

# セキュアスマートアクセス

MCOP（ワンタイムパスワード）認証  
ソフトウェアトークン方式

Windows 端末 操作マニュアル

- 第 1.3 版 -



## 目次

1.	はじめに .....	3
2.	本サービスを使用するための要件 .....	7
3.	Step.1 初期設定 .....	13
4.	Step.2 本サービスへの接続 .....	20
5.	Step.3 本サービスからの切断 .....	26
6.	トラブルシューティング .....	28



## セキュアスマートアクセス

### 1. はじめに

1.1.	本書の目的 .....	4
1.2.	本書の対象者 .....	4
1.3.	利用までの流れ.....	4

## 第 1 章 はじめに

### 1.1. 本書の目的

本書は、SSA オプション「セキュアスマートアクセス」サービス(以降、本サービスと記載)を利用するための手順書です。

### 1.2. 本書の対象者

本サービスを契約した企業管理者にて、認証基盤に登録されたユーザ(端末)が対象です。

### 1.3. 利用までの流れ

本サービスは、Windows 端末から SSL-VPN トンネル(通信を SSL にて暗号化)を通じて、社内ネットワークなどに接続するためのサービスです。また、本サービスを利用するには、企業管理者が認証基盤にユーザを登録した後、通知されるメールが必要となります。利用までのおおまかな流れを下記に示します。

表 1 利用までの流れ

項目	概要
認証基盤にユーザ情報を登録	本サービスを利用するために、認証基盤へユーザ情報を登録します。この作業は企業管理者が行います。
Step.1 初期設定	認証基盤から通知されるメールを使用し、パスワード(端末)を登録します。
Step.2 接続	ブラウザを起動し、ユーザ(端末)認証を行います。 認証後、SSL-VPN トンネルが確立されます。 ※以降、本書では上記動作を「SSL-VPN 接続」と記載します。
Step.3 切断	アプリを終了し、SSL-VPN トンネルを切断します。

本サービスをはじめて利用する場合、Step.1 までの作業を行った後、Step.2～3 で本サービスがご利用出来ます。2 回目以降の場合、Step.2～3 で本サービスがご利用出来ます。

