Appendix 1

RFC3779 日本語訳

<Appendix 1 について >

- この資料は、IETF において策定された RFC3779　を日本語に翻訳したものです。
  - 内容の理解を図るために翻訳されたもので、内容確認には原文をご利用下さい。
  - 日本語訳は本調査研究の一環として作成されたものです。日本語訳に関するお問い合わせは著者に行なわないで下さい。

Network Working Group　　C. Lynn
Request for Comments: 3779　　S. Kent
Category: Standards Track　　K. Seo
BBN Technologies
June 2004

IP アドレスおよび AS 識別子のための X.509 の拡張

本文書の位置づけ

本文書はインターネットコミュニティのためのインターネット標準化過程プロトコルを定義し、改良のための議論と提案を求めている。本プロトコルの標準化の段階および状態については「Internet Official プロトコル Standard」(STD 1)の最新版を参照してほしい。本文書の配布は制限されない。

著作権表示

要約

本文書は、2 つの X.509 v3 証明書拡張を定義する。最初のものは IP アドレスブロックのリスト、またはプリフィックスを証明書のサブジェクトに結合するものである。2 番目のものは、自律システム識別子のリストを証明書のサブジェクトに結合するものである。これらの拡張は､拡張領域内に含まれる IP アドレスおよび自律システム識別子をサブジェクトが使用することを認証するために使用することができる。

目次

1. はじめに

本文書は、一連の IP アドレスおよび自律システム識別子の使用権の、IANA から地域インターネットレジストリ(RIR)を通じてインターネットサービスプロバイダ(ISP)およびユーザ組織への以上を認証する、2 つの X.509 v3 証明書拡張を定義する。最初のものは、IP アドレスブロック(しばしば IP アドレスプリフィックスと表される)を、証明書のサブジェクト(秘密鍵の保有者)に結合するものである。2 番目のものは、自律システム(AS)識別子のリストを証明書のサブジェクト(秘密鍵の保有者)に結合するものである。証明書の発行者は、一連の IP アドレスブロックおよび AS 識別子の管理権を証明書のサブジェクトに移譲する(「割り振る」)権威を持つエンティティ(たとえば IANA、地域インターネットレジ

ストリ、または ISP) である。これらの証明書は、一連の IP アドレスプリフィックスおよび AS 識別子の使用権を確認する、スケーラブルな手段を提供する。これらは、Secure BGP [S-BGP]などのルーティングプロトコルがルーティング情報の正当性や正確さを確認したり、インターネットルーティングレジストリが受信するデータを確認したりするために使用することができる。

セクション 2 および 3 は、この使用で定義され、従わなければならない(MUST)拡張領域のエンコーディングに関するいくつかの規則を指定する。これらのエンコーディング規則は、以下の目的で使用される。最初に、これらは拡張領域の値の固有のエンコーディングに帰着する。2 つの拡張領域のインスタンスは、オクテットごとに等しいかどうかを比較することができる。第 2 に、これらは、情報を最小サイズでエンコーディングすることができる。第 3 に、これらの規則によって、依存者が証明書パス検証を行うときに、ワンパスアルゴリズムを使うことができる。特に、依存者は複数の境界の場合(隣接、重複、または包含)を扱うために、情報をソートしたりサブセットチェックアルゴリズムの中に余分なコードを実装したりする必要がない。

1.1. 用語

読者は「インターネット X.509 公開鍵基盤 証明書と証明書失効リスト(CRL)のプロファイル」[RFC3280]、「インターネットプロトコル」[RFC791]、「インターネットプロトコルバージョン 6(IPv6)のアドレス体系」[RFC3513]、「インターネットレジストリにおける IP 割り振りのガイドライン」[RFC2050]、および関係する地域インターネットレジストリアドレス管理ポリシードキュメントに記載されている用語および概念を熟知しているものとみなされる。重要な用語には、以下のものが含まれる。

割り振り - リソースの管理権の、中間組織への移譲([RFC2050]参照)。

割り当て - リソースの管理権の、エンドユーザ組織への移譲管理権([RFC2050]参照)。

自律システム (AS) - 1 つの管理ポリシーで単独の技術的管理下にあり、1 つまたは複数の内部ゲートウェイプロトコルとメトリックを使用して自律システム内のパケットのルーティング方法を決定し、外部ゲートウェイプロトコルを使用して他の自律システムへのパケットのルーティングの方法を決定する、ルーターの集合。

自律システム番号 - 自律システムを識別する 32 ビットの数字。

委任- IP アドレスブロックまたは AS 識別子の管理権(すなわち使用権)を、証明書をエンティティに発行することによって委任すること。

第 1 オクテット- DER エンコードされたビット文字列の値の最初のオクテット[X.690]。

IP v4 アドレス- 「.」で区切られた 4 個の 0～255 の範囲の十進数としてあらわされる 32 ビットの識別子。10.5.0.5 は IPv4 アドレスの例である。

IP v6 アドレス- 「:」で区切られた 8 個の 0～ffff の範囲の 16 進数として表される 128 ビットの識別子。2001:0:200:3:0:0:0:1 は IPv6 アドレスの例である。:0: フィールドの文字列は「::」に置き換えてもよいため、2001:0:200:3::1 は直前の例と同じアドレスを表す([RFC3513]参照)。

プリフィックス あるアドレスの初期ビットのいくつかで構成されるビット文字列。アドレスの後ろに「/」および初期ビットの個数が続くものとしてあらわされる。10.5.0.0/16 および 2001:0:200:3:0:0:0:0/64(または 2001:0:200:3::/64)プリフィックスの例である。プリフィックスは、下位のゼロフィールドを省略することによって短縮されることが多いが、示された数のイニシャルビットを含むのに十分なフィールドがあるべきである。10.5/16 および 2001:0:200:3/64 は、短縮されたプリフィックスの例である。

地域インターネットレジストリ (RIR) - IP アドレスおよび AS 識別子の管理を地域内で行うことを IANA に承認された団体。本文書の作成の時点では、AfriNIC、APNIC、ARIN、LACNIC、および RIPE NCC がある。

使用権 - IP アドレスプリフィックスに関しては、インターネット全体でプリフィックスの通知を発信することができる AS を指定することを承認されていること。自律システム識別子に関しては、その自律システム識別子を使って他のネットワークオペレータに自分自

