データ暗号化／上書き消去
使用説明書

KYOCERA
Document Solutions

はじめに

この説明書ではデータ暗号化／上書き消去機能（以下セキュリティー機能）を正しく導入・運用するための手順とシステムの初期化手順を説明しています。

組織の責任者は、本書を読んで内容を理解していただくことを想定しています。

- セキュリティー機能の導入に際して、本機の管理者には、信頼のできる人物を選出してください。
- 選出した管理者に対しては、所属する組織のセキュリティー方針や運用ルールを遵守し、また製品の使用説明書の記載に従って適切な操作ができるよう、十分な指導を行ってください。
- 一般ユーザーに対しては、所属する組織のセキュリティー方針や運用ルールを遵守して適切な操作が行えるよう、十分な指導を行ってください。

■一般ユーザー編：一般ユーザーおよび管理者の両方がお読みください。

■管理者編：セキュリティー機能の導入・運用を担当する管理者がお読みください。

一般ユーザー編 一般ユーザーおよび管理者の両方がお読みください

セキュリティー機能

セキュリティー機能には、上書き消去機能と暗号化機能があります。

参考：セキュリティー機能を導入すると、本機起動時に「セキュリティー機能を実行中です。」と表示され、起動に時間がかかることがあります。

上書き消去機能

複合機は、読み込んだ原稿やプリントジョブを一時的にハードディスク /SSD や FAX メモリーにデータとして保存し、そのデータから出力します。また、さまざまなデータをユーザーが登録しておくこともできます。それらのデータにおける実際のデータ領域は、出力後やユーザーが削除した後も、他のデータにより上書きされるまでハードディスク /SSD や FAX メモリーに残存するため、特殊なツールなどで復元すると機密漏えいの原因となる可能性があります。

セキュリティー機能は、出力後のデータや削除したデータの、不要なデータ保存領域を上書きして消去し（以降、上書き消去）、復元できないようにします。

上書き消去は自動的に行われるため、特別な操作は必要ありません。

参考：各作業を途中でキャンセルすると、その直後から、ハードディスク /SSD 内および FAX メモリー内に読み込まれたデータの上書き消去が開始されます。

上書き消去の方式について

上書き消去方式の変更は、ハードディスクを装着している場合に設定できます。上書き消去には、次の 2 種類の方式があります。変更はいつでも可能です。

◆ 1 回上書き方式

不要なデータ保存領域（上書き消去の場合）またはすべての領域（システムの初期化の場合）に「0」を上書きし、データの復元を不可能にします。

◆ 3 回上書き方式（DoD）（初期値）

米国国防総省（DoD）の規格に準拠した上書き方法で、ハードディスクや FAX メモリーの不要なデータ保存領域（上書き消去の場合）またはすべての領域（システムの初期化の場合）に、特定の文字、その補数、ランダムな文字の書き込みなどを行いデータの復元を不可能にします。高度な復元作業でもデータの復元が不可能になり、1 回上書き方式に比べセキュリティーが強化されます。

