セキュリティーテクニカルサポートペーパー Version10.4 添付資料

各機能の適応機種一覧リスト

<カラー複合機>

	C360i/C300i/C250i	C4050i/C3350i	C3320i	C4000i/C3300i	C650i/C550i/C450i	C750i	C287i/C257i/C227i	C450iS/C360iS/C300iS/C250iS	C751i/C651i/C551i	C451i/C361i/C301i/C251i	C4051i/C3351i	C3321i	C4001i/C3301i
I. 公衆電話回線に対するセキュリティー													
1. FAX回線に対するセキュリティー	○	○	○	–	○	○	○	○	○	○	○	○	–
2. 宛先２度入力	○	○	○	–	○	○	○	○	○	○	○	○	–
3. チェーンダイアル	○	○	○	–	○	○	○	○	○	○	○	○	–
4. 宛先確認画面表示	○	○	○	–	○	○	○	○	○	○	○	○	–
5. 複数宛先禁止	○	○	○	–	○	○	○	○	○	○	○	○	–
6. 相手機確認送信	○	○	○	–	○	○	○	○	○	○	○	○	–
II. LAN接続に対するセキュリティー													
1. ネットワークプロトコルに対する対応	○	○	○	○	○	○	○	○	○	○	○	○	○
2. ユーザー認証	○	○	○	○	○	○	○	○	○	○	○	○	○
3. ネットワーク経由の装置管理セキュリティー													
(1) アドレス帳一括登録時のセキュリティー	○	○	○	–	○	○	○	○	○	○	○	○	–
(2) bizhub OpenAPI	○	○	○	○	○	○	○	○	○	○	○	○	○
4. データ通信の暗号化	○	○	○	○	○	○	○	○	○	○	○	○	○
5. 検疫ネットワーク対応	○	○	○	○	○	○	○	○	○	○	○	○	○
6. 双方向証明書検証	○	○	○	○	○	○	○	○	○	○	○	○	○
7. ウイルスに対する対応	○	○	○	○	○	○	○	○	○	○	○	○	○
8. ウイルススキャン機能	○	○	○	×	○	○	○	○	○	○	○	○	×
9. 外部からのUSBメモリを介してのウイルスへの対応状況	○	○	○	–	○	○	○	○	○	○	○	○	–
10. Linux kernelの定常監視	○	○	○	○	○	○	○	○	○	○	○	○	○
11. USB I/Fバスとの分離	○	○	○	○	○	○	○	○	○	○	○	○	○
12. 無線LANと有線LANとの通信分離	○	○	○	○	○	○	○	○	○	○	○	○	○
III. MFP本体内データのセキュリティー													
1. 画像処理及び出力処理におけるセキュリティー	○	○	○	○	○	○	○	○	○	○	○	○	○
2. HDD一時保存データ上書き削除機能	–	–	–	–	–	–	–	–	–	–	–	–	–
3. HDD、SSD及びmicroSD廃棄時のデータ完全消去	○	○	○	○	○	○	○	○	○	○	○	○	○
4. 全データ削除後のレポート出力機能	○	○	○	○	○	○	○	○	○	○	○	○	○
5. HDD、SSD及びmicroSD内データの暗号化による保護	○	○	○	○	○	○	○	○	○	○	○	○	○
6. 自己暗号化によるSSDの保護	○	○	×	×	○	○	○	○	○	○	○	×	×
7. PDFファイルの暗号化	○	○	○	–	○	○	○	○	○	○	○	○	–
8. ユーザー認証													
(1) 外部サーバと装置内部での認証機能	○	○	○	○	○	○	○	○	○	○	○	○	○
(2) ユーザー/部門単位での出力上限値管理	○	○	○	○	○	○	○	○	○	○	○	○	○
(3) カラー・モノクロ別出力権限と出力上限値管理	○	○	○	○	○	○	○	○	○	○	○	○	○
9. ボックスのセキュリティーとその活用	○	○	○	○	○	○	○	○	○	○	○	○	○
10. メールデータの暗号化	○	○	○	–	○	○	○	○	○	○	○	○	–
11. メールの署名機能	○	○	○	–	○	○	○	○	○	○	○	○	–
12. Scan to Me, Scan to Home & Scan to Authorized Folder	○	○	○	–	○	○	○	○	○	○	○	○	–
13. 監査ログによるアクセス管理	○	○	○	○	○	○	○	○	○	○	○	○	○
14. 認証を受けた暗号モジュールの採用	○	○	○	○	○	○	○	○	○	○	○	○	○
15. TPMによるデータ保護	○	○	–	–	○	○	○	○	○	○	○	–	–
IV. 出力データのセキュリティー													
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	○	○	○	○	○	○	○	○	○	○	○	○	○
(2) コピーガード機能/パスワードコピー機能	○	–	–	–	○	○	–	○	○	○	–	–	–
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ー	○	○	○	○	○	○	○	○	○	○	○	○	○
2. 認証＆プリント（ワンタッチセキュリティー）	○	○	○	○	○	○	○	○	○	○	○	○	○
VI. モバイル機器との連携におけるセキュリティー													
1. AirPrintに対するセキュリティー	○	○	○	○	○	○	○	○	○	○	○	○	○
2. Mopriaに対するセキュリティー	○	○	○	○	○	○	○	○	○	○	○	○	○
3. Google Cloud Printに対するセキュリティー	○	○	○	○	○	○	○	○	○	○	○	○	○
4. Konica Minolta Print Serviceに対するセキュリティー	○	○	○	○	○	○	○	○	○	○	○	○	○
5. PageScope Mobileに対するセキュリティー	○	○	○	○	○	○	○	○	○	○	○	○	○
VII. PKIカード認証システム													
1. PKIカードを使用したログイン	○	○	–	–	○	○	○	○	○	○	○	–	–
