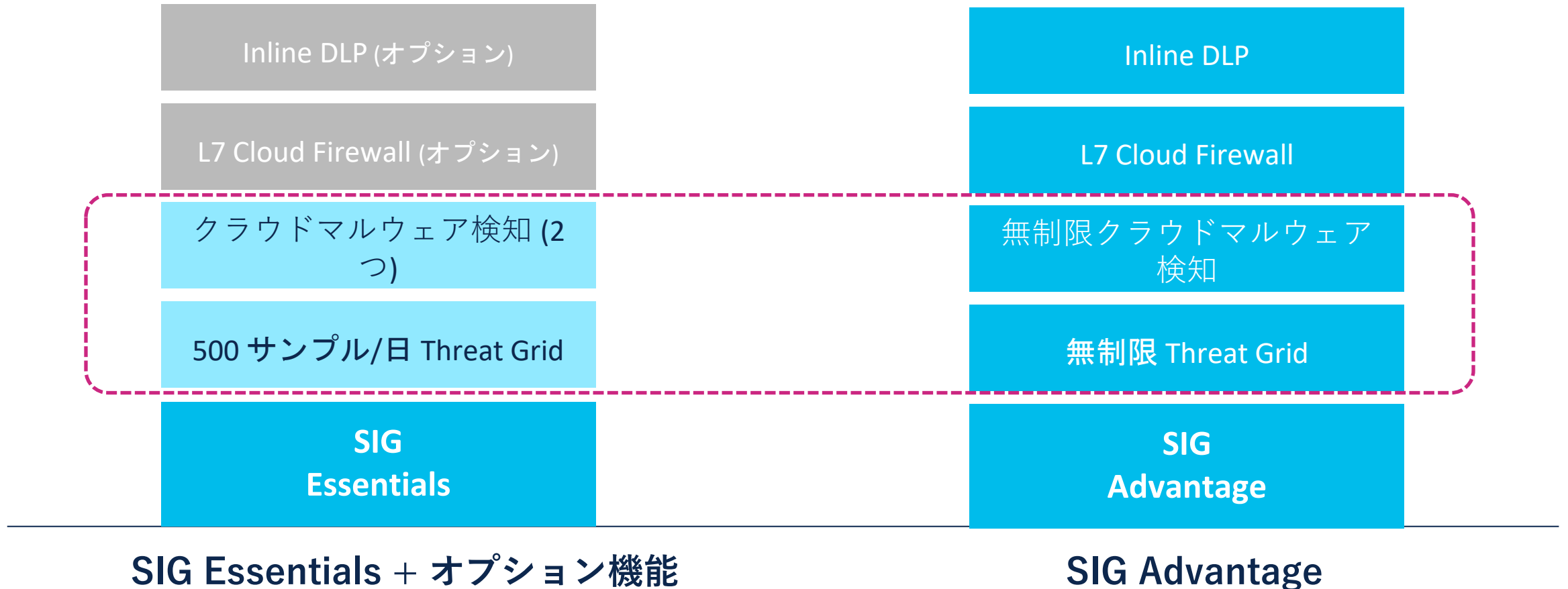


# Umbrellaパッケージ比較表詳細

	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	○	○	○	○
Cisco SecureX の提供	○	○	○	○
S3 ログ管理	○	○	○	○
Multi-Org コンソール	○	○	○	○
Umbrella DNS セキュリティ *	○	○	○	○
Umbrella DNS セキュリティ (モバイル端末向け) *	○	○	○	○
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	—	○ (Proxy 利用時)	○	○
ファイル インスペクション - AMP (含: 遡及的アラート)	—	○ (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)	○	○
Investigate コンソール + オン・デマンド エンフォースメント API	オプション	○	○	○
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)
インライン 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

