KONICA MINOLTA

Giving Shape to Ideas

bizhub PRESS C1070/C1070P/C1060/C71hc

ユーザーズガイド　セキュリティー編

本書に、乱丁、落丁などがありましたら、サービス実施店もしくは、最寄の販売店にご連絡ください。新しいものとお取替えいたします。

もくじ

MEMO

1 はじめに

1 はじめに

1.1 ご挨拶

このたびは弊社製品をお買上げいただき、誠にありがとうございます。

このユーザーズガイドには、セキュリティー機能について記載しています。セキュリティー強化機能の使い方、セキュリティー強化機能使用時の機械の操作について知りたい場合は、このユーザーズガイドをお読みください。

また、このユーザーズガイドはいつでも見られる場所に大切に保管してください。

1.1.1 マニュアルの構成と使い方

本体のユーザーズガイドは、次の冊子マニュアルと**ユーザーズガイド** CD という構成になっています。

詳しい機能や操作方法をお知りになりたいときは、**ユーザーズガイド** CD に収められている HTML **ユーザーズガイド**をご覧ください。

冊子マニュアルの名称	概要
すぐに使えるかんたん操作ガイド IC-602	機械の基本操作や、**イメージコントローラー** IC-602 をお使いになるうえで必要となるプリンタードライバーとアプリケーションのインストール方法、消耗品の交換方法などを記載しています。
すぐに使えるかんたん操作ガイド Fiery カラーサーバー	機械の基本操作や、**イメージコントローラー** IC-308 をお使いになるうえで必要となるプリンタードライバーとアプリケーションのインストール方法、消耗品の交換方法などを記載しています。この冊子マニュアルは、bizhub PRESS C71hc の構成には含まれません。
安全にお使いいただくために	機械を安全にお使いいただくために守っていただきたい注意事項とお願いを記載しています。 製品をお使いの前に必ずお読みください。
ユーザーズガイド セキュリティー編（本書）	セキュリティー機能について記載しています。 セキュリティー強化機能の使い方、セキュリティー強化機能を使ったときの機械の操作に関する内容を知りたい場合にお読みください。

ユーザーズガイド CD 内のマニュアルの名称	概要
HTML ユーザーズガイド	基本的な操作方法、より便利にお使いいただくための機能、メンテナンス方法、簡単なトラブルの対処方法、その他さまざまな設定方法について説明しています。

メンテナンスやトラブルの対処には、製品についての基本的な技術知識が必要です。メンテナンスやトラブルの対処は、本書および**ユーザーズガイド** CD に収められている HTML **ユーザーズガイド**で説明している範囲内で行ってください。

お困りの際には、サービス実施店にご連絡ください。

1.2 ページの見かた

1.2.1 本文中の記号について

本書は、さまざまな情報を記号で記載しています。

ここでは、製品を正しく安全にお使いいただくために、本書で使用している記号について説明します。

安全にお使いいただくために

⚠ 警告

- この表示を無視して、誤った取扱いをすると、人が死亡または重傷を負う可能性が想定される内容を示しています。

⚠ 注意

- この表示を無視して、誤った取扱いをすると、人が傷害を負う可能性が想定される内容及び物的損害のみの発生が想定される内容を示しています。

重要

本機や原稿に損害をあたえる可能性が想定される内容を示しています。物的損害を避けるために指示に従ってください。

手順文について

✔ このチェック記号は、手順文の前提条件や、手順を実行する前にあらかじめ知っておいたほうが良い情報を示しています。

1 このスタイルの 1 は、最初の手順を表します。

2 このスタイルの番号は、連続する手順の順番を表します。

➔ この記号は、手順文の補足的な説明を表します。

手順の動作を
イラストで
表しています。

➔ この記号は、目的のメニューにアクセスする操作パネルの遷移を表します。

目的の画面を表示しています。

参照
参照先を表しています。

必要に応じてごらんください。

キー記号について

[ ]

タッチパネル上のキー名称、コンピューター画面上のキー名称、ユーザーズガイド名称などを表します。

文中の太字

操作パネル上のキー名称、部品名称、製品名、オプション名などを表します。

2 セキュリティー機能

2 セキュリティー機能

2.1 セキュリティー機能

2.1.1 セキュリティーモード

bizhub PRESS C1070、bizhub PRESS C1070P、bizhub PRESS C1060、および bizhub PRESS C71hc には、セキュリティー機能に関して 2 つのモードがあります。

通常モード

機械が単独で使用されていて、利用者からの不正なアクセスや操作が行われにくい場合に使用します。工場出荷時に設定されているモードです。通常モードの操作については、それぞれのユーザーズガイドをごらんください。

外部ネットワーク（インターネット）に接続された本機からのデータや情報の漏洩を防ぐため、専門的なセキュリティーの知識がなくても、一定のセキュリティーを保つ簡単セキュリティー設定があります。

参照
簡単セキュリティー設定については、2-6 ページをごらんください。

セキュリティー強化モード

機械がネットワークや電話線などを介して外部と接続する可能性がある場合、セキュリティー強化モードを使用します。機械を管理するために任命された管理者が、このドキュメントに従って機械を管理することで、一般利用者に対してデータ保護の立場から、より安全な操作環境を提供します。

セキュリティー強化モードを使用するには、サービス実施店による下記の設定が必要ですので、サービス実施店にお問い合わせください。

サービス実施店は、機械に CE 認証の CE パスワードと管理者パスワードを設定します。サービス実施店は、サービスエンジニア（CE）の作業を行うとき、CE パスワードを入力します。管理者は、サービス実施店から管理者パスワードを取得し、セキュリティー強化モード関連の設定をするとき入力します。

管理者は、取得した管理者パスワードを他者に漏洩しないでください。

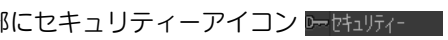
管理者パスワードを取得した管理者は、セキュリティー強化モードが使用できるようになった機械に以下の順番で設定をします。

1. セキュリティー強化モード
2. HDD ロックパスワード
3. ユーザー登録の追加、変更、削除

管理者は、ユーザーに対し下記の指導をお願いします。

- 各自のパスワードを他者に漏洩しないこと
- ユーザー認証によるログインを行い機械操作を終了したときは、必ずログアウトすること

HDD への不正なアクセスを防止するため、セキュリティー強化モードを必ず設定してください。

セキュリティー強化モードが ON 状態の機械は、画面右下部にセキュリティーアイコン 

を表示します。

セキュリティー強化モードを OFF にした場合は、セキュリティーアイコンが消えます。また、誤って管理者がセキュリティー強化モードを OFF にした場合は、サービス実施店に連絡してください。セキュリティー環境や設定をサービスエンジニア（CE）に確認してもらってから、セキュリティー強化モードを再度設定してください。

2.1.2 セキュリティー環境

セキュリティー強化モードのご利用が推奨される使用環境

機械が電話回線やネットワークによって監視されている環境

セキュリティー環境の整備

責任者および管理者は、セキュリティー強化モードのご利用とともに、下記の使用環境を整えることをおすすめします。

本機を使用するためのクライアント PC は、OS やアプリケーション（ウイルスソフト、プリンタードライバー、ブラウザなど）に対して、公開されている最新の更新プログラムを適用し、セキュアな状態で使用してください。

