ホワイトペーパー

DNS ベストプラクティス

筆者：
Craig Sanderson、
Infoblox 、プリンシパル・サイバー・セキュリティ・ストラテジスト

目次

1. はじめに 3

2. DNS がサイバーレジリエンス、多層防御、ゼロトラストに与える影響 3

3. DNS の脅威ベクトル 4

4. DNS セキュリティのベストプラクティス 4

4.1 プロテクティブ DNS 5

4.2 DNS プロトコルの保護 7

4.3 DNS サービスおよびインフラストラクチャの保護 7

5. 総括と提言 8

このホワイトペーパーでは、Domain Name System（DNS）が、2 つの目的を達成するベストプラクティスを提供することについて模索します。目的の 1 つは、DNS プロトコルとインフラストラクチャを保護して誤用や設定ミスを軽減すること、もう 1 つは、DNS を利用してゼロトラストおよび/または多層防御のセキュリティリスク管理アプローチの一部としてネットワークセキュリティの追加レイヤーを提供することです。

1. はじめに

ユーザーが、IP アドレスではなくドメイン名（例：www.example.com）を使用してインターネット・リソースにアクセスするには、ドメイン名を IP アドレスに変換し、再度変換してその逆に戻すシステムが必要です。この変換は、Domain Name System（DNS）の主要タスクです。現代組織のネットワーク展開において、DNS インフラストラクチャは、社内またはインターネットへのすべてのネットワーク通信にとってミッションクリティカルです。もし失敗すれば、アプリケーションやユーザーとともにネットワーク全体がダウンする可能性があります。したがって、DNS は組織のデジタル弾力性にとって重要な要素であり、定期的に評価または再評価する必要があります。

このような評価には、特に暗号化された DNS プロトコルを採用する場合に、DNS サーバーが組織のニーズを満たすのに十分な能力を有しているかどうかの評価を含める必要があります。アセスメントには、DNS インフラが高度な回復力と冗長性を備えたアーキテクチャの一部として最適化されていることを確認するために、サーバーの健全性と構成の見直しも含める必要があります。さらに組織は、サイバーセキュリティ・アーキテクチャの基盤レイヤーとしての DNS の大きな可能性を活用するために、DNS プラットフォーム内に制御を実装する必要があります。

DNS プラットフォームは、オンプレミス、クラウド、すべての IoT デバイスを含む、ネットワーク上のすべての種類のクライアントですでに使用されています。そのため、DNS インフラストラクチャが提供する保護は、デバイスの種類にかかわらず、そのインフラストラクチャを名前解決に利用するすべてのクライアントに利益をもたらします。このため、組織や政府は、サイバーセキュリティ戦略の基盤要素として DNS を採用することが推奨されます。

2.DNS がサイバーレジリエンス、多層防御、ゼロトラストに与える影響

ネットワーク・セキュリティのベストプラクティスにおける最近の進展により「多層防御」という概念に対する注目が高まっています。これは、どの防御策も完全ではないため、最善の防御は複数の保護層から成り立つという考え方です。このスタイルのサイバー防御により、侵害に対する耐性が高まり、ゼロトラストの原則にさらに厳密に準拠した、より柔軟でスケーラブルかつ回復力のあるシステムが実現します。

ゼロトラストの原則では、要素、ノード、またはサービスを暗黙的に信頼することはできないという前提があります。しかし、DNS はゼロトラスト戦略において見過ごされがちな要素であり、暗黙の信頼が置かれると大きなギャップを生むことになります。

DNS をゼロトラストの原則と整合させるために、組織は情報源を推測するのではなく、DNS を活用して検証し、セキュリティポリシーを適用し、エンドユーザやシステムが悪意のあるまたは許可されていないリソースへアクセスすることを防止し、デジタル・フォレンジックとインシデント対応のために資産の可視性を提供する必要があります。

これはDNSの役割が純粋に運用上のものから、インターネットセキュリティを提供し、ネットワークの回復力を強化するためのより大規模なツールへと移行していることを示しています。

ゼロトラストは、場所中心のモデルからアイデンティティ、コンテキスト、データ中心のアプローチへと移行しており、時間の経過とともに変化するユーザー、システム、アプリケーション、データ、資産間でのきめ細かいセキュリティ制御を提供します。DNS 解決は、任意のパブリックドメイン名をクエリする エンドポイント に公開されている可能性があるため、組織は DNS を保護し、ゼロトラストネットワークの制御を回避するルートとして使用されないようにする必要があります。これには、特定のクラスの エンドポイント に対する DNS 保護サービスの実装や、特定の DNS リゾルバー構成が含まれる場合があります。DNS セキュリティは、エンドポイント・セキュリティ・ソリューションの導入が困難であった製造業や重要なインフラストラクチャに存在する IoT デバイスと運用テクノロジーのセキュリティを保護する上では特に役立ちます。

