KYOCERA Document Solutions Inc.

京セラ製　複合機・プリンターの

セキュリティーホワイトペーパー

バージョン 082020/ 2020 年 8 月 25 日

©2020 KYOCERA Document Solutions Inc.

目次

©2020 KYOCERA Document Solutions Inc.

©2020 KYOCERA Document Solutions Inc.

©2020 KYOCERA Document Solutions Inc.

©2020 KYOCERA Document Solutions Inc.

はじめに

複合機/プリンターには、標準で OS が組み込まれており、PC と同様に、HDD や SSD が装着されている機種もあります。オフィス内の複合機/プリンターは、さまざまな重要情報を扱います。一方、ネットワークを介しての不正アクセス、ネットワーク上を流れる情報の盗聴や改ざん、HDD からの情報漏えいなど、複合機/プリンターは、近年の高度化かつ多様化された脅威にさらされています。京セラドキュメントソリューションズは、お客様に私たちの複合機/プリンターを安心してご使用いただくために、積極的なセキュリティー対策を講じており、これらの脅威に対抗すべく、さまざまなセキュリティー機能を複合機/プリンターに搭載しています。また、これらのセキュリティー機能は、適切に設計、実装、生産する工程を経て、お客様のお手元で正しく機能することが、第三者機関により客観的に評価される CC 認証（ISO15408）を取得しています。更に、MFP が備えるべきセキュリティー基準として 2009 年に制定された国際標準 IEEE2600.1/IEEE2600.2、および日本と米国でデジタル複合機を政府が調達する際にセキュリティー要件とされているハードコピーデバイスプロテクションプロファイル(HCD-PP)[*1] に適合した認証の取得と、米国のセキュリティー認証機関「NIST」[*2] が定めた暗号モジュールに関するセキュリティー規格「FIPS140-2」[*3] の認定製品を搭載し、更なるセキュリティー強化を図っております。

*1： 当社製品は只今評価段階です。
*2：NIST (National Institute of Standards and Technology) 米国国立標準技術研究所の略称。
*3：FIPS (Federal Information Processing Standard) 連邦情報処理規格の略称。

本文書では、複合機/プリンターに搭載されているセキュリティー機能について、私たちの製品がどのようにして脅威に対処し、セキュリティー運用維持を可能にしているかについて説明しています。製品をご購入いただいたお客様に、この文書をご活用いただけることを願っています。

©2020 KYOCERA Document Solutions Inc.

識別認証認可

識別認証

識別認証とは、利用者が本人であるかどうかを確認する作業です。たとえば、利用者を特定するためのユーザーID と、本人しか知りえないパスワードを入力させることにより、本人であることを確認することです。（図１）
識別認証機能を使用するには、複合機/プリンターに、ログインユーザー名とログインパスワードを設定して、あらかじめユーザー登録をする必要があります。つまり、あらかじめ登録されたユーザーのみが、複合機/プリンターを使用することができます。さらに、ユーザーごとに「一般ユーザー権限」または「管理者権限」というように、適切に権限を与えることができます。また、ユーザー別に使用可能な機能制限をかけることもできます。このように、正しいログインユーザー名とログインパスワードが入力されたときのみに、複合機/プリンターを使用することができるため、不正使用を排除することができます。ユーザーのアクセスログを基に、だれが、いつ、どれぐらいの頻度でアクセスしたかも、後ほど追跡することもできます。

ユーザー認証

複合機/プリンターを使用することができる正しいユーザーを識別し、情報へのアクセスを制御し、情報を保護する機能です。
これにより保護資産へのアクセス制御および保護を実現することができます。
入力されたログインユーザー名とログインパスワードがあらかじめ登録されたものと一致すれば、ユーザーが認証され、複合機/プリンターへのログインができます。

パスワードポリシー

解析が困難なパスワードを設定させるために、パスワードポリシーを設定することができます。パスワードの最小の長さ、パスワードの複雑さ、パスワードの有効期間を指定することが可能です。設定したパスワードポリシーに該当しないパスワードを設定することを禁止します。これにより、一般ユーザーが簡単なパスワードを設定してしまうことを防ぎ、不正にアクセスされることを防止します。

アカウントロックアウトポリシー

アカウントロックアウトは、設定時間内に所定回数以上のログインを試み、ログインに失敗した場合に、そのアカウントを一時的にロックアウトする機能です。ロックアウトまでの失敗回数（１～１０回）や、ロックアウト期間（１～６０分）の設定をします。パスワードを間違えたログインの失敗が設定回数以上になると、そのユーザーアカウントを無効にします。このポリシー設定により、パスワードクラック攻撃による、複合機/プリンターへの攻撃を成功させる可能性を極力低くします。

認証方式

複合機/プリンターは以下の認証方式を持っています。

ローカル認証

複合機/プリンター内のローカルユーザーリストに登録されたユーザー情報でユーザーを認証します。登録されているユーザーだけが複合機/プリンターにアクセスすることができます。

ネットワーク認証

認証サーバーを使用してユーザーを認証します。認証サーバーに登録されているユーザー情報でログインができます。サーバータイプは、〔NTLM〕〔Kerberos〕を選択することができ、サードパーティーの認証サーバーとの連携も可能です。

Kerberos 認証

Kerberos 認証は、ネットワーク上において、クライアントと認証サーバー間で認証を行います。また、複数のサーバーと複数のユーザー認証情報を一元管理し、ユーザーはシングルサインオンが可能です。ここで、通信経路を暗号化することができます。

©2020 KYOCERA Document Solutions Inc.

NTLM 認証

NTLM 認証は、複合機/プリンターをネットワークにつなぐときのネットワークログオンに利用されます。ネットワーク上において、パスワードが平文で流れないように、チャレンジ＆レスポンス方式を採用して、複合機/プリンターとサーバー間で認証を行います。この際、サーバーからのチャレンジデータは暗号化されており、暗号化で使用される暗号鍵は、NTLM ハッシュが使われます。

図 1

複合機/プリンター―ログイン

操作パネルから、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するほかに、以下のログイン手段を使用することもできます。

ID カード認証　（オプション）

ID カード認証は、ID カードのみでのログインと、 ID カードをカードリーダーにかざして、パスワードを入力する方法があります。ID カード認証は、ローカル認証で使用することができます。（図２）

複合機/プリンターの中にあるユーザーリスト、外部の認証サーバーの中にあるユーザーリスト、あるいはサードパーティーの認証サーバーに、あらかじめ ID カード情報を登録しておくと、ID カードで認証することができます。現在使用されている社員カード等の ID カードを使用し、識別認証することで、部門管理やユーザー管理機能が使用できます。また、ID カードと紐づいたユーザー情報により機能制限を行うことができます。（図３）

図 2

図 3

認可

ユーザーごとに、使用できる機能を制限することができます。使用制限できる項目は、プリンター印刷（カラー）、コピー印刷（フルカラー）、送信、ファクス送信、ボックス保存、外部メモリー保存などです。使用制限することにより、複合機からの情報漏えいの可能性を下げることができます。また、「ユーザー」、「管理者」、「機器管理者」というように、ユーザー権限ごとに、複合機/プリンターの機器設定のアクセス制限を行うことができます。さらに、複合機/プリンターの中には、集約制限、両面制限、エコプリント制限機能

©2020 KYOCERA Document Solutions Inc.

