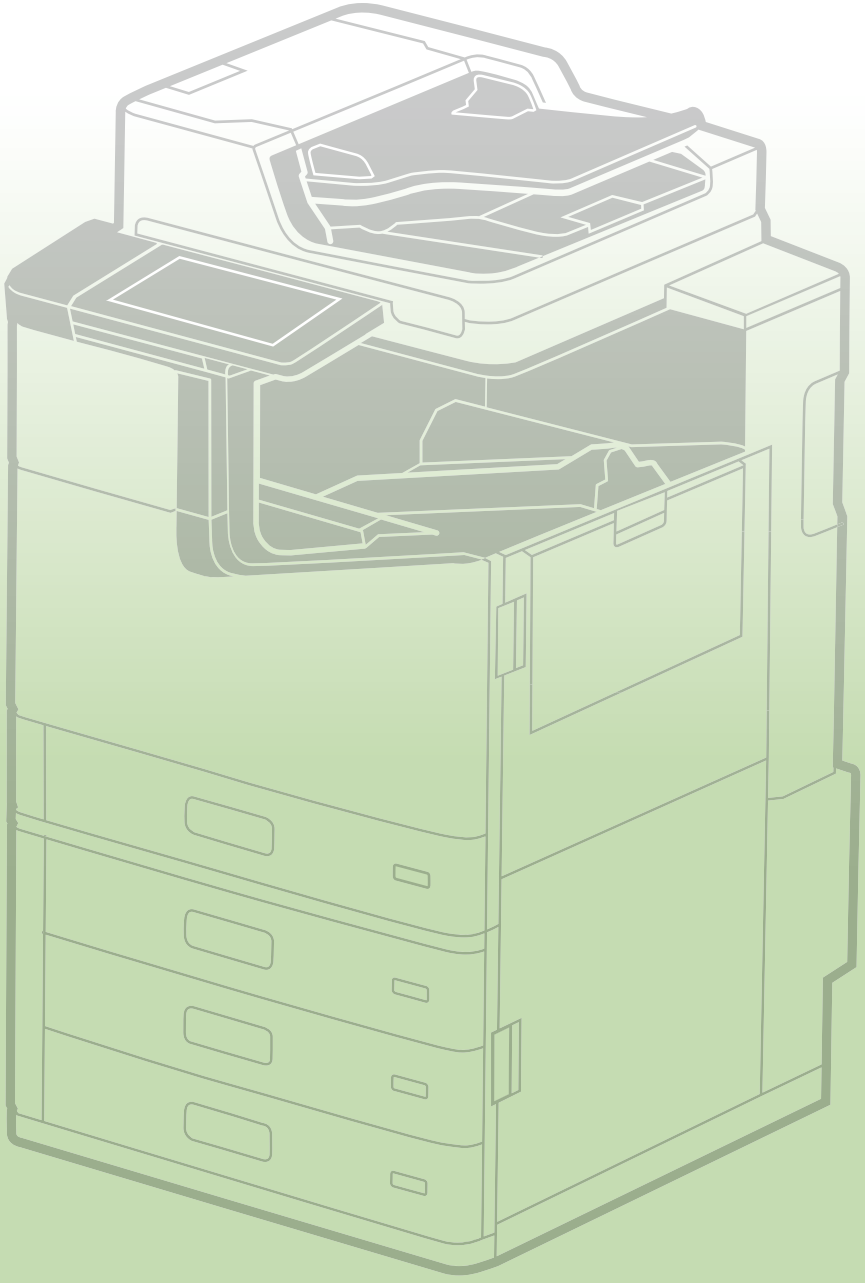
EPSON
EXCEED YOUR VISION

セキュリティーガイドブック



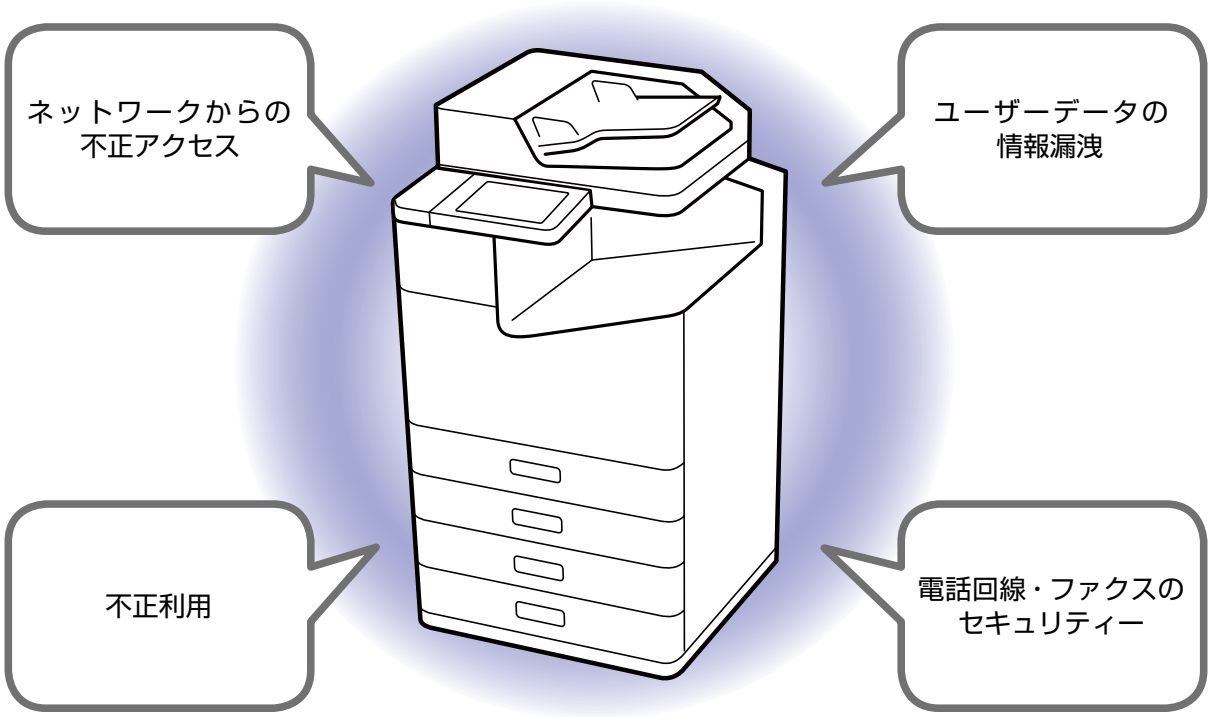
目次

1. 本書のご案内

情報化社会の発展に伴い、さまざまな機器がネットワークにつながるようになりました。

エプソンでは、お客様の利便性向上のために、製品のネットワーク対応機能の強化を進めています。

エプソンの製品にはさまざまな機能が搭載されており、特にネットワークに接続して使用する場合は、コンピューターやサーバーなどと同様にセキュリティーへの適切な配慮が必要です。



本書では、エプソンのセキュリティーに対する取り組みのご紹介とお客様へのお願い、利用可能なセキュリティー機能のご案内をしています。セキュリティーの設定方法は、製品のマニュアルでご確認ください。

2. セキュリティーに対するエプソンの取り組み

エプソンでは、お客様に製品を安心かつ安全にお使いいただくために、セキュリティーに関して以下の取り組みをしています。

1. 製品のセキュリティーを製品品質の根幹として捉えています。
   企画段階からお客様がご利用を終了するまでの、ライフサイクルにおけるセキュリティーを考慮したモノづくりを行っています。
2. お客様に対してセキュリティーに関する情報提供や啓発を積極的に行っています。
3. 脆弱性への対応を継続して行っています。
   - 業界標準ツールによる脆弱性試験を実施し、脆弱性のない製品を出荷するように努めています。
   - 製品のファームウェアで使用しているオープンソースソフトウェアの脆弱性情報を定常的に監視しています。
   - 新たな脆弱性が見つかった場合は速やかに分析を行い、情報や対策を提供します。
4. セキュリティー規格に対応しています。
   - FASEC1
     FASEC とは、一般社団法人 情報通信ネットワーク産業協会（CIAJ）がファクス通信のセキュリティー向上を目指して制定したガイドラインの呼称です。
     誤送信や誤接続を防止する機能、受信紙の放置防止機能、確実に送信できたことを確認する機能によってファクスのセキュリティーが向上します。
   - ISO15408/IEEE2600.2
     ISO15408 はセキュリティーに関する国際的な評価・認証制度です。
     複合機用のプロファイルである IEEE2600.2 に適合しており、第三者による評価・認証を受けたセキュリティー機能を備えています。

