3. 情報の漏洩を防止する

文書の複製を抑止・ガードする

本機のプリンター機能では、プリンタードライバーの設定で、不正コピーを抑止・ガードするための地紋をつけて印刷することができます。
不正コピー抑止は、プリンタードライバーで設定した文字列地紋（「コピー禁止」などの任意の文字列）が浮き上がるため、不正な文書複製を抑止します。
不正コピーガードは、プリンタードライバーで不正コピーガード専用の地紋を設定して印刷すると、その文書の読み取りを行った際に文書全体がグレー地に変換されるため、文書情報の漏洩を防止します。ただし、グレー地に変換するためには、文書の読み取りを行う複写機／複合機に不正コピーガードモジュールが必要です。
詳細については、以下を参照してください。

♦ **不正コピー抑止機能**
プリンタードライバーで不正コピー抑止印刷を設定して印刷します。
設定方法については、「不正コピー抑止印刷設定（プリンタードライバーの設定）」を参照してください。

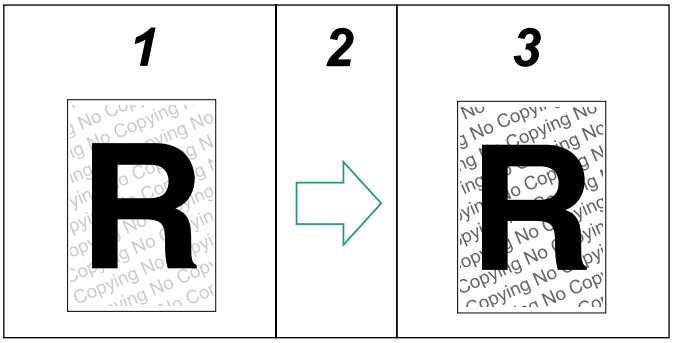
♦ **不正コピーガード機能**
プリンタードライバーで不正コピーガード印刷を設定して印刷します。
設定方法については、「不正コピーガード印刷設定（プリンタードライバーの設定）」を参照してください。

参照

・P.60 「不正コピー抑止印刷設定（プリンタードライバーの設定）」
・P.61 「不正コピーガード印刷設定（プリンタードライバーの設定）」

不正コピー抑止機能

プリンタードライバーで不正コピー抑止のための背景地紋と文字列地紋（任意の文字列「コピー禁止」など）を設定した文書を印刷することができます。不正コピー抑止のための地紋をつけて印刷した文書を、本機、または他の複写機／複合機でコピーや蓄積を行うと、文字列地紋（「コピー禁止」など）が浮き上がるため、不正な文書複製を抑止します。



BBK004S

重要

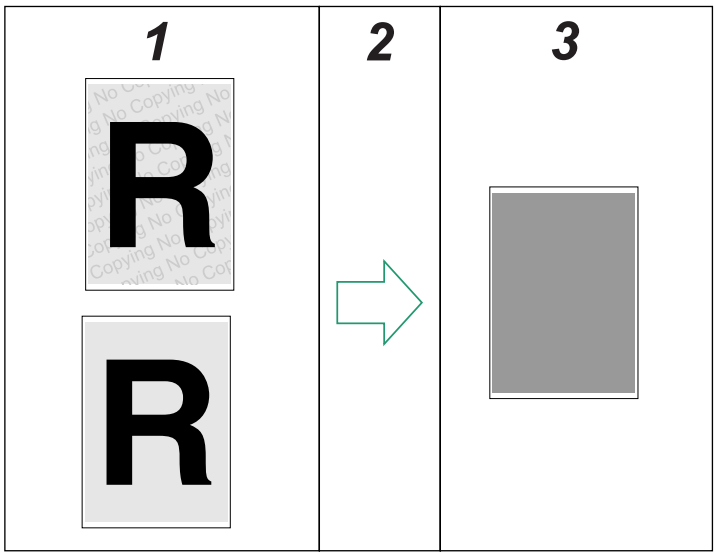
- 不正コピー抑止機能は、文書の複製を抑止するものであり、情報漏洩を防止するものではありません。
- 地紋効果は、コピー結果を、すべて保証しているものではありません。
- 不正コピー抑止印刷した文書のコピー結果は、使用する機種と原稿読み取りの設定条件により異なります。

補足

- 不正コピー抑止印刷のための文字列地紋を効果的に浮き上がらせるために、文字列サイズは 70 ～ 80pt（最低 50pt）、文字列角度は 30 ～ 40 度の範囲内で設定してください。
- 本機にユーザー認証が設定されている場合、プリンター機能を使用するにはログインユーザー名とログインパスワードがプリンタードライバーに設定されている必要があります。プリンタードライバーのヘルプを参照してください。

不正コピーガード機能

プリンタードライバーで不正コピーガードのための地紋を設定した文書（以降、不正コピーガード文書と呼びます）を印刷することができます。不正コピーガード文書をコピーしたときにグレー地に変換する効果を得るためには、オプションの不正コピーガードモジュールが搭載されている必要があります。不正コピーガード文書を、不正コピーガードモジュールが搭載された複写機／複合機でコピーや蓄積を行うと、文書の全体をグレー地に変換し、不正なコピーからガードします。不正コピーガードモジュールを搭載した機器で不正コピーガード文書を検知したときに、本機からブザー音が鳴ります。また、不正コピーのログが残ります。



