v6gtl-id	システム設計時	運用時	Webアプリ実装時	クライアントアプリ実装時	ハードウェア実装時（ハードウェア搭載のソフトウェアの実装時も含む）	仕様	同一リンクからの攻撃	Short Name	Short Description	v6pc/v6app-swg	v6pc/v6fix-swg	v6pc/v6HGW-swg	v6pc/sec-wg	NIST/sp800-119	IPv6検証協議会（tvc）	RFC/Draft（問題の定義または発生源はs、ソリューションの提案はs）	備考
v6gtl-01	○	○		○			×	アドレスの変化に対するアプリケーション挙動に対する不安	アプリケーションにおいては、デュアルスタックの名前解決結果(A+AAAA)について、AAAAを優先した後、Aを利用する動作のみならず、RFC6555(Happy Eyeball)実装や名前解決結果のキャッシュの使い方によっては、当初接続を確立させたプロトコルではなく別のプロトコルを利用してしまう可能性があるため、名前解決結果と処理方法の組み合せ方によっては、認証手続きの矛盾や意図しない接続、プログラムそのものの脆弱性を引き起こす可能性がある。	○				○	○		
v6gtl-02	○	○			△		×	PMTU DiscoveryとICMPフィルタリング	IPv4ネットワークでは、ICMPがセキュリティ脆弱性の元になるという考え方により、ファイアーウォールなどの機器でのフィルタリングが行われている。一方、IPv6ネットワークにおけるICMPv6は、通信確立上不可欠な機能（Path MTU Discovery）として存在している。そのため、IPv4ネットワークと同じポリシーでICMPv6のフィルタリングを行ってしまうと通信を開始できない事象を引き起こす場合がある。DoS Attack やスキャニングなどの脅威への対策を考慮しつつ、フィルタリング可能なICMPv6のみをフィルタリングするようにネットワークポリシーを調整する必要がある。	○						RFC2979 RFC4890	
v6gtl-03	○	○			△		○	ICMPv6リダイレクト問題	IPv4と同様に、IPv6ネットワークにおいてもICMPv6のリダイレクトメッセージが規定されている。これを利用し、悪意を持った者が、偽造したICMPv6リダイレクトをターゲットに送り、別の送信先に誘導することで、パケットの盗聴、DoS、通信不能、ルーティングリソースの枯渇が引き起こされる可能性がある。このため、ルータを越えたリダイレクトメッセージの破棄、自端末をソースアドレスとするリダイレクトメッセージの破棄といった自衛方法の導入の他、本問題に対する対処策を含んだベンダー機器の選定、ルータや接続端末への認証機構の導入なども合わせて検討する必要がある。	○					3.1.14	RFC4443	
v6gtl-04	○	○			○	○	×	IPv4 mapped IPv6 address利用時の意図しない通信	RFC3493(Basic Socket Interface Extensions for IPv6)において、デュアルスタックの処理を行う為に、AF_INET6はIPv4 mapped addressを利用してIPv4依存のアプリケーションを処理するように定義された。しかし、このAPIの目的とは別に、トランスレータなどでIPv6onlyノードとIPv4ネットワークをつなぐ手段としてパケットの転送処理に利用するケース(RFC6145,SIITなど)もある。後者の場合、セキュリティポリシーを意識、調整せずに処理することでポリシーバイオレーションとなり、意図しないプロトコル通過となる場合がある。 2つのプロトコル間を意図せず中継することのセキュリティ上の具体的な問題は、RFC6169(トンネルプロトコルの問題指摘)と同じ。	○						draft-itojun-v6ops-v4mapped-harmful-02 (d) RFC6169 (d)	
v6gtl-05			○	○		○	×	Happy Eyeballの悪用	応答の速いコネクションを利用することを提案しているRFC6555(Happy Eyeball)では、細かな制御については記載がなく、実装依存となっている。このため、脆弱性を伴うの可能性（SYN/ACKのタイミング や介入によるバッファオーバーフロー等）がある。また、多くのWebサイトでは1ページ中に多数のコネクションを張る設計になっており、IPv4とIPv6の通信が混在してしまうケースが考えられるが、接続確立に利用されたアドレスは正規の通信とみなされ、一定期間セキュリティアプライアンスのチェックを逃れてしまう可能性がある。これにDNSの登録を悪用するなど複合的な手法を用いると、さらにセキュリティリスクを増大させる可能性がある。	○							
v6gtl-06	○	○	△	△			×	キャプティブポータルとDNSに関する課題	IPv6に正しく対応していないDNSサーバとリゾルバの実装に起因する課題である。AAAAクエリに対してAレコードの値を返す実装と、Windows XPのようにその誤ったAレコード応答をそのまま通信に利用する実装により、キャプティブポータルを正しく利用できなくなる。	○	Sec.4					RFC4074(d)	
