社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－DPS－122（9）
2005－CSEC－28（9）
2005／3／22

ITU-T 勧告 X.509 の改訂作業に関する報告

辻　宏郷†,　山口　純一††

†三菱電機株式会社,　††ISO/IEC JTC1/SC6/WG8 国内委員会主査
E-Mail: †hirosato@iss.isl.melco.co.jp, ††Jun.Yamaguchi@shorei.jp

あらまし　ITU-T 勧告 X.509（ISO/IEC 9594-8 と同等規格）は PKI の基本事項を規定した国際標準であり，同仕様に基づく公開鍵証明書は,国内外において携帯電話等の各種製品に実装されている．筆者らは，ISO/IEC JTC1/SC6/WG8 及び対応国内委員会のメンバーとして，同規格の標準化を担当している．本発表では，今年中に制定予定の X.509 第五版（2005 年版）における改訂内容について報告する．また，既発行の X.509 第三版･第四版に対する訂正作業や今後の改訂計画，IETF PKIX WG におけるプロファイル仕様との関係について触れる．

キーワード　X.509,　PKI,　公開鍵証明書,　PMI,　属性証明書,　標準化活動

A Report on Revision of ITU-T Recommendation X.509

Hirosato TSUJI† and Jun'ichi YAMAGUCHI††

†Mitsubishi Electric Corporation, ††ISO/IEC JTC1/SC6/WG8
E-Mail: †hirosato@iss.isl.melco.co.jp, ††Jun.Yamaguchi@shorei.jp

Abstract　ITU-T Recommendation X.509 (also published as ISO/IEC 9594-8) is the international standard which defines a framework of public-key certificates for PKI (Public Key Infrastructure). The X.509-based certificates are implemented on various products, e.g. mobile phones. We, as members of ISO/IEC JTC1/SC6/WG8, have been maintaining X.509 and related standards. In this paper, we introduce the overview of the next edition of X.509. We also mention the correction of existing standards, the future work items and the relationship to their profile specifications developed by IETF PKIX WG.

Key words　X.509, PKI, public-key certificate, PMI, attribute certificate, international standardization

1. はじめに

PKI（Public Key Infrastructure）は，公開鍵暗号アルゴリズム及び公開鍵証明書を用いて，認証･電子署名･暗号化等を実現する基盤技術である．ITU-T 勧告 X.509（ISO/IEC 9594-8 と同等規格）は，PKI の基本事項を規定した国際標準であり，同仕様に基づく公開鍵証明書は，国内外において携帯電話等の各種製品に実装されている．筆者らは，ISO/IEC JTC1/SC6/WG8 及び対応国内委員会（情報処理学会情報規格調査会 SC6/ディレクトリ SG）のメンバーとして，同仕様の標準化を担当している．本稿では，同仕様の標準化動向について，今年中に制定予定の X.509 第五版（2005 年版）を中心に紹介する．

2. X.509 第五版における改訂

現時点における X.509 の最新版は，2000 年 3 月に発行された第四版[1]である．2000 年 6 月にプラ

ハ（チェコ）で開催された SC6 会議において，第四版の改訂作業にて盛り込むことができなかった拡張項目について，新規作業の開始提案を日本から行った．この結果，国際投票を経て，X.509 第五版を発行するための改訂作業を開始することとなった．毎年二回の編集会議，各段階における国際投票を経て，2005 年 2 月現在，第五版は国際標準規格として出版するための最終投票の準備中である（**表1**）．本節では，日本から提案した拡張項目を中心として，X.509 第五版[2]における改訂内容の概要を紹介する．

表1　X.509 第五版制定までの過程

時期	会議開催地	進捗
2000.06	プラハ	新規作業提案
2000.11	オーランド	1st WD 作成
2001.01	ジュネーブ	2nd WD 作成
2001.11	フラグスタッフ	3rd WD 作成
2002.02	ジュネーブ	4th WD 作成
2002.11	ワシントン DC	5thWD 作成
2003.02	ロンドン	PDAM 作成
2003.09	ジュネーブ	同レビュー
2004.03	ジュネーブ	FPDAM 作成
2004.11	オーランド	同投票結果審議
2005.xx	―	DIS 投票

