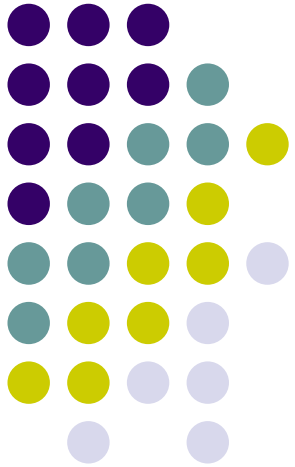
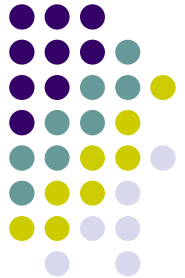
経路制御の安全性向上
～ soBGPとS-BGP ～

2004.10.15

NTT情報流通プラットフォーム研究所
外山勝保　重松光浩
toyama.katsuyasu@lab.ntt.co.jp
pshige@nttlabs.com

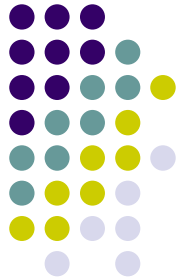


ドメイン間の動的経路制御に関する脆弱性



- 動的経路制御の脆弱性
  - 受け取った経路情報のOrigin ASが、本当に正しいのか？
  - 受け取った経路情報が、正しいASパスで伝播してきているのか？

- 実際に経路のhijackingも起きている
  - more-specific な経路がどこからともなく流れてきて、、、more-specificな経路には負けてしまう

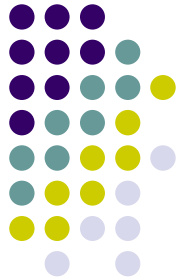


どうすればよいか？

- **現在のアプローチ**
  - IRR＋経路フィルタ
    - Prefixフィルタ、AS-PATHフィルタで、疑わしい経路を取り除く

- **電子署名を導入するアプローチ**

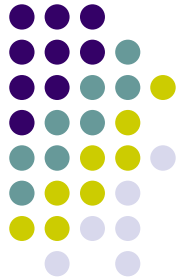
  電子署名技術を利用し、情報の正当性を検証できる枠組を構築
  - **soBGP**
    - CISCO:　James Ng, Russ White, …　(IETF55, 2002)
  - **S-BGP**
    - BBN:　Stephen Kent, Charles Lynn, …　(IETF42,1998)

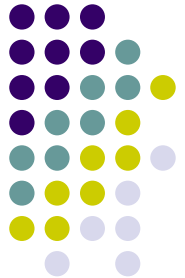


soBGP vs. S-BGP

- 解こうとする問題は、両者ともほぼ同じ
  - 経路情報のOrigin ASが正しいか検証する
  - 経路情報のAS PATHが正しいか検証する
- では、違いはどこにあるか？
- ここでは
  - soBGPとS-BGPそれぞれの概要を示し、
  - 違いを比較する

soBGP

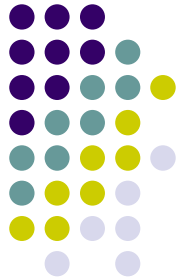




soBGPの証明書

- EntityCert
  - **あるASにおいて、そのAS番号と、そのASで用いる公開鍵**(public key)**または公開鍵の束の関係を証明するもの**
    - **例：** AS7521**の持つ公開鍵**
- AuthCert
  - **あるASが、あるアドレス空間の広告を認可する証明書**
    - **例：** AS7521**は**210.173.160.0/19**を広告できる**
- PrefixPolicyCert
  - AuthCert ＋ Prefix**に関するポリシー**
    - **ポリシーの例： そのアドレス空間のなかで許される最大**prefix**長など**
- ASPolicyCert
  - **あるASから見た、他の**AS**との接続関係を証明するもの**
    - **組み合わせてAS**パスの正当性を確認するための「パーツ」

