第１章　法人ＩＢのご利用にあたって

１．特徴

本サービスは、インターネットを利用してお客様のパソコンから総合振込、給与・賞与振込、都度振込、口座振替請求、ペイジー（税金・各種料金の払込み）等の法人向け取引を行っていただくことができるインターネットバンキングサービスです。

２．利用条件

（１）推奨環境の確認

Ｐ７「ご利用前にご確認ください！」の推奨環境およびＯＳ・ブラウザの設定を必ず確認してください。

（２）通信環境

インターネットに接続できる通信環境であれば回線の種類に制限はありませんが、通信環境により画面表示に時間がかかる場合がありますので、ＡＤＳＬ、光ファイバー回線でのご利用を推奨いたします。

（３）Ｅメールアドレス

完了通知や異常通知等の重要な連絡をＥメールにて通知するため、Ｅメールアドレスをご用意ください。

なお、携帯電話でのＥメール受信も可能とします。

（４）プリンタ

各種帳票印刷や画面のハードコピーをするためにはプリンタが必要となります。

３．利用者管理

本サービスでは、１契約で複数の利用者を設定することができ、それぞれの利用者が各種取引をご利用いただくことができます。また、利用者ごとに利用権限を設定することで、業務に合ったかたちで、安全に取引を行うことが可能です。

本サービスの利用者は、３種類の利用権限（「管理者」「承認者」「一般者」）によりお客様ＩＤを管理していただきます。

（１）管理者とは

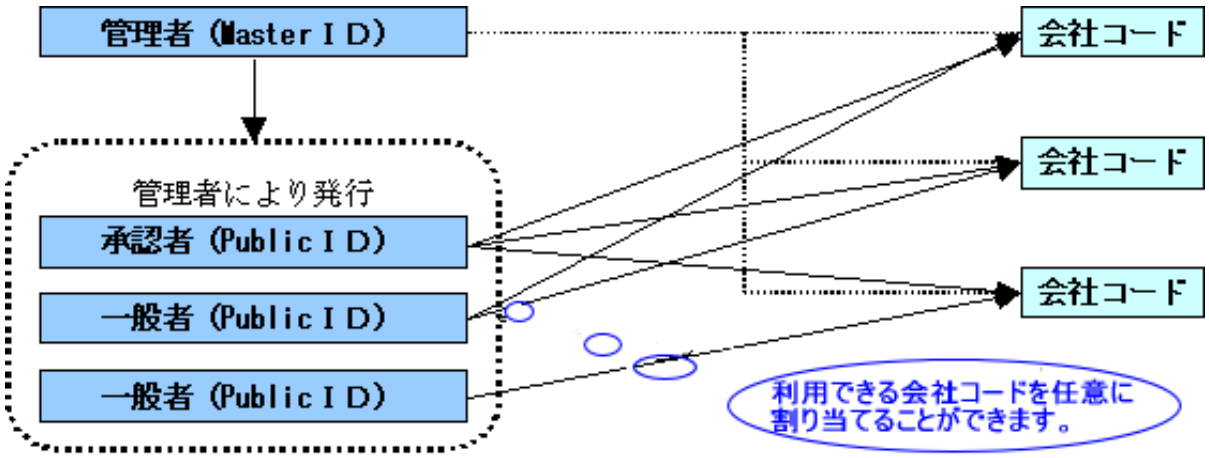
本サービスの利用責任者で、本サービスに用意されているすべてのサービスをご利用いただけます。

管理者は１契約１名で、当金庫から『MasterＩＤ』を１ＩＤ発行いたします。

（２）承認者および一般者とは

承認者とは主に振込・口座振替データの承認処理を行う利用者とし、一般者とは主に振込・口座振替データの作成処理を行う利用者とします。

承認者および一般者のお客様ＩＤ（PublicＩＤ）は、合わせて最大９９個まで管理者により発行いただけます。



（注）会社コードとは、決済口座に付与された番号とします。

４．権限管理

利用権限別のサービスは次のとおりとします。

なお、管理者は承認者および一般者の利用権限をお客様ＩＤ単位に変更できますので、利用者に応じた権限管理を行っていただけます。

＜利用権限別サービス一覧＞

カテゴリ	サービス	利用権限		
		管理者	承認者	一般者
各種照会	残高照会	○	○	○
	入出金明細照会	○	○	○
	取引状況照会	○	○	○
振込・口座振替	総合振込	○	○	○
	給与･賞与振込	○	○	○
	都度振込	○	○	○
	口座振替	○	○	○
	ＷＥＢ承認業務	○	○	×
	外部ファイル登録	○	○	○
手数料照会	振込手数料照会	○	○	×
	口座振替手数料照会	○	○	×
契約情報登録・照会	企業情報照会	○	○	○
	振込契約情報	○	○	○
	口座振替契約情報	○	○	○
	利用開始登録	○	×	×
明細情報登録・照会	振込先明細登録	○	○	○
	口座振替明細情報	○	○	○
管理機能	ＩＤメンテナンス	○	○	○
	ＩＤロック解除	○	×	×
	カレンダー管理	○	○	×
	利用履歴照会	○	×	×

