セキュリティーホワイトペーパー

キヤノン複合機/プリンターの NIST SP 800-171/NIST SP 800-172 への対応

Version 1.00

2022/1/15

本書の趣旨

このドキュメントでは、キヤノン複合機/プリンターにおける重要情報を管理・保護するためのサイバーセキュリティー対策について説明します。また、キヤノン複合機/プリンターがサイバーセキュリティーに関するセキュリティーガイドラインにどのように対応するかを示します。

このドキュメントで示す「キヤノン複合機/プリンター」の対象機種は、以下の URL からご確認ください。
https://oip.manual.canon/USRMA-7491-zz-CSPS-jaJP/

対象機種およびこのドキュメントの内容は更新されることがあります。対策を実施する前に、最新版のドキュメントをマニュアルポータルサイトで確認することをおすすめします。

マニュアルポータルサイト：
https://oip.manual.canon/

このドキュメントでは、サイバーセキュリティーガイドラインとして、米国国防総省、防衛省等の取引企業に対して準拠が要求されている NIST SP 800-171、その補足である NIST SP 800-172 への対応を示します。これらのガイドラインは、特定の製品やその機能に対する要件ではなく、重要情報を管理する企業・組織及びそのシステムに対する要件を定めています。そのため、ガイドラインへの適合には、主に企業・組織側の対応が求められますが、そのシステムに含まれる複合機/プリンターがどのように重要情報を取り扱い、管理しているかを理解することは重要です。その理解のためにこのドキュメントを活用できます。尚、現在 NIST SP 800-171 や NIST SP 800-172 の要件を基にした第三者評価/認証のプロセスとして CMMC 2.0*[1]の制度化が検討されています。今後、CMMC が制度化された際にはこのドキュメントを更新する予定です。

このドキュメントは、企業・組織のセキュリティー管理者やキヤノン複合機/プリンターの設定とメンテナンスを担当する管理者を対象としています。キヤノン複合機/プリンターは、お客様が使用する際に、システムによって処理および保存される重要情報の管理とセキュリティーを促進するのに役立つ、多数の標準機能とオプション機能を提供します。最終的に、情報のセキュリティー保護に最適な方法を選択するのはお客様の責任です。

このドキュメントに記載されている情報を使用することによって、悪意のある攻撃やお客様のキヤノン複合機/プリンターの悪用が防止されることをキヤノンが保証するものではありません。また、お客様の環境及び複合機/プリンターがこのドキュメントで説明するセキュリティーガイドラインに適合することをキヤノンが保証するものではありません。

---

*[1] CMMC(Cybersecurity Maturity Model Certification)：米国国防総省が規定するサイバーセキュリティー成熟度モデルに対する認証。

本対策はお客様により実施していただくものになります。お客様の作業を代行する場合は別途費用が発生する場合があります。

このドキュメントで紹介する機能には、キヤノン複合機/プリンターの標準機能とオプション機能の両方が含まれます。仕様および入手方法は予告なく変更されることがあります。

目次

1 はじめに 5

2 キヤノン複合機/プリンターのサイバーセキュリティー対策について 7

2.1 識別/保護 8

2.2 検知/対応/復旧 11

3 サイバーセキュリティーガイドラインへの対応 13

3.1 サイバーセキュリティーガイドライン 13

3.1.1 NIST SP 800-171 13

3.1.2 NIST SP 800-172 14

3.2 キヤノン複合機/プリンターのサイバーセキュリティーガイドラインへの対応 15

4 まとめ 19

5 Appendix 20

5.1 NIST SP 800-171 要件対応表 21

5.2 NIST SP 800-171 要件対応表 37

1 はじめに

企業・組織においてシステムで取り扱う重要情報を管理・保護し、不正アクセスや機密データ漏洩等のサイバーセキュリティーリスクへの対策を備えることは不可欠です。近年ますます高度化、複雑化するサイバーセキュリティーリスクに対して企業・組織が効果的に対策を実施するために、標準フレームワークやセキュリティーガイドラインが発行されています。

標準フレームワークとしては、2014 年に米国国立標準技術研究所(以降、NIST) から Cybersecurity Framework (以降、CSF)が発行されました。正式名称は、「重要インフラのサイバーセキュリティーを改善するためのフレームワーク」(Framework for Improving Critical Infrastructure Cybersecurity)です。NIST CSF は、重要インフラのサイバーセキュリティーリスクマネジメントの改善を目的として作成され、米国に限らず様々な国の企業・組織で参考にされています。このようなフレームワークを、サイバーセキュリティーリスクを管理するためのツールとして使用することで、組織は重要サービスを提供するうえで最も必要な対策を判断し、投資の優先順位を決定することが可能となり、結果として投資の効果を最大限に引き出すことができます。

NIST CSF に則って、より具体的にサイバーセキュリティーの管理要件や対策を規定したガイドラインが整備されており、2015 年には NIST から「非連邦政府組織およびシステムにおける管理対象非機密情報 CUI(Controlled Unclassified Information)の保護」 として NIST SP 800-171 が発行されました。CUI[*2]は、機密ではないが、管理対象となる重要な情報のことを指します。本書では分かり易さのため、CUI を重要情報と表記する場合があります。近年、自組織内のセキュリティー対策に限らず、サプライチェーン全体で同レベルのセキュリティー対策が備えられていることが重視されています。サプライチェーンの関係者間でそれぞれの企業・組織がどのようなセキュリティー基準に従ってセキュリティー対策を行っているかを示すことがサプライチェーンリスクマネジメントとして求められます。実際に、米国国防総省と取引をする企業・組織には NIST SP 800-171 に準拠して重要情報を管理していることが要求されています。日本の防衛省でも 2019 年から NIST SP 800-171 と同レベルの調達基準を設けることが試行導入されています。今後、米国に限らず各国の企業・組織にて NIST SP 800-171 相当のセキュリティー基準を求められることが予想されるため、NIST SP 800-171 のセキュリティー基準に従って企業・組織のセキュリティー対策を行うことは有効と考えられます。

このドキュメントは、 キヤノン複合機/プリンターを導入及び運用するお客様のサイバーセキュリティー対策の検討を支援することを目的としています。このドキュメントでは、まず、サイバーセキュリティー対策として、キヤノン複合機/プリンターがどのようなソ

[*2] CUI(Controlled Unclassified Information)：管理対象非機密情報。NARA(National Archives and Records Administration：米国国立公文書記録管理局)の CUI レジストリーで管理されており、例えば、製品の設計図や仕様書などが該当。

リューションを提供しているかを NIST CSF に沿って説明します。そして、サイバーセキュリティーガイドラインとして NIST SP 800-171、その補足である NIST SP 800-172、これらのガイドラインで求められる要件を満たすためにキヤノン複合機/プリンターが提供する機能及び推奨する設定を示しています。Appendix の「要件対応表」には、さらに詳細な要件とキヤノン複合機/プリンターの機能との対応付け、お客様の企業・組織側で実施すべき対策例について記載しています。

2 キヤノン複合機/プリンターのサイバーセキュリティー対策について

複合機/プリンターは企業・組織のシステムのネットワークに接続され、文書データ等の重要情報を取り扱います。そのため、複合機/プリンターに対してもその他の情報機器と同じようにセキュリティー対策が不可欠です。キヤノン複合機/プリンターはサイバーセキュリティー対策として必要な「識別(Identify)」、「保護(Protect)」、「検知(Detect)」、「対応(Respond)」、「復旧(Recover)」の５つの要素を達成できるように機能を備えています。これらの５つの要素は NIST CSF でフレームワークコアの機能として定められたものです。これらの５つの機能に対して網羅的に対応することで、サイバーセキュリティーリスクからの防御にとどまらず、サイバーセキュリティーリスクの早期の発見と復旧を可能とします。特に、近年の高度化するサイバー攻撃に対しては、サイバー攻撃を受けた際/後の対策として「検知」、「対応」、「復旧」の機能が重視されており、キヤノン複合機/プリンターにおいてもそれらの機能に対する対策を強化してきました。

