RFC1636 IAB インターネットアーキテクチャのおけるセキュリティについてのワークショップの報告(1994)

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	本書は、インターネットの達人たちによって幅広い視野から書かれたセキュリティについてのアイディアを含む作業ノート類として見なされる必要があり、セキュリティのみならず、ルーティング、移動性、リアルタイムサービスおよびプロバイダー要件を含みます。				
	ほとんど誰もが、インターネットが、より良いセキュリティを必要していることに合意します。				
	要件の 1つは、「エンド to エンド」通信のために守秘性、認証およびインテグリティをサポートすることです。				
	「ポイント to ポイント」アプリケーションについて、ワークショップでは、既存のセキュリティ テクニックは、守秘、認証およびインテグリティのサービスを効果的にサポートするのに適当であると考えました。				
	既存の技術は、マルチキャスト グループ全体のレベルにおいて、守秘性、認証およびインテグリティ をサポートするのに適格です。個別のマルチキャスト源泉のレベルにおいて、認証とインテグリティをサポートすることは、性能に限界があり、技術進歩が要求されるでしょう。				
	「エンド to エンド」制御は、末端システムもしくはユーザ識別子に基づく必要があり、下位層の識別子もしくはロケーター情報ではありません。この要件は、既知の鍵配布と暗号技術的テクニック を応用することから成るエンジニアリング作業を生み出すはずです。				
	すべてのホストは、自体のセキュリティ防護をもちますが、これらの防護の強度は、それらを運用管理する労力に依存します。注意深いホストのセキュリティ運用管理 とは、良い(クラックしにくい)パスワードを設定する原則をユーザに強制するのみならず、カーネルやアプリケーションにあるセキュリティホールを塞ぐことを意味します。				
	れらの拡張は、アーキテクチャについて、 資源の盗用を防ぐためと、認可されていないトラフックによるサービス妨害を防ぐための両方のために、ユーザが利用を認可されていない資源にさわることができないようにするための新しい一連のセキュリティ論点を提起します。				
	これらの資源は、 ネットワーク内における仮想的チャネルとして使われます。ここで、各仮想的チャネルは、パケット の特定の構成部分もしくは「クラス」によって使われることが意図されています。				
	Secure QOS (すなわち、不正な仮想的チャネルの利用に対する保護)は、アクセスコントロールメカニズムの 1形態です。一般に、これは、認可された「クラス」 を定義する何らかの形態の状態確立(設定)に基づきます。この設定は、管理設定(典型的には、 先行して、ユーザの集合のためのもの)を通じて行われる可能性があり、あるいは、これは、パケットまたは特別なメッセージの中の制御情報(典型的には、 利用時にフロー/データの発信元または受信者によるもの)を通じて動的に行われる可能性があります。状態の確立に加えて、 成功パケットが確立されたクラスに属するようにするために、何らかの形態の認証が必要とされます。解決すべき一般的なケースは、マルチキャスト グループです。それは、一般に、マルチキャスト問題は、構成部分として、2者の場合を含むからです。このワークショップは、QOS 問題をセキュアにするためのアプローチを開発しました。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	ネットワーク運用は、（ルーターや DNS サーバーを含む）ネットワーク インフラストラクチャを設定・運用するために使われる 管理と制御のプロトコルに依存します。ネットワーク インフラストラクチャにおける攻撃は、ユーザの視点からは、サービス妨害をもたらす可能性がありますが、ネットワーク 運用者の視点からは、攻撃からのセキュリティは、ネットワーク コントロールと管理メッセージについて認証とインテグリティを要求します。				
	ルーティング プロトコルをセキュアにすることは、まさにエンジニアリングの仕事であるように考えられます。このワークショップは、次のように結論づけました。 a) すべてのルーティング情報交換は、隣のルーター間において認証される必要がある。 b) すべての経路情報の源泉は、認証される必要がある。 c) 経路情報投入者である機関を認証することは実現可能であるが、その経路情報（例： 集合点（aggregation））の運用の認証については、さらなる考慮を要する。				