を持っているものがあります。集約なしの権限が無いユーザーは、2in1　以上の設定をしないと、コピーできない、というような制限ができます。

認可方式

複合機/プリンターは以下の認可方式を持っています。

ローカル認可

ローカル認証の際、複合機本体に登録されたローカルユーザーリストの認可情報を用いて行う、認可機能です。ユーザーごとに使用を制限することができます。

ネットワーク認可（グループ認可）

ネットワーク認証時に取得したグループ情報と、複合機本体のグループ認可情報で、認可処理を行います。認証サーバーに登録されたグループごとに、複合機の使用制限を設定することができます。登録されたグループが、制限された範囲で複合機を使用することにより、より安全に複合機を使用することができます。

機能単位ログイン

ゲスト認可設定にすると、プリント制限、（カラー）プリント制限、コピー制限、（カラー）コピー制限、（フルカラー）コピー制限、エコプリント制限などの機能単位でログインを制限します。ログイン制限をかけた機能については、ログイン認証が求められるので、予め設定された限られたユーザーのみが、その機能を使用することができます。利便性を維持しつつも、外部へ情報漏えいしないように、セキュリティーが適切に維持されています。

ユーザー権限の管理

ユーザー権限の管理では、それぞれユーザーに与えられた権限の範囲内のみの機能の使用が許可されます。「機器管理者」、「管理者」、「一般ユーザー」といったユーザー権限があります。加えて、いくつかの管理者権限を一般ユーザーに付与することもできます。これにより、権限を持たないユーザーが、不正に許可されていない機能を使用することはできません。

セッション管理

ユーザーが認証され、複合機へログインしてからログアウトするまでの間をセッションとして管理します。以下の管理機能があります。

オートパネルリセット

オートパネルリセットは、一定時間操作がないと、自動的にログアウトし、設定内容が自動的にリセットされて初期状態に戻る機能です。操作終了後リセットされるまでの時間を設定することができます。ログオフ操作がされなかった場合のなりすましによる複合機への不正アクセスを制限することができます。

©2020 KYOCERA Document Solutions Inc.

ネットワークセキュリティー

セキュア通信のための設定

当社の複合機/プリンターでは、ある範囲での IP アドレス、ポート番号を設定することにより、その使用許可範囲外からのネットワーク上のやりとりを制限することができます。また、TLS サーバー証明書においても、安全性の高いハッシュ関数を設定することが可能であり、ネットワーク上のデータ改ざん、盗聴、なりすましを防止することができます。
当社の複合機/プリンターは、お客様が設定されるセキュリティーポリシーに従って運用いただくことを願っています。セキュリティー簡単設定の機能を使用することにより、管理者がセキュリティーポリシーに適したレベル（すなわち、レベル 1、レベル 2、レベル 3）を選択することができます。選択されたレベルに応じて、ネットワーク設定、インターフェイスブロック設定、ログ設定等の複数のセキュリティー機能を簡単に一括で設定することができます。加えて、セキュリティー設定機能を使用することにより、あるセキュリティー機能に限定して個別に設定調整することも可能です。これにより、お客様のセキュリティーポリシーに最も適した状態で、当社の複合機/プリンターを安全に使用することができます。

IP Filter 設定

IP Filter とは、複合機/プリンターへのアクセスを IP アドレスやプロトコルの種類によって制限する機能です。この機能は、アクセスを許可する IP アドレス（およびサブネットマスクの組合せで）の範囲を指定し、その指定された範囲内の IP アドレスを有するクライアントからのアクセスのみに制限することができます。また、いくつか許可する通信プロトコルを選択して、そのプロトコルを有効に設定することができます。IPv4 と IPv6 を対象に、1 台の PC からの通信、複数台の PC からの通信を設定することができます。また、IPP(リモートでプリンターの制御を行うプロトコル)、HTTP（Web サーバーと Web ブラウザー間でデータをやり取りするためのプロトコル）などのプロトコルも設定できます。これにより、複合機/プリンターへの不正なアクセスを制限することができます。

ポート設定

IPP、SMTP などのプロトコルを使用して通信を行う際に、必要なポート番号だけを有効に設定する事により、有効に設定されていないポートを使用できなくします。

Protocol	Port No.	設定	概要
FTP サーバー	TCP 21	有効/無効	FTP サーバーは、文書を受信するためのプロトコルです。
HTTP	TCP 80	有効/無効	HTTP プロトコルは、WWW サーバーとブラウザーの間で、ウェブページのデータを送受信する際のプロトコルです。
NetBEUI	TCP 139	有効/無効	NetBEUI プロトコルは、ファイル共有やプリントサービスを利用するための小規模ネットワーク用プロトコルです。文書を受信するためのプロトコルです。
HTTPS	TCP 443	有効/無効	HTTPS プロトコルは、TLS で暗号化するプロトコルです。
IPP over TLS	TCP 443	有効/無効	IPP over TLS は、インターネット印刷に使用する IPP に、伝送路を暗号化する TLS を組み合わせたプロトコルです。IPP プロトコルでの通信で、証明書を付加することができます。
LPD	TCP 515	有効/無効	LPD プロトコルは、テキストファイルや PostScript ファイルの印刷を想定した印刷システムです。
IPP	TCP 631	有効/無効	IPP は、インターネットなどの TCP/IP ネットワークを通じて印刷データの送受信や印刷機器の制御を行うプロトコルです。

©2020 KYOCERA Document Solutions Inc.

Protocol	Port No.	設定	概要
ThinPrint	TCP 4000	有効/無効	シンクライアント環境における印刷技術である、ThinPrint を利用できます。TLS にも対応しています。
WSD スキャン	TCP 5358	有効/無効	WSD は、Windows Vista において新たなネットワーク接続を実現するプロトコルであり、複合機やプリンタデバイスの検知（インストール）やデータ送受信がより容易に使用できます。MFP/Printer で読み取った原稿イメージを WSD 対応の P C にファイルとして保存させます。
WSD 印刷	TCP 5358	有効/無効	WSD は、Windows Vista において新たなネットワーク接続を実現するプロトコルであり、複合機やプリンタデバイスの検知（インストール）やデータ送受信がより容易に使用できます。
Enhanced WSD	TCP 9090	有効/無効	Enhanced WSD は、ネットワークに接続したさまざまなデバイスを簡単につないで利用するための手続きを規定します。複合機/プリンターのステータスを、このポート 9090 を経由してステータスモニターによりモニターできます。
Enhanced WSD over TLS	TCP 9091	有効/無効	Enhanced WSD(TLS)は、Enhanced WSD で TLS を使用したセキュリティープロトコルであり、暗号化、認証、安全性（改ざん防止）を提供します。
RAW	TCP 9100-9103	有効/無効	RAW プロトコルは、LPR とは異なる手順で印刷する方法です。一般にポート番号として 9100 を使い、SNMP や MIB などを使ってプリンターを制御します。

Protocol	Port No.	設定	概要
SNMPv1/v2	UDP161	有効/無効	SNMP プロトコルは、ネットワーク内の管理情報の通信に使用されます。リードコミュニティー名とライトコミュニティー名を使用して、正常な通信を行うことができます。
SNMPv3	UDP161	有効/無効	SNMP プロトコルは、ネットワーク内の管理情報の通信に使用されます。ユーザー名とパスワードを使用して、正常な通信を行うことができます。認証オプションや暗号通信オプションが利用できます。
DSM スキャン		有効/無効	DSM（分散スキャン管理）は、Windows Server 2008 R2 の機能で、これを使用して、ユーザーの多い大きな組織のスキャン管理ができます。
FTP クライアント		有効/無効	FTP クライアントは、ネットワークでファイルの転送を行うための通信プロトコルです。
LDAP		有効/無効	LDAP サーバー上のアドレス帳を外部のアドレス帳として参照し、ファクス番号とメールアドレスを宛先に指定することができます。
LDAP over TLS		有効/無効	LDAP over TLS は、LDAP 通信を安全に行うため、伝送路を暗号化する TLS を使用したプロトコルです。
POP3		有効/無効	POP3 は、電子メールを受信するための標準プロトコルです。
POP3 over TLS		有効/無効	POP3 over TLS は、電子メール受信に使用する POP3 に、伝送路を暗号化する TLS を組み合わせたプロトコルです。
SMTP		有効/無効	SMTP は、電子メールを送信するためのプロトコルです。

©2020 KYOCERA Document Solutions Inc.

