

Genesys 7.6

Security

Deployment Guide

このマニュアルに記載されている内容は所有権付きの機密情報であり、Genesys Telecommunications Laboratories, Inc. の書面 による事前の承諾がない限り開示も複製もできません。

Copyright © 2007-2008 Genesys Telecommunications Laboratories, Inc. All rights reserved.

Genesys について

Genesys Telecommunications Laboratories, Inc. は Alcatel-Lucent 社の子会社であり、コール センター向けソフトウェアを事業の柱 としています。インタラクション(情報のやり取り)を適切に進めることが事業の成功をもたらし、企業の評価につながると Genesys は認識しています。この認識に基づいて Genesys が提供する顧客サービス ソリューションは、80 か国に及ぶグローバル 2000 企 業、政府機関、電気通信サービス事業者を対象に、毎日1億件を超える顧客のインタラクションを管理しています。音声、電子メー ル、Web といったチャネル間での洗練されたルーティング、およびレポート処理によって、顧客の求める最適なリソースへの接続 を迅速に、しかも一度で可能にします。Genesys は、顧客サービス、ヘルプ デスク、オーダー デスク、回収業務、電話によるセー ルスやサービス、ワークフォース管理などの業務向けに ソリューションを提供しています。詳細については、 http://www.genesyslab.com にアクセスしてください。

どの製品にも個別のオンライン マニュアルが用意されていて、Genesys テクニカル サポートの Web サイト上か、または Genesys に連絡して入手できる Documentation Library DVD で閲覧できます。詳細については、営業担当者にお問い合せください。

注意

このマニュアルでは、発刊時の完全かつ正確な内容記載を実現するよう細心の注意が払われていますが、もしなんらかの誤りがあっても Genesys Telecommunications Laboratories, Inc. はその責任を負うことはできません。このマニュアルに記載されている情報の 変更または修正(あるいはその両方)は、今後のバージョンに反映されます。

システムのセキュリティについてのお客様の責任

ご使用のシステムのセキュリティについては、お客様が責任を負うものとします。無断使用を防ぐための製品管理についても、お客様が責任を負うものとします。システム管理者は、この製品に付属しているすべてのマニュアルに目を通して、装備された機能を完 全に理解する必要があります。これにより、Genesys 製品のライセンス外使用による余計な経費がかからないようにすることがで きます。

商標

Genesys、Genesys のロゴ、および T-Server は、Genesys Telecommunications Laboratories, Inc. の登録商標です。このマニュアル で参照されている他の商標および企業名はすべて、他社が所有権を有します。Crystal モノスペース フォントは、Software Renovation Corporation (www.SoftwareRenovation.com)の許可のもと使用されています。

VAR が提供するテクニカル サポート

VAR (value-added reseller : 付加価値再販業者)からサポート契約を購入した場合、テクニカル サポートについては当該 VAR にお 問い合せください。

Genesys が提供するテクニカル サポート

Genesys から直接サポート契約を購入した場合、以下の各地域の Genesys テクニカル サポート窓口までお問い合せください。

地域	電話	電子メール
北米、中南米	+888-369-5555 または +506-674-6767	<pre>support@genesyslab.com</pre>
欧州、中東、アフリカ	+44-(0)-118-974-7002	<u>support@genesyslab.co.uk</u>
アジア太平洋	+61-7-3368-6868	<pre>support@genesyslab.com.au</pre>
日本	+81-3-6361-8950	<pre>support@genesyslab.co.jp</pre>

テクニカル サポート窓口にお問い合せいただく前に、連絡先の情報、および手順全般について*『*Genesys Technical Support Guide』 を参照してください。

注文、およびライセンス情報

Genesys 製品の注文、およびライセンスに関する情報全般については、『Genesys 7 Licensing Guide』を参照してください。

発行元

Genesys Telecommunications Laboratories, Inc. <u>www.genesyslab.com</u>

マニュアルバージョン: 76g_dep-security_03-2008_v7.6.001.00



目次

	手順目次	7
本書について		9
	対象読者	10
	章の要約	10
	表記上の規則	12
	関連資料	14
	このマニュアルに関するご意見	14
第1章	はじめに	15
	概要	
	データの機密保護と整合性	
	サービスの可用性	16
	サービスの整合性	16
	セキュリティ構築	17
	セキュリティおよび標準に関する適合性	17
パートI	データの機密保護と整合性	19
第2章	新規ユーザのデフォルト アクセス禁止	21
	機能の要約	
	セキュリティ上の利点	21
	サポートするコンポーネント	22
	機能の説明	
	機能の設定	22
	設定オプション	23
第3章	アクティビティなしのタイムアウト	25
	機能の要約	25
	セキュリティ上の利点	25
	サポートするコンポーネント	26

	機能の説明	
	機能の設定	27
	設定オプション	27
第4章	ログの特定データの非表示	29
	機能の要約	29
	セキュリティ上の利点	
	サポートするコンポーネント	
	機能の説明	
	機能の設定	
	設定オプション	
第5章	ログイン時のセキュリティ パナー	
	機能の要約	
	セキュリティ上の利点	34
	サポートするコンポーネント	
	機能の説明	34
	機能の構築	
	アプリケーション設定中のセキュリティ バナーのインストー	・ル37
	レジストリによるセキュリティ バナーの設定	41
パート II	サービスの可用性	49
第6章	アプリケーションの冗長性	51
	機能の要約	51
	セキュリティ上の利点	51
	サポートするコンポーネント	51
	機能の説明	52
	冗長タイプ	53
	機能の設定	56
第7章	プロキシ サーバとパラレル サーバ	57
	機能の要約	57
	セキュリティ上の利点	
	サポートするコンポーネント	
	機能の説明	
	機能の設定	

パート III	サーバ整合性 —Transport Layer Security	61
第8章	Genesys Transport Layer Security の紹介	63
	機能の要約	63
	セキュリティ上の利点	64
	サポートするコンポーネント	64
	環境の前提条件	66
	略語	66
第9章	Security Pack のインストール	67
	サポートされるオペレーティング システム	67
	Security Pack のインストール	68
第 10 章	証明書の生成とインストール	71
	OpenSSL を使用した証明書生成	71
	· 認証機関の設定	72
	CA を使用した証明書生成	74
	証明書のインストール	75
	Windows 証明書サービスを使用した証明書生成	78
	証明書の生成	79
	証明書の取得	84
	MMC を使用した証明書の管理	84
	証明書管理のための MMC の設定	84
	証明書のエクスポート	85
	PKCS #12 から PEM への変換	87
	リモート コンピュータからの証明書の取得	87
第11章	Genesys TLS の設定	89
	概要	89
	安全なポートの設定	90
	セキュリティ証明書の割り当て	91
	ホストへの証明書の割り当て	92
	アプリケーションへの証明書の割り当て	96
	ポートへの証明書の割り当て	100
	ホスト証明書を使用するためのサーバ アプリケーションの設定	102
	安全なクライアント接続の設定	103
	Configuration Server との安全な接続	105
	Configuration Server と DB Server 間の安全な接続の設定	107

	安全な HA 同期接続の設定	111
	冗長サーバの設定	111
第 12 章	Genesys TLS のトラブルシューティング	115
	安全な接続を確立できない場合	115
パートIV	サーバ整合性 — クライアント側ポート定義	117
第 13 章	クライアント側ポート定義	119
	機能の要約	119
	セキュリティ上の利点	
	サポートするコンポーネント	120
	既知の問題と推奨事項	120
	機能の設定	121
	作業の流れ	121
	Configuration Server 接続の設定	121
	クライアント接続の設定	127
索引		131





手順目次

アプリケーション設定中のセキュリティ バナーのインストールと設定38
要約 — 冗長アプリケーションの設定
UNIX への Security Pack のインストール
サーバ タイプのアプリケーションの安全なポートの設定
ホストへの証明書の割り当て92
以前に割り当てた証明書のホストからの削除
アプリケーションへの証明書の割り当て
以前に割り当てた証明書のアプリケーションからの削除
ポートへの証明書の割り当て100
以前に割り当てた証明書のポートからの削除101
ホスト証明書を使用するためのサーバ アプリケーションの設定102
安全なクライアント接続の設定104
Configuration Server の自動検出ポートの設定106
DB Server と Configuration Server の構成ファイルの変更108
冗長サーバ間の安全な接続の設定
Installation Wizard (インストール ウィザード)を使用した Configuration Server との接続の設定 (UNIX の場合)
Installation Wizard (インストール ウィザード)を使用した Configuration Server との接続の設定 (Windows の場合)123
手動による Configuration Server との接続の設定
Configuration Manager を使用した Configuration Server の クライアント接続への追加
クライアント接続の設定





本書について

*『Genesys 7.6 Security Deployment Guide』*をご利用いただき、ありがとうござい ます。このマニュアルは最新のリリース7.6のためのもので、Genesysソフト ウェアのいくつかのセキュリティ機能の構築と構成について説明しています。 このマニュアルは、同製品のリリース7.6に対してのみ有効です。

注: このマニュアルで、Genesys のすべてのセキュリティ機能を取り上げているわけではありません。多くのセキュリティ機能が、Genesys の他のマニュアルで説明されています。たとえば、『Framework 7.6 Deployment Guide』にはユーザ管理についての情報が記載されています。これらは広範な機能であるため、このマニュアルでは、すべてのセキュリティ上のニーズを1か所にまとめて簡単に説明しています。
 同製品の他のリリース用に作成されたこのマニュアルのバージョンに

ついては、Genesys テクニカル サポートの Web サイトにアクセスしてく ださい。また、Genesys Order Management から電子メール (<u>orderman@genesyslab.com</u>) で Documentation Library CD をご注文い ただけます。

この序文では、このマニュアルの概要について説明し、主な読者を明示しま す。また、表記上の規則についても説明し、参考資料を紹介します。以下の項 から構成されます。

- 対象読者(10ページ)
- 章の要約(10ページ)
- 表記上の規則(12ページ)
- 関連資料(14ページ)
- ・ このマニュアルに関するご意見(14ページ)

Genesys ソフトウェアには、多くのセキュリティ機能が組み込まれています。 主なものを以下に示します。

- 認証
- 許可
- 監査トレール
- データ抑止
- データ暗号化
- 安全な接続

この『Deployment Guide』では、これらのセキュリティ機能を設定するために 必要な手順について説明します。一部の機能は、共に使用する個々のコンポー ネントに合わせてカスタマイズできます。その場合は、セキュリティ機能をカ スタマイズする詳細について、『Deployment Guide』や『User's Guide』などの 製品マニュアルを参照してください。

対象読者

このマニュアルは、主にシステムインテグレータ、システム管理者、コンタ クトセンター管理者、オペレータを対象としており、以下の項目についての 基本的知識が必要です。

- CTI (Computer-Telephony Integration:コンピュータとテレフォニーの統合)
 に関する概念、処理、用語、アプリケーション
- ネットワークの設計と運用
- ご使用のネットワーク構成

最新リリースの製品マニュアルに記載されているGenesys製品のアーキテク チャと機能についても熟知している必要があります。

章の要約

このマニュアルでは、いくつかのセキュリティ機能の構築について説明します。安全な環境を計画する際に役立つように、以下のように構成されています。

15ページの第1章「はじめに」では、コンタクトセンターが直面するリスクと情報流出の種類について説明し、対策となる Genesys のセキュリティ機能を取り上げます。

パートI:データの機密保護と整合性

このパートでは、無許可のユーザからデータを保護するためのセキュリティ機能について説明します。

- 21ページの第2章「新規ユーザのデフォルトアクセス禁止」では、新規 ユーザにアクセス権が自動的に付与されることを防ぐ方法について説明 します。
- 25ページの第3章「アクティビティなしのタイムアウト」では、アクティ ビティなしの時間の設定について説明します。この時間がすぎると、表示 されたすべてのデータが非表示になり、ユーザが作業を続けるためには再 度認証が必要になります。
- 29 ページの第4章「ログの特定データの非表示」では、ログとログレポートにユーザが必要とする項目だけを表示する方法について説明します。



 33ページの第5章「ログイン時のセキュリティバナー」では、ユーザがシ ステムにログインしたときに表示できるセキュリティバナーを設計して 構成する方法について説明します。

パートII:サービスの可用性

このパートでは、中断のないデータアクセスを可能にするセキュリティ機能について説明します。

- 51ページの第6章「アプリケーションの冗長性」では、システムが中断なく機能するように、冗長アプリケーションを構成する方法について説明します。
- 57ページの第7章「プロキシサーバとパラレルサーバ」では、効率的に サービスを提供し、サーバ障害によるサービスへの影響を最小限にするために、プロキシサーバとパラレルサーバを構成する方法について説明します。

パートIII: サービス整合性 — Transport Layer Security

このパートでは、Genesys TLS (Transport Layer Security)機能を使用して、転送 中にデータを保護するためのセキュリティ機能について説明します。

- 63ページの第8章「Genesys Transport Layer Security の紹介」では、Genesys TLS 実装の概要と特定の Genesys の構築に合わせた一般的ガイドラインに ついて説明します。
- 67ページの第9章「Security Pack のインストール」では、Genesys Security Pack を UNIX にインストールして構成する方法について説明します。
- 71ページの第 10章「証明書の生成とインストール」では、証明書生成のために、オープン ソースの OpenSSL ツールと Windows 証明書サービスを使用する一般的手順について概要を説明します。
- 89ページの第 11章「Genesys TLS の設定」では、安全な接続でセキュリティ 証明書を使用するために、Genesys アプリケーションを構成する方法について説明します。
- 115 ページの第 12 章「Genesys TLS のトラブルシューティング」では、ご使用の環境における TLS のトラブルシューティングについて説明します。

パートⅣ: サービス整合性 – クライアント側ポート定義

このパートでは、Genesysのクライアント側ポート定義を使用して、転送中に データを保護するためのセキュリティ機能について説明します。

 119ページの第13章「クライアント側ポート定義」では、特定のサーバア プリケーションに接続するためのクライアントパラメータの指定方法に ついて説明します。

表記上の規則

このマニュアルでは、いくつかの表記上の規則を採用しています。この項では、特定の情報に関する概要を記載しています。

マニュアル バージョン番号

このマニュアルの表紙裏の下部には、マニュアルバージョン番号が記載されています。バージョン番号は、このマニュアルに新しい情報が追加されると変更されます。以下にバージョン番号の例を示します。

g_dep-security_03-2008_v7.6.001.00

このマニュアルについてGenesysテクニカル サポートへお問い合せいただく際 には、この番号が必要になります。

字体スタイル

斜体

このマニュアルでは、強調、マニュアルのタイトル、専門的な用語の定義(または初回参照時)、および数学的な変数を表す目的で斜体が使用されます。

- **例**: 詳細については、『Genesys 7 Migration Guide』を参照してください。
 - *慣例、および恒例*は、特定の業界や職業で一般的に認知、および実施され る行為を指します。
 - このオプションには、この値を使用しないでください。
 - 数式を表す場合。たとえば、「x+1=7でxが表すのは...」。..

モノスペース フォント

teletypeやtypewritertextのように表記されるモノスペースフォントは、プログラミングの識別子やGUI要素を表す目的で使用されます。

この対象には、ディレクトリ、ファイル、フォルダ、構成オブジェクト、パ ス、スクリプト、ダイアログボックス、オプション、フィールド、テキスト、 リストボックス、操作モード、ラジオボタンを含むすべてのボタン、チェッ クボックス、コマンド、タブ、CTIイベント、エラーメッセージなどの名前、 オプションの値、論理引数、コマンド構文、コード例などが含まれます。

- **例:** [Show variables on screen] チェック ボックスをオンにします。
 - [Summation] ボタンをクリックします。
 - [プロパティ]ダイアログボックスで、実際の環境のホストサーバの値を 入力します。
 - [Operand] テキストボックスに数式を入力します。
 - [OK] をクリックし、[プロパティ] ダイアログ ボックスを閉じます。

- 以下の表に、EventError イベントの発生時に T-Server が送信する全エ ラーメッセージを示します。
- inbound-bsns-calls オプションに真を選択した場合、ローカル エージェントで確立されたインバウンド通話はすべてビジネス通話として認識されます。

モノスペースは、構成やインストールの手順、またはコマンドラインで、ユー ザが手動で入力する必要のあるテキストを表す場合にも使用されます。

例: • コマンドラインに exit と入力します。

このマニュアルで使用される画面キャプチャ

このマニュアルで使用する画面キャプチャは製品GUI (graphical user interface: グラフィカルユーザインタフェース)から取得されていますが、スペル、大文 字の使い方、文法など、小さな誤りが含まれている場合があります。これに該 当する誤りについては、訂正により製品のインストール、構成、および通常の 利用に問題が生じる場合を除いて、画面キャプチャにテキストを付記する形で 説明しています。たとえば、オプション名に慣用上の誤りが含まれている場合 でも、当該オプション名が製品GUIでそのまま表示されていれば、その誤りは 上記の方法では訂正されていません。

角かっこ

角かっこは、論理引数、コマンド、プログラミング構文に含まれるオプション に該当する特定のパラメータや変数を表します。該当するパラメータや値は、 コマンド、引数、コードブロックの処理が行われるうえで必須ではありませ ん。このオプション情報を使用するかどうかは、ユーザが判断します。以下に 例を示します。

smcp_server -host [/flags]

不等号かっこ

不等号かっこは、ユーザが指定する必要のある値のプレースホルダを表しま す。エンタープライズ環境に固有のDNやポート番号などが該当します。以下 に例を示します。

```
smcp server -host <confighost>
```

関連資料

必要に応じて下記に示す資料も参照してください。

- Genesys Documentation Library DVD に収録されている 『Genesys Technical Publications Glossary』。このマニュアルで使用されている Genesys と CTI の 用語、および頭字語の広範なリストを提供しています。
- 同じく Genesys Documentation Library DVD に収録されている『Genesys 7 Migration Guide』。Genesys 製品リリース 5.1 以降から Genesys 7.x リリース 全般への移行戦略が記載されています。詳細については、Genesys テクニ カル サポートにお問い合せください。
- この製品のRelease Notes (リリースノート)およびProduct Advisories (製品 に関するアドバイス)は、Genesys テクニカル サポートの Web サイト (http://genesyslab.com/support)で入手できます。

サポートされているハードウェアやサード パーティ ソフトウェアに関する情報については、Genesysテクニカル サポートのWebサイトで公開されている以下のマニュアルで入手できます。

- *[Genesys Supported Operating Systems and Databases.]*
- [Genesys Supported Media Interfaces]

Genesys 製品マニュアルは、以下の場所から入手できます。

- Genesys テクニカル サポートの Web サイト (http://genesyslab.com/support)。
- Genesys Documentation Library CD。これは、Genesys Order Management より、 電子メールで注文できます。アドレスは<u>orderman@genesyslab.com</u>で す。

このマニュアルに関するご意見

このマニュアルに関するご意見/ご要望は、

Techpubs.webadmin@genesyslab.comまで、電子メールでお寄せください。

記載内容の誤りや欠落、不正確な点、構成、取り扱うテーマ、範囲など、この マニュアルに関するご意見をお待ちしています。ご意見の内容については、こ のマニュアルに記載された内容とその記載要領に限定させていただきます。製 品自体に関するご意見については、Genesysテクニカルサポートまでご連絡く ださい。

お客様からご意見をお寄せいただいた時点で、そのご意見については、お客様 に対する一切の義務を負うことなく、Genesysが適切であるとみなす任意の方 法で使用、および配布する非排他的権利がGenesysに与えられるものとします。





はじめに

この章では、コンタクトセンター環境に固有のセキュリティ上のリスクと要件の概要、およびこうしたリスクに対するGenesysの対応策について説明します。

この章は、以下の項から構成されます。

- 概要(15ページ)
- データの機密保護と整合性(16ページ)
- サービスの可用性(16ページ)
- サービスの整合性(16ページ)
- セキュリティ構築(17ページ)
- セキュリティおよび標準に関する適合性(17ページ)



データ ネットワークに固有のリスクと脅威は、コンタクト センターにも該当 します。一般に、コンタクト センター ソリューションに共通するリスクは、 以下のカテゴリに分類されます。

- データの機密保護と整合性
- サービスの可用性
- サービスの整合性

この章では、これらのリスクについて1つずつ説明し、対策となるGenesysのセキュリティ機能について取り上げます。

注: このマニュアルで、Genesys のすべてのセキュリティ機能を取り上げて いるわけではありません。多くのセキュリティ機能が、Genesys の他の マニュアルで説明されています。たとえば、『Framework 7.6 Deployment Guide』にはユーザ管理についての情報が記載されています。このマニュ アルは、機能の展開に合わせて記述されており、それぞれのセキュリ ティ機能について1か所にまとめて簡単に説明されています。

データの機密保護と整合性

無許可のデータアクセスとユーザアクセス権の乱用は、マルチユーザ環境に 共通の問題です。データの正確さの確保と、そのライフサイクル中にデータを 即座に利用できることがビジネスに必須の条件です。データ、ソフトウェア、 または構成が、無許可のユーザによって破壊されたり改ざんされることを防ぐ 必要があります。

顧客の機密情報の流出は、コンタクトセンターに対する訴訟や顧客を失うこ とにつながる可能性があります。プライバシとして、顧客が所有するデータだ けでなく、トランザクションと呼の統計、場合によっては特定のコンタクトセ ンターの顧客であるという身元も保護する必要があります。

Genesys では、ユーザ認証などの標準的なセキュリティ機能に加えて、データの機密保護のために以下のセキュリティ機能も用意しています。

- 新規ユーザのデフォルトアクセス禁止
- アクティビティなしのタイムアウト
- ログイン時のセキュリティバナー
- ログの特定データの非表示

サービスの可用性

コンタクトセンターのサービスやサービス利用の中断は、直接的な収入の減少 や顧客の不満につながる可能性があります。オンラインサービスでは、ダウン タイムを最小限にし、完全なパフォーマンスを維持することが最優先事項です。 可用性とは、堅牢で質の高いソフトウェアを使用し、ネットワークへの侵入と DoS攻撃を防止し、冗長サーバ構成を使用して、ネットワークリソースとコン ピュータリソースを保護することです。

Genesys では、サービス可用性のために以下のセキュリティ機能を用意しています。

- 冗長性
- プロキシサーバとパラレルサーバ

サービスの整合性

16ページの「データの機密保護と整合性」で述べたように常駐するデータを保護するだけでなく、通信チャンネルを介して送信されるときもデータを保護する必要があります。

Genesys では、データとサービスの整合性のために以下のセキュリティ機能を 用意しています。

- TLS (Transport Layer Security)
- クライアント側ポート定義

セキュリティ構築

このマニュアルでは、上述の項で述べたGenesysのセキュリティ機能のそれぞれについて説明します。これらの機能をシステム全体にインストールする場合、またはすべての製品に一貫性を持つようにインストールする場合の構築手順の詳細についても説明します。コンポーネントや製品によって構築プロセスが異なる場合は、特定の手順について、該当する製品マニュアルを紹介しています。