3. DNS の脅威ベクトル

DNS インフラストラクチャは、攻撃キャンペーンにおける一般的な脅威ベクトルです。[1]DNS サービスに対する脅威は、重大な運用障害や、データ、整合性、機密性の損失につながる可能性があります。さらに、ALPHV Blackcat などの多くの脅威アクターは、悪意のあるドメインを利用して大規模なランサム攻撃を開始します。[2]以下は、DNS サービスだけでなく、組織が依存するすべてのシステムを危険にさらす可能性のある侵害について例示した、非網羅的なリストです。

a) 分散型サービス拒否：悪意のある攻撃者は、DNS サーバー／サービスに対してサービス拒否（DoS）攻撃を実行するために、大量のクエリを送信する可能性があります。攻撃者は、多数のサードパーティーの DNS クライアントを使用して攻撃を補助する可能性があります（分散型 DoS または DDoS）。

b) 不正な構成変更：DNS 通信を可能にするプラットフォームレベルの構成ファイルは、不十分な保護により破損したり、不正に変更されたりする可能性があります。その結果、DNS ホスト間の通信の途絶から DNS サービス自体の完全な障害に至るまで、さまざまな混乱が発生します。

c) Dangling CNAME の悪用：DNS の CNAME レコードが 2 つのドメイン名をリンクしている場合、レコードが指す正規名の親ドメインがターゲット組織に登録された状態を維持していないリスクがあります。その結果、脅威者がその親ドメインを登録し、DNS の解決は、最終的に脅威者が管理するドメインに解決されることになります。CNAME レコードが悪用されるもう 1 つの可能性は、正規名がドメイン所有者によって使用されなくなった IP アドレスに解決され、攻撃者がその IP アドレスを制御できるようになった場合、その IP アドレスを利用して攻撃が行われる場合です。

d) レイム・デレゲーションの悪用：ドメインは DNS 階層のあるレベルから別のレベルに委任されます。多くの場合、最上位ドメインからそのドメインを登録する組織に委任されます。委任を設定する際には、ドメインの権限を持つ DNS サーバーを指定する必要があります。権限のないネームサーバーにゾーンを委任することをレイム・デレゲーション（Lame Delegation）と呼びます。レイム・デレゲーションは、場合によってはドメインの乗っ取りにつながる可能性があります。サブドメインが DNS のホスティングプロバイダーに委任され、そのドメインに対する DNS サービスの契約が失効した場合、脅威アクターは、委任されたサーバーを管理するプロバイダーと契約し、そのサブドメインを自分の管理下でホストすることで、サブドメインの解決を乗っ取ることができます。これにより、脅威アクターは解決リクエストを自分のインフラストラクチャにリダイレクトし、ドメイン名の良好な評判を利用することができます。。

e) 類似ドメインの悪用：脅威アクターは、類似ドメインやタイポスクワッティング・ドメインを広範囲に利用してターゲットの組織になりすまします。合法的な組織の肯定的な評判を利用することで、脅威アクターはフィッシングやマルウェアキャンペーンの成功率を大幅に高めます。これらの類似ドメインには、正規のドメインを微妙に変化されたものが含まれていたり、テキストやその他の文字の置換を使用して、合法的な組織が所有しているとユーザーに信じさせるようなドメインが登録される場合があります。

f) DGA と Ransomware-as-a-Service：ドメイン生成アルゴリズム（DGA）は、悪意のあるアクターがコマンド＆コントロール（C2）通信のために多数のドメイン名を生成し、マルウェアの配布と検出の回避を容易にします。Blackcat などの RaaS（Ransomware-as-a-Service）は、C2 通信に DNS を使用します。

4. DNS セキュリティのベストプラクティス

DNS の本来の目的は、ホストや IP アドレスのマッピング、メールルーティング情報などの情報を配布することであり、従来はネットワーク通信を保護するツールとは見なされていませんでした。しかし、DNS は今日ほぼすべてのネットワーク通信を可能にする上で重要な役割を果たしており、それらの通信を監視するだけでなく管理するための効果的なツールにもなっています。そのため、DNS セキュリティは、DNS インフラストラクチャとプロトコルの保護だけでなく、組織

1 https://www.cisa.gov/news-events/news/cisa-launches-its-protective-dns-resolver-general-availability-federal-agencies

