信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

セコムあんしんテレワーク（USBリモート端末）サービス管理者マニュアル

ver.5.0r3 公開版

セコムトラストシステムズ株式会社

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

目次

第１章　サービスについて

第２章　トラブルシューティング

第３章　VPNゲートウェイについて

第１章
サービスについて

1．提供資料一覧

分類	資料名	説明
ヒアリングシート	USBリモート端末 サービス管理者情報シート	ご契約時にご記入いただいたシートです。サービス管理者を変更いただく際に、更新が必要となります。
	ネットワーク構成確認シート	ご契約前にご記入いただいたネットワーク構成確認シートです。
一覧表	USBリモート端末一覧表 ※詳細は「本章　４．USBリモート端末一覧表の見方」に記載	管理情報が記載されています。 ・USBリモート端末情報 ・証明書情報 ・VPN接続情報 ・契約情報
マニュアル	セコムあんしんテレワーク（USBリモート端末）サービス管理者マニュアル	本資料です。
	セコムあんしんテレワーク（USBリモート端末）利用者マニュアル	利用手順が記載されています。USBリモート端末初回利用時にご利用ください。

2．サービス管理者

2.1 概要

セコムあんしんテレワーク（USBリモート端末）（以下「本サービス」といいます）をご利用いただく際、お客様にてサービス管理者（最大３名）を登録していただきます。
サービス管理者には、以下のサービスを提供いたします。

①サービスデスクの提供

サービス管理者は、機器障害、端末紛失、契約変更等に関して、
弊社サービスデスク宛てにお問い合わせいただけます。
（サービスデスクにはサービス管理者からお問い合わせください）

②FortiCloud管理Webシステムの提供

サービス管理者には、ユーザーのVPN接続履歴情報が確認できるFortiCloud管理Webシステムへのアクセス用アカウントを提供します。

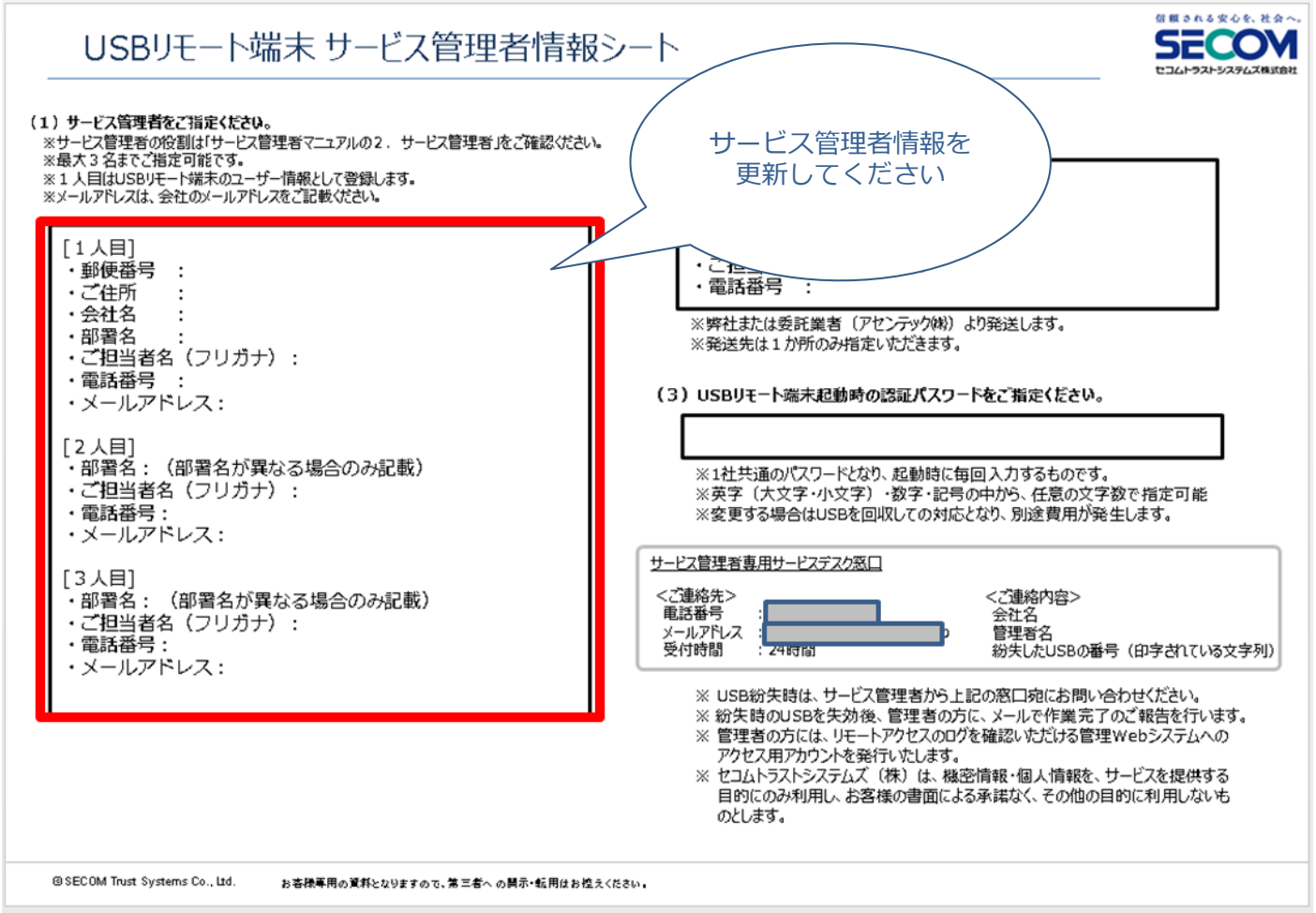
③本サービスに関する情報の提供

- 機器メンテナンス等でサービス停止する際、その停止事由、期日、時間帯等をサービス管理者に通知します。
- 年次で、USBリモート端末の契約情報と、4年毎の端末交換の案内をサービス管理者に通知します。

2．サービス管理者

2.2 サービス管理者の変更方法

サービス管理者を変更する際、「USBリモート端末 サービス管理者情報シート」の
サービス管理者情報を更新のうえ、弊社サービスデスク宛てにメールで送付ください。



USBリモート端末 サービス管理者情報シート

サービス管理者情報を
更新してください

（1）サービス管理者をご指定ください。
※サービス管理者の役割は「サービス管理者マニュアルの2．サービス管理者」をご確認ください。
※最大３名までご指定可能です。
※１人目はUSBリモート端末のユーザー情報として登録します。
※メールアドレスは、会社のメールアドレスをご記載ください。

［１人目］
・郵便番号　：
・ご住所　　：
・会社名　　：
・部署名　　：
・ご担当者名（フリガナ）：
・電話番号　：
・メールアドレス：

［２人目］
・部署名：（部署名が異なる場合のみ記載）
・ご担当者名（フリガナ）：
・電話番号：
・メールアドレス：

［３人目］
・部署名：（部署名が異なる場合のみ記載）
・ご担当者名（フリガナ）：
・電話番号：
・メールアドレス：

・電話番号　：

※弊社または委託業者（アセンテック㈱）より発送します。
※発送先は１か所のみ指定いただきます。

（3）USBリモート端末起動時の認証パスワードをご指定ください。

※1社共通のパスワードとなり、起動時に毎回入力するものです。
※英字（大文字・小文字）・数字・記号の中から、任意の文字数で指定可能
※変更する場合はUSBを回収しての対応となり、別途費用が発生します。

サービス管理者専用サービスデスク窓口

<ご連絡先>
電話番号　：
メールアドレス　：
受付時間　：24時間

<ご連絡内容>
会社名
管理者名
紛失したUSBの番号（印字されている文字列）

※ USB紛失時は、サービス管理者から上記の窓口宛にお問い合わせください。
※ 紛失時のUSBを失効後、管理者の方に、メールで作業完了のご報告を行います。
※ 管理者の方には、リモートアクセスのログを確認いただける管理Webシステムへの
アクセス用アカウントを発行いたします。
※ セコムトラストシステムズ（株）は、機密情報・個人情報を、サービスを提供する
目的にのみ利用し、お客様の書面による承諾なく、その他の目的に利用しないも
のとします。

3．USB起動補助ディスク

USBリモート端末の納品時に、「USB起動補助ディスク」を1枚同梱しております。
これは、ご使用のPCのBIOS / UEFIが、USBリモート端末からの起動に
対応していない場合にご利用いただくものです。

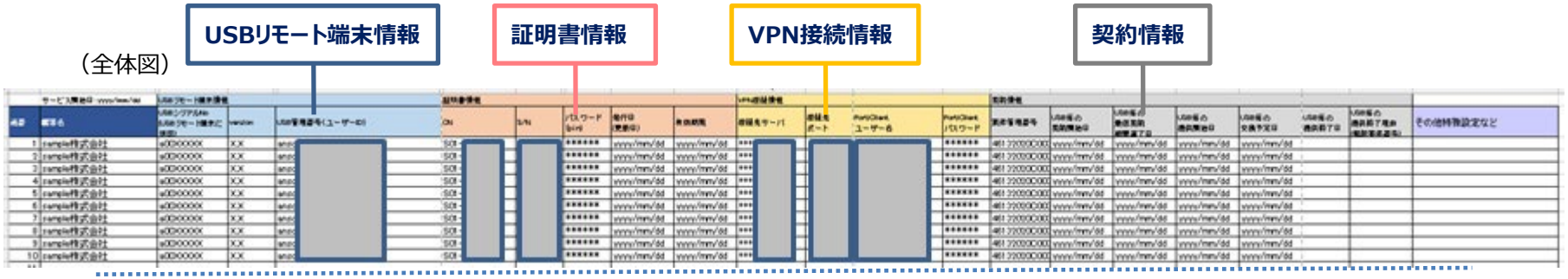
詳しい利用方法に関しては、「第２章　9.　USB起動補助ディスクの利用」をご参照ください。

※ USB起動補助ディスクを多数配布したい場合は、ディスクを複製してご利用ください。
※ USB起動補助ディスクには、認証情報や個体識別情報等の機密情報は一切保存されていません。

4．USBリモート端末一覧表の見方

USBリモート端末一覧表は4つの情報に分かれております。

（全体図）



		①		②	③	④
		サービス開始日：yyyy/mm/dd	USBリモート端末情報			
通番	顧客名			USBシリアルNo（USBリモート端末に刻印）	version	USB管理番号（ユーザーID）
1	sample株式会社			a00XXXXX	XX	ansc-
2	sample株式会社			a00XXXXX	XX	ansc-
3	sample株式会社			a00XXXXX	XX	ansc-
4	sample株式会社			a00XXXXX	XX	ansc-
5	sample株式会社			a00XXXXX	XX	ansc-
6	sample株式会社			a00XXXXX	XX	ansc-
7	sample株式会社			a00XXXXX	XX	ansc-
8	sample株式会社			a00XXXXX	XX	ansc-
9	sample株式会社			a00XXXXX	XX	ansc-
10	sample株式会社			a00XXXXX	XX	ansc-

【USBリモート端末情報】

①サービス開始日：セコムあんしんテレワーク（USBリモート端末）サービスの開始日

②USBシリアルNo：USBリモート端末に刻印されているシリアルナンバー

③version：USBリモート端末の専用OSのバージョン

④USB管理番号（ユーザーID）：USBリモート端末の管理番号（USB本体のシール情報）

4．USBリモート端末一覧表の見方

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫	⑬
証明書情報					VPN接続情報			
CN	S/N	パスワード (pin)	発行日 (更新日)	有効期限	接続先サーバ	接続先 ポート	FortiClient ユーザー名	FortiClient パスワード
S01		******	yyyy/mm/dd	yyyy/mm/dd	.jp			******
S01		******	yyyy/mm/dd	yyyy/mm/dd	.jp			******
S01		******	yyyy/mm/dd	yyyy/mm/dd	.jp			******
S01		******	yyyy/mm/dd	yyyy/mm/dd	.jp			******
S01		******	yyyy/mm/dd	yyyy/mm/dd	.jp			******
S01		******	yyyy/mm/dd	yyyy/mm/dd	.jp			******
S01		******	yyyy/mm/dd	yyyy/mm/dd	.jp			******
S01		******	yyyy/mm/dd	yyyy/mm/dd	.jp			******
S01		******	yyyy/mm/dd	yyyy/mm/dd	.jp			******
S01		******	yyyy/mm/dd	yyyy/mm/dd	.jp			******

【証明書情報】

USBリモート端末に埋め込まれているVPN接続用の証明書情報です

⑤CN：証明書のコモンネーム

⑥S/N：証明書のシリアル番号

USB管理番号に対応しています

⑦証明書パスワード：証明書のパスワード

⑧発行日（更新日）：証明書の発行日（更新日）

⑨証明書有効期限：証明書の有効期限

有効期限を過ぎると利用できなくなります

【VPN接続情報】

⑩接続先サーバ：VPNゲートウェイ（FortiGate）の接続先サーバ名

⑪接続先ポート：VPNゲートウェイ（FortiGate）の接続先ポート

⑫FortiClientユーザー名：VPNゲートウェイ（FortiGate）接続時のユーザザ名

⑬FortiClientパスワード：VPNゲートウェイ（FortiGate）接続時のパスワード

4．USBリモート端末一覧表の見方

⑭	⑮	⑯	⑰	⑱	⑲	⑳	
契約情報							
案件管理番号	USB毎の契約開始日	USB毎の最低契約期間満了日	USB毎の提供開始日	USB毎の交換予定日	USB毎の提供終了日	USB毎の提供終了理由(解約案件番号)	その他特殊設定など
46132020C003	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd			
46132020C003	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd			
46132020C003	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd			
46132020C003	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd			
46132020C003	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd			
46132020C003	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd			
46132020C003	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd			
46132020C003	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd			
46132020C003	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd			
46132020C003	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd	yyyy/mm/dd			

【契約情報】

⑭案件管理番号：弊社用の管理番号

⑮USB毎の契約開始日：USBリモート端末毎の契約開始日

⑯USB毎の最低契約期間満了日：USBリモート端末毎の契約期間満了日（「USB毎の契約開始日」の2年後）

⑰USB毎の提供開始日：USBリモート端末毎の提供開始日

⑱USB毎の交換予定日：「USB毎の提供開始日」の4年後で、USBリモート端末の提供終了となる日です。
4年を超えて利用する場合、USBリモート端末交換の申込みが必要です（作業費：¥4,000/本）
USBリモート端末を交換しても、最低契約期間は継承されます。

⑲USB毎の提供終了日：USBリモート端末の交換・解約・紛失等でUSBリモート端末の提供が終了した日

⑳USB毎の提供終了理由（解約案件番号）：USBリモート端末の提供終了の理由

5．動作環境とご留意事項

5.1 動作環境

USBリモート端末の起動に必要なPCスペック

CPU　　：Intel core i3、i5、i7（Intel系CPU　64bit、1GHz以上）など
メモリ　　：3GB以上
起動方法　　：USBドライブ起動に対応
コネクタ　　：USB　Type-A（USB2.0、またはUSB3.0）
無線LAN(Wi-Fi)規格：IEEE 802.11 a/b/g/n/ac　（他機器や電子レンジの干渉が少ない5GHz帯を推奨）

※起動順位変更ツールを使用する場合は、Windows Vista以降のOSで、.NET Framework 3.0以上が必要。

※ USBドライブ起動に未対応の場合、CDドライブがあれば、「USB起動補助ディスク」を
併用する事で起動可能となります。 詳細は「第２章　９．USB起動補助ディスクの利用」を参照ください。

事前にご利用するPCにて、USBリモート端末での起動が可能かご確認いただくようお願いいたします。

5．動作環境とご留意事項

5.2 自宅PCについて

①USBリモート端末の起動には、BIOS/UEFIの設定が必要になる場合があります。PCによっては、
起動の都度BIOS/UEFIの設定が必要となる場合があります。

②有線LANもしくは無線LAN(Wi-Fi)をご利用ください。
無線LAN(Wi-Fi)受信機によっては、ご利用できない場合があります。
その場合は、有線LAN接続をご利用ください。

③Apple社製PCは、サポート対象外となります。

④Bluetoothはご利用いただけません。

⑤PCによっては、個別の機能が利用できないことがあります。
事前に動作確認してください。
（確認項目）

- Wi-Fi受信機
- 有線LANポート
- キーボード
- タッチパッド、マウス
- LCDモニタ
- 外部ディスプレイ出力　※HDMI, DVI, VGA等
- サウンド出力
- マイク入力

5．動作環境とご留意事項

5.3 会社PCについて

①会社PCは、あらかじめ電源を入れた状態でご利用ください。ログインしておく必要はありません。

②会社PCの機種によっては、スリープ状態になると接続できなくなる場合があります。
自動的にスリープにならないよう、設定を変更してください。

③ご利用の環境によっては、リモートデスクトップ接続の許可、NLA（ネットワークレベル認証）の無効化、Remote Desktop Usersグループへのユーザー追加を行っていただく必要があります。
詳細は「第２章　18. リモートデスクトップ接続できない」を参照ください。

④会社PCが「Azure Active Directory」に参加していると、接続できない場合があります。

⑤会社PCがWindows 10 Home等のHomeエディションでは、Windowsの機能制限により接続できません。

5．動作環境とご留意事項

5.4 自宅PCの通信環境について

自宅PCの通信環境により接続できない、また不安定になる場合があります。

（接続が不安定になる要因の例）

①ルーターの設定

②LANケーブルの接続不良

③契約回線の通信制限（データ容量上限オーバー）

④Wi-Fiルーターの電波の状況

6．年次のご契約内容の報告について

サービス開始日から１年毎にサービス管理者様宛にUSBリモート端末一覧表をお送りし、
ご契約内容を報告いたします。

※サービス開始日はUSBリモート端末一覧表の「本章　4．　USBリモート端末一覧表の見方」の①に該当します。

報告の際、１年以内に交換が必要なUSBリモート端末の管理番号をご案内いたしますので、
交換をご希望の場合は、サービスデスク宛てにご連絡ください。
USBリモート端末をご返送いただく際の配送費用は、お客様のご負担となります。

7．サービスデスクについて

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

サービスデスクは、以下のようなときにご利用いただけます。

・USBリモート端末の紛失時において、利用停止したい場合
・USBリモート端末の不具合が疑われる場合

※USBリモート端末の不具合については、本マニュアルのトラブルシューティングをご確認の上、ご連絡ください。

・VPNゲートウェイの不具合が疑われる場合
・本サービスの契約内容を変更・更新したい場合

① 問合せ方法

以下情報を準備いただいた上で**サービス管理者**よりお問合せください。

・サービス名「セコムあんしんテレワーク（USBリモート端末）」
・会社名
・サービス管理者名（ご本人のお名前）
・USBリモート端末に刻印されている文字列
・お問合せ内容

② お問合せ先：サービスデスク

電話番号、メールアドレスは「USBリモート端末 サービス管理者情報シート」に記載

③ 受付時間 ： 24 時間 365 日

④ USBリモート端末 紛失対応時間帯 ： 24 時間 365 日

VPNゲートウェイ 不具合対応時間帯 ： 月曜日 ～金曜日　9：00 ～17 ：00
〔土日祝日、年末年始（ 12 月 30 日～ 1月 3日）は除きます〕

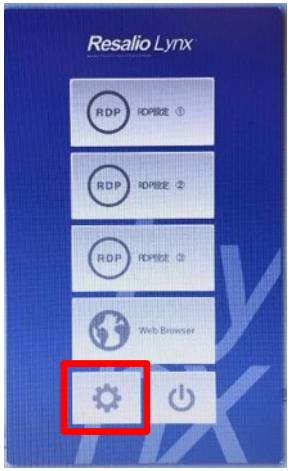
上記以外の 対応時間帯 ： 月曜日 ～金曜日　9：00 ～18 ：00
〔土日祝日、年末年始（ 12 月 30 日～ 1月 3日）は除きます〕

第２章
トラブルシューティング

1．USBリモート端末設定変更後の保存方法

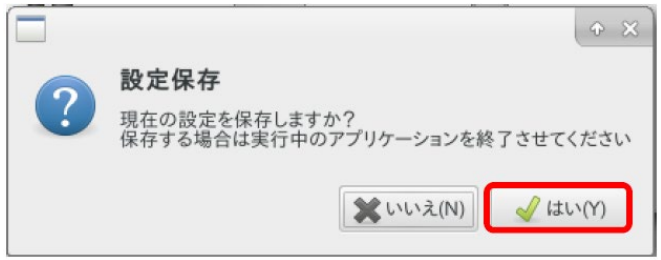
USBリモート端末の設定を変更し、その設定を保存したい場合、以下の手順を実施してください。

