

COMSUITE Portal クイックリファレンス

2025 年 3 月

COMSUITE
GLOBAL TRANSACTION BANKING SOLUTIONS

目次

第 1 章 接続・ログイン編	2
1-1 パソコンの動作環境を確認する	3
1-2 ログインする	4
1-3 パスワードを変更する	8
第 2 章 セキュリティ編	10
2-1 ご注意いただきたい事項	11
2-2 本サービスのセキュリティ機能	13
2-3 お客さま側でのセキュリティ管理	14
2-4 真正なサーバーであることを確認する	17
2-4-1 ブラウザのアドレスバーに表示されるアドレスを確認する	17
2-4-2 通信先サーバーの SSL 証明書を表示して確認する	18

第 1 章 接続・ログイン編

- 1-1 パソコンの動作環境を確認する
- 1-2 ログインする
- 1-3 パスワードを変更する

1-1 パソコンの動作環境を確認する

本サービスの利用には、指定のオペレーティングシステム(OS)、ブラウザソフト、PDF 閲覧ソフトが必要です。
最新の動作環境は、以下の URL にアクセスし、カスタマーサポートをご参照ください。

URL: <https://ebusiness.bk.mufig.jp/login/>

1-2 ログインする

本サービスでは、本人確認のために OTP トークンによる認証を行います。OTP トークンは当行より発行します。ログインや、各サービスでの承認時などに必要となります。