身を特定するネットワークを運営することを承認されていること。

後続オクテット - DER エンコードされたビット文字列の値の 2 番目から最後までのオクテット[X.690]。

トラストアンカー - 証明書パス検証を行うときに信頼する証明書([RFC3280]参照)。

本文書中の「MUST（しなければならない)」「MUST NOT（してはならない)」「REQUIRED（要求される)」「SHALL（すべきである)」「SHALL NOT（すべきでない)」「SHOULD（したほうがよい)」「SHOULD NOT（しないほうがよい)」「RECOMMENDED（推奨される)」「MAY（してもよい)」「OPTIONAL（選択できる)」というキーワード群は、[RFC2119]での記述のとおりに解釈される。

2. IP アドレス委任拡張領域

この拡張は、IP アドレスをエンディティに属する公開鍵に結合することによって、それらのアドレスの割り振りをおこなう。

2.1. コンテキスト

IP アドレス空間は現在、名目上 IANA をルートとするが RIR によって管理される階層によって管理されている。IANA は IP アドレス空間を RIR に割り振り、RIR は次に IP アドレス空間をインターネットサービスプロバイダ(ISP)に割り振り、ISP は IP アドレス空間を下流のプロバイダ、顧客などに割り振る。RIR はまた、エンドエンティティである組織、すなわち他の組織に空間を移譲しない組織に IP アドレス空間を割り当てることもできる。(割り振りおよび割り当てのプロセスについては、[RFC2050]および関連する RIR ポリシードキュメントを参照。)

IP アドレス委任拡張は、IP アドレスブロックが適切に委任されること、すなわちエンティティが IP アドレス空間を使用または再割り振りすることを承認することを検証できるようにすることを目的とする。したがって、IP アドレス空間を割り振るための既存の管理の枠組みの固有の権威性を利用することは意味がある。上記のセクション 1 で説明したように、これはこのセクションで説明する拡張領域を持つ証明書を発行することによって達成される。この拡張領域内の情報を使用する 1 方法の例としては、ある組織が特定の IP アドレスブロックへの経路を通知する BGP UPDATE を発信することを承認されていることを確認するために、あるエンティティがこの情報を使用するというものがある。[RFC1771]、[S-BGP]などを参照。

2.1.1. IP アドレスまたはプリフィックスのエンコーディング

IP アドレスには、IPv4 および IPv6 の 2 つの系統がある。

IPv4 アドレスとは、「.」で区切られた 4 個の 0～255 の範囲の十進数としてあらわされる 32 ビットの数字である。10.5.0.5 は IPv4 アドレスの例である。

IPv6 アドレスとは、「:」で区切られた 8 個の 0～ffff の範囲の 16 進数として表される 128 ビットの数字。2001:0:200:3:0:0:0:1 は IPv6 アドレスの例である。IPv6 アドレスはしばしば、値が 0 である隣接するフィールドを持つ。このような 0 フィールドのグループは、2 個のセミコロン("::")によって短縮することができる。したがって前の例は、2001:0:200:3::1 と表すことができる。

アドレスプリフィックスとは、最上ビットが同じである 2^k 個の連続したアドレスの集合である。たとえば、10.5.0.0～10.5.1.255 の 512 個の IPv4 アドレスの集合は、上位 23 ビットがすべて同じである。このアドレスの集合は、スラッシュ("/")と定数であるビットの数を集合内の最下位アドレスに付加することによって表される。例の集合のプリフィックスは 10.5.0.0/23 で、2^(32-23) = 2^9 個のアドレスが含まれる。2001:0:200:0:0:0:0:0 ～ 2001:0:3ff:ffff:ffff:ffff:ffff:ffff(2^89 個のアドレス)の集合は、

2001:0:200:0:0:0:0:0/39 または同等に 2001:0:200::/39 とあらわされる。プリフィックスは、最下位のゼロフィールドを省略することによって短縮してもよいが、示された 数の定数ビットを含むのに十分なフィールドがあるべきである。例の IPv4 プリフィックスを省略した形式は、10.5.0/23 であり、IPv6 プリフィックスのものは 2001:0:200/39 である。

IP アドレスまたはプリフィックスは、IP アドレス委任拡張領域内では、定数最上位ビットを含む DER エンコードされた ASN.1 ビット文字列としてエンコードされる。ビット文字列の DER エンコーディングはビット文字列タイプ(0x03)、それに続く値オクテットの数(のエンコード)、それに続く値で構成される[X.690] を思い出すこと。値は、最後の値オクテット内で未使用のビット数を指定する「第 1 オクテット」と、それに続くビット文字列を含む「後続オクテット」で構成される。(IP アドレスについては、長さのエンコーディングは単に長さである。)

単独のアドレスの場合は、すべてのビットは定数であるため、IPv4 アドレスのビット文字列には 32 ビットある。アドレス 10.5.0.4 の DER エンコーディング内の後続オクテットは 0x0a 0x05 0x00 0x04 である。最終オクテットのすべてのビットが使用されるため、第 1 オクテットは 0x00 である。したがって、DER エンコードされたビット文字列内のオクテットは以下のとおりである。

```
タイプ 長さ 未使用ビット ...
0x03 0x05   0x00   0x0a 0x05 0x00 0x04
```

同様に、プリフィックス 10.5.0/23 の DER エンコーディングは以下のとおりである。

```
タイプ 長さ 未使用ビット ...
0x03 0x04   0x01   0x0a 0x05 0x00
```


この場合、3 個の後続オクテットには 24 ビットが含まれるが、プリフィックスは 23

個しか使用していないため､最終オクテット内に未使用のビットが１つある｡したがって､第１オクテットは１である(DER では､すべての未使用ビットがゼロビットにセットされなければならない(MUST))｡

IPv6 アドレス 2001:0:200:3:0:0:0:1 の DER エンコーディングは以下のとおり。

```
タイプ 長さ 未使用ビット ...
0x03 0x11   0x00   0x20 0x01 0x00 0x00 0x02 0x00 0x00 0x03
                   0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x01
```

プリフィックス 2001:0:200/39 は最終オクテットに未使用ビットを 1 つ含むが、その DER エンコーディングは以下のとおり。

```
タイプ 長さ 未使用ビット ...
0x03 0x06   0x01   0x20 0x01 0x00 0x00 0x02
```

2.1.2. IP アドレスの範囲のエンコーディング

任意の隣接する IP アドレス範囲は隣接するプリフィックスの集合で表現できるが、最下位アドレスと最上位アドレスを含むシーケンスとして範囲をエンコードすることによって、より簡潔な表現が得られる。ここで各アドレスはビット文字列としてエンコードされる。シーケンス内では、範囲内の最下位アドレスを表すビット文字列は、アドレスからすべての最下位ゼロビットを取り除くことで形成され、範囲内の最上位アドレスを表すビット文字列は、すべての最下位 1 ビットを取り除くことで形成される。DER ビット文字列エンコーディングでは、最終オクテット内のすべての未使用ビットがゼロビットにセットされなければならない(MUST)｡プリフィックスは､常に範囲として表現することができるが、範囲は常にプリフィックスとして表現することはできないことに注意。