Protocol	Port No.	設定	概要
SMTP over TLS		有効/無効	SMTP over TLS は、電子メール送信に使用する SMTP に、伝送路を暗号化する TLS を組み合わせたプロトコルです。
SMB クライアント		有効/無効	SMB プロトコルは、ネットワークを通じてファイル共有やプリンター共有を実現するプロトコルです。V3.0 をサポートしています。
eSCL		有効/無効	eSCL は、Mac OS X からのリモートスキャンに使用するためのプロトコルです。
eSCL over TLS		有効/無効	eSCL over TLS は、eSCL プロトコルの通信に TLS 証明書が付加されています。eSCL over TLS プロトコルでのすべての通信を暗号化します。
LLTD		有効/無効	LLTD は、ネットワーク構成を検出し、サービス品質の診断を行うプロトコルです。
Privet		有効/無効	Privet は、ローカルネットワーク上のクラウド接続されたデバイスを見つけ出し、デバイスに関する情報を得るためのインターフェイスを提供し、そしてローカルにプリントジョブを送信するなどのアクションを実行させるプロトコルです。
DNS over TLS	TCP 853	有効/無効	DNS over TLS は、伝送路を暗号化する TLS を使用して、DNS リクエストとレスポンスを暗号化するプロトコルです。
SCEP		有効/無効	SCEP は、デバイスに証明書を自動的に発行するプロトコルです。
OCSP/CRL		有効/無効	CRL は、CA により取消された証明書のシリアルナンバーを提供するリストです。 OCSP は、ウェブブラウザーと他のクライアントに、個々の証明書のステータスをリアルタイムで問い合わせするプロトコルです。
REST		有効/無効	REST は、分散システムにおいて複数のソフトウェアを連携させるのに適したウェブアプリケーションのアーキテクチャーです。
REST over TLS		有効/無効	REST over TLS は、REST の通信に TLS 証明書が付加されています。REST over TLS プロトコルでのすべての通信を暗号化します。
Bonjour		有効/無効	Bonjour は、デバイスを自動的に検出するネットワーク技術です。
VNC		有効/無効	Virtual Network Computing（ヴァーチャル・ネットワーク・コンピューティング、略称 VNC）は、デバイスの GUI を、ネットワーク接続上遠隔で管理するための、RFP プロトコルを使用するリモートコントロールソフトウェアです。
VNC over TLS		有効/無効	VNC over TLS は、デバイスの GUI を、クライアント PC とデバイスとの間において TLS を通じて、ネットワーク接続上遠隔で管理するための、RFP プロトコルを使用するリモートコントロールソフトウェアです。
Enhanced VNC over TLS		有効/無効	Enhanced VNC over TLS は、正当な管理者が One Time Password（ワン・タイム・パスワード、略称 OTP）によりデバイスへアクセスし、遠隔でデバイスの GUI を管理するための、RFP プロトコルを使用するリモートコントロールソフトウェアです。OTP ベースのデバイスへのセキュアアクセスは、アクセスコントロールのセキュリティー強化を図っています。

©2020 KYOCERA Document Solutions Inc.

ハッシュ関数の設定

自己証明書、CSR 証明書の受け入れに対しても、TLS に使用している暗号技術において、安全性の高いハッシュ関数のサポートが可能になります。これによっても、ユーザー環境に応じたセキュリティー対策を講じることができます。

認証プロトコル

認証プロトコルとは、安全な通信を行うために認証を実現することを目的とする通信プロトコルです。当社の複合機/プリンターでは、ネットワーク認証に対応した IEEE802.1x と、電子メール送信に対応した SMTP 認証や POP before SMTP の認証プロトコルをサポートしています。これにより、成りすましを防止することができます。

IEEE802.1X

IEEE802.1x とは、IEEE（米国電気電子協会）が定めた認証に関する規格です。これは、ネットワークの接続時に、認証されたユーザーに対してのみ通信を許可する規格であるため、不正なユーザーがネットワークに接続することを防ぐことができます。このように、認証されない機器のネットワーク接続を禁止する IEEE802.1x に対応していますので、情報漏えいの防止に効果を発揮しています。当社複合機/プリンターは、以下の 4 種類の認証方式を採用しています。

PEAP-TLS/PEAP (Protected Extensible Authentication Protocol-Transport Layer Security)

クライアントは ID と証明書を利用して認証を行い、認証サーバーの証明書も同時にチェックを行います。

EAP-PEAP (Extensible Authentication Protocol-Protocol Extensible Authentication Protocol)

クライアントは ID/パスワードにより認証を行い、認証サーバーは証明書の Common Name のみのチェックを行います。

EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling)

シスコシステムズ社が開発した IEEE802.1.x/EAP 認証方式のひとつです。
クライアントは、ユーザーID とパスワードにより認証サーバーの相互認証を行い、PAC(Protected Access Credential)により、ユーザーに対して一意的な共有秘密鍵に基づいてトンネルが確立されます。

EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security)

クライアントはユーザーID とパスワードによる認証、認証サーバー側では電子証明書による認証を行います。
EAP-TLS は、クライアントとサーバー相互に電子証明書を発行し認証を行うが、EAP-TTLS はクライアント証明書の代わりにユーザーID とパスワードによる認証を行うことで導入が EAP-TLS より容易です。認証サーバー側では電子証明書が利用されるため、セキュリティー性が高くなっています。

SMTP 認証

SMTP 認証とは、E-mail 送信時に SMTP サーバーに接続する際に、SMTP サーバーで、ID、パスワードの認証を行い、認証された場合にのみ、E-mail 送信を許可する機能です。SMTP サーバーへの接続を制限することで、不正な第三者が SMTP サーバーを介して E-mail 送信をすることを防ぐことができます。

POP before SMTP

POP before SMTP とは、SMTP サーバーから電子メールを送信する際に、まず、POP 認証を行います。POP 認証が完了してから、ある一定の時間内にメール送信が可能となります。電子メール送信時に POP 認証を行うことで、なりすましを防ぐことができます。

©2020 KYOCERA Document Solutions Inc.

