中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）関連資料

設定解説資料
（YAMAHA VPN ルーター）

ver1.2（2025.03）

本書は、総務省の調査研究事業により作成したものです。

本書に関する問い合わせ先（個別のシステムおよび環境に関する御質問については、製品の開発元にお問い合わせください。）
総務省 サイバーセキュリティ統括官室
Email telework-security@ml.soumu.go.jp
URL https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

目次

1 はじめに

(ア) 本書の目的

本書は、「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第 2 部に記載されているチェックリスト項目について、YAMAHA VPN ルーターを利用しての具体的な作業内容の解説をすることで、管理者が実施すべき設定作業の理解を助けることを目的としています。

(イ) 前提条件

利用する機器により使用可能な機能が異なります。**本資料では YAMAHA　RTX830VPN ルーターの利用を前提としております。**

(ウ) 本書の活用方法

本書は、中小企業のセキュリティ管理担当者やシステム管理担当者（これらに準ずる役割を担っている方を含みます）を対象として、その方々がチェックリスト項目の具体的な対策を把握できるよう、第 2 章ではチェックリスト項目に紐づけて解説内容と解説ページを記載しています。本書では第 3 章にて管理者向けに、設定手順や注意事項を記載しています。

表 1. 本書の全体構成

章題	概要
1 はじめに	本書を活用するための、目的、本書の前提条件、活用方法、免責事項を説明しています。
2 チェックリスト項目と設定解説の対応表	本書で解説するチェックリスト項目と、その項目に対応する設定作業手順および注意事項の解説が記載されたページを記載しています。
3 管理者向け設定作業	対象のチェックリスト項目に対する管理者向けの設定手順や注意事項を解説しています。

(エ) 免責事項

本資料は現状有姿でご利用者様に提供するものであり、明示であると黙示であることを問わず、正確性、商品性、有用性、ご利用者様の特定の目的に対する適合性を含むその他の保証を一切行うものではありません。本資料に掲載されている情報は、2024 年 11 月 5 日時点の各製品の操作画面を基に作成しており、その後の製品仕様の更新、追加、変更、削除もしくは部分改廃により、画面表示等に差異が生じる可能性があります。本資料は、初期出荷状態の製品を単体動作させている環境を利用して設定手順を解説しています。本製品をご利用者様の業務環境で利用する際には、本資料に掲載している設定により業務環境システムに影響がないかをご利用者様の責任にて確認の上、実施するようにしてください。本資料に掲載されている製品仕様・設定方法について不明点がありましたら、製品提供元へお問い合わせください。

2 チェックリスト項目に対応する設定作業一覧

本書で解説しているチェックリスト項目、対応する設定作業解説および注意事項が記載されているページは下記のとおりです。

表 2. チェックリスト項目と管理者向け設定作業の紐づけ

チェックリスト項目	対応する設定作業	ページ
3-2 アクセス制御・認可 **インターネット経由で社内システムにアクセスがあった際には、ファイアウォールやルーター等において、不要なポートへの通信や不要な IP アドレスからの通信を遮断する。**	・アクセス制限確認	P.5
5-4 脆弱性管理 **テレワーク端末から社内にリモートアクセスするための VPN 機器等には、メーカーサポートが終了した製品を利用せず、最新のセキュリティアップデートを適用する。**	・最新のセキュリティアップデート	P.10
7-2 インシデント対応・ログ管理 **テレワーク端末と接続先の各システムの時刻を同期させる。**	・時刻同期確認	P.11
7-3 インシデント対応・ログ管理 **テレワーク端末からオフィスネットワークに接続する際のアクセスログを収集する。**	・ログ収集設定	P.13
9-2 アカウント・認証管理 **テレワーク端末のログインパスワードや、テレワークで利用する各システムの初期パスワードは必ず変更するよう設定する。**	・初期パスワード設定変更	P.15
10-1 特権管理 **テレワーク端末やテレワークで利用する各システムの管理者権限は、業務上必要な最小限の人に付与する。**	・管理者の権限付与	P.17
10-2 特権管理 **テレワーク端末やテレワークで利用する各システムの管理者権限のパスワードには、強力なパスワードポリシーを適用する。**	・管理者昇格パスワード設定	P.19
10-3 特権管理 **テレワーク端末やテレワークで利用する各システムの管理者権限は、必要な作業時のみ利用する。**	・管理者権限の管理	P.20

