



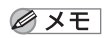
imageRUNNER
ADVANCE

C5051/C5051F/C5045/C5045F
C5035/C5035F/C5030/C5030F

機能追加／変更のお知らせ

はじめに

本製品の機能に、追加／変更がございます。このお知らせをお読みになり、取扱説明書とともに保管してください。



本書で使われている画面は、特にお断りがない限り、imageRUNNER ADVANCE C5051 にスーパー G3FAX ボード、インナーフィニッシャー・A1、2 段カセットペディスタル・AD1 が装着されている場合のものです。

※ Canon、Canon ロゴ、imageRUNNER ADVANCE はキヤノン株式会社の商標です。

目次

システムバージョンアップ時の注意事項	4
デフォルト設定の変更内容がクリアされます.....	4
オプションに関する変更	5
オプションが追加されました.....	5
設定 / 登録に関する変更	6
設定 / 登録一覧表.....	6
追加項目.....	6
削除項目.....	9
オートクリアの設定変更を制限できるようになりました（オートクリア移行時間の制限）.....	9
IPSec 設定で登録するセキュリティポリシーの暗号化アルゴリズムが変更されました.....	10
SNMPv1 で専用コミュニティを設定できるようになりました SNMPv3 の暗号化アルゴリズムに AES を選択できるようになりました.....	14
SNMPv1 で専用コミュニティを設定する.....	14
SNMPv3 ユーザーを追加する.....	15
フルカラー時の色味を鮮やかにできるようになりました（フルカラー時の鮮やかさ設定）.....	15
用紙のサドル折り位置を調整できるようになりました（折り位置の調整）.....	16
PDF の下限バージョンを指定できるようになりました（PDF の下限バージョン指定）.....	16
Rights Management サーバーを設定できるようになりました（Rights Management サーバー設定）.....	16
PCL のステータスプリント、フォントリストを出力できるようになりました（PCL）.....	18
PCL プリントを設定できるようになりました（PCL 設定）.....	18
PCL 設定メニューについて.....	18
PCL 設定メニューの設定項目.....	20
プリンタードライバーからのジョブ制限を詳細に指定できるようになりました.....	27
メールアドレスの入力を補完できるようになりました（メールアドレスの入力補完）.....	27
認証ユーザー名をファクス送信時に発信人の名称として使用できるようになりました（認証ユーザー名を発信人として使用）.....	28
ファクスの通信モードを設定できるようになりました【G4】（通信モード）.....	28
相手先の発信元記録をつけてファクスをプリントできるようになりました【G4】（相手先発信元記録（G4））.....	29
ボックスのセキュリティを設定できるようになりました（ボックスのセキュリティ設定）.....	29
ボックスの暗証番号を 7 桁固定にする.....	29
プリンタードライバーから保存時のプリント設定の変更を制限する.....	30
メモリーメディアへのファイル保存／プリントを制限できるようになりました（メモリーメディア設定）.....	30
宛先表エクスポート時にパスワードを含めるかどうか設定できるようになりました.....	31
SSL 暗号化通信に必要な鍵ペアを生成する際に、署名アルゴリズムと鍵のアルゴリズムを選択できるようになりました.....	31
監査ログの取得を設定できるようになりました（監査ログを取得）.....	32
FIPS 140-2 に準拠した暗号方式を使用できるようになりました（暗号方式を FIPS 140-2 準拠にする）.....	33
スキャン機能に関する変更（[ファクス]、[スキャンして送信]、[スキャンして保存]）	34
[ファクス]、[スキャンして送信]、[スキャンして保存] でフリーサイズを選択してスキャンできるようになりました.....	34
[スキャンして送信]、[スキャンして保存] で Rights Management サーバーのポリシー適用 PDF を生成できるようになりました.....	35
プリント機能に関する変更（[コピー]、[保存ファイルの利用]、[セキュアプリント]、状況確認 / 中止）	37
[コピー]、[保存ファイルの利用] で中綴じフィニッシャー・C1 装着時にサドル折りを設定してプリントできるようになりました.....	37

[セキュアプリント]と状況確認/中止画面で、割込/優先プリントできるようになりました (割込/優先プリント).....	37
ジョブ状況画面にプリント待ち時間が表示されるようになりました.....	39
プリンタードライバーから2色カラーでプリントできるようになりました.....	40
[ウェブブラウザー]でWebページのプリントが非対応になりました.....	42
PCLプリンタードライバーに対応してプリントできるようになりました.....	42
アドバンスドボックスに関する変更.....	43
アドバンスドボックス管理者がコンピューターからアクセスしたときの操作権限が拡がりました.....	43
アドバンスドボックス内のファイルが画像表示できるようになりました.....	43
カスタムメニュー機能に関する変更.....	45
[カスタムメニュー]でマイボタンの使用を制限できるようになりました(マイボタンの使用).....	45
リモート UI 機能に関する変更.....	47
URI 送信を設定できるようになりました (URI 送信設定).....	47
本機のアドバンスドボックスをループバックアドレスで宛先に指定する.....	52
監査ログを管理できるようになりました (監査ログのエクスポート/クリア).....	53
監査ログ管理機能と管理できるログの種類について.....	53
ログを管理する.....	54
アドレス帳のエクスポート/インポートにパスワードを含めることができるようになりました.....	58
宛先表をファイルに保存する (エクスポート).....	58
宛先表をファイルから読み込む (インポート).....	59
鍵ペアとサーバー証明書、CA 証明書のアルゴリズムが変更されました.....	61
鍵ペアとサーバー証明書.....	61
CA 証明書.....	61
MEAP 機能に関する変更.....	62
SMS は常時、SSL 暗号化通信で使用するようになりました.....	62
SMS 使用時に MEAP アプリケーションの設定情報を管理できるようになりました (MEAP アプリケーションの設定情報管理).....	63
SMS 使用時に MEAP アプリケーションのログを管理できるようになりました (MEAP アプリケーションのログ管理).....	65
アプリケーションログのダウンロード.....	65
アプリケーションログの削除.....	66
SSO-H 使用時にデフォルトパスワードでのログインを許可できるようになりました (管理者がデフォルトのパスワードで運用することを許可する).....	68
クラウドサービスが利用できるようになりました.....	70
情報セキュリティ規格 (IEEE 2600) について.....	71
IEEE 2600 で定められたセキュリティについて.....	71

システムバージョンアップ時の注意事項

デフォルト設定の変更内容がクリアされます

システムバージョンアップのため、コントローラーバージョンの先頭2桁を「50」以上にしたときは、以下のデフォルト設定の変更がクリアされます。

■ [保存ファイルの利用]→[ボックス]→[送信する]

- ファイル形式の設定
- その他の機能の設定

■ [受信トレイ]→[システムボックス]→[メモリー受信ボックス]→[送信する]

- ファイル形式の設定
- その他の機能の設定

デフォルトの設定を変更している場合は、あらかじめ設定を確認のうえ、システムバージョンアップ完了後に再度設定を行ってください。

-  **メモ** • コントローラーバージョンを確認するには、操作パネルの **123** (カウンター確認) を押したあと、[デバイス構成確認] を押します。
- デフォルト値は、[保存ファイルの利用]、[受信トレイ]ともに、以下のとおりです。
 - ファイル形式の設定：PDF (高圧縮)
 - その他の機能の設定：設定なし

オプションに関する変更

オプションが追加されました

本製品の性能を高めることができるオプション製品が以下のように追加されました。

■ G4FAX ボード

ISDN 回線を使用して複数の受信機を接続し、用途に応じて受信する機械を選択することができます。また、スーパー G3FAX ボードよりファクスの通信時間が早くなります。



- スーパーG3FAX ボード、G3回線増設キット、リモートFAX送信キットと同時に装着することはできません。
- G4FAXボードを装着した場合、リモートファクスのサーバー機としてお使いになることはできません。

■ コピーカードリーダー・F1

コントロールカードを使用して部門別 ID 管理を行います。

■ PCLエミュレーション拡張キット

PCL プリンターとして使用するためのオプションです。PCL プリンタードライバは、Windows 英語版にのみ対応しています。ドライバー画面は英語で表記されています。

■ PCLバーコードプリント拡張キット・D1

バーコードプリントを行なうためのオプションです。

設定 / 登録に関する変更

設定 / 登録一覧表

-  **メモ** 機器情報配信項目の表示は以下のとおりです。機器情報配信機能については、e-マニュアル>セキュリティを参照してください。
- ：機器情報配信対象
 - ×：機器情報配信対象外

追加項目

■ 環境設定：タイマー／電力設定

以下の項目が追加されました。

設定／登録項目	設定項目	工場出荷時の状態	機器情報配信項目	参照ページ
オートクリア移行時間の制限	ON、OFF	OFF	○	P.9

■ 環境設定：ネットワーク

[IPSec 設定] と [SNMP 設定] に太字の項目が追加されました。

設定／登録項目	設定項目	工場出荷時の状態	リモート UI による設定	機器情報 配信項目	参照ページ
IPSec 設定 *1					P.10
登録：IKE 設定					
IKE モード	メイン、アグレッシブ	メイン	○	×	
認証方式	事前共有鍵方式、電子署名方式	事前共有鍵方式	○	×	
認証 / 暗号化アルゴリズム	自動、手動指定	自動	○	×	
	認証 / 暗号化アルゴリズム：手動指定				
	・ 認証 SHA1、 SHA2	SHA1	○	×	
	・ 暗号 3DES-CBC、AES-CBC	3DES-CBC	○	×	
	・ DH グループ Group1 (762)、Group2 (1024)、Group14 (2048)、 ECDH-P256、ECDH-P384	Group2 (1024)	○	×	
登録：IPSec 通信設定					
有効期間：時間	1 ～ 65535 分	480	○	×	
有効期間：サイズ	1 ～ 65535 MB	65535	○	×	
PFS	ON、OFF	OFF	○	×	
認証 / 暗号化アルゴリズム	自動、手動指定	自動	○	×	
	認証 / 暗号化アルゴリズム：手動指定				
	ESP、 ESP(AES-GCM)、AH(SHA1)	ESP	○	×	
	ESP 設定時： ESP 認証 SHA1、NULL	SHA1	○	×	
	ESP 暗号 3DES-CBC、AES-CBC、NULL	3DES-CBC	○	×	
接続モード	トランスポートモード、表示のみ		○	×	

設定／登録項目	設定項目	工場出荷時の状態	リモート UI による設定	機器情報 配信項目	参照ページ
SNMP 設定					P.14
SNMPv1 を使用	ON、OFF	ON	○	○	
専用コミュニティ設定					
専用コミュニティ	ON、OFF	ON	○	×	
MIB アクセス権限	読込 / 書込、読込のみ	読込 / 書込	○	×	
SNMPv3 を使用	ON、OFF	OFF	○	×	P.15
ユーザー設定					
ユーザー設定の有効 / 無効		-	○	×	
登録	ユーザー名、MIB アクセス制限、セキュリティ設定、認証アルゴリズム (MD5、SHA1)、認証パスワード、暗号化アルゴリズム (DES、 AES)、暗号化パスワード	-	○	×	
詳細 / 編集	ユーザー名、MIB アクセス制限、セキュリティ設定、認証アルゴリズム (MD5、SHA1)、認証パスワード、暗号化アルゴリズム (DES、 AES)、暗号化パスワード	-	○	×	
削除	-	-	○	×	

*1 IPsec セキュリティボードを有効にしているときに表示される項目です。

■ 調整／メンテナンス：画質調整

以下の項目が追加されました。

設定／登録項目	設定項目	工場出荷時の状態	機器情報配信項目	参照ページ
フルカラー時の鮮やかさ設定	標準、レベル 1、レベル 2	標準	×	P.15

■ 調整／メンテナンス：動作調整

以下の項目が追加されました。

設定／登録項目	設定項目	工場出荷時の状態	機器情報配信項目	参照ページ
折り位置の調整 *2	位置：－ 2.0 mm ～＋ 2.0 mm (0.25 mm 間隔)	0 mm	×	P.16

*2 中綴じフィニッシャー・C1 を装着している場合に表示される項目です。

■ ファンクション設定：共通

[ファイル生成] に、以下の項目が追加されました。

設定／登録項目	設定項目	工場出荷時の状態	機器情報配信項目	参照ページ
PDF の下限バージョン指定	指定しない、1.5、1.6、1.7	指定しない	○	P.16
Rights Management サーバー設定				
サーバーの URL	サーバーの URL：最大 128 文字	(空欄)	×	P.16
ユーザー名	ユーザー名：最大 128 文字	(空欄)	×	
パスワード	パスワード：最大 32 文字	(空欄)	×	
ユーザー毎パスワードを使用	ON、OFF	OFF	×	

■ ファンクション設定：プリンター

太字の項目が追加されました。

設定／登録項目	設定項目	工場出荷時の状態	機器情報配信項目	参照ページ
PCL^{*3}				P.18
ステータスプリント	プリント	—	×	
フォントリスト	プリント	—	×	
プリンタージョブの制限	ON、OFF	OFF	○	P.27
	・ ON 設定時 許可するジョブの選択 プリント保留、プリント保留 +セキュアプリント	プリント保留	×	

^{*3} PCL エミュレーション拡張キットを有効にしている場合に表示される項目です。

また、[プリンター設定] の [仕様設定] に [PCL 設定] が追加されました。詳しくは「PCL プリントを設定できるようになりました (PCL 設定)」(→ P.18) を参照してください。

■ ファンクション設定：送信

[E メール/ファクス設定] と [ファクス設定] に、以下の項目が追加されました。

設定／登録項目	設定項目	工場出荷時の状態	機器情報配信項目	参照ページ
E メール/ファクス設定				
メールアドレスの入力補完	ON、OFF	ON	○	P.27
ファクス設定^{*4}				
認証ユーザー名を発信人として使用	ON、OFF	OFF	○	P.28
通信モード ^{*5}	G3-G4、G3 のみ	G3-G4	○	P.28

^{*4} スーパー G3FAX ボード、G4FAX ボード、リモート FAX 送信キットのいずれかを装着している場合に表示される項目です。

^{*5} G4FAX ボード装着時に表示される項目です。

■ ファンクション設定：受信／転送

以下の項目が追加されました。

設定／登録項目	設定項目	工場出荷時の状態	機器情報配信項目	参照ページ
相手発信元記録 (G4) ^{*5}	つける、つけない	つける	○	P.29

^{*5} G4FAX ボード装着時に表示される項目です。

■ ファンクション設定：ファイル保存／利用

[ボックス設定] に以下の項目が追加されました。また、[メモリーメディア設定] が追加されました。

設定／登録項目	設定項目	工場出荷時の状態	機器情報配信項目	参照ページ
ボックス設定				
ボックスのセキュリティー設定	ボックス暗証番号7桁固定 / アクセス制限：ON、OFF	OFF	○	P.29
	プリンタードライバーから保存時のプリントの表示：ON、OFF	ON	○	P.29
メモリーメディア設定				
スキャン/プリント機能を使用	スキャン機能を使用：ON、OFF	ON	○	P.30
	プリント機能を使用：ON、OFF	ON	○	P.30

■ 宛先設定

以下の項目が追加されました。

設定／登録項目	設定項目	工場出荷時の状態	機器情報配信項目	参照ページ
アドレス帳エクスポートの対象にパスワードを含める	ON、OFF	OFF	○	P.31

■ 管理設定：デバイス管理

太字の項目が追加されました。

設定／登録項目	設定項目	工場出荷時の状態	機器情報配信項目	参照ページ
証明書設定				P.31
証明書設定：鍵生成：ネットワーク通信用の鍵生成				
鍵の名前	最大 24 文字	(空欄)	×	
署名アルゴリズム	SHA1、SHA256、SHA384、SHA512	SHA1	×	
鍵のアルゴリズム	RSA	RSA	×	
鍵の種類	512、1024、 2048、4096	512	×	P.32
監査ログを取得	ON、OFF	OFF	×	
暗号方式を FIPS 140-2 準拠にする ^{*1}	ON、OFF	OFF	×	P.33

*1 IPsec セキュリティボードを有効にしているときに表示される項目です。

削除項目

■ ファンクション設定：共通

「スキャン動作」から以下の項目が削除されました。

設定／登録項目	設定項目	工場出荷時の状態	機器情報配信項目
スキャン動作			
リモートスキャン時のデータ圧縮率	高圧縮、普通、低圧縮	普通	○

オートクリアの設定変更を制限できるようになりました（オートクリア移行時間の制限）

本機能を「ON」に設定すると、一般ユーザーは以下の機能进行操作できなくなります。

- [環境設定]（設定／登録）の [オートクリア移行時間]（→e-マニュアル＞設定/登録）
- [環境設定]（設定／登録）の [オートクリア後の機能]（→e-マニュアル＞設定/登録）

1 ㊟（設定／登録）→ [環境設定] → [タイマー / 電力設定] → [オートクリア移行時間の制限] を押します。

2 [ON] または [OFF] を選択したあと、[OK] を押します。

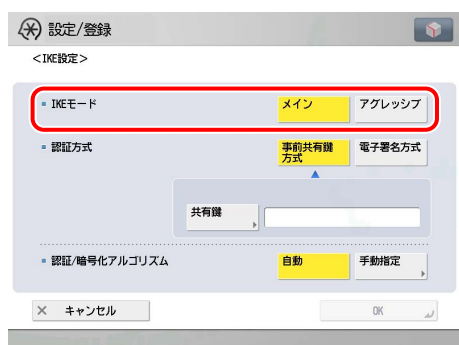
IPSec 設定で登録するセキュリティポリシーの暗号化アルゴリズムが変更されました

[IPsec 設定] で新しいセキュリティポリシーを登録する際、[IKE 設定] と [IPSec 通信設定] で使用する認証と暗号化のアルゴリズムが変更されました。[IKE 設定] と [IPSec 通信設定] の設定方法は以下のとおりです。

重要 この機能は、IPSec セキュリティボードが装着されている場合に使用できます。

メモ [IPsec 設定] でのセキュリティポリシー登録方法については、e-マニュアル > ネットワークを参照してください。

- 1 (設定／登録) → [環境設定] → [ネットワーク] → [TCP/IP 設定] → [IPSec 設定] を押したあと、<IPSec を使用> を「ON」にします。
- 2 <ポリシー外パケットの受信> の [登録] を押します。→ポリシー名に名称を入力したあと、[IKE 設定] を押します。
- 3 登録画面で [IKE 設定] を押して IKE フェーズ 1 で使用するモードを選択します。



[メイン]：メインモードを設定します。IKE セッション自体を暗号化するため、セキュリティが強固です。

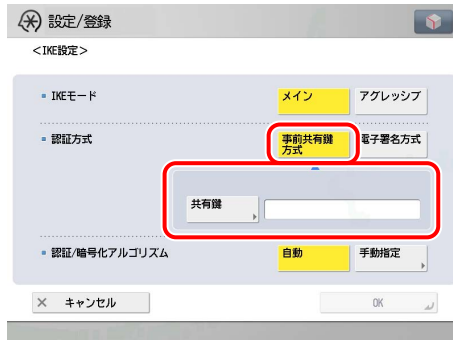
[アグレッシブ]：アグレッシブモードを設定します。暗号化されないため IKE セッションが高速化します。

4 IKE 設定画面で IKE フェーズ 1 に使用する認証方式を指定します。

事前共有鍵方式を選択する場合は、事前共有鍵を準備してください。電子署名方式を選択する場合は、事前に CA 証明書の登録（→ e-マニュアル＞セキュリティ）、鍵ペアファイルと証明書ファイルのインストール（→ e-マニュアル＞リモート UI）を行ってください。

