

京都大学情報環境機構における DNS フィルタリングの導入と運用について

石井 良和¹⁾, 山口 倉平¹⁾, 片桐 統¹⁾, 戸田 庸介¹⁾

1) 京都大学 情報部

ishii.yoshikazu.3e@kyoto-u.ac.jp

Operation of DNS filtering at Institute for Information Management and Communication, Kyoto University

Yoshikazu Ishii¹⁾, Souhei Yamaguchi¹⁾, Osamu Katagiri¹⁾, Yosuke Toda¹⁾

1) Information Management Department, Kyoto Univ.

概要

京都大学情報環境機構では、セキュリティ向上のため DNS の名前解決の段階で悪性サイトへの通信をブロックする DNS フィルタリングを学内ネットワークに導入した。本稿では、DNS フィルタリングの導入について説明し、運用によって得られた知見を紹介する。

1 はじめに

昨今、フィッシングによる個人情報の窃取や、ランサムウェアをはじめとするウイルス感染による被害など、情報セキュリティの脅威が増加している。これらの攻撃は、正規のページに似たサイトにアクセスさせて個人情報を入力させるものや、マルウェア感染を引き起こすサイトにアクセスさせてウイルス感染させるといった手口が使われている[1]。このような悪意のあるサイトを悪性サイトと呼び、京都大学においても、悪性サイトを介した情報セキュリティインシデントが起きており対策を行う必要があった。

悪性サイトへの通信を防御する対策として、ファイアウォールでの IP アドレスでの通信遮断や、IDS のような通信内容で攻撃を検知して遮断するセキュリティ対策があげられる。しかしながら、IP アドレスは1つのホストに対して複数の IP アドレスが動的に割り当てられることが可能で、IDS においても、Web 閲覧時の通信は暗号化通信が一般的で、通信内容から攻撃を検知することが困難となってきた。このような状況下において、DNS の名前解決の段階で悪意のある通信をブロックできる DNS フィルタリングはセキュリティ対策として有用であると考えられる。

京都大学情報環境機構（以下、「本学」という。）では、フィッシングやマルウェア配布サイトなど

のドメイン情報が蓄積された、脅威ドメイン情報を参照して悪性サイトへのアクセスを名前解決の段階で防止する、DNS フィルタリングを、2024 年 3 月に、全学の情報通信基盤である学術情報ネットワーク（Kyoto University Integrated information Network System、以下「KUINS」と呼ぶ。）に導入し、運用を開始した[2][3]。

本稿では、DNS フィルタリング導入に向けた取り組みと、運用状況について紹介する。

2 DNS フィルタリングの導入

2.1 DNS フィルタリングの構成と動作

本学で導入した DNS フィルタリングは、学内の内部 DNS キャッシュサーバと、クラウド上の脅威ドメイン情報と連携して動作するネットワーク型で構成される。（図 1）

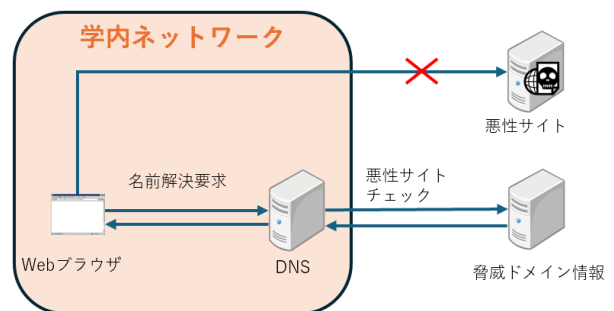


図 1. システム概要図

DNS キャッシュサーバは、クライアントから名前解決の要求があると、クラウド上の脅威ドメイン情報をチェックして、問題がなければそのままドメインの IP アドレスをクライアントに返し、悪性サイトであった場合は、本来返す本物の IP アドレスの代わりに、予め用意したブロック通知用の Web サイトの IP アドレスを、クライアントに返す。