3 管理者向け設定作業

ここでは「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」の第 2 部に記載されているチェックリスト項目のうち、本製品の管理者が実施すべき対策の設定手順や注意事項を記載します。

3-1　チェックリスト 3-2 への対応

3-1-1 アクセス制限確認

VPN ルーターはインターネットから社内に接続するために利用する機器です。一般的には、社内ネットワークとインターネットの境界に設置されています。そのため、インターネットからのアクセスを許可する通信が必要最小限となるよう、VPN ルーターのファイアウォールを設定することが重要です。インターネットからのアクセス許可ルールによって許可する通信を必要最小限とすることで、**不正アクセスによる内部データの改ざんや盗聴等、セキュリティ上のリスクを低減**させることができます。
以降の説明では、機器に設定されているファイアウォール設定の確認方法を解説します。

本書では、YAMAHA ルーターの設定管理画面に Web UI でアクセスした場合を想定して解説しています。設定管理画面（Web UI）へのアクセス方法は、各環境によって異なるため、構築担当者、構築ベンダー、または製品提供元に確認するようにしてください。初期状態の YAMAHA ルーターについては、以下の URL で設定管理画面へのアクセス方法が解説されています。

【参考】ヤマハルーターWebGUI 操作マニュアル
URL：http://www.rtpro.yamaha.co.jp/RT/manual/rtx830/Webgui.pdf

ファイアウォール設定の確認

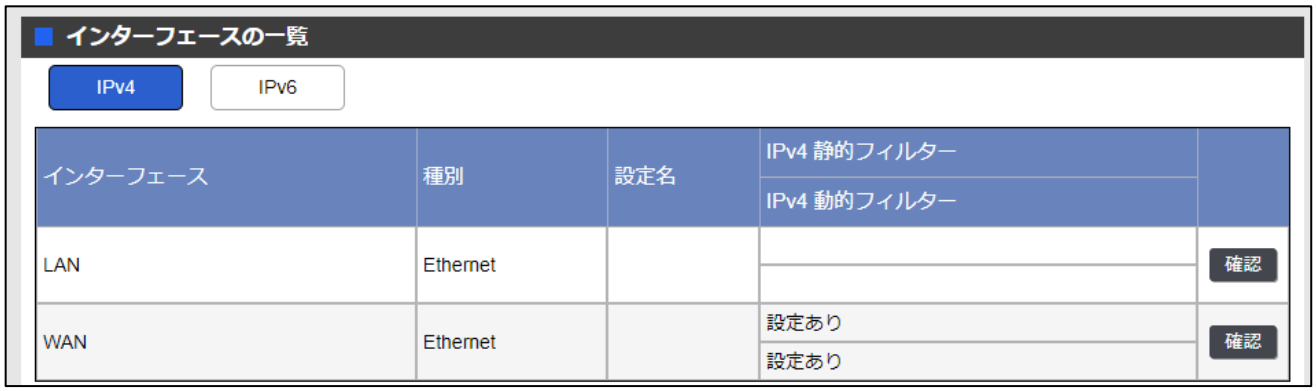
【手順①】

管理画面にアクセスし、画面上部にある「詳細設定」を選択後、左側の「セキュリティ」-「IP フィルター」をクリックします。

右側に IP フィルターの設定が可能なインターフェースの一覧が表示されます。ここでは、IPv4 フィルターを設定します。

【手順②】

インターフェースの一覧からインターネット側に相当する WAN インターフェースの「確認」をクリックします。ここでは LAN インターフェースが社内ネットワーク側、WAN インターフェースがインターネット側という想定で解説しています。



【手順③】

下図のような確認対象インターフェースの IP フィルターの一覧が表示されます。この一覧に、業務上不要なサービスが許可されていないかを確認します。送信元アドレス欄に『 * 』、タイプ欄に『pass』または『pass-log』と記載されているルールについてはインターネット上のすべてのホストからのアクセスを許可するルールになります。一般的に、VPN ルーターとして利用している機器について、インターネット上のすべてのホストからのアクセスを許可しなければならないケースは少ないため（VPN 接続のためのルールを除く）、アクセス許可の制限がされていない場合や不要だと思われる許可ルールを確認した場合は、本当に必要な通信ルールであるかについて、構築担当者や構築ベンダーに確認するようにしてください。なお、フィルタールールの見方については、『参考 フィルタールール画面の見方』を参照してください。

