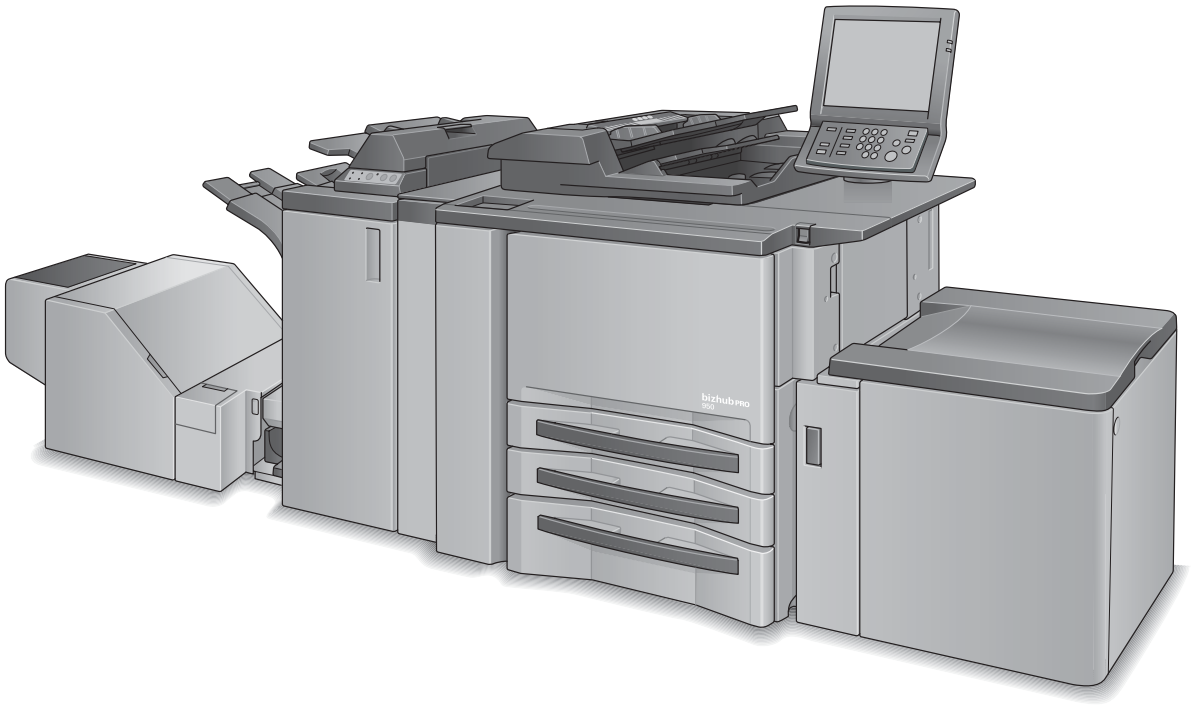
KONICA MINOLTA

The essentials of imaging

bizhub PRO 950

ユーザーズガイド　セキュリティー編



- セキュリティー機能
- セキュリティー強化モード
- 使用後の残存データの保護・消去
- 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時のHDD保存機能
- セキュリティー関連の管理者操作

登録商標について

- KONICA MINOLTA、KONICA MINOLTAロゴ、The essentials of imagingは、コニカミノルタホールディングス株式会社の登録商標です。
- PageScope、bizhub、bizhub PROは、コニカミノルタビジネステクノロジーズ株式会社の商標です。

免責

- 本書の一部または全部を無断で使用、複製することはできません。
- 製造会社および販売会社は、本書を運用した結果の影響につきましては、一切の責任を負いかねますのでご了承ください。
- このユーザーズガイドに記載されている情報は、予告なく変更される場合があります。

bizhub PRO 950 ユーザーズガイド

セキュリティー編

全体制御ソフトウェアのバージョンは、以下の通りです。
（本ソフトウェアは、画像制御プログラムとコントローラ制御プログラムで構成されています。）

画像制御プログラム（画像制御　I１）のバージョン：
A0Y50Y0-00I1-G00-10
A0Y50Y0-00I1-G00-20

コントローラー制御プログラム（ICコントローラー P）のバージョン：
A0Y5001-00P1-G00-10
A0Y5001-00P1-G00-11
A0Y5001-00P1-G00-20

ROMバージョン表示機能について

表紙に記載したbizhub PRO 950の全体制御ソフトウェア（画像制御プログラム／コントローラ制御プログラム）のバージョンは、サービス管理者（CE）のサービスモードのROMバージョン表示機能を使って確認できます。

ROMバージョンを表示させると、画像制御プログラム／コントローラー制御プログラムのバージョンが以下の様に表示されます。

A0Y50Y0-00I1-G00-**
画像制御プログラム（画像制御 I1): G00-2桁（例：G00-**）

A0Y5001-00P1-G00-**
コントローラー制御プログラム(IC コントローラー P):G00-2桁 (例:G00-**)

