

FutureNet XR Series ⇔ *DOVPN*

接続設定ガイド

Ver 1.0.0

センチュリー・システムズ株式会社

目次

はじめに	3
改版履歴	4
1. 基本設定例	5
1-1. 構成例	5
1-2. 設定例	6
1-2-1. センタールータ (XR)	6
1-2-2. VPNクライアント (携帯端末)	11
2. センター経由での IPsec 通信設定例	18
2-1. 構成例	18
2-2. 設定例	19
2-2-1. センタールータ (XR_A)	19
2-2-2. 拠点ルータ (XR_B)	23
2-2-3. VPNクライアント (携帯端末)	25
3. サポートデスクへのお問い合わせ	31
3-1. サポートデスクへのお問い合わせに関して	31
3-2. サポートデスクのご利用に関して	31

はじめに

- FutureNet はセンチュリー・システムズ株式会社の登録商標です。
- DOVPN は日立ビジネスソリューション株式会社の日本における登録商標です。
- Windows は、米国マイクロソフト社の米国およびその他の国における登録商標です。
- 本書に記載されている会社名、製品名は、各社の商標および登録商標です。
- DOVPN のインストール方法および詳細な操作方法につきましては、DOVPN「取扱説明書」をご覧ください。
- 本ガイドは、以下の FutureNet XR 製品に対応しております。
 - ・ XR-510/C
 - ・ XR-540/C
 - ・ XR-730/C
 - ・ XR-1100 シリーズ
- 本書の内容の一部または全部を無断で転載することを禁止しています。
- 本書の内容については、将来予告なしに変更することがあります。
- 本書の内容については万全を期しておりますが、ご不審な点や誤り、記載漏れ等お気づきの点がありましたらお手数ですが、ご一報下さいますようお願い致します。
- 本書は XR-510/C Ver3.5.0, DOVPN は Ver2.1β をベースに作成しております。IPsec および IPsec KeepAlive において、ご使用されている製品およびファームウェアのバージョンによっては、一部機能および設定画面が異なっている場合もありますので、その場合は各製品のユーザーズガイドを参考に、適宜読みかえてご参照および設定を行って下さい。
- 本書を利用し運用した結果発生した問題に関しましては、一切責任を負いかねますのでご了承下さい。

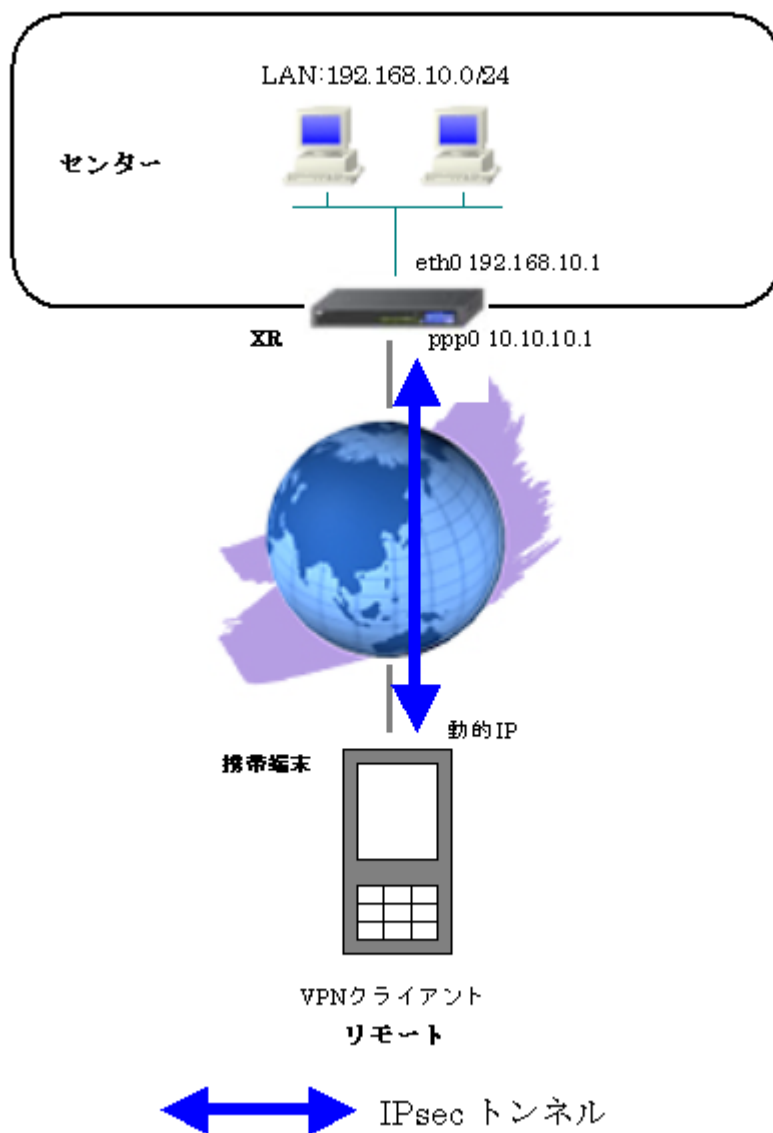
改版履歴

Version	更新内容
1.0.0	初版

1. 基本設定例

携帯端末にインストールして使用する VPN クライアント「DOVPN」を利用することにより、外出先などのリモートからも IPsec によるインターネット VPN が利用可能です。この設定例では、携帯端末でのセンター LAN 側へのリモートアクセスを実現しています。

1-1. 構成例



1-2. 設定例

1-2-1. センタールータ (XR)

ポイント

VPN クライアントをインストールした携帯端末と IPsec 接続するための設定を行います。

VPN クライアントをインストールした携帯端末は動的 IP アドレスを取得しているため、IKE モードとしてアグレッシブモードを使用しています。

<<インターフェース設定>>

[Ethernet0 の設定]

<input checked="" type="radio"/> 固定アドレスで使用	
IP アドレス	192.168.10.1
ネットマスク	255.255.255.0
MTU	1500

