管　理　番　号
CD08－01－00－ 2355

CAFIS®

接続条件設計書

ＣＡＦＩＳ－ＴＣＰ／ＩＰ手順編

（プラチナⅡ）

第１．０版

平成 30 年　 5 月

株式会社ＮＴＴデータ

(Blank Page)

NTTDATA CONFIDENTIAL

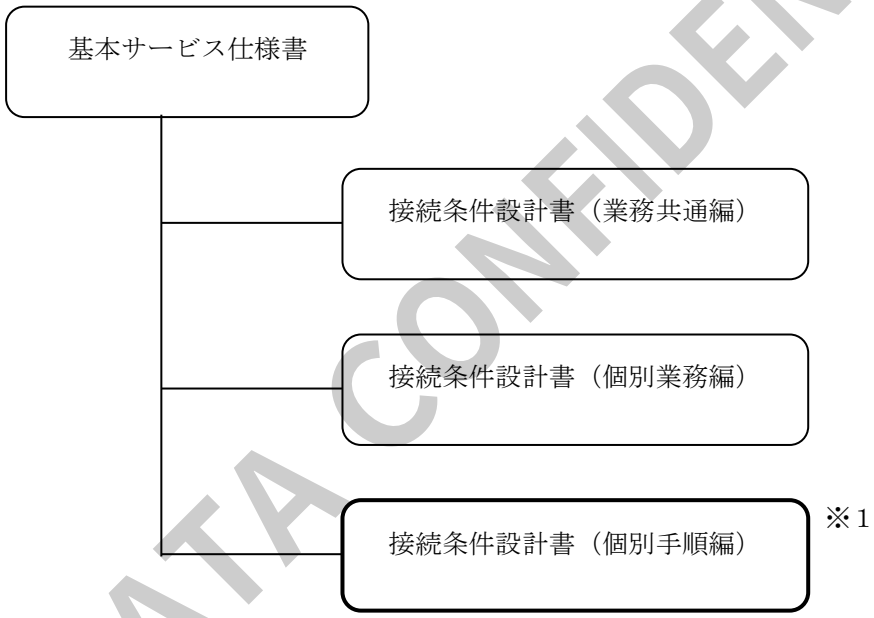
はじめに

本書は、株式会社ＮＴＴデータ（以下、ＮＴＴ ＤＡＴＡと言う）が運用するクレジット情報データ通信システム（Credit And Finance Information System）CAFIS®（以下、ＣＡＦＩＳと言う）の接続条件における、ＣＡＦＩＳ－ＴＣＰ／ＩＰ手順（プラチナⅡ）（以下、ＴＣＰ／ＩＰ手順と言う）について記述したものです。

【本書の位置づけ】

本書は、ＣＡＦＩＳの接続条件設計書の中で「個別手順編」の位置づけとなります。

ＣＡＦＩＳサービスで取扱う各業務仕様については、別冊の「個別業務編」を参照してください。



※１　各手順に応じた接続条件設計書が存在します。

Ｂ改手順

ＨＩ手順（ＥＢＣＤＩＣコード、シフトＪＩＳコード）

ＣＡＦＩＳ－ＰＳ手順（ＥＢＣＤＩＣコード、シフトＪＩＳコード）

ＣＡＦＩＳ－ＴＣＰ／ＩＰ手順（プラチナⅡ）

本書を「ＣＡＦＩＳ」接続以外の目的で使用することを禁じます。

本書は予告なく変更されることがあります。

本書を無断で他に転載することを禁じます。

本書を他に譲渡することを禁じます。

「CAFIS®」は、ＮＴＴ ＤＡＴＡの登録商標です。

NTTDATA CONFIDENTIAL

(Blank Page)

NTTDATA CONFIDENTIAL

修正履歴(1/1)	資　料　名	ＣＡＦＩＳ 接続条件設計書（CAFIS-TCP/IP 手順編（プラチナⅡ））			
項番	修　　正　　内　　容	修正理由	修正頁	旧　頁	修正年月
1	初版を作成。	－	－	－	H30.4

NTTDATA CONFIDENTIAL

NTTDATA CONFIDENTIAL

目　　　次

NTTDATA CONFIDENTIAL

(Blank Page)

NTTDATA CONFIDENTIAL

第１章　概　要

１．１ ネットワーク構成

ＴＣＰ／ＩＰ手順による接続を行う場合のネットワーク構成を図１．１－１に示します。

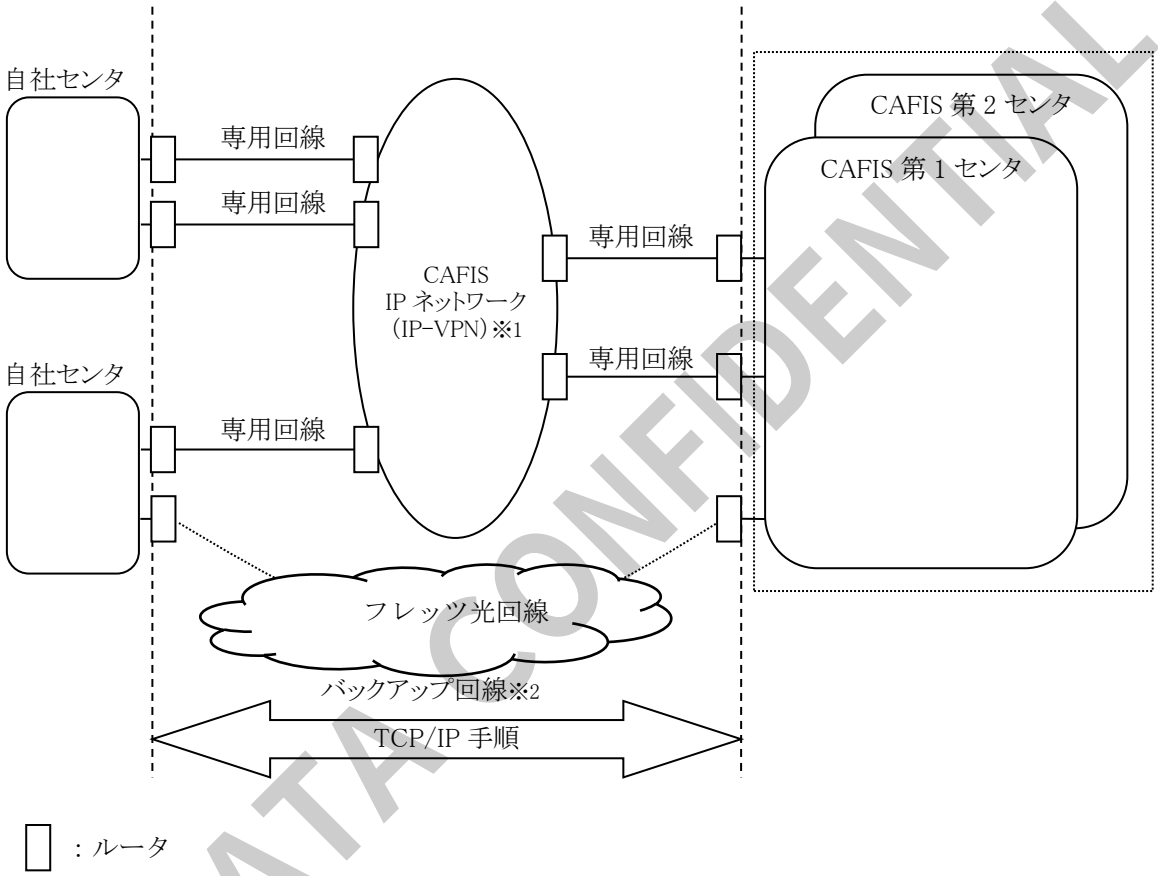


図１．１－１　ＴＣＰ／ＩＰ手順によるネットワーク構成図

※１　ＣＡＦＩＳ　ＩＰネットワーク（ＩＰ－ＶＰＮ）：経路帯域保証型のＩＰ網
※２　バックアップ回線：専用線障害時の迂回回線（オプション機能）

１．２　接続回線

本手順で利用できる接続回線は、光専用回線（イーサ回線）および光専用回線（イーサ回線）障害時のバックアップ回線（オプション機能）であるフレッツ光回線となります。

NTTDATA CONFIDENTIAL

１．３　伝送符号

１．３．１　文字コード

本インターフェースでの伝送符号は、「シフトＪＩＳコード」とします。

１バイト文字　：　JIS　X　0201　（ＡＮＫ文字）　および
　　JIS　X　0211　（C0 集合制御文字の一部）　（注１）
２バイト文字　：　JIS　X　0208 - 1997
　　（漢字 JIS は第 1 水準、第 2 水準とし外字は認めません）（注２）

（注１）　使用できる文字コード

コード値	定義文字	説明
０７	ＢＥＬ	ＢＥＬ符号
０Ａ	ＮＬ（ＬＦ）	改行
１２	ＤＣ２	出力装置制御
１８	ＣＡＮ	取消
１Ａ	ＳＵＢ	置換

上記コード値は他手順においてＣＡＦＩＳセンタで利用可能な伝送符号（JIS7,EBCDIC）に変換可能な文字となります。
上記以外の制御文字を受信した場合、ＣＡＦＩＳセンタにて電文破棄する場合があります。

（注２）　漢字コード

本手順としてシフトＪＩＳコードを利用することにより、漢字コードの利用が可能となります。ただし、漢字コードが利用できるのは、各業務の接続条件設計書においてデータ部内の項目属性に漢字コードの利用が可能となっている業務のみとします。
漢字コードの利用が許容されていない業務において利用された場合、提携先のセンタに正しく通知できない場合があります。

