「医療情報システムの安全管理に関するガイドライン」で使用することが容認されているインターネット VPN の実現を目的として PacketiX VPN ソフトウェアを使用することが技術的に可能であることを示す資料 (リスクアセスメント結果)

2012 年 5 月 11 日
ソフトイーサ株式会社 通信事業部
se-vpn3-support@softether.co.jp

概要

本資料は、ソフトイーサ株式会社が開発・販売しているインターネット VPN を構築するための VPN ソフトウェアである PacketiX VPN (http://www.softether.com/jp/vpn3/) が、『平成 18 年度「医療情報システムの安全管理に関するガイドライン」の実装事例に関する報告書』 (平成 19 年 3 月 HEASNET 公表、http://www.heasnet.jp/open/document/report2007/A01.pdf、以下「報告書」) が提示しているセキュリティ要件に適合していることを技術的に示すために作成したものである。

ネットワークにおける脅威に関するリスクアセスメント結果表

報告書で指摘されているネットワークにおける脅威 (PP) の一覧 (「4.2 ネットワークにおける脅威とセキュリティ対策の整理」における「4.2.1 ch セキュリティ」の(1)に記載) について、PacketiX VPN をインターネット VPN のために用いることで、これらの各脅威に対して十分に対応することができることを示すため、以下に技術的に整理した。

類型	脅威	PacketiX VPN においてこの脅威に対応することができるかどうか	左記事実を証する根拠文書
T1	平文伝送	PacketiX VPN では暗号化に IPsec における IKE および ESP と同等以上の認証・鍵交換・暗号化およびメッセージ認証の仕組みを用いており、具体的には、IPsec で一般的に使用されている暗号化アルゴリズムである DES、3DES および AES を使用することが可能である。暗号強度は 56bit から 256bit まで選択可能であり、現時点で AES 256bit を使用することにより、現実的な解読は困難である。	VPN マニュアル「2.1 VPN 通信プロトコル」、「12.4 PacketiX VPN プロトコル仕様」 FIPS 197 FIPS PUB 180-1

類型	脅威	PacketiX VPN においてこの脅威に対応することができるかどうか	左記事実を証する根拠文書
T2	共有パスワード	PacketiX VPN においては、認証方法は「パスワードによるユーザー認証」と X.509 証明書および RSA 秘密鍵を用いた「PKI によるユーザー認証」の 2 種類に対応している。パスワードによるユーザー認証を用いて VPN 接続時の認証を行う場合、ダイジェスト認証方式 (SHA-1 160bit) により、パスワード本文がいかなる時点でもネットワークを流れないようにして認証することが可能である。また、一旦本ソフトウェアで VPN を構築した後は、すべての伝送路が、T1 において説明したように強固な暗号トンネルによって実現されるため、その中でユーザーが使用したプロトコルで仮に平文パスワードが流れた場合でも、そのデータは実際のインターネット上を流れることがない。	VPN マニュアル「2.2 ユーザー認証」 FIPS PUB 180-1
T3	辞書攻撃	PacketiX VPN においては、認証方法は「パスワードによるユーザー認証」と X.509 証明書および RSA 秘密鍵を用いた「PKI によるユーザー認証」の 2 種類に対応している。「PKI によるユーザー認証」を用いる場合は、辞書攻撃は原理上不可能である。「パスワードによるユーザー認証」を用いる場合において、攻撃者が仮に当該パスワードを暗号化したハッシュデータを入手した場合において、パスワードの長さが約 8 文字以上で複雑である場合 (一般的に辞書攻撃に対して耐性が強いパスワードである場合) は、ハッシュ関数 (SHA-1 160bit) を用いている現状では、解読を現実的な時間で終わらすことはできないため、安全である。ユーザーが脆弱なパスワードを使用している場合は、辞書攻撃または VPN サーバーに対するブルーとフォースアタック等により攻撃が成功する場合があるため、「パスワードによるユーザー認証」を用いる場合においては約 8 文字以上で複雑なパスワードを使用するようにユーザーに指導するか、もしくは「PKI によるユーザー認証」を使用することを要する。この事項は、PacketiX VPN に限らず、他の VPN やリモートアクセス可能なシステムすべてで言える共通事項である。	VPN マニュアル「2.2 ユーザー認証」 FIPS PUB 180-1
T4	推定攻撃	報告書でいう「推定攻撃」とはブルートフォースアタックのことである。PacketiX VPN における VPN の通信トンネルは IPsec における IKE および ESP と同等以上の認証・鍵交換・暗号化およびメッセージ認証の仕組みを用いており、具体的には、IPsec で一般的に使用されている暗号化アルゴリズムである DES、3DES および AES を使用することが可能である。共有暗号における暗号強度は 56bit から 256bit まで選択可能であり、現時点で AES 256bit を使用することにより、現実的なブルートフォースアタックによる鍵の割り	VPN マニュアル「2.1 VPN 通信プロトコル」、「12.4 PacketiX VPN プロトコル仕様」 FIPS 197

