WIDE Technical-Report in 2006

WIDE moCAにおける MacOS&Safariブラウザ対応に関する報告

wide-tr-moca-macossafari-02.pdf

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

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

WIDE moCA(members oriented Certification Authority)における MacOS&Safari ブラウザ対応に関する報告

2006 年 1 月 27 日
moCA WG
櫻井三子(mine@ax.jp.nec.com),
森島直人(naoto@dl.naist.jp), 垣内正年 (masato@itc.naist.jp),
太田英憲(hidenori@iss.isl.melco.co.jp),稲田龍(Ryu.Inada@fujixerox.co.jp),
鈴木茂哉(shigeya@wide.ad.jp),川本芳久(kawamoto@wide.ad.jp),
許先明(seirios@matrix.iri.co.jp),民田雅人(minmin@wide.ad.jp)

概要:

PKI(Public Key Infrastructure)技術を用いた WIDE プロジェクト内部向け認証インフラの一つである moCA(members oriented Certification Authority)では、WIDE メンバに対して毎年 WIDE メンバ証明書を発行して配付している。WIDE メンバが普段利用している端末の OS は、Windows, UNIX, MacOS 等さまざまであることから、WIDE メンバ証明書はさまざまな OS とブラウザの組み合わせで利用されてきた。しかし、以前から MacOS 上でブラウザに Safari を用いて(以下、MacOS&Safari ブラウザと表記)、WIDE メンバ証明書を利用すると特定の Web サーバへのアクセスに失敗する場合があることが報告されていた。この問題を解決すべく 2005 年 8 月に調査を行った結果、WIDE で発行している CA 証明書の符号化方法が正しくないことが主因であることが判明した。

本問題への対処として CA 証明書の再発行が必要となったため、moCA WG では CA 証明書の再配付による混乱を避ける方法を検討した。その結果、WIDE ROOT CA 証明書、moCA 証明書についてそれぞれ正規の証明書を 2 種類利用するという形での運用を行うことで解決できることが判明したため、2005 年 9 月に上記手法を用いての対策を実施した。

目次:

1. MacOS&Safari ブラウザの組み合わせで Web アクセスに失敗する問題 2
2. 調査および分析 2
2.1 証明書の符号化の調査 2
2.2 サーバ設定の調査 3
2.3 問題の分析 3
3. 対処方法 5
4. まとめ 5
謝辞 6
参考文献 6

付録. アナウンス内容(2005 年 9 月 5 日) 7
改版履歴 14
Copyright Notice 14

1. MacOS&Safari ブラウザの組み合わせで Web アクセスに失敗する問題

WIDE メンバ証明書を使って Web アクセスが行えるよう設定されている Web サーバには、WIDE メンバ専用サーバ(https://member.wide.ad.jp/wide-confidential/) や WIDE 合宿申し込み用サーバなどがある。かねてより、MacOS&Safari ブラウザの組み合わせで操作した場合、WIDE 合宿申し込み用サーバへのアクセスが拒否されると報告されていた。そのため、WIDE 合宿申し込み用サーバの設定チェックを一度実施したが、原因はつかめなかった。具体的な不具合を下記に記載する:

(a)CA 証明書を MacOS の Keychain に登録していても、
(証明書を利用しようとするたびに) 無効な機関により署名されていますという警告表示が出る。
(b) WIDE 合宿申し込みサーバへのアクセスだけ拒否される(他のサーバを利用する場合には、アクセスできる)。

この問題のため、MacOS を使っている人が WIDE メンバ証明書を使って WIDE 合宿申し込みを行うには、例えば Mozilla 等の別のブラウザをインストールする必要があり不便な状況となっていた。

