簡体字版

地方公共団体の公共性個人認証服务

北海道认证局 运用章程

Ver. 1．5

2013 年 7 月 8 日

北海道

修订过程

Ver	日期	修订内容
1.0	2004 年 1 月 29 日	首版发行
1.1	2005 年 1 月 19 日	因更改实施规则改版
1.2	2006 年 11 月 1 日	因修正法律改版
1.3	2008 年 9 月 19 日	因认证局私钥更新改版
1.4	2009 年 4 月 1 日	因联系地址变更改版
1.5	2013 年 7 月 8 日	因实施部分修正过的住民基本台帐法(平成21年法律第 77 号)改版

1．前言

本运用章程，针对北海道的公共性个人认证服务下属在都道府县各个认证局（以下称为「北海道 CA」），为发行住民基本台帐上有记录的居民的电子证明书等（使用者的证明书以下称「电子证明书」。），制定其有关认证业务的营运方针，旨在将居民与国家或地方公共团体的机关等之间的申请・申报等手续实现电子化，。

此外，本运用章程的构架遵循了 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」。然而参照其它章程的部分只保留了标题，参照内容有所注明。

1-1 概要

北海道 CA，针对北海道范围内的，市町村住民基本台帐上有记录的居民，根据其申请不仅发行电子证明书,和其他北海道 CA 运行时必要的证明书,而且针对其它公共性个人认证服务，即在各都道府县下属认证局，或政府认证的基层认证局等为进行相互认证而设置的公共性个人认证服务过渡认证局(以下称「个人认证 BCA」)，北海道 CA 还发行相互认证证明书与其进行互换。尚且，制订失效资讯（有关电子证明书失效的信息。以下同。）、失效记录（CRL/ARL）（记载有关电子证明书等失效信息。以下同），失效资讯文件（称失效记录（CRL）存档。以下同），以及针对「有关涉及数字签名的地方公共团体认证业务的法律」（以下称「根据法」。）的第 17 条第 4 项规定的验证签名者，或者该条第 6 项规定的验证团体签名者的要求，给以提供服务。

此外，北海道 CA 将本运用章程确定为关于北海道 CA 的认证业务运营方针，不独立执行 CP（证明书政策）以及 CPS（认证实施章程）。

1-2 识别

北海道 CA 的证明书政策编号如下所示。

北海道 CA 电子证明书等政策

电子证明书政策以及北海道 CA 相互认证证明书政策

1.2.392.200149.8.5.1.1.10

试验用电子证明书政策以及北海道 CA 相互认证证明书政策

1.2.392.200149.8.5.1.0.10

官职证明书验证服务器证明书政策

1.2.392.200149.8.5.1.200

试验用官职证明书验证服务器证明书政策

1.2.392.200149.8.5.1.0.200

OCSP 响应器证明书政策

1.2.392.200149.8.5.1.300

试验用 OCSP 响应器证明书政策

1.2.392.200149.8.5.1.0.300

1-3 运用体制与证明书的适用范围

1-3-1 参与者

(1) 总务大臣

总务大臣根据根据法，向指定认证机关下达指示。

(2) 公共性个人认证服务都道府县协议会

公共性个人认证服务都道府县协议会（以下称「协议会」。），履行联系及调整关于个人认证系统实现一元化营运的重要事项关联事务。

(3) 北海道知事

北海道知事，将以下所示的北海道 CA（北海道认证局）机能予以整备。

(4) 北海道 CA

北海道 CA，与市町村长相互配合・协作，履行发行电子证明书和其它证明书，制订失效记录（CRL/ARL），提供确认电子证明书的有效性方法等证明书发行・失效资讯管理业务。同时履行北海道知事的私钥面临危险或发生灾害时的紧急应对。

此外，针对使用者在国家或地方公共团体所接收的网上文件，给予提供为验证数字签名所需要的的官职以及职责证明书的有效性确认方法。

(5) 个人认证 BCA

个人认证 BCA，依照协议会制定的运用章程，履行与北海道 CA 等在各都道府县下属认证局，以及政府认证的基层过渡认证局（以下称「政府认证基层 BCA」。）等相互认证时使用的证明书等的发行业务。

(6) 指定认证机关

指定认证机关，按照根据法的规定，受北海道知事委托，履行有关实施认证业务的事务(以下称「认证事务」)。

(7) 市町村长

北海道范围内的市町村长，在受理电子证明书的发行申请以及失效申请后，履行申请者的本人核实，向申请者交付北海道 CA 发行的电子证明书等职责。

(8) 申请者 / 使用者

申请者，即根据根据法第 3 条 1 项的规定，申请发行电子证明书的人。（也可由代理人申请。但这种情况需符合「有关涉及数字签名的地方公共团体认证业务的法律实施规则」（以下称「根据法规则」。）第 5 条规定。）。使用者，即住民基本台帐上有记录，接受电子证明书发行的人。

使用者，通过与国家或地方公共团体的机关等之间的网上申请・申报，可以利用电子证明书。针对北海道知事或指定认证机关，可要求公开与自己相关的认证业务资讯(指电子证明书的发行记录，失效资讯及失效资讯文件。以下同)。对所公开的认证业务资讯，可要求更改，添加或删除其全部或一部分内容。此外，针对认证事务等有所不服时，根据行政不服审查法，可以向总务大臣提出审查请求。同时，针对使用者在国家或地方公共团体的机关所接收的网上公函，对验证数字签名所需要的的官职以及职责证明书的有效性加以确认。

(9) 验证签名者

指以下机关或人员中，为接受确认电子证明书有效性方法的提供，根据根据法第 17 条第 1 项规定事先呈报并被赋予访问权限的人。

① 利用资讯通信技术履行行政手续的相关法律第 2 条第 2 号所规定的行政机关等(以下称「行政机关等」)。

② 法院

③行政机关等遵照法律规定所指定，登录或者认可的人，即根据针对行政机关等等的申请、呈报或其它手续所伴随的必要事项，以电磁方式接受提供，并向行政机关等自行将其提供，或回应其查询业务者。

④「有关数字签名及认证业务的法律」(以下称「数字签名法」。) 第 8 条规定的认可认证企业。

⑤ 由总务大臣认可的，履行数字签名法第 2 条第 3 项规定的特定认证业务，符合「有关涉及数字签名的地方公共团体认证业务的法律实施令」(以下称「根据法的政令」。) 规定标准的人。

⑥ 按照根据法的政令决定的，针对行政机关等或法院的申请、呈报或其它手续所需要的电磁记录予以提供的团体。

通过北海道 CA 所提供的失效记录（CRL/ARL）等，接受其提供的用以确认电子证明书有效性的方法，验证使用者在网上的申请・呈报等相关的数字签名。

(10) 确认签名者

指基于根据法第 17 条第 5 项规定，按照根据法的政令决定的人员。

接受如下决定的验证团体签名者提供的，电子证明书的有效性确认结果，验证使用者在网上的申请・呈报等相关的数字签名。

(11) 验证团体签名者

指以下人员中，为接受确认电子证明书有效性方法的提供，按照根据法第 17 条第 5 项规定事先呈报并被赋予访问权限的人。

①按照根据法的政令决定的，基于法律规定而受他人委托，履行向行政机关等以及法院提出申请，呈报或其他手续的人，其所属团体。

②按照根据法的政令决定的，针对行政机关等或法院的申请、呈报或其它手续所需要的电磁记录予以提供的人，其所属团体或机关。

通过北海道 CA 所提供的失效记录（CRL/ARL）等，接受其提供的用以确认电子证明书有效性的方法，然后针对收到确认签名者回信的使用者通过网上申请・呈报等所传送电子证明书

附件，确认其有效性，将结果向确认签名者做出回答。

(12) 验证签名者等

指验证签名者以及验证团体签名者。

1-3-2 适用性・适用环境等

服务类型及用途如以下 4 项所示。

① 基于以下用途给予发行电子证明书。
- ・行政机关等及法院的网上申请・呈报手续相关的数字签名
- ・验证签名者等履行本人核实
- ・确认签名者履行本人核实

此外，电子证明书的有效期限为自电子证明书发行日起算 3 年。

② 基于以下用途给予发行相互认证证明书。
- ・通过个人认证 BCA，与政府认证基层 BCA 等的相互认证

此外，相互认证证明书的有效期限为自相互认证证明书发行日起算 5 年。

③ 基于以下用途给予发行官职证明书验证服务器证明书。
- ・针对使用者在国家或地方公共团体网上接收的公函，为验证数字签名所需要的官职证明书或职责证明书的有效性，提供确认方法。