2 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a
https://blogs.infoblox.com/threat-intelligence/dns-early-detection-breaking-the-blackcat-ransomware-kill-chain/

全体のセキュリティ戦略における重要なセキュリティ制御および主要な要素へと発展しました。「DNSSEC」（DNS セキュリティ拡張と呼ばれる特定のプロトコルの略）は、「DNS セキュリティ」というより広範な概念の一部に過ぎず、他のベストプラクティスと併せて実装する必要があることに注意すべきです。

次のセクションでは、DNS セキュリティのベストプラクティスにおいて考慮すべき、次の 3 つの重要な要素について議論します。

- プロテクティブ DNS の採用
- DNS プロトコルの保護
- DNS サービスおよびインフラストラクチャの保護

4.1 プロテクティブ DNS

プロテクティブ DNS は、DNS クエリと応答を分析し、脅威を軽減するためのアクションを実行するセキュリティ機能が強化された DNS サービスです。プロテクティブ DNS は、スパイウェアやウイルスを配信しようとするマルウェア、ランサムウェア、フィッシング、その他の Web リンク中心の攻撃を防ぎ、悪意のある Web サイトへのアクセスをブロックします。プロテクティブ DNS は、ベンダーからのサービスとして提供する、内部 DNS インフラストラクチャに導入する、またはその 2 つを組み合わせて提供することも可能です。外部から提供されるプロテクティブ DNS と内部に導入されたプロテクティブ DNS を組み合わせて使用することには、潜在的な利点があります。このアプローチはすべてのケースに適用できるわけではありませんが、実行可能な場合はこのハイブリッド方式を採用することをお勧めいたします。世界各国の政府によるプロテクティブ DNS プラットフォームの導入や、欧州連合の DNS4EU イニシアティブによって証明されるように、[3]プロテクティブ DNS の使用は DNS のベストプラクティスとなっています。

プロテクティブ DNS を採用することの成果には、以下が含まれます。

Blocking or redirecting harmful traffic in real time before malicious activity starts.

Blocking categories of traffic. This is typically traffic that doesn't conform to an organizations policies.

Visibility into real-time DNS query and response history for digital forensics.

Integration with an organization's wider security ecosystem.

Facilitating an organizations responsibility to comply with regulatory or contractual requirements for blocking traffic to disallowed sites.

3 https://www.joindns4.eu/
https://www.ncsc.gov.uk/information/pdns
https://www.forgov.qld.gov.au/information-and-communication-technology/cyber-security/cyber-security-services/system-and-email-hardening/protective-dns-service/implement-a-protective-dns-service
https://www.cisa.gov/resources-tools/services/protective-domain-name-system-resolver

a. threat intelligence とテレメトリ

組織の攻撃対象領域は絶えず拡大しているため、悪意のある通信について監視して、できるだけ早く阻止することが極めて重要です。DNS は、他のネットワーク技術が出現しても変わらず、組織からモバイル エンドポイント まで、あらゆる環境でユーザーを保護するのに適しています。さらに、DNS は脅威に対する最も早期の接続となることが多く、複雑な多段階攻撃を進行する前に阻止できます。セキュリティ制御ポイントとしての DNS は、セキュリティスタック内の他のメカニズムとは異なり、単一の種類の脅威に限定されません。詐欺、資格情報の盗難、ランサムウェア、データの持ち出しからユーザーと組織を保護できます。

このアプローチには、threat intelligence とそれを DNS リゾルバーに統合する能力が必要です。threat intelligence は、レスポンスポリシーゾーン（RPZ）などのメカニズムを通じて DNS インフラストラクチャで活用され、さまざまなアーキテクチャを通じて DNS 解決チェーンにシームレスに統合できます。

b. 名前解決フィルタリング

名前解決フィルタリングとは、DNS 解決にポリシーを適用する DNS インフラストラクチャを指す用語です。これらのポリシーは通常、セキュリティに関連しています。たとえば、プロテクティブ DNS の実装では、フィッシング・キャンペーンで使用されることが知られているドメイン名や、マルウェアのコマンド・アンド・コントロールインフラストラクチャを識別するドメイン名の解決を拒否することがあります。プロテクティブ DNS は、これらのドメイン名を IP アドレスや他の種類のデータに解決する代わりに、通常、NXDOMAIN（「存在しないドメイン」を意味する）などの他の形式の DNS 応答を返し、検索されているドメイン名が存在しないことを示します。プロテクティブ DNS の実装は、ポリシーをトリガーするドメイン名のクエリをログに記録します。これらのクエリはマルウェアによる感染やその他の悪意のある活動を示す可能性があるからです。