機能の構築の一部を別の手順の一部として行う場合は、このマニュアルにはそ の手順の概要だけが記載されています。手順の詳細については、該当する製品 マニュアルを紹介しています。

セキュリティおよび標準に関する適合性

Genesys製品は、コンタクトセンターソリューションの完全な機能の一部を構成するものとして設計されており、ソリューションにはGenesys以外のコン ポーネントと顧客のシステムが含まれることがあります。Genesys製品は、顧客が独自のコンタクトセンターソリューションを設計するために適切な柔軟性を備えています。このため、顧客がGenesys製品を使用して、EDPD (European Data Protection Directive:欧州データ保護指令)、ISO 177999、HIPAA、PCI DSSなどのセキュリティ関連の業務標準に準拠することが可能です。ただし、Genesys製品は顧客が使用する単なるツールであり、こうした標準の準拠を保証または強制するものではありません。Genesys製品の使用によってこうした業務標準に準拠するかどうかは、すべて顧客の責任になります。こうした業務標準だけでなく、地域の該当するセキュリティ要件にも準拠するように、顧客が適切な手段を講じることをお奨めします。





パート

データの機密保護と整合性

このマニュアルのパート I では、データを安全に保護し、整合性を確保するためにGenesysが提供する機能について説明します。以下の章から構成されます。

- 21 ページの第2章「新規ユーザのデフォルトアクセス禁止」
- 25ページの第3章「アクティビティなしのタイムアウト」
- 29ページの第4章「ログの特定データの非表示」
- 33ページの第5章「ログイン時のセキュリティバナー」

パート I: データの機密保護と整合性





新規ユーザのデフォルト アクセス 禁止

この章では、新規ユーザにアクセス権が自動的に付与されることを防ぐ方法について説明します。

この章は、以下の項から構成されます。

- 機能の要約(21ページ)
- 機能の説明(22ページ)
- 機能の設定(22ページ)

アクセス権とアクセス グループの詳細については、『Framework 7.6 Deployment Guide』を参照してください。

機能の要約

デフォルトでは、リリース7.6アプリケーションで作成される新規ユーザに、自動的にデフォルト特権が割り当てられることはありません。つまり、新規ユー ザにはまったく特権がなく、インタフェースにログインしたり、デーモンア プリケーションを使用することはできません。システム管理者または適切なア クセス権を持つ別の既存ユーザが、新規ユーザに適切なアクセス権を与える必 要があります。

デフォルトではこの機能が有効です。これはリリース7.6で作成する新規ユー ザだけに適用されます。必要に応じてこの機能を無効にできます。

セキュリティ上の利点

GUI (Graphical User Interface: グラフィカル ユーザ インタフェース)で直接作 成したり、SDK (Software Development Kit: ソフトウェア開発キット)を使用し たり、新規ユーザはさまざまな方法で作成できます。新規ユーザにすべてのデ フォルト特権や特定のデフォルト特権を与える必要がない場合もあります。こ の機能は、ユーザの作成方法に関係なく、ユーザにデフォルト特権が割り当て られることを防止します。

サポートするコンポーネント

この機能はConfiguration Managerで設定します。Configuration Server 7.5以前で はサポートされません。

Genesys Desktop

Genesys Supervisor Desktopは無料の機能をサポートします。詳細については、 *『Genesys 7.6 Desktop Deployment Guide』*を参照してください。

機能の説明

リリース7.6以前では、システムに新規ユーザが追加されると、自動的にデフォルト特権が割り当てられました。この機能が逆になります。リリース7.6で作成する新規ユーザは、自動的にデフォルト特権が割り当てられることはありません。つまり、新規ユーザにはまったく特権がなく、インタフェースにログインしたり、デーモンアプリケーションを使用することはできません。システム管理者または新規ユーザのアカウント変更のアクセス権を持つ既存ユーザが、新規ユーザを明示的に適切なアクセスグループに追加する必要があります。

デフォルトでは、この新機能はリリース7.6で作成したユーザのみに適用され ます。また、必要に応じて機能を無効にできます。

前リリースとの 互換性 りリース7.5以前のConfiguration Server アプリケーション オブジェクトを Configuration Server 7.6にインポートし、これに対して新規ユーザを作成した場 合はこの機能が適用されます。ただし、7.5以前のConfiguration Server アプリ ケーション オブジェクトのそれぞれで、手動でこの機能を無効にした場合は 適用されません。

機能の設定

注: この項がご使用の環境に該当するかについては、上述の「サポートする コンポーネント」を参照してください。

デフォルトでは、no-default-access設定オプションによって、リリース 7.6で作成するすべての新規ユーザに対してこの機能が有効になります。リ リース7.6用のConfiguration Serverアプリケーションテンプレートでは、この オプションがデフォルト値のゼロに設定されています(0-デフォルトアクセ ス権禁止)。この機能を無効にするには、オプションを1に設定します(1-デ フォルトアクセス権)。 前リリースの リリース7.6のConfiguration Server にインポートしたリリース7.5以前の Configuration Server アプリケーション オブジェクトに対して、この機能も自動 的に有効になります。後方互換性を維持するためには、インポートした Configuration Serverアプリケーション オブジェクトのそれぞれに対して、[オ プション]タブのsecurityセクションに、手動でno-default-accessオプ ションを追加する必要があります。そして、オプションを1に設定して、機能 を無効にします(1-デフォルトアクセス権)。これで、元のリリースの規則に 基づいて、インポートしたアプリケーションに対して作成する新規ユーザにデ フォルト特権が割り当てられます。

新規ユーザへの この機能の対象となる新規ユーザに許可を割り当てるには、各ユーザの[プロ 許可割り当て パティ]ダイアログボックスの[Member Of]タブを使用します。詳細につい ては、*Framework 7.6 Configuration Manager のヘルプ*を参照してください。

設定オプション

Security セクション

このセクションには、セキュリティ機能関連の設定オプションがあります。こ のセクションの名前はsecurityにし、Configuration Serverアプリケーション オブジェクトの[オプション]タブで設定する必要があります。

no-default-access

デフォルト値:0 有効値:以下のいずれか:

- 0 デフォルトアクセス権禁止
- 1 デフォルトアクセス権付与

有効になるタイミング:即時

このアプリケーションで作成した新規ユーザに、デフォルト特権を割り当てるか指定します。このオプションがない場合は、デフォルト値だとみなされます。

前リリースとの後方互換性を維持するためには、Configuration Server 7.6 にイ ンポートしたリリース 7.5 以前の Configuration Server アプリケーション オブ ジェクトすべてに、このオプションを手動で追加し、値を1に設定する必要が あります。これで、7.6 より前のリリースと同様に、これらのオブジェクトに 対して作成した新規ユーザが、デフォルト アクセス グループに自動的に割り 当てられます。







アクティビティなしのタイムアウト

この章では、アクティビティなしのタイムアウトについて説明します。この時 間がすぎると、アクティビティなしのユーザがセッションを継続するには、再 度認証される必要があります。

- この章は、以下の項から構成されます。
- 機能の要約(25ページ)
- 機能の説明(26ページ)
- 機能の設定(27ページ)

機能の要約

アクティビティなしのタイムアウトは設定可能な時間で、この時間内はユーザ がアクティビティなしの状態でもセッションに影響はありません(システムに 対する何らかの操作が不要)。タイムアウトがすぎると、ユーザがセッション からロックアウトされ、すべてのセッションの表示が最小化されます。セッ ションを継続するには、ユーザが再度ログインする必要があります。または、 ログインせずに、任意の人がセッションを完全に閉じることもできます。

注: この機能では、アクティビティとは、マウスを使用する(クリック、移動、またはスクロール)、キーを押す、ウィンドウのアクティブと非アクティブを切り替える、またはオペレーティングシステム自体のタイムアウト機能によって生成された警告を承認することです。

セキュリティ上の利点

セッションにログインしているときに、ユーザがコンピュータを使用しなかっ たり、コンピュータから離れたりすると、(許可の有無に関わらず)だれでもそ のセッションにアクセスできるようになります。アクティビティなしのタイム アウト機能によって、別の人がシステムを表示したりシステムにアクセスする 可能性を最小限にできます。これはベストエフォート式です。タイムアウト の時間が短いと、ログインしたユーザが何回もログインを繰り返すことになり 不便ですが、システムが他人に露出するリスクは小さくなります。

サポートするコンポーネント

以下のコンポーネントがこの機能をサポートします。

- Configuration Manager
- Solution Control Interface
- Interaction Routing Designer
- Outbound Contact Manager

機能の説明

アクティビティなしのタイムアウトと同じ時間、ユーザのアクティビティがない場合は、すべての表示画面が最小化され(一部のモーダルダイアログ画面を除く)、再ログインダイアログボックスが表示されます。サーバとの接続は保持する必要があります。しかし、何らかの原因で接続が失われた場合は、アプリケーションのHA (High Availability:高可用性)機能が自動的に接続を試みます。

再ログイン ダイアログ ボックスで、ユーザが以下のいずれかの操作を行うこ とができます。

- パスワードを入力し、[OK]をクリックする。ユーザが認証され、以下のいずれかの状況が発生します。
 - ◆ ユーザが元のユーザと異なる場合は、アクセスが許可されない。
 - → ユーザが元のユーザと同一の場合は、ユーザが再度ログインし、可能な 限りセッション状態が復元される。
- [キャンセル]をクリックして、アプリケーションを終了する。確認ダイア ログボックスが表示され、アプリケーションを終了することをユーザが確 認するよう求められます。

いずれの場合でも、ユーザが再認証されなければ、現在のセッションにアクセスできません。

パスワード変更 Configuration Manager と Interaction Routing Designerでは、許可された人がアプ リケーションのユーザパスワードを変更できます。ユーザがログイン中で、ア クティビティなしのタイムアウトがすぎる前に、パスワードが変更されると、 ユーザが非アクティブ状態になります。この場合は、再ログインダイアログ ボックスで新しいパスワードを使用する必要があります。古いパスワードは無 効なパスワードだと解釈され、アクセスが許可されません。

> Configuration Managerでは、システム管理者が別のアプリケーションのユーザ パスワードも変更できます。ユーザがログイン中で、アクティビティなしのタ イムアウトがすぎる前に、パスワードが変更されると、ユーザが非アクティブ 状態になります。この場合は、再ログインダイアログボックスで古いパスワー ドを使用する必要があります。新しいパスワードは無効なパスワードだと解釈 され、アクセスが許可されません。

機能の設定

注: この項では、ほとんどのコンポーネントで使用されるこの機能の標準的な設定方法を説明します。26ページの「サポートするコンポーネント」で取り上げたものを含む一部のコンポーネントでは、この機能の実装が異なる場合があります。その場合は、詳細について、製品マニュアルを参照してください。

アクティビティなしのタイムアウトはアプリケーション レベルで設定するため、アプリケーションによって方法が異なる場合があります。デフォルトではこの機能が無効なため、タイムアウトをゼロ以外の値に設定して、機能を有効にする必要があります。

アクティビティなしのタイムアウトは、**アプリケーション**オブジェクトの[**オ プション**]タブを使用して、設定オプションinactivity-timeoutで指定 します。アプリケーションテンプレートがある場合は、このオプションがデ フォルト値に設定されています。

設定オプション

Security セクション

このセクションには、セキュリティ機能関連の設定オプションがあります。こ のセクションの名前はsecurityにし、Configuration Serverアプリケーション オブジェクトの[オプション]タブで設定する必要があります。

inactivity-timeout

デフォルト値:0 有効値:負以外の整数 変更が有効になるタイミング:即時

アプリケーションにログインしたユーザが非アクティブになるまでの時間(分単位)を指定します。この時間がすぎると、アプリケーション画面が最小化され、ユーザの再認証が必要になります。デフォルト値の0(ゼロ)の場合、機能が無効になります。

このオプションは、**アプリケーション** オブジェクトの [**オプション**] タブで設 定します。





この章では、ログメッセージの選択したデータを非表示にする方法について 説明します。

この章は以下のトピックから構成されます。

- 機能の要約(29ページ)
- 機能の説明(30ページ)
- 機能の設定(30ページ)

機能の要約

この機能で、Genesysコンポーネントが生成するログメッセージの選択した データを非表示にできます。

セキュリティ上の利点

この機能によって、無許可のユーザがログメッセージの特定のデータを見る ことができないようにします。トラブルシューティングなどの目的でログを他 者に配信する場合に、この機能を使用して、他者には公開したくない機密デー タを非表示にすることができます。また、サードパーティが提供するデータ がログに添付されることもあるため、こうしたデータの機密を保護するために も役立ちます。

サポートするコンポーネント

すべてのGenesysサーバアプリケーションがこの機能をサポートします。

機能の説明

この機能で、Genesysコンポーネントが生成するログ メッセージの選択した データを非表示にできます。データそのものをアスタリスク(*)と置き換えて 非表示にしたり、ログ出力からデータ フィールド全体を削除したりできます。

機能の設定

この機能は、以下の2つの設定オプションを、サーバ アプリケーション オブ ジェクトの[オプション]タブで定義して実装します。

- log-filter-sectionオプションのdefault-filter-type。ログのす べてのデータのトリートメントを定義します。
- log-filter-dataセクションのいくつかの<key name>オプション。ロ グの特定のキーのトリートメントを定義します。これは、 default-filter-typeで指定したデフォルトトリートメントより優先 されます。

設定オプション

Log-Filter セクション

このセクションで、ログのすべてのデータのトリートメントを定義します。こ のセクションはlog-filterという名前にする必要があります。

default-filter-type

デフォルト値: copy 有効値:以下のいずれか:

 copy
 KVListペアのキーと値がログにコピーされます。

 hide
 KVListペアのキーがログにコピーされ、値がアスタリスクと置き換えられます。

skip KVListペアがログにコピーされません。

変更が有効になるタイミング:即時

KVList の情報 (UserData、Extensions、および Reasons) をログに表示す るデフォルトの方法を指定します。この設定は、log-filter-data セクショ ンで明示的に定義したものを除く、すべての KVList ペアの属性に適用されま す。

例

```
[log-filter]
default-filter-type=copy
デフォルト ログ フィルタ設定を使用したログの例を以下の示します。すべて
のデータが表示されます。
message RequestSetCallInfo
  AttributeConsultType
                       3
```

AttributeOriginalConnID	008b012ece62c8be
AttributeUpdateRevision	2752651
AttributeUserData	[111] 00 27 01 00
'DNIS'	'8410'
'PASSWORD'	'111111111'
'RECORD_ID'	'8313427'
AttributeConnID	008b012ece62c922

Log-Filter-Data セクション

このセクションで、ログの特定のデータのトリートメントを定義します。これ はlog-filterセクションの一般的設定より優先されます。このセクションは log-filter-dataという名前にする必要があります。

<キー名>

デフォルト値:copy 有効値:以下のいずれか:

所定のKVListペアのキーと値がログにコピーされます。 copy hide 所定のKVListペアのキーがログにコピーされ、値がアスタリス クと置き換えられます。 skip KVListペアがログにコピーされません。

変更が有効になるタイミング:即時

ログのキー名で定義された KVList ペアを表示する方法を指定します。所定の KVList ペアについては、この設定が log-filter セクションで定義したデ フォルトの KVList の表示方法より優先されます。

注: T-Server アプリケーション オブジェクトの場合は、T-Server 共通の設定 オプション log-trace-flags が-udata に設定されている場合は、 log-filter-data セクションのオプションの設定とは関係なく、ユー ザデータがログに書き込まれません。log-trace-flags オプション の詳細については、ご使用の T-Server のマニュアルを参照してください。

例

[log-filter-data] PASSWORD=hide

PASSWORD オプションをhide に設定したログの例を以下に示します。 PASSWORDフィールドのデータがアスタリスク(****)に置き換えられていま す。

message RequestSetCallInfo

AttributeConsultType	3
AttributeOriginalConnID	008b012ece62c8be
AttributeUpdateRevision	2752651
AttributeUserData	[111] 00 27 01 00
'DNIS'	'8410'
'PASSWORD'	! * * * * !
'RECORD_ID'	'8313427'
AttributeConnID	008b012ece62c922





ログイン時のセキュリティ バナー

この章では、ログイン時にユーザに表示するセキュリティバナーを設定して インストールする方法について説明します。

この章は、以下の項から構成されます。

- 機能の要約(33ページ)
- 機能の説明(34ページ)
- 機能の構築(36ページ)

機能の要約

セキュリティバナーは、ユーザがアプリケーションにログインしたときに表示される個別のウィンドウです。このウィンドウの内容はシステム管理者が定義します。アプリケーションの使用条件や免責事項などを表示することができます。1つのセキュリティバナーを複数のアプリケーションで使用したり、それぞれのアプリケーションで異なるセキュリティバナーを使用することができます。

セキュリティバナーは、以下のいずれかの方法で有効にして設定します。

- アプリケーションの設定中。
- アプリケーションのインストール前またはインストール後。アプリケーションのホストレジストリに特定のレジストリ項目を作成する。

さまざまな企業ポリシに応じて、各アプリケーションに異なるセキュリティ バナーを設定することができます。

セキュリティ上の利点

セキュリティバナーは、実際は物理的または仮想的にシステムを保護するものではありません。しかし、無許可のユーザが使用条件などのアクセス制限を 侵害して、システムにアクセスした場合に、法的な保護となります。

最も厳格なセキュリティバナーの設定では、ユーザがバナーの内容に同意し なければアプリケーションへのログインを許可されません。インストール時に 選択したオプションに応じて、さまざまなレベルのセキュリティを設定できま す。

サポートするコンポーネント

以下のコンポーネントが、この章で説明するセキュリティバナーの実装をサ ポートします。

- Configuration Wizards (構成ウィザード)
- Configuration Manager
- Solution Control Interface
- Interaction Routing Designer
- Outbound Contact Manager

Genesys Desktop

Genesys Desktop は概念としてセキュリティバナーをサポートしますが、この マニュアルで取り上げる方法とは異なる方法で実装する必要があります。イン ストール手順が異なることに加えて、セキュリティバナーに関連するすべて の URL を HTTP 形式 (http://) にする必要があります。詳細については、 『Genesys Desktop 7.6 Deployment Guide』を参照してください。

機能の説明

セキュリティバナーは、Genesysアプリケーションにログインする前にユーザ が定義したセキュリティメッセージを表示し、ユーザにメッセージに同意す る手段を提供するためのものです。メッセージの内容は任意のURLとして設定 し、Microsoft Internet Explorer 4.0以降でアクティブな文書として表示できる文 書を指定します。冗長性を確保するため、複数のURLを設定できます。 以下に示すセキュリティバナーの特徴を、各アプリケーションに応じてさま ざまに設定できます。

- セキュリティバナーを表示する回数。たとえば、各ユーザに対して1回、 各タイプのアプリケーションについて各ユーザに対して1回、またはすべてのログインに対して表示する。
- セキュリティバナーを表示するか、またはユーザの確認が必要か。
- セキュリティバナーのターゲット URL を使用できない場合の動作。

- セキュリティバナーウィンドウのタイトルと大きさ。
- セキュリティバナーをロードし、画面に表示するまでのタイムアウト。このタイムアウトがすぎた場合は、セキュリティバナーのロード中に「Downloading terms of use... Please wait... (使用条件をダウンロードしています ... しばらくお待ちください ...)」という中間メッセージが表示される。

デフォルトでは、セキュリティバナーウィンドウにユーザが定義したテキスト、2つのボタン([受け入れ]と[拒否])、およびチェックボックス([I Accept. Do not show this again.])が表示されます。アプリケーションにログインするユーザは、[受け入れ]をクリックしなければ、ログインダイアログボックスに進むことができません。ユーザが[拒否]をクリックするか、ウィンドウの内容に同意せずにセキュリティバナーウィンドウを閉じると、アプリケーションが終了します。

上述のように、タイムアウトがすぎる前にセキュリティバナーを取得して表示できない場合は、常に「Downloading terms of use... Please wait...(使用条件をダウンロードしています...しばらくお待ちください...)」という中間メッセージが表示されます。このときに、ユーザが[キャンセル]をクリックしてウィンドウを閉じることができます。条件を受け入れることができるのは内容が完全に表示された場合だけです。

セキュリティバナーを表示できなかった場合にも、アプリケーションへの ユーザのログインを許可するか指定する必要があります。許可しない場合は、 セキュリティバナーを表示できないときはアプリケーションが終了します。

セキュリティバナーをまったく取得できない場合は、エラーメッセージが表示されます。エラーメッセージには、[受け入れ]と[拒否]ボタンの代わりに、[終了]ボタンが表示されます。ソフトウェアにデフォルトのエラーページが用意されていますが、独自のものを設定することもできます。エラーページの動作は、以下のように、セキュリティバナーを表示できない場合にもアプリケーションへのユーザのログインを許可するかどうかによって異なります。

- ユーザのログインを許可した場合。エラーページが(開いている場合は)自動的に閉じ、ログインダイアログボックスが表示されます。これで、ユーザがアプリケーションにログインできます。
- ユーザのログインを許可しない場合。ソフトウェアに組み込まれたエラー ページが表示され、エラーコードが表示されます。ログインダイアログ ボックスは表示されず、ユーザはログインできません。HTTP エラーにつ いては、HTTP の仕様を参照してください。システムエラーについては、 Microsoft 社の技術マニュアルを参照してください。
- 警告! セキュリティ バナーが確実にロードできるように、必要に応じてローカルファイルを含む複数の冗長 URL を使用することをお奨めします。

機能の構築

注: この項がご使用のコンポーネントに該当するか確認するには、34ページ の「サポートするコンポーネント」を参照してください。

以下の3つのステップで、セキュリティバナーを構築します。

- エディタを使用して、必要なセキュリティバナーおよびカスタマイズした エラーページ(オプション)を設計して作成します。
- セキュリティバナー文書をファイルまたはWeb コンテンツとして構築し、 URL を記録します。インストールされた Microsoft Internet Explorer (IE) が 各 URL を解決可能で、IE ウィンドウ内にアクティブページとして表示で きる必要があります。
- 3. 以下のいずれかの方法で、URLを設定します。
 - GUI アプリケーションのインストール中に指示に従う(37ページの「アプ リケーション設定中のセキュリティバナーのインストール」を参照)。
 - ・レジストリ項目を直接変更する(41ページの「レジストリによるセキュ リティバナーの設定」を参照)。
- 警告! レジストリを誤って編集すると、システム全体に重大な問題が発生し、 オペレーティングシステムを再インストールしなければ解決できなく なる可能性があります。Genesys は、レジストリ編集によって発生した 問題の解決については責任を負いません。ご自身の責任でレジストリを 編集してください。 レジストリを編集する場合は、編集前にレジストリファイルのバック アップを作成することを強くお奨めします。
- 注: セキュリティ バナーを設定したアプリケーションをアンインストール しても、セキュリティ バナーの設定パラメータはレジストリから削除さ れません。パラメータを削除するには、セキュリティ バナーを有効にし ないで、アプリケーションを再インストールする必要があります。

