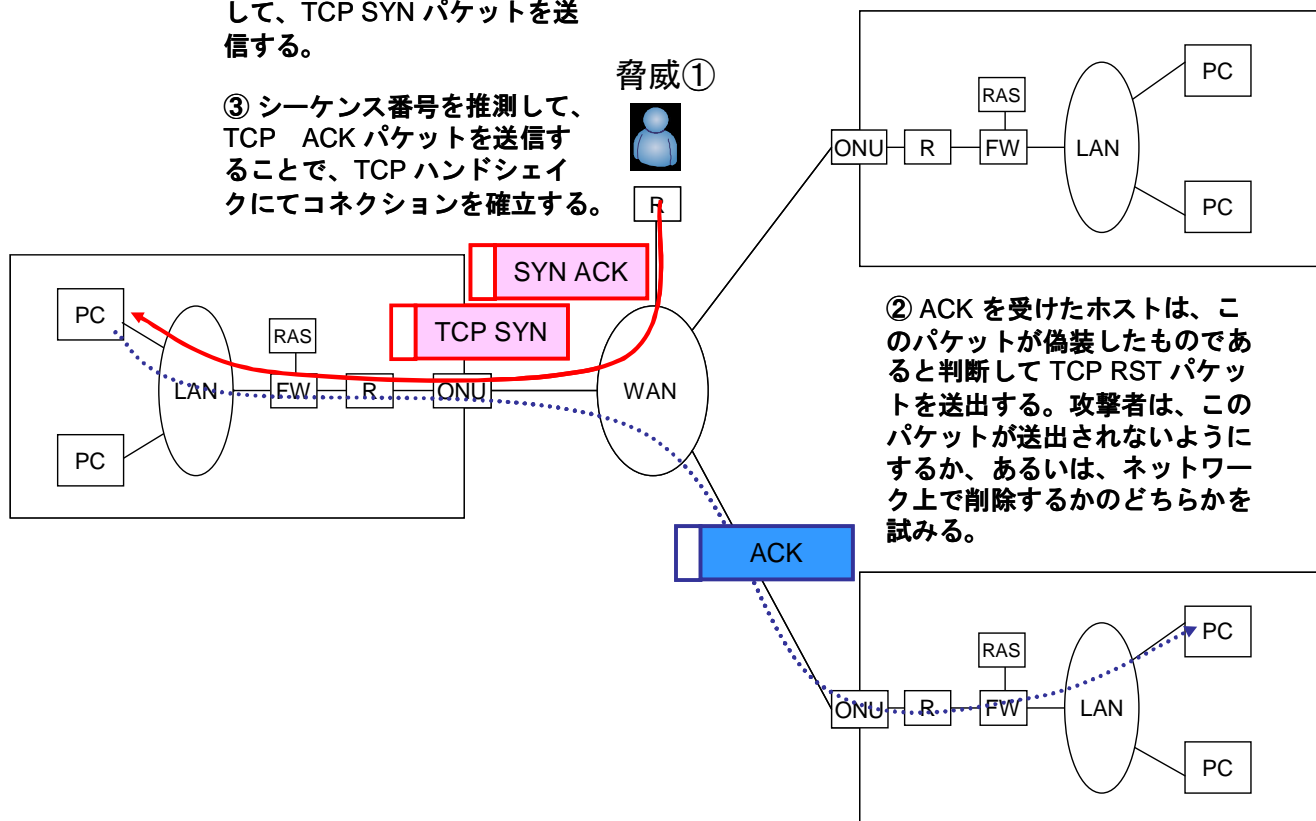


項番	T16. シーケンス番号推測攻撃	脅威の区分	改ざん	守るべき資産	TCPコネクション	対象	AP/NW
解説	攻撃者は標的に信頼されたホストの口を塞ぎ、標的に話しかける際に、信頼されたホストの IP アドレスを偽装して、次に最初に使われるシーケンス番号を推測することに基づく 3 ウェイハンドシェイクを完了させる。標的への通常のコネクションはシーケンス番号の状態の情報を集めるのに使用され、このシーケンス全体が、アドレスに基づく認証と組み合わせられて、攻撃者が標的となるホスト上でコマンドを実行できるようになる可能性がある。						
対策の概要	<ul style="list-style-type: none"> <li>- 共通鍵/公開鍵認証によるエンティティ認証</li> <li>- 暗号ペイロード</li> <li>- メッセージ認証</li> </ul>						

脅威発生イメージ

① 送信元の IP アドレスを偽装して、TCP SYN パケットを送信する。

③ シーケンス番号を推測して、TCP ACK パケットを送信することで、TCP ハンドシェイクにてコネクションを確立する。



② ACK を受けたホストは、このパケットが偽装したものであると判断して TCP RST パケットを送出する。攻撃者は、このパケットが送出されないようにするか、あるいは、ネットワーク上で削除するかのどちらかを試みる。

<対策の概要>

- ・共有鍵や証明書(公開鍵)を使用してエンティティ認証を行っている場合には、シーケンス番号を予測することが難しいため、パケットを挿入することができなくなる。
- ・暗号ペイロードを使用している場合には、攻撃者が暗号ペイロードを偽装することができないため、攻撃は成功しない。
- ・メッセージ認証を使用している場合には、データ生成元認証を使用することにより、送信元の偽装を防ぐことができる。
- ・否認防止のために、証拠収集やアーカイビングを実施することで、攻撃を検知することが可能となる。
- ・インGRESSフィルタリングを使用することで、接続元を制限することができる。

脅威の内容 収集した情報からシーケンス番号を偽装し、IP アドレスの詐称とあわせて TCP のコネクションを確立する。

対策

対策の内容	参考文献	対策表との対比		リスク	
		方法	有効度	頻度	影響度
最も普及したアクセスコントロールメカニズムは、単純なユーザ名/パスワードです。ユーザは、利用しようとしているホストに、ユーザ名と再利用可能なパスワードを入力します。このシステムは、単純な待ち伏せ攻撃に対して脆弱です。ここで、攻撃者は、回線外でパスワードを盗聴し、新しいセッションを開始し、そのパスワードを入力します。この脅威は、TLSやIPSECのような暗号化されたコネクション上にそのプロトコルを置くことによって緩和できます。防護されていない(平文)ユーザ名/パスワードシステムは、IETF標準において許容されていません。	RFC3552	ユーザ名/パスワード	△	高	しばしば、それゆえ、このトラフィックを読むことができる攻撃者は、パスワードを捕捉し、それをリプレイすることができます。換言すれば、攻撃者は、サーバーに対してコネクションを開始し、クライアントのふりをして、捕捉されたパスワードを使ってログインすることができます。
ユーザ名/パスワードよりも高いセキュリティを要求するシステムは、しばしば、ワンタイムパスワードスキームかチャレンジレスポンスのいずれかを採用します。ワンタイムパスワードスキームにおいて、ユーザには、パスワードのリストが提供され、これは、順番に毎回1つずつ使わなければならないものです。(しばしば、これらのパスワードは、何らかの秘密鍵から生成されるので、ユーザは、単純に、順番に次のパスワードを計算できます。)SecureIDやDESGoldは、このスキームの流派です。	RFC3552	ユーザ名/ワンタイム	△	高	ユーザ名/パスワードよりも高いセキュリティを要求するシステムは、しばしば、ワンタイムパスワード[OTP]スキームかチャレンジレスポンスのいずれかを採用します。
企業のように比較的大きな機関によって通常とられているパスワード盗聴に対する予防措置は、OTP(ワンタイムパスワード)システムを使用することです。	RFC2504				
両種のスキーム(ワンタイムパスワードスキームかチャレンジレスポンススキーム)は、リプレイ攻撃に対する防護を提供しますが、しばしば、「オフライン鍵検索攻撃」(待ち伏せ攻撃の1形態)に対して脆弱なままです。:既述のように、しばしば、ワンタイムパスワードやレスポンスは、共有された秘密から計算されます。攻撃者が使われている関数を知っている場合、彼は、正しい出力を作り出すものを発見するまで、すべての共有された秘密の候補を単に試すことができます。共有された秘密がパスワードであり、「辞書攻撃」をしかけることができる場合、これは容易になります。(「単なる乱雑な文字列ではなく、通常の単語(もしくは文字列)のリストを試すこと」を意味します。)これらのシステムは、しばしば、積極的な攻撃に対しても脆弱です。通信セキュリティがセッション全体について提供されない限り、攻撃者は、単に、認証が行われるまで待って、コネクションをハイジャックすることができます。	RFC3552	ユーザ名/チャレンジ	△	高	ユーザ名/パスワードよりも高いセキュリティを要求するシステムは、しばしば、ワンタイムパスワード[OTP]スキームかチャレンジレスポンスのいずれかを採用します。