プロテクティブ DNS は、通常、オンプレミスの DNS サービスに構成された RPZ、クラウドベースの安全な再帰 DNS サービス、またはその 2 つの組み合わせを使用して実装されます。

安全な再帰 DNS サービスもインターネット上で利用可能です。サービスは通常、ウェブベースのコントロールパネルを提供することで、管理者が組織のクライアントからの問い合わせに適用される解決ポリシーをカスタマイズできるようにします。クラウドアプローチでは、より高いスケーラビリティ、ストレージ、演算処理能力を提供しますが、機密性の損失、より高いレイテンシ、および DNS クエリを迅速かつ正確にその発信元に帰属させる際の課題などの欠点があります。組織は、オンプレミスとクラウドベースのセキュア DNS サービスを組み合わせて使用し、それぞれのメリットを享受することを検討できます。特定の DNS デプロイメントにおける最適な選択は、ネットワークとその利用者の具体的なニーズに応じて異なります。

c. デジタルフォレンジックおよびインシデント対応のための DNS

政府機関および規制対象企業は、コンプライアンス要件を満たすために、DNS トラフィックのロギングを行う堅牢なメカニズムを実装する必要があります。ロギングは、デジタルフォレンジックおよびインシデント対応を可能にするために、現在および過去両方の DNS トラフィックを記録する必要があります。これらの DNS ログは、他のシステムログと統合され、ネットワークアクティビティの他のログとの相関を容易にし、可視性と監査可能性を向上させる必要があります。

完全なDNSトラフィックロギングがリソース集約型であると判断された場合、組織はクラウドベースのソリューション、効率的なロギング方法（例：DNSTAP）、または選択的ロギングを検討することができます。しかし、セキュリティおよびコンプライアンスの目的を支援するために、プロテクティブ DNS サービスによって悪意のあるまたは許可されていないと分類されたドメインに関連するDNSクエリと応答は常に記録されることが不可欠です。感染や悪意のある活動を示す可能性のあるクエリを迅速に通知するために、組織はネームサーバーまたはセキュアな再帰DNSサービスからのプロテクティブ DNSログをSIEMまたはログ分析プラットフォームと統合する必要があります。

4.2 DNS プロトコルの保護

DNS プロトコルは、Web ブラウジング、メール、その他のミッションクリティカルアプリケーションを可能にするために、サービスを見つける上で不可欠です。その結果、次世代ファイアウォールなどの従来のセキュリティプラットフォームは、DNS トラフィックを制限も検査もすることなく通過させることがよくあります。脅威アクターは、データ流出の手段として DNS を利用することが増えています。米国サイバーセキュリティ・社会基盤安全保障庁（CISA）は、「DNS インフラストラクチャは攻撃キャンペーンにおいて一般的な脅威ベクトルである」と述べています。[4] 脅威アクターは、盗まれたデータを DNS パケットに埋め込み、DNS インフラストラクチャを利用して、脅威アクターが管理する DNS サーバーにそのデータを中継することがよくあります。 DNS プラットフォームは、データの流出の試みで受信した再帰的 DNS リクエストを評価するのに理想的な位置にあります。

a. DNSサービスの整合性を保護する

DNS プロトコルの整合性を保護することは、インターネット通信のセキュリティと信頼性を確保するために重要です。DNS セキュリティ拡張 (DNSSEC) は、暗号署名を用いて DNS 応答を認証し、キャッシュポイズニングや中間者攻撃を防ぐ重要な役割を果たします。さらに、トランザクション署名 (TSIG) は、共有秘密鍵を使用してゾーン転送と動的更新を不正な変更から保護し、DNS サーバー間の相互認証と整合性検証を可能にすることで、DNS セキュリティを強化します。これらのメカニズムを、レート制限、異常の監視、厳格なアクセス制御の実施などのベストプラクティスとともに実装することで、進化するサイバー脅威に対する DNS インフラストラクチャの信頼性と回復力を維持するのに役立ちます。さらに、組織は、ユーザーが意図的または不注意に許可されていない公開インターネットベースの DNS サービスを使用しないように確認する必要があります。

b. プロトコルを保護するための暗号化された DNS と認証の使用

スタブリゾルバーとそれが照会する再帰的DNSサーバーとの間の通信は、従来、暗号化されていませんでした。スタブリゾルバーとDNSサーバーが交換するDNSメッセージはバイナリエンコーディングですが、そのエンコーディングは広く理解されており、簡単にデコードできます。したがって、この通信は傍受とスプーフィングの両方の対象となっており、機密情報が漏洩したり、攻撃者が疑いのないユーザーを悪意のあるサイトにリダイレクトしたりする可能性があります。