下図の IP フィルター設定は一例です。最適な IP フィルター設定は環境によって異なるため、自社の環境にあった IP フィルター設定は構築ベンダー等と協議の上、各社で適切な IP フィルターを作成してください。なお、この設定例は静的フィルターで設定されるルールの例です。YAMAHA ルーターでは、静的フィルターと動的フィルターの 2 種類が存在します。各フィルターの違いについては、『参考 静的フィルターと動的フィルターについて』を参照してください。

評価順	番号	タイプ	プロトコル	送信元アドレス 送信元ポート番号	宛先アドレス 宛先ポート番号
1	102100	pass	TCP	*	172.16.1.1
				*	telnet
2	102101	pass	TCP	*	172.16.1.1
				*	22
3	102102	pass	*	*	172.16.1.1
				*	www
4	102107	pass-log	UDP	*	172.16.1.1
				*	500
5	102103	pass-log	ESP		

以下の条件に合致するルールはインターネットからのアクセスが制限されていない可能性があります。
送信元アドレス欄：『 * 』
タイプ欄：『pass』または『pass-log』

参考 フィルタールール画面の見方

■静的フィルター

① 評価順	② 番号	③ タイプ	④ プロトコル	⑤ 送信元アドレス / 送信元ポート番号	⑥ 宛先アドレス / 宛先ポート番号
1	102100	pass	TCP	*	172.16.1.1
				*	telnet
2	102101	pass	TCP	*	172.16.1.1
				*	22
3	102102	pass	*	*	172.16.1.1
				*	www
4	102107	pass-log	UDP	*	172.16.1.1
				*	500
5	102103	pass-log	ESP	*	172.16.1.1
				-	-

■動的フィルター

① 評価順	② 番号	④ プロトコル / ルール	⑤ 送信元アドレス	⑥ 宛先アドレス	⑦ ログ	⑧ タイムアウト
1	102100	FTP	192.168.100.1...	172.16.1.1...	on	
2	102101	HTTP	192.168.100.2...	172.16.1.2...	on	

① 評価順
評価順の上位行（若番）が下位行に優先して処理されます。

② フィルター番号

③ タイプ
pass（許可）、reject（遮断）など、制御対象通信の処理を指定できます。

④ プロトコル指定
TCP、UDP などのプロトコルを指定できます。

⑤ 制御対象通信の送信元 IP アドレス（上段）
*とすることで全てのアドレスを指定可能できます。
制御対象通信の送信元ポート番号（下段）
制限したいポート番号の値もしくは www 等のサービス名を指定できます。

⑥ 制御対象通信の宛先 IP アドレス（上段）
*とすることで全てのアドレスを指定可能です。
制御対象通信の宛先ポート番号（下段）
制限したいポート番号の値もしくは www 等のサービス名を指定できます。

⑦ ログ出力設定
on/off を指定できます。on の場合は該当ルールによって通信が処理された際にログに記録します。

⑧ タイムアウト
動的フィルターとして保持するセッションの継続時間のことを指します。
セッションについては、『参考　静的フィルターと動的フィルターについて』にて解説しています。

参考　静的フィルターと動的フィルターについて

YAMAHA の VPN ルーターで設定可能なフィルターの種類は以下の 2 種類があります。

●静的フィルター

通信の状態に関わらず、予め定められたルールに従い、常に同じ動作をするフィルターを指します。例えば、インターネットにアクセスして何らかのファイルをダウンロードする場合、ファイアウォールでは往きと戻りの双方向の通信を許可する静的フィルターのルールを設定する必要があります。

●動的フィルター

予め定めた条件に適合する通信の有無によって、許可されるルールが動的に変化するフィルターを指します。具体的には、ある往き方向の通信が通過した際に、該当の通信が終了するまでの間、当該通信内容（IP アドレス、通信プロトコル・ポート等）をセッション情報として記憶し、セッション情報の戻り方向に適合する通信を動的に許可します。例えば、インターネットにアクセスして何らかのファイルをダウンロードする場合、ファイアウォールで往きの通信を動的フィルターとして設定すると、戻りの通信は設定をしなくても動的に自動で許可されます。

