第 9 章　経路情報交換における不正利用排除

内容

- RFC3779 の概要
- soBGP の概要とモデル
- S-BGP の概要とモデル

9. 経路情報交換における不正利用排除

本章では、経路交換を行う場合に事故／故意にかかわらず不正な経路情報が混入することによって起こりえるリスクに対しどのようなアプローチがあり、そのアプローチがどのように問題を解決するかを述べる。

構成は、大きく以下の3つに分れている。

- PKI の枠組みを利用して経路情報（IP アドレスブロックと AS 番号）を電子証明書[RFC3280[1]]へ対応するための拡張について
- soBGP を用いた経路交換システムに関して
- S-BGP を用いた経路交換システムに関して

soBGP、S-BGP 両システムとも目的は Origin AS、IP アドレスブロックの検証と AS PATH の検証である。両システムは目的が同じであるが、アプローチ方法が異なる。

soBGP は証明書情報の交換を BGP 経由で行うアプローチを取り、S-BGP は BGP 以外の手段を用いて証明書の交換を行うアプローチをとっている。

[1] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC3280)
http://www.ietf.org/rfc/rfc3280.txt

9.1. RFC3779 の概要

[RFC3779[2]]は、現在 PKI で利用されている X.509v3 証明書[RFC3280]の拡張領域に対して以下に示す 2 種類の情報を定義した RFC である。

- IP アドレス情報
- AS 番号情報

IP アドレス情報用証明書を作成する時には、「アドレスファミリー」「通信方法」と「IP アドレスブロック」もしくは「IP アドレス・プリフィクス」が入り、AS 番号情報用証明書を作成する際には「AS 番号」もしくは「AS 番号ブロック」が入る。

証明書は、IANA/RIR/LIR や「割り振り組織」として認可された権威ある組織が署名する事により、入手した「IP アドレスブロック」や「AS 番号」が正当な手段により取得され、提供された事が検証可能になる。

本 RFC で定義された情報を利用する主な利用例としては、BGP 等の経路制御プロトコルが上げられるが、他組織から経路制御プロトコル経由で渡された「IP アドレスブロック」や「AS 番号」が正当な情報であるかの検証や、IRR に登録されている情報の信憑性の確認する、と言った利用法が考えられる。

9.1.1. IP アドレス情報用拡張の概要

IP アドレス情報を証明書内で認識する為に利用される extnID は「iso(1).identified-organization(3).dod(6).internet(1).security(5).mechanisms(5).pkix(7).id-pe(1).id-pe-ipAddrBlocks(7)」=「1.3.6.1.5.5.7.1.7」で定義済みである。

「IP アドレスブロック」を情報として証明書に入れる場合は 2 つ方法が用意されている。

[2] X.509 Extensions for IP Address and AS Identifiers (RFC3779)
http://www.ietf.org/rfc/rfc3280.txt

一つは「プリフィクス長」を指定する方法、もう一つは IP アドレスブロックを最小アドレスと最大アドレスの範囲を指定する方法である。

- プリフィクス長による指定 ： 10.0.32/20
- 最小アドレスと最大アドレスの範囲を指定： min 10.2.48.0, max 10.2.64.255

図 9-1 に IP アドレスブロック「129.0.68/22」の符号化例を示す。IPv6 アドレスの符号化においても考え方は同様である。

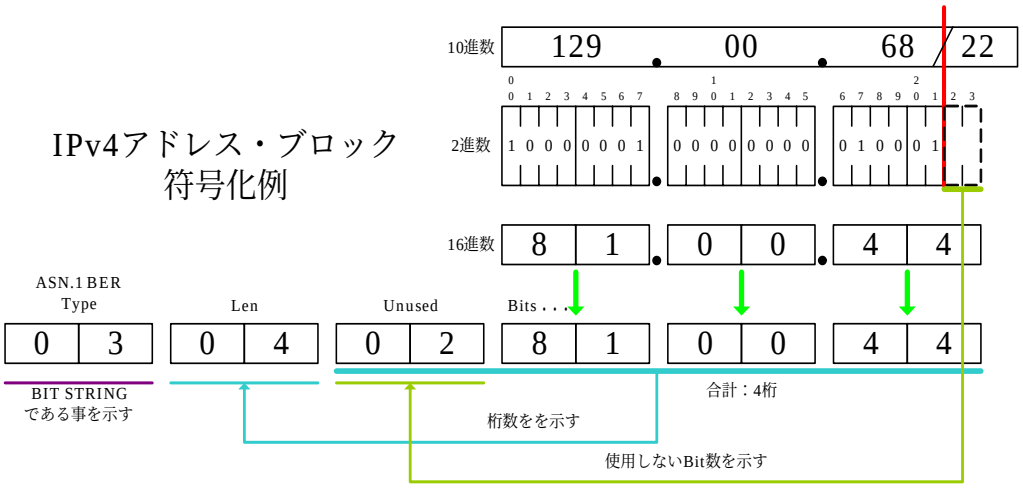


図 9-1　IPv4 アドレスブロック符号化例

その他情報として、「アドレスファミリー　→　IPv4/IPv6」「通信方法　→　Unicast/Multicast」があり、上記「IP アドレスブロック」と合わせて証明書が作成される。

IP アドレスブロック符号化全体例を図 9-2 に示す。

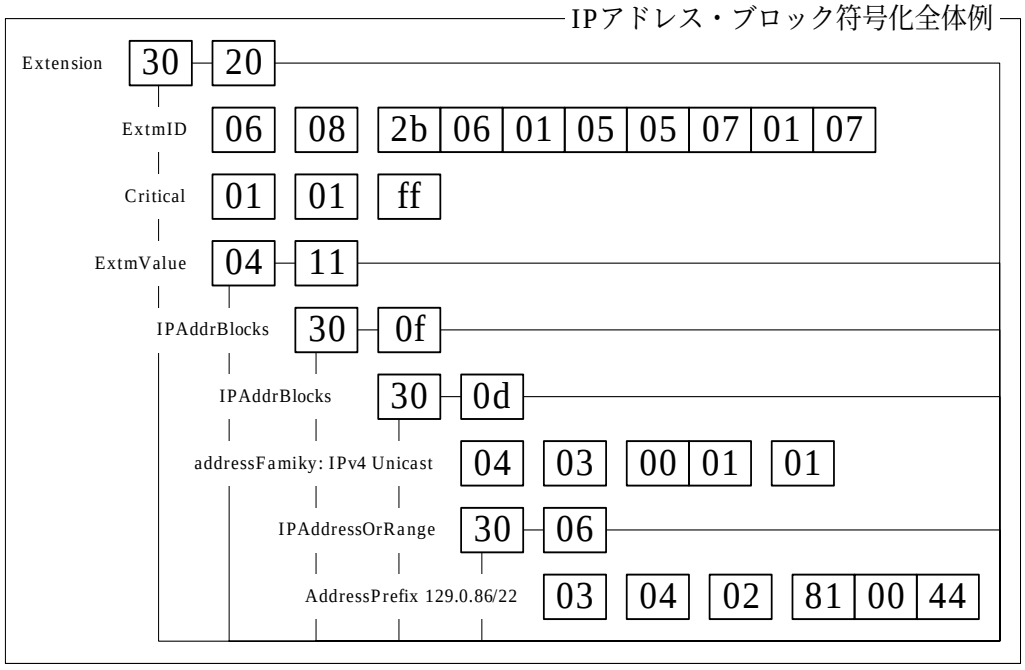


図 9-2　IPv4 アドレスブロック符号化 全体例

9.1.2. AS 番号情報用拡張の概要

AS 番号情報用を証明書内で認識するために利用される extnID は、「iso(1).identified-organization(3).dod(6).internet(1).security(5).mechanisms(5).pkix(7).id-pe(1).id-pe-autonomousSysIds(8)」=「1.3.6.1.5.5.7.1.8」で定義済みである。

「AS 番号」を情報として証明書に入れる場合は 2 つ方法が用意されている。一つは、「AS 番号」を指定する方法、もう一つは AS 番号を最小 AS 番号と最大 AS 番号を範囲で指定する方法である。

- AS 番号による指定 ： 135
- 最小 AS 番号と最大 AS 番号を範囲で指定： min 3000, max 3999

図 9-3 に AS 番号「6434」の符号化例を示し、AS 番号全体例は図 9-4 に示す。

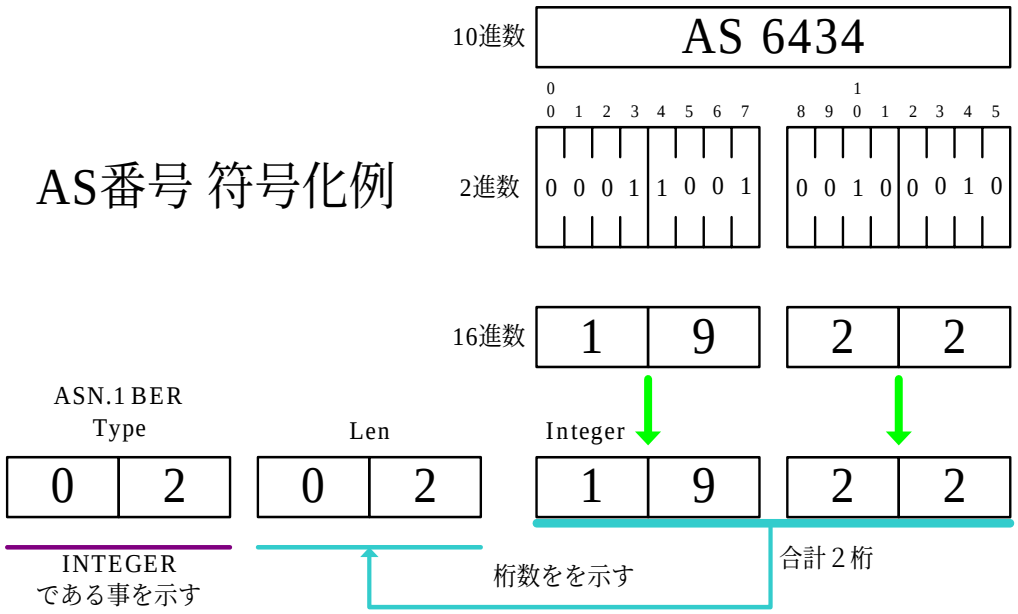


図 9-3　AS 番号符号化例

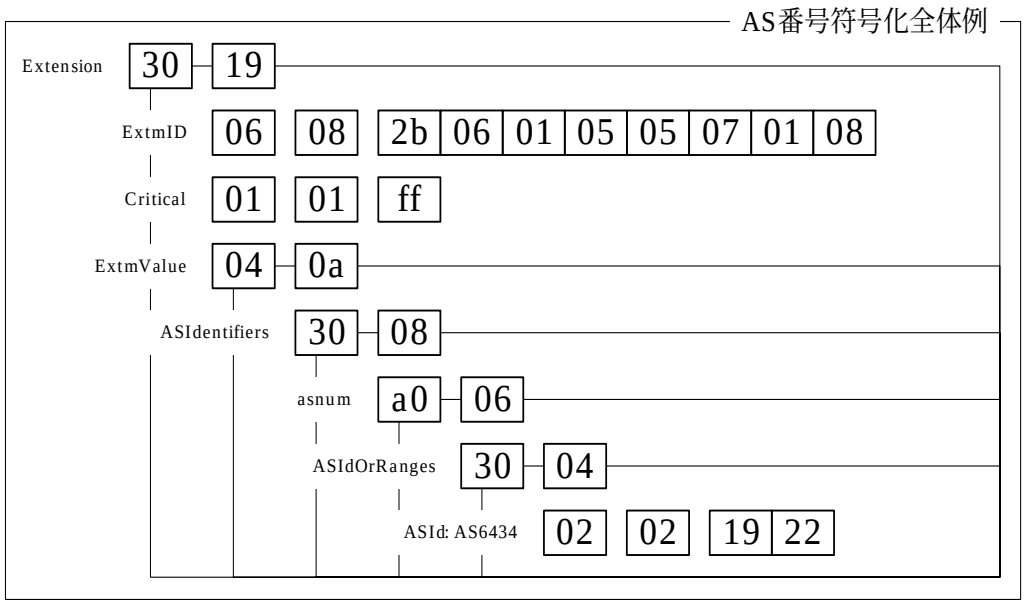


図 9-4　AS 番号符号化 全体例

以上、IP アドレスブロックと AS 番号の 2 種類のうちいずれかを利用し証明書が作成される。

9.2. soBGP の概要とモデル

本節では、経路情報を保護するための提案である soBGP につて、その概要と JPNIC で運用が考えられている IP アドレス証明書システムと JPIRR システムとの連携モデルについて述べる。

9.2.1. soBGP の概要

soBGP の目的は、不正経路情報の発見、除去を自動化する事である。実現方法として、経路生成者が経路情報に対して署名し、作成した証明書を BGP セキュリティ・メッセージで配布する。受取者は受信した証明書を検証する事により、経路情報の真偽を確認する事が可能となり、偽情報を除去する為の情報として利用する事が出来る。証明書の配布→受信→署名検証→証明書の登録／偽情報の排除を自動化する為の提案である。

soBGP で定義されている証明書に含まれる経路情報は主に「AS 番号」「IP アドレス情報」「隣接トランジット AS 番号」「隣接非トランジット AS 番号」がある。定義外の情報に関して検証する手段は提供されない。

9.2.1.1. BGP への拡張

soBGP では、証明書を交換する為に BGP[RFC4271]を拡張し実装される。一つは、隣接する機器同士で[RFC2842[3]]を利用した機能確認を行う（capability code は未決である）機能、二つ目は、BGP で証明書を配布する機能である。証明書配布機能を拡張する為に BGP タイプ・コード（BGP Type Code は未決である）を追加しセキュリティ・メッセージを定義する。

機能確認では、接続先機器が soBGP を利用可能であるかの確認を行い、その結果により soBGP の動作を決定できる仕組みを運用者に提供する。簡単な動作例としては、「接続された機器が soBGP 利用を拒否した時、BGP セッションを停止する」といった運用が可能

[3] Capabilities Advertisement with BGP-4 (RFC2842)
http://www.ietf.org/rfc/rfc2842.txt

になる。この様な接続機器同士の機能確認の仕組みは BGP→soBGP 移行期間には必要な機能である。

新たに定義された BGP タイプ･コードを利用した BGP メッセージ(セキュリティ･メッセージ)では、soBGP の動作を決定するオプションや証明書の送受信などを行うために利用する。簡単な動作としては、「証明書を受信した機器は、証明書を検証し自身の管理テーブルへ登録する。検証出来ない証明書は捨てられると共に経路情報も経路テーブルから削除する」といった動作である。

セキュリティ･メッセージ･フォーマットを図 9-5 に示す。

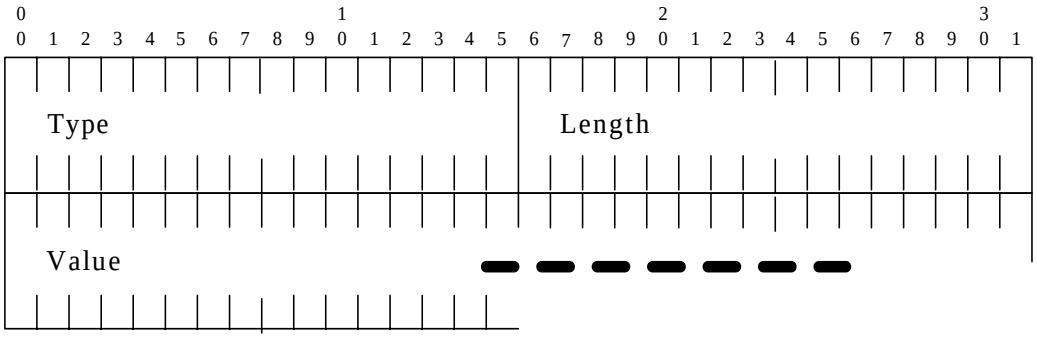


図 9-5　セキュリティ･メッセージ･フォーマット

Type は Value フィールドのデータ種別を示し、Length は Value フィールドのサイズを示す。この様なフォーマットは、TLV (Type,Length,Value) と呼ばれており、本調査でも TLV を利用する。Value フィールドには「SECURITY Option」「Request」「Cluster List」定義されている。

(1) SECURITY Option

本データは、機能確認が行われた後、最初に隣接した機器間で交換が行われる。目的は機器間でのセキュリティ･メッセージをどの様に受け取るかを接続先に伝える事である。

本オプションは、BGP セッション開始時に一度交換され、オプション変更をする

際には BGP セッションのリセットが必要である。

SECURITY Option TLV フォーマットを図 9-6 に示す。

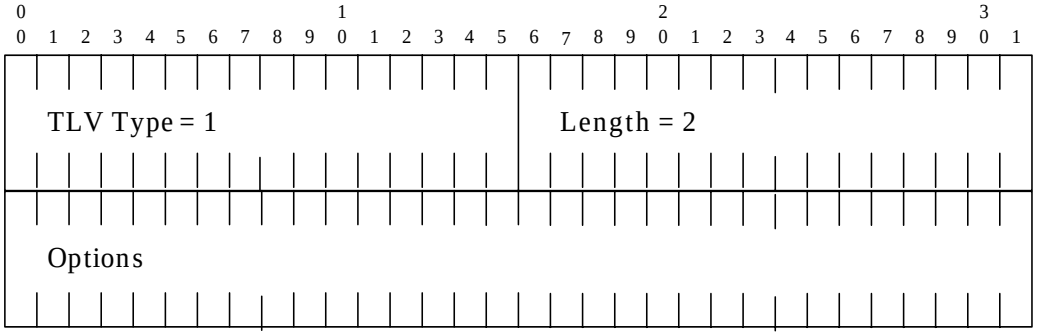


図 9-6　SECURITY Option TLV フォーマット

Option 部分は各ビット単位で意味を表す。

Bit0 の役割は、接続先機器へ経路情報(NLRI)を先に送るのか、証明書→NLRI の順で送るのかを指示する為に利用する。前者の場合には経路収束時間は現状と同等程度であるが、一定期間不正な経路が経路テーブルへ入り込む可能性がある（Routing Information Base(RIB)の更新は行われない）。後者の場合はすべての経路情報を検査した後、経路テーブルへ登録されるため、前者より経路テーブルの更新時間が長く必要である。

Bit1 と Bit2 は既に検証を終えた経路情報について、セキュリティ情報を再検証せずに処理される事を接続先機器へ伝える。Bit1 がセットされている場合は検証済み経路情報が接続先へ送られる事を示しており、Bit2 がセットされている場合は検証済み経路情報を送る事を接続先へ要求し、自身では再検証を行わない事を示している。

Bit1 と Bit2 は iBGP で利用する事で再検証にかかるリソースを軽減されることになるが、eBGP で利用すると不正な経路情報の検証ができない可能性がある為、利用は禁止されている。

⑵ Request TLV

Request TLV は、特定の証明書を指定し接続先に対して要求する。

Request TLV フォーマットを図 9-7 に示す。

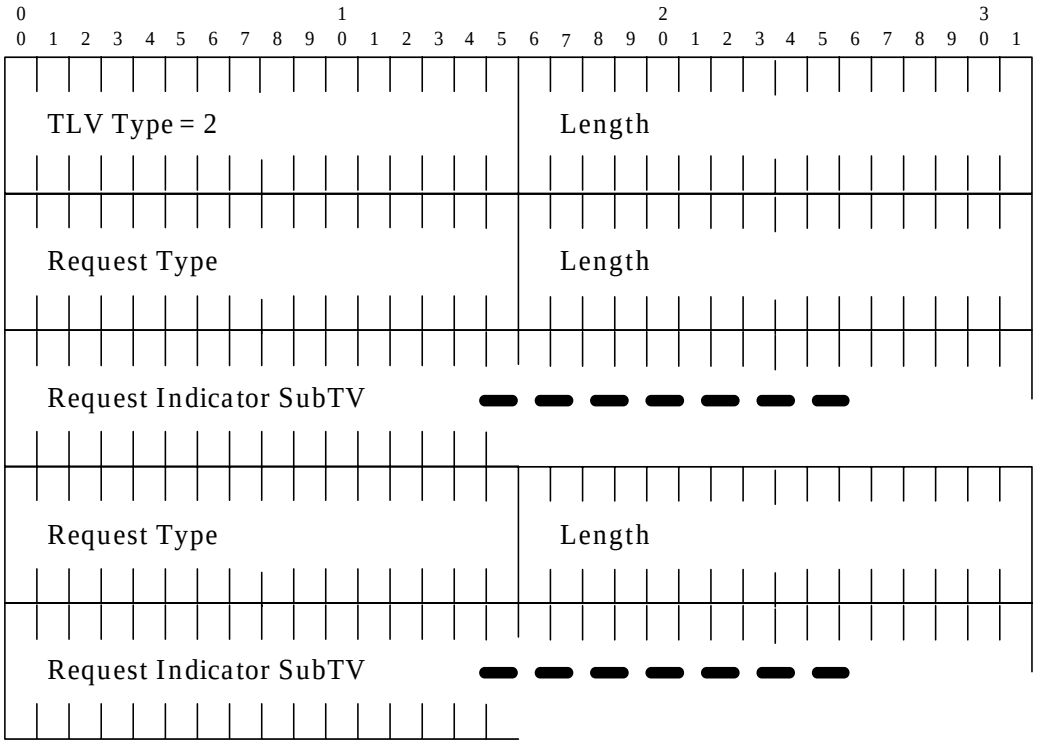


図 9-7　Request TLV フォーマット

Request TLV は、「Request Indicator」で示された条件で「Request Type」で示されている証明書に関して接続先に対して証明書を送る様に要求する。

- 「Request Indicator」にマッチする「EntityCerts」
- 「Request Indicator」にマッチする「ASPolicyCerts」
- 「Request Indicator」にマッチする「PrefixPolicyCerts」
- 「Request Indicator」にマッチするあらゆる証明書

「Request Indicator」には、「割り当て済み/Origin AS 番号」、「署名者/AS 割り当て組織 AS 番号」、「IPv4 アドレス」、「IPv6 アドレス」、「開始シリアル番号」そして「終了シリアル番号」の 6 種類が現在定義されている。

⑶ Cluster List TLV

Cluster List TLV は、受けた経路を Refrect(iBGP で利用される Route Refection と似た動作)して転送する場合に利用し、ClusterID には Reflect した BGP ルータ ID を示す。

