VeriSign®
The Value of Trust℠

Managed PKI for SSL

Administrator's Guide

CUSTOMER MANUAL

ベリサイン マネージド PKI for SSL

管理者ガイド

mpki-support@verisign.co.jp

VeriSign Japan K.K..rev_5.0.

ベリサイン マネージド PKI for SSL 管理者ガイド

VeriSign Japan K.K. rev5.0

発行: 2009 年 5 月

注意

本書は、VeriSign,Inc が、Managed PKI for SSL Control Center（管理者用コントロールセンター）で公開している「Managed PKI for SSL Administrator's Guide」を日本ベリサイン株式会社が参考のために翻訳したものであり、お客様を何ら拘束するものではございません。

また、日本ベリサイン株式会社は本書をもって、お客様に対し、何らの表明・保証をおこなうものではございません。

免責事項について

日本ベリサイン株式会社は、本書の情報の正確さと完全性を保つべく努力を行っています。ただし、日本ベリサイン株式会社は本書に含まれる情報に関して、(明示、黙示、または法律によるものを問わず)いかなる種類の保証も行いません。日本ベリサイン株式会社は、本書に含まれる誤り、省略、または記述によって引き起こされたいかなる（直接または間接の)損失または損害についても責任を負わないものとします。

さらに、日本ベリサイン株式会社は、本書に記述されている製品またはサービスの適用または使用から生じたいかなる責任も負わず、特に本書に記述されている製品またはサービスが既存または将来の知的所有権を侵害しないという保証を否認します。本書は、本書の読者に対し、本書の内容に従って作成された機器または製品の作成、使用、または販売を行うライセンスを与えるものではありません。最後に、本書に記述されているすべての知的所有権に関連するすべての権利と特権は、特許、商標、またはサービス・マークの所有者に属するものであり、それ以外の者は、特許、商標、またはサービス・マークの所有者による明示的な許可、承認、またはライセンスなしにはそのような権利を行使することができません。日本ベリサイン株式会社は、本書に含まれるすべての情報を事前の通知なく変更する権利を持ちます。

商標について

VeriSign、VeriSign のロゴ、VeriSign Trust Network、ベリサイン マネージド PKI、およびその他の商標、サービスマーク、およびロゴは、VeriSign,Inc.とその関連会社の米国およびその他の国における登録商標または商標です。本書に記載の他の商標およびサービスマークはそれぞれ各社に所有権があります。

本書に記載された特徴または機能、あるいはその両方がご使用のソフトウェアやお客さまのサービス契約に含まれない場合もあります。本ベリサインプロダクトの特徴や機能の詳細については、ベリサイン担当窓口までお問い合わせください。

目次

改訂履歴

1997 年 5 月　初版

2004 年 7 月　rev_2

2005 年 8 月　rev_3

2006 年 3 月　rev_3.1

2006 年 8 月　rev_3.2

2006 年 12 月　rev_3.3

2007 年 2 月　rev_3.4

2007 年 11 月　rev_4.0

2009 年 5 月　rev_5.0

第1章　はじめに

ベリサイン マネージド PKI for SSL は、企業内のあらゆるドメインをセキュアに運用する上で欠かせないサーバ ID（Digital ID、サーバ証明書とも呼ばれます）を、貴組織で発行し、管理するための手段を提供するものです。ベリサイン マネージド PKI for SSL の管理者は、以下のことを行います。

- ベリサイン マネージド PKI for SSL のオプション設定
- 申請ウェブページのカスタマイズと、組織内の申請者が申請を行うときの支援
- サーバ ID のリクエストの内容確認と、各リクエストに対する承認／拒否の決定
- ライフサイクル全体を通じたサーバ ID の管理
- 管理者 ID とベリサイン マネージド PKI for SSL サービスの更新

ベリサイン マネージド PKI for SSL サービスを管理していく上で、追加の管理者が必要になることもあります。このような場合には、追加の管理者に管理責任を割り当てる、割り当てた管理責任を削除する、追加の管理者が ID の登録、管理、更新を正しく行えるようにするということを実施可能です。

注　本資料は 2009 年 2 月の時点でのベリサイン マネージド PKI for SSL システムをベースに記述しております。実際の画面に表示されるページが本書に示されているページと異なることがあるかもしれませんのでご注意ください。

ベリサイン マネージド PKI for SSL について

インターネットを介したビジネスでは、その企業の通信（インターネット、イントラネット、エクストラネットのいずれであれ）がセキュアであることを保証する手段が必須になります。SSL サーバ証明書と Secure Sockets Layer（SSL）プロトコルは、認証された暗号化通信をクライアントとサーバ間で実現するための、最も便利で信頼できる手段です。ウェブブラウザとウェブサイトのサーバ間で、サーバ ID を使用してセッションが開始されることにより、ユーザはそのサーバがなりすましでなく、認可を受けた組織に属するものであることが確信できます。ブラウザとサーバ間のすべての通信が暗号化されるので、本来の受信者以外の人物に盗聴されたり解読されたりすることはありません。ベリサイン マネージド PKI for SSL を利用した場合、貴組織がサーバに対するサーバ ID

の発行と管理を行い、ベリサインがバックエンドの公開鍵暗号基盤（PKI）の機能を受け持ちます。サーバ ID とベリサイン マネージド PKI for SSL の組み合わせは、ウェブサイト、イントラネット、またはエクストラネットを認証するための、インターネットの標準の証明書です。

ベリサイン マネージド PKI for SSL によって、組織内の各個人はサーバ ID の申請者となり、サーバ ID は申請者が管理するサーバに格納され、関連付けられます。申請者は、ウェブベースのサブスクライバーサービスページを使用して、サーバに代わって以下のアクティビティを行います。

サーバ ID の申請（証明書申請ページの記入と送信）
サーバ ID の検索
サーバ ID の更新
サーバ ID の再発行
サーバ ID の失効
登録済みドメイン名の表示

サーバ ID について

ベリサイン マネージド PKI for SSL では、ベリサイン製品のセキュア・サーバ ID、グローバル・サーバ ID、セキュア・サーバ ID EV とグローバル・サーバ ID EV と同等のものを発行することができます。

本書について

本書は、ベリサイン マネージド PKI for SSL の管理者向けのガイドです。管理者は、サーバ ID の申請があった場合、申請内容を確認後、申請者ならびに ID の発行先となるウェブサイトの実在性を検証し、申請の承認または拒否を決定します。また、管理者は、申請者の申請ページを作成するとともに、申請者に対するテクニカルサポートも行います。

本書の構成

本書は、以下の構成になっています。

第 2 章「責任範囲」: ベリサイン マネージド PKI for SSL を提供するための管理者の責任と組織の責任について概要を述べます。

第 3 章「コントロールセンターの設定と使用」: ベリサイン マネージド PKI for SSL の設定と使用について詳しく説明します。ベリサイン マネージド PKI for SSL システムのガイ

ドツアーでは、登録の申請、承認、管理のプロセスをご紹介します。
第 4 章「管理者 ID とサーバ ID の管理」：日々の証明書管理業務（サーバ証明書の申請の承認と拒否、サーバ ID の管理など）を行うためのコントロールセンターの使い方について、詳しく説明します。

ベリサインのマネージド PKI for SSL 担当窓口

ベリサイン マネージド PKI for SSL サービスについてサポートが必要な場合は、以下の URL にアクセスしてください。

ベリサイン ウェブサイト：http://www.verisign.co.jp/serveronsite

または電話もしくはメールでお問い合わせください。
電子メール：mpki-support@verisign.co.jp
電話番号：044-520-7210

FAQ

ベリサイン マネージド PKI for SSL ヘルプデスク：

http://www.verisign.co.jp/serveronsite/help/

ベリサイン マネージド PKI for SSL 管理者用 FAQ：

https://support.verisign.co.jp/ssl/faq/indexa.html

（※アクセスには管理者証明書が必要となります）

日本ベリサイン営業部

サービスもしくはオプションの追加購入、更新、販売関連のご質問については、電話もしくはメールでお問い合わせください。

電子メール：mpki-ssl@verisign.co.jp

電話番号：03-3271-7013

第2章　責任範囲

この章では、ローカル登録局（LRA）としての組織の責任と管理者の責任について述べます。

概　要

ベリサインは認証局（CA）を運営しております。CA とは、証明書の発行、管理、失効、および更新を行い、証明書のライフサイクル全体にわたって申請者を支援する主体です。CA は、これらの機能をローカル登録局（LRA）に権限を委譲し、操作を行うことができます。ただし、証明書を実際に作成して署名するのは CA です。

ベリサイン マネージド PKI for SSL を使用することで、貴組織は VeriSign Trust Network（VTN）内のベリサイン マネージド PKI for SSL クラス 3 認証局（CA）の LRA となり、CA（ベリサイン）に代わって証明書管理機能を果たします。管理者の責任には、サーバ ID の申請や更新などの申請者支援、サーバ ID の申請の承認、サーバ ID の失効などがあります。管理者が VTN サーバ ID についてこれらの機能を果たすときには、ベリサイン認証局運用規定（CPS）におけるローカル登録局管理者（LRAA）の役目を果たすことになります。

あなたも含め、組織によって任命されたベリサイン マネージド PKI for SSL 管理者はすべて、このマニュアルに記載されている処理を行う人物です。

管理者及び組織によって任命された追加管理者はすべて、このマニュアルに記載されているアクティビティを行うことが認められた人物です。

証明書管理業務の大半は、ウェブベースの管理者用画面(コントロールセンター)を使用して行います。コントロールセンターのセキュアなウェブページ上では、サーバ ID の申請内容の確認、申請の承認、拒否、サーバ ID の管理、サーバ ID の確認、管理者アクティビティの確認、追加のサーバ ID（管理者 ID を含む）の申請などの業務を行うことができます。

- コントロールセンターへのアクセス方法などの詳細については、第 3 章「コントロールセンターの設定と使用」を参照してください。

- サーバIDの日常管理業務の詳しい手順については、第 4 章「管理者IDとサーバIDの管理」を参照してください。

貴組織の責任

貴組織は、サーバ ID 申請者にサーバ ID の要求方法を指示します。次に、サーバ ID 申請者とサーバ ID が発行されるウェブサイトの実在（予定を含む）と取得の意思確認を行うことにより、要求を検証します。