次節では、キヤノン複合機/プリンターが提供するサイバーセキュリティー対策に有効なセキュリティー機能について、NIST CSF のフレームワークコアの５つの機能を利用して説明します。

フレームワークコアの５つの機能

識別 (Identify)	システム、人、データ、機能に対するサイバーセキュリティーリスクの管理に必要な理解を深める。
保護 (Protect)	重要サービスの提供を確実にするための適切な保護対策を検討し、実施する。
検知 (Detect)	サイバーセキュリティーイベントの発生を識別するのに適した対策を検討し、実施する。
対応 (Respond)	検知されたセキュリティーインシデントに対処するための適切な対策を検討し、実施する。
復旧 (Recover)	レジリエンスを実現するための計画を策定・維持し、サイバーセキュリティーインシデントによって阻害されたあらゆる機能やサービスを元に戻すための適切な対策を検討し、実施する。

2.1 識別/保護

➢ ユーザーの認証/アクセス制御

キヤノン複合機/プリンターは、承認されたユーザーのみが機器およびその機能（印刷、コピー、スキャン、送信機能など）にアクセスできるようにするために管理者が使用できる認証オプションを多数搭載しています。

ログインサービス(User Authentication)

ユーザーごとに登録した情報により個人認証を行うため、複合機/プリンターにアクセス可能なユーザーを限定することができます。ネットワーク上の Active Directory や LDAP サーバーを認証サーバーとして追加指定して、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。また、IC カードを使用したユーザー認証にも対応しており、暗証番号と併用することで多要素認証を実現することができます。

ACCESS MANAGEMENT SYSTEM

権限レベル（ロール）ごとに使用できる機能を割り当てたり、新しいロールを作成したりすることができます。これにより、「A さんはコピー禁止」、「B さんは全機能利用 OK」という具合にユーザーごとに異なるロールを設定することもできるため、さらにきめ細かいユーザー管理が可能です。

アドバンスドボックスの認証管理

キヤノン複合機/プリンターに搭載されているストレージには、「アドバンスドボックス」と呼ばれる公開スペースがあります。アドバンスドボックスは、SMB または WebDAV プロトコルによって同一ネットワーク上で公開することも可能です。アドバンスドボックスを公開する際に認証設定を行うことで不正アクセスを防止できます。

➢ ネットワークの認証/アクセス制御

悪意のある第三者による通信内容の盗聴や改ざん、なりすましなどにより、正規ユーザーに想定外の損失をもたらす恐れがあります。大切なデータや情報を守るため、ネットワークのセキュリティーを高めるさまざまな対策を用意しています。

ファイアウォール設定

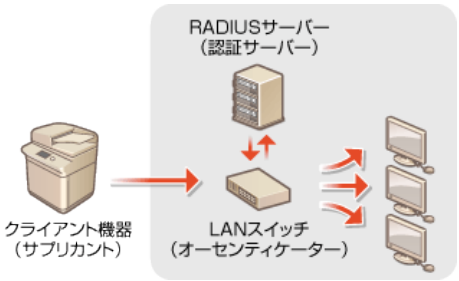
ファイアウォール設定を行うことで、特定の IP アドレスを持つ機器との通信だけを許可し、第三者の不正アクセス、ネットワークへの攻撃や侵入を遮断できます。

プロキシー設定

プロキシー設定を行うことで、ウェブサイトの閲覧時にプロキシーサーバーを経由して外部に接続できます。プロキシーサーバーを使うとより安全にウェブサイトを閲覧することができるため、セキュリティーの向上が期待できます。

IEEE 802.1X 認証

IEEE 802.1X を導入したネットワークにクライアントとして接続することができます。
IEEE 802.1X を導入することで認証されていない機器からの通信要求を遮断できます。



➢ データセキュリティー

キヤノン複合機/プリンターは、業界標準のアルゴリズムを使用してデータ暗号化を行うことで、内蔵ストレージに保存されているデータや、ネットワークを介して伝

送中のデータを確実に保護します。ストレージやネットワークのデータ暗号化には FIPS 140[*3]認証を取得した暗号モジュールを使用しています。

ストレージデータの暗号化

複合機/プリンターのストレージには、アドバンスドボックスやユーザーボックス内のファイル、アドレス帳の登録情報、残存するジョブデータ、パスワード情報などが保存されています。キヤノン複合機/プリンターは、これらのデータを常時、暗号化することにより、情報を不正に読み取られることを防いでいます。

TPM(Trusted Platform Module)

キヤノン複合機/プリンターは、機密情報を安全に管理するため TPM チップを搭載しています。複合機/プリンターに記録されているパスワード、TLS 通信用公開鍵ペア、ユーザー証明書などの機密情報を TPM チップで保護された暗号鍵により暗号化します。これにより、複合機/プリンターの物理解析や不正アクセスによる機密情報の漏えいを抑止できます。

TLS 暗号化通信(ネットワークデータの暗号化)

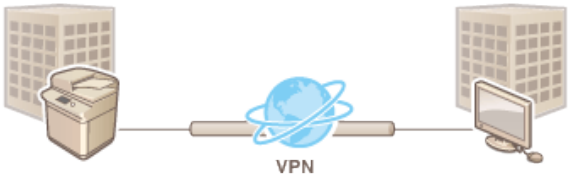
パソコンなどの機器から複合機/プリンターにアクセスしてデータをやりとりする際に、盗聴、改ざん、なりすましなどを防ぐために、TLS 暗号化通信を利用することができます。

IPSec 通信(ネットワークデータの暗号化)

TLS 暗号化通信は Web ブラウザーや電子メールクライアントなど、特定のアプリケーションで暗号化する技術ですが、IPSec 通信は IP プロトコルのレベルで暗号化を行います。そのため、さらに汎用性の高いセキュリティーを実現できます。

---

*3 FIPS(Federal Information Processing Standards) 140：暗号モジュールに対するセキュリティー要件を規定した米国連邦情報処理標準規格。



さらにキヤノン複合機/プリンターは、ユーザーの操作によっては情報流失につながる機能や、悪用される恐れのある機能に対して使用条件を設定し、機能を制限することで文書データを保護することが可能です。

留め置き印刷

「印刷物放置による持ち去り」や「意図しない情報開示」、「ミスプリント防止」などの目的で、管理者によって強制的にいったん印刷する文書を複合機/プリンター内に留めることができます。留め置かれた文書データはユーザーやグループに紐づけて管理され、不正な印刷を防止します。

メモリーメディアの使用の制限

USB メモリーなどのメモリーメディアは手軽で便利な反面、適切に管理されていない環境下では逆に情報漏えいの要因となる恐れがあります。メモリーメディアの使用を禁止して、スキャン文書をメモリーメディアに保存できなくしたり、メモリーメディア内のデータを印刷できないようにすることができます。

2.2 検知/対応/復旧

- セキュリティーモニタリング

サイバーセキュリティー対策として、システムの動作を監視し、システムや組織に影響を及ぼす可能性のあるイベントを検知・追跡し、対応することが求められます。キヤノン複合機/プリンターは、機器の使用を監視するためにログ機能を搭載しています。機器がどのように使用されているかを確認／分析するために、ログを活用することが有効です。

監査ログ機能

監査ログ機能を利用してセキュリティーのイベントを監査することが可能です。例えば、ユーザー認証のログによって機器への不正アクセスやその試行がないか、また印刷や文書送信、設定変更などの機器利用時のログによって機器の不正使用がないかを監査することができます。また、SIEM[*4]システムとの連携により、ログの収集／分析やセキュリティーインシデントの通知が可能となります。

[*4] SIEM: Security Information and Event Management システム内の機器やソフトウェアのログを収集・管理・分析し、セキュリティーインシデントを検知するシステム

- サイバーレジリエンス

サイバーレジリエンスとは、サイバー攻撃による被害を最小化するために、システムが攻撃を受けた場合、それを検知し速やかに元の状態に復旧するよう備えることです。「サイバー攻撃の検知」、「検知したサイバー攻撃への対応」、「サイバー攻撃による被害からシステムを復旧」の三つの観点で対応することが求められます。キヤノン複合機/プリンターは、サイバーレジリエンス対策のための機能を備えています。