ユーザ名/パスワードよりも高いセキュリティを要求するシステムは、しばしば、ワンタイムパスワードスキームかチャレンジレスポンスのいずれかを採用します。チャレンジレスポンススキームにおいて、ホストとユーザは、何らかの秘密を共有します。(これは、パスワードとして現れます。)ユーザを認証するために、ホストは、ユーザに(乱雑に生成された)チャレンジを提供します。ユーザは、チャレンジとその秘密に基づいていくつかの関数を計算し、それをホストに提供し、ホストはそれを検証します。しばしば、この計算は、DESGoldカードのような携帯デバイスで処理されます。	RFC3552				
両種のスキーム(ワンタイムパスワードスキームかチャレンジレスポンススキーム)は、リプレイ攻撃に対する防護を提供しますが、しばしば、「オフライン鍵検索攻撃」(待ち伏せ攻撃の1形態)に対して脆弱なままです。:既述のように、しばしば、ワンタイムパスワードやレスポンスは、共有された秘密から計算されます。攻撃者が使われている関数を知っている場合、彼は、正しい出力を作り出すものを発見するまで、すべての共有された秘密の候補を単に試すことができます。共有された秘密がパスワードであり、「辞書攻撃」をしかけることができる場合、これは容易になります。(「単なる乱雑な文字列ではなく、通常の単語(もしくは文字列)のリストを試すこと」を意味します。)これらのシステムは、しばしば、積極的な攻撃に対しても脆弱です。通信セキュリティがセッション全体について提供されない限り、攻撃者は、単に、認証が行われるまで待って、コネクションをハイジャックすることができます。	RFC3552				
数多くの鍵の問題を解決するためのひとつのアプローチは、認証する主体間を仲介するオンラインの「信用できる第三者(trustedthirdparty)」を使うことです。(一般的にKDC(KeyDistributionCenter)と呼ばれる)信用できる第三者は、共通鍵またはパスワードをシステム中の各主体と共有します。各主体は、まず、KDCと連絡を取ります。KDCは、ランダムに生成された両者の鍵で暗号化された共通鍵を含むチケットを各主体に提供します。正しいペアのみが共通鍵を復号できるので、そのチケットを信用できる協定を確立するために使うことができます。今日に至るまで最も普及したKDCシステムは、[KERBEROS]です	RFC3552				
自動化された鍵管理は、セッション鍵を確立するために使われる必要があります。	RFC4107				
自動化された鍵管理テクニックと関連づけられたプロトコルは、ピアが生きていることを確認し、再生(replay)攻撃から護り、短期セッション鍵の源泉を認証し、プロトコル状態情報を短期セッション鍵と関連づけ、「フレッシュな短期セッション鍵が生成されていること」を確認します。さらに、自動化された鍵管理プロトコルは、暗号アルゴリズムについての交渉メカニズムを含めることによって、相互運用可能性を向上させることができます。これらの可変な機能は、マニュアル鍵管理で達成することが不可能、もしくは、極めて面倒です。	RFC4107				
Kerberos は、分散ネットワークセキュリティシステムであり、セキュアでないネットワークに認証機能を提供します。アプリケーションの要求に従って、インテグリティと暗号化の機能も提供することができます。	RFC2196				
4.3 自動鍵配送 IP セキュリティを広く展開し利用するには、インターネット標準規模の鍵管理プロトコルが必要となる。	RFC1825				



<p>IPsec は、IP 層に導入されるので、ネットワークのコードにまで入り込む可能性があります。これを実装することは、一般に、新しいハードウェアか、あるいは、新しいプロトコルスタックのいずれかを要求します。他方、これは、アプリケーションにとっては、相当に透過的です。IPsec 上で動作するアプリケーションは、それらのプロトコルをまったく変更することなく、向上したセキュリティを得ることができます。しかし、少なくとも、IPsec がより広く配備されるまでは、大部分のアプリケーションは、「自身のセキュリティメカニズムを規定する代わりに、IPsec の上で動作するもの」と想定しては、いけません。大部分の最近の OS (オペレーティングシステム) は、利用可能な IPsec をもっています。大部分のルーターは、少なくとも、コントロールパスについては、もっていません。TLS を使うアプリケーションは、アプリケーション固有の認証の利点を生かすようにする可能性が高いです。</p>	RFC3631																										
<p>IPsec についての鍵管理は、証明書か、「共有された秘密」のいずれかを使うことができます。明白な理由によって、証明書が選択されます。しかし、それらは、システム管理者に、より多くの頭痛をもたらす可能性があります。</p>	RFC3631																										