BBK005S

重要

- 不正コピーガードモジュールが搭載されていない複写機／複合機で、不正コピーガードのための地紋が入った文書をコピーすると、文字列を入れている場合は文字列が浮き上がります。ただし、使用する複写機／複合機の機種と原稿読み取りの設定条件によって、文字の浮き上がり方は異なります。

補足

- 不正コピーガードのための文書には、文字列を設定して印刷することも可能です。ただし、不正コピーガードモジュールが搭載された複写機／複合機でのコピー結果は、グレー地に変換されるため文字列は浮き上がりません。
- 誤検知が発生した場合は、サービス実施店に相談してください。

印刷時の制限事項

不正コピー抑止のための文書、また不正コピーガードのための文書を印刷する場合の制限事項は以下のとおりです。

♦ **不正コピー抑止 / 不正コピーガード文書印刷時共通**
- RPCS プリンタードライバーを使用した印刷のみに対応しています。
- 解像度 200dpi での印刷には対応していません。
- 印刷するデータに対して、部分的に地紋をつけることはできません。
- 文字列地紋はプリンタードライバーの文字列テキストボックスで入力した文字のみ入れることができます。
- 地紋をつけて印刷するため、通常の印刷に比べると出力に時間がかかります。

♦ **不正コピーガード文書印刷時のみ**
- 用紙サイズは B5 以上を使用してください。
- 用紙種類は普通紙、または白色度 70%以上の再生紙を使用してください。
- 両面印刷は可能ですが、裏面の文字や模様が透けることにより、機能が正常に動作しない場合があります。

おことわり

1. 当社は、不正コピー抑止地紋による不正コピー抑止効果および不正コピーガード機能が、常時有効に機能することを保証するものではありません。使用する用紙ならびにコピー機の機種および設定条件等によっては、不正コピー抑止地紋による不正コピー抑止効果および不正コピーガード機能が有効に機能しない場合もあります。この点をご理解の上、ご使用ください。
2. 不正コピー抑止地紋および不正コピーガード機能を使用または使用できなかったことにより生じた損害については、当社は一切その責任をおいかねますので、あらかじめご了承ください。

不正コピー抑止印刷と不正コピーガード印刷の設定

不正コピー抑止印刷設定（プリンタードライバーの設定）

出力文書に対してプリンタードライバーで不正コピー抑止印刷を設定します。
本機にユーザー認証が設定されている場合、プリンター機能を使用するにはログインユーザー名とログインパスワードがプリンタードライバーに設定されている必要があります。プリンタードライバーのヘルプを参照してください。
プリンタードライバーでの不正コピー抑止印刷の操作については、プリンタードライバーのヘルプを参照してください。

1 **プリンタードライバーの設定画面を表示します。**

2 **［編集］タブの「不正コピー抑止」のチェックボックスをチェックします。**

3 [詳細] をクリックします。

4 「不正コピー抑止文字列」グループの「文字列」ボックスに文字列を入力します。
その他、フォントの種類、スタイル、サイズ等を設定します。

5 [OK] をクリックします。

不正コピーガード印刷設定（プリンタードライバーの設定）

この機能を使用して出力した印刷用紙を、不正コピーガードモジュール搭載の複写機／複合機でコピーや蓄積すると、全体をグレー地にします。
出力文書に対してプリンタードライバーで不正コピーガード印刷を設定します。
本機にユーザー認証が設定されている場合、プリンター機能を使用するにはログインユーザー名とログインパスワードがプリンタードライバーに設定されている必要があります。詳しくはプリンタードライバーのヘルプを参照してください。
プリンタードライバーでの不正コピーガード文書を印刷するときの操作については、プリンタードライバーのヘルプを参照してください。
不正コピーガードの詳細については、「不正コピーガード機能」を参照してください。

1 プリンタードライバーの設定画面を表示します。

2 [編集] タブの「不正コピー抑止」のチェックボックスをチェックします。

3 [詳細] をクリックします。

4 「不正コピー抑止地紋」グループの「不正コピーガード」をチェックします。

5 文字列を入れたい場合は、「不正コピー抑止文字列」グループの「文字列」ボックスに文字列を入力します。
その他、フォントの種類、スタイル、サイズ等を設定します。

6 [OK] をクリックします。

参照

・P.59 「不正コピーガード機能」

文書を他人に見せないように印刷する

この機能を使用するためには、プリンター機能が必要です。
本機の設置場所がユーザーの席から離れている場合など、移動する間に印刷した文書を他人に見られてしまうことがあります。このように他人に見せたくない文書を印刷するときは、機密印刷機能を利用します。

♦ **機密印刷機能**
プリンターの機密印刷機能を使用し、出力文書を機密印刷文書として本機に蓄積してから印刷します。本機の操作パネルを使用して印刷し、印刷した文書をすぐに回収できるため、他人に見られることを防止することができます。

補足

・一時的な文書の保存をする場合には、プリンタードライバーの「印刷方法」で［プリンターに保存する］を選択します。また、［プリンターに保存するジョブを共有する］を選択すると、ジョブの共有ができます。

機密印刷を設定する

プリンタードライバーで出力文書に機密印刷を設定します。
ユーザー認証を設定している場合、プリンタードライバーでユーザー認証のためのログインユーザー名とログインパスワードが設定されている必要があります。設定方法は、プリンタードライバーのヘルプを参照してください。
ユーザー認証が設定されていない場合でも機密印刷することができます。設定方法は、『ソフトウェアガイド』「いろいろな印刷」を参照してください。

