

開発環境リモートアクセス利用案内書

(開発パートナー様向け)

1.1 版

本書の閲覧範囲:
開発パートナー様限り

2020 年 4 月 15 日 発行
KDDI 株式会社
技術統括本部 情報システム本部

KDDI CONFIDENTIAL PROPRIETARY
Copyright© 2020 KDDI CORPORATION, All Rights Reserved.

改版履歴

No.	日付	項 No.	区分	変更内容	Ver	備考	更新
1	2020/4/14		初版	初版作成	1.0	接続テスト	
2	2020/4/15		1.1 版	接続テスト結果より、各補足追記	1.1	パートナー展開初版	
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							
27							
28							
29							
30							

目次

1. 概要.....	3
1.1. 目的.....	3
1.2. 実現構成.....	3
2. 提供条件・順守事項.....	4
2.1. PC 側の制約事項.....	4
2.1.1. 共通	4
2.2. 利用における順守事項	4
2.2.1. 共通	4
2.3. 接続方法について	5
2.3.1. VPN ソフトインストールおよび設定	5
2.3.2. AWS 及び開拠点 PC へのリモート接続.....	5
2.4. 情報共有サイトについて.....	10

新型コロナウイルス拡大による「開発拠点閉鎖」「外出危険」「駆け付け不可」等の状態に陥った場合であっても、開発パートナーが在宅環境(※)から遠隔での開発業務の円滑な遂行を実現します。

※自宅、もしくは開発パートナー各社が別途用意する拠点

開発環境へは AWS 経由にてアクセスする構成となります。



2. 提供条件・順守事項

2.1. PC 側の制約事項

2.1.1. 共通

リモート元 PC	項目	推奨環境
	ハード	メモリは 4GB 以上を推奨。 ※2GB 以下だと、 スワップの発生により描画に影響が出る可能性あり。
	ネットワーク	有線接続を推奨。WiFi の場合は、WiFi ルーターからなるべく近い場所。 以下の速度確認サイトでの確認で、20Mbps 以上が安定的に出ている環境 インターネット回線の速度確認サイト https://fast.com/ja/

・複数人での同一 PC 利用不可、1 人での複数デバイス利用不可とします。



	環境	利用に必要な条件				
リモート元 PC (私有 PC or 社有 PC)	ハード	家族共有の PC ではない				
		Windows 8.1 / Windows 10(1809 以降のビルド)/Mac OS(10.13 以降のビルド)が利用可能 ※ Windows 7 SP1 / Windows 10(1803 以前のビルド)/ macOS(10.12 以前のビルド)はサポート対象外				
		下表で「○」となっているウイルス対策ソフトがインストールされている。				
				Windows8.1	Windows10 (1809 以降)	macOS (10.13 以降)
		有償 ソフト	ウイルスバスタークラウド	○	○	×
			ESET インターネットセキュリティ	○	○	×
			カスペルスキーセキュリティ	○	○	×
		無償 ソフト	Windows Defender	×	○	—
			Avira Free Antivirus	○	○	×
			Avast アンチウイルス	○	○	○
AVG 無料アンチウイルス	○		○	○		
最新のセキュリティパッチが適用されている						
P2P ソフト(Winny などのファイル共有ソフト等)がインストールされていない						

2.2. 利用における順守事項

2.2.1. 共通

- ・ 自宅 PC は自宅内、もしくは開発パートナー各社が別途用意する拠点から持ち出し・移動不可とする。
拠点設定の場合はワイヤーロックで施錠すること。
- ・ リモートアクセス終了時、リモートアクセス先 PC は必ずログオフすること。
(ログイン状態のまま終了、**リモートアクセス先 PC シャットダウンは実施しないこと。**)
- ・ 1 台の自宅 PC から商用リモートと開発リモートの同時接続は実施しないこと。
(商用リモート者と開発リモート者を役割分担してそれぞれ接続は可能)

