WIDE Technical-Report in 2007

WIDEプロジェクトにおけるCA鍵対の変更

wide-tr-moca-cakeypairchange-00.pdf

WIDE Project : http://www.wide.ad.jp/

If you have any comments on this document, please contact to ad@wide.ad.jp

WIDE プロジェクトにおける CA 鍵対の変更

2007 年 1 月 5 日
moCA WG
櫻井三子(mine@ax.jp.nec.com)

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。

目次:

1. 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 WG の CA)の 2 つがあった(図 1)。

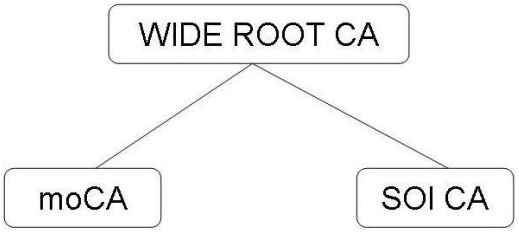

図 1. 2006 年 1 月時点の WIDE プロジェクト内 CA

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[1]。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. CA 鍵対の変更

2.1 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 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。

表 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	RSA2,048bit→RSA 4,096bit	より安全性を高めるためと、4,096bit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[2]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。

2.2 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 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。

表 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	RSA2,048bit→RSA 4,096bit	より安全性を高めるためと、4,096bit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→ members 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[2]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。

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。

3. CA 証明書の配布

3.1 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 証明書が有効期限ぎれとなる前には、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)。

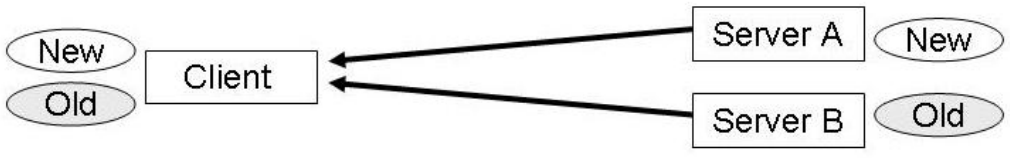

図 2. WIDE メンバに配布すべき CA 証明書

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特に問題は報告されていない。

3.2 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 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。

図 3. Web サーバ管理者に配布すべき CA 証明書

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 4)。Web サーバ管理者への通知を CA 証明書の期限切れの約 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特に問題は報告されなかった。

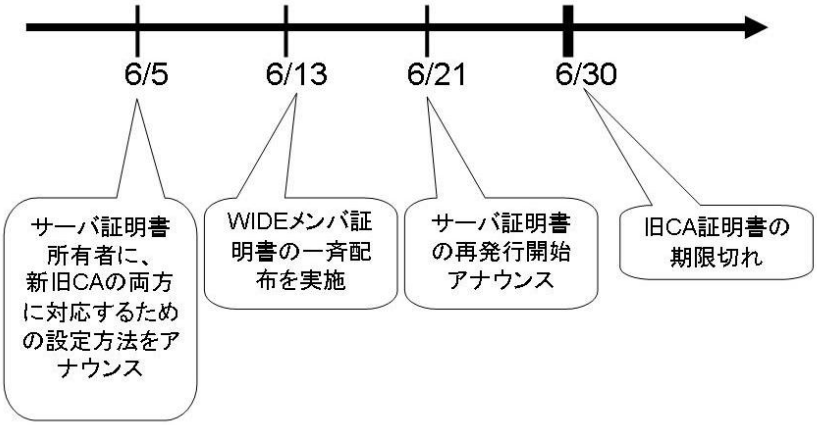

図 4. CA 証明書配布に関する通知

4. 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、一つの 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。

参考文献

[1] Housley, Polk, Ford, Solo: Internet X.509 Public Key Infrastructure Certificate

and Certificate Revocation List (CRL) Profile, RFC 3280,,
http://www.ietf.org/rfc/rfc3280.txt?number=3280
[2] JIPDEC(日本情報処理開発協会) 電子商取引推進センター,OSIオブジェクト管理制度,,
http://www.ecom.or.jp/ecpc/osi/osi_object.htm

改版履歴

2007-01-05　第 0 版