同一ホストの複数アプリケーションのセキュリティ バナー 構築

1 つのホストにセキュリティ バナーをサポートする複数のアプリケーション がインストールされている場合に、セキュリティ バナーを使用するには、以 下のいずれかの手順を行います。

各タイプのアプリケーションを個々に設定する。

この場合、1つのアプリケーションだけにセキュリティバナーを設定する ことを選択すると (for this オプション)、他のすべてのアプリケーションの セキュリティバナーが無効だとみなされます。他のアプリケーションでも
バナーを使用したい場合は、他のアプリケーションそれぞれについて、バ ナーを有効にして設定する必要があります。次回のアプリケーションのイ ンストールでは、for all オプションを選択できますが、このオプションで 設定されるのは次回のインストールのデフォルト値のみです。以前のイン ストールには影響しません。

• すべてのアプリケーションに1つのセキュリティバナーを設定する。

この場合、特定のホストのすべてのアプリケーション (for all) のセキュリ ティバナーの内容と動作が同じになります。実質的には、これらの設定が デフォルト (default) 設定になります。各アプリケーションに対して、セ キュリティバナーを有効にして設定する必要はありません。これを選択し た場合、次回にインストールするセキュリティバナーのあるアプリケー ションに対して、以下のいずれかを実行できます。

- デフォルト設定には影響を与えずに、1つのアプリケーションだけに(for this) 個別の設定を行う。
- すべてのアプリケーションのセキュリティ バナーを設定するオプション(for all)を選択して、デフォルト設定を無効にし、必要に応じて設定を変更する。デフォルト値はインストールインタフェースに表示され、上書きまたはそのままにできます。これらの値のいずれかを変更すると、以前にインストールしたものおよび次回にインストールするものを含めて、デフォルト値を使用するすべてのアプリケーションに影響します。

ー般に、アプリケーションを設定する際には、設定プログラムが最初にアプリケーション固有(for this)のセキュリティバナー設定を検索します。見つからない場合は、すべてのアプリケーションに共通(for all)の設定を検索します。いずれの場合でも、すでに定義されているセキュリティバナー属性が継承されます。セキュリティバナー設定がまったく見つからない場合は、デフォルトでセキュリティバナーが無効になります。この場合は、ユーザが最初からセキュリティバナーを有効にして設定する必要があります。

アプリケーション設定中のセキュリティ バナーのインストール

34ページの「サポートするコンポーネント」に記載されたコンポーネントの場合は、セキュリティバナーのインストールと設定がアプリケーションのイン ストール手順に組み込まれています。アプリケーションをインストールした後 で、セキュリティバナーをインストールすることもできます。

アプリケーションのインストール手順の詳細については、ご使用のアプリケー ションのマニュアルを参照してください。アプリケーションをインストールす る際に[Enable Security Banner]オプションを選択した場合のみ、以下 の手順を行います。

手順: アプリケーション設定中のセキュリティ バナーのインス トールと設定

目的:サポートするコンポーネントのセキュリティ バナーをインストールして設定します。

サポートするコンポーネント:

- Configuration Wizards (構成ウィザード)
- Configuration Manager
- Solution Control Interface
- Interaction Routing Designer
- Outbound Contact Manager

前提条件

- 上記のいずれかのコンポーネントをインストールする際に、Installation Wizard (インストールウィザード)の [Security Banner Configuration] ページが表示される。
- セキュリティバナーとカスタムエラーページ(使用する場合)を作成して URLを指定した。

手順開始

- インストール中のアプリケーションの Installation Wizard (インストール ウィザード)の [Security Banner Configuration] ページで、以下 の手順を行います。
 - a. [Select Security Banner behavior and configuration] セクションで、これから定義するセキュリティバナーをセキュリティ バナー機能をサポートするすべてのアプリケーションで使用するか、 特定のタイプのアプリケーションだけで使用するか選択します。
 - **b.** [次へ]をクリックします。
- 2. [Security Banner Parameters] ページで、以下のようにセキュリ ティバナーのパラメータを指定します。
 - a. 特定のタイプのアプリケーションを次回に起動したときに、ユーザに セキュリティバナーを表示する方法を指定します。以下の方法を選択 できます。
 - [Until each user chooses to turn it off]— セキュリ ティバナーに [I Accept. Do not show this again.] チェッ クボックスが表示されます。これはデフォルトではオフです。ユー ザがこのオプションを選択して、[受け入れ]をクリックすると、 ユーザが起動するアプリケーションには関係なく、次回以降はそ のユーザにはセキュリティバナーが表示されません。すべてのア

プリケーションのセキュリティバナーを無効にするには、各 Windows ユーザアカウントが明示的にこのオプションを選択し て、[受け入れ]をクリックする必要があります。

- [Until each user chooses to turn it off once for each application type]—セキュリティバナーに[I Accept. Do not show this again.] チェック ボックスが表示されま す。これはデフォルトではオフです。ユーザがこのオプションを 選択して、[受け入れ]をクリックすると、ユーザが同じタイプの アプリケーションを起動するときには、次回以降はそのユーザに セキュリティバナーが表示されません。ただし、セキュリティバ ナーがアクティブな別のタイプのアプリケーションをユーザが起 動すると、毎回セキュリティバナーが表示されます。同じタイプ のアプリケーションのセキュリティバナーを無効にするには、各 Windows ユーザアカウントが明示的にこのオプションを選択し て、[受け入れ]をクリックする必要があります。
- [Every time the application starts]—セキュリティバ ナーに [I Accept. Do not show this again.] チェック ボックスが表示されません。Genesys アプリケーションを起動する 際に、すべてのユーザに対して、毎回セキュリティバナーが表示 されます。
- 注:最初のオプション([Until each user chooses to turn it off])または2番目のオプション([Until each user chooses to turn it off once for each application type])を選択した場合に、ユーザがセキュリティバナー ウィンドウで[I Accept. Do not show this again.]を選択すると、次回以降にインストールするすべてのアプリケーションにこの設定が適用されます。これは、許可された人が手動でレジストリから削除する必要があります。詳細については、44ページの「AckMode」を参照してください。
- **b.** 指定されたURLで、セキュリティバナーメッセージを表示できない場合の処理を指定します。以下の方法を選択できます。
 - [Proceed to login without banner]— ユーザがアプリ ケーションにログインできます。
- 警告!以下のオプションを選択すると、URL で指定された文書を取得または表示できない場合に、アプリケーションへのアクセスを効果的に無効にできます。
 - [Exit, no login dialog box is displayed]—ユーザの ログインが許可されません。
- c. (オプション)セキュリティバナーウィンドウのタイトルバーに表示 するタイトルを指定します。
 タイトルを指定しない場合は、以下のようにウィンドウタイトルが取 得されます。

- セキュリティバナーが HTML ファイルの場合 —<title> 要素
- セキュリティバナーがHTMLファイルだが、<title>要素がない 場合 —URLアドレス
- セキュリティバナーがHTMLファイルでない場合—URLアドレス すべての場合に、タイトルバーのタイトルの後にアプリケーション名 が続きます。
- **注:** 再ブランドリソースがある場合は、対応する再ブランドリソースの ほうが優先されます。
- d. セキュリティバナーを表示するタイムアウト(ミリ秒単位)を指定します。デフォルトは 3000 です。この時間内に文書全体を表示できない場合は、セキュリティバナー自体が表示されるまで、「Downloading terms of use ... Please wait ..., (使用条件をダウンロードしています...しばらくお待ちください...)」という中間メッセージが表示されます。
- e. セキュリティバナーウィンドウ、中間ウィンドウ、およびエラーウィンドウ(ある場合)の高さと幅(ピクセル単位)を指定します。デフォルト値は、それぞれ180および360ピクセルです。
 これらの値を指定しない場合は(デフォルト)、指定したURLの文書の内容全体が収まるウィンドウサイズになります。ウィンドウを画面の作業域より大きくすることはできません。毎回のログインで文書のサイズが保持されます。表示後は、標準IEツールを使用してサイズを変更できます。
- **注**: セキュリティ バナー文書の正確な画面サイズを判断できない場合は、 高さと幅のパラメータを指定することをお奨めします。

f. [次へ]をクリックします。

- セキュリティバナーに表示するテキストを含む各文書の [Security Banner Documents] ページで、文書の URL を指定して、[追加]をク リックします。すべての URL を追加したら、[次へ]をクリックします。 この URL を指定しない場合は、他のすべてのオプションが無視され、以 下のように処理されます。
 - 古いセキュリティバナービットマップが設定されている場合は、それ を表示する。
 - それ以外の場合は、セキュリティバナーが表示されない。
- [Security Banner Error Documents] ページで、以下のいずれかを 行います。
 - 39ページのステップ2bで[Proceed to login without banner]
 を選択した場合は、[次へ]をクリックします。このページにはURL
 を入力しないでください。

それ以外の場合は、エラー文書のURL(デフォルトエラーページまたは独自に作成したもの)を指定します。[追加]をクリックします。すべてのURLを追加したら、[次へ]をクリックします。

手順終了

次のステップ

必要に応じて、アプリケーションのインストールを終了します。手順の詳細については、製品マニュアルを参照してください。

レジストリによるセキュリティ バナーの設定

警告! レジストリを誤って編集すると、システム全体に重大な問題が発生し、 オペレーティングシステムを再インストールしなければ解決できなく なる可能性があります。Genesys は、レジストリ編集によって発生した 問題の解決については責任を負いません。ご自身の責任でレジストリを 編集してください。 レジストリを編集する場合は、編集前にレジストリファイルのバック アップを作成することを強くお奨めします。

セキュリティバナー機能とURLは、アプリケーションホストのレジストリで 定義されます。HKEY_LOCAL_MACHINE レジストリキーのアクセス権を持 つ人(通常はシステム管理者)だけが、セキュリティバナーを設定して維持で きます。この許可を持つ人が以下の手順を行います。

- セキュリティ バナーおよびカスタマイズしたエラー ページのターゲット URL を指定する。
- 必要に応じて、ウィンドウをカスタマイズする。
- その後でレジストリ項目を変更して、必要に応じて動作を変更する(ローカ ルまたはリモートで実行可能)。

セキュリティ バナー機能の設定

以下のレジストリキーを使用して、セキュリティバナー機能を設定します。 HKEY LOCAL MACHINE\SOFTWARE\GCTI\Unilogin\Banner

このキーの値で、すべてのアプリケーションのデフォルトの動作を指定しま す。以下のように、サブキーで、特定のアプリケーションに対して項目を再定 義できます。

HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\
<CfgAppType>

<CfgAppType>は、42ページの表1に示したアプリケーションタイプの数値です。

たとえば、Configuration Managerに固有の値(アプリケーションタイプ19)を指 定するには、以下のようにレジストリサブキーを定義します。

HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\19

表示して使用するセキュリティバナーを選択すると、まず、ライブラリが対応するサブキーを検索し、サブキーがない場合はデフォルトキーを使用します。

文字列はSTRINGまたはEXPANDABLE_STRINGレジストリ値として入力でき ます。EXPANDABLE_STRINGとして入力すると、パーセント記号(%)で囲まれ た環境変数文字列が、(%HOMEDRIVE%%HOMEPATH%\default.htmにある)環 境変数で定義された値と置き換えられます。整数はDWORDまたはSTRINGレジ ストリ値として入力可能で、10進数を表します。

表 1: CfgAppType でサポートされるアプリケーション タイプ

СfgAppType	アプリケーション
13	Outbound Contact Manager
19	Configuration Manager Wizard Manager
44	Solution Control Interface
51	Interaction Routing Designer

URL の設定

セキュリティ バナーの URL と関連するエラー ページは、以下のレジストリ キーで設定します。

- すべてのアプリケーション : HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\URLs\ <seq_number>
- 特定のアプリケーション

 HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\<CgfA
 ppType>\<seq number>

<seq_number>は、複数のURLのシーケンス番号です。複数のURLはシーケンス番号の順序で試されます。

URLはErrorPage (44ページを参照)およびURL (47ページを参照)レジストリ オプションで指定します。

例 以下に、サンプルのレジストリ項目を示します。 KEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\URLs\1\UR L=http://MyServer1/Banner.htm HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\URLs\2\U RL=http://MyServer2/Banner.htm HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\URLs\3\U RL=%SystemRoot%\AdminContacts.htm HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\Unilogin\Banner\URLs\3\E
rrorPage=1

これによって、以下の動作を指定します。

ダイアログがMyServer1からBanner.htmを取得しようとします。このファ イルを取得できない場合は、MyServer2からBanner.htmを取得しようとし ます。このファイルを取得できない場合は、system32ディレクトリにあるカ スタム エラーページを取得して表示しようとします。このページを表示でき ない場合は、デフォルトエラーページが表示されます。

セキュリティ バナーのレジストリ項目

この項では、セキュリティバナーの外観と動作を指定してカスタマイズする ためのレジストリオプションについて説明します。これらのオプションは、レ ジストリのアクセス権があり、十分な知識を持つユーザだけが使用してください。

 注:特に記載がない限り、この項で取り上げるレジストリ項目は、アプリ ケーションの設定中にセキュリティバナーをインストールする際に表 示されるオプションと同等です。

AckMandatory

デフォルト値:0

有効値:以下のいずれか:

- 0 セキュリティバナーの内容を確認せずに、ログインを続行できます。ログインダイアログボックスが表示されます。
- 1 アプリケーションが終了します。 ログイン ダイアログ ボックスは表示されません。

変更が有効になるタイミング:アプリケーションの再起動後

何らかの原因で、URL オプション (47 ページを参照) で指定した文書を表示で きない場合でも、アプリケーションへのログインを許可するかどうかを指定し ます。

警告! このオプションを1に設定すると、URL で指定された文書を取得また は表示できない場合に、アプリケーションへのアクセスを効果的に無 効にできます。

AckMode

デフォルト値:0 有効値:以下のいずれか:

- 0 ユーザが、すべてのアプリケーションに対して、次回以降のすべてのロ グインでセキュリティバナーを非表示にすることを選択できます。
- 1 ユーザが、現在のアプリケーションのみに対して、次回以降のすべての ログインでセキュリティバナーを非表示にすることを選択できます。
- 2 ユーザがセキュリティバナーの非表示を選択できません。ユーザがアプ リケーションにログインするたびに、バナーの内容を受け入れる必要が あります。

変更が有効になるタイミング:アプリケーションの再起動後

セキュリティバナーを非表示にするオプションを、ユーザに対して表示する かどうかを指定します。非表示の場合、次にアプリケーションを起動するとき に、セキュリティバナーの内容を受け入れる必要がなくなります。

このオプションを 0 または 1 に設定すると、セキュリティバナー ウィンドウ に [I Accept. Do not show this again.] チェック ボックスが表示さ れます。ユーザがこのチェック ボックスをオンにすると、現在のアプリケー ション (0 か 1) またはセキュリティ バナーが設定されたすべてのアプリケー ション (1) について、次回以降にアクセスするときにはセキュリティ バナーが 表示されません。

 注: 0または1のオプションを選択した場合、現在のアプリケーション(0か 1)またはすべてのアプリケーション(1)にログインするときにセキュリ ティバナーを再度表示するには、この項目を手動でレジストリから削除 する必要があります。このレジストリ項目と値はインストール間で保持 されます。つまり、アプリケーションをアンインストールしても削除さ れず、アプリケーションを再インストールしても、消去またはリセット されません。

このオプションを 2 に設定すると、セキュリティ バナー ウィンドウに [I Acknowledge. Don't show this again.] チェック ボックスが表示さ れず、アプリケーションにアクセスする際に毎回、セキュリティ バナーが表 示されます。

ErrorPage

1

デフォルト値:0 有効値: 0

- セキュリティバナーが表示されます。
- エラーページが表示されます。

変更が有効になるタイミング:アプリケーションの再起動後

カスタム エラーページを使用する場合に必要です。URL がエラーページまた はセキュリティ バナーを指定するように設定します。エラーページを表示す る場合は、[受け入れ]および [拒否]ボタンの代わりに、ウィンドウに [終 了]ボタンが表示されます。この設定を使用して、デフォルトエラーページ をカスタム エラーページと置き換えることができます。

Height

デフォルト値:なし 有効値:180より大きい正の整数 変更が有効になるタイミング:アプリケーションの再起動後

Width

デフォルト値:なし 有効値:359より大きい正の整数 変更が有効になるタイミング:アプリケーションの再起動後

(オプション)これら2つのオプションで、セキュリティバナーとエラーページウィンドウの文書領域の寸法(ピクセル単位)を指定します。これらの値を 指定しない場合は(デフォルト)、URLオプションで指定した文書の内容全体 が収まるウィンドウサイズになります(47ページを参照)。ウィンドウを画面 の作業域より大きくすることはできません。毎回のログインで文書のサイズが 保持されます。表示後は、標準 IE ツールを使用してサイズを変更できます。

NoCompleteTimeout

デフォルト値:2000 有効値:負以外の整数 変更が有効になるタイミング:アプリケーションの再起動後

WebBrowser コントロールから、ダウンロード進行状況または状態の通知を受け取るまでのタイムアウト(ミリ秒単位)を指定します。文書をダウンロードして表示するために、セキュリティバナーダイアログが、WebBrowser コントロールの形で IE のコンポーネントを使用します。場合によっては、セキュリティ上の理由で、WebBrowser コントロールがクライアントにナビゲーションのキャンセルを検出する手段を提供しないことがあります。このタイムアウトによって、こうした状況を適切に検出して処理できます。

このタイムアウトをすぎても、WebBrowser コントロールから進行状況や状態 が通知されない場合は、文書の取得が失敗したとみなされます。このタイムア ウトがすぎると、現在の URL で指定された文書を取得しようとする試みが破 棄され、ダイアログが URL リストの次の URL を取得しようとします。このと き、URL がリストの最後の URL の場合は、「System error 0x80004004: Operation aborted (システム エラ-0x80004004: 操作が破棄されま した)」というエラーメッセージがユーザに対して表示されます。

このオプションをゼロ(0)に設定すると、ダウンロードの失敗またはキャンセルの検出に進行状況と状態の通知は使用されません。

注: NoCompleteTimeout は、レジストリのアクセス権を持つ十分な知識 のあるユーザだけが使用してください。アプリケーションの設定中にセ キュリティバナーをインストールする際に、同等のオプションは表示さ れません。この場合は、デフォルト値が適切だとみなされます。

注: セキュリティバナー文書の正確な画面サイズを判断できない場合は、高 さと幅のパラメータを指定することをお奨めします。

ShowUpTimeout

デフォルト値: 3000 有効値:負以外の整数 変更が有効になるタイミング:アプリケーションの再起動後

セキュリティバナーウィンドウが、URL オプション(47 ページを参照)で指 定した文書のロードを試みるタイムアウト(ミリ秒単位)を指定します。内容 を表示する前にこのタイムアウトがすぎると、中間ウィンドウに 「Downloading terms of use... Please wait... (使用条件をダウ ンロードしています...しばらくお待ちください...)」)というメッセージ が表示されます。このときに、ユーザが[キャンセル]をクリックしてウィ ンドウを閉じることができます。条件を受け入れることができるのは内容が完 全に表示された場合だけです。

文書を取得できない場合は、以下に示すように、ウィンドウの動作が AckMandatory オプションの値に依存します。

- AckMandatory=0の場合は、自動的にウィンドウが閉じて(開いていた場合)、ログインダイアログボックスが表示されます。これで、ユーザがアプリケーションにログインできます。
- AckMandatory=1の場合は、ソフトウェアに組み込まれたエラーページ が表示され、エラーコードが示されます。HTTPエラーについては、HTTP の仕様を参照してください。システムエラーについては、Microsoft 社の 技術マニュアルを参照してください。ログインダイアログボックスは表 示されないため、ユーザはログインできません。

Title

デフォルト値:なし 有効値:任意の文字列、または空白 変更が有効になるタイミング:アプリケーションの再起動後

(オプション) セキュリティ バナー ウィンドウのタイトル バーに表示するタ イトルを指定します。このオプションに値を指定しない場合は、以下のように タイトルが取得されます。

- セキュリティバナーが HTML ファイルの場合 ---<title> 要素
- セキュリティバナーがHTMLファイルだが、<title>要素がない場合— URLアドレス
- セキュリティバナーが HTML ファイルでない場合 URL アドレス

すべての場合に、タイトルバーのタイトルの後にアプリケーション名が続きます。

注: 再ブランド リソースがある場合は、対応する再ブランド リソースのほうが優先されます。

URL

デフォルト値:なし。後方互換性のため

有効値:インストールされた IE アプリケーションが解決可能で、IE ウィンド ウ内にアクティブ ページとして表示可能な URL アドレス

変更が有効になるタイミング:アプリケーションの再起動後

(必須)セキュリティバナーウィンドウに表示する文書のURLを指定します。 この値を指定しない場合は、他のすべてのオプションが無視され、以下のよう に処理されます。

- 古いセキュリティ バナー ビットマップが設定されている場合は、それを 表示する。
- それ以外の場合は、セキュリティバナーが表示されない。





パート

サービスの可用性

このマニュアルのパートIIでは、システムを中断なく運用してサービスの可用 性を確保するために、Genesysが提供する機能について説明します。

以下の章から構成されます。

- 51ページの第6章「アプリケーションの冗長性」
- 57 ページの第7章「プロキシサーバとパラレルサーバ」

パート II: サービスの可用性





アプリケーションの冗長性

この章では、アプリケーションの障害に備えて、ご使用の環境をより堅牢にするために、冗長アプリケーションを使用する方法について説明します。

- この章は、以下の項から構成されます。
- 機能の要約(51ページ)
- 機能の説明 (52 ページ)
- 機能の設定(56ページ)

機能の要約

冗長アプリケーション(通常はサーバアプリケーション)は、アプリケーション に障害が発生した場合にバックアップ機能を提供します。つまり、1つのサー バ(プライマリサーバ)のサービスが、切断など何らかの原因で停止した場合で も、サービスをほとんど停止することなく、他のサーバ(バックアップサーバ) がプライマリサーバとして動作します。

セキュリティ上の利点

冗長アプリケーションを使用することによって、DoS攻撃などセキュリティ関連の攻撃でアプリケーションのサービスが停止した場合でも、機能およびデー タ喪失のリスクが大幅に減少します。

サポートするコンポーネント

冗長性をサポートするコンポーネントのリスト、およびそれぞれがサポートする冗長タイプについては、54ページの表2を参照してください。

機能の説明

冗長アプリケーションは、アプリケーションに障害が発生した場合の機能喪失 とデータ喪失の可能性に対応します。

完全なアプリケーションの故障は、内部欠陥(無限ループなど)や外部イベント (電源障害)が原因の可能性があります。その結果は、プロセスの応答なしや終 了として現れます。通常、ソリューション コンポーネントが停止すると、ソ リューションが顧客のインタラクションを処理できなくなります。