2. 調査および分析

2.1 証明書の符号化の調査

2005 年 8 月、WIDE の CA 証明書とそれ以外の機関の CA 証明書を比較していたメンバから、WIDE の CA 証明書のフィールドのうち、X.509 の basicConstraints 拡張フィールドの符号化が誤っているのではないかと指摘があった。

basicConstraints 拡張フィールドとは、当該証明書が CA 証明書か否かを示すためのフィールドで、RFC3280[1]では下記の ASN.1 表記で定義されている:

```
BasicConstraints ::= SEQUENCE {
    cA                      BOOLEAN DEFAULT FALSE,
    pathLenConstraint       INTEGER (0..MAX) OPTIONAL }
```

このフィールドではその証明書が CA 証明書である場合、BasicConstraints.cA の値を TRUE とする必要がある。
X.509 形式の証明書では、拡張フィールドを DER(Distinguished Encoding Rule)形式で符号化することとなっており、DER 符号化に関して定義している X.690[2]によれば、BOOLEAN TRUE は 0xff と符号化しなくてはならない:

“If the encoding represents the boolean value TRUE, its single contents octet shall have all eight bits set to one.“ ([2] 11.1 Boolean values より)

ところが、WIDE の CA 証明書では、BOOLEAN TRUE を DER 形式ではなく BER(Basic Encoding Rule)形式による符号化にしたがって 0x01 と符号化していた。本件は Challenge PKI 2001[3]に参加した際にも、個別に指摘を受けたことがあったが、当時は具体的な不具合が見られなかったことから、WIDE ROOT CA や moCA の証明書について修正をしていなかった。今回の指摘により、MacOS における証明書ライブラリの BOOLEAN 解釈が厳格であり、WIDE ROOT CA 証明書や moCA 証明書が「CA 証明書ではない」と解釈されて Web アクセス自体を拒否されている可能性が高いことがわかってきた。

そこで、まずは WG 内での実験として、WIDE ROOT CA 証明書や moCA 証明書について basicConstraints 拡張フィールドの符号化を修正した版を作成し、MacOS&Safari ブラウザの環境にインストールして Web アクセスを試みた。RFC 3280 の 6.1.1 に記載されている内容から、ルート CA 証明書の解釈については特別扱いをしている可能性があるため、moCA の証明書のみを修正すれば不具合が解消されると実験開始前は予想していたが、結果として WIDE ROOT CA および moCA の証明書の両方とも修正する必要があった。以上で、(a)の解決策が見つかり、(a)を解決すると、(b)も解決されることがわかった。

2.2 サーバ設定の調査

(b)の解決のため、WIDE 合宿申し込みサーバの設定を 2005 年 9 月に調査した。その結果、サーバ側に設定されている moCA 証明書が古く、有効期限切れとなっていることがわかった。そのためサーバに設定する CA 証明書を符号化修正版にし、期限切れの物を更新することで問題を解決した。なお、有効期限切れとなっていた moCA 証明書は、テスト用に臨時発行されたもので正式な証明書ではなかった。サーバの SSL 設定の際に誤って配付した可能性があるが原因を究明するには至らなかった。

2.3 問題の分析

(a)と(b)の問題は相互に絡みあっていた。例えば、SSL のクライアント認証時には、サーバ側に moCA 証明書が必要になる。クライアント認証の際、moCA 証明書はクライアント

から送信されるか、サーバの証明書データベースに登録されているものが使われる(どちらを優先するかは実装による)。(a)により、moCA 証明書は CA 証明書と認識されていないため、クライアントからは送信されない。この場合、サーバの証明書データベースの moCA 証明書が使われるはずだが、有効期限切れとなっており正しく利用できるものではなかった。そのため、クライアント認証の確認が失敗してしまう(図 1)。これを解決するには、(a)を解決するか、サーバ側に設定する CA 証明書を最新にするかが必要である。