多くのデータ量を上書き消去する場合、3 回上書き方式（DoD）は 1 回上書き方式に比べ所要時間が増加することがあります。

参考：SSD および FAX メモリーについては 1 回上書き方式になります。

暗号化機能

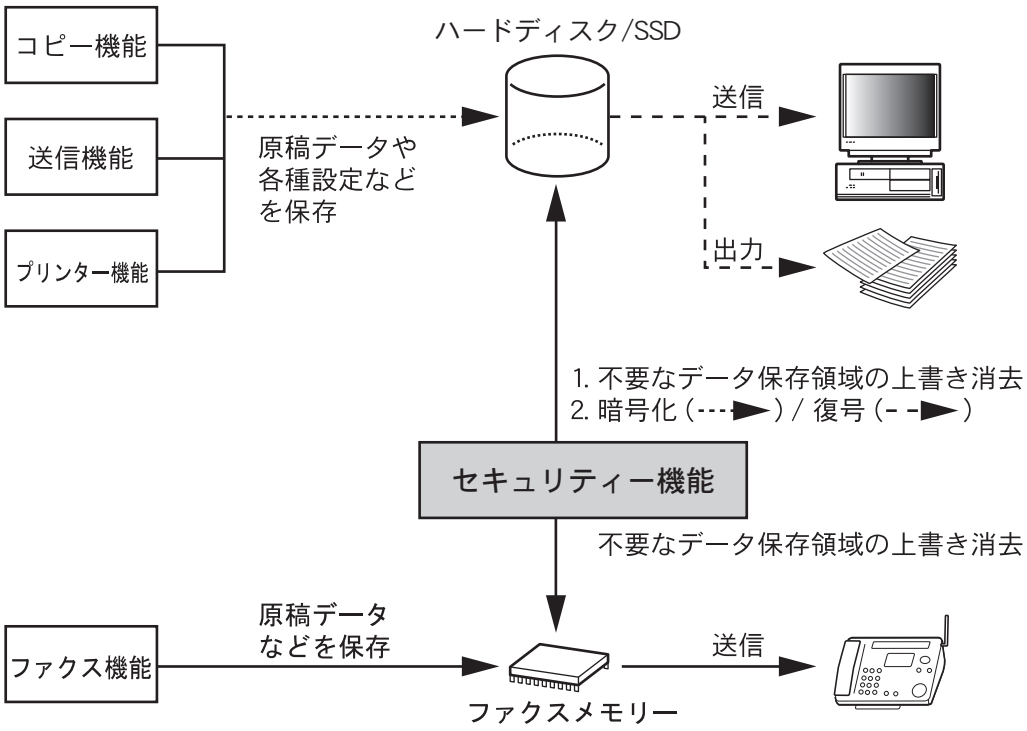
複合機は、読み込んだ原稿データやユーザーが登録したデータをハードディスク /SSD に保存します。このため、万一ハードディスク /SSD が盗難に遭うと、データの流出や改ざんのおそれがあります。

セキュリティー機能は、データをハードディスク /SSD に保存するとき、暗号化して書き込みます。通常の出力や操作以外では復号（解読）できないため、万一の場合のセキュリティーが強化されます。

暗号化は自動的に行われるため、特別な操作の必要はありません。

注意：暗号化によりセキュリティーは強化されますが、文書ボックスへ保存したデータは、通常の出力操作で復号されます。絶対に漏洩させたくないデータは、文書ボックスに保存しないでください。

セキュリティー機能



- 本機にハードディスクを装着している場合、セキュリティー機能を導入すると、ファクス受信データの保存先は、SSD からハードディスクに変更されます。保存先を SSD に設定したい場合は、サービス担当者に問い合わせしてください。

セキュリティー機能導入後のタッチパネルの表示

アイコンの表示

セキュリティー機能が導入され、正しく機能している状態を「セキュリティーモード」といいます。セキュリティーモード時は、タッチパネル右下にアイコンが表示されます。

注意：通常の画面にアイコンが表示されない場合は、セキュリティーモードになっていない可能性があります。サービス担当者にお問い合わせください。

上書き消去中のアイコンの形状変化

表示されているアイコンとその内容は次のとおりです。

アイコン表示	内容
	ハードディスク /SSD や FAX メモリーに不要になったデータがある。
	不要になったデータを上書き消去中。
	不要になったデータの上書き消去完了。

注意：アイコン  が表示時は電源スイッチを切らないでください。ハードディスク /SSD や FAX メモリーが破損するおそれがあります。

参考：上書き消去中に電源スイッチを切ると、消去されなかったデータが残ります。電源スイッチを入れ直してください。自動的に上書き消去が再開します。

上書き消去 / 初期化中に電源スイッチを切ってしまった場合、まれにハードディスクアイコンが変わらないときがあります。これは、消去中のデータが破損し、上書き消去できなくなるためです。その後に発生する不要になったデータは上書き消去されますが、正常な状態に戻すには、システムの初期化を行ってください（13 ページの**システムの初期化**を参照して、管理者が行ってください）。

管理者編　　セキュリティー機能の導入・運用を担当する管理者がお読みください

セキュリティー機能の導入、運用に際して、なにか問題があった場合は、お買い上げの販売店または弊社のサービス担当者にご連絡ください。

セキュリティー機能の導入

導入前の注意

- メンテナンスを行うサービス担当者が、機械供給先のサービス担当者であることを確認してください。
- 本機は人の出入りが管理されている安全な場所に設置し、機械への不正アクセスを防止できるようにしてください。
- 導入中にシステムが初期化されるため、ハードディスク /SSD に保存されているデータはすべて削除されます。使用中の複合機にセキュリティー機能を導入する場合は特にご注意ください。
- 機械を接続するネットワークは、ファイアウォールなどの外部ネットワークから守られた環境で使用してください。
- 再コピー機能は使用できなくなります。
- システムメニューの［**調整 / メンテナンス**］→［**システムの初期化**］が非表示になります。
- セキュリティー機能の導入に際し、本機の設定を次のように変更してください。

