3.3 PKI の利用

事前共有鍵の代わりに公開鍵証明書を利用して VPN 接続を行うことも可能です。

証明書には情報として有効期限や登録されている情報等が機関より正しいものと署名を受けたものとなるので、これらの情報を元に VPN 接続が行われることになりより安全な暗号 化通信の環境を実現可能となります。

PKIの利用に際しては証明書を発行する機関である CA(認証局)が必要になります。公的 (パブリック)にサービスとして利用できるものからプライベート目的で自社内で構築、 利用されるものまで多種ありますが目的や環境等に従って適切なものを選択してください。 ここではプライベート CA の場合について解説を行いますが発行される証明書の形式や設 定方法については概ね同じとなります。

●Secure VPN Client の設定

基本的な流れとしては基礎編で行った設定をベースに認証鍵を事前共有鍵から証明書へと 置き換えるだけです。

・ルート CA 証明書のインストール

事前に CA の証明書をファイルの形式で入手しておき、VPN Client がインストールされて いる端末のデスクトップ等に置いておきます。

証明書ファイル(dit-privateCA4.crt を開いた時)

御書 【	2 🗙
全般 詳細 証明のパス	
証明書の情報	_
この CA ルート証明書は信頼されていません。信頼を有効にするには この証明書を信頼されたルート証明機関のストアにインストールしてくだ さい。	
	-
発行先 : dit-privateCA4	
発行者 : dit-privateCA4	
有効期間 2010/04/15 から 2021/04/15	
証明書のインストール() … 発行者のステートメント(S)	
OK	

・タスクマネージャよりポリシーエディタを実行し、ウィンドウを開きます。

🔡 NET-G Secure VPN Client ポリシー エディタ	? 🛛
セキュリティ ポリシー 鍵管理	
ポリシー: 📧 デフォルト 💌	E 🗿 💆
 IPsec 前フィルタ VPN 接続 セキュアな接続 セキュアなネットワーク デフォルト応答 IPsec 後フィルタ すべてのトラフィックを許可 	規則の評価順序
道加(A) 肖明除(B) プロパティ(P) 説明 NET-G Secure VPN Client 2.4.0.2 Windows XP Version 5.1 (Build 2600: Service Pack] [[2世斤(<u>D</u>)] 3)
OK キャンセル	

・鍵管理タブより、信頼された証明書 -> 認証局を選択し右クリックしてインポートを選択します。

🔡 NET-G Secure VPN Client ポリシー エディタ	
セキュリティ ポリシー 鍵管理	
■ 💼 信頼されたポリシー サーバ	
□ ☑ 信頼された証明書	
□ □ □ リモー リストから選択	

・"ファイルを開く"ウィンドウより CA 証明書のファイルを選択します。

ファイルを開く	
ファイルの場所型:	🞯 รี.20トップ 💽 🔗 📂 🖽 -
は 最近使ったファイル で テスクトップ マイドキュメント	 □ マイドキュメント □ マイコンピュータ □ マイネットワーク □ clientp12 □ dit-privateCA4.crt
ער דאר דאר דאר די ארב אר	
ک -CHe¢ ک	ファイル名(N): dit-privateCA4.crt 【駅(①) ファイルの種類(T): All certificates (*.cer; *.crt; *.pem; *.pfx; *.p12; *.p7t) キャンセル ご読み取り専用ファイルとして開く(P)

・以下のようなウィンドウが表示されますので、"はい"を選択します。

証明書を	受け入れ 🥐 🔀
Ť	信頼された認証局に証明書を追加してもよろしいですか?
	証明書のフィンガープリント: 5179 35f2 1e62 80de 9b55 7cc2 b9c6 ac80 2df6 14cd
	表示(V). はい いいえ

・下記のように認証局の項目の中に新しく CA 証明書が追加されますので、適用で反映させます。

🔡 NET-G Secure VPN Client ポリシー エディタ	? 🗙
セキュリティ ポリシー 鍵管理	
 □ ▼ 信頼された証明書 □ ▲ 認証局 □ ▼ 認証局 	

