Canon

imageRUNNER
ADVANCE

SECURITY GUIDE

セキュリティーガイド

複合機に対するキヤノンの取り組み

複合機は情報機器です。オフィス内で重要な情報を扱うため、ネットワークに接続された際の不正アクセスや、機密データ漏洩等のセキュリティーリスクへの対策が不可欠です。キヤノンでは、複合機のセキュリティー対策に積極的に取り組んでいます。お客様が安心してご使用いただけるように、機器の高機能化や時代とともに増大し多様化する、様々なセキュリティーニーズに対して迅速に対応できるよう努めています。

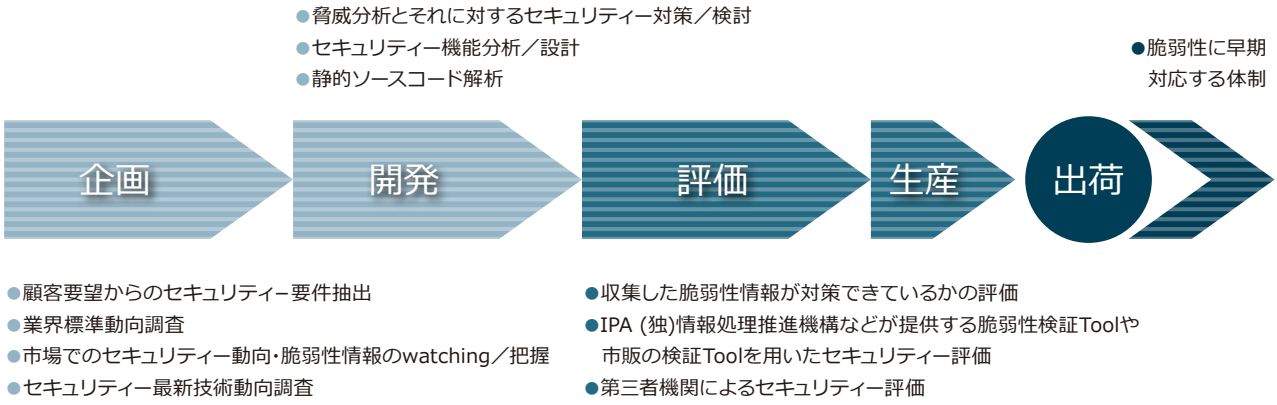
製品開発の企画・設計段階においては、セキュリティーの最新動向にアンテナを張り、脅威分析に基づいたセキュリティー機能やセキュリティーソリューションをいち早く製品に反映させています。製品評価においても外部機関による評価方法を含め徹底的なセキュリティー評価を行っています。

特に imageRUNNER ADVANCE シリーズにおいては、MFP 分野におけるセキュリティ要求仕様 (プロテクションプロファイル、PP) として HCD-PP に対応し、第三者機関が客観的に保証する CC（Common Criteria）認証（ISO ／ IEC 15408）を取得していきます。

このようにキヤノンの複合機はセキュリティー脅威に対して、最大限の対策を施していますが、世の中の技術進化とともに、セキュリティー脅威は日々高度化・多様化し、現在想定できていない問題が発見される可能性があります。

万一新しいセキュリティーに対する深刻な脅威や、製品での問題が発見された場合には、対策等の情報を発信できるような体制を取っています。

この文書では、複合機に生じる様々なセキュリティーリスクと、そのリスクに対する具体的な対策について説明します。



セキュリティー規格（ガイドライン）に準拠した取り組み

HCD-PP

HCD-PP(ハードコピーデバイスプロテクションプロファイル v1.0) は、デジタル複合機における日米政府調達用の PP として、2015 年に策定されました。これに対応することで、認証、暗号化、入出力管理などのセキュリティー機能を総合的に強化し、第三者によるネットワークシステムへの不正アクセス、不正操作によるデータ改ざんや情報漏洩を抑止できます。

