脅威と対策表3

BCP	RFC		中項目	脅威		攻撃	定義	要件	回避策	リスク	事例・影響	必要度
72	3552	インターネットの脅威モデル	待ち伏せ攻撃	-		-	待ち伏せ攻撃において、攻撃者は、ネットワークからパケットを読みますが、書き込みません。					
72	3552	インターネットの脅威モデル	待ち伏せ攻撃	データを回線から盗聴		データを回線から盗聴	待ち伏せ攻撃の古典的な例は、もともとプライベートなデータを回線から盗聴することです。	このような攻撃をしかける最も単純なやり方は、被害者と同じLAN上にいることです。(イーサーネット、803およびFDDIを含む)最も卑近なLANの設定において、回線上のいかなるマシンでも、同一のLAN上のいかなる他のマシン宛のすべてのトラフィックを読むことができます。	「スイッチングハブでは、特定のマシン宛てのトラフィックは、そのマシンが存在するセグメントだけに送られるので、この種の盗聴を実質的により困難にすること」を覚えておいてください。	同様に、2人の被害者のマシン間の通信パスにおいて、ホストをコントロールできる攻撃者は、彼らの通信に待ち伏せ攻撃をしかけることができます。	パスワード盗聴攻撃は、任意のパケットを読むことができる攻撃者によってしかけられる可能性があります。これは、一般に、待ち伏せ攻撃[INTAUTH]と呼ばれます。	
72	3552	インターネットの脅威モデル	待ち伏せ攻撃	データを回線から盗聴		データを回線から盗聴			例えば、SSLは広範に利用可能であるにもかかわらず、多くのクレジットカード取引は、いまだに平文でインターネット上を転送されています。	そのトラフィックが侵されたマシンを通るようにルーティングインフラストラクチャを侵すことも可能です。これは、被害者のマシン上で待ち伏せ攻撃を行うように、ルーティングインフラストラクチャに対する積極的な攻撃を含む可能性があります。	一般に、攻撃の目標は、「送信者と受信者がプライベートに保ちたい情報を入手すること」です。このプライベート情報は、電子的な世界で有用なクレデンシャル、かつ／または、ビジネスの機密情報のような電子的な世界の外界で有用なパスワードやクレデンシャルを含む可能性があります。	
72	3552	インターネットの脅威モデル	待ち伏せ攻撃	データを回線から盗聴		データを回線から盗聴				無線通信チャネルには、特別に考慮に値する事項があり、特に最近人気が高まっている8011を使うような無線に基づくLANについて考慮する価値があります。データは、単に、よく知られた周波数でブロードキャストされるので、攻撃者は、その転送内容を単に受け取ることができる必要があるだけです。このようなチャネルは、待ち伏せ攻撃に対して特に脆弱です。多くのこのようなチャネルが暗号技術的防護を備えていますが、品質が低く、ほとんど使用に耐えないことがよくあります[WEP]。	ビジネスの機密情報は、日常的に平文の電子メールで、ネットワーク上を送られています。	
72	3552	インターネットの脅威モデル	待ち伏せ攻撃	パスワード盗聴		OSの小さなセキュリティホールを攻略	これまで、パスワードファイルを復元するために積極的な攻撃によってOSの小さなセキュリティホールを攻略することも可能でした。	それゆえ、我々は、低レベルの積極的な攻撃をオフラインの待ち伏せ攻撃と組み合わせます。		これらのセキュリティホールは、前述のオフラインのパスワード復元テクニックを使うことによって、実際のアカウントにすることに成功する可能性があります。		
		インターネットの脅威モデル	待ち伏せ攻撃	パスワード盗聴		オフラインでの暗号技術的攻撃	多くの暗号技術的プロトコルは、「オフライン攻撃」の対象となります。	このようなプロトコルにおいて、攻撃者は、被害者の秘密鍵を使って処理されたデータを復元し、それから、その鍵について暗号技術的攻撃をしかけます。				
72	3552	インターネットの脅威モデル	待ち伏せ攻撃	パスワード盗聴		暗号解読ツール	Unixパスワードは、一方向性関数を使って暗号化されますが、このような暗号化されたパスワード[KLEIN]を解読するツールが存在します。			NISが使われるとき、暗号化されたパスワードは、ローカルネットワーク上を転送され、それゆえ、攻撃者はパスワードを盗聴し攻撃することができます。		
72	3552	インターネットの脅威モデル	待ち伏せ攻撃	パスワード盗聴		辞書攻撃	パスワードは、特に脆弱な標的を作ります。なぜなら、それらは、典型的には低エントロピーであるからです。	パスワードに基づく、数多くの有名なチャレンジアンドレスポンスプロトコルは、「辞書攻撃」に対して脆弱です。攻撃者は、チャレンジレスポンスを捕捉し、(辞書ファイルのような)よくある単語リストから正しい応答をもたらすパスワードを発見するまで、各項目を試す処理を行います。		NISが使われているとき、同様の攻撃は、ローカルネットワーク上でしかけられる可能性があります。		
72	3552	インターネットの脅威モデル	待ち伏せ攻撃	パスワード盗聴		パスワード盗聴	パスワード盗聴は、資源を無権限に利用するために行われます。多くのプロトコル([TELNET],[POP],[NNTP]等)は、クライアントをサーバーに認証させるために、共有パスワードを使います。このパスワードは、クライアントからサーバーに、通信チャネル上を平文で転送されます。	「攻撃のログイン段階は、積極的であるが、実際のパスワード捕捉フェイズは、待ち伏せによること」を銘記してください。さらに、サーバーがコネクションの起点アドレスをチェックしない限り、ログイン段階では、いかなる特別なネットワークのコントロールを要求しません。		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。		
72	3552	インターネットの脅威モデル	積極的な攻撃	-		-	攻撃がネットワークへの書き込みを含むとき、我々は、これを積極的な攻撃と呼びます。					

72	3552	インターネットの脅威モデル	積極的な攻撃	リプレイ攻撃		リプレイ攻撃	リプレイ攻撃において、攻撃者はメッセージの順序を回線外に記録し、それらを当初受け取った主体に再送します。			「攻撃者はメッセージを理解できる必要がないこと」を銘記してください。単に、それらを補足して再送するだけでよいのです。	例えば、クレジットカードによる購入や株取引のように、何らかのサービスを要求するためにS/MIMEメッセージが使われる事例を検討します。攻撃者が、被害者の邪魔をするだけの場合、サービスを2回実行することを望む可能性があります。攻撃者はメッセージを補足し、たとえそれを理解できなくても再送することにより、結果的にトランザクションを2回実行させることが可能です。	
72	3552	インターネットの脅威モデル	積極的な攻撃	メッセージ挿入		メッセージ挿入	メッセージ挿入攻撃において、攻撃者は、いくつかの選択された属性についてメッセージを偽装し、ネットワーク中に挿入します。しばしば、このメッセージは、攻撃者の身元を偽装するために偽装された発信元アドレスをもちます。					