Ethernet0 に関する設定をします。

※IP アドレスの設定を変更した場合、その設定した IP アドレスが即反映されます。

[Ethernet1 の設定]

<input checked="" type="radio"/> 固定アドレスで使用	
IP アドレス	0
ネットマスク	255.255.255.0
MTU	1500

Ethernet1 に関する設定をします。

PPPoE 接続で使用するため、IP アドレスに「0」を設定しています。

<<PPP/PPPoE 設定>>

[接続先設定 1]

ユーザID	test1@centurysys
パスワード	test1pass

PPPoE 接続で使用するユーザ ID, パスワードを登録します。

[接続設定]

接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> BRI(64K) <input type="radio"/> BRI MP(128K) <input type="radio"/> Leased Line(64K) <input type="radio"/> Leased Line(128K) <input type="radio"/> RS232C
接続形態	<input type="radio"/> 手動接続 <input checked="" type="radio"/> 常時接続 <input type="radio"/> スケジューラ接続
RS232C/BRI接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続
IPマスカレード	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
ステータフルパケット インスペクション	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得
デフォルトルートの設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効

PPPoE 接続するインタフェース、および接続形態を選択します。

※この例では、XR 配下の端末からのルータ経由でのインターネットアクセスも可能になっています。

PPPoE特殊オプション (全回線共通)	<input checked="" type="checkbox"/> 回線接続時に前回のPPPoEセッションのPADTを強制送出 <input checked="" type="checkbox"/> 非接続SessionのIPv4Packet受信時にPADTを強制送出 <input checked="" type="checkbox"/> 非接続SessionのLCP-EchoRequest受信時にPADTを強制送出
-------------------------	--

PPPoE の再接続性を高めるために、PPPoE 特殊オプションを設定しています。

<<フィルタ設定>>

[入力フィルタ]

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート	ICMP type/code	送信元MACアドレス	LOG
ppp0	パケット受信時	許可	udp		500		500			<input type="checkbox"/>
ppp0	パケット受信時	許可	esp							<input type="checkbox"/>

IKE パケット、ESP パケットが破棄されないようにするために「入力フィルタ」で「許可」を設定しています。

＜＜各種サービスの設定＞＞

＜IPsec サーバ＞

[本装置側の設定 1]

インターフェースのIPアドレス	<input type="text" value="10.10.10.1"/>
上位ルータのIPアドレス	<input type="text" value="%ppp0"/>
インターフェースのID	<input type="text"/> (例: @xr.centurysys)

XR の WAN 側インタフェースの IP アドレス、および上位ルータの IP アドレスを設定します。PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMP の設定 1]

IKE/ISAKMP ポリシーのパラメータは以下のとおりです。

設定項目	パラメータ
IKE/ISAKMP ポリシー名	VPN_Client
リモート IP アドレス	0.0.0.0
インタフェースの ID	@dovpn
モード	Aggressive
暗号化アルゴリズム	AES-128
認証アルゴリズム	SHA1
DH グループ	Group2
ライフタイム	3600 (秒)
事前共有鍵 (Pre Shared Key)	ipseckey

IKE/ISAKMPポリシー名	VPN_Client
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	0.0.0.0
上位ルータのIPアドレス	
インターフェースのID	@dovpn (例:@xr.centurysys)
モードの設定	aggressive モード
transformの設定	1番目 group2-aes128-sha1
	2番目 使用しない
	3番目 使用しない
	4番目 使用しない
IKEのライフタイム	3600 秒 (1081~28800秒まで)

VPNクライアントに対するIKE/ISAKMPポリシーを設定します。

XRにおけるIDの設定では”@”を付けますが、DOVPNでは、”@”を付けない形式で設定してください。

DOVPNでも”@”を付けて設定すると接続できません。

鍵の設定	
<input checked="" type="radio"/> PSKを使用する <input type="radio"/> RSAを使用する <small>(X509を使用する場合はRSAに設定してください)</small>	ipseckey

事前共有鍵(PSK)として「ipseckey」を設定しています。

[IPsec ポリシーの設定 1]

使用する
 使用しない
 Responderとして使用する
 On-Demandで使用する

VPN クライアントの IP アドレスが不定のため、「Responder として使用する」を選択します。

設定項目	パラメータ
使用する IKE ポリシー名	VPN_Client (IKE1)
本装置の LAN 側のネットワークアドレス	192.168.10.0/24
相手側の LAN 側のネットワークアドレス	空欄
暗号化アルゴリズム	AES-128
認証アルゴリズム	SHA1
PFS (DH グループ)	使用する (Group2)
ライフタイム	28800 (秒)
DISTANCE	1

使用するIKEポリシー名の選択	VPN_Client (IKE1) ▼
本装置側のLAN側のネットワークアドレス	192.168.10.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	(例:192.168.0.0/24)
IPsecのTransformの選択	aes128-sha1 ▼
PFS	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
DH Groupの選択(PFS使用時に有効)	group2 ▼
SAのライフタイム	28800 秒 (1081~86400秒まで)
DISTANCE	1 (1~255まで)

