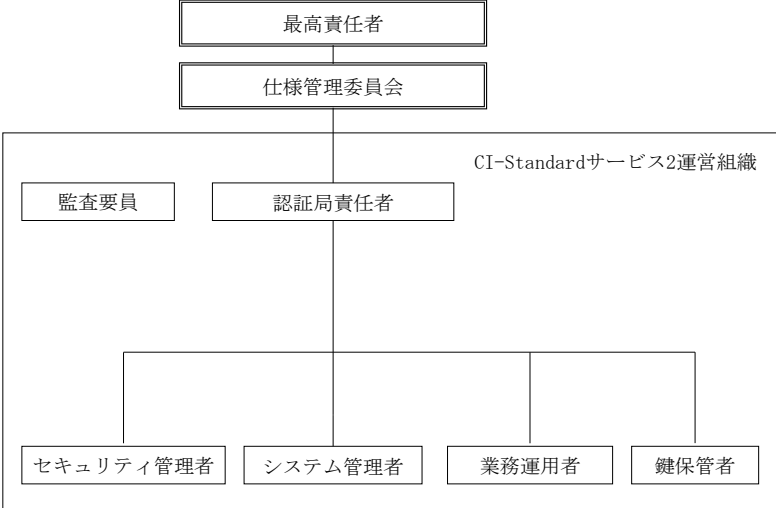
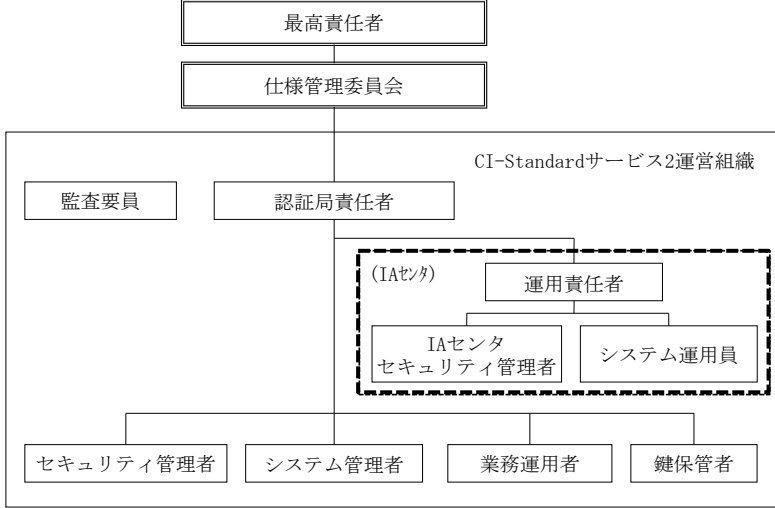


CI-Standardサービス2運用規程 新旧対照表

(破線、下線部分は変更部分)

変更 (Ver1.60)	現行 (Ver1.50)
<p>1.3 運営体制と証明書^{の適用範囲}</p> <p>図1-1 CI-Standardサービス2の運営体</p>  <pre> graph TD A[最高責任者] --> B[仕様管理委員会] B --> C[CI-Standardサービス2運営組織] C --> D[監査要員] C --> E[認証局責任者] E --> F[セキュリティ管理者] E --> G[システム管理者] E --> H[業務運用者] E --> I[鍵保管者] </pre>	<p>1.3 運営体制と証明書^{の適用範囲}</p> <p>図1-1 CI-Standardサービス2の運営体制</p>  <pre> graph TD A[最高責任者] --> B[仕様管理委員会] B --> C[CI-Standardサービス2運営組織] C --> D[監査要員] C --> E[認証局責任者] E --> F[運用責任者] F --> G[IAセンターセキュリティ管理者] F --> H[システム運用員] E --> I[セキュリティ管理者] E --> J[システム管理者] E --> K[業務運用者] E --> L[鍵保管者] </pre>

CI-Standardサービス2運用規程 新旧対照表

(破線、下線部分は変更部分)