クライアント PC から本機に送信される機密プリントファイル、認証プリントファイルは、暗号化されていません。機密プリントファイル、認証プリントファイルを保護するために、暗号通信機や盗聴検知機器を設置するなど盗聴防止対策を行ってください。

- 管理者の資質：
  責任者は、管理者として十分な知識、技術、および経験を持った、信頼がおける人物を選出して、管理を依頼します。
- サービスエンジニア（CE）の保証：
  責任者または管理者は、サービスエンジニア（CE）と保守契約を締結したことを確認した上で、セキュリティー強化モードを使用します。保守契約には、サービスエンジニア (CE) が不正な行為をしない旨を明記します。
- セキュアなローカルネットワーク：
  ファイアウォールで保護された内部ネットワーク環境に機械を接続して、外部ネットワークから機械へアクセスできないようにしてください。また、内部ネットワークに不正な機器が接続されないように管理してください。
- 管理者は、機械を関係者だけが操作できる場所に設置にします。夜間は施錠管理されている場所に、昼間は管理者が監視可能な場所に設置して、HDD などの部品が盗難されないように、および機械内部を解析するような特殊装置が接続されないように管理してください。また、本体から取外した HDD 等も本体同様に管理してください。
- 管理者は、設置作業やメンテナンス作業などのサービスエンジニア（CE）が行う作業に立ちあってください。
- 管理者は、機械に設定されている日時設定値にくるいがないか定期的に確認し、管理してください。

2.1.3 セキュリティー強化モードの内容

下記のセキュリティー項目が強化されます。

メモリーや HDD にある使用後の残存データの保護と消去

メモリーや HDD に保存される画像データには、AHA 圧縮データと非圧縮データ（TIFF 形式、PDF 形式および PS データの 3 種類）があります。AHA 圧縮データが書込まれたメモリーや HDD の画像領域は、使用後のデータを消去して開放されます。通常モード時は、データを完全に消去していないので、不正な手段で読まれてしまう場合があります。セキュリティー強化モードでは、圧縮データか非圧縮データかにかかわらず、保存したメモリーや HDD の画像領域を、画像とは関係しないデータですべて上書きしてから、その領域を開放します。

パスワードの強化

セキュリティー関連のパスワードは 5 種類あります。

- CE パスワード
- 管理者パスワード
- ユーザーパスワード
- 部門名パスワード
- HDD ロックパスワード

CE パスワード、管理者パスワードは、8 文字の半角英数字（英字は大文字と小文字を区別）に決められています。

部門名パスワードは、1 ～ 8 文字の半角英数字（英字は大文字と小文字を区別）で設定します。

ユーザーパスワードは 1 ～ 64 文字の半角英数字（英字は大文字と小文字を区別）で設定しますが、セキュリティー強化モードの場合、8 文字未満のユーザーパスワードは使用できなくなります。64 文字以上のパスワードを入力すると最終文字が 64 文字目として認識されます。

HDD ロックパスワードは、8 ～ 32 文字の半角英数字（英字は大文字と小文字を区別）で設定します。32 文字以上のパスワードを入力すると最終文字が 32 文字目として認識されます。

CE パスワード、管理者パスワード、部門名パスワードは、8 文字以上のパスワードを入力すると最終文字が 8 文字目として認識されます。

また、上記 5 種類のパスワード入力時に誤ったパスワードを入力したとき、約 5 秒間再入力を受付けなくなります。

セキュリティー関連のパスワードを忘れてしまった場合は、パスワードの種類によって下記のように対応してください。

- ユーザーパスワード、部門名パスワードをお忘れになったときは、お客様の管理者の方にお問い合わせください。
- 管理者パスワード、HDD ロックパスワードをお忘れになったときは、サービス実施店にお問い合わせください。

不正なアクセスやデータの改ざんを防止するため、各パスワードを定期的に変更してください。

データへのアクセス

HDD に格納されているボックスにデータを保存したり、保存したデータを出力したりするときは、管理者があらかじめ設定している強化されたパスワードを入力してユーザー認証を得なければならないようにします。

スキャンデータをボックスに保存するときは、強化されたパスワードを設定するとセキュリティーを高めることができます。スキャンデータを保存したフォルダーやボックスの削除は、管理者だけができます。ボックスの属性を変更したときは、強化されたパスワードによるユーザー認証が必要になります。また、保存したスキャンデータを利用するときも、ユーザー認証が必要になります。

本体 NIC の設定

セキュリティー強化モードを ON にしている場合、本体 NIC を使用できません。

外部からのアクセス禁止

CS Remote Care 以外の電話回線からは、一切アクセスできません。

監査ログの作成、保存、解析

セキュリティー機能の動作に関する履歴を、監査ログとして作成、保存します。セキュリティーに関する操作の日時、操作した者を特定できる情報、操作内容、および操作結果が保存され、不正なアクセスに対する解析ができます。このログは、監査ログ用のメモリー領域が枯渇すると上書きされます。

管理者の認証

管理者の認証データは、サービス実施店が設定します。管理者は、管理者パスワードを入力して認証を得ます。この認証データは、機械に対して 1 つだけ登録できます。

管理者モード

管理者が入力した管理者パスワードが認証されると、機械は管理者モードになります。管理者モードでは、各種機能の設定を変更できます。

管理者モードの使用中に本機から離れる場合は、必ず管理者モードを終了してください。

IC カード

セキュリティー強化モードを ON にすると、IC カードによるユーザー認証はできなくなります。

USB 接続ポートの機能

セキュリティー強化モードを ON にしても、USB 接続ポートで下記機能は使用できます。

- USB メモリー ISW
- リストやレポートの USB 保存
- 出力紙濃度調整の用紙カテゴリー登録
- 濃度バランス調整のデータ登録
- USB チャート印刷（CE 用）
- キーボード、マウス

プリンターについて

PC から印刷を行う場合は、プリンターコントローラーとプリンタードライバーが必要です。セキュリティー強化モードを設定したプリンターコントローラーを使用するときは、プリンタードライバーでユーザー名を入力すると、印刷データを本体内のメモリーまたは HDD に保存できます。保存したデータは、保存時にプリンタードライバーで入力したユーザー名、およびそのユーザー名のパスワードを使って出力できます。他人のユーザー名を使って印刷データを保存したときは、保存したデータを他人が印刷できることになるので注意してください。

セキュリティー強化モードを設定したプリンターコントローラーとプリンタードライバーについては、サービス実施店にお問い合わせください。

プリンターコントローラーおよびプリンタードライバーの操作方法は、それぞれのユーザーズガイドをごらんください。

2.1.4 セキュリティー強化モードによって保護が強化されるデータ

セキュリティー強化モードによって、不正にすり替えられた HDD へのデータの書込みを防止します。

また、管理者が管理する下記のデータも保護が強化されます。

- ユーザーのデータ
- 機械を管理するデータ

セキュリティー強化モードで保護対象にならないデータについて

機械と PC をローカルネットで接続しているとき、PC で入力したパスワードはセキュリティー強化モードの対象外です。このような PC ではパスワードの漏洩のおそれがあるので、パスワードを入力しないでください。

