Internet Week 2015
D1 DNS DAY

セキュリティ関連の話題（脆弱性対応・攻撃対応）

2015年11月19日

一般財団法人日本データ通信協会
テレコム・アイザック推進会議
Telecom-ISAC Japan
齋藤　和典

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

脆弱性対応

ここ1年の脆弱性情報

		概要
2014/12/09	BIND	Geo IP機能を有効にしている場合にBIND 9.10.xが停止
2014/12/09	BIND Unbound PowerDNS	悪意のある委任設定により、CPU、メモリ等のシステム資源の過度な消費。
2015/02/19	BIND	DNSSEC検証を有効にしている場合にBIND 9.Xが停止
2015/04/27	PowerDNS	外部からの攻撃によりPowerDNS Authoritative Server、PowerDNS Recursorが停止
2015/07/08	BIND	DNSSEC検証を有効にしている場合にBIND 9.Xが停止
2015/07/29	BIND	外部からの攻撃によりBIND 9.Xが停止
2015/09/03	BIND	外部からの攻撃によりBIND 9.10.2/9.9.7が停止
2015/09/03	BIND	DNSSEC検証を有効にしている場合にBIND 9.Xが停止
2015/09/03	PowerDNS	外部からの攻撃によりPowerDNS Authoritative Serverが停止
2015/11/11	PowerDNS	外部からの攻撃によりPowerDNS Authoritative Serverが停止

（http://jprs.jp/tech/より抜粋）

7/29のBIND 9の脆弱性に関する動き

■ 概要

ISC社のアナウンスを受け、JPRSは（緊急）として注意喚起を実施している。

対象はBIND 9.1.0以降の全てのバージョンとしており、加えてキャッシュDNSサーバ及び権威DNSサーバの双方が対象となることから、対象が広範囲に渡ることが懸念されており、速やかな対応が強く推奨されている。

対策では、設定やパケットのスクリーニングによる回避は難しいことから、ISC社より提供されている脆弱性を修正したパッチバージョンの適用や、ディストリビュータが今後リリースするパッチの適用が求められている。

８月4日現在、カゴヤジャパンおよび株式会社21Companyより、本脆弱性を利用した攻撃により同社が運用DNSサービスが停止したとの障害情報が発表されている。

時刻	概要	URL
2015/7/28 10:00（US時間）	ISC社より脆弱性情報のアナウンス	https://kb.isc.org/article/AA-01272
2015/7/29 11:10	JPRSより注意喚起	http://jprs.jp/tech/security/2015-07-29-bind9-vuln-tkey.html
2015/7/29（US時間）	PoC公開	
2015/7/31 00:45	カゴヤジャパンの運用するDNSサーバに対して脆弱性を利用した攻撃の発生	http://www.kagoya.jp/news/201507315891.html
2015/7/31 00:45	Fitコールの運用するDNSサーバに対して脆弱性を利用した攻撃の発生	http://fitcall.ne.jp/info/fault/15/07/31_120502.shtml
2015/7/31 22:03	株式会社21Companyの運用するDNSサーバに対して脆弱性を利用した攻撃の発生	http://faq.21-domain.com/index.php?action=news&newsid=143&newslang=ja

各社の動向

ISC Knowledge Base

Home
Favo

Search the Knowledgebase

Search | Advanced Search

Top → Software Products → BIND9 → Security Advisories

CVE-2015-5477: An error in handling TKEY queries can cause named to exit with a REQUIRE assertion failure

Author: **Michael McNally** Reference Number: **AA-01272** Views: **28591**
Created: **2015-07-28 10:00** Last Updated: **2015-07-30 23:27**

75 Rating/ 2 Voters ★★★☆☆

A deliberately constructed packet can exploit an error in the handling of queries for TKEY records, permitting denial of service.

CVE:	CVE-2015-5477
Document Version:	2.1
Posting date:	28 July 2015
Program Impacted:	BIND
Versions affected:	9.1.0 -> 9.8.x, 9.9.0->9.9.7-P1, 9.10.0->9.10.2-P2
Severity:	Critical
Exploitable:	Remotely

Description:

An error in the handling of TKEY queries can be exploited by an attacker for use as a denial-of-service vector, as a constructed packet can use the defect to trigger a REQUIRE assertion failure, causing BIND to exit.

Impact:

Both recursive and authoritative servers are vulnerable to this defect. Additionally, exposure is not prevented by either ACLs or configuration options limiting or denying service because the exploitable code occurs early in the packet handling, before checks enforcing those boundaries.