72	3552	インターネットの脅威モデル	積極的な攻撃	メッセージ削除		Morrisのシーケンス番号推測攻撃	このブラインド攻撃において、アドレスが偽装されているホストは、攻撃されているホストから偽装されたTCPSYNパケットを受け取ります。このSYNパケットの受信は、RSTを生成します。これは、不正なコネクションを切断します。(攻撃が成功するように)RSTを送らないようにするためにMorrisは、SYNパケットが失われて応答されないように、ホストのキューのバッファを溢れさせることを記述しています。			逆に、Morrisのシーケンス番号推測攻撃[SEQNUM]は、任意のパケットを読むことはできないが書ける攻撃者によって、しかけられる可能性があります。攻撃者にネットワークに書き込むことを要求する攻撃は、積極的な攻撃として知られています。		
72	3552	インターネットの脅威モデル	積極的な攻撃	メッセージ削除		Morrisのシーケンス番号推測攻撃				Morrisのシーケンス番号推測攻撃[SEQNUM]は、しばしば、メッセージ削除攻撃に、成功することを要求します。		
72	3552	インターネットの脅威モデル	積極的な攻撃	メッセージ削除		メッセージ削除	メッセージ削除攻撃において、攻撃者は、回線上からメッセージを削除します。					
72	3552	インターネットの脅威モデル	積極的な攻撃	メッセージ変更		カットアンドペースト攻撃	「この特定の攻撃は、攻撃者がクレジットカード番号をメッセージの原本からカットして、新しいメッセージにペーストするので、カットアンドペースト攻撃として知られていること」を覚えておいてください。	IPsecESPが、いかなるMAC無しに使われている場合、攻撃者が同一マシン上の被害者宛の暗号化されたトラフィックを読むことは可能です。攻撃者は、コントロールしているポートに対応するIPヘッダを、暗号化されたIPパケットに添付します。パケットがホストによって受信されるとき、これは自動的に復号され、攻撃者のポートに転送されます。	両攻撃は、暗号化する際に常にメッセージ認証を使うことによって避けることができます。この攻撃は、以下の場合にのみ可能であることを銘記してください。	この攻撃は、以下の場合にのみ可能であることを銘記してください。 (1)MACチェックが使われていない場合(理由:この攻撃は壊れたパケットを生成する) (2)「ホストtoホスト」SAが使われている場合(理由:「ユーザtoユーザ」SAは、SAと関連づけられたポートと標的ポートの間の不整合をもたらす。)受信するマシンが単一ユーザ用である場合、この攻撃は実現不可能です。		
72	3552	インターネットの脅威モデル	積極的な攻撃	メッセージ変更		セッションハイジャック攻撃		IPsecESPが、いかなるMAC無しに使われている場合、攻撃者が同一マシン上の被害者宛の暗号化されたトラフィックを読むことは可能です。攻撃者は、コントロールしているポートに対応するIPヘッダを、暗号化されたIPパケットに添付します。パケットがホストによって受信されるとき、これは自動的に復号され、攻撃者のポートに転送されます。同様のテクニックが、セッションハイジャック攻撃をしかけるのに使われます。	両攻撃は、暗号化する際に常にメッセージ認証を使うことによって避けることができます。	この攻撃は、以下の場合にのみ可能であることを銘記してください。 (1)MACチェックが使われていない場合(理由:この攻撃は壊れたパケットを生成する) (2)「ホストtoホスト」SAが使われている場合(理由:「ユーザtoユーザ」SAは、SAと関連づけられたポートと標的ポートの間の不整合をもたらす。)受信するマシンが単一ユーザ用である場合、この攻撃は実現不可能です。		
72	3552	インターネットの脅威モデル	積極的な攻撃	メッセージ変更		メッセージ変更	メッセージ変更攻撃において、攻撃者は、回線からメッセージを削除し、それを変更し、ネットワーク中に再投入します。攻撃者がメッセージ中にデータを送ることを望むが、同時に、その一部を変更することを望む場合、この種の攻撃は特に有効です。				攻撃者がインターネット越しの物品の購入を攻撃することを望む事例を考えます。攻撃者は、被害者のクレジットカード番号をもっていないので、被害者が発注するのを待ち、配送先を自身のものに(また、おそらく物品の記述を)書き換えます。	

72	3552	インターネットの脅威モデル	積極的な攻撃	ブラインド攻撃		ブラインド攻撃	パケットを偽装する能力は、任意のパケットを受け取る能力とは関連していません。事実、偽装されたパケットを送ることができてもレスポンスを受け取らない積極的な攻撃があります。			「すべての積極的な攻撃がアドレス偽装を要求するわけではないこと」を銘記してください。しかし、攻撃が発見された場合、「身元を隠すために他人のアドレスにを偽装すること」は、よくあることです。	各プロトコルは、特定の積極的な攻撃に影響されやすいですが、経験では、「数多くの攻撃の共通パターンがあらゆるプロトコルに当てはまること」を示しています。次節では、数多くのこのようなパターンを記述しており、既知のプロトコルに応用されたそれらの具体的な例を提供しています。	
72	3552	インターネットの脅威モデル	積極的な攻撃	中間者による攻撃		ARP詐称	攻撃者は、ARPを被害者のIPアドレスと自身のMACアドレスで詐称します。	「中間者による攻撃をARP詐称によってローカルネットワーク上でしかけること」もよくあることです。		「中間者による攻撃をARP詐称によってローカルネットワーク上でしかけること」もよくあることです。		
72	3552	インターネットの脅威モデル	積極的な攻撃	中間者による攻撃		セッションハイジャック攻撃		攻撃者がTCPハンドシェイクにおけるクライアントTCPコネクションをハイジャックできる場合、（おそらく、サーバーが応答する前にクライアントのSYNに応答することによって）攻撃者は、サーバーへのコネクションを開いて、中間者による攻撃を始めることができます。		この種の攻撃をしかけるためのツールが入手可能です。		
72	3552	インターネットの脅威モデル	積極的な攻撃	中間者による攻撃		セッションハイジャック攻撃	中間者による攻撃は、上記テクニックを特別な形態で組み合わせます。:攻撃者は、「送信者から受信者宛」と「受信者から送信者宛」のふりをするために通信ストリームを破壊します。: AliceとBobが考えていること: Alice<----------Bob 起きていること: Alice<----------＞攻撃者<----------Bob	これは、上記の形態の攻撃とは根本的に異なります。なぜなら、これは、データストリーム自体ではなく、通信主体の身元を攻撃するからです。したがって、通信ストリームのインテグリティを提供する多くのテクニックは、中間者による攻撃に対して防護するのに不十分です。	「中間者による攻撃を予防するために、トランザクションの一方を認証することのみが必要不可欠であること」を銘記してください。このような状況において、両者は、一方のみが認証されている協定を確立することができます。このようなシステムにおいて、攻撃者は、認証されていない相手のふりをして、協定を開始できますが、正規のコネクション上を送られたデータを転送したり、それにアクセスできません。これは、Web電子商取引においては、許容可能な状況です。ここでは、サーバーのみが認証される必要があります。（あるいは、クライアントは、クレジットカード番号のような何らかの非暗号技術的メカニズムによって別個に認証されます。）	中間者による攻撃は、プロトコルが「エンティティ間認証」を欠いているとき、常に可能です。		