クラス 3 証明書によって規定されている保証レベルと同等の手段によって申請者検証を行うのは、ベリサインではなく「権限委譲を受けている貴組織の責任」となります。

管理者は、貴組織の組織名とドメイン名を含む証明書がウェブサイトに導入することを貴組織が承認しているかどうかを確認し、サーバ ID 申請者が申請の人物であるかどうかを確認します。また、人事記録やウェブサイトレコードなどの適切な社内文書を使用して、実在確認と組織への所属を検証した後、その他の情報について確認します。これらの確認後、管理者は証明書発行申請を承認または拒否します。

組織がサーバ ID 申請を承認すると、ベリサイン マネージド PKI for SSL サービスがその申請内容をベリサイン（CA）に処理依頼をし、申請者にサーバ ID が発行されます。サーバ ID を受け取った方は、申請者と呼ばれます。ベリサインは、証明書リポジトリ（データベース）にサーバ ID を公開します。これにより、リポジトリを確認することでサーバ ID とその有効性情報が入手できるようになります。

ベリサイン マネージドPKI for SSL申請者規約

ベリサインは管理者の参考用に、ベリサイン マネージド PKI for SSL 契約を http://www.verisign.co.jp/repository/index.html に掲載しています。申請者は、この契約の条項に従う必要があります。

サーバIDの失効責任

組織には、不要になったサーバ ID を失効する権限と責任があります。管理者は、ベリサイン認証局運用規定（CPS）に従い、以下の場合にサーバ ID を失効する責任があります。

- サーバ ID の秘密鍵の紛失、盗難、改変、無許可の開示、もしくはその他の危殆化があった場合。

- サーバ ID に関連付けられた主体が CPS もしくは適用可能な申請者規約に基づく重大な義務に違反した場合。
- CPS もしくは申請者規約に基づく個人の義務の遂行が不可抗力、天災、コンピュータもしくは通信障害、規則、条令、もしくはその他の法律、正式な行政措置（輸出規制管理を担当する機関による処置を含むが、これに限らない）、もしくは個人の妥当な制御を超えるその他の原因によって遅延(もしくは妨げられ)、結果として、別の人物の情報が著しく脅かされた、もしくは危殆化した場合。
- サーバ ID がベリサイン CPS、もしくは本書で要求されている手順に著しく反した方法で発行されたことがわかった場合。
- サーバ ID がサーバ ID の対象として主張された以外の主体に対して発行された場合。
- サーバ ID がサーバ ID の対象として指名されている主体と関連付けられている申請者の許可を得ずに発行された場合。これは、たとえば名前または存在確認に関する虚偽または改変された情報に基づいてサーバ ID を取得した場合に該当します。
- 申請者が組織の傘下の個人(組織)でなくなった場合。

  失効の詳細については、下記 URL にあるベリサイン CPS を参照してください。

  http://www.verisign.co.jp/repository/CPS/index.html

失効猶予期間

ID の発行後 1 ヶ月以内に失効された場合は、ID のライセンス数は戻ります。これを失効猶予期間といいます。この猶予期間内に失効された場合、管理者によって失効されたか申請者によって失効されたかに関係なく、ID のライセンス数は戻ります。

ベリサイン マネージドPKI for SSL管理者の追加任命

管理者は、追加の管理者が必要であると判断した場合、追加の管理者IDを申請することができます。その場合は、ベリサイン営業担当（mpki-ssl@verisign.co.jp）までご連絡ください。

なお、管理者を追加する場合は、アカウントの登録時に管理者が入力した組織名と部署名をお知らせ頂く必要があります。

管理者の適性

ベリサイン認証局運用規定（CPS）では、ID の発行に関連して、ベリサイン マネージド PKI for SSL の管理を行う候補の方に対して、教育、トレーニング、認定、および調査要件を規定しています。

さらに、ベリサインは、あらゆる組織のベリサイン マネージド PKI for SSL 管理者が以下の技能を持つことを推奨しています。

- ベリサイン マネージド PKI for SSL のサーバ ID と統合しようとしているアプリケーションについての十分な知識
- 貴組織の PKI によって保護されるデータとリソースの知識
- PKI の知識
- インターネットアプリケーション、ウェブブラウザ、および HTML を扱うスキル
- プロジェクト管理スキル

管理者の権限の設定

コントロールセンターの Administrators Wizard より管理者の管理責任の設定や削除をすることができます。

管理者の権限は、以下のように分かれており、フル権限から読み取り専用権限まで様々です。

- Security Administrator
- Configuration Administrator
- Certificate Management Administrator
- EV Certificate Management Administrator
- Read-only

注 管理者の権限については、22 ページの「Administrators」で詳しく述べます。

組織によって登録された管理者には、初期設定でセキュリティ管理者としてすべての権限（フルアクセス）が割り当てられます。セキュリティ管理者の権限を持った管理者は、自分の管轄の範囲内で、自分以外の管理者に追加の権限を割り当てる、または削除することができます。

ベリサイン マネージドPKI for SSLのIDライセンスのプランニング

ベリサイン マネージド PKI for SSL の ID ライセンスは、単位に基づきます。1 単位は、1 枚のサーバ ID の使用によって 1 台のサーバを 1 年間保護することを表します。

サーバ ID は、さまざまな単位で購入できます。例えば、1 つのサーバ ID で複数のサーバの保護や（例：負荷分散）、2 年間／3 年間有効なサーバ ID の発行もできます。使用する単位数を計算するには、以下の式を用います。

[SSL 有効期間] x [ID によって保護されるサーバ数] = 使用単位数

たとえば、2 年間有効なサーバ ID で 10 台のサーバを保護する場合、使用単位数は 20 です。

1 年間または 2 年間あるいは 3 年間のサーバID運用期間

サーバ ID の有効期間は、1 年または 2 年あるいは 3 年です。管理者は、これらのオプションを申請者のサーバ ID 申請フォームに表示する方法を設定します。申請者は、サーバ ID 申請時に、申請フォームに表示されたオプションから選択することができます。2 年間のサーバ ID は 2 ライセンスとして、3 年間のサーバ ID は 3 ライセンスとしてカウントされます。

複数サーバのライセンス

あるコモンネームに限定して同じサーバ ID を使用し、かつ、複数のサーバ間で負荷を分散することができます。ただし、サーバごとにライセンスが必要なので、ライセンス数は購入した単位数だけ計上されます。

サーバIDの追加注文

IDの追加が必要な場合は、ベリサイン営業担当(mpki-ssl@verisign.co.jp）までご連絡ください。

申請者サービスの提供

申請者とは、自分の管轄にあるサーバに代わってサーバ ID の申請や管理を行う組織内の人です。管理者は申請者に対して、組織の証明書サブスクライバーサービスページの URL を通知してください。この URL は、コントロールセンターの[Certificate Management]ー[Subscriber Services]ページで参照できます。

申請者は、サブスクライバーサービスページで自分のサーバ ID に対して以下のアクティビティを行います。

- サーバ ID の申請
- サーバ ID の検索
- サーバ ID の更新
- サーバ ID の再発行
- サーバ ID の失効
- 登録済みドメイン名の表示

申請者が行う登録申請

申請者がサーバ ID の申請もしくは更新を行うときには、管理者に提示されたサブスクライバーサービスページの URL にアクセスします。申請者は、申請ページの以下のフィールドに入力します。

[申請者情報]

申請者は、自分の氏名、メールアドレス、およびサーバ ID 取得申請のためのその他の情報を入力します。

[サーバソフトウェアおよび CSR(Certificate Signing Request、証明書申請ファイル）]

証明書署名要求（CSR）は、組織の公開鍵、名前、所在地、および URL を含んだ暗号化ファイルです。申請者はウェブサーバを使用して、2 つのファイル（秘密鍵と CSR）を生成します。CSR を生成するための手順は、ウェブサーバのタイプによって異なります。

特定のウェブサーバの CSR を生成するには、以下をご覧ください。

http://www.verisign.co.jp/server/help/csr/index.html

ユーザが CSR を生成するときには、[Organization]、[Organizational Unit]、[Country]、[State]、[Locality]、および[Common Name]フィールドに入力する必要があります。

注 申請者は自分の秘密鍵をフロッピーディスクなどにバックアップして、安全な場所に保管してください。ベリサインには秘密鍵のコピーはありませんので、秘密鍵を紛失もしくは破損した場合、申請者はサーバ ID を使用できなくなります。

[証明書取得オプション]

このセクションに、サーバ ID の有効期間が表示されます。管理者は、あらかじめ標準の有効期間として 1 年間または 2 年間あるいは 3 年間を選択します。管理者が、申請者が有効期間を選択できるようにした場合は、申請者はここで有効期間を変更できます。有効期間を選択できないようにした場合、このオプションは選択できません。

[チャレンジフレーズ]

管理者が管理者 ID の申請を行ったときと同じように、申請者はチャレンジフレーズを入力する必要があります。チャレンジフレーズは、ID を取得する際と更新の際に必要となります。チャレンジフレーズは、なりすましの被害を避けるために、他人には推測されにくい文字列を選んでください。チャレンジフレーズを忘れた場合、サーバ ID が危殆化した場合、もしくは紛失した場合には更新や失効ができません。なお、チャレンジフレーズには英字のみを使用し、アクセント記号の付いた文字や句読点を使用しないでください。ベリサインではチャレンジフレーズの管理を行っておりません。チャレンジフレーズを忘れた場合は、管理者に再設定を依頼してください。

[管理者への連絡事項]

管理者は、確認を容易にするために、このフィールドに特殊な情報を入力するように申請者に要求することができます。(英語のみ)

[証明書利用規約]

サーバ ID を取得するには、ベリサイン Digital ID 申請者規約に同意していただく必要があります。

申請者のサポート

ベリサインは、管理者による申請者のサポートを支援するために、以下の資料を用意しています。

- **申請と証明書ライフサイクルのそれぞれの機能に関するオンラインヘルプ**

  申請者が使用するページには、証明書の申請から取得までの各プロセスに関するオンラインヘルプがあります。

- ベリサイン **ウェブサイト**

  ベリサイン ウェブサイトには、管理者と申請者向けに、ベリサインサーバ ID に関する一般情報を含んだ FAQ があります。

ベリサイン マネージド PKI for SSL ヘルプデスク：

http://www.verisign.co.jp/serveronsite/help/

ベリサイン マネージド PKI for SSL 管理者用 FAQ：

https://support.verisign.co.jp/ssl/faq/indexa.html

（※アクセスには管理者証明書が必要となります）

申請者の秘密鍵の保護

管理者には、申請者がサーバ ID に関連付けられた秘密鍵を正しく生成し保護できるように予防措置を講じる義務があります。秘密鍵の保護は、サーバ ID の適正な使用にとって不可欠です。辞書にあるような一般的な名前や語句を避け、容易に推測できないパスワードで自らサーバ ID を保護するよう申請者に指示してください。また、以下の URL にあるベリサインの「“Digital ID”および“秘密鍵“の保護に関するよくある質問」を読むように申請者に指示してください。

http://www.verisign.co.jp/repository/faq/digitalid_security.html

サーバ ID 申請者には、自分の秘密鍵を危殆化、紛失、開示、改変、あるいは不正使用から保護する責任があります。組織は、サーバ ID 申請者に適切な指示を与えて、この責任を遂行させなければなりません。