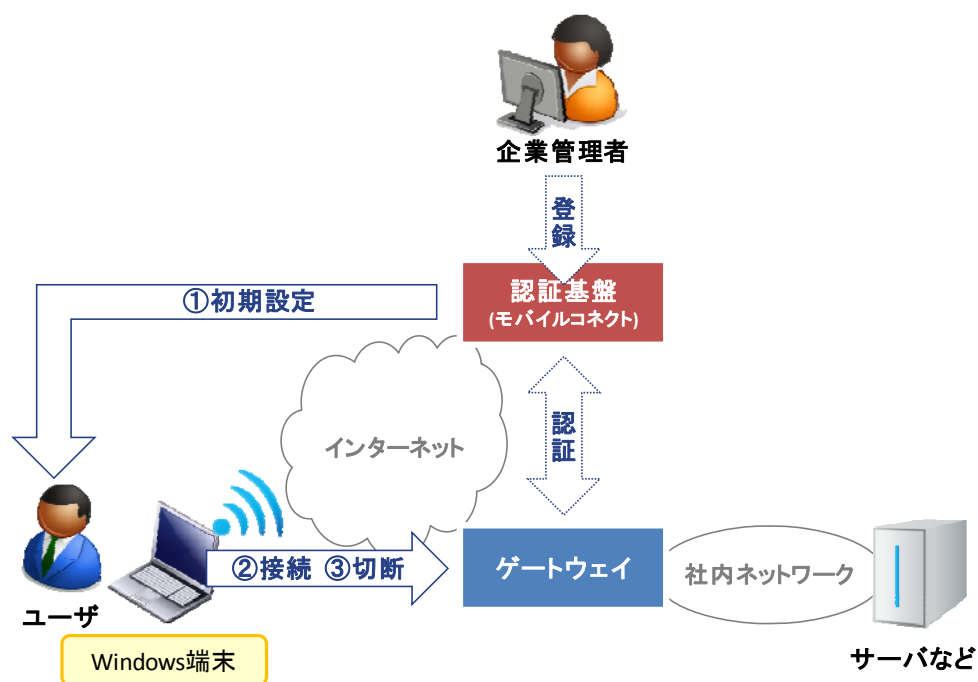


図 1 利用までの流れ

## 第 1 章 はじめに

### 1.4. 画面の名称について

本書で画面操作の説明を行う際、下記の名称を使用します。

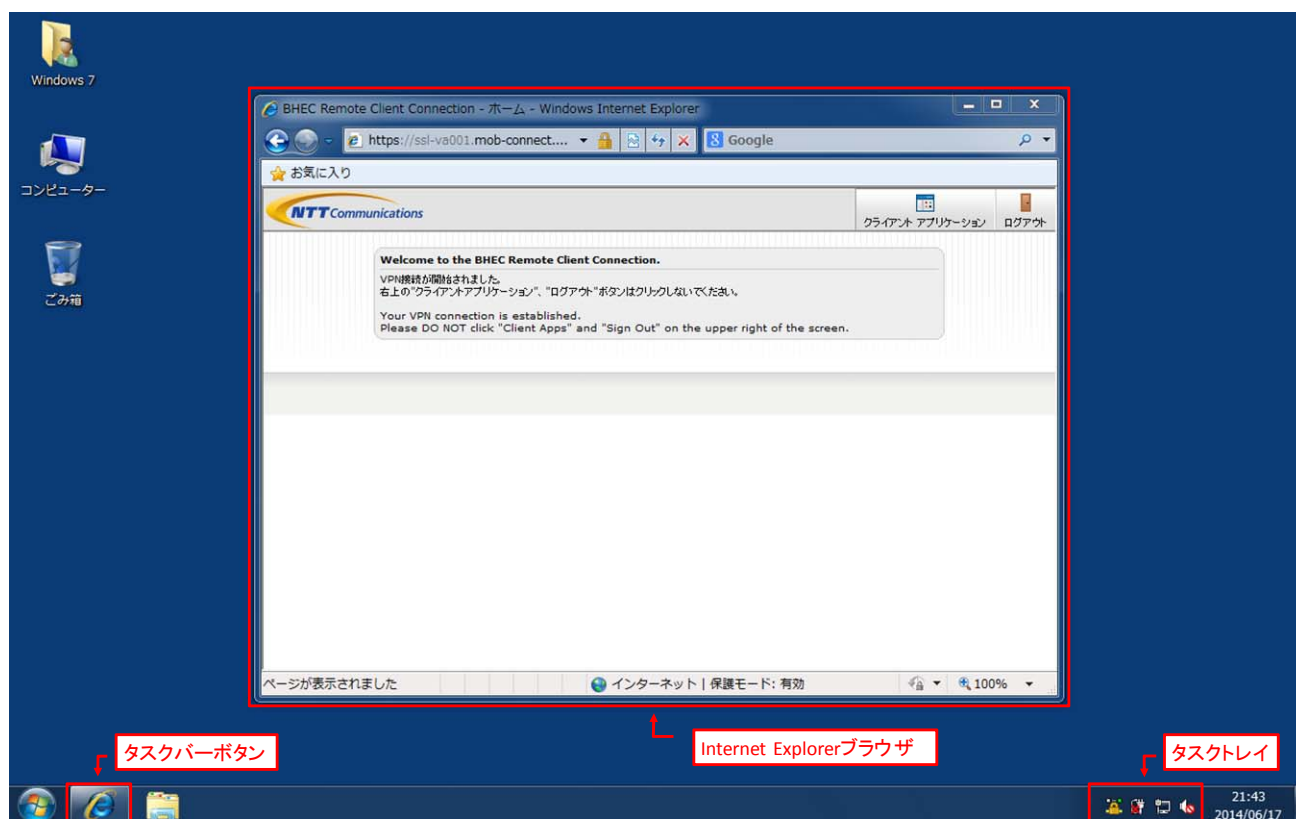


図 2 Windows 7 の画面名称

### 本書で掲載されている画面について

掲示されている画面は、操作手順を伝えるものであり、実際に表示される画面とは異なる可能性があります。

## セキュアスマートアクセス

### 2. 本サービスを使用するための要件

2.1.	端末 .....	8
2.2.	ネットワーク環境 .....	9
2.3.	ブラウザ設定 .....	9
2.4.	認証ポリシー .....	12

## 第 2 章 本サービスを使用するための要件

### 2.1. 端末

(1) 本サービスは、下記 Windows 端末での動作をサポートしています。

- ※ 下記では Microsoft 社で各 OS 毎にサポート対象としている最新ブラウザのみ記載しています。  
 下記以外のブラウザでも、Microsoft 社のサポートする 32bit の標準ブラウザ以上であればサポート対象に含まれます。なお、**64bit ブラウザはサポート対象にふくまれておりません。**

表 2 サポート Windows OS／ブラウザー一覧

OS	ブラウザ
Windows 7 SP1(32/64bit)	Internet Explorer 11
Windows 8.1(32/64bit)	Internet Explorer 11
Windows 10(32/64bit)	Internet Explorer 11

(2) 本サービスを使用する Windows 端末に SSL-VPN を行うためのプログラムがインストール、実行されます。このため、**ログインユーザは管理者権限である必要があります。**

(3) 本サービスに接続した際、下記アプリケーションがインストールされます。なお、申し込み内容、環境によっては、インストールされないアプリケーションがあります。

表 3 インストールアプリケーション一覧

アプリケーション	記載
JuniperSetupClientControl Class	Juniper 用 ActiveX
Juniper Networks, Inc. Setup Client	セットアップクライアント
Juniper Networks Network Connect x.x.x	ネットワークコネク、NC

(4) SSL-VPN 接続の際、Windows 端末の hosts ファイルにゲートウェイの FQDN、IP アドレスが追記される場合があります。

#### hosts ファイルの変更について

hosts ファイルが変更される際、ウィルス対策ソフトなどがファームウェアの防止として、hosts ファイルの変更が阻害される場合があります。阻害された場合、環境によってはポータル画面等が正しく表示されない場合や、SSL-VPN 接続が切断されるなどの問題が発生する可能性があります。



## 第 2 章 本サービスを使用するための要件

### 2.2. ネットワーク環境

- (1) 本サービスを使用するには、インターネットに接続されている必要があります。
- (2) 端末から SSL-VPN 接続を行うゲートウェイまでの通信区間で、SSL 通信および、Proxy 等で SSL-VPN 通信を阻害されずに通信できる必要があります。

### 2.3. ブラウザ設定

- (1) ブラウザの詳細設定で TLS 1.0 が使用できるよう、設定されている必要があります。

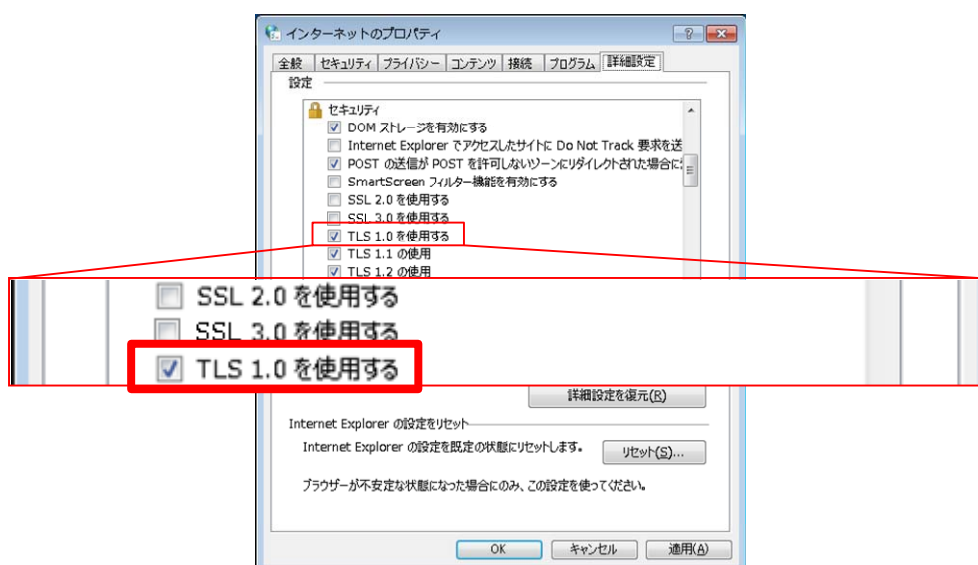


図 3 SSL の設定

(2) インターネットゾーンの ActiveX コントロールとプラグイン設定値が、ActiveX のダウンロード、インストール、実行が行える必要があります。※標準設定になっている