セキュリティー強化モードの ON/OFF について

セキュリティー強化モードの ON/OFF は、管理者が行います。

管理者は、セキュリティー強化モードを必ず ON にしてください。セキュリティー強化モードを OFF にすると、データ漏洩の危険がありますので、特にご注意ください。

2.1.5 使用後の残存データの保護と消去

コピー、スキャン、およびプリンターの各モードのデータは、一時的にメモリーや HDD に保存され、ボックスへの格納などの操作をしなければ使用後に消去されます。

データは特殊な圧縮方法で圧縮されているので、一般的に外部で解凍できません。また、圧縮データを消去する場合は、その一部を破壊したり上書きしたりするので、解凍すること自体ができなくなります。

- メモリーに一時的に保存されたデータは、ジョブの中断または終了時点で不正データでの上書きクリアされます。
- 複数のメモリーに保存されているデータは、同じタイミングで不正データでの上書きクリアされます。

ボックスに格納されたデータは、削除指令が出されたときに不正データでの上書きクリアされます。

- 外部にデータを送信した場合は、完了時に不正データでの上書きクリアします。
- 管理者が各ボックスの削除指令を出したとき、不正データでの上書きクリアします。

2.1.6 簡単セキュリティー設定

簡単セキュリティー設定で設定する内容を説明します。

簡易 IP フィルタリング：本機への接続を制限する

簡易 IP フィルタリングによって、本機に接続できる機器を IP アドレス（IPv4/IPv6）で制限します。下記の選択ができます。

［簡単セキュリティー設定］－［簡易 IP フィルタリング］で下記の項目のうち 1 つを選択します。

［フィルタリングなし］

IP フィルタリングは無効となって、すべての IP アドレスからの通信と接続します。

［IP アドレス連動］

IPv4 の場合、本機に設定されている IP アドレスの末尾以外が同じ IP アドレスが設定されている機器だけ接続を許可します。IPv6 の場合、本機に設定されている IP アドレスと、上位 64bit が同じ IP アドレスが設定されている機器だけ接続を許可します。

［サブネットマスク連動］

本機に設定されている IP アドレスとサブネットマスクやプレフィックスを使って、接続できる IP アドレスの範囲を制限します。

管理者パスワード：管理者認証機能が OFF のとき、管理者パスワードを変更して管理者認証機能を ON にする

セキュリティー警告表示の［今すぐ設定］を押した後の［管理者パスワード］で新パスワードを設定します。

設定する管理者パスワードは、半角 8 文字固定です。

管理者認証機能が OFF になっている機械の管理パスワードを設定すると、管理者認証機能が自動的に ON になります。

重要
管理者認証機能が ON になっていても、管理者パスワードがデフォルトのままでセキュリティー警告表示設定が［表示する］に選択されている場合は、セキュリティー警告表示が表示されます。管理者は、速やかにデフォルトの管理者パスワードを任意のパスワードに変更してください。

重要
パスワード規約に準じていないパスワードを設定していて［パスワード規約設定］の［有効］を選択しようとしたとき、パスワード変更のダイアログが表示され、パスワードを変更しなければ［有効］を選択できません。また、［パスワード規約設定］を［有効］にしていて、パスワード規約に準じていないパスワードを入力すると、設定が拒否されます。

重要
設定したパスワードは忘れないようにしてください。万一お忘れになったときは、サービス実施店にお問い合わせください。

パスワード規約設定：パスワード規約を有効にするか無効にするか選択する

［簡単セキュリティー設定］－［パスワード規約設定］で［有効］または［無効］を選択します。

［有効］を選択すると、下記のパスワード規約に基づいて、本機に設定するパスワードを通常より厳格にして、パスワード規約に準じたパスワードだけ設定できます。また、パスワード規約に準じたパスワードで登録したフォルダーやジョブだけアクセスできるようにします。

パスワード規約

パスワードの半角文字数を限定します（8 文字以上）。8 文字未満で受付けていたパスワードも、8 文字未満では設定できなくなります。また、同一文字だけのパスワードを禁止します（例：aaaaaaaa）。パスワード規約の対象になるパスワードは、下記のとおりです。

管理者パスワード

ユーザーパスワード

部門パスワード

HDD 保存・フォルダーパスワード

一時保存ジョブ（セキュリティー印刷）や HDD 保存ジョブに設定するパスワード

スキャン設定・ボックス登録時のパスワード

SNMP 設定の各パスワード

英字の大文字と小文字は区別します。

記号は半角記号だけ使用できます。

変更前と同じパスワードの設定は禁止します。

Web Utilities 設定：Web Utilities 機能を使用するかしないか選択する

［簡単セキュリティー設定］－［Web Utilities 設定］で［使用する］または［使用しない］を選択します。

Web Utilities の機能を使用するかどうかを選択します。

Web Utilities の機能をセキュリティー管理できないときは、安全のため使用できないようにします。

PSWC 設定：PageScope Web Connection 機能を使用するかしないか選択する

［簡単セキュリティー設定］－［PSWC 設定］で［使用する］または［使用しない］を選択します。

PageScope Web Connection の機能を使用するかどうかを選択します。

PageScope Web Connection の機能をセキュリティー管理できないときは、安全のため使用できないようにします。

セキュリティー警告表示設定：セキュリティー警告表示を表示するかしないか選択する

［簡単セキュリティー設定］－［セキュリティー警告表示設定］で［表示する］または［表示しない］を選択します。

［表示する］を選択すると、機械が下記の状態のとき、セキュリティー警告表示画面が表示されます。

表示条件

- 管理者パスワードがデフォルトのままで変更されていない
- 管理者認証機能が OFF になっている

セキュリティー警告表示画面の表示タイミング

- 本体の電源を ON にしたとき
- 節電状態（ローパワー、シャットオフ）から復帰したとき
- ウィークリータイマーの時間外パスワード入力待機中

2.2 セキュリティー関連の管理者操作

セキュリティー強化モードの ON/OFF は、管理者が設定メニュー画面で設定します。その前提として、機械に CE パスワードおよび管理者パスワードを設定します。管理者パスワードの設定はサービス実施店が行います。また、管理者パスワードの変更は、管理者が行います。管理者パスワードの設定方法や詳しい使い方については、HTML ユーザーズガイドをご覧ください。

機械のデータを漏洩や不正アクセスから守るため、必ず管理者をたててセキュリティー強化モードを設定してください。ユーザー登録の追加、変更、削除をする前に、セキュリティー強化モード、HDD ロックパスワードを設定してください。

2.2.1 セキュリティー強化モードの ON/OFF

セキュリティー強化モードの ON/OFF の設定について説明します。

1 **操作パネル**の**設定メニュー／カウンター**を押して、設定メニュー画面を表示します。

2 ［03 管理者設定］を押します。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、［02 管理者設定］を押します。

パスワード入力画面が表示されます。

3 管理者パスワードを入力します。

➔ 8 文字の半角英数字や記号の管理者パスワードを入力し、［OK］を押します。

➔ 半角英字は大文字と小文字の区別をします。

➔ 間違ったパスワードや 8 文字未満の半角英数字や記号を入力して［OK］を押すと、［パスワードが一致しません　しばらくお待ち下さい］というメッセージを表示して、5 秒間いずれのキーやボタンも機能しなくなります。5 秒後に再度正しいパスワードを入力してください。