変更 (Ver1.60)	現行 (Ver1.50)																																														
<p>1.3 運営体制と証明書の適用範囲</p> <p style="text-align: center;">表 1-1 組織・職務とその役割</p> <table border="1"> <thead> <tr> <th>組織・職務</th> <th>業務・役割</th> </tr> </thead> <tbody> <tr> <td>最高責任者</td> <td>業務運用に関わる責任者の任命</td> </tr> <tr> <td>仕様管理委員会</td> <td>各種規程類の仕様変更時における妥当性の検討 危殆化、および災害時等の緊急時対応方針の検討</td> </tr> <tr> <td>認証局責任者</td> <td>本サービスの遂行に関する責任</td> </tr> <tr> <td>セキュリティ管理者</td> <td>認証局各施設の物理的セキュリティおよび同監査に関する責任 秘密情報の管理 アーカイブデータの管理</td> </tr> <tr> <td>システム管理者</td> <td>情報基盤の構築と維持 認証局運営上のシステム等の開発・運用・保守</td> </tr> <tr> <td>業務運用者 A</td> <td>タイプ A において、業務運用者 D に対する帯同と証明書の発行支援および失効支援 タイプ B において、証明書の申込受付、審査、発行、失効 CA の判断に基づく証明書の失効</td> </tr> <tr> <td>業務運用者 D</td> <td>タイプ A において、証明書の申込受付、審査、発行、失効</td> </tr> <tr> <td>鍵保管者</td> <td>電子証明書署名鍵をバックアップした USB メモリの保管</td> </tr> <tr> <td>監査要員</td> <td>定期監査</td> </tr> </tbody> </table>	組織・職務	業務・役割	最高責任者	業務運用に関わる責任者の任命	仕様管理委員会	各種規程類の仕様変更時における妥当性の検討 危殆化、および災害時等の緊急時対応方針の検討	認証局責任者	本サービスの遂行に関する責任	セキュリティ管理者	認証局各施設の物理的セキュリティおよび同監査に関する責任 秘密情報の管理 アーカイブデータの管理	システム管理者	情報基盤の構築と維持 認証局運営上のシステム等の開発・運用・保守	業務運用者 A	タイプ A において、業務運用者 D に対する帯同と証明書の発行支援および失効支援 タイプ B において、証明書の申込受付、審査、発行、失効 CA の判断に基づく証明書の失効	業務運用者 D	タイプ A において、証明書の申込受付、審査、発行、失効	鍵保管者	電子証明書署名鍵をバックアップした USB メモリの保管	監査要員	定期監査	<p>1.3 運営体制と証明書の適用範囲</p> <p style="text-align: center;">表 1-1 組織・職務とその役割</p> <table border="1"> <thead> <tr> <th>組織・職務</th> <th>業務・役割</th> </tr> </thead> <tbody> <tr> <td>最高責任者</td> <td>業務運用に関わる責任者の任命</td> </tr> <tr> <td>仕様管理委員会</td> <td>各種規程類の仕様変更時における妥当性の検討 危殆化、および災害時等の緊急時対応方針の検討</td> </tr> <tr> <td>認証局責任者</td> <td>本サービスの遂行に関する責任者</td> </tr> <tr> <td>セキュリティ管理者</td> <td>認証局各施設の物理的セキュリティおよび同監査に関する責任者 秘密情報の管理者 アーカイブデータの管理者</td> </tr> <tr> <td>システム管理者</td> <td>情報基盤の構築と維持 認証局運営上のシステム等の開発・運用・保守</td> </tr> <tr> <td>業務運用者 A</td> <td>タイプ A において、業務運用者 D に対する帯同と証明書の発行支援および失効支援 タイプ B において、証明書の申込受付、審査、発行、失効 CA の判断に基づく証明書の失効</td> </tr> <tr> <td>業務運用者 D</td> <td>タイプ A において、証明書の申込受付、審査、発行、失効</td> </tr> <tr> <td>鍵保管者</td> <td>電子証明書署名鍵をバックアップした USB メモリの保管</td> </tr> <tr> <td>監査要員</td> <td>定期監査</td> </tr> <tr> <td>運用責任者</td> <td>IA センタ運用における責任者</td> </tr> <tr> <td>IA センタ セキュリティ管理者</td> <td>IA センタのシステム操作権限の管理</td> </tr> <tr> <td>システム運用員</td> <td>IA センタのシステム操作権限の登録、削除 IA センタの設備の保守</td> </tr> </tbody> </table>	組織・職務	業務・役割	最高責任者	業務運用に関わる責任者の任命	仕様管理委員会	各種規程類の仕様変更時における妥当性の検討 危殆化、および災害時等の緊急時対応方針の検討	認証局責任者	本サービスの遂行に関する責任者	セキュリティ管理者	認証局各施設の物理的セキュリティおよび同監査に関する責任者 秘密情報の管理者 アーカイブデータの管理者	システム管理者	情報基盤の構築と維持 認証局運営上のシステム等の開発・運用・保守	業務運用者 A	タイプ A において、業務運用者 D に対する帯同と証明書の発行支援および失効支援 タイプ B において、証明書の申込受付、審査、発行、失効 CA の判断に基づく証明書の失効	業務運用者 D	タイプ A において、証明書の申込受付、審査、発行、失効	鍵保管者	電子証明書署名鍵をバックアップした USB メモリの保管	監査要員	定期監査	運用責任者	IA センタ運用における責任者	IA センタ セキュリティ管理者	IA センタのシステム操作権限の管理	システム運用員	IA センタのシステム操作権限の登録、削除 IA センタの設備の保守