2．1　パス構築時の issuer・subject の取り扱い

公開鍵証明書を検証する際の証明パス構築処理において，上位証明書の subject と下位証明書の issuer の判定基準については，従来の X.509 には明確な規定が存在しなかった．X.509 第五版では，両者の値を，X.501（ISO/IEC 9594-2）に規定された **distinguishedNameMatch** 照合規則を用いて判定すべきことが追記された．また，証明書エクステンションに設定された名前の別名（**issuerAltName**，**subjectAltName**）については，パス構築時の判定に使用しないことが追記された．

2．2　CRL 代理発行時の権限委譲の明確化

CA（Certification Authority）は，自らが発行した証明書に対応する失効情報を記載する CRL（Certificate Revocation List）の代理発行を，他の CA に依頼することができる．従来の X.509 には，この権限委譲の方法が明確に規定されていなかった．X.509 第五版では，発行する証明書の **CRL Distribution Points** エクステンションを用いて，CRL を代行発行する CA へのポインタを明確に示すべきことが追記された．

2．3　CRL 代替手段としての OCSP の参照

従来の X.509 では，CA が証明書の失効を通知するために，CRL 発行以外の手段を用いてよいと規定されている．X.509 第五版では，この代替手段の具体例として，IETF PKIX WG の規定した OCSP（Online Certificate Status Protocol）[9]を明示的に参照する記述を追加した．

2．4　未来における証明書失効の事前通知

CRL に記載する証明書の失効日時は，その CRL の発行日時と等しいか，それ以前の日時でなければならない（未来に失効する証明書を記載できない）という制限が存在する．従来の X.509 にはこの制限事項が明記されていなかったため，X.509 第五版にて追記した．この制限事項の下では，例えば市町村の統合や会社の合併等で近未来に多くの証明書を一括して失効させる必要が生じた場合，失効時前に発行する CRL に記載することで未来における失効を事前通知することができなかった．今回，未来における失効を CRL に記載する手段として，**To Be Revoked** という CRL エクステンションを新たに定義した．

2．5　グループに属する証明書の一括失効

同一の条件（証明書発行者・失効理由・失効日時）でグループに属する多くの証明書が失効した場合（未来の失効でない場合）に，その様なグループに属する証明書をまとめて CRL に記載する方法として，**Revoked Groups** という CRL エクステンション（前述の **To Be Revoked** の派生型）を新たに定義した．

2．6　期限切れ証明書の CRL への記載

通常，有効期間を経過した期限切れ証明書は，CRL には記載しない．期限切れ証明書が CRL に記載されていることを明確に示す手段として，X.509 第五版では **Expired Certs On CRL** という CRL エクステンションを新たに定義した．

2.7 Subject Directory Attributes エクステンションのクリティカル指定

Subject Directory Attributes エクステンションは, 公開鍵証明書の所有者の属性を, 公開鍵と共に証明するために用いられる. CA が AA (Attribute Authority) を兼ねており, かつ証明する属性の寿命が公開鍵と等しいという条件が成立する場合, 同属性を含む公開鍵証明書のみで公開鍵証明書＋属性証明書と同等の効果を得ることができる. しかしながら, 従来の X.509 の規定では, 同エクステンションをクリティカル (＝その内容を解釈できなければ証明書を使用不可の意) 指定できなかった. X.509 第五版において, この制限を撤廃した.

2.8 証明書照合規則の拡張

証明書照合規則は, ディレクトリ上に格納された公開鍵証明書を取得する際の検索条件の指定等に用いられる. X.509 第五版では, 新たな照合規則として, **Enhanced Certificate Match** 照合規則を追加し, 主要な証明書エクステンションの値を指定可能とした.

2.9 PMI に関する規定の拡充

PMI (Privilege Management Infrastructure) とは, 属性証明書または属性情報を含む公開鍵証明書を用いて, PKI と併用することによって, 認可サービス等を実現するための権限管理 (属性の証明) を提供する基盤技術である. 従来の X.509 では, 属性証明書の形式や関連するエクステンション・属性・オブジェクトクラス等を定義していたが, X.509 第五版では以下に示す定義を追加し, 規定の拡充を行った.

- **Indirect Issuer** エクステンション
- **Protected Privilege Policy** 属性
- **XML Privilege Information** 属性
- **Protected Privilege Policy** クラス
- **SOA Identifier** 照合規則

2.10 用語定義の追加

以下に示す用語は, PKI において一般に用いられているが, 従来の X.509 では明確な定義が与えられていないまま使用していた. X.509 第五版において, これらの用語の定義を追加した.