起動時のシステム検証/ランタイムシステム保護

システムの完全性を検証するソリューションとして、ハードウェアを起点とした起動時のシステム検証機能と稼働時にソフトウェアの変更を監視し不正な変更を防止するランタイム保護機能を提供しています。それにより、システムに悪意あるコードが混入しないよう常に監視できます。ランタイム保護機能には、アローリスト(ホワイトリスト)方式のマルウェア対策技術を搭載し、信頼されたアプリケーションしか動作しないよう制御すると共に、システムの不正変更の防止を実現しています。

ファームウェア/アプリケーションの改ざん防止

ファームウェアのアップデートやアプリケーションのインストールを実施する際には、デジタル署名による検証を実施し、不正なプログラムのインストールを防止しています。

データのバックアップ／リストア機能

管理者は、必要に応じてデータのバックアップ／リストア機能を用いて、機器のデータや設定をバックアップまたは復元することが可能です。

これらはキヤノン複合機/プリンターが提供するセキュリティー対策の一部です。キヤノン複合機/プリンターは、そのほかにも様々なセキュリティー機能を搭載しており、お客様の環境に合わせて柔軟にカスタマイズ可能です。詳細は、キヤノンのホームページをご覧ください。

3 サイバーセキュリティーガイドラインへの対応

キヤノン複合機/プリンターのサイバーセキュリティー対策がサイバーセキュリティーガイドラインで定められるセキュリティー要件にどのように対応しているのかを説明します。このドキュメントでは、サイバーセキュリティーガイドラインとして、NIST SP 800-171、NIST SP 800-172 への対応を示します。

3.1 サイバーセキュリティーガイドライン

3.1.1 NIST SP 800-171

米国政府機関の情報システムが準拠を義務付けられている、重要情報の処理、保存、転送に関する規定(連邦情報処理規格（FIPS）200『連邦政府情報および情報システムに関する最低限のセキュリティー要件』および、NIST SP 800-53『連邦政府情報システムおよび組織のためのセキュリティーおよびプライバシー管理策』)から、重要情報を共有する非政府機関の情報システムに必要となる推奨要件を導出したのが NIST SP 800-171 です。そのため、NIST SP 800-171 に適合することによって、重要情報を処理、保存、転送するシステムの構成要素に対する保護レベルを政府機関の情報システムと同等に保つことが可能になります。なお、NIST SP 800-171 は米国国防総省、防衛省等の取引企業に対して準拠が要求されています。

NIST SP 800-171 では重要情報を保護するための 110 個のセキュリティー要件が、14 のファミリで構成され規定されています。それぞれのファミリには、そのファミリの一般的なセキュリティトピックに関連する要件が含まれています。また、セキュリティー要件は基本となる「基本セキュリティー要件」と、それを達成するために追加で必要な「派生セキュリティー要件」から構成されています。

セキュリティー要件ファミリ

ファミリ	説明
アクセス管理	システムへアクセスできるユーザー／デバイスの制限
意識向上と訓練	組織の人員に対するセキュリティー教育と訓練
監査と説明責任	システムの監査と監査情報に対する追跡および説明責任の維持
構成管理	システムの構成基準の確立と管理
識別と認証	システムを利用するユーザー／デバイスの識別と認証
インシデント対応	インシデントに対する追跡と報告
メンテナンス	システムに対するメンテナンスの実施
記憶媒体の保護	メディア内の重要情報の保護と重要情報に対するアクセスの制限
要員のセキュリティー	システムにアクセスできる個人の審査
物理的保護	システムに対する物理的アクセスの制限
リスク評価	システムに対するリスク評価
セキュリティー評価	組織のセキュリティー管理策の評価
システムと通信の保護	システム境界における通信の監視・制御・保護
システムと情報の完全性	システムと情報に関する完全性の確保

3.1.2 NIST SP 800-172

NIST SP 800-172 では、NIST SP 800-171 の補足として、重要情報をより高度な標的型攻撃である Advanced Persistent Threat(APT)から保護するのに役立つ、強化されたセキュリティー要件を規定しています。2021 年 2 月に公開されました。

NIST SP 800-172 は、以下及び下図で説明する 3 つの戦略(PRA, DLO, CRS)からなる多層防御戦略による APT 対策を規定しています。NIST SP 800-172 の要件はそれぞれ、PRA, DLO, CRS のいずれかの戦略、もしくは複数の戦略を実施するための要件となります。基本対策である NIST SP 800-171 の要件に加え、多層防御を実現する NIST SP 800-172 の要件にも対応することで、仮に APT で組織のシステムに不正侵入されたとしても、侵入による影響(損害)の抑制や迅速なシステム回復により多層的に APT の影響を最小化することが期待できます。

- PRA(Penetration-Resistant Architecture)

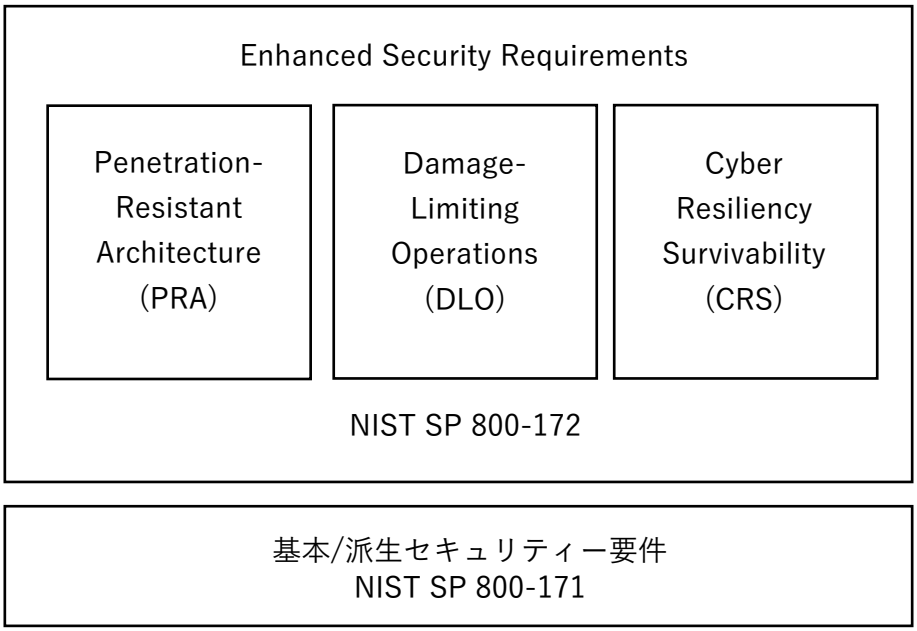
  攻撃者やマルウェアが組織のシステムに侵入しそのまま常駐する機会を、技術と手続きにより抑制するアーキテクチャとする戦略

- DLO(Damage-Limiting Operations)

  「『攻撃者による侵害の検知』および『侵害の影響の制限』」をする組織の能力を手続き及び運用で最大化する戦略

- CRS(Cyber Resiliency Survivability)

  ミッションまたは事業活動を最大化するために、サイバーリソースの侵害に対する準備、対処、回復、及び適応能力を提供するためのシステム、ミッション、事業機能を設計する戦略



NIST SP 800-172 では NIST SP 800-171 と同様の 14 のファミリから構成され、35 個のセキュリティー要件が規定されています。

3.2 キヤノン複合機/プリンターのサイバーセキュリティーガイドラインへの対応

これらのサイバーセキュリティーガイドラインへ対応するため、キヤノン複合機/プリンターがどのようなセキュリティー対策を提供しているか、キヤノン複合機/プリンターをどのように運用すべきかを説明します。これらのガイドラインは重要情報を管理する企業・組織に対する要件を定めたものであり、特定の製品やその機能に対する要件を定めたものではありません。そのため、今回ガイドラインへの対応を