2. PKIカードを使用したLDAP検索	○	○	–	–	○	○	○	○	○	○	○	–	–
3. PKIカードを使用したSMB送信	○	○	–	–	○	○	○	○	○	○	○	–	–
4. PKIカードを使用したE-mail送信（S/MIME)	○	○	–	–	○	○	○	○	○	○	○	–	–
5. PKIカードプリント	○	○	–	–	○	○	○	○	○	○	○	–	–
6. Scan To Me/Scan To Home	○	○	–	–	○	○	○	○	○	○	○	–	–
VIII. MFP自己保護に関するセキュリティー													
1. Firmware検証機能	○	○	○	○	○	○	○	○	○	○	○	○	○
IX. CS Remote Careに関するセキュリティー													
1. 基本的なセキュリティと収集データ	○	○	○	○	○	○	○	○	○	○	○	○	○
2. LTEを用いた場合のセキュリティーについて	○	○	○	○	○	○	○	○	○	○	○	○	○
3. メールでのセキュリティー	○	○	○	○	○	○	○	○	○	○	○	○	○
4. HTTP通信でのセキュリティー	○	○	○	○	○	○	○	○	○	○	○	○	○
5. DCAでのセキュリティー	○	○	○	○	○	○	○	○	○	○	○	○	○
X. Remote Panelに関するセキュリティー													
1. 通信、接続トリガー	○	○	○	○	○	○	○	○	○	○	○	○	○
2. 認証	○	○	○	○	○	○	○	○	○	○	○	○	○
3. Access Code	○	○	○	○	○	○	○	○	○	○	○	○	○
4. 監査ログ	○	○	○	○	○	○	○	○	○	○	○	○	○
XI. World Wide Remote Service Platformに関するセキュリティー													
1. WWRSPFとMFP間の通信	○	○	○	○	○	○	○	○	○	○	○	○	○
2. WWRSPFとXMPP PF間の通信（MFPに依存しない）													
3. XMPP PFとMFP間の通信	○	○	○	○	○	○	○	○	○	○	○	○	○
4. WWRSPFからMFPへの通信	○	○	○	○	○	○	○	○	○	○	○	○	○
5. WWRSPFとCSRC連携（MFPに依存しない）													
6. RSA (Remote Service Agent) を使った通信													
7. RSA Edgeの登録とRSA CloudおよびAWS IoTとの接続に必要な情報の取得													
8. RSA EdgeとRSA Cloudの通信													
9. RSA EdgeとAWS IoTの通信													
XII. bizhub Remote Accessに関するセキュリティー													
1. ペアリング	○	○	○	○	○	○	○	○	○	○	○	○	○
2. 通信、接続トリガー	○	○	○	○	○	○	○	○	○	○	○	○	○
3. タイムアウトによる自動切断	○	○	○	○	○	○	○	○	○	○	○	○	○
4. 管理者モード中のセキュリティ	○	○	○	○	○	○	○	○	○	○	○	○	○
5. リモート操作中に切断された時のセキュリティー	○	○	○	○	○	○	○	○	○	○	○	○	○
6. ユーザー認証・部門認証併用時のセキュリティー	○	○	○	○	○	○	○	○	○	○	○	○	○
XIII. CSRA (CS Remote Analysis) に関するセキュリティー													
1. HTTP通信でのセキュリティー	○	○	○	○	○	○	○	○	○	○	○	○	○
XIV. MFP内蔵SaaS GWに関するセキュリティー													
1. SaaS GWとクラウドとの通信	○	○	○	○	○	○	○	○	○	○	○	○	○
2. 通信上の保護と暗号化	○	○	○	○	○	○	○	○	○	○	○	○	○
3. なしすましの防止	○	○	○	○	○	○	○	○	○	○	○	○	○
XV. Remote Deployment Toolsに関するセキュリティー													
1. 通信の安全性 2. アクセス制限 3. データの管理 4. 電子署名 5. ウイルス対策	○	○	○	○	○	○	○	○	○	○	○	○	○
XVI. CWHに関するセキュリティー													
1. 2-way HTTPS通信でのセキュリティー	○	○	○	○	○	○	○	○	○	○	○	○	○
2. 1-way HTTPS通信でのセキュリティー	○	○	○	○	○	○	○	○	○	○	○	○	○
XVII. ユーザー情報の保護													
1. 個人情報の表示制限	○	○	○	○	○	○	○	○	○	○	○	○	○
2. 管理者パスワード設定	○	○	○	○	○	○	○	○	○	○	○	○	○
3. 簡易IPフィルタリング	○	○	○	○	○	○	○	○	○	○	○	○	○
4. 簡単セキュリティ設定へのショートカット表示	○	○	○	○	○	○	○	○	○	○	○	○	○
XVIII. Fleet RMMに関するセキュリティー													
1. 通信の安全性 2. アクセス制限 3. データの管理 4. 電子署名 5. ウイルス対策	○	○	○	○	○	○	○	○	○	○	○	○	○
XIX. MarketPlaceに関するセキュリティ													
1. クッキー	○	○	×	○ *23	○	○	○	○	○	○	○	×	○ *23
2. 暗号化	○	○	×	○ *23	○	○	○	○	○	○	○	×	○ *23
3. アカウント作成	○	○	×	○ *23	○	○	○	○	○	○	○	×	○ *23
4. アナリティクスツール	○	○	×	○ *23	○	○	○	○	○	○	○	×	○ *23
5. DDoSプロテクション	○	○	×	○ *23	○	○	○	○	○	○	○	×	○ *23
6. Konica Minolta MarketPlaceアプリケーション	○	○	×	○ *23	○	○	○	○	○	○	○	×	○ *23

