広域イーサ用１Gbps 暗号装置

T-Cypher GigaEther

セキュリティポリシ

Ver.1.2

2008 年 12 月 11 日

NTT エレクトロニクス株式会社

改定履歴

2008/04/07	：新規作成
2008/11/25	：試験機関の所見に基づく修正 文章中の誤字を修正
2008/12/11	：文章中の誤字を修正

目次

1 序章

本書は、NTT エレクトロニクス（株）が製造する「広域イーサ用１Gbps 暗号装置（製品名：T-Cypher GigaEther)」（以下、本装置と呼ぶ）の公開セキュリティポリシを示すものである。

本装置が準拠するセキュリティ評価基準、暗号モジュールタイプ、及びセキュリティレベルは次のとおりである。

- セキュリティ評価基準：JCMVP 暗号モジュールセキュリティ要件　平成１9 年 10 月 29 日　独立行政法人 情報処理推進機構
- 暗号モジュールタイプ：マルチチップスタンドアロン型
- セキュリティレベル：レベル２

JCMVP 暗号モジュールセキュリティ要件が引用する暗号モジュール評価基準第 0.1 版の 11 分類のセキュリティ要求事項に対する本製品の実装レベルは以下の通りである。

表 1-1　セキュリティ要求事項と実装レベル

分類	実装レベル
1. 暗号モジュールの仕様	2
2. 暗号モジュールのポートとインターフェース	2
3. 役割、サービス、及び認証	2
4. 有限状態モデル	2
5. 物理的セキュリティ	3
6. 動作環境	N/A※1
7. 暗号鍵管理	2
8. 電磁妨害/電磁両立性（EMI/EMC）	N/A※2
9. 自己テスト	2
10. 設計保証	2
11. その他の攻撃への対処	N/A※1

※1　N/A：適応外

※2　VCCI クラス A／IT3001（JEIDA-52）

1.1 用語定義

表 1-2　用語定義

用語	意味
LAN	ローカルエリアネットワーク
ルータ	ネットワークとネットワークを中継する通信装置
SW	通信回線を切り替える通信装置
DCE	広域通信網へ接続するための装置
フレーム	ネットワーク内を流れるデータ
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SDRAM	Synchronous Dynamic Random Access Memory
SRAM	Static Random Access Memory

2 概要

本装置は、LAN 内のルータ/SW と広域通信網の DCE の間に設置され、広域通信網上のレイヤ 2 フレームを暗号化することにより、レイヤ 2 フレームの盗聴を防止する製品である。

本装置はフレームを暗号化・復号するため、対向する復号・暗号化機能を有する装置（以下、対向装置と呼ぶ）が必要である。

対向装置として使用可能なものは、本装置及び NTT エレクトロニクス（株）が製造する「10／100M 広域イーサ用暗号装置（製品名：T-Cypher ETHER10／ETHER100）」（以下、従来機と呼ぶ）である。

2.1 システム概要

本装置のネットワーク接続図と動作モードについて説明をする。

本装置は、基本的に対向装置がない拠点*1との通信は不可能である。ただし、ネットワーク上に順次に設置していく段階で、対向装置がない拠点との通信も可能する動作モード（設置モード）を有している。