画像制御プログラム／コントローラー制御プログラムのバージョンを確認されるとき、お間違えのないようご注意ください。

マニュアル体系について

本機には、次のユーザーズガイドが用意されています。

■ ユーザーズガイド（コピー編） 印刷物 ユーザーズガイド CD
機械の概要やコピー操作について記載しています。
設置・取扱いの注意事項、電源の入れ方/切り方、用紙補給のしかた、紙づまりのなどのトラブル対処のしかたや、機械のコピー操作に関する内容を知りたい場合は、このユーザーズガイドをごらんください。

■ ユーザーズガイド（POD管理者編） 印刷物 ユーザーズガイド CD
日頃の使い方に合わせて機械をカスタマイズ設定したり、機械を管理する方法を記載しています。
用紙の登録やトレイの調整、ネットワーク設定を含む機械の設定や管理に関する内容を知りたい場合は、このユーザーズガイドをごらんください。

■ ユーザーズガイド（ネットワークスキャナー編） 印刷物 ユーザーズガイド CD
ネットワークスキャナー機能の操作について記載しています。
保存、読出し機能、スキャナー（Scan to HDD、Scan to E-mail、Scan to FTP、Scan to SMB）の使い方を知りたい場合は、このユーザーズガイドをごらんください。

■ ユーザーズガイド（セキュリティー編）＜本書＞ 印刷物 ユーザーズガイド CD
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関する内容を知りたい場合は、このユーザーズガイドをごらんください。

■ 商標/ライセンス ユーザーズガイド CD
商標およびライセンスについて記載しています。
本製品をお使いになる前に必ずお読みください。

■ ユーザーズガイド（プリンター編） ユーザーズガイド CD
プリンター機能の操作について記載しています。
PCLドライバー、Adobe PSドライバー、PageScope Web Connectionのユーザーモードに関する使用方法について知りたい場合は、このユーザーズガイドをごらんください。

■ ユーザーズガイド（PostScript3 Plug-inドライバー編） ユーザーズガイド CD
プリンター機能の操作について記載しています。
Plug-inドライバーのユーザーモードに関する使用方法について知りたい場合は、このユーザーズガイドをごらんください。

■ クイックガイド（プリンター編） 印刷物
ユーザーズガイド（プリンター編）のインストール部分を抜粋しています。

安全に正しくお使いになるため、操作の前に必ずユーザーズガイド コピー編
「第1章 設置・取扱いの注意」をお読みください。

もくじ

セキュリティー機能 1
■ 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 3
使用後の残存データの保護・消去 4
セキュリティー機能時のユーザー認証 5
■ ユーザーの登録 6
■ ユーザーの変更 10
■ ユーザーの削除 14
■ ユーザーによるパスワードの変更 17
セキュリティー強化モード時のHDD保存機能 19
■ データの保存（コピー） 19
■ データの保存（ボックス） 23
■ データの読出し／削除 26
■ 機密プリントデータの出力 30
セキュリティー関連の管理者操作 34
■ セキュリティー強化モードのON/OFF 34
■ HDDロックパスワード 37
■ 一時データ上書き削除 40
■ 全データ上書き削除 43
■ 監査ログのプリント 46
■ 監査ログの解析 48

セキュリティー機能

bizhub PRO 950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。通常モードはそれぞれのユーザーズガイドをごらんください。

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外部との接続の可能性がある場合に使用します。管理者を設定し、その管理者が本ガイドに従って機械を管理することで、一般利用者はデータ保護の立場からより安全な操作環境が提供されます。
セキュリティー強化モードのON/OFFやその他の制御はお客様の管理者だけが行うことができます。また、その管理者の設定はサービス実施店が行います。

セキュリティー強化モードをONにするためには、サービス実施店によって機械にCE認証パスワードおよび管理者パスワードが設定されている必要があります。
本体NICが設定されている場合は、セキュリティー強化モードの設定ができません。セキュリティー強化モードを設定する場合は、サービス実施店にお問い合わせください。

一般利用者の所有する個人ボックスやHDD（HDD1/HDD2）への不正なアクセスを防止するよう、セキュリティー強化モードをご利用になることをお勧めします。

セキュリティー強化モードがONされているかどうかは、管理者にお問い合わせください。

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

- 機械が社内のローカルネットに接続されているか、ファイアーウォールを介してインターネットに接続されている。また保守用に、一般の電話回線に接続されている。
- 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。

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勧めします。

- 機械設置場所
  機械は関係者のみが操作できる場所に設置します。また、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ください。
- 利用者の教育
  管理者は機械のセキュリティーを維持するための教育・啓蒙を利用者に実施します。利用者は管理者が設定したパスワード、自ら設定したパスワードを他者に知られないように管理します。ユーザーボックス作成時には、管理者はユーザー認証の解除方法を利用者に教育し、利用者は作業終了時にユーザー認証解除を行ってください。
- 管理者の資質
  責任者は管理者として十分な知識・技術そして経験をもち、かつ信頼のおける人物を選出し、管理を依頼します。
- サービス管理者（CE）の保証
  責任者または管理者はサービス管理者（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管理者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
  通信内容の盗聴を防ぐ機器、例えばWEP暗号（802.11x）などを用いたネットワークの構築を推奨します。