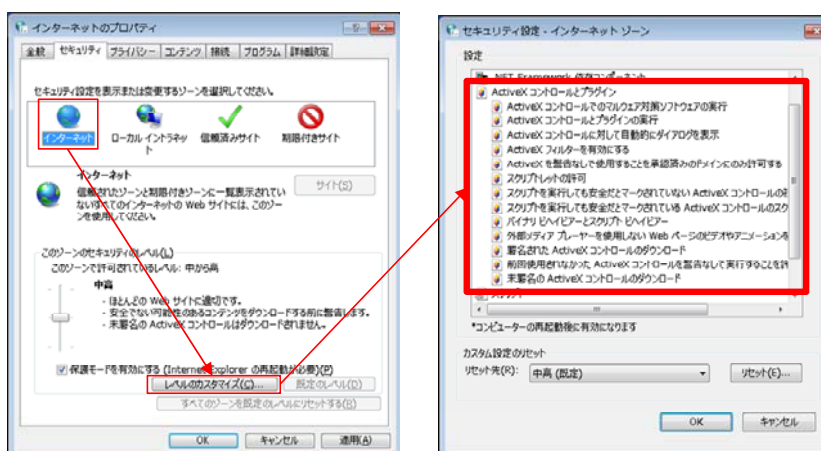


図 4 ActiveX の設定

表 4 ActiveX の設定詳細

項目	設定値
ActiveX コントロールでのマルウェア対策ソフトウェアの実行	有効
ActiveX コントロールとプラグインの実行	有効
ActiveX コントロールに対して自動的にダイアログを表示	無効
ActiveX フィルターを有効にする	有効
ActiveX を警告なしで使用することを承認済みのドメインにのみ許可する	有効
スクリプトレットの許可	無効
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	無効
スクリプトを実行しても安全だとマークされている ActiveX コントロールのスクリプトの実行	有効
バイナリビヘイビアとスクリプトビヘイビア	有効
外部メディアプレーヤーを使用しない Web ページのビデオやアニメーションを表示する	無効
署名された ActiveX コントロールのダウンロード	ダイアログ
前回使用されなかった ActiveX コントロールを警告なしで実行するのを許可する	無効
未署名の ActiveX コントロールのダウンロード	無効

## 第 2 章 本サービスを使用するための要件

(3) InPrivate ブラウズが無効になっている必要があります。

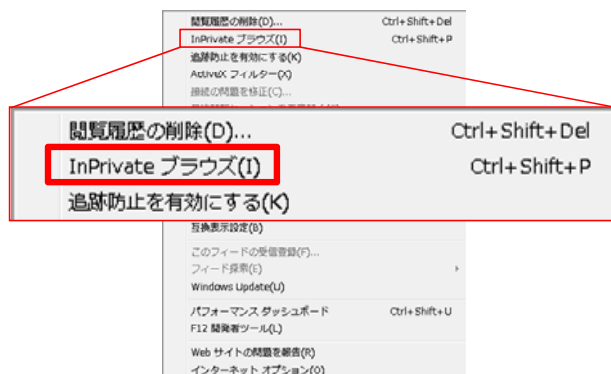


図 5 InPrivate ブラウズの設定

### InPrivate ブラウズ 無効



### InPrivate ブラウズ 有効



図 6 InPrivate ブラウズの無効、有効状態の画面差異

## ブラウザ設定に関する注意

ブラウザ設定は本サービスを使用するための設定です。ブラウザ設定の変更についてはセキュリティポリシーに関係するため詳細は企業管理者にお問い合わせ下さい。

### 2.4. 認証ポリシー

- (1) ユーザ(端末)認証は、MC アプリより行います。この際、登録したモバイルコネクタイムパスワード(以降、MCOP と記載)は 120 日間有効です。  
※有効期限を超過した場合、次回アクセス時にパスワード変更画面に遷移します
- (2) MCOP パスワードは 8 文字以上、15 字以内で設定してください。また、MCOP パスワードには、固定数字を 4 文字まで登録することが可能です。
- (3) 5 回連続して認証を失敗した場合、ユーザアカウントがロックされ、企業管理者がロックを解除するまで、本サービスを使用することは出来ません。

## セキュアスマートアクセス

### 3. Step.1 初期設定

3.1.	認証方式について .....	14
3.2.	MCOP 認証について .....	15
3.3.	MCOP 認証 .....	16

### 3.1. 認証方式について

SSA サービスの認証方式のうち、ソフトウェアトークンによるワンタイムパスワード方式 MCOP 認証方式について記載しています。

#### (1) MCOP 認証

ユーザ ID と MCOP で認証を行う方式。エヌ・ティ・ティ・コミュニケーションズが開発した、ワンタイムパスワードです。表示される乱数の中から「位置」と「順番」をあらかじめ登録しておき、認証時に送信するパスワード情報が毎回異なる認証方式です。

認証方式方式につきましては、契約によるものです。

## 第3章 Step.1 初期設定

### 3.2. MCOP 認証について

MCOP 認証画面に表示される乱数の中から「位置」と「順番」を登録し、認証情報として使用します。乱数は、毎回変更されるため、入力した MCOP パスワード情報が第三者に知られても「位置」と「順番」情報が漏洩しない高セキュリティの認証方式です。

例)

