Konica Minolta Security White Paper

セキュリティ基本方針と

対応技術に関する報告書

Version 7.0.1

July 30, 2013

KONICA MINOLTA

コニカミノルタの製品は、セキュリティの面においてさまざまな技術を搭載しておりますが、コニカミノルタのセキュリティポリシーに従ったお客様による正しい運用が前提条件となります。本記載内容を参考に、コニカミノルタの製品を運用いただきたく何卒ご理解の程お願いいたします。各種設定については、ユーザーマニュアルをご覧下さい。また、ここに記された内容は万全なセキュリティを保証するものではないことをあらかじめご了承ください。

Active Directory は、マイクロソフト社の商標です。
VxWorks は、ウインドリバー社の登録商標です。
Adobe Acrobat は、アドビシステムズ社の登録商標です。
FeliCa は、ソニー株式会社の登録商標です。
Linux は、Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。

目次

第1章　はじめに

ネットワークの基盤が整備されITが普及した現在社会に於いては、膨大な情報が流通し、ビジネスの中心には、様々な形で情報が集まり、より高度な情報資産として姿を変え活用されています。企業活動に於いてはこの情報資産を守ること、即ちリスクをマネージすることが重要な課題となります。

本書では、コニカミノルタの bizhub, Konica Minolta, Sitios, DiALTA の各シリーズが提供するセキュリティ基本機能を紹介します。

Ⅰ. セキュリティ基本方針

1. セキュリティ最新技術の搭載

コニカミノルタは、次項に分類されるさまざまな脅威からお客様の情報資産を守るため、あらゆる角度から、最新のセキュリティ機能を開発・提供します。

① ネットワーク経由の不正アクセスと情報漏洩
② 機器の直接操作による不正使用と情報漏洩
③ 電子情報・紙情報の改竄、複製、消去
④ 人災、機器障害からの情報破壊
⑤ ログ等によるトレース機能

2. 第3者機関による認証取得

コニカミノルタは、セキュリティ機能の実装を客観的に証明する為、平成 16 年 3 月以降の MFP（A4/20枚機以上のほとんどの機種）において ISO15408 の認証を取得しています。

ISO15408 の認証取得は、初期の Firmware をベースに認証取得を実施します。
メンテナンスリリースなどの ROM をリリースした場合、今後保証継続制度は利用しないこととしますが、セキュリティ機能は、そのまま維持する様に対応します。

また、今回、搭載した MES（RSA BSAFE Micro Edition Suite）暗号モジュールが FIPS140-2 の認証を取得しました。
これにより、ソフトウェアが堅牢で安全であることが証明され、FIPS140-2 の認証を必須とする機関への販売が可能になります。（対象機種: C754/654/554/454/364/284/224）

Ⅰ. 公衆電話回線に対するセキュリティ

1. FAX 回線に対するセキュリティ

FAX 回線は FAX プロトコルのみを使用した通信であり、これ以外の通信プロトコルはサポートしておりません。
公衆回線を通して異なるプロトコルで外部より侵入された場合や FAX データとしては伸張できないデータを送付された場合には内部のソフトウェア処理でエラーとなり通信は遮断されます。

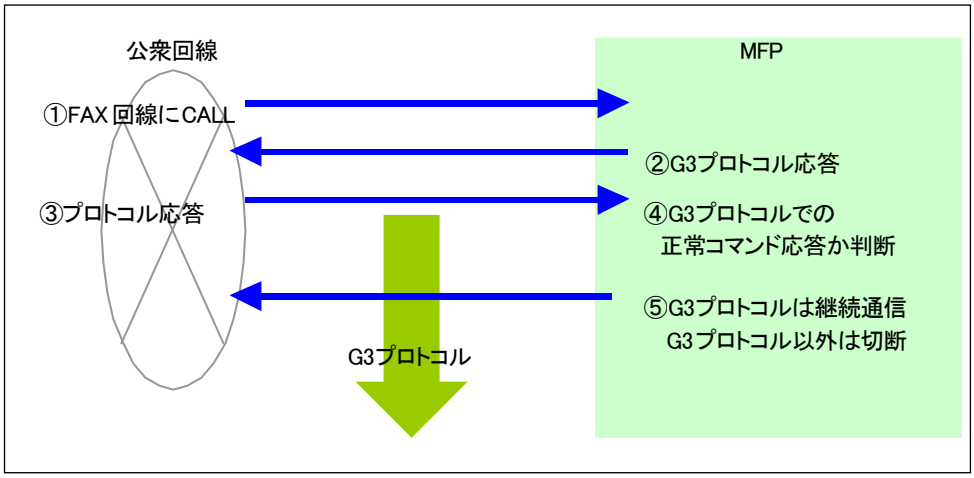


図1－1

2. 宛先2度入力

FAX 送信の宛先を電話番号で入力する場合、再度電話番号を入力し、一致することを確認することで、電話番号の入力間違いによる誤送信を防ぎます。
また、短縮番号へ電話番号を登録する場合にも、再度電話番号を入力し、一致することを確認することで、電話番号の入力間違いによる誤送信を防ぎます。

3. チェーンダイアル

FAX 送信時の宛先入力として、短縮番号やテンキーでの直接入力を組み合わせて行うことができるため、市外番号などを短縮番号に登録して利用することで、誤入力を防ぐことができます。

4. 宛先確認画面表示

送信の宛先（短縮番号、電話番号等）の入力時に、入力した宛先を再度操作パネルに表示/確認後に送信することで、誤送信を防ぎます。

5. 複数宛先禁止

送信時の宛先を入力を1宛先のみ許可する設定にすることで、意図しない宛先に送信することを防ぎます。

6. 相手機確認送信

FAX 送信開始時に、相手機から受信する FAX プロトコル信号（CSI）により相手機の電話番号を確認し、一致する場合のみ送信することで、より安全に送信することができます。

Ⅱ. LAN 接続に対するセキュリティ

1. ネットワークプロトコルに対する対応

ポートごとに動作 ON/OFF の設定が可能です。

必要でないポートは OFF することで外部からの侵入を防止できます。

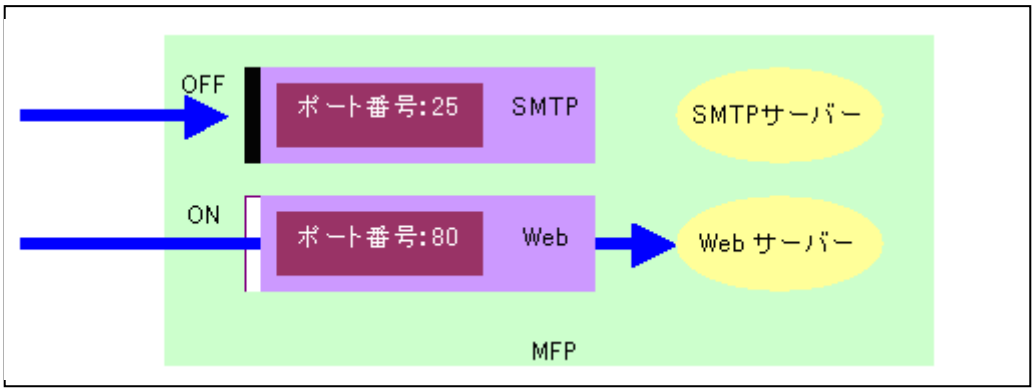


図2－1

また、IP アドレスのフィルタリング機能を持ち、アクセスを許可するアドレスと許可しないアドレスを指定する事により、アクセスを許可する機器をネットワーク上で選別する事が可能になります。

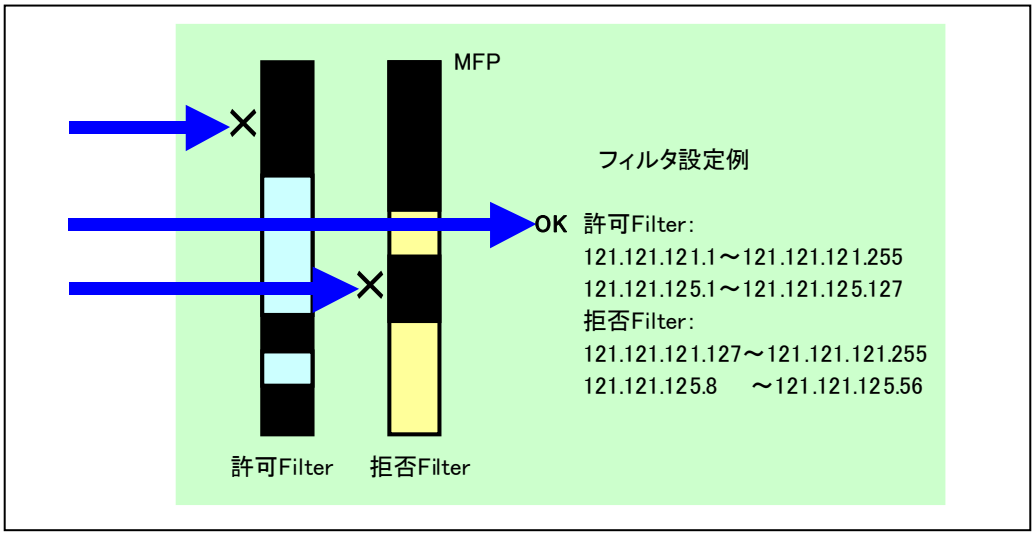


図２－２

2. ユーザー認証

Active Directory サービスを利用したネットワーク認証機能により、ネットワークを使用した機能に対してユーザー認証が可能です。また、ネットワークを使用した機能だけでなく、本体を使用する場合であっても、ユーザー認証設定で、Active Directory の認証設定がされている場合には、Active Directory での認証を行います。

