Empowered by Innovation NEC

Internet Week 2014 DNSのセキュリティ
ブロードバンドルータにおける問題（オープンリゾルバ）の解説、対策の説明

2014年 11月 20日

NECプラットフォームズ株式会社

開発事業本部 アクセスデバイス開発事業部

川島 正伸

目次

- 世間が注目！？　家庭用ルータが引き起こすネット障害
- ブロードバンドルータにおけるDNSプロキシ機能とは？
- DNSプロキシ機能の必要性
- オープンリゾルバ問題
- オープンリゾルバによるDNSリフレクター攻撃
- オープンリゾルバによるDNS水責め攻撃
- なぜオープンリゾルバになってしまうのか？
- 対策方法
- 課題
- ブロードバンドルータとDNSのセキュリティに関連する話

はじめに

- ブロードバンドルータにおけるDNS実装は各社により多様であり、また同一ベンダ内であっても機種やバージョンによって仕様が異なるケースもある為、本資料では近年の一般的な状況について説明しています。

- また、通信事業者の提供しているホームゲートウェイ等は各社の考え方、個別事情を反映した仕様になっているケースが多い為、本資料のスコープ外としています。

世間が注目！？　家庭用ルータが引き起こすネット障害

- Cloudflareのプレゼン「The curse of the Open Recursor」
  日本がオープンリゾルバ数で、アジアワースト1になっている。
  ブロードバンドルータによる影響も確認された。
  [2013/02/26　APRICOT 2013]

- JPNIC, JPRS, JPCERT/CC からオープンリゾルバに関する注意喚起
  [2013/04/18]

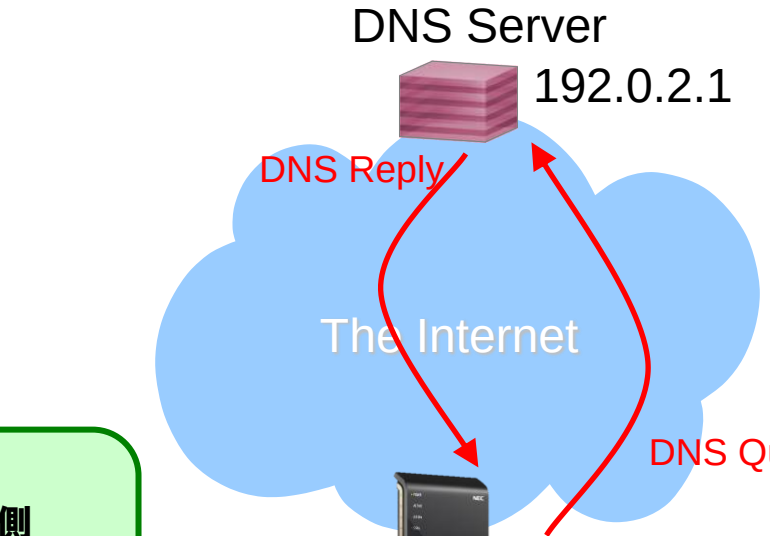
- 複数のブロードバンドルータがオープンリゾルバとして機能してしまう問題
  JVN#62507275　*[2013/09/19　JVN(Japan Vulnerability Notes)]*

- 2400万台の家庭用ルーターがDNSベースのDDoS攻撃に悪用可能、Nominum調査　*[2014/04/04　Internet Watch]*

- 日本国内のオープン・リゾルバを踏み台としたDDoS 攻撃発生に起因すると考えられるパケットの増加について
  [2014/07/23　警察庁 Cyber police]

- ルータ攻撃 ネット障害 480万世帯に影響　*[2014/08/02　読売新聞朝刊]*

ブロードバンドルータにおけるDNSプロキシ機能とは？



一般的に、
DHCPを使用してルータのLAN側IPアドレスをDNSサーバアドレスとしてホストに通知する。
（≠ISPのキャッシュDNSサーバアドレス）

DHCP

DNSプロキシ機能

DNS Reply

.254

192.168.1.0 / 24

.1

DNS Query

IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0
DNS Server : 192.168.1.**254**