以下に設置モード OFF の場合と設置モード ON の場合のネットワーク構成図を図 2-1及び図 2-2に示す。

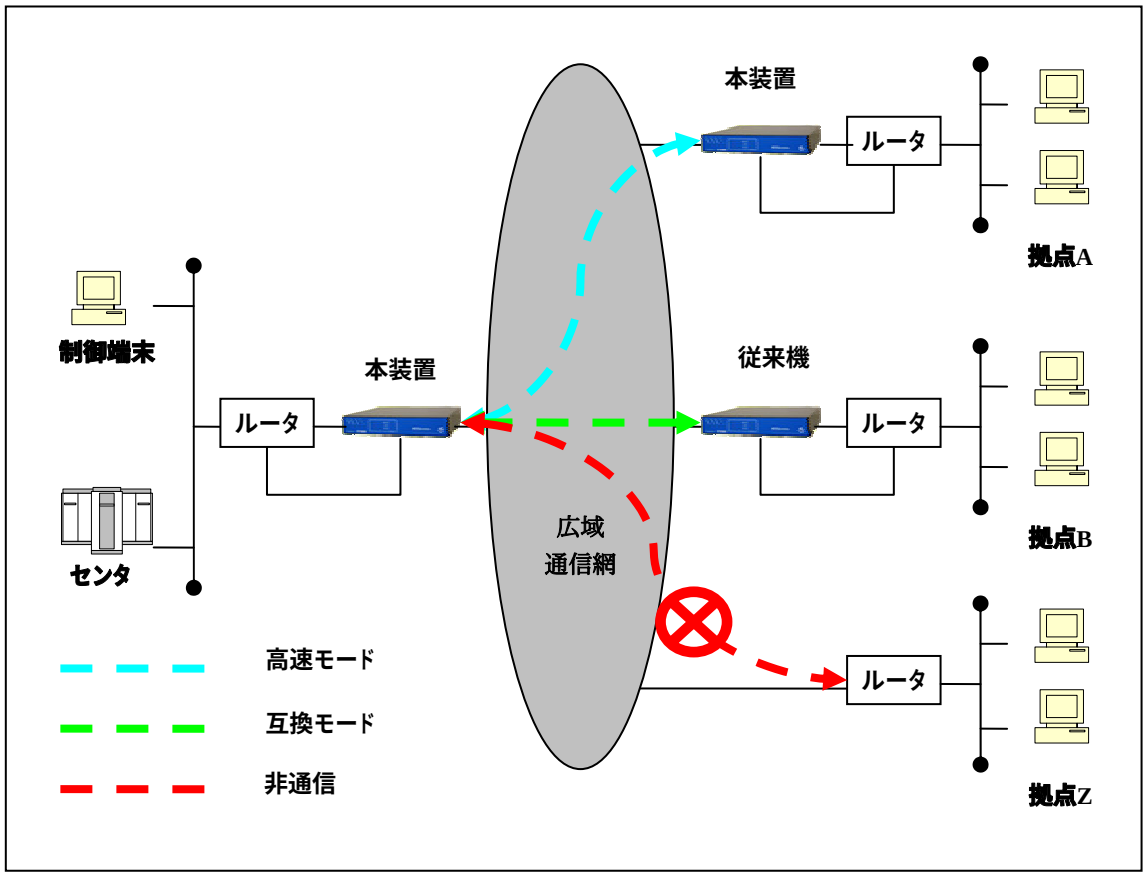


図 2-1　ネットワーク接続構成図（設置モード OFF）

1 対向装置が設置されていない、又は設置されていても電源投入されていない拠点

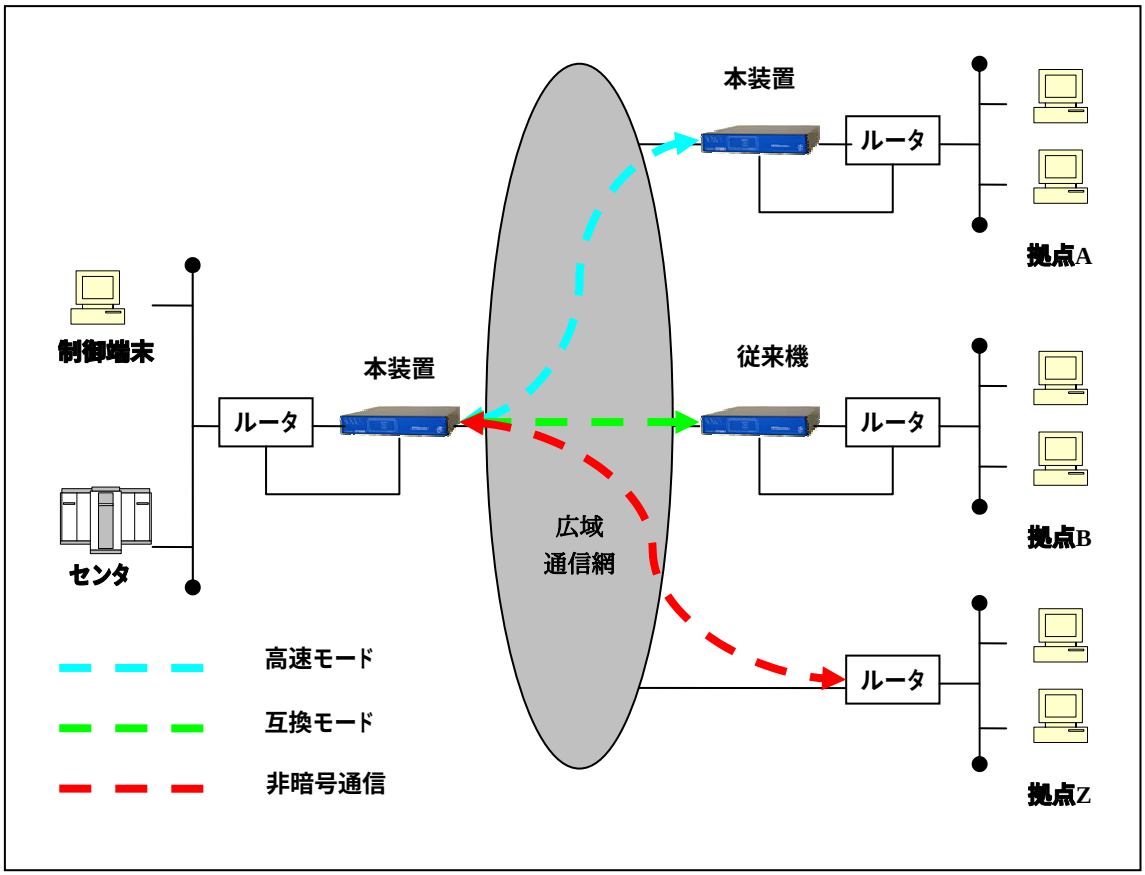


図 2-2　ネットワーク接続構成図（設置モード ON）

設置モード OFF　　：対向装置が見つからない場合、フレームを破棄し通信を行わない。
設置モード ON　　：対向装置が見つからない場合、非暗号通信を行う。

本装置は、以下に示す 2 つの動作モードを有する。

（1）　高速モード

高速モードは、本装置－本装置間の場合の動作モードであり、ジャンボフレーム送受が可能であり、承認された動作モードで動作する。

本モードを使用するには、対向装置が本装置である必要がある。

（2）　互換モード（JCMVP 適合範囲外）

互換モードは、本装置－従来機間の場合の動作モードであり、ジャンボフレームの送受がなく、一部 JCMVP に承認されていないセキュリティ機能を使用して動作する。

本モードを使用するには、対向装置が従来機である必要がある。

※電源投入後、本装置は高速モードで動作する。各対向装置が従来機の場合、従来機との通信中は自動的に互換モードへ移行する。通信終了後、自動的に高速モードへ移行する。

2.2 装置概要

2.2.1　　ブロック図

本装置のブロック図を図 2-3に示す。また、この中で暗号境界と外部との物理的ポートを示す。
物理的ポート（ブロック図 網掛け部分）は以下に示す。

- ●LAN ポート　　：平文データの入出力
- ●WAN ポート　　：暗号文／平文データの入出力、制御入力、及び状態出力
- ●コントロールポート　：制御入力、及び状態出力
- ●LED 表示　　：状態出力