※**通信路の安全は、**IPSec**や**BGP**ピアでの**MD5**利用で対応。**

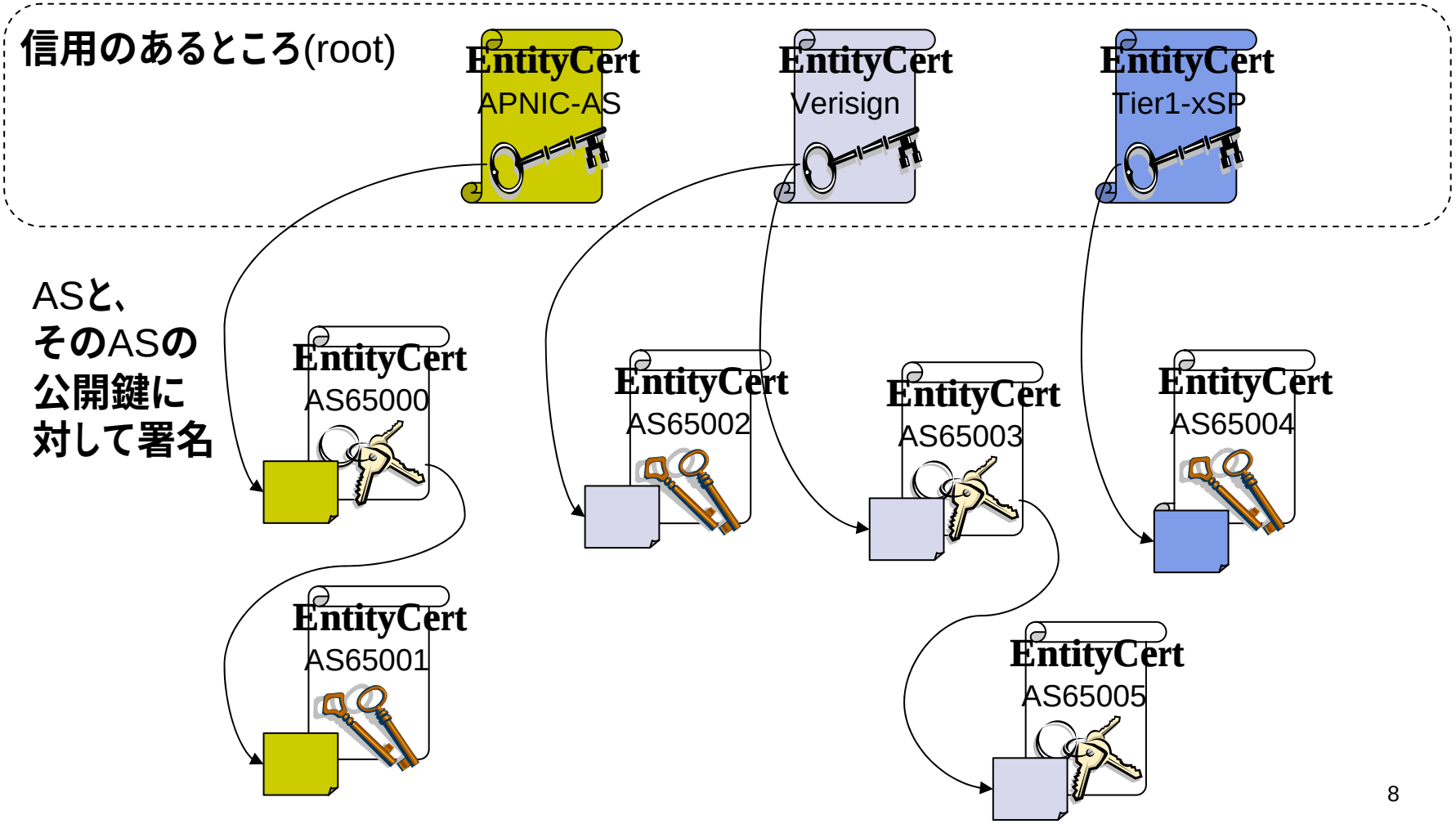


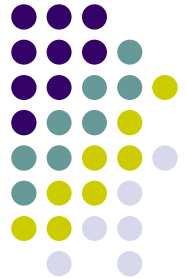
(1)各ASが持つ鍵の認証

- **鍵配送問題** (key distribution)
  - **データの署名や暗号化に使う鍵を受け取ること、そして受け取った鍵が、我々が持ち主と信じる参加者のものであると検証するための何らかの手段がなければならない。**

- EntityCert
  - **鍵配送に関しては、**soBGP**では**EntityCert**を用いる。**
  - EntityCert**とは、**AS**番号を公開鍵**(public key)**または公開鍵の束に結びつけるもの。**
    - **その公開鍵は、そのAS**が他のさまざまな証明書に署名するときに用いる秘密鍵**(private keys)**に対応するもの**
    - TLS(Transport Layer Security) **やIPsecと似ている。**
  - **あるEntityCertを受け取ったときに我々が直面する主な問題は、その証明書が運ぶ鍵が本当にそれを広告したASの鍵であるかどうかを知ること。**
  - soBGP**ではこの問題を、第三者機関が署名したEntityCertを要求し、このAS**がこの鍵を所有していることを検証することで解決する。

(1)各ASが持つ鍵の認証



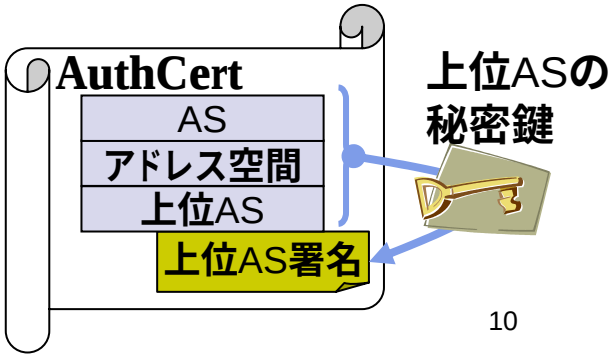


(1)各ASが持つ鍵の認証

- EntityCert (cont'd)
  - **少数の**"root key"**を別経路（インターネット以外）で配送することにより、（インターネット上で）広告される**EntityCert**を検証することができるようになる。**
  - **さらにこれらによって、正しい**ASm/key**の組に関するデータベースを構築でき、さらに多数の**EntityCert**を検証可能となる。**
  - **このように**EntityCert**は、例えば最上位のバックボーンサービスプロバイダや**Verisign**のような鍵認証サービスプロバイダなどの少数の良く知られた**EntityCert**の上に構築された信頼の網("Web of trust")を形成する。**
  - **各**AS**が**EntityCert**で配送するのは公開鍵。秘密鍵は完全に機密とし、ネットワーク上の安全な機器に保管しておき（場合によってはネットワーク上になくとも良い）、必要に応じて証明書に署名する。公開鍵は特別な保護機構など必要なく、晒しておいてよい。**