確認するために、まず各ガイドラインの要件から複合機/プリンターに関連する要件を抽出し、抽出した要件に対して、重要情報を保護するためにキヤノン複合機/プリンターが提供する機能をどのように活用できるかを確認しました。また、キヤノン複合機/プリンターの機能を正しく活用するための機器の設定についても確認しました。

ガイドラインの要件に対応する機能としてキヤノン複合機/プリンターは次の機能を提供しています。各機能の説明は 2 章を参照ください。また、機能を適切に活用するために推奨する設定を示します。各ガイドラインの要件と機能の対応及び設定項目の詳細は、Appendix の「要件対応表」に記載しています。設定の際には要件対応表を活用ください。

ガイドラインに対応する機能と推奨設定

機能	推奨設定	対応する NIST SP 800-171/172 のファミリ
ユーザー認証/アクセス制御	機器を利用するユーザーを管理するためユーザー認証機能を有効にし、利用者の設定をしてください。また、アクセス制限機能(ACCESS MANAGEMENT SYSTEM)やパスワードポリシー、ロックアウト設定を適切に設定してください。 アドバンスドボックスを利用する場合は認証管理を設定してください。	アクセス管理 監査と説明責任 識別と認証 システムと通信の保護
ファイアウォール設定	ファイアウォール設定を行い機器との通信を管理してください。	アクセス管理 システムと通信の保護
プロキシー設定	プロキシー設定を行ってください。	アクセス管理 システムと通信の保護
TLS 設定	TLS 暗号化通信を利用するよう設定してください。また、環境に応じてサーバー証明書の検証を実施するよう設定してください。 さらに、信頼できる認証局によって発行されたサーバー鍵・証明書を機器に登録し、TLS 暗号化通信の使用鍵として設定することでよりセキュリティーを向上させることができます。 暗号方式を FIPS 140 準拠にするよう設定してください。	アクセス管理 識別と認証 システムと通信の保護
IPSec 設定	環境に応じて IPSec 設定を設定してください。	アクセス管理 システムと通信の保護
IEEE 802.1X 設定	IEEE 802.1X を導入する場合は IEEE 802.1X の設定をしてください。	アクセス管理

機能	推奨設定	対応する NIST SP 800-171/172 のファミリ
監査ログ	監査ログ機能を有効化してください。SIEM システムと連携する場合は、Syslog 設定を行ってください。 また、機器の日時を正しく設定して下さい。SNTP 設定によりサーバーと時刻同期を行うことも可能です。	アクセス管理 監査と説明責任 インシデント対応
メモリーメディアの使用の制限	USB メモリーなどのメモリーメディアの使用を禁止するよう設定してください。	記憶媒体の保護
留め置き印刷	機能を有効化してください。	システムと通信の保護
ストレージデータの暗号化	常に有効のため設定不要です。	監査と説明責任 識別と認証 システムと通信の保護
TPM(Trusted Platform Module)	機能を有効化してください。 TPM の設定を有効にしたら、ただちに TPM キーを USB メモリーにバックアップしてください。	システムと通信の保護
起動時のシステム検証	機能を有効化してください。	構成管理 システムと情報の完全性
ランタイムシステム保護	機能を有効化してください。	構成管理 システムと情報の完全性
ファームウェア/アプリケーションの改ざん防止	常に有効のため設定不要です。	構成管理 システムと情報の完全性

ガイドラインではシステム内の機器を正しく運用・管理することが求められます。機器を管理するために役立つ機能として、キヤノン複合機/プリンターは以下の機能を提供しています。

機器の管理機能

機能	推奨設定	対応する NIST SP 800-171/172 のファミリ
セキュリティーポリシー設定	セキュリティーポリシー機能により情報セキュリティーに関わる機器の設定を一括して適用／管理することができます。	構成管理
機器情報の表示	カウンター/機器情報により、本体のシリアル No.や IP アドレス、バージョン、オプションなどのデバイス構成を確認することができます。	構成管理
SMS（Service Management Service）	キヤノン複合機/プリンターには機器に搭載されている機能を拡張/最適化するための MEAP（Multifunctional Embedded Application Platform）という仕組みが搭載されています。 SMS を利用して、MEAP アプリケーションのインストールや使用状況を確認することができます。	構成管理
ファームウェアの定期アップデート	定期的に新しいファームウェアをチェックして、自動的にアップデートを行うことができます。	構成管理 システムと情報の完全性
すべてのデータ/設定の初期化	機器を廃棄または再利用の際、機器に保存されたデータを完全に消去することができます。	メンテナンス システムと通信の保護
データのバックアップ／リストア	機器のメンテナンスのために機器に保存されているデータをバックアップ/リストアすることができます。	メンテナンス

Appendix の「要件対応表」には、各ガイドラインで規定された要件毎に、要件に対応するためにキヤノン複合機/プリンターのこれらの機能をどのように活用できるか、どのように設定・運用すべきかを記載しています。また、ガイドラインの要件を達成するために企業・組織側で実施すべき対策例についても記載しています。詳細は Appendix の「要件対応表」をご覧ください。

4 まとめ

キヤノン複合機/プリンターはサイバーセキュリティー対策として様々なソリューションを提供しています。これらを適切に運用することで NIST SP 800-171、NIST SP 800-172 で規定されたセキュリティー要件の中で情報機器に対して求められる要件に対応することが可能となります。最終的に、NIST SP 800-171、NIST SP 800-172 で求められるサイバーセキュリティー対策を実施するのは、お客様の企業・組織です。キヤノンはお客様のサイバーセキュリティー対策を支援しています。

