Protective DNS サービス刷新による脅威防御の強化

五十嵐 一浩 1)

1) 成城大学 メディアネットワークセンターセンター

kaz@seijo.ac.jp

Security Posture Improvement by Upgrading Protective DNS Infrastructure

Kazuhiro Igarashi 1)

1) Media Network Center, Seijo Univ.

概要

成城大学では 2021 年 4 月より Cisco Systems 社の Umbrella を採用して学内ユーザーに Protective DNS サービスの提供を開始したが，導入前に期待していた効果を十分発揮出来ないまま運用を継続してきた．その一方で，情報セキュリティを取り巻くトレンドは常に変化しており，大学も日々新しい脅威への対策に追われているため，効率的なソリューションが必要となっている．そこで，本学の求める Protective DNS の要件を再考し，サービス契約更新のタイミングに合わせて，Infoblox 社の Threat Defense へと刷新した．本稿では，その経緯と現在の運用状況について報告する．

１ はじめに

成城大学ではコロナ禍の影響で，2020 年当時，遠隔授業形態が必須となったことから，学生の保護者より「自宅で授業を受ける学生の情報セキュリティ対策」についての問い合わせを受けるようになった．その頃，まだ学内には BYOD 反対派の声が多かったこともあり，学生の個人所有デバイス向けに大学がマルウェア対策ソフトを提供するという枠組みなど認められるはずもなく，利用者に向けたありきたりな啓発活動の実施が精一杯という状況が続いていた．

そのような大学の実情に適していたのが Cisco Umbrella[1](以下，「 Umbrella 」と言う) であり，文教向けに用意されたパッケージでは，教職員数のライセンス購入で学生分が無償となる特典を享受することが出来る．

DNS を活用した不要なトラフィック制御だけであれば，広告をブロック出来る Pi-hole[2] を検討したこともあったが，悪しきサイトへの接続を遮断するためには高精度な脅威インテリジェンスが不可欠であると判断し，2021 年 4 月に全学情報セキュリティ対策の一環として Cisco 社の Umbrella を導入した．

緊急事態宣言下においては，本学教職員も在宅勤務体制を指示されていたが，原則は大学へ出勤しての勤務であったため，学外で遠隔授業を受ける学生以外の通信トラフィックは Umbrella の DNS Forwarder を介して制御することが出来るようになった．

２ 活かせなかった Umbrella 特典

Protective DNS 導入の動機ともなった学生の自宅環境へのサービス展開については，実施前の検討プロジェクトを立ち上げて，本学メディアネットワークセンターに勤務する学生スタッフ数名に参加してもらった．

学外から接続するデバイスの DNS クエリーを制御するには，学生の PC に Umbrella エージェントのインストールが必要となる．覚悟してはいたが，やはりこの点が学生の個人所有 PC へのサービス展開を困難にした．

情報セキュリティ対策の向上を目指す我々職員や保護者の思惑に反して，学生スタッフからの評価は，「自宅での活動まで大学に監視されたくない」，「（職員の勤務）時間外のブロック解除対応が不安」，「参照したいサイトがブロックされたらエージェントをアンインストールするだろう」などと，ネガティブな意見が多かった．

加えて，エージェントをインストールした PC の管理問題も浮上した．Umbrella の文教向けパッケージでは API の利用が出来ないため，仮に 6000 人規模の学生ユーザーがエージェントをインストールした場合，それらの PC を効率的に管理する方法が無い．個人所有の PC 名からは利用者の特定が不可能であるため，卒業時のエージェント削除を徹底させることも難しいと判断し，学生に対する Umbrella エージェント配布は見送ることとなった．