障害が発生したアプリケーションは機能を実行できないため、このタイプの障害の検出と修正には外部メカニズムが必要になります。Management Layerがこのようなメカニズムとして機能します。アプリケーション障害を検出するために、Management LayerではLocal Control Agent (LCA)と呼ばれる簡単なモニタリングコンポーネントを使用します。LCAは常にアプリケーションとの接続を維持し、アプリケーションが存在し、通信可能であることを確認します。アプリケーション障害と接続障害を明確に区別するために、特定のアプリケーションをモニタするLCAは、常にアプリケーション自体が実行されるコンピュータに常駐します。

LCAは各ホストに1つインストールされ、そのホストのすべてのGenesysアプ リケーションに接続できます。接続が切断すると、LCAがSolution Control Server (SCS)に対してメッセージを生成し、SCSでシステム設定に応じて、適切な修 復アクションが選択されて実行されます。SCSはAdvanced Disconnect Detection Protocol (ADDP)を使用して、LCAとの接続喪失を認識します。接続喪失はホス トの障害(特定のホストで実行されるすべてのGenesysコンポーネントの障害) として解釈されます。

バックアップ アプリケーションが設定され実行されている場合は、いわゆる 高可用性ライセンスがあれば、Management Layerが自動的に処理をそのアプリ ケーションに切り替えます。アプリケーションがサーバの場合は、クライアン トが自動的にバックアップ サーバに接続します。

リリース7.0以降の場合は、Management Layerがさらに堅牢な切り替え機能を 提供します。特に、実行中のアプリケーションがサービスを提供できない状況 を検出して、この状況をアプリケーション障害として扱います。このために、 サービス利用不可のアプリケーション状況が役立ちます。

アプリケーションの状況がサービス利用不可に変化したことがレポートされ ると、アプリケーションにバックアップサーバが設定され実行されている場 合は、Management Layerが自動的に処理をバックアップサーバに切り替えま す。サービス利用不可の状況で、プライマリアプリケーションとバックアッ プアプリケーションの両方が実行されている場合は、バックアップアプリ ケーションがサービスを提供可能であるとレポートする場合があります(バッ クアップアプリケーションの状況が開始に変化)。この場合は、Management Layerが自動的に処理をバックアップアプリケーションに切り替えます。アプ リケーション障害によるスイッチオーバと同様に、サービス利用不可に関連し たスイッチオーバを実行するには、HAライセンスが必要です。 注: 一部のアプリケーションはサービス利用不可の状況をサポートし、適切 な状況でこれをレポートしますが、レポートしないアプリケーションも あります。たとえば、T-Server が CTI リンクとの接続を失った場合、 T-Server が状況をサービス利用不可に変更します。Management Layer は、 アプリケーションが提供する情報に基づいて動作し、アプリケーション のサービス利用不可を自動的に検出することはできません。アプリケー ション側でサービス利用不可の状況がサポートされるかについては、ア プリケーションのマニュアルを参照してください。

冗長タイプ

ウォーム スタンバイ

Genesysでは、ウォーム スタンバイという用語は次のような冗長タイプを表し ます。バックアップ サーバアプリケーションが初期化され、プライマリ サー バの処理を引き継ぐ準備ができています。ウォーム スタンバイ冗長タイプで は、障害を検出する間に発生したインタラクションを処理できない可能性が最 小限になります。また、バックアップ サーバをオンラインにする必要がなく、 ソリューションの可用性が高くなります。

Management Layerが、バックアップサーバの役割をプライマリに変更するまでは、バックアップサーバはクライアント要求を処理できません。プライマリサーバと同じサーバで実行されるLCAの接続が切断すると、プライマリプロセスの障害がレポートされます。その結果、Management Layerが、バックアッププロセスに役割をバックアップからプライマリに変更するよう指示し、以前のバックアップがサービスに対する新しい要求すべての処理を開始します。

注: プライマリモードに切り替えるには、プライマリ Configuration Server の 障害の間、バックアップ Configuration Server が Configuration Database と のアクティブな接続を維持している必要があります。

バックアッププロセスが処理を引き継ぐと、すぐに通常動作が復元されます が、フォルト管理は続行されます。つまり、障害が発生したプロセスの再起動 の試行が繰り返されます。再起動が成功すると、このプロセスにバックアップ の役割が割り当てられます。

Solution Control Serverが、ホストのLCAとの接続が失われたことを検出すると、 バックアップ アプリケーションが設定されている場合は、Solution Control Serverがホストのすべてのアプリケーションのスイッチオーバを実行します。 これには、以下の2つの例外があります。

 バックアップモードの Configuration Server が、プライマリモードの別の Configuration Server を検出すると、スイッチオーバコマンドを無視します。 つまり、Configuration Server がプライマリモードになっているホストに常 駐する LCA がダウンすると、SCS が、使用可能な LCA のある別のホスト のバックアップモードの Configuration Server をプライマリモードに切り 替えるように要求します。要求を受け取ると、この Configuration Server が、 プライマリモードの Configuration Server がダウンしているかチェックしま す。ダウンしているかどうかは、2 つの Configuration Server の接続喪失に よって示されます。この接続がダウンしている場合にのみ、バックアップ モードの Configuration Server がプライマリモードに切り替えられます。接 続が存在する場合は、スイッチオーバは実行されません。

 バックアップモードの SCS がプライマリモードの SCS を検出できる場合 は、自身のスイッチオーバを実行しません。つまり、バックアップモード の SCS が、プライマリモードの SCS があるリモートホストに常駐する LCA との接続を失うと(原因は、LCA のダウンまたはネットワークタイ ムアウトによる SCS の切断)、バックアップモードの SCS が、自身がプラ イマリモードのリモート SCS とまだ接続しているかどうかチェックしま す。この接続も失われると、SCS がプライマリモードに切り替わります。

ホット スタンバイ

Genesysでは、ホット スタンバイという用語は次のような冗長タイプを表しま す。バックアップ サーバ アプリケーションが初期化されたままで、クライア ントが起動時にプライマリ サーバとバックアップ サーバの両方に接続し、 バックアップ サーバのデータがプライマリ サーバと同期されます。データ同 期とバックアップとの既存のクライアント接続によって、コンポーネントの高 可用性が保証されます。ホット スタンバイ冗長タイプの詳細については、適 切な製品マニュアルを参照してください。

サポートするコンポーネント

表2は、冗長性をサポートするGenesysコンポーネントと、それぞれの冗長タイプを示しています。

表 2: サポートされる冗長タイプ

コンポーネント	スタンバイ			
コンハーインド	ホット	ウォーム		
Solution Control Server	×			
Message Server		×		
DB Server		×		
Configuration Server	×			
Stat Server		×		
T-Server	×	×		
Network T-Server	ת			



– 、 .+² → 、, L	スタンバイ			
コンホーネント	ホット	ウォーム		
Load Distribution Server (LDS)	×			
Universal Routing Server (URS)	×			
Interaction Server		×		
Universal Contact Server (UCS)		×		
Call Progress Detection (CPD) Server		×		
Outbound Contact Server (OCS)		×		
E-mail Server Java		×		
Web API Server		×		
Chat Server		×		
Contact Center Analyzer (CCA) Data Sourcer	×			
SIP Server	×	×		
Genesys Voice Platform (GVP)	×b			
Integration Server (GIS)	×			
IVR Server		×		

表 2: サポートされる冗長タイプ(続き)

a. Network T-Server はウォームまたはホット スタンバイをサポートしません。代わりに、 ロード シェアリング冗長スキーマを使用します。詳細については、ご使用の T-Server の『Framework 7.6 Network T-Server Deployment Guide』を参照してください。

b. Resource Manager $\mathcal{O}\mathcal{P}$

機能の設定

冗長性を持つGenesysアプリケーションの設定は、アプリケーションタイプに よってさまざまです。この項では、一般的な高レベルの手順だけを説明しま す。詳細情報およびご使用の環境で冗長アプリケーションを設定する詳細な手 順については、適切な製品マニュアルを参照してください。

手順:

要約 --- 冗長アプリケーションの設定

目的: 冗長アプリケーションを設定するための一般的な要約を取り上げます。 一部のコンポーネントでは手順がいくらか異なる場合があります。詳細情報お よびご使用の環境で冗長性を設定する詳細な手順については、適切な製品マ ニュアルを参照してください。

手順開始

- プライマリ アプリケーションのアプリケーション オブジェクトを作成します。
- 2. プライマリアプリケーションをインストールします。
- バックアップ アプリケーションのアプリケーション オブジェクトを設定 します。
- 4. バックアップアプリケーションをインストールします。
- プライマリ アプリケーション オブジェクトで、バックアップ アプリケーション オブジェクトを追加し、ドロップダウン リストから [冗長タイプ] を選択します。

手順終了





プロキシ サーバとパラレル サーバ

この章では、大規模な構成をより効率的にするために、プロキシモードまた はパラレルモードで実行されるアプリケーションの使用方法について説明し ます。

- この章は、以下の項から構成されます。
- 機能の要約(57ページ)
- 機能の説明(59ページ)
- 機能の設定(59ページ)

機能の要約

プロキシ サーバとパラレル サーバによって大規模な構成の効率性が向上し、 障害による損害を限定的なものに抑えることができます。

いずれの構成も分散構成の一種ですが、以下のように、サーバ間に作業負荷を 分散する方法が異なります。

- プロキシ環境では、各プロキシサーバが作業負荷の一部を負担し、負担した負荷だけに対して処理を実行します。
- パラレル環境では、作業負荷がすべてのサーバに分散され、1つのサーバができる限り負荷を均衡させようとします。

プロキシサーバは、地理的に広い範囲に分散したシステムの場合に特に有効 です。プロキシ環境では、1つのサーバに属するクライアント数が複数のサー バ(プロキシモードで実行)に分散され、これらすべてが中央のサーバ(マスタ) に集中します。

パラレル サーバはロード シェアリングが可能です。これは、パラレルで実行 される1つのサーバの複数のインスタンスで、これらのインスタンス間に負荷 を分散します。

セキュリティ上の利点

プロキシ サーバとパラレル サーバの利用によって、サーバのサービスが停止 しても機能とデータの喪失を最小限に抑えることができます。

- 1つのプロキシサーバに障害が発生したときに失われるのは、このプロキシサーバに関連したクライアントだけです。1つのサーバインスタンスだけのプロキシを使用しない環境では、この1つのサーバが停止すると、すべてのクライアントが失われます。
- パラレル構成のサーバに障害が発生すると、新しい要求が残りのサーバに 分散されます。

サポートするコンポーネント

以下のコンポーネントは、何らかのプロキシ構成またはパラレル構成(または 両方)をサポートします。構成の詳細とご使用のシステムに実装する方法については、適切な製品マニュアルを参照してください。

- Solution Control Server— 分散 Solution Control Server
- Message Server
- Configuration Server
- Load Distribution Server (LDS)—T-Server プロキシモードの場合
- Universal Routing Server (URS)
- Interaction Server
- Call Progress Detection (CPD) Server
- E-mail Server Java
- Web API Server
- Chat Server
- Call Concentrator
- Network SIP Server
- Stream Manager
- Interaction Concentrator—LDS は非サポート
- Genesys Voice Platform (GVP)
- Voice Genie
- IVR Server



機能の説明

プロキシ サーバとパラレル サーバが大規模構成につきものの効率性の問題に 対処し、アプリケーション障害の際の機能とデータの喪失を最小限に抑えま す。

プロキシサーバは、地理的に広い範囲に分散したシステムの場合に特に有効 です。プロキシ環境では、サーバに接続する必要があるクライアントが複数の サーバ(プロキシモードで実行)に分散され、これらすべてが中央のサーバ(マ スタ)に集中します。1つのプロキシサーバに障害が発生すると、このサーバ に接続するクライアントだけが失われます。一方、単一サーバ環境では、1つ のサーバに障害が発生するとシステム全体が失われます。

パラレルサーバはロードシェアリングが可能です。これは、パラレルで実行 される1つのサーバの複数のインスタンスで、これらのインスタンス間に負荷 を分散します。パラレルサーバの1つに障害が発生すると、新しい要求が残り のサーバに分散されるため、サービスが失われることはありません。

機能の設定

プロキシまたはパラレルのGenesysサーバの構成は、サーバタイプによってさ まざまです。詳細情報およびご使用の環境でプロキシまたはパラレルサーバ を設定する詳細な手順については、適切な製品マニュアルを参照してください。



パート

サーバ整合性 —Transport Layer Security

このマニュアルのパートIIIでは、Genesys Transport Layer Security (TLS)の機能 を使用するための手順について説明します。また、OpenSSLツールキットと Windows証明書サービスを使用して、証明書を作成する例も取り上げます。こ の機能をサポートするGenesysコンポーネント間で安全なデータ交換を行うた めに、セキュリティ証明書をインストールし、コンポーネントを設定する手順 についても説明します。

以下の章から構成されます。

- 63 ページの第 8 章「Genesys Transport Layer Security の紹介」
- 67 ページの第 9 章 「Security Pack のインストール」
- 71ページの第 10章「証明書の生成とインストール」
- 89 ページの第 11 章「Genesys TLS の設定」
- 115 ページの第 12 章「Genesys TLS のトラブルシューティング」

パート III: サーバ整合性 — Transport Layer Security





8

Genesys Transport Layer Security の紹介

この章では、Genesys Transport Layer Security (TLS)の実装と、ご使用の Genesys 環境における構築の一般的ガイドラインについて説明します。以下の項から構成されます。

• 機能の要約(63ページ)

機能の要約

リリース7.5以降では、Genesysコンポーネント間で安全なデータ交換を行うために、オプションでTransport Layer Securityプロトコルを使用できます。TLSは インターネットの安全な通信を実現するための業界標準プロトコルで、SSL 3.0 (Secure Sockets Layer: セキュア ソケット レイヤ)に取って代わるものです。

すべてのGenesysコンポーネントはConfiguration Managerで設定されます。コン ポーネント間の安全なデータ交換を有効にするには、ホスト オブジェクトと コンポーネントを表すアプリケーション オブジェクトで、追加のパラメータ を設定する必要があります。

 注: このマニュアルの手順は、Genesys 設定の既存の接続に Transport Layer Security (TLS) 機能を追加することを前提としています。つまり、アプリ ケーションがすでにインストールされ、正しく設定され、ホストへの関 連付け、およびコンポーネント同士の関連付けが行われている必要があ ります。新規ホスト、アプリケーション、およびこれらの関連付けの設 定の詳細については、『Framework 7.6 Deployment Guide』を参照してく ださい。 Genesys TLS 機能を使用するには、事前に以下の手順を行う必要があります。

- UNIX の場合は、Genesys コンポーネントを実行する各ホスト コンピュー タに Security Pack をインストールします。67 ページの第9章を参照してく ださい。
- UNIX または Windows プラットフォームで証明書を作成してインストール します。71 ページの第 10 章を参照してください。
- 3. Configuration Manager で、アプリケーション固有またはホスト固有の設定 を行います。89ページの第 11 章を参照してください。

OpenSSLツールキットとWindows証明書サービスを使用して、証明書と対応す る秘密鍵を作成して管理できます。

セキュリティ上の利点

TLSは強力な認証、メッセージの秘匿性、および整合性を実現します。TLSで は、さまざまな暗号化オプションを使用してデータ転送の安全性を確保しま す。また、TLSはサーバ認証(オプションでクライアント認証)も行い、安全な 通信に関わる人や組織の身元を証明します。さらに、整合性チェック値によっ てデータの整合性も保証します。データ流出に対する保護だけでなく、TLSプ ロトコルはマスカレード攻撃、中間者攻撃、バケツリレー攻撃、ロールバック 攻撃、リプレイ攻撃に対する防御にも役立ちます。

サポートするコンポーネント

この項では、安全なデータ交換をサポートするコンポーネントの接続について 取り上げます。

注: リリース 7.5 以降では、いくつかの Genesys コンポーネントが Genesys TLS をサポートします。Genesys コンポーネントのサポートの詳細につ いては、該当する製品マニュアルを参照してください。

Configuration Layer コンポーネント

以下のように、すべてのConfiguration Layerの接続で安全なデータ交換がサポートされます。

- Configuration Server と Configuration Manager の間
- Configuration Server と Configuration Server Proxy の間
- Configuration Server と DB Server の間
- プライマリとバックアップ Configuration Server の間

Management Layer コンポーネント

以下に示すManagement Layerの接続で安全なデータ交換がサポートされます。

• Solution Control Server (SCS) と Solution Control Interface (SCI)の間

- SCS と Configuration Server/Configuration Server Proxy の間
- SCI と Configuration Server/Configuration Server Proxy の間
- SCI と DB Server の間
- プライマリとバックアップ Solution Control Server の間
- Message Server と DB Server の間

Media Layer コンポーネント

以下に示すMedia Layerの接続で安全なデータ交換がサポートされます。

- T-Server の間
- Network T-Server の間
- T-Server と Network T-Server の間
- ・ T-Server/Network T-Server と Configuration Server/Configuration Server Proxyの間
- ホット スタンバイモードのプライマリとバックアップ T-Server の間
- T-Server と、新しい T-Library で作成したカスタム クライアント アプリケー ションの間

Universal Routing コンポーネント

すべてのUniversal Routing コンポーネントと、この機能をサポートする Frameworkコンポーネントの間で、安全なデータ交換がサポートされます。

Outbound Contact コンポーネント

以下のOutbound ContactとFrameworkの接続で安全なデータ交換がサポートされます。

- Outbound Contact Server と CPD Server/CPD Proxy Server の間
- Outbound Contact Server と Configuration Server/Configuration Server Proxy の間
- Outbound Contact Server と T-Server の間
- Outbound Contact Server と DB Server の間
- CPD Server と CDP Proxy Server の間
- CPD Server と T-Server の間
- CPD Server/CDP Proxy Server と Configuration Server/Configuration Server Proxy の間

注: リリース 7.5 では、Message Server とそのクライアントの間の接続では、 安全なデータ交換がサポートされません。

環境の前提条件

このマニュアルの手順は、Genesys設定の既存の接続にGenesys TLS機能を追加 することを前提としています。つまり、アプリケーションがすでにインストー ルされ、正しく設定され、ホストへの関連付け、およびコンポーネント同士の 関連付けが行われている必要があります。これらのFrameworkコンポーネント の詳細と構築手順については、『Framework 7.6 Deployment Guide』を参照して ください。

サポートされるプラットフォーム

 注: Genesys 製品がサポートされるオペレーティング システムであっても、 Genesys TLS がサポートされない場合があります。UNIX ベースのオペレーティング システムの場合は、詳細について、69 ページの「環境変数の設定」を参照してください。

サポートされるWindowsバージョンについては、『Genesys 7 Supported Operating Systems and Databases』ホワイトペーパで、Genesysリリース7.xでサポートされるオペレーティングシステムとデータベースシステムを確認してください。この文書はGenesysテクニカルサポートのWebサイト http://genesyslab.com/support/dl/retrieve/default.asp?item=B6C52FB62DB42BB229 B02755A3D92054&view=itemにあります。

略語

このマニュアルでは、以下の用語と略語が使用されます。

CA	Certification Authority:認証機関
PEMフォーマット	証明書をエンコードするために使用できる テキスト(ASCII)フォーマット
PKCS	Public-Key Cryptography Standards : 公開鍵暗号化標準
PKI	Public Key Infrastructure :公開鍵インフラストラクチャ
TLS	Transport Layer Security







Security Pack のインストール

この章では、Genesys Security Pack を UNIX にインストールして構成する方法 について説明します。Security Pack には、共有ライブラリや CA (Certification Authority:認証機関)の例などのコンポーネントが含まれています。これを使 用して、証明書を生成し、Genesys コンポーネントがインストールされた UNIX コンピュータに導入することができます。

- この章は、以下の項から構成されます。
- サポートされるオペレーティング システム (67 ページ)
- Security Pack $\mathcal{O} \not\prec \mathcal{V} \not\prec \vdash \mathcal{V} (68 \, \overset{\frown}{\sim} \overset{\smile}{\mathcal{V}})$
- **注:** Genesys Security Pack on UNIX は、Genesys コンポーネントがインストー ルされた各UNIXホスト コンピュータにインストールする必要がありま す。

サポートされるオペレーティング システム

Genesys Security Pack on UNIXは、以下のオペレーティング システムでサポートされます。

オペレーティング システム	バージョン
AIX 32ビットモード	5.2, 5.3
HP-UX 32ビットモード	11.0、11.11
HP-UX 64ビットモード	11.0、11.11、11i v2
Linux 32ビットモード	RHEL 3.0、RHEL 4.0

表 3: サポートされるオペレーティング システム

表 3:	サポー	ト	されるオ	-ペレー	-ティ	ング	システ	ム(続き)
------	-----	---	------	------	-----	----	-----	----	----	---

オペレーティング システム	バージョン
Solaris 32ビットモード	8, 9
Solaris 64ビット モード	8, 9, 10

Security Pack のインストール

Security Packのインストールは、以下の手順で行います。

- 1. UNIX に Security Pack をインストールします。
- 2. オペレーティングシステムに対応する環境変数を設定します。

手順 : UNIX への Security Pack のインストール

手順開始

- Security Pack 7.5製品CDのsecurity_packディレクトリで、オペレーティングシステムに対応するディレクトリを開き、install.sh というシェルスクリプトを見つけます。
- コマンド ラインに以下のコマンドを入力して、コマンド プロンプトから スクリプトを実行します。
 sh install.sh
- 3. 要求されたら、Security Pack をインストールするコンピュータのホスト名 を指定します。
- 4. Security Pack をインストールするディレクトリを完全なパスで指定します。

インストール プロセスが終了すると、インストールが成功したというメッ セージが表示されます。ステップ4で、指定したディレクトリにSecurity Pack がインストールされます。

手順終了

次のステップ

• 69ページの「環境変数の設定」

環境変数の設定

Security Packをインストールしたら、オペレーティングシステムに対応した環 境変数を設定し(表4を参照)、Security Packライブラリのパスを指定する必要が あります。

表 4: 環境変数

オペレーティング システム	環境変数名
AIX	LIBPATH
HP-UX 32ビットモード	SHLIB_PATH
HP-UX 64ビットモード	LD_LIBRARY_PATH
Linux	LD_LIBRARY_PATH
Solaris	LD_LIBRARY_PATHおよび/または LD_LIBRARY_PATH_64





10 証明書の生成とインストール

この章では、オープンソースの OpenSSL ツールと Windows 証明書サービスを 使用して、証明書を生成する一般的な手順について概要を説明します。特定の 環境における証明書生成の実際の手順は、IT 部門のセキュリティ ポリシや使 用するツールによって大きく異なるため、この章で説明する手順とは異なる場 合があります。事前にネットワーク管理者に相談してから、Genesys コンポー ネント間の安全なデータ交換のために証明書を生成することをお奨めします。

この章は、以下の項から構成されます。

- OpenSSL を使用した証明書生成 (71 ページ)
- Windows 証明書サービスを使用した証明書生成 (78 ページ)
- MMC を使用した証明書の管理(84ページ)