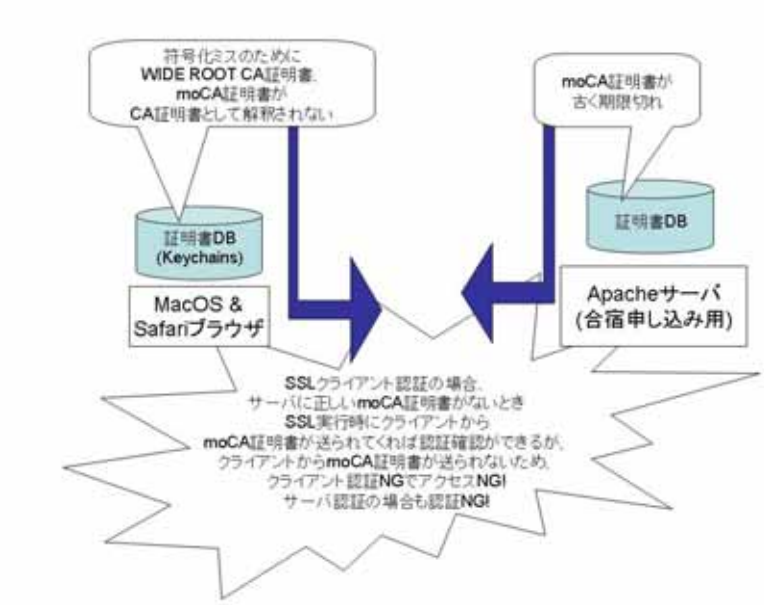

図 1 MacOS&Safari の問題分析結果

また、moCA では、WIDE メンバ証明書だけでなく Web サーバの証明書も発行しており、サーバ認証でもクライアント認証でも moCA 証明書が必要になる。したがって、サーバ認証の場合もクライアント認証と同様に失敗する。サーバが Apache の場合、CA 証明書が有効期限切れになると、SSL 実行時にサーバからブラウザに対して CA 証明書を送信しないことを調査中に確認した。なお、サーバ認証に失敗した場合は、Apache サーバーの設定によってページを表示するかどうかを選択できるため即 Web アクセス NG となるとは限らない。

さらに、サーバから CA 証明書が送信される場合、MacOS&Safari ブラウザは、サーバから送信される moCA 証明書を優先して認証確認を行うことを確認した。そのため、ブラウザ側だけが moCA 証明書を符号化修正版にすればよい訳ではなく、サーバ側も同様に修正版にしないと警告表示は出ることがわかった。

これらの調査結果をまとめると表 1 のようになる。今回は、根本的に問題を解決するため、(a)の解決策から先に実施した。

表 1 MacOS&Safari 問題の調査結果のまとめ

ブラウザに、符号化修正前のWIDE ROOT CA証明書、moCA証明書を登録したとき

	ブラウザによるCA証明書解釈		サーバに設定されているmoCA証明書の状態(Apacheサーバ)	
ブラウザの種類	WIDE ROOT CA	moCA	符号化修正前(通常)	期限切れ
Safari on MacOS X	CAでない(警告)	CAでない(警告)	サーバアクセスOK(警告は出る)	サーバアクセスNG
Internet Explorer 6.0 on Windows	CA	CA	サーバアクセスOK	サーバアクセスOK

ブラウザに、符号化修正後のWIDE ROOT CA証明書、moCA証明書を登録したとき

	ブラウザによるCA証明書解釈		サーバに設定されているmoCA証明書の状態(Apacheサーバ)		
ブラウザの種類	WIDE ROOT CA	moCA	符号化修正前(従来)	期限切れ	符号化修正版
Safari on MacOS X	CA	CA	サーバアクセスOK(警告は出る)	サーバアクセスOK	サーバアクセスOK
Internet Explorer 6.0 on Windows	CA	CA	サーバアクセスOK	サーバアクセスOK	サーバアクセスOK

3. 対処方法

調査により、(a)の解決策として CA 証明書の再発行が必要となったが、この場合再配付の方法が大きな問題となる。CA 証明書は、WIDE メンバ証明書を毎年配付する際に一緒に配付しているため、同じ手段を使って配付することはできる。しかし、すべての環境で不具合が出る訳ではないため、WIDE メンバ全員に配付しなおすと混乱を招く可能性がある。