MCOP パスワードを左上から 4 つずつ、中列 2 段目左から 4 つずつ登録した場合。



図 7 登録した MCOP パスワード情報

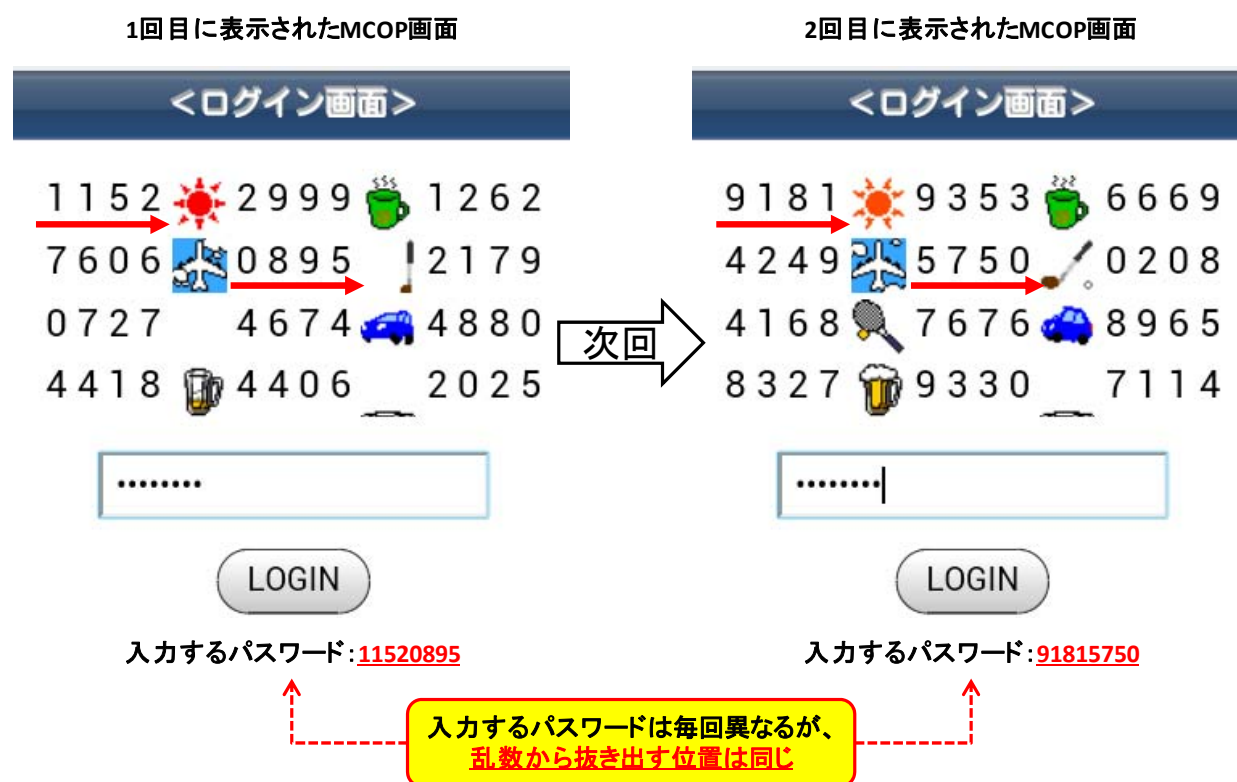
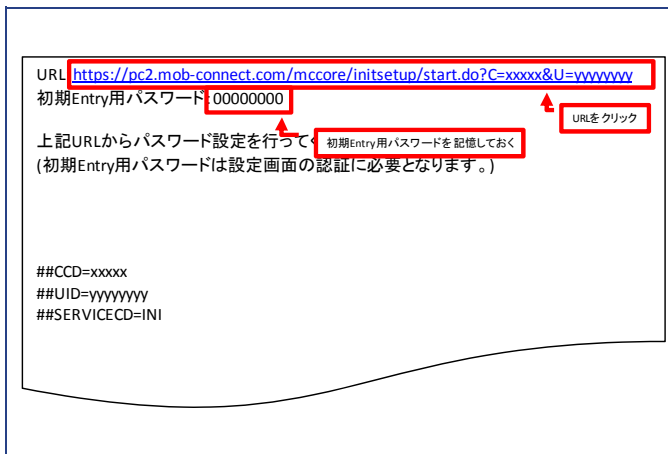


図 8 MCOP パスワード入力例

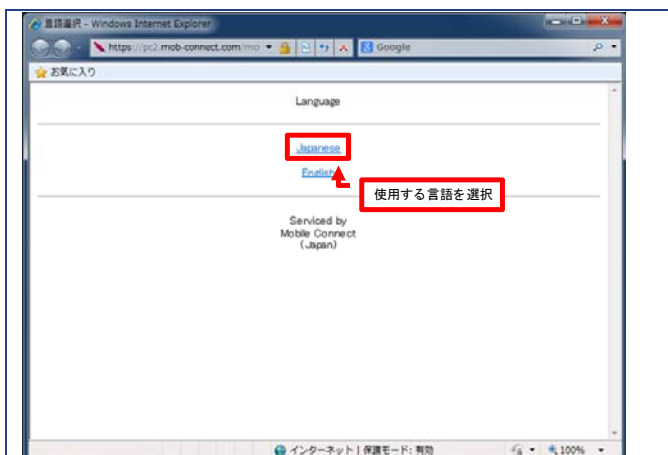
## 第3章 Step.1 初期設定

### 3.3. MCOP 認証

#### (1) 初期設定メールの確認

 <p>URL <a href="https://pc2.mob-connect.com/mccore/initsetup/start.do?C=xxxxx&amp;U=yyyyyy">https://pc2.mob-connect.com/mccore/initsetup/start.do?C=xxxxx&amp;U=yyyyyy</a></p> <p>初期Entry用パスワード 00000000</p> <p>上記URLからパスワード設定を行って、初期Entry用パスワードを記憶しておく (初期Entry用パスワードは設定画面の認証に必要となります。)</p> <p>##CCD=xxxxx ##UID=yyyyyy ##SERVICECD=INI</p>	<p>初期設定メールに記載されている URL にアクセスします。</p>
--	--------------------------------------

