

Cisco Umbrella概要

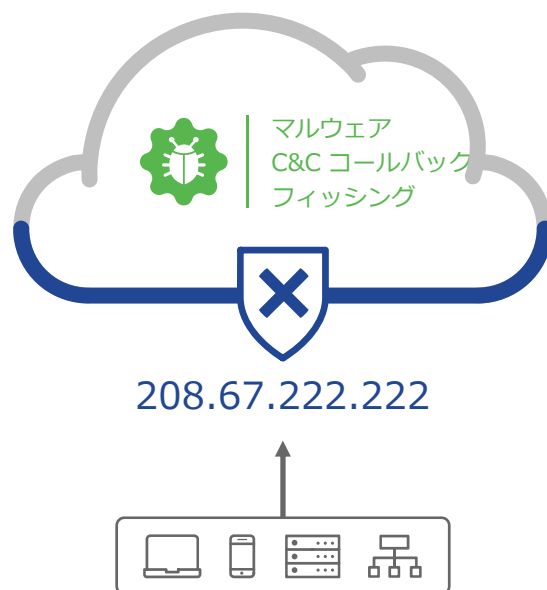
リモートワーク・クラウドサービス活用時代に
向けたセキュリティ対策

2017年6月

株式会社ソリトンシステムズ

Cisco Umbrella

- 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」はDNSの名前解決を利用したセキュリティ対策機能を提供。
 - URLやIPアドレス（例：マルウェアによる接続先IPアドレスの指定）によるフィルタリングやファイルのウイルススキャンにも対応。
 - C&Cサーバへの通信も遮断。
 - 怪しげなリクエストをプロキシで調査。
- 「ユーザーがアクセスしようとしているのがマルウェア配布サイトだったら、名前解決を拒否する」といったアクセス制御が可能。
 - エンドポイントやネットワークに到達する前にマルウェアによる通信を遮断。

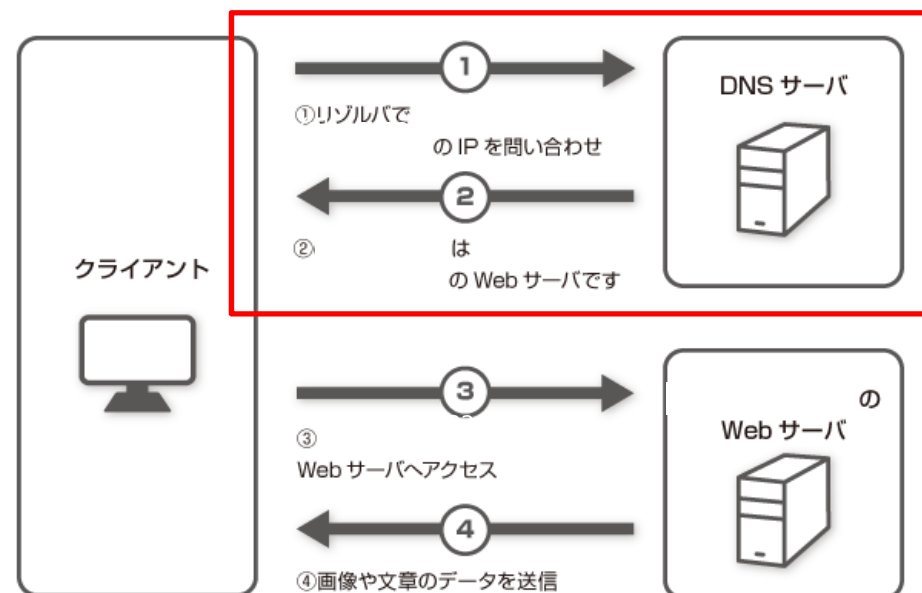
- Yahooのサイトにアクセスする際、どうしますか？

1. ブラウザのアドレスに 118.151.231.231 を打ち込む
2. ブラウザのアドレスに www.yahoo.co.jp を打ち込む

DNS (Domain Name System) は、人が判読可能なコンピューターのホスト名とネットワーク機器で使用する IP アドレスのマッピングを提供します。