VPN クライアントに対して IPsec 通信を行う IP アドレスの範囲を設定します。

携帯端末が動的 IP のため、「相手側の LAN 側のネットワークアドレス」について、この項目を“空欄”に設定します。

【IPsec サーバ】

IPsecサーバ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動
----------	--

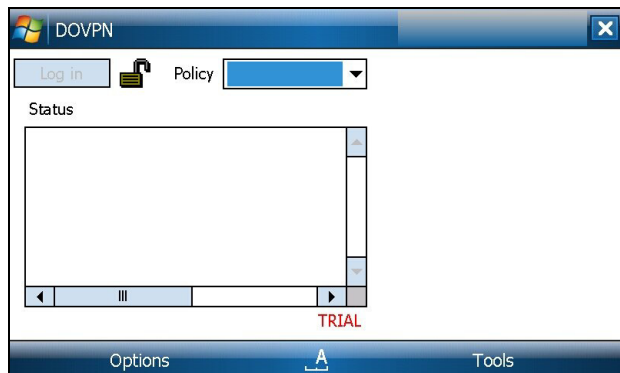
IPsec サーバ機能を起動します。

1-2-2. VPN クライアント（携帯端末）

ポイント

DOVPN をインストールした携帯端末と XR との IPsec 接続になります。
本設定例では、IKE モードとしてアグレッシブモードを使用しています。

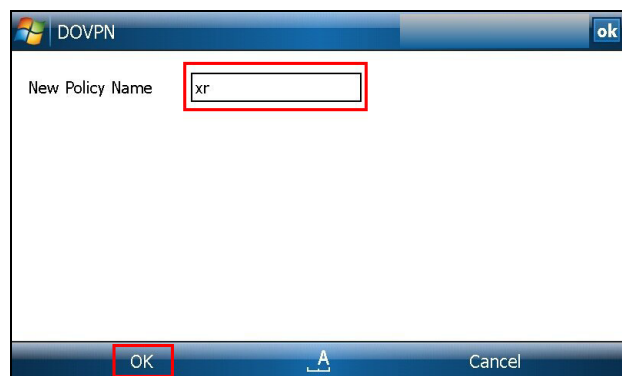
<<ポリシーの新規作成>>



DOVPN を起動すると、上記画面が表示されます。

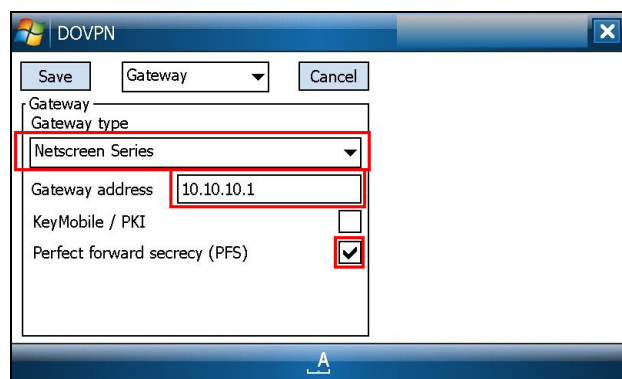


「Option」をタップし、リストから「Policy」→「New」を選択します。



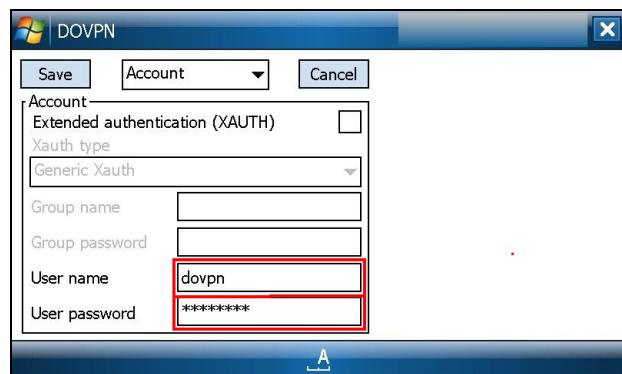
「New Policy Name」の項目でポリシー名を設定します。
本設定例では「xr」と設定しています。
設定後、「OK」をタップします。

<<Gateway の設定>>



「Gateway type」でプルダウンメニューより「NetScreen Series」をタップします。
「Gateway address」の項目には、XRのWAN側IPアドレスを設定します。本設定例では「10.10.10.1」を設定しています。
「KeyMobile/PKI」の項目は、チェックの必要はありません。
「Perfect forward secrecy (PFS)」の項目は、PFSを使用する場合は、チェックします。本設定例ではチェックをしています。

<<Account の設定>>

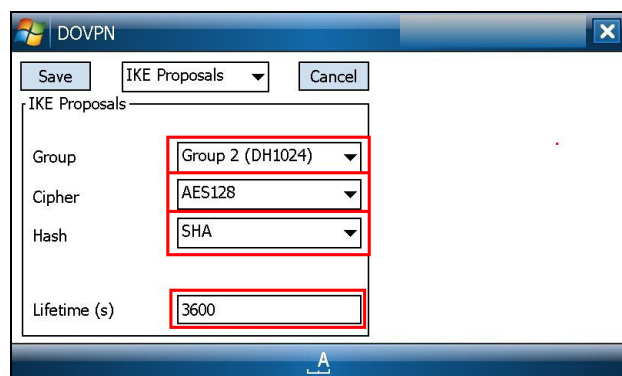


XAUTH は使用しないため、「Extended authentication」の項目は、チェックの必要はありません。

「User name」の項目では、XR の IKE/ISAKMP 設定で設定したインタフェースの ID を設定します。本設定例では、「dovpn」を設定しています。

「User password」の項目では、XR の IKE/ISAKMP 設定で設定した Pre shared key (PSK) を設定します。本設定例では、「ipseckey」を設定しています。

