重複で、手を取り合って、垣根を越えて
- JPRSが発信する技術情報の概要とその心 –
～ランチのおともにDNS～

2015年11月19日

Internet Week 2015 ランチセミナー

株式会社日本レジストリサービス（JPRS）

森下 泰宏・平林 有理

講師自己紹介

- 森下 泰宏（もりした やすひろ）
  - 日本レジストリサービス（JPRS） 広報宣伝室
  - 主な業務内容：技術広報担当として、ドメイン名・DNSに関する技術情報の広報全般を担当
  - 一言：五十にして天命を・・・果たして知ったのか？
- 平林 有理（ひらばやし ゆうり）
  - 日本レジストリサービス（JPRS） システム部
  - 主な業務内容：レジストリシステム、周辺システムの開発・運用及び、そのネットワークの運用を担当
  - 一言：森下さんがBINDに出会った年に生まれました

本日の内容

1. JPRSが発信している技術情報の概要
2. 最近発信した注意喚起の振り返り
3. 注意喚起を読む（対応する）際に
   注目してほしいポイント
4. 今後の課題と展望

「手を取り合って、垣根を越えて」いくために必要なこと

前半二つを平林が、後半二つを森下が担当します

1. JPRSが発信している技術情報の概要

このパートの内容

- JPRSが発信している技術情報の概要
  - どんなものがあるか（種類）
  - 誰にどんなことを伝えようとしているか（目的・対象）
  - 発信の形態・最近の状況

JPRSが発信している技術情報の種類

- 注意喚起
  - 脆弱性情報に関する注意喚起
  - 脆弱性情報以外の注意喚起
- お知らせ
- 設定ガイド
- 技術解説
- JPRSトピックス＆コラム
- 技術動向報告
- JPRS技術陣による対外発表

技術コミュニティのMLを活用、
より速やかな情報共有を図る

「重複をお許しください」
の対象

「重複をお許しください」とは（1/2）

① JPRSから
② 技術コミュニティのメーリングリストに
③ マルチポストされるメール

注意喚起を公開した旨のメールの**書き出し部分**

– 現在はJANOG MLとDNSOPS.JP MLの二つ

「重複をお許しください」とは（2/2）

（緊急）BIND 9の致命的な脆弱性に関する注意喚起の掲載について - メッセージ (テキスト形式)

ファイル　メッセージ

2015/07/29 (水) 11:11

Yasuhiro Orange Morishita / 森下泰宏 <yasuhiro@jprs.co.jp>

（緊急）BIND 9の致命的な脆弱性に関する注意喚起の掲載について

宛先　dnsops@dnsops.jp

JPRS の森下/Orange です。重複をお許しください。

この部分

JPRS では本日、BIND 9 の脆弱性に関する以下の注意喚起文書を、
「JPRS DNS 関連技術情報」に掲載しました。

■（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 -
<http://jprs.jp/tech/security/2015-07-29-bind9-vuln-tkey.html>

今回の脆弱性は、

・BIND 9.1.0 以降すべてが対象
・権威・キャッシュ（リゾルバー）の双方が対象
・TKEY のバグであるが、TKEY を使ってなくても対象

2015年7月29日のDNSOPS.JP MLへのポスト
（※受信メールのイメージ）

注意喚起

- 目的：情報の周知と対応の促進
- 対象：日本のDNSサーバー運用者・利用者
- 大きく二つに分類
  - 脆弱性情報に関する注意喚起
  - 脆弱性情報以外の注意喚起
- DNS関連技術情報 <http://jprs.jp/tech/> で公開

基本的に、「何かしないといけない」ことを
知らせたい場合に出される情報

注意喚起（脆弱性情報）

- DNSの実装に関する脆弱性情報が中心
  - BIND、NSD/Unbound、PowerDNS、etc.
- 開発元の脆弱性情報公開を受けた、日本語での情報提供
  - 開発元の脆弱性情報公開にできる限り追従
    - 情報公開を把握後、速やかに準備開始
  - BINDについてはサブスクリプションにより情報を先行入手、一般公開日に合わせて情報公開
    - BIND Subscription