Cluster List TLV フォーマットを図 9-8 に示す。

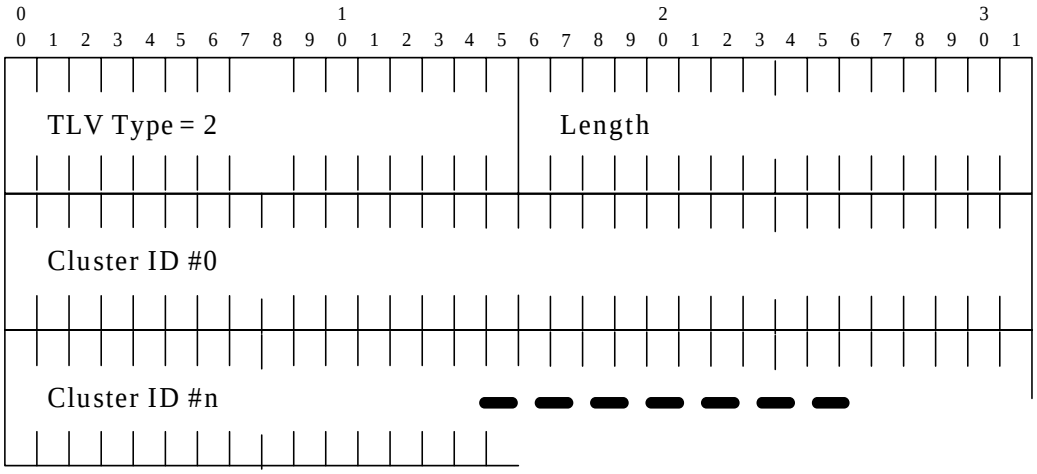


図 9-8　Clister List TLV フォーマット

BGP Refection を利用する BGP ルータは、受け取った BGP セキュリティ・メッセージに ClusterList TLV が定義されているかを確認する必要がある。すでに Cluster List に自身の ID が存在するときには、本メッセージを削除する。自身の ID が存在しないときには追加し、ClusterList TLV が存在しないときには、自身で生成し、追加する。

9.2.1.2. soBGP の情報信頼モデル

soBGP は、公開鍵基盤(PKI)の枠組みを用いて証明書の信頼性を確保する。検証方法は[RFC3280]に従い行われる。

soBGP で基本となる証明書(EntityCert：後述)を Verisign や RIR 等の AS 運用管理組織から信頼されている第 3 組織が運営する認証局を用いて署名する事により、証明書の信頼性を確保し、EntityCert の対となる PrivateKey によりさらに別の証明書に対し署名する事が可能である。検証者は証明書内の認証局名とその署名を確認しながら自身が信用する認証局の署名まで繰り返し確認を行い、自身が信用する認証局が署名までたどり着けない場合には、その証明書は不正に作成されたものであると判断し関わる情報は全て破棄し、CRL や有効期限についても確認が行われ失効している証明書に関しても破棄する。

9.2.1.3. soBGP で利用する証明書

soBGP で利用される証明書は、Entity Certificate(EntityCert)、Authorization Certificate(AuthCert)、Policy Certificate(PolicyCert)の3種類がある。

- EntityCert → AS 運用組織と証明書内の公開鍵が検証可能
- AuthCert → AS が広告する IP アドレスブロック(Origin)である事が検証可能
- PolicyCert →ASPolicyCert と PrefixPolicyCert の2種類あり、前者は AS に関連したポリシ、後者は IP アドレスブロックに関連したポリシが検証可能

⑴ EntityCert に関して

EntityCert は、AS が利用している公開鍵(PublicKey)を配布する為に利用され、AS 番号と公開鍵(PublicKey)が含まれる。 EntityCert に含まれる公開鍵は、AS が発行する様々な証明書を署名する際に利用する秘密鍵(PrivateKey)に対応する公開鍵である。

EntityCert のフォーマットは[RFC3280]で定義され、「AS 番号」は[RFC3779]を

利用し、証明書への署名は[RFC3279[4]]で定義されているsha1withRSAEncryptionを利用する。

EntityCert作成には、EntityCert発行申請者（AS運用組織）がPublicKey/PrivateKeyペアを作成後、AS番号を含んだEntityCert CSRを作成する。作成したEntityCert CSRを証明書発行者（認証局）へ送付する。

EntityCert CSRを受け取った認証局は内容を検証し、情報が正規なものであか検証した後、EntityCert CSRに署名しEntityCertを作成する。作成したEntityCertをAS運用組織へ返送する。

AS運用組織は受け取ったEntityCertを[RFC3280]に基づき検証、問題無ければEntityCertの広告／配布を開始する。

この時点でAS運用組織はEntityCertと対になるPrivateKeyを用いて他の証明書に対して署名可能となる。

soBGPでは、EntityCertをシステム内で一意に識別する為にCertificateSerialNumberとIssuerAltNameを利用する。このフィールドは必ず証明書に含まれていなければならない。

EntityCertの配布法は複数ある。

[4] Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC3279)
http://www.ietf.org/rfc/rfc2842.txt

- AS 運用者自身が運用している公開レジストリ若しくは一般に信用されている IP レジストリシステム等に登録し参照者が必要なときに取得する方法
- ネットワークを利用せずに、郵送などの手段を利用する方法
- soBGP で BGP 新たに定義されたセキュリティ・メッセージを利用する方法

初めの2種類に関しては、全てのAS運用者が新しいEntityCertを取得→検証→設定するのに時間必要である為、実際に経路を広告した時、受信側で広告した経路用 EntityCert の検証終了していない可能性がある(つまり経路が破棄される)。最後のセキュリティ・メッセージを利用した場合は、経路制御機器にて即座にその経路に関する EntityCert の検証が可能である。しかし、この方法では、経路制御機器やその他リソースに対して経路交換/検証処理にかかる割合がより大きくなる、また物理回線に占める経路交換情報の比率が上がる事になる(利用者の利用可能帯域が下がる)。

EntityCert を受け取った組織は、[RFC3280]に従い証明書を発行した認証局の署名、有効期限、認証局が発行している CRL も含めて検証を行う。問題が無ければ、EntityCert 内の AS 番号と PublicKey を経路制御機器内に保存し、AS 番号にマッチした組織から広告されたセキュリティ・メッセージ内の経路情報に関して PublicKey を利用した検証準備が出来た事になる。

検証する際に自組織が信頼している第3者機関認証局の証明書も EntityCert(RootEntityCert)として登録し広告しなければならないが、RootEntityCert は自己署名されている為、自動検証は不可能である。RootEntityCert のみは人手により検証され、経路制御機器へ設定する。この時、RootEntityCert が多すぎると運用付加(主に経路制御機器への登録作業)が増大する。また、各組織が独自の判断で第3者機関認証局を選択すると認証局ポリシの違いから不正な経路が紛れ込む可能性も大きくなる。そこで、IANA/RIR/LIR 等の一般的に認知されている権威ある組織が作成した EntityCert を soBGP で利用する場合の最上位の RootEntityCert として定義し手動で登録することにより運用負荷や認証局ポリシの違いから起こりうるリスクの軽減等が可能である。

EntityCert 交換概要を図 9-9 に示す。

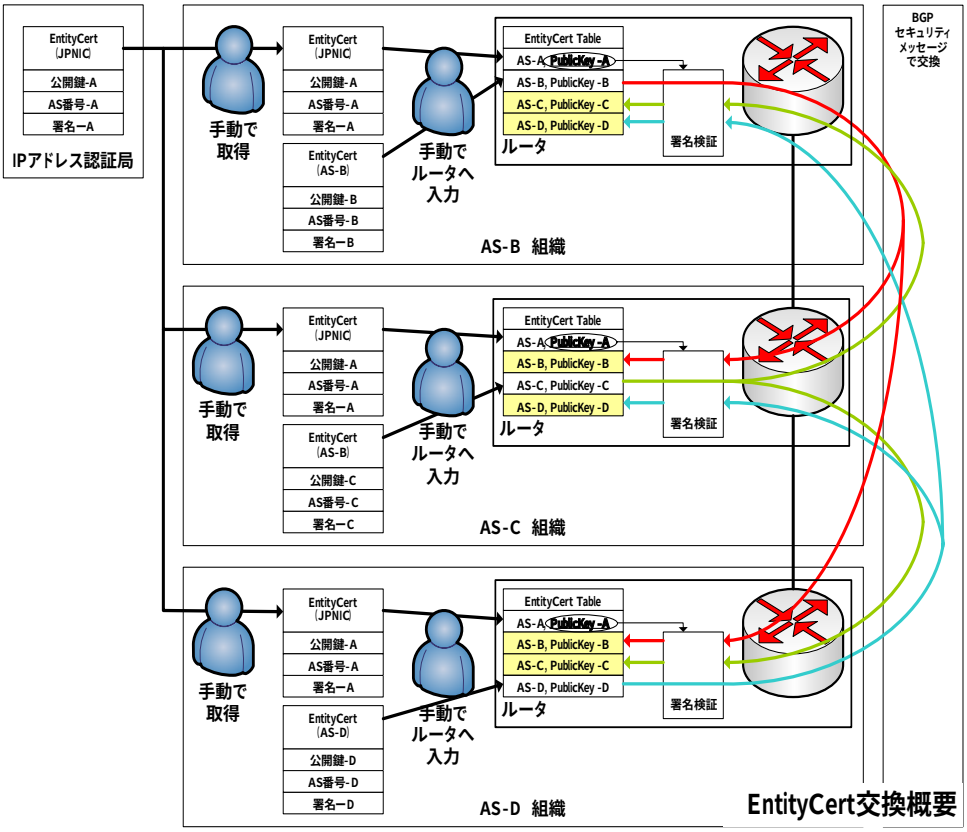


図 9-9　EntityCert を交換する際の概要

EntityCert 証明書は様々な理由で失効するが、有効期限を検査する為に経路制御機器では時刻同期をする必要がある。また、破棄ﾘｽﾄ(CRL)の配布は ASPolicyCert(後述)にて行う。

CRL により EntityCert が失効した時は、失効した EntityCert で検証した情報は全て破棄しなければならない。証明書の有効期限が満了した時には、有効期限が切れる前の証明書で利用した PublicKey/PrivateKey と新しい有効期限で作成された EntityCert が配布された場合には AuthCert と PolicyCert は継続して利用が可能である。しかし、有効期限満了後まったく新しい EntityCert(PrivateKey/PublicKey の再利用はしない)の場合には古い EntityCert で検証した経路情報は破棄しなければならない。

⑵ AuthCert に関して

AuthCert は、AS 運用者が自身を Origin とする IP アドレスブロックであることを証明する為に利用する。自 AS 番号、広告する IP アドレスブロック、IP アドレスブロックを割り振った AS 番号(上位の AS 番号や RIR 等)と IP アドレスの割り振り/割り当てを行った組織の署名が含まれる。

AuthCert を作成するには、後述する署名 TLV 以外の TLV をまとめた後、[RFC3279]で定義されている方法で署名を生成し、署名 TLV を作成する。利用した TLV と署名 TLV を合わせて AuthCert としてセキュリティ・メッセージで広告する。この時、署名に用いられる PrivateKey は IP アドレスブロックを割り当てた組織の EntityCert PublicKey と対となっている物を利用する。AuthCert は、割り当て側が全て作成しても、各々が必要な箇所を埋めても問題は無い。最終的に署名 TLV を作成するのは割り当て側組織である。

AuthCert は、自身を広告する事も可能であるが、後述する PrefixPolicyCert に埋め込まれ、各組織へ配布する形態が考えられている。

AuthCert(PrefixPolicyCert)配送の概略を図 9-10 に示す。

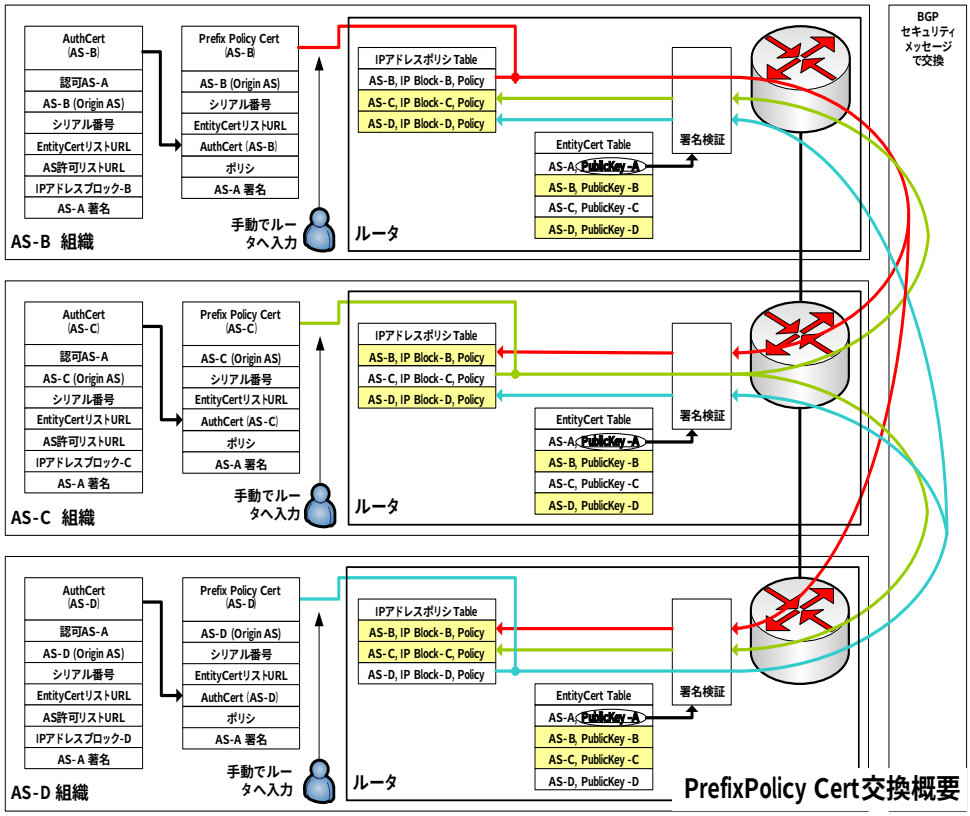


図 9-10　AuthCert 配布の概要

AuthCert の検証には、署名した組織の EntityCert を検証者が持っていなければならない。EntityCert が無い場合は AuthCert を破棄する。EntityCert を取得／検証後、AuthCert の再取得／再検証を行う。EntityCert を検証者が持っている場合には、その中にある PublicKey を利用して AuthCert を検証し、問題が無ければさらに AuthCert 破棄リストを確認し、破棄されていなければ、AuthCert の Address Prefix TLV にある Prefix と Authorized Originator TLV にある AS 番号を利用することが可能である。もし、自己署名された AuthCert を受信したときには注意が必要である。慎重に確認し、個別に判断を下さなければならない。

AuthCert を破棄するためには 3 つの方法がある。一つ目は署名した EntityCert を破棄する。この場合は、個別の IP アドレスブロックの破棄は出来ない。残り 2 つの方法では、IP アドレスブロック別に破棄可能な方法である。二つ目は、AuthCert 用の破棄リストを作成し、この破棄リストを「Authorizing AS Validation List Uniform Resource Locator」で示す。三つ目は、ASPolicyCert(後述)内にある「Authorization Certificate Validity List」を利用する。

AuthCert で利用されるセキュリティ・メッセージ・フォーマットを図 9-11 に示す。

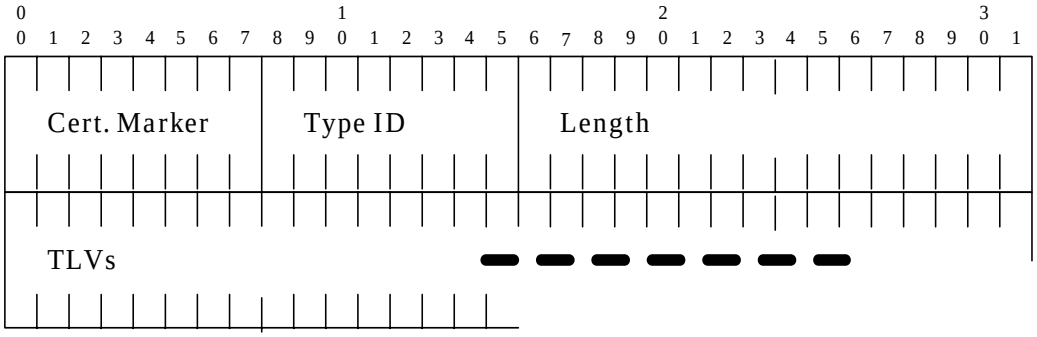


図 9-11　AuthCert セキュリティ・メッセージ・フォーマット

Cert. Marker は、soBGP で利用する証明書であることを示す 162 (0xa2)である。Type Id はメッセージ・タイプを示し、AuthCert の場合は「1」を指定する事が規定されている。Length は以降続く TLV 群の長さを示す。

TLV には「Authorizing AS」、「Authorized Originator」、「Serial Number」、「Authorizing AS EntityCert Uniform Resource Locator」、「Authorizing AS Validation List Uniform Resource Locator」、「Address Prefix」そして「Signature」の7種類がある。

「Authorizing AS」TLV は、IP アドレス割り振り／割り当て組織の AS 番号を表す。

Authorizing AS TLV フォーマットを図 9-12 に示す。

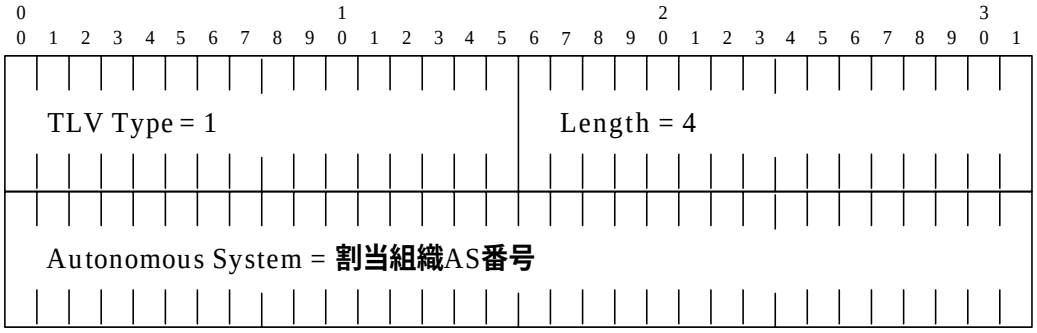


図 9-12　Authorizing AS TLV のフォーマット

「Authorized Originator」TLV は、IP アドレス割り振り／割り当て組織より IP アドレスを割り振り／割り当てられた運用者の AS 番号を表す。

Authorized Originator TLV フォーマットを図 9-13 に示す。

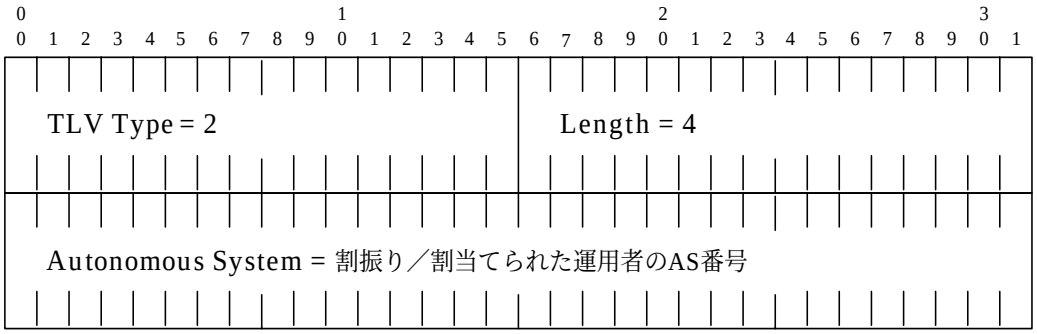


図 9-13　Authorized Originator のフォーマット

「Serial Number」TLV は、IP アドレス割り当て組織により管理され設定する。

Serial Number TLV フォーマットを図 9-14 に示す。

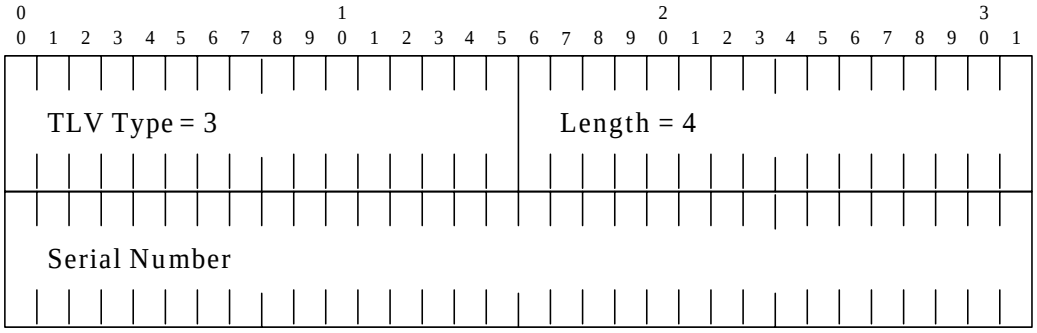


図 9-14　Serial Number TLV のフォーマット

「Authorizing AS EntityCert Uniform Resource Locator」TLV は、IP アドレス割り振り／割り当て組織の最も新しい EntityCert の配布場所を表す URL である。本 TLV は、AuthCert を受け取った機器に既に EntityCert が存在するときには、利用されない可能性や必要無い物として広告しない事もある。

Authorizing AS EntityCert Uniform Resource Locator TLV フォーマットを図 9-15 に示す。

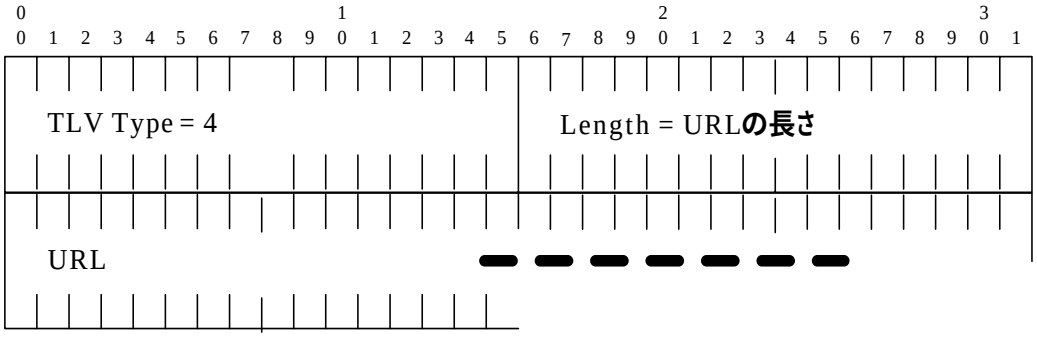


図 9-15　Authorizing AS EntityCert Uniform Resource Lcator TLV フォーマット

「Authorizing AS Validation List Uniform Resource Locator」TLV は、AuthCert の有効／無効を表す最新リストの配布場所を示す URL である。内容は、有効 IP アドレスブロックと無効 IP アドレスブロックを区別できるような形で構成される(ASPolicyCert を参照)。この TLV は、ポリシによっては利用されない可能性がる。また、必要ない物として広告されない可能性もある。