3　Umbrella 運用から見えた課題

Umbrella ポリシーの Security Settings は主にカテゴリーの組合せで構成されているが，”Categories To Block” で選択できる項目の粒度が細やかでなく，また日本語コンテンツのサイト分類精度も低いため，管理者がカテゴリーの説明だけでリスク高と判断してブロック対象にしてしまうと，意図せぬサイトが誤検知でブロックされる事象が頻発した．（例えば，本学の構成員が運営している kyouju.com ドメインは Command and Control カテゴリ扱いでブロックされてしまう．）適切なカテゴリへの修正依頼にも即座に対応してもらえないため，運用現場は膨大な Allow list のメンテナンスを覚悟せざるを得ない．

ポリシーでは Content Categories による制御も可能ではあるが，これらについても日本語コンテンツ分類精度が低いことで生じる誤検知回避のため，予め用意された 103 項目のカテゴリの内，わずか 10 項目しかブロック出来ずにいた．それでもブロック解除リクエストがあがって来るのだが，これは blog.livedoor.jp のようなブログサービスがドメインごとブロック対象カテゴリに分類されていたりする粒度の粗さにも起因していると思われる．

また，Umbrella ではブロックされた際に表示される警告ページ内にブロック解除リクエストフォームのリンクが用意されているので，ユーザーにとっては気軽にリクエスト解除申請が出来るのだが，これは誤検知が多い事を前提にデザインされたインターフェイスであると理解して良いのかもしれない．

ブロック解除リクエストを受けたら，管理者は当該サイトが無害なものかを判断して対応する必要がある．Umbrella ではブロックページ内の “Diagnostic Info” から図 1 のような診断情報の確認が可能である．

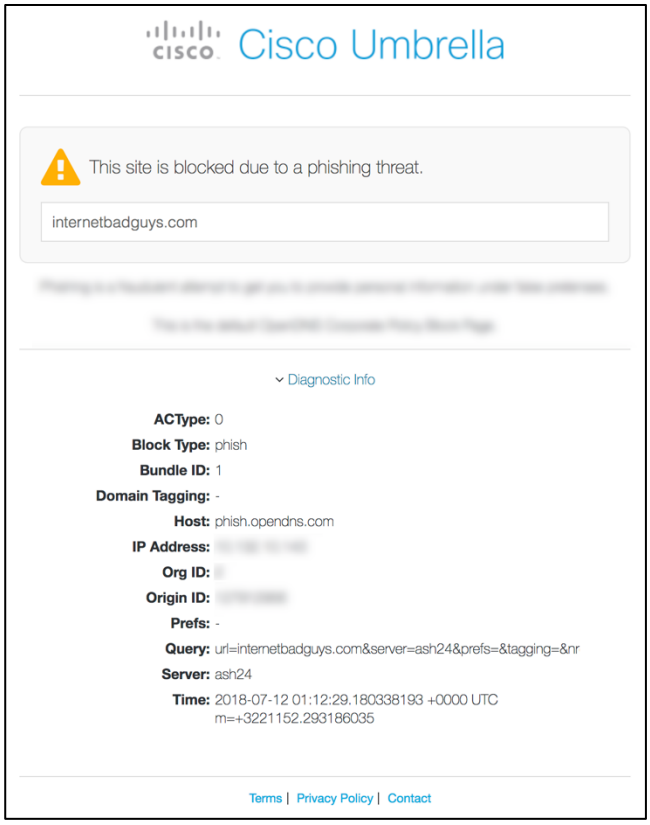

図 1　An example block page with the diagnostic info[3]

診断情報とは言うものの，これだけで管理者が無害なサイトかどうかを判断するのは困難である．利用者への説明責任を果たすためにも，申請毎に担当職員が VirusTotal[4] で URL スキャンした結果や，Umbrella 以外の DNS キャッシュサーバー経由で確認した実際のコンテンツから判断して対応せざるを得ないという煩雑な運用を余儀無くされていた．

4　Protective DNS 刷新のきっかけ

自宅から接続する学生向け情報セキュリティ対策としての期待はついえ，日々の運用は多少煩雑になったとはいえ，名前解決のフェーズにてリスクの高いコンテンツへのアクセスを抑止する手法は，少人数で全学システムを運用する管理者にとって，効率の良いソリューションであることは間違いない．限られた予算を工面して毎年契約を更新して来たのだが，為替レートの影響や度重なる価格改定によって経常予算の確保が厳しくなり始めていた．

