

Smart-in 機能仕様書

第 1.0 版 2017 年 10 月 3 日

改訂履歴

[illegible]

目次

1.	はじめに.....	1
2.	機能概要.....	2
2.1.	機能イメージ.....	2
2.2.	機能一覧.....	3
2.3.	電話認証（コールバック）.....	4
2.3.1.	シーケンス.....	4
2.3.2.	発信電話番号について.....	4
2.3.3.	個人情報の取り扱い.....	4
2.3.4.	コールバック待ちタイマー.....	5
2.3.5.	管理機能.....	5
2.3.6.	提供リソース.....	5
2.4.	電話認証（プレコール）.....	6
2.4.1.	シーケンス.....	6
2.4.2.	発信電話番号について.....	6
2.4.1.	個人情報の取り扱い.....	6
2.4.2.	提供リソース.....	7
2.5.	電話認証（プレコールオート）.....	8
2.5.1.	シーケンス.....	8
2.5.2.	発信電話番号について.....	8
2.5.3.	個人情報の取り扱い.....	8
2.5.4.	迷惑電話対策機能.....	9
2.5.5.	提供リソース.....	9
3.	ネットワーク条件.....	10
3.1.	インターネットを介した接続構成.....	10
3.1.1.	諸条件.....	10
3.2.	自社ネットワーク内にオンプレミス形式で設置した場合の接続構成.....	11
3.2.1.	諸条件.....	11

1. はじめに

Smart-in®は、株式会社あいびし社が提供する、携帯電話を利用した本人認証のシステムです。
ID・PW（パスワード）方式による本人認証の仕組みだけでは困難となってきたインターネットセキュリティの安心・安全を確保する全く新しいサービスです。

特徴

1. ID、PW での本人認証完了後は携帯電話による本人確認を実施することで不正ログインを排除
2. 未利用時の携帯着信により第三者の不正ログイン操作を検知、“なりすまし”を排除
3. 「情報（ID、PW）と物（携帯電話）による二要素認証」、「インターネットと電話網連携による確実な2経路認証」、「ID、PW 認証後に電話番号による二段階認証」、利用者からの入力（ID、PW）と銀行からの電話接続及び応答による相互認証」により、簡単で安全・確実な認証を実現