事前準備として、OTP トークンをご用意ください。

なお、初めてログインする場合とパスワード初期化後にログインする場合は、この後の「■初回のログイン・パスワード初期化後のログインの場合」を参照してください。

OTP トークン



ブラウザのアドレス欄に、COMSUITE の URL を入力します。

URL: <https://ebusiness.bk.mufig.jp/login/>

 この URL にアクセス後、表示されるログイン画面をお気に入り(ブックマーク)に登録すると、 がお気に入りのアイコンとして表示されます。

ログイン画面



ログイン画面が表示されます。

[カスタマーID]欄、[ユーザーID]欄、[パスワード]欄に、COMSUITE カスタマーID、COMSUITE ユーザーID、パスワードをそれぞれ入力します。

 初めてログインする場合とパスワード初期化後にログインする場合は、この後の「■初回のログイン・パスワード初期化後のログインの場合」を参照してください。

上記を入力すると、OTP を入力できるようになります。

OTP トークンの[1]番ボタンを押し、トークンに表示された OTP を [ワンタイムパスワード(OTP)] 欄に入力します。

 ログイン をクリック

パスワード変更画面

パスワードの有効期限が切れている場合は、パスワード変更画面が表示されます。

ログイン画面で入力したパスワードを
[現在のパスワード] 欄に入力します。

新しく設定するパスワードを
[新しいパスワード] 欄と
[新しいパスワード(確認)] 欄に入力します。

パスワードに関するルールについては、
以下を参照してください。

 1-3 パスワードを変更する

次へ をクリック

COMSUITE Portal のトップページ



COMSUITE Portal のトップページが表示
されます。

ダイレクトリンクから、利用するサービスを
クリックしてください。

■初回のログイン・パスワード初期化後のログインの場合

ブラウザのアドレス欄に、COMSUITE の URL を入力します。

URL: <https://ebusiness.bk.mufg.jp/login/>

 この URL にアクセス後、表示されるログイン画面をお気に入り(ブックマーク)に登録すると、 がお気に入りのアイコンとして表示されます。

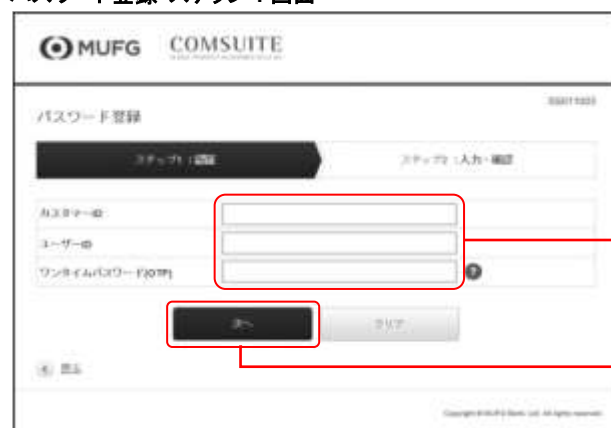
ログイン画面



ログイン画面が表示されます。

パスワード登録 をクリック

パスワード登録 ステップ 1 画面



パスワード登録 ステップ 1 画面が表示されます。

[カスタマーID]欄、[ユーザーID]欄、
[ワンタイムパスワード(OTP)]欄に
それぞれ入力します。

次へ をクリック

パスワード登録 ステップ 2 画面

パスワード登録 ステップ 2 画面が表示されます。

新しく設定するパスワードを
[新しいパスワード] 欄と
[新しいパスワード(確認)] 欄に入力します。

パスワードに関するルールについては、
以下を参照してください。

 1-3 パスワードを変更する

登録 をクリック

COMSUIE Portal のトップページ



COMSUIE Portal のトップページが表示されます。

ダイレクトリンクから、利用するサービスを
クリックしてください。



エラーが表示される場合は、以下をご確認ください。

- ・パスワード登録済みの場合は、パスワード登録できません。ログイン画面よりログインしてください。
- ・OTPトークンが有効化されていない場合は、パスワード登録できません。アドミニストレーターにご確認ください。
- ・既にOTPトークンをお持ちの方で新しいOTPトークンを受け取った方については、新しいOTPトークンでのログインが確認できるまでは新しいOTPトークンでのパスワード登録はできません。パスワード登録が必要な場合は、古いOTPトークンをご利用ください。(新しいOTPトークンでのログインが確認できるまで、古いOTPトークンをお持ちください。)
- ・カスタマーID、ユーザーID、ワンタイムパスワードのいずれかが正しくない場合は、パスワード登録できません。入力内容をご確認の上、再度お試しください。

1-3 パスワードを変更する

パスワードはセキュリティ強化の観点から定期的に変更を行ってください。変更については文字数・内容・有効期限などに留意して設定してください。

トップページ



「管理」をクリック

「管理」メニュー画面



「マイ・プロフィール」の「パスワード変更」をクリック

パスワード変更画面



別ウインドウで、パスワード変更画面が表示されます。

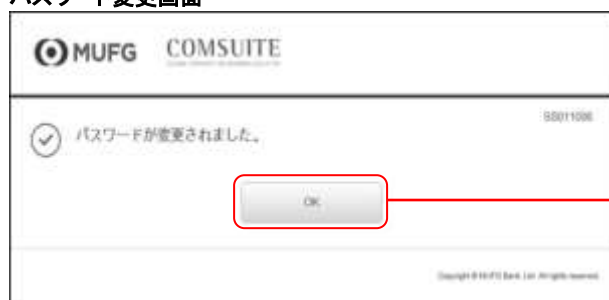
これまで使用していたパスワードを入力
新しいパスワードを入力



- パスワードに使用可能な文字は①数字(0～9)、②英字(A～Z、a～z(大文字・小文字の両方を使用してください))、③記号(!#\$%&()+-=?@_等)の3種類です。
- 上記①②③の3種類の文字をすべて含む8桁～16桁のパスワードを設定してください。
- ここで設定したパスワードは90日間有効で、定期的に変更する必要があります。

次へ をクリック

パスワード変更画面



OK をクリック



- パスワードは本人確認のため大切なものです。他人に知られないよう十分ご注意ください。
- パスワードのメモは作らないでください
- パスワードは定期的に変更してください。
- パスワードは再利用をしないようにしてください。
- 他で使用しているパスワードと同じものは避け、忘れにくいパスワードをご利用ください。
- 他人が簡単に予測できたり、または個人情報が含まれるものは避けてください。(例: 名前、電話番号、誕生日など)
- 同じ文字の連続や、すべて数字、すべてアルファベットによるパスワードは避けてください。
- パスワードは他人と共用しないでください。
- 有効期限を過ぎますと、新しいパスワードに変更していただくまでは、本システムをご利用いただくことができません。
- パスワードは有効期限内であっても変更することができます。

第 2 章 セキュリティ編

- 2-1 ご注意いただきたい事項
- 2-2 本サービスのセキュリティ機能
- 2-3 お客さま側でのセキュリティ管理
- 2-4 真正なサーバーであることを確認する
 - 2-4-1 ブラウザのアドレスバーに表示されるアドレスを確認する
 - 2-4-2 通信先サーバーの SSL 証明書を表示して確認する

