

暗号技術調査研究委員会報告書

平成 11 年 3 月

暗号技術調査研究委員会
(財)社会安全研究財団委託研究事業

暗号技術調査研究委員会名簿

委員長	辻 井 重 男	中央大学理工学部教授
委 員	小森谷 宏	(社) 日本防犯設備協会専務理事
委 員	須 藤 修	東京大学社会情報研究所助教授
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

暗号技術調査研究委員会名簿

目 次

第1章 ネットワーク社会の犯罪に対する脆弱性と暗号技術	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) 暗号技術の基本原則	4
(2) 暗号技術の分類	5
(3) 認証機関等の概要	6
3 暗号技術普及の必要性	10
第2章 民間企業等におけるネットワークの利用状況及びセキュリティ対策に係る調査結果	11
1 調査の目的、調査実施要領及び回答企業の概要	11
(1) 調査の目的	11
(2) 調査実施要領等	11
2 ネットワークを利用した企業内及び企業間におけるデータ交換並びに当該データ交換におけるセキュリティ対策の現状について	12
(1) ネットワークを利用したデータ交換の現状	12
(2) ネットワークを利用したデータ交換におけるセキュリティ対策の現状	21
3 一般消費者を対象としたサービスの提供状況及びセキュリティ対策の現状について	29
(1) ネットワークを利用した一般消費者向けサービスの提供状況	29
(2) サービス提供に係るセキュリティ対策の現状	31
4 暗号技術及び認証機関の認知度、利用状況等について	37
(1) 暗号技術の認知度及び利用状況	37
(2) 認証機関の認知度、利用状況等	40
(3) キーリカバリー機能の必要性	48
5 政府等に対する情報セキュリティに関する要望事項	50
(1) 暗号技術に関するもの	50
(2) 情報公開及び啓蒙に関するもの	50
(3) 規制や法整備に関するもの	50
(4) 認証機関の位置付けに関するもの	51
第3章 情報セキュリティ対策の課題と暗号技術の普及を図る施策の在り方	52
1 企業等の情報セキュリティ対策の現状と課題	52
(1) 企業等の情報セキュリティ対策の現状と問題点	52
(2) 企業等の情報セキュリティ対策の課題	53
2 暗号技術の普及を図る施策の在り方	54
(1) 企業等の情報セキュリティ意識の高揚方策	54
(2) 利用しやすい優良な暗号製品等の開発・普及及び利用しやすい認証機関の整備方策	58

<付録>

○ 調査表