通信経路の保護

通信経路の保護とは、ネットワーク通信のセキュリティーを確保することです。用途や暗号化方式により、通信経路を保護するためのさまざまなプロトコルがあります。当社の複合機/プリンターは、以下のプロトコルに対応しており、ネットワーク通信上のデータ改ざんや情報漏えいを防止することができます。

SNMPv3

SNMP とは、ネットワークに接続する機器を監視し、制御するための標準的なプロトコルです。SNMPv3 は、認証機能と暗号化機能をサポートしており、データの機密性を守ることができます。

IPv6

IPv6 とは、IPv4 に代わる新しい IP プロトコルです。当社は、IPv6 の認証ロゴ を Phase2 まで取得しています。この認証ロゴを取得したことにより、当社が使用する IPv6 は、ルーターと接続ができること、PING など基本的な制御プロトコルが使用できることなど、基本的な接続ができることに加えて、より安全なセキュリティー対策が講じられている下での接続性が保証されています。

IPsec

IPsec は、IP パケット単位で暗号化することにより、通信データの盗聴や改ざんから守る機能をもつプロトコルです。IP sec を使用してデータを送受信するには、IPsec 通信可能な PC がネットワーク上に接続されており、かつ、IPsec 通信可能な複合機/プリンターがネットワーク上に接続されており、この両方に、IPsec 接続可能な設定がなされていることです。PC から複合機/プリンターへ送信される印刷データ、そして複合機から PC へ送信されるスキャンされたデータを、IPsec を使用して暗号化します[*4]。より確実にデータのやりとりを行うことができます。また、ホスト・ホスト間の通信において、安全性の高いハッシュアルゴリズムが使用可能です。
*4: IPSec 通信は、FIPS 認証済み暗号モジュールを使用した暗号化通信です。

TLS

TLS とは、Web アクセスなどでやりとりするデータを暗号化するための仕組みです。また、相互に信頼できる正しい通信相手であるかを確認する機能も備わっています。当社複合機/プリンターは、この暗号化プロトコルである TLS の TLS1.0、TLS1.1、TLS1.2、TLS1.3 をサポートしており、ネットワーク通信上のデータ改ざんや盗聴を防止することができます。また、サーバー・クライアント間の通信において、安全性の高いハッシュアルゴリズムが使用可能です。以下、TLS で暗号化をサポートするプロトコルです。

IPP over TLS

IPP over TLS とは、インターネットなど TCP/IP ネットワーク上で印刷データをやりとりする IPP に、通信経路を暗号化する TLS を組合せた、インターネットプリンティングプロトコルです。これにより、ネットワークを通じて複合機/プリンターに安全にプリント指示ができます。

HTTP over TLS

HTTP over TLS とは、TCP/IP ネットワーク上で、Web ブラウザーなどとの間でデータを送受信する HTTP に、通信経路を暗号化する TLS を組み合わせたプロトコルです。PC と複合機/プリンター間のデータ通信をする際に、情報漏えいや、第三者による改ざんの危険性を抑えます。

FTP over TLS

FTP over TLS とは、TCP/IP ネットワーク上でファイル転送に使用する FTP に、通信経路を暗号化する TLS を組み合わせたプロトコルです。FTP プロトコルを使用して複合機/プリンターからスキャンデータを送信する際、TLS を使用して通信経路を暗号化しています。より安全性の高い通信を行うことができます。

©2020 KYOCERA Document Solutions Inc.

ThinPrint over TLS（オプション）

ThinPrint over TLS とは、印刷データを圧縮し、印刷処理に割り当てる帯域幅の制御を行う ThinPrint に、通信経路を暗号化する TLS を組み合わせたプロトコルです。速やかに、かつ、安全な印刷環境を提供するものです。

SMTP over TLS

SMTP over TLS とは、E-mail 送信にサーバーと複合機/プリンター間の通信経路を暗号化する TLS を組み合わせたプロトコルです。通信中に、盗聴、なりすまし、改ざんを防ぐことができます。

POP3 over TLS

POP3 over TLS とは、E-mail 受信用プロトコルの POP3 にサーバーと複合機/プリンター間の通信経路を暗号化する TLS を組み合わせたプロトコルです。通信中に、盗聴、なりすまし、改ざんを防ぐことができます。

S/MIME

S/MIME とは、メールの暗号化や、電子署名を行うための標準技術です。当社複合機にユーザー証明書や中間証明書が登録されていれば、そのユーザーの公開鍵を使用して、複合機から送信されるメッセージを暗号化することができます。これにより、送信中のメッセージが第三者に盗聴されることを防ぎます。また、当社複合機にデバイス証明書がインストールされていれば、その複合機の秘密鍵を使用した電子署名（送信元複合機/プリンターの識別）を付加することができます。これにより、第三者によるメッセージ送信者のなりすましや改ざんを防ぐことができます。（送信元の保証）

Wi-Fi Direct®（オプション）

Wi-Fi Direct デバイスは、アクセスポイントを経由することなく、相互に接続することができます。つまり、ルータを使用する必要がありません。Wi-Fi Direct デバイスは、必要とする際に、独自のネットワークを設定します。そのネットワークは、インフラストラクチャーネットワークから独立したセキュリティードメインで運用されます。Wi-Fi Direct は、容易に接続設定が行える WPS と、WPA2-PSK (Personal)を使用していることで、MFP/プリンター側が提供する独立ネットワークに、認証されないデバイスが接続されることを防止します。これにより、不正な Wi-Fi デバイスによる MFP/プリンターの不正使用を防止しています。

電子メール送受信制限

当社のシステムでは、電子メール送受信時に、以下の送受信制限を設けることにより、誤送信や、不正使用者による悪事などを防ぐことができます。

電子メール送信先許可・拒否設定

電子メール送信先許可・拒否設定機能を使用すると、電子メール送信の宛先を制限することができます。送信先許可ドメインを設定することにより、設定されている宛先にのみ送信を行うことや、送信先拒否ドメインを設定することにより、設定されている宛先への送信を禁止することができます。これにより、誤送信をなくすことができます。

電子メール送信元許可・拒否設定

当社の複合機/プリンターには、電子メールを受信して、添付ファイルを印刷する機能があります。電子メール送信元許可・拒否設定の機能により、電子メール受信の際、設定に従って、電子メール受信を制限することができます。受信許可ドメインを設定することにより、設定されている宛先からの受信を許可することや、受信拒否ドメインを設定することにより、設定されている送信元からの受信を拒否することができます。これにより、過剰に送られてくるメールなどの悪意のあるいたずらに対する、セキュリティー対策がとられています。

©2020 KYOCERA Document Solutions Inc.

自動証明書管理

当社の複合機/プリンターは、SCEP、OCSP、CRL を使用することにより、証明書を自動的に管理（証明書の設定、検証、更新、有効期限日等）することができます。認証および TLS 暗号機能を有する自動証明書管理を導入することにより、複雑な手間をかける必要がなく、セキュリティーを強化できます。証明書の有効期限日の検証や更新を行うことで、失効した証明書を使用してしまうというセキュリティー問題を払拭することができます。また、証明書の鍵長 4096 ビット暗号をサポートしているので、証明書および PKI ベースの攻撃からも守っています。自動証明書管理はお客様が設定するセキュリティーポリシーに遵守させることができます。

証明書の取得（SCEP サーバー経由）

証明書発行の要求は、管理者によりシステムに入力された情報から作成された CRL とともに、デバイス証明書を管理する SCEP サーバーへ送信されます。SCEP サーバーから取得された CA 証明書は検証されたうえで、複合機/プリンターのデバイス証明書として自動的に登録することができます。
CA 証明書管理の自動化によるプロセスの簡素化に加えて、セキュリティーが必然と維持されます。
管理者権限を有するユーザーのみが、SCEP サーバーを設定することができます。