自宅よりリモートアクセスを利用する場合の通信費や電気代は利用者個人あるいは開発パートナー各社にて負担を行うものとする。

- ・ 個人で所有している無線通信機器(Wi-Fi ルーター等)にてリモートアクセスを行う場合、無線通信機器利用にかかるすべての費用は利用者個人あるいは開発パートナー各社にて行うものとする。

2.3. 接続方法について

2.3.1. VPN ソフトインストールおよび設定

1. 接続元 PC に VPN ソフトをダウンロード、インストールして下さい。
(以下当社にて接続検証済みとなります)
WindowsOS 利用の場合は「<http://www.openvpn.jp>」より「OpenVPN」を入手して下さい。
MacOS 利用の場合は「<https://tunnelblick.net>」より「Tunnelblick」を入手して下さい。
2. 「別紙. client-vpn-user-guide.pdf」を参照のうえ、当社構築の「AWS Client VPN」に接続して下さい。
 - ✓ 「設定ファイル(.ovpn)」、「クライアント証明書(.cert)」、「証明書秘密鍵(.key)」は当社より提示させて頂きます。(接続元 PC 内でのファイル設置パスは任意で構いません)
 - ✓ VPN ソフト起動時に表示される警告メッセージ等は無視(全て OK)して頂いて問題ありません。
 - ✓ 「設定ファイル(.ovpn)」をクライアントソフトで import する前に以下を必ず実施して下さい。
 - ✓ **AWS への VPN 接続が確認できたのち、当社提示の「設定ファイル(.ovpn)」、「クライアント証明書(.cert)」、「証明書秘密鍵(.key)」は接続元 PC より必ず削除して下さい。(ゴミ箱内含む)**

1. テキストエディタにて「設定ファイル(.ovpn)」を開く。
2. 設定ファイル(.ovpn)末尾に「クライアント証明書(.cert)」、「証明書暗号鍵(.key)」の記載を追記し保存

```
<cert>
※以下「クライアント証明書(.cert)」の記載
Certificate:
XXXXXXXXXXXXXX
XXXXXXXXXXXXXX
-----END CERTIFICATE-----
</cert>

<key>
※以下「証明書暗号鍵(.key)」の記載
-----BEGIN PRIVATE KEY-----
XXXXXXXXXXXXXX
XXXXXXXXXXXXXX
-----END PRIVATE KEY-----
</key>
```

2.3.2. AWS 及び開拠点 PC へのリモート接続

1. 接続元 PC からリモートデスクトップ接続を起動し、接続先 IP アドレスとして以下を指定して下さい。
(ログイン ID、PW は当社より提示させて頂いた情報をご利用下さい)

AWS ログイン ID の数字が**奇数**の方は、「**192.168.1.100**」

AWS ログイン ID の数字が**偶数**の方は、「**192.168.2.100**」

※AWS へリモートデスクトップ接続する際の **ID は「@」以降のドメインも含めて入力して下さい。**

※AWS へリモートデスクトップ接続する際の **パスワードは各利用者様にて任意に変更できません。**

KDDI にて定期的に変更する運用となりますので、**KDDI にて変更時は別途周知させて頂きます。**

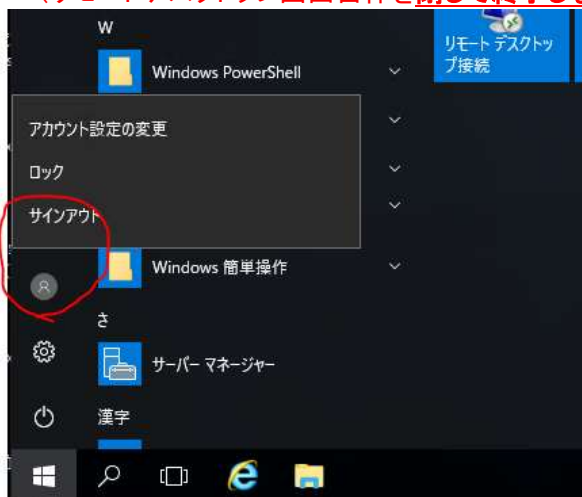
※ご自宅のルータに設定されているローカルサブネットが 192.168.1.0/24 もしくは 192.168.2.0/24 を含んでいる場合、AWS へのリモートデスクトップ接続はできませんのでご注意ください。