①メニュー画面の「コントロールパネル(歯車マーク)」をクリックします。



②コントロールパネルが表示されたら、「設定保存」をダブルクリックします。

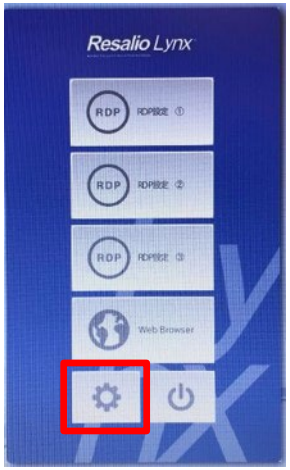
「設定保存」ダイアログで「はい」をクリックします。



2．設定情報の消去

リモートデスクトップ接続先、 Wi-Fi設定やコントロールパネルで設定した内容を消去したい場合は以下の手順を行います。

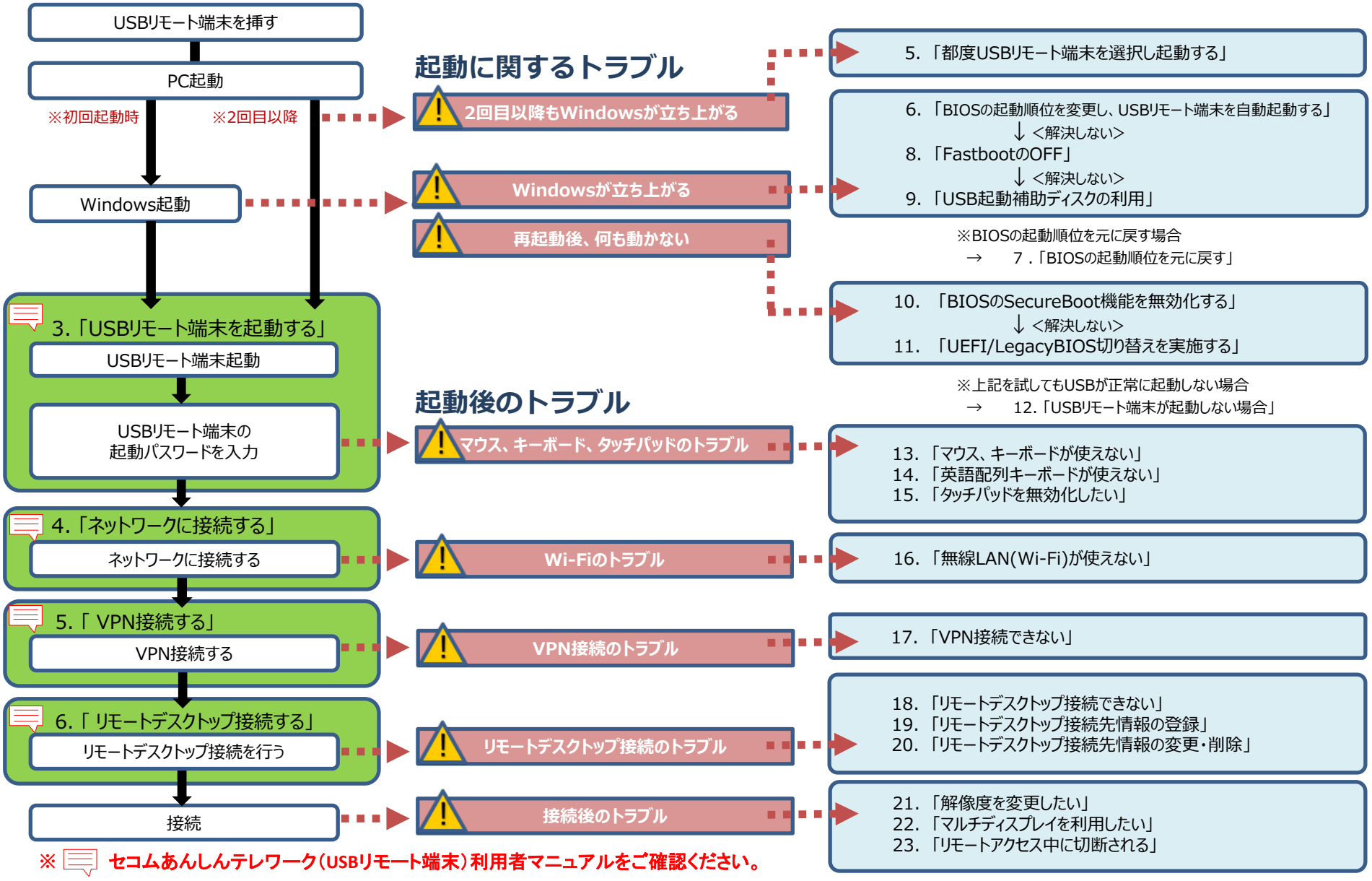
①メニュー画面の「コントロールパネル（歯車マーク)」をクリックします。



②コントロールパネルが表示されたら「設定消去」をダブルクリックします。

③「設定消去」ダイアログが表示されるので、「はい」 をクリックして完了です。

3．トラブルシューティングフローチャート



4．BIOS/UEFIの起動方法

USBリモート端末を利用するうえで、ご使用PCの BIOS/UEFI（※）画面で
設定情報の確認や変更を実施することがあります。
BIOS/UEFI画面を起動する方法は以下となります。
※BIOS/UEFI：OSの起動設定やPCと接続機器の入出力設定を制御するプログラムです。

①ファンクションキーを使う場合
PCの電源を入れた直後、メーカーロゴ画面で指定のキーを押すと、BIOS/UEFIの設定画面が表示されます。指定のキーはメーカーや機種で異なるため、ご使用PCのマニュアルまたはメーカーのWEBサイトを参考にしてください。

例）

ＨＰ	：F2またはF10
ＶＡＩＯ	：F3またはF4キーを押しながら、電源を入れます
ｍｏｕｓｅ	：F2
Ａｔｒｕｓｔ	：Delete

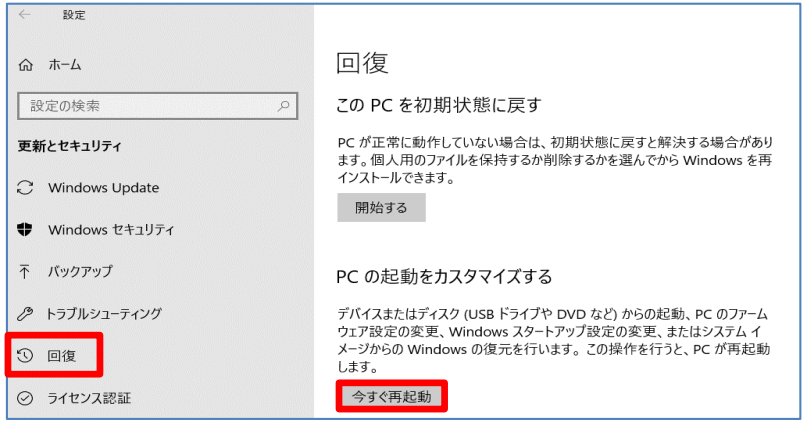
4．BIOS/UEFIの起動方法

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

②Windows設定画面を使う場合
以下の手順を行います。
・USBリモート端末を挿した状態でWindowsを起動します。

・「スタートボタン」→「設定ボタン」→「更新とセキュリティ」をクリックします。
※ Windows8.1の場合、画面の右上隅または、右下隅にカーソルを合わせると表示される
メニュー（チャーム）を表示し、「設定ボタン」を選択してください。

・設定画面が開くので、「回復」→
「今すぐ再起動」をクリックします。

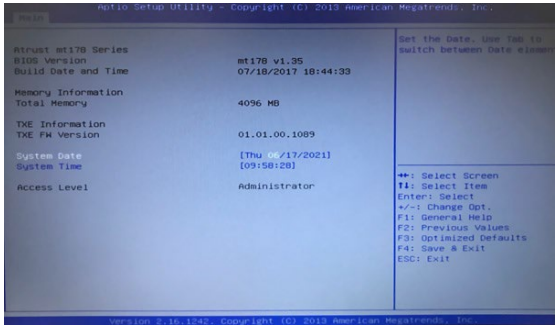


4．BIOS/UEFIの起動方法

・再起動後「オプションの選択」画面が表示されます。
「トラブルシューティング」→「詳細オプション」→「UEFIファームウェアの設定」→
「再起動」をクリックします。

・再起動後、BIOS画面が表示されます。

BIOS画面の表示例　※メーカーによって画面は異なります。



5．都度USBリモート端末を選択し起動する

BIOS画面やWindows設定画面から、明示的にUSBリモート端末を起動させる方法をご紹介します。
利用ケースに応じてお試しください。

①ファンクションキーを使って起動する場合
以下の手順を行います。
・USBリモート端末を挿した状態にします。
・PCの電源をいれ、BIOS画面で起動デバイスを選択する画面を表示させ、
上から、CD-ROM や USB-CDROM といったCDに関する項目、あるいはHAGIWARAといった
デバイスの名称の項目を選択し、USBリモート端末を起動させます。
（BIOS画面の起動方法はメーカー・機種によって異なりますので、メーカーのWEBサイトにて
ご確認ください。）

例）

ＨＰ	PCの電源を入れ、F9キー連打で起動オプション画面を表示させます。 ↑↓カーソルキーを使い、起動するデバイスを選択して、Enterキーを押します。
ｍｏｕｓｅ	PCの電源を入れ、F7キー連打でBoot Device 選択画面を表示させます。 ↑↓カーソルキーを使い、起動するデバイスを選択して、Enterキーを押します。

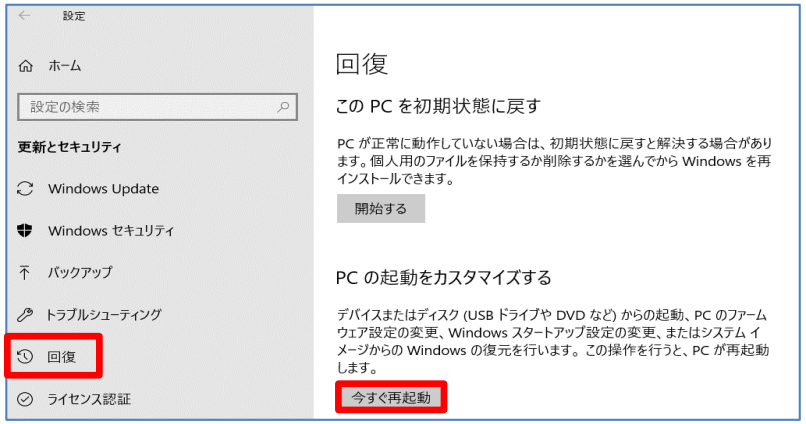
5．都度USBリモート端末を選択し起動する

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

②Windows設定画面から起動する場合
以下の手順を行います。
・USBリモート端末を挿した状態でWindowsを起動します。

・「スタートボタン」→「設定ボタン」→「更新とセキュリティ」をクリックします。
※ Windows8.1の場合、画面の右上隅または、右下隅にカーソルを合わせると表示される
メニュー（チャーム）を表示し、「設定ボタン」を選択してください。

・設定画面が開くので、「回復」→
「今すぐ再起動」をクリックします。



5．都度USBリモート端末を選択し起動する

・再起動後「オプションの選択」画面が表示されます。
「デバイスの使用」をクリックします。

・CD-ROM や USB-CDROM といったCDに関する項目、あるいはHAGIWARAといったデバイスの名称の項目を選択してください。
USBリモート端末が起動します。

6．BIOSの起動順位を変更し、USBリモート端末を自動起動する

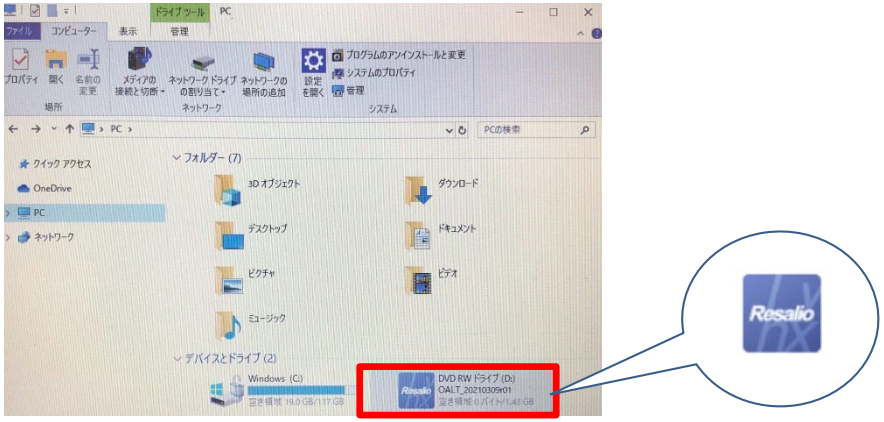
BIOSの起動順序を変更することによって、電源投入時、再起動時に自動的にUSBリモート端末が起動するようになります。

①起動順位変更ツールを使う場合

Windows上で起動順位を変更できる「起動順位変更ツール」を用意しています。
BIOSやUEFIのセットアップ画面に入ることなく、USBリモート端末の起動順位をPCのローカルディスクよりも上位にすることが可能です。
「起動順位変更ツール」を実行しても、USBリモート端末が起動しない場合は、「②BIOS画面で変更する場合」を確認してください。

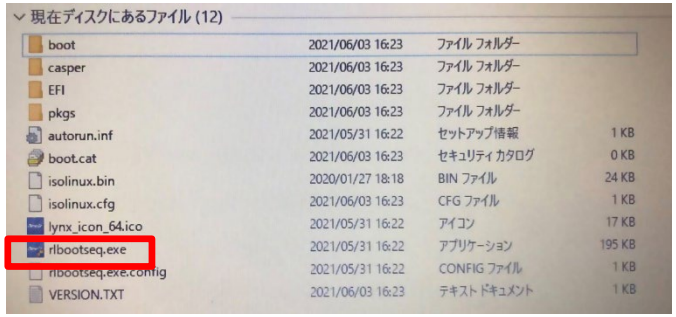
※Windows Vista以降のOSで、.NET Framework 3.0以上が必要です。
※あらかじめ、USBリモート端末をPCに挿してから、以下操作を実施してください。

・Windowsキー+Eキーでエクスプローラを開き、「PC」を選択します。
USBリモート端末はDVD-ROMとして表示されますので、ダブルクリックして中を開きます。

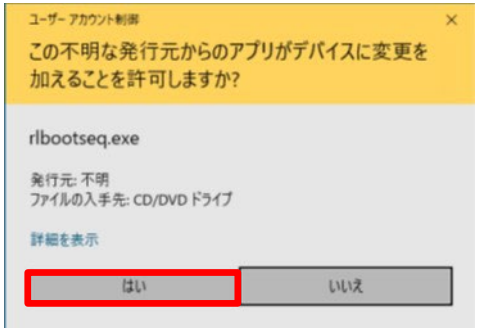


6．BIOSの起動順位を変更し、USBリモート端末を自動起動する

・「rlbootseq.exe」をダブルクリックして実行します。



・「ユーザーアカウント制御」のダイアログが表示されたら「はい」をクリックします。

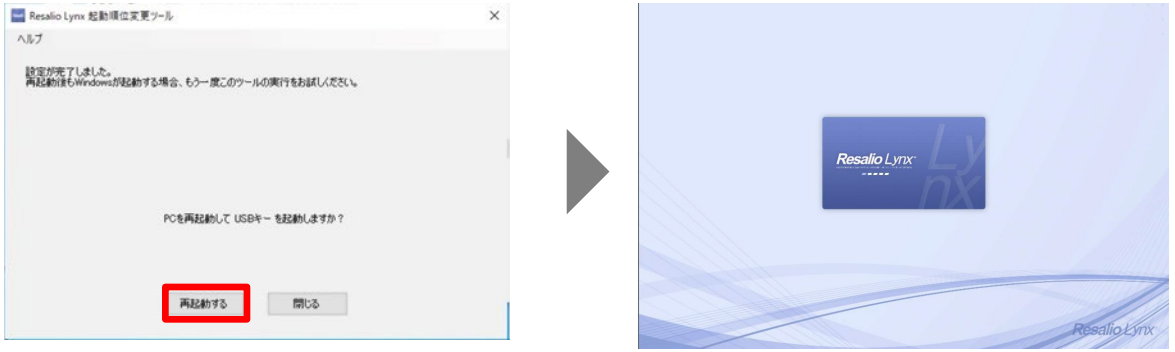


・起動順位変更ツールが起動します。「USBキーの起動順位を先頭にする」をクリックします。

6．BIOSの起動順位を変更し、USBリモート端末を自動起動する

・「USB CD」または「CD」（環境によっては、表記が異なる場合があります。）が「Windows Boot Manager」よりも上位にあることを確認して、「変更する」をクリックします。

・「設定が完了しました。」と表示されたら、順位変更は完了です。USBリモート端末をPCに挿したまま、「再起動する」をクリックしてください。起動順位の変更が成功すると、USBリモート端末の起動画面が表示されます。



6．BIOSの起動順位を変更し、USBリモート端末を自動起動する

②BIOS画面で変更する場合

「起動順位変更ツール」を実行しても、USBリモート端末が起動しない場合、BIOSの起動順位を確認してください。

※あらかじめ、USBリモート端末をPCに挿してから、以下操作を実施してください。

・BIOSの画面を開きます。
「本章　４．　BIOS/UEFIの起動方法」を実施してください。

・BIOS画面のデバイスの起動順位を変更する画面にて、デバイスの起動順（Boot順）を、CD-ROM や USB-CDROM といったCDに関する項目、あるいはHAGIWARAといったデバイスの名称の項目が最初に起動するように設定を変更してください。
なお、BIOSの設定画面はメーカー・機種によって異なります。BIOSの設定変更方法は、メーカーのWEBサイトにてご確認ください。

例）ＨＰ
ノートブックPCの場合：[Storage] (ストレージ) を選択し、[Boot Options] (ブートオプション) を選択します。
デスクトップPCの場合：[System Configuration] (システム構成) を選択し、[Boot Order] (ブート順) を選択します。
表示される画面に従い、順序を変更します。

ＶＡＩＯ	[BIOS設定を起動]→[Boot Configuration]メニューから↑↓で変更する起動デバイスを選択し、＋(F6キー)－(F5キー)で優先度を変更して、[Save] で保存します。
ｍｏｕｓｅ	[Boot]メニューから↑↓で [Boot Option #1] を選択しEnterキーを押します。 表示されたBoot Option 画面で起動したいデバイスを選択し、 [Save & Exit] で保存します。
Ａｔｕｒｓｔ	BootタブよりBoot Option Priorities で [Boot Option #1~#4] を↑↓で選択し、Enterキーを押します。起動したいデバイスを↑↓で選択後Enterキーを押し、[Save & Exit] で保存します。

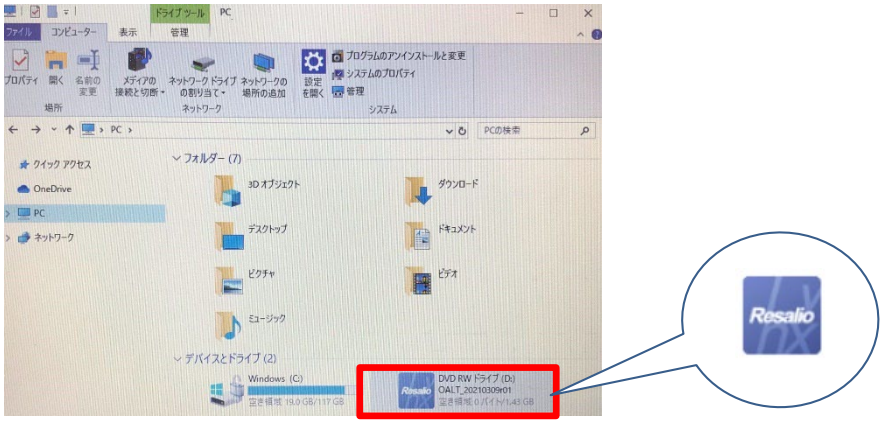
7．BIOSの起動順位を元に戻す

「起動順位変更ツール」には、USBリモート端末の起動順位を元に戻す（PCのローカルディスクよりも下位にする）機能があります。

※Windows Vista以降のOSで、.NET Framework 3.0以上が必要です。
※一部の機器では起動順位変更ツールに対応しておりません。

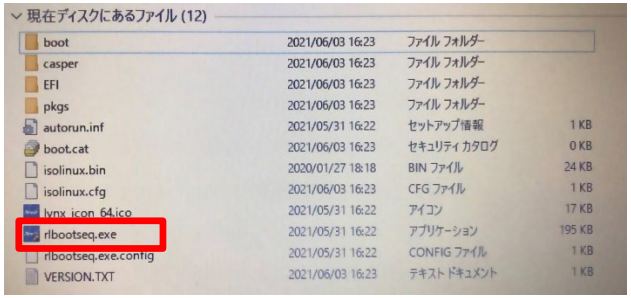
①USBリモート端末を外し、PCの電源をいれ、Windowsを起動します。
　Windows起動後、USBリモート端末をPCに挿します。

②WindowsをWindowsキー+Eキーでエクスプローラを開き、「PC」を選択します。
　USBリモート端末はDVD-ROMとして表示されますので、ダブルクリックして中を開きます。