FASEC（ファセック）

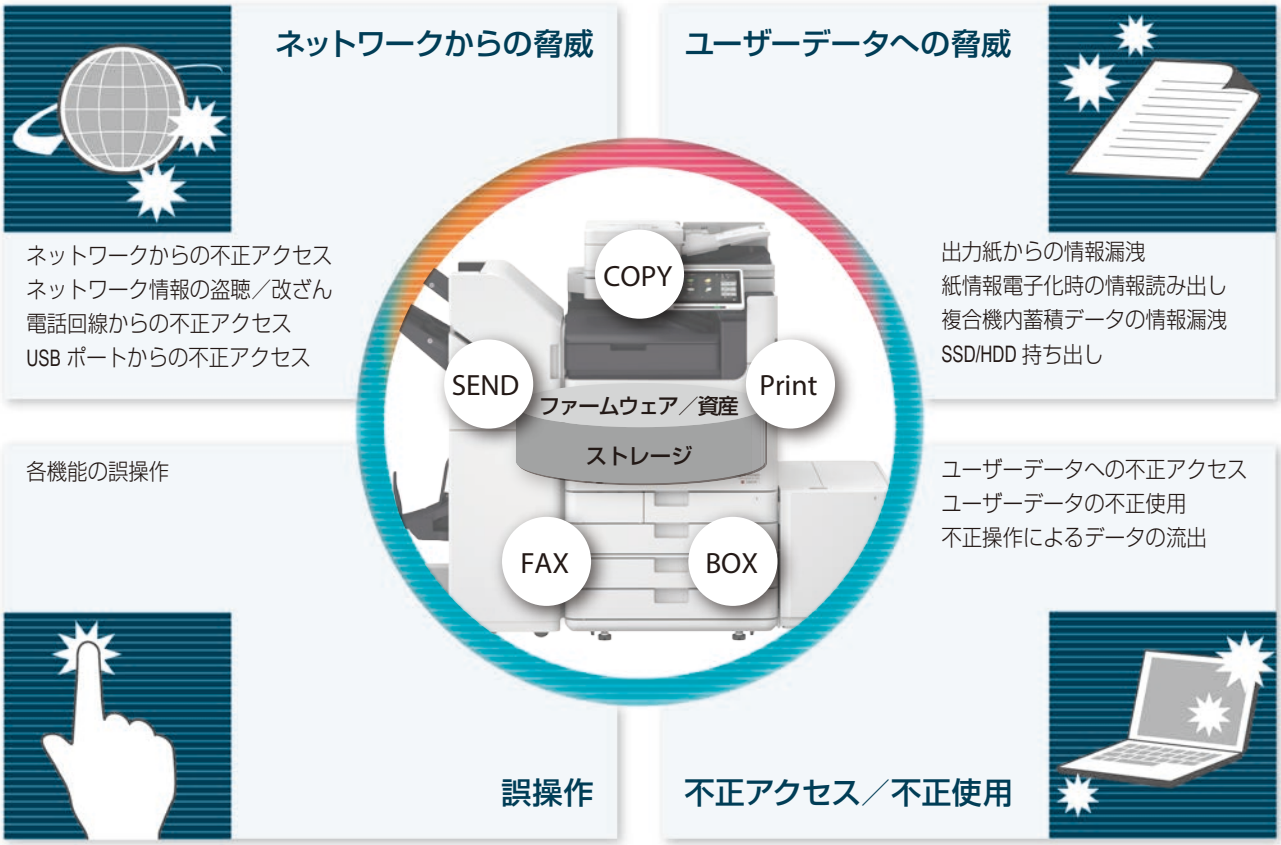
「FASEC」とは、情報通信ネットワーク産業協会（CIAJ）がファクシミリ通信のセキュリティー向上を目指して設定したガイドラインです。この制限機能を搭載していることで、ファクス番号の入力ミスや、登録した宛先の選択ミスなどの誤送信が引き起こす情報漏洩を抑制します。

BMSec

「BMSec」とは、ビジネス機械・情報システム産業協会（JBMIA）が、ネットワーク機能付きの事務機（プリンター、スキャナー、ファクス、デジタルコピー機、デジタル複合機）に関する基本的なセキュリティ要件を定義した事務機セキュリティガイドラインの呼称です。これに適合することで、認証、暗号化、データ保護などのセキュリティー機能を広範に強化し、セキュリティリスクを軽減することができます。

脅威と対策

複合機を取り巻く脅威



● 複合機におけるライフサイクルセキュリティー

キヤノンの複合機では、導入・運用から撤去・廃棄までのライフサイクルに応じた機能やサービスを提供します。
以降のページではそれぞれの段階で利用できる機能を説明します。