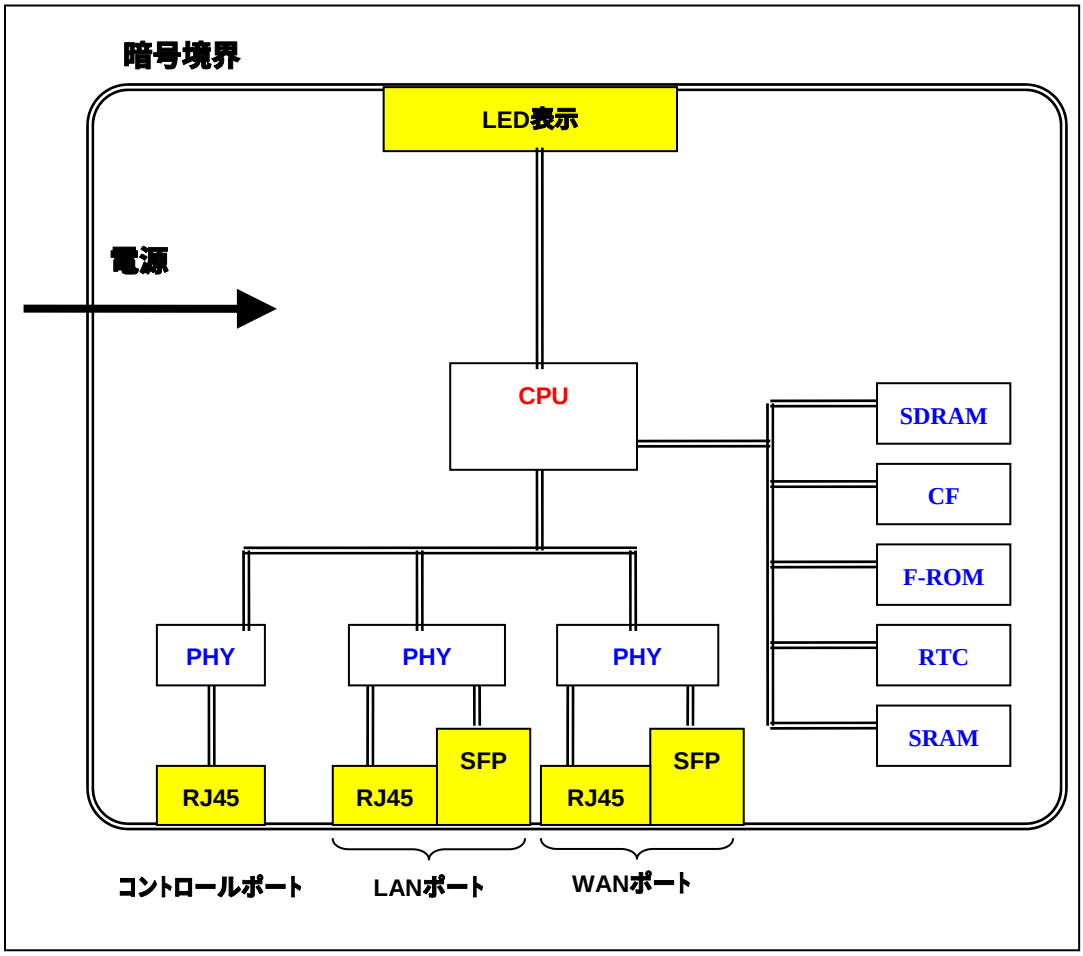


図 2-3　ブロック図

その他の役割を以下に示す。

- ●CPU　：プロセッサ
- ●PHY　：変換機（デジタル⇔アナログ）
- ●SDRAM　：大容量揮発性メモリ
- ●CF　：コンパクトフラッシュ（ファームウェア、ログ等を格納）
- ●F-ROM　：Bootloader を格納
- ●RTC　：Real Time Clock（カレンダー／時計）
- ●SRAM　：暗号鍵､及びその他の CSP を格納。内蔵バッテリにより、バックアップされ、タンパー検出時にクリアされる

2.2.2　　物理的形状

(1)　前面

(2)　背面

(3) 正面


1000M
10M
100M
SETUP
ACT
BYPASS
ERROR
POWER
CONT
LAN
WAN
DPLX
NTT Electronics

(4) 裏面


WAN
RJ-45
SFP
LAN
RJ-45
SFP
CONT
AC100V
POWER
ON
OFF

2.2.3 機能概要

本装置が有する機能一覧を表 2-1示す。

表 2-1 機能一覧

#	機能名（サービス）	概要
1	管理機能	パスワードによるログイン、装置の設定、ログ管理、装置のリセット ファームウェアのアップロード等
2	監視機能	装置状態を監視
3	自動時刻補正機能	装置内時間の自動補正
4	タンパー検出機能	装置開放時の秘密情報自動消去
5	自己診断機能	パワーアップ自己テスト／条件自己テスト
6	状態表示機能	LED 表示
7	対向装置自動検出機能	対向装置の自動検出
8	認証・鍵交換機能	装置間の認証、暗号鍵を配送
9	MAC アドレス自動学習機能	MAC アドレス管理テーブルの自動生成
10	暗号化／復号機能	暗号通信
11	ReKey 機能	暗号通信に必要なセッション鍵を更新