此外，官职证明书验证服务器证明书的有效期限，为自官职证明书验证服务器证明书的有效日起算 1 年。

④ 基于以下用途给予发行 OCSP 响应器证明书。
- ・验证签名者等通过 OCSP 响应器查询方法，提供电子证明书的有效性确认方法。

此外，OCSP 响应器证明书的有效期限为自 OCSP 响应器证明书有效日起算 1 年。

1-3-3 运用章程的负责人

本运用章程的负责人为北海道知事。

1-3-4 联系地址

有关本运用章程查询窗口如下所示。

北海道
住　　址：　邮编 060-8588 北海道札幌市中央区北 3 条西 6 丁目
部　　门：　综合政策部科学和 IT 促进局信息政策课
受理时间：　上午 8 点 45 分～下午 5 点 30 分
电　　话：　011-204-5171
传　　真：　011-232-3962
电子邮箱地址：sogo.joho2@pref.hokkaido.lg,jp

2．一般规定

2-1 义务

2-1-1 总务大臣的义务

(1)指定认证机关的指定、停止废止的批准、解除指定、向北海道知事的通知或公开
(2)监督指定认证机关时必要的命令
(3)针对指定认证机关要求必要的汇报以及实施入内检查
(4)指定认证机关的干部选任或免职许可及免职命令
(5)指定认证机关制定的认证事务管理章程以及项目计划的认可及更改命令
(6)针对指定认证机关作出的处罚等相关的不服陈情给以应对
(7)制定伴随认证业务事宜的设施等的技术标准
(8)涉及认证业务的技术评估相关的调查、研究
(9)认定验证签名者所涉及的事务
(10)要求验证签名者等针对业务进展状况作必要的汇报
(11)向使用者告知、宣传有关公共性个人认证服务的资讯

2-1-2 北海道知事的义务

(1)基于市町村长针对申请者的姓名・出生年月日・性别・住址（以下称「基本 4 信息（申请者为外国籍居民时，在其住民票上记载该外国籍居民的通称的情况下，则需基本 4 信息及通称。以下同。）」以及公钥的告知，给予发行电子证明书
(2)出示北海道 CA 与个人认证 BCA 之间的相互认证有关的正确资讯以及交换相互认证证明书
(3)发行个人签名证明书
(4)发行链接证明书
(5)发行运行用的关联证明书
(6)收到使用者的网上失效申请时，进行本人核实及制作失效资讯
(7)制作使用者在市町村窗口进行失效申请的失效资讯
(8)制作因使用者的住址或者姓名变更，以及死亡等事实发生时的失效资讯
(9)当发现使用者的电子证明书的相关证明项目与该电子证明书的记录有出入时，制作失效资讯。
(10)北海道知事的私钥处于危险时(指因私钥丢失、泄漏等无法管理、或者已持有怀疑时。以下同)，制作出自该私钥发行的所有证明书的失效资讯以及向个人认证 BCA 的汇报。
(11)向验证签名者提供电子证明书有效性的确认方法（指使用 OCSP 协议来回答失效资讯查询的方法（以下称「OCSP 响应器查询方法」。）和失效记录（CRL/ARL）提供方法）
(12)向使用者提供确认国家或地方公共团体的官职或职责证明书有效性的方法
(13)制作和公布失效资讯以及失效资讯文件的提供状况报告
(14)针对认证业务资讯的公开请求给以公开
(15) 针对认证业务资讯的更正请求等给以更正
(16)北海道知事密钥对的设置与私钥的安全管理
(17)实施监查、根据监查结果进行改善等
(18)设置实施认证业务设备
(19)依照本运用章程实施有关各种证明书的发行、更新以及失效业务
(20)针对发行完毕的所有证明书以及失效记录(CRL/ARL)在必要期间内给以保管，并且，针对各证明书的发行、更新以及失效相关的监察日志及保管资讯给以必要期间内的保管
(21)随时确定系统的运转监测正常进行，以 24 小时稳定运行为目标
(22)有效期为 72 小时的失效记录（CRL/ARL）相关的失效资讯，每 24 小时发行一次
(23)应对使用者的投诉及咨询

(24)向指定认证机关委托认证事务以及向总务大臣汇报、公开
(25)向指定认证机关通知有关变动等的失效资讯
(26)根据需要向指定认证机关下达指示
(27)要求指定认证机关作必要的汇报以及实施入内检查
(28)解除指定认证机关的委托以及向总务大臣汇报、公开
(29)针对指定认证机关所设定的电子证明书发行手续费以及提供资讯手续费给以批准
(30)实施有关与指定认证机关的认证事务费用协议并交付
(31)指定认证机关停止或废止认证事务时，进行认证事务的实施
(32)与验证签名者签定协议
(33)要求验证签名者针对业务实施情况做出必要的汇报
(34)对认证业务相关的资讯进行适当管理
(35)做好认证业务资讯的保密工作
(36)向使用者告知、宣传有关公共性个人认证服务的资讯
(37)制订及确定本运用章程

2-1-3 市町村长的义务

(1)实施发行时或失效时的申请者，以及失效申请者的本人核实(是否存在，是否为本人)
(2)确认代理申请者为真正代理人
(3)针对失效申请，确认失效事项
(4)确认其他申请手续的妥当处理
(5)提供设置具有适当强度配对锁的装置（设置使用者的密钥对生成装置，以下称「密钥对生成装置」。）
(6)向北海道知事通知申请者的基本 4 信息及申请者的公钥
(7)向北海道知事通知失效申请
(8)向使用者交付电子证明书以及北海道知事的个人签名证明书
(9)向申请者・使用者说明电子证明书的使用目的的限制，以及有关不正当使用时的惩罚条例
(10)做好密钥对生成装置、受理窗口的终端机等系统的保养・安全管理
(11)应对监察以及根据监察结果进行改善
(12)妥当处理认证业务的相关资讯
(13)做好认证业务资讯的保密工作
(14)向申请者征收发行电子证明书的发行手续费
(15)受理认证业务资讯的公开要求以及更正要求
(16)按照使用者的申请进行密码初始化、解冻（指作为防止滥用措施，5 次以上密码输入错误时 IC 卡无法使用这一状态的解除）、消除密钥对等
(17)帮助使用者取得使用者终端机用的使用者客户软件（使用电子证明书必需的软件）
(18)应对使用者的投诉及咨询
(19)向使用者告知、宣传有关公共性个人认证服务的资讯

2-1-4 指定认证机关的义务

(1)受北海道知事的委托，实施认证事务（实施本运用章程「2-1-2 北海道知事的义务」中从(1)到(13)、(16)以及(18)到(22)）
(2)制定认证事务管理章程
(3)制订项目计划及收支预算并提交项目报告及收支结算报告
(4)设置认证业务资讯保护委员会
(5)妥当处理认证业务相关的资讯
(6)做好认证业务资讯的保密工作

(7)针对认证业务资讯的公开请求给以公开
(8)针对认证业务资讯的更正请求等给以更正
(9)应对使用者的投诉及咨询
(10)向验证签名者等征收资讯提供手续费

2-1-5 使用者的义务

(1)在电子证明书的发行申请书、失效申请书等上记载正确的内容
(2)做好私钥以及储存该私钥的 IC 卡的安全管理
(3)定期更改且安全管理用来激活储存在 IC 卡里的私钥的密码
(4)私钥处于危险时立即申请失效
(5)电子证明书禁止使用于其他目的
(6)缴纳发行手续费

2-1-6 验证签名者的义务

(1)利用北海道 CA 发行的电子证明书，验证所附的数字签名
(2)验证北海道 CA 发行的电子证明书（该电子证明书是否为北海道知事所发行、该电子证明书是否已失效）
(3)通过验证使用者的网上申请・呈报等所执行的数字签名，来进行使用者的认证，除此之外的目的则禁止使用电子证明书
(4)接受失效资讯及失效资讯文件的提供时，与北海道知事签订协议
(5)接受并实施总务大臣以及北海道知事的汇报要求
(6)做好失效资讯等的保密工作并妥善使用
(7)确保失效资讯等的安全
(8)缴纳资讯提供手续费

2-1-7 验证团体签名者的义务

(1)确认北海道 CA 发行的电子证明书尚未失效
(2)通过验证从验证签名者那里取得的有关使用者的数字签名，来进行使用者的认证，除此之外的目的则禁止使用电子证明书
(3)接受失效资讯及失效资讯文件的提供时，与北海道知事签订协议
(4)接受并实施总务大臣以及北海道知事的汇报要求
(5)做好失效资讯等的保密工作并妥善使用
(6)确保失效资讯等的安全
(7)缴纳资讯提供手续费