・ついで同じウィンドウの下の方の自分の鍵を選択し、右クリックでインポートを選びま す。

🔡 NET-G Secure VPN Client ポリシー エディタ	
セキュリティ ポリシー 鍵管理	_
・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	
OK キャンセル 適用	

・事前に発行、入手しておいた自身の証明書(PKCS#12形式)を選びます。

ファイルを開く	? 🔀
ファイルの場所型:	デスクトップ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ マ
していたいです。 最近使ったファイル デスクトップ デスクトップ	 □ マイドキュメント □ マイコンピュータ □ マイネットワーク □ clientp12 □ dit-privateCA4.crt
₹1 ⊒)°Ľ1-9	ファイル名(N): client.p12
የ1 ሐ୬ዮፓーク	ファイルの種類(①: All certificates (*.cer; *.crt; *.pem; *.pfx; *.p12; *.p7と ¥ャンセル □ 読み取り専用ファイルとして開く(®)

・パスワードが設定されている場合はパスワードを入力します。

パスワードを入力	×
PKCS#12 ファイルを解読するパスワードを入力してください。	

OK キャンセル	

・確認が求められるので、"はい"を選択します。



・適用を選択して反映させます。

📲 NET-G Secure VPN Client ポリシー エディタ	? 🗙
セキュリティ ポリシー 鍵管理	
 winxp リストから選択 追加 リモートホスト ディレクトリ サービス ディレクトリ サービス ディレクトリ ホスト キー 加 ジェホスト キー 通加 ご加 	
<u>追加(D)</u> 削除(R) ブロパティ(P) 表示(V)	
項目を選択してください。	
OK キャンセル 適用	

・後は定義してある VPN 接続の設定を開き、認証鍵としてインポートした CA の証明書を 選択して Secure VPN Client の方の設定は終了となります。

規則のフロ	パティ	? 🔀
全般	羊糸田	
IJ£−ŀ:	エンドポイント —	
	ゲートウェイ IP アドレス:	10.0.220
-T	リモート ネットワーク:	lan 🗸 🗔
IPsec /	IKE 候補	
?	認証鍵	dit-privateca4 証明書
0	候補テンプレート:	normal 💌
		設定

●SSG の設定

Secure VPN Client と同じようにまずは CA 証明書のインポートを行います。

・WebUI にログイン後、左欄のメニューの Objects から Certificates を選択します。

🖉 ssg5-isdn: Juniper-Scree	enOS 6.1.0r7	.0 - Windows Ir	nternet Explorer						
C C v Intp://10.00220/nswebuihtml					🖌 🗟 🐓 🗙 🍺 Live Search			P •	
ファイル(E) 編集(E) 表示(<u>V</u>)	お気に入り(<u>A</u>)	ツール① ヘルプ	(H)						
🚖 お気に入り 🍰 💋 おすすめ	ንታイト 🔹 🧧 Ho	tMail の無料サービス	🕻 🙋 Web スライス ギャラリー 🔹						
ssg5-isdn:Juniper-ScreenOS	6.1.0r7.0					📩 • 🖻 ·	🖃 🖶 • 🕂 -	ジ(P)・ セーフティ(S)・	უ−ル©▼ 🕢 🎽
	Objects	> Certificates						ssg5-isd	in ?
	Load	💿 Cert 🔘 CR	L File:	参照	Load				
	Show	Local 💙	Default Cert Validation	n Settings					New
E E NETWORKS			(_
SSG5-ISDN		Issuer	Friendly Name	Туре	Serial#	Expired	Status	Configure	
– Home				No	entry available				
Configuration									
Security									
 Objects 									
Users IP Pools									
Certificates									
 Reports Wizards 									
telp									
- Logout									
Toggle Menu									
							🔞 🌏 インターネッ	F 🧃	+ 🔍 100% + 🛒