	証明書用 DNS 名の利点は、「DNS 名の利用が、インターネットにおけるセキュリティの広範囲における利用を促進すること」を期待します。DNS 名が、将来、X.509 に基づく証明書 のような、より能力のある命名メカニズムによって置き換えることができることが期待されます。				
	「証明書 のためにどの名前空間を使うかという質問は、これらの名前を取得するためのインフラストラクチャを構築する問題とは独立したものであること」				
	ファイアウォールは、インターネット トポロジーにおいて接続された特定のセグメントを隔離するために使われる可能性があります。このようなセグメントが外部インターネットへ複数のリンクをもつとき、接続されたファイアウォールマシンは、すべてのリンク上にあることが要求されます。				
	「ファイアウォールは、セキュリティ機能 を 1ヵ所に集約し、管理・インストール・設定を単純化するので、ファイアウォールの考え方は、非常に力強い。」				
	ファイアウォールは、「柔らかく噛みごたえのある内部をもった硬くバリバリとした殻」を提供します。すなわち、ファイアウォールは、セキュリティ の間違ったセンスを助長し、ファイアウォール境界内部のセキュリティを緩くさせることになります。				
	ファイアウォール支持者は、「ファイアウォール は、追加的な対策として重要である」と反論します。				
	良いセキュリティのために数多くのホストを設定すること。このより基本的な問題が解決できた場合、ファイアウォールは、一般に、必要不可欠ではなくなります。				
	ファイアウォールは、組織体全体を通じて、組織体における最善のセキュリティの拡張ができるようにします。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	IP 層ファイアウォール上のこのシナリオの主要な利点は、「生の IP データグラムは、決してファイアウォールを通過しないこと」				
	すべての恩恵を得るためには、アプリケーション層ファイアウォールは、各アプリケーションについて個別にコードを書かれなければなりません。				
	通常、ファイアウォールルーターは、一式のフィルタリングルールをもち、各ルールは、「パケット属性」と「対処」を規定します。				
	ファイアウォールにおける高速データグラム転送パスは、各到着パケットを、すべての有効なルールのすべてのパケット属性に照らして処理し、属性が一致したとき、対応する対処を行います。				
	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うるように、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。				
	「これは、1つの可能なメカニズムの部分的なスケッチとして意図されているに過ぎないこと」を強調ておきます。				
	セキュリティは、「各ファイアウォールがデータ パケットが実際に C から来たことを検証することができること」を要求します。				
	ファイアウォール ルーターは、再認証を要求する可能性があります。その原因は、次のとおりです。: ＊ ルーティングの変更によって、パスに追加された。 ＊ 属性の項目が期限切れとなった。 ＊ おそらく許容可能な属性のリストを失うクラッシュ後に、新たに再活性化された。				
	IP 層ファイアウォールにおいて、このような偽装を防ぐために、3つのメカニズムのクラスがあります。				
	マルチキャスト トラーフィックにファイアウォール通過を許すために必要とされるルールは、送信者ではなく、受信者によって提供される必要があります。				
	マルチキャスト通信は、以前の節に記述された 3つのレベルのセキュリティのいずれをも使うことができますが、すべてのファイアウォールは、データ ストリーム の起点者と同一の秘密を共有する必要があるでしょう。その秘密は、受信者に他のチャネルを通じて提供される必要があり、（資源が受信者の率先によって行われる RSVP と同様のやり方で、）受信者が率先してファイアウォールに転送されます。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	セキュリティパケットについての透過性 　上述のメカニズムを運用することについて、クライアントコンピュータとファイアウォールによって信頼されている認証・認可サーバーの間に使われている「認証が要求される」通知と認証／認可プロトコルは、すべてのファイアウォールによって自動的に転送されなければなりません。				