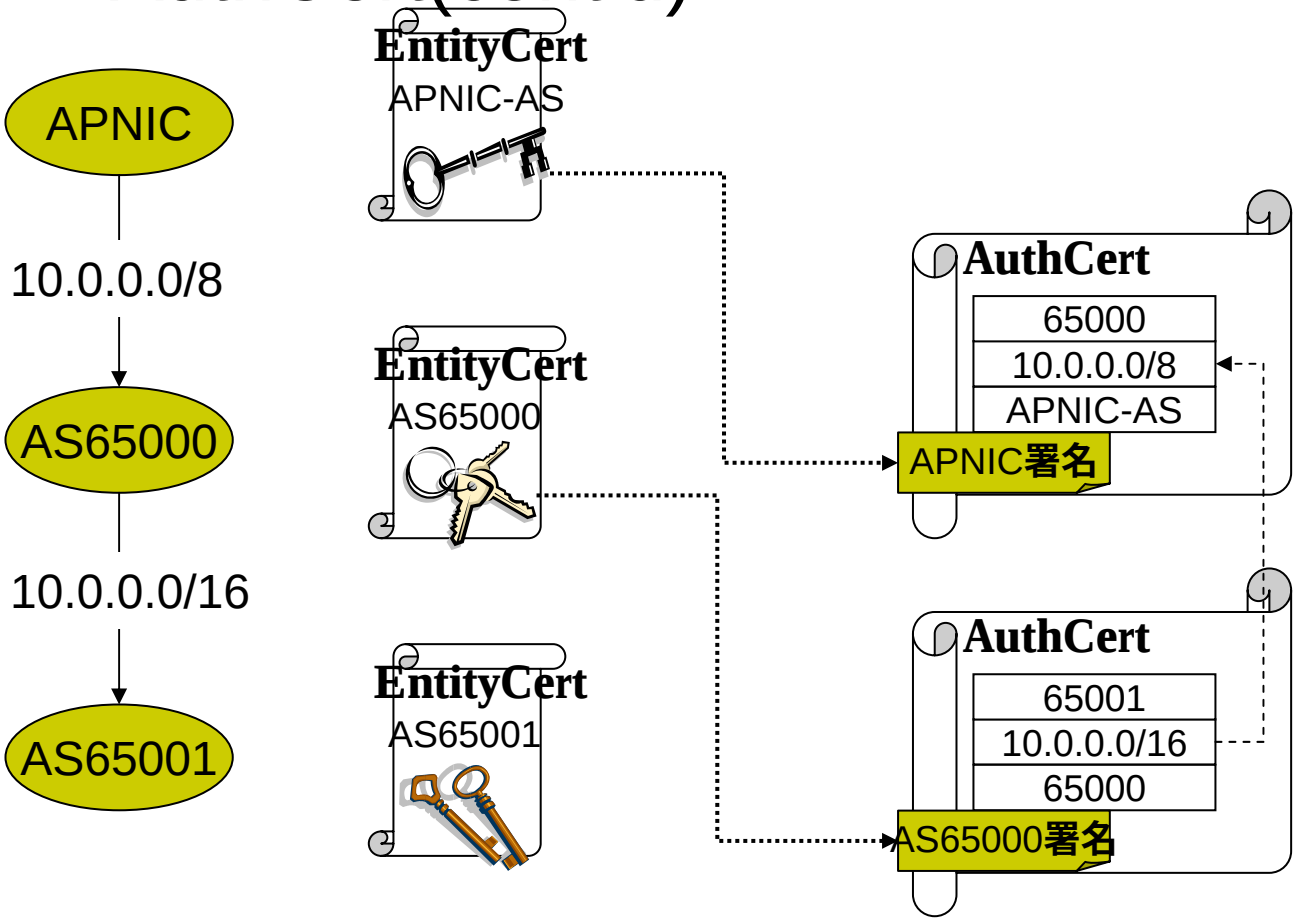
(2)PrefixやIPアドレスの認証

- AuthCert
  - ASごとに公開鍵を配送可能となったので、各ASがあるアドレス空間の広告を認可する証明書を構築できる。これを認可証明書(Authorization Certificate)、AuthCertと呼ぶ。
  - AuthCertは、ASと、そのASが広告するアドレス空間を結びつける。
    - 具体的には、
      - アドレス空間(Prefix)
      - そのアドレス空間を広告するAS
      - そのアドレス空間をそのASに割り振った上位AS
      - その上位ASの秘密鍵で付した署名



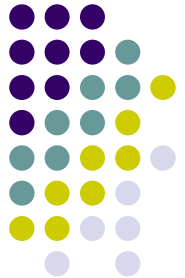
(2)PrefixやIPアドレスの認証

- AuthCert(cont'd)



★確認(2)
・10.0.0.0/16のSuperset 10.0.0.0/8のAuthCertの署名をAPNIC-ASの公開鍵で検証し、上位ASが割振る権限を持つかを確認

★確認(1)
・10.0.0.0/16のAuthCertの署名をAS65000の公開鍵で検証

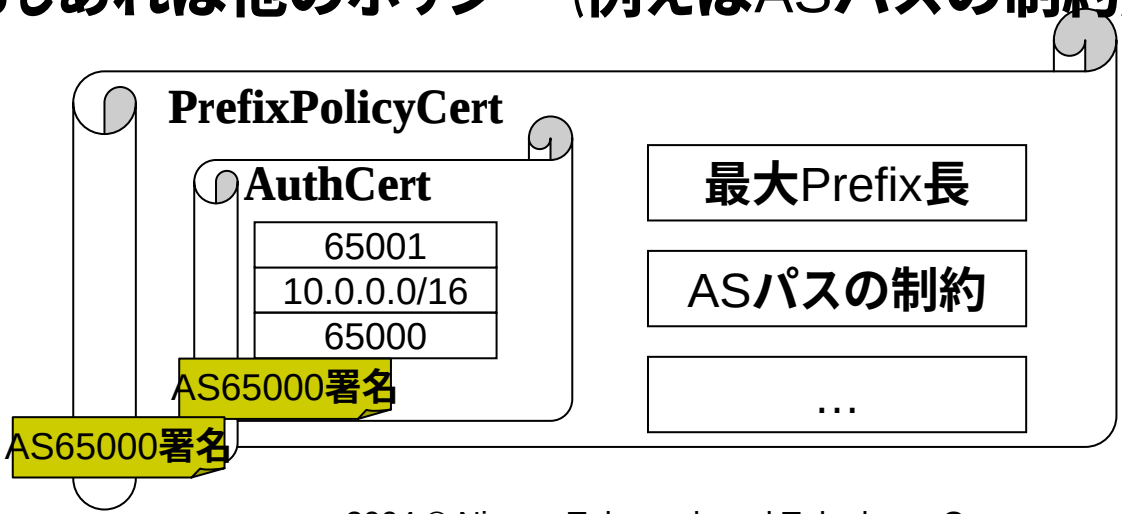


(2)PrefixやIPアドレスの認証

- AuthCert (cont'd)
  - **プロバイダでは何らかのデバイスにて、アドレス空間と、その空間内の**prefix**の広告を認可された**AS**との対応表を構築する。そのデータベースに対して、受け取った**Update**メッセージを検証する**
  - **ここでは個々の**prefix**でなくアドレス空間を用いている。なぜなら**AuthCert**はそのアドレス空間内であれば**prefix**をいくつでも広告できることを認めているから。これによってシステム内の証明書数を減らし、必要とされる暗号処理全体を減らすことになる。**
    - **もし**prefix**ごとに認可したいなら、個々の**prefix**ごとに**AuthCert**を構築しても良い**

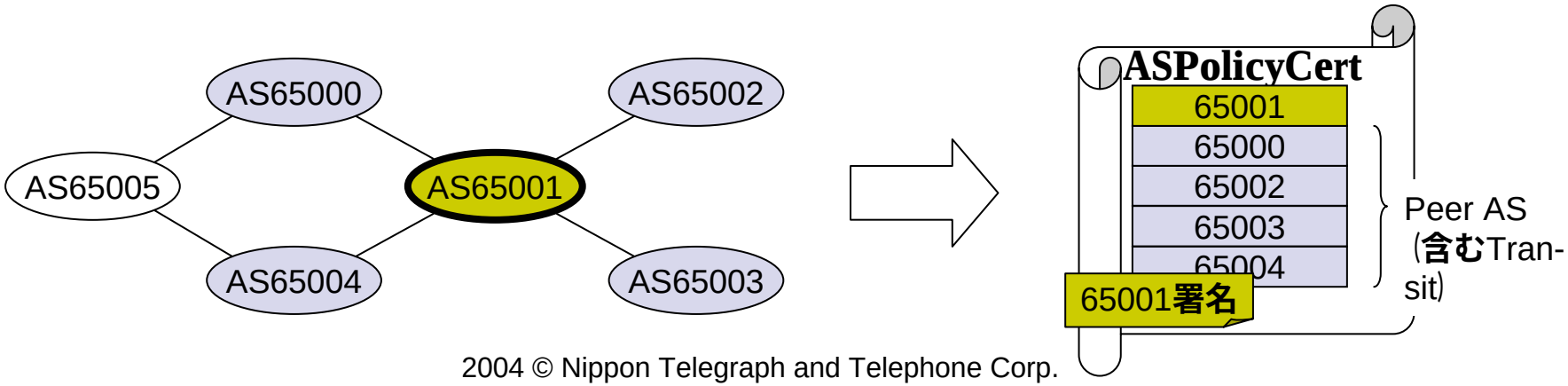
(2)PrefixやIPアドレスの認証

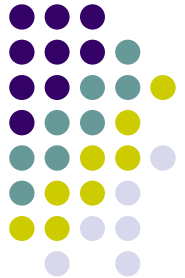
- PrefixPolicyCert
  - PrefixPolicyCertは、一つのAuthCertと幾つかのポリシー、そしてそのASの秘密鍵で作成された署名から構成される。
    - AuthCertはsoBGPでは個々の証明書として広告されるのではなくPrefixPolicyCertに包まれる。
  - ポリシーとは、そのアドレス空間の中で許される最大prefix長や、もしあれば他のポリシー（例えばASパスの制約）など。