- メモリーやHDDにある使用後の残存データの保護・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（TIFF形式とPDF形式、PS）データの3種類があります。AHA圧縮データが書き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が、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恐れがあります。セキュリティー機能では下記のように確実にデータを消去してから画像領域を開放します。
  圧縮データか非圧縮データかに拘らず、保存したメモリーやHDDの画像領域を画像と無関係なデータで全て上書きした後にその領域を開放します。

- パスワードの強化
  パスワードは8～64文字の半角英数字(大文字と小文字は区別する）で構成されます。
  パスワード入力を間違えたときは、5秒間再入力を受け付けません。
- 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、保存したデータをプリントするときは、管理者があらかじめ設定した上記のように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、上記のように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られます。スキャンデータを保存したフォルダーまたはボックス自体の削除は管理者以外できなくなり、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、ユーザー認証を得なければならなくなります。

- 本体NICの設定
  セキュリティー強化モードをオンにしている場合、本体NICを使用することはできません。

- 外部からのアクセス禁止
  CS Remote Care以外の電話回線からのアクセスは全てできません。

- 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、操作を行った者を特定できる情報、操作内容、操作結果が保存され、不正なアクセスに対する解析が可能になります。また、監査領域が枯渇される時に上書きされます。

- 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
  管理者は、管理者パスワードを入力し認証されると管理者モードに入り各種機能の設定を変更する操作が可能となります。
  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させてから離れてください。

■ 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保護が強化されるデータ（対ユーザー）には下記のものがあります。

個人フォルダー（パスワード付き）が扱うデータ

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がローカルネットで接続されているとき、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でパスワードを入力するとパスワードの漏洩の恐れがありますので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。

セキュリティー強化モードがOFFの場合、データ漏洩の危険がありますので、特にご注意ください。

セキュリティー強化モードがONのときにデータへの不正アクセスや漏洩の事実がもしあったとしても、管理者が監査ログを解析しないと気が付かないことがあります。管理者が長時間不在になる場合は、ご注意ください。

使用後の残存データの保護・消去

コピー/スキャン/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は消去されます。

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する手段がありません。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ますので、解凍すること自体不可能になります。

メモリーに一時的に保存されたデータはジョブの中断、終了時点で不正データでの上書きクリアを行います。
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を行います。
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を行います。
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を行います。
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を行います。

セキュリティー機能時のユーザー認証

セキュリティー機能では、パスワードの設定条件が厳しくなります。ユーザー名およびパスワードの認証が必要です。管理者は、管理者設定でユーザー名およびパスワードを設定します。

ユーザー名： 1～64文字（英数字、日本語）
パスワード： 8～64文字（半角英数字）
大文字と小文字の区別をします。
認証時にパスワードを間違えたときは5秒間再入力を受け付けません。

パスワードに、名前、誕生日、社員番号など他人が容易に推測できるようなものを設定しないでください。

通常モードで設定したパスワードが8～64文字ではない場合、セキュリティー機能で使用できません。その場合、管理者にセキュリティー強化モードをいったんOFFしてもらい、上記条件に従ったパスワードを設定し直してください。

機械が下記の条件になると、再びユーザー名およびパスワードによる認証が必要になります。

主電源スイッチをOFFにする
副電源スイッチをOFFにする
ボックスのデータ出力動作を完了する
操作パネルの【パワーセーブ】を1秒間以上押す
オートリセット/オートシャットオフ機能が動作する

ユーザーがHDD内のパスワードが設定されているボックスにアクセスするとき、パスワードの認証操作は全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、部門振分け数を変更する必要があります。詳しくはPOD管理者編のユーザーズガイドをごらんください。

■ ユーザーの登録

セキュリティー機能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 〔06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文字の管理者パスワードを入力し〔OK〕を押します。

管理者設定メニュー画面が表示されます。

詳しく説明します

- 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。しばらくお待ちください」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。

4 〔03ユーザー認証/部門管理〕を押します。

5 〔03ユーザー認証設定〕を押します。

ユーザー認証設定画面が表示されます。

6 〔追加〕を押して、ユーザー登録追加画面を表示させます。

7 〔ユーザー No.〕、〔ユーザー名〕、〔パスワード〕、〔所属部門〕を登録します。

ユーザー登録追加画面

ユーザー No.の設定

ユーザー No.設定画面

(1) ユーザー登録追加画面の〔ユーザー No.〕を押します。
(2) 表示されたポップアップ画面のテンキーを使用して、任意のユーザー No.を入力します。
(3)〔OK〕を押すと、ユーザー登録追加画面に戻ります。

