1. JPNIC プライマリルート認証局の電子証明書の入手と確認の手順

概要

一般社団法人日本ネットワークインフォメーションセンター(以下、当センター)では、インターネットの アドレス資源管理やネットワーク運用の安全性向上のため、認証局が運用しています。認証局とは、 SSL/TLS などで通信相手の認証などに使われる、電子証明書を発行する仕組みです。

電子証明書は、偽造することや改変することが技術的に難しいものですが、適切に利用しなければ、 偽造されたものが、あたかも正しいものであるかのように表示されてしまうことがあります。例えば https を 使ってアクセスしている Web サーバが、実は悪意のある別の Web サーバであっても、https の認証の 結果が良好であるような表示(鍵マーク等)がされてしまうことがあります。これを防ぐためには、電子証 明書を利用する前に認証局の電子証明書(以下、認証局証明書と呼びます)を適切に入手し、設定す ることが重要です。

ここでは、JPNIC プライマリルート認証局の認証局証明書を適切に設定する手順を説明します。

1.1. JPNIC プライマリルート認証局の認証局証明書について

JPNIC プライマリルート認証局は、資源管理者証明書を発行している「JPNIC 資源管理認証局」の 認証局の上位に位置する認証局です。JPNIC プライマリルート認証局の認証局証明書は、JPNIC で 運用されている認証局の認証局証明書を正しいものであるかどうかを確認するために使われます。従っ て JPNIC から発行されたユーザやサーバの電子証明書を検証するには、JPNIC プライマリルート認 証局の証明書を「適切に」入手する必要があります。ここで言う適切さとは下記の二点を意味します。

a. フィンガープリントが正しいこと

当センターが配布している認証局証明書のデータと同一であること

b. 認証局証明書としての有効性

認証局証明書の有効性を確認した結果、問題がないこと

正しさが確認できていない認証局証明書を使うと、当センターから発行されていない電子証明書が、 あたかも当センターから発行されたかのように表示されてしまうことがあります。これは、Web サーバのな りすましや利用者のなりすましの原因になります。

1.2. JPNIC プライマリルート証明書とフィンガープリントの入手方法

1.2.1. JPNIC プライマリルート証明書の入手と確認

認証局証明書は、下記の Web ページから入手できます。

JPNIC 認証局のページ http://jpnic-ca.nic.ad.jp/

この Web ページでは、個人情報や認証に関わる情報入力を促されることはありません。異なる場合には、本書末尾にあるご連絡先までお知らせ下さい。

1.2.2. 利用規約とフィンガープリント

当センターで別途申請者に配布している「JPNIC 認証局証明書 利用規約」をご覧下さい。JPNIC 認証局証明書を利用された場合、この規約に書かれた事項に同意されたものとみなされます。

便宜上、下記のWebページにて、本規約に記載されている「JPNIC プライマリルート認証局のフィン ガープリント」を提供しています。

JPNIC 認証局 fingerprint のページ https://serv.nic.ad.jp/capub/fingerprint.html

★ 2012 年 8 月 14 日以前に発行された資源管理カードをご利用の場合 「JPNIC プライマリルート認証局 S2」に加えて、従来の「JPNIC プライマリルート認証局 S1」をインストー ルしておく必要があります。インストール方法につきましては、資源管理カードと共に郵送されました 「資源管理者証明書 セットアップマニュアル」をご覧下さい。