OpenSSLはUNIXとWindowsでの証明書生成に使用できますが、Windows証明 書サービスはWindows Serverオペレーティングシステムでのみ使用可能です。 ただし、両方のツールで作成した証明書を、WindowsとUNIXオペレーティン グシステム両方で実行されるアプリケーション間の安全なデータ交換に使用 できます。

UNIXで安全な接続が必要になる可能性のあるアプリケーションを使用する場合は、OpenSSLを使用することをお奨めします。すべてのアプリケーションをWindowsで実行する場合は、Windows証明書サービスをお奨めします。

OpenSSL を使用した証明書生成

この項では、OpenSSL ツールを使用した証明書作成の例を取り上げます。この手順は、以下のステップから構成されます。

- 1. CA (Certification Authority: 認証機関)を設定します (72 ページを参照)。
- ステップ1で設定した CA を使用して証明書を生成します (74 ページを参照)。
- 3. UNIX や Windows に証明書をインストールします (75 ページを参照)。

Security Packをインストールしたディレクトリで、以下のスクリプトを見つけます。

- create_ca.sh—CA ファイルと生成した証明書を格納する CA 構造を作成します。
- create_cert.sh—UNIXおよびWindowsコンピュータで使用する証明書 を作成します。
- **注:** インストールされるファイルについては、67ページの第9章を参照して ください。

証明書を生成するために使用するスクリプトには、OpenSSLツールキットが必要です。これは、以下のOpenSSLプロジェクトのWebサイトで入手できます。 http://www.openssl.org

Windowsオペレーティング システム用のOpenSSLツールのビルド バイナリ は、同様にOpenSSLプロジェクトのWebサイトの以下のURLで入手できます。 http://www.slproweb.com/products/Win32OpenSSL.html

認証機関の設定

注: コール センター環境全体で、1 つの CA インスタンスのみを使用することを推奨します。

CAを設定するには、以下の手順を行います。

- 1. CA ファイル (スクリプト、設定ファイル、生成した証明書)を格納する CA ディレクトリを作成します。
- 2. create_ca.sh と create_cert.sh スクリプトを、インストール パッ ケージから作成した CA ディレクトリにコピーします。スクリプトに実行 許可があることを確認します。
- 以下のコマンドラインでパラメータを指定して(表5を参照)、bashシェルからcreate_ca.shスクリプトを実行します。 create_ca.sh [-keySz KEY_SIZE] [-time VALID_TIME] -CN COMMON_NAME [-E EMAIL] [-OU ORG_UNIT] [-O ORGANIZATION] [-L LOCALITY] [-S STATE] [-C COUNTRY]

表 5: CA スクリプトのパラメータ

パラメータ	説明
KEY_SIZE	(オプション) CAの秘密鍵のサイズ(ビット)。デフォルト 値は2048ビット
VALID_TIME	(オプション) CAの有効期間(日)。デフォルト値は356日
表 5: CA スクリプトのパラメータ(続き)

パラメータ	説明
COMMON_NAME	(必須) CAの名前
EMAIL	(オプション) CAの責任者の電子メール アドレス
ORG_UNIT	(オプション) CAの責任部署の名前
ORGANIZATION	(オプション) CAの責任組織の名前
LOCALITY	(オプション)市町村名
STATE	(オプション)州または地域の名前
COUNTRY	(オプション)国を示す2文字の略語

例:

create_ca.sh -CN "Basic Certification Authority" -E "youremail@yourdomain.com" -OU "Department" -O "Genesys Telecommunication Labs" -L "Daly City" -S CA -C US

認証機関ファイル

スクリプトが正しく実行されると、以下のようなデータ構造が作成されます。

- ca conf—このディレクトリには、以下のファイルが格納されます。
 - ◆ ca cert.pem—CAの自己署名証明書ファイル
 - 注: 安全なデータ交換が必要となる可能性がある Genesys コンポーネン トのホストとなる各コンピュータに、このファイルをコピーする必 要があります。詳細については、75ページの「証明書のインストー ル」を参照してください。
 - ca_priv_key.pem—CAの秘密鍵
 このファイルを使用して、特定のCAが発行するすべての証明書に署名します。ファイルは読み取り専用で、CA管理者アカウント以外は読み 取れないようにします。
 - ◆ ca.db—OpenSSL ツールキットが使用する内部 CA データベース
 - ◆ serial.num— 次に生成される証明書のシリアル番号が格納される内部CAファイル。シリアル番号で、CAが生成する証明書を一意に識別します。
 - ◆ ca.conf— 内部 CA 設定ファイル
- repository—CAが生成するファイルを格納するディレクトリ。詳細については、「鼎Aを使用した証明書生成 î」を参照してください。

CA を使用した証明書生成

CAを設定したら、CAを使用して証明書を生成します。

注: 同じ CA を使用して、特定の環境のすべての証明書を生成することをお 奨めします。

特定のホストコンピュータの証明書を生成するには、以下の手順を行います。

- 1. CAファイルが格納された CA ディレクトリに移動します。
- 2. 以下のコマンドラインでパラメータを指定して(表6を参照)、bash シェ ルから create_cert.sh スクリプトを実行します。 create_cert.sh [-keySz KEY_SIZE] [-time VALID_TIME] host HOST_NAME -CN COMMON_NAME [-OU ORG_UNIT] [-0 ORGANIZATION] [-L LOCALITY] [-S STATE] [-C COUNTRY] 例: create cert.sh -host myHOST.domain1.domain2.com -CN

create_cert.sh -host myHOST.domain1.domain2.com -CN myWorkstation

表 6: 証明書スクリプトのパラメータ

パラメータ	説明
KEY_SIZE	(オプション)ホストの秘密鍵のサイズ(ビット)。デ フォルト値は2048ビット
VALID_TIME	(オプション)証明書の有効期間(日)。デフォルト値 は100日
HOST_NAME	(必須) DNSホストの完全な名前
COMMON_NAME	(必須)ホストの名前
ORG_UNIT	(オプション)部署名
ORGANIZATION	(オプション)組織名
LOCALITY	(オプション)市町村名
STATE	(オプション)州または地域の名前
COUNTRY	(オプション)国を示す2文字の略語

ホストの証明書ファイル

スクリプトが正しく実行されると、repositoryディレクトリに以下のファイ ルが作成されます。

- <serial #> <host name> cert.pem—UNIX 用のホスト証明書
- <serial #>.pem—UNIX 用の証明書生成の補助ファイル
- <serial_#>_<host_name>_priv_key.pem—UNIX 用のホストの秘密鍵
- <serial_#>_<host_name>_cert.pfx—Windows用のPKCS #12ファイ ルフォーマット、秘密鍵、および証明書 ここで、
 - <serial_#>は生成された証明書のシリアル番号。これは、特定のCA が生成するすべての証明書に対して一意の番号です。
 - <host_name>はホストコンピュータ名。完全なDNSホスト名の最初の 部分です。

証明書のインストール

証明書を生成したら、UNIXまたはWindowsにインストールします。

 注: CA の自己署名証明書ファイル ca_cert.pem、およびこの CA が発行した最低 1 つの証明書を、安全なデータ交換が必要となる可能性がある Genesys アプリケーションのホストとなる各コンピュータにインストールする必要があります。

UNIX の場合

UNIX ホスト コンピュータに証明書をインストールするには、以下の手順を行います。

- 1. ca cert.pemファイルをコンピュータにコピーします。
- 2. <serial_#>_<host_name>_cert.pemおよび
 <serial_#>_<host_name>_priv_key.pemファイルを、コンピュータ
 のローカルディレクトリにコピーします。
- 3. このホストコンピュータで実行されるすべてのGenesysアプリケーション が、これらのファイルを読み取れることを確認します。
- 警告! <serial_#>_<host_name>_priv_key.pem ファイルには、重要な セキュリティ情報が格納されています。このファイルにアクセスでき るのが、このタイプの情報に対して作業を行う許可を持っている人だ けであることを確認します。

Configuration Manager を使用して、UNIX で安全なデータ交換をサポートする ようにアプリケーションを設定する場合は、以下のようになります。

- ca_cert.pemファイルの完全なパスが、[証明書] プロパティの[信頼され た CA] テキストボックスにコピーされる。
- <serial_#>_<host_name>_cert.pemファイルの完全なパスが、[証明 書] プロパティの [証明書] テキスト ボックスにコピーされる。
- <serial_#>_<host_name>_priv_key.pem ファイルの完全なパスが、 [証明書]プロパティの[証明書キー]テキストボックスにコピーされる。

詳細については、89ページの第 11章を参照してください。

Windows の場合

注: サーバアプリケーションの場合は、ローカル コンピュータ アカウント に証明書をインストールする必要があります。クライアント アプリケー ションの場合は、現在のユーザ アカウントに証明書をインストールする 必要があります。詳細については、84 ページの「MMC を使用した証明 書の管理」を参照してください。

Windows コンピュータに証明書をインストールするには、以下の手順を行います。

- Windows の [スタート]メニューで、[ファイル名を指定して実行]を選択し、mmc コマンドを実行して、Microsoft 管理コンソール (MMC) を起動します。
- 2. MMC の左側のペインで、[証明書]フォルダをクリックします(左側の ペインに[証明書]フォルダがない場合は、84 ページの「MMC を使用し た証明書の管理」を参照)。
- 3. [信頼されたルート証明書機関]フォルダを右クリックし、ショートカットメニューから[すべてのタスク]> [インポート]を選択します。証明書のインポートウィザードが起動します。
- 4. 最初のウィザードページで [次へ]をクリックします。
- 5. [**インポートする証明書ファイル**]ページで、CAの設定中に作成された ca cert.pemファイルの完全な名前を入力し、[次へ]をクリックします。
- 6. [証明書ストア]ページで、[証明書をすべて次のストアに配置する]を 選択します。[証明書ストア]テキストボックスが[信頼されたルート証 明書機関]に設定されていることを確認します。[次へ]をクリックします。
- **7.** [完了] をクリックします。
- 8. 左側のペインで、[証明書]フォルダをクリックします。
- 9. 左側のペインで、[個人]フォルダを右クリックして、ショートカットメニューから[すべてのタスク] > [インポート]を選択します。証明書のインポートウィザードが起動します。
- 10. 最初のウィザードページで [次へ]をクリックします。

- **11.** [**インポートする証明書ファイル**] ページで、証明書の生成中に作成され た<serial_#>_<host_name>_cert.pfxファイルの完全な名前を入力 します。[次へ]をクリックします。
- [パスワード]ページで[次へ]をクリックします。
 PKSC #12 フォーマットのホスト証明書は、空のパスワードで生成されます。
- 13. [証明書ストア]ページで、[証明書をすべて次のストアに配置する]を 選択します。[証明書ストア]テキストボックスが[個人]に設定されて いることを確認します。[次へ]をクリックします。
- 14. [完了]をクリックします。
- **15.** F5 を押して、MMC の表示を更新します。
- 16. 左側のペインで、[証明書] > [個人] > [証明書]を選択します。
- 17. 右側のペインで、リストからインポートした証明書を見つけて、ダブルク リックします(図1を参照)。

🚡 Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates] 🛛 📃 🗙					
🚡 File Action View Favorites Window Help 📃 🛃 🔟					_ 8 ×
← → 🗈 🖬 📭 😰 🛱					
Console Root		Issued To 🖉	Issued By	Expiration Date	Intended Purposes
E 🗐 Certificates (Local Computer)		techpubs4.us.int.genes	vienna	8/15/2008	Client Authenticatic
E Personal					
Certificates					
Trusted Root Certification Authorities					
Certificates					
Enterprise Trust					
Intermediate Certification Authorities					
Trusted Publishers					
Third-Party Root Certification Authorit					
Trusted People					
Other People	-				
		•			•
Personal store contains 1 certificate.					

図 1: Microsoft 管理コンソールのウィンドウ

- 18. [証明書]ダイアログボックスで、[詳細]タブをクリックします。
- 19. 証明書の拇印を表示するには、リストから [拇印] を選択します。16 進数の数字からなる拇印が、ダイアログボックスの下部に表示されます(図 2 を参照)。

Certificate	? ×
General Details Certification Path	1
	[
Show: <all></all>	<u> </u>
Field	Value 🔺
Certificate Template Inform	Template=1.3.6.1.4.1.311.21
Authority Key Identifier	KeyID=96 c8 8d 55 8a b2 06 f
CRL Distribution Points	[1]CRL Distribution Point: Distr
Authority Information Access	[1]Authority Info Access: Acc
Enhanced Key Usage	Client Authentication (1.3.6.1
Application Policies	[1]Application Certificate Polic
Thumbprint algorithm	sha1
Thumbprint	3f 49 99 6a 9f c9 36 50 24 d5 💌
3f 49 99 6a 9f c9 36	50 24 d5 23 5e 43 b9 41
54 ao 78 50 50	
1	
	At Droperties
	Copy to File
	04

図 2: [証明書]ダイアログボックス —[詳細]タブ

Windows 証明書サービスを使用した証明書生成

この項では、Windows証明書サービスを使用した証明書作成の例を取り上げます。

Genesys TLS機能を使用するには、セキュリティ証明書が以下の要件を満たす 必要があります。

- 1. Genesys サーバアプリケーションが使用する証明書が、serverAuth、 clientAuth、および emailProtection の拡張属性を持っている。
- **2.** Genesys GUI アプリケーションが使用する証明書が、clientAuth および emailProtection の拡張属性を持っている。

サーバおよびGUIアプリケーションの証明書テンプレートが、これらの要件を 満たすように正しく設定されている必要があります。

注: この項で取り上げる例は、Windows証明書サービスがインストールされ、 設定されていることを前提としています。Windows 証明書サービスのイ ンストールと設定方法については、Windows の適切なマニュアルを参照 してください。



Windows証明書サービスで証明書を生成する手順は、以下のステップから構成 されます。

- Windows Server オペレーティング システムが実行され、Windows 証明書 サービスがインストールされ設定されているコンピュータで、証明書を生 成します (79ページを参照)。
- 2. 証明書を取得します (84 ページを参照)。
- Genesys アプリケーションのホストとなるコンピュータに証明書をインストールします。このコンピュータが、証明書を生成したコンピュータと異なる場合は、証明書をエクスポートする必要があります。詳細については、 85ページの「証明書のエクスポート」を参照してください。
- 4. 証明書を PKCS #12 フォーマットから PEM フォーマットに変換します (87 ページを参照)。このステップは、Windows で作成した証明書を UNIX に インストールする場合に必要です。

リモート コンピュータから証明書を入手したい場合は、87ページの「リモート コンピュータからの証明書の取得」を参照してください。

証明書の生成

証明書を生成するには、以下の手順を行います。

 Web ブラウザを起動して、以下の URL を入力します。 http://<server-name>/certsrv

ここで、<server-name>は、Windows Server オペレーティング システム が実行され、Windows 証明書サービスがインストールされ構成されている サーバです。

Microsoft 証明書サービスの [Welcome (ようこそ)](または [Home (ホーム)])ページで、[Request a certificate (証明書を要求する)] リンクをクリックします (80 ページの図 3 を参照)。

🚰 Microsoft Certificate Services - Microsoft Internet Explorer	_ [] ×
File Edit View Favorites Tools Help	<u></u>
🔾 Back 🔹 🕑 👻 🖹 😰 🏠 🔎 Search 👷 Favorites 🧭 🌭 💯 🔹 🧾 🐭 📖	
Address 🍘 http://vienna/certsrv/	s » 🔁 🔹
Microsoft Certificate Services vienna	Home
Welcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate over the Web, sign and encrypt messages, and, depending upon the type of certificate request, perform other security tasks.	with you
You can also use this Web site to download a certificate authority (CA) certificate, certificate, or certificate revocation list (CRL), or to view the status of a pending request.	icate
For more information about Certificate Services, see Certificate Services Documentation	on.
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	
e Succel intre	net //

図 3: Microsoft 証明書サービスの [Home] ページ

3. [Request a Certificate (証明書の要求)] ページで、[advanced certificate request (証明書の要求の詳細設定)] リンクをクリックします(図4を参照)。

🚈 Microsoft Certificate Services - Microsoft Internet Explorer		<u>_ ×</u>
File Edit View Favorites Tools Help		
🕓 Back 🔹 🕤 👻 😰 🐔 🔎 Search 👷 Favorites 🛷 🙆 👻 👻 💌	- 27 - 2	
Address 🙆 http://vienna/certsrv/certrgus.asp	💌 🔁 Go	Links » 📆 🔹
		A
Microsoft Certificate Services vienna		Home
Barrussta Cartificata		
Request a Certificate		
Select the certificate type:		
User Certificate		
Or, submit an <u>advanced certificate request</u> .		
a) hone		d intranat
		an incranec //.

図 4: [Request a Certificate (証明書の要求)] ページ

4. [Advanced Certificate Request (証明書の要求の詳細設定)] ページで、[Create and submit a request to this CA (このCAへ要求を作成し送信する)] リンクをクリックします(図5を参照)。



図 5: [Advanced Certificate Request (証明書の要求の詳細設定)] ページ

- 5. [Advanced Certificate Request (証明書の要求の詳細設定)] ページで、以下の情報を入力します。
 - **a.** [Certificate Template (証明書テンプレート)]テキストボック スで、適切な証明書テンプレートを選択します(MutualTLS2 など)。
 - **b.** [Name (名前)]テキストボックスに、DNSホストの完全な名前を入力 します。
 - c. [Key Options (キー オプション)]で、以下の手順を行います。
 - [Create new key set (新しいキー セットを作成する)]を選 択します。
 - [Key Size (**キーのサイズ**)] テキスト ボックスで、キーのサイ ズを指定します。
 - 必要に応じて、[Automatic key container name (自動キー コンテナ名)]または[User specified key container name (ユーザ指定のキー コンテナ名)]を選択します。
 - [Mark key as exportable (エクスポート可能なキーとして としてマークする)]を選択します。
 - d. [Submit (送信)]をクリックします(82ページの図6を参照)。

Microsoft Certific	ate Services - Microsoft Internet Explorer	
File Edit View	Favorites Tools Help	27
😋 Back 🔹 💮 🔹 [🕴 😰 🏠 🔎 Search 🥠 Favorites 🛷 😥 📲 🛛 💭 📽 🗮	
Address 🙆 http://vi	enna/certsrv/certrgma.asp 🗾 🔂 Go	Links » 🐔 🔹
10 A A A A A		
Microsoft Certifi	cate Services vienna	Home
Advanced Ce	rtificate Request	
Cortificato Tom	late:	
certificate rein	MutualTI S2 V	
	Wuldan Loz	
Identifying Infor	mation For Offline Template:	
Name:	John Johnson	
E-Mail:	johnson@mydomain.com	
Company:	Genesys	
Department:	Engineering	
City:	Daly City	
State:	CA	
Country/Region:	US	
Key Options:		
	Create new key set	
CSP:	Microsoft RSA SChannel Cryptographic Provider	
Key Usage:	@ Exchange	
Key Size:	1024 Min: 1024 (common key sizes: 1024 2048 4008 8192 16384) Max16384	
	Automatic key container name O User specified key container name	
	I Mark keys as exportable	
	Export keys to file	
	Enable strong private key protection	
	Store certificate in the local computer certificate store Stores the certificate in the local computer store	
	instead of in the user's certificate store. Does not install the root CA's certificate. You must be an	
	administrator to generate or use a key in the local	
	machine store.	
Additional Optio	ns:	
Request Format:	CMC OPKCS10	
Hash Algorithm:	SHA-1	
	Univ used to sign request.	
	Li Save request to a file	
Attributes:		
	X	
Friendly Name:		
-	Output a	
	Submit >	-
e]	Local	intranet //

図 6: [Advanced Certificate Request (証明書の要求の詳細設定)] ページ

証明書の要求を送信すると、確認ページが表示され、次に [Certificate Issued (証明書は発行されました)] ページが表示されます。
 [Certificate Issued (証明書は発行されました)] ページで、
 [Install this certificate (この証明書のインストール)] リンクをクリックします(図7を参照)。

🚰 Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
🚱 Back 🔹 🕤 🖌 🖹 🛃 🐔 🔎 Search 👷 Favorites 🛛 😥 🕹 🔛 🗸 📮 🐭 😩	
Address 🕘 http://vienna/certsrv/certfnsh.asp 💌 ラ Go	Links » 📆 🔹
	1
Microsoft Certificate Services vienna	Home
Certificate Issued	
The certificate you requested was issued to you	
Install this certificate	
Done Sector	intranet

図 7: [Certificate Issued (証明書は発行されました)] ページ

 表示されるシステム警告プロンプトを受け入れると、[Certificate Installed (インストールされた証明書)]ページが表示されます(図8 を参照)。

Microsoft Certificate Services - Microsoft Internet Explorer		_ 🗆 🗙
File Edit View Favorites Tools Help		
🔇 Back 🔹 🕤 👻 😰 🐔 🔎 Search 👷 Favorites 🙆 🔹 🍇 🏢 🗸 💭 🐲 👯		
Address 🙆 http://vienna/certsrv/certmpn.asp 💌 🄁 Go	Links »	🔁 •
		^
Microsoft Certificate Services vienna	<u>Ho</u>	me
Out Sector Installed		
		_
Your new certificate has been successfully installed.		
		_
		*
Done Succession Contraction Succession Contraction Con	ntranet	11.