ユーザー名の設定

ユーザー名入力画面

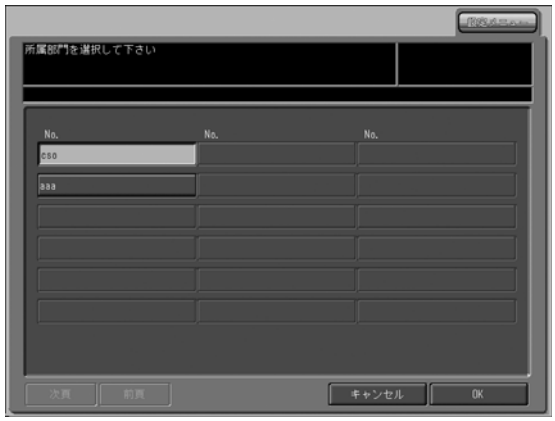
(1) ユーザー登録追加画面の〔ユーザー名〕を押します。

(2) ユーザー名入力画面が表示され、任意のユーザー名を入力します。
(3)〔OK〕を押すと、ユーザー登録追加画面に戻ります。

パスワードの設定
パスワード入力画面

(1) ユーザー登録追加画面の〔パスワード〕を押します。
(2) パスワード入力画面が表示され、任意のパスワードを入力します。
(3)〔OK〕を押すと、ユーザー登録追加画面に戻ります。

所属部門の設定
所属部門設定画面



(1) ユーザー登録追加画面の〔所属部門〕を押します。
(2) 所属部門設定画面が表示され、任意の所属部門を押して反転させます。
(3)〔OK〕を押すと、ユーザー登録追加画面に戻ります。

8 〔OK〕を押します。

入力が終わったら、ユーザー登録追加画面にある〔OK〕を押します。
ユーザー認証設定画面に戻ります。

■ ユーザーの変更

セキュリティー機能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 〔06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文字の管理者パスワードを入力し〔OK〕を押します。

管理者設定メニュー画面が表示されます。

詳しく説明します

- 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。しばらくお待ちください」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。

4 〔03ユーザー認証/部門管理〕を押します。

5 〔03ユーザー認証設定〕を押します。

ユーザー認証設定画面が表示されます。

6 変更したいユーザー名を押して、反転させます。

7 〔変更〕を押して、ユーザー登録変更画面を表示させます。

8 〔ユーザー名〕、〔パスワード〕、〔所属部門〕を変更します。

ユーザー登録変更画面

ユーザー名の変更

ユーザー名入力画面

(1) ユーザー登録変更画面の〔ユーザー名〕を押します。
(2) ユーザー名入力画面が表示され、任意のユーザー名を入力します。
(3)〔OK〕を押すと、ユーザー登録変更画面に戻ります。

パスワードの変更

パスワード入力画面

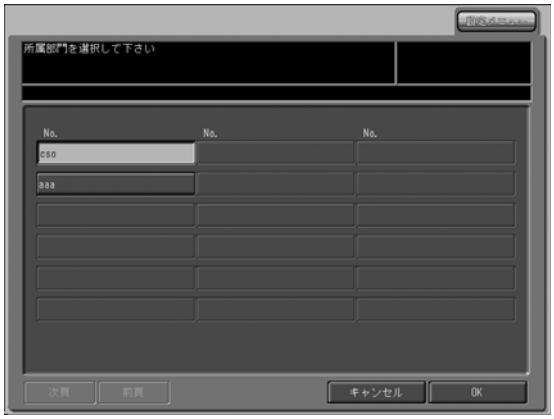
(1) ユーザー登録変更画面の〔パスワード〕を押します。

詳しく説明します

現在のパスワードを新パスワードとして設定することはできません。

(2) パスワード入力画面が表示され、任意のパスワードを入力します。
(3)〔OK〕を押すと、ユーザー登録変更画面に戻ります。

所属部門の変更
所属部門設定画面



(1) ユーザー登録変更画面の〔所属部門〕を押します。
(2) 所属部門設定画面が表示され、任意の所属部門を押して反転させます。
(3)〔OK〕を押すと、ユーザー登録変更画面に戻ります。

9 〔OK〕を押します。

入力が終わったら、ユーザー登録変更画面にある〔OK〕を押します。
ユーザー認証設定画面に戻ります。

■ ユーザーの削除

セキュリティー機能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 〔06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文字の管理者パスワードを入力し〔OK〕を押します。

管理者設定メニュー画面が表示されます。

詳しく説明します

- 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。

4 〔03ユーザー認証/部門管理〕を押します。

5 〔03ユーザー認証設定〕を押します。

ユーザー認証設定画面が表示されます。

6 削除するユーザー名を押して反転させます。

7 〔削除〕を押します。
削除確認のポップアップ画面が表示されます。

〔はい〕を押します。選択したユーザーが削除され、同時に個人フォルダーの削除も行なわれます。

■ ユーザーによるパスワードの変更

ユーザー認証で必要なパスワードをユーザーが変更することができます。管理者によってユーザー登録された後、ユーザー自身でパスワードを再設定することをおすすめします。

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 〔01環境設定〕を押します。

環境設定メニュー画面が表示されます。

3 〔08ユーザーパスワード変更〕を押します。
ユーザー認証画面が表示されます。

4 〔ユーザー名〕を押し、ユーザー名を入力します。
画面上にユーザー名が表示されます。

5 〔パスワード〕を押し、現在のパスワードを入力します。
入力したパスワードは、********で表示されます。

6 認証が成功すると、ユーザー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、新パスワードを入力します。
〔OK〕を押します。