1 **プリンタードライバーの設定画面を表示します。**

2 **［基本］タブの「印刷方法」で［機密印刷］を選択します。**

3 **［印刷方法の詳細］をクリックします。**

4 **ユーザー ID とパスワードを入力します。**
ここでのパスワードは、機密印刷文書のためのパスワードです。機密印刷文書を印刷するとき、操作パネルで同じパスワードを入力してください。
機密印刷のパスワードはデータ通信時に暗号化されます。
ユーザー ID は半角英数字 8 文字以内で入力してください。
パスワードは半角数字 4 桁～ 8 桁で入力してください。

5 **［OK］をクリックします。**
確認のメッセージが表示されます。

6 **パスワードを再入力します。**

7 **［OK］をクリックします。**

8 **印刷を実行します。**

補足

・設定方法について、詳しくは『ソフトウェアガイド』またはプリンタードライバーのヘルプを参照してください。

機密印刷文書を印刷する

機密印刷文書を印刷したいユーザーは、本機の前に移動し、操作パネルで機密印刷文書を印刷します。
機密印刷文書の印刷にはパスワードが必要です。ユーザーが設定したパスワードを忘れた場合は、文書管理者がパスワードの変更を行えます。
Web Image Monitor からも設定することができます。Web Image Monitor のヘルプを参照してください。

1 **[文書印刷] を押します。**

2 **[▲][▼]キーを押して「機密印刷文書」を選択し、[文書リスト]を押します。**
ログインしているユーザーの機密文書のみ表示されます。
保存文書を印刷する場合は「保存文書」を選択し、[文書リスト] を押します。

3 **[▲] [▼] キーを押して印刷する機密文書を選択し、[印刷] を押します。**
パスワード入力画面が表示されます。

4 **パスワードを入力し、[OK] キーを押します。**
「機密印刷を設定する」の手順 **4** で設定したパスワードを入力します。

5 **[印刷] を押します。**
機密印刷文書が印刷されます。

補足

・ユーザー認証のログイン、ログアウトの方法は、「ユーザー認証が設定されているとき」を参照してください。

参照

・P.50 「ユーザー認証が設定されているとき」

機密印刷文書を消去する

文書作成者（オーナー）が操作します。機密印刷文書を消去するには、機密印刷文書のパスワードが必要です。パスワードを忘れた場合には、文書管理者にパスワードの変更を依頼してください。文書管理者が文書を消去することもできます。
Web Image Monitor からも設定することができます。Web Image Monitor のヘルプを参照してください。

1. [文書印刷] を押します。
2. [▲][▼]キーを押して「機密印刷文書」を選択し、[文書リスト]を押します。
   保存文書を削除する場合は「保存文書」を選択し、[文書リスト] を押します。
3. [▲] [▼] キーを押して対象文書を選択し、[消去] を押します。
   パスワード入力画面が表示されます。
4. 機密文書のパスワードを入力し、[OK] キーを押します。
5. [消去] を押します。
   文書が消去されます。

機密印刷文書のパスワードを変更する

文書作成者（オーナー）が操作します。文書管理者も操作することができます。
文書作成者（オーナー）がパスワードを忘れた場合には、文書管理者がパスワードの変更を行います。
Web Image Monitor からも設定することができます。Web Image Monitor のヘルプを参照してください。

1. [文書印刷] を押します。
2. [▲][▼]キーを押して「機密印刷文書」を選択し、[文書リスト]を押します。
3. [▲] [▼] キーを押して対象文書を選択し、[変更] を押します。
4. 設定されているパスワードをスクロールキーで入力し、[OK] キーを押します。
   文書管理者が操作する場合は入力する必要はありません。
5. [OK] キーを押します。
6. 新しいパスワードを入力し、[OK] キーを押します。
7. 確認用パスワードを入力し、[OK] キーを押します。

機密印刷文書ロック解除の設定

セキュリティー強化機能の「文書保護強化」を［する］に設定した場合、誤ったパスワードを 10 回入力すると文書はロックされ、アクセスできなくなります。ここでは、ロックされた文書の解除方法を説明します。
文書管理者のみロックされた文書のロックを解除することができます。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。
Web Image Monitor からも設定することができます。Web Image Monitor のヘルプを参照してください。
「文書保護強化」について詳しくは、「セキュリティー強化機能を設定する」を参照してください。

1 ［文書印刷］を押します。

2 [▲][▼]キーを押して「機密印刷文書」を選択し、[文書リスト]を押します。

3 ［▲］［▼］キーを押して対象文書を選択し、［変更］を押します。

4 [▲][▼]キーを押して「文書ロック解除」を選択し、[OK]キーを押します。

5 ［ロック解除］を押します。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」
・P.129 「セキュリティー強化機能を設定する」

アドレス帳の登録情報を保護する

アドレス帳のデータに対して、ユーザーのアクセス権を設定することができます。
この設定により、登録されたユーザー以外の第三者に対してアドレス帳のデータの不正利用を防止することができます。
また、アドレス帳のデータを暗号化し、データの読み取りを防止することができます。

アドレス帳のアクセス権を設定する

アドレス帳登録者が設定します。フルコントロールの設定になっているユーザーもアクセス権を設定することができます。
ユーザー管理者も設定することができます。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。

1. Web Image Monitor を起動し、管理者モードでログインします。
2. [アドレス帳] をクリックします。
3. 変更したいユーザーをクリックし、[変更] をクリックします。
   名前、登録番号、ユーザーコードから検索できます。
4. ユーザーのアクセス権を変更し、[OK] をクリックします。
5. [戻る] をクリックします。
6. 管理者モードからログアウトします。
7. Web Image Monitor を終了します。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」