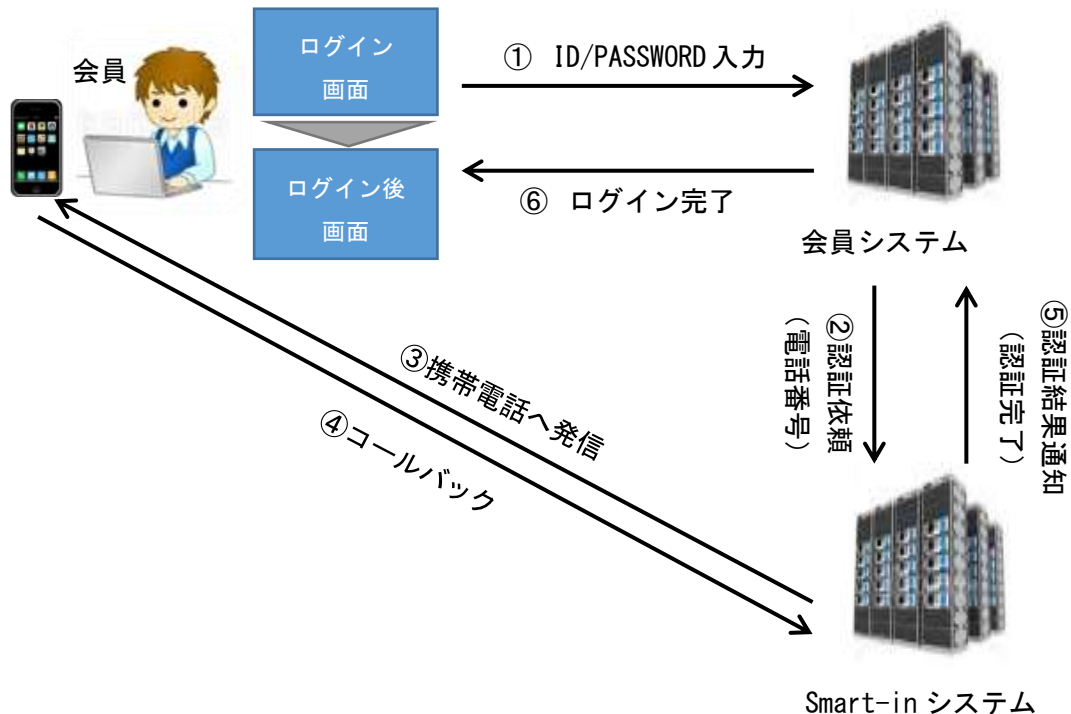
本書は、Smart-in の機能について説明しています。

※Smart-in®は、株式会社あいびしの登録商標です。

2. 機能概要

2.1. 機能イメージ

ログインを要する一般的な Web サービス等に Smart-in のコールバック認証を組み込んだ場合のイメージを下記に記述します。



- ① ログイン画面に ID/PASSWORD を入力します
- ② 導入企業システム内に予め登録されている電話番号を取り出し、その電話番号に対する認証依頼を Smart-in システムへ送信します
Smart-in システムから認証結果通知が返送されてくるまで数十秒要する為、画面には「認証中です」などを表示します。
- ③ 依頼された電話番号へ発信する。携帯電話側では、数回コール音が鳴り自動的に切断されまので応答する必要はありません。
- ④ 着信履歴などからかかってきた電話番号へコールバックします。Smart-in システム側で発信番号を認識すると応答せず自動的に切断しますので課金されません。
- ⑤ 会員システムへ認証結果「認証完了」を返します。
一定時間コールバックがなかった場合は、「認証タイムアウト」を返します。
- ⑥ Smart-in 認証が完了した場合は、正常ログインとしてログイン後の画面へ遷移します。