予め登録されたユーザーとパスワードの組み合わせで使用権限が与えられます。

登録ユーザー以外は装置の使用ができない為、内部データの保護ができます。

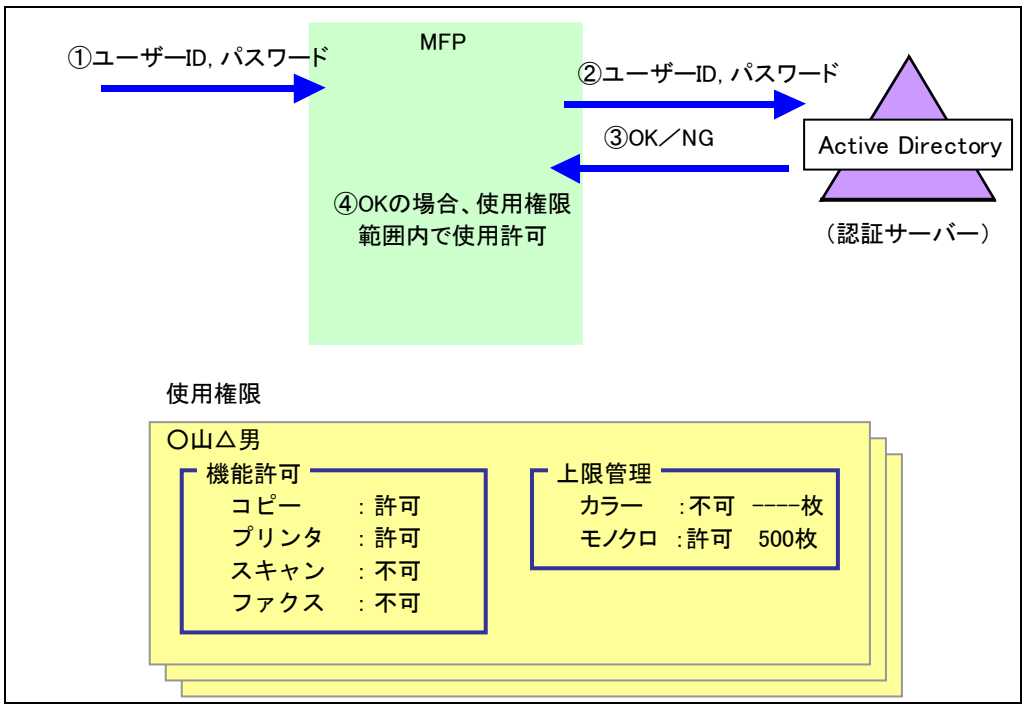


図2－3

3. ネットワーク経由の装置管理セキュリティ

(1) アドレス帳一括登録時のセキュリティ

ネットワークからのアドレス帳一括登録には、装置の管理者パスワードの入力を必要とします。装置の管理者パスワードが不正であれば登録できません。

この機能により本体に登録されているアドレス帳が一括で改竄されることを防ぐことができます。

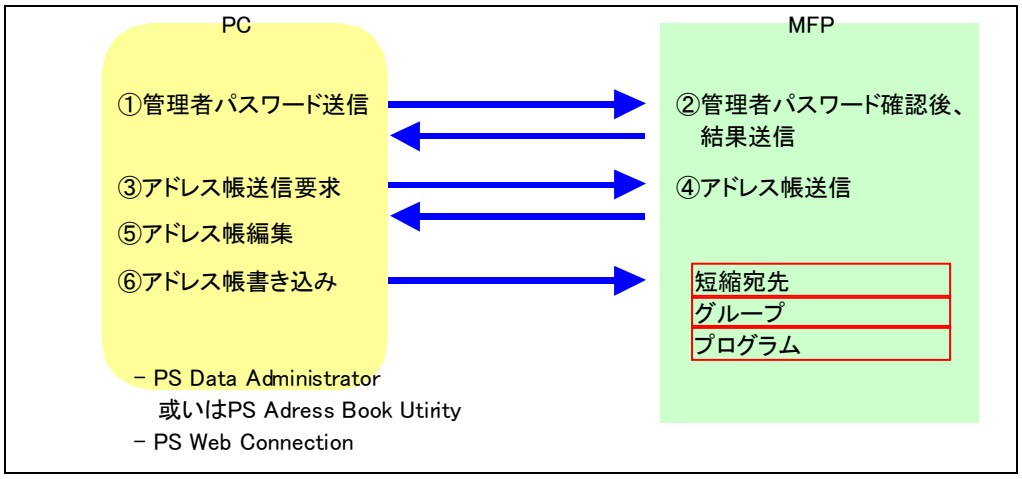


図2－4

(2) bizhub OpenAPI

bizhub OpenAPI では、SSL 暗号化プロトコルを使い、ネットワーク越しに装置の情報を取得／設定する事が可能となります。また、bizhub OpenAPI 独自のパスワードを設定する事で、より安全に通信を行う事ができます。

PageScope Data Administrator によるユーザー認証情報の設定は bizhub OpenAPI を使うことで、装置の安全を守ります。

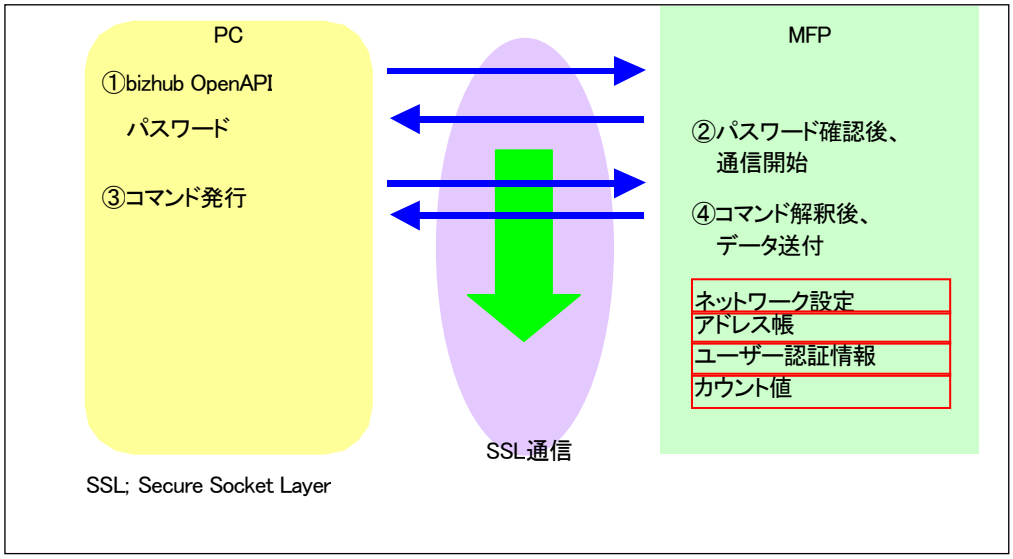


図2－5

4. データ通信の暗号化

LDAP サーバ、PageScope Data Administrator (或いは Address Book Utility)、PageScope Web Connection と本体間のデータ通信には、SSL 暗号化プロトコルを採用しています。ネットワーク間でやりとりするデータを暗号化することで内容を保護します。更に、通信プロトコルに依存しない、暗号化対応が可能である、IPsec の採用を行い、IPv6 化の対応と合わせた、通信の暗号化を行っています。

5. 検疫ネットワーク対応

LAN への接続段階で、ネットワーク機器の認証を行い、物理的なポートを対象として、MFP の LAN への接続を管理できる、IEEE802.1X 機能を有している。認証は、RADIUS (Remote Access Dial In User System)サーバで行われ、LAN への接続制御は、対応したスイッチングハブで行なわれます。本機能により、認証が許可された MFP だけが、LAN 環境への接続が許可されます。

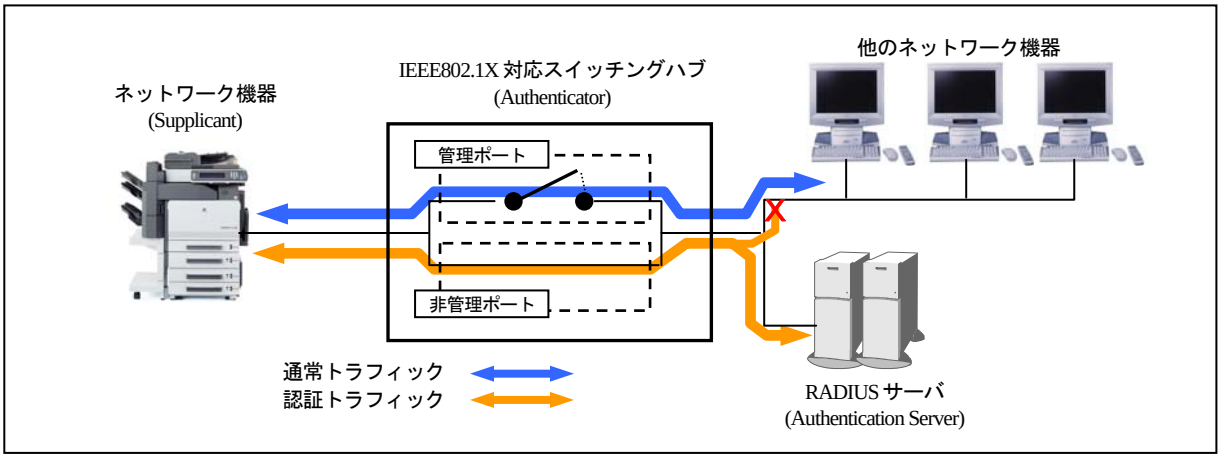


図2－6

6. 双方向証明書検証

従来の MFP は、自身の装置内にある証明書を、通信相手に通知し、MFP の正当性を確認する機能を有している。更に、通信相手の正当性を、MFP 装置自身が、検証する事で、双方向で正当性を確認した上で、通信制御を行い、MFP 及び通信相手の「なりすまし」防止を行います。

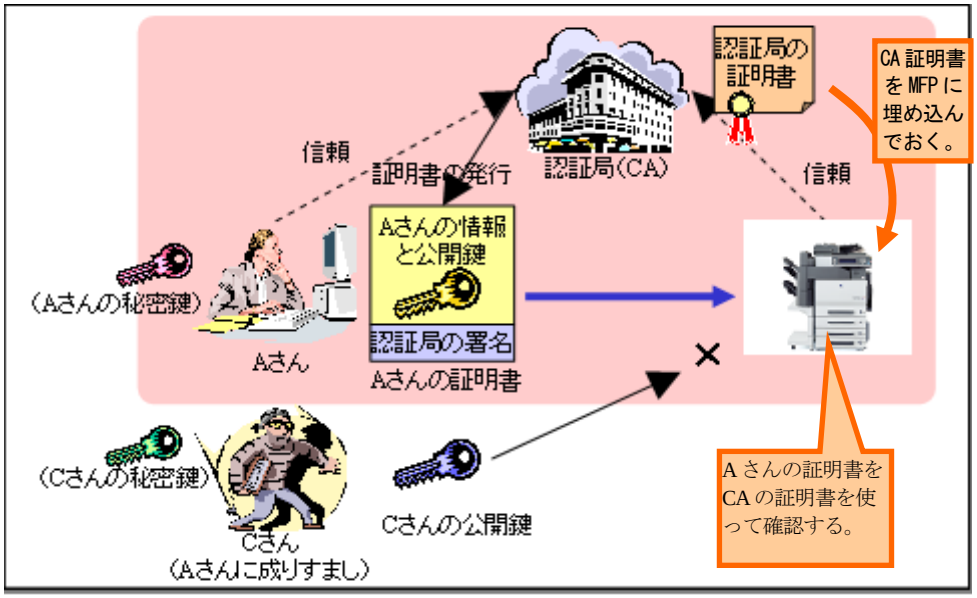


図2－7

7. ウイルスに対する対応

本体に内蔵しているコントローラの OS には機種により VxWorks または Linux kernel を採用しています。組み込み機器用の OS である VxWorks をターゲットとしたウィルスは稀有と考えられます。

EFI 社 fiery のサーバタイプコントローラは、Windows 系の OS を採用していますが、必要な Windows セキュリティーパッチを適時に供給することにより、Windows の脆弱性への対策を行っています。

8. 外部からの USB メモリを介してのウイルスへの対応状況

USB メモリを介してのウイルスは USB メモリを指しただけで実行されてしまいウイルス感染するケースが主ですが、MFP には USB メモリを指しただけで実行ファイルを起動するといった仕組みがありませんので、これらのウイルスによる影響はありません。

MFP には USB メモリを接続し、USB メモリの画像データをプリントする、またスキャンした画像データやボックスに保存された画像データを USB メモリに保存する機能がありますが、これらの機能はユーザーの操作によって実行されるもので、自動で実行するものではありません。

9. Linux kernel の定常的監視

Linux kernel については、脆弱性公開情報、及びセキュリティーパッチの有無を定常的に監視し、公開された脆弱性が MFP 機能に影響しないか確認しています。

Ⅲ. MFP 本体内データのセキュリティ

1. 画像処理及び出力処理におけるセキュリティ

スキャナから読み込んだデータは画像処理後圧縮され、本体内のメモリ（揮発性のDRAM）に書き込まれます。さらにプリントデータは伸張処理後プリンタへ送られ用紙上にプリントされます。データは１ページごとにメモリ上に重ね書きされるためデータの再出力は不可能です。