証明書の失効状況のチェック

証明書の失効状況をチェックするためには、(1) OCSP レスポンダのリクエストを送信する、(2)CRL と比較するといった 2 つの方法があります。
セキュリティー意識あるユーザーに応じた方法を選択することが可能です。
管理者権限を有するユーザーのみが、OCSP/CRL を設定することができます。

プロトコル毎のサーバー証明書の検証レベルの設定

ユーザーのセキュリティー環境によっては、接続先サーバーに応じてサーバー証明書の検証レベルが異なる場合があります。このため、当該機能を使用することにより、プロトコル毎（SMTP/POP3/FTP/LDAP/HTTP/DNS 等）にサーバー証明書の検証レベル（レベル 0 から 3）を設定することができます。サーバー証明書の検証レベルは、次のとおり設定することができます。レベル 0：検証なし、レベル 1：期限チェックのみ行う、レベル 2：期限チェックおよびチェーン検証を行う、レベル 3：期限チェック、チェーン検証、および失効確認を行う。
ただし、接続先サーバーとの通信は TLS 使用のセキュア通信が条件です。
正当な接続先かつ正当なサーバー証明書を確認することができます。
管理者権限を有するユーザーのみが、本機能を設定することができます。

デバイス証明書の検証レベルの設定

当該機能を使用することにより、デバイス証明書の検証レベル（レベル 0 から 3）を設定することができます。デバイス証明書の検証レベルは、次のとおり設定することができます。レベル 0：検証なし、レベル 1：期限チェックのみ行う、レベル 2：期限チェックおよびチェーン検証を行う、レベル 3：期限チェック、チェーン検証、および失効確認を行う。
ただし、クライアント側との通信は、TLS 使用のセキュア通信が条件です。
信頼されるデバイス証明書を複合機/プリンター側で保持しておくことができます。
管理者権限を有するユーザーのみが、本機能を設定することができます。

©2020 KYOCERA Document Solutions Inc.

保存データプロテクト

保存データの保護

複合機/プリンター内の HDD や SSD には、重要なデータが保存されており、このデータが流出されないように保護しなくてはなりません。当社は、以下の機能を提供することにより、この保存データに対する保護対策がとられています。より安全に当社の複合機/プリンターを利用していただくことができます。

HDD/SSD 暗号化

HDD/SSD 暗号化機能は、文書、ユーザー設定、機器情報などを複合機内の HDD や SSD に保存する際に、これらの情報を暗号化して保存することができるセキュリティー機能です。暗号化には、暗号アルゴリズムとし AES(Advanced Encryption Standard: FIPS PUB 197)、鍵長は、機種により異なりますが、128 ビットと 256 ビットがあります。また、当社複合機には FIPS140-2 を満たす暗号モジュール[*5] を搭載しております。万が一、悪意のある第三者が複合機内から HDD や SSD を持ち出したとしても、保存されている情報が流出されることから守ることができます。

*5 :暗号モジュールは、当社により設計および実装されています。当社は、暗号モジュールに対する FIPS140-2 認証を来年取得予定です。

HDD 上書き消去

HDD 上書き消去は、HDD に保存しているユーザー設定、機器情報、画像イメージなど、さまざまな重要情報を読み出すことができないようにすることができるセキュリティー機能です。

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に保存し、出力します。また、ユーザーはさまざまな設定値を登録しておくこともできます。それらのデータの実際のデータは、出力後やユーザーが削除した後も、他のデータで上書きされるまでハードディスクに残っているため、特殊なツールなどで復元することが可能であり、情報漏えいの原因となる可能性があります。HDD 上書き消去機能を使用すると、出力後のデータや削除したデータの、実際のデータを無意味なデータで上書きし、元のデータを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。各ジョブを途中でキャンセルした場合でも、その直後から、ハードディスク内に読み込まれたデータの上書き消去が開始されます。

HDD 上書き消去は、次の 2 種類の方式がありますが、機種により設定可能な方式が異なります。

◆ 1 回上書き方式

1 回上書き方式はハードディスクの不要なデータを固定値で 1 回上書きし、データの復元を困難にします。

◆ 3 回上書き方式（A）

3 回上書き方式（A）はアメリカ国防省の DoD 5220.22-M に適合させた方式で、HDD の不要なデータを上書きします。不要なデータは、1）固定値で上書きを行った後に、2）その補数で上書きを行い、3）さらにランダムデータで上書きを行った後、最後に検証を行います。データの復元を困難にします。（図４）

なお、一括データを上書き消去する際、3 回上書き方式（A）は、1 回上書き方式よりも、所要時間がかかることがあります。

©2020 KYOCERA Document Solutions Inc.

図4

Trusted Platform Module

Trusted Platform Module は当社の複合機に搭載されており、画像データや証明書といった機密情報を保護することができます。HDD の暗号化に使用される暗号鍵は、Trusted Platform Module 内にあるルート暗号鍵により、暗号化されています。証明書は同じルート暗号鍵により、暗号化されています。ルート暗号鍵は Trusted PlatformModule 内に強固に保護されているので、このセキュリティーチップの外部に公開されることはありません。HDD の暗号鍵およびルート暗号鍵は、別々に保存されています。たとえ HDD が複合機から取り外されたとしても、HDD に保存されているデータは安全に保護されているため、漏洩することはありません。

セキュリティーデータの完全消去

複合機/プリンターを廃棄するとき、リース終了で返却するときなど、複合機/プリンター内の個人情報や機密情報などが残存していては外部に情報が流出してしまいます。そうさせないために、セキュリティーデータの完全消去は、内部に保持しているデータ、残存データすべてを、DoD の 3 回上書き方式（A）、DoD の 7 回上書き方式（A）、もしくは BSI/VSITR の 7 回上書き方式（B）により（機種により異なる）、完全に消去することができるセキュリティー機能です。

◆3 回上書き方式（A）

3 回上書き方式（A）はアメリカ国防省の DoD 5220.22-M に適合させた方式で、HDD のすべてのデータ領域を上書きします。すべてのデータ領域は、1）固定値で上書きを行った後に、2）その補数で上書きを行い、3）さらにランダムデータで上書きを行った後、最後に検証を行います。のちに、高度な復元作業を施されたとしても、データの復元が不可能です。書き込み回数は 3 回、そのうえ検証は 1 回です。

◆7 回上書き方式（A）

7 回上書き方式（A）はアメリカ国防省の DoD 5220.22-M ECE に適合させた方式で、HDD のすべてのデータ領域を上書きします。DoD 5220.22-M ECE は DoD 5220.22-M の拡張したバージョンです。すべてのデータ領域は、DoD5220.22-M 方式とランダムデータでの 1 回上書きとにより 2 度実施されます。のちに、かなり高度な復元作業を施されたとしても、データの復元は不可能です。書き込み回数は 7 回です。

◆7 回上書き方式（B）

7 回上書き方式（B）はドイツ連邦情報技術安全庁（BSI）により定められた規格である VSITR に適合させた方式で、HDD のすべてのデータ領域を上書きします。すべてのデータ領域は、ゼロ(0x00)で上書きを行った後に、固定値(0xff)で上書きを行います。これを連続して 3 回実施します。さらにデータ領域は固定値(0xAA)で上書きされます。のちに、かなり高度な復元作業を施されたとしても、データの復元は不可能です。書き込み回数は 7 回です。

なお、一括データを上書き消去する際、7 回上書き方式（A）および（B）は、3 回上書き方式（A）よりも、所要時間がかかることがあります。

セキュリティーデータの完全消去の機能には、完全消去が予約された時間に確実に実行するための設定が可能な完全消去予約、完全消去実行前に管理者やサービスマンに通信する完全消去実行通知、データを完全消去した後に自動印刷されるデータ消

©2020 KYOCERA Document Solutions Inc.

