

IETF における標準化 ディプロイメント状況

関谷 勇司
東京大学 情報基盤センター
WIDE Project

2011年 IETF 標準化動向

- 以下のエリアから、主な WG を抜き出して動向を説明します
 - Routing Area
 - Ops & Mgmt Area
 - Security Area
 - Internet Area
 - Transport Area
- 2011年の動きに特化して説明します
- スライドは 33 枚あります
 - 20分 / 34枚 = 35秒/枚
- 時間の許す限り**爆速で**行きます
 - いつから 20分になった?? <= 今年

の前に。。。

- 直近の IETF
 - 82nd IETF : 台北 (台湾) 2011/11/13 - 18
- これからの予定
 - 83rd IETF : **パリ (フランス)** 2012/03/25 – 30
 - 84th IETF : バンクーバ (カナダ) 2012/07/29 – 08/03
 - 85th IETF : アトランタ (アメリカ) 2012/11/04 – 09
 - 86th IETF : オーランド (アメリカ) 2013/03/10 – 15
 - 87th IETF : **ベルリン (ドイツ)** 2013/07/28 – 08/02
 - XXXth IETF : **富士山 (日本?)**

ROUTING AREA 動向

Inter-Domain Routing (idr) WG

- RFC6286
 - Autonomous-System-Wide Unique BGP Identifier for BGP-4
 - BGP ID を 4-octet に拡張する
- Active Internet-Draft : 24本
 - draft-ietf-idr-add-paths-06
 - multipath 拡張
 - draft-ietf-idr-aigp-06
 - Accumulated IGP Metric Attribute for BGP
 - draft-ietf-idr-deprecate-as-sets-06
 - AS_SET と AS_CONFED_SET の使用を控える
 - いくつかの BGP 拡張と相性が悪い / 使用ケースが稀である
 - draft-ietf-idr-dynamic-cap-13
 - BGP Dynamic Update Capability

IS-IS for IP Internets (isis) WG

- RFC6119
 - IPv6 Traffic Engineering in IS-IS
- RFC6165
 - Extensions to IS-IS for Layer-2 Systems
- RFC6213
 - IS-IS BFD-Enabled TLV
- RFC6326
 - Transparent Interconnection of Lots of Links (TRILL) Use of IS-IS
- Active Internet-Draft : 6本
 - TRILL 関連 : 2本
 - Sequence Number 拡張 (replay attack)
 - IS-IS TE Metric

Keying and Authentication for Routing Protocols (karp) WG

- 2010年に作られた WG
 - まだ RFC は無い
 - 毎回 BoF は開催されている
- Active Internet-Draft : 6本
 - draft-ietf-karp-ospf-analysis-02, draft-ietf-karp-routing-tcp-analysis-00
 - Analysis of OSPF, BGP, LDP, PCEP, and MSDP Security
 - draft-ietf-karp-threats-reqs-03
 - Routing protocol に対する脅威とその解決への requirements
 - draft-ietf-karp-design-guide-08
 - Routing Protocol のメッセージを認証するための枠組み

Layer 2 Virtual Private Networks (l2vpn) WG

- RFC6074
 - L2VPN のためのシグナリングプロトコル定義 (LDP and L2TPv3)
- RFC6136
 - L2VPN OAM Requirements
- RFC6246
 - VPLS Interoperability
- Active Internet-Draft : 11本
 - draft-ietf-l2vpn-arp-mediation-18
 - L2VPN で結ばれたデバイス間での ARP 中継
 - draft-ietf-l2vpn-pbb-vpls-pe-model-04
 - PBB + VPLS PE を行う際の拡張定義
 - draft-ietf-l2vpn-vpls-mcast-09
 - VPLS における Multicast Tree の多重化

Layer 3 Virtual Private Networks (I3vpn) WG

- RFC6368
 - BGP/MPLS IP VPN
- Active Internet-Draft : 9本
 - draft-ietf-l3vpn-ospfv3-pece-09
 - PE-CE 間のルーティングに OSPFv3 を用いる拡張
 - draft-ietf-l3vpn-2547bis-mcast-10
 - MVPN に必要な MPLS/BGP エlement 定義
 - Multicast VPN (MVPN) 関連のドラフト数本
- VPN for Datacenter
 - Cloud のためのネットワーク取り回し