v6gtl-07	○	○					×	IPv6からIPv4へのフォールバックに関する課題	デュアルスタックノードがIPv6を優先的に利用するため、IPv6の接続性に問題があるとIPv4通信にフォールバックする。実装によっては、切り替えに時間がかかったり、もしくは切り替わらない場合がある。		○					RFC3483(s)	
v6gtl-08	○	○					×	DNSの問い合わせに関する課題	DNSサーバの実装によっては、AAAAもしくはAレコードのみの登録情報に対して、登録のないRRへの問い合わせにNX_DOMAINを応答する実装がある。また、キャッシュDNSサーバの設定において、AAAAレコードの応答を実施しない設定が可能で、この場合にはIPv6通信が不可能となる。キャッシュDNSサーバへの問い合わせにIPv4/IPv6のどちらを用いるかはリゾルバの実装依存であるため、そもそもどちらで通信しても同じ結果が得られることが想定されており、結果が異なる場合に意図したサイトへの通信が行われない可能性がある。		○					RFC4074(d) RFC3901(s) RFC4472(s) RFC4942(d)	
v6gtl-09	○	○					×	品質の悪いトンネルに関する課題	6to4やTeredoといった無保証なリレールータを利用するトンネル接続では、通信品質の悪い経路を利用した通信となる場合があり、接続性が保証されない。また、リレールータが信用できない場合には盗聴の危険性がある。		○				3.3.1.1	RFC3964(d) RFC6081(d)	
v6gtl-10	△	○			△		○	不正RAに関する課題	想定していない、もしくは意図的な不正RAにより、端末の通信に混乱・阻害・盗聴という問題が発生する。この問題は不正なDHCPサーバ設置と似た問題ではあるが、同一セグメントの端末に対して一斉にネットワーク設定を追加できる点で、不正RAの問題のほうが脅威である。		Sec.6				3.1.13 3.1.22	RFC6104(d) RFC6105(s)	http://gurubert.de/greylisting http://hopnet.free.fr/milter-greylist/
v6gtl-11	○	○			△		×	デュアルスタックサイトのプロトコル別品質	回線品質やサーバ処理能力に関して、IPv4とIPv6とで異なる場合があり、応答時間や到達性に違いが生じる可能性がある。		○						
v6gtl-12	○	○					×	アドレス選択に関する課題（マルチプレフィックスに関する課題）	複数のIPv6プレフィックス情報を有する端末が通信を行う際に、選択する始点アドレスによっては通信ができない場合がある。		○					RFC5220(d)	http://www.soumu.go.jp/main_content/000009743.pdf
v6gtl-13	△	△				△	×	IPv6ブリッジ機能（IPv6パススルー機能）サポートのみで「IPv6対応ルータ」であると誤認識されていることに関する課題	NTT東西が提供するIPv6サービスへの対応機器として「IPv6パススルー機能」を有する家庭用ルータが存在する。これらの製品は、フルのIPv6機能に対応していないにも関わらず、パッケージに「IPv6対応」と記載されている場合があり、利用者が誤って購入しIPv6インターネット接続サービスが利用できない場合がある。		○						
v6gtl-14	△	△			○			「IPv6対応ルータ」におけるブリッジ・フィルタに関する課題	IPv6パススルー機能を有する家庭用ルータでは、IPv6フィルタ機能がないものが多く、IPv6のセキュリティ的に問題がある。		○						
v6gtl-15	○						×	DNSへの登録に関する課題	IPv6においてアドレスを自動で割り当てる場合、IPv4とは異なり事前に正引き、逆引の事前登録が不能であり、新規接続されたnodeの名前解決を期待する事が出来ない。これは、サービスの実装によっては問題となる事がある。(例:SMTPやP2P)		○						
v6gtl-16	○	△					×	メールシステムの対応に関する課題	MXレコードにAAAAレコードのみが登録されている場合、MTAによっては送受信に問題が発生するものが存在する。		○						
v6gtl-17	○	○					×	MTAの逆引きによる迷惑メール対策に関する課題	メールシステムをIPv6対応した際に、受信先における逆引きチェックのための通信ができない場合がある。MTAではIPv6の場合も逆引き登録を行う必要がある。		○						
v6gtl-18	○	○					×	グレイリスティングにおける課題	グレイリスティングはIPアドレスをベースにした一時拒否フィルタリング手法である。ただし、既存のフィルタリングプログラムはIPv4アドレスを前提として処理しているため、グレイリスティングのIPv6対応が必要となるが、IPv6アドレス空間の広大さから運用上の困難が想定される。		○						