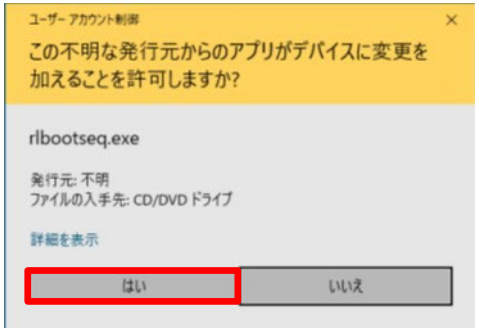


7．BIOSの起動順位を元に戻す

③「rlbootseq.exe」をダブルクリックして実行します。



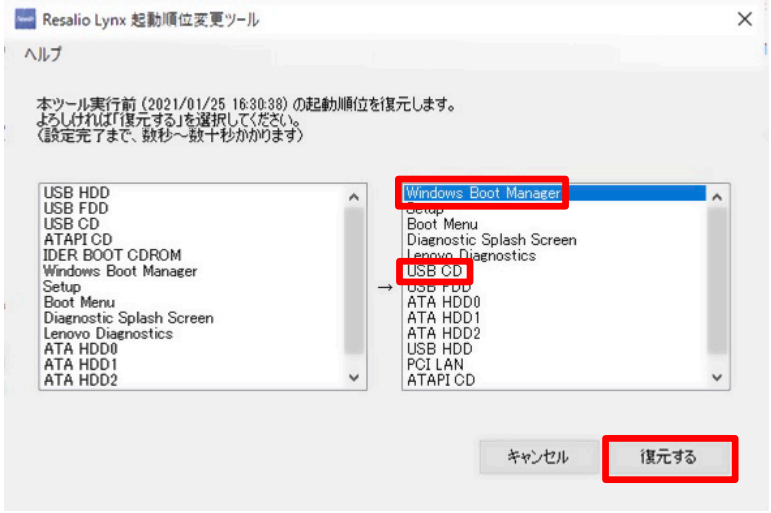
④「ユーザーアカウント制御」のダイアログが表示されたら「はい」をクリックします。



⑤起動順位変更ツールが起動します。「起動順位を元に戻す」をクリックします。

7．BIOSの起動順位を元に戻す

⑥「Windows Boot Manager」が「USB CD」（環境によっては、異なる表記の場合があります。）
より上位にあることを確認して、「復元する」をクリックします。



⑦「起動順位の復元が完了しました。」と表示されたら完了です。USBリモート端末を挿したまま、
「再起動する」をクリックします。起動順位の変更が成功すると、Windowsが起動します。

8．FastBootのOFF

FastBootの設定がONになっていると、USBリモート端末が起動しないことがあります。
USBリモート端末が起動しない場合、FastBootの設定をOFFにして、ご確認ください。

①BIOSの画面を開きます。
「本章　４．BIOS/UEFIの起動方法」を実施してください。

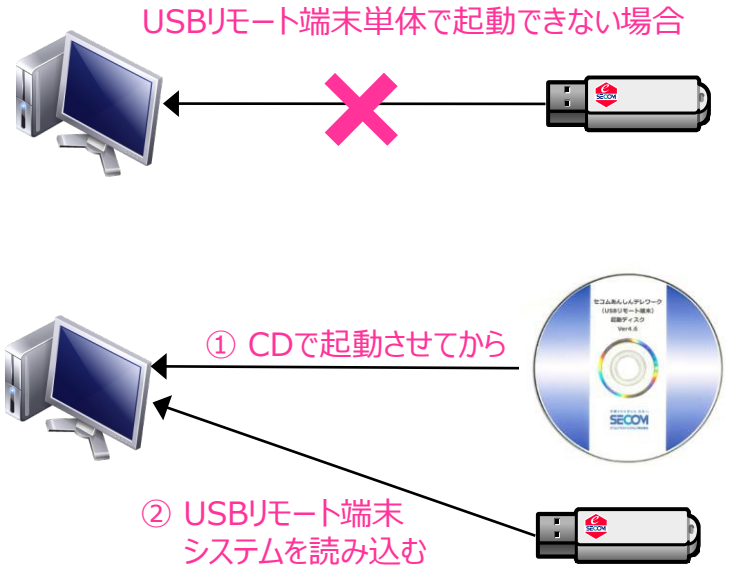
②BIOS画面のFastBootを変更する画面にて、FastBootの設定をOFFにしてください。
※メーカー、機種によってFastBootの項目が無い場合があります。無い場合は確認不要です。

なお、BIOSの設定画面はメーカー・機種によって異なります。BIOSの設定変更方法は、
メーカーのWEBサイトにてご確認ください。

例）
ＨＰ
セキュリティメニューの[Secure Boot Configuration] を選択し、Enter キーを押します。 [Fast Boot] の項目で [無効] を選択します。または [詳細設定（Advanced）] → [ブートオプション（Boot Options）] → [高速起動（Fast Boot）] のチェックを外します。

9．USB起動補助ディスクの利用

ご使用のPCのBIOS/UEFIが、USBリモート端末からの
起動に対応していない場合、
PC内蔵のCDドライブから起動することで、
USBリモート端末をご利用になれる場合があります。



＜ご留意事項＞

・USB起動補助ディスクは、USBリモート端末からの起動に対応しない問題を解決するためのものです。 USB起動補助ディスクを利用しても他の要因により起動しない場合があります。

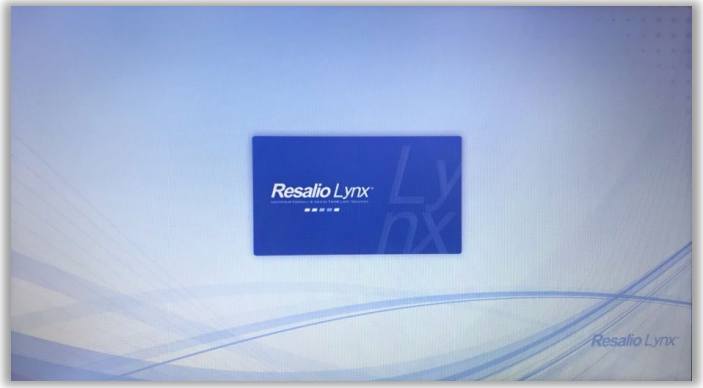
・USB起動補助ディスクのバージョンと、USBリモート端末のバージョンが異なっていると、正常に動作しない可能性があります。USBリモート端末の交換等によりバージョンが変更になった際は、利用するUSB起動補助ディスクも差し替える必要がありますので、ご注意ください。

9．USB起動補助ディスクの利用

<USB起動補助ディスクのご利用方法>

事前準備：BIOS/UEFI設定画面を開き、PCの起動設定を確認してください。
その際、デバイスの起動順（Boot順）として、CD-ROM や DVD-ROM
といったCDに関する項目が最初に起動するように設定を変更してください。
※「本章　6．BIOSの起動順位を変更し、USBリモート端末を自動起動する」を
ご参考ください。

①USB起動補助ディスクを、自宅PCのCDドライブに挿入します。
②自宅PCの電源を切り、改めて電源を入れます。
③以下の画面が表示されたら、USBリモート端末を挿します。



④USBリモート端末が青く点滅し、USBリモート端末が起動します。
その後は「セコムあんしんテレワーク（USBリモート端末）利用者マニュアル」の
内容に従ってご利用ください。

１０．BIOSのSecureBoot機能を無効化する

BIOSの起動順位を変更しても、USBリモート端末が起動しない場合で、かつ　SecureBoot（事前に許可されたデバイスのみ利用可能とする）の機能がある場合は、ご使用のPCにおいてBIOSのSecureBootを無効化してください。
※起動方法を切り替えた場合、PCにインストールされているOSが起動しない場合があります。
その場合、USBリモート端末利用終了後は起動設定を元に戻してください。

①BIOSの画面を開きます。
「本章　４．　BIOS/UEFIの起動方法」を実施してください。

② SecureBootの設定を変更する画面にて、 SecureBootが有効になっている場合は
無効に変更してください。
※メーカー、機種によってSecureBootの項目が無い場合があります。無い場合は確認不要です。

なお、BIOSの設定画面はメーカー・機種によって異なります。BIOSの設定変更方法は、
メーカーのWEBサイトにてご確認ください。

例）

ＨＰ

[システム構成] メニューを選択し、 [ブートオプション] を選択し、Enter キーを押します。
[セキュアブート(Secure Boot)] を選択し、Enterキーを押して [無効（Disabled）] に変更します。

ｍｏｕｓｅ

[Security] メニューを選択して、表示された画面で [Secure Boot] を選択し、Enter キーを押します。
[Disabled] に変更します。

１１．UEFI/Legacy BIOS切り替えを実施する

SecureBootを無効にしても、USBリモート端末が起動しない場合は、ご使用のPCのブートモードがUEFIモードならLegacyBIOSに、LegacyBIOSモードならUEFIに変更してください。

※起動方法を切り替えた場合、PCにインストールされているOSが起動しない場合があります。
その場合、USBリモート端末利用終了後は起動設定を元に戻してください。

①BIOSの画面を開きます。
「本章　４．BIOS/UEFIの起動方法」を実施してください。

②BIOS画面のUEFI/LegacyBIOSを切り替える画面にて、ブートモードの設定を切り替えます。
※メーカー、機種によってUEFI/LegacyBIOSを切り替える項目が無い場合があります。
無い場合は確認不要です。
なお、BIOSの設定画面はメーカー・機種によって異なります。BIOSの設定変更方法は、
メーカーのWEBサイトにてご確認ください。

例）

ＨＰ

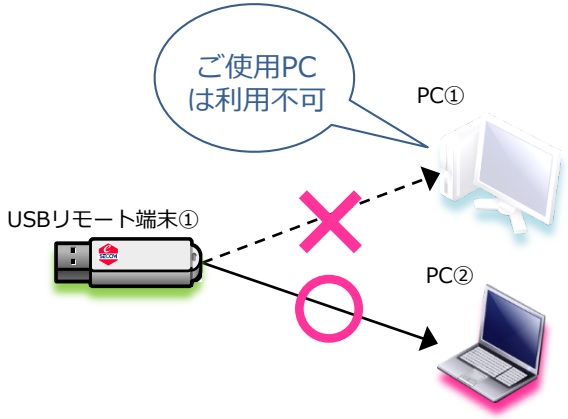
[セキュリティ] メニューから [安全なブートの構成] ([Secure Boot Configuration]) を選択し、Enterキーを押します。安全なブートの構成 (Secure Boot Configuration) ウインドウが起動します。 [安全なブート] (Secure Boot) の項目を選択し、右向き矢印キーを押して [有効] から [無効] に変更すると、自動的に [レガシーサポート] (Legacy Support) の値が [無効] から[有効] に切り替わります。

Ａｔｒｕｓｔ

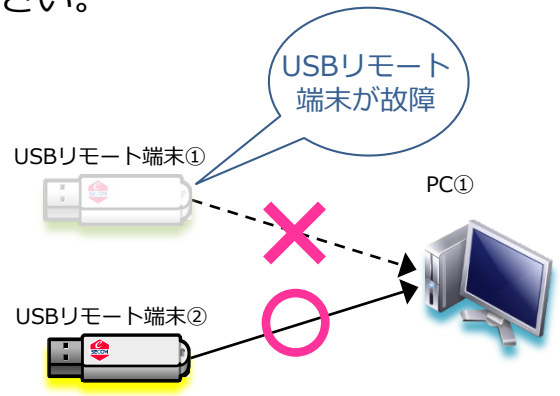
[Advanced] タブを選択し、 [CSM Configuration] を選択し、[Enter] を押します。 [Boot option filter] を選択し、Enterキーを押して [UEFI and Legacy] に変更します。

１２．USBリモート端末が起動しない場合

・他のPCにおいてUSBリモート端末が起動した場合、USBリモート端末の問題ではなく、ご使用のPCの問題と思われます。他のPCをご利用いただく等ご検討ください。



・ご使用のPCで、他のUSBリモート端末が起動した場合、
ご使用のPCの問題ではなく、USBリモート端末が故障していると思われます。
管理者を通して弊社サービスデスク宛てにお問い合わせください。



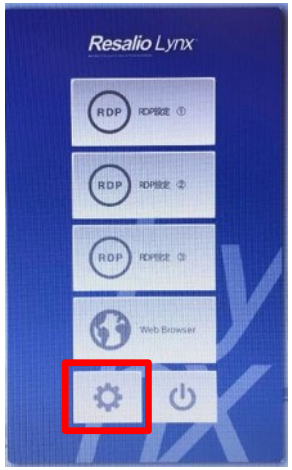
１３．マウス、キーボードが使えない

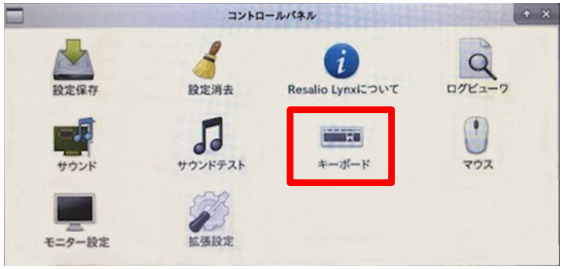
自宅PCでUSBリモート端末を起動した際、マウス・キーボードが反応しない場合は、USBリモート端末が自宅PCのマウス・キーボードに対応していないことが想定されます。

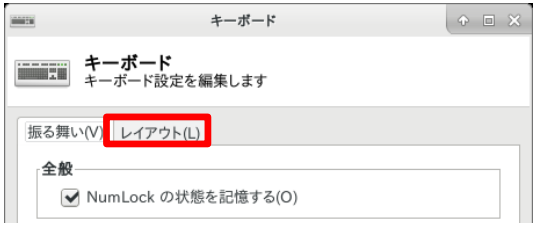
ノートPCの場合、本体付属のマウス・キーボードではなく、USB外付けのマウス・キーボードを使うことでUSBリモート端末を利用できることがあります。

１４．英語配列キーボードが使えない

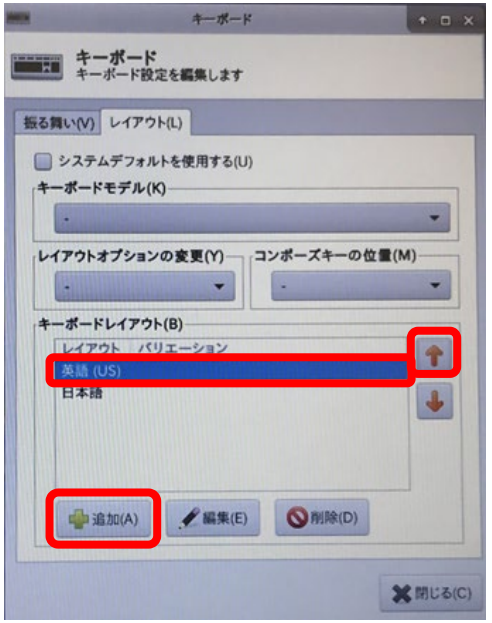
英語配列キーボード（USキーボード）をご利用されていて、キーボード配列が合わず、記号等が入力できない場合は以下の手順を行います。
（USBリモート端末は日本語配列キーボードがデフォルト設定となっています。）
①メニュー画面の「コントロールパネル(歯車マーク)」→「キーボード」 → 「レイアウト」 の順に選択します。







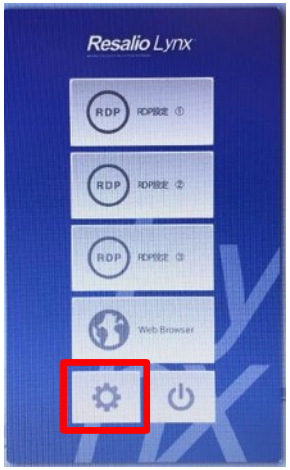
②「追加」をクリックし、 「英語 (US)」 を選択し、「キーボードレイアウト」にて「英語 (US)」を上部に移動させお試しください。

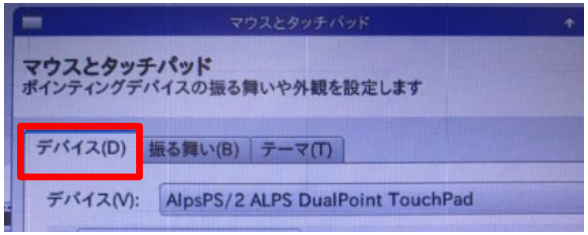


１５．タッチパッドを無効化したい

※あらかじめマウスを用意した上で以下設定を試してください。

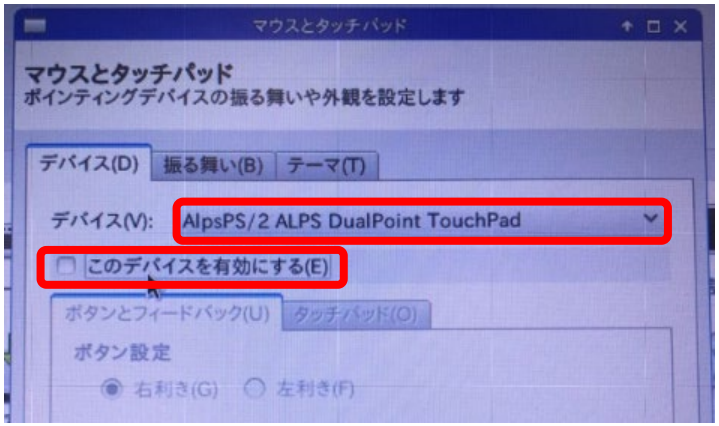
①メニュー画面の「コントロールパネル(歯車マーク)」→「 マウス」→「デバイス」の順に選択します。





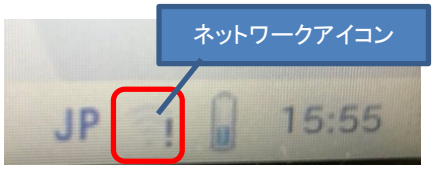
②タッチパッドのデバイスを選択し、「このデバイスを有効にする」のチェックを外して改善されるかお試しください。

※チェックを外すとタッチパッドが無効になります。

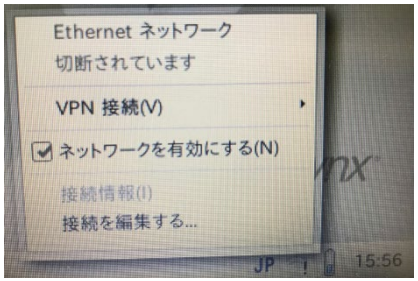


１６．無線LAN(Wi-Fi)が使えない

①USBリモート端末の画面右下のネットワークアイコンをクリックした時に、Wi-Fi情報が表示されない場合



※ネットワークが接続されていないと「！」が表示されます



←Wi-Fi情報が表示されない

→USBリモート端末が、お使いの内蔵Wi-Fi受信機に対応しておりません。
以下の方法でネットワークに接続できるかお試しください。

【Wi-Fiが使用できない場合の対応方法】

・Wi-Fiは使わず、有線LANを利用

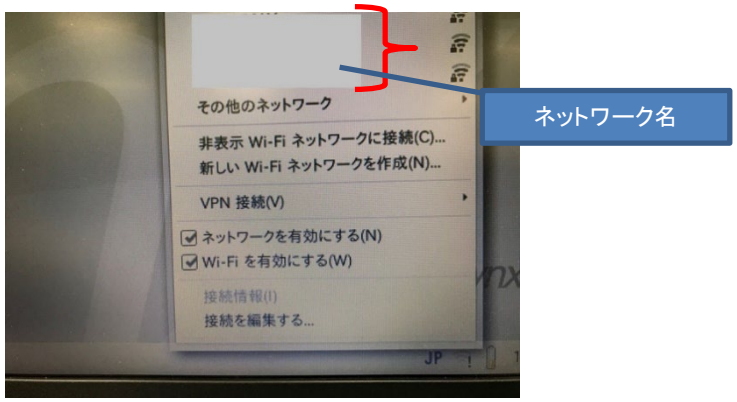
・Wi-Fiを有線化する機器（無線LANイーサネットコンバータ）を購入いただき、有線化した上で有線LANで接続
※「無線LANイーサネットコンバータ」をお客様ご自身で設定いただく必要があります。

・Wi-FiルータとPCをUSBで繋ぎ、USB経由で接続
※Wi-Fiルータの種類により利用可能です。

・USB外付けWi-Fi受信機を購入いただき、 Wi-Fi受信機を利用して接続
※「USB外付けWi-Fi受信機」を、USBリモート端末が認識しない可能性があります。

１６．無線LAN(Wi-Fi)が使えない

②Wi-Fi情報で接続したいネットワーク名が見つからない場合



その他のネットワークをクリックして、接続したいネットワークが表示されるかご確認ください。

※その他のネットワークをクリックしても接続したいネットワークが表示されない場合は、
ご利用のWi-Fi環境の通信規格や無線チャンネルの確認等を行ってみてください。

