# 第 57 回 IETF ミーティング参加報告書

富士ゼロックス株式会社
稲田 龍
セコム株式会社
松本 泰
漆島賢二
セコムトラストネット株式会社
島岡政基
NPO 日本ネットワークセキュリティ協会
安田直義


2003/7/13-18 にオーストリアのウィーンの Austria Center Vienna にて開催された第 57 回 IETF(Internet Engineering Task Force: http://www.ietf.org/ )ミーティング に NPO 日本ネットワークセキュリティ協会(略称: JNSA http://www.jnsa.org/)が 2002 年度に情報処理振興事業協会セキュリティセンター(略称: IPA/ISEC http://www.ipa.go.jp/security/) より委託を受けた事業である JNSA Challenge PKI 2002 プロジェクトの派生物である Internet-Draft ”Memorandum of Multi Domain PKI interoperability”(セコムトラストネット株式会社島岡政基氏著)に関しての島岡氏の発表と議論を PKIX-WG にて行う目的で JNSA 安田直義氏、セコム株式会社 松本 泰氏、漆島賢二氏およびセコムトラストネット島岡政基氏と共に参加したので報告する。

第 57 回 IETF ミーティングの参加者は 27 カ国から XXX の組織で、総勢 1,331 人であった。前回の San Francisco での第 56 回が 1,640 人であり、アトランタの第 55 回 IETF ミーティングの参加者は 34 カ国から 334 の組織で、総勢 1,706 人であった。横浜の第 54 回 IETF が 2,064 人、第 53 回のミネアポリスの IETF が 1,756 人であ

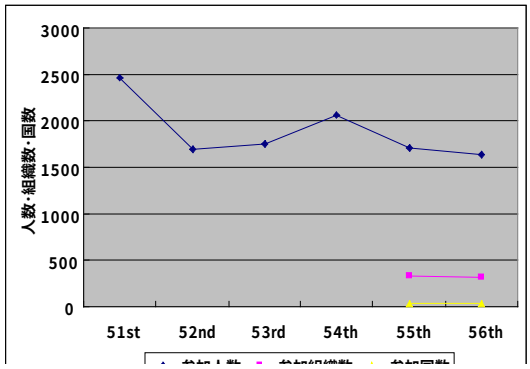



図 1 IETF ミーティング参加人数の推移

った。同時テロ以前のロンドンで行われた第 51 回 IETF が 2,457 人であったことを考えると、年に一度の米国外でのミーティングである事もあって、出席者は少ない。米国での IT バブルの崩壊の影響は、いまだ強く残っている事が感じられた。

# 概観

## PKIX-WG で島岡氏の発表に関して

今回の出張の主たる目的であるセコムトラストネットの島岡政基氏の発表に関して報告する。

島岡氏は、JNSA の行った JNSA Challenge PKI 2001/2002 の中心人物の一人でありテストケース/テスト環境の設計、報告書の作成などを精力的に行ってきた。

JNSA Challenge PKI 2001/2002 の活動を通じ、またアジア PKI フォーラムでの活動において島岡氏はいわゆる Multi Domain PKI に関しての定義が曖昧であり不要な誤解、理解の不足により相互接続性が阻害されていると感じた。そのため、いわゆる Multi Domain PKI に関しての状況を整理しまとめた Internet-Draft ”Memorandum of Multi Domain PKI interoperability” を執筆した。

当初は、PKIX-WG のチェアである Steve Kent 氏(BBN Net)および Tim Polk 氏(NIST)と相談の上、WG Draft として公開する予定であったが IESG の方針により PKIX-WG は、これ以上、Work Items を増やさない方針であるとの Tim Polk 氏の助言により島岡氏個人の Personal Draft として公開する事となった。

Tim Polk 氏との事前協議により、今回の PKIX-WG にて 10 分間の時間をもらい、島岡氏がこの Internet-draft を書く背景の説明と内容の説明を行い今後の予定などを発表した。

また､IETF 開催前の 7/2 に下記のようなメールを PKIX-WG のメーリングリストに投稿し PKIX メンバーに対して周知を図った。

Date: Wed, 02 Jul 2003 23:07:13 +0900
From: Masaki SHIMAOKA <shimaoka@secom.ne.jp>
To: ietf-pkix@imc.org
Subject: I-D: multi-domain PKI Interoperability
Cc: mpki@jnsa.org
Reply-To: mpki@jnsa.org, shimaoka@secom.ne.jp
Message-Id: <20030702230029.2FB3.SHIMAOKA@secom.ne.jp>