アドレス帳を暗号化する

ユーザー管理者が設定します。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。
アドレス帳のデータを暗号化します。この設定により、アドレス帳データの読み取りを防止できます。

1. [メニュー] キーを押します。
2. [▲] [▼] キーを押して [セキュリティー管理] を選択し、[OK] キーを押します。

3 ［▲］［▼］キーを押して［セキュリティー強化］を選択し、［OK］キーを押します。

4 ［▲］［▼］キーを押して［アドレス帳暗号化］を選択し、［OK］キーを押します。

5 ［▲］［▼］キーを押して［する］を選択し、［暗号鍵］を押します。

6 ［入力］を押します。

7 スクロールキーと［OK］キーで暗号鍵を入力し、［入力終了］キーを押します。
暗号鍵は、半角英数字 32 文字以内で入力してください。

8 確認画面が表示されたら、［入力］を押します。

9 暗号鍵を再入力し、［OK］キーを押します。

10 メッセージを確認し、［実行する］を押します。
アドレス帳の暗号化の処理時間は、ユーザー数の登録件数によって処理時間が異なります。また、処理実行中は、本機を使用できません。
暗号化 / 復号化中に電源スイッチを「Off」にしないでください。実行中に電源スイッチを「Off」にすると、データがこわれる可能性があります。
暗号化中に［中止］を押した場合は、データは暗号化されません。
復号化中に［中止］を押した場合は、データは暗号化されたままです。

11 メッセージを確認し、［確認］を押します。

12 ［メニュー］キーを押します。

補足

・アドレス帳の暗号化を行ったあとに追加したユーザーも暗号化されます。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」

蓄積データを暗号化する

この機能を使用するためには、オプションの蓄積文書暗号化カードが必要です。
本機に蓄積されるアドレス帳データ、認証情報、蓄積文書などをデータの記録時に暗号化して、情報の漏洩を防止します。
機器の故障時、機器の入れ替え時などに既存のデータを引き継ぐ場合、データが暗号化されていても新しい機器に引き継ぐことができます。データの引継ぎはサービス実施店に依頼してください。
暗号化されたデータの復元には、データ暗号化設定時に生成される暗号鍵を使用します。暗号鍵は途中で変更することも可能です。

♦ 暗号化の対象となるデータ

電源を切ってもデータを保持する本体搭載メモリー、またはハードディスクに蓄積される以下のデータが暗号化されます。

- アドレス帳
- ユーザー認証データ
- 一時保存されている文書データ
- ログ
- ネットワーク I/F 設定情報
- 機器設定情報

SD カードを取り付ける

蓄積文書暗号化カードの取り付け方法の説明です。

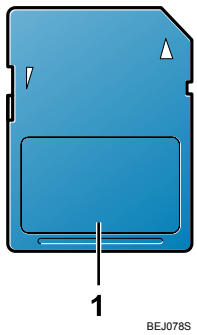
⚠注意

・SD カードは、子供の手に触れないようにしてください。もし子供が誤って SD カードを飲み込んだ場合は、直ちに医師の診断を受けてください。

重要

・お使いの機種によって取り付ける位置が異なります。よくご確認の上作業を行ってください。
・SD カードに、物理的衝撃を与えないでください。

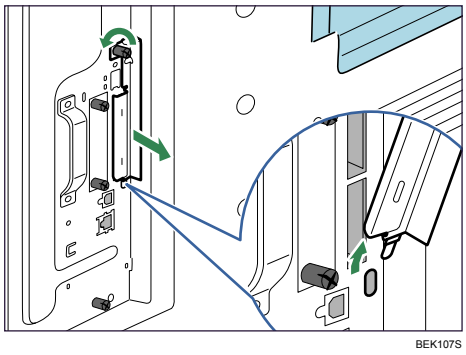
1 同梱品を確認します。



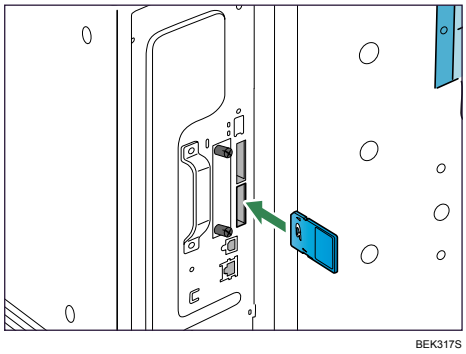
1. SD カード

2 本体の電源を切り、電源プラグをコンセントから抜きます。

3 コインねじを外し、拡張カード用のスロットカバーを傾けながら取り外します。

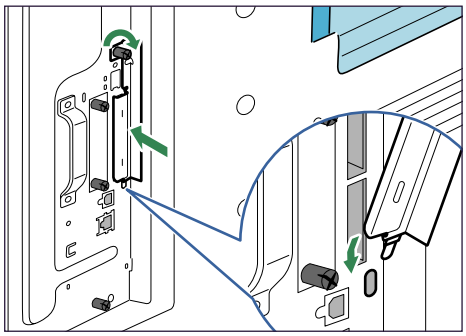


4 カチッと音がするまで、拡張カードをスロットに差し込みます。



スロット 2 に蓄積文書暗号化カードを差し込みます。

5 スロットカバーをスロット下部の穴に差し込み、スロットカバーを取り付けます。コインねじを締めて固定します。



BEK150S

補足

- 本体を使用中は、装着したカードに触れないでください。少し押しただけで外れてしまうことがあります。必ずスロットカバーを取り付けてください。
- 装着した SD カードが正しく取り付けられたかどうかは、操作部に表示されるメニューを確認します。装着した SD カードによって、操作部に表示されるメニューが異なります。
  - 蓄積文書暗号化カード：［セキュリティー管理］に ［機器データ暗号化設定］が表示されます。
- 正しく取り付けられない場合は、最初の手順からやり直してください。それでも正しく取り付けられない場合は、サービス実施店に相談してください。
- 蓄積文書暗号化カードは、本体から抜いても設定は有効です。