(1) 装置の制御及び状態の監視

本装置の制御及び状態監視は、管理機能／監視機能／自動時刻補正機能／タンパー検出機能／状態表示機能を使用することで行われる。

管理機能は、制御端末から Web を用いてのパスワード認証により、使用可能な状態になる。

管理機能は、以下の機能を有する。

- パスワードの変更
- SI の変更
- ホストネームの設定
- 日付・時刻の設定（SNTP 設定）
- ReKey 間隔設定
- CONTROL ポート設定
- データポート設定（WAN、LAN のスピード等）
- SNMP 設定
- 暗号通信モード設定（暗号サービス、バイパスサービス等）
- ステータス表示
- ログ管理
- 自己テスト
- 装置再起動
- ファームウェアアップロード
- 装置初期化（工場出荷状態にもどす。ただし、ログ等はクリアしない。）

監視機能は、装置状態を監視し、SNMP を使用して、制御端末へ状態出力データを送信する。以下の状態を監視する。

- 暗号装置起動
- バッテリ電圧の低下
- FAN 停止検出
- 温度異常検出
- タンパー検出
- ポートアップ／ダウン
- ログインエラー（規定回数エラーによるロック）
- 認証・鍵交換エラー（失敗／認証エラー／タイムアウト）
- ReKey エラー（失敗／タイムアウト）
- 暗号通信モード設定
    - 個別バイパス　ON／OFF
    - 全体バイパス　ON／OFF／SETUP

自動時刻補正機能は、制御端末より SNTP を使用し、時刻を取得、本装置の時刻を修正する。

タンパー検出機能は、筐体が開けられた場合、SRAM をクリアする。

状態表示機能は、LED 表示を使用し、装置状態を出力する。

(2)　装置の起動

装置電源が ON になると、まず自己診断機能（パワーアップ自己テスト）が実行される。本装置の暗号化／復号機能が有効に機能するためには、対向装置自動検出機能で互いの起動を確認し、認証・鍵交換機能でセッション鍵の配送を行うとともに、MAC アドレス自動学習機能で互いの装置配下にある端末の MAC アドレスを共有する必要がある。

本装置は、レイヤ 2 フレームでの暗号を目的としているため、宛先及び送信元の MAC アドレスから暗号に必要なセッション鍵を検索するメカニズムを有している。このため、配下にある端末の MAC アドレスを自動学習する必要がある。

(3) 暗号化／復号機能

暗号化／復号機能が提供するサービスを表 2-2に示す。

表 2-2 暗号化／復号機能が提供するサービス

#	サービス	概要
1	暗号サービス	レイヤ 2 フレームの暗号通信
2	バイパスサービス	レイヤ 2 フレームの非暗号通信 ・個別バイパス：特定対向装置間のフレームを非暗号で通信する。 ・全体バイパス：対向装置の有無にかかわらず、全フレームを非暗号で通信する。

(4) ReKey 機能

ReKey 機能は、設定された時刻に自動で、暗号化／復号機能で使用する暗号鍵（セッション鍵）の更新、配送を行う。

暗号鍵の生成は、マスター側の装置が行い、スレーブ側の装置へ配送する。

マスター及びスレーブは、管理機能での設定内容を認証・鍵交換時に比較し決定する。

ReKey の実行間隔及び時刻は、管理機能で設定内容を認証・鍵交換時に比較し決定する。

2.3 セキュリティ機能

本装置は、各動作モードにおいて使用するセキュリティ機能が異なる。ここでは、各動作モードで使用するセキュリティ機能、及びレイヤ 2 フレームの暗号処理について記載する。

2.3.1 高速モード

高速モードは、実装されたセキュリティ機能がすべて承認された機能を使用して動作する。承認された動作モードである。

実装している６つのセキュリティ機能を、表 2-3に示す。

表 2-3 高速モードでのセキュリティ機能

カテゴリ	アルゴリズム名
共通鍵＜128 ビットブロック暗号＞	AES(FIPS 197) 暗号利用モード：CBC／OFB
ハッシュ	SHA256(FIPS 180-2)
公開鍵＜署名＞	RSASSA-PKCS1-v1_5(鍵長 3072 ビット)
公開鍵＜守秘＞	RSAES-PKCS1-v1_5(鍵長 3072 ビット)
メッセージ認証	HMAC-SHA-256 (FIPS 198)
乱数生成	PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

表 2-4 セキュリティ強度

アルゴリズム	機能	鍵長（bits）	セキュリティ強度（bits）
AES	暗号化	256	256
RSA	署名・守秘	3072	128

フレームの暗号処理では､暗号アルゴリズムとして AES を使用し､鍵長は 256bit を使用する。フレームの暗号対象、及び暗号利用モードを図 2-4に記載する

（1）フレームの暗号対象

Header + 1Byte	1st Block	2nd Block	・・・	(N-1)th Block	Nth Block	FCS
対象外	CBC				OFB	対象外

Header + データ部１Byte　　：暗号対象外
1st Block ～ (N-1)th Block　　：暗号対象（暗号利用モード：CBCモード）
Nth Block　　：暗号対象（暗号利用モード：OFBモード）
FCS　　：暗号対象外