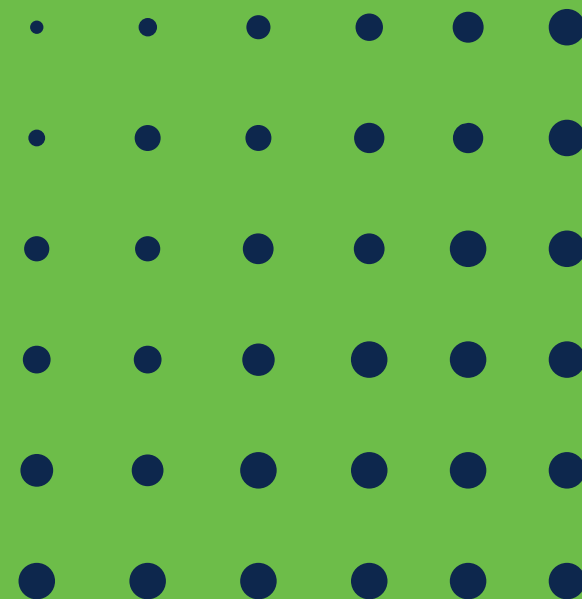
\*Domain Filtering, Security Blocking, App Discovery & Blocking, Network and Branch Protection

# (参考) SIG AdvantageとSIG Essentialの違い



Threat Grid サンドボックスおよびクラウドマルウェア検知のニーズがある案件では、SIG Advantage による提案を推奨

# 第三者機関評価 事例 参考リンク集



# 第三者 (AV-TEST) による 検証結果(2020/10)



- 2020年9～10月に AV-TEST にて実施  
(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

- 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

## DNS レイヤ テスト

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%

## ウェブレイヤ テスト

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	SIG Essentials	96.39%	0.65%
Zscaler Internet Access	Transformation	89.67%	0.69%
Palo Alto Networks Prisma Access	Prisma Access for Mobile Users	73.15%	1.29%
Netskope Secure Web Gateway	NG-SWG	61.90%	4.53%
Akamai Enterprise Threat Protector	Advanced Threat	58.43%	1.89%



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

# 第三者評価 Radicati Corporate Web Security - Market Quadrant 2021

## シスコの強み

- シスコの Web セキュリティソリューションは、アプライアンス、クラウドベース、ネットワーク統合、またはハイブリッドソリューションとして導入できる幅広いポートフォリオを提供
- アンブレラとセキュア ウェブ アプライアンスのライセンスを柔軟に変更できるため、クラウドへの移行が容易で、ハイブリッドシナリオにも対応
- Cisco Umbrella は、通常は別々のソリューション（通常は異なるベンダーのもの）が必要となる幅広い Web セキュリティ機能を単一のプラットフォームで提供
- 多くのオンプレミス機器にトラフィック・リダイレクション機能を統合

<https://learn-umbrella.cisco.com/analyst-report-library/the-radicati-groups-corporate-web-security-market-quadrant-2021>