プリフィックス 10.5.0/23 で表現されるアドレスは、10.5.0.0～10.5.1.255 である。最下位アドレスは 16 個のゼロビットで終わるが取り除かれている。結果の 16 ビット文字列の DER エンコーディングは以下のとおり。

```
タイプ 長さ 未使用ビット ...
0x03 0x03   0x00   0x0a 0x05
```

最上位アドレスは 9 個の 1 ビットで終わるが取り除かれている。結果の 23 ビット文字

列の DER エンコーディングは以下のとおり。

```
タイプ 長さ 未使用ビット ...
0x03 0x04   0x01   0x0a 0x05 0x00
```


プリフィックス 2001:0:200/39 は、最下位アドレス(2001:0:200::)の DER-エンコーディングが以下のとおりであるような範囲としてエンコードできる。

```
タイプ 長さ 未使用ビット ...
0x03 0x06   0x01   0x20 0x01 0x00 0x00 0x02
```

最上位アドレス(2001:0:3ff:ffff:ffff:ffff:ffff:ffff)は、90 個の最下位 1 ビットを取り除くと 38 ビット文字列となり、以下のようにエンコードされる。

```
タイプ 長さ 未使用ビット ...
0x03 0x06   0x02   0x20 0x01 0x00 0x00 0x00
```

特殊な場合として、すべての IP アドレスブロック、すなわちすべてゼロビットのプリフィックスは、長さオクテットが 1、第 1 オクテットがゼロ、後続オクテットなしで DER エンコードしなければならない(MUST)。

```
タイプ 長さ 未使用ビット ...
0x03 0x01   0x00
```

IP アドレスに関しては、一連のゼロビットは意味を持つことに注意。たとえば、以下

の 10.64/12 の DER エンコーディング。

```
タイプ 長さ 未使用ビット ...
0x03 0x03  0x04  0x0a 0x40
```

は、10.64.0/20 の DER エンコーディングとは異なる。

```
タイプ 長さ 未使用ビット ...
0x03 0x04  0x04  0x0a 0x40 0x00
```

2.2. 仕様

2.2.1. OID

この拡張の OID は、id-pe-ipAddrBlocks である。

```
id-pe-ipAddrBlocks  OBJECT IDENTIFIER ::= { id-pe 7 }
```

ここで [RFC3280] は以下のように定義する。

```
id-pkix  OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
         dod(6) internet(1) security(5) mechanisms(5) pkix(7) }

id-pe    OBJECT IDENTIFIER ::= { id-pkix 1 }
```


2.2.2. クリティカリティ

この拡張は、クリティカルであるものとする(SHOULD)。この拡張の目的とする用途は、拡張領域で指定される IP アドレスのブロックの使用権を暗示することである。CA は拡張

をクリティカルとマークして、証明書が発行された目的のために依存者が証明書を利用するためには、拡張領域の意味を理解しなければならない(MUST)という注意を伝える。個の拡張領域を含む証明書を使用する、新規作成されたアプリケーションは、この拡張を認識するものと期待される。

2.2.3. 文法

```
id-pe-ipAddrBlocks      OBJECT IDENTIFIER ::= { id-pe 7 }

IPAddrBlocks        ::= SEQUENCE OF IPAddressFamily

IPAddressFamily     ::= SEQUENCE {    -- AFI & オプション SAFI --
   addressFamily        OCTET STRING (SIZE (2..3)),
   ipAddressChoice      IPAddressChoice }

IPAddressChoice     ::= CHOICE {
   inherit              NULL, -- 発行者から継承 --
   addressesOrRanges    SEQUENCE OF IPAddressOrRange }

IPAddressOrRange    ::= CHOICE {
   addressPrefix        IPAddress,
   addressRange         IPAddressRange }

IPAddressRange      ::= SEQUENCE {
   min                  IPAddress,
   max                  IPAddress }

IPAddress           ::= BIT STRING
```

2.2.3.1. タイプ IPAddrBlocks

IPAddrBlocks タイプは、IPAddressFamily タイプのシーケンスである。

2.2.3.2. タイプ IPAddressFamily

IPAddressFamily タイプは、addressFamily および ipAddressChoice 要素を含むシーケンスである。

2.2.3.3. 要素 addressFamily

addressFamily 要素は、2 オクテットのアドレスファミリ識別子(AFI)をネットワークバイトオーダーで含み、オプションで 1 オクテットの後続アドレスファミリ識別子(SAFI)がそれに続くオクテット文字列である。AFI および SAFI はそれぞれ[IANA-AFI]および[IANA-SAFI]で指定される。

特定の AFI とオプションの SAFI に対して、承認が与えられていない場合は、IPAddrBlocks シーケンス内の AFI/SAFI に対して、IPAddressFamily メンバーがあってはならない(MUST NOT)。

AFI と SAFI の固有の組み合わせに対して、IPAddressFamily シーケンスは 1 だけでなくてはならない(MUST)。各シーケンスは、addressFamily の値で昇順に並んでいなくてはならない(MUST) (オクテットは符号なしの量として扱う)。SAFI のない addressFamily は、SAFI を含むものより前に置かなければならない(MUST)。IPv4 と IPv6 の両方のアドレスが指定された場合は、IPv4 アドレスを IPv6 アドレスより前に置かなければならない(MUST)(IPv4 AFI の 0001 は IPv6 AFI の 0002 より小さいため)。

2.2.3.4. 要素 ipAddressChoice およびタイプ IPAddressChoice

ipAddressChoice 要素のタイプは IPAddressChoice である。IpAddressChoice タイプは inherit または addressesOrRanges 要素のいずれかの CHOICE である。

2.2.3.5. 要素 inherit

IPAddressChoice CHOICE に inherit 要素が含まれている場合は、指定された AFI およびオプションの SAFI に対する承認された IP アドレスの集合が、addressesOrRanges 要素

を含む IPAddressChoice を含む証明書が見つかるまで、再帰的に発行者の証明書、または発行者の発行者の証明書からとられる。

2.2.3.6. 要素 addressesOrRanges

addressesOrRanges 要素は IPAddressOrRange タイプのシーケンスである。addressPrefix および addressRange 要素は、以下のバイナリ表現を用いてソートしなければならない(MUST)。