※会員システムとは：会員サービスを提供し、サービス提供時に個人認証を行うシステムです。

2.2. 機能一覧

Smart-in の機能を下記一覧に示す。

表 2-1 Smart-in 機能一覧

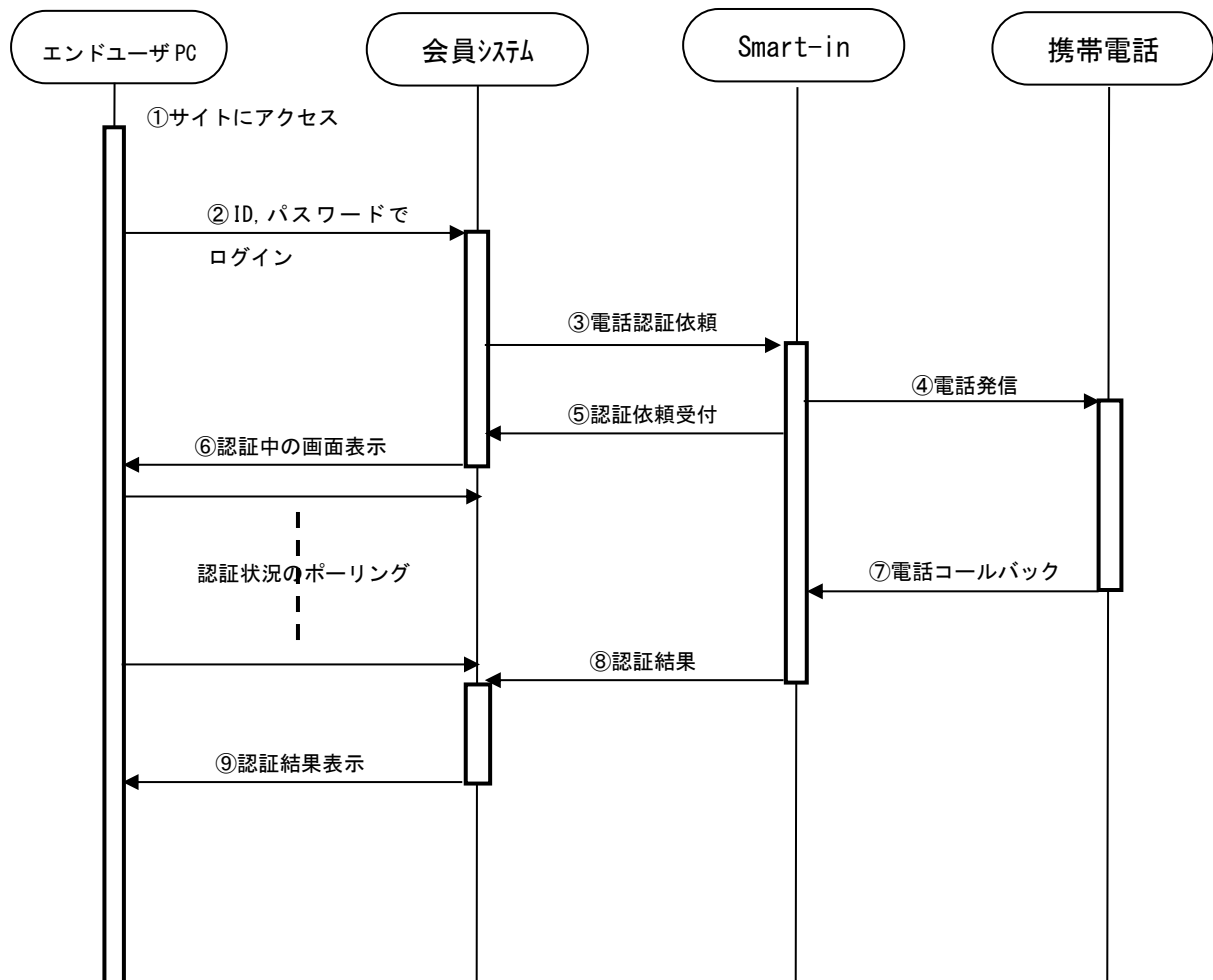
項番	機能名称	機能概要	備考
1	電話認証（コールバック）	<p>会員システムの要求で、指定された電話へ発信し、その後の対象電話番号からの折返し着信で、認証を行う機能。</p> <p>折返し着信があると会員システムへ「認証完了」を通知する。</p> <p>Smart-in→電話：数回コール音が鳴り自動的に切断する。</p> <p>電話→Smart-in：発信電話番号を認識すると自動切断する。</p>	
2	電話認証（プレコール）	<p>電話からの着信を受けると、その電話番を記録する。（電話番号はハッシュ化）</p> <p>その後、会員システムからの問合せに着信の有無を返す。着信記録があった場合は「認証完了」を返す。</p> <p>※着信の記録保持時間は、要求時の指定で変更可能。</p>	
3	電話認証（プレコールオート）	<p>会員システムの要求で、指定された電話からの着信を一定時間待つ。</p> <p>対象電話番号から着信があると会員システムへ「認証完了」を通知する。</p> <p>■迷惑電話対策機能</p> <p>指定電話以外からの着信には、応答し「サービス対象外の電話番号」である旨を音声ガイダンスする。</p> <p>※着信の記録保持時間は、要求時の指定で変更可能。</p>	
4	SMS 送信認証（コールバック）	<p>会員システムの要求で、指定された電話へSMSを送信し、その後の対象電話番号からの折返し着信で、認証を行う機能。</p> <p>折返し着信があると会員システムへ「認証完了」を通知する。</p>	SMS 送信については、別途キャリアとの契約が必要です。
5	SMS 送信	<p>会員システムの要求で、指定された電話へSMSを送信する。</p>	

2.3. 電話認証（コールバック）

会員システムの要求で、指定された電話へ発信し、その後の対象電話番号からの折返し着信で、認証を行う機能です。

2.3.1. シーケンス

以下に接続シーケンスを記述します。



2.3.2. 発信電話番号について

発信時に使用する電話番号は、一つの契約 ID に対して複数電話番号を使用することができます。複数電話番号が登録された場合、発信時に使用する順番は電話番号の登録順となります。冗長化で複数の Smart-in サーバーを設置した場合は、サーバー毎に使用する電話番号指定します。