➔ 認証がうまくいかなかった情報は、監査ログとして保存します。

管理者設定メニュー画面が表示されます。

4 ［10 セキュリティー設定］を押します。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、［07 セキュリティー設定］を押します。

5 ［03 セキュリティー強化設定］を押します。

6 セキュリティー強化設定の ON/OFF を選択します。

➔ セキュリティー強化設定モードを ON にする場合は［ON］、OFF にする場合は［OFF］を選択します。

7 ［OK］を押します。

➔ 再起動を確認するダイアログが表示されます。

➔ ［はい］を押します。

8 機械は再起動し、変更した設定になります。

2.2.2 HDD ロックパスワード

セキュリティー強化モードを ON にすると、HDD に設定されているロックパスワードの初期値を新たなロックパスワードとして（8 ～ 32 文字の半角英数字、英字は大文字と小文字の区別あり）設定できます。ロックパスワードをかけることで、不正にすり替えられた HDD の持出しによるドキュメントデータの漏洩を保護します。HDD 単体で外部からアクセスされた場合は、ロックパスワードが一致しないと、HDD 内部のデータを読出すことができません。

重要

名前、誕生日、社員番号など、他人が容易に推測できるパスワードを設定しないでください。

パスワードは、他の人に教えたり、知られたりしないように注意してください。

1 **操作パネル**の**設定メニュー／カウンター**を押して、設定メニュー画面を表示します。

2 ［03 管理者設定］を押します。

➔ HDD ロックパスワードは、セキュリティー強化モードを ON にしたときだけ機能します。セキュリティー強化モードを OFF にしていると、［セキュリティー強化機能を設定して下さい］というメッセージが表示されます。

➔ セキュリティー強化モードを使用する時には、HDD ロックパスワードを必ず設定してください。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、[02 管理者設定] を押します。

パスワード入力画面が表示されます。

3 管理者パスワードを入力します。

➔ 8 文字の半角英数字や記号の管理者パスワードを入力してから、[OK] を押します。
➔ 半角英字は大文字と小文字の区別をします。
➔ 間違ったパスワードや 8 文字未満の半角英数字や記号を入力して [OK] を押すと、[パスワードが一致しません　しばらくお待ち下さい] というメッセージを表示して、5 秒間いずれのキーやボタンも機能しなくなります。5 秒後に、正しいパスワードを入力しなおしてください。
➔ 認証がうまくいかなかった情報は、監査ログとして保存します。

管理者設定メニュー画面が表示されます。

4 ［10 セキュリティー設定］を押します。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、［07 セキュリティー設定］を押します。

5 ［02 HDD 管理設定］を押します。

HDD 管理設定メニュー画面が表示されます。

6 ［01 HDD ロックパスワード］を押します。

HDD ロックパスワード画面が表示されます。

7 ［現パスワード］を押して現パスワードを入力してから、［OK］を押します。
初回パスワードは 13 文字の半角英数字の本体シリアル No です。

➔ 本体シリアル No は、設定メニュー画面の右上、または出力した監査ログの右上に 13 文字の半角英数字で表示されています。詳しくは、セキュリティー関連の管理者操作、「監査ログの出力」をごらんください。

8 認証が成功したら、［新パスワード］を押して新パスワードを入力します。

重要
名前、誕生日、社員番号など、他人が容易に推測できるパスワードを設定しないでください。

➔ HDD ロックパスワードは、半角の英数字で 8 ～ 32 文字を入力します。
➔ 間違ったパスワードや 8 文字未満の半角英数字を入力して［OK］を押すと、［パスワードが一致しません　しばらくお待ち下さい］という警告メッセージが表示され、5 秒間いずれのキーやボタンも機能しなくなります。5 秒後に再度正しいパスワードを入力してください。
➔ 認証がうまくいかなかった情報は監査ログとして保存されます。
➔ パスワードを変更した情報は、監査ログとして保存します。
➔ 現在のパスワードを、新パスワードとして設定できません。
➔ 入力が終わったら、［OK］を押します。

9 ［確認入力］を押して、再度、同じパスワードを入力します。

➔ 入力が終わったら、［OK］を押します。

10 HDD ロックパスワード画面の［OK］を押します。

2.2.3 一時データ上書き削除

HDD や DRAM に一時的に保存するドキュメントデータを利用できないように削除するか、しないかを選択します。消去する場合、そのモードを 2 つのうちから 1 つ選択します。

1 **操作パネル**の**設定メニュー／カウンター**を押して、設定メニュー画面を表示させます。

2 ［03 管理者設定］を押します。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、［02 管理者設定］を押します。

パスワード入力画面が表示されます。

3 管理者パスワードを入力します。

➔ 8 文字の半角英数字や記号の管理者パスワードを入力し［OK］を押します。

➔ 半角英字は大文字と小文字の区別をします。

➔ 間違ったパスワードや 8 文字未満の半角英数字や記号を入力して［OK］を押すと、［パスワードが一致しません　しばらくお待ち下さい］というメッセージを表示し、5 秒間いずれのキーやボタンも機能しなくなります。5 秒後に再度正しいパスワードを入力してください。

➔ 認証がうまくいかなかった情報は、監査ログとして保存します。

管理者設定メニュー画面が表示されます。

4 ［10 セキュリティー設定］を押します。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、［07 セキュリティー設定］を押します。

5 ［02 HDD 管理設定］を押します。

HDD 管理設定メニュー画面が表示されます。

6 ［02 一時データ上書き削除設定］を押します。

一時データ上書き削除設定画面が表示されます。

7 一時データの上書き削除をするかどうかを選択します。

➔ する場合は［する］を、しない場合は［しない］を押します。

8 上書き削除する場合はモードを選択します。

➔ ［モード 1］または［モード 2］を押します。消去モードの設定方法や詳しい使い方については、HTML ユーザーズガイドをご覧ください。

➔ 一時データの上書き削除をしない場合はどちらのモードを選択しても変わりません。

9 一時データ上書き削除設定画面の［OK］を押します。

10 **副電源スイッチ**を OFF にして、**主電源スイッチ**を OFF にします。

➔ ［冷却中です　冷却後に自動的に電源が切れます］と表示されている間は主電源を切らないでください。

11 10 秒以上待ちます。

12 **主電源スイッチ**を ON にして、**副電源スイッチ**を ON にします。

2.2.4 全データ上書き削除

HDD に保存されているドキュメントデータをすべて削除します。そのとき、消去モードを 8 つのうちから 1 つを選択します。

1 **操作パネル**の**設定メニュー／カウンター**を押して、設定メニュー画面を表示させます。

➔ 全データ上書き削除の機能を使用する場合は、サービス実施店にお問い合わせください。

2 ［03 管理者設定］を押します。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、［02 管理者設定］を押します。

パスワード入力画面が表示されます。

3 管理者パスワードを入力します。

➔ 8 文字の半角英数字や記号の管理者パスワードを入力し［OK］を押します。

➔ 半角英字は大文字と小文字の区別をします。

➔ 間違ったパスワードや 8 文字未満の半角英数字や記号を入力して［OK］を押すと、［パスワードが一致しません　しばらくお待ち下さい］というメッセージを表示し、5 秒間いずれのキーやボタンも機能しなくなります。5 秒後に再度正しいパスワードを入力してください。

