

認証機関等調査研究委員会報告書

平成 11 年 6 月

認証機関等調査研究委員会
(財)社会安全研究財団委託研究事業

認証機関等調査研究委員会名簿

委員長 大貫 啓行 麗澤大学国際経済学部教授

委員 鈴木 邦芳 (社) 日本防犯設備協会専務理事

委員 御手洗伸太郎 警察庁生活安全企画課
セキュリティシステム対策室長

事務局 警察庁生活安全企画課

目 次

認証機関等調査研究委員会名簿

目 次

第1章 認証機関の必要性	1
1 ネットワーク社会の犯罪に対する脆弱性	1
2 暗号技術の概要	4
（1）暗号技術の基本原理	4
（2）暗号技術の分類	5
（3）認証機関等の概要	5
3 暗号技術普及の必要性	10
第2章 認証機関等の業務に係る脅威	11
1 認証機関の業務に係る脅威及びその方法	11
（1）公開鍵の不正登録又はすり替え	11
（2）失効させるべき公開鍵又は公開鍵証明証の利用	11
（3）公開鍵証明証の偽変造	11
2 鍵回復機関の業務に係る脅威	12
第3章 認証機関に関するガイドライン等	13
1 認証機関の在り方をめぐる国内の検討状況	13
2 各ガイドライン等の内容	13
（1）情報セキュリティビジョン策定委員会報告書	13
（2）認証局運用ガイドライン（1.0版）	15
（3）ネットワーク認証業務に関するガイドライン	19
第4章 鍵回復機関に関するガイドライン等	21
1 鍵回復機関の在り方をめぐる国内の検討状況	21
2 報告書の内容	21
第5章 認証機関等に対する調査の概要及び結果	23
1 調査の内容	23
2 調査対象会社の概要	23
（1）認証機関	23
（2）鍵回復機関	24
3 調査の結果	24
（1）従業員等内部者による不正行為の防止方策	24
（2）部外者による不正行為の防止方策	28
第6章 認証機関の適格性及び業務の適正性を確保するための課題	31
1 業務を行っている認証機関の現状	31
2 ネットワークの安全を確保する役割を担う公的性格を持つ認証機関として発展するための課題	31

- (1) 本人確認を行う能力の具備 31
- (2) 公的性格の機関としての自覚の必要性 31

<付録>

- 質問事項

<参考資料>

- 認証局運用ガイドライン（1.0版）
- ネットワーク認証業務に関するガイドライン

↑ 4リンク