

目次

1. はじめに	1
2. 目的及び用語の定義	3
2.1. 目的及び背景	3
2.2. 用語の定義	4
3. 証明書用途の再確認	12
3.1. 医師に対する証明書用途	12
3.2. 医療機関に対する証明書用途	14
4. 現状把握	16
4.1. 厚生労働省の動向	16
4.2. 地域医療サービスの提供サービスと PKI 使用用途	17
4.2.1. Hot Project が提供しているサービス	17
4.2.2. Hot Project の今後の計画	19
4.2.3. OCHIS が提供しているサービス	19
4.3. 他保健医療福祉分野認証局の提供サービスと PKI 使用用途	21
4.3.1. Medicertified 電子証明書発行サービス	21
4.3.2. MEDIS HPKI 電子証明書発行サービス（署名用）	23
4.3.3. MEDIS HPKI 電子証明書発行サービス（認証用）	25
4.3.4. 今後の計画	26
4.4. GPKI/LGPKI/JPKI の提供サービスと PKI 使用用途	26
5. 日医認証局	29
5.1. 開発の現状	29
5.1.1. 開発区分について	29
5.1.2. 第一期開発	30
5.1.3. 第二期開発	30
5.2. 認証局の提供機能と第二期開発見直し内容	31
5.2.1. 認証局の提供する機能・役割	31
5.2.2. 第二期見直し計画	33
5.3. 今後の予定	34

6.	モデルの検討	35
6.1.	日医認証局の位置付け	35
6.2.	保健医療福祉分野 PKI の将来像と各 PKI ドメインとの連携	36
6.3.	地域医師会を中心とした地域医療 PKI との連携	37
6.4.	他保健医療福祉分野 PKI との連携	38
6.5.	GPKI/LGPKI/JPKI との連携	38
6.6.	実施計画の検討	39
7.	短期実現モデル	41
7.1.	単一認証局モデル	43
7.1.1.	日医署名用認証局 単一認証局モデル	43
7.1.2.	日医認証用認証局 単一認証局モデル	44
7.1.3.	日医プライベート認証局 単一認証局モデル	45
7.2.	階層型モデル	47
7.2.1.	日医署名用認証局 階層型モデル	47
7.2.2.	日医認証用認証局 階層型モデル	48
7.2.3.	日医プライベート認証局 階層型モデル	49
8.	中期実現モデル	52
8.1.	階層型接続モデル	52
8.2.	ブリッジ型接続モデル	54
8.3.	相互認証型接続モデル	56
9.	技術的検討	58
9.1.	運用における検討事項・主なシステム要件	58
9.1.1.	共通機能	59
9.1.2.	単一認証局モデル	59
9.1.3.	階層型接続モデル	59
9.1.4.	相互認証型接続モデル	60
9.1.5.	ブリッジ型接続モデル	60
9.1.6.	GPKI 接続	60
9.1.7.	その他検討が必要な機能	61
9.1.8.	必要と想定されるシステム機能一覧	61

9.2.	現状システムとの対比	62
9.2.1.	日医認証局の実装機能	63
9.2.2.	共通機能.....	64
9.2.3.	単一認証局モデル	65
9.2.4.	階層型接続モデル	65
9.2.5.	相互認証型接続モデル	65
9.2.6.	ブリッジ型接続モデル	65
9.2.7.	GPKI 接続.....	66
9.2.8.	その他検討が必要な機能.....	66
9.2.9.	必要と想定されるシステム機能対応状況一覧	66
10.	今後の課題	70
10.1.	実運用へ向けた課題.....	70
10.2.	短期モデルの実現へ向けた課題.....	71
10.2.1.	システム構築課題.....	71
10.2.2.	業務課題	72
10.2.3.	モデルごとの課題分類.....	73
10.3.	必要と想定される RA 機能	74
10.4.	ルート認証局の鍵管理方法	75
11.	事例調査.....	76
11.1.	海外における医療関連 PKI 使用事例	76
11.1.1.	AMA (American Medical Association, アメリカ医師会)	76
11.1.2.	CMA (California Medical Association, カリフォルニア医師会)	77
11.2.	海外における相互運用事例	77
11.2.1.	カナダ政府.....	78
11.2.2.	アメリカ連邦政府.....	78
11.2.3.	オーストラリア政府	79
11.2.4.	韓国政府	80
11.2.5.	ドイツ政府.....	80
12.	おわりに	82
	別紙.....	84
	参考文献	84