出力完了や転送完了と同時にメモリからジョブデータ（圧縮データ）が削除され、第三者による再出力、再転送を防止します。

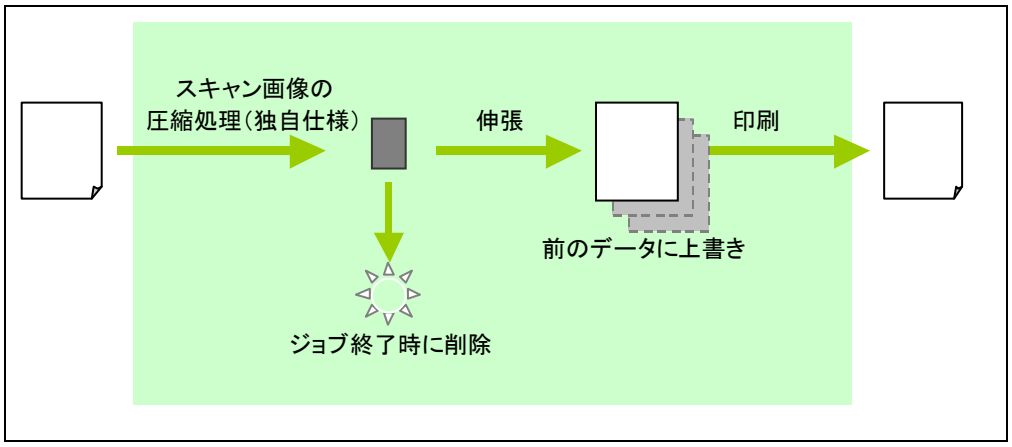


図3－1

HDD 内に蓄えられるジョブデータは、独自の圧縮データの形で保存されます。このため仮に内部データを読み出すことができても解析は極めて困難です。

また、HDD 内のデータは全て暗号化して保存されますので、万一 HDD を取り出されてもデータの機密性は保持されます。（オプション）

HDD はロックパスワードを利用すれば、万一 HDD を取り出されてもデータの機密性は保持されます。

セキュアプリント機能を使用した場合、プリントジョブは本体内のメモリに一旦保存され、本体のパネルでパスワードが入力されてからプリント動作を開始します。この機能により、本人以外がプリント用紙を持ち去ることを防止します。

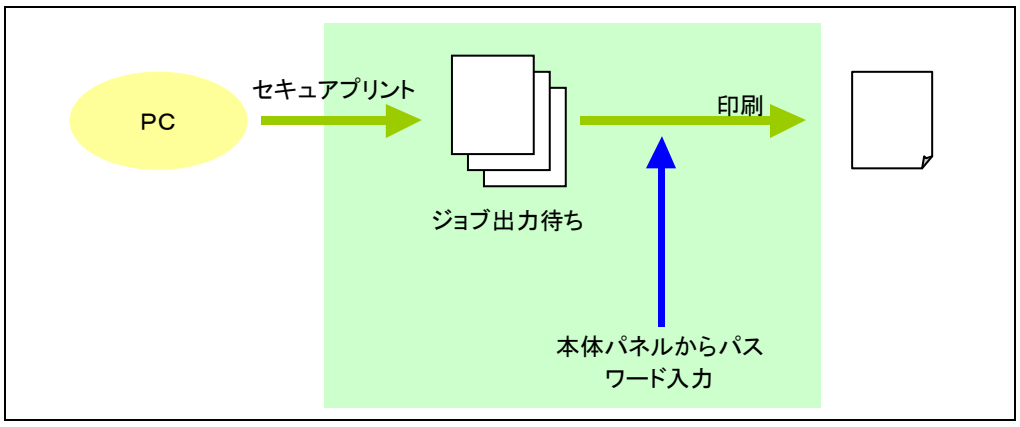


図3－2

2. ユーザー認証

本体に搭載した認証機能、Active Directory などの外部サーバや PageScope Authentication Manager を利用する認証をサポートしています。パスワードによる認証のほか、PageScope Authentication Manager を利用して非接触 IC カードやバイオメトリクスによる認証が可能です。

MFP のコピー、プリント、スキャン、ファックスの機能やカラー機能の利用に関し、本体の使用権限をユーザー認証と組み合わせて制限することができます。また、権限レベルによって、アクセス可能な FAX や E-mail などの登録宛先を制限することができます。

(1)外部サーバを使用して認証を行う事が可能ですが、ネットワーク上に外部サーバを用意できない場合でも、装置内部に認証機能を持つためユーザー認証機能が可能です。

(2)ユーザー単位や部門単位で出力枚数データの上限値を設定して使用制限を管理できます。

(3)カラーとモノクロ別に出力権限や上限値を設定する事も可能です。

3. ボックスのセキュリティとその活用

ボックス内のデータを安全に守るために、ユーザー認証に加えてボックスへのアクセスもパスワードで保護しています。

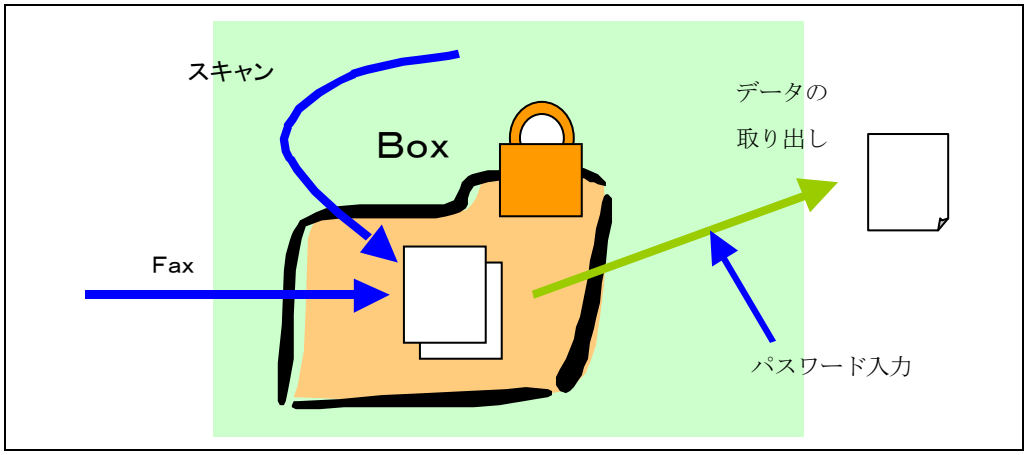


図3－3

4. HDD 廃棄時のデータ完全消去

ハードディスクの内部データは設定により乱数などの上書きで消去できます。

MFP 本体を廃棄した後に機密が漏洩することを防止できます。

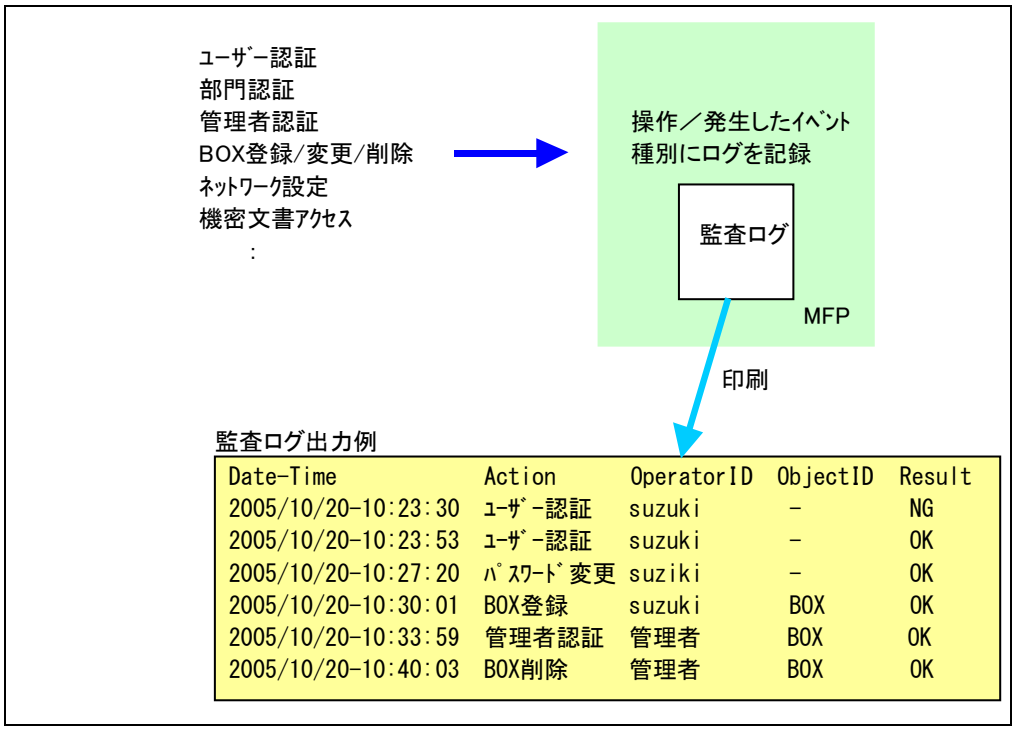
5. HDD 内データのパスワードと暗号化による保護

ハードディスクをパスワードによりロックできます。ハードディスクを MFP 本体から取り外し、PCに取付けても、パスワードが合致しないと内部データを覗く事はできません。さらに、ハードディスク内のデータを AES で暗号化できます。ハードディスク内のデータを読み出されたとしても、暗号化の鍵がなければ復号化できません。

6. 監査ログによるアクセス管理

セキュリティ機能の動作に関する履歴を監査ログとして保存します。

不正なアクセスに対して、トレースすることができます。



Date-Time	Action	OperatorID	ObjectID	Result
2005/10/20-10:23:30	ユーザー認証	suzuki	-	NG
2005/10/20-10:23:53	ユーザー認証	suzuki	-	OK
2005/10/20-10:27:20	パスワード変更	suziki	-	OK
2005/10/20-10:30:01	BOX登録	suzuki	BOX	OK
2005/10/20-10:33:59	管理者認証	管理者	BOX	OK
2005/10/20-10:40:03	BOX削除	管理者	BOX	OK

図3－4

7. PDF ファイルの暗号化

本体でスキャンしたデータを PDF 形式のファイルで保存する際、共通鍵による暗号化ができます。暗号化した PDF ファイルを Adobe Acrobat で開く時に、共通鍵の入力が必要となります。

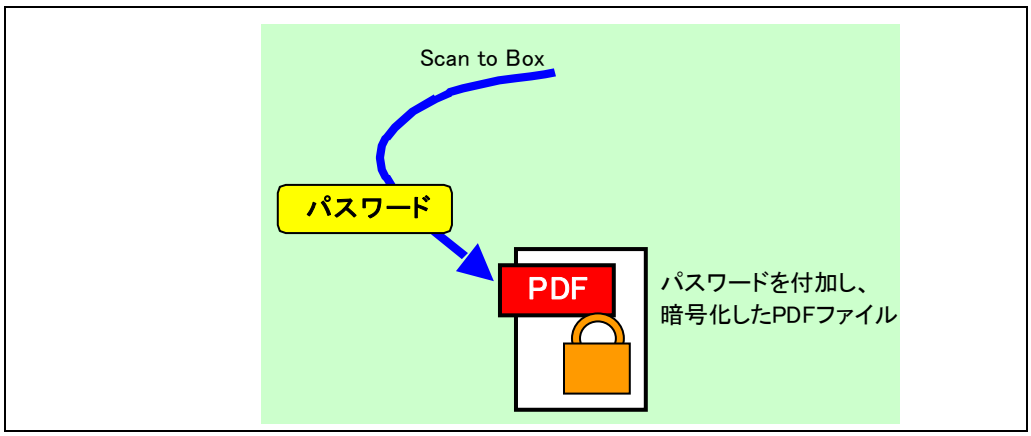


図3－5

8. メールデータの暗号化

送信者は MFP にてメールを発信する際に、受信者の証明書(公開鍵:アドレス帳への登録が可能)を使ってメールを暗号化し、受信者は PC 上で、自分の秘密鍵を使ってメールを復号する事ができます。これにより、メールの内容を他人に傍受される事なく、安全な送受信が可能になります。ネットワーク上から公開鍵を取得するには、LDAP サーバに登録された証明書を使用します。