5 Appendix

Reference

- NIST CSF

  https://www.nist.gov/cyberframework

- NIST SP 800-171 Revision2

  https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

- NIST SP 800-172

  https://csrc.nist.gov/publications/detail/sp/800-172/final

5.1　NIST SP 800-171 要件対応表

ガイドラインの要件に対応するための設定を行う際には、この要件対応表をご活用ください。

NIST SP 800-171 rev2 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンター側の対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.1 アクセス管理 Basic (基本セキュリティー要件)	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	本要件は、システム・プロセス・デバイスそれぞれへのアクセスを適切なユーザーに限定することを要求するものです。本要件に対応する本機の機能を利用することで、各種アクセス制限を実現できます。	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。 **ACCESS MANAGEMENT SYSTEM** 権限レベル（ロール）ごとに使用できる機能を割り当てたり、新しいロールを作成したりすることができます。	＜ユーザー管理＞を設定する ＜ACCESS MANAGEMENT SYSTEMを使用＞を有効にする	本機を使用する際に、アカウント管理を実施してください。 アカウント管理としては次のような対応が必要です。 ・ユーザーアカウントの作成 ・アクセス制御ポリシーに従った権限の付与 ・パスワードの管理 　デフォルトパスワードの変更 　パスワードポリシーの設定 ・不要になったアカウントの削除
	3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	本要件は、アクセス権を有するユーザーに対して、ユーザー属性別に利用機能の制限を要求するものです。本要件に対応する本機の機能を利用することで、ユーザーのロール別の機能制限を実現できます。	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。 **ACCESS MANAGEMENT SYSTEM** 権限レベル（ロール）ごとに使用できる機能を割り当てたり、新しいロールを作成したりすることができます。	＜ユーザー管理＞を設定する ＜ACCESS MANAGEMENT SYSTEMを使用＞を有効にする	本機を使用する際に、アカウント管理を実施してください。 アカウント管理としては次のような対応が必要です。 ・ユーザーアカウントの作成 ・アクセス制御ポリシーに従った権限の付与 ・パスワードの管理 　デフォルトパスワードの変更 　パスワードポリシーの設定 ・不要になったアカウントの削除
3.1 アクセス管理 Derived (派生セキュリティー要件)	3.1.3	Control the flow of CUI （Controlled Unclassified Information） in accordance with approved authorizations.	本要件は、システム間のCUI（Controlled Unclassified Information）トラフィックフローの制御を要求するものです。本要件に対応する機能として、本機はファイアウォール，プロキシ等のトラフィックフロー制御機能を提供しています。組織は、組織が定義した CUI 制御フローポリシーに則り、本機にファイアウォール等を適切に設定する必要があります。	**ファイアウォール** ファイアウォールとは、外部ネットワークからの不正アクセスを防止し、ローカルエリア内のネットワークへの攻撃や侵入を防ぐシステムです。お使いのネットワーク環境で、特定の外部IPアドレスからの通信を制限することで、危険と思われる外部からのアクセスをあらかじめ遮断できます。 **プロキシー設定** ウェブサイトの閲覧時にプロキシーサーバーを経由して外部に接続します。プロキシーサーバーを使うとより安全にウェブサイトを閲覧することができるため、セキュリティーの向上が期待できます。	＜ファイアウォール設定＞を設定する ＜プロキシー設定＞を有効にする	ユーザーは承認された情報フロー制御を実施するために、ファイアーウォール、プロキシーサーバー等のトラフィックフロー制御機能を適切に構築してください。 本機に対して適切なネットワーク設定を実施してください。
	3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	本要件は、組織に属する個人の適切な職務分離を要求するものです。本要件の主な責務は組織側であり、組織側の職務定義・分離が必要となります。一方、組織側の対応をサポートする機能として、本機は管理者・一般ユーザーなどのデフォルトロールに加え、独自ロールの設定と各種機能の利用制限をカスタマイズできる機能を提供しています。例えば、組織で定義した職務に応じた独自ロールを設定し、利用することで、本機の機能利用においても適切な職務分離が実現できます。	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。 **ACCESS MANAGEMENT SYSTEM** 権限レベル（ロール）ごとに使用できる機能を割り当てたり、新しいロールを作成したりすることができます。	＜ユーザー管理＞を設定する ＜ACCESS MANAGEMENT SYSTEMを使用＞を有効にする	ユーザーは個人の職務を分離し、職務に応じたアクセス制御ポリシーを定義してください。 本機にアクセスするユーザーのアカウントに対してアクセス制御ポリシーに従った権限の付与を実施してください。
	3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	本要件は、システムを利用するユーザーに対して、職務別の最小特権を要求するものです。本機には、印刷・コピーなどの基本機能が利用可能なロールである一般ユーザーとは別に、設定変更などの特権を有する管理者ロールが用意されています。さらに独自ロールの設定と各種機能の利用制限をカスタマイズできる機能も持っています。	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。 **ACCESS MANAGEMENT SYSTEM** 権限レベル（ロール）ごとに使用できる機能を割り当てたり、新しいロールを作成したりすることができます。	＜ユーザー管理＞を設定する ＜ACCESS MANAGEMENT SYSTEMを使用＞を有効にする	ユーザーは最小特権の原則を適用し、必要な最小限のアクセス許可を割り当てるようアクセス制御ポリシーを定義してください。 本機にアクセスするユーザーのアカウントに対してアクセス制御ポリシーに従った権限の付与を実施してください。
	3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	本要件は、特権ユーザーが非セキュリティー機能を利用するときは、非特権アカウントを別途利用することを要求するものです。本要件の主な責務は、組織側であり、組織に属する個人(特権ユーザー)は、利用機能に応じてアカウントを使い分ける必要があります。本機においては、特権アカウントである管理者ロールと、非特権アカウントである一般ユーザーロールとがあるため、利用機能に応じて、ユーザー側でアカウントを切り替えることで、本要件を実現できます。	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。 **ACCESS MANAGEMENT SYSTEM** 権限レベル（ロール）ごとに使用できる機能を割り当てたり、新しいロールを作成したりすることができます。	＜ユーザー管理＞を設定する ＜ACCESS MANAGEMENT SYSTEMを使用＞を有効にする	ユーザーは特権アカウントの使用を制限し、非セキュリティー機能にアクセスするときは、非特権アカウントを利用するようアクセス制御ポリシーを定義してください。そのために、非セキュリティー機能にアクセスするときに使用する非特権アカウントを作成してください。 本機にアクセスするユーザーのアカウントに対してアクセス制御ポリシーに従った権限の付与を実施し、非セキュリティー機能利用時は非特権アカウントに切り替えてから本機を利用するように運用してください。
	3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	本要件は、非特権ユーザーが特権機能を実行してしまった際に、監査できるように例えばログなどを残すことを要求するものです。本機は、ロール別に特権・非特権ユーザーの機能実行を制御しているだけでなく、設定変更などの特権機能実行に関するログを監査ログとして残す機能を持っています。	**監査ログ機能** 本機がどのように使用されているかを確認／分析したいときは、ログを活用することができます。	監査ログ機能を有効にする	ユーザーは特権アカウントの使用を制限し、非セキュリティー機能にアクセスするときは、非特権アカウントを利用するようアクセス制御ポリシーを定義してください。 本機にアクセスするユーザーのアカウントに対してアクセス制御ポリシーに従った権限の付与を実施してください。 本機がアクセス制御ポリシーに従い適切に利用されているか利用状況を監査ログにより監査してください。

