

ご利用推奨環境と パソコンの設定

目次

1. 推奨環境

ご利用のパソコンの推奨環境を確認します。

- (1) 推奨環境1
- (2) パソコンの設定概要2

2. ブラウザの設定

「朝日ビジネスWEB」をご利用いただく前のパソコン設定する手順についての説明です。

- 2.1 ブラウザの設定4
 - 2.1.1 セキュリティの設定を行う4
 - 2.1.2 プライバシーの設定を行う6
 - 2.1.3 SmartScreen フィルター機能を有効にする設定9
 - 2.1.4 互換表示設定を行う (IE10/IE11 のみ)9
 - 2.1.5 ブラウザの再起動 11
- 2.2 ネットワークの設定を確認する 11

3. 無料セキュリティソフト「Rapport (ラポート)」のインストール

インターネットバンキング専用のウィルス対策ソフト「Rapport (ラポート)」の使用をおすすめします。11

別紙 スタート画面からデスクトップ画面への切替方法

ご案内

この「別冊」は朝日ビジネスWEBをご利用のお客さま専用です。

電子証明書・その他の操作に関することは、「操作説明書」WEB版をご覧ください。

朝日ビジネスWEB ご利用推奨環境とパソコンの設定

1. 推奨環境

朝日ビジネスWEBの推奨環境は以下のとおりです。

推奨環境には、開発元のサポートが終了し、セキュリティ更新プログラム等の提供が行われていないOSやブラウザは含まれません。

また、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、インターネットバンキングの動作等に不具合や一部制約が生じる可能性があることから、完全な動作保証はできないことをご理解お願いいたします。

なお、推奨環境対象外のOSやブラウザをご利用になる場合は、お客さま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) 推奨環境

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対象外です。

OS	Internet Explorer
Windows Vista SP2 (32bit 版)	8.0、9.0
Windows 7 SP1(32bit 版/ 64bit 版)	8.0、9.0、10.0、11.0
Windows 8 (32bit 版/ 64bit 版)	10.0
Windows 8.1(32bit 版/ 64bit 版)	11.0