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。
環境設定メニュー画面が表示されます。

9 〔終了〕を押します。
コピー画面が表示されます。

詳しく説明します

- 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。

必ず守ってください

パスワードに、名前、誕生日、社員番号など他人が容易に推測できるようなものを設定しないでください。

詳しく説明します

- 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することはできません。

セキュリティー強化モード時のHDD保存機能

データを保存/出力する場合、HDDに格納されているボックスを使用します。データ漏洩/改ざん防止のため、パスワードが設定されているボックスの使用をお勧めします。
重要な機密文書などを保存する際は、必ずセキュリティー強化モードを設定してください。
管理者は、何らかの理由で一時的にセキュリティー強化モードをOFFした場合、OFFしたことを利用者に伝えて下さい。
ボックスへのデータ保存や保存されているデータの出力操作については別に説明しています。詳細は、ネットワークスキャナー編のユーザーズガイドをごらんください。

■ データの保存（コピー）

セキュリティー強化モード時に、HDDに格納されているボックスにデータをコピーしながら保存する手順を説明します。

1 表示されているユーザー認証画面の〔ユーザー名〕、〔パスワード〕の各ボタンを押して、それぞれ入力します。

ユーザー認証画面の〔ユーザー名〕を押すと、ユーザー名入力画面が表示されます。
設定したユーザー名を入力し、〔OK〕を押します。

ユーザー認証画面に戻ります。

詳しく説明します

- 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。

ユーザー認証画面の〔パスワード〕を押すと、パスワード入力画面が表示されます。
設定したパスワードを入力し、〔OK〕を押します。

ユーザー認証画面に戻ります。

2 〔OK〕を押します。
コピー画面が表示されます。

3 コピー画面の〔出力設定〕を押します。

4 出力設定画面の〔HDD保存〕を押します。

個人のボックス一覧画面が表示されます。

5 任意の個人のボックスを選択して、〔OK〕を押します。

個人のボックスにパスワードを設定している場合、パスワードを入力します。
個人のファイル選択画面が表示されます。

6 〔新規保存〕を押します。

ファイル名入力画面が表示されます。

7 ファイル名を入力して、〔OK〕を押します。

8 操作パネルの【スタート】を押します。出力を開始します。HDDへの保存も開始します。

9 作業終了後に操作パネルの【ID】を押して、認証を解除します。
認証画面が表示されて、作業できなくなります。

■ データの保存（ボックス）

セキュリティー強化モード時に、HDD に格納されているボックスにデータを保存します。

1 表示されているユーザー認証画面の〔ユーザー名〕、〔パスワード〕の各ボタンを押して、それぞれ入力します。

ユーザー認証画面の〔ユーザー名〕を押すと、ユーザー名入力画面が表示されます。
設定したユーザー名を入力します。
〔OK〕を押すと、ユーザー認証画面に戻ります。

ユーザー認証画面の〔パスワード〕を押すと、パスワード入力画面が表示されます。
設定したパスワードを入力します。
〔OK〕を押すと、ユーザー認証画面に戻ります。

詳しく説明します

- 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。

2 〔OK〕を押します。

コピー画面が表示されます。

3 〔保存〕タブを押し、〔スキャンして HDD へ保存〕を選択します。

個人のボックス一覧画面が表示されます。

4 任意の個人のボックスを選択し、〔OK〕を押します。

個人のボックスにパスワードを設定している場合、パスワードを入力します。
個人のファイル選択画面が表示されます。

5 〔新規保存〕を押します。

6 ファイル名を入力して、〔OK〕を押します。

スキャン画面が表示されます。

7 操作パネルの【スタート】でファイルを読み込み、保存します。

8 作業終了後に操作パネルの【ID】を押し、認証を解除します。

認証画面が表示されて、作業できなくなります。

■ データの読出し／削除

セキュリティー強化モード時に、HDD に格納されているボックスのデータを読出し／削除します。

1 表示されているユーザー認証画面の〔ユーザー名〕、〔パスワード〕の各ボタンを押して、それぞれ入力します。

ユーザー認証画面の〔ユーザー名〕を押すと、ユーザー名入力画面が表示されます。
設定したユーザー名を入力し、〔OK〕を押します。

ユーザー認証画面に戻ります。
ユーザー認証画面の〔パスワード〕を押すと、パスワード入力画面が表示されます。
設定したパスワードを入力し、〔ＯＫ〕を押します。

ユーザー認証画面に戻ります。

2 〔OK〕を押します。
コピー画面が表示されます。

3 〔読出し〕タブを押します。

個人のボックス一覧画面が表示されます。

4 任意の個人のボックスを選択して、〔OK〕を押します。

個人のボックスにパスワードを設定している場合、パスワードを入力します。
個人のファイル選択画面が表示されます。

5 ファイルの読出しまたは削除を行います。

読出す場合
(1) 読み出すファイル名を選択して〔＞＞＞〕を押します。

詳しく説明します

- 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。

(2)〔自動〕、〔プルーフ〕、〔ウェイト〕のいずれかのボタンを選択し、〔OK〕を押します。
(3) テンキーで設定部数を入力します。

(4) 読み出すファイルの出力ページを設定します。
〔出力ページ変更〕を押します。
1ページのみ出力する場合は、〔ページ指定〕を押します。テンキーでページ番号を入力します。
全ページ出力する場合は、〔全ページ〕を押します。
〔OK〕を押して出力します。