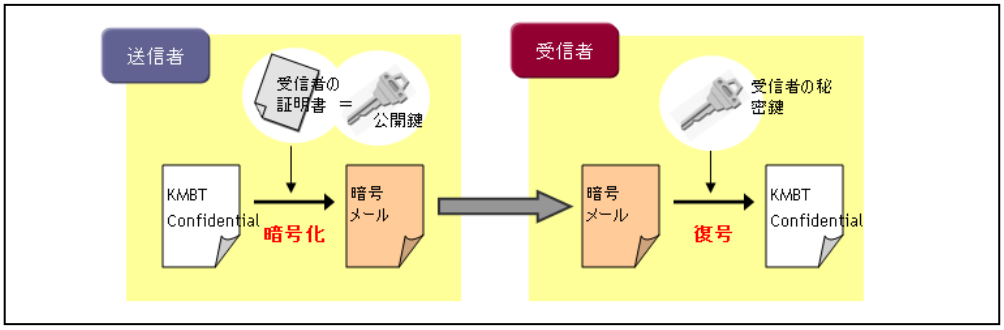


図3－6

9. メールの署名機能

送信者は MFP の秘密鍵でメールに署名をつけ、受信者は MFP の証明書で署名の検証を行います。これにより、受信者は、改竄が無いことを検証する事ができます。

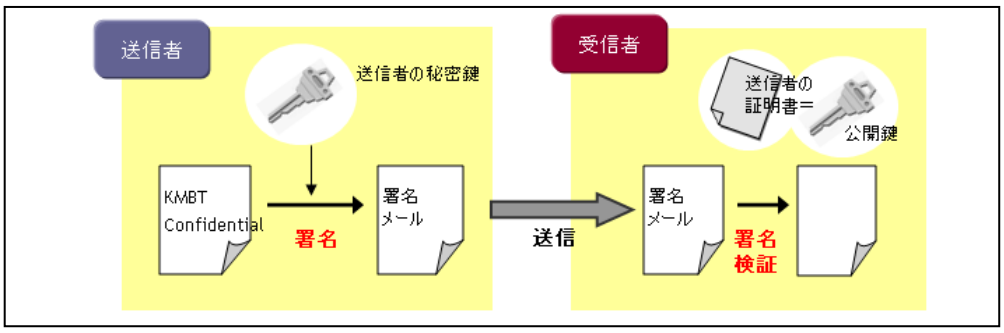


図3－7

10. Scan to Me, Scan to Home & Scan to Authorized Folder

スキャンデータの自分宛への送信が簡単に利用できます。

ユーザー認証を設定している場合、登録宛先の欄に「Me」のボタンと、管理者設定で機能を有効にすることにより「Home」のボタンが表示されます。

宛先の「Me」を選択した場合は、認証されている利用者の E-mail アドレスへ送信し、「Home」を選択した場合は、あらかじめ登録された PC フォルダへ送信するので、ワンタッチで簡単かつ確実なファイル送信が行えます。

SMB 宛先の[ユーザーID]と[パスワード]の欄に何も登録しないでおくことで、ログインしたユーザーが、自分の SMB 宛先をアドレス帳から選択して送信する場合に、ユーザー認証のユーザー名とパスワードをそのまま使用しますので、SMB の認証を自分以外の SMB 宛先の利用を制限することができます。

また、管理者設定により宛先の登録範囲や直接入力を制限・禁止することで、送信先を管理者が管理している宛先のみに送信できるように規制をかけることができます。

図3－8

11. HDD データ上書き削除機能

HDD 上書き削除機能の設定により、ハードディスクに一時的に保存されたデータは、プリントやスキャンなどのジョブの完了、ボックス保存文書の削除操作など、画像データの利用終了時に上書き消去されます。

ハードディスク上の不要になった画像データが再利用されるリスクを軽減できます。

12. 認定を受けた暗号モジュールの採用

MFP 内部には、OpenSSL / MES（RSA BSAFE Micro Edition Suite）等の、暗号モジュールを搭載し、暗号化や認証機能を達成してきました。FIPS140-2 の認定を受けた MES 暗号モジュールを利用している主な機能は、下記になります。

1. スキャンデータ配信時の暗号化通信
   Scan to WebDAV, TWAIN 等の SSL 通信時。Scan to E-Mail の S/MIME 送信時。
2. PSWC の SSL 通信時
3. PDF 暗号化ファイル生成機能

Ⅳ. 出力データのセキュリティ

1. コピーセキュリティー機能

(1) コピープロテクト印字機能

コピーやプリントによる出力文書(原本)に地紋を埋め込み、複製文書には“コピー”などの模様を浮かび上がらせる事で、明確に原本と複製との区分ができます。
また、出力に使用された MFP のシリアル No や出力日時を地紋に設定する事もできます。シリアル No と出力日時が入った複製文書と上記の監査ログとの組み合わせで不正コピーを行ったユーザーの特定が可能です。

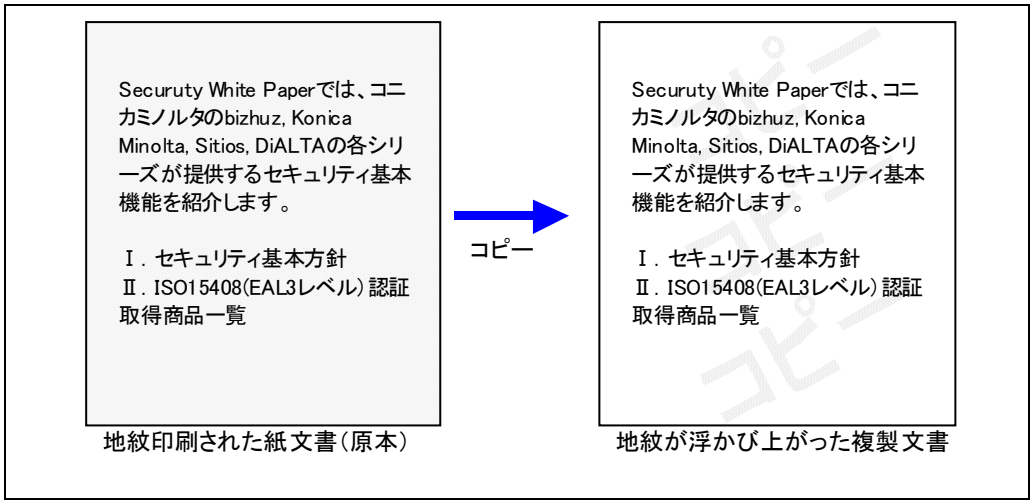


図4－1

(2)コピーガード機能／パスワードコピー機能

コピーやプリント時に特殊な地紋セキュリティーパターンを付加して出力した原稿を 2 次コピーしようとしても、コピーガード機能では、コピーが禁止されているというメッセージが出てコピーされません。また、パスワードコピー機能では、予めパスワードを設定しておいたパスワードを入力した場合に限り、地紋セキュリティパターンを付加した 2 次コピーが許可されます。

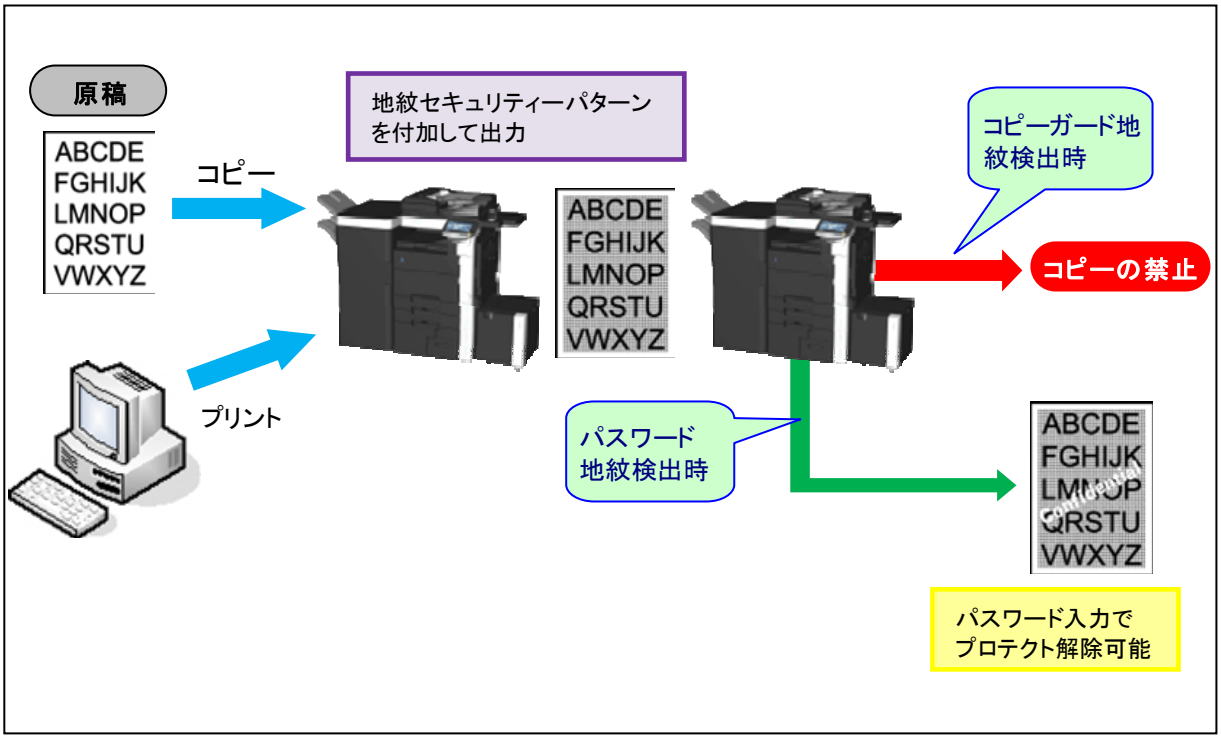


図4－2

V. 認証装置

1. 生体認証装置のデータに関するセキュリティ

生体認証装置、AU-101/102 のデータは非常にセキュリティの高い扱いで管理されている為、不法に利用する事は不可能である。

—生体データとしての指静脈—

静脈は体内にあり、指紋の様に不用意に読み取られる事はない。従って、偽造する事は非常に困難である。

－本システムで採用しているデータ処理方法—

このシステムは、「U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments (BVMPP-MR) Version 1.0」に基づくセキュリティガイドラインに対応している。種々の重要なセキュリティ/プライバシーに関する仕様をこのシステムで対応している。

