



SWIFTNet Messaging Services

SWIFTNet 6.1

サービスディスクリプション (Service Description)

本書は SWIFTNet サービスおよび製品について説明しています。特に、SWIFTNet メッセージングソリューション、SWIFTNet コアメッセージングサービス、技術およびオペレーション環境について説明しています。本書は SWIFTNet ユーザー、SWIFT パートナー、SWIFT サービスビューローのスタッフを対象としています。

本書は日本語参考訳です。英語版が優先します。

2007 年 12 月 6 日



免責事項

著作権

Copyright © S.W.I.F.T. SCRL (“SWIFT”), Avenue Adèle 1, B-1310 La Hulpe, Belgium, or its licensors, 2007. All rights reserved.

本書を組織内でコピーすることは構いません。但し、以下の法的事項を必ず記載してください。

守秘義務

本書には SWIFT およびサードパーティの機密情報が含まれています。SWIFT から事前に書面による許可を得ずに、本書を外部に開示することはできません。

免責事項

内容は作成時点で最新のものですが、適宜変更される場合があります。必ず最新版を参照するようにしてください。

翻訳版について

本書は日本語参考訳です。英語版が優先します。

商標

SWIFT、S.W.I.F.T.、SWIFT ロゴ、Sibos、SWIFTNet、SWIFTAlliance、SWIFTStandards、SWIFTReady および Accord は S.W.I.F.T. SCRL の商標です。SWIFTSolutions、SWIFTWatch、SWIFTSupport など SWIFT から派生したその他のサービスおよび製品名は S.W.I.F.T. SCRL の商標です。SWIFT は S.W.I.F.T. SCRL の商号です。本書に記載されているその他の全ての製品または企業名は各所有者の商号、商標、または登録商標です。

序文

本書について

本書は SWIFTNet サービスおよび製品について説明しています。特に、SWIFTNet メッセージングソリューション、SWIFTNet コアメッセージングサービス、技術およびオペレーション環境について説明しています。

本書の最新版は、www.swift.com > Ordering & Support > Documentation で入手して頂くことができます。

ノート 本サービスディスクリプションおよび *SWIFT 一般条件 (SWIFT General Terms and Conditions)* そしてその他関連サービス文書は、SWIFT と顧客の間における SWIFTNet メッセージングサービスの使用条件などに関する契約条項において必要不可欠なものです。

本書の対象者

本書は SWIFT ユーザー、SWIFT パートナー、SWIFT サービスビューローのスタッフを対象としています。

SWIFT 定義による用語

本書には、顧客、ユーザー、SWIFT のサービスおよび製品など、SWIFT の文書において使用された場合に特定の意味を持つ用語が含まれています。本書もしくは SWIFT Glossary で定義されているこうした用語は、以下のように強調表示されています：SWIFT は、安定した標準メッセージングサービスおよびインターフェースソフトウェアを顧客に提供しています。

重要な変更

本バージョンでは、以下の主要な変更について記載されています：

- オptionalリリース SWIFTNet 6.1 に関連する機能や特長：
 - 新たな SWIFTNet FileAct HeaderInfo ブロック (3.2.2.2, “HeaderInfo”を参照してください)
 - SWIFTNet FileAct 用の新たなコピー機能 (3.4, “SWIFTNet Copy”を参照してください)
 - SWIFTNet FileAct ストアアンドフォワード用に増大されたファイルサイズ (3.2.3.7, “あらゆるファイルコンテンツの送信”を参照してください)
 - 先進的な配信管理 (デリバリーコントロール) 機能のサポート (3.5.5, “先進的な配信管理 (デリバリーコントロール)”を参照してください)
 - SWIFTNet FileAct と SWIFTNet FIN、または SWIFTNet InterAct 間における通信フローの自動分離 (3.2.3.12, “SWIFTNet FileAct により使用されるリソースの自動制御”を参照してください)
- SWIFTNet PKI に関連した変更：

- オフラインで証明書管理を行う、新たな SWIFT Secure Channel アプリケーションに関する情報 (6.8.2, “オフライン証明書管理”を参照してください)
- SWIFTNet PKI セクションの新たなレイアウト

関連文書

SWIFTNet のユーザーである場合、以下の文書が直接関係します。:

- *HSM Box Terms and Conditions*
- *HSM Card, Reader, and Token Terms and Conditions*
- *Interface Vendor Specifications for SWIFTNet InterAct and FileAct*
- *SWIFT By-laws*
- *SWIFT コーポレートルール*
- *SWIFT Data Retrieval Policy*
- *SWIFT General Terms and Conditions*
- *SWIFT Glossary*
- *SWIFT Personal Data Protection Policy*
- *SWIFT Price List*
- *SWIFT Service Bureau Policy*
- *SWIFTNet Certificate Administration Guide*
- *SWIFTNet Connectivity Packs*
- *SWIFTNet Implementation Guide*
- *SWIFTNet Link Interface Specifications*
- *SWIFTNet Naming and Addressing Guide*
- *SWIFTNet Network Access Control Guide*
- *SWIFTNet Resilience Guide*
- *SWIFTNet Service Administration Guide*
- *SWIFTNet Service Design Guide*

SWIFTNet メッセージングサービスのご利用度合いにより、有意義だと思われる文書が他にも沢山あります。より詳細な情報については、SWIFT サポートサービスを参照してください。

目次

1	はじめに	11
1.1	セキュア IP ネットワークへのアクセス	11
1.2	SWIFTNet Link およびインターフェースソフトウェア	12
1.2.1	SWIFTNet Link	12
1.2.2	インターフェース	12
1.3	SWIFTNet 公開鍵基盤(PKI)	13
1.4	SWIFTNet メッセージングサービスへの登録	14
2	SWIFTNet メッセージングソリューション	15
2.1	主要コンセプトおよび用語集	15
2.2	メンバーもしくは市場インフラにより管理されるソリューション	16
2.2.1	主な役割および責任	16
2.2.2	登録と適格条件	17
2.3	SWIFT 管理ソリューション	18
2.3.1	主な役割および責任	18
2.3.2	汎用メッセージングソリューション	19
2.3.2.1	概要	19
2.3.2.2	登録と適格条件	19
2.3.3	ビジネス固有の SWIFT ソリューション	20
3	SWIFTNet コアメッセージングサービス	21
3.1	SWIFTNet InterAct	21
3.1.1	SWIFTNet InterAct の作業モード	21
3.1.1.1	リアルタイムメッセージングモード	22
3.1.1.2	リアルタイム照会回答モード	22
3.1.1.3	ストアアンドフォワードメッセージングモード	22
3.1.2	メッセージ構成とキーヘッダーフィールド	23
3.1.3	SWIFTNet InterAct の標準機能	24
3.1.3.1	認証管理	25
3.1.3.2	クローズドユーザーグループ管理	26
3.1.3.3	Role-Based Access Control (ロールベースアクセス管理)	26
3.1.3.4	機密性の管理	27
3.1.3.5	整合性管理	27
3.1.3.6	メッセージの検証	28
3.1.3.7	セントラルメッセージルーティング	28
3.1.3.8	独自参照とタイムスタンプ	29
3.1.4	SWIFTNet InterAct の付加価値オプション機能	29
3.1.4.1	メッセージプライオリティ	29
3.1.4.2	否認防止 (Non-repudiation)	30
3.1.4.2.1	発信元の否認防止	30
3.1.4.2.2	発信の否認防止	30
3.1.4.2.3	受信の否認防止	32
3.1.4.3	送信完了通知	32

3.1.5	サービスアドミニストレーターが定義できる機能	33
3.2	SWIFTNet FileAct	33
3.2.1	SWIFTNet InterAct の作業モード	33
3.2.1.1	リアルタイムのファイル送信モード	33
3.2.1.2	リアルタイムのファイルダウンロードモード	34
3.2.1.3	ストアアンドフォワードのファイル送信モード	35
3.2.2	ファイル送信構成とキーヘッダーフィールド	35
3.2.2.1	ファイル送信構成	35
3.2.2.2	HeaderInfo	37
3.2.3	SWIFTNet FileAct の標準機能	37
3.2.3.1	認証管理	38
3.2.3.2	クローズドユーザーグループ管理	39
3.2.3.3	Role-Based Access Control (ロールベースアクセス管理)	39
3.2.3.4	機密性の管理	40
3.2.3.5	整合性管理	40
3.2.3.6	セントラルファイルルーティング	41
3.2.3.7	あらゆるファイルコンテンツの送信	41
3.2.3.8	ファイルの同時送信	42
3.2.3.9	実行中のファイル送信をキャンセル	42
3.2.3.10	ファイル送信ステータスと進捗状況	42
3.2.3.11	断続的な通信エラーの処理	43
3.2.3.12	SWIFTNet FileAct により使用されるリソースの自動制御	43
3.2.3.13	汎用 SWIFTNet FileAct ディレクトリ	43
3.2.4	SWIFTNet FileAct の付加価値オプション機能	44
3.2.4.1	ファイルのプライオリティ	44
3.2.4.2	否認防止 (Non-repudiation)	44
3.2.4.2.1	発信元の否認防止	45
3.2.4.2.2	発信の否認防止	45
3.2.4.2.3	受信の否認防止	47
3.2.4.3	送信完了通知	47
3.2.5	サービスアドミニストレーターが定義できる機能	48
3.3	SWIFTNet Browse	48
3.3.1	特定の機能	50
3.4	SWIFTNet Copy	51
3.4.1	機能	51
3.4.1.1	SWIFTNet Copy の作業モード	51
3.4.1.1.1	Y-Copy モード	51
3.4.1.1.2	T-Copy モード	53
3.4.1.2	SWIFTNet Copy サービスパラメータ	53
3.4.1.3	SWIFTNet Copy の処理	54
3.4.1.4	SWIFTNet Copy 通常モード/フォールバック (代替) モード	55
3.4.1.5	緊急変更	55
3.4.1.6	パイロットサービス	56
3.4.2	セキュリティおよび管理	56
3.4.3	責任範囲	56
3.4.3.1	サービスアドミニストレーター	56

3.4.3.2	システムオペレーター	57
3.4.3.3	サービス登録機関	58
3.5	ストアアンドフォワード作業モード	58
3.5.1	キューの種類	58
3.5.2	送信モード	59
3.5.3	メッセージもしくはファイルの不達	60
3.5.4	ストアアンドフォワードにおけるアクセス管理	61
3.5.5	先進的な配信管理（デリバリーコントロール）	62
3.6	セントラルルーティングルール	62
3.6.1	ルーティングルールのフォーマット	63
3.6.2	ルーティングの行動様式	65
3.6.3	複数のルーティングアドレスを使用する	65
3.6.4	別のエンドポイントアドレスに通信をルーティングする	66
3.6.5	リクエストに一致する MRR ルールがない場合のルーティング行動様式	66
3.6.6	複数の MRR ルールが同ランクだった場合のルーティングの挙動	67
3.6.7	MRR とストアアンドフォワードキュー	67
4	SWIFTNet 技術環境	68
4.1	SWIFTNet インフラストラクチャとセントラルシステム	68
4.2	SWIFTNet Integration Testbed	69
4.2.1	目的	69
4.2.2	ITB での SWIFTNet サービス	70
4.2.3	可用性とパフォーマンス	71
4.2.4	サポート	71
4.2.5	責任範囲	71
4.3	SWIFTNet 本番環境	72
4.3.1	SWIFTNet 本番環境の役割	72
4.3.2	SWIFTNet システムの耐障害性	72
4.3.3	オペレーティング状況に異常がある場合	73
4.4	SWIFTNet と FIN の間におけるブリッジ	73
5	セキュア IP ネットワーク	74
5.1	セキュア IP ネットワークの概要	75
5.2	SIPN アクセス構成	75
5.3	低通信量のダイアルアクセス	76
5.3.1	低通信量のダイアルアクセスに向いているユーザーとは	76
5.3.2	アクセス説明	76
5.3.3	初期不良が発生した後の復旧	77
5.4	SWIFT が管理する常時接続回線サービス	77
5.4.1	コンタクトポイント	78
5.4.2	Managed-Customer Premises Equipment（加入社宅内機器）	78
5.4.3	接続構成	79
5.4.4	Dual-I 構成	80
5.4.5	複数回線構成での Single-P	83
5.4.6	Dual-P 構成	84

5.5	ユーザーネットワーク構成	86
6	SWIFTNet 公開鍵基盤(PKI)	88
6.1	概要	88
6.1.1	コンポーネント	88
6.1.2	証明書管理	89
6.1.3	キーとパスワードの管理	90
6.1.4	暗号化機能	91
6.2	ロール	92
6.2.1	ユーザー ロール	92
6.2.1.1	エンティティ	92
6.2.1.2	代理人	93
6.2.1.3	Security Officer (セキュリティオフィサー)	93
6.2.1.4	Shared Security Officer (シェアードセキュリティオフィサー)	95
6.2.1.5	エンティティ、エンドユーザー、代理人の関係	95
6.2.2	SWIFT ロール	96
6.2.2.1	証明書認証 (Certification Authority)	96
6.2.2.2	登録機関 (Registration Authority)	96
6.2.2.3	SWIFTNet ディレクトリアドミニストレーター (Directory Administrator)	97
6.2.2.4	Policy Management Authority (ポリシーマネジメントオーソリティ)	97
6.3	証明書	97
6.3.1	フォーマット	97
6.3.2	タイプと使用先	98
6.3.2.1	テストおよび本番の証明書	98
6.3.2.2	SWIFTNet InterAct、SWIFTNet FileAct、Web Certificates	98
6.3.2.3	SNL Instance Certificate	99
6.3.2.4	ビジネス証明書および簡易証明書	99
6.3.2.5	SWIFTNet CA 証明書	100
6.3.2.6	証明書使用の概要	100
6.3.3	証明書の期限切れ	101
6.3.4	Certificate Revocation List (証明書破棄リスト)	101
6.4	公開鍵と秘密鍵	102
6.4.1	SWIFTNet InterAct と SWIFTNet FileAct キー	102
6.4.2	ウェブ認証鍵	103
6.5	パスワード	104
6.6	Hardware Security Modules (ハードウェアセキュリティモジュール)	106
6.6.1	USB ベースの HSM	106
6.6.2	LAN ベースの HSM	107
6.7	セキュリティオフィサーおよびシェアードセキュリティオフィサーの登録	107
6.7.1	セキュリティオフィサー (SO) の登録	108
6.7.2	シェアードセキュリティオフィサーの登録	109
6.8	オンラインおよびオフラインでの証明書管理	109
6.8.1	エンティティおよび証明書のオンライン管理	109
6.8.2	オフライン証明書管理	110
6.8.3	証明書管理責任	111

6.8.4	記録のアーカイブ	112
6.9	エンティティと証明書管理	112
6.9.1	エンティティの登録	112
6.9.2	証明書用のアプリケーション	113
6.9.3	証明書の発行と配布	113
6.9.4	証明書とキーの更新	114
6.9.5	エンティティの回復	115
6.9.6	エンティティの破棄	115
6.9.7	エンティティの無効化	117
6.9.8	エンティティの破棄、回復、無効化	117
7	身元の確認および認証	119
8	登録および終了	120
8.1	登録	120
8.2	終了	120
9	オーダー	121
10	SWIFT サポート	122
11	ロールと責任	123
11.1	SWIFT のロールと責任範囲	123
11.1.1	一般	123
11.1.1.1	サービスの導入と条件	123
11.1.1.2	サービスの変更	123
11.1.2	SWIFTNet メッセージング特定のロールと責任範囲	124
11.1.3	SWIFTNet PKI 特定のロールと責任範囲	124
11.1.4	セキュア IP ネットワークへのアクセスサービス	125
11.1.4.1	専用回線 DSL および ISP 加入者回線での SIPN アクセス	125
11.1.4.1.1	専用回線でのアクセス	125
11.1.4.1.2	モニタリングおよび構成のアップデート	126
11.1.4.1.3	接続障害が発生した場合のアクション	126
11.1.4.1.4	専用回線を通じた VPN ボックスのメンテナンス	126
11.1.4.2	ダイヤルアップ回線でのセキュア IP ネットワークへのアクセス	127
11.1.4.2.1	ダイヤルアップ回線でのアクセス	127
11.1.4.2.2	構成アップデート	128
11.1.4.2.3	代替接続のフェイルオーバー	128
11.1.4.2.4	ダイヤルアップ回線を通じた VPN ボックスのメンテナンス	128
11.2	ユーザーのロールと責任範囲	129
11.2.1	一般	129
11.2.1.1	解釈	129
11.2.1.2	関連する契約条件の順守	129
11.2.1.3	アクセス、所有、使用	130
11.2.1.4	事前の変更通知が必要な場合	130
11.2.1.5	オペレーティング要件	130
11.2.1.6	アクセスと協力	130
11.2.1.7	守秘義務	131

11.2.2	SWIFTNet メッセージング特定のロールと責任範囲	131
11.2.2.1	サービスアドミニストレーターのロールおよび責任範囲	131
11.2.2.2	顧客の責任範囲	132
11.2.3	SWIFTNet PKI： 特定のロールと責任範囲	133
11.2.3.1	登録	133
11.2.3.2	セキュリティオフィサー	133
11.2.3.3	エージェント	134
11.2.3.4	有効化シークレット、証明書、秘密鍵に関する責任	134
11.2.3.5	エージェントによる秘密鍵の使用	135
11.2.3.6	取引先の証明書への依存	135
11.2.3.7	サービスビューロー	137
11.2.3.8	HSM	137
11.2.4	セキュア IP ネットワークに特定のロールへのアクセスサービスと責任範囲	137
11.2.4.1	セキュア IP ネットワークへの接続	137
11.2.4.2	ユーザーの利用（用途限定）	138
11.2.4.3	VPN ボックスの取扱い	139
11.2.4.4	SNL-VPN 接続	139

1 はじめに

前提条件

SWIFTNet をご利用頂くには、ユーザー環境において以下の条件を満たす必要があります:

- **SWIFT セキュア IP ネットワークへのアクセス**

セキュア IP ネットワーク(SIPN)にアクセスする際、ユーザーは異なる回線容量や耐障害性を持つ複数の接続方法および構成から選択することができます。

- **SWIFTNet Link およびインターフェースソフトウェア**

SWIFTNet Link (SNL) ソフトウェアはインターフェースソフトウェアにとって必要不可欠です。インターフェースソフトウェアと一体化していても構いませんし、分離しているものを別途入手しても構いませんが、全ての SWIFTNet ユーザーが必要とするものです。インターフェースソフトウェアは以下の製品/サービスにおいて使用可能です: SWIFTAlliance Gateway、SWIFTAlliance WebStation、サードパーティが提供しているインターフェース。

- **SWIFTNet 公開鍵基盤(PKI)**

ユーザーが個人もしくはアプリケーションを SWIFTNet サービスにアクセスさせたい場合、セキュリティオフィサー(SO)に登録し、適切な認証が付与される必要があります。

- **SWIFTNet メッセージングサービスへの登録**

ユーザーは、適切な SWIFT メッセージングサービスに登録する必要があります。

パイロット (テストアンドトレーニング) もしくは実稼働の本番環境において SWIFTNet メッセージングサービスを使用することができるのは、SWIFT ユーザーのみです。

ユーザーは、特定の SWIFTNet メッセージングソリューションとの関連において SWIFTNet サービスを使用します。メッセージングソリューションに関するより詳細な情報は“SWIFTNet メッセージングソリューション” ページの 15 を参照してください。

1.1 セキュア IP ネットワークへのアクセス

概要

セキュア IP ネットワーク (SIPN)は、SWIFT のグローバルネットワークです。SWIFTNet ユーザーコミュニティに SWIFT サービスを提供するために使用されます。

アクセス方法

ユーザーが SWIFTNet サービスにアクセスするには、2つの方法があります:

- **SWIFT に直接接続**

ユーザーが自社のネットワークアクセス機器を使用して、SWIFTNet に直接接続します。

- **SWIFT に間接接続**

サードパーティ (SWIFT ユーザーもしくはサービスビューロー) を通じて SIPN に接続します。ユーザーは、サードパーティと合意した接続方法とインターフェースソフトウェアを使用し、SWIFT とは無関係にサードパーティと接続します。

ノート 直接接続、間接接続のいずれの場合も、ユーザーは様々な技術的ソリューション（ダイヤルアップ、常時接続回線アクセスなど）を使用して SIPN にアクセスすることができます。最適な接続方法を決定するために、ユーザーは予測される通信量や必要な耐障害性のレベルなど、その他の要素についても考慮に入れる必要があります。技術的な詳細については、“セキュア IP ネットワーク” ページの 74 を参照してください。

1.2 SWIFTNet Link およびインターフェースソフトウェア

1.2.1 SWIFTNet Link

説明

SWIFTNet Link (SNL)は、ユーザーが SWIFTNet メッセージングサービスの機能にアクセスするために必要とする、必須ソフトウェアです。SNL を使用することにより、SWIFTNet メッセージングサービスを使用するアプリケーションの技術的な相互運用性およびセキュリティが強化されます。

ユーザーは、SNL を使用するにあたって以下の方法から選択することができます：

- SWIFT ソフトウェアインターフェースのいずれかを使用する（SWIFTAlliance Gateway または SWIFTAlliance WebStation）
- サードパーティが提供しているインターフェースを使用する
- SNL ソフトウェアに直接接続するアプリケーションを導入する

SWIFT に直接接続しているユーザーは、どちらのインターフェースを使用して SWIFTNet サービスにアクセスするかを選択することができます。サービスビューローを通じて接続しているユーザーは、サービスビューローオプションの中から選択することができます。

1.2.2 インターフェース

SWIFT インターフェース

SNL と接続する SWIFT ソフトウェアは：

- **SWIFTAlliance Gateway です。**

SWIFTAlliance Gateway は、高スループットおよび社内アプリケーションとの密接な相互作用を必要とする環境向けのインターフェースです。また、アプリケーション間の情報伝達にも最適です。

SWIFTAlliance Gateway に関するより詳細な情報は、*SWIFTAlliance Gateway Service Description* を参照してください。

ノート SNL は、SWIFTAlliance Gateway には内蔵されていません。別途 SNL を購入し、SWIFTAlliance Gateway 環境に組み込む必要があります。

- **SWIFTAlliance WebStation**

SWIFTAlliance WebStation は、コミュニケーションが個人対アプリケーションである環境向けのインターフェースです。ユーザーは、SWIFTNet を通じてアクセスできるウェブサーバ

ーにブラウザアクセスすることができるほか、ローカルにある特定のサービスに特化されたモジュールのサービス GUI (Service GUI、グラフィカルユーザーインターフェース) を使用することもできます。

SWIFTAlliance WebStation に関するより詳細な情報は、*SWIFTAlliance WebStation Service Description* を参照してください。

ノート SWIFTAlliance WebStation には、内蔵型 SNL が搭載されています。つまり、ユーザーは SWIFTAlliance WebStation を使用するために別の SNL を購入/構成する必要はありません。しかしながら、WebStation が SWIFTNet メッセージングサービスにアクセスするために SWIFTAlliance Gateway もしくは SWIFTAlliance Starter Set を使用している場合はこの限りではありません。

サードパーティ提供のインターフェース

ベンダーは、デベロッパーツールキットを使用することにより、自社のインターフェースソリューションを導入して SWIFTNet にアクセスすることができます。

デベロッパー向け情報

自社製インターフェースの導入に関するより詳細な情報は、以下を参照してください。:

- *Interface Vendor Specifications for SWIFTNet InterAct and FileAct*
- *SWIFTAlliance WebStation Developers Toolkit*
- *SWIFTAlliance Gateway Service Description*
- *SWIFTAlliance WebStation Developers Toolkit*
- *SWIFTAlliance WebStation Service Description*
- *SWIFTNet Link Developers Toolkit*
- *SWIFTNet Link Interface Specifications*
- *SWIFTNet Link Service Description*
- *SWIFTNet Service Design Guide*

1.3 SWIFTNet 公開鍵基盤(PKI)

概要

SWIFTNet 公開鍵基盤(PKI)は必須機能であり、SWIFTNet Link (SNL)および全ての SWIFTNet サービスに安全性と信頼性を提供します。

SWIFTNet PKI は、以下の用途で使用されます:

- 認証
- 受領事実の事後否認防止
- 整合性

PKI キー

ビジネスアプリケーションは、これらの機能を SWIFTNet PKI の暗号機能を提供する SNL アプリケーションプログラミングインターフェース(API)を通じて使用することが可能です。暗号機

能は、各エンティティ（個人またはアプリケーション）が固有の PKI キーを持つ**秘密/公開 PKI キー**が使用されています。

各エンティティは、エンティティの公開鍵および秘密鍵が組み込まれている固有の PKI セキュリティプロフィールを保持しています。各 PKI セキュリティプロフィールの公開鍵は、SWIFT が保証します。

PKI 証明書とプロフィールの保存

SWIFT は、SWIFT で生成した証明書を、ユーザーが登録したエンティティの識別名(DN)と共に SWIFTNet ディレクトリに保存します。ユーザーは、PKI セキュリティプロフィールをハードウェアセキュリティモジュール(HSM)もしくはハードディスクなどのローカル環境に保存します。ユーザーが選択したパスワードが PKI セキュリティプロフィールを保護します。

SWIFTNet PKI に関するより詳細な情報は、“SWIFTNet 公開鍵基盤(PKI)” ページの 88 および *SWIFTNet Certificate Administration Guide* を参照してください。

1.4 SWIFTNet メッセージングサービスへの登録

概要

これらのサービスを使うにあたり、ユーザーは SWIFTNet メッセージングサービスに登録する必要があります。

パイロット（テストアンドトレーニング）もしくは実稼働の本番環境において SWIFTNet メッセージングサービスを使用することができるのは、SWIFT ユーザーのみです。本番環境に関するより詳細な情報は“SWIFTNet 本番環境の役割” ページの 72 を参照してください。

2 SWIFTNet メッセージングソリューション

概要

ユーザーは、SWIFTNet メッセージングソリューションとの関連において SWIFTNet サービスを使用します。SWIFTNet メッセージングサービスは、SWIFTNet InterAct、SWIFTNet FileAct、SWIFTNet Browse、SWIFTNet FIN です。

SWIFTNet メッセージングソリューションごとに、サービスアドミニストレーターが一人必要となります。

SWIFTNet ユーザーは、市場インフラソリューションおよびメンバー管理ソリューションのサービスアドミニストレーターになることが可能です。

SWIFT は、汎用およびビジネス固有の SWIFTNet メッセージングソリューションの両方において、サービスアドミニストレーターの役割を務めます。

2.1 主要コンセプトおよび用語集

定義

このセクションは、SWIFTNet メッセージングソリューションの主要コンセプトおよび用語を定義しています。

SWIFTNet メッセージングソリューション (SWIFTNet messaging solution)

SWIFTNet メッセージングソリューションは、ソリューションに固有のルールやポリシーを補完する一連の SWIFTNet サービスです。特定の業務目的のために、単一のサービスアドミニストレーターもしくは SWIFT がルールおよびポリシーを管理します。

SWIFTNet サービス (SWIFTNet service)

SWIFTNet サービスは、特定の方法で構成された一つもしくは複数の SWIFTNet メッセージングサービスを組み合わせたものです。SWIFTNet サービスは、SWIFTNet メッセージングソリューションとの関連で使用されます。SWIFTNet メッセージングサービスは、SWIFTNet InterAct、SWIFTNet FileAct、SWIFTNet Browse、SWIFTNet FIN です。

SWIFTNet メッセージングソリューションは、オペレーション構成のキータイプごとに分離させることが可能なよう、異なる SWIFTNet サービスを使用します。例えば、パイロット稼働（テストアンドトレーニング）とライブ稼働を分離させたい場合や、ストアアンドフォワード稼働とリアルタイム稼働を分離させたい場合などです。各メッセージングサービスにはサービスプロフィールとサービス名があり、クローズドユーザーグループ(CUG)が伴われています。

サービスプロフィール (Service profile)

サービスプロフィール (*service profile*)は、特定の SWIFTNet サービス向けの SWIFTNet メッセージングサービスの構成を説明します。

サービス名

サービス名は SWIFTNet サービスを識別します。ユーザーがサービスとの関連で使用する SWIFTNet InterAct メッセージと SWIFTNet FileAct トランザクションのヘッダーに記載されません。

2.2 メンバーもしくは市場インフラにより管理されるソリューション

2.2.1 主な役割および責任

概要

メンバーもしくは市場インフラにより管理されている各ソリューションは、サービスアドミニストレーター、サービス登録者、そして SWIFT に対して特定の役割および責任を負っています。また MA-CUG（メンバー管理が行われている CUG）の場合には、スポンサーメンバーに対しても同様の役割と責任を負います。

スポンサーメンバー

スポンサーメンバーは、MA-CUG サービスのサービスアドミニストレーターが SWIFT メンバーではない場合に、MA-CUG を保証するメンバーです。

SWIFT メンバーは、SWIFT の出資者として正式に登録されている SWIFT ユーザーです。

サービスアドミニストレーター

サービスアドミニストレーターは、1 つもしくは複数の SWIFTNet サービスを管理する責任がある SWIFT ユーザーです。

サービスアドミニストレーターは、管理している各 SWIFTNet サービスに対して以下を実行しなくてはなりません:

- **SWIFTNet サービスの構成の定義（サービスプロフィールを使用）。** サービスアドミニストレーターは、サービスの構成定義（後に修正された場合はその修正事項も）が SWIFT に遅滞なく適切に連絡されていることを確実にします。
- **サービス固有のオペレーションルールおよびサービス登録機関に適用されるポリシーの定義。** またサービスアドミニストレーターは、全てのサービス登録機関がそれらのオペレーションルールとポリシーにアクセスすることができ、また順守することを確実にしなければなりません。
- **SWIFTNet サービスへの登録を管理。** サービスアドミニストレーターは、該当サービスの適格条件を満たしていると SWIFT に連絡されている SWIFT ユーザーのみ、SWIFTNet サービスに登録することを認めます。またサービスアドミニストレーターは、SWIFTNet サービスのクローズドユーザーグループ(CUG)に登録を許可されるべき、もしくは除名されるべきサービス登録機関を SWIFT に連絡します。これらは入会/除名手続きに従って行われます。

サービスアドミニストレーターの特殊責任に関するより詳細な情報については、“ロールと責任” ページの 123 の *MA-CUG Service Description* および *Service Administration Agreement* を参照してください。

サービスアドミニストレーター関連の登録機関

サービスアドミニストレーター関連の登録機関は、MA-CUG サービスの中のロールです。他の全ての MA-CUG サービス登録機関とメッセージの送受信を行うことができます。

SWIFT ユーザーのうち、サービスアドミニストレーターと同じ金融機関に所属しているユーザーのみがサービスアドミニストレーター関連登録ユーザーとなることができます。同じ金融機関に所属していると見なされるには、通信を集約する目的で SWIFT ユーザーと同じグループに所属していると SWIFT に登録する必要があります。通信の集約と関連する一般条件に関するより詳細な情報は *SWIFT 価格表 (Price List)* を参照してください。

MA-CUG に登録されると、サービスアドミニストレーター関連登録ユーザーは、サービス登録機関の承認/取り消しを実行することができるようになります。サービスアドミニストレーターは、登録機関に承認されたとして登録ユーザーの指定および承認をする必要があります。

サービス登録機関

各 SWIFTNet サービスには、一もしくは複数のユーザー（機関）が登録しています。登録機関は、サービスアドミニストレーター（もしくはサービスアドミニストレーター関連登録機関）が該当する SWIFTNet サービスへの登録を承認した SWIFT ユーザーおよび SWIFT パートナーです。サービス登録機関の特殊責任に関するより詳細な情報に関しては、“ロールと責任” ページの 123 および *MA-CUG Service Description* を参照してください。

システムオペレーター

システムオペレーターは、SWIFTNet Copy サービスでコピー先の操作を行うユーザーのことで、サービスアドミニストレーターは、自身がシステムオペレーターの役割を果たすか、その役割を果たすサービス登録機関を指定します。

SWIFT

SWIFT は、サービスアドミニストレーターが要求した SWIFTNet メッセージングサービスをサービスプロフィールフォーム (*Service Profile Form*) と *Service Administration Agreement* に基づいて構成およびオペレーションを実行します。

2.2.2 登録と適格条件

概要

メンバー管理もしくは市場インフラ管理されているソリューションのサービスアドミニストレーターは、サービス登録機関の SWIFTNet サービスへの登録を定義します。またサービスアドミニストレーターは、サービスプロフィールを通じて、ユーザーが SWIFTNet サービス内で送受信することができるメッセージタイプを指定するクローズドユーザーグループ(CUG)を定義します。CUG ルールに関するより詳細な情報は、*SWIFTNet Messaging Operations Guide* を参照してください。

メンバー管理もしくは市場インフラ管理されたソリューションに登録するにあたり、登録機関は加盟登録されている SWIFT ユーザーである必要があります。SWIFT とサービスアドミニストレーターは、市場インフラ管理もしくはメンバー管理されたソリューションに登録するための特定条件に合意しなくてはなりません。メンバー管理されたクローズドユーザーグループ内のサービス登録機関 (*Service Participants within Member Administered Closed User Groups*) カテゴリに SWIFT ユーザーとして登録されている場合、最低限の入会条件で入会することができます。

SWIFT ユーザーとして登録する場合およびその入会条件に関するより詳細な情報については、*Corporate Rules* を参照してください。

登録を希望する候補は以下の条件を満たしている必要があります：

- サービスアドミニストレーターもしくはサービスアドミニストレーター関連登録機関の顧客である
- サービスアドミニストレーターもしくはサービスアドミニストレーター関連登録機関の顧客であることを証明できる
- 現在 SWIFT ユーザーである、もしくは登録にあたりユーザーとなる予定である 既に SWIFT ユーザーである場合は、サービスアドミニストレーターの承認により、メンバー管理されたクローズドユーザーグループ(MA-CUG)の登録機関となることが可能です。

まだ SWIFT ユーザーではない場合、適切なカテゴリの MA-CUG 内のサービス登録機関 (Service Participant within MA-CUG) に SWIFT 加盟機関として登録することができます。

2.3 SWIFT 管理ソリューション

概要

SWIFT 管理ソリューションには 2 種類あります:

- ・ 汎用メッセージソリューション。登録しているユーザーが、SWIFTNet メッセージングサービスを使用してデータを相互 (バイラテラル) に送受信することを可能にします。
- ・ ビジネス固有の SWIFT ソリューション。SWIFTNet の機能、メッセージ標準のルールブック、そして標準メッセージの送受信に関するビジネスルールを一体化させたものです。SWIFT は、これらのソリューションをユーザーのクローズドコミュニティに提供します。ビジネス固有のソリューションは、限られたクローズドユーザーグループ(CUG)の登録機関が特定の業務目的で SWIFTNet メッセージングサービスを使うことを可能にします。

これらのソリューションには、主要な付加価値アプリケーション (SWIFTNet Accord など) が含まれている場合もあります。

2.3.1 主な役割および責任

概要

SWIFT 管理されているサービスのうち、登録しているユーザーおよび SWIFT が特定の役割 (ロール) および責任を負うものがあります。

ユーザーの登録

SWIFT が管理している各 SWIFTNet サービスには、一人もしくは複数のユーザーが登録しています。サービスに登録している SWIFT ユーザーのことです。登録者が負う特定の責任に関するより詳細な情報は、“ロールと責任” ページの 123 を参照してください。

SWIFT

サービスアドミニストレーターとして、SWIFT は以下に関する責任があります:

- ・ **サービスプロフィールの定義**: SWIFT は、SWIFT 管理サービスのサービスプロフィールを定義します。
- ・ **サービス固有のオペレーションルールの定義**: サービスに登録しているユーザーに適用される、サービス固有のルールやポリシーを定義します。

サービス登録管理

サービスの適格条件を満たしていると SWIFT に証明した SWIFT ユーザーに対してのみ、SWIFT は SWIFT 管理サービスへの登録を承認します。

2.3.2 汎用メッセージングソリューション

2.3.2.1 概要

概要

汎用メッセージングソリューションはデベロッパーテスト、パイロット（テストアンドトレーニング）、ライブ稼働に使用することができます。

汎用 SWIFTNet FileAct

汎用 SWIFTNet FileAct は、登録しているユーザー間でのファイル送信を可能にします。以下のテーブルにある 6 つのサービスを組み合わせます。

汎用 SWIFTNet FileAct サービス

目的	モード	サービス名
ライブ稼働	ストアアンドフォワード	swift.generic.fast
	リアルタイム	swift.generic.fa
パイロット（テストアンドトレーニング）オペレーション	ストアアンドフォワード	swift.generic.fastlp
	リアルタイム	swift.generic.falp
デベロッパーテスト	ストアアンドフォワード	swift.generic.fastlx
	リアルタイム	swift.generic.falx

SWIFTNet FileAct に関するより詳細な情報は“SWIFTNet FileAct” ページの 33 を参照してください。オペレーションに関する情報は、*SWIFTNet Messaging Operations Guide* を参照してください。

SWIFTNet FIN

SWIFTNet FIN は、登録しているユーザー間での SWIFTNet FIN メッセージの送受信を可能にします。SWIFTNet FIN サービスに関するより詳細な情報は、*SWIFTNet FIN Service Description* を参照してください。

2.3.2.2 登録と適格条件

概要

ユーザーは、登録を希望する汎用メッセージングソリューションに関連する SWIFTNet サービスに登録することで、そのソリューションに登録することができます。

適格条件

汎用ソリューションの適格条件は以下のとおりです：

- ・ **パイロット（テストアンドトレーニング）オペレーションおよびライブ稼働**

以下のテーブルに表示されている全ての SWIFT メンバー、SWIFT サブメンバー、そして SWIFT 加盟者のカテゴリは、汎用 SWIFTNet FileAct のライブおよびパイロット（テストアンドトレーニング）に登録する適格条件を満たしています。

登録機関のカテゴリ

汎用 SWIFTNet FileAct を使用する適格条件を満たしている SWIFT 加盟者カテゴリ
1. 非出資メンバー (MEWS)
2. 非出資金融機関 (NSFI)
3. 証券会社 (BROK)
4. 証券保管振替機関と清算会社 (CSDS)
5. ファンド管理会社 (FUAD)
6. 投資顧問 (IMIS)
7. マネーブローカー (MONE)
8. 取引所 (EXCH)
9. 代理店 (REPO)
10. カストディーおよびノミニー業務を行う会社 (Subsidiary Providers of Custody and Nominee Services、CUST)
11. 貿易会社 (TRAD)
12. 信託会社 (TRUS)
13. 旅行小切手発行体 (TRAV)

• デベロッパーテスト

SWIFTNet ユーザーおよび SWIFT 加盟パートナーは、テスト環境にある汎用サービスを使用することができます。SWIFTNet FIN と汎用 SWIFTNet FileAct とは別に、テスト環境は汎用 SWIFTNet InterAct と汎用 SWIFTNet Browse (デベロッパーテストのみ) もサポートしています。詳細については、「ITB での SWIFTNet サービス」ページの 70 を参照してください。

SWIFTNet FIN の適格条件および利用制限に関するより詳細な情報は、*SWIFT Corporate Rules* および *SWIFTNet FIN Service Description* を参照してください。

2.3.3 ビジネス固有の SWIFT ソリューション

概要

SWIFT は、各業務分野（バルクペイメントなど）に固有のビジネスソリューションを提供します。

これらのソリューションは、以下のいずれに基づいても問題ありません:

- 汎用 SWIFTNet ソリューション。例えば、バルクペイメントでのファイル相互交換が可能な汎用 SWIFTNet FileAct など。
- ビジネス固有のソリューション
- 複数の SWIFT 管理ソリューションを組み合わせたもの

SWIFT は、複数のビジネス固有ソリューションのサービスアドミニストレーターの役割を担います。これらのソリューションに関するより詳細な情報は、それぞれ該当するサービスディスクリプションを参照してください。

3 SWIFTNet コアメッセージングサービス

概要

SWIFTNet コアメッセージングサービスは以下のとおりです:

- SWIFTNet InterAct
- SWIFTNet FileAct
- SWIFTNet Browse
- SWIFTNet FIN

これらの SWIFTNet メッセージングサービスは、SWIFTNet 公開鍵基盤 (PKI) と SWIFTNet ネーミングポリシーの機能を使用します。SWIFTNet PKI に関するより詳細な情報は、“SWIFTNet 公開鍵基盤(PKI)” ページの 88 を参照してください。SWIFTNet ネーミングおよびアドレッシングポリシーに関するより詳細な情報は、*SWIFTNet Naming and Addressing Guide* を参照してください。

本書は SWIFTNet InterAct、SWIFTNet FileAct、SWIFTNet Browse の機能について説明していません。SWIFTNet FIN に関するより詳細な情報は、*SWIFTNet FIN Service Description* を参照してください。

3.1 SWIFTNet InterAct

概要

ユーザーは、多様なソリューションの一環として以下を含む SWIFTNet InterAct を使用することができます:

- 市場インフラ管理ソリューション
- メンバー管理ソリューション
- SWIFT 管理ソリューション

ノート 本セクションに記載されている SWIFTNet InterAct の説明は、ユーザーがこのサービスをメッセージングサービスとして使用する場合に適用されます。SWIFT が、SWIFTNet InterAct をその他のメッセージングサービス用 (SWIFTNet FIN など) の送信メカニズムとして、もしくは SWIFTNet 管理メッセージ用として使用する場合は、必ずしも同じように適用されません。

3.1.1 SWIFTNet InterAct の作業モード

概要

ユーザーは、SWIFTNet InterAct を 3 つの異なる作業モードで使用することができます: リアルタイムメッセージング、リアルタイムでの照会回答、ストアアンドフォワードメッセージングです。

サービスアドミニストレーターが、SWIFTNet InterAct のストアアンドフォワードとリアルタイム作業モードの両方をメッセージングソリューションで組み合わせたい場合、異なるサービス名を使用する必要があります。

本セクションでは、SWIFTNet InterAct の 3 つの作業モードについてより詳細に説明していません。

3.1.1.1 リアルタイムメッセージングモード

概要

このモードは、メッセージをリアルタイムで送信することができます。送信者は、受信者がメッセージを受信したことを示す配信確認(ACK)、もしくはエラーメッセージを直ちに受信します。受信者が送信者に後ほど返信したい場合、別のリアルタイムメッセージで返信することができます。リアルタイムモードは、送信者/受信者が同時に SWIFTNet に接続している必要があります。また、両者とも SWIFTNet InterAct を使用する準備が整っていなければなりません。手順に関するより詳細な情報は、*SWIFTNet Messaging Operations Guide* を参照してください。