設定項目			**設定値**
ユーザー / 部門管理	ユーザー管理設定	ローカルユーザーリスト	管理者のパスワードを変更する
システムメニュー	日付 / タイマー / 節電	日付 / 時刻	日付／時刻を設定する

- 本機にハードディスクを装着している場合、セキュリティー機能を導入すると、ファクス受信データの保存先は、SSD からハードディスクに変更されます。保存先を SSD に設定したい場合は、サービス担当者に問い合わせしてください。

導入中の作業

セキュリティー機能の導入は、サービス担当者または管理者が行います。

サービス担当者または管理者はシステムメニューにログイン後、暗号化コードを入力します。

暗号化コードについて

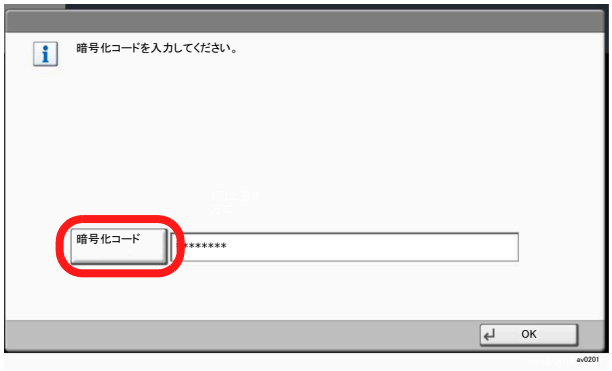
暗号化コードは、データの暗号化に必要なコードで、8 桁の英数字（0 ～ 9、A ～ Z、a ～ z）を入力します。工場出荷時は 00000000 となっています。

実際にはこの暗号化コードを元に暗号鍵が作成されるため、工場出荷時の値のまま運用しても、セキュリティー上問題はありません。

注意：入力した暗号化コードは、安全に管理し、絶対に忘れないでください。何らかの理由で再度、暗号化コードの入力が必要になった場合、同じ暗号化コードを入力しないとハードディスク /SSD に保存されていたデータは、セキュリティー上安全のためにすべて削除されます。

導入手順

操作手順は次のとおりです。



1 [システムメニュー / カウンター] キーを押してください。

2 [システム / ネットワーク] を押してください。

ユーザー管理が無効の場合、ユーザー認証画面が表示されます。ログインユーザー名とログインパスワードを入力し、[ログイン] を押してください。

ここでは管理者の権限でログインしてください。ログインユーザー名とログインパスワードの工場出荷時の値については、本体の使用説明書を参照してください。

3 「オプション機能」の [次へ] を押してください。

4 オプション機能画面が表示されます。「データ暗号化 / 上書き消去」を選択し、[起動] を押してください。

5 この機能を起動します。大容量記憶装置は、データが消去され、暗号化フォーマットが実施されます。問題がなければ、[はい] を押してください。

6 画面の指示にしたがって、電源スイッチを入れ直してください。

7 暗号化コードを入力する画面が表示されます。暗号化コードを変更する場合は、以下の手順で変更してください。暗号化キーを変更しない場合は、手順１０に進みます。

8 [暗号化コード] を押します。

9 [バックスペース] を押して、「00000000」を消してから、暗号化コード 8 桁の英数字（0 ～ 9、A ～ Z、a ～ z）を入力して、[OK] を押します。

10 [OK] を押します。ハードディスク /SSD のフォーマットが開始されます。

11 フォーマットが終了したら、画面の指示にしたがって、電源スイッチを入れ直してください。

12 オープニング画面が表示されたあと、ホーム画面右下にアイコン（ハードディスクの不要になったデータの上書き消去完了アイコン）が表示されているか確認してください。

導入後の作業

本機をよりセキュアにご使用いただくために、本機の設定を次のように変更してください。本機でシステムの初期化を行った場合、導入前の設定に戻りますので、同様に変更してください。メンテナンス作業を行った場合も設定値を確認してください。