Hi all,
As Ryu said in last IETF meeting, I am writing a Inetenet-Draft for multi-domain PKI interoperability as a best current practice. This fruit is based on several multi-domain PKI interoperability experiments and documents.
# This is an individual submission.
Here is an abstract of this I-D.
Title : Memorandum for multi-domain PKI Interoperability
Author(s) : M. Shimaoka
Filename : draft-shimaoka-multidomain-pki-00.txt
Pages : 16
Date : June 2003

===== Abstract =====
This memo is used to share the awareness necessary to deployment of multi-domain PKI. Scope of this memo is to establish trust relationship and interoperability between plural PKI domains. Both single-domain PKI and multi-domain PKI are established by the trust relationships between Certification Authorities (CAs). Typical and primitive PKI models are specified as single-domain PKI. Multi-domain PKI established by plural single-domain PKI is categorized as multi-trust point model and single-trust point model. Multi-trust point model is based on trust list model, and single-trust point model is based on cross-certification.
===== Abstract =====

The I-D has already published on IETF repository, but I revised several parts after that.
So, please refer the following URLs:
http://www.jnsa.org/mpki/
http://www.jnsa.org/mpki/draft-shimaoka-multidomain-pki-00.txt
URL above invites you to our activity for multi-domain PKI interoperability framework, as you know as what reported in past IETF meetings.
If you are interested in this, please let me know.
Thanks in advance for any comments.
---
Masaki SHIMAOKA
SECOM Trust.net
System Engineering Dpt.

発表は、好意的に受け入れられた。

特に Tim Polk 氏は「非常によくまとまった発表であり、今後の RFC3280 の後継の RFC に対しても反映したい」というコメントを受け取っていた。事実上、最大限の賛辞であり島岡氏の Internet-Draft が高く評価されたと感じた。おそらく、PKIX-WG が No more New Work Item の状態でなければ、文句なく WG Draft として PKIX-WG で(おそらく BCP もしくは Informational)RFC として制定される道をとったものと思われる。

発表の後に、Matt Cooper 氏(Orion Security/ draft-ietf-pkix-certpathbuild-00.txt の作者)と意見交換を行い、Multi Domain PKI に関してのパス構築/パス検証に関しての意見の交換と簡単な議論を行い、協力する事を約束した。後日、以下に示すメールを Matt Cooper 氏より受け取った。

From: "Matt Cooper" <mcooper@orionsec.com>
To: <hidenori@iss.isl.melco.co.jp>, <sec@jnsa.org>, <Ryu.Inada@fujixerox.co.jp>, <shimaoka@secom.ne.jp>
Cc: "'Santosh Chokhani'" <chokhani@orionsec.com>, <cwallace@orionsec.com>, <mcooper@orionsec.com>
Subject: Certificate Path Building
Date: Mon, 21 Jul 2003 13:15:29 -0400

Message-ID: <00ae01c34fab$ced36bf0$9700a8c0@hq.orionsec.com>

All,

Thank you for your interest and kind comments on the Certificate Path Building draft at the IETF meeting. I wanted to send an email to you so that each of you would have my contact information. For those of you that asked me to review documents you had written, if you could provide me with current versions or a URL for retrieving them, I will read them as soon as I have time.

I look forward to hearing your comments and suggestions on the draft. I am starting working on the 01 version now and would very much like to incorporate your feed back.