NIST SP 800-171 rev2 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンター側の対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.1 アクセス管理 Derived (派生セキュリティー要件)	3.1.8	Limit unsuccessful logon attempts.	本要件は、システム利用時のログイン試行の制限(e.g. ログイン試行が既定回数失敗した場合、ロックアウト)を要求するものです。本機は、ユーザー認証失敗時にアカウントロックする機能を持っています。別途、アカウントロックするまでの認証失敗回数や、ロックアウトしてから認証を再受付するまでのインターバル時間の設定も可能です。	**ロックアウト機能** 連続したログオン試行を制限するため、ロックアウト設定が可能です。 設定された回数のログオン失敗を検知すると、システムはアカウントを一時的にロックします。	＜ロックアウト設定＞を有効にする	アカウントロックするまでの認証失敗回数や、ロックアウトしてから認証を再受付するまでのインターバル時間などのログオン試行失敗を制限するポリシーを定義してください。 ユーザーはログオン試行を制限するため、本機のロックアウト設定を適切に設定してください。
	3.1.9	Provide privacy and security notices consistent with applicable CUI （Controlled Unclassified Information） rules.	本要件は、適用可能な CUI（Controlled Unclassified Information） 規則に応じ、システム利用者にプライバシーとセキュリティーに関する通知を提供することを要求するものです。本要件の主な責務は組織側であり、本機は対象外です。	N/A	-	ユーザーは情報システムにアクセスする際、適用可能なCUI （Controlled Unclassified Information）規則と整合性のあるプライバシーとセキュリティーに関する通知を実施してください。
	3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	本要件は、非アクティブな時間が所定時間過ぎた場合、セッションロックし、スクリーンセーバや固定画像などのパターン画像でシステム画面を不可視化することを要求するものです。本機は、オートクリア機能によりセッションロックするまでの非アクティブ時間の設定が可能です。オートクリアが実行されると固定画像が表示されます。	**オートクリア機能** 本機を一定時間タッチパネルディスプレーを操作しなかったとき、オートクリアが実行され自動的にログアウトします。ログアウト後、認証画面が表示されます。	＜オートクリア移行時間＞を設定する	スクリーンセーバなどによるセッションロックを使用してください。 ユーザーはポリシーに従いオートクリア移行時間を設定してください。
	3.1.11	Terminate (automatically) a user session after a defined condition.	本要件は、非アクティブな時間が所定時間過ぎた場合、自動的に利用者のセッションを終了することを要求するものです。本機は、ユーザーログイン後に非アクティブな時間が所定時間過ぎた場合、強制ログオフによりセッションを終了する機能を持っています。また本機は、セッション終了後に、新たにセッションを開始する際(本機の再利用をする際)は再度ログイン認証を要求するようになっています。	**オートクリア機能** 本機を一定時間タッチパネルディスプレーを操作しなかったとき、オートクリアが実行され自動的にログアウトします。 リモートUIを一定時間操作しない場合も、自動的にセッションを終了します。新しくセッションを開始する際は、再度ユーザー認証を要求します。	＜オートクリア移行時間＞を設定する	セッションロックする際の非アクティブな所定時間を決定してください。 ユーザーはポリシーに従いオートクリア移行時間を設定してください。
	3.1.12	Monitor and control remote access sessions.	本要件は、リモートアクセスの監視を要求するものです。本機は、リモートUIなどのリモートアクセス時にログを残す機能を持っています。	**監査ログ機能** 本機がどのように使用されているかを確認／分析したいときは、ログを活用することができます。	監査ログ機能を有効にする	本機がアクセス制御ポリシーに従い適切に利用されているか利用状況を監査ログにより監査してください。
	3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	本要件は、リモートアクセス時のセッション保護(機密性保護)を要求するものです。本機は、リモートUIなどの 本機へのリモートアクセス時に FIPS140認証を取得した暗号モジュールを用いて通信路のデータを暗号化する機能を持っています。	**TLS暗号化通信** パソコンなどの機器から本機にアクセスしてデータをやりとりする際に、盗聴、改ざん、なりすましなどを防ぐために、TLS暗号化通信を利用することができます。 また、設定によりFIPS140-2準拠のアルゴリズムの使用に限定することが可能です。 **IPSec通信** TLS暗号化通信はWebブラウザーや電子メールクライアントなど、特定のアプリケーションで暗号化する技術ですが、IPSec通信はIPプロトコルのレベルで暗号化を行います。そのため、さらに汎用性の高いセキュリティーを実現できます。	＜TLS設定＞を設定する各機能/アプリケーションの設定で＜TLSを使用＞を有効にする。また、環境に応じてサーバー証明書の検証を実施するよう設定する。 <IPSecを使用＞を有効にする ＜暗号方式をFIPS 140-2準拠にする＞を有効にする	システムにリモートアクセスする際は、TLSやIPSecといった暗号メカニズムに則ったセッション保護機能を利用してください。 ユーザーはネットワーク通信を保護するために本機に対して適切なネットワーク設定を実施してください。
	3.1.14	Route remote access via managed access control points.	本要件は、管理されたアクセスポイントを介したリモートアクセスのルーティングを要求するものです。本要件の主な責務は組織側です。組織側の対応をサポートする機能として、本機はファイアウォール機能を提供しており、本機にアクセスするネットワークを制限することが可能です。	**ファイアウォール** ファイアウォールとは、外部ネットワークからの不正アクセスを防止し、ローカルエリア内のネットワークへの攻撃や侵入を防ぐシステムです。お使いのネットワーク環境で、特定の外部IPアドレスからの通信を制限することで、危険と思われる外部からのアクセスをあらかじめ遮断できます。	＜ファイアウォール設定＞を設定する	ユーザーは管理されたアクセスポイントによるリモートアクセスのルーティングを実施してください。 本機に対して適切なネットワーク設定を実施してください。
	3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	本要件は、特権コマンドやセキュリティー関連情報(監査ログなど)へのリモートアクセスを認可することを要求するものです。組織が定めたアクセス制御ポリシーに従い、本機のロール別の機能制限及びユーザ認証機能を用いることで、リモートアクセスにより実行可能な特権機能やセキュリティー関連情報へのアクセスを特定のユーザーに制限することができます。例えば、特定のIT管理者のみにリモートUIを介した設定変更などの本機に影響を与える特権機能の利用を許可したり、監査ログの閲覧を許可するように制御できます。	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。 **ACCESS MANAGEMENT SYSTEM** 権限レベル（ロール）ごとに使用できる機能を割り当てたり、新しいロールを作成したりすることができます。	＜ユーザー管理＞を設定する ＜ACCESS MANAGEMENT SYSTEMを使用＞を有効にする	本機にアクセスするユーザーのアカウントに対してアクセス制御ポリシーに従った権限の付与を実施してください。 ユーザー管理やセキュリティー設定など、本機の重要な設定は管理者が統括して行ってください
	3.1.16	Authorize wireless access prior to allowing such connections.	本要件は、組織内で利用する無線アクセスを行うデバイス(e.g. スマートフォン、タブレット)の適切な管理を要求するものです。本要件の主な責務は組織側であり、組織はデバイス管理ガイドラインとして、例えば、BYOD（Bring Your Own Device)等の利用を許可するデバイスのタイプやデバイスの設定要件、接続時の認証要件などを定め、運用する必要があります。本機は組織側で定めた管理ガイドラインの運用をサポートする機能として、IEEE802.1X認証により本機に無線LAN接続をするデバイスを認証したり、無線ダイレクト機能そのものを有効・無効に設定できます。	**IEEE 802.1X対応** 本機はIEEE 802.1X認証を導入したネットワークにクライアントとして接続することができます。 **無線LAN** 無線LANルーター（アクセスポイント）を介して、本機とパソコンやモバイル本機を無線で接続することが可能です。利用には管理者による設定が必要です。 また、IEEE 802.1X認証が導入されたネットワーク環境への接続にも対応しています。	＜IEEE 802.1X設定＞を有効にする ＜無線LAN設定＞を設定する ＜ダイレクト接続設定＞を無効にする	ユーザーはアクセス制御ポリシーに従って、無線接続を許可する前に無線アクセスを許可してください。IEEE 802.1X認証を導入することで認証サーバーに認証されたクライアント機器にのみネットワーク接続を許可することも可能です。 本機に対して適切なネットワーク設定を実施してください。無線LANのダイレクト接続設定は無効に設定してください。