Authorizing AS Validation List Uniform Resource Locator TLV フォーマットを図 9-16 に示す。

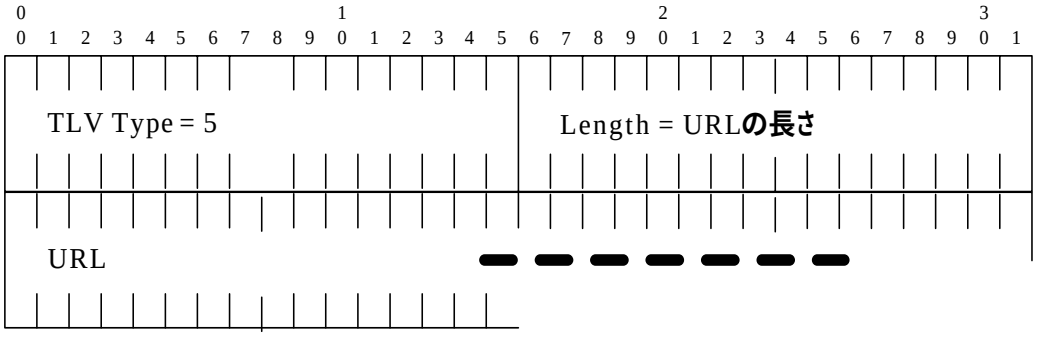


図 9-16　Authorizing AS Validation List Uniform Resource Locator TLV フォーマット

「Address Prefix」TLV は、IP アドレス割り振り組織から割り当てられた IP アドレスブロックを表す。「Address Family Identifier」には、[IANA-AFI[5]]にある値を指定し、「Subsequent AFI」には[IANA-SAFI[6]]にある値を指定する。また「NLRI Data」には[RFC2858]セクション 4 にある形式で IP アドレス・プリフィクスを指定する。

Address Prefix TLV フォーマットを図 9-17 に示す。

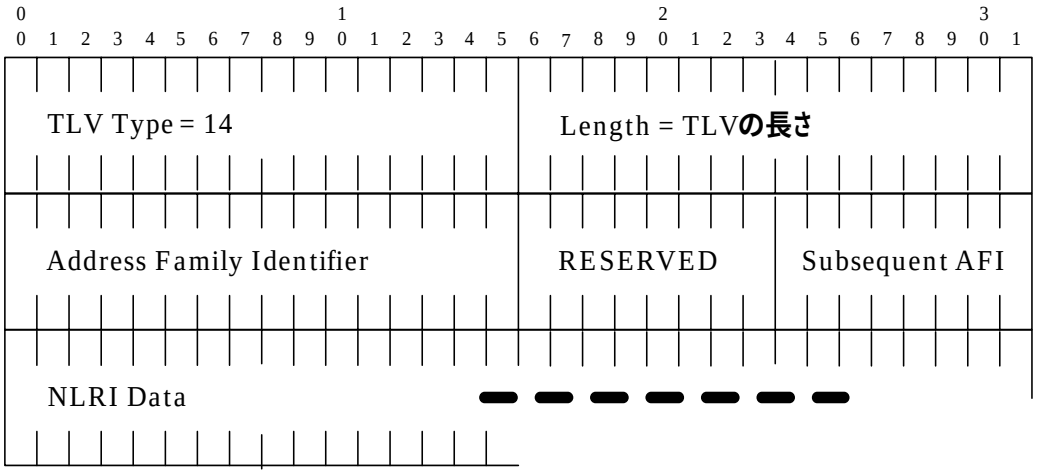


図 9-17　Address Prefix TLV のフォーマット

[5] http://www.iana.org/assignments/address-family-numbers
[6] http://www.iana.org/assignments/safi-namespace

「Signature」TLV は、AuthCert の署名が入る。「Signature Type」には署名アリゴリズムを示し、現在は1のみが定義されている。

Signature Type = 1 は、[RFC3279]で定義されている sha1withRSAEncryption を利用することを表す。

「Number of Issuers」は、後に続く割り振り／割り当て組織の組織数を表し、もし Number of Issuers>1 である時は各組織で作られた EntityCert の PublicKey は同じでなければならない。つまり、異なる 2 つ以上の EntityCert PrivateKey で一つの AuthCert を署名することはできない。

「Entity Certificate Issuer Autonomous System」は割り振り組織の AS 番号が入り、「Entity Certificate Serial Number」には割り当て組織の EntityCert に利用したシリアル番号が入る。

「Signature」は Signature Type で生成した署名が入る。

Signature TLV フォーマットを図 9-18 に示す。

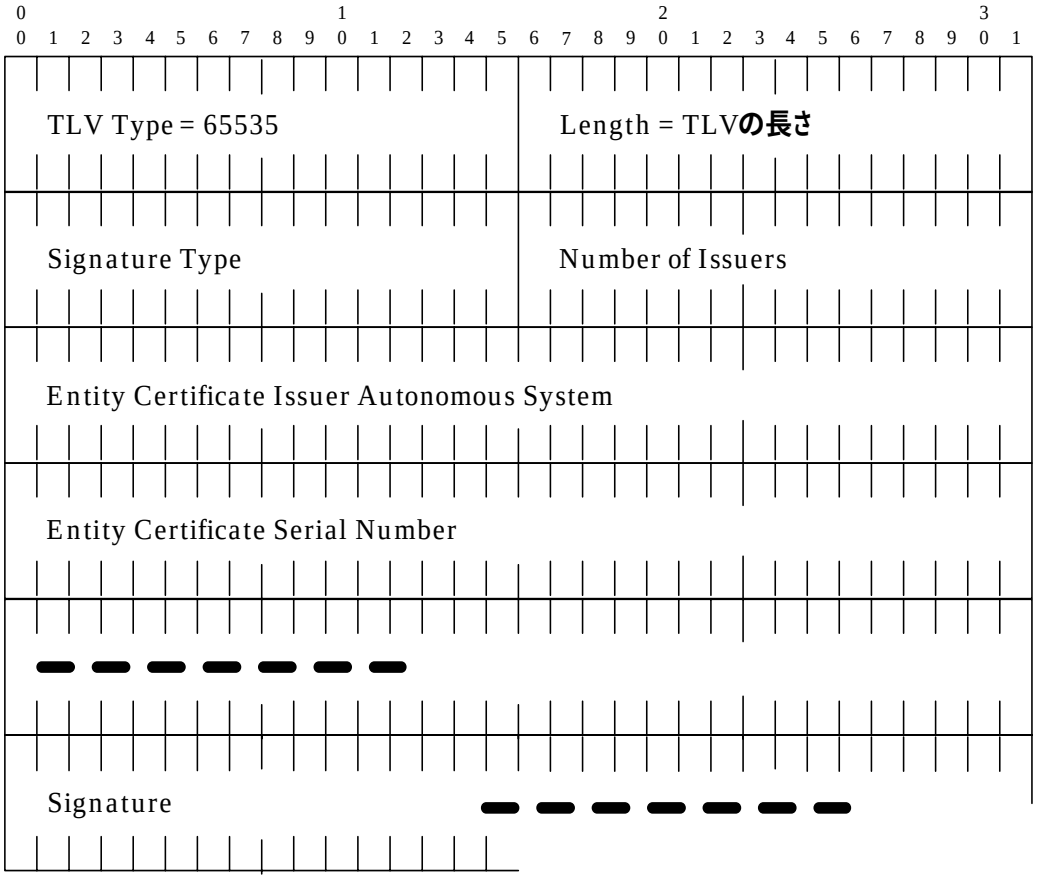


図 9-18　Signature TLV フォーマット

⑶ PrefixPolicyCert に関して

PrefixPolicyCert は、IP アドレスブロックの最大プリフィクス長や AS_PATH の確認の有無等、Origin AS が指定したポリシを証明するために利用する。IP アドレスブロックの Origin AS 番号、AuthCert、ポリシ、署名が含まれる。

PrefixPolicyCert CSR は、IP アドレスブロックの Origin AS 組織が作成する。

PrefixPolicyCert 作成には、署名 TLV 以外の TLV をまとめた後、[RFC3279] で定義されている方法で署名を生成し、署名 TLV を作成する。利用した TLV と署名 TLV を合わせて PrefixPolicyCert としてセキュリティ・メッセージで広告する。この時、署名に用いられる PrivateKey は IP アドレス割り振り／割り当て組織 AS

の EntityCert PublicKey と対になる物である。

PrefixPolicyCert の検証には大きく 2 つのステップがある。これは、PrefixPolicyCert が AuthCert を内包している為である。初めに PrefixPolicyCert に付いている署名の検証、次に PrefixPolicyCert に内包されている AuthCert に付いている署名の検証を行う。双方とも EntityCert を検証者が持っていなければならない。もしどちらか一方の EntityCert が無い場合でも PrefixPolicyCert は破棄され、正規の EntityCert を取得後、再検証を行う。EntityCert を検証者が持っている場合には、EntityCert PublicKey を利用して署名を検証し、問題ない場合に AuthCert 内にある IP アドレスブロックが PrefixPolicyCert 内にあるポリシの範囲で利用可能である。署名が自己署名であった場合には慎重に確認したうえで個別に判断を下さなければならない。

PrefixPolicyCert を破棄する(もしくは有効にしない)ためには 2 つの方法がある。一つ目は EntityCert を破棄することにより署名検証不可にする。もう一つは PrefixPolicyCert 個別に破棄が可能で ASPolicyCert(後述)にある「Prefix Policy Certificate Validity List」TLV を利用する。この TLV で破棄が指定された PrefixPolicyCert は破棄されなければならない。

PrefixPolicyCert で利用されるセキュリティ・メッセージ・フォーマットを図 9-19 に示す。

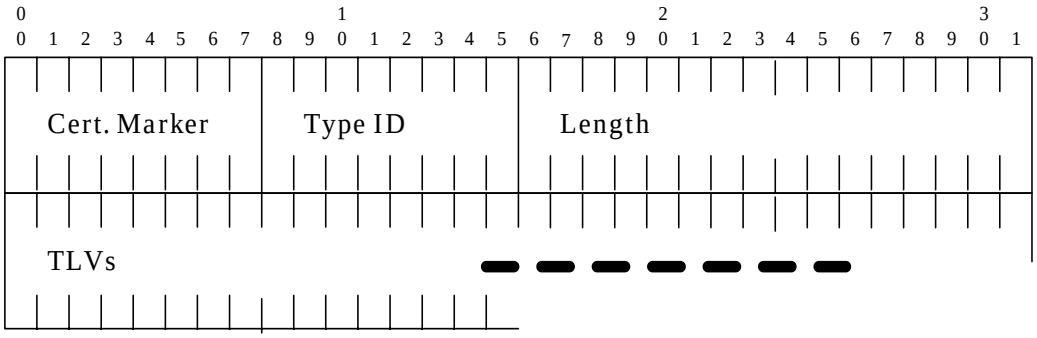


図 9-19　PrefixPolicyCert セキュリティ・メッセージ・フォーマット

Cert. Marker は、soBGP で利用する証明書であることを示す 162 (0xa2)、Type Id はメッセージのタイプを表し、PrefixPolicyCert の場合は「2」を指定することが規

定されている。Length は以降続く TLV 群の長さを示す。

TLV には「Originating Autonomous System」、「Serial Number」、「Serial Number」、「Authorizing AS EntityCert Uniform Resource Locator」、「AuthCert」、「Policies」、「SubTVs」そして「Signature」の 8 種類がある。

「Originating Autonomous System」TLV は Origin AS 番号を表す。

Originating Autonomous System TLV フォーマットを図 9-20 に示す。

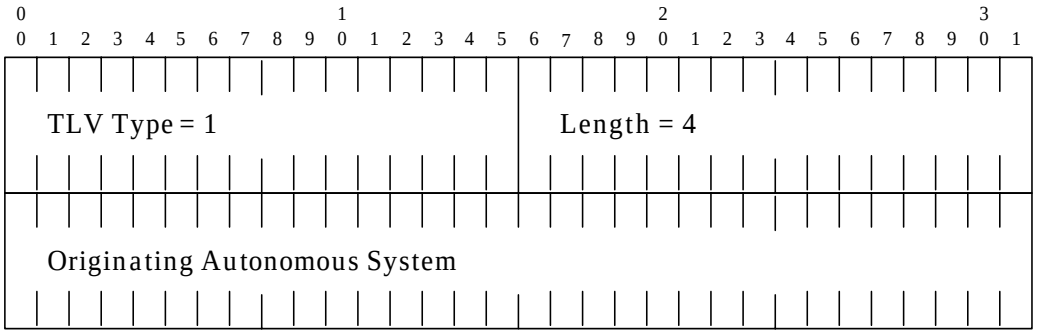


図 9-20　Originating Autonomous System TLV フォーマット

「Serial Number」TLV は、PrefixPolicyCert のシリアル番号を表す。

Serial Number TLV フォーマットを図 9-21 に示す。

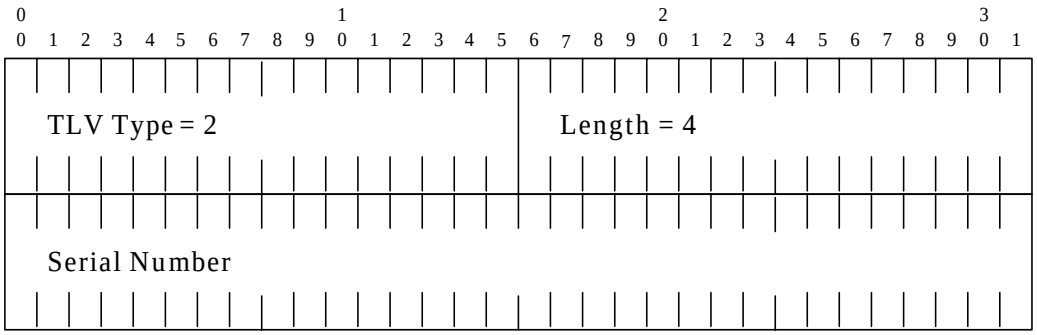


図 9-21　Serial Number TLV フォーマット

「Authorizing AS EntityCerts Uniform Resource Locator」TLV は、IP アドレス割り振り／割り当て組織の最も新しい EntityCert の配布場所を表す URL である。本 TLV は、PrefixPolicyCert を受信した機器に既に EntityCert が存在する時には、利用されない可能性、必要ないものとして広告されない可能性がある。

Authorizing AS EntityCerts Uniform Resource Locator TLV フォーマットを図 9-22 に示す。

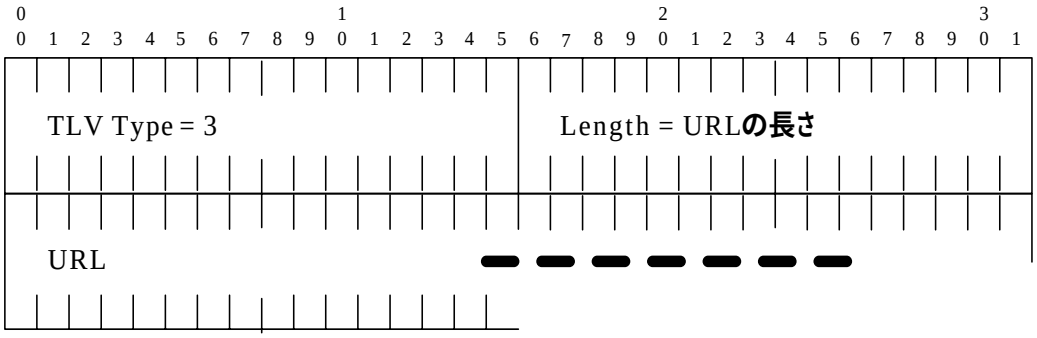


図 9-22 Authorizing AS EntityCerts Uniform Resource Locator TLV フォーマット

「AuthCert」TLV は、AuthCert がそのまま埋め込まれる。PrefixPolicyCert でポリシを示したい IP アドレスブロックに該当する AuthCert が入る。

AuthCert TLV フォーマットを図 9-23 にしめします。

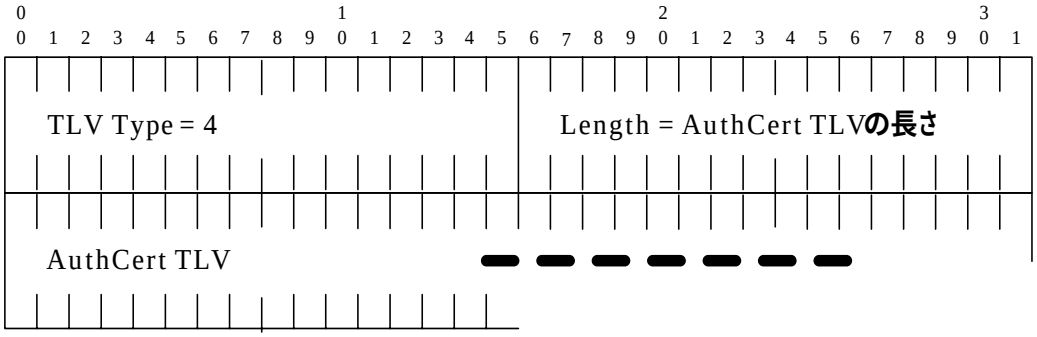


図 9-23　AuthCert TLV フォーマット

「Policies」TLV は、AuthCert 内で示されている IP アドレスブロックに対するポリシを指定する。Option はビット・フィールドで各々のビットをセットすることでポリシを指定し、SubTV(後述)によりポリシの拡張を行う。

Policies TLV フォーマットを図 9-24 に示す。

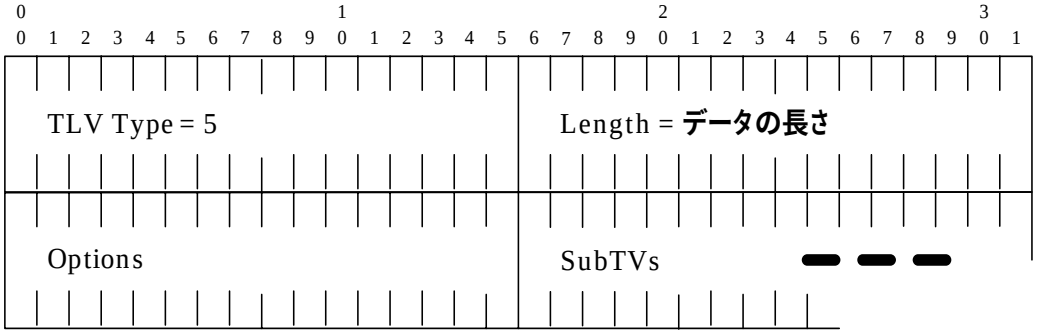


図 9-24　Policies TLV フォーマット

「Options」の Bit0 がセットされた場合、AS_PATH が検証できない経路情報に関しては利用すべきでないことを表し、Bit1 がセットされた場合 AS_PATH の 2 番目の AS に関する情報が検証できない場合には、この AS にかかわる経路情報は利用すべきでないことを表す。他のビットに関しては未定義となっているが将来利用される予定である。

「SubTVs」は、AuthCert 内で示されている IP アドレスブロックに対してオプション・ポリシを指定する。TV Type によりオプションを指定し、必要なパラメータをデータ部に記述する。現在は、3 種類のタイプが定義されている。

SubTVs フォーマットは図 9-25 に示す。

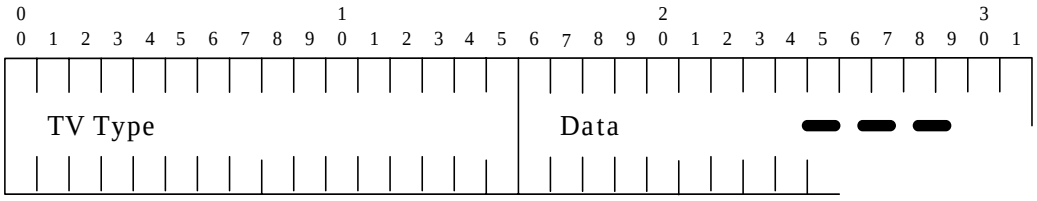


図 9-25　SubTVs フォーマット

TV Type が 1 の時は、AuthCert 内の全ての IP アドレスブロックに関して、Data 部に示された AS 番号が AS_PATH に含まれる事を必要とし、TV Type が 2 の時には、AuthCert 内のいずれかの IP アドレスブロックに関して、Data 部に示された AS 番号が AS_PATH に含まれる事を必要とする。TV Type が3の時には、Data には AuthCert 内にある IP アドレスブロックで利用可能な最大 Prefix 長を示す。

「Signature」TLV は、PrefixPolicyCert 証明書の署名である。「Signature Type」には署名アルゴリズムが入り現在は1のみが定義されている。Signature Type = 1 は、[RFC3279]で定義されている sha1withRSAEncryption を利用することを表し、「Number of Issuers」は後に続く割り振り／割り当て組織の組織数を示す。Number of Issuers > 1 である時は、各組織で作られた EntityCert PublicKey は同じでなければならない。つまり異なる 2 つ以上の EntityCert で一つの PrefixPolicyCert を署名することは出来ない。「Entity Certificate Issuer Autonomous System」は割り振り／割り当て組織の AS 番号、「Entity Certificate Serial Number」には割り振り／割り当て組織の EntityCert に利用したシリアル番号、「Signature」は Signature Type で生成した署名が入る。

Signature TLV フォーマットを図 9-26 に示す。

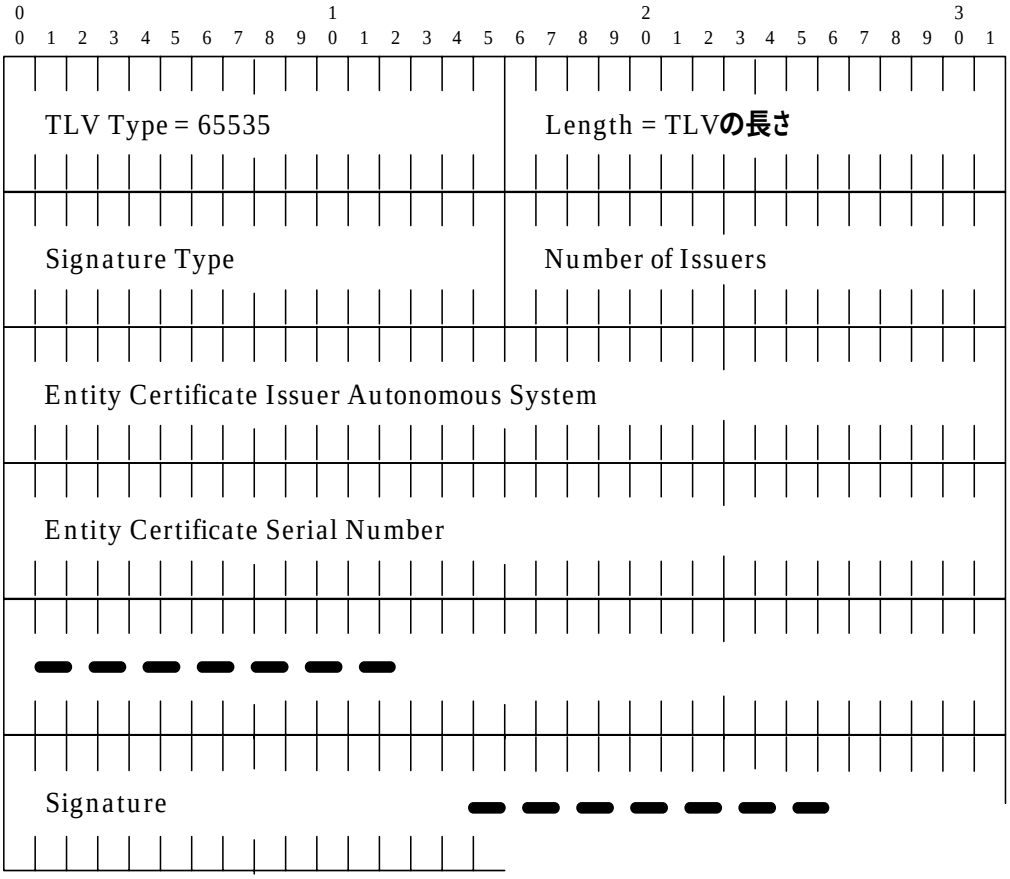


図 9-26　Signature TLV フォーマット

⑷ ASPolicyCert に関して

ASPolicyCert は、隣接組織の AS 番号等、組織単位のポリシを証明するために利用する。トランジット AS リスト、非トランジット AS リストや「Authorization Certificate Validity List」等が含まれる。

