JPCERT CC®

IPv6 セキュリティテスト手順書(一般公開版)

2013 年度版

一般社団法人 JPCERT コーディネーションセンター

2014 年 04 月 28 日

JPCERT CC®

目次

1. IPv6 セキュリティテスト（2013 年版）とは

1.1 セキュリティテストの概要

「IPv6 セキュリティテスト」とは、IPv6 対応機器のセキュリティ上の問題を検証するテストです。本テストは、一般社団法人 JPCERT コーディネーションセンター（以下、JPCERT/CC）が作成したテスト項目、手順に従って IPv6 対応機器ベンダが実施し、その検証結果は JPCERT/CC Web サイトで「IPv6 セキュリティテスト検証済製品リスト（2013 年度版）」として公開されます。
本書と「IPv6 セキュリティテスト検証済製品リスト（2013 年度版）」は、IPv6 対応機器の購入を検討されている企業や組織のシステム担当者の方に、機器選定時の参考資料としてご利用いただくことを目的としています。

JPCERT/CC の IPv6 に関する取り組みの詳細については以下を参照ください。
IPv6 プロトコルのセキュリティ課題に対する取り組み
https://www.jpcert.or.jp/pr/2013/ipv6project.html

本取り組みにご賛同いただき、自社製品の「IPv6 セキュリティテスト検証済製品リスト」への掲載をご希望される場合は、本 IPv6 セキュリティテスト手順書に従った検証を実施いただき、そのテスト結果を「情報提供票」フォームに記入して、JPCERT/CC 担当者までお送りください。

1.2 注意事項

1. 提供いただいた検証情報は、「IPv6 セキュリティテスト検証済製品リスト」に含めて、JPCERT/CC の Web ページなどにて公開します。
2. 検証対象機種、バージョンは、各ベンダ様にて選定ください。
3. ご提供いただいた情報は原則そのまま掲載いたします。外部への公開を意図されない情報が含まれていないかなど、事前に確認をお願いします。
4. IPv6 セキュリティテスト検証済製品リストの個別の検証結果などに関するお問い合わせは、各ベンダ様にお願いいたします。

JPCERT CC®

1.3 IPv6 セキュリティテスト 2013 年度版検証項目

2013 年度の検証項目は、以下 15 項目です。各項目の対象脆弱性については、「IPv6 プロトコル仕様に関する脆弱性調査報告書（以下、「調査報告書」）を合わせてご覧ください。

※調査報告書は、製品開発者向けにのみ提供しております。

項番	項目名	項目識別子
1	タイプ 0 ルーティングヘッダ処理の無効化	2013-ipv6sec-0001
2	ホップバイホップオプションヘッダによるルータへの DoS 攻撃	2013-ipv6sec-0002
3	特大ペイロードオプション利用における実装上の課題	2013-ipv6sec-0003
4	不正なフラグメントヘッダによるパケット情報の上書きの対応　完全上書き（前）	2013-ipv6sec-0004
5	不正なフラグメントヘッダによるパケット情報の上書きの対応　完全上書き（後）	2013-ipv6sec-0005
6	不正なフラグメントヘッダによるパケット情報の上書きの対応　部分上書き（前）	2013-ipv6sec-0006
7	不正なフラグメントヘッダによるパケット情報の上書きの対応　部分上書き（後）	2013-ipv6sec-0007
8	細かいフラグメントヘッダを利用した DoS 攻撃 tiny fragment の実装確認	2013-ipv6sec-0008
9	細かいフラグメントヘッダを利用した DoS 攻撃 大量の tiny fragment	2013-ipv6sec-0009
10	第一フラグメントパケットのみを送信することによる DoS 攻撃	2013-ipv6sec-0010
11	単一フラグメントヘッダを利用した DoS 攻撃 atomic fragment の実装確認	2013-ipv6sec-0011
12	単一フラグメントヘッダを利用した DoS 攻撃 大量の atomic fragment	2013-ipv6sec-0012
13	フラグメント ID 予測による経路外攻撃者からの攻撃	2013-ipv6sec-0013
14	近隣探索サービスを利用したルータへの DoS 攻撃	2013-ipv6sec-0014
15	ルータに対する大量の不正パケット送信による DoS 攻撃	2013-ipv6sec-0015