そのような折，2024 年 5 月に政府がインフラ事業者や大学を守るため，Protective DNS を無償提供するとの報道[5]があった．一瞬期待を寄せはしたものの，その対象に私立大学が含まれていないことが判明し落胆した．

ただ，情報収集する中で，政府が採用する Protective DNS が Infoblox Threat Defense[6] (以下，「Threat Defense」と言う) であると知り，無謀にも小さな私立大学単体で政

府推奨レベルの Protective DNS の採用に挑戦すべく，本学の要件を再考し，Umbrella との機能比較を中心に Threat Defense の PoC (Proof of Concept) を開始した．

５　Threat Defense のシステム構成

Threat Defense も Umbrella と同じように，学内に展開した DNS Forward Proxy (以下「DFP」と言う) と呼ばれる DNS キャッシュサーバーが，ユーザーからの DNS クエリーを受け，Infoblox Cloud DNS Firewall (以下，「 DNS Firewall 」と言う) を経由して権威 DNS サーバーに問い合わせを行う．DFP は定義されたポリシーに従ってユーザーに応答を返す（図２）．

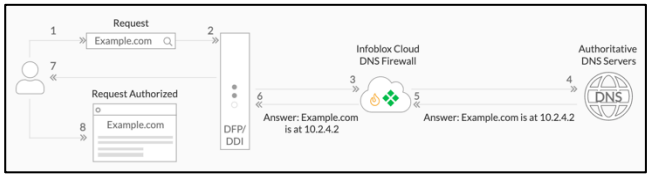

図２　DFP と Infoblox Cloud DNS Firewall の構成

DFP に適用するポリシーは，Custom List, Feeds and Threat Insight, Category Filter と Application Filter の 4 種類の Rule Type を複数定義して構成する．

Umbrella の Security Settings で設定する項目を， Threat Defense では Feeds and Threat Insight の各 Object を選択して設定することが可能であるが, Object の種類は Umbrella に比べ，より DNS の脅威を意識して纏められ，命名されている．例えば，Umbrella の “Newly Seen Domains” は Threat Defense では “Zero Day DNS” と表現されている．また，Threat Defense には DGA (Domain Generation Algorithm) や Data Exfiltration といった Feed もあり，管理者は Umbrella よりも細やかな条件でポリシーを作成することが出来る．

学内ユーザーへのサービス展開は，ISC DHCP Server[7] の option domain-name-servers パラメータで設定している IP アドレスの値を Umbrella の DNS Forwarder から Infoblox DFP に変更するだけなので，想定外の不具合があった際にも容易に切り戻しが可能であり，安心して PoC に臨むことが出来た．

６　ブロック解除対応の改善

クラウドのリソースを消費するサービスの PoC は長期で実施することが難しく，加えて開始した時期も 2024 年 12 月と遅かったこともあり，次年度の Protective DNS サブスクリプション更新前に判断材料となる評価項目を絞り込んだ上で効率的に実施する必要に迫られた．

着目した点は，Feed や Category Filter の誤検知に対する精度である．前述した通り，Umbrella では検知精度の問題で 10 項目程度しかブロック出来ていなかったが，Thread Defense では細分化されたサブカテゴリの恩恵もあり，50 以上の項目をブロック設定することが出来た．誤検知によるブロック解除要望は PoC 期間中に 2 件だけ報告されていたが，いずれもジェンダー平等の研究者からのものであったため，ブロック設定していた Adult カテゴリ内の Gay, Lesbian or Bisexual サブカテゴリーを Allow する事で対応した．