これらの脅威に対処するために、Internet Engineering Task Force（IETF）は、一般に暗号化 DNS と総称される DNS に対するいくつかの拡張機能を開発しました。これらのプロトコルはすべて、スタブリゾルバーと再帰 DNS サーバー間の通信を暗号化し、オプションで再帰 DNS サーバーがスタブリゾルバーに対して自らを認証できるようにし、傍受やなりすましの脅威に対処します。

c. DNS のハイジーンとベストプラクティス

設定ミスやドメイン/DNSリゾルバーの登録失効の悪用は、脅威アクターにとって比較的容易に実行でき、DNSの整合性が深刻に損なわれる可能性があります。

脅威アクターは、フィッシングなどの攻撃が信頼できる組織が所有するドメインに関連付けられている場合、成功する可能性がはるかに高いことを証明しています。その結果、彼らは、標的組織に所有されていないが、類似したドメインを登録することがよくあります。さらに懸念すべきは、権威あるドメインの衛生安全管理が不十分であると、脅威アクターが信頼された組織の所有するドメインを乗っ取る可能性があることです。

4.3 DNS サービスおよびインフラストラクチャの保護

DNS アプライアンスは、他のネットワークアプライアンスと同様に、管理の容易さ、セキュリティ、パフォーマンスのために最適化された専用アプライアンスです。汎用サーバーは、これらのアプライアンスが提供するチューニングには及ばず、そのため、ネットワークサービスとしての DNS の重要性を考慮すると、組織は重大なリスクにさらされることになります。

4 https://www.cisa.gov/news-events/news/cisa-launches-its-protective-dns-resolver-general-availability-federal-agencies

組織では一般的に、DNS や DHCP をホストする Windows サーバーを、非常に重要なアイデンティティインフラである Active Directory（AD）と併用しています。AD はユーザーのアクセスと権限を管理し、重要な情報を保存するため、大きな攻撃対象領域を作り出し、サイバー攻撃に対して脆弱性があります。

この職務分離がない場合、攻撃者が一般的なエスカレーションパスをたどり、Active Directory を標的にすると、DNS サービスとそれに依存するネットワークが危険にさらされます。DNS が組織のサイバーセキュリティ戦略でより重要な役割を果たすようになると、専用の DNS サーバーはこれらのリスクを軽減するために不可欠になります。

同様に、脅威アクターは、DNS システムの整合性に影響を与えたり、サービス拒否を引き起こしたりする可能性のある、DNS で発見された脆弱性を悪用しようとすることがよくあります。

安全なDNSに関するさらなるガイダンスについては、最新のNIST SP 800-81: Secure Domain Name System (DNS) デプロイメントガイドを参照してください。

5. まとめと推奨事項

このホワイトペーパーでは、組織のデジタル弾力性とサイバーセキュリティを維持する上での DNS インフラストラクチャの重要性について解説します。本書では、DNS サーバーが十分な容量を持ち、最適に構成されていることを確認するために、定期的な評価の必要性を強調しています。また、サイバーセキュリティ・アーキテクチャの基盤レイヤーとしての DNS を活用することで、そのインフラストラクチャを利用するすべてのクライアントにメリットとなることも強調されています。

進化する DNS セキュリティの脅威に対処するために、ネットワークおよびセキュリティの担当者に次の高レベルの推奨事項を提示します。

- 技術的に可能な限り、プロテクティブ DNS を導入し、ネットワーク全体に以下を含む追加のセキュリティ機能を提供しましょう。
  - » 有害または悪意のあるトラフィックをリアルタイムでブロックする
  - » 組織のポリシーに準拠していないカテゴリのトラフィックをフィルタリングする
  - » デジタルフォレンジックおよびインシデント対応を支援するための、リアルタイムおよび過去の DNS クエリと応答データ。
  - » 多層防御またはゼロトラストアプローチの一環として、より広範なセキュリティエコシステムとの統合
  - » 許可されていないサイト（著作権違反、法的制限など）へのトラフィックをブロックするための規制または契約上の要件を遵守する組織の責任を促進すること。
- 可能な限り、内部および外部の DNS トラフィックを暗号化してください。
- 攻撃対象領域を減らすために専用の DNS サーバーを導入してください。
- DNS の展開と DNS プロトコルが可能な限り安全で回復力があることを確保するためのすべての技術的指導に従ってください。

追加情報については、Infoblox チーム（ga@infoblox.com）までお問い合わせください。

Infoblox株式会社
〒107-0062 東京都港区南青山2-26-37
VORT外苑前I
3F

03-5772-7211
www.infoblox.com

バージョン：20250131v3