#### (2) 使用言語の選択

	<p>起動されたブラウザから使用する言語をクリックします。</p>
--	-----------------------------------

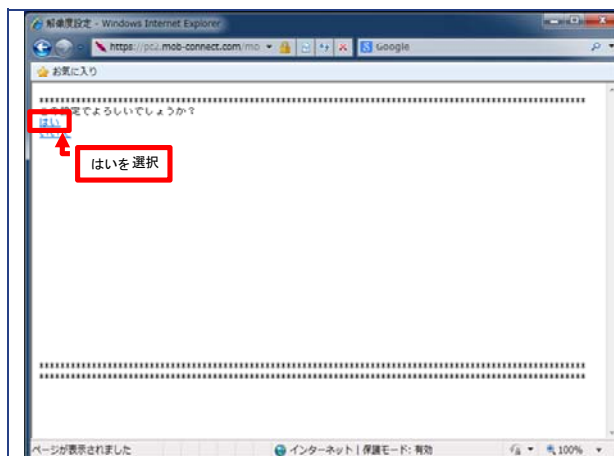
#### (3) 解像度の選択

	<p>解像度をクリックします。</p>
---	---------------------



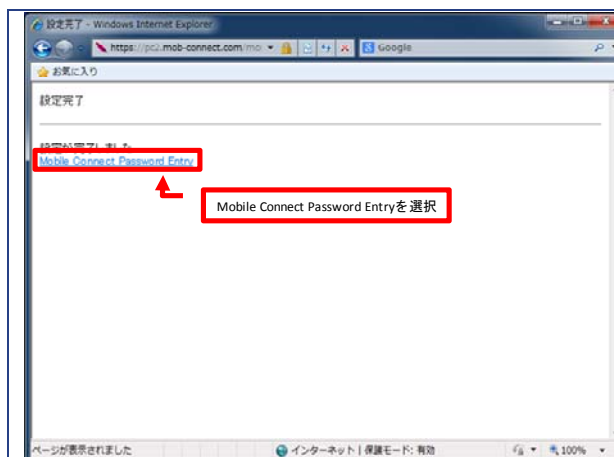
## 第3章 Step.1 初期設定

### (4) 設定の確認



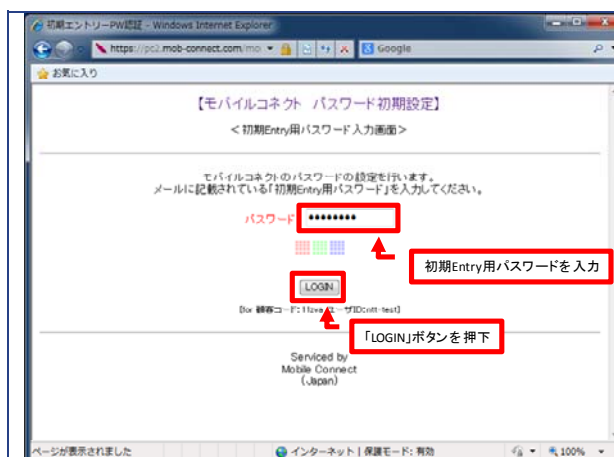
テキストが画面内に表示されることを確認し、「はい」をクリックします。

### (5) 画面設定完了



画面設定が完了しました。続いてパスワード設定を行います。

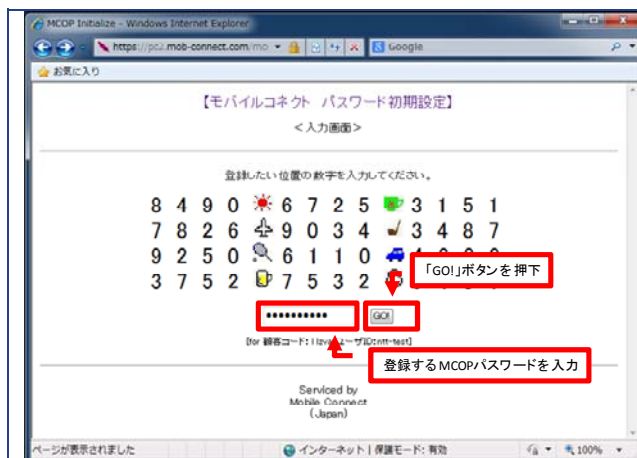
### (6) 初期 Entry 用パスワード入力



メールに記載されていた初期 Entry パスワードを入力し、「LOGIN」ボタンを押下します。

### 第3章 Step.1 初期設定

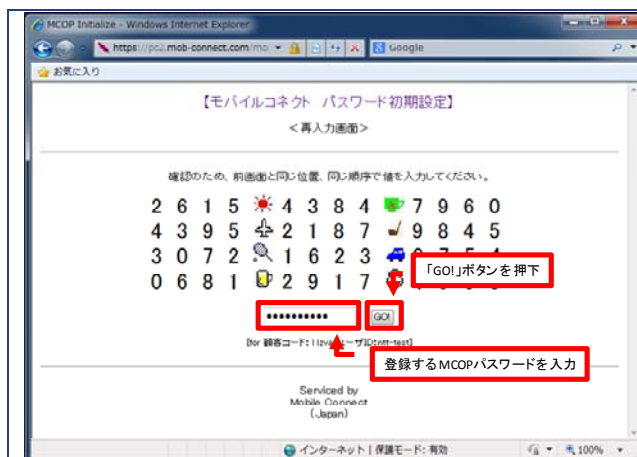
#### (7) MCOP パスワードの登録(1 回目)