      <https://www.isc.org/bind-subscription-2/>

注意喚起（脆弱性情報以外）

- 重要なイベントの発生・発生予告を受けて実施
  - セキュリティインシデントの発生
  - セキュリティイシューの把握
  - DNSの運用に影響するイベントの発生
- 最近の事例（抜粋）
  - 共用DNSサービスにおける危険性とその対策（2012年）
  - キャッシュポイズニング攻撃の危険性増加に伴うDNSサーバーの設定再確認（2014年）
  - 登録情報の不正書き換えによるドメイン名ハイジャックとその対策（2014年）
  - ルートサーバーのIPアドレス変更（2013、2014、2015年）

お知らせ

- DNSの運用全般に関するお知らせ
- 目的：情報の伝達・周知
- 対象：日本のDNSサーバー運用者・利用者
- 最近の事例（JP DNSサーバー関連）
  - .jpゾーンにおけるKSKロールオーバーの完了（2011年）
  - JP DNSサーバーに設定されるDNSSEC関連情報の内容一部変更（2011年）
  - JP DNSサーバーに設定されるDS RRのTTL値の変更（2013年）
  - DNS.JPゾーンの収容変更（2014年）

設定ガイド

- ある項目を簡単に設定するためのガイド
- 目的：脆弱性対応や設定改善への活用
- 対象：日本のDNSサーバー運用者・利用者
- DNS関連技術情報 <http://jprs.jp/tech/> で公開
- 最近の事例
  - オープンリゾルバー機能を停止するには【BIND編】（2013年）
  - キャッシュポイズニング攻撃対策（2014年～）
    - 基本対策編（公開済）
    - 応用対策編（準備中）

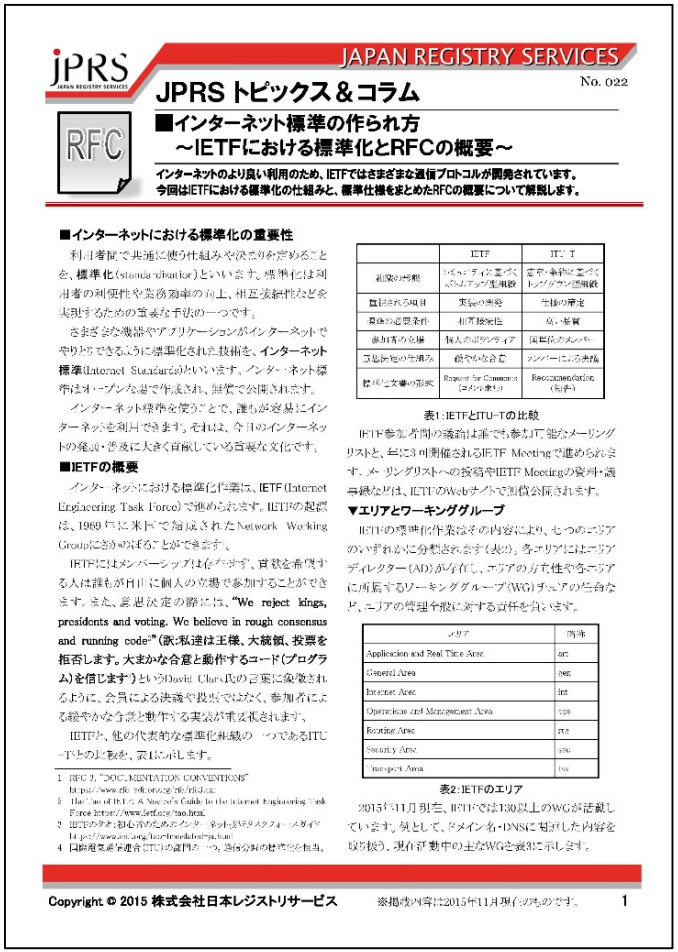
技術解説

- ある項目に特化した技術解説・翻訳・まとめ
- 目的：その項目に関するより深い、体系的な情報提供
- 対象：より詳しい内容を知りたい技術者
- DNS関連技術情報 <http://jprs.jp/tech/> で公開
- 最近公開した技術解説
  - DNSSEC関連情報（2010年～）
  - 幽霊ドメイン名脆弱性について（2012年）
  - DNSリフレクター攻撃について（2013年）
  - IT専門家のための名前衝突の確認および抑止方法ガイド（2014年）