特筆すべきはブロック解除依頼の対応時に絶大な効果を発揮する脅威インジケータの調査ツール Dossier[8] である．該当ドメインに関する 13 項目から分析した結果を可視化することで, IT リテラシーの低い利用者に対しても客観的に，根拠に基づいた説明が出来るため，ブロック解除依頼対応時の煩雑さは大きく軽減される．

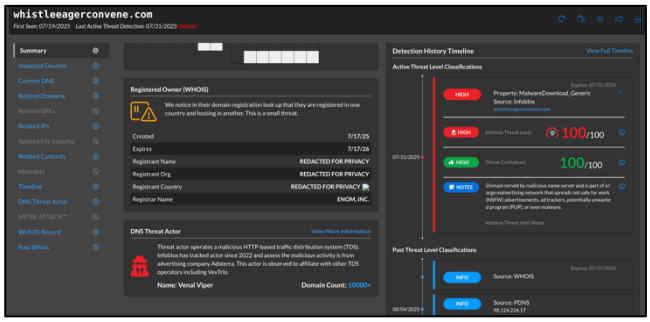

図３　Dossier で確認出来る脅威アクターやタイムライン

７　サービス刷新の効果

PoC で十分以上の改善が期待出来ると確信し，2025 年 4 月から Threat Defense の本番運用を開始した．PoC のタイミングが良かったこともあり，今回は PoC 環境をそのまま本番環境として利用する事が出来たので，システム構築作業の負荷も低く，切替え時の問題も発生しなかった．

日々の運用では，Dashboard が秀逸であり，学内からの DNS クエリーに関する脅威とその状況を一目で把握することが可能である．また，それぞれのグラフの要素をクリックしてドリルダウンすることで，問題の DNS クエリーを発生させたデバイスの IP アドレスまで確認することが出来る．

Protective DNS の恩恵によって，センター職員が対応する情報セキュリティインシデントを名前解決のフェーズで大幅に減らせるというコンセプトは理解していたが，誤検知の少ない Threat Defense の導入により，未然に防ぐことが出来た脅威の可視化も可能になり，漸くその効果を実感することが出来た．加えて，Dashboard には DNS クエリーをブロックした事で節約できた推定帯域も表示される．図４では 1 ヶ月間で 6.7TB もの無駄な通信を発生させ

ずに済んだことが分かる．しかも，その約半分がカテゴリーフィルターによるものであることから，精度の高い フィルター実装の重要性を再認識させられた．

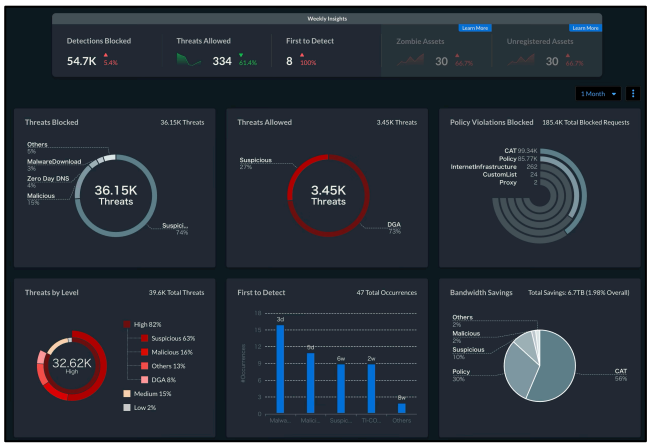

図４　Threat Defence の Dashboard

８　DoH (DNS over HTTPS) の課題

Threat Defense の Policy 設定では Feeds and Threat Insight の Public_DOH と Public_DOH_IP をブロックすることが推奨されている．Umbrella では制限していなかったこれらの Feed をブロックした途端，ブロックされた URL 集計の上位が Anonymizer カテゴリで占有された．最近の Web ブラウザーはデフォルトで DoH や DoQ (DNS over QUIC) を使用するようになっているものもあり，管理者が期待した通りの DNS フィルタリングを実施出来ていなかった事に気づかされた．

