

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、従来型の対策では不十分
- 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
- クラウドアプリケーションの識別・評価機能を活用したシャドー IT の取組
- 統合運用プラットフォームである Cisco Threat Response を活用した運用効率の向上と自動化

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、潤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、デジタル化の推進などを掲げ、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 蛭本 浩義 氏

課題

事業の成長に伴い全国に拠点と取引先が増え続けるアイペット損害保険は、顧客や代理店に Web サービスを展開し、クラウドやモバイルなど ICT を積極的に活用する IT 環境です。

情報システム部 シニアテクニカルリーダーの蛭本浩義氏は、セキュリティ課題を次のように話します。

「サイバー攻撃手法は日々高度化する中、クラウドサービスがより複雑化し、Web フィルタで分類できない通信が 6 割以上を占めるようになるなど、インターネットを安全に利用することが難しくなっていました。また、プロキシを通らない特殊環境のインターネット通信が存在していたため、すべてのインターネット通信を可視化しコントロールすることもできていませんでした。」
これらの解決策として、脅威インテリジェンスの活用に着目。当初は、複数社の脅威インテリジェンスサービスをピックアップし、POC（概念実証）を実施していました。



アイベ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
蛭本 浩義 様

「実際の攻撃で使われている IP やドメインの情報、いわゆる IoC (Indicator of Compromise) と呼ばれる脅威インテリジェンスはその量と精度が増していて、これを活用したサイバー対策は効果が高く、今後主流の対策の 1 つになると考えていました。特に、Cisco Umbrella はサイバー攻撃の調査で有名な Cisco Talos (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) の脅威インテリジェンスが反映されていることを知り、インテリジェンスの量だけでなく品質にも期待し、シスコの Web フォームから問い合わせしました。」(蛭本氏)

巧妙、複雑化するサイバーセキュリティ対策に 脅威インテリジェンスサービスとしての Cisco Umbrella に期待しました

ソリューション

同社は Cisco Umbrella による POC を実施。社内すべての DNS 通信を約 1 ヶ月間検査したところ、延べ 700 件以上の危険通信をブロックできる効果が得られたとのこと。蛭本氏は社内にその効果を示し、正式に導入が採択されました。

圧倒的な検知力とデプロイメントのしやすさを評価

採用の決め手について、蛭本氏は「決めては検知力の高さとインテリジェンスの品質です。Newly ドメイン検出機能や DNS 特有の脅威検知機能など、セキュリティ機能も充実していました。さらに Cisco Talos のレベルの高い調査結果がオプションサービスの Cisco Umbrella Investigate に反映されており、セキュリティ運用に役立つことがわかりました。また、クラウドアプリケーションを識別し評価する機能がシャドー IT 対策に活用できたことも評価ポイントです。クラウドサービスのため既存設備の設定変更だけで利用でき、リーズナブルな料金設定も導入しやすい点です。」と話します。

フルプロキシモードでの活用で https も含めたあらゆる通信を可視化

また、同社では Cisco Umbrella のフルプロキシモードでの活用を施行。これは DNS レイヤのセキュリティと Investigate から得られる脅威インテリジェンスに加えてセキュア Web ゲートウェイ、ファイアウォール、クラウド アクセス セキュリティ プローカ (CASB) 機能をすべて単一の統合クラウドコンソールで実行する Secure Internet Gateway Essentials により提供されます。

この理由について、蛭本氏は次のように話します。

「暗号化通信 (https) を使った脅威を解析する環境を整えるためには、フルプロキシモード (Web ゲートウェイ) で SSL デコードする必要がありました。クラウド管理、シャドー IT 対策を行うためにも必要でした。」

導入ソリューション

DNS レイヤでユーザを最前線で保護するクラウドセキュリティ

Cisco 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、「セキュア インターネット ゲートウェイ: 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できる、最も簡単かつ迅速に導入可能なクラウド型セキュア DNS です。

業界初の DNS の技術により インターネット上の脅威を未然に防御

- すべてのプロトコルとポートが保護対象悪意あるサイトをアクセス前にブロック
- 目的に応じた柔軟にカスタマイズ可能なアクセスポリシーを設定
- マルウェア (ランサムウェア) 対策にも有効