3. 設置時に行っていただきたいこと

製品本体の工場出荷時の設定は、セキュリティー面で必ずしも万全な状態になっているわけではありません。セキュリティー確保のため、設置時には以下をお読みいただき、ご利用環境に応じて必要な設定をしていただくようにお願いしています。

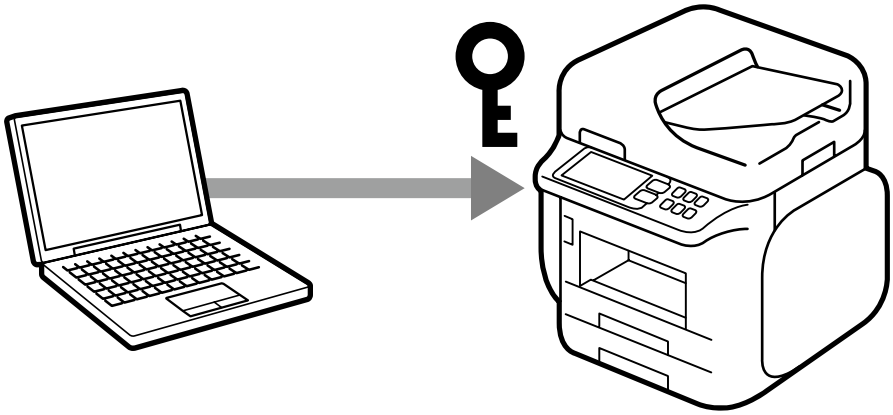
3-1. 管理者パスワード

設置時には製品に管理者パスワードを個別に設定することを強く推奨しています。

管理者パスワードが未設定、または工場出荷設定のままの場合、製品内に保持されている本体設定やネットワーク設定が不正に参照されたり、または変更されたりするリスクがあります。また、ID やパスワード、アドレス帳等の個人情報や機密情報が漏えいするリスクもあります。

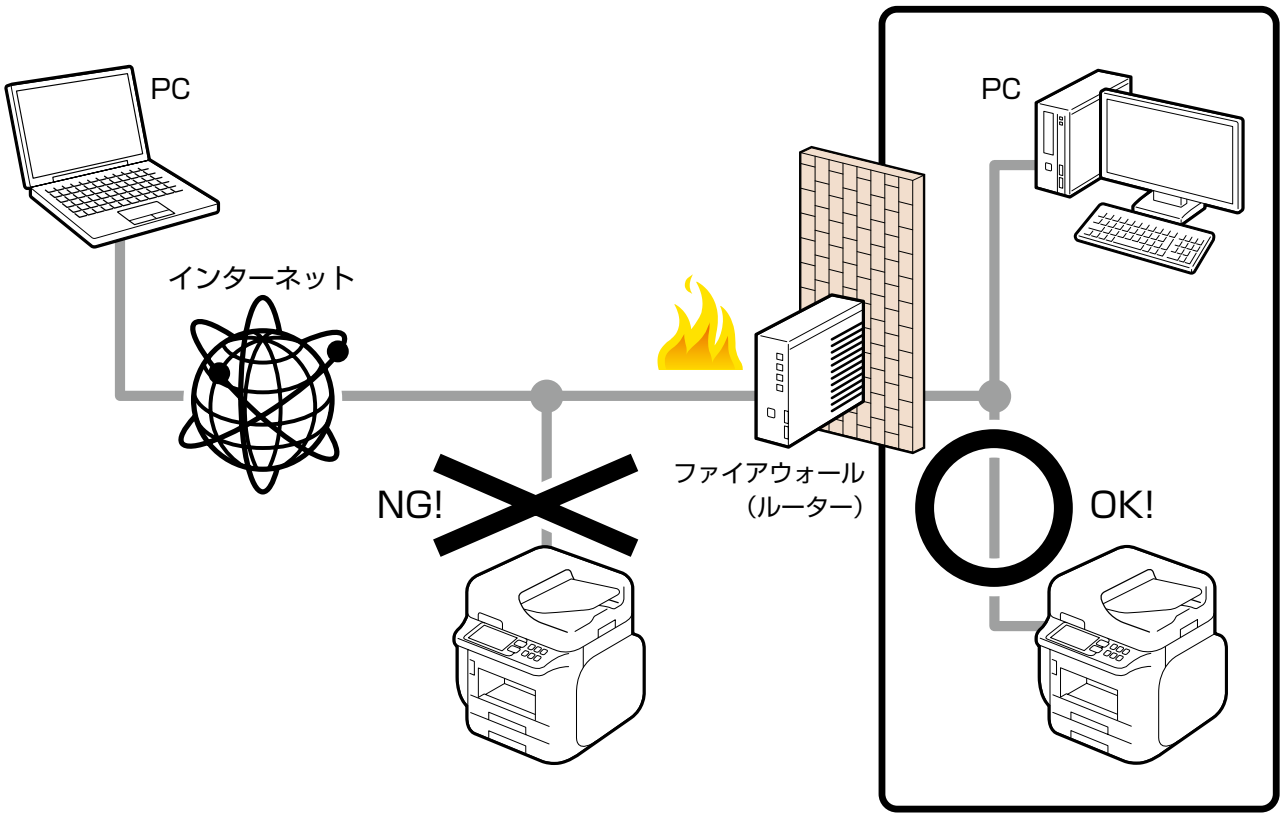
管理者パスワードは、英文字だけでなく、記号や数字を取り混ぜて 8 文字以上にする等、他者に推測されにくい複雑な文字列にしてください。管理者パスワードは、製品の操作パネルで直接設定、またはネットワーク経由で設定できます。

なお、製品によってはセキュリティー強化のため工場出荷時に個別のパスワードが設定されています。



3-2. インターネットへの接続

製品はインターネットに直接接続せず、ファイアウォールで保護されたネットワーク内に設置してください。その際には、プライベート IP アドレスを設定して運用することを推奨します。



製品のネットワーク機能には印刷の他に、Web 管理画面などの管理用のインターフェイスも含まれています。エプソンでは脆弱性試験を実施し、脆弱性のない製品を出荷するように努めていますが、インターネットに直接接続されると、不正操作や情報漏えいなど、お客様のネットワークに思わぬセキュリティーリスクを抱えることになります。

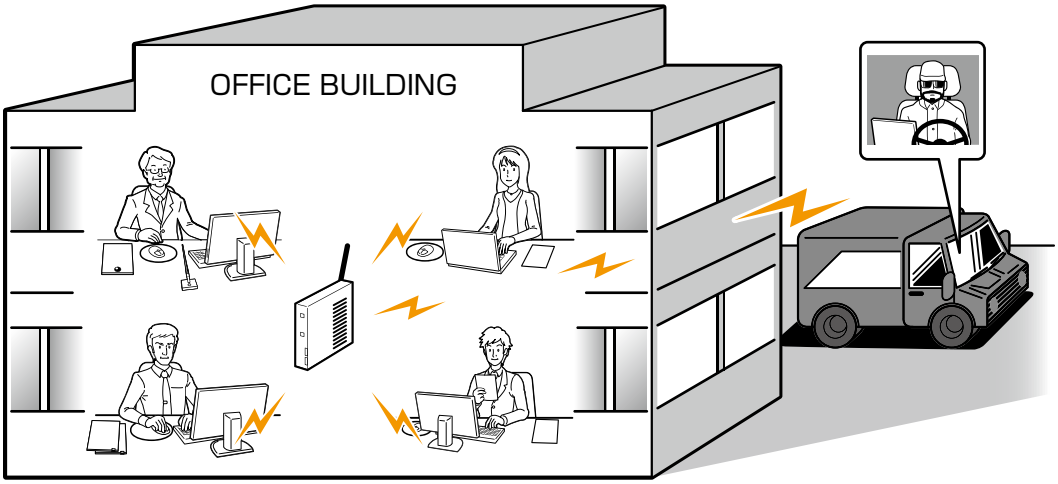
3-3. 無線 LAN ネットワーク

無線 LAN 使用時は、無線 LAN のセキュリティーを適切に設定してください。

無線 LAN のセットアップに WPS(Wi-Fi Protected Setup) や AOSS™ をお使いいただくと、安全性が高い複雑なパスフレーズや暗号化キーをご利用の無線 LAN 環境にも簡単に接続できます。

無線 LAN の利点は、コンピューターやスマートフォン端末と電波で通信するために、電波が届く範囲であれば自由にネットワークへ接続できることです。その反面、セキュリティーの設定を適切に行わないと、悪意のある第三者によって以下のような問題が発生する場合があります。