その他の技術情報発信（1/2）

- JPRSトピックス＆コラム
  - ドメイン名・DNS関連項目をコンパクトに解説したコラム
  - 紙版・PDF版の双方を配布・公開
- 技術動向報告
  - IETF Meetingなどにおける最新動向
  - メールマガジン「FROM JPRS」・Webサイトで配信
- JPRS技術陣による対外発表
  - セミナー・イベントでの発表
  - 関連会議での活動（IETF・DNS-OARC・学会など）
  - 原稿執筆・インタビューなど

その他の技術情報発信（2/2）



JAPAN REGISTRY SERVICES

No. 022

JPRS トピックス＆コラム

■インターネット標準の作られ方 ～IETFにおける標準化とRFCの概要～

インターネットのより良い利用のため、IETFではさまざまな通信プロトコルが開発されています。今回はIETFにおける標準化の仕組みと、標準仕様をまとめたRFCの概要について解説します。

■インターネットにおける標準化の重要性

利用者間で共通に使う仕組みや決まりを定めることを、**標準化**(standardization)といいます。標準化は利用者の利便性や業務効率の向上、相互接続性などを実現するための重要な手法の一つです。

さまざまな機器やアプリケーションがインターネットで繋がりやすくするように標準化された技術を、**インターネット標準**(Internet Standards)といいます。インターネット標準はオープンな場で作成され、無償で公開されます。

インターネット標準を使うことで、誰もが容易にインターネットを利用できます。それは、今日のインターネットの発展・普及に大きく貢献している重要な文化です。

■IETFの概要

インターネットにおける標準化作業は、IETF (Internet Engineering Task Force)で進められます。IETFの起源は、1969年に米国で組成されたNetwork Working Groupにさかのぼることができます。

IETFにはメンバーシップは存在せず、貢献を希望する人は誰もが自由に個人の立場で参加することができます。また、意思決定の際には、**"We reject kings, presidents and voting. We believe in rough consensus and running code"**（訳：私達は王様、大統領、投票を拒否します。大まかな合意と動作するコード（プログラム）を信じます）というDavid Clark氏の言葉に象徴されるように、会員による決議や投票ではなく、参加者による緩やかな合意と動作する実装が重要視されます。

IETFは、他の代表的な標準化組織の一つであるITU-Tとの比較を、表1に示します。

	IETF	ITU-T
組織の特徴	ベストエフォートを基本とするボトムアップ型組織	産官・条約に基づくトップダウン型組織
意思される項目	実装の奨励	仕様の策定
標準の必要条件	相互接続性	良い仕様
参加者の立場	個人の専門家ベース	国単位のメンバー
意思決定の手順	緩やかな合意	メンバーによる承認
標準と文書の形式	Request for Comments（ネットの草分け）	Recommendation（伝統）

表1：IETFとITU-Tの比較

IETF参加者間の議論は誰でも参加可能なメーリングリストと、年に3回開催されるIETF Meetingで進められます。メーリングリストへの投稿やIETF Meetingの資料・議事録などは、IETFのWebサイトで無償公開されます。

▼エリアとワーキンググループ

IETFの標準化作業はその内容により、七つのエリアのいずれかに分類されます（表2）。各エリアにはエリアディレクター（AD）が存在し、エリアの方向性や各エリアに所属するワーキンググループ（WG）グループの当合など、エリアの管理全般に対する責任を負います。

エリア	略称
Application and Real Time Area	art
General Area	gen
Internet Area	int
Operations and Management Area	ops
Routing Area	rtg
Security Area	sec
Transport Area	tsv

表2：IETFのエリア

2015年11月現在、IETFでは130以上のWGが活動しています。例として、ドメイン名・DNSに関連した内容を次ページに、現在活動中の主なWGを表3に示します。