(3)ASパスの認証

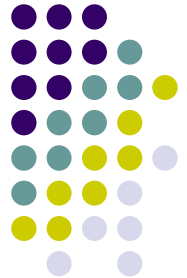
- 目標
  - ある経路を広告するASが本当にその目的地までのパスを持っているのかを検証できること
  - soBGPではインターネットワーク全体のパスに関する構成図を構築する
- ASPolicyCert
  - インターネットワークに接続した各ASは、ピアのリストを含み、その発生者(originator)の秘密鍵で署名されたASPolicyCertという証明書を構築する。
  - 「トランジットピア」のリストを用いてインターネットワークの構成図を構築する
  - 各ASのASPolicyCertをつなぎ合わせて全体のトポロジーを構成する。
    - AS間の接続性を確認する際には、あるAS-xが別のAS-yに接続していると言うとき、逆にAS-yからみてAS-xが接続しているかが鍵となる。





(4)証明書の配送

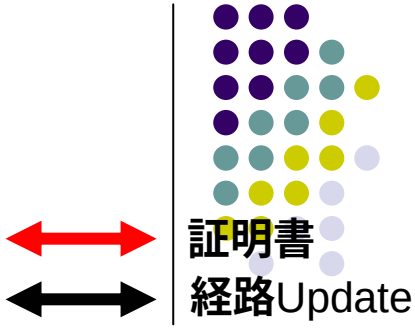
- 課題
  - セキュリティに関する課題の一つにセキュリティ情報をインターネットワーク上でどう配送するかがある。
  - 経路に関するセキュリティ情報を経路システムを使って配送したくない。
- 解法
  - soBGPドラフトでは、新たなBGPメッセージとしてSECURITYメッセージを定義。EntityCert、PrefixPolicyCert、ASPolicyCertを配送するときはこのメッセージ型を使う
  - それ以外の方法もIETFでは検討されている。



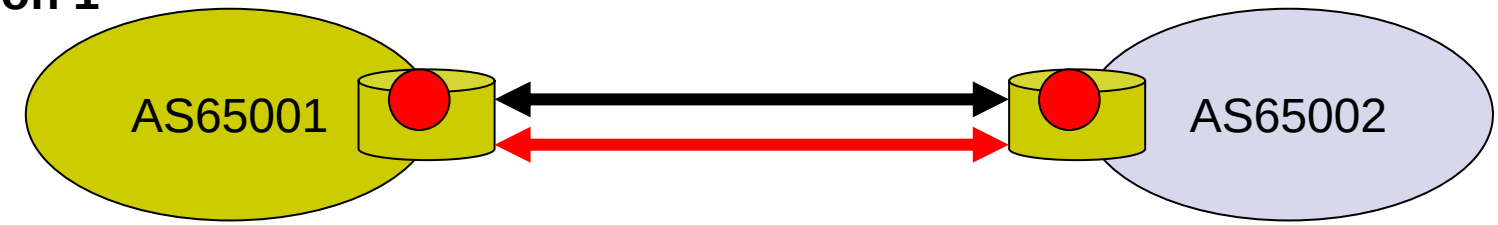
soBGPの普及

- **実際運用されているところに普及させるのは一番難しい問題。**soBGP**では広範囲なオプションを用意している。**
- Option 1
  - **直接証明書を交換し、ボーダールータで処理する方法**
    - **受け取った証明書を検証できるぐらい暗号処理力のあるルータが、証明書を交換し、証明書を処理し、データベースを構築する。これに基づき受け取った**Update**に関してセキュリティ確認する。**
    - **エッジとなるルータのみで証明書の処理を行い、同じ**AS**間はそれを共有すればよい**
- Option 2
  - **ボーダールータは証明書を受け取るが、処理はしない方法**
    - **受け取った証明書は、それぞれの内部処理サーバに転送されて処理される。**
    - **ボーダルータが**Update**を受け取ったとき、サーバに問い合わせる。**
- Option 3
  - **処理サーバ間で直接証明書を受け渡しする方法**
    - **証明書はサーバ間で直接受け渡し**
    - **ボーダルータは、**Update**が来たときにサーバへ問い合わせる**