v6gtl-19	○	○					×	ブラックリストデータベースサービス（DNSBL）に関する課題	DNSBLはIPアドレスを利用したブラックリストデータベースを利用して、迷惑メール送信元からのメール受信を拒否する技術である。ただし、IPv4アドレスを前提として運用されているため、MTAをIPv6対応した場合に利用できない可能性がある。		○						http://www.ieice.org/jpn/books/kaishikiji/2010/201006.pdf http://www.janog.gr.jp/meeting/janog24/program/d2p5.html http://itpro.nikkeibp.co.jp/article/Watcher/20091015/338865/
v6gtl-20		○					×	アクセス回線におけるトラブルの切り分けに関する課題	IPv6インターネット接続サービスでは、アクセス回線事業者とISPのほかに、ユーザには見えない事業者（VNEやローミング）が存在する場合がある。そのため、通信トラブルがユーザから見えない事業者にて発生した場合、ユーザから見えている事業者のコールセンタのみで解決できない場合がある。		○						
v6gtl-21	○	○			△		×	L2マルチキャスト未対応機器に関する課題	L2マルチキャスト機能に未対応もしくは不具合があるL2機器が存在する場合、マルチキャスト通信を行うNDPが利用できず、IPv6通信ができなくなる。一部の端末が未対応な場合には、未対応な端末から他の端末へは、パケットは送信できるが受信できないといった非対称障害となる場合がある。		○						
v6gtl-22	○	○			△		△	IPv6マルチキャスト通信が宅内通信に悪影響を与える課題	映像配信サービスなどでIPv6マルチキャスト通信が利用される場合、必要のない機器にまでマルチキャスト通信が届くことで機器が高負荷状態となり、正常な通信に影響がでる場合がある。特に無線アクセスポイントをブリッジ接続している場合、無線通信区間に輻輳が発生する場合がある。		○					RFC4541(d)	
v6gtl-23	○	○				○	×	実装としてのミニマムスペックがないことに関する課題	家電やセンサー機器をIPv6ネットワークに接続する際の最低限必要なスペックが共通・共有化されておらず、実装によっては正常に通信できない場合がある。		○					RFC4294	
v6gtl-24						○	×	一時アドレス利用に関する課題 （そもそもこれが問題になるのか？）	IPv6アドレスの下位64ビットをランダムに変更する仕様（RFC4941）が、どのようなケースで推奨でき、どのようなことを解決するのか、正しい理解が共有化されていない。そのため、サーバの待ち受けアドレスとして使うような誤った利用があったり、企業ネットワークなどのIPアドレスの管理が困難になる。固定IPアドレスを前提としたPush型サービス利用に制限が出るなどの問題もある。		○						
v6gtl-25						○	×	IPv6アドレスのトレーサビリティに関する課題（EOUIの問題）	ISPにおけるIPv6プレフィックス割り当てがIPv4グローバルアドレス割り当てと比較してスタティック性が高い運用となる可能性があること、下位64ビットがMACアドレスを用いた運用となる場合があることから、IPv4とは異なるトレーサビリティが生じる場合がある。		○				3.3.1.3 3.3.1.4 3.3.1.8		
v6gtl-26		○			○		×	CGNやトランスレーションに関する課題	CGN、トランスレータの影響により、一部のアプリケーションやサービスにおいてユーザの期待通りに動作しない問題が発生する。具体的には、同時セッション数の制限や、サービス側で利用者のIPアドレスを特定できない点、プロトコル内でIPアドレスを持つ通信ができないなどの課題がある。		○						
v6gtl-27	○	○				○	×	誤解されそうな表現や古い情報に関する課題	「IPv6環境ではIPsecが必ず実装されている」、「グローバルアドレスを利用するためセキュリティが低下する」、「IPv6をアンインストールすると動作が速くなる」などの古い情報や誤った情報による混乱がある。		○						
v6gtl-28	○	○					×	IPv4で複数サブネットを利用している環境へのIPv6導入時の課題	IPv4とIPv6でトポロジが異なるネットワークとなる場合、ネットワークアクセスポリシがIPv4とIPv6で合致しない可能性があり、セキュリティ的に問題がある。		○						
v6gtl-29	○	○			○	○	○	DynamicVLAN（MACアドレスVLAN）とIPv6の相性が悪い問題（L2ネットワークとIPv6の課題）	MACアドレスVLANの実装では、一般的にマルチキャスト通信や不明なMACアドレス宛の通信がフラッディングされる。IPv6ではインターフェースに複数のアドレスを設定する仕様であることから、マルチキャストであるRAがすべてのポートに送信されることで意図しないセグメント設定が追加される。		○						
v6gtl-30		○					×	PMTUD BlackHoleに関する課題	ICMPv6が経路の途中でフィルタリングされている場合、PMTUDが実施できず、通信ができなくなる。		○						v6gd1-02を参照。
v6gtl-31		○			○		×	CPEの独自ドメインを解決できないことに関する課題	IPv6パススルー機能を有する家庭用ルータのホストにて、IPv6のDNSサーバが有効化されている場合、IPv6によるDNSクエリが発生するため、IPv4によるDNSクエリを期待しているCPEでは「setup」のような家庭用ルータ固有のドメインが解決できない場合がある。		○						