Routing Area Working Group (rtgwg)

- Active Internet-Draft : 1本
- 先日の IETF での BoF の主な話題
 - IP/LDP Fast Reroute using MRT (Maximally Redundant Trees)
 - Algorithms for computing MRT for IP/LDP Fast Reroute
 - 要するに MRT を使った IP/LDP (Label Distribution Protocol) の Fast Reroute がアツい

Secure Inter-Domain Routing (sidr) WG

- RFC ずっと無し
 - だいぶ前からある WG なんですが。。。
 - 難しいんですね
- Active Internet-Draft : 29本 !
 - draft-ietf-sidr-arch-13
 - draft-ietf-sidr-ghostbusters-15
 - draft-ietf-sidr-origin-ops-13
 - draft-ietf-sidr-res-certs-22
 - draft-ietf-sidr-rpki-rtr-20
 - 番号に苦労が見られます
 - RFC Editor Queue にたまっているものが多い
- 先日の IETF での BoF
 - BGPSEC ネタ : 5件
 - RPKI => BGPSEC (Prefix Validation) という当然の流れ

OPS & MGMT AREA 動向

Address Resolution for Massive numbers of hosts in the Data center (armd) WG

- Active Internet-Draft : 2本
 - 主に Problem Statement
- Large L2 Network における ARP storm の解決
- 先日の IETF での BoF
 - Data Center Architecture
 - Problem Statement
- まだ Problem Statement と分析の段階

Domain Name System Operations (dnsop) WG

- RFC6168
 - Requirements for Management of Name Servers for the DNS
- RFC6303
 - Locally Served DNS Zones
- RFC6304
 - AS112 Nameserver Operations
- RFC6305
 - PRISONER.IANA.ORG !
 - 攻撃じゃないよー
- Active Internet-Draft : 3本
 - draft-ietf-dnsop-dnssec-dps-framework-05
 - 組織もしくはゾーン管理者が DNSSEC の Policy と実オペレーションを定義するためのフレームワーク
 - draft-ietf-dnsop-resize-13
 - UDP パケットに収まる応答サイズに関する考察
 - draft-ietf-dnsop-rfc4641bis-08
 - ゾーン管理者への DNSSEC 指針

Global Routing Operations (grow) WG

- RFC6382
 - Unique Origin ASNs per Node for Globally Anycasted Services
 - 32bit AS を使い、Anycast Service Node はそれぞれ独自の Origin AS を使うことを推奨する BCP
- RFC6396
 - MRT Routing Information Export Format
 - ようやく RFC になりました
- RFC6397
 - Routing Information Export Format with Geo-Location Extensions
- RFC6441
 - Time to Remove Filters for Previously Unallocated IPv4 /8s
 - 時代を反映した RFC ですね
- Active Internet-Draft : 6本
 - BGP Monitoring Protocol
 - FIB Suppression with Virtual Aggregation
- 先日の IETF における BoF
 - IX BGP Route Server Operations
 - Jumbo Frames at IXs

IPv6 Site Renumbering (6renum) WG

- IETF 81 から
- 「IPv6 の Renumbering は IPv4 より簡単にできるはずだ!!」が実現できてないのはなぜなのを分析する WG
- Active Internet-Draft : 3本
 - draft-carpenter-6renum-static-problem-00
 - draft-jiang-6renum-enterprise-01
 - draft-liu-6renum-gap-analysis-02
- 先日の IETF での BoF
 - 上記 3つのドラフトに対する発表
 - どうなるかわかりませんが、これから

Operational Security Capabilities for IP Network Infrastructure (opsec) WG

- RFC6094
 - Routing Protocol に使う暗号認証アルゴリズムの実装要求をまとめた文章
- RFC6192
 - Router の Control Plane を悪意あるトラフィックから守るための指針
- RFC6274
 - IPv4 プロトコル実装に関するセキュリティ評価
 - ヘッダの各フィールドのチェック方法と、IP ヘッダオプションの取り扱いに関する注意事項
- Active Internet-Draft : 1本
 - draft-ietf-opsec-efforts-17
 - Snapshot of the current efforts in various Standards Developing Organizations
- 先日の IETF での BoF
 - Operational Security Considerations for IPv6 Networks
 - 情報収集の段階