削除する場合
(1) 削除するファイル名を選択して、〔ファイル削除〕を押します。削除確認のポップアップ画面が表示されます。
(2)〔はい〕を押します。

(3) 選択したファイルが削除され、ファイル選択画面にもどります。

6 作業終了後に操作パネルの【ID】を押し、認証を解除します。
認証画面が表示され、作業できなくなります。

■ 機密プリントデータの出力

PC側での機密プリント指令：

PC側で機密プリント出力設定を行なう場合、あらかじめパスワード付きの機密フォルダーを登録している必要があります。最大8文字の機密フォルダー名（半角英数字）を入力します。

機械側での機密プリントの出力：

1 表示されているユーザー認証画面の〔ユーザー名〕、〔パスワード〕の各ボタンを押して、それぞれ入力します。

ユーザー認証画面の〔ユーザー名〕を押すと、ユーザー名入力画面が表示されます。
設定したユーザー名を入力し、〔OK〕を押します。

ユーザー認証画面に戻ります。

ユーザー認証画面の〔パスワード〕を押すと、パスワード入力画面が表示されます。
設定したパスワードを入力し、〔OK〕を押します。

ユーザー認証画面に戻ります。

2 〔OK〕を押します。
コピー画面が表示されます。

3 〔読出し〕タブを押します。

個人のボックス一覧画面が表示されます。

4 〔機密フォルダー〕を押し、機密のボックス一覧画面を表示させます。

詳しく説明します

- 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。

5 任意の機密のボックスを選択して、〔OK〕を押します。

6 機密プリントで設定した機密パスワードを入力します。
〔OK〕を押します。
機密のファイル一覧画面が表示されます。

7 任意の機密のファイルを押して選択します。

8 〔自動〕、〔プルーフ〕、〔ウェイト〕のいずれかのボタンを選択して出力して、〔OK〕を押します。
(1) テンキーで設定部数を入力します。

(2) 読み出すファイルの出力ページを設定します。
〔出力ページ変更〕を押します。
1ページのみ出力する場合は、〔ページ指定〕を押します。テンキーでページ番号を入力します。
全ページ出力する場合は、〔全ページ〕を押します。
〔OK〕を押して出力します。

9 作業終了後に操作パネルの【ID】を押し、認証を解除します。
認証画面が表示され、作業できなくなります。

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は管理者が管理者操作によって行ないます。その前提として、機械に8文字のCE認証パスワードおよび管理者パスワードが設定されていなければなりません。管理者パスワードの設定をサービス実施店にお申し出ください。また管理者パスワードを変更する場合は、管理者がパスワードを変更して下さい。（管理者パスワードの変更手順は、ユーザーズガイドPOD管理者編を御覧下さい。）
機械のデータを漏洩や不正アクセスから守るため、管理者をたててセキュリティー強化モードをご利用になることをおすすめします。

■ 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の設定方法を説明します。

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

2 〔06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文字の管理者パスワードを入力し〔OK〕を押します。