○：利用可能　　×：利用不可

５．ＷＥＢ承認業務

作成された総合振込、給与・賞与振込、口座振替データを承認者がチェックする機能としてご利用いただけます。

なお、作成されたデータに不備がある場合は差戻し処理を行い、データの修正を行うことができます。

６．セキュリティ

本サービスでは、お客様のデータをインターネット上で安全に授受するために、セキュリティ対策を行っています。

主なセキュリティ対策は、次のとおりです。

（1）認証管理

本サービスの利用にかかる本人確認については、「ＩＤ・パスワード方式」および「電子証明書方式」の２通りがありますが、現在はセキュリティ強化を目的として、ご新規の契約について、電子証明書方式のご利用を義務化させていただいてます。

「電子証明書方式」を選択される場合は、別途申込手続きが必要になります。お申込がない場合は、「ＩＤ・パスワード方式」をもって、本人確認をします。

①ＩＤ・パスワード方式

お客様ＩＤおよびログインパスワードによりご契約者本人であることを確認する方式。

②電子証明書方式

電子証明書およびログインパスワードによりご契約者本人であることを確認する方式。

電子証明書のご利用にあっては、**別冊「法人インターネットバンキング電子証明書マニュアル」**（以下「電子証明書利用マニュアル」という）をご用意しておりますのでご参照ください。

■パスワードの種類と利用シーン

お客様ＩＤに加えて、お客様ＩＤごとに設定した４種類のパスワードによる認証管理を行っています。

パスワード種類	利用シーン
ログインパスワード	ログインで使用していただきます。
登録確認用パスワード	振込・口座振替データの登録で使用していただきます。
承認用パスワード	ＷＥＢ承認業務で使用していただきます。
都度送信振込確認用パスワード	都度振込で振込確定時に使用していただきます。

■パスワード誤入力について

４種類のパスワード共に、パスワード入力を６回連続で誤った場合は、パスワードがロックされ、それ以降、本サービスのご利用ができなくなります。

＜対応方法＞

ＩＤ種別	解除方法
MasterＩＤ	管理者によるロック解除できませんので、当金庫に連絡してください。 ロック解除依頼書を書面で提出いただきます。
PublicＩＤ	管理者によりロック解除いただけますので、ご対応ください。

■重複ログイン規制について
同一の利用者ＩＤによる重複ログインはできません。

（２）通信暗号化技術

インターネット通信時における通信暗号化技術として「ＳＳＬ　２５６ｂｉｔ」を採用し、第３者への通信内容の漏洩防止を図っております。

また、Ｃｏｏｋｉｅ機能も必須とします。

（注１）ＳＳＬ：Secure Socket Layer

（注２）Ｃｏｏｋｉｅからの第３者への漏洩を防止するため、認証情報（ログインパスワード等）や顧客情報（口座番号等）のＣｏｏｋｉｅへの書込みは行いません。

（３）強制ログアウト

本サービス利用中に１５分以上何も取引を行わない場合は、強制ログアウトとなり本サービスの利用ができなくなります。
継続してサービスを利用するためには再度ログインを行ってください。

（４）ブラウザ操作における禁止操作

本サービスでは、画面間でのデータや認証情報の整合性を保つため、ブラウザ標準機能を利用した画面遷移は原則禁止としています。

そのため、万が一使用された場合はエラー画面を表示し、以降のサービス利用ができなくなりますので、再度ログインを行ってください。

■「お気に入り」および「履歴」を使用した画面遷移

ログイン後のサービス画面での「お気に入り」および「履歴」を使用した画面遷移を禁止します。
ただし、ログイン画面は上記操作を使用した画面遷移を可能としますが、接続失敗については、お客様の利用環境に依存するため、動作保証は行いません。
なお、上記操作にはキーボードのファンクションキーによる操作も含みます。

■標準ボタンを使用した画面遷移

標準ボタン（  ：「進む」、  ：「戻る」、  ：「中止」、  ：「更新」）による画面遷移を禁止します。

なお、上記操作にはキーボードのファンクションキーによる操作も含みます。

■ＵＲＬ直接入力による画面遷移

ＵＲＬを直接入力した場合の画面遷移を禁止します。

（５）無料セキュリティソフト「Rapport（ラポート）」の提供

当金庫では、無料セキュリティソフト「Rapport（ラポート）※１」の提供をしています。インターネットバンキング専用のウィルスに対応したセキュリティソフトです。インターネットバンキングを狙ったウィルスの検知・駆除が可能です。不正送金の被害を防止するため、Rapport のご利用をおすすめします。