証明書ディレクトリの管理

組織のディレクトリサーバを使用して、申請者に関する最新情報を組織全体で共有できます。ベリサイン マネージド PKI for SSL では、新規に取得した証明書や失効した証明書のリストをダウンロードして、組織のディレクトリサーバにインポートできます。ベリサイン マネージド PKI for SSL には、これらのリストをダウンロードするために、[Certificate Management]ページに 2 つのオプションがあります。

- [Download CRL]リンクでは、証明書失効リスト（CRL）をダウンロードできます。これは、失効した証明書のシリアル番号のリストです。CRLにデジタル署名がされており、管理者がCRLの内容の完全性と真正性を確認してダウンロードできるようになっています。CRLは毎日、夜間に更新されています。CRLのダウンロードの詳細については、33 ページの「CRLのダウンロード」を参照してください。
- [Update Directory]リンクでは、LDAP Data Interchange Format（LDIF）でディレクトリファイルの更新とダウンロードができます。LDIFディレクトリファイルを使用すると、Lightweight Directory Access Protocol（LDAP）標準に準拠している任意のディレクトリサービスに証明書情報をエクスポートできます。LDIFディレクトリファイルのダウンロードの詳細については、36 ページの「LDAPディレクトリファイルのダウンロード」を参照してください。

レポートと監査証跡の処理

コントロールセンターには、レポート機能と監査証跡機能の両方が含まれています。管理者は以下のことができます。

- サーバ ID 要求、サーバ ID、および監査証跡レコードの動的な照会と表示
- 用途に応じた標準レポートの生成
- すべての管理者が監査目的で行ったアクティビティのログファイルの生成

レポートによって、申請、発行、および拒否された申請者と管理者の証明書（証明書内の各フィールドの詳細も含めて）の確認や、各証明書の現在のステータスを調べることができます。監査証跡を使用すると、管理者のアクティビティや、サーバID要求に関連するすべてのイベントを確認することができます（これらのリソースの使用については、35 ページの「レポートの管理」と 38 ページの「管理者監査証跡リンク」を参照してください）。定期的に発行したサーバIDを確認してください。

その他の責任

このセクションでは、管理者のその他の責任について述べます。

ベリサイン マネージドPKI for SSLの更新

管理者 ID やベリサイン マネージド PKI for SSL サービスは、1 年毎に更新を行う必要があります。

注 ベリサイン マネージドPKI for SSL管理者IDとサービスの更新については、41 ページの「サーバIDの更新」を参照してください。

追加ドメインの注文

ベリサイン マネージドPKI for SSLでは、証明書を認証する追加ドメインを注文できます。追加ドメインについてはベリサイン弊社営業担当（mpki-ssl@verisign.co.jp）までお問い合わせください。なお、サービス契約時にはドメイン数無制限で無料登録が可能です。また、契約更新時にはさらに追加登録が可能です。

登録済みの有効ドメイン名は、以下の手順で確認することができます。

1 コントロールセンターの[Certificate Management]ページで[Subscriber Services]をクリックします。

2 URL へのリンクを選択して表示された画面内から、[登録済みドメイン名]をクリックします。

第3章　コントロールセンターの設定と使用

ベリサイン マネージド PKI for SSL の使用を開始するには、管理者によって管理者 ID の申請が完了しており、ID がブラウザにダウンロードされていなければなりません。管理者 ID は、コントロールセンターとの通信を安全に行うための証明書です。

コントロールセンターについて

ベリサイン マネージド PKI for SSL とのインターフェースは、ウェブベースのコントロールセンターになります。管理者はインターフェースを使用して全ての作業を行います。

コントロールセンターへは、管理者のみが、管理者 ID を使用してアクセスすることができます。管理者がコントロールセンターにアクセスすると、ベリサインはブラウザからベリサイン マネージド PKI for SSL 管理者 ID を読み取って管理者を認証します。

コントロールセンターへのアクセス

コントロールセンターにアクセスするには、以下のコントロールセンターURL をブラウザに入力します。コントロールセンターでは、安全な通信が行われるよう、セキュア HTTP プロトコル（HTTPS）を使用しています。一般的な http ではなく、https と入力してください。

- コントロールセンターにアクセスするには：

  https://enterprise-ssl-admin.verisign.com/OnSiteHome.htm

初めてコントロールセンターにアクセスする場合は、Enrollment Wizard を実行して、ベリサイン マネージド PKI for SSL を設定する必要があります。

ベリサイン マネージドPKI for SSLの初期設定

このセクションでは、ベリサイン マネージド PKI for SSL を設定する手順を詳しく述べます。

Step 1　　コントロールセンターへのアクセスと申請の設定

1　ベリサイン マネージド PKI for SSL 管理者 ID の取得手順が記載されている

メールを開いて、リンクをクリックして以下の URL 上のコントロールセンターにアクセスします。

https://enterprise-ssl-admin.verisign.com/OnSiteHome.htm

2　画面上にある[Configuration]リンクをクリックします。

3　画面左にある[Enrollment]をクリックします。

Step 2　　Enrollment Wizard の実行

Enrollment Wizard は、サーバ ID 申請ページの内容をカスタマイズするためのものです。

申請者がサーバ ID を要求する際に使用する申請ウェブページの設定を変更したい場合は、Enrollment Wizard を実行してください。

Enrollment Wizardページ：

申請者サポート用の電子メールアドレスの入力、およびサーバ ID 申請ページのカスタマイズ

1　「Select Certificate Types to Offer」
申請ページから申請者が選択できるサーバ ID の種類を設定します。

2　「Enter the Email Address for Technical Support」
申請者がサーバ ID に関する質問を送信するときに、その問い合わせの宛先となる電子メールアドレスを入力します。

ヒント　特定の個人の電子メールアドレスではなく、電子メールエイリアスを入力しておくことをお勧めします。管理者が退職した場合でも、申請者ページや電子メールウィザードのアドレスを変更する必要がありません。

3　「Select Language」

“Language”から申請ページに表示したい言語を選択します。

図 3-1 [Select Language]

4　「Customize Account Name」

申請ページ上部に表示されるアカウント名の表示を変更することができます。

- 申請時にご登録いただいた O および OU 名の表示のまま使用する場合は[Use Default:<お客様の O、OU 名>]を選択します。
- 表示を変更したい場合は、[Use the following:]を選択し、表示したい名称を入力します。

※　日本語（UTF-8 エンコーディング）の入力が可能です。

5　「Customize Subscriber Instructions」

申請ページ画面内に注釈を挿入します。

- 申請ページ画面の上方に表示したい場合は、”Introduction”チェックボックスにチェックをし、コメントを入力します。
- 申請ページ画面の下方に表示したい場合は、”Footnote”チェックボックスにチェックをし、コメントを入力します。

※　日本語（UTF-8 エンコーディング）の入力が可能です。

6　「Customize Enrollment Requirements」

ここでは、申請者の申請オプションをカスタマイズします。

- 必須フィールドと任意フィールドを指定します。[Include on Subscriber Enrollment Page]セクションで、チェックボックスをチェックすることによって、申請ページに表示するフィールドを指定します。
  - サーバ ID を取得するために証明書申請者が必ず入力しなければなら

ないフィールドについては、[Required]を選択します。

－　申請時に証明書申請者が選択しなくてもよいフィールドについては、[Optional]を選択します。

■　申請ページに表示するカスタムフィールドを 10 個まで定義します。ユーザ定義の新しいフィールドを申請ページに追加したい場合は、左側の[Include on Subscriber Enrollment Page]をクリックして、新しいフィールドラベルをテキストボックスに入力し、必要に応じて[Description]に各フィールドの説明を入力してください。

7　「Select Certificate Lifecycle Options」

「Validity Period」

■　申請者のサーバ ID のデフォルトの有効期限を設定します。[Default Validity Period]セクションで、[1 Year]または[2 Year]あるいは[3 Year]を選択します。

※　サーバが 2 年間／3 年間有効のサーバ ID を必要としないとわかっている場合は、デフォルトとして[1 Year]を選んでください。

申請者が証明書申請時にサーバ ID の有効期間を変更できるようにします。変更できるようにする場合には[Subscriber Override]フィールドで[Yes]を選択します。申請者がデフォルトの有効期間を変更できないようにしたい場合は、[No]を選択します。

「Subject Alternative Names」

チェックのはずれたデフォルト設定のままでご利用ください。

「Subscriber Override」

■　証明書の有効期間を常に固定にするか否かの設定をします

Yes　・・・申請画面内で、1 Year／2 Year／3 Year の選択が可能となります

No　・・・上記の Default Validity Period で設定した有効期間がすべての証明書に適用され、証明書申請時に有効期間の選択をすることができません

「Certificate Revocation」

■　[Subscribers can revoke their certificates]を選択した場合、申請ページの”Revoke”リンクが表示され、申請者はエンドユーザ申請ページから

証明書を Revoke（失効）することができます。

- [Only Administrators can revoke certificates]を選択した場合、申請ページの”Revoke”リンクは表示されず、管理者のみが証明書の Revoke（失効）を行うことができます。

8　申請ページのカスタマイズが終了したら、[Continue]をクリックします。
設定が保存されると、Enrollment Wizard の最後のページが表示されます。このページには、申請者申請ページへのリンクが含まれています（図 3-2）。申請ページには、管理者が変更した点が反映されています。申請ページの右上部分に貴組織のロゴを追加表示したい場合は、コントロールセンターの Logo Wizard を使用してください。