2. 検証手順

2.1 検証環境と導入手順について

<一般公開版では削除しています>

2.2 作業に当たって

<一般公開版では削除しています>

2.3 DoS に陥る可能性のある検証項目の評価方法について

DoS 攻撃の対策は非常に難しく、ファイアウォールなどの外部機器で行うことが一般的です。本検証では、DoS 攻撃を受けた場合の根本的な対策は外部機器で行われるものとし、攻撃を受けても再起動などの影響が発生しないこと、攻撃後に元の状態に回復できることを評価しました。

DoS に陥る可能性のある検証項目の評価基準
1. リブートしないこと 2. ハングアップしないこと 3. DoS 攻撃が終わった後に通常状態に戻ること

3. 各項目の評価の実施

(1) タイプ 0 ルーティングヘッダ処理の無効化

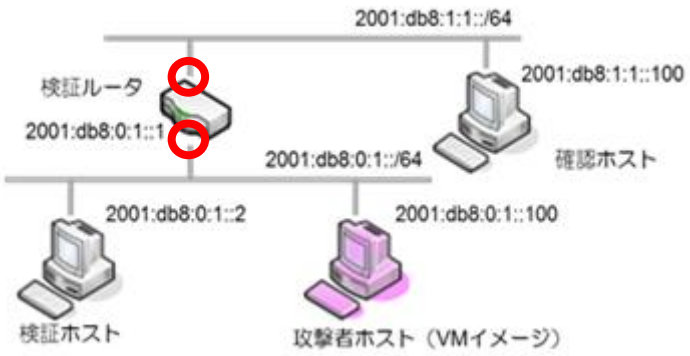
【識別番号】

2013-ipv6sec-0001

【IPv4 との比較】

IPv4 におけるソースルーティングオプションに同様の問題が存在する

【検証構成】



【検証手順】

<一般公開版では削除しています>

【検証結果例】

<一般公開版では削除しています>

【合否判定】

検証ツールの結果が FAILED となること

(2) ホップバイホップオプションヘッダによるルータへの DoS 攻撃

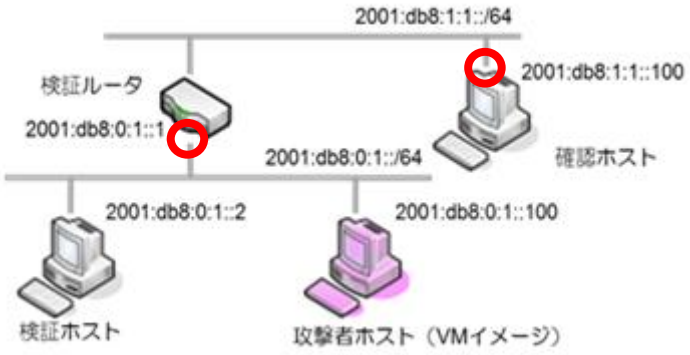
【識別番号】

2013-ipv6sec-0002

【IPv4 との比較】

IPv4 におけるヘッダオプションに同様の問題が存在する

【検証構成】



【検証手順】

<一般公開版では削除しています>

【検証結果例】

<一般公開版では削除しています>

【合否判定】

検証ツールの結果が FAILED となること

(3) 特大ペイロードオプション利用における実装上の課題

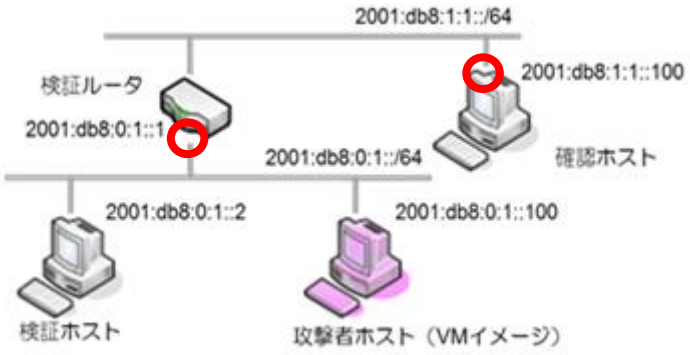
【識別番号】

2013-ipv6sec-0003

【IPv4 との比較】

IPv6 特有の問題