※１「Rapport（ラポート）」は日本 IBM 株式会社が提供する無料セキュリティソフトです。

【Rapport の概要】

項目	内容
特徴	・インターネットバンキングを狙ったウィルスを検知・駆除します。 ・インターネットバンキングで使用する通信情報の改ざんを防ぎます。 ・インストールするだけで、自動的に機能します。また、ほかのセキュリティソフトとの併用ができます。 （ただし、セキュリティソフトによりインストールや利用する際に特別な操作が必要な場合もあります。）
対象	パソコン
利用料金	無料
利用方法	当金庫ＷＥＢサイトに掲載されている「無料セキュリティソフト（Rapport）の提供開始について」のご案内ページ、またはログイン画面で表示されるポップアップ画面よりダウンロードしてください。

・当金庫ＩＢホームページからの「Rapport（ラポート）」のダウンロードについて

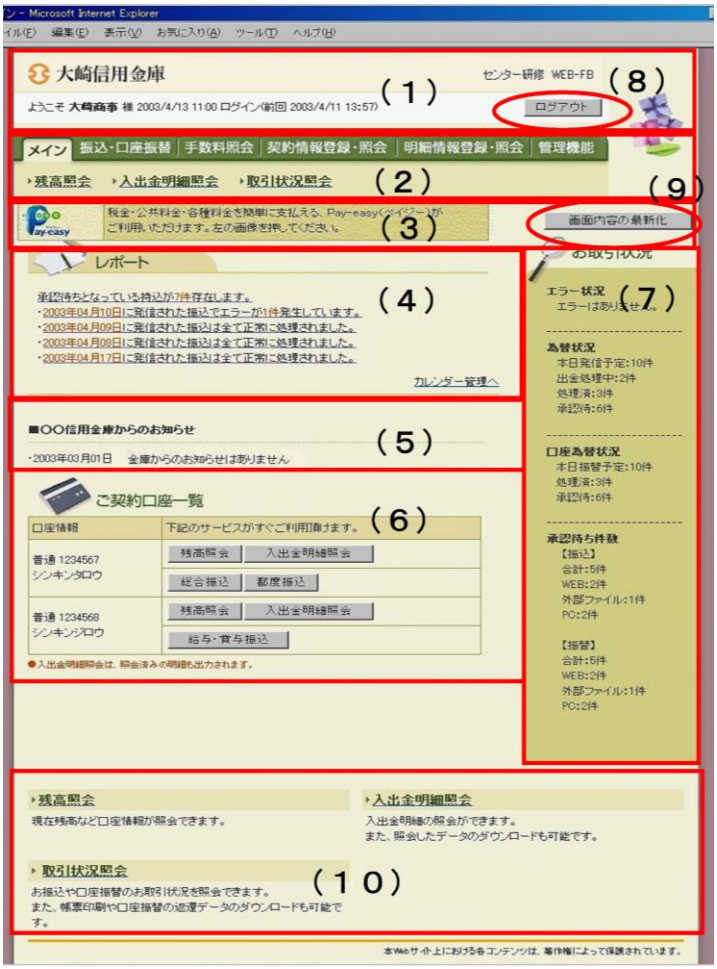
「Rapport（ラポート）」に関するお問い合わせは、日本ＩＢM株式会社のカスタマーサポートまでお願いいたします。

IBM Trusteer Rapport　　平日 9：00～21：00

７．メイン画面構成

メイン画面とは、ログインした後に表示される画面で、各サービスメニューや取引状況等を表示します。

≪メイン画面イメージ≫



（1）ヘッダー

ログインしているユーザ名称、ログイン日時、前回ログイン日時を表示します

（2）メニュー

法人インターネットバンキングにて取扱いできるサービスを分類したメニューを表示します。

なお、利用不可のサービスメニューは、クリックできません。

（3）マルチペイメントサービスリンクボタン

マルチペイメント（税金・各種料金の払込み）へのリンクを表示します。

（4）レポート

エラーメッセージやお客様が設定したメモ情報等を表示します。

メモ情報はカレンダー管理機能にて設定します。

（5）大和信用金庫からのお知らせ

重要なお知らせを表示します。

（6）契約口座一覧

契約している口座でご利用いただけるサービスのショートカットメニューを表示します。利用不可のサービスメニューはクリックできません。

（7）お取引状況

エラー状況や為替・口座振替の処理状況、承認待ちの状況を表示します。

（8）ログアウトボタン

（9）最新化ボタン

ボタンを押下すると、画面の再読込みを行い最新画面を表示します。

(10) メイン画面サブメニュー

メイン画面のサブメニューでは「残高照会」、「入出金明細照会」、「取引状況照会」、「税金・各種料金の払込み」のメニューを選択できます。

.