- 印刷データやスキャンデータ、ID やパスワードなどの個人情報が盗み見られる（盗聴）
- 通信内容が不正に書き換えられてしまう（改ざん）
- 特定の人物や機器になりすまして通信が行われる（なりすまし）



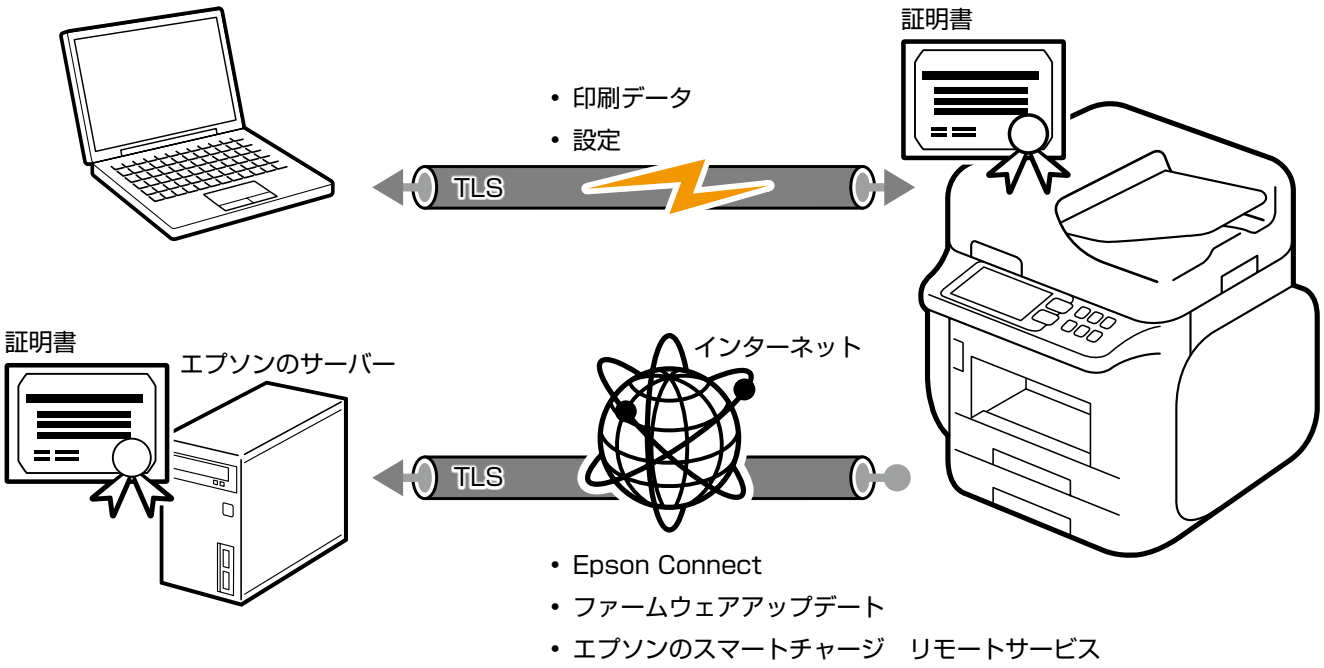
無線 LAN のセットアップ手順は、製品のマニュアルをご覧ください。

4. ネットワークセキュリティー

4-1. TLS 通信

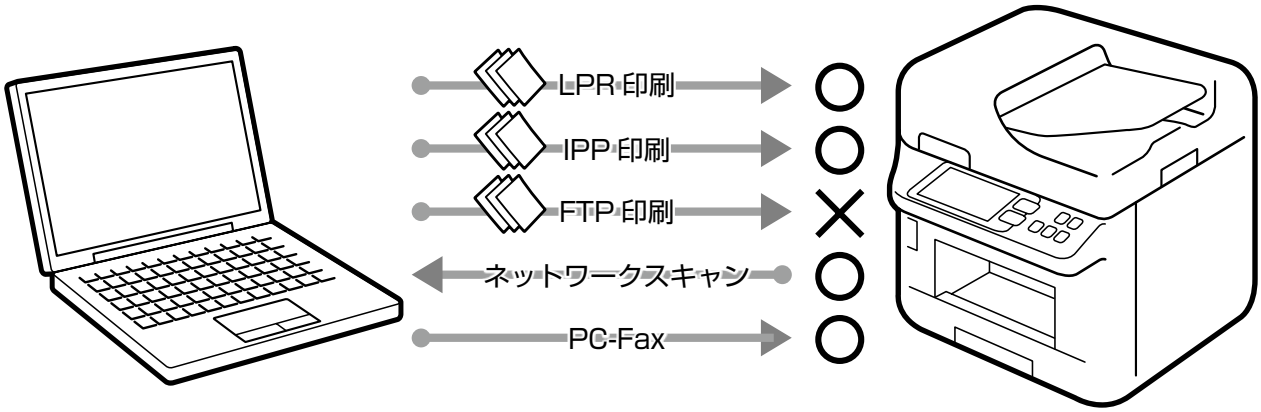
ブラウザー経由での製品の設定や IPPS プロトコルでの印刷では、通信の内容が TLS によって保護されるため、設定情報や印刷データ内容の漏えいが防げます。CA 署名証明書のインポートによるサーバー検証機能を使って社内の認証基盤 (PKI) と連携することで、不正な機器への情報送信も防げます。暗号強度は、より安全性の高い暗号化アルゴリズムを使用するよう設定できます。また、Epson Connect やファームウェアアップデートなどで製品からインターネット上のエプソンサーバーにアクセスする場合も TLS で保護されます。

TLS のバージョンは、TLS1.1/TLS1.2/TLS1.3 に対応しています。また、使用する TLS のバージョンと暗号強度を選択できます。



4-2. プロトコルの許可・禁止制御

製品は、印刷、スキャン、PC-FAX 送信時にさまざまなプロトコルで通信を行います。各プロトコルや機能は個別に許可と禁止の設定ができ、意図されない利用によるセキュリティーリスクを未然に防ぐことができます。



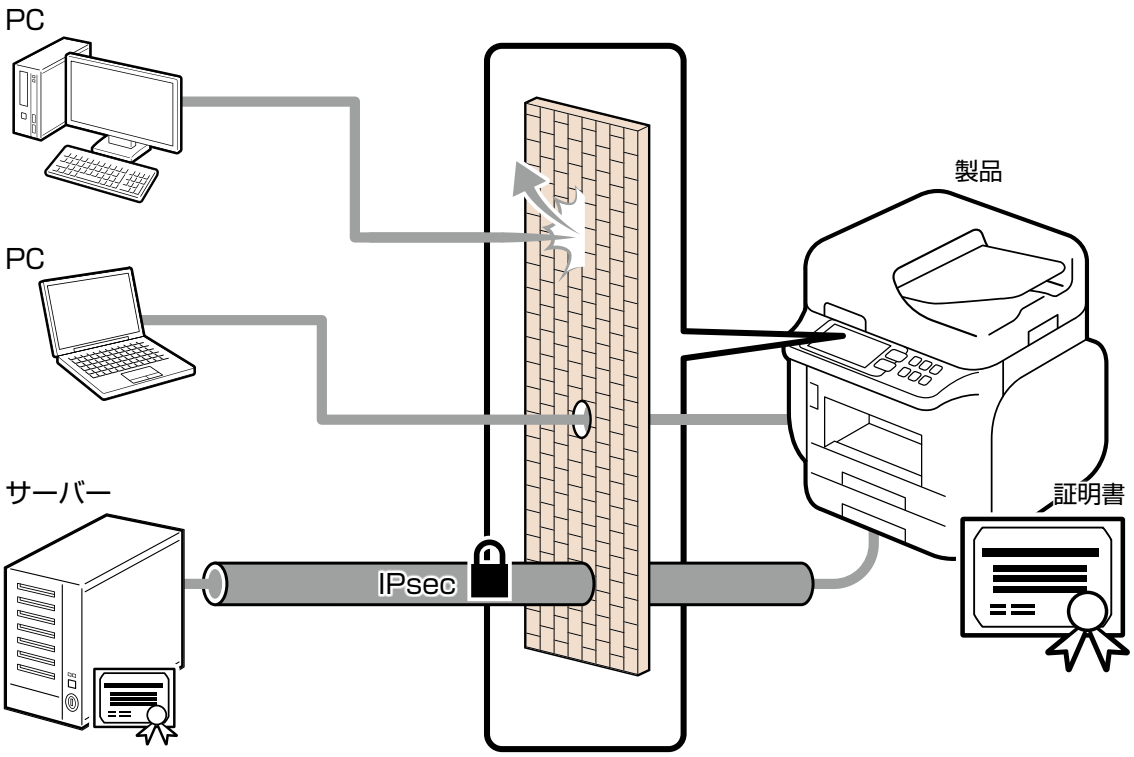
禁止できるプロトコルおよび機能は以下の通りです。

- Bonjour
- SLP
- WSD
- LLTD
- LLMNR
- LPR
- RAW（Port9100/ 任意ポート）
- IPP/IPPS
- FTP
- SNMP
- SSL/TLS
- Microsoft ネットワーク共有
- ネットワークスキャン（EPSON Scan）
- PC-FAX