IPv6 Operations (v6ops) WG

- RFC : 10本
 - RFC6105 : IPv6 RA Guard
 - RFC6177 : IPv6 Address Assignment to End Sites
 - RFC6204 : Basic Requirements for IPv6 Customer Edge Routers
 - 末端の具体的な技術が RFC になって来ました
- Active Internet-Draft : 11本
 - IPv6 Multihoming without NAT
 - Operational Neighbor Discovery Problems
 - 攻撃者による /64 空間のスキャン問題と対策
- 先日の IETF での BoF
 - 2コマありました
 - ドラフトに関する発表と議論が主です
- 活発な議論が引き続き行われそうです

SECURITY AREA 動向

DNS-based Authentication of Named Entities (dane) WG

- IETF80 から
- RFC6394
 - DNS Based Authentication of PKIX
 - TLS で使う証明書を DNS のレコードを用いて認証するにあたっての Use Cases と Requirements
- Active Internet-Draft : 1本
 - draft-ietf-dane-protocol-12
 - こっちが先じゃないの？
 - TLSA レコードの定義

Transport Layer Security (tls) WG

- RFC6066
 - TLS Extensions : TLS 1.2 への新たな属性の追加
- RFC6176
 - Prohibiting Secure Sockets Layer (SSL) Version 2.0
 - SSL 2.0 の脆弱性を受けて、使用しないように勧告する文章
- Active Internet-Draft : 2本
 - draft-ietf-tls-dtls-heartbeat-03
 - TLS/DTLS に対する heartbeat 追加拡張 (keepalive/PMTU)
 - draft-ietf-tls-rfc4347-bis-06
 - DTLS (Datagram Transport Layer Security) 1.2

Managed Incident Lightweight Exchange (mile) WG

- IETF82 (先日の IETF から作られた WG)
 - Incident Information を迅速に共有し、かつ属性を capability として定義
 - RID (Real-time Inter-network Defense) に活用
- Active Internet-Draft : 3本
 - draft-ietf-mile-template-00
 - IODEF (Incident Object Description Exchange Format) を XML schema として定義

INTERNET AREA 動向

dnsext WG

- RFC6195
 - Domain Name System IANA Considerations
 - DNS の New RR や OpCode、RCODE の最新定義
 - Obsoletes RFC5395, Updated RFC1183/RFC3597
- Active Internet-Draft : 5本
 - draft-ietf-dnsext-dnssec-bis-updates-14
 - 幾つかの DNSSEC 関連 RFC の Errata 修正や、記述が足りない部分を補足
 - draft-ietf-dnsext-rfc2672bis-dname-25
 - DNAME RR (Zone Redirection) の改定版
 - Interoperability Issue for Reverse zone ?
- DNSSEC の deploy がとりあえず start したため、一段落した感もある

IPv6 Maintenance (6man) WG

- RFC6164
 - Using 127-bit IPv6 Prefixes on Inter-Router Links
- RFC6436
 - Rational Update to the IPv6 Flow Label Specification
 - Flow label が有効に使われていない現状への準拠と新たな利用方法
- RFC6437
 - Flow Label の最低限の要求について述べた文章
- RFC6438
 - Using the IPv6 Flow Label for Equal Cost Multipath Routing and Link Aggregation in Tunnels
 - トンネルされたパケットを効率的に ECMP させる手法
- Active Internet-Draft : 13本
 - draft-ietf-6man-addr-select-considerations-04
 - Address Selection Policy の変更に関する考察
 - draft-ietf-6man-rfc3484-revise-05
 - Update to Default Address Selection for IPv6

Transparent Interconnection of Lots of Links (trill) WG

- RFC : 4本
 - RFC6325, RFC6327, RFC6439 : RBridges
- Active Internet-Draft : 7本
 - RBridge 関連拡張
- 先日の IETF での BoF
 - 2コマ開催
 - ICMP based OAM
 - TRILL over MPLS
 - TRILL over IP
 - MTU negotiation
 - RBridge Aggregation
 - VLAN load balancing
- Base Spec が RFC として発行されたので、その拡張が増えた