1 RFC 7, "DOC. MENTATION CONVENTIONS" http://www.rfc-editor.org/rfc/rfc7.txt
2 The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force https://www.ietf.org/tao.html
3 IETFの学び初心者のためのインターネット技術テクノロジーガイド http://www.ietf.org/tao-friendly-ja.html
4 国際電気通信連合ITUの略称の一つ。国際分野の標準化を担当。

Copyright © 2015 株式会社日本レジストリサービス　※掲載内容は2015年11月現在のものです。　1

JPRS トピックス&コラム No.22
「インターネット標準の作られ方」

セミナー・イベントでの発表
（DNS Summer Days 2015）

2. 最近発信した注意喚起の振り返り

このパートの内容

- JPRSが最近発信した注意喚起の振り返り
  - 最近1年間でJPRSが発信した脆弱性情報の紹介
  - そのうち、今年最も話題になった一つを取り上げ、重要な項目がどのように書かれていたかを振り返る

最近発信した脆弱性情報（2014年12月～2015年11月）

JPRSにおける文書公開・更新日	CVE	対象となる実装
2014年12月9日	CVE-2014-8680	BIND
2014年12月9日・12月25日	CVE-2014-8500 CVE-2014-8602 CVE-2014-8601	BIND Unbound PowerDNS Recursor
2015年2月19日	CVE-2015-1349	BIND
2015年4月27日・5月7日・7月8日	CVE-2015-1868	PowerDNS Authoritative Server PowerDNS Recursor
2015年7月8日	CVE-2015-4620	BIND
2015年7月29日・7月31日	CVE-2015-5477	BIND
2015年9月3日	CVE-2015-5986	BIND
2015年9月3日	CVE-2015-5722	BIND
2015年9月3日	CVE-2015-5230	PowerDNS Authoritative Server
2015年11月11日	CVE-2015-5311	PowerDNS Authoritative Server

事例：CVE-2015-5477

- （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31日更新）

  <http://jprs.jp/tech/security/2015-07-29-bind9-vuln-tkey.html>

- 特徴：

  ① リモートからのDNS問い合わせ一発でnamedを落とせる
  ② 多くのバージョンのBINDが対象となる
  ③ 権威DNSサーバー・フルリゾルバーの双方が対象となる
  ④ namedの設定やオプションでは回避できない

  いわゆる「BINDコロリ」と呼ばれるものの一種

- PoCが出回り、国内の複数ISPにおいて被害が発生
  - これによりJPRSの注意喚起を更新（7月29日、7月31日）

注意喚起に含まれるべき五つの項目（詳細はパート3で解説）

① 対象となるソフトウェア・バージョン
② 不具合の原因
③ 危険性
④ 対象の範囲
⑤ 必要な対策

- これらの項目が、注意喚起の概要にどのように書かれていたのか?

注意喚起（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。

注意喚起（概要）

①対象となるソフトウェア

②不具合の原因

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。

③危険性

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[redacted]、対象が広範囲にわたっています。該当するBIND 9.x[redacted]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。

④対象の範囲

⑤必要な対策

注意喚起（概要：追加部分）

（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。

（2015年7月31日追加）本脆弱性のPoC（Proof of Concept：実証コード）が既にネット上で公開されており、日本国内のサービスプロバイダーからの被害事例も報告されています。改めて即時の対応を強く推奨します。

注意喚起（概要：追加部分）

（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

危険性の上昇
（③の状況変化）

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。

緊急性の上昇
（⑤の状況変化）

（2015年7月31日追加）本脆弱性のPoC（Proof of Concept：実証コード）が既にネット上で公開されており、日本国内のサービスプロバイダーからの被害事例も報告されています。改めて即時の対応を強く推奨します。