MCOP パスワードに設定する位置  
に表示されている数字を順番に入  
力します。

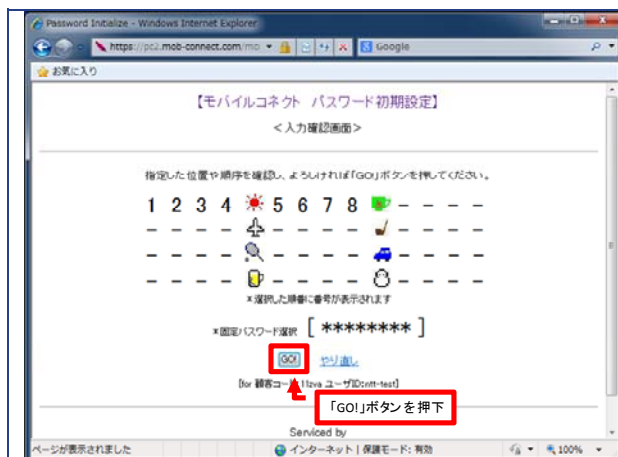
※「3.2MCOP 認証について」を  
参照

#### (8) MCOP パスワードの登録(2 回目)



MCOP パスワードを確定させるた  
め、再度 MCOP パスワードに設定  
する位置に表示されている数字を  
順番に入力します。

#### (9) MCOP パスワードの確認



表示された MCOP パスワードが  
正しいことを確認し、「GO!」ボタ  
ンを押下します。

### 第3章 Step.1 初期設定

#### (10) MCOP パスワード設定終了



ブラウザを閉じて下さい。

以上で MCOP パスワードの初期設定は完了です。

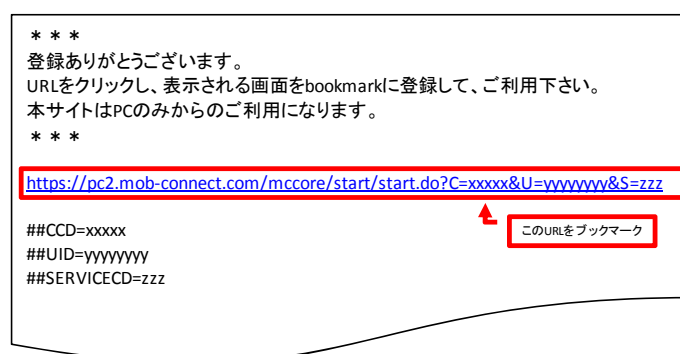
## セキュアスマートアクセス

### 4. Step.2 本サービスへの接続

#### 4.1. 接続 ..... 21

#### 本サービスへの接続方法について

本サービスはブラウザから特定の URL にアクセスして接続します。このため、本サービスを利用する特定の URL をブックマーク等に登録することを推奨します。



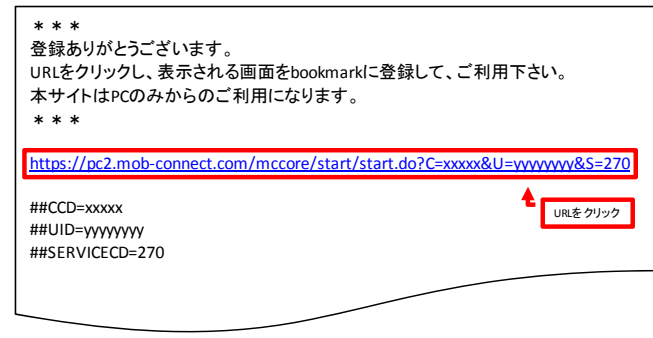
#### 初回接続と 2 回目以降の接続について

本サービスに接続した際、ActiveX、プログラムのダウンロード、インストール、実行が行われます。  
2 回目以降の接続では、ActiveX、プログラムが自動で実行されます。

## 第 4 章 Step.2 本サービスへの接続

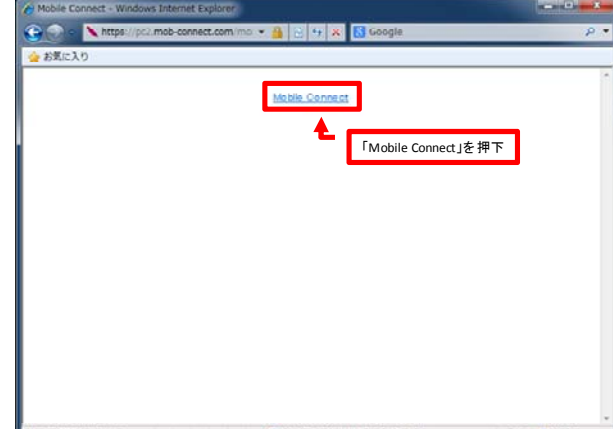
### 4.1. 接続

#### (1) 利用開始 URL へアクセス




利用開始メールに記載されている URL にアクセスします。

#### (2) Mobile Connect への接続



「Mobile Connect」を押下します。

#### (3) 認証の実行

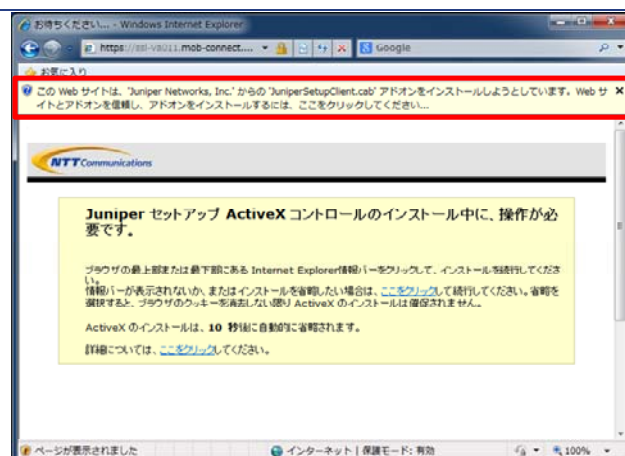


登録した MCOP パスワードを入力し、「Login」をクリックします。

## 第 4 章 Step.2 本サービスへの接続

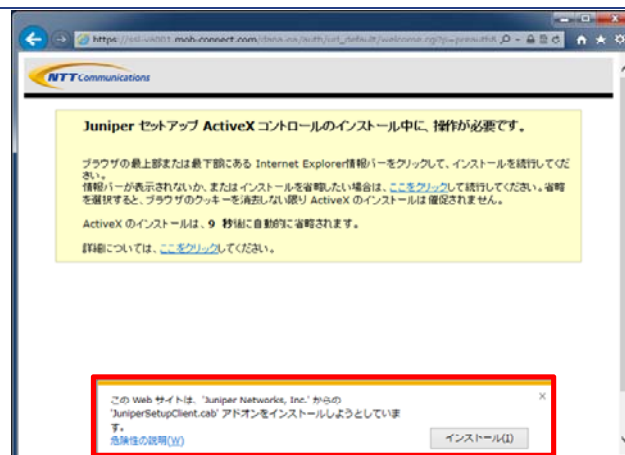
### (4) ActiveX のインストール(初回のみ)

#### 「Internet Explorer 8」での表示



ブラウザ上部に表示されるイエローバーをクリックし、ActiveX をインストールする。

#### 「Internet Explorer 9 / 10」での表示



ブラウザ下部に表示されるイエローバーをクリックし、ActiveX をインストールする。

## プログラムのインストールについて

本サービスは、ブラウザからプログラムをダウンロード、インストール、実行します。この際、**ログインしているユーザ権限は管理者権限**である必要があります。また、下記ウィンドウが表示された場合、指示に従いプログラムのダウンロード、インストール、実行を行って下さい。