平成 26 年 9 月 5 日現在

※Internet Explorer は米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

【留意事項】

1. Internet Explorer10.0/11.0 をご利用いただく場合は、「互換表示設定」を実施してください。

「互換表示設定」の設定方法は、本書 10 ページを参照ください。

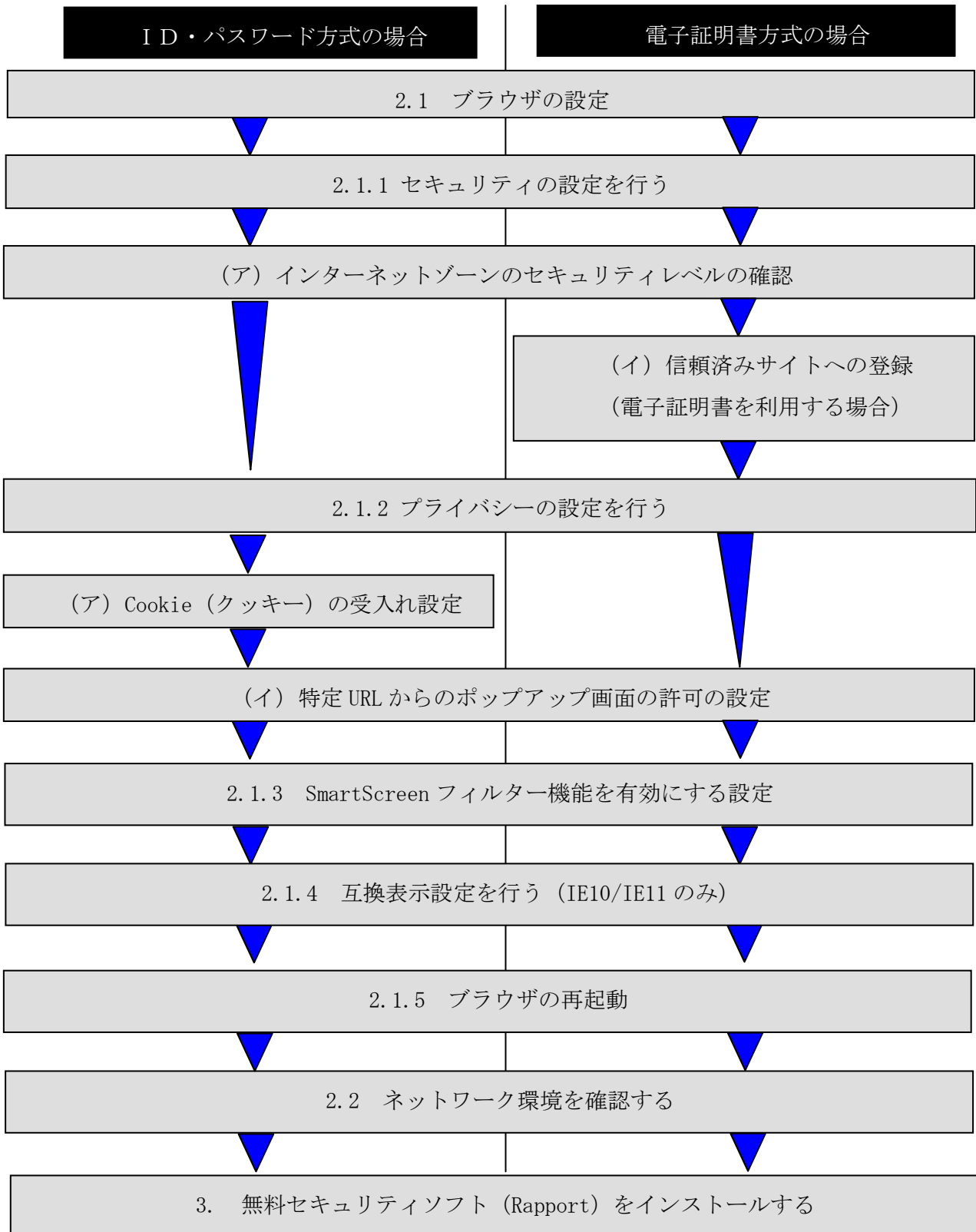
Internet Explorer 10.0/11.0 の「互換表示設定」を実施しない場合、画面表示崩れおよび電子証明書の取得・更新時にエラー（認証方式が電子証明書方式の場合）が発生します。

2. 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、ウイ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。
3. ソフトウェアキーボードご利用時に「この Web ページがクリップボードへアクセスするのを許可しますか？」というメッセージがダイアログボックスで表示された場合には、「アクセスを許可する」を選択して継続してください。
4. 電子証明書方式の場合は、Internet Explorer8.0/Internet Explorer9.0 の 64bit 版は、推奨環境対象外です。
5. Windows8 Internet Explorer 10.0 および Windows8.1 Internet Explorer 11.0 は、デスクトップ画面から起動してください。
デスクトップ画面への切替方法は、本書の最終ページ【別紙】を参照ください。
スタート画面から起動する Internet Explorer 10.0/11.0 は、推奨環境対象外です。
6. Windows 7 Professional および Ultimate の各エディションにおいて仮想化機能の「Windows XP Mode」では、ご利用いただけません。
7. Macintosh についてはご利用いただけません。
また、仮想環境構築ソフトウェア（Boot Camp、Parallels Desktop 等）を利用して Windows を動作させた環境についてもご利用いただけません。
8. WindowsRT は、推奨環境対象外です。