類型	脅威	PacketiX VPN においてこの脅威に対応することができるかどうか	左記事実を証する根拠文書
		出しは不可能となっている。	
T5	NIS, 解読ツールの存在	PacketiX VPN における VPN の通信トンネルは IPsec における IKE および ESP と同等以上の認証・鍵交換・暗号化およびメッセージ認証の仕組みを用いており、具体的には、IPsec で一般的に使用されている暗号化アルゴリズムである DES、3DES および AES を使用することが可能である。AES 256bit を使用する場合、現時点で現実的なブルートフォースアタックによる鍵の割り出しが可能な解読ツールは存在していない。	VPN マニュアル「2.1 VPN 通信プロトコル」、「12.4 PacketiX VPN プロトコル仕様」 FIPS 197
T6	トポロジーの破壊	PacketiX VPN における VPN の通信トンネルは IPsec における IKE および ESP と同等以上の認証・鍵交換・暗号化およびメッセージ認証の仕組みを用いており、具体的には、VPN 接続を受け付ける側 (VPN サーバー) と VPN 接続を開始する側 (VPN クライアントまたは VPN ブリッジ) の両者が双方を X.509 証明書および RSA 秘密鍵を用いた PKI 認証によって正確に認証することができる。これにより、報告書で指摘されているような、攻撃者がトポロジーを破壊するなどして通信経路上に割り込んでいる場合であっても、中間者攻撃は VPN トンネルを接続する際に検出され、接続が確立せず、攻撃は必ず失敗する。また、一旦確立された VPN トンネル内の通信は IPsec で一般的に使用されている暗号化アルゴリズムである DES、3DES および AES によって暗号化されており、MD5 または SHA-1 によってデジタル署名されているため、盗聴や IP ヘッダの改ざんその他の攻撃は不可能である。	VPN マニュアル「2.2 ユーザー認証」、「2.3 サーバー認証」 FIPS 197
T7	同一リンク上の判別	PacketiX VPN には「IP アクセス制御リスト」機能が付属しており、同一リンクローカルネットワーク上に存在するホストか否かを IP アドレスおよびサブネットマスクによって指定したルールによって許可または拒絶することによりアクセス制御を行うことが可能である。したがって、あらかじめ許可されたネットワーク以外である外部ネットワークからの攻撃はこの時点で拒絶され、VPN コネクションを確立するためのネゴシエーションフェーズにすら攻撃者はたどり着くことができない。	VPN マニュアル「3.5.11 IP アクセス制御リストによる接続元の限定」
T8	常用プロトコルでの攻撃	VPN については無関係 (この脅威はファイアウォールに関するものである)。	
T9	内部の脅威	VPN については無関係 (この脅威はサーバーに関するものである)。	
T10	情報の不正コピー	VPN については無関係 (この脅威はサーバーに関するものである)。	

