第 XXVIII 部

公開鍵証明書を用いた
利用者認証技術

第 28 部
公開鍵証明書を用いた利用者認証技術

第 1 章　moCA ワーキンググループ 2006 年度の活動

moCA ワーキンググループでは CA（Certification Authority）の振る舞いや証明書の扱いに注目し、WIDE プロジェクト内で CA の運用実験を行っている。具体的には、WIDE プロジェクトにおけるルート CA である WIDE ROOT CA、WIDE メンバに対する証明書の発行・失効・更新を行う moCA（members oriented CA）の運用を行っている。また、SOI ワーキンググループなど特定のワーキンググループ活動目的に応じて構築された CA を WIDE ROOT CA が認証する活動を行ってきた。これらの活動を通じて、利用環境や利用法に関する情報交換を行っている。2006 年度は、すべての CA 証明書の有効期限が切れる年であったため、CA 鍵対の変更と、毎年行っている WIDE メンバ証明書の更新とを並行して進めることが運用上の課題となった。下記に、おもな活動について報告する。

- CA 鍵対の変更
- 運用上の工夫

第 2 章　CA 鍵対の変更

2.1 概要

WIDE プロジェクト内で PKI（Public Key Infrastructure）技術の運用ノウハウ習得のために運用している自己運用型 CA（Certification Authority）の証明書が 2006 年 6 月に有効期限切れとなるのに備え、CA 鍵対の変更を行った。

2006 年 3 月からルート CA 鍵対の変更を開始した後、中間 CA 鍵対の変更、中間 CA 運用者からエンドユーザへの CA 証明書の配布を順次行った。中間 CA では、クライアント証明書とサーバ証明書の両方を発行しており、エンドユーザや Web サーバ管理者に負担がかからない CA 証明書の配布方法を検討し実行した。結果として、2006 年 6 月の有効期限切れには間に合ったが、新しい CA 証明書を確認するための周知徹底に漏れがあるなど、スムーズな変更とは行かなかった。

CA 証明書の有効期間は 10 年としたが、運用経験をもっと積むため、3 年後をメドに再度 CA 鍵対の変更を実施する予定である。

2.2 WIDE プロジェクト内の CA について

WIDE プロジェクト内の CA は、自己運用型のルート CA である WIDE ROOT CA を頂点とする階層構造をとっており、2006 年 1 月時点では、中間 CA には moCA（members oriented CA）、SOI CA（SOI ワーキンググループの CA）の 2 つがあった（図 2.1）。

PKIX では CA の鍵対のうち公開鍵が X.509 形式の証明書として管理され、有効期限を設定している [88]。CA 証明書の有効期限が切れると、階層下にあるすべての証明書を発行し直す必要がある。WIDE プロジェクト内の CA 証明書の有効期限は、すべてルート CA と同じにしており、2006 年 6 月 30 日に有効期限が切れる設定にしていた。

CA 証明書は、証明書を用いたクライアント認証やサーバ認証で必要なため、エンドユーザやサーバ管理者に配布されている。商用 CA サービスの場合、CA 証明書は Web ブラウザや Web サーバの証明書データベースに格納する形で提供される。CA 証明書が新しくなったときには証明書データベースが自動更新されるようなしくみをとっており、エンドユー

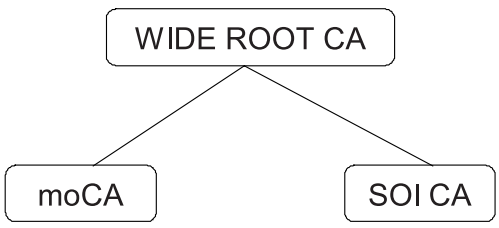

図 2.1. 2006 年 1 月時点の WIDE プロジェクト内 CA

表 2.1. ルート CA 証明書に関する変更点

変更点	変更内容	変更理由
鍵長	RSA 2,048 bit → RSA 4,096 bit	より安全性を高めるためと、4,096 bit の鍵が使われているケースが少なく効率面で問題ないかを確認するため。
CA 証明書の有効期間	6 年→ 10 年	鍵長が長くなったため。
CA の名称	ROOT CA → WIDE ROOT CA 02	過去のルート CA 鍵対の変更実験の教訓から、ルート CA の名称を変えたほうが混乱を避けやすいため。また、Web ブラウザの証明書データベースの表示上 “WIDE” と入れないと見つけにくいため。
CA ポリシー ID	記載なし→ JIPDEC から正式に取得した Object ID[111] から割り当て、CA 証明書に掲載	CA ポリシーの存在を示すためと、WIDE プロジェクト外との連携に備えるため。