3. 注意喚起を読む（対応する）際に注目してほしいポイント

このパートの内容

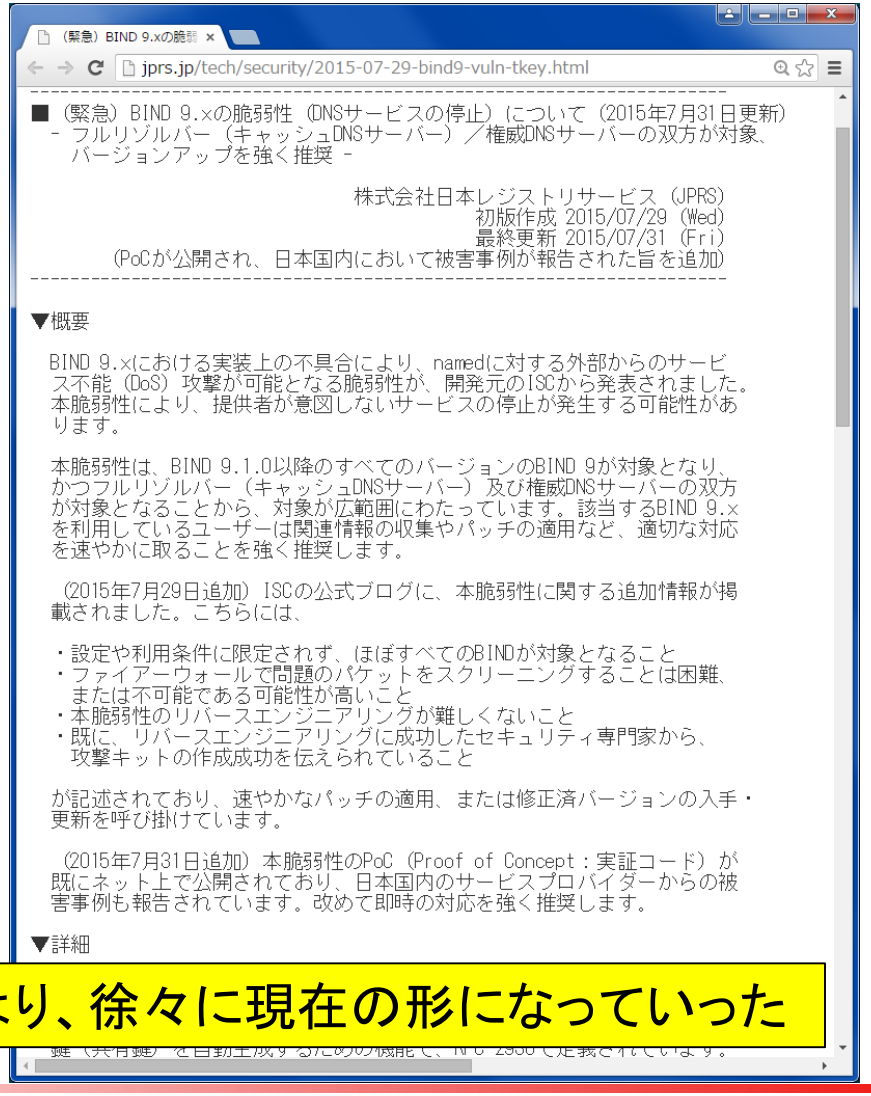
- 注意喚起（脆弱性情報）の構成と内容
- 公開された注意喚起を読む（対応する）際に注目してほしいポイント

注意喚起をどのように受け止め、どう行動してほしいのかという、発信者（JPRS）の思いを解説

注意喚起（脆弱性情報）の標準的な文章構成

- タイトル・初版作成日・最終更新日
- 概要
- 詳細
  - 本脆弱性の背景（オプション）
  - 本脆弱性の概要（注）
  - 対象となるバージョン
  - 影響範囲
- 一時的な回避策（影響軽減策）
- 解決策
- JP DNSサーバーにおける対応状況（オプション）
- 参考リンク
- 連絡先
- 更新履歴

