
IRS Workshop Update
NTT Communications 吉田友哉
Intec NetCore 近藤邦昭
JANOG15 in 掛川

IRS (Inter-domain Routing Security) Workshop の動機

- ドメイン内はISPが個別に防御
  - Route-Filter, Access-Listなど
- Inter-DomainとなるIX設備は事業者が防御
  - データセンタのセキュリティなど

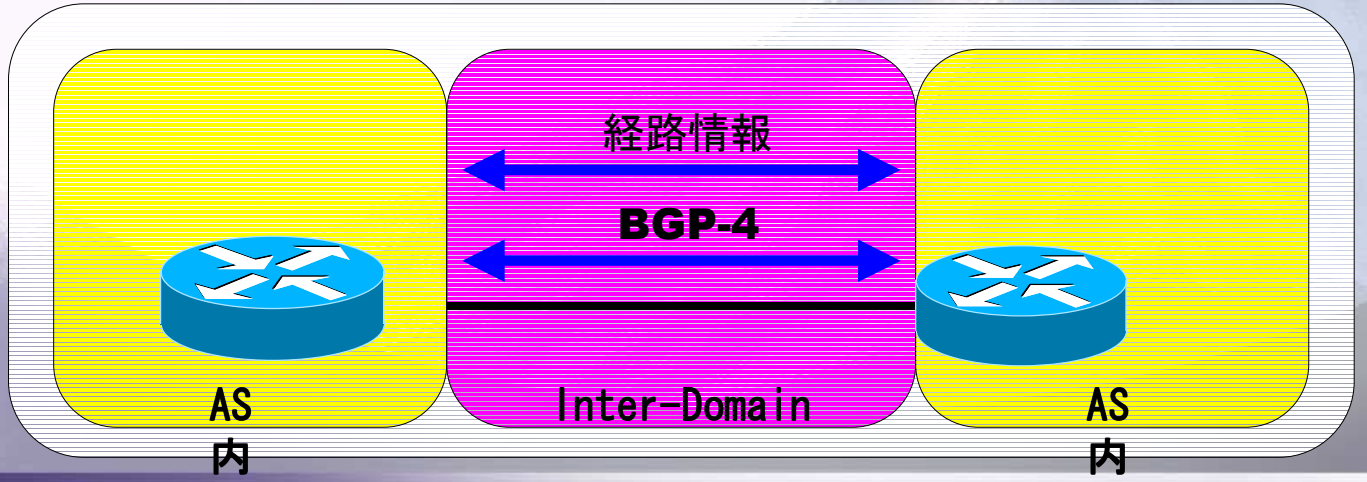
- しかし、Inter-Domainのプロトコル的な防御、Inter-Domainを流れている経路そのものの信憑性などについては、ISPなどが個別にその信憑性を確かめるなどは難しい
  - 経路自体は綿密な運用である程度は回避可能
  - プロトコル的な問題は、そもそも対応が難しい

- IRSの現状と問題点を明らかにする必要がある

IRSとは （ここでのフォーカス）

- AS内についてはISPで個別に対応しているのが前提
- Inter-Domainで使われているプロトコルのセキュリティ上の問題
- Inter-Domainでやり取りされる経路情報の信憑性の維持に関する問題
- その他、Inter-Domainネットワーク上で、ASが個別に対応してもインターネット全体として、セキュリティ上の問題が発生しうる問題を取り扱う

- 基本的に、ISPが個別に対応すればよいことについては扱わない



過去のIRS

- 第一回：IRS1
  - 2004年7月7日
  - Cisco赤坂
  - 50名限定
  - IRSの動向、TCP Vulnerability対策など
- 第二回：IRS2
  - 2004年10月15日
  - 神田神保町　Hosted by JPCERT/CC
  - 60名限定
  - sBGP/So-BGP, xSPでの一般的Filterについて、uRPFなど
- 第三回：IRS3
  - 2005年1月13日
  - Cisco赤坂
  - 50名限定
  - DDoS AttackのTips、xSPでのFiltering Policyの提案など

扱われている内容

- TCP Vulnerability
- DNS Anycast + uRPF
- sBGP/so-BGP
- DDoS Attack Defencing Tips
- xSP Generalized Filtering Policy Proposal