＜生体データの再現＞

HDD には、(登録時の)読み取りデータの特徴に基づき算出された乱数データが登録される。HDD 内のデータから元の静脈データを再現する事は理論上不可能である。

＜HDD 内のデータ構造＞

HDD 内のデータ構造は公にされていない。従って、偽造やなり済ましは不可能である。

＜認証装置内にデータ消去＞

装置内のデータは、RAM に一時的に保管された際暗号化され、MFP に転送された後、消去される。

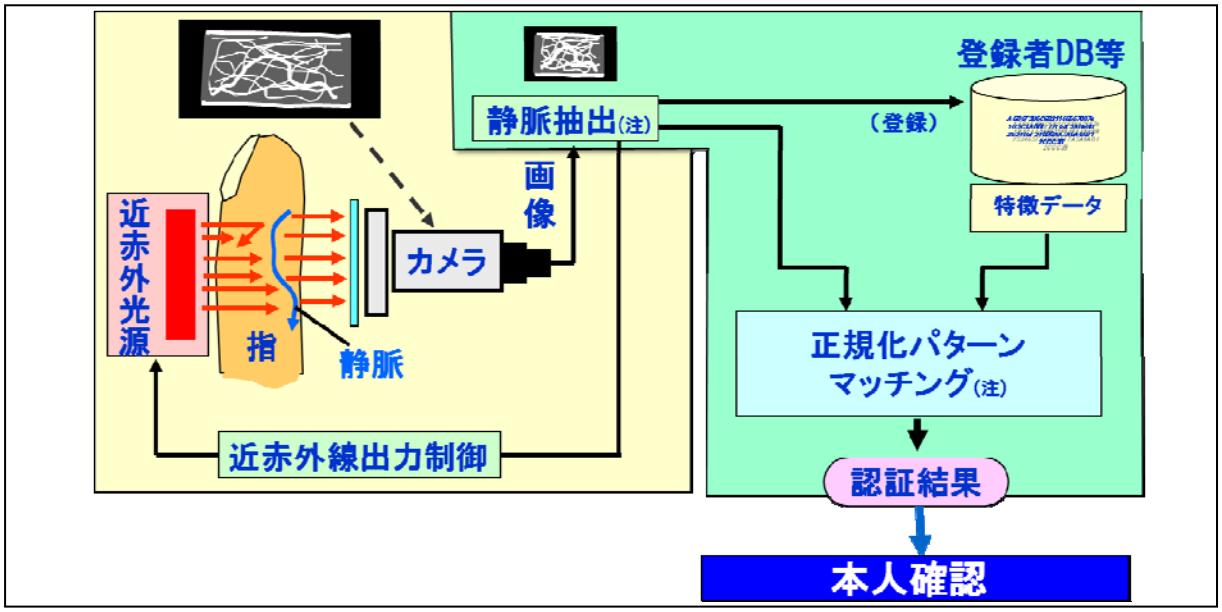


図5－1

「U.S. Government Biometric Verification Mode Protection Profile for Medium Robustness Environments (BVMPP-MR) Version 1.0：
http://www.commoncriteriaportal.org/public/files/ppfiles/PP_VID10140-PP.pdf 参照

2. 認証＆プリント（ワンタッチセキュリティプリント）

ユーザー認証機能との連携により、シンプルで機密性の高いプリント作業が実現します。プリント出力物が、他人に持ち去られたり、覗き見されたりする事はなくなります。また、生体認証装置やカード認証装置を利用することで、認証が簡単に行えます。

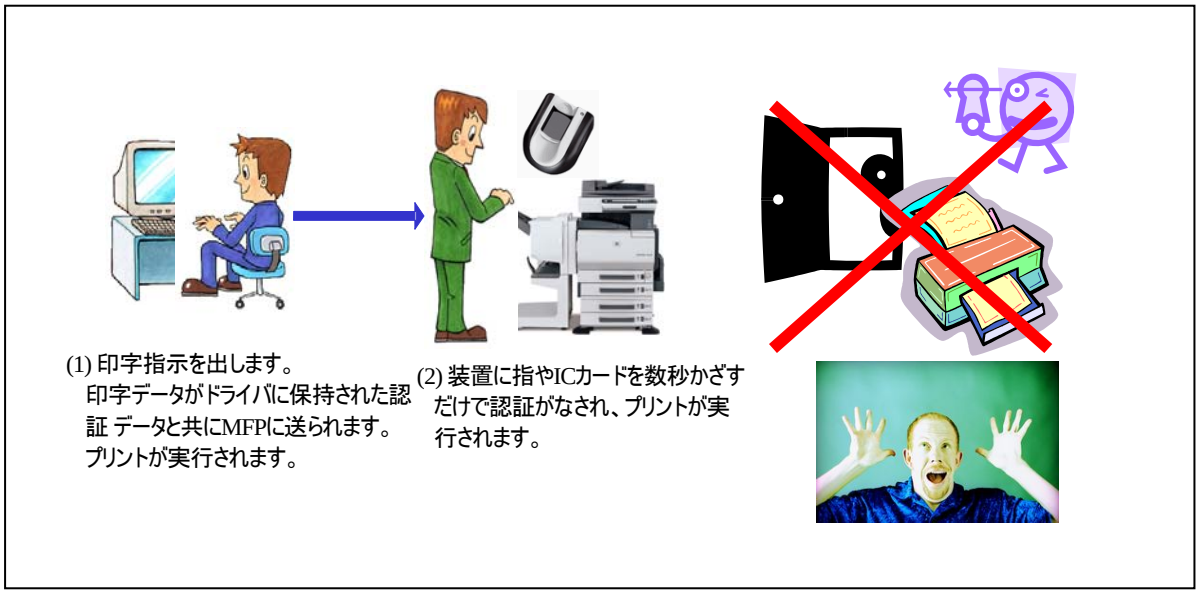


図5－2

Ⅵ. PageACSES との連携による機能拡張

MFP 本体に PageACSES を連携させる事により、セキュリティ機能の拡張と操作性の改善が図れます。

＜概要＞

ファイル毎の認証機能（PageACSES Pro 版のみ）

個々のユーザーに対し、ファイル毎に、閲覧、修正、印刷の権限設定を行う事ができます。MFP 本体で Scan した重要文書は、この認証機能と画像ファイルの暗号化により、外部への漏洩と不正な改竄が防止されます。

IC カードを使用したユーザー認証

ユーザー認証に非接触 IC カード（FeliCa）を使用し、パスワードを入力する事無しに MFP へのログインが可能になります。

1. 認証スキャン

スキャンデータをそのまま直接外部送信することを阻止します。IC カード情報により暗号化された状態でクライアント PC に送られたデータは、IC カードを使って取り出します。同時にコピー、プリント、スキャンに関する操作記録のログをとることができます。