NTTDATA CONFIDENTIAL

１．３．２ バイナリデータ

本手順においては、８単位符号での伝送が可能となることから、バイナリデータの疎通を可能とします。

バイナリデータの疎通は、各業務の接続条件設計書において、データ部の項目属性がバイナリデータの利用可能となっている項目のみとします。

本手順をご利用頂く場合には、利用申し込み時にバイナリデータの取扱について「透過的に扱う」または「エンコード実施後キャラクタで扱う」のどちらかを選択して頂きます。「エンコード実施後キャラクタで扱う」を選択された場合には、ＣＡＦＩＳセンタから送信する電文については一律エンコードを実施した状態で送信します。

（1） バイナリデータの使用方法

バイナリデータ項目を扱う場合には、使用可能な業務において以下に示す共通フォーマットを利用します。共通フォーマットを表１．３．２－１に示します。

共通フォーマットは、各業務の接続条件設計書で記載されているデータ部の一部です。

表１．３．２－１ バイナリデータ疎通時のフォーマット

項番	項目名	桁数	内容
1	フォーマット種別	1	‘B’固定 （バイナリデータの利用可能を示す）
2	エンコード種別	1	エンコードの有無を示す。 ‘０’：エンコード無 ‘１’：Base６４によるエンコード
3	予備	2	スペース
4	格納データレングス	4	後続の格納データのレングスを１０進標記で示す
5	格納データ	可変	バイナリデータ （項番２のエンコード種別が１の場合にはエンコード後のデータ）

NTTDATA CONFIDENTIAL

（２） 取扱コードの変換について

ＣＡＦＩＳセンタの手順には、バイナリデータを透過的に扱えない手順があります。

また、本手順をご利用であってもバイナリデータの取扱を「エンコード後キャラクタで扱う」と指定された場合、バイナリデータを透過的に扱えないことになります。

したがって、取引の提携先センタの手順いかんによってはバイナリデータを中継できない場合があります。この場合にはＣＡＦＩＳセンタで提携センタへデータを中継する際に、表１．３．２－１で示した項目内容に準拠した形でエンコード種別を変更し、格納データ部をキャラクタにエンコードした後、取引を中継します。

また、バイナリデータ疎通の出来ない手順のお客様から本手順をご利用のセンタ（透過的な伝送可能）へ取引を中継する場合には、逆にＣＡＦＩＳセンタでデコードしバイナリデータに変換した後、取引を中継します。

図１．３．２－１にイメージ図を示します。

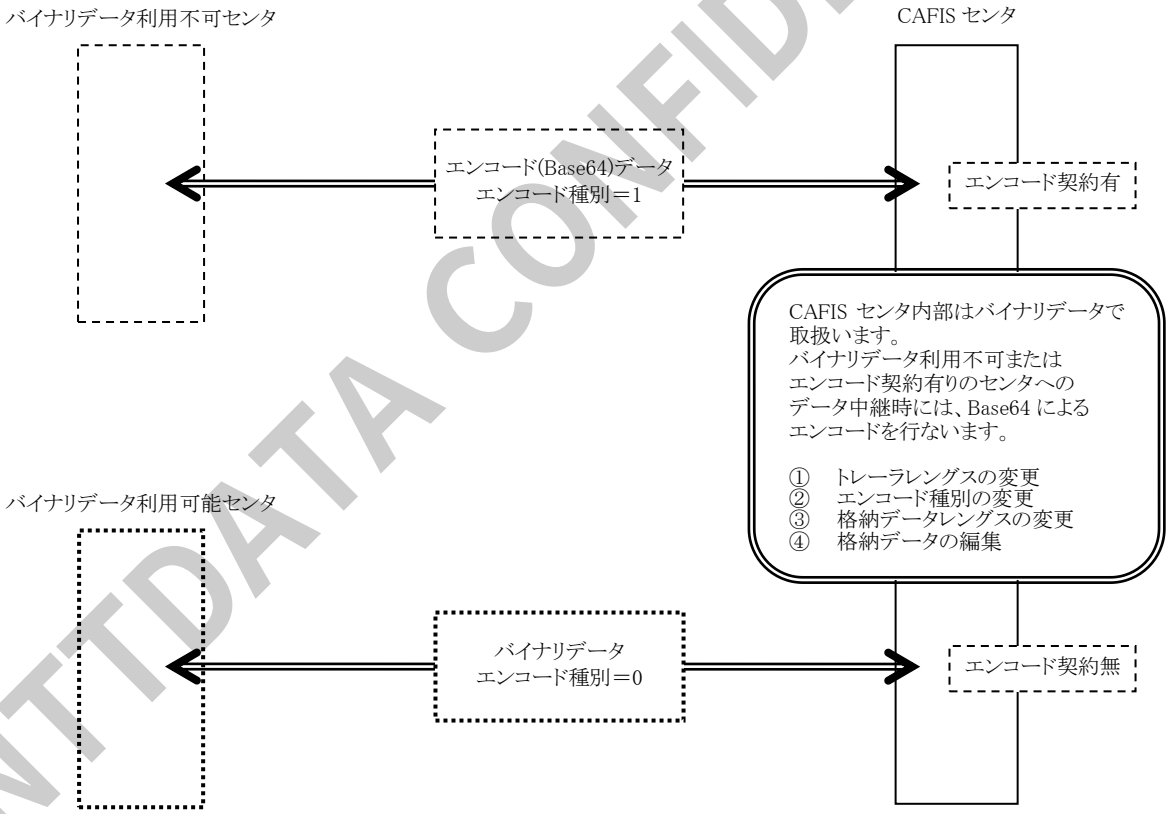


図１．３．２－１　伝送符号イメージ図

NTTDATA CONFIDENTIAL

（３） チェック

ＣＡＦＩＳセンタではバイナリデータのエンコード／デコードを行うために、各手順に対応したエンコード種別が設定されていることのチェックを行います。

本手順におけるチェック内容を表１．３．２－２に示します。

表１．３．２－２ チェック内容

ﾁｪｯｸ契機	事象	エラーの内容および原因	CAFIS センタでの処理	エラー発生時の対応
要求受信	エンコード種別不正	エンコード種別に‘１’（Base64 にてエンコード）と設定されている場合、Base64 で規定されている文字以外が設定されている	異常報告応答 Ｃ１７	処理を中止し、電文内容を調査する。
報告受信			電文破棄 （取消確認指令送信） (注)	提携センタからの申告により電文内容を調査する。

（注）障害電文に対する報告電文（取消報告・取消確認報告）に対しては、チェックは行いません。

NTTDATA CONFIDENTIAL

１．４　電文の暗号化

ＴＣＰ／ＩＰ手順を使用してＣＡＦＩＳセンタと接続する場合、取り扱う電文は他手順で取扱われているＣＡＦＩＳ業務電文と同じものを使用します。

各業務に対応する電文構成については、各業務の接続条件設計書を参照してください。

また、本手順においてはデータの漏洩および改竄を防止することを目的とし、自社センタ側ＶＰＮルータとＣＡＦＩＳセンタ側ＶＰＮルータ間について「ＩＰｓｅｃ※」を利用して暗号化を行います。

暗号化のイメージ図を図１．４―１に示します。

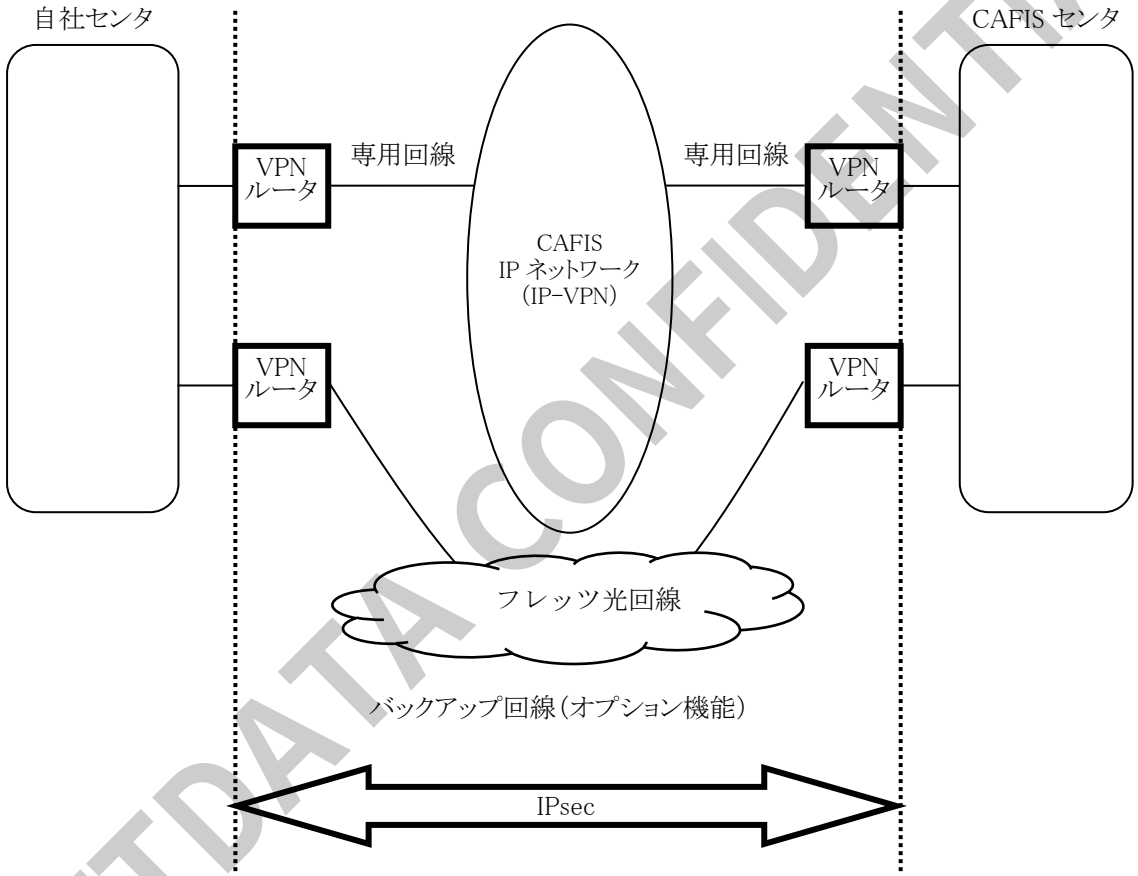


図１．４－１　暗号化イメージ図

（注）　自社センタ側のＶＰＮルータはＣＡＦＩＳセンタ指定の機器を設置して頂き、ＣＡＦＩＳセンタ側で保守を行うことを前提としております。

※ＩＰｓｅｃ：ＩＰパケットの暗号化と認証を行うＴＣＰ／ＩＰ環境下で汎用的に用いることができるセキュリティ技術。ネットワーク層で動作する。

NTTDATA CONFIDENTIAL

１．５　バックアップ回線

専用回線に障害が発生し、専用回線による自社センタ～ＣＡＦＩＳセンタ間の通信が出来ない場合、フレッツ光回線をバックアップ回線としてご利用が可能です。（バックアップ回線はオプション機能となります）