図 2-4 暗号対象及び暗号処理

2.3.2　　互換モード

互換モードは、実装されたセキュリティ機能に独自仕様のセキュリティ機能が一部含まれる。承認されていない動作モードである。実装している６つのセキュリティ機能を、表 2-5に示す。

表 2-5 互換モードでの承認されたセキュリティ機能

カテゴリ	セキュリティ機能
メッセージ認証	HMAC-SHA-256(FIPS 198)
乱数生成	PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

表 2-6 互換モードでの承認されていないセキュリティ機能

カテゴリ	セキュリティ機能
共通鍵＜128 ビットブロック暗号＞	AES(FIPS 197) 暗号利用モード：独自
ハッシュ	SHA1(FIPS 180-2)
公開鍵＜署名＞	RSA(鍵長 1024 ビット)
公開鍵＜守秘＞	RSA(鍵長 1024 ビット)

フレームの暗号処理では、AES CBC モードと、暗号対象の一部に独自仕様を使用する。鍵長は 192bit である。

3 モジュールインターフェース

ここでは､本装置が提供するサービスによって定義される論理的インターフェースと本装置が有する物理的ポートの対応を示す。

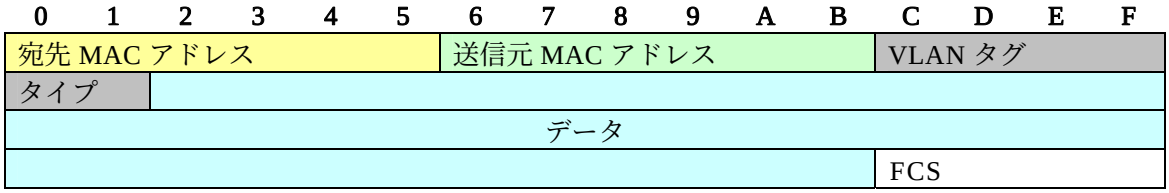
表 3-1 論理的インターフェース

論理的インターフェース	内容	物理的ポート
データ入力インターフェース	本装置が、処理するためのデータを入力するパス。	LAN ポート WAN ポート
データ出力インターフェース	本装置が、処理したデータを出力するパス	LAN ポート WAN ポート
制御入力インターフェース	本装置を制御するためのデータを入力するパス	WAN ポート コントロールポート
状態出力インターフェース	本装置の状態を出力するパス	WAN ポート コントロールポート LED 表示
電源インターフェース	本装置が、起動するのに必要な電力を供給するパス。	電源ポート

3.1 データフォーマット

ここでは、各論理的インターフェースで扱うデータフォーマットを記載する。

以下は、各論理的インターフェースで共通のデータフォーマットである。



宛先 MAC アドレス　：6 バイト
送信元 MAC アドレス　：6 バイト
VLAN タグ　：可変長（0 or 4 バイト）
タイプ　：2 バイト
データ　：可変長
FCS　：4 バイト

3.1.1 データ入力インターフェース及びデータ出力インターフェース

データ入力インターフェース及びデータ出力インターフェースが、扱うデータを表 3-2に示す。

表 3-2 データ入力インターフェース及びデータ出力インターフェースのデータタイプ

#	データタイプ	内容
1	ブロードキャストフレーム	非暗号処理対象フレーム。 宛先 MAC アドレスが、 「0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF」 であるデータ。
2	マルチキャストフレーム	非暗号処理対象フレーム。 宛先 MAC アドレス先頭１バイトの最下位ビットが 1 であるデータ。ただし、装置間通信フレームは除く。
3	ユニキャストフレーム	暗号処理対象フレーム。※1 ブロードキャストフレーム及びマルチキャストフレーム以外のデータ。
4	装置間通信フレーム	暗号処理対象フレーム。※2 装置間で情報を交換するためのフレーム。 宛先 MAC アドレスが、 「0x01, 0x00, 0xD9, 0x06, 0x07, 0x01」、 又は 「0x01, 0x00, 0xD9, 0x06, 0x07, 0x02」、 かつ 送信元 MAC アドレスが、 「0x00, 0x00, 0xD9, 0x07, 0x**, 0x**」（後ろ 2 バイトは装置 ID） であるデータ。

※ 1 暗号サービスの場合、暗号処理を行う。

※ 2 認証・鍵交換後、暗号処理を行う。

3.1.2 制御入力インターフェース

制御入力インターフェースは、コントロールポート経由の制御入力データのすべてを扱う。

3.1.3 状態出力インターフェース

状態出力インターフェースは､管理機能／監視機能／自動時刻補正機能で出力される状態出力データ及び LED 表示のデータを扱う。

4 役割とサービス、認証メカニズム

本装置の利用者認証は役割ベース認証である。利用者はクリプトオフィサ役割、ユーザ役割及びネットワークユーザ役割のいずれかを担うことができる。

それぞれの役割に付与されたサービスは表 4-1のとおりである。

表 4-1 提供するサービスと役割

#	サービス(機能)	詳細	役割			
			No Role	クリプトオフィサ	ユーザ	ネットワークユーザ
1	管理機能	装置情報の取得		●	●	
		装置情報の設定		●		
		マニュアル時刻設定		●		
		対向装置情報取得		●	●	
		対向装置正常確認		●		
		個別バイパス設定		●		
		クリプトオフィサ パスワード設定		●		
		ユーザ パスワード設定			●	
		SI 情報設定		●		
		ログの取得		●	●	
		ログの削除		●		
		暗号モード設定		●		
		ネットワーク設定		●		
		ファームウェア アップロード		●		
		装置初期化		●		
		装置再起動		●		
		SNMP 設定		●		
2	監視機能	SNTP 設定		●		
3	自動時刻補正機能			●		

