繁体字版

地方公共團體的官方個人認證服務

北海道認證局 運用章程

Ver. 1．5

2013 年 7 月 8 日

北海道

修訂過程

Ver	日期	修訂內容
1.0	2004 年 1 月 29 日	首版發行
1.1	2005 年 1 月 19 日	因更改實施規則改版
1.2	2006 年 11 月 1 日	因修正法律改版
1.3	2008 年 9 月 19 日	因認證局私密金鑰更新改版
1.4	2009 年 4 月 1 日	因聯繫地址變更改版
1.5	2013 年 7 月 8 日	因實施部分修正過的住民基本台帳法(平成 21 年(法律第 77 號)改版

1. 前言

本運用章程，針對北海道的官方個人認證服務下屬在都道府縣各個認證局（以下稱為「北海道 CA」），為發行住民基本台帳上有記錄的居民的電子憑證等（使用人的證明書以下稱「電子憑證」。），制定其有關認證業務的營運方針，旨在將居民與國家或地方公共團體的機關等之間的申請・登記等手續實現電子化。

此外，本運用章程的構架遵循了 IETF(Internet Engineering Task Force)中的 PKIX(Public-Key Infrastructure X.509) Working Group 的 RFC(Request For Comments) 2527 「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」。然而參照其它章程的部分只保留了標題，參照內容有所注明。

1-1 概要

北海道 CA，針對北海道範圍內的，市町村住民基本台帳上有記錄的居民，根據其申請不僅發行電子憑證，和其他北海道 CA 運行時必要的證明書，而且針對其它官方個人認證服務，即在各都道府縣下屬認證局，或政府認證的基層認證局等為進行相互認證而設置的官方個人認證服務過渡認證局(以下稱「個人認證 BCA」)，北海道 CA 還發行相互認證證明書與其進行互換。尚且，制訂失效資訊（有關電子憑證失效的資訊。以下同。）、失效記錄（CRL/ARL）（記載有關電子憑證等失效資訊。以下同），失效資訊文件（稱失效記錄（CRL）存檔。以下同），以及針對「涉及數位簽章的地方公共團體認證業務相關法律」（以下稱「根據法」。）的第 17 條第 4 項規定的驗證簽名者，或者該條第 6 項規定的驗證團體簽名者的要求，給以提供服務。

此外，北海道 CA 將本運用章程確定為關於北海道 CA 的認證業務運營方針，不獨立執行 CP（證明書政策）以及 CPS（認證實施章程）。

1-2 識別

北海道 CA 的證明書政策編號如下所示。

北海道 CA 電子憑證等政策

電子憑證政策以及北海道 CA 相互認證證明書政策

1.2.392.200149.8.5.1.1.10

試驗用電子憑證政策以及北海道 CA 相互認證證明書政策

1.2.392.200149.8.5.1.0.10

官職證明書驗證伺服器證明書政策

1.2.392.200149.8.5.1.200

試驗用官職證明書驗證伺服器證明書政策

1.2.392.200149.8.5.1.0.200

OCSP 回應器證明書政策

1.2.392.200149.8.5.1.300

試驗用 OCSP 回應器證明書政策

1.2.392.200149.8.5.1.0.300

1-3 運用體制與證明書的適用範圍

1-3-1 參與者

(1) 總務大臣

總務大臣依據根據法，向指定認證機關下達指示。

(2) 官方個人認證服務都道府縣協議會

官方個人認證服務都道府縣協議會（以下稱「協議會」。），履行聯繫及調整關於官方個人認證系統實現一元化營運的重要事項關聯事務。

(3) 北海道知事

北海道知事，將以下所示的北海道 CA（北海道認證局）機能予以整備。

(4) 北海道 CA

北海道 CA，與市町村長相互配合・協作，履行發行電子憑證和其它證明書，制訂失效記錄（CRL/ARL），提供確認電子憑證的有效性方法等證明書發行・失效資訊管理業務。同時履行北海道知事的私密金鑰面臨危險或發生災害時的緊急應對。

此外，針對使用人在國家或地方公共團體所接收的網上文件，給予提供為驗證數位簽章所需要的的官職以及職責證明書的有效性確認方法。

(5) 個人認證 BCA

個人認證 BCA，依照協議會制定的運用章程，履行與北海道 CA 等在各都道府縣下屬認證局，以及政府認證的基層過渡認證局（以下稱「政府認證基層 BCA」。）等相互認證時使用的證明書等的發行業務。

(6) 指定認證機關

指定認證機關，依據根據法的規定，受北海道知事委託，履行有關實施認證業務的事務（以下稱「認證事務」）。

(7) 市町村長

北海道範圍內的市町村長，在受理電子憑證的發行申請以及失效申請後，履行申請人的本人核實，向申請人交付北海道 CA 發行的電子憑證等職責。

(8) 申請人 / 使用人

申請人，即依據根據法第 3 條 1 項的規定，申請發行電子憑證的人。（也可由代理人申請。但這種情況需符合「涉及數位簽章的地方公共團體認證業務相關法律實施規則」（以下稱「根據法規則」。 ）第 5 條規定。）。使用人，即住民基本台帳上有記錄，接受電子憑證發行的人。

使用人，通過與國家或地方公共團體的機關等之間的網上申請・登記，可以利用電子憑證。針對北海道知事或指定認證機關，可要求公開與自己相關的認證業務資訊(指電子憑證的發行記錄，失效資訊及失效資訊文件。以下同)。對所公開的認證業務資訊，可要求更改，添加或刪除其全部或一部分內容。此外，針對認證事務等有所不服時，根據行政不服審查法，可以向總務大臣提出審查請求。同時，針對使用人在國家或地方公共團體的機關所接收的網上公函，對驗證數位簽章所需要的的官職以及職責證明書的有效性加以確認。

(9) 驗證簽名者

指以下機關或人員中，為接受確認電子憑證有效性方法的提供，依據根據法第 17 條第 1 項規定事先呈報並被賦予訪問權限的人。

① 利用資訊通信技術履行行政手續的相關法律第 2 條第 2 號所規定的行政機關等(以下稱「行政機關等」)。
② 法院
③ 行政機關遵照法律規定所指定，登錄或者認可的人，即根據針對行政機關等的申請、呈報或其它手續所伴隨的必要事項，以電磁方式接受提供，並向行政機關等自行將其提供，或回應其查詢業務者。
④「數位簽章及認證業務之相關法律」（以下稱「數位簽章法」。）第 8 條規定的認可認證企業。
⑤ 由總務大臣認可的，履行數位簽章法第 2 條第 3 項規定的特定認證業務，符合「涉及數位簽章的地方公共團體認證業務相關法律實施令」（以下稱「根據法的政令」。）規定標準的人。
⑥ 按照根據法的政令決定的，針對行政機關等或法院的申請、呈報或其它手續所需要的電磁記錄予以提供的團體。

通過北海道 CA 所提供的失效記錄（CRL/ARL）等，接受其提供的用以確認電子憑證有效性的方法，驗證使用人在網上的申請・呈報等相關的數位簽章。

(10) 確認簽名者

指基於根據法第 17 條第 5 項規定，按照根據法的政令決定的人員。

接受如下決定的驗證團體簽名者提供的，電子憑證的有效性確認結果，驗證使用人在網上的申請・呈報等相關的數位簽章。

(11) 驗證團體簽名者

指以下人員中，為接受確認電子憑證有效性方法的提供，依據根據法第 17 條第 5 項規定事先呈報並被賦予訪問權限的人。

① 按照根據法的政令決定的，基於法律規定而受他人委託，履行向行政機關等以及法院提出申請，呈報或其他手續的人，其所屬團體。
② 按照根據法的政令決定的，針對行政機關等或法院的申請、呈報或其它手續所需要的電磁記錄予以提供的人，其所屬團體或機關。

通過北海道 CA 所提供的失效記錄（CRL/ARL）等，接受其提供的用以確認電子憑證有效性的方法，然後針對收到確認簽名者回信的使用人通過網上申請・呈報等所傳送電子憑證附件，確認其有效性，將結果向確認簽名者做出回答。

(12) 驗證簽名者等

指驗證簽名者以及驗證團體簽名者。

1-3-2 適用性・適用環境等

服務類型及用途如以下 4 項所示。

① 基於以下用途給予發行電子憑證。
- 行政機關等及法院的網上申請・呈報手續相關的數位簽章
- 驗證簽名者等履行本人核實
- 確認簽名者履行本人核實

此外，電子憑證的有效期限為自電子憑證發行日起算 3 年。

② 基於以下用途給予發行相互認證證明書。
- 通過個人認證 BCA，與政府認證基層 BCA 等的相互認證

此外，相互認證證明書的有效期限為自相互認證證明書發行日起算 5 年。

③ 基於以下用途給予發行官職證明書驗證伺服器證明書。
- 針對使用人在國家或地方公共團體網上接收的公函，為驗證數位簽章所需要的官職證明書或職責證明書的有效性，提供確認方法。