設置	運用		廃棄
●ネットワーク保護の設定	●本体内データ保護	●ユーザー認証	●全データ設定の初期化
●パスワード保護の設定	●本体内バックアップ	●誤操作防止	●SSD/HDD 抜取り／破壊サービス
●適切な機能制限	●プリントデータ保護	●不正使用防止	
	●スキャンデータ保護	●不正操作追跡	

まず考慮すべき事　IT 管理者は以下の設定を必ず行ってください

● ネットワーク保護のための手段

ネットワークに接続された複合機は様々な情報機器と連携しています。
その反面、ネットワーク上では、不正アクセスや盗聴による脅威にもさらされます。
正しいネットワーク設定を行うことで、リスクを抑止することができます。

必ず行っていただきたい設定

・プライベート IP アドレス設定

グローバル IPアドレス設定をしていると、外部から不正アクセスされる可能性があります。導入後は必ず「プライベート IPアドレス」に設定してください。

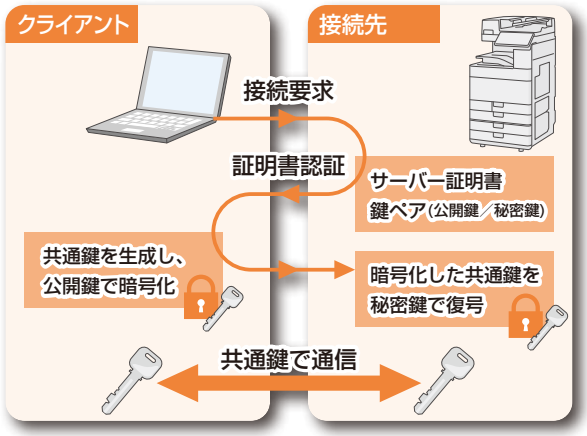
・ファイアウォール設定

特定の外部 IPアドレスや MAC アドレスからの通信を制限することで、外部からの危険なアクセスを予め遮断できます。

ネットワーク環境に応じた設定

・通信経路暗号化（TLS）

ユーザーがブラウザーを通して複合機にアクセスする際に、サーバー証明書を導入し、TLS による安全な暗号化通信を実現します。TLS 通信ではサーバー証明書の公開鍵を利用して、ユーザーと複合機双方のみで使用できる共通鍵を生成することで外部からのデータの盗聴、改ざん、なりすましを防ぎます。
なお、TLS のバージョンは 1.3 をサポートします。

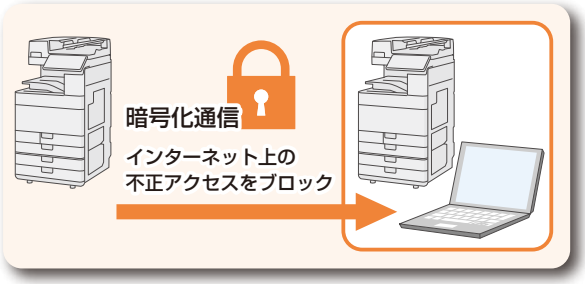


・IEEE802.1X 認証

IEEE802.1x 認証は、あらかじめ決められた端末機器以外がコンピュータ・ネットワークに参加しないよう接続規制する規格です。ネットワーク接続にこの認証方式を導入することで、サーバー認証されていない端末機器からの通信をブロックすることができます。複合機の設定を行うことで IEEE802.1x 認証環境のネットワークに接続可能です。

・IPSec 通信

IPSec はインターネットの基本プロトコルである IP にセキュリティー機能が追加されているため、アプリケーションソフトウェアやネットワーク構成に依存しない優れたセキュリティープロトコルです。IPSec 通信の設定により、IPネットワーク上で送受信される IP パケットの盗聴、改ざん、なりすましなどを防ぎます。通信の暗号化に利用する暗号技術は、米国連邦政府が策定した標準規格 FIPS140-2 に準拠しています。