ザやサーバ管理者はあまり意識することがない。

しかし、WIDE プロジェクト内の CA のように自己運用型の CA の場合は、Web ブラウザや Web サーバの証明書データベースへの格納をエンドユーザにも実施してもらう必要がある。もし古い CA 証明書の有効期限が切れる前に新しい CA 証明書を配布し終わらないと、提供している認証サービスが停止してしまう。

また、ルート CA 鍵対の変更は、ルート CA 構築時と同様に慎重に行う必要があり、CA の信頼性継続のために極めて重要なイベントである。

2.3 CA 鍵対の変更

2.3.1 ルート CA 鍵対の変更

ルート CA 鍵対の変更にあたって考慮したことは、変更タイミングと鍵対変更の信頼性確保である。

変更タイミングについては、中間 CA が発行する証明書の運用サイクルに合うように決定した。中間 CA のうち、SOI CA が発行する証明書は 4 月を起点にした 1 年サイクル、moCA が発行する証明書は 6 月を起点にした 1 年サイクルとなっていた。そこで、最も早く証明書の更新が行われる 2006 年 4 月に間に合うように、2006 年 3 月にルート CA 鍵対を変更することにした。

鍵対変更の信頼性確保については、鍵対変更の一連の手続きにおいてできるだけ複数人が立ち会う形にした。具体的には下記を実施した。

- CA オペレータ 2 名と CA オペレータ以外の 1 名の立ち会いのもとで鍵対を生成
- その 3 名で CA 証明書のフィンガープリントを生成直後に確認
- 確認したフィンガープリントを印刷し、立会人が署名
- 署名つきのフィンガープリントを公開
- 鍵対変更の模様を録画し、5 月研究会にて録画を見せて鍵対変更を報告

また、表 2.1 にルート CA 証明書の記載内容に関する今までとの違いをまとめる。

2.3.2 中間 CA 鍵対の変更（moCA の場合）

中間 CA である moCA では、毎年 6 月に WIDE メンバ証明書と呼ぶクライアント証明書を配布しており、WIDE メンバ証明書は WIDE メンバ専用 Web ページの閲覧や研究会申し込みの際のクライアント認証に用いられている。また、クライアント証明書に加え Web サーバ証明書も毎年 6 月を期限切れとする 1 年サイクルで発行している。

そこで、moCA の CA 鍵対の変更を 2006 年 5 月に実施し、ルート CA の場合と同様に 5 月研究会で報告を行った。

表 2.2 に moCA 証明書の記載内容に関する今までとの違いをまとめる。

中間 CA のポリシーを示すにあたっては、上位 CA のポリシー ID を掲載すべきか、中間 CA のポリシー ID を掲載すべきかで議論となったが、両方の考え方があるとのことで、今回は中間 CA のポリシー ID を掲載した。

2.4 CA 証明書の配布

2.4.1 moCA における WIDE メンバへの CA 証明書配布

WIDE メンバへのルート CA や moCA の証明書配布は WIDE メンバ証明書配布と同時に行っている。moCA では Web サーバ証明書も発行しているため、ルート CA や moCA の証明書は、Web サー

表 2.2.　moCA 証明書に関する変更点

変更点	変更内容	変更理由
鍵長	RSA 2,048 bit → RSA 4,096 bit	より安全性を高めるためと、4,096 bit の鍵が使われているケースが少なく効率面で問題ないかを確認するため。
CA 証明書の有効期間	6 年→ 10 年	鍵長が長くなったため。
CA の名称	members only CA → menbers oriented CA	正式名称に合わせるため。
CA ポリシー ID	記載なし→ JIPDEC から正式に取得した Object ID[111] から割り当て、CA 証明書に掲載	CA ポリシーの存在を示すためと、WIDE プロジェクト外との連携に備えるため。

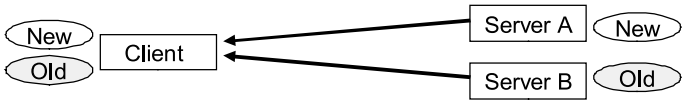

図 2.2.　WIDE メンバに配布すべき CA 証明書

図 2.3.　Web サーバ管理者に配布すべき CA 証明書

バの認証にも使われる。

Web サーバの現在の実装では、サーバ証明書を一つしか持つことができない。全ての Web サーバの証明書が一斉に新しい CA のもとでの証明書に変わることは現実的でないため、サーバ証明書は新か旧かのどちらかの状態になる。旧の CA 証明書が有効期限切れとなる前には、新旧どちらの Web サーバも認証できる必要がある。そのため、Web サーバを認証する WIDE メンバに新旧の両方の CA 証明書を配布しておく必要がある（図 2.2）。