(参考)

HDD暗号アルゴリズム(AES)													
SSD暗号アルゴリズム(AES)	○ (AES256)	○ (AES256)			○ (AES256)	○ (AES256)	○ (AES256)	○ (AES256)	○ (AES256)	○ (AES256)	○ (AES256)		
μSD暗号アルゴリズム(AES)			○ (AES256)	○ (AES256)			○ (AES256)					○ (AES256)	○ (AES256)

*23 : C3300i、C3301iは非サポート

セキュリティーテクニカルサポートペーパー Version10.4 添付資料

各機能の適応機種一覧リスト

<モノクロ複合機>

	958/808/758	306i/266i/246i/226i	650i/550i/450i/360i/300i	750i	4750i/4050i	4700i	950i/850i	751i/651i/551i/451i/361i/301i	4751i/4051i	4701i
I. 公衆電話回線に対するセキュリティー										
1. FAX回線に対するセキュリティー	○	○	○	○	○	–	○	○	○	–
2. 宛先２度入力	○	○	○	○	○	–	○	○	○	–
3. チェーンダイアル	○	○	○	○	○	–	○	○	○	–
4. 宛先確認画面表示	○	○	○	○	○	–	○	○	○	–
5. 複数宛先禁止	○	○	○	○	○	–	○	○	○	–
6. 相手機確認送信	○	○	○	○	○	–	○	○	○	–
II. LAN接続に対するセキュリティー										
1. ネットワークプロトコルに対する対応	○	○	○	○	○	○	○	○	○	○
2. ユーザー認証	○	○	○	○	○	○	○	○	○	○
3. ネットワーク経由の装置管理セキュリティー										
(1) アドレス帳一括登録時のセキュリティー	○	○	○	○	○	–	○	○	○	–
(2) bizhub OpenAPI	○	○	○	○	○	○	○	○	○	○
4. データ通信の暗号化	○	○	○	○	○	○	○	○	○	○
5. 検疫ネットワーク対応	○	○	○	○	○	○	○	○	○	○
6. 双方向証明書検証	○	○	○	○	○	○	○	○	○	○
7. ウイルスに対する対応	○	○	○	○	○	○	○	○	○	○
8. ウイルススキャン機能	×	○	○	○	○	×	○	○	○	×
9. 外部からのUSBメモリを介してのウイルスへの対応状況	○	○	○	○	○	–	○	○	○	–
10. Linux kernelの定常監視	○	○	○	○	○	○	○	○	○	○
11. USB I/Fバスとの分離	○	○	○	○	○	○	○	○	○	○
12. 無線LANと有線LANとの通信分離	○	○	○	○	○	○	○	○	○	○
III. MFP本体内データのセキュリティー										
1. 画像処理及び出力処理におけるセキュリティー	○	○	○	○	○	○	○	○	○	○
2. HDD一時保存データ上書き削除機能	○	—	—	—	—	-	—	—	—	-
3. HDD、SSD及びmicroSD廃棄時のデータ完全消去	○	○	○	○	○	○	○	○	○	○
4. 全データ削除後のレポート出力機能	○	○	○	○	○	○	○	○	○	○
5. HDD、SSD及びmicroSD内データの暗号化による保護	○	○	○	○	○	○	○	○	○	○
6. 自己暗号化によるSSDの保護	×	○	○	○	○	×	○	○	○	×
7. PDFファイルの暗号化	○	○	○	○	○	–	○	○	○	–
8. ユーザー認証										
(1) 外部サーバと装置内部での認証機能	○	○	○	○	○	○	○	○	○	○
(2) ユーザー/部門単位での出力上限値管理	○	○	○	○	○	○	○	○	○	○
(3) カラー・モノクロ別出力権限と出力上限値管理	○	○	○	○	○	○	○	○	○	○
9. ボックスのセキュリティーとその活用	○	○	○	○	○	○	○	○	○	○
10. メールデータの暗号化	○	○	○	○	○	–	○	○	○	–
11. メールの署名機能	○	○	○	○	○	–	○	○	○	–
12. Scan to Me, Scan to Home & Scan to Authorized Folder	○	○	○	○	○	–	○	○	○	–
13. 監査ログによるアクセス管理	○	○	○	○	○	○	○	○	○	○
14. 認証を受けた暗号モジュールの採用	○	○	○	○	○	○	○	○	○	○
15. TPMによるデータ保護	○	—	○	○	○	–	○	○	○	–
IV. 出力データのセキュリティー										
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	○	○	○	○	○	○	○	○	○	○
(2) コピーガード機能/パスワードコピー機能	○	—	○	○	○	–	○	○	○	–
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ー	○	○	○	○	○	○	○	○	○	○
2. 認証＆プリント（ワンタッチセキュリティー）	○	○	○	○	○	○	○	○	○	○
VI. モバイル機器との連携におけるセキュリティー										
1. AirPrintに対するセキュリティー	○	○	○	○	○	○	○	○	○	○
2. Mopriaに対するセキュリティー	○	○	○	○	○	○	○	○	○	○
3. Google Cloud Printに対するセキュリティー	○	○	○	○	○	○	○	○	○	○
4. Konica Minolta Print Serviceに対するセキュリティー	○	○	○	○	○	○	○	○	○	○