	1) 入り方向の呼び出しが無いこと。（xterm 問題） 2) 固定ポート番号。（portmapper または tcpmux 無し） 3) 全体の再指図が良い。（アプリケーション ゲートウェイ） 4) プロトコル中において再指図をしない。 5) 暗号強度の乱数である 32 bit シーケンス番号。 6) 固定長とヘッダー フィールドの数。 Type フィールドは良いが、固定ポート番号がある場合、それらは不要である。				
	アプリケーション層ファイアウォールと比較すると、IP 層ファイアウォールのスキームは、数多くの便益を提供することができます。: ＊ エンドホストに追加的認証が要求されない。 ＊単一認証プロトコルを、すべての意図するアプリケーションに使うことができる。 ＊IP 層ファイアウォールは、あまり性能劣化をもたらさない。 ＊IP 層ファイアウォールは、TCP 接続を配布することなく、クラッシュしても状態回復できる。 ＊経路がオープンな TCP 接続を配布することなく変更できる。 ＊失敗を引き起こす 1点というものが無い。 ＊これは、アプリケーションと独立している。				
	ネットワーク資源において高価な、そのような QOS の価値を求めるユーザを認証・認可する必要性があり、これらの資源の盗用を防ぎ、他者によるサービス妨害攻撃を防ぐことが必要不可欠です。				
	「たとえ QOS サポートが無くても、いかなるインターネット層セキュリティメカニズムにおけるパス設定もまた、エンジニアリング上の良い理由があること」				
	「リアルタイム QOS について、暗黙のパス設定過程に基づいた代替的提案があること」を銘記する必要があります。				
	パス設定プロセスをセキュアにするために、我々は、「パス設定リクエストには、要求者が既知で、かつ、当該リクエストを行う権限をもつことを示す信用に足る保証を提供するユーザクレデンシャル を伴うこと」を要求します。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	この認可のシンプルなバージョンは、ルーターの管理インターフェイス上のパスワードである可能性があります。（このようなパスワード スキームの限界は、よく知られており、ここにおける論点ではありません。）設定が個々のアプリケーションによって行われることを要求する場合、いくつかのユーザ固有の認可が想定されなければなりません。				
	「LLID は、少なくとも概念的には、ユーザのアドレスとは区別されること」				
	「ユーザの権限は、使われているアドレスによって判定されないこと」				
	「LLID は、それが表現する QOS パラメータをルーターが識別できるようにする構文を具現する」 ことについて特に要件はありませんが、そのような構造を強いることについて、妨げるものもありません。				
	「IP データグラムが、ネットワークの様々な段階において、パケットをクラス分けするために使うことができる 1つの LLID を含むこと」				
	LLID の属性は、可能な限り、広範な要件に適合するように抽出される必要があります。 ＊ （後述する）有効期間は、セキュリティ プロトコルの要求（堅牢さと効率性のバランスをとること）と、アプリケーションの要求（LLID が期限切れとなったとき、再度、新規のパス設定を扱う必要があること）の両方に適合しなければならない。自動的に再度、新規のパス設定リクエストを行うサービス は、有用な端末機能となるであろう。 ＊信頼の程度は、我々が合理的に適合させられる最も厳正な要件に適合するように、十分に高くなければならない。 ＊LLID 構造の粒度は、ネットワーク中のいかなる資源選択についても、パケットクラス分けを十分に細かく分類できるものでなければならない。それゆえ、我々は、「アプリケーションからの各パケットのストリームが個別の LLID をもつこと」を期待する必要がある。複数のストリームを 1つの LLID または 1つの認証子に集約することは、ほとんどあり得ない。				
	少なくとも、内容的に LLID の利用を検証することが必要不可欠です。すなわち、「認可されたやり方において言明されていること」を確認することです。				
	それゆえ、LLID の利用は、LLID に基づいて QOS の判断を行うルーターによって認証される必要があります。（すべてのルーターが LLID に「注意を払う」わけではないことに注意。）				