- Certification Practice Statement
- self-issued certificate
- self-signed certificate
- cross certificate
- trust anchor
- self-issued AC

なお, X.509 では, 自己発行証明書 (self-issued certificate) 及び自己署名証明書 (self-signed certificate) は, CA が発行した証明書のみを規定対象とすることが明記された. このことは, IETF PKIX 仕様の一つである RFC 3820[12]で規定された代理証明書 (proxy certificate) は, X.509 の規定範囲外であることを意味する.

2.11 用語定義の見直し

以下に示す用語は, 従来の X.509 では PKI 固有の定義となっていたため, PKI と PMI の両方で使用可能となる様に, 用語定義の見直しを行った.

- certificate user
- certificate serial number
- end entity

2.12 Name Constraints エクステンションの具体的な使用例

公開鍵証明書に設定可能な **Name Constraints** エクステンションは, CA が発行する各証明書の対象者名 (所有者名) の制約を明記することによって, CA のドメイン (証明書の発行範囲) に制約を与えるために用いられる. 同エクステンションは使用法が難解であるため, 解釈誤りを生じることがあった (3.1 節参照). 従来の X.509 においても, 同エクステンションの具体的な使用例を Annex (参考: 標準としての規定外) として記述していたが, X.509 第五版において, 全面的に書き換え・訂正を行った. なお, 置換するための文章・具体例の記述は, 全て日本が執筆を担当した.

2.13 証明パス検証における証明ポリシーのコントロール方法に関するガイドライン追加

証明パス検証においては, 検証条件の一つとして, 証明ポリシーに関する初期値を設定することによって, 検証を行う際の証明ポリシー要件を指定する. X.509 第五版において, 初期値の指定例を説明する Annex (参考) を追加した.

3. X.509 第三版･第四版に対する訂正

X.509 を含む ITU-T 勧告 X.500 シリーズの標準化を担当している ISO/IEC JTC1/SC6/WG8, ITU-T SG17/Q2 では, 最新版およびその一つ前の版の標準規格を保守対象としている. 現時点では, X.509 第四版と 1997 年 8 月に発行された X.509 第三版[5] に対する保守を行っている. 通常, ITU-T 勧告は, 四年周期の改訂において内容の見直しを実施しているが, 至急訂正すべき誤りが検出された場合は, 国際投票の上, 標準に対する技術的訂正 (Technical Corrigendum) を発行している. 現時点では, X.509 第四版に対する 3 冊の TC, X.509 第三版に対する 6 冊の TC を発行している. 本節では, これらの TC において規定された訂正の内, 適用前の規定に大きな影響を与える項目について紹介する.

3.1 Name Constraints エクステンションの置換

X.509 第三版において追加規定された **Name Constraints** エクステンションの仕様には, 不明確な箇所が存在した. このため, 規定を明確化するための文章を追加すると共に, 一部パラメータを拡張する必要性で合意が得られ, X.509 第三版に対する TC3[6]及び X.509 第四版に対する TC1[3]にて, 訂正することとなった. この時, 訂正前の同エクステンションを IETF PKIX 仕様の RFC 2459[10] が参照しているおり, 同仕様を実装済の各製品に影響を与えることが判明した.
そこで, この訂正措置では, RFC 2459 が参照している同エクステンションを全て一旦削除し, 相異なる (異なるオブジェクト識別子の割り当てられた) **Name Constraints** エクステンションを新たに定義追加した. 従って, 本訂正前後の同エクステンションは, 全く別物という扱いとなっている.

3.2 Key Usage エクステンションの値変更

Key Usage エクステンションは, 証明書に含まれる公開鍵の用途を示す証明書エクステンションである. X.509 第三版以降, 同エクステンションで指定可能な鍵用途として, **digitalSignature, nonRepudiation** 等が規定されており, X.509 第四版においても, それらの規定を継承していた.
電子署名の検証に使用可能な公開鍵を示す場合, **digitalSignature, nonRepudiation** のいずれか一方, あるいは両方を設定すべきか否かについて, これまでの X.509 では明確な規定が存在しなかった. このため, 相異なる解釈の実装が存在していることが判明した.
X.509 第四版に対する TC3[4]にて, 後者の名前を **contentCommitment** に変更すると共に, それぞれに明確な規定を追加した. なお, X.509 第三版については, 既存の実装を考慮して, 訂正を行わず, 従来の規定通りとすることとした.