DNSの役割

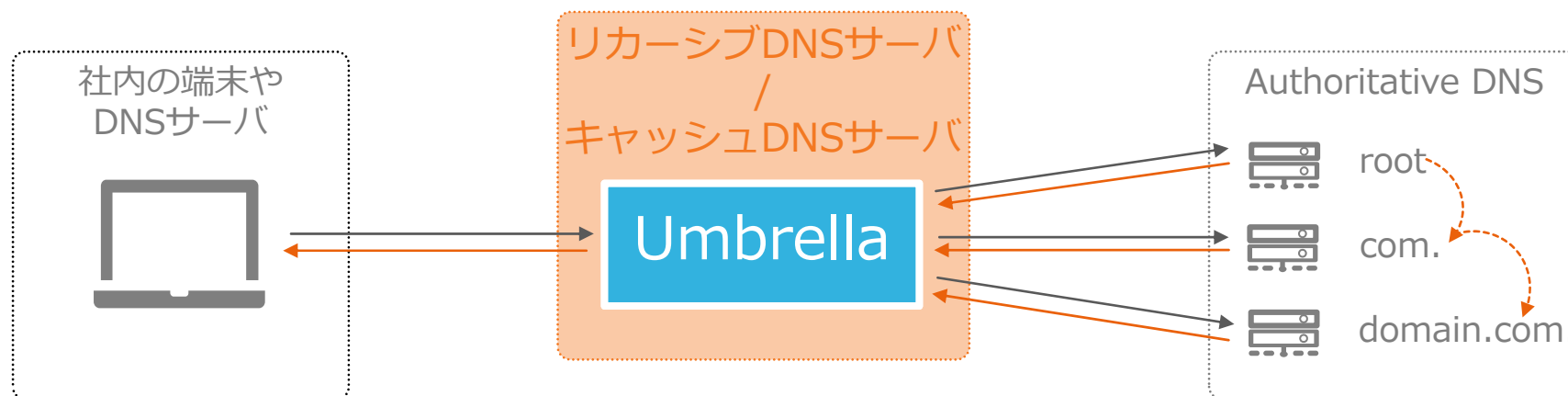
- ドメイン名(yahoo.co.jp)とIPアドレス(118.151.231.231)を結び付け、Webサーバへのアクセスを可能にしているのがDNS