	原則として、LLID 言明の有効性は、すべてのルーターにおいて必要不可欠ではありませんが、すべてのパケットについてチェックされる必要があります。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	LLID の利用を検証するための、いくつかの候補となるテクニックがあります。我々は、3つの基礎的なテクニックを識別しました。 * デジタル署名 * 印付け（sealing） * 一時的パスワード				
	長期的、つまり半永久的な LLID に釣り合う利点は、ルーターの手動設定でパケットクラスを確立するといった原始的なパス設定手法が実用的なものになることです。				
	「遅延は、重要な論点ではあるが、セキュリティの関心事によって影響を受けない題材である」とみています。RSVP や ST-II のような資源確保プロトコルの設計者は、今日、これらのプロトコルの遅延について議論しています。パス設定リクエストメッセージに認証子を追加することは、それを検証するのに必要とされる処理を増やし、認証サービスをもったメッセージ交換さえ意味する可能性がありますが、パス設定段階に要する時間は、既にラウンドトリップ遅延のオーダーとなっており、実質的には影響を与えません。しかし、パス設定プロトコルのための高レベルの認証と認可の手法の設計は、「この過程は、パケット毎処理レベルまでは要求されませんが、かなり時間的に厳しい処理であること」				
	「少なくとも、システムは、短期において、認可されていない用法を許す 一連のパス設定リクエストを使う攻撃に対して脆弱であること」				
	「サービス妨害攻撃は、パス設定過程を無効なパス設定リクエストによって溢れさせることによって上乗せされる可能性があり、これらのすべては、処理され、棄却される必要があること」				
	「受信者の加入は、明示的パス設定段階を要求すること」				
	「ブラックネットワーク区画を越えて、レッドネットワーク区画に至るパケットの旅において、可能な限りパケットをエンコードする暗号化ユニットを使うこと」				
	「システムは、その構成要素に最小権限を求めるように構築されたときに最も堅牢である」				
	特定の経路について、我々がパケットを配信するルーターを信頼しないかぎり、サービスの仮定に、正当化できるものはありません。				
	その他に我々がネットワーク上に配備しなければならない要件は、ルーティングに関するものです。ファイアウォールがある場合、我々は、そのルーティングアーキテクチャがそのファイアウォールを迂回しないことを信頼しなければなりません。				
	この種の「黙示的（implicit）」 LLID は、特にホストが、移動するときに、その IP アドレスを変更できる場合、短命でなければなりません。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	現行 IPv4 ヘッダーは、LLID を検証する認証子フィールドをもちません。認証子フィールドは、オプションとして運ばれる可能性があります。; それを追加することは、ネットワーク資源確保に堅牢さをもたらします。認証子の作成について上述した、あらゆるスキームが利用可能です。例外は、シンプルなパスワードによる認証子が使われた場合、LLID は、無作為に抽出できないので、これは、明示的な分離したフィールドでなければなりません。				
	「パス設定プロトコルをもたない現在のインターネットは、サービス妨害攻撃に対してセキュアにすることができないこと」				
	「管理インターフェイスを使って行われるパス設定について、LLID を検証するためには、発信元とルーターの間で共有された秘密は、長期に渡って維持管理されなければならず、これは、手作業でパス設定されなければならないこと」				
	「ルーターは各送信元アドレスごとに個別の FQ（fair queueing）クラスを暗黙的に作成できること」				
	、ある送信元からのトラフィックが、その他を排除してしまうほどにネットを溢れさせることを防ぐこと				
	「パケット中の LLID とアドレスが概念的に区別される場合、かつ、LLID を検証するのに適する手段がある場合、そのアドレスを検証する理由は無いこと」				