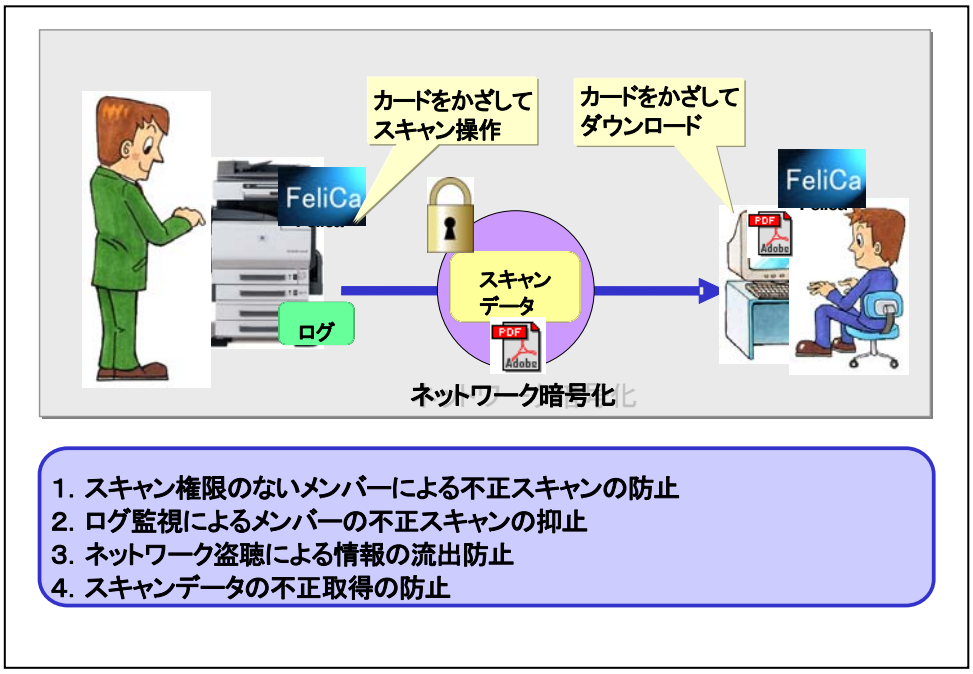


図6－1

2. 認証プリント

印刷する時にプリントデータが暗号化され、IC カードを使って自分の送ったプリントジョブが取り出せます。

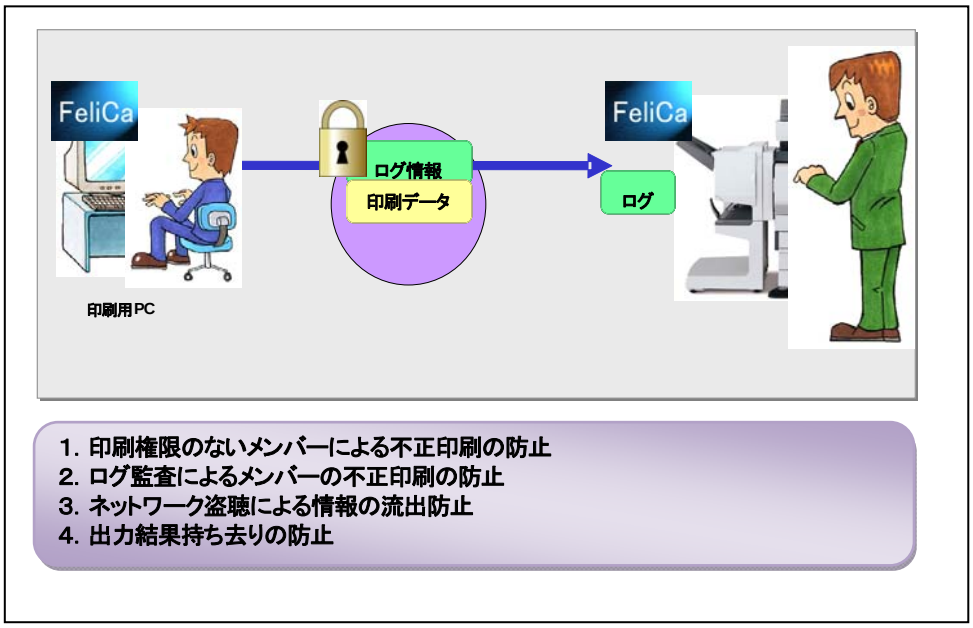


図6－2

3. ファイルのセキュリティ

（PageACSES Pro のみ）

PageACSES Pro を使って、PDF ファイルに対して利用権限がつけられます。外部にそのファイルが流出した場合でも暗号化されており安全です。

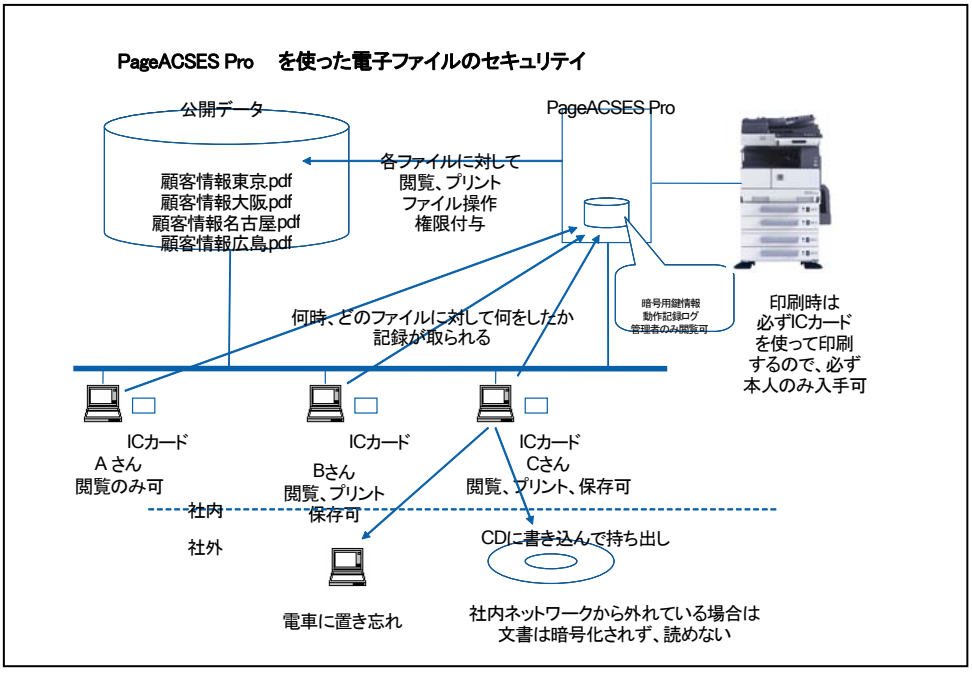


図6－3

Ⅶ. PKI カード認証システム

＜概要＞

PKI カードは暗号化/復号化、電子署名の機能を持ったカードです。このカードと MFP の機能を連携させることにより、セキュリティレベルの高い MFP の使用環境を構築することができます。

1. PKI カードを使用したログイン

カードリーダーに PKI カードを挿入し、PIN を入力すると、Active Directory への認証を実施します。その際、Active Directory から MFP に送られてくるデジタル証明書を MFP で検証することができます。

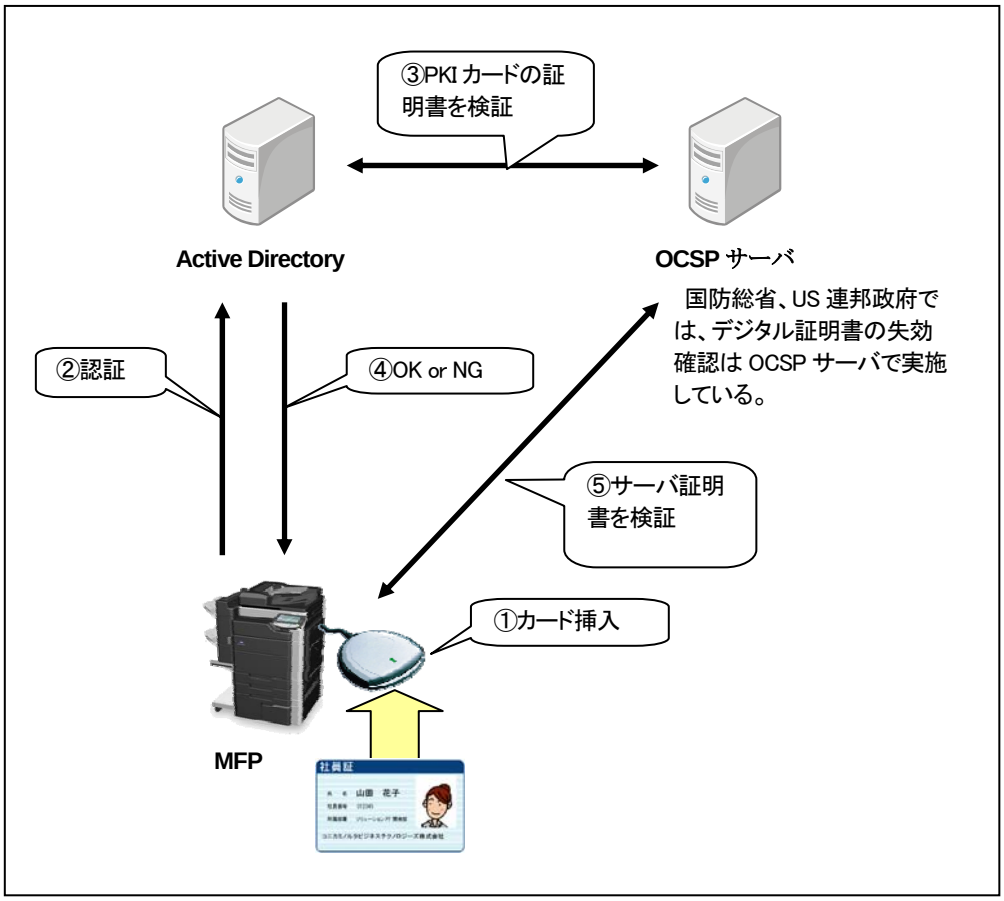


図7－1

2. PKI カードを使用した LDAP 検索

LDAP サーバーで宛先検索を行うときに、Active Directory 認証で取得した Kerberos 認証チケットを使用して LDAP サーバーにログインします。1 度の認証でアクセスできるため、利便性の高いシングルサインオン環境を構築することができます。

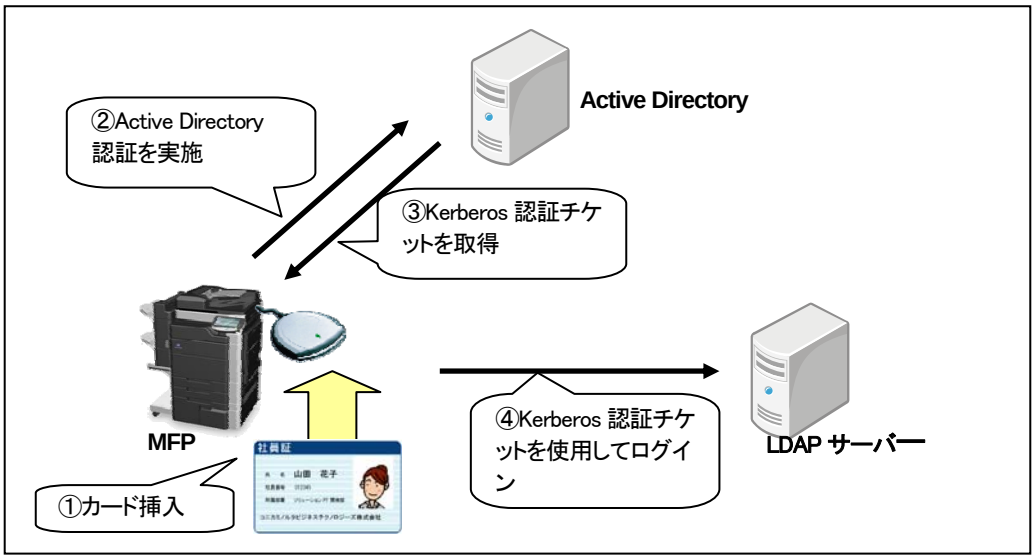


図7－2

3. PKI カードを使用した SMB 送信

スキャンしたデータを SMB 送信するときに、ActiveDirectory 認証で取得した Kerberos 認証チケットを使用して宛先のコンピューターにログインします。1 度の認証でアクセスできるため、利便性の高いシングルサインオン環境を構築することができます。また、認証チケットを使用することで、ネットワーク上にパスワードを流さない運用が可能になるため、安全に SMB 送信を行うことができます。

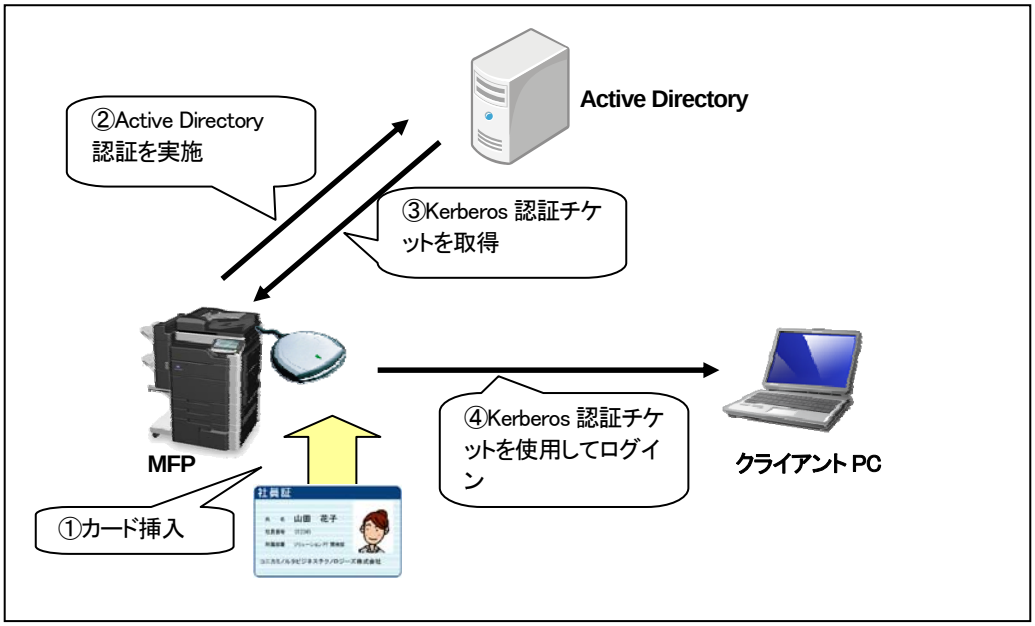


図7－3

4. PKI カードを使用した E-mail 送信（S/MIME）

E-mail 送信時に PKI カードを使用してデジタル署名を実施することができます。デジタル署名を実施することにより、E-mail の送信元を証明することができます。

また、宛先の証明書が登録されていれば、E-mail の暗号化を組み合わせて送信することもできます。E-mail を暗号化して送信することで、伝送経路上での第 3 者への情報漏洩を防止できます。

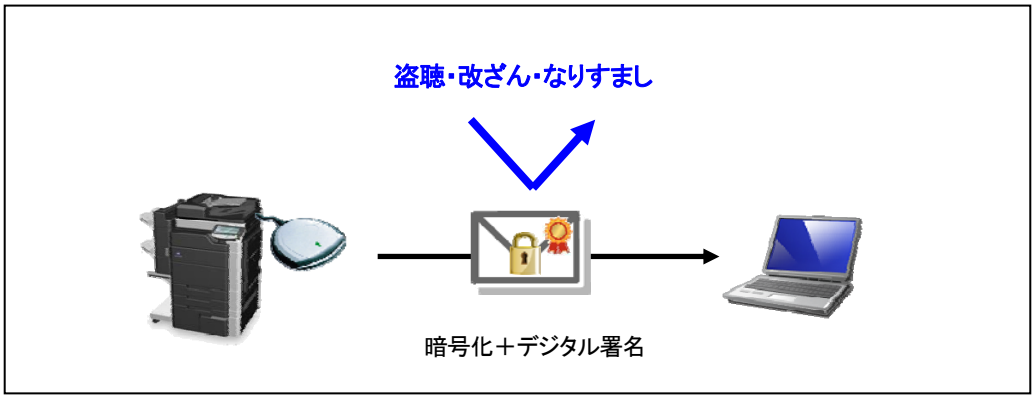


図7－4

5. PKI カードプリント

プリンタドライバから印刷データを PKI カードで暗号化して MFP に送信します。印刷データは MFP の PKI 暗号化ボックスに蓄積され、同じユーザーが MFP で PKI カード認証を実施することで、復号化してプリントすることができます。

