

平文	
char(1)	DataSubVersion (旧データでは、ver.2.00～は“5”, ver.2.70～は“6”)
char(1)	reserved=NULL(0)
char(1)	MissTypeLimit
char(1)	fBroken
string[16]	TokenStr = “_AttacheCaseData” “Atc_Broken_Data”
const int(4)	DATA_FILE_VERSION = 105
const int(4)	TYPE_ALGORISM = 1:Rijndael
const int(4)	AtcHeaderSize : 暗号化ヘッダのデータサイズ
byte[32] IV	暗号化されたヘッダのInitialization Vector (IV)
暗号化	
const string	“Passcode:AttacheCase¥n”
const string	“LastDateTime:” + DateTimeToStr(Now()) + “¥n”
string[]	{ Fn_[n]:FilePath ¥t FileSize ¥t FileAttr ¥t 更新日 ¥t 更新時 ¥t 作成日 ¥t 作成時 ¥n }
string[]	{ U_[n]:FilePath ¥t FileSize ¥t FileAttr ¥t 更新日 ¥t 更新時 ¥t 作成日 ¥t 作成時 ¥n }
byte[32] IV	暗号化本体のIV
DATA_MAIN	CBCモードで暗号化される本体データ

32
bytes

平文		
short 2bytes	暗号化したアプリケーションのバージョン(3xxxx)	2
char[1]	ミスタイプ回数制限(デフォルト:3)	1
char[1]	ファイルを破壊するか否か(デフォルト:false=0)	1
char[16] 16 bytes	ファイル・シグニチャ ="_AttacheCaseData" "Atc_Broken_Data"	16
int 4bytes	暗号化データバージョン(=130) 105 < x < 200	4
int 4 bytes	暗号化ヘッダーデータサイズ	4
byte[8] 8 bytes	ランダムソルト→Rfc2898DeriveBytesクラスから「key」と「IV」を導出する	8
	トークン(="atc3¥n")	
暗号化		
string[]	[格納されているファイル情報のリスト] NUM:FilePath ¥t FileSize ¥t FileAttr ¥t 更新日 ¥t 更新時 ¥t 作成日 ¥t 作成時 ¥t チェックサム ¥n	
byte[]	CBCモードで暗号化される本体データ	

合計:
24 bytes

合計:
28 bytes

合計:
36 bytes