4-3. IPsec/IP フィルタリング

IPsec/IP フィルタリング機能を使用すると、IP アドレス、サービスの種類、受信や送信のポート番号などでフィルタリングができます。これらを組み合わせることによって、特定のクライアントからのデータや特定の種類のデータを通過させるか遮断するか、設定することができます。さらに IPsec による保護を組み合わせることで、より強固なセキュリティー通信ができます。

IPsec による保護には、IP パケット単位での保護（暗号化および認証）が含まれるため、セキュアでない印刷プロトコルやスキャンプロトコルも保護の対象になります。IPsec の認証方式では、事前共有キーと証明書がサポートされています。



サポートされている鍵交換方式およびアルゴリズムは以下の通りです。

鍵交換方式

- IKEv1
- IKEv2

ESP 暗号アルゴリズム

- AES-CBC-128
- AES-CBC-192
- AES-CBC-256
- AES-GCM-128
- AES-GCM-192
- AES-GCM-256
- 3DES

ESP および AH 認証アルゴリズム

- SHA-1
- SHA-256
- SHA-384
- SHA-512
- MD5

基本ポリシーは製品にアクセスする全てのクライアントに影響します。より細かくアクセスを制御するには、個別ポリシーを設定します。

4-4. IEEE802.1X 認証

IEEE802.1X は、ネットワーク機器のポート毎にアクセス制御をおこなうための規格です。IEEE802.1X によるネットワークは RADIUS サーバー（認証サーバー）と認証機能を持ったスイッチングハブによって構成されます。

エプソンの製品は IEEE802.1X ネットワークへの接続が可能なため、機密性が高い情報を扱うネットワーク環境で安全にご使用いただけます。

以下の認証方式および暗号アルゴリズムをサポートしています。

認証方式

- EAP-TLS
- PEAP-TLS
- PEAP/MSCHAPv2
- EAP-TTLS

暗号アルゴリズム

- AES128
- AES256
- 3DES
- RC4

4-5. SNMPv3

SNMPv3 を使うと、対応する機器管理ツールとの状態監視や設定変更の SNMP 通信（パケット）を認証・暗号化できます。ネットワーク経由での設定変更や、状態監視での機密性が確保できます。

4-6. WPA3

最新の Wi-Fi（無線 LAN）の認証 / 暗号化技術である WPA3 に対応しています。WPA3 を使用することで、情報漏えいのリスクをさらに低くすることができます。

4-7. インターフェイス間の分離

製品は、USB インターフェイス、標準有線 LAN インターフェイス、増設有線 LAN インターフェイス、無線 LAN インターフェイス、公衆電話回線インターフェイスなどを持っています。それぞれのインターフェイスは独立していて、直接転送機能やルーティング機能は搭載されていません。よって、製品を介して公衆電話回線からネットワークへの侵入、無線 LAN から有線 LAN へのアクセス、インターネットからコンピューター経由で USB 接続された製品への不正アクセス、のようなリスクはありません。

5. 本体接続の保護

5-1. コンピューターとの USB 接続の ON/OFF

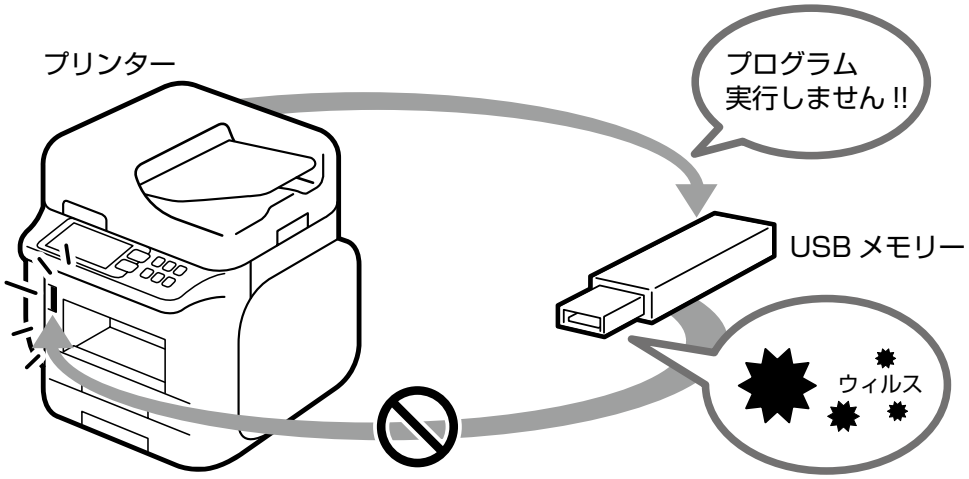
コンピューターからの USB 接続による製品へのアクセスを無効にできます。ネットワークを経由せずに直接コンピューターからの印刷やスキャンを禁止したいときに設定します。

5-2. 外部メモリーインターフェイスの ON/OFF

メモリーカードや USB メモリーのインターフェイスを無効にすることができます。オフィス内にある機密文書の不正なスキャンによるデータ持ち出しを未然に防止できます。

5-3. USB メモリーを介してのウイルスへの対応

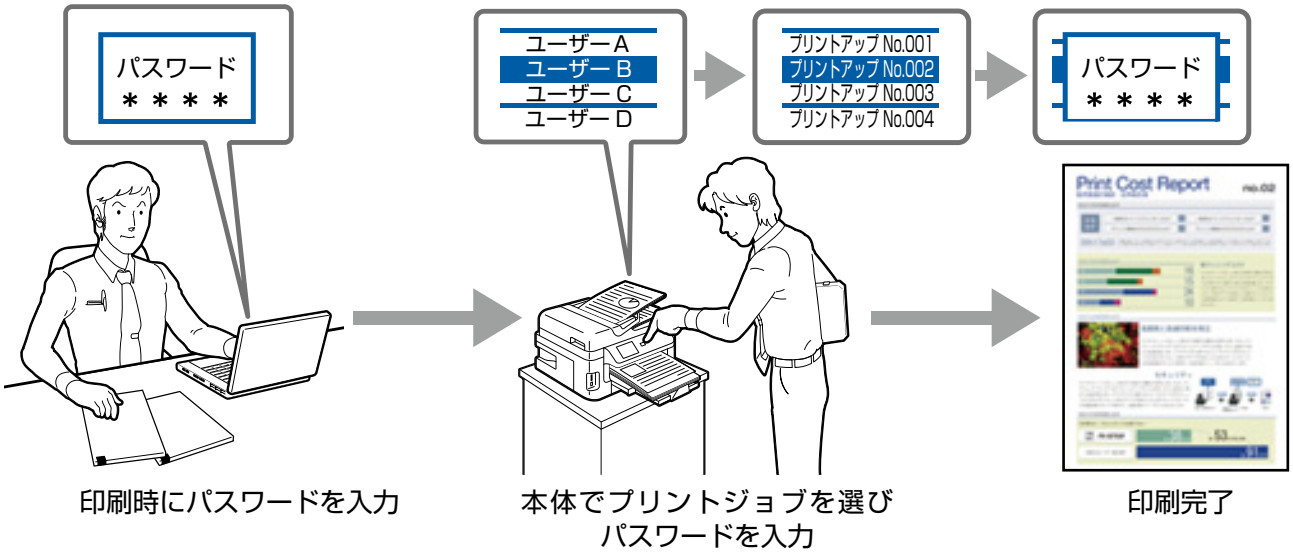
エプソンの製品には USB メモリー内のプログラム実行機能がないため、USB メモリーを介した製品へのウイルス感染の危険性はありません。