そこで、MacOS ユーザに向けて CA 証明書の修正版を提供する旨のアナウンスを行うが、それ以外のユーザは作業不要で従来どおりの CA 証明書を引き続き使えるようにした(この方法で問題が起きないことも実験期間に確認した)。つまり、WIDE ROOT CA 証明書と moCA 証明書に関してはそれぞれ 2 種類の証明書を正規に持つことになった。そのため、CA 証明書をブラウザにインストールする際に証明書の正当性を確認するためのフィンガープリント情報が 2 種類存在することになった旨のアナウンスも同時に行った(付録参照)。

4. まとめ

今回の検討と対策の実施により MacOS & Safari ブラウザの組み合わせでも警告が出る

ことなく WIDE メンバ証明書を利用できるようになった。また、付随する効果として MacOS X 標準で付いてくる Mail.app で S/MIME による暗号メールが WIDE/moCA 発行の証明書を用いて利用できるようになった。

不具合の主因と判明した X.509 形式の証明書の符号化問題は以前から指摘されていたが、具体的な不具合が出てもすぐには符号化問題との関係がわからず、具体的な調査に入る前に長時間が経過してしまった。CA 証明書の再発行と再配付は困難であるという気持ちが、余計に対処を遅らせることになった点は反省しなければならない。なお、今回は MacOS&Safari 固有の現象だけでなく、サーバ側の設定の問題も絡んでいたため問題が大きくなったが、Web アクセスに失敗するほどの問題は他ではほぼ起きないであろうと考えられる。

不具合の対処として必要となった CA 証明書の再配付については、運用方法との関わりで気づいた点があった。moCA WG の運用実験では、個人の証明書の有効期間を 1 年に設定した上で、ユーザに配付している。この更新した個人証明書を配付する際に、必ず CA 証明書(WIDE ROOT CA および moCA)をも再配付している。 これは、ユーザにとっては全く負担がかからず、最新の CA 証明書をユーザに配付できるというメリットがある。このような運用方法を採用しているため、今回のように CA 証明書の再配付を必要とするような場合でも、最長でも 1 年で CA 証明書が更新されることが期待できる。今後もさまざまな経験を積みながら、運用上合理的な CA を追求してゆきたい。

謝辞

PKI の普及という目標を理解してくださり、運用上の不具合にも関わらず調査へのご協力や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] ITU-T, Information Technology – ASN.1 Encoding Rules: Specifications of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), X.690, http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf

[3] Japan Network Security Association, ISEC Information Technology Promotion Agency: Implementation Problems on PKI, http://www.ipa.go.jp/security/fy13/report/pki_interop/chalange2001.html

付録. アナウンス内容(2005 年 9 月 5 日)

(Japanese message is followd by English one.)
moCA WG より重要なお知らせです。

MacOS X & Safari をお使いの皆様へ

これまで WIDE メンバ証明書を使った WIDE 合宿申し込みページへの
アクセスができないと報告を受けておりました。
原因がわからず対策を打てないままご不便をおかけしていましたが、
このたび対処方法が見つかりましたので、対処内容をリリース
させていただきます。

他の皆様へ

下記不具合のない方につきましては、対処の必要はありません。
ただし、今回の対処により、CA 証明書、具体的には、
WIDE ROOT CA 証明書、moCA 証明書についてそれぞれ
正規の証明書が 2 種類という形での運用となります。従っ て、
フィンガープリントを確認される場合には注意が必要となります。
現在の段階では、正規の証明書が 2 種類有っても利用上の問題は発生
しないことを moCA WG 内の実験で確認しております。

この 2 種類の正規証明書という形態は、あくまでも現在判明 した問題
点を解決するための経過措置であり、次回の証明書更新の際には、問
題対処済みの証明書に置き換えることになります。

今後の WIDE メンバ証明書配付や、Web サーバ証明書配付では
今回の対処で発行した「符号化問題対応版」の CA 証明書を配付
するように移行していきます。
なお、Web サーバに設定している CA 証明書も、「符号化問題対応版」
に入れ替えていただくように別途お勧めしていきます。