専用回線からフレッツ光回線への通信ルート切替処理については、付録「バックアップ回線機能概要」を参照して下さい。

NTTDATA CONFIDENTIAL

(Blank Page)

NTTDATA CONFIDENTIAL

第2章　通 信 制 御 仕 様

２．１　概　要

本章で説明する通信制御仕様は、単一回線による接続・複数回線による接続等、物理的なネットワーク構成には依存せず、全て同じ制御仕様で動作することとします。

ＴＣＰ／ＩＰ手順では、ＣＡＦＩＳセンタから要求を行い、自社センタの応答によって確立されたＴＣＰコネクションを論理回線とみなし、電文の送受信を行います。

電文送受信における概要図を図２．１－１に示します。

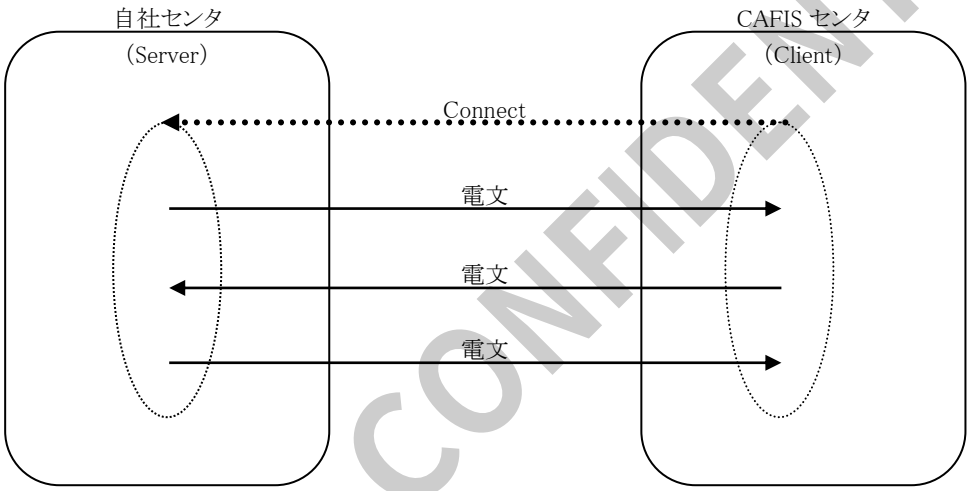


図２．１－１　電文送受信概要図

NTTDATA CONFIDENTIAL

２．２ ＴＣＰ(Transmission Control Protocol)

２．２．１　実装仕様

ＴＣＰの仕様については、ＲＦＣ７９３に準拠します。

２．２．２　コネクション数

接続コネクション数は、自社センタ毎に任意にご指定可能です。
（1会社コードあたり最大１０コネクション）

２．２．３　ポート番号

（１）　自社センタ（コネクション応答側）

コネクション応答側である自社センタのＣＡＦＩＳセンタ接続用ポート番号は、予めＣＡＦＩＳセンタから指定した番号となります。

【ＣＡＦＩＳセンタ接続用ポート番号】

商用サービス　：　２０１０

試験用（伝送制御試験・機能試験・総合確認試験）　：　２００９

上記ポート番号での取り扱いが出来ない場合は、商用サービスは２０Ｎ０（Ｎは１～９の整数）、試験用は２０Ｎ９（Ｎは０～９の整数）を指定して頂きます。

（２）　ＣＡＦＩＳセンタ（コネクション要求側）

コネクション要求側であるＣＡＦＩＳセンタのポート番号は、特に規定せずＣＡＦＩＳセンタ側で自動付与いたします。

NTTDATA CONFIDENTIAL

２．３　ＩＰ(Internet　Protocol)

２．３．１　実装仕様

ＩＰの仕様については、ＲＦＣ７９１に準拠します。

２．３．２　ＩＰアドレス

（１）　自社センタ側

自社センタ側（サーバ、ルータ）のＩＰアドレスは、任意にご指定可能です。
ただし、一部使用できないＩＰアドレスがあります。ご指定のＩＰアドレスが使用不可であるＩＰアドレスと重複した場合の対処については、ＣＡＦＩＳセンタで決定させて頂きます。

（２）　ＣＡＦＩＳセンタ側

ＣＡＦＩＳセンタのＩＰアドレスは、ＣＡＦＩＳセンタ側の収容位置およびネットワークの切替により複数存在します。
自社センタからの、電文送信時の宛先ＩＰアドレスは、コネクション要求時のＣＡＦＩＳセンタのＩＰアドレスを使用することとします。
また、使用するＩＰアドレスの範囲は事前にＣＡＦＩＳセンタより通知します。

（３）　ＮＡＴ変換（Network Address Translation）

自社センタ側に設置するルータでは、ＮＡＴ変換を実施しています。

NTTDATA CONFIDENTIAL

２．４　ソケット制御

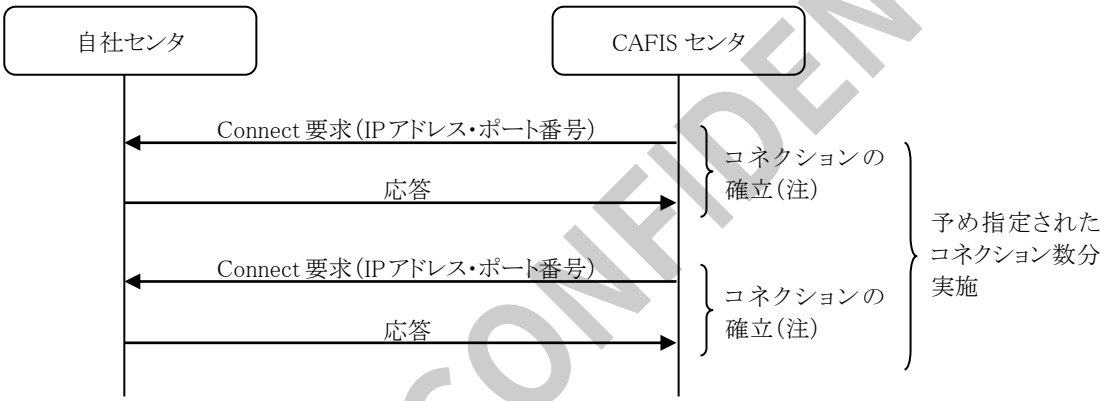
２．４．１　コネクション制御

（１）　コネクションの確立

ＴＣＰコネクションの確立は、ＣＡＦＩＳセンタから予め指定された自社センタのポート番号およびＩＰアドレス宛にコネクション確立要求を発行することにより行います。

コネクションの確立は、予め指定されたコネクション数分行います。コネクションが確立できない場合には、一定間隔で新たな確立を試みます。

コネクション確立イメージについて、図２．４．１－１、図２．４．１－２に示します



（注）３方向ハンドシェイク（ＳＹＮ+ＳＹＮ／ＡＣＫ＋ＡＣＫ）を便宜的に図示

図２．４．１－１ コネクション確立イメージ（正常）

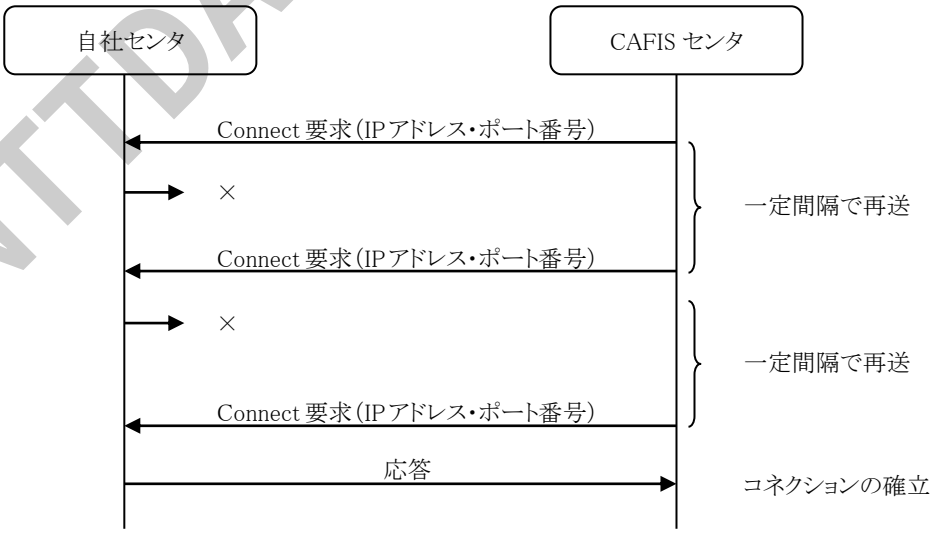


図２．４．１－２ コネクション確立（再送）イメージ

NTTDATA CONFIDENTIAL

（２） コネクション数

１自社センタあたりの最大コネクション数は１０とします。
ご利用頂くコネクション数については、任意にご指定可能です。
自社センタ側は、決められた数以上のコネクションをＣＡＦＩＳセンタから受け付けた場合には全コネクションを切断し、再度ＣＡＦＩＳセンタからのコネクション確立を待ちます。