・SNMP（Simple Network Management Protocol ）

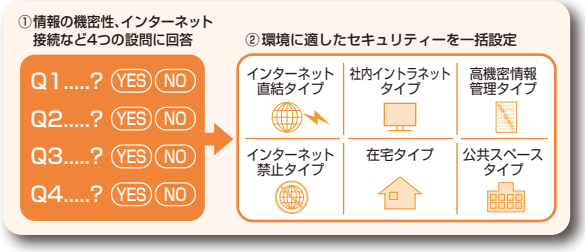
SNMP はネットワークの一括管理を行なうプロトコルで、SNMPv1 と SNMPv3 をサポートしています。複合機に接続された通信機器をネットワーク経由で監視、制御します。SNMPv3 では、セキュリティー設定において、認証や暗号化の設定をすることができます。

※その他プロトコルにも許可（ON）／禁止（OFF）制御可能

印刷ポート：LPD（LPR）／ RAW ／ FTP ／ WSD ／ IPP

・おすすめセキュリティー設定

複雑なネットワークやセキュリティーの設定をナビゲート。「社内イントラネットタイプ」「インターネット直結タイプ」「公共スペースタイプ」など 6 つのタイプから使用環境を選択すれば、環境に応じた適切な設定を一括で行えます。環境が不明の場合も、最大 4 つの設問に回答するだけでタイプを表示。簡単にセキュリティー設定が可能です。



導入時のセキュリティー対策

● データアクセスに対するパスワード保護

機器内データ（設定値やプリントデータ）にアクセスする人を制限するため、
機器管理の管理者パスワードをデフォルト値から必ず変更してください。

・ローカルデバイス認証（管理者パスワード）

※ユーザー認証については 9 ページをご参照ください。

● 各種機能制限

使用しない機能を OFF にすることで、セキュリティーリスクを減らします。

・セキュリティポリシー設定機能

情報セキュリティーの基本方針や対策基準といったセキュリティポリシーは多くの組織で定められており、パソコンや複合機などの情報機器はこれに従って運用されることを望まれます。セキュリティポリシー設定機能を用いると、ダイレクト接続などのネットワークの設定や認証ユーザーのパスワードの桁数やロックアウトの設定など、セキュリティポリシーに関連する複数の設定を一括で変更することができます。これにより設定漏れを少なくし、より確実にセキュリティポリシーに従った状態で複合機を運用することができます。

・各機能のアクセス制限

ユーザー毎に使用できる機能を細かく制限することができます。例えば、カラー出力や両面出力等のコピー／プリントに関わる機能制限を行ったり、設定／登録の各種設定行為を制限できます。

・リモート UI の ON ／ OFF 及びアクセス制限

ネットワーク上のコンピューターから、ジョブの処理状況や消耗品の残量を確認することができるリモート UI 機能について利用しない場合は OFF に設定できます。また、管理者以外の一般ユーザーのアクセスの禁止設定やアクセス時の暗証番号を設定する事で機器の不正操作防止や機器内のデータを保護できます。

・USB インターフェースの ON ／ OFF

USB ポートを有する複合機に PC を接続したり、USB メモリーの装着により、機器内のデータが不正アクセス、および盗難される危険があります。必要に応じて管理者が USB ポートの使用を許可（ON）／禁止（OFF）することで機器内データの流出を防ぎます。

● 改ざん防止

・起動時の改ざん検知

本体起動時にファームウェアや MEAP アプリケーション※など、システムソフトウェア全体に関してプログラムが改ざんされていないか検証を行い、安全性を確認します。万が一、改ざんを検知した場合は起動を停止することで、不正プログラムの動作による被害を未然に防ぎます。現在想定できない未知の攻撃に対しても有効であり、より強固なセキュリティを実現することができます。

※ 複合機上で稼働することが可能なアプリケーションです。

・ファームウェアの改ざん防止

複合機では、ファームウェアの更新時や、MEAP アプリケーション※ のインストール時に暗号化と署名による検証を行うので、不正なプログラムのインストールを防ぐことができます。

・稼働時の改ざん検知（ランタイムシステム保護機能）

本体稼働時、ファームウェアや MEAP アプリケーション※が改ざんされていないかをホワイトリストと呼ばれる信頼リストと照合することで、不正な未知のプログラムの起動を防ぎます。

・改ざん検知後の自動復旧（NIST SP800-193 準拠）

起動時改ざん検知機能の拡張として、“自動復旧”（NIST SP800-193）に対応します。従来、起動時改ざん検知で不正を検知した際に E コードを表示して起動処理を停止していたが、本対応により自動で復旧し起動処理を継続します。