既存の WIDE メンバには旧の CA 証明書が既に配布されているが、新規のメンバや旧の WIDE メンバ証明書を紛失したメンバにも旧の CA 証明書を配布するため、WIDE メンバ証明書更新時には新旧の CA 証明書を含めて配布した。

MacOS 上の Safari ブラウザへの証明書インストールに関して、昨年と同様の方法でインストールしても CA 証明書がうまく認識されていないと思われる不具合があったが、いまだ原因究明中である。それ以外の環境ではとくに問題は報告されていない。

2.4.2 moCA における Web サーバ管理者への CA 証明書配布

Web サーバ管理者へのルート CA や moCA の証明書配布は Web サーバ証明書配布と同時に行っている。このとき配布されたルート CA や moCA の証明書は、WIDE メンバ証明書を用いたクライアント認証に使われる。

CA 鍵対が変更されたことにより、WIDE メンバ証明書の有効期限が切れる前に新しい CA 鍵対のもとで発行した WIDE メンバ証明書を配布すると、旧の CA 証明書の有効期限が切れる直前には新旧とも有効な WIDE メンバ証明書が存在することになる。Web ブラウザの現在の実装では、クライアント証明書を複数管理することができるからである。そのため、Web サーバ管理者としては、新旧の WIDE メンバ証明書でクライアント認証ができるようにする必要がある（図 2.3）。そこで、Web サーバ管理者に新しい CA 証明書を配布し、Web サーバに追加登録してもらうことにした。

計画としては、Web サーバ証明書の更新を WIDE メンバ証明書の更新より前に行って Web サーバ管理者に新しい CA 証明書を Web サーバ証明書の更新に合わせて配布する予定であった。しかし、Web サーバ側の設定確認徹底が難しい点や準備不足な点があり、Web サーバ管理者への新しい CA 証明書配布と Web サーバ証明書の更新は時期を分けて実施した（図 2.4）。Web サーバ管理者への通知を CA 証明書

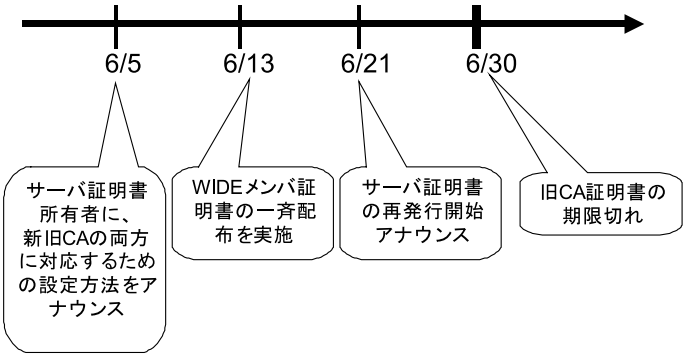

図 2.4.　CA 証明書配布に関する通知

の期限切れの約 3 週間前に行ったが、Web サーバ管理者にとっては二度手間となるためか、Web サーバ証明書の更新作業前に新しい CA 証明書設定を行ったケースは少なかったようだ。

Web サーバへの新 CA 証明書の設定に関してとくに問題は報告されなかった。

2.5 まとめ

2006 年 3 月からルート CA 鍵対の変更を開始した後、中間 CA 鍵対の変更、CA 証明書の配布を順次行った。2006 年 6 月の有効期限切れには間に合ったが、新しい CA 証明書を確認するためのフィンガープリント情報の周知徹底に漏れがあり、スムーズな変更とは行かなかった。一度周知したつもりでも、各自が作業にとりかかるタイミングに合わせて再通知を行う必要がある。

中間 CA での対処として、moCA においては WIDE メンバ証明書配布と Web サーバ証明書配布のタイミングに合わせた CA 証明書の配布を試みたが、計画した日程や順序どおりに実行できない点があった。計画を見直すと、周知のような細かいが運用上重要な点を初期の段階で考慮していなかった点が反省点として挙げられる。また、CA の特徴を見直すと、1 つの CA でクライアント証明書も Web サーバ証明書も発行しているため対処が複雑になったかもしれない。しかし、CA 証明書が共通であるということは CA 証明書の配布数が少なくてすむことでもあることから全体として大きな問題とは言い切れない。

今回の反省を受け、CA 鍵対の変更をスムーズに行うための運用経験をもっと積む必要があると認識している。CA 証明書の有効期間は 10 年としたが、3 年後をメドに再度 CA 鍵対の変更を実施する予定である。

謝辞

PKI の普及という目標を理解してくださり、技術的な問題ばかりでなく、PKI 運用者としてのアナウンスやふるまいに対してもフィードバックをしてくださっている WIDE プロジェクトの皆様に深く感謝いたします。