➔ 認証がうまくいかなかった情報は、監査ログとして保存します。

管理者設定メニュー画面が表示されます。

4 ［10 セキュリティー設定］を押します。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、[07 セキュリティー設定] を押します。

5 [02 HDD 管理設定] を押します。

HDD 管理設定メニュー画面が表示されます。

6 [03 全データ上書き削除設定] を押します。

全データ上書き削除設定画面が表示されます。

7 消去モードを選択して、[削除実行] を押します。

➔ 消去モードの設定方法や詳しい使い方については、HTML ユーザーズガイドをご覧ください。

重要

[削除実行] で削除すると HDD のデータはすべて再利用できません。必要なデータは事前に別のデバイスに保存してください。

8 データ上書き削除設定画面の [前画面] を押します。

2.2.5 監査ログの出力

機械に保存されているデータにアクセスすると、監査ログを自動的に生成します。保存されたすべての監査ログデータは、以下の手順で出力できます。

1 **操作パネル**の**設定メニュー／カウンター**を押して、設定メニュー画面を表示します。

2 [03 管理者設定] を押します。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、[02 管理者設定] を押します。

パスワード入力画面が表示されます。

3 管理者パスワードを入力します。

➔ 8 文字の半角英数字や記号の管理者パスワードを入力し [OK] を押します。
➔ 半角英字は大文字と小文字の区別をします。
➔ 間違ったパスワードや 8 文字未満の半角英数字や記号を入力して [OK] を押すと、[パスワードが一致しません　しばらくお待ち下さい] というメッセージを表示し、5 秒間いずれのキーやボタンも機能しなくなります。5 秒後に再度正しいパスワードを入力してください。
➔ 認証がうまくいかなかった情報は、監査ログとして保存します。

管理者設定メニュー画面が表示されます。

4 ［01 環境設定］を押します。

5 ［06 リスト／カウンター］を押します。

リスト／カウンター画面が表示されます。

6 ［監査ログレポート］を選択して、［印刷モードへ］を押します。

7 出力します。

➔ **操作パネル**の**スタート**を押します。

➔ 出力を中止する場合は、**操作パネル**の**ストップ**を押します。中止確認のダイアログを表示します。［中止］を選択すると、出力を中止します。

➔ 出力が終了したら、［印刷モード終了］を押します。リスト／カウンター画面にもどります。

2.2.6 監査ログの解析

監査ログは、機械に保存されているデータに不正なアクセスや改ざんなどがあったとき、または定期的（1か月に 1 回程度）に、管理者が解析する必要があります。

監査ログに保存される項目の数は、750 件／月以下を想定しています。月に 750 件以上の保存が想定される場合は、750 件前後の期間で定期的に解析してください。

Audit log report P.1
2013/01/10 13:44
A50U021901002
TC:2712

No	date/time	id	action	result	No	date/time	id	action	result
0001	2012/10/13 11:23	-1	16	OK	0002	2012/10/13 11:23	-1	15	OK
0003	2012/10/13 11:21	-1	15	OK	0004	2012/10/13 11:20	-1	15	OK
0005	2012/10/13 11:16	-2	03	OK	0006	2012/10/13 11:16	-2	02	OK
0007	2012/10/13 11:15	-2	02	NG	0008	2012/10/13 11:15	-3	11	NG
0009	2012/10/13 11:14	-3	11	NG	0010	2012/10/13 11:14	-3	11	NG
0011	2012/10/13 10:56	2	11	OK	0012	2012/10/13 10:54	-2	02	OK
0013	2012/10/13 10:54	2	07	OK	0014	2012/10/13 10:53	-2	02	OK
0015	2012/10/13 10:53	-3	11	NG	0016	2012/10/13 10:52	-3	11	NG
0017	2012/10/13 10:51	1	11	OK	0018	2012/10/13 10:51	-3	11	NG
0019	2012/10/13 10:50	1	11	OK	0020	2012/10/13 10:50	-3	11	NG
0021	2012/10/13 10:49	-3	11	NG	0022	2012/10/13 10:49	1	11	OK
0023	2012/10/13 10:43	1	07	OK	0024	2012/10/13 10:43	-2	02	OK
0025	2012/10/13 10:42	-2	02	OK	0026	2012/10/13 10:40	-2	03	OK
0027	2012/10/10 13:33	-1	16	OK	0028	2012/10/05 21:02	-1	15	OK

監査ログの記載事項

監査ログには、下記の情報が記載されています。

1. date/time：ログ保存の対象になる操作が行われた年月日、および時間を記載します。
2. id：操作を行った人物、またはセキュリティー保護の対象を特定します。
- 「-1」：サービスエンジニア（CE）による操作
- 「-2」：管理者による操作
- 「-3」：未登録ユーザーによる操作
- 上記以外の整数：それぞれのセキュリティー保護対象を表しています。
  ユーザー ID：1 ～ 1000 の数字
3. action：操作の内容を特定します。
   詳細は、下記の対応表で確認できます。
4. result：操作の結果を記載します。
   パスワード認証に関する結果に対しては、成功または失敗を OK/NG で表示します。
   パスワードによる認証を伴わない操作の結果は、すべて成功（OK）と記載されます。

監査ログに保存される項目の対応表

No	操作内容	監査 id	保存される action	監査結果
1	CE 認証	CE ID	01	OK/NG
2	管理者認証	管理者 ID	02	OK/NG
3	セキュリティー強化モードの設定／変更	管理者 ID	03	OK
4	監査ログの印刷／ USB メモリー一括出力	CE ID/ 管理者 ID	04	OK
5	CE パスワードの変更／登録	CE ID	05	OK
6	管理者パスワードの変更／登録	CE ID/ 管理者 ID	06	OK
7	管理者によるユーザーの作成	ユーザー ID	07	OK

No	操作内容	監査 id	保存される action	監査結果
8	管理者によるユーザーパスワードの変更／登録	ユーザー ID	08	OK
9	管理者によるユーザーの削除	ユーザー ID	09	OK
10	管理者によるユーザーの属性変更	ユーザー ID	10	OK
11	ユーザーのパスワード認証	ユーザー ID[*1] ／未登録ユーザー ID[*2]	11	OK/NG
12	ユーザーによるユーザーの属性変更（ユーザーパスワード変更など）	ユーザー ID	12	OK
13	（欠番）			
14	（欠番）			
15	保存ジョブへのアクセス（一時保存、HDD 保存ジョブの印刷／HDD 保存ジョブの一時保存への読出し／一時保存ジョブの HDD 保存）	ユーザー ID	15	OK
16	保存ジョブの削除	ユーザー ID	16	OK
17	（欠番）			
18	（欠番）			
19	HDD ロックパスワードの変更	管理者 ID	19	OK
20	日時設定	ユーザー ID	20	OK