5. PageScope Mobileに対するセキュリティー	○	○	○	○	○	○	○	○	○	○
VII. PKIカード認証システム										
1. PKIカードを使用したログイン	○	—	○	○	○	–	○	○	○	–
2. PKIカードを使用したLDAP検索	○	—	○	○	○	–	○	○	○	–
3. PKIカードを使用したSMB送信	○	—	○	○	○	–	○	○	○	–
4. PKIカードを使用したE-mail送信（S/MIME)	○	—	○	○	○	–	○	○	○	–
5. PKIカードプリント	○	—	○	○	○	–	○	○	○	–
6. Scan To Me/Scan To Home	○	○	○	○	○	–	○	○	○	–
VII. MFP自己保護に関するセキュリティー										
1. Firmware検証機能	○	○	○	○	○	○	○	○	○	○
IX. CS Remote Careに関するセキュリティー										
1. 基本的なセキュリティと収集データ	○	○	○	○	○	○	○	○	○	○
2. LTEを用いた場合のセキュリティーについて	○	○	○	○	○	○	○	○	○	○
3. メールでのセキュリティー	○	○	○	○	○	○	○	○	○	○
4. HTTP通信でのセキュリティー	○	○	○	○	○	○	○	○	○	○
5. DCAでのセキュリティー	○	○	○	○	○	○	○	○	○	○
X. Remote Panelに関するセキュリティー										
1. 通信、接続トリガー	○	○	○	○	○	○	○	○	○	○
2. 認証	○	○	○	○	○	○	○	○	○	○
3. Access Code	○	○	○	○	○	○	○	○	○	○
4. 監査ログ	○	○	○	○	○	○	○	○	○	○
XI. World Wide Remote Service Platformに関するセキュリティー										
1. WWRSPFとMFP間の通信		○	○	○	○	○	○	○	○	○
2. WWRSPFとXMPP PF間の通信（MFPに依存しない）										
3. XMPP PFとMFP間の通信		○	○	○	○	○	○	○	○	○
4. WWRSPFからMFPへの通信		○	○	○	○	○	○	○	○	○
5. WWRSPFとCSRC連携（MFPに依存しない）										
6. RSA (Remote Service Agent) を使った通信										
7. RSA Edgeの登録とRSA CloudおよびAWS IoTとの接続に必要な情報の取得										
8. RSA EdgeとRSA Cloudの通信										
9. RSA EdgeとAWS IoTの通信										
XII. bizhub Remote Accessに関するセキュリティー										
1. ペアリング	○	○	○	○	○	○	○	○	○	○
2. 通信、接続トリガー	○	○	○	○	○	○	○	○	○	○
3. タイムアウトによる自動切断	○	○	○	○	○	○	○	○	○	○
4. 管理者モード中のセキュリティ	○	○	○	○	○	○	○	○	○	○
5. リモート操作中に切断された時のセキュリティー	○	○	○	○	○	○	○	○	○	○
6. ユーザー認証・部門認証併用時のセキュリティー	○	○	○	○	○	○	○	○	○	○
XIII. CSRA(CS Remote Analysis)に関するセキュリティー										
1. HTTP通信でのセキュリティー		○	○	○	○	○	○	○	○	○
XIV. MFP内蔵SaaS GWに関するセキュリティー										
1. SaaS GWとクラウドとの通信	○	○	○	○	○	○	○	○	○	○
2. 通信上の保護と暗号化	○	○	○	○	○	○	○	○	○	○
3. なしすましの防止	○	○	○	○	○	○	○	○	○	○
XV. Remote Deployment Toolsに関するセキュリティー										
1. 通信の安全性 2. アクセス制限 3. データの管理 4. 電子署名 5. ウイルス対策	○	○	○	○	○	○	○	○	○	○
XVI. CWHに関するセキュリティー										
1. 2-way HTTPS通信でのセキュリティー	×	○	○	○	○	○	○	○	○	○
2. 1-way HTTPS通信でのセキュリティー	×	○	○	○	○	○	○	○	○	○
XVII. ユーザー情報の保護										
1. 個人情報の表示制限	○	○	○	○	○	○	○	○	○	○
2. 管理者パスワード設定	○	○	○	○	○	○	○	○	○	○
3. 簡易IPフィルタリング	○	○	○	○	○	○	○	○	○	○
4. 簡単セキュリティ設定へのショートカット表示	○	○	○	○	○	○	○	○	○	○
XVIII. Fleet RMMに関するセキュリティー										
1. 通信の安全性 2. アクセス制限 3. データの管理 4. 電子署名 5. ウィルス対策	○	○	○	○	○	○	○	○	○	○
XIX. MarketPlaceに関するセキュリティ										
1. クッキー	○	○	○	○	○	○	○	○	○	○
2. 暗号化	○	○	○	○	○	○	○	○	○	○
3. アカウント作成	○	○	○	○	○	○	○	○	○	○
4. アナリティクスツール	○	○	○	○	○	○	○	○	○	○
5. DDoSプロテクション	○	○	○	○	○	○	○	○	○	○
6. Konica Minolta MarketPlaceアプリケーション	○	○	○	○	○	○	○	○	○	○