2-1 ご注意いただきたい事項

本サービスでトラブル等の原因となる操作について説明します。

ブラウザでご注意いただきたい事項



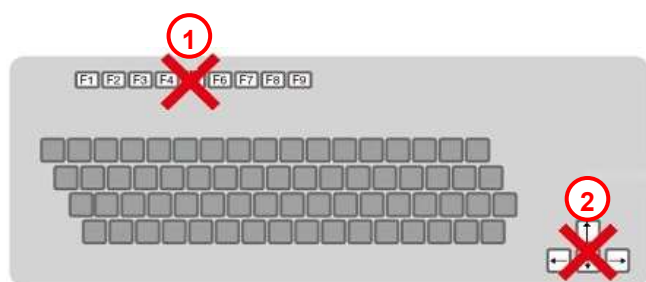
- ① **アドレス(URL)の直接入力禁止**
ログイン後は、アドレスを直接入力して、他のメニューや本サービス以外のサイトに移動することはできません。
- ② **ブラウザ上部のアドレスバーやツールバーにある[←][→][⌂][X]などのボタンは使用禁止**
正常に機能しない場合があります。必ず本サービス画面内のボタンを利用してください。
- ③ **ブラウザやタブの右上の[X]閉じるボタンは使用禁止**
[X]をクリックすると、正常に終了できず次回ご利用時に正常にログインできない場合があります。必ず画面右上の[Logout]をクリックしてサービスを終了してください。

マウス操作でご注意いただきたい事項



- ① **左クリックは1回(ダブルクリック禁止)**
テキストリンクやボタンを2回続けてクリック(ダブルクリック)せず、必ず1回のみ操作してください。
- ② **ブラウザの「前に戻る」「次に進む」は禁止**
マウスの右クリックなどで、「前に戻る」「次に進む」を操作するとエラーメッセージが表示されたり、正確に操作できなくなる場合があります。必ず画面上のメニューやテキストリンク、ボタンなどをクリックして画面を表示してください。

キーボードでご注意いただきたい事項



- ① 画面を更新するファンクションキーを使用しないでください。
- ② ブラウザの[戻る]ボタン、[進む]ボタンに相当するファンクションキーを使用しないでください。

2-2 本サービスのセキュリティ機能

お客さまに安心してご利用いただくため、インターネットなどを通じたお取引にともなうさまざまなリスクに対し、万全のセキュリティ体制で臨んでいます。

■インターネットなどを通じたリスクについて

- (1) インターネットでは一般的に、情報の「改ざん」、「盗難」、契約者本人への「なりすまし」、コンピューターシステムへの「不正なアクセス」など、悪意の第三者による攻撃リスクがあります。
- (2) また、「ハードウェア障害」、「ソフトウェア障害」、「回線障害」などによりお取引ができなくなるリスクがあります。

■本サービスは、以下のようなセキュリティ機能を備えています。

- (1) お客さまと当行の間で送受信される口座照会、送金指図等の通信データはすべて SSL (Secure Socket Layer) という暗号化技術を用いることにより、お客さまの重要な情報を保護しています。
- (2) お客さまの本人確認には、カスタマーID、ユーザーID、パスワードに加えて、OTP トークンで生成されるワンタイムパスワード (1 回使い切りのパスワード) により認証を行う、高いレベルの本人確認方法を採用しています。また、送金指図や利用者の登録変更などの承認操作でも OTP トークンから生成される取引承認コードの入力により、一層安全性を高めています。
- (3) 他人の不正なアクセスがないか確認できるよう、ログイン時に前回のログイン時刻を表示します。
- (4) パスワード、ワンタイムパスワード、取引承認コードの入力を連続して所定回数以上間違えた場合、セキュリティのためそのユーザーID はロックアウトされ、アドミニストレーターによってロックアウト解除の操作が行われるまでシステムを利用できなくなります。
(アドミニストレーターのユーザーID がロックアウトされ、他にロックアウト解除の承認者がいない場合は、お取引店への所定の手続きが必要となります)
- (5) ログイン後に万一お客さまがパソコン等から離席され、その間に第三者に不正に操作されることを防止するため、一定時間操作がない場合には自動的にログアウトし、操作を終了いたします。
- (6) 本サービスの主要機器は二重化等の対応により、バックアップ体制を整備しています。
- (7) セキュリティシステムに関する定期的なレベルアップを行っています。
- (8) 銀行サーバーに複数のファイアーウォールを設け、インターネットからの不正なアクセスを防いでいます。万が一、不測の事態が発生した場合でも即時に対応する体制を敷いています。