[*1]：ユーザー認証に成功したとき、およびユーザー名は登録しているがパスワードが不一致だったとき、監査ログ ID をユーザー ID として保存します。

[*2]：未登録ユーザー名でユーザー認証に失敗したとき、監査ログ ID を未登録ユーザー ID として保存します。

監査ログの解析目的は、下記の内容を把握して、対策を講じることです。

- データに対する攻撃の有無
- 攻撃の対象
- 攻撃の内容
- 攻撃による結果

具体的な解析方法は、以下を参照してください。

不正が行われた事象の特定：パスワード認証

パスワード認証（action 01、02、11）の結果に「NG」と記載されている場合は、パスワードによって保護されている対象が攻撃された可能性があります。

- パスワード認証の失敗（NG）のログは、操作した人物を id で特定し、パスワード認証が失敗した時間に、不正な行為があったどうかを示します。
- パスワード認証が成功（OK）した場合でも、action が正当な操作対象の人物によって行われたかどうかの確認ができます。特に、失敗（NG）の連続の後に成功（OK）した場合や、通常の操作時間外のパスワード認証に関しては、不正な行為である可能性が高いので、十分な確認が必要です。

不正が行われた事象の特定：パスワード認証以外の保護対象に対するアクション

パスワード認証以外の操作結果は、すべて成功（OK）と記載されるので、不正行為の有無は action および id によって判断します。

- 操作の時間を確認し、特定した対象を操作した人物が不正な行為を行ったかどうかを確認します。

不正行為発見時の対応

監査ログを解析した結果、パスワードが漏洩したことが判明した場合は、至急、パスワードを変更してください。

- パスワードが改ざんされて、本来の所有者がアクセスできなくなる場合も考えられます。管理者は、そういう事態になっていないかユーザーと連絡を取合い、そのときはパスワードの変更や保存しているデータを削除して対応する必要があります。
- 保存したはずのドキュメントが保存されてない場合や内容が変更されていた場合も、不正な行為が行われている可能性があります。同様の対応が必要です。

監査ログの USB メモリー一括出力時のトラブル

USB メモリーの接続が認識できない場合は、[USB メモリーの接続を認識できません] と表示され、一括出力処理できません。

作業中に書き込み失敗や USB メモリーの容量不足などのエラーが起きた場合は、[エラーが発生しました] と表示され、一括出力を中断します。

2.3 セキュリティー強化モード時のユーザー認証

セキュリティー強化モードが ON になると、ユーザー認証に関する機能が下記のように強化されます。

- 設定メニュー画面の［03 管理者設定］―［04 ユーザー認証／部門管理］―［01 認証方式］の「ユーザー認証」が自動的に［本体装置認証］に設定されます。
- bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、［02 管理者設定］－［03 ユーザー認証／部門管理］－［01 認証方式］の「ユーザー認証」が自動的に［本体装置認証］に設定されます。
- ユーザーのデータ保護が必要な以下の機能を使用するときは、必ずユーザー認証が必要になります。
  - ［ジョブリスト］タブ―［一時保存ジョブ］を押したとき
  - ［HDD 読出し］タブを押したとき
  - ［コピー］タブを押したとき
  - ［スキャン］タブを押したとき
- ユーザー認証時に入力するユーザー名に対するパスワード（ユーザーパスワード）は、8 ～ 64 文字の半角英数字（英字は大文字と小文字を区別）でなければ、使用できなくなります。8 文字未満のユーザーパスワードを設定しているユーザー名を引続き使用する場合は、管理者がユーザーパスワードを 8 文字以上に変更する必要があります。
- ユーザー認証時にユーザー名やユーザーパスワード（または部門名や部門名パスワード）の入力を間違えたとき、約 5 秒間再入力を受付けなくなります。
- セキュリティー強化モードを ON にすると、IC カードによるユーザー認証はできなくなります。

ユーザーが HDD 内のパスワードが設定されているファイルにアクセスすると、パスワードの認証操作はすべて監査ログとして保存されます。

最初はユーザー認証ができないようになっています。ユーザー認証を設定する場合、必要に応じて部門振分け数を変更する必要があります。ユーザー認証の設定方法や詳しい使い方については、HTML ユーザーズガイドをご覧ください。

2.3.1 ユーザー登録の追加

セキュリティー強化モード時に必要となるユーザー名およびパスワードを登録します。

1 **操作パネル**の**設定メニュー／カウンター**を押し、設定メニュー画面を表示させます。

2 ［03 管理者設定］を押します。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、[02 管理者設定] を押します。

パスワード入力画面が表示されます。

3 管理者パスワードを入力します。

8 文字の半角英数字や記号の管理者パスワードを入力し [OK] を押します。

➔ 半角英字は大文字と小文字の区別をします。

➔ 間違ったパスワードや 8 文字未満の半角英数字や記号を入力して [OK] を押すと、[パスワードが一致しません　しばらくお待ち下さい] というメッセージを表示して、5 秒間いずれのキーやボタンも機能しなくなります。5 秒後に再度正しいパスワードを入力してください。

➔ 一世代前のパスワードは、設定できません。

➔ 認証がうまくいかなかった情報は、監査ログとして保存します。

➔ 入力した文字数だけ「*」が画面上に表示されます。

管理者設定メニュー画面が表示されます。

4 ［04 ユーザー認証／部門管理］を押します。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、［03 ユーザー認証／部門管理］を押します。

ユーザー認証／部門管理メニュー画面が表示されます。

5 ［02 ユーザー認証設定］を押します。

ユーザー認証設定メニュー画面が表示されます。

6 ［02 ユーザー登録］を押します。

ユーザー登録画面が表示されます。

7 ［追加］を押します。

ユーザー登録追加画面が表示されます。

8 ［ユーザー No.］を押します。

画面のテンキー、[▼]、または [▲] を押して、任意のユーザー No. を入力します。
➔ ユーザー No. は、半角数字を 1 ～ 1000 の範囲で設定できます。

[OK] を押すと、ユーザー登録追加画面にもどります。

9 [ユーザー名] を押します。

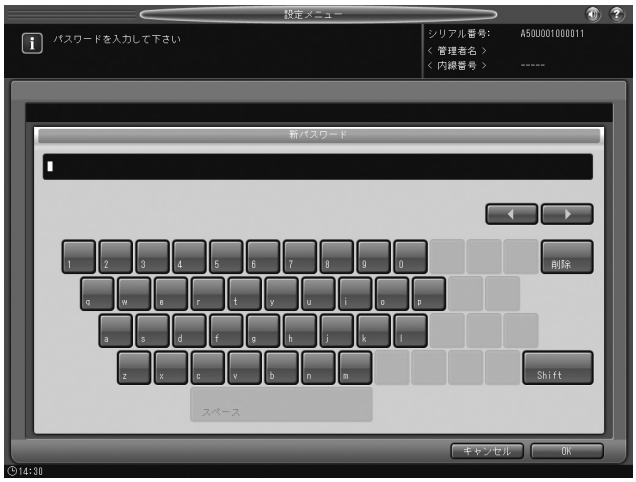
ユーザー名入力画面が表示されます。任意のユーザー名を入力します。
➔ ユーザー名は、全角の漢字、ひらがな、カタカナ、英字で 32 文字、半角の英数字、記号、カタカナで 64 文字まで入力できます。重複するユーザー名は、使用できません。