此外，官職證明書驗證伺服器證明書的有效期限，為自官職證明書驗證伺服器證明書的有效日起算 1 年。

④ 基於以下用途給予發行 OCSP 回應器證明書。
- 驗證簽名者等通過 OCSP 回應器查詢方法，提供電子憑證的有效性確認方法。

此外，OCSP 回應器證明書的有效期限為自 OCSP 回應器證明書有效日起算 1 年。

1-3-3 運用章程的負責人

本運用章程的負責人為北海道知事。

1-3-4 聯繫地址

有關本運用章程查詢窗口如下所示。

北海道
住 址：地址 060-8588 北海道札幌市中央區北 3 條西 6 丁目
部 門：綜合政策部科學和 IT 促進局信息政策課
受理時間： 上午 8 點 45 分～下午 5 點 30 分
電 話：011-204-5171
傳 真：011-232-3962
電子郵箱地址：sogo.joho2@pref.hokkaido.lg,jp

2．一般規定

2-1 義務

2-1-1 總務大臣的義務

(1)指定認證機關的指定、停止廢止的批准、解除指定、向北海道知事的通知或公開
(2)監督指定認證機關時必要的命令
(3)針對指定認證機關要求必要的彙報以及實施入內檢查
(4)指定認證機關的幹部選任或免職許可及免職命令
(5)指定認證機關制定的認證事務管理章程以及項目計劃的認可及更改命令
(6)針對指定認證機關作出的處罰等相關的不服陳情給以應對
(7)制定伴隨認證業務事宜的設施等的技術標準
(8)涉及認證業務的技術評估相關的調查、研究
(9)認定驗證簽名者所涉及的事務
(10)要求驗證簽名者等針對業務進展狀況作必要的彙報
(11)向使用人告知、宣傳有關官方個人認證服務的資訊

2-1-2 北海道知事的義務

(1)基於市町村長針對申請人的姓名・出生年月日・性別・住址（以下稱「基本 4 資料（申請人為外國籍居民時，在其住民票上記載該外國籍居民的通稱的情況下，則需基本 4 資料及通稱。以下同。 ）」以及公開金鑰的告知，給予發行電子憑證
(2)出示北海道 CA 與個人認證 BCA 之間的相互認證有關的正確資訊以及交換相互認證證明書
(3)發行個人簽名證明書
(4)發行鏈接證明書
(5)發行運行用的關聯證明書
(6)收到使用人的網上失效申請時，進行本人核實及制作失效資訊
(7)制作使用人在市町村窗口進行失效申請的失效資訊
(8)制作因使用人的住址或者姓名變更，以及死亡等事實發生時的失效資訊
(9)當發現使用人的電子憑證的相關證明項目與該電子憑證的記錄有出入時，制作失效資訊。
(10)北海道知事的私密金鑰處於危險時（指因私密金鑰丟失、洩露等無法管理、或者已持有懷疑時。以下同），制作出自該私密金鑰發行的所有證明書的失效資訊以及向個人認證 BCA 的彙報。
(11)向驗證簽名者提供電子憑證有效性的確認方法（指使用 OCSP 協議來回答失效資訊查詢的方法（以下稱「OCSP 回應器查詢方法」。）和失效記錄（CRL/ARL）提供方法）
(12)向使用人提供確認國家或地方公共團體的官職或職責證明書有效性的方法
(13)制作和公佈失效資訊以及失效資訊文件的提供狀況報告
(14)針對認證業務資訊的公開請求給以公開
(15)針對認證業務資訊的更正請求等給以更正
(16)北海道知事金鑰對的設置與私密金鑰的安全管理
(17)實施監查、根據監查結果進行改善等
(18)設置實施認證業務設備
(19)依照本運用章程實施有關各種證明書的發行、更新以及失效業務
(20)針對發行完畢的所有證明書以及失效記錄（CRL/ARL）在必要期間內給以保管，並且，針對各證明書的發行、更新以及失效相關的監察日誌及保管資訊給以必要期間內的保管
(21)隨時確定系統的運轉監測正常進行，以 24 小時穩定運行為目標

(22)有效期為 72 小時的失效記錄（CRL/ARL）相關的失效資訊，每 24 小時發行一次
(23)應對使用人的投訴及諮詢
(24)向指定認證機關委託認證事務以及向總務大臣彙報、公開
(25)向指定認證機關通知有關變動等的失效資訊
(26)根據需要向指定認證機關下達指示
(27)要求指定認證機關作必要的彙報以及實施入內檢查
(28)解除指定認證機關的委託以及向總務大臣彙報、公開
(29)針對指定認證機關所設定的電子憑證發行手續費以及提供資訊手續費給以批准
(30)實施有關與指定認證機關的認證事務費用協議並交付
(31)指定認證機關停止或廢止認證事務時，進行認證事務的實施
(32)與驗證簽名者簽定協議
(33)要求驗證簽名者針對業務實施情況做出必要的彙報
(34)對認證業務相關的資訊進行適當管理
(35)做好認證業務資訊的保密工作
(36)向使用人告知、宣傳有關官方個人認證服務的資訊
(37)制訂及確定本運用章程

2-1-3 市町村長的義務

(1)實施發行時或失效時的申請人，以及失效申請人的本人核實(是否存在，是否為本人)
(2)確認代理申請人為真正代理人
(3)針對失效申請，確認失效事項
(4)確認其他申請手續的妥當處理
(5)提供設置具有適當強度金鑰對的裝置（設置使用人的金鑰對裝置，以下稱「金鑰對產生器」。）
(6)向北海道知事通知申請人的基本 4 資料及申請人的公開金鑰
(7)向北海道知事通知失效申請
(8)向使用人交付電子憑證以及北海道知事的個人簽名證明書
(9)向申請人・使用人說明電子憑證的使用目的的限制，以及有關不正當使用時的懲罰條例
(10)做好金鑰對產生器、受理窗口的終端機等系統的保養・安全管理
(11)應對監察以及根據監察結果進行改善
(12)妥當處理認證業務的相關資訊
(13)做好認證業務資訊的保密工作
(14)向申請人徵收發行電子憑證的發行手續費
(15)受理認證業務資訊的公開要求以及更正要求
(16)按照使用人的申請進行密碼初始化、解鎖（指作為防止濫用措施，5 次以上密碼輸入錯誤時 IC 卡無法使用這一狀態的解除）、消除金鑰對等
(17)幫助使用人取得使用人終端機用的使用人客戶軟體（使用電子憑證必需的軟體）
(18)應對使用人的投訴及諮詢
(19)向使用人告知、宣傳有關官方個人認證服務的資訊

2-1-4 指定認證機關的義務

(1)受北海道知事的委託，實施認證事務（實施本運用章程「2-1-2 北海道知事的義務」中從(1)到(13)、(16)以及(18)到(22)）
(2)制定認證事務管理章程
(3)制訂項目計劃及收支預算並提交項目報告及收支結算報告
(4)設置認證業務資訊保護委員會

(5)妥當處理認證業務相關的資訊
(6)做好認證業務資訊的保密工作
(7)針對認證業務資訊的公開請求給以公開
(8)針對認證業務資訊的更正請求等給以更正
(9)應對使用人的投訴及諮詢
(10)向驗證簽名者等徵收資訊提供手續費

2-1-5 使用人的義務

(1)在電子憑證的發行申請書、失效申請書等上記載正確的內容
(2)做好私密金鑰以及儲存該私密金鑰的 IC 卡的安全管理
(3)定期更改且安全管理用來啟動儲存在 IC 卡裡的私密金鑰的密碼
(4)私密金鑰處於危險時立即申請失效
(5)電子憑證禁止使用於其他目的
(6)繳納發行手續費

2-1-6 驗證簽名者的義務

(1)利用北海道 CA 發行的電子憑證，驗證所附的數位簽章
(2)驗證北海道 CA 發行的電子憑證（該電子憑證是否為北海道知事所發行、該電子憑證是否已失效）
(3)通過驗證使用人的網上申請・呈報等所執行的數位簽章，來進行使用人的認證，除此之外的目的則禁止使用電子憑證
(4)接受失效資訊及失效資訊文件的提供時，與北海道知事簽訂合約
(5)接受並實施總務大臣以及北海道知事的彙報要求
(6)做好失效資訊等的保密工作並妥善使用
(7)確保失效資訊等的安全
(8)繳納資訊提供手續費

2-1-7 驗證團體簽名者的義務

(1)確認北海道 CA 發行的電子憑證尚未失效
(2)通過驗證從驗證簽名者那裡取得的有關使用人的數位簽章，來進行使用人的認證，除此之外的目的則禁止使用電子憑證
(3)接受失效資訊及失效資訊文件的提供時，與北海道知事簽訂合約
(4)接受並實施總務大臣以及北海道知事的彙報要求
(5)做好失效資訊等的保密工作並妥善使用
(6)確保失效資訊等的安全
(7)繳納資訊提供手續費