v6gtl-32	○	○				○	×	FWのフィルタ設定に関する課題	IPv4では、ホームネットワーク内部においてプライベートアドレスが利用されることが多く、実質的にNATがフィルタとして動作しており、外部から内部へのパケットの疎通等を制限していた。内部ネットワークにもグローバルアドレスが利用されるIPv6においては、IPv4と同様のアクセス制限を実施するためには、IPv4でのNAT装置と同じ位置にFW装置を置いて、パケットフィルタリングを設定する必要がある。このフィルタにおいては、フィルタをすることの是非をはじめとし、ディフォルトのフィルタはどうあるべきか、フィルタしてはならない制御パケットの設定、外部から内部への通信の許可手法等の検討課題が存在する。		○	○				4890(s, ICMPv6推奨フィルタ)	
v6gtl-33	○	○			△		×	断片化パケットのフィルタに関する課題	IPv6ではパケットの断片化/再構成は、エンドノードが経路MTUに従って実施することとなっている。このため、中間のノードではパケットの断片化/再構成は実施されない。しかしながら、経路の途中に存在するFWなどでは、パケットの中身を検査するために断片化されたパケットを再構成する必要がある。この再構成には、多大な資源を必要とする可能性があり、断片化機構に対するDoS攻撃などのターゲットになる可能性がある。また、RFC5722で提起されているような重複パケットの処理に関する問題等も考慮する必要がある。また、再構成をしない場合、本来フィルタすべきパケットを通してしまうといったことも発生する可能性がある。			○		3.2.1	5722(d,s)	
v6gtl-34					△	△	×	拡張ヘッダチェーンの走査に関する課題	IPv6では拡張ヘッダを必要に応じて定義することで、プロトコルの拡張性を確保している。拡張ヘッダは、IPv6ヘッダの後に数珠つなぎ状に配置される（拡張ヘッダチェーン）こととなっており、拡張ヘッダが複数存在する場合には通常、上位プロトコルのデータは、拡張ヘッダチェーンの最後に出現することになる。このため、中間のノードでパケットの中身を検査する場合、拡張ヘッダチェーンをすべて走査する必要がある。家庭用ルータなどの資源が限られた中間ノードでは、この作業に必要な資源の確保が困難になる可能性がある。この課題は、v6gd1-32 にあげている「断片化パケットのフィルタに関する課題」とも関連し、影響が拡大する可能性がある。			○				
v6gtl-35	○		○			△	×	FQDNを用いたACLにおける逆引き問題	一部のFirewall、tcp_wrappers、Apacheでは、FQDNもしくはドメイン名に対するマッティングを用いたアクセスコントロールが可能なものがあが、現状、IPv6においては、クライアント側のアドレスの逆引き登録をしている例が一般的ではなく、かつ、プライバシーアドレス拡張などで定期的に変更されるため、IPv6においては、利用が期待できない。								
v6gtl-36	△	○					×	稼働監視等における、FQDNを用いることによる課題	稼働監視システムを利用する際に、監視対象ノードの指定をFQDNで行う場合、IPv6/IPv4フォールバックが発生することにより、望んだ情報を取得できない可能性がある。								
v6gtl-37	○	○			△		×	アドレス省略記法に起因するセキュリティ問題	IPv6アドレスをRFCに基づき処理した場合、省略記法によって短縮することが可能であり、その結果sort等の処理を実施する際に期待した結果とならない可能性がある。処理量によっては、負荷が増大することも想定される。		○		○			RFC5952(s)	
v6gtl-38	○	○				△	×	IPv4/IPv6トンネル(入れ子)混在問題	デュアルスタック対応している機器、OSが存在している場合、IPv6通信を意識、想定していない状況であっても機器/OSの設定、接続構成などの環境が整うことで意図しない、あるいは意識しないトンネルによるIPv4/IPv6通信が発生する。				○			RFC3964(s) RFC4891(s)	
v6gtl-39	○		○	○			×	Translatorによるアドレス変換とcookieの不整合に起因する認証問題	エンドユーザとサーバで利用しているIPのVersionが異なり、かつ中間段にTranslatorが存在する場合、TranslatorはIP Addressのみを変換し、cookieのデータは変更しないため、cookie内のアドレス情報と通信に利用されるアドレス情報が異なったものになる可能性がある。その結果、サーバ側のアプリケーションの実装によっては、cookieの取り扱い時にBuffer overflowを引き起こしたり、認証に利用する情報が一致しないことによる認証失敗などの問題が発生する可能性がある。				○				
v6gtl-40		○			△	△	○	詐称した近隣要請広告（NS/NA）メッセージを用いた通信の妨害	攻撃ノードが、任意のノードからの近隣要請に対して、使われていないリンク層アドレスを格納した広告を返答したようになりますまことでDoS攻撃が可能となる。また、攻撃ノードから近隣ノードに対して一方的に NA を送付することでも、同様に DoS 攻撃を成立させることが可能となる。						3.1.1	RFC3756(d, s)	