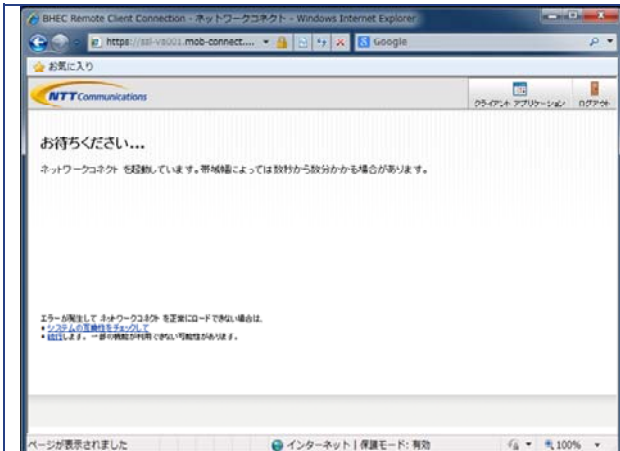
## 管理者権限が必要なプログラムのインストール



「はい」ボタンを押下して下さい。

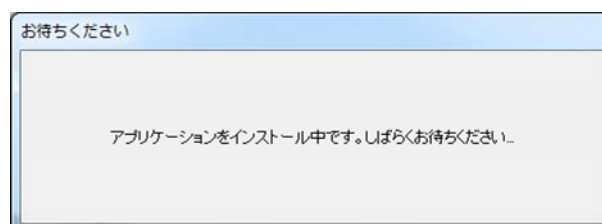
## 第4章 Step.2 本サービスへの接続

### (5) NC のダウンロード、インストール、実行

	<p>プログラムが自動でダウンロード、インストール、実行されます。</p>
---	---------------------------------------

### 表示されるウィンドウについて

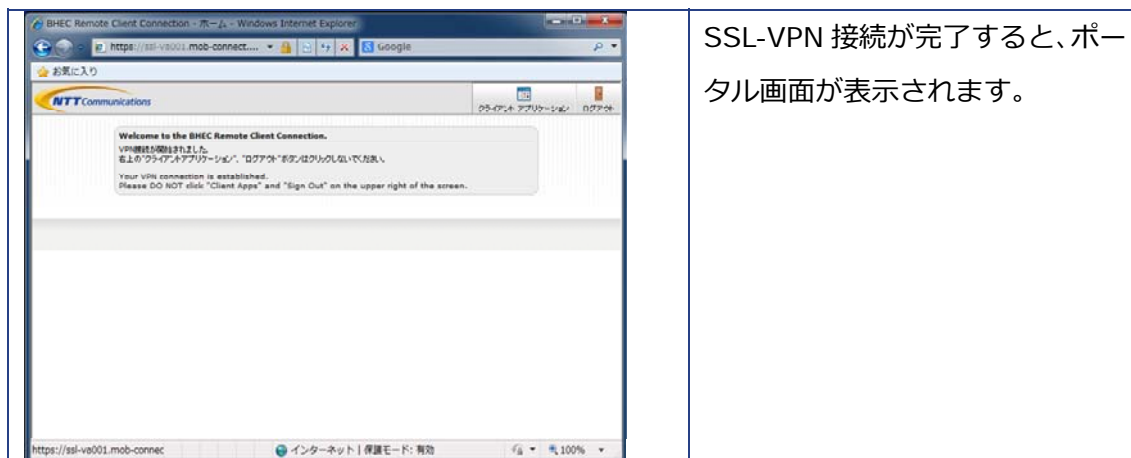
プログラムをダウンロード、インストール、実行する際、下記のようなプログラムのウィンドウが表示されますが、**すべて自動で処理されるため、操作しないで下さい。**





## 第 4 章 Step.2 本サービスへの接続

### (6) SSL-VPN 接続完了



以上で本サービスへの接続は完了です。

### タスクトレイに表示されるアイコンについて

SSL-VPN 接続が完了すると、タスクトレイに下記アイコンが表示されます。正常に接続出来ている場合、オレンジ色で表示されます。また、通信中はランプが緑色に点灯します。



図 9 タスクトレイに表示されるアイコン

## セキュアスマートアクセス

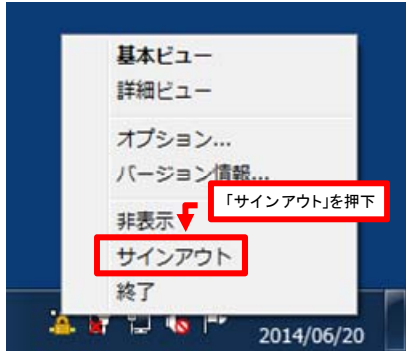
### 5. Step.3 本サービスからの切断

5.1. 切断 .....	27
---------------	----

## 第 5 章 Step.3 本サービスからの切断

### 5.1. 切断

#### (1) MC アプリの起動

	<p>タスクトレイのネットワーク接続アイコンを右クリックし、「サインアウト」を押下します。</p>
---	---

以上で本サービスへの接続は切断されます。

## セキュアスマートアクセス

### 6. トラブルシューティング

6.1.	代表的なトラブルとトラブルシューティング .....	29
6.1.1.	ログインできない。 .....	29
6.1.2.	正しい ID、パスワードで認証しても、認証に失敗する。 .....	29
6.2.	端末に依存したトラブルとトラブルシューティング .....	30
6.2.1.	SSL-VPN 接続が完了するまで時間がかかる。 .....	30
6.2.2.	SSL-VPN 接続できない .....	31