2.3.3. 個人情報の取り扱い

会員システムから認証要求の packets に電話番号が含まれます。packet は、アプリケーションレベルで独自の暗号化を行います。またミドルレベルで SSL 通信を行います。Smart-in サーバー内では、電話番号は発信完了まではメモリ内で保持されます。その後ハッシュ化して DB に保存します。コールバック時の着信電話番号は、ハッシュ化したデータで照合されます。

2.3.4. コールバック待ちタイマー

認証依頼のパケットの中にコールバック待ちタイマーが指定できます。

コールバック待ちタイマー：60sec～600sec

2.3.5. 管理機能

認証依頼が行われた電話番号の数をカウントします。記録する電話番号はハッシュ化します。

2.3.6. 提供リソース

開発用に提供するリソースについて説明いたします。

提供リソース一覧（Smart-in フォルダ内）

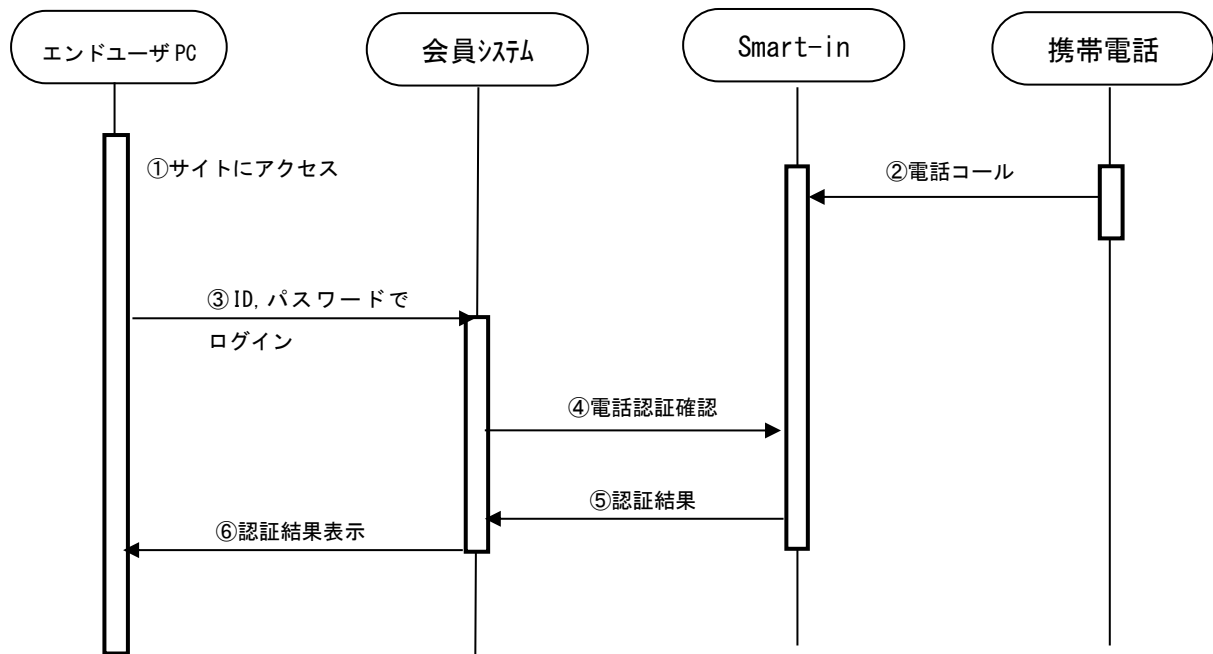
No.	ディレクトリ名/ファイル名	概要
1	Smart-in デベロッパーズガイド.pdf	開発者向けに、インタフェース仕様の説明、サンプルコードなどを記載しています。
2	インタフェース仕様書.pdf	Smart-in システムとのインタフェース仕様を記載しています。
3	Lib/Java /smart-in-api.jar	アプリケーションレベルでの暗号化/復号化を実施する為のモジュールです。 No.3 Java 用 No.4,5 Linex 用 No.6 Windows Server（2003R2 以降）用 ※OS の種類が異なる場合は別途プログラムソースからのコンパイルの必要があるため、サポートセンターまでお問い合わせください。
4	Lib /Linux/32bit/sin_crypt	
5	Lib /Linux/64bit/sin_crypt	
6	Lib/Windows/sin_crypt.exe	
7	sample/php/	PHP 向けサンプルファイルが格納されているディレクトリです。 利用方法は、Smart-in デベロッパーズガイドを参照下さい。
8	sample/C#/	Windows 向けサンプルファイルが格納されているディレクトリです。 利用方法は、Smart-in デベロッパーズガイドを参照下さい。