72	3552	インターネットの脅威モデル	積極的な攻撃	詐称（スプーフィング）攻撃		詐称（スプーフィング）攻撃	IPがIPsec無しで使われるとき、送信者のアドレスについての認証機能はありません。その結果、攻撃者が任意の発信元アドレスをもったパケットを作ることは、自然なことです。	特定の状況下において、このようなパケットは、ネットワークによってフィルタリングされる可能性があります。例えば、多くのパケットフィルタリングファイアウォールは、「外部」インターフェイスに到着する「内部」ネットワークの発信元アドレスをもったすべてのパケットをフィルタリングしています。しかし、「これはファイアウォール内部の攻撃者に対する防護を提供しないこと」を銘記してください。		一般に、設計者は、「攻撃者はパケットを偽装できる」と想定する必要があります。		
72	3552	インターネットの脅威モデル	トポロジーに関する論点	「パス上」対「パス外」		-	データグラムが、ホスト間を転送されるようにするためには、一般に、何ヵ所か中間リンクやゲートウェイを通過しなければなりません。このようなゲートウェイは、通常、パス上を転送されるいかなるデータグラムをも読むこと、変更すること、および削除することができます。あなたがパス上にいる場合、これにより多様な攻撃をしかけることが、はるかに容易になります。	アプリケーションプロトコル設計者は、「すべての攻撃者はパス外にいる」と想定してはなりません。		当然ながら、パス外のホストは、いかなるホストからでも来たように見える任意のデータグラムを転送できますが、他のホストを意図したデータグラムを受け取ることができるとは限りません。それゆえ、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。		MUST NOT
72	3552	インターネットの脅威モデル	トポロジーに関する論点	「パス上」対「パス外」		-		可能であれば、プロトコルは、ネットワークを完全にコントロールできる攻撃者からの攻撃に耐えるように設計される必要があります。				SHOULD
72	3552	インターネットの脅威モデル	トポロジーに関する論点	「パス上」対「パス外」		-		しかし、設計者には、パス上の攻撃者のみならず、パス外の攻撃者によってしかけられる攻撃をより重視することが期待されます。				

72	3552	インターネットの脅威モデル	トポロジーに関する論点	リンクとローカル		-	パス上の特殊ケースは、同一リンク上にいることです。		状況によっては、ローカルネットワーク上のホストと、そうでないホストを区別することが望まれます。このための標準的テクニックは、IPTTL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。		
72	3552	インターネットの脅威モデル	共通論点			-	各システムのセキュリティ要件は固有ですが、一定の共通要件が数多くのプロトコルにあります。単純なプロトコル設計者がこれらの要件に直面したとき、しばしば、彼らは、たとえより良いソリューションが利用可能でも、明らかではあるがセキュアでないソリューションを選択します。この章は、多くのプロトコルにある数多くの論点や、それらに対応する際に有用である可能性があるセキュリティ技術の共通部分を記述します。					
72	3552	インターネットの脅威モデル	ユーザ認証	チャレンジレスポンスとワンタイムパスワード	チャレンジレスポンス	-	チャレンジレスポンスのスキームにおいて、ホストとユーザは、何らかの秘密を共有します。(これは、しばしば、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く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。	両種のスキームは、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。	「チャレンジレスポンス」タイプのシステムは、ユーザが生成したパスワードの代わりに乱雑に生成された共有鍵を使うことによって、辞書攻撃に対してセキュアにできます。鍵が十分に大きい場合、鍵検索攻撃は非現実的になります。	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。	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。	
72	3552	インターネットの脅威モデル	ユーザ認証	チャレンジレスポンスとワンタイムパスワード	チャレンジレスポンス	-	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。	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。)		
72	3552	インターネットの脅威モデル	ユーザ認証	チャレンジレスポンスとワンタイムパスワード	チャレンジレスポンス	-		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。				
72	3552	インターネットの脅威モデル	ユーザ認証	チャレンジレスポンスとワンタイムパスワード	ワンタイムパスワード	-	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。	両種のスキームは、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。		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。	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。	
72	3552	インターネットの脅威モデル	ユーザ認証	チャレンジレスポンスとワンタイムパスワード	ワンタイムパスワード	-	SecureIDやDESGoldは、このスキームの流派です。	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。		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。		