1. JPNIC プライマリルート証明書を入手します	JPNIC 認証局のページ(http://jpnic-ca.nic.ad.jp/)の			
6 7°	「JPNIC フライマリルート認証局証明書」			
	jpinc-pinnary-root-ca-32.cer をようシロードしょ す。			
2. 「ファイルのダウンロード」画面が表示 されますので、"保存"ボタンをクリックし ます。	ファイルのダウンロード - セキュリティの警告 このファイルを聞くか、または保存しますか? 名称: jpnic-primary-root-ca-s2.cer 発語: セキューリティ証明書: 133 KB #語: セキューリティ証明書: 133 KB			
	発信元 jpnic-canic.ad jp 間K(0) (保存(S)) ごをつわれる (人ターネットのファイルは役に立ちますが、このファイルの推測はコンピューターに問題を起こす可能性があります。実信元が14歳での次に、次告は、このソフトウェアを開いたの14年にありないで代表に、人気を見た自己的問題を認った。			
3. 保存する場所をテスクトッフなどに選 択し、"保存"ボタンをクリックします。 ⇒ ファイルのダウンロードが始まります。	日本日本の新知() ● ML(250:M2) ● M			
4. 保存した JPNIC プライマリルート証明 書ファイルをダブルクリックします。(ファ イル名は「jpnic-primary-root-ca-s2.cer」又 は「jpnic-primary-root-ca-s2」となります)	新しいフォルダ □□× ファイル(E) 編集(E) ※ 『 ppic-primary- root-ca-s2.cer 1 (個のオブジ)1.33 KB マイ: //			
5. 入手した証明書は、発行先と発行者と同 ーになっている「自己署名証明書」です。「証 明書は信頼されていません」と表示されま す。内容を確認するため、"証明書のインス トール"ボタンをクリックしてください。				
⇒ 「証明書のインポートウィザード」の画 面が表示されます。 	CO			
6. インポートウィザードでは、「証明書を すべて次のストアに配置する(P)」をクリッ クし、証明書ストアとして「信頼されたル ート証明機関」を選択します。				

1.2.3. JPNIC プライマリルート証明書の設定手順(Internet Explorer)



8. まだ信頼していない証明書をインス トールしようとしているため、「セキュ リティ警告」ダイアログボックスが表示 されます。

拇印(sha1)の値と、「JPNIC 認証局利用 規約」(色のついた紙)や JPNIC NewsLetter の最後のページなどに載せ られている「JPNIC プライマリルート 証明書のフィンガープリント」の値と等 しいことを確認します。

確認後は、"はい"ボタンをクリックし ていください。

⇒正しくインポートされたことが表示 されます。これで a. フィンガープリン トが正しいこと の確認ができました。 JPNIC プライマリルート証明書の設定 は完了です。

【保存したファイル】 「4.」で保存した JPNIC プライマリル ート証明書ファイルは必要ありません ので、削除しても問題ありません。



1 注意

証明書の拇印と JPNIC プライマリルート証明書の フィンガープリントの値が異なる場合には証明書の 安全性を確認できません。"いいえ"ボタンをクリッ クして設定作業を中止してください。

※SHA-1 により算出したフィンガープリントは、40 桁の 16 進数であり、「0」~「9」及び「A」~「F」の文 字の組合せで示されます。ただし、フィンガープリン トを表示するソフトウェアの種類又はバージョンに より、大文字又は小文字の相違等表示方法が異な ることがあります。

 9. ブラウザの"ツール"メニューの"インターネットオプション"を選択してください。 ⇒「インターネットオプション」画面が表示されます。 	●1000 Top Dec ●1000
10. 「インターネットオプション」画面 の"コンテンツ"タブを選択し、"証明書" ボタンをクリックしてください。 ⇒「証明書」画面が表示されます。	インターネット オブション 21× 全級 セキュリティ フランツ ボンランツ アドバイザ ジンランツ アドバイザ ジンランツ アドバイザ ジンランツ 海谷ノターネット 「日本 有効にする(2)」 「日本 第二 「日本 「日本 「日本 第二 「日本 第二 「日本 第二 「日本 第二 「日本 第二 「日本 第二
 11.「信頼されたルート証明機関」タブ を選択し、発行先の「JPNIC Primary Root Certification Authority S2」をクリックし、画 面下部の"表示"ボタンをクリックしてくだ さい。 ⇒JPNIC Primary Root Certification Authority S2の「証明書」画面が表示されます。 	MAX I BFX(5) (TATD) GA 12563A GA