・ページ上段の"参照"を選択し、CA の証明書ファイルを指定して、Load ボタンでインポートを行います。

Load	💿 Cert 🔘 CRL	File: C:\Documents and Set 逐照 [Load
Show	Local 💌	Default Cert Validation Settings	

・Showの項目にて CAを選択して表示させると下記のよう追加されているのが分かります。

Issuer	Friendly Name	Туре	Serial#	Expired	Status	Configure
Class 3 Public Primary Certificatio <u>Server Settings</u>	5	CA	70bae41d10d92934b638ca7b03ccbabf	08-01-2028 23:59	Active	<u>Detail,Remove</u>
dit-privateCA4 Server Settings	10	CA	00028b71	04-15-2021 08:04	Active	<u>Detail,Remove</u>
Secure Server Certification Authori <u>Server Settings</u>	2	CA	02ad667e4e45fe5e576f3c98195eddc0	01-07-2010 23:59	Active	<u>Detail</u>
Class 3 Public Primary Certificatio <u>Server Settings</u>	7	СА	75337d9ab0e1233bae2d7de4469162d4	01-18-2015 23:59	Active	<u>Detail,Remove</u>

追加された CA (ここでは dit-privateCA4)の Server Settings を選択し、CRL 確認を無効 にします。証明書の失効確認をきちんと行う場合は CRL のままとし、関連するパラメータ も正しく設定するようにしてください。

CA Server Settings		
X509 Certificate Path Validation Level	O Full	 Partial
Certificate Revocation Check Settings		
Check Method	○ CRL ○ C	OCSP O None

OK で終了します。

・SSG では PKCS#12 形式の証明書インポートができないので、新しくリクエストファイ ルを作成します。

・Objects -> Certificates ページの右上の New を選択します。

Load	◎ Cert ○ CRL File: 参照 Load								
Show	r Local 🕶 Default Cert Validation Settings								
	Issuer Friendly Name Type Serial# Expired Status Configure								
	No entry available								

・環境に応じて値(ここでは IP Address)を入力し、下欄の Generate ボタンをクリック します。

Certificate Subject Information	
Name:	test-ssg1
Phone:	
Unit/Department:	
Organization:	dit
County/Locality:	JP
State:	
Country:	
E-mail:	
IP Address:	10.0.220
FQDN:	

・しばらくした後、以下のような画面になったら、"Save To File"でデスクトップにファイルとして保存します。

ファイルのダウンロー	ㅋ ㅋ ㅋ ㅋ ㅋ ㅋ ㅋ ㅋ ㅋ ㅋ ㅋ ㅋ ㅋ ㅋ ㅋ ㅋ ㅋ ㅋ ㅋ
このファイルを開く	か、または保存しますか?
愛 発	名前: _pkcs10.txt 種類: テキスト文書 信元: 10.0.0.220
	開(Q) 保存(S) キャンセル
インター を起こす 存したり	ネットのファイルは役に立ちますが、ファイルによってはコンピューターに問題 ものもあります。発信元が信頼できない場合は、このファイルを開いたり保 しないでください。 <u>危険性の説明</u>

SSG の画面はそのままでも一度閉じても問題ありません。保存したファイルを認証局の管理者に渡し証明書を発行してもらい、再度証明書のファイルをもらいデスクトップ等に同じく保存しておきます。

・Objects -> Certificates を選択すると下記のようになっています。

Load ④ Cert 〇 CRL File: 参照 Load									
Show Local V Default Cert Validation Settings									
	Issuer Friendly Name Type Serial# Expired Status Configure						Configure		
	-	-	LOCAL	000000000000000000000000000000000000000	-	Key Pair	<u>Detail,Remove</u> Submit Request		

・上段の File から保存した証明書ファイルを参照で選択し、Load でインポートすると下記 のように変わります。Show 項目が Local となっている箇所に SSG 自身の証明書が、CA となっている箇所で CA の証明書が確認できます。