2-1-8 確認簽名者的義務

(1)利用北海道 CA 發行的電子憑證，驗證所附的數位簽章
(2)驗證北海道 CA 發行的電子憑證（該電子憑證是否為北海道知事所發行、該電子憑證是否已失效）
(3)通過驗證使用人的網上申請・呈報等所執行的數位簽章，來進行使用人的認證，除此之外的目的則禁止使用電子憑證
(4)對從驗證團體簽名者得到的答覆給以保密並妥善使用
(5)確保從驗證團體簽名者得到答覆的安全

2-1-9 資訊儲藏庫的義務

北海道 CA 制作失效記錄（CRL/ARL）之後，將其公開于資訊儲藏庫，以使驗證簽名者等可確認電子憑證的有效性。

此外，保管其他資訊並公開。

2-2 責任

2-2-1 總務大臣的責任

總務大臣，遵照根據法的規定，肩負進行指定認證機關的指定，管理・監督指定認證機關實施安全並妥當的認證事務的責任。

2-2-2 北海道知事的責任

北海道知事，針對使用人及驗證簽名者等，在履行發行電子憑證、相互認證證明書、個人簽名證明書、鏈接證明書、其他業務上所需證明書以及制作涉及這些證明書的失效記錄（CRL/ARL），並提供確認電子憑證以及官職或職責證明書有效性的方法等業務時，需遵照本運用章程妥當執行業務。

此外，在委託指定認證機關執行認證業務時，肩負管理・監督指定認證機關實施安全並妥當的認證事務的責任。

2-2-3 市町村長的責任

市町村長，在履行發行電子憑證、受理失效申請及本人核實等業務時，需遵照本運用章程妥當執行業務。

2-2-4 指定認證機關的責任

指定認證機關，受北海道知事的委託履行以下的認證事務。針對使用人及驗證簽名者等，在履行發行電子憑證、相互認證證明書、個人簽名證明書、鏈接證明書、其他業務上所需證明書以及制作涉及這些證明書的失效記錄（CRL/ARL），並提供確認電子憑證以及官職或職責證明書有效性的方法等業務時，需遵照本運用章程妥當執行業務。

2-2-5 使用人的責任

使用人，遵照本運用章程利用本服務。

2-2-6 驗證簽名者的責任

驗證簽名者，遵照本運用章程驗證電子憑證。

2-2-7 驗證團體簽名者的責任

驗證團體簽名者，遵照本運用章程確認電子憑證的有效性。

2-2-8 確認簽名者的責任

確認簽名者，遵照本運用章程驗證電子憑證。

2-3 財務上的責任

當毫無理由將責任歸咎于北海道 CA，由此行為產生的損失，北海道知事將不負任何損失賠償責任。

當出於某種原因北海道 CA 需要擔當責任時，北海道知事在法令等規定範圍內實施損害賠償。

2-4 說明與執行

2-4-1 適用法令

遵循根據法和其他相關法令。

2-4-2 服務的分工或合併、運用體制等的變更與告知

營運體制等有變更時, 立即通過以下方法向使用人、驗證簽名者公佈。

・協議會的網站(Web)

・北海道的網站(Web)

此外，指定認證機關更改名稱或者變更主要事務所的所在地時，需向總務大臣及北海道知事呈報。

2-4-3 接受監察命令和彙報工作及入內檢查

在總務大臣下達監察方面必需的，有關執行認證事務的命令時，以及北海道知事下達妥當執行認證事務的指示時，指定認證機關必需接受該命令和指示。

此外，總務大臣及北海道知事要求彙報有關認證事務執行情況或者要求入內檢查時，指定認證機關必需接受該要求。

2-4-4 解決糾紛的手續

有關本運用章程發生的訴訟，所有當事人需將札**幌**地方法院作為一審的專門管轄法院。

2-5 費用

電子憑證的發行、失效資訊及失效資訊文件的提供及認證業務資訊的公開等相關費用，按照根據法的規定來決定。

2-6 公開與資訊儲藏庫

2-6-1 關於北海道 CA 資訊的公開

北海道 CA 將以下資訊公佈于協議會的網站(Web)上。

・根據法及相關法令

・本運用章程

・與北海道 CA 相互認證的 CA 名稱

・與北海道 CA 的相互認證被取消的 CA 名稱

・北海道知事的私密金鑰面臨危險的相關資訊　等

北海道 CA 將以下資訊公佈于官方個人認證服務的資訊儲藏庫上。

・個人簽名證明書

・相互認證證明書

・鏈接證明書

・個人簽名證明書、相互認證證明書、鏈接證明書的失效記錄（ARL）

・使用人的電子憑證等的失效記錄（CRL）

2-6-2 公開頻率

公開資訊的更新頻率如下所示。

・根據法及相關法令和本運用章程等的章程最新版隨時載于網站(Web) 。

・個人簽名證明書、相互認證證明書、鏈接證明書一旦發行・更新則立即公開。
・失效記錄（CRL/ARL）每天更新一次。

2-6-3 公開資訊的訪問限制

遵照根據法及相關法令和本運用章程的章程，不設訪問限制。
此外，針對資訊儲藏庫的以下資訊也不設訪問限制。

・個人簽名證明書
・相互認證證明書
・鏈接證明書
・個人簽名證明書、相互認證證明書、鏈接證明書的失效記錄（ARL）
但對資訊儲藏庫上公開的使用人電子憑證的失效記錄（CRL），實行訪問限制。

2-6-4 資訊儲藏庫相關事項

資訊儲藏庫一天 24 小時，一年 365 天開放使用。但因定期保養，有暫時無法使用的可能。

2-7 執行情況的監察

2-7-1 執行情況的監察頻率

北海道知事實施一年一度的由監察人進行的定期執行情況監察，並且根據需要實施定期監察以外的臨時監察。

2-7-2 監察人的識別與資格

北海道 CA 的監察，由精通監察業務及認證業務者執行。

2-7-3 監察人與被監察部門的關係

北海道知事，選任與北海道 CA 無利害關係的人作為監察人。

2-7-4 監察項目

認證業務遵照根據法及相關法令，且遵照本運用章程來執行，以此作為核心實施監察。

2-7-5 監察結果的處理

監察結果，由監察人以監察報告的形式提交給北海道知事。北海道知事根據情況需要，向各市村町長、指定認證機關告知監察報告。

2-7-6 監察指正事項的應對

指定認證機關確認監察指正事項，根據重要程度或緊急程度實施妥當的應對措施。評估其結果之後，向北海道知事彙報。北海道知事則確認指定認證機關針對監察指正事項所實施的應對措施。

2-8 保密與保護個人資訊

2-8-1 視為機密的資訊與個人資訊的處理

北海道 CA，將因資訊洩露而導致有可能損害北海道 CA 認證業務信譽的資訊視為機密資訊經管。並且妥當保護使用人的個人資訊。

針對包含視為機密的資訊及使用人個人資訊的資訊，決定管理包含該資訊的資料及電磁儲存介質的負責人（按照本運用章程「5-2-1-1 北海道 CA 的工作人員」規定，作為認證局管理負責人），進行安全管理。如果發生個人資訊洩露情況時，根據所定手續另行尋找對策。

2-8-2 無需視為機密的資訊

北海道 CA 保管的資訊中，個人簽名證明書、鏈接證明書、相互認證證明書、官職證明書驗證伺服器證明書、OCSP 回應器證明書、這些證明書的失效資訊、本運用章程等，作為公開資訊明確公佈，不視為機密資訊。

2-8-3 證明書失效資訊的公佈

北海道 CA 對所發行的個人簽名證明書、鏈接證明書、相互認證證明書及營運方面的相關證明書，其失效資訊給以公佈。無需公佈具體失效理由。此外，電子憑證的失效資訊按照根據法，僅提供給驗證簽名者。

2-8-4 針對執法機關的資訊公開

無任何規定。

2-8-5 民事手續方面的資訊公開

無任何規定。

2-8-6 基於證明書使用人要求的資訊公開

使用人要求公開自己的認證業務資訊時，在核實本人的基礎上給以公開。

2-8-7 基於其他理由的資訊公開

無任何規定。

2-8-8 基於證明書使用人要求的資訊更正等

使用人要求更正自己的認證業務資訊時，在核實本人的基礎上給以更正。

2-9 智慧財產權

無任何規定。

3．識別與認證

3-1 初次申請發行證明書

3-1-1 名稱形式

電子憑證的發行名義人名稱及使用人名稱，按照 X.500 識別名（DN：Distinguished Name）的形式設定。

3-1-2 名稱意義的相關事項

電子憑證的發行名義人名稱，根據知事的職稱來記載。

並且，儲存在電子憑證上的使用人基本 4 資料，記載在電子憑證的擴展區域內。儲存使用人基本 4 資料用的擴展區域資訊如下所示。

subjectAltName		
	common Name	姓名（申請人為外國籍居民，且在其住民票上記載該外國籍居民的通稱的情況下，姓名與通稱）
	dateOfBirth	出生年月日
	gender	性別
	address	住址