2.4. 電話認証（プレコール）

電話からの着信を受けると、その電話番号を記録し、その後会員システムからの問合せに着信の有無を返します。

2.4.1. シーケンス

以下に接続シーケンスを記述します。



2.4.2. 発信電話番号について

着信に使用する電話番号は、一つの契約 ID に対して複数電話番号を使用することができます。
冗長化で複数の Smart-in サーバーを設置した場合は、サーバー毎に使用する電話番号指定します。

2.4.1. 個人情報の取り扱い

着信を受けつけた電話番号はハッシュ化して DB に保存します。
会員システムからのパケットに指定する電話番号は同様にハッシュ化します。このハッシュ化された電話番号を照合します。
(ハッシュ化の為のライブラリを Smart-in 側から提供します)

アプリケーションレベルで独自の暗号化は行いません。ただしミドルレベルで SSL 通信を行います。

2.4.2. 提供リソース

開発用に提供するリソースについて説明いたします。

提供リソース一覧

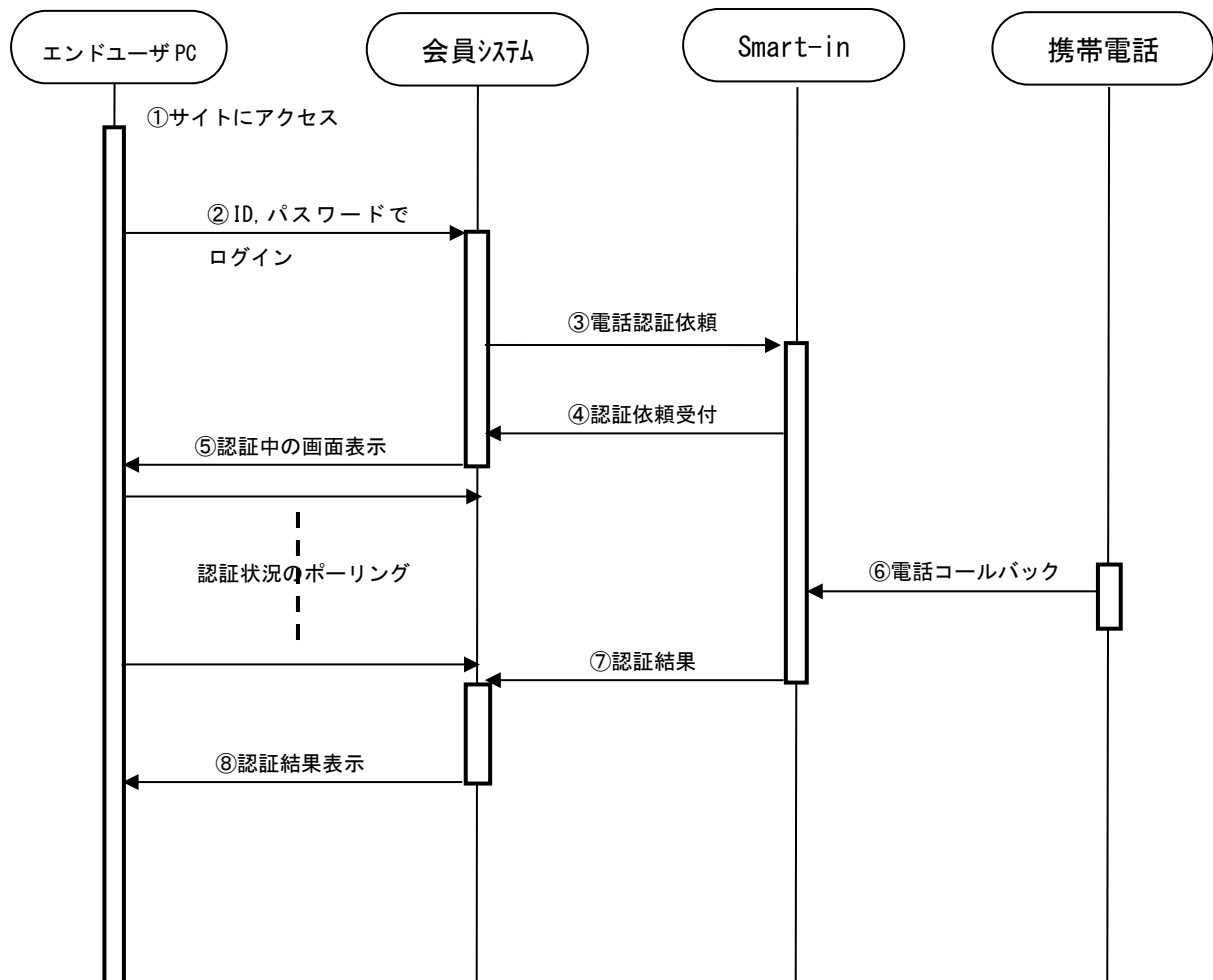
No.	ディレクトリ名/ファイル名	概要
1	Smart-in デベロッパーズガイド.pdf	開発者向けに、インタフェース仕様の説明、サンプルコードなどを記載しています。
2	Smart-in インタフェース仕様 PreCall.pdf	Smart-in システムとのインタフェース仕様を記載しています。
3	Lib /Linux/64bit/sin_crypt	電話番号をハッシュ化する為のモジュールです。 No.3 Linux 用
4	Lib/Windows/authcode_crypt.exe	No.4 Windows Server (2003R2 以降) 用 ※OS の種類が異なる場合は別途プログラムソースからのコンパイルの必要があるため、サポートセンターまでお問い合わせください。
5	sample/	PHP 向けサンプルファイルが格納されているディレクトリです。 利用方法は、Smart-in インタフェース仕様 PreCall を参照下さい。