去完了レポート（消去されたデータと完全消去が実施された日時を含む）、完全消去が実施された後にユーザーが複合機/プリンターを使用できないようにする完全消去後のシステムロック機能があります。これは、管理者がこれらの機能を設定し、実行することができます。これにより、機器設定を工場出荷時の状態に戻すことができます。

アクセス制限

複合機内では、データを安全に保存することができる、「ユーザーボックス」、「ジョブボックス」、「ファクスボックス」を作成することができます。 このボックス内のデータに対し、アクセス制限を行うことができます。

ユーザーボックス

ユーザーが、複合機内にデータを保存するためにユーザーボックスを作成することができます。各ボックスには、使用量の制限、データの保存期間、パスワードを設定することができます。（図５）

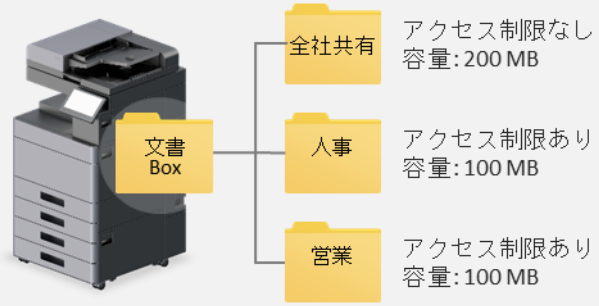

図５

ボックスパスワード

ボックスにパスワードを設定して、アクセスできるユーザーを制限することができます。パスワードは 16 文字まで入力することができます。

使用量制限

ハードディスクの容量を保つために、ボックスの容量を制限することができます。

所有者設定

ユーザーボックスの所有者に設定されたユーザーのみがアクセスできるようになり、設定されていないユーザーからのアクセスを制限することができます。また、ボックスを共有するかどうかを設定する「共有設定」を行うことができます。ユーザー管理が有効の場合に表示されます。共有していれば、所有者設定されていないユーザーでも、ボックスへのアクセスができます。利便性を保ちつつも、不正なアクセスから守ることができますので、適切なセキュリティーを維持することができます。

ドキュメントの保管期限

一定期間後に、保存したドキュメントを自動消去することができることより、いつまでも保管していることがないので、情報漏えいの機会が少なくなります。

削除タイミング

印刷が終了すると、文書をボックス内から自動的に削除することができます。削除忘れがなく、第三者による閲覧の機会から守ることができます。

ジョブボックス

プライベートプリント、クイックコピー、試し刷り後保留、ジョブ保留を、ジョブボックスを使用してデータを保存することができます。なお、これらのボックスをユーザーが削除したり、新たなボックスを作成したりすることはできません。PIN コードを設定することによりアクセス

©2020 KYOCERA Document Solutions Inc.

制限をかけることができます。（図６）

図６

一時保存文書の自動消去

ジョブボックスのプライベートプリント、クイックコピー、試し刷り後保留の一時保存文書を、保存した一定時間後に自動的に消去するように設定することができます。必要な期間だけ保存するので、権限のない者により閲覧される機会がすくなくなります。

ファクスボックス

ファクス受信データを保存する複合機内のボックスをファクスボックスと呼びます。メモリー転送機能を使って、ファクス受信データをファクスボックスに保存することができます。送信元のＦコードやファクス番号でそれぞれのボックスに振り分けることで、重要な文書をすばやく確認することができます。ファクス受信データは、複合機のパネル上で内容確認することができます。必要なファクスはそのまま印刷、不要なファクスは削除することができます。（図７）

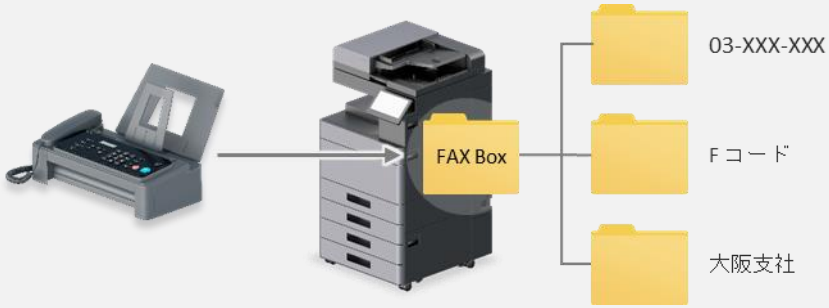

図７

ボックスパスワード

ボックスにパスワードを設定して、アクセスできるユーザーを制限することができます。パスワードは 16 文字まで入力することができます。

所有者設定

ボックスの所有者に設定されたユーザーのみがアクセスできるようになり、設定されていないユーザーからのアクセスを制限することができます。また、ボックスを共有するかどうかを設定する「共有設定」を行うことができます。ユーザー管理が有効の場合に表示されます。共有していれば、所有者設定されていないユーザーでも、ボックスへのアクセスができます。

利便性を保ちつつも、不正なアクセスから守ることができますので、適切なセキュリティーを維持することができます。

削除タイミング

印刷が終了すると、受信データをボックス内から自動的に削除することができます。無駄に長く情報を保存することによる危険性がなく、適時に削除することにより、適切なセキュリティー状態を維持することができます。

©2020 KYOCERA Document Solutions Inc.

Print セキュリティー

セキュアプリント

複合機/プリンターのプリント機能として、「セキュアプリント」という機能があります。社外秘密の書類や、個人情報を含む書類を、他人に見られることなく、プリントアウトしたいときに、他人の印刷物と紛れてしまわないよう、セキュアプリント機能を使用することができます。

プライベートプリント

プライベートプリントは、PC から送られてきたプリントジョブが、一旦、複合機/プリンター内に蓄積され、操作パネル上で操作されるまでジョブが印刷されないよう指定する機能です。アプリケーションソフトウェアから印刷するとき、プリンタードライバーでアクセスコードを指定します。印刷する際には、操作パネルでアクセスコードを入力することによって用紙に印刷されます。印刷終了後にデータは消去されます。また印刷前に主電源スイッチを切ったときも、データは消去されます。従って、より高いセキュリティーが維持されています。

不正コピー抑止

コピー時に、下記の機能により、紙文書のセキュリティーを強化することにより、不正コピーを抑止することができます。

スタンプ印字

文書の重要度などがひと目でわかるスタンプ機能を採用しており、ユーザーがいくつかのスタンプを選ぶことができます。なかでも、スタンプの種類により、たとえば、「CONFIDENTIAL」、「複製厳禁」、「秘」といったように、不正コピーを抑止する効果があるものがあります。ユーザーが、スタンプ印字を編集することもできます。また、頁数を連続して表示する連番の機能もあります。

セキュリティーウォーターマーク

プリントする文書にコピーすると浮き出る地紋（テキストやパターン）を背景に埋め込むことができます。地紋が付加された印刷物をコピーすると、文字が浮かびあがり、不正にコピーされたことがわかるようになります。（図８）

図８

©2020 KYOCERA Document Solutions Inc.