組織・職務	業務・役割																																														
最高責任者	業務運用に関わる責任者の任命																																														
仕様管理委員会	各種規程類の仕様変更時における妥当性の検討 危殆化、および災害時等の緊急時対応方針の検討																																														
認証局責任者	本サービスの遂行に関する責任																																														
セキュリティ管理者	認証局各施設の物理的セキュリティおよび同監査に関する責任 秘密情報の管理 アーカイブデータの管理																																														
システム管理者	情報基盤の構築と維持 認証局運営上のシステム等の開発・運用・保守																																														
業務運用者 A	タイプ A において、業務運用者 D に対する帯同と証明書の発行支援および失効支援 タイプ B において、証明書の申込受付、審査、発行、失効 CA の判断に基づく証明書の失効																																														
業務運用者 D	タイプ A において、証明書の申込受付、審査、発行、失効																																														
鍵保管者	電子証明書署名鍵をバックアップした USB メモリの保管																																														
監査要員	定期監査																																														
組織・職務	業務・役割																																														
最高責任者	業務運用に関わる責任者の任命																																														
仕様管理委員会	各種規程類の仕様変更時における妥当性の検討 危殆化、および災害時等の緊急時対応方針の検討																																														
認証局責任者	本サービスの遂行に関する責任者																																														
セキュリティ管理者	認証局各施設の物理的セキュリティおよび同監査に関する責任者 秘密情報の管理者 アーカイブデータの管理者																																														
システム管理者	情報基盤の構築と維持 認証局運営上のシステム等の開発・運用・保守																																														
業務運用者 A	タイプ A において、業務運用者 D に対する帯同と証明書の発行支援および失効支援 タイプ B において、証明書の申込受付、審査、発行、失効 CA の判断に基づく証明書の失効																																														
業務運用者 D	タイプ A において、証明書の申込受付、審査、発行、失効																																														
鍵保管者	電子証明書署名鍵をバックアップした USB メモリの保管																																														
監査要員	定期監査																																														
運用責任者	IA センタ運用における責任者																																														
IA センタ セキュリティ管理者	IA センタのシステム操作権限の管理																																														
システム運用員	IA センタのシステム操作権限の登録、削除 IA センタの設備の保守																																														
<p>(2) 本サービス運営組織</p> <p>本サービスにおける認証局は、証明書発行データの登録、審査(内容チェック)を行い、証明書の発行、失効等の運営業務を行う。</p> <p>本サービス運営組織には、認証局責任者、セキュリティ管理者、システム管理者、業務運用者、鍵保管者、保守要員および監査要員を置く。それぞれの権限については、本規程5.2節において規定する。</p> <p>本サービスの運営は、NDNが行う。</p>	<p>(2) 本サービス運営組織</p> <p>本サービスにおける認証局は、証明書発行データの登録、審査(内容チェック)を行い、証明書の発行、失効等の運営業務を行う。</p> <p>本サービス運営組織には、認証局責任者、セキュリティ管理者、システム管理者、業務運用者、鍵保管者、保守要員、<u>運用責任者、IAセンタセキュリティ管理者、システム運用員</u>および監査要員を置く。それぞれの権限については、本規程5.2節において規定する。</p> <p>本サービスの運営は、NDNが行う。</p>																																														