v6gtl-41		○			△	○	×	RH0（Route Type 0）を用いた通信の妨害	RH0を利用して細工されたパケットによりルーティングループを引き起こすことが可能である。						3.1.2	RFC5095(d, s)	
v6gtl-42		○			△	○	○	OSPFv3の未知のLSAを用いた通信の妨害	OSPFv3ではLSタイプフィールド内にUビットが用意されており、未知のLSAを柔軟に処理できる実装となっている。このUビットが1の場合は、LSAは未知であることを意味し、ルータは既知のLSAとみなしてLSDBに集約しなければならない。そして、LSタイプフィールドに書き込まれたフラディングスコープに従いフラッドされる。従って、あるノード が大量の無意味なLSAをフラッドすることで、ルータのLSDB が増大し、大量のLSA がフラッドしてしまうことになる。これにより、ルータのLSDBをオーバーフローさせ、セグメント内で大量にフラッドされたLSAでDoS 攻撃を行うことが可能であると考えられる。						3.1.3		実装上は未知のLSAをフラッディングしない設定が搭載されることにより対応 可能と考えられる。
v6gtl-43		○			△	○	○	近隣キャッシュを溢れさせることによる通信の妨害	攻撃者はアドレスの異なる大量の近隣要請メッセージを発行し、そのすべての近隣要請メッセージに対して近隣広告メッセージを送信する。このとき、ルータはすべてのアドレスに対する近隣ノードリストを近隣キャッシュに保管しなければならないため、攻撃者はルータの近隣キャッシュを溢れさせることができると考えられる。						3.1.4	RFC3756(d, s)	

v6gtl-id	システム設計時	運用時	Webアプリ実装時	クライアントアプリ実装時	ハードウェア実装時（ハードウェア搭載のソフトウェアの実装時も含む）	仕様	同一リンクからの攻撃	Short Name	Short Description	v6pc/v6app-swg	v6pc/v6fix-swg	v6pc/v6HGW-swg	v6pc/sec-wg	NIST/sp800-119	IPv6検証協議会（tvc）	RFC/Draft（問題の定義または発生源はd、ソリューションの提案はs）	備考
v6gtl-44					△	○	○	P2Pリンクによるパケットループ	IPv6の最小サブネットが/64であるため、ルータ間のポイントツーポイント(P2P)のリンク にも/64を割り当てることがある。この場合、利用されるアドレスは2つで、その他のアド レスは利用されず、広大な空きアドレスが存在することになる。この空きアドレス宛てに 送信されたパケットは、ルータの実装によっては、P2P リンク内でパケットのTTLが期限切れになるまでループしてしまう等の問題があり、DoS 攻撃に使用される可能性が あることがが指摘されている。						3.1.5	RFC6164(d, s) RFC4443(s)	
v6gtl-45						○	×	6to4を用いるReflected DoS	現状の6to4では、ある6to4ルータが信頼できるかどうかを判定するためのメカニズムが存在しない。このため6to4の仕組みを悪用して送信元アドレスを偽装し、Reflected DoS攻撃が行われる可能性がある。						3.1.6	RFC3964(d)	
v6gtl-46		△				△	○	Multicast Listener Discovery（MLD）を用いた通信の妨害	攻撃者がMulticast Listener Reportメッセージ(もしくはグローバルスコープマルチキャスト)を大量に送付す ることにより、境界ルータのマルチキャストルーティングテーブルを溢れさせることができる可能性がある。また、攻撃者が詐称したMulticast Listener Doneメッセージを送信することにより、マルチキャストストリームを受信しているノードの情報をマルチキャストルーティングデー モンから削除させることができる可能性がある。						3.1.7		
v6gtl-47		△				△	△	大量セッション作成によるNAT66(NAT64)状態テーブルの枯渇	悪意のある端末が2の64条個のアドレス空間を使用して自らのIPv6アドレスを変化させながら らコネクションを大量に作成した場合、NAT機器が内部にコネクションについての情報を保持しながらアドレス変換を行っているケースでは、攻撃によりNAT機器の状態テー ブルが枯渇してサービスが妨害される恐れがある。IETFで議論されているNAT66ではステートレスな (NAT の状態テーブルを保持し ない) アドレス変換手法が定義されているが、FreeBSDにおけ るpfなど、実装によっ ては状態テーブルを保持しているため、このような攻撃に対する注意が必要であると考えられる。						3.1.8	RFC4966(d) RFC6296(s)	
v6gtl-48		△			△	△	○	MACアドレスの異なる大量のパケット送信によるスイッチFDBの枯渇	IPv6ではIPv4より多くのMACアドレスを同時に使用することが可能なため、それらが一斉に使用された場合に、イーサーネットフレームを転送するスイッチのFDBが枯渇し、サービスが妨害される可能性がある。						3.1.9		