3-1-3 說明名稱形式的規則

遵照 X.500 識別名的章程。

3-1-4 名稱的一致性

北海道 CA 發行的電子憑證 subject 欄位的名稱需統一使用。

3-1-5 關於名稱糾紛的解決方法

無任何規定。

3-1-6 商標的認識・認證・作用

無任何規定。

3-1-7 記錄在電子憑證擴展區域的名稱種類和形式

使用人的姓名、通稱（僅限於接受電子憑證交付的人是外國籍居民，且在其住民票上記載該外國籍居民的通稱的情況。）、住址、出生年月日、性別等均使用漢字、平假名、片假名、英文字母及阿拉伯數位等記錄。

3-1-8 記錄在電子憑證擴展區域的名稱記錄方法相關規則

記錄姓名等使用的漢字，僅限於使用住址所在地的市村町受理窗口的終端機所採用的文字種類（JISX0208、JISX0212）之漢字。

姓名等存在不能使用的漢字時，則按照使用人的選擇，使用現有的相似漢字（以下稱「代替文字」。）

使用代替文字時，需在擴展區域加以注明。

3-1-9 使用人的識別與認證相關事項

初次發行申請按照以下方法進行申請者本人核實。當本人核實中發現疑點時，則不給予發行電子憑證。

① 發行申請書上填寫的基本 4 資料與住民基本台帳的記錄事項核對，確認該申請人即為住民基本台帳上所記錄的人。（實際存在的確認）

② 根據申請人出示的公共機關發行的，附有照片的身份證明(根據法規則第 6 條第 1 項規定的證明材料)，來確認申請人即為住民基本台帳上所記錄的人(本人的確認)。

3-1-10 代理申請時的識別與認證相關事項

由代理人申請時，通過以下方法進行代理人的本人核實及確認代理權的擁有。

① 確認持有申請者本人的簽名及蓋章的委託書，該印章的印鑒證明書，書面查詢該申請人時其答覆資料及住址所在地市町村長認可的資料

② 代理人的本人核實，由出示公共機關發行的附有照片的身份證明等進行確認（根據法規則第 5 條第 1 項規定的證明材料）

3-1-11 確認持有私密金鑰證據的方法

根據申請人使用住址所在地的市町村所設置的金鑰對產生器，且遵照根據法及相關法令設置金鑰對，以此進行確認。

3-2 電子憑證的更新

電子憑證更新時，通過以下方法進行使用者本人核實。當本人核實中發現疑點時，則不給予更新電子憑證。

① 更新申請書上填寫的基本 4 資料與住民基本台帳的記錄事項核對，確認該申請人即為住民基本台帳上所記錄的人。（實際存在的確認）

② 根據申請人出示的公共機關發行的，附有照片的身份證明來確認申請人即為住民基本台帳上所記錄的人(本人的確認)。

然而，對因更新致使電子憑證失效的私密金鑰，使用人需按規定方法消除。

3-3 失效後的重新發行

實施與初次申請發行時相同的本人核實手續。

3-4 失效申請

3-4-1 停止使用服務的失效申請

通過使用人的私密金鑰，進行附有數位簽章的網上申請，或者在住址所在地市町村的窗口進行書面申請。

針對使用者的本人核實，網上申請時通過驗證數位簽章來核實。在住址所在地市町村的窗口書面申請時，實施與發行電子憑證時相同的本人核實手續。

3-4-2 使用人的私密金鑰面臨危險時的失效申請

迅速前往住址所在地的市町村窗口，進行書面失效申請。

針對使用者的本人核實，實施與發行電子憑證時相同的本人核實手續。

4．運用事項

4-1 電子憑證的發行申請

4-1-1 發行申請・受理手續

電子憑證的發行申請・受理手續如下進行。

① 申請人提交住址所在地市町村的發行申請書時，同時提交 IC 卡。需更新時，提交儲存電子憑證的 IC 卡。

② 住址所在地的市町村長通過核對住民基本台帳的記錄內容，確認使用人實際存在的同時，還需根據出示公共機關發行的，附有照片的駕駛執照、護照等身份證明，確認申請者為本人。當本人核實中發現疑點時，則不給予發行電子憑證。

③ 申請人通過使用住址所在地的市町村窗口配備的金鑰對產生器，設置金鑰對。將設置的金鑰對中的公開金鑰通知住址所在地的市町村窗口。

此外，通過以下手續，可由代理人進行申請。當（１）或（２）發現疑點時，則不給以發行電子憑證。

（１）代理人，需提交或出示有申請者本人的簽名及蓋章的委託書(僅限於同時附有該印章的印鑒證明書的情況）以及可以確認代理人本人的駕駛執照，護照等。

（２）針對電子憑證的發行申請，為確認申請人是本人以及該申請出自本人意願，根據郵件或其他由住址所在地市町村長認可的方法，實施對該申請者的書面查詢，代理人則需提交該答覆資料，並出示住址所在地市町村長認可的資料。

（３）代理人，使用金鑰對產生器，設置金鑰對，公開金鑰需通知住址所在地市町村。然而，密碼的輸入（打開私密金鑰）由住址所在地的市町村長實施。

4-1-2 發行申請書的格式、必要記載事項

發行申請書上記載以下事項。

・申請的年月日

・姓名（注音假名）、通稱（僅限於接受電子憑證交付的人是外國籍居民，且在其住民票上記載該外國籍居民的通稱的情況。 ）、住址、出生年月日及性別，和與姓名、通稱及住址相關的代替文字

・代理人申請時，除以上事項之外添加代理人的姓名、住址

4-1-3 私密金鑰的電磁記錄介質

儲存在具有防短波功能的 IC 卡內。

4-2 電子憑證的發行

4-2-1 發行手續

電子憑證的發行手續如下所示。

① 住址所在地的市町村長通知北海道知事有關申請人的基本 4 資料及公開金鑰。

② 北海道知事發行電子憑證，通知住址所在地的市町村長。

4-2-2 電子憑證的形式

依照 ITU-T 勸告 X.509 (03/2000)，在擴展區域使用漢字、平假名、片假名、英文字母及阿拉伯數位記錄使用人的姓名、通稱、住址、出生年月日和性別。

此外，在擴展區域記錄的姓名、通稱及住址使用了代替文字時，需在擴展區域加以注明。

subjectAltName		
	commonName	姓名（申請人為外國籍居民，且在其住民票上記載該外國籍居民的通稱的情況下，姓名與通稱）
	dateOfBirth	出生年月日
	gender	性別
	address	住址
	substituteCharacterOfCommonName	姓名代替文字的使用資訊
	substituteCharacterOfAddress	住址代替文字的使用資訊

4-2-3 發行申請的拒絕

在符合以下事由的情況下，北海道知事將拒絕發行申請。

・已取得有效的電子憑證，且尚未登載在失效記錄（CRL）上

然而，萬一出現重複發行的情況時，北海道知事在瞭解清楚之後立即將最新發行日的電子憑證給予失效。

4-3 電子憑證的交付

4-3-1 交付手續

電子憑證的交付手續如下所示。

① 住址所在地的市町村長，在申請人的 IC 卡上儲存電子憑證及北海道知事的個人簽名證明書

② 住址所在地的市町村長，向申請人告知利用本服務的相關注意事項，同時交付電子憑證的影本

4-3-2 告知事項

住址所在地的市町村長向申請人告知以下事項。

・私密金鑰、其電磁儲存介質的 IC 卡、啟動 IC 卡的密碼，均屬使用人的責任範圍，需嚴加管理

・私密金鑰或者其電磁儲存介質 IC 卡丟失・被盜等的情況下，立即向住址所在地的市町村窗口呈報，進行失效申請，不得延誤

4-4 電子憑證的失效及暫停使用

4-4-1 職權失效的事由

4-4-1-1 職權失效的事由

電子憑證的職權失效事由如下所示。

・使用人的基本 4 資料的變更

・發現使用人電子憑證所記載的事項，與該電子憑證的有關使用人的住民票記載事項有出入時

・發現電子憑證的重複發行時

・北海道知事的私密金鑰面臨危險時

4-4-1-2 有權使證明書失效者

北海道知事有權行使。

4-4-1-3 北海道知事的私密金鑰面臨危險時的失效手續

北海道知事的私密金鑰發生危險時，北海道知事行使職權將在該私密金鑰上簽名的所有電子憑證失效，記錄在失效記錄（CRL/ARL）上的同時，還需通過網站(Web) 等給予公佈。