3-2　チェックリスト 5-4 への対応

3-2-1　　最新のセキュリティアップデート

VPN 機器を利用する際は、製品提供元からリリースされる最新バージョンを利用します。古いバージョンの VPN 機器は脆弱性をついたサイバー攻撃や不正アクセス等の標的となりやすいため、特に注意します。最新バージョンにアップデートすることは、**脆弱性をついたサイバー攻撃に対して有効な対策となる**ため、定期的にアップデートがないか確認することを推奨します。

現在のファームウェアリビジョン確認

【手順①】

画面上部にある「管理」を選択後、左側の「保守」-「ファームウェアの更新」をクリックします。
右側にある現在のファームウェアリビジョンからリビジョンを確認することができます。

3-3　チェックリスト 7-2 への対応

3-3-1　　時刻同期確認

VPN 機器とアクセス先の各システムの時刻を同一のものにするため、VPN 機器の時刻設定を行います。各機器の時刻を一致させることで、**インシデント発生時のアクセスログ等の調査の際に、正確な調査を行う**ことができます。

日付と時刻確認

【手順①】

画面上部にある「管理」を選択後、左側の「本体の設定」をクリックします。

右側にある日付と時刻の設定から現在の日時を確認します。日時が正確でない場合は、次の手順「日付と時刻設定」を行ってください。