<<IKE Proposals の設定>>



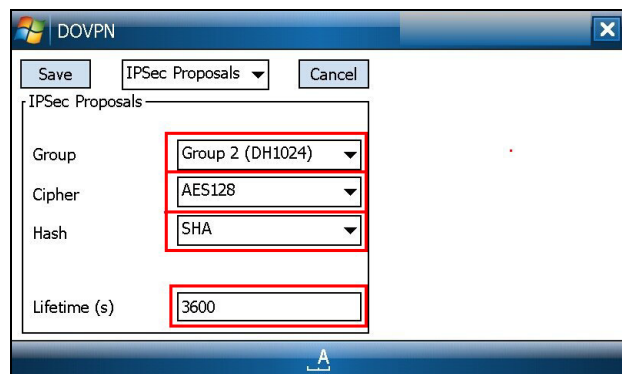
IKE Proposal を設定します。

本設定例では「Group」は「Group2 (DH1024)」、 「Cipher」は「AES128」、 「Hash」は「SHA」を選択しています。

また IKE Lifetime も設定可能です。

本設定例では、「3600 秒」を設定しています。

<<IPSec Proposals の設定>>



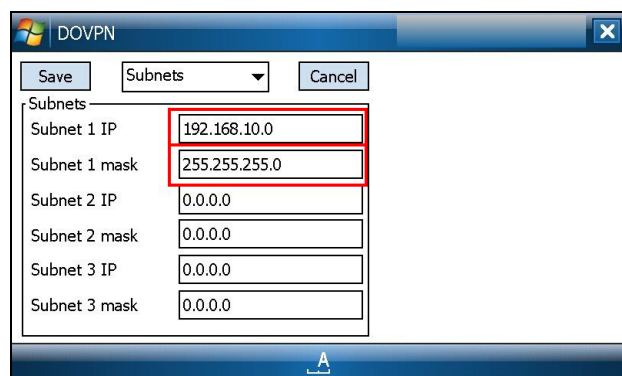
IPSec Proposal を設定します。

本設定例では「Group」は「Group2 (DH1024)」、 「Cipher」は「AES128」、 「Hash」は「SHA」を選択しています。

また IKE Lifetime も設定可能です。

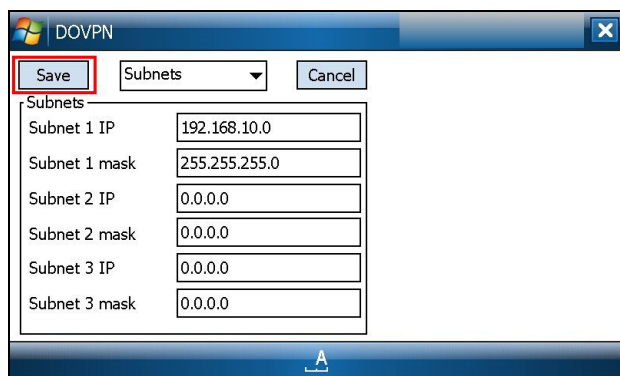
本設定例では、「3600 秒」を設定しています。

<<Subnets の設定>>

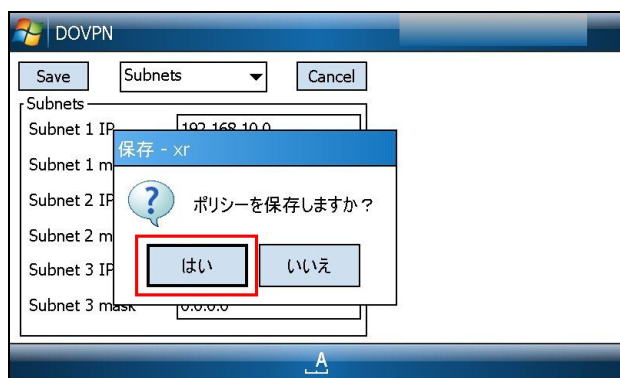


ここでは IPsec 経由でアクセスしたいネットワークを設定します。

本設定例では対向XRのLAN側ネットワークアドレス「192.168.10.0」、サブネットマスク「255.255.255.0」を設定しています。



設定完了後、「Save」をタップします。

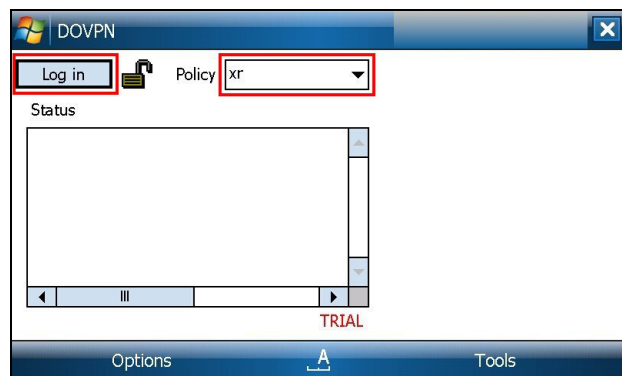


「Save」タップ後、「ポリシーを保存しますか?」と表示されますので、「はい」をタップします。



これで設定完了です。

<<IPsec の接続>>



先ほど作成したポリシー「xr」が選択されている状態で「Log in」をタップすることにより IPsec 接続を開始します。

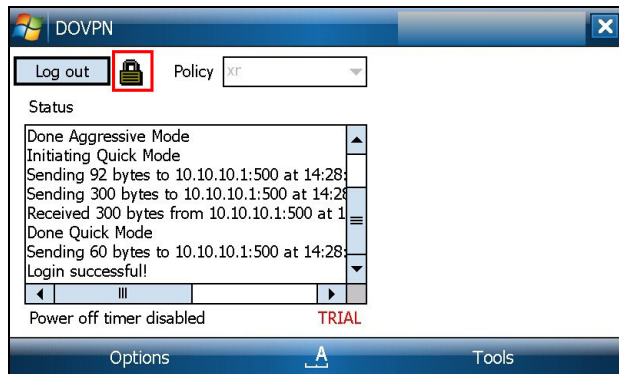
ログイン中（接続完了）の場合、ウインドウが以下のように変わります。



なおログアウト中は以下の表示になります。



また VPN ウィンドウではログイン中の場合、以下のように表示されます。

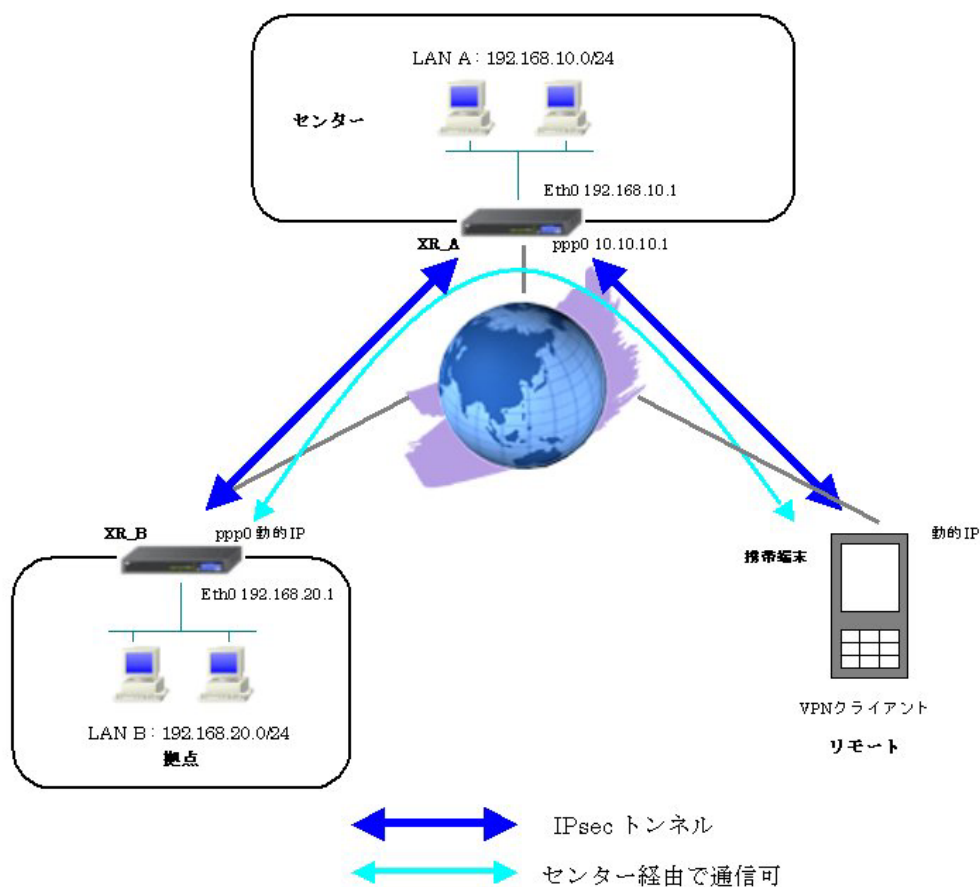


2. センター経由での IPsec 通信設定例

本設定例では、DOVPN のデフォルトルートを中心にセンター側 XR とすることでセンター経由で拠点側 LAN へもアクセス可能とし、インターネットアクセスもセンター側 XR 経由でアクセスします。

また本設定例では、XR に関しましては IPsec 設定に関してのみ記載（センター側のみ DNS サーバ設定あり）しております。その他の設定に関しましては、インターネット VPN 設定例集 IPsec 編の「IPsec を利用したセンター経由インターネット接続例」をご参照下さい。

2-1. 構成例



2-2. 設定例

2-2-1. センタールータ (XR_A)

ポイント

XR_B(拠点)および携帯端末と IPsec 接続するための設定を行います。

XR_B(拠点)および携帯端末は動的 IP のため、IKE モードとしてアグレッシブモードを使用しています。

携帯端末が IPsec 経由で名前解決ができるように、DNS キャッシュ機能を起動しています。

<<各種サービスの設定>>

<IPsec サーバ>

[本装置側の設定 1]

インターフェースのIPアドレス	10.10.10.1
上位ルータのIPアドレス	%ppp0
インターフェースのID	<input type="text"/> (例:@xr.centurysys)

XR の WAN 側インタフェースの IP アドレス、および上位ルータの IP アドレスを設定します。PPP/PPPoE 接続で固定 IP を取得する場合は、「上位ルータの IP アドレス」は「%ppp0」に設定します。