#	サービス(機能)	詳細	役割			
			No Role	クリプトオフィサ	ユーザ	ネットワークユーザ
4	タンパー検出機能	秘密情報自動消去	●			
5	自己診断機能	パワーアップ自己テスト	●			
		手動セルフテスト		●		
6	状態表示機能	LED 表示	●			
7	対向装置自動検出機能	対向装置の検出	●			
		対向装置の登録				●
8	認証・鍵交換機能	RSA 鍵ペア生成				●
		装置間認証		●		●
		セッション鍵生成		●※1		●
		マスター鍵生成		●※1		●
		マルチキャスト鍵生成		●※1		●
9	MAC アドレス自動学習機能	MAC アドレス学習	●			●
10	暗号化／復号機能	暗号化				●
		復号				●
11	ReKey 機能	セッション鍵生成				●

※1　装置が再起動した際に新しい鍵を生成する。

4.1 クリプトオフィサ役割

クリプトオフィサ役割に与えられたサービス、及び各サービスにおいて利用する承認されたセキュリティ機能を表 4-2に示す。

表 4-2 クリプトオフィサ役割のサービスと承認されたセキュリティ機能

#	サービス	セキュリティ機能
1	管理機能	HMAC-SHA-256(FIPS 198)
		SHA-256（FIPS 180-2）
		AES（FIPS 197）暗号利用モード：CBC
2	監視機能	なし
3	自動時刻補正機能	なし
4	自己診断機能	AES（FIPS 197）暗号利用モード：CBC／OFB
		RSASSA-PKCS1-v1_5
		RSAES-PKCS1-v1_5
		SHA-256（FIPS 180-2）
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1
		HMAC-SHA-256(FIPS 198)
5	対向装置自動検出機能	SHA-256（FIPS 180-2）
6	認証・鍵交換機能	AES（FIPS 197）暗号利用モード：CBC
		RSASSA-PKCS1-v1_5
		RSAES-PKCS1-v1_5
		SHA-256（FIPS 180-2）
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1
7	MAC アドレス自動学習機能	AES（FIPS 197）暗号利用モード：CBC
		SHA-256（FIPS 180-2）
8	暗号化／復号機能	AES（FIPS 197）暗号利用モード：CBC／OFB
9	ReKey 機能	AES（FIPS 197）暗号利用モード：CBC
		SHA-256（FIPS 180-2）
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

4.2 ユーザ役割

ユーザ役割に与えられたサービス、及び各サービスにおいて利用する承認されたセキュリティ機能を表 4-3に示す。

表 4-3　ユーザ役割のサービスと承認されたセキュリティ機能

#	サービス	セキュリティ機能
1	管理機能	なし

4.3 ネットワークユーザ役割

ネットワークユーザ役割では、に与えられたサービス、及び各サービスにおいて利用する承認されたセキュリティ機能を表 4-4に示す。

表 4-4　ネットワークユーザ役割のサービスと承認されたセキュリティ機能

#	サービス	セキュリティ機能
1	認証・鍵交換機能	AES（FIPS 197）暗号利用モード：CBC
		RSASSA-PKCS1-v1_5
		RSAES-PKCS1-v1_5
		SHA-256（FIPS 180-2）
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1
2	MAC アドレス自動学習機能	AES（FIPS 197）暗号利用モード：CBC
		SHA-256（FIPS 180-2）
3	暗号化／復号機能	AES（FIPS 197）暗号利用モード：CBC／OFB
4	ReKey 機能	AES（FIPS 197）暗号利用モード：CBC
		SHA-256（FIPS 180-2）
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

4.4 認証メカニズム

4.4.1 クリプトオフィサ役割

利用者がクリプトオフィサ役割に就く場合、パスワードによる認証が必要となる。認証に用いるパスワードのルール、及び認証のメカニズムを以下に示す。

- パスワードは、半角 6 文字以上、16 文字以下を設定する。
- 入力可能な文字は、半角英数字、及び半角アンダーバーとする。
- 認証失敗回数が規定回数（3 回）を越えた場合、10 分間認証を行えない状態になる。

4.4.2 ユーザ役割

利用者がユーザ役割に就く場合、パスワードによる認証が必要となる。認証に用いるパスワードのルール、及び認証のメカニズムを以下に示す。

- パスワードは、半角 6 文字以上、16 文字以下を設定する
- 入力可能な文字は、半角英数字、及び半角アンダーバーとする。
- 認証失敗回数が規定回数（3 回）を越えた場合、10 分間認証を行えない状態になる。

4.4.3 ネットワークユーザ役割

利用者がネットワークユーザ役割に就く場合、Security Information による認証が必要となる。認証に用いる Security Information のルール、及び認証のメカニズムを以下に示す。

- Security Information は、半角 6 文字以上、63 文字以下を設定する
- 入力可能な文字は、全角文字（日本語を含む)、半角英数字、及び記号（ASCII0x20～0x7E）とする。（全角文字は、1 文字で半角文字 2 文字分と換算する）
- 1 秒間での認証回数は、1000 回以上行うことはできない。