日付と時刻設定

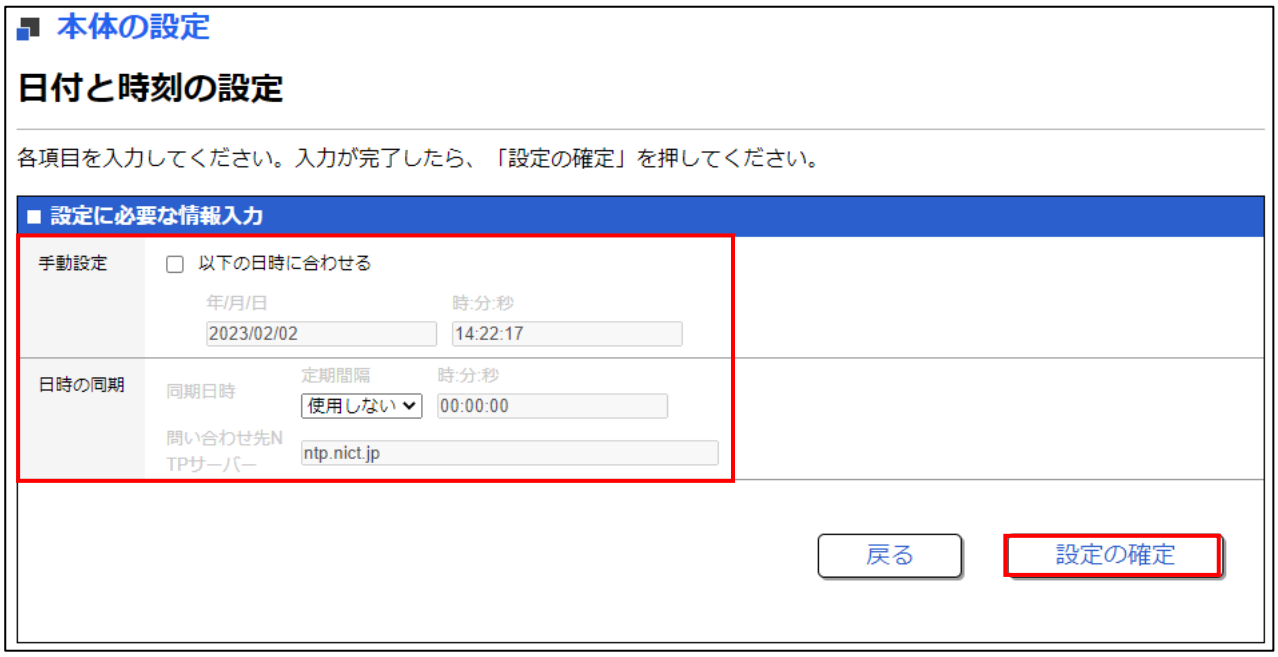
【手順①】

画面上部にある「管理」を選択後、左側の「本体の設定」をクリックします。

右側にある日付と時刻の設定から「設定」をクリックします。

【手順②】

設定に必要な情報入力欄が表示されるので、必要な情報を入力し、「設定の確定」をクリックします。



3-4　チェックリスト 7-3 への対応

3-4-1　　ログ収集設定

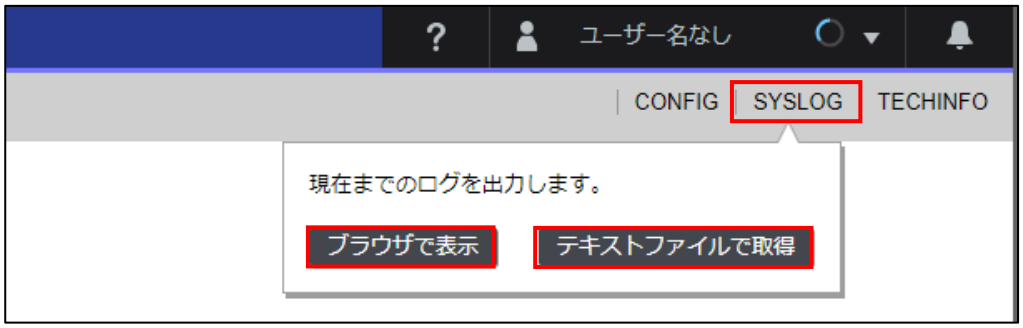
ログ収集の設定を行っていない場合、悪意のある第三者から攻撃を受けた際に原因究明や調査を行うことができなくなってしまいます。VPN 機器でログを収集することで、**悪意のある第三者から不正アクセス等のサイバー攻撃にあった際に、原因を調査することが可能**となるため、ログ確認やログ収集の設定を行います。

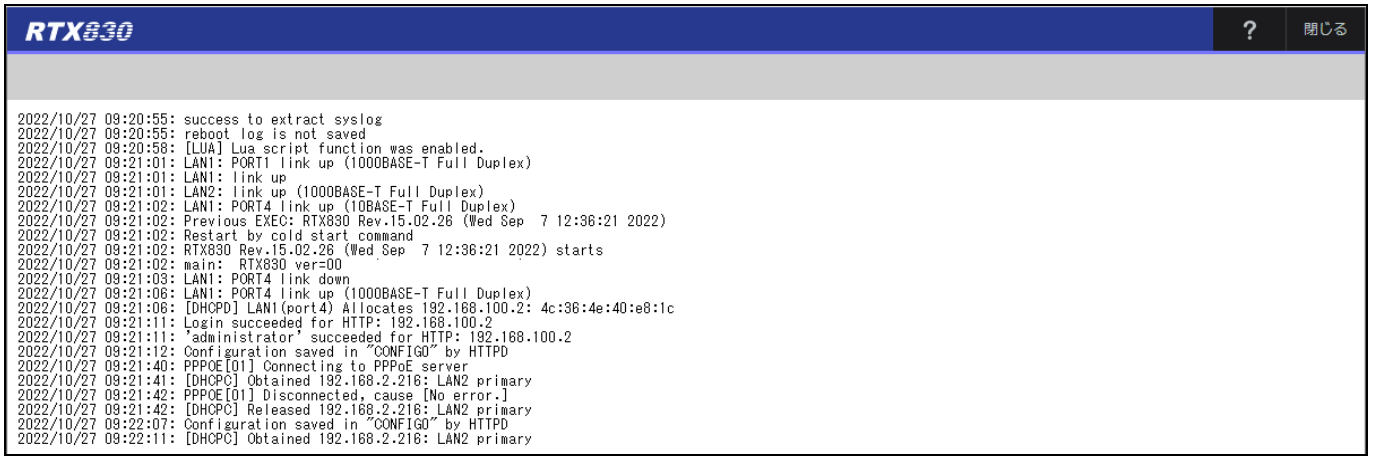
ログ確認

【手順①】

ダッシュボード画面右上にある「SYSLOG」をクリックします。クリック後、「ブラウザで表示する」または「テキストファイルで取得」を選択することで、それぞれの方法でログを確認することが可能です。