（注）「本脆弱性の背景」を書かない場合、独立項目としない場合あり

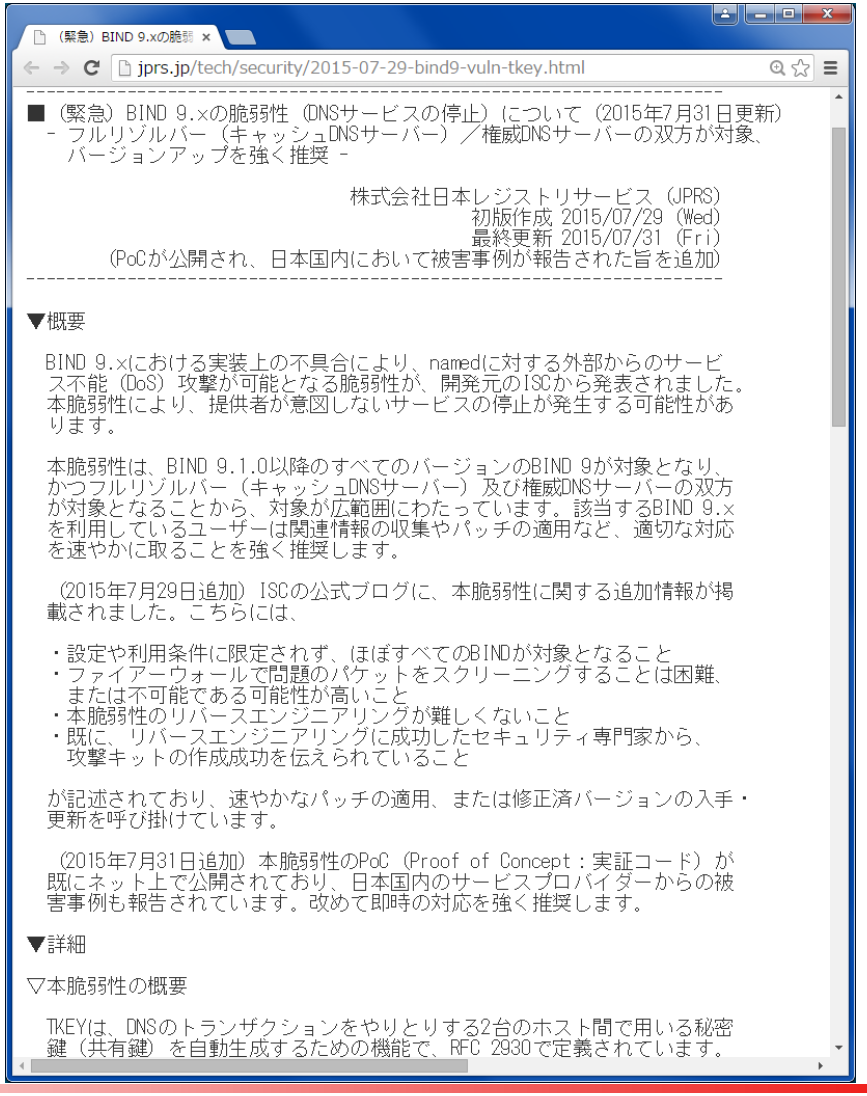


経験の蓄積により、徐々に現在の形になっていった

以降で説明する項目

- タイトル・初版作成日・最終更新日
- 概要
- 詳細
  - 本脆弱性の背景（オプション）
  - 本脆弱性の概要（注）
  - 対象となるバージョン
  - 影響範囲
- 一時的な回避策（影響軽減策）
- 解決策
- JP DNSサーバーにおける対応状況（オプション）
- 参考リンク
- 連絡先
- 更新履歴

（注）「本脆弱性の背景」を書かない場合、独立項目としない場合あり


（緊急）BIND 9.xの脆弱
jprs.jp/tech/security/2015-07-29-bind9-vuln-tkey.html

■（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31日更新）
- 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）
最終更新 2015/07/31（Fri）
（PoCが公開され、日本国内において被害事例が報告された旨を追加）

▼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。

（2015年7月31日追加）本脆弱性のPoC（Proof of Concept：実証コード）が既にネット上で公開されており、日本国内のサービスプロバイダーからの被害事例も報告されています。改めて即時の対応を強く推奨します。

▼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。

タイトル・概要

- 以下の5項目について、簡潔に記述

  ① 対象となるソフトウェア・バージョン
  ② 不具合の原因
  ③ 危険性
  ④ 対象の範囲
  ⑤ 必要な対策

- 発信者の思い（ポイント）
  - 現場の担当者が概要・影響範囲を把握できる
  - 現場の担当者が上司（責任者）に見せ、説明できる
  - 外部に説明する際のリファレンス（参照先）になる