5　有限状態モデル

別紙参照。

6 物理的セキュリティ

本装置は、硬いカバーに覆われ内部構造が見えない構造になっている。放熱対策のため FAN を使用するが、外部からアクセスができないような保護している。

本装置は、秘密情報保護のためタンパー検出機能を有している。タンパー検出機能は、筐体が開けられた場合、SDRAM、又は SRAM にある秘密情報（暗号鍵等）をクリアする。タンパー検出機能が動作した場合、装置の再起動はできなくなる。

また、筐体が開けられたことがわかるように、タンパーシールによって証跡が残る仕組みをとっている。

7　動作環境

本装置は、限定された動作環境でのみ動作する。したがって、動作環境のセキュリティ要件は、適用外とする。

8 暗号鍵管理

CSP（Critical Security Parameter）は、本装置で使用する暗号鍵、セキュリティ情報及びパスワードである。CSP 一覧を表 8-1に示す。

表 8-1 CSP 一覧

#	CSP 識別名	説明	格納メモリ （暗号文／平文）
1	HMAC 鍵	工場出荷時に、埋め込まれる。 ファームウェアロード時に使用する。 タンパー検出時にクリアする。	SRAM （平文）
2	Security Information （SI）	クリプトオフィサが装置に設定する。 装置間通信フレームの一部として使用するものと認証・鍵交換時の署名の一部として使用するものである。 タンパー検出時にクリアする。	SRAM （平文）
3	パスワード	クリプトオフィサ／ユーザが装置に設定する。 クリプトオフィサ／ユーザが装置にログインするときに使用する。 タンパー検出時にクリアする。	SRAM （平文）
4	ファームウェア用鍵	工場出荷時に、埋め込まれる。 ファームウェアアップロード時に使用する。 タンパー検出時にクリアする。	SRAM （平文）
4	RSA 秘密鍵	装置内で自動生成する。 認証・鍵交換時に、認証コードを生成するために使用する。 装置再起動、装置初期化、タンパー検出時にクリアする。	SDRAM （平文）
5	RSA 公開鍵	装置内で自動生成する。 認証・鍵交換時に、マスター鍵、マルチキャスト鍵、セッション鍵を暗号化するために使用する。 装置再起動、装置初期化、タンパー検出時にクリアする。	SDRAM （平文）
6	マスター鍵	認証・鍵交換時に装置内で自動生成する。 Rekey 時にセッション鍵を暗号化するために使用する。 装置再起動、装置初期化、タンパー検出時にクリアする。	SDRAM （平文）
7	マルチキャスト鍵	認証・鍵交換時に装置内で自動生成する。装置間通信フレームを暗号化するために使用する。 装置再起動、装置初期化、タンパー検出時にクリアする。	SDRAM （平文）
8	セッション鍵	認証･鍵交換及び Rekey 時に装置内で自動生成する。ユーザデータの暗号化・復号のために使用する。 装置再起動、装置初期化、タンパー検出時にクリアする。	SDRAM (平文)

また、各 CSP とサービスのアクセス権限を表 8-2に示す。

表 8-2　CSP とサービス

CSP 識別名 / 役割/サービス	H-MAC 鍵	SI	パスワード	ファームウェア用鍵	RSA 秘密鍵	RSA 公開鍵	マスター鍵	セッション鍵	マルチキャスト鍵
管理機能	R	RW	RW	R	C	C	C	C	C
監視機能	－	－	－	－	－	－	－	－	－
自動時刻補正機能	－	－	－	－	－	－	－	－	－
タンパー検出機能	C	C	C	C	C	C	C	C	C
自己診断機能	R	－	－	－	RW	RW	R	R	R
対向装置自動検出機能	－	－	－	－	－	－	－	－	－
認証・鍵交換機能	－	R	－	－	R	R	RW	RW	RW
MAC アドレス自動学習機能	－	－	－	－	－	－	－	－	R
暗号化／復号通信機能	－	－	－	－	－	－	－	R	－
ReKey 機能	－	－	－	－	－	－	R	RW	－

R　：読み出し可
W　：書き込み可
C　：消去

8.1 鍵入力

手動による鍵入力の機能は有していない。

8.2 鍵生成

RSA 鍵ペア（RSA 秘密鍵及び RSA 公開鍵）、マスター鍵、マルチキャスト鍵、及びセッション鍵は、暗号装置内部で承認された RNG を用いて生成する。

承認された RNG で使用する xkey は、常に変化するハードウェア情報を利用する。また、xkey 長は、生成する鍵長と同じかそれ以上とする。xseed については、使用しない。

8.3 鍵配送

認証・鍵交換では、マスター鍵、マルチキャスト鍵、及びセッション鍵を配送する。配送する際には、承認されたセキュリティ機能（RSAES-PKCS1-v1_5）で暗号化する。鍵配送のセキュリティ強度は 128bit である。

ReKey では、セッション鍵を配送する。配送する際には、承認されたセキュリティ機能（AES）で暗号化する。

8.4 鍵のゼロ化

鍵のゼロ化が行われるケースと対応する CSP を表 8-3に示す。

表 8-3　鍵のゼロ化ケースと CSP の対応

CSP / ケース	HMAC 鍵	SI	パスワード	ファームウェア用鍵	RSA 秘密鍵	RSA 公開鍵	マスター鍵	セッション鍵	マルチキャスト鍵
電源 OFF	－	－	－	－	○	○	○	○	○
装置再起動	－	－	－	－	○	○	○	○	○
装置初期化	－	○	○	－	○	○	○	○	○
タンパー検知	○	○	○	○	○	○	○	○	○