2-1-8 确认签名者的义务

(1)利用北海道 CA 发行的电子证明书，验证所附的数字签名
(2)验证北海道 CA 发行的电子证明书（该电子证明书是否为北海道知事所发行、该电子证明书是否已失效）
(3)通过验证使用者的网上申请・呈报等所执行的数字签名，来进行使用者的认证，除此之外的目的则禁止使用电子证明书
(4)对从验证团体签名者得到的答复给以保密并妥善使用
(5)确保从验证团体签名者得到答复的安全

2-1-9 信息储藏库的义务

北海道 CA 制作失效记录（CRL/ARL）之后，将其公开于信息储藏库，以使验证签名者等可确认电子证明书的有效性。

此外，保管其他资讯并公开。

2-2 责任

2-2-1 总务大臣的责任

总务大臣，遵照根据法的规定，肩负进行指定认证机关的指定，管理・监督指定认证机关实施安全并妥当的认证事务的责任。

2-2-2 北海道知事的责任

北海道知事，针对使用者及验证签名者等，在履行发行电子证明书、相互认证证明书、个人签名证明书、链接证明书、其他业务上所需证明书以及制作涉及这些证明书的失效记录（CRL/ARL），并提供确认电子证明书以及官职或职责证明书有效性的方法等业务时，需遵照本运用章程妥当执行业务。

此外，在委托指定认证机关执行认证业务时，肩负管理・监督指定认证机关实施安全并妥当的认证事务的责任。

2-2-3 市町村长的责任

市町村长，在履行发行电子证明书、受理失效申请及本人核实等业务时，需遵照本运用章程妥当执行业务。

2-2-4 指定认证机关的责任

指定认证机关，受北海道知事的委托履行以下的认证事务。针对使用者及验证签名者等，在履行发行电子证明书、相互认证证明书、个人签名证明书、链接证明书、其他业务上所需证明书以及制作涉及这些证明书的失效记录（CRL/ARL），并提供确认电子证明书以及官职或职责证明书有效性的方法等业务时，需遵照本运用章程妥当执行业务。

2-2-5 使用者的责任

使用者，遵照本运用章程利用本服务。

2-2-6 验证签名者的责任

验证签名者，遵照本运用章程验证电子证明书。

2-2-7 验证团体签名者的责任

验证团体签名者，遵照本运用章程确认电子证明书的有效性。

2-2-8 确认签名者的责任

确认签名者，遵照本运用章程验证电子证明书。

2-3 财务上的责任

当毫无理由将责任归咎于北海道 CA，由此行为产生的损失，北海道知事将不负任何损失赔偿责任。

当出于某种原因北海道 CA 需要担当责任时，北海道知事在法令等规定范围内实施损害赔偿。

2-4 说明与执行

2-4-1 适用法令

遵循根据法和其他相关法令。

2-4-2 服务的分工或合并、运用体制等的变更与告知

营运体制等有变更时，立即通过以下方法向使用者、验证签名者公布。

・协议会的网站(Web)

・北海道的网站(Web)

此外，指定认证机关更改名称或者变更主要事务所的所在地时，需向总务大臣及北海道知事呈报。

2-4-3 接受监察命令和汇报工作及入内检查

在总务大臣下达监察方面必需的，有关执行认证事务的命令时，以及北海道知事下达妥当执行认证事务的指示时，指定认证机关必需接受该命令和指示。

此外，总务大臣及北海道知事要求汇报有关认证事务执行情况或者要求入内检查时，指定认证机关必需接受该要求。

2-4-4 解决纠纷的手续

有关本运用章程发生的诉讼，所有当事人需将札幌地方法院作为一审的专门管辖法院。

2-5 费用

电子证明书的发行、失效资讯及失效资讯文件的提供及认证业务资讯的公开等相关费用，按照根据法的规定来决定。

2-6 公开与信息储藏库

2-6-1 关于北海道 CA 信息的公开

北海道 CA 将以下资讯公布于协议会的网站(Web)上。

・根据法及相关法令

・本运用章程

・与北海道 CA 相互认证的 CA 名称

・与北海道 CA 的相互认证被取消的 CA 名称

・北海道知事的私钥危殆化时的相关资讯 等

北海道 CA 将以下资讯公布于公共性个人认证服务的信息储藏库上

・个人签名证明书

・相互认证证明书

・链接证明书

・个人签名证明书、相互认证证明书、链接证明书的失效记录（ARL）

・使用者的电子证明书等的失效记录（CRL）

2-6-2 公开频率

公开资讯的更新频率如下所示。

・根据法及相关法令和本运用章程等的章程最新版随时载于网站(Web)。
・个人签名证明书、相互认证证明书、链接证明书一旦发行・更新则立即公开。
・失效记录（CRL/ARL）每天更新一次。

2-6-3 公开资讯的访问限制

遵照根据法及相关法令和本运用章程的章程，不设访问限制。

此外，针对信息储藏库的以下资讯也不设访问限制。

・个人签名证明书
・相互认证证明书
・链接证明书
・个人签名证明书、相互认证证明书、链接证明书的失效记录（ARL）
但对信息储藏库上公开的使用者电子证明书的失效记录（CRL），实行访问限制。

2-6-4 信息储藏库相关事项

信息储藏库一天 24 小时，一年 365 天开放使用。但因定期保养，有暂时无法使用的可能。

2-7 执行情况的监察

2-7-1 执行情况的监察频率

北海道知事实施一年一度的由监察人进行的定期执行情况监察，并且根据需要实施定期监察以外的临时监察。

2-7-2 监察人的识别与资格

北海道 CA 的监察，由精通监察业务及认证业务者执行。

2-7-3 监察人与被监察部门的关系

北海道知事，选任与北海道 CA 无利害关系的人作为监察人。

2-7-4 监察项目

认证业务遵照根据法及相关法令，且遵照本运用章程来执行，以此作为核心实施监察。

2-7-5 监察结果的处理

监察结果，由监察人以监察报告的形式提交给北海道知事。北海道知事根据情况需要，向各市村町长、指定认证机关告知监察报告。

2-7-6 监察指正事项的应对

指定认证机关确认监察指正事项，根据重要程度或紧急程度实施妥当的应对措施。评估其结果之后，向北海道知事汇报。北海道知事则确认指定认证机关针对监察指正事项所实施的应对措施。

2-8 保密与保护个人信息

2-8-1 视为机密的资讯与个人信息的处理

北海道 CA，将因信息泄漏而导致有可能损害北海道 CA 认证业务信誉的资讯视为机密资讯

经管。并且妥当保护使用者的个人信息。

针对包含视为机密的资讯及使用者个人信息的资讯，决定管理包含该资讯在内的资料及电磁储存介质的负责人（按照本运用章程「5-2-1-1 北海道 CA 的工作人员」规定，作为认证局管理负责人），进行安全管理。如果发生个人信息泄漏情况时，根据所定手续另行寻找对策。

2-8-2 无需视为机密的资讯

北海道 CA 保管的资讯中，个人签名证明书、链接证明书、相互认证证明书、官职证明书验证服务器证明书、OCSP 响应器证明书、这些证明书的失效资讯、本运用章程等，作为公开资讯明确公布，不视为机密资讯。

2-8-3 证明书失效资讯的公布

北海道 CA 对所发行的个人签名证明书、链接证明书、相互认证证明书及营运方面的相关证明书，其失效资讯给以公布。无需公布具体失效理由。此外，电子证明书的失效资讯按照根据法，仅提供给验证签名者。

2-8-4 针对执法机关的资讯公开

无任何规定。

2-8-5 民事手续方面的资讯公开

无任何规定。

2-8-6 基于证明书使用者要求的资讯公开

使用者要求公开自己的认证业务资讯时，在核实本人的基础上给以公开。

2-8-7 基于其他理由的资讯公开

无任何规定。

2-8-8 基于证明书使用者要求的资讯更正等

使用者要求更正自己的认证业务资讯时，在核实本人的基础上给以更正。

2-9 知识产权

无任何规定。

3．识别与认证

3-1 初次申请发行证明书

3-1-1 名称形式

电子证明书的发行名义人名称及使用者名称，按照 X.500 识别名（DN：Distinguished Name）的形式设定。

3-1-2 名称意义的相关事项

电子证明书的发行名义人名称，根据知事的职称来记载。

并且，储存在电子证明书上的使用者基本 4 信息，记载在电子证明书的扩展区域内。储存使用者基本 4 信息用的扩展区域资讯如下所示。

subjectAltName		
	common Name	姓名（申请者为外国籍居民，且在其住民票上记载该外国籍居民的通称的情况下，姓名与通称）
	dateOfBirth	出生年月日
	gender	性别
	address	住址