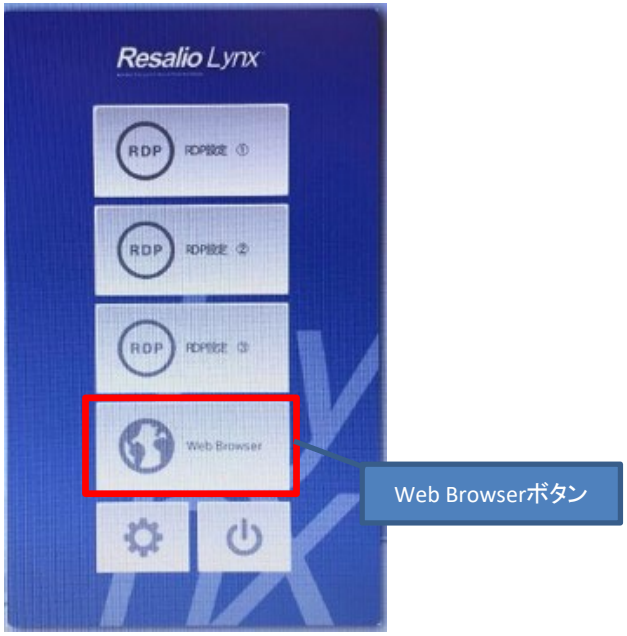
１７．VPN接続できない

ネットワークが繋がった状態でも、VPN接続ができない場合は、以下をご確認ください。

※ネットワークに繋がった状態

インターネットに接続できていないことが原因です。
メニュー画面の「Web Browser」ボタンをクリックして
ブラウザを立ち上げ、以下のURLを手入力して
インターネットに接続できていることをご確認ください。

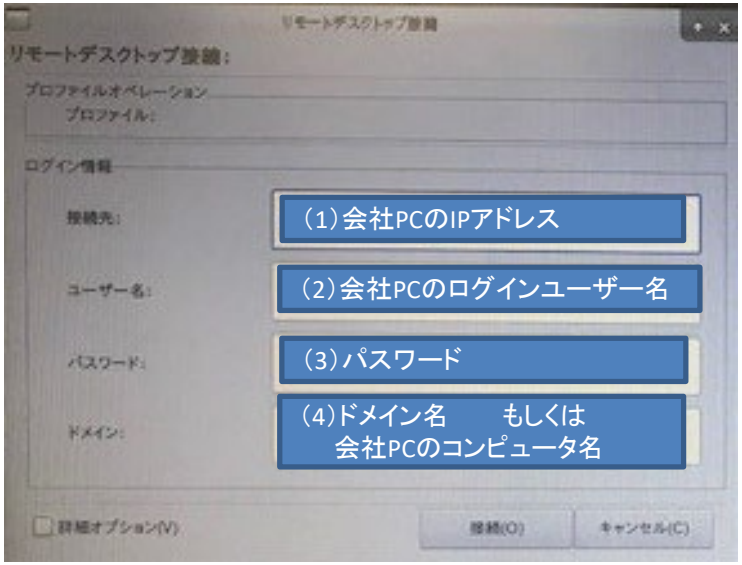
セコムトラストシステムズHP：https://www.secomtrust.net/



１８．リモートデスクトップ接続できない

原因１　リモートデスクトップ接続画面のログイン情報の入力が誤っている

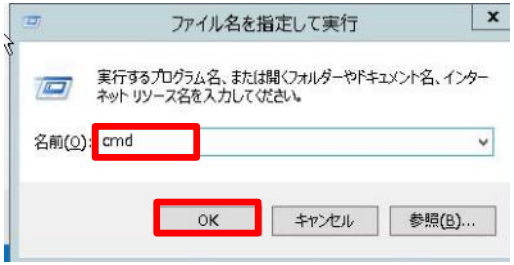
リモートデスクトップ接続のログイン情報が正しいか確認してください。



ログイン情報	入力内容
接続先	(1)会社PCのIPアドレス
ユーザー名	(2)会社PCにログインする際に使用するユーザー名
パスワード	(3)会社PCのログインユーザーのパスワード
ドメイン	(4)会社PCがドメインに所属している場合：ドメイン名 会社PCがワークグループ環境の場合：会社PCのコンピュータ名

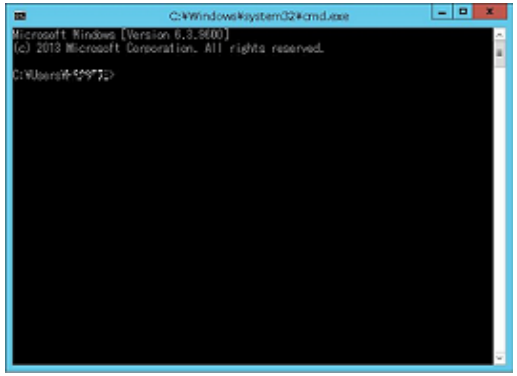
確認方法

①「Windows」ロゴを右クリック し、 「ファイル名を指定して実行」をクリックします。
　名前に「cmd」を入力し、「OK」をクリックします。

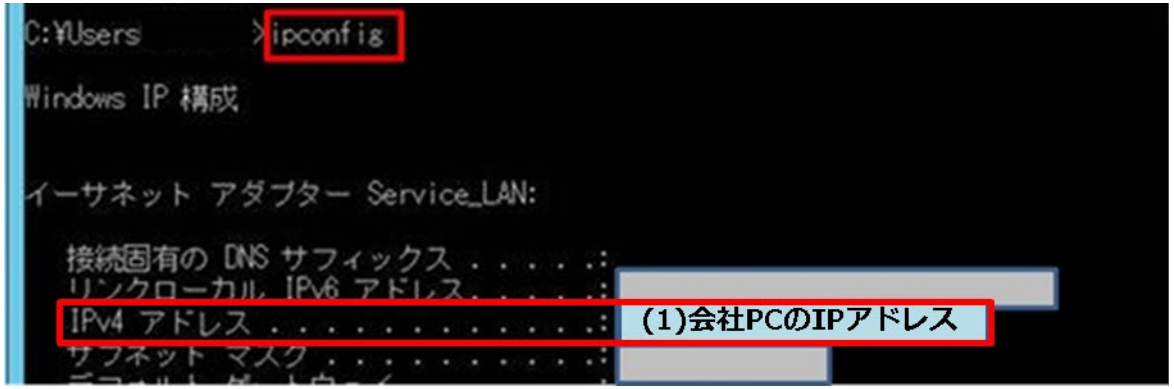


１８．リモートデスクトップ接続できない

②コマンドプロンプトが表示されます。



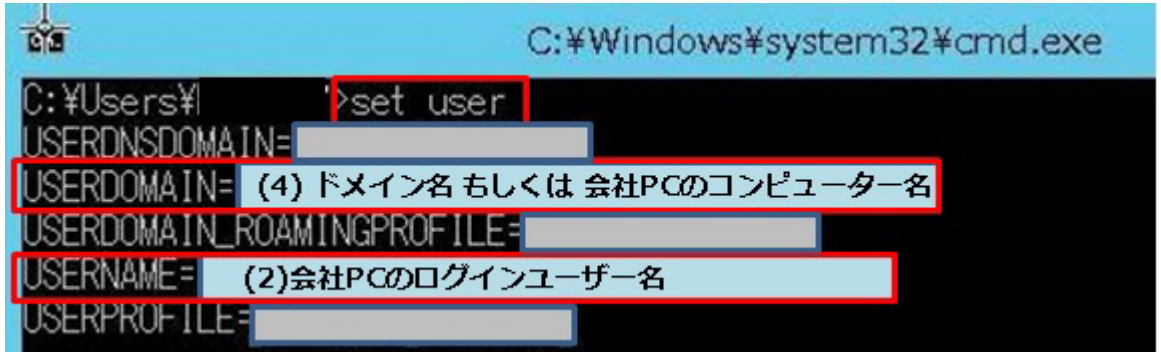
③コマンドプロンプトで「ipconfig」と入力してEnterキーを押してください。
「(1)会社PCのIPアドレス」にあたる「IPv4 アドレス」を確認してください。



１８．リモートデスクトップ接続できない

④コマンドプロンプトで「set user」と入力してください。
「(2)会社PCのログインユーザー名」にあたる「USERNAME」を確認してください。
「(4)ドメイン名　もしくは　会社PCのコンピューター名」にあたる「USERDOMAIN」を確認してください。

※（4）は会社PCがドメインに所属している場合 ドメイン名が表示され、
会社PCがワークグループ環境の場合 会社PC名が表示されます。

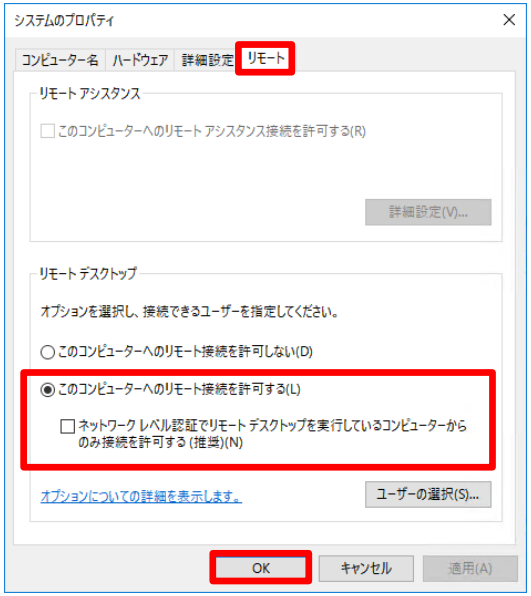


１８．リモートデスクトップ接続できない

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

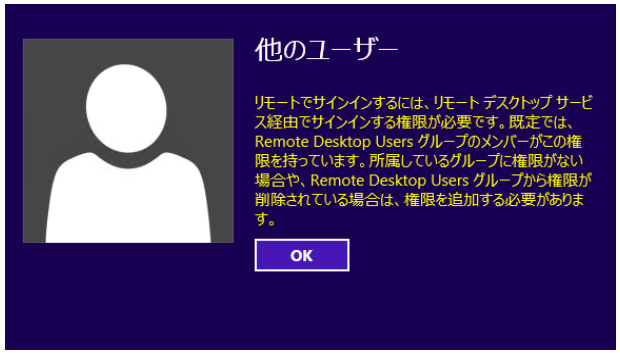
原因２　会社PCの設定でリモート接続を許可していない
会社PCにて、以下の項目を設定する必要があります。

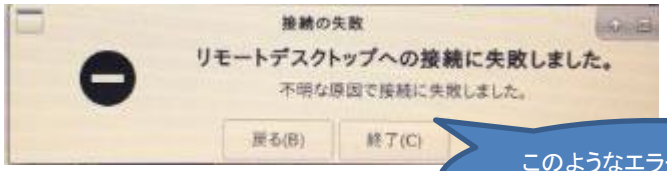
①会社PCに管理者権限のユーザーでログインします。
②「Windows」ロゴを右クリック し、 「システム」をクリックします。
③「システムの詳細設定」をクリックします。
④「リモート」タブより、「このコンピューターへのリモート接続を許可する」にチェックを入れ、
「ネットワークレベル認証でリモートデスクトップを実行しているコンピューターから
のみ接続を許可する」のチェックを外して「OK」をクリックしてください。



１８．リモートデスクトップ接続できない

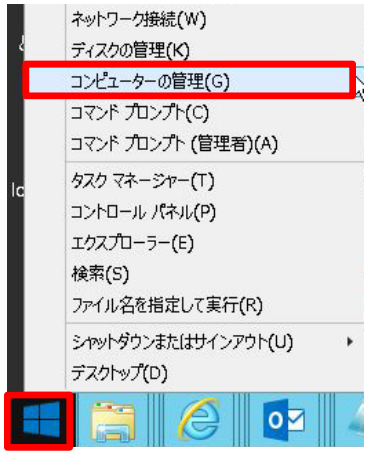
原因３　リモート接続する権限が付与されていない
リモートデスクトップ接続時に以下のようなエラーが出る場合、該当ユーザーが会社PCにリモートデスクトップする権限が付与されていません。会社PCにて設定変更をしてください。



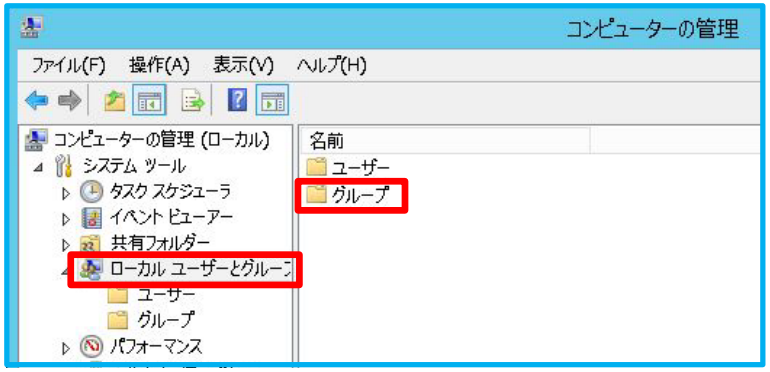


このようなエラーが出る場合もあります

①会社PCに管理者権限のユーザーでログインします。
「スタートメニュー」（Windowsマーク）を右クリック してメニューを表示し、
「コンピューターの管理」をクリックします。

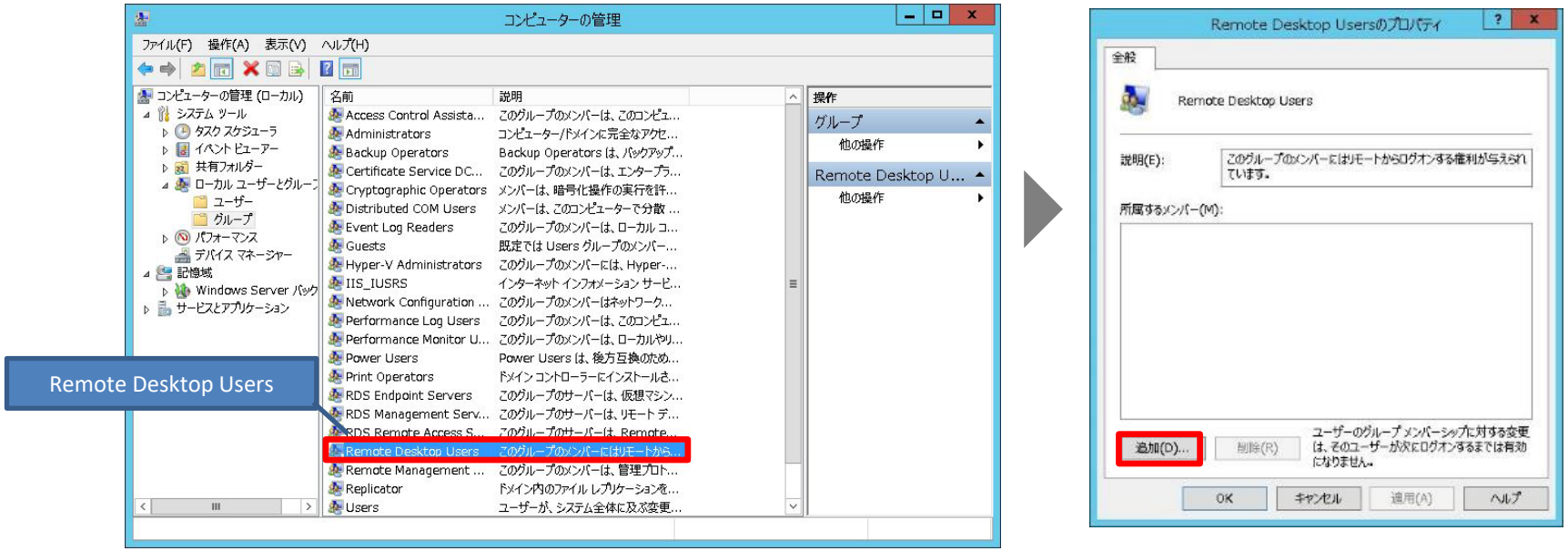


②「ローカルユーザーとグループ」をクリックし、「グループ」をダブルクリックします。

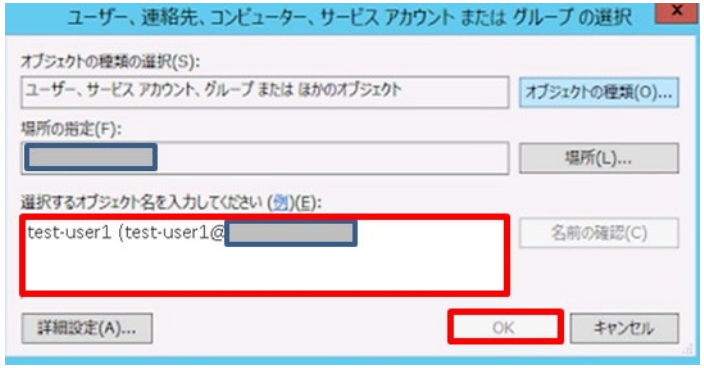


１８．リモートデスクトップ接続できない

③「Remote Desktop Users」をダブルクリックし、プロパティが表示されたら 「追加」をクリックします。

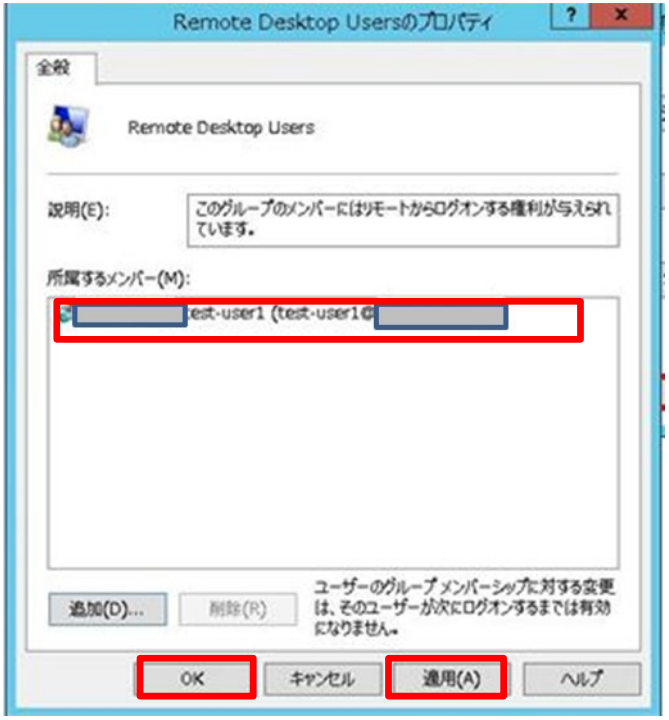


④「選択するオブジェクト名を入力してください」の項目でRemote Desktopでアクセスしたいユーザーを入力し、「OK」をクリックします。



１８．リモートデスクトップ接続できない

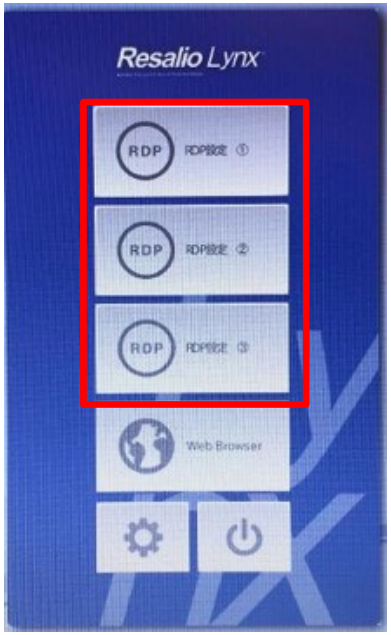
⑤「所属するメンバー」の項目に指定したユーザーが追加されていることを確認し、
「適用」 → 「OK」の順にクリックし、画面を閉じます。

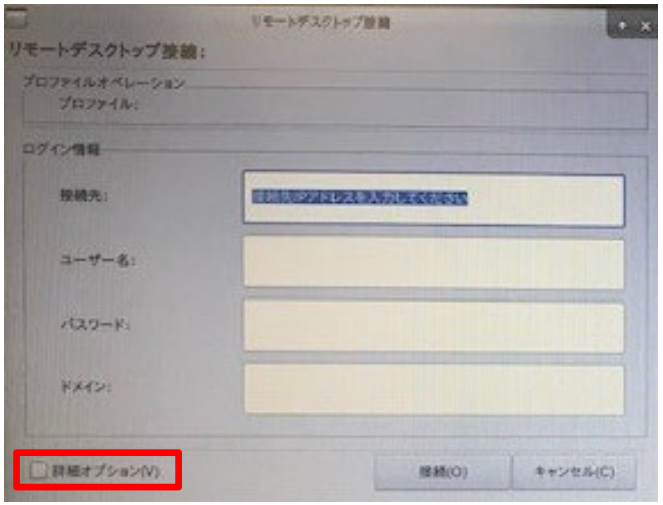


１９．リモートデスクトップ接続先情報の登録

USBリモート端末では、リモートデスクトップの接続先の情報（接続先のIPアドレス、ユーザー名、ドメイン）をプロファイルという単位で管理しています。
プロファイルの内容はユーザー自身で変更可能です。※パスワードは登録できません。