<範囲内の最下位 IP アドレス> | <プリフィックスの長さ>

ここで"|" は連結を表す。この表現内のオクテット(a.b.c.d | IPv4 の長さ または s:t:u:v:w:x:y:z | IPv6 の長さ)は、DER エンコードされたビット文字列値のオクテットではないことに注意。たとえば、以下の 2 つの addressPrefix があるとする。

IP アドレス	長さ	DER エンコーディング			
		タイプ	長さ	未使用ビット...	
10.32.0.0	12	03	03	04	0a 20
10.64.0.0	16	03	03	00	0a 40

32 は 64 より小さいため、プリフィックス 10.32.0.0/12 は、プリフィックス 10.64.0.0/16 より前にこなければならない(MUST)。一方、DER ビット文字列でソートされるとすると、未使用ビットオクテットは逆の順序でソートされるため、順序は逆になる。拡張領域内の IPAddressOrRange choice のペアは、重複してはならない(MUST NOT)。隣接するアドレスプリフィックスまたは範囲は単独の範囲または、可能であれば常に、単独のプリフィックスに組み合わせなければならない(MUST)。

2.2.3.7. タイプ IPAddressOrRange

IPAddressOrRange タイプは、addressPrefix(IP プリフィックスまたはアドレス)または addressRange (IP アドレス範囲)要素の CHOICE である。

この仕様では、プリフィックスとしてエンコードできるアドレス範囲は、IPAddress 要素(ビット文字列)を用いてエンコードしなければならず(MUST)、プリフィックスとしてエンコードできない範囲は IPAddressRange(2 つのビット文字列を含むシーケンス)を用いてエンコードしなければならない(MUST)。以下の擬似コードは、所定のアドレス範囲のエンコードを選択する方法を説明するものである。

```
LET  N = 範囲の最下位および最上位アドレス内の、一致する最上位ビットの数
IF 最下位アドレスに残っているすべてのビットがゼロビット
 AND 最上位アドレスに残っているすべてのビットが 1 ビット
THEN 範囲は N ビット IP アドレスとしてエンコードしなければならない(MUST)
ELSE 範囲 IPAddressRange としてエンコードしなければならない(MUST)
```

2.2.3.8. 要素 addressPrefix およびタイプ IPAddress

addressPrefix 要素は IPAddress タイプである。IPAddress タイプはアドレスの最上位(左側の)N ビットが定数であり、残りのビット(IPv4 では 32-N ビット、IPv6 では 128-N ビット)がゼロまたは 1 のいずれかであるような IP アドレスの範囲を定義する。たとえば、IPv4 プリフィックス 10.64/12 はアドレス 10.64.0.0～10.79.255.255 に対応し、10.64/11 は 10.64.0.0～10.95.255.255 に対応する。IPv6 プリフィックス 2001:0:2/48 はアドレス 2001:0:2::～2001:0:2:ffff:ffff:ffff:ffff:ffff を表す。

IP アドレスプリフィックスは、ビット文字列としてエンコードされる。ビット文字列の DER エンコーディングは、文字列の第 1 オクテットを使って、最終後続オクテットのうちのいくつが未使用であるかを指定する。

DER エンコーディングでは、これらの未使用ビットがゼロビットにセットされなければ

ならない(MUST)と指定している。

例:

```
          128.0.0.0         = 1000 0000.0000 0000.0000 0000.0000 0000
        ～ 143.255 255 255 = 1000 1111.1111 1111.1111 1111.1111 1111
      エンコードするビット文字列 = 1000
                        タイプ 長さ 未使用ビット...
  エンコーディング = 0x03 0x02   0x04   0x80
```

2.2.3.9. 要素 addressRange およびタイプ IPAddressRange

addressRange 要素はタイプ IPAddressRange である。IPAddressRange タイプは、最小(要素 min)と最大(要素 max)の IP アドレスを含むシーケンスで構成される。各 IP アドレスはビット文字列としてエンコードされる。IPAddressRange 内の最小アドレスの意味論的解釈は、指定されていないすべてのビット(完全な長さの IP アドレスに関して)がゼロビットであるということである。IPAddressRange 内の最大アドレスの意味論的解釈は、指定されていないすべてのビット(完全な長さの IP アドレスに関して)が 1 ビットであるということである。最小アドレスのビット文字列は、最小アドレスからすべての最下位ゼロビットを取り除くことで得られる。最大アドレスのビット文字列は、最大アドレスからすべての最下位 1 ビットを取り除くことで得られる。

例:

```
          129.64.0.0         = 1000 0001.0100 0000.0000 0000.0000 0000
        to 143.255.255.255   = 1000 1111.1111 1111.1111 1111.1111 1111
         最小ビット文字列 = 1000 0001.01
         最大ビット文字列 = 1000
  エンコーディング = シーケンス {
              タイプ 長さ 未使用ビット ...
      min     0x03 0x03   0x06   0x81        0x40
      max     0x03 0x02   0x04   0x80
            }
```

証明書パス検証を行うときに IP アドレスブロックの比較を簡素化するために、最大 IP アドレスは値が 1 であるビットを少なくとも 1 つ含んでいなければならない(MUST)。すなわち、後続オクテットは省略されたりすべてゼロであったりしてはならない。

2.3. IP アドレス委任拡張領域証明書パス検証

IP アドレス委任拡張領域を含む証明書の証明書パス検証には、追加の処理が必要である。パス内の各証明書が検証されるときに、その証明書の IP アドレス委任拡張領域内の IP アドレスが発行者の証明書の IP アドレス委任拡張領域内の IP アドレスに含まれていなければならない(MUST)。そうなっていない場合は、検証は失敗しなければならない(MUST)。

証明書パス検証のトラストアンカーである証明書または IP アドレス委任拡張領域を含む証明書、およびパス上のすべての証明書は、それぞれ IP アドレス委任拡張領域を含まなければならない(MUST)。許されるアドレス範囲の初期集合は、トラストアンカー証明書からとられる。