Command Center RX で変更する項目

<table>
<tr><th colspan="6">設定項目</th><th>設定値</th></tr>
<tr><td rowspan="2">デバイス設定</td><td rowspan="2">節電 / タイマー</td><td colspan="3" rowspan="2">節電 / タイマー設定</td><td rowspan="2">タイマー設定</td><td>オートパネルリセット</td><td>オン</td></tr>
<tr><td>パネルリセット時間</td><td>任意</td></tr>
<tr><td rowspan="5">機能設定</td><td rowspan="3">プリンター</td><td rowspan="3">プリンター設定</td><td colspan="2">基本</td><td>リモート印刷</td><td>禁止する</td></tr>
<tr><td rowspan="2">Google Cloud Print 設定
（「設定 / 登録」選択）</td><td rowspan="2">Privet（クラウドデバイスローカル検出のプロトコルと API）</td><td>ローカル検出</td><td>オフ</td></tr>
<tr><td>ローカル印刷</td><td>オフ</td></tr>
<tr><td>ファクス /i-ファクス</td><td>ファクス /i-ファクス設定</td><td>ファクス設定</td><td>リモート設定</td><td>ファクスリモート診断</td><td>オフ</td></tr>
<tr><td rowspan="3">条件付き受信 / 転送</td><td rowspan="3">設定 / 登録</td><td colspan="2" rowspan="2">条件付き受信 / 転送設定</td><td>条件付き受信 / 転送</td><td>「すべての受信に適用する」または「特定の受信に適用する」</td></tr>
<tr><td rowspan="2">転送設定</td><td>転送</td><td>オン</td></tr>
<tr><td>転送先</td><td>任意の転送先</td></tr>
</table>

設定項目						設定値
ネットワーク設定	TCP/IP	TCP/IP 設定		Bonjour 設定	Bonjour	オフ
				IPsec 設定	IPsec	オン
					制限	許可
		IPsec ルール * (任意のルール№.の「設定 / 登録」選択) ルール№. : 1 ～ 10	ポリシー		ルール	オン
					鍵管理方式	IKEv1
					カプセル化モード	トランスポート
			IP アドレス		IP バージョン	IPv4
					IP アドレス	送信先端末の IP アドレス
					サブネットマスク	任意
			認証	ローカル側	認証方式	事前共有キー
					事前共有キー	任意
			鍵交換 (IKE phase1)			任意（ただし、モードは Main Mode を選択）
			データ保護 (IKE phase2)			任意（ただし、プロトコルは ESP を選択）
	プロトコル	プロトコル設定		印刷プロトコル	NetBEUI	オフ
					LPD	オフ
					FTP（受信）	オフ
					IPP	オフ
					IPP over SSL	オン
					IPP 認証	オフ
					RAW	オフ
					WSD 印刷	オフ
					POP3（メール受信）	オフ
				送信プロトコル	SMTP（メール送信）	オン
					FTP クライアント（送信）	オン
					SMB	オフ
					WSD スキャン	オフ
					DSM スキャン	オフ
					eSCL	オフ
					eSCL over SSL	オフ
				その他プロトコル	SNMPv1/v2c	オフ
					SNMPv3	オフ
					HTTP	オフ
					HTTPS	オン
					Enhanced WSD	オフ
					Enhanced WSD (SSL)	オン
					LDAP	オフ
					IEEE802.1X	オフ
					LLTD	オフ
					REST	オフ
					REST over SSL	オフ
					VNC(RFB)	オフ
					VNC(RFB) over SSL	オフ
					Enhanced VNC(RFB) over SSL	オフ

設定項目						設定値
セキュリティー設定	デバイスセキュリティー	デバイスセキュリティー設定	編集権限		アドレス帳	管理者のみ許可
					ワンタッチキー	管理者のみ許可
			認証セキュリティー設定	パスワードポリシー設定	パスワードポリシー	オン
					パスワードの有効期間	任意
					パスワードの長さ	オン　8 文字以上
					パスワードの複雑さ	任意
				ユーザーアカウントロックアウト設定	ロックアウトポリシー	オン
					ロックまでの回数	任意
					ロックアウト期間	任意
					ロックアウト対象	すべて
	ネットワークセキュリティー	ネットワークセキュリティー設定	セキュアプロトコル設定	SSL		オン
				サーバー機能時の設定	TLS バージョン	SSL3.0/TLS1.0：無効 TLS1.1：無効、TLS1.2：有効
					有効な暗号方式	ARCFOUR：無効、DES：無効、3DES：有効、AES：有効、AES-GCM：任意
					HTTP セキュリティー	セキュア（HTTPS）
					IPP セキュリティー	セキュア（IPPS）
					Enhanced WSD セキュリティー	セキュア（Enhanced WSD over SSL）
				クライアント機能時の設定	TLS バージョン	SSL3.0/TLS1.0：無効 TLS1.1：無効、TLS1.2：有効
					有効な暗号方式	ARCFOUR：無効、DES：無効、3DES：有効、AES：有効、AES-GCM：任意
					証明書チェック	オン