[IKE/ISAKMP の設定 1]

IKE/ISAKMPポリシー名	XR_B
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	0.0.0.0
上位ルータのIPアドレス	<input type="text"/>
インターフェースのID	@ipsec1 (例:@xr.centurysys)
モードの設定	aggressive モード
transformの設定	1番目 group2-aes128-sha1
	2番目 使用しない
	3番目 使用しない
	4番目 使用しない
IKEのライフタイム	3600 秒 (1081~28800秒まで)

XR_B(拠点)に対する IKE/ISAKMP ポリシーを設定します。

鍵の設定	
<input checked="" type="radio"/> PSKを使用する <input type="radio"/> RSAを使用する <small>(X509を使用する場合は RSAに設定してください)</small>	ipseckey1

事前共有鍵(PSK)として「ipseckey1」を設定しています。

[IPsec ポリシーの設定 1]

<input type="radio"/> 使用する <input type="radio"/> 使用しない <input checked="" type="radio"/> Responderとして使用する <input type="radio"/> On-Demandで使用する

XR_B(拠点)の IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	XR_B (IKE1) ▼
本装置側のLAN側のネットワークアドレス	0.0.0.0/0 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (例:192.168.0.0/24)
PH2のTransformの選択	aes128-sha1 ▼
PFS	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
DH Groupの選択(PFS使用時に有効)	group2 ▼
SAのライフタイム	28800 秒 (1081~86400秒まで)
DISTANCE	1 (1~255まで)

XR_B(拠点)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

[IKE/ISAKMP の設定 2]

IKE/ISAKMPポリシー名	VPN_Client
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	0.0.0.0
上位ルータのIPアドレス	
インターフェースのID	@dovpn (例:@xx.centurysys)
モードの設定	aggressive モード
transformの設定	1番目 group2-aes128-sha1
	2番目 使用しない
	3番目 使用しない
	4番目 使用しない
IKEのライフタイム	3600 秒 (1081~28800秒まで)

VPN クライアントに対する IKE/ISAKMP ポリシーを設定します。

XR における ID の設定では”@”を付けますが、DOVPN 側では、”@”を付けない形式で設定してください。DOVPN でも”@”を付けて設定すると接続できません。

鍵の設定	
<input checked="" type="radio"/> PSKを使用する <input type="radio"/> RSAを使用する <small>(X509を使用する場合は RSAに設定してください)</small>	ipseckey2

事前共有鍵(PSK)として「ipseckey2」を設定しています。

[IPsec ポリシーの設定 2]