（３） コネクションの切断

自社センタからコネクションの切断が行われた場合、ＣＡＦＩＳセンタから新たなコネクション確立を行います。

（４） コネクションの監視

ＣＡＦＩＳセンタはコネクション確立後、コネクションの接続状態を Keep Alive 機能により確認します。
Keep Alive において一定時間監視することにより接続状態を確認できなかった場合には、新たなコネクションの確立を行います。
また、自社センタで使用できる全てのコネクションが切断された場合、ＣＡＦＩＳセンタは自社センタの障害を認識します。
（障害認識後の処理は、ＣＡＦＩＳセンタからコネクション要求を自社センタへ送信し、コネクションが確立した場合、開始指令の送信を行います。）

Keep Alive 機能の詳細については、ＲＦＣ１１２２を参照して下さい。

NTTDATA CONFIDENTIAL

２．４．２　データ伝送

（１）　単一コネクションの場合のデータ伝送方式

１コネクションにより接続を行う場合は、コネクションレベルで全二重通信を行います。
単一コネクションの場合のデータ伝送方式例を図２．４．２－１に示します。

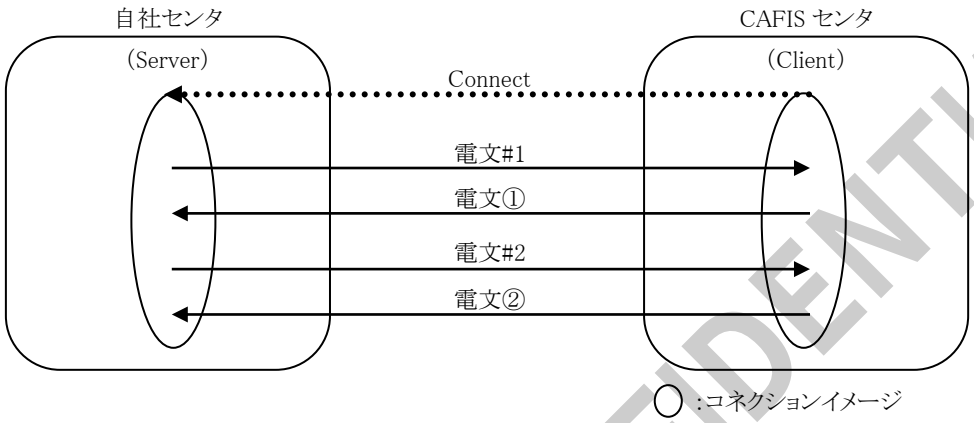


図２．４．２－１　単一コネクションの場合のデータ伝送方式例

（２）　複数コネクションの場合のデータ伝送方式

電文送信時、確立されたコネクションをラウンドロビンで選択し、電文の送受信を行います。
(要求電文と報告電文が同一コネクションで取り扱われるとは限りません)
複数コネクションの場合のデータ伝送方式例を図２．４．２－２に示します。

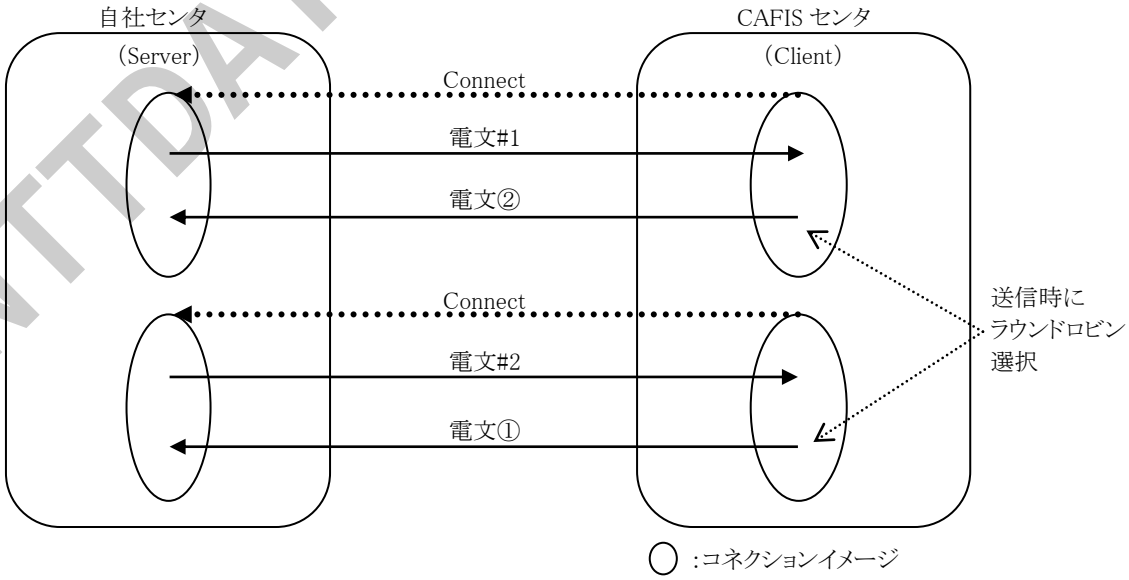


図２．４．２－２　複数コネクションの場合のデータ伝送方式例

NTTDATA CONFIDENTIAL

（３） 電文組立／分割

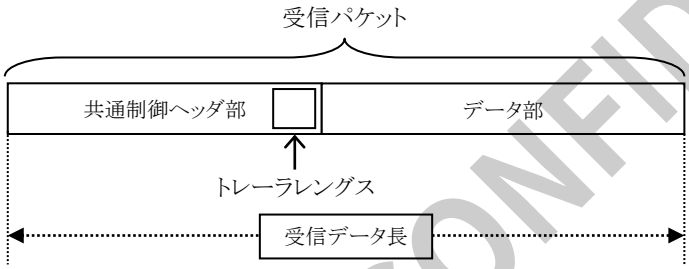
データパケットの再送に伴うバッファリング等で、１データパケット内に複数電文が存在する場合や１電文が複数パケットに分割される場合があります。このため、共通制御ヘッダ部のトレーラレングスをもとに電文の組立／分割を行います。

電文組立／分割において、トレーラレングス分の電文を受信できず電文組立に失敗した場合は、電文受信側で当該コネクションを切断し、ＣＡＦＩＳセンタから新たにコネクションを確立します。