3.3 Issuing Distribution Point エクステンションの定義変更と AA Issuing Distribution Point エクステンションへの分離

Issuing Distribution Point エクステンションは, CRL の配布点, CRL が indirect CRL であるか否か, CRL が分割発行されたものであるか否か (失効したユーザ証明書のみを記載, 失効した CA 証明書のみを記載, あるいは特定の理由で失効した証明書のみを記載) を示す CRL エクステンションである. 同エクステンションは, X.509 第四版において, 属性証明書に対応するための拡張を行ったが, 定義が不十分であり, CRL の様々な分割発行方法に対応できないことが判明した.
X.509 第四版に対する TC3 にて, 同エクステンションの定義を第三版の状態に戻すと共に, 一部不明瞭であったパラメータの意味を明確化した. 同時に, 属性証明書に対応するために, 新たに **AA Issuing Distribution Point** エクステンションを追加定義した.

3.4 Extended Key Usage エクステンション用の値追加

Extended Key Usage エクステンションは, 証明書によって証明された公開鍵の用途を示す証明書エクステンションであり, 鍵用途を示す一つ以上のオブジェクト識別子を設定することによって用いられる. 同エクステンションに設定可能なオブジェクト識別子として, 任意の目的に使用可能であることを示す値 **anyExtendedKeyUsage** (**= { 2 5 29 37 0 }**) を追加した.
本追加の必要性の議論は X.509 第四版の発行後に行われたが, 第五版の発行を待たずに至急追加するために, X.509 第四版に対する訂正措置 (TC1 にて修正) として実施された.

4. IETF PKIX 仕様との関係

公開鍵証明書及び CRL のプロファイル仕様として, IETF PKIX WG が規定した RFC 3280[7]が広く参照されている. また, 属性証明書のプロファイル仕様として, 同 WG が規定した RFC 3281[8]が参照されることがある. 本節では, これら IETF PKIX 仕様と X.509 の関係について述べる.

4.1 現時点において参照可能な X.509

前節で述べた通り, X.509 は, ある時点において二種類の版が保守対象となっており, また誤りが検出された場合は, 訂正するための TC が発行される. TC は規定上の誤りを訂正するために発行される仕様であり, 原則として無視できない. このことから, 現時点では, 以下に示す二種類の X.509 が存在していることになる.

(a) X.509 第四版＋TC1＋TC2＋TC3
(標準としてのステータスは"In force")

(b) X.509 第三版＋TC1+…+TC6
(標準としてのステータスは"Superseded")

なお, 今年中に X.509 第五版が発行された後, (b) は保守対象外 ("Withdrawn") となる. この場合, 新たに誤りが検出されても訂正等は行われないため, X.509 第三版 (＋TCs) を国際標準規格として参照することは, 実質的に困難となる.

4.2 X.509 と RFC 3280 の関係

RFC 3280 は, X.509 第三版のサブセット仕様をベースとして, X.509 第四版や TC の規定の一部を部分的に取り入れた仕様となっている. RFC 3280 は, その前版にあたる RFC 2459 との互換性を維持するために, 一部の TC で行われた規定の訂正を無視している.

即ち, RFC 3280 は, X.509 第三版で規定された公開鍵証明書 **v3** 形式・CRL **v2** 形式・エクステンションに加えて, X.509 第四版で拡張・追加された以下のエクステンションを参照している.

- **CRL Distribution Points**
  (PMI 対応でパラメータを追加)
- **Issuing Distribution Point**
  (PMI 対応でパラメータを追加)
- **Reason Code** (PMI 対応で値を追加)
- **Freshest CRL**

また, X.509 第四版に対する TC1 で追加された以下の値を参照している.

- **anyExtendedKeyUsage**

しかしながら, X.509 第四版に対する TC1 で置換された新しい **Name Constraints** エクステンションは参照していない. さらに, X.509 第四版に対する TC3 で **Issuing Distribution Point** エクステンションの定義は第三版相当に戻す (PMI 対応で追加したパラメータを削除する) こととなったが, RFC 3280 は対応していない.

従って, 前述の (a) (b) の何れとも互換性に欠ける点があるため, 厳密には「RFC 3280 は X.509 のサブセット仕様である」と見なすことはできない. 但し, PMI 対応で拡張された部分を使用しない限りは, RFC 3280 は X.509 第三版のほぼサブセットと考えられる. なお, X.509 第三版が保守対象外となることから, IETF PKIX WG では, RFC 3280 の将来の版において, 参照先を X.509 第四版または第五版に変更すると共に, X.509 との不整合な点を解消することを検討している. X.509 と RFC 3280 の関係を**図1**に示す.