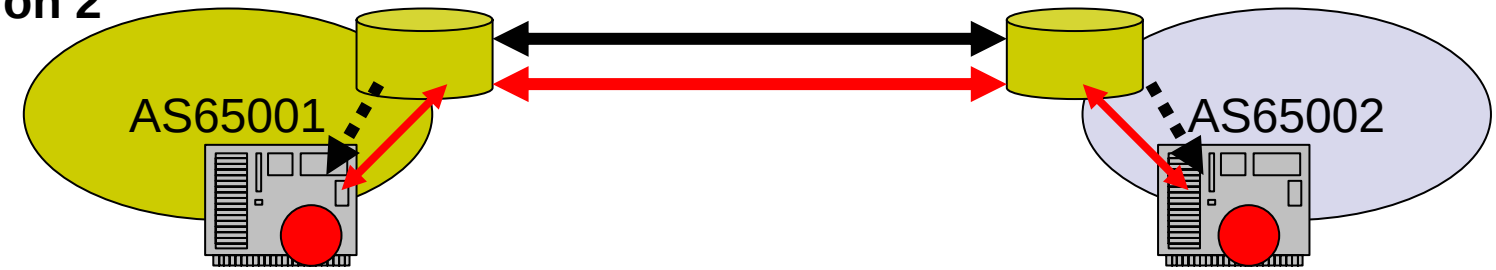
証明書の配送経路



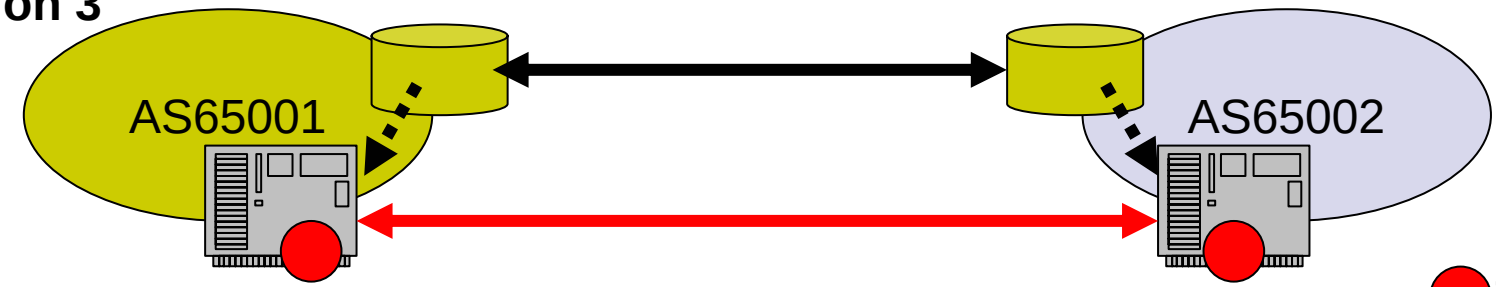
Option 1



Option 2

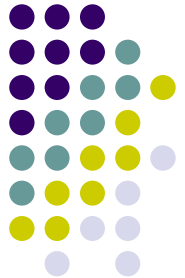


Option 3



証明書処理

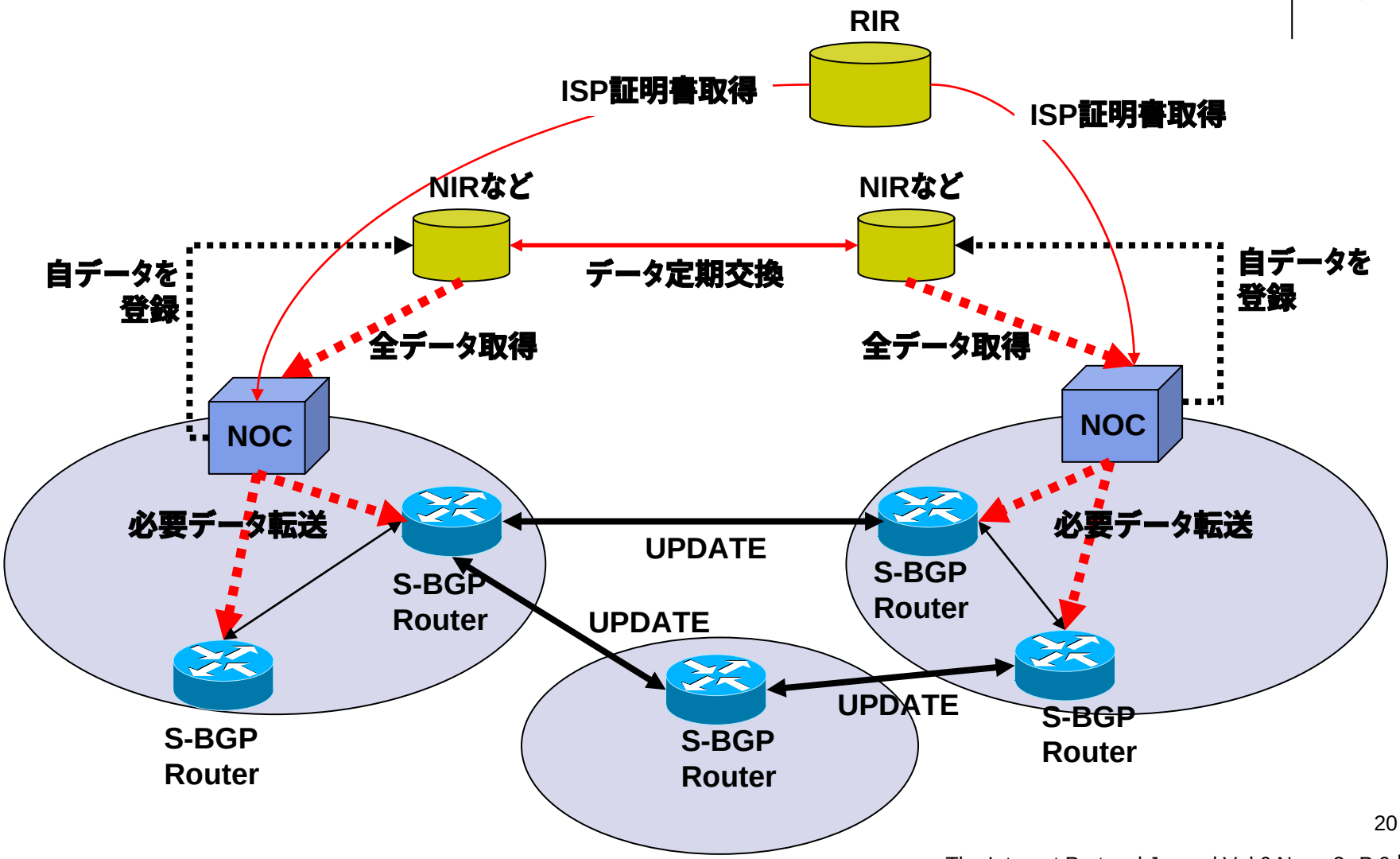
S-BGP



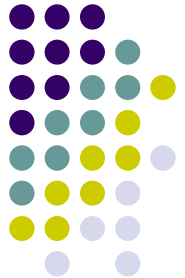
S-BGPの構成要素

- Public Key Infrastracture (PKI)
  - AS, IP prefixとISP公開鍵との関連付けを表現
  - IPSec用の鍵
- Address Attestation (AA)
  - AS と IP prefixとの関連付けをIP所有のASが署名
- Route Attestation (RA)
  - RAを受け取る隣接するAS(の集合)をS-BGPルータが署名
- IPSec
  - BGPセッションの通信路を守る

S-BGPの構成要素間の関係

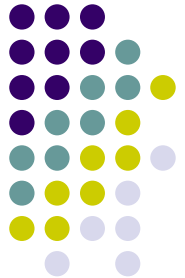


The Internet Protocol Journal Vol.6 Num. 3 P.9より引用



Attestation (証明書)

- Address Attestation
  - AS と IP prefixとの関連付けを証明
  - ISPが署名を行なう
  - PKIリポジトリに保管, 参照される
- Route Attestation
  - RAを受け取る隣接するAS(の集合)を証明
  - S-BGPルータがISP(AS)の代理で署名
  - UPDATEの新しいパス属性(ATTEST属性, optional, transitive)で伝播

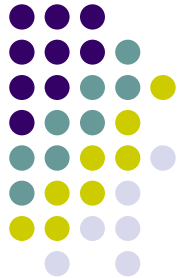


PKIリポジトリー

- **登録データ**
  - Certificate
    - ISP**公開鍵と**AS**の関連付け**
    - ISP**公開鍵と**IP prefix **の関連付け**
    - **ルータ公開鍵と**AS**との関連付け**
  - Certificate Revocation List (CRL)
    - **失効証明書リスト**
  - Address Attestation (AA)
    - IP Prefix**と**AS**番号の関連付け**
    - **一度割り当てられると更新頻度が大きくないため，リポジトリ経由の配布で十分と考える**

- **登録データの管理/更新/利用**
  - RIR, NIR**などが保持，定期的に交換**
  - ISP**は自データを登録，その他の全データを取得**, NOC**等に蓄積**