＜パケットイメージ＞

① 電文組立／分割が不要な場合

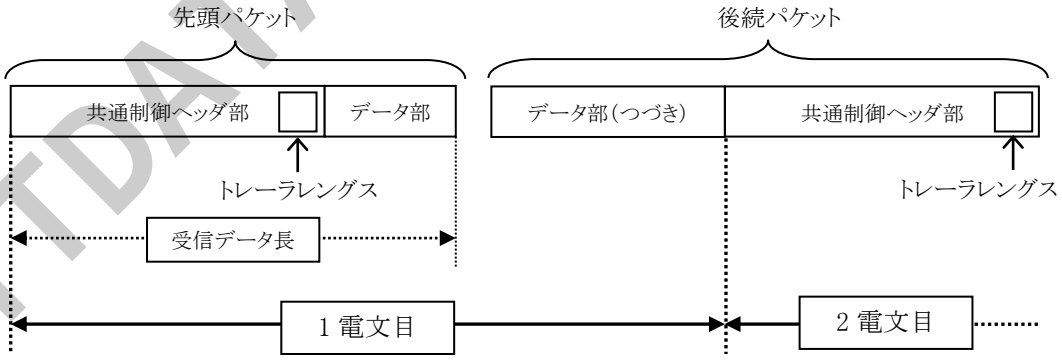
◆ 受信データ長 ＝ 共通制御ヘッダ部（６３）＋トレーラレングス長



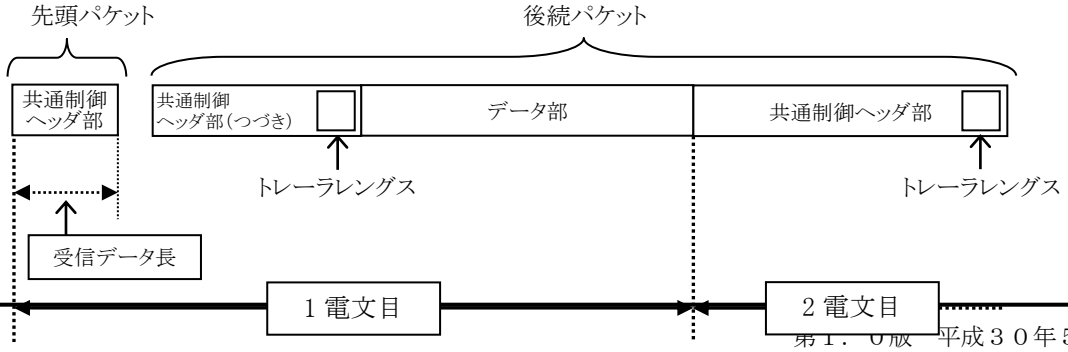
② 電文組立／分割が必要な場合

◆ 受信データ長 ≠ 共通制御ヘッダ部（６３）＋トレーラレングス長

(a) 先頭パケットにトレーラレングスを含む場合



(b) 先頭パケットにトレーラレングスを含まない場合

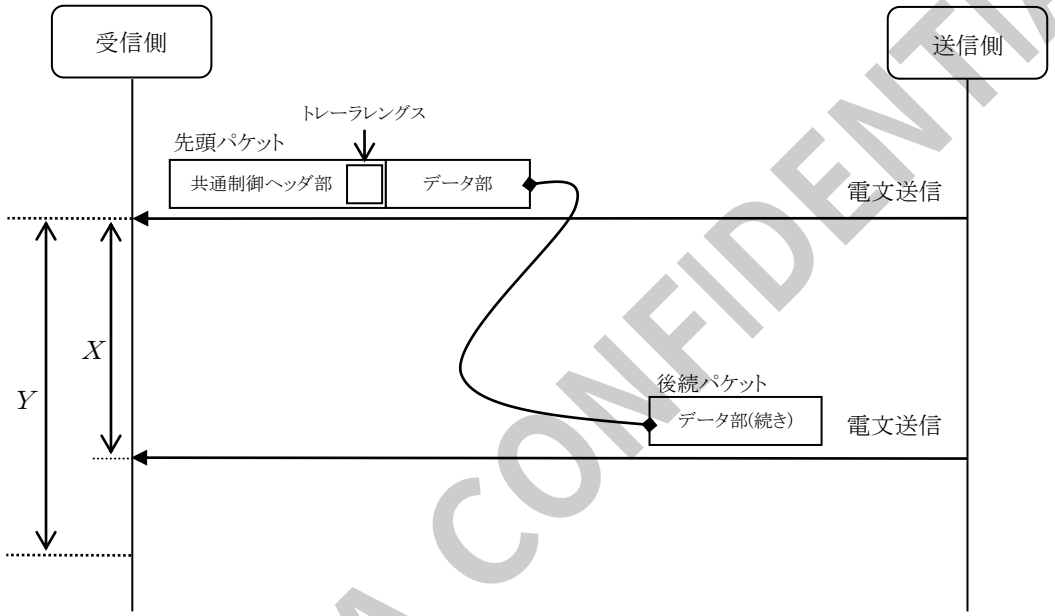


NTTDATA CONFIDENTIAL

（４） 電文組立／分割における後続パケット受信待ちタイマ

１電文が複数パケットに分割された場合において正常な電文送受信は、先頭パケットを受信後、受信側で設定した後続パケット受信待ちタイマ内で後続パケットを受信します。その後、共通制御ヘッダ部のトレーラレングスをもとに受信した先頭パケットと後続パケットを電文に組立てます。

複数パケットに分割された電文の正常な送受信の概要図を図２．４．２－３に示します。なお、後続パケット受信待ちタイマは、受信側で任意に設定可能です。



Ｘ：先頭パケット受信後から後続パケット受信までの経過時間

Ｙ：受信側で設定した後続パケット受信待ちタイマ

図２．４．２－３　複数パケットに分割された電文の正常送受信概要図

ネットワーク障害が発生した場合、現状のＣＡＦＩＳセンタでは通信断を検知してから無通信状態が４８秒以上経過した回線を回線障害と認識します。回線や通信機器が冗長化されている箇所では、回線障害を認識する前に障害箇所の切替処理を行います。

自社センタが電文受信中にネットワーク障害が発生し、切替処理をした場合においても自社センタで該当コネクションを切断せず、正常に電文送受信を処理させるには、後続パケット受信待ちタイマとして４８秒以上に設定することを推奨いたします。（本件はＣＡＦＩＳセンタとの接続にあたっての必須要件ではありません。）

なお、４８秒未満に設定された場合は、メンテナンスや障害発生時のネットワーク切替完了前に該当コネクションが切断され、回線障害となる可能性がございますことにご注意ください。

NTDATA CONFIDENTIAL

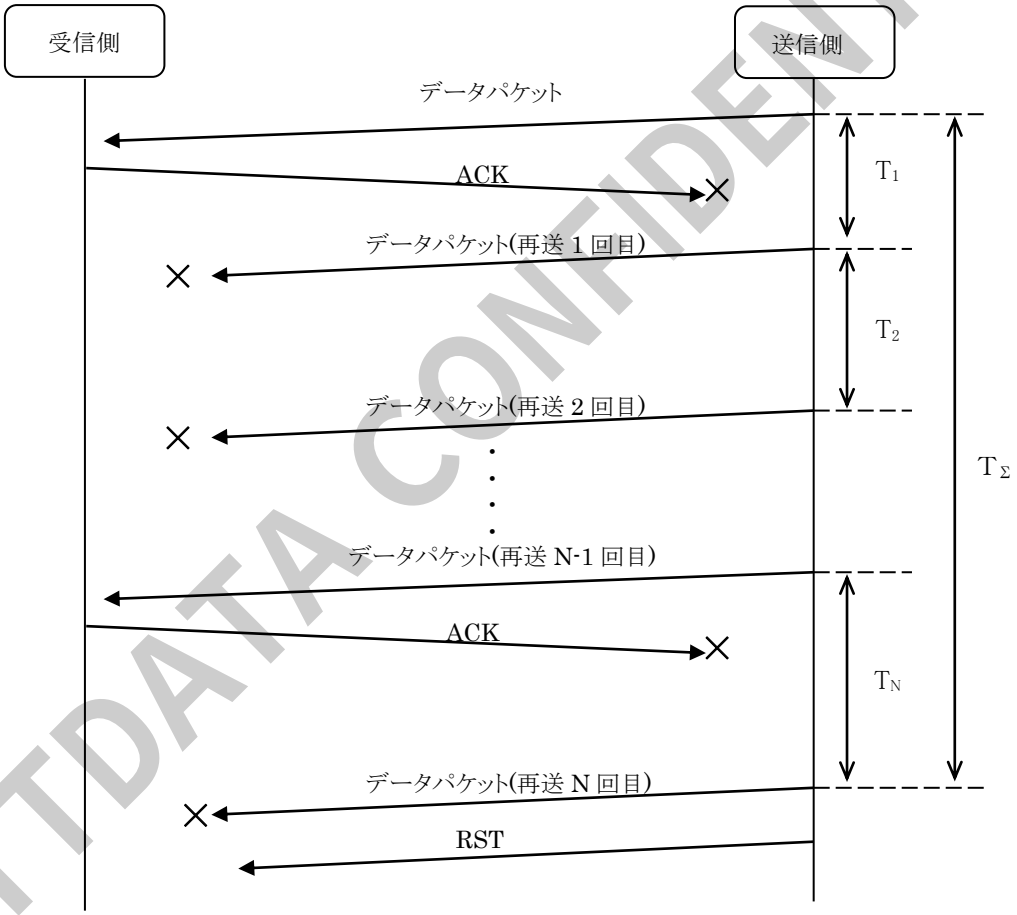
（５） ＴＣＰ再送制御

ＴＣＰデータパケットを送信後、応答確認パケット(ACK)を受信しない場合（*）、再送制御により、設定した再送タイマ（T_n：ｎは回数）経過後に同一データパケットが再送されます。

設定した再送回数(Ｎ回)分再送が行われますが、それでもＡＣＫを受信しないと、送信側はRSTパケットを送信し、コネクションを切断します。

ＴＣＰデータパケットの再送処理の概要図を図２．４．２－４に示します。

(*) 送信したパケットは受信側で正常に受信されるが、ACK が送信側にて正常に受信できない場合、もしくは送信したパケットが受信側で正常に受信できない場合を指します。



T_n ： ｎ回目の再送時における再送タイマ

Ｎ ： 再送回数

T_Σ ： Ｎ回分の再送タイマ合計値；$T_1+T_2+\cdots+T_n$

図２．４．２－４ TCP データパケットの再送処理概要図

後続パケット受信待ちタイマ同様、再送タイマ合計値（T_Σ）を４８秒以上になるよう設定することを推奨いたします。（本件はＣＡＦＩＳセンタとの接続にあたっての必須要件ではありません。）

NTTDATA CONFIDENTIAL

（６） Keep Alive 監視

ＣＡＦＩＳセンタから自社センタへの Keep Alive 監視の処理・設定値については、後述する「２．４．３ネットワーク監視」をご参照ください。

自社センタにおきまして、Keep Alive 監視を有効とする場合は、後続パケット受信待ちタイマ同様、Keep Alive による監視がコネクション異常と判断するまでの時間（Keep Alive 応答待ちタイマと Keep Alive 応答待ちカウンタの掛け合わせた値（*））を４８秒以上になるよう設定することを推奨いたします。（本件はＣＡＦＩＳセンタとの接続にあたっての必須要件ではありません。）