3-1-3 说明名称形式的规则

遵照 X.500 识别名的章程。

3-1-4 名称的一致性

北海道 CA 发行的电子证明书 subject 栏位的名称需统一使用。

3-1-5 关于名称纠纷的解决方法

无任何规定。

3-1-6 商标的认识・认证・作用

无任何规定。

3-1-7 记录在电子证明书扩展区域的名称种类和形式

使用者的姓名、通称（仅限于接受电子证明书交付的人是外国籍居民，且在其住民票上记载该外国籍居民的通称的情况。）、住址、出生年月日、性别等均使用汉字、平假名、片假名、英文字母及阿拉伯数字等记录。

3-1-8 记录在电子证明书扩展区域的名称记录方法相关规则

记录姓名等使用的汉字，仅限于使用住址所在地的市村町受理窗口的终端机所采用的文字种类（JISX0208、JISX0212）之汉字。

姓名等存在不能使用的汉字时，则按照使用者的选择，使用现有的相似汉字（以下称「代用文字」。）

使用代用文字时，需在扩展区域加以注明。

3-1-9 使用者的识别与认证相关事项

初次发行申请按照以下方法进行申请者本人核实。当本人核实中发现疑点时，则不给予发行电子证明书。

① 发行申请书上填写的基本 4 信息与住民基本台帐的记录事项核对，确认该申请者即为住民基本台帐上所记录的人。（实际存在的确认）

② 根据申请者出示的公共机关发行的，附有照片的身份证明(根据法规则第 6 条第 1 项规定的证明材料)，来确认申请者即为住民基本台帐上所记录的人(本人的确认)。

3-1-10 代理申请时的识别与认证相关事项

由代理人申请时，通过以下方法进行代理人的本人核实及确认代理权的拥有。

① 确认持有申请者本人的签名及盖章的委托书，该印章的印鉴证明书，书面查询该申请者时其答复资料及住址所在地市町村长认可的资料

② 代理人的本人核实，由出示公共机关发行的附有照片的身份证明等进行确认（根据法规则第 5 条第 1 项规定的证明材料)

3-1-11 确认持有私钥证据的方法

根据申请者使用住址所在地的市町村所设置的密钥对生成装置，且遵照根据法及相关法令设置密钥对，以此进行确认。

3-2 电子证明书的更新

电子证明书更新时，通过以下方法进行使用者本人核实。当本人核实中发现疑点时，则不给予更新电子证明书。

① 更新申请书上填写的基本 4 信息与住民基本台帐的记录事项核对，确认该申请者即为住民基本台帐上所记录的人。（实际存在的确认）

② 根据申请者出示的公共机关发行的，附有照片的身份证明来确认申请者即为住民基本台帐上所记录的人(本人的确认)。

然而，对因更新致使电子证明书失效的私钥，使用者需按规定方法消除。

3-3 失效后的重新发行

实施与初次申请发行时相同的本人核实手续。

3-4 失效申请

3-4-1 停止使用服务的失效申请

通过使用者的私钥，进行附有数字签名的网上申请，或者在住址所在地市町村的窗口进行书面申请。

针对使用者的本人核实，网上申请时通过验证数字签名来核实。在住址所在地市町村的窗口书面申请时，实施与发行电子证明书时相同的本人核实手续。

3-4-2 使用者的私钥危殆化时的失效申请

迅速前往住址所在地的市町村窗口，进行书面失效申请。

针对使用者的本人核实，实施与发行电子证明书时相同的本人核实手续。

4．运用事项

4-1 电子证明书的发行申请

4-1-1 发行申请・受理手续

电子证明书的发行申请・受理手续如下进行。

① 申请者提交住址所在地市町村的发行申请书时，同时提交 IC 卡。需更新时，提交储存电子证明书的的 IC 卡。

② 住址所在地的市町村长通过核对住民基本台帐的记录内容，确认使用者实际存在的同时，还需根据出示公共机关发行的，附有照片的驾驶执照、护照等身份证明，确认申请者为本人。当本人核实中发现疑点时，则不给予发行电子证明书。

③ 申请者通过使用住址所在地的市町村窗口配备的密钥对生成装置，设置密钥对。将设置的密钥对中的公钥通知住址所在地的市町村窗口。

此外，通过以下手续，可由代理人进行申请。当（１）或（２）发现疑点时，则不给以发行电子证明书。

（１）代理人，需提交或出示有申请者本人的签名及盖章的委托书(仅限于同时附有该印章的印鉴证明书的情况）以及可以确认代理人本人的驾驶执照，护照等。

（２）针对电子证明书的发行申请，为确认申请者是本人以及该申请出自本人意愿，根据邮件或其他由住址所在地市町村长认可的方法，实施对该申请者的书面查询，代理人则需提交该答复资料，并出示住址所在地市町村长认可的资料。

（３）代理人，使用密钥对生成装置，设置密钥对，公钥需通知住址所在地市町村。然而，密码的输入（打开私钥）由住址所在地的市町村长实施。

4-1-2 发行申请书的格式、必要记载事项

发行申请书上记载以下事项。

・申请的年月日

・姓名（注音假名)、通称（仅限于接受电子证明书交付的人是外国籍居民，且在其住民票上记载该外国籍居民的通称的情况。)、住址、出生年月日及性别，和与姓名、通称及住址相关的代用文字

・代理人申请时，除以上事项之外添加代理人的姓名、住址

4-1-3 私钥的电磁记录介质

储存在具有防短波功能的 IC 卡内。

4-2 电子证明书的发行

4-2-1 发行手续

电子证明书的发行手续如下所示。

①　住址所在地的市町村长通知北海道知事有关申请者的基本 4 信息及公钥。

③　北海道知事发行电子证明书，通知住址所在地的市町村长。

4-2-2 电子证明书的形式

依照 ITU-T 劝告 X.509 (03/2000)，在扩展区域使用汉字、平假名、片假名、英文字母及阿拉伯数字记录使用者的姓名、通称、住址、出生年月日和性别。

此外，在扩展区域记录的姓名、通称及住址使用了代用文字时，需在扩展区域加以注明。

subjectAltName		
	commonName	姓名（申请者为外国籍居民，且在其住民票上记载该外国籍居民的通称的情况下，姓名与通称）
	dateOfBirth	出生年月日
	gender	性别
	address	住址
	substituteCharacterOfCommonName	姓名代用文字的使用信息
	substituteCharacterOfAddress	住址代用文字的使用信息