以上、よろしくお願い致します。

問題解決のためのガイド(日本語版)

[対処により不具合が解消される端末環境]

MacOS X & Safari

現時点では MacOS X 10.3(Panther)及び MacOS X 10.4 (Tiger)のみで確認しております。

[解消される不具合]

WIDE メンバ証明書を使った WIDE 合宿申し込みサーバ
"https://widecamp.e-side.co.jp/ ” へのアクセスを拒否される

[今回の対処を実施するメリット]

MacOS X 標準で付いてくる
Mail.app で、SMIME が利用できるようになります。

また、今後、(WIDE 関連の)SSL 対応 Web サーバで「符号化問題対応版」
の CA 証明書設定が浸透すると、
WIDE メンバ専用ページへの最初のアクセス時の警告
「無効な機関により署名されています」が表示されなくなります。

[原因]

直接はサーバ側の設定が影響していると思われ、
正確な原因究明がまだ必要です。
しかし、端末側でも下記の問題があり、
下記を解決すると、不具合を回避できることがわかりました。

(Internet Explorer, Mozilla 等では不具合が出ていないものの)
WIDE ROOT CA 証明書、moCA 証明書の符号化に問題があり、
MacOS X & Safari では、CA の証明書と認識できていなかった。

[対処方法]

WIDE ROOT CA 証明書と moCA 証明書の符号化問題対応版をリリースします。
これらの CA 証明書の入れ替えを行ってください。
WIDE ROOT CA 証明書を X509 Anchors に入れるのがコツです。

新しい WIDE ROOT CA 証明書のフィンガープリント
sha1 フィンガープリント
be 97 ae 7f c0 37 d2 cb c5 f2 3b eb d3 2c f5 07 74 c3 ef fe

新しい moCA 証明書のフィンガープリント
sha1 フィンガープリント:
27 fa 6b c3 25 6d 4f 0f 6b 3d f2 a5 b6 8a 83 0a 53 33 7f 45

(a) Tiger の場合

1. キーチェーンアクセスを使って、キーチェーン
「ログイン」やキーチェーン「X509Anchors」から
以前にインストールした moCA 証明書、WIDE ROOT CA 証明書を消す。

キーチェーンアクセスは「アプリケーションフォルダー下のユーティリティーフォルダ」にあります。
X509Anchors を変更する際には特権ユーザーのパスワードが必要となります。

2. 新しい moCA 証明書をキーチェーン「ログイン」に追加する。
http://moca.wide.ad.jp/moca-for-macos050818.cer

3. 新しい WIDE ROOT CA 証明書をキーチェーン
「X509Anchors」 に追加する。
http://member.wide.ad.jp/wg/moca/wideroot-for-macos050822.cer

(b) Panther やそれより前の場合

1. キーチェーンアクセスを使って、キーチェーン

「ログイン」やキーチェーン「X509Anchors」から
以前にインストールした moCA 証明書、WIDE ROOT CA 証明書を消す。

2. 証明書キーチェーンがない場合、「キーチェーンを追加」で、
/System/Library/Keychains/X509Anchors (ルート CA)
/System/Library/Keychains/X509Certificates (中間 CA)
を追加。

3. 新しい moCA 証明書をキーチェーン「X509Certificates」に追加する。
http://moca.wide.ad.jp/moca-for-macos050818.cer

3. 新しい WIDE ROOT CA 証明書をキーチェーン「X509Anchors」 に追加する。
http://member.wide.ad.jp/wg/moca/wideroot-for-macos050822.cer

[さらなる調査について]

今後、より正確な原因究明の調査を行い、別途レポートにまとめる予定です。

[関連 URL]
http://member.wide.ad.jp/wg/moca/wide_root_ca.html
http://moca.wide.ad.jp/

日本語版は以上
----- + ---------- + ---------- + ---------- + ----------

This is an IMPORTANT notice from moCA Working Group.