All versions of BIND 9 from BIND 9.1.0 (inclusive) through BIND 9.9.7-P1 and BIND 9.10.2-P2 are vulnerable.

Operators should take steps to upgrade to a patched version as soon as possible.

CVSS Score: 7.8

CVSS Vector: (AV:N/AC:L/Au:N/C:N/I:N/A:C)

For more information on the Common Vulnerability Scoring System and to obtain your specific environmental score please visit:
https://nvd.nist.gov/cvss.cfm?calculator&version=2&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:C)

(出典) https://kb.isc.org/article/AA-01272

■（緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（2015年7月29日公開）
- フルリゾルバー（キャッシュDNSサーバー）／権威DNSサーバーの双方が対象、バージョンアップを強く推奨 -

株式会社日本レジストリサービス（JPRS）
初版作成 2015/07/29（Wed）

▼概要

BIND 9.xにおける実装上の不具合により、namedに対する外部からのサービス不能（DoS）攻撃が可能となる脆弱性が、開発元のISCから発表されました。本脆弱性により、提供者が意図しないサービスの停止が発生する可能性があります。

本脆弱性は、BIND 9.1.0以降のすべてのバージョンのBIND 9が対象となり、かつフルリゾルバー（キャッシュDNSサーバー）及び権威DNSサーバーの双方が対象となることから、対象が広範囲にわたっています。該当するBIND 9.xを利用しているユーザーは関連情報の収集やパッチの適用など、適切な対応を速やかに取ることを強く推奨します。

（2015年7月29日追加）ISCの公式ブログに、本脆弱性に関する追加情報が掲載されました。こちらには、

・設定や利用条件に限定されず、ほぼすべてのBINDが対象となること
・ファイアーウォールで問題のパケットをスクリーニングすることは困難、または不可能である可能性が高いこと
・本脆弱性のリバースエンジニアリングが難しくないこと
・既に、リバースエンジニアリングに成功したセキュリティ専門家から、攻撃キットの作成成功を伝えられていること

が記述されており、速やかなパッチの適用、または修正済バージョンの入手・更新を呼び掛けています。

▼詳細

▽本脆弱性の概要

TKEYは、DNSのトランザクションをやりとりする2台のホスト間で用いる秘密鍵（共有鍵）を自動生成するための機能で、RFC 2930で定義されています。

BIND 9.xにはTKEYリソースレコード（RR）の取り扱いに不具合があり、TKEY RRに対する特別に作成された問い合わせにより、namedが異常終了を起こす障害が発生します（*1）（*2）。

(出典) http://jprs.jp/tech/security/2015-07-29-bind9-vuln-tkey.html

障害発生状況

- カゴヤジャパン、株式会社21Companyより、以下のような障害が発生したことが発表されている

KAGOYA JAPAN

障害情報2015年07月31日

ビジネスパートナー | 障害・メンテナンス情報 | 会社概要 | Google™カスタム検索 | 検索

共用サーバー | マネージド専用サーバー | クラウド型専用サーバー | VPS | root権限付専用サーバー | データセンター

TOP > 障害・メンテナンス情報 > 【重要：11888】DNSサーバー障害発生と復旧のお知らせ（7月31日午前11時更新）

障害情報

前の情報　次の情報

【重要：11888】DNSサーバー障害発生と復旧のお知らせ（7月31日午前11時更新）

2015年07月31日

平素は当社サービスをご利用いただき誠にありがとうございます。
7月31日0時45分頃より当社DNSサーバーにおきまして、名前解決ができない障害が発生いたしました。
本障害は1時25分に復旧しております。

==========
障害概要：当社権威DNSサーバーにおけるDNSサービスの停止
停止時間：7月31日0時45分より1時25分
影響内容：ご利用ドメインの名前解決ができないため、
　　サーバーへアクセスできない
原因　　：BIND 9.xの脆弱性(CVE-2015-5477)に対する攻撃
　　現在、原因であるBIND 9.xの脆弱性対応の準備を進めており、
　　準備が整い次第実施を予定しています。
　　実施日時決定次第、ご連絡いたします。
==========