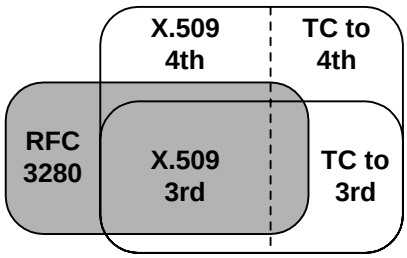

図1 X.509 と RFC 3280 の関係

4.3 X.509 と RFC 3281 の関係

RFC 3281 は, X.509 第四版で規定された属性証明書 **v2** 形式のプロファイル仕様であり, 電子メール・IPSec・WWW 等のセキュリティで用いるためのエクステンションや属性を追加定義している. RFC 3281 では, 属性証明書の有効期間を短く設定して発行することによって, 主として失効処理を伴わない使用法を前提としている. CRL を用いる場合は, RFC 3280 を参照しており, この場合は, 前項で述べた通り, X.509 とは一部互換性に欠ける箇所が存在する.

4.4 他の PKIX 仕様との関係

IETF PKIX 仕様の一つである RFC 3739[11]で規定された特定証明書 (Qualified Certificate),

RFC 3820 で規定された代理証明書は, いずれも RFC 3280 のプロファイルとなっている. 従って, 先に述べた X.509 と RFC 3280 の互換性問題を継承していると言える.

5. 今後の改訂計画

X.509 第五版の改訂作業の末期において提案された拡張については, 審議期間が十分に確保できないことから, 次々版 (第六版) での検討項目とすることとなった. 次回編集会議 (本年 3〜4 月) 以降にて作業着手予定であり, 主として PMI 分野での規定拡充作業が中心になると考えられる. また, 発行済の X.509 における未解決の問題点 (**Policy Constraints** エクステンションにおける **skipCerts** パラメータの解釈の相違) については, 訂正方法を引き続き検討中である.

6. おわりに

本稿では, ITU-T 勧告 X.509 の最新動向について報告した. X.509 第五版は, 国際標準として出版するための最終投票 (DIS 投票) を経て, 本年中に制定される見込みである.

表 2 X.509 **の改訂履歴**

X.509 **の版**	**主な規定内容**
第一版 (1988)	公開鍵証明書 **v1** 形式 CRL **v1** 形式
第二版 (1993)	公開鍵証明書 **v2** 形式
第二版用 TC (1995)	公開鍵証明書 **v3** 形式 CRL **v2** 形式 PKI エクステンション
第三版 (1997)	属性証明書 **v1** 形式 (注) PKI エクステンション (追加)
第四版 (2000)	属性証明書 **v2** 形式 PKI エクステンション (追加) PMI エクステンション
第四版用 TC (2001,2004)	PKI エクステンション (置換) PMI エクステンション (追加)
第五版 (2005)	PKI エクステンション (追加) PMI エクステンション (追加)

(**注**) フォーマットに問題が検出されたため, X.509 第四版にて廃止された.

謝辞

X.509 改訂作業に従事している国際委員会 (ISO/IEC JTC1/SC6/WG8, ITU-T SG17/Q2) 及び対応国内委員会 (情報処理学会情報規格調査会 SC6/ディレクトリ SG) のメンバー, 関係者各位に感謝の意を表します.

参考文献

[1] ITU-T Recommendation X.509(2000), Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks (2000)
[2] ISO/IEC JTC1/SC6 N12793: Revised Text of Public-Key and Attribute Certificate Enhancements FPDAM 4 (2005)
[3] ITU-T Recommendation X.509(2000) - Technical Corrigendum 1 (2001)
[4] ITU-T Recommendation X.509(2000) - Technical Corrigendum 3 (2004)
[5] ITU-T Recommendation X.509(1997), Information technology - Open systems interconnection - The Directory: authentication framework (1997)
[6] ITU-T Recommendation X.509(1997) - Technical Corrigendum 3 (2001)
[7] RFC 3280, Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile (2002)
[8] RFC 3281, An Internet Attribute Certificate Profile for Authorization (2002)
[9] RFC 2560, Internet X.509 Public Key Infrastructure - Online Certificate Status Protocol - OCSP (1999)
[10] RFC 2459, Internet X.509 Public Key Infrastructure - Certificate and CRL Profile (1999)
[11] RFC 3739, Internet X.509 Public Key Infrastructure: Qualified Certificate Profile (2004)
[12] RFC 3820, Internet X.509 Public Key Infrastructure (PKI) - Proxy Certificate Profile (2004)