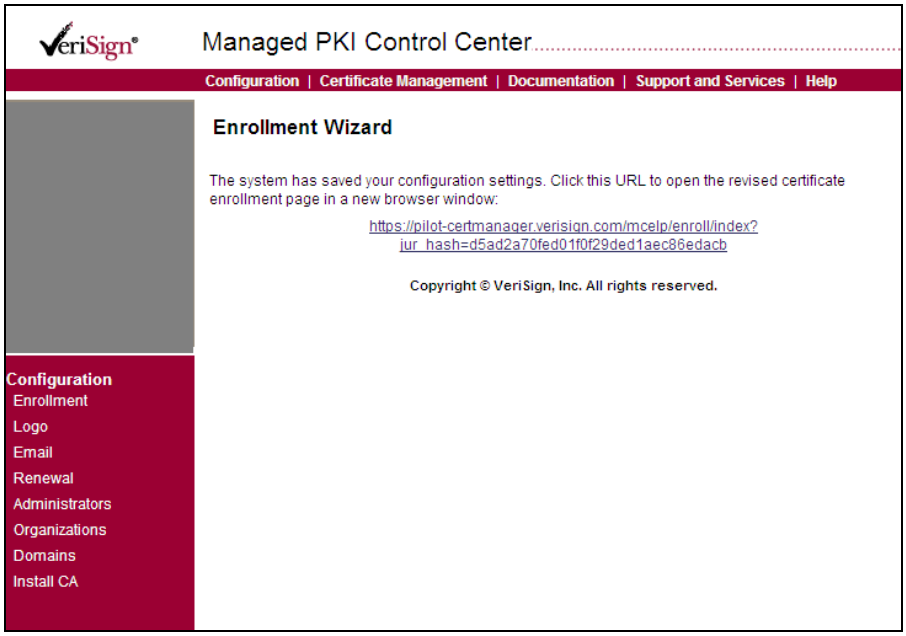

図 3-2 Enrollment Wizard の最後のページ

Enrollment Wizard を再実行することにより、申請ページにさらに変更を加えることもできます。

Step 3　　証明書更新の設定

Renewal Wizard では、申請者のサーバ ID の有効期限が切れる際に送信する更新通知メールの配信時期および更新申請の承認方法を設定することができます。すべてのサーバ ID には有効期間が設定されており、1 年間または 2 年間あるいは 3 年間のいずれかです。

一般に、申請者には、電子メールによって新しいサーバ ID の申請と取得を行う URL が記載された更新通知が送られます。また、セキュリティを高めるために、申請者の更新プロセスにステップを追加することができます。

1　コントロールセンターの[Configuration]ページにある[Renewal]リンクをクリックして、Renewal Wizard を起動します。

2　Renewal Wizard ページの設定をします。

a　Specify the Authentication Mode for Certificate Renewal Requests
（更新承認有無の指定）

申請者の更新要求として[Instant Issue]もしくは[Manual Approval]を選択します。

－[Instant Issue]（即時発行）－申請者が元のサーバ ID のチャレンジフレーズと証明書署名要求（CSR）を入力すると、更新されたサーバ ID が自動的に発行されます。一致が認められなかった場合は、新規と同じく管理者による承認待ちの状態になり、発行には管理者による承認が必要です。

－[Manual Approval]（手動承認）－管理者がすべてのサーバ ID 更新要求に対する認証、および承認を行います。

b　Specify the Renewal Notice Period（更新通知期間の指定）

サーバ ID の更新通知を送信する時期を指定します。デフォルトは[1 Week]です（これをオフにすることはできません）。[1 Week]に加えて、[2 Weeks]、[3 Weeks]、 [1 Month]および[2 Months]を選択することもできます。

※少なくとも[1 Month]にはチェックすることをお勧めします。

ベリサイン マネージドPKI for SSL の設定の完了

ベリサイン マネージド PKI for SSL の設定が終了し、使用する準備ができました。ベリサイン マネージド PKI for SSL の設定はいつでも変更できます。

Step 4　　サーバ ID の要求

ベリサイン マネージド PKI for SSL の設定が終わったら、サーバ ID を申請して、設定を確認してみてください。サーバ ID を申請することによって、申請ページの設定を確認して、申請者が実際に行う操作を理解できます。

※テストモードが特別用意されているわけではございません。通常の申請を行い、設定が反映されているかご確認いただく事となります。

1　[Certificate Management]ページの[Subscriber Services]リンクをクリックして、サブスクライバーサービスページの URL にアクセスします。

2　[証明書の選択]からサーバ ID のタイプを選び[進む]をクリックします。

3　申請ページに入力して送信し、サーバ ID を要求します。

Step 5　サーバ ID 要求の承認

申請したサーバIDに対し、その要求を承認します。サーバIDを承認することによって、証明書の認証設定を確認できます。これらは、管理者が申請者のサーバID要求を承認するときと同じステップです。申請者の要求を承認する際の詳しい手順については、28 ページの「証明書要求の処理」を参照してください。

サーバ ID 要求を承認するには：

1　コントロールセンターの[Certificate Management]ページで[Process Requests]をクリックします。[Process Requests]ページには、すべてのサーバ ID 要求が表示されます。

2　サーバ ID 要求を承認するには、[Approve]をクリックします。コントロールセンターは要求をベリサインに送信し、ベリサインでサーバ ID が生成されます。要求の確認メールが届き、その後、2 通目のメールとして、サーバ ID を含んだ電子メールが届きます。

3　電子メールに記載されている説明に従って、サーバ ID をウェブサーバにインストールします。インストール手順については、各サーバベンダから提供されているマニュアルを参照してください。

コントロールセンターの概要

コントロールセンターは、組織のベリサイン マネージド PKI サービスの管理において管理者が行うすべての業務へのインターフェースです。コントロールセンターの各ページには、プロセスに沿ったオンラインヘルプ(英語)が含まれています。コントロールセンターは、管理者の責任を反映した以下のような構成になっています。これらのリンクは、コントロールセンターの上部ナビゲーションバーにあります。

- **Configuration**：ベリサイン マネージド PKI for SSL サービスの設定とカスタマイズを行うためのウィザード
- **Certificate Management**：サーバ ID 申請の承認と拒否、失効と再発行、その他の証明書管理業務など、申請者のサーバ ID を管理するページ
- **Documentation/Support and Services/Help**：本機能はご利用いただけません。

  追加管理者、サーバID、ドメインの追加を希望される場合は、日本ベリサイン営業担当（mpki-ssl@verisign.co.jp）までご連絡ください。

Configuration

[Configuration]ページには、ベリサイン マネージド PKI for SSL を設定、カスタマイズするための設定ウィザードへのリンクがあります。ウィザードにアクセスするには、左のフレームにある[Configuration]リストからウィザードを選択します。

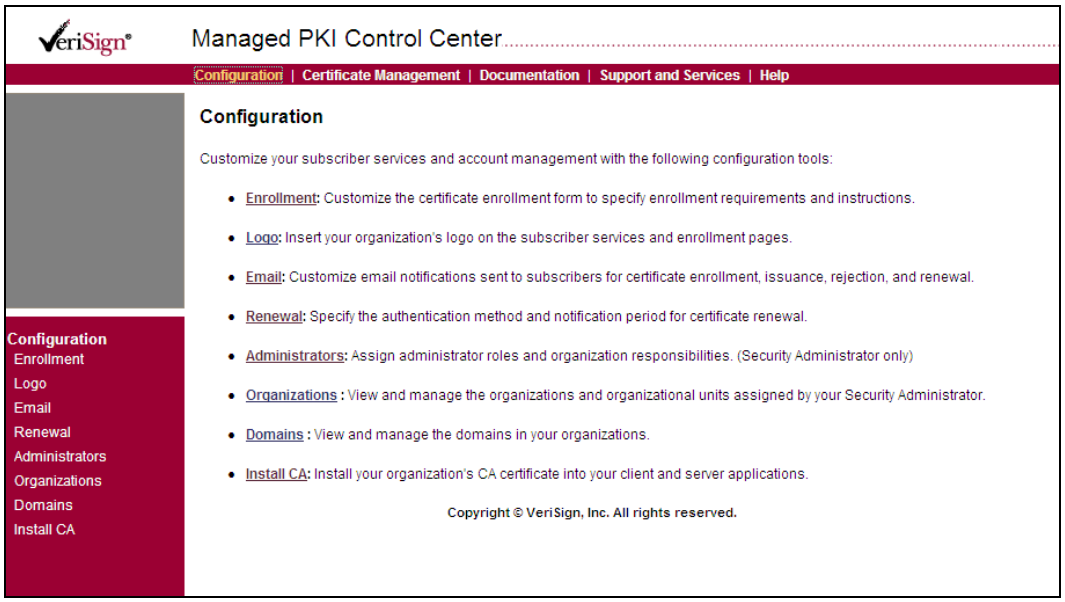

図 3-3 サーバ ID の[Configuration]ページ

Enrollment Wizard

[Enrollment]リンクをクリックすると、Enrollment Wizard を実行して、申請ページに含める情報を指定することによって、申請者ページをカスタマイズできます。Enrollment Wizard には以下のステップが表示されます。これらの詳しい説明は、14～18 ページにあります。

- 「Select Certificate Types to Offer」では、申請ページから申請者が選択できるサーバ ID の種類を設定します。
- 「Enter the Email Address for Technical Support」では、申請者がサーバ ID と証明書ライフサイクル機能に関する質問を送信する送信先の電子メールアドレスを入力します。
- 「Customize Account Name」では、申請ページに表示したいアカウント名をカスタマイズします。
- 「Customize Subscriber Instructions」では、申請ページに表示したい注釈を入力します。
- 「Select language」では、申請ページに表示したい言語を選択します。

- 「Customize Enrollment Requirements」オプションもしくは必須フィールドを選択／追加することによって、申請者のサーバ ID 申請ページをカスタマイズします。
- 「Customize Certificate Lifecycle Options」では、申請者のサーバ ID のデフォルト有効期限を設定します。またオプションを選択することにより、申請者が証明書申請時にサーバ ID の有効期間を変更できるようにします。

Logo Wizard

Logo Wizard を使用すると、貴組織のロゴを申請者の申請ページに追加表示することができます。追加する組織のロゴを選択するには、[Use my logo]を選択して、[参照]ボタンを使用して、申請ページに表示したい.gif ファイルを開きます。

E-mail Wizard

E-mail Wizard を使用すると、ベリサイン マネージド PKI for SSL から自動送信される電子メールメッセージ（申請確認、承認、拒否、更新、および失効）の内容や送信先アドレス情報を変更できます。