● 不正アクセスに対する安全性

・電話回線から

ファクス機能を有する複合機は、電話回線により外部とつながっています。しかし、複合機内部には公衆回線網（WAN）経由でネットワーク回線網（LAN）にアクセスする機能が存在しない為、公衆回線経由によって複合機にアクセスし、ハッキング行為を行うことは不可能です。

・USB 接続から

PC と複合機を USB 接続する主なユースケースとして印刷機能と Scan 機能がありますが、USB 接続時のデータ処理経路と LAN 経由のデータ処理経路は完全分離しており、USB から LAN へのハッキングを行うことは不可能です。

運用時のセキュリティー対策
ユーザーデータ保護

● 本体内データ保護

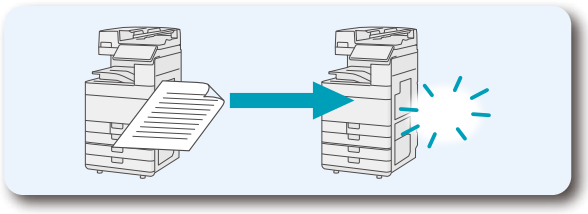
スキャンした文書や、PC から送信されたプリントデータは機器内の SSD/HDD にある「ボックス」や「アドバンスドボックス」に保存されます。また SSD/HDD 内には Eメールやファクスの宛先などの個人情報が登録された「アドレス帳」も保管することができ、これらユーザーデータを保護するために、以下の機能を用意しています。

・SSD/HDD 暗号化

ボックス内に保管した文書やアドレス帳などの登録情報、一時的に蓄積されるジョブデータやパスワード情報など、本体に格納されたデータを暗号化します。万一、SSD/HDD の盗難等がおきても、機密情報漏洩を防ぎます。

・データ完全消去

コピーやプリントなど複合機へのデータの送受信が行われる際、本体内にジョブデータが一時的に蓄積されます。それを完全に消去することで、データ流出を防ぎます。消去方法は複数から選択することができます。



・HDD ロック機能

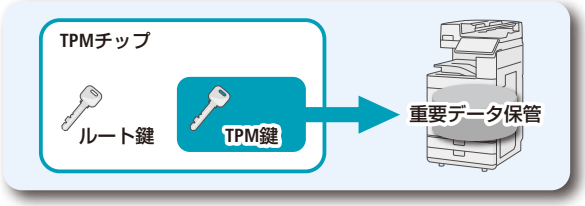
複合機本体内の HDD を不正に抜き取られた場合には、プログラムデータの改ざんやユーザーデータの盗み見などの危険性があります。このような脅威は、HDD ロック機能により守ることができます。お客様が特に操作することなく、機器が自動的に HDD のパスワードロックを有効にするので、各種データを保護することができます。

・TPM 機能

複合機内にはパスワードや暗号鍵などの多くの機密情報が保管されています。TPM（Trusted Platform Module）機能では以下の方法でセキュリティーを維持しています。

・複合機内の重要データとルート鍵を別々に管理
・ルート鍵はセキュリティチップ（TPM）により安全管理

すべての機密情報は TPM チップ内のルート鍵で暗号化してから保存され、ルート鍵はチップ外に流出することはありません。複合機内の物理的解析やネットワークを介した不正アクセスから、安全に保護されます。
また、最新の複合機から TPM2.0 に対応しています。



ユーザーデータ保護

● 本体内バックアップ

さまざまなデータ（受信・記録保存したデータや、アドレス帳、設定／登録の設定内容など）が SSD/HDD に保存されています。万一、SSD/HDD に不具合が発生した時は、これらが消失することがあります。大切なデータは定期的にバックアップ／エクスポートを行ってください。パスワードを指定しデータを暗号化した上でバックアップを行うことで、さらにセキュリティーを強化できます。