【検証構成】



【検証手順】

<一般公開版では削除しています>

【検証結果例】

<一般公開版では削除しています>

【合否判定】

検証対象機器が、以下の DoS の評価基準を満たすこと

・リブートしないこと

・ハングアップしないこと

・DoS 攻撃が終わった後に通常状態に戻ること

攻撃前から攻撃後まで、ping6 2001:db8:1:1::100 を実施し、通常状態に戻ることを確認する

(4) 不正なフラグメントヘッダによるパケット情報の上書きの対応　完全上書き（前）

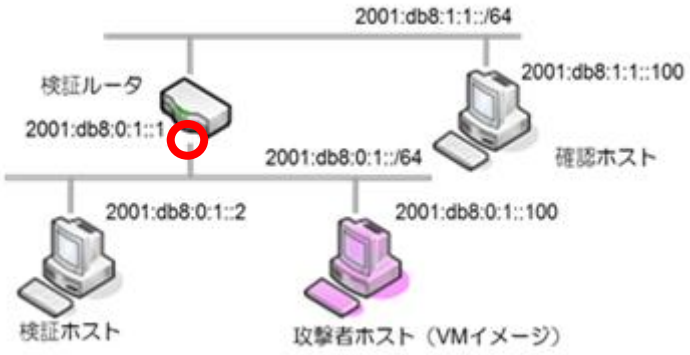
【識別番号】

2013-ipv6sec-0004

【IPv4 との比較】

IPv4 のフラグメントにも同様の問題が存在する

【検証構成】



【検証手順】

<一般公開版では削除しています>

【検証結果例】

<一般公開版では削除しています>

【合否判定】

検証ツールの結果が FAILED となること

(5) 不正なフラグメントヘッダによるパケット情報の上書きの対応　完全上書き（後）

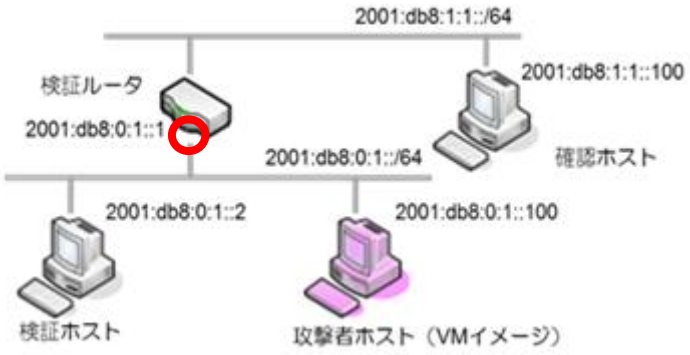
【識別番号】

2013-ipv6sec-0005

【IPv4 との比較】

IPv4 のフラグメントにも同様の問題が存在する

【検証構成】



【検証手順】

<一般公開版では削除しています>

【検証結果例】

<一般公開版では削除しています>

【合否判定】

検証ツールの結果が FAILED となること

(6) 不正なフラグメントヘッダによるパケット情報の上書きの対応　部分上書き（前）

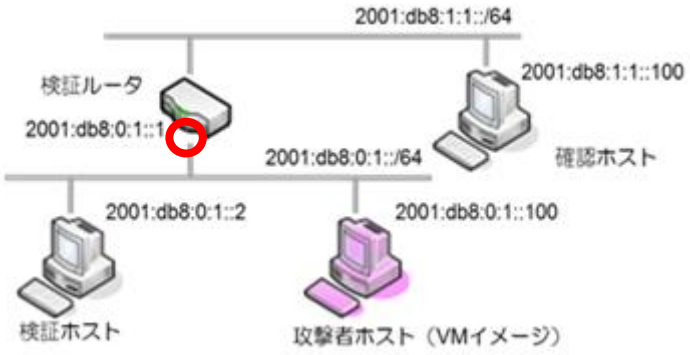
【識別番号】

2013-ipv6sec-0006

【IPv4 との比較】

IPv4 のフラグメントにも同様の問題が存在する

【検証構成】



【検証手順】

<一般公開版では削除しています>

【検証結果例】

<一般公開版では削除しています>

【合否判定】

検証ツールの結果が FAILED となること