（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。

1. ブラウザの設定
 - ・セキュリティの設定を行う
 - （ア）インターネットゾーンのセキュリティレベルの確認
 - （イ）信頼済みサイトへの登録（電子証明書方式のみ）
 - ・プライバシーの設定を行う
 - （ア）Cookie（クッキー）の受入れ設定（ID・パスワード方式のみ）
 - （イ）特定 URL からのポップアップ画面の許可の設定
 - ・SmartScreen フィルター機能を有効にする設定
 - ・互換表示設定を行う（IE10/IE11 のみ）
 - ・ブラウザの再起動
2. ネットワークの設定を確認する
3. 無料セキュリティソフト（Rapport）をインストールする



次ページ以降は、パソコンの設定を記述しています。

2. ブラウザの設定

2.1 ブラウザの設定

IE 8、IE 9、IE 10、IE 11のブラウザにおいて、以下の手順でインターネットオプションを設定します。

※ツールのアイコン



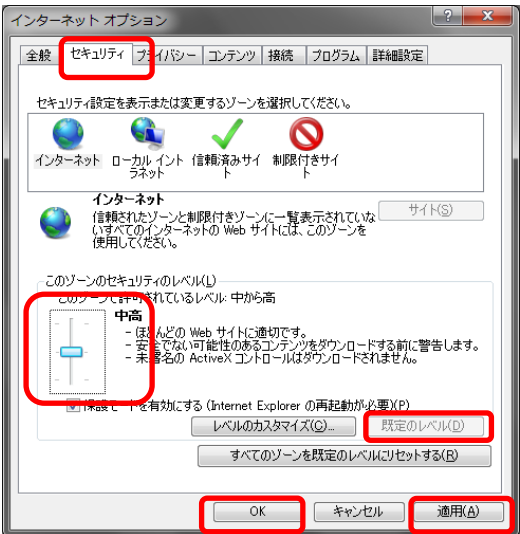
- ①Internet Explorer (ブラウザ) を起動します。
- ②Internet Explorer のメニューの【ツール】(または歯車マーク) をクリックし、「インターネットオプション」を表示します。

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。

- ・インターネットゾーンのセキュリティレベルが「中高」(規定レベル) になっていること。
- ・信頼済みサイトへの登録 (電子証明書を利用する場合)

(ア) 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」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。

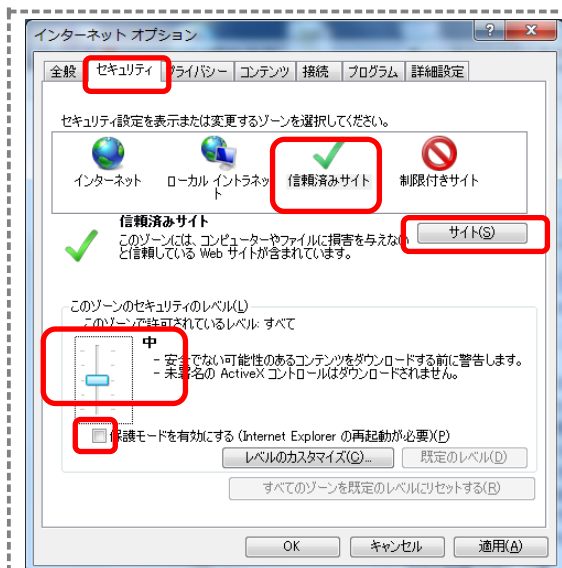
※ セキュリティレベルが「中高」でない場合、既定のレベルをクリックすると、セキュリティレベルが「中高」に変更されます。

変更後、適用をクリックし、OKをクリックします。

(イ) 信頼済みサイトへの登録（電子証明書を利用する場合）

電子証明書をご利用になる場合、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。

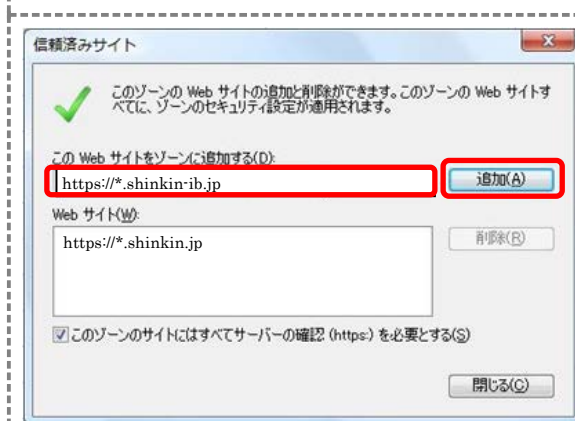
② 信頼済みサイトのゾーンのセキュリティレベルが「中」になっていることを確認します。