メッセージ文を編集するときは、以下のガイドラインを参照してください。

- 行は自動的に折り返されないので、各行末で改行を挿入する必要があります。
- $$variable_name$$として示されるテキストは、メッセージ受信者の個人情報を表します。たとえば、$$NAME$$フィールドは申請者の名前を表し、これによってメッセージを特定の個人向けにできます。この目的以外では、メッセージ内で 2 つのドル記号（$$）を使用しないでください。
- メッセージには特殊な書式設定を含めないでください。電子メールは ASCII（プレーンテキスト）形式で申請者に送信されるので、書式設定は失われます。

Renewal Wizard

Renewal Wizard を使用すると、申請者のサーバ ID の有効期限が切れる際に送信する更新通知メールの配信時期と、更新申請に対する承認方法を設定できます。

ここでは、以下を設定します。

- サーバ ID の更新申請の承認方法
- 更新通知を送信する時期

Administrators

Administrators を使用すると、複数のベリサイン マネージド PKI for SSL 管理者に管理責任や各ウィザードへのアクセス権限を割り当てたり削除したりすることができます。適切なベリサイン マネージド PKI for SSL 管理者の[View Edit]をクリックします。割り当てる、もしくは削除する管理者の権限を選択して、[Save]をクリックします。表 3-1 に、管理者のタイプと権限を示します。

追加のベリサイン マネージドPKI for SSL管理者を任命する方法については、6 ページの「ベリサイン マネージドPKI for SSL管理者の追加任命」を参照してください。なお、ここでチェックを全て外すと“Read-Only”権限になります。

表 3-1 ベリサイン マネージド PKI for SSL 管理者のタイプと権限

管理者タイプ	許される業務	ウィザードへのアクセス
Security Administrator	他の管理者への権限（管理者権限とウィザードアクセス）の割り当て。	すべての管理者機能
Configuration Administrator	ベリサイン マネージドPKI for SSLの設定、申請ページの内容の指定、データベースおよびレポート機能の管理。	Logo、E-mail、Renewal、およびEnrollment
Certificate Management Administrator	サーバID要求の承認と拒否、サーバIDの失効、他の管理者への要求の割り当て、証明書ライフサイクルの管理。認証プロセスを容易にするために、Certificate Management Administrator権限を特定のグループの申請者を知っている管理者に割り当てることもできます。	なし
EV Certificate Management Administrator	EV証明書申請の承認と拒否、証明書の失効、他の管理者への要求の割り当て、および証明書ライフサイクルの管理。	なし
Read-only	現在の要求、証明書データ、およびログファイルの表示。管理者変更および追加管理者発行時にはデフォルトで当権限が割り当てられます（※）。	なし

※ Read-onlyの管理者に権限を付与するには、ベリサインへ依頼ください。
メールアドレス：server-onsite@verisign.co.jp

Organizations

本機能はご利用いただけません。

Domains

認証局にて登録しているドメイン名を確認いただけます。

※ [Delete Domains][Change EV Status][Add Domains]のボタンは日本ベリサインではご利用いただけません。

※ 誤って「Delete Domain」ボタン押下された場合、利用可能なドメインが削除されてしまいますのでご注意ください。

Install CA

中間 CA 証明書または Root CA 証明書がこちらからダウンロード可能です。

※こちらのリンクは日本で提供している全てのサービスに対応しておりません。以下の日本ベリサインの Web サイトから必要な中間 CA 証明書を入手いただけますようお願いいたします。

https://www.verisign.co.jp/repository/intermediate.html

Certificate Management

[Certificate Management]ページ（図 3-4）には、管理者業務を行うためのリンクがあります。 [Bookmark the Managed PKI Control Center]をクリックすると、管理者画面にブックマークをつけることができます。

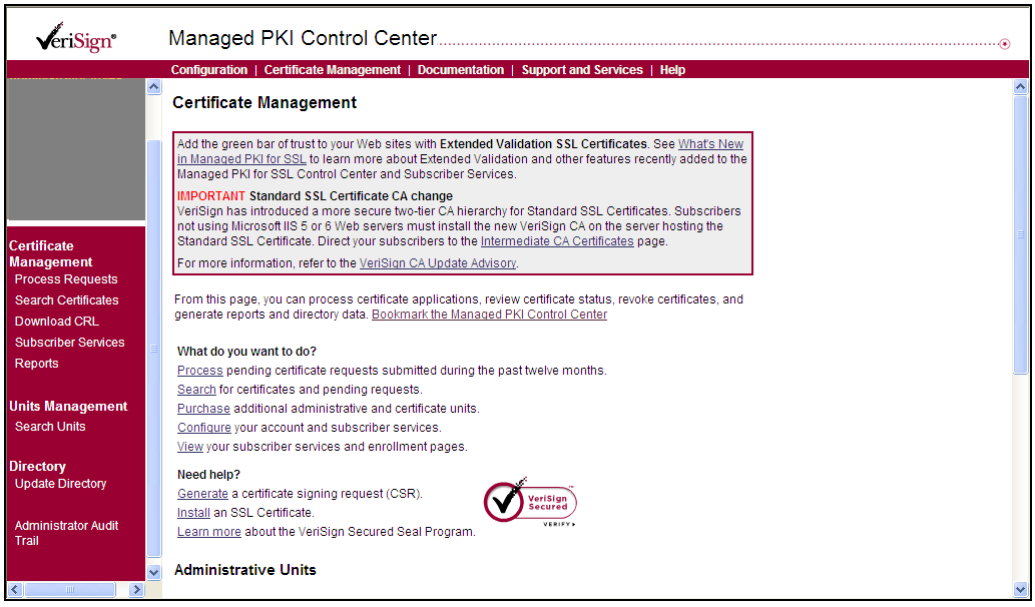

図 3-4 [Certificate Management]ページ

[Certificate Management]ページのオプション

[Certificate Management]ページには、以下のオプションがあります。サーバIDの管理の詳しい手順については、第 4 章「管理者IDとサーバIDの管理」を参照してください。

- **[Process Requests]**は、まだ承認／拒否されていないすべてのサーバ ID 要求のリストを表示します。割り当てられていない要求、もしくは管理者に割り当てられた要求だけがリストに表示されます。要求ごとの申請情報を確認して、要件を満たしているかどうかを判断し、承認／拒否することができます。
- **[Search Certificates]**をクリックすると、特定の期間について、証明書の要求および証明書をサーバ ID データベースから検索できます。申請者の名前、電子メールアドレス、サーバ ID シリアル番号、Organization、Organizational Unit、サーバ ID の種類、要求が割り当てられた管理者、証明書のステータスもしくは証明書の発行日によって検索できます。このオプションを使用すると、証明書情報の確認、証明書の再発行、失効、管理者の割り当て、チャレンジフレーズの変更および証明書の監査証跡の表示ができます。
- **[Download CRL]**をクリックすると、失効したサーバ ID のシリアル番号のリスト（証明書失効リスト、CRL）をダウンロードすることができます。ベリサインは CRL にデジタル署名して、管理者が内容の完全性と真正性を確認できるようにしています。ベリサインは、標準 CRL サービスを毎日夜間に更新しています。
- **[Subscriber Services]**には、サブスクライバーサービスページへのリンクがあります。この URL をユーザに通知してください。
- **[Reports]**では、ベリサイン マネージド PKI for SSL サービスのステータスとアクティビティに関するさまざまなレポートを要求できます。
- **[Unit Management [Search Units]**には、管理者証明書、ドメイン名およびサーバ ID の申請数、使用済みの数、残数が表示されています。Administrative Units の表は日本ベリサインでは使用しておりません。
- **[Directory[Update Directory]**をクリックすると、新規申請者のリストをダウンロードして、組織のディレクトリサーバにインポートできます。
- **[Administrator Audit Trail]**をクリックすると、管理者によって実行された重要な操作を表示できます。指定した管理者と期間の監査証跡が表示されます。

Documentation

[Documentation]ページには、ベリサインからダウンロードできるドキュメントへのリンクがあります。本機能は日本ベリサインではご利用頂けません。

以下の日本ベリサインの Web サイト（管理者用 FAQ）からマニュアル等のドキュメントをダウンロードいただけます。

https://support.verisign.co.jp/ssl/faq/indexa.html

※アクセスには管理者証明書が必要となります。

Support and Services

サポート窓口のコンタクト情報が記載されています。
[Support and Service]以下のメニュー機能はご利用いただけません。

ライセンスの追加申請およびドメイン名の追加申請の際は、ベリサイン営業担当（mpki-ssl@verisign.co.jp）までご連絡ください。

Help

[Help]リンクをクリックすると、ベリサイン マネージド PKI for SSL のオンラインヘルプシステム(英語)が開きますが、本機能は日本ベリサインではご利用頂けません。

第4章　管理者IDとサーバIDの管理

この章では、コントロールセンターを使用して、証明書要求の承認と拒否など、通常の証明書管理業務を行う方法を説明します。コントロールセンターにはレポート機能もあり、承認／拒否された申請、発行／失効されたサーバ ID など、管理者証明書とサーバ ID アクティビティの履歴を表示することができます。

サーバID要求の認証

管理者は、サーバ ID を要求している各主体の実在性を検証する責任があります。申請者とウェブサイトの実在を検証して、申請データの正確さを確認できたら、証明書要求を承認することができます。要求者の実在を検証し、申請フォームに入力された情報が正しいことを確認するプロセスを「認証」といいます。一般に、組織が従業員に関して以前から保持している情報（従業員の雇用や ID バッジの発行に使用された情報など）だけで、証明書申請者が証明書の申請を許可されるための検証要件の大部分が満たされます。ただし、管理者が承認するのはサーバ ID 要求なので、発行される証明書の対象となるウェブサーバが組織の公認サイトであることも確認する必要があります。管理者は、サーバ ID 申請者認証プロセスを規定した厳格な手順、すなわちベリサイン認証局運用規定（CPS）に従わなければなりません。ベリサイン CPS のコピーは、下記のベリサイン ウェブサイトから入手できます。

http://www.verisign.co.jp/repository/CPS/index.html

証明書要求の処理

証明書要求を承認／拒否するには、コントロールセンターにアクセスします（14 ページの「コントロールセンターへのアクセス」を参照してください）。コントロールセンターの[Certificate Management]ページから、各要求を表示して、申請情報の詳細を確認し、サーバID要求を承認／拒否できます。これらの業務が、管理者の主要な仕事です。

要求の処理

[Certificate Management]ページの[Process Requests]リンクをクリックすると、まだ承認／拒否されていないすべての証明書要求のリストが表示されます（図 4-1 参照）。どの管理