ASPolicyCert 作成には署名 TLV 以外の TLV をまとめた後、[RFC3279]で定義されている方法で署名を生成し、署名 TLV を作成、利用した TLV と署名 TLV を合わせて ASPolicyCert としてセキュリティ・メッセージで広告する。署名に用いられる PrivateKey は自 AS 用の EntityCert PublicKey で検証可能な PrivateKey である。ASPolicyCert は Origin AS 組織が作成する。

ASPolicyCert TLV と署名 TLV をまとめ、セキュリティ・メッセージで各組織へ配布される。概略を図 9-27 に示す。

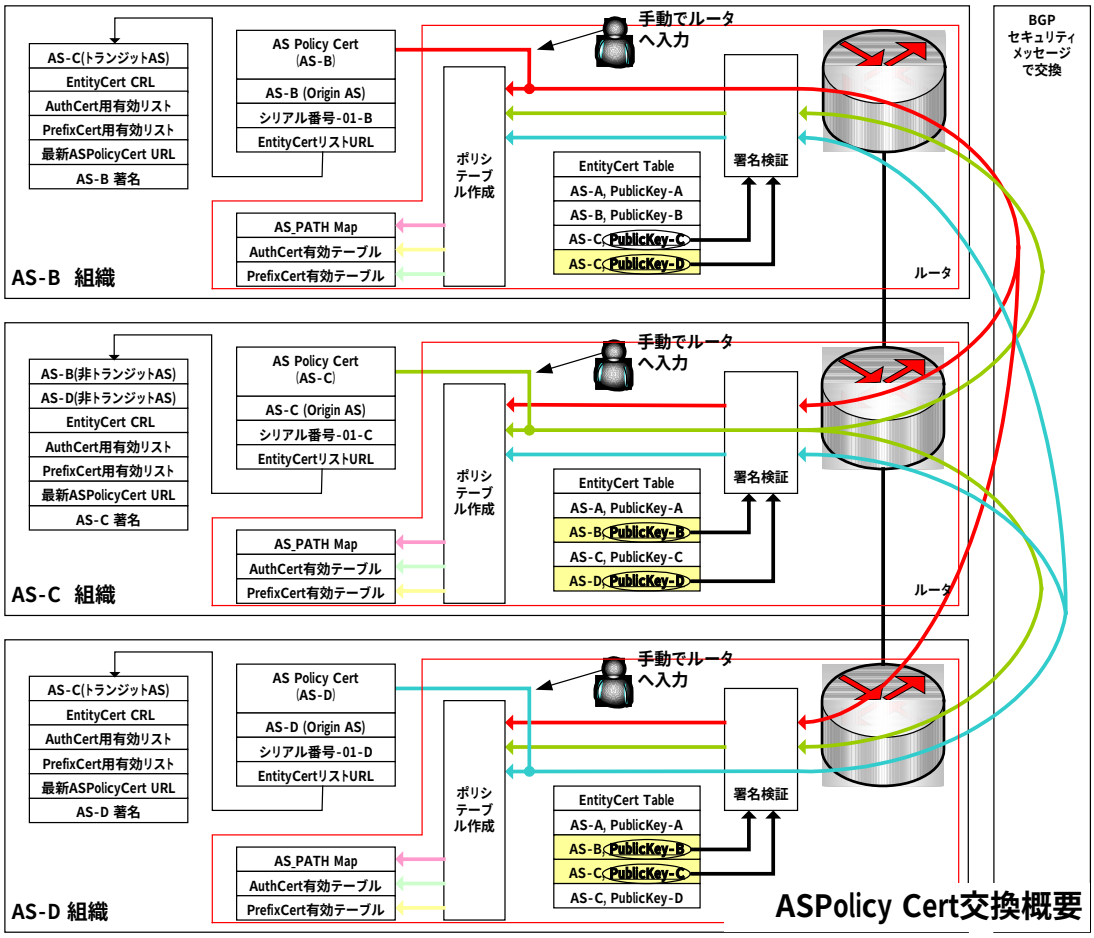


図 9-27　ASPolicyCert 配布概略

ASPolicyCert の検証には、署名した組織の EntityCert を検証者が取得していなければならない。EntityCert が無い時には、ASPolicyCert を信用してはならない。EntityCert を取得後、再検証を行う。EntityCert PublicKey を利用して ASPolicyCert を検証し問題なければ、さらに EntityCert の CRL を確認後、ASPolicyCert 内にある情報（隣接 AS リストや Validation List 等）が利用可能である。自己署名された ASPolicyCert を受信した場合には注意が必要である。慎重に確認したうえで個別判断を下さなければならない。

ASPolicyCert は、一度登録されると署名検証に必要な EntityCert を破棄する以外の方法では自動で破棄されることはない。AS が存在し相互接続されている

環境では必ず広告される。ポリシの変更をする時には内容を変更し署名した新しい ASPolicyCert を広告することで ASPolicyCert は上書きされる。

ASPolicyCert で利用されるセキュリティ・メッセージ・フォーマットを図 9-28 に示す。

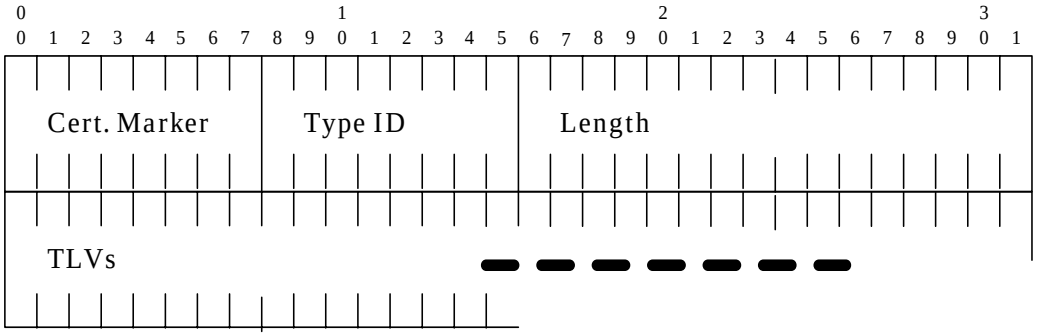


図 9-28　ASPolicyCert セキュリティ・メッセージ・フォーマット

Cert. Marker は、soBGP で利用する証明書であることを示す 162 (0xa2)、Type ID はメッセージ・タイプを表し、ASPolicyCert の場合は「3」を指定することが規定されている。Length は以降続く TLV 群の長さを示す。

TLV には「Originating Autonomous System」、「Serial Number」、「Authorizing AS EntityCert Uniform Resource Locator」、「Attached Transit Autonomous Systems」、「Attached Non-transit Autonomous Systems」、「Revoked Entity Certificate List」、「Authorization Certificate Validity List(With Validity Ranges)」、「Prefix Policy Certificate Validity List(With Validity Ranges)」、「Most Recent AS Policy Certificate Uniform Resource Locator」そして「Signature」の11種類がある。

「Originating Autonomous System」TLV は Origin AS 番号を表す。

Originating Autonomous System TLV フォーマットを図 9-29 に示す。

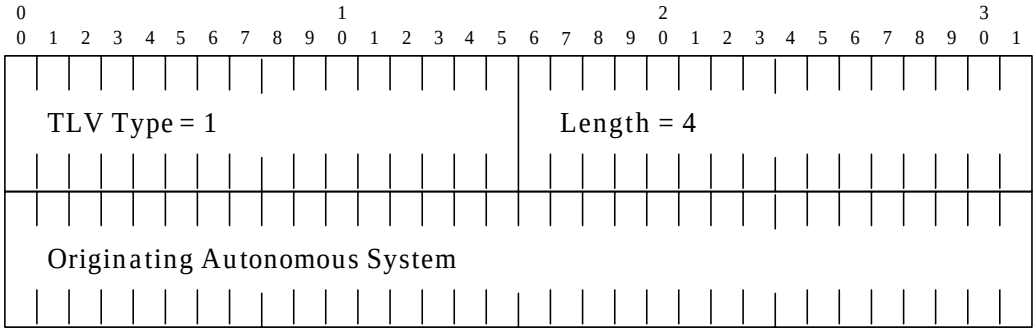


図 9-29　Originating Autonomous System TLV フォーマット

「Serial Number」TLV は署名者により管理され設定される。

Serial Number TLV フォーマットを図 9-30 に示す。

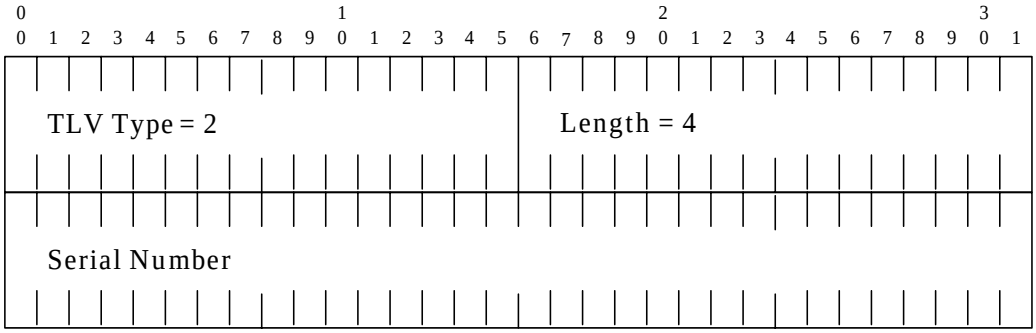


図 9-30　Serial Number TLV フォーマット

「Authorizing AS EntityCert Uniform Resource Locator」TLV は、署名した EntityCert の配布場所を示す URL である。この TLV は、ASPolicyCert を受信した機器に既に EntityCert が存在する場合は、利用されない可能性がある、必要無い物として本 TLV は広告しない可能性もある。

Authorizing AS EntityCert Uniform Resource Locator TLV フォーマットを図 9-31 に示す。

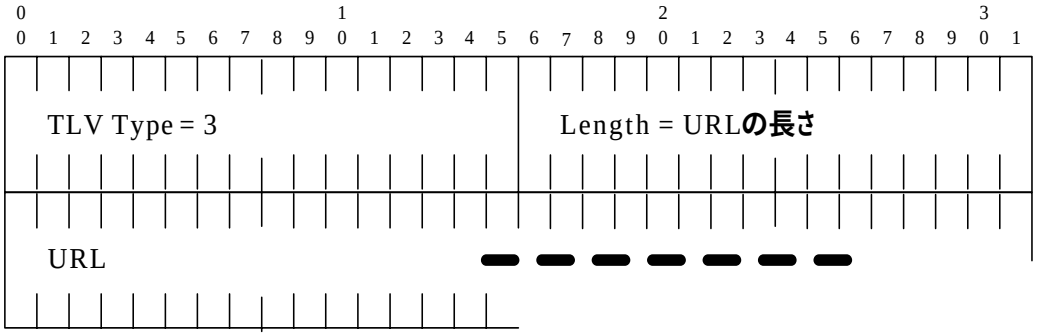


図 9-31　Authorizing AS EntityCert Uniform Resource Locator TLV フォーマット

「Attached Transit Autonomous Systems」TLV は、自組織と接続されているトランジット AS を表す。自組織が複数のトランジット AS が接続されている場合には、本 TLV は一つのセキュリティ・メッセージ内複数現れる。「Address Family Identifier」には[IANA-AFI]にある値を指定,「Subsequent AFI」には[IANA-SAFI]ある値を指定,「Autonomous Systems」には自組織に接続されているトランジット AS を指定する。

Attached Transit Autonomous Systems TLV フォーマットを図 9-32 に示す。

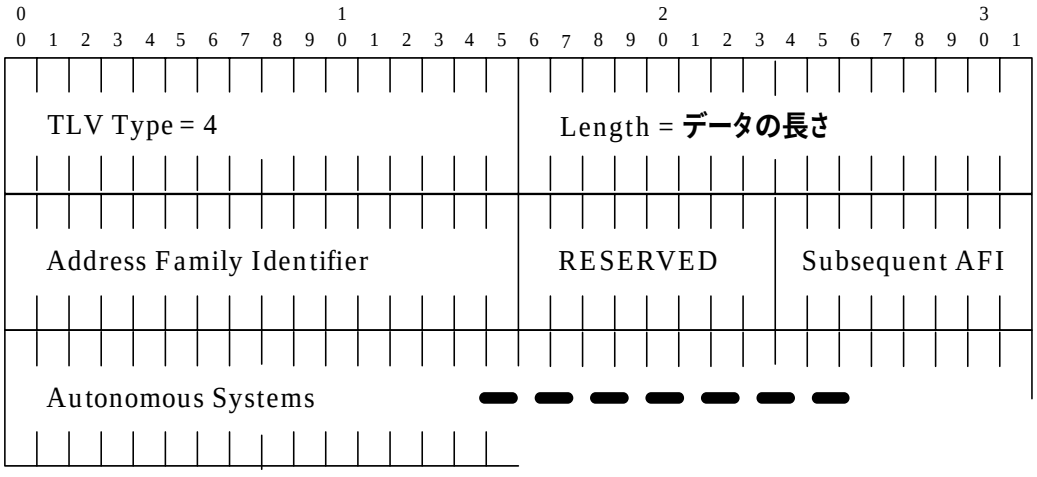


図 9-32　Attached Transit Autonomous Systems TLV フォーマット

「Attached Non-transit Autonomous Systems」TLV は、自組織と接続されている非トランジット AS を表す。自組織が複数の非トランジット AS が接続されている

場合には、本 TLV は一つのセキュリティ・メッセージ内複数現れる。「Address Family Identifier」には、[IANA-AFI]にある値を指定、「Subsequent AFI」には[IANA-SAFI]にある値を指定、「Autonomous Systems」には自組織に接続されている非トランジット AS を指定する。

Attached Non-transit Autonomous Systems TLV フォーマットを図 9-33 に示す。

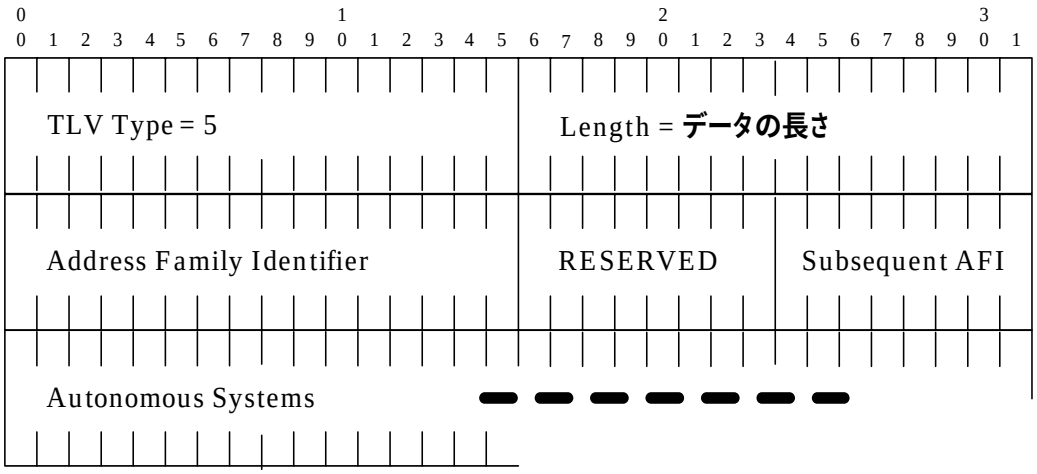


図 9-33　Attached Non-transit Autonomous Systems TLV フォーマット

「Revoked Entity Certificate List」TLV は、自組織の EntityCert 破棄証明書リストを表し、フォーマットは[RFC3280]に定義されている破棄証明書を利用する。

Revoked Entity Certificat List TLV のフォーマットを図 9-34 に示す。

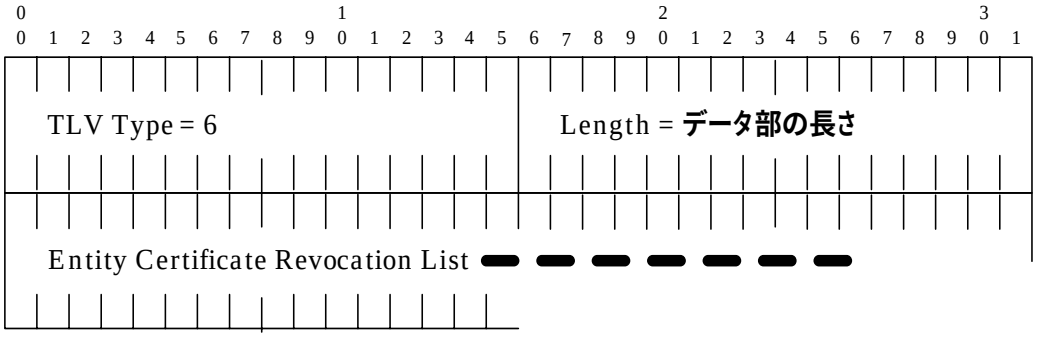


図 9-34　Revoked Entity Certificat List TLV フォーマット

「Authorization Certificate Validity List」TLV は、Origin AS が作成した AuthCert 証明書に対して「Validity Ranges」SubTV に指定されたシリアル番号の証明書が有効か無効かを示す。無効を示された AuthCert は削除されなければならない。

Authorization Certificate Validity List TLV のフォーマットを図 9-35 に示す。

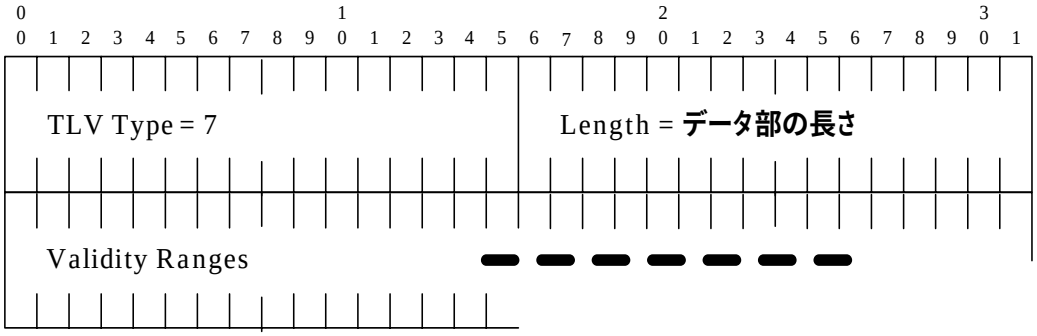


図 9-35　Authorization Certificate Validity List TLV フォーマット

「Validity Ranges」SubTV は、シリアル番号の範囲を指定して有効／無効を示す。「SubTV Type」へは有効／無効を指定し、「Size of Range」へは範囲を指定する。また、「Lowest Authorization Serial Number」へは最小のシリアル番号を指定する。

この SubTV は「Prefix Policy Certificate Validity List」TLV でも利用する。

Validity Ranges SubTV のフォーマットを図 9-36 に示す。

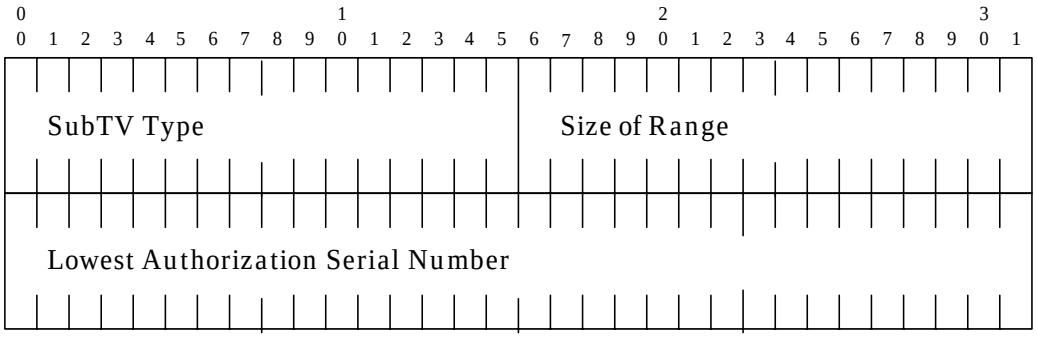


図 9-36　Validity Ranges SubTV フォーマット

「Prefix Policy Certificate Validity List」TLV は、Origin AS が作成した PrefixPolicyCert に対して「Validity Ranges」SubTV に指定されたシリアル番号の証明書が有効か無効かを示す。無効を示された PrefixPolicyCert は削除されなければならない。

Prefix Policy Certificate Validity List TLV のフォーマットを図 9-37 に示す。

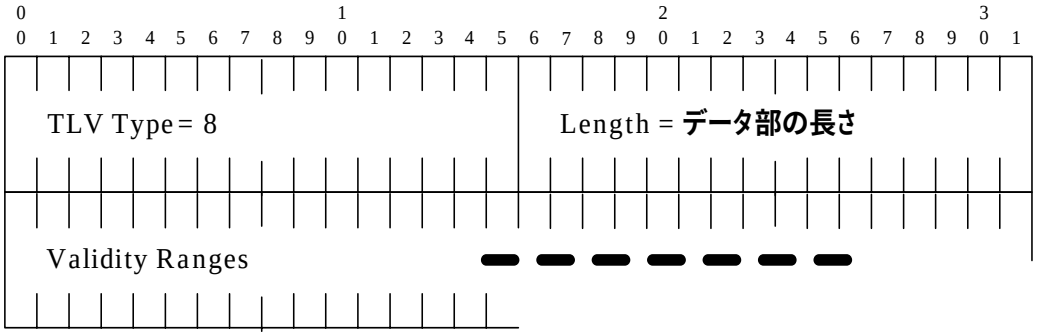


図 9-37　Prefix Policy Certificate Validity List」TLV フォーマット

「Most Recent AS Policy Certificate Uniform Resource Locator」TLV は、Origin AS が作成した最新の ASPolicyCert がある配布場所の URL を示す。

Most Recent AS Policy Certificate Uniform Resource Locator TLV のフォーマットを図 9-38 に示す。