・バックアップ／リストアできるデータ

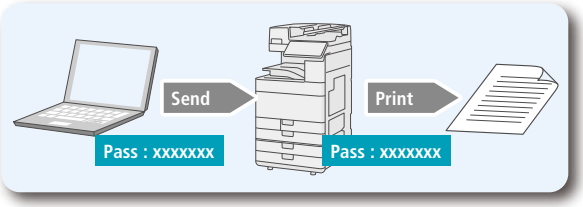
- 設定 / 登録の基本情報
- ボックス／ファクスボックス／システムボックス／アドバンスドボックスファイル
- アドレス帳（SSD/HDD のバックアップ時などでは、ファイルにエクスポートすることができます）
- ボックス／ファクスボックス／システムボックスの設定
- アドバンスドボックスの属性情報
- アドバンスドボックス内文書の属性情報
- イメージ合成のフォーム
- 鍵／証明書／ CRL
- セキュリティポリシー設定

など

● プリントデータ保護

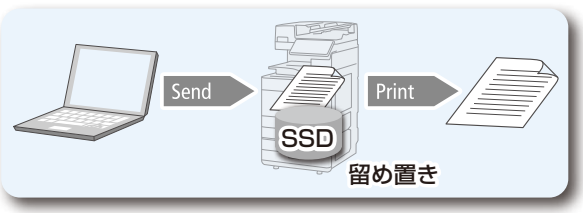
・セキュアプリント

プリンタードライバーから印刷指示をする際、セキュアプリントを選択しユーザー名とパスワードを入力すると、プリントデータを複合機内で待機させることができます。待機した文書を複合機のパネルから選択し、パスワードを入力することによって、初めてプリントアウトが開始されるため、出力用紙の放置による情報流出を抑止でき、ドキュメントの機密を保護します。



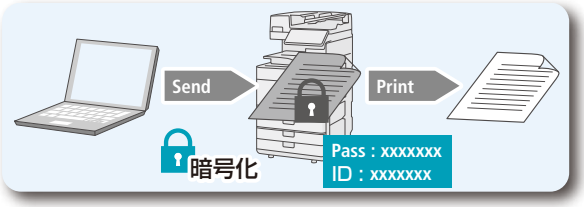
・強制留め置き印刷

印刷物の放置による「持ち去り」や「意図しない情報開示」、「ミスプリント」などを防止するために、印刷する文書を本機内にいったん強制的に留めるように設定できます。



・暗号化セキュアプリント

セキュアプリントするプリントデータをコンピューターで暗号化し、複合機で復号することによって、さらにセキュリティーを強化することができます。プリントするデータを他のユーザーに見られることを防ぎ、情報の漏洩を防止できます。



運用時のセキュリティー対策

ユーザーデータ保護

● スキャンデータ保護

・暗号化 PDF

スキャンデータ（PDF）にパスワードなどを設定することにより、暗号化された PDF を作成できます。利用時に、正しいパスワードを入力しない限り、文書を開いたり、印刷や変更をしたりすることはできないため、情報の漏洩や改ざんを防ぐことができます。

・電子署名つき PDF／XPS 通信機能

PDF／XPS ファイルに電子署名をつけてデータの改ざんを防ぐことができます。

・電子署名の種類

- 機器署名
- ユーザー署名
- 可視署名（PDF ファイルのみ対象）

● SSD と HDD のデータ消去の特性について

	SSD	HDD
ジョブ毎消去（都度消去）	・SSD がデバイスから抜き取られても、格納されたデータは、標準搭載されているストレージ暗号化チップにより、常に AES 256bit で暗号化されています。PC や異なる MFP でデータの読み書きが不可能なため対応が不要です。	・HDD 抜き取りによる情報漏洩を防ぐ目的で「ハードディスク完全消去設定」が用意されています。
全データ初期化（一括消去）	・「0 データ 1 回書き込み」に加え、SSD 内のデータ暗号化の暗号化鍵を消去し、SSD に格納されていた全データを消去します。	・撤去 / 入れ替え時にデータを完全消去する目的で「全データ / 設定の初期化」があります。 ・一括消去には、複数回の上書き消去がありますが、これは、HDD 特有の消去方法で、消去にかなりの時間を要するため、撤去作業の遅延を招いていました。

運用時のセキュリティー対策

情報流出の防止

● 不正使用防止／抑止

個人情報や証明書、機密情報など大切なデータを印刷する場合には、情報流出の抑止などの対策が必要です。
地紋印字は、不正印刷の心理的抑止効果が期待でき、機密文書の流出を抑止する事ができます。