(7) 不正なフラグメントヘッダによるパケット情報の上書きの対応　部分上書き（後）

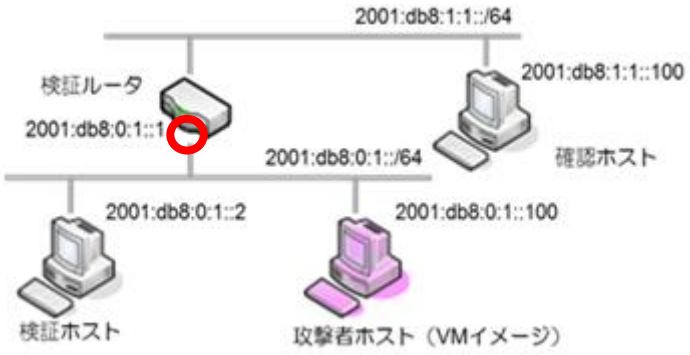
【識別番号】

2013-ipv6sec-0007

【IPv4 との比較】

IPv4 のフラグメントにも同様の問題が存在する

【検証構成】



【検証手順】

<一般公開版では削除しています>

【検証結果例】

<一般公開版では削除しています>

【合否判定】

検証ツールの結果が FAILED となること

(8) 細かいフラグメントヘッダを利用した DoS 攻撃 tiny fragment の実装確認

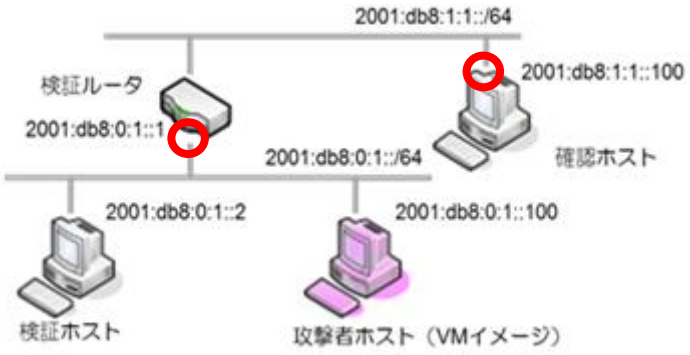
【識別番号】

2013-ipv6sec-0008

【IPv4 との比較】

IPv4 のフラグメントにも同様の問題が存在する

【検証構成】



【検証手順】

<一般公開版では削除しています>

【検証結果例】

<一般公開版では削除しています>

【合否判定】

検証対象機器が、以下の DoS の評価基準を満たすこと

・リブートしないこと

・ハングアップしないこと

・DoS 攻撃が終わった後に通常状態に戻ること

攻撃前から攻撃後まで、ping6 2001:db8:1:1::100 を実施し、通常状態に戻ることを確認する

(9) 細かいフラグメントヘッダを利用した DoS 攻撃大量の tiny fragment

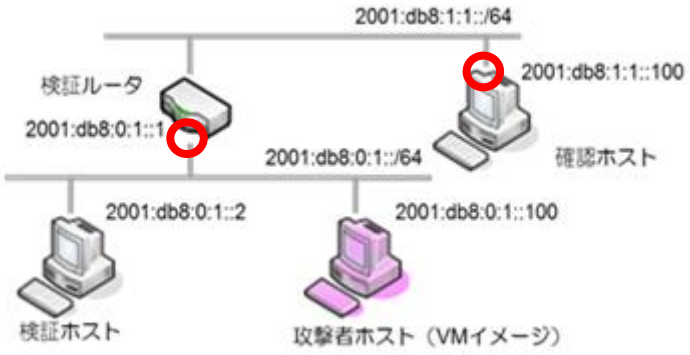
【識別番号】

2013-ipv6sec-0009

【IPv4 との比較】

IPv4 のフラグメントにも同様の課題が存在する

【検証構成】



【検証手順】

<一般公開版では削除しています>

【検証結果例】

<一般公開版では削除しています>

【合否判定】

検証対象機器が、以下の DoS の評価基準を満たすこと

・リブートしないこと

・ハングアップしないこと

・DoS 攻撃が終わった後に通常状態に戻ること

攻撃前から攻撃後まで、ping6 2001:db8:1:1::100 を実施し、通常状態に戻ることを確認する