6. 印刷、スキャンのセキュリティー

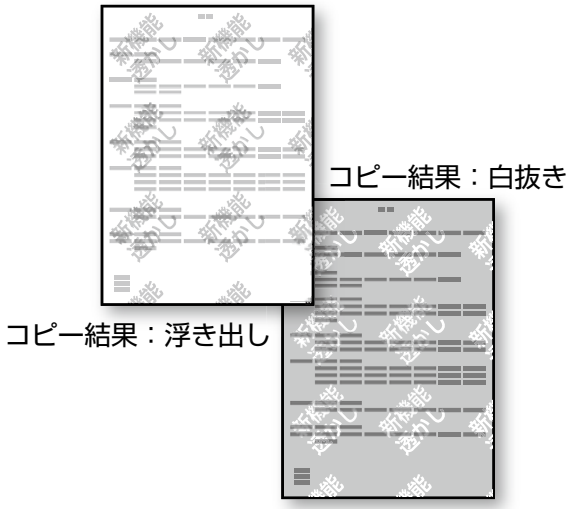
6-1. パスワード印刷

プリンタードライバーでパスワードを設定して印刷する「パスワード印刷」を使うと、出力用紙の不正閲覧による情報漏えいが防止できます。



6-2. 透かし印刷

透かし印刷を使ってコンピューターから印刷すると、透かしパターン（地紋）が埋め込まれた原本が作成できます。この原本をコピーやスキャンすると「コピー」や「複写」といった文字が浮き上がるため、原文かコピーかが一目で見分けられ、コピーによる不正利用が抑制できます。

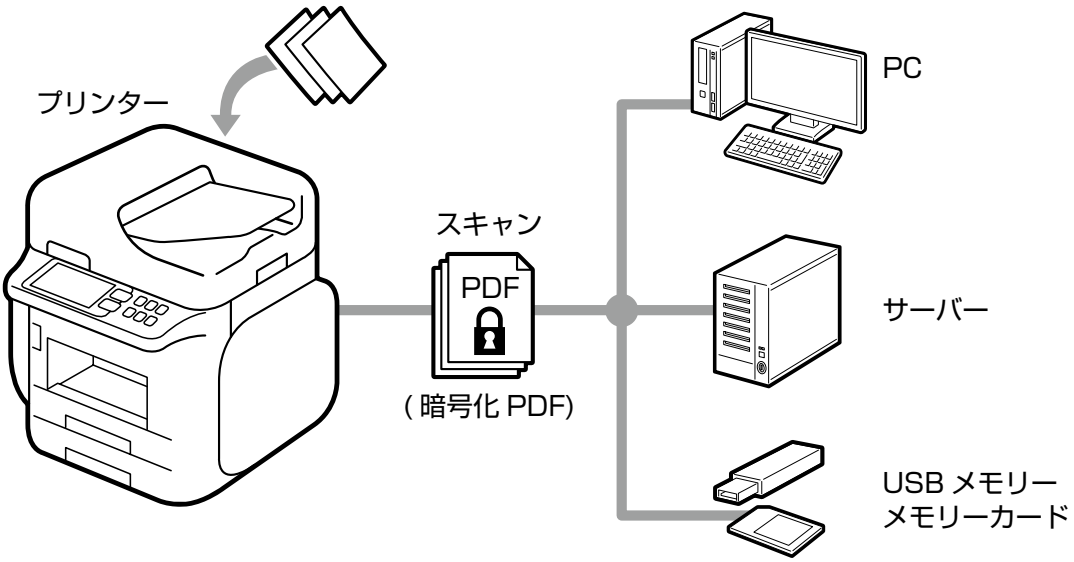


6-3. スタンプマーク機能

マル秘、重要などのスタンプマーク（テキストまたは BMP 形式）を文書に重ねて印刷することができます。さらに「ユーザー名」または「コンピューター名」も選択できます。文書の取り扱いの注意を受け手に喚起させることで、不正利用を抑止します。

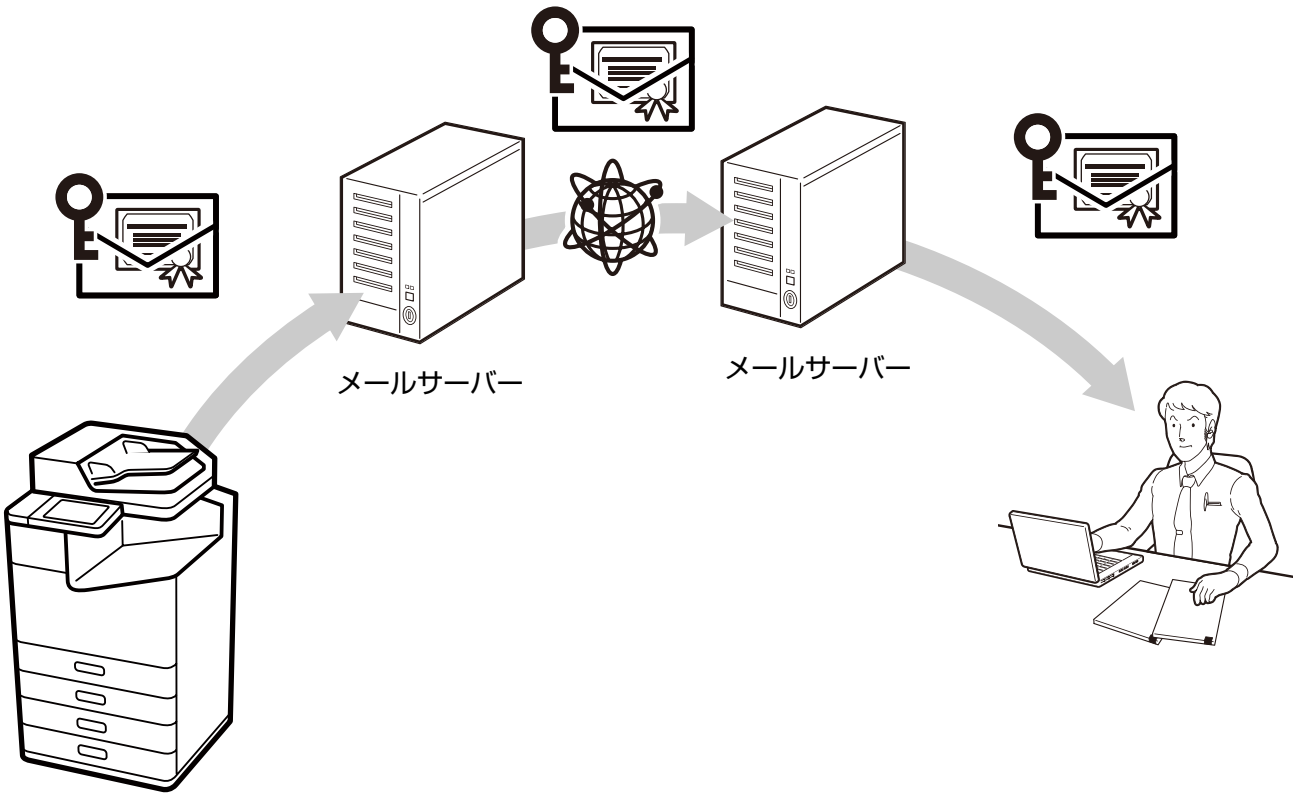
6-4. 暗号化 PDF

スキャンしたデータを暗号化 PDF に変換できます。これにより、スキャンした文書の第三者による不正閲覧が防止できます。



6-5. S/MIME

S/MIME を使用すると、スキャン to メール機能やファクス転送のメール機能において、メールに電子署名を付与したり暗号化したりできます。メールが複数のメールサーバーを経由する場合でも、メールを偽造や盗聴、改ざんから保護することができます。



サポートしているアルゴリズムは以下の通りです。

暗号化アルゴリズム

- AES-128
- AES-192
- AES-256
- 3DES

電子署名のハッシュアルゴリズム

- SHA-1
- SHA-256
- SHA-384
- SHA-512
- MD5

6-6. メールアドレス宛先ドメイン制限

メールアドレスのドメイン名に制限ルールを適用することで、スキャン to メール機能やファクス転送のメール機能において、誤送信による情報漏えいのリスクを軽減できます。

6-7. スキャン to フォルダー機能、スキャン to メール機能、メール通知の認証パスワード

近年、パスワード強度を高めるために長いパスワードを設定することが推奨されています。スキャン to フォルダー機能、スキャン to メール機能、メール通知で使用する認証パスワードを最大 70 文字まで設定できるようになりました。これにより、ファイルサーバーやメールサーバーにより長いパスワードを設定して運用することができます。

6-8. PDL からのファイルアクセスのデフォルト無効化

PDL（ページ記述言語）からのファイルアクセスを無効化することで、プリンター内部のファイルを盗み取る悪意のある印刷データからの情報漏洩リスクを防ぎます。もしも悪意のある印刷データが送られたとしても、ファイルを読み取られることなく製品を安全に使用できます。

6-9. セキュア印刷

印刷の通信経路をセキュアに保護したい場合は、TLS によって暗号化された IPPS が利用できます。

7. ファクスセキュリティー

7-1. 直接ダイヤル制限

電話番号を直接テンキーで入力する場合、宛先を２回入力して一致したときのみファクス送信するように設定できます。また、電話番号を直接テンキーで入力することを禁止し、ワンタッチダイヤルやアドレス帳に登録されている宛先にのみファクス送信できるように設定することもできます。電話番号の入力ミスによる誤送信の情報漏えいリスクが軽減できます。