・地紋印字

「コピー禁止」など文言を隠し文字（潜像）として出力紙の背景に埋め込み、出力紙をコピーすると文字列（模様）が浮かび上がります。これにより文書の不正コピーによる情報流出を抑止できます。

※地紋はスタンプ、日付、部数、機体番号、ID ／ユーザー名、部門 ID が選択できます。

地紋を埋め込んだデータ

運用時のセキュリティー対策

アクセス制限・誤操作防止

● ユーザー認証

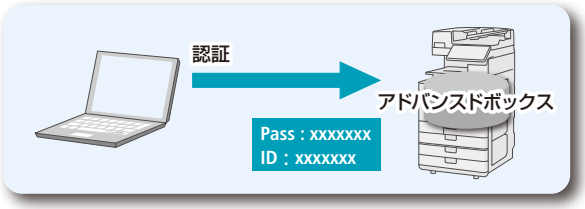
ユーザー認証により、利用者個人の識別ができます。ユーザー認証には Active Directory サーバーやデバイス本体に登録されているユーザー情報を利用しており、都合に応じて単独または併用使用を選ぶことができます。ユーザー情報として、ユーザー名／パスワードのほか、部門 ID やロール（権限）などを管理します。ユーザー認証を行うことで、複合機へのアクセス制限やユーザーごとに設定した機能制限により、機器の不正操作防止や機器内のデータを保護できます。

・ログインアプリケーション（UA、IC カード認証その他ログインアプリケーション）

User Authentication は、複合機だけを認証先とするほか、ネットワーク上の ActiveDirectory ／ LDAP サーバー／ Microsoft Entra ID を認証サーバーとして追加指定し、これらに登録されている既存のユーザー情報を活用することも可能です。
IC カード認証は、ID やパスワードを覚えておく必要がなく、簡単に認証操作ができます。

・アドバンスドボックス認証

アドバンスドボックスを使用する時や、ネットワーク上に公開してファイルサーバーとして使用する時のユーザーに対して認証管理をすることができます。



・ログイン時の 2 要素認証に対応（NIST SP800-171 に対応）

ローカル UI の 2 要素認証（IC カード＋暗証番号、またはパターン認証）に加えリモート UI の 2 要素認証（パスワード＋ワンタイムパスワード）が可能となります。

・パスワード再利用禁止と禁止期間の設定（NIST SP800-171 に対応）

管理者は、利用者がパスワード変更の際に、「以前のパスワードの使用を制限」の設定や、「パスワードの変更禁止期間の設定」の設定をすることができます。

● 誤操作防止

・パスワード都度入力（都度認証）

宛先を登録する際、送信ごとにパスワード入力を要求する設定にすることができます。これによりパスワードを知らない人が勝手に送信することを抑止します。

・Eメール送信「自分へ送信」限定機能
・ファイル送信「マイフォルダー」限定機能

ユーザーモードの管理者設定において、Eメール送信や、ファイル送信の際、送信先をログインユーザーの Eメールアドレスや専用フォルダへ限定することができます。送信先を限定することにより、ドキュメント情報の誤送信による情報漏洩を防止できます。

・FAX 番号確認入力

テンキーダイヤル入力時に宛先を 2 度入力することで、誤送信を抑止します。

運用時のセキュリティー対策

セキュアな運用維持

● 不正操作追跡

・監査ログ

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

- ユーザー認証ログ
- ジョブログ
- ボックス文書操作ログ
- ボックス認証ログ
- アドバンスドボックス保存ログ／操作ログ
- ネットワーク接続ログ
- 本体管理ログ
- 一括エクスポート／インポートログ
- 監査ログ管理機能のログ
- MEAPアプリケーション管理ログ
- ソフトウェアの登録／更新ログ
- セキュリティポリシーログ
- 留め置きプリントログ

● SIEM（Security Information and Event Management、セキュリティ情報イベント管理）対応

複合機に格納している監査ログを Syslogプロトコルを使って SIEM 側へ送信することができます。
SIEMの管理下で複合 機の監査ログを一元管理・分析し、不正を検知すると、管理者にアラートを通知します。