Thanks again and very best regards,

Matt Cooper
Orion Security Solutions
1489 Chain Bridge Road, Suite 300
McLean, Virginia 22101
mcooper@orionsec.com
Visit our website!
http://www.orionsec.com <http://www.orionsec.com/>

このメールに対して島岡氏は以下のように答えている。

Date: Tue, 22 Jul 2003 20:55:42 +0900
From: Masaki SHIMAOKA <shimaoka@secom.ne.jp>
To: "Matt Cooper" <mcooper@orionsec.com>
Subject: Re: Certificate Path Building
Cc: <hidenori@iss.isl.melco.co.jp>, <sec@jnsa.org>,
  <Ryu.Inada@fujixerox.co.jp>, "'Santosh Chokhani'" <chokhani@orionsec.com>,
  <cwallace@orionsec.com>, mpki@jnsa.org
In-Reply-To: <00ae01c34fab$ced36bf0$9700a8c0@hq.orionsec.com>
References: <00ae01c34fab$ced36bf0$9700a8c0@hq.orionsec.com>
Message-Id: <20030722195850.CD4E.SHIMAOKA@secom.ne.jp>

Dear Cooper,

I also thank you for your interesting documentation.
I am going to send my comments for your I-D to PKIX ML, ASAP.

My I-D is here;
http://www.jnsa.org/mpki/draft-shimaoka-multidomain-pki-00.txt

and some related documents are linked from below.
http://www.jnsa.org/mpki/

BTW, my project work was affected by your co-worker Hesse's documents.
  "Managing Interoperability in Non-Hierarchical Public Key
  Infrastructures", NDSS 2002
So, we will not go in the wrong direction, I believe:)

Best Regards,

このメールの中で約束した draft に対して以下のコメントを PKIX-WG のメーリングリストに投稿している。

Date: Wed, 23 Jul 2003 12:11:58 +0900
From: Masaki SHIMAOKA <shimaoka@secom.ne.jp>
To: ietf-pkix@imc.org
Subject: Re: I-D ACTION:draft-ietf-pkix-certpathbuild-00.txt

In-Reply-To: <200307031532.LAA16682@ietf.org>
References: <200307031532.LAA16682@ietf.org>
Message-Id: <20030722191927.CD43.SHIMAOKA@secom.ne.jp>

Dear Cooper,

> A New Internet-Draft is available from the on-line Internet-Drafts directories.
> This draft is a work item of the Public-Key Infrastructure (X.509) Working Group of the IETF.
>
> Title : Internet X.509 Public Key Infrastructure:
> Certification Path Building
> Author(s) : M. Cooper, Y. Dzambasow
> Filename : draft-ietf-pkix-certpathbuild-00.txt
> Pages : 59
> Date : 2003-7-3

This is an excellent trial.

Sorry for my delayed comments below.

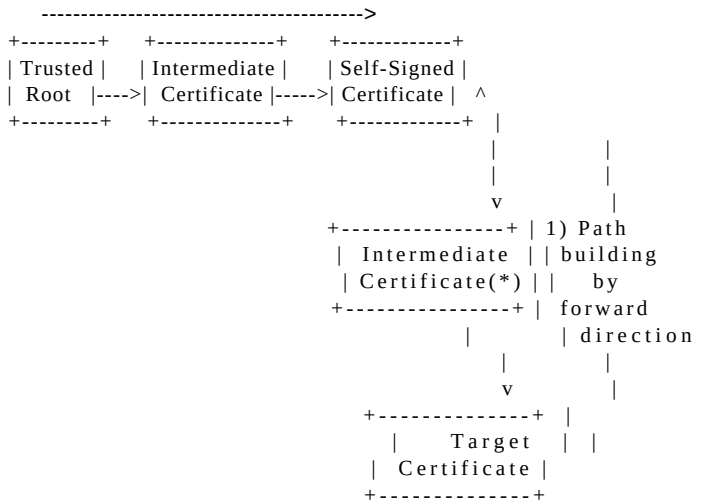
1. path building over http

This text gives an example as path building algorithm based over LDAP.
Shall we consider also about a path building algorithm over http?
# I know and agree that basically path building is used in the environment which have directory system.
IMHO, path building over http may be achieved using cAIssuers accessMethod in AIA extension, but it only describes single path like strict hierarchy.

2. forward direction vs. reverse direction

My basic opinion is shown below as hybrid path building.
=====
Path building in the forward direction is very useful for tree topology that each node has unique parent.
However, when each node has plural parent (e.g., mesh PKI or bi-lateral cross-certified PKI), this method is useful only a bit.
First, therefore, a builder SHOULD attempt to build a path in the forward direction till a self-signed certificate (or maybe intermediate certificate issued by plural CAs).
Then, the builder MAY attempt to build the remain path either way.