ファクスセキュリティー

FASEC

FASEC とは、情報通信ネットワーク産業協会（CIAJ）が制定したファクシミリ通信のセキュリティーガイドラインの呼称です。FASEC のロゴマークは、誤送信の防止、ダイヤルトーン検出による誤接続の防止、受信紙の放置の防止、および、確実に送信されたことの確認などの機能要件を持つことを必須とする、FASEC に準拠したファクシミリを備えた複合機に使用されます。当社は、このロゴを取得しています（日本国内のみ）。

ファクス暗号化通信

送信側で原稿を暗号化して通信する方法です。通信途中にある送信画像データを第三者が何らかの方法により盗み見ようとした場合でも、本当の原稿の内容を知ることはできません。送られた画像データは受信側で復号化し元の原稿にもどして印刷されます。第三者には知られてはならないような機密文書などを送る際に比較的有効な通信方法です。
暗号通信を行うためには、相手機が同方式の暗号通信機能を備えた当社機であることが必要です。
暗号通信では、原稿の暗号化、復号化を行うために、送信側と受信側で同じ暗号鍵を使用しますが、その暗号鍵が送信側と受信側で合致しない場合、暗号通信は成立しません。したがって、送信側と受信側であらかじめ取り決めを行い、両者で同じ暗号鍵を登録しておく必要があります。

送受信制限

あらかじめ通信条件（許可ファクス番号/許可 ID 番号）を登録し、送受信制限を設定しておき、通信条件を満たすときだけ、送受信を可能にする機能です。この機能を使うと、通信する相手先を限定することができます。また、受信制限を拒否リストに設定すると、拒否ファクス番号に登録された相手先と自局ファクス番号を登録していない相手先からの受信を拒否することができます。送信に関しては、許可 TEL リストとアドレス帳に登録されている宛先に限定することができます。

誤送信防止

重要な書類を誤った宛先にファクス送信しないように、送信時にファクス番号を必ず二度入力することができます。アドレス帳、テンキー、短縮ダイヤルでも、ファクス誤送信防止機能を設定できます。さらに、再宛先の禁止が設けられています。前回送信した宛先が残らないので、誤って同じ宛先に送信してしまうことを妨げることができます。また、他の人に送信した宛先が見られないので、情報漏えいの防止に有効です。加えて、ユーザー認証オンの場合にはログアウトした時点で、宛先情報が消されます。

二度入力

テンキーからファクス番号を直接入力して送信する際、確認のために同じ番号を複数回入力するように設定することができます。複数回の入力が一致した場合のみ、宛先を有効にすることができます。押し間違いによる誤送信を抑止することができます。これはユーザーが設定することができます。

©2020 KYOCERA Document Solutions Inc.

ファクス番号のテンキー入力の禁止

ファクス送信するときに、操作パネルからのテンキーでの直接入力を制限することができます。宛先表に登録された宛先だけを送信先にすることができますので、アドレス帳やワンタッチキーに登録された相手先以外にファクス送信することができなくなります。これは、ファクス番号の入力ミスによる誤送信や不正利用の抑止に有効です。

送信前の宛先確認

送信前の宛先確認を設定している場合、スタートキーを押すと、宛先を確認するための画面が表示されます。必ずすべての送り先を操作パネルに表示しないと、確認完了キーは機能しません。相手先に送信する前に再度確認することができるので、誤送信を防ぐことができます。

使用禁止時間

受信したファクスの印刷を禁止する時間帯を設定することができるセキュリティー機能です。使用禁止時間を設定すると、禁止時間中はファクスの印刷以外にも、コピー印刷、プリント印刷、メール受信印刷、USB からの印刷、送信、Network ファクス送信など、すべての動作が禁止されます。PIN コード入力による制限が可能であり、一時解除が可能です。人の少ない夜間に出力することを禁止したりするなど、複合機の不正使用を防止することができます。

F コード通信

Ｆコード通信とは、ITU-T（国際電気通信連合）の勧告に準拠したサブアドレスやパスワードを付加して送受信する通信を言います。Ｆコードを使用することにより、本来当社の複合機間でしかできなかった親展通信（受信側機に設けられた原稿受け渡しボックスに送る通信）や、ポーリング通信（受信側から操作して送信側の原稿を受信する通信）などの通信が他社機との間でも可能になります。また、Ｆコード通信を使用して、受信した原稿をＦコードボックスに保存するなど、より安全に通信を行うことができます。

F コード親展送受信

相手機に親展ボックスが設けられていると、サブアドレスやパスワードを指定して、相手機内のボックスに、重要書類など、他人に見られたくない書類を、機密性を確保しながら、親展送信することができます。受信した原稿を印刷せずに、予め登録しておいたファクスボックスに保存されるので、誰にも見られずに印刷することができます。

F コード掲示板送受信

F コードを使用することによって、相手先が、Ｆコード掲示板送信機能を備えていれば、情報漏えいすることなく、安全に通信することができます。

メモリー転送

ファクスを受信したとき、受信画像を他のファクスやコンピューターに転送したり、印刷を設定したりすることができます。転送設定を有効にすると、受信したすべての画像を指定先に転送することができます。他のファクス、メール送信、フォルダー（SMB）送信、フォルダー（FTP）送信に転送することができます。また、設定した複合機内のユーザーボックスに受信した画像を転送して保存することもできます。受信用紙が放置されたままといった状態を防ぐことができます。（図９）

©2020 KYOCERA Document Solutions Inc.

図9

不正侵入に対する安全対策

当社複合機のファクス機能とネットワーク機能は、各々分離されています。ファクス回線から入ってきたデータは、ファクス機能が処理します。ファクス機能を有する複合機を踏み台にして電話回線からネットワークへの侵入アクセスや、複合機内部への不正アクセスができない構成になっています。

©2020 KYOCERA Document Solutions Inc.

Send セキュリティー

送信前の宛先確認

送信前などに宛先の番号や件名などを画面上で確認できます。宛先設定ミスなどによる誤送信を未然に防ぐことができます。ユーザーによる設定により、送信前に強制的に操作パネルに表示させることもできます。

同報送信の禁止

同報送信とは、1 回の操作で同じ原稿を複数の宛先に送ることができる機能です。この機能を管理者が禁止・許可する設定を行うことができます。禁止に設定された場合、宛先を 2 件以上含むグループの選択は不可能になります。グループに宛先が意図せずに追加されて意図していない宛先に送信されてしまうことを防ぐことができます。

新規宛先の入力

操作パネルからの直接入力を制限し、アドレス帳、ワンタッチキーなどの、あらかじめ宛先表に登録された宛先だけを送信先にすることができます。ファクス番号の入力ミスによる誤送信や不正利用の防止に有効です。

PDF 暗号化機能

ファイル形式で PDF または高圧縮 PDF を選択すると、パスワード設定や暗号化により、スキャンされた文書を安全に保護することができます。 パスワードを入力することにより、PDF の表示、印刷および編集に対して、制限をかけることができます。安全に PC やサーバーに保存したり、電子メールで送信することができます。

ファイルへのデジタル署名

当該機能は、ファイルへデジタル署名を付加することで、セキュリティーを強化することができます。
予め当社複合機にデジタル証明書と秘密鍵/公開鍵ペアとを登録しておきます。スキャンした後、そのデバイス証明書と鍵ペアとを用いてデジタル署名が生成されます。そしてデジタル署名が付加されたファイルが当該複合機で生成されます。
この過程により、受信者は、デジタル署名されたファイルがどの複合機で生成されたか、デジタル署名が付加されたファイルが生成された後に、ファイルが改ざんされているか否か、を検証することができます。

FTP 暗号送信

FTP 暗号送信機能を使用する際に、「TLS」を使用することにより、通信路を暗号化して FTP 暗号送信を行うことができます。送信中のセキュリティーが維持されているので、送信データの改ざんや盗聴の危険性を抑えることができます。

©2020 KYOCERA Document Solutions Inc.