個人のプライバシー保護強化を否定する事は出来ないが，大学のネットワークが SINET を利用している以上，国立情報学研究所学術情報ネットワーク加入規定[9] を遵守する必要がある．加入規定第 6 条の遵守事項で，目的外のネットワーク利用を制限するには DNS フィルタリングが不可欠と考えるが，同条の第 3 項では通信の秘密を侵害しないことも謳われており，「どのサイトにアクセスしたのか」までを通信の秘密であると主張されてしまうと，ネットワーク運用者としては今後 Protective DNS を活用出来なくなってしまうため，状況にあわせて迅速に学内運用基準を修正できる組織体制が求められている．

９　今後の展開

本学で提供する Protective DNS サービスは，Umbrella から Threat Defense に切り替えたことにより，運用負荷を下げると同時に， DNS クエリーを確度の高いレベルで制御出来るようになったと考えている．しかしながら，DoH をブロックしたことで，学内専用 Wi-Fi を避けて制限の緩い eduroam のみを使う利用者がいることも把握しており，今後は eduroam 用ネットワークにも Threat Defense DFP を実装することを検討している．

他にも，iCloud+ を課金して契約している利用者からは，プライベートリレーが学内で使えないといった不満の声もあり，DoH, DoQ に関する課題は当面スマートな解決策が見当たりそうにない．大学が BYOD 推進に舵を切った今，学外でパブリック DNS をセキュアに使うことは大切であるが，大学に来た際に使う Wi-Fi が，様々なセキュリティ対策を講じた学内ネットワークであると認識してもらうところから始めなければならないというのが現状であると感じている．

高リスクな DNS クエリーを出し続ける学生 PC の存在を把握しても，適切なタイミングで直接当事者にコンタクト出来ないケースが多いという課題は Umbrella 運用の頃から抱えている．成城の建学の精神である「独立独行の人を」 IT の領域でも「育てる」ためには，学生に対する啓発活動が必須であると理解している．間接的にではあるが，普段使いの学内 IT サービスを通じて，情報セキュリティの本質を理解し，学んでいける環境を提供出来るよう，これからも尽力していきたい．

参考文献

[1] Cisco Systems, Inc., “Cisco Umbrella | Leader in Cloud Cybersecurity and SASE Solutions”. https://umbrella.cisco.com/, (参照 2025-07-21)

[2] Pi-hole, “Pi-hole | Networking-wide Ad Blocking”. https://pi-hole.net/, (参照 2025-07-21)

[3] Cisco Systems, Inc., “How to Read the Diagnostic Information on Block Pages | Cisco Umbrella”. https://support.umbrella.com/hc/en-us/articles/115004584946-How-to-Read-the-Diagnostic-Information-on-Block-Pages, (参照 2025-07-22)

[4] “VirusTotal”. https://www.virustotal.com/gui/home/url, (参照 2025-07-22)

[5] 読売新聞オンライン, “インフラ事業者や大学を国が守る，悪質サイトへの接続防ぐサービスを政府が無償提供” . https://www.yomiuri.co.jp/politics/20240515-OYT1T50134/, (参照 2025-07-22)

[6] Infoblox Inc., “Infoblox Threat Defense: Protective DNS Security - Infoblox”. https://www.infoblox.com/products/threat-defense/, (参照 2025-07-22)

[7] Internet Systems Consortium, Inc., “ISC DHCP - ISC”.

https://www.isc.org/dhcp/, (参照 2025-07-28)
[8] Infoblox Inc., “Infoblox Dossier – Infoblox Threat Defense – Infoblox Documentation Portal”. https://docs.infoblox.com/space/BloxOneThreatDefense/272106087/Infoblox+Dossier, (参照 2025-08-06)
[9] 国立情報学研究所, “国立情報学研究所学術情報ネットワーク加入規定” . https://www.sinet.ad.jp/wp-content/uploads/2018/11/201811_kanyuu-kitei.pdf, (参照 2025-08-06)