SYSLOG が取得できていない場合は、次の手順「SYSLOG 収集設定」を行ってください。





SYSLOG 収集設定

【手順①】

画面上部にある「管理」を選択後、左側の「保守」-「SYSLOG の管理」をクリックします。右側から SYSLOG の設定欄の「設定」をクリックします。

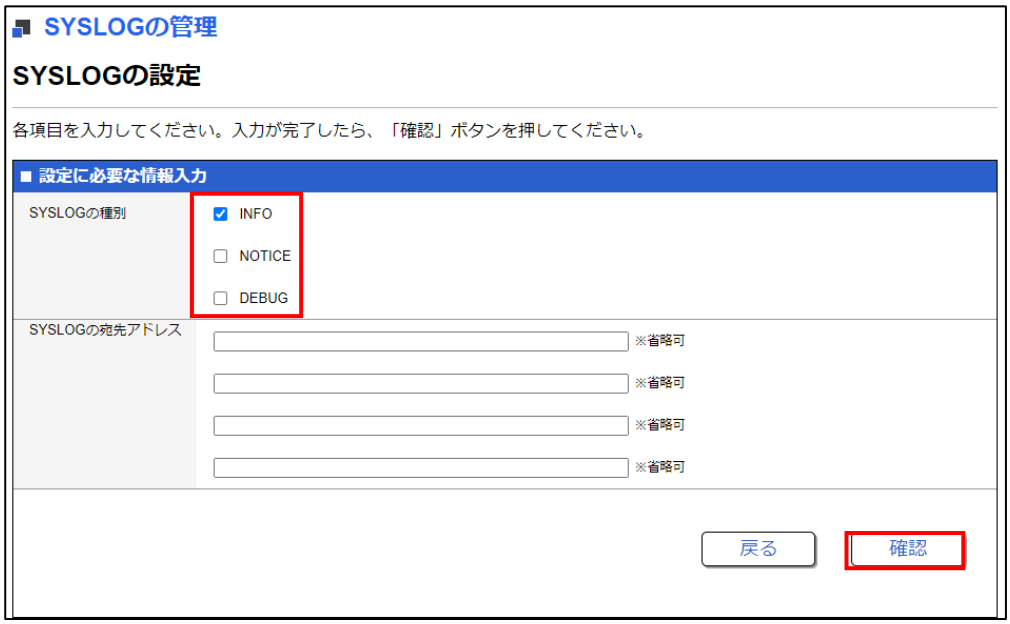
【手順②】

SYSLOG 設定に必要な情報を入力後、「確認」をクリックします。

INFO ログ：通常のログ情報を出力

NOTICE：パケットフィルタリングで落としたパケット情報等を出力

DEBUG：障害解析等のために ISDN や PPP のデバッグ情報を出力



3-5　チェックリスト 9-2 への対応

3-5-1　　初期パスワード設定変更

初期パスワードは、誰が把握しているかわからないので、VPN 機器の初期パスワードは速やかに変更することで**悪意のある第三者から不正アクセスされるリスクを低減**します。

パスワード設定変更

【手順①】

画面上部にある「管理」を選択後、左側の「アクセス管理」-「ユーザーの設定」をクリックします。
右側にあるユーザーの設定欄から任意のユーザーの「設定」をクリックします。

【手順②】

「ユーザーの設定に必要な情報入力」から新しいパスワードを入力します。

【手順③】

入力後、「確認」をクリックします。

【手順④】

設定を確認後、「設定の確定」をクリックします。

3-6　チェックリスト 10-1 への対応

3-6-1　　管理者の権限付与

管理者権限を付与するユーザーを限定することで、VPN 機器の設定変更を行えるユーザーを必要最小限に抑え、**悪意のある第三者からの意図しない不正アクセスや設定変更等による攻撃リスクを低減**することができます。