TCP Vulnerability

- 2004年4月21日の公表を受けて
  - ISPの対応
    - eBGP Peer に対して、MD5を積極的に実施 or 相手からリクエストがあればMD5を実施
  - IX事業者の対応
    - 基本的には関与せず、JPIXではIXセグメントのアドレスをFilter
- 各ベンダでのMD5の実装の差異について
  - 相互接続における問題の報告と情報共有
- MD5以外の対応策について議論
  - GTSM（Generalized TTL Security Mechanism）:RFC3682
  - Unicast RPF
  - Transit Filtering / Receive Filtering
  - Private Address の利用
    - ICMP echo reply が filter される可能性あり
  - Non routable での対応
    - IXでは有効か

DNS Anycast + uRPF

- DNS Anycast / uRPF とは
  - DNS Anycast（RFC3258参照）
    - Root DNS の負荷分散、耐障害性を実現するAnycast技術
  - uRPF: unicast Reverse Path Forwarding（RFC3704参照）
    - 経路情報を用いたIngress Filtering 手法＝uRPFも、最近では広く利用されつつある
- DNS Anycast と uRPF の複合利用時に、相互に干渉する恐れがあるため、その問題意識の共有、議論
  - Transit, Peer の関係等による非対称経路によるFiltering
  - マルチホームの問題をひきずっているに過ぎない

➔ DNS Hijack 問題

  - 継続議論、何らか文書にまとめる予定
- Coordinator
  - MEX石田さん、吉田

sBGP/So-BGP

- Routing Hijack などに代表される、ドメイン間の動的経路制御の脆弱性を解決する方法の1つとして挙げられている、sBGP/So-BGPに関する現状をまずは確認し、意識共有を図る

- So-BGP
  - ASやprefixの関係などを示す証明書を用いた経路等の検証を実施
  - 信頼の出来るroot定め（Web of Trust model）、rootによって署名された証明書を各ASが各自署名をして作成し、下流は上流の公開鍵で検証する
- sBGP
  - PKIを利用
  - あらかじめ、レジストリなどのrootが、ASの公開鍵と該当ASや、ASとprefixの関係などを証明したデータベースを蓄積し、ISPは上位レポジトリから取得したAAと、実際に配信されてきたRAとを比較し、情報の信憑性を検証する
- 両者とも根っこは同じで、OriginASの正しさ、AS-PATHの正しさを検証し、適切に経路配信がなされることがゴール

- 今年少し実装が出てきそうなので、継続的にwatchしていく

DDoS Attack Defencing Tips

- (D)DoS Attackをどのように回避するかについて議論
  - Ciscoが持つDDoS回避ツールのXT5600シリーズの手法についての解説(旧:Riverhead製品)
  - このほかxSPで利用可能と思われる手法について議論
    - uRPFを応用したもの
      - カスタマエッジに導入することで対カスタマのトラフィックについて、効率よく対応できないか?
    - Remote Triggered Black Hole
      - xSPの入り口で、不要なトラフィックを排除。そのときの問題点など
      - トラフィックを排除することで、サービス停止を招き、思うつぼでは?
    - IP source tracker
      - tracking対象のIPアドレスを事前に指定、そこ宛パケットのsourceの入力I/Fを把握
    - NetFlow利用の攻撃検知
      - Arbor製品のようなものを利用して検知できないだろうか?
      - 検知できれば、それを利用してワーニングをあげられないだろうか?

xSP Generalized Filter Policy Proposal

- xSP(特にBGPを運用しているようなところ)で、一般的に設定すべきFilterの設定とはどんなものであるかを検討し、文書化を目指す。
  - Packet Filter
    - 顧客収容ルータでのSpecial Use AddressのFilterとか
  - Prefix Filter
    - AS境界ルータでのDefault RouteのFilterとか
- 現状
  - 目次案が出来てきた状態
- 目標
  - 次回IRS(4月くらい)を目標にDraft版を出す予定
  - Draft版は、IRSで揉みjanog@janogからもコメントをもらう予定
- Coordinator
  - DTI馬渡さん


Any Comments or Questions