設定項目						設定値
管理設定	認証	設定 / 登録	認証設定	基本	認証	ローカル認証
				ローカル認可設定	ローカル認可	オン
				ゲスト認可設定	ゲスト認可	オフ
				簡単ログイン設定	簡単ログイン	オフ
	履歴設定	履歴設定		ジョブ履歴	受取人アドレス	本機の管理者のアドレス
					自動送信	オン
				ログイン履歴設定	ログイン履歴	オン
					受取人アドレス	本機の管理者のアドレス
					自動送信	オン
				デバイス履歴設定	デバイス履歴	オン
					受取人アドレス	本機の管理者のアドレス
					自動送信	オン
				セキュリティー通信エラー履歴設定	セキュリティー通信エラー履歴	オン
					受取人アドレス	本機の管理者のアドレス
					自動送信	オン

本機で変更する項目

設定項目			設定値
システムメニュー	システム / ネットワーク	セキュリティーレベル	最高
	インターネット	インターネットブラウザー	使用しない

各設定の変更方法については本機の**使用説明書**および Command Center RX **操作手順書**を参照してください。
設定を変更後、本機が正しく動作することを確認するために、システムメニューの［**ソフトウェア検証**］を行ってください。［**ソフトウェア検証**］は導入後も定期的に行ってください。
この他にセキュリティー機能導入後に行う作業には、セキュリティーパスワードの変更とハードディスク消去方式の変更があります。
作業方法は、11 ページを参照してください。
本機の管理者は定期的に各種履歴を保管するとともに、不正アクセスや異常な操作が行われていないかどうかを確認してください。
また、一般ユーザーの登録に際しては社内規定に応じた権限を付与するとともに、退職などで利用されなくなったユーザーアカウントはすみやかに削除してください。

IPsec 設定について

IPsec 機能を有効にすることで通信経路を暗号化し、データを保護することが出来ます。IPsec 設定を行う際には、以下の点に注意してください。

- IPsec ルールで設定する値は、送信先端末に合わせてください。設定が合っていない場合は通信エラーとなります。
- IPsec ルールで設定する IP アドレスは、本機に設定する SMTP サーバー、FTP サーバーの IP アドレスと一致させてください。
- 一致していない場合は、メール送信、FTP 送信で送信したデータが暗号化されません。
- IPsec ルールで設定する事前共有キーは、英数記号を使って、安易に推測されない 8 文字以上を使用してください。

セキュリティー機能の設定変更

セキュリティーパスワードの変更

セキュリティー機能の設定を変更するには、セキュリティーパスワードの入力が必要です。このセキュリティーパスワードを工場出荷時の値から変更して、管理者だけがセキュリティー機能を操作できるようにします。セキュリティーパスワードを変更する操作手順は、次のとおりです。

1 ［**システムメニュー / カウンター**］キーを押してください。

2 ［**システム / ネットワーク**］を押してください。

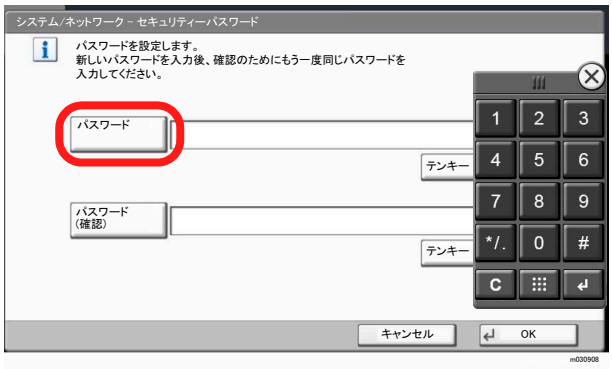
3 ユーザー管理が無効の場合、ユーザー認証画面が表示されます。ログインユーザー名とログインパスワードを入力し、［**ログイン**］を押してください。

ここでは管理者の権限でログインしてください。ログインユーザー名とログインパスワードの工場出荷時の値については、本体の**使用説明書**を参照してください。

4 「データセキュリティー」の［**次へ**］を押してください。

5 「SSD の初期化」の［**次へ**］を押してください。

参考：ハードディスクを装着している場合は、「ハードディスクの初期化」と表示されます。ハードディスクと SSD を装着している場合は、「ハードディスク /SSD の初期化」と表示されます。