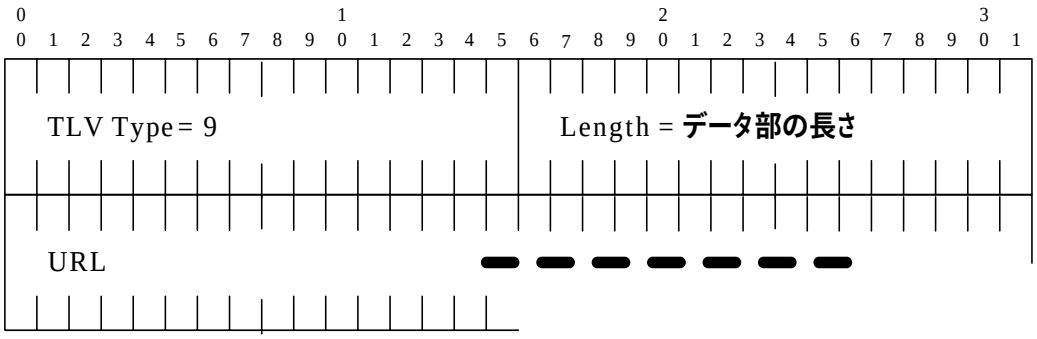


図 9-38　Most Recent AS Policy Certificate Uniform Resource Locator TLV フォーマット

「Signature」TLV は、ASPolicyCert の署名である。「Signature Type」には署名アルゴリズムが入り現在は 1 のみが定義されている。Signature Type = 1 は、[RFC3279]で定義されている sha1withRSAEncryption を利用することを表し、「Number of Issuers」は署名組織の数を示す。もし Number of Issuers > 1 である時には各組織で作られた EntityCert の PublicKey は同じでなければならない。つま

り、異なる 2 つ以上の EntityCert で一つの ASPolicyCert を署名することは出来ない。「Entity Certificate Issuer Autonomous System」は Origin AS の AS 番号が入り、「Entity Certificate Serial Number」には Origin AS の EntityCert に利用したシリアル番号が入る。「Signature」は Signature Type で生成した署名が入る。

Signature TLV のフォーマットを図 9-39 に示す。

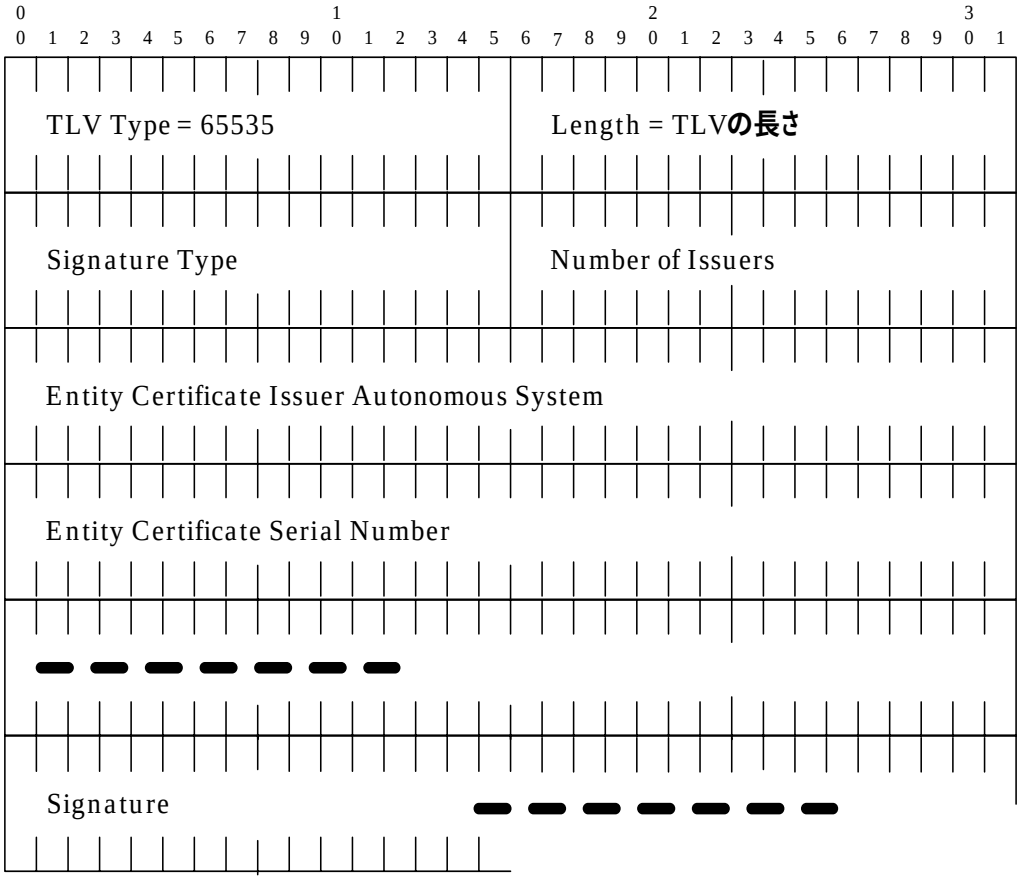


図 9-39　Signature TLV フォーマット

⑸ 各証明書の関係図

各証明書の関係図を図 9-40 に示す。

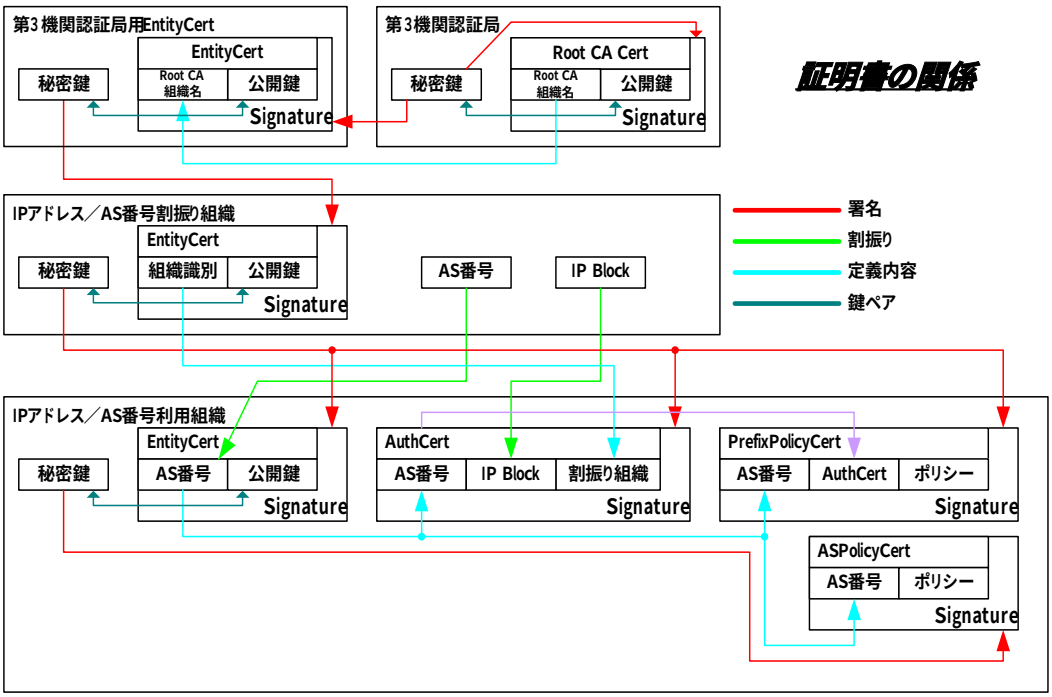


図 9-40　各証明書の関係図

9.2.1.4. 署名の確認

各署名の確認は、図 9-40「証明書の関係」の Signature の矢印を逆向きにたどり、最終的には第 3 機関の認証局の CA にたどり着き終わる。ただし、常に第 3 機関の認証局の CA で確認することは行っていない、なぜなら第 3 機関の認証局の CA まで確認するには人手を介さなければできないからである。自動化するには初めに手動で信用した EntityCert 内の情報を soBGP システムに手動で登録しておき、soBGP ではこの情報を Root して扱うことにより署名の確認が自動化される。

9.2.1.5. soBGP 動作の概略

soBGP 動作概要を図 9-41 に示す。

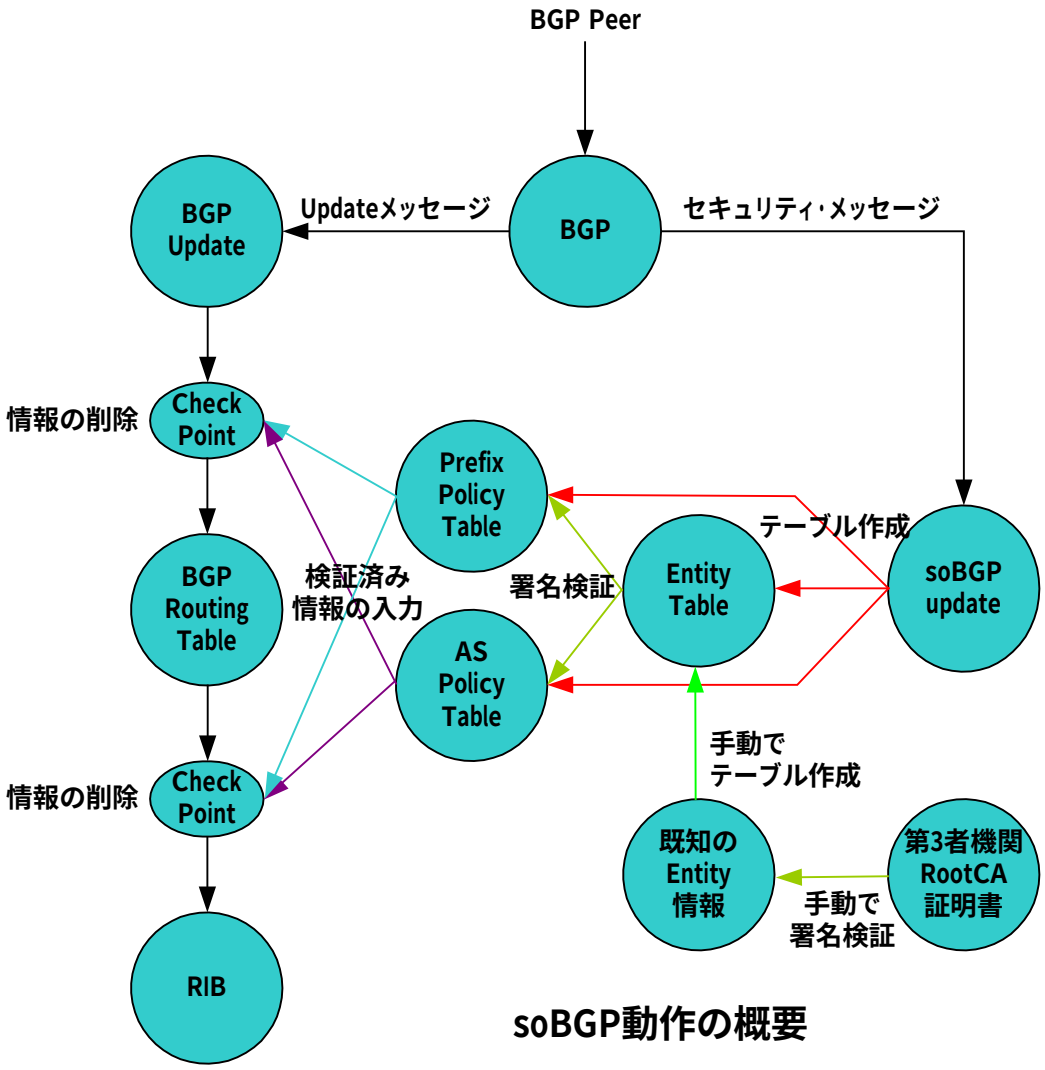


図 9-41　soBGP 動作概要

soBGP を開始する際には、既知の EntityCert(本書では RootEntityCert と呼ぶ)を取得し第 3 者機関の CA 証明書で署名の検証を行い問題がなければルータへ手動で入力しテーブルを作成する。主なデータは{Serial 番号、AS 番号、PublicKey}である。

次に、BGP Peer 間で Capability 確認を行い双方で動作可能であれば、セキュリティ・メッセージの交換を開始する。最初に交換されるセキュリティ・メッセージである Security Option を交換し、図中のどちらの Checkpoint を利用するかを決定する。BGP Routing Table 以前の Checkpoint で経路情報の確認を行う際にはすべての経路情報に関する証明書がないと Routing Table に追加されない。つまり、Routing Table 作成に時間がそれなりにかかる。BGP Routing Table 後の Checkpoint を選択した場合には、Routing Table の構

築には既存の状態と変わらないが、実際の RIB へのインストールは証明書の検証後ということになる。前者は正常な証明書がないものは Routing Table に載らないので経路情報として確認することができない、その代わり Routing Table に費やすリソースは減る。後者は正常な証明書がなくても Routing Table にのるので経路情報を確認することが可能である。その経路情報を見ながら手動で例外を作成することも可能となる。しかしルータのリソースは必要である。

次は EntityCert、PrefixPolicyCert、ASPolicyCert を受信して、到着順に署名の確認を行う。もし、必要な証明書が無い時には、その都度 BGP Peer へリクエストし必要な証明取得を試みた後、再度検証を行う。もし、検証に必要な証明書が取得できないときにはその受信した Cert は破棄される。署名の確認の取れた PrefixPolicyCert と ASPolicyCert のポリシは Checkpoint へ渡され、経路情報への確認を行い問題なければ利用を開始する。しかし、問題があった経路情報に関しては破棄される。

Checkpoint での検証例としては、ASPolicyCert が持つトランジット AS リストと非トランジット AS リストから AS 接続図を作成し、この接続図を基にして AS_PATH の検証が可能である。また、PrefixPolicyCert が持つ最大 Prefix Length では Origin AS が意図していない長さの Prefix を持った経路情報の検証が可能である。

9.2.2. IP アドレス証明書システムと JPIRR の連携モデル

本節では、JPNIC で現在運用されている IP アドレス証明書システムと JPIRR と soBGP の連携について述べる。

IP アドレス証明書システムは、JPNIC が IP アドレスブロックや AS 番号をサービス・プロバイダへ割り振りを行う際に自動的に IP アドレス情報を含んだ証明書を作成するシステムの事である。詳細は、JPNIC 資料を参照、JPIRR は前章を参照。

連携モデルを作る前に証明書に署名する際に利用される PrivateKey の保護について述べておく必要がある。soBGP の利用をするということは、すべての AS 運用者が同じセキュリティレベルにあることが要求される。これは、AS 運用者が PrivateKey を利用した署名行為を行うからである。PrivateKey が一つでも漏洩しそのまま放置されると情報を詐称する事が可能となり soBGP を利用する意味がなくなる。soBGP システム全体を保護するためにも PrivateKey を保護するための統一ポリシを作成し運用者全体が統一した PrivateKey の運

用を行うことが必要である。

ただし、各組織で PrivateKey の適切な運用を行うためには、設備投資、人的リソースの増大等いろいろな面で各組織に負担がかかる。つまりは、soBGP 導入に関して積極的になれない要素となる。各組織の運用、設備投資を最小限に抑えた形で PrivateKey 運用ポリシとシステムを構築することが重要である。

9.2.2.1. soBGP における JPNIC の役割

図 9-40「証明書の関係」にて主な役割は定義されている。「IP アドレス／AS 番号割振り組織」が JPNIC に当たるが、自身が割り振った情報に対しての署名処理と認証局の運用／管理ポリシの作成が主な役割となる。

9.2.2.2. 連携システム概要

ここでは JPNIC で現行動いている IP レジストリシステムと soBGP で必要とされる証明書システムの連携をまとめる。

連携システムの目的は正確な情報(IP レジストリシステムに登録されている情報)を元に EntityCert 証明書や署名した TLV を Secure な環境下で効率よく作成し、Routing システムへ渡す事、Routing システムからの証明書や署名確認の問い合わせに対して迅速に応答する事である。

連携システムは、IP アドレス認証局、IP アドレス証明書システム、AS 内証明書システム、AS 内認証局が soBGP に関わる証明書や署名つき TLV を作成するために必要となる。また、JPIRR への情報を提供することにより JPIRR に登録されている情報の検証を行う事も考えられる。本調査では、認証局としてのポリシを述べる事はしないが、本調査にある連携システムでは、全ての認証局運営組織は同じセキュリティレベルが定義されているポリシを共通で利用し認証局運用する事がセキュリティ上重要である。理由は、署名されたデータは Routing システム介して全ての組織に広告されるためである。これは、経路制御システムで署名つき TLV を交換している組織は全て同一セキュリティドメインであるといえる。

連携システム概略図を図 9-42 に示す。

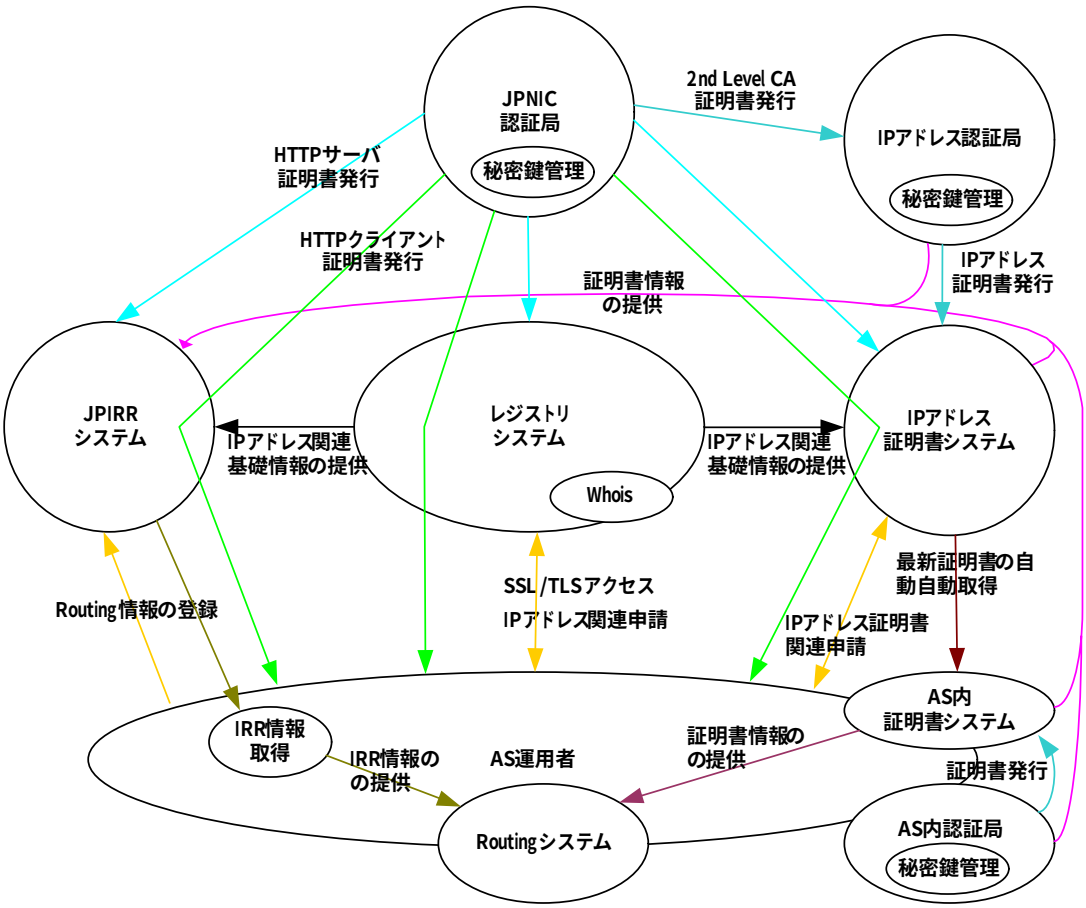


図 9-42　連携システム概略図

⑴ IP アドレス認証局

IP アドレス認証局は、JPNIC にて管理／運用され、その機能は JPNIC が割り振り／割り当てを行った IP アドレスブロックや AS 番号等の情報を含む CSR (EntityCert)や TLV 群(AuthCert, PrefixPolicyCert)への署名である。

⑵ IP アドレス証明書システム

IP アドレス証明書システムは、JPNIC にて管理／運用され、その主な機能は

AS 運用者の認証処理、AS 運用者からの証明書もしくは TLV 群への署名要求を受け付け、IP アドレス認証局への橋渡しを行い、署名された物を申請組織へ返送する。また、作成された署名物は必要であれば JPIRR 等の他のレジストリシステムへ配布することも考えられる。

⑶ AS 内証明書システム

AS 内証明書システムは、各 AS 運用者により管理／運用され、その主な機能は AS 番号等を含む CSR(EntityCert)や自身が再割り振り／割り当てを行った IP アドレスブロック情報を含む TLV 群(AuthCert, PrefixPolicyCert, ASPolicyCert)の作成と下位組織からの署名申請を受け、AS 内認証局への橋渡しを行い、署名された物を申請組織へ返送する。また、作成された署名物は必要であれば JPIRR 等の他のレジストリ・システムへ配布することも考えられる。

⑷ AS 内認証局

AS 内認証局は、各 AS 運用者により管理／運営され、その機能は AS 番号等の情報を含む CSR (EntityCert)や TLV 群(AuthCert, PrefixPolicyCert)への署名である。

9.2.2.3. soBGP 初期設定概要

利用を開始する際に必要なのは、基本となる最上位 EntityCert 証明書(RootEntityCert)を作成することである。RootEntityCert を作成するのに適当と思われるのは、RIR 等の権威ある機関で、ここでは JPNIC が RootEntityCert を作成し運用すると仮定し、第 3 認証局としては JPNIC 認証局／JPNIC IP アドレス認証局を利用する。

新たに RootEntityCert を作成するに当たり、JPNIC は RootEntityCert で利用する PublicKey/PrivateKey のペアを作成し[RFC3280]に準拠した CSR を作成、AS 番号は[RFC3779]に準拠して拡張領域に定義する。CSR には新たに作成した PublicKey を含め JPNIC IP アドレス認証局の PrivateKey で署名し、証明書(RootEntityCert)として発行し、一般公開する。

AS 運用者は公開された RootEntityCert を入手し、JPNIC IP アドレス認証局が発行している CA 証明書にて RootEntityCert が改竄されていないか署名の検証を行う。問題無ければ RootEntityCert 内の SubjectAltName、シリアル番号、AS 番号、PublicKey をルータへ設定する。

これで、soBGP を利用するための準備が整ったことになる。

9.2.2.4. 自 AS で利用する EntityCert 作成概要

AS 内証明書システムにて PublicKey/PrivateKey 生成後 EntityCert CSR を作成し IP アドレス証明書システムへ IP アドレス認証局の署名を申請する。受け取った IP アドレス証明書システムは、レジストリシステム等を利用して CSR の内容を確認、問題無ければ IP アドレス認証局へ CSR を転送し、IP アドレス認証局の PrivateKey にて署名された証明書が返信されるのを待つ。返信された証明書はそのまま申請者へ送信される。

証明書を受信した AS 内証明書システムは EntityCert をセキュリティ・メッセージにてルータへ広告する。この時、受信したルータは RootEntityCert を利用して送られてきた EntityCert の署名を確認問題が無ければ SubjectAltName、シリアル番号、AS 番号、PublicKey を自身のテーブルに登録する。

