2013.08.28 V00.02

ダイナミック IP を使用しているレピータ及びアクセスポイントからの D-STAR 網への接続に対するセキュリティー対策について

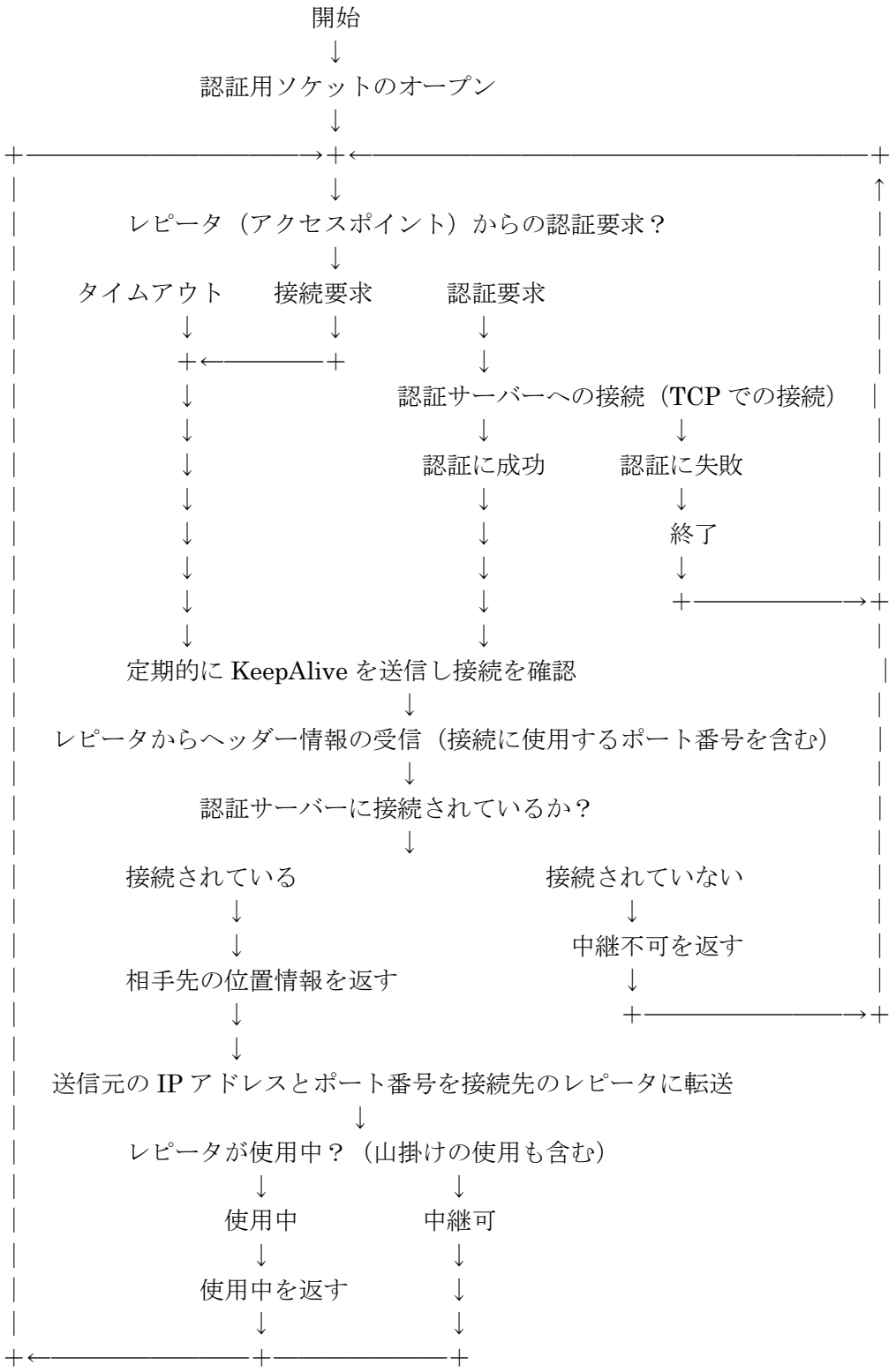
安田　聖　７Ｍ３ＴＪＺ

現在Ｄ－ＳＴＡＲレピータ網へのレピータ及びアクセスポイントの接続に関しは、セキュリティー対策が施されていません。このため、レピータ網への接続に使用されるクライアントによっては正常な通信が阻害され可能性があります。この為、今後レピータやアクセスポイントからの接続を認める場合は、パスワード等の認証方式を導入する必要があります。