類型	脅威	PacketiX VPN においてこの脅威に対応することができるかどうか	左記事実を証する根拠文書
T11	セッション乗っ取り	PacketiX VPN によって一旦確立された VPN トンネル内の通信は IPsec で一般的に使用されている暗号化アルゴリズムである DES、3DES および AES によって暗号化されており、MD5 または SHA-1 によってデジタル署名されているため、セッション乗っ取りは不可能である。この機能を実現するために、IPsec における IKE および ESP と同等以上の認証・鍵交換・暗号化およびメッセージ認証の仕組みを用いている。	VPN マニュアル「2.1 VPN 通信プロトコル」、「12.4 PacketiX VPN プロトコル仕様」 FIPS 197
T12	ARP 詐称（IP アドレス詐称）	まさにこの攻撃を防止するためのセキュリティポリシーである『「IP アドレスの重複を禁止」ポリシー』が PacketiX VPN に搭載されている。本ポリシーを有効にすることにより、ARP 詐称（IP アドレス詐称）が禁止される。さらに、アクセスリストにより特定のユーザーまたはコンピュータのみ特定の IP アドレスを使用することが可能になるため、さらに厳密な安全性を実現することができる。	VPN マニュアル「3.5.9 セキュリティポリシー」、「3.5.10 アクセスリストによるパケットフィルタリング」 RFC 826
T13	アクセスの証明	PacketiX VPN には、VPN サーバーにおいて、VPN トンネル内を流れた全パケットをディスクにログ保存することができる機能が標準で付加されている。この機能は、他の VPN 製品 (IPsec など) には搭載されているものがほとんどなく、特筆するべき機能である。保存された各パケットが流れた VPN トンネルを確立した時刻や元 IP アドレス、ユーザー名および認証のために使用された X.509 証明書の内容および MD5・SHA-1 ハッシュデータもセキュリティログに記録されるため、これらのデータをアクセスの証明に用いることが可能である。	VPN マニュアル「3.10 ロギングサービス」
T14	TCP SYN パケット挿入	PacketiX VPN は VPN トンネルを TCP 上で構築するため、仮に TCP における SYN パケット挿入が行われた場合でも、それ以降のネゴシエーションを続行することができない (攻撃者が返答パケットを受け取らない場合は認証を開始するために必要な共有情報をサーバー側から受け取れない) ため、この攻撃は行えない。	VPN マニュアル「2.1 VPN 通信プロトコル」、「12.4 PacketiX VPN プロトコル仕様」
T15	TLS RST 偽装	本攻撃は、TCP 上で VPN を使用する場合の弱点である。通常の SSL-VPN ソフトウェア等はこの攻撃に対抗することができず、利用者の立場から見ると、攻撃の影響でセッションが切断されてしまい、結果的に通信妨害が成功してしまうことになる。そこで、	VPN マニュアル「2.1 VPN 通信プロトコル」

類型	脅威	PacketiX VPN においてこの脅威に対応することができるかどうか	左記事実を証する根拠文書
		PacketiX VPN では VPN トンネルを構成する IPsec における IKE および ESP と同等以上の認証・鍵交換・暗号化およびメッセージ認証の仕組みを用いている TCP コネクションが切断攻撃を受けにくいようにするため、常時複数本のコネクション (最大 32 本まで) を並列で確立するほか、仮に攻撃を受けてコネクションが切断された場合を含めて何らかの原因で切断された場合は、直ちに当該切断によって発生した本数減少分のコネクションを新たに確立することで、ユーザーに対しては全く影響を出すことがないように技術上の工夫をしている。この機能は十分検証されており、優れた品質を持つ。したがって、TLS RST 偽装によるセッション切断攻撃に対抗することが可能である。	
T16	シーケンス番号推測攻撃	PacketiX VPN は IPsec における IKE および ESP と同等以上の認証・鍵交換・暗号化およびメッセージ認証の仕組みを用いており、この通信トンネルを TCP 上で使用しているため、仮に TCP におけるシーケンス番号推測攻撃が行われた場合でも、ネゴシエーションを続行したり、特定の VPN トンネルをハイジャックしたりすることができないため、この攻撃は行えない。	VPN マニュアル「2.1 VPN 通信プロトコル」、「12.4 PacketiX VPN プロトコル仕様」
T17	MAC チェック未使用	PacketiX VPN によって一旦確立された VPN トンネル内の通信は IPsec で一般的に使用されている MAC (メッセージ認証・デジタル署名) のためのアルゴリズムである SHA-1 を用いて、攻撃者による差分攻撃等のメッセージ変更攻撃を防止している。	VPN マニュアル「2.1 VPN 通信プロトコル」、「12.4 PacketiX VPN プロトコル仕様」 FIPS PUB 180-1
T18	ホスト to ホスト SA	PacketiX VPN の VPN クライアントソフトウェア機能 (仮想 LAN カード機能) はカーネルモードで動作し、ユーザーモードアプリケーションとの間の通信は特定の TCP や UDP によるポートを用いた通信ではなく、ユーザーモードとカーネルモード間で利用できるユーザーからは一般的に制御不能な通信チャネル (IRP) を用いて内部的に通信を行う。そのため、攻撃者が対象ホストを物理的に利用することができる場合であっても、本攻撃を仕掛けることは、通常は不可能である。もし攻撃者がカーネルモードおよびシステム権限で動作するプログラムを強制的に書き換えることができる権限と技術的能力を持っていればこの限りではないが、それは他の VPN ソフトウェア (IPsec 等) でも全く同様	"SoftEther VPN の内部構造", 情報処理学会第 17 回コンピュータシステムシンポジウム論文集

