PICK OUT! No.14
JPNIC ブログコーナー

不審なトラフィックやスパムメールを発見するための手法として、RBL（Reputation Block List）があります。一つだけではないので、どのRBLを使えば良いのか、評価方法を考えてみました。

dom_gov_team　2024年7月25日　ICANN技術文書　ドメイン名

https://blog.nic.ad.jp/2024/9890/

ブロックリスト（RBL）のより効果的な使い方を探る －OCTO-037のご紹介－

RBLはReputation Block Listの略で、スパムやフィッシングなど悪意あるコンテンツに利用されていると考えられるIPアドレスやドメイン名、URLのリストのことです。特にISPやメールサービスプロバイダーでは、不審なトラフィックを発見したりユーザーを保護したりするための一般的な手法の一つとしてこのRBLが使われます。

ICANN OCTOの研究プロジェクトでもRBLが使用されており、以前このブログシリーズでも紹介したDAARや、DAARのデータを組み込んだITHIのメトリクスにおいてRBLが重要な情報源になっています。また、2024年2月に新しく発表されたOCTOのプロジェクトであり、DAARの進化版とも言えるDomain MetricaでもRBLの組み込みが見込まれています。

このようにインターネット上の脅威からユーザーや資源を保護するため、本稿ではRBL自体をどのように評価して利用するのが良いのか検討します。

■評価方法の検討

あるRBLを評価する上で、目的、仕組み、メタデータ、情報源、収集範囲、項目の定期的な再評価、信頼性といった観点からそのRBLの特徴を掴むことができます。

このような定性的な特徴の他に、直接的または間接的に判断できる定量的な指標も考えられます。定量的な指標の単位や導出方法は必ずしも決まっていませんが、原文※1では実際にOCTOが使用しているデータセットを使ってグラフ等に可視化された比較例も掲載されています。

さらにRBLのデータそのものから得られる直接的な指標として、量、オーバーラップ、即時性、更新頻度（訳注）があります。またRBLを他のデータと比較して得られる間接的な指標として、活発度、精度、正確性があります。
https://blog.nic.ad.jp/2024/9890/ では、もう少し詳しく説明してありますのでご参照ください。

※1　https://www.icann.org/en/system/files/files/octo-037-11dec23-en.pdf
（訳注）原文では Churn。

■RBLの限界と補完性

こうした指標で実際のRBLを見てみると、RBLそれぞれの特徴を捉えることができ、新たにそのRBLを使用すべきかどうかの判断材料となります。ただし、あるプロジェクトに対してこのRBLが適している、ということは言えても、一般論としてどのRBLが優れている/劣っていると言うのは難しいのです。

OCTOで行っているような研究プロジェクトの他にも、RBLはファイアウォールやフィルタリングなどセキュリティ実務でよく使用されます。本稿では概要のみご紹介していますが、原文では実際に比較した結果や、その算出に用いたPythonコードも公開されていますので、ご興味のある方はぜひ原文もご覧ください。

カテゴリー

- ICANN技術政策文書
- IETF
- Internet Week
- IPアドレス
- JPNICからのお知らせ
- JPNICについて
- JPNICのイベント
- アクセス数Top 10
- インターネットガバナンス
- インターネットの技術
- コラム
- ドメイン名
- 他組織からのお知らせ
- 他組織のイベント

PICK OUT BLOG 2024 7.25

JPNIC BLOG JPNICブログ