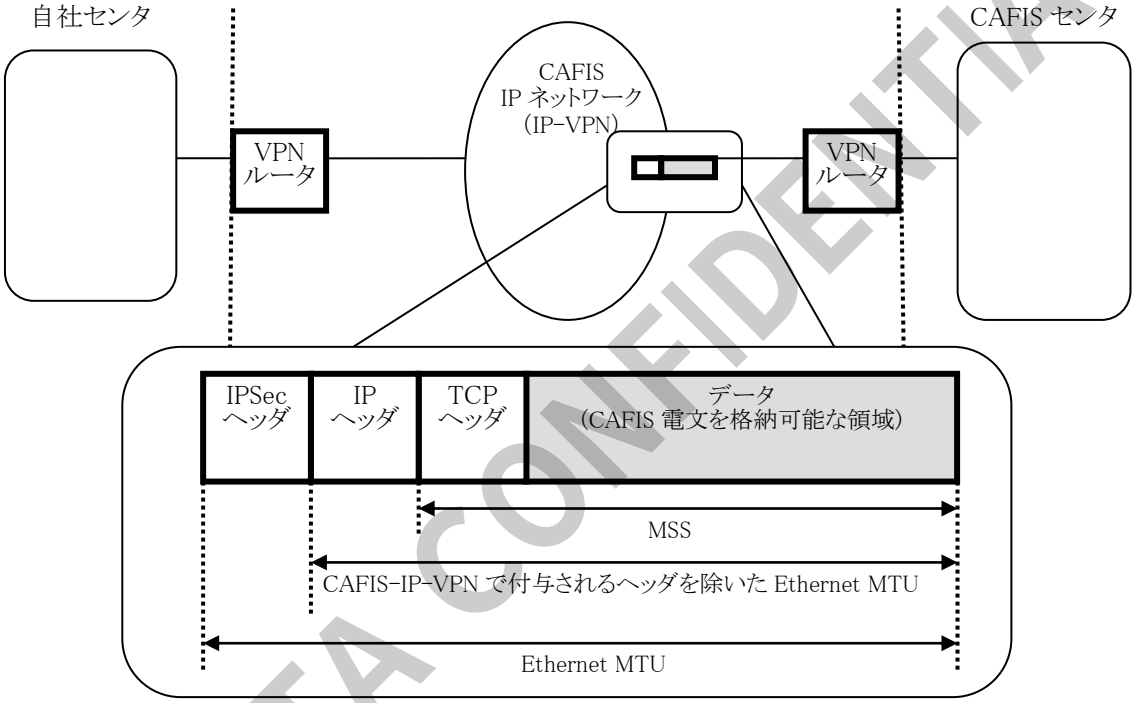
(*)表 2.4.3-1 参照。タイマ②×カウンタ①のことを示す。

NTTDATA CONFIDENTIAL

（７） ＭＳＳ・ＭＴＵについて（データ長の制限）

ＣＡＦＩＳ－ＴＣＰ/ＩＰでは、暗号化のためのオーバヘッドを考慮して下記の値を推奨致します。
（本件はＣＡＦＩＳセンタとの接続にあたっての必須要件ではありません。）

推奨ＭＴＵ ： １４１４［ｂｙｔｅ］
推奨ＭＳＳ ： １３７４［ｂｙｔｅ］



・各ヘッダの詳細はRFC2401・791・793をご参照ください。
・Ethernet MTUは1500バイトで計算しております。

図２．４．２－５ ＩＰパケット概念図

NTTDATA CONFIDENTIAL

２．４．３ ネットワーク監視

（１） 各種タイマおよびカウンタ

本手順で使用するＣＡＦＩＳセンタ側でのネットワーク監視タイマおよびカウンタ、処理説明の図番を表２．４．３－１に示します。

表２．４．３－１ ネットワーク監視タイマおよびカウンタ

項番	名称	数値	用途	図番 (図中タイマ名)
1	無通信監視タイマ	40秒	自社センタ～CAFISセンタ間の無通信状態が継続した場合、Keep Alive 送信における接続状態の有効確認の監視タイマ	図2.4.3-1 (タイマ①)
2	Keep Alive 応答待ちタイマ	6秒	CAFISセンタから自社センタへの Keep Alive が無応答の場合、接続状態の有効確認 Keep Alive 応答待ちタイマ	図2.4.3-2 (タイマ②)
3	Connect 要求応答待ちタイマ 1	80秒	CAFISセンタが回線障害を認識した場合、CAFISセンタから自社センタへの Connect 要求応答待ちタイマ	図2.4.3-3 (タイマ③)
4	Connect 要求応答待ちタイマ 2	180秒	CAFISセンタが回線障害を認識し、Connect 要求応答待ちタイマ1がタイムオーバした場合、CAFISセンタから自社センタへの Connect 要求応答待ちタイマ	図2.4.3-3 (タイマ④)
5	Keep Alive 応答待ちカウンタ	8回	CAFISセンタから自社センタへの Keep Alive が無応答の場合、接続状態の有効確認 Keep Alive 応答待ちカウンタ	図2.4.3-2 (カウンタ①)
6	Connect 要求送信カウンタ 1	4回	CAFISセンタが回線障害を認識した場合、CAFISセンタから自社センタへの Connect 要求送信カウンタ	図2.4.3-3 (カウンタ②)