詳細

- 詳しいことを知りたい人向けの情報を記述
  - 脆弱性の背景、内容、対象バージョン、影響範囲
- 「本脆弱性の背景」を記述するかどうか
  - 特別な機能や新機能など、追加の説明が必要な場合
    - Dynamic Update、DNSプリフェッチ、TKEY、OPENPGPKEYなど
    - そういう機能にバグが潜んでいることが多い（特にBIND）
- 発信者の思い（ポイント）
  - 開発元が公開した情報が正確に伝わる
  - 現場の担当者が技術的に納得し、作業をしやすくなる

一時的な回避策（影響軽減策）

- 回避策・影響軽減策の有無・手法を記述
- 一般的なセキュリティアドバイザリの「ワークアラウンド（Workarounds）」に相当
- 開発元が公開した情報をそのまま翻訳
  - 一時的な回避策が存在しない場合も多い（特にBIND）

解決策

- 根本的な問題解決策を記述
- 一般的なセキュリティアドバイザリの「解決策（Solution）」に相当
- 開発元が公開した情報をそのまま翻訳
  - 多くの場合、ソフトウェアのバージョンアップやベンダー（ディストリビューター）がリリースするパッチの適用

JP DNSサーバーにおける対応状況

- JP DNSサーバーにおける対応状況を記述
  - JP DNSサーバーにおける対応の必要性・対応状況を特に示したい場合（オプション）
    - 主に、権威DNSサーバーに影響する脆弱性
- 記述例
  - JP DNSサーバーは本脆弱性の対象となりません。
  - JP DNSサーバーでは本脆弱性への対応を完了しています。

参考リンク

- 元となる情報へのリンクを記述
  - オリジナルの脆弱性情報
  - 必要なソフトウェア・パッチの入手先
  - MITRE社のCVE情報
- 情報公開時点では、CVE情報のリンク先の内容は「** RESERVED **」となっていることがほとんど
  - 後で参照する際、有用な情報となる
- 発信者の思い（ポイント）
  - 現場の担当者の情報元確認や作業の手間が少なくなる

4. 今後の課題と展望

「手を取り合って、垣根を越えて」いくために必要なこと

より良い情報発信とは?

- 本来の目的を達成できるものであること
  - 注意喚起の場合、対応の促進
  - 技術解説の場合、知識の習得・活用
- 実現のための手法例
  - 日本語での情報提供
    - 多くの日本人にとって、言葉の壁は大きい
  - 情報発信するチャンネルの拡大
  - さまざまなメディアの活用
  - 関係機関・関連各位との連携・協調

発信者自身の経験（SECCON 2014）

- 長野大会「DNS Security Challenge」
  <http://2014.seccon.jp/dns-security-challenge.html>
  – 運営サポート（問題作成監修・講演・問題読み上げ）
- これからを担う、
  若い方々へのリーチ不足を強く実感
  – これから知識を習得しようとしている方々

「DNSを勉強するにはこれからどうしたらいいですか」
という質問を多くいただいた

発信者自身の経験（SECCON 2014）

- 決勝戦・全国大会カンファレンス
  <http://2014.seccon.jp/finals.html>
  – 講演を担当（DNSセキュリティ最新動向）
- セキュリティに関心を持つ層へのリーチ不足を実感
  – 講演終了後、「DNS関連の技術動向を聞く機会があまりなかったので助かりました」というコメントを多くいただいた

「必要とする情報を欲している」「しかし、それが伝わっていない」という層が確実に存在することを強く実感

「手を取り合って、垣根を越えて」いくために

- インターネットは本来、連携・協調（手を取り合う）により成立するネットワーク
  - DNSでは特に、関係者間の連携・協調が不可欠
- 分野・領域を越えた（垣根を越えた）連携が、今後ますます重要になる
  - 昨年の「DNS DAY」のテーマの一つでもあった
  - 次世代への技術の伝承も重要な課題（世代の垣根越え）
- 「手を取り合って、垣根を越えて」いくために・・・

JPRSでは今後も各関連各位と協力しながら、さまざまな形で情報発信を続けていきます

That’s it!