者にも割り当てられていない要求、もしくは自分に割り当てられた要求だけがリストに表示されます。ベリサインの CPS に従って、各要求を承認するか拒否するかを判断します。これは、申請者に対するサーバ ID の発行を承認する際に、管理者としての責任を確実に果たすための有効な方法です。

注 [Process Requests]は、Certificate Management もしくは Security Administrator の権限を持つ管理者だけが使用できます。 （23 ページの「表 3-1 ベリサイン マネージド PKI for SSL 管理者のタイプと権限」を参照してください。）

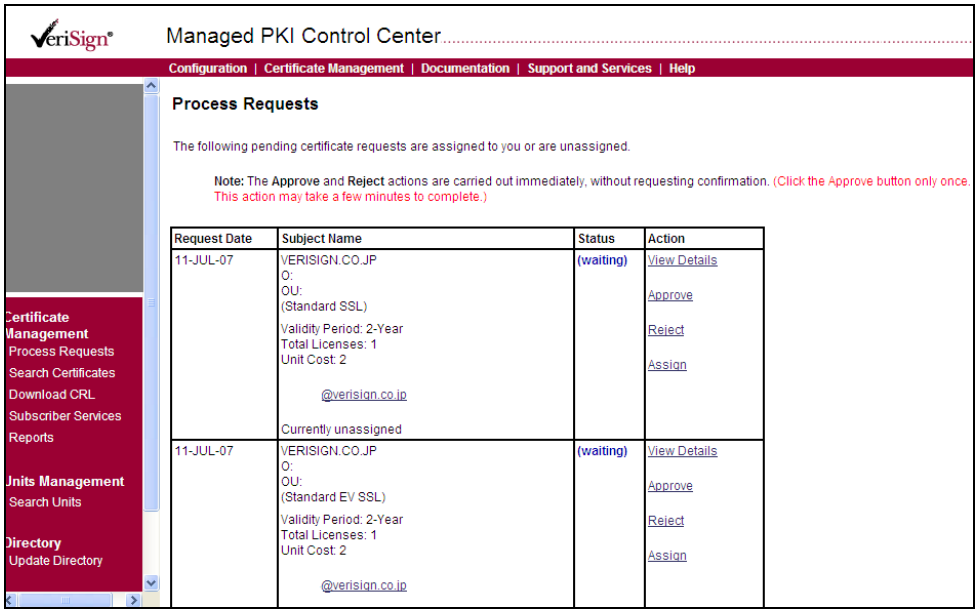

図 4-1 [Process Requests]ページ

[Request Date]

[Process Requests]ページの[Request Date]列には、証明書の申請日付が表示されます。

[Subject Name]

[Subject Name]列には、証明書保有者に対応する情報が表示されます。この列には、コモンネーム、Organization 名、Organizational Unit 名、証明書のタイプ、証明書の有効年数、ライセンス使用数、ユニット使用数、申請者の電子メールアドレス、この証明書要求に割り当てられた管理者が含まれます（どの管理者にも割り当てられていない要求、もしくは自分に割り当てられた要求だけがリストに表示されます)。

[Status]

[Status]列には、証明書のステータスが表示されます。保留中の証明書（まだ処理されて

いない証明書要求）の場合、「waiting」と表示されます。

[Actions]

[Process Requests]ページの[Action]列では、以下の操作ができます。

- [View Details] : [View Details]をクリックすると、証明書申請者によって入力された申請情報がすべて表示されます。この情報が正確であり、組織の CPS に準拠しているかどうかをチェックしてください。

  - この画面から、監査記録用に証明書にコメントを付けたり、コメントを申請者に送信することができます。
  - 証明書要求を検証するには、申請者の本人性と、証明書が発行されるコモンネームが組織の公認サイトであることを確認してください。また、証明書に記載されるその他の情報が正確であることを確認してください。

    情報が確認できたら、[Approve]をクリックしてサーバ ID 要求を承認します。要求は管理者の秘密鍵を使用して署名されて、ベリサインに送信されます。ベリサインで証明書が生成され、署名され、ベリサイン証明書リポジトリに入力されます。

    ベリサインは、証明書を含んだ電子メールメッセージを申請者（もしくは E-mail Wizard で指定された受信者）に送信します。証明書申請者は証明書をウェブサーバにインストールして使用します。

    ベリサインセキュアドシールは、申請者のオンラインカスタマーに対して、ウェブサイトの運営主体が合法的な実在の存在であり、サイトとの通信が SSL 暗号化によって保護されることを保証します。ベリサインセキュアドシールプログラムの詳細については、下記のページをご覧ください。

    http://www.verisign.co.jp/securesite/sitelist.html

注 申請フォームにタイプミスやその他の間違いがあった場合は、要求を拒否して、新しい要求を提出するように申請者に依頼してください。これにより、証明書情報の正確さが保証されます。

- **[Approve]** : 証明書を確認せずに、要求を直ちに承認するには、[Approve]をクリックします。このアクションは、[View Details]リンクの[Approve]機能と同じです。
- **[Reject]** : サーバ ID 要求を検証できなかった場合は、要求を拒否しなければなりません。要求を拒否するには、[Reject]をクリックします。その後、電子メールメッセージが申請者に送信されます。以下の理由が 1 つ以上ある場合は、要求を拒否できます。

- 申請者が CPS 要件を満たしていない場合
- 要求に情報が不足している場合
- 不正な要求であると確信した場合
- 申請情報に間違いがある場合
- 証明書を要求しているウェブサイトが組織の公認サイトでない場合

■ **[Assign]**：[Assign]機能を使用して、特定の要求を特定のベリサイン マネージド PKI for SSL 管理者に割り当てることによって、組織のワークフローを管理できます。[Assign]をクリックすると、[Review Assignment]ページが表示されます（図 4-2 参照）。ベリサイン マネージド PKI for SSL 管理者を選択して、[Assign]をクリックします。そのベリサイン マネージド PKI for SSL 管理者が[Process Requests]もしくは[View Requests]をクリックすると、その管理者に割り当てられたすべての要求が表示されます。

注 Certificate Management Administrator 以上の権限を持つ管理者でなければ、他のベリサイン マネージド PKI for SSL 管理者に要求を割り当てることはできません。

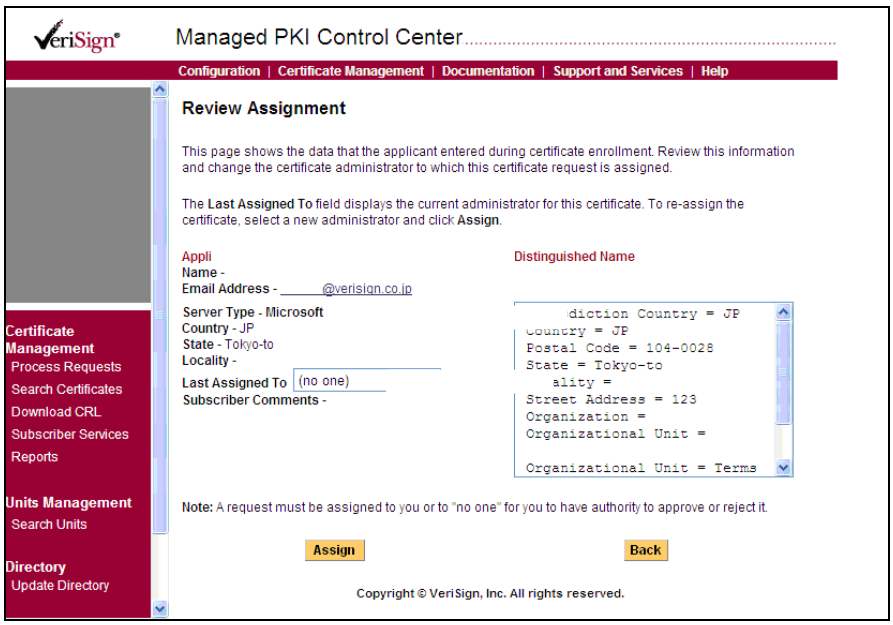

図 4-2 別のベリサイン マネージド PKI for SSL 管理者への要求の割り当て

証明書および証明書の要求の検索

[Certificate Management]ページの[Search Certificates]リンクをクリックすると、特定のサーバ ID を検索できます。検索条件に一致する証明書のリストがコントロールセンターに

表示されたら、申請情報と証明書の詳細を確認したり、証明書の監査証跡を確認したり、証明書を再発行することができます。

検索条件には、コモンネーム、電子メールアドレス、証明書のシリアル番号、Organization 名、Organizational Unit 名、サーバ ID の種類、この証明書要求に割り当てられた管理者を指定できます。証明書が承認された日付の範囲や、表示したい証明書のタイプを以下から指定することもできます。

- All Requests and Certificates（すべての要求および証明書）
- Pending Requests（承認されていない保留中の要求）
- Approved Requests（承認された要求）※日本ベリサインでは使用しておりません。
- Valid Certificates（有効な証明書）
- Revoked Certificates（失効された証明書）
- Expired Certificates（期限切れの証明書）
- Deactivated Certificates（無効化された証明書）
- Expired in 30 days (from today)（30 日以内に期限が切れる証明書）
- Expired in 60 days (from today)（60 日以内に期限が切れる証明書）
- Expired in 90 days (from today)（90 日以内に期限が切れる証明書）