<p>3.1.1. ESP Encryption and Authentication Algorithms</p> <p>These tables list encryption and authentication algorithms for the IPsec Encapsulating Security Payload protocol.</p> <table border="1"> <thead> <tr> <th>Requirement</th> <th>Encryption Algorithm (notes)</th> </tr> </thead> <tbody> <tr> <td>MUST</td> <td>NULL (1)</td> </tr> <tr> <td>MUST-</td> <td>TripleDES-CBC [RFC2451]</td> </tr> <tr> <td>SHOULD+</td> <td>AES-CBC with 128-bit keys [RFC3602]</td> </tr> <tr> <td>SHOULD</td> <td>AES-CTR [RFC3686]</td> </tr> <tr> <td>SHOULD NOT</td> <td>DES-CBC [RFC2405] (3)</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Requirement</th> <th>Authentication Algorithm (notes)</th> </tr> </thead> <tbody> <tr> <td>MUST</td> <td>HMAC-SHA1-96 [RFC2404]</td> </tr> <tr> <td>MUST</td> <td>NULL (1)</td> </tr> <tr> <td>SHOULD+</td> <td>AES-XCBC-MAC-96 [RFC3566]</td> </tr> <tr> <td>MAY</td> <td>HMAC-MD5-96 [RFC2403] (2)</td> </tr> </tbody> </table>	Requirement	Encryption Algorithm (notes)	MUST	NULL (1)	MUST-	TripleDES-CBC [RFC2451]	SHOULD+	AES-CBC with 128-bit keys [RFC3602]	SHOULD	AES-CTR [RFC3686]	SHOULD NOT	DES-CBC [RFC2405] (3)	Requirement	Authentication Algorithm (notes)	MUST	HMAC-SHA1-96 [RFC2404]	MUST	NULL (1)	SHOULD+	AES-XCBC-MAC-96 [RFC3566]	MAY	HMAC-MD5-96 [RFC2403] (2)	RFC4305				
Requirement	Encryption Algorithm (notes)																										
MUST	NULL (1)																										
MUST-	TripleDES-CBC [RFC2451]																										
SHOULD+	AES-CBC with 128-bit keys [RFC3602]																										
SHOULD	AES-CTR [RFC3686]																										
SHOULD NOT	DES-CBC [RFC2405] (3)																										
Requirement	Authentication Algorithm (notes)																										
MUST	HMAC-SHA1-96 [RFC2404]																										
MUST	NULL (1)																										
SHOULD+	AES-XCBC-MAC-96 [RFC3566]																										
MAY	HMAC-MD5-96 [RFC2403] (2)																										
<p>ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality. The set of services provided depends on options selected at the time of Security Association (SA) establishment and on the location of the implementation in a network topology.</p>	RFC4303																										