第 3 章　運用上の工夫

WIDE メンバに対する証明書の発行・失効・更新を行う moCA（members oriented CA）の運用に関して、下記の改善を図った。

- WIDE メンバ証明書配布メッセージの工夫
  - 鍵対配布メッセージと（鍵対を取り出すための）秘密情報配布メッセージを分離
  - 鍵対配布メッセージの英語対応を追加
- WIDE メンバ証明書再発行要求用の専用窓口を設置

  今までは再発行要求を moCA WG メーリングリスト宛に送付する方法をとっていたが、プライバシー保護のために moCA オペレータ宛に送付する方法に変更した。

また、WIDE メンバ証明書配布について、メール以外で配布する方法を検討したが、WIDE メンバに負担なく配布することを考えると現在の運用方法が妥当との結論に達し、変更に至らなかった。さらに、WIDE メンバ証明書の更新タイミングに合わせて、WIDE メンバ証明書の記載内容に下記の変更を加えた。

- 無線 LAN などのネットワーク接続時の認証（802.1x）で WIDE メンバ証明書を使えるようにするために、extKeyUsage 拡張フィールドを追加
- WIDE メンバ証明書の名前欄（Subject フィールド）の一意性を確保するために、WIDE 番号、氏名に加え、発行回数を追加した（2 回目の発行以降）

これらの改善や仕様変更にはプログラムの変更をともなったが、プログラムの変更後の確認が不十分であったために、下記のミスが発生した。

(1) WIDE メンバ証明書配布時に、当事者以外の秘密情報が混入
(2) WIDE メンバ証明書の Subject フィールドの符号化ミス

(1) の対策として、事態の説明と希望者への再発行を実施した。また、CA オペレータの作業前に行うべきチェック項目を明文化し、作業の都度にチェックしてから配布作業に取り掛かるように変更した。(2) については、大きな不具合が報告されていないこともあり、再発行時点から修正版を配布することにした。同じミスを繰り返さないよう、より慎重に WIDE メンバ証明書配布を実施したい。

第 4 章　まとめ

2006 年の CA 鍵対の変更では、CA の信頼性を高めるために複数人で CA 鍵対作成時の確認を行うなどの工夫を行ったが、WIDE メンバ証明書の配布まで含めるとスムーズに行かない点があった。CA 鍵対の有効期間を 10 年としたものの、3 年後をメドに再度 CA 鍵対の変更を行って運用経験を積む必要があると認識している。

今後も運用を行いながら習得したノウハウをドキュメントにまとめる活動を行っていくほか、802.1x のようなネットワーク接続時の認証場面で証明書がスムーズに使われるように実験活動を継続してゆきたい。

付録　フィンガープリントの一覧

概要

本報告書は WIDE ルート CA の適切な利用のため、CA 証明書のフィンガープリントを記述したものである。このフィンガープリントは WIDE ルート CA の運用管理者によって正しさが確認されたもので、ユーザ環境に保存された WIDE ルート CA の証明書データが、オリジナルの証明書データと同一のものであるかどうかを確認するために使われる。

WIDE ルート CA の証明書を入手し、フィンガープリントを確認することは重要である。フィンガープリントの確認が行われていない WIDE ルート CA の証明書を使ってしまうと、間違った証明書が正しいものだとみなされてしまい、https や S/MIME などの証明書を使った認証処理において、なりすまし行為が行われてしまう危険性が高い。その場合にはすぐにその CA 証明書の利用をやめ、正しい CA 証明書を入手しなおすことをお勧めする。WIDE ルート CA の証明書の入手元である URL を以下に示す。

WIDE ルート CA の証明書（名称：WIDE ROOT CA 02）
`http://www.wide.ad.jp/ca/widerootcacert_4096.cer`

フィンガープリント

2006 年 1 月現在の WIDE ルート CA の証明書のフィンガープリントを以下に示す。フィンガープリントは数字の 0〜9 とアルファベットの A〜F までを組み合わせた文字列である。表示を行うソフトウェアによって文字列の間にコロンやスペースが入れられたり逆に省略されたりすることがあるが、その違いは無視してよく、文字列が合っていることを確認すればよい。

WIDE ROOT CA 02

sha1 フィンガープリント
4C:57:B2:D5:6B:94:C2:5F:F2:CA:4A:D1:A8:3D:A4:C0:6F:EE:5C:2C

md5 フィンガープリント
D2:2E:63:73:4A:DC:B6:93:33:0E:A8:09:6F:53:A3:72

sha1 と md5 の両方の値を使って確認することをお勧めする。