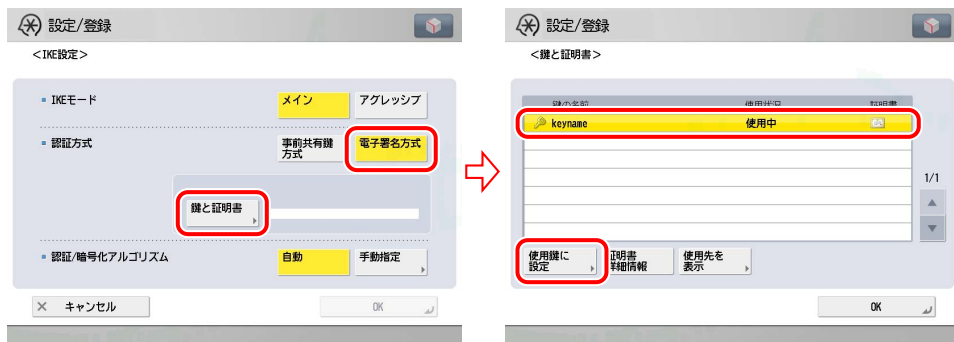
● 事前共有鍵方式を設定する：

- <認証方式>の「事前共有鍵方式」→「共有鍵」を押して、事前共有鍵を入力します。



● 電子署名方式を設定する：

- <認証方式>の「電子署名方式」→「鍵と証明書」を押して、使用したい鍵ペアを選択したあと「使用鍵に設定」を押してIPSecに使用する鍵ペアを登録します。



「Device Signature Key」（機器署名用鍵ペア）、および「AMS」（アクセス制限用鍵ペア）は使用鍵に設定できません。

📌 重要

署名アルゴリズムの「RSA-MD5」、「RSA-MD2」を使用している鍵ペアを選択した場合に IPSec 通信を FIPS（連邦情報処理規格：Federal Information Processing Standards）140-2 に準拠させたときは、この鍵ペアを設定したポリシーは無効（OFF）になります。（→ FIPS 140-2 に準拠した暗号方式を使用できるようになりました（暗号方式を FIPS 140-2 準拠にする）：P.33）

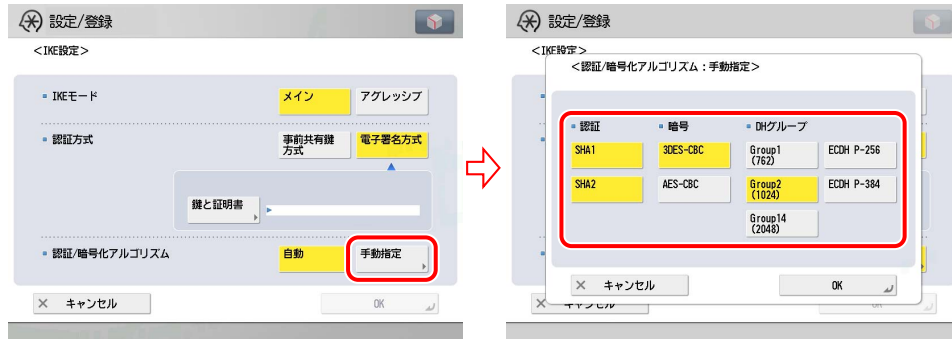
📝 メモ

- 鍵と証明書画面で鍵ペアを選択したあと「証明書詳細情報」を押すことによって、証明書の内容を確認できます。また、証明書詳細情報画面で「証明書検証」を押して証明書を検証することもできます。
- 鍵と証明書画面で<使用状況>に「使用中」と表示されている鍵ペアを選択したあと「使用先を表示」を押すことによって、鍵ペアの用途を確認できます。

5 IKE 設定画面で、IKE フェーズ 1 に使用する認証と暗号化のアルゴリズムを選択します。

● 認証と暗号化のアルゴリズムを指定する：

- <認証/暗号化アルゴリズム>の「手動指定」を押して、IKE SAに適用する認証と暗号化のアルゴリズムを選択します。



< 認証 > の [SHA1]： 認証アルゴリズムに SHA1 (Secure Hash Algorithm 1) を設定します。160 ビットのハッシュ値をサポートします。

< 認証 > の [SHA2]： 認証アルゴリズムに SHA2 (Secure Hash Algorithm 2) を設定します。256 ビット、および 384 ビットのハッシュ値をサポートします。

< 暗号 > の [3DES-CBC]： 暗号化アルゴリズムに 3DES (Triple Data Encryption Standard)、暗号モードに CBC (Cipher Block Chaining) を設定します。3DES は、DES を 3 回行うため処理時間は長くなりますが、暗号の強度は高まります。CBC では、前のブロックの暗号化結果が次のブロックに連鎖され、暗号を解読しにくくすることができます。

< 暗号 > の [AES-CBC]： 暗号化アルゴリズムに AES (Advanced Encryption Standard)、暗号モードに CBC を設定します。AES は、128、192、および 256 ビットの鍵長の暗号鍵をサポートします。サポートする鍵長が長いと、暗号の強度が高まります。CBC では、前のブロックの暗号化結果が次のブロックに連鎖され、暗号を解読しにくくすることができます。

< DH グループ > の [Group1(762)]： DH (Diffie-Hellman) 鍵交換方式に Group1 を設定します。Group1 では、762 ビットの MODP (Modular Exponentiation) をサポートします。

< DH グループ > の [Group2(1024)]： DH 鍵交換方式に Group2 を設定します。Group2 では 1024 ビットの MODP をサポートします。

< DH グループ > の [Group14(2048)]： DH 鍵交換方式に Group14 を設定します。Group14 では 2048 ビットの MODP をサポートします。

< DH グループ > の [ECDH-P256]： 256 ビットの鍵長の ECDH (Elliptic Curve Diffie Hellman) 鍵交換方式を設定します。

< DH グループ > の [ECDH-P384]： 384 ビットの鍵長の ECDH 鍵交換方式を設定します。

● 認証と暗号化のアルゴリズムを自動で設定する：

- <認証/暗号化アルゴリズム>の「自動」を押します。

認証と暗号化のアルゴリズムの優先順位は、以下のとおりです。

優先順位	認証アルゴリズム	暗号化アルゴリズム	DH 鍵交換方式
1	SHA1	AES（128 ビット）	Group2
2	SHA2（256 ビット）		
3	SHA2（384 ビット）		
4	SHA1	AES（192 ビット）	
5	SHA2（256 ビット）		
6	SHA2（384 ビット）		
7	SHA1	AES（256 ビット）	
8	SHA2（256 ビット）		
9	SHA2（384 ビット）		
10	SHA1	3DES	
11	SHA2（256 ビット）		
12	SHA2（384 ビット）		

6 登録画面で「IPSec 通信設定」を押して、SA の有効時間や有効タイプ、および PFS（Perfect Forward Security）を指定します。



<有効期間>の「時間」と「サイズ」：生成される IKE SA と IPSec SA の有効期間を指定します。有効期間内のセキュリティポリシーが適用された IPSec 通信では鍵交換のネゴシエーションを行わずにパケットを送受信できます。「時間」と「サイズ」のいずれかを必ず設定してください。両方を設定した場合は、「時間」と「サイズ」のどちらか一方が設定値に達したときに SA の有効期限が切れます。

<PFS> を「ON」：PFS 機能を有効にすると、1 つの暗号鍵が第三者に知られてしまっても、他の暗号鍵には被害が波及しないため、機密性が向上します。

<PFS> を「OFF」：PFS 機能を無効にした場合、1 つの暗号鍵が第三者に知られると、他の暗号鍵も予測される怖れがあります。<PFS> を「ON」に設定した場合は、通信先の PFS も有効にする必要があります。

7 IPSec 通信設定画面で、IKE フェーズ 2 に使用する認証と暗号化のアルゴリズムを選択します。

● 認証と暗号化のアルゴリズムを指定する：

- <認証/暗号化アルゴリズム>の「手動指定」を押します。
- 認証方式のアルゴリズムを設定します。



設定できる認証と暗号化のアルゴリズムは、以下のとおりです。

認証方式	説明
[ESP]	<ESP 認証> [SHA1]：ESP 認証方式のアルゴリズムに SHA1 を設定します。160 ビットのハッシュ値をサポートします。 [NULL]：ESP 認証方式のアルゴリズムを設定しません。 <ESP 暗号> [3DES-CBC]：ESP 暗号化方式のアルゴリズムに 3DES、暗号モードに CBC を設定します。3DES は、DES を 3 回行うため処理時間は長くなりますが、暗号の強度は高まります。CBC では、前のブロックの暗号化結果が次のブロックに連鎖され、暗号を解読しにくくすることができます。 [AES-CBC]：ESP 暗号化方式のアルゴリズムに AES、暗号モードに CBC を設定します。AES は、128、192、および 256 ビットの鍵長の暗号鍵をサポートします。サポートする鍵長が長いと、暗号の強度が高まります。CBC では、前のブロックの暗号化結果が次のブロックに連鎖され、暗号を解読しにくくすることができます。 [NULL]：ESP 暗号化方式のアルゴリズムを設定しません。

認証方式	説明
[ESP(AES-GCM)]	128 ビット、192 ビット、および 256 ビットの鍵長の AES-GCM (Advanced Encryption Standard - Galois Counter Mode) を設定します。AES-GCM は、暗号化と認証を同時に行うアルゴリズムです。
[AH(SHA1)]	AH 認証方式のアルゴリズムに SHA1 を設定します。160 ビットのハッシュ値をサポートします。

重要 IPsec 通信を FIPS 140-2 に準拠させた場合は、認証方式に [ESP(AES-GCM)] を設定しているポリシーは無効 (OFF) になります。同時に、このポリシーの認証アルゴリズムは SHA1 へ、暗号アルゴリズムは 3DES-CBC へ自動的に変更されます。(→ FIPS 140-2 に準拠した暗号方式を使用できるようになりました (暗号方式を FIPS 140-2 準拠にする) : P.33)

● 認証と暗号化のアルゴリズムを自動で設定する：

□ <認証/暗号化アルゴリズム>の [自動] を押します。

ESP 認証・暗号化方式が設定されます。認証と暗号化のアルゴリズムの優先順位は、以下のとおりです。

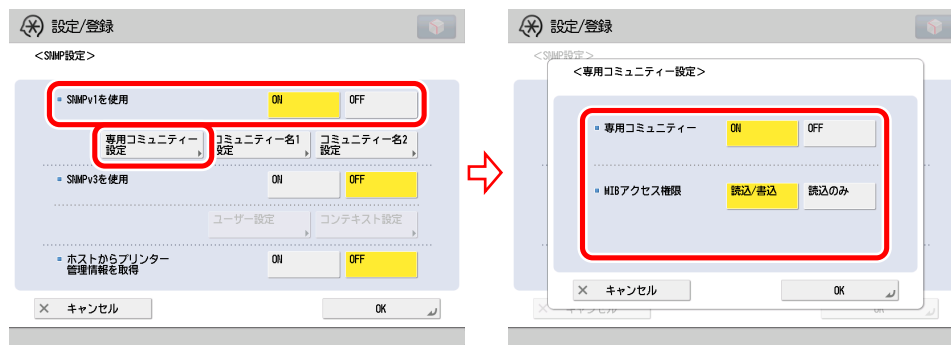
優先順位	ESP 認証方式のアルゴリズム	ESP 暗号化方式のアルゴリズム
1	SHA1	AES (128 ビット)
2	SHA1	AES (192 ビット)
3	SHA1	AES (256 ビット)
4	SHA1	3DES

**SNMPv1 で専用コミュニティを設定できるようになりました
SNMPv3 の暗号化アルゴリズムに AES を選択できるようになりました**

メモ SNMP 設定の詳細については、e-マニュアル>ネットワークを参照してください。

SNMPv1 で専用コミュニティを設定する

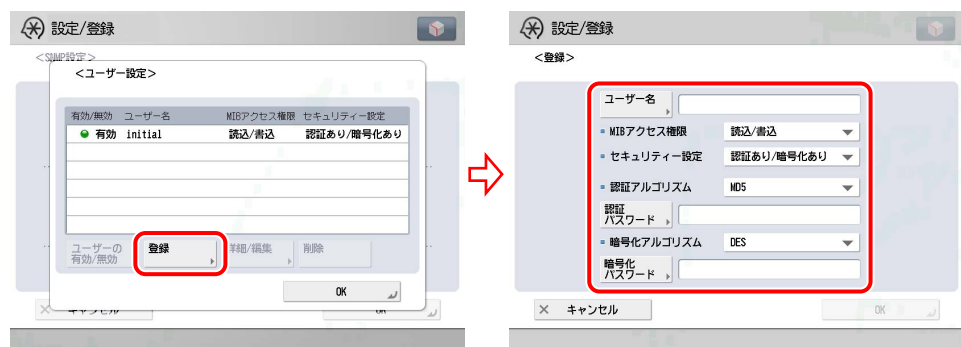
- 1 ネットワーク画面の [SNMP 設定] で、SNMPv1 を設定します。
- 2 [専用コミュニティ設定] → [ON] を押したあと、<MIB アクセス権限> を設定します。



SNMPv3 ユーザーを追加する

- 1 ネットワーク画面の [SNMP 設定] で、SNMPv3 を設定します。
- 2 <SNMPv3 を使用> を「ON」にして、[ユーザー設定] → [登録] を押したあと、ユーザー名、MIB アクセス権限、セキュリティを設定します。

- セキュリティ設定ドロップダウンリストから [認証あり/暗号化あり] を選択した場合：
認証アルゴリズムを以下から選択して、認証パスワードを入力します。
 - MD5
 - SHA1暗号化アルゴリズムを以下から選択して、暗号化パスワードを入力して [OK] を押します。
 - DES
 - AES
- セキュリティ設定ドロップダウンリストから [認証あり/暗号化なし] を選択した場合：
認証アルゴリズムを以下から選択して、認証パスワードを入力して [OK] を押します。
 - MD5
 - SHA1
- セキュリティ設定ドロップダウンリストから [認証なし/暗号化なし] を選択した場合：
[OK] を押します。



フルカラー時の色味を鮮やかにできるようにになりました（フルカラー時の鮮やかさ設定）

コピーまたは保存ファイルの利用からプリントするときの色合いをより鮮やかにできます。ジョブごとに設定するのではなく、すべてのジョブのデフォルトを一括で設定できます。

-  **メモ**
- コピーまたは保存ファイルの利用の [カラー選択] で [フルカラー] を選択している場合、または [自動(カラー/白黒)] を選択してフルカラーと認識されている場合に有効になります。
 - コピーまたは保存ファイルの利用の [ワンタッチ調整] で [レトロ調モノクロ] を選択している場合、本機能は使用できません。

- 1 (設定/登録) → [調整/メンテナンス] → [画質調整] → [フルカラー時の鮮やかさ設定] を押します。
- 2 [標準]、[レベル 1] または [レベル 2] を選択したあと、[OK] を押します。

選択する項目

- [標準]： 原稿の色味を再現します。
[レベル 1]： [標準] よりも色味を鮮やかにします。
[レベル 2]： [レベル 1] よりも色味を鮮やかにします。

-  **メモ**
- 設定は、本製品の主電源スイッチを入れなおしたあとに有効になります。
 - 電源の入れかた／切りかたは、e-マニュアル> お使いになる前にを参照してください。

用紙のサドル折り位置を調整できるようになりました（折り位置の調整）

サドル折りを行う場合の用紙の折り位置を調整できます。

-  **重要** この機能は、中綴じフィニッシャー・C1 を装着している場合に使用できます。

- 1  （設定／登録）→ [調整 / メンテナンス] → [動作調整] → [折り位置の調整] を押します。
- 2 調整する用紙サイズを選択します。
- 3 [▼] [▲] を押して折り位置を調整したあと、[OK] を押します。

PDF の下限バージョンを指定できるようになりました（PDF の下限バージョン指定）

PDF 生成時に付与するバージョンの下限を指定できます。

-  **重要** 本設定では、PDF 生成時に付与され得るバージョン範囲の下限を指定します。PDF に設定する機能によっては、本設定で指定したバージョンよりも上になる場合があります。

-  **メモ** ファクス、Iファクスの送信では、この設定は無効になります。

- 1  （設定／登録）→ [ファンクション設定] → [共通] → [ファイル生成] → [PDF の下限バージョン指定] を押します。
- 2 [指定しない]、[1.5]、[1.6] または [1.7] を選択したあと、[OK] を押します。

Rights Management サーバーを設定できるようになりました（Rights Management サーバー設定）

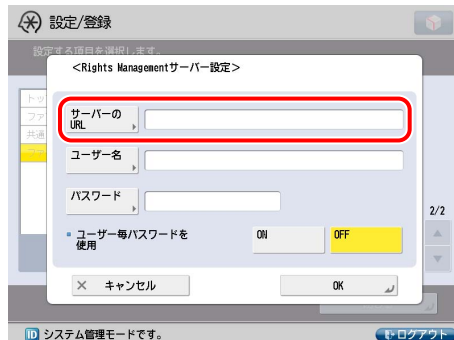
本機は、Adobe LiveCycle Rights Management との連携によって閲覧権限などが管理された PDF を生成できます。ここでは、Adobe LiveCycle Rights Management サーバーに接続するときの設定について説明しています。

Rights Management サーバーを利用した PDF を生成する手順については、「[スキャンして送信]、[スキャンして保存] で Rights Management サーバーのポリシー適用 PDF を生成できるようになりました」（→ P.35）を参照してください。

-  **重要**
- 本機能を設定するには、Adobe LiveCycle Rights Management ESまたはAdobe LiveCycle Rights Management ES2 が必要です。詳細については、お買い求めの販売店へお問い合わせください。
 - 本機能を設定するには、Adobe LiveCycle Rights Managementサーバーと本製品がイントラネットやインターネットで接続されている必要があります。

1 ④ (設定／登録) → [ファンクション設定] → [共通] → [ファイル生成] → [Rights Management サーバー設定] を押します。

2 Adobe LiveCycle Rights Management サーバーの URL を入力します。



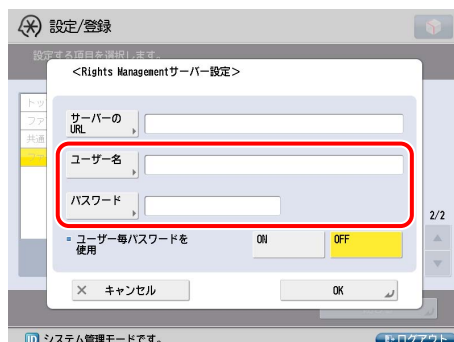
サーバーの URL は、「https://<IP アドレスまたはホスト名>:<ポート番号>」の形式で入力してください。

入力例：

- https://192.168.1.21:8443
- https://RMServer.host.canon.jp:8443

重要 IP アドレス、ホスト名、ポート番号については、Adobe LiveCycle Rights Management サーバーの管理者にお問い合わせください。

3 必要に応じて、Adobe LiveCycle Rights Management サーバーにログインするためのユーザー名とパスワードを入力します。



手順4で「ユーザー毎パスワードを使用」を「ON」にする場合、ここにユーザー名とパスワードを入力する必要はありません。

「ユーザー毎パスワードを使用」を「OFF」にする場合でも、ユーザー名とパスワードをジョブごとに毎回入力する場合は、空欄にします。

4 「ユーザー毎パスワードを使用」の「ON」または「OFF」を選択します。

本機能を利用した PDF を生成するときは、Adobe LiveCycle Rights Management サーバーへのログイン画面が表示されます。

手順3でユーザー名とパスワードを入力して、「ユーザー毎パスワードを使用」が「OFF」の場合、ログイン画面にはユーザー名とパスワードが自動入力された状態で表示されます。ユーザー名とパスワードが未入力のときは、ジョブごとに毎回入力する必要があります。

「ユーザー毎パスワードを使用」が「ON」の場合は、Adobe LiveCycle Rights Management サーバーにログインするためのユーザー名とパスワードを、ジョブごとに入力します。

5 [OK] を押します。

PCL のステータスプリント、フォントリストを出力できるようになりました (PCL)

重要 この機能は、PCL エミュレーション拡張キットを有効にしている場合に使用できます。

● PCLステータスプリント

共通メニューの内容に加えて、PCL 設定メニューの設定内容がプリントされます。

1. Ⓢ (設定／登録) を押したあと、[ファンクション設定] を押します。
2. [プリンター] を押します。
3. [レポート出力] を押します。
4. [PCL] を押します。
5. [ステータスプリント] を押して出力します。

● PCLフォントリスト

PCL モードで使えるフォントの一覧がプリントされます。

1. Ⓢ (設定／登録) を押したあと、[ファンクション設定] を押します。
2. [プリンター] を押します。
3. [レポート出力] を押します。
4. [PCL] を押します。
5. [フォントリスト] を押して出力します。