ここが、DNS

これは、Webリクエスト

Cisco UmbrellaはDNS レイヤでセキュリティ機能を提供する画期的なソリューションです



リカーシブDNSとは、端末がDNS問い合わせを行う際に、代理で名前解決（ドメイン名→IPアドレス）を行うことである。

UmbrellaのDNSサーバを使うことにより、名前解決時に悪意のある問い合わせ先の場合は、そのアクセスを遮断する、ということが実行できます。

Cisco Umbrella の仕組み

3) 解析結果に基づき制御



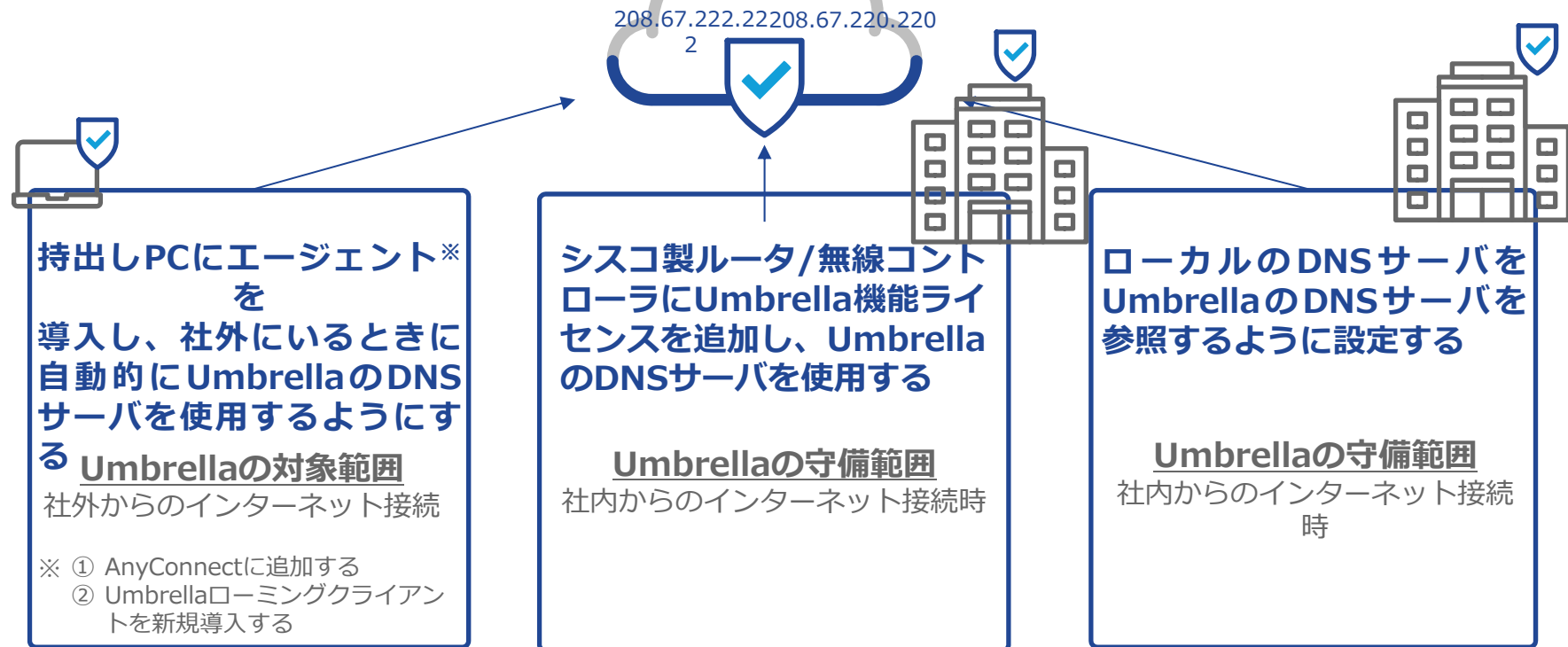
2) Umbrellaによる解析



1) インターネットへの通信が発生 →Umbrellaのサーバへ問合せ



導入パターン Cisco Umbrella



※ IPレイヤでの制御を行うには端末にUmbrellaローミングクライアントがインストールされている必要があります。Umbrella機能が追加されたAnyConnect によるIPレイヤでの制御については今後対応予定です。

UMBRELLAファミリー比較

UMBRELLAファミリ比較	Roaming	Branch	WLAN	Professional	Insights	Platform
Protection						
保護対象ネットワーク	ローミング環境のみ	イントラネットのみ	イントラネットのみ	○両方	○両方	○両方
任意のポートでマルウェア、フィッシング、およびC2コールバックを防止	○	○	○	○	○	○
60のコンテンツカテゴリを使用して許可可能な使用ポリシーを強制	×	○	○	○	○	○
Enforcement						
DNS層で悪質なドメイン要求とIP応答をブロックする	○	○	○	○	○	○
インテリジェントプロキシ: 悪意のあるURLパスをブロックし、IPレイヤで直接IP接続をブロックする	×	×	×	×	○	○
インテリジェントプロキシ: AVエンジンとCiscoAMPを使用したURLおよびファイル検査のプロキシリスクドメイン	×	×	×	×	○*予定	○*予定
サンドボックス: Threat Grid Sample Packでのファイル分析	×	×	×	×	×	○*予定
Visibility						
リアルタイムで全社的な活動の検索とスケジュールされたレポート	○	○	○	○	○	○
ローカルとグローバルの活動を比較して標的とする攻撃を特定する	×	×	×	×	○	○
1800以上のクラウドアプリを分類し、クラウドとIoTの使用リスクを特定	×	×	×	×	×	○
Management						
カスタムブロック/許可リスト、組込ブロックページ、バイパスオプション	許可リストと組込ブロックページ1つ	○	○	○	○	○
内部ネットワークまたはADユーザ/グループごとの施行と可視性	×	内部ネットワーク(AD不可)のみ	SSID、AP、APグループ、ユーザグループごと(AD不可)	×	○	○
Amazon S3バケットと統合したログ保持	×	×	×	×	○	○
Platform package exclusive						
サードパーティのブロックリストを実施/管理するためのAPIベースの統合	×	×	×	×	×	○
Intelligent Console	※オプション					○
Investigate API	※オプション					
Additional Options						
サポートオプション - すべてのパッケージにはオンラインと電子メールのサポートが含まれています	※Basicサポート以外はオプション					
Multi-Org Console - 分散された組織の集中管理	×	×	×	×	※オプション	

Umbrella は以下のようなお客様のニーズに応えます

- 社外から VPN を張らせることを 100% 強制できていない
- (SaaS 等) クラウドへの移行を進めている
- オンプレミス型 Proxy はバージョンアップやサイジングなどが手間
- ブランチや工場等からのダイレクト インターネットアクセスを検討
- グローバル拠点に対するセキュリティ対策を簡単に実施・管理したい
(特に、小規模拠点でセキュリティを適用できていない)
- ランサムウェアを過去経験し対策の必要性を感じている
- セキュリティの実装が不安な IoT 機器おける標的型攻撃対策が必要

価格(税抜標準価格)

- Umbrella Professional

100ユーザー	年額	¥704,640	～
1000ユーザー	年額	¥4,089,600	～

詳細はお問い合わせ下さい。