2.5. 電話認証（プレコールオート）

会員システムの要求で、指定された電話からの着信を一定時間待ちます。対象電話番号から着信があると会員システムへ「認証完了」を通知します。

2.5.1. シーケンス

以下に接続シーケンスを記述します。



2.5.2. 発信電話番号について

着信に使用する電話番号は、一つの契約 ID に対して一つの電話番号を使用することができます。同じ電話番号でコールバック・プレコールと併用使用することはできません。

2.5.3. 個人情報の取り扱い

会員システムからのパケットに指定する電話番号はハッシュ化します。このハッシュ化された電話番号を DB に保存します。

（ハッシュ化の為にライブラリを Smart-in 側から提供します）

着信を受けつけた電話番号はハッシュ化して DB のデータと照合します。

アプリケーションレベルで独自の暗号化は行いません。ただしミドルレベルで SSL 通信を行います。

2.5.4. 迷惑電話対策機能

- ①プレコールオートの認証要求で登録が無い電話番号からの着信は、電話番号と着信日時を DB へ記録します。
- ②着信応答し、音声応答します。音声ガイダンスの有無はサーバ側の設定となります。詳細につきましてはシステム構築マニュアル（「項番 5.5.1.1 外部定義ファイルを設定する」の wrongnumber_playback 属性）をご参照ください。音声応答機能はなしのオプション機能となります。
- ③記録したログの消去時間は、企業ごとに設定可能です。
- ④ログデータは、管理 UI から照会可能です。