[OK] を押すと、ユーザー登録追加画面にもどります。

10 [パスワード] を押します。

パスワード入力画面が表示されます。手順 9 で入力したユーザー名に対応したユーザーパスワードを入力します。
➔ ユーザーパスワードは、半角の英数字（英字は大文字と小文字を区別）で 8 ～ 64 文字を入力します。

重要
8 文字以上の半角英数字のパスワードを設定してください。8 文字未満のパスワードはセキュリティー強化モード時には使用できません。



［OK］を押すと、ユーザー登録追加画面にもどります。

11 ［E-mail アドレス］を押します。

E-mail アドレス入力画面が表示されます。

➔ E-mail アドレスは、半角の英数字および記号で 320 文字まで入力できます。

［OK］を押すと、ユーザー登録追加画面にもどります。

12 ［所属部門］を押します。

所属部門設定画面が表示されます。任意の所属部門を選択します。

重要

認証方式の［ユーザー認証／部門認証連動］が［連動する］に設定されていると、［所属部門］を設定できます。

重要

所属部門は事前に登録が必要です。ここでは登録されている所属部門から 1 つを選択します。

［OK］を押すと、ユーザー登録追加画面にもどります。

13 ［上限設定］を押します。

➔ ここでは、認証を得て印刷できるようになったユーザーの出力枚数の上限値を設定します。

➔ 「管理方式」右の［トータル管理］を押し、「上限設定」右の［有効］を押して、［上限値］を押します。

➔ テンキーまたは［▲］、［▼］を押して、上限値を入力します。上限値は、0 ～ 99,999,999 の範囲で設定できます。

➔ ［OK］を 2 回押すと、ユーザー登録追加画面にもどります。

➔ カラーとブラックの出力上限値を個別に設定できます。

➔「管理方式」右の［個別管理］を押し、「上限設定 - カラー」右、および「上限設定 - ブラック」右の［有効］を押して、［上限値］を押します。

➔ テンキーまたは［▲］、［▼］を押して、上限値を入力します。上限値は、0 ～ 99,999,999 の範囲で設定できます。

［OK］を 2 回押すと、ユーザー登録追加画面にもどります。

14 「使用可能な機能」右の［コピー操作］［スキャン操作］［プリンター印字］［HDD 一時保存操作］を押して、ユーザーの使用を可能にする本機の機能を選択します。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、「使用可能な機能」右の［プリンター印字］［HDD 一時保存操作］から選択します。

15 「出力許可（印刷）」右の［カラー］、［ブラック］を押して、ユーザーに使用を認める印刷の種類を選択します。

16 ［OK］を押します。

➔ 入力が終わったら、ユーザー登録画面にある［前画面］を押します。
ユーザー認証設定メニュー画面にもどります。

2.3.2 ユーザー登録の変更

セキュリティー強化モード時に必要となるユーザー名およびパスワードを変更します。

1 **操作パネル**の**設定メニュー／カウンター**を押し、設定メニュー画面を表示させます。

2 ［04 管理者設定］を押します。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、[02 管理者設定] を押します。

パスワード入力画面が表示されます。

3 管理者パスワードを入力します。

8 文字の半角英数字や記号の管理者パスワードを入力し [OK] を押します。

➔ 半角英字は大文字と小文字の区別をします。

➔ 間違ったパスワードや 8 文字未満の半角英数字や記号を入力して [OK] を押すと、[パスワードが一致しません　しばらくお待ち下さい] というメッセージを表示、5 秒間いずれのキーやボタンも機能しなくなります。5 秒後に再度正しいパスワードを入力してください。

➔ 認証がうまくいかなかった情報は、監査ログとして保存します。

管理者設定メニュー画面が表示されます。

4 ［04 ユーザー認証／部門管理］を押します。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、［03 ユーザー認証／部門管理］を押します。

ユーザー認証／部門管理メニュー画面が表示されます。

5 ［02 ユーザー認証設定］を押します。

ユーザー認証設定メニュー画面が表示されます。

6 ［02 ユーザー登録］を押します。

ユーザー登録画面が表示されます。

7 変更したいユーザー No. とユーザー名が表示されているボタンを選択します。

8 ［変更］を押すと、ユーザー登録変更画面が表示されます。

➔ ユーザー No. は変更できません。

9 ユーザー名を変更する場合、［ユーザー名］を押します。

10 変更するユーザー名を入力します。

➔ ユーザー名は、全角の漢字、ひらがな、カタカナ、英字で 32 文字、半角の英数字、記号、カタカナで 64 文字まで入力できます。重複するユーザー名は、使用できません。

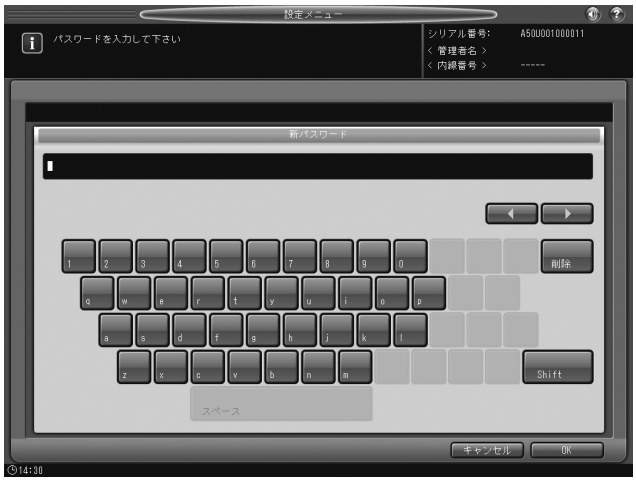
［OK］を押すと、ユーザー登録変更画面にもどります。

11 パスワードを変更する場合、［パスワード］を押します。

➔ パスワード入力画面を表示します。手順 9 で入力したユーザー名に対応した新しいユーザーパスワードを入力します。

➔ ユーザーパスワードは、半角の英数字（英字は大文字と小文字を区別）で 8 ～ 64 文字を入力します。

➔ 現在のパスワードを新パスワードとして設定できません。



［OK］を押すと、ユーザー登録変更画面にもどります。

12 E-mail アドレスを変更する場合、[E-mail アドレス] を押します。

➔ E-mail アドレス入力画面を表示します。

➔ E-mail アドレスは、半角の英数字および記号で 320 文字まで入力できます。

[OK] を押すと、ユーザー登録変更画面にもどります。

13 所属部門を変更する場合、[所属部門] を押します。

➔ 所属部門設定画面を表示します。任意の所属部門を選択します。

重要

認証方式の [ユーザー認証／部門認証連動] が [連動する] に設定されていると、[所属部門] を設定できます。

重要

所属部門は事前に登録されている必要があります。所属部門設定画面の所属部門名ボタンを 1 つ選択します。

[OK] を押すと、ユーザー登録変更画面にもどります。

14 上限設定を変更する場合は、[上限設定]を押します。認証を得て印刷できるようになったユーザーの出力枚数の上限値を変更します。

➔「管理方式」右の[トータル管理]を押し、「上限設定」右の[有効]を押し、[上限値]を押します。

➔ テンキーまたは[▲]、[▼]を押して、上限値を入力します。上限値は、0 ～ 99,999,999 の範囲で設定できます。

➔ [OK]を 2 回押すと、ユーザー登録画面にもどります。

➔ カラーとブラックの出力上限値を個別に変更できます。

➔「管理方式」右の[個別管理]を押し、「上限設定 - カラー」右、および「上限設定 - ブラック」右の[有効]を押し、[上限値]を押します。

➔ テンキーまたは［▲］、［▼］を押して、上限値を入力します。上限値は、0 ～ 99,999,999 の範囲で設定できます。

［OK］を 2 回押すと、ユーザー登録画面にもどります。

15 「使用可能な機能」右の［コピー操作］［スキャン操作］［プリンター印字］［HDD 一時保存操作］を押して、ユーザーに使用を認める本機の機能を選択します。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、「使用可能な機能」右の［プリンター印字］［ＨＤＤ 一時保存操作］から選択します。