(10) 第一フラグメントパケットのみを送信することによる DoS 攻撃

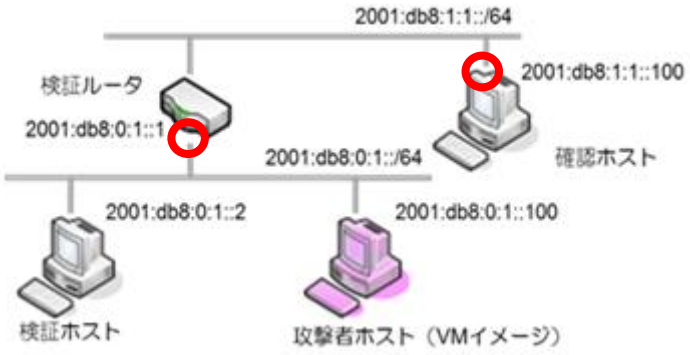
【識別番号】

2013-ipv6sec-0010

【IPv4 との比較】

IPv4 のフラグメントにも同様の課題が存在する

【検証構成】



【検証手順】

<一般公開版では削除しています>

【検証結果例】

<一般公開版では削除しています>

【合否判定】

検証対象機器が、以下の DoS の評価基準を満たすこと

・リブートしないこと

・ハングアップしないこと

・DoS 攻撃が終わった後に通常状態に戻ること

攻撃前から攻撃後まで、ping6 2001:db8:1:1::100 を実施し、通常状態に戻ることを確認する

(11) 単一フラグメントヘッダを利用した DoS 攻撃 atomic fragment の実装確認

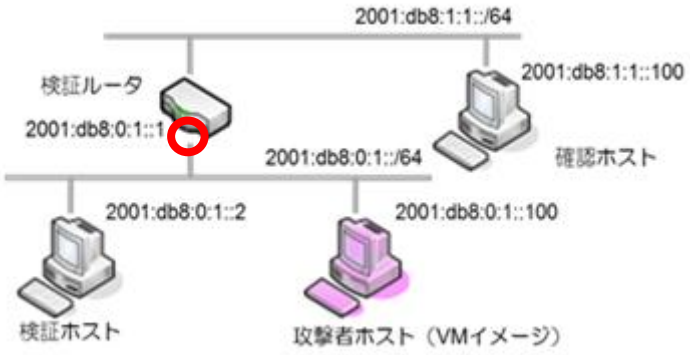
【識別番号】

2013-ipv6sec-0011

【IPv4 との比較】

IPv6 特有の課題

【検証構成】



【検証手順】

<一般公開版では削除しています>

【検証結果例】

<一般公開版では削除しています>

【合否判定】

検証ツールの結果が PASSED となること

(12) 単一フラグメントヘッダを利用した DoS 攻撃大量の atomic fragment

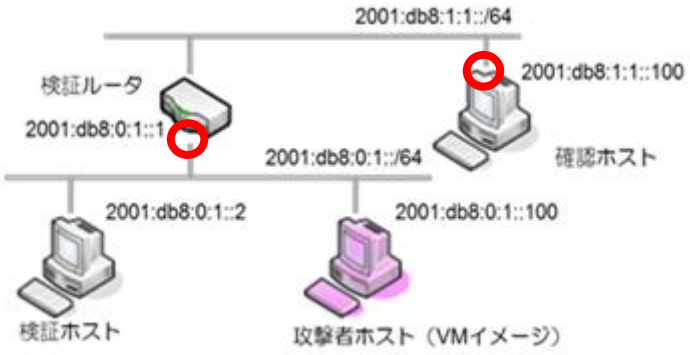
【識別番号】

2013-ipv6sec-0012

【IPv4 との比較】

IPv6 特有の課題

【検証構成】



【検証手順】

<一般公開版では削除しています>

【検証結果例】

<一般公開版では削除しています>

【合否判定】

検証対象機器が、以下の DoS の評価基準を満たすこと

・リブートしないこと

・ハングアップしないこと

・DoS 攻撃が終わった後に通常状態に戻ること

攻撃前から攻撃後まで、ping6 2001:db8:1:1::100 を実施し、通常状態に戻ることを確認する