図 4-3 に、有効な証明書の検索結果の例を示します。

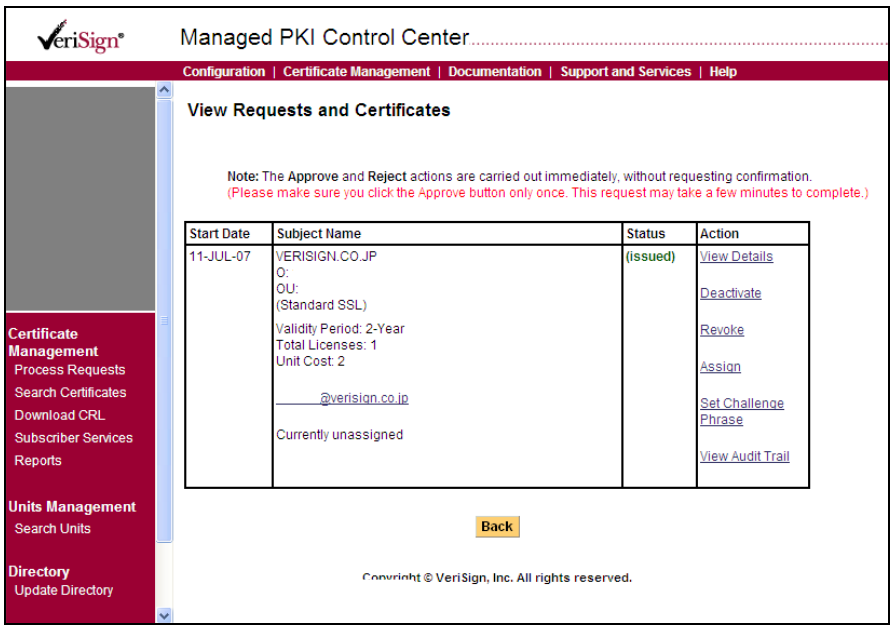

図 4-3 [View Requests and Certificates]ページの検索結果

注 他の管理者によって承認されたサーバ ID もリストに表示されます。

検索結果として表示される[View Requests and Certificates]ページでは、以下のアクションを実行できます。これらのアクションは、Certificate Management Administrator 以上の権限を割り当てられた管理者だけが実行できます。

- **[View Details]**をクリックすると、証明書申請者によって入力された申請情報と証明書データがすべて表示されます。

  必要な場合は、電子メールアドレス、氏名、役職、従業員 ID、すべての[Additional Field]など、サーバ ID の担当窓口情報を編集できます。

- **[Deactivate]**をクリックすると、証明書を無効化することができます。無効化された証明書は CRL に追加されません。無効化処理は、申請者が証明書を紛失した場合、または何らかの理由で証明書を利用できない場合、不要となった場合など、セキュリティ上の問題以外の理由でのみ行ってください。

- **[Revoke]**をクリックすると、証明書を失効し、CRL に追加することができます。証明書の秘密鍵が危殆化したおそれがある場合など、セキュリティ上の問題が発生した場合に失効処理を行ってください。証明書の失効についての詳細は、ベリサイン CPS の第 9 章を参照してください。

  http://www.verisign.co.jp/repository/CPS/index.html

- **[Assign]**をクリックすると、特定の要求を特定のベリサイン マネージド PKI for SSL 管理者に割り当てることによって、組織のワークフローを管理できます。この機能の詳細については 31 ページの「Assign」を参照してください。

- **[Set Challenge Phrase]**をクリックすると、申請者が元のチャレンジフレーズを忘れた場合に、新しいチャレンジフレーズを上書きすることができます。

- **[View Audit Trail]**をクリックすると、サーバIDに対して記録されたすべてのアクションが表示されます。これには、申請、承認／拒否、失効、割り当てなどのアクションが含まれます。この機能の詳細については、38 ページの「管理者監査証跡（Administrator Audit Trail）リンク」を参照してください。

CRLのダウンロード

[Certificate Management]ページの[Download CRL]リンクをクリックすると、失効された証明書のシリアル番号のリストをダウンロードすることができます。このようなリストは、証明書失効リスト（CRL）と呼ばれます。ベリサインは CRL にデジタル署名して、管理

者が内容の完全性と真正性を確認できるようにしています。ベリサインは、標準 CRL サービスを毎日夜間に更新しています。

ブラウザは CRL を自動的にチェックして、通信相手のサイトもしくはデバイスのサーバ ID の有効性を確認します（ブラウザがそのように設定されていた場合。詳しくは、ブラウザのドキュメントを参照してください）。

サブスクライバーサービスの管理

[Certificate Management]ページの[Subscriber Services]リンクは、管理者が申請者および申請者に提供できるサブスクライバーサービスページへのリンクになっています。申請者は、以下の操作を行う際、サブスクライバーサービスページを使用します。

- サーバ ID の申請

  申請者は、管理者が Enrollment Wizard で作成した[ベリサイン マネージド PKI for SSL 証明書発行サービス]ページに入力して送信します。

- サーバ ID の再発行

  申請者は、秘密鍵が壊れたりして使用できない状態になっている際に、ライセンス数の消費なしに、サーバ ID を再発行することができます。ただし、同一 DN（Distinguished Name、同一の証明書の件名＝同一のサーバ名）のサーバ ID のみ再発行可能となります。

  注　有効期間は変更できません。再発行後の証明書の満了日はオリジナルのものと同一になります。

- サーバ ID の更新

  申請者は、サーバ ID を有効期限の 3 ヶ月前から更新でき、その場合も現在の証明書の有効期間が短縮されることはありません。

- サーバ ID の失効

  申請者は、他人が自分の秘密鍵のコピーを入手したと思われる場合や、証明書が不正利用されたと思われる場合には、サーバ ID を失効することができます。申請者が自分の証明書を失効すると、Revoked Certificate レポートで管理者に通知されます。

  申請者が失効を要求するには、まず、名前、電子メールアドレス、もしくはシリアル番号を入力して、証明書を検索し、次に、証明書のチャレンジフレーズを入力します。

  ※　サブスクライバーページに「サーバ ID の失効」を表示させるためには、管理者

画面[Configuration]ページの[Enrollment] Wizard の一番下の[Certificate Revocation]オプションで[Subscribers can revoke their certificates]オプションにチェックが入っている必要があります。

- サーバ ID の検索

  申請者は、サーバ ID を電子メールアドレス、もしくはコモンネームによって検索できます

- 登録済みドメイン名の表示

  申請者はこのページを使用して、管理者がベリサイン マネージド PKI for SSL に登録したドメイン名のリストを表示できます。

レポートの管理

[Certificate Management]ページの[Reports]リンクをクリックすると、証明書要求、証明書、および監査証跡レコードに関するレポートを動的に照会し、表示できます。レポートは、「詳細(Detail)」、「要約(Summary)」、および「証明書枚数(Units)」の 3 種類を出力することができます。詳細レポートには、証明書要求と証明書の現在のステータスリストが含まれます。要約レポートには、詳細レポートにリストされた証明書要求に関する集約情報が含まれます。また、証明書枚数レポートには、発行された証明書の枚数や種類が含まれます。レポート生成は、管理者がレポート生成ページの送信ボタンをクリックしたときに開始される非同期サービスです。正常に完了すると、レポートをダウンロードするための URL を含んだ電子メールが指定された電子メールアドレスに送信されます。

証明書サービスのステータスと作業に関するレポートを要求してダウンロードするには、[Reports]リンクをクリックします。受信するレポートのタイプ（詳細もしくは要約）を選択します。レポートは、申請され発行された証明書の確認、管理者の作業の確認、および内部監査に役立ちます。図 4-4 に、詳細レポートの書式と内容の例を示します。図 4-5 に、要約レポートの書式と内容の例を示します。

注 レポートには、特定のイベントのみが含まれます。監査証跡とサーバ ID のディレクトリを定期的に確認して、申請者に発行したサーバ ID を管理してください。

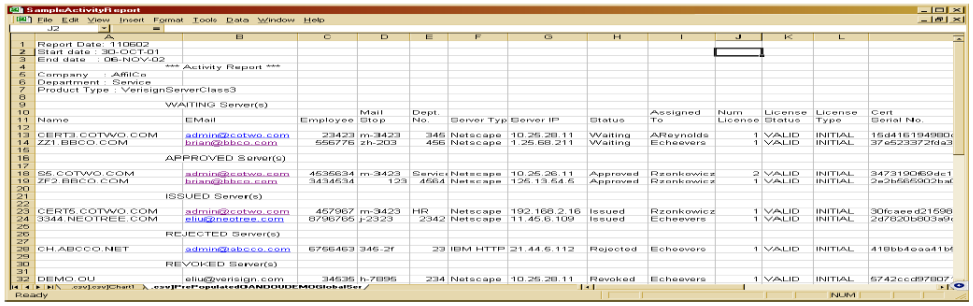

図 4-4 詳細レポート

```
Report Date: 011501
Start date : 01-JAN-01
End date   : 01-JAN-01
                    ***Activity Summary Report***

Company   : Class3-02
Department : Test
Product Type : VeriSignServerClass3



Number Issued:          3
Number Enrolled:        0
Number Rejected:        0
Number Revoked:         0
```

図 4-5 要約レポート

組織のディレクトリの更新

ベリサイン マネージド PKI for SSL は、管理者が承認したすべてのサーバ ID のリポジトリを保持します。このデータから、システムは証明書ディレクトリデータファイル（LDAP Data Interchange Format）を準備します。これを組織のディレクトリサーバにインポートできます。ディレクトリサーバを使用して、サーバ ID 申請者に関する最新情報を組織全体で容易に共有できます。

LDAPディレクトリファイルのダウンロード

ベリサイン マネージド PKI for SSL は、Lightweight Directory Access Protocol（LDAP）ディレクトリサービス標準をサポートしています。ベリサインは、LDAP Data Interchange Format（LDIF）でディレクトリファイルを提供します。LDIF ディレクトリファイルを使用すると、LDAP 標準に準拠している任意のディレクトリサービスに証明書情報をエクスポートできます（ディレクトリツリー構造に合わせてディレクトリファイルを構成しな

ければならない場合があります。詳しくは、ディレクトリのドキュメントを参照してください)。

[Certificate Management]ページの[Update Directory]リンクをクリックすると、LDIF 形式のディレクトリファイルの更新およびダウンロードができます。ディレクトリ生成は、管理者が[Update Directory]ページの送信ボタンをクリックしたときに開始される非同期サービスです。正常に完了すると、ディレクトリファイルをダウンロードするための URL を含んだ電子メールが指定された電子メールアドレスに送信されます。