（注）表２．４．３－１に記述した数値は、現状のＣＡＦＩＳセンタにおける設定値であり、今後変更することがあります。

NTTDATA CONFIDENTIAL

（２）　各種監視手順

本手順でのネットワーク監視手順を以降に示します。

① Keep Alive 応答正常受信時の処理

自社センタ～ＣＡＦＩＳセンタ間における Keep Alive 応答正常受信時の処理を図２．４．３－１に示します。

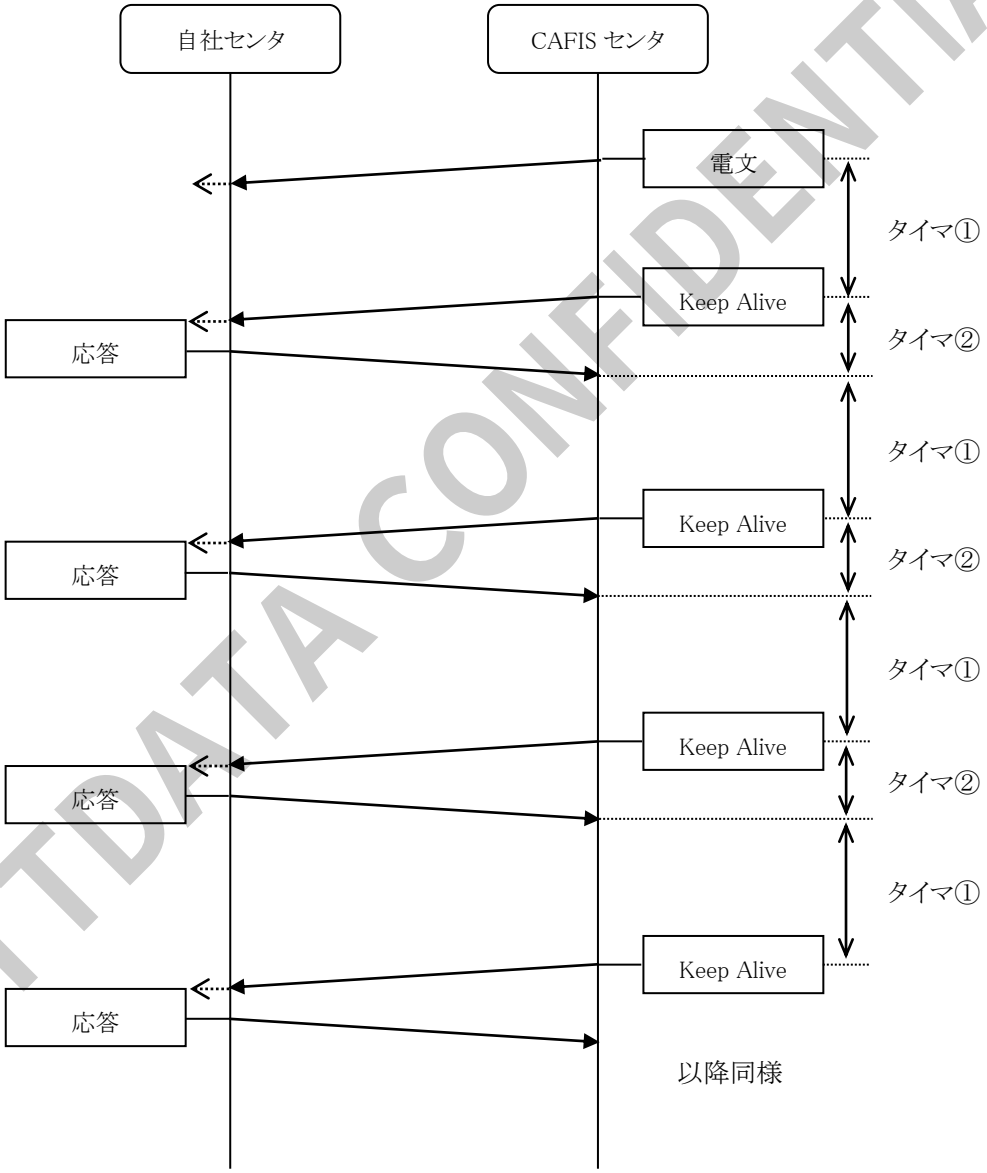


図２．４．３－１ Keep Alive 応答正常受信の処理

NTTDATA CONFIDENTIAL

② Keep Alive 応答受信タイムオーバ時の処理

自社センタ～ＣＡＦＩＳセンタ間における Keep Alive 応答受信タイムオーバ時の処理を図２．４．３－２に示します。

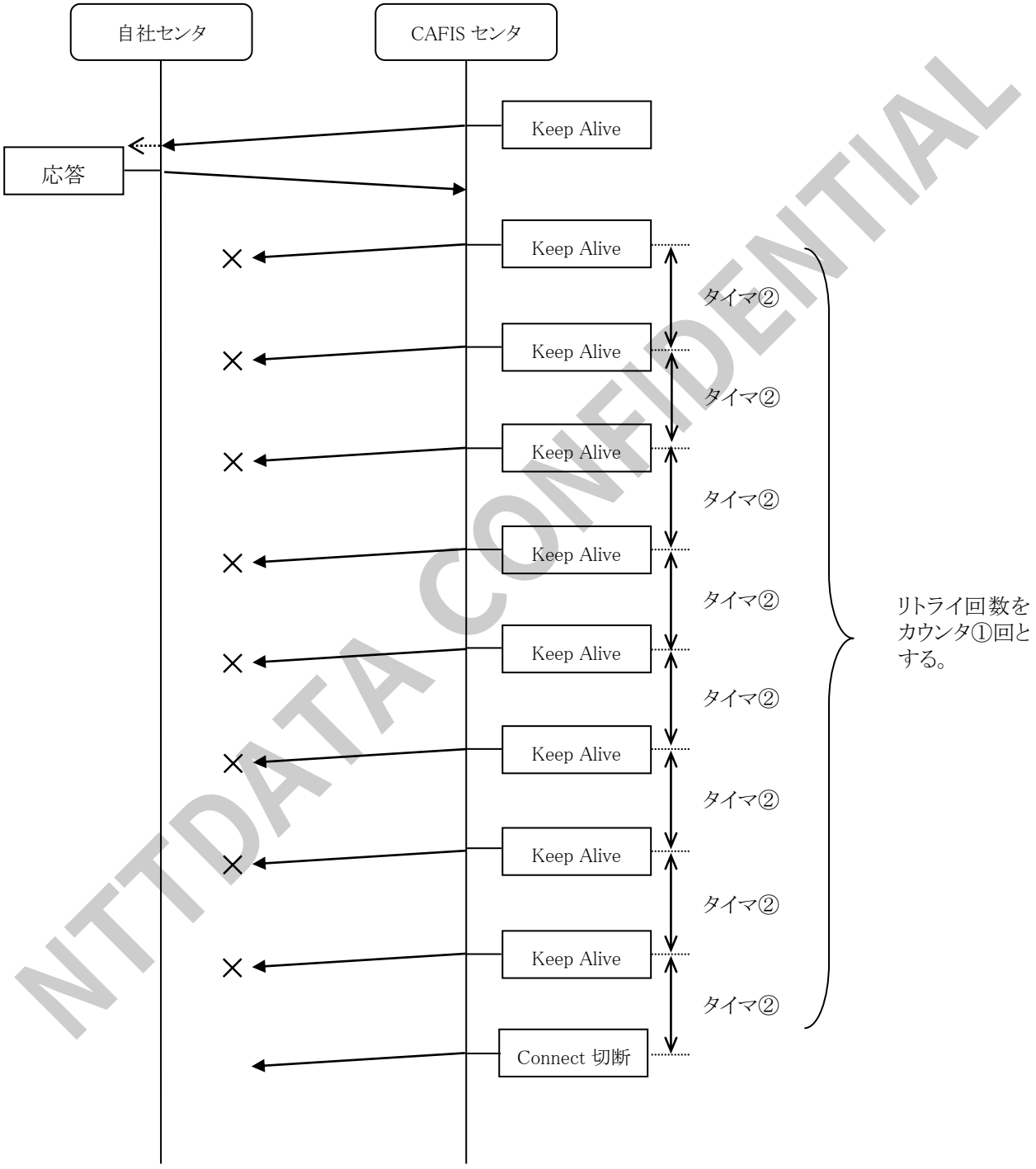


図２．４．３－２ Keep Alive 応答受信タイムオーバ時の処理

NTTDATA CONFIDENTIAL

③ Connect 応答受信タイムオーバ時の処理

自社センタ～ＣＡＦＩＳセンタ間における Connect 応答受信タイムオーバ時の処理を図２．４．３－３に示します。

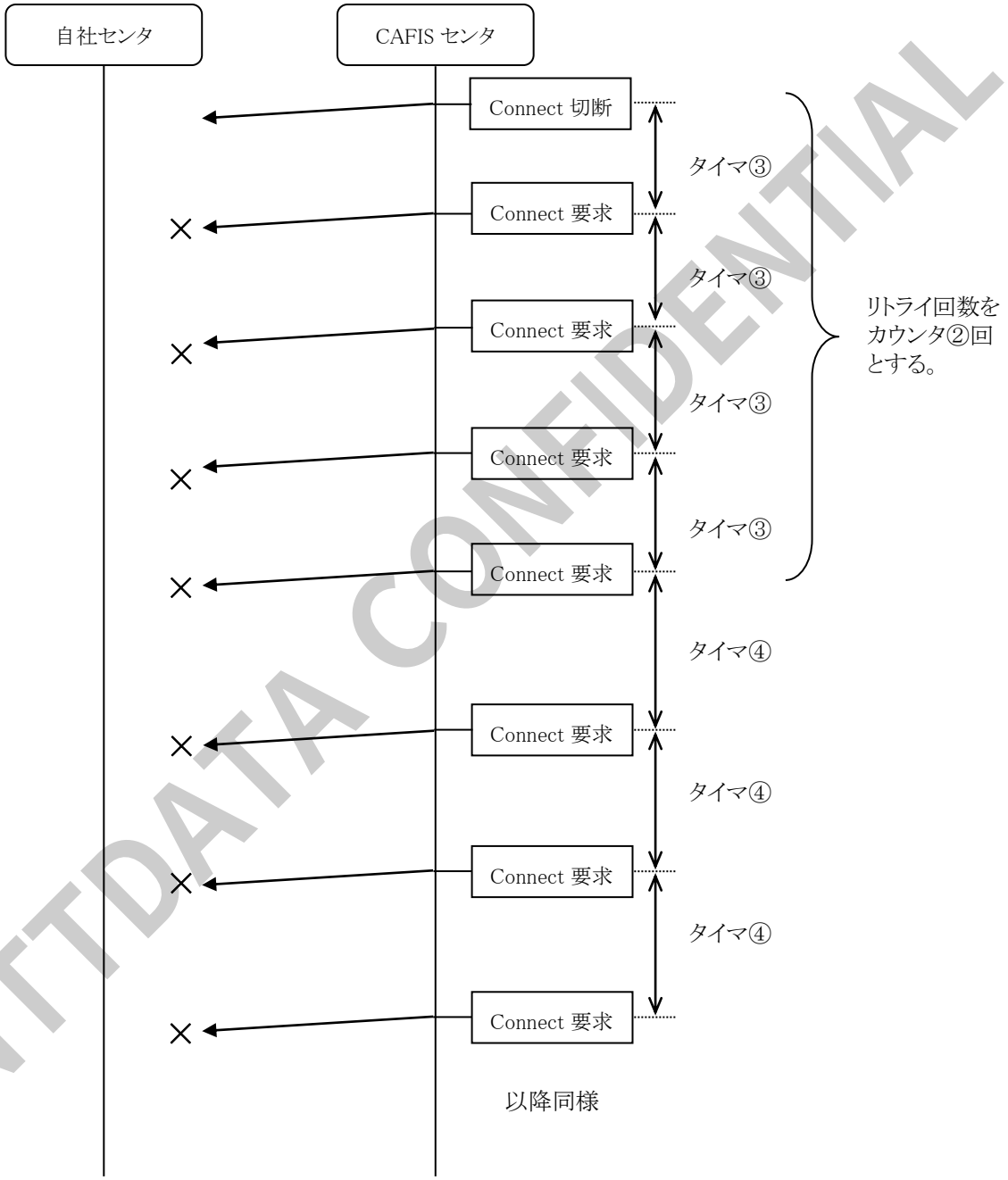


図２．４．３－３ Connect 要求応答受信タイムオーバ時の処理

NTTDATA CONFIDENTIAL

２．５　　経路制御

サーバアプリケーションが定義する仮想的な通信路のことを本手順書では「経路」と呼びます。報告電文は必ず、要求電文と同じ経路で送信されます。自社センタは要求電文に対する報告電文を受信するまでは、同一経路で新たに要求電文を送信することはできません。

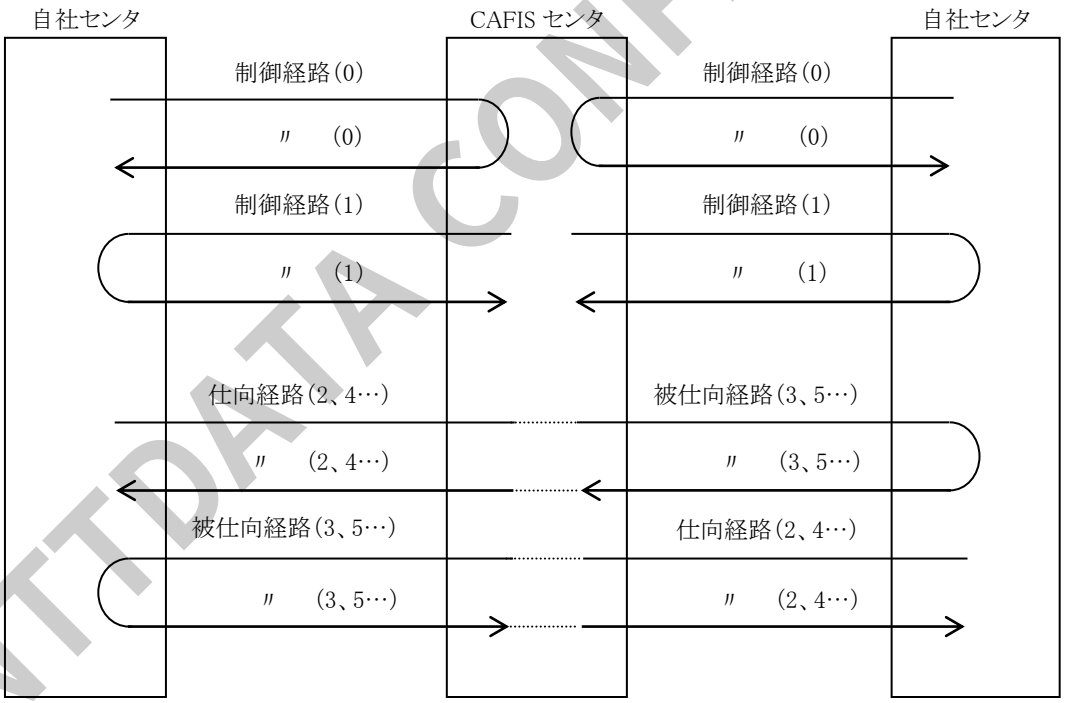
経路番号はＣＡＦＩＳセンタで取扱う電文全てに対して設定される４桁の番号です。共通制御ヘッダ部の先頭に設定され、取引種類（制御／業務）、方向（仕向／被仕向）および関連取引の引き当てに使用されます。