6 現在のセキュリティーパスワードを入力してください工場出荷時は 000000 となっています。

7 「セキュリティーパスワード」の［**変更］を押してください。**

8 ［**パスワード**］を押して、新しいセキュリティーパスワードを 6 ～ 16 桁の英数字記号で入力してください。

9 ［**パスワード（確認）**］を押して、同じパスワードをもう一度入力してください。

10 ［OK］を押してください。

注意：セキュリティーパスワードは 11111111 や 12345678 など推測されやすい番号の使用はできるだけ避けてください。

データ上書き消去方法の変更

データの上書き消去方式を変更することができます。消去方式の詳細については、2 ページの**上書き消去機能**を参照してください。ハードディスクを装着していない場合は、消去方式の変更はできません。

参考：ここで設定した消去方式は、上書き消去機能とハードディスクの初期化の両方で用いられます。個別に設定することはできません。

操作手順は次のとおりです。

1 ［**システムメニュー / カウンター**］キーを押してください。

2 ［**システム / ネットワーク**］を押してください。

3 ユーザー管理が無効の場合、ユーザー認証画面が表示されます。ログインユーザー名とログインパスワードを入力し、［**ログイン**］を押してください。

ここでは管理者の権限でログインしてください。ログインユーザー名とログインパスワードの工場出荷時の値については、本体の**使用説明書**を参照してください。

4 「データセキュリティー」の［**次へ**］を押してください。

5 「ハードディスクの初期化」の［**次へ**］を押してください。

6 セキュリティーパスワードを入力してください。工場出荷時は 000000 となっています。

7 「データ上書き消去方法」の［**変更**］を押してください。

8 ［**3 回上書き方式**（DoD）］（初期値）または［**1 回上書き方式**］を押してください。

9 ［OK］を押してください。

システムの初期化

システムの内容を完全に消去することができます。本体の使用を中止するときなどに行ってください。

注意：初期化中に電源スイッチを切ると、ハードディスク /SSD が破損し、初期化が完了しなくなるおそれがあります。

参考：万一初期化中に電源スイッチを切ってしまった場合は、電源スイッチを入れ直してください。自動的に初期化が再開します。

システムの初期化の操作手順は、次のとおりです。

1 ［**システムメニュー / カウンター**］キーを押してください。

2 ［**システム / ネットワーク**］を押してください。

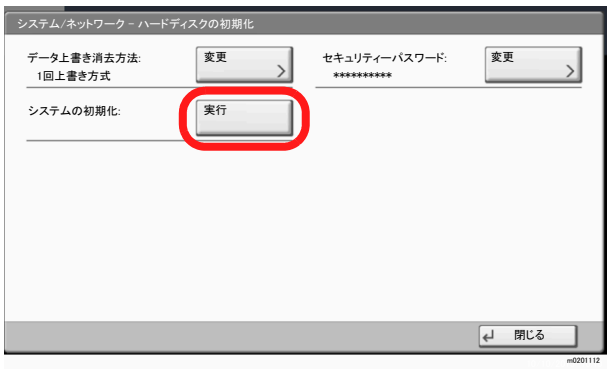
3 ユーザー認証画面が表示された場合は、ログインユーザー名とログインパスワードを入力して、［**ログイン**］を押してください。

ここでは管理者の権限でログインしてください。ユーザー認証画面が表示されない場合は、手順 4 に進んでください。

4 「データセキュリティー」の［**次へ**］を押してください。

5 「SSD の初期化」の［**次へ**］を押してください。

参考：ハードディスクを装着している場合は、「ハードディスクの初期化」と表示されます。ハードディスクと SSD を装着している場合は、「ハードディスク /SSD の初期化」と表示されます。



6 セキュリティーパスワードを入力してください。工場出荷時は 000000 となっています。

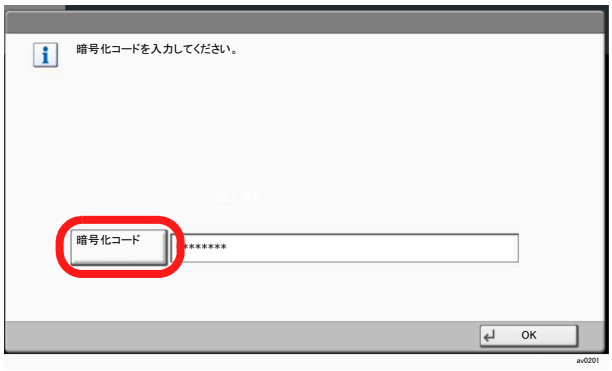
7 「システムの初期化」の［**実行**］を押してください。

8 初期化の確認画面が表示されます。［**はい**］を押してください。初期化が開始されます。

9 初期化完了の画面が表示されたら、電源スイッチを入れ直してください。

こんな表示が出たら

何らかの理由で本機の暗号化コード情報が失われると、電源を入れたときに次の画面が表示されます。



次の操作を行ってください。

1 ［**暗号化コード**］を押して、セキュリティー機能導入中に入力した暗号化コードを入力してください。

注意：以前と異なる暗号化コードを入力しても作業を強制的に続行することはできますが、ハードディスク/SSD に保存されていたデータはすべて削除されますのでご注意ください。