3. 自律システム識別子委任拡張領域

この拡張領域は、自律システム(AS)識別子をエンティティに属する公開鍵に結合することによって、その AS 識別子のエンティティへの割り振りを行う。

3.1. コンテキスト

AS 識別子委任は現在、名目上 IANA をルートとするが RIR によって管理される階層によって管理されている。IANA は AS 識別子を RIR に割り振り、RIR は次に AS 識別子をエンドエンティティである組織、すなわち他の組織に AS 識別子を移譲しない組織に AS 識別子を割り当てる。AS 識別子委任拡張領域は、AS 識別子が適切に委任されること、すなわちエンティティがこれらの AS 識別子を使用することを承認することを検証できるようにすることを目的とする。したがって、AS 識別子を管理するため既存の枠組みの固有の権威性を利用することは意味がある。上記のセクション 1 で説明したように、これはこのセクションで説明する拡張領域を持つ証明書を発行することによって達成される。この拡張領域内の情報を使用する 1 方法の例としては、あるエンティティが、ある組織が AS 識別子で指定さ

れる AS を管理する承認を得ているかどうかを確認するために、この領域を使用することがある。AS 識別子の割り振りを表すためにこの拡張領域を使用することは、AS 識別子が管理される手続きや、AS がいつ使われるべきかを変更することを意図するものではない。[RFC1930]参照。

3.2. 仕様

3.2.1. OID

この拡張の OID は、id-pe-autonomousSysIds である。

```
id-pe-autonomousSysIds  OBJECT IDENTIFIER ::= { id-pe 8 }
```

ここで [RFC3280] は以下のように定義する。

```
id-pkix  OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
         dod(6) internet(1) security(5) mechanisms(5) pkix(7) }

id-pe    OBJECT IDENTIFIER ::= { id-pkix 1 }
```


3.2.2. クリティカリティ

この拡張は、クリティカルであるものとする(SHOULD)。この拡張の目的とする用途は、拡張領域内の AS 識別子の使用権を暗示することである。CA は拡張をクリティカルとマークして、証明書が発行された目的のために依存者が証明書を利用するためには、拡張領域の意味を理解しなければならない(MUST)という注意を伝える。個の拡張領域を含む証明書を使用する、新規作成されたアプリケーションは、この拡張を認識するものと期待される。

3.2.3. 文法

```
id-pe-autonomousSysIds  OBJECT IDENTIFIER ::= { id-pe 8 }

ASIdentifiers       ::= SEQUENCE {
    asnum               [0] EXPLICIT ASIdentifierChoice OPTIONAL,
    rdi                 [1] EXPLICIT ASIdentifierChoice OPTIONAL}

ASIdentifierChoice  ::= CHOICE {
   inherit              NULL, -- 発行者から継承 --
   asIdsOrRanges        SEQUENCE OF ASIdOrRange }

ASIdOrRange         ::= CHOICE {
    id                  ASId,
    range               ASRange }

ASRange             ::= SEQUENCE {
    min                 ASId,
    max                 ASId }

ASId                ::= INTEGER
```

3.2.3.1. タイプ ASIdentifiers

ASIdentifiers タイプは 1 つまたはそれ以上の形式の自律システム識別子(AS 番号(asnum 要素内)またはルーティングドメイン識別子(rdi 要素内))を含むシーケンスである。ASIdentifiers タイプに複数の形式の識別子が含まれている場合は、asnum エントリは rdi エントリより前に置かれなければならない(MUST)。AS 番号は BGP によって使用され、ルーティングドメイン識別子は IDRP ないに指定される[RFC1142]。

3.2.3.2. 要素 asnum、rdi、およびタイプ ASIdentifierChoice

asnum および rdi 要素は、どちらもタイプ ASIdentifierChoice である。ASIdentifierChoice タイプは inherit または asIdsOrRanges 要素の CHOICE である。

3.2.3.3. 要素 inherit

ASIdentifierChoice に inherit 要素が含まれている場合、承認された識別子の集合は、asIdsOrRanges 要素を含む ASIdentifierChoice を含む証明書が見つかるまで、再帰的に発行者の証明書、または発行者の発行者の証明書からとられる。特定の形式の AS 識別子に対して承認が与えられていない場合は、対応する asnum/rdi メンバーが ASIdentifiers シーケンスないにあってはならない(MUST NOT)。

3.2.3.4. 要素 asIdsOrRanges

asIdsOrRanges 要素は、ASIdOrRange タイプのシーケンスである。asIdsOrRanges シーケンス内の項目のペアは、重複してはならない(MUST NOT)。任意の隣接する一連の AS 識別子は、可能であれば常に単独の範囲に組み合わせなければならない(MUST)。asIdsOrRanges 要素内の AS 識別子は、数値の増える順にソートされなければならない(MUST)。

3.2.3.5. タイプ ASIdOrRange

ASIdOrRange タイプは単独の整数(ASId)または単独のシーケンス(ASRange)の CHOICE である。

3.2.3.6. 要素 id

id 要素はタイプ ASId を持つ。

3.2.3.7. 要素 range

range 要素はタイプ ASRange を持つ。

3.2.3.8. タイプ ASRange

ASRange タイプは min および max 要素からなるシーケンスで、AS 識別子の値の範囲を指定するために使用される。

3.2.3.9. 要素 min および max

min および max 要素はタイプ ASId を持つ。min 要素は、範囲内の最小の AS 識別子を指定するために使用され、max 要素は範囲内の最大の AS 識別子の値を指定する。

3.2.3.10. タイプ ASId

ASId タイプは INTEGER である。

3.3. 自律システム識別子委任拡張領域証明書パス検証

自律システム識別子委任拡張領域を含む証明書の証明書パス検証には、追加の処理が必要である。パス内の各証明書が検証されるときに、その証明書の自律システム識別子委任拡張領域内の AS 識別子が発行者の証明書の自律システム識別子委任拡張領域に含まれていなければならない(MUST)。 そうなっていない場合は、検証は失敗しなければならない(MUST)。自律システム識別子委任拡張領域を含む証明書の証明書パス検証のトラストアンカーである証明書および、パス上のすべての証明書は、それぞれ自律システム識別子委任拡張領域を含まなければならない(MUST)。許される AS 識別子の初期集合は、トラストアンカー証明書からとられる。

4. セキュリティ上の配慮

本仕様は 2 つの X.509 拡張を説明する。X.509 証明書はデジタル署名されるため、追加のインテグリティサービスは不要である。これらの拡張領域を持つ証明書は、秘密にする必要はなく、これらの証明書に対する無制限の匿名によるアクセスは、セキュリティ上の問題を生じない。

しかし､本仕様の範囲外のセキュリティ要素が証明書ユーザに提供される保証に影響する。このセクションは、実装者、管理者、およびユーザが考慮すべき重要な問題を強調する。