暗号化設定を有効にする

機器管理者が設定します。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。

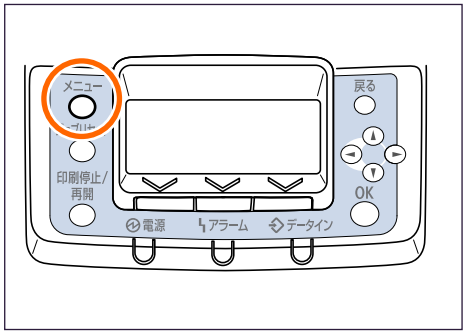
初回セットアップ時、また暗号化の設定を解除したあとに再度設定が必要になったときは、以下の手順で暗号化設定を有効にします。

重要

- 暗号鍵は、障害時のデータリカバリーなどに必要になります。出力されるバックアップ用データ暗号鍵は大切に保管してください。
- 暗号化の設定は、操作パネルでの設定手順を完了し、電源スイッチを一度「Off」/「On」して本機が再起動された後に有効になります。
- ハードディスクに引き継ぐデータがある場合は、再起動に約 2 時間かかります。
- ハードディスク上書き消去機能と暗号化機能を同時に設定していると、ハードディスク上書き消去機能が実行されたあと、電源スイッチを「Off」/「On」した段階で暗号化が開始されます。
- ハードディスク上書き消去機能と暗号化機能を同時に設定すると、ハードディスク上書き消去機能で乱数方式を選択し書き込み回数を 3 回に設定した場合、両機能が完了するまでに約 4 時間かかります。

・ハードディスクにデータを引き継がず、[初期化] を選択して暗号化を設定すると、再起動後の時間が短くなりますが、すべてのデータが初期化されます。また、再起動後に暗号化が実行されている途中で再度電源を切ったときにもすべてのデータが初期化されます。アドレス帳などの重要なデータは、暗号化の前にバックアップを取っておくことをお勧めします。

1 **[メニュー] キーを押します。**



BEJ008S

2 **[▲] [▼] キーを押して [セキュリティー管理] を選択し、[OK] を押します。**

3 **[▲] [▼] キーを押して [機器データ暗号化] を選択し、[OK] を押します。**

4 **画面に [暗号化] が表示されていることを確認し、[OK] を押します。**

5 **ハードディスクに引き継ぐための初期化しないデータを選択します。**
すべてのデータをハードディスクに引き継ぐときは [全て引継]、機器の設定データのみをハードディスクに引き継ぐときは [ファイルシステム] を選択します。すべてのデータを初期化する場合は [初期化] を選択します。

6 **[印刷] キーを押します。**
バックアップ用機器データ暗号鍵が印刷されます。

7 **[実行] を押します。**

8 **[確認] を押します。**

9 **[メニュー] キーを押します。**
通常の画面に戻ります。
本体の電源をいったん切って、再度電源を入れなおしてください。
詳細は、『かんたんセットアップ』「電源を入れる」を参照してください。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」

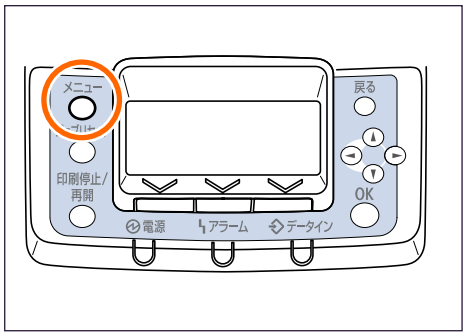
暗号鍵を印刷する

機器管理者が操作します。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。
暗号鍵を再印刷するときは、以下の手順で印刷します。

重要

・暗号鍵は、障害時のデータリカバリーなどに必要になります。出力されるバックアップ用データ暗号鍵は大切に保管してください。

1 [メニュー] キーを押します。



BEJ008S

2 [▲] [▼] キーを押して [セキュリティー管理] を選択し、[OK] を押します。

3 [▲] [▼] キーを押して [機器データ暗号化設定] を選択し、[OK] を押します。

4 [機器データ暗号鍵印刷] を選択し、[OK] を押します。

5 [印刷] キーを押します。
バックアップ用機器データ暗号鍵が印刷されます。

6 [メニュー] キーを押します。
通常の画面に戻ります。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」

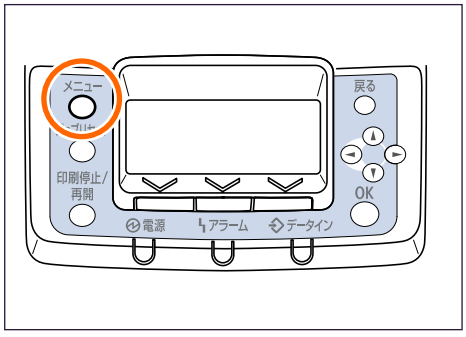
暗号鍵を更新する

機器管理者が操作します。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。
暗号鍵を別のものに変更することができます。機器が正常に動作している状態のときに変更可能です。