暗号化コードは、セキュリティーパスワードとは、異なります。

2 電源スイッチを入れ直してください。

使用済み製品の廃棄

使用済み製品を廃棄される場合は、システムの初期化を実施し、ハードディスク /SSD とファクスメモリーに保存されたデータを消去してください。

使用済み製品を廃棄される場合は、購入元または弊社のサービス担当者にご連絡ください。

付録

出荷時設定値一覧

セキュリティーモードに関する設定の初期値は次のとおりです。

Command Center RX で変更する項目

<table>
<tr><th colspan="6">設定項目</th><th>設定値</th></tr>
<tr><td rowspan="2">デバイス設定</td><td rowspan="2">節電 / タイマー</td><td colspan="2" rowspan="2">節電 / タイマー設定</td><td rowspan="2">タイマー設定</td><td>オートパネルリセット</td><td>オン</td></tr>
<tr><td>パネルリセット時間</td><td>120 秒</td></tr>
<tr><td rowspan="6">機能設定</td><td rowspan="3">プリンター</td><td rowspan="3">プリンター設定</td><td colspan="2">基本</td><td>リモート印刷</td><td>許可する</td></tr>
<tr><td rowspan="2">Google Cloud Print 設定
(「設定 / 登録」選択)</td><td rowspan="2">Privet（クラウドデバイスローカル検出のプロトコルと API)</td><td>ローカル検出</td><td>オン</td></tr>
<tr><td>ローカル印刷</td><td>オン</td></tr>
<tr><td>ファクス /i-ファクス</td><td>ファクス /i-ファクス設定</td><td>ファクス設定</td><td>リモート設定</td><td>ファクスリモート診断</td><td>オフ</td></tr>
<tr><td rowspan="3">条件付き受信 / 転送</td><td rowspan="3">設定 / 登録</td><td colspan="2" rowspan="2">条件付き受信 / 転送設定</td><td>条件付き受信 / 転送</td><td>オフ</td></tr>
<tr><td rowspan="2">転送設定</td><td>転送</td><td>オフ</td></tr>
<tr><td>転送先</td><td>無し</td></tr>
<tr><td rowspan="11">ネットワーク設定</td><td rowspan="11">TCP/IP</td><td colspan="2" rowspan="3">TCP/IP 設定</td><td>Bonjour 設定</td><td>Bonjour</td><td>オン</td></tr>
<tr><td rowspan="2">IPsec 設定</td><td>IPsec</td><td>オフ</td></tr>
<tr><td>制限</td><td>許可</td></tr>
<tr><td rowspan="8">IPsec ルール
(任意のルール№.の「設定 / 登録」選択)
ルール№. : 1 ～ 10</td><td colspan="2" rowspan="3">ポリシー</td><td>ルール</td><td>オフ</td></tr>
<tr><td>鍵管理方式</td><td>IKEv1</td></tr>
<tr><td>カプセル化モード</td><td>トランスポート</td></tr>
<tr><td colspan="2" rowspan="5">IP アドレス</td><td>IP バージョン</td><td>IPv4</td></tr>
<tr><td>IP アドレス</td><td>無し</td></tr>
<tr><td>サブネットマスク</td><td>無し</td></tr>
</table>

設定項目						設定値
ネットワーク設定	TCP/IP	IPsec ルール (任意のルール№.の「設定 / 登録」選択) ルール№. : 1 ～ 10	認証	ローカル側	認証方式	事前共有キー
					事前共有キー	無し
			鍵交換 (IKE phase1)		Mode	Main Mode
					Hash	SHA1
					暗号化	3DES, AES-CBC-128, AES-CBC-192, AES-CBC-256
					Diffie-Hellman グループ	modp1024(2)
					有効期間 (時間)	28800 秒
			データ保護 (IKE phase2)		プロトコル	ESP
					Hash	SHA1
					暗号化	3DES, AES-CBC-128, AES-CBC-192, AES-CBC-256
					PFS	オフ
					有効期間測定	時間およびデータサイズ
					有効期間 (時間)	3600 秒
					有効期間 (データサイズ)	100000KB
					拡張シーケンス番号	オフ