この機能は、情報通信ネットワーク産業協会が制定したガイドライン「FASEC1」に準拠しています。

7-2. 宛先一覧確認

ファクス送信前に選択した宛先を確認することができます。宛先の指定ミスによる誤送信での情報漏えいのリスクが軽減できます。

この機能は、情報通信ネットワーク産業協会が制定したガイドライン「FASEC1」に準拠しています。

7-3. ダイヤルトーン検出

ダイヤルトーン（交換機が発信する、発呼可能を知らせる音）が検出できたことを確認してからファクス送信するため、誤送信が防止できます。

この機能は、情報通信ネットワーク産業協会が制定したガイドライン「FASEC1」に準拠しています。

7-4. 受信ファクスの放置対策

「見てからファクス印刷」は、受信したファクスを受信ボックスに保存（メモリー受信）し、操作パネルで確認してから印刷するよう設定できます。これにより、印刷された受信ファクスがそのまま放置されることによる情報漏えいや、受信ファクス印刷物の紛失を防止します。

また、受信ボックスへのアクセス時にパスワードを要求するよう設定すると、不正利用者による勝手な印刷や削除を防止します。

この機能は、情報通信ネットワーク産業協会が制定したガイドライン「FASEC1」に準拠しています。

7-5. 送信確認レポート

通信結果レポート、転送結果レポート、通信管理レポートなど、送信内容を確認できるレポートを印刷することで、正しい宛先に確実にファクス送信されたか確認できます。

この機能は、情報通信ネットワーク産業協会が制定したガイドライン「FASEC1」に準拠しています。

7-6. ファクス受信データのバックアップ消去

ファクス受信データのバックアップデータ※は操作パネルから消去できます。また、バックアップデータを自動消去するように設定することもでき、ファクス受信データの不正な再印刷を防止できます。

※ファクス受信データのバックアップデータは、印刷結果が不鮮明な場合や印刷結果を紛失した場合に再印刷できるよう、製品内に保持されています（工場出荷設定）。

7-7. 複数宛先送信の制限

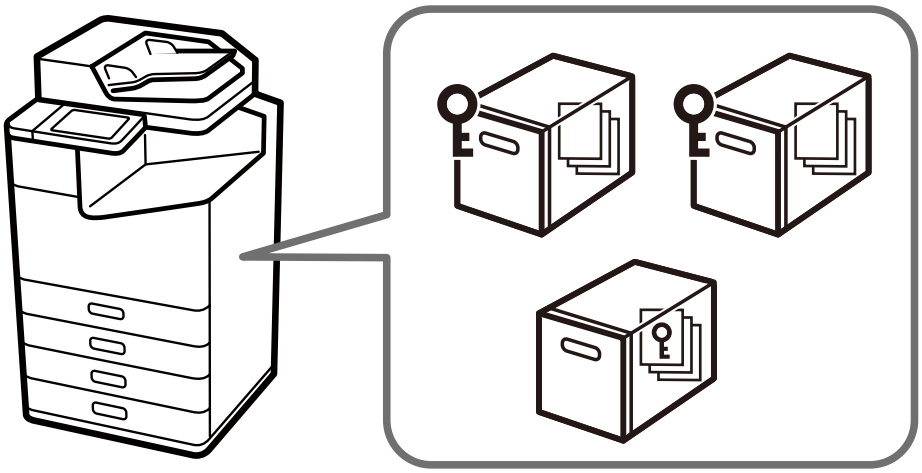
宛先を 1 カ所しか選択できないように設定できます。

複数の宛先を指定できないようにすることで、意図しない宛先への誤送信や情報漏えいリスクが軽減できます。

8. ユーザーデータの保護

8-1. ボックスのセキュリティー

ボックスを搭載している機種では、共有ボックスや文書に固有のパスワードを設定できます。パスワードにより、情報漏えいや紛失、文書の不正な改ざんを防止することができます。また、ボックス操作を利用者制限の対象にできます。共有ボックスを使用しない場合は、共有ボックス機能を使用禁止にすることもできます。



8-2. アドレス帳の保護

製品のアドレス帳の一括編集時に、管理者パスワードが要求されるため（管理者パスワード設定時）、アドレス帳情報の漏えいや不正な改ざんが防止できます。また、一括読み出し（エクスポート）は暗号化ファイルとして保存できるため、製品の入れ替えやバックアップ時に、ファクス番号やメールアドレスなどの個人情報の漏えいが防止できます。

8-3. 製品が処理する文書データの取り扱い

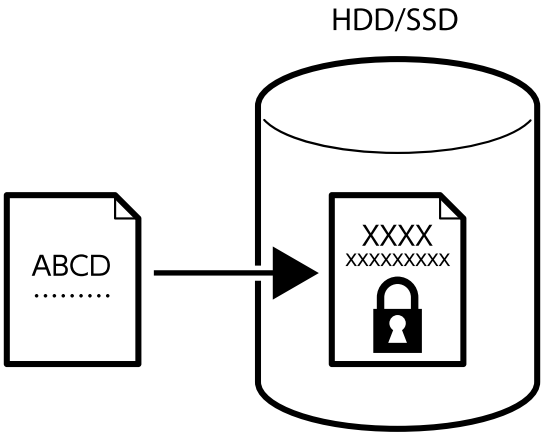
印刷・コピー・スキャンのデータは製品内に一時的に保持されますが、目的のジョブが終了したとき、または機器の電源が切れたときに消去されます。

また、ファクスデータは送受信が完了すると消去されます。なお、ファクス受信データはバックアップ機能によりデータを保持していますが、設定を変更することで自動消去するようにできます（7-6参照）。

8-4. HDD/SSD へ記録するデータの暗号化

本体内蔵の HDD/SSD にデータ記録する際、常に暗号化してお客様のデータを保護しています。万が一、悪意のある第三者に攻撃されても、そのままのデータが見えることはありません。また、もしも HDD/SSD が盗難にあったとしてもお客様の重要な情報は漏えいしません。

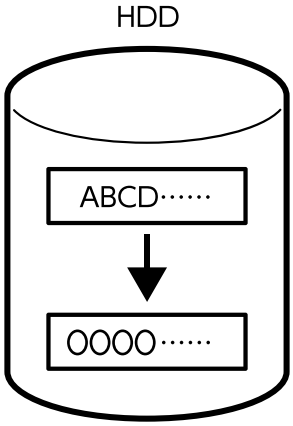
HDD/SSD は自己暗号化ドライブが搭載されており、文書データは AES-256 で暗号化されます。



8-5. ジョブデータの逐次消去

この機能を有効にすると、本体のハードディスクに一時記録されたジョブデータは、特定パターンで上書き消去され、復元することができなくなります。これにより、悪意のある第三者による残存ジョブデータからのデータ復元を防止できます。

また、ハードディスク全体を消去する際には、「自己暗号化ドライブ内部のキー変更による消去（Secure Erase）」と、「キー変更による消去と空の値 (0) で上書き消去（完全な消去）」の２つから選択できます。



8-6. パスワード暗号化

製品内部に保持されるパスワードを暗号化できます。暗号化する情報は以下の通りです。

- 管理者パスワード
- 利用者制限ユーザーのパスワード
- スキャン to ネットワークフォルダー機能の共有フォルダーにアクセスする際の認証パスワード、および証明書の秘密鍵など