MacOS X & Safari users,

Some people have reported to the moCA WG that
they couldn't access to the WIDE camp application page.
Through our investigation, one measure has been
found and is released now.
So, please follow the guide described below.

All other WIDE members,

 Any action is not required if you don't experience
the same problem, but please let us announce that
the WIDE ROOT CA and moCA each have two certificates,
*** both of which are correct ***.
Just be careful when you confirm the CA fingerprints,
because two kinds of fingerprints are displayed on
the moCA WG web pages.
Any problem due to the existence of two kinds of CA
certificates wasn't revealed through
several experiments within moCA WG.

This status is temporal. By the next key update,
the changeover will be gradually progressed and
each CA will have only one certificate again.

Apology for your inconvenience,

moCA Working Group

 ----- o ----- o ----- o ----- o -----
The guide to fix the WIDE camp web page
(https://widecamp.e-side.co.jp/)
access problem

[the target PC environment]

  MacOS X & Safari

  the moCA WG has examined the versions of
  MacOS X 10.3(Panther) and 10.4(Tiger).

[the additional merit of this fix]

  1. S/MIME with Mail.app can be used.

2. The warning message "This certificate
   is signed by invalid authority." won't
   be seen after a while when the WIDE
   members only page is accessed with Safari.

[the cause of the problem]

further investigation is needed, though
it's anticipated something wrong is
server side's configuration.

But encoding problem is found in the WIDE
ROOT CA and the moCA certificates and
these certificates aren't accepted as
CA certificates in MacOS X and Safari environment.
This fix of encoding problem is related
to the fix of the access problem.
So, the fix of encoding problem is released at first.

[the measure]

Replace the WIDE ROOT CA certificate and
the moCA certificate to the new ones,
which are called
"encoding problem fixed version" certificates.
The key point is to install the WIDE ROOT CA certificate
to the "X509 Anchors".

The fingerprint of new WIDE ROOT CA certificate
sha1 fingerprint:
be 97 ae 7f c0 37 d2 cb c5 f2 3b eb d3 2c f5 07 74 c3 ef fe

The fingerprint of new moCA certificate
sha1 fingerprint:
27 fa 6b c3 25 6d 4f 0f 6b 3d f2 a5 b6 8a 83 0a 53 33 7f 45

(a) in case of Tiger

1. remove the old WIDE ROOT CA and moCA certificates
   using KeyChain access.
   These certificates might be installed in "Login" or
   "X509 Anchors".

   KeyChain access is found in "utility folder" under
   "application folder".
   The root privilege is required when "X.509 Anchors"
   is changed.

2. Please install the new moCA certificate to KeyChain "Login".
   The URL is http://moca.wide.ad.jp/moca-for-macos050818.cer

3. Please install the new WIDE ROOT CA certificate to
   KeyChain "X509 Anchors".
   The URL is
   http://member.wide.ad.jp/wg/moca/wideroot-for-macos050822.cer

(b) in case of Panther or older version

1. remove the old WIDE ROOT CA and moCA certificates
   using KeyChain access.
   These certificates might be installed in "Login" or
   "X509 Anchors".

2. "Add KeyChain" if the certificate KeyChain doesn't exist.
   add
   /System/Library/Keychains/X509Anchors (for root CAs)
   /System/Library/Keychains/X509Certificates
   (for subordinated CA)

3. Please install the new moCA certificate to KeyChain

"X509Certificates".
The URL is http://moca.wide.ad.jp/moca-for-macos050818.cer

4. Please install the new WIDE ROOT CA certificate to
KeyChain "X509 Anchors".
The URL is
http://member.wide.ad.jp/wg/moca/wideroot-for-macos050822.cer

[related URL (japanese only)]
http://member.wide.ad.jp/wg/moca/wide_root_ca.html
http://moca.wide.ad.jp/

改版履歴
2006/01/05　第 0 版
2006/01/19　第 1 版　　表現を修正
2006/01/27　第 2 版　　誤記を修正