DNSにおけるアクセス制御の一検討

4H－02

山岡 正輝　田中 俊介　松田 栄之
(株)NTTデータ 開発本部
e-mail: {yamaoka, shun, matu }@rd.nttdata.co.jp

1. はじめに

DNS(Domain Name System)は，インターネットにおいて IP アドレスを特定する重要な役割を担っている[1,2]. しかし，インターネットは，元来，研究者間の通信基盤として発展してきたという経緯もあり，共通基盤である DNS における不正利用対策は十分であるとはいえない. 特に，アクセス制御という観点からみると，基本的には，どの利用者からの問い合わせであっても問い合わせ対象の IP アドレスを回答するという仕組みが実現されており，セキュリティ上，問題となる可能性も考えられる.

そこで，本稿では，DNS の問い合わせ元を DNS サーバ側で認証し，認証結果によって IP アドレスを回答するか否かを決定するアクセス制御機能をもった DNS を提案する.

2. DNSにおけるセキュリティ対策と問題点

現在のインターネットでは，基本的には，どの利用者からの問い合わせであっても問い合わせ対象の IP アドレスを回答するという DNS の仕組みが実現されている. しかしながら，すべての DNS 問い合わせに対して無制限に IP アドレスを回答することは，不正アクセスにつながるきっかけを与えることになりかねない. 特に，企業内や家庭などでネットワーク内のセキュリティを確保したい場合には，企業内や家庭の機器がもつIPアドレスを外部からは知ることができないように DNS を設定することが望まれる.

企業内や家庭の機器がもつ IP アドレスを外部からは知ることができないようにDNSを設定する方法には，bind8 に実装されているアクセス制御機能[3]を用いる方法がある. IPアドレスによって問い合わせ元を識別し，識別結果に基づいて DNS サーバでゾーン単位のアクセス制御を実現している.

しかしながら，DHCP 等による IP アドレスの動的付与を用いてネットワークに接続する場合には，同じIPアドレスであっても時間によって利用者が異なる可能性なども想定される. したがって，利用者によってアクセスを制御することを考えた場合，IP アドレスにより問い合わせ元を識別する方法では，アクセス制御リストの維持が困難になることが予想される. また，単なる識別では，成りすましに対抗できないという問題も生じる. さらに，ゾーン単位でのアクセス制御では，同一の DNS ゾーンに属する WWW サーバやメールサーバなどのサービスごとに DNS のアクセス制御を実現することが困難であるという問題もある. サービスごとの設定を可能にするためには，リソースレコード単位で設定できることが望ましい. 以上の DNS でのアクセス制御の現状を表1にまとめる.

表 1 DNS のアクセス制御の現状

問い合わせ元の識別	ゾーン単位のアクセス制御	リソースレコード単位のアクセス制御
IP アドレスによる識別	○	×
ユーザ名による識別	×	×

(○:現状の DNS で実現可能，×:現状の DNS では実現不可能)

3. 提案する DNS のアクセス制御方式

本稿では，IP アドレスまたはユーザ名を用いて DNS サーバ側で問い合わせ元を認証でき，かつ，認証結果に基づいてリソースレコード単位でアクセス制御設定が可能な DNS を提案する. 以下，提案する DNS をアクセス制御機能付き DNS(AC-DNS)と呼ぶ.

3.1. DNS 問い合わせ元の認証方式

サーバ側がクライアントを認証する方式としては，チャレンジレスポンス方式や時刻同期方式，カウンタ同期方式があげられる. 時刻同期方式やカウンタ同期方式は，チャレンジレスポンス方式に比べて，サーバ側で生成した乱数値をクライアントに送信する手間が省けるという利点がある. しかし，不特定のサーバやクライアント間での通信によって全体が構成されている DNS において同期をとることは難しく，適用しがたい.

本稿で提案する AC-DNS では，チャレンジレスポンス方式を採用する. まず，DNS サーバ側でチャレンジデータを生成し，クライアントリゾルバに送信する. クライアントリゾルバでは，受け取ったチャレンジデータに対して IP アドレスまたはユーザの秘密鍵により署名を施して DNS サーバに送信する. DNS サーバでは，クライアントの IP アドレスまたはユーザに対応する公開鍵によって署名を検証する. これによって，DNS サーバ側で DNS 問い合わせ元の認証を行うことができる.

A study of DNS access control
Masaki YAMAOKA, Shunsuke TANAKA and Shigeyuki MATSUDA,
Research and Development Headquarters, NTT DATA CORPORATION

クライアントリゾルバと AC-DNS サーバ間の処理フローを図 1に示す. 処理は, 既存の DNS プロトコルに従った DNS 問い合わせ回答フェーズと, 提案する AC-DNS プロトコルに従った AC-DNS 問い合わせ回答フェーズとから構成される. DNS 問い合わせ回答フェーズで DNS 回答が返却された場合には, AC-DNS 問い合わせ回答フェーズは実行されない. また, DNS 問い合わせ回答フェーズを先に実行することで, クライアントリゾルバが AC-DNS 対応でない場合でも対応可能となる.