エンドユーザ

ホストのDNS問合せ先は、ルータのLAN側IPアドレス宛となる。つまり、ホストからはルータがDNSサーバにみえる。

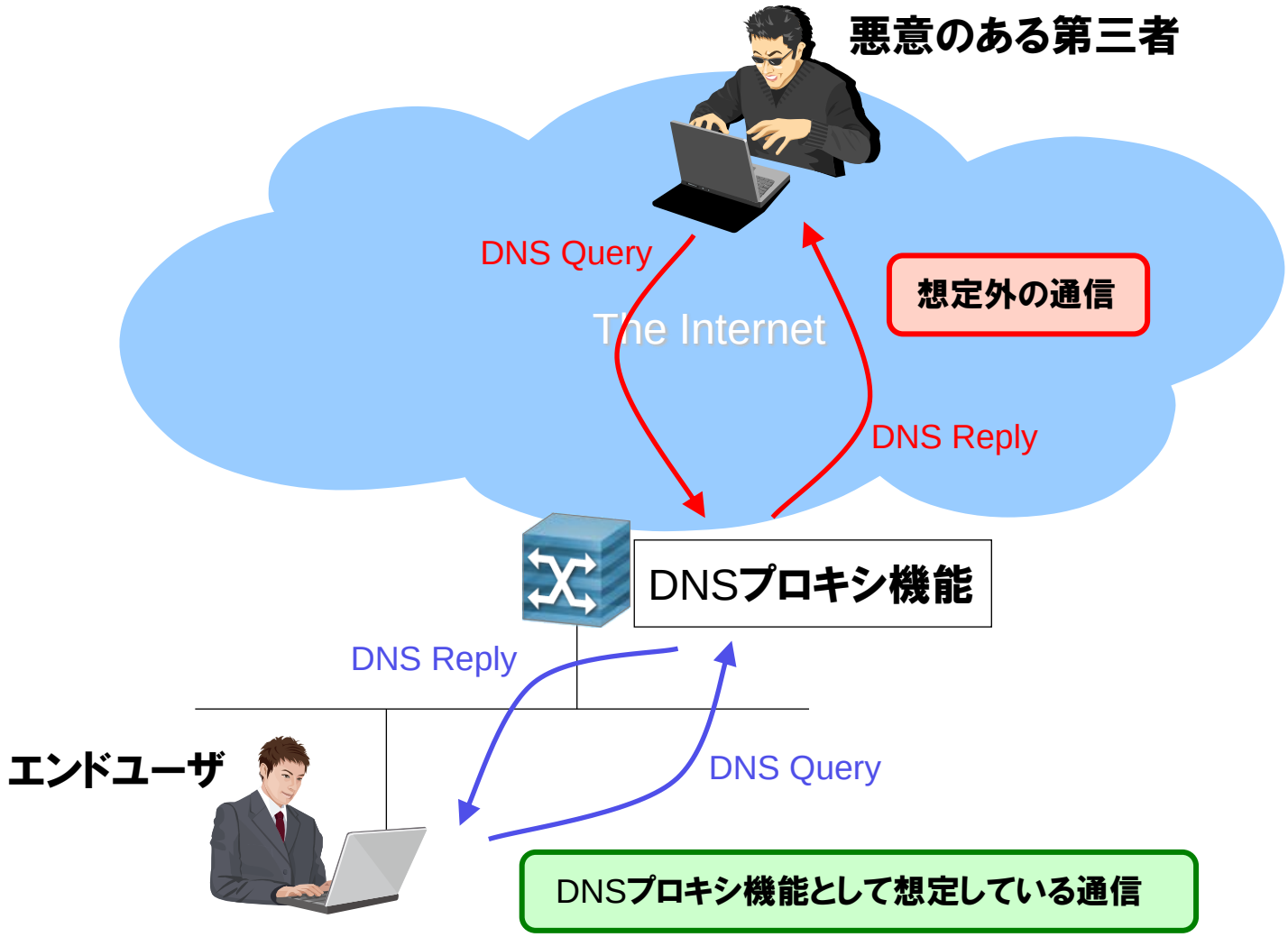
名前解決依頼・応答を中継するDNSプロキシ（フォワーダ）として動作

DNSプロキシ機能の必要性

- WAN側のInternet接続が確立する前に（もしくはWAN側状態によらず）、LAN側のホストにDNSサーバアドレスを通知することで、Web-GUI（ユーザインタフェース）へのアクセスが可能。
  - 専用のFQDNを使用してアクセスすることで、ユーザの利便性、サポート容易性を考慮。
    - IPアドレス直打ちよりもわかりやすく、一般ユーザには敷居が低い。
    - IPv6アドレスの場合、直打ちは困難。
      - fe80::1 などとしてもユーザにはなんだかサッパリわからない。☹