ディレクトリデータを取得するには：

1　[Update Directory]リンクをクリックします。[Update Directory]ページが表示されます（図 4-6）。

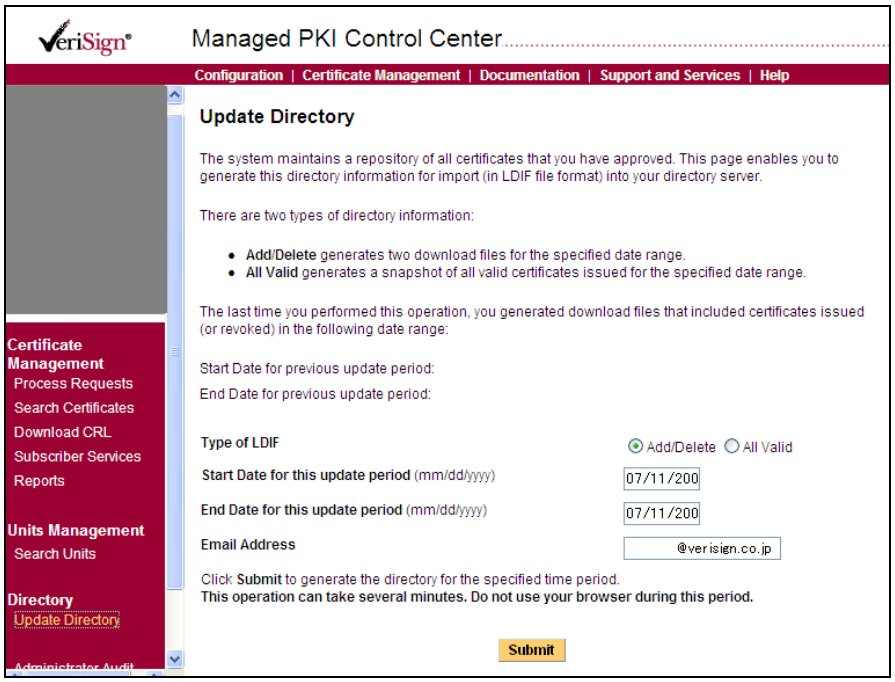

図 4-6 [Update Directory]ページ

2　以下のダウンロードファイル形式の 1 つを選択します。

- [Add/Delete]を選択すると、指定した期間の 2 種類のダウンロードファイルが表示されます。
  - Format A には、有効な発行された証明書がすべて含まれます。
  - Format D には、削除された（一般には失効された）すべての証明書が含まれます。

  [All Valid]を選択すると、特定の日付の範囲に発行されたすべての有効な証明書のスナップショットが表示されます。

3　[Start Date]および[End Date]フィールドに日付の範囲を入力して、[Email Address]フィールドに電子メールアドレスを入力した後、[Submit]をクリックします。

4 ファイルの準備ができると、入力した電子メールアドレスに通知メールが送信されます。電子メールに記載されている説明に従って、ディレクトリファイルをダウンロードして、ディレクトリサーバにインポートしてください（サーバには、これらのファイルをインポートするためのディレクトリがあります)。

管理者監査証跡(Administrator Audit Trail)リンク

[Certificate Management]ページの[Administrator Audit Trail]リンクをクリックすると、以下のアクションの日付、時刻（GMT)、担当した管理者名など、管理者に関連するすべてのイベントのアクティビティログファイルが表示されます。

- サーバ ID 要求の承認／拒否
- 有効な証明書の失効／再発行
- Enrollment Wizard の変更
- 管理者に追加、変更、もしくは削除された管理者権限

特定の管理者の名前によって検索したり、日付の範囲によって検索を絞り込んだりすることができます。指定した管理者と期間の監査証跡が表示されます。

注 [Administrator Audit Trail]機能では、管理者証明書によって管理者を識別します。期限切れもしくは失効された管理者の監査証跡が必要な場合もあるので、これらの管理者証明書はコントロールセンターから削除されません（ただし、管理者がこれらの証明書を使用してコントロールセンターにアクセスすることはできなくなります)。[Search by Administrator :]フィールドには、管理者証明書が有効でない場合、そのステータスが表示されます。

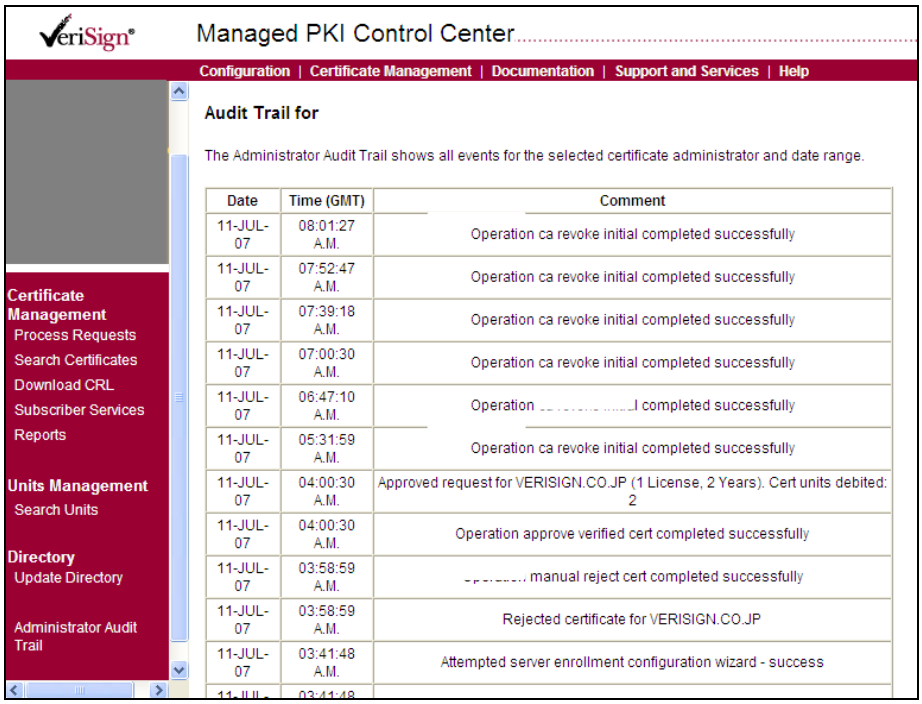

図 4-7 Administrator Audit Trail ログファイル

証明書監査証跡

[Search Certificates]の検索結果として表示される[View Requests and Valid Certificates]ページの[View Audit Trail]リンクをクリックすると、その証明書に関連するすべてのイベントのアクティビティログファイルが表示されます。ログには、以下の作業の日付、時刻（GMT）、および担当管理者と、その作業について管理者によって追加されたコメントが含まれます。

- 別の管理者へのサーバ ID 要求の割り当て
- サーバ ID 要求の承認／拒否
- サーバ ID の失効／再発行

証明書監査証跡には、証明書申請の要求日時と証明書の発行日時も示されます。

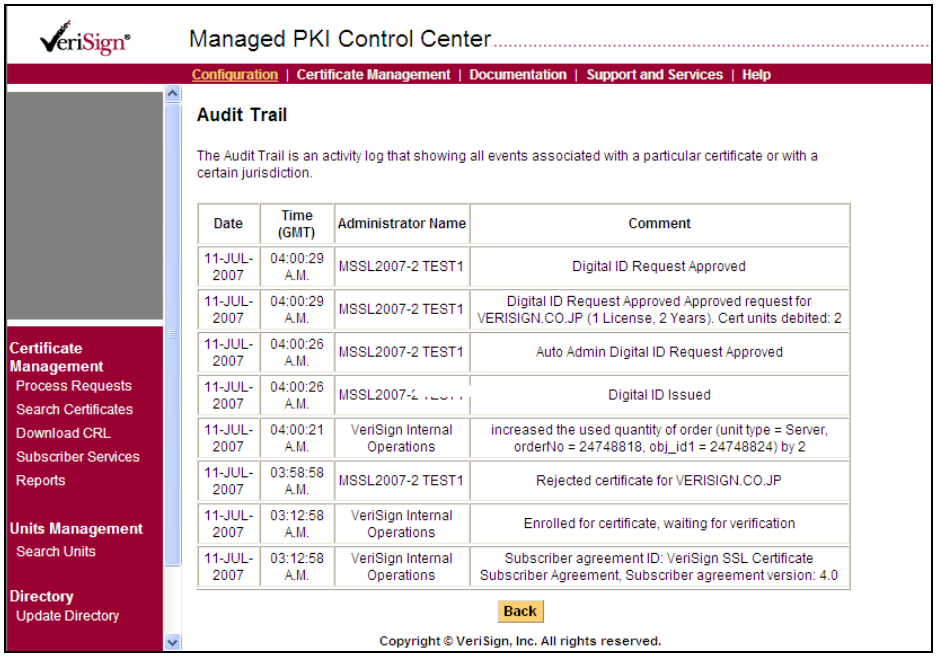

図 4-8 [Certificate Audit Trail]ページ

証明書有効性チェックへの応答

ベリサイン マネージド PKI for SSL 管理者だけでなく、ルータ、ウェブサーバ、電子メール受信者などのネットワークデバイスやアプリケーションの利用者も、次のような方法でサーバ ID の有効性（有効、期限切れ、失効）をチェックできます。

- 証明書失効リスト（CRL）
- ウェブクエリ（ベリサインの[Digital ID Center]ページで検索）
- コントロールセンター

ネットワークデバイスやアプリケーションの利用者もしくは管理者が受け取る応答は、有効性をチェックする方法によって異なります。表 4-1 に、証明書有効性ステータスの要求に対して、一時停止されている証明書がどのように表示されるかを示します。

表 4-1　証明書有効性要求への応答

証明書のステータス	CRL	ウェブクエリ	コントロールセンター
Valid（有効）	表示されない	Valid	issued
Expired（期限切れ）	表示されない	Expired	Expired
Revoked （失効）	Revoked	Revoked	Revoked

サーバIDの更新

管理者の証明書管理業務には、サーバ ID とベリサイン マネージド PKI for SSL サービスの更新が含まれます。

サーバIDの更新

セキュリティ対策として、すべてのサーバ ID には有効期限が定められています。有効期限が過ぎると、申請者はその証明書を使用できなくなります。ベリサイン マネージド PKI for SSL では、申請者は期限切れになる前にサーバ ID を更新することができ、その場合も、現在の証明書の有効期間が短縮されることはありません。更新されたサーバ ID は、発行日から有効になります。

Renewal Wizard を使用すると、申請者に新しいサーバ ID を申請するように通知する更新通知メールの配信時期と更新申請に対する承認方法を設定できます。更新通知メールのデフォルトの配信時期は、有効期限の 1 週間前です。

管理者証明書とベリサイン マネージドPKI for SSLの更新

コントロールセンターにアクセスするには、管理者証明書とベリサイン マネージド PKI for SSL サービスが有効でなければなりません。管理者証明書やベリサイン マネージド PKI for SSL を中断することなく使い続けるには、期限切れ前に更新する必要があります。

注 ベリサインは、ベリサイン マネージド PKI for SSL の有効期限の 1 ヶ月前に、管理者に通知メールを送信します。

ベリサイン マネージドPKI for SSL管理者証明書の更新

ベリサイン マネージドPKI for SSLサービスの更新については、ベリサイン営業担当（mpki-ssl@verisign.co.jp）までご連絡ください。