<p>このメモでは、IPSEC 暗号ペイロードの改訂版 [ESP] および IPSEC 認証ヘッダの改訂版 [AH] での認証の仕組みとして、SHA-1 アルゴリズム [FIPS-180-1] と組み合わせた HMAC アルゴリズム [RFC-2104] の使用方法について説明する。HMAC-SHA-1 は、データ生成元認証とインテグリティ保護を提供する。</p>	RFC2404																										
<p>暗号ハッシュ関数を使用してメッセージ認証を行なう仕組みである HMAC について記述する。HMAC は、MD5 や SHA-1 などの反復暗号ハッシュ関数を秘密の共有鍵と組み合わせて使用する。HMAC の暗号としての強度は、使用しているハッシュ関数のプロパティに依存する。</p>	RFC2104																										
<p>この文書の執筆時点では、特定の暗号アルゴリズムとともに HMAC-SHA-1-96 アルゴリズムを使用することを妨げる問題は知られていない。</p>	RFC2104																										
<p>暗号ハッシュ関数を使用してメッセージ認証を行なう仕組みである HMAC について記述する。HMAC は、MD5 や SHA-1 などの反復暗号ハッシュ関数を秘密の共有鍵と組み合わせて使用する。HMAC の暗号としての強度は、使用しているハッシュ関数のプロパティに依存する。</p>	RFC2104																										
<p>HMAC [RFC2104] は、選好される shared-secret 認証テクニックです。両者が同一の秘密鍵を知っている場合、HMAC は、あらゆる任意のメッセージを認証するために使えます。これは、乱雑なチャレンジを含み、これは、「HMAC は、古いセッションのリプレイを予防するために採用できること」を意味します。</p>	RFC3631																										
<p>ESP は守秘性、データ生成元認証、コネクションレスインテグリティ、リプレイ防止サービス (部分的なシーケンスインテグリティの形式)、そして限定されたトラフィックフロー 守秘性を提供するために使用される。提供されるサービスは、セキュリティアソシエーションの確立時に選択されたオプションとその実装の配置に依存する。守秘性は、他のどのサービスとも独立して選択してもよい。ただし、(ESP 自身、または別に AH を使用することによって提供される) インテグリティや認証を伴わないで守秘性を使用した場合、そのトラフィックは守秘性サービスを弱めることになるある形態の積極的攻撃を受けやすくなる可能性がある ([Bel96] を参照のこと)。データ生成元認証とコネクションレスインテグリティは連携しているサービスであり (以降、まとめて「認証」と呼ぶ)、(オプションの) 守秘性と組み合わせてオプションとして提供される。リプレイ防止サービスは、データ生成元認証が選択される場合にのみ選択され、これは完全に受信側の判断で選択される。(デフォルトでは、送信側でリプレイ防止に使用されるシーケンス番号をインクリメントすることが要求されるが、このサービスは受信側がシーケンス番号をチェックする場合のみ有効となる)。トラフィックフロー守秘性のためにはトンネルモードを選択する必要がある。これは、トラフィックを集約することによって実際の送信元と宛先を隠すことが可能な、セキュリティゲートウェイに実装するのが最も効果的である。ここで、守秘性と認証はいずれもオプションではあるが、少なくともこのうち 1 つは選択されなければならない (MUST) ことに注意すること。</p>	RFC2406	ESP	◎	中	暗号の基づいたシステムのセキュリティは、選ばれた暗号のアルゴリズムの強さ、およびそれらのアルゴリズムと共に使用されるキーの強さの両方に依存します。そのセキュリティは、さらに総合体系のセキュリティを回避する非暗号の方法がないことを保証するためにシステムによって使用されるプロトコルのエンジニアリングおよび管理に依存します。																						
<p>暗号ペイロード (Encapsulating Security Payload: ESP) [RFC-1827] は、ペイロードデータを暗号化することによって、IP データグラムに機密性を提供するものである。この仕様では US Data Encryption Standard (DES) アルゴリズムの暗号ブロック連鎖 (Cipher Block Chaining: CBC) モード [FIPS-46, FIPS-46-1, FIPS-74, FIPS-81] の変形を用いた ESP の利用法について記述している。トリプル DES (3DES) として知られるこの変形は、平文のそれぞれのブロックを 3 回に渡って処理し、それぞれの回では異なる鍵が使用される [Tuchman79]。</p>	RFC1851																										