16 「出力許可（印刷）」右の［カラー］、［ブラック］を押して、ユーザーに使用を認める印刷の種類を選択します。

17 ［OK］を押します。

➔ 入力が終わったら、ユーザー登録画面にある［前画面］を押します。
ユーザー認証設定メニュー画面にもどります。

2.3.3 ユーザー登録の削除

セキュリティー強化モード時に必要となるユーザー名およびパスワード、さらに個人フォルダーを削除します。

1 **操作パネル**の**設定メニュー／カウンター**を押し、設定メニュー画面を表示させます。

2 ［03 管理者設定］を押します。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、［02 管理者設定］を押します。

パスワード入力画面が表示されます。

3 管理者パスワードを入力します。

➔ 8 文字の半角英数字や記号の管理者パスワードを入力し［OK］を押します。

➔ 半角英字は大文字と小文字の区別をします。

➔ 間違ったパスワードや 8 文字未満の半角英数字や記号を入力して［OK］を押すと、［パスワードが一致しません　しばらくお待ち下さい］というメッセージを表示し、5 秒間いずれのキーやボタンも機能しなくなります。5 秒後に再度正しいパスワードを入力してください。

➔ 認証がうまくいかなかった情報は、監査ログとして保存します。

管理者設定メニュー画面が表示されます。

4 [04 ユーザー認証／部門管理] を押します。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、[03 ユーザー認証／部門管理] を押します。

ユーザー認証／部門管理メニュー画面が表示されます。

5 ［02 ユーザー認証設定］を押します。

ユーザー認証設定メニュー画面が表示されます。

6 ［02 ユーザー登録］を押します。

ユーザー登録画面が表示されます。

7 削除するユーザー名を押します。

8 ［削除］を押します。

➔ 削除確認のダイアログを表示します。

［はい］を押します。選択したユーザーを削除し、同時に個人フォルダーも削除されます。

2.3.4 ユーザーによるパスワードの変更

ユーザーは、ユーザー認証で必要なパスワードを変更できます。管理者がユーザー登録した後、ユーザーが自分自身のパスワードを再設定することをおすすめします。

重要

ユーザー認証を得ていない状態でユーザーパスワードを変更するとき、変更するユーザーパスワードに割当てられたユーザー名を入力する必要があります。

1 **操作パネル**の**設定メニュー／カウンター**を押し、設定メニュー画面を表示します。

2 ［02 ユーザー設定］を押します。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、[01 ユーザー設定] を押します。

ユーザー設定メニュー画面を表示します。

3 [08 パスワード変更] を押します。

➔ bizhub PRESS C1070P または bizhub PRESS C71hc をご使用の場合は、[04 パスワード変更] を押します。

パスワード変更画面を表示します。

4 ［ユーザー名］を押し、変更するパスワードに割当てられたユーザー名を入力します。

［OK］を押します。

5 ［現パスワード］を押し、手順 4 で入力したユーザー名に対応した現パスワードを入力します。

［OK］を押します。
入力したパスワードは、******** で表示されます。

➔ 半角英字は大文字と小文字の区別をします。

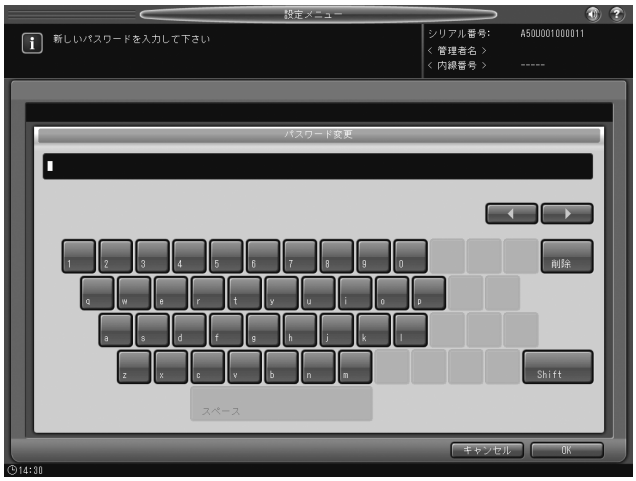
➔ 間違ったパスワードや 8 文字未満の半角英数字を入力して［OK］を押すと、［パスワードが一致しません］というメッセージを表示し、5 秒間いずれのキーやボタンも機能しなくなります。5 秒後に再度正しいパスワードを入力してください。

➔ 認証がうまくいかなかった情報は、監査ログとして保存します。

6 パスワード変更画面になり、新規パスワードを設定します。

➔ [新パスワード] を押し、手順 4 で入力したユーザー名に対応した新パスワードを入力します。

➔ ユーザーパスワードは、半角の英数字（英字は大文字と小文字を区別）で 8 ～ 64 文字を入力します。



[OK] を押します。

重要

名前、誕生日、社員番号など他人が容易に推測できるパスワードを設定しないでください。

➔ パスワードの設定がうまくいかなかった情報は監査ログとして保存されます。

➔ 現在のパスワードを、新パスワードとして設定できません。

7 再度、同じパスワードを確認のため入力します。

➔ [確認入力] を押し、再度、新パスワードを入力します。

[OK] を押します。

8 [OK] を押します。

ユーザー設定メニュー画面が表示されます。

9 [[設定メニュー] 終了] を押します。

設定メニュー画面を表示する前の画面にもどります。

MEMO

3 索引

3 索引

3.1 項目別索引

3.2 キー索引

MEMO

MEMO

MEMO

MEMO

MEMO

お問い合わせは

■ 販売店連絡先

《販売店 連絡先》

販売店名

電話番号

担当部門

担当者

■ 保守・操作・修理・サポートのお問い合わせ

この商品の保守・操作方法・修理・サポートについてのお問い合わせは、お買い上げの販売店、サービス実施店にご連絡ください。

《保守・操作・修理・サポートのお問い合わせ先》

TEL

コニカミノルタ ビジネスソリューションズ株式会社

〒105-0023　東京都港区芝浦1-1-1

当社についての詳しい情報はインターネットでご覧いただけます。　**http://bj.konicaminolta.jp**

当社に関する要望、ご意見、ご相談、その他お困りの点などございましたら、お客様相談室にご連絡ください。
お客様相談室電話番号　フリーダイヤル：0120-805039（受付時間 ： 土、日、祝日を除く9:00～12:00 / 13:00～17:00）

国内総販売元
コニカミノルタ ビジネスソリューションズ株式会社

製造元
コニカミノルタ株式会社

A50U957223

Printed in China
2015. 1