72	3552	インターネットの脅威モデル	ユーザ認証	チャレンジレスポンスとワンタイムパスワード	ワンタイムパスワード	-		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。		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。)		

72	3552	インターネットの脅威モデル	ユーザ認証	ホスト認証		–	ホスト認証は、特別な問題をもたらします。ごく普通に、サービスのアドレスは、例えばURL[URL]のように、DNSホスト名を使って表現されます。このようなサービスをリクエストするとき、「相手が証明書をもっている者であることのみならず、その証明書が期待されるサーバーの身元に対応することも」確認する必要があります。重要なことは、「証明書と期待されるホスト名をセキュアに結合すること」です。		セキュリティ機能をプロトコル中に提供することは、困難である可能性があります。認証と鍵確立のメカニズムを選択する問題以外に、それらをプロトコルに統合する必要があります。(IPsecとTLSに組み込まれた)この問題に対する対応のひとつは、下位層のセキュリティプロトコルを作り、「新しいプロトコルは、そのプロトコルの上で動作するようにする」と主張することです。最近、普及したこれ以外のアプローチは、「一般的なアプリケーション層のセキュリティフレームワークを設計すること」です。このアイディアは、「あなたがプラグ可能な形態で、様々なセキュリティメカニズムを交渉することを認めるプロトコルを設計すること」です。次に、アプリケーションプロトコル設計者は、セキュリティプロトコルPDUを、そのアプリケーションプロトコルで運ぶようにします。このようなフレームワークの例には、GSS-API[GSS]やSASL[SASL]が含まれます。	例えば、通常、リクエストが一定のホスト名に対するものである場合、証明書が身元をIPアドレスの形態でを含むことは許容できません。これは、「エンドtoエンド」セキュリティを提供しません。なぜなら、ホスト名とIPの対応付けは、セキュアな名前解決[DNSSEC]が使われない限りセキュアでないからです。これは、ホスト名がアプリケーション層に現れながら、認証が何らかの下位層において行われるとき、特別な問題です。		
72	3552	インターネットの脅威モデル	ユーザ認証	まだ普及していないシステム		–	数多くのプロトコル([EKE],[SPEKE],[SRP])が、セキュアにユーザのパスワードを共有鍵に入れるようにすることができ、これは、暗号技術的プロトコルへの入力として使うことができます。	上記のスキームより良いやり方ありますが、それらは、典型的には、通信セキュリティ(最低限、メッセージインテグリティ)がコネクションをセキュアにするために採用されない限り、あまりセキュリティを高めません。	同様に、そのユーザは、公開鍵証明書を使って認証することができます(例:S-HTTPクライアント認証)。これらの手法は、典型的には、より完成されたセキュリティプロトコルの一部として使われています。	通信セキュリティ(最低限、メッセージインテグリティ)がコネクションをセキュアにするために採用されない限り、あまりセキュリティを高めません。なぜなら、そうしないと、攻撃者は、まれに、認証が行われた後にコネクションをハイジャックできるからです。		
72	3552	インターネットの脅威モデル	ユーザ認証	まだ普及していないシステム		–				これらのプロトコルの採用についての障害のひとつは、「それらの知的財産権の状態が全く不明確であること」でした。		
72	3552	インターネットの脅威モデル	ユーザ認証	ユーザ名/パスワード		–	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。		
72	3552	インターネットの脅威モデル	ユーザ認証	共有鍵	鍵配布センター	–	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て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。				
72	3552	インターネットの脅威モデル	ユーザ認証	共有鍵		辞書攻撃	「チャレンジレスポンス」タイプのシステムは、ユーザが生成したパスワードの代わりに乱雑に生成された共有鍵を使うことによって、辞書攻撃に対してセキュアにできます。	このアプローチは、ユーザによって記憶されたり打鍵されるときよりも、鍵が終端に設定されるときに最もうまくいきます。なぜなら、ユーザには、十分に長い鍵を覚えるのに問題があるからです。	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)	パスワードに基づくシステムのように、共有鍵システムは、管理問題をわずらいます。通信主体の各ペアは、自らが合意した鍵をもたなければなりません。これは、そこにたくさんの鍵がある状況をもたらします。		
72	3552	インターネットの脅威モデル	ユーザ認証	証明書		–	証明書は、エンティティの身元をその公開鍵に結合する署名されたクレデンシャルです。証明書の署名者は認証局(CA)であり、この証明書自体は、何らかの上位CAによって署名される可能性があります。	単純なアプローチは、[TLS]もしくは[S/MIME]のように、すべてのユーザが何らかのプロトコル固有のやり方で認証するのに使う証明書[PKIX]をもつようにすることです。		このシステムが働くようにするために、ひとつ、もしくは複数のCAにおける信頼は、オフラインで確立されなければなりません。このようなCAは、「トラステッドルート」もしくは「ルートCA」と呼ばれます。クライアント/サーバーシステムにおけるこのアプローチに対する主要な障害は、「クライアントが証明書をもっていることを要求すること」であり、これは採用の問題である可能性があります。		

72	3552	インターネットの脅威モデル	ユーザ認証			-		要するに、資源に対するアクセスコントロールを行うすべてのシステムは、ユーザを認証する何らかのやり方を必要とします。ほとんど無数の、このようなメカニズムが、この目的のために設計されてきました。				
72	3552	インターネットの脅威モデル	否認防止			-	署名する主体がメッセージを否認するための最も容易なやり方は、「プライベート鍵が侵されてしまい、どこかの攻撃者が(署名利用者であるとは限りませんが)異議を唱えられているメッセージに署名してしまった」と主張することによります。	この攻撃に対して防護するために、署名利用者は、「署名者の鍵が署名時点において侵されていないこと」を実証する必要があります。これは、証明書失効情報がアーカイブ化されたストレージ、および、メッセージが署名された時刻を確立するためのタイムスタンプサーバーを含む実質的なインフラストラクチャを要求します。	否認防止のための単純なアプローチは、単にコンテンツ上で公開鍵デジタル署名を使うことです。発信者(署名者)であることを望む主体は、当該メッセージにデジタル的に署名します。相手(署名利用者)は、後で、「一定時点において署名者が異議を唱えられているメッセージに合意していたこと」の証明としてデジタル署名を指すことができます。残念ながら、このアプローチでは不十分です。	これらすべての複雑性は、否認防止を実際に配備するのが困難なサービスにします。		