①メニュー画面で、接続情報を登録したい「RDP設定」ボタンをクリックします。
　(①～③まで登録できます)
「リモートデスクトップ接続」画面が表示されるので、「詳細オプション」をクリックします。

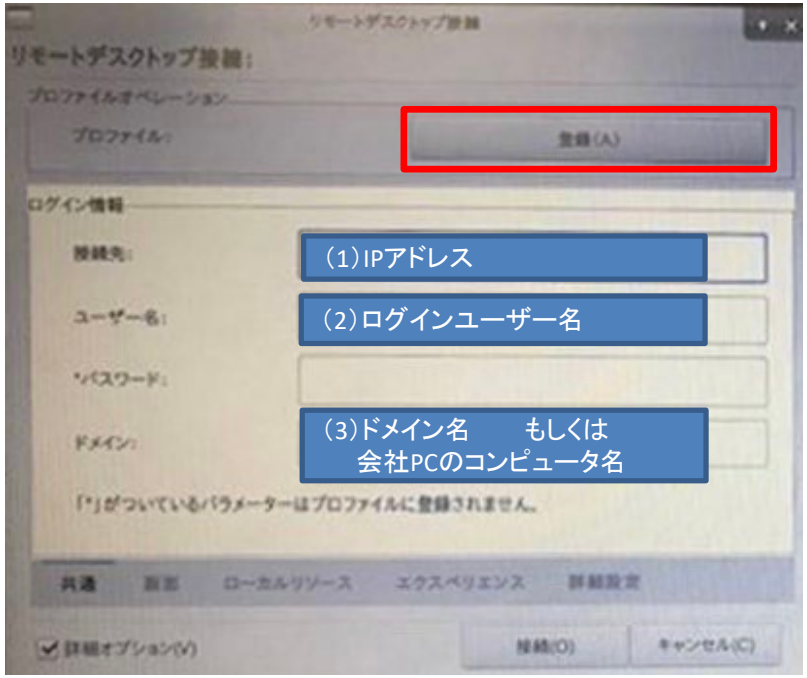




１９．リモートデスクトップ接続先情報の登録

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

②登録したいログイン情報を入力します。※パスワードは登録できません。
　入力後、「登録」をクリックします。



ログイン情報	入力内容
接続先	(1)会社PCのIPアドレス
ユーザー名	(2)会社PCにログインする際に使用するユーザー名
ドメイン	(3)会社PCがドメインに所属している場合：ドメイン名 会社PCがワークグループ環境の場合：会社PCのコンピュータ名

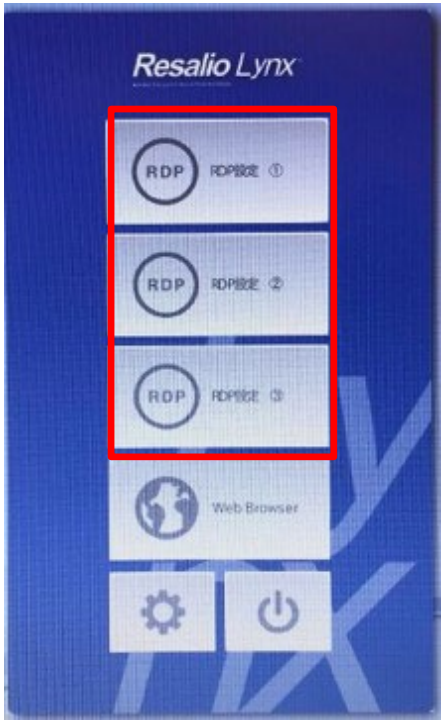
１９．リモートデスクトップ接続先情報の登録

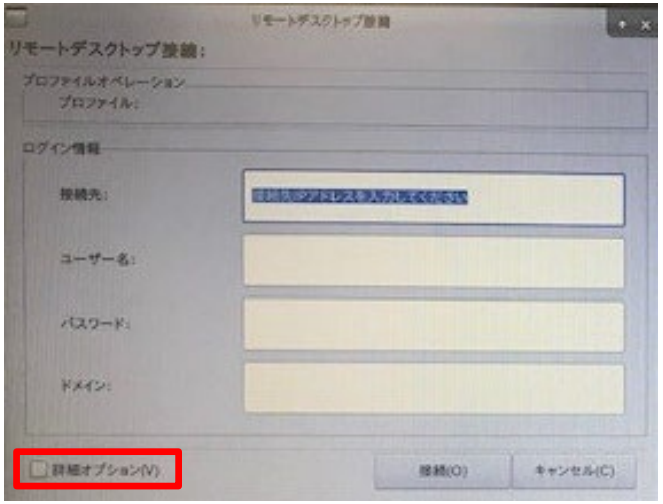
③「プロファイルを登録」画面が表示されるので、「変更」→「OK」ボタンをクリックします。

④設定を保存するため「本章１．USBリモート端末設定変更後の保存方法」を実行します。

２０．リモートデスクトップ接続先情報の変更・削除

①メニュー画面で、接続情報を変更したい「RDP設定」ボタンをクリックします。
(①～③まで登録できます)
「リモートデスクトップ接続」画面が表示されるので、「詳細オプション」をクリックします。





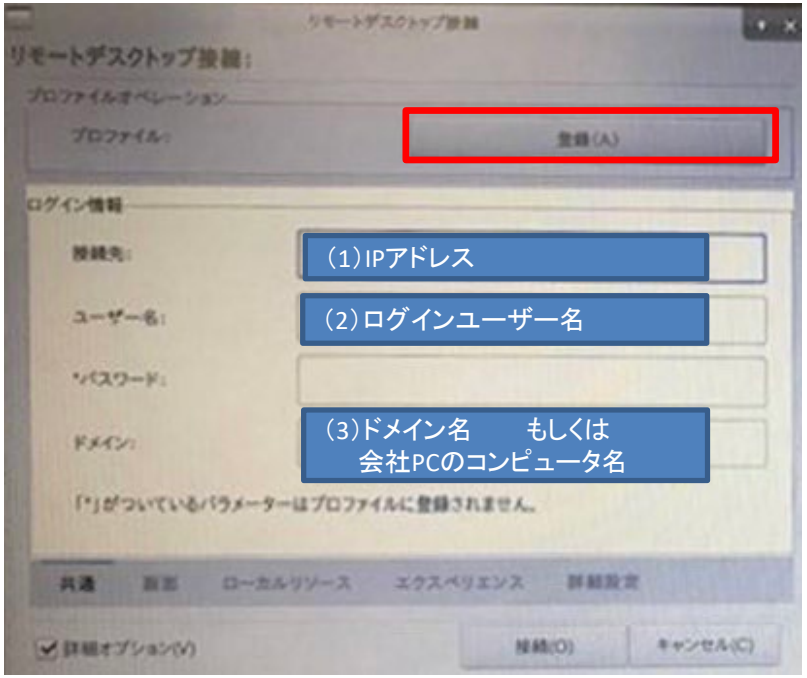
２０．リモートデスクトップ接続先情報の変更・削除

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

②リモートデスクトップ接続先情報を変更する場合、下記(1)～(3)の設定を変更します。
リモートデスクトップ接続先情報を削除する場合、下記(1)～(3)の設定を全て削除してください。

設定を変更したら、「登録」をクリックします。

ログイン情報	入力内容
接続先	(1)会社PCのIPアドレス
ユーザー名	(2)会社PCにログインする際に使用するユーザー名
ドメイン	(3)会社PCがドメインに所属している場合：ドメイン名 会社PCがワークグループ環境の場合：会社PCのコンピュータ名



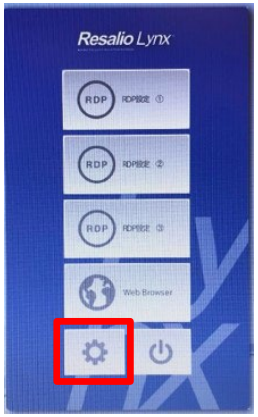
２０．リモートデスクトップ接続先情報の変更・削除

③「プロファイルを登録」画面が表示されるので、「変更」→「OK」ボタンをクリックします。

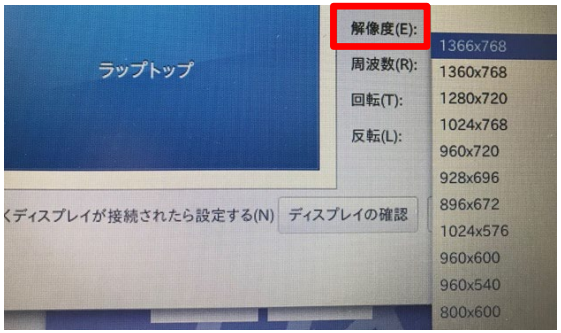
④設定を保存するため「本章１．USBリモート端末設定変更後の保存方法」を実行します。

２１．解像度を変更したい

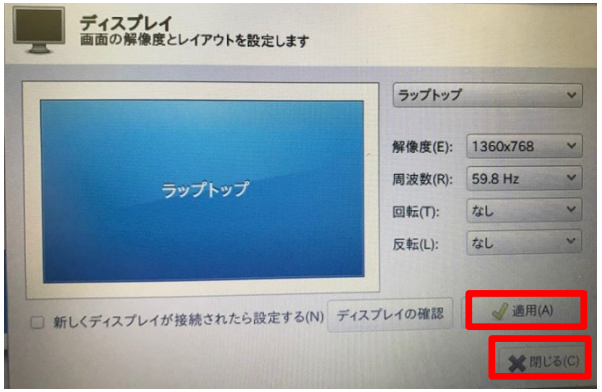
①メニュー画面の「コントロールパネル(歯車マーク) 」→「モニター設定」を選択します。



②高い解像度の設定項目があれば、そちらを選択してください。



←解像度を選択



←「適用」を選択し、「閉じる」で画面を閉じる

※高い解像度が表示されない場合

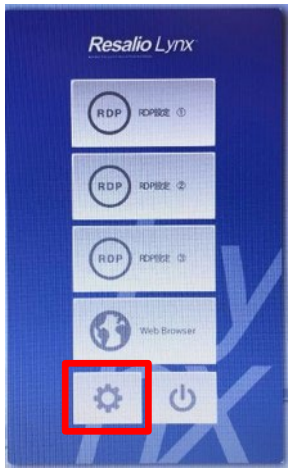
USBリモート端末が、お使いのモニターに対応していません。

ノートPCの画面が使えない場合、別途外部モニターを繋ぐことで利用できることがあります。

「適用」 → 「OK」の順にクリックし、画面を閉じます。

２２．マルチディスプレイを利用したい

①PCとマルチディスプレイとして利用したいモニターをケーブルで接続します。
②メニュー画面の「コントロールパネル(歯車マーク)」をクリックします。
③コントロールパネルが表示されたら 「モニター設定」をダブルクリックします。

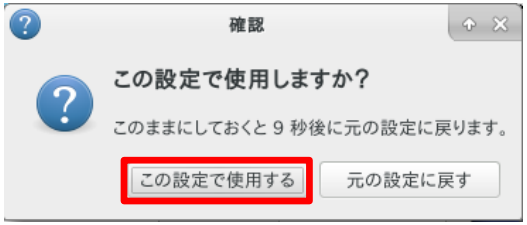


④使用したいモニターを選択し、「このディスプレイ出力を使う」にチェックを入れます。

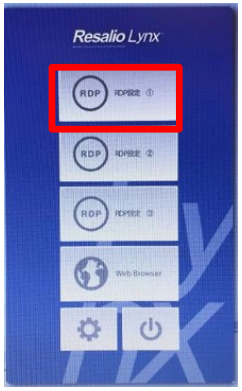
※この画面で、使用したいモニターが表示されない場合は、
モニターをご利用いただけません。

２２．マルチディスプレイを利用したい

⑤「確認」ダイアログが表示されるので、「この設定で使用する」をクリックして適用します。



⑥メニュー画面の 「RDP設定」 をクリックし、通常のリモート接続操作を行います。



⑦正常に接続できると、会社PCのデスクトップが表示され、マルチディスプレイが利用できます。

２３．リモートアクセス中に切断される

リモートアクセス後、利用中に意図せず切断されてしまう場合は、以下項目をご確認ください。

【原因】

------無線LAN(Wi-Fi)をご使用いただいている場合------

①Wi-Fiルーターのセキュリティ設定

Wi-Fiルーターのセキュリティ（暗号化形式）がWEPに設定されている場合、WPA2に変更することで事象が改善される場合があります。

②Wi-Fiルーターが省電力モードに設定されている

省電力モードになっていると、VPN接続が途中で切断されることがあります。
省電力モードをオフにしてお試しください。

③Wi-Fiルーターと自宅PCの距離

Wi-Fiルーターから自宅PCが遠く離れた場合は、接続が不安定となります。
自宅PCを近くに置くことで改善される場合があります。

２３．リモートアクセス中に切断される

----有線LANをご使用いただいている場合----

④LANケーブルの不良（故障、圧迫等）

LANケーブルの接続不良により接続が切断されることがあります。
LANケーブルを交換して接続できるかどうかご確認ください。

----その他----

⑤お使いのインターネット回線の通信障害

インターネット回線、並びにプロバイダが不安定になると、接続が切断されてしまいます。
通常のインターネットアクセスが可能か確認し、不可能な場合はプロバイダにご確認ください。

⑥データ通信量の上限を超えている

データ通信量の上限が設定されているポケットWi-Fiや、スマートフォンからのテザリングをご使用いただいている場合、所定のデータ通信量を超えると通信制限がかかり接続が切断されることがあります。
ご契約内容をご確認の上、自宅環境に固定回線がある場合にはそちらでお試しください。

第３章
VPNゲートウェイに関する事項

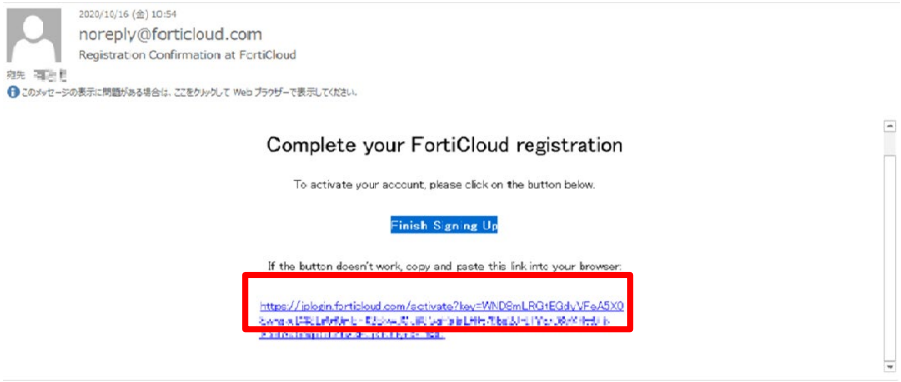
1．FortiCloud管理Webシステム 利用開始手順

サービス管理者を登録・変更すると、申請いただいたサービス管理者様のメールアドレス宛に、FortiCloud管理Webシステム（以下管理Webシステム）よりメールが届きます。利用開始手続きとして、次ページ以降の手順を実施してください。

なお、管理WebシステムはInternetExplorerに対応しておりません。
ブラウザでのアクセス時にはFireFoxやGoogleChrome、MicrosoftEdgeといったInternetExplorer以外のブラウザをご利用ください。

1．FortiCloud管理Webシステム 利用開始手順

①ご契約後noreply@forticloud.comより招待メールがサービス管理者のメールアドレス宛てに届いております。届いた招待メール内のリンクを選択します。

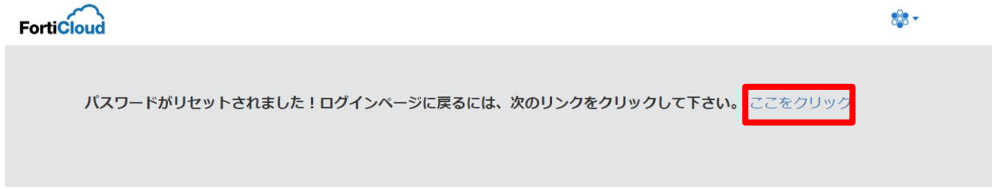


②パスワード入力画面が表示されるので、ログイン時に使用したいパスワードを入力し「サブミット」をクリックします。

1．FortiCloud管理Webシステム 利用開始手順

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

③「パスワードがリセットされました！」が表示されたら、同ページ内の「ここをクリック」をクリックします (※)。
※同内容が英語で表示される場合もあるので、その場合は同ページ内の「here」をクリックします。

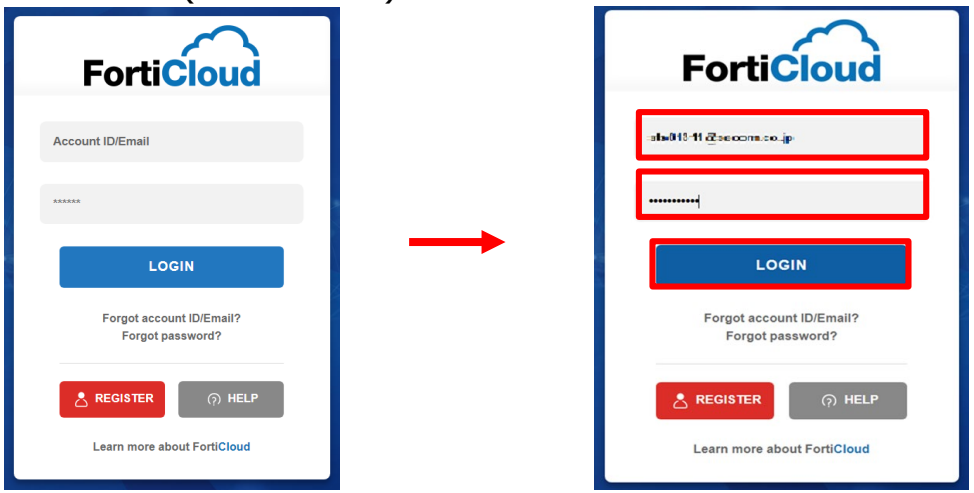


④FortiCloudのトップページに遷移するので、画面右上の「ログイン」をクリックします。

1．FortiCloud管理Webシステム 利用開始手順

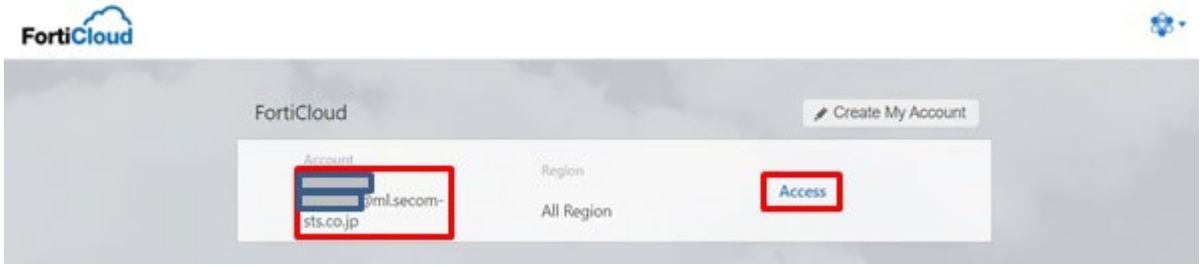
⑤「Single Sign On Support ～」のポップアップが表示された場合は「Continue」をクリックします。

⑥ログイン画面が表示されるので、<Account ID/Email>欄にユーザ名(メールアドレス)を、<******>(パスワード)欄に②で登録したパスワードを入力し、「LOGIN」をクリックします。