※ 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。（ただし、Windows XP では表示されません。）

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）

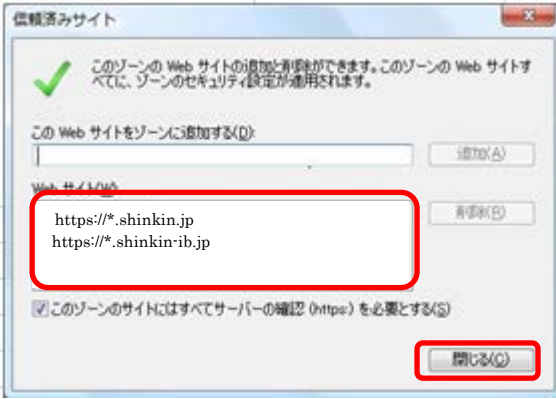
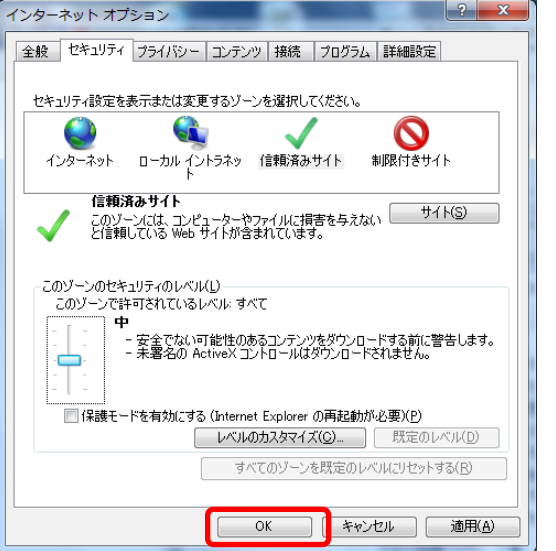
⑥ URLを入力後、「追加」をクリックします。

※ 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（朝日ビジネスWEBをご利用の場合）

https://*.shinkin.jp（朝日でんさいサービスをご利用の場合）

	<p>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。</p>
	<p>⑧ OKをクリックします。</p> <ul style="list-style-type: none"> ※ 「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。(ただし、Windows XP では表示されません) ※ 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

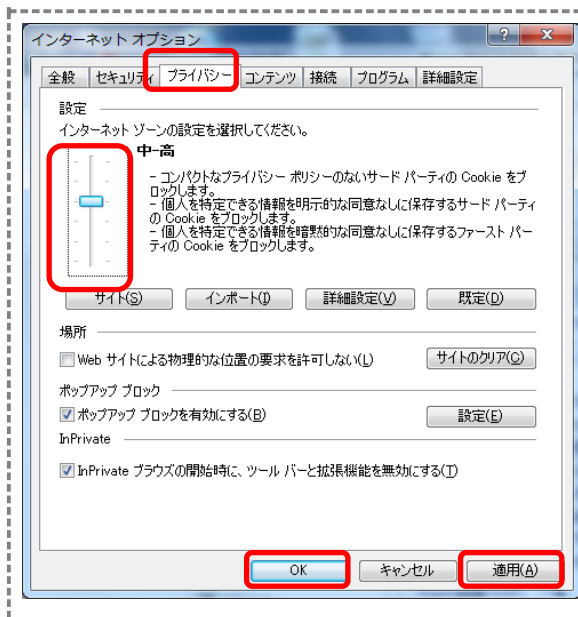
プライバシーの設定として以下を確認します。

- ・ Cookie (クッキー) の受入れ設定 (ID・パスワード方式を利用する場合)
- ・ 特定 URL からのポップアップ画面の許可の設定

(ア) Cookie (クッキー) の受入れ設定 (ID・パスワード方式を利用する場合)