72	3552	インターネットの脅威モデル	否認防止			-				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ことを試みる可能性があります。	多くの状況において、署名する主体の鍵は、スマートカードに保存されますが、署名されるメッセージは、署名利用者によって示されます。	
72	3552	インターネットの脅威モデル	否認防止			-				この問題は、キヨスクのような状況で、特に署名利用者が署名者が署名に使うインフラストラクチャをコントロールするとき、厳しくなります。		
72	3552	インターネットの脅威モデル	認可vs.認証	アクセスコントロールリスト		-	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。	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。	認可メカニズムのよくある形態のひとつは、ACL(アクセスコントロールリスト)です。これは、資源にアクセスすることを認可されたユーザをリストするものです。各資源に対する個々の認可を指定することは、面倒であるので、資源は、しばしば、親資源のACLが子資源に継承されるように階層的に配置されます。これは、システム管理者に最高位のポリシーを設定し、必要不可欠なときにそれらを優先することを許容します。			
72	3552	インターネットの脅威モデル	認可vs.認証	証明書に基づくシステム		-	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すが(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。		これらのより複雑な属性を強制するためのメカニズムは、まだ完成していません。ひとつのアプローチは、単に、どの種類の証明書が浸透できるかを記述しているポリシーをACLに添付することです。			
72	3552	インターネットの脅威モデル	認可vs.認証	証明書に基づくシステム		-	例えば、証明書について、有効な署名を示すことは、認可を意味しません。署名は、信用できるルートを含む証明書チェインを辿らなければならず、そのルートは、一定の条件の下で信用されなければなりません。例えば、AcmeMISCAとAcmeAccountingCAの両方がAcmeWebサーバーによって「信用」されていても、AcmeMISCAによって発行された証明書を保持するユーザは、AcmeAccountingCAによって発行された証明書を保持するユーザとは異なるWebアクセス権限をもつ可能性があります。					
72	3552	インターネットの脅威モデル	認可vs.認証	証明書に基づくシステム		-			これ以外のアプローチは、証明書拡張[PKIX,SPKI]としてか、独立した「属性証明書」としてのいずれかによって、その情報を証明書とともに運ぶことです。			

72	3552	インターネットの脅威モデル	トラフィックセキュリティを提供する	IPsec		-		2つのホスト間のトラフィックのためのIPsecプロトコル（具体的にはAHとESP）は、トランスポートセキュリティを提供できます。IPsecプロトコルは、様々な粒度のユーザ認証をサポートします。例えば、「IPサブネット」、「IPアドレス」、「FQDN（FullyQualifiedDomainName）」、個々のユーザ（"Mailboxname"）が含まれます。これらの様々なレベルの識別は、IPsecの本質的な部分であるアクセスコントロール機能に対する入力として採用されています。		IPsec実装によっては、すべての身元タイプはサポートしていない可能性があります。特に、セキュリティゲートウェイは、「ユーザtoユーザ」認証を提供しない可能性、または、アプリケーションに認証情報を提供するメカニズムをもつ可能性があります。		
72	3552	インターネットの脅威モデル	トラフィックセキュリティを提供する	IPsec		-		AHもしくはESPが使われているとき、アプリケーションプログラマは、（AHもしくはESPがシステム全体で利用可能とされている場合）何もしなくてよい可能性があり、あるいは、特定のソフトウェアの変更を行う必要がある可能性があります。		（例：特定のsetsockopt()コールを追加する。）（使われているAHもしくはESPの実装に依存します。）残念ながら、IPsec実装をコントロールするためのAPIは、まだ標準化されていません。		
72	3552	インターネットの脅威モデル	トラフィックセキュリティを提供する	IPsec		-			IPsecが確実に利用可能な環境において、これは、アプリケーション通信トラフィックを防護するための可変的オプションを提供します。保護されるべきトラフィックがUDPである場合、IPsecやアプリケーション固有のオブジェクトセキュリティは、唯一の選択肢です。	他のプロトコルをセキュアにするためにIPsecを使うことについての主な障害は、採用です。	現在、IPsecの主要な用途は、VPNアプリケーション用であり、特にリモートネットワークアクセス用です。セキュリティ管理者とアプリケーション開発者の間の極めて密接な調整無しには、VPNの利用は、個々のアプリケーションにセキュリティサービスを提供するのに適していません。なぜなら、このようなアプリケーションには、「どのセキュリティサービスが実際に提供されていたか」を判定することが困難であるからです。	
72	3552	インターネットの脅威モデル	トラフィックセキュリティを提供する			-		セキュアな設計を施されたプロトコルは、取り扱いに注意を要するすべてのトラフィックをセキュアにする何らかのメカニズムを適用しなければなりません。（インテグリティ確保、認証および暗号化を意味します。）ひとつのアプローチは、[DNSSEC],[S/MIME],[S-HTTP]のように、プロトコル自体をセキュアにすることです。これは、そのプロトコルに最も適合するセキュリティを提供しますが、正しく行うには相当な労力も要求します。				
72	3552	インターネットの脅威モデル	トラフィックセキュリティを提供する			-		多くのプロトコルは、利用可能なチャネルセキュリティシステムのひとつを使って、適切にセキュアにすることができます。我々は、最も普及している2つ（IPsec[AH,ESP]と[TLS]）を検討します。				
72	3552	インターネットの脅威モデル	トラフィックセキュリティを提供する	IPsec		-		しかし、設計者は、「IPsecが利用可能である」と想定してはなりません。				MUST NOT
