

Premium DNS Databaseのカバー率が 578%向上

WhoisXML APIでご提供している Premium [DNS Database Download](#)のカバー率が、この数カ月で大幅に向上しました。2024年の最新の測定では、DNSレコードの総数が2023年5月と比較して578%増加したことが確認されました。

中でもAレコードは1,313%、AAAAレコードは700%増加しました。DNS Database Downloadサービス全体では、現在353億件を超えるDNSレコードを収録しています。

今回の機能強化は、脅威の監視・検出のためのパッシブDNS分析を拡充するものです。今や業界最高水準のカバー率を誇るPremium DNS Database Downloadで、以下のことが可能になります：

- **脅威の監視、検知、対応の迅速化**：悪意あるドメイン名とIPアドレスをより多く追跡、検出できます。データベースに含まれている多様なDNSレコードを活用すれば、これまで以上に攻撃インフラを発見しやすくなります。
- **セキュリティプラットフォームにDNSの全体像を提供**：DNSの知見をSIEM、エンドポイントセキュリティおよびネットワークインテリジェンスプラットフォームに統合することで、潜在的な脅威を多面的に捉え、インシデントの全体像を把握することができます。
- **広範囲にわたるアセット検出**：DNSのカバー範囲が拡大したことで、外部の攻撃サーフェスをより正確に把握できるようになりました。セキュリティリスクをもたらす可能性のある放置されたアセットを検出しやすくなります。



- **脅威アクターの戦術・技術・手順（TTP）をより深く理解**：攻撃者のドメイン名、IPアドレスおよびサーバーの関連性を突き止めることが容易になります。脅威アクターのコマンド&コントロール（C&C）サーバー、通信チャネル、潜在的な攻撃ベクトルに関する知見を得ることができます。

さまざまなDNSレコードで幅広いインテリジェンスを提供

WhoisXML APIのDNS Database Downloadには「Standard」、「Premium」という2種類のサービスがありますが、そのどちらにおいても、以下を含む広範なDNSレコードをカバーしています：

- **Aレコード**：ドメイン名に関連付けられたIPv4アドレス。
- **AAAAレコード**：ドメイン名に関連付けられたIPv6アドレス。
- **MXレコード**：ドメイン名に宛てたメールが送信されるメールサーバー。
- **NSレコード**：ドメイン名の権威ネームサーバー。
- **TXTレコード**：ドメイン名に関する情報（テキスト形式）。
- **CNAMEレコード**：ドメイン名の正式名。
- **SOAレコード**：更新間隔、管理者のメールアドレスなど、ドメイン名の管理情報。
- **PTRレコード**：IPアドレスに関連付けられたドメイン名。

ご提供するデータベースのファイルには、各DNSレコードについて、ドメイン名、IPアドレス、関連する他のDNSレコード、レコードの最終更新のタイムスタンプといった重要データが含まれています。

DNS Database Downloadは、データベース全体を収録したCSVファイルと、データベース全体に対する日次、週次、月次の差分を収録した更新ファイルにてご利用いただけます。詳細につきましては、[こちら](#)をご参照ください。

データベースのサンプルは[こちら](#)でダウンロードいただけます。脅威ハンティング、アセット検出などにおけるDNS Database Downloadの具体的な活用方法につきましては、[こちら](#)までお気軽にお問い合わせください。