図 8: [Certificate Installed (インストールされた証明書)] ページ

証明書の取得

83 ページのステップ6で、証明書をインストールしなかった場合は、以下の手順で証明書を取得してインストールできます。

- Microsoft 証明書サービスの [Home (ホーム)] ページで (80 ページの図 3 を参照)、[View the status of a pending certificate request (保留中の証明書の要求の状態)] リンクをクリックします。
- リストから適切な要求を選択します。
 証明書の要求が承認されると、[Certificate Issued (証明書は発行 されました)]ページが表示されます。
- **3.** [Install this certificate (この証明書のインストール)] リンク をクリックして、証明書をインストールします。

MMC を使用した証明書の管理

Microsoft管理コンソール(MMC)を使用して、Windowsプラットフォームで証明 書を管理できます。詳細については、*Microsoft管理コンソールのヘルプ*を参照 してください。

証明書管理のための MMC の設定

証明書管理のために MMC を設定するには、以下の手順を行います。

- 1. Windows の [スタート]メニューで、[ファイル名を指定して実行]を選 択し、mmc コマンドを実行して、Microsoft 管理コンソールを起動します。
- 2. [ファイル] > [スナップインの追加と削除]を選択します。
- 3. [スナップインの追加と削除]ダイアログボックスで、[追加]をクリックします。
- **4.** [スタンドアロン スナップインの追加]ダイアログボックスで、リストから[証明書]を選択し、[追加]をクリックします。
- 5. [証明書スナップイン]ダイアログボックスで、[コンピュータ アカウ ント]を選択し、[次へ]をクリックします。
 - **注:** クライアントアプリケーションの証明書を管理するには、[ユーザ アカウント]オプションを選択します。
- 6. [コンピュータの選択]ダイアログボックスで、[ローカル コンピュー タ (このコンソールを実行しているコンピュータ)]を選択し、[完了] をクリックします。
- [スタンドアロン スナップインの追加]ダイアログボックスで、[閉じる]をクリックします。

8. [スナップインの追加と削除]ダイアログボックスで、[OK]をクリック します。

左側のペインの[コンソールルート]に[証明書]項目が追加されます (85ページの図9を参照)。

🌇 Console1 - [Console Root]		
📸 File Action View Favorites Window	/ Help	X
🔁 Console Root	Name	
🖻 🚳 Certificates (Local Computer)	Certificates (Local Computer)	
🗄 📄 Personal		
Trusted Root Certification Authoritie		
Enterprise Trust		
Intermediate Certification Authoritie		
Trusted Publishers		
Third Dayty Deat Cartification Author		
Trusted People		
Other People		
in in it capito		
	<u> </u>	

図 9: 証明書管理のための MMC の設定

MMC設定をファイルに保存するには、[ファイル] > [名前を付けて保存]を 選択します。

証明書のエクスポート

証明書と秘密鍵を別のコンピュータにインストールするには、以下の手順でエ クスポートする必要があります。

- 1. Windows の [スタート]メニューで、[ファイル名を指定して実行]を選 択し、mmc コマンドを実行して、Microsoft 管理コンソールを起動します。
- 2. 保存したコンソール設定を開くか、[ファイル] > [スナップインの追加 と削除]を選択します。
- **3.** [スナップインの追加と削除]ダイアログボックスで、[追加]をクリックします。
- **4.** [スタンドアロン スナップインの追加]ダイアログボックスで、リストから[証明書]を選択し、[追加]をクリックします。
- 5. [証明書スナップイン]ダイアログボックスで、[コンピュータ アカウ ント]を選択し、[次へ]をクリックします。
- 6. [コンピュータの選択] ダイアログ ボックスで、[ローカル コンピュー タ (このコンソールを実行しているコンピュータ)]を選択し、[完了] をクリックします。

- [スタンドアロン スナップインの追加]ダイアログボックスで、[閉じる]をクリックします。
- 8. [スナップインの追加と削除]ダイアログボックスで、[OK]をクリック します。

左側のペインの[コンソールルート]に[証明書]項目が追加されます (86ページの図 10 を参照)。

🚡 Console1 - [Console Root\Certificates (Loca	l Computer)\Personal\Cert	ificates]			
📸 File Action View Favorites Window H	elp				×
Console Root	Issued To 🛆	Issued By	Expiration	Intended P	Friendly
E- Certificates (Local Computer)	techpubs.domain1.domain	vienna	8/15/2008	Client Auth	<none></none>
E-Personal					
Certificates					
Trusted Root Certification Authorities					
Enterprise Trust					
Intermediate Certification Authorities					
Trusted Publishers					
Untrusted Certificates					
Third-Party Root Certification Authorities					
I rusted People					
the concerneepie					
Personal store contains 1 certificate.					

図 10: MMC による証明書のエクスポート

- 右側のペインで、リストから証明書を見つけて、右クリックします。ショートカットメニューから[すべてのタスク]>[エクスポート]を選択して、証明書のエクスポートウィザードを起動します。
- 10. 最初のウィザードページで [次へ]をクリックします。
- **11.** 次のページで、[はい、秘密キーをエクスポートします]を選択し、[次 へ]をクリックします。
- **12.** [エクスポート ファイルの形式]ページで、使用可能なエクスポートファ イルフォーマットは PKCS #12 だけです。[次へ]をクリックします。
- **13.** [パスワード]ページで、パスワードを入力して確認します。[次へ]を クリックします。
- **14.** [エクスポートするファイル]ページで、証明書のパスとファイル名を指定します。[次へ]をクリックします。
- 15. [完了]をクリックして、エクスポート手順を終了します。

PKCS #12 から PEM への変換

Windowsで作成した証明書をUNIXプラットフォームにインストールする必要 がある場合は、OpenSSLを使用して、以下のコマンドラインを入力します。 openssl pkcs12 -nodes -passin pass:<password> -in <pfx file> -out <pem file>

ここで、

- <password>はPKCS#12ファイルのエクスポートセッションで設定した パスワード。このフィールドは空でもかまいません。
- <pfx file>はPKCS #12フォーマットの証明書ファイルの名前。
- <pem file>は出力ファイルの名前。

変換後に、<pem file>に証明書および秘密鍵データが格納されます。これ で、証明書と秘密鍵データに個別の2つのテキストファイルを作成して、以下 のフォーマットで、それぞれに対応するデータをコピーできます。

---BEGIN CERTIFICATE---

[証明書データ]

---END CERTIFICATE---

 秘密鍵ファイルで、以下のように、"---BEGIN RSA PRIVATE KEY---"と"---End RSA PRIVATE KEY---"で囲まれた RSA 秘密鍵データを、 RSA 秘密鍵データファイルにコピーします。

---BEGIN RSA PRIVATE KEY---

[秘密鍵データ]

---END RSA PRIVATE KEY---

リモート コンピュータからの証明書の取得

リモートコンピュータから証明書を取得するには、以下の手順を行います。

- 1. Windows の [スタート]メニューで、[ファイル名を指定して実行]を選 択し、mmc コマンドを実行して、Microsoft 管理コンソールを起動します。
- 2. [ファイル] > [スナップインの追加と削除]を選択します。
- 3. [スナップインの追加と削除]ダイアログボックスで、[追加]をクリッ クします。
- **4.** [スタンドアロン スナップインの追加]ダイアログボックスで、リストから[証明書]を見つけて選択します。[追加]をクリックします。
- 5. [証明書スナップイン]ダイアログボックスで、[コンピュータ アカウ ント]を選択し、[次へ]をクリックします。

- **6.** [コンピュータの選択] ダイアログ ボックスで、[別のコンピュータ]を 選択し、リモート ターゲット コンピュータの名前を入力するか、[参照] ボタンを使用して検索します。[完了]をクリックします。
- 7. [スナップインの追加と削除] ダイアログ ボックスで、[OK] をクリック します。

メイン スナップイン コンソール ウィンドウの [コンソール ルート]の 下に、新しいスナップイン項目が追加されます。

ターゲットコンピュータのすべての証明書の例を参照したり、特定の証明 書の情報を表示したりできます。選択したオプションによっては、MMC で、ターゲットコンピュータの証明書をリモートから管理することもでき ます。

- 8. 左側のペインで、[証明書] > [個人] > [証明書]を選択します。
- 9. 右側のペインで、リストから証明書を見つけて、ダブルクリックします (77 ページの図1を参照)。
- 10. [証明書]ダイアログボックスで、[詳細]タブをクリックします。
- 11. リストから [拇印] を選択します。16 進数の数字からなる拇印が、ダイ アログボックスの下部に表示されます(例については、78 ページの図2を 参照)。
- 12.16 進数の数字は、セキュリティ設定に使用します。詳細については、89 ページの第 11 章を参照してください。



1 1 Genesys TLS の設定

証明書を作成してホスト コンピュータにインストールしたら、証明書を安全 な接続で使用するために、Genesys アプリケーションを設定する必要がありま す。デフォルトでは、Genesys アプリケーション間の接続は安全な接続ではあ りません。この章では、この設定の方法について説明します。以下の項から構 成されます。

- 概要(89ページ)
- 安全なポートの設定(90ページ)
- ・ セキュリティ証明書の割り当て(91ページ)
- ホスト証明書を使用するためのサーバアプリケーションの設定 (102 ページ)
- ・ 安全なクライアント接続の設定(103ページ)
- Configuration Server と DB Server 間の安全な接続の設定 (107 ページ)
- 安全な HA 同期接続の設定 (111 ページ)

概要

設定手順は、以下のステップから構成されます。

- サーバアプリケーションに対して、新しい安全なポートを追加するか、既存のサーバポートを安全な接続用に変更して、アプリケーションが使用する証明書を設定します(ホスト証明書を推奨)。
- クライアント アプリケーションに対して、安全なサーバ ポートに接続す るように接続設定を変更します。
 - **注:** サーバタイプのクライアントに対しては、サーバアプリケーション に必要な設定手順を行います。

参加するクライアントとサーバアプリケーションのタイプには関係なく、すべての安全な接続を同じ方法で設定します。唯一の例外はConfiguration Server

の接続です。この接続の詳細については、107ページの「Configuration Serverと DB Server間の安全な接続の設定」を参照してください。

注: この章で取り上げる手順は、Genesys 7.6 環境の既存の接続に Genesys Transport Layer Security (TLS) を追加することを前提としています。つま り、アプリケーションがすでにインストールされ、正しく設定され、ホ ストへの関連付け、およびコンポーネント同士の関連付けが行われてい る必要があります。新規ホスト、アプリケーション、およびこれらの関 連付けの設定の詳細については、『Framework 7.6 Deployment Guide』を 参照してください。

以前のリリースのGenesysコンポーネントを使用している場合は、リリース 7.6 にアップグレードしてから、コンポーネント間の安全な接続を設定する必要があります。

安全なポートの設定

リリース7.5では、Genesys TLSをサポートするサーバアプリケーションが、複数のサーバポートをサポートするように変更されました。これによって、同時にすべてのサーバ接続にではなく、セキュリティが必要な接続にだけ安全な通信を設定することができます。特定のサーバとの接続に安全なデータ交換機能を使用する場合は、安全な接続用に新しいポートを設定し、既存の安全でないポートはセキュリティが不要な接続用にそのままにしておくことをお奨めします。

手順 : サーバ タイプのアプリケーションの安全なポートの設定

手順開始

- 1. [アプリケーション プロパティ]ダイアログ ボックスを開きます。
- 2. [サーバ情報]タブをクリックします。
- [ポート] セクションで、[ポートの追加] をクリックします。[Port Properties] ダイアログボックスが表示されます(91ページの図11を参照)。



🜉 secure [techpubs4:301	0] Properties 🛛 🗙
Port Info Certificate Adva	anced
Port ID.	secure
Communication Port	5678 💽 🚺
Cognection Protocol	
HA sync:	Г
Listening <u>M</u> ode:	C Unsecured
	Secured
OK	Cancel Help

図 11: [Port Properties] ダイアログ ボックス

- **4.** [Port Properties] ダイアログ ボックスの [ポート情報] タブで、以下の手順を行います。
 - **a.** [ポート ID] ボックスに、ポート ID を入力します。
 - **b.** [通信ポート] ボックスに、新しいポートの番号を入力します。
 - c. [接続プロトコル]ボックスで、必要に応じて、接続プロトコルを選択 します。
 - d. [安全]オプションを選択します。ポートの設定対象のアプリケーションがConfiguration Serverの場合は、代わりに[Auto Detect]オプションを選択します。106ページの「Configuration Serverの自動検出ポートの設定」を参照してください。
 - e. [OK]をクリックします。
- 5. [OK] をクリックして、新しい設定を保存します。

手順終了

セキュリティ証明書の割り当て

安全な接続用の新しいサーバ ポートを作成したら、以下のいずれかの方法で 証明書を設定します。

- 証明書をホストに割り当て、この証明書を使用して、このホストにある任意のサーバアプリケーションの任意の安全なポートを介して、安全なデータ交換を行います。
- サーバアプリケーションに証明書を割り当て、この証明書を使用して、このアプリケーションの任意の安全なポートを介して、安全なデータ交換を行います。アプリケーションに割り当てた証明書は、ホストに割り当てた証明書より優先されます。

- サーバ アプリケーションの特定のポートに証明書を直接割り当て、この ポートを介して、安全なデータ交換を行います。ポートに割り当てた証明 書は、ホストやアプリケーションに割り当てた証明書より優先されます。
- 注: アプリケーションやポートを個別の証明書で保護する特別な理由がない限り、ホストレベルで証明書を割り当て、ホスト証明書を使用して、ホストに常駐するすべてのアプリケーションに安全なデータ交換を提供することをお奨めします。

Configuration Manager で、セキュリティ関連のプロパティを表示するには、以下の手順を行います。

- 1. Configuration Manager のメイン メニューで、[ビュー] > [オプション] を選択します。
- **2.** [オプション] ダイアログ ボックスで、[Show advanced security information] チェック ボックスをオンにします。
- 3. [OK] をクリックします。
- **注**: 安全なデータ交換を設定する前に、特定の Genesys コンポーネントが実行されるホスト コンピュータに証明書がインストールされ、証明書情報を取得できることを確認する必要があります。75ページの「証明書のインストール」を参照してください。

ホストへの証明書の割り当て

ホスト証明書を使用して、そのホストの任意のサーバアプリケーションの任 意のポートを介して、安全なデータ交換を行うには、まず、ホストに証明書を 割り当て、サーバアプリケーションを設定する必要があります。

手順:

ホストへの証明書の割り当て

手順開始

- Configuration Manager で、安全な接続が必要なサーバアプリケーションがあるホストを選択します。アプリケーションがあるホストの名前を見つけるには、アプリケーションのプロパティを確認します。
- **2.** [ホスト プロパティ]ダイアログ ボックスを開きます。
- 3. [一般] タブを開き、[デフォルトの証明書] セクションで、生成してイ ンストールした証明書の値を指定します。この手順は、アプリケーション が実行されるプラットフォームによって異なります。

Windows の場合:

a. [証明書の参照]ボタンをクリックします。

b. [<ホスト名>ホストについて証明書を選択してください]ダイアログボックスで、リストから証明書を選択し、[OK]をクリックします(図 12を参照)。

インストールされる証明書については、75ページの「証明書のインストール」を参照してください。

🛄 techpubs4 [techpub	s4:3010] Properties	×
General Security Dep	endency	
<u>N</u> ame:	techpubs4	
<u>I</u> P Address:	172 . 21 . 9 . 247	
OS Information		
<u>O</u> S Type:	Windows Server 2003	
<u>∨</u> ersion:		
LCA Port	4999	
Solution Control Server:	📡 [None] 💽 🚅	
Default Certificate		
<u>C</u> ertificate:		
D Select ce	ertificate on host "techpubs4"	? ×
Certil Select th	ne certificate you want to use.	
I		
	he Trend Telesded Du	Evine Research Eveloption
Issued	Tto Issued Intended Pu	Friendry name Expiration
	npubs4.us.in QA_DCO Server Autn	techpubs+ 10/30/200
		>
	OK Cano	el <u>V</u> iew Certificate

図 12: ホストの設定: Windows の場合の証明書の選択

これで、証明書情報が [ホスト プロパティ] ダイアログ ボックスのそれ ぞれのフィールドに表示されます (94 ページの図 13 を参照)。

📕 techpubs4 [techpubs4:3010] Properties	×
General Security Dependency	
Name: techpubs4	
_P Address: 172 . 21 . 9 . 247 □ OS Information	
OS Type: Windows Server 2003	
⊻ersion: 🔽	
LCA Port 4999	
Solution Control Server: 🚺 [None] 💽 🚄	
Default Certificate Certificate: 9A AB DB C4 02 29 3A 73 35 9	
Description: techpubs.domain1.domain2.com, vie	
Certificate Key:	
Irusted CA:	
State Enabled	
E OK Cancel Apply Help	

図 13: ホストの設定 : Windows の [デフォルトの証明書] セクション

UNIX の場合:

- a. [証明書]テキストボックスで、
 <serial_#>_<host_name>_cert.pem ファイルの完全なパスを指定します。
- b. [証明書キー]テキストボックスで、
 <serial_#>_<host_name>_priv_key.pemファイルの完全なパス を指定します。
- c. [信頼されたCA]テキストボックスで、ca_cert.pemファイルの完全 なパスを指定します。

インストールされるファイルについては、75 ページの「証明書のインス トール」を参照してください。

注: [解説] プロパティはオプションです。

これで、証明書情報が [ホスト プロパティ] ダイアログ ボックスのそれ ぞれのフィールドに表示されます (95 ページの図 14 を参照)。

👼 techpubs4 [techpubs4:3010] Properties	×
General Annex Security Dependency	
Name: techpubs4	•
IP Address: 172 . 21 . 9 . 247	
OS Type: Windows Server 2003	•
⊻ersion:	-
LCA Port 4999	- -
Solution Control Server: 🔀 SCS	- 🖻
Default Certificate Certificate: //home/tech/sec/aix_ce	rt.pem 💕
Description:	
Certificate Key: /home/tech/sec/aix_pri	v_key.pem
Irusted CA: //home/tech/sec/techpu	ibs_dco.pem
☑ <u>S</u> tate Enabled	
B OK Cancel Apply	Help

図 14: ホストの設定: UNIX の [デフォルトの証明書] セクション

手順終了

ホストの[付加情報]タブ

ホスト オブジェクトを設定すると、[**ホスト** プロパティ]ダイアログボック スの[デフォルトの証明書]セクションで指定した証明書情報が、[付加情報] タブの[セキュリティ]セクションにも表示されます。[セキュリティ]セク ションの設定オプションは、[デフォルトの証明書]セクションのものと同様 で、ホストに割り当てられた証明書のパラメータを表しています。

手順:

以前に割り当てた証明書のホストからの削除

手順開始

- 1. [ホスト プロパティ]ダイアログ ボックスを開きます。
- 2. [一般] タブの [デフォルトの証明書] セクションで、すべての証明書パ ラメータを削除し、[OK] をクリックします。

手順終了

アプリケーションへの証明書の割り当て

注: アプリケーションやポートを個別の証明書で保護する特別な理由がない限り、ホストレベルで証明書を割り当て、ホスト証明書を使用して、ホストに常駐するすべてのアプリケーションに安全なデータ交換を提供することをお奨めします。

アプリケーションの証明書を使用して、特定のサーバアプリケーションの任 意のポートを介して、安全なデータ交換を行うには、まず、このアプリケー ションに証明書を割り当て、サーバアプリケーションの設定を行う必要があ ります。

手順:

アプリケーションへの証明書の割り当て

手順開始

- **1.** [**アプリケーション プロパティ**]ダイアログ ボックスを開きます。
- 2. [サーバ情報]タブをクリックします。
- 3. [証明書ビュー] セクションで [アプリケーション] オプションを選択し、 [証明書のプロパティ] ボタンをクリックします。
- **4.** [証明書のプロパティ]ダイアログボックスで、セキュリティパラメー タを指定します。この手順はプラットフォームによって異なります。

Windows の場合:

- **a.** [証明書の参照] ボタンをクリックします。
- b. [<ホスト名>ホストについて証明書を選択してください]ダイアログボックスで、リストから証明書を選択し、[OK]をクリックします(96ページの図15を参照)。

インストールされる証明書については、75ページの「証明書のインストール」を参照してください。

(techpubs4:3010] Property	rties
Certificate	
<u>C</u> ertificate: Description:	9a ab db c4 02 29 3a 73 35 90 b0 6
Certificate <u>K</u> ey:	
Irusted CA:	
	OK Cancel Help

図 15: アプリケーションの設定: Windows の場合の証明書の選択

c. [証明書のプロパティ]ダイアログ ボックスで、[OK]をクリックしま す。

これで、[**サーバ情報**]タブの[証明書ビュー]セクションに、割り当て た証明書の値が表示されます(図16を参照)。

TServer_NEC_2 [techpubs4:3010] Properties
Connections Options Annex Security Dependency General Switches Server Info Start Info
Host: Techpubs4 Ports ID A Listening port Secu Conn H Idefault 5588 Secure 8899 Yes
Add Port Edit Port Delete Port Certificate View Certification Certification
Certificate: "9a ab db c4 02 29 3a 73 35 90 b0 65 2f 3d 32 b5 1e aa f1 7c" Description:""
Backup Server: 💭 [None] 💽 📂 Redundancy Type: Hot Standby
Reconnect Attempts: 1
B OK Cancel Apply Help

図 16: アプリケーションの設定:アプリケーション証明書の割り当て (Windows)

UNIX の場合:

- a. [証明書] テキスト ボックスで、
 <serial_#>_<host_name>_cert.pem ファイルの完全なパスを指定します。
- b. [証明書キー]テキストボックスで、
 <serial_#>_<host_name>_priv_key.pemファイルの完全なパス を指定します。
- **c.** [信頼されたCA]テキストボックスで、ca_cert.pemファイルの完全 なパスを指定します(図17を参照)。

インストールされるファイルについては、75 ページの「証明書のインストール」を参照してください。



(techpubs4:3010] Prop	erties 🗙
Certificate	
Certificat	s: /home/tech/sec/aix_cert.pem
Description	n l
Certificate <u>K</u> e	y: /home/tech/sec/aix_priv_key.pem
Irusted C/	/home/tech/sec/techpubs_dco.pem
	OK Cancel Help

図 17: アプリケーションの設定: UNIX の証明書の設定

d. [証明書のプロパティ]ダイアログボックスで、[OK]をクリックしま す。

これで、[サーバ情報]タブの[証明書ビュー]セクションに、割り当て た証明書の値が表示されます (98 ページの図 18 を参照)。

😹 TServer_NEC [techpubs4:3010] Properties 🛛 🛛 🔀				
Connections Options Annex Security Dependency General Switches Server Info Start Info				
Host: 🕢 techpubs4				
ID A Listening port Secu Conn H				
Secure 5678 Yes				
Add Port Edit Port Delete Port				
C Host © Application				
Certificate: "/home/tech/sec/aix_cert.pem" Description:"" Key: "/home/tech/sec/aix_priv_key.pem"				
Backup Server: 🚺 [None]				
Redundancy Type: Not Specified				
Reconnect Timeout: 10				
Reconnect Attempts: 1				
B OK Cancel Apply Help				

図 18: アプリケーションの設定:アプリケーション証明書の割り当て (UNIX)

5. [アプリケーション プロパティ] ダイアログ ボックスで、[OK] をクリッ クして新しい設定を保存します。

手順終了

アプリケーションの[オプション]タブ

サーバアプリケーションを設定すると、[アプリケーション プロパティ]ダ イアログボックスにある[サーバ情報]タブの[証明書]セクションで指定し た証明書情報が、[オプション]タブの[セキュリティ]セクションにも表示さ れます。[セキュリティ]セクションの設定オプションは、[証明書]セクショ ンのものと同様で、アプリケーションに割り当てられた証明書のパラメータを 表しています(99ページの図19を参照)。

😹 TServer_NEC	[techpubs4	:3010] F	roperties	×
General Connections	Switches Options	S Annex	erver Info Security	Start Info Dependency
Security	•		🗙 🔜 🗴 Value	0 🙀 🕲
Enter text her <u>abs</u> certificate <u>abs</u> certificate- <u>abs</u> trusted-ca	e key	7	Enter text here "/home/tech/ "/home/tech/ "/home/tech/	sec/aix sec/aix sec/tec

図 19: アプリケーションの設定: セキュリティ オプション

手順:

以前に割り当てた証明書のアプリケーションからの削除

手順開始

- 1. [アプリケーション プロパティ] ダイアログ ボックスを開きます。
- 2. [サーバ情報]タブをクリックします。
- 3. [証明書ビュー] セクションで、[証明書のプロパティ] ボタンをクリックします。
- **4.** [証明書のプロパティ] ダイアログボックスで、すべての証明書パラメー タを削除し、[OK] をクリックします。