2-3 お客さま側でのセキュリティ管理

安全な環境下で本サービスをお使いいただくためには、お客さま側でもセキュリティの管理をしていただく必要があります。

以下にお客さま側でのセキュリティ管理について説明します。

ご利用時の管理

- (1) ログインしたままパソコンから離れないように気をつけてください。操作を終了する時は、必ずログアウトしてください。またログアウト時には、すべてのブラウザ画面を閉じてください。操作中以外は、OTP トークンを安全な場所に保管してください。
- (2) Internet Explorer において「インターネットオプション」の「セキュリティ」の設定を必要以上に緩和しないことをおすすめします。すなわち、「インターネット」のセキュリティの設定レベルはできるだけ「中」以上に設定し、インターネットをご利用の際は、「ActiveX コントロールに対して自動的にダイアログを表示」や「スクリプトを実行しても安全だとマークされていない ActiveX コントロールの初期化とスクリプトの実行」については、ダイアログでかならず確認することをおすすめします。
- (3) 本サービスをご利用いただいているパソコンを、本サービスのユーザーではない方と共用している場合、本サービスからダウンロードしたデータの取り扱い管理には十分ご注意ください。
- (4) ユーザー別に「ログ」メニューより本サービスの利用状況を照会することができます。不正アクセス、不正操作の監視などに利用できますので、定期的にチェックすることをおすすめします。照会期間を指定することで必要なログのみ照会することができます。

ユーザーID、パスワード、OTP トークンの管理

- (1) カスタマーID、ユーザーID、パスワード、OTP トークン（OTP トークンから生成されるパスワード、チャレンジコードを入力することで生成されるレスポンスコード・取引認証コードを含みます）は、本システムをご利用されるお客さまを認証するための大切なものです。登録・取り扱い・管理には十分ご注意ください。

パスワードの取り扱いについて

パスワードを設定・変更する際は、下記の点に注意しながら行い、第三者にパスワードを知られないようにしてください。

- 1) パスワードの機密を維持する。
- 2) パスワードのメモを安全に保管している場合以外は、パスワードのメモは作らない。
- 3) パスワードは定期的に変更し、古いパスワードの再利用または使い回しは行わない。
- 4) 以下に基づいて、最低 8 文字以上の高品質なパスワードを設定する。
 - 忘れにくいパスワードにする。
 - 他の Web サイトで使っているパスワードと同じパスワードは避ける。
 - 他人が簡単に予測できたり、または個人に関する情報に基づくパスワードは避ける。
例) 名前、電話番号、誕生日等
 - 同じ文字の連続、すべて数字、すべてアルファベットのパスワードは避ける。
 - 辞書攻撃に弱い弱なパスワード（すなわち、辞書に含まれる語から成り立つもの）は避ける。
 - 個人用のパスワードを共有しない。

- (2) 各ユーザーの責任を明確化するためにも、ユーザーID、OTP トークンを他のユーザーと共有することは避けてください。
- (3) ユーザーごとの権限は、アドミニストレーターが、お客さまのご利用方法にあわせ、常に最新の設定を維持するようお願いいたします。また、異動、退職などをきっかけとした見直し、定期的な見直しをおすすめします。
- (4) 銀行からお客さまに、パスワード、OTP トークンから生成されるパスワード、チャレンジコードを入力することで生成されるレスポンスコード・取引認証コードをお伺いすることはございません。
- (5) ユーザーID、パスワード、不正使用や身に覚えのない操作が行われた疑いがある場合等、その他不審な点があれば、お取引店までお問い合わせください。
- (6) 万が一、OTP トークンを紛失された場合は、カスタマーサポートに掲載されている三菱UFJ銀行 OTP トークン紛失受付デスクまですみやかにご連絡ください。