	a) パケット中で運ばれる LLID (Low-Level IDentifier) を、パケット中のアドレスと概念的に分離することが重要です。 b) 各パケット中で 1つの LLID が運ばれます。これは、複数の LLID が使われている場合よりもルーターにおける追加的な状態（保持の必要性）を意味する可能性がありますが、1つだけ LLID を使うことは、より拡張性があります。 c) ホップごとの LLID 認証メカニズムは、秘密の配布を制限する、高度に拡張可能なアプローチを提供する可能性があります。しかし、その堅牢さの限界は、網羅的に調査されなければなりません。 d) 統計的サンプリングもしくは事後検出メカニズムは、性能問題に対応するためにルーターに採用される可能性があります。				
	認証サービスの目的は、単に名前を検証すること、もしくは、より緻密には「メッセージ」の起点を検証すること				
	認可サービスは、認証された名前に対してどのサービスが利用可能であるかを判定します。				
	我々は、認証は、インターネット規模のサービスとなる一方、認可（authorization）は、 各資源について、どのアクセスが認可されるかについて特定のものであることを期待します。				
	認証サービスは、認可サービスの実現を容易にするように設計される必要があり、「ワイルドカード」をサポートする必要があります。				
	個人は、認可を様々な源泉から得る可能性があります。純粋に身元に基づくアクセスコントロール システムを使うとき、そのユーザは、それぞれのサービスにアクセスすることが許されている役割に応じて、複数の身元（すなわち、DN）を得る必要があります。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	代替的アプローチのひとつは、ユーザについて非常に少数の身元をもち、（ユーザの ID と結びつけられた権限を授与する）認可の授与者が（署名した）クレデンシャルをもつことです。このように追加的な署名がなされたクレデンシャルは、「ケイ パビリティ（capabilities）」として知られています。こうして、ユーザは、一般的な身元クレデンシャル（例： X.509 証明書）を通じて彼女の身元を確立することができ、要求されるケイパビリティを提示することによって認可を確立することができます。				
	信頼パス中の特定のパスに従うことによって、人は、信頼を確立することと、ユーザが「認可されたグループ」に属することを見せることの両方ができます。				
	「<huitema@sophia.inria.fr> と <huitema@iab.isoc.org> は、同一人物について 2つの名前ですが、ユーザが、すべての彼のトークンが見えることを望まない場合が多くあること」を知ること				
	ローカル環境を離れるために、我々は、ローカル クレデンシャルのみを必要とします。; 遠隔サーバーに接続するためには、我々は、宛先のクレデンシャルのみを必要とします。それゆえ、我々は、1つ、もしくは、おそらく 2つのクレデンシャルを必要とします。クレデンシャルは、宛先から配布される可能性があります。一般的なクレデンシャル； ワイルドカード；「FTP 提供の」トークンで十分であることは、よくあることでしょう。				
	各パケットは、「複数の発信元からのパケットが、数多くの受信者によって、独立して復号されることができること（特に、喪失パケットがある場合）」を確保するために、独立した暗号技術的処理を要求します。				
	許容可能とするために、認証プロトコルは、パケット喪失に耐性がなければなりません。				
	プラグアンドプレイ運用について、ネットワークに「プラグされた」新しいマシンは、以下の事項が必要です。: (1) 他のデバイスと通信できるように、ロケーターを得る。 (2) 識別されつように名前を登録、または、獲得する。（例： マシン名） (3) ネットワーク上で利用可能なサービスを発見する。（例： プリンター、ルーター、ファイルサーバー等） (4) ネットワーク上の他のシステムと通信できるように発見する。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	このような環境において、同様なプラグアンドプレイ能力が必要とされますが、その新しいデバイスは、これらの機能を果たす前に、「認証され」なければならなりません。発見過程における各手順において、新しいデバイスは、サービス について学習する前に、自身を認証させなければなりません。 この手順は、以下のとおり。: ＊スマート カード、スマート ディスク、もしくは、同様のデバイスから HLID （高位層識別子）を得る。 ＊名前を登録し、他のサービスの場所を発見するために、その HLID を使って、最初のプラグアンドプレイサーバーに自身を認証させる。 ＊その HLID に基づいて、ネットワーク上で利用可能なサービス（例：プリンタ、ルーター、ファイルサーバー等）を発見する。 ＊ネットワーク上の他のシステムと通信できるように、それらを発見する。				