4-4-2 出自使用人的失效申請

4-4-2-1 出自使用人的失效申請事由

申請失效的理由如下所示。

・使用人希望停止使用本服務的申請

・使用人的私密金鑰面臨危險時的申請

4-4-2-2 停止使用服務的失效申請手續

通過以下的任何一種方法，可辦理停止使用本服務的失效手續。

① 受理附有數位簽章的網上申請。失效申請已受理之事宜會網上通知使用人。

② 住址所在地的市町村窗口受理書面失效申請。委託北海道知事進行失效處理。失效申請已受理之事宜會記載在書面上交付給使用人。

4-4-2-3 使用人的私密金鑰面臨危險等情況下的失效申請手續

使用人的私密金鑰面臨危險等情況下的失效申請手續如下所示。

① 住址所在地市町村受理書面失效申請。

② 委託北海道知事進行失效處理。失效處理已完成之事宜會記載在書面上交付給使用人。

4-4-2-4 使用人的電子憑證失效後的恢復方法

經過失效處理的電子憑證，不予進行恢復。通過重新辦理申請手續，發行新的電子憑證。

4-4-2-5 使用人的私密金鑰處於危險情況的恢復方法

通過重新辦理申請手續，發行新的電子憑證。

4-4-3 失效記錄（CRL/ARL） 的注意事項

將截止到指定時間受理完畢的失效資訊，反映到每天制作一次的最新失效記錄（CRL/ARL）上，制作好的失效記錄（CRL/ARL）迅速向被認可的驗證簽名者等公佈。

並且，提供給驗證簽名者等的失效記錄（CRL/ARL），一天 24 小時，一年 365 天開放使用。但因定期保養，有暫時無法使用的可能。

4-4-4 失效資訊的提供方法

4-4-4-1 失效資訊的提供方法

作為確認電子憑證有效性的方法，提供以下 2 種方法。

① OCSP 回應器查詢方法（使用 RFC2560 所規定的 OCSP 協議）

② 失效記錄（CRL/ARL）的提供方法（使用 RFC2251 所規定的 LDAPV3 協議）

4-4-4-2 OCSP 回應器查詢方法的答覆內容

針對識別電子憑證的發行人資訊和根據序號進行的網上查詢，分清在查詢這段時間該電子憑證是否有效、去向不明以及是否失效，如已經失效的情況下，答覆其失效事由。失效事由如下所示。

失効事由		
1	keyCompromise	使用人的私密金鑰處於危險情況。
2	cACompromise	北海道知事的私密金鑰處於危險情況。
3	affiliationChanged	電子憑證的記載內容發生了變更。
4	superseded	電子憑證已更新。
5	cessationOfOperation	電子憑證已不需要(不再使用。)

4-4-4-3 OCSP 回應器查詢方法事項

事先向北海道知事呈報，以取得訪問權。

4-4-4-4 失效記錄 （ CRL/ARL ）提供方法的答覆內容

失效記錄（CRL/ARL）的格式遵循 ITU-T 勸告 X.509(03/2000)。

失效記錄（CRL）原則上以市町村為單位制作成分類 CRL，記載已失效的電子憑證序號、失効事由（與本運用章程「4-4-4-2 OCSP 回應器查詢方法的答覆內容」的失効事由相同）及失効年月日。驗證簽名者等適當獲取儲存在資訊儲藏庫裡的失效記錄（CRL/ARL），進行電子憑證的驗證。

4-4-4-5 提供失效記錄 （CRL/ARL） 的必要事項

需事先向北海道知事呈報，以取得訪問權。

4-4-5 暫停使用相關事項

北海道知事發行的電子憑證不履行暫停使用。

4-4-6 暫停使用申請人

無任何規定。

4-4-7 要求暫停使用手續

無任何規定。

4-4-8 暫停使用期間

無任何規定。

4-4-9 失效記錄（CRL/ARL） 的發行頻率

有效期為 72 小時的失效記錄（CRL/ARL）每 24 小時發行一次。當北海道知事的私密金鑰處於危險狀況時，立即進行失效記錄（CRL/ARL）的發行。

4-4-10 發行失效記錄（CRL/ARL） 的最長拖延時間

最後發行的失效記錄（CRL/ARL），在其有效期滿之前即發行新的的失效記錄（CRL/ARL）。

4-4-11 失效記錄（CRL/ARL）的確認

驗證簽名者必需根據北海道知事發行的失效記錄（CRL/ARL），確認電子憑證的有效性。

4-5 制作有關失效資訊等的提供情況報告

指定認證機關，針對所保存的失效資訊及失效資訊文件的提供情況，制作成報告。指定認證機關必須將該報告公佈于公報，且放置在指定認證機關的辦公室 5 年，供一般閱覽。

報告的記載事項如下所示。

・失效資訊等的提供對象
・失效資訊等的提供年月
・提供的失效資訊件數
・失效資訊等的提供方法

4-6 相互認證證明書的發行申請

向個人認證 BCA 申請發行相互認證證明書，按照個人認證 BCA 所規定的步驟進行。

4-7 相互認證證明書的發行

北海道知事，根據規定手續，確認營運個人認證 BCA 者的真偽。按照個人認證 BCA 規定手續完成連接試驗後，針對個人認證 BCA 提出的發行證明書的要求，發行附有北海道知事簽名的相互認證證明書。

4-8 相互認證證明書的領取

北海道知事，根據規定手續，接受個人認證 BCA 發行的相互認證證明書，將領取書交給個人認證 BCA。同樣，北海道知事給個人認證 BCA 發行的相互認證證明書，按照規定手續交給個人認證 BCA，收取領取書。通過這些領取的確認，完成相互認證證明書的相互接收。

此外，北海道知事把與個人認證 BCA 相互交換的相互認證證明書進行配套，制作配套相互認證證明書，登記在資訊儲藏庫裡。

4-9 相互認證證明書的更新

以下(1)～(4)的情況下，北海道知事需對相互認證證明書及配套相互認證證明書進行更新。

在此進行的更新相互認證證明書的發行申請，發行及領取的各個手續，遵循本運用章程「4-6 相互認證證明書的發行申請」、「4-7 相互認證證明書的發行」及「4-8 相互認證證明書的領取」規定。此外，立即將資訊儲存庫裡的配套相互認證證明書調換成最新的。

(1) 個人認證 BCA 發行的相互認證證明書即將過期時

(2) 發行給個人認證 BCA 的相互認證證明書即將過期時

(3) 個人認證 BCA 發行的相互認證證明書的記載內容發生變更時

(4) 發行給個人認證 BCA 的相互認證證明書的記載內容發生變更時

4-10 相互認證證明書的失效

4-10-1 失效事由

當北海道 CA 或者個人認證 BCA 發生以下情況時，北海道 CA 需將發行給個人認證 BCA 的相互認證證明書失效、個人認證 BCA 同樣將發行給北海道 CA 的相互認證證明書失效。

・私密金鑰面臨危險
・相互認證證明書的更新
・相互認證的結束（包含因違反相互認證基準，結束相互認證的情況）

4-10-2 失效申請人

個人認證 BCA 向北海道 CA 提出的失效申請，由個人認證 BCA 的負責人執行。
北海道 CA 向個人認證 BCA 提出的失效申請，由北海道知事執行。

4-10-3 失效申請及失效處理步驟

相互認證證明書的失效申請，按照個人認證 BCA 規定的手續進行。

4-11 安全性監查手續

4-11-1 安全性監查程序

內部監查人(參照本運用章程「5-2-1 具有良好信譽的工作人員與其職責」)將記錄北海道 CA 系統及資訊儲藏庫發生事態的日誌，與業務實施記錄核對，進行確認是否有非法運作等異常事態的安全性監查。

4-11-2 監查日誌所記錄的資訊

將北海道 CA 系統及資訊儲藏庫的安全性相關的重要事項作為對象，記錄訪問日誌及操作日誌等的監查日誌。

・關於發行手續的操作・運轉日誌
・關於失效手續的操作・運轉日誌
・關於確認有效性的所有訪問・運轉日誌
・關於北海道知事的金鑰對設置的操作日誌
・針對系統、各種帳簿等的訪問日誌
・北海道 CA 的設備房間的出入記錄

監查日誌包括以下資訊。

・事態及處理的種類
・發生時間
・處理結果
・事態發生原由的識別資訊（操作員 ID、系統名稱等）

4-11-3 監查日誌的檢查週期

內部監查人以周為單位進行安全性監查。

4-11-4 監查日誌的保管期間

保管期間為一年。

4-11-5 監查日誌的保護

針對監查日誌，實施防止竄改措施。而且監查日誌的備份以月為單位儲存于外部儲存設備，在具有適當進出管理的房間內，將其保管在可以上鎖的保存庫裡。

監查日誌的閱覽及刪除由內部監查人妥善實施。

4-11-6 備份監查日誌的步驟

以日為單位進行備份，以月為單位儲存在外部儲存設備裡。

4-11-7 檢查監查日誌的通知

進行監查日誌的檢查，不通知導致該事態發生的人。

4-11-8 脆化性的驗證

根據監查日誌的檢查，針對運行方面及系統方面的脆化性進行評估。

4-11-9 監查日誌的收集系統

監查日誌的收集機能，即作為北海道 CA 的一項機能，從系統啟動開始，將有關安全的重要事態作為監查日誌進行收集。

4-12 記錄的保管（存檔）

4-12-1 使用紙張保管的資訊

4-12-1-1 保管資訊的種類

以下資訊進行保管

（北海道知事）

・制定本運用章程的相關資料
・舉行主要典禮的相關資料
・與驗證簽名者等的協議相關資料
・認證業務資訊的公開・更正等的相關資料
・監查報告 等

（指定認證機關）

・指定認證機關的指定・変更的相關資料
・認證事務管理章程
・設備及安全措施的相關資料
・項目計劃・收支預算的相關資料
・項目報告・收支結算報告
・認證業務資訊的公開・更正等的相關資料
・失效資訊及び失效資訊文件的提供狀況報告
・手續費的相關資料 等