この度、ご利用の皆様には大変ご迷惑をお掛けいたしましたこと
お詫び申し上げます。

(出典) http://www.kagoya.jp/news/201507315891.html

21-domain/21ip/ssl.ne.jp FAQお知らせ

BIND 9.xの脆弱性によるDNSサービスの障害のご報告

平素より弊社サービスをご愛顧頂き誠に有り難うございます。

2015年7月31日22時3分より発生しておりましたBIND 9.xの脆弱性
に関する障害につきまして、8月1日11時に名前解決が可能な状態と
なりました。

この度攻撃を受けたサーバにつきましては既に最新のバージョンへの
更新が完了しておりますが、引き続き緊急体制で全てのDNSサーバへの
対策を行ってまいります。

ご利用の皆様にはご迷惑をお掛けいたしました事を深くお詫び申し上げます。

平素より弊社サービスをご愛顧頂き誠に有り難うございます。

2015年7月31日22時3分より弊社のDNSに対してBIND 9.xの脆弱性を突いた
攻撃が確認され、DNSサービスの障害が発生しております。

http://jprs.jp/tech/
http://internet.watch.impress.co.jp/docs/news/20150731_714526.html

現在緊急の対策を行っておりますが、全てのDNSサーバの対策が完了次第
改めてご報告させて頂きます。
ご利用の皆様にはご迷惑をお掛けしております事を深くお詫び申し上げます。