v6gtl-49					△	○	×	Pad1オプションを用いた通信の妨害	攻撃者がPad1オプションを大量に指定したパケットを大量に送信し、受信側ホストにパディングの処理を強制的に発生させることで、多大なCPUやメモリを消費させ、受信側ホス トのサービスを妨害することができる可能性がある。						3.1.12		きちんとしたOS実装、FWであれば問題はない。
v6gtl-50		○					○	不正なDADを用いたIPv6アドレスの取得の妨害	近隣要請に対して、同一リンク内の不正なノードが要請を受け取った時に、即座に自身も同アドレスでDADを行っているように振舞うか、要請に応 えて広告を出しているように振舞うことで、対象ノードのアドレス取得を妨害することが可能であると考えられる。						3.1.15	RFC3756(d, s)	
v6gtl-51		○					○	マルチキャストを用いたネットワークに関する情報の収集	攻撃者は特定機能ノード宛マルチキャストパケット(ex. all-routers multicast address, all-nodes multicast address)を送信し応答を記録することで、ネットワークに関する情報を取得できると考えられる。						3.1.16	draft-gont-opsec-ipv6-host-scanning-01	
v6gtl-52		○			△	△	○	詐称したマルチキャストパケットを用いた通信の妨害	ICMPv6ではIPv4でのICMPと違いマルチキャスト宛てのパケットに対するエラー返答が許されている。このためにエラーメッセージ(ICMP Parameter Problem)を生じさせるようなパケットをマルチキャストアドレス宛に送信すると大量のICMPエラーメッセージトラフィックが発生すると考え られる。このトラフィックを引き起こしたメッセージの送信元アドレスを詐称することでホストに対してDoS攻撃が可能であると考えられる。						3.1.17	RFC4443(d, s)	
v6gtl-53						△	○	DHCPv6を用いた通信の盗聴	攻撃者がMフラグをIに指定したRA（＝ステートフルアドレス自動構成モード）を配布した上で、自らをDHCPv6サーバとして指定し、さらにDHCPv6 によって自らをDNSサーバとして指定することにより、クライアント同士間の通信を盗聴することができる。すなわち、クライアント側から他のシステムに対して、名前解決を伴うデータ通信を行った場合、攻撃者ノードはクライアント側からの問い合わせに対して、自分のDNS サーバを用いて自分のアドレスを記載したAAAAレコードを返す。その結果、クライアント側から通信相手に向かうトラフィックが攻撃ノードに向かうため、トラフィックの内容を盗聴することができる。						3.1.18	RFC3315(d, s)	
v6gtl-54		○				○	○	DHCPv6 Solicitメッセージを用いたメモリとアドレスプールの枯渇	DHCPサーバとクライアント間の通信中に、攻撃者はMACアドレスとDUIDを変化させた要請メッセージを大量に発行し、DHCPサーバからの広告メッセージに対しては一切応答しないことにより、DHCPサーバの多大なメモリを消費させることができ、サービスを妨害することができる。また、同様の要請メッセージを用いて、DHCPサーバからの広告メッセージに対してRequestメッセージを送信し、シーケンスを完遂させることで、DHCPサーバの持つアドレスプールを枯渇させられる可能性がある。						3.1.19	RFC3315(d, s)	
v6gtl-55		○					○	脆弱性攻撃ツールを用いたIPv6ホストへの攻撃	これまで、IPv4においては機器の対応、運用ノウハウの蓄積などにより、安全なネットワーク環境が構築されてきた。しかし、IPv6においては、機器の対応、ノウハウの蓄積等がまだあまりなく、デフォルトの設定のまま運用されている可能性がある。また、IPv4ではNATで保護されていた環境が、IPv6ではNATが使用されないことが多いため、FWが適切に設定されていない場合は危険にさらされる可能性がある。						3.1.20		
v6gtl-56						○	○	MTU調整を悪用した通信妨害	攻撃者が詐称したパケット過大メッセージを不正に出すことで正常なパスMTU探索を阻害し、MTUの値を減少させ伝送効率を落とすことが可能であると考えられる。						3.1.21	RFC1981(d)	中継段で実施される可能性がある。MTUが1280になることによる複合的な問題の発生も考えられる。
v6gtl-57		△				○	○	マルチキャストDNSを使用した虚偽の情報の送信	LLMNR やmDNSではマルチキャストを利用して同一リンク上のホストに対してDNSの問い合わせを送信する、あるいはマルチキャストを使用して名前とIPアドレスの組を同一リンク上ホストへの広告を行う。しかし、これらの名前解決には認証の機構が備わっていないため、悪意のある端末が問い合わせに対して正規のホストを詐称して応答したり、正規のホスト名を詐称して情報を広告することが可能である。これにより、アプリケーショントラフィックが利用者の意図しない宛先に誘導され、盗聴などの中間者攻撃が成立するおそれがある。						3.1.23	RFC4795(d,s) draft-cheshire-dnsext-multicastdns-15(d,s)	