Load ④ Cert 〇 CRL File: 参照 Load								
Show Local Default Cert Validation Settings								
Issuer	Friendly Name	Туре	Serial#	Expired	Status	Configure		
	12	LOCAL	00024612	08-26-2010 05:52	Activo	Datail Remove		

・以上で証明書ファイルのインポートは終わりました。

・VPNs -> AutoKey Advanced -> Gateway から該当するフェーズ1設定を Edit で開き、 Advanced 項目から下記の証明書を指定する箇所で SSG 自身の証明書と CA 証明書を指定 します。

Always Send	
Preferred Certificate(optional)	
Local Cert	CN=test-ssg1,CN=ssg5-isdn.,CN=rsa-key,CN=016909 💌
Peer CA	CN=dit-privateCA4,O=dit,C=JP
Peer Type	X509-SIG V
Use Distinguished Name for Peer ID	

また、セキュリティレベルにて暗号の設定は rsa-か dsa-で始まるものを選択します。

Security Level	
Predefined	🖸 🔿 Standard 🔿 Compatible 🔿 Basic
User Defined	Oustom
	Phase 1 Proposal
	pre-g2-aes128-sha 💌 🛛 rsa-g2-aes128-sha 💌
	None None

さらに、Objects -> Users からクライアント証明書とユーザを結び付ける設定を行います。 Local Groups から該当するユーザを一旦外した後で、ユーザを Edit で選択します。

	Auth	th/IKE/XAuth/L2TP User	
User Name Status	testuser Enable	O Disable	
 IKE User Simple Identity Use Distinguishe 	d Name For ID	Number of Multiple Logins with Same ID 1	
CN OU	DIT-PC		
Organization	dit		
State			
Country E-mail	JP		
Container			

ここで入力を行うのはクライアントの証明書の内容です。

参考: Internet Explore で証明書の中身を開いた時

証明書	?	K
全般 詳細 証明のパス		_
表示(<u>S</u>): 〈すべて〉	*	
フィールド	値	
■ バージョン	V3	
ロンリアル番号 「「「「署名アルゴリズム」	u2 bc 38 sha1RSA	
至 発行者	dit-privateCA4, dit, JP	
	2010年4月20日 11:08:24 2010年7月19日 11:38:24	
📛 サブジェクト	DIT-PC, dit, JP 💌	
CN = DIT-PC		
O = dit C = JP		
	プロパティの編集(E)) ファイルにコピー(C)	
	ОК	ו

・以上の設定を全て行い、Secure VPN Client から VPN 接続を行うと証明書の内容に基づいて接続が行われます。下記は証明書ベースで接続した場合の SSG のログになります。

Date / Time	Level	Description
2010-05-28 15:05:58	info	IKE 10.0.0.200 Phase 2 msg ID 7672a24c: Completed negotiations with SPI 5b6460b3, tunnel ID 32801, and lifetime 3600 seconds/409600 KB.
2010-05-28 15:05:57	info	IKE 10.0.0.200 Phase 2 msg ID 7672a24c: Responded to the peer's first message.
2010-05-28 15:05:57	info	IKE 10.0.0.200 Phase 1: Completed Aggressive mode negotiations with a 28800-second lifetime.
2010-05-28 15:05:57	info	IKE 10.0.0.200 Phase 1: Completed for user testuser.
2010-05-28 15:05:57	notif	PKI: No revocation check, per config, for cert with subject name CN=DIT-PC,O=dit,C=JP,.
2010-05-28 15:05:57	info	IKE<10.0.0200> Phase 1: IKE responder has detected NAT in front of the remote device.
2010-05-28 15:05:57	info	IKE 10.0.0.200 Phase 1: Responder starts AGGRESSIVE mode negotiations.
2010-05-28 15:05:49	notif	All logged events or alarms were cleared by admin netscreen