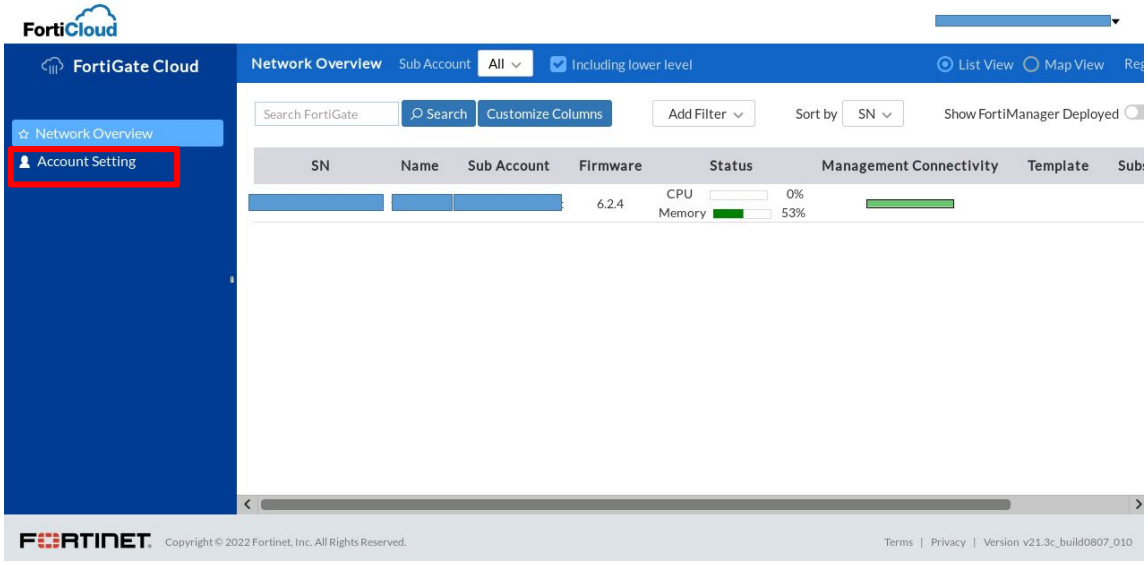


1．FortiCloud管理Webシステム 利用開始手順

⑦「****@ml.secom-sts.co.jp」というアカウントが表示された場合は、「Access」をクリックします。

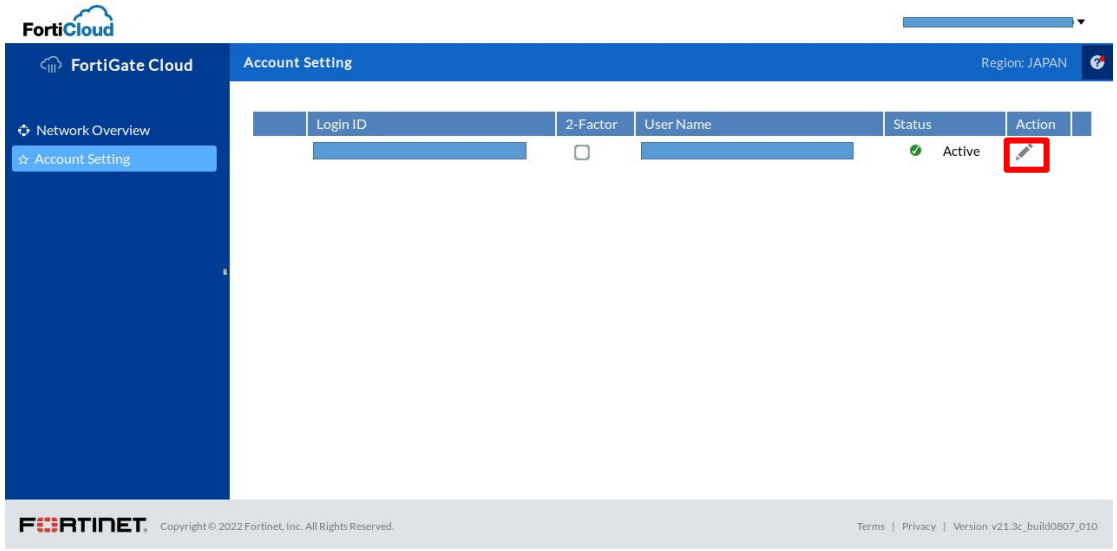


⑧ログインに成功すると、FortiGate Cloudの画面が表示されます。
初回は仕様上言語が英語になっているので、日本語に変更します。
「Account Setting」をクリックします。

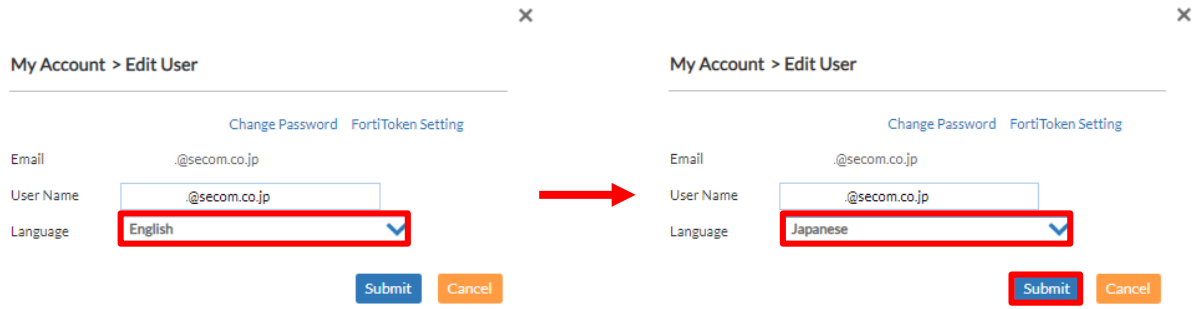


1．FortiCloud管理Webシステム 利用開始手順

⑨「User Name」が自身のメールアドレスであることを
確認し、Action欄の鉛筆マークをクリックします。



⑩ユーザー編集画面が表示されるので、「Language」をプルダウンメニューからJapaneseに
変更し、「Submit」をクリックします。



1．FortiCloud管理Webシステム 利用開始手順

⑪画面右上の自身のメールアドレスをクリックし、プルダウンメニューから「Logout」を選択し、FortiCloudからログアウトします。

⑫再度ログインし、日本語表記になっていれば言語変更完了です。
この後の運用方法については、「本章　2．FortiCloud管理Webシステム ログ確認手順」を参照ください。

2．FortiCloud管理Webシステム ログ確認手順

2.1 概要

FortiCloud管理Webシステムでは、以下情報をログを通じて確認が可能です。

①VPN接続ユーザ情報 (VPN接続実施時間、認証の成功/失敗記録　等)

… VPNログにより確認可能です。
確認方法は「2.3 VPNログ確認手順」をご覧ください。

②VPN接続後の社内端末アクセス情報 (アクセス実施時間、ユーザ情報　等)

… トラフィックログにより確認可能です。
確認方法は「2.4 トラフィックログ確認手順」をご覧ください。

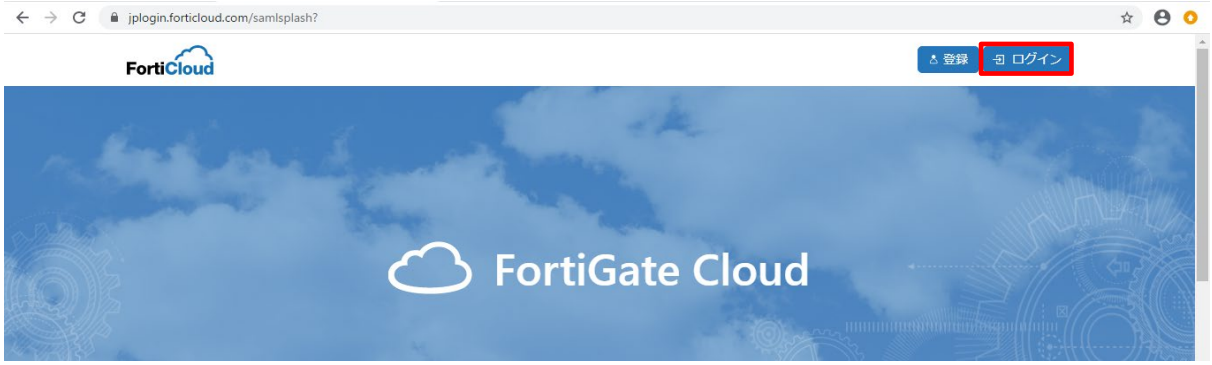
2．FortiCloud管理Webシステム ログ確認手順

2.2 共通確認手順

①Webブラウザから以下URLにアクセスします。

URL	https://jplogin.forticloud.com/

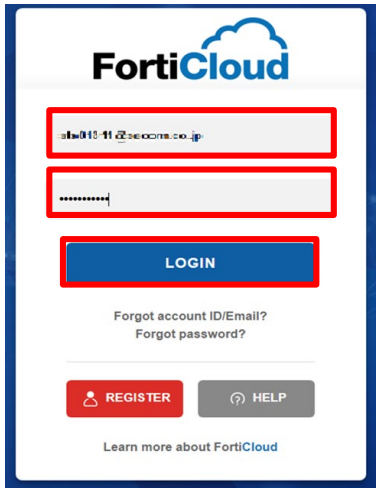
②画面右上の「ログイン」をクリックします。



2．FortiCloud管理Webシステム ログ確認手順

2.2 共通確認手順

③ユーザ名とパスワードを入力して「LOGIN」をクリックします。



④ログインに成功したら「アクセス」をクリックします。

2．FortiCloud管理Webシステム ログ確認手順

2.2 共通確認手順

⑤管理対象の機器一覧が表示されますので、ログ確認を行いたい機器をクリックします。
※図中ではSN(シリアル番号)、名称(ホスト名)、サブアカウントは伏せています。
クリックすると「>分析」、「>Sandbox」が出てくるので「>分析」を
クリックします。

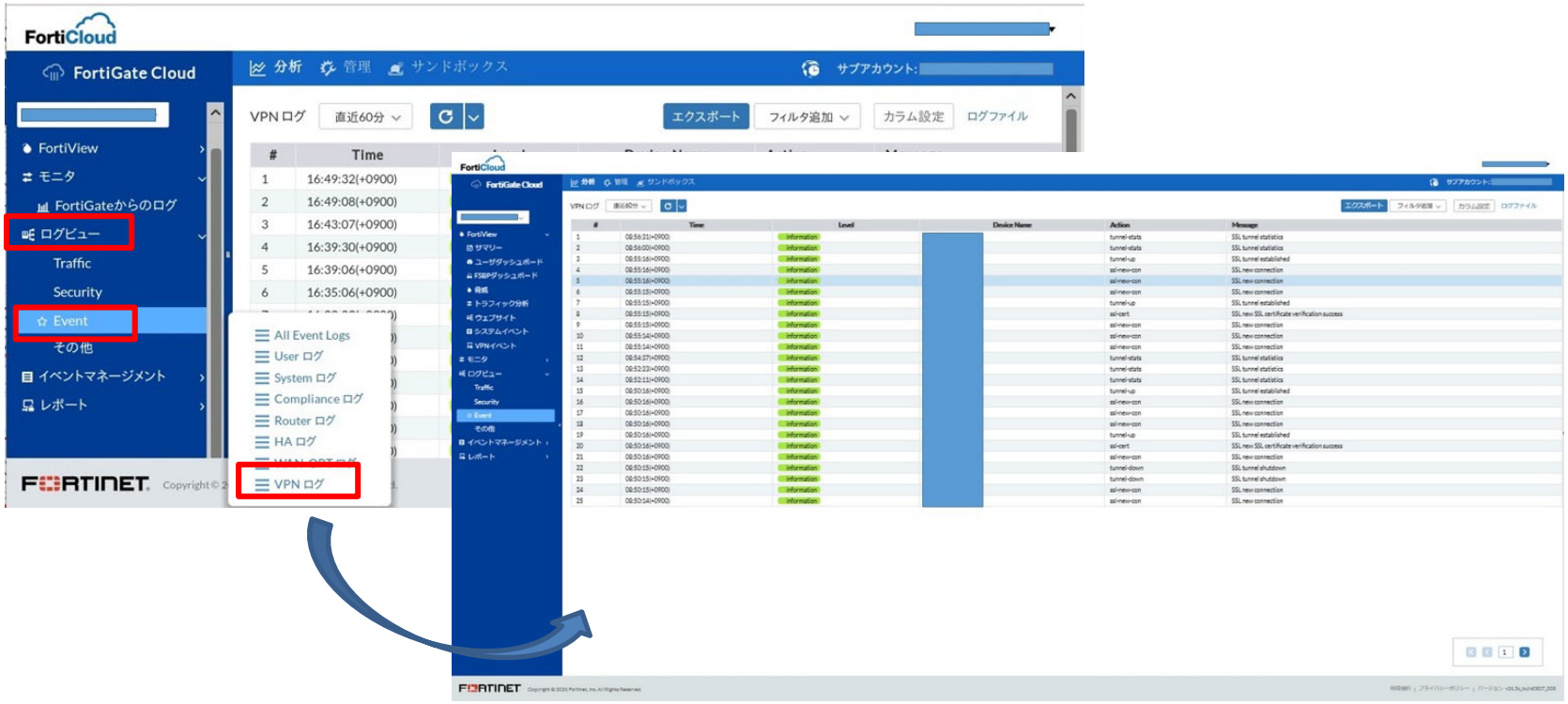
2．FortiCloud管理Webシステム ログ確認手順

2.2 共通確認手順

⑥-1【VPNログ】

画面遷移後、左メニューで「ログビュー」をクリックし、出てくる中項目の中から
「Event」をクリック⇒「VPNログ」をクリックすればリモートアクセスログが、表示されます。

【VPNログ】



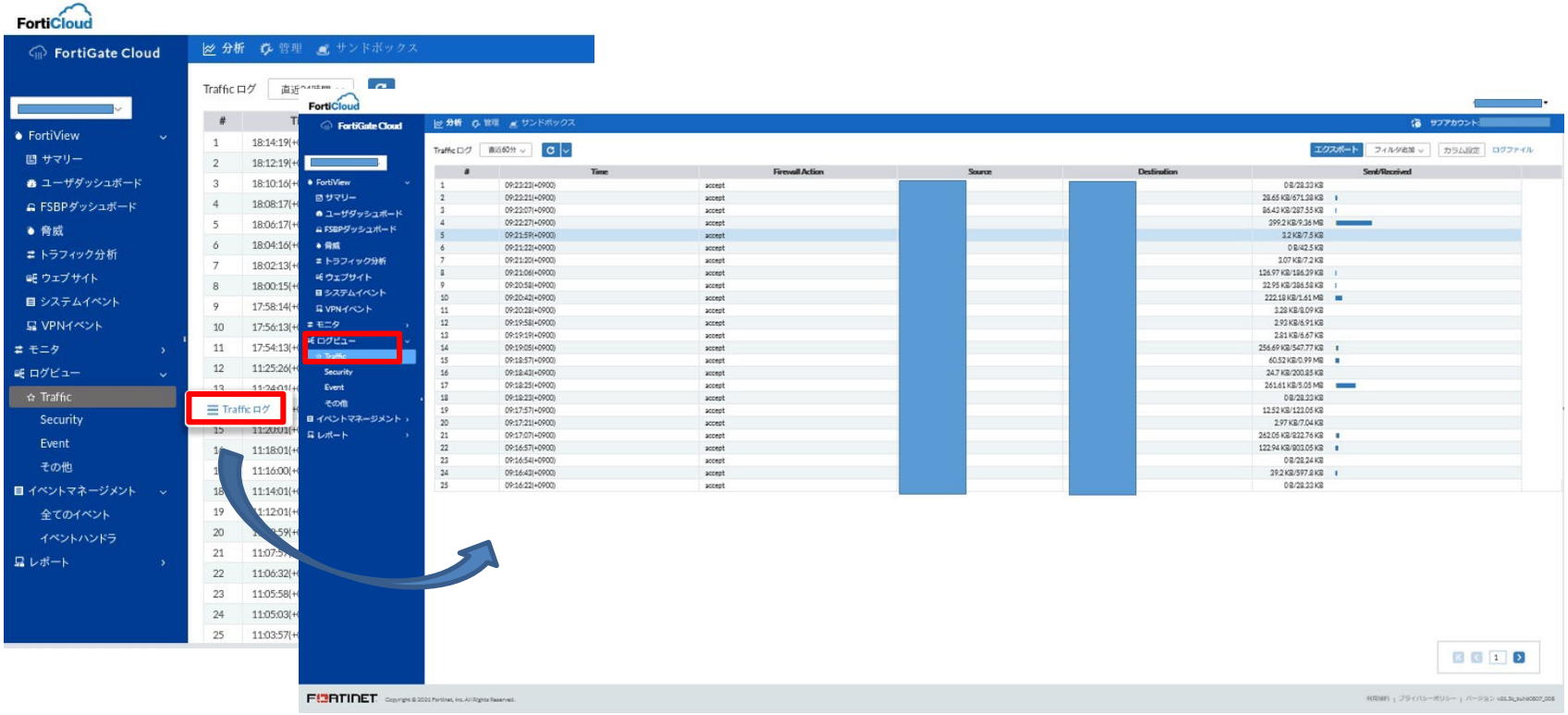
2．FortiCloud管理Webシステム ログ確認手順

2.2 共通確認手順

⑥-2【トラフィックログ】

画面遷移後、左メニューで「ログビュー」をクリックし、出てくる中項目の中から
「Traffic」をクリック⇒「Trafficログ」をクリックすればトラフィックログが、表示されます。

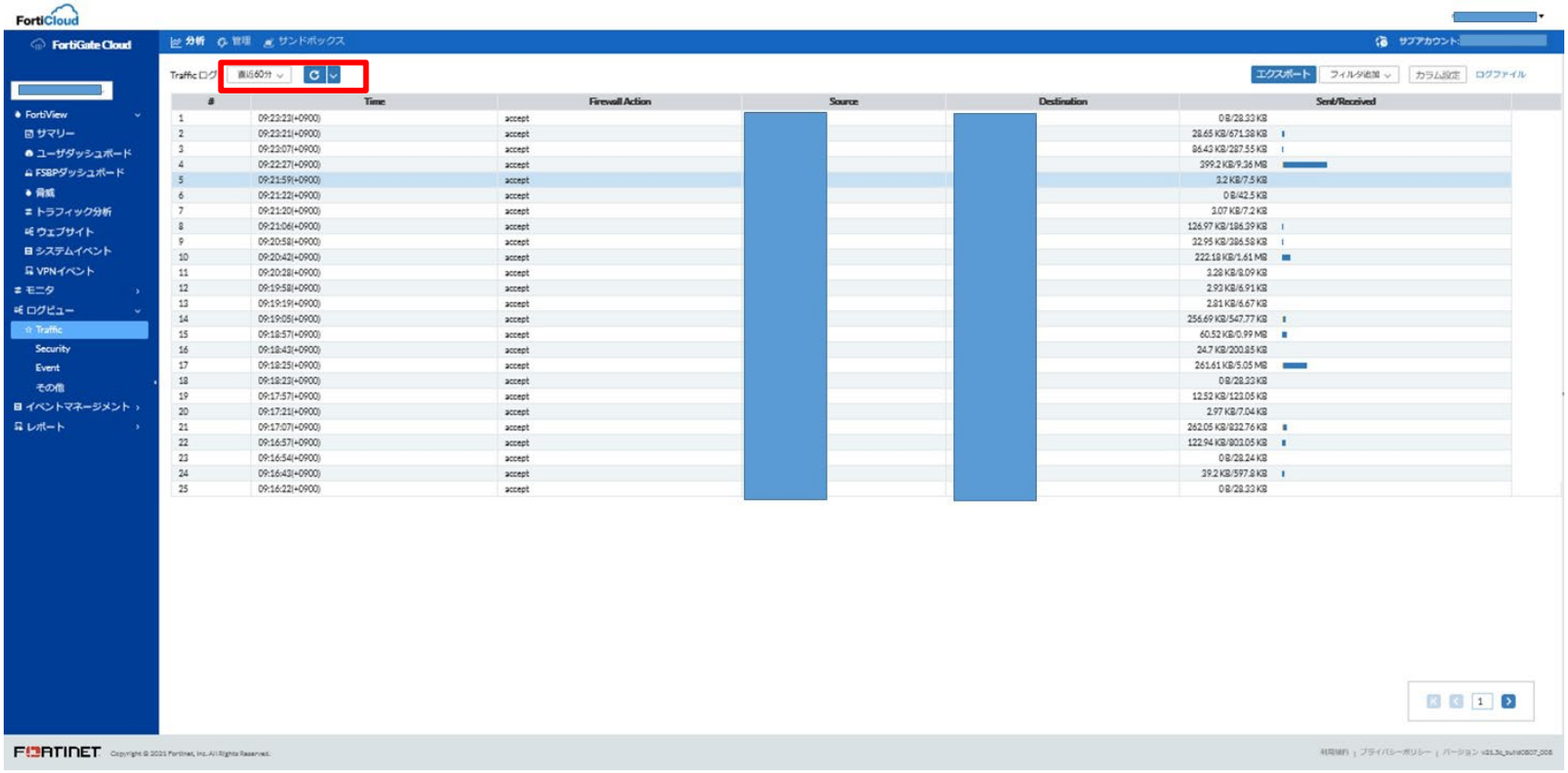
【トラフィックログ】



2．FortiCloud管理Webシステム ログ確認手順

2.2 共通確認手順

⑦左上のプルダウンメニューから時間帯指定のログ表示が可能です。
デフォルトでは直近60分のログしか表示されないので、適宜時間帯の指定が必要です。

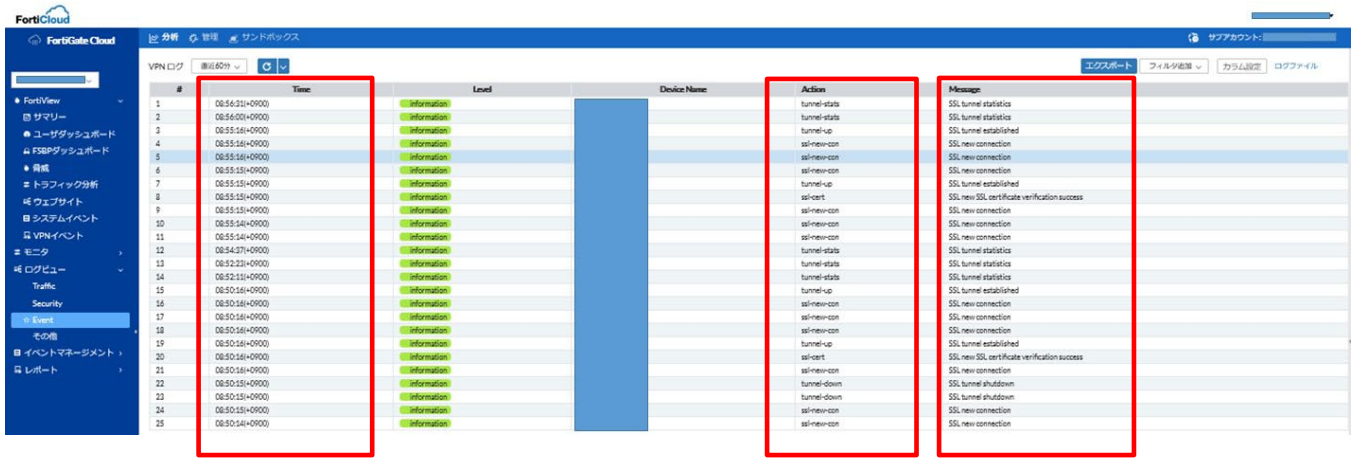


時間帯は「直近60分」「直近24時間」「直近7日」「直近30日」「指定」の5パターンから選択できます。
「指定」を選択した場合、ログ表示開始日時と終了日時を指定することで、その期間中のログが表示されます。