- 複数の接続先が存在する場合におけるDNSサーバ選択問題回避
  - インターネット接続とフレッツ網接続など、DNSの管理ドメインが異なる複数の接続先がある場合、DNSプロキシ機能が適切なDNSサーバへ問合せを行う。
    - DNSプロキシ機能を提供しなかった場合、ホスト側で適切なDNSサーバを選択できない問題がある。

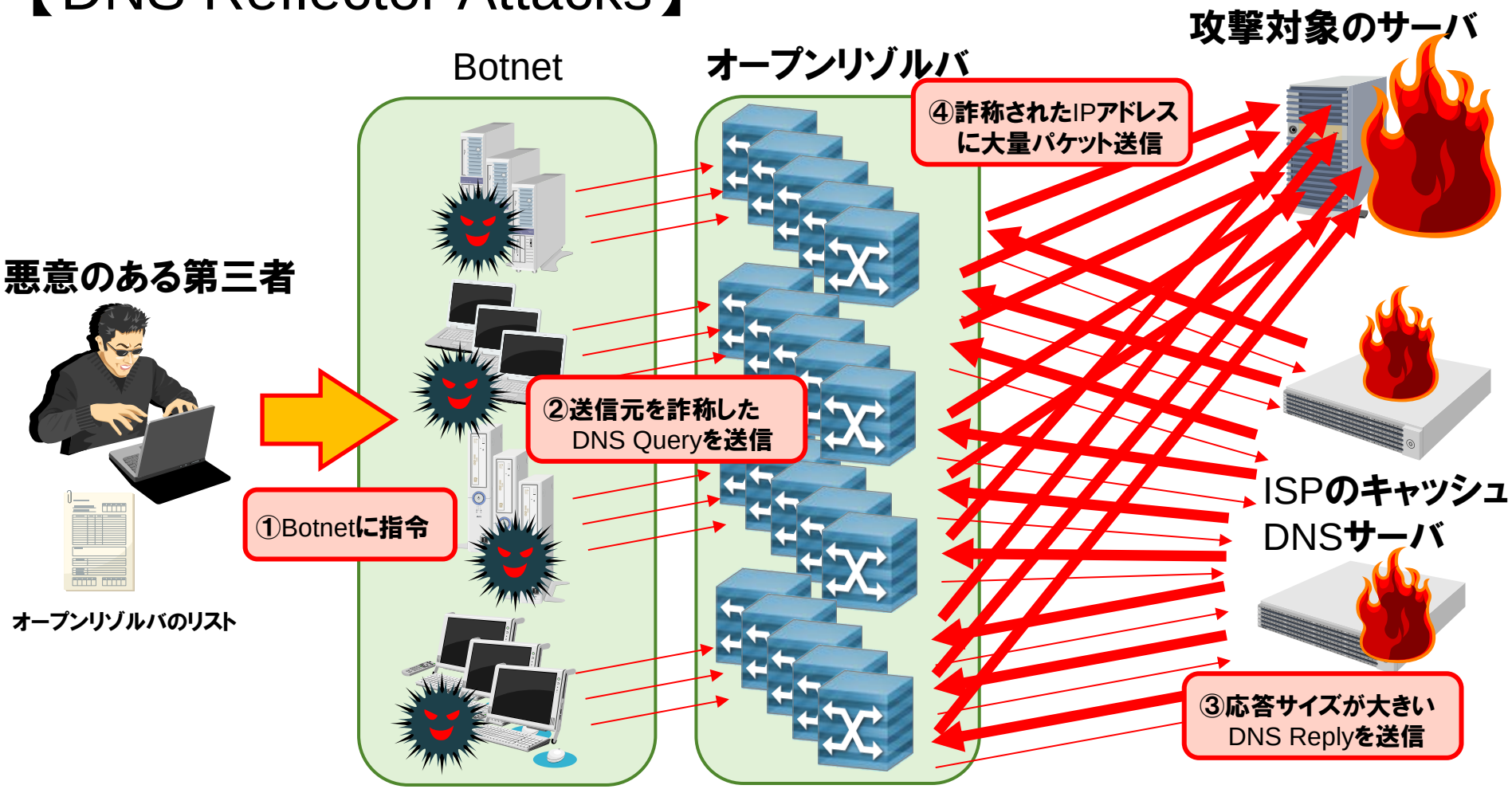
オープンリゾルバ問題



DNSプロキシ機能の意図に反して、WAN側からのDNS Queryに応答してしまう問題

オープンリゾルバによるDNSリフレクター攻撃

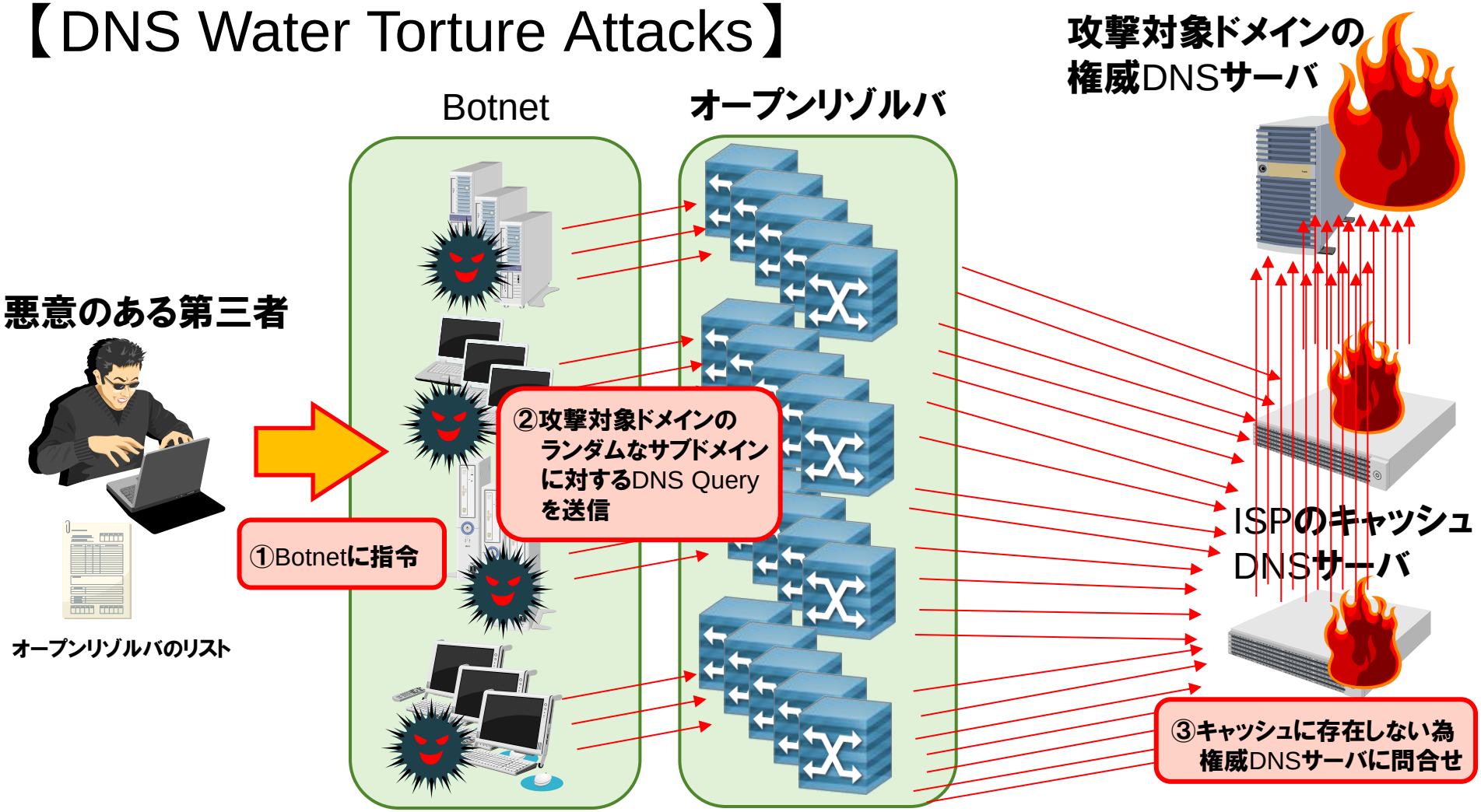
【DNS Reflector Attacks】



アドレス詐称およびDNS応答が大きくなるようなQueryを送信して攻撃対象を狙うDoS攻撃

オープンリゾルバによるDNS水責め攻撃

【DNS Water Torture Attacks】



攻撃対象ドメインに存在しないランダムなサブドメインに対するQueryを送信するDoS攻撃

なぜオープンリゾルバになってしまうのか？

そもそも、なぜブロードバンドルータがオープンリゾルバになってしまうの？

PPPoE接続でNAT利用しているような一般的な使い方をしているケースでは、オープンリゾルバにはなりません。

では、どんな条件下で発生するの？

エンドユーザが設定変更により、
WAN側からのDNS要求に応答するように
意図的に設定しているケース

製品の動作条件や設定内容と、
ISPとの接続方式との組合せ条件により、