ブラウザの Cookie について、プライバシーレベルを「中 - 高」以下 (「すべての Cookie をブロック」、「高」以外) にする必要があります。

なお、既定レベルは「中」です。



① 「プライバシー」タブを選択し、「すべての Cookie をブロック」または「高」以外に設定されていることを確認します。

※ 「すべての Cookie をブロック」または「高」に設定されている場合、正常に動作しません。スライダのつまみを移動して、設定を変更してください。

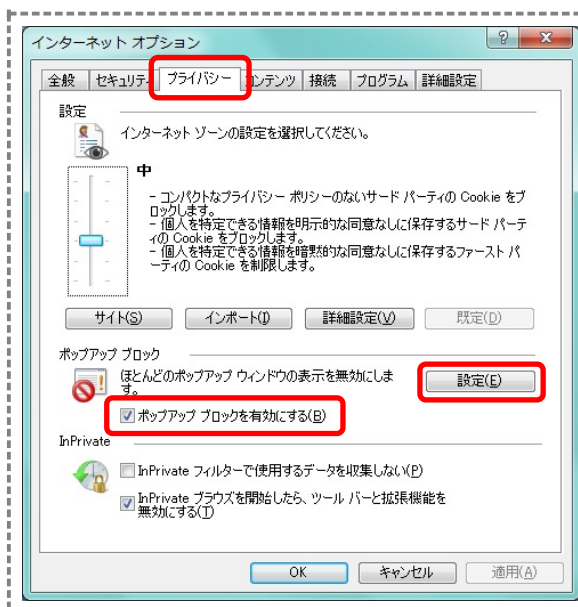
② **適用** をクリックし、**OK** をクリックします。

※ 設定を変更していない場合は、OKのみをクリックします。

※ 設定を取り止める場合は、キャンセル をクリックします。

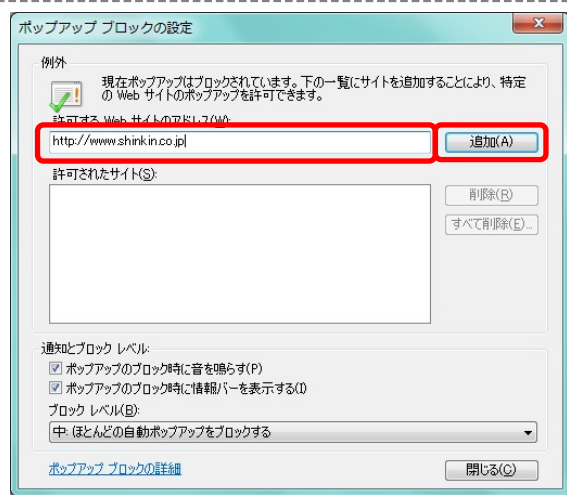
(イ) 特定 URL からのポップアップ画面の許可の設定

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。

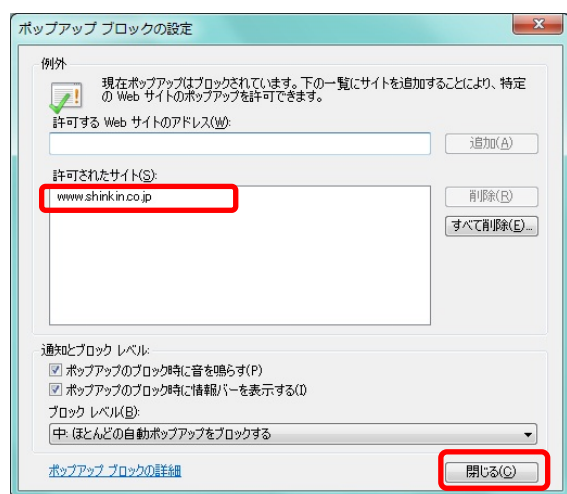


① 「プライバシー」タブを選択し、「ポップアップブロックを有効にする」にチェックを入れて、**設定** をクリックします。

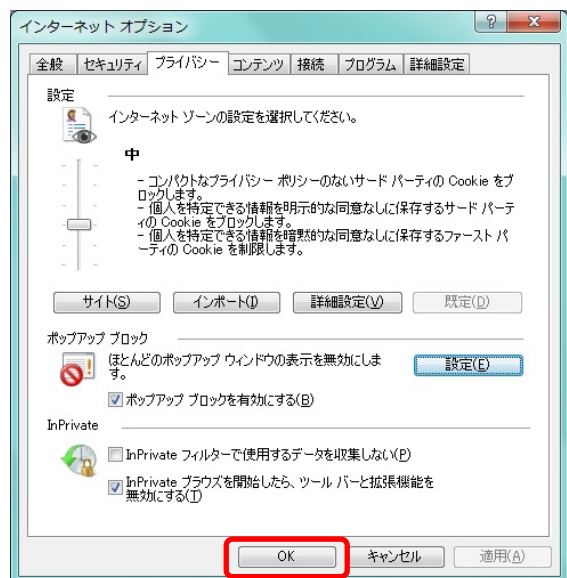
⇒ 「ポップアップブロックの設定」画面が表示されます。