<p>通信する組織の間で共有される秘密の 3DES 鍵は、実際には 168 ビットの長さである。この鍵には DES アルゴリズムによって使用される 3 つの独立した 56 ビットが含まれる。この 3 つのそれぞれの 56 ビットの副鍵に、パリティビットとして使用するバイト毎の最下位ビット (least significant bit) を足して、64 ビット (8 バイト) として格納される。</p>	RFC1851																										
<p>暗号ペイロード (ESP) [Kent98] は、保護すべきペイロードデータを暗号化することによって、IP データグラムに機密性を提供する。この仕様では、CBC モード暗号アルゴリズムの ESP での利用法について説明する。</p>	RFC2451																										
<p>IPsec 上で動作する SMTP コネクションは、送信者と最初のホップとなる SMTP ゲートウェイ間、あるいは、あらゆる接続された SMTP ゲートウェイ間のメッセージについて守秘性を提供することができます。すなわち、これは、SMTP コネクションのためにチャネルセキュリティを提供します。メッセージが直接、クライアントから受信者のゲートウェイに行く状況において、(受信者は、ゲートウェイを信用しなければなりません) これは、実質的なセキュリティを提供する可能性があります。リプレイ攻撃に対する防護は提供されています。なぜなら、データ自体は防護されており、パケットはリプレイできないからです。</p>	RFC3552																										
<p>AES の選考は、以下のいくつかの特性を基本として行われた。</p> <ul style="list-style-type: none"> <li>+ セキュリティ</li> <li>+ 機密扱いではないこと</li> <li>+ 一般に公開されていること</li> <li>+ 世界中で特許権使用料が無料で利用できること</li> <li>+ 最低 128 ビットのブロックサイズを扱えること</li> <li>+ 最低、128 ビット、192 ビット、256 ビットの鍵長を扱えること</li> <li>+ スマートカードを含め、様々なソフトウェアおよびハードウェアにおける計算効率とメモリ要件</li> <li>+ 実装の柔軟性、単純性、そして、容易性</li> </ul>	RFC3602																										
<p>AES は、政府指定の暗号となるだろう。AES は、最低でも次世紀までは、政府の取扱注意 (機密扱いなし) 情報を保護するのに十分であると予測される。また、それは、ビジネスや金融機関にも広く採用されると予測される。</p> <p>IETF IPsec ワーキンググループは、将来的には AES を IPsec ESP のデフォルト暗号として採用し、仕様に適合した IPsec 実装に含まれる MUST のステータスにするつもりである。</p>	RFC3602																										
<p>3.2. Authentication Header</p> <p>The implementation conformance requirements for security algorithms for AH are given below. See Section 2 for definitions of the values in the "Requirement" column. As you would suspect, all of these algorithms are authentication algorithms.</p> <table border="1"> <thead> <tr> <th>Requirement</th> <th>Algorithm (notes)</th> </tr> </thead> <tbody> <tr> <td>MUST</td> <td>HMAC-SHA1-96 [RFC2404]</td> </tr> <tr> <td>SHOULD+</td> <td>AES-XCBC-MAC-96 [RFC3566]</td> </tr> <tr> <td>MAY</td> <td>HMAC-MD5-96 [RFC2403] (1)</td> </tr> </tbody> </table>	Requirement	Algorithm (notes)	MUST	HMAC-SHA1-96 [RFC2404]	SHOULD+	AES-XCBC-MAC-96 [RFC3566]	MAY	HMAC-MD5-96 [RFC2403] (1)	RFC4305																		
Requirement	Algorithm (notes)																										
MUST	HMAC-SHA1-96 [RFC2404]																										
SHOULD+	AES-XCBC-MAC-96 [RFC3566]																										
MAY	HMAC-MD5-96 [RFC2403] (1)																										