NIST SP 800-171 rev2 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンター側の対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.1 アクセス管理 Derived (派生セキュリティー要件)	3.1.17	Protect wireless access using authentication and encryption.	本要件は、認証と暗号化機能を用い、システムへの無線アクセスを保護することを要求するものです。本機は、無線アクセス時に PSK(pre-shared key)やIEEE802.1X によるデバイス認証を行う機能やデータ暗号化を行う機能を具備します。IEEE802.1X 認証を用いることで、安全な無線接続が可能です。	**IEEE 802.1X対応** 本機はIEEE 802.1X認証を導入したネットワークにクライアントとして接続することができます。 **無線LAN** 無線LANルーター（アクセスポイント）を介して、本機とパソコンやモバイル本機を無線で接続することが可能です。利用には管理者による設定が必要です。また、IEEE 802.1X認証が導入されたネットワーク環境への接続にも対応しています。	＜IEEE 802.1X設定＞を有効にする ＜無線LAN設定＞を設定する ＜ダイレクト接続設定＞を無効にする	ユーザーはアクセス制御ポリシーに従って、認証と暗号化を用いて無線アクセスの保護を実施してください。IEEE 802.1X認証を導入することで認証サーバーに認証されたクライアント機器にのみネットワーク接続を許可することも可能です。 本機に対して適切なネットワーク設定を実施してください。データ暗号方式には安全なアルゴリズムを選択してください。
	3.1.18	Control connection of mobile devices.	本要件は、組織内で利用する(組織内のシステムに接続する)モバイル機器の適切な管理を要求するものです。組織側の対応が必要な要件であり、本機は対象外です。例えば組織はモバイル機器利用ガイドラインを策定し、以下のような方法でモバイル機器を管理する必要があります。 ・EMM（Enterprise Mobility Management）/MDM で管理 ・モバイル機器の識別 ・モバイル機器内ソフトの構成管理 ・モバイル機器へのウイルスチェック ・モバイル機器の設定管理	N/A	-	ユーザーはアクセス制御ポリシーに従って組織で利用するモバイル機器の管理、接続の制御を実施してください。
	3.1.19	Encrypt CUI（Controlled Unclassified Information）on mobile devices and mobile computing platforms.	本要件は、モバイル機器内に保存される CUI（Controlled Unclassified Information） の暗号化による保護を要求するものです。モバイル機器に関する要件であり、非モバイル機器である本機は対象外です。	N/A	-	ユーザーはアクセス制御ポリシーに従って組織で利用するモバイル機器の管理、接続の制御を実施してください。なお、CUI（Controlled Unclassified Information）の機密性および完全性の保護のため、モバイル機器全体の暗号化もしくはコンテナレベルの暗号化を推奨します。
	3.1.20	Verify and control/limit connections to and use of external systems.	本要件は、組織外の外部システム(外部のクラウドサービスなど)への接続の検証・制御・制限を要求するものです。本要件の主な責務は組織側であり、組織は外部システム利用に関するポリシーを策定し、運用する必要があります。本機は組織側の対応をサポートする機能として、外部システムから本機へのアクセスを制御可能な IP フィルタ機能を持っています。	**ファイアウォール** ファイアウォールとは、外部ネットワークからの不正アクセスを防止し、ローカルエリア内のネットワークへの攻撃や侵入を防ぐシステムです。お使いのネットワーク環境で、特定の外部IPアドレスからの通信を制限することで、危険と思われる外部からのアクセスをあらかじめ遮断できます。 **プロキシー設定** ウェブサイトの閲覧時にプロキシーサーバーを経由して外部に接続します。プロキシーサーバーを使うとより安全にウェブサイトを閲覧することができるため、セキュリティーの向上が期待できます。	＜ファイアウォール設定＞を設定する ＜プロキシー設定＞を有効にする	ユーザーは組織のセキュリティーポリシーおよび手順に従って、外部情報システムの使用に関する条件を設定し、外部情報システムへの接続を制御及び制限してください。 本機に対して適切なファイアウォール設定およびプロキシー設定を行ってください。
	3.1.21	Limit use of portable storage devices on external systems.	本要件は、外部システム上で組織が管理する可搬ストレージ(e.g. 外付けHDD, USBメモリー)の使用制御を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。例えば組織は、管理者の承認が得られた場合に限り外部システムで可搬ストレージを許可するように外部システム利用に関するポリシーを策定、運用する必要があります。	N/A	-	ユーザーは組織のセキュリティーポリシーおよび手順に従って、外部情報システムの使用に関する条件を設定し、外部情報システムへの接続を制御及び制限してください。 外部システム上でのポータブルストレージデバイスの使用を制限してください。
	3.1.22	Control CUI（Controlled Unclassified Information）posted or processed on publicly accessible systems.	本要件は、外部公開するシステム上に掲載または、システム上で処理する CUI（Controlled Unclassified Information） に関する制御を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。例えば、組織は Web サイトなどの公開システム上に CUI（Controlled Unclassified Information） を掲載可能な従業員の管理や、掲載前レビューを実施することで、公開システム上に掲載・処理される CUI を制御する必要があります。	N/A	-	ユーザーは一般にアクセス可能なシステムにおいて掲載または処理される情報を管理、制御してください。
3.2 意識向上と訓練 Basic (基本セキュリティー要件)	3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	本要件は、組織の従業員のセキュリティー意識に関するトレーニングを要求するものです。本要件の主な責務は組織側であり、本機は対象外です。例えば、組織は社内へのポスター掲示や研修などで、セキュリティーに関する注意事項(e.g. 不審なメールの添付ファイルやリンクは開かない)を周知徹底する必要があります。	N/A	-	セキュリティーに関する注意事項(e.g. 不審なメールの添付ファイルやリンクは開かない)を周知徹底するためのセキュリティートレーニングを実施してください。セキュリティートレーニングを実施する頻度を定めてください。
	3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	本要件は、組織の従業員に対し、役割別(e.g. ソフトウェア開発者、システム開発者、ネットワーク管理者など)に適切なセキュリティートレーニングを要求するものです。本要件の主な責務は組織側であり、本機は対象外です。	N/A	-	従業員に対し、役割別(e.g. ソフトウェア開発者、システム開発者、ネットワーク管理者など)に適切なセキュリティートレーニングを実施してください。セキュリティートレーニングを実施する頻度を定めてください。

NIST SP 800-171 rev2 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンター側の対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.2 意識向上と訓練 Derived (派生セキュリティー要件)	3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	本要件は、組織内部で生じる脅威とその報告に関するセキュリティートレーニングを要求するものです。本要件の主な責務は組織側であり、本機は対象外です。	N/A	-	組織内部で生じる脅威とその報告に関するセキュリティートレーニングを実施してください。具体的には、内部者の潜在的な脅威を示す可能性のある高リスク行動について周知し、報告する方法を定めたうえで周知してください。高リスク行動の例は、過度で長期的な仕事への不満、業務遂行に必要でない情報へのアクセスの試行、説明のつかない財源へのアクセス、同僚からのいじめやセクハラ、職場での暴力、その他の組織の方針、手続、指示、規則又は慣行に対する重大な違反です。
3.3 監査と説明責任 Basic (基本セキュリティー要件)	3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	本要件は、不適切なシステムアクティビティー監視のために、監査ログの記録を要求するものです。本機は、自身に対する種々の操作を記録する監査ログ機能を具備します。	**監査ログ機能** 本機がどのように使用されているかを確認／分析したいときは、ログを活用することができます。ログには操作日時、ユーザー名、操作の種類、機能の種類、操作結果などの情報が記録されます。	監査ログ機能を有効にする	ユーザーは監査すべき事象を決定してください。また、監査対象の事象について、監査の頻度を定めてください。必要に応じて監査に必要な追加情報を識別してください。監査対象の事象に対し、何を不適切な状態とするか、閾値等を定めてください。監査体制を構築してください。 本機に対して監査ログ機能の設定を行い、適切に監査を実施してください。
	3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	本要件は、特定のユーザーが引き起こしたアクション・イベントを一意にトレース可能であることを要求するものです。本機は、自身に対する種々の操作を記録する監査ログ機能を持っています。監査ログには監査イベントごとにユーザーIDやタイムスタンプを記録できるため、ユーザーレベルでイベントをトレース可能です。	**監査ログ機能** 本機がどのように使用されているかを確認／分析したいときは、ログを活用することができます。ログには操作日時、ユーザー名、操作の種類、機能の種類、操作結果などの情報が記録されます。	監査ログ機能を有効にする	ユーザーは監査すべき事象を決定してください。また、監査対象の事象について、監査の頻度を定めてください。必要に応じて監査に必要な追加情報を識別してください。監査対象の事象に対し、何を不適切な状態とするか、閾値等を定めてください。監査体制を構築してください。 本機に対して監査ログ機能の設定を行い、適切に監査を実施してください。
3.3 監査と説明責任 Derived (派生セキュリティー要件)	3.3.3	Review and update logged events.	本要件は、監査対象となる事象のレビューと、状況に応じた監査対象の変更を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。例えば、組織はインシデント発生時に監査ログをレビューし、現状の監査ログの記録項目だけでは追跡困難と判断した場合、次回以降はインシデントの追跡ができるように監査ログへの記録対象を追加する必要があります。 本機は組織側の対応をサポートする機能として、監査ログに記録する項目を変更する機能を利用できます。	**監査ログ機能** 本機がどのように使用されているかを確認／分析したいときは、ログを活用することができます。ログには操作日時、ユーザー名、操作の種類、機能の種類、操作結果などの情報が記録されます。	監査ログ機能を有効にする	ユーザーは監査対象の事象を定期的にレビューし、適切な事象が監査対象となるように監査対象を必要に応じて見直してください。 本機に対して監査ログ機能の設定を行い、適切に監査を実施してください。
	3.3.4	Alert in the event of an audit logging process failure.	本要件は、監査ログ記録に失敗した際にアラートを発することを要求するものです。本機は、監査ログ機能に何らかのエラーが生じた場合、操作パネル上にアラートを出す機能を持っています。	**監査ログ機能** 本機がどのように使用されているかを確認／分析したいときは、ログを活用することができます。ログには操作日時、ユーザー名、操作の種類、機能の種類、操作結果などの情報が記録されます。	監査ログ機能を有効にする	ユーザーは監査プロセス失敗時に組織のシステムがアラートを発出するように設定し、アラート発出時の対応を定め運用してください。例えば、組織のシステムの監査プロセス失敗時に、組織が定めた担当者にアラートを通知するように設定し、当該担当者はアラートの解消(監査プロセスの復旧)を行う必要があります。 本機に対して監査ログ機能の設定を行い、適切に監査を実施してください。本機の操作パネルもしくはリモートUI上に監査ログ機能に関するエラーが表示された場合は、リモートUIのログ管理画面を表示し、エラーを確認し対処してください。対処方法の詳細は、本機のオンラインマニュアルを参照してください。
	3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	本要件は、監査ログのレビュー、分析、報告を介した疑わしいアクティビティーへの対応を要求するものです。本要件の主な責務は組織側であり、組織はシステムに対する監査ログをレビュー、分析し、適宜インシデントレスポンスを実施する必要があります。本機は組織側の対応をサポートする機能として、本機に対する種々の操作を記録する監査ログ機能を持っています。	**監査ログ機能** 本機がどのように使用されているかを確認／分析したいときは、ログを活用することができます。ログには操作日時、ユーザー名、操作の種類、機能の種類、操作結果などの情報が記録されます。	監査ログ機能を有効にする	ユーザーは監査ログのレビュー、分析、調査等を通じ、組織のシステムの異常の兆候を発見し、疑わしいアクティビティーに対処する監査体制を構築してください。 本機に対して監査ログ機能の設定を行い、適切に監査を実施してください。
	3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.	本要件は、監査ログ分析と報告をスムーズにするために、監査ログのシュリンク(インシデント追跡に繋がる記載以外のノイズを削除)、報告書作成を要求するものです。本要件の主な責務は組織側であり、組織は監査ログから必要な情報を抽出し、報告書を作成する必要があります。本機は組織側の対応をサポートする機能として、本機に対する種々の操作を記録する監査ログ機能を持っており、組織で簡素化する際にベースとなる監査ログを取得できます。	**監査ログ機能** 本機がどのように使用されているかを確認／分析したいときは、ログを活用することができます。ログには操作日時、ユーザー名、操作の種類、機能の種類、操作結果などの情報が記録されます。	監査ログ機能を有効にする	ユーザーは監査ログから情報を取得し、簡素化し、報告書を作成する監査体制を構築してください。 本機に対して監査ログ機能の設定を行い、適切に監査を実施してください。