2.5.5. 提供リソース

開発用に提供するリソースについて説明いたします。

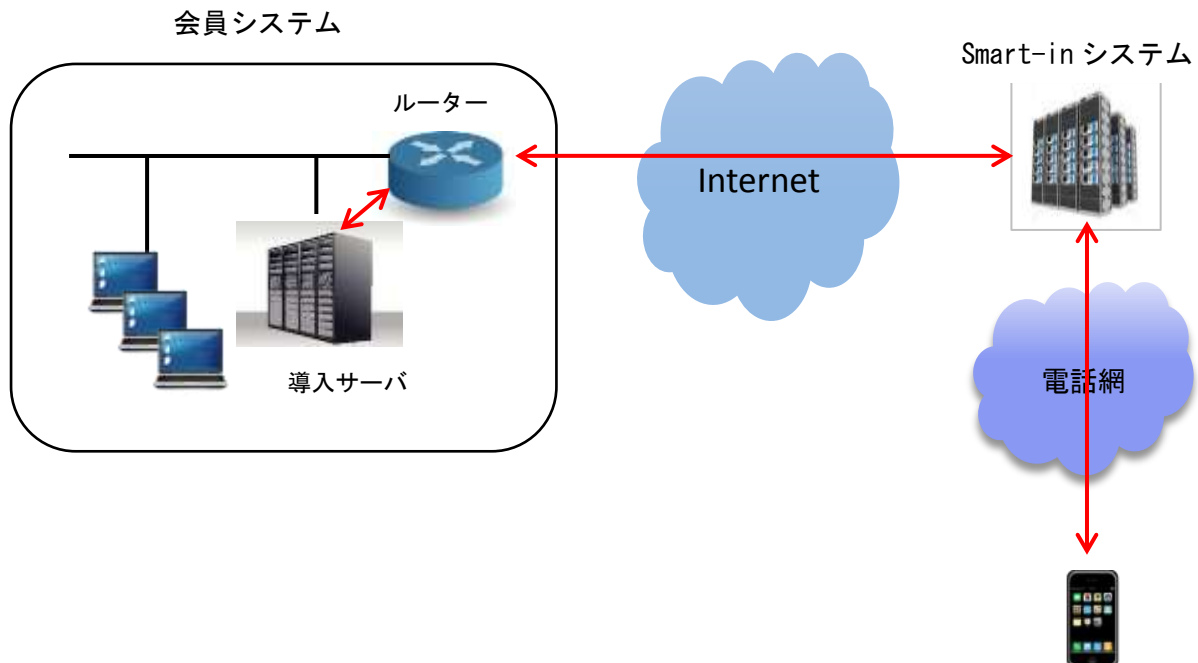
提供リソース一覧

No.	ディレクトリ名/ファイル名	概要
1	Smart-in デベロッパーズガイド. pdf	開発者向けに、インタフェース仕様の説明、サンプルコードなどを記載しています。
2	Smart-in インタフェース仕様 PreCall. pdf	Smart-in システムとのインタフェース仕様を記載しています。
3	Lib /Linux/64bit/sin_crypt	電話番号をハッシュ化する為のモジュールです。 No.3 Linux 用
4	Lib/Windows/authcode_crypt. exe	No.4 Windows Server（2003R2 以降）用 ※OS の種類が異なる場合は別途プログラムソースからのコンパイルの必要があるため、サポートセンターまでお問い合わせください。
5	sample/	PHP 向けサンプルファイルが格納されているディレクトリです。 利用方法は、Smart-in インタフェース仕様 PreCall を参照下さい。