- ② 「許可する Web サイトのアドレス」に、「http://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。

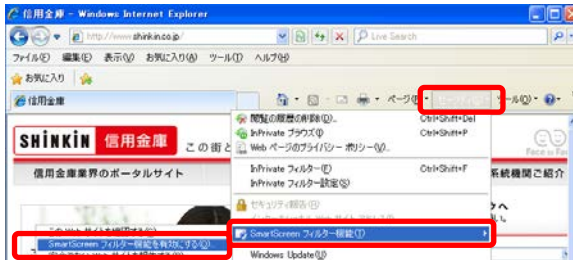
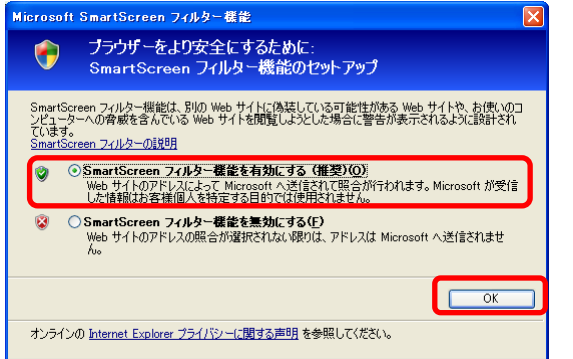


- ④ 「プライバシー」タブ画面の**OK** をクリックします。

※ 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 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

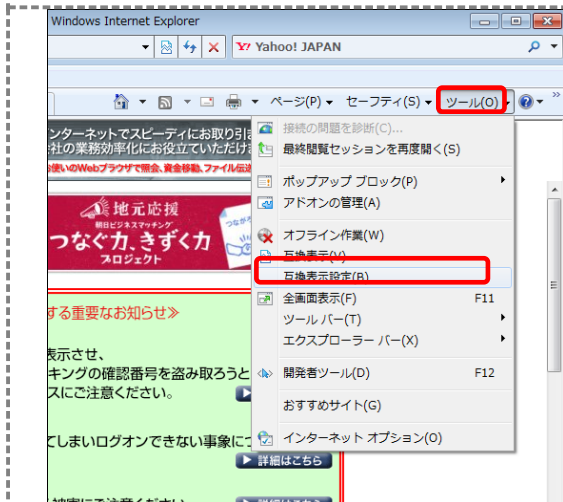
	<p>① コマンドバーの「セーフティ」のメニューより「SmartScreen フィルター機能」を選択し、「SmartScreen フィルター機能を有効にする」をクリックします。</p> <p>⇒ 「Microsoft SmartScreen フィルター機能」ダイアログが表示されます。</p> <p>※ 「SmartScreen フィルター機能」を選択した後、「SmartScreen フィルター機能を無効にする」と表示されることがあります。 (SmartScreen フィルター機能を有効にしている場合)</p>
	<p>② 「SmartScreen フィルター機能を有効にする (推奨)」にチェックを入れて、OKをクリックします。</p>