印刷データは、MFP で PKI カードによる認証が成功してはじめてプリントが可能になるため、データの機密性を保持することができます。

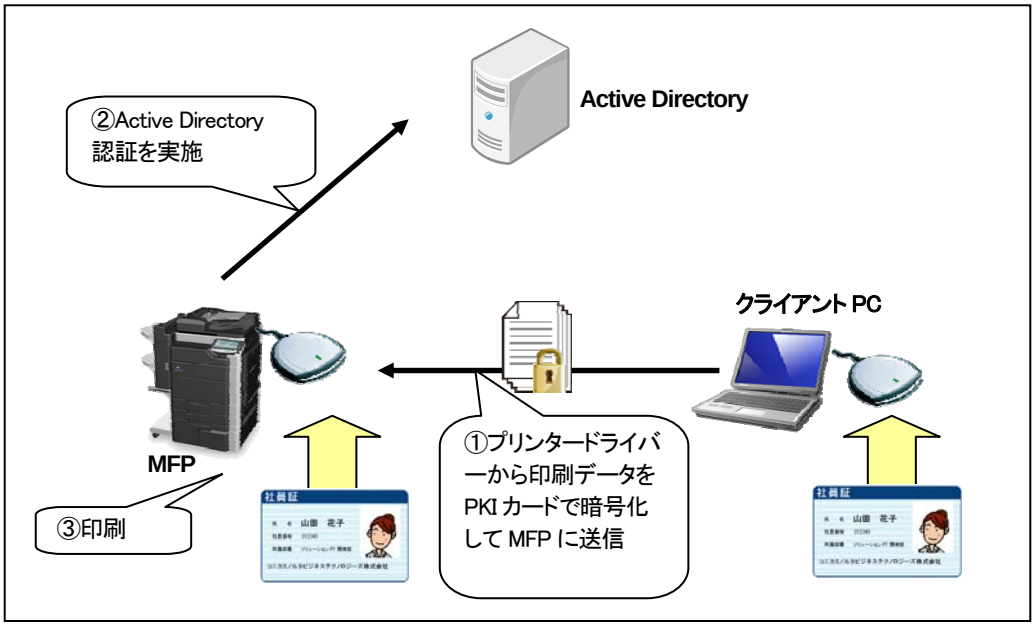


図7－5

6. Scan To Me / Scan To Home

スキャンしたデータを自分の E-mail アドレスやコンピューターに送信する機能です。自分の E-mail アドレスや Home フォルダーのパスは Active Directory 認証時に取得するので、簡単に送信することができます。

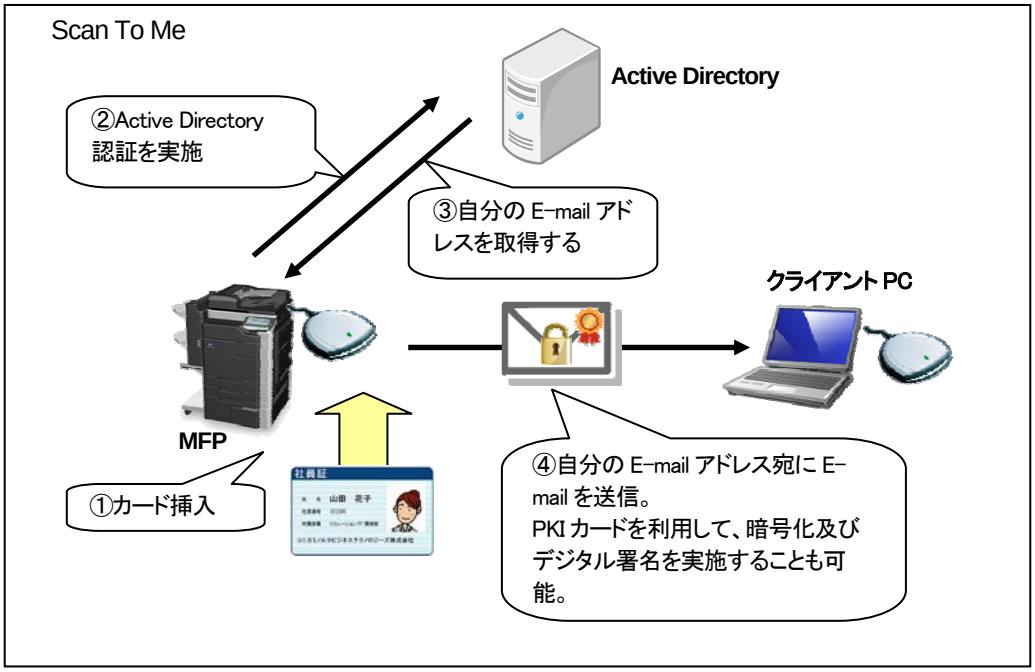


図7－6

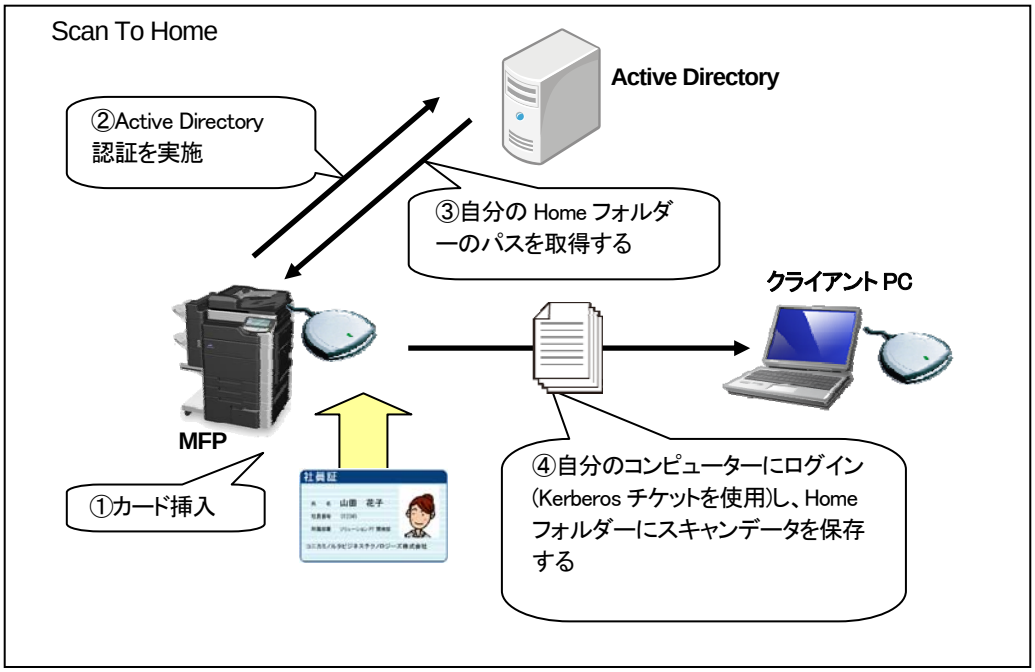


図7－7

Ⅷ. MFP 自己保護に関するセキュリティ

1. Firmware 検証機能

MFP 本体 Firmware の書き換え時に、Firmware データが改ざんされていないかハッシュ値チェックを行います。ハッシュ値が一致しない場合は警告を出し、Firmware 書き換えを行いません。

また、セキュリティ強化モードを利用している場合、主電源 ON 時にもハッシュ値チェックを行います。ハッシュ値が一致しない場合は警告を出し、MFP 本体の起動を禁止します。

Ⅸ. CS Remote Care に関するセキュリティ

1. 公衆回線を使用（モデム、FAX）した際のセキュリティ

公衆回線を使用した遠隔診断システムでは、本体と CS Remote Care（以下 CSRC）ホストとの間で通信を行って本体データを送信したり、本体の設定を変更したりします。遠隔診断システムで通信を行うには、CSRC ホストとデバイスの双方にあらかじめ登録した ID を使って、接続通信を行います。この通信では CSRC ホストの登録内容とデバイスの送信内容とが一致するかを確認し、通信が正常終了すると、以降、遠隔診断通信を行うことが可能な状態になります。遠隔診断通信は、通信毎に ID を確認の上、通信を行います。通信時に ID が合致しないと通信を行いません。
また、CSRC が収集するデータは、カウンタ値などのサービス情報であり、ファクス宛先や個人情報に関係する内容は含まれません。

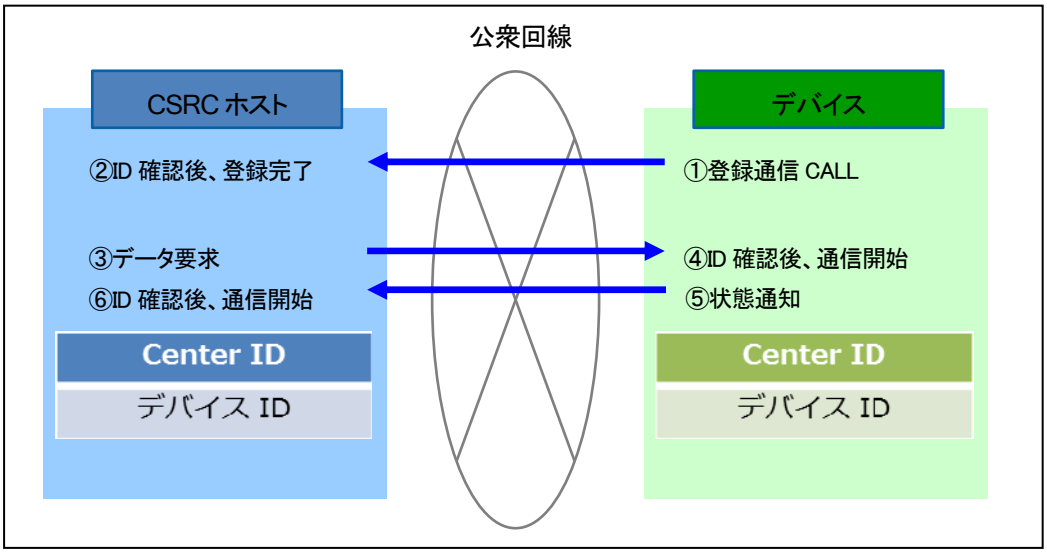


図9－1

2. メールでのセキュリティ

・送信データ暗号化

本体および CSRC ホストで暗号鍵(共通鍵)を使用し、データを暗号化します。

※本体およびセンターで暗号化可否設定可能

共通鍵暗号方式では、本体とセンターの暗号化と復号で同じ鍵を使用しています。

これにより、メールの内容を他人に傍受される事なく、安全な送受信が可能になります。

・ID などの確認

送受信メールには、送信元や送信先が確認可能な情報(CenterID やシリアル No)が含まれています。

この情報が合致するか確認を行い、正しい送受信先かどうか確認しています。

また、センターから送信されたメールには、メール ID が割り振られています。

MFP からの応答メールには、応答元メールのメール ID が利用されています。

センターが送信したメール ID と一致するかチェックし、ID の確認を行います。

・不正メールの排除

上記の ID などの確認で、送信元や送信先が確認可能な情報(CenterID やシリアル No)やメール ID が一致しなかった場合、

その送受信メールは不正データと見なし、データ登録は行わずに排除します。

3. HTTP 通信でのセキュリティ

・送信データ暗号化

本メールと同じく、本体および CSRC ホストで暗号鍵(共通鍵)を使用し、データを暗号化します。

※本体および CSRC ホストで暗号化可否設定可能

共通鍵暗号方式により、デバイスと CSRC ホストの暗号化と復号で同じ鍵を使用しています。

また、HTTP 通信では SSL を設定できます。(HTTPS)