説明

メッセージはリクエストと呼ばれています。送信者はリクエスター、受信者はリスポンダーと呼ばれています。

リクエスターの SWIFTNet Link (SNL) が、リクエストの管理フィールドにある指示に従ってリクエストデータ本体（ペイロード）に署名したものを SWIFTNet のセントラルシステムに送信すると、そこから受信者であるリスポンダーに送信されます。

受信者（リスポンダー）は、リクエストの送信者（リクエスター）にメッセージの配信確認(ACK)を返信します。つまり、リスポンダー（受信者）の SNL は、返信の管理フィールドにある指示に基づいてデータ本体に署名するということです。その後、リスポンダーから SWIFTNet システムを経てリクエスターに返信されます。

3.1.1.2 リアルタイム照会回答モード

概要

このモードは、照会回答をリアルタイムでやりとりすることができ、受信者からの返信もしくはエラーメッセージもリアルタイムで届きます。リアルタイム照会回答モードは、送信者/受信者が同時に SWIFTNet に接続している必要があります。また、両者とも SWIFTNet InterAct を使用する準備が整っていなければなりません。手順に関するより詳細な情報は、*SWIFTNet Messaging Operations Guide* を参照してください。

説明

送信者が受信者に照会を送信します。このメッセージはリクエストと呼ばれています。送信者はリクエスター、受信者はリスポンダーと呼ばれています。

リクエスターの SWIFTNet Link (SNL) が、リクエストの管理フィールドにある指示に従ってリクエストデータ本体（ペイロード）に署名したものを SWIFTNet のセントラルシステムに送信すると、そこから受信者であるリスポンダーに送信されます。

受信者（リスポンダー）は、リクエストの送信者（リクエスター）に回答を返信します。つまり、リスポンダー（受信者）の SNL は、返信の管理フィールドにある指示に基づいてデータ本体に署名するということです。その後、リスポンダーから SWIFTNet システムを経てリクエスターに返信されます。

3.1.1.3 ストアアンドフォワードメッセージングモード

概要

このモードでは、メッセージを送信するとまず SWIFTNet セントラルシステムのキューに保存されます。メッセージは、受信者が SWIFTNet に接続し、受信できる状態になるまで（またはメッセージが期限切れとなるまで）キューに保存されます。つまり、送信者/受信者が同時に SWIFTNet に接続している必要はないということです。送信者が送信完了通知を要求した場合、メッセージが受信者のもとに配信された時点で SWIFT が発行します。

説明

送信者が受信者にメッセージを送信します。送信者はリクエスター、受信者はレスポンドーと呼ばれています。

リクエスターは、メッセージをレスポンドーに送信するよう SWIFTNet Link (SNL) に指示します。

リクエスターの SWIFTNet Link (SNL) が、メッセージの管理フィールドにある指示に従ってリクエストデータ本体（ペイロード）に署名したものを SWIFTNet のセントラルシステムに送信すると、そこから受信者であるレスポンドーに送信されます。

レスポンドーがメッセージを受信すると、配信確認(ACK)を SWIFT に送信します。

手順に関するより詳細な情報は、*SWIFTNet Messaging Operations Guide* を参照してください。

3.1.2 メッセージ構成とキーヘッダーフィールド

概要

SWIFTNet InterAct 交換は、SWIFTNet InterAct リクエストと、それに対する SWIFTNet InterAct レスポンスから構成されています。リクエストとレスポンスフローは、同様のメッセージ構成とキーヘッダーフィールドを使用します。

メッセージ構成に関するより詳細な情報は、*SWIFTNet Messaging Operations Guide* を参照してください。デベロッパー情報に関しては *SWIFTNet Service Design Guide*、*SWIFTNet Link Interface Specification*、*Interface Vendor Specifications for SWIFTNet InterAct and FileAct* を参照してください。

SWIFTNet InterAct リクエスト

通常、SWIFTNet InterAct リクエストには以下の要素が含まれています:

リクエスト要素	説明	
ヘッダー	ヘッダーに含まれるフィールド	
	リクエスター	メッセージ送信者のアドレスです。
	レスポンドー	メッセージ受信者のアドレスです。
	サービス名	送信されたメッセージのサービス名です。
	リクエストタイプ	サービスに関連して使用可能なリクエストタイプが含まれています。リクエストタイプに関するより詳細な情報は、 <i>SWIFTNet Messaging Operations Guide</i> を参照してください。
	リクエスト参照	オプションの文字列です。リクエスト参照は、1000 文字まで使用できる swift.fin を除き、他のいかなるサービスの場合も 30 文字を超えることはできません。SWIFT は、このフィールドに固有のクライアントアプリケーション参照を含めることを推奨します。
	プライオリティ	メッセージの優先度（普通もしくは至急）です。
ペイロード	ペイロード（データ本体）にはビジネスデータが含まれています。リアルタイムモードではメッセージ 1 件あたり最大 100,000 バイト、ストアアンドフォワードモードでは最大 80,000 バイトです。メッセージサイズが大きくなると共に、送信にかかる時間も長くなります。送信時間は、リクエスターおよびレスポンドーの双方がセキュア IP ネットワーク(SIPN)に接続している回線の容量に依存します。細い回線での接続をサポートするため、ペイロードサイズを約 30,000 バイトまでに抑えることを強く推奨します。	
管理ブロック	SWIFTNet がオプションとして適用しなければならないメッセージング機能（否認防止など）を示します。	

リクエスト要素	説明
セキュリティブロック	エンドユーザーが使用できる、アプリケーション間セキュリティ機能（デジタル署名など）オプションを示します。
エンドツーエンド配信管理ブロック	オプションである、エンドツーエンド配信管理プロトコルの XML 構成が含まれています。

SWIFTNet InterAct レスポンス

通常、SWIFTNet InterAct レスポンスには以下の要素が含まれています：

レスポンス要素	説明	
ヘッダー	ヘッダーに含まれるフィールド	
	レスポnder	メッセージ受信者のアドレスです。
	レスポンス参照	オプションの文字列です (30 文字以下)。SWIFT は、このフィールドに固有のクライアントアプリケーション参照を含めることを推奨します。
ペイロード	ペイロードにはビジネスデータが含まれており、メッセージ 1 件あたり最大 100,000 バイトまでとなっています。メッセージサイズが大きくなると共に、送信にかかる時間も長くなります。送信時間は、リクエスターおよびレスポnderの双方がセキュア IP ネットワーク(SIPN)に接続している回線の容量に依存します。細い回線での接続をサポートするため、ペイロードサイズを約 30,000 バイトまでに抑えることを強く推奨します。	
管理ブロック	SWIFTNet がオプションとして適用しなければならないメッセージング機能（否認防止など）を示します。	
セキュリティブロック	エンドユーザーが使用できる、アプリケーション間セキュリティ機能（デジタル署名など）オプションを示します。	
エンドツーエンド配信管理ブロック	オプションである、エンドツーエンド配信管理プロトコルの XML 構成が含まれています。	

3.1.3 SWIFTNet InterAct の標準機能

概要

標準機能とは、SWIFTNet InterAct 利用料により適用可能な SWIFTNet InterAct の機能ことです。SWIFTNet InterAct 利用料により適用される標準機能の詳細については、*SWIFT Price List* を参照してください。

SWIFTNet InterAct 標準機能

SWIFTNet InterAct には、以下の標準機能が搭載されています：

- 認証管理：
 - 送信者認証 (SWIFT が管理)
 - 送信者認証 (受信者が管理)
 - SWIFTNet Link 認証管理
- クローズドユーザーグループ(CUG)管理
- ロールベースアクセス管理 (RBAC)
- 機密性の管理：

- SWIFTNet Link(SNL) 暗号化
- 仮想プライベートネットワーク (VPN) ボックス暗号化
- 整合性管理
 - SWIFT による整合性管理
 - 受信者による整合性管理
- メッセージバリデーション
- セントラルメッセージルーティング
- 独自参照とタイムスタンプ

3.1.3.1 認証管理

概要

SWIFTNet InterAct は、以下の 3 種類の標準認証管理およびその補完機能を提供しています：
SWIFT による送信者認証管理、受信者による送信者認証管理、SWIFTNet Link(SNL)認証管理。

ノート SWIFT は、SWIFTNet InterAct を使用して機密性の高いメッセージを送信する場合は、エンドツーエンド署名を使用することを強く推奨します。

SWIFT による送信者認証管理

SWIFT は、SWIFT がメッセージを受信した時点で有効な SWIFTNet PKI 証明書を持っているユーザーから送信された SWIFTNet InterAct メッセージのみを送信します。

SWIFT は、InterAct メッセージのヘッダーに送信者の BIC8 が記載され、秘密鍵で署名された SWIFTNet InterAct のみを送信します。つまり、SWIFT は全ての SWIFTNet InterAct リクエストおよび SWIFTNet InterAct レスポンスをこのように管理しています。

上記の条件を満たさないリクエストは、受信者（レスポnder）に送信されません。その場合、SWIFT は送信者（リクエスター）にエラーメッセージを送信します。

認証に関するより詳細な情報は、“SWIFTNet 公開鍵基盤(PKI)” ページの 88 を参照してください。

送受信される各メッセージについて、SWIFTNet システムはメッセージを署名するために使用されている PKI 証明書が破棄されていないかどうかをチェックします。

受信者による送信者認証

送信されてくるメッセージに対し、受信者側で送信者認証を適用させることができます。そのために、送信者がリクエスト（もしくはレスポンス）を送信する際にエンドツーエンド署名を選択し、受信者は送信されてきたリクエスト（もしくはレスポンス）を受信する際にそのエンドツーエンド署名を検証します。

否認防止オプションが使用されている場合、ユーザーはエンドツーエンド署名を使用しなければなりません。受信者による送信者認証は、SWIFTNet InterAct リクエストおよび SWIFTNet InterAct レスポンスの両方に適用することができます。

認証における PKI に関するより詳細な情報は、“SWIFTNet 公開鍵基盤(PKI)” ページの 88 を参照してください。エンドツーエンド署名の使用に関するより詳細な情報は、*SWIFTNet Link Service Description* を参照してください。

SWIFTNet Link 認証管理

SWIFT は、SWIFT が付与した有効な鍵を持つ SWIFTNet から送信された SWIFTNet InterAct メッセージのみを送信します。

つまり、SWIFT は全ての SWIFTNet InterAct リクエストおよび SWIFTNet InterAct レスポンスをこのように管理しています。上記の条件を満たさないリクエストは、受信者（レスポンドー）に送信されません。上記の条件を満たさないレスポンスは、受信者（元のリクエスター）に送信されません。

3.1.3.2 クローズドユーザーグループ管理

送信されるメッセージ

SWIFT は、ファイルの送受信をするユーザーが当該サービスのクローズドユーザーグループ (CUG) で構成されている場合に限り、SWIFTNet InterAct メッセージを送信します。

SWIFT は、サービスアドミニストレーターが提供する指示に従って CUG を構成します。

SWIFT は、SWIFTNet InterAct メッセージのうち、送信者、受信者、そしてサービスアドミニストレーターが該当サービス向けに定義したメッセージタイプの組み合わせが有効なものが含まれているもののみを送信します。

CUG 管理は、全ての SWIFTNet InterAct リクエストに適用されます。CUG 管理条件を満たしていないリクエストがレスポンドーに送信されることはありません。

3.1.3.3 Role-Based Access Control (ロールベースアクセス管理)

説明

サービスアドミニストレーターがロールベースアクセス管理(RBAC)を選択した場合、SWIFT は適切な RBAC プロフィールを持つ機関内のエンティティ（個人またはアプリケーション）により送信された SWIFTNet InterAct メッセージのみを送信します。

適切な RBAC プロフィールは、交換されるメッセージとの関連で、サービスに対して少なくとも 1 つのロールを持っているものとしてエンティティに割り当てられています。

SWIFT は、サービスアドミニストレーターが RBAC を使用すると選択したサービスに関連して送受信される全ての SWIFTNet InterAct リクエストに、RBAC 管理を適用します。RBAC 管理が適用されている場合、その管理条件を満たさないリクエストはレスポンドーに送信されません。

それに加え、サービスアドミニストレーターはサービスアドミニストレーターがこの管理機能を選択した場合、SWIFT が SWIFTNet InterAct メッセージと共に送信者のサービス関連 RBAC プロフィール情報を送信するかどうかを決定することができます。

SWIFT は、メッセージと共に送信者のサービス関連 RBAC プロフィール情報を送信することにより、送信者がメッセージに必要なアクセス管理プロフィールを持っているかどうかを受信者が検証できるようにします。

SWIFT は、各ユーザーの RBAC プロフィールを以下のように定義します:

- RBAC を使用する全てのサービス向けに、サービスアドミニストレーターはサービスで許可されているロールおよび全ての関連するクオリファイヤーもしくはバリューペアについて定義します。
- SWIFT は、サービスを使用する各機関に適用されるロール、クオリファイヤー、バリューペアを構成します。

- その後、特定の機関の RBAC 代表者 (Delegator。通常はセキュリティオフィサー) が全てもしくは一部のロール、クオリアファイヤー、バリュースペアをエンドユーザーに割り当てます。エンドユーザーは個人もしくはアプリケーションです。

RBAC に関するより詳細な情報は、*SWIFTNet Certificate Administration Guide* を参照してください。

3.1.3.4 機密性の管理

説明

SWIFTNet InterAct は、以下の 3 種類の標準機密性管理およびその補完機能を提供しています:

- SWIFTNet Link(SNL) 暗号化
- 仮想プライベートネットワーク (VPN) ボックス暗号化
- SWIFTNet セントラルシステムによる機密性保護

SWIFTNet リンク暗号化

SWIFT は、ユーザーの SWIFTNet Link と SWIFTNet セントラルシステムのフロントエンドプロセッサ間で送受信される、全ての SWIFTNet メッセージを暗号化します。

SWIFT は、全ての SWIFTNet InterAct リクエストおよび SWIFTNet InterAct レスポンスをこのように処理します。

VPN ボックス暗号化

SWIFT は、ユーザーの VPN ボックスと SWIFT が管理しているセキュア IP ネットワーク(SIPN) バックボーンアクセスポイント間の送受信において、SWIFTNet InterAct メッセージを含む全ての SIPN 通信を暗号化しています。

SWIFT は、全ての SWIFTNet InterAct リクエストおよび SWIFTNet InterAct レスポンスをこのように処理します。

SWIFTNet セントラルシステムによる機密性保護

SWIFT は、SWIFTNet セントラルシステムに保存されている SWIFTNet InterAct メッセージを、認証されていないアクセスおよびディスクロージャーから保護します。

3.1.3.5 整合性管理

概要

SWIFTNet InterAct は、以下の 3 種類の標準整合性管理およびその補完機能を提供しています:

- SWIFT による整合性管理
- 受信者による整合性管理

SWIFT による整合性管理

SWIFT は、メッセージがユーザーの SWIFTNet Link (SNL)から SWIFTNet セントラルシステムに送信される間に、その署名されたコンテンツに変更がなかったメッセージのみ送信します。

SWIFT による整合性管理は、送信者が作成した PKI 署名に基づいています。この検証方法はメッセージの署名された部分にのみ適用されます。整合性管理は、全ての SWIFTNet InterAct リクエスト/レスポンスに適用されます。

上記の条件を満たさないリクエストは、受信者（リスポンダー）に送信されません。条件を満たさないレスポンスの場合、元のリクエスターにエラー警告が送信されます。

受信者による整合性管理

送信者がエンドツーエンド署名を選択した場合、SWIFT は署名がつけられたメッセージの内容がユーザーにより使用されている SWIFTNet Link 間での送受信中に変更されていないことを、SWIFTNet InterAct メッセージの受信者が検証できるようにします。

整合性の検証という文脈において、エンドツーエンドとは取引先の SWIFTNet Link(SNL)間を意味します。受信者による整合性管理は、送信者が作成した PKI 署名に基づいています。受信者の SNL は署名を検証し、結果をアプリケーションに送信します。この方法は、送信者がエンドツーエンド署名を選択した場合にのみ適用されます。また、適用されるのはメッセージの署名された部分のみです。

否認防止オプションが選択されている場合、ユーザーは整合性管理を使用しなくてはなりません。

整合性管理は、SWIFTNet InterAct リクエストおよび SWIFTNet InterAct レスポンスの両方に適用することができます。

認証における PKI に関するより詳細な情報は、“SWIFTNet 公開鍵基盤(PKI)” ページの 88 を参照してください。エンドツーエンド署名に関するより詳細な情報は、*SWIFTNet Link Service Description* を参照してください。

3.1.3.6 メッセージの検証

概要

サービスアドミニストレーターがメッセージの検証を使用することを選択すると、ペイロードがメッセージのペイロードに関連する検証ルールに対してシンタックス的に（そして場合によっては意味的にも）従っている場合、SWIFT は SWIFTNet InterAct メッセージを警告メッセージなしで送信します。

つまり、SWIFT はサービスアドミニストレーターがメッセージの検証オプションを使用すると選択したサービスにおいて、ユーザーが送受信する全ての SWIFTNet InterAct リクエスト/レスポンスにメッセージの検証を適用させるということです。サービスアドミニストレーターがメッセージの検証を選択した場合、条件を満たさなかったリクエストはリスポンダーに送信されないか、警告通知を伴って送信されます。同様に、メッセージ検証の条件を満たさなかったレスポンスは元のリクエスターに送信されないか、警告通知を伴って送信されます。サービスアドミニストレーターがメッセージの検証を使用することを選択した場合、全てのメッセージペイロード（メッセージ本体）がいかなる意味でも変換されておらず、SWIFT が読むことができる形式であることを確かにしなければなりません。

SWIFT は、ビジネスコミュニティの関連するメンバーと連携して検証ルールの構築および保守を行います。

3.1.3.7 セントラルメッセージルーティング

概要

SWIFT は、事前に定義されている受信者のセントラルルーティングルールに従い、SWIFTNet InterAct メッセージ（リクエスト）をストアアンドフォワードキューもしくは SWIFTNet Link (SNL)に送信します。

ノート リアルタイム SWIFTNet InterAct リクエストに対するレスポンスは、リクエストが発信された SWIFTNet Link に送信されます。

受信者は、ルーティングルールを各自で管理します。SWIFT は、それらのルールを SWIFT Message Reception Registry (MRR) に保存します。セントラルルーティングルールの構成に関するより詳細な情報については、“セントラルルーティングルール” ページの 62 を参照してください。

柔軟なオペレーション

SWIFTNet のメッセージルーティング機能は、以下を提供することでオペレーションの柔軟性を高めます:

- メッセージの送受信をより円滑にするため、異なる SNL に受信メッセージを散在させる (例: アプリケーションごとなど)
- 受信側の同じ SNL 内にある、異なるアプリケーションへのメッセージルーティング
- ユーザーのアクティブサイトが災害や事故などで稼働不能となった場合、メッセージを緊急時対応サイトにルーティングする
- メッセージを異なるストアアンドフォワードキューにルーティング

3.1.3.8 独自参照とタイムスタンプ

概要

SWIFT は、メッセージを受信者に送信する前に、全ての SWIFTNet InterAct メッセージに独自参照と SWIFT タイムスタンプを付けます。これは全ての SWIFTNet InterAct リクエストに適用されます。

3.1.4 SWIFTNet InterAct の付加価値オプション機能

概要

付加価値オプション機能を使用するには、SWIFTNet InterAct メッセージ料金のほかに追加料金を支払う必要があります。付加価値オプション機能に関するより詳細な情報は、*SWIFT 価格表 (Price List)* を参照してください。

SWIFTNet InterAct オプション機能

SWIFTNet InterAct には、オプションで以下の付加価値機能があります。:

- メッセージプライオリティ
- 受領事実の事後否認防止
- 送信完了通知

3.1.4.1 メッセージプライオリティ

説明

SWIFTNet InterAct は、オプション機能としてメッセージプライオリティの使用をサポートしています。ユーザーは、プライオリティを通常 (Normal) もしくは至急 (Urgent) に設定することができます。

これにより、そのメッセージを取り扱うべき優先度を受信者に知らせることができます。また、この機能を使用してストアアンドフォワードキューからメッセージをプライオリティ順にソートして取得することもできます。

3.1.4.2 否認防止 (Non-repudiation)

概要

サービスアドミニストレーターもしくはメッセージの送信者（またはその両方）が否認防止を選択した場合、SWIFT は SWIFTNet InterAct メッセージの送受信をそれに先立つ 124 日間にわたって確認（また要求があった場合にはその証明を発行）することができます。発信の否認防止の場合、リクエストおよびレスポンス両方の送信に対して適用されます。受信の場合、受信者がリクエストの署名をレスポンスにコピーした上で否認防止を選択すると、リクエストの受信に対して適用されます。

否認防止オプションは、サービスごとに必須、オプション、利用不可にすることができます。各サービスのサービスアドミニストレーターがそのいずれにするかを決定します。必須となっているサービスの場合、そのサービス内で送受信される全てのメッセージ（リクエストとレスポンス）に否認防止オプションが自動的に適用されます。

3.1.4.2.1 発信元の否認防止

概要

発信元の否認防止は、有効な SWIFTNet PKI 証明書を持っている発信者が特定の SWIFTNet InterAct メッセージ（リクエストまたはレスポンス）に署名した、とユーザーが確認できるデータへのアクセスを可能にします。有効な SWIFTNet PKI 証明書とは、メッセージの署名者 DN フィールドに表示されている識別名(DN)に対して SWIFT が発行したものです。

SWIFT は、SWIFTNet InterAct のエンドツーエンドオプションを使用することで発信元の否認防止を提供します。エンドツーエンド署名オプションに関するより詳細な情報は、“SWIFTNet 公開鍵基盤(PKI)” ページの 88 を参照してください。

ノート ユーザーは、発信元の否認防止をエンティティレベルで設定することができます。例えば、特定のエンティティの識別名(DN)に添付する信用レベルについて、送信者/受信者ともに合意したものを設定することができます。

3.1.4.2.2 発信の否認防止

概要

発信の否認防止は、受信したメッセージ（リクエストまたはレスポンス）の発信元、発信時間、そして正しい受信者であることを確認できるデータへのアクセスを可能にします。

発信の否認防止を使用するには、ユーザーが SWIFTNet InterAct メッセージ（リクエストもしくはレスポンス）の否認防止オプションおよびエンドツーエンド署名オプションを使用する必要があります。

サービスの発信の否認防止がオプションとなっている場合、発信者はメッセージのうち否認防止オプションが必要なものを SWIFTNet Link(SNL)に指示します。

主な特長

SWIFTNet InterAct にある発信の否認防止オプションの主な特長は以下の通りです：

- **SWIFTNet Link(SNL)による否認防止プロセス**

否認防止オプションが選択されているメッセージを送信する場合、送信者はそのメッセージについてエンドツーエンド署名オプションを選択しなければなりません。

送信者の SWIFTNet Link (SNL)は、メッセージが発信された現地時間(UTC)を含む **SwiftRequestRef** もしくは **SwiftResponseRef** をメッセージに自動的に追加します。現地時

間は、自動的に UTC に変換されます。SNL は、署名されたメッセージにこれらの参照を挿入します。

• 時間の整合性チェック

SWIFTNet セントラルシステムは、*発信時間*と*セントラルシステムでの処理時間*を比較します。通常、これらは近い時間になっています。時間差が 5 分以上だった場合、SWIFTNet は警告を記録します。警告は SWIFTNet により受信者にも送信されるので、受信者側で適切な対応をとることができます。

• メッセージを安全に保存

ユーザーが SWIFTNet 本番環境（パイロット（テストアンドトレーニング）、サービスのライブモードを含む）で送受信するメッセージについて、SWIFT はそれらのメッセージ（リクエストまたはレスポンス）のヘッダーフィールド、データ本体（ペイロード）、そして署名を SWIFT オペレーティングセンター（OPC）に安全に保存します。

ノート しかしながら、通常では起こりえない災害や事故などによりサイトが完全に稼働不能となり、OPC にも影響が出たような場合、サイトが稼働不能となった時点から 90 分前までの間に記録された否認防止データの復元について SWIFT は保証するものではありません。

• 復元および再検証

否認防止を選択した送信者および受信者は、メッセージの発信から 124 日以内であれば、メッセージの復元を SWIFT に依頼することができます。

クリーンアッププロセスのタイミングなどにより、124 日間以上メッセージが保存されている場合もありますが、SWIFT では復元可能な期間を「メッセージ発信後 124 日以内」と定めています。

否認防止機能により、特定のデータを復元することができます。例えばユーザー間でなんらかの争議となった場合、以下の情報を復元することが可能です：

- エンドツーエンド署名および SWIFT が追加した全ての情報を伴ったメッセージ（スイッチングの時間など）
- ユーザーがメッセージ内で使用した証明書に関連する全てのデータ（証明書履歴、作成や破棄についてなど）

ノート 否認防止を使用したい場合、エンドツーエンド認証を使用する必要があります。またエンドツーエンド認証と同時に使用できないため、暗号化機能を選択してはいけません。

ユーザーの責任

否認防止機能を使用したいが、サービスアドミニストレーターが定義した否認防止を自動的に適用されたくない場合、ユーザーは SWIFTNet InterAct メッセージを送信する際に否認防止オプションを選択する必要があります。また、使用しているアプリケーションが *SWIFTNet Service Design Guide* に記載されている否認防止オプションのガイドラインを順守していることを保証する必要があります。

メッセージの再検証を要求する場合は、SWIFT が提供しているフォームを提出し、必要な手順に従って手続きします。メッセージの再検証を要求する手順については、*SWIFTNet Messaging Operations Guide* を参照してください。

SWIFT の責任

ユーザーが正式に再検証を要求し、その復元する情報が否認防止オプションがつけられている SWIFTNet メッセージもしくはファイルに関連している場合、SWIFT は通常 5 営業日以内にユーザーが指定した方法により再検証および復元を実行します。

3.1.4.2.3 受信の否認防止

主な特長

発信の否認防止と同様です（“主な特長” ページの 30 を参照してください）。

リアルタイムモードで受信の否認防止を実現するには、SWIFTNet InterAct リクエストの受信者がリクエストの署名をレスポンスのペイロードに挿入し、SWIFTNet InterAct レスポンスで否認防止オプションを選択して、送信者にレスポンスを返信する必要があります。

ストアアンドフォワードモードで受信の否認防止を実現するには、SWIFTNet InterAct リクエストの署名を、受信者が SWIFT に送信する配信確認(ACK)にコピーする必要があります。ユーザーは、署名を配信確認(ACK)にコピーするのがインターフェースなのかアプリケーションなのかをベンダーに確認することができます。

ユーザーの責任

受信の否認防止機能を使用したいが、サービスアドミニストレーターが定義した否認防止を自動的に適用されたくない場合、ユーザーは SWIFTNet InterAct リクエストもしくはレスポンスを送信する際に否認防止オプションを選択する必要があります。また、使用しているアプリケーションが *SWIFTNet Service Design Guide* に記載されている否認防止オプションのガイドラインを順守していることを保証する必要があります。

リアルタイムモードで否認防止オプションを使用するには、SWIFTNet InterAct リクエストの受信者がリクエストの署名をレスポンスのペイロードに挿入することに、SWIFTNet InterAct メッセージの送信者・受信者ともに同意する必要があります。送信者は、受信者がレスポンスのペイロードに署名を挿入していることを検証し、対応しているリクエストと確認しなくてはなりません。

メッセージの復元を要求する場合は、SWIFT が提供しているフォームを提出し、必要な手順に従って手続きします。メッセージの復元を要求する手順については、*SWIFTNet Messaging Operations Guide* を参照してください。

SWIFT の責任

ユーザーが正式に再検証を要求し、その復元する情報が否認防止オプションがつけられている SWIFTNet メッセージもしくはファイルに関連している場合、SWIFT は通常 5 営業日以内にユーザーが指定した方法により再検証および復元を実行します。

3.1.4.3 送信完了通知

概要

メッセージの送信者が、ストアアンドフォワードモードのサービスに対して SWIFTNet InterAct を使用する場合、オプションとして送信完了通知を要求することができます。その場合、SWIFT は SWIFTNet InterAct メッセージを受信者に送信した際に送信完了通知を作成します。送信完了通知は、送信者が指定した SWIFT のキューに保存されます。

3.1.5 サービスアドミニストレーターが定義できる機能

概要

各サービスアドミニストレーターは、サービスプロフィールの一環として特定の SWIFTNet InterAct 機能を定義することができます。

サービスアドミニストレーターが定義できるのは、以下のいずれかに該当する機能です：

- **使用不可**：当該サービスには使用できない機能です。
- **必須**：当該サービスに関連して送受信される全てのメッセージに使用される必要がある機能です。
- **ユーザー選択**：メッセージの送信者が、メッセージ送信の際に選択できる機能です。

これらの機能の定義に関するより詳細な情報は、*SWIFTNet Messaging Operations Guide* を参照してください。

3.2 SWIFTNet FileAct

概要

ユーザーは、多様なソリューションの一環として以下を含む SWIFTNet InterAct を使用することができます：

- 市場インフラ管理ソリューション
- メンバー管理ソリューション
- SWIFT 管理ソリューション
- 汎用 SWIFTNet FileAct

3.2.1 SWIFTNet InterAct の作業モード

概要

ユーザーは、SWIFTNet InterAct を 3 つの異なる作業モードで使用することができます：

- リアルタイムのファイル送信モード
- リアルタイムのファイルダウンロードモード
- ストアアンドフォワードのファイル送信モード

本セクションでは、これらのモードについて説明しています。SWIFTNet FileAct のオペレーションに関するより詳細な情報は、*SWIFTNet Messaging Operations Guide* を参照してください。

ノート SWIFTNet FileAct は、ファイル内容を検証するものではありません。

3.2.1.1 リアルタイムのファイル送信モード

概要

リアルタイムファイル送信モードでは、ファイルをリアルタイムで送信することができます。送信者は、受信者がメッセージを受信したことを示す配信確認(ACK)、もしくはエラーメッセー

ジを直ちに受信します。受信者が送信者に後ほど返信したい場合、別のリアルタイムメッセージで返信することができます。リアルタイムファイル送信モードは、送信者/受信者が同時に SWIFTNet に接続している必要があります。また、両者とも SWIFTNet FileAct を使用する準備が整っていなければなりません。

ノート SWIFT は、エコノミーモードでのダイヤルアップ回線および専用線を使用した、リアルタイム送信モードの SWIFTNet FileAct はサポートしていません。エコノミーモードに関するより詳細な情報は、“接続構成” ページの 79 を参照してください。

リアルタイム送信モードでのファイル送信に関するより詳細な情報は、*SWIFTNet Messaging Operations Guide* を参照してください。SWIFT が提供する付加価値機能のプロセスなどに関する全詳細については、“SWIFTNet FileAct の標準機能” ページの 37 を参照してください。

説明

ファイルの送信は、まず送信者と受信者の間で交渉メッセージ (negotiation message) がやりとりされます。受信者は、この要求を受理もしくは拒否することができます。受信者が拒否した場合、ファイル送信は実行されず、送信者には拒否されたことを示すエラーメッセージが返信されます。

ファイルの送信者は、ファイルが送信されたことを明確にする確認を要求することができます。この場合、受信者は送信完了通知を返信しなくてはなりません。通常、受信者はファイルが安全なストレージ環境に保存された後に送信完了通知を送信します。送信完了通知を送信することにより、受信者はそのファイルを所有していることを明確にします。送信者がこのような送信確認を要求していない場合、受信者が送信完了通知を送信することはできません。

ファイル送信に否認防止機能が選択されている場合、ユーザーは送信完了通知オプションを使用する必要があります。

3.2.1.2 リアルタイムのファイルダウンロードモード

概要

リアルタイムファイルダウンロードモードでは、リアルタイムでリクエストを送信し、受信者から特定のファイルを受け取ることができます。リアルタイムファイルダウンロードモードは、送信者/受信者が同時に SWIFTNet に接続している必要があります。また、両者とも SWIFTNet FileAct を使用する準備が整っていなければなりません。

リアルタイムファイルダウンロードモードでのファイル送信に関するより詳細な情報は、*SWIFTNet Messaging Operations Guide* を参照してください。SWIFT が提供する付加価値機能のプロセスなどに関する全詳細については、“SWIFTNet FileAct の標準機能” ページの 37 を参照してください。

説明

ファイルの送信は、まずファイルダウンロードのリクエスターとレスポンドーの間で交渉メッセージ (negotiation message) がやりとりされるところから始まります。レスポンドーは、この要求を受理もしくは拒否することができます。レスポンドーが拒否した場合、ファイル送信は実行されず、リクエスターには拒否されたことを示すエラーメッセージが返信されます。

ファイルダウンロードのレスポンドーは、ファイルが送信されたことを明確にする確認を要求することができます。この場合、ファイルダウンロードのリクエスター (ファイルの受信者) はレスポンドーに送信完了通知を返信します。リクエスターは、ファイルが安全なストレージ環境に保存された後に送信完了通知を送信します。送信完了通知を送信することにより、リクエスターはそのファイルを所有していることを明確にします。リクエスターがこのような送信確認を要求していない場合、レスポンドーが送信完了通知を送信することはできません。

ファイル送信に否認防止機能が選択されている場合、ユーザーは送信完了通知オプションを使用する必要があります。

3.2.1.3 ストアアンドフォワードのファイル送信モード

概要

ストアアンドフォワードファイル送信モードでは、メッセージを送信するとまず SWIFTNet セントラルシステムのキューに保存されます。ファイルは、受信者が SWIFTNet に接続し、受信できる状態になるまで（またはファイルが期限切れとなるまで）キューに保存されます。つまり、送信者/受信者が同時に SWIFTNet に接続している必要はないということです。送信者が送信完了通知を要求した場合、ファイルが受信者のもとに配信された時点で SWIFT が発行します。

ストアアンドフォワードのファイル送信モードでのファイル送信に関するより詳細な情報は、*SWIFTNet Messaging Operations Guide* を参照してください。

説明

ファイルの送信は、まず送信者と SWIFT の間で交渉メッセージ (negotiation message) がやりとりされるところから始まります。SWIFT が拒否した場合、ファイル送信は実行されず、送信者には拒否されたことを示すエラーメッセージが返信されます。

実際のファイル送信に先立ち、SWIFT と受信者の間で交渉メッセージがやりとりされます。受信者は、この要求を受理もしくは拒否することができます。拒否された場合、ファイル送信は実行されず、送信者のキューには拒否されたことを示すエラーメッセージが SWIFT から返信されます。

受信者が交渉メッセージを受理した場合、受信者は SWIFT のセントラルストレージシステムからファイルを取得しなければなりません。

受信者が SWIFT に配信確認を送信した時点で、ファイルは**送信完了**と見なされます。受信者は、ファイルが安全なストレージ環境に保存された後に配信確認を送信します。この配信確認を送信することにより、受信者はそのファイルを所有していることを明確にします。

ファイルの送信者は、オプションとしてファイルが送信されたことを明確にする確認を要求することができます。

ファイルの送信者がファイル送信の確認を要求した場合、SWIFT は受信者からの配信確認(ACK)を受信した後に、送信者の当該キューに送信完了通知を送信します。

SWIFT が提供する付加価値機能のプロセスなどに関する全詳細については、“SWIFTNet FileAct の標準機能” ページの 37 を参照してください。

3.2.2 ファイル送信構成とキーヘッダーフィールド

3.2.2.1 ファイル送信構成

概要

SWIFTNet FileAct 交換は、ファイル内容の送信後に自動的に行われる SWIFTNet FileAct による交渉リクエストと交渉レスポンスから構成されています。

ファイル送信構成に関するより詳細な情報は、*SWIFTNet Messaging Operations Guide* を参照してください。デベロッパー情報に関しては *SWIFTNet Service Design Guide*、*SWIFTNet Link Interface Specification*、*Interface Vendor Specifications for SWIFTNet InterAct and FileAct* を参照してください。

SWIFTNet FileAct 交渉リクエスト (negotiation request)

通常、SWIFTNet FileAct 交渉リクエストには以下の要素が含まれています:

リクエスト要素	説明	
ヘッダー	ヘッダーに含まれるフィールド	
	リクエスター	ファイル送信者のアドレスです。
	レスポンス	ファイル受信者のアドレスです。
	サービス名	送信されたファイル送信のサービス名です。
	リクエストタイプ	サービスに関連して使用可能なリクエストタイプが含まれています。リクエストタイプに関するより詳細な情報は、 <i>SWIFTNet Messaging Operations Guide</i> を参照してください。
	リクエスト参照	オプションの文字列です。リクエスト参照は 30 文字を超えることはできません。SWIFT は、このフィールドに固有のクライアントアプリケーション参照を含めることを推奨します。
	送信参照	ファイル送信の独自参照です。
	その他のフィールド	その他のフィールドに関する情報は、 <i>SWIFTNet Messaging Operations Guide</i> を参照してください。
管理ブロック	SWIFTNet がオプションとして適用しなければならないメッセージング機能（否認防止など）を示します。	
セキュリティブロック	エンドユーザーが使用できる、アプリケーション間セキュリティ機能（デジタル署名など）オプションを示します。	
エンドツーエンド配信管理ブロック	オプションである、エンドツーエンド配信管理プロトコルの XML 構成が含まれています。また、HeaderInfo 構成を含めることもできます（3.2.2.2, "HeaderInfo" ページの 37 を参照してください）。	

SWIFTNet FileAct 交渉レスポンス (negotiation response)

通常、SWIFTNet FileAct 交渉レスポンスには以下の要素が含まれています:

レスポンス要素	説明	
ヘッダー	ヘッダーに含まれるフィールド	
	レスポンス	ファイル受信者のアドレスです。
	レスポンス参照	オプションの文字列です（30 文字以下）。SWIFT は、このフィールドに固有のクライアントアプリケーション参照を含めることを推奨します。
管理ブロック	SWIFTNet がオプションとして適用しなければならないメッセージング機能（否認防止など）を示します。	

レスポンス要素	説明
セキュリティブロック	エンドユーザーが使用できる、アプリケーション間セキュリティ機能（デジタル署名など）オプションを示します。
エンドツーエンド配信管理ブロック	オプションである、エンドツーエンド配信管理プロトコルの XML 構成が含まれています。

ファイル内容

SWIFTNet FileAct はあらゆるファイル内容をサポートしています。ファイル内容に関する情報は、“あらゆるファイルコンテンツの送信” ページの 41 を参照してください。

3.2.2.2 HeaderInfo

説明

HeaderInfo は FileAct ヘッダーの一部で、XML 構造です。これにより、ファイル送信に関連するキーサマリー情報を特定することが可能になるほか、SWIFTNet セントラルシステムおよび受信者のアプリケーションをこれらのパラメータで実行することが可能になります。またオプションのコピー機能を使用することにより、HeaderInfo の内容が自動的にコピーされ、コピー先に送信することができます。

HeaderInfo の使用

このヘッダーに含まれている情報フィールド明確かつ構造化されて定義されています。例えば、大量小口決済（Bulk Payments）のヘッダーには「合計額」、「合計送金数」、「通貨」など一括送金に関連するサマリー情報を含めることができます。

受取人は、ファイルを開いたりその内容を処理することなくこの情報を使用することができます。例えば、ファイルのルーティングや、監査のためにデータを記録するために使用することができます。

一般的に、ヘッダーブロックの使用はオプションです。しかし、この情報ブロックの使用を決定するコミュニティもあると思います。その場合、SWIFT は各コミュニティと連携して必要なフィールドを定義し、関連ソリューションのドキュメント内でその使用が明記されていることを確実にします。

HeaderInfo フィールドに関するより詳細な情報は、*SWIFTNet Messaging Operations Guide* を参照してください。

3.2.3 SWIFTNet FileAct の標準機能

概要

標準機能とは、SWIFTNet FileAct 利用料を適用可能な SWIFTNet FileAct の機能のことです。SWIFTNetFileAct 利用料により適用される標準機能の詳細については、*SWIFT Price List* を参照してください。

SWIFTNet FileAct の標準機能は以下の通りです。

SWIFTNet FileAct 標準機能

SWIFTNet FileAct には以下の標準機能が搭載されています：

- 認証管理：
 - 送信者認証（SWIFT が管理）
 - 送信者認証（受信者が管理）

- SWIFTNet Link 認証管理
- クローズドユーザーグループ(CUG)管理
- ロールベースアクセス管理 (RBAC)
- 機密性の管理：
 - SWIFTNet Link(SNL) 暗号化
 - 仮想プライベートネットワーク (VPN) ボックス暗号化
 - SWIFTNet セントラルシステムによる機密性保護
- 整合性管理
 - SWIFT による整合性管理
 - 受信者による整合性管理
- セントラルファイルルーティング
- あらゆるファイルコンテンツの送信
- 実行中のファイル送信をキャンセル
- ファイル送信ステータスと進捗状況
- 断続的な通信エラーの処理
- 送信速度の自動制御

3.2.3.1 認証管理

概要

SWIFTNet FileAct は、以下の 3 種類の標準認証管理およびその補完機能を提供しています：

- 送信者認証 (SWIFT が管理)
- 送信者認証 (受信者が管理)
- SNL 認証管理

ノート SWIFT は、SWIFTNet FileAct を使用して機密性の高いファイルを送信する場合は、エンドツーエンド署名を使用することを強く推奨します。

SWIFT による送信者認証管理

SWIFT は、SWIFT がファイルを受信した時点で有効な SWIFTNet PKI 証明書を持っているユーザーから送信された SWIFTNet FileAct ファイルのみを送信します。

SWIFT は、メッセージのヘッダーに送信者の BIC8 が記載され、秘密鍵で署名された SWIFTNetFileAct ファイルのみを送信します。SWIFT は、これを全ての SWIFTNet FileAct 送信リクエストに適用します。

これらの検証条件を満たさないファイル送信リクエストは、受信者に送信されません。

認証に関するより詳細な情報は、“SWIFTNet 公開鍵基盤(PKI)” ページの 88 を参照してください。

送受信される各ファイルについて、SWIFTNet システムはファイルを署名するために使用されている PKI 証明書が破棄されていないかどうかをチェックします。

受信者による送信者認証

送信されてくるメッセージに対し、受信者側で送信者認証を適用させることができます。そのために、送信者がファイル送信リクエスト（もしくはレスポンス）を送信する際にエンドツーエンド署名を選択し、受信者は送信されてきたファイル送信リクエスト（もしくはレスポンス）を受信する際にそのエンドツーエンド署名を検証します。