※ 別途 SIEMの導入が必要です。

撤去・廃棄時のセキュリティー対策

ユーザーデータ保護

撤去・廃棄された複合機からの情報漏洩と言う脅威があります。
この脅威への対策として、次のような機能やサービスが用意されていますので、ご活用ください。

・全データ・設定の初期化

本体に格納されているデータを上書きすることで、完全消去（初期化）できます。本体を返却したり廃棄する時などに有効です。

・SSD/HDD 抜取り・破壊サービス

取り扱う文書の機密性が高いお客様には、廃棄や入替えの際に、複合機へ搭載されている SSD/HDD を破壊し、情報漏洩に備えるサービスを提供しています。後日、破壊された SSD/HDD の画像を添えた報告書を発行します。なお、破壊後の SSD/HDD はお客様に返却、もしくはキヤノン MJ で引き取り後、材質別分類、プレス・溶解等の工程を得てリサイクルします。

機種毎の搭載機能一覧表 ○標準機能で対応　△オプション装着で対応　×非対応

		目的	機能名	imageRUNNER ADVANCE DX C5800シリーズ／C3900シリーズ／C359F 8700シリーズ／6800シリーズ／6700シリーズ／4900シリーズ
全般	P.2	ガイドラインに準拠した取り組み	IEEE2600（CC認証）	○
			HCD-PP	○※1
			BMSec	○
			FASEC	○
導入時の対策	P.4	ネットワーク保護設定	プライベートIPアドレス設定	○
			ファイアウォール設定	○
			通信経路暗号化	○
			IEEE802.1X認証	○
			IPSec通信	○
			SNMP	○
			プロトコルの許可／禁止制御	○
			おすすめセキュリティー設定	○
	P.5	パスワード保護設定	ローカルデバイス認証	○
		適切な機能制限	セキュリティポリシー	○
			各機能のアクセス制限	○※2
			リモートUIのON／OFF及びアクセス制限	○
			USBインターフェースON／OFF	○
		改ざん防止	起動時の改ざん検知	○
			ファームウェアの改ざん防止	○
			稼働時の改ざん検知（ランタイムシステム保護機能）	○
			改ざん検知後の自動復旧（NIST SP800-193準拠）	○
運用時の対策	P.6	本体内データ保護	SSD/HDD暗号化	○
			データ完全消去	○※3
			HDDロック機能	○※3
			TPM機能	○
	P.7	本体内バックアップ	バックアップ／リストア	○
		プリントデータ保護	セキュアプリント	○
			強制留め置き印刷	○
			暗号化セキュアプリント	○
	P.8	スキャンデータ保護	暗号化PDF	○
			電子署名つきPDF／XPS	○
			データ消去の特性について	–
		不正使用防止／抑止	地紋印字	○
	P.9	ユーザー認証	ログインアプリケーション	○※4／△※5
			アドバンスドボックス認証	○
			ログイン時の2要素認証	○
			パスワード再利用禁止と禁止期間の設定	○
		誤操作防止	パスワード都度入力（都度認証）	○
			Eメール送信「自分へ送信」	○
			ファイル送信「マイフォルダー」	○
			FAX番号確認入力	○
	P.10	不正操作追跡	監査ログ	○
			SIEM対応	○
対策撤去・廃棄時の		初期化	全データ・設定の初期化	○
		SSD/HDDサービス	SSD/HDD抜取り・破壊サービス	○※6

※1 iR-ADV C3900 シリーズ / C359F は 2023年冬認証取得予定　※2 ユーザー認証＋AccessManagementSystem　※3 iR-ADV 8700 シリーズ / 6700 シリーズのみ
※4 UA・SSO-H・部門 ID　※5 ICカード認証 for MEAP ADVANCE　※6 HDD 抜取り・提出・破壊サービス / SSD 抜取り・破壊サービス

必要なオプションは製品情報（カタログ・価格表・ユーザーマニュアル）にてご確認ください。

製品に関する情報はこちらでご確認いただけます。

キヤノン オフィス向け複合機 ホームページ
canon.jp/office-mfp

キヤノンお客様相談センター
イメージランナー
アドバンス
0570-08-0056
※おかけ間違いのないようにご注意願います。

受付時間(平日)9:00～17:00（土・日・祝日および年末年始弊社休業日は休ませていただきます。）
※受付時間は予告なく変更する場合があります。あらかじめご了承ください。

キヤノン株式会社
キヤノンマーケティングジャパン株式会社
〒108-8011　東京都港区港南2-16-6 CANON S TOWER