使用する
 使用しない
 Responderとして使用する
 On-Demandで使用する

VPN クライアントの IP アドレスが不定のため、「Responder として使用する」を選択します。

使用するIKEポリシー名の選択	VPN_Client (IKE2) ▼
本装置側のLAN側のネットワークアドレス	0.0.0.0/0 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	(例:192.168.0.0/24)
PH2のTransFormの選択	aes128-sha1 ▼
FFS	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
DH Groupの選択(FFS使用時に有効)	group2 ▼
SAのライフタイム	28800 秒 (1081~86400秒まで)
DISTANCE	1 (1~255まで)

VPN クライアントに対して IPsec 通信を行う IP アドレスの範囲を設定します。

携帯端末が動的 IP のため、「相手側の LAN 側のネットワークアドレス」について、この項目を“空欄”に設定します。

【IPsec サーバ】

IPsecサーバ
 停止
 起動

IPsec サーバ機能を起動します。

【DNS キャッシュ】

DNSキャッシュ
 停止
 起動

携帯端末が IPsec 経由で名前解決ができるように、DNS キャッシュ機能を起動します。

2-2-2. 拠点ルータ (XR_B)

ポイント

XR_A(センター)に対して IPsec 接続を行います。WAN 側 IP アドレスが動的 IP アドレスであるため、IKE モードとしてアグレッシブモードを使用しています。

<<各種サービスの設定>>

<IPsec サーバ>

[本装置側の設定 1]

インターフェースのIPアドレス	<input type="text" value="%ppp0"/>
上位ルータのIPアドレス	<input type="text"/>
インターフェースのID	<input type="text" value="@ipsec1"/> (例:@xr.centurysys)

PPPoE 接続で WAN 側(ppp0)インタフェースの IP アドレスが不定のため「%ppp0」、インタフェースの ID として「@ipsec1」を設定します。

[IKE/ISAKMP の設定 1]

IKE/ISAKMPポリシー名	<input type="text" value="XR_A"/>
接続する本装置側の設定	本装置側の設定1 ▼
インターフェースのIPアドレス	<input type="text" value="10.10.10.1"/>
上位ルータのIPアドレス	<input type="text"/>
インターフェースのID	<input type="text"/> (例:@xr.centurysys)
モードの設定	aggressive モード ▼
transformの設定	1番目 <input type="text" value="group2-aes128-sha1"/> ▼
	2番目 <input type="text" value="使用しない"/> ▼
	3番目 <input type="text" value="使用しない"/> ▼
	4番目 <input type="text" value="使用しない"/> ▼
IKEのライフタイム	<input type="text" value="3600"/> 秒 (1001~28800秒まで)

XR_A(センター)に対する ISAKMP ポリシーの設定を行います。

鍵の設定	ipseckey1
<input checked="" type="radio"/> PSKを使用する <input type="radio"/> RSAを使用する <small>(X509を使用する場合は RSAに設定してください)</small>	

事前共有鍵(PSK)として「ipseckey1」を設定します。

[IPsec ポリシーの設定 1]

使用する
 使用しない
 Responderとして使用する
 On-Demandで使用する

XR_A(センター)に対して IKE のネゴシエーションを行うため、「使用する」を選択します。

使用するIKEポリシー名の選択	XR_A (IKE1) ▼
本装置側のLAN側のネットワークアドレス	192.168.20.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	0.0.0.0/0 (例:192.168.0.0/24)
PH2のTransformの選択	aes128-sha1 ▼
FFS	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
DH Groupの選択(FFS使用時に有効)	group2 ▼
SAのライフタイム	28800 秒 (1081~86400秒まで)
DISTANCE	1 (1~255まで)

XR_A(センター)に対して IPsec 通信を行う IP アドレスの範囲を設定します。

この例では、IPsec 通信を行う宛先 IP アドレスを「0.0.0.0/0」に設定しています。

[IPsec Keep-Alive 設定]

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作Option 1 <small>※</small>	動作Option 2 <small>※</small>	interface	backup SA
1	<input checked="" type="checkbox"/>	192.168.20.1	192.168.10.1	30	3	60	<input checked="" type="checkbox"/>	<input type="checkbox"/>	ipsec0 ▼	

XR_A(センター)に対する IPsec トンネルの障害を検出するための IPsec KeepAlive を設定します。

【IPsec サーバ】

IPsecサーバ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動
----------	--

IPsec サーバ機能を起動します。

2-2-3. VPN クライアント（携帯端末）

ポイント

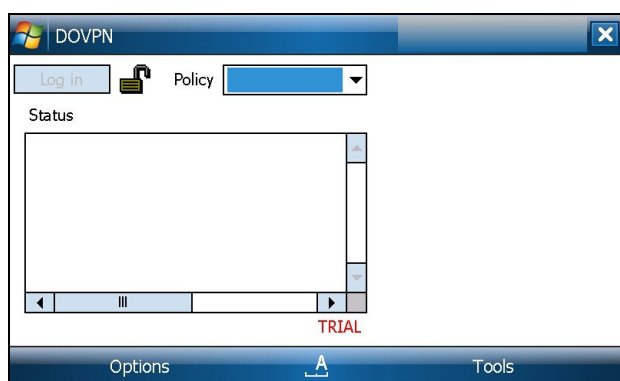
DOVPN をインストールした携帯端末と XR_A(センター)で IPsec 接続を行います。