否認防止オプションが使用されている場合、ユーザーはエンドツーエンド署名を使用しなければなりません。ユーザーは SWIFTNet FileAct ファイル送信リクエストに受信認証管理を適用させることが可能です。

認証における PKI に関するより詳細な情報は、“SWIFTNet 公開鍵基盤(PKI)” ページの 88 を参照してください。エンドツーエンド署名に関するより詳細な情報は、*SWIFTNet Link Service Description* を参照してください。

SWIFTNet Link 認証管理

SWIFT は、SWIFT が付与した有効な鍵を持つ SWIFTNet Link から送信された SWIFTNet FileAct ファイルのみを送信します。

より正確には、SWIFT はこれを全ての SWIFTNet FileAct 送信リクエストに適用します。この認証管理の条件を満たさないファイル送信リクエストは、受信者に送信されません。

3.2.3.2 クローズドユーザーグループ管理

説明

SWIFT は、ファイルの送受信をするユーザーが当該サービスのクローズドユーザーグループ (CUG) で構成されている場合に限り、SWIFTNet FileAct ファイルを送信します。SWIFT は、CUG のサービスアドミニストレーターが提供する指示に従って CUG を構成します。

SWIFT は、サービスアドミニストレーターにより定義された送信者、受信者、そしてファイルタイプの有効な組み合わせに合致している SWIFTNet FileAct のみを送信します。ファイルタイプは、ファイル送信リクエストのリクエストタイプフィールドに記載されているものを参照することに注意してください。

SWIFT は、これを全ての SWIFTNet FileAct 送信リクエストに適用します。これらの管理条件を満たさないファイル送信リクエストは、受信者に送信されません。

3.2.3.3 Role-Based Access Control (ロールベースアクセス管理)

説明

サービスアドミニストレーターがロールベースアクセス管理 (RBAC) を選択すると、SWIFT は適切な RBAC プロフィールを持つユーザーが送信者である場合のみ、SWIFTNet FileAct ファイルを送信します。適切な RBAC プロフィールとは、ファイルが送信されるサービスにおいて少なくとも 1 つのロールがユーザーに割り当てられているものです。

SWIFT は、サービスアドミニストレーターが RBAC を使用すると選択したサービスに関連して送受信される全ての SWIFTNet FileAct ファイル送信リクエストに、RBAC 管理を適用します。サービスアドミニストレーターが RBAC 管理を選択した場合、SWIFT はこの管理条件を満たしていないファイル送信リクエストを受信者に送信しません。

またサービスアドミニストレーターがこのオプションを選択した場合のみ、SWIFT は受信者に送信者のサービス関連 RBAC プロフィール情報を SWIFTNet FileAct ファイル送信リクエストと

共に送信します。これにより、受信者は送信者がファイル送信に必要なアクセス管理プロフィールを持っているかどうかを検証することができます。

RBAC に関するより詳細な情報は、*SWIFTNet Service Design Guide* を参照してください。

3.2.3.4 機密性の管理

説明

SWIFTNet FileAct は、以下の標準機密性管理およびその補完機能を提供しています：

- SWIFTNet Link(SNL) 暗号化
- 仮想プライベートネットワーク (VPN) ボックス暗号化
- SWIFTNet セントラルシステムによる機密性保護

SWIFTNet リンク暗号化

SWIFT は、ユーザーの SWIFTNet Link と SWIFTNet セントラルシステムのフロントエンドプロセッサ間で送受信される、全ての SWIFTNet FileAct ファイルを暗号化します。

SWIFT は、このプロセスを全ての SWIFTNet FileAct ファイル送信リクエストおよび実際に送信されたファイルに適用します。

VPN ボックス暗号化

SWIFT は、ユーザーの VPN ボックスと SWIFT が管理しているセキュア IP ネットワーク(SIPN) バックボーンアクセスポイント間の送受信において、SWIFTNet FileAct ファイルを含む全ての SIPN 通信を暗号化しています。

SWIFT は、このプロセスを全ての SWIFTNet FileAct ファイル送信リクエストおよび実際に送信されたファイルに適用します。

SWIFTNet セントラルシステムによる機密性保護

SWIFT は、SWIFTNet セントラルシステムに保存されている SWIFTNet FileAct ファイルを、認証されていないアクセスおよびディスクロージャーから保護します。

SWIFT は、このプロセスを全ての SWIFTNet FileAct ファイル送信リクエストおよび実際に送信されたファイルに適用します。

3.2.3.5 整合性管理

説明

SWIFTNet FileAct は、以下の標準整合性管理およびその補完機能を提供しています：

- SWIFT による整合性管理
- 受信者による整合性管理

SWIFT による整合性管理

SWIFT は、送信者と受信者の SWIFTNet Link 間で送受信されている間にファイル内容に変更がなかった SWIFTNet FileAct ファイルのみを配信します。

SWIFT は、これを全ての SWIFTNet FileAct ファイル送信に適用します。この管理条件を満たさないファイル送信は、受信者に送信されません。

受信者による整合性管理

送信者がエンドツーエンド署名を選択した場合、SWIFT は署名がつけられたメッセージの内容がユーザーにより使用されている SWIFTNet Link 間での送受信中に変更されていないことを、SWIFTNet FileAct ファイルの受信者が検証できるようにします。

エンドツーエンドとは、ここでは取引先の SNL 間のことを指します。

否認防止オプションが選択されている場合、受信者は整合性管理を使用しなくてはなりません。

受信者が整合性管理を適用するには、ファイル送信リクエストの送信者が送信の際にエンドツーエンド署名オプションを選択し、受信者はそのリクエストを受信した際にエンドツーエンド署名を検証する必要があります。

SWIFTNet FileAct を使用して機密性の高いファイルを送信する際は、整合性管理を使用することが強く推奨されます。

PKI 認証に関するより詳細な情報は、“SWIFTNet 公開鍵基盤(PKI)” ページの 88 を参照してください。エンドツーエンド署名に関するより詳細な情報は、*SWIFTNet Link Service Description* を参照してください。

3.2.3.6 セントラルファイルルーティング

説明

SWIFT は、事前に定義されている受信者のセントラルルーティングルールに従い、SWIFTNet FileAct ファイルをストアアンドフォワードキューもしくは SWIFTNet Link (SNL) に送信します。

ノート リアルタイムのダウンロードモードでは、SWIFT はファイル送信リクエストの発信元である SWIFTNet Link にファイルを送信します。

受信者は、ルーティングルールを各自で管理します。SWIFT は、それらのルールを SWIFT Message Reception Registry (MRR) に保存します。セントラルルーティングルールの構成に関するより詳細な情報については、“セントラルルーティングルール” ページの 62 を参照してください。

3.2.3.7 あらゆるファイルコンテンツの送信

説明

SWIFTNet FileAct は、1 ファイル/250MB まで送信することができます。

ASCII やバイナリデータなど、あらゆる種類のコンテンツを送信することができます。

ファイルのコンテンツに関する責任は、全てユーザーにあります。ユーザーは、ファイルのコンテンツがいかなるセキュリティ上のリスクも生じさせないものであることを確実にしなければなりません。特に、ウィルスなど送信者、SWIFT、受信者をリスクに晒す危険性のあるデータがコンテンツに含まれていないことを保証する必要があります。

ファイル内容の変換（ファイル圧縮など）はユーザーの責任となります。バイラテラルファイルの圧縮に関するより詳細な情報は、*SWIFTNet Messaging Operations Guide* を参照してください。

送信者は、ファイルを送信する前にファイルを最新のアンチウィルスソフトウェア（できれば複数のウィルス検出システムを持つもの）でチェックすることが推奨されます。また、受信者側でも同様にチェックすることが推奨されます。

変換されたファイル（圧縮や暗号化など）を送受信する際は、送信側で変換ファイルに対応しているアンチウィルスソフトウェアを使用してチェックすることが強く推奨されます。アンチウィルスソフトウェアが変換ファイルに対応していない場合、送信側で変換する前にファイルをチ

ェックすることを推奨します。受信側でも、変換ファイルを元に戻した際にまたウィルスチェックをすることが推奨されます。

3.2.3.8 ファイルの同時送信

説明

ユーザーは複数のファイルを同時に送信することができます：回線容量にもよりますが、30 ファイルの並列送信が可能です。回線容量ごとの推奨される並列送信ファイル数については、*SWIFTNet Connectivity Packs* を参照してください。

ノート SWIFTNet FileAct にアクセス可能なインターフェースを使用しているユーザーの場合、同時に送信できるファイル数がデフォルトとは異なることがあります。これは使用するインターフェースソフトウェアによっても異なります。

3.2.3.9 実行中のファイル送信をキャンセル

説明

リアルタイムモードで SWIFTNet FileAct を使用している場合、送信者/受信者ともに実行中のファイル送信をキャンセル（中止）させることができます。ストアアンドフォワードモードで SWIFTNet FileAct を使用している場合、送信者は SWIFT に送信中のファイルしかキャンセルすることができません。受信者は、SWIFT から送信されている途中のファイルしかキャンセルできません。送信は、送信リクエスト中にシステムが自動的に割り当てる固有のファイル送信参照を参照します。

SWIFT がファイル送信を完了させている、もしくは SWIFT の参照が正しくない場合、ファイル送信は中止できません。これらの場合、SWIFT はファイル送信を中止せず、エラーメッセージを送信します。

3.2.3.10 ファイル送信ステータスと進捗状況

説明

SWIFTNet FileAct は、ファイル送信ステータスと進捗状況を以下のようにモニターします。：

- **ファイル送信のステータスを取得**

ユーザーは、ファイル送信中いつでも当該ファイルのステータスを照会することができます。

- **ファイル送信イベントに登録**

ファイル送信の開始時、SWIFTNet FileAct はファイル送信中に状態が変化するごとに呼び出しをするルーティンの識別子を提供します。

ノート ストアアンドフォワードモードで SWIFTNet FileAct を使用する場合、ファイルの送信者がモニターできるのは送信者から SWIFT に送信される間のみです。つまり、SWIFT から受信者に送信される間について送信者はモニターできないということです。また、受信者側についても同様の制限があります。

3.2.3.11 断続的な通信エラーの処理

説明

ファイル送信が開始されると、SWIFTNet FileAct は送信が完了、中止、または特定のエラーにより終了されるまでモニターします。

また特定の通信エラーが発生した場合は自動的に回復します。

3.2.3.12 SWIFTNet FileAct により使用されるリソースの自動制御

説明

SWIFTNet FileAct は、複数の SWIFTNet サービス (SWIFTNet FIN、SWIFTNet InterAct など) が回線を同時に使用している場合、SWIFTNet への接続がファイル送信によって全てふさがれてしまうのを防ぐよう設計されています。

SWIFTNet FileAct は、リソースを管理する以下の機能があります:

- **送信速度の調整**

SWIFTNet FileAct は、ファイルをいくつかに分割して送信します。その分割ファイルを何秒ごとに SWIFTNet Link(SNL)で発信するかは、パラメータで定義します。デフォルトでは 0 秒に設定されていますが、SNL をインストールする際にユーザーが 0 ~ 120 秒の間で設定することができます。また至急用および通常用として、別の秒数を設定しておくこともできます。

- **SNL における通信の自動分割**

SWIFTNet Link 6.1 では、SWIFTNet FileAct と SWIFTNet FIN、または SWIFTNet InterAct 間における通信フローの自動分割が導入されています。この機能は、両方の通信フローが同時に同じ SNL にある場合、一方のフローがもう一方に過度の影響を与えないように制御します。

つまり、SWIFTNet FileAct の通信と SWIFTNet FIN もしくは SWIFTNet InterAct の通信が同時に高スループットとなった場合、SWIFTNet FileAct は SWIFTNet Link のメッセージングリソースの 50 パーセント以上を使用することはできないということです。これにより、同時に存在している SWIFTNet FIN もしくは SWIFTNet InterAct (またはその両方) の通信フローを効果的に保護します。仮に、特定の時点において SWIFTNet FileAct 通信のみ、もしくは SWIFTNet FIN か SWIFTNet InterAct 通信のみしかない場合、SNL リソース全体をその通信フロー用として使うことができます。

この機能は SNL 6.1 がインストールされると自動的に有効となるため、構成する必要はありません。

3.2.3.13 汎用 SWIFTNet FileAct ディレクトリ

説明

SWIFT は、www.swift.com にある SWIFTNet サービスディレクトリ (SWIFTNet Services Directory。限定コンテンツ) の一環として、汎用 SWIFTNet FileAct ユーザーに関するアドレスリングデータを網羅したディレクトリを発行しています。汎用 SWIFTNet FileAct ディレクトリは週次ベースで更新され、ユーザーが自身のバックオフィスアプリケーションと共に使用できる情報などがダウンロードできるようになっています。

汎用 SWIFTNet FileAct ディレクトリに関するユーザーコミットメントについては、“顧客の責任範囲” ページの 132 を参照してください。

3.2.4 SWIFTNet FileAct の付加価値オプション機能

概要

オプションの付加価値機能には、SWIFTNet FileAct 料金のほかに追加料金がかかります。価格に関するより詳細な情報については、*SWIFT Price List* を参照してください。

SWIFTNet FileAct のオプション付加価値機能は以下の通りです。

オプション機能

SWIFTNet InterAct には、オプションとして以下の付加価値機能があります：

- ファイルのプライオリティ
- 受領事実の事後否認防止
- 送信完了通知

3.2.4.1 ファイルのプライオリティ

説明

SWIFTNet FileAct には、ファイルごとにプライオリティをつけられるオプション機能があります。普通もしくは至急のいずれかを選択します。

以下のような場合に、プライオリティ機能で優先度を示すことができます：

- 当該ファイルを、特定の至急レベルで扱う必要があることを取引先に示す
- キューからプライオリティ順に送信されるようにする（ストアアンドフォワードモードのみ）
- ファイル送信のプライオリティに従い、ペーシングパラメータを調整

ノート SWIFTNet FileAct のペーシングパラメータは、ユーザーが SWIFTNet FileAct でのファイル送信とその他の通信（SWIFTNet InterAct や SWIFTNet FIN など）を同時に使用した場合の影響を軽減するためのテクニカルパラメータです。

3.2.4.2 否認防止（Non-repudiation）

概要

サービスアドミニストレーターもしくはメッセージの送信者（またはその両方）が否認防止を選択した場合、SWIFT は SWIFTNet FileAct ファイルの送受信をそれに先立つ 124 日間にわたって確認（また要求があった場合にはその証明を発行）することができます。発信の否認防止の場合、ファイルの発信に対して適用されます。受信の否認防止の場合、ファイルの受信に対して適用されます。

サービスアドミニストレーターは、当該サービスの否認防止オプションを必須、オプション、使用不可から選択して定義することができます。

ファイル送信での否認防止とは

否認防止は、発信元、発信、そして送信もしくは復元されたファイルの受信（オプション）における信頼性を確認できるデータにユーザーがアクセスできるようにします。ユーザーは、これらの情報を送信者の身元、ファイル送信が開始された時間、送信されたデータの整合性など、SWIFTNet PKI ベースの検証を用いて確認することができます。

発信元、発信、ファイルの受信の正当性を得るには、送信者と受信者の双方が本書で説明されている必要な手順を実行しなくてはなりません。

3.2.4.2.1 発信元の否認防止

概要

発信元の否認防止は、有効な SWIFTNet PKI 証明書を持っている発信者がファイルダイジェストに署名した、とユーザーが確認できるデータへのアクセスを可能にします。有効な SWIFTNet PKI 証明書とは、送信リクエストの署名者 DN フィールドに表示されている識別名(DN)に対して SWIFT が発行したものです。

発信元の否認防止を使用するには、ユーザーが SWIFTNet FileAct でエンドツーエンド署名オプションを使用する必要があります。エンドツーエンド署名オプションに関するより詳細な情報は、“SWIFTNet 公開鍵基盤(PKI)” ページの 88 を参照してください。

ノート ユーザーは、発信元の否認防止をエンティティレベルで設定することができます。例えば、特定のエンティティの識別名(DN)に添付する信用レベルについて、送信者/受信者ともに合意したものを設定することができます。

3.2.4.2.2 発信の否認防止

概要

発信の否認防止は、受信したファイルの発信元、ファイル送信が開始された時間、そしてファイルの送信先の信頼性をユーザーが確認できるデータへのアクセスを可能にします。

発信の否認防止を使用するには、ユーザーが SWIFTNet FileAct 送信リクエストの否認防止オプションおよびエンドツーエンド署名オプションを使用する必要があります。

サービスに対してサービスアドミニストレーター が発信の否認防止を必須として定義すると、そのサービス内における全てのファイル送受信に否認防止が適用されます。

サービスの発信の否認防止が任意となっている場合、発信者はファイルのうち否認防止オプションが必要なものを SWIFTNet Link(SNL)に指示します。

リアルタイムモードでのファイル送信に否認防止オプションを使用する場合、送信完了通知を使用しなければなりません。

否認防止のため、ユーザーは常にエンドツーエンド署名を使用する必要があります。

主な特長

SWIFTNet FileAct にある発信の否認防止オプションの主な特長は以下の通りです:

- **SWIFTNet Link(SNL)による否認防止プロセス**

否認防止オプションが選択されたファイル送信リクエストが送信されると、以下の追加プロセスが適用されます:

送信者の SNL が、**プットファイル**もしくは**ゲットファイル**リクエストのファイル送信が開始された現地時間 (UTC) を含む **TransferRef** を自動的に追加します。SNL は、ユーザーが署名しなくてはならないメッセージにこれらの参照を含めます。

TransferRef には、発信した現地時間が簡略化された形式で記載されています。**プットファイル**もしくは**ゲットファイル**リクエストの送信者は、エンドツーエンド署名オプションを選択する必要があります。送信者の SNL は、**プットファイル**もしくは**ゲットファイル**リクエストのファイル送信の開始時にファイルダイジェストに署名します。

プットファイルもしくはゲットファイル送信リクエストの受信者は、これらのリクエストに対するレスポンスの署名として否認防止オプションおよびエンドツーエンドオプションを選択する必要があります。

プットファイルもしくはゲットファイルリクエストの受信者の SNL は、送信リクエストのレスポンスのヘッダーとペイロードが署名されていることを確認した後、その署名されている情報に TransferRef を自動的に追加します。この参照には、プットファイルもしくはゲットファイルリクエストに対するレスポンスの発信時間が含まれています。

• 送信完了通知

送信者が、リアルタイムモードでのファイル送信に否認防止オプションを選択した場合、ファイルの受信者は送信者に送信完了通知を送信しなくてはなりません。この送信完了通知には、否認防止オプションとエンドツーエンド署名オプションが選択されている必要があります。

• 時間の整合性チェック

SWIFTNet セントラルシステムは、*発信時間*と*セントラルシステムでの処理時間*を比較します。通常、これらは近い時間となっています。時間差が 5 分以上だった場合、SWIFTNet は警告を記録します。警告は SWIFTNet により受信者にも送信されるので、受信者側で適切な対応をとることができます。

• 否認防止データを安全に保存

リアルタイムモードでの SWIFTNet 本番環境（パイロット（テストアンドトレーニング）、サービスのライブモードを含む）において、特定のファイル要素は SWIFT オペレーティングセンター（OPC）で安全に保存されます。保存されるのは、プットファイルもしくはゲットファイルリクエスト（リクエストとレスポンス）ヘッダー要素、ファイル概要、送信完了通知、そして署名です。

ストアアンドフォワードモードで送信されたファイルの場合は、プットファイルリクエストのヘッダー要素、ファイルダイジェスト、受信者が SWIFT に送信した配信確認、SWIFT オペレーティングシステムに保存されている署名が保存されます。

ノート しかしながら、通常では起こりえない災害や事故などによりサイトが完全に稼働不能となり、OPC にも影響が出た場合、サイトが稼働不能となった時点から 90 分前までの間に記録された否認防止データの復元について SWIFT は保証するものではありません。

• 復元および再検証

否認防止オプションが選択されたファイルの送信者および受信者は、ファイルが送信された後 124 日間中であれば、否認防止に関連するデータの復元を SWIFT に依頼することができます。

クリーンアッププロセスのタイミングなどにより、124 日間以上メッセージが保存されている場合もありますが、SWIFT では復元可能な期間を「メッセージ発信後 124 日以内」と定めています。

ユーザーは、否認防止プロセスを特定のデータ復元に使用することができます。例えばユーザー間でなんらかの争議となった場合、SWIFT は以下の情報を復元することが可能です：

- エンドツーエンド署名および SWIFT が追加した情報（スイッチングの時間など）を伴った、プットファイルもしくはゲットファイルリクエスト（リアルタイムモードのみ）
- ユーザーがメッセージ内で使用した証明書に関する全てのデータ（証明書履歴、作成や破棄についてなど）

- 受信者が否認防止を選択して受信の確認を送信していた場合、送信完了通知（リアルタイムモード）もしくは配信確認（ストアアンドフォワードモード）

ファイルの送信者および受信者は、元のファイルを SWIFT に提出し、そのファイルダイジェストを SWIFT で再度計算してプットファイルもしくはゲットファイルリクエストと比較することを依頼できます。

なんらかの争議があった場合、ファイルの発信や受信などを証明するため、送信者および受信者はこのような情報の復元を SWIFT に依頼することができます。そうした依頼があった場合、SWIFT は（その他のデータのなかでも特に）ファイルデータおよびファイル送信の一意識別参照情報を提出するよう依頼者に求めます。これはファイル送信の一意識別参照情報もしくは RequestRef フィールドにあたります。SWIFT は、ファイル送信の復元を容易にするため、RequestRef フィールドにユーザー独自に一意識別参照参照を入れておくことを推奨します。

ユーザーが正式に再検証を要求し、その復元する情報が否認防止オプションがつけられている SWIFTNet メッセージもしくはファイルに関連している場合、SWIFT は通常 5 営業日以内にユーザーが指定した方法により再検証および復元を実行します。

3.2.4.2.3 受信の否認防止

概要

受信の否認防止は、送信者および受信者がファイルの受信者の身元を確認するため、または受信者がファイルを受信したかどうかを確認するためなどに利用可能なデータへのアクセス手段を提供します。

主な特長

受信の否認防止は、発信の否認防止が選択されているファイル送信で使用することができます。ファイルの受信者がリアルタイムモードで送信完了通知（必須）を送信、もしくはストアアンドフォワードモードで配信確認を送信している場合に使用可能となります。

主な特長は発信の否認防止と同様です（“主な特長” ページの 45 を参照してください）。

ユーザーの責任

受信の否認防止を使用するには、ユーザーは以下を実行する必要があります：

- 送信リクエストを送信する際、否認防止オプションを選択（サービスアドミニストレーターの定義により、サービスに否認防止が自動的に適用される場合を除く）
- リアルタイムモードでファイルを受信した場合は、送信完了通知（必須）を送信
- ファイル送信に使用するアプリケーションが、*SWIFTNet Service Design Guide* に記載されている否認防止オプションのガイドラインを順守していることを保証する

ユーザーが正式に再検証を要求し、その復元する情報が否認防止オプションがつけられている SWIFTNet メッセージもしくはファイルに関連している場合、SWIFT は通常 5 営業日以内にユーザーが指定した方法により再検証および復元を実行します。

3.2.4.3 送信完了通知

説明

ユーザーが SWIFTNet FileAct をリアルタイムモードで使用した場合、ファイルの送信者が送信完了通知を要求している場合のみ受信者が配信確認を送信するというオプション機能が使用可能となります。

また、送信者がサービスに対して SWIFTNet FileAct をストアアンドフォワードモードで使用するすると、送信完了通知オプションが選択可能となります。送信者がこれを選択すると、SWIFT は受信者から配信確認を受信した際に送信完了通知を作成します。この送信完了通知により、ファイルが受信されたことが示されます。送信完了通知は、送信者が指定した SWIFT のキューに保存されます。

送信者は、送信したファイルに対応するダイジェストが送信完了通知に含まれていることを確認し、受信者から送信されてきた送信完了通知を検証する必要があります。検証が失敗した場合はファイルが受信されていないものと見なし、送信者は問題を解決するために受信者と連絡を取らなくてはなりません。

送信者が否認防止をリアルタイムモードで使用した場合（“否認防止 (Non-repudiation)” ページの 30 を参照）、送信者は送信完了通知オプションを選択する必要があります。それに加え、受信者が送信完了通知を送信する際に、否認防止オプションが適用されていることを保証する必要があります。

その他の場合、送信完了通知はオプションとなっています。例えば、受信者がファイルを受信しており、ファイルの所有責任は受信者にあることを送信者が明確にしたい場合などに使用します。

リアルタイムモードの場合、送信完了通知が必須となっているファイルを受信した受信者は、送信者に送信完了通知を送信しなくてはなりません。また、各送信完了通知は前回のファイル送信と関連している必要があります。

3.2.5 サービスアドミニストレーターが定義できる機能

説明

各サービスアドミニストレーターは、サービスプロフィールの一環として特定の SWIFTNet FileAct 機能を定義することができます。

サービスアドミニストレーターが定義できるのは、以下のいずれかに該当する機能です：

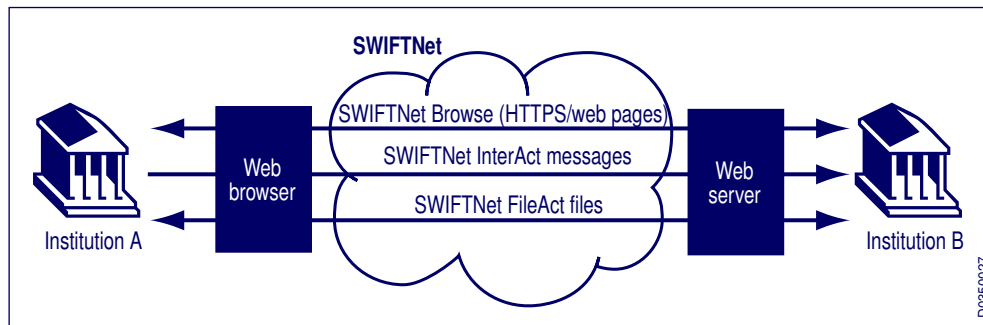
- **使用不可**：当該サービスには使用できない機能です。
- **必須**：当該サービスに関連して送受信される全てのファイルに使用される必要がある機能です。
- **ファイルベースごとに選択可能**：PUTファイルもしくはGETファイル送信リクエストの送信者は、これを送信する際に機能を選択することが可能です。

これらの機能の定義に関するより詳細な情報は、*SWIFTNet Messaging Operations Guide* を参照してください。

3.3 SWIFTNet Browse

概要

SWIFTNet Browse は、ユーザーが SWIFTAlliance WebStation を使用してアクセスできる SWIFTNet メッセージングサービスです。



SWIFTAlliance WebStation は、SWIFTNet Browse、SWIFTNet InterAct、SWIFTNet FileAct に基づいたビジネスサービスにおける個人対アプリケーションのコミュニケーションにグラフィカルユーザーインターフェース(GUI)を使用しています。

SWIFTAlliance WebStation は、以下のモードで稼働します:

- サービスにおける、グラフィカルユーザーインターフェース(GUI)モード
- ブラウズモード

SWIFTAlliance WebStation に関するより詳細な情報は、*SWIFTAlliance WebStation Service Description* を参照してください。

SWIFTNet Browse は、SWIFTAlliance WebStation で標準ブラウザを使用しているオペレーターがサービスプロバイダーのウェブサーバーに安全にアクセスできるよう、セキュア IP ネットワーク(SIPN)と SWIFTNet を経由した、安全なブラウズベースのアクセスを可能にします。また、強固な安全性を実現するため異なる種類のコミュニケーションチャンネルを組み合わせます。

SWIFTNet Browse は、個人対アプリケーションで使用するためのものです。また、HTML ベースのインターフェースでの使用が想定されています。SWIFTNet Browse により利用可能となったコミュニケーションチャンネルを、アプリケーション間のデータ送信のために使用しないでください。SWIFTNet Browse 通信の送受信が可能なのは、SWIFTAlliance WebStation を伴った SWIFT ソフトウェア、ウェブサーバー、そしてブラウザのみです。

SWIFTNet Browse は、HTTPS と SWIFTNet InterAct もしくは SWIFTNet FileAct (またはその両方) メッセージングサービスなど、異なるテクニカルデータチャンネルを組み合わせます。HTTPS は HTML データの交換に使用されており、データ交換の大部分に使用されています。標準の SWIFTNet InterAct および SWIFTNet FileAct メッセージングサービスも、ブラウズセッション内でメッセージやファイルの交換をするために使用することができます。

SWIFTNet Browse の処理の背景において、以下のデータタイプを交換するためにユーザーは SWIFTNet InterAct もしくは SWIFTNet FileAct (またはその両方) を使用する必要があります。:

- 署名付メッセージ
- 自動処理される金融データ

署名付メッセージ

ブラウズセッションを安全に実行するため、ブラウズセッションごとに少なくとも一件の SWIFTNet InterAct と共に SWIFTNet Browse を使用しなくてはなりません。ユーザーはこの必須 SWIFTNet InterAct メッセージに必ず署名をつける必要があります、またそのメッセージにはリクエストタイプ **swlogon** が含まれている必要があります。

SWIFT は、機密性の高いメッセージやデータの送受信には SWIFTNet InterAct もしくは SWIFTNet FileAct (またはその両方) を使用することを推奨します。

SWIFTNet InterAct および SWIFTNet FileAct を使用することにより、SWIFTNet PKI ベースの認証や否認防止などのセキュリティ機能を利用することができます。

自動処理される金融データ

送信した金融データを受信者が自動処理することが想定される場合、SWIFTNet InterAct もしくは SWIFTNet FileAct（またはその両方）で送信する必要があります。

金融データとは、エンドツーエンド金融取引プロセスの一環として SWIFTNet が処理する全てのデータを指します。例えば、取引開始データ、取引確認データ、トランザクションレポートデータ、取引のプロセスをサポートするオペレーションのデータなどが該当しますが、これ以外にも様々なものが含まれます。

3.3.1 特定の機能

概要および背景

SWIFTNet Browse は、標準ブラウザを使用してセキュア IP ネットワーク(SIPN)経由でビジネスサービスにアクセスできる、個人対アプリケーションアクセスを提供します。

SWIFTNet Browse は、SWIFTAlliance WebStation とサービスプロバイダーが当該ビジネスサービスのためにホストしているウェブサーバー間における HTTPS インターアクション（セキュアソケットレイヤー [SSL]の上に HTTP）に基づいています。

SWIFTNet Browse は、サーバーとクライアントの両方が認証される、双方向の認証方式を持った SSL ハンドシェイク管理を使用しています。

SWIFTNet Browse 用として、ユーザーはウェブクライアントとウェブサーバーの両方に SWIFTNet ウェブ証明書を使用します。これらの証明書は、SWIFTNet セキュリティポリシーの制約下にあります。SWIFT ポリシーとして、ユーザーは全てのサーバーが相互認証するように構成しなければなりません。認証およびウェブ証明書に関するより詳細な情報は、*SWIFTNet Certificate Administration Guide* を参照してください。

SWIFTNet Browse を使用するにあたり、ユーザーは SWIFTNet PKI 証明書を使用しなくてはなりません。他の証明書を使用することはできません。

SWIFTNet InterAct および SWIFTNet FileAct との統合

SWIFTAlliance WebStation は、SWIFTNet InterAct もしくは SWIFTNet FileAct に対して SWIFTNet Browse がコールを開始できる機能を内蔵しています。これらのコールは、SWIFTNet Browse アプリケーションに透過的な方法で統合することが可能です。SWIFTNet Browse にコールを統合させる方法に関するより詳細な情報は、デベロッパーのドキュメントを参照してください。

HTTPS での送受信における整合性管理

整合性を保つため、SWIFT はクライアントサーバーとサービスプロバイダーのウェブサーバー間での送信中にデータが変更されていない SWIFTNet Browse データのみを送信します。

これは HTTPS で送受信される全ての SWIFTNet Browse データに適用されます。

HTTPS での送受信における機密性管理

SWIFT は、ユーザーの VPN ボックスと SWIFT が管理しているセキュア IP ネットワーク(SIPN)バックボーンアクセスポイント間の送受信において、SWIFTNet Browse データを含む全ての SIPN 通信を暗号化しています。

これは HTTPS で送受信される全ての SWIFTNet Browse データに適用されます。

3.4 SWIFTNet Copy

概要

SWIFTNet Copy は、サービス登録機関とサービスアドミニストレーターにより定義された1つもしくは複数のコピー先との間におけるメッセージフローのコピー生成を可能にします。

SWIFTNet Copy は、サービス内のサービス登録機関間における通信フローのモニタリングと管理を行う、柔軟性と安全性の高いシンプルな機能を提供します。

SWIFT は現在、SWIFTNet Copy を SWIFTNet FileAct においてのみ提供しています。SWIFT は FileAct ヘッダー（HeaderInfo 部分が使用された場合はそれも含めて）をコピーしますが、ファイルの内容はコピーしません。

ノート ファイル送信の際、SWIFTNet Copy はストアアンドフォワードモードに基づいて行います。

3.4.1 機能

3.4.1.1 SWIFTNet Copy の作業モード

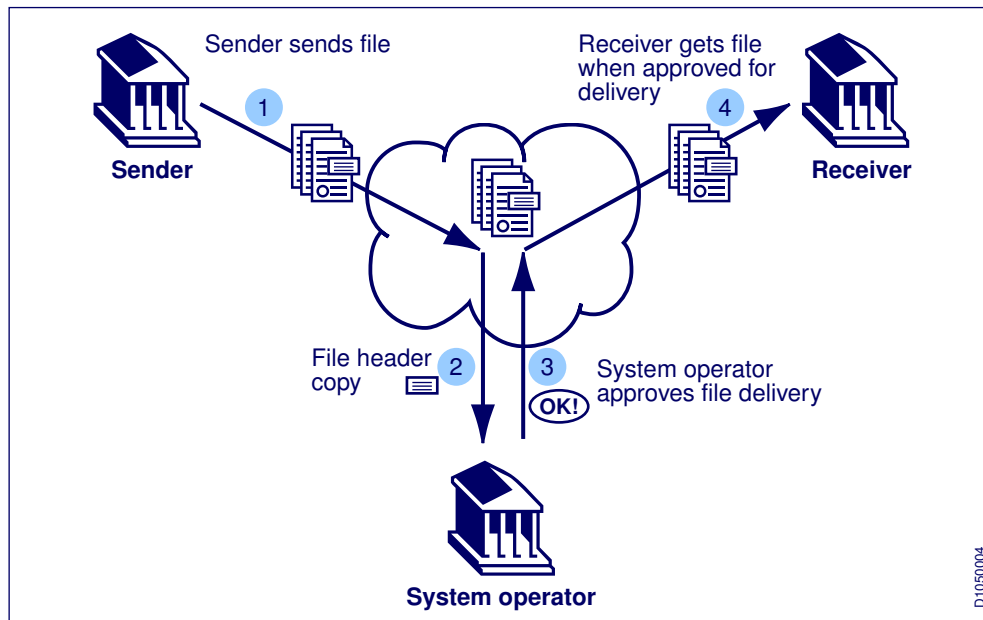
3.4.1.1.1 Y-Copy モード

概要

このモードでは、SWIFT はすぐにファイルを送信しません。SWIFT は、コピー先を操作するシステムオペレーター（コピー先を操作するユーザー。サービスアドミニストレーター自身、もしくはサービスアドミニストレーターにより任命されたほかのユーザー）のコピー先に FileAct ヘッダーをコピーします。その後、システムオペレーターはファイル送信を承認または拒否します。システムオペレーターは、コピーされたヘッダーファイル情報およびその他の情報に基づいてファイル送信の承認・拒否を決定します。システムオペレーターがファイル送信を承認すると、SWIFT は当該ファイルを受取人に送信します。システムオペレーターが拒否した場合、SWIFT は送信者に拒否通知を送信します。

通常、Y-Copy はサービス登録機関間における金融取引の管理、清算、決済を行うため、送金決済システムや証券システムなどの市場インフラにより導入されます。

Y-Copy フロー



送信オーソリゼーション

システムオペレーターは、ファイル送信の承認または拒否を行うために Y-Copy オーソリゼーション (Y-Copy Authorisation) もしくは拒否メッセージを使用します。

オーソリゼーション関連情報

システムオペレーターがファイル送信を承認する場合、決済参照などオーソリゼーションに関連する特定の情報を伝達することができます。SWIFTはこの情報を送信者に送信する Y-Copy オーソリゼーション通知に含めると共に、受信者用のファイル送信にも付加します。

拒否通知

システムオペレーターがファイル送信を拒否した場合、送信者は拒否通知を受け取ります。この拒否通知には拒否理由を記載することができます。

オーソリゼーションと送信のモニタリング

Y-Copy では以下のオプションを使用することができます:

- **オーソリゼーション通知**

システムオペレーターがファイル送信を承認した際、SWIFT が送信者にオーソリゼーション通知を送信するかどうかを決定する機能です。このオプションの使用可否はサービスアドミニストレーターが決定します。使用可能である場合、サービスアドミニストレーターは SWIFT がこれを自動的に適用するか、それとも送信者がファイル送信ごとに選択できるようにするかを決定します。

- **送信完了通知**

通常の SWIFTNet オプションの一環として、ユーザーは送信したメッセージやファイルの配信状況のモニタリングを SWIFT に要求することができます。その場合、SWIFT は送信者に送信完了通知を送信します。Y-Copy モードでは、この送信完了通知はシステムオペレーターに FileAct ヘッダーのコピーが送信されたことではなく、オリジナルの送信ファイルが受信者に送信されたことに基づいて通知されます。

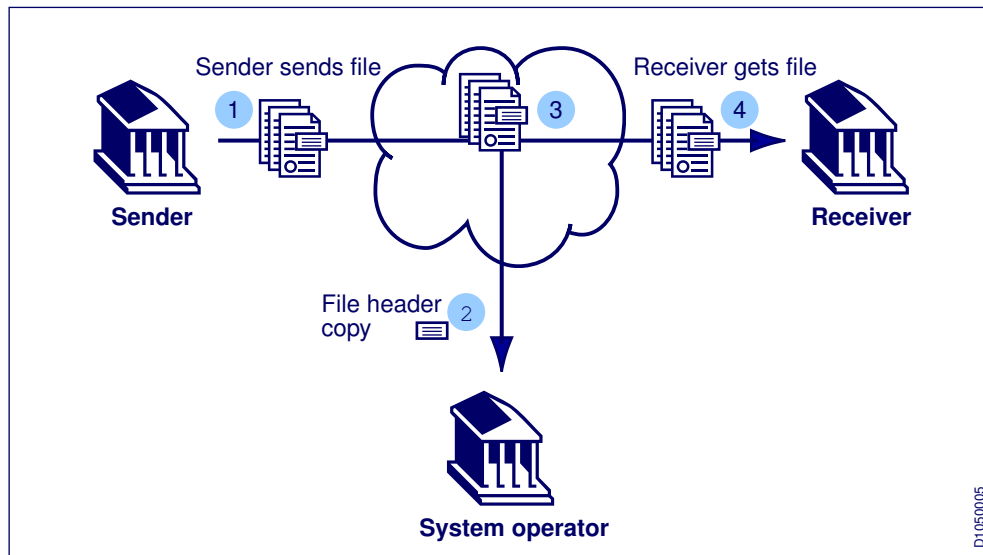
3.4.1.1.2 T-Copy モード

概要

このモードでは、SWIFTNet はファイルを受取人に送信すると同時に、ファイルヘッダーのコピーをシステムオペレーターのコピー先（1つもしくは複数）に送信します。システムオペレーター（サービスアドミニストレーター自身、もしくはサービスアドミニストレーターにより任命されたほかのユーザー）は、コピー先を操作するユーザーです。

通常、サービス登録機関間における金融取引に関する情報を取得するため、金融機関の本社、市場インフラ、中央機関、監督当局などが T-Copy を導入します。また、特定のオペレーションを会計事務所などのサードパーティにアウトソースするため、サービスアドミニストレーターが T-Copy の導入を決定することもできます。

T-Copy フロー



3.4.1.2 SWIFTNet Copy サービスパラメータ

概要

SWIFTNet Copy を使用するサービスのサービスアドミニストレーターは、SWIFT との合意のもとに、導入スケジュールを策定してサービスの監督とオペレーションを行うためのパラメータを定義する必要があります。また SWIFT は、パラメータを定義するサポートを提供します。サービスパラメータ（ライブおよびパイロット環境用）を定義するため、サービスアドミニストレーターは *SWIFTNet Service Profile Form* の SWIFTNet Copy セクションを完了させる必要があります。

ノート 技術文書において、用語「サードパーティ」は「システムオペレーター」と同義語になります。

SWIFTNet Service Profile Form

SWIFTNet Service Profile Form には、以下のパラメータが含まれています。

SWIFTNet Copy サービスパラメータ

パラメータ	内容
SWIFTNet Copy サービス機能の使用目的	テキストでの説明

パラメータ	内容
コピーモード	T-Copy または Y-Copy
コピーモードの使用	任意または必須
システムオペレーターコピー先	コピー先が 1 つ (Y-Copy)、コピー先が 1 つもしくは複数 (T-Copy)
オーソリゼーション通知	使用不可(Not available)、オプション(optional)、必須 (Y-Copy のみ)
フォールバックモード	クローズド (Closed)、バイパス (Bypass)、T-Copy

サービスアドミニストレーターは、特に以下のアクションを実行する必要があります:

- ライブおよびパイロットで使用するサービスモード、コピー先、コピーされた情報のサービスアドミニストレーターの使用目的、サービスを運用するルールを決定するサービス定義パラメータなど、SWIFTNet Copy 要件の定義。このパラメータは SWIFTNet Copy サービスプロフィールを形成します。
- SWIFTNet Copy サービス内で十分な通信網を構築し、SWIFTNet Copy の全サービス登録機関にサービスプロフィールの詳細を送信する
- SWIFTNet Copy サービスのユーザー詳細をグループ内で配布する。

ノート サービスが本番稼働している場合、サービスアドミニストレーターは日常および非常事態の両方において通信方法が適切かつ十分であることを保証する必要があります。これにより、SWIFTNet Copy およびその下にあるサービスの両方に影響する、日常業務における通信が全ユーザーに対して確保されます。