(参考)

HDD暗号アルゴリズム (AES)	○ (AES256)									
SSD暗号アルゴリズム (AES)		○ (AES256)	○ (AES256)	○ (AES256)	○ (AES256)		○ (AES256)	○ (AES256)	○ (AES256)	
μSD暗号アルゴリズム (AES)		○ (AES256)				○ (AES256)				○ (AES256)

セキュリティーテクニカルサポートペーパー Version10.4 添付資料

各機能の適応機種一覧リスト

<カラーモノクロ　プログラッシブプリント機>

	bizhub PRO 1100	AccurioPress 6136/6120/6136P	AccurioPress C2070/C2070P/C2060 + IC-603	AccurioPress C2070/C2070P/C2060 + IC-313 + IC-417	AccurioPress C2070/C2070P/C2060 + IC-314	AccurioPress C6100/C6085 + IC-604	AccurioPress C6100/C6085 + IC-313 + IC-315	AccurioPress C6100/C6085 + IC-314	AccurioPress C3080/C3080P/C3080PV/C3070/C3070L + IC-605	AccurioPress C3080/C3080P/C3080PV/C3070/C3070P/C3070L + IC-313	AccurioPress C3080/C3080P/C3070/C3070P/C3070L + IC-314	AccurioPress C14000/C12000	AccurioPress C14000/C12000 + IC-610	AccurioPress C14000/C12000 + IC-319/318	AccurioPress C7100/C7090	AccurioPress C7100/C7090 + IC-609	AccurioPress C7100/C7090 + IC-319/318L	AccurioPress C4080/4070 AccurioPrint C4065	AccurioPress C4080/4070 AccurioPrint C4065 + IC-609	AccurioPress C4080/4070 AccurioPrint C4065 + IC-317/419	AccurioPress 6272P	AccurioPrint 2100	AccurioPress 7136/7120/7136P
I. 公衆電話回線に対するセキュリティー																							
1. FAX回線に対するセキュリティー	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
2. 宛先２度入力	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
3. チェーンダイアル	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
4. 宛先確認画面表示	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
5. 複数宛先禁止	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
6. 相手機種認識	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
II. LAN接続に対するセキュリティー																							
1. ネットワークプロトコルに対する対応	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
2. ユーザー認証	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3. ネットワーク経由の装置管理セキュリティー																							
(1) アドレス帳一括登録時のセキュリティー	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
(2) bizhub OpenAPI	△*17	△*17	△*17	–	–	△*17	–	–	△*17	–	–	△*17	△*17	–	△*17	△*17	–	△*17	△*17	–	△*17	△*17	△*17
4. データ通信の暗号化	○	○	○	○	○	○	○	○	○	–	○	○	○	○	○	○	○	○	○	○	○	○	○
5. 検疫ネットワーク対応	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
6. 双方向証明書検証	○*19	○*19	○*19	–	–	○*19	–	–	○*19	–	–	○*19	○*19	–	○*19	○*19	–	○*19	○*19	–	○*19	○*19	○*19
7. ウイルスに対する対応	○	○	○	–	○	○	–	○	○	–	○	○	○	–	○	○	–	○	○	–	○	○	○
8. ウイルススキャン機能	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
9. 外部からのUSBメモリを介してのウイルスへの対応状況	○	○	○	–	○	○	○	○	○	–	○	○	○	–	○	○	–	○	○	–	○	○	○
10. Linux kernelの定常監視	○	○	○	–	–	○	–	–	○	–	–	○	○	–	○	○	–	○	○	–	○	○	○
11. USB I/Fバスとの分離	○	○	○	–	○	○	–	○	○	–	○	○	○	–	○	○	–	○	○	–	○	○	○
12. 無線LANと有線LANとの通信分離	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
III. MFP本体内データのセキュリティー																							
1. 画像処理及び出力処理におけるセキュリティー	○	○	○	–	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
2. HDD一時保存データ上書き削除機能	○	○	○	–	○	○	–	○	○	–	○	–	○	–	–	○	–	–	○	–	○	–	–
3. HDD、SSD及びmicroSD取扱時のデータ完全消去	○	○	○	–	–	–	–	–	○	–	–	○	○	–	○	○	–	○	○	–	○	○	○