PCL プリントを設定できるようになりました (PCL 設定)

重要 この機能は、PCL エミュレーション拡張キットを有効にしている場合に使用できます。

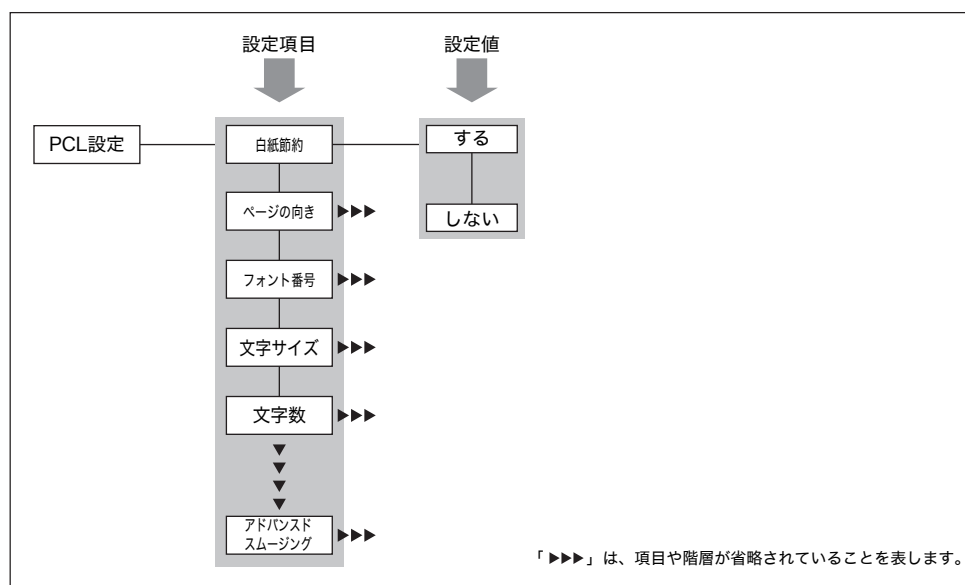
PCL 設定メニューについて

ここでは、PCL 設定メニューの機能と構造、操作手順について説明します。

■PCL設定メニューの機能

PCL 設定メニューでは、タイムアウトやフォント置換、文字やイメージの色処理などの設定をします。

■PCL設定メニューの構造

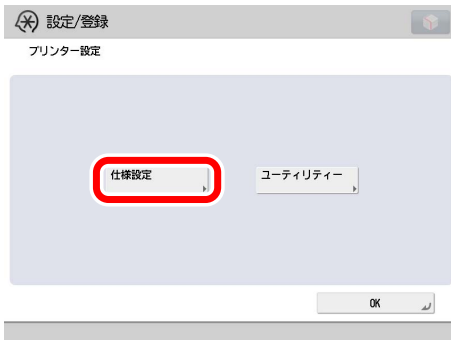


■PCL設定メニューの操作の流れ

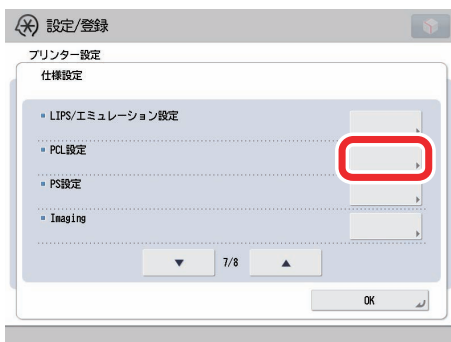
ここでは、白紙節約を「しない」に設定する手順を例に説明します。

- 1 (設定／登録) を押したあと、[ファンクション設定] → [プリンター] → [プリンター設定] を押します。

- 2 [仕様設定] を押します。



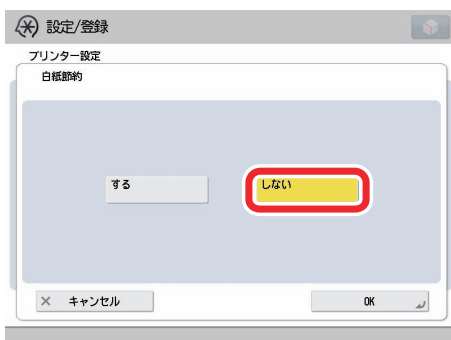
- 3 [PCL 設定] を押します。



- 4 [白紙節約] を押します。



- 5 [しない] を押します。



6 [OK] を押します。



PCL 設定メニューの設定項目

- メモ
- PCL 設定メニューは、PCL プリンターのみ表示されます。
 - 太字で示されている設定値は、工場出荷時の値です。

■ 白紙節約

する、しない

ソフトウェアから送られたページ終了コードとページ終了コードの間に印字するデータがない場合、白紙を排出させるかどうかを設定します。

［する］を設定すると、白紙は排出されません。紙の節約になります。

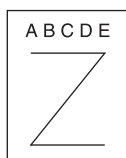
［しない］を設定すると、白紙が排出されます。

■ ページの向き

縦、横

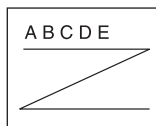
用紙を縦に使うか、横に使うかを設定します。

［縦］に設定すると、用紙カセット内での用紙の向きにかかわらず、用紙を縦に使うで印刷されます。



縦

［横］に設定すると、用紙カセット内での用紙の向きにかかわらず、用紙を横に使うで印刷されます。



横

■ フォント番号

0 ～ 104

本製品のプリンター機能で使用するフォントのタイプフェイスを対応するフォント番号で指定できます。指定できる番号は 0 から 104 です。

■文字サイズ

4.00 ～ **12.00** ～ 999.75 point (0.25 point 単位)

「フォント番号」で選択された番号がプロポーションナルフォントに対応する場合、本設定が PCL 設定メニューに表示されます。標準で使用するフォントの文字サイズを指定することができます。文字サイズは 0.25 point 単位で設定できます。

 **メモ** 本機能は「フォント番号」で 1 から 78 を選択した場合に設定できます。

■文字数

0.44 ～ **10.00** ～ 99.99 cpi (0.01 cpi 単位)

「フォント番号」で選択された番号が固定幅のスケラブルフォントに対応する場合、「文字数」が PCL 設定メニューに表示されます。標準で使用するフォントの文字数を指定できます。文字数は 0.01 cpi 単位で調節できます。cpi は、Characters Per Inch の略で、1 インチあたりの文字数を表します。

 **メモ** 本機能は「フォント番号」で 0 または、79 から 104 を選択した場合に設定できます。

■行数

5 ～ **64** ～ 128 行

1 ページに何行印刷するかを設定できます。5 から 128 行の間で設定します。

■文字コード

ARABIC8, DESKTOP, GREEK8, HEBREW7, HEBREW8, ISO4, ISO6, ISO11, ISO15, ISO17, ISO21, ISO60, ISO69, ISOCYR, ISOGRK, ISOHEB, ISOL1, ISOL2, ISOL5, ISOL6, LEGAL, MATH8, MCTEXT, MSPUBL, PC775, **PC8**, PC850, PC852, PC862, PC864, PC866, PC8DN, PC8GRK, PC8TK, PC1004, PIFONT, PSMATH, PSTEXT, ROMAN8, VNINTL, VNMATH, VNUS, WIN30, WINBALT, WINL1, WINL2, WINL5

ホストコンピューターに最も適した文字コードを選択できます。

■ユーザー定義用紙サイズの設定

する、しない

ユーザー定義用紙サイズを設定できます。[する] を選択すると、ユーザー定義用紙サイズを入力できます。プリンタードライバーから設定されたユーザー定義用紙サイズのみを選択できます。]

 **メモ** プリンタードライバーから設定されたユーザー定義用紙サイズのみを選択できます。

■単位

ミリメートル、インチ

ユーザー定義用紙サイズの指定に使う単位を設定できます。

■幅

139.7 ~ **457.2** ~ 1200mm

ユーザー定義用紙サイズの幅を設定できます。幅は0.1mm単位で139.7mmから1200mmの間で指定できます。端が切れて印刷されてしまう場合に、この機能は有効です。印字する幅を広げることで、切れてしまったテキストも正しく印刷できるようになります。ただし、印刷に使用する用紙の実際の幅以上に、印字する幅を指定することはできません。

■高さ

99.0 ~ **320.0**mm

ユーザー定義用紙サイズの高さを設定できます。高さは0.1mm単位で99.0mmから320mmの間で指定できます。

端が切れて印刷されてしまう場合に、この機能は有効です。印字する高さを広げることで、切れてしまったテキストも正しく印刷できるようになります。ただし、印刷に使用する用紙の実際の高さ以上に、印字する高さを指定することはできません。

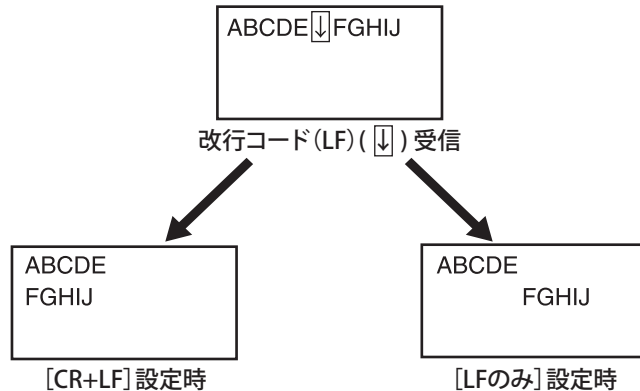
■LF機能

CR+LF、**LFのみ**

改行コード（LF）を受信したときに、復帰コード（CR）を付け足すかを指定できます。

〔CR+LF〕を設定した場合、改行コードを受信すると、印字ヘッドは次の行の先頭に移動します。

〔LFのみ〕を設定した場合、改行コードを受信すると、印字ヘッドは次の行へ垂直に移動して水平方向の位置は変わりません。（次の行の先頭には戻りません。）



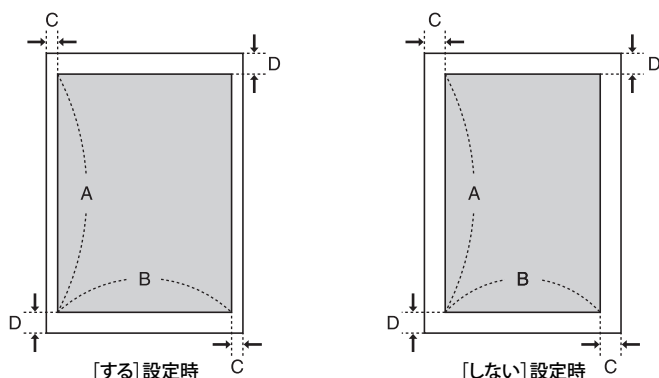
■A4印字領域横幅拡大

する、しない

A4 用紙の横幅の印字可能領域をレター用紙の横幅まで広げるかを設定できます。

[する] を設定した場合、A4 用紙で上下の端から 4.23mm、左右の端から 3.18mm の部分が印刷可能領域になります。横幅の印刷領域のみが広がります。

[しない] を設定した場合、A4 用紙で上下左右の端から 4.23mm の部分が印刷可能領域になります。



印字可能領域

設定	する	しない
A: 長さ	287.87mm	
B: 幅	203.4mm	200.03mm
C: 左右の余白	3.18mm	4.23mm
D: 上下の余白	4.23mm	

- メモ
- この設定はA4用紙にのみ有効です。
 - この設定はページの向きが縦の場合にのみ有効です。

■中間調選択

テキスト： 解像度、階調、誤差拡散
グラフィックス： 解像度、階調、誤差拡散
イメージ： 解像度、階調、誤差拡散

モノクロデータでの中間調の表現方法を設定します。

印刷データは点で表されます。精細な階調や輪郭、陰影はディザパターンによって表現されます。ディザパターンは点の集まりのことです。この表現方法を中間調処理と呼びます。

たとえば、文字や線の輪郭をはっきりとさせるディザパターンを使ったり、画像やグラフの階調を滑らかにするディザパターンを使うことで、最も適した色調を得られます。

[解像度]を選択すると、文字をはっきりとした輪郭で印刷できます。文字や細い線を印刷するのに適しています。

[階調]を選択すると、滑らかな階調と輪郭を両立した印刷ができます。グラデーションを使用したグラフや画像を印刷するのに適しています。

[誤差拡散]を選択すると、[階調]を選択した場合よりも高精細な印刷ができますが、定着させたトナーの安定性は若干劣ります。細かい文字や細い線、(CAD データのような) 輪郭線を印刷するのに適しています。

■RGB入力プロファイル

テキスト：	sRGB 、Gamma 1.5、Gamma 1.8、Gamma 2.4、ダウンロードプロファイル
グラフィックス：	sRGB 、Gamma 1.5、Gamma 1.8、Gamma 2.4、ダウンロードプロファイル
イメージ：	sRGB 、Gamma 1.5、Gamma 1.8、Gamma 2.4、ダウンロードプロファイル

使用中のモニターの特性に適した、RGB プロファイル（RGB（赤青緑）カラーモデルを用いたカラーデータ）を選択できます。RGB カラーモデルで作成されたカラーイメージやカラーグラフィックスを含んだ文書を印刷する際に、本設定が適用されます。

「テキスト」、「グラフィックス」、「イメージ」といったデータの種類ごとに設定することができます。

- [sRGB]
一般的なWindowsコンピューターのモニターの業界標準画質に設定されます。sRGB 対応モニターをお使いの場合、モニター上の色に近い色味で印刷されます。
- [Gamma 1.5]、[Gamma 1.8]、[Gamma 2.4]
RGBデータのガンマ補正の度合いを選択できます。値が大きいほど、暗く印刷されます。
- [ダウンロードプロファイル]
プロファイルは最大100個保存できます。

-  **メモ** • imageWARE Enterprise Management Consoleからもプロファイルをダウンロードできます。
• CMS（マッチング）／ガンマで [CMS] が選択されている場合のみ、本設定は有効です。

■出力プロファイル

テキスト：	Normal 、Photo
グラフィックス：	Normal 、Photo
イメージ：	Normal 、Photo

印刷しようとしているデータに適切なプロファイルを定義することができます。本項目はすべての印刷ジョブのデータに適用されますので、正しいプロファイルが選択されていることを確認してください。

「テキスト」、「グラフィックス」、「イメージ」といったデータの種類ごとに設定することができます。

ほとんどの場合、テキストデータとグラフィックスデータには [Normal] を、イメージデータには [Photo] を選択することをお勧めします。

- [Normal]
モニターに表示された色に近い色味で印刷されます。
- [Photo]
写真のような色味で印刷されます。

-  **メモ** CMS（マッチング）／ガンマで [CMS] が選択されている場合のみ、本設定は有効です。

■マッチング方法

テキスト：	色み優先、 鮮やかさ優先 、色差最小
グラフィックス：	色み優先、 鮮やかさ優先 、色差最小
イメージ：	色み優先 、鮮やかさ優先、色差最小

「RGB 入力プロファイル」が適用される際の印刷方法を設定します。本製品では、以下のようなカラーレンダリングスタイルを選択することができます。

「テキスト」、「グラフィックス」、「イメージ」といったデータの種類ごとに設定することができます。

- [色み優先]
写真やビットマップイメージの印刷に適した色味を提供します。
- [鮮やかさ優先]
プレゼンテーション資料用のアートワークやグラフなどの印刷に適した色味を提供します。
- [色差最小]
CMS（マッチング）／ガンマで [CMS] が選択されている場合のみ、本設定は有効です。

- メモ**
- 「解像度」が「スーパーファイン（1200dpi）」に設定されている場合は、本機能は使用できません。
 - 「出力プロファイル」を「Normal」に設定し、「マッチング方法」を「色み優先」に設定すると、プリンタードライバーでマッチング方法を「モニタ色にあわせる」に設定したのと同様の設定になります。
 - 「出力プロファイル」を「Photo」に設定し、「マッチング方法」を「色み優先」に設定すると、プリンタードライバーでマッチング方法を「写真調」に設定したのと同様の設定になります。
 - 「出力プロファイル」を「Photo」に設定し、「マッチング方法」を「鮮やかさ優先」に設定すると、プリンタードライバーでマッチング方法を「VIVIDフォト」に設定したのと同様の設定になります。

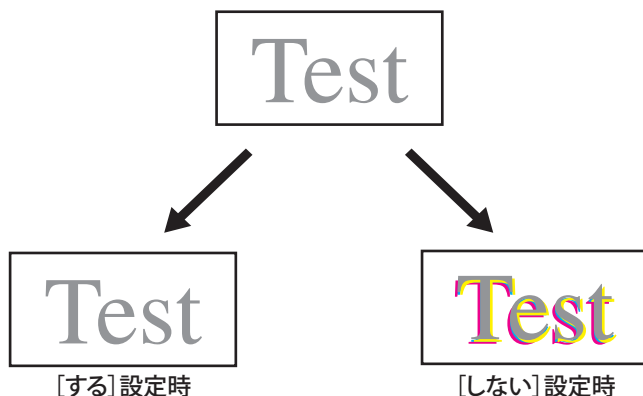
■グレー補償

テキスト：	する、しない
グラフィックス：	する、しない
イメージ：	する、しない

黒色（K）トナーのみを使うかの指定を、「テキスト」、「グラフィックス」、「イメージ」といったデータの種別ごとに設定できます。

「する」を選択した場合、黒色と灰色のデータは黒色（K）トナーのみを使って印刷され、トナー色の混合が軽減されます。

「しない」を選択した場合、黒色と灰色のデータも4色（CMYK）すべてを使って印刷されます。暗い部分のグラデーションの再現性は「する」の場合より向上します。



■CMS（マッチング）選択

プリンター、ホスト

プリンター側とホスト側（プリンタードライバー）のどちらで色処理を行うかを設定します。

「プリンター」に設定すると、プリンター側で色処理が行われます。

「ホスト」に設定すると、プリンター側では色処理が行われません。

■CMS（マッチング）／ガンマ

テキスト： **ガンマ**、CMS
グラフィックス： **ガンマ**、CMS
イメージ： **ガンマ**、CMS

カラーマッチングを行うか、ガンマ値を用いてカラー補正を行うかを、「テキスト」、「グラフィックス」、「イメージ」といったデータの種類ごとに設定できます。

本項目の設定を変更すると、以下の設定項目の有効／無効が切り替わります。

○：有効
×：無効

	[ガンマ]	[CMS]
「RGB 入力プロファイル」	×	○
「マッチング方法」	×	○
「出力プロファイル」	×	○
「ガンマ補正」	○	×

■ガンマ補正

テキスト： 1.0、**1.4**、1.8、2.2
グラフィックス： 1.0、**1.4**、1.8、2.2
イメージ： 1.0、**1.4**、1.8、2.2

原稿中の最も明るい部分や最も暗い部分を損なわないように、印刷結果の明るさを調節することができます。印刷した結果がオリジナル画像（スキャナで読み込む前の写真やモニター上で作成されたグラフィックスなど）に比べて明るいときや、明るさを変えて出力したいときなどに設定します。設定値が大きいほど暗く印刷されます。[1.4] が補正なしの状態です。

「テキスト」、「グラフィックス」、「イメージ」といったデータの種類ごとに設定することができます。

 **メモ** CMS（マッチング）／ガンマで [CMS] が選択されている場合のみ、本設定は有効です。

■アドバンスドスムージング

アドバンスドスムージング： しない、**スムーズ 1**、スムーズ 2
グラフィックスに適用： する、**しない**
テキストに適用： **する**、しない

グラフィックス（アプリケーションソフトで作成されたイラスト）や文字の輪郭を滑らかにプリントするか設定できます。

[スムーズ 1] よりも [スムーズ 2] の方がより滑らかになるようなスムージング処理を行います。まず、[スムーズ 1] に設定し、それでもデータが滑らかにならない場合は、[スムーズ 2] に設定してください。

「グラフィックスに適用」と「テキストに適用」の [する] ／ [しない] を切り替えることで、スムージング処理を行う対象を選択することもできます。

 **重要** • 本項目はグラフィックスデータとテキストデータに対するスムージング処理の設定を行います。イメージデータは設定できません。
• 「解像度」の設定が [スーパーファイン（1200dpi）] に設定されている場合、本項目の「テキストに適用」の設定は無効になります。