重要

- 暗号鍵は、障害時のデータリカバリーなどに必要になります。出力されるバックアップ用データ暗号鍵は大切に保管してください。
- 暗号鍵の更新を行うと、新しい暗号鍵を使用して暗号化を行います。新しい暗号鍵を使用した暗号化設定は、操作パネルでの設定手順を完了し、電源スイッチを一度「Off」/「On」して本機が再起動された後に有効になります。ハードディスクに引き継ぐデータがある場合は、再起動に時間がかかります。

1 [メニュー] キーを押します。



BEJ008S

2 [▲] [▼] キーを押して [セキュリティー管理] を選択し、[OK] を押します。

3 [▲] [▼] キーを押して [機器データ暗号化設定] を選択し、[OK] を押します。

4 [機器データ暗号鍵更新] を選択し、[OK] を押します。

5 ハードディスクに引き継ぐための初期化しないデータを選択します。
すべてのデータをハードディスクに引き継ぐときは [全て引継]、機器の設定データのみをハードディスクに引き継ぐときは [ファイルシステム] を選択します。すべてのデータを初期化する場合は [初期化] を選択します。

6 [印刷] キーを押します。
バックアップ用機器データ暗号鍵が印刷されます。

7 [実行] を押します。

8 [確認] を押します。

9 [メニュー] キーを押します。

通常の画面に戻ります。
本体の電源をいったん切って、再度電源を入れなおしてください。
詳細は、『かんたんセットアップ』「電源を入れる」を参照してください。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」

3

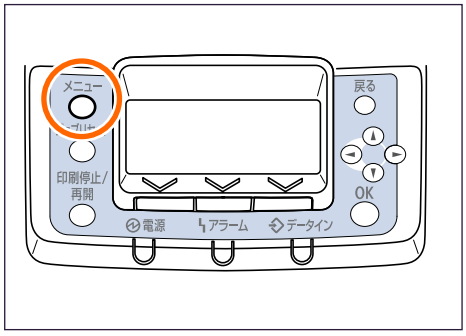
暗号化を解除する

機器管理者が操作します。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。
データの暗号化が不要になったとき、暗号化の設定を解除することができます。

重要

・暗号化の解除は、操作パネルでの設定手順を完了し、電源スイッチを一度「Off」/「On」して本機が再起動された後に有効になります。ハードディスクに引き継ぐデータがある場合は、再起動に時間がかかります。
・暗号化解除の設定で［初期化］を選択しても、データはハードディスクから消去されないため、廃棄のときなどに注意してください。

1 [メニュー] キーを押します。



BEJ008S

2 [▲] [▼] キーを押して [セキュリティー管理] を選択し、[OK] を押します。

3 [▲] [▼] キーを押して［機器データ暗号化設定］を選択し、[OK] を押します。

4 [暗号化解除] 選択し、[OK] を押します。

5 ハードディスクに引き継ぐための初期化しないデータを選択します。

すべてのデータをハードディスクに引き継ぐときは［全て引継］、機器の設定データのみをハードディスクに引き継ぐときは［ファイルシステム］を選択します。すべてのデータを初期化する場合は［初期化］を選択します。

6 **［実行］を押します。**

7 **［確認］を押します。**

8 **［メニュー］キーを押します。**

通常の画面に戻ります。
本体の電源をいったん切って、再度電源を入れなおしてください。
詳細は、『かんたんセットアップ』「電源を入れる」を参照してください。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」

ハードディスクのデータを上書き消去する

この機能を使用するためには、オプションのセキュリティーカードが必要です。
本機に拡張 HDD を取り付けた場合、搭載されたハードディスクには、蓄積された文書やアドレス帳、ユーザーコード別カウンターを記録します。
一時的に保存されたジョブのデータを自動で上書き消去（メモリー自動消去）したり、本機を廃棄するときに、ハードディスクに蓄積されているすべてのデータを上書き消去（メモリー全消去）することで、データ漏洩を防止することができます。