8-7. TPM

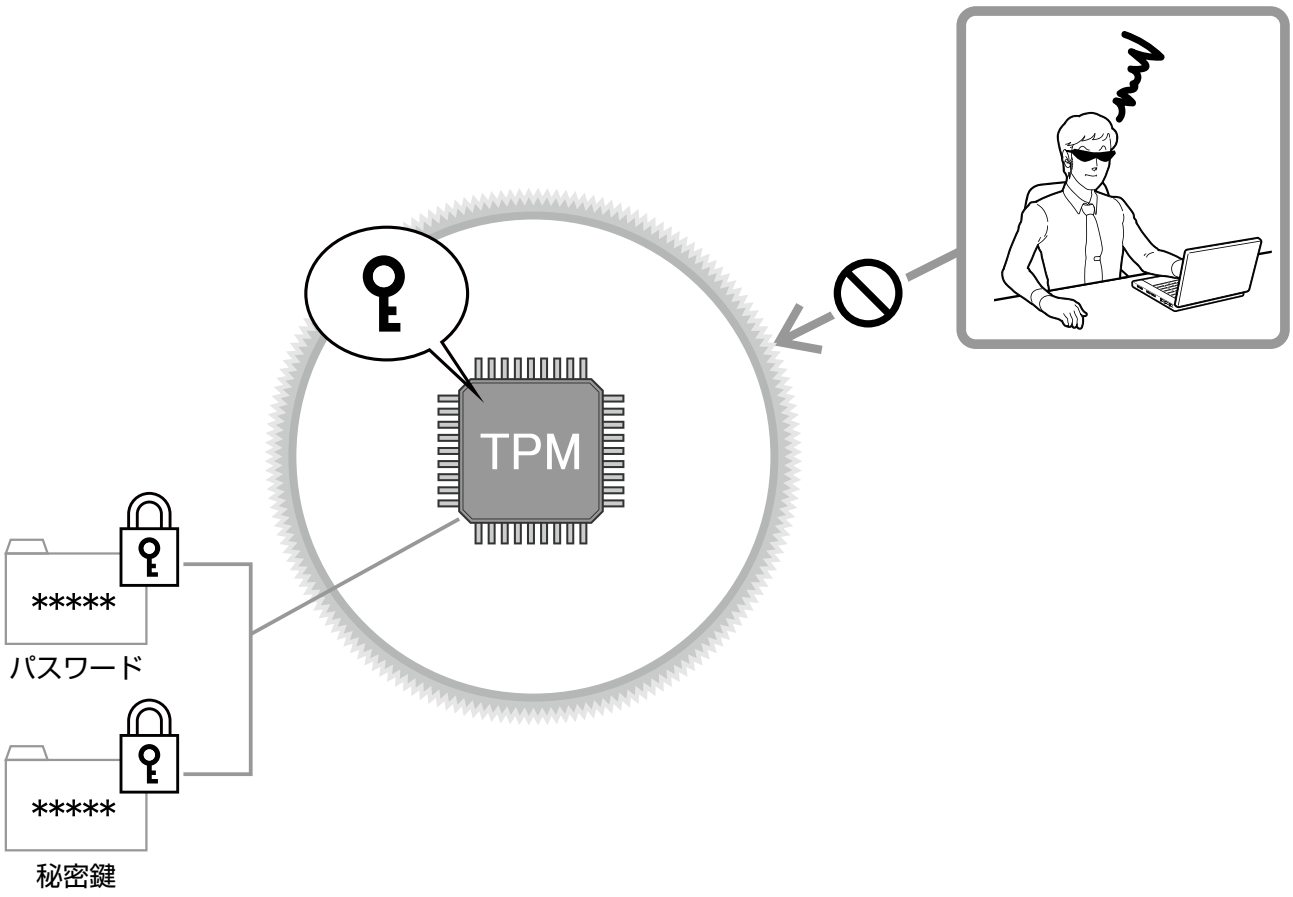
TPM（Trusted Platform Module）搭載機種では、以下のようにセキュリティーレベルが向上します。

暗号化されたパスワードや秘密鍵の情報を復元するための暗号キーが TPM チップに保存されます。TPM チップには、プリンター外部からはアクセスできないため、ハードウェアレベルの不正な解析から保護できます。

ブラウザー経由の設定（Web Config）のセッションで使用される乱数に、TPM の真正乱数が使用されます。

暗号化 HDD/SSD の認証キーの生成に、TPM の真正乱数が使用されます。

製品は、TPM2.0 チップを搭載しています。



8-8. ハードディスクのミラーリング

オプションの増設ハードディスクを搭載すると、1 台のハードディスクが故障した場合でも保存したデータを失うことなく、もう 1 台のハードディスクで全ての機能を継続して使用できます。

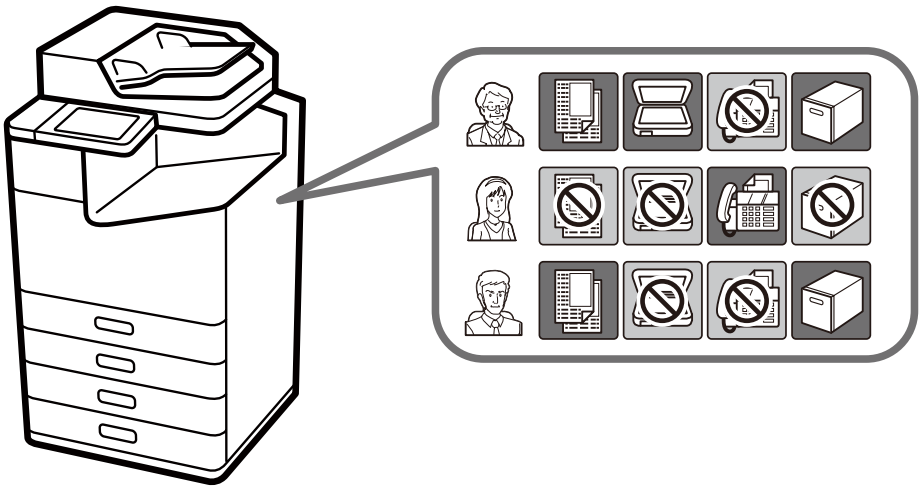
9. 操作の制限 – 不正利用の防止 –

9-1. パネルロック

パネルロックを使用すると、本体パネルからの各種設定変更時に管理者パスワードの入力が必要になります。オープンオフィスや公共施設等において、本体パネルから直接設定画面に入ることができなくなるため、利用者による設定変更を防止できます。

9-2. 利用者制限

ユーザーごとに、印刷、スキャン、コピー、ファクス※、ボックスの機能を制限することができます。ユーザーの業務内容や役割に応じた最小限の機能のみを許可することで、文書データの漏えいや不正閲覧のリスクが低減できます。また、操作パネルからのログイン後、一定時間操作がないと自動でログアウトされます。

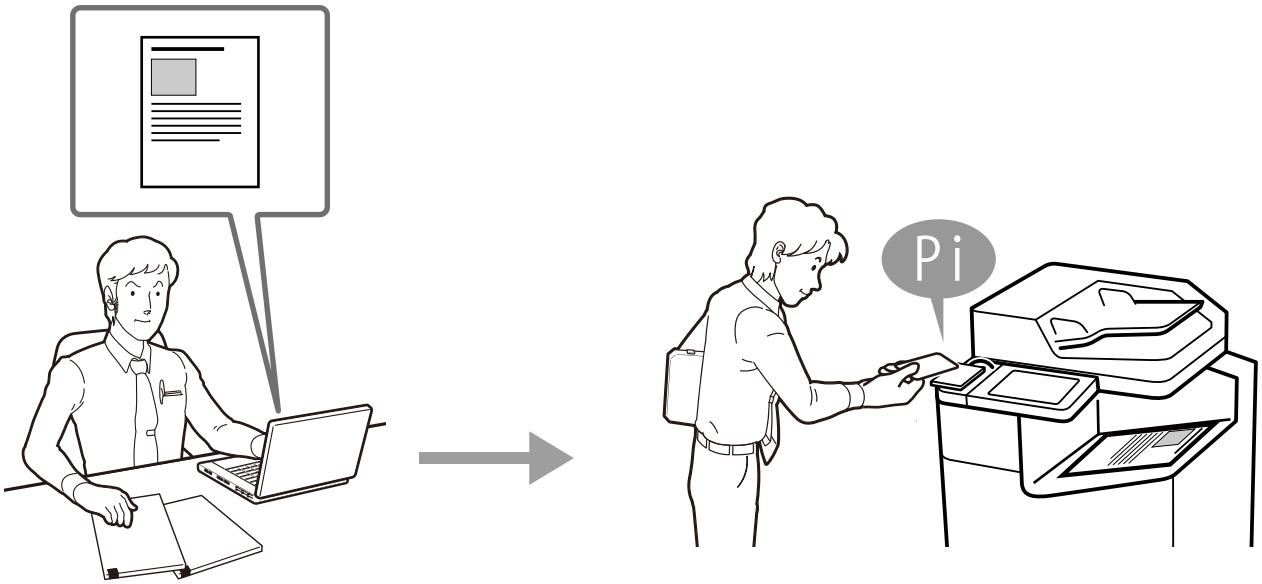


※ファクスは、送信のみ利用者制限がかけられます。

9-3. 認証印刷／認証スキャン

オプションの Epson Print Admin（エプソン プリント アドミン）/Epson Print Admin Serverless（エプソン プリント アドミン サーバーレス）を導入すると、IC カードなどの認証装置を使って、目の前で認証して印刷ができます。印刷物が放置されることによる取り違えや、印刷物からの情報漏えいが防止できます。