 **メモ** • 「グラフィックスに適用」と「テキストに適用」は、「アドバンスドスムージング」が [スムーズ1] または [スムーズ2] に設定されている場合にのみ表示されます。
• プリンタードライバーで「アドバンスドスムージング」を [パネル優先] に設定している場合にのみ、タッチパネルの「グラフィックスに適用」と「テキストに適用」の設定が適用されます。
• アドバンスドスムージングの効果は、文字やグラフィックスのパターンによって異なります。

プリンタードライバーからのジョブ制限を詳細に指定できるようになりました

プリンタードライバーからのジョブを受け付けるかどうかの設定をします。

 **メモ** 本機能の設定をする場合は、管理者としてログインする必要があります。管理者の種類については、e-マニュアル > セキュリティを参照してください。

1  (設定／登録) → [ファンクション設定] → [プリンター] → [プリンタージョブの制限] を押します。

2 [ON] または [OFF] を選択したあと、[OK] を押します。

選択する項目

[ON] : プリンタードライバーからのジョブを制限します。

[OFF] : プリンタードライバーからのジョブを制限しません。

● [ON] を選択した場合 :

☐ [プリント保留] または [プリント保留＋セキュアプリント] を選択したあと、[OK] を押します。

< 許可するジョブの選択 >

[プリント保留] : ボックスへの保存、合成のフォーム登録を許可します。

[プリント保留＋セキュアプリント] : ボックスへの保存、合成のフォーム登録、セキュアプリントを許可します。

● [OFF] を選択した場合 :

☐ [OK] を押します。

メールアドレスの入力を補完できるようになりました (メールアドレスの入力補完)

E メールアドレスを新規に入力するときに、本製品のアドレス帳に登録されている E メールアドレスから前方一致するアドレスを表示します。

 **メモ** • あらかじめ本製品のアドレス帳に E メールアドレスを登録しておく必要があります。
• アクセス番号で制限されている E メールアドレスは表示されません。

1  (設定／登録) → [ファンクション設定] → [送信] → [E メール / ファクス設定] → [メールアドレスの入力補完] を押します。

2 [ON] または [OFF] を選択したあと、[OK] を押します。

選択する項目

[ON] : E メールアドレスを新規に入力するときに、本製品のアドレス帳に登録されている E メールアドレスから前方一致するアドレスを表示します。

[OFF] : E メールアドレスを新規に入力するときに、本製品のアドレス帳に登録されている E メールアドレスから前方一致するアドレスを表示しません。

認証ユーザー名をファクス送信時に発信人の名称として使用できるようになりました（認証ユーザー名を発信人として使用）

SSO-H による認証でログインしている場合は、発信人の名称リストの「100」にログインユーザー名が表示されます。本設定を「ON」にすると、「100」のログインユーザー名が発信人名称の初期値になります。

 **重要** この機能は、FAX ボードを装着しているリモート FAX 送信キットを有効にしている場合に使用できます。

 **メモ** • SSO-Hによるログインサービスについてはe-マニュアル＞MEAP認証システム設定を参照してください。
• 本設定が「OFF」の場合は「00」のユーザー略称が発信人名称の初期値となります。ユーザー略称の登録については、e-マニュアル＞設定/登録を参照してください。

1 （設定／登録）→ [ファンクション設定] → [送信] → [ファクス設定] → [認証ユーザー名を発信人として使用] を押します。

2 [ON] または [OFF] を選択したあと、[OK] を押します。

ファクスの通信モードを設定できるようになりました【G4】（通信モード）

相手先と通信するとき、G4 モードで通信するか、G3 モードで通信するかを設定できます。

 **重要** この機能は、G4FAX ボードを装着している場合に使用できます。

1 （設定／登録）→ [ファンクション設定] → [送信] → [ファクス設定] → [通信モード] を押します。

2 [G3-G4] または [G3 のみ] を選択したあと、[OK] を押します。

選択する項目：

[G3-G4]： 相手先が ISDN 回線に接続されている G4 ファクスや G3 ファクスの場合は、通信モードを [G3-G4] に設定してください。

[G3 のみ]： 相手先が G3 ファクスであることが明らかな場合や [G3-G4] に設定してエラーが起きたときは、通信モードを [G3 のみ] に設定してください。

相手先の発信元記録をつけてファクスをプリントできるようになりました【G4】（相手先発信元記録（G4））

相手先の発信元端末 ID などを記録紙につけてプリントするかどうかを選択できます。

- 重要**
- この機能は、G4FAXボードを装着している場合に使用できます。
 - 回線を増設した場合、この設定が機能するのは回線1（標準回線）のみです。回線1（標準回線）にてお使いください。

1 （設定／登録）→ [ファンクション設定] → [受信／転送] → [ファクス設定] → [相手発信元記録（G4）] を押します。

2 [つける] または [つけない] を選択します。

● [つける] を選択した場合：

- ☐ 発信元記録位置を選択したあと、[OK] を押します。

選択する項目：

[画像の内側]： 画像の内側に発信元記録をプリントします。

[画像の外側]： 画像の外側に発信元記録をプリントします。

● [つけない] を選択した場合：

- ☐ [OK] を押します。

ボックスのセキュリティーを設定できるようになりました（ボックスのセキュリティー設定）

ボックスに保存されるファイルのセキュリティーを向上させる設定を行います。

ボックスの暗証番号を7桁固定にする

ボックスにファイルを保存するときの暗証番号は1桁から設定できます。本機能を「ON」に設定すると、暗証番号を7桁に固定できます。

- 重要** 本機能を「ON」に設定する前に7桁未満の暗証番号を登録していた場合、その暗証番号をそのまま使用することは可能です。ただし、セキュリティーを維持するために、7桁で登録しなおしてください。

- メモ**
- 本機能を「ON」に設定したときは、システムボックス、ファクスボックスの暗証番号も7桁固定となります。
 - ボックスの暗証番号を設定する方法については、e-マニュアル＞設定/登録を参照してください。
 - システムボックス、ファクスボックスの暗証番号を設定する方法については、e-マニュアル＞設定/登録を参照してください。

1 （設定／登録）→ [ファンクション設定] → [ファイル保存／利用] → [ボックス設定] を押します。

2 [ボックスのセキュリティー設定]→[ボックス暗証番号7桁固定 / アクセス制限]を押します。

3 [ON] または [OFF] を選択したあと、[OK] を押します。

- メモ** 設定変更は、本体の主電源スイッチを入れなおしたあとに有効になります。主電源スイッチを入れなおす方法は、e-マニュアル＞お使いになる前にを参照してください。

プリンタードライバーから保存時のプリント設定の変更を制限する

[ファンクション設定] (設定／登録) の < プリンタードライバーから保存時のプリント > は、プリンタードライバーを使ってファイルをコンピューターからボックスに保存するときに、そのファイルをプリントするかどうか設定する機能です。

本機能を「OFF」に設定すると、< プリンタードライバーから保存時のプリント > の設定を変更できなくなります。

 **メモ** < プリンタードライバーから保存時のプリント > の詳細については、e-マニュアル > 設定／登録をご参照ください。

- 1  (設定／登録) → [ファンクション設定] → [ファイル保存／利用] → [ボックス設定] を押します。
- 2 [ボックスのセキュリティ設定] → [プリンタードライバーから保存時のプリントの表示] を押します。
- 3 [ON] または [OFF] を選択したあと、[OK] を押します。

 **メモ** 設定変更は、本体の主電源スイッチを入れなおしたあとに有効になります。主電源スイッチを入れなおす方法は、e-マニュアル > お使いになる前にを参照してください。

メモリーメディアへのファイル保存／プリントを制限できるようになりました (メモリーメディア設定)

メモリーメディアへのファイルの保存や、メモリーメディアにあるファイルのプリントを制限します。

[プリント機能を使用] を「OFF」に設定している場合の画面例 (保存ファイルの利用)



- 1  (設定／登録) → [ファンクション設定] → [ファイル保存／利用] → [メモリーメディア設定] → [スキャン／プリント機能を使用] を押します。
- 2 [スキャン機能を使用] または [プリント機能を使用] を選択したあと、[ON] または [OFF] を選択します。

宛先表エクスポート時にパスワードを含めるかどうか設定できるようになりました

リモート UI で宛先表をエクスポートするときに、宛先に登録されているパスワードを含めるかどうか設定できます。

- メモ**
- エクスポート対象とするかどうか設定できるのは、以下のパスワードです。
 - ファクス宛先の、Fコード送信のためのパスワード
 - ファイルサーバー宛先（外部公開時のアドバンスドボックスを含む）の認証パスワード
 - 宛先表のエクスポートについては、「宛先表をファイルに保存する（エクスポート）」（→ P.58）を参照してください。

1 (設定／登録) → [宛先設定] → [アドレス帳エクスポートの対象にパスワードを含める] を押します。

2 [ON] または [OFF] を選択したあと、[OK] を押します。

選択する項目

[ON]： エクスポートするファイルにパスワードを含めます。

[OFF]： エクスポートするファイルにパスワードを含めません。

重要 本設定が「OFF」のときは、インポート先で宛先にパスワードを登録しなおす必要があります。

SSL 暗号化通信に必要な鍵ペアを生成する際に、署名アルゴリズムと鍵のアルゴリズムを選択できるようになりました

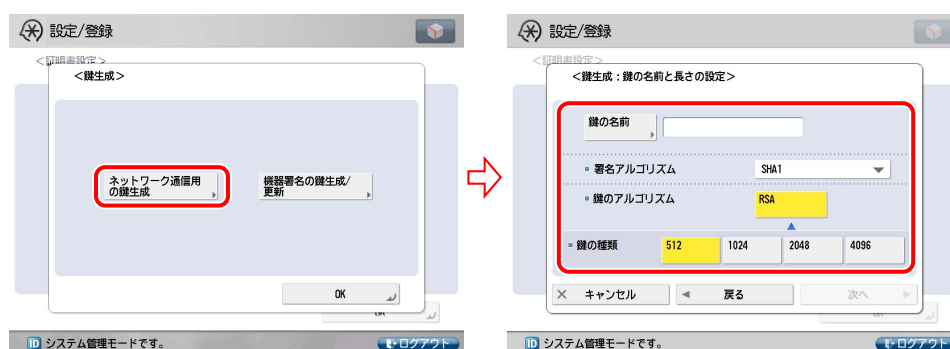
鍵ペアの生成方法は以下のとおりです。

1 (設定／登録) → [管理設定] → [デバイス管理] を押します。

2 [証明書設定] → [鍵生成] を押します。

3 [ネットワーク通信用の鍵生成] を押す→次の項目を設定します。

[ネットワーク通信用の鍵生成]と[機器署名の鍵生成 / 更新]が表示されるのは、機器署名を有効にしているときです。



選択する項目

- [鍵の名前] : 鍵ペアの名前を入力します。
- < 署名アルゴリズム > : 署名に利用するハッシュ関数を選択します。(SHA1、SHA256、SHA384、SHA512)
SHA384 と SHA512 のハッシュ関数をサポートしているのは、1024 ビット以上の長さの鍵です。[SHA384] または [SHA512] を設定する場合は、< 鍵の種類 > で [1024]、[2048]、または [4096] を選択してください。
- < 鍵のアルゴリズム > : RSA (Rivest Shamir Adleman)
- < 鍵の種類 > : 鍵の長さを選択します。(512、1024、2048、4096)

 **重要** 鍵ペアの名前は、半角 24 文字以内で設定してください。全角文字は入力しないでください。

 **メモ** 鍵ペアの名前に、「Device Signature Key」(機器署名用鍵ペアの名前)、および「AMS」(アクセス制限用鍵ペアの名前)を設定することはできません。

監査ログの取得を設定できるようになりました (監査ログを取得)

本機能を「ON」に設定すると、以下のログを生成できます。生成したログは、リモート UI を使用して管理 (エクスポート / クリア) できます。

- ボックス文書操作ログ
- ボックス認証ログ
- ネットワーク接続ログ
- 本体管理ログ

 **メモ** 監査ログの管理機能の詳細については、P.53 を参照してください。

- 1  (設定 / 登録) → [管理設定] → [デバイス管理] → [監査ログを取得] を押します。
- 2 [ON] または [OFF] を選択したあと、[OK] を押します。

 **メモ** 設定変更は、本体の主電源スイッチを入れなおしたあとに有効になります。主電源スイッチを入れなおす方法は、e-マニュアル > お使いになる前にを参照してください。

FIPS 140-2 に準拠した暗号方式を使用できるようになりました（暗号方式を FIPS 140-2 準拠にする）

本機能を「ON」に設定すると、以下で使用されている暗号化方式を米国政府の FIPS 140-2 に準拠させることができます。

- [環境設定]（設定／登録）の [IPSec設定]（→e-マニュアル＞ネットワーク）

[暗号方式を FIPS 140-2 準拠にする]を「ON」に設定した場合、IPSec 通信の認証／暗号化アルゴリズムに「AES-GCM」を使用しているポリシーが無効（OFF）になります。同時に、このポリシーの認証アルゴリズムは SHA1 へ、暗号アルゴリズムは 3DES-CBC へ自動的に変更されます。

また、署名アルゴリズムに「RSA-MD5」、「RSA-MD2」を使用する証明書が設定されているポリシーも無効（OFF）になります。



- 本機能は、IPSecセキュリティボードを有効にしているときにのみ使用できます。（→e-マニュアル＞オプションについて）
- 使用している証明書の署名アルゴリズムを確認する方法については、e-マニュアル＞セキュリティを参照してください。

1 （設定／登録）→ [管理設定] → [デバイス管理] → [暗号方式を FIPS 140-2 準拠にする] を押します。

2 [ON] または [OFF] を選択したあと、[OK] を押します。



- 設定変更は、本体の主電源スイッチを入れなおしたあとに有効になります。主電源スイッチを入れなおす方法は、e-マニュアル＞お使いになる前にを参照してください。

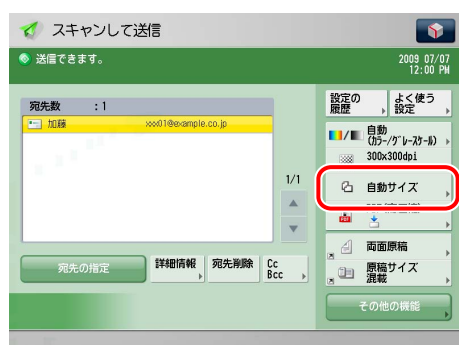
スキャン機能に関する変更（[ファクス]、[スキャンして送信]、[スキャンして保存]）

[ファクス]、[スキャンして送信]、[スキャンして保存] でフリーサイズを選択してスキャンできるようになりました

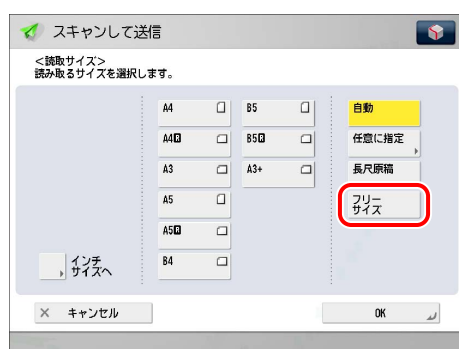
[フリーサイズ] を使うと、不定形サイズの原稿を両面読取でスキャンできます。ここでは [スキャンして送信] の画面を例に説明します。

- 重要**
- [フリーサイズ] は、原稿がA3より小さい場合に使ってください。
 - A3よりも長い原稿を読み込む場合は [長尺原稿] を使ってください。ただし両面読取はできません。
 - [フリーサイズ] を選択する場合は、原稿をフィーダーにセットしてください。原稿台ガラスにセットしても読み込むことはできません。
 - [スキャンして保存] では、アドバンスドボックス/ネットワーク/メモリーメディアへ保存するときに、[フリーサイズ] を選択できます。

1 原稿をセットして宛先を指定したあと、読取サイズボタンを押します。



2 [フリーサイズ] を押します。



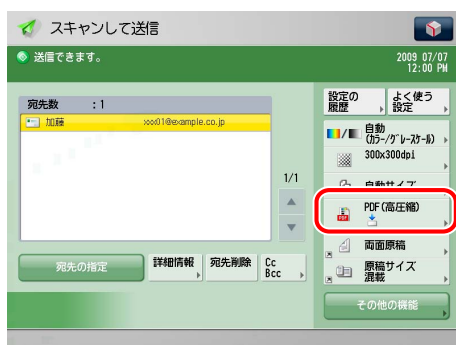
3 [OK] を押します。

[スキャンして送信]、[スキャンして保存] で Rights Management サーバーのポリシー適用 PDF を生成できるようになりました

Adobe LiveCycle Rights Management サーバーに設定されているセキュリティーポリシーによって閲覧権限などが管理された PDF を生成できます。ここでは [スキャンして送信] の画面を例に説明します。

-  **メモ**
- [ポリシーを適用する] を使用するには、Adobe LiveCycle Rights Management ESまたはAdobe LiveCycle Rights Management ES2が必要です。詳しくはお求めになった販売店にお問い合わせください。
 - [ポリシーを適用する] を使用するには、以下の条件が必要です。
 - Adobe LiveCycle Rights Managementサーバーと本製品がイントラネットやインターネットで接続されている
 - [Rights Managementサーバー設定] でAdobe LiveCycle Rights ManagementサーバーのURLが設定されている (→Rights Managementサーバーを設定できるようになりました (Rights Managementサーバー設定) : P.16)
 - [ポリシーを適用する] は、以下の機能と同時に設定できません。
 - 暗号化する
 - タイムスタンプ
 - PDFをPDF/A準拠にする

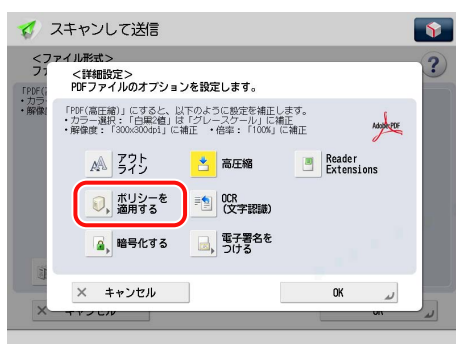
1 原稿をセットして宛先を指定したあと、ファイル形式ボタンを押します。



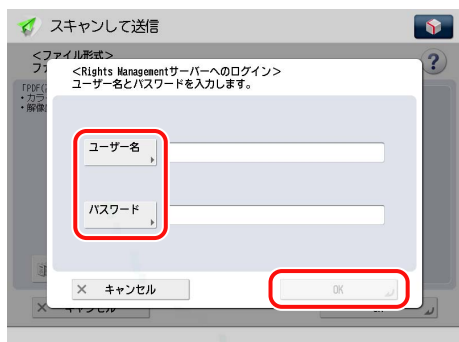
2 [PDF] を選択したあと、[詳細設定] を押します。

[詳細設定] が表示されていない場合は、<ファイル形式>の画面で [ポリシーを適用する] を押します。

3 [ポリシーを適用する] を押します。



4 Adobe LiveCycle Rights Management サーバーにログインするためのユーザー名とパスワードを入力したあと、[OK] を押します。



重要

ログイン画面は、[Rights Management サーバー設定] の設定内容によって異なります。

- [Rights Managementサーバー設定] でユーザー名とパスワードを入力して、ユーザー毎パスワードを使用を「OFF」に設定している場合、ログイン画面は [Rights Managementサーバー設定] で設定したユーザー名とパスワードが自動入力された状態で表示されます。
- [Rights Managementサーバー設定] でユーザー毎パスワードを使用を「ON」に設定している場合、ログイン画面でユーザーごとにユーザー名とパスワードの入力が必要です。なお、SSO-Hなどのログインサービスを使用している場合は、[パスワードを保存] を「ON」に設定するとユーザー名とパスワードが保存され、保存したユーザーが次回ログインすると自動入力された状態で表示されます。