オペレーションを開始させるにあたり、全ての当事者（システムオペレーターおよびサービスに登録しているユーザー）は SWIFTNet インターフェースの SWIFTNet Copy サービスパラメータを、ライブおよびパイロットサービスの両方用として構築する必要があります。

サービスアドミニストレーターの責任を侵害することなく、SWIFT は www.swift.com 上にあるサービスに適用される SWIFTNet Copy パラメータを発行する権利を有します。

3.4.1.3 SWIFTNet Copy の処理

コピーされた情報

T-Copy と Y-Copy モードの両方において、コピーされた情報は SWIFTNet FileAct のテクニカルヘッダー（送信者、受信者、ユーザー参照などのフィールドが含まれる）およびそれが使用されている場合はビジネスヘッダー（HeaderInfo）から構成されています。

またテクニカルヘッダーには、受信者およびシステムオペレーターが整合性検証や認証検証を行うためのセキュリティ関連情報が含まれています。

オープンとクローズ

サービスの SWIFTNet Copy 機能は、オープン (*open*) またはクローズ (*closed*) のいずれかの状態になっています。通常の実行中はオープンとなっています。

通常では起こり得ない非常事態において、システムオペレーターはフォールバック（代替）モードに切り替えなくてはならない場合があります（“SWIFTNet Copy 通常モード/フォールバック（代替）モード” ページの 55 を参照してください）。

サービスの SWIFTNet Copy 機能がクローズで、コピー処理対象のファイルが送信されている場合、ファイルの送信者は適切なエラーコードが記載された否定確認 (Negative Acknowledgement、NAK) を受け取ります。

ノート サービスオペレーターによりフォールバックモード (代替モード) でのオペレーションを要求された場合、SWIFT は一度サービスをクローズしてからフォールバックモードで再度オープンさせなくてはならない場合があります。

送信のモニタリング、送信失敗、重複防止などオペレーション上の関連事項についてのより詳細な情報は、*SWIFTNet Messaging Operations Guide* を参照してください。

3.4.1.4 SWIFTNet Copy 通常モード/フォールバック (代替) モード

通常モード

通常の状態において SWIFTNet Copy 機能はオープンとなっており、通常モードで稼働することを示します。

フォールバックモード

非常事態時には (アプリケーションに重大な問題が発生した場合や災害時など)、システムオペレーターはフォールバック (代替) モードに切り替えなくてはならない場合があります。フォールバックモードは、サービスアドミニストレーターがサービスパラメータを定義する際に決定したモードです。

フォールバックモードは、緊急時に変更することで有効化されます。緊急時の変更に関するより詳細な情報は、“緊急変更” ページの 55 を参照してください。

フォールバックモードシナリオ

サービスアドミニストレーターは、サービス定義の際に以下のフォールバックシナリオから 1 つ選択する必要があります:

- Y-Copy モードで稼働している SWIFTNet Copy 用
 - Y-Copy モードから T-Copy モードへの切り替え
 - Y-Copy モードからバイパス (Bypass) モードへの切り替え
 - Y-Copy モードからサービスをクローズ状態にする
- T-Copy モードで稼働している SWIFTNet Copy 用
 - T-Copy モードからバイパス (Bypass) モードへの切り替え
 - T-Copy モードからサービスをクローズ状態にする

フォールバックモードおよび各モードにおける通信処理の結果に関するより詳細な情報は、*SWIFTNet Messaging Operations Guide* を参照してください。

3.4.1.5 緊急変更

説明

通常の状態において、SWIFTNet Copy パラメータに緊急変更 (モード変更、ユーザーのサービス離脱など) が導入される時間は 45 分となっています。これは SWIFT カスタマーサービスセンター (CSC) がシステムオペレーター代表を承認し、当該システムオペレーターから確認のファックスを受理した時点からの時間となります。

3.4.1.6 パイロットサービス

テスト送信の交換

コピー機能を使用するサービスに登録している全てのユーザーは、テスト目的でファイル送信を行うことができるパイロットサービスを利用することができます。SWIFTは、テスト目的でファイルをコピー先（サービスアドミニストレーターが定義）にコピーします。

3.4.2 セキュリティおよび管理

SWIFTNet Copy サービスとコピー機能

SWIFTは、SWIFTNet Copyを特定のSWIFTNetサービスの機能として導入します。どの通信フローにコピー機能が適用されるかはサービスアドミニストレーターが定義します。

SWIFTNet Copy サービスに登録しているユーザーに対する変更は、変更日の少なくとも14日前までにカスタマーオーダリングサービス（COS）がサービスアドミニストレーターから正しいアップデート情報を受理していることを前提に、休止時間（Allowable Downtime Window、ADW）中に行われます。

電子署名および認証

ファイルの送信者およびシステムオペレーターは、通信をエンドツーエンドで署名することができます。これにより認証と整合性の確認が可能となるため、SWIFTは使用を強く推奨します。SWIFTNet PKIの導入方法により、ファイルの送信者はPKI署名を1つしか計算する必要がありません。この署名はファイルの受信者およびシステムオペレーター用として、2つのデータセットで使用されます。システムオペレーターとファイルの受信者は、PKI署名を使用してファイルの送信者を認証します。

データ認証および整合性に関するより詳細な情報は、*SWIFTNet Messaging Operations Guide*を参照してください。

3.4.3 責任範囲

3.4.3.1 サービスアドミニストレーター

要件

サービスアドミニストレーターに適用される要件に関するより詳細な情報は、“サービスアドミニストレーターのロールおよび責任範囲” ページの131を参照してください。

また、サービスアドミニストレーターが1つもしくは複数のservice participantをシステムオペレーターとして指定した場合、各システムオペレーターが適用される全ての要件を順守することを保証するものとします。いずれの場合においても、第三者をシステムオペレーターとして指名したサービスアドミニストレーターが、その指名先がサービスアドミニストレーターに属する場合と同様に、コピー先のオペレーションに関する全責任を負うものとします。

3.4.3.2 システムオペレーター

SWIFTNet インターフェース要件

システムオペレーター（既に SWIFTNet ユーザーであり、SWIFTNet インターフェースを所有している）は、インターフェースが SWIFTNet Copy をサポートしていることを供給者に確認する必要があります。SWIFTNet インターフェース構成は、サービスアドミニストレーターが定義したコピー先が含まれるよう修正される必要があります。またシステムオペレーターは、SWIFTNet インターフェースがサービスのニーズをサポートするために十分な接続を保持していることを保証する必要があります。

適切な SWIFTNet インターフェースを所有していない場合、システムオペレーターは SWIFTNet のインターフェースを入手する必要があります。インターフェースは、SWIFTNet Copy サービスを運用するために必要な通信の送受信ができるものである必要があります。

システムオペレーターの実行責任

サービスアドミニストレーターは通信プロセスにおいてサードパーティの役割を果たし、以下を行う必要があります：

- ・ モニタリングまたは管理機能、もしくはその両方を実行するために必要なファイル送信の要素を十分に取得する
- ・ その介入が、受信機関への情報送信に影響しないことを保証する

サービスに登録し、かつコピーの対象となっているユーザー間のファイル送受信において、SWIFT はテクニカルヘッダーおよびビジネスヘッダー（HeaderInfo）をサービスアドミニストレーターが定義したコピー先にコピーします。

ライブ稼働およびパイロットのいずれの場合でも、Y-Copy モードにおいてシステムオペレーターは受信した各ファイルヘッダーコピーについて以下を行う必要があります：

- ・ コピーの受信を SWIFT に配信確認する。この配信確認は「拒否」であってはなりません。
- ・ 通信の承認または拒否をします。つまり、システムオペレーターは Y-Copy 承認もしくは Y-Copy 拒否を SWIFT に送信します。

システムオペレーターは、SWIFTNet インターフェースおよびその他のシステムが Y-Copy モードにキューされている SWIFTNet Copy ファイルの処理を過度に遅延させることなく、予測される最大通信量を取扱えることを保証する必要があります。

システムオペレーターは、サービス定義にて定義された全てのファイルタイプを送信・受信できなくてはなりません。

またシステムオペレーターは、バイパスモードでの稼働が Y-Copy モードでの稼働に戻るなど、システムがフォールバック手続きを取扱えることを保証する必要があります。フォールバック手続きを開始させるにあたり、システムオペレーターはカスタマーサービスセンター（CSC）に連絡して変更を依頼する必要があります。フォールバックが必要となった問題原因が解決された際には、システムオペレーターは通常の実行モードに戻すためにフォールバック手続きを再度行わなければなりません。

3.4.3.3 サービス登録機関

SWIFTNet インターフェース要件

SWIFTNet Copy を使用するサービスに登録しているユーザーは、以下を行う必要があります:

- サービスに関連したメッセージやファイルの送受信ができる SWIFTNet インターフェースの保持
- 保持している SWIFTNet インターフェースが SWIFTNet Copy をサポートしていることを供給者に確認

SWIFTNet Copy を使用しているサービスでファイルの送受信を行うため、ユーザーの SWIFTNet インターフェースは以下を行うことができる必要があります:

- サービスアドミニストレーターが認証したファイル、サービスアドミニストレーターが情報を供給したファイルの受信
- エンドツーエンド署名が使用されている場合に SWIFTNet PKI 電子署名を追加する

ノート SWIFTNet Copy を使用しているサービスに登録した全ての SWIFTNet ユーザーは、サービスアドミニストレーターから当該サービスのサービスプロフィールを受け取ります。これにより、サービスに登録しているユーザーは必要に応じて SWIFTNet インターフェースを構成することが可能になります。

サービス登録機関に適用されるその他の要件に関するより詳細な情報については、“顧客の責任範囲” ページの 132 を参照してください。

3.5 ストアアンドフォワード作業モード

3.5.1 キューの種類

概要

ストアアンドフォワードキューには、一般キューそしてオプションの追加キューの 2 種類があります。

一般キュー

各ストアアンドフォワードユーザーは、ストアアンドフォワード一般キューを 1 セット持っています。これには、ライブ稼働用のキューとパイロット（テストおよびトレーニング用）オペレーション用のキューがそれぞれ 1 つずつ含まれています。これらの一般キューは、ユーザーがストアアンドフォワード作業モードで SWIFTNet InterAct もしくは SWIFTNet FileAct を使用する SWIFTNet メッセージングソリューションに初めて登録する際、SWIFT が自動的に作成します。

ストアアンドフォワード一般キューを識別するため、SWIFT はユーザーの BIC を使用します。一般キューは、SWIFTNet InterAct メッセージと SWIFTNet FileAct ファイルの両方を取り扱うことができます。

オプションの追加キュー

適切なオンラインオーダーフォームでのお申し込みをすることで、ユーザーはストアアンドフォワードキューの追加作成を要求することができます。複数のストアアンドフォワードキューを使用することにより、受信者に届けられる前に送信されてくるメッセージやデータをより効果的に分離させることが可能です。

SWIFT は、オプションの追加キューを識別するためにユーザーの BIC と拡張子を組み合わせたものを使用します。

オプションの追加キューにおいて、SWIFTNet が適切なルートをたどり適切なキューに到着するかどうかの責任は、セントラルルーティングルールを設定するユーザーにあります。

セントラルルーティングルールに関するより詳細な情報については、“セントラルルーティングルール” ページの 62 を参照してください。

ノート ユーザー BIC 間で同じストアアンドフォワードキューを共有することはできません。

3.5.2 送信モード

キューをオープンする

ユーザー（受信者）は、キューからメッセージやファイルを受信できるようにするために、まず SWIFT にメッセージを送信してキューをオープンする必要があります。キューは、プッシュモードもしくはプルモードでオープンすることができます。他のアプリケーションが既に開いているキューをオープンしようとした場合、受信者が強制的にオープン (*forced-open*) コマンドを使用していない限り、SWIFT はエラー警告を發します。受信者が強制的にオープンコマンドを使用している場合、SWIFT は他のアプリケーションが使用していたそのキューを閉じ、受信者用として再度オープンします。

ノート SWIFT は、SWIFT サービスの Allowable Downtime Window (ADW) が開始される前に、キューのオープンセッションをクローズすることを強く推奨します。ADW の開始前にキューが閉じられていない場合、ADW 中に強制的にクローズされる可能性があります。こうした場合、ADW 後にもう一度キューをオープンする必要があります。

プッシュ送信モード

プッシュ送信モードでは、SWIFT はキューに滞留している全てのメッセージやファイル通知などを、キューが空になるまで送信します。

空のキューに新規のメッセージやファイルが受信された場合は、直ちに送信されます。受信者から SWIFT にキューのクローズを指示するメッセージが送信されると、SWIFT は当該キューから受信者にメッセージを送信することを中止します。

デフォルト設定では、SWIFT はメッセージやファイルなどを先着順 (FIFO) に送信します。しかしながら、受信者のほうでこの送信順を変更することができます (SWIFTNet InterAct を先に送信する、優先度の高いメッセージを先に送信するなど)。送信順に関するより詳細な情報は、*SWIFTNet Service Design Guide* を参照してください。

ノート キューをオープンする前に、ユーザーはメッセージが送信される先のアプリケーションが起動していることを確認します。アプリケーションは、メッセージを受信した際にそれを確認する必要があります。また、メッセージの確認ができなくなった場合はすぐにセッションをクローズする必要があります。

大量のメッセージやファイルを受信する場合に、プッシュ送信モードを使用することが推奨されます。SWIFTAlliance Gateway および SWIFTNet Link をベースにしたインターフェースは、プッシュ送信モードをサポートしています。

ただし、SWIFTAlliance WebStation が SWIFTNet に直接接続されている場合、プッシュ送信モードは使用できません。

プル送信モード

プル送信モードでは、受信者はキューから取得したいメッセージやファイルごとに SWIFT にプルリクエストを送信します。SWIFT は、リクエストされたメッセージもしくはファイルを受信者に送信します。キューが空だった場合はその旨の通知を送信します。キューから次のメッセージやファイルを受信するには、受信者はまず前回のプルリクエストによって SWIFT から送信されてきたメッセージやファイルの受信の配信確認をし、それから次のプルリクエストを送信する必要があります。

空のキューに新規のメッセージやファイルが受信された場合、SWIFT は受信者からプルリクエストが来るまでそのまま待機しています。

デフォルト設定では、SWIFT はメッセージやファイルなどを先着順（FIFO）に送信します。しかしながら、受信者のほうでこの送信順を変更することができます（SWIFTNet InterAct を先に送信する、優先度の高いメッセージを先に送信するなど）。

プルモードは、メッセージ件数が少ない場合や、手動のインターフェースでファイルを送信する場合などに推奨されます。SWIFTAlliance WebStation はこのモードを使用しています。また全てのタイプの SWIFTNet Link、セキュア IP ネットワーク(SIPN)接続もプル送信モードをサポートしています。

しかし、大量のメッセージやファイルを受信する場合は使用しないほうが良いでしょう。

SWIFTNet FileAct

送信モード（プッシュ/プル）に関わらず、SWIFT は受信者がファイルを SWIFT の中央管理サーバから取得した時点で送信完了と見なします。このため、受信者は SWIFT にファイル取得リクエスト（Fetch File request）を送信する必要があります。

またファイルを受信した時点で、受信者は配信確認を SWIFT に送信する必要があります。プル送信モードでは、受信者はこの配信確認を次のプルリクエストに含めて送信することが可能です。

3.5.3 メッセージもしくはファイルの不達

不達の理由

SWIFT は、ストアアンドフォワードモードの SWIFTNet InterAct メッセージおよび SWIFTNet FileAct ファイルがシステムティックに送信されるよう、様々な手段を講じています。しかし、以下に示すいくつかのケースでは送信不達となる場合があります：

- 受信者が、メッセージもしくはファイルを拒否：
 - 受信者は、ストアアンドフォワードファイルやメッセージの受信を拒否することができません。SWIFT がメッセージを送信し、受信者が否定確認（negative acknowledgement）を送信するとメッセージは拒否されます。SWIFT から送信された交渉メッセージを受信者が拒否した（ファイル送信は実行されない）場合、そして SWIFT がファイルを送信して受信者がそれに対して否定確認（negative acknowledgement）を送信した場合に、ファイルは拒否されます。いずれの場合も、SWIFT は受信者から拒否された旨の不達通知を送信

者のキュー送信します。送信者は、当該メッセージまたはファイルについてそれ以上、送信処理をしてはいけません。

• **タイムアウトにより、SWIFT が送信処理を中止:**

- SWIFT がメッセージまたはファイルを受信してから 14 日間以内に送信を完了できなかった場合、SWIFT は送信者の当該キューに不達通知を送信します。

• **送信の試みが何度も失敗したため、SWIFT が送信処理を中止:**

- 同じメッセージもしくはファイルの送信が 10 回以上にわたり失敗した場合、SWIFT は送信者の当該キューに不達通知を送信します。

送信の試みを中止した後、SWIFT はそのメッセージもしくはファイルに重複警告を添付して再送信するよう連絡します。送信者は、既にそのメッセージもしくはファイルを送信していることを受信者に警告します。

災害などによる SWIFT オペレーティングセンターへの影響

災害などにより SWIFT オペレーティングセンターになんらかの被害があった場合、SWIFT はその 30 分前までにストアアンドフォワードモードで送信された SWIFTNet InterAct メッセージもしくは SWIFTNet FileAct ファイルを送信できない可能性があります。このような場合、SWIFT は影響を受けたユーザーが送信したメッセージの識別をサポートします。

SWIFT オペレーティングセンターで事故などがあり、それによってメッセージやファイルの送信者に影響が出た場合、不達メッセージやファイルの識別および適切な修正措置の実行は送信者の責任となります。

ノート 潜在的な事故や災害を全て防止することはできませんが、SWIFT ではそれに備えて危機管理をしており、影響を最小限に留める努力をしています。

3.5.4 ストアアンドフォワードにおけるアクセス管理

ストアアンドフォワードと RBAC

サービスがストアアンドフォワードモードを使用していてロールベースアクセス管理(RBAC)ロールも使用している場合、SWIFTNet はメッセージもしくはファイルのオーソリゼーションを付与したユーザーに所属するロールが、ファイルやメッセージと共に受信者に送信されるようになります。このサービスはサービスアドミニストレーターが希望した場合のみ適用されます。

ストアアンドフォワードメカニズムも RBAC を使用します。ユーザーは、ストアアンドフォワードキューと情報のやりとりをする際に RBAC ロールが必要となります。キューと情報の送受信をするには、特定の SWIFTNet InterAct メッセージを SWIFT が管理している **swift.snf** サービスに送信します。SWIFT は、潜在的なリスポンダーとしてストアアンドフォワードを使用するビジネスサービスに参加している各機関が、**swift.snf.control** センtralサービスの参加者であることを確実にします。

SWIFT は、ストアアンドフォワードサービスに登録している機関に単一の RBAC ロールインスタンス (**SnFRequestor**) を提供します。このロールは、その機関用としてキューにアクセスする全てのタイプのユーザーリクエストのアクセス管理を行います。ロールには、単一のクオリファイヤー (キュー) があります。ロールには、機関が使用できるキューのリストが含まれています。機関の RBAC 代表者 (権限委任者) は、このロールを機関の 1 つもしくは複数のエンティティに付与することができます。

SWIFT がユーザーのためにストアアンドフォワードキューを作成するごとに、SWIFT はそのキュー名をユーザーの **SnFRequestor** ロールクオリファイヤーキューに追加します。

この時点で、ユーザーの RBAC 代表者（権限委任者）はエンティティがキューにアクセスできるように組織内の他の社員もしくはアプリケーションに値を付与することができます。

また SWIFT は、ユーザーがストアアンドフォワードモードで通信した際にキューへのアクセスを確認します。特にリクエストのオーソリゼーション付与者は、SWIFT からリクエストに関連した送信完了通知や中止通知を送信するキューに対して適切な RBAC ロールを持っている必要があります。

3.5.5 先進的な配信管理（デリバリーコントロール）

概要

SWIFTNet リリース 6.1 は、順序番号（シーケンス番号。現在は送信済の送信もカバー）および不達メッセージレポートなどの先進的な配信管理機能に対応しています。上記のいずれもストアアンドフォワードモードで送受信されたメッセージに適用されます。

SWIFT は、インプットおよびアウトプット期間の先進的な配信管理をサポートしています。これらの管理はメッセージ途切れやメッセージの割込みを検出するほか、重複の検出および防止を行うよう設計されています。また、発注配信（ordered delivery）もサポートしています（FIFO など）。

インプットチャンネル

この機能は、送信者から受信者への FIFO（first-in-first-out、先着順）配信および一回のみ（once-and-only-once）配信をサポートしており、重複の取扱いを最小限に抑えます。この機能は、現在 SWIFTNet InterAct でのみ使用可能です。

メッセージ送信の際、送信インターフェースはシーケンス番号を使用します。これにより、受信インターフェースは受信したメッセージの順序を確認することができ、必要に応じて再度順序の並び替えをすることができます。また異常な順序の途切れや割込みがあった場合に、それを検出することが可能です。より詳細な技術情報に関しては、*SWIFTNet Interface Vendor Specifications for SWIFTNet InterAct and FileAct* を参照してください。

下位互換性を確保するため、SWIFTNet 6.1 での本機能の使用はオプションとなっています。将来的なリリースにおいて必須機能となる予定です。

不達通信レポート

ユーザーが SWIFT に対し、不達通信（SWIFTNet InterAct メッセージ、SWIFTNet FileAct ファイル）に関するレポートを要求することができる機能です。SWIFT は要求を受理すると、必要な情報を抽出して不達メッセージレポートをユーザーに送信します。

SWIFTNet FIN の場合、これはシステムメッセージにより実行されます。システムメッセージに関する技術情報の詳細は、*SWIFTNet Interface Vendor Specifications for SWIFTNet InterAct and FileAct* を参照してください。

3.6 セントラルルーティングルール

概要

ルーティングルールは、SWIFT がメッセージなどをどのキューもしくは SNL エンドポイントに送信するかを決定します。受信者は、ルーティングルールを各自で定義します。ユーザーはサービスに登録した際にルーティングルールを定義し、SWIFT はこれを SWIFTNet セントラルシステムに保存します。

3.6.1 ルーティングルールのフォーマット

説明

ルーティングルールには、以下の4つのフィールドがあります。SWIFT はこれらのフィールドを、SWIFTNet InterAct リクエストもしくは SWIFTNet FileAct 送信リクエストの対応するヘッダーフィールドと一致させます。:

- サービス名
- リクエストタイプ
- リクエスター DN
- リスポンダー DN

SWIFT は、これらのフィールドを使用して適切なルーティングルールを識別します。以下のセクションは、SWIFT がルールを選択する方法を説明しています。

各セントラルルーティングルールには、SWIFT が SWIFTNet InterAct メッセージもしくはファイル送信リクエストをどこにルートするべきかを指示する1つもしくは複数の以下のようなフィールドが含まれています。:

- リアルタイムモード用:
 - 最初の SWIFTNet Link(SNL) ID および SNL エンドポイント
 - オプションとして、1つ、2つ、もしくは3つの追加 SNL ID/SNL エンドポイント
 - アクティブエンドポイントインジケータは、4つのアドレスのうち現在 SWIFT がどのルートで送信しているかを示します。
- ストアアンドフォワードモード用:
 - キュー名

以下の表はセントラルルーティングルールの各フィールドを説明しています。

MRR フィールド	フォーマット	制約など
リクエスター DN	<i>SWIFTNet Naming and Addressing Guide</i> を参照してください。	このフィールドは特定の値、ワイルドカード、もしくはワイルドカードを伴った値を含むことができます。ルールはサブツリーに属する全てのリクエスターを受け入れ、特定の値から開始されます。 メモ: このフィールドには通常、ワイルドカードが含まれます。また通信のルーティングは通常、リクエスターの身元には依存しません。
リスポンダー DN	<i>SWIFTNet Naming and Addressing Guide</i> を参照してください。	このフィールドは特定の値、もしくはワイルドカードを伴った値を含むことができます。 ユーザーは、リスポンダー DN を所有する金融機関のプライマリ BIC が bic8 である場合、少なくとも2つのレベルを指定する (o=bic8, o=swift) 必要があります。リスポンダー DN 制約に関するより詳細な情報は、 <i>SWIFTNet Naming and Addressing Guide</i> を参照してください。
サービス名	<i>SWIFTNet Naming and Addressing Guide</i> を参照してください。	このフィールドにワイルドカードを含めることはできません。 SWIFTNet InterAct メッセージもしくはファイル送信リクエスト内のフィールドにあるサービス名と、

MRR フィールド	フォーマット	制約など
		MRR ルールのサービス名は正確に一致しなければなりません。
リクエストタイプ	<i>SWIFTNet Naming and Addressing Guide</i> を参照してください。	このフィールドは特定の値、ワイルドカード、もしくはワイルドカードを伴った値を含むことができません。
MRR ルールオーダー	0 ~ 999 までの整数です。	MRR ルールオーダーの値に従って、リクエスター DN、レスポナー DN、サービス名、リクエストタイプフィールドが一致している全ての MRR ルール一式の中から、最小値の MRR ルールが選択されます。 メモ：各レスポナー機関の MRR ルールは慎重に考慮する必要があります。これは、一致する MRR ルールはどのような状況においても、独自かつ最小値のメッセージ受領レジストリ (Message Reception Registry、MRR) ルールオーダー値を生成するからです。
第一 SNL ID	SNL ID です。フォーマットは以下のようになります： sn112345	リアルタイムモードでのみ使用されます。
第一 SNL エンドポイント	エンドポイントに要求されるフォーマットと値を決定するには、アプリケーションもしくはインターフェースの説明書を参照してください。 SWIFTAlliance Gateway にファイルルーティングさせるためにユーザーが使用しなければならないエンドポイントについては、 <i>SWIFTAlliance Gateway File Transfer Interface Guide</i> を参照してください。	リアルタイムモードでのみ使用されます。
第二 SNL ID	SNL ID です。フォーマットは以下のようになります： sn112345	リアルタイムモードでのみ使用されます。
第二 SNL エンドポイント	「第一 SNL エンドポイント」フィールドと同じフォーマットです。	リアルタイムモードでのみ使用されます。
第三 SNL ID	SNL ID です。フォーマットは以下のようになります： sn112345	リアルタイムモードでのみ使用されます。
第三 SNL エンドポイント	「第一 SNL エンドポイント」フィールドと同じフォーマットです。	リアルタイムモードでのみ使用されます。
第四 SNL ID	SNL ID です。フォーマットは以下のようになります： sn112345	リアルタイムモードでのみ使用されます。
第四 SNL エンドポイント	「第一 SNL エンドポイント」フィールドと同じフォーマットです。	リアルタイムモードでのみ使用されます。
現在アクティブなアドレス	SNL ID およびエンドポイント	リアルタイムモードでのみ使用されます。

MRR フィールド	フォーマット	制約など
キュー名	SWIFTNet Naming and Addressing Guide を参照してください。	ストアアンドフォワードモードでのみ使用されません。

ノート メッセージなどをルーティングする際、エンドポイント番号に基づいたアドレスに優先順位はありません。また SWIFT がルーティングするのは、現在アクティブなアドレス対してのみです。

3.6.2 ルーティングの行動様式

説明

Message Reception Registry (メッセージ受取レジストリ、MRR) は、SWIFTNet InterAct メッセージもしくはファイル送信リクエストのリクエストヘッダーに含まれるサービス名、リクエストタイプ、リクエスト、レスポンスなどの値を使用して動作します。

全ての SWIFTNet MRR ルールセットの中から、SWIFT は可能性のあるサービス名、リクエストタイプ、リクエスト、レスポンス基準に一致するルールを選択します。

この絞り込まれた MRR ルールセットの中から、SWIFT は起因する MRR ルールオーダーの値に従って最も低い番号のルールを選択します。

SWIFT がこのルールを SWIFTNet InterAct 用として評価する際、メッセージは以下のようにルーティングされます:

- リアルタイムモードでは、メッセージは特定の SNL にルーティングされ、その SNL 内で特定の SNL エンドポイントアドレスにルーティングされます。
- ストアアンドフォワードモードでは、メッセージは特定のキューにルーティングされます。

SWIFT がこのルールを SWIFTNet FileAct 用に評価する際、以下が実行されます:

- リアルタイムモードでは、ファイル送信リクエストは特定の SNL にルーティングされ、その SNL 内で特定の SNL エンドポイントアドレスにルーティングされます。
- ストアアンドフォワードモードでは、ファイル送信リクエストは特定のキューにルーティングされます。

3.6.3 複数のルーティングアドレスを使用する

概要

リアルタイムモードを使用しているサービスに関連する各ルーティング(MMR)ルールに対し、ユーザーは 1～4 つのエンドポイントアドレスを定義することができます。また、各ルールにはその 4 つのエンドポイントアドレスのうち現在メッセージなどのルーティングに使用されているのがどれかを示す、アクティブアドレスインジケータがあります。

これらのアドレスが何を示すかは、ユーザーが定義することができます。例えば、最初のアドレスはメインサイトを、2 番目のアドレスは災害用サイトを示すなどです。

3.6.4 別のエンドポイントアドレスに通信をルーティングする

概要

ユーザーは、取引先や SWIFT とは関係なく、通信のルーティングをルーティングルールで定義されている別のアドレスに変更することが可能です。

MMR アクティブアドレスの値を変更するには、**サイトマネージャー**（swift.rug インターナルサービスの）ロールが必要です。多くの場合、セキュリティオフィサー（SO）がロールベースアクセス管理（RBAC）ロールの権限を委任します。

権限委任者は、ビジネス証明書の保持者にリクエストに署名しそれを認証する権限を持つ**サイトマネージャー**ロールを付与します。

`swiftnet reroute` コマンドを発行するオペレーターは、RBAC で**サイトマネージャー**ロールを持っている必要があります。

手順

このコマンドは、SNL-C、SWIFTAlliance WebStation、SWIFTNet Portal で実行することができます。

MRR セカンダリフラグは以下のように変更することが可能です：

- SNL コマンド `swiftnet reroute` を、ユーザーが所持しているシステムにて実行する。このコマンドに関するより詳細な情報は、*SWIFTNet Admin Services: Operational Interface*（SNL Documentation Set に付属）を参照してください。
- SWIFTAlliance WebStation 機能を使用して変更する。SWIFTAlliance WebStation に関するより詳細な情報は、*SWIFTAlliance WebStation User Guide* を参照してください。
- SWIFTNet Portal の `Routing` 機能を使用する。SWIFTNet Portal に関するより詳細な情報は、*SWIFTNet Portal User Guide* を参照してください。

再ルーティング可能なルーティング

ユーザーは、以下を実行することができます：

- 現在アクティブとなっている特定のアドレスから、別のアドレスに通信を再ルーティングする
- 特定のアドレスに全ての通信を再ルーティングする（サービス名、リクエスター、リスポンダー DN、リクエストタイプの任意の組み合わせにより範囲を特定することができます）
- 現在アクティブな特定のアドレスから別のアドレスに通信を再ルーティングする（サービス名、リクエスター、リスポンダー DN、リクエストタイプの任意の組み合わせにより範囲を特定することができます）

ノート いずれのケースにおいても、使用されるアドレスは関係するルーティングルールにて使用可能となっている必要があります。

3.6.5 リクエストに一致する MRR ルールがない場合のルーティング行動様式

概要

マッチング処理に使用される MRR アルゴリズムは、いずれか 1 つの MRR ルールが一致するか一致するルールが 1 つもないか、というように処理します。

MRR ルールで一致するものがない場合、SWIFT はリクエスターにエラーメッセージを送信します。SWIFTNet InterAct メッセージもしくはファイル送信リクエストが不達となるのを防ぐため、多くのユーザーは少なくとも 1 つは一致する MRR ルールを準備して全てを「キャッチ」できるようにし、そうした不達リクエストがないようにしています。ユーザーは、これらのルールタイプをリクエスター DN、レスポンス DN、そしてリクエストタイプワイルドカードで定義することができます。

また、より特定の MRR ルールのほうがレスポンスの要求に対して適切にリクエストをルーティングできる場合に、この「全てをキャッチ」ルールが発動されないよう、非常に高いルールオーダー値を持つよう設定しておくことができます。

3.6.6 複数の MRR ルールが同ランクだった場合のルーティングの挙動

挙動

一致した全てのルールセットのうち、MRR ルールオーダーで同ランクのものが複数あった場合、最初に遭遇したルールが適用されます。これにより、やがてルーティングの挙動に一貫性がなくなってしまうことがあります。

レスポンス機関に適用する全ての MRR ルールセットを慎重に考慮することにより、一貫性のないルーティングの挙動になることを防ぐことができます。

3.6.7 MRR とストアアンドフォワードキュー

挙動

ストアアンドフォワードモードを使用している SWIFTNet InterAct もしくは SWIFTNet FileAct サービスに関連したルーティングルールに対し、ルーティングルールは SNL エンドポイントではなくキュー名を指定します。

4 SWIFTNet 技術環境

概要

本章は、SWIFTNet メッセージングサービスを提供する、SWIFTNet インフラストラクチャおよびセントラルシステムのコア部分について説明しています。

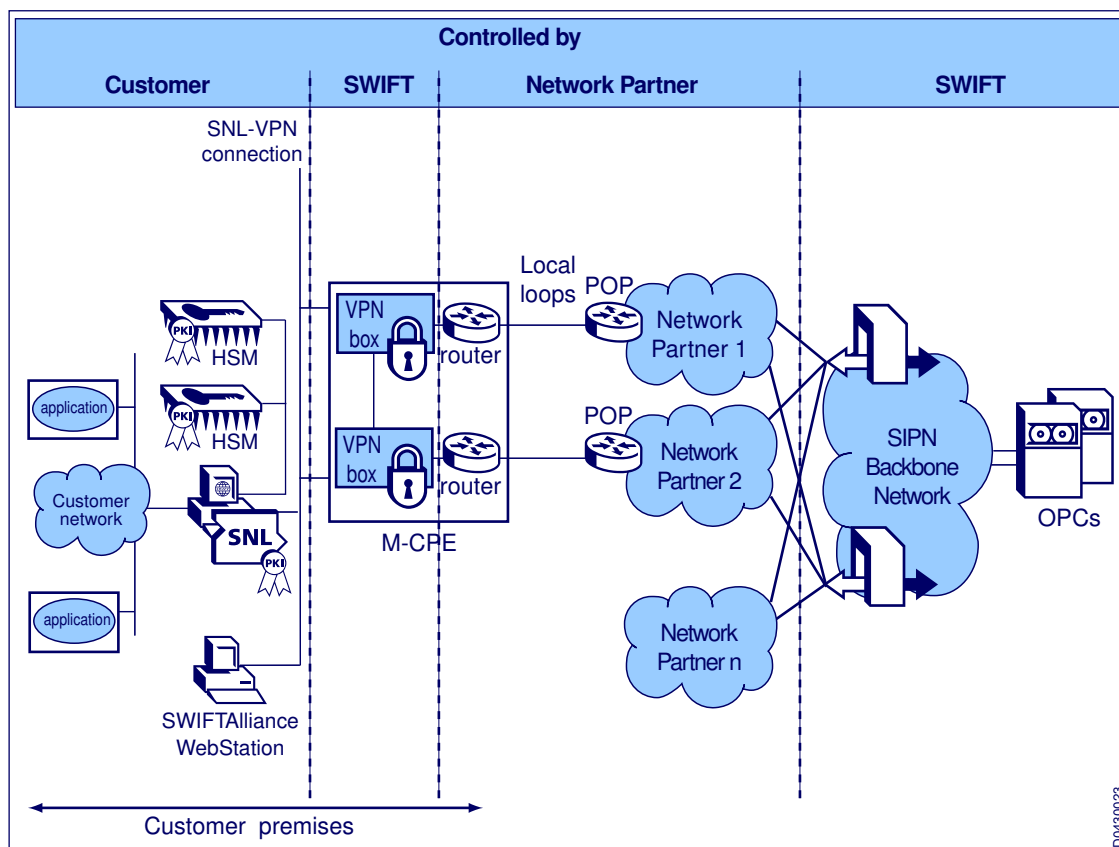
4.1 SWIFTNet インフラストラクチャとセントラルシステム

SWIFTNet インフラストラクチャに含まれるもの

SWIFTNet インフラストラクチャには以下のコンポーネントが含まれています：

- SWIFT オペレーティングセンター(OPC)から操作する SWIFTNet スイッチやフロントエンドプロセッサを含む、SWIFTNet セントラルシステム
- セキュア IP ネットワーク(SIPN)
- ユーザー拠点 (premises) に設置される SWIFTNet コンポーネント (Managed Customer Premises Equipment (M-CPE)、SWIFTNet Link(SNL)、ハードウェアセキュリティモジュール (HSM)ボックスなど)

下図は、SWIFTNet インフラストラクチャのコンポーネントを示しています。



D0630023

セントラルシステム

SWIFT のオペレーティングシステム(OPC)内で稼働している SWIFTNet セントラルシステムにより、多くの SWIFTNet メッセージング機能が提供されています。

SWIFTNet セントラルシステムの主要部分は以下の通りです:

- SWIFTNet スイッチ
- SWIFTNet PKI セキュリティシステム (証明書認証システムなど)
- SWIFTNet ディレクトリシステム
- データストレージ、管理サービス、システム管理、ネットワーク管理機能などのために使用されるシステム

SWIFT は、OPC の SWIFTNet システムを物理的に導入します。また、全ての SWIFTNet システムに対して完全なサイト冗長性 (代行機能) を提供します。

SWIFT は、SWIFTNet Integration TestBed (ITB)と本番環境の 2 つのオペレーティング環境を提供するため、SWIFTNet システムを論理的に構成します。

SWIFTNet ITB は、ソフトウェアの開発テスト用の SWIFTNet メッセージング環境を提供します。この環境は、本番環境で稼働しているライブビジネスサービスからは切り離されています。

4.2 SWIFTNet Integration Testbed

4.2.1 目的

説明

SWIFTNet Integration TestBed (ITB)は、ソフトウェアアプリケーションと SWIFTNet サービスの統合性をテストするために、市場インフラストラクチャ、サービスプロバイダー、アプリケーションベンダーなどが利用することができます。以下、本書ではアプリケーションベンダーをアプリケーションデベロッパーとします。ユーザーは、ITB をデベロッパーのテストに使用することができます。しかし本番環境での通信に使用することはできません。

通常、統合テストフェーズはユーザーが隔離された環境での一連のテストを完了させた後に行われます。これらのテストにはスタブライブラリーを使用します。統合テストフェーズに入る前に、SWIFTNet サービスおよびアプリケーション製品の両方が、品質と安定性において高いレベルに到達している必要があります。通常、このフェーズは一連のパイロットテストもしくはは正式受取テストの前に実施されます。

また ITB は、新規にリリースされた SWIFTNet サービスに対してソフトウェアアプリケーションやサービスをテストするために、アプリケーションデベロッパーが繰り返し使用することが可能です。

ノート SWIFTNet FIN の場合、デベロッパーテスト環境に関連する情報はベンダー別に提供されます。

ITB へのアクセス

ユーザーが ITB にアクセスする場合、ITB 専用の設定が必要となります。ユーザーは本番環境と同じ SIPN 接続を通じて ITB 環境にアクセスすることができますが、SNL、証明書、サービス名などの要素は ITB 特定 (専用) のものとなります。つまり、ITB 環境と本番環境で SNL や証明書などを共有することはできないということです。

4.2.2 ITB での SWIFTNet サービス

説明

SWIFTNet Integration Testbed (ITB) で使用可能な SWIFTNet メッセージングサービスは、SWIFTNet InterAct、SWIFTNet FileAct、SWIFTNet Browse です。ユーザーは、これらのサービスを SWIFT がサービスアドミニストレーターからの要求により ITB に導入したサービス、もしくは SWIFT が ITB に導入した SWIFT 管理サービスに関連するサービスにて使用することができます。

SWIFT が ITB に導入した SWIFTNet メッセージングサービスは、最新かつ十分に適格なリリースのものです。一般ルール、コンテンツ、頻度、可用性、そして SWIFTNet リリースのサポートに関するより詳細な情報は、*SWIFTNet Release Policy* を参照してください。

ITB で使用可能な SWIFTNet メッセージングサービスの機能は、SWIFT が本番環境に導入した（もしくは導入予定の）SWIFTNet メッセージングサービスのものと同様です。しかしながら、ITB のパフォーマンスおよび可用性の特徴などは本番環境のそれと異なります。ITB はパフォーマンステストや破壊試験用として設計されていないため、そのような目的での使用は想定されていません。

ITB には、専用の証明書認証が組み込まれています。この証明書認証はビジネス環境のものとは異なるため、メッセージがテストメッセージであることを常に証明することができます。また、SWIFT は ITB と本番環境を厳密に分離させているため、ユーザーはその 2 つの環境の間でメッセージをやりとりすることはできません。

SWIFT 一般サービス

SWIFT は、ITB でいくつかの一般サービスのテストができるようにしています。これにより、デベロッパーは市場インフラ管理もしくはメンバー管理ソリューションに登録することなく、SWIFTNet InterAct、SWIFTNet FileAct、SWIFTNet Browse を使用するアプリケーションのテストをすることが可能となっています。

• 汎用 SWIFTNet FileAct

このサービスは、ITB でテストしているデベロッパーのほか、パイロット（テストアンドトレーニング）オペレーション、そして本番環境でのライブオペレーションで使用することができます。サービス名や使用モードなどに関するより詳細な情報は、“汎用メッセージングソリューション” ページの 19 を参照してください。

• 汎用 SWIFTNet InterAct

ITB でテストしているデベロッパーのみが使用できるサービスです。リアルタイムモード、ストアアンドフォワードモードの両方で使用することができます（下記参照）：

目的	モード	サービス名
デベロッパーテスト	ストアアンドフォワード	swift.generic.iastrx
	リアルタイム	swift.generic.ialx

• 汎用 SWIFTNet Browse

ITB でテストしているデベロッパーのみが使用できるサービスです（下記参照）：

目的	モード	サービス名
デベロッパーテスト	リアルタイム	swift.generic.br!x

- **SWIFTNet Copy で使用可能なサービス**

デベロッパーテストのため、SWIFT は SWIFTNet Copy 機能を含んだ構成のサービスをいくつか使用できるようにします。これにより、多様なコピーフローのテストが可能となります。より詳細な情報に関しては、SWIFT パートナーマネジメントにご連絡ください。

Allowable Downtime Windows (休止時間、ADW)