手順終了

注: アプリケーションへの証明書割り当てから、ホストへの割り当てに切り 替えると、アプリケーションの証明書パラメータが削除されます。

ポートへの証明書の割り当て

注: アプリケーションやポートを個別の証明書で保護する特別な理由がない限り、ホストレベルで証明書を割り当て、ホスト証明書を使用して、ホストに常駐するすべてのアプリケーションに安全なデータ交換を提供することをお奨めします。

ポート証明書を使用して、サーバアプリケーションの特定のポートを介して、 安全なデータ交換を行う場合は、以下の手順を行います。

手順:

ポートへの証明書の割り当て

手順開始

- **1.** [**アプリケーション プロパティ**] ダイアログ ボックスを開きます。
- 2. [サーバ情報]タブをクリックします。
- 3. [ポート]セクションで、安全な接続が必要なポートを選択し、[ポートの編集]をクリックします (90 ページの「安全なポートの設定」を参照)。
- **4.** [Port Properties] ダイアログ ボックスで [証明書] タブをクリック し、[証明書のプロパティ] ボタンをクリックします。
- 5. [証明書のプロパティ]ダイアログボックスで、セキュリティパラメー タを指定します。この手順はプラットフォームによって異なります。

Windows の場合:

- **a.** [証明書の参照] ボタンをクリックします。
- **b.** [<ホスト名>ホストについて証明書を選択してください] ダイアログ ボックスで、リストから証明書を選択し、[OK]をクリックします

インストールされる証明書については、75ページの「証明書のインストール」を参照してください。

UNIX の場合:

- a. [証明書] テキスト ボックスで、
 <serial_#>_<host_name>_cert.pem ファイルの完全なパスを指定します。
- b. [証明書キー]テキストボックスで、
 <serial_#>_<host_name>_priv_key.pemファイルの完全なパス を指定します。
- c. [信頼されたCA]テキストボックスで、ca_cert.pemファイルの完全 なパスを指定します。

インストールされるファイルについては、75 ページの「証明書のインス トール」を参照してください。 **注:** [解説] プロパティはオプションです。

6. [証明書のプロパティ]ダイアログボックスで、[OK]をクリックします。 これで、[証明書]タブの[ポート証明書]セクションに、割り当てた証 明書の値が表示されます(図 20 を参照)。

👺 New Port Info [techpubs4:3010] Properties	X
Port Info Certificate Advanced	1
Certificate: "36 88 A9 3C 09 BD 91 2A C8 71 E0 A 40 B4 BD 82 C0 74 43 04 70" Description: "techpubs1.domain1.domain2.com, vienna, exp: 8/15/2008" Key: "" CA: ""	
OK Cancel Help	

図 20: [Port Properties] ダイアログ ボックス —[証明書] タブ

- **注:** [Port Properties] ダイアログ ボックスの [拡張] タブには、別 の形で証明書パラメータが表示されます。このタブは将来使用する ために確保されています。
- 7. [Port Properties] ダイアログボックスで、[OK] をクリックします。
- **8.** [**アプリケーション プロパティ**]ダイアログボックスで、[OK] をクリックして新しい設定を保存します。

手順終了

手順:

以前に割り当てた証明書のポートからの削除

手順開始

- 1. [アプリケーション プロパティ]ダイアログ ボックスを開きます。
- 2. [サーバ情報]タブをクリックします。
- 3. [ポート] セクションで、証明書を削除するポートを選択し、[ポートの 編集]をクリックします

- **4.** [Port Properties] ダイアログ ボックスで [証明書] タブをクリックし、[証明書のプロパティ] ボタンをクリックします。
- 5. [証明書のプロパティ] ダイアログボックスで、すべての証明書パラメー タを削除し、[OK] をクリックします。

手順終了

ホスト証明書を使用するためのサーバ アプリケー ションの設定

ホストに証明書を割り当てたら、それを使用し、ホストに常駐する任意のサー バアプリケーションの任意の安全なポートを介して、安全なデータ交換を行 うことができます。

手順:

ホスト証明書を使用するためのサーバ アプリケーション の設定

前提条件

• 92ページの「ホストへの証明書の割り当て」

手順開始

- **1.** [**アプリケーション プロパティ**]ダイアログ ボックスを開きます。
- 2. [サーバ情報]タブをクリックします。
- 3. [ポート] セクションで、安全なポートを設定します (90 ページの「安全 なポートの設定」を参照)。
- **4.** [証明書ビュー] セクションで、[ホスト] オプションが選択されている ことを確認し、デフォルトで、このサーバとの安全な接続にホスト証明書 を使用することを指定します。
- 5. [OK] をクリックして、新しい設定を保存します(103ページの図21を参照)。

🙀 T-Server_Swit	chNECwith₩z	[techpubs4:301	0]Properties 🗙	
Connections	Options Ar	nnex Security	Dependency	
General	Switches	Server Info	Start Info	
	Host: 🛐 t	echpubs4	- 🗃	
Ports				
ID 🔺	Listening	port Secu C	onn H	
eesure	5050 5051	Vee		
secure	3031	165		
1				
	Add Port	Edit Port	Delete Port	
Certificate Vier	N			
 Host 	C Ap	plication		
Certificate: "9/	AB DB C4 02 3	29 3A 73 35 90 BO	65 🔺 🚮	
Description: "te	chpubs.domain	1.domain2.com		
D				
Backup Server: 🔛 T-Server_SwitchNECwitl 🗾 🖆				
Redundanc	y Type: Hot S	tandby	•	
Reconnect T	imeout: 10	-		
Reconnect Al	tempts: 1	-		
СКОК	Cancel	Apply	Help	

図 21: アプリケーションの設定:ホスト証明書の選択

手順終了

安全なクライアント接続の設定

サーバアプリケーションの安全なポートを設定したら、これらのポートに接続するように、クライアントアプリケーションの設定を変更する必要があります。この手順を行うのは、Genesysアプリケーション間で転送されるデータを保護するために、特に対策が必要な接続に対してのみです。

注: クライアントアプリケーションの安全な接続を設定する前に、アプリケーションが実行されるコンピュータに証明書がインストールされていることを確認する必要があります。75ページの「証明書のインストール」を参照してください。

サーバ タイプとユーザ インタフェース タイプのクライアント アプリケー ションに、同じ設定手順を使用します。

手順: 安全なクライアント接続の設定

手順開始

- クライアントアプリケーションの [アプリケーション プロパティ]ダイ アログボックスを開きます。
- 2. [接続]タブをクリックします。
- 3. 安全な接続を設定するサーバを選択し、[編集]をクリックします。
- [Connection Properties] ダイアログボックスの [ポート ID] ボックスで、上述の設定ステップでサーバに作成した安全なポートを選択します。読み取り専用の [接続モード]プロパティは、この接続が安全であることを示しています (104 ページの図 22 を参照)。

注: [証明書]および [拡張] タブはこの設定では使用しません。

🥦 New Connection Info	[techpubs4:3010] Properties	×
General Certificate Ad	vanced	
Server:	"SCS"	- <u>-</u>
Connection Protocol:		-
Local Timeout:	0	
<u>R</u> emote Timeout:	0	
Irace Mode:	[Unknown Trace Mode]	•
Connection Mode:	C Unsecured	
	Secured	
[OK Cancel	Help

図 22: アプリケーションの接続:サーバ アプリケーションの安全なポートの選択

5. [OK] をクリックします。これで、[アプリケーション プロパティ] ダイ アログボックスの[接続]タブで、この接続の[セキュリティ]プロパ ティが [はい]に設定されます(図 23 を参照)。



👌 SCI [teo	hpubs4:3010] Propertie	5		X
General	Connections	Options Ann	nex Securit	y Dependency	١.
Server	A		Security	Connection	
🛛 💭 Log	DAP				
SCS			Yes		

図 23: [アプリケーション プロパティ]ダイアログ ボックス —[接続] タブ

6. [OK] をクリックして、新しい接続設定を保存します。

次回にこのアプリケーションを起動するときには、安全な接続を介してサーバ に接続します。

手順終了

Configuration Server との安全な接続

クライアントアプリケーションとConfiguration Serverとの安全な接続を設定 するには、以下の手順を行います。

新しいクライアント接続

- サーバタイプの新しいクライアントアプリケーションの場合は、アプリケーションをインストールするときに、Installation Wizard(インストールウィザード)を使用して、Configuration Serverの自動検出ポート番号を指定します。Installation Wizard(インストールウィザード)によって、これらのパラメータが以下のように伝搬されます。
 - サーバの[アプリケーションプロパティ]ダイアログボックスの[開始 情報]タブの[コマンド ライン引数]テキストボックス
 - サーバアプリケーションの startServer.bat ファイル (Windows)または run.sh ファイル (UNIX)
 - レジストリ エディタの [Application] フォルダの ImagePath
- Configuration Server のアプリケーション オブジェクトをクライアントの [接続] タブに追加して、クライアントアプリケーションの設定を変更し ます。103 ページの「安全なクライアント接続の設定」を参照してくださ い。ただし、104 ページのステップ4で、自動検出ポートを選択します。
- ユーザ インタフェース タイプのクライアント アプリケーションの場合 は、アプリケーションを起動し、表示される [Log In] ダイアログボッ クスに Configuration Server の自動検出ポート番号を入力します。

既存のクライアント接続

- Configuration Server のアプリケーション オブジェクトで、Configuration Server の自動検出ポートを確認するか作成します。
- Configuration Server のアプリケーション オブジェクトをクライアントの [接続]タブに追加して、クライアントアプリケーションの設定を変更し ます。103 ページの「安全なクライアント接続の設定」を参照してくださ い。ただし、104 ページのステップ4で、自動検出ポートを選択します。
- クライアント アプリケーションを起動する方法に応じて、サーバ タイプ のクライアント アプリケーションに対して、Configuration Server に対して 指定した自動検出ポートのポート ID に対応するように、以下の場所でポー ト情報を変更します。
 - ◆ サーバの [アプリケーションプロパティ] ダイアログ ボックスの [開始 情報] タブの [コマンド ライン引数] テキスト ボックス
 - サーバアプリケーションの startServer.bat ファイル (Windows)または run.sh ファイル (UNIX)
 - レジストリ エディタの [Application] フォルダの ImagePath

手順 : Configuration Server の自動検出ポートの設定

目的: クライアントが Configuration Server に安全に接続できるように、 Configuration Server アプリケーションの自動検出ポートを設定するには、以下 の手順を行います。

手順開始

- **1.** Configuration Server の [**アプリケーション プロパティ**] ダイアログ ボッ クスを開きます。
- 2. [サーバ情報]タブをクリックします。
- 3. [ポート]セクションで、[ポートの追加]をクリックします。
- **4.** [Port Properties] ダイアログ ボックスの [ポート情報] タブで、以下の手順を行います。
 - **a.** [ポート ID] テキスト ボックスに、ポート ID を入力します。
 - **b.** [通信ポート] ボックスに、新しいポートの番号を入力します。
 - c. [接続プロトコル]ボックスで、必要に応じて、接続プロトコルを選択 します。
 - **d.** [自動検出 (アップグレード)]オプションを選択します(107ページの 図24を参照)。

🗑 New Port Info [techpubs4:3010] Properties 🛛 🗙	
Port Info Certificate Advanced	
Port ID:	autodetect
Communication Port	5555 💽 🚺
Cognection Protocol:	· ·
HA sync:	E
Listening <u>M</u> ode:	C Unsecured
	C Secured
	 Auto Detect (Upgrade)
OK	Cancel Help

図 24: Configuration Server アプリケーションのポート プロパティ

e. [OK]をクリックします。

アプリケーションにセキュリティパラメータが設定されている場合は、自動-検出ポートを介して接続する際に、Configuration Server がセキュリティ設定の有効性をチェックします。結果に応じて、クライアントが安全なモードで接続するか、Configuration Server によって接続を拒否されます。

5. [OK] をクリックして、新しい設定を保存します。

手順終了

Configuration Server と **DB Server** 間の安全 な接続の設定

Configuration Managerで、Genesysコンポーネント間の安全なデータ交換のすべての接続を設定できます。唯一の例外は、Configuration ServerとConfiguration DatabaseのDB Serverとの接続です。これら2つのコンポーネント間の安全な接続を設定するには、それぞれの構成ファイルを変更する必要があります。

手順:

DB Server と Configuration Server の構成ファイルの変更

手順開始

- DB Server の構成ファイルに、dbserver-nの形式で新しいセクションを 追加します。nは任意の正数です。このセクションで、DB Server の追加の 待機ポートを設定します。詳細については、『Framework 7.6 Configuration Options Reference Manual』の該当する章を参照してください。
- **2.** 新しいセクションで、port オプションを使用して、DB Server との安全な 接続に使用するポートの番号を指定します。
- transport オプション (110 ページを参照)を使用して、このポートを安 全なポートとして指定し、安全な接続に使用する証明書のパラメータを指 定します。詳細については、「DB Server のサンプル構成ファイル」を参照 してください。
- Configuration Server 構成ファイルの [dbserver] セクションで、port オ プションの値を、DB Server に指定した安全なポートに対応するように変 更します。
- [dbserver] セクションにtransportオプションを追加し、Configuration Database との安全な接続を指定し、安全な接続に使用する証明書のパラ メータを指定します。詳細については、Configuration Server のサンプル構 成ファイルを参照してください。
- 6. Configuration Server と DB Server を再起動します。

手順終了

注: 安全なデータ交換を設定する前に、特定の Genesys コンポーネントが実 行されるホスト コンピュータに証明書がインストールされ、証明書情報 を取得できることを確認する必要があります。

DB Server のサンプル構成ファイル

Configuration Layer の DB Server のサンプル構成ファイルを以下に示します。 [dbserver-1] セクションで、このサーバとの安全な接続を設定します。

```
[dbserver]
host = localhost
port = 4040
management-port = 4581
dbprocesses_per_client = 1
dbprocess_name =./dbclient_sybase
oracle_name =./dbclient_oracle
informix_name =./dbclient_informix
sybase_name =./dbclient_sybase
db2_name =./dbclient_db2
```
```
connect_break_time = 1200
tran_batch_mode = off
[dbserver-1]
port = 4333
transport=tls=1;certificate=9a ab db c4 02 29 3a 73 35 90
b0 65 2f 3d 32 b5 1e aa f1 7c
[log]
```

```
verbose = standard
all = stderr
```

```
[lca]
lcaport = 4999
```

Configuration Server のサンプル構成ファイル

Configuration Server のサンプル構成ファイルを以下に示します。Configuration Server と DB Server の両方を同じホスト コンピュータで実行する場合は、 [dbserver] セクションの port と transport オプションの値を、上述の DB Server のサンプル構成ファイルと対応するように設定します。

```
[confserv]
port = 2020
management-port = 2021
server = dbserver
history-log-file-name = histlog
history-log-expiration = 30
history-log-client-expiration = 1
history-log-max-records = 1000
encryption = false
encoding = utf-8
[log]
verbose = standard
all = stderr
[hca]
schema = none
[soap]
port = 5555
[dbserver]
host = db-host
port = 4333
dbengine = mssql
dbserver = db-config
dbname = config
username = user1
password = user1pass
```

```
reconnect-timeout = 10
response-timeout = 600
transport=tls=1;certificate = 9a ab db c4 02 29 3a 73 35
90 b0 65 2f 3d 32 b5 1e aa f1 7c
```

安全な接続の設定オプション

transportオプションを使用して、DB ServerとConfiguration Serverの初期の 安全な接続を確立するために必要な証明書関連のパラメータを指定します。

transport

デフォルト値 :tls=0	
有効値:	
tls=0	通常の(安全でない)接続を使用します。
Windowsの場合:	安全な接続を使用します。
tls=1;certificate= <value></value>	certificateオプションで、証明書の値を指 定します。証明書の詳細については、71ページ の「OpenSSLを使用した証明書生成」を参照し てください。
UNIXの場合:	安全な接続を使用します。
tls=1; certificate= <path>; [certificate-key=<path>]; trusted-ca=<path></path></path></path>	<pre>certificateオプションで、 <serial_#>_<host_name>_cert.pem ファイルの完全なパスを指定します。 certificate-keyオプションで、 <serial_#>_<host_name>_priv_key. pemファイルの完全なパスを指定します(秘密 鍵を証明書と共に格納する場合は除く)。 trusted-caオプションで、ca_cert.pem ファイルの完全なパスを指定します。</host_name></serial_#></host_name></serial_#></pre>

transportオプションは、ポート設定を含むDB Serverの構成ファイルの任意 のセクション、およびConfiguration Serverの構成ファイルのConfiguration Databaseセクションで指定します。

注: transport オプションの有効値では、区切り文字「;」と「=」の前後 にスペースは使用できません。



安全な HA 同期接続の設定

この項では、高可用性(HA)構成におけるプライマリおよびバックアップ コン ポーネント間の安全な接続を設定する方法について説明します。

注: 高可用性構成で安全な接続をサポートするコンポーネントについては、 64ページの「サポートするコンポーネント」を参照してください。これ らのGenesysコンポーネントに高可用性環境を設定する詳細については、 該当する製品マニュアルを参照してください。

冗長サーバの設定

複数ポート構成が可能なリリース7.5以降では、特定のポートの[Port Properties]ダイアログボックスの[HA同期]チェックボックスをオンにして、HA同期接続を設定できます。これによって、フェイルオーバ後に、元のプライマリサーバが新しいプライマリサーバに接続するために、このポートを使用します。[HA同期]チェックボックスがオフの場合は、元のプライマリサーバが、新しいプライマリサーバのデフォルトポートに接続します。

注: 冗長サーバ間の HA 同期接続に、ポート レベルで割り当てた証明書を持 つポートを使用することはお奨めできません。安全な接続は、ホスト レ ベルまたはアプリケーション レベルで設定する必要があります。

手順:

冗長サーバ間の安全な接続の設定

手順開始

- 冗長ペアのプライマリ サーバとバックアップ サーバのプロパティの [サーバ情報]タブで、同じ[ポート ID]を持つ新しいポートを作成し、 [待機モード]を[Secure]に設定します。
 - **注:** ホット スタンバイ冗長ペアのサーバに複数のポートを設定する際に は、プライマリ サーバとバックアップ サーバの [ポート ID] と [待機モード]の設定が一致している必要があります。
- 各サーバの [Port Properties] ダイアログボックスで、[OK] をクリッ クして新しい設定を保存します。次に、それぞれの [アプリケーション プ ロパティ] ダイアログボックスで、[適用] をクリックします。
- 3. 各サーバの [アプリケーション プロパティ]ダイアログボックスで、先 ほど作成したポートを選択し、[編集]をクリックします。

 [Port Properties] ダイアログ ボックスで、[HA 同期] チェック ボッ クスをオンにし、[OK] をクリックします。[アプリケーション プロパ ティ] ダイアログ ボックスの [ポート] セクションに、このポートが HA 同期接続の安全なポートとして表示されます(図 25 を参照)。

📕 secure [techpubs4:301	10] Properties	×
Port Info Certificate Adv	anced	
Port ID	; secure	
Communication Port	5678 💽 🚺	
Cognection Protocol	•	
HA sync	 I 	
Listening <u>M</u> ode	C <u>U</u> nsecured	
	Secured	
OK	Cancel Help	

- 図 25: プライマリ T-Server の安全なポート設定の例
- 5. [適用]をクリックして、設定の変更内容を保存します(113ページの図 26 を参照)。

😹 TServer_NEC [techpubs4:3010] Properties	×
Connections General	Options Annex Security Dependency Switches Server Info Start Info	ļ
	Host: 🛐 techpubs4 💽 💕	
Ports		L
ID 🚔	Listening port Secu Conn HA	
🖳 default	8888	
Secure	5678 Yes Yes	
	Add Port Edit Port Delete Port	
Certificate View	C Application	
Certificate: "Cl 70 2E A6 41 1 Description:"te	D 22 84 DA E6 D9 65 D2 44 1F B5 41 A E A4 B5 65'' echpubs.domain1.domain2.com ,	
<u>B</u> ackup	Server: 🔛 TServer_NEC_2 📃 🗾 🚅	
Redundanc	y Type: Hot Standby	
<u>R</u> econnect T	imeout: 10 🚊	
Reconnect Al	ttempts: 1 👻	
СК ОК	Cancel <u>A</u> pply Help	

図 26: プライマリ T-Server の設定の例

手順終了





12 Genesys TLS のトラブル シューティング

この章では、ご使用の環境で Genesys Transport Layer Security (TLS) のトラブル シューティングを行う際の情報について説明します。以下の項から構成されま す。

• 安全な接続を確立できない場合(115ページ)

安全な接続を確立できない場合

クライアントとサーバ間の安全な接続を確立できない場合は、以下の項目を確認してください。

- Genesys コンポーネントが Genesys TLS 機能をサポートしているか(該当する製品マニュアルを参照)。
- オペレーティングシステムが Genesys TLS をサポートしているか(69ページの「環境変数の設定」を参照)。
- CAの自己署名証明書ファイル、およびこのCAが発行した最低1つの証明書 が、クライアントおよびサーバアプリケーションが実行されるホストコ ンピュータにインストールされているか。
- (UNIXの場合) Genesys Security Pack on UNIXが、Genesys コンポーネントが インストールされたそれぞれのUNIXホスト コンピュータにインストール されているか。
- (UNIXの場合)オペレーティングシステムに対応する環境変数が正しく設定されているか(69ページの表4を参照)。
- (UNIXの場合)オペレーティングシステムに対応する環境変数が、LCA環境でも正しく設定されているか(69ページの表4を参照)。
- (Windows の場合)サーバアプリケーションの場合はローカル コンピュー タアカウント、クライアント GUI アプリケーションの場合は現在のユー ザアカウントに、証明書がインストールされているか。

例:

- CA 証明書を含めて、設定された証明書の有効期限がすぎていないか。
- DB Serverを構成ファイルから起動するときに、安全なポートを開けない場合、transport オプションが正しく設定されているか、区切り文字「;」と「=」の前後にスペースが挿入されていないか。
- コールセンター環境全体で、1つのCAインスタンスのみを使用することを 推奨。
- 特定のホストの証明書は、完全なホスト名を指定して生成されるため、ア プリケーションが実行されるホストに証明書をインストールした場合、ホ スト名が以下の2つの要件を満たしているか。
 - ・ホスト名の [対象] フィールドに、ホストの FQDN (Fully Qualified Domain Name: 完全ドメイン名) が含まれているか(図 27 を参照)。
 - ホスト名が、他のコンピュータで解決される名前と一致しているか。

ertificate General Details Certification P	ath	?
Show: <a>All>	V	
Field	Value	•
E Version	٧3	
🔚 Serial number	57 d0 a3 ec 00 00 00 00 00 41	
🔚 Signature algorithm	sha1RSA	
EIssuer	vienna, viennad, genesyslab, 🦷	
🖃 Valid from	Wednesday, August 16, 2006	
🖃 Valid to	Friday, August 15, 2008 2:37:	
🚍 Subject	techpubs2.domain1.domain2.com	
Public key	RSA (1024 Bits)	•
CN = techpubs2.domain1.doma	in2.com	
	Edit Properties Copy to File	
	ОК	