オープンリゾルバとなってしまうことがある。

**いち早く発生条件を特定した上で、
対策方法の迅速な提供が必要。**

対策方法

適切なアクセスコントロールの実施（ベンダ／エンドユーザ双方で実施可）

- WAN側からのDNS問合せに応答しない
  - ブロードバンドルータでは基本的にLAN側からのDNS問合せに応答すれば、DNSプロキシ機能として必要十分である。

送信元検証（Source Address Validation）の実施（ベンダ／エンドユーザ双方で実施可）

- 詐称された送信元IPアドレスによる通信を許可しない
  - RFC2827[BCP38] Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing の適用

上記対策の施された最新ファームウェアを提供（ベンダとしての根本対策）

課題

ベンダが対策済ファームウェアを提供しただけでは対策にならない

- 実際にエンドユーザが対策済ファームウェアを適用するまで問題は未解決
  - ファームウェアのオンラインバージョンアップ機能を使って対策ファームウェアを適用できるケースもあるが、ユーザの設定内容に依存。

古い機種、オンラインバージョンアップ機能を設定していないケースではベンダだけでは対処できない。

- メディアや業界コミュニティと連携してユーザ啓蒙活動も必要？
  - オープンリゾルバ確認サイトでの確認など。
- 攻撃の深刻度によっては、ISPや通信事業者とベンダとが情報共有を行いつつ、IP53B(Inbound Port 53 Blocking)の適用も視野に。