5 適用するポリシーをリストから選択したあと、[OK] を押します。

ポリシーリストには、Adobe LiveCycle Rights Management サーバーに登録されているポリシーが表示されます。

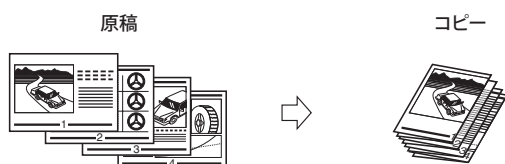
重要

- 表示可能なポリシー数は64件までです。
- 本機では、AES128bitで暗号化されたポリシーのみ適用できます。

プリント機能に関する変更（[コピー]、[保存ファイルの利用]、[セキュアプリント]、状況確認 / 中止）

[コピー]、[保存ファイルの利用] で中綴じフィニッシャー・C1 装着時にサドル折りを設定してプリントできるようになりました

サドル折りは、用紙を2つ折りして出力する機能です。



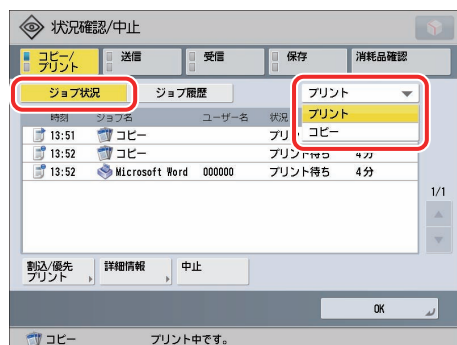
- 重要**
- サドル折りは中綴じフィニッシャー・C1のみの機能です。
 - 用紙は1枚ごとにサドル折りされて排紙されます。
 - 第2原図、OHPフィルム、パンチ済み紙、インデックス紙、ラベル用紙、はがき、封筒はサドル折りできません。
 - サドル折りを設定する場合は、同時に両面コピーを設定する必要があります。

メモ サドル折りできる用紙サイズは、305 × 457 mm、A3、B4、A4R です。

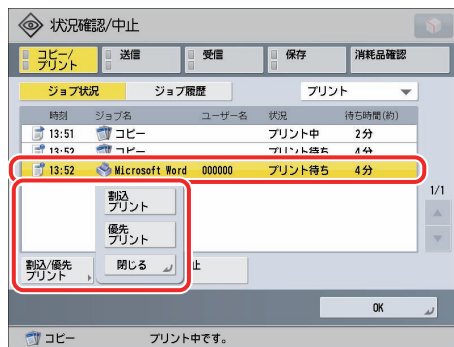
[セキュアプリント] と状況確認 / 中止画面で、割込 / 優先プリントできるようになりました（割込 / 優先プリント）

実行中のジョブを中断して、選択したジョブを優先的にプリントできます。ここでは、状況確認 / 中止画面での操作を説明します。

- 1 （状況確認 / 中止） → [コピー / プリント] を押します。
- 2 [ジョブ状況] を押したあと、ドロップダウンリストで表示させたいジョブの種類を選択します。



3 ジョブを選択して、[割込 / 優先プリント] を押します。



実行中のジョブを中断して、選択したジョブを優先的にプリントする場合は、[割込プリント] を押してください。

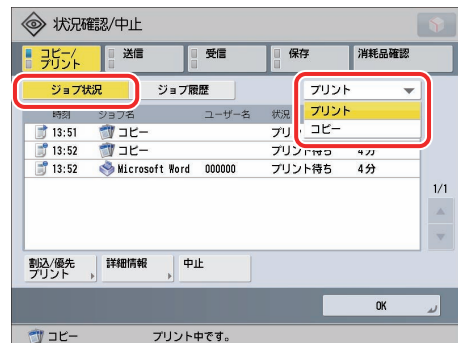
選択したジョブを実行中のジョブの次に優先的にプリントする場合は、[優先プリント] を押してください。

- 重要**
- 割り込みプリント中のジョブを、別のジョブが追い越して割り込むことはできません。追い越して割り込もうとした場合、そのジョブは割り込み中のジョブが終了したあとに実行されます。
 - 割込プリント待機中のジョブを選択して、割込プリントや優先プリントを行うことはできません。
 - 別のジョブにより割り込まれたジョブ、用紙なしジョブ、トナーなしジョブなど、一度実行中になってから中断したジョブは、ジョブが再開した場合、そのジョブに対して割り込みを行うことはできません。割込プリントを実行した場合でも、その操作は無視されます。
 - ファクス受信プリントに対して別のファクス受信プリントの割り込みを行うことはできません。
 - 複数枚のコピー／プリントジョブに対して割込プリントを行った場合、残りのプリント枚数を中断して割り込みます。ただし、以下の仕上げ機能を使用している場合は、プリントが部数単位で終了してから割り込みます。
 - ホチキス
 - 製本
 - サドル折り

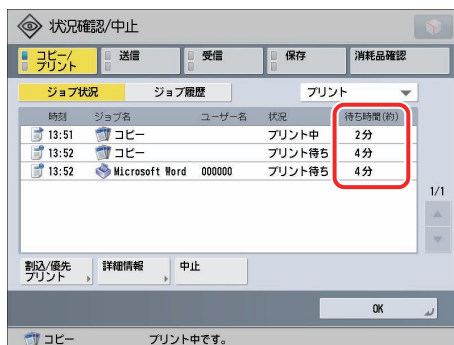
ジョブ状況画面にプリント待ち時間が表示されるようになりました

コピー／プリントジョブのジョブ状況画面に、プリントが終了するまでの予測時間が表示されます。画面を表示する手順は以下のとおりです。

- 1 (状況確認／中止) → [コピー / プリント] を押します。
- 2 [ジョブ状況] を押したあと、ドロップダウンリストで表示させたいジョブの種類を選択します。

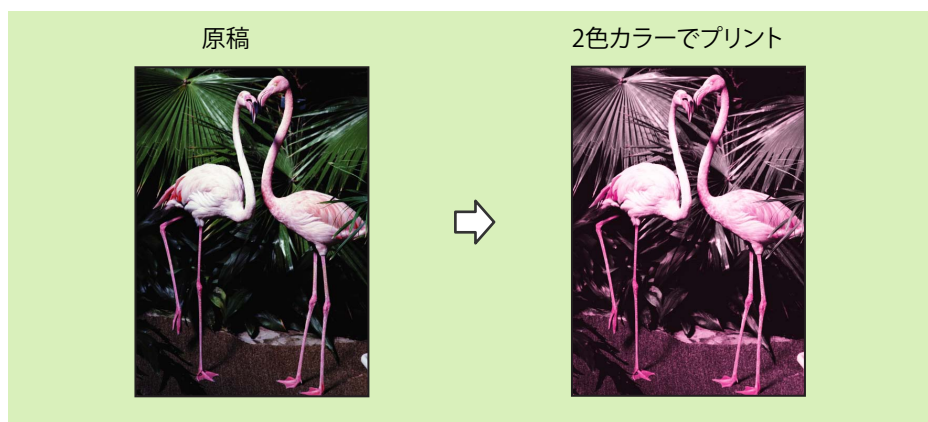


プリントが終了するまでの予測時間が表示されます。



プリンタードライバーから2色カラーでプリントできるようになりました

プリンタードライバーの「色数の設定」ダイアログボックスで「2色カラー」を選択すると、黒と指定した1色でプリントします。ここではWindowsでの操作を説明します。

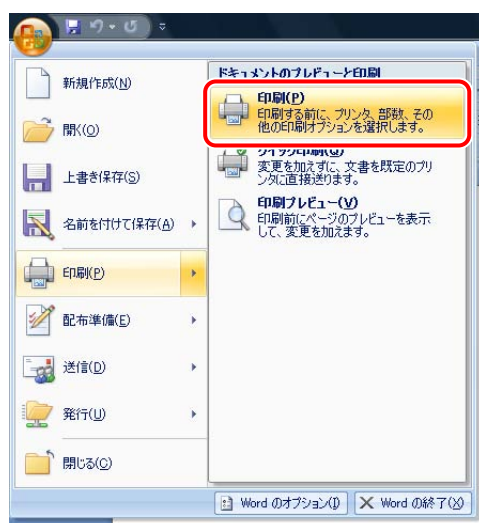


重要 この機能をお使いになるには、以下のプリンタードライバーが必要です。

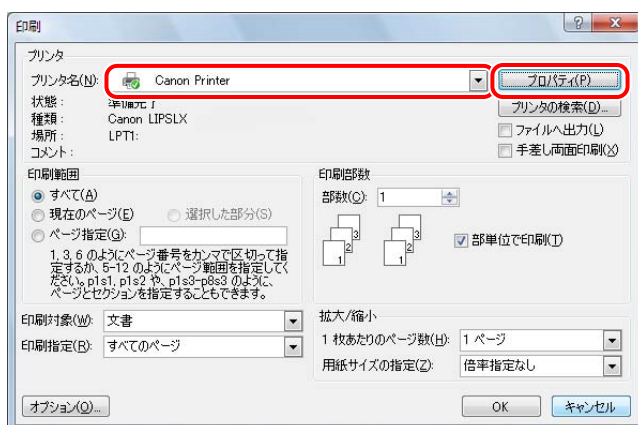
- Windows : LIPS LXプリンタードライバー Version 20.40以降
- Macintosh : LIPS LX プリンタードライバー Version 2.20以降

メモ Macintosh での操作については、プリンタードライバーに付属のヘルプを参照してください。

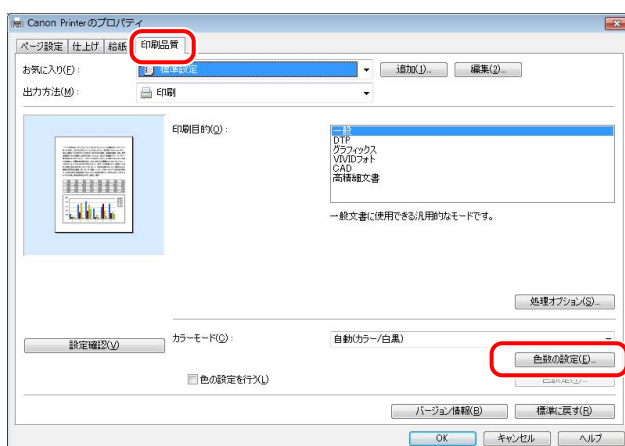
1 アプリケーションソフトウェアのメニューから「印刷」を選択します。



2 お使いのプリンターを選択したあと、[詳細設定]（または [プロパティ]）をクリックします。

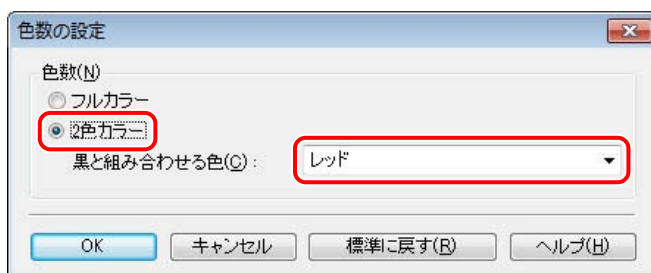


3 [印刷品質] タブをクリックし、[色数の設定] をクリックします。



メモ [色数の設定] が表示されないときは、[コントロールパネル] からプリンターのプロパティ画面を表示したあと、[デバイスの設定] タブをクリックし、[デバイス機能] をクリックしたあと [デバイス機能の設定] ダイアログボックスで [機能バージョン] を [2.0 以上] に設定します。

4 [2 色カラー] を選択し、[黒と組み合わせる色] から色を選択します。



5 [OK] をクリックします。

[ウェブブラウザ] で Web ページのプリントが非対応になりました

[ウェブブラウザ] でタッチパネルディスプレイに表示中のウェブページをプリントできなくなりました。

- **メモ** • タッチパネルディスプレイにウェブページを表示するには、ウェブブラウザ拡張キットが有効になっている必要があります。
- PDFファイルを表示してプリントすることは可能です。

PCL プリンタードライバーに対応してプリントできるようになりました

PCL プリンタードライバーは、一般的なビジネス用アプリケーションとともに使用できます。PCL5c プリンタードライバー（カラープリンター用）、および PCL6 プリンタードライバー（カラー／モノクロプリンター用）があります。PCL6 ドライバーは、PCL5c ドライバーより、印刷品質および印刷速度の点で優れています。PCL プリンタードライバーは、Windows 英語版にのみ対応しています。ドライバー画面は英語で表記されています。また、Macintosh には対応していません。



- **重要** この機能は、PCL エミュレーション拡張キットを有効にしている場合に使用できます。
- **メモ** PCL プリンタードライバーをインストールする場合、メニュー画面およびインストール画面は英語で表記されています。インストール手順は、「Printer Driver Installation Guide」（英語版）を参照してください。

アドバンスドボックスに関する変更

アドバンスドボックス管理者がコンピューターからアクセスしたときの操作権限が拡がりました

アドバンスドボックスが SMB または WebDAV サーバーとして外部公開されている場合、アドバンスドボックスの管理者はコンピューターのエクスプローラから以下の操作が可能です。

- 一般ユーザーが作成した [個人スペース] へアクセスして、フォルダー／ファイルの編集
- ファンクション設定（設定／登録）→ [ファイル保存/利用] → [アドバンスドボックス設定] → [外部からの書込禁止] を「ON」に設定している場合のフォルダー／ファイルの編集

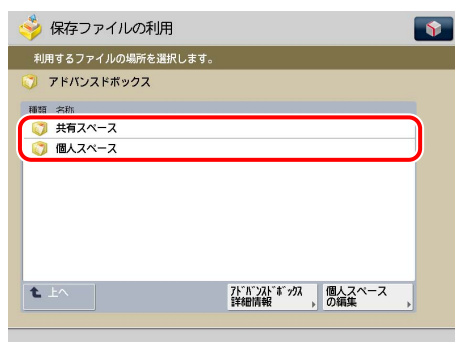
 **メモ** アドバンスドボックスを使用するユーザーの登録や外部公開設定については、e-マニュアル>セキュリティを参照してください。

アドバンスドボックス内のファイルが画像表示できるようになりました

ボックスに保存されているファイルだけでなく、アドバンスドボックス／ネットワーク／メモリーメディアに保存されているファイルの画像をタッチパネルディスプレイに表示できるようになりました。ここでは、アドバンスドボックスを例に説明します。

 **重要** PDF ファイルの画像表示は、PS 拡張キットまたはダイレクトプリント拡張キット（PDF/XPS 用）が必要です。

- 1 メインメニュー画面で [保存ファイルの利用] を押したあと、格納場所の選択画面で [アドバンスドボックス] を押します。
- 2 スペース選択画面で目的のスペースを選択します。



- 3 目的のファイルがある階層を表示します。
- 4 画像を表示するファイルを選択したあと、[画像表示] を押します。



 **メモ** 複数のファイルを選択して「画像表示」を押した場合は、選択されている（色つき）ファイルのみ画像が表示されます。

5 [◀] [▶] を押して確認したいページを選択します。



6 画像を表示するファイルを選択したあと、「画像表示」を押します。

[] [] を押して画像の倍率を変更することができます。

拡大した画像は、[◀] [▶] [▼] [▲] を押して、表示箇所を移動することができます。

 で表示されている画像の位置を確認することができます。

カスタムメニュー機能に関する変更

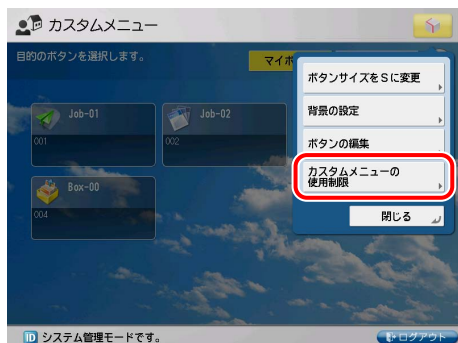
[カスタムメニュー]でマイボタンの使用を制限できるようになりました(マイボタンの使用)

- メモ**
- カスタムメニューの使用制限の設定は、システム管理者、またはSSO-Hのシステムアドミニストレータ(Administrator)/ネットワークアドミニストレータ(NetworkAdmin)/デバイスアドミニストレータ(DeviceAdmin)が行えます。管理者の種類については、e-マニュアル>セキュリティを参照してください。
 - 認証機能を使用していない場合は、マイボタンは表示されません。

1 カスタムメニューで、を押します。

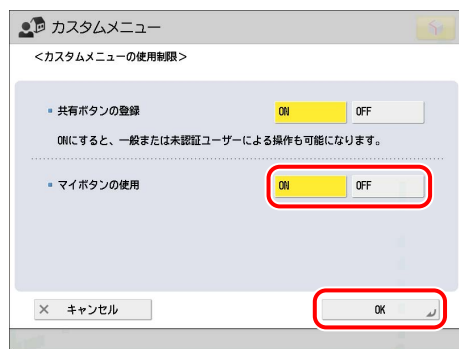


2 [カスタムメニューの使用制限]を押します。



- メモ**
- システム管理者情報のみ設定して、認証機能を使用していない場合は、[カスタムメニューの使用制限]を押したあとに、ログイン画面が表示されます。システム管理部門IDとシステム管理暗証番号を入力してください。工場出荷時の初期値は、それぞれ「7654321」に設定されています。(→e-マニュアル>セキュリティ)

3 [マイボタンの使用] を押したあと、[OK] を押します。



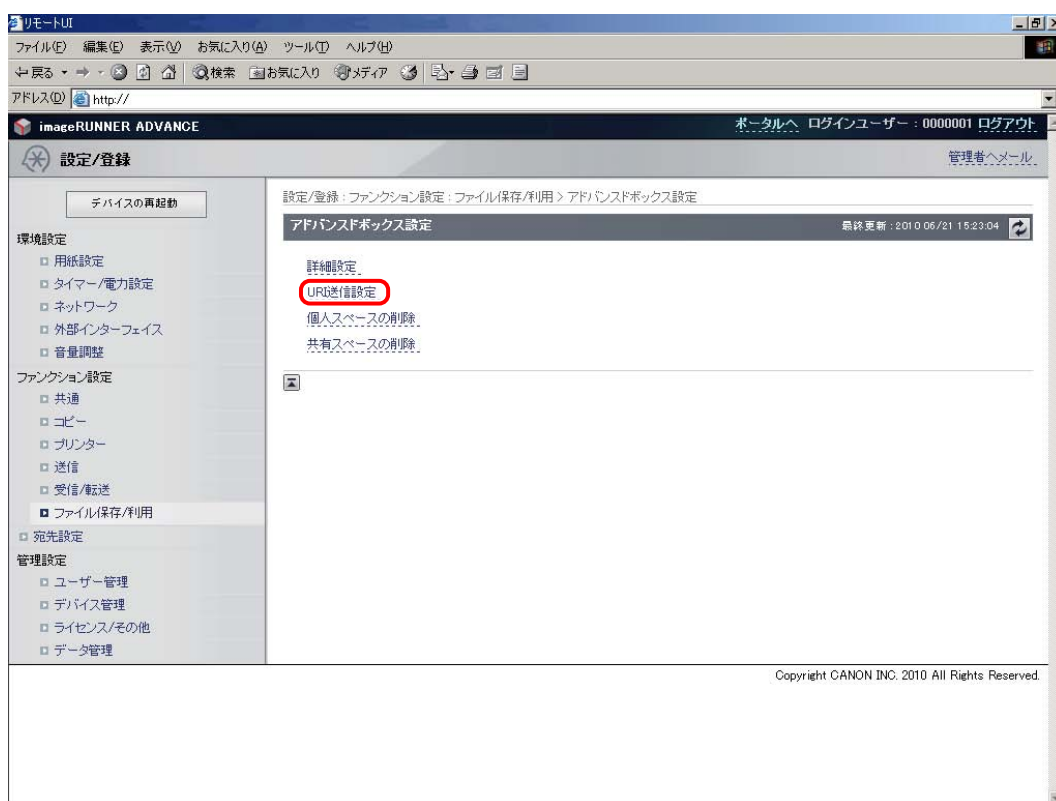
[マイボタンの使用]:マイボタンの使用を設定します。「ON」に設定した場合は、マイボタンを使用できます。「OFF」に設定した場合は、マイボタンを使用できません。