SSL により、「デバイス⇔WebDAV サーバ」および「WebDAV サーバ⇔CSRC ホスト」の通信データで暗号化を行っています。

・HTTP プロトコルが持つ数多くのセキュア機能を流用可能

HTTP プロトコルは環境に依存せず、認証、Proxy、SSL などのセキュア機能を多く利用する事が出来ます。

SSL では、公開鍵暗号や秘密鍵暗号、デジタル証明書、ハッシュ関数などのセキュリティ技術を組み合わせ、データの盗聴や改ざん、なりすましを防ぐことができます。

センターにおいても、これらのセキュア機能を利用することで、

顧客環境にマッチしたセキュリティ対策を施行することが可能です。

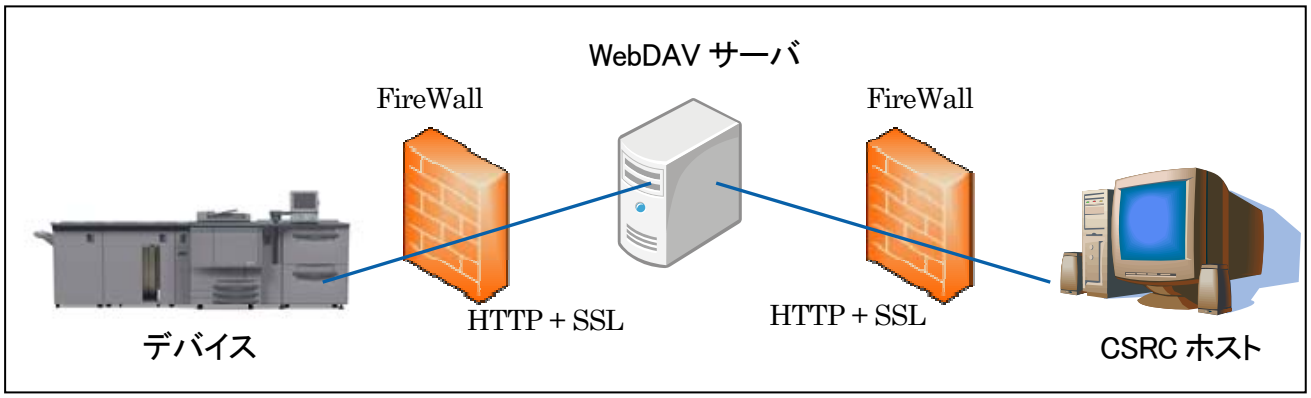


図9－2

4. プロダクト認証

・End to End のデータ保障

HTTP 通信では、インターネット上の WebDAV サーバに対して読み書きを行います。
そのため、情報漏洩などのセキュリティ面で若干の脆弱性が存在します。
プロダクト認証では、セキュリティ面をより強固にするため、SSL のクライアント認証を行うことで、デバイス⇔WebDAV サーバ、WebDAV サーバ⇔CSRC ホストの通信の妥当性を保障します。
プロダクト認証は、まずライセンス管理サーバより利用者に対してユニークなライセンスコードを発行します。
発行されたコードを証明書発行サーバへ登録することによって、証明書発行サーバにクライアント証明書とサーバ証明書が発行できます。
クライアント証明書は MFP およびセンターで利用し、サーバ証明書は利用者のメールアドレスに送信され、WebDAV に設定することにより
デバイス⇔WebDAV サーバ、WebDAV サーバ⇔CSRC ホストの通信のデータ保障が高まります。

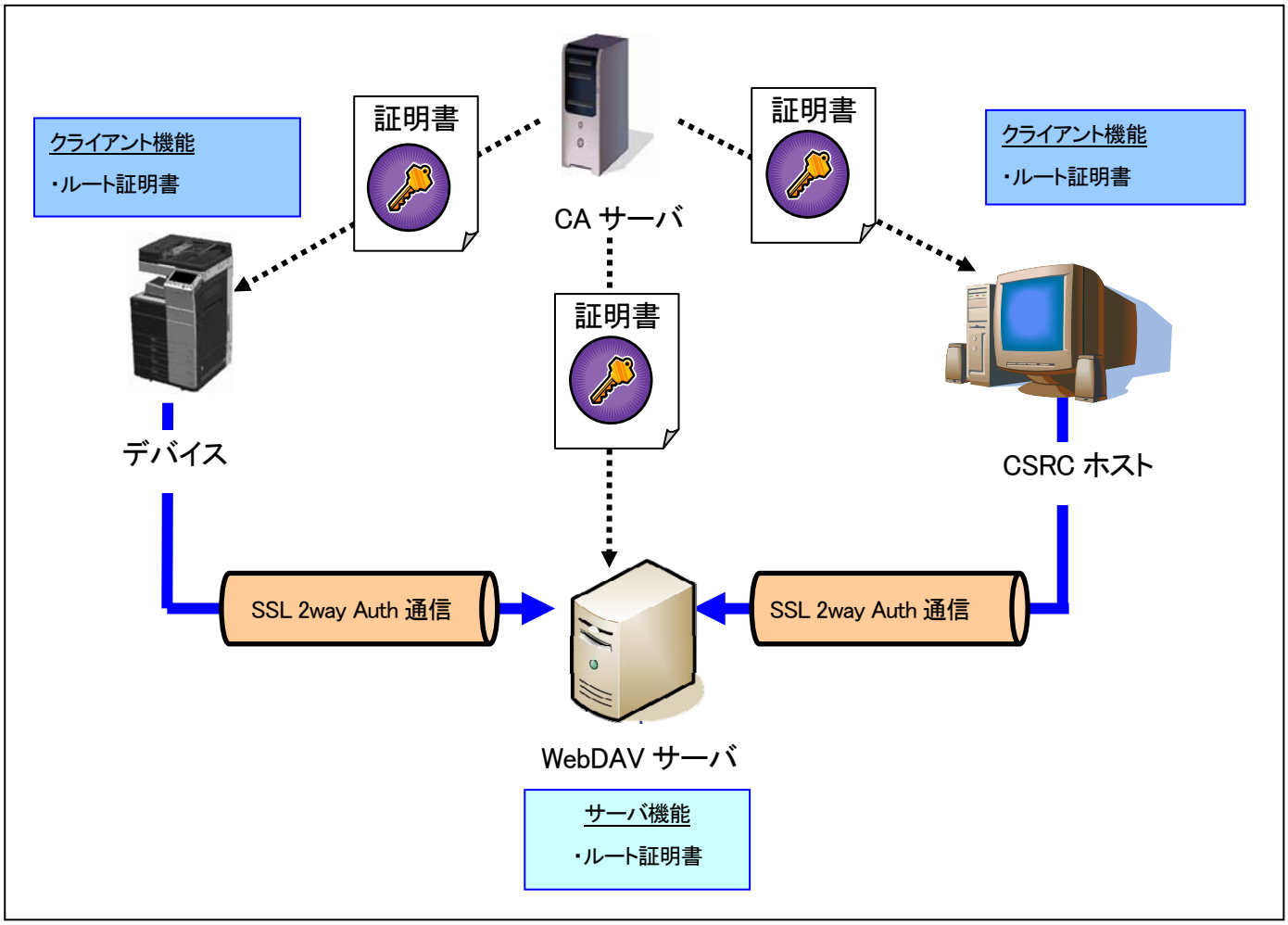


図9－3

5. DCA でのセキュリティ

・DCA-デバイス間の SNMPv3 通信

DCA（Device Collection Agent）では、装置との通信方法として SNMPv1 と SNMPv3 通信をサポートします。

SNMPv1 通信では、平文のデータがネットワーク経路上を流れるため、外部からパケットをキャプチャされてしまう可能性がある環境の場合、通信中のデータが盗聴されてしまう危険性があります。

また、SNMPv1 通信における唯一の認証である「コミュニティ名」も同時に漏れてしまうため、流出した「コミュニティ名」で管理されている装置の MIB に格納されたすべてのデータにアクセスすることが可能となってしまいます。

SNMPv3 通信では、SNMPv1 通信のコミュニティ名に相当する「ユーザー名」に加え、認証のための仕組みが追加されており、装置へのアクセスに対して堅牢性を高めます。また、通信経路を流れるデータはすべて暗号化されており、同じ暗号化方式・暗号鍵を知らない限り、データを盗聴することは困難になります。

・DCA-CSRC ホスト間の通信

DCA と CSRC ホストとの間の通信は、HTTP プロトコル上で SSL を使用して、暗号化通信をしています。

また、DCA には固有の ID が割り当てられ、通信毎にこの ID を確認の上、データ転送を行います。

通信時にこの ID が一致しない場合、データ転送は実施されないようになっています。

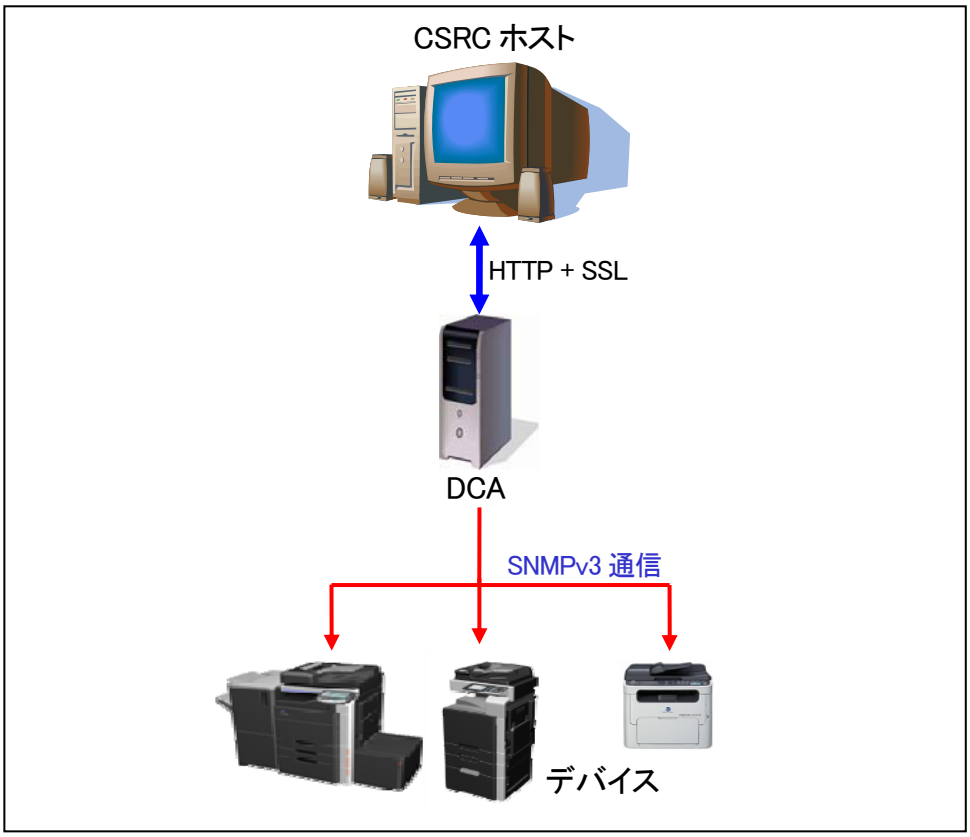


図9－4