簡単・迅速な導入

- クラウドベースのソリューションのため、追加のハードウェアなどは不要

働き方改革に最適

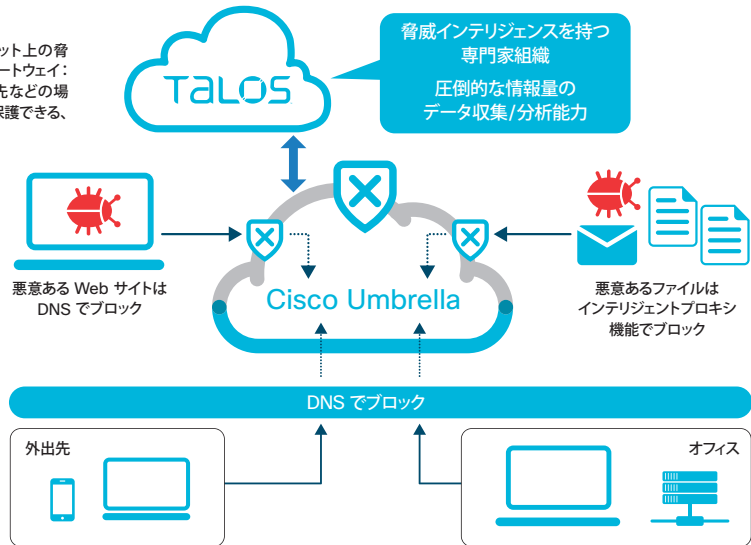
- 社内、社外、VPN 接続の ON/OFF を問わず、あらゆる場所、ユーザ、デバイスを保護

業界最高水準の検知率、最新の脅威に対応

- 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

インターネットの利用状況を可視化

- 脅威に関するさまざまな情報をグラフィカルに可視化
- 意図せず利用しているクラウドアプリケーションなどの「シャドー IT」も見え化する



Cisco Umbrella は、DNS の設定を変更するだけで簡単に導入でき、LAN を利用するすべての社内ユーザ、リモートユーザを保護できるクラウドセキュリティ サービスです。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。お客様側でソフトウェアやデータを更新する手間がかかりません。

結果～今後

業務上必要となるアクセス先除外などのきめ細かな設定を経て導入された Cisco Umbrella。全社展開後、接続の確立前に悪意のある接続先 (ドメイン、IP、URL) へのリクエストをブロックした数が毎月 500 ～ 3,500 件にも上るなど、確かな成果を發揮しています。

同社はフルプロキシ化の社内展開も順次進め、Cisco Umbrella から得られる複合化した通信ログと DNS ログを総合ログ管理プラットフォーム (SIEM) で取り込み、脅威調査ツールである Cisco Umbrella Investigate を活用し、日々のセキュリティ運用を行っています。

加えて同社では、Cisco Umbrella との連携も可能なエンドポイントセキュリティとして Cisco AMP for Endpoints の導入も検討しているとのこと。

「アンチウイルスでは防御できないセキュリティ対策に加え、テレワークと地方拠点拡大に伴い、侵入してしまった脅威を遠隔地から取り除くセキュリティ運用を目指しています。」(蛭本氏)

Cisco Umbrella で得られた情報を基に、今後さらに包括的なセキュリティの構築を目指すとする蛭本氏は、シスコへの期待を含めて次のように話します。

「当社は、低い運用コストで高度なセキュリティ対策を実現することを目指しています。そのためには、SIEM を使ったログの活用だけでなく、個別に運用しているエンドポイントとネットワークセキュリティ製品を連携させ、手順化した運用を自動化していくことを考えています。シスコへは、脅威インテリジェンスの量と質を高いレベルで維持していただくことはもちろん、各種セキュリティセンサーの連携とセキュリティ運用を行うためのプラットフォームである Cisco Threat Response、Cisco SecureX に期待しています。」

その他の詳細情報

Cisco Umbrella の詳細は、www.cisco.com/jp/go/umbrella を参照してください。

シスコセキュリティの詳細は、www.cisco.com/jp/go/security を参照してください。

アイペット損害保険株式会社



本社所在地 東京都港区六本木一丁目 8 番 7 号
代表者 代表取締役社長 山村鉄平
設立 2004 年 5 月 11 日
資本金 4,118 百万円 (2020 年 3 月 31 日現在)
従業員数 473 名 (2020 年 3 月 31 日現在)
URL <https://www.ipet-ins.com>

2004 年にペット保険事業をスタートし、現在 17 期目を迎えるペット保険専門の損害保険会社。2018 年にはマザーズに上場を果たし、現在、保有契約件数は 50 万件を超え、業界第 2 位のシェアを有す。主にペット医療費用保険やペット手術費用保険など、ペットの診療費の補償に特化した保険サービスを展開。昨年 2 月には第一生命ホールディングスと業務提携し事業基盤を強化、今年 10 月には持株会社化も控え、事業領域の更なる拡大を目指している。

シスコ コンタクトセンター

自社導入をご検討されているお客様へのお問い合わせ窓口です。
製品に関して | サービスに関して | 各種キャンペーンに関して | お見積依頼 | 一般的なご質問

お問い合わせ先

お電話での問い合わせ

平日10:00-12:00, 13:00-17:00

0120-092-255

お問い合わせウェブフォーム

cisco.com/jp/go/vdc_callback



©2020 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における商標登録または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(1502R) この資料の記載内容は2020年7月現在のものです。この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>