4. 全データの初期後のレポート出力機能	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
5. HDD、SSD及びmicroSDのデータの暗号化による保護	○	○	○	△*2	△*2	○	△*2	△*2	○	△*2	△*2	○	○	△*2	○	○	△*2	○	○	△*2	○	○	○
6. 自己暗号化によるSSDの保護	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
7. PDFファイルの暗号化	○	○	○	○	–	○	○	–	○	○	–	○	○	○	○	○	○	○	○	○	○	○	○
8. ユーザー認証																							
(1) 外部サーバと装置内部での認証機能	○	○	○	○	–	○	○	–	○	○	–	○	○	○	○	○	○	○	○	○	○	○	○
(2) ユーザー・部門単位での出力上限値管理	○	○	○	○	–	○	○	–	○	○	–	○	○	○	○	○	○	○	○	○	○	○	○
(3) カラー・モノクロ別出力権限と出力上限値管理	○	○	○	○	–	○	○	–	○	○	–	○	○	○	○	○	○	○	○	○	○	○	○
9. ボックスのセキュリティーとその活用	–	–	–	○	–	–	○	–	–	○	–	–	○	–	○	○	–	○	○	–	○	○	–
10. メールデータの暗号化	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
11. メールの署名機能	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
12. Scan to Me、Scan to Home & Scan to Authorized Folder	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
13. 監査ログによるアクセス管理	○	○	○	○	–	○	–	–	○	○	–	○	○	○	○	○	○	○	○	○	○	○	○
14. 認証を受けた暗号モジュールの採用	○	○	○	–	○	○	–	○	○	–	○	○	○	–	○	○	–	○	○	–	○	○	○
15. TPMによるデータ保護	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
IV. 出力データのセキュリティー																							
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	–	–	–	–	–	–	–	–	–	–	–	○	○	○	○	○	○	○	○	–	–	–	–
(2) コピーガード機能/パスワードコピー機能	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
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ー	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
2. 認証＆プリント（ワンタッチセキュリティー）	○*21	○*21	○*21	–	–	○*21	–	–	○*21	–	–	○*21	–	–	○*21	–	–	○*21	–	–	○*21	○*21	○*21
VI. モバイル機器との連携におけるセキュリティー																							
1. AirPrintに対するセキュリティー	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
2. Mopriaに対するセキュリティー	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
3. Google Cloud Printに対するセキュリティー	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
4. Konica Minolta Print Serviceに対するセキュリティー	○	○	○	–	–	○	–	–	○	–	–	○	–	–	○	–	–	○	–	–	○	○	○
5. PageScope Mobileに対するセキュリティー	○	○	○	–	–	○	–	–	○	–	–	○	–	–	○	–	–	○	–	–	○	○	○
VII. PKIカード認証システム																							
1. PKIカードを使用したログイン	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
2. PKIカードを使用したLDAP検索	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
3. PKIカードを使用したSMB送信	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
4. PKIカードを使用したE-mail送信（S/MIME）	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
5. PKIカードプリント	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
6. Scan To Me/Scan To Home	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
VIII. MFP自己保護に関するセキュリティー																							
1. Firmware検証機能	○	○	○	–	–	○	–	–	○	–	–	○	○	–	○	○	–	○	○	–	○	○	○
IX. CS Remote Careに関するセキュリティー																							
1. 基本的なセキュリティと収集データ	○	○	○	–	–	○	–	–	○	–	–	○	–	–	○	○	–	○	○	–	○	○	○
2. LTEを用いた場合のセキュリティーについて	○	○	○	–	–	○	–	–	○	–	–	○	–	–	○	○	–	○	○	–	○	○	○
3. メールでのセキュリティー	○	○	○	–	–	○	–	–	○	–	–	○	–	–	○	○	–	○	○	–	○	○	○
4. HTTP通信でのセキュリティー	○	○	○	–	–	○	–	–	○	–	–	○	–	–	○	○	–	○	○	–	○	○	○