XR_A(センター)経由で拠点およびインターネット側への通信をするため、Subnets 設定で「0.0.0.0/0」を設定しています。

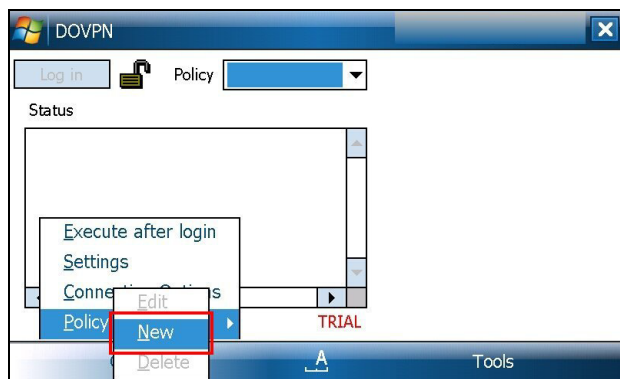
また IPsec 経由での名前解決用に DNS 設定を行っています。

本設定例では、IKE モードとしてアグレッシブモードを使用しています。

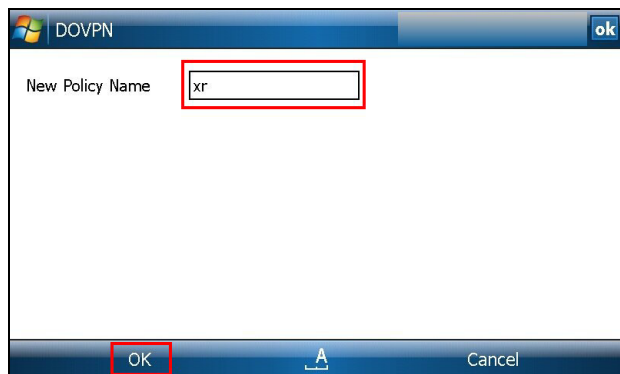
<<ポリシーの新規作成>>



DOVPN を起動すると、上記画面が表示されます。

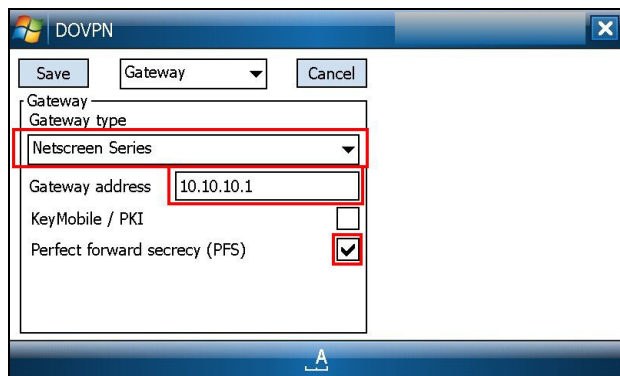


「Option」をタップし、リストから「Policy」->「New」を選択します。



「New Policy Name」の項目でポリシー名を設定します。
ここでは「xr」と設定しています。
設定後、「OK」をタップします。

<<Gateway の設定>>



「Gateway type」でプルダウンメニューより「NetScreen Series」をタップします。
「Gateway address」の項目には、XRのWAN側IPアドレスを設定します。本設定例では「10.10.10.1」を設定しています。
「KeyMobile/PKI」の項目は、チェックの必要はありません。
「Perfect forward secrecy (PFS)」の項目は、PFSを使用する場合は、チェックします。本設定例ではチェックをしています。

<<Account の設定>>

XAUTH は使用しないため、「Extended authentication」の項目は、チェックの必要はありません。

「User name」の項目では、XR の IKE/ISAKMP 設定で設定したインタフェースの ID を設定します。本設定例では、「dovpn」を設定しています。

「User password」の項目では、XR の IKE/ISAKMP 設定で設定した Pre shared key (PSK) を設定します。本設定例では、「ipseckey2」を設定しています。