管理者設定メニュー画面が表示されます。

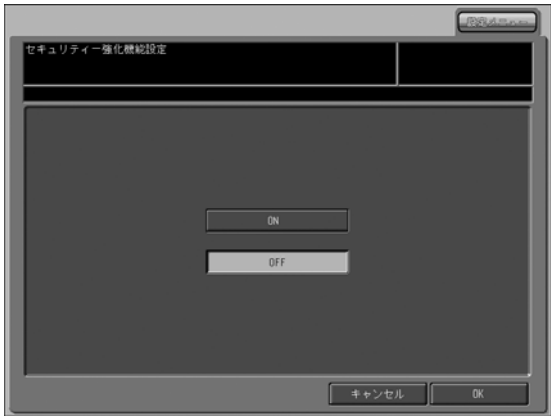
詳しく説明します

- 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。

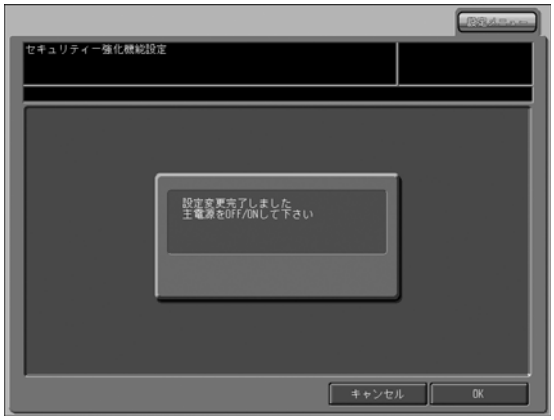
4 〔07セキュリティー設定〕を押します。

5 〔03セキュリティー強化モード〕を押します。

6 セキュリティー機能のON/OFFを設定します。
セキュリティー機能を使用する場合は〔ON〕、使用しない場合は〔OFF〕を押して反転させます。



7 〔OK〕を押します。
セキュリティー強化設定の変更確認のポップアップ画面が表示されます。
〔はい〕を押します。



8 副電源スイッチをオフにして、主電源スイッチをOFFにします。

9 10秒以上待ちます。

10 主電源スイッチをオンにして、副電源スイッチをオンにします。

必ず守ってください

「電源OFF処理中です　主電源をきらないでください」の表示が消えてから主電源スイッチをオフにしてください。

■ 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にロックパスワード（8～32文字/半角英数字、大文字と小文字の区別あり）を設定できます。ロックパスワードをかけることで、HDDの内容を保護します。HDD単体で外部からアクセスされた場合、ロックパスワードが一致しないとHDD内部のデータは読み出すことができません。

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 〔06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文字の管理者パスワードを入力し〔OK〕を押します。

管理者設定メニュー画面が表示されます。

詳しく説明します

- HDDロックパスワードはセキュリティー強化モードON時のみ機能します。セキュリティー強化モードOFF時には「セキュリティー強化機能を設定してください」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時にはHDDロックパスワードを設定することをおすすめします。

詳しく説明します

- 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。

4 〔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 HDDロックパスワード変更〕を押します。

HDD管理パスワード変更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ます。
(初回パスワードは、本体シリアルNo、9桁)

〔OK〕を押します。

8 認証が成功すると、〔新パスワード〕を押して入力します。
認証が成功するまではボタンを押しても反応しません。
〔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。
〔OK〕を押します。

10 HDD管理パスワード変更画面の〔OK〕を押します。

必ず守ってください

パスワードに、名前、誕生日、社員番号など他人が容易に推測できるようなものを設定しないでください。

詳しく説明します

- 本体シリアルNoは、設定メニュー画面の左上または監査ログプリントの右上に9桁で表示されてます。
  詳しくは、セキュリティー関連の管理者操作、「監査ログのプリント」を参照して下さい。
- 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することはできません。

■ 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、そのレベルを2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、設定メニュー画面を表示させます。

2 〔06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文字の管理者パスワードを入力し〔OK〕を押します。

管理者設定メニュー画面が表示されます。

詳しく説明します

- 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。

4 〔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 〔04 一時データ上書き削除〕を押します。

一時データ上書き削除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〕または〔しない〕を押します。

8 上書き削除する場合はモード選択します。
〔モード1〕または〔モード2〕を押します。

詳しく説明します

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画面の〔ＯＫ〕を押します。

■ 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全て削除します。そのとき、消去レベルを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、設定メニュー画面を表示させます。

2 〔06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文字の管理者パスワードを入力し〔OK〕を押します。

管理者設定メニュー画面が表示されます。

必ず守ってください

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申し出ください。

詳しく説明します

- 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。

4 〔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 〔05全データ上書き削除〕を押します。

全データ上書き削除画面が表示されます。

7 消去モードを選択し、〔削除実行〕を押します。

8 全データ上書き削除画面の〔前画面〕を押します。

必ず守ってください

〔削除実行〕で削除するとHDDのデータは全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。

■ 監査ログのプリント

機械に保存されているデータに対してアクセスされたとき、監査ログが自動的に生成されます。保存されたすべての監査ログデータを出力します。

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

2 〔06 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 文字の管理者パスワードを入力し〔OK〕を押します。

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 〔04管理リストプリント〕を押します。

管理リストプリント画面が表示されます。

6 〔監査ログレポート〕を選択し、〔コピー〕タブを押します。

7 操作パネルの【スタート】を押します。

詳しく説明します

プリントを中止する場合は、操作パネルの〔ストップ〕を押します。中止確認のポップアップ画面が表示されます。〔中止〕を選択すると、プリントが中止されます。

■ 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対して不正なアクセスや改ざんなどの事実があったとき、または定期的（一ヶ月に１回程度）に、管理者によって解析される必要があります。
監査ログに保存される項目の使用頻度は、750件／月以下を想定しています。月に750件以上使用することが想定される場合には、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
2009/04/16 16:03
A0Y5001902002
TC:1724