2) Path building by the reverse direction




(*) Not self-signed certificate.
# I know more consideration yet is required for this.
=====

And this topic has one problem.
Some subordinate CA populate their CA certificate to issuedToThisCA of crossCertificatePair attribute in their own (CA) directory entry. On the other hand, most cross-certified (not subordinate) CA also populates their cross-certificate to same location.
When a path builder attempts hybrid building as above, the builder in second step (reverse direction) does not require obtaining the subordinate CA information.

In almost (hierarchical) PKI, path building may finish before second step.
Only in some complex PKI, path building may need second step. Anyway, this hybrid algorithm is useful for every PKI, I think.

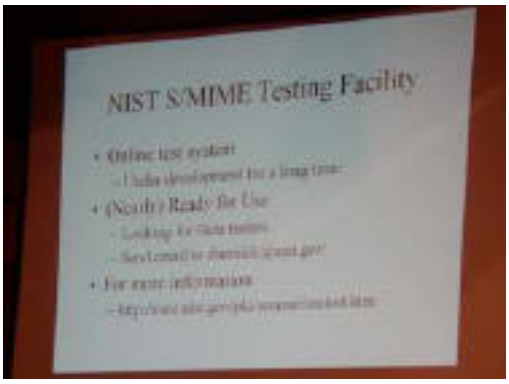
3. Static path vs. Dynamic path
Static certification path means that the client is given beforehand all certificates and all revocation information required for path validation.
On the other hand, dynamic certification path means that the client at least must obtain some certificates and revocation information required for path validation. Dynamic certification path may use some certificates and revocation information in certificate store or local cache.
For a client that cannot build a certification path dynamically, we should consider static certification path, e.g., SSL/TLS handshake.

Your I-D describes that how build a certification path, and my 'memo for mPKI' I-D aims to support how to design a certification path.
So I hope to review our documents each other frequently.

Best Regards,
---
Masaki SHIMAOKA

SECOM Trust.net
System Engineering Dpt.

# NIST の S/MIME Test Suite に関して




S/MIME WG のセッションにおいて NIST の Tim Polk 氏が NIST が開発している S/MIME Test Suite に関して発表を行った。

この Test Suite は、特定のメールアドレスに対して S/MIME メッセージを送るとその S/MIME メッセージの妥当性、正当性を評価しレポートするものの様である。

S/MIME WG の終了後、Tim Polk 氏と NIST 版 S/MIME Test Suite の構成と日本語に対するサポートの状況を問い合わせたところ、できる限りのサポートをしていただけることとのことで

あった。Tim Polk 氏より、7/21 の週にリマインダーとして具体的な依頼事項を記述したメールがほしいとのことであったので下記のようなメールを送った。

問い合わせを行った内容は、

1. この Test Suite のソースコードが公開される予定があるか?
2. 公開されるのなら、ソースコードを変更し Challenge PKI 2002 の成果物である GPKI Test Suite に同梱して配布してかまわないか?

の 2 点である。

Tim Polk 氏には、55th IETF/56th IETF の PKIX-WG にて JNSA が Challenge PKI 2001/2002 を行っておりその成果物として GPKI Test Suite を公開した事を報告してあり、また http://www.jnsa.org/mpki/にて Challenge PKI Project の成果物を公開している事を知らせてある。これらに関しても Tim Polk 氏は高く評価をしている。

To: tim.polk@nist.gov
Cc: nao@dit.co.jp, yas-matsumoto@secom.co.jp, shimaoka@secom.ne.jp,
sawano@orangesoft.co.jp, Ryu.Inada@fujixerox.co.jp
Subject: S/MIME Test Suite
From: Ryu Inada <Ryu.Inada@fujixerox.co.jp>
Message-Id: <200307211757.FDE42396.BuJOBSZVE@fujixerox.co.jp>

Dear Tim.

As we talked after S/MIME WG in IETF, we are interest in NIST's S/MIME Test Suite, and want to localize(or internationalize ?) for Japanese environments/and or to customize to fit our Test Suites.

We have some question about S/MIME Test Suite.
1. Is this Test Suite's source code will be open to public ?
2. If 1's answer is yes, Is it possible to modify and
distribution with our Test suite ?

Thank you.
--
Ryu Inada
Ryu.Inada@fujixerox.co.jp

以上