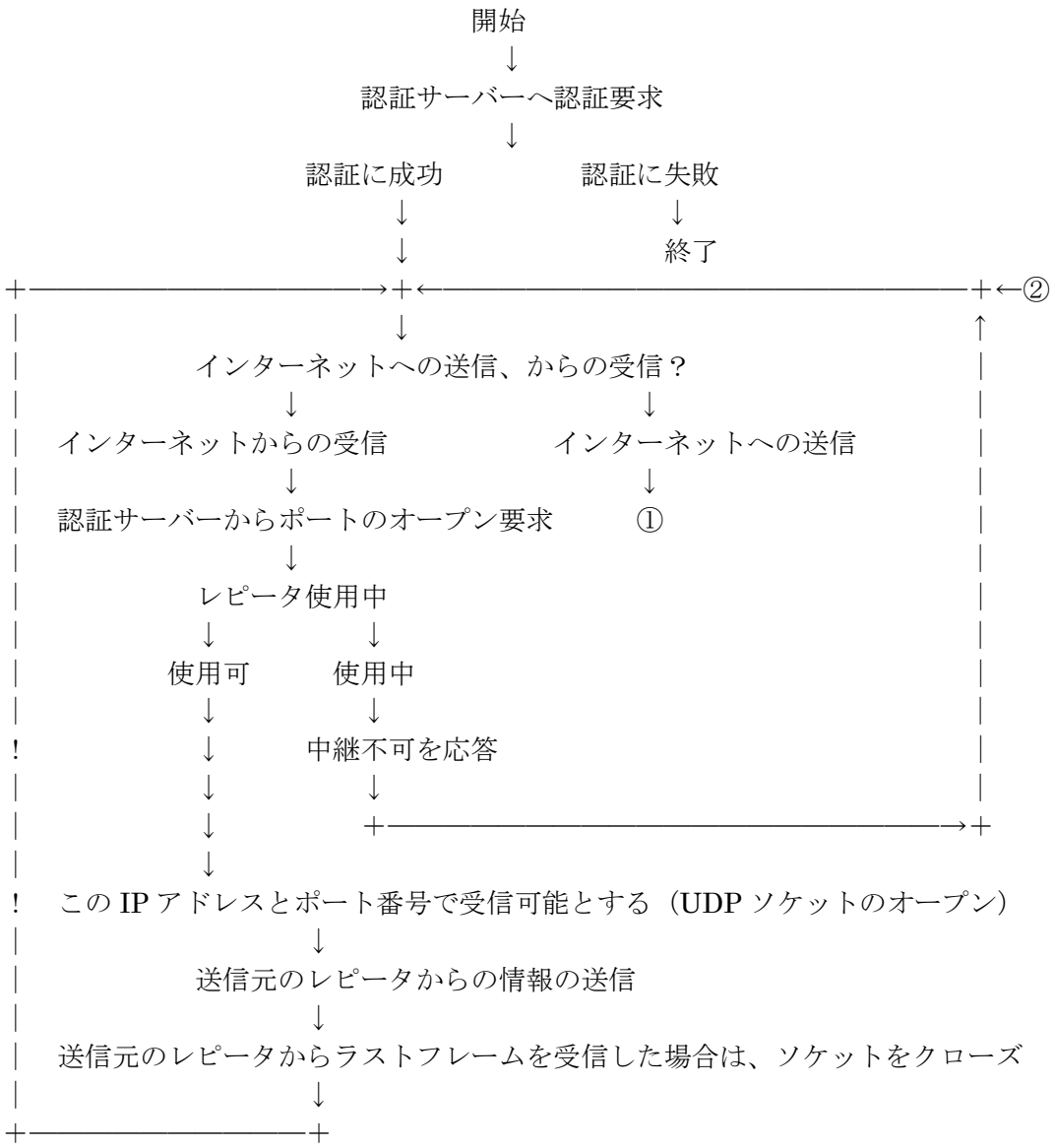
認証サーバーを設置し（複数の設置を可能とする)、アクセスポイントのネットワーク接続時にユーザーＩＤとパスワードでの認証を受け、認証に成功した場合のみネットワークへの接続を認めるとともに、以後レピータ間（Ｐ２Ｐ）の通信に関してはヘッダー情報の送信に先立ち認証サーバー経由で相手のレピータ（もしくはアクセスポイント）に送信元のＩＰアドレスとポート番号を渡し、そのＩＰアドレスとポートに関して通信が終了するまで（ラストフレームを受信するまで）ソケットを開ける方法[1]です。この方法が実現できれば、これまでのようにルーターでポートを開ける必要がなく全てのポートが閉じられているホテル等の移動先からでも交信が可能となります。