NIST SP 800-171 rev2 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンター側の対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.3 監査と説明責任 Derived (派生セキュリティー要件)	3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	本要件は、監査ログに記録されるタイムスタンプのソースとして信頼できる情報源(NTPサーバー)を用い、システムの時刻を同期させることを要求するものです。本機は、時刻同期用に NTP サーバーを設定可能であり、同期した時刻は監査ログのタイムスタンプとしても用いられます。	**SNTP設定** SNTPはネットワーク上のタイムサーバーを基準にして時刻を調整するためのプロトコルです。参照先に信頼できるNTPサーバーを指定することにより、タイムスタンプの精度を担保することができます。	<SNTP設定>を設定する	ユーザーは組織のシステムが参照するタイムサーバやポーリング間隔等を定め、システムが正しく時刻同期及びタイムスタンプ生成できるようにしてください。 本機のNTPサーバーアドレスおよびポーリング間隔を設定してください。
	3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	本要件は、監査ログに対する不正アクセス、改ざん、削除への保護を要求するものです。本機は、ユーザー認証機能によるアクセス制御で、監査ログに対する操作を適切なユーザーのみに制限することが可能です。また、監査ログはストレージデータの暗号化機能により暗号化されて本機内に保存されます。ストレージに直接アクセスしての監査ログ改変・削除は困難です。また、監査ログをファイルとして外部出力することでバックアップを取ることも可能であり、ログを削除されても復元できます。	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。 **監査ログ機能** 本機がどのように使用されているかを確認／分析したいときは、ログを活用することができます。ログには操作日時、ユーザー名、操作の種類、機能の種類、操作結果などの情報が記録されます。 **ストレージデータの暗号化** 本機のストレージには、アドバンスドボックスやユーザーボックス内のファイル、アドレス帳の登録情報、残存するジョブデータ、パスワード情報などが保存されています。これらのデータを暗号化することにより、情報を不正に読み取られることを防いでいます。	<ユーザー管理>を設定する 監査ログ機能を有効にする	ユーザーは監査機能の管理者を定めてください。 監査機能の管理者のみが本機の監査ログ機能にアクセス可能になるように本機のユーザ管理機能で設定してください。本機のストレージデータの暗号化機能に対する設定は不要です。
	3.3.9	Limit management of audit logging functionality to a subset of privileged users.	本要件は、監査ログ機能の管理を一部の特権ユーザーのみに制限することを要求するものです。本機は、監査ログ機能にアクセス可能なユーザーをユーザー認証により制限することが可能です。例えば、管理者のみが監査ログ機能にアクセス可能となるように設定することが可能です。	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。 **監査ログ機能** 本機がどのように使用されているかを確認／分析したいときは、ログを活用することができます。ログには操作日時、ユーザー名、操作の種類、機能の種類、操作結果などの情報が記録されます。	<ユーザー管理>を設定する 監査ログ機能を有効にする	ユーザーは監査機能の管理者を定め、その管理者のみに特権を与えてください。 監査機能の管理者のみが本機の監査ログ機能にアクセス可能になるように本機のユーザ管理機能で設定してください。
3.4 構成管理 Basic (基本セキュリティー要件)	3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	本要件は、組織のシステムの構成管理（(e.g. OSバージョン、インストールアプリ等の統制）を要求するものです。本要件の主な責務は組織側であり、組織は自社内のシステムの構成ベースラインを定めた上で、システム構成の管理・統制を行う必要があります。本機は組織側の対応をサポートする機能として、本機のカウンター/機器情報にて、本機のバージョンやオプションなどのデバイス構成を表示する機能を具備しています。	**カウンター/機器情報** 本体のシリアルNo.やIPアドレス、バージョン、オプションなどのデバイス構成を確認することができます。ストレージ内のデータの暗号化に関わるセキュリティーチップのバージョン情報も、ここから確認することができます。	<デバイス構成確認>を表示する	ユーザーは本機のシステムコンポーネントの情報をもとに構成ベースラインを構築し、文書化したうえで管理してください。 構成ベースラインは定期的にレビューする必要があり、システムに変更が加えられる場合は、構成ベースラインの確認と変更が必要となります。 構成ベースラインの構築時には本機のデバイス情報表示機能を用いることによりシステムコンポーネントの情報を得ることができます。
	3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	本要件は、組織のシステムのセキュリティー設定管理を要求するものです。本要件の主な責務は組織側であり、組織は自社内のシステムのセキュリティー設定ベースライン(セキュリティーポリシー)を定めた上で、自社内のシステムに対しセキュリティー設定の適用・統制を行う必要があります。本機は組織側の対応をサポートする機能として、セキュリティーポリシー設定による簡易なセキュリティー設定機能や、インポート／エクスポート機能による設定ファイルを用いた一括設定機能を具備しています。	**セキュリティーポリシー** 本機のセキュリティーポリシーを設定することで、情報セキュリティーに関わる本機の設定を一括して適用／管理することができます。 本機のセキュリティーポリシー設定は、インポート／エクスポートすることができます。複数の機器に同じポリシーを適用することで、組織全体の機器を同一の設定状態で管理することができます。	<セキュリティーポリシー設定>を設定する	ユーザーは組織のセキュリティー方針に従って機器のセキュリティー設定を規定してください。 規定したセキュリティー設定は組織内で運用されているすべての機器に適用してください。 セキュリティーポリシーの設定には、本機のセキュリティーポリシー設定機能を利用することができます。 セキュリティーポリシーの設定項目として、無線ポリシー・通信の運用ポリシー・認証の運用ポリシーなどがあげられます。 設定したセキュリティーポリシーは、インポート／エクスポートすることが可能であり、複数の機器に対して同一のセキュリティーポリシーを設定することができます。
3.4 構成管理 Derived (派生セキュリティー要件)	3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.	本要件は、組織のシステム変更に関して、変更内容の追跡、