

暗号技術
応募書類等作成要領

平成12年6月

情報処理振興事業協会
セキュリティセンター

暗号技術応募書類等作成要領

暗号技術の応募書類等の作成に際しては、「暗号技術公募要領」の「4.2 評価のために必要な情報の提出」に従って下さい。

文書については、全て日本工業規格A4判として下さい。

電子データについては、ファイル形式は、Microsoft WORD形式、JUSTSYSTEM 一太郎形式、Adobe PDF形式 Adobe PostScript 形式 (Level 2.0 以上)のいずれかとし、以下のファイル名を使用して下さい。

電子媒体については、全ての電子データをCD-R、CD-RW、光磁気ディスクのいずれかにまとめて入れ、暗号名と申請社名を記入したラベルを添付して下さい。

- (1) 暗号技術応募書 (様式別添)
 - (和文) : 「応募書1」または「call-1」
- (2) 暗号技術概要説明書 (様式別添) :
 - (和文) : 「応募書2」または「call-2」
 - (英文) : 「応募書2e」または「call-2e」
- (3) 暗号技術仕様書
 - (和文) : 「応募書3」または「call-3」
 - (英文) : 「応募書3e」または「call-3e」
- (4) 自己評価書
 - (和文) : 「応募書4」または「call-4」
 - (英文) : 「応募書4e」または「call-4e」
- (5) テストベクタ : 「応募書5」または「call-5」
- (6) サンプルコード : 「応募書6」または「call-6」
- (7) 公開の状況等に関する情報
 - (和文) : 「応募書7」または「call-7」
- (8) 知的所有権に関する情報
 - (和文) : 「応募書8」または「call-8」
- (9) 会社概要表 (様式別添)
 - (和文) : 「応募書9」または「call-9」

各ページ内での各項目の記入スペースの配分は応募者の任意とする

受付番号

暗号技術概要説明書

1. 暗号名:		
分類: 1. 公開鍵暗号 2. 共通鍵暗号 3. ハッシュ関数 4. 疑似乱数生成		
詳細分類	公開鍵暗号	1. 守秘 2. 認証 3. 署名 4. 鍵共有
	共通鍵暗号	1. ストリーム暗号 2. 64bitブロック暗号 3. 128bitブロック暗号
2. 暗号の概要		
2.1 設計方針:		
2.2 想定するアプリケーション:		

各ページ内での各項目の記入スペースの配分は応募者の任意とする

受付番号

--

2.3 ベースとして用いる理論、技術：

利用実績・参考文献等：

会 社 概 要 表

会 社 名			
(代表者氏名)	()		
所在地(都市名)		関係会社	
設 立 年 月			
資 本 金			
社 員 数	人	技術者数	人
主要加盟団体			
会社の主要業務：			
主 要 株 主	株 主 名	持 株 割 合	
		(%)	