## 第 6 章 トラブルシューティング

### 6.1. 代表的なトラブルとトラブルシューティング

#### 6.1.1. ログインできない。

認証に失敗した場合、認証エラー画面が表示されます。ブラウザを閉じ、再度アクセスして下さい。

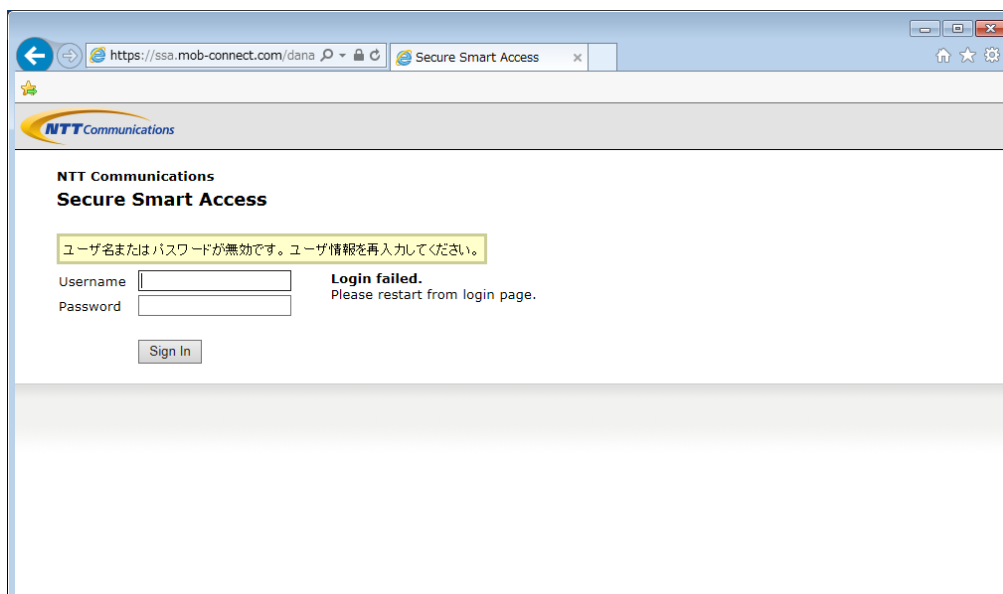


図 8 ログインエラー画面

#### 6.1.2. 正しい ID、パスワードで認証しても、認証に失敗する。

以前に「認証に失敗した」情報がブラウザにキャッシュされている可能性があります。ブラウザを閉じた後、キャッシュを削除し、再度アクセスして下さい。

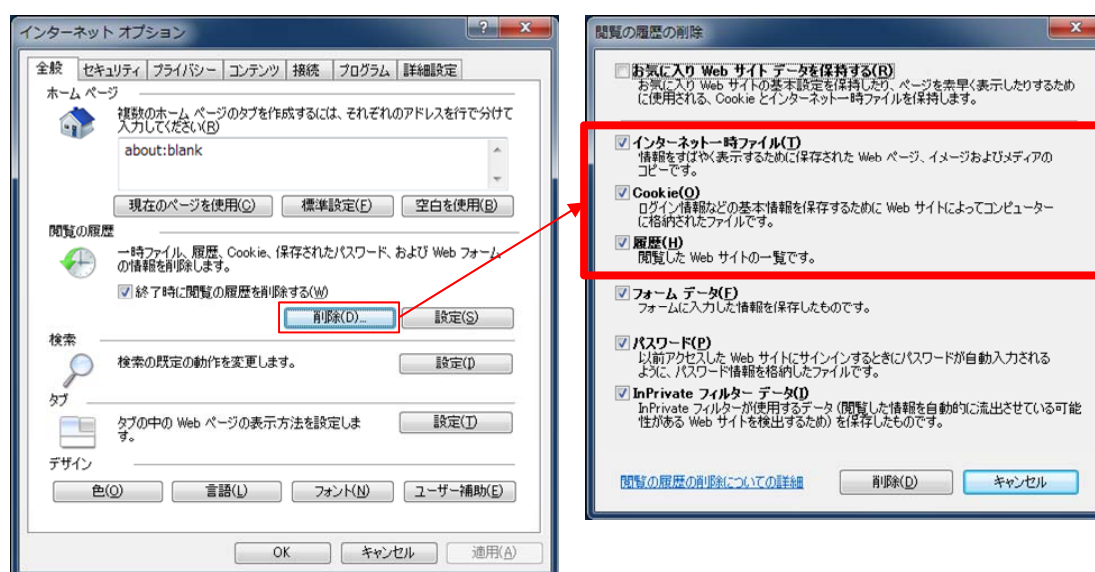


図 9 ブラウザのキャッシュ削除

## 6.2. 端末に依存したトラブルとトラブルシューティング

## 6.2.1. SSL-VPN 接続が完了するまで時間がかかる。

## 【ケース①】

データ通信端末(USB 型のダイヤルアップアダプターなど)を使用した接続方式の場合、SSL-VPN 接続が完了するまで時間がかかることがあります。この場合、データ通信端末のドライバを最新版にアップデートすることで、事象が改善されたケースがあります。

表 5 過去に改善の報告があった端末一覧

メーカー	端末
HUAWEI	HWD12

## 【ケース②】

スマートデバイス(iOS 端末、Android 端末など)を使用した USB テザリング接続方式の場合、SSL-VPN 接続が完了するまで時間がかかることがあります。この場合、USB テザリング接続方式から WiFi テザリング接続方式等に変更することで、事象が改善されたケースがあります。

## 【ケース③】

接続元の国、地域や施設などの制限により、SSL-VPN 接続が完了するまで時間がかかる、もしくは SSL-VPN 接続ができないことがあります。この場合、施設などの管理者に相談いただく、接続元の国、地域を変更することで、事象が改善されたケースがあります。

## 第 6 章 トラブルシューティング

### 6.2.2. SSL-VPN 接続できない

#### 【ケース①】

端末にインストールされているソフトウェアの干渉により、SSL-VPN 接続ができないことがあります。この場合、下記ソフトウェアをアンインストールすることで、事象が改善されたケースがあります。

表 6 干渉の可能性があるソフトウェア一覧

カテゴリー	例
通信データを圧縮、動的 IP を割り振る	MEGA PLUS 等キャリアサービス Venturi Client 等
ファイル共有ソフト	Limewire 等
他社製 VPN	Cisco VPN Client 等
ウィルス対策、クライアントファイアウォール	BlackICE CheckPoint Integrity Agent 5.1 CheckPoint Secure Remote IPsec client Escan Antivirus Kaspersky AV Kerio Personal Firewall McAfee Privacy Suite ウィルスセキュリティ ZERO
その他	Bonjour Service(Apple 社) MyMedia(富士通社) iPass 認証ソフト(iPass 社) ビジネスパケットカウンタ(KDDI 社) PPPoE ダイアルアップソフト等

#### 【ケース②】

SSL-VPN 接続に使用するネットワークアダプタに適用されているドライバとの干渉により、SSL-VPN 接続ができないことがあります。この場合、下記ドライバを無効化することで、事象が改善されたケースがあります。

表 7 干渉の可能性があるドライバー一覧

ネットワークアダプタ	ドライバ
Juniper Network Connect Virtual Adapter	Deterministic Network Enhancer パケット スケジューラ ミニポート

### 【ケース②】

端末にインストールされている無線 LAN ソフトウェアの設定で、「有線 LAN に接続すると自動的に無線 LAN を切断する」旨の設定がある場合、SSL-VPN 接続ができないことがあります。この場合、設定を無効にすることで、事象が改善されたケースがあります。

表 8   設定問題の可能性のあるソフトウェア一覧

メーカー	ソフトウェア
ソニー社	Smart Network
東芝社	ConfigFree
富士通社	Plugfree NETWORK
パナソニック社	ネットセレクター2
インテル社	PROSet/Wireless WiFi
B・Stream	ConnectPartner