2.1.4 互換表示設定を行う (IE10/IE11 のみ)

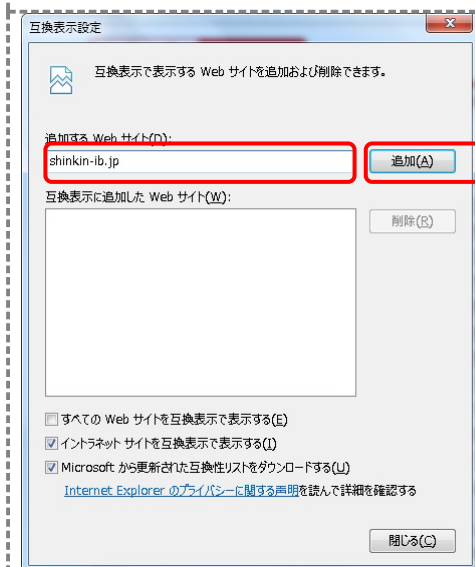
Internet Explorer 10.0/11.0 をご利用いただく場合は、「互換表示設定」を実施してください。Internet Explorer 10.0/11.0 の「互換表示設定」を実施しない場合、画面表示崩れおよび電子証明書の取得・更新時にエラーが発生します。

⇒設定方法は、次ページを参照ください。

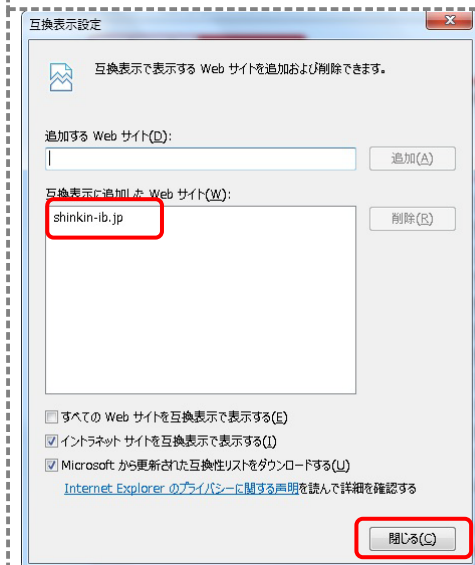
【互換表示設定の方法】



①Internet Explorer のメニューの【ツール】をクリックし、「互換表示設定」をクリックします。



②「追加する Web サイトに「shinkin-ib.jp」を入力し、**追加**をクリックします。



③「互換表示に追加した Web サイト」に入力した内容が表示されたことを確認し、**閉じる**をクリックします。

※ 「すべての Web サイトを互換表示で表示する」にチェックが入っていないことを確認してください。

2.1.5 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。

2.2 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オン画面が表示されない等の不具合が発生した場合は、お客さま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み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、お客さまのネットワーク管理者にご確認ください。

3. 無料セキュリティソフト（Rapport）をインストールする

コンピュータウィルスを用いてインターネットバンキングを悪用した不正送金事件が発生しています。当金庫では、インターネットバンキング専用のウィルス対策ソフト「Rapport（レポート）※」の使用をおすすめします。

※Trusteer（IBM 社）が提供するウィルス対策ソフトです。

1. 特徴

- (1) 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。
- (2) 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。
- (3) 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。以下の URL を参照ください。

他のセキュリティソフトとの互換性：

(<http://www.trusteer.com/ja/support/compatibility-other-security-software>)