(13) フラグメント ID 予測による経路外攻撃者からの攻撃

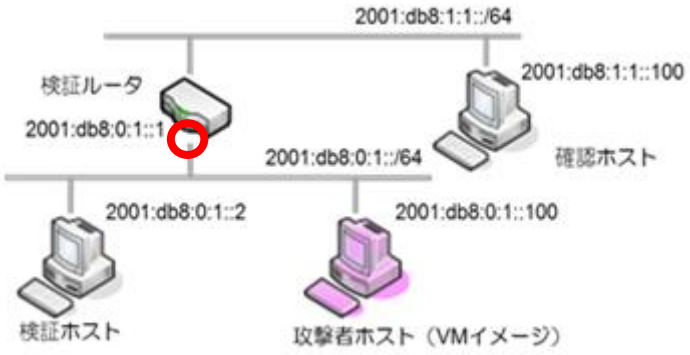
【識別番号】

2013-ipv6sec-0013

【IPv4 との比較】

IPv4 のフラグメントにも同様の問題が存在する

【検証構成】



【検証手順】

<一般公開版では削除しています>

【検証結果例】

<一般公開版では削除しています>

【合否判定】

検証ツールの結果が"Randomized IDs"となること

(14) 近隣探索サービスを利用したルータへの DoS 攻撃

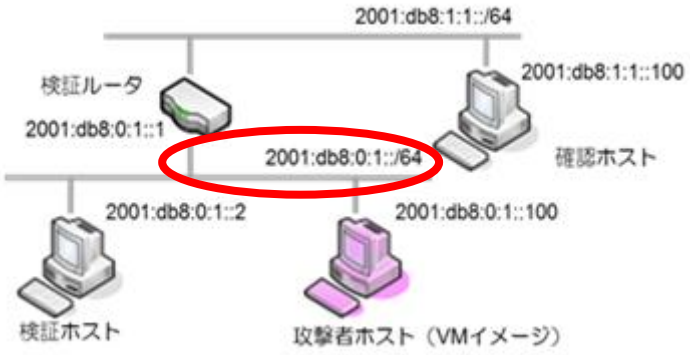
【識別番号】

2013-ipv6sec-0014

【IPv4 との比較】

IPv4 における ARP に同様の問題が存在する

【検証構成】



【検証手順】

<一般公開版では削除しています>

【検証結果例】

<一般公開版では削除しています>

【合否判定】

検証対象機器が、以下の DoS の評価基準を満たすこと

・リブートしないこと

・ハングアップしないこと

・DoS 攻撃が終わった後に通常状態に戻ること

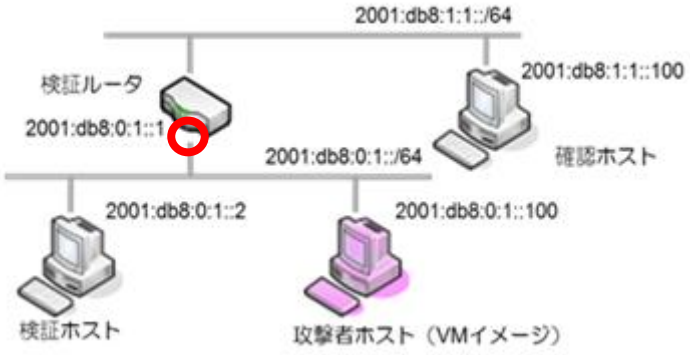
攻撃前から攻撃後まで、ping6 2001:db8:1:1::100 を実施し、通常状態に戻ることを確認する

(15) ルータに対する大量の不正パケット送信による DoS 攻撃 (MTU サイズよりも小さく分割したエコー要求)

【識別番号】

2013-ipv6sec-0015

【検証構成】



【検証手順】

<一般公開版では削除しています>

【検証結果例】

<一般公開版では削除しています>

【合否判定】

検証対象機器が、以下の DoS の評価基準を満たすこと

・リブートしないこと

・ハングアップしないこと

・DoS 攻撃が終わった後に通常状態に戻ること

攻撃前から攻撃後まで、ping6 2001:db8:1:1::100 を実施し、通常状態に戻ることを確認する。