この時点でルータ内の EntityCert テーブルには、RootEntityCert と自身の EntityCert の 2 つが登録されていることになる。

対となる PrivateKey は AS 内認証局にて管理し、AS 内証明書システムの要求にしたがい必要な署名を行ために利用する。

EntityCert 作成手順概要を図 9-43 に示す。

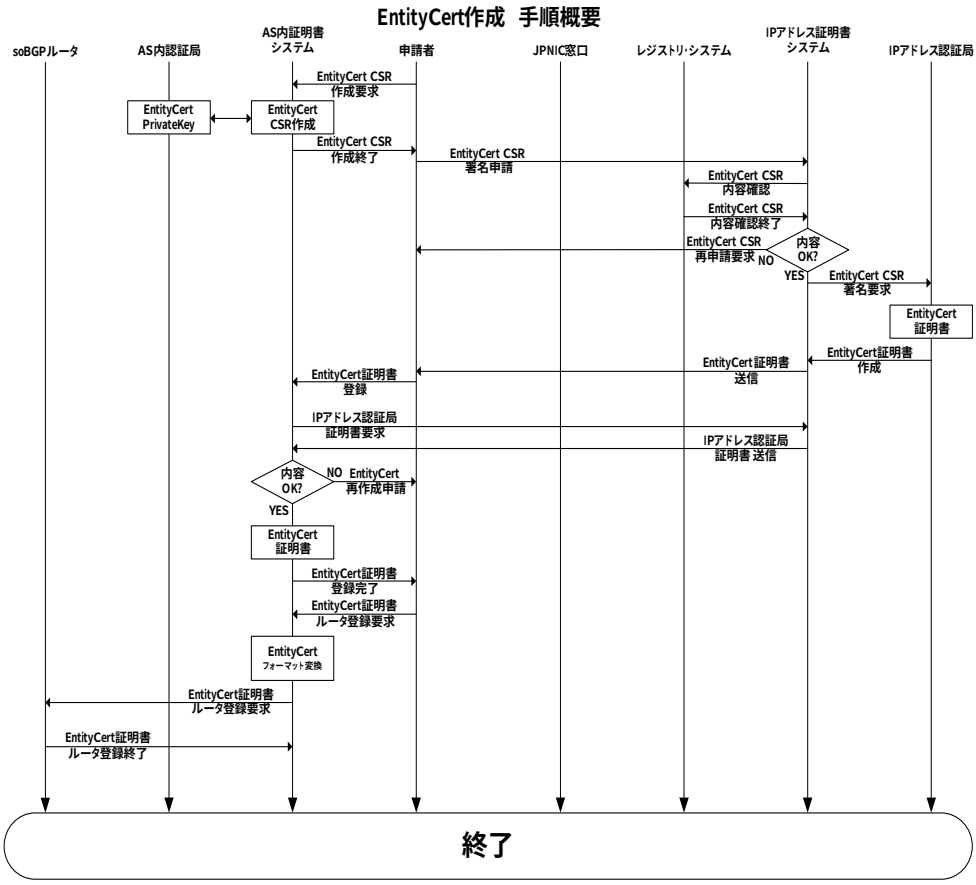


図 9-43　EntityCert 作成手順概要

9.2.2.5. 自 AS 用の PrefixPolicyCert 作成概要

AS 内証明システムに JPNIC から割振りを受けた IP アドレスブロックをデータに持つ AuthCert TLV を作成するように指示をだす。作成された TLV を IP アドレス証明書システムへ IP アドレス認証局の署名を申請する。IP アドレス証明書システムは TLV の内容をレジストリシステム等で確認を行い問題が無ければ、IP アドレス認証局に対して TLV を送信し、受け取った認証局は署名し、IP アドレス証明書システムへ返送される。署名つき TLV 受け取った IP アドレス証明書システムは、AS 内証明システムへ返送する。署名つき TLV を受け取った AS 内証明システムは署名を確認し、問題が無ければ次に PrefixPolicyCert TLV を作成し再度 AuthCert と同様なプロセスをたどり署名つき PrefixPolicyCert TLV をセキュリティ・メッセージにてルータへ広告する。

受け取ったルータは TLV 内の署名フィールドにある署名した EntityCert もしくは

RootEntityCert にて検証を行い問題が無ければ、AuthCert を取り出し AuthCert の署名を確認し問題が無ければ、PrefixPolicy テーブルに TLV 内の情報を追加する。

AuthCert(AC)TLV & PrefixPolicyCert(PP)TLV 作成手順概要を図 9-44 に示す。

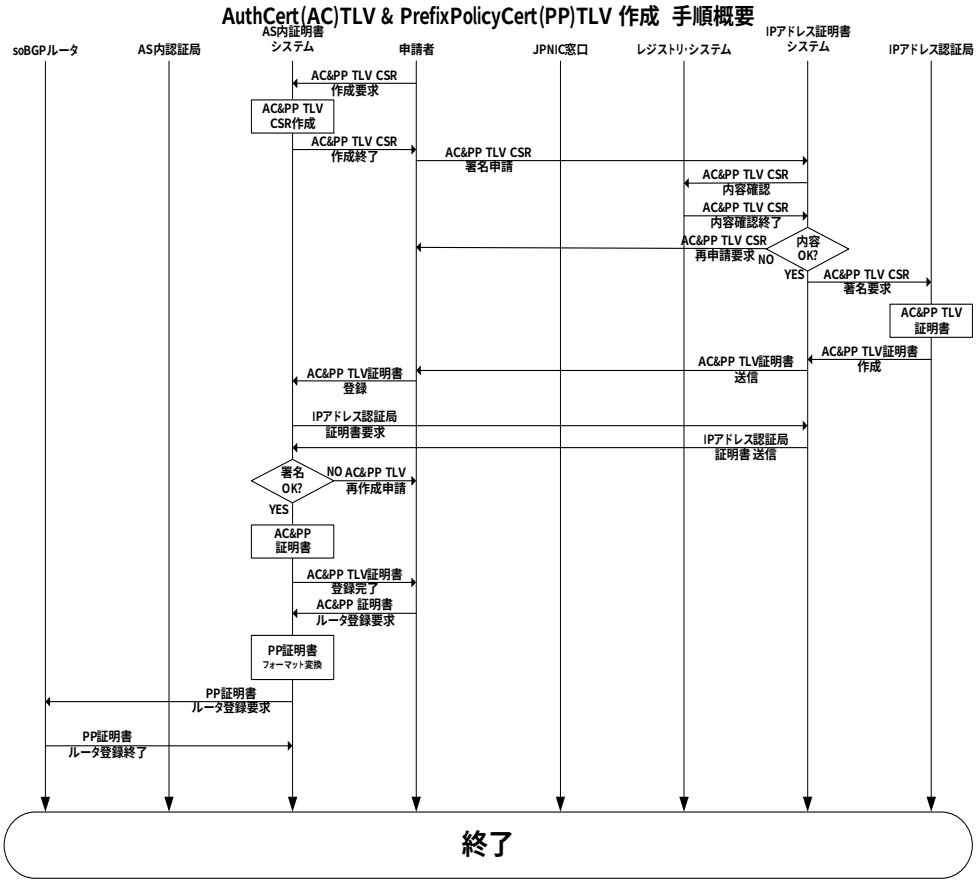


図 9-44　AuthCert(AC)TLV & PrefixPolicyCert(PP)TLV 作成手順概要

9.2.2.6. 自 AS 用の ASPolicyCert 作成概要

AS 内証明システムに ASPolicyCert TLV 作成の指示を出す。作成された TLV を自 AS 認証局へ送信し、認証局で署名後 AS 内証明システムに返信する。受け取った AS 内証明システムは署名を検証後、問題が無ければセキュリティ・メッセージを利用してルータへ ASPolicyCert を広告する。

受け取ったルータは EntityCert で署名を検証し問題が無ければ ASPolicy テーブルへ TLV 内の情報を追加する。

AS policy(AP)TLV 作成手順概要を図 9-45 に示す。

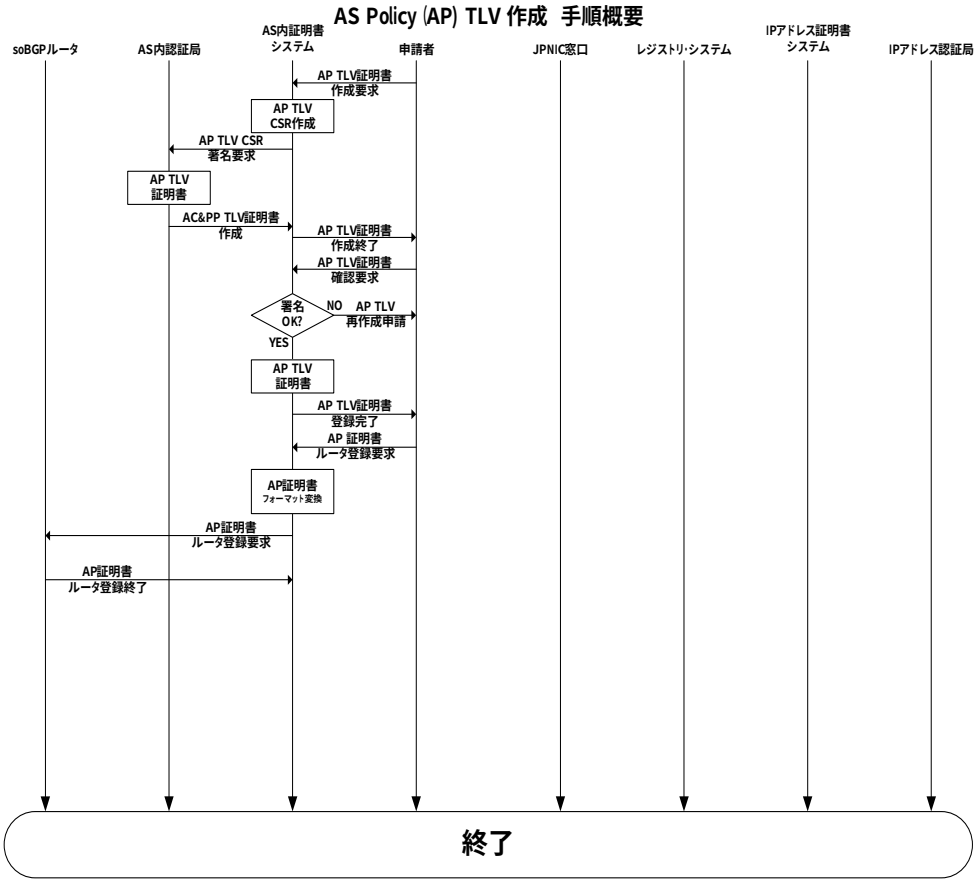


図 9-45　AS policy(AP)TLV 作成手順概要

この時点でルータには、RootEntityCert、EntityCert、PrefixPolicyCert、ASPolicyCert の情報が追加されている。この状態で BGP Update で送られてきた経路情報を Checkpoint で確認可能な状態になったことになる。

9.2.2.7. EntityCert の破棄について

署名検証後は、必ず CRL の検証を行う。EntityCert の破棄については EntityCert 内の URL を参照し最新の CRL を取得後行われ、破棄が確認された EntityCert に関してはテーブルから削除される。

9.2.2.8. PrefixPolicy＆AuthCert の破棄について

特定の PrefixPolicy や AuthCert の破棄を行う場合には ASPolicyCert 内に定義される各々の Validity List を確認して破棄マークがとなっている物に関して PrefixPolicy テーブルから削除が行われる。

9.2.3. その他

すでに記述したが、soBGP の TLV のフォーマットには URL が入るフィールドが有る。これは外部の証明書リポジトリをアクセスするために利用されるが、現時点では仕様が明確になっていないので今回は記述しない。

以上で連携システムの概略に関しての説明を終える。次節では、soBGP とは別なアプローチで経路情報の保護を行う仕組みを提供する S-BGP に関して述べる。

9.3. S-BGP の概要とモデル

本節では、経路交換システムを保護するため提案である S-BGP について、その概要と JPNIC で運用が考えられている IP アドレス証明書システムと JPIRR システムとの連携モデルについて述べる。

9.3.1. S-BGP 概要

S-BGP の目的は不正経路情報の発見、除去を自動化する事にある。実現方法としては、新たに定義する BGP Path Attribute を利用して RA 証明書(後述)を組織間で交換し、受信した証明書を検証することにより経路情報の真偽を確認することが可能となり、偽情報を除去する事が実現する。証明書の配布→受信→署名検証→証明書の登録／偽情報の排除までを S-BGP の枠組みで自動化する。

S-BGP で問題なのは、証明書情報を BGP とは別な仕組みで交換され、その交換方法には時間がかかることである、つまり新たに交換したい IP アドレスブロックに関して様々な前処理をし、証明書情報を全ての運用者に配り終わった後で広告を開始しないと新たに広告した IP アドレスブロックは破棄されてしまう可能性がある。

S-BGP では、BGP セッション開始前の接続先の確認と通信路の保護もその枠組みの中に含まれ、IPsec を利用するように定義されている。

S-BGP 概略を図 9-46 で示す。

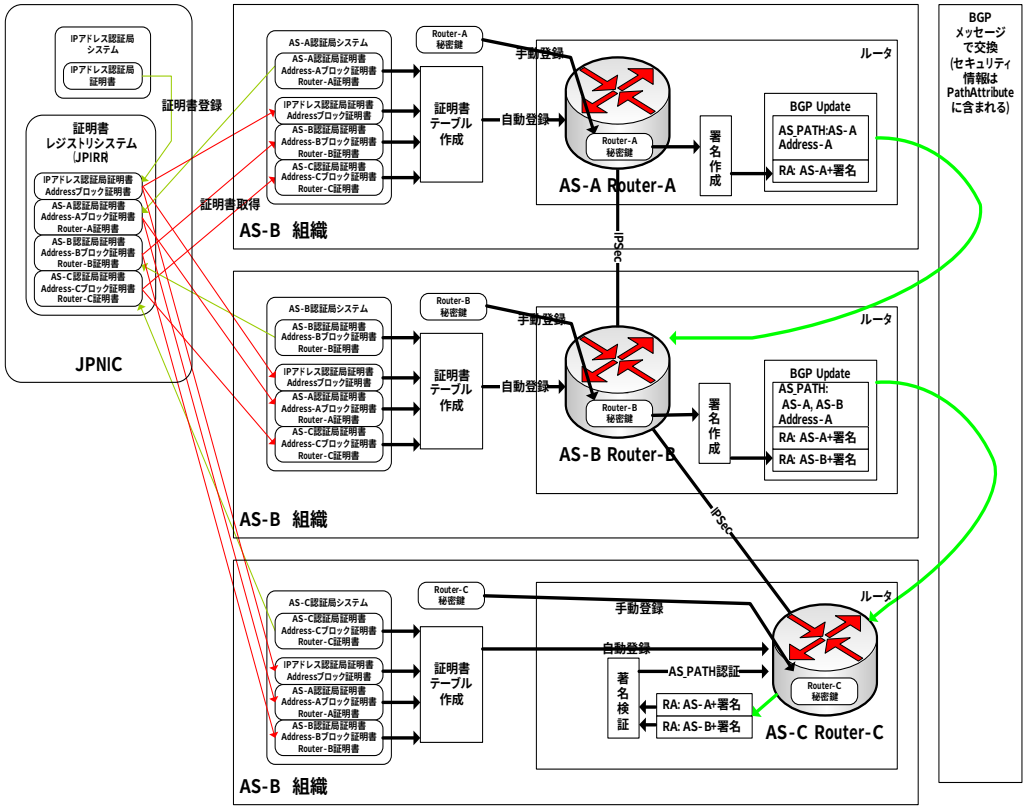


図 9-46　S-BGP 概略図

9.3.1.1. BGP Path Attribute について

BGP Update の最大長は、4096 バイトである。新たに定義する Path Attribute を利用するにしてもこの制限を超える事は出来ない。S-BGP の証明書情報はこの大きさに収まるサイズにしなくてはならない。

Path Attribute には、Route Attestations(後述)と Address Attestations(後述)を含んでいる。

BGP Path Attribue のエンコーディングを図 9-47 で示す。

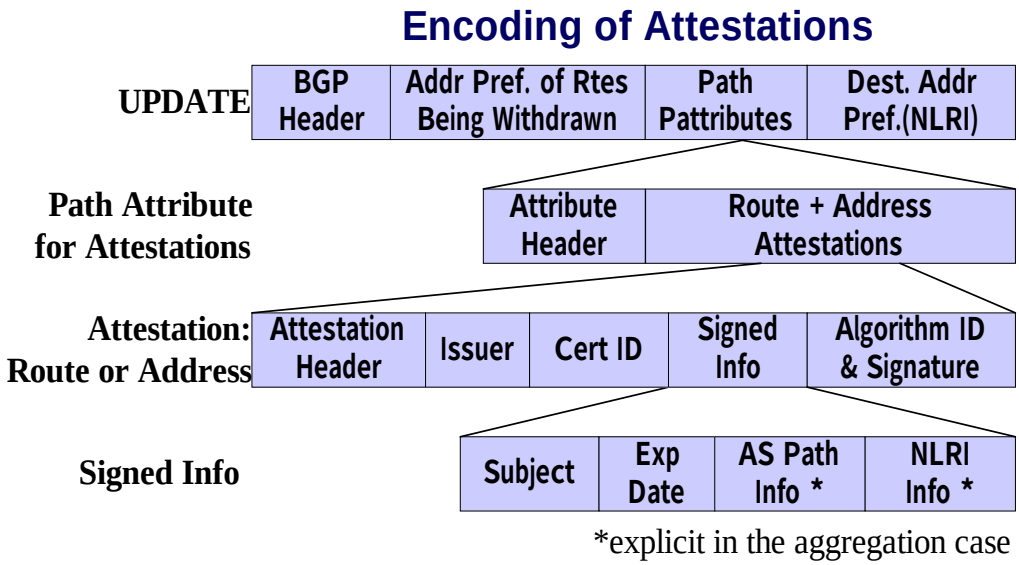


図 9-47　BGP Path Attribue のエンコーディング

実際の Address もしくは Route Attestation メッセージ･フォーマットを図 9-48 に示す。

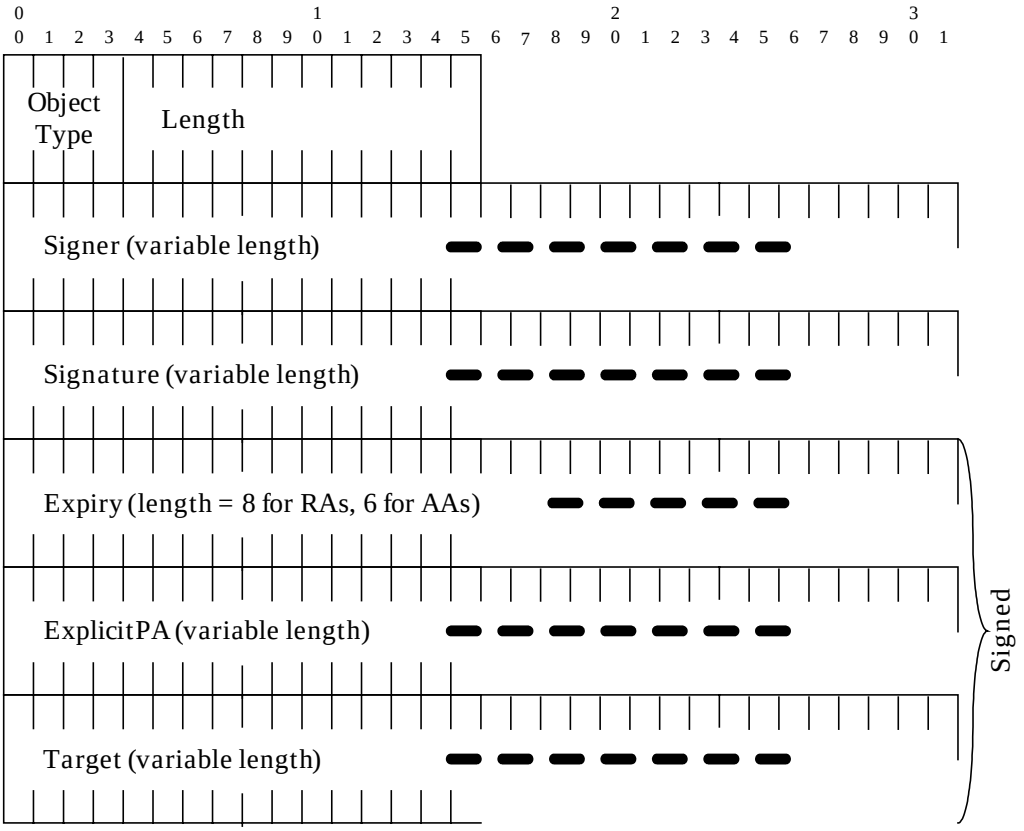


図 9-48　Address もしくは Route Attestation フォーマット

メッセージの基本は Part Code+Length であり、Code は 4 ビット、Length は 12 ビットとなり、合計 16 ビット(2 オクテット)となる。

Part Code と Length のフォーマットを図 9-49 に示す。

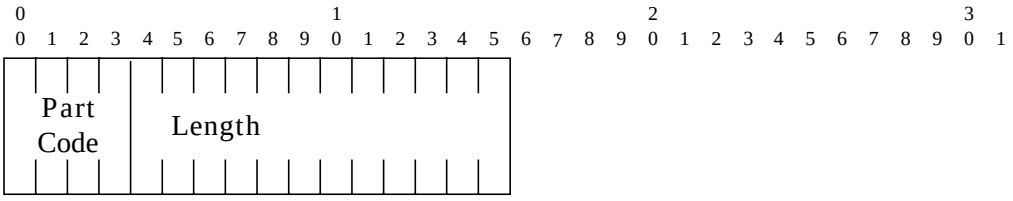


図 9-49　Part Code と Length のフォーマット

⑴ Object Type

証明したい情報の種別を示される。Code が 8 の時の種別は、「Route Attestation(RA)」、Code が9の時の種別は「Address Attestation(AA)」、Code が 14 の時は続くデータは「Extract File Authenticator」を示す。

Object Type のフォーマットを図 9-50 に示す。

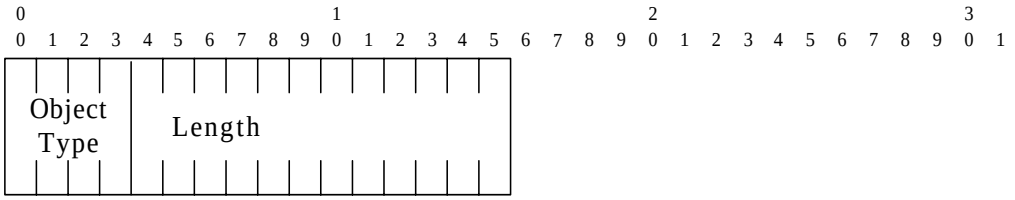


図 9-50　Object Type フォーマット

⑵ Signer

署名の際に利用したデータが示される。利用 Code は1、SignerLength には SignerData の長さ+2 オクテット、AFI は[IANA-AFI]にある値を指定する。SignerData には AFI に対応した情報を入れる。