【DNS 問い合わせ回答フェーズ】

クライアントリゾルバが AC-DNS サーバに対して DNS 問い合わせを出す. AC-DNS サーバでは, 問い合わせの対象となっているリソースレコードのアクセス制御リスト(Access Control List : ACL)をチェックし, 問い合わせの対象となっているリソースレコードがアクセス制御されている場合, DNS 回答をせず, クライアントリゾルバに AC-DNS 対応通知を出す. アクセス制御されていない場合, DNS 回答を返却する.

【AC-DNS 問い合わせ回答フェーズ】

クライアントリゾルバが AC-DNS サーバに対してチャレンジデータ要求を出す. チャレンジデータ要求を受け取った AC-DNS サーバは, チャレンジデータをクライアントリゾルバに送信する. クライアントリゾルバは, チャレンジデータに対して IP アドレスまたはユーザの秘密鍵により署名を施し, AC-DNS サーバに署名を付与した AC-DNS 問い合わせを出す. AC-DNS サーバは, IP アドレスまたはユーザに対する公開鍵を用いて署名を復号化し, 得られたデータが自らが発したチャレンジデータと等しいかをチェックすることによって署名を検証し, DNS 問い合わせ元を認証する. AC-DNS サーバは, 認証結果を元に, 問い合わせ対象のリソースレコードに対する ACL をチェックし, ACL に基づいた DNS 回答をクライアントリゾルバに返却する.

3.2. 認証結果に基づくアクセス制御方式

認証結果に基づいてリソースレコード単位でアクセス制御設定が可能な方式を提案する.

リソースレコード単位でアクセス制御設定するために, ゾーンファイルの TXT リソースレコードにアクセス制御リストを格納する. アクセス制御リストでは, ポジティブリスト方式を採用し, アクセスを許可する IP アドレスまたはユーザ名を記述する. 図 2に TXT リソースレコードに記述するアクセス制御リストの例を示す. この場合, ホスト名 mail に対する MX レコードの DNS 問い合わせに対しては, 問い合わせ元が 10.8.1.0/24 の IP アドレスの場合は, ゾーンファイルに書かれている MX レコードの値を DNS 回答として返却する. しかし, それ

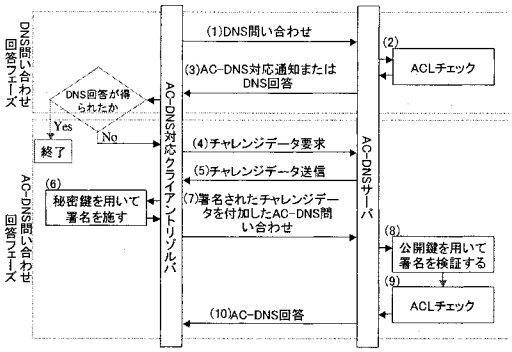

図 1 AC-DNS の処理フロー

```
mail    IN TXT "ACL MX host 10.8.1.0/24"
video   IN TXT "ACL A user Hiiroshi"
camera  IN TXT "ACL A user Takashi"
```

図 2 アクセス制御リストの例

以外の IP アドレスからの問い合わせの場合には, MX レコードの値を返さない.

このように, アクセス制御リストをゾーンファイルに記述することにより, DNS のゾーン転送によりセカンダリ DNS サーバにもアクセス制御リストが転送され, プライマリ DNS サーバとセカンダリ DNS サーバ間でのアクセス制御リストの同期に対する特別な措置は不要となるなどのメリットも生じる.

以上の方式により, IP アドレスまたはユーザ名による DNS 問い合わせ元の認証, および, リソースレコード単位でのアクセス制御を実現することが可能となる.

4. まとめ

DNS の問い合わせ元を IP アドレスまたはユーザ名により DNS サーバ側で認証する方式, および, 認証結果に基づいて DNS 回答を返却するか否かを決定する DNS のアクセス制御方式を提案した. 今後, ローカル DNS サーバが介在した場合の認証方式を検討し, アクセス制御機能付き DNS を実装する予定である.

謝辞

本研究は, 通信・放送機構(TAO)の委託研究テーマ「次世代 DNS に関する研究開発」の一環として行われているものです.

参考文献

[1] RFC 1034, "Domain names – concepts and facilities", 1987 年.

[2] RFC 1035, "Domain names – implementation and specification".1987 年.

[3] DNS&BIND 第3版, オライリージャパン, 1999 年.