SWIFT は、SWIFTNet Integration Testbed (ITB) 環境の定期メンテナンスを毎週金曜日の 12:00 GMT から土曜日の 08:00 GMT に行います。この休止時間中、SWIFTNet ITB はずっと使用不可能になる場合と、断続的に使用不可能になる場合があります。いずれにしても、この休止時間により本番環境のネットワークが影響を受けることはありません。

ADW および業務継続ウィークエンドの詳細なスケジュールは、www.swift.com > Ordering & Support > Operational Status > ADW schedule に掲載されます。

4.2.3 可用性とパフォーマンス

説明

SWIFTNet Integration Testbed (ITB) 環境の可用性は本番環境より低く、SWIFT が新たな SWIFTNet リリースを ITB に導入した後の 4 週間ほどは特にその傾向が強くなります。

また、ITB 環境は災害などにより影響を受けた SWIFT オペレーティングセンターを復旧させるために用意されているものではないため、そのような状況での使用はできません。

ITB 環境は、本番環境のようなパフォーマンスレベルに対応するようには設計されていません。サービスやアプリケーションのパフォーマンステスト（スループットや経過時間など）を実行する際は、このことに留意してください。

4.2.4 サポート

説明

SWIFT は、24 時間営業のサポートサービスを年中無休でユーザーに提供しています。また、ITB ユーザーには「ベストエフォート（最善の努力）」ベースのサポートを提供しています。但し、問題や照会については、ITB 環境に関連するものより本番環境に関連するものが常に優先されます。

ITB ユーザーがユーザーサービス組織にアクセスする場合は、一般 SWIFT ユーザーが使用しているものと同様のチャンネルを使用します。

4.2.5 責任範囲

SWIFT の責任範囲

SWIFT の役割は、Integration TestBed (ITB) 基盤をユーザーに提供し、そのオペレーションとサポートを行うことに厳密に制限されています。ITB 環境の可用性、パフォーマンス、サポートに関してサービスレベルでの責任を負うものではありません。

アプリケーションデベロッパーの責任範囲

アプリケーションデベロッパーは、統合テストの仕様確定、作成、実行、管理について責任を負います。アプリケーションデベロッパーが特定の限定パフォーマンステストを実行したい場合、もしくは ITB の限定された継続期間に関して特別な要求がある場合などは、まずそのような要求を SWIFT がサポートできるかどうかを SWIFT と調整する必要があります。

4.3 SWIFTNet 本番環境

4.3.1 SWIFTNet 本番環境の役割

説明

SWIFTNet 本番環境の役割は、ユーザーが使用できるようにアプリケーションの完全導入をサポートすることです。サポートは、パイロット（テストアンドトレーニング）のフレームワークもしくはライブサービスのいずれかの中で行われます。本番環境は、Integration TestBed (ITB) 環境では提供されないレベルのサービス（可用性やサポートなど）を提供します。

一般ルール、コンテンツ、頻度、可用性、そして SWIFTNet リリースのサポートに関するより詳細な情報は、*SWIFTNet Release Policy* を参照してください。

Allowable Downtime Windows（休止時間、ADW）

SWIFT は、定期メンテナンスおよび業務継続テストを休止時間（Allowable Downtime Window、ADW）に計画します。このメンテナンス時間およびテスト時間は土曜日の 16:00 GMT に開始されます。メンテナンス時間中、SWIFTNet メッセージングサービス（SWIFTNet FIN、SWIFTNet InterAct、SWIFTNet FileAct、SWIFTNet Browse）は以下のように中断されます：

- **メンテナンス時間**

2 時間、8 時間、もしくは 12 時間かかるメンテナンス時間中、SWIFTNet メッセージングサービスにおいて接続の喪失、サービス中断などが発生する可能性があります。また例外的に長時間にわたるサービス中断が発生する場合があります。

- **業務継続テストおよび障害回復テスト**

12 時間かかるこれらのテスト時間中、SWIFTNet メッセージングサービスは断続的に使用不可能になります。休止時間中、サービス中断が延長される場合があります。

ADW および業務継続ウィークエンドの詳細なスケジュールは、www.swift.com > Ordering & Support > Operational Status > ADW schedule に掲載されます。

4.3.2 SWIFTNet システムの耐障害性

災害などが発生した場合に関する概要

SWIFTNet システムの耐障害性は、災害などにより SWIFT オペレーティングセンター(OPC)が影響を受けた際における迅速なサービス復旧を含めたりカバリーシナリオに基づいています。

SWIFTNet システムは、ヨーロッパ大陸およびアメリカの OPC にて稼働されています。SWIFT は、単一障害点を排除するよう OPC 環境を設計しています。各 OPC は、SWIFT の通常業務全体を運用できるように設計されているだけでなく、ローカルで完全な冗長性が実現されています。

OPC 間の全てのネットワークが、通信量全体をカバーできる経路が少なくとも 2 つ存在するように設計がなされています。

4.3.3 オペレーティング状況に異常がある場合

説明

本書に記載されているサービスレベルは、通常のオペレーティング状況であることを前提としています。これには、本番系および待機系 SWIFT オペレーティングセンター(OPC)における、単一コンポーネントによる障害シナリオでの回復オペレーションも含まれます。SWIFTNet は耐障害性に優れており、異常事態が発生した際もユーザーの業務に影響を与えることはありません。しかしながら、非常に稀なケース（SWIFT OPC がなんらかの災害により破壊された、冗長化された同コンポーネントの双方に障害が発生する、SWIFT OPC の切り替え時にコンポーネントに障害が発生するなど）においては、通常のサービスレベルを満たせない可能性があります。このような場合には、データ損失の可能性もあります。

4.4 SWIFTNet と FIN の間におけるブリッジ

FIN ブリッジ

SWIFTNet FIN をサポートするため、SWIFT は SWIFTNet セントラルシステムと FIN セントラルシステムの間ユーザーからは直接見えないテクニカルブリッジを設置しています。これにより、ユーザーは既存の FIN アプリケーションに変更を加えることなく、SWIFTNet 接続を通じて FIN を使用することが可能となります。

FIN ブリッジは、受信した FIN メッセージを SWIFTNet エンベロープに入れ、CBT に送信します。CBT は、FIN メッセージが SWIFTNet エンベロープから取得されていることを保証します。通常、CBT の中に含まれる SNL によって、PKI に基づく全てのセキュリティ機能が実行されます。

5 セキュア IP ネットワーク

概要

SWIFT セキュア IP ネットワーク(SIPN)は、SWIFTNet メッセージングサービスに接続するユーザー向けに、高度に安全かつ非常に信頼性のあるネットワーク接続サービスを提供します。ネットワークは、非常に高いレベルの相互運用性が実証されている技術、インターネットプロトコル(IP)をベースにしています。

本セクションは、マルチベンダー SIPN (MV-SIPN)モデルでの SIPN アクセス構成について説明しています。

接続パックの完全インストール

SWIFT が接続を稼働させる前に、ユーザーは全ての代替回線を含めた接続パック構成全体をインストールしておく必要があります。Dual-I 接続構成を選択した場合、ユーザーは両方の回線（一次専用回線と代替用のダイヤルアップ回線）をインストールし、両方の回線が使用可能であることを確認した時点でインストール完了と見なします。

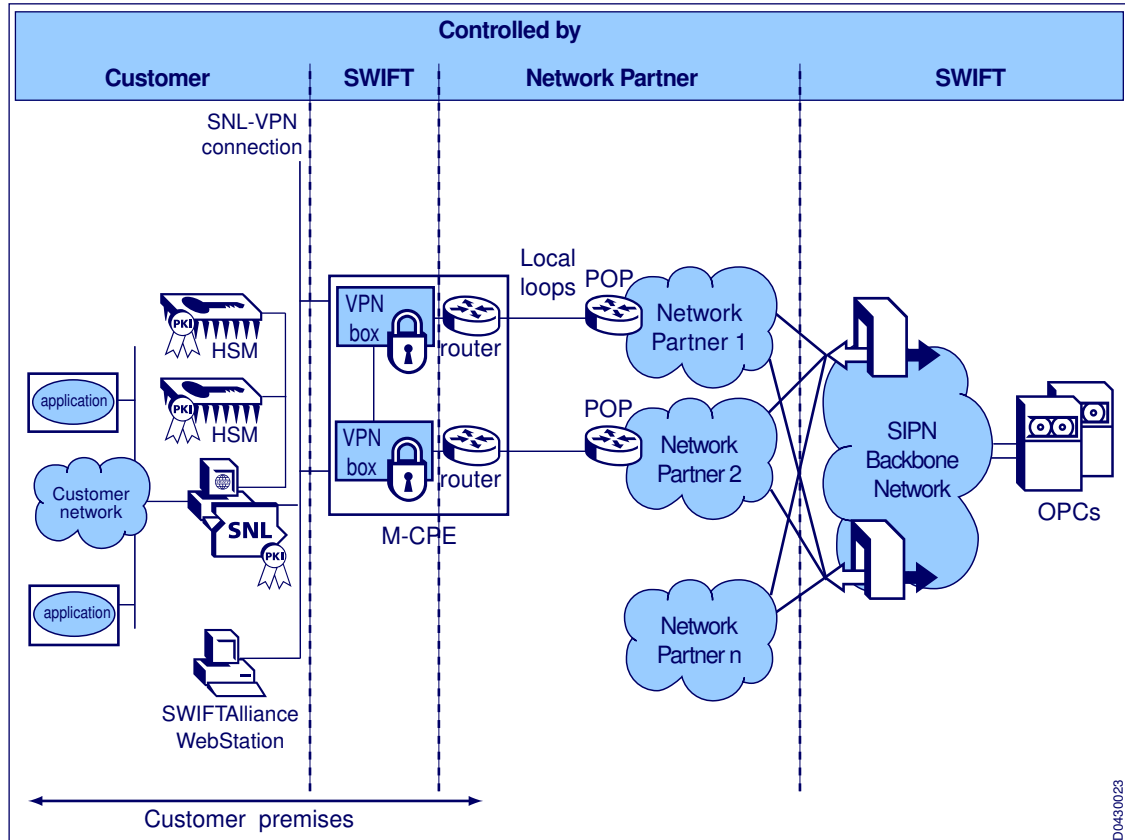
SWIFT では接続パックの部分的インストールを認めていません。接続パックに関するより詳細な情報は、*SWIFTNet Connectivity Packs* を参照してください。

5.1 セキュア IP ネットワークの概要

セキュア IP ネットワークとは

セキュア IP ネットワーク (SIPN) は、SWIFT が提供している安全かつ耐障害性の高い、グローバルなプライベートネットワークです。SIPN はインターネットプロトコル技術をベースにしており、SWIFTNet サービスおよび製品が必要とする強固な通信サービスを実現しています。

マルチベンダーアーキテクチャの概要



ユーザーは、Points-of-Presence (PoP、アクセスポイント) に接続して SIPN にアクセスします。PoP は SIPN への出入口となるノード（接続ポイント）で、世界各国に設置されています。

5.2 SIPN アクセス構成

概要

SWIFT は、SIPN (MV-SIPN) にマルチベンダーモデルを採用しています。MV-SIPN モデルは、ユーザーが SIPN に接続するための一連のソリューションを提供しています。

接続ポートフォリオは、機能の主要な 3 つの分野で定義されます：

• 接続タイプ

ユーザーは、ダイヤルアップ接続もしくは常時接続回線のいずれも使用することができます。SWIFT は、容易に加入できるダイヤルアップ回線のみでのソリューションを提供するこ

とができるほか、スピードと信頼性に優れた常時接続回線での構成を提供することもできます。

- **耐障害性**

SWIFT は、コンポーネントの冗長性を提供することで多様なレベルの耐障害性を実現しています。

- **スループット**

ユーザーの要件を満たすため、SWIFT はダイヤルアップの公衆交換電話網(PSTN)から 6Mb の専用回線まで、多様なアクセス速度に対応しています。

ダイヤルアップソリューション

ユーザーは、仮想プライベートネットワーク(VPN)ボックスおよびダイヤルアップモデムを使用して接続を構築することができます。SWIFT は PSTN 接続を推奨します。SWIFT の許可があれば、例外的な状況において総合デジタル通信網 (ISDN) で接続することもできます。予備機器があり、代替の SIPN Point-of-Presence (PoP) にダイヤルアップ接続する能力があれば、設備機器類や PoP に障害があった場合の代替とすることができます。

SWIFT によって管理され、高い耐障害性を持つ構成

SWIFT によって管理され、高い耐障害性を持つ構成は、常時接続回線、ルーター、一次接続として VPN ボックス、そして代替としてダイヤルアップもしくは専用回線（それぞれ Dual-I および Dual-P 管理の加入社宅内機器 [M-CPE] として知られています）から構成されています。これらのタイプの構成は、冗長性コンポーネントを構成する可能性を提供し、VPN ボックス、ルーター、PoP、回線などに障害が発生した際における代替への自動切換えを特長としています。

5.3 低通信量のダイヤルアクセス

5.3.1 低通信量のダイヤルアクセスに向いているユーザーとは

概要

公衆交換電話網(PSTN)を通じてのダイヤルアップ接続は、通信量が少ないユーザーに向いています。またダイヤルアップ接続は、一次通信リンクに障害があった場合の予備代替ソリューションとして有用です。

ユーザーは SWIFT 仮想プライベートネットワーク(VPN)ボックスおよびモデムを使用してダイヤルアップ接続を構築することができます。

ダイヤルアップの接続モードとして、PSTN がデフォルト/推奨モードです。SWIFT の許可があれば、例外的な状況において総合デジタル通信網 (ISDN) で接続することもできます。このような場合、ユーザーはモデムの代わりに適切なターミナルアダプタを VPN ボックスに接続する必要があります。

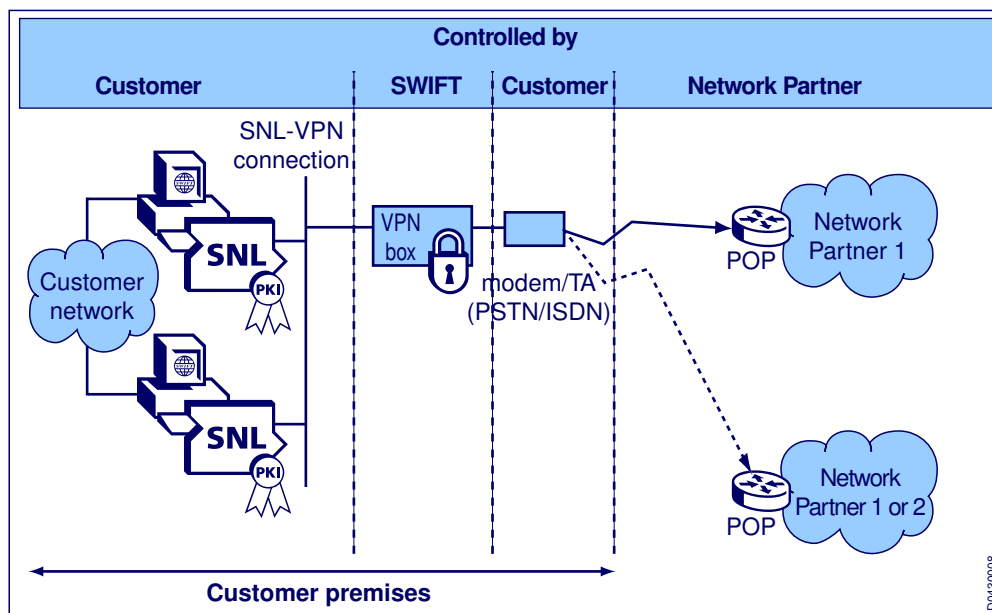
5.3.2 アクセス説明

コンポーネントの接続方法

VPN ボックスは、PSTN もしくは ISDN を経由して直接 SIPN Point-of-Presence (PoP) に接続しています。

ユーザーは、SWIFT が指定した再販業者に直接 VPN ボックスを注文しなければなりません。

標準ダイヤルアクセス



ユーザーは、SNL-VPN 接続を確実にしなければなりません（“ユーザーネットワーク構成” ページの 86 を参照してください）

機器類

標準オプション

特性	タイプ
VPN ボックス	Juniper Netscreen ボックス
PSTN 用	ローカル要件を満たすモデム
ISDN 用	ローカル要件を満たすターミナルアダプタ

5.3.3 初期不良が発生した後の復旧

ローカル PoP に初期不良が発生した後の復旧

ローカル PoP へのアクセスに障害が発生すると、SWIFT は代替システムとしてダイヤルアップアクセスを提供します。これを実現するため、SWIFT は VPN ボックスが代替 PoP に自動的にダイヤルアップするよう構成します。また可能であれば、SWIFT は複数のベンダーに分散されている PoP を選択し、少なくとも 1 つの番号は外国の PoP 用であるようにします。

5.4 SWIFT が管理する常時接続回線サービス

概要

SWIFT が管理する常時接続回線構成は、ユーザーがセキュア IP ネットワーク (SIPN) に接続するための完全なソリューションを提供します。SIPN は SWIFT に管理された、非常に安全かつ信頼性の高い、ワールドワイドに展開されている、仮想のプライベートインターネットプロトコル (IP) ネットワークです。SIPN は、IP およびその関連技術をベースにしています。SIPN は、SWIFTNet メッセージングサービスが必要とする安全かつ信頼性の高い通信サービスを提供します。

5.4.1 コンタクトポイント

SWIFTによる単一のコンタクトポイントの提供

接続のインストールが完了し、回線が使用可能であると SWIFT が判断すると、SWIFT はユーザー拠点（premises）における Managed-Customer Premises Equipment (M-CPE) から SIPN バックボーンへの接続状態を監視することに加え、一次回線サポートを提供する単一のコンタクトポイントを提供します。

初回注文時のサービスの接続は、ユーザーの責任となります。また、これらのサービスのインストールおよび保守に関しては、ユーザーおよび1つもしくは複数の SWIFT ネットワークパートナーの責任となります。

ユーザーの責任範囲に関するより詳細な情報は、“ロールと責任” ページの 123 を参照してください。

サービス品質保証契約

SWIFT は、ネットワーク接続サービスレベルをネットワークパートナー (NP) と一元的に交渉しています。これにより SWIFT は、コミュニティ全体のパワーを集約して交渉を有利にすることが可能となっています。

ノート サービス品質保証契約 (SLA) は、ISP 加入者回線接続オプションには適用されません。

SWIFT は、ネットワークパートナーと合意したサービスレベルが順守されているかどうかを監視します。適用可能なサービス品質保証契約(SLA)に関する詳細情報について知りたい場合、ユーザーは各接続に関する情報をネットワークパートナーに問い合わせることができます。

SLA について、ネットワークパートナーとユーザーは自由に直接交渉できます。しかしながら、そうした場合 SWIFT はユーザーの接続に適用されている SLA をネットワークパートナーが順守しているかどうかに関するフォローアップはできません。SLA に関する事柄は全て、ユーザーとネットワークパートナーの間で直接やりとりすることになります。従って、ネットワークパートナーと SLA を契約する際、ユーザーはそれが SIPN 接続のサービスレベルに関して全ての局面をカバーしていることを確実にしなければなりません。これにはモニタリングと契約履行も含まれます。

5.4.2 Managed-Customer Premises Equipment (加入社宅内機器)

接続性

Point-of-Presence (PoP) への常時接続回線およびオプションとしてダイアルアップの代替接続は、Managed-Customer Premises Equipment (加入社宅内機器、M-CPE) からネットワークに接続します。SWIFT は、ユーザーのネットワークである M-CPE、そして M-CPE から PoP への接続をユーザーの接続性および冗長性に関する選択に基づいて構成します。

ユーザーは、希望するアクセス構成を SWIFT に連絡しなくてはなりません。

接続性におけるその他のサービスについては、ユーザーが1社もしくは複数のネットワークパートナーに連絡して取り決めます。M-CPE の導入は、ユーザーの要件およびネットワークインフラによります。

5.4.3 接続構成

構成オプション

SWIFT は、以下のいずれかの接続オプションに基づいて、ユーザーのネットワークと M-CPE 間、そして最寄の PoP への接続を構成します。:

- **Dual-I**

Dual-I M-CPE は、アクティブ/待機構成された 2 つの VPN ボックスから構成されています。アクティブ VPN ボックスは、インターネットサービスプロバイダー加入者回線(ISP Local Loop) もしくはデジタル加入者回線(DSL)を通じ (DSL エントリー)、常時接続回線でルーターに接続されます。待機 VPN ボックスは、公衆交換電話網(PSTN)もしくは総合デジタル通信網(ISDN)のいずれかのダイヤルアップ接続を使用します。

- **専用線接続での Dual-I**

この Dual-I 接続には、ルーターを 1 つとアクティブ/待機構成された VPN ボックスが 2 つ必要です。一次仮想プライベートネットワーク(VPN)ボックスとルーターにより、一次接続が導入されます。このルーターは、ユーザーが選択したネットワークパートナーにおける最寄の PoP まで専用回線で接続されます。待機 VPN ボックスは、アクティブ VPN ボックスと同じ、もしくは異なるネットワークパートナーに属する異なる PoP に、PSTN もしくは ISDN (外部の ISDN ターミナルアダプタ) により接続されています。上限 4 つの接続まで可能ですが、少なくとも 1 つは異なる国への接続である必要があります。

- **ISP 加入者回線での Dual-I**

ISP 加入者回線での接続オプションは、ローカルのネットワークパートナーのほかに選択肢がないユーザー向けに、ローカルのインターネットサービスプロバイダー(ISP)のインフラを通じて SWIFT のセキュア IP ネットワーク(SIPN)にアクセスできるように設計されています。Dual-I アクセス構成でこのオプションを使用する場合、VPN ボックス、1 つもしくは複数のルーター、そしてインターネット専用線もしくは DSL 接続 (“接続構成” ページの 79 を参照) が必要となります。

- **DSL 接続での Dual-I**

Dual-I DSL エントリーと呼ばれるこの Dual-I 構成では、一次 VPN ボックスは DSL ルーターと (インターネットではない) DSL 回線を通じて最寄の PoP に接続されます。二次の待機 VPN ボックスはダイヤルアップ回線で接続されます。

- **複数回線接続での Single-P**

複数回線の構成は、ネットワーク障害から回復できない M-CPE を使用します。独自専用線を通じて SWIFT に接続する、独自 VPN ボックスから構成されています (“複数回線構成での Single-P” ページの 83 を参照してください)。

- **Dual-P**

Dual-P 接続では、アクティブ/待機構成されている 2 つの VPN ボックスおよびルーターが必要となります。各ルーターは専用線で接続されます。2 本の専用線はどちらも同じ容量を持ち、異なる PoP に接続されます。ユーザーは、両回線とも 1 社のネットワークパートナーのものを使用するか、耐障害性を高めるために 1 回線ずつ 2 社に分割するかを決定します (“Dual-P 構成” ページの 84 を参照してください)。

これらの構成オプションの耐障害性はそれぞれ異なります。また接続構成の可用性は、地理的な位置などによって様々です。

5.4.4 Dual-I 構成

常時接続回線および ISDN/PSTN 代替を持つ M-CPE

このタイプの Managed-Customer Premises Equipment (M-CPE)は、アクティブ/待機構成された2つのVPNボックスから構成されています（“専用線での Dual-I M-CPE” ページの 80 を参照）。アクティブVPNボックスは常時接続回線（専用線、ISP 加入者回線、DSL エントリー）され、待機VPNボックスはPSTN または ISDN ダイアルアップ接続されます。

SWIFTNet Link(SNL)のホストが M-CPE に接続します。複数のVPNボックス複数ののは同一場所に配置および相互接続され、1つのホストのように使用されます。

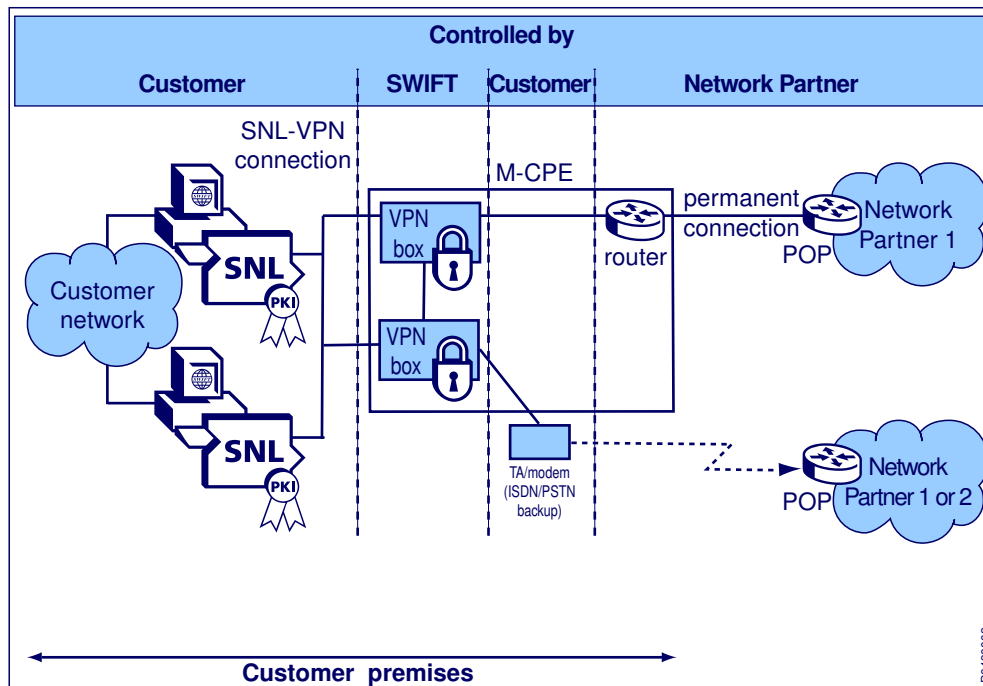
VPNボックスは、以下のように自動的に代替システムへの接続切り替え、もしくは復旧するよう構成されています：

- プライマリVPNボックスに障害が発生すると、代替のセカンダリVPNボックスに接続が切り替えられる
- プライマリVPNボックスの接続が復旧されると、セカンダリVPNボックスは待機状態に戻る

ISDNの代替回線は64 Kbpsです。最適な構成にするには、一次回線と代替回線の回線容量が同じである必要があります。構成に一次回線より低容量の代替回線が含まれている場合、ユーザーはそれを同じ容量のものに変更しなければなりません。

ノート 一次回線の容量が上限64 Kbpsである場合、Dual-I M-CPEの代替としてPSTNダイアルアップ回線を使用することができます。それ以外の場合、Dual-I M-CPEの代替として使用できるのはISDNのみです。

専用線での Dual-I M-CPE

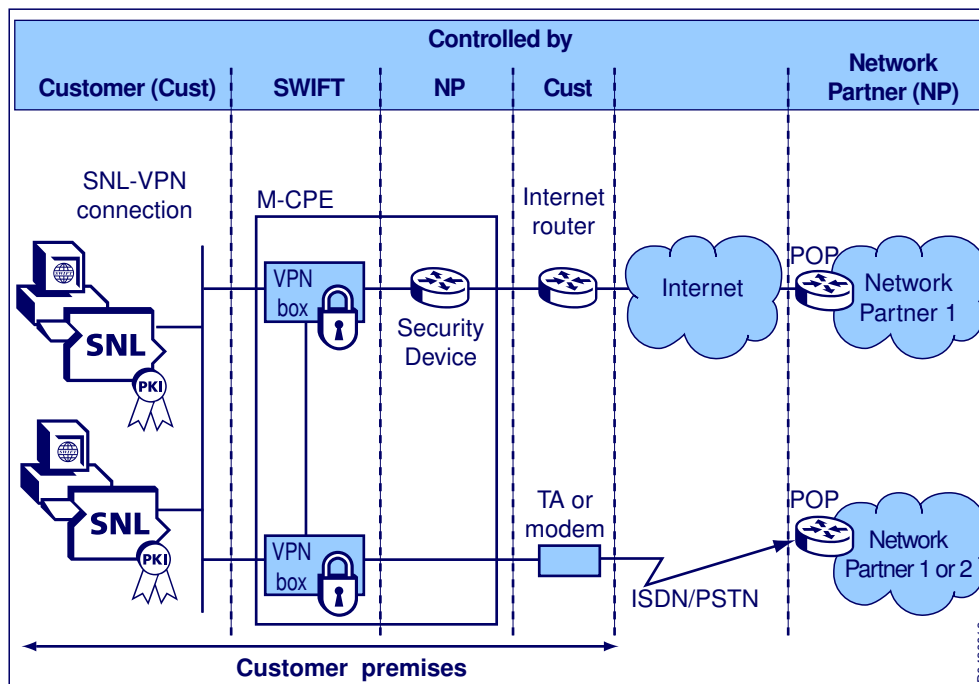


アクティブVPNボックスは、SWIFT 公認のネットワークパートナーの Points-of-Presence (PoP) に専用線で接続されるルーターに接続します。

ISP 加入者回線での Dual-I M-CPE

この特定の構成では、アクティブ VPN ボックスは、ISP への専用線でインターネットに接続もしくは ADSL モデムを通じて ISP に接続するネットワークパートナーの VPN およびファイアウォールに接続します。待機 VPN ボックスは、依然としてダイヤルアップ回線で接続されます。

ISP 加入者回線での Dual-I M-CPE

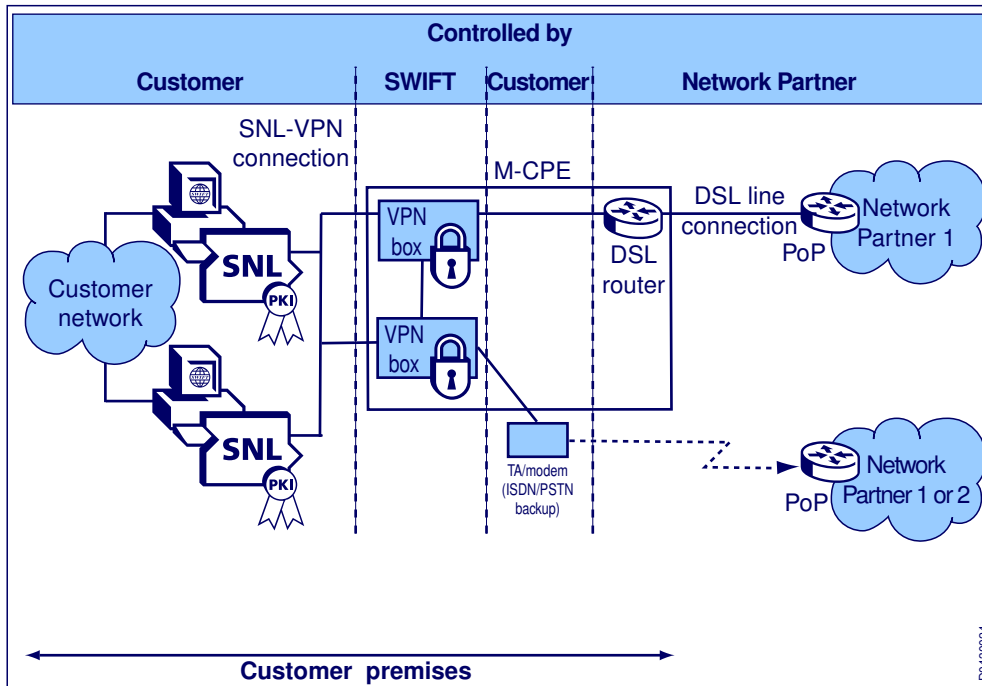


同一場所に置かれたデュアル構成の場合、通常 3 メートルの距離で設置された 2 つの VPN ボックスの間をデジタル加入者回線 (DSL) モデムで直接接続します。こうした場合、ケーブル配線はネットワークパートナーが提供します。

2 つの仮想プライベートネットワーク (VPN) ボックス間の距離として、SWIFT が許可するのは最大 100 メートルまでです。ユーザーが VPN ボックス間を 3 メートル以上あけて設置する場合、ケーブル配線はユーザーが提供する必要があります。また、接続の中にネットワーク機器 (リピーターなど) を導入してはいけません。

ユーザーは、両方のソリューションに対し SNL-VPN 接続を保証する必要があります (“ユーザーネットワーク構成” ページの 86 を参照してください)。

Dual-I DSL エントリー



一次 VPN ボックスは DSL ルーターに接続され、そこから DSL 回線で最寄の PoP に接続されています。待機している二次 VPN ボックスはダイヤルアップ回線で接続されており、一次接続に障害が発生した際は自動的にフェイルオーバー（障害迂回）を実行します。

設計特性

下記は、常時回線接続され、代替として ISDN もしくは PSTN 接続を持つ Dual-I M-CPE の設計特性です。

設計特性	タイプ
VPN ボックス	Juniper Netscreen ボックス
PSTN 用	宅内要件を満たすモデム
ISDN 用	宅内要件を満たすターミナルアダプタ
ルーター	ネットワークパートナーが決定

耐障害性

- 自動保護**

障害から VPN ボックス、常時回線（ルーターを含む）、そして Point-of-Presence (PoP)を保護します。
- 自動復旧**

一次 VPN、ルーター、回線に障害が発生すると、二次 VPN ボックスは認証されたユーザーの通信がある場合に ISDN もしくは PSTN 代替を実行します。

ノート 一回線の容量が上限 64 Kbps である場合、Dual-I M-CPE の代替として PSTN ダイヤルアップ回線を使用することができます。それ以外の場合、Dual-I M-CPE の代替として使用できるのは ISDN のみです。

5.4.5 複数回線構成での Single-P

概要

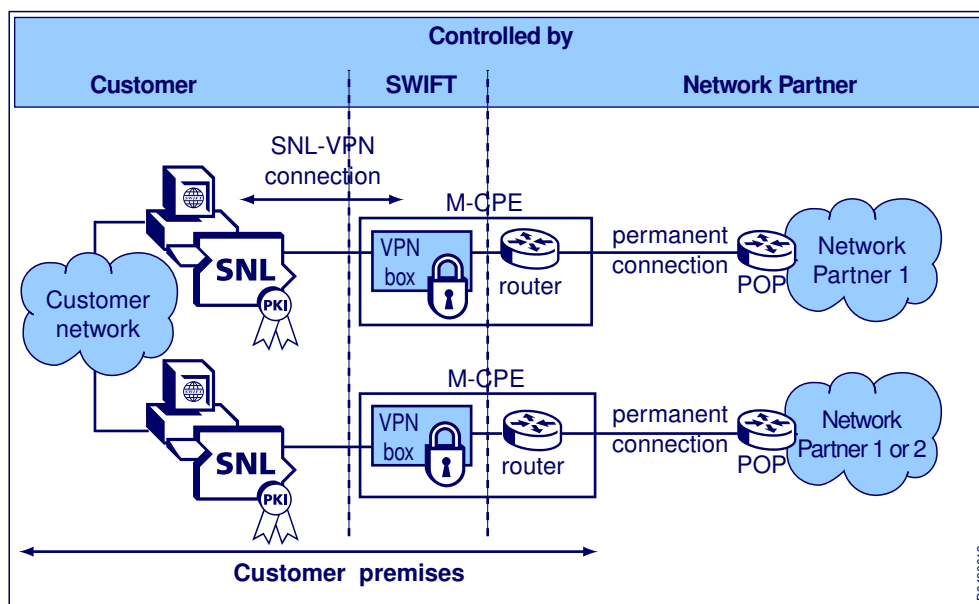
複数回線構成は、ネットワーク障害から復旧できない Managed Customer Premises Equipment (M-CPE)を使用します。Single-P は、仮想プライベートネットワーク(VPN)ボックス、ルーター、そして Point-of-Presence (PoP)に接続する専用線から構成されています。Single-P で障害が発生した場合、それを使用している SWIFTNet Link(SNL)は SWIFT に通信できなくなるため、ユーザーは別の M-CPE に接続している別の SSWIFTNet Link(SNL)を使用しなくてはなりません（ユーザーが SNL 代替ルーティングオプションを使用していない場合）。代替ルーティングに関するより詳細な情報は、*SWIFTNet Connectivity Packs* を参照してください。

接続障害に対応するため、ユーザーは適切なフェイルオーバーの環境を構築する必要があります。

切り替えは手動もしくは自動（複数の集合体の場合）のどちらも可能です。

ノート Single-P が適しているのは、複数回線構成をするユーザーのみです。

複数回線の M-CPE



ユーザーは、SNL-VPN 接続を確実にしなければなりません（“ユーザーネットワーク構成” ページの 86 を参照してください）

マルチライン構成の使用

本番環境サイトと障害発生時専用サイトを運用している金融機関は、アプリケーションの通信をその両者間で切り替えることができます。この場合、障害発生時専用サイトを常時待機状態にしておくことも可能なほか、その他の通信用（テスト通信など）に使用することも可能です。

接続サイトを 1 つ以上運用していて SWIFTNet への窓口が 1 つ以上ある金融機関は、十分な回線容量を準備していて、アプリケーション通信をサイト間で切り替えられる場合に限り、その他のサイトに対する代替の役割を果たすことができます。

複数回線構成の利点

複数回線接続のうち、2 つの部分（いずれもアプリケーションと Single-P ネットワークアクセスにより構成）は、リモートにすることができます。2 つの Single-P は互いに依存していない

ため、相互接続されている必要がありません。従って、複数回線は2つのサイト間で迅速な切り替えを必要とするユーザーに適しています。

2つの回線は同時に使用することができます。2つの Single-P はそれぞれ独立しているため、Dual-I や Dual-P 構成のように一次回線/代替回線が存在しません。当然、ユーザーは重要な通信が全て1本の回線でまかなえるように回線容量を準備しておく必要があります（もう1本の回線で障害が発生した時のため）。

複数回線構成の不利点

ネットワークに障害が発生した際は、アプリケーションを切り替える必要があります。これは Dual-P がアプリケーションの切り替えを意識させることなく接続性を復旧してくれるのと比較すると、少し不便です。

複数回線構成は、回線の1つに障害があった場合は復旧可能ですが、2つともに障害があった場合は復旧できません。プライマリサイトで Dual-P を使用し、代替サイトも持っている構成と比較すると、複数回線構成は無防備だと言えます。

これらの折衷案として、プライマリサイトで Dual-P を使用し、障害発生時サイトで Single-P を使用することが考えられます。しかしながら、その場合はプライマリサイトの Dual-P が復旧している間に障害発生時サイトに切り替わらないよう、切り替え手順を慎重に設計する必要があります。

ノート なお、複数回線構成は Single-P と Dual-P SIPN アクセスモードでの組み合わせのみ可能であることに注意してください。

設計特性

以下は、常時接続回線を持つ Single-P の設計特性です。Single-P が適しているのは、複数回線構成をするユーザーのみです。

設計特性	タイプ
VPN ボックス	Juniper Netscreen ボックス
ルーター	ネットワークパートナーが決定

耐障害性

• 自動保護

複数回線構成は、ネットワーク障害から復旧できない Managed Customer Premises Equipment (M-CPE)を使用します。ネットワーク障害が発生した際は、アプリケーション切り替えが必要となります。

• 自動復旧

ユーザーは、VPN ボックスに障害が発生した際にルーター、回線、アプリケーションが代替の複数回線パスに切り替わるよう、自動復旧が構成されていることを確実にしなければなりません。

5.4.6 Dual-P 構成

常時接続回線と常時代替を持つ M-CPE

この M-CPE は、アクティブ/待機構成され、いずれもルーターと専用線での接続を持つ2つの VPN ボックスから構成されています（“Dual-P M-CPE” ページの 85 を参照してください）。

SWIFTNet Link(SNL)のホストは M-CPE に接続します。VPN ボックス（複数の）は同一場所に配置および相互接続され、1つのホストのように使用されます。

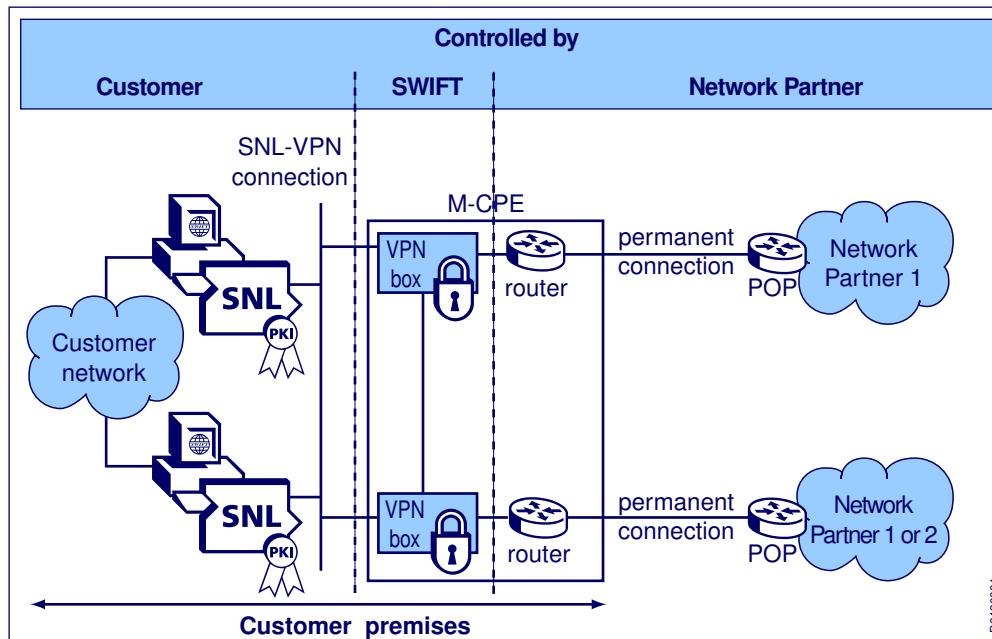
VPN ボックスは、以下のように自動的に代替システムへの接続切り替えおよび復旧するよう構成されています:

- プライマリ VPN ボックスに障害が発生すると、代替のセカンダリ VPN ボックスに接続が切り替えられます
- プライマリ VPN ボックスの接続が復旧される。すると、セカンダリ VPN ボックスは待機状態に戻ります

全てのネットワークコンポーネント (VPN ボックスも含め) は、ユーザーエリアにて復旧することが可能です。回線もしくは VPN ボックスに障害が発生した場合は代替回線が使用され、ルーティングプロトコルは障害が発生した VPN ボックスを迂回して再ルーティングします。同一の場所に設置されたデュアル構成の場合、通常 3 メートルの距離で設置された 2 つの VPN ボックスの間を直接接続します。この場合、ネットワークパートナーがケーブル配線を提供します。