リモート UI 機能に関する変更

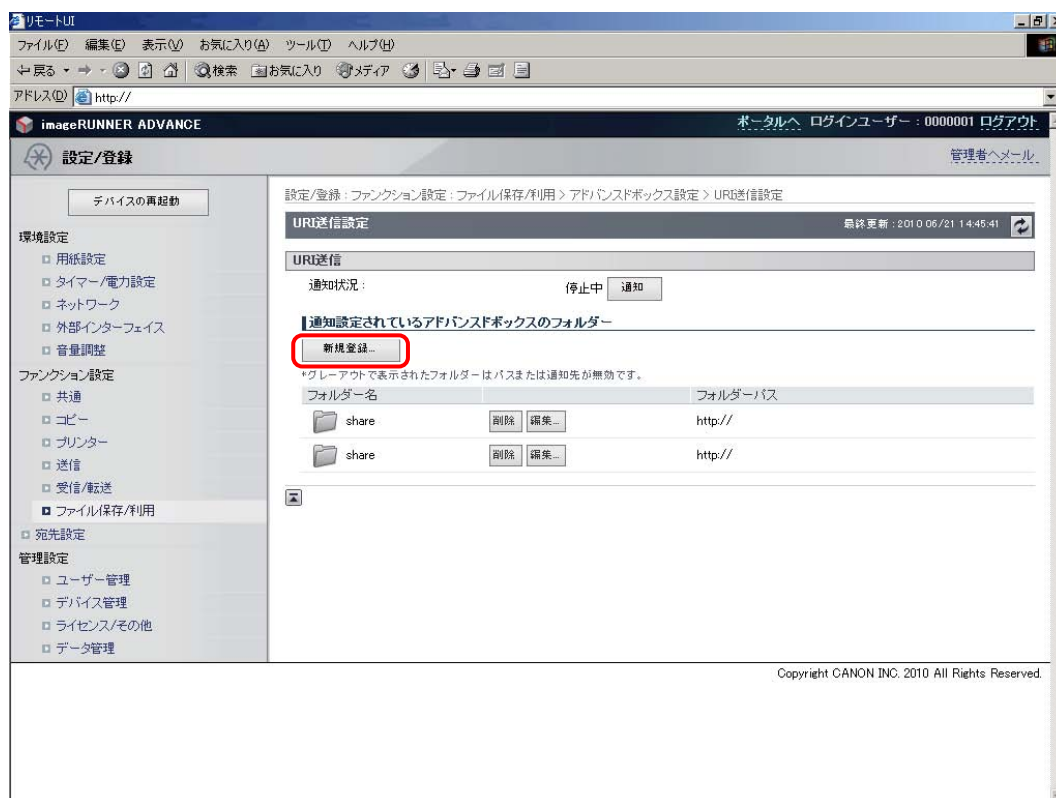
URI 送信を設定できるようになりました（URI 送信設定）

URI 送信設定では、本機のアドバンスドボックス内にファイルが保存されたときに、E メールを送信して通知する設定ができます。E メールにはファイル名を含めたフォルダーへのパス（URI:Uniform Resource Identifier）が記載されます。

- 1 [設定 / 登録] をクリックして、ファンクション設定に表示されるメニューから [ファイルの保存 / 利用] を選択したあと、[アドバンスドボックス設定] をクリックします。
- 2 [URI 送信設定] をクリックします。



3 [新規登録] をクリックします。



4 通知対象となるフォルダーへのパスを入力します。

● アドバンスドボックスをSMBサーバーとして公開している場合：

- 本機のホスト名またはIPアドレスに「¥share」または「¥users」をつけ、その次に「¥フォルダー名」を入力します。

入力例：

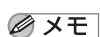
- ¥192.168.1.21¥share¥documents （共有スペースの直下にある「documents」というフォルダーを指定する場合）
- ¥192.168.1.21¥users¥suzuki （個人スペースの直下にある「suzuki」というフォルダーを指定する場合）

● アドバンスドボックスをWebDAVサーバーとして公開している場合：

- 「http(s)://<本機のIPアドレスまたはホスト名>/<shareまたはusers>/<フォルダ名>」の形式で入力します。

入力例：

- http://192.168.1.21/share/documents （SSL無効時で、共有スペースの直下にある「documents」というフォルダーを指定する場合）
- https://192.168.1.21/users/suzuki （SSL有効時で、個人スペースの直下にある「suzuki」というフォルダーを指定する場合）



本機に imagePASS が装着されている場合は、ポート番号（SSL 無効時：18080、SSL 有効時：18443）を指定する必要があります。

入力例：

- http://192.168.1.21:18080/share/documents （SSL無効時で、共有スペースの直下にある「documents」というフォルダーを指定する場合）

5 指定 E メールアドレスへ通知するタイミングを選択します。

選択する項目

[スキャンして保存で保存先として指定したとき]：

タッチパネルディスプレイの [スキャンして保存] から、アドバンスドボックス内の指定フォルダーへファイルが保存されるごとに通知します。なお、サブフォルダー内にファイルが保存されたときやフォルダーが追加されたときは通知しません。

[送信 / 転送機能でループバックアドレスを指定したとき]：

送信 / 転送機能を使用して、ループバックアドレス（ネットワーク上で自機を表すアドレス）から、アドバンスドボックス内の指定フォルダーへファイルが保存されるごとに通知します。なお、サブフォルダー内にファイルが保存されたときやフォルダーが追加されたときは通知しません。ループバックアドレスでの指定は、[スキャンして送信] や [転送設定] で本機のアドバンスドボックスを宛先にするときに使用します。（→本機のアドバンスドボックスをループバックアドレスで宛先に指定する：P.52）

[フォルダー内の文書とサブフォルダーの合計が 700 個に達したとき]：

手順 4 で通知対象に指定したフォルダー内の、ファイルとサブフォルダーの合計が 700 個に達したときに通知します。サブフォルダー内のファイルとフォルダーは、カウントされません。

[フォルダー内の文書とサブフォルダーの合計が 900 個に達したとき]：

手順 4 で通知対象に指定したフォルダー内の、ファイルとサブフォルダーの合計が 900 個に達したときに通知します。サブフォルダー内のファイルとフォルダーは、カウントされません。

 **メモ** 指定したフォルダー内に保存できるファイルとサブフォルダーの合計は、最大 1000 個です。

6 [宛先の選択] をクリックして通知先の E メールアドレスを指定したあと、[OK] をクリックします。

 **メモ** 通知先に選択できるのは、アドレス帳に登録されている E メールアドレス 1 件、もしくは E メールアドレスグループ 1 件です。

7 Eメールの件名を入力します。

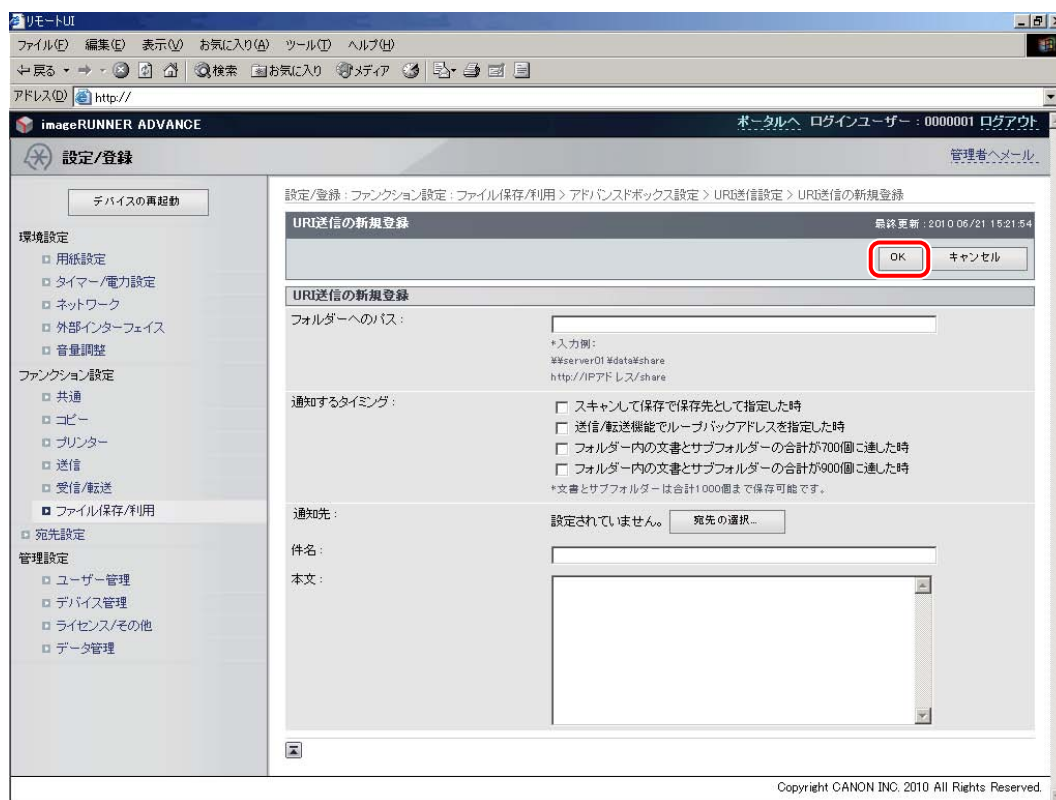
半角 40 文字まで入力できます。

8 Eメールの本文を入力します。

半角 140 文字まで入力できます。

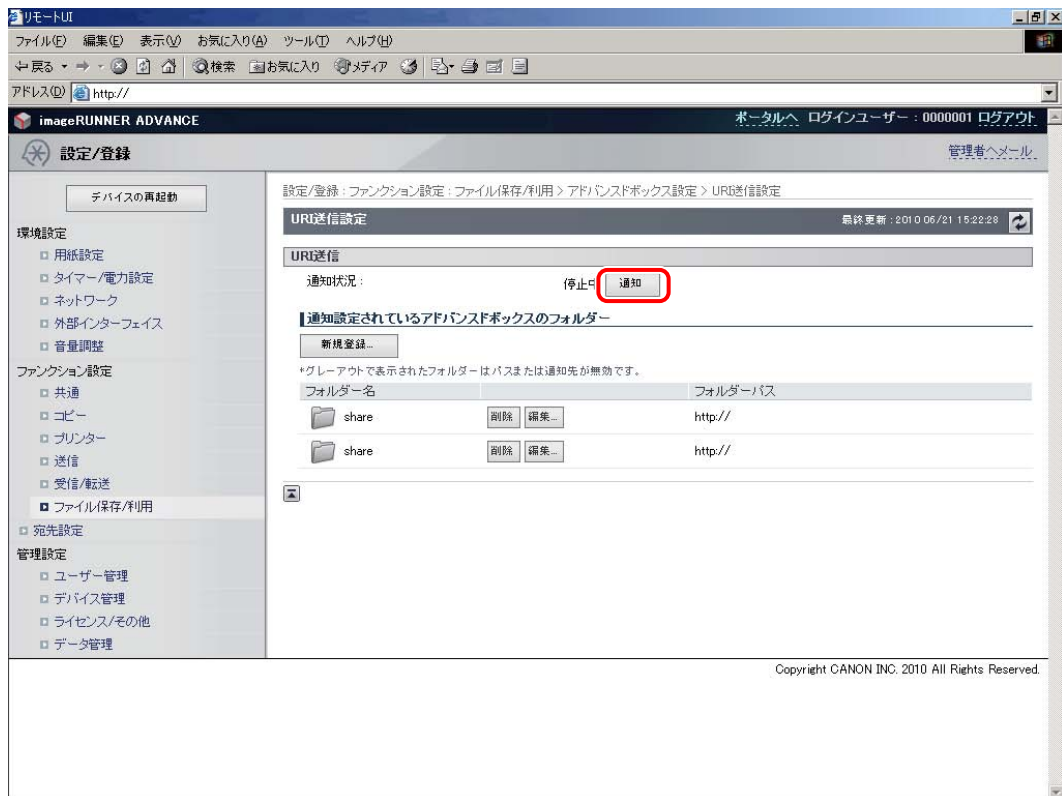
 **メモ** Eメールの本文には、ここを入力した文字列のほかに、手順 4 で指定したフォルダーへのパスとファイル名が記載されます。

9 [OK] をクリックします。



URI 送信設定の登録が終了しました。

10 [通知] をクリックします。



通知状況が「通知中」に変わり、登録されているすべての URI 送信設定が有効になります。

URI 送信の通知を停止したい場合は、「停止」をクリックします。

● 登録済みのURI送信設定を削除する場合：

- 削除したいフォルダーの「削除」をクリックします。

● 登録済みのURI送信設定を編集する場合：

- 編集したいフォルダーの「編集」をクリックします。

本機のアドバンスドボックスをループバックアドレスで宛先に指定する

本機のアドバンスドボックスをループバックアドレスでアドレス帳に登録する際は、[ホスト名] を以下のように入力します。

- **メモ** • アドバンスドボックスをアドレス帳に登録する方法の詳細については、e-マニュアル> スキャンして送信を参照してください。
- ループバックアドレスで指定すると、[ファンクション設定]（設定／登録）の[外部からの書き込み禁止]を「ON」に設定している場合でもアドバンスドボックスに保存できます。（→e-マニュアル> セキュリティ）

■送信プロトコルに [Windows(SMB)] を選択した場合

1 以下のように入力します。

入力例：
共有スペースに保存する場合： \\127.0.0.1\share
個人スペースに保存する場合： \\127.0.0.1\users

- **重要** ループバックアドレスは以下のとおりです。
- IPアドレス（IPv4形式）の場合：
127.0.0.1
- IPアドレス（IPv6形式）の場合：
::1
- ホスト名の場合：
localhost

■送信プロトコルに [WebDAV] を選択した場合

1 以下のように入力します。

入力例：
http:// 127.0.0.1

- **重要** • [ホスト名] は、以下の形式で入力してください。
- SSL無効時：
http://IPアドレスまたはホスト名
- SSL有効時：
https://IPアドレスまたはホスト名
- ループバックアドレスは以下のとおりです。
- IPアドレス（IPv4形式）の場合：
127.0.0.1
- IPアドレス（IPv6形式）の場合：
::1
- ホスト名の場合：
localhost
- 送信先のimageRUNNER ADVANCE機にimagePASSが装着されている場合は、[ホスト名] を以下のように入力してください。
- imagePASSを装着した他機のアドバンスドボックスへ送信する場合：
SSL無効時：http://IPアドレスまたはホスト名:18080
SSL有効時：https://IPアドレスまたはホスト名:18443
- imagePASSを装着した本機のアドバンスドボックスへ本機から送信する場合（ループバックアドレスで指定）：
IPv4形式の場合
SSL無効時：http://127.0.0.1:18080
SSL有効時：https://127.0.0.1:18443
IPv6形式の場合
SSL無効時：http://::1:18080
SSL有効時：https://::1:18443
ホスト名の場合
SSL無効時：http://localhost:18080
SSL有効時：https://localhost:18443

**メモ**

imagePASS を装着した本機のアドバンスドボックスへ本機から送信する場合、[プロキシサーバーの使用] を「ON」に設定しているときは、ループバックアドレスでの指定では送信できない場合があります。その場合は、imagePASS の IP アドレスを入力してください。

監査ログを管理できるようになりました（監査ログのエクスポート / クリア）

**重要**

監査ログ管理機能を使用または使用できなかったことによって発生した損害については、弊社はその責任を追いかねますので、あらかじめご了承ください。

監査ログ管理機能と管理できるログの種類について

本機能を使用すると、本体内に保存されるログをリモート UI で収集／管理できるようになります。管理者は、収集されたログを確認することで、本体がどのように使用されているかを調査できます。

■ ログの種類について

本機能で管理できるのは、次のようなログになります。

- ユーザー認証ログ
 - ユーザー認証の認証状況と、ユーザー情報の登録／変更／削除に関するログです。
 - ログイン／ログアウトのログ
 - ユーザー認証の成功／失敗のログ
 - SSO-Hで管理されているユーザー情報の登録／変更などのログ
 - Access Management Systemのロール管理（追加／設定／削除）のログ
- ジョブログ
 - コピー／ファクス／スキャン／送信／プリントジョブの完了に関するログです。
- ボックス文書操作ログ
 - ボックス／システムボックス／ファクスボックス内のデータの操作に関するログです。
- ボックス認証ログ
 - ボックス／システムボックス／ファクスボックスの認証状況に関するログです。
- ネットワーク接続ログ
 - IPSec通信に失敗したときのログです。
- 本体管理ログ
 - 本体のⓈ（設定／登録）の内、ネットワークやセキュリティに関する設定を変更したときのログです。また、本体の日付／時刻設定の変更も本体管理ログに含まれます。
- 監査ログ管理機能のログ
 - 本機能を使用して行える、ログのエクスポートや削除に関するログです。

**重要**

- 本機能で管理可能なログの件数は、ログの種類にかかわらず2万件までです。ログがいっぱいになった場合は、古いログが順に消去されて、新しいログに上書きされます。
- スリープ時の消費電力が「多い」に設定されている場合、本体がスリープ状態になっているときはログの収集が行われません。

**メモ**

本項目で紹介したログは、ユーザー操作の過程において本体システムでの処理により複数個、収集される場合があります。

ログを管理する

重要 ログを管理する場合は、管理者としてリモート UI にログインしている必要があります。

- メモ**
- 収集したログとエクスポートしたログには、日時、ユーザー名、操作種別、結果（OK/NG）の項目が含まれます。ジョブログには、他にジョブの種類についての項目が含まれます。
 - ネットワーク接続ログ、ボックス認証ログ、ボックス文書操作ログ、本体管理ログを生成する場合は、「監査ログを取得」を「ON」に設定したあと、本体を再起動します。（→e-マニュアル>セキュリティ）

■ログの収集を開始／停止する

ログの収集を開始／停止できます。収集したログは、ひとつの監査ログファイルに保存されます。

- メモ**
- 保存されたログは、収集された日付順に表示されない場合があります。
 - 工場出荷時は、ログの収集は停止の設定になっています。
 - ログの収集の開始または停止を設定すると、次に切り替えるまでは同じ状態が維持されます。本体の再起動では、設定は切り替わりません。
 - ログの収集の開始を設定すると、設定後に生成されたログが収集されます。設定前に生成されたログは収集されません。

- 1** [設定 / 登録] → [デバイス管理] → [監査ログのエクスポート / クリア] → [監査ログ情報] → < 監査ログの収集 > の [開始] をクリックします。



■ログの保存件数と収集／保存日時を確認する

本体から収集したログの保存件数と、収集／保存した日時を確認できます。

- 1 [設定 / 登録] → [デバイス管理] → [監査ログのエクスポート / クリア] → [監査ログ情報] をクリックします。



表示される項目

- [現在のログ保存件数]： 現在保存されているログの件数が表示されます。
- [ログの最終収集日時]： 最後に本体からログを収集した日時が表示されます。
- [ログの最終保存日時]： 最後に本体から収集したログを保存した日時が表示されます。

■収集したログをエクスポートする

本体から収集した各種ログを、一括して CSV 形式でコンピューターに保存できます。

メモ 本体から収集した各種ログをエクスポートする際には、SSL または IPsec をご使用下さい。SSL を使用する場合は、「SSL を使用」を「ON」に設定したあと、本体を再起動します（→ e-マニュアル > リモート UI）。IPsec を使用する場合は、「e-マニュアル > ネットワーク」を参照してください。

エクスポートされるログに記載されているログの種類の番号は、以下のログの種類と対応します。

4098	ユーザー認証ログ
1001/8193	ジョブログ
8197	ボックス文書操作ログ
8199	ボックス認証ログ
8200	ネットワーク接続ログ
8198	本体管理ログ
3001	監査ログ管理機能のログ

1 [設定 / 登録] → [デバイス管理] → [監査ログのエクスポート / クリア] をクリックします。

2 < 監査ログのエクスポート > の [エクスポート] をクリックします。



エクスポートを行ったあと自動的にログを削除する場合は、「エクスポート後にログを本体から削除する」にチェックマークを付けます。

メモ 「エクスポート後にログを本体から削除する」にチェックマークを付けた場合は、「エクスポート」をクリックしたあと、必ず「保存」をクリックしてください。「キャンセル」をクリックすると、ログが保存されないまま削除されます。