（市町村長）

・申請發行電子憑證的相關資料（發行申請書等）
・申請電子憑證失効的相關資料（失効申請書等）
・認證業務資訊的公開・更正等的相關資料 等

4-12-1-2 保管期間

保管期間為 10 年。然而申請發行電子憑證的相關資料為 13 年。

4-12-1-3 保管資訊的保護

保管在指定認證機關的資訊，在實施防止竄改措施的同時，還需保管在具有適當的進出管理的房間裡設有可以上鎖的保存庫內，並實施顧及溫度、濕度等環境因素的保護措施。保管在市町村及都道府縣的資訊，需保管于適當的地方。

4-12-1-4 保管資訊的驗證

每年實施一次確認記載保管資訊的紙張狀態、可閱讀性。

4-12-2 以數碼資料形式保管的資訊

4-12-2-1 保管資訊的種類

以下資訊保管在指定認證機關

・失效申請書（向北海道知事網上申請時）
・電子憑證
・相互認證證明書
・個人簽名證明書
・鏈接證明書
・官職證明書驗證伺服器證明書
・OCSP 回應器證明書
・失效資訊
・失效記錄（CRL/ARL）
・失效資訊文件
・失效記錄（CRL/ARL）提供方法的使用記錄
・OCSP 回應器查詢方法的使用記錄
・各種日誌（監視用日誌、啟動停止日誌、操作日誌）等

4-12-2-2 保管期間

保管期間為 10 年。然而，已發行的電子憑證為 13 年，失效資訊則從該失效資訊的登記日起，到該失效記錄的相關電子憑證之有效期滿日為止。

4-12-2-3 保管資訊的保護

針對保管資訊，在實施訪問限制的同時，還需實施防止竄改措施。

保管資訊以月為單位儲存于外部儲存設備，保管在具有適當進出管理的房間內且可以上鎖的保存庫裡。

4-12-2-4 備份保管資訊的程序

保管資訊以日為單位進行備份，以月為單位儲存在外部儲存設備裡。

4-12-2-5 記錄上附加時間戳記的注意事項

針對保管資訊，需附加時間戳記。

4-12-2-6 保管資訊的驗證

對存有保管資訊的外部儲存設備，每年實施一次確認其可閱讀性。

4-13 北海道知事的鎖的更新

每 5 年一次進行北海道知事金鑰對的更新。

金鑰對更新時，發行構築新舊公開金鑰認證路徑的鏈接證明書，公開在資訊儲藏庫上。

4-14 鎖面臨危險時與損害時的修復

4-14-1 硬體、軟體或者資料受到損害時的應對措施

硬體，軟體或者資料受到損害時，利用備份硬體、軟體以及資料迅速進行修復工作。

4-14-2 北海道知事的私密金鑰處於危險時的應對措施

應對措施如下所示。

・停止發行電子憑證的業務

・將出自該私密金鑰簽名的所有電子憑證、相互認證證明書等失效，記錄在失效記錄（CRL/ARL）上並公佈

・通知個人認證 BCA

4-14-3 發生災害時設備的確保

因災害導致設備受損時，確保預備機器，利用備份資料進行運作。

4-15 投訴・諮詢的處理

針對認證事務等相關的投訴・諮詢，北海道知事、指定認證機關及市町村長必須努力進行適當且迅速的處理。

4-16 系統運用

履行安全且妥當的系統運用。詳情另行規定。

4-17 認證事務的結束

無任何規定。

4-18 認證事務的停止、廢除

指定認證機關，在停止或廢除全部或部分認證事務等的情況下，必須得到總務大臣的批准。

而且，由此致使北海道知事實施認證事務的情況時，指定認證機關必須進行以下事項。

・向北海道知事交接必須交接的認證事務。

・將必須交接的認證事務相關的帳簿、材料、資料及電磁儲存介質等交給北海道知事。

此外，還需執行總務大臣或北海道知事認為有必要的事項。

5．實體方面、手續方面、人事方面的安全管理

5-1 實體方面的安全管理

5-1-1 北海道 CA

5-1-1-1 設施的位置和建造

北海道 CA 的設施需設置在不易受水災、地震、火災和其它災害影響的地方，建築構造上採取防震、防火及防止非法進入等措施。此外，所使用的機器等需設置在能防災及防止非法進入的安全之地。

5-1-1-2 實體的進出管理

按照北海道 CA 設施內的各個房間執行業務的重要程度，實施多種安全等級的進出管理。有操作權限的人根據可以識別的 IC 卡及生物體認證裝置進行認證。

各房間的進出權限，則根據本運用章程「5-2 手續方面的安全管理」規定的各個工作人員的業務情況，由北海道 CA 的認證管理負責人授予。

針對北海道 CA 的設施，安置監視人員，通過監視系統實施 24 小時、365 天的監視。

5-1-1-3 電力與空調

北海道 CA 不僅要確保機器運作所需的充分容量的電源，還要採取針對突然斷電、停電、電壓・頻率變化的相應措施。當發生商業用電源斷絕供給的情況時，需在所定時間內轉換成由發電機發電的電源供給。

通過設置空調設備，適當維持機器等的運作環境及工作人員的工作環境。

5-1-1-4 防汛措施

設有北海道 CA 設備的建築物、室內需設置漏水檢測器，對房頂、地板採取防水措施。

5-1-1-5 防震措施

設有北海道 CA 設備的建築物需具備防震構造，採取防止機器・用具的翻倒及掉落等措置。

5-1-1-6 防火措施

設有北海道 CA 設備的建築物需具備防火構造，房間劃分防火區，置備滅火設備。

5-1-1-7 防電磁波措施

根據北海道 CA 設施內的各個房間所執行的業務重要程度，置備防止電磁波攻擊以及防止電磁波引起的資訊洩露設備。

5-1-1-8 介質（磁介質等）管理

針對儲存保管資訊、備份資料的介質，不僅需保管在具有適當進出管理的房間內並可以上鎖的保存庫裡，而且按照規定手續實施適當的移動出入管理。

5-1-1-9 廢棄物處理

針對存有作為機密資訊的資料・儲存介質，按照規定手續進行妥當的廢棄處理。

5-1-1-10 外部備份

無任何規定。

5-1-2 市町村的設施

5-1-2-1 設施的位置與建造

作為住址所在地的市町村設施。

5-1-2-2 實體的操作管理

金鑰對產生器、受理窗口終端機設置在住址所在地市町村的工作人員可以監視的地方。此外，對金鑰對產生器、受理窗口終端機實施適當的保養。

操作受理窗口終端機需實施使用人的本人核實。操作人的認證，以 ID / 密碼方式進行。

5-1-2-3 保管資訊的管理

本運用章程「4-12-1-1 保管資訊的種類」的相關資料，需保管在適當的地方。

5-1-2-4 廢棄物處理

針對存有秘密資訊的資料・儲存介質及受理窗口終端機、金鑰對產生器等的廢棄，按照規定手續進行妥當的廢棄處理。

5-2 手續方面的安全管理

5-2-1 具有良好信譽的工作人員與其職責

5-2-1-1 北海道 CA 的工作人員

北海道 CA 系統運行的相關工作人員如下所示。

(1) 認證局管理負責人

認證局管理負責人即營運北海道 CA 的負責人， 履行以下業務。

・認證業務的總括
・北海道知事的私密金鑰發生危險及發生災害等緊急情況時的應對總括
・對工作人員下達指示及確認工作結果
・用於控制 HSM（安全管理北海道知事的私密金鑰裝置）功能的鎖（以下稱「管理鎖」。）的保養管理。
・針對請求公開認證業務資訊的應對管理
・針對請求更正認證業務資訊的應對管理
・諮詢・投訴處理的應對管理
・認證業務資訊保護委員會的管理
・置備認證業務相關的帳簿
・制作失效資訊等的提供情況報告
・房間出入管理