- (4) 無料でご利用できます

2. 利用環境

Rapport（レポート）でサポートされている OS、ブラウザは、以下の URL を参照ください。

(<http://www.trusteer.com/ja/support/supported-platforms>)

※スマートフォン、タブレット端末、携帯電話は対象外です。

3. Rapport（レポート）のインストール

(1) Rapport（レポート）インストール方法

当金庫の「無料セキュリティソフト Rapport（レポート）のご案内」サイト（URL は下記参照）を参照ください。

URL : <http://www.shinkin.co.jp/info/kyotsu/oshirase/20141010/index.html>

無料セキュリティソフト (Rapport) のご案内

コンピュータウイルスを用いてインターネットバンキングを悪用した不正送金事件にご注意ください。当金庫では、インターネットバンキング専用のウイルスに対応したセキュリティソフト「**Rapport** (レポート)※」の使用をおすすめします。
※「Rapport」は、IBM社が提供する無料セキュリティソフトです。

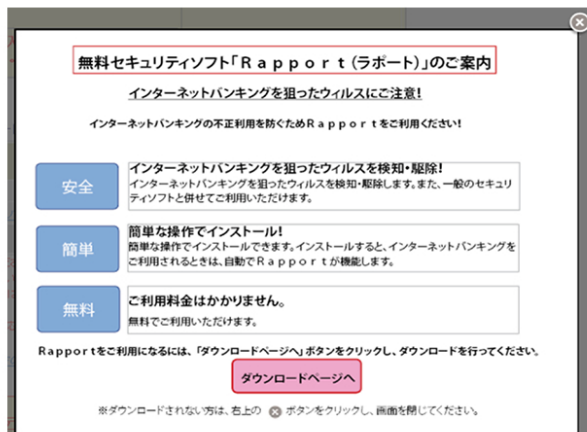
1. 特徴

1 インターネットバンキングを狙ったウイルスを検知・駆除します。

(2) インストール推奨するポップアップ画面

当金庫インターネットバンキングのログオンページへアクセスすると、ポップアップ画面が表示される場合があります。このポップアップ画面は、お客さまに Rapport のインストールをおすすめする画面です。Rapport のインストール後は、表示されません。

【表示されるポップアップ画面】



(3) Rapport (レポート) 利用時の留意点

- ・「Rapport (レポート)」は、IBM 社が提供するソフトウェアであり、当金庫が提供するものではありません。
- ・本ソフトウェアの利用に当たっては、IBM 社が定める使用許諾契約に同意する必要があります。
- ・本ソフトウェアはインターネットバンキングを攻撃対象とするウィルス対策ソフトです。インターネットバンキングに特化しているため、市販のウィルス対策ソフトと併せてご利用ください。
※本ソフトウェアは他のウィルス対策ソフトとの相性により、パソコンの動作が不安定になる場合があります。事前に、IBM 社サポートサイトに掲載されている「他のセキュリティ製品との互換性について」をご確認ください。
- ・本ソフトウェアは、パソコン専用です、スマートフォンやタブレット端末では、ご利用できません。
- ・本ソフトウェアをインストールするためには、パソコンの管理者権限でログインする必要があります。
- ・本ソフトウェアは、IBM 社により予告なく変更または廃止される場合があります。
- ・本ソフトウェアを利用しても、ウィルスによる被害を受ける可能性が完全になくなるわけではありません。
- ・本ソフトウェアを利用した結果、お客さまが何らかの被害を受けた場合でも、当金庫は責任を負いません。

4. お問い合わせ先

Rapport(レポート)に関するお問い合わせは、Trusteer カスタマーサポートまでお願いいたします。

Trusteer カスタマーサポート <http://www.trusteer.com/ja/support>

パソコンの設定が終わりましたら、管理者／利用者共に開通確認・電子証明書取得等を行ってください。
詳細は、『朝日ビジネスWEB』操作説明書（WEB版）を参照ください。