これらの拡張は承認情報、すなわち IP アドレスまたは AS 識別子の使用権を表す。これらは、BGP のセキュアバージョン[S-BGP]をサポートするために開発されたが、他のコンテキストで利用することもできる。セキュア BGP のコンテキストでは、これらの拡張領域を含む証明書は可能性として機能する。証明書は、秘密鍵の保有者(サブジェクト)が拡張領域に現される IP アドレスまたは AS 識別子を使用することを承認されていることを主張する。この機能モデルの結果として、一般的な PKI の慣習とは異なり、サブジェクトフィールドは概してセキュリティ目的とは関係ない。

5. 謝辞

著者は、Charles Gardiner、Russ Housley、James Manger、および Jim Schaad の本仕様への貢献に対し感謝の意を表します。

付録 A -- ASN.1 モジュール

この標準的付録は、準拠 PKI コンポーネントによって使用される IP アドレスおよび AS 識別子拡張領域について ASN.1 文法で説明する。

```
IPAddrAndASCertExtn { iso(1) identified-organization(3) dod(6)
```

```
        internet(1) security(5) mechanisms(5) pkix(7) mod(0)
        id-mod-ip-addr-and-as-ident(30) }
    DEFINITIONS EXPLICIT TAGS ::=
BEGIN
     -- Copyright (C) インターネットソサエティ (2004)--
     -- 本 ASN.1 モジュールの本バージョンは、RFC 3779 の一部である。   --
     -- 完全な法律上の表示については、RFC 自身を参照のこと。          --

-- すべてエキスポート --

IMPORTS

-- PKIX 固有の OID およびアーク --
    id-pe FROM PKIX1Explicit88 { iso(1) identified-organization(3)
              dod(6) internet(1) security(5) mechanisms(5) pkix(7)
              id-mod(0) id-pkix1-explicit(18) };

-- IP アドレス委任拡張領域 OID --

id-pe-ipAddrBlocks  OBJECT IDENTIFIER ::= { id-pe 7 }

-- IP アドレス委任拡張領域文法 --

IPAddrBlocks        ::= SEQUENCE OF IPAddressFamily

IPAddressFamily     ::= SEQUENCE { -- AFI とオプションの SAFI --
   addressFamily        OCTET STRING (SIZE (2..3)),
   ipAddressChoice      IPAddressChoice }

IPAddressChoice     ::= CHOICE {
   inherit              NULL, -- 発行者から継承 --
   addressesOrRanges    SEQUENCE OF IPAddressOrRange }

IPAddressOrRange    ::= CHOICE {
   addressPrefix        IPAddress,
   addressRange         IPAddressRange }
```

```
   IPAddressRange      ::= SEQUENCE {
      min                 IPAddress,
      max                 IPAddress }

   IPAddress           ::= BIT STRING
```



```
   -- 自律システム識別子委任拡張領域 OID --

   id-pe-autonomousSysIds  OBJECT IDENTIFIER ::= { id-pe 8 }

   -- 自律システム識別子委任拡張領域文法 --

   ASIdentifiers       ::= SEQUENCE  {
       asnum               [0] ASIdentifierChoice OPTIONAL,
       rdi                 [1] ASIdentifierChoice OPTIONAL }

   ASIdentifierChoice  ::= CHOICE {
      inherit              NULL, -- 発行者から継承 --
      asIdsOrRanges        SEQUENCE  OF ASIdOrRange }

   ASIdOrRange         ::= CHOICE {
       id                  ASId,
       range               ASRange }

   ASRange             ::= SEQUENCE  {
       min                 ASId,
       max                 ASId }
```

```
ASId                ::= INTEGER

END
```

付録 B -- IP アドレス委任拡張領域の例

以下の IPv4 ユニキャストアドレスプリフィックスを指定する、重要な X.509 v3 証明書拡張

1) 10.0.32/20 すなわち 10.0.32.0～10.0.47.255
2) 10.0.64/24 すなわち 10.0.64.0～10.0.64.255
3) 10.1/16 すなわち 10.1.0.0 ～10.1.255.255
4) 10.2.48/20 すなわち 10.2.48.0～10.2.63.255
5) 10.2.64/24 すなわち 10.2.64.0～10.2.64.255
6) 10.3/16 すなわち 10.3.0.0 ～10.3.255.255、および
7) 発行者の証明書からすべての IPv6 アドレスを継承

は、以下のとおり(16 進):

```
30 46                       Extension {
   06 08 2b06010505070107     extnID        1.3.6.1.5.5.7.1.7
   01 01 ff                   critical
   04 37                      extnValue {
      30 35                     IPAddrBlocks {
         30 2b                    IPAddressFamily {
            04 03 0001  01         addressFamily: IPv4 Unicast
                                    ipAddressChoice
            30 24                     addressesOrRanges {
```

```
                                    IPAddressOrRange
        03 04 04 0a0020              addressPrefix10.0.32/20
                                    IPAddressOrRange
        03 04 00 0a0040              addressPrefix10.0.64/24
                                    IPAddressOrRange
        03 03 00 0a01                addressPrefix   10.1/16
                                    IPAddressOrRange
        30 0c                        addressRange {
           03 04 04 0a0230              min         10.2.48.0
           03 04 00 0a0240              max         10.2.64.255
                                      } --addressRange
                                    IPAddressOrRange
        03 03 00 0a03                addressPrefix   10.3/16
                                  } -- addressesOrRanges
                                } -- IPAddressFamily
  30 06                         IPAddressFamily {
     04 02 0002                  addressFamily: IPv6
                                   ipAddressChoice
     05 00                           inherit from issuer
                                } -- IPAddressFamily
                              } -- IPAddrBlocks
                            } -- extnValue
                          } -- Extension
```

この例は、プリフィックスと範囲がどのようにソートされるかを示す。

+ プリフィックス1の未使用ビット(4)がプリフィックス2の未使用ビット(0)より大きくても、プリフィックス 1 はプリフィックス 2 より前に置かれなければならない(MUST)。

+ プリフィックス 2 のビット文字列エンコーディングのオクテット数(4)がプリフィックス 3 のビット文字列エンコーディングのオクテット数(3)より大きくても、プリフィックス 2 はプリフィックス 3 より前に置かれなければならない(MUST)。

+ プリフィックス 4 と 5 は隣接している(アドレスの範囲 10.2.48.0～10.2.64.255 を表す)ので、1 つの範囲に組み合わせなければならない(MUST)(範囲は単独のプリフィックス