4-2-3 发行申请的拒绝

在符合以下事由的情况下，北海道知事将拒绝发行申请。

・已取得有效的电子证明书，且尚未登载在失效记录（CRL）上

然而，万一出现重复发行的情况时，北海道知事在了解清楚之后立即将最新发行日的电子证明书给予失效。

4-3 电子证明书的交付

4-3-1 交付手续

电子证明书的交付手续如下所示。

① 住址所在地的市町村长，在申请者的 IC 卡上储存电子证明书及北海道知事的个人签名证明书

② 住址所在地的市町村长，向申请者告知利用本服务的相关注意事项，同时交付电子证明书的复印件

4-3-2 告知事项

住址所在地的市町村长向申请者告知以下事项。

・私钥、其电磁储存介质的 IC 卡、激活 IC 卡的密码，均属使用者的责任范围，需严加管理

・私钥或者其电磁储存介质 IC 卡丢失・被盗等的情况下，立即向住址所在地的市町村窗口呈报，进行失效申请，不得延误

4-4 电子证明书的失效及暂停使用

4-4-1 职权失效的事由

4-4-1-1 职权失效的事由

电子证明书的职权失效事由如下所示。

・使用者的基本 4 信息的变更

・发现使用者电子证明书所记载的事项，与该电子证明书的有关使用者的住民票记载事项有出入时

・发现电子证明书的重复发行时

・北海道知事的私钥危殆化

4-4-1-2 有权使证明书失效者

北海道知事有权行使。

4-4-1-3 北海道知事的私钥危殆化时的失效手续

北海道知事的私钥发生危殆化，北海道知事行使职权将在该私钥上签名的所有电子证明书失效，记录在失效记录（CRL/ARL）上的同时，还需通过网站(Web)等给予公布。

4-4-2 出自使用者的失效申请

4-4-2-1 出自使用者的失效申请事由

申请失效的理由如下所示。

・使用者希望停止使用本服务的申请

・使用者的私钥面临危殆化的申请

4-4-2-2 停止使用服务的失效申请手续

通过以下的任何一种方法，可办理停止使用本服务的失效手续。

① 受理附有数字签名的网上申请。失效申请已受理之事宜会网上通知使用者。

② 住址所在地的市町村窗口受理书面失效申请。委托北海道知事进行失效处理。失效申请已受理之事宜会记载在书面上交付给使用者。

4-4-2-3 使用者的私钥面临危殆化等情况下的失效申请手续

使用者的私钥面临危殆化等情况下的失效申请手续如下所示。

① 住址所在地市町村受理书面失效申请。

② 委托北海道知事进行失效处理。失效处理已完成之事宜会记载在书面上交付给使用者。

4-4-2-4 使用者的电子证明书失效后的恢复方法

经过失效处理的电子证明书，不予进行恢复。通过重新办理申请手续，发行新的电子证明书。

4-4-2-5 使用者的私钥处于危殆化情况的恢复方法

通过重新办理申请手续，发行新的电子证明书。

4-4-3 失效记录（CRL/ARL）的注意事项

将截止到指定时间受理完毕的失效资讯，反映到每天制作一次的最新失效记录（CRL/ARL）上，制作好的失效记录（CRL/ARL）迅速向被认可的验证签名者等公布。

并且，提供给验证签名者等的失效记录（CRL/ARL），一天 24 小时，一年 365 天开放使用。但因定期保养，有暂时无法使用的可能。

4-4-4 失效资讯的提供方法

4-4-4-1 失效资讯的提供方法

作为确认电子证明书有效性的方法，提供以下 2 种方法。

① OCSP 响应器查询方法（使用 RFC2560 所规定的 OCSP 协议）

② 失效记录（CRL/ARL）的提供方法（使用 RFC2251 所规定的 LDAPV3 协议）

4-4-4-2 OCSP 响应器查询方法的答复内容

针对识别电子证明书的发行人资讯和根据序列号进行的网上查询，分清在查询这段时间该电子证明书是否有效、去向不明以及是否失效，如已经失效的情况下，答复其失效事由。失效事由如下所示

失效事由		
1	keyCompromise	使用者的私钥处于危殆化情况。
2	cACompromise	北海道知事的私钥处于危殆化情况。
3	affiliationChanged	电子证明书的記載内容发生了变更。
4	superseded	电子证明书已更新。
5	cessationOfOperation	电子证明书已不需要(不再使用。)

4-4-4-3 OCSP 响应器查询方法事项

事先向北海道知事呈报，以取得访问权。

4-4-4-4 失效记录（CRL/ARL）提供方法的答复内容

失效记录（CRL/ARL）的格式遵循 ITU-T 劝告 X.509(03/2000)。

失效记录（CRL）原则上以市町村为单位制作成分类 CRL，记载已失效的电子证明书序列号、失效事由（与本运用章程「4-4-4-2 OCSP 响应器查询方法的答复内容」的失效事由相同）及失效年月日。验证签名者等适当获取储存在信息储藏库里的失效记录（CRL/ARL），进行电子证明书的验证。

4-4-4-5 提供失效记录（CRL/ARL）的必要事项

需事先向北海道知事呈报，以取得访问权。

4-4-5 暂停使用相关事项

北海道知事发行的电子证明书不履行暂停使用。

4-4-6 暂停使用申请者

无任何规定。

4-4-7 要求暂停使用手续

无任何规定。

4-4-8 暂停使用期间

无任何规定。

4-4-9 失效记录（CRL/ARL）的发行频率

有效期为 72 小时的失效记录（CRL/ARL）每 24 小时发行一次。当北海道知事的私钥处于危险状况时，立即进行失效记录（CRL/ARL）的发行。

4-4-10 发行失效记录（CRL/ARL）的最长拖延时间

最后发行的失效记录（CRL/ARL），在其有效期满之前即发行新的的失效记录（CRL/ARL）。

4-4-11 失效记录（CRL/ARL）的确认

验证签名者必需根据北海道知事发行的失效记录（CRL/ARL），确认电子证明书的有效性。

4-5 制作有关失效资讯等的提供情况报告

指定认证机关，针对所保存的失效资讯及失效资讯文件的提供情况，制作成报告。指定认证机关必须将该报告公布于公报，且放置在指定认证机关的办公室 5 年，供一般阅览。

报告的记载事项如下所示。

・失效资讯等的提供对象
・失效资讯等的提供年月
・提供的失效资讯件数
・失效资讯等的提供方法

4-6 相互认证证明书的发行申请

向个人认证 BCA 申请发行相互认证证明书，按照个人认证 BCA 所规定的步骤进行。

4-7 相互认证证明书的发行

北海道知事，根据规定手续，确认营运个人认证 BCA 者的真伪。按照个人认证 BCA 规定手续完成连接试验后，针对个人认证 BCA 提出的发行证明书的要求，发行附有北海道知事签名的相互认证证明书。

4-8 相互认证证明书的领取

北海道知事，根据规定手续，接受个人认证 BCA 发行的相互认证证明书，将领取书交给个人认证 BCA。同样，北海道知事给个人认证 BCA 发行的相互认证证明书，按照规定手续交给个人认证 BCA，收取领取书。通过这些领取的确认，完成相互认证证明书的相互接收。

此外，北海道知事把与个人认证 BCA 相互交换的相互认证证明书进行配套，制作配套相互认证证明书，申报在信息储藏库里。

4-9 相互认证证明书の更新

以下(1)～(4)的情况下，北海道知事需对相互认证证明书及配套相互认证证明书进行更新。

在此进行的更新相互认证证明书的发行申请，发行及领取的各个手续，遵循本运用章程「4-6 相互认证证明书的发行申请」、「4-7 相互认证证明书的发行」及「4-8 相互认证证明书的领取」规定。此外，立即将信息储存库里的配套相互认证证明书调换成最新的。

(1) 个人认证 BCA 发行的相互认证证明书即将过期时

(2) 发行给个人认证 BCA 的相互认证证明书即将过期时

(3) 个人认证 BCA 发行的相互认证证明书的记载内容发生变更时

(4) 发行给个人认证 BCA 的相互认证证明书的记载内容发生变更时

4-10 相互认证证明书的失效

4-10-1 失效事由

当北海道 CA 或者个人认证 BCA 发生以下情况时，北海道 CA 需将发行给个人认证 BCA 的相互认证证明书失效、个人认证 BCA 同样将发行给北海道 CA 的相互认证证明书失效。

・私钥危殆化
・相互认证证明书的更新

・相互认证的结束（包含因违反相互认证基准，结束相互认证的情况）

4-10-2 失效申請人

个人认证 BCA 向北海道 CA 提出的失效申请，由个人认证 BCA 的负责人执行。
北海道 CA 向个人认证 BCA 提出的失效申请，由北海道知事执行。

4-10-3 失效申请及失效处理步骤

相互认证证明书的失效申请，按照个人认证 BCA 规定的手续进行。

4-11 安全性监查手续

4-11-1 安全性监查程序

内部监查人(参照本运用章程「5-2-1 具有良好信誉的工作人员与其职责」)将记录北海道 CA 系统及信息储藏库发生事态的日志，与业务实施记录核对，进行确认是否有非法运作等异常事态的安全性监查。

4-11-2 监查日志所记录的资讯

将北海道 CA 系统及信息储藏库的安全性相关的重要事项作为对象，记录访问日志及操作日志等的监查日志。

・关于发行手续的操作・运转日志
・关于失效手续的操作・运转日志
・关于确认有效性的所有访问・运转日志
・关于北海道知事的密钥对设置的操作日志
・针对系统、各种帐簿等的访问日志
・北海道 CA 的设备房间的出入记录