3. ネットワーク条件

3.1. インターネットを介した接続構成

会員システムが Smart-in システムとインターネットを介して接続される場合のイメージ図と諸条件について記述する。

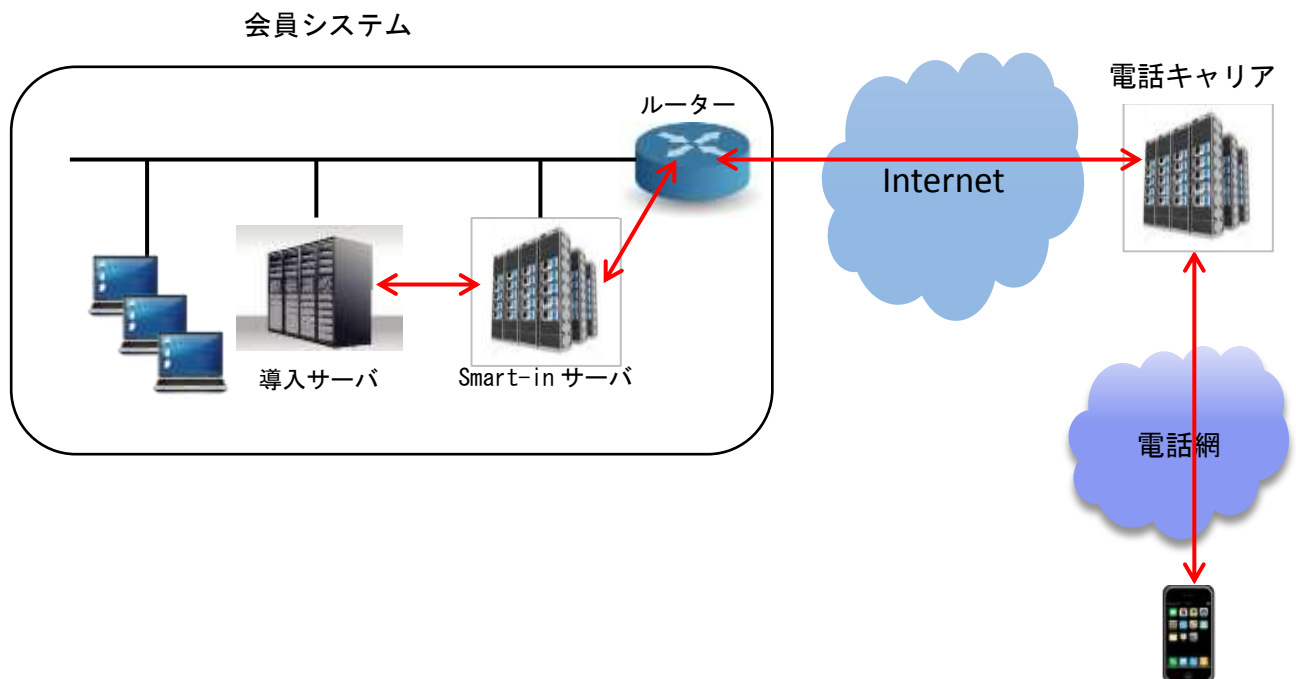


3.1.1. 諸条件

- ① Smart-in システムに接続するサーバにグローバル IP アドレスが必要になります。
Smart-in システム側から認証結果を https で POST する為です。
接続するサーバがイントラネット内に設定されている場合は、ルータにてポートフォワードが必要になります。
- ② Smart-in システムに接続するサーバ内に OpenSSL (※) のミドルウェアが必要になります。
暗号化／復号化モジュール (sin_crypt) で必要になります。
※Linux の場合 (Windows の場合は、再頒布パッケージが必要になります)
- ③ Smart-in システムと接続には、下記プロトコル／ポートを使用いたしますので
ファイアウォールを介す場合は、下記プロトコル／ポートを解放して頂く必要があります。
https/443
- ④ Smart-in システムから携帯電話へ発信する番号 (発番号) は、1 契約当たり原則 1 番号となりますが、
複数番号の設定も可能です。

3.2. 自社ネットワーク内にオンプレミス形式で設置した場合の接続構成

会員システムが Smart-in システムを自社内のネットワークに設置した場合のイメージ図と諸条件について記述いたします。



3.2.1. 諸条件

- ① Smart-in サーバに接続するサーバ内に OpenSSL (※) のミドルウェアが必要になります。
Smart-in との通信パケットの暗号化／復号化処理で必要になります。
暗号化／復号化モジュール (sin_crypt) で必要になります。
※Linux の場合 (Windows の場合は、再頒布パッケージが必要になります)
- ② Smart-in サーバは、電話キャリアと接続する為、下記プロトコル／ポートを使用いたします。
ルーター・ファイアウォールを介す場合は、下記プロトコル／ポートを解放して頂く必要があります。
 - ・ 外部向け通信 (DMZ から Internet)
UDP/5060
 - ・ 内部向け通信 (Internet から DMZ)
UDP/9051