Corporate Web Security - Market Quadrant 2021

## MARKET QUADRANT – CORPORATE WEB SECURITY

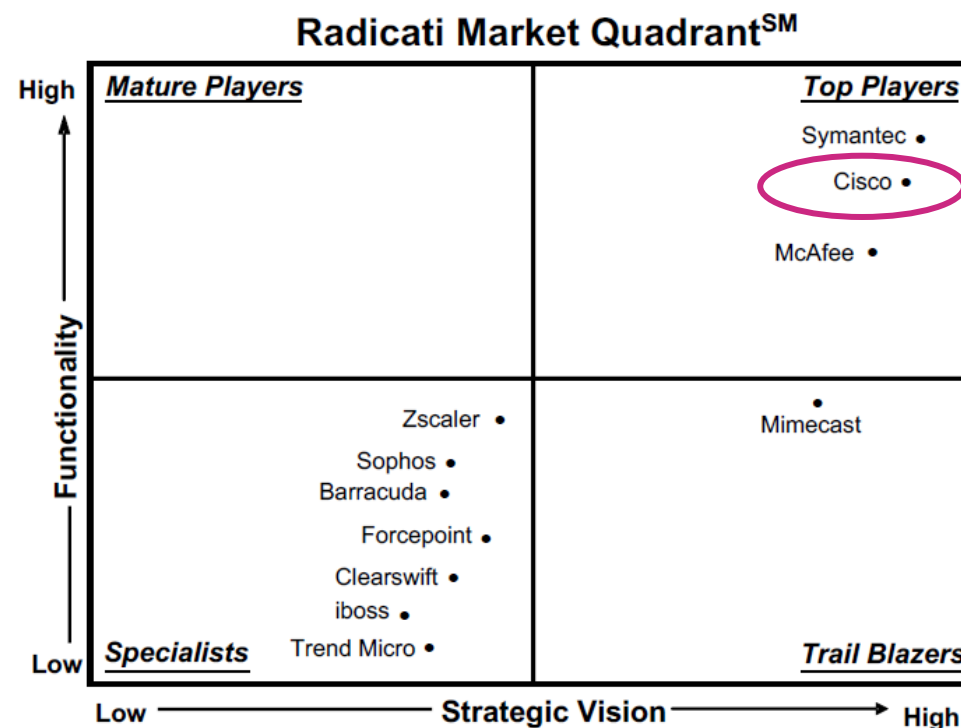


Figure 3: Corporate Web Security Market Quadrant, 2021\*

# 導入事例

- 国内で民間・公共共に多数事例あり

シスコ セキュリティ導入事例

## 株式会社北國銀行

全拠点からのローカルブレイクアウトと  
エンドポイントセキュリティ強化により  
クラウド時代のワークスタイル環境を実現



**製品 & サービス**

- Cisco SD-WAN
- Cisco Umbrella
- Cisco AnyConnect
- Cisco ASA

**課題**

- 事業環境変化やテクノロジー進化を捉え、銀行特有のネットワークの姿を本格的に見直ししたい
- クラウドをフル活用するためには全社員が安全にインターネットに接続できる環境が求められる
- 増大するトラフィックに備え、センター集中型のネットワークとセキュリティから脱却したい

**ソリューション**

- Cisco SD-WAN により全拠点からのローカルブレイクアウトを実現
- 利便性の低い VDI から FAT クライアント化し、エンドポイントセキュリティに Cisco Umbrella を導入、AnyConnect VPN とも連携
- PoC 実施により実用性を検証、プロジェクトを早期に立ち上げ

**課題**

北陸地方を代表する地方銀行である株式会社北國銀行は、他行に先駆けた積極的な ICT 利活用企業としても知られています。今回、同行はクラウドサービスのフル活用が可能なインターネットネイティブなネットワークのあるべき姿を目指し、Cisco SD-WAN と Umbrella を導入。全拠点から直接インターネットに接続するローカルブレイクアウトおよび、DNS レイヤによるエンドポイントセキュリティの強化により、どこからでもシンプルに安全かつ利便性の高い、クラウド時代のワークスタイル環境を実現しました。

**クラウドをフル活用するインターネットネイティブなネットワークの実現には SD-WAN と Umbrella によるエンドポイントセキュリティ強化が最適と考えました。**

——株式会社北國銀行システム部システム企画課 新谷直樹 氏

北陸地方を代表する地方銀行である株式会社北國銀行。石川県金沢市を本拠地に、北陸三県に105店舗および東京、大阪、愛知、シンガポールにも支店を展開しています。2014年には全社にシンククライアント端末を展開、2021年には国内初となるパブリッククラウドを活用したフルバンキングシステム稼働が計画中であるなど、積極的な ICT 利活用企業としても知られています。