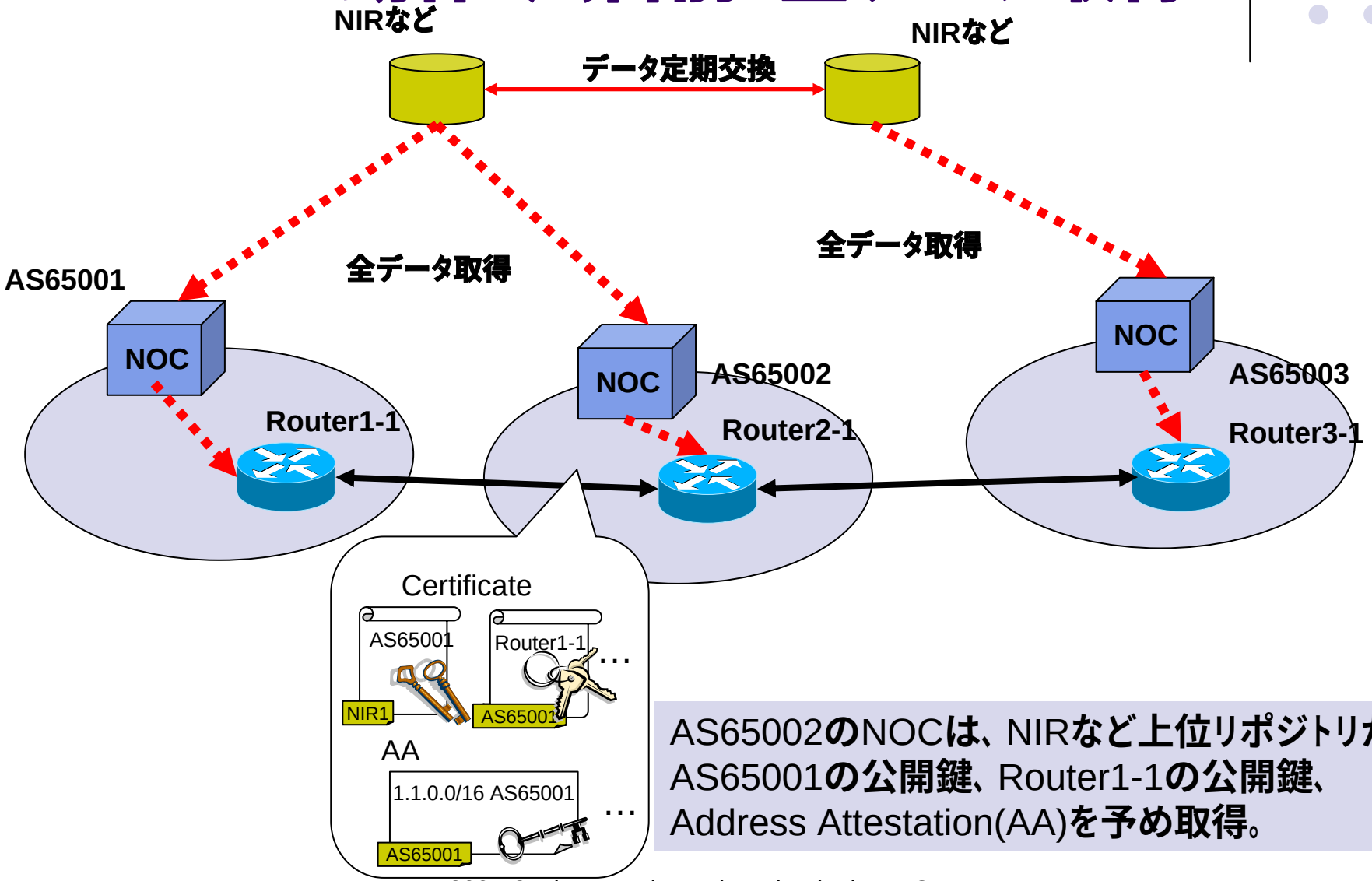
※Route Attestation**は、**UPDATE**メッセージで送付される。**



UPDATEの有効性チェック

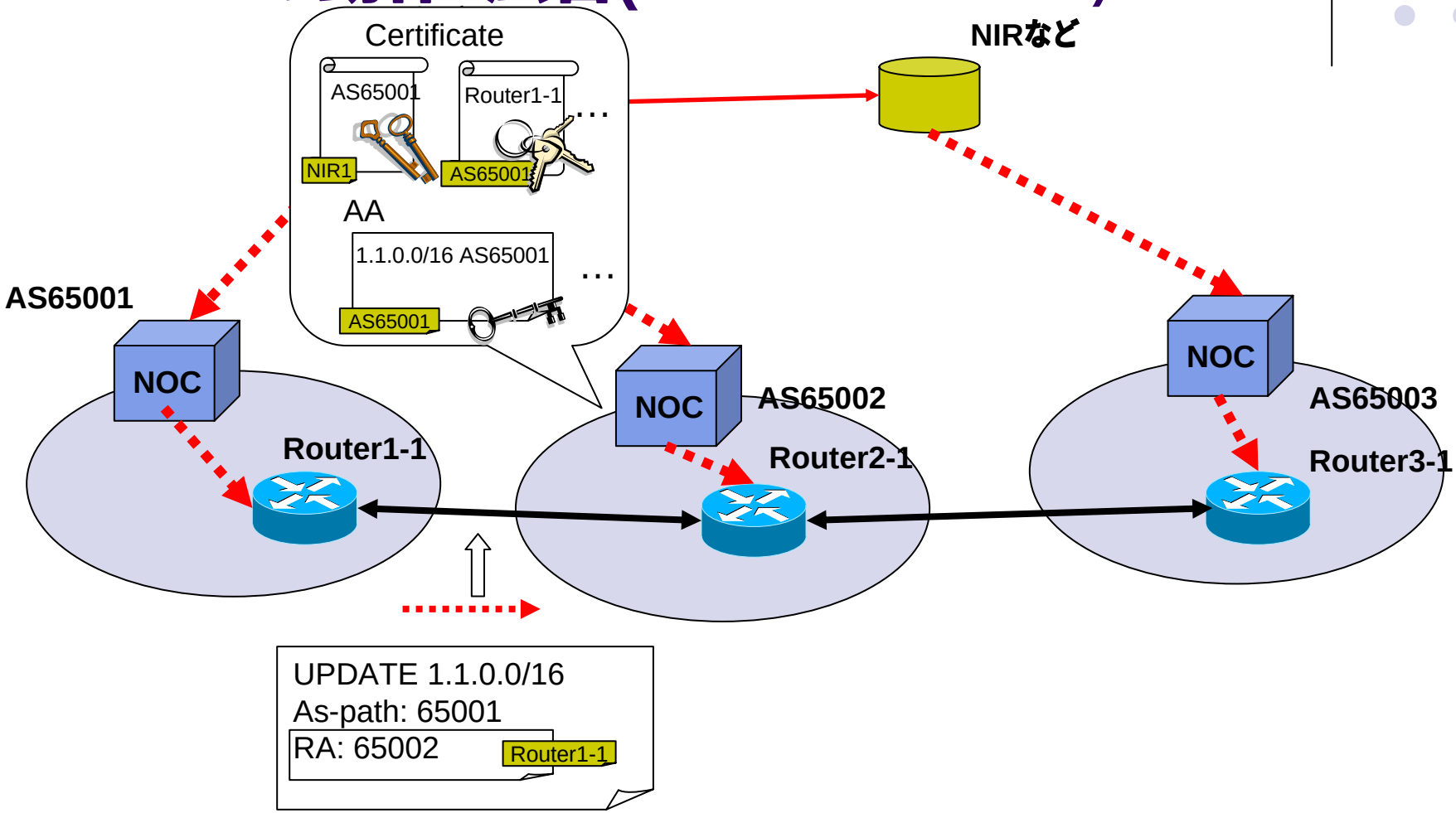
- AS_1からのAS_nまでたどった経路のチェックのために，AS_{n+1}が要求するのは
  - ① Prefix を所有するISP の公開鍵
  - ② Prefix の AA
  - → ①②から 経路のオリジンASが判明
  - ③ たどってきたASのRA
  - ④ 通ったルータの公開鍵
  - → ③④から AS Pathの検証可能