2 つの仮想プライベートネットワーク (VPN) ボックス間の距離として、SWIFT が許可するのは最大 100 メートルまでです。ユーザーが VPN ボックス間を 3 メートル以上あけて設置する場合、ケーブル配線はユーザーが提供する必要があります。また、接続の中にネットワーク機器 (リピーターなど) を導入してはいけません。

Dual-P M-CPE



ユーザーは、SNL-VPN 接続を確実にしなければなりません (“ユーザーネットワーク構成” ページの 86 を参照してください)

設計特性

下記は、常時回線接続および代替常時回線を持つ Dual-P M-CPE の設計特性です。

設計特性	タイプ
VPN ボックス	Juniper Netscreen ボックス
ルーター	ネットワークパートナーが決定

耐障害性

- **自動保護**

常時回線、Point-of-Presence (PoP)全体、一次 VPN ボックス、ルーターは単一障害点に対して保護されています。通常の状態では、通信は全てアクティブリンクを経由していき、待機リンクは非アクティブのままとなります。

- **自動復旧**

前記のテーブルに記載された要素に障害が発生すると、二次 VPN ボックスは一次 VPN ボックスを経由した通信は不可能であると認識し、待機常時回線とルーターに通信を再ルーティングします。

ノート SWIFT は、全てのサイトに対して 1 つの Dual-P にある 2 回線を 2 つの異なるネットワークパートナーに分けた構成を推奨しています。この構成は、全てのサイトに最大限の耐障害性を提供します。接続の片方が失われることが、SNL およびアプリケーションに対して透過的になります。

5.5 ユーザーネットワーク構成

安全なメッセージ送受信

SWIFTNet の設計上、ユーザーのアクセス構成と SWIFT 間におけるメッセージ送受信の安全性および信頼性は、マルチベンダーセキュア IP ネットワーク(MV-SIPN)に依存しています。

セキュリティリスクを最小限にするため、ユーザーは SWIFTNet 関連の通信とそれをサポートするインフラ（ユーザーの責任範囲にあるもの）の両方を保護する必要があります。ユーザーの責任となるのは、ネットワークのうち SWIFTNet Link(SNL)ホストと VPN ボックス間（SNL-VPN 接続）の通信部分です。

複数の SNL ホストがある場合、ユーザーはそのセグメントも保護しなければなりません。

SNL-VPN 接続の保護

ユーザーは、SWIFT のサービスおよび製品の不正使用から SNL-VPN 接続を保護すると共に、これらのサービスおよび製品の整合性や信頼性を損なう可能性があるセキュリティ違反行為から保護する必要があります。

SNL-VPN 接続の安全性を確保するため、ユーザーは以下を特に実行しなければなりません：

- SNL ホストと VPN ボックス間の通信を、盗聴パケットから保護
- SNL ホスト環境を、不正アクセスから物理的に保護
- SNL ホスト環境を、ネットワークを通じた不正アクセスから保護
- VPN ボックスへの、不正な通信の侵入を防止

外部ネットワークへの接続

SNL ホストをホストしているユーザーネットワークが SIPN 以外の外部ネットワーク（インターネットやその他の公衆通信回線など）に接続している場合、ユーザーは SNL-VPN 接続を保護するために何らかの保護対策を取る必要があります。こうした対策には、適切に構成されたデバイス（ファイアーウォールなど）の導入が必要です。

ユーザーは、SNL ホストと VPN ボックスの接続において、直接ユーザーの物理的管理下でない接続を選択することができます。

ユーザーが同一の場所に設置しない構成を選択した場合、非コロケーションの必須構成要件を遵守しなければなりません。つまり、ユーザーは SWIFTAlliance Gateway 製品もしくは専用の安全なネットワークリンクのどちらを使用するか選択できるということです。SWIFT は他の構成を許可していません。

ユーザーのファイヤーウォールは、*SWIFTNet Network Configuration Tables Guide* に記載されている要件を満たす必要があります。それを満たしている場合、ユーザーは SWIFTNet 6.0 と互換性のある SWIFTNet Link、SWIFTAlliance WebStation、SWIFTAlliance Gateway のリリースを導入することが可能となります。SWIFTNet Network Configuration Tables Guide にあるアドレス情報は機密情報です。ユーザーはその機密性を保持しなければなりません。

ユーザーによる SNL-VPN 接続の保護をサポートするために、SWIFT が定義した必須構成要件に関するより詳細な情報は、*SWIFTNet Network Access Control Guide* を参照してください。

いずれの場合でも、ユーザーはセキュリティ問題に積極的に取り組まなくてはなりません。

6 SWIFTNet 公開鍵基盤(PKI)

6.1 概要

はじめに

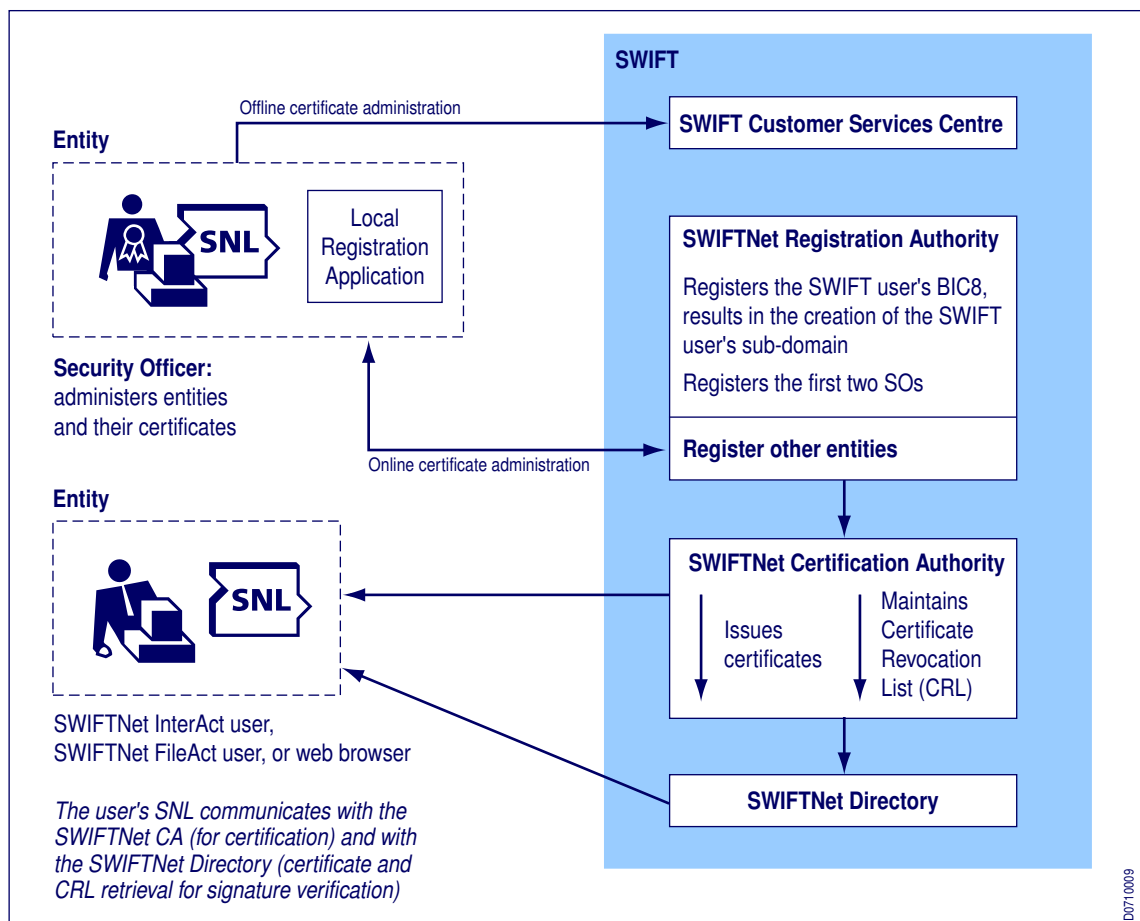
SWIFTNet サービス内における安全なメッセージ送受信を提供するため、SWIFT は SWIFTNet 用に公開鍵基盤 (PKI) を定義および導入しています (以下、SWIFTNet PKI)。

SWIFTNet PKI は、SWIFT が定義および導入した標準、製品、サービスと、それら標準、製品、サービスおよびそれらの間における関係を管理するために SWIFT が承認したポリシーの総称です。

6.1.1 コンポーネント

SWIFTNet PKI コンポーネントの概要

下図は、SWIFTNet PKI コンポーネントの概要を示しています。



SWIFTNet PKI には以下のコンポーネントが含まれます:

- SWIFTNet Certification Authority (SWIFTNet CA) — 証明書認証
- SWIFTNet Registration Authority (SWIFTNet RA) — 登録機関

- SWIFTNet PKI Directory (SWIFTNet Directory) – ディレクトリ

SWIFTNet PKI を使用するユーザーのエンティティは以下の通りです:

- セキュリティオフィサー (SO)
- SWIFTNet RA が、SWIFTNet PKI およびそのサブドメイン内で登録および認証したエンティティ

SWIFTNet CA は、SWIFTNet RA および様々なユーザーの SO が登録したエンティティに対して証明書を作成します。

SWIFTNet RA は、新規登録を行うハイレベルの登録機関です。

SWIFTNet RA は以下を行います:

- ユーザーの SO 登録
- SWIFTNet PKI 内にユーザーのサブドメインを作成し、それらをユーザーの SO の管理下に置く
- 必要に応じ、サブドメインを無効または削除する

Local Registration Application (LRA)は、エンティティ用の証明書を SO がオンラインで管理できるようにします。

SWIFTNet Directory は、エンティティ、SWIFTNet PKI 証明書、SWIFTNet CA Certificate Revocation Lists (証明書破棄リスト) を発行します。

SO は、SWIFTNet PKI のユーザー特定サブドメイン内のエンティティや証明書を管理します。

エンティティには、SWIFTNet RA および SO が登録した全てのエンティティが含まれます。エンティティは、SO を含め、秘密鍵を所有し使用できると考えられる全てのものが該当します。

SWIFTNet PKI の使用には、以下の前提条件が適用されます:

- ユーザーは、SWIFTNet 本番環境において秘密鍵と証明書の両方を使用していることを確認すること
- ユーザーは、証明書が有効であることを確認すること
- ユーザーは、証明書が用途に適していることを確認すること

6.1.2 証明書管理

オンライン管理

SWIFT は、証明書のオンライン管理方法として以下を提供しています:

- **すぐに使用可能なクライアントアプリケーション**

Local Registration Application (LRA、ローカル登録アプリケーション)は、SWIFTAlliance WebStation に組み込まれており、SO が使用することが想定されています。

- **Application Programming Interface (API) アプリケーションプログラミングインターフェース**

SWIFTNet Link Developers Toolkit は、これを Local Registration Application API として指定します。サードパーティのベンダーはこの API を使用し、SO が使用するオンライン LRA を構築します。

LRA 機能

SO は、LRA を使用して自身の証明書および他のエンティティの証明書を管理します。認証されたエンティティが SO の権限内にある限り、SO はその証明書を管理することができます。

オンライン LRA により、セキュリティオフィサー(SO)は以下を行うことができます:

- エンティティを含めた SWIFTNet Directory 内にノードを作成
- 証明書の発行の開始
- 証明書を破棄してエンティティの回復を開始
- エンティティおよび証明書の無効化

LRA に関するより詳細な情報は、*SWIFTNet Certificate Administration Guide* を参照してください。

証明書管理リクエストの処理

Local Registration Application (LRA) クライアントアプリケーションは、オンラインの証明書管理リクエストを処理するため、LRA サーバーに接続します。LRA サーバーは、Certification Authority (CA、証明書認証)および SWIFTNet Directory に接続されています。LRA は、SWIFT のセントラル LRA サーバーとの通信に SWIFTNet InterAct を使用します。

6.1.3 キーとパスワードの管理

SWIFTNet InterAct および SWIFTNet FileAct 用の鍵管理アプリケーション (Key Management Application)

SWIFTNet InterAct と SWIFTNet FileAct が通信する場合、その背景で SWIFTNet Link (SNL) はエージェントに鍵管理アプリケーション (KMA) を提供します。エージェントは以下のタスクを行うために KMA を使用します:

- 公開鍵および秘密鍵の生成
- パスワードによる鍵へのアクセス管理
- パスワードの変更
- HSM および SNL のハードディスクにある証明書のリストアップ

ウェブ証明書の管理

SWIFTNet Browse が通信する場合には、標準的なブラウザはウェブ証明書にパスワードと鍵管理を提供します。ブラウザはパスワードを必要としませんが、SWIFT はウェブ証明書とキーを保護するためにパスワードを使用することを強く推奨します。

ウェブサーバー

SWIFTNet Browse によりサポートされているウェブサーバーは、秘密鍵/公開鍵ペアおよび証明書署名リクエスト (Certificate Signing Request、CSR) を生成するツールをそれぞれ持っています。ユーザーは標準ブラウザで Entrust Authority Enrolment Server for Web に接続し、CSR を提出して証明書を取得します。その後、証明書はウェブサーバーにインストールされます。

6.1.4 暗号化機能

SWIFTNet Link セキュリティ機能

SWIFT 製/サードパーティ製に関わらず、全ての SWIFTNet インターフェースは SWIFTNet Link (SNL)と相互運用することができます。

エンドツーエンドセキュリティをサポートするため、SNL は SWIFTNet InterAct および SWIFTNet FileAct に以下の暗号化機能を提供します：

- **署名**：SNL を通じ、送信者は SWIFTNet InterAct および SWIFTNet FileAct メッセージに署名するために秘密署名鍵を使用することができます。これにより承認、整合性、発信元の否認防止が実現されます。
- **署名の検証**：SNL を通じ、受信者はメッセージの整合性と信頼性を検証するために通信先の公開検証キーを使用することができます。
- **暗号化**：SNL を通じ、送信者は機密性を確保するために通信先の公開暗号化キーを使用して SWIFTNet InterAct メッセージを暗号化することができます。
- **復号化**：SNL を通じ、受信者は秘密復号化キーを使用して SWIFTNet InterAct メッセージを復号化することができます。

取引先の認証

SNL を通じ、受信者は署名されたメッセージの署名者識別名 (DN) が証明書のエンティティ DN と対応していることを検証することができます。

証明書の検証

取引先の SWIFTNet InterAct および SWIFTNet FileAct 証明書の信頼性を確認するため、ユーザーはその証明書が有効であることを検証しなければなりません。ユーザーは SNL を使用して以下の証明書情報を確認することができます：

- 証明書の期限日
- 証明書の目的 (署名、暗号化など)
- 技術環境 (SWIFTNet InterAct、SWIFTNet FileAct、ウェブ証明書など)
- 証明書の破棄ステータス。ユーザーはこれを証明書破棄リスト (CRL) で確認することができます。
- 証明書の信頼性。ユーザーは SWIFTNet 証明書認証 (Certification Authority、CA) 署名を検証することができます。

6.2 ロール

6.2.1 ユーザー ロール

6.2.1.1 エンティティ

説明

エンティティは、証明書のテクニカルユーザーです。SWIFTNet Directory 内にある出口ノード (end-node) は識別名 (DN) で識別され、証明書を保持している、もしくは証明書を保持する予定となっています。

エンティティの証明書は、SWIFTNet InterAct もしくは SWIFTNet FileAct 内において、ユーザーの判断により以下のいずれかの代理となることができます:

- 名前を特定した個人
- 匿名の個人 (ユーザーやセキュリティオフィサー[SO]など)
- アプリケーション、またはシステム

エンティティの証明書は、SWIFTNet Browse 内において、ユーザーの判断により以下のいずれかの代理となることができます:

- ブラウザ
- HTTP サーバー

SO の身元

SWIFT はエンティティを DN で識別します。DN には、SWIFT ユーザーの BIC8 が含まれています。エンティティが証明書を持っている場合、DN は証明書に含まれています。

基本的に、取引先にとって DN は BIC8 を含んでいるということ以外、無意味です。しかしながら、SWIFTNet にあるビジネスサービスのサービスアドミニストレーターは証明された DN を義務付けることができます。

証明された DN を義務付けたサービスアドミニストレーターは、それを適切なガイドラインにてサービス登録者に通知する必要があります。

エンティティの識別に関するより詳細な情報は、*SWIFTNet Naming and Addressing Guide* を参照してください。

種類

SWIFTNet InterAct と SWIFTNet FileAct メッセージおよびファイルにおいて、エンティティは署名者 DN、暗号化 DN、承認者 DN の形で存在することができます。

承認されたアクティビティ

エンティティもしくはその代理は以下のことを行います:

- 秘密鍵のパスワード付与
- メッセージの署名および暗号化
- 署名の検証およびメッセージの復号化

6.2.1.2 代理人

定義

エンティティの代理人は、ユーザー（登録企業）の社員もしくは役員、またはサービスビューローの社員もしくは役員で、個人のものではないエンティティの証明書と秘密鍵の管理を行います。信頼の連鎖を保持するにあたり、代理人の役割は非常に重要です。

承認されたアクティビティ

代理人は以下のことを行います：

- 秘密鍵の生成および証明書の取得
- パスワードの保護および変更
- サインオン/サインオフを単独では実行できないアプリケーションの代わりにそれを実行
- 秘密鍵の保護
- 秘密鍵およびパスワードの漏洩（疑いがある場合も含め）や紛失が発生した際に、SO に通知

自動的に任命

以下の場合には、代理人が自動的に任命されます：

- エンティティの識別名(DN)に関連する有効化シークレットを受け取ると、エンティティの代理人となります（後に、SO がエンティティの証明にその有効化シークレットを使用するかどうかに関わらず）
- 代理人に、エンティティの証明書に関連するパスワードもしくは秘密鍵を渡された人は、SO がそのエンティティ用に任命したその他の代理人と共に共同の代理人となります（共有証明書）

非人称エンティティ

エンティティが以下の物である場合、代理人は人間となります：

- ソフトウェア
- ハードウェア
- 組織単位
- サービス

6.2.1.3 Security Officer （セキュリティオフィサー）

定義

セキュリティオフィサー(SO)は、ユーザーの証明書の管理に対して責任を持ちます。SWIFT が登録した SO は、セキュリティに関連する全てのことについて SWIFT との窓口となります。

登録されたセキュリティオフィサーがその役割を中止する場合、ユーザーは可能な限り早い段階でその旨を SWIFT に通知し、当該セキュリティオフィサーを契約終了とする、もしくは代替する必要があります。

信頼の連鎖を保持するため、SWIFT は証明書ステータス、SWIFTNet Directory における権限範囲、ロールプロフィールを検証し、承認された SO のみが証明書管理リクエストを SWIFT に発行できるようにします。

オンラインおよびオフライン機能

オンライン機能を持っている SO は、ローカル登録アプリケーション (Local Registration Application、LRA) を使用し、SWIFTNet を通じて証明書を管理します。これを行うには、SO は有効な証明書および *CertificateAdministration* RBAC ロールを保持してはなりません。

LRA 機能を使用できない場合、オフライン機能を持っている SO は SWIFT セキュアチャネル (www.swift.com > Ordering & Support > Support > Secure Channel) を通じて SWIFT にオフライン介入依頼を提出することにより証明書を管理することができます。この場合、SO はセキュアチャネルにアクセス権がある swift.com アカウントを持っている必要があり、認証には個人のセキュアコードカードを使用します。SO がまだ SWIFT セキュアチャネルにアクセス可能ではない場合、電話、ファックス、メールで SWIFT カスタマーサービスセンター (CSC) に連絡することによりオフライン介入を提出することができます。オフライン SO は、RBAC のオフライン介入を依頼することはできません。

4eyes 承認

SO による未承認のアクションや不正行為に対するユーザー保護を強化するため、SWIFT は証明書管理およびロール管理における 4eyes ロールプロファイル (4eyes role profiles) をオプションで提供しています。

ユーザーがこのオプションを有効にしている場合、2 人のセキュリティオフィサー (SO) がオンラインリクエストを提出しなければなりません。SWIFT は、*CertificateAdministration4eyes* ロールまたは *Delegator4eyes* ロール (もしくはその両方) を各 SO に付与することでこれを実現します。SWIFT は、ユーザーが 4eyes 承認を適用した場合、追加 SO も定義してオペレーションレベルに一貫性を持たせることを推奨します。

SWIFT は、SO で *CertificateAdministration* および *Delegator* (権限委任者) ロールの両方を持っている場合、RBAC ロールの *CertificateAdministration4eyes* そして *Delegator4eyes* を組み合わせて自身に付与することを推奨します。4eyes 承認の導入に関するより詳細な情報は、*SWIFTNet Certificate Administration Guide* を参照してください。

権限範囲

SWIFTNet Directory 内で SO が管理できる範囲として SWIFT が許可しているエリアを、*権限範囲* (scope of authority) と言います。SWIFT は、SO の上位 SWIFTNet Directory ノードのサブツリーとして権限範囲を定義します。つまり、ユーザーが下位レベルで追加 SO を定義した場合、ユーザーが権限範囲を制御できるということです。SWIFT が最初の 2 人の SO に対して定義する権限範囲は、ユーザーのドメインと同等です。これには全ての下位ドメインが含まれます。

承認されたアクティビティ

SO は、LRA を使用して以下を行います:

- 証明書申込者の識別および承認
- 証明書要件のため、申込者の有効化シークレットを取得
- 問題がある証明書の破棄
- 証明書を必要としなくなったエンティティの無効化

SO の作成方法、SO のロールおよびタスク、ユーザーの SWIFTNet PKI における正しい設定および管理に関する推奨案についてのより詳しい情報は、*SWIFTNet Certificate Administration Guide* を参照してください。

6.2.1.4 Shared Security Officer (シェアードセキュリティオフィサー)

定義

シェアードセキュリティオフィサー (SSO)は、複数の企業の証明書を管理します。SSOは、それらの企業（ユーザー）が指定します。

SSO機能を使用する場合、SWIFTは *CertificateAdministration* ロールに加えて特定のロールをSSOに付与します。SWIFTは、この追加ロールをロールベースアクセス管理 (RBAC)サービスで定義します。SSOロールに関するより詳細な情報については、*SWIFTNet Certificate Administration Guide* を参照してください。SWIFTは、SSOからオンラインリクエストを受け取るごとにこのロールの有無を検証します。

サービスビューローは、SSOの管理企業となることはできません。SWIFTは、サービスビューローSSOの詳細をSWIFTNet Directoryに入力することはしません。

作成

SSOの作成方法に関するより詳細な情報は、*SWIFTNet Certificate Administration Guide* を参照してください。

権限範囲

SWIFTNet Directory内でシェアードセキュリティオフィサー(SSO)が管理できる範囲としてSWIFTが許可しているエリアを、*権限範囲 (scope of authority)* といいます。SWIFTは、SSOの上位SWIFTNet Directoryノードのサブツリーとして*権限範囲*を定義するほか、SWIFTがSSOを登録した追加ユーザーのドメインを定義します。SWIFTは常にSSOを企業レベルで登録するため、権限範囲とユーザーのドメインは同等となります。これには全ての下位ドメイン、ユーザードメイン、そしてSWIFTがユーザーに指定したその他全ての下位ドメインが含まれます。

承認されたアクティビティ

シェアードセキュリティオフィサー(SSO)は、証明書管理機能（SSOが証明書を管理している各ユーザーの）を使用して以下を行います：

- 証明書申込者の識別と承認
- 証明書に必要な有効化シークレットの取得
- 問題がある証明書の破棄
- 証明書を必要としなくなったエンティティの無効化

SSOのロールおよびタスクに関するより詳細な情報は、*SWIFTNet Certificate Administration Guide* を参照してください。

6.2.1.5 エンティティ、エンドユーザー、代理人の関係

個人に複数のロールが付与される可能性

エンティティ、ユーザー、そして代理人の各ロールは、場合によって同じ人が担うことができます。

エンティティが特定の個人である場合、その個人は必然的に同じ証明書の代理人かつエンドユーザーでもあるということになります（“エンティティ” ページの 92 を参照してください）。その他の場合、代理人は“代理人” ページの 93 で説明されているように、自動的に任命された個人です。

リレーションシップの概要

以下は、エンティティ、エンドユーザー、そして代理人の間におけるリレーションシップについての概要です

エンティティ、エンドユーザー、そして代理人の間におけるリレーションシップ

エンティティの代表	例	代理人
特定された個人	<i>john-smith</i>	エンドユーザー
匿名の個人	<i>testuser, so3</i>	任命された個人
ウェブブラウザ	<i>%02</i>	
アプリケーション	<i>clsgateway2</i>	

6.2.2 SWIFT ロール

6.2.2.1 証明書認証 (Certification Authority)

SWIFT が運用

SWIFTNet 証明書認証 (CA) システムは SWIFT が運用しています。

承認されたアクティビティ

SWIFTNet CA は以下を行います:

- サービス登録者に証明書を発行
- SWIFTNet Directory を証明書を発行
- 登録者の証明書を破棄
- SWIFTNet Directory で証明書破棄リスト (Certificate Revocation List、CRL) を発行

6.2.2.2 登録機関 (Registration Authority)

定義

SWIFTNet 登録機関 (Registration Authority、RA) は SWIFT が運営しています。SWIFTNet RA は、ユーザーのセキュリティオフィサー (SO) およびシェアードセキュリティオフィサー (SSO) を識別し、承認します。SO に証明書が発行されると、次に SO がローカルの登録機関となってユーザーのエンティティを識別し、承認します。

承認されたアクティビティ

SWIFTNet RA は以下を行います:

- ユーザーの識別と承認
- SO の識別と承認
- SSO の識別と承認
- SO の破棄
- SSO の破棄

- ユーザー、SO、SSO のリカバリー
- LRA リクエストの検証

識別と承認、そしてユーザーが提供しなければならない信用証明などに関するより詳細な情報は、“証明書” ページの 97 を参照してください。

6.2.2.3 SWIFTNet ディレクトリアドミニストレーター (Directory Administrator)

定義

SWIFTNet Directory は、登録エンティティ、デジタル証明書、CRL の身元を発行するオペレーション情報のオンラインレポジトリです。SWIFT は、登録プロセスにおいて SWIFTNet Directory エントリーを作成し、デジタル証明書は証明書プロセスの結果として追加されます。

6.2.2.4 Policy Management Authority (ポリシーマネジメントオーソリティ)

定義

SWIFT が運営しているポリシーマネジメントオーソリティ (Policy Management Authority、PMA) は、PKI ポリシーの保守を行うほか、可能であれば争議などを解決します。

6.3 証明書

6.3.1 フォーマット

SWIFTNet PKI 証明書のフォーマット

SWIFTNet PKI 証明書は X.509 に準拠しており、以下の情報が含まれています:

- DN の書式で、エンティティおよびその企業の身元識別
- 証明書バージョン
- SWIFTNet CA が発行した証明書を個別識別するシリアル番号
- SWIFTNet CA の身元識別
- 公開鍵および暗号アルゴリズム識別子
- 証明書の有効期間 (発効日と期限日)
- 証明書の目的 (デジタル署名や暗号化など)
- SWIFTNet CA 署名
- ポリシー ID (オプション)

6.3.2 タイプと使用先

6.3.2.1 テストおよび本番の証明書

テスト環境および本番環境

ITB 環境と SWIFTNet 本番環境は異なるネットワーク環境のため、どちらにもそれぞれの証明書認証 (CA) が存在します。ITB 環境はテスト使用のみですが、本番環境はパイロットおよびライブモードの両方をホストすることができます。

本番環境と Integration TestBed (ITB)環境の分離を強化するために、SWIFT はテスト環境用に本番環境では有効ではない証明書を発行します。

6.3.2.2 SWIFTNet InterAct、SWIFTNet FileAct、Web Certificates

証明書と SWIFTNet ディレクトリ階層の分離

SWIFTNet InterAct および SWIFTNet FileAct は、SWIFTNet Browse (HTTPS)とは物理的に異なる証明書を必要とします。

技術的な理由により、SWIFT は SWIFTNet InterAct および SWIFTNet FileAct 証明書を使用するエンティティと、ウェブ証明書を使用するエンティティを、2つの異なるロジカル SWIFTNet ディレクトリ階層に定義します。これらの階層は、それぞれ異なるルートを持ちます。SWIFT は、両方のタイプの証明書を持つエンティティを両方の階層で定義します。

SWIFTNet InterAct および SWIFTNet FileAct 証明書

SWIFT は、管理証明書 (破棄、回復、更新、無効にすることができる証明書) を発行することで、ユーザーが暗号鍵に関連するセキュリティリスクを管理するのをサポートします。SWIFTNet Link 暗号化モジュールは、これらの管理証明書を使用します。SWIFTNet InterAct および SWIFTNet FileAct 用として、エンティティは常に証明書を2つ受け取ります: 1つは暗号化用で、もう1つは署名の検証用です。

SWIFTNet Link は、SWIFTNet InterAct および SWIFTNet FileAct の証明書を、必要に応じてもしくは証明書がローカルキャッシュメモリに存在しない場合に、SWIFTNet ディレクトリから読み出します。

ウェブ証明書 (Web certificates)

SWIFT は、SWIFTNet Browse にあるウェブ証明書の管理は行いません。例えば、これらの証明書の破棄をサポートしていません (回復は可能です)。SWIFTNet Browse ウェブ証明書は2年間で期限切れとなります。SWIFTNet InterAct および SWIFTNet FileAct 証明書とは異なり、ウェブ証明書を使用するのは SWIFTNet Link 暗号化モジュールではなく、標準ウェブブラウザです。SWIFTNet Browse の場合、各ブラウザはユーザーが安全なセッションを構築するために使用できるウェブ証明書をそれぞれ1つずつ受け取ります。ユーザーは、この証明書を SWIFTNet メッセージの署名に使用することはできません。ウェブキーは、署名と暗号化の両方に使用されます。

SWIFT は、ウェブ証明書をブラウザおよびウェブサーバーなどのローカルに保管するほか、SWIFTNet ディレクトリで中央管理します。

ウェブ証明書が期限切れになった場合、セキュリティオフィサー(SO)が新たな証明書を取得します。

6.3.2.3 SNL Instance Certificate

説明

SWIFTNet に直接接続する SWIFTAlliance WebStation にあるものも含め、各 SWIFTNet Link (SNL)は自身の SNL インスタンス証明書 (SNL Instance Certificate) を保持しています。この証明書は、SWIFT がユーザーの SNL システムを認証することを可能にします。SNL インスタンス証明書は、SNL の導入中にシステムにより自動的に作成されます。SNL は、この証明書および対応する鍵を内部目的のために使用します。ユーザーは、SNL インスタンス証明書およびそれに対応する PKI セキュリティプロフィールを、*SWIFTNet Certificate Administration Guide* で説明されているように管理しなければなりません。

6.3.2.4 ビジネス証明書および簡易証明書

証明書の 2 つのクラス

SWIFTNet PKI 証明書には、ビジネス証明書および簡易証明書という 2 つのクラスがあります。これらの証明書は、キープロテクションにおいて異なるレベルのポリシーを持ち、信頼のレベルも異なります。

ビジネス証明書

ビジネス証明書は、ポリシー ID 「1.3.21.6.1」および「1.3.21.6.2」を含む SWIFTNet InterAct および SWIFTNet FileAct 証明書です。ビジネス証明書は、SWIFTNet ユーザーに高いレベルの認証および否認防止を提供します。

またユーザーは、このクラスのデジタル証明書を使用してユーザープロフィールのアップデートに関して SWIFT に連絡することができます。SWIFT はまた、SO にもビジネス証明書を発行します。

ユーザーは、エンティティおよび代理人がビジネス証明書に対応する秘密鍵やパスワードを共有しないことを保証し、秘密鍵やパスワードが秘匿されるようにしなくてはなりません。

ポリシー ID

ポリシー ID は、ビジネス証明書を以下のように個別識別します：

- SWIFT が割り当てたポリシー ID 「1.3.21.6.2」のビジネス証明書は、ハードウェアセキュリティモジュール (HSM) に保存しておかなくてはなりません。

本番環境の SWIFTNet FIN メッセージに署名する場合、ユーザーはハードウェアセキュリティモジュール (HSM) に保存されている証明書を使用しなければなりません。SWIFT は、ポリシー ID 「1.3.21.6.2」の有無をチェックすることで、本番環境の SWIFTNet FIN メッセージの送信に正しい証明書タイプが使用されていることを検証します。将来的には、SWIFTNet InterAct および SWIFTNet FileAct の通信に適用される予定です。

- SWIFT がビジネス証明書に割り当てたポリシー ID で、ディスクに保存しておいて良いものは「1.3.21.6.1」です。

データベースの証明書は、暫定的な SWIFTNet FIN 以外の SWIFTNet メッセージを署名するために使用することができます。

簡易証明書およびウェブ証明書にはポリシー ID は含まれていません。

簡易証明書

簡易証明書は、ポリシー ID を持たない SWIFTNet InterAct、SWIFTNet FileAct 証明書です。これらの証明書は、パイロット (テストアンドトレーニング) サービスでのメッセージ送信におい

てのみ使用されます。また、簡易証明書は以下のように高レベルでの認証や否認防止を必要としないメッセージの保護に使用することができます:

- ブラウザ(SWIFTNet Browse)とウェブサーバー間における(HTTPS)ウェブセッション
- ユーザーと SWIFT 間でのセッションを開始するためのメッセージ送信
- ユーザーと SWIFT 間におけるサービスをモニターするための通信

サービスアドミニストレーター

サービスアドミニストレーターは以下を実行する必要があります:

- 環境に応じて、使用する証明書のタイプを決定
- ユーザーが正しいタイプの証明書を使用していることを検証

暗号化の強度

ビジネス証明書で秘密鍵やパスワードを保護しているポリシーのレベルは簡易証明書のそれより高いレベルですが、暗号化の強度はどちらの証明書も同じです。

6.3.2.5 SWIFTNet CA 証明書

ストレージと使用

SWIFTNet Certificate Authority (CA、証明書認証)証明書は、エンティティ認証中に鍵保管ストレージデバイスに安全に送付されます。この証明書は、通信先の証明書を検証する必要があるごとに使用されます (“暗号化機能” ページの 91 を参照してください)。

破棄 (Revocation)

非常に例外的な状況において、SWIFT は SWIFTNet CA 証明書の破棄を実行することができます。そうした場合、SWIFT はユーザーにその旨を通知し、影響を受けるエンティティ全てに新たな証明書を再発行します。

6.3.2.6 証明書使用の概要

使用可能な機能およびその機能性

エンティティおよび代理人は、以下の表に示すように証明書を使用することができます。

証明書利用の比較表

証明書クラス	SWIFTNet InterAct および SWIFTNet FileAct		SWIFTNet Browse
	業務	簡易	ウェブ
ポリシー ID の有無	1.3.21.6.2 ⁽¹⁾ および 1.3.21.6.1	無し	無し
管理 ⁽²⁾	はい	はい	いいえ
ストレージ	はい - HSM およびディスク ⁽⁴⁾	はい - HSM またはディスク	いいえ
ライブサービス	はい	いいえ	該当なし
パイロット (テストアンドトレーニング) サービス	はい	はい	該当なし

証明書クラス	SWIFTNet InterAct および SWIFTNet FileAct		SWIFTNet Browse
	業務	簡易	ウェブ
Integration Testbed 環境	はい	はい	はい
本番環境 ⁽³⁾	はい	はい	はい

(1) HSM のみ

(2) 破棄および自動更新

(3) パイロットおよびライブ稼働を含む

(4) ポリシー ID 1.3.21.6.1 用のみ

6.3.3 証明書の期限切れ

有効期間

SWIFTNet は SWIFTNet InterAct、SWIFTNet FileAct を認証します。ウェブ証明書は発行から 24 ヶ月で期限切れとなります。SWIFT は証明書の期限切れをエージェントに通知しません。

SWIFTNet InterAct、SWIFTNet FileAct、ウェブ証明書の有効期限

証明書の種類	有効期限
SWIFTNet InterAct および SWIFTNet FileAct の署名検証用証明書	発行から 24 ヶ月後
SWIFTNet InterAct および SWIFTNet FileAct の暗号化証明書	発行から 24 ヶ月後
SWIFTNet Browse 証明書	発行から 24 ヶ月後

6.3.4 Certificate Revocation List (証明書破棄リスト)

定義

証明書破棄リスト(Certificate Revocation List、CRL)は、期限切れになる前に SO により破棄された証明書の識別子を一覧にした、署名入りのリストです。SWIFTNet CA は、SWIFTNet Directory にある全ての SWIFTNet PKI クライアントが使用可能な CRL を発行します。CRL は、証明書破棄プロセスが実行された後に更新されます。

証明書破棄に関するより詳細な情報は、“エンティティの破棄” ページの 115 を参照してください。

SWIFT は、証明書が期限切れとなった後、少なくとも 6 ヶ月間はその証明書および CRL を保管します。

6.4 公開鍵と秘密鍵

6.4.1 SWIFTNet InterAct と SWIFTNet FileAct キー

署名および暗号化のための同時キー発行

SWIFTNet InterAct と SWIFTNet FileAct サービス用として、認証の前に 2 つのペアキーが同時に作成されます。1 つは署名用で、もう 1 つは暗号化用です。これらの鍵は、ユーザーが署名および暗号化を利用するかどうかに関わらず作成されます。両方のペアキーに、関連した証明書がつけられています。

公開鍵の特性

公開鍵には以下の特性が適用されます：

- 公開鍵は、SWIFT により証明書に含められる
- SWIFTNet Directory にて証明書を発行
- 公開鍵は、ユーザーの取引先に使用される

署名ペアキー

署名をするペアキーは、秘密署名鍵(private signing key)と公開検証鍵(public verification key)から構成されています。

暗号化ペアキー

暗号化を行うペアキーは、秘密復号化鍵(private decryption key)と公開暗号鍵(public encryption key)から構成されています。HSM で保管されている場合、過去 3 つまでの復号化ペアキーが保存されます。

ストレージ

SWIFTNet InterAct と SWIFTNet FileAct の秘密鍵が SWIFTAlliance WebStation のスタンドアロンモードで作成された場合、ユーザーはそれをスマートカードおよび HSM トークンに保管することができます。秘密鍵を SWIFTAlliance Gateway もしくは SWIFT 以外のベンダーが提供しているインターフェース上で作成した場合、ユーザーはそれを 1 つもしくは複数の HSM、またはハードディスクに保管することができます。SWIFT は公開鍵を証明書の中に含め、SWIFTNet Directory に保管して中央管理します。

鍵の長さ (Key length)

鍵の長さは、暗号の強度を決定します。SWIFTNet Phase 2 で、鍵の長さは 1024 ビットから 2048 ビットにアップグレードされました。

有効期間

以下の表は、秘密鍵と証明書の有効期間を示しています。

鍵	有効期限
SWIFTNet InterAct および SWIFTNet FileAct 秘密署名鍵 (private signing key)	18 ヶ月間
SWIFTNet InterAct および SWIFTNet FileAct 公開署名検証鍵と証明書 (public signature verification key and certificate)	24 ヶ月間

鍵	有効期限
SWIFTNet InterAct および SWIFTNet FileAct 秘密復号化鍵 (private decryption key)	期限切れ無し
SWIFTNet InterAct および SWIFTNet FileAct 公開暗号化鍵と証明書 (public encryption key and certificate)	24 ヶ月間

署名ペアキーと証明書は、秘密署名鍵が期限切れになるまでの 100 日間に更新されます。暗号化ペアキーと証明書は、公開暗号化鍵（および証明書）が期限切れになるまでの 100 日間に更新されます。

秘密鍵に適用されるルール

ユーザーは、ビジネス証明書に対応する秘密鍵とパスワードの機密性を常に保ち、エンティティおよび代理人がこれらの鍵やパスワードを共有しないよう保証する必要があります。

ユーザーは、破棄された証明書に属する秘密鍵をエンティティが使用しないようにしなければなりません。

ノート ユーザーは、簡易証明書に対応する秘密鍵やパスワードを、自身のドメイン内で共有することができます。

6.4.2 ウェブ認証鍵

定義

SWIFT は、各証明書に対して SWIFTNet Browse ウェブ証明書を 1 通発行します。ウェブ証明書には、関連したペアキーが 1 組あります。ペアキーは、秘密認証鍵(private authentication key)と公開認証鍵(public authentication key)から構成されています。秘密認証鍵はハードディスクに保管されます。公開認証鍵は、SWIFT により証明書に含まれます。

使用

ユーザーは、クライアント (SWIFTNet Browse ブラウザ) と (ウェブ) サーバーを認証するため、セキュア SWIFTNet Browse セッション(SSL)の開始時に秘密認証鍵と公開認証鍵 (証明書) を使用します。これらの鍵は、ランダムに作成された、シンメトリックな非 PKI 関連鍵を安全に交換するために使用されます。このキー交換の後、SWIFT は SWIFTNet Browse の通信を確保し、整合性および暗号化のためにこのシンメトリックキーを使用します。HTTPS 通信の署名に個別の秘密認証鍵は使用されないため、SWIFTNet Browse ウェブ証明書と秘密認証鍵は否認防止を提供しません。HTTPS 通信は、ランダムに作成されたシンメトリック認証鍵によって保護されます。

保護

標準的なブラウザにおいてウェブ認証鍵の保護にパスワードの使用は必須ではありませんが、SWIFT はパスワードの使用を強く推奨します。

期限

秘密認証鍵は 18 ヶ月で期限切れとなります。公開認証鍵は、証明書と共に 24 ヶ月で期限切れとなります。

鍵の長さ (Key length)

鍵の長さは、暗号の強度を決定します。SWIFTNet Phase 2 で、ウェブキーの長さは 1024 ビットから 2048 ビットにアップグレードされました。

6.5 パスワード

パスワードの使用要件

SWIFT は、ユーザーのエンティティがパスワードを使用する場面に対し、発行された秘密鍵へのアクセスを保護するメカニズムを提供します。

SWIFTNet InterAct と SWIFTNet FileAct の処理の背景において、クライアントモジュールにログオンする全てのエンティティもしくはその代理人はパスワードが必要となります。

SWIFTNet Browse の処理の背景において、標準的なブラウザはウェブ証明書にパスワードと鍵管理を提供します。ブラウザはパスワードを必要としませんが、SWIFT はエンティティの秘密鍵を保護するためにパスワードを使用することを強く推奨します。