によってエンコードできないため)。

+ 範囲の max 要素内 6 個の連続するゼロビットが、値の意味論的解釈にとって重要であることに注意(すべての未使用ビットは、ゼロでなく 1 と解釈されるため)。min 要素内の 4 個の連続するゼロビット(したがって、min 要素のエンコーディング内の(4)個の未使用ビット)は重要ではなく、取り除かなくてはならない(MUST)。(DER エンコーディングでは、最後の後続オクテット内の未使用ビットはすべてゼロにセットしなくてはならない(MUST))。

+ プリフィックス 4 と 5 で形成される範囲は、範囲の SEQUENCE タグ(30)がプリフィックス 6 のエンコードに使用されるビット文字列(03)のタグより大きくても、プリフィックス 6 より前に置かれなければならない(MUST)。

+ IPv4 のアドレスファミリ識別子(0001)は IPv6 の識別子(0002)より小さいので、IPv4 情報は IPv6 情報より前に置かれなければならない(MUST)。

IPv6 プリフィックス 2001:0:2/48 および IPv4 プリフィックス 10/8 と 172.16/12 を指定し、すべての IPv4 マルチキャストアドレスを発行者の証明書から継承する拡張領域は、以下のとおり(16 進):

```
   30 3d                       Extension {
      06 08 2b06010505070107     extnID        1.3.6.1.5.5.7.1.7
      01 01 ff                   critical
      04 2e                      extnValue {
         30 2c                     IPAddrBlocks {
            30 10                    IPAddressFamily {
               04 03 0001 01          addressFamily: IPv4 Unicast
                                       ipAddressChoice
               30 09                     addressesOrRanges {
```

```
                                    IPAddressOrRange
          03 02 00 0a                addressPrefix   10/8
                                    IPAddressOrRange
          03 03 04 b010              addressPrefix   172.16/12
                                  } -- addressesOrRanges
                                } -- IPAddressFamily
    30 07                       IPAddressFamily {
       04 03 0001 02             addressFamily: IPv4 Multicast
                                  ipAddressChoice
       05 00                        inherit from issuer
                                } -- IPAddressFamily
    30 0f                       IPAddressFamily {
       04 02 0002                addressFamily: IPv6
                                  ipAddressChoice
       30 09                        addressesOrRanges {
                                      IPAddressOrRange
          03 07 00 200100000002       addressPrefix  2001:0:2/47
                                  } -- addressesOrRanges
                                } -- IPAddressFamily
                              } -- IPAddrBlocks
                            } -- extnValue
                             } -- Extension
```


付録 C -- AS 識別子委任拡張領域の例

AS 番号 135、3000～3999、5001 を指定し、すべてのルーティングドメイン識別子を発行者の証明書から継承する拡張領域は以下のとおり(16 進)

```
   30 2b                        Extension {
```

```
06 08 2b06010505070108      extnID        1.3.6.1.5.5.7.1.8
01 01 ff                    critical
04 1c                       extnValue {
   30 1a                      ASIdentifiers {
      a0 14                     asnum
                                  ASIdentifierChoice
         30 12                      asIdsOrRanges {
                                      ASIdOrRange
            02 02 0087                  ASId
                                      ASIdOrRange
            30 08                       ASRange {
               02 02 0bb8                 min
               02 02 0f9f                 max
                                        } -- ASRange
                                      ASIdOrRange
            02 02 1389                  ASId

                                    } -- asIdsOrRanges
                                  } -- asnum
      a1 02                       rdi {
                                    ASIdentifierChoice
         05 00                        inherit from issuer
                                  } -- rdi
                                } -- ASIdentifiers
                              } -- extnValue
                            } -- Extension
```

付録 D -- X.509 属性証明書の使用

この付録では、属性証明書 ([RFC3281]で指定されるように、AC) を、地域インターネットレジストリ(RIR)からエンドユーザ組織へIPアドレスブロックまたはAS識別子の使用権を伝えるために使用するという提案に起因する問題について議論する。

AS 識別子と IP アドレスブロックの 2 つのリソースは、現在異なる方法で管理されている。AS 識別子の使用権を持つすべての組織は、その承認を RIR から直接受ける。IP アドレスブ

ロックの使用権を持つ組織は、その承認を直接 RIR から、または間接的にたとえば下流のサービスプロバイダから受け、その下流のサービスプロバイダは別のサービスプロバイダから承認をうけ、サービスプロバイダは RIR から承認を受ける。

将来 AS 識別子が再割り振りされるかもしれないので、メカニズムは 3 レベルの階層に依存すべきではないことに注意。

RFC 3281 のセクション 1 で、承認情報を伝える拡張領域を持つ公開鍵証明書(PKC)を使用するよりも AC を使用するほうが望ましい理由が 2 つ述べられている。

「承認情報は、PKC 拡張領域におくことも、別の属性証明書(AC)におくこともできる。承認情報を PKC に置くことは、通常 2 つの理由で望ましくない。第 1 に、承認情報は、アイデンティティと公開鍵の結合とは異なる寿命を持つことがよくある。商人情報が PKC 拡張領域におかれると、一般的な結果として PKC の使用可能な寿命が短縮される。第 2 に、PKC の発行者は通常、承認情報に関する権威を持たない。この結果、PKC の発行者は権威をもつものから承認情報を得るという余分のステップを踏まなければならない。」

「これらの理由により、承認情報は PKC とは独立させるほうがよいことが多い。しかし、承認情報はアイデンティティに結合する必要もある。AC はこの結合を提供する。それは単に、デジタル署名(または保証)されたアイデンティティと属性の集合である。」

IP アドレスと AS 識別子の承認の場合、これらの理由は当てはまらない。第 1 に、公開鍵証明書は承認のためだけに発行されるので、証明書の寿命は承認の寿命に正確に対応し、それは発行者と承認を受けるエンティティとの間の契約関係に結びついていることが多い。サブジェクト名と発行者名は証明書パス検証の間に連鎖のために使用されるだけであり、物理的なエンティティに対応する必要はない。PKC 内のサブジェクト名は、実際に発行 CA によってランダムに割り当てられ、リソースの保有者に制限つきの匿名性を与えてもよい。第 2 に、証明書の階層は、証明書の発行者が承認情報に関する権威を持つように構築されている。

したがって、上に引用した最初の段落は AS 番号と IP アドレスブロックの割り振りの場合には当てはまらない。リソースはアイデンティティではなく PKC 内の公開鍵に対応する秘密鍵の保有者に結合されているため、2 番目に引用した段落の要点は当てはまらない。

RFC 3281 は、それに準拠する属性証明書が満たさなければならないいくつかの要件を指定している。S-BGP に関係して、より重要な要件は以下のとおりである。

1 セクション 1 から: 「本仕様では、AC 連鎖の使用は推奨されない(NOT RECOMMEND)。その他の(将来的な)仕様は、AC 連鎖の仕様を扱うかもしれない。」