8. ご利用の前にご確認ください！

法人ＩＢをご利用になる場合、Ｐ７～Ｐ１５の確認が必要になります。
お客様のご利用環境を確認してください。**最新情報は当金庫ホームページをご確認ください。**
なお、推奨環境には、開発元サポートが終了し、セキュリティ更新プログラム等の提供が行なわれていないＯＳやブラウザは含まれません。
推奨環境については動作確認をしておりますが、パソコンの機種や設定において多くの差異が存在します。そのため、ＩＢシステムの動作等に不具合や一部制約が生じることから、完全な動作保証ができないことをご理解ください。
なお、推奨環境対象外のＯＳやブラウザをご利用される場合は、お客様の責任においてご使用いただくようお願いいたします。

（1） OSとブラウザについて

以下の Windows パソコンのみでのご利用となり、スマートフォンやタブレットは推奨環境の対象外です。

OS[*1]	Internet Explorer[*1]	プラグインソフト
Windows 8.1	11.0	Adobe Reader （本サービスにて作成する帳票を閲覧する場合）
Windows 10	11.0	

【留意事項】

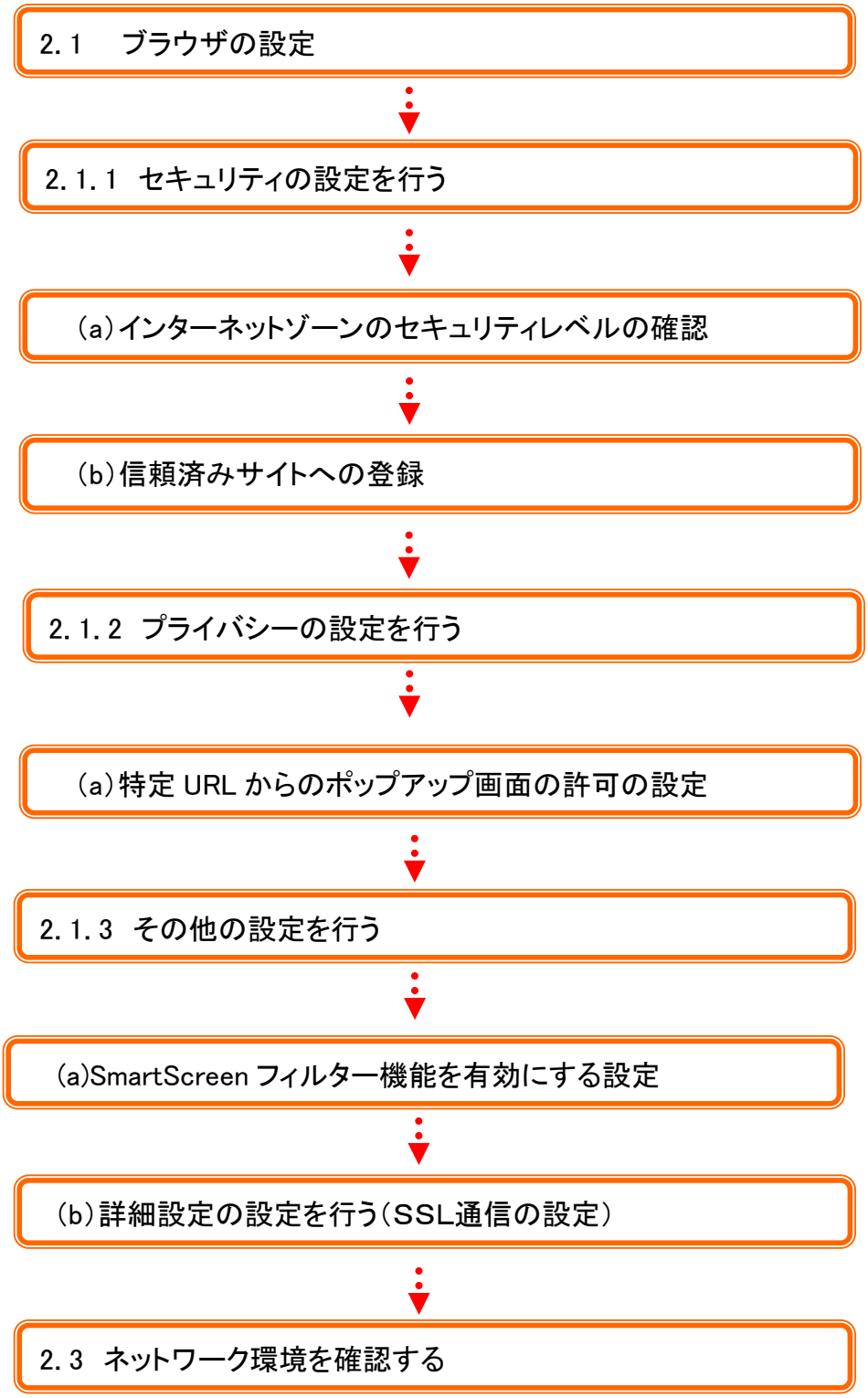
1. セキュリティ上の脆弱性を防止するため、最新のセキュリティパッチの適用、ウィルス対策ソフトの導入を必ず実施するようお願いします。
2. Adobe Reader のバージョンが古い場合、帳票を閲覧できない場合がありますので最新版にアップデートするようお願いします。
3. Windows8.1 Internet Explorer11.0 は、デスクトップ画面から起動してください。
   スタート画面から起動する Internet Explorer11.0 は、推奨環境対象外です。
4. セキュリティの観点からオートコンプリート機能を使用してお客様 ID とパスワードを保存しないようご注意ください。お客様 ID とパスワード保存した場合は削除およびオートコンプリート機能の無効を実施してください。
5. WindowsRT は、推奨環境対象外です。
6. Windows10 のデフォルトブラウザ（MicrosoftEdge）は、電子証明書の取得・更新においては、推奨環境対象外となっております。
7. Mac の Boot Camp を使用した Windows は、推奨環境対象外です。