监查日志包括以下信息。

・事态及处理的种类
・发生时间
・处理结果
・事态发生原由的识别信息（操作员 ID、系统名称等）

4-11-3 监查日志的检查周期

内部监查人以周为单位进行安全性监查。

4-11-4 监查日志的保管期间

保管期间为一年。

4-11-5 监查日志的保护

针对监查日志，实施防止窜改措施。而且监查日志的备份以月为单位储存于外部储存设备，在具有适当进出管理的房间内，将其保管在可以上锁的保管库里。

监查日志的阅览及删除由内部监查人妥善实施。

4-11-6 备份监查日志的步骤

以日为单位进行备份，以月为单位储存在外部储存设备里。

4-11-7 检查监查日志的通知

进行监查日志的检查，不通知导致该事态发生的人。

4-11-8 脆化性的验证

根据监查日志的检查，针对运行方面及系统方面的脆化性进行评估。

4-11-9 监查日志的收集系统

监查日志的收集机能，即作为北海道 CA 的一项机能，从系统启动开始，将有关安全的重要事态作为监查日志进行收集。

4-12 记录的保管（存档）

4-12-1 使用纸张保管的资讯

4-12-1-1 保管资讯的种类

以下资讯进行保管

（北海道知事）

・制定本运用章程的相关资料
・举行主要典礼的相关资料
・与验证签名者等的协定相关资料
・认证业务资讯的公开・更正等的相关资料
・监查报告　等

（指定认证机关）

・指定认证机关的指定・变更的相关资料
・认证事务管理章程
・设备及安全措施的相关资料
・项目计划・收支预算的相关资料
・项目报告・收支结算报告
・认证业务资讯的公开・更正等的相关资料
・失效资讯及び失效资讯文件的提供状况报告
・手续费的相关资料　　等

（市町村长）

・申请发行电子证明书的相关资料（发行申请书等）
・申請电子证明书失效的相关资料（失效申请书等）
・认证业务资讯的公开・更正等的相关资料　等

4-12-1-2 保管期间

保管期间为 10 年。然而申请发行电子证明书的相关资料为 13 年。

4-12-1-3 保管资讯的保护

保管在指定认证机关的资讯，在实施防止窜改措施的同时，还需保管在具有适当的进出管理的房间里设有可以上锁的保管库内，并实施顾及温度、湿度等环境因素的保护措施。保管在市町村及都道府县的资讯，需保管于适当的地方。

4-12-1-4 保管资讯的验证

每年实施一次确认记载保管资讯的纸张状态、可阅读性。

4-12-2 以数码资料形式保管的资讯

4-12-2-1 保管资讯的种类

以下资讯保管在指定认证机关

・失效申请书（向北海道知事网上申请时）
・电子证明书
・相互认证证明书
・个人签名证明书
・链接证明书
・官职证明书验证服务器证明书
・OCSP 响应器证明书
・失效资讯
・失效记录（CRL/ARL）
・失效资讯文件
・失效记录（CRL/ARL）提供方法的使用记录
・OCSP 响应器查询方法的使用记录
・各种日志（监视用日志、启动停止日志、操作日志）等

4-12-2-2 保管期间

保管期间为 10 年。然而，已发行的电子证明书为 13 年，失效资讯则从该失效资讯的申报日起，到该失效记录的相关电子证明书之有效期满日为止。

4-12-2-3 保管资讯的保护

针对保管资讯，在实施访问限制的同时，还需实施防止窜改措施。

保管资讯以月为单位储存于外部储存设备，保管在具有适当进出管理的房间内且可以上锁的保管库里。

4-12-2-4 备份保管资讯的程序

保管资讯以日为单位进行备份，以月为单位储存在外部储存设备里。

4-12-2-5 记录上附加时间戳的注意事项

针对保管资讯，需附加时间戳。

4-12-2-6 保管资讯的验证

对存有保管资讯的外部储存设备，每年实施一次确认其可阅读性。

4-13 北海道知事的锁的更新

每 5 年一次进行北海道知事密钥对的更新。

密钥对更新时，发行构筑新旧公钥认证路径的链接证明书，公开在信息储藏库上。

4-14 锁面临危殆化时与损害时的修复

4-14-1 硬件、软件或者资料受到损害时的应对措施

硬件，软件或者资料受到损害时，利用备份硬件、软件以及资料迅速进行修复工作。

4-14-2 北海道知事的私钥处于危殆化时的应对措施

应对措施如下所示。

・停止发行电子证明书的业务

・将出自该私钥签名的所有电子证明书、相互认证证明书等失效，记录在失效记录（CRL/ARL）上并公布

・通知个人认证 BCA

4-14-3 发生灾害时设备的确保

因灾害导致设备受损时，确保预备机器，利用备份资料进行运作。

4-15 投诉・咨询的处理

针对认证事务等相关的投诉・咨询，北海道知事、指定认证机关及市町村长必须努力进行适当且迅速的处理。

4-16 系统运用

履行安全且妥当的系统运用。详情另行规定。

4-17 认证事务的结束

无任何规定。

4-18 认证事务的停止、废除

指定认证机关，在停止或废除全部或部分认证事务等的情况下，必须得到总务大臣的批准。而且，由此致使北海道知事实施认证事务的情况时，指定认证机关必须进行以下事项。

・向北海道知事交接必须交接的认证事务。

・将必须交接的认证事务相关的帐簿、材料、资料及电磁储存介质等交给北海道知事。

此外，还需执行总务大臣或北海道知事认为有必要的事项。

5．实体方面、手续方面、人事方面的安全管理

5-1 实体方面的安全管理

5-1-1 北海道 CA

5-1-1-1 设施的位置和建造

北海道 CA 的设施需设置在不易受水灾、地震、火灾和其它灾害影响的地方，建筑构造上采取防震、防火及防止非法进入等措施。此外，所使用的机器等需设置在能防灾及防止非法进入的安全之地。

5-1-1-2 实体的进出管理

按照北海道 CA 设施内的各个房间执行业务的重要程度，实施多种安全等级的进出管理。有操作权限的人根据可以识别的 IC 卡及生物体认证装置进行认证。

各房间的进出权限，则根据本运用章程「5-2 手续方面的安全管理」规定的各个工作人员的业务情况，由北海道 CA 的认证管理负责人授予。

针对北海道 CA 的设施，安置监视人员，通过监视系统实施 24 小时、365 天的监视。

5-1-1-3 电力与空调

北海道 CA 不仅要确保机器运作所需的充分容量的电源，还要采取针对突然断电、停电、电压・频率变化的相应措施。当发生商业用电源断绝供给的情况时，需在所定时间内转换成由发电机发电的电源供给。

通过设置空调设备，适当维持机器等的运作环境及工作人员的工作环境。

5-1-1-4 防汛措施

设有北海道 CA 设备的建筑物、室内需设置漏水检测器，对房顶、地板采取防水措施。

5-1-1-5 防震措施

设有北海道 CA 设备的建筑物需具备防震构造,采取防止机器･用具的翻倒及掉落等措置。

5-1-1-6 防火措施

设有北海道 CA 设备的建筑物需具备防火构造，房间划分防火区，置备灭火设备。

5-1-1-7 防电磁波措施

根据北海道 CA 设施内的各个房间所执行的业务重要程度，置备防止电磁波攻击以及防止电磁波引起的信息泄漏设备。

5-1-1-8 介质（磁介质等）管理

针对储存保管资讯、备份资料的介质，不仅需保管在具有适当进出管理的房间内并可以上锁的保管库里，而且按照规定手续实施适当的移动出入管理。

5-1-1-9 废弃物处理

针对存有作为机密资讯的资料・储存介质，按照规定手续进行妥当的废弃处理。

5-1-1-10 外部备份

无任何规定。

5-1-2 市町村的设施

5-1-2-1 设施的位置与建造

作为住址所在地的市町村设施。

5-1-2-2 实体的操作管理

密钥对生成装置、受理窗口终端机设置在住址所在地市町村的工作人员可以监视的地方。此外，对密钥对生成装置、受理窗口终端机实施适当的保养。

操作受理窗口终端机需实施使用者的本人核实。操作人的认证，以 ID / 密码方式进行。

5-1-2-3 保管资讯的管理

本运用章程「4-12-1-1 保管资讯的种类」的相关资料，需保管在适当的地方。

5-1-2-4 废弃物处理

针对存有秘密资讯的资料・储存介质及受理窗口终端机、密钥对生成装置等的废弃，按照规定手续进行妥当的废弃处理。

5-2 手续方面的安全管理

5-2-1 具有良好信誉的工作人员与其职责

5-2-1-1 北海道 CA 的工作人员

北海道 CA 系统运行的相关工作人员如下所示。

(1) 认证局管理负责人

认证局管理负责人即营运北海道 CA 的负责人， 履行以下业务。

・认证业务的总括
・北海道知事的私钥发生危殆化及发生灾害等紧急情况时的应对总括
・对工作人员下达指示及确认工作结果
・用于控制 HSM（安全管理北海道知事的私钥装置）功能的锁（以下称「管理锁」。）的保养管理。
・针对请求公开认证业务资讯的应对管理
・针对请求更正认证业务资讯的应对管理
・咨询・投诉处理的应对管理
・认证业务资讯保护委员会的管理
・置备认证业务相关的帐簿
・制作失效资讯等的提供情况报告
・房间出入管理
・应对遵循情况的监查，以及针对其指正事项实施改正管理
・其他有关北海道 CA 的营运及运用总括
・个人信息的管理