デバイス管理

ジョブ管理

デバイスのキューにあるジョブについての情報や、履歴を確認することができます。「印刷ジョブ状況」、「送信ジョブ状況」、「保存ジョブ状況」、「予約ジョブ状況」の 4 種類のステータス、および、「印刷ジョブ履歴」、「送信ジョブ履歴」、「保存ジョブ履歴」の 3 種類のジョブ履歴を使用することができます。ユーザー名、時間、送信先など特定のジョブに関する詳細な情報を参照することができるので、必要なときに追跡調査が可能です。プリンタードライバーから印刷する際にファイルをジョブ名に使用するかどうかの設定が可能です。（図１０）

図１０

ジョブ情報参照権限

ユーザーの権限に応じて、ジョブ履歴参照画面を切り替えすることができます。ジョブステータス詳細情報とジョブ履歴の、ジョブ情報参照権限の設定や、ファクス通信履歴参照権限があります。ユーザー認証がオンの際に、本人だけが、自分のジョブ履歴情報を確認することができます。管理者が参照できる画面では、すべてのジョブ履歴情報を確認することができます。

監査履歴

複合機/プリンターの監査履歴を取得することができます。この履歴の内容により、操作したユーザー、日時、結果を確認することができます。監査履歴には、ログイン履歴、デバイス履歴、セキュリティー通信エラー履歴などがあります。複合機/プリンターの管理者は、これらの履歴を確認することにより、複合機/プリンターが、安全に使用されているか、危険にさらされていないか、など、調査することができます。

ログイン履歴

ユーザー認証のログイン履歴を蓄積することができます。万が一、複合機/プリンターの不正操作や、複合機/プリンター内のドキュメントの改ざんや漏洩が発生した場合でも、ログイン履歴を調査し、不正アクセスを追跡することに役立てることができます。

デバイス履歴

ファームウェアのアップデート、および、複合機/プリンターの設定変更などの履歴を蓄積することができます。管理者がシステムメニュ

©2020 KYOCERA Document Solutions Inc.

ーから変更した内容が記録されます。

セキュリティー通信エラー履歴

セキュアなネットワーク通信の失敗の履歴を確認することにより、正しくネットワーク通信ができているか、把握することができます。度重なる通信失敗などがある場合は、不正アクセスの可能性を調べることができます。

履歴管理

監査履歴およびジョブ履歴を確実に管理することができます。これらは、セキュリティー事故などの追跡調査に役立てることができます。

ジョブ履歴送信(電子メールアドレス)

管理者が設定した履歴件数に達した際に、管理者が指定した電子メールアドレスに夫々のジョブ履歴を送信することができます。

Syslog

syslog プロトコルを使用することにより、複合機/プリンターの監査履歴を SIEM サーバー*6 へリアルタイムで送信することができます。監査履歴を収集および一元的に管理します。加えて、脅威となる事象をいち早く検知および分析します。第三者による不正アクセスの試みや、機械設定の不正変更、データ漏洩など異常が検出されたとき、管理者に速やかに通知します。これにより、セキュリティーリスクの緩和と管理者の負担が軽減されるため、セキュリティーの信頼性と、管理者の業務の効率性が向上します。
*6：ユーザー環境にて SIEM サーバーの設定が必要です。

セキュリティー機能の完全性の検証

当社では以下の機能によりセキュリティー機能の完全性を確認します。セキュリティー機能の実行モジュールが改ざんされていないこと、かつ、正しく動作していることを確認することができます。同様に、セキュリティー機能が使用するデータの完全性も確認することができます。

電子署名付きファームウェア

ファームウェアに対して電子署名を付与し、ファームウェアの正当性を確認することができます。複合機/プリンターを動作させる働きをするファームウェアに対して、悪意のある第三者による改ざんを防止することができます。また、複合機/プリンターを踏み台にしてのネットワークへの侵入や、これらの機器の破壊からも守ることができます。

セキュアブート

セキュアブートは、実行前において、正当なファームウェアを使用して、複合機が起動しようとしているか、を確認するための機能です。ファームウェアの正当性はファームウェアに電子署名が付与されていることで確認することができます。複合機が起動する時、ファームウェアは RAM に展開されます。その時、複合機にアップロードされているファームウェアのハッシュ値と、電子署名から作成されたハッシュ値とが同一であることを確認します。たとえ悪意のある者が不当なファームウェアを作成したとしても、電子署名を偽造できないので正当性の検証を掻い潜ることはできません。従って、たとえファームウェアが悪意のある者により改ざんされたとしても、それを実行することはできません。セキュアブートは、複合機を踏み台にしての機器の破壊から守ることができます。

ランタイムデータ整合性チェック

ランタイムデータ整合性チェックは、複合機が起動した後、複合機が操作されている間においても、RAM に展開されたファームウェアが改ざんされることなしに、ファームウェアの正当性が維持されているかどうかを定期的に検証するための機能です。たとえファームウ

©2020 KYOCERA Document Solutions Inc.

ェアが悪意をもって書き換えられたとしても、それを検知することができます。そして、システムエラーとして警告が発されます。ランタイムデータ整合性チェックは、上記のセキュアブート機能とともに使用されることで、ファームウェア改ざんに対するセキュリティー対策として、より高い効果が期待されます。

©2020 KYOCERA Document Solutions Inc.

使用制限

使用制限

当社の複合機/プリンターでは、以下のような使用制限をかけることができます。複合機/プリンターの操作を制限することができるので、複合機/プリンター内に保存されているデータへのアクセスを制限することができます。

インターフェイスブロック

インターフェイスごとにアクセスをブロック（制限）することができます。たとえば、USB デバイス、USB ホスト、オプションインターフェイス（スロット１）、オプションインターフェイス（スロット２）をブロックすることができます。ネットワークインターフェイスは、プロトコルごとにアクセスを制限することができます。

USB ストレージクラスの論理ブロック

USB メモリーを複合機/プリンターの USB ポートに接続することにより、複合機/プリンターのデータに不正アクセスされたり、もしくは、データが漏洩したりするリスクがあります。管理者が、複合機/プリンターの USB ストレージクラスの使用をオフすることにより、ID カードリーダーを複合機の USB ホストインターフェイスに接続して使用することはできますが、USB メモリーを複合機/プリンターの USB ホストインターフェイスに差込んでも使用できないように制限することができます。USB ホストインターフェイスから USB メモリー経由での情報漏えいや、ウィルス感染から守ることができます。

操作パネルロック

複合機/プリンターの操作パネルからの操作を制限することができます。パーシャルロックは、３段階に分けて設けられており、パネルからの入出力に関わる設定、ジョブの実行に関わる設定、用紙に関わる設定への移行を禁止するという、禁止したいレベルに応じた設定が可能です。操作パネルロックは、システムメニューの操作と、ジョブキャンセルの操作を禁止することができます。複合機/プリンター本体を不正に操作することを防ぐことができます。

京セラドキュメントソリューションズ株式会社

大阪市中央区玉造 1 丁目 2 番 28 号　〒540-8585
TEL: 06-6764-3555（大代表）
http://www.kyoceradocumentsolutions.co.jp/

©2020 KYOCERA Document Solutions Inc.