ポイント

・ブラウザの利用について
電子証明書発行処理は、Microsoft Edge でなく、
Internet Explorer  で行ってください。

(2)パソコンの設定概要

本サービスをご利用いただくには管理者／利用者共に、以下の設定が必要になります。



本サービスをご利用いただくには、以下の設定が必要になります。

なお、**設定内容の最新情報は、当金庫ホームページで確認いただくようお願いいたします。**

2.1 ブラウザの設定

以下の手順でインターネットオプションを設定します。

① Internet Explorer（ブラウザ）を起動します。

② Internet Explorer のメニューの【ツール】（または歯車マーク）をクリックし、「インターネットオプション」を表示します。

メモ

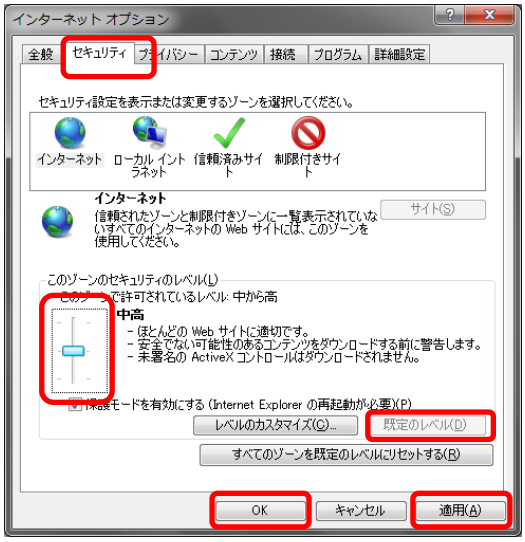
Windows10 における Internet　Explorer11 の利用方法