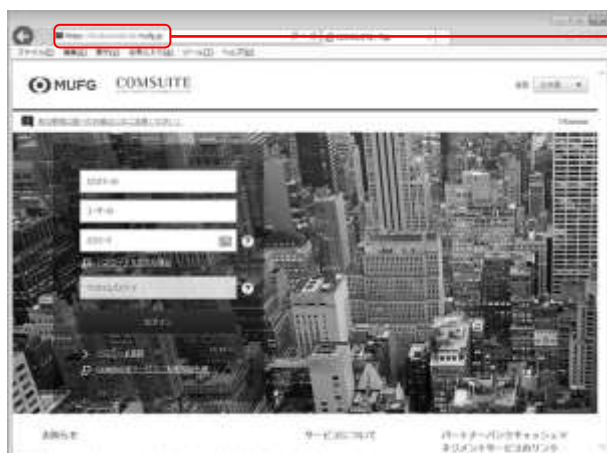
パソコン環境の管理

- (1) パソコンウィルスの感染を防ぐため、ご使用のパソコンにウィルスチェックソフトウェアをインストールすることをおすすめします。また、同ソフトウェアのパターンファイルは、常に最新のものに更新してください。
- (2) E メールをご利用の場合、送信者が不明であったり、不審な添付ファイルを受け取った場合は、それらのファイルの扱いに注意してください。
- (3) ご使用のパソコンがインターネットに接続されている場合、ハッカー・プログラムからパソコンを守るため、信頼に欠ける情報源からソフトウェアなどをダウンロードすることは控えてください。
- (4) スクリーンセーバー機能のあるパソコンなどは、スクリーンセーバーを稼働させてください。また、パスワードが設定できるものは、パスワードの設定も行ってください。
- (5) 帳票を印刷した場合は、プリンター上に放置しないことをおすすめします。

2-4 真正なサーバーであることを確認する

「フィッシング詐欺」と呼ばれる手法により、偽画面（当行の真正なサイトではない画面）を通じて利用者の ID やパスワード等を不正に取得する犯罪が発生しています。この対策として、本サービスでは、以下の方法で当行の真正なサーバーから送信された画面であることを確認することができます。

2-4-1 ブラウザのアドレスバーに表示されるアドレスを確認する



ブラウザアドレスバーに表示されるアドレスが「<https://e.ebusiness.bk.mufg.jp/>」から始まっていることを確認

2-4-2 通信先サーバーの SSL 証明書を表示して確認する

■Internet Explorer をご利用の場合

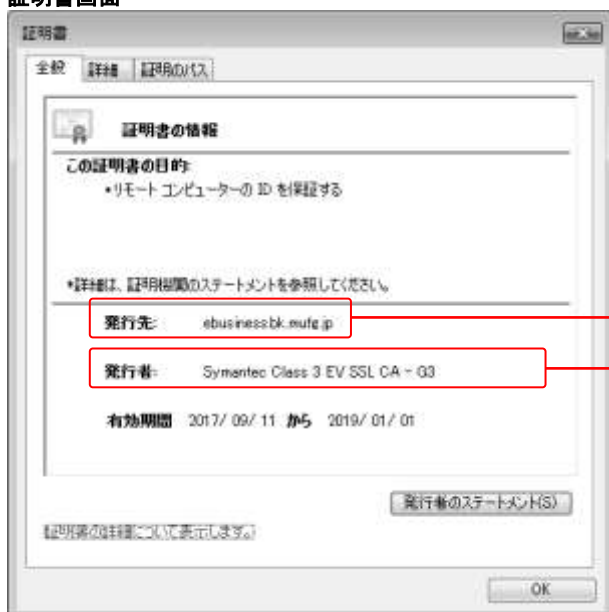
ログイン画面



アドレスバーの右に鍵アイコンが表示されていることを確認

鍵アイコンをクリック

証明書画面



証明書の内容を確認

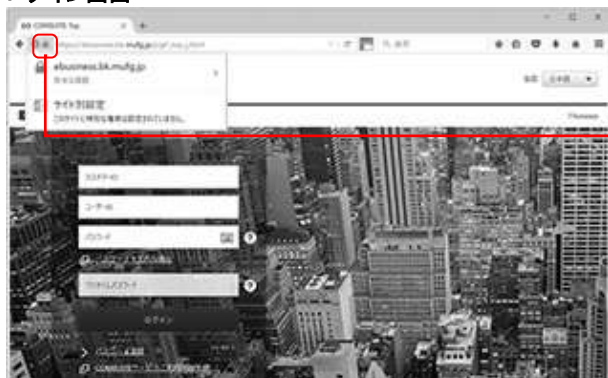
表示される「証明書」が以下の内容であれば、COMSUI TE の真正なサーバーです。