3 画面の指示に従って、ファイルの保存場所を指定します。

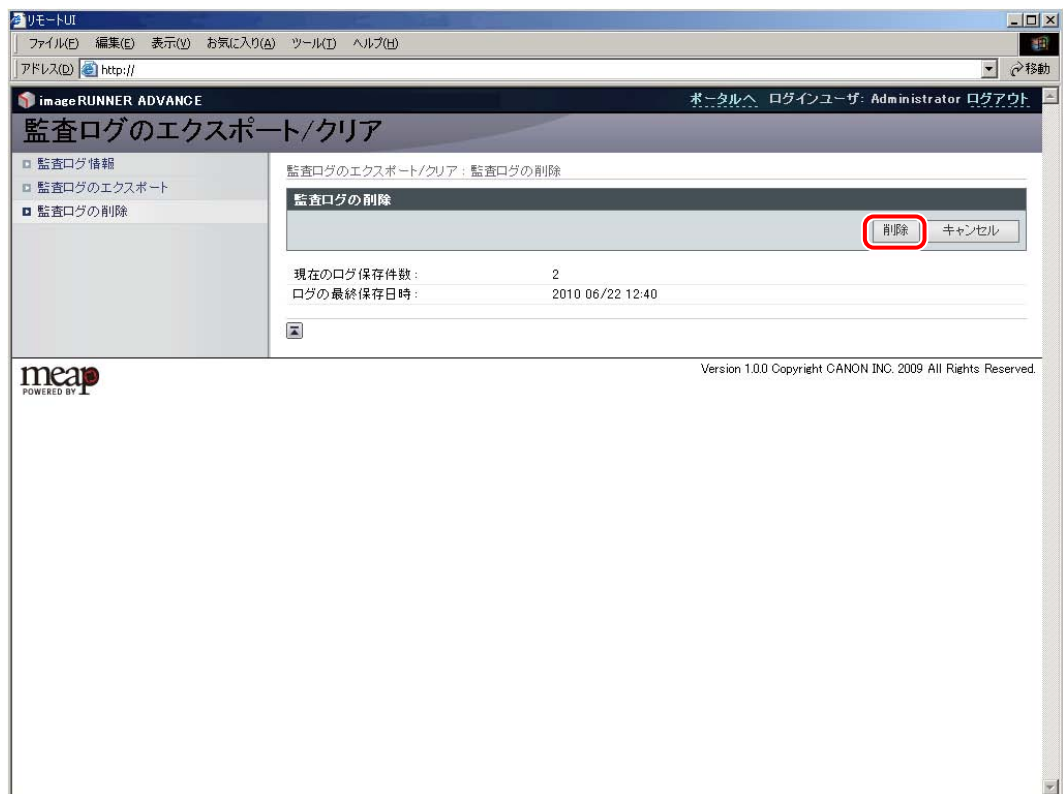
-  **メモ**
- エクスポート実行中は、ログの収集が停止されます。
 - 本体の表示言語の設定がログを収集したときとエクスポートしたときとで異なる場合、ファイルの内容が文字化けすることがあります。

■収集したログを削除する

本体から収集したログを、一括して削除できます。

1 [設定 / 登録] → [デバイス管理] → [監査ログのエクスポート / クリア] をクリックします。

2 < 監査ログの削除 > の [削除] をクリックします。



3 [OK] をクリックします。

■エラーが表示されたときには

本機能で管理されるメモリー領域に何らかのエラーが発生した状態で、ログのエクスポートや削除を実行すると、リモート UI 上に「エラーが発生したため、監査ログの管理領域が壊れた可能性があります。システムの初期化を行います。」というメッセージが表示されます。

1 [OK] をクリックします。

メモリー領域の初期化が実行され、正常な状態に回復されます。

-  **メモ**
- 初期化するとログの収集が停止し、それまでに収集したログはすべて削除されます。再度ログの収集を開始するには、「e-マニュアル > リモート UI」を参照してください。
 - エラーが発生した場合、タッチパネルディスプレイ上に「エラーのため監査ログを取得できません。」というメッ

アドレス帳のエクスポート／インポートにパスワードを含めることができるようになりました

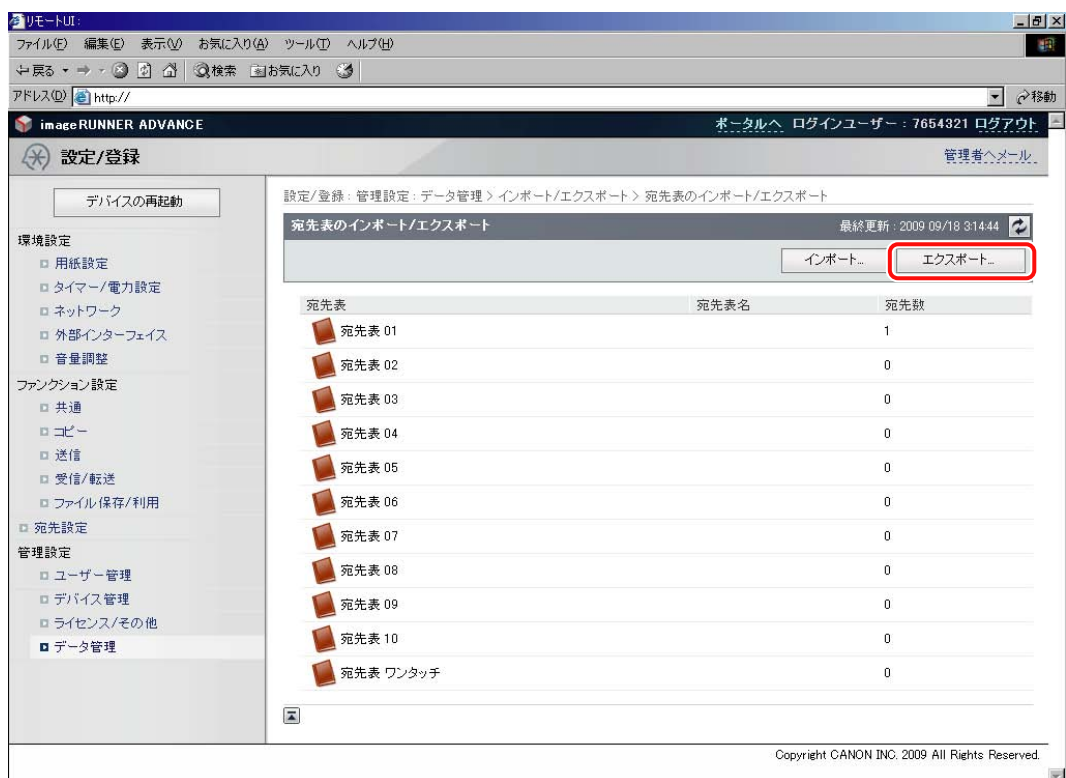
〔宛先表〕と〔デバイス設定（転送設定、アドレス帳、送信のよく使う設定）〕のアドレス帳のパスワード情報を暗号化してエクスポートできます。また、暗号化されたパスワード情報を複合化してインポートできます。ここでは、宛先表のエクスポート／インポート方法について説明します。デバイス設定のアドレス帳もパスワード情報の暗号化／複合化については、同様の手順となります。

メモ 宛先表／アドレス帳のエクスポート／インポート時にパスワード情報を含めるときは、あらかじめ〔宛先設定〕（設定／登録）の〔アドレス帳エクスポートの対象にパスワードを含める〕をONにする必要があります。（→宛先表エクスポート時にパスワードを含めるかどうか設定できるようになりました：P.31）

宛先表をファイルに保存する（エクスポート）

宛先表の情報をファイルとしてコンピューターに保存できます。

- 1 〔設定／登録〕をクリックして、管理設定に表示されるメニューから〔データ管理〕を選択したあと、〔インポート／エクスポート〕→〔宛先表〕→〔エクスポート〕をクリックします。



宛先表に暗証番号が設定されている場合は、暗証番号を入力する画面が表示されます。宛先表の暗証番号を入力したあと、〔OK〕をクリックします。

2 宛先表とファイルの保存形式を選択したあと、[エクスポート開始] をクリックします。

表示される項目

- [宛先表]： ドロップダウンリストから、ファイルに保存する宛先表を選択します。
- [フォーマット]： ファイルの保存形式を選択します。
- ・[専用フォーマット] の場合は、保存したファイルを同じ機種にインポートできます。
 - ・[LDAP フォーマット] の場合は、保存したファイルを他のアプリケーションソフト（Microsoft Internet Explorer、Netscape Navigator、Microsoft Outlook、Eudora など）で利用できます。他のアプリケーションでは、LDAP データとしてインポートしてください。
- [パスワード]： 宛先表の認証情報を暗号化するためのパスワードを入力します。
- [確認入力]： パスワードを再度入力します。異なるパスワードを入力した場合は、エラーのダイアログボックスが表示されます。



- [パスワード] と [確認入力] は、以下の設定を行ったときに表示されます。
[設定/登録] → [宛先設定] → [アドレス帳のエクスポート設定] → [アドレス帳エクスポートの対象にパスワードを含める] にチェックマークを付けたとき
- [LDAPフォーマット] で保存できるのは、Eメールアドレスとファクス番号のみです。宛先表に登録されているすべての情報を保存する場合は、[専用フォーマット] を選択してください。
- 宛先表の名称はエクスポートされません。
- ファクスドライバーの宛先表にインポートする場合は、[専用フォーマット] を選択してください。[LDAPフォーマット] ではインポートできません。

3 画面の指示に従って、ファイルの保存場所を指定します。

宛先表をファイルから読み込む（インポート）

コンピューターに保存したファイルから、宛先表の情報を本製品に読み込むことができます。

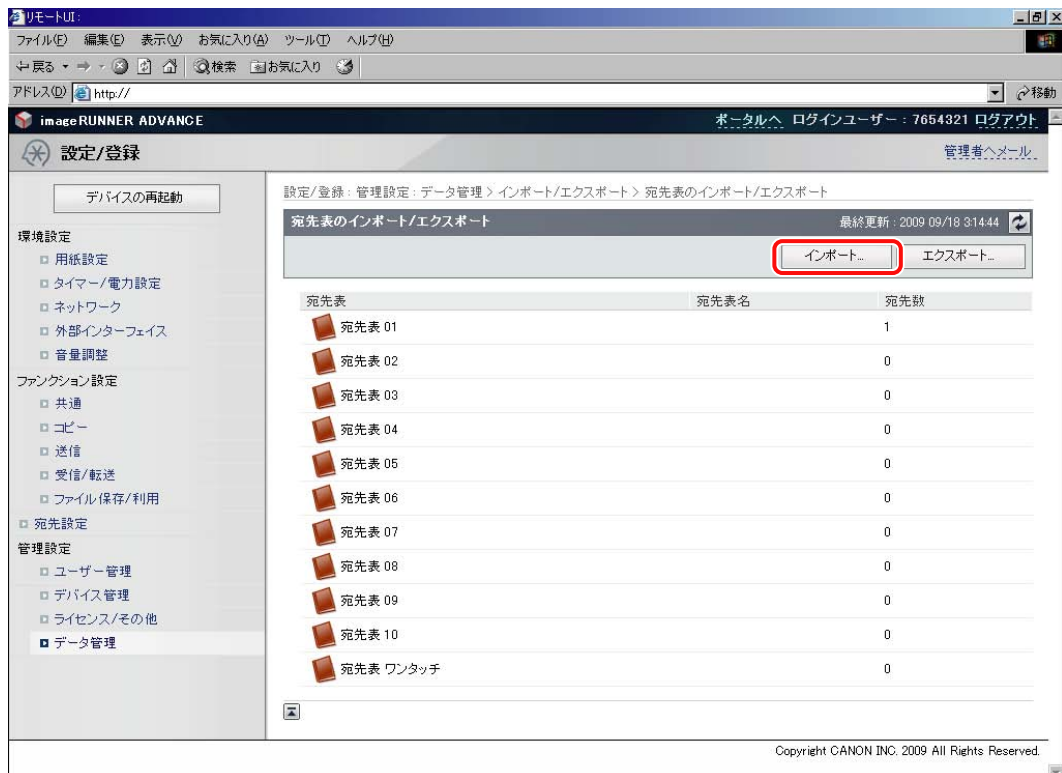


- **重要** 宛先表（削除後に上書き）、転送設定、設定/登録のインポートを行うと、よく使う設定ボタンに登録されている内容は削除されます。
- 本製品が原稿を読み込んでいるときは、インポートを行うことはできません。



- **メモ** 宛先表には最大1800件の宛先を登録できます（200件はワンタッチボタン用の宛先です）。宛先はそれぞれの情報が1件として扱われます。宛先を追加インポートするときは、すでに登録されている宛先との合計が1800件を超えないようにしてください。
- LDAPフォーマットのファイルをインポートするときは、Eメールアドレスまたはファクス番号が登録されている宛先が、本製品に登録されます。登録する宛先が1800件を超えないようにしてください。
- 宛先表のワンタッチボタンの情報は、LDAPフォーマットではインポートできません。

- 1 [設定 / 登録] をクリックして、管理設定に表示されるメニューから [データ管理] を選択したあと、[インポート / エクスポート] → [宛先表] → [インポート] をクリックします。



宛先表に暗証番号が設定されている場合は、暗証番号を入力する画面が表示されます。アドレス帳の暗証番号を入力したあと、[OK] をクリックします。

- 2 インポートするファイルを選択したあと、必要な設定をして、[インポート開始] をクリックします。

表示される項目

- [宛先表] : ドロップダウンリストから、更新する宛先表を選択します。
- [インポート方法] : 宛先表の更新方法を選択します。
- ・[追加] の場合は、読み込まれたファイルの宛先が追加されます。現在登録されている宛先は変更されません。
 - ・[削除後に上書き] の場合は、現在登録されている宛先が削除され、読み込んだファイルの内容に更新されます。
- [ファイルへのパス] : 読み込むファイルの場所を指定します。
- [フォーマット] : ファイルの保存形式を選択します。
- ・[専用フォーマット] の場合は、同じ機種からコンピューターに保存したファイルをインポートします。
 - ・[LDAP フォーマット] の場合は、他のアプリケーションソフトからインポートします。

暗号化された宛先をインポートする場合は、[宛先表の認証情報を復元化する] にチェックマークを付けたあと、パスワードの項目を入力してください。

重要

- ・宛先表1～10をインポートする場合、[インポート方法] の [追加] を選択すると、すでに同じ名称の宛先が本製品に登録されていても、同一名称で新たに登録されます。
- ・宛先表のワンタッチボタンをインポートする場合は、[インポート方法] の [追加] が [上書き] に切り替わります。
- ・[インポート方法] で [削除後に上書き] を選択すると、本製品に登録されている宛先をすべて削除してから、読み込んだファイルの内容が登録されます。

-  **メモ**
- 「LDAPフォーマット」を選択できるのは、Eメールアドレスとファクス番号のみです。宛先表のワンタッチボタンの内容は、LDAPフォーマットではインポートできません。宛先表に登録されているすべての情報を保存する場合は、「専用フォーマット」を選択してください。
 - 宛先表の名称はインポートされません。

鍵ペアとサーバー証明書、CA 証明書のアルゴリズムが変更されました

鍵ペアとサーバー証明書

本製品で使用可能な鍵ペアと証明書のアルゴリズムは以下のとおりです。

署名アルゴリズム	鍵の長さ
sha1RSA/sha256RSA/sha384RSA* /sha512RSA*/MD2RSA**/MD5RSA**	512 ビット /1024 ビット /2048 ビット /4096 ビット

* 鍵の長さが 1024 ビット以上の場合のみ使用できます。

** リモート UI からのインストール時のみ使用できます。

本製品で使用可能な鍵ペアと証明書のフォーマットは以下のとおりです。

証明書フォーマット	ファイルフォーマット	ファイル拡張子
X.509v1/X.509v3*	PKCS#12	.pfx/.p12

* リモート UI からのインストール時のみ使用できます。

CA 証明書

本製品で使用可能な証明書のアルゴリズムは以下のとおりです。

署名アルゴリズム	鍵の長さ
sha1RSA/sha256RSA/sha384RSA* /sha512RSA*/MD2RSA/MD5RSA	512 ビット /1024 ビット /2048 ビット /4096 ビット
sha1DSA	1024 ビット /2048 ビット /3072 ビット

* 鍵の長さが 1024 ビット以上の場合のみ使用できます。

本製品で使用可能な証明書のフォーマットは以下のとおりです。

証明書フォーマット	ファイルフォーマット	ファイル拡張子
X.509v1/X.509v3	PKCS#12	.pfx/.p12

MEAP 機能に関する変更

SMS は常時、SSL 暗号化通信で使用するようになりました

SMS を SSL 暗号化通信で使用するには、事前に鍵ペアとサーバー証明書を使用鍵として設定しておく必要があります。本製品にはプリインストール済みの鍵ペアとサーバー証明書が登録されています。ここでは、この鍵ペアとサーバー証明書を使用鍵に設定する方法について説明します。

 **メモ** 使用鍵を設定せずに SMS にアクセスすると、「HTTP 500 内部サーバーエラー」が表示されます。このエラーが出たときは必ず本手順に従って、SSL の使用鍵を設定してください。

- 1  (設定／登録) → [環境設定] → [ネットワーク] → [TCP/IP 設定] → [SSL 設定] を押します。
- 2 [鍵と証明書] を押します。
- 3 「Default Key」（プリインストール済みの鍵ペアとサーバー証明書）を選択したあと、[使用鍵に設定] を押します。
- 4 [はい] → [OK] を押します。

-  **メモ**
- 本製品の操作パネルで SSL 暗号化通信に必要な鍵ペアと自己署名型サーバー証明書を作成する方法については、「e-マニュアル > セキュリティー」を参照してください。
 - SMS は「管理設定」（設定／登録）の [MEAP 設定] - [SSL 設定] の ON/OFF に関わらず、使用鍵を設定することで、常時、SSL 暗号化通信で行います。

SMS 使用時に MEAP アプリケーションの設定情報を管理できるようになりました (MEAP アプリケーションの設定情報管理)

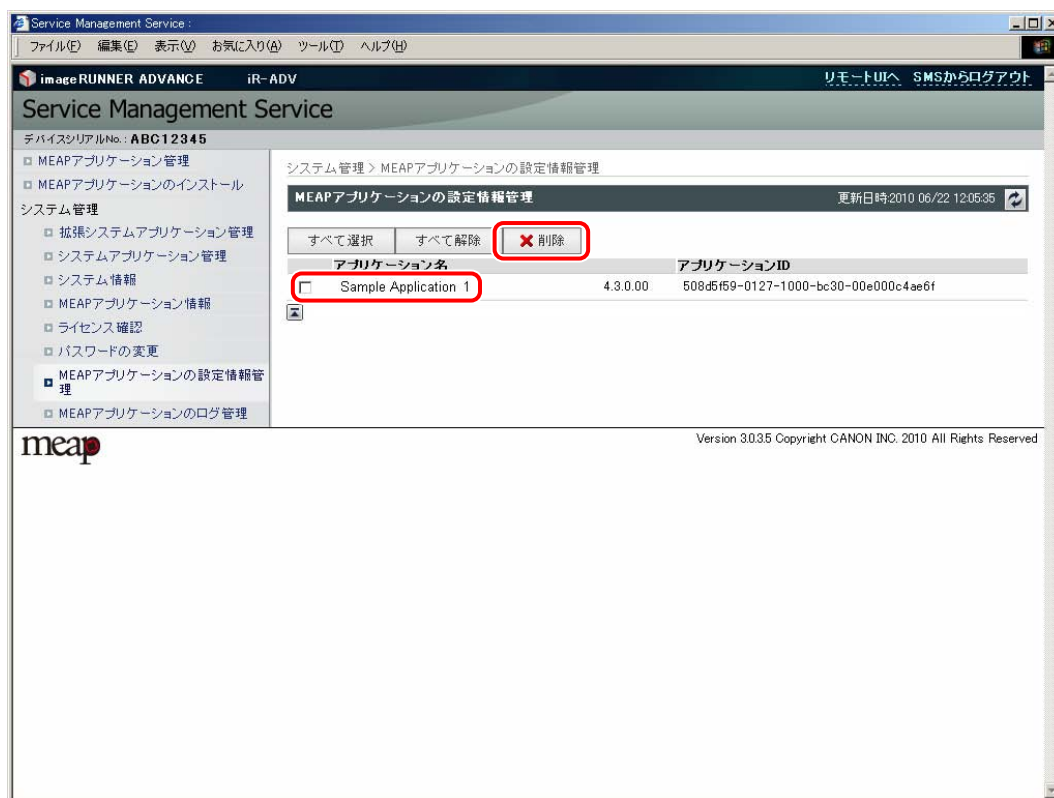
アプリケーションデータの削除を行います。

1 [MEAP アプリケーションの設定情報管理] をクリックします。



[MEAP アプリケーションの設定情報管理] ページが表示されます。

2 削除する MEAP アプリケーションにチェックマークを付けたあと、「削除」をクリックします。



「選択した MEAP アプリケーションの設定情報を削除します。よろしいですか?」というメッセージが表示されます。

 **メモ** 登録されている全てのアプリケーションを選択するには、「すべて選択」をクリックします。

3 削除する内容を確認して、「はい」をクリックします。

「MEAP アプリケーションの設定情報を削除しています ... しばらくお待ちください。」というメッセージが表示されたあと、削除が始まります。

削除が成功すると、完了をお知らせするメッセージが表示され、「MEAP アプリケーションの設定情報管理」ページに戻ります。

SMS 使用時に MEAP アプリケーションのログを管理できるようになりました (MEAP アプリケーションのログ管理)