ブロードバンドルータとDNSのセキュリティに関連する話

DNSプロキシ機能におけるキャッシュの必要性

- キャッシュヒットによるレスポンスタイム短縮が近年の高速回線化により、大きなメリットにならない
- カミンスキー攻撃に代表されるキャッシュポイズニング攻撃の対策などに追従していくのは得策ではない。（労多くして功少なし）

名前衝突(Name Collision)問題への対処

- 新gTLDの委任開始に伴い、衝突ドメインにおけるサービス利用不可や情報漏えいのリスクがある為、衝突リスクのあるドメインを使用せず、正式にドメインを取得するなどの対応が求められる。

最後に

- DNSは複数の構成要素から成り立っているシステムであり、ベンダだけでセキュリティ対策できるものではない。

- ベンダは、ISPや通信事業者との連携はもちろんのこと、業界コミュニティを通じた情報共有、議論を積極的に行うことで、DNSのセキュリティ維持や品質向上に努めるべきである。

Orchestrating a brighter world

世界の想いを、未来へつなげる。

未来に向かい、人が生きる、豊かに生きるために欠かせないもの。
それは「安全」「安心」「効率」「公平」という価値が実現された社会です。

NECは、ネットワーク技術とコンピューティング技術をあわせ持つ
類のないインテグレーターとしてリーダーシップを発揮し、
卓越した技術とさまざまな知見やアイデアを融合することで、
世界の国々や地域の人々と協奏しながら、
明るく希望に満ちた暮らしと社会を実現し、未来につなげていきます。

Empowered by Innovation

NEC