(出典)
http://faq.21-domain.com/index.php?action=news&newsid=143&newslang=ja

ISPでの脆弱性対応例

会場にて

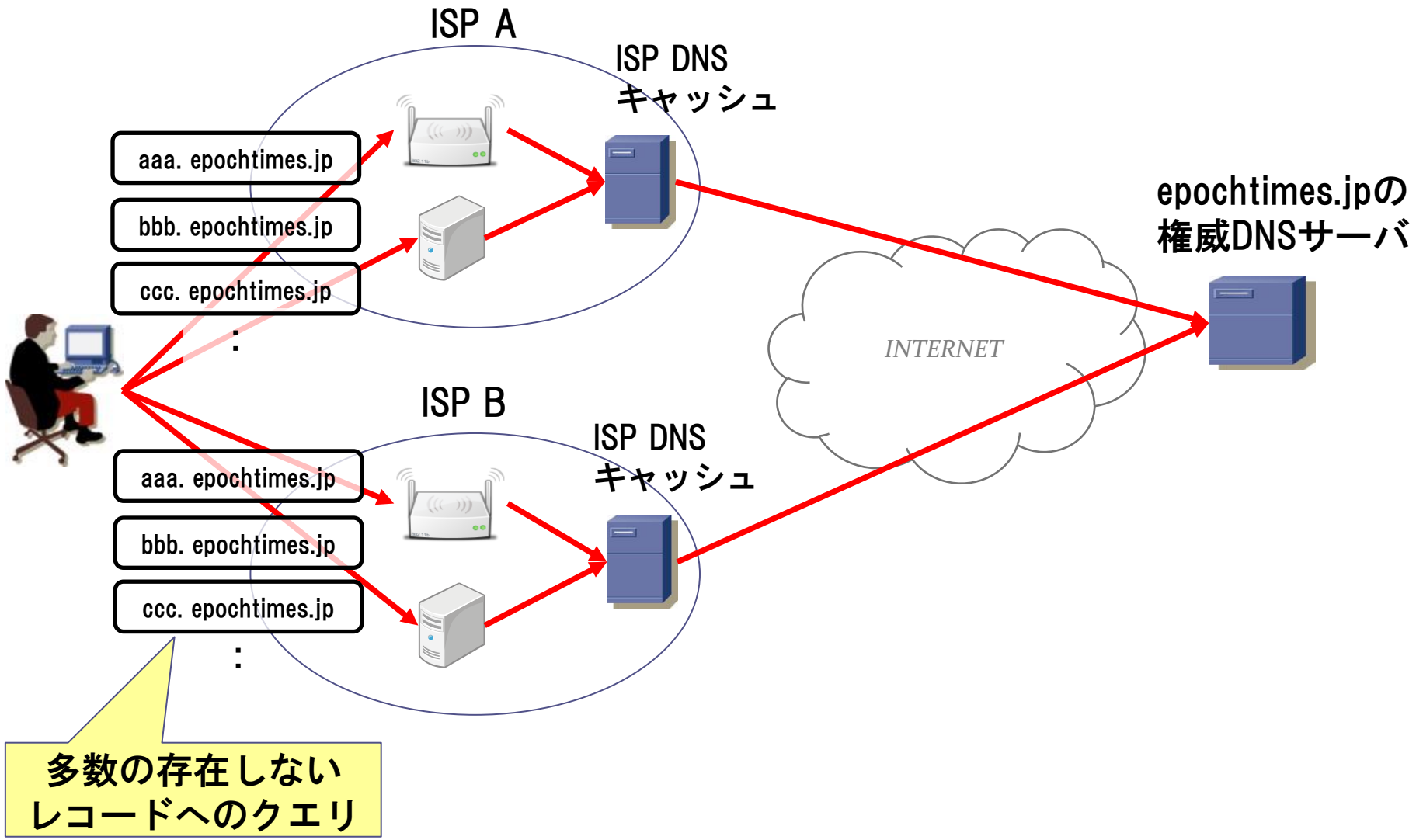
攻撃対応

攻撃事例（epochtimes.jp）

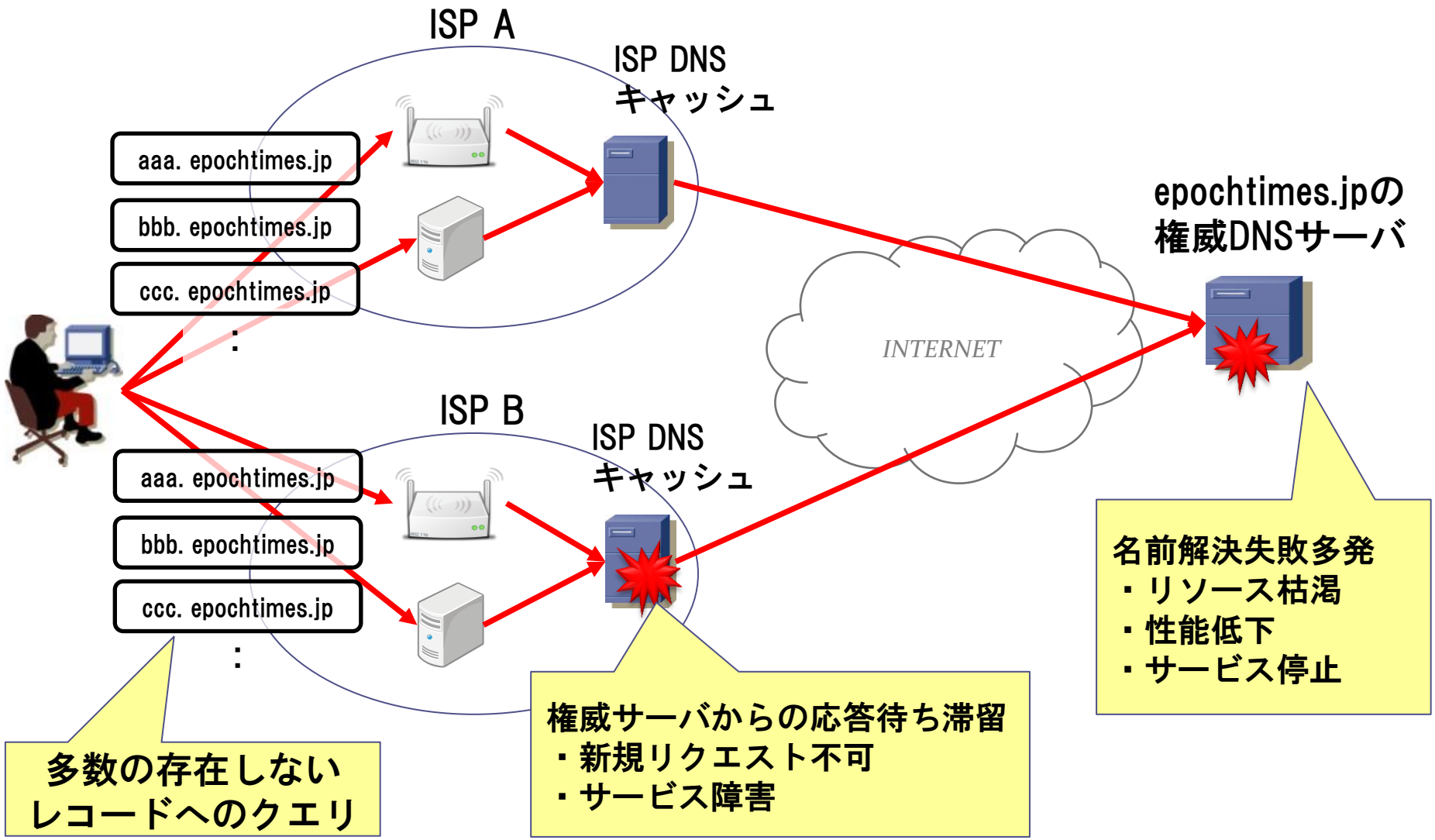
- 発生日時
  - 2015/2/3～2/6
- 発生個所
  - epochtimes.jpの権威サーバ
  - 一部ISPのキャッシュサーバ
- 被害状況
  - epochtimes.jpの権威サーバと同じサーバに収容したドメインの名前解決不可
  - 一部ISPキャッシュサーバでの応答遅延、名前解決不可
- 原因
  - epochtimes.jpへのランダムサブドメイン攻撃