図 27: [証明書のプロパティ]: [対象] フィールド



パート

レクティン サーバ整合性 — クライアント側 ポート定義

このマニュアルのパートIVでは、サーバとデータの整合性を確保するために Genesysが提供するクライアント側ポート定義機能を実装する方法について説 明します。

以下の章から構成されます。

• 119ページの第 13章「クライアント側ポート定義」





13 クライアント側ポート定義

この章では、特定のサーバアプリケーションに接続するためのクライアント パラメータの指定方法について説明します。以下の項から構成されます。

- 機能の要約(119ページ)
- 機能の設定(121ページ)

機能の要約

クライアント側ポート定義機能によって、クライアントアプリケーション (サーバタイプ)が、サーバアプリケーションに接続する前に接続パラメータ を定義できます。これによって、サーバアプリケーションがクライアント接 続の数を制御できます。さらに、クライアントアプリケーションがファイア ウォールの背後にある場合に、サーバアプリケーションが事前に定義された 接続パラメータを検証して、クライアント接続を受け入れることが可能です。

セキュリティ上の利点

クライアント側ポート定義機能によって、顧客が、ファイアウォールを通過で きる接続を精密に定義し、ファイアウォールを介したデータ接続をより適切に 制御することが可能になります。その結果、悪意のあるアプリケーション レ ベルの大量の要求が同じサーバ側ポートに集中するDoS (Denial-of-Service: サービス不能)攻撃に対するリスクを小さくすることができます。DoS攻撃に よって、サーバアプリケーションのパフォーマンスが低下したり、不安定に なったり、同じサーバやネットワークの他のアプリケーションに悪影響が出る 可能性があります。

サポートするコンポーネント

この機能は、以下のコンポーネントに適用されます。

- Media T-Server (Configuration Server/Configuration Server Proxy と接続する場合)
- Network T-Server (Configuration Server/Configuration Server Proxy と接続する 場合)
- Universal Router Server (Configuration Server/Configuration Server Proxy、 T-Server、Custom Server と接続する場合)
- Custom Server (Configuration Server/Configuration Server Proxy と接続する場合)
- Outbound Contact Server (Configuration Server/Configuration Server Proxy および T-Server と接続する場合)
- CPD Server および CPD Proxy Server (Configuration Server/Configuration Server Proxy および T-Server と接続する場合)

既知の問題と推奨事項

クライアント側ポート定義の現在の実装には、いくつか既知の問題がありま す。

- この機能をアクティブにするには、クライアントパラメータを入力する必要があります。その際に、Genesys Installation Wizard (Genesys インストールウィザード)を使用することをお奨めします。
- リリース7.6では、Media Configuration Wizard (メディア構成ウィザード)は、 クライアント側ポート定義機能の構成をサポートしません。T-Server と Configuration Server 間にポートが制限されたファイアウォールが使用され る環境に、T-Server をインストールする場合は、最初にそのような T-Server を手動で構成してインストールする必要があります。
- T-Serverのインストール中にクライアント側ポート定義機能を有効にする と、T-Serverの起動時に、ログにより、この機能に関連したコマンドラインパラメータに関する警告メッセージがレポートされます。このメッセージは無視して問題ありません。
- クライアントの Configuration Server に対する接続パラメータを、複数の異なる場所で手動で定義する場合は、これらの項目が同一になるようにします。
- 設定された冗長コンポーネントにこの機能を追加する場合は、プライマリ サーバのアプリケーション オブジェクトで指定したポート番号(およびオ プションで IP アドレス)が、バックアップ サーバのアプリケーション オ ブジェクトに自動的に伝搬されます。バックアップ サーバのアプリケー ション オブジェクトで、これらのパラメータを手動で訂正する必要があり ます。

機能の設定

作業の流れ

表7に、クライアント側ポート機能を設定するための主なステップを示します。 順序どおりにすべてのステップを行う必要があります。.

表 7:	作業の流れ —	クライ	(アン	ト側ポー	ト定義の設定
------	---------	-----	-----	------	--------

目的	関連手順とアクション
 クライアントのインストール中に Genesys Installation Wizard (Genesys インストール ウィザード)を使用して(推奨)、または手 動で、クライアントの接続パラメータ(ポー ト番号、オプションで IP アドレス)を指定 します。 	 これらのパラメータがConfiguration Serverとの最初の 接続に使用されます。必要に応じて、以下の手順を行 います。 122 ページの「Installation Wizard (インストール ウィ ザード)を使用した Configuration Server との接続の 設定 (UNIX の場合)」 123 ページの「Installation Wizard (インストール ウィ ザード)を使用した Configuration Server との接続の 設定 (Windows の場合)」 125 ページの「手動による Configuration Server との接 続の設定」
 Configuration Server のアプリケーション オ ブジェクトをクライアントの [接続]設定 に追加し、クライアントの接続パラメータ (ポート番号、またはポート番号と IP アド レス)を Configuration Server の接続プロパ ティに追加します。 	これらのパラメータが、Configuration Serverとの再接 続に使用されます。 以下の手順を行います。 • 126 ページの「Configuration Manager を使用した Configuration Server のクライアント接続への追加」
3. クライアントの接続パラメータをサーバの 接続プロパティに追加します。	クライアントがConfiguration Server以外のサーバア プリケーションと接続する機能を使用するために、以 下の手順を行います。 • 127 ページの「クライアント接続の設定」

Configuration Server 接続の設定

この項では、Genesys Installation Wizard (Genesysインストール ウィザード)を使 用して、または手動で、Configuration Serverとの接続を設定する方法について 説明します。インストールが完了したら、Configuration Managerでクライアン トの**アプリケーション** オブジェクトに変更を加えます。

手順:

Installation Wizard (インストール ウィザード)を使用した Configuration Server との接続の設定 (UNIX の場合)

手順開始

- ウィザード設定の際に、コンポーネントのインストール パッケージがコ ピーされたディレクトリで、install.sh というシェル スクリプトを見 つけます。
- 2. コマンドプロンプトに sh およびファイル名を入力して、スクリプトを実行します。たとえば、sh install.sh と入力します。
- コンポーネントの製品マニュアルの指示に従って、インストールを続行します。
- 4. コンポーネントと Configuration Server 間の接続についてのプロンプトが表示されます。

Client Side Port Configuration (クライアント側ポート設定) Select the option below to use a Client Side Port. (クライアント側ポートを使用するには、以下のオプションを選択します) If you select this option, the application can use Client Side Port number for initial connection to Configuration Server. (このオプションを選択すると、最初に Configuration Server に接続するために、アプリケーションが Client Side Port 番号を使用できます) Do you want to use Client Side Port option (y/n)? (Client Side Port オプションを使用しますか (はい/いいえ))

- 5. プロンプトが表示されたら、「はい」として Y を入力します。
- 6. 以下のプロンプトが表示されます。

クライアントアプリケーションが、Configuration Server との TCP/IP 接続 に使用するポート番号を入力します。インストール スクリプトによって、 コンポーネントのポート番号の使用可能性は検証されません。必ず、この 接続専用の一意のポートを指定する必要があります。

- 7. Enter を押します。
- 以下のプロンプトが表示されます。
 Client Side IP Address (optional), the following values can be used: (クライアント側 IP アドレス (オプション)。以下の値を使用できます)

(オプション) クライアント アプリケーションが、Configuration Server との TCP/IP 接続に使用する IP アドレスを入力します。

- 注: Genesys Installation Wizard (Genesys インストール ウィザード)を使用 してクライアントをインストールする際に、ポート番号(およびオ プションで IP アドレス)を指定することをお奨めします。後でこの 機能を有効にする場合は、コンポーネントを再インストールして、 インストール中にクライアントの接続パラメータを定義するか、手 動でパラメータを指定します。手動の場合は、125 ページの「手動 による Configuration Server との接続の設定」を参照してください。
- 9. コンポーネントの製品マニュアルを参照して、コンポーネントのインス トールを完了します。

インストール中に、クライアントの事前に定義されたポート番号

- (- transport-port <port number>)およびIPアドレス
- (- transport-address <IP address>)(指定した場合)が、自動的 に以下の場所に追加されます。
- サーバの [アプリケーションプロパティ]ダイアログボックスの [開始情報]タブの [コマンドライン引数] テキストボックス(Management Layer を使用してアプリケーションを開始するため)
- サーバアプリケーションのrun.shファイル(起動ファイルを使用して アプリケーションを起動するため)
- レジストリエディタの[アプリケーション]フォルダの ImagePath (アプリケーションを Windows サービスとして起動するため)

手順終了

次のステップ

 126ページの「Configuration Managerを使用したConfiguration Serverのクライ アント接続への追加」

手順:

Installation Wizard (インストール ウィザード)を使用した Configuration Server との接続の設定 (Windows の場合)

手順開始

- 1. コンポーネントの製品マニュアルの指示に従って、Genesys Installation Wizard (Genesys インストール ウィザード)を起動します。
- [Client Side Port Configuration] ページで、
 [Use Client Side Port] チェック ボックスをオンにします(図 28 を 参照)。

Genesys Installation Wizard	×
Client Side Port Configuration	
Select the option below to use a Client Server can use the Client Side Port nur	: Side Port. If you select this option, the Universal Routing mber for initial connection to Configuration Server.
✓ <u>Use Client Side Port</u> This option allows user to c	configure Client Side Port parameters.
Configuration Options	
Specify Client Side Port Number.	Port:
Specify Client Side IP Address.	IP Address:
	< <u>B</u> ack <u>N</u> ext > Cancel

図 28: Installation Wizard (インストール ウィザード): クライアント側接続パラメータの指定

- クライアントアプリケーションと関連付けた Configuration Server に接続す るために、以下の手順で、コンポーネント(クライアント)のパラメータ を指定します。
 - [ポート]: クライアントアプリケーションが、Configuration Server との TCP/IP 接続に使用するポート番号を入力します。インストールスクリ プトによって、コンポーネントのポート番号の使用可能性は検証されま せん。必ず、この接続専用の一意のポートを指定する必要があります。
 - (オプション)[IP アドレス]: クライアント アプリケーションが、 Configuration Server との TCP/IP 接続に使用する IP アドレスを入力します。
 - 注: Genesys Installation Wizard (Genesys インストール ウィザード)を使用 してクライアントをインストールする際に、ポート番号(およびオ プションで IP アドレス)を指定することをお奨めします。後でこの 機能を有効にする場合は、コンポーネントを再インストールして、 インストール中にクライアントの接続パラメータを定義するか、手 動でパラメータを指定します。手動の場合は、125 ページの「手動 による Configuration Server との接続の設定」を参照してください。
- 4. コンポーネントの製品マニュアルを参照して、コンポーネントのインス トールを完了します。

インストール中に、クライアントの事前に定義されたポート番号

- (- transport-port <port number>)およびIPアドレス
- (- transport-address <IP address>)(指定した場合)が、自動的 に以下の場所に追加されます。

- サーバの [アプリケーション プロパティ] ダイアログ ボックスの [開始情報] タブの [コマンド ライン引数] テキスト ボックス(Management Layer を使用してアプリケーションを開始するため)
- サーバアプリケーションのstartServer.batファイル(起動ファイ ルを使用してアプリケーションを起動するため)
- レジストリエディタの[アプリケーション]フォルダの ImagePath (アプリケーションを Windows サービスとして起動するため)

手順終了

次のステップ

 126ページの「Configuration Managerを使用したConfiguration Serverのクライ アント接続への追加」

手順: 手動による Configuration Server との接続の設定

要約

コンポーネントの起動時に使用されるクライアントの接続パラメータを、コマ ンドラインパラメータとして追加して設定します。Genesysコンポーネント は、Management Layer、起動ファイル、手動の手順、またはWindows Services Managerを使用して起動できます。サーバアプリケーションの場合は、通常、 これらすべての手順にコマンドラインパラメータと実行可能ファイル名が必 要です。

手順開始

- クライアントアプリケーションを起動する手順に応じて、以下のパラメー タのいずれかまたは両方をアプリケーションのコマンドラインに追加し ます。
 - -transport-port <port number>
 - -transport-address <IP address>(指定した場合)

ここで、

- <port number>は、クライアントがConfiguration ServerとのTCP/IP接 続に使用するポート番号
- <IP address>は、クライアントがConfiguration ServerとのTCP/IP接続 に使用する IP アドレス
- 手動でアプリケーションを起動するには、以下の例のように、クライアントの接続パラメータをアプリケーションのコマンドラインに追加します。
 <switch> server.exe -host <Configuration Server host>

-port <Configuration Server port> -app <T-Server Application> -l <license address> -nco [X]/[Y] - transport-port <port number>
-transport-address <IP address>

Genesys コンポーネントの起動の詳細については、コンポーネントの製品 マニュアルを参照してください。

手順終了

次のステップ

 126ページの「Configuration Managerを使用したConfiguration Serverのクライ アント接続への追加」

手順:

Configuration Manager を使用した Configuration Server のクライアント接続への追加

目的: Configuration Server に再接続するために、クライアントの接続パラメー タを指定するには、以下の手順を行います。

手順開始

- クライアントアプリケーションの [アプリケーション プロパティ]ダイ アログ ボックスを開きます。
- 2. [接続] タブをクリックします。
- 3. [追加]をクリックします。
- [New Connection Info Properties] ダイアログボックスで、[参照] ボタンをクリックし、クライアントが接続する Configuration Server のアプ リケーション オブジェクトを選択して、[OK] をクリックします。
- 5. [拡張] タブをクリックします。
- 6. [転送プロトコルのパラメータ]テキストボックスに、以下のパラメータ のいずれかまたは両方を入力します。
 - port=<port number>
 - address=<IP address>

ここで、

- <port number>は、クライアントがサーバとの TCP/IP 接続に使用するポート番号
- <IP address>は、クライアントがサーバとのTCP/IP 接続に使用する IP アドレス(またはホスト名)

両方のパラメータを指定する場合は、以下のようにセミコロンで区切ります(例については、図 29 を参照)。

port=<port number>;address=<IP address>

注: ここで指定するパラメータは、クライアントのインストール中に指 定したパラメータと同じである必要があります。

🔀 UR	_Serve	r [techpubs4:3010] Properties	×
6	General	Tenants Server Info Start Info	
Co	nnection	IS Options Annex Security Dependency	-i -
_			
S	erver 4	Secured Connection	
	Confse	erv l	
5	Mose N	Non Conserver 760	tion X
i i î	SCS	rew connection into [techpubs4:3010] Proper	rties 🔼
Ĩ	Stat	General Certificate Advanced	
2	TSer	Transa at Distance Descentions	
2	🕽 TSer	Transport Protocol Parameters:	
		pon=7000,audiess=132.100.0.201	
	_		T
1		Application Parameters:	

図 29: アプリケーションの接続 : Configuration Server アプリケーションの追加

6. [OK] をクリックして、新しい接続設定を保存します。

手順終了

クライアント接続の設定

他のアプリケーションに接続するときのクライアント側ポート定義を有効に するには、以下の手順を行います。

手順: クライアント接続の設定

目的: Configuration Server 以外のサーバアプリケーションと接続するためのク ライアントのパラメータを指定するには、以下の手順を行います。

前提条件

- 122 ページの「Installation Wizard (インストール ウィザード)を使用した Configuration Server との接続の設定 (UNIX の場合)」
- 123 ページの「Installation Wizard (インストール ウィザード)を使用した Configuration Server との接続の設定 (Windows の場合)」
- 126ページの「Configuration Managerを使用したConfiguration Serverのクライ アント接続への追加」

手順開始

- クライアントアプリケーション(サーバタイプ)の[アプリケーション プ ロパティ]ダイアログボックスを開きます。
- 2. [接続] タブをクリックします。
- 3. クライアントが接続するサーバを選択し、[編集]をクリックします。
- [Connection Properties] ダイアログボックスで、[拡張] タブをク リックします(図 30 を参照)。

Server	*	Secured	Cor	nection	
💭 Inte	ractionServer		add	lp -	
💭 Mea	ssage_Server			L L	
💭 Stal	t_Server		defa	ault l	
TSe	erver_AvayaCM		defa	ault l	
L TSe	erver_AvayaCM				
CC	STUDE AUDUSE M				
53 🖾	TServer_AvayaCM ([techpubs4:			
	TServer_AvayaCM	[techpubs4: dvanced	3010	Properties	

図 30: アプリケーションの接続: サーバ アプリケーションの選択

- 7. [転送プロトコルのパラメータ]テキストボックスに、以下のパラメータ のいずれかまたは両方を入力します。
 - port=<port number>
 - address=<IP address>

ここで、

- <port number>は、クライアントがサーバとのTCP/IP接続に使用する ポート番号
- <IP address>は、クライアントがサーバとの TCP/IP 接続に使用する IP アドレス(またはホスト名)

両方のパラメータを指定する場合は、以下のようにセミコロンで区切ります(例については、図 30 を参照)。

port=<port number>;address=<IP address>

- 注: 設定された冗長コンポーネントにこの機能を追加する場合は、プラ イマリサーバのアプリケーション構成オブジェクトで指定したポー ト番号(およびオプションでIPアドレス)が、バックアップサーバ のアプリケーション構成オブジェクトに自動的に伝搬されます。 バックアップサーバのアプリケーションオブジェクトで、これらの パラメータを手動で訂正する必要があります。
- 8. [OK] をクリックして、新しい接続設定を保存します。

手順終了





A

AckMandatory				
レジストリ オプション.......	÷	÷		.43
AckMode				
レジストリ オプション.......	÷	÷		.44
ADDP				.52
Advanced Disconnect Detection Protocol				
ADDP を <i>参照</i>				

С

ca_cert.pem ファイル
ca.conf ファイル
ca_conf ファイル ディレクトリ
ca.db ファイル
ca_priv_key.pem ファイル
CA 認証機関を <i>参照</i>
Configuration Server
サンプル構成ファイル
create_ca.sh スクリプト
create_cert.sh スクリプト

D

DB Server							
サンプル構成ファイル				÷			108
default-filter-type							
設定オプション・・・							.30
例				÷			.31

Е

ErrorPage							
レジストリ オプション							.44

G

Genesys TLS				
コンポーネントのサポート...				.64
サポートされるプラットフォーム				.66
紹介				.63
接続				

Configuration Layer							. 64
Management Layer							. 64
Media Layer							. 65
設定							. 89

Η

Height							
レジストリ オプション							45
HTTP エラー							35

I

inactivity-timeout									
設定オプション									27

L

52
31
32

Μ

Ν

NoCompleteTimeout							
レジストリ オプション							45
no-default-access							
設定オプション							23

Ρ

PEM ファイル フォーマット					
変換					79
PKCS #12 ファイル フォーマット					75

変換	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	. 79, 87

R

S

-
security
設定オプションのセクション
Security Pack on UNIX
インストール
環境の設定
security セクション
アクティビティなしのタイムアウト
新規ユーザのデフォルト アクセス禁止
<pre><serial_#>_<host_name>_cert.pem ファイル75</host_name></serial_#></pre>
<pre><serial_#>_<host_name>_cert.pfx ファイル75</host_name></serial_#></pre>
<pre><serial_#>_<host_name>_priv_key.pem ファイル .75</host_name></serial_#></pre>
serial.num ファイル
<pre><serial_#>.pem ファイル</serial_#></pre>
ShowUpTimeout
レジストリ オブション

T TLS

120
Transport Layer Security を <i>参照</i>
Transport Layer Security
transport 設定オプション 108, 110

U

JRL							
レジストリ オプション							.47

Width

Width								
レジストリ オプション		÷	÷	÷	÷	÷		.45

あ

アクティビティなしのタイムアウト
security セクション
機能の説明
設定オプション
アプリケーション障害
ADDP
アプリケーションの冗長性
定義
バックアップ サーバ
プライマリ サーバ
安全な接続
Configuration Server と DB Server の間 107
Configuration Server の設定
アプリケーションへの証明書の割り当て96

う

ウォーム スタンバイ																	53	3
------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	----	---

え

エラー									
HTTP エラー									35
システム エラー									35

か

環境変数.																						69	
-------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	----	--

き

<+-	-名	3	>													
設定	定っ.	ť	プ	シ	Ξ	2	/									31
例																32

<

クライアント側ポー	۲	定	Ì羛	5						
作業の流れの構成										.121
紹介										.119

こ

高可用性 (HA)							
アプリケーション障害							. 52
サービス利用不可							. 52
構成ファイル							
Configuration Server .							.109
DB Server							.108

t

サービス利用不可						
アプリケーション状況						52, 53

し

•									
システム エラー									35
冗長タイプ									
ウォーム スタンバイ									53
サポートするコンポーネント									54
ホット スタンバイ									54
証明書									
CA による生成									74
MMC によるエクスポート									85
MMC による管理									84
OpenSSL による生成									71
UNIX へのインストール									75
Windows 証明書サービスによ	る	生	E成	ζ.					79
Windows へのインストール							7	6,	83

アプリケーションへの割り当て
取得
スクリプトのパラメータ
ホストへの割り当て
リモート コンピュータからの取得......87
新規ユーザ
デフォルト アクセス禁止の設定
新規ユーザのデフォルト アクセス禁止
7.6 より前のユーザ
security セクション
機能の説明
許可の割り当て
設定オプション

せ 生成

工成
CAによる証明書
OpenSSLによる証明書
· Windows 証明書サービスによる証明書
セキュリティ バナー
CfgAppType 值
HTTP $\pm \overline{2}$
システム エラー 35
設定中のインストール 37
1000000000000000000000000000000000000
レジストリニトス設定 41
レンストリの例
設定オノション
default-filter-type
inactivity-timeout
no-default-access
transport
< 十一名 >
設定オプションのヤクション
log-filter
log-filter-data
security
-

に 認証機関

認訨機関						
スクリプトのパラン	メータ	 				.72
設定......		 		÷		.72
ファイル名		 				.73

は

バックアップ サーバ								.51
パラレル サーバ								
定義......								.59

ふ ファイル フォーマット

PEM											79
PKCS #12							1	75,	, 7	9,	87
プライマリ サーバ											51
プロキシ サーバ											
定義											59

ほ

ホット スタンバイ																		54
-----------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	----

ま

マニュアル											
規則											12
ご意見.											14
章の要約											10
対象読者											10

り 略i

	咯語																									66
--	----	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	----

れ

レジストリ オプション	/								
AckMandatory									43
AckMode									44
ErrorPage									44
Height									45
NoCompleteTimeout	t								45
ShowUpTimeout									46
URL									47
Width									45

ろ

ログイン時のセキュリティ バナー	
機能の説明	47
ログの特定データの非表示	
log-filter-data セクション	32
log-filter セクション	31
機能の説明	32
設定オプション	32