利用者パスワードおよびアプリケーションパスワード

SWIFTNet は、証明書が人間 (SO など) により保持されているのか、それともアプリケーション (SWIFTNet FIN コンピュータベースターミナルなど) により保持されているのかに依存する、パスワードルール (password rules) を定義します。SO は、証明書およびリカバリーの設定を実行する際、使用するパスワードタイプを特定することができます。SWIFT は、各タイプの証明書を一連のルールを実行する特定のパスワードポリシーにリンクします。ルールは以下のテーブルを参照してください。

パスワードタイプに準じたパスワードルール

	利用者パスワード	アプリケーションパスワード
パスワードの最小文字数	8	17
パスワードの最大文字数	20	20
パスワードの複雑性	<ul style="list-style-type: none"> 各文字を n 回以上使用してはならない (n=パスワードの文字数を 2 で割り、1 を足した数字) 少なくとも小文字を 1 つ含んでいなくてはならない 少なくとも大文字を 1 つ含んでいなくてはならない 少なくとも数字を 1 つ含んでいなくてはならない パスワードの文字数を 2 で割ったものと同等もしくはそれ以上の長さの、プロフィール名のサブストリングを含んではならない 	<ul style="list-style-type: none"> 各文字を n 回以上使用してはならない (n=パスワードの文字数を 2 で割り、1 を足した数字) パスワードの文字数を 2 で割ったものと同等もしくはそれ以上の長さの、プロフィール名のサブストリングを含んではならない
有効期間	90 日間	2 年間
履歴リストの長さ	8	8
作成者	エンドユーザー	ランダム (推奨)
HSM に保存されている場合に許容されるログイン失敗回数	5	5

利用者パスワードおよびアプリケーションパスワードポリシーを使用する

- プロフィールのパスワードが日常的に人間により入力される（アプリケーションに要求された際）場合、利用者パスワードポリシーを選択します。より短いパスワードを使用することができるほか、より頻繁にパスワードを変更することができます。プロフィールが SWIFTNet ユーザーである人間のオペレーターとやりとりをする場合、通常はこのポリシーを使用します。
- プロフィールのパスワードがアプリケーションに保存されており、必要に応じてアプリケーションにより自動的に使用される場合、アプリケーションパスワードポリシーを選択します。利用者パスワードより長いパスワードが要求され、また変更できる頻度も少なくなります。アプリケーションパスワードポリシーを使用すべきケースとして、プロフィールが FIN インターフェースにより使用されている、もしくは「バーチャル」な（複数の）SWIFTNet ユーザーである人間のオペレーターに位置するセキュリティプロフィールにより使用されている場合があります。

パスワードに使用できる文字

US-ASCII 文字セット（特殊文字含む）で印刷可能なものに対応していますが、空白およびダッシュ(-)は使用できません。

パスワード管理機器

SWIFTNet InterAct および SWIFTNet FileAct において、エンティティ（もしくはそのエージェント）は以下のタスクを実行するために鍵管理アプリケーション（Key Management Application、KMA）を使用することができます：

- パスワードの作成を可能にする
- パスワードの変更を可能にする
- パスワードが作成および変更された場合、それをパスワードルールに従って検証する

SWIFTNet Browse 証明書を使用する場合、標準的なブラウザはウェブ証明書用にパスワード管理機能を提供しています。

パスワードの共有

ユーザーは、ビジネス証明書に対応するパスワードの機密性を保持し、エンドユーザーもしくはエンティティの代理人と共有されていないことを保証する必要があります。

簡易証明書に対応するパスワードは、ユーザーのドメイン内でエンドユーザー間やエンティティの代理人の間で共有することができます。簡易証明書にはウェブ証明書が含まれます。いずれの場合も、ユーザーはパスワードがそのユーザー専用であることを認識する必要があります。責任者（担当者）以外に、パスワードへのアクセスを許可してはいけません。

パスワードの更新

SWIFT は、パスワードを更新する推奨頻度を発表しています（手順テーブルに記載された有効期間に注意してください）。期限の切れたパスワードが使用された場合、SWIFTNet Link 6.0 はユーザーが SWIFTNet PKI オペレーションを実行することをブロックしません（警告が生成されるだけです）。ただし、SWIFTNet インターフェースがパスワードの更新を強制することがあります。例えば、SWIFTAlliance WebStation は期限切れとなったパスワードを強制的に更新します。

期限切れとなったパスワードの破棄

SWIFT は、期限切れとなったパスワードを公開せず破棄することを推奨します。

6.6 Hardware Security Modules (ハードウェアセキュリティモジュール)

概要

ハードウェアセキュリティモジュール (HSM) は、PKI 秘密鍵の保管およびデジタル署名の作成を保護する、不正防止機能を持つデバイスです。

ユーザーが使用する HSM のタイプは、ハードウェアプラットフォーム、通信量、そして運用する PKI 証明書の数に依存します。ユーザーが使用できる HSM タイプは以下の通りです：

- 通信量が少ない場合：USB (Universal Serial Bus、ユニバーサルシリアルバス) ベースの HSM
- 通信量が少ない～多い場合：LAN (Local Area Network、ローカルエリアネットワーク) ベースの HSM

HSM の導入、構成、オペレーションに関するより詳細な情報は、*SWIFTNet Link Installation and Administration Guide* を参照してください。

6.6.1 USB ベースの HSM

USB ベースの HSM フォーマット

SWIFT は、2 種類の USB ベース HSM を提供しています：

- **HSM カード**：HSM カードはクレジットカードのような外観をしており、HSM カードリーダーに挿入します。HSM カードから情報の読み取り、そしてカードへの情報書き込みをするためのデバイスです。USB ポートで PC に接続します。
- **HSM トークン (tokens)**：キーリングに付けられるほど小型で軽量のデバイスで、USB ポートで PC に接続します。

署名が必要なメッセージが送信される際に使用されるため、HSM は必要不可欠なものです。HSM が使用不能になっていると、メインメッセージフロー (Main Message Flow) が阻まれてしまいます。事の重要性を鑑み、SWIFT は盗難や紛失に備えて常に HSM のスペアを用意しておくことをユーザーに義務付けています。

USB ベース HSM の利点

USB ベースの HSM には、以下の利点があります：

- **セキュリティ**：機密情報が USB ベース HSM を離れることはありません。情報は、所有先 (HSM) と既知情報 (証明書パスワード) という二因子セキュリティにより保護されています。USB ベース HSM は FIPS 140-2 (または 140-1) レベル 2 セキュリティ標準に準拠しています。
- **ポータビリティ**：秘密鍵が入れられたカードおよびトークンは、ユーザーが持ち歩くことができます。

USB ベース HSM の機能

HSM の主要機能には、以下が組み込まれています：

- 内蔵型の暗号化アプリケーションおよびセキュリティアプリケーション (証明書の保管と処理も含む)
- 各 HSM もしくは HSM トークンは証明書を 1 通ずつ保持

- ・ カード（もしくはトークン）上でのキー作成。つまり、重要な秘密鍵がカード（もしくはトークン）を離れないため、ネットワークやユーザーの PC を通じての盗聴は不可能
- ・ 外部の攻撃からのハードウェアおよびソフトウェアの保護

6.6.2 LAN ベースの HSM

HSM ボックス

LAN ベースの HSM ソリューションは HSM ボックスと呼ばれています。HSM ボックスは複数の証明書を保管することができるハードウェアボックスで、LAN でアクセスすることができます。

HSM ボックスはラックマウントすることができ、必要なコネクタや電源ケーブル一式と共に提供されます。また、HSM ボックスと共に PIN エントリーデバイス（PED）も提供されます。PIN エントリーデバイスは HSM ボックスにて特定の機密性の高いオペレーション前に必要となる認証を行うために利用するデバイスであり、認証時は PED キーおよび PIN コードを利用します。PED はテンキーを持つハンドヘルド型のデバイスで、HSM ボックスにケーブルで接続します。

HSM は署名が必要なメッセージが送信される際に使用されるため、必要不可欠なものです。HSM が使用不能になっていると、メインメッセージフロー（Main Message Flow）が阻まれてしまいます。事の重要性を鑑み、SWIFT はユーザーが本番環境において少なくとも 2 つの HSM ボックスを持つよう義務付けています。

HSM ボックスの利点

HSM ボックスは、キーの漏洩を防ぐためアクティブ型の不正防止システムと反応メカニズムが組み合わされているほか、データ暗号化および自分自身と SWIFTNet Link (SNL)間における双方向認証が行われています。HSM ボックスは FIPS 140-2 レベル 3 セキュリティ標準に準拠しています。

HSM ボックスは非常に高い耐障害性を必要とする構成に適しており、ユーザーは 1 つのクラスターに 2 つの HSM ボックスを設置することができます。

HSM ボックスの特長

HSM ボックスは、各ボックスごとに 250 の署名を保存することができます。HSM が LAN に設置されるため、複数の SNL で HSM を共有することができます。

ユーザーの通信量に応じ、また SWIFTNet 接続パックに従い、HSM ボックスは 3 つのスループットクラス（低、中、高）に対応しています。

接続パック（Connectivity Packs）に関するより詳細な情報は、*SWIFTNet Connectivity Packs* を参照してください。

6.7 セキュリティオフィサーおよびシェアードセキュリティオフィサーの登録

概要

SO の登録などの手続きや管理は、SWIFT のウェブサイト www.swift.com で行うことができます。Ordering & Support ページにあるオンラインフォームから、SO の登録、変更、解除が可能です。

原則

SWIFT はセキュリティオフィサー（SO）を、以下を行うことができる権限を持った個人として登録します：

- SWIFTNet ユーザーのその他のエンティティを登録
- 登録されたエンティティの鍵や証明書の管理
- SWIFTNet PKI に関連する問題について SWIFT と連絡を取り合う

6.7.1 セキュリティオフィサー（SO）の登録

セキュリティオフィサーのカテゴリ

SWIFT は以下の 2 つのカテゴリの SO を登録します：

- セキュリティに関してオフラインで SWIFT に連絡することができる SO
- セキュリティに関してオフラインで SWIFT に連絡することができ、オンラインのローカル登録アプリケーション（LRA）でセキュリティを管理することができる SO

ユーザーの SO は、その他のオンライン SO を追加登録することができます。

ノート シェアードセキュリティオフィサー（SSO）は、SWIFT にオフライン/オンラインの両方で連絡できる SO と同様のカテゴリに入ることに注意してください。

SO の登録に関するより詳細な情報は、*SWIFTNet Certificate Administration Guide* および *SWIFTNet Secure Channel Guide* を参照してください。

セキュリティオフィサーの登録

SWIFT が登録する主担当の SO2 名は、オンラインおよびオフライン証明書管理の両方の権限を保持します。後ほど、ユーザーは追加の SO をオンラインで（LRA を使用）登録、もしくはオフラインで SWIFT に登録（www.swift.com にあるフォームを使用）することができます。

オンラインで登録された SO は、LRA を通じてオンラインで証明書管理を行うことができます。SWIFT に登録された SO は、セキュアチャンネルにアクセスする必要があります。オフライン SO を www.swift.com に登録する場合は、当該 SO は www.swift.com にアカウントがあり、セキュアチャンネルへのアクセスが許可されている必要があります。

セキュアチャンネルへの登録に関するより詳細な情報は、*SWIFT Secure Channel User Guide* を参照してください。

ノート オンライン SO がその役割を中止する場合、ほかの SO は LRA を通じてそのエンティティを無効化する必要があります。オフライン SO がその役割を中止する場合、ユーザーは www.swift.com にあるフォームを使用して SWIFT に連絡する必要があります。

セキュリティオフィサーの身元を証明

SO の身元および権限は、ユーザー組織の人事部（HR）代表、もしくは公人（公証人など）により証明および確認される必要があります。

SWIFTNet セキュリティフォームに署名する SO は、ユーザー組織の人事部代表、もしくは公人と面談する必要があります。SO は人事部代表者もしくは公人の前で、*身分証明*（*Personal Identity Authentication*）および*権限確認*（*Authority Confirmation*）フォームに署名しなければなりません。また人事部代表者もしくは公人のいずれかもこのフォームに署名し、セキュリティ

オフィサーの写真付きの身分証明書、もしくはその他の公的な身分証明書を検証したことを証明します。

6.7.2 シェアードセキュリティオフィサーの登録

説明

シェアードセキュリティオフィサー (SSO) は、あるユーザー (管理機関) の SO が他のユーザー (被管理機関) により、その証明書を管理する機関として指定された際に作成されます。従って、各被管理機関の BIC8 コード下にあるユーザードメイン (全てのサブドメインも含む) は、SSO の権限範囲となります。

SSO は、セキュリティに関してオフラインモードで SWIFT に連絡することができ、ローカル登録アプリケーション (LRA) でセキュリティを管理することができます。これは、SSO を指定したユーザーの全てのユーザードメイン (サブドメインも含む) に適用されます。

ユーザーにより供給される SSO の詳細

SSO の登録方法に関するより詳細な情報は、*SWIFTNet Certificate Administration Guide* を参照してください。

SSO の身元の証明

手続きは“セキュリティオフィサー (SO) の登録” ページの 108 に記載されているものと同様です。

6.8 オンラインおよびオフラインでの証明書管理

6.8.1 エンティティおよび証明書のオンライン管理

ローカル登録アプリケーション (Local Registration Application) の設定

ユーザーがセキュリティオフィサー (SO) を登録した後、SWIFT がオンラインローカル登録アプリケーション (LRA) を提供する際の前提条件は以下の通りです:

- ユーザーは SWIFTNet 接続にアクセスする必要があります。
- ユーザーは SWIFTNet Link にアクセスする必要があります。この接続は SWIFTAlliance WebStation に含まれている、もしくは SWIFTAlliance Gateway インターフェースと共に使用されているサードパーティのインターフェースプロバイダーによるビジネスアプリケーションと統合することができます。

ローカル登録アプリケーション (Local Registration Application) の使用

セキュリティオフィサー (SO) は、ローカル登録アプリケーション (LRA) を通じてオンライン登録を行います。これは SO が SWIFTNet InterAct メッセージを使用して LRA から直接 SWIFTNet 登録機関 (Registration Authority) に要求を送信するため、オンライン管理と呼ばれています。

セキュリティオフィサー (SO) が自身を認証すると、SO のユーザードメインにあるエンティティや証明書を管理するために、オンラインの Local Registration Application (LRA、ローカル登録アプリケーション) が使用できるようになります。シェアードセキュリティオフィサー (SSO) の場合、SSO が権限を持つ全てのユーザードメインに適用されます。

SWIFT は、SO のリクエストメッセージを全て記録、認証、および検証し、常に署名および（適用される場合は）暗号化されたメッセージを返信します。また、この返信メッセージも SWIFT で記録されています。

SWIFT は、以下をチェックすることでメッセージを検証します：

- SO が *CertificateAdministration* に関連するロールを持っている
- SO が有効なビジネス証明書を持っている
- エンティティがユーザーのドメインに属している
- SO の権限範囲にエンティティが含まれている
- エンティティの証明書が、必要なアクションに対応するライフサイクル状態にある

LRA は、全ての SO リクエストに SWIFTNet InterAct および SWIFTNet FileAct メッセージを使用します。

代理人の要件

代理人は、エンティティの認証およびリカバリーのために認証されている必要はありません。しかしながら、代理人はこれらの認証もしくはリカバリー中のエンティティに対応する有効化シークレットを取得し、使用します。

代理人による証明書の発行およびリカバリーアクションをサポートしているのは、SWIFTNet InterAct と SWIFTNet FileAct メッセージングというよりは、SWIFTNet の独自プロトコルだと言えるでしょう。SWIFT は代理人のアクションも記録しています。

6.8.2 オフライン証明書管理

オンライン管理が使用できない場合

オンラインのローカル登録アプリケーション（Local Registration Application、LRA）が使用できないことによるセキュリティリスクを最小限にするため、SWIFT はバックアップとしてオフラインでの証明書管理を提供しています。

セキュリティオフィサー（SO）は、SWIFT セキュアチャネル、電話、ファックス、メールを通じて SWIFT にオフライン介入依頼を提出し、*オフライン管理*を行います。SO が直接 SWIFTNet 登録機関（Registration Authority）に連絡するのではなく SWIFT に連絡するため、これはオフライン管理と呼ばれています。

SO がオフライン介入を依頼する必要がある例として、以下があげられます：

- LRA が稼働しておらず、エンティティを緊急に管理する必要がある
- オンライン SO が誰もいない場合（例：SO 全員が同時にパスワードを紛失した、同時に証明書が期限切れになったなど）
- SO の有効化シークレットが期限切れになった
- 証明書および鍵の更新期間より長く契約している SO が存在しない（“証明書とキーの更新”ページの 114 を参照してください）。
- SNL インスタンス証明書に関連したエンティティを管理するため

ノート 緊急事態の場合、オフライン SO は通常の実操作を復旧させるため、SWIFT にオフライン介入を依頼する必要があります。これには料金がかかる場合があります（詳細は *SWIFT Price List* を参照してください）。

SO は、以下のタスクを行うオフライン介入を依頼することができます:

- 証明書の破棄
- 証明書の回復
- 証明書の無効化
- 有効化シークレットの再発行
- SNL インスタンス証明書の管理

オフライン管理に関するより詳細な情報は、*SWIFTNet Certificate Administration Guide* を参照してください。

SWIFT セキュアチャネル (Secure Channel)

SWIFT セキュアチャネルは、SO によるオフライン介入の提出および管理を可能にするアプリケーションです。リクエストは www.swift.com を通じて SWIFT カスタマーセキュリティマネジメント (CSM) に送信されます。SO は、所属企業の swift.com アドミニストレーターによりセキュアチャネルアプリケーションへのアクセスが許可され、リクエストを認証するためのセキュアコードカード (Secure Code Card) を SWIFT から受け取っている必要があります。より詳細な情報は、*SWIFT Secure Channel User Guide* を参照してください。

オフラインリクエストを行うセキュリティオフィサーの認証

セキュリティオフィサー (SO) がオフライン介入依頼を SWIFT セキュアチャネルを通じて提出すると、SWIFT は www.swift.com へのログインおよびパスワードと、個人のセキュアコードカードのワンタイムパスワードを組み合わせて利用して、SO を認証します。SO が SWIFT カスタマーサービスセンターに連絡することでオフライン介入依頼を提出した場合、SWIFT は秘密のパスフレーズを使用して SO を承認します。

6.8.3 証明書管理責任

エンティティおよび証明書ライフサイクル

エンティティおよび証明書のライフサイクルに関するより詳細な情報は、*SWIFTNet Certificate Administration Guide* を参照してください。

SWIFTNet InterAct および SWIFTNet FileAct 証明書

以下のテーブルは、SWIFTNet InterAct および SWIFTNet FileAct 証明書の状態を変更するアクションと、その責任者について示しています。

責任者	アクション
代理人	証明書発行
代理人	リカバリー
自動	期限切れ
自動	更新
SO (SSO を含む)	破棄
SO (SSO を含む)	無効化
SO (SSO を含む)	証明書発行の準備
SO (SSO を含む)	リカバリーの準備

ウェブブラウザ証明書

以下のテーブルは、ウェブ証明書の状態を変更するアクションと、その責任者について示しています。

責任者	アクション
代理人	証明書発行
自動	期限切れ
代理人	リカバリー

6.8.4 記録のアーカイブ

証拠としての監査証跡

証拠を保持するため、SWIFT は証明書ライフサイクルに関連する記録にタイムスタンプを押して保存します。

保存される記録には以下が含まれます：

- SO がオンラインのローカル登録アプリケーション（LRA）に発行し、SWIFT が受理した全てのリクエスト
- SO が SWIFT に提出した全てのオフラインリクエスト、および SWIFT の回答
- エンティティのステータス変更の全て
- 有効/期限切れの証明書全て
- 証明書破棄リスト

異常なオペレーティング状態に関するより詳細な情報は“オペレーティング状況に異常がある場合” ページの 73 を参照してください。

6.9 エンティティと証明書管理

6.9.1 エンティティの登録

エンティティの登録

信頼の連鎖を保持するため、SWIFTNet RA は、認証されたセキュリティオフィサー（SO）がユーザーのエンティティを SWIFTNet 公開鍵基盤（PKI）に登録するリクエストを提出したことを検証します。

認証および識別に関するより詳細な情報は、*SWIFTNet Certificate Administration Guide* を参照してください。

ウェブサーバーエンティティの登録

ウェブサーバーエンティティは、その他のエンティティと比較して登録および構成が複雑なため（ドメイン名システム[DNS]など）オンラインでの登録はできません。SWIFT カスタマーオーダーリングサービス（Customer Ordering Services、COS）に申込書を送信する必要があります。

6.9.2 証明書用のアプリケーション

ユーザーの責任範囲

サービスアドミニストレーターによっては、SWIFTNet に個人認証を義務付けています。証明書に個人名が記載される場合、ユーザーはその個人の身元を独立した情報源で確認し、検証および認証する必要があります。

セキュリティオフィサー(SO)は、以下を確実にしなければなりません:

- その個人がユーザー企業の社員だった場合、SO は企業の該当書類で身元を確認する必要があります。
- その個人が社員ではない（契約社員など）場合は、本人の身分証明書を確認します。それに加え、その個人の直属の上司が証明書のリクエストを正式に申請します。

SO 主導での手続き

証明書プロセスの準備に関するより詳細な情報については、*SWIFTNet Certificate Administration Guide* を参照してください。

この手順の最後に、エンティティ用の新たなノードが SWIFTNet Directory に *証明書の準備完了 (ready for certification)* というステータスで作成され、代理人は有効化シークレットを取得しているという状態になります。

機密性保護のため、SWIFTNet 登録機関 (Registration Authority、RA) は、ユーザー用に発行する有効化シークレットを暗号化されたチャネルもしくは通常の郵便を使用してユーザーの SO に送信します。RA が有効化シークレットを郵便で送付する場合、2 通の封印された封筒で 2 人の異なる SO に送ります。

2 人の SO うち、まず 1 人に封印された封筒で有効化シークレットを送付します。この最初の封筒を受理したことをユーザーが確認しない限り、SWIFT は 2 通目の封筒を送付しません。2 通目の封筒がユーザーの元に届かなかつた場合、ユーザーは SWIFT カスタマーサービスセンター (Customer Service Centre、CSC) まで連絡しなくてはなりません。また有効化シークレットを使用しないとユーザーが決定した場合も SWIFT CSC に連絡し、封筒を安全な環境下で破棄する必要があります。

6.9.3 証明書の発行と配布

エージェント主導での手続き

証明書プロセスに関するより詳細な情報は、*SWIFTNet Certificate Administration Guide* を参照してください。

このプロセスの完了時には、ペアの署名鍵とペアの暗号化ペア鍵が生成され、それぞれのペアの鍵に関連する証明書が SWIFTNet Directory に記載され、エンティティには *認証* ステータスがつけられます。なお、このプロセスの完了にはエージェントによる受理も含まれています。

ユーザーが有効化シークレットを使用できない場合、SWIFT カスタマーセンター (Customer Service Centre、CSC) に連絡する必要があります。

エンティティのキー発行に関して、ユーザーはエージェントが独占管理していることを確実にしなければなりません。これはエンティティレベルでの否認防止を実現するにあたり、非常に重要です。

ノート ウェブ証明書用のパスワード作成はオプションであり、使用するブラウザによって決定することができます。SWIFT は、秘密鍵を保護するためにエージェントがパスワードを作成し使用することを強く推奨します。

証明書

信頼の連鎖を保持するため、SWIFTNet 証明書認証 (Certification Authority、CA) はユーザーの SO に発行した有効化シークレットを検証することで、証明書リクエストがエンティティから送信されたものであることを検証します (エンティティが証明のために設定されている場合)。

検証鍵の証明書

信頼の連鎖を保持するため、SWIFTNet CA は検証鍵を認証して個別の秘密鍵に対応することを確実にします。

これにより、SWIFTNet メッセージおよびファイルの受信者は電子署名の信頼性を検証するために送信者の検証鍵を使用することが可能となります。

暗号化鍵の証明書

信頼の連鎖を保持するため、SWIFTNet CA は公開暗号化鍵を認証して個別の秘密鍵に対応することを確実にします。

これにより、SWIFTNet メッセージの送信者は、受信者の公開暗号化鍵を使用してメッセージを受信者のために暗号化することができます。

6.9.4 証明書とキーの更新

更新プロセス

ユーザーのオペレーション環境が正しく設定されている場合、SWIFTNet InterAct と SWIFTNet FileAct の秘密鍵およびその証明書は自動的に更新されます。

ノート セキュリティをより確かなものにするため、証明書の更新は常にペアの鍵の更新と同時に行われます。これにより、更新された証明書は常に新たに生成された公開鍵を持っていることとなります。この両方を同時に行う更新プロセスは、再キー (re-key) オペレーションとも呼ばれています。

更新頻度に関するより詳細な情報は、“SWIFTNet InterAct と SWIFTNet FileAct キー” ページの 102 を参照してください。更新プロセスに関するより詳細な情報は、*SWIFTNet Certificate Administration Guide* を参照してください。

エージェントへの通知

SWIFT は証明書の更新をエージェントに通知しません。自動更新を正常に行うため、エージェントは少なくとも 3 ヶ月に 1 回はサインインする必要があります。また、SWIFTNet CA への接続も使用可能である必要があります。

重要 これらの通知および更新に関する事柄は、SWIFTNet Link (SNL) インスタンス証明書にも適用されます。SNL は、SNL が開始される際に SNL インスタンス証明書にサインインします。つまり、ユーザーは少なくとも 3 ヶ月に 1 回は SNL インスタンスを再起動する必要があるということです。より良いオペレーションの実践という観点からは、各 SNL を毎月一回再起動することが推奨されます。

SWIFTNet PKI 証明書を使用するタイムクリティカルなアプリケーションに関し、エージェントは自動更新を見込んで監視する必要があります。

SNL は証明書の発行日および次回の更新日を提供します。

6.9.5 エンティティの回復

オンラインおよびオフラインでの回復

ユーザーは、オンライン/オフラインのいずれにおいてもエンティティの回復を設定することができます。SWIFT は、オフライン設定は緊急時における回復にのみ制限することを強く推奨します。なお、オフライン回復の設定は SWIFT により課金されることに注意してください。

オンラインでの回復

データ破損や秘密鍵の紛失によりユーザーがシステムを使用できなくなるのを最小限にするため、SWIFT はオンラインでの回復機能を提供しています。

ユーザーが破損もしくは紛失する可能性があるのは、SWIFTNet InterAct および SWIFTNet FileAct の秘密鍵です。また、これらの証明書や秘密鍵は自動更新が上手くいかなかった場合には期限切れとなってしまいます。そうした場合、ユーザーは当該証明書および秘密鍵が関連しているエンティティを回復させることで、新たな証明書と秘密鍵を直ちに要求することができます。

回復中のエンティティプロファイルを保護するため、ユーザーは以前とは異なるパスワードを選択しなくてはなりません。

エンティティの回復が必要となる一般的な状況については、“SWIFTNet InterAct および SWIFTNet FileAct の場合” ページの 117 のテーブルに記載されています。

回復プロセス

回復プロセスにおいて、SWIFT は秘密鍵や証明書を新規に作成します。回復プロセスに関するより詳細な情報は、*SWIFTNet Certificate Administration Guide* を参照してください。

6.9.6 エンティティの破棄

証明書の破棄

秘密鍵に問題がある場合、ユーザーがそれを誤用する期間を最小限にするため、SWIFT はオンラインで証明書を破棄できる機能を提供しています。

破棄を要求できるのはエージェント（SO を通じて）、SO、SWIFT です。

セキュリティオフィサーが証明書を破棄しなければならない場合

鍵もしくはパスワードに問題があると考えられ、その使用を防止しなければならない場合、セキュリティオフィサーは SWIFTNet InterAct および SWIFTNet FileAct の証明書に関連しているエンティティを破棄しなければなりません。

証明書の破棄が必要となる一般的な状況については、“SWIFTNet InterAct および SWIFTNet FileAct の場合” ページの 117 の表に記載されています。

証明書の破棄における SWIFT の権利

以下の状況において、SWIFT は（SWIFT 主導で）ユーザーの証明書を破棄できる権利があります：

- ユーザーの証明書が誤用/悪用されている強い疑いがある場合。このような場合、SWIFT は事前に SO と連絡を取ります。
- SWIFT が CA のルート鍵を更新し、ユーザーが証明書の更新に失敗した場合。このような場合、SWIFT は証明書の破棄を SO に事前に通知します。

SWIFT の主導でユーザーの証明書を破棄する場合、SWIFT はその旨をユーザーに事前に連絡するために最善の努力をします。

破棄プロセス

破棄プロセスの実行後、SWIFT は適切な証明書破棄リスト (Certificate Revocation List、CRL) に破棄された証明書のシリアル番号を更新し、SWIFTNet ディレクトリにそれをアップロードします。破棄プロセスに関するより詳細な情報は、*SWIFTNet Certificate Administration Guide* を参照してください。

証明書破棄のステータス確認

証明書を破棄するプロセスの実行後、証明書破棄リスト (Certificate Revocation Lists、CRL) が更新されます。送受信される各メッセージについて、SWIFTNet システムはメッセージを署名するために使用されている PKI 証明書が破棄されていないかどうかをチェックします。証明書が破棄されたものである場合、SWIFT はそのメッセージを拒否します。

証明書をオンラインで破棄した後のステータス確認

送受信される各メッセージについて、SWIFTNet システムはメッセージを署名するために使用されている PKI 証明書が破棄されていないかどうかをチェックします。SWIFT は、少なくともメッセージが送信される 5 分前までに実行されたオンラインでの破棄がチェックリストに入れていることを確実にします。

ノート SWIFT オペレーティングセンターが災害に遭った場合、その災害の 90 分前までにユーザーが送信した証明書の破棄要求は完全に処理されていない可能性があります。このような場合、ユーザーからの依頼により、SWIFT は影響を受けた破棄要求をユーザーが追跡するのをサポートします。

証明書をオフラインで破棄した後のステータス確認

送受信される各メッセージについて、SWIFTNet システムはメッセージを署名するために使用されている PKI 証明書が破棄されていないかどうかをチェックします。SWIFT は、メッセージが送信される 2 時間前までに SWIFT に到着したオフラインでの破棄要求で有効なもの（および破棄を依頼したセキュリティオフィサーが承認されたもの）が、全てチェックリストに含まれていることを保証します。

ノート SWIFT セキュアチャネルのユーザーの場合、以下の条件が全て満たされている場合に破棄要求が有効となります：

- SWIFT セキュアチャネルを通じて、セキュリティオフィサーが破棄要求を提出している
- 2 人目のセキュリティオフィサーが破棄要求を承認している（必要に応じて）
- セキュリティオフィサーが破棄要求の確認メールを受信している

法的責任

遅延期間中（オンラインでの破棄は 5 分、オフラインは 2 時間）の場合、破棄要求が受理されていても証明書は有効と認識されることに注意してください。

証明書の破棄要求が出された時間と、SWIFT がその証明書で署名されたメッセージを一元的に拒否し始める時間までの期間中は、その証明書が有効と解釈された場合の責任は全てユーザーにあります。

破棄プロセスに関するより詳細な情報は、*SWIFTNet Certificate Administration Guide* を参照してください。

6.9.7 エンティティの無効化

セキュリティオフィサーがエンティティを無効化する必要がある場合

セキュリティオフィサー (SO) は、SWIFTNet InterAct または SWIFTNet FileAct 証明書に関連しているエンティティを永久に無効化することができます (ウェブ証明書に関連しているエンティティを無効化することはできません)。また、ユーザーのセキュリティオフィサーはユーザーがもう必要としないエンティティを無効にする必要があります。SWIFT はエンティティが無効にされた理由については記録しません。

エンティティを無効化する状況に関するより詳細な情報は、“エンティティの破棄、回復、無効化” ページの 117 を参照してください。

SWIFT がエンティティを無効化できる場合

例外的なケースにおいて、SWIFT もエンティティを無効化できます (例: 顧客が SWIFT ユーザーではなくなった場合など)。状況はケースバイケースで個別に判断されます。

SWIFT がユーザーのエンティティを無効化する場合、SWIFT はその旨を事前にユーザーに連絡する最善の努力をします。

無効化プロセス

ユーザーの SO は、エンティティを無効化する前に、まずエンティティを破棄する必要があります。

SWIFT がそのユーザー (エンティティ) を SWIFTNet Directory から除外すると、更新プロセスが無効化されます。無効化は撤回できず、一度無効にしたものは永続的にそのままです。無効化プロセスに関するより詳細な情報は、*SWIFTNet Certificate Administration Guide* を参照してください。

6.9.8 エンティティの破棄、回復、無効化

SWIFTNet InterAct および SWIFTNet FileAct の場合

以下の表は、SWIFTNet InterAct および SWIFTNet FileAct エンティティのパスワード変更、もしくは証明書の回復、破棄、無効化をセキュリティオフィサーが実行しなければならない状況について示しています。エンティティの破棄、回復、無効化が SWIFT インターフェースでどのように処理されるかについてのより詳細な情報は、関連する SWIFTNet インターフェースガイドを参照してください。

状況	パスワード変更	破棄	回復	無効化
セキュリティプロフィールの紛失。HSM または SNL ホストが紛失もしくは盗難されたことが原因である可能性がある場合。また、ディスク上でプロフィール情報を保存しているバックアップが紛失または盗難されたことが原因である可能性がある場合。		X	X	
パスワードの不正開示、盗難、期限切れ間近。 この場合、セキュリティプロフィールはコピーされていません。セキュリティプロフィールがコピーされた場合は、破棄および回復する必要があります。	X			

状況	パスワード変更	破棄	回復	無効化
パスワードを忘れた			x	
エンティティが不要となった		x		x
個人証明書を保持していたエンドユーザーが退職した		x		x
匿名の証明書（非個人）を保持していたエンドユーザーが退職した	x			
共有証明書のパスワードを知っているエンドユーザーが退職した	x			
証明書と鍵の自動更新が失敗した後にエンドユーザー証明書が期限切れとなった			x	
有効化シークレットの漏洩		x	x	
有効化シークレットが上手く働かない		x	x	
証明書をディスクから HSM (HSM からディスク) に移動させたい			x ⁽¹⁾	
証明書クラス（簡易証明書からビジネス証明書になど）、ポリシー ID、パスワードポリシーの変更			x	

(1) ポリシー ID とパスワードポリシーの両方に変更がない場合は破棄の実行も推奨されます。

ウェブ証明書の場合

ウェブ証明書は管理できないため、介入が必要とされる状況は限定されています。

状況	回復
パスワードを忘れた	x
ウェブ証明書の期限が切れた	x

7 身元の確認および認証

概要

SWIFTNet ネーミングスキームは ISO-9362 (銀行業務) を統合します。これには銀行が使用する通信メッセージ、銀行コード (BIC)、Business Entity Identifier (BEI) が含まれます。このスキームは、SWIFT ユーザーとオペレーション可能なエンティティをより柔軟性が高く幅広い分野をカバーする技術標準 (X.500 準拠の識別名[DN]) 上で識別します。

SWIFTNet ネーミングスキーム

SWIFT は SWIFTNet ネーミングスキームを使用して以下を作成します:

- メッセージアドレスやメッセージのルーティング指示などに含まれる、送信者/受信者を識別するための取引先名
- SWIFT が SWIFTNet 公開鍵基盤 (PKI) で登録したエンティティを識別するための証明書名

SWIFTNet メッセージには通常、取引先名および証明書名識別子の両方が含まれています。SWIFT は SWIFT ユーザーとして登録されているユーザーを識別するため、それぞれに BIC もしくは BEI を割り当てています。SWIFT は SWIFTNet サービスのいずれかに登録している SWIFT ユーザーに、機関 DN を割り当てます。機関 DN には BIC が含まれており、SWIFT ユーザーの SWIFTNet PKI サブドメインにおけるルート役割を果たします。このサブドメインには SWIFT ユーザーのエンティティの登録名 (識別名[DN]) が全て含まれています。

SWIFT ユーザーのサブドメイン内で SWIFT が定義したエンティティの登録 DN は、2つの部分から構成されています:

- 機関 DN : `o=bankabcd,o=swift` または `o=bankabcd,c=ww`
- 機関 DN の前に、SWIFT が階層的に配置したエンティティ固有の部分 (例: `cn=john-doe,o=bankabcd,o=swift`)

8 登録および終了

8.1 登録

前提条件

SWIFT が金融機関や事業法人に SWIFTNet（公開鍵基盤[PKI]を含む）の使用を許可するにあたり、以下の手続きが必要となります：

- 各団体は、SWIFT ユーザー、SWIFT パートナー、もしくはサービスビューロー（場合によっては）として登録しなければなりません。適用される登録手続きに関するより詳細な情報は（SWIFT ユーザーの認証も含め）、www.swift.com > Ordering & Support > *SWIFT User Handbook* の Ordering and the *SWIFT Corporate Rules* にある「SWIFT のオンラインオーダー機能」を参照してください。
- ユーザーは特定の SWIFTNet サービスに登録している必要があります。SWIFTNet サービスへの参加は、サービスへのアクセスを規定する登録手続きおよび特定の認証を定義するサービスアドミニストレーターにより承認されます。サービスアドミニストレーターが SWIFTNet サービスを許可すると、ビジネスサービスのプロバイダーが認証方法および登録手続きを定義します。

登録方法

SWIFTNet サービスに登録するには、適切な申し込みフォームに記入のうえ提出してください。SWIFTNet に申し込むと、PKI への申し込みも自動的に行われます。

8.2 終了

ユーザーの無効化

期限切れの証明書や秘密鍵が間違っていて使用されるのを防ぐため、SWIFTNet RA はユーザーが SWIFTNet メッセージングサービスで使用しなくなった証明書を破棄および無効化します。

無効化する際の確認

SWIFTNet RA が SWIFTNet ユーザーを無効化（接続停止）した場合、SWIFTNet RA は全ての既存証明書を破棄し、対応するノードを無効化したことをユーザーの担当者 2 名にメールで連絡します。

9 オーダー

SWIFT サービスおよび製品のオーダー

SWIFT のサービスおよび製品の利用にあたり、ユーザーは当該サービスに登録・製品をオーダーする必要があります。

関連情報

SWIFT のオンラインオーダーに関するより詳細な情報は、www.swift.com > Ordering & Support > Ordering を参照してください。

10 SWIFT サポート

SWIFT ユーザー向けのサポート

SWIFT のサービスおよび製品に関連した問題やご質問がある場合は、SWIFT までお問い合わせください。SWIFTSupport は、SWIFT ユーザー向けのサポートサービスです。全ての SWIFT ユーザーがご利用頂けます。

SWIFTSupport サービスのご利用にあたり、ユーザー企業に所属している個人（利用者）は、事前に登録する必要があります。SWIFTSupport への登録方法に関するより詳細な情報は www.swift.com > Ordering & Support を参照してください。

関連情報

SWIFTSupport サービスに関するより詳細な情報は *SWIFTSupport Service Description* を参照してください。

11 ルールと責任

概要

本セクションは、以下の SWIFT サービスおよび製品の機能およびそのルールと責任について説明しています:

- SWIFTNet FileAct
- SWIFTNet InterAct
- SWIFTNet Browse
- SWIFTNet 公開鍵基盤(PKI)
- セキュア IP ネットワーク (SIPN) への SWIFTNet 接続サービス

11.1 SWIFT のルールと責任範囲

11.1.1 一般

契約の約定

サービス文書 (Service documentation) に定められている適用条件に従って、SWIFT はサービスおよび製品に関する契約を締結し正式に認可されたユーザーに対し、SWIFT の当該サービスおよび製品へのアクセスやその利用を許可します。

11.1.1.1 サービスの導入と条件

導入のタイミング

SWIFT は必要とされる注文書や関連文書が全て必要に応じて記入および署名されていることを確認し受理した後、サービスの導入を速やかに開始します。

サービス条件

SWIFT は本書 (Service Description) に記載されている事項に従い、SWIFT のサービスおよび製品を提供するよう最善の努力を払います。

11.1.1.2 サービスの変更

SWIFT とサービスの変更

SWIFT は以下の目的のため、SWIFT のサービスおよび製品全体もしくはその一部をいつでも (一般的には、事前通知されている正当なダウンタイムウィンドウ中に) 一時停止、交換、もしくは変更することができます:

- 定期メンテナンスを実行するため、またはより一般的に SWIFT サービスの管理作業 (サービスマネジメントサービス) を実行するため
- SWIFT が SWIFT のサービスおよび製品の全体もしくはその一部を、*SWIFTNet Release Policy* に記載されている内容からアップグレードまたは変更する場合
- セキュリティのため、もしくは適切なパフォーマンスのため

- SWIFT およびそのユーザーや、SWIFT のサービスおよび製品全体もしくはその一部に関係しているサービス管理者に対して監督権限がある規制機関、関係当局、その他の組織や団体、政府機関などからの命令、指示、要求に従うため
- ユーザーもしくは関係するサービス管理者に実質的な不履行があった場合

SWIFT のサービスおよび製品においてこのような一時停止、交換、変更を行う場合、SWIFT は関係するユーザーに十分な期間を空けて事前通知します。また緊急の場合にはできる限り早く通知します。

11.1.2 SWIFTNet メッセージング特定のロールと責任範囲

概要

SWIFT は本書（Service Description）に記載されている事項、特に以下のセクションに記載されている事項に基づき、SWIFTNet メッセージングサービスで規定されている特定のロールや責任範囲に従うべく商業的に最善の努力を払います。:

- “SWIFTNet InterAct” ページの 21
- “SWIFTNet FileAct” ページの 33
- “SWIFTNet Browse” ページの 48
- “SWIFTNet メッセージングソリューション” ページの 15

11.1.3 SWIFTNet PKI 特定のロールと責任範囲

SWIFTNet PKI 特定のアクティビティ

本書（Service Description）に記載されている通り、SWIFT は以下を行います:

- 認証局（Certification Authority）、登録機関（Registration Authority）、ポリシー管理局（Policy Management Authority）、SWIFTNet Directory の構築および運営
- 証明書失効リスト（Certificate Revocation List、CRL）の保守および配布
- ログの保守およびアーカイブ

SWIFT は、当該契約を SWIFT と締結している正規のユーザーに対し、SWIFTNet 公開鍵基盤（PKI）を提供するためにこれらのアクションを行います。SWIFT はあらゆる面において本書（Service Description）に基づき SWIFTNet PKI を提供します。