SD カードを取り付ける

セキュリティーカードの取り付け方法の説明です。

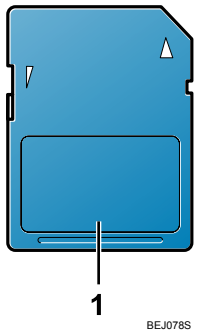
⚠注意

・SD カードは、子供の手に触れないようにしてください。もし子供が誤って SD カードを飲み込んだ場合は、直ちに医師の診断を受けてください。

重要

・SD カードに物理的衝撃を与えないでください。

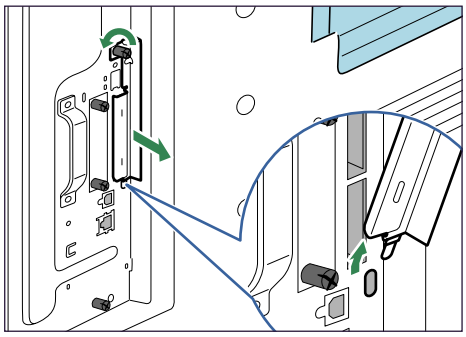
1 同梱品を確認します。



1. SD カード

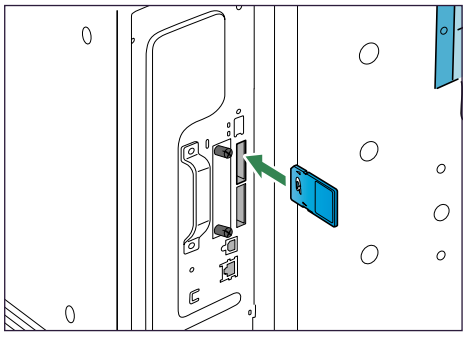
2 本体の電源を切り、電源プラグをコンセントから抜きます。

3 コインねじを外し、拡張カード用のスロットカバーを傾けながら取り外します。



BEK107S

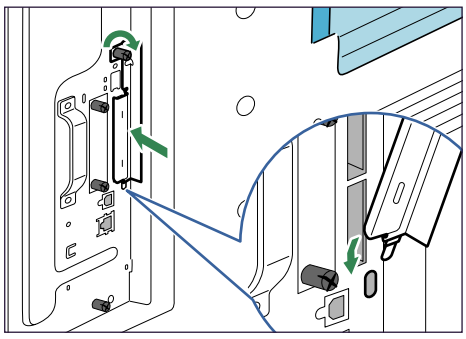
4 カチッと音がするまで、拡張カードをスロットに差し込みます。



BEK316S

スロット 1 にセキュリティーカードを差し込みます。

5 スロットカバーをスロット下部の穴に差し込み、スロットカバーを取り付けます。コインねじを締めて固定します。



BEK150S

補足

・本体を使用中は、装着したカードに触れないでください。少し押しただけで外れてしまうことがあります。必ずスロットカバーを取り付けてください。
・装着した SD カードが正しく取り付けられたかどうかは、操作部に表示されるメニューを確認します。装着した SD カードによって、操作部に表示されるメニューが異なります。
  ・セキュリティーカード : 最初の階層に、［メモリー内残存データ状態確認］が表示されます。
・正しく取り付けられない場合は、最初の手順からやり直してください。それでも正しく取り付けられない場合は、サービス実施店に相談してください。

メモリー自動消去設定

本機に拡張 HDD を取り付けた場合、PC から本機に出力されたデータは、ハードディスクに一時的に保存されます。メモリー自動消去設定を使用すると、ハードディスク内に残っているデータを自動的に上書き消去することができます。
上書き消去は、ジョブごとに自動的に行われます。
印刷動作が優先され、上書き処理はこれらのジョブが終わったあとに開始されます。

消去方式

消去方式は次の中から選択できます。

♦ **NSA [*1] 方式**
データを乱数 2 回、ゼロ 1 回で上書きします。

♦ **DoD [*2] 方式**
データを固定値、固定値の補数、乱数で上書きし、検証処理を行います。

♦ **乱数方式**
データを指定された回数の乱数で上書きします。乱数の書き込み回数は 1 ～ 9 回まで選択でき、工場出荷時は 3 回に設定されています。

[*1] National Security Agency（米）国家安全保障局
[*2] Department of Defense（米）国防総省

補足

・工場出荷時は「乱数」に設定されています。

メモリー自動消去設定を使用する

機器管理者が設定します。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。

重要

・セキュリティーカード導入前やメモリー自動消去設定を「しない」に設定されていたときのハードディスク使用領域は、メモリー自動消去設定を「する」に設定後も残存データが上書きされないことがあります。
・ハードディスク上書き消去機能と、ハードディスクに蓄積された文書を暗号化する機能を同時に設定すると、ハードディスク上書き消去機能で乱数方式を選択し書き込み回数を 3 回に設定した場合、両機能が完了するまでに約 4 時間かかります。

1 **[メニュー] キーを押します。**

2 **[▲] [▼] キーを押して [セキュリティー管理] を選択し、[OK] キーを押します。**

3 **[▲] [▼] キーを押して [メモリー自動消去設定] を選択し、[OK] キーを押します。**

4 **[▲] [▼] キーを押して、[する] を選択し、[消去方式] を押します。**
消去方式は、[NSA 方式]、[DoD 方式]、[乱数方式] のいずれかを選択します。
「NSA 方式」を選択した場合は、手順 **7** へ進んでください。
「DoD 方式」を選択した場合は手順 **8** へ進んでください。
[乱数方式] を設定する場合は手順 **5** へ進んでください。

5 **[▲] [▼] キーを押して [乱数方式] を選択し、[OK] キーを押します。**

6 **1~9 の間で [▲] [▼] キーを押して書き込みの回数を入力し、[OK] キーを押します。**
メモリー自動消去が設定されます。

7 **「NSA 方式」を選択し、[OK] キーを押します。**
メモリー自動消去が設定されます。

8 **「DoD 方式」を選択し、[OK] キーを押します。**
メモリー自動消去が設定されます。

補足

・メモリー自動消去が完了する前に本機の電源スイッチを「Off」にすると、上書き消去は一時中断され、データはハードディスク内に残ったままとなります。途中で中止することはできません。また、ハードディスクが壊れることがありますので、上書き処理中に本機の電源を切られないように必ず確認してください。
・万一、メモリー自動消去が完了する前に本機の電源スイッチを「Off」にした場合は、本機の電源スイッチを再び「On」にしたときに、メモリー自動消去を続きから行います。

・上書き消去中にエラーが発生したときは、本機の電源スイッチを一度「Off」にしてください。再び本機の電源スイッチを「On」にし、手順をやり直してください。
・ハードディスク上書き消去機能と、ハードディスクに蓄積された文書を暗号化する機能を組み合わせて設定した場合、上書き消去機能によるハードディスクへの書き込みも暗号化されます。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」