v6gtl-58					○	△	○	Anycast DNSを使用した虚偽の情報の送信	IPv6を使用する機器の一部では、名前解決に使用するDNSサーバのアドレスとしてエニーキャストを使用したアドレスが既定値として設定されている。手動でのDNSサーバの指定を行わない場合、もしくはアドレスの自動設定のシーケンスでDNSサーバの指定が行われない場合には、このエニーキャストアドレスがDNSサーバとして使用される。このエニーキャストアドレスはサイトローカル（現在のIPv6の仕様からはRFC3879にて削除されている）を用いているため、グローバルなIPv6ネットワーク上には存在しないアドレスとなっている。しかし、悪意のある端末はルータ広告（RA）を使用することで、エニーキャストアドレス宛のパケットを自端末に誘導することが可能である。この時、悪意のある端末でDNSサーバを動作させれば、問い合わせに対して任意のIPアドレスを応答として返すことができるため、アプリケーショントラフィックが利用者の意図しない宛先に誘導されて、盗聴などの中間者攻撃が成立する恐れがある。						3.1.24		
v6gtl-59				○		△	○	虚偽のDHCPv6サーバで広告した虚偽のDNSサーバからの大量のAAAA レコードの送信によるアプリケーショントラフィックの妨害	悪意のあるDNSサーバが、ホストからの名前の問い合わせに対して大量の（実在しないアドレスを示す）AAAAレコードを含むパケットを応答として送信した場合、問題のある実装をしているアプリケーションプログラムは、得られた大量の応答に対して順に接続を試みるため、接続が失敗するまでの時間を大きく引き延ばされ、事実上アプリケーションが利用不能になる可能性がある。						3.1.25		
v6gtl-60	○	○					×	マルチホーム化によるIDS回避	マルチホーミング・マルチプレフィックス環境において複数のIPアドレスを持つホスト同士で通信を行う際に、TCPであれば複数のコネクションを結ぶ必要があるところ、SCTPを用いると1つのアソシエーションで済ませることが可能となる。このマルチホーミングを利用することによって、アソシエーションを結ぶ際に送信者と受信者のもつアドレスを交換し保持するので途中でアソシエーションを切ることなく異なる経路にデータを送信し続ける経路切り替えが可能となる。セッションを張ったまま経路の切り替えが行えることから、どの経路にデータを流すのかを特定されることなく、様々な経路にデータを送信することができる。そのため、攻撃を検知する方としては攻撃される経路の予測に基づいた対策が取りにくいと考えられる。						3.2.2		本質的にはNW設計の問題。
v6gtl-61	○	○					×	経路の非対称性を利用したIDS回避	トンネリング技術を用いるとパケットの行きと帰りの経路が異なる、いわゆる経路の非対称性の問題が発生することがある。例えばトンネリング技術の一つである6to4のフレームワークでは、6to4ホストからIPv6ホストへの経路と、IPv6ホストから6to4ホストへの経路は一般に異なる。すなわち、6to4ホストとIPv6ホスト間の相互通信であっても、介在するリレールータが関与するのは一方向だけという場合がある。ルータの中には、TCP/UDP などのセッション単位をステートフルに監視するタイプのセキュリティシステムを搭載しているものがあるが、こうした方法が無効となる可能性がある。						3.2.3		本質的にはNW設計の問題。
v6gtl-62	○	○	○	○			×	IPv6でのリモートエクスプロイト攻撃による未対応IDSの回避	IPv4環境では、攻撃対象のホストのOSやサーバアプリケーションが持つ脆弱性をネットワーク経由で突いて侵入を行う、リモートエクスプロイト攻撃が極めて多く発生してきた。近年ではこの攻撃手法はマルウェアにも実装され、多くのマルウェアがリモートエクスプロイト攻撃によって世界中に蔓延する結果をもたらしている。リモートエクスプロイト攻撃の多くはアプリケーションレイヤの脆弱性を突くことで成立するため、たとえL3のプロトコルがIPv4からIPv6に変更されたとしても、上位のアプリケーションが同様の脆弱性を持つ限り、リモートエクスプロイト攻撃が成立する可能性が高いと考えられる。そのため、IPv6対応のIDS/IPSは、IPv4だけでなく、IPv6のリモートエクスプロイト攻撃についても検知できる必要があるが、現状のIDS/IPSの中にはIPv6に関する機能がIPv4と比較して不足している可能性がある。						3.2.4		
v6gtl-63	△	○			○	○	×	大量のセッションの作成によるFWのセッションテーブル枯渇	悪意のある端末がIPv6の2^64個の広大なアドレス空間を使用して、自らのアドレスを変化させながらコネクションを大量に作成した場合、ファイアウォールのステートフルインスペクション用の状態テーブルはIPv4の場合よりも容易に枯渇し、サービスが妨害される恐れがある。						3.2.5		