・應對遵循情況的監查，以及針對其指正事項實施改正管理
・其他有關北海道 CA 的營運及運用總括
・個人資訊的管理

(2) 私密金鑰管理人

私密金鑰管理人，即使用北海道知事的私密金鑰等相關業務的負責人，履行如下業務。然而，該工作由多位私密金鑰管理人執行。

・保管管理北海道知事私密金鑰等的備份介質

・北海道知事私密金鑰等的設置、發行個人簽名證明書時的 HSM 操作

・北海道知事私密金鑰等更新時的 HSM 操作

・北海道知事私密金鑰等備份，以及從備份進行復原時的 HSM 操作

(3) 受理負責人

受理負責人，履行相互認證證明書等的發行、更新及失效申請的受理、與個人認證 BCA 的聯繫調整業務及申請資料等的管理。

(4) 審查負責人

審查負責人，履行審查相互認證證明書等的發行、更新及失效申請等業務。

(5) 審查批准人

審查批准人，履行針對審查負責人進行的相互認證證明書等的發行申請、更新申請及根據失效申請的審查結果給予批准的業務。

(6) 高級操作人員

高級操作人員，即使用北海道知事的私密金鑰履行以下業務。此外，該工作由多位高級操作人員執行。

・HSM 的活性化及非活性化

・個人簽名證明書的發行、更新、失效處理

・相互認證證明書的發行、更新、失效處理

・官職證明書驗證伺服器證明書的發行、更新、失效處理

・OCSP 回應器證明書的發行、更新、失效處理

・北海道 CA 電子憑證等政策的設定登錄及變更

・其它北海道 CA 系統的運用管理業務

(7) 資訊儲藏庫操作人員

資訊儲藏庫操作人員，即履行資訊儲藏庫的設定管理等相關業務。

(8) 一般操作人員

一般操作人員，即履行網路機器等的運用及維護管理等業務。

(9)內部監查人

內部監查人，即履行以下北海道 CA 系統及資訊儲藏庫的日誌相關業務。

・監查日誌的檢查

・已監查過的日誌刪除

5-2-1-2 市町村的工作人員

市町村的工作人員，履行電子憑證的發行・失效時嚴格的本人核實，以及發行・失效相關的事務，並且針對該事務使用的機器等進行妥善管理。

5-2-2 北海道 CA 各個工作人員的職權分工與下達指示方法

各個工作人員行使職權的分工與下達指示方法如以下規定所示。

① 職權分工
從人的安全角度考慮進行職務分工，由被授予權限的多位工作人員履行設施的運用・管理。

② 認證局管理負責人的權限
針對重要的業務指示，認證局管理負責人按照另行規定的指定手續，向各個工作人員下達指示。

③ 高級操作人員的權限
高級操作人員，按照另行規定的手續，向一般操作人員下達各種工作指示及確認結果。此外，發行相應工作人員的權限登記以及證明書。

5-2-3 北海道 CA 各個工作人員的識別與認證事項

・各個工作人員進行系統操作時，系統執行識別・認證運作工作人員是否為正當權限人。

・各個工作人員的認證使用 IC 卡或密碼來實施。密碼需定期更換。

・按照各個工作人員的職責，將各工作人員可以訪問的秘密資訊控制到最低限度。

5-3 北海道 CA 在人事方面的安全管理

5-3-1 工作人員的個人背景審核與認可程序

按照所需的審核程序，通過雇用前資料(履歷表、推薦信)審查，實施經歷調查。

5-3-2 針對工作人員的培訓程序

按照教育訓練計畫，對各工作人員實施必要的培訓。

5-3-3 工作人員之間的業務交接、頻率和順序

認證局管理負責人根據文件，規定業務交替方式。

5-3-4 不被認可的行動

各個工作人員行使了不被認可的行動時，按照已有的規定進行懲戒處分。

5-3-5 提供給各個工作人員的文件

根據各自的訪問權限，各個工作人員可以閱覽文件(運用程序、操作步驟等)。

6．技術的安全管理

6-1 設置和下載金鑰對

6-1-1 北海道知事的鎖

6-1-1-1 北海道知事的金鑰對設置人、制鎖方法

北海道知事的金鑰對，由多位私密金鑰管理人使用本運用章程「6-1-1-3 設置金鑰對的硬體/軟體」規定的設備進行制鎖。

6-1-1-2 鎖長

根據 RSA 加密方式，使用 2048 比特的鎖。

6-1-1-3 設置金鑰對的硬體/軟體

相當於 FIPS140-1 等級 3 的 HSM。

6-1-1-4 私密金鑰的使用目的

用於數位簽章。

6-1-1-5 領取個人認證 BCA 的公開金鑰

為互換相互認證證明書，北海道 CA 需安全可靠地領取個人認證 BCA 的公開金鑰。

6-1-1-6 發送北海道知事的公開金鑰

北海道知事的個人簽名證明書，在發行電子憑證時儲存在 IC 卡裡，然後交付給使用人，並且通過安全可靠的方法發送給驗證簽名者等。

6-1-2 使用人的鎖

6-1-2-1 使用人的金鑰對設置人、制鎖方法

使用人本人利用住址所在地市町村的金鑰對產生器進行制鎖。

6-1-2-2 向住址所在地市町村等安全提供使用人公開金鑰的方法

住址所在的地市町村直接從使用人那裡領取儲存在 IC 卡裡的公開金鑰。

6-1-2-3 鎖長

根據 RSA 加密方式，使用 1024 比特的鎖。

6-1-2-4 設置金鑰對的硬體/軟體

住址所在地市町村的金鑰對產生器。

6-1-2-5 私密金鑰的使用目的

用於數位簽章。

6-2 保護私密金鑰

6-2-1 北海道知事的私密金鑰

6-2-1-1 保管私密金鑰要求的基準

使用相當於 FIPS140-1 等級 3 的 HSM 加以保護。

6-2-1-2 私密金鑰的多人控制

多位私密金鑰管理人通過 HSM 的控制對私密金鑰加以保護。

6-2-1-3 私密金鑰的委託保管 （第三方支付擔保）

不實施私密金鑰的委託保管。

6-2-1-4 私密金鑰的備份

私密金鑰的備份，由多位私密金鑰管理人操作。

從 HSM 備份的私密金鑰，以加密方式進行安全保管。但私密金鑰管理人不得將備份介質帶出其保管房間之外。

6-2-1-5 私密金鑰的保管 （存檔）

不實施私密金鑰的存檔。

6-2-1-6 加密模組內私密金鑰的儲存

私密金鑰通過多位私密金鑰管理人的操作，在 HSM 中設置，儲存到加密模組內。

6-2-1-7 私密金鑰的活性化

私密金鑰由多位私密金鑰管理人操作，將其活性化。

6-2-1-8 私密金鑰的非活性化

私密金鑰由多位私密金鑰管理人操作，將其非活性化。

6-2-1-9 私密金鑰的廢棄

廢棄加密模組內的私密金鑰，由多位私密金鑰管理人通過初始化加密模組等方法，使其處於完全不能使用的狀態。然而，如果將加密模組帶出室外時，則將加密模組實體毀壞。

此外，所廢棄的私密金鑰，其備份用的加密模組同樣需要廢棄。

6-2-2 使用人的私密金鑰

6-2-2-1 關於保管私密金鑰的要求基準

在具有防短波功能的 IC 卡內，按照「官方個人認證服務卡應用程式外部介面格式書 1.1 版」，裝載卡的應用程式，保護私密金鑰無法從 IC 卡上直接被讀出。

6-2-2-2 私密金鑰的委託保管 （第三方支付擔保）

北海道知事不接受使用人私密金鑰的委託保管，而且不認可使用人將其私密金鑰委託給第三者進行保管。

6-2-2-3 私密金鑰的備份

私密金鑰保管在 IC 卡內，不進行備份。

6-2-2-4 私密金鑰儲存在加密模組（IC 卡）內

使用人的私密金鑰，通過住址所在地市町村的金鑰對產生器的設置，儲存在使用人的 IC 卡裡。儲存在 IC 之後，在金鑰對產生器設置的私密金鑰，需從金鑰對產生器上徹底刪除。