画面下の Windows スタートアイコンをクリック→スクロールバーを使用し、Windows アクセサリ→Internet Explorer をクリックします。

2.1.1 セキュリティの設定を行う

セキュリティの設定として以下を確認します。

（a）インターネットゾーンのセキュリティレベルの確認



① 「セキュリティー」タブを選択し、「このゾーンのセキュリティレベルが「中高」であることを確認します。

※ セキュリティレベルが「中高」でない場合、既定のレベルをクリックすると、セキュリティレベルが「中高」に変更されます。

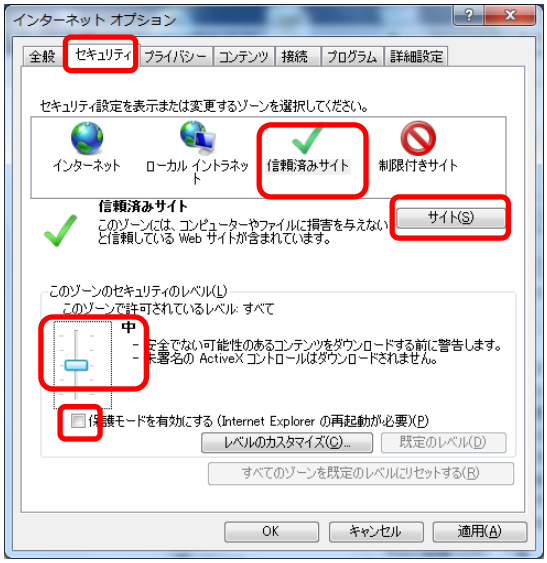
変更後、適用をクリックし、

OKをクリックします。

(b) 信頼済みサイトへの登録

次のＵＲＬを信頼済みサイトへ登録してください。

なお、「信頼済みサイト」のセキュリティレベルは既定のレベルである「中」に設定されていることをご確認ください。



① 「セキュリティ」タブを選択し、信頼済みサイトを選択します。

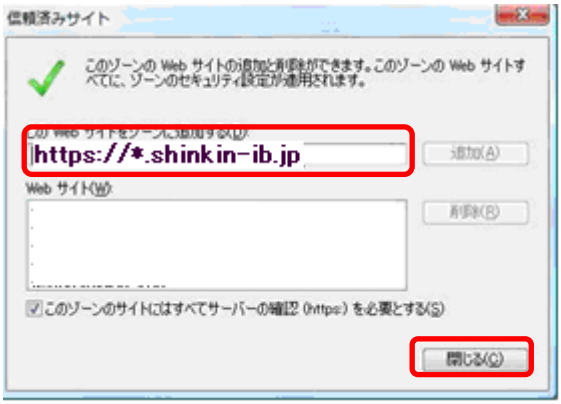
② 信頼済みサイトのゾーンのセキュリティレベルが「中」になっている事を確認します。

※ 信頼済みサイトのゾーンのセキュリティレベルが「中」でない場合、既定のレベルをクリックすると、セキュリティレベルが「中」に変更されます。

③ 「保護モードを有効にする」が無効（チェックが入っていない）であることを確認します。

④ 「信頼済みサイト」からサイトをクリックします。

⇒「信頼済みサイト」画面が表示されます。



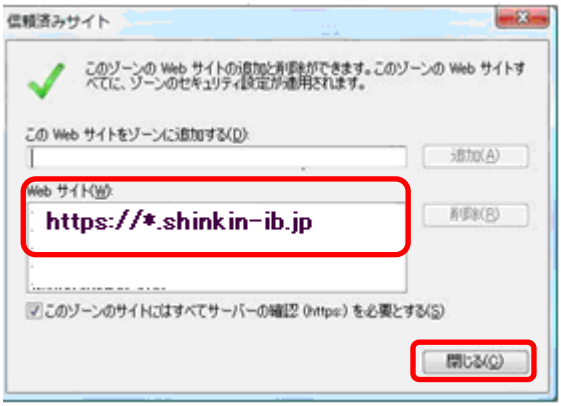
⑤ 「この Web サイトをゾーンに追加する」の入力欄に以下の『「信頼済みサイト」へ登録するＵＲＬ』を追加します。（半角）

⑥ ＵＲＬを入力後、追加をクリックします。

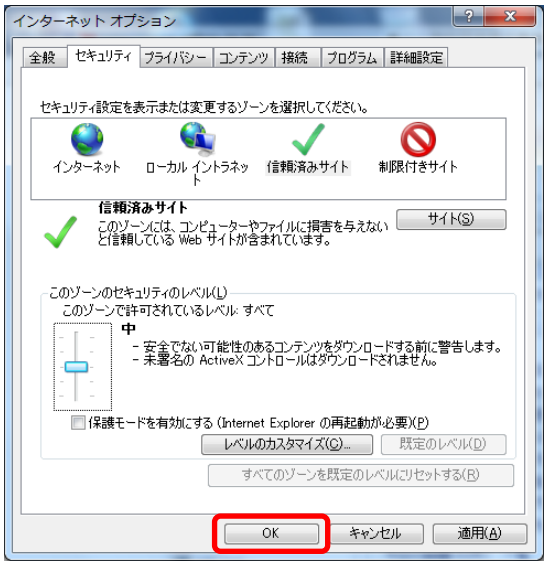
※ 設定を取り止める場合は、閉じるをクリックします。

●「信頼済みサイト」へ追加するＵＲＬ

https://*.shinkin-ib.jp



⑦「Web サイト」欄に、入力した URL が追加されたことを確認し、閉じるをクリックします。



⑧ OKをクリックします。

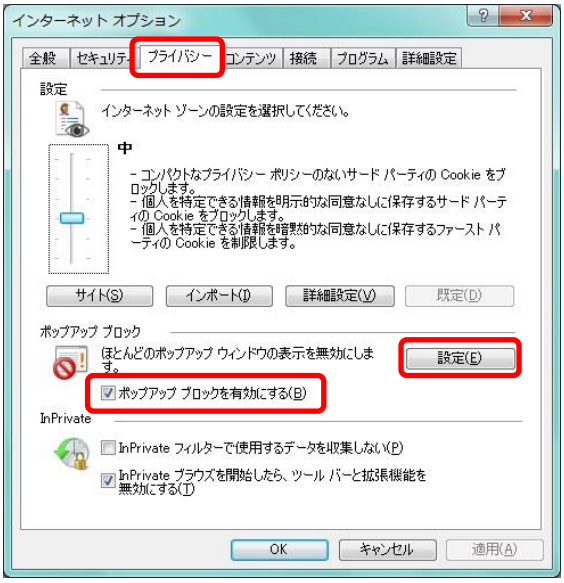
※ 「保護モードを有効にする」にはチェックが入っていないことを確認してください。