ご自宅のルータのローカルサブネットについて、192.168.1.0/24 と 192.168.2.0/24 を含めないように設定してください。

※リモートデスクトップ接続時に表示される警告メッセージ等は無視(全て OK)して問題ありません。

※作業終了後は必ずリモートデスクトップ先 OS にて「サインアウト」を実施して下さい。

(リモートデスクトップ画面自体を閉じて終了しないようにして下さい)



2. RDP 先画面よりリモートデスクトップ接続を起動し、接続先開発拠点 PC の IP アドレスを指定して下さい。

3. 開発拠点 PC を利用するうえでの補足事項は以下を参照して下さい。

- ・ 開発拠点 PC の smartOn は撤廃せず、代用コードを使用することでカードを設置せずともログイン可能な環境を提供する。
- ・ 代用コードは KDDI システム主管 GL から管理元責任者に提供する。管理元責任者は担当者以外に代用コードが漏洩しないよう十分な対策をとること。
- ・ 代用コードの利用には、PC 認証(smartOn 用)のキャッシュが端末に存在している必要がある。キャッシュの有効期間である **7 日以上連続して未ログイン期間を発生させない**よう留意すること。万が一 7 日を超過した場合は復旧措置が必要となる。復旧用の期限付きパスワードは KDDI システム主管 GL に問い合わせること。その際、以下の情報を通知すること。

●氏名：

●ユーザ ID(P/S 番)：

●コンピュータ名：

●ディスク名称：

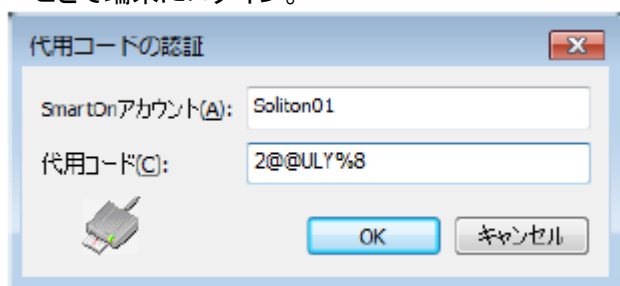
*「ディスク名称」はログオン画面の KDDI ロゴの下に表示されている。(例:本番環境_GAT_KDDI_2.4.0.1)

<代用コードでのログイン方法>

ログオン画面にて「Windows アカウント」「Windows パスワード」を入力し、「オプション」をクリックし、表示されるメニューから「代用コード」をクリック。



代用コードの認証画面にて、アカウント(S または P 番号)と発行された代用コードを入力し「OK」をクリックすることで端末にログイン。

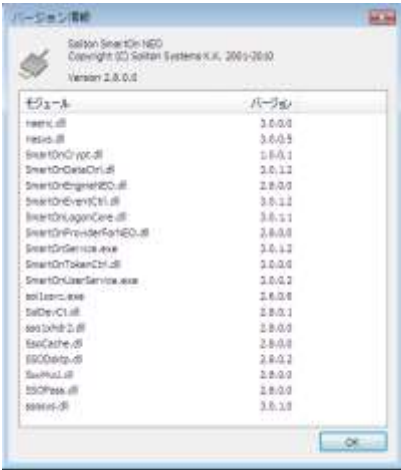


＜端末キャッシュ消失時の復旧手順＞

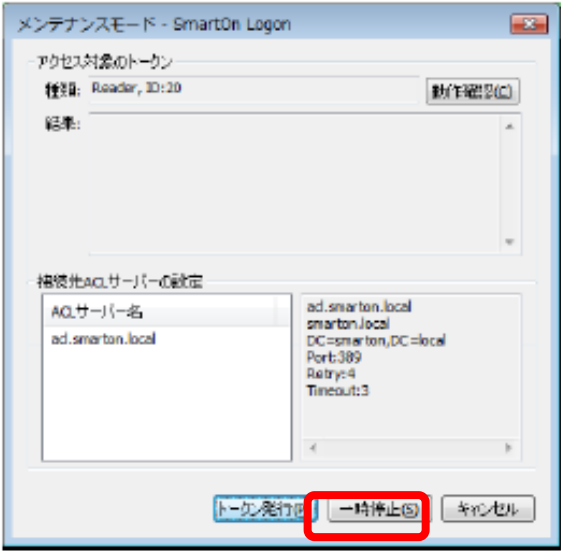
ログイン画面にて「オプション」をクリックし、表示されるメニューから「バージョン情報(V)」をクリック。