(2) 私钥管理人

私钥管理人，即使用北海道知事的私钥等相关业务的负责人，履行如下业务。然而，该工作由多位私钥管理人执行。

・保管管理北海道知事私钥等的备份介质
・北海道知事私钥等的设置、发行个人签名证明书时的 HSM 操作

・北海道知事私钥等更新时的 HSM 操作

・北海道知事私钥等备份，以及从备份进行复原时的 HSM 操作

(3) 受理负责人

受理负责人，履行相互认证证明书等的发行、更新及失效申请的受理、与个人认证 BCA 的联系调整业务及申请资料等的管理。

(4) 审查负责人

审查负责人，履行审查相互认证证明书等的发行、更新及失效申请等业务。

(5) 审查批准人

审查批准人，履行针对审查负责人进行的相互认证证明书等的发行申请、更新申请及根据失效申请的审查结果给予批准的业务。

(6) 高级操作人员

高级操作人员，即使用北海道知事的私钥履行以下业务。此外，该工作由多位高级操作人员执行。

・HSM 的活性化及非活性化

・个人签名证明书的发行、更新、失效处理

・相互认证证明书的发行、更新、失效处理

・官职证明书验证服务器证明书的发行、更新、失效处理

・OCSP 响应器证明书的发行、更新、失效处理

・北海道 CA 电子证明书等政策的设定登录及变更

・其它北海道 CA 系统的运用管理业务

(7) 信息储藏库操作人员

信息储藏库操作人员，即履行信息储藏库的设定管理等相关业务。

(8) 一般操作人员

一般操作人员，即履行网路机器等的运用及维护管理等业务。

(9)内部监查人

内部监查人，即履行以下北海道 CA 系统及信息储藏库的日志相关业务。

・监查日志的检查

・已监查过的日志删除

5-2-1-2 市町村的工作人员

市町村的工作人员，履行电子证明书的发行・失效时严格的本人核实，以及发行・失效相关的事务，并且针对该事务使用的机器等进行妥善管理。

5-2-2 北海道 CA 各个工作人员的职权分工与下达指示方法

各个工作人员行使职权的分工与下达指示方法如以下规定所示。

① 职权分工

从人的安全角度考虑进行职务分工，由被授予权限的多位工作人员履行设施的运用・管理。

② 认证局管理负责人的权限

针对重要的业务指示，认证局管理负责人按照另行规定的指定手续，向各个工作人员下达指示。

③ 高级操作人员的权限

高级操作人员，按照另行规定的手续，向一般操作人员下达各种工作指示及确认结果。此外，发行相应工作人员的权限申报以及证明书。

5-2-3 北海道 CA 各个工作人员的识别与认证事项

・各个工作人员进行系统操作时，系统执行识别・认证运作工作人员是否为正当权限人。
・各个工作人员的认证使用 IC 卡或密码来实施。密码需定期更换。
・按照各个工作人员的职责，将各工作人员可以访问的秘密资讯控制到最低限度。

5-3 北海道 CA 在人事方面的安全管理

5-3-1 工作人员的个人背景审核与认可程序

按照所需的审核程序，通过雇用前资料(履历表、推荐信等)审查，实施经历调查。

5-3-2 针对工作人员的培训程序

按照教育训练计划，对各工作人员实施必要的培训。

5-3-3 工作人员之间的业务交接、频率和顺序

认证局管理负责人根据文件，规定业务交替方式。

5-3-4 不被认可的行动

各个工作人员行使了不被认可的行动时，按照已有的规定进行惩戒处分。

5-3-5 提供给各个工作人员的文件

根据各自的访问权限，各个工作人员可以阅览文件(运用程序、操作步骤等)。

6．技术的安全管理

6-1 密钥对设置和下载

6-1-1 北海道知事的锁

6-1-1-1 北海道知事的密钥对设置人、制锁方法

北海道知事的密钥对，由多位私钥管理人使用本运用章程「6-1-1-3 设置密钥对的硬件/软件」规定的设备进行制锁。

6-1-1-2 锁长

根据 RSA 加密方式，使用 2048 比特的锁。

6-1-1-3 设置密钥对的硬件/软件

相当于 FIPS140-1 等级 3 的 HSM。

6-1-1-4 私钥的使用目的

用于数字签名。

6-1-1-5 领取个人认证 BCA 的公钥

为互换相互认证证明书，北海道 CA 需安全可靠地领取个人认证 BCA 的公钥。

6-1-1-6 发送北海道知事的公钥

北海道知事的个人签名证明书,在发行电子证明书时储存在 IC 卡里,然后交付给使用者，并且通过安全可靠的方法发送给验证签名者等。

6-1-2 使用者的锁

6-1-2-1 使用者的密钥对设置人、制锁方法

使用者本人利用住址所在地市町村的密钥对生成装置进行制锁。

6-1-2-2 向住址所在地市町村等安全提供使用者公钥的方法

住址所在的地市町村直接从使用者那里领取储存在 IC 卡里的公钥。

6-1-2-3 锁长

根据 RSA 加密方式，使用 1024 比特的锁。

6-1-2-4 设置密钥对的硬件/软件

住址所在地市町村的密钥对生成装置。

6-1-2-5 私钥的使用目的

用于数字签名。

6-2 保护私钥

6-2-1 北海道知事的私钥

6-2-1-1 保管私钥要求的基准

使用相当于 FIPS140-1 等级 3 的 HSM 加以保护。

6-2-1-2 私钥的多人控制

多位私钥管理人通过 HSM 的控制对私钥加以保护。

6-2-1-3 私钥的委托保管（第三方支付担保）

不实施私钥的委托保管。

6-2-1-4 私钥的备份

私钥的备份，由多位私钥管理人操作。

从 HSM 备份的私钥，以加密方式进行安全保管。但私钥管理人不得将备份介质带出其保管房间之外。

6-2-1-5 私钥的保管（存档）

不实施私钥的存档。

6-2-1-6 加密模块内私钥的储存

私钥通过多位私钥管理人的操作，在 HSM 中设置，储存到加密模块内。

6-2-1-7 私钥的活性化

私钥由多位私钥管理人操作，将其活性化。

6-2-1-8 私钥的非活性化

私钥由多位私钥管理人操作，将其非活性化。

6-2-1-9 私钥的废弃

废弃加密模块内的私钥，由多位私钥管理人通过初始化加密模块等方法，使其处于完全不能使用的状态。然而，如果将加密模块带出室外时，则将加密模块实体毁坏。

此外，所废弃的私钥，其备份用的加密模块同样需要废弃。

6-2-2 使用者的私钥

6-2-2-1 关于保管私钥的要求基准

在具有防短波功能的 IC 卡内，按照「公共性个人认证服务卡应用程式外部接口格式书 1.1 版」，装载卡的应用程式，保护私钥无法从 IC 卡上直接被读出。

6-2-2-2 私钥的委托保管（第三方支付担保）

北海道知事不接受使用者私钥的委托保管，而且不认可使用者将其私钥委托给第三者进行保管。

6-2-2-3 私钥的备份

私钥保管在 IC 卡内，不进行备份。

6-2-2-4 私钥储存在加密模块（IC 卡）内

使用者的私钥，通过住址所在地市町村的密钥对生成装置的设置，储存在使用者的 IC 卡里。储存在 IC 之后，在密钥对生成装置设置的私钥，需从密钥对生成装置上彻底删除。