<p>AH provides authentication for as much of the IP header as possible, as well as for next level protocol data. However, some IP header fields may change in transit and the value of these fields, when the packet arrives at the receiver, may not be predictable by the sender. The values of such fields cannot be protected by AH. Thus, the protection provided to the IP header by AH is piecemeal.</p>	RFC4302	メッセージ認証	◎	中	コネクション認証について HMAC を使うことの残念な欠点は、「その秘密は、両者によってクリアに知られていないなければならないこと」であり、鍵が長期間使われるとき、この秘密は、望まれないものとなります。																						
<p>IP 認証ヘッダ (IP Authentication Header (AH)) は、IP データグラムに対してコネクションレスインテグリティとデータ生成元認証 (これ以降は、単に「認証」と呼ぶことにする) を提供し、さらにリプレイに対する保護を提供するために使用される。後者はオプションのサービスであり、セキュリティアソシエーションが確立される際に受信側によって選択される場合がある (デフォルトでは、リプレイ防止に使用されるシーケンス番号のインクリメントを送信側に要求するが、受信側がシーケンス番号をチェックする場合のみサービスが有効となる)。AH は上位層プロトコルに加え、IP ヘッダの可能な限り多くの部分の認証を提供する。しかしながら、一部の IP ヘッダフィールドは転送中に変わることがあり、パケットが受信側に到達した時のこのフィールドの値が送信側に予測できないものとなることがある。このようなフィールドの値は AH によっては保護されない。従って AH が IP ヘッダに提供する保護は、ある程度断片的なものになる。</p>	RFC2402																										
<p>暗号ハッシュ関数を使用してメッセージ認証を行なう仕組みである HMAC について記述する。HMAC は、MD5 や SHA-1 などの反復暗号ハッシュ関数を秘密の共有鍵と組み合わせて使用する。HMAC の暗号としての強度は、使用しているハッシュ関数のプロパティに依存する。</p>	RFC2104																										
<p>HMAC [RFC2104] は、選好される shared-secret 認証テクニックです。両者が同一の秘密鍵を知っている場合、HMAC は、あらゆる任意のメッセージを認証するために使えます。これは、乱雑なチャレンジを含み、これは、「HMAC は、古いセッションのリプレイを予防するために採用できること」を意味します。</p>	RFC3631																										
<p>3.1 透明性</p> <p>証拠を収集するために使用する手法は、透過的かつ再現可能である必要があります。あなたは、利用した手法を詳細に再現することを備える必要があります、それらの手法を独立の専門家によってテストされる必要があります。</p>	RFC3227																										

<p>3.2 収集ステップ</p> <ul style="list-style-type: none"> <li>* 証拠は、どこにあるか？どのシステムがインシデントに巻き込まれているか、また、どのシステムから証拠が収集されるかをリストする。</li> <li>* 何が関連し、また管理可能でありそうかを確立する。失敗が疑われるとき、不足しているのではなく、集めすぎている。</li> <li>* 各システムについて、関連する揮発性の順序を入手する。</li> <li>* 変更するための外部経路を削除する。</li> <li>* 揮発性の順序に従い、第 5 章で検討するルールで証拠を収集する。</li> <li>* システムの時計のずれの程度を記録する。</li> </ul>	RFC3227				
<p>4.1 カストディの連鎖</p> <p>あなたは、「どのように証拠が発見されたか」、「どのように扱われたか」および「それについて起きたすべての事項」を明確に記述することができるはずだ。下記事項が、文書化される必要がある。</p> <ul style="list-style-type: none"> <li>* どこで/いつ/誰によって、証拠が発見、収集されたか。</li> <li>* どこで/いつ/誰によって、証拠が対処、検査されたか。</li> <li>* 誰が証拠のカストディとなり、その期間は、どのように、それは保存されたか。</li> <li>* いつ、証拠のカストディを変えたか、いつ、どのように転送が行われたか。(送付番号等を含む。)</li> </ul>	RFC3227	否認防止	△	中	さらに、署名利用者は、署名者を騙して、署名しようとしているメッセージとは違うメッセージに署名させるを試みる可能性があります。