2．FortiCloud管理Webシステム ログ確認手順

2.3 VPNログ確認手順

①「2.2 共通確認手順」の ⑥-1 の手順に従って、VPNログ画面まで遷移します。
その後、表示されたログを確認します。



各フィールドの意味は以下の通りです。

Time　　：ログが記録された時間です。

Action　　：各ログの示す動作です。各動作の説明は以下の通りです。

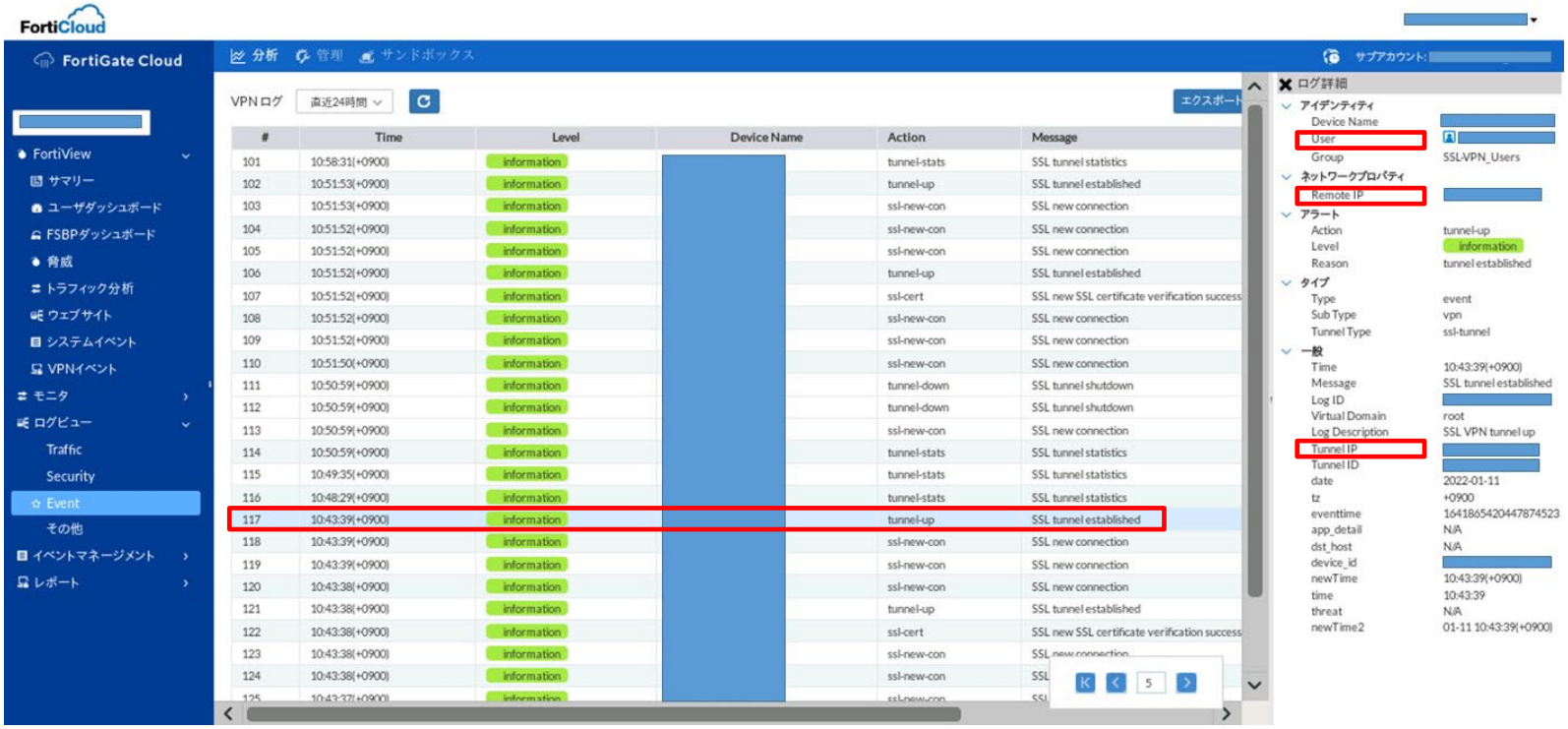
- tunnel-up...VPN接続ユーザの認証成功、クライアントアドレス割り当て済
- tunnel-down... VPN接続ユーザの接続切断
- tunnel-stats…70分ごとに記録される、 VPN接続ユーザセッションログ
- ssl-login-fail...パスワード不一致等の要因により、認証失敗

Message　　：ログの内容です。

2．FortiCloud管理Webシステム ログ確認手順

2.3 VPNログ確認手順

② 確認したいログをダブルクリックすると、右メニューで詳細情報が確認できます。



詳細情報でのみ確認出来る情報の中で、重要な情報を以下に記載します。

User　　：VPN接続を実施しているユーザIDです。

Remote IP　　：VPN接続ユーザの送信元グローバルアドレスです。

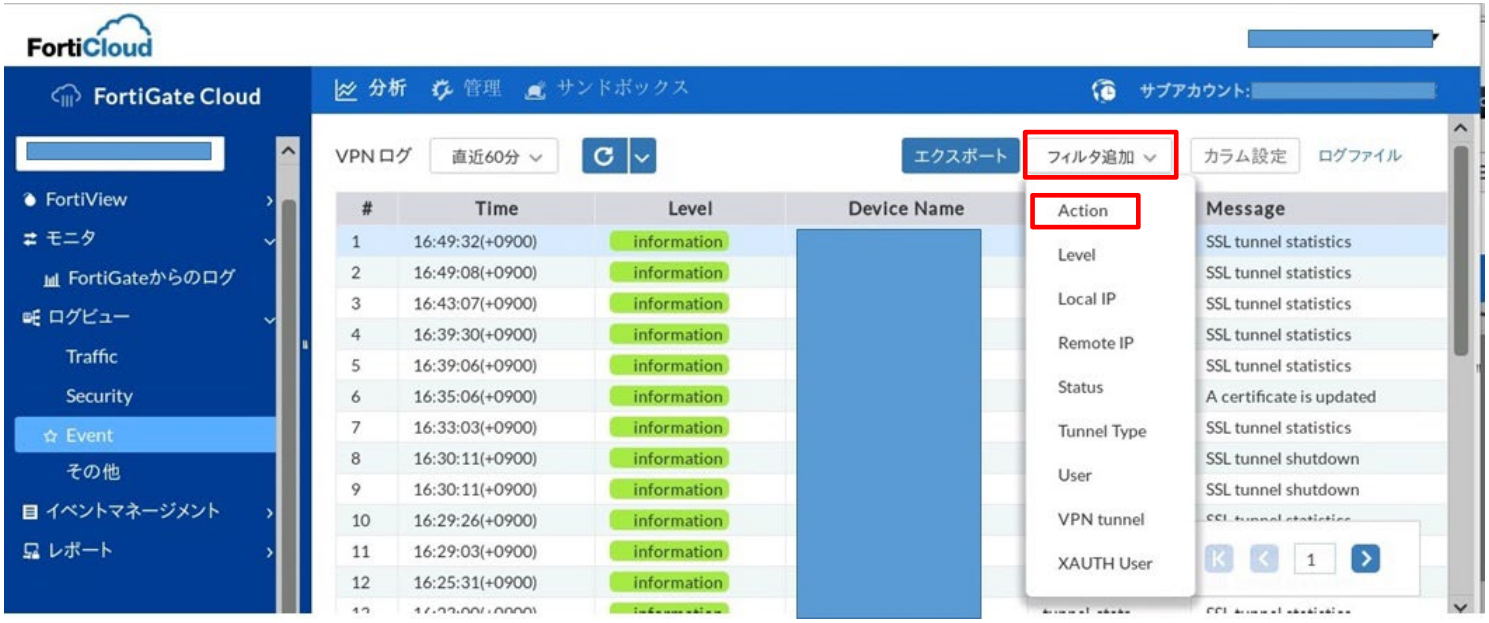
Tunnel IP　　：VPN接続ユーザに割り当てられた社内接続用アドレスです。

2．FortiCloud管理Webシステム ログ確認手順

2.3 VPNログ確認手順

③ VPN接続開始時のログは、以下手順でログの絞り込みを行うことで確認可能です。

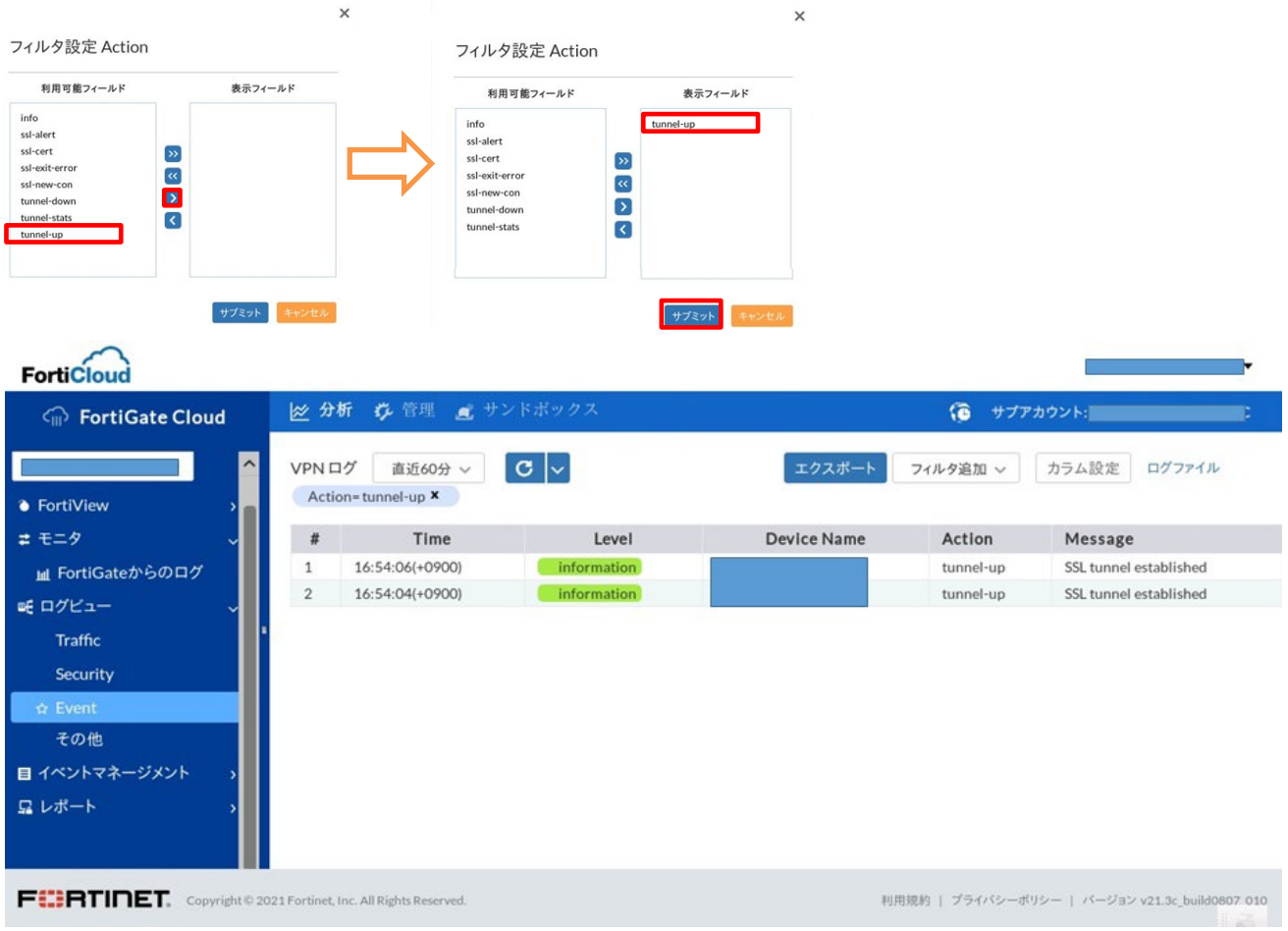
まず、ログ画面右上の「フィルタ追加」を選択し、表示されたプルダウンメニューから「Action」を選択します。



2．FortiCloud管理Webシステム ログ確認手順

2.3 VPNログ確認手順

「tunnel-up」を選択して「>」をクリックし、表示フィールドに移動したら「サブミット」をクリックすることで表示されます。

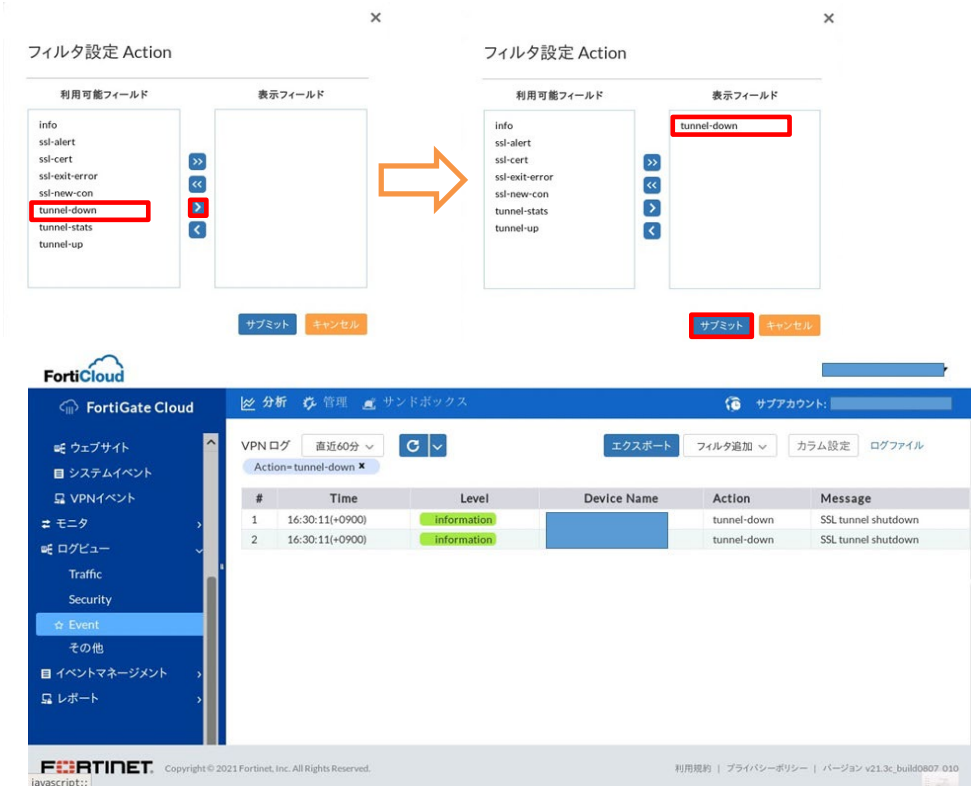


2．FortiCloud管理Webシステム ログ確認手順

2.3 VPNログ確認手順

④ ③と同様に、VPN接続終了時のログが確認可能です。

ログ画面右上の「フィルタ追加」を選択し、表示されたプルダウンメニューから「Action」を選択した後、 「tunnel-down」を選択して「>」をクリックし、表示フィールドに移動したら「サブミット」をクリックすることで表示されます。