v6gtl-64	○	○				○	×	中間者攻撃によるバインディング管理鍵の入手及び移動ノードへのなりすまし	Mobile IPv6における往復経路確認手順（Return Routability Procedure）では、ホームテスト、気付けテストという二重のテストによって移動ノードがホームエージェントに認められたノードであることを確認することになっている。しかしこのテストでは暗号路を用いることが強制されていないため、MNのすべての通信を見ることができる中間者を仮定した場合、中間者は2 つのテストの結果生成されるバインディング管理鍵を入手することができ、移動ノードになりすますことができてしまうと考えられる。						3.3.1.2 3.3.1.5	RFC6275	
v6gtl-65						△	○	MACアドレスのcompany_id特定による可変アドレス空間24 ビットに対するスキャン行為	IEEE 48-bit MAC識別子からIEEE EUI-64識別子を生成する方法から分かるように、company idを一つに絞り込めば、可変のアドレス空間は24 ビットしか残らないため、IPv4より容易にスキャン行為を行うことができる可能性がある。例えばある会社のセットトップボックスに脆弱性が見つかった場合、その会社のcompany idが絞り込めるため、従来は脆弱性を持つノードを発見するために1セグメントあたり64ビットのネットワークスキャンを行う必要があったところが、24 ビットのネットワークスキャンで可能となる。						3.3.1.10		
v6gtl-66	○	△					×	多重カプセル化によりセキュリティデバイスの負荷を増大させるサービス妨害	カプセル化されたパケットの中身は別プロトコルで記述されているため、カプセルの外側のプロトコルから解釈することができない。カプセル化されたパケットの中身をセキュリティ等のために確認したいと考えた場合、一旦カプセル化を解き、中身のプロトコルに従い解釈する必要がある。セキュリティデバイスにとっては一重のカプセル化ならば大きな負荷にはならないが、カプセル化が多重であった場合にどこまで解いて確認してよいか判断が難しくなる。危険なパケットが入っている可能性を考えてカプセル化されている限り何重でもパケットを解き続けることは、それ自体が大きな負担になり脆弱性にもなり得る。						3.3.2.2		
v6gtl-67		○			△	○	○	特定のリンクローカルやエリアを指定し、意図的に無意味な OSPFv3 LSA を大量に フラッドすることによるルータに対するDoS 攻撃	フラディングスコープは、LSAヘッダ内のS1、S2の2ビットの値を設定する事で明示できる。こ れにより、従来バージョンでは、スコープを超えた無意味なLSAがフラッドされていたのに対して、新バージョンではスコープ外にフラッドする無意味なLSAを抑制する事が可能になった。しかし、その一方で、特定のリンクローカルやエリアを指定し、意図的に無意味なLSAを大量にフラッドする事でルータに対する DoS 攻撃が行えてしまう可能性がある。						3.3.2.5		v6gdl-41を参照。
v6gtl-68	○	○					×	アドレスの変更によるセキュリティデバイスの回避	IPv6では、一つのインターフェースに複数のアドレスを付与すること可能であるため、通信に用いるアドレスをランダムに変更することができる。このためIPv4環境と比較して、問題のある通信を検知することが難しくなることが考えられる。例えば、C&C(Command and Control)サーバとの通信において、パケット毎に送信先アドレスを変えることによって、セキュリティデバイスを回避できる可能性がある。						3.3.3.1		
v6gtl-69		○			○	○	×	感染システムのIPsec暗号化利用によるセキュリティデバイスの回避	IPsecは、攻撃者の振る舞いを隠すことに悪用される可能性がある。例えば、サイト 内のあるシステムがボットに感染した場合、そのボットはC&C(Command and Control) サーバから新しい攻撃コードをダウンロードする際に、IPsecのESPを用いて通信内容を暗号化することによって、内部ネットワークとの境界に置かれたセキュリティデバイスを回避できる可能性がある。						3.3.3.2		

※ 表の見方について（行項目の説明）

v6gtl-id	各課題について一意に割り当てたID番号です。
システム設計時～同一リンクからの攻撃	その課題がどの時点で問題となるか、あるいは何に依存した課題であるかを分類しています。
Short Name～Short Description	課題のタイトル及び説明です。
v6pc/v6app-swg～RFC/Draft	課題の指摘元を表します。v6pc/v6app-swg～v6pc/sec-wgは、それぞれIPv6普及・高度化推進協議会のアプリケーションのIPv6対応検討SWG、IPv6導入に起因する問題検討SWG、IPv6家庭用ルータSWG、セキュリティWGでの指摘事項です。NIST/sp800-119は、米国National Institute of Standards and TechnologyのSP800-119ドキュメントでの指摘事項です。IPv6検証協議会(tvc)は、IPv6技術検証協議会のセキュリティ評価・対策検証部会最終報告書での指摘事項です。RFC/DraftはIETFでのRFC及びInternet-Draftsでの指摘事項です。