No	date/time	id	action	result	No	date/time	id	action	result
0001	2009/04/16 16:03	-2	04	OK	0002	2009/04/15 15:34	0	14	OK
0003	2009/04/15 15:22	0	13	OK	0004	2009/04/15 15:22	0	13	OK
0005	2009/04/15 15:08	0	13	OK	0006	2009/04/15 15:07	0	13	OK
0007	2009/04/15 15:07	0	13	OK	0008	2009/04/15 15:01	0	13	OK
0009	2009/04/15 15:01	0	13	OK	0010	2009/04/15 15:01	0	13	OK
0011	2009/04/14 12:36	1	13	OK	0012	2009/04/14 12:31	1	13	OK
0013	2009/04/14 12:31	1	13	OK	0014	2009/04/14 12:30	1	13	OK
0015	2009/04/14 12:30	1	13	OK	0016	2009/04/13 12:51	-3	11	NG
0017	2009/04/13 12:42	1	07	OK	0018	2009/04/10 15:22	1	13	OK
0019	2009/04/10 15:22	1	13	OK	0020	2009/04/10 14:24	-3	11	NG
0021	2009/04/10 14:24	-3	11	NG	0022	2009/04/10 14:24	-3	11	NG
0023	2009/04/10 11:25	-1	05	OK	0024	2009/04/10 11:25	-1	05	OK
0025	2009/04/10 11:25	-1	01	OK	0026	2009/04/10 11:24	-2	02	OK
0027	2009/04/10 11:22	-2	02	OK	0028	2009/04/10 11:21	-2	02	OK
0029	2009/04/03 15:39	1	13	OK	0030	2009/04/03 14:12	1	13	OK
0031	2009/04/03 11:58	-1	01	OK	0032	2009/04/03 11:58	-2	02	OK
0033	2009/04/03 11:57	-2	02	OK	0034	2009/04/03 11:56	-2	02	OK
0035	2009/04/02 10:32	1	13	OK	0036	2009/04/02 10:16	1	13	OK
0037	2009/04/02 10:09	1	13	OK	0038	2009/04/02 10:07	1	09	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なわれた年月日と時間が記載されます。
2. id：操作を行なった人物、またはセキュリティー保護対象を特定します。
   「-1」：サービス管理者による操作
   「-2」：管理者による操作
   「-3」：未登録のユーザーによる操作
   それ以外の整数：それぞれのセキュリティー保護対象を表していますが、下記IDでその保護対象を限定します。
   ユーザーID（1～1000の数字）
   機密ユーザーID（1～99999の数字）
3. action：操作された内容を特定します。対応表でactionの示す操作内容を確認します。
4. result：操作内容の結果が記載されます。パスワード認証に関する結果に対しては、成功/失敗をOK/NGで表示します。パスワードによる認証操作を伴わない操作の結果は、すべて成功（OK）が記載されます。

監査ログに保存される項目の対応表

No	操作	id	保存される action	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	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
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/ 未登録ユーザー ID	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	ファイルへのアクセス (ドキュメントデータの読出し)	ユーザー ID	13	OK
14	ファイルの削除(ドキュメントデータの削除)	ユーザー ID	14	OK
15	ファイルの属性変更	ユーザー ID	15	OK
16	機密プリントパスワード認証	機密ユーザー ID/ 未登録ユーザー ID	16	OK/NG
17	機密プリントファイルへのアクセス	機密ユーザー ID	17	OK
18	機密プリントファイルの削除	機密ユーザー ID	18	OK
19	HDD ロックパスワードの変更	管理者 ID	19	OK

監査ログの解析目的は

データに対する攻撃の有無
攻撃の対象
攻撃の内容
攻撃による結果を把握し、対策を講じることです。

具体的な解析方法は次ページをご参照ください。

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、16）の結果に「NG」が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への攻撃の可能性があります。

- 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（NG）した時間に不正な行為を行ったかどうかを確認します。
- パスワード認証が成功（OK）の場合でも、actionが正当な操作対象の人物によって行われたのかどうかを確認します。特に、認証が失敗（NG）の連続の後に成功（OK）した場合や、通常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全て成功（OK）と記載されるので、不正行為の有無の判断はactionとidによって判断します。

- id だけでは攻撃された対象を特定できないので、アクションと全ページの対応表を参照して、不正行為の対象が個人のボックスか機密のボックスかを特定します。
- 操作された時間を確認し、特定した対象を操作する人物に不正な行為を行ったかどうかを確認します。

(例)

ボックスに保存されていたドキュメントが不正な認証によってプリントされた場合、以下の監査ログが保存されます。

1. ボックスへのパスワード認証：
   action ＝11
   id ＝認証の対象となったボックス
   result ＝OK/NG
2. ボックス内のドキュメントへのアクセス：
   action ＝13
   id ＝認証の対象となったボックス

上記の操作が行われた日時を確認し、該当する個人のボックスまたは機密のボックスのドキュメントへの操作が正当な個人のボックスまたは機密のボックス所有者によって行われたものかを確認します。

不正行為発見時の対応

- 監査ログ解析の結果、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、本来の所有者のアクセスが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り合い、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。

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

〒103-0023 東京都中央区日本橋本町1丁目5番4号

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）

KONICA MINOLTA

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 ビジネステクノロジーズ株式会社
〒100-0005 東京都千代田区丸の内一丁目6番1号 丸の内センタービルディング

A0Y5956611

Printed in China
2009. 8