自社センタにおいて取引の同時仕掛可能数が経路数となります。

２．５．１　経路の種類

経路は制御電文の送受信に使用する「制御経路」、被仕向電文の送受信に使用する「被仕向経路」および仕向電文の送受信に使用する「仕向経路」の３種類とします。

各経路の概要を図２．５．１－１に、経路番号を表２．５．１－１に示します。



（注）（ ）内の数字は経路番号を示す。

図２．５．１－１　各経路の概要

NTTDATA CONFIDENTIAL

表２．５．１－１　経路番号

経路の種類	経路番号
制御経路	0:自社センタからの制御要求送信 1:CAFISセンタからの制御要求送信
仕向経路	偶数番号 2、4、6、……、(有効経路数 - 2)
被仕向経路	奇数番号 3、5、7、……、(有効経路数 - 1)

※例 … 経路数６３経路の場合

・仕向経路の最大経路番号：１２６

・被仕向経路の最大経路番号：１２７

２．５．２　経路の数

制御経路は回線数によらず２固定となります。（回線数が増えても増加なし）

仕向経路と被仕向経路は必ず同じ数となります。

１会社コードとして設定できる最大経路数は仕向経路＝被仕向経路＝１８９経路です。

２．５．３ 経路、コネクションおよび回線の関係

経路、コネクション、回線はそれぞれ独立して管理することとし、相互のくくりつけは行いません。

２．５．４ 経路の選択

取引発生の際は空き経路を任意に選択します。

NTTDATA CONFIDENTIAL

２．５．５ 同一経路による取引が必要となるケース

取消確認指令電文は元となる取引と同一経路を使用して送信します。
取消確認再指令電文は、元となる取引および取消確認指令と同一経路を使用して送信します。
取消再指令電文は、取消指令電文と同一経路を使用して送信します。

NTTDATA CONFIDENTIAL

２．５．６ 経路開放のタイミング

（１） 仕向経路開放タイミング

仕向経路開放タイミングを図２．５．６－１に示します。

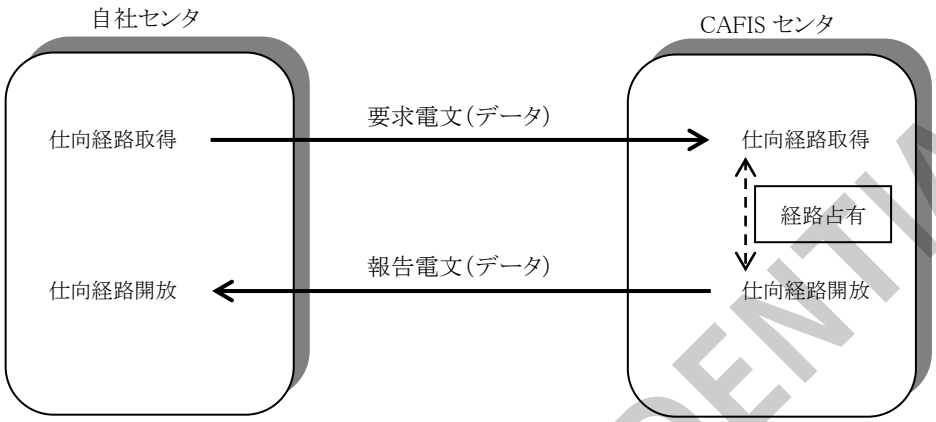


図２．５．６－１ 仕向経路開放のタイミング

（２） 被仕向経路開放タイミング

被仕向経路開放タイミングを図２．５．６－２に示します。

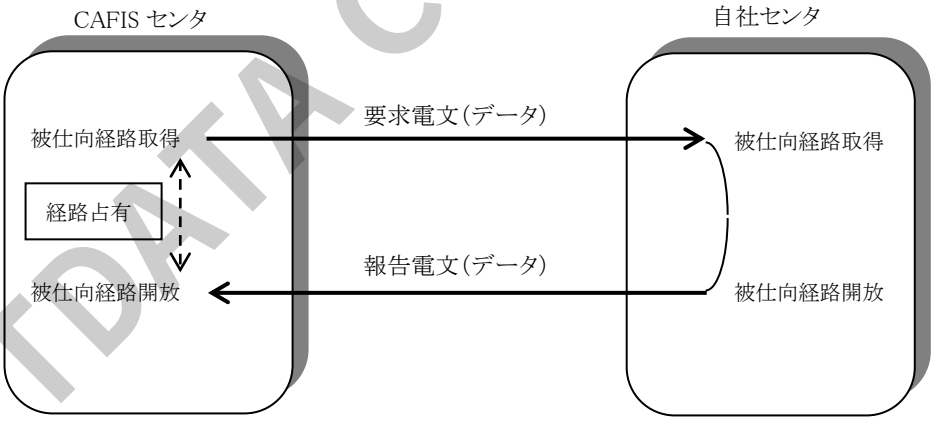


図２．５．６－２ 被仕向経路開放のタイミング

NTTDATA CONFIDENTIAL

＜付録＞　　バックアップ回線機能概要

オプション機能であるバックアップ回線における処理内容について以降に示します。

＜目　次＞

NTTDATA CONFIDENTIAL

修正履歴	資料名	ＣＡＦＩＳ 接続条件設計書（CAFIS-TCP/IP 手順編（プラチナⅡ）＜付録＞）			
項番	修　正　内　容	修正理由	修正頁	旧　頁	修正年月
1	新規作成	－	－	－	H30.3

NTTDATA CONFIDENTIAL

NTTDATA CONFIDENTIAL

第１章　概　要

バックアップ回線を設定している自社センタにおいて専用回線に障害が発生した場合、専用回線からバックアップ回線へ自動的に切替り、フレッツ光回線を経由したルートでＣＡＦＩＳセンタと通信を確立します。また、障害が復旧した場合には、バックアップ回線から専用回線へ自動的に切戻ります。

専用回線からバックアップ回線への回線切替／切戻処理概要を図１．１－１に示します。

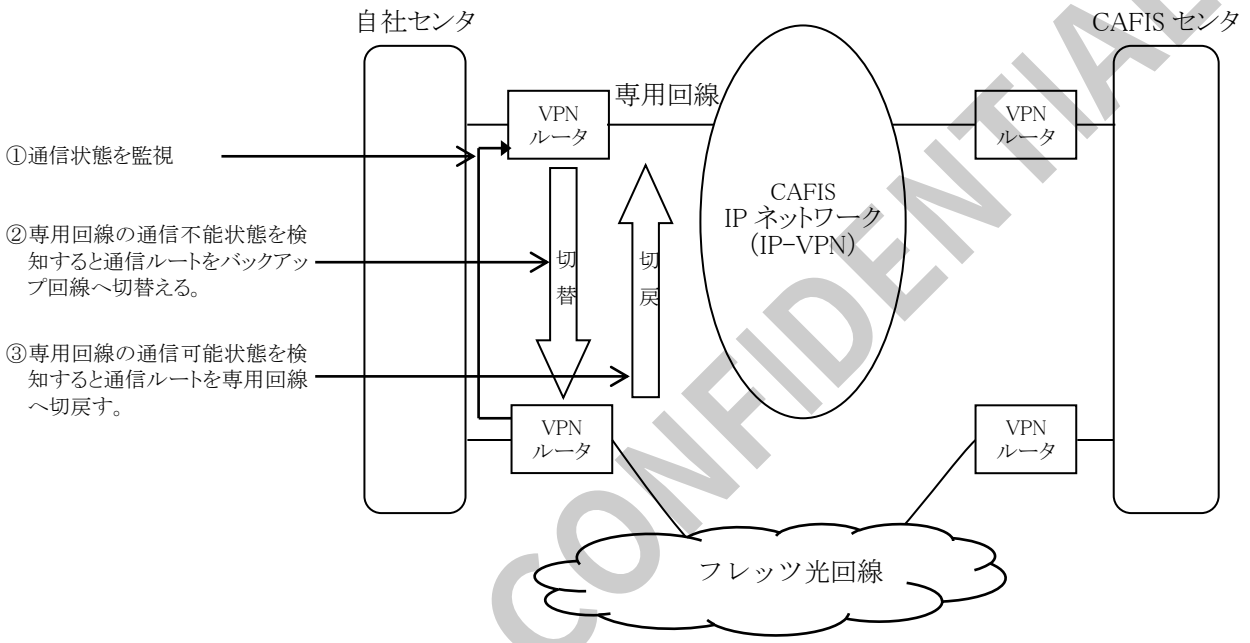


図１．１－１　回線切替／切戻処理概要図

自社センタ側のバックアップ回線接続ＶＰＮルータが専用回線接続ＶＰＮルータの通信状態を監視しており、専用回線の障害発生により通信不能状態を検知するとフレッツ光回線を経由した通信ルートへ回線切替処理を行います。また、障害復旧により専用回線の通信可能状態を検知すると専用回線を経由した通信ルートへ回線切戻処理を行います。

回線切替／切戻処理は、専用回線の通信可否状態で自動的に行われます。また処理により送信出来なかったパケットは、処理動作完了後に再送されます。

NTDATA CONFIDENTIAL

(Blank Page)

NTTDATA CONFIDENTIAL

ＣＡＦＩＳ 接続条件設計書（ＣＡＦＩＳ－ＴＣＰ／ＩＰ手順編（プラチナⅡ））

［第１．０版］　平成３０年５月

作成責任者
株式会社ＮＴＴデータ　　カード&ペイメント事業部　　IT サービス企画担当

Ｃｏｐｙｒｉｇｈｔ©２０１８　ＮＴＴ　ＤＡＴＡ
Ｒｅｖｉｓｅｄ　　２０１８　ＮＴＴ　ＤＡＴＡ

複製厳禁・無断転載禁止