CI-Standardサービス2運用規程 新旧対照表

(破線、下線部分は変更部分)

変更 (Ver1.60)	現行 (Ver1.50)																				
<p>4.2 証明書の発行 本認証局は、本認証局側で生成した利用者の公開鍵に、本認証局の署名を付して利用者証明書を発行する。 なお、証明書発行方式は一括発行方式とし、証明書発行情報ファイルと共に一括化されて登録用端末に出力される。 一括化出力された利用者証明書は、暗号化記録媒体(セキュリティUSBメモリ)に格納し、RA事務室に搬送する。</p>	<p>4.2 証明書の発行 本認証局は、本認証局側で生成した利用者の公開鍵に、本認証局の署名を付して利用者証明書を発行する。 なお、証明書発行方式は一括発行方式とし、証明書発行情報ファイルと共に一括化されて登録用端末に出力される。 一括化出力された利用者証明書は、暗号化記録媒体(<u>セキュリティUSB等</u>)に格納し、RA事務室に搬送する。</p>																				
<p>5.2 手続面の管理 証明書の発行、更新、失効等の重要な業務の実施に当たっては、要員の職務権限を分離し、相互牽制を行う。 重要な業務の指示は、最高責任者が本認証局責任者に対して行い、本認証局責任者は各要員に指示する。各要員がシステム操作を行う際、システムは、操作員が正当な権限者であることの識別、認証を行う。 各要員別権限を表5-1に定義する。</p>	<p>5.2 手続面の管理 証明書の発行、更新、失効等の重要な業務の実施に当たっては、要員の職務権限を分離し、相互牽制を行う。 重要な業務の指示は、最高責任者が本認証局責任者に対して行い、本認証局責任者は各要員に指示する。各要員がシステム操作を行う際、システムは、操作員が正当な権限者であることの識別、認証を行う。 各要員別権限を表5-1、<u>5-2</u>に定義する。</p>																				
<p>5.2 手続面の管理 表5-2(削除)</p>	<p>5.2 手続面の管理</p> <p style="text-align: center;">表 5-2 認証設備室要員別権限</p> <table border="1" data-bbox="1240 855 2038 1283"> <thead> <tr> <th>要員区分</th> <th>指名</th> <th>入室権限</th> <th>操作権限</th> <th>入室権限についてのアクセス権限チェック方式</th> </tr> </thead> <tbody> <tr> <td>運用責任者</td> <td>最高責任者</td> <td>なし</td> <td>なし</td> <td>—</td> </tr> <tr> <td>IA センタ セキュリティ 管理者</td> <td>運用責任者</td> <td>なし</td> <td>なし</td> <td>—</td> </tr> <tr> <td>システム 運用員</td> <td>運用責任者</td> <td>あり</td> <td>あり</td> <td>・ID カードシステムと生体認証システム</td> </tr> </tbody> </table>	要員区分	指名	入室権限	操作権限	入室権限についてのアクセス権限チェック方式	運用責任者	最高責任者	なし	なし	—	IA センタ セキュリティ 管理者	運用責任者	なし	なし	—	システム 運用員	運用責任者	あり	あり	・ID カードシステムと生体認証システム
要員区分	指名	入室権限	操作権限	入室権限についてのアクセス権限チェック方式																	
運用責任者	最高責任者	なし	なし	—																	
IA センタ セキュリティ 管理者	運用責任者	なし	なし	—																	
システム 運用員	運用責任者	あり	あり	・ID カードシステムと生体認証システム																	

CI-Standardサービス2運用規程 新旧対照表

(破線、下線部分は変更部分)

変更 (Ver1.60)	現行 (Ver1.50)
<p>6.2.9 電子証明書署名鍵を<u>廃棄</u>する方法</p> <p>電子証明書署名鍵の有効期間が満了した場合または電子証明書署名鍵の使用を中止する場合(認証局終了時の処置)は、第三者組織の立会者(認証局責任者が「<u>鍵廃棄立会者指名通知書</u>」により指名した本認証局の要員以外の者)の立会いのもと、システム管理者2人と鍵保管者2人の合議制操作により、CAサーバにおいて電子証明書署名鍵を完全に初期化する。また、電子証明書署名鍵の復元のために保管したUSBメモリも、鍵保管者が合議制操作により完全に初期化する。</p> <p>鍵の<u>廃棄</u>に参加した第三者組織の立会者および鍵保管者は「<u>鍵廃棄の宣誓書</u>」に署名する。</p> <p>なお、電子証明書署名鍵のバックアップを再取得するに伴い、既に保管してあった電子証明書署名鍵を<u>廃棄</u>する場合も本規定を準用する。</p>	<p>6.2.9 電子証明書署名鍵を<u>破壊</u>する方法</p> <p>電子証明書署名鍵の有効期間が満了した場合または電子証明書署名鍵の使用を中止する場合(認証局終了時の処置)は、第三者組織の立会者(認証局責任者が「<u>鍵破壊立会者指名通知書</u>」により指名した本認証局の要員以外の者)の立会いのもと、システム管理者2人と鍵保管者2人の合議制操作により、CAサーバにおいて電子証明書署名鍵を完全に初期化する。また、電子証明書署名鍵の復元のために保管したUSBメモリも、鍵保管者が合議制操作により完全に初期化する。</p> <p>鍵の<u>破壊</u>に参加した第三者組織の立会者および鍵保管者は「<u>鍵破壊の宣誓書</u>」に署名する。</p> <p>なお、電子証明書署名鍵のバックアップを再取得するに伴い、既に保管してあった電子証明書署名鍵を<u>破壊</u>する場合も本規定を準用する。</p>