S-BGPの動作：広告前・全データ取得



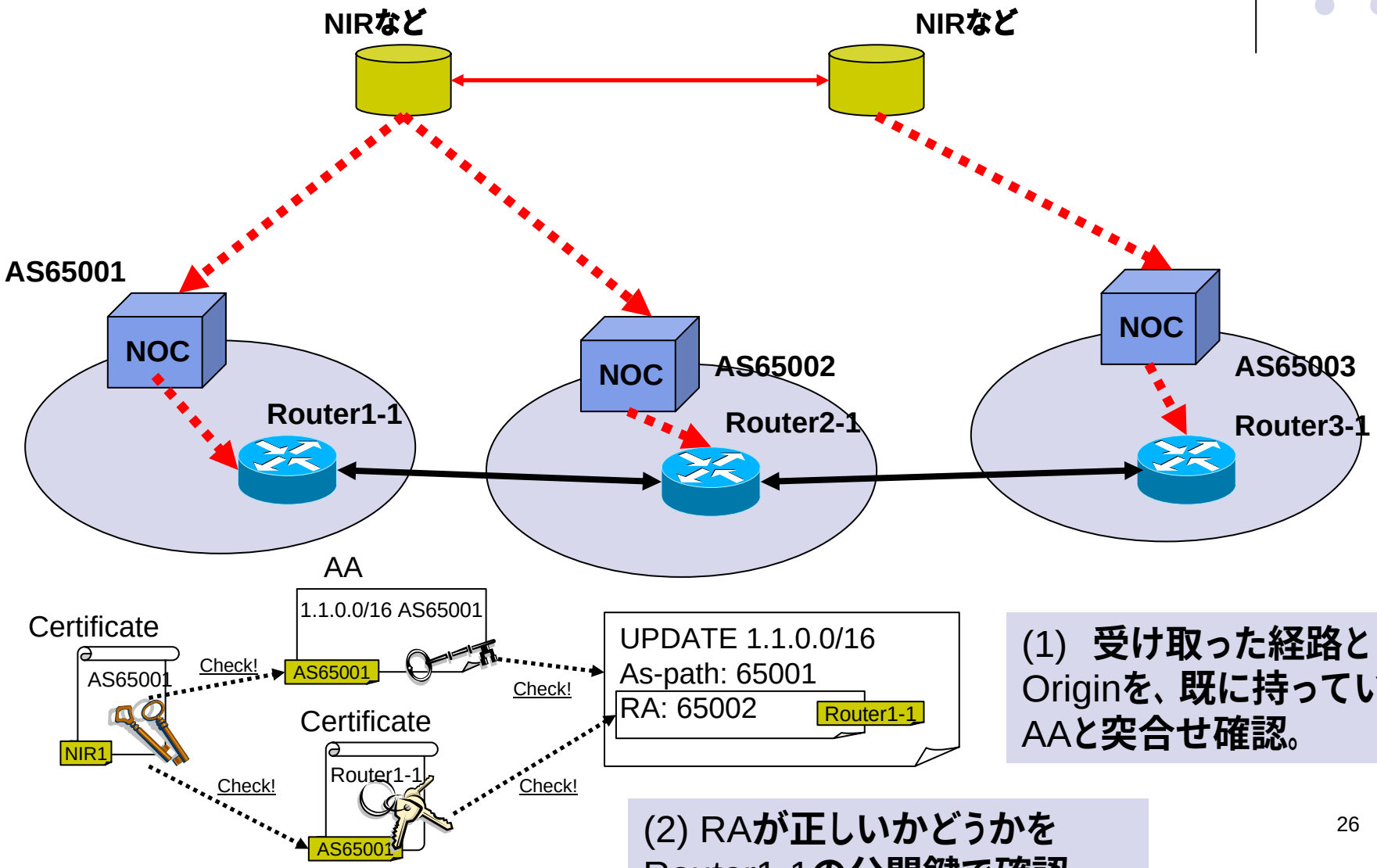
AS65002のNOCは、NIRなど上位リポジトリから
AS65001の公開鍵、Router1-1の公開鍵、
Address Attestation(AA)を予め取得。

S-BGPの動作：広告(AS65001→AS65002)