12. "証明のパス"タブを選択すると、 証明のパスが最上位に記載されます。

「この証明書は問題ありません。」という メッセージが確認できれば b. 認証局証 明書としての有効性の確認ができている ことになります。

これで JPNIC プライマリルート証明書が 正しく Web ブラウザにインストールさ れていることが確認できました。

- 証明のパス(P)	/ Root Certification A	uthority S2	
		証明書の表	ज्र ⊻
証明書の状態(<u>S</u>):			
この証明書は問題あり	ません。		

1.2.4. JPNIC プライマリルート証明書の設定手順(Firefox)

1. 認証局証明書を入手します。	JPNIC 認証局のページ(http://jpnic-ca.nic.ad.jp/)に リンクがあります。「JPNIC プライマリルート認証局 証明書」jpnic-primary-root-ca-S2.cer をダウンロ ードします。
2. 「証明書のダウンロード」画面が表示されますので、入手した証明書が正しいことを確認するために"表示"ボタンをクリックします。	正時度のダウンロード X) 新した2022月 のわめ を住舗するとを確認する。 次の用途のために「証明書記22月後、名称子可約「を住舗しますか? この認証期を増イメールユーザの特定に使用する。 この認証期を増イメールユーザの特定に使用する。 この認証期を対かったうた。 この認証期を対応に使用する。 この認証期を対応に使用する。 この認証期を対応では値する前にに認証期の証券目表、ポリシーそして手続きを確認してください。 表示 QK キャンセル 人のブ
3. 証明書ビューアが表示されたら、画面下 部の「フィンガープリント」が表示されま すので、これらが等しいことを確認しま す。SHA-1 Fingerprint と MD5 Fingerprint の両方を確認して下さい。	正明書ビューア*OU=JPNIC Primary Root Certification Authority S2.0=Japan Net(×) 一該① 詳細① 摩因不明の問題により、この証明書の有効性を検証できませんでした。 発行対象 一般名称(CN) 一般名称(CN) 「証明書に記載されていません〉 40歳(0) Japan Network Information Center 部門(010) JPNIC Primary Root Certification Authority S2 ジビアビルを発表のためを見ます。 ①
▶ 注意 証明書の拇印と JPNIC プライマリルート 証明書のフィンガープリントの値が異な る場合には証明書の安全性を確認でき ません。"閉じる"ボタンをクリックして設 定作業を中止してください。 ※SHA-1 により算出したフィンガープリン トは、40 桁の 16 進数であり、「0」~「9」 及び「A」~「F」の文字の組合せで示され ます。ただし、フィンガープリントを表示す るソフトウェアの種類又はバージョンによ り、大文字又は小文字の相違等表示方 法が異なることがあります。	907月番号 004710.5034A204494F6 第行者 - 般名称 (CN) 〈証明書に記載されていません〉 組織(0) Japan Network Information Center 副門(0) JPINC Primary Root Certification Authority S2 証明書の有効期間 2012/02/25 確明書のマンガーブリント C94F-B6FC957144-D4-BC-4436-AB3BC9-E5612B-AC-7245 MD5 フィンガーブリント 435937FC-409D-7D95014621-AD325E476F
確認後は 闭しる ボダンをグリックし てください。これで a.フィンガープリント が正しいこと の確認ができました。	
⇒「証明書のダウンロード」画面に戻りま す。 4. [Wob サイトを特定する トキーニの認証	[18]建0/9ウンロード
4. · WeD サイトを行足りるとさ、この認証 局を信頼する 」「この認証局による Web	新しい記録記局 (CA)を信頼するとき確認でする。

局を信頼する。」、「この認証局による Web サイトの識別を信頼する。」または「この 認証局を Web サイトの特定に使用す る。」にチェックをして "OK "ボタンをク リックしてください。何も表示されません が、これで設定は完了です。次に進みます。