今回のプロジェクトで目指した方向性を、システム部システム企画課長 新谷直樹氏は「クラウド

シスコ Umbrella 導入事例

## 学校法人早稲田大学

ソフトの不正利用防止、常時 SSL 化対策として  
セキュア インターネットゲートウェイを全学に展開



**製品 & サービス**

- Cisco Umbrella

**課題**

- イリーガルサイトからの不正ソフトウェアやアカウント入手を防止したい
- 常時 SSL 化に伴う暗号化通信のセキュリティに不安

**ソリューション**

- DNS レイヤセキュリティで危険サイトへのアクセスを未然にブロック、SSL 通信の検査も実現
- クラウドサービスならではの導入、展開のしやすさも評価

**結果 ~ 今後**

- 短時間による過剰なブロックもなく、運用負担もかからない
- 計画中のキャンパス SD-WAN セキュリティとしても期待

創立 150 周年を迎える 2032 年のあるべき姿をイメージして 2012 年に策定した中長期計画「Waseda Vision 150」を継承、さらに進化させる新たなスローガンとして「世界で輝く WASEDA」を掲げ、その実現に向けさまざまなトランスフォーメーションを実行中の早稲田大学。外国人学生、海外派遣学生ともに国内の大学でトップクラスの同大学は、多様化する学びの場に対応する新たなセキュリティとして Cisco Umbrella を導入。ソフトウェアやアカウント不正利用の温床となるイリーガルサイトへのアクセス防止や、常時 SSL 化にも適合した DNS レイヤセキュリティを全学展開しました。

**多様化、分散化するキャンパスにおいて、場所やデバイスを問わずにセキュリティを確保できる Cisco Umbrella の意義は、非常に大きいと感じています。**

——早稲田大学 情報企画部 橋 仁志 氏

早稲田大学は、創立 150 周年を迎える 2032 年を見据えた中長期計画「Waseda Vision 150」に基づき、情報基盤の整備を進めています。早稲田大学 情報企画部 事務副部長の高橋智広氏は「多様な学びの場の提供」をキーワードに、効率化だけでなく新たな価値の創出を ICT の活用により実現していきたいと考えています。本年 4 月に LMS (Learning Management System) を刷新するなど、ポストコロナに向けた安全、安心な新たな学びの基盤創りに注力しています。」と語ります。

シスコ セキュリティ導入事例

## アイペット損害保険株式会社

巧妙化する脅威に対し  
セキュア インターネット ゲートウェイを導入  
サイバー対策強化とクラウドのガバナンス強化に取り組む



**製品 & サービス**

- Cisco Umbrella

**課題**

- 巧妙化するインターネットの脅威に対し、従来の対策では不十分
- 暗号化された通信の可視化は工数とコスト負担が大きい

**ソリューション**

- 脅威インテリジェンスサービスとして Cisco Umbrella に期待
- 圧倒的な検知力とデプロイメントのしやすさを評価
- DNS とフルプロキシによるすべてのインターネット通信を可視化

**結果 ~ 今後**

- 毎月 500 ~ 3,500 件の脅威通信ブロックによるサイバーリスクの低減

取り扱い店舗数、保有契約数などで業界トップクラスの実績を誇るペット保険のリーディングカンパニー、アイペット損害保険株式会社。2004 年の創業以来、「ペットとの共生環境の向上とペット産業の健全な発展を促し、思いのある豊かな社会を創る」を経営理念として成長を続け、2020 年 3 月には保有契約件数 50 万件を突破しました。2020 年 5 月に公表した中期経営計画では、ペット保険事業の持続的な成長に加え、持株会社への移行と事業領域の拡大、デジタルイノベーションの推進などを掲げ、さらなる発展を目指す同社は今回、セキュア インターネット ゲートウェイ Cisco Umbrella を導入。サイバー対策強化とクラウドのガバナンス強化に取り組んでいます。

**シスコのセキュリティは、脅威インテリジェンスのレベルの高さに驚いたと共に、クラウドによる提供と運用上の自動化、統合の思想にも共感しています。**

——アイペット損害保険株式会社 情報システム部 セキュリティチーム シニアテクニカルリーダー 榎本 浩義 氏

# 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 -](#)



# 14日間フリートライアル

- [Umbrella 14日間フリートライアル](#)  
こちらよりぜひお試しください



SECURE