アプリケーションのログデータのダウンロードや削除ができます。

アプリケーションログのダウンロード

1 [MEAP アプリケーションのログ管理] をクリックします。

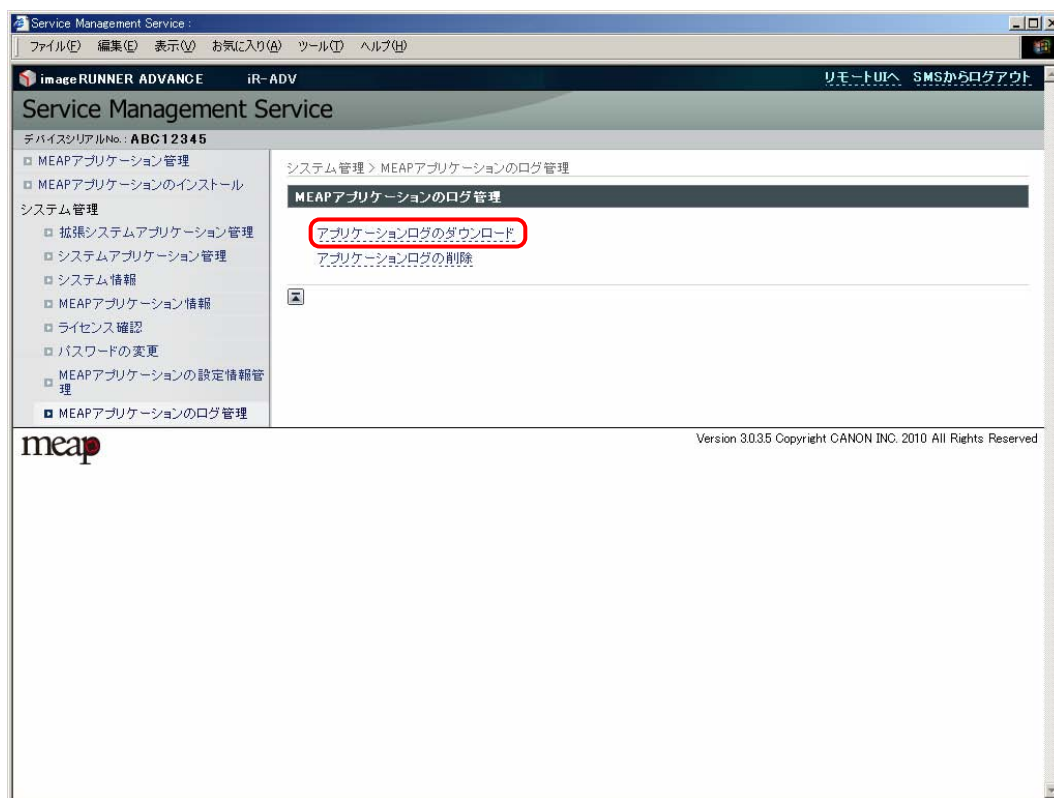
The screenshot displays the 'Service Management Service' web interface. On the left sidebar, under 'MEAPアプリケーション管理', the option 'MEAPアプリケーションのログ管理' is highlighted with a red rectangle. The main content area is titled 'MEAPアプリケーション管理' and includes a table of installed applications and a resource usage table.

アプリケーション名	インストール日	状態	ライセンス
Sample Application 1	4.3.0.00 2010 06/15	開始	不要
Sample Application 2	4.3.0.00 2010 06/15	インストール済み	不要
Sample Application 3	4.3.0.00 2010 06/15	インストール済み	不要

リソース名	使用量	残量	使用率
ストレージ	29879 KB	1018697 KB	3%
メモリー	4260 KB	126812 KB	3%
スレッド	33	223	13%
ソケット	39	217	15%
ファイル記述子	29	227	11%

[MEAP アプリケーションのログ管理] ページが表示されます。

2 [アプリケーションログのダウンロード] をクリックします。



表示されたダイアログボックスに従ってログファイルのダウンロードを行います。

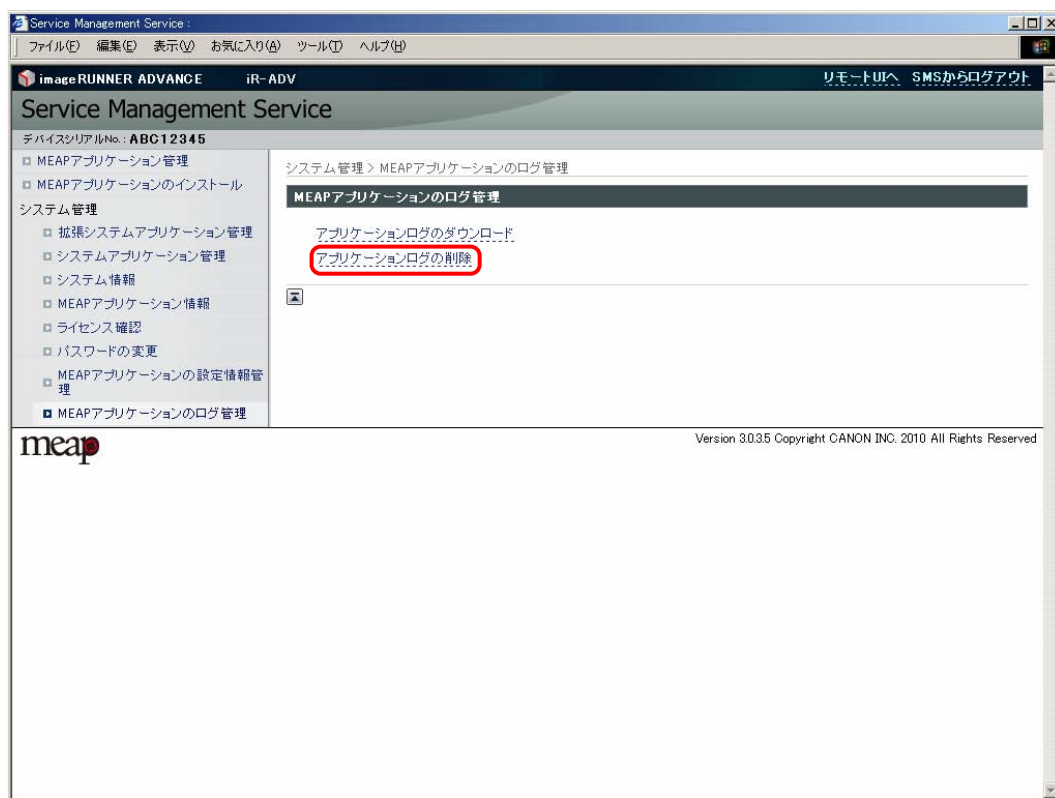
アプリケーションログの削除

1 [MEAP アプリケーションのログ管理] をクリックします。



[MEAP アプリケーションのログ管理] ページが表示されます。

2 [アプリケーションログの削除] をクリックします。



[アプリケーションログの削除] ページが表示されます。

「アプリケーションのログをすべて削除します。よろしいですか？」と表示されます。

3 [はい] をクリックします。

削除が成功すると、完了をお知らせするメッセージが表示され、[MEAP アプリケーションのログ管理] ページに戻ります。

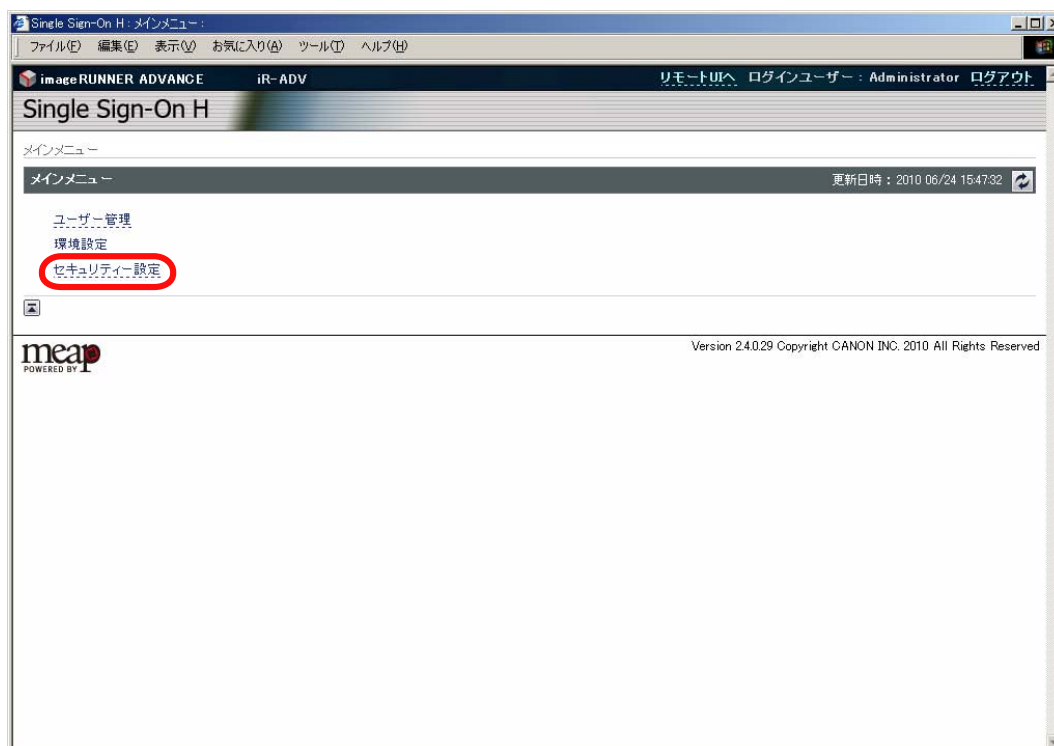
SSO-H 使用時にデフォルトパスワードでのログインを許可できるようになりました（管理者がデフォルトのパスワードで運用することを許可する）

タッチパネルディスプレイから、システムアドミニストレーター（Administrator）が工場出荷時のユーザー名とパスワードで本体にログインするときに、パスワードの変更を促す画面が表示されないように設定できます。

重要 工場出荷時のパスワードのままです SSO-H を使用すると、セキュリティ面で問題が起こる可能性があります。パスワードを変更して SSO-H を使用することをおすすめします。

メモ パスワードの有効期限が切れた場合は、この設定にかかわらずパスワードの変更画面が表示されます。

1 ログインしたあと、[セキュリティ設定] をクリックします。



[セキュリティ設定] ページが表示されます。

2 [管理者がデフォルトのパスワードで運用することを許可する] にチェックマークを付けます。

Single Sign-On H - セキュリティ設定

imageRUNNER ADVANCE iR-ADV リモートURL ログインユーザー: Administrator ログアウト

Single Sign-On H

メインメニュー > セキュリティ設定

セキュリティ設定 更新日時: 2010/06/24 15:48:40

更新 キャンセル

パスワードの運用設定

☒ 管理者がデフォルトのパスワードで運用することを許可する

パスワードのポリシー設定

☐ パスワードの長さを設定する
最小文字数: 1 文字以上 * パスワードに必要な最小文字数を設定します。

☐ パスワードの有効期間を設定する
有効期間: 7 日間 (1~180)

☐ パスワードの複雑さを設定する

- ☐ 3文字以上連続する文字列の使用を禁止する
- ☐ 英大文字(A~Z)を1文字以上使用する
- ☐ 英小文字(a~z)を1文字以上使用する
- ☐ 数字(0~9)を1文字以上使用する
- ☐ アルファベット以外の文字(0, \$, #, %など)を1文字以上使用する

ロックアウトのポリシー設定

ロックアウト機能の有効条件:

- ☐ デバイスの操作パネルからのログイン時
- ☐ リモートアクセス(ネットワーク上のコンピュータなど)からのログイン時
- ☐ デバイスのWebサービスを利用してのログイン時
- ☐ アプリケーションへの認証情報の設定時

アカウントのロックアウトのしきい値: 3 回ログインに失敗 * 設定値を超えた時点でアカウントをロックアウトします。

ロックアウト時間: 3 分 (1~60)

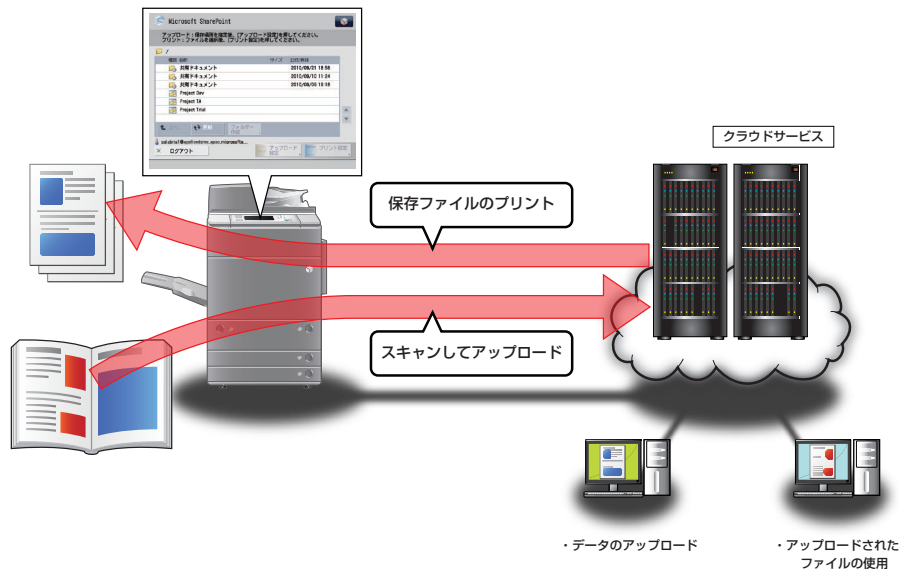
meap POWERED BY 1

Version 2.4.0.29 Copyright CANON INC. 2010 All Rights Reserved

3 [更新] をクリックします。

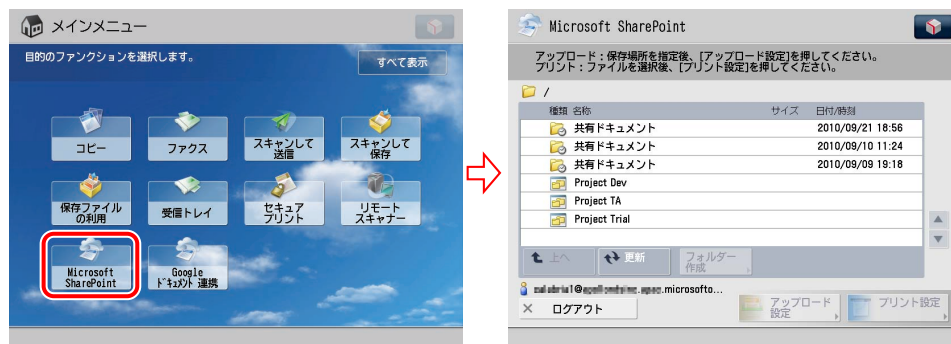
クラウドサービスが利用できるようになりました

Scan and Print for imageRUNNER ADVANCE は、デバイスからクラウドサービスを利用できるようにする MEAP アプリケーションです。本機能を使用することで、クラウドサービスにスキャンしたデータをアップロードしたり、保存されているファイルをプリントできます。



Scan and Print for imageRUNNER ADVANCE で利用できるクラウドサービスは、Microsoft SharePoint Online、Google ドキュメントです。

例：SharePoint Online の場合



- メモ**
- Scan and Print for imageRUNNER ADVANCEの導入については、担当セールスにお問い合わせください。
 - クラウドサービスを利用するには、あらかじめアカウントを取得する必要があります。アカウントの取得には利用規約等への同意が求められます。詳しくは、各クラウドサービスの提供会社のホームページ等を参照してください。
 - アップロード／プリントするファイル形式によっては、オプションが必要です。詳細については、「Scan and Print for imageRUNNER ADVANCE ユーザーズガイド」を参照してください。

情報セキュリティ規格（IEEE 2600）について

本製品は、IEEE Std 2600TM-2008（以下、IEEE 2600）という複合機・プリンターの情報セキュリティに関する国際的な規格に準拠しており、IEEE 2600 で定められたセキュリティを実現することができます。

-  **メモ**
- IEEE 2600 で定められた各セキュリティ要件に関する本製品での対応については、下記「IEEE 2600 で定められたセキュリティについて」を参照してください。
 - 本製品のみではIEEE 2600.1 CC 認証は取得しておりません。

IEEE 2600 で定められたセキュリティについて

IEEE 2600 で定められたセキュリティ機能要件と、本体でその要件を満たすために使用する機能は、下記のとおりです。

セキュリティ機能要件	本機で使用する機能	内容
ユーザー認証／ユーザー情報管理 本体を使用するユーザーを認証管理して、不正アクセスを防止	SSO-H(Single Sign-On H)	・ユーザー名／パスワードを登録して、本機を使用するユーザーの個人認証を行います。 ・ユーザー情報として、ユーザー名／パスワードのほか、部門IDやロール（権限）などを管理します。
アクセス制御 ユーザーごとの機能操作を制限	ACCESS MANAGEMENT SYSTEM 拡張キット ^{*1}	ユーザーごとにプリントやコピーなどの機能に対してアクセス制限を行います。
監査ログ ^{*2} セキュリティに関わるユーザー操作を監視	監査ログの生成／エクスポート	ユーザー認証ログやジョブログなどを生成して、リモートUIからcsv形式でエクスポートできます。
残存データの消去 本体内のハードディスク等に残存するデータを完全消去	データ消去キット ^{*1}	ハードディスク内の不要なデータを削除する際に、データを上書き消去します。
本体内のデータ保護 ^{*3} ハードディスク内の各種データや機密情報を保護	HDD データ暗号化／ミラーリングキット ^{*1}	ボックスの保存ファイル、アドレス帳の登録情報やパスワード情報などハードディスクに格納されたデータを暗号化します。
ネットワーク上のデータ保護 暗号化通信により送受信データを保護	IPSec セキュリティボード ^{*1}	暗号化通信のためのセキュリティポリシーを作成して、IPネットワーク上で送受信されるデータを盗聴、改ざんやなりすましの脅威から保護します。
ソフトウェア検証 セキュリティ機能の自己検証	IPSec セキュリティボード ^{*1}	IPSec 設定が有効時、本体起動時に暗号モジュールの自己テストを自動的に行います。

^{*1}：オプション

^{*2}：「スキャンして保存」／「保存ファイルの利用」のアドバンスドボックス／ネットワーク／メモリーメディアの操作は、監査の対象外となります。

^{*3}：メモリーメディア内のファイルは、暗号化されません。