<<IKE Proposals の設定>>

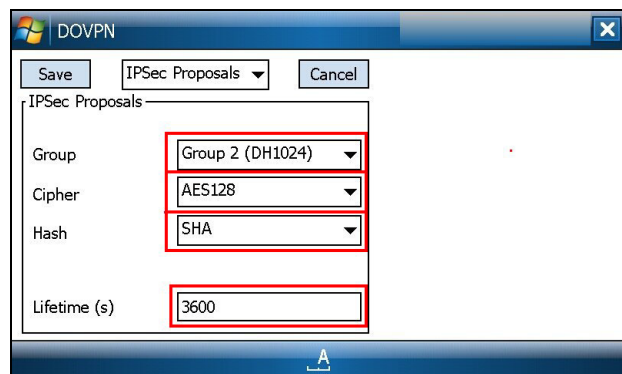
IKE Proposal を設定します。

本設定例では「Group」は「Group2 (DH1024)」、 「Cipher」は「AES128」、 「Hash」は「SHA」を選択しています。

また IKE Lifetime も設定可能です。

本設定例では、「3600」秒を設定しています。

<<IPSec Proposals の設定>>



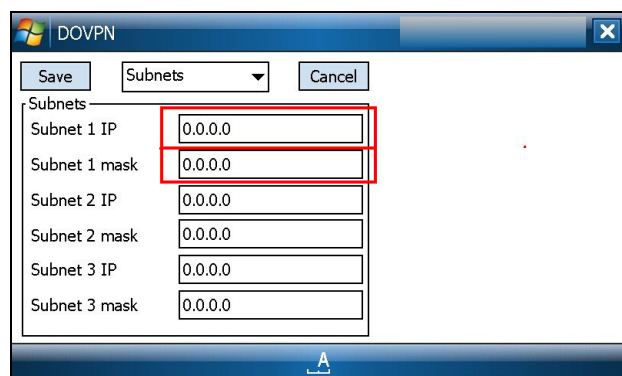
IPSec Proposal を設定します。

本設定例では「Group」は「Group2 (DH1024)」、 「Cipher」は「AES128」、 「Hash」は「SHA」を選択しています。

また IKE Lifetime も設定可能です。

本設定例では、「3600」秒を設定しています。

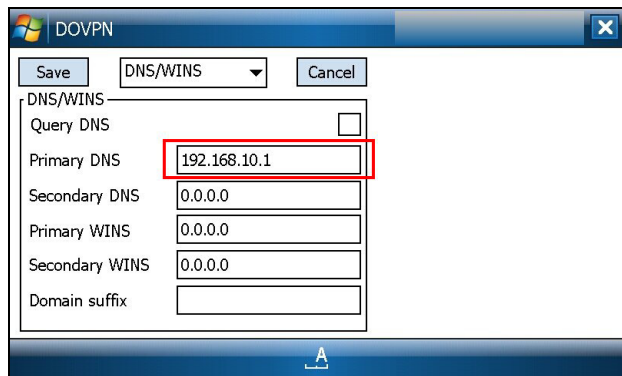
<<Subnets の設定>>



ここでは IPsec 経由でアクセスしたいネットワークを設定します。

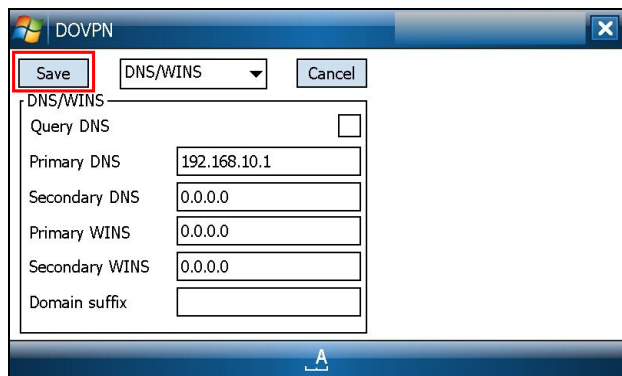
本設定例ではセンター側 LAN, 拠点側 LAN およびインターネットアクセスを IPsec 経由で行いますので、「Subnet 1 IP」 および 「Subnet 1 mask」は「0.0.0.0」と設定します。

<<DNS/WINS の設定>>

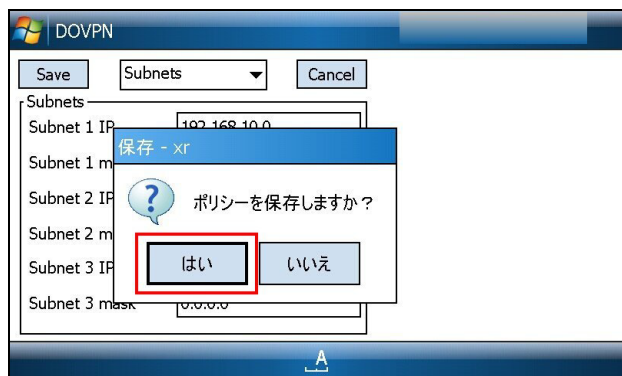


ここでは DNS サーバの設定をします。

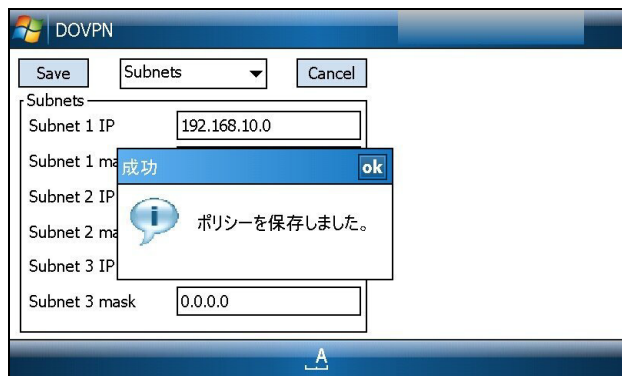
本設定例ではセンター側 XR で DNS 機能を有効にしていますので、Primary DNS サーバの IP アドレスとして「192.168.10.1」を設定しています。



設定完了後、「Save」をタップします。

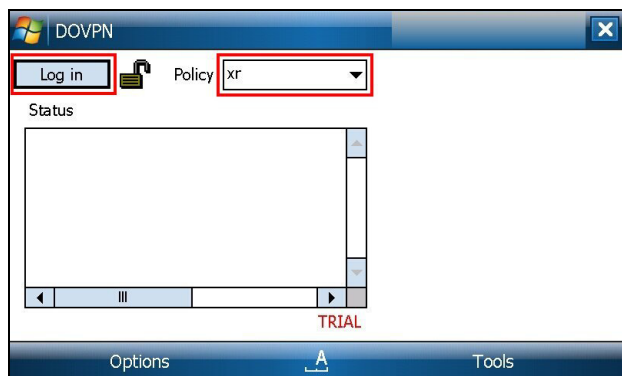


「Save」タップ後、「ポリシーを保存しますか?」と表示されますので、「はい」をタップします。



これで設定完了です。

<<IPsec の接続>>



先ほど作成したポリシー「xr」が選択されている状態で「Log in」をタップすることにより IPsec 接続を開始します。

ログイン中（接続完了）の場合、ウインドウが以下のように変わります。



3. サポートデスクへのお問い合わせ

3-1. サポートデスクへのお問い合わせに関して

XR 製品に関してサポートデスクにお問い合わせ頂く際は、以下の情報をお知らせ頂けると効率よく対応させていただきますので、ご協力をお願い致します。

- ご利用頂いている XR の製品名およびバージョン番号
- ご利用頂いているネットワーク構成
- 不具合の内容および不具合の再現手順（何を行った場合にどのような問題が発生したのかをできるだけ具体的にお知らせ下さい）
- VPN クライアントと接続する、または接続している XR の設定ファイル、ログ、IPsec のステータス情報（取得方法に関しましては、ご利用頂いている製品のユーザーズガイドをご参照下さい）
- DOVPN を XR 製品以外でご利用頂く場合に関しましては、ご購入された代理店および販売店様へお問い合わせ下さい。

3-2. サポートデスクのご利用に関して

電話サポート

電話番号： **0 4 2 2 - 3 7 - 8 9 2 6**

電話での対応は以下の時間帯で行います。

月曜日 ～ 金曜日 10:00 AM - 5:00 PM

ただし、国の定める祝祭日、弊社の定める年末年始は除きます。

電子メールサポート

E-mail： support@centurysys.co.jp

F A X サポート

FAX 番号： **0 4 2 2 - 5 5 - 3 3 7 3**

電子メール、FAX は 毎日 24 時間受け付けております。

ただし、システムのメンテナンスやビルの電源点検のため 停止する場合があります。 その際は弊社ホームページ等にて事前にご連絡いたします。

FutureNet XR Series ⇔ DOVPN 接続設定ガイド

Ver1.0.0

2008年3月

発行 センチュリー・システムズ株式会社

2008 CENTURYSYSTEMS INC. ALL rights reserved.