IANA から RIR へ、RIR から ISP へ、ISP から DSP への割り振りおよびエンド組織への割り当てには、少なくとも IP アドレスブロックに関しては連鎖の仕様が必要である。上位者の AC をどのように見つけ、それをどのように処理するかについての説明が提供されなければならない。本文書の読者は、連鎖を避けることができるような方法を提案することを奨励される。

2 セクション 4.2.9 から: 「セクション 4.3 はこのプロファイルとともに用いてもよい(MAY)拡張領域および、それらがクリティカルとマーク付けされるかどうかを定義する。他のクリティカルな拡張領域が使用される場合、AC はこのプロファイルに準拠しない。しかし、他のクリティカルでない拡張領域が使用される場合、AC はこのプロファイルに準拠する。」

これは、本仕様で定義される委任拡張領域(クリティカルである)が、単純に AC におくことはできないということを意味する。クリティカルとマーク付けされていなければ使用できるが、意図される用途では、思いもよらぬアプリケーションによって拡張領域を含む証明書がアイデンティティ証明書として使用されることがないように、クリティカルであることが必要である。

3 セクション 4.5 から: 「AC の発行者は、PKC の発行者でもあることはできない(MUST

NOT)。つまり、AC の発行者は同時に CA でもあることはできない。」

これは、各 AC の発行者が、AC 保有者の公開鍵を含む PKC を発行するために、独立した CA を必要とすることを意味する。AC の発行者は保有者の PKC を発行することができず、PKC の発行者は AC に署名することができない。したがって、PKI 内の各エンティティは、CA のほかに AC 発行者を運営する必要がある。PKC が使用された場合に比べて、属性証明書のサポートを処理するために、2 倍の数の証明書発行者と CRL が必要になる。単独の目的で証明書を発行する発行者が 2 つあると、不整合が生じる可能性もある。

RFC 3281 の AC モデルは、AC 保有者属性または承認を実証したいときに、保有者が AC を AC 検証者に提示するということを含意する。本文書で定義される拡張領域の意図する用途では、AC 検証者(NOC)と AC の発行者(すべての RIR および NOC)との間の直接の相互作用はない。

主張される使用権の対象への署名があれば、「AC 検証者」は AC の保有者の PKC を見つけることができるが、サブジェクトの AC を見つける直接的な方法はない。

4 セクション 5 から: 「4. AC の発行者は、(設定またはその他の方法によって)AC の発行者として直接信用されなければならない(MUST) 。」

これは、IP アドレスブロックの使用権の場合には事実ではない。IP アドレスブロックは階層を通じて割り振られる。AC の証明書パス検証には、委任階層を上って連鎖をたどる必要がある。各依存者(NOC)が他のすべての NOC を「信用」するように設定しなければならないことは適切ではなく、このような「信用」は、提案されたセキュリティメカニズムが回避するように設計されている失敗に帰する。何千もの個々の信用される ISP ごとの AC の発行者ではなく、信頼されるルートを持つ単独の PKI が使用される。

AC を適切に検証するために必要な作業の量は、本文書で定義される証明書拡張領域

を PKC に置くメカニズムの場合よりも多い。AC に加えて、検証されるべき証明書は 2 倍になる。AC をサポートするために必要な管理負荷が著しく増加する可能性がある。

参考文献

引用規格

[IANA-AFI] http://www.iana.org/assignments/address-family-numbers.

[IANA-SAFI] http://www.iana.org/assignments/safi-namespace.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Level", BCP 14, RFC 2119, March 1997.

[RFC3280] Housley, R., Polk, W., Ford, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[X.690] ITU-T Recommendation X.690 (1997) | ISO/IEC 8825-1:1998, "Information Technology - ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

参考情報

[RFC791] Postel, J., "Internet Protocol -- DARPA Internet Program Protocol Specification", RFC 791, September 1981.

[RFC1142] D. Oran, Ed., "OSI IS-IS Intra-domain Routing Protocol", RFC 1142, February 1990.

[RFC1771] Rekhter, Y. and T. Li, Eds., "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, March 1995.

[RFC1930] Hawkinson, J. and T. Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)", BCP 6, RFC 1930, March 1996.

[RFC2050] Hubbard, K., Kosters, M., Conrad, D., Karrenberg, D. and J. Postel, "Internet Registry IP Allocation Guidelines", BCP 12, RFC 2050, November 1996.

[RFC3513] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003.

[RFC3281] Farrell, S. and R. Housley, "An Internet Attribute Certificate Profile for Authorization", RFC 3281, April 2002.

[S-BGP] S. Kent, C. Lynn, and K. Seo, "Secure Border Gateway Protocol (S-BGP)," IEEE JSAC Special Issue on Network Security, April 2000.

執筆者の連絡先

Charles Lynn

BBN Technologies
10 Moulton St.
Cambridge, MA 02138
USA

Phone: +1 (617) 873-3367
EMail: CLynn@BBN.Com

Stephen Kent
BBN Technologies
10 Moulton St.
Cambridge, MA 02138
USA

Phone: +1 (617) 873-3988
EMail: Kent@BBN.Com

Karen Seo
BBN Technologies
10 Moulton St.
Cambridge, MA 02138
USA

Phone: +1 (617) 873-3152
EMail: KSeo@BBN.Com

完全な著作権表示

知的所有権

IETF は、本文書で説明される技術の実装または使用に関連すると主張する知的財産権またはその他の権利の正当性または範囲または、そのような権利に基づくライセンスが利用できるまたはできない範囲に関して、特定の立場をとらない。また、IETF はそのような権利を特定するための独立した努力を行ったと主張するものでもない。RFC 文書内の権利に関する手続きについての情報は、BCP 78 および BCP 79 に見られる。

IETF 事務局に行われた IPR 開示、利用可能になったライセンスの保証、またはこのような所有権の一般的ライセンスまたは使用許可を得るために、本仕様の実施者またはユーザによって試みられた結果は、IETF オンライン IPR レポジトリ http://www.ietf.org/ipr で

入手することができます。

IETF は、本標準を実装するために必要になるかもしれない技術をカバーする可能性のある著作権、特許または特許申請、またはその他の所有権を、利害関係者が知らせることを推奨する。情報は IETF ietf-ipr@ietf.org に送信してください。

謝辞

RFC エディターの職務に関する財政援助は現在インターネットソサエティによって提供されている。