<p>4.2 どこに、どのようにアーカイブするか</p> <p>可能な場合、(あまり使われていない保存メディアではなく)普通に利用されているメディアが、アーカイビングに利用される必要があります。証拠へのアクセスは、厳格に制限される必要があり、明確に文書化される必要があります。認可されていないアクセスを検知することができる必要があります。</p>	RFC3227				
<p>認可は、認証された主体が特定の資源もしくはサービスにアクセスする権限を有するか否かを判定する過程です。密接に関連していますが、「認証と認可は、別個の 2 つのメカニズムであること」を認識することが重要です。おそらく、この密接な組み合わせに起因して、認証は、しばしば誤って認可を意味すると考えられています。認証は単に主体を識別し、認可は「人々が特定の行為をできる」か否かを定義します。</p>	RFC3552				
<p>認可は、認証に依拠することが必要不可欠ですが、認証単独では認可を意味しません。むしろ、行為をするための認可をする前に、認可メカニズムは、その行為が許可されているか否かを判定するように作られねばなりません。</p>	RFC3552				
<p>守秘性 (Confidentiality) : 情報にアクセスすることが認可されていない者が、たとえ、その情報の器(例: コンピュータのファイルやネットワークパケット)を見る可能性があっても、その情報を読めないようにする情報の防護。</p>	RFC1704	認証と認可	△	中	ユーザ名とパスワードのような単純な認証メカニズムを使うとき、認証と認可の区別は、直感的に理解できませんが(すなわち、誰もがシステム管理者アカウントとユーザアカウントの相違を理解していますが)、より複雑な認証メカニズムについては、しばしば、その区別が無くなっています。
<p>データインテグリティ (data integrity) サービス: 認可されていないデータの変更に対して防護するセキュリティサービス。意図的な変更(破壊を含む)とアクシデントによる変更(喪失を含む)の両方を含む。データへの変更が検知可能であることを確認することによる。</p>	RFC3365				
<p>ポリシー コントロール レベルは、2つの別個の機能である認証と認可から成ります。認証は、主張されたユーザの身元を検証する機能です。認証機能は、組織体中の 1 ユーザが他の組織体に認証されるように、インターネットをまたいで配布される必要があります。一旦、ユーザが認証されたら、次は、「そのユーザがそのローカル資源に対してアクセスすることが認可されているか」を判定する認可サービスの仕事です。認可が通った場合、ファイアウォール中のフィルタは、アクセスを許可するように更新することができます。</p>	RFC1636				
<p>BCP 38, RFC 2827 は、偽装されたアドレスでネットワークにアクセスするトラフィックを拒否することによって、分散型サービス妨害攻撃の影響を制限し、「トラフィックについて、その正しい発信元ネットワークを追跡可能であることを確保し易くすることを意図しています。インターネットをこのような攻撃から防護することの副次的効果として、この解決策を実装しているネットワークは、また、この攻撃や、ネットワーク機器に対する偽装されたマネジメントアクセスのような他の攻撃からも自身を護ります。これが問題を生む可能性があると場合があります。(例: マルチホーミングによる場合)本書は、現在のインGRESSフィルタリングの運用的メカニズムを記述し、インGRESSフィルタリングに関する一般的な論点を吟味し、特に、マルチホーミングの影響について探求します。このメモは、RFC 2827 を更新します。</p>	RFC3704				
<p>RFC 2827 は、「ISP が、顧客ネットワークによって正規に使われていない発信元アドレスから彼らのネットワークに流入してくるトラフィックを棄却することによって、その顧客のトラフィックを警備すること」を推奨します。そのフィルタリングは、その発信元アドレスが、いわゆる「Martian アドレス (0.0.0.0/8, 10.0.0.0/8, 127.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 224.0.0.0/4, 240.0.0.0/4 中のあらゆるアドレスを含む予約されたアドレス [3])」であるトラフィックを含みますが、これに限られません。</p>	RFC3704	インGRESS フィルタリ ング	△	中	ブラインド攻撃において、攻撃者は偽装されたIPアドレスを使うことができ、被害者が攻撃者のパケットをフィルタリングすることを極めて困難にしています。