（初のjpドメインへのランダムサブドメイン攻撃と言われている）

攻撃の概要

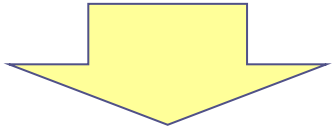


攻撃の概要



ISPでの対応

- 現状、増強で対処
- それでもダメなら遮断が考えられる
  - クエリを常時確認して、ランダムサブドメイン攻撃に使われるクエリを割り出し、遮断
  - しかし、上記は、通信の秘密の侵害(窃用等)に当たりうる



遮断できない！！

通信の秘密のガイドラインの改定

- 通信の秘密のガイドライン（正式名称：電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン）の改定中
- 改定により、正当業務行為として違法性が阻却される
- 改定版は、2015年11月末リリース予定

改定のポイント

- DNS の機能を悪用したDDoS 攻撃に用いられている名前解決要求に係る通信の遮断
  - DNSAmp攻撃やランダムサブドメイン攻撃による攻撃等への対処で、DNSサーバを通過する全ての名前解決要求に係るFQDNを常時確認し、リストに基づいて、FQDNが一致する場合に当該名前解決要求に係る通信を遮断

通信の秘密のガイドラインの改定内容

また、DNSAmp攻撃やランダムサブドメイン攻撃によるサイバー攻撃等から事業者設備に生じる侵害を防止するために、自社DNSサーバを通過する全ての名前解決要求に係るFQDNを常時確認し、攻撃に係る名前解決要求のFQDNのリストに基づいて、名前解決要求に係るFQDNとリストにあるFQDNが一致する場合に当該名前解決要求に係る通信を遮断することは通信の秘密の侵害(窃用等)に当たりうる。

(次のスライドに続く)

※注意：改定案からの抜粋です。正式版では変更となる可能性があります。

通信の秘密のガイドラインの改定内容

しかしながら、当該行為は攻撃によりISPの通信設備が過負荷状態になることによるインターネットアクセスやメールの遅延等の発生を防止し、もって、インターネット接続役務等の電気通信役務の安定的提供を図るためのものであり、また、侵害される通信の秘密も名前解決要求に係るFQDNのみと相当な限度で行われることに加え、その手法についても攻撃に係る通信のみを遮断するものであるから、正当業務行為として違法性が阻却されると考えられる※。

※詳細な検討は「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第二次とりまとめ」（以下「第二次とりまとめ」という。） P22参照

（http://www.soumu.go.jp/main_content/000376396.pdf）

※注意：改定案からの抜粋です。正式版では変更となる可能性があります。

[参考] 通信の秘密のガイドラインの改定のポイント

DNS の機能を悪用したDDoS攻撃に用いられている名前解決要求に係る通信の遮断	DNSAmp攻撃やランダムサブドメイン攻撃による攻撃等への対処で、DNSサーバを通過する全ての名前解決要求に係るFQDNを常時確認し、リストに基づいて、FQDNが一致する場合に当該名前解決要求に係る通信を遮断
脆弱性を有するブロードバンドルータ利用者への注意喚起	リフレクション攻撃に悪用され得る脆弱性やPPPoE認証の情報を窃取され得る脆弱性を有するブロードバンドルータを、ネットワーク上で調査し、契約者の接続ログから、当該ブロードバンドルータを保有している契約者を特定し、契約者に対して注意喚起
C&C サーバ等との通信の遮断における有効な同意	個別の同意を取得していない場合であっても、契約約款等に基づく事前の包括同意として、マルウェア感染端末とC&Cサーバ等との通信をレピュテーションDBに基づいて遮断
他人のID・パスワードを悪用したインターネットの不正利用への対処	電気通信役務の不正享受への対処 他人の認証情報を悪用したインターネットの不正利用への対処 従来SMTP認証だったものにPPPoE認証も追加
IP電話等の不正利用への対策	IP電話等の電話サービスの不正利用への対処