72	3552	インターネットの脅威モデル	トラフィックセキュリティを提供する	IPsec		-		IPv6の特別な事例において、AHとESPの両方を実装することが必須です。それゆえ、「IPv6専用プロトコルまたはIPv6専用実装では、AH/ESPはすでに利用可能である」と想定することは合理的です。				
72	3552	インターネットの脅威モデル	トラフィックセキュリティを提供する	IPsec		-		しかし、自動的鍵管理(IKE)は、実装することが要求されていないので、プロトコル設計者は、「これが在るであろう」と想定してはいけません。				SHOULD NOT
72	3552	インターネットの脅威モデル	トラフィックセキュリティを提供する	IPsec		-		一般的なアプリケーション層プロトコルのためのセキュリティポリシーは、「IPsecが意図された配備環境で利用可能である」と信じる何らかの根拠がない限り、「IPsecが使われなければならない」と述べるだけではいけません。				SHOULD NOT

72	3552	インターネットの脅威モデル	トラフィックセキュリティを提供する	SSL/TLS	バーチャルホスト	-	「ポート分離」アプローチがTLSに使われている場合、TLSは、いかなるアプリケーション層トラフィックが送られる前に交渉されます。			これは、[HTTP]のようなバーチャルホストを使うプロトコルについて問題を起こす可能性があります。なぜなら、サーバーは、「TLSハンドシェイクにおいて、どの証明書をクライアントに提供するか」を知らないからです。まだ広く普及するには新し過ぎますが、TLSホスト名拡張[TLSEXT]は、この問題を解決するのに使うことができます。		
72	3552	インターネットの脅威モデル	トラフィックセキュリティを提供する	SSL/TLS	リモート認証とTLS	-		「クライアントが証明書をもっている場合、SSLに基づくクライアント認証が使えること」を覚えておいてください。これを容易にするためにSASLは、「外部」メカニズムを提供し、これによって、SASLクライアントは、サーバーに「私の身元については外部チャネルを調べて下さい」と伝えることができます。明らかに、これは、上記の階層化(layering)による攻撃の対象ではありません。		残念ながら、このSASLとTLSの組み合わせは、期待するほど強くはありません。積極的な攻撃者が、このコネクションをハイジャックすることは容易です。クライアントは、SSLコネクションの中間者となります。(我々は、通常この攻撃を防ぐサーバーを認証しているのではないことを思い出してください。)次に、単純に、SASLハンドシェイクをプロキシします。以降、少なくとも攻撃者に関しては、コネクションが平文であるかのようになります。この攻撃を予防するために、クライアントは、サーバーの証明書を検証する必要があります。	しかし、サーバーが認証された場合、チャレンジレスポンスは、さほど望まれなくなります。あなたが既に強化されたチャネルをもっている場合、単純なパスワードが良いといえます。事実、それらは、チャレンジレスポンスより優れていることを論証できます。なぜなら、それらは、「パスワードがサーバー上において平文で蓄積されること」を要求しないからです。それゆえ、チャレンジレスポンスシステムを伴う鍵が侵されることは、単純なパスワードが使われた場合よりも深刻です。	
72	3552	インターネットの脅威モデル	トラフィックセキュリティを提供する	SSL/TLS	リモート認証とTLS	-				TLSの利用における困難のひとつは、「サーバーは証明書で認証されること」です。これは、従前、唯一の認証の形態がクライアントとサーバー間で共有されたパスワードであった環境において不便です。認証されたサーバー無しにTLSを使うことを試みて(すなわち、アノニマスDHもしくは、自己署名されたRSA証明書を使って)、次に(SASLwithCRAM-MD5のような)何らかのチャレンジレスポンスメカニズムを通じて認証します。		
72	3552	インターネットの脅威モデル	トラフィックセキュリティを提供する	SSL/TLS		-	現在、最も普及したアプローチは、SSLもしくは、その後継であるTLSを使うことです。これらは、アプリケーション層においてTCP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。すなわち、これらは、TCP上で動作します。		IPsecが利用不能であり、かつ、トラフィックがTCPのみである環境において、TLSは選択肢となる手法です。なぜなら、アプリケーション開発者は、TLS実装をパッケージに含めることによって、容易にその存在を確保できるからです。	残念ながら、このSASLとTLSの組み合わせは、期待するほど強くはありません。積極的な攻撃者が、このコネクションをハイジャックすることは容易です。クライアントは、SSLコネクションの中間者となります。(我々は、通常この攻撃を防ぐサーバーを認証しているのではないことを思い出してください。)次に、単純に、SASLハンドシェイクをプロキシします。以降、少なくとも攻撃者に関しては、コネクションが平文であるかのようになります。この攻撃を予防するために、クライアントは、サーバーの証明書を検証する必要があります。		
72	3552	インターネットの脅威モデル	トラフィックセキュリティを提供する	SSL/TLS		-		使われている2つの主要なアプローチは、TLSコネクションについて別個の登録ポート番号を採用するアプローチ(例:HTTPoverTLSのポートは、443番)[HTTPTLS]と、[UPGRADE]もしくは[STARTTLS]のように基盤プロトコルからTLSに対して上方に交渉するためのメカニズムをもつアプローチです。		上方交渉アプローチが使われたとき、「両者がTLSを使うことを望むとき、攻撃者が平文によるコネクションを強いることができない」ように注意を払わなければなりません。		
72	3552	インターネットの脅威モデル	トラフィックセキュリティを提供する	SSL/TLS		-		「TLSは、TCPまたはSCTPのような信頼できるプロトコルに依存すること」を銘記してください。		これは、UDPを使うデータグラムプロトコルをセキュアにするためには使えません。		

72	3552	インターネットの脅威モデル	トラフィックセキュリティを提供する	SSL/TLS		-				TLSは、IPsecが無いIP層の攻撃の影響を受けます。	これらの攻撃は、何らかのサービス妨害またはコネクション切断の形態をとります。例えば、攻撃者は、SSLコネクションを切断するために、TCPRSTを偽装する可能性があります。TLSは、「切断攻撃」を検知するメカニズムをもっていますが、これらは、被害者に攻撃されていることを単に知らせるだけで、このような攻撃に直面したとき、コネクション存続性を提供しません。逆に、IPsecが使われている場合、このような偽装されたRSTを、TCPコネクションに影響を与えずに棄却できます。偽装されたRSTもしくは、TCPコネクション上の他のこのような攻撃が懸念される場合、AH/ESPもしくはTCPMD5オプション[TCPMD5]が選好される選択肢です。	