なお、本学でブロックしているのは、フィッシングとマルウェア配布サイトとスパムサイトを対象とし、コンテンツ内容でのブロックは行わない。

2.2 DNS フィルタリングの導入

DNS フィルタリングを学内全体に導入すると KUINS を利用する様々な機器に影響を与えることから、導入の約 1 年前から運用開始までの間に PoC を複数回行い、検証範囲を増やしながら、影響を確認したうえで、学内ネットワーク全体への導入を実施した。

PoC を進める中で判明したこととして、特にメールサーバでの送信元ドメイン確認やスパムチェック機能に影響がみられた。これはメールサーバで DNS フィルタリングによって悪性サイトと判定された場合の動作についても、A レコードはブロック通知用の Web サイトの IP アドレスを返し、MX レコードや TXT レコードの場合は、Answer Section がない status「NO ERROR」を返していたためであった。そのため、DNS フィルタリングが適用された評価用の DNS サーバを用意し、サーバ管理者に DNS フィルタリングが動作する環境で本来受信するはずのメール送受信に影響がないか確認を依頼した。影響があり回避できないサーバについては、DNS フィルタリングが適用されない他の DNS を参照するなどの対応を要した。

3 DNS フィルタリングの運用

3.1 フィルタリング状況

4 月 8 日から 9 月 30 日における 1 日当たりのブ

ロック数を図 2 に、ブロックしたドメイン数を図 3 に示す。1 日当たり、平均約 29,000 件がブロックされていることが分かる。8 月以降はブロック件数が 35%減少しており、これは授業期間が終わり夏季休暇に入ったためと考えられる。ブロックしたドメイン数は、1 日当たり、平均 3,250 件であった。こちらも同様に夏季休暇中は授業期間に比べて、約 25%の減少がみられた。

全体の DNS クエリー数に対してブロックした割合は、平日が約 0.1%から 0.2%を占め、休日になると約 0.4%から 0.5%を占めている。

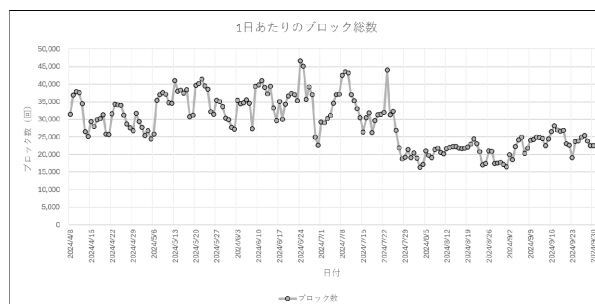


図 2. 1 日あたりのブロック総数

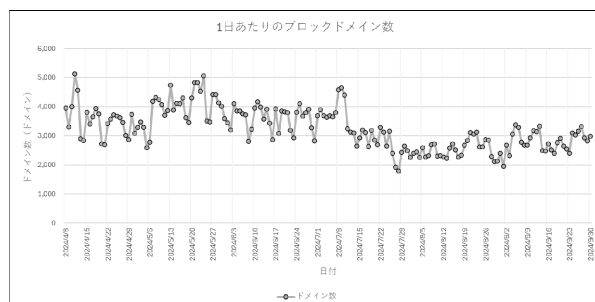


図 3. 1 日あたりのブロックドメイン数

週ごとのブロック件数を図 4 に示す。曜日ごとの差はほとんどなく、同じような推移でブロックしていることが分かる。

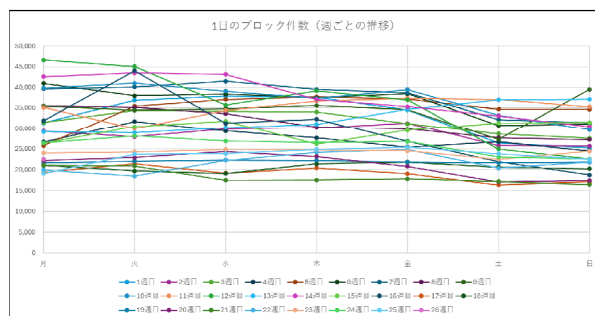


図 4. 1 日のブロック件数 (週ごと)