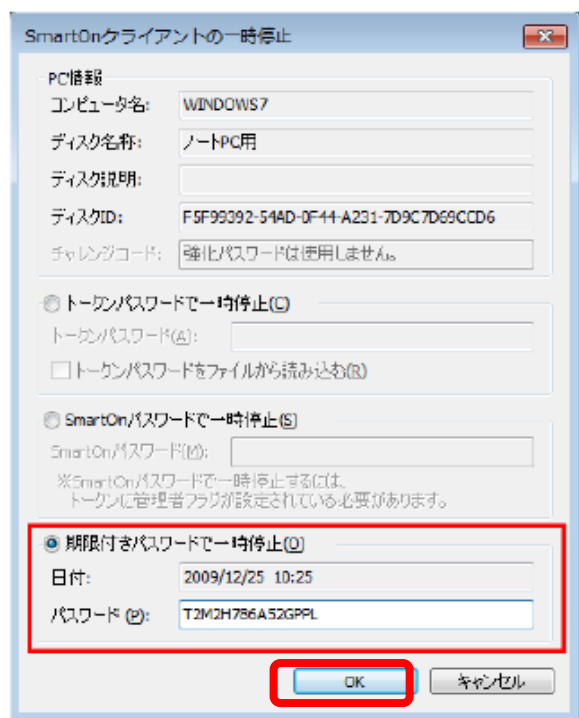
上記画面で「バージョン情報」をクリックしてバージョン情報画面を表示。



バージョン情報画面で、[Ctrl]+[Alt]キーを押したまま[k]を入力してメンテナンスモードを起動し、
[一時停止(S)]ボタンをクリック。



PC認証クライアントの一時停止画面が表示されるので[期限付きパスワードで一時停止]を選択し、KDDI システム主管 GL から指示されたパスワードを入力。



SmartOnクライアントの一時停止

PC情報

コンピュータ名: WINDOWS7

ディスク名称: ノートPC用

ディスク説明:

ディスクID: F5F99392-54AD-0F44-A231-7D9C7D69CCD6

チャレンジコード: 強化パスワードは使用しません。

☒ トークンパスワードで一時的停止(Q)

トークンパスワード(A):

☐ トークンパスワードをファイルから読み込む(R)

☒ SmartOnパスワードで一時的停止(S)

SmartOnパスワード(P):

※SmartOnパスワードで一時的停止するには、トークンに管理者フラグが設定されている必要があります。

☒ 期限付きパスワードで一時的停止(Q)

日付: 2009/12/25 10:25

パスワード (P): T2M2H786A52GPPL

OK キャンセル

SmartOn クライアントが停止し、通常の Windows 認証画面が表示される。PCにログオン可能な Windows アカウント、パスワードを入力し、ログオン。ログオン後コンピュータを再起動すると、再び IC カード認証の画面が表示されるようになる。ログオン後は速やかに再起動を実施すること。



SmartOn ID

SmartOnクライアントの一時停止

Windowsアカウント

Windowsパスワード

→

WINDOWS7

2.4. 情報共有サイトについて

以下サイトにて、開発環境をご利用頂く上での周知事項を公開しますので、リモートアクセスの都度ご確認くださいようお願いします。

情報共有サイト URL <http://192.168.1.119> or <http://192.168.2.119>

※AWS へ VPN 接続後、接続元 PC のブラウザにアクセスして下さい。

※ご利用の接続先 IP によってアクセス先 URL を変えて下さい。



以 上