72	3552	インターネットの脅威モデル	トラフィックセキュリティを提供する	リモートログイン		-	特別な事例においては、IPsecまたはSSL/TLSを使うのではなく、直接アプリケーション中においてチャネルレベルのセキュリティを提供する価値がある可能性があります。そのような事例のひとつは、リモート端末セキュリティです。キャラクタは、典型的には、クライアントからサーバーに1キャラクタずつ送られます。	リモート端末サービスを利用するとき、しばしば、「他種の通信サービスをセキュアに行うこと」が望まれます。リモートログインを提供することに加えて、SSH[SSH]も、任意のTCPポートについてセキュアなポートフォワーディングを提供します。それゆえ、ユーザに任意のTCPに基づくアプリケーションをSSHチャネル上で動作させることを許容します。	SSL/TLSとAH/ESPは、すべてのパケットを認証し、暗号化するので、これは、20bitのデータ拡大を意味する可能性があります。telnet暗号化オプション[ENCOPT]は、メッセージインテグリティを断念することによって、この拡大を予防します。	「ファイアウォール を迂回して不正に使われている場合や、不正にセキュアでない内部アプリケーションを外界に露出している場合、SSHポートフォワーディングは、セキュリティ論点である可能性があること」を覚えておいてください。		
72	3552	インターネットの脅威モデル	サービス妨害攻撃とその対策	分散型サービス妨害		DDoS	より危険なのは、分散型サービス妨害攻撃[DDOS]です。DDoSにおいて、攻撃者は、標的マシンを同時に攻撃するように、数多くのマシンを準備します。通常、これは、数多くのマシンに攻撃のリモートによる開始ができるプログラムをしかけることによって達成されます。実際に攻撃を行うマシンは、「ゾンビ」と呼ばれ、真の攻撃者とは別の場所にいる善意の第三者によって保持されている可能性が高いものです。	DDoS攻撃は、対抗するのが極めて困難である可能性があります。なぜなら、ゾンビは、しばしば、正規のプロトコル要求を行って、単に本当のユーザを混雑によって押し出しているいるように見えるからです。	DDoS攻撃は阻止するのが困難ですが、プロトコル設計者は、プロトコルを設計する際に、この種の攻撃を認識していることが期待されます。			
72	3552	インターネットの脅威モデル	サービス妨害攻撃とその対策			DoS	サービス妨害攻撃は、日常避け難い現実と見なされています。問題のひとつは、「攻撃者は、しばしば被害者を迷惑させるために多くのサービス妨害攻撃から選択できること」であり、これらの攻撃の大部分が阻止できないので、普通の有識者は、しばしば、「可能性はあっても予防できない多くの他のサービス妨害攻撃があるとき、サービス妨害攻撃のうちの一種を防護する点はない」と想定します。		完全なDoS防護は困難であるので、DoSに対するセキュリティは、実用主義的に扱われなければなりません。特に、防護することが望まれる攻撃には、効率的に防護することができないものがあります。目的は、防護する費用に対して十分に高い深刻さがある攻撃に対して防護することによってリスクを管理するものである必要があります。攻撃の厳しさと防護の費用の両者は、技術変化に伴って変化し、それゆえ防護しなければならない攻撃も変化します。			
72	3552	インターネットの脅威モデル	サービス妨害攻撃とその対策				インターネット標準の著者は、そのプロトコルが影響を受けるサービス妨害攻撃について記述しなければなりません。	この記述は、このようなサービス妨害攻撃を避ける試みが、非合理的である旨か、範囲外であるかのいずれかの理由を含まなければなりません。	しかし、サービス妨害攻撃のすべてが同等であったり、より重要であるわけではありません。非現実的でない場合、サービス妨害攻撃がより困難になるようにプロトコルを設計することが可能です。	サービス妨害攻撃は、日常避け難い現実と見なされています。問題のひとつは、「攻撃者は、しばしば被害者を迷惑させるために多くのサービス妨害攻撃から選択できること」であり、これらの攻撃の大部分が阻止できないので、普通の有識者は、しばしば、「可能性はあっても予防できない多くの他のサービス妨害攻撃があるとき、サービス妨害攻撃のうちの一種を防護する点はない」と想定します。		

72	3552	インターネットの脅威モデル	サービス妨害攻撃とその対策	ブラインド攻撃	メッセージ挿入	TCPSYNサービス妨害攻撃	まず、攻撃者は、ひとつのパケットを送ることによって、被害者に膨大な資源（この場合はメモリ）を浪費させることができます。次に、攻撃者は、この行為を被害者から全くデータを受け取らずに行うことができるので、攻撃は、匿名で行うことができます。（それゆえ、膨大な数の偽装された発信元アドレスを使います。）	TCP/IPは、3ウェイハンドシェイクの設計に起因して、（2に記述されている）SYNフラッド攻撃に対して脆弱です。	[PHOTURIS]は、PhoturisにおいてSYNフラッド攻撃に似ている攻撃を予防するものであり、詰まり対策メカニズムを仕様としています。Photurisは、攻撃者に返される「クッキー」を生成するために、時間が可変の秘密を採用しています。このクッキーは、処理を進めるための交換のために、以降のメッセージにおいて返されなければなりません。興味深い機能は、「このクッキーは、後で交換において被害者によって再生成でき、それゆえ、攻撃者が被害者からのパケットを受信できることが証明されるまでは、被害者は状態を保持する必要はありません。	最近のSYNフラッド攻撃[TCPSYN]は、両方の属性を実証しています。：SYNフラッド攻撃は、容易・匿名・効果的であるので、攻撃者にとって他の攻撃よりも魅力的です。	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。	
72	3552	インターネットの脅威モデル	サービス妨害攻撃とその対策	ブラインド攻撃	メッセージ挿入	TCPSYNサービス妨害攻撃		例えば、サービス妨害攻撃は、標的とされたホストに指図された一連の偽のTCPSYNパケットを注入することによって、しかけられる可能性があります。標的となるホストは、自身のSYNで応答し、新しいコネクションのためにカーネルデータ構造を用意します。	例えば、TCPSYNサービス妨害攻撃[TCPSYN]は、送信者のアドレスを偽装することなく、しかけられて成功する可能性があります。	また、TCPの設計が、この攻撃を可能にしています。	攻撃者は、3ウェイハンドシェイクを完結させないので、用意しているコネクション終点は、ひたすらカーネルメモリを埋めながら待つことになります。典型的なTCPスタック実装は、この「半開き」状態のコネクション数を制限しており、この制限に達したとき、正規のホストからも、それ以上のコネクションを開始することができません。	