※ 設定を取り止める場合は、キャンセルをクリックします。

2.1.2 プライバシーの設定を行う

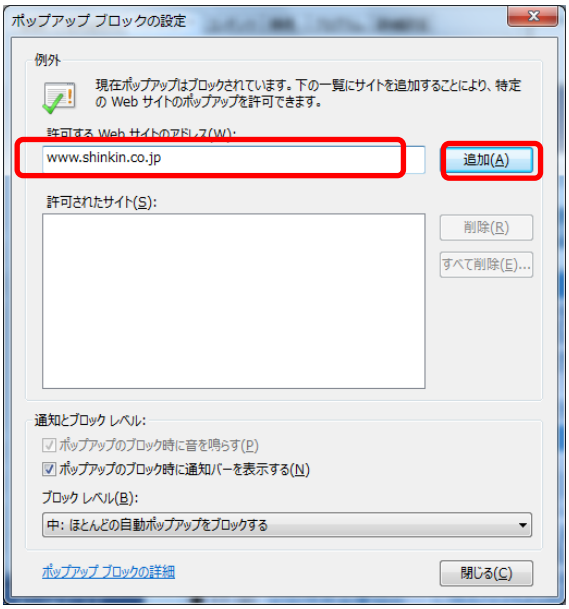
（a）特定 URL からのポップアップ画面の許可の設定

ご利用になるパソコンについて、以下の設定を行ってください。

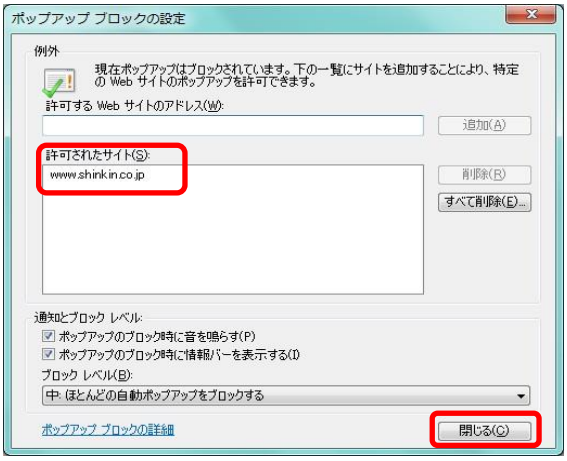


① 「プライバシー」タブを選択し、「ポップアップブロックを有効にする」にチェックを入れて、設定をクリックします。

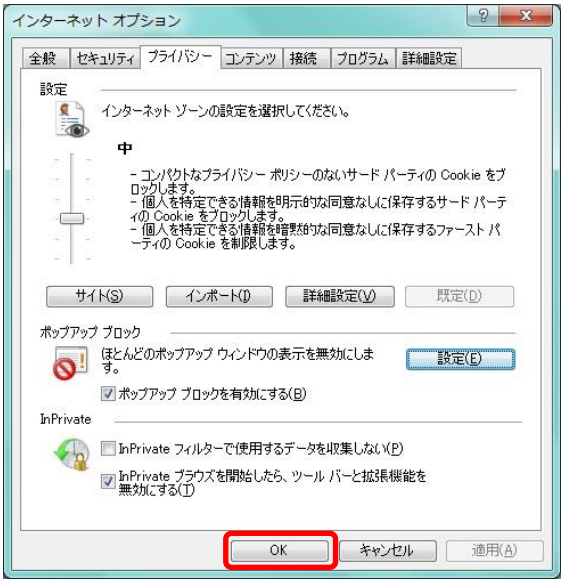
⇒「ポップアップブロックの設定」画面が表示されます。



② 「許可する Web サイトのアドレス」に、「www.shinkin.co.jp」の URL を入力し、追加をクリックします。



③ 「許可されたサイト」に入力した URL が表示されたことを確認し、閉じるをクリックします。



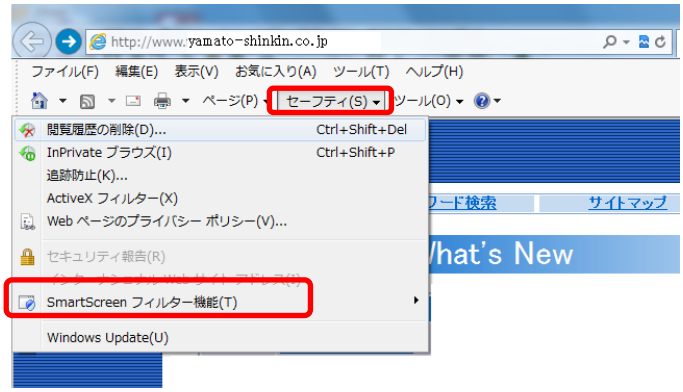
④ 「プライバシー」タブ画面のOKをクリックします。

※ 設定を取り止める場合は、キャンセルをクリックします。

2.1.3 その他の設定を行う

（a） SmartScreen フィルター機能を有効にする設定

インターネットバンキングのログイン画面にアクセスした際に、ブラウザのアドレスバーを緑色に表示するため、「SmartScreen フィルター機能」を有効にします。

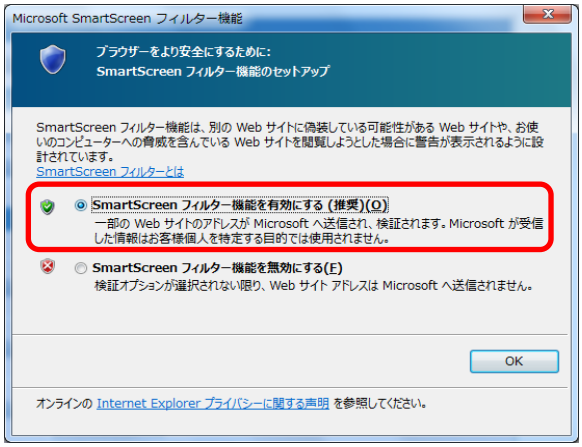


① コマンドバーの「セーフティ」のメニューより「SmartScreen フィルター機能」を選択し、「SmartScreen フィルター機能を有効にする」をクリックします。