Locator/ID Separation Protocol (lisp) WG

- まだ RFC 無し
- Active Internet-Drafts : 12本
 - draft-ietf-lisp-16
 - Basic Specs
 - draft-ietf-lisp-alt-09
 - LISP + ALT による distributed index system の定義
 - draft-ietf-lisp-ms-12
 - LISP map resolver/server を定義した文章
 - draft-ietf-lisp-multicast-11
- 先日の IETF での BoF
 - キャンセルされました
- 実験としての LISP 網は存在するが、実運用とは違うレベル
 - 動作するための Basic Specs は決まりつつある

Multiple Interface (mif) WG

- RFC6418
 - Multiple Interfaces and Provisioning Domains
Problem Statement
- RFC6419

Source Address Validation Improvements (savi) WG

- まだ RFC 無し
- Active Internet-Draft : 6本
 - draft-ietf-savi-dhcp-10
 - DHCP を利用した Source Address Filtering 手法
 - draft-ietf-savi-fcfs-10
 - First Come First Serve の原理で DAD 等に用いられた ND パケットを用いて学習し、ポートとのマッピングを作成することで Source Address Validation を行う
 - draft-ietf-savi-framework-05
 - 末端で Source Address Validation を行うためのフレームワークを定義した文章
 - draft-ietf-savi-send-06
 - SEND を利用した Source Address Validation
- 先日の IETF での BoF
 - Requirements of SAVI solution
 - Problem and enhance RPF

Softwire WG

- RFC6333
 - DS Lite による IPv4 アドレス節約手法
- RFC6334
 - DHCPv6 Option for DS Lite
 - AFTR (Address Family Transition Router) の Tunnel Endpoint 発見のための DHCPv6 Option
- Active Internet-Draft : 8本
- 先日の IETF における BoF
 - 2コマ
 - 4rd & 4v6
 - DS Lite Multicast
 - SA46T Multicast
 - Address & Port Mapping
- DS Lite を中心としているが、以前複数のトンネル手法に関して議論が行われている

TRANSPORT AREA 動向

Behavior Engineering for Hindrance Avoidance (behave) WG

- RFC : 6本
 - RFC6146 : Stateful NAT64
 - RFC6147 : DNS64
 - RFC6144 : Framework for IPv4/IPv6 Translation
- Active Internet-Draft : 6本
 - draft-ietf-behave-lsn-requirements-05
 - draft-ietf-behave-sctpnat-05
 - draft-ietf-behave-v4v6-bih-06
- 先日の IETF での BoF
 - CGN に関する話題 (Logging, NAT44 + DS Lite, NAT444)
- 昔行われた議論が回っている気もするが、より現実的になって移行への手法が議論され、定義されている

Multipath TCP (mtcp) WG

- RFC6181
 - Threat Analysis for MPTCP
- RFC6182
 - Architectural Guidelines for Multipath TCP Development
- RFC6356
 - New Congestion Control for Multipath (Coupled Congestion Control Algorithm)
- Active Internet-Draft : 2本
 - draft-ietf-mptcp-api-03
 - draft-ietf-mptcp-multiaddressed-04
 - こっちが先じゃないか ??

総括

- IPv4 アドレス枯渇にともなう移行技術
 - インターネットの経路制御をより信頼のおけるものにする技術
 - クラウドに利用される技術
 - 騙されないための技術
-
- これら技術の標準化が活発に行われている感があります

Common Control and Measurement Plane (ccamp) WG

- RFC6060
 - GMPLS PBB-TE
- RFC6107
 - Hierarchical Label Switched Paths
- RFC6162
 - GMPLS and Wavelength Switched Optical Networks
- RFC6205
 - Lambda Switch Capable Label Switching Routers
- RFC6344
 - Virtual Concatenation and GMPLS
- RFC6373
 - MPLS-TP (Transport Profile)
- RFC6378
 - GMPLS Asymmetric Bandwidth Bidirectional Label Switched Paths
- Internet-Drafts
 - GMPLS + α がたくさん