Signer のフォーマットを図 9-51 に示す。

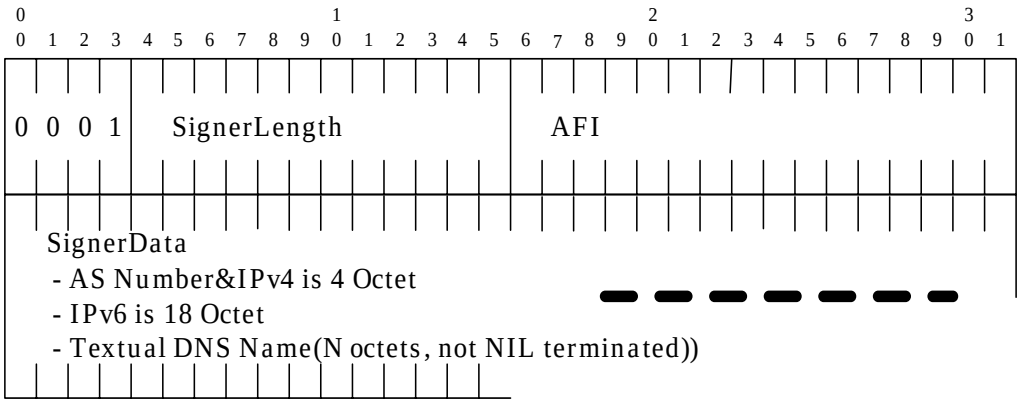


図 9-51　Signer のフォーマット

⑶ Signature

SignerData を基にした署名が示される。Code は 2、SignatureLength はデータの長さ、Signature Algorithm ID(SigAlgID)は署名を作成したときの方法が表され、[IANA-SAN]に有る値をとる。現在は、3(DSA/SHA1[RFC2536[7]、DSA、SHA-1])を使用する。KeyId は複数の認証局により SignerData が署名されたときに、どの認証局かを判別するために利用され、KeyId に対応する証明書内の項目は SubjectKeyIdentifier を利用する。CoverageLen は CoverageMask の長さを指定する。Object Type が AA の場合には CoverageLen は 0 になる。Object Type が RA の時 CoverageMask を利用し署名したときの PATH 属性の状態を記録する。

Signature は SigAlgID で指定された方法で作成された署名が入る。

Signature のフォーマットを図 9-52 に示す。

[7] DSA KEYs and SIGs in the Domain Name System (DNS) (RFC2536)
http://www.ietf.org/rfc/rfc2536.txt

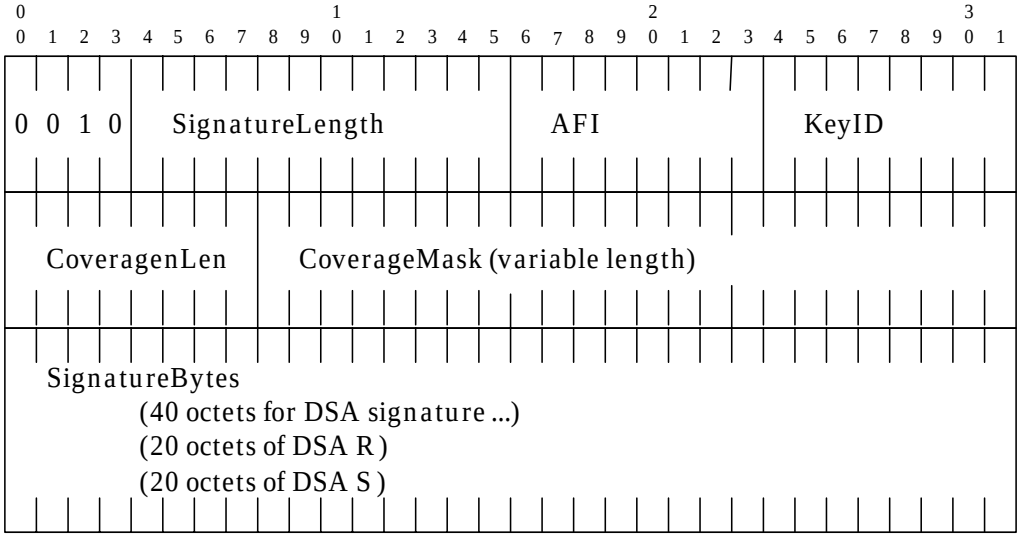
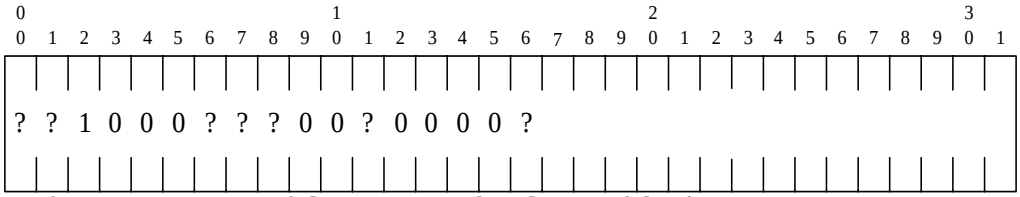


図 9-52　Signature のフォーマット



0: NLRI or MP_REACH_NLRI; 1: ORIGIN; 2: AS PATH;
6: ATOMIC AGGREGATE; 7: AGGREGATOR; 8: COMMUNITIES
11: DPA; 16: EXTENDED COMMUNITY; ... (others to be defined)

図 9-53　CoverageMask フォーマット

⑷ Expiry

証明書の有効期限が示される。Code は 3、ExpiryLength は、データの長さを表し Object Type が AA の時は 4、RA の時は 6 である。Year には西暦を、Month には月を Day には日を入れる。RA の時には A ビットと RASC がさらに必要になる。A ビットは Route の集約が行われた事を表し、RASC は集約が行われた個数を示す。

Expiry のフォーマットを図 9-54 に示す。

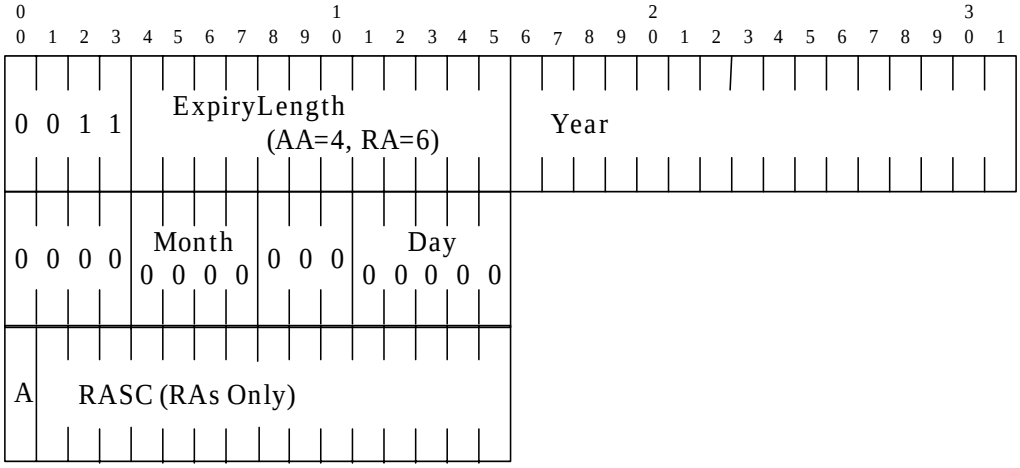


図 9-54　Expiry フォーマット

⑸ ExplicitPA

AS 組織では、複数の下位組織からの IP アドレスブロックを集約し一つの大きい IP アドレスブロックと新たな Path Attribute を広告するケースがある。集約以前の Path Attribute を保存する際に利用される。Code は 4、ExplicitPALength はデータの長さを表す。

ExplicitPA のフォーマットを図 9-55 に示す。

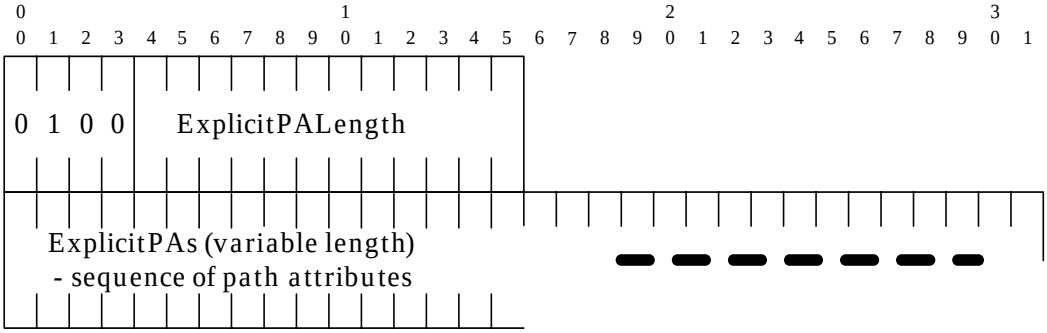


図 9-55　ExplicitPA のフォーマット

IP アドレス Prefix は、対照となる IP アドレスブロックが表される。AddressFamilyIndicator は [IANA-AFI] を利用し、SAFI へは [IANA-SAFI][RFC2858]を利用する。もし、RA 用であれば MaxPrefixLen は 0 がセットされる。AA 用であるときには受信した IP アドレスブロックに関して受け入れ可能な Prefix の最大長を設定する。もし、この Prefix 最大長を超えた IP アドレスブロックを受信した際には、その IP アドレスブロックは破棄される。

Prefix Encoding のフォーマットを図 9-56 で示す。

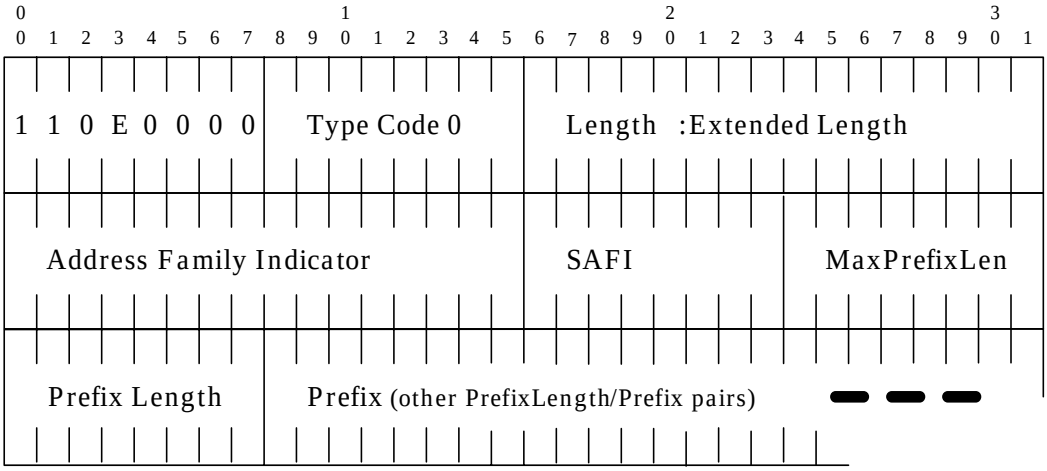


図 9-56　Prefix Encoding のフォーマット

(1) Target

メッセージが RA の時には、AS_PATH に追加した AS 番号を示し、AA の時には IP アドレスブロックの Origin AS を示している。Code は 5、TargetLength にはデータの長さ、AFI は AS 番号を示す 18 ([IANA-AFI]を利用) を指定する。その後一つ以上の AS 番号が続く。

Target Part のフォーマットを図 9-57 に示す。

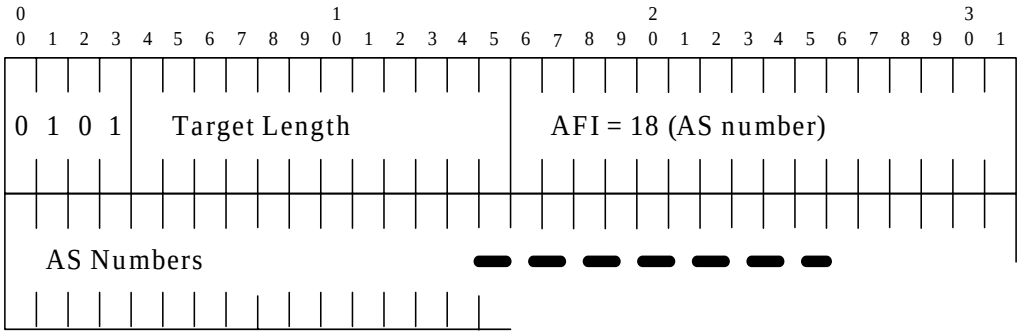


図 9-57　Target Part のフォーマット

9.3.1.2. S-BGP の情報信頼モデル

S-BGP は、公開鍵基盤(PKI)の枠組みを用いて、利用する証明書の信頼性を確保する。実際の確認方法に関しては RFC3280 に従い、証明書の参照先には証明書レジストリ(後述)を利用する。

S-BGP は、IANA 認証局の Root 証明書を全ての AS 運用組織が信用することで成り立つ。また、各組織の認証局のセキュリティ運用ポリシは IANA 認証局と同等もしくは、より厳しいものでなくてはならない。セキュリティポリシが IANA 認証局のものより下回る場合秘密鍵漏洩等の事故による重大な事故が起こる可能性が増大する。

9.3.1.3. S-BGP で利用する証明書

S-BGP で利用される証明書は、「運用組織の CA 証明書」、「RouterID-CA 証明書」、「Address Attestations」そして「Route Attestation」の 4 種類ある。

⑴ Address Attestations に関して

Address Attestations は、Origin AS と IP アドレスブロックを示し、自組織で作成する。

Address Attestations を作成するには、[RFC3280]を利用して証明書基本フォーマットを作成、[RFC3779]を利用して「AS 番号」と「IP アドレスブロック」を拡張領域へ書き込む。証明書は 、[IANA-SAN[8]]にある 3 番(SHA-1/DSA)を使用し、運用組織の CA の PrivateKey を利用して署名する。

署名が終了した証明書は、証明書リポジトリシステムへ登録し公開する。

⑵ Route Attestation に関して

Route Attestation は自組織が AS_PATH に自 AS を追加したことを示し、自組織で作成する。

Route Attestations を作成するには、BGP Path Attribute の Object Type=3 に沿ってデータを構築し[IANA-SAN]にある 3 番(SHA-1/DSA)を使用し機器用の RouterID-CA の PrivateKey を利用して署名を作成し「Signature」フィールドへ埋め込む。出来たデータを Path Attribute に追加して BGP Update を再構築し Next Hop AS へ送信する。

各 AS 単位で同様な動作を行い、AS_PATH に AS を追加すると共に RA を追加する。最終的にあて先 AS 番号を持つ経路交換機器が受け取った時に RA の署名を順に検証することで AS_PATH が正しい事を証明出来る。

受信した Origin AS 番号と IP アドレス・プリフィクスに関しては AA を用いて検証する事で正しい事を証明する。

この 2 つの検証結果が良好な場合に限り経路情報は改竄されていないといえる。

8 SIG (0) ALGORITHM NUMBERS
http://www.iana.org/assignments/sig-alg-numbers

⑶ RouterID-CA 証明書に関して

RouterID-CA 証明書は経路制御機器で署名した RA 証明書を検証するために利用し、AS_PATH に AS 番号を追加する経路制御機器で作成する。この証明書は単一 AS にひとつとは限らない、複数の経路制御機器が AS_PATH へ AS 番号を追加する可能性がある時には複数の RouterID-CA 証明書を作成し、どの機器で AS 番号を AS_PATH へ追加したかを検証可能にすることが必要である。

RouterID-CA 証明書を作成するには、[RFC3280]を利用して証明書基本フォーマットを作成、[RFC3779]を利用して「AS 番号」を拡張領域へ書き込む。証明書は [IANA-SAN] にある 3 番(SHA-1/DSA)を使用し、運用組織の CA の PrivateKey を利用して署名する。

署名が終了した証明書は、証明書リポジトリシステムへ登録し公開する。

⑷ 運用組織のＣA証明書に関して

運用組織の CA 証明書は自組織が AS を運用していることを示し、自組織で CSR を作成する。

運用組織の CA 証明書を作成するには、RFC3280 を利用して証明書基本フォーマットを作成、RFC3779 を利用して「AS 番号」と「IP アドレスブロック」を拡張領域へ書き込む。証明書は [IANA-SAN]にある 3 番(SHA-1/DSA)を使用し、上位の割り振り／割り当て組織 CA の PrivateKey を利用して署名する。

署名が終了した証明書は、証明書リポジトリシステムへ登録し公開する。

⑸ 各証明書の関係図

各証明書の関係を図 9-58 に示す。

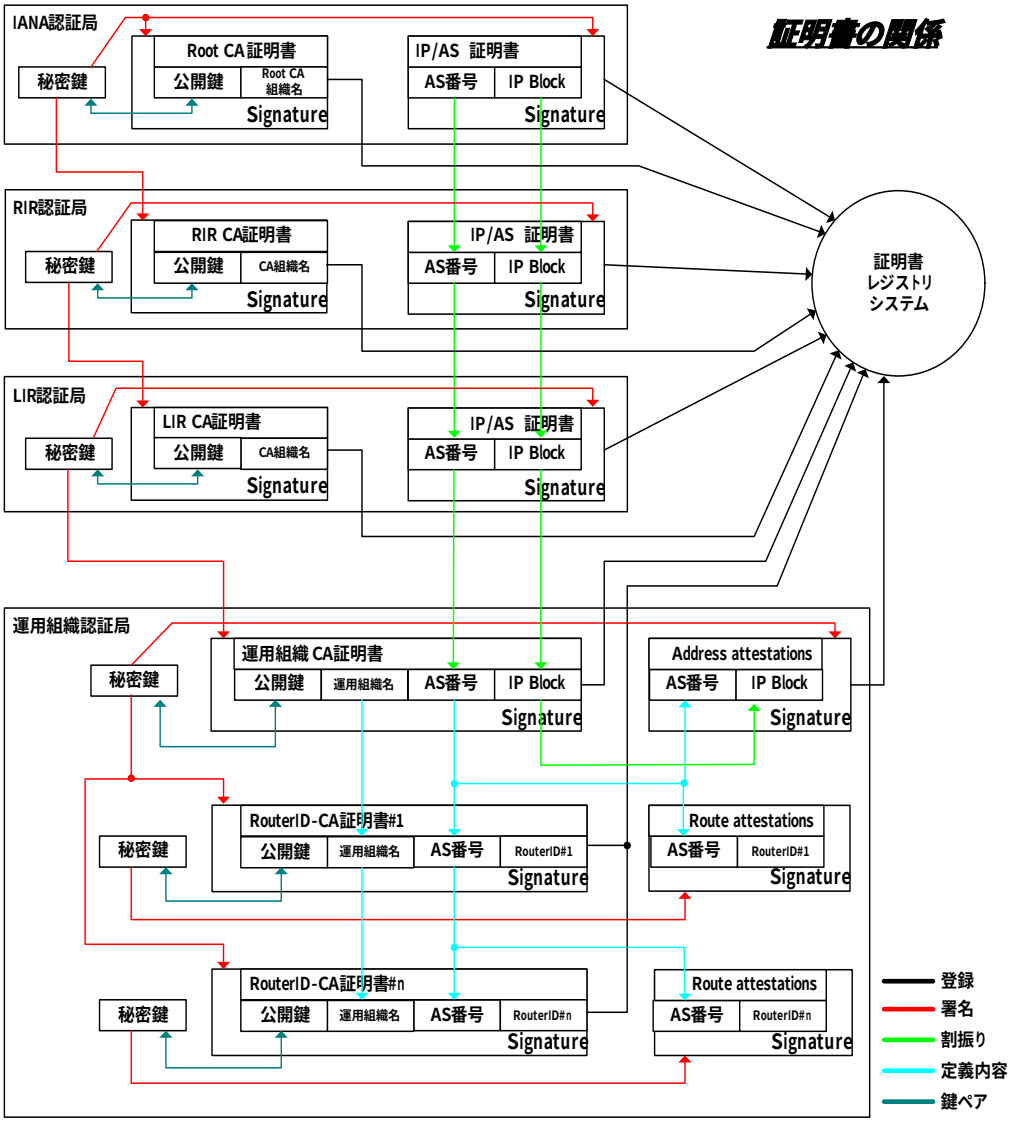


図 9-58 各証明書の関係

9.3.1.4. 署名の確認

各署名の確認は、「証明書の関係」図の Signature の矢印を逆向きにたどり、最終的には IANA 認証局の CA 証明書にたどり着き終わる。

9.3.1.5. S-BGP 動作の概略

S-BGP の動作概要を図 9-59 に示す。

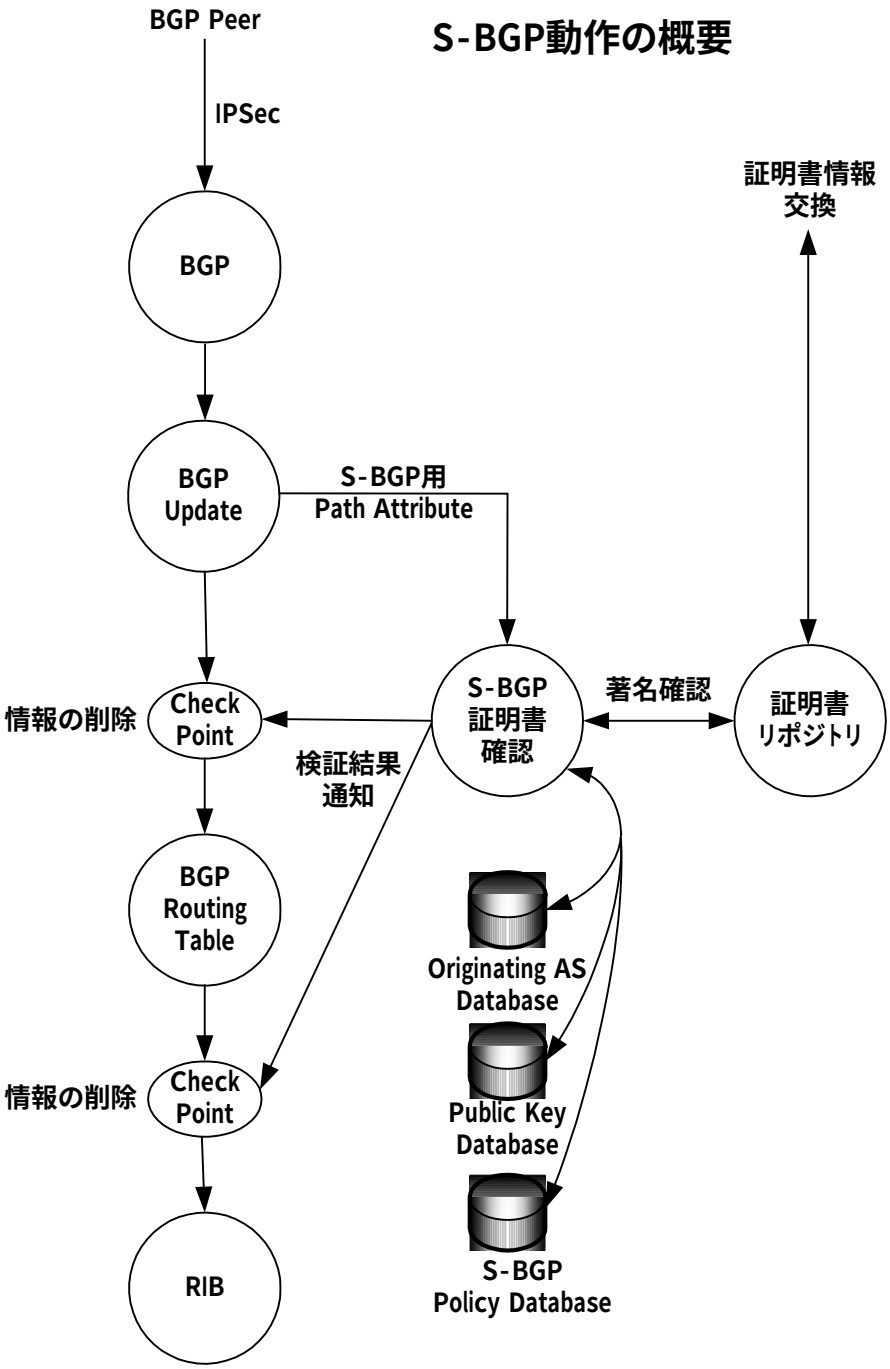


図 9-59　S-BGP の動作概要

S-BGP システムでは、初めに自組織の証明書情報と証明書破棄ﾘｽﾄ(CRL)の公開と他組織の証明書情報と CRL を取得し、取得した証明書情報から 3 種類の Database を作成する。一つ目は、「Originating AS Database」、この Database は「Address Attestations」証明書を検証後、証明書内から Origin AS 番号と IP アドレス Prefix を取り出して作成する。二つ目は「Public Key Database」、この Database は様々な証明書から作成され、証明書検証後の証明書内に有る AS 番号もしくは運用組織と PublicKey を取り出して作成する。三つ目は、「S-BGP Policy Database」、この Database は AS を運用する上でのﾎﾟﾘｼをまとめた物である。この 3 種類のデータを整形し経路交換機器へ設定する。証明書情報に関する処理が終了した後、S-BGP で利用する通信路の確立処理を行う。