○：消去対象
－：消去対象外

各ケースは、以下の条件で発生する。

- ●電源 OFF　　：手動による操作
- ●装置再起動　　：管理機能によるリモート操作／エラー状態からの復旧
- ●装置初期化　　：管理機能によるリモート操作
- ●タンパー検知　　：筐体が開けられた場合

9 自己テスト

9.1 パワーアップ自己テスト

パワーアップ自己テストは、本装置の電源が ON になったときに自動的に実行されるテストである。ファームウェア完全性テスト及び、暗号アルゴリズムテスト、RBG エントロピーテスト、及びその他の重要テストが行われる。

9.1.1 ファームウェア完全性テスト

ファームウェア完全性テストでは、ファームウェアの HMAC を除く読み出し部分のメッセージ認証を用いて HMAC と比較を行い、完全性を保証する。メッセージ認証は、SHA‐256 を用いた HMAC である。メッセージ認証に失敗した場合、エラー状態になり「LED 表示」に表示される。

9.1.2 暗号アルゴリズムテスト

暗号アルゴリズムテストでは、既知解テスト（Known Answer Test ：以下、KAT と呼ぶ）を実行する。既知解テストで実行するアルゴリズムは、表 9-1に示す。

表 9-1 既知解テストを実行するアルゴリズムとテスト方法

アルゴリズム	既知解テスト方法
AES	192bit の鍵による CBC モード暗号化
	192bit の鍵による CBC モード復号
	256bit の鍵による CBC モード暗号化
	256bit の鍵による OFB モード暗号化
	256bit の鍵による CBC モード復号
	256bit の鍵による OFB モード復号
SHA256	SHA256 のメッセージダイジェスト生成
HMAC	HMAC-SHA256 によるメッセージ認証子生成
乱数生成	既存 xkey による擬似乱数生成
RSA	RSAES-PKCS1-v1_5 の鍵ペア整合性テスト
	RSASSA-PKCS1-v1_5 の鍵ペア整合性テスト

9.1.3 RBG エントロピーテスト

乱数生成時に使用する xkey(320bit)は、64 ビットの構成要素を 5 個連結し作成する。作成方法は連続乱数生成テストと同じように、初回生成の場合 2 回作成し、異なることを検証し使用する。2 回目生成以降の場合、前回作成した xkey と異なることを検証する。

9.1.4 その他の重要機能テスト

(1) ファームウェアを SDRAM に展開する前に、SDRAM の書き込み／読み出し機能が正しく動作することを確認する。

9.2 条件自己テスト

条件自己テストは、特定の条件（鍵ペア使用／乱数生成／ファームウェアアップロード等）が発生するときに、実行されるテストである。鍵ペア整合性テスト、連続乱数生成テスト、ファームウェアアップロードテスト、及びバイパステストが行われる。

9.2.1 鍵ペア整合性テスト

鍵ペア整合性テストでは、鍵ペアが使用される際に、任意の値の暗号化／復号及び署名生成／署名検証を行うことで、鍵ペアが正しいことを保証する。復号結果が暗号化する前のデータと一致しない場合、又は署名生成／署名検証に失敗した場合、エラー状態になり「LED 表示」に表示される。

9.2.2 連続乱数生成テスト

連続乱数生成テストでは、生成した乱数40バイトを、前回生成した乱数40バイトと比較することで実行される。電源ON後、前回生成された乱数が存在しない場合は、まず乱数生成を1 回実行してその結果の40バイトを前回生成された乱数として保存した後、続けて乱数生成をもう1回実行し、そこで生成された乱数40 バイトを1回目に生成された乱数40バイトと比較することで実行される。

9.2.3 ファームウェアアップロードテスト

ファームウェアアップロードテストでは、HMAC-SHA-256 を用いてメッセージ認証子を生成し、外部で事前に計算した結果と検証することで、正しいファームウェアであることを保証する。検証に失敗した場合は、ファームウェアアップロードが失敗したことを、コントロールポート経由で通知し、受け取ったファームウェアは破棄する。

9.2.4 バイパステスト

バイパステストでは、二つのフラグで暗号処理が正しく行われたことを確認する。二つのフラグはバイパス設定フラグと非暗号フラグである。処理概要は以下の通りになる。

i. バイパスが設定された場合、バイパス設定フラグと非暗号フラグを ON にする。
ii. バイパスが解除された場合、バイパス設定フラグを OFF とする。
iii. 暗号処理終了後、バイパス設定フラグが OFF で非暗号フラグが ON の場合、暗号処理が正しく行われたか検証する。
iv. 検証に成功した場合、既知解テストを実施する。
v. 既知解テストが成功した場合、非暗号フラグを OFF にする。
vi. 出力データ送信手前で、バイパス設定フラグが OFF の場合、非暗号フラグが OFF であることを検証する。

10 設計保証

設計資料又は独立した資料として、状態遷移モデルの図又は表が必ず含まれていること。

設計資料及び証拠資料を、以下に示す。

- ●広域イーサ用１Gbps 暗号装置T-Cypher GigaEther 基本仕様書
- ●広域イーサ用１Gbps 暗号装置T-Cypher GigaEther ハードウェア基本仕様書
- ●広域イーサ用１Gbps 暗号装置T-Cypher GigaEther ファームウェア機能仕様書
- ●広域イーサ用１Gbps 暗号装置T-Cypher GigaEther 取扱説明書

11 その他の攻撃への対処

本装置において、その他の攻撃（DPA／SPA／タイミング攻撃／故障解析等）への対策は、行わない。したがって、その他の攻撃に対するセキュリティ要件は、適用外とする。