→「Microsoft SmartScreen フィルター機能」ダイアログが表示されます。

※ツールバーの「ツール」メニューより「SmartScreen フィルター機能」を選択する場合も上記操作と同様になります。

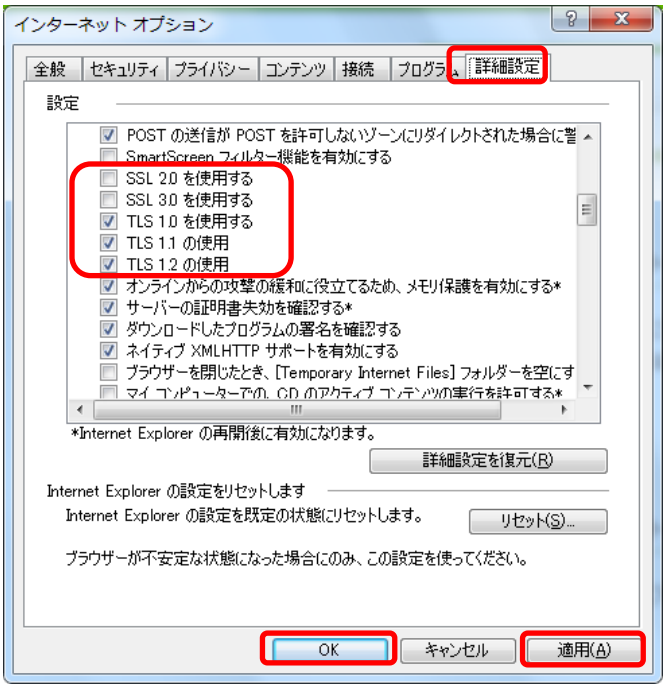
※「SmartScreen フィルター機能」を選択した後、「SmartScreen フィルター機能を無効にする」と表示されることがあります。(SmartScreen フィルター機能を有効にしている場合)



② 「SmartScreen フィルター機能を有効にする(推奨)」にチェックを入れて「ＯＫ」をクリックします。

（b）詳細設定の設定を行う（ＳＳＬ通信の設定）

ご利用になるパソコンについて以下の設定を行ってください。



① 「詳細設定」タブを選択し、設定のセキュリティ欄の「SSL2.0 を使用する」「SSL3.0 を使用する」のチェックを外します。

② 「TLS1.0 を使用する」「TLS1.1 の使用」「TLS1.2 の使用」にチェックを入れます。

③ 適用 をクリックし。OK をクリックします。

※設定を取りやめる場合は、キャンセル をクリックします。

2.2 ブラウザの再起動

インターネットオプションの設定内容を反映するため、全てのブラウザを閉じてから再起動してください。

2.3　ネットワークの設定を確認する

信頼済みサイトへ登録した場合であってもログイン画面が表示されない等の不具合が発生した場合は、お客様のネットワーク環境において、ブラウザで設定した信頼済サイトがファイヤーウォール等でブロックされていないかご確認ください。

なお、ファイヤーウォールの設定詳細については、お客様のネットワーク管理者にご確認ください。