経路交換機器間で IPsec-ESP [RFC2406[9]]にて接続先の認証した後暗号化通信を開始する。

BGP セッションが確立し、経路交換が開始されると、「Route Attestation」を含んだ BGP Update を受け取とった経路交換機器は自身の AS 番号を AS_PATH へ追加すると共に RA を Path Attribute へ追加して次の AS へ転送する。宛先となっている AS が BGP Update を受け取ると全ての RA 情報を検証し問題なければ、ルーティングテーブルへ登録する。

Origin AS と IP アドレス Prefix の確認は BGP Update で受け取った Origin AS と IP アドレス Prefix を「Address Attestations」内にある情報と比較し同じであれば経路情報は正常であることを表す。

9.3.2. IP アドレス証明書システムと JPIRR の連携モデル

本節では、JPNIC で現在運用されている IP アドレス証明書システムと JPIRR と S-BGP の連携について述べる。

IP アドレス証明書システムは、JPNIC が IP アドレスブロックや AS 番号をサービス･プロバイダへ割り振りを行う際に自動的に証明書を作成するシステムの事である。

[9] IP Encapsulating Security Payload (ESP) (RFC2406)
http://www.ietf.org/rfc/rfc2536.txt

連携モデルを作る前に証明書に署名する際に利用される PrivateKey の保護について述べておく必要がある。S-BGP の利用をするということは、すべての AS 運用者が同じセキュリティレベルにあることが要求される。これは AS 運用者が PrivateKey を利用した署名活動を行うからである。PrivateKey が一つでも漏洩しそのまま放置されると情報を詐称する事が可能となり S-BGP を利用する意味がなくなる。S-BGP システム全体を保護するためにも PrivateKey を保護するための統一ポリシを作成し運用者全体が統一した PrivateKey の運用を行うことが必要である。

ただし、各組織で PrivateKey の適切な運用を行うためには、設備投資、人的リソースの増大等いろいろな面で各組織に負担がかかる。つまりは、S-BGP 導入に関して後ろ向きの要素となる。各組織の運用,設備投資を最小限に抑えた形で PrivateKey 運用ポリシとシステムを構築することが重要である。

9.3.2.1. S-BGP における JPNIC の役割

図 9-58「証明書の関係」にて主な役割は定義されている。「IP アドレス／AS 番号割振り組織」が JPNIC に当たるが、自身が割り振った情報に対しての署名処理と認証局の運用／管理ポリシの作成が主な役割となる。

9.3.2.2. 連携システム概要

ここでは、JPNIC で現行稼動している IP レジストリシステムと S-BGP で必要とされる証明書システムの連携をまとめる。

連携システムの目的は正確な情報（IP レジストリシステムに登録されている情報）を元に運用組織で利用する証明書を Secure な環境下で効率よく作成し経路制御システムや証明書レジストリ・システムへ提供する事を目的としている。

連携システムは、IP アドレス認証局、IP アドレス証明書システム、AS 内証明書システム、AS 内認証局が S-BGP に関わる証明者、AA や RA を作成するために必要となる。また、JPIRR へ情報を提供する事により JPIRR に登録されている情報の検証を行うことも考えられる。本調査では認証局としてのポリシを述べる事はしないが、本連携システムでは全ての認証局運営組織は同じセキュリティレベルが定義されているポリシを共通で利用し認証局

運用する事がセキュリティ上重要である。理由は署名されたデータは Routing システムや証明書レジストリを介して全ての組織に広告されるためである。これは、システムで署名つき TLV を交換している組織は全て同一セキュリティドメインであるといえる。

連携システム概略を図 9-60 に示す。

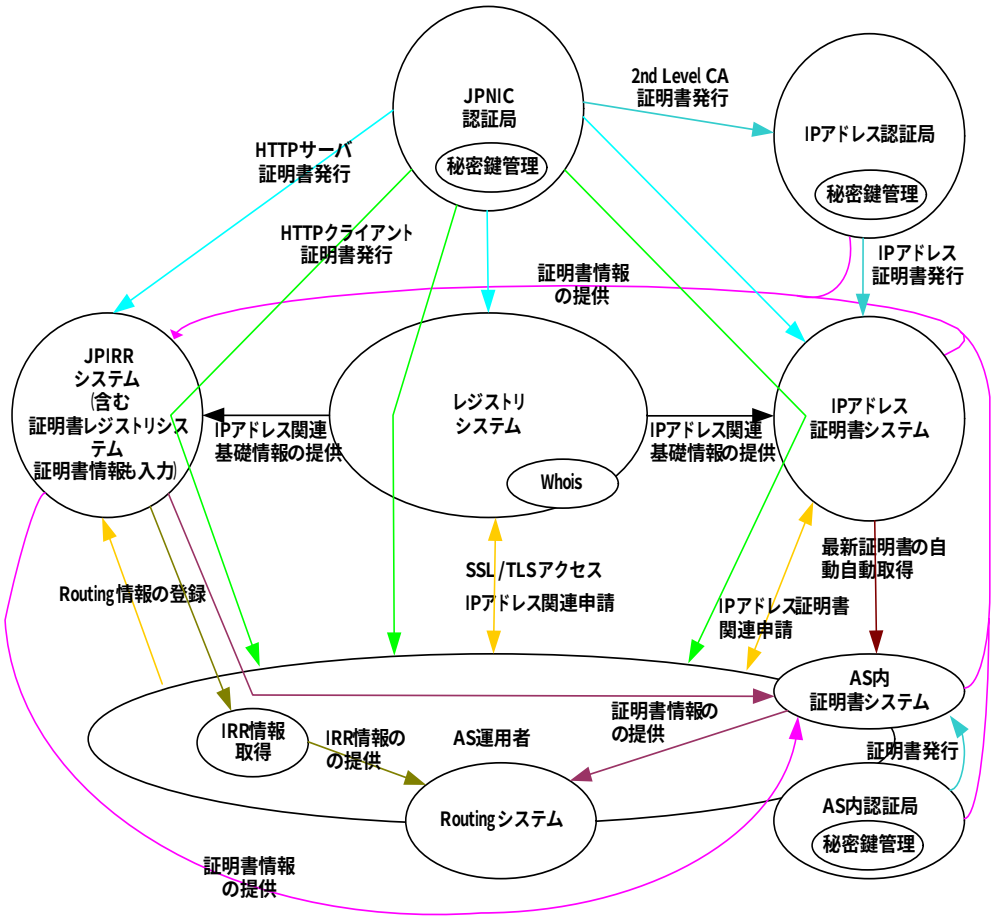


図 9-60　連携システム概略図

(1) 証明書レジストリ・システム

証明書レジストリ・システムは、S-BGP で利用する必要情報と公開鍵を公開するためのシステムである。公開する証明書の種類は、運用組織の CA 証明書, RouterID-CA#n 証明書, Address Attestations 等があげられる。

⑵ IP アドレス認証局

IP アドレス認証局は、JPNIC にて管理／運用され、その機能は JPNIC が割り振りを行った IP アドレスブロックや AS 番号等の情報を含む CSR (運用組織の CA 用)への署名である。

⑶ IP アドレス証明書システム

IP アドレス証明書システムは、JPNIC にて管理／運用され、その主な機能は AS 運用者の認証処理、AS 運用者からの証明書への署名要求を受け付け、IP アドレス認証局への橋渡しを行い、署名された物を申請組織へ返送する。また、作成された署名物は必要であれば JPIRR 等の他のレジストリ・システムへ配布することも考えられる。

⑷ AS 内証明システム

AS 内証明書システムは、各 AS 運用者により管理／運用され、その主な機能は AS 番号等を含む CSR や自身が再割り振りを行った IP アドレスブロック情報を含む CSR の作成と下位組織からの署名申請を受け、AS 内認証局への橋渡しを行い、署名された物を申請組織へ返送する。また作成された署名物は必要であれば JPIRR 等の他レジストリ・システムへ配布することも考えられる。

⑸ AS 内認証局

AS 内認証局は各 AS 運用者により管理／運営され、その機能は AS 番号等の情報を含む CSR や署名の必要なデータへの署名である。

9.3.2.3. S-BGP 初期設定概要

利用を開始する際に必要なのは、自身の AS を証明する証明書(組織証明書)を作ることである。この証明書は IANA/RIR 等の権威ある機関で署名する。ここでは JPNIC が IANA/RIR の代わりとして署名を行うと仮定し、JPNIC 認証局／JPNIC IP アドレス認証局を利用する。

9.3.2.4. 自 AS で利用する組織証明書作成概要

AS 内証明書システムにて PublicKey/PrivateKey 生成後、組織 CSR を作成し IP アドレス証明書システムへ IP アドレス認証局の署名を申請する。受け取った IP アドレス証明書システムはレジストリシステム等を利用して CSR の内容を確認し、問題が無ければ IP アドレス認証局へ CSR を転送し、IP アドレス認証局の PrivateKey にて署名された証明書が返信されるのを待つ。返信された証明書は、そのまま申請者へ送信される。

証明書を受信した AS 内証明書システムは、組織証明書を検証後、証明書レジストリシステムへ登録すると共にルータ用のフォーマットに変更してルータへ設定する。

対となる PrivateKey は、AS 内認証局にて管理し、AS 内証明書システムの要求に従い必要な署名を行ために利用する。

組織証明書作成手順概要を図 9-61 に示す。

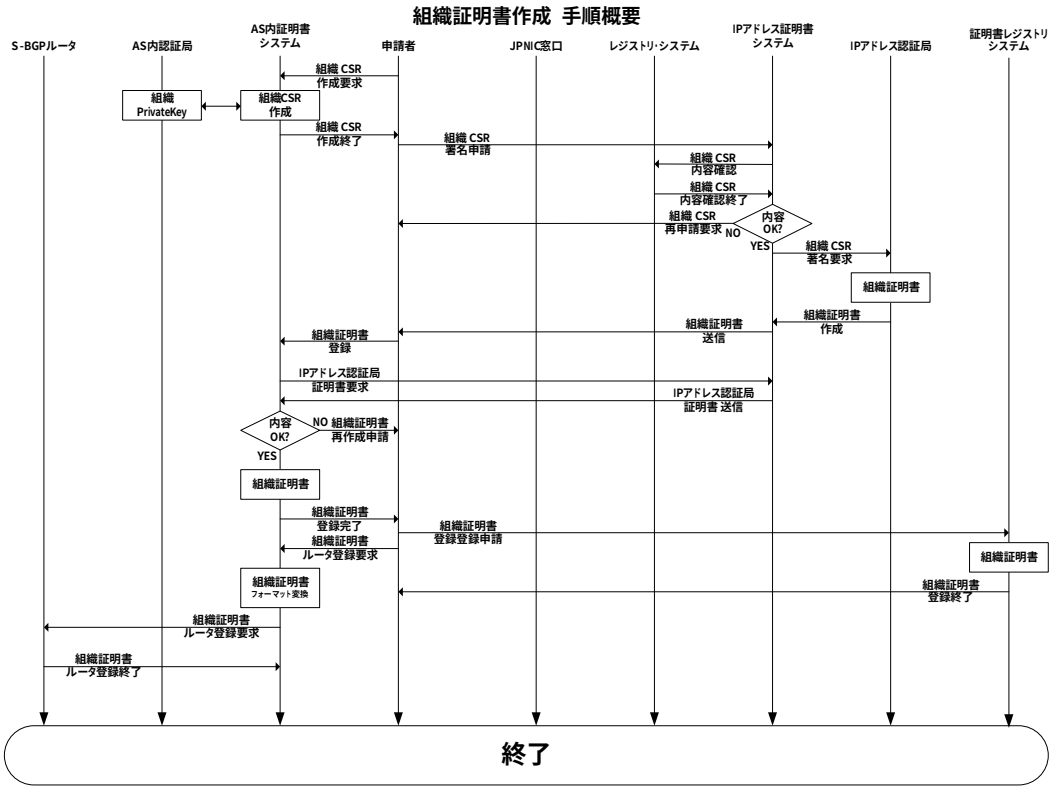


図 9-61　組織証明書作成手順概要

9.3.2.5. Address Attestations (AAs)証明書作成概要

AS内証明書システムにJPNICから割り振りを受けた、IPアドレスブロックをデータに持つAA CSRを作成するように指示を出す。また、AS内認証局に対して今作成したCSRを署名するように指示を出す。受け取った認証局は署名後、AA 証明書としてAS内証明書システムへ返送する。受け取ったAS内システムは著名を確認後問題なければ、証明書レジストリシステムへ登録すると共に、フォーマットをルータ用に変換後、ルータを設定する。

Address Attestations(AA)証明書作成手順概要を図 9-62 に示す

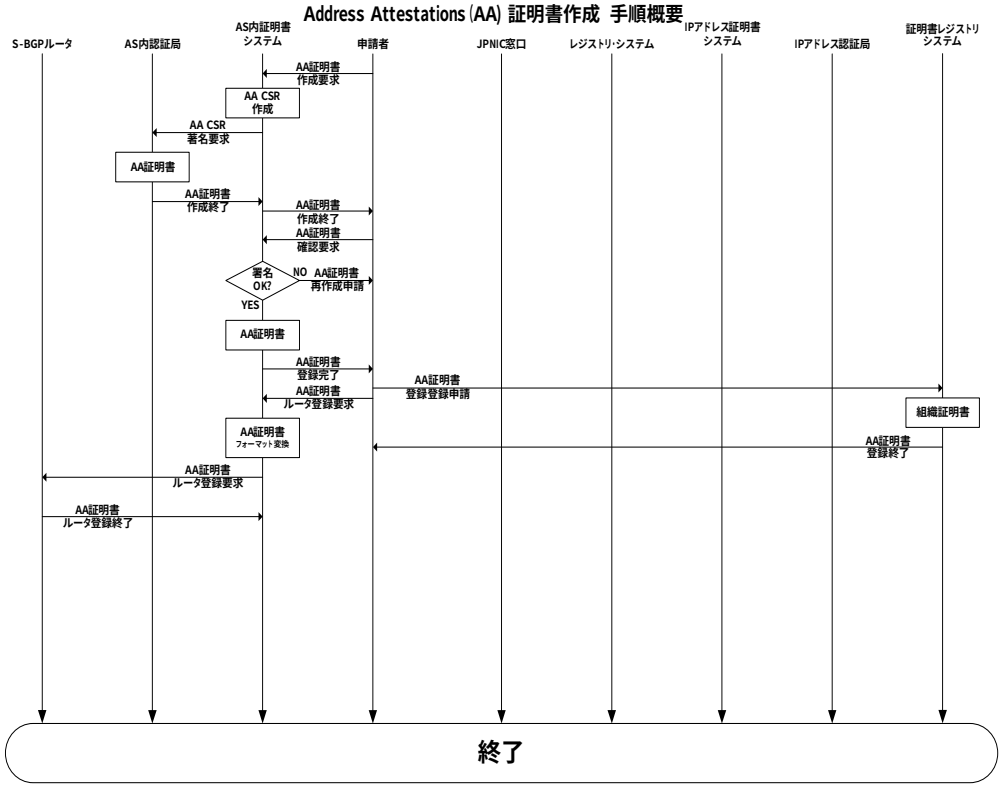


図 9-62　Address Attestations(AA)証明書作成手順概要

9.3.2.6. Route Attestations (RAs)証明書作成概要

AS 内証明書システムにて PublicKey/PrivateKey 生成後、RA CSR を作成し AS 内証明書システムへ AS 内認証局の署名を申請する。受け取った AS 内認証局は CSR を自身の PrivateKey にて署名し AS 内証明書システムへ RA 証明書として返送する。AS 内証明書システムは返送されて来た RA 証明書の署名を確認し問題がなければ証明書レジストリへ登録する。

次に AS 内証明書システムは RA 秘密鍵をルータへ転送し、ルータ自身が RA を作成できるように設定する。

Route Attestations(RA)証明書作成手順概要を図 9-63 に示す。

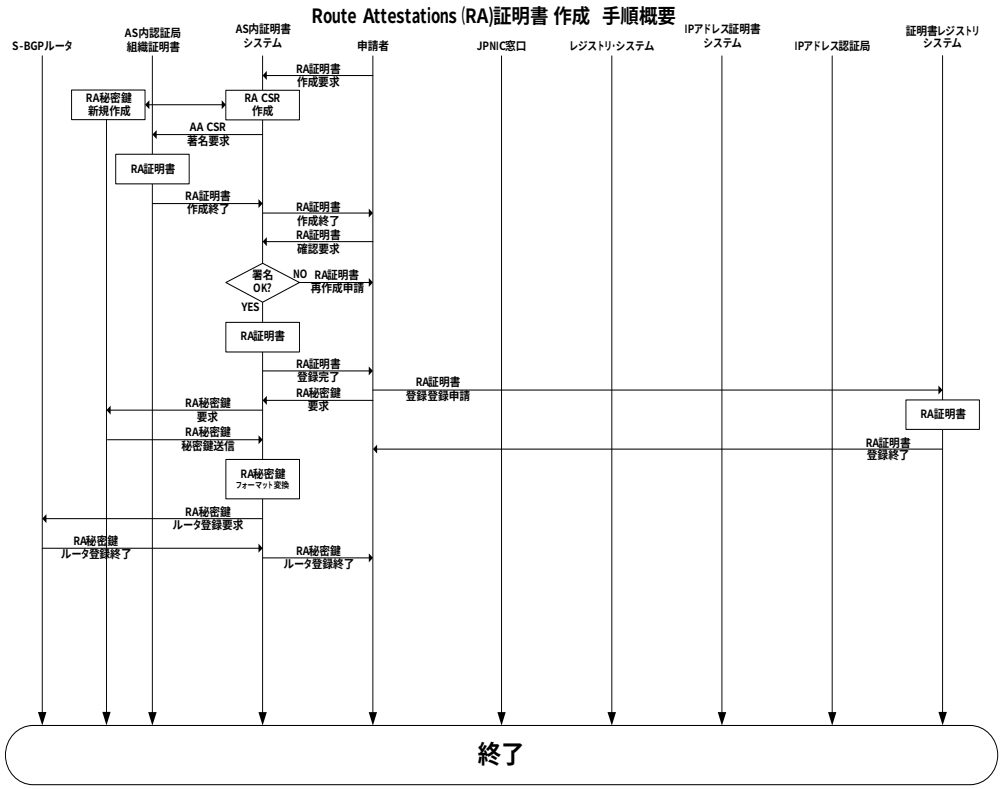


図 9-63　Route Attestations(RA)証明書作成手順概要

この時点でルータには、組織証明書テーブル、AA 証明書テーブル、RA 秘密鍵の情報が追加されたことになる。この状態で BGP Update で送られてきた経路情報が Checkpoint で確認可能な状態になったことになる。

9.3.2.7. 各種証明書の破棄について

署名検証後は必ず CRL の検証を行う。証明書の破棄については証明書内の URL を参照し最新の CRL を取得後行われるか、証明書レジストリ・システムから CRL を取得したものが利用される。破棄が確認された証明書に関してはテーブルから削除するように AS 内証明書システムがルータへ指示を出す。

以上で連携システムの概略に関しての説明を終える。

9.4. 考察とまとめ

本章では、インターネットの経路制御において経路情報を登録する登録機構であるインターネット・ルーティング・レジストリに着目し、経路制御の安全性と、インターネット・ルーティング・レジストリに登録される情報の正確性、信憑性、信頼性の向上について解説、検討、および考察を行った。

この調査の結果では、近年のインターネットに広告される経路数は増加の一途であり、減少する見込みはない。一方で、インターネットに経路を広告する方法は BGP-4 が開発された当初より劇的な変化はなく、開発当初は問題が無かったものでも、現時点のような広範囲にインターネットが普及した状態では、経路制御にセキュリティ的にいくつかの問題があることが明らかになった。

このような問題を解決するための手段としては、経路制御の運用上、経路フィルタをするなどが現時点では最良であるが、厳しい経路フィルタはそれ相応の運用の手間が必要であり、多少セキュリティ的には問題があっても運用上妥当な手間で実施できるレベルにセキュリティレベルと落として運用しているのが実情である。

そこで、本調査研究では、IP レジストリにおける IP アドレス証明書基盤として、「IP レジストリシステムと IRR システムの連携とその認証・承認の強化による IRR 登録情報の正確性・信憑性・信頼性の向上」というアプローチと「soBGP/S-BGP という提案されている新プロトコルの具体的な運用モデルの考察」について調査・検討・考察を行った。

この調査・検討・考察の結果、IP レジストリシステムと IRR システムの連携、および IP アドレス証明書を用いた認証システムを導入することにより、IRR に登録される情報の正確性・信憑性を向上させるのに有効であることが明らかとなった。

また、soBGP/S-BGP は、現時点では現状の運用に若干の問題はあるものの、プロトコルそのものの効果としては、インターネットに流れる経路情報を正しく保つのに効果があることがわかった。

しかし、ここで有効と明らかになったシステムは、いずれもインターネット全体で普及した段階で有効となるものである。つまり、日本国内のみの様な一部の地域、もしくは閉域で利

用しても、それらの領域のみの情報に対してのみ有効なのである。

現状の経路制御のセキュリティを考えると、何らかの対策が必要であることは明らかであり、これらの対策はインターネットに接続しているコミュニティ全体で実施していく必要がある。本調査では、インターネットの経路制御のセキュリティ向上に対する有効な手段を考察し検討しており、この調査報告書で記載されているような機構をインターネットレジストリで導入することの、早急に検討する必要があると考えられる。