6-2-2-5 私密金鑰的活性化

使用人的私密金鑰，由使用人輸入密碼將其活性化。

6-2-2-6 私密金鑰的非活性化

通過操作 IC 卡，使私密金鑰非活性化。

6-2-2-7 私密金鑰的廢棄

使用人的私密金鑰進行廢棄時， 使用人利用住址所在地市町村的受理窗口終端機，以及金鑰對產生器將其廢棄。

6-3 關於金鑰對設置管理的其它方面

6-3-1 北海道知事的鎖

6-3-1-1 公開金鑰的保管

將包含在個人簽名證明書內的公開金鑰，根據本運用章程「4-12 記錄的保管（存檔）」規定的期間，保管在已實施防止竄改措施的檔案裡。

6-3-1-2 公開金鑰、私密金鑰的使用期間

北海道知事的個人簽名證明書的有效期為 10 年。私密金鑰的使用期限自製鎖日起算 5 年，每過 5 年進行更新。

然而，當估計到密碼的安全性脆化時，有可能考慮改變加密方式，即時進行鎖的更新等情況。

6-3-2 使用人的鎖

使用人的公開金鑰和私密金鑰的使用期限，自製鎖日起算 3 年。

然而，當估計到密碼的安全性脆化時，有可能考慮改變加密方式，即時進行鎖的更新等情況。

6-4 活性化資料

6-4-1 北海道知事的鎖

6-4-1-1 活性化資料的產生與下載

儲存北海道知事私密金鑰的 HSM 活性化資料，通過管理鎖來設定。

6-4-1-2 活性化資料的保護

使儲存北海道知事私密金鑰的 HSM 活性化所必需的管理鎖，需安全保管。

6-4-2 使用人的鎖

6-4-2-1 活性化資料的產生與下載

使用人私密金鑰的活性化資料（密碼），由使用人自己通過利用金鑰對產生器設置金鑰對的時候，設定到 IC 卡裡。

6-4-2-2 活性化資料的保護

使用人私密金鑰的活性化資料必須定期變更，安全保管 。

6-5 電腦的安全管理

6-5-1 電腦的安全功能注意事項

北海道 CA 的相關系統，需使用信譽良好的 OS，具備訪問限制、各個工作人員的識別與認證功能、監查日誌及存檔資料的收集功能以及系統復原功能等。

6-5-2 電腦的安全評估

隨時實施系統的安全評估。

6-6 系統壽命的安全管理

6-6-1 系統開發的安全管理

有關本服務的開發，修正或者變更，需根據規定手續，由信譽良好的組織或環境下實施運作。已開發、修正或變更的系統，通過試驗環境的驗證，得到認證管理局負責人的批准之後引入使用。而且，系統規格及驗證報告進行書面保管。

6-6-2 系統運用方面的安全管理

6-6-2-1 北海道 CA

為維持管理本服務的相關系統，定期進行 OS 及軟體的安全檢查。而且，將該檢查結果進行書面保管。

6-6-2-2 市町村

為維持管理本服務的相關系統，妥善進行金鑰對產生器及受理窗口終端機的 OS 及軟體的安全管理。

6-7 網路安全管理

為防止非法進入，將經由外部網路所必要的網上服務的認可，縮減到最小限度。此外，實施檢驗非法侵入等充分的安全保護措施。資訊儲藏庫內保存的資訊中，其公開資訊需通過防火牆提供。

6-8 加密模組的技術管理

按照本運用章程「6-1-1-3 設置金鑰對的硬體/軟體」、「6-2-1-1 關於保管私密金鑰的要求基準」的規定。

7. 證明書和失效記錄（CRL/ARL）的內容

7-1 證明書

7-1-1 電子憑證

電子憑證記載如下資訊。詳情根據 Profile 設計書決定。

・版本編號（X.509 證明書格式的版本編號）
・序號（北海道 CA 內為識別已發行過的證明書所用的號碼）
・簽名演算法（北海道知事在該電子憑證簽名時使用的演算法資訊）
・發行人資訊（發行該電子憑證的北海道知事名，用 X.500 識別名記載）
・有效期的開始日（該電子憑證的發行日）
・有效期的結束日（發行日 3 年後）
・公開金鑰（使用人的公開金鑰）
・擴展資訊（記載使用人的基本 4 資料或鎖的使用目的等）

7-1-2 相互認證證明書

與個人認證 BCA 實施相互認證時所必需的相互認證證明書記載如下資訊。詳情根據 Profile 設計書決定。

・版本編號（X.509 證明書格式的版本編號）
・序號（北海道 CA 內為識別已發行過的證明書所用的號碼）
・簽名演算法（北海道知事在該相互認證證明書簽名時使用的演算法資訊）
・發行人資訊（發行該相互認證證明書的北海道知事名，用 X.500 識別名記載）
・有效期的開始日（該相互認證證明書的有效開始日）
・有效期的結束日（該相互認證證明書的有效開始日起算 5 年後）
・公開金鑰（相互認證 CA 的公開金鑰）
・擴展資訊

7-1-3 個人簽名證明書

北海道知事的個人簽名證明書記載如下資訊。詳情根據 Profile 設計書決定。

・版本編號（X.509 證明書格式的版本編號）
・序號（北海道 CA 內為識別已發行過的證明書所用的號碼）
・簽名演算法（北海道知事在該個人簽名證明書簽名時使用的演算法資訊）
・發行人資訊（發行該個人簽名證明書的北海道知事名，用 X.500 識別名記載）
・有效期的開始日（該個人簽名證明書的發行日）
・有效期的結束日（發行日 10 年後）
・公開金鑰（北海道知事的公開金鑰）
・擴展資訊

7-1-4 鏈接證明書

北海道知事的鎖更新時所必需的鏈接證明書記載如下資訊。詳情根據 Profile 設計書決定。

・版本編號（X.509 證明書格式的版本編號）
・序號（北海道 CA 內為識別已發行過的證明書所用的號碼）
・簽名演算法（北海道知事在該連結證明書簽名時使用的演算法資訊）
・發行人資訊（發行該連結簽名證明書的北海道知事名，用 X.500 識別名記載）
・有效期的開始日（OldWithNew：舊版金鑰對的制鎖日、NewWithOld：新版金鑰對的制鎖日）

・有效期的結束日（OldWithNew：舊版個人簽名證明書的有效期結束日、NewWithOld：舊版個人簽名證明書的有效期結束日）
・公開金鑰（OldWithNew：舊版公開金鑰、NewWithOld：新版公開金鑰）
・擴展資訊

7-2 失效記錄 （ CRL/ARL ）

7-2-1 電子憑證的失效記錄（CRL）

電子憑證失效記錄（CRL）記載如下資訊。詳情根據 Profile 設計書內的 CRL 的 Profile 決定。

・版本資訊（CRL 格式的版本編號）
・簽名演算法（北海道知事在該 CRL 上簽名時使用的演算法資訊）
・發行者資訊（發行該 CRL 的北海道知事名，用 X.500 識別名記載）
・有效期的開始日（該 CRL 的有效開始日）
・有效期的結束日（該 CRL 的有效開始日起算 3 天后）
・下次更新預定日（該 CRL 的有效開始日 1 天后）
・已失效的證明書資訊（序號、失效年月日、失效事由）
・擴展資訊

7-2-2 相互認證證明書的失效記錄（ARL）

相互認證證明書的失效記錄（ARL）記載如下資訊。詳情根據 Profile 設計書內的 ARL 的 Profile 決定。

・版本資訊（ARL 格式的版本編號）
・簽名演算法（北海道知事在該 ARL 上簽名時使用的演算法資訊）
・發行者資訊（發行該 ARL 的北海道知事名，用 X.500 識別名記載）
・有效期的開始日（該 ARL 的有效開始日）
・有效期的結束日（該 ARL 的有效開始日起算 3 天后）
・下次更新預定日（該 ARL 的有效開始日 1 天后）
・已失效的證明書資訊（序號、失效年月日、失效事由）
・擴展資訊

7-2-3 個人簽名證明書的失效記錄（ARL）

個人簽名證明書的失效記錄（ARL）記載如下資訊。詳情根據 Profile 設計書內的 ARL 的 Profile 決定。

・版本資訊（ARL 格式的版本編號）
・簽名演算法（北海道知事在該 ARL 上簽名時使用的演算法資訊）
・發行者資訊（發行該 ARL 的北海道知事名，用 X.500 識別名記載）
・有效期的開始日（該 ARL 的有效開始日）
・有效期的結束日（該 ARL 的有效開始日起算 3 天后）
・下次更新預定日（該 ARL 的有效開始日 1 天后）
・已失效的證明書資訊（序號、失效年月日、失效事由）
・擴展資訊

7-2-4 鏈接證明書的失效記錄（ARL）

鏈接證明書的失效記錄（ARL）記載如下資訊。詳情根據 Profile 設計書內的 ARL 的 Profile 決定。

・版本資訊（ARL 格式的版本編號）

・簽名演算法（北海道知事在該 ARL 上簽名時使用的演算法資訊）
・發行者資訊（發行該 ARL 的北海道知事名，用 X.500 識別名記載）
・有效期的開始日（該 ARL 的有效開始日）
・有效期的結束日（該 ARL 的有效開始日起算 3 天后）
・下次更新預定日（該 ARL 的有效開始日 1 天后）
・已失效的證明書資訊（序號、失效年月日、失效事由）
・擴展資訊

8．運用章程的管理

8-1 運用章程的更改管理

北海道知事，根據需要對本運用章程進行更改。

8-2 公佈及通知

本運用章程有所更改時，北海道知事需立即將更改的運用章程在網站(Web)上公佈。同時向使用人、驗證簽名者等以及確認簽名者通知。

8-3 運用章程的認可手續

根據北海道知事的決定給以批准有效。