類型	脅威	PacketiX VPN においてこの脅威に対応することができるかどうか	左記事実を証する根拠文書
		のことである。	
T19	ウィルス混入後の転送	VPN については無関係 (この脅威はサーバーに関するものである)。	
T20	情報の破壊・書換え	VPN については無関係 (この脅威はサーバーに関するものである)。	
T21	メッセージ盗聴後再送	これは一般的に「Reply 攻撃」と呼ばれるものである。PacketiX VPN は VPN トンネルの確立時に IPsec における IKE と同等の仕組みによって毎回異なる鍵およびセッション ID を作成するほか、一旦確立された VPN トンネル内の通信は IPsec で一般的に使用されている MAC (メッセージ認証・デジタル署名) のためのアルゴリズムである SHA-1 を用いて、攻撃者による差分攻撃等のメッセージ変更攻撃を防止しているため、Reply 攻撃は不能である。	PacketiX VPN プロトコル仕様」 FIPS PUB 180-1
T22	自動発呼による再送	本脅威は ISDN に関するものであり VPN については無関係。	
T23	TCP SYN フラッド攻撃	PacketiX VPN Server 2.0 における設定ファイルの「ServerConfiguration」ノード内の「DisableDosProction」が「false」に設定されている場合 (デフォルト) はこの攻撃を防止することができる。	PacketiX VPN マニュアル「3.3.12 障害回復」における「DoS 攻撃からの自動防衛」
T24	DDoS	本来、DDoS 攻撃を受けた場合は、IPsec (IKE) を用いる場合、その他の VPN ソフトウェアを用いる場合など、いかなる場合であっても、根本的な脅威への対処方法は現時点では発明されておらず、これは PacketiX VPN についても同様である。しかしながら、PacketiX VPN においては、「IP アクセス制御リスト」機能が付属しており、VPN 接続を受け付ける処理を開始する以前に TCP コネクションが VPN サーバーに接続してきた段階で接続元の IP アドレスを判別しアクセス制御を行うことが可能である。したがって、あらかじめ許可された IP アドレス以外からの攻撃はこの時点で拒絶され、VPN コネクションを確立するためのネゴシエーションフェーズにすら攻撃者はたどり着くことができない。	VPN マニュアル「3.5.11 IP アクセス制御リストによる接続元の限定」
T25	災害・物理的破壊	PacketiX VPN を搭載したネットワーク機器に倒壊防止対策等の保護措置を施すことによって当然に対応可能である。	
T26	不正な用法	VPN については無関係 (この脅威は Web サーバーに関するものである)。	
T27	不適切な用法	VPN については無関係 (この脅威はメールサーバーに関するものである)。	

類型	脅威	PacketiX VPN においてこの脅威に対応することができるかどうか	左記事実を証する根拠文書
T28	なりすまし	PacketiX VPN においては、認証方法は「パスワードによるユーザー認証」と X.509 証明書および RSA 秘密鍵を用いた「PKI によるユーザー認証」の 2 種類に対応しており、他の VPN (IPsec など) と同様に、適切なアクセス管理設定を行っている場合は、なりすましの被害に遭わない。	VPN マニュアル「2.2 ユーザー認証」
T29	サービス中断による不正処理	VPN については無関係 (この脅威は各種サーバー等通信アプリケーションに関するものである)。	
T30	改ざん	PacketiX VPN によって一旦確立された VPN トンネル内の通信は IPsec で一般的に使用されている MAC (メッセージ認証・デジタル署名) のためのアルゴリズムである SHA-1 を用いて、攻撃者による改ざんを防止している。	VPN マニュアル「2.1 VPN 通信プロトコル」、「12.4 PacketiX VPN プロトコル仕様」 FIPS PUB 180-1
T31	過失・盗難・紛失	他の VPN (IPsec 等) と同様に、適切な管理を行うことで防止できる。	