SWIFT は SWIFTNet PKI の契約終了を定期的に処理しようとは考えていません。SWIFTNet PKI の解除に関連する活動を、SWIFT はプロジェクトという形で計画および実行します。

法人組織

電子署名に関連する調査に協力するため、SWIFT はユーザーからの要請に応じて、SWIFTNet が発行した証明書に含まれる識別名（DN）に対応する法人組織の情報を提供します。

リスク管理

SWIFT は SWIFT の管理下にある SWIFTNet PKI の提供に伴うセキュリティリスクを定期的に評価し、それらのリスクを管理するための手段を実行します。

オペレーション標準

SWIFT は SWIFTNet PKI を運営するにあたり、これらの責任を実行する際に個人とグループの説明責任が分離されるよう、組織計画を作成しています。SWIFT は、SWIFTNet PKI のオペレーションに直接関係する SWIFT の社員を調査および訓練するために、様々な対策を講じています。

正確なデータ処理

SWIFT は、証明書に関連する処理情報および SWIFTNet PKI の提供に関するその他の情報は、全て本書（Service Description）に従って正確に管理および処理されていることを保証します。

終了

SWIFT が、SWIFT 一般契約条件（SWIFT General Terms and Conditions）に記載されている条件に基づいて SWIFTNet PKI を終了させる場合、SWIFTNet 証明書認証（Certification Authority）により発行された全ての証明書も併せて破棄および無効化されます。

HSM ボックスのサポートおよびメンテナンス

機器（一つもしくは複数の HSM ボックス）の供給もしくは使用に問題が発生した場合、ユーザーは速やかにその旨を SWIFT サポートセンターに通知する必要があります。かかる通知を受け取った場合、SWIFT はこれに関連する SWIFTSupport サービスディスクリプションに従って取扱います。

メンテナンスには、SWIFT によりその旨が妥当に事前通知された機器のアップグレードも含まれます。かかるアップグレードの実行はユーザーの責任です。またメンテナンスサービスには、機器を仕様に合わせておくことができなかつた場合、SWIFT の裁量権によりその修理もしくは交換を行うことが含まれています。

ユーザーは、機器の使用に関して SWIFT 通知の有効なガイドラインや指示に必ず従う必要があります。関連するドキュメントおよび契約条件の入手は、ユーザーの責任となります。

11.1.4 セキュア IP ネットワークへのアクセスサービス

11.1.4.1 専用回線 DSL および ISP 加入者回線での SIPN アクセス

11.1.4.1.1 専用回線でのアクセス

概要

ユーザーは、セキュア IP ネットワーク（SIPN）に接続するためのデジタル加入者回線（Digital Line Subscriber、DSL）専用回線およびインターネットサービスプロバイダー加入者回線（Internet Service Provider Local Loop、ISP Local Loop）につき、SWIFT と直接購入・契約することはありません。ハードウェアや導入をサポートする SWIFT ネットワークパートナー（Network Partner）にソリューションを発注する必要があります。但し SWIFT がサービスを計画、構成、有効化、テストできるよう、ユーザーは SWIFT ネットワークパートナーに発注したことを SWIFT に連絡する必要があります。

Points-of-Presence（PoP）サイトにおけるアクセスポート

ユーザーまたはそのネットワークパートナーにより仮想プライベートネットワーク（VPN）ボックスのインストールが確認された後、SWIFT はユーザーの接続構成に従って VPN ボックスを構成し、必要に応じてそのアップデートを行います。

VPN を構成した後、SWIFT はアクセスサービスを有効化してユーザーまたはネットワークパートナーが SIPN にアクセスできることを確認し、ユーザーまたはネットワークパートナーにテストが成功したことおよびアクセス可能であることを連絡します。

SWIFT とネットワークパートナーの役割

ネットワークパートナーは、VPN ボックスを実際にインストールし、それが適切に機能していることを確認します。SWIFT は、アクセスサービスを有効化し、当該ユーザーが SIPN にアクセスできるかどうかをテストします。SWIFT はユーザーが前提条件を全て満たしている場合のみ、そのアクセスを有効にします。

11.1.4.1.2 モニタリングおよび構成のアップデート

SWIFT によるモニタリングおよびアップデート対象

SWIFT は、ユーザーの SIPN 接続およびアクセスを継続的にモニタリングしているほか、SIPN 全体の可用性についてもモニタリングしています。SWIFT はサービスドキュメント (service documentation) に記載されている条件に従って、SIPN またはユーザーによる接続もしくはアクセス (もしくはその両方) の一時停止、交換、変更 (場合によって) する権利を有しています。更に、SWIFT はサービスドキュメント (service documentation) の契約条件に従ってユーザーの VPN ボックス構成のアップデートを行う責任があります。SIPN へのユーザーの接続またはアクセスの変更 (ユーザーの希望によるもの) を反映させるため、構成のアップデートが必要な場合、SWIFT は当該アップデートを休止時間中 (allowable downtime window) に実行します。

11.1.4.1.3 接続障害が発生した場合のアクション

概要

接続障害が発生した場合、SWIFT が唯一の窓口となり、障害調査に関する責任を一手に引き受けます。

SWIFT はユーザーに情報を提供するよう努力しますが、かかる接続障害を解決するプロセスにおいて必ずしもユーザーに連絡を取るとは限りません。SWIFT は、VPN ボックスの基本的なチェックをするにあたりユーザーの協力を求める場合があります。例えば、リセット、ケーブルのチェック、LED 表示のチェック等です。

SWIFT は、IP 接続の状況をユーザーの VPN ボックスまでモニターします。接続障害を検知した場合、SWIFT はその調査を行った後、かかる障害を修正して接続を復旧するために行う処理について、関係するネットワークパートナーに適宜連絡します。

代替接続

SWIFT はユーザーの接続オプションに基づいて、代替接続をサポートするフェイルオーバーメカニズムを導入しています。このメカニズムには、代替回線、Managed-Customer Premises Equipment (管理されたユーザー宅内機器、M-CPE) の代替システム (フォールバック) のほか、ダイアルアップ回線での接続の場合は代替の Points-of-Presence (PoP) が含まれます。

構成に専用回線が含まれている場合、SWIFT は問題解決・プライマリ接続への戻しに必要な処理につき、関連するネットワークパートナーに連絡します。

11.1.4.1.4 専用回線を通じた VPN ボックスのメンテナンス

ポリシー

SWIFT は VPN ボックスのメンテナンスに以下のポリシーを適用します:

- SWIFT は、テクノロジーを最新のものに保ちサービスを漸進的に向上させるため、VPN ボックスのメンテナンスアップデートを行います。頻度として、年間 2 回以上のアップデートを行う予定はありません。

SWIFT はユーザーの介在を必要としない集中管理型のメンテナンスを提供しており、ユーザーへの影響を最小限に抑えています。

- SWIFT は、VPN ボックスの構成をユーザーコミュニティ全体で同期化させることを目標としています。限られた期間内にユーザー全体で整合性を取るため、アップデートは数ヶ月ごとに一括で行われます。
- Dual-I 構成の場合、SWIFT は通常、メンテナンスアップデートをプライマリ常時接続回線を通じてダウンロードします。しかし耐障害性の問題により、SWIFT の裁量で代わりに代替用のダイヤルアップ回線を使用することがあります。いずれの場合も、VPN ボックスのメンテナンスアップデートに関する全ての通信コストはユーザーが負担するものとします。
- SWIFT は、メンテナンスアップデートを標準の SWIFTNet Allowable Downtime Window（休止時間枠、ADW）に当たるよう計画します。また全体的なリスクが最小限になるように計画を管理します。

アップグレードを開始する前に、SWIFT はアップグレードの内容やその利点、全体的なスケジュールについて一般的な通知を出します。アップデートのスケジュールに関して、ユーザーが影響を与えることはありません。

アップグレードもしくはメンテナンスのプロセスに失敗した場合、その修正プロセスは SWIFT が管理します。

11.1.4.2 ダイヤルアップ回線でのセキュア IP ネットワークへのアクセス

11.1.4.2.1 ダイヤルアップ回線でのアクセス

概要

ダイヤルアップ回線で接続する場合、ユーザーは直接 SWIFT に発注することができます。接続を設定するため、SWIFT はユーザーの所在地（ロケーション）や要件をネットワークパートナーに連絡します。

PoP サイトでのアクセスポート

サービスドキュメントに適宜定められた条件に従い、SWIFT は:

- 関連する 1 つ以上の Point-of-Presence (PoP) サイトにあるアクセスポートを使用可能にし、構成します。SWIFT がその完全な裁量権の元で定義した関連 PoP サイトをユーザーに通知します。SWIFT は本件においては、可用性実現の統制の面から、合理的に可能な範囲で国際電話料金も含めたユーザーのコストを負担します。また SWIFT は、かかる PoP サイトをいつでも変更できる権利を有します。ユーザーによるセキュア IP ネットワーク (SIPN) へのアクセスの一時停止、交換、変更が合理的に必要な場合、ユーザーは設備機器やサービスを自己負担にて適宜除去、調整、移動、交換する必要があります。
- ユーザーが SWIFT に通知した接続構成、もしくはユーザー用の接続構成に基づいて、仮想プライベートネットワーク (VPN) ボックスを構成します。
- ユーザーの SIPN へのアクセスを、ユーザーまたはネットワークパートナー用に有効化します。アクセスを有効化した後、SWIFT はその旨をユーザーまたはネットワークパートナーに通知します。

ノート SWIFT はユーザーが前提条件を全て満たしている場合にのみ、そのアクセスを有効にします。ダイヤルアップ回線のサービスをテストするのはユーザーの責任です。

11.1.4.2.2 構成アップデート

SWIFT によるモニタリングおよびアップデート対象

SWIFT はサービスドキュメントの契約条件に従ってユーザーの仮想プライベートネットワーク (VPN) ボックス構成のアップデートを行う責任があります。ユーザーが SIPN への接続またはアクセスに関して要求した変更を反映させるために、構成のアップデートが必要な場合、SWIFT はユーザーが次にダイヤルアップ回線での接続を開始した際、もしくはユーザーと合意した時間にかかる変更を行います。これにより、ユーザーは当該目的のためだけに回線を開くことができます。

11.1.4.2.3 代替接続のフェイルオーバー

概要

SWIFT はユーザーの接続オプションに基づいて、代替接続をサポートするフェイルオーバーメカニズムを導入しています。このメカニズムには、代替回線、M-CPE 機器の代替システム (フォールバック) のほか、3 つの異なる代替 Points-of-Presence (PoP) が含まれています (3 つの代替 PoP のうち、1 つは外国に設置されます)。

11.1.4.2.4 ダイヤルアップ回線を通じた VPN ボックスのメンテナンス

VPN ボックスの予備を提供

SWIFT はダイヤルアップ回線を使用しているユーザーに、VPN ボックスのメンテナンスサービスを提供しています。ユーザーが SWIFT 指定の供給者に注文した各 VPN ボックスにつき、SWIFT は予備の VPN ボックスとして使用する 2 つめの VPN ボックスを手配します。プライマリ VPN ボックスに不具合が生じた場合、ユーザーは予備の VPN ボックスを有効化するよう SWIFT に連絡する必要があります。

また SWIFT は、ユーザーが新たに予備の VPN ボックスを入手できるよう手配します。

予備の VPN ボックスを提供されるにあたり、ユーザーは必要と思われる全ての輸入状 (インポートドキュメント)、許可証、承諾書などを SWIFT に提供する必要があります。

SWIFT は VPN ボックスのメンテナンスに以下のポリシーを適用します:

- SWIFT は、テクノロジーを最新のものに保ちサービスを漸進的に向上させるため、VPN ボックスのメンテナンスアップデートを行います。頻度として、年間 2 回以上のアップデートを行う予定はありません。
- SWIFT は、VPN ボックスの構成をユーザーコミュニティ全体で同期化させることを目標としています。限られた期間内にユーザー全体で整合性を取るため、アップデートは数ヶ月ごと一括で行われます。
- ダイヤルアップ回線接続パックのアップデートは、ユーザーが SWIFTNet に接続する場合にのみ行われます。予備の VPN ボックスは、ライブ環境での使用のために有効化されるまでアップデートされません。アップデートの際は、SWIFT が最新の構成をダウンロードします。
- 全体的なリスクが最小限になるよう、メンテナンスのスケジュールを管理します。
- アップグレードを開始する前に、SWIFT はアップグレードの内容やその利点、全体的なスケジュールについて一般的な通知を出します。アップデートのスケジュールに関して、ユーザーが影響を与えることはありません。
- VPN ボックスのメンテナンス中、一定のサービス中断が必要となります。アップグレードもしくはメンテナンスのプロセスに失敗した場合、その修正プロセスは SWIFT が管理します。

11.2 ユーザーのロールと責任範囲

11.2.1 一般

11.2.1.1 解釈

SWIFT 顧客とは

SWIFT 顧客とは (SWIFT ユーザー、SWIFT パートナー、サービスビューロー)、SWIFT のサービスと製品を 1 つ以上登録もしくは発注している顧客を指します。サービスアドミニストレーター (Service Administrator) も SWIFT 顧客です。

不明確さを回避するため、本サービスディスクリプション内において“顧客”に言及している場合、顧客の従業員、役員、代理人、請負人などといった (これらだけに限定されない) 顧客の責任範囲にある全ての人間が含まれることを明確にしておきます。

11.2.1.2 関連する契約条件の順守

契約条件

顧客は、適用されるサービスドキュメントに記載されている全ての契約条件に従い、これに準拠して SWIFT のサービスと製品を入手、所有、使用しなければなりません。なお、適用されるサービスドキュメントには、SWIFT のサービスと製品に関する一般契約条件および本サービスディスクリプションが含まれますが、これに限定されるものではありません。

顧客は特に、以下を行う必要があります:

- SWIFT のサービスと製品の提供を受けることに関連して何らかの問題がある場合には、速やかに SWIFT に通知すること。
- かかる問題を SWIFT が認識および調査するにあたって協力・支援し、特に SWIFT により、もしくは SWIFT 用に適宜提供されたガイドラインや指示などに従うこと。これには VPN ボックスのリセット、ケーブルのチェック、LED 表示のチェックなど、オンサイトでの基本的な検証も含まれます。
- 問題が顧客の責任範囲にある場合、かかる問題を顧客自身で修正すること。
- SWIFT のサービスと製品の提供を受けることに関連した問題を解決するために、SWIFT 主導で実行されるリカバリーやフォールバック手順、SWIFT により要求されたアクションに対して、適切かつ速やかに対応すること。
- SWIFT のサービスと製品の提供を受けるにあたり、その整合性を損なう可能性があるセキュリティ違反行為もしくは違反未遂を認識した場合、SWIFT に速やかに通知すること。また、顧客は SWIFT のサービスと製品の不正使用 (一部でも全体でも) を認識した場合も SWIFT に速やかに通知しなければなりません。

顧客が SWIFT のサービスと製品を入手、所有、使用する際は、以下を行う必要があります:

- SWIFT により提供された、もしくは SWIFT 用として提供された、現時点で有効なポリシーや指示に従うこと。
- 代替手順のオペレーションを含め、システム上にあるデータの整合性と安全性を保証にすること。また顧客は、意図されていないデータアクセスやディスクロージャーによるデータ損失または破損によって発生する損失や損害に対し、対応策を講じている必要があります。
- 常に適正な業界慣行および関連する全ての適用法令や規制を厳に順守すること。いかなる適用法令、規制、第三者の権利をも侵害しないことを保証するため、また必要に応じ、必要で

あるあらゆる許諾、承認、許可を得ること。これには銀行規制、マネーロンダリング規制法、競争法（独占禁止法）、プライバシー法、個人情報保護法、データ通信法に加え、暗号化の使用やインポート/エクスポート管理を規制する法律が含まれますが、これに制限されるものではありません。

11.2.1.3 アクセス、所有、使用

ユーザーの責任範囲

ユーザーは SWIFT のサービスと製品の使用に関して唯一の（単独の）責任を有しています。

SWIFT のサービスと製品にアクセス、所有、使用するユーザーの権利は個人的なものであり、ユーザーの事業運営のため、もしくは当該状況で適用される SWIFT ポリシーに準じ、SWIFT のサービスと製品へのアクセスまたはその使用が必要である社員もしくはユーザーの責任下にある個人を除き、ユーザーは第三者に対して SWIFT のサービスと製品へのアクセスを許可してはならないものとします。

11.2.1.4 事前の変更通知が必要な場合

ユーザーの手順

ユーザーが基盤（インフラストラクチャ）の変更を行う際、SWIFT から提供されている SWIFT のサービスと製品に対して影響する可能性がある場合は、少なくともその三週間前に SWIFT にその旨を通知する必要があります。これにはユーザーのセキュア IP ネットワーク（SIPN）への接続構成の変更も含まれますが、これに限定されるものではありません。

11.2.1.5 オペレーティング要件

ユーザーの責任範囲

SWIFT のサービスと製品の提供・使用に関して必要なオペレーティング要件を全て保持しているもしくは満たしていることについて、ユーザーは唯一かつ排他的な責任を負うものとします。特にユーザーは、SWIFT のサービスと製品を本サービスディスクリプションで指定されているように使用するにあたり、必要もしくは妥当であるハードウェア、ソフトウェア、およびその他の機器、設備、サービス（必要に応じ、SWIFT もしくはサードパーティのいずれによって提供されたかに関わらず）を入手、使用、保守（必要に応じて）する必要があります。

ユーザーは、かかる機器やサービスの導入、オペレーション、使用、保守（必要に応じて）に必要な全てのライセンスおよび権利を保有しており、これを継続的に維持できることを保証するものとします。さらに、ユーザーはかかる機器やサービスが常に適切に機能していることを保証するものとします。かかる機器やサービスが、PoP や SIPN の、もしくはより一般的に SWIFT のサービスと製品のパフォーマンス、オペレーション、セキュリティを低下させたもしくは妨害した場合、SWIFT はユーザーまたはサードパーティに対していかなる債務を負うことなく、また SWIFT の権利および救済措置を侵害することなく、かかる機器やサービスの全体もしくは一部との接続を直ちに停止する権利に加え、その他の妥当な手段を実行する権利を有するものとします。

11.2.1.6 アクセスと協力

ユーザーが提供するもの

ユーザーは、SWIFT およびその請負業者（コントラクター）もしくは代理業者（エージェンツ）のユーザーエリアへの合理的なアクセスを許可するものとします。またユーザーは、SWIFT が SWIFT のサービスと製品を提供するにあたり、そしてより一般的に SWIFT の義務、権利、救済措置を実行するために必要なものとして合理的に要求する全ての情報、機器、サービスを提供するものとします。

11.2.1.7 守秘義務

ユーザーの守秘義務

ユーザーは、SWIFT およびその供給者の利益のため、SWIFT のサービスと製品およびその関連ドキュメントを機密事項として扱うものとします。

11.2.2 SWIFTNet メッセージング特定のルールと責任範囲

11.2.2.1 サービスアドミニストレーターのルールおよび責任範囲

サービスアドミニストレーター契約

クローズドユーザーグループ (CUG) サービスを設立するにあたり、サービスアドミニストレーターと SWIFT は事前にサービスアドミニストレーションにおける合意 (Service Administration Agreement) を締結しなければなりません。SWIFT 理事会に 1 つもしくは複数の CUG の設立を申請するため、サービスアドミニストレーターは、サービス承認リクエストフォーム (Service Approval Request Form, SARF) に適宜記入および署名の上、SWIFT に返送する必要があります。

合理的な理由に基づき以下の状況が発生した場合、その他の権利や救済措置を侵害することなく、SWIFT は CUG の設立申請を拒否する、および既存の CUG 内における SWIFTNet メッセージングサービスの提供を終了させる権利を有するものとします:

- SWIFTNet メッセージングサービスの提供もしくは使用が、適用法令や規制、第三者の権利を侵害している、もしくは侵害する可能性がある場合
- SWIFTNet メッセージングサービスの提供もしくは使用が、SWIFT の評判、ブランド、業務上の信用や誠意に悪影響を及ぼす、もしくは及ぼす可能性がある場合

サービスアドミニストレーターの特定のルールと責任範囲

サービスディスクリプションに記載されているその他のルールや責任に加え、サービスアドミニストレーターは以下を行う必要があります:

- 関連する全てのクローズドユーザーグループ (CUG) の管理。サービスアドミニストレーターは、制限なく CUG への登録を決定しなければなりません。特に、サービスアドミニストレーターは参加者 (サービスパーティシパント) の CUG への登録を迅速に承認すること、また場合によっては拒否すること、および既に CUG に登録されている参加者 (サービスパーティシパント) の退会を決定する、唯一かつ排他的な責任を負うものとします。
- 関連する CUG での SWIFTNet メッセージングサービスの提供について、SWIFT との主要連絡窓口になります。サービスアドミニストレーターは、制限なく、SWIFT が全ての関連情報、フォーム、その他のドキュメントを既存の参加者 (サービスパーティシパント) および参加者 (サービスパーティシパント) となる見込みのある相手への配布をサポートするものとします。
- 上述のフォームやその他のドキュメントが正確かつ適切に記入および処理されるよう、SWIFT をサポート。
- CUG における SWIFTNet メッセージングサービスの初期サービスパラメータの定義および将来的な修正を、SWIFT と協力および合意の上で遅滞なく実行。
- 全ての参加者 (サービスパーティシパント) が、初期サービスパラメータとその将来的な修正について認識していることを保証する。これには、CUG を設立するコピー先や目的、CUG 内に特定の SWIFT のサービスと製品を導入するための詳細なども含まれます。これは参加者 (サービスパーティシパント) がそのオペレーションを理解し、関連する義務 (特にサー

ビスアドミニストレーターにより定義されたあらゆるサービスパラメータや目的に従って CUG 内における SWIFTNet メッセージングサービスを使用すること、適用法令や規制を順守すること、いかなる第三者やその取引先および顧客の権利を侵害しないこと) の順守を促すためです。

- サービスアドミニストレーターとしての義務を制限なく遂行するために必要な能力および権限を有していることを保証する。上述の義務には、サービスパーティシパントクローズドユーザーグループ (CUG) への登録、拒否、停止させることが含まれます。

サービスアドミニストレーターのロールおよび責任範囲 (詳細)

サービスアドミニストレーターは前述に加えて、以下を実行する必要があります:

- 標準オペレーションルールを使用して、管理しているライブサービス毎に、1つのオペレーションルール (Operational Rules) テンプレートを作成完了および承認する。
- 必要に応じて、テンプレートの内容をアップデートします。サービスアドミニストレーターは、かかるアップデートを自らの裁量により、もしくは SWIFT がテンプレートを変更したことを受けて行うことができます。
- 適用されるテンプレートが、サービスアドミニストレーターが SWIFT に提供したサービスプロファイルに定義したように、対応する SWIFTNet メッセージングサービスにおける SWIFT の構成に常に合致していることを保証します。
- 管理している全てのライブサービスに関して、完了および承認された最新のテンプレートの全内容をサービス登録機関および SWIFT に供します。サービスアドミニストレーターは、SWIFT が新たなテンプレートを利用可能にした日付から 6 ヶ月以内に、もしくは新たなサービスがライブ稼働する日付 (6 ヶ月以降にライブ稼働となるサービスの場合) までにこれを行わなければなりません。また SWIFT は、完了したテンプレートをユーザーに提供する権利を有します。

最後に、サービスアドミニストレーターは、サービス登録機関を関連するサービスのクローズドユーザーグループ (CUG) に登録、拒否、停止させることを含めて、サービスアドミニストレーターとしての義務を制限なく遂行するために必要な能力および権限を有していることを保証しなければなりません。

ノート 不明確さを回避するため、CUG への登録はサービスアドミニストレーターの承認を受けるものとします。

11.2.2.2 顧客の責任範囲

一般的な顧客のロールおよび責任範囲

SWIFTNet メッセージングサービスのユーザーとして、顧客は以下を行う必要があります:

- *SWIFTNet Messaging Operations Guide* に記載されている、ポリシーやその他の顧客の責任の順守
- *SWIFTNet Messaging Operations Guide* に記載されているガイドラインに従い、SWIFT が SWIFTNet FileAct および SWIFTNet InterAct 用として構成したセントラルルーティングルールの指定
- ストアアンドフォワードモードの SWIFTNet InterAct および SWIFTNet FileAct のキューを、少なくとも 5 日に一回は空にする

ノート ストアアンドフォワードモードを使用しているサービスのサービスアドミニストレーターは、キューを空にすることに関してより厳しいルールを義務付けることもできます。

- 本番サービス内のサービス登録機関として承認された最新のテンプレートで、サービスアドミニストレーターが提供しているオペレーションルールが設定された場合、即座に有効となります。

汎用 SWIFTNet FileAct ユーザー

汎用 SWIFTNet FileAct のユーザーは、www.swift.com（限定コンテンツ）で入手可能汎用 SWIFTNet FileAct ディレクトリ（SWIFTNet Services Directory の一部）にて公開されているソリューションに参加することに同意し、ソリューションにおけるオペレーションステータス（テスト/本番）を変更する前に汎用 SWIFTNet FileAct ディレクトリをアップデートする責任を負うものとします。

11.2.3 SWIFTNet PKI：特定のロールと責任範囲

11.2.3.1 登録

正確かつ完全な情報提供

ユーザーは、SWIFTNet 公開鍵基盤（PKI）への登録に際し、正式名称およびセキュリティオフィサー（SO）の身元を含め、正確かつ完全な情報を提供しなくてはなりません。

11.2.3.2 セキュリティオフィサー

任命および人数

ユーザーは、ユーザーのドメイン内にあるエンティティ用の証明書の申請およびその管理をサービスドキュメントに従って行うため、最初に 2 名の SO を任命する必要があります。

ユーザーのドメイン内のエンティティが異なるタイムゾーンにある場合、SWIFT はタイムゾーンごとに少なくとも 1 名の SO を任命するよう推奨します。

SO の身元

ユーザーは、SWIFT とのコミュニケーションにおいて SO が常に正確かつ真正な身元を提示することを保証する必要があります。これには、オンラインまたはオフラインに関わらず、最初の登録手続き、証明書の発行、メンテナンス、破棄要求が含まれます。

ユーザーは、ユーザーのエージェントとの全てのコミュニケーションにおいて、SO が常にエージェントの正しい身元を確認することを保証する必要があります。

義務

ユーザーは、SO が本サービスディスクリプションで定義されている SO の義務およびその権限範囲に従うことを保証する必要があります。不明確さを回避するため、ユーザーは、ユーザーが SO を雇用したがどうかに関わらず、セキュリティオフィサーの行動、過失、不作為に関する責任を常に負うものとします。

SWIFTNet Certificate Administration Guide

ユーザーは、*SWIFTNet Certificate Administration Guide* は SO の優れた実践規範について記述されていると合意するものとします。*SWIFTNet Certificate Administration Guide* は、SWIFT と

ユーザー間におけるいかなる契約にも含まれません。従って、いずれの当事者も *SWIFTNet Certificate Administration Guide* に記述されている条件に何ら縛られるものではありません。

11.2.3.3 エージェント

エージェントの任命

ユーザーは、そのドメイン内にあるエンティティごとに少なくとも 1 エージェントを任命する必要があります。エージェントは、エンティティに関連する有効化シークレット、公開鍵と秘密鍵、パスワードを安全に取扱うこと（ユーザー向けおよびその代理として）に関して責任があります。特定の義務が SWIFTNet サービスで提供されているその他のサービスと矛盾しない場合、エージェントはかかる義務の実行を自動化することができますが、矛盾がある場合には事前に SWIFT の許可を得る必要があります。

エンティティが特定の個人である場合、ユーザーはエージェントとエンティティが同一人物であることを保証する必要があります。

エージェントによるサービスの使用

ユーザーは、そのエージェントが SWIFTNet PKI を使用し、サービスドキュメントに記載されている義務を遂行することを確実にしなければなりません。

エージェントに関するユーザーの責任

不明確さを回避するため、ユーザーはそのエージェントの行動、過失、不作為に関して責任を負うものとします。

11.2.3.4 有効化シークレット、証明書、秘密鍵に関する責任

有効化シークレット

有効化シークレットは、SWIFT がユーザーの組織を承認するために使用する機密情報です。このため、ユーザーは有効化シークレットを保護し、SWIFT が有効化シークレットを提供した際の使用目的内で使用される場合のみ、組織を代表する人物として承認された個人に限定して公開することを保証する必要があります。

証明書の受理

本サービスディスクリプションの“証明書の発行と配布” ページの 113 で説明されている、証明書の発行およびその手続きの正常な完了には、その結果として発行される公開鍵証明書のエージェントによる受理も含まれていることにユーザー（およびユーザーのドメイン内にあるエージェントの代理として）は合意するものとします。

秘密鍵に関する責任

ユーザーは、本条項に基づいてそのドメイン内で証明書を受理し、証明書破棄リスト（Certificate Revocation List、CRL）によりその証明書を破棄していない場合、かかる証明書に対応する秘密鍵に関連するあらゆる行為、過失、不作為に関してユーザーが絶対的な責任を持つと SWIFT が見なすことに合意するものとします。特に、しかしこれに制限されることなく、メッセージまたはファイルに電子署名を付けるために秘密鍵を使用する場合については、ユーザーによる個人的な認証であると SWIFT は見なします。

11.2.3.5 エージェントによる秘密鍵の使用

秘密鍵および証明書破棄要求の保護

ユーザーは、そのセキュリティオフィサー（SO）およびエージェントが本サービスディスクリプションの“ユーザー ロール” ページの 92 および“証明書” ページの 97 に記載されている全ての手順に従い、また適正な業界慣行に従うことを保証する必要があります。

またユーザーは、そのエージェントが本サービスディスクリプションの“エンティティの破棄、回復、無効化” ページの 117 に記載されている手順を即座に実行することを保証する必要があります。

キーおよびパスワードの保護

ユーザーは、本サービスディスクリプションの“公開鍵と秘密鍵” ページの 102 で許可されている範囲を除き（暗号化証明書および簡易署名の検証用の証明書のみ）、証明書に関するあらゆるパスワード、秘密鍵、有効化シークレットを秘密にする必要があります、共有してはならないものとします。

エージェントは、証明書に関するその他の情報についても即座にセキュリティオフィサーに連絡する必要があります。

意図された目的でのみ秘密鍵および証明書を使用

ユーザーは、エージェントが以下の場合においてのみエンティティの秘密鍵の使用を許可することを保証する必要があります：

- 本サービスディスクリプションで別途許可されていない限り、関連するエンティティ（場合によってはエージェント）が使用
- 関連するユーザーの業務目的のために使用
- 関連する証明書が有効であることをエージェントが検証した後に使用
- セキュア IP ネットワークで使用（ビジネス証明書および簡易証明書）

ユーザーは、SWIFTNet メッセージングサービスを使用しているユーザーコミュニティ以外において、エージェントもしくはその他のエンティティの電子署名や証明書の利用をエージェントが許可および可能な状態にしないことを保証する必要があります。

11.2.3.6 取引先の証明書への依存

SWIFTNet InterAct および SWIFTNet FileAct 用の証明書に依存する場合の前提条件

ビジネス証明書、簡易証明書、暗号化証明書に関連する電子署名に依存する事前条件として、ユーザーは取引先がその証明書を SWIFTNet でのみ使用しており、エージェントが以下を正常に確立していることを保証する必要があります：

- 証明書が有効であること。証明書破棄の確認は SWIFT が行いますが、ユーザーレベルでその他の確認も行われます。
- 証明書が期限切れとなっていないこと
- 証明書が、本サービスディスクリプションの“証明書” ページの 97 に記載されている正しいフォーマットであること
- エージェントの意図する利用目的に適切な証明書であること

- ・ 証明書内の識別名 (DN) が署名されたメッセージまたはファイルの識別名と一致し、メッセージまたはファイルに付けられた電子署名が公開検証鍵と対応し、署名が有効であること (証明書が署名されたメッセージまたはファイルと関連して検証されている場合)

SWIFTNet Browse 用のウェブ証明書を利用する場合の前提条件

ウェブ証明書に関連した電子署名を利用する場合の前提条件として、ユーザーはエージェントが以下を正常に確立していることを保証する必要があります:

- ・ 証明書が有効な CA 署名検証用証明書の下で発行されていること
- ・ 証明書が有効であること。
- ・ 証明書が、本サービスディスクリプションの“証明書” ページの 97 に記載されている正しいフォーマットであること
- ・ エージェントの意図する利用目的に適切な証明書であること

SWIFTNet InterAct および SWIFTNet FileAct 用として取引先の署名検証用証明書の利用

取引先の証明書が利用に必要な前提条件を満たしている場合、ユーザーはビジネス証明書に関連した電子署名を利用することができます。

取引先の証明書の利用は、ユーザーの業務目的の場合のみ、また以下の範囲内においてのみ可能となります:

- ・ 証明書に対応する秘密鍵の使用は、証明書の当該ユーザードメイン内にあるユーザーに帰属させることができます。これはユーザーレベルでの発信元の否認防止となります。
 - ・ 電子署名により署名されたファイルダイジェストまたはメッセージが、送信時から変更されていないこと。これはメッセージまたはファイルの整合性を保つためです。
 - ・ SWIFT またはユーザーが属している CUG との間で合意されている、その他の利用方法
- 上述されたもの以外の署名検証用証明書の利用は、全てユーザーの責任となります。

SWIFTNet InterAct および SWIFTNet FileAct 用として取引先の暗号化証明書の利用

取引先の証明書が利用に必要な前提条件を満たしている場合、本サービスディスクリプションの“フォーマット” ページの 97 および“公開鍵と秘密鍵” ページの 102 に記載されている通り、暗号化を使用するユーザーは暗号化秘密鍵および暗号化証明書を使用する必要があります。

暗号化を使用するユーザーは、暗号化秘密鍵および暗号化証明書を利用することができます。この場合の利用は、ユーザーの業務目的、および暗号化証明書を使用して暗号化されたシンメトリックキーの機密性を保証するためだけに行われるものとします。

SWIFTNet InterAct および SWIFTNet FileAct の暗号化証明書の利用は、本トピックで記述されているもの以外、全てユーザーの責任となります。

取引先の SWIFTNet Browse 用ウェブ証明書の利用

取引先の証明書が利用に必要な前提条件を満たしている場合、ユーザーはウェブ証明書を使用して構築したセキュアなセッション (安全なセッション) を利用することができます。

ウェブ証明書の利用は、ユーザーの業務目的のため、もしくは以下の範囲内においてのみ行われるものとします:

- ・ セキュアセッションに参加しているエンティティを持っているユーザーの識別
- ・ セキュアセッション中のデータ交換の整合性評価
- ・ セキュアセッションの機密性の保証

- ・ SWIFT またはユーザーが所属している CUG との間で合意されているその他の利用方法
上述されたもの以外のウェブ証明書の利用は、全てユーザーの責任となります。

11.2.3.7 サービスビューロー

サービスビューローに対するユーザーの責任

ユーザーは、必要に応じて、サービスドキュメントに基づいて特定の権利および義務を行使するため（例えばユーザーの SO が持つ日常的な機能全体もしくはその一部を解除するなど。ただしこれに限定されるものではありません）自らの裁量および責任でサービスビューロー（またはサービスビューローの責任下にある特定の個人）を指定することができます。

不明確さを回避するため、これはサービスドキュメントに定められたユーザーの義務の変更または軽減するものではなく、SWIFT はサービスビューロー（またはその責任下にある特定の個人）のあらゆる行為、過失、不作為をサービスビューローに関連するユーザーのものとし見なします。

11.2.3.8 HSM

HSM に関するユーザーの責任

HSM 機器の選択、インストール、利用はユーザー単独の責任となります。ユーザーは、SWIFT に関連する機器の利用に関して、ガイドラインや指示に必ず従う必要があります。関連するドキュメントおよび契約条件の利用は、ユーザーの責任となります。

11.2.4 セキュア IP ネットワークに特定のルールへのアクセスサービスと責任範囲

11.2.4.1 セキュア IP ネットワークへの接続

ダイヤルアップ回線での接続

ユーザーは、SWIFT が指定した Point of Presence (PoP) に接続するために必要なサービスや機器を所有および保守する必要があります。特に、ユーザーは SWIFT が指定した供給者に仮想プライベートネットワーク (VPN) ボックスを発注し、公衆交換電話網 (PSTN) 回線とモデム（例外的な状況においては、総合デジタル通信網 [ISDN] 回線とターミナルアダプタ）を信頼できる任意の供給者に発注する必要があります。

ユーザーがすべての前提条件を満たしている場合、ユーザーのネットワーク接続を有効化するのには SWIFT の責任となります。より詳細については“SWIFT のルールと責任範囲” ページの 123 を参照してください。

専用回線での接続

常時接続回線で接続する場合、ユーザーはセキュア IP ネットワーク (SIPN) の接続と VPN ボックスの購入を、指定のネットワークパートナーを通じて行う必要があります。

指定のネットワークパートナーの国別リストが www.swift.com > Partners > Network Partners に掲載されています。これらのネットワークパートナーは、SWIFT と合意した技術要件およびパフォーマンス要件に従ってユーザーにインターネットプロトコル - 仮想プライベートネットワーク (IP-VPN) 接続を提供することに同意しています。

ネットワークパートナーの選択、および SWIFT が定義もしくは SWIFT 向けに定義された仕様やその他の要件に従って SIPN に接続するためのネットワークパートナー（一社もしくは複数）との契約は、ユーザーが完全かつ排他的に責任を負うものとします。

ノート Dual-I 構成の場合、ユーザーはダイヤルアップ回線と専用回線のコンポーネントをそれぞれ別個に扱う必要があります。また、ユーザーは専用回線およびダイヤルアップ回線のサービス条項に記載されている全ての前提条件に対処する必要があります。

回線の耐障害性

SWIFT は、単一障害点（single points of failure）に対して高い耐障害性と保護を提供するように接続パックを設計しています。しかし、SWIFT の直接管理化にない要素に関して、SWIFT は上述のような保護を自動的に保証することはできません。特に Dual-P 構成の場合、SWIFT は 2 本の専用回線、もしくは 2 つのアクセスポイントの分散については保証できません。

ユーザーは以下を実行する必要があります：

- 専用回線の分散が必要であることをネットワークパートナーに指示する
- PoP の分散が導入されていることをネットワークパートナーに確認する

ネットワークアクセス

SWIFT は、SWIFTNet メッセージングサービスに適格かつ登録しているユーザーに限定してネットワークアクセスを提供しています。

SWIFT は、ユーザーに侵入テストやその他の危害を与える可能性があるアクセスを許可していません。

稼働前に、ユーザーは全ての代替回線を含めた接続パック構成全体をインストールする必要があります。例えばユーザーが Dual-I 接続構成を選択した場合、ユーザーが両方の回線（専用回線と代替回線）をインストールし、全ての回線でオペレーション可能であることが確認された時点で、インストールが完了したと見なされます。SWIFT は一部分のみのインストールを認めていません。

SWIFT の法的責任

不明確さを回避するため、また適用される法律で禁止されていない限り、ユーザーのネットワークプロバイダーの選択およびネットワークプロバイダー（ネットワークパートナーを含む）が提供するサービスや設備機器に関して、SWIFT は何ら責任を負うものではありません。SWIFT は、ネットワークプロバイダー（ネットワークプロバイダーを含む）および当事者がユーザーに提供するサービスおよび設備機器に関して、明示あるいは非明示を問わず、法定ないしその他の方法で定められているあらゆる保証を明確に除外し放棄するものとします。これには、制限なしに当事者が提供するサービスの品質に関するあらゆる保証についても含まれます。また、これはネットワークパートナーの財政状態および資本力についても同様です。

前述の事項は、SIPN に接続するにあたり、サービスおよび製品の提供元（VPN ボックスなど）としてユーザーが選択した全ての供給者に等しく適用されます。

11.2.4.2 ユーザーの利用（用途限定）

用途限定の受諾

ユーザーは、仮想プライベートネットワーク（VPN）ボックス、および公衆交換電話網（PSTN）もしくは ISDN 回線（いずれもダイヤルアップ回線での接続の場合）を、セキュア IP ネットワーク（SIPN）に接続するためにのみ使用することに合意するものとします。

11.2.4.3 VPN ボックスの取扱い

概要

ユーザーは所有している全ての VPN ボックスを大切に取扱うものとし、SWIFT 向けに規定、もしくは SWIFT が規定した、または VPN ボックスの製造メーカーもしくはプロバイダーが規定したあらゆる要件、指示、その他の契約条件に従うものとしします。

ユーザーは、ネットワークパートナーがインストールする接続パックのいかなるコンポーネントも改竄してはいけません。特に、SWIFT から明確に別途指示されていない限り（例えばテスト目的でなど）、ユーザーは VPN ボックスおよびルーターの変更、改変、改竄を行ってはならないものとしします。ネットワークパートナーがこれらの機器をインストールした後、ユーザーは VPN ボックス、ルーター、ISDN ターミナルアダプタ、PSTN モデムのコンセントを抜いたり、電源を切ったりしてはならず、またそれらの機器の接続やケーブルを改竄してはならないものとしします。

VPN ボックスのコンセントを抜いたり、電源を切る必要がある場合（メンテナンス目的でなど）、ユーザーは少なくともその一週間前までに SWIFT にその旨を連絡しなければなりません。連絡がない場合、VPN ボックスの喪失は自動的に接続障害として検知され SWIFT の障害修正メカニズムが有効となるため、VPN ボックスの停止時間が事前に計画され SWIFT と合意されていることは非常に重要です。

11.2.4.4 SNL-VPN 接続

ルールと責任

SWIFTNet Link (SNL) と VPN ボックス間の接続は、ユーザー単独の責任となります。ユーザーは、接続が安全であることを保証し、SWIFT のサービスおよび製品の不正使用、およびその整合性や信頼性を損なう可能性があるセキュリティ違反行為から保護する必要があります。

安全な接続に関するより詳細な情報は、“SWIFTNet 技術環境” ページの 68 を参照してください。

SNL と VPN ボックス間の安全な接続に関してユーザーをサポートするため、SWIFT は構成要件の仕様をドキュメント化しています。ユーザーが、同一場所にはない構成（SNL と VPN ボックスがユーザーの直接管理下にはない）を選択した場合、これらの構成要件は必須であり、ユーザーは SWIFTAlliance Gateway または専用のセキュアネットワークリンクを使用するいずれかの必須構成から選択しなければなりません。

構成要件に関するより詳細な情報は、*SWIFTNet Network Access Control Guide* を参照してください。