72	3552	インターネットの脅威モデル	サービス妨害攻撃とその対策	サービス妨害の回避	メッセージ挿入	TCPSYNサービス妨害攻撃		設計者は、ブラインドサービス妨害攻撃を予防するためにあらゆる可能な試みを行う必要があります。				
72	3552	インターネットの脅威モデル	サービス妨害攻撃とその対策	サービス妨害の回避	ブラインド攻撃		攻撃者にあなたからのデータを受信できることを証明させる		ブラインド攻撃は、攻撃者に「被害者からのデータを受信できること」を証明することを強いることによって打ち破ることができます。よくあるテクニックのひとつは、「攻撃者がメッセージ交換の初期に得られたはずの情報を使って返信すること」を要求することです。この対策が行われた場合、攻撃者は、（追跡を容易にする）自身のアドレスを使うか、攻撃を開始したホストまでの経路をたどれてしまうアドレス偽造を使用しなければなりません。			
72	3552	インターネットの脅威モデル	サービス妨害攻撃とその対策	サービス妨害の回避					あなたよりも少ない資源しかもたない攻撃者が攻撃をしかけるとき、あなたよりも多くの資源を消費する場合では、攻撃者は効果的な攻撃をしかけることができません。よくあるテクニックのひとつは、攻撃者に暗号技術的操作のような時間がかかる操作を要求することです。「攻撃者が本質的に十分なCPUの処理能力を集結できる場合、サービス妨害攻撃をしかけ続けることができること」を銘記してください。例えば、このテクニックは、[TCPSYN]に記述されている分散型の攻撃をくい止めません。			
72	3552	インターネットの脅威モデル	サービス妨害攻撃とその対策	サービス妨害の回避					それゆえ、（少なくとも詐称攻撃においては）小さなサブネット上のホストは、攻撃者にとって無用です。なぜなら、この攻撃は、攻撃対抗手段を配備できるようにサブネットにトレースバックできるからです。（これは、攻撃者の位置を知るのに十分です。）（例えば、境界ルーターは、そのサブネットからのトラフィックすべてを棄却するように設定できます。）よくあるテクニックのひとつは、「攻撃者がメッセージ交換の初期に得られたはずの情報を使って返信すること」を要求することです。			

72	3552	インターネットの脅威モデル	サービス妨害攻撃とその対策	ブラインドサービス妨害				攻撃者が、被害者からのトラフィックを受け取ることができなければならない場合、攻撃者は、ルーティング基盤を操作するか、自身のIPアドレス使うかのいずれかをしなければなりません。	両者は、被害者に攻撃者を追跡し、かつ／または、攻撃者のトラフィックを棄却する機会を提供します。	ブラインドサービス妨害攻撃は、特に有害です。ブラインド攻撃において、攻撃者は顕著な優位性をもちます。		
72	3552	インターネットの脅威モデル	オブジェクトセキュリティ対チャネルセキュリティ	サービス妨害の回避				区別は、いつも明確であるとは限りません。例えば、S-HTTPは、単一のHTTPトランザクションのためにはオブジェクトレベルセキュリティを提供しますが、Webページは、典型的には、複数のHTTPトランザクション（基本ページと数多くのインラインのイメージ）から成ります。それゆえ、Webページ全体の観点からは、これは、むしろ、チャネルセキュリティのように見えます。Webページ用のオブジェクトセキュリティは、ページ毎の非開示のためのセキュリティと、単一ユニットとして組み込まれているすべてのコンテンツから成ります。				
72	3552	インターネットの脅威モデル	オブジェクトセキュリティ対チャネルセキュリティ	ファイアウォールとネットワークトポロジー				ネットワークをファイアウォールを使って外部ネットワークと内部ネットワークに区切ることは、3つの理由によって、「彼らのプロトコルがこのような環境に配備される」と安全に想定することはできません。 (1) 閉じた環境中で採用されるように設計されたプロトコルは、しばしば、後でインターネット上に採用されるようになり、それゆえ、深刻な脆弱性を作り出します。[SOAP]や[HTTP]のような一般的なアプリケーション層プロトコルを通過するようになってきています。これらの一般的なプロトコルに基づいたネットワークプロトコルは、一般に、「ファイアウォールがそれらを防いでくれる」と想定できません。 (2) トポロジー的に接続されていないように見えるネットワークは、接続されている可能性があります。その理由のひとつは、「ネットワークが外界からのアクセスを許可するように再設定された」可能性があります。 (3) システムに対する最も深刻なセキュリティ上の脅威は内部者からであり、外部者からではありません。内部者は、定義からして内部ネットワークにアクセスできるので、ファイアウォールのようなトポロジーによる防護では、それらを防いでくれません。				
72	3552	インターネットの脅威モデル	オブジェクトセキュリティ対チャネルセキュリティ				オブジェクトセキュリティとチャネルセキュリティを概念的に区別することが有用です。オブジェクトセキュリティは、データオブジェクト全体に適用されるセキュリティ手段をいいます。チャネルセキュリティ手段は、オブジェクトを透過的に運ぶことができるセキュアチャネルを提供しますが、そのチャネルは、オブジェクト境界について特別な知識をもちません。			電子メールメッセージの事例を考えます。メッセージがIPsecもしくはTLSによってセキュアにされたコネクション上を運ばれるとき、そのメッセージは、転送中は防護されています。しかし、これは、受信者のメールボックス中や、途中の中間スプールファイルでは防護されていません。さらに、メールサーバーは、一般に、ユーザではなくデーモンとして動作するので、一般的に、メッセージの認証は、ユーザー認証ではなく、単にデーモン認証を意味するに過ぎません。さらに、メールのトランスポートは、「ホップbyホップ」なので、たとえユーザが中継の最初のホップを認証する場合でも、認証は、受信者によって安全に検証されることができません。	
72	3552	インターネットの脅威モデル	オブジェクトセキュリティ対チャネルセキュリティ				「オブジェクトセキュリティとチャネルセキュリティの相違は視点の問題であること」を銘記してください。プロトコルスタックのある層におけるオブジェクトセキュリティは、しばしば、直上の層からはチャネルセキュリティのように見えます。それゆえ、IP層から見れば、各パケットは、個々にセキュアにされたオブジェクトのように見えます。しかし、Webクライアントの視点からは、IPsecは、単にセキュアなチャネルを提供します。			逆に、電子メールメッセージがS/MIMEまたはOpenPGPで防護されているとき、受信者によって検証・復号されるまで、メッセージ全体が暗号化され、インテグリティが確保されます。これは、メッセージを送ったマシンではなく、実際の送信者についての強い認証も提供します。これはオブジェクトセキュリティです。さらに、受信者は、署名されたメッセージの真正性を第三者に提供できます。	