5. DCAでのセキュリティー	○	○	○	–	–	○	–	–	○	–	–	○	–	–	○	○	–	○	○	–	○	○	○
X. Remote Panelに関するセキュリティー																							
1. 通信、接続トリガー	○	○	○	–	–	○	–	–	○	–	–	○	–	–	○	–	–	○	–	–	○	○	○
2. 認証	○	○	○	–	–	○	–	–	○	–	–	○	–	–	○	–	–	○	–	–	○	○	○
3. Access Code	○	○	○	–	–	○	–	–	○	–	–	○	–	–	○	–	–	○	–	–	○	○	○
4. 監査ログ	○	○	○	–	–	○	–	–	○	–	–	○	–	–	○	–	–	○	–	–	○	○	○
XI. World Wide Remote Service Platformに関するセキュリ																							
1. WWSPFとMFP間の通信	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
2. WWSPFとXMPP PF間の通信（MFPに依存しない）	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
3. XMPP PFとMFP間の通信	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
4. WWSPFからMFPへの通信	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
5. WWSPFとCSRC連携（MFPに依存しない）	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
6. RSA (Remote Service Agent) を使った通信																							
7. RSA Edgeの登録とRSA CloudおよびAWS IoTとの接続に必要な情報の取得																							
8. RSA EdgeとRSA Cloudの通信																							
9. RSA EdgeとAWS IoTの通信																							
XII. bizhub Remote Accessに関するセキュリティー																							
1. ペアリング	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
2. 通信、接続トリガー	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
3. タイムアウトによる自動切断	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
4. 管理者モード中のセキュリティー	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
5. リモート操作中に切断された時のセキュリティー	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
6. ユーザー認証・部門認証併用時のセキュリティー	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
XIII. CSRA(CS Remote Analysis)に関するセキュリティー																							
1. HTTP通信でのセキュリティー	○	○	○	○	–	○	○	–	○	–	–	○	–	–	○	–	–	○	–	–	○	○	○
XIV. MFP内蔵SaaS GWに関するセキュリティー																							
1. SaaS GWとクラウドとの通信	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
2. 通信上の保護と暗号化	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
3. なしすましの防止	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
XV. Remote Deployment Toolsに関するセキュリティー																							
1. 通信の安全性 2. アクセス制限 3. データの管理 4. 電子署名 5. ウイルス対策	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
XVI. CWHに関するセキュリティー																							
1. 2-way HTTPS通信でのセキュリティー	–	–	–	–	–	–	–	–	–	–	–	○	–	–	○	–	–	○	–	–	–	○	○
2. 1-way HTTPS通信でのセキュリティー	–	–	–	–	–	–	–	–	–	–	–	○	–	–	○	–	–	○	–	–	–	○	○
XVII. ユーザー情報の保護																							
1. 個人情報の表示制限					–			–			–	○	○	–	○	○	–	○	○	–		○	○
2. 管理者パスワード設定	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3. 使用ボックスリンク	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
4. 簡単セキュリティ設定へのショートカット表示	○*24	○*24	○*24	–	–	○*24	–	–	○*24	–	–	○*24	–	–	○*24	–	–	○*24	–	–	○*24	○*24	○*24
XVIII. Fleet RMMに関するセキュリティー																							
1. 通信の安全性 2. アクセス制限 3. データの管理 4. 電子署名 5. ウイルス対策	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
XIX. MarketPlaceに関するセキュリティー																							
1. クッキー 2. 暗号化 3. アカウント作成 4. アナリティクスツール 5. DDoSプロテクション 6. Konica Minolta MarketPlaceアプリケーション	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