発行先: ebusiness.bk.mufg.jp

発行者: Symantec Class 3 EV SSL CA - G3

■Firefox をご利用の場合

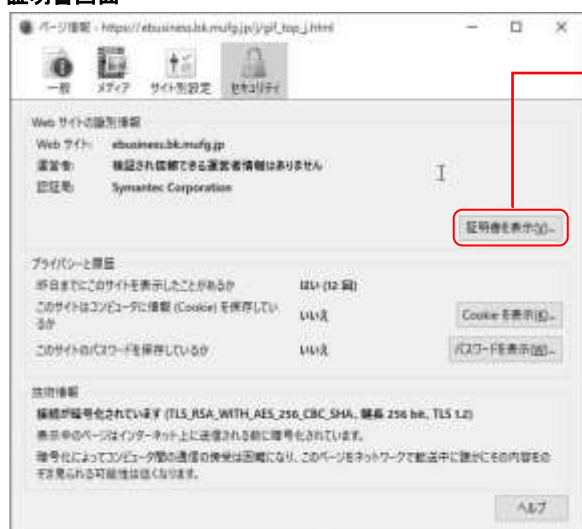
ログイン画面



アドレスバーの左に鍵アイコンが表示されていることを確認

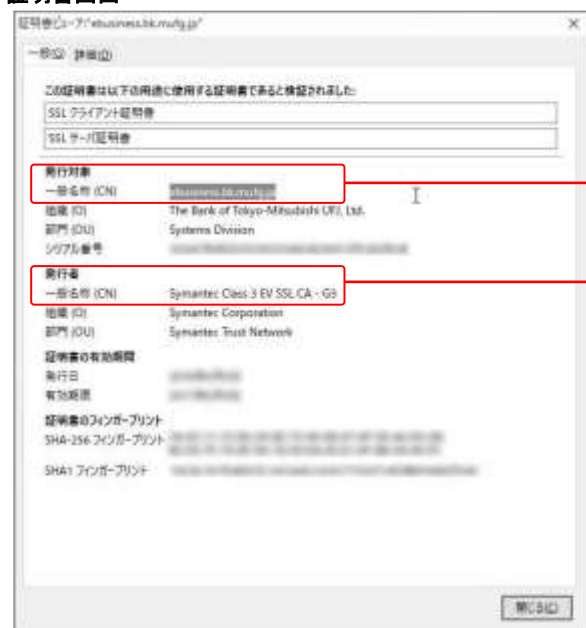
鍵アイコンをクリック

証明書画面



「証明書を表示(V)...」をクリック

証明書画面



証明書の内容を確認

表示される「証明書」が以下の内容であれば、COMSUITE の真正なサーバーです。

発行対象 一般名称(CN):
ebusiness.bk.mufig.jp

発行者 一般名称(CN):
Symantec Class 3 EV SSL
CA - G3

■Safari をご利用の場合

証明書画面



アドレスバーの左に鍵アイコンが表示されていることを確認

鍵アイコンをクリック

証明書画面



証明書の内容を確認

表示される「証明書」が以下の内容であれば、COMSUITE の真正なサーバーです。

タイトル: ebusiness.bk.mufg.jp

発行元: Symantec Class 3 EV SSL CA - G3

ご留意事項・商標

■ ご留意事項

- このクイックリファレンスは各商品の基本契約書(以下、基本契約書)にもとづき提供されています。このクイックリファレンスについては基本契約書の規定が適用されます。
- このクイックリファレンスの内容は、予告なしに変更することがありますので、ご了承ください。なお、最新版は COMSUITE ログイン画面の「カスタマーサポート」に掲載しています。
- このクイックリファレンスのご利用に際しては、機器やソフトの使用方法、制限事項などの前提条件を十分ご理解いただいた上でご活用ください。
- このクイックリファレンスの所有権は、株式会社三菱 UFJ 銀行(以下、「当行」)に帰属します。このクイックリファレンスは、基本契約書にもとづいてお客さまに貸与され、お客さま以外の第三者に貸与することはできません。
- このクイックリファレンスの著作権は、当行に帰属します。このクイックリファレンスの内容の一部または全部を複製することはできません。ただし、利用者が個人的用途に用いる場合に、1 部のみ複製することはこの限りではありません。

■ 商標

- COMSUITE、GCMS Plus は、株式会社三菱 UFJ 銀行の日本およびその他の国における登録商標または商標です。
- 本文中では、「Microsoft® Windows® Operating System」のことを単に「Windows」と記述しています。Microsoft、Windows、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。
- Safari は、米国および他の国々で登録された Apple Inc.の商標です。
- Firefox、Firefox ロゴは、米国 Mozilla Foundation の米国およびその他の国における商標または登録商標です。
- Symantec は、Symantec Corporation の米国およびその他の国における商標または登録商標です。
- その他、記載されている会社名、製品名は、各社の登録商標または商標です。
- 本文中には、™および®等の商標マークを明記していません。