週ごとのブロックドメイン数を図 5 に示す。土日に若干の減少が確認できるものの、平日に差はほとんどなく推移していることが分かる。

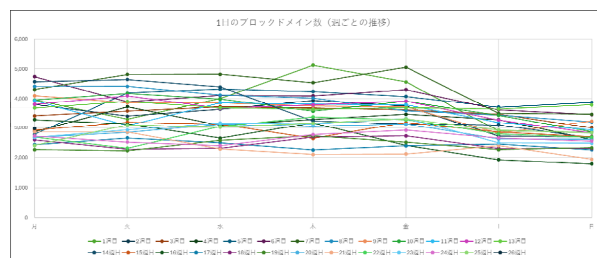


図 5.1 日のブロックドメイン数（週ごと）

3.2 過検知の対応

本学で導入した DNS フィルタリングは、リアルタイムで更新されるクラウド上の脅威ドメイン情報を元に、悪性サイトかどうかを判定している。脅威ドメイン情報では悪性サイトと判定されたケースであっても、正規のサイトである可能性がある。そのため、構成員には過検知が疑われる場合は、相談するよう周知した上で運用を開始した。

利用者から相談があれば、管理者によって接続先のサイトを評価し、過検知の疑いが高い場合は、ホワイトリストに登録して通信を許可している。管理者によるドメインの評価は、本学で導入しているサンドボックスでアクセスしてページの確認や、ドメイン評価サイト[4]を用いて評価している。

4月から9月の間に利用者から21件相談があり、すべてホワイトリストに登録している。月に平均3.5件の相談があり、最大で月に7件の相談を受け付け対応した。

3.3 DNS フィルタリングの活用

学内にフィッシングメールが届き、メールの本文中に記載されたフィッシングサイトのドメインを、DNS フィルタリングのブラックリストに登録した。これにより、構成員がフィッシングサイトに誤ってアクセスしてしまったとしても、通信をブロックできる。攻撃対象が限定的な標的型攻撃や、まだ広まっていない悪性サイトの場合、脅威ドメイン情報に未登録である可能性が高いと考えられるが、ブラックリストを活用することで、脅威ドメイン情報への登録を待たずに、早急な対策を行うことが可能である。

4 おわりに

本学における DNS フィルタリングの導入と運用について紹介した。本学的环境においては、6カ月の間、名前解決を一定の割合でブロックしており、DNS フィルタリングの効果が確認できた。ブロック件数に対して、過検知の相談が少ないこと、休日が平日にかけて約0.3%程度ブロック率が高いことから、構成員が Web ブラウザ利用中にブロックされるケースよりも、メールサーバの送信元確認や SPF レコードの検証など、常時名前解決を行っている機器でブロックされているケースが多いと推察する。今後、ブロックされた機器の確認等を通じて、ブロックの効果と影響について注視していきたい。

過検知については、サンドボックスではドメイン自体は安全と判定し、JavaScript の使い方が危険と判定している傾向がみられる。特に本学では学会のサイトをブロックするケースが多くみられ、事前に学会サイトのドメイン名をホワイトリストに設定することを検討している。

今後の DNS フィルタリング活用の展望として、学内から複数の通報があったフィッシングメールの悪性サイトを、自動的にブラックリストに登録する仕組みを検討していきたい。

今後、導入した DNS フィルタリングを適切に運用し、さらなる情報セキュリティの向上を図りたい。

参考文献

- [1] IPA 独立行政法人情報処理推進機構、情報セキュリティ 10 大脅威 2024、<https://www.ipa.go.jp/security/10threats/10threats2024.html>.
- [2] 京都大学情報環境機構広報誌「Info!」No.29、<https://www.iimc.kyoto-u.ac.jp/info29.pdf>
- [3] 京都大学情報環境機構広報誌「Info!」No.30、https://www.iimc.kyoto-u.ac.jp/info30_r3.pdf
- [4] VirusTotal、<https://www.virustotal.com/>