 運動書のダウンロード
 ★

 新して収益に用くCA)を信頼すると参幅記づする。
 :>

 :次の用途の応めに"証明書記詰用」(名称不明)"を信頼しますか?
 「

 「
 この総証証券をWeb サイトの特定に使用する。

 「
 この総証証券を電子メールユーザの特定に使用する。

 「
 この総証証券をセンフトウェア製作者の特定に使用する。

 この総証証券を取りつりェア製作者の特定に使用する。
 この総証券を応信数する前に、認証券の証明書を寄査

 ○
 「

 ○
 「

 ○
 「

 ・
 」

 ・
 」

 ・
 」

 ・
 」

 ・
 」

 ・
 」

 ・
 」

 ・
 」

 ・
 」

 ・
 」

 ・
 」

 ・
 」

 ・
 」

 ・
 」

 ・
 」



2. JPNIC 資源管理認証局証明書の入手と確認の手順

2.1. Internet Explorer での設定手順

1. JPNIC 資源管理認証局証明書の入手

JPNIC 資源管理認証局証明書

(JPNIC-Resource-Service-CA-S2.cer)をダウンロ ードします。

2. JPNIC 資源管理認証局証明書の表示

入手した証明書ファイルをダブルクリックす ると右のダイアログが表示されます。

発行先が

「JPNIC Resource Service Certification Authority S2」

発行者が

「JPNIC Primary Root Certification Authority S2」

であることを確認してください。

3. 証明のパスの確認

証明のパスが

「JPNIC Primary Root Certification Authority S2」

で始まっていることを確認して下さい。

JPNIC 認証局のページ (http://jpnic-ca.nic.ad.jp/)にリンクがあります。





2.2. Firefox での設定手順

1. JPNI	C 資	源管	會理	認訂	E局	証明]書(の入	、手	
JPNIC	資	源	管	理	認	証	局	証	明	書
(JPNIC	C-Re	eso	urce	e-Se	ervio	ce-C	CA-S	S2.c	cer)	を

JPNIC 認証局のページ(http://jpnic-ca.nic.ad.jp/) にリンクがあります。

ダウンロードします。

ツール(T) → オプション(O) → 証明書を 表示(S) から「認証局証明書」タブを開 きます。	Ediga マネージャ
2. インポート	2回2月回明書を含わ7ァイルを選択してください ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
インポート(M)をクリックし、ダウンロ ードしたファイルを選択します。	アイドルを含めれている Importance - Service - CA - S2.cer 第1010-571039 アイドネコシント 第101-571039 アイドネコシント アイドネコシント アイドル省(1)0- アイドネコシント Importance - Service - CA - S2.cer アイドル省(1)0- Importance - Service - CA - S2.cer アイリル省(1)0- Importance - Service - CA - S2.cer
3. 証明書のインストール	正明書のインポート 新しい初耳島(CA)を信頼するとうせからわています。本当にこの初耳島を信頼しますか?
「この認証局による Web サイトの識別 を信頼する。」にチェックをし、証明書を 表示をクリックします。	*名前のない認証局*が行う認証のから、信頼するものを選択してください。 ✓ この認証局による Web サイトの識別を信頼する この認証局による メールユーザの識別を信頼する この認証局による メールユーザの識別を信頼する 認証局を信頼する場合はその目的に関わらず、認証局の証明書が間違いないこと、認証ポリシーや認証実施規 定に問題がないことを確認してください。
4. 証明書選択の設定	
ツール(T) → オプション(O) →詳細で、 "毎回自分で選択する"を選びます。	 →般 タブ コンデンツ プログラム プライバシー セキュリティ Sync 詳細 一般 ネットワーク 更新 暗号化
この設定により、クライアント証明書を使 う際に必ず確認のダイアログボックスが 表示され、Web申請システム以外のサーバ に不用意に証明書を提示することを避け ることができます。	プロトコル マ SLS 30を使用する(3) 「 SLS 30を使用する(3) マ TLS 10を使用する(1) 「 証明書 ワ 「 1070個人証明書を要求(UC228*) ○ 自動的にご選択する(1) ○ 毎回自分で選択する(0) ご 毎回自分で選択する(0) ● 毎的にご選択する(2) ● 毎回自分で選択する(0) ● 毎回自分で選択する(2) ● 毎回自分で選択する(2)