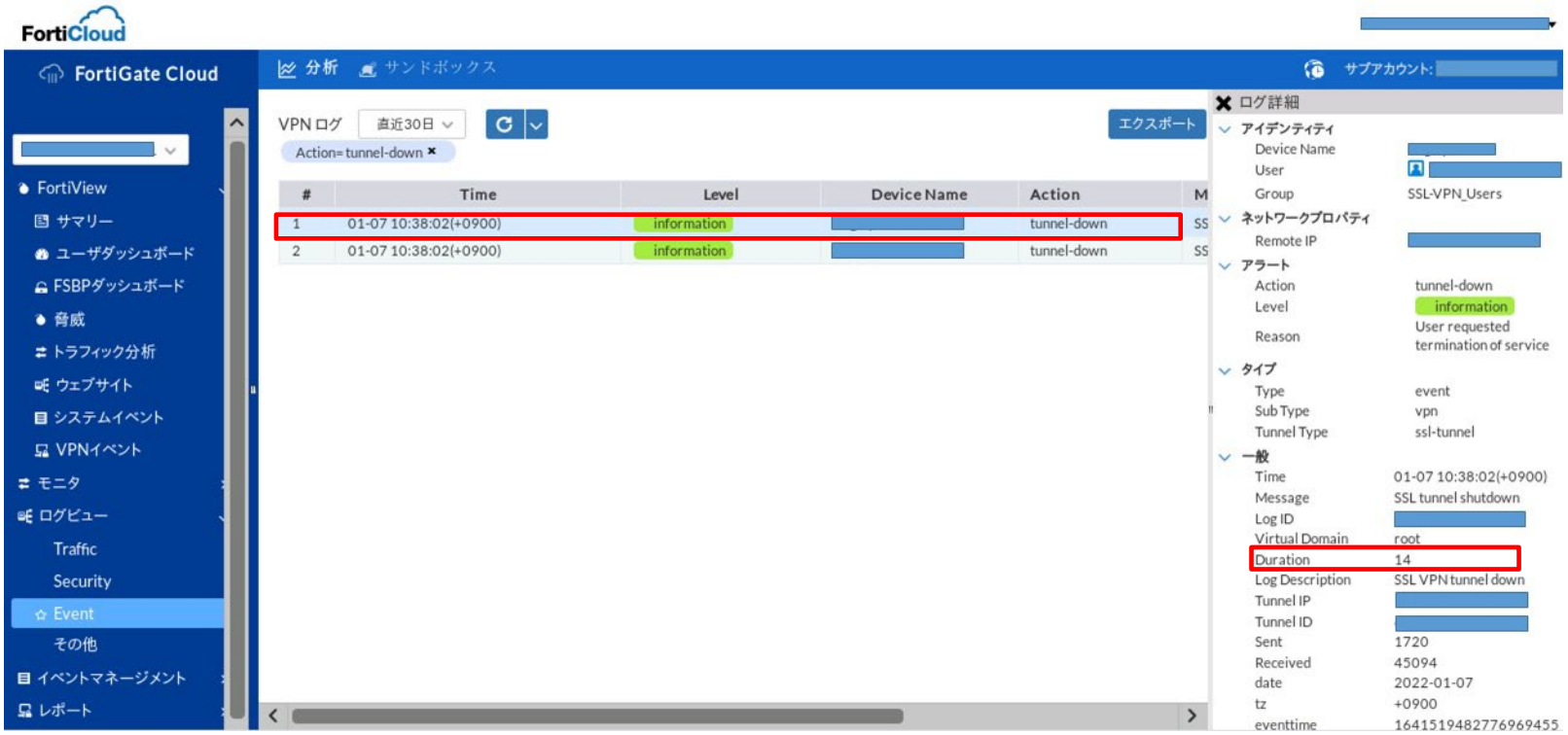


2．FortiCloud管理Webシステム ログ確認手順

2.3 VPNログ確認手順

VPN接続終了時のログからユーザの接続時間が確認可能です。

確認したいログをダブルクリックし、詳細情報を表示させます。
「Duration」がユーザの持続時間（単位：秒）です。



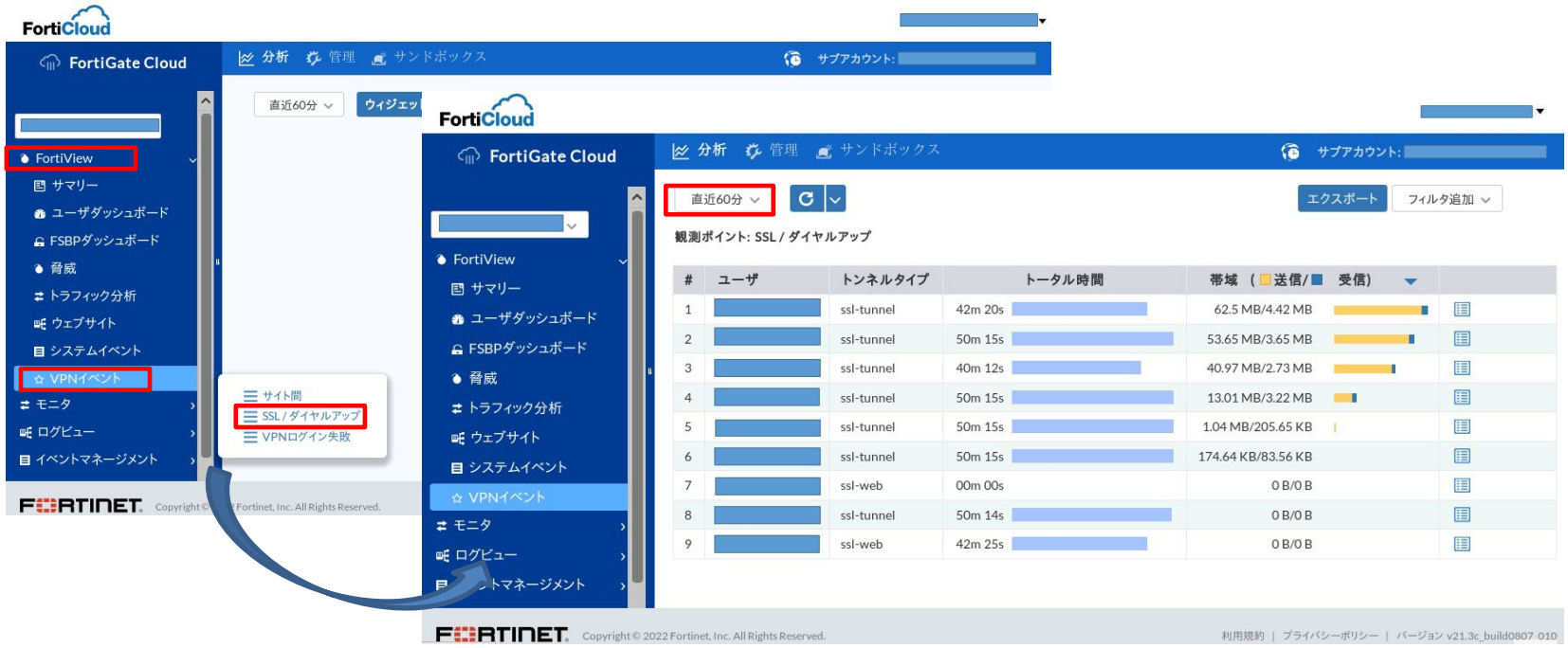
2．FortiCloud管理Webシステム ログ確認手順

2.3 VPNログ確認手順

（補足）

FortiView機能では、特定期間のユーザの接続時間、通信量がチャートで確認できます。

左メニューで「FortiView」をクリックし、出てくる中項目の中から「VPNイベント」をクリック
⇒「SSL／ダイヤルアップ」をクリックします。
期間を変更するには、左上のプルダウンメニューから時間帯を指定します。

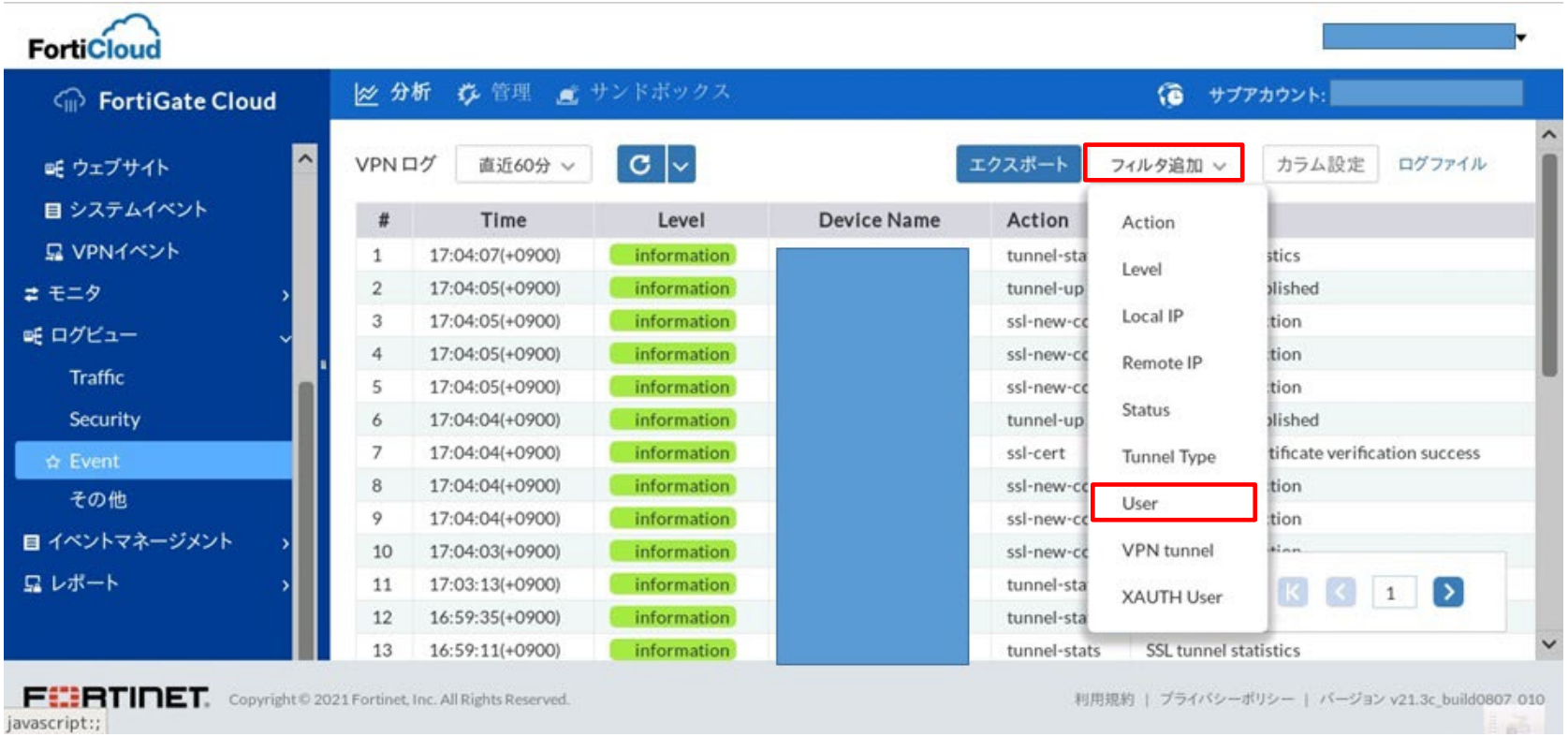


2．FortiCloud管理Webシステム ログ確認手順

2.3 VPNログ確認手順

⑤ 特定ユーザのVPN接続関連ログのみ表示させることが可能です。

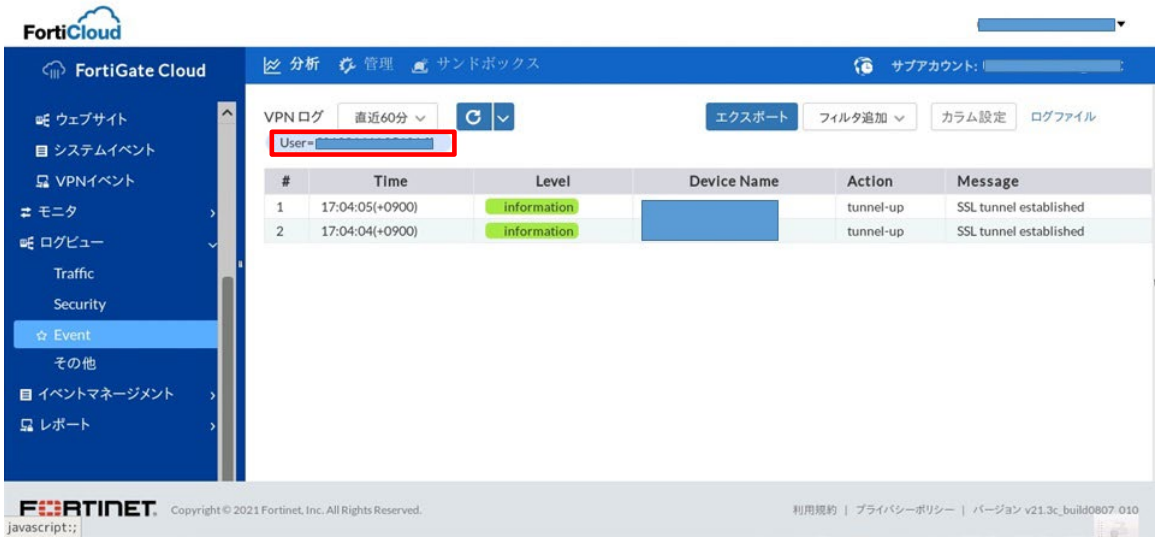
まず、ログ画面右上の「フィルタ追加」を選択し、表示されたプルダウンメニューから「User」を選択します。



2．FortiCloud管理Webシステム ログ確認手順

2.3 VPNログ確認手順

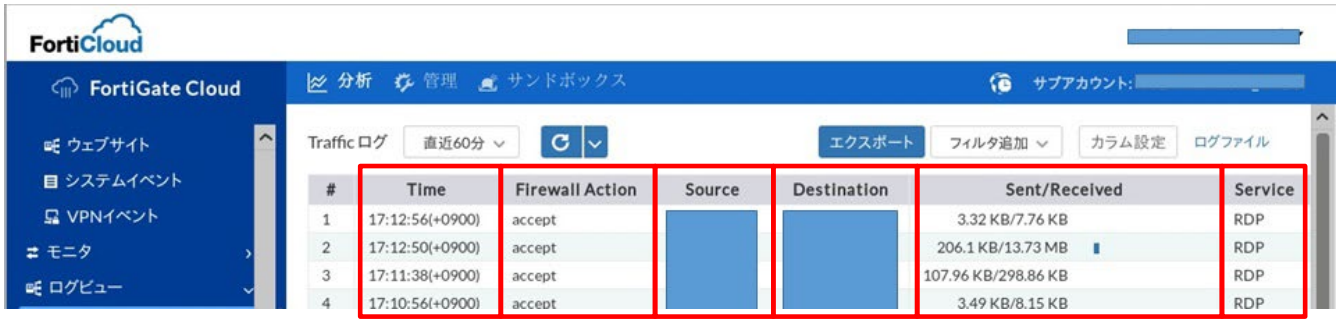
検索したいユーザIDを選択して「>」をクリックし、表示フィールドに移動したら「サブミット」をクリックすることで表示されます。



2．FortiCloud管理Webシステム ログ確認手順

2.4 トラフィックログ確認手順

①「2.2 共通確認手順」の ⑥-2 の手順に従って、トラフィックログ画面まで遷移します。
その後、表示されたログを確認します。



各フィールドの意味は以下の通りです。

Time ：ログが記録された時間です。

Firewall Action ：VPNゲートウェイ通過時の通信動作です。各動作の説明は以下の通りです。

- accept...許可され、正常に通信が終了
- client-rst...許可され、クライアント起因で通信が中断
- sever-rst...許可され、サーバ起因で通信が中断
- deny...許可されず、通信に失敗

Source ：送信元アドレスです。リモートアクセス認証後、VPNゲートウェイによりクライアントに割り当てられたアドレスとなります。

Destination ：宛先アドレスです。RDP先となる社内端末のアドレスとなります。

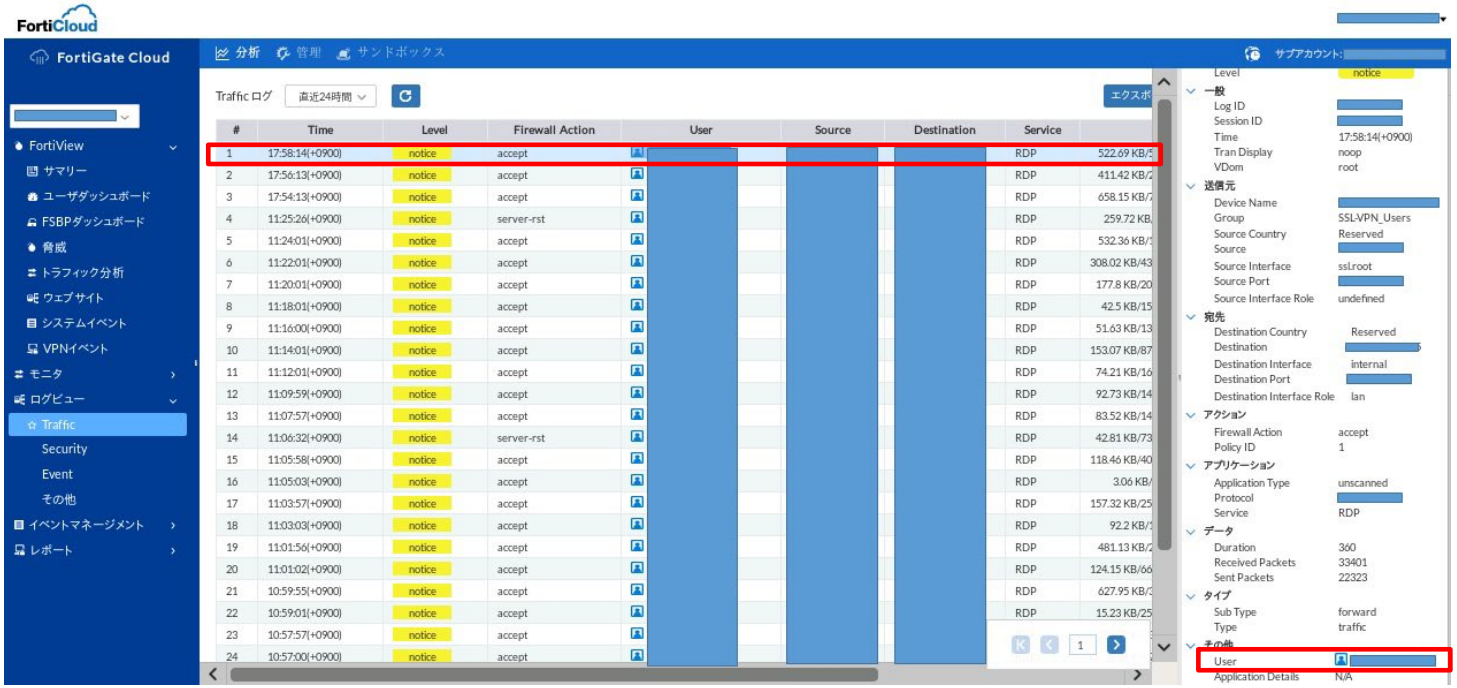
Sent/Received ：当該通信時の送信/受信通信量です。

Service ：必ずRDP (リモートデスクトップ) が表示されます。

2．FortiCloud管理Webシステム ログ確認手順

2.4 トラフィックログ確認手順

② 確認したいログをクリックすると、右メニューで詳細情報が確認できます。

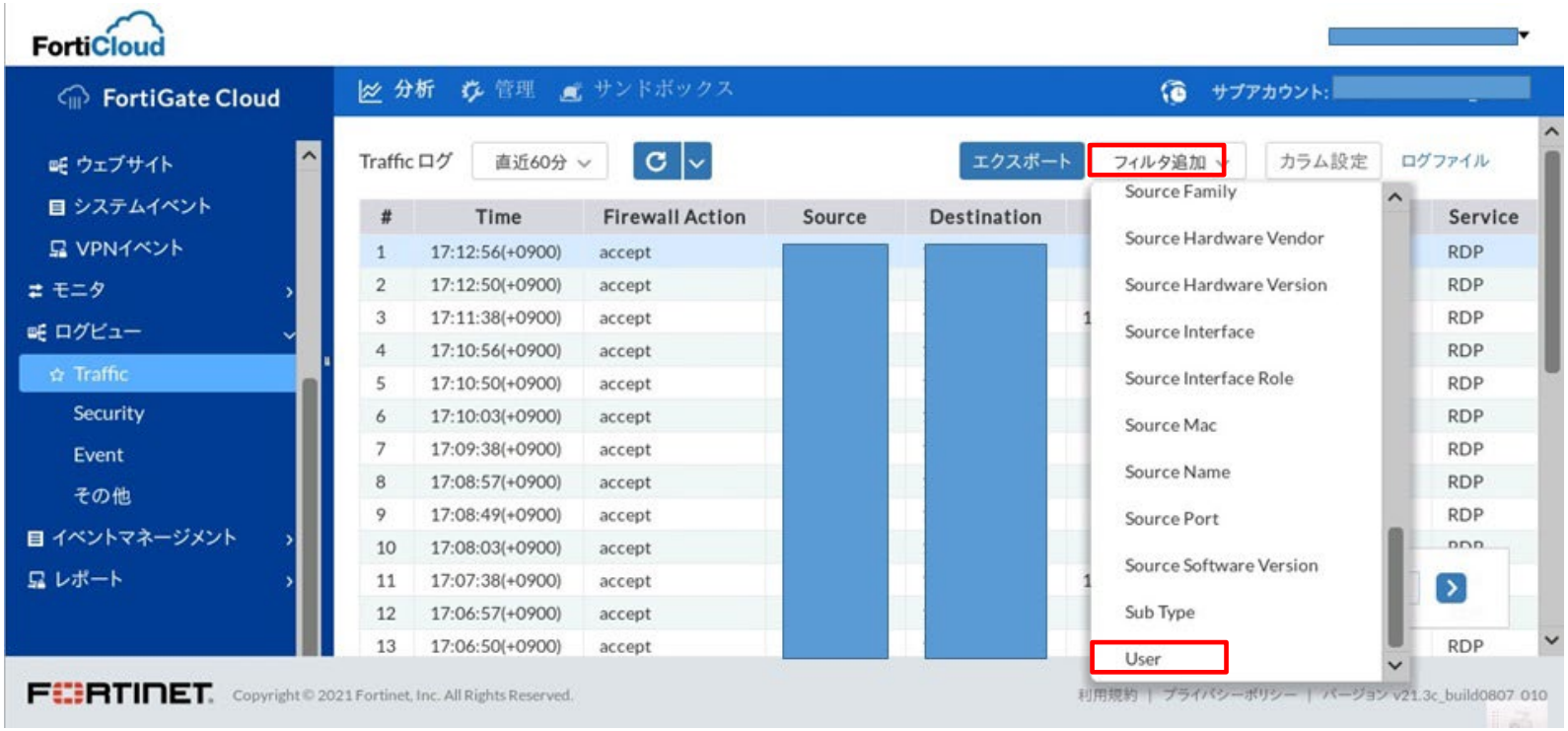


基本的に①で見れる内容と大きな差はございませんが、User欄にリモートアクセスユーザのIDが表示されますので、どのユーザのアクセスかを識別することが可能です。

2．FortiCloud管理Webシステム ログ確認手順

2.4 トラフィックログ確認手順

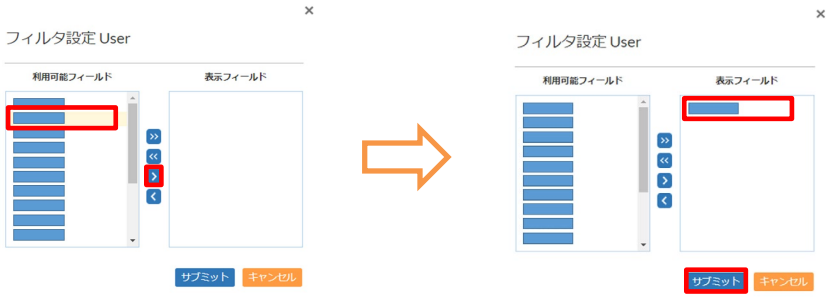
③ 特定ユーザの、社内端末へのアクセスログを検索することが可能です。
まず、ログ画面右上の「フィルタ追加」を選択し、表示されたプルダウンメニューから「User」を選択します。



2．FortiCloud管理Webシステム ログ確認手順

2.4 トラフィックログ確認手順

フィルタ設定画面が表示されたら、検索したいユーザIDを選択し、「>」をクリックします。
その後、表示フィールド側に選択したIDが移動したら"サブミット"をクリックします。



2．FortiCloud管理Webシステム ログ確認手順

2.4 トラフィックログ確認手順

特定ユーザの通信に絞ったトラフィックログが表示されます。