3

メモリー自動消去設定を使用しない

機器管理者が設定します。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。

1 **「メモリー自動消去設定を使用する」の手順 1 ～ 3 と同様に操作します。**

2 **［▲］［▼］キーを押して［しない］を選択し、［OK］キーを押します。**
上書き消去は行われません。

補足

・メモリー自動消去設定を再度実行するときは、「メモリー自動消去設定を使用する」の手順をやり直してください。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」

上書き消去できるデータ／できないデータ

上書き消去できるデータと、上書き消去できないデータは以下のとおりです。

上書き消去できるデータ	・印刷のデータ ・機密印刷 / 試し印刷 / 保留印刷 / 保存文書（プリンターに保存）のデータ *1 ・スプール印刷のデータ ・RTIFF エミュレーションの印刷データ ・RPGL/2 エミュレーションの印刷データ ・PDF ダイレクトプリントのデータ
上書き消去できないデータ	アドレス帳に登録されているデータ *2
	ユーザーコード別カウンター
	イメージオーバーレイデータ *3

*1 機密印刷 / 試し印刷 / 保留印刷のデータは、出力されてはじめて上書き消去の対象となります。保存文書は削除しない限り上書き消去はできません。
*2 アドレス帳に登録されているデータの不正利用を防ぐために暗号化することができます。詳しくは「アドレス帳を暗号化する」を参照してください。
*3 イメージオーバーレイデータは削除されてはじめて上書き消去の対象となります。

参照

・P.66 「アドレス帳を暗号化する」

メモリー全消去

本機を移設または廃棄するときに、ハードディスクに蓄積されているすべてのデータを一括上書き消去することができます。

重要

・ユーザーコード、ユーザーコード別カウンター、アドレス帳、ユーザースタンプ、ユーザーがダウンロードしたプリンターフォント、Embedded Software Architecture を用いたアプリケーション、SSL 機器証明書、および本機のネットワーク設定もメモリー全消去の対象となっています。メモリー全消去後に使用する場合はサービス実施店に相談してください。
・メモリー全消去が完了する前に本機の電源スイッチを「Off」にすると、上書き消去は一時中断され、データはハードディスク内に残ったままとなります。途中で中止することはできません。また、ハードディスクが壊れることがありますので、上書き処理中に本機の電源を切られないように必ず確認してください。
・メモリー全消去を行う前に、Ridoc IO Admin を利用して、ユーザーコード、ユーザーコード別カウンター、アドレス帳のデータをバックアップすることをお勧めします。詳細については Ridoc IO Admin のヘルプを参照してください。
・メモリー全消去の実行時は本機の操作はできません。メモリー全消去の一時停止の操作のみできます。乱数方式を選択して書き込み回数を 3 回に設定した場合、約 2 時間かかります。

メモリー全消去を使用する

機器管理者が操作します。管理者認証のログイン、ログアウトの方法については、「操作部での管理者認証でのログインのしかた」「操作部での管理者認証でのログアウトのしかた」を参照してください。

1 **本機に接続されている、電源ケーブル以外のケーブルを取り外します。**

2 **[メニュー] キーを押します。**

3 **[▲] [▼] キーを押して [セキュリティー管理] を選択し、[OK] キーを押します。**

4 **[▲] [▼] キーを押して [メモリー全消去] を選択し [OK] キーを押します。**

5 **消去方式を選択します。**

消去方式は、[NSA 方式]、[DoD 方式]、[乱数方式] のいずれかを選択します。
[NSA 方式] を設定する場合は、手順 **8** へ進んでください。
「DoD 方式」を設定する場合は手順 **9** へ進んでください。
[乱数方式] を設定する場合は手順 **6** へ進んでください。

6 **[▲][▼]キーを押して「乱数方式」を選択し、[OK]キーを押します。**

7 **1~9 の間で[▲][▼]キーを押して書き込みの回数を入力し、[OK]キーを押します。**

8 **[▲][▼]キーを押して「NSA 方式」を選択し、[OK]キーを押します。**

9 **「DoD 方式」を選択し[OK]キーを押します。**

10 **[消去する]を押します。**
本機が自動的に再起動し、メモリー全消去を開始します。

11 **メモリー全消去が完了したら[確認]を押して電源を切ります。**

補足

・万一、メモリー全消去が完了する前に本機の電源スイッチを「Off」にした場合は、本機の電源スイッチを再び「On」にしたときに、メモリー全消去を続きから行います。
・メモリー全消去中にエラーが発生したときは、本機の電源スイッチを一度「Off」にしてください。再び本機の電源スイッチを「On」にし、手順 **2** から行ってください。
・メモリー全消去中は、メモリー全消去の一時停止以外の操作はできません。メモリー全消去機能で乱数方式を選択し書き込み回数を 3 回に設定した場合、完了するまでに約 2 時間かかります。
・ハードディスク上書き消去機能と、ハードディスクに蓄積された文書を暗号化する機能を組み合わせて設定した場合、上書き消去機能によるハードディスクへの書き込みも暗号化されます。

参照

・P.27 「操作部での管理者認証でのログインのしかた」
・P.28 「操作部での管理者認証でのログアウトのしかた」
・P.78 「消去方式」

メモリー全消去を一時停止する

重要

・メモリー全消去は中止できません。

1 **メモリー全消去処理中に[一時停止]を押します。**

2 **[一時停止する]を押します。**
メモリー全消去は一時停止されます。

3 **本機の電源を切ります。**

補足

・本機の電源スイッチを再び「On」にするとメモリー全消去が再開されます。