<p>本書において検討されるフィルタリング手法では、正当なプリフィックス (IP アドレス) からのフラッディング (洪水) 攻撃に対しては全く何もませんが、起点となったネットワークの中にある攻撃者が、境界におけるフィルタリングルールに合わない偽ったソースアドレスを使用して、この種の攻撃を仕掛けることを防ぎます。攻撃者が、正規に通知されているプリフィックス (IP アドレス) の範囲内には、偽った発信元アドレスを使用することをばむために、すべてのインターネット接続プロバイダーには、この文書に記述されたフィルタリングを実装することが強く勧められます。いいかえれば、ISP が、複数のダウンストリームネットワークの経路情報を持っていて、これらの経路情報以外から来たトラフィックを防ぐために、厳格なトラフィックフィルタリングが使用される必要があります。</p>	RFC2827				
<p>この種のフィルタリングを実装することの利点には、他に、「発信者の本当の発信元を容易に追跡することができるようになること」があります。それは、攻撃者は、正規の、実在する到達可能な発信元アドレスを使用する必要があるからです。</p>	RFC2827				
<p>チェックサムは、たとえその侵入者が物理的なネットワークへの直接のアクセスができて、にせのバケットを受け取ることを防ぎます。シーケンス番号や、他のユニークな(一意の)識別子と併用することで、チェックサムは、「リプレイ (真似) 攻撃という、古い(当時は適切だった)ルーティング情報が侵入者、もしくは誤動作させられるルーターによって返送される攻撃も防ぐことができます。概ね完全なセキュリティは、シーケンス(通番)ないし固有な識別子とルーティング情報の完全な暗号化によって可能です。これは侵入者がネットワークのトポロジー(構成)を推定するのを防ぎます。暗号化の欠点は、情報を処理するのにかかるオーバーヘッド(負荷)です。</p>	RFC2198	トポロジーの 破壊	-	中	攻撃がデータを受け取ることができることに依拠する場合、パス外のホストは、まず、自身をパス上におくために、トポロジーを壊さなければなりません。これは決して不可能ではありませんが、よくあるとも限りません。
<p>このための標準的テクニックは、IP TTL の値 [IP] を検証することです。TTL は、各転送者によって、減算されなければならないので、プロトコルは、「TTL が 255 にセットすること」と、「すべての受信者が TTL を検証すること」を命令できます。次に、受信者は、「確認しているパケットは、同一のリンク上からのものである」と信じる根拠をもちます。トンネリングシステムがある状態でこのテクニックを使用するときは注意が必要です。そのようなシステムでは、TTLを減算せずにパケットを通過させる可能性があるからです。</p>	RFC3552	同一リンクの 判別	-	中	トンネリングシステムがある状態でこのテクニックを使用するときは注意が必要です。そのようなシステムでは、TTLを減算せずにパケットを通過させる可能性があるからです。

<p>&lt;以前に記述されていた内容を以下にまとめる&gt;</p>	
<p>それゆえ、あるマシンにコネクションを開くとき、あなたは非常に強い確信をもってどんなシーケンス番号が、その次のコネクションに使用されるかを知ることができます。そして、そこが 攻撃されるのです。</p>	RFC1948
<p>良いシーケンス番号は、暗号技術による認証の代わりになるものではありません。いいところ、それらは一時しのぎの手段です。</p>	RFC1948
<p>各コネクション(つまり、各 4 つの要素 &lt;localhost, localport, remotehost, remoteport&gt; から成る集合)に独立したシーケンス番号空間を与えること</p>	RFC1948
<p>それでもなお、偽のコネクションと実際のコネクションの間隔は、程度の差こそあれ、在ることにはかわりがないので、攻撃者がそのようなパケットをキャプチャできないようにすることが重要です。それらを見せしめる典型的な攻撃には、盗聴と [8] で検討した様々なルーティング攻撃の両方があります。</p>	RFC1948
<p>パスワード、暗号技術的な鍵、および同様なセキュリティ用途に使う推測困難な乱数の生成する</p>	RFC1750
<p>コネクションのための最初のシーケンス番号の選択はランダムではありません。むしろ、古い状態のパケットが新しい同一のコネクションの実現 [6, Appendix A] において受け入れられる可能性を最小限にするように選択される必要があります。</p>	RFC2196
<p>6.2. 暗号技術的に強いシーケンス English 一連の乱数が生成されなければならない場合、攻撃者は、そのシーケンス中の何らかの値を学習する可能性があります。一般に、攻撃者が、知っている値から他の値を予測できるようではいけません。</p>	RFC4086
<p>いくつかの公的標準と、広く配備された例が、現在、鍵もしくは他の暗号技術的に乱雑な数の生成のために存在します。</p>	RFC4086
<p>インGRESSフィルタリングを使用して偽ったトラフィックを制限する</p>	RFC2827
<p>コネクションのための最初のシーケンス番号の選択はランダムではありません。むしろ、古い状態のパケットが新しい同一のコネクションの実現において受け入れられる可能性を最小限にするように選択される必要があります。</p>	RFC2196