認証方式として、LDAP 連携、本体登録ユーザー、みなし認証が使用できます。



9-4. パスワードポリシー

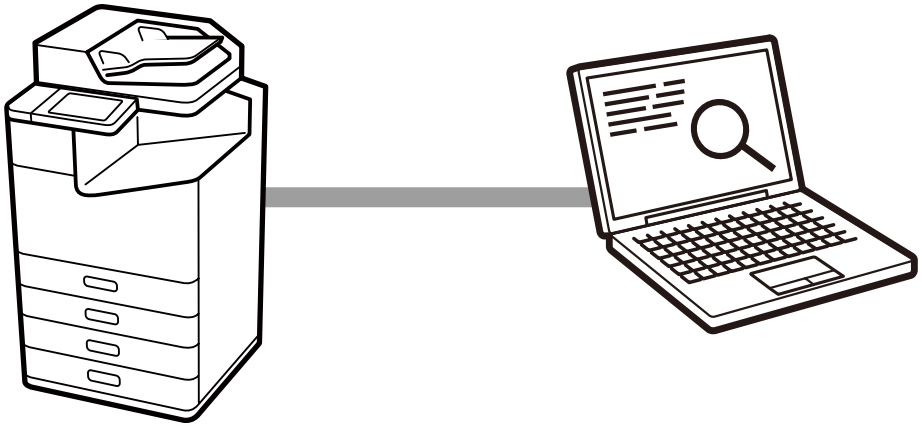
管理者パスワード、利用者制限パスワード、ファクスボックスパスワードにパスワードポリシーを設定できます。下記のように文字数や、文字種の組み合わせなどの条件を設定することで、パスワードの漏えいリスクを軽減できます。

- パスワードの最少文字数
- パスワードに英大文字を含める / 含めない
- パスワードに英小文字を含める / 含めない
- パスワードに数字を含める / 含めない
- パスワードに記号を含める / 含めない

9-5. 監査ログ

印刷、コピー、スキャン、ファクス送受信の履歴や設定変更の記録を、本体に監査ログとして記録できます。定期的に監査ログを確認することで、不正利用の早期発見やインシデント（セキュリティー上の問題）発生後の追跡調査が可能です。

なお、監査ログは最大 20,000 件保持されます。



10. 本体セキュリティー

10-1.自動ファームウェアアップデート

自動ファームウェアアップデートを設定すると、指定日時にファームウェアを自動更新することができます。指定日時に更新されるので、業務に支障をきたすことなく、常に最新のファームウェアをご利用いただけます。

10-2.不正なファームウェアアップデートに対する保護

ファームウェアアップデート時に管理者パスワードによる認証を行い、ファームウェアを書き換える前に製品本体へ送信されたファームウェアが正規のものか署名により検証します。また、製品との通信は HTTPS で保護されます。これにより、悪意のある第三者からの不正なファームウェアの変更を防止します。

10-3.セキュアブート

起動時に製品のファームウェアが正規のものか署名により検証します。不正なファームウェアに書き換えられていることを検知した場合は、起動を停止してファームウェアのアップデートを促します。

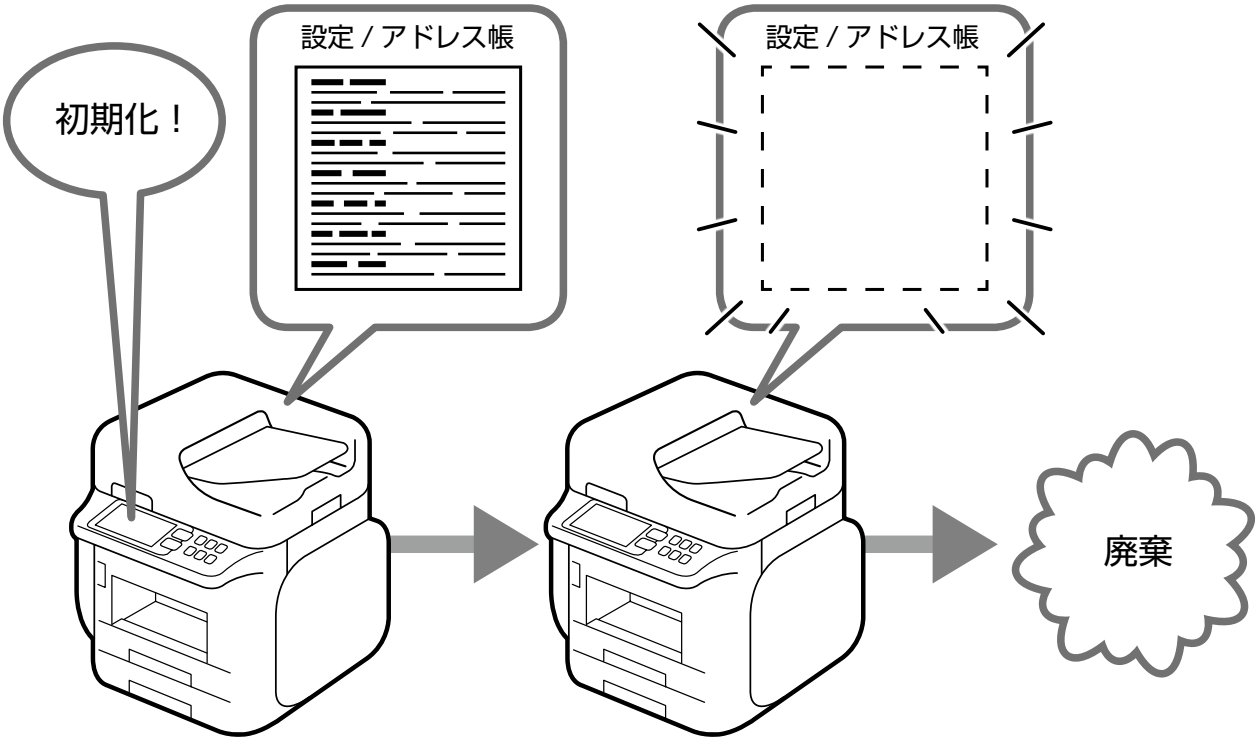
10-4.マルウェア侵入検知

製品の動作中ファームウェア内にマルウェアが侵入していないか常に監視しています。マルウェアを検知した場合は、再起動して不正なマルウェアを排除します。

11. 譲渡、廃棄時のセキュリティー対策

11-1.本体の初期化

本体の廃棄や譲渡時には、機密情報漏えい防止のために、全ての設定や本体に記録されているデータ（本体内蔵 HDD/SSD を含む）を工場出荷時の状態に戻すこと（初期化）ができます。



12. セキュリティー規格への準拠

12-1.ISO15408/IEEE2600.2™

ISO/IEC 15408 認証取得製品は、情報セキュリティーに関する国際的な規格である IEEE Std. 2600.2™-2009 ※1 に適合しています。

IEEE Std. 2600.2™

IEEE Std. 2600.2™ とは、複合機・プリンターが備えるべき情報セキュリティーの要求仕様を規定した国際的な規格です。主要なセキュリティー機能として、「ユーザー識別認証機能」「アクセス制御機能」「残存データ消去機能」「ネットワーク保護機能」「セキュリティー管理機能」「自己テスト機能」「監査ログ機能」などがあり、この規格に準拠することで、複合機・プリンターのセキュリティー機能を総合的に強化することができます。

ISO/IEC 15408

ISO/IEC 15408 は、CC：Common Criteria とも呼称されており、IT 製品やシステムが適切に設計され、その設計が正しく実装されていることを第三者機関が客観的に評価する国際的な規格です。

ISO/IEC 15408 認証は、ファームウェアやマニュアル等の構成要素バージョンを特定し評価されます。ご購入時の製品のファームウェアバージョンは、認証されたバージョンと異なる場合があります。

認証バージョンでご使用の場合、製品の機能を一部制限させていただくことがあります。

本（CCRA）認証マークは、本製品の評価が「IT セキュリティ評価及び認証制度（JISEC*2）」の定めに従って実施されたこと、および本製品に対する評価結果が検証されたことを示すものであり、本製品に脆弱性が全くないことの保証および特定の運用環境で必要なすべてのセキュリティー機能が装備されていることの保証を意味するものではありません。

※1：U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0（IEEE Std. 2600.2™-2009）

※2：JISEC (Japan Information Technology Security Evaluation and Certification Scheme)

EPSON エプソン販売株式会社 〒160-8801 東京都新宿区新宿四丁目1番6号 JR新宿ミライナタワー
セイコーエプソン株式会社 〒392-8502 長野県諏訪市大和3-3-5

NPD6296-03 JA

2022 年 12 月発行