[1] 相手の IP アドレスとポート番号でソケットをオープンし、空の送信を一度行えば受信が可能になります。

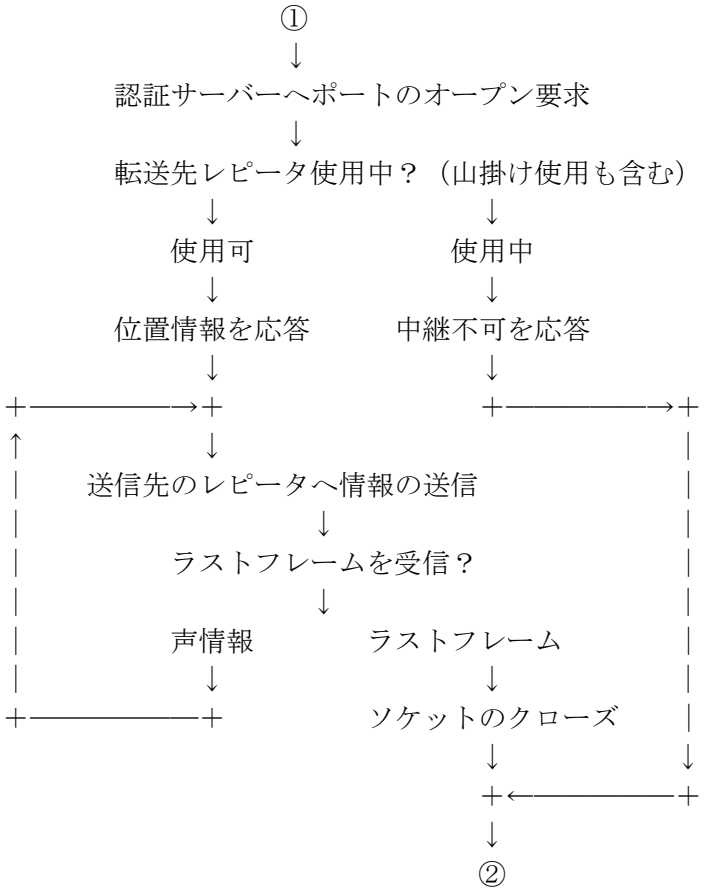
認証サーバーでの処理


開始
認証用ソケットのオープン
レピータ（アクセスポイント）からの認証要求？
タイムアウト
接続要求
認証要求
認証サーバーへの接続（TCP での接続）
認証に成功
認証に失敗
終了
定期的に KeepAlive を送信し接続を確認
レピータからヘッダー情報の受信（接続に使用するポート番号を含む）
認証サーバーに接続されているか？
接続されている
接続されていない
中継不可を返す
相手先の位置情報を返す
送信元の IP アドレスとポート番号を接続先のレピータに転送
レピータが使用中？（山掛けの使用も含む）
使用中
中継可
使用中を返す

レピータでの処理　１／２


開始
認証サーバーへ認証要求
認証に成功
認証に失敗
終了
②
インターネットへの送信、からの受信？
インターネットからの受信
インターネットへの送信
認証サーバーからポートのオープン要求
①
レピータ使用中
使用可
使用中
中継不可を応答
このIPアドレスとポート番号で受信可能とする（UDPソケットのオープン）
送信元のレピータからの情報の送信
送信元のレピータからラストフレームを受信した場合は、ソケットをクローズ

レピータでの処理　２／２


①
認証サーバーへポートのオープン要求
転送先レピータ使用中？（山掛け使用も含む）
使用可
使用中
位置情報を応答
中継不可を応答
送信先のレピータへ情報の送信
ラストフレームを受信？
声情報
ラストフレーム
ソケットのクローズ
②

補足

現在のゲートウエイ用の PC をルーターを使用してインターネットに接続されている場合は、ルーターの一部のポートをオープンにしなければ動作しませんが、ルーターの多くが内側から送信された TCP/UDP パケットに対するお応答は受け取れるように動作します。この機能を利用してレピータ用のシステムは常に認証サーバー経由で接続する方法です。但し、この接続は PTT が押されてから離されるまでの間で、押されるたびにポートをオープンする方法です。認証サーバーと接続がゲートウエイ用のシステムとの間で稼働中常に確立していれば、このソケットを使用してポートのオープンを要求する方法です。最初の認証要求は、ルーター内側からの要求ですので、ルーターでポートのオープンの必要はありません。（この方法が使用できれば、ホテル等の回線も利用可能になります。）

言い換えると勝手口を認証サーバーに繋いだままにし、接続したいレピータに対して認証サーバーを経由して勝手口から入り、玄関を内側から開けてもらう方法です。（接続要求先に対して、送信を試みればルーター等のポートが開きます。）この方法であればポートが閉じられていても接続が可能となり、また認証サーバーにアクセスできなければアクセスできないことになります。このため、セキュリティー対策になります。