(参考)

HDD暗号アルゴリズム (AES)	○ (AES128/256) *22	○ (AES128/256) *22	○ (AES128/256) *22		○ (AES128)	○ (AES128/256) *22		○ (AES128)	○ (AES128/256) *22		○ (AES128)	○ (AES256)	○ (AES256)		○ (AES256)	○ (AES256)		○ (AES256)	○ (AES256)		○ (AES128/256) *22	○ (AES128/256) *22	○ (AES128/256) *22
SSD暗号アルゴリズム (AES)	○ (AES128) *23	○ (AES128) *23	○ (AES128) *23		–	○ (AES128) *23		–	○ (AES128) *23		–	○ (AES256)	–		○ (AES256)	–		○ (AES256)	–		○ (AES128) *23	○ (AES256)	○ (AES256)
μSD暗号アルゴリズム (AES)												–	–		–	–		–	–			–	–

*2：HDD内のデータ暗号化機能には非対応、Scan to HDDは共用フォーマットで圧縮、出力/転送時に削除されるのは管理データのみでデータ自体は削除されない。
*17：特定のアプリにのみ使用可
*19：クライアント証明書サポート
*21：AU201+PaperScope MyPrintManager接続時に可
*22：ジョブ保存領域(画像データは256bit/それ以外は128bit
*23：機械設定情報を暗号化する
*24：USB使用設定は対象外となります