設定項目					設定値
ネットワーク設定	プロトコル	プロトコル設定	印刷プロトコル	NetBEUI	オン
				LPD	オン
				FTP（受信）	オン
				IPP	オフ
				IPP over SSL	オン
				IPP 認証	オフ
				RAW	オン
				WSD 印刷	オン
				POP3（メール受信）	オフ
			送信プロトコル	SMTP（メール送信）	オフ
				FTP クライアント (送信)	オン
				SMB	オン
				WSD スキャン	オン
				DSM スキャン	オフ
				eSCL	オン
				eSCL over SSL	オン
			その他プロトコル	SNMPv1/v2c	オン
				SNMPv3	オフ
				HTTP	オン
				HTTPS	オン
				Enhanced WSD	オン
				Enhanced WSD (SSL)	オン
				LDAP	オフ
				IEEE802.1X	オフ
				LLTD	オン
				REST	オン
				REST over SSL	オン
				VNC(RFB)	オフ
				VNC(RFB) over SSL	オフ
				Enhanced VNC(RFB) over SSL	オン

設定項目						設定値
セキュリティー設定	デバイスセキュリティー	デバイスセキュリティー設定	編集権限		アドレス帳	制限しない
					ワンタッチキー	制限しない
			認証セキュリティー設定	パスワードポリシー設定	パスワードポリシー	オフ
					パスワードの有効期間	オフ
					パスワードの長さ	オフ
					パスワードの複雑さ	3 文字以上の連続した文字は含まない
				ユーザーアカウントロックアウト設定	ロックアウトポリシー	オフ
					ロックまでの回数	3 回
					ロックアウト期間	1 分
					ロックアウト対象	リモートログインのみ
	ネットワークセキュリティー	ネットワークセキュリティー設定	セキュアプロトコル設定	SSL		オン
				サーバー機能時の設定	TLS バージョン	SSL3.0/TLS1.0：有効 TLS1.1：有効、TLS1.2：有効
					有効な暗号方式	ARCFOUR：有効、DES：無効、3DES：有効、AES：有効、AES-GCM：無効
					HTTP セキュリティー	セキュア（HTTPS）
					IPP セキュリティー	セキュア（IPPS）
					Enhanced WSD セキュリティー	セキュア（Enhanced WSD over SSL）
				クライアント機能時の設定	TLS バージョン	SSL3.0/TLS1.0：有効 TLS1.1：無効、TLS1.2：無効
					有効な暗号方式	ARCFOUR：有効、DES：有効、3DES：有効、AES：有効、AES-GCM：無効
					証明書チェック	オン

設定項目						設定値
管理設定	認証	設定 / 登録	認証設定	基本	認証	オフ
				ローカル認可設定	ローカル認可	オフ
				ゲスト認可設定	ゲスト認可	オフ
				簡単ログイン設定	簡単ログイン	オフ
	履歴設定	履歴設定		ジョブ履歴	受取人アドレス	無し
					自動送信	オフ
				ログイン履歴設定	ログイン履歴	オフ
					受取人アドレス	無し
					自動送信	オフ
				デバイス履歴設定	デバイス履歴	オフ
					受取人アドレス	無し
					自動送信	オフ
				セキュリティー通信エラー履歴設定	セキュリティー通信エラー履歴	オフ
					受取人アドレス	無し
					自動送信	オフ

本機で変更する項目

設定項目			設定値
システムメニュー	システム / ネットワーク	セキュリティーレベル	高い
	インターネット	インターネットブラウザー	使用しない

本機のカスタムボックス初期値

設定項目	設定値
ボックス所有者	未設定
ボックス共有設定	所有者のみ

お客様相談窓口のご案内

弊社製品についてのお問い合わせは、下記のナビダイヤルへご連絡ください。市内通話料金でご利用いただけます。

京セラドキュメントソリューションズ株式会社
京セラドキュメントソリューションズジャパン株式会社

〒158-8610　東京都世田谷区玉川台2丁目14番9号

http://www.kyoceradocumentsolutions.co.jp

お客様相談窓口

0570-046562

市内通話料でOK ナビダイヤル® 市内通話料金でご利用いただけます。

受付時間
● 9:00～12:00 / 13:00～17:00
（土曜、日曜、祝日および当社指定休日は除く）

2018.9
3MS2V8KDJA0