以下では、ユーザーに管理者権限を付与する手順を記載しています。

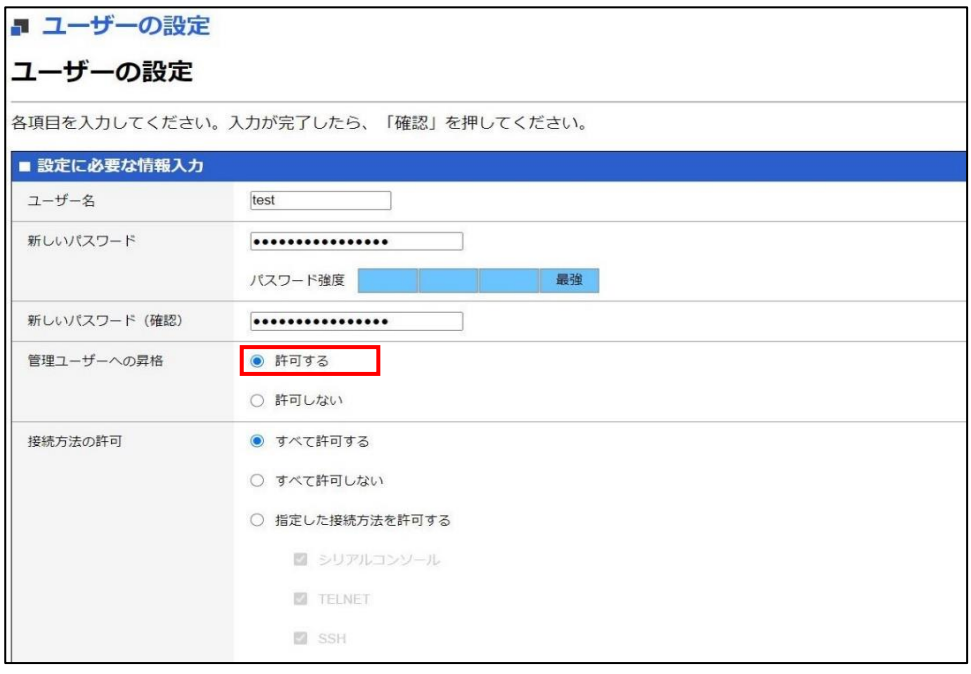
管理者権限の付与

【手順①】

画面上部にある「管理」を選択後、左側の「アクセス管理」-「ユーザーの設定」をクリックします。
右側にあるユーザーの設定欄から任意のユーザーの「設定」をクリックします。

【手順②】

ユーザーの「設定に必要な情報入力」欄の「管理ユーザーへの昇格」から、「許可する」にチェックを入れます。



【手順③】

必要情報を入力後、「確認」をクリックします。

【手順④】

ユーザー情報を確認後、「設定の確定」をクリックします。

3-7　チェックリスト 10-2 への対応

3-7-1　　管理者昇格パスワード設定

パスワード強度が弱いパスワードを使用した場合、パスワードが解読され、不正アクセスを受けるおそれがあります。そのため、適切なパスワードを設定することが重要です。設定するパスワードは「中小企業等向けテレワークセキュリティの手引き」のP.96 に記載の「パスワード強度」を参考に設定することを推奨します。

VPN 機器の管理者のパスワードを長いものや複雑なものにすることで**悪意のある第三者からの意図しない不正アクセスや設定変更等の攻撃リスクを低減**することができます。

管理者昇格権限のパスワード変更

【手順①】

画面上部にある「管理」を選択後、左側の「アクセス管理」-「ユーザーの設定」をクリックします。

右側にある管理パスワードの設定欄から「設定」をクリックします。

【手順②】

下図のような画面の表示後「新しいパスワード」を入力し、「パスワードの暗号化」-「暗号化する」を選択し、「確認」をクリックします。

【手順③】

入力内容の確認画面が表示されるので、「設定の確定」をクリックします。

3-8　チェックリスト 10-3 への対応

3-8-1　　管理者権限の管理

作業ミスによるシステムやデータへの悪影響を防ぐために、**一般ユーザーのアカウントを作成し、普段はそのアカウントを利用、管理者用アカウントの利用は最小限に留める**ことを推奨します。

【謝辞】
本設定解説資料の策定及び更新を行うにあたっては、ヤマハ株式会社の関係各所の方々に多大なるご協力をいただきました。この場をお借りして深く御礼申し上げます。