	人間には、パスポートとして働き、ローカル ネットワークによって検証可能な HLID が授けられなければなりません。この HLID は、グローバルに固有であり、かつ、何らかの認知されている機関によって登録／割り当てされなければなければなりません。				
	人間がマシンをローカル ネットにプラグするとき、そのマシンは、自身をネットに、人間の HLID で識別させます。ローカル ネットが、誰にでもそのネットワーク上 にプラグアンドプレイすることを許可するポリシーを持つ場合、訪問者に無制限のアクセスと特権を許可する HLID とアドレスの割り当てを無視します。より可能性があることとして、ローカルネットは、訪問者に、アドレス、もしくは、いかなる特権を許可する前に HLID を認証します。				
	この点について、HLID は、ローカル ネットワークへの訪問者のみを認証しました。;「どのサービスもしくは資源を、その訪問者が使う資格を与えられているか」の論点は、対応されてきませんでした。新しいユーザを認証できるようにするために、オーバーヘッドが低いアプローチを開発することが望まれます。				
	グローバルな認証インフラストラクチャを開発・配備することは、重要な目的ですが、数年かかります。短期における、その他の有用なアプローチは、チャレンジ／レスポンス によるユーザ認証スキーム（例： S/Key）の利用です。				
	一時的な鍵は、TCP 接続を開始する SYN ハンドシェイクにおいて交換される可能性があります。				
	鍵は、鍵交換プロトコル、データ 暗号化アルゴリズム、接続を復号するのに使われるべき鍵を仕様とする新しいオプションを使って交換することができます。				
	「TCP オプションは、制限されたデータ量しか運べないこと」				
	セキュリティ問題の外部的診断を行う 組織体は、自身のパスワードの強度をチェックするために、CRACK や他のツールを使うことが強く推奨される必要があります。様々なセキュリティ 探査を外部から実施することも有用でしょう。このことが非常に慎重を要する論点であるので、このような探査については、正しい支援を得るための何らかの配慮が必要です。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	セキュリティリスク公開チャネルを決定する 　どのチャネルがセキュリティリスクの情報を普及するために使われる必要があるか？				
	ワンタイム パスワードの利用促進 　入手可能なパッケージ: S/Key, SecurID, Enigma, Digital Pathways.				
	プロトコル開発者のためのセキュリティ親和性とファイアウォール親和性についてのガイドラインを策定し公開する。				
	脅威を隔離するためにトポロジーを制御する。				
	プライバシーポリシーを設定する。: ＊常に ＊可能である限り ＊「サイトセキュリティハンドブック（Site Security Handbook）」を更新する。 ＊Kerberos の利用を支援する。				
	これらの活動は、いくつかのプロトコル設計と変更を要求します。; しかし、それらは、既存のセキュリティ技術を使うので、研究を要しません。 ＊認証プロトコル o 技術の選択の問題がある。公開鍵暗号技術は、一般的に、優位にあると考えられているが、特許となっており、比較的長い計算時間がかかる。共通鍵暗号技術（Kerberos で使われている Needham-Schroeder アルゴリズムなど）には、技術的な欠点があるが、特許とされていない。共通鍵暗号に基づくシステムや認証のみのためのシステムは、特許の対象となることなく、自由に輸出可能である。 ＊Kerberos を押し出す o 公開鍵暗号技術を使うメカニズムと相互運用できるようにするために、Kerberos 上でエンジニアリングが必要。 ＊PEM/RIPEM/PGP... を押し出す ＊認証された DNS を開発する ＊鍵管理メカニズムを開発する ＊証明書サーバー インフラストラクチャの設定 o 可能なサーバー メカニズム（DNS、Finger、SNMP、電子メール、Web および FTP を含む。） ＊Web のための認証をエンジニアリングする				