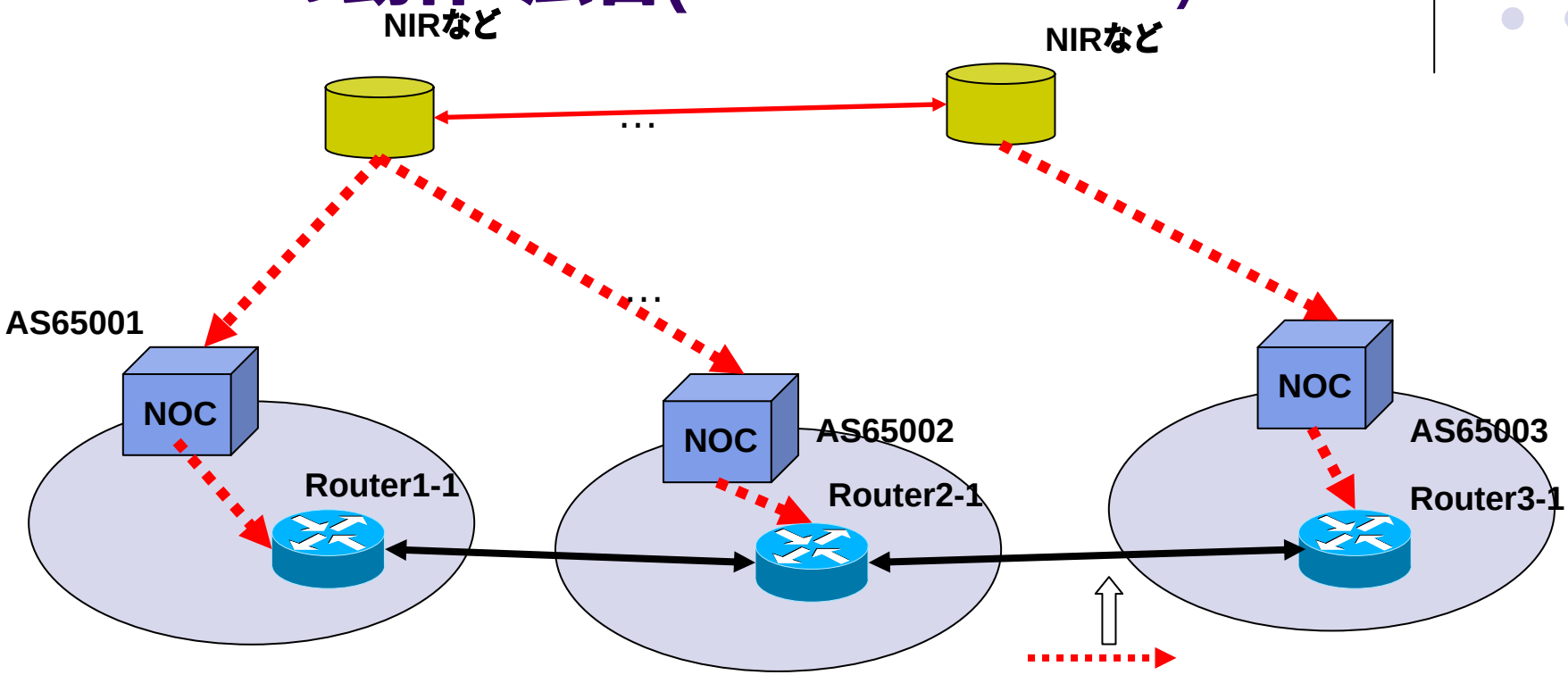


AS65002のルータ2-1は、AS65001のRouter1-1からUPDATEを受ける（Route Attestation含む）。

S-BGPの動作：検証@AS65002

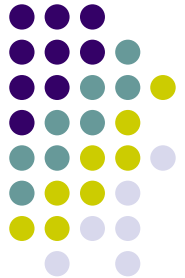


S-BGPの動作：広告(AS65002→AS65003)



(1) AS65002のRouter2-1は、ASを代表してRAを作って署名し、既存のRAに付加して隣のAS65003へ送る。

比較



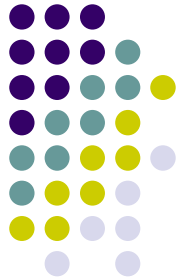
soBGPとS-BGPの比較(1)

	soBGP	S-BGP
公開鍵	“EntityCert” **各ASが持つ公開鍵を、上位機関が証明。階層構造は定義せず。信用できるもの同士** ⟨Web of trust⟩	PKIを利用。”certificate” **各ASが持つ公開鍵を、上位レジストリが証明。ルータの鍵はASが証明。最上位(root)はICANN、IANA。即ち現在のレジストリ階層を基盤。**
アドレス空間とASの関係	“AuthCert”と”PrefixPolicyCert”	“Address Attestation”
AS間の関係	“ASPolicyCert”	“Route Attestation”
証明書の配送	・”**Cert”はBGPのSECURITYメッセージで配送。またはIETFで検討中の別の配送手法を使い、BGP以外で転送。**	・Certificate, CRLs, Address Attestation **はリポジトリに登録。リポジトリへの登録、参照はBGP以外のセッション。** ・Route Attestationは、S-BGPのUPDATEメッセージのATTEST属性で配送。

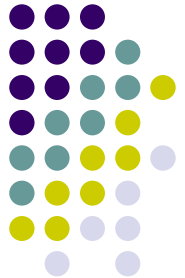
soBGPとS-BGPの比較(2)

	soBGP	S-BGP
Originの確からしさ	OK: Root はさまざま。署名者が信用できる範囲で 確認可能(Web of trust)	OK: レジストリ階層に基づく構成。信用度は高いと思われる。
AS Pathの確からしさ	OK: ASパスのグラフを構築し確認	OK: UPDATEメッセージ伝達経路に沿った確認
BGP4への変更箇所	メッセージ型としてSECURITYメッセージを追加。証明書類 (*Cert)を伝送。	UPDATEメッセージに、path attribute (ATTEST)を追加。Route Attestationを伝送。
段階的普及 (既存BGPとの共存)	可能	可能
ASパスの確認処理	いつでも (遅延評価可能)・どこでも (ルータ以外でも) 可能	メッセージを受けたときに、ルータで実施 (アドオンカードの必要性)
情報伝達のBGPセッション依存度	Option 3の方式であればBGPに非依存。 それ以外はBGPに依存。	Certificate, CRLs, AAは非依存。 RAはBGPに依存 (UPDATEメッセージで送受される)
署名の階層における唯一のRoot	存在しない。署名者を信用できる範囲で利用。	現在のアドレス・ASN割り当て階層 (ICANN/RIR/NIR….)
証明書を経路情報より早く入手できる？	・証明書はアドレスが割振られたときに作成。作成後すぐに配布可能。即ちUPDATE到着時に証明書は利用可	・Certificate、AAは事前準備。 ・RAはUPDATEとともに送信。RA確認はUPDATE到着時。処理時間要。

soBGPとS-BGPの比較(今回できなかったもの)



- パフォーマンス
  - データ量、計算量、必要な処理能力…
  - 客観的に比較してみることが必要。
    - まずは机上で。実装がS-BGPしかない。
    - S-BGPの文書では、一応計算量を見積もっている。
- 移行
  - 非soBGP/S-BGP ASが入っているときの影響



まとめ

- Origin ASの認証
  - 比較的実現しやすそう
  - S-BGP、soBGPともに、あまり差があるとは思えない。
    - RIRなど「中央集権型の階層関係」を用いる(S-BGP)か
    - 「分散型」Web of Trustを用いるか (soBGP) か
- ASパスの認証
  - 必要性は高い
  - しかし、どの方法でも実現性には疑問。

Reference

- soBGP
  - ftp://ftp-eng.cisco.com/sobgp/index.html
  - draft-white-sobgparchitecture-00
  - draft-weis-sobgp-certificates-02
  - draft-ng-sobgp-bgp-extensions-02
  - draft-white-sobgp-bgp-deployment-01
- S-BGP
  - http://www.net-tech.bbn.com/sbgp/sbgp-index.html
  - draft-clynn-s-bgp-protocol-01
  - draft-ietf-pkix-x509-ipaddr-as-extn-02