6-2-2-5 私钥的活性化

使用者的私钥，由使用者输入密码将其活性化。

6-2-2-6 私钥的非活性化

通过操作 IC 卡，使私钥非活性化。

6-2-2-7 私钥的废弃

使用者的私钥进行废弃时，使用者利用住址所在地市町村的受理窗口终端机，以及密钥对生成装置将其废弃。

6-3 关于配对锁设置管理的其它方面

6-3-1 北海道知事的锁

6-3-1-1 公钥的保管

将包含在个人签名证明书内的公钥，根据本运用章程「4-12 记录的保管（存档）」规定的期间，保管在已实施防止窜改措施的档案里。

6-3-1-2 公钥、私钥的使用期间

北海道知事的个人签名证明书的有效期为 10 年。私钥的使用期限自制锁日起算 5 年，每过 5 年进行更新。

然而，当估计到密码的安全性脆化时，有可能考虑改变加密方式，即时进行锁的更新等情况。

6-3-2 使用者的锁

使用者的公钥和私钥的使用期限，自制锁日起算 3 年。

然而，当估计到密码的安全性脆化时，有可能考虑改变加密方式，即时进行锁的更新等情况。

6-4 活性化资料

6-4-1 北海道知事的锁

6-4-1-1 活性化资料的产生与下载

储存北海道知事私钥的 HSM 活性化资料，通过管理锁来设定。

6-4-1-2 活性化资料的保护

使储存北海道知事私钥的 HSM 活性化所必需的管理锁，需安全保管。

6-4-2 使用者的锁

6-4-2-1 活性化资料的产生与下载

使用者私钥的活性化资料（密码），由使用者自己通过利用密钥对生成装置设置配对锁的时候，设定到 IC 卡里。

6-4-2-2 活性化资料的保护

使用者私钥的活性化资料必须定期变更，安全保管。

6-5 电脑的安全管理

6-5-1 电脑的安全功能注意事项

北海道 CA 的相关系统，需使用信誉良好的 OS，具备访问限制、各个工作人员的识别与认证功能、监查日志及存档资料的收集功能以及系统恢复功能等。

6-5-2 电脑的安全评估

随时实施系统的安全评估。

6-6 系统寿命的安全管理

6-6-1 系统开发的安全管理

有关本服务的开发，修正或者变更，需根据规定手续，由信誉良好的组织或环境下实施运作。已开发、修正或变更的系统，通过试验环境的验证，得到认证管理局负责人的批准之后引入使用。而且，系统规格及验证报告进行书面保管。

6-6-2 系统运用方面的安全管理

6-6-2-1 北海道 CA

为维持管理本服务的相关系统，定期进行 OS 及软件的安全检查。而且，将该检查结果进行书面保管。

6-6-2-2 市町村

为维持管理本服务的相关系统，妥善进行密钥对生成装置及受理窗口终端机的 OS 及软件的安全管理。

6-7 网路安全管理

为防止非法进入，将经由外部网路所必要的网上服务的认可，缩减到最小限度。此外，实施检验非法侵入等充分的安全保护措施。信息储藏库内保存的资讯中，其公开资讯需通过防火墙提供。

6-8 加密模块的技术管理

按照本运用章程「6-1-1-3 设置密钥对的硬件/软件」、「6-2-1-1 关于保管私钥的要求基准」的规定。

7. 证明书和失效记录（CRL/ARL）的内容

7-1 证明书

7-1-1 电子证明书

电子证明书记载如下资讯。详情根据 Profile 设计书决定。

・版本编号（X.509 证明书格式的版本编号）
・序列号（北海道 CA 内为识别已发行过的证明书所用的号码）
・签名演算法（北海道知事在该电子证明书签名时使用的演算法资讯）
・发行人信息（发行该电子证明书的北海道知事名，用 X.500 识别名记载）
・有效期的开始日（该电子证明书的发行日）
・有效期的结束日（发行日 3 年后）
・公钥（使用者的公钥）
・扩展资讯（记载使用者的基本 4 信息或锁的使用目的等）

7-1-2 相互认证证明书

与个人认证 BCA 实施相互认证时所必需的相互认证证明书记载如下资讯。详情根据 Profile 设计书决定。

・版本编号（X.509 证明书格式的版本编号）
・序列号（北海道 CA 内为识别已发行过的证明书所用的号码）
・签名演算法（北海道知事在该相互认证证明书签名时使用的演算法资讯）
・发行人信息（发行该相互认证证明书的北海道知事名，用 X.500 识别名记载）
・有效期的开始日（该相互认证证明书的有效开始日）
・有效期的结束日（该相互认证证明书的有效开始日起算 5 年后）
・公钥（相互认证 CA 的公钥）
・扩展资讯

7-1-3 个人签名证明书

北海道知事的个人签名证明书记载如下资讯。详情根据 Profile 设计书决定。

・版本编号（X.509 证明书格式的版本编号）
・序列号（北海道 CA 内为识别已发行过的证明书所用的号码）
・签名演算法（北海道知事在该个人签名证明书签名时使用的演算法资讯）
・发行人信息（发行该个人签名证明书的北海道知事名，用 X.500 识别名记载）
・有效期的开始日（该个人签名证明书的发行日）
・有效期的结束日（发行日 10 年后）
・公钥（北海道知事的公钥）
・扩展资讯

7-1-4 链接证明书

北海道知事的锁更新时所必需的链接证明书记载如下资讯。详情根据 Profile 设计书决定。

・版本编号（X.509 证明书格式的版本编号）
・序列号（北海道 CA 内为识别已发行过的证明书所用的号码）
・签名演算法（北海道知事在该链接证明书签名时使用的演算法资讯）
・发行人信息（发行该链接签名证明书的北海道知事名，用 X.500 识别名记载）
・有效期的开始日（OldWithNew：旧版密钥对的制锁日、NewWithOld：新版密钥对的制锁日）
・有效期的结束日（OldWithNew：旧版个人签名证明书的有效期结束日、NewWithOld：旧

版个人签名证明书的有效期结束日）
・公钥（OldWithNew：旧版公钥、NewWithOld：新版公钥）
・扩展资讯

7-2 失效记录（CRL/ARL）

7-2-1 电子证明书的失效记录（CRL）

电子证明书失效记录(CRL)记载如下资讯。详情根据 Profile 设计书内的 CRL 的 Profile 决定。

・版本资讯（CRL 格式的版本编号）
・签名演算法（北海道知事在该 CRL 上签名时使用的演算法资讯）
・发行者信息（发行该 CRL 的北海道知事名，用 X.500 识别名记载）
・有效期的开始日（该 CRL 的有效开始日）
・有效期的结束日（该 CRL 的有效开始日起算 3 天后）
・下次更新预定日（该 CRL 的有效开始日 1 天后）
・已失效的证明书资讯（序列号、失效年月日、失效事由）
・扩展资讯

7-2-2 相互认证证明书的失效记录（ARL）

相互认证证明书的失效记录（ARL）记载如下资讯。详情根据 Profile 设计书内的 ARL 的 Profile 决定。

・版本信息（ARL 格式的版本编号）
・签名演算法（北海道知事在该 ARL 上签名时使用的演算法资讯）
・发行者信息（发行该 ARL 的北海道知事名，用 X.500 识别名记载）
・有效期的开始日（该 ARL 的有效开始日）
・有效期的结束日（该 ARL 的有效开始日起算 3 天后）
・下次更新预定日（该 ARL 的有效开始日 1 天后）
・已失效的证明书资讯（序列号、失效年月日、失效事由）
・扩展资讯

7-2-3 个人签名证明书的失效记录（ARL）

个人签名证明书的失效记录（ARL）记载如下资讯。详情根据 Profile 设计书内的 ARL 的 Profile 决定。

・版本信息（ARL 格式的版本编号）
・签名演算法（北海道知事在该 ARL 上签名时使用的演算法资讯）
・发行者信息（发行该 ARL 的北海道知事名，用 X.500 识别名记载）
・有效期的开始日（该 ARL 的有效开始日）
・有效期的结束日（该 ARL 的有效开始日起算 3 天后）
・下次更新预定日（该 ARL 的有效开始日 1 天后）
・已失效的证明书资讯（序列号、失效年月日、失效事由）
・扩展资讯

7-2-4 链接证明书的失效记录（ARL）

链接证明书的失效记录(ARL)记载如下资讯。详情根据 Profile 设计书内的 ARL 的 Profile 决定。

・版本信息（ARL 格式的版本编号）
・签名演算法（北海道知事在该 ARL 上签名时使用的演算法资讯）

・发行者信息（发行该 ARL 的北海道知事名，用 X.500 识别名记载）
・有效期的开始日（该 ARL 的有效开始日）
・有效期的结束日（该 ARL 的有效开始日起算 3 天后）
・下次更新预定日（该 ARL 的有效开始日 1 天后）
・已失效的证明书资讯（序列号、失效年月日、失效事由）
・扩展资讯

8．运用章程的管理

8-1 运用章程的更改管理

北海道知事，根据需要对本运用章程进行更改。

8-2 公布及通知

本运用章程有所更改时，北海道知事需立即将更改的运用章程在网站(Web)上公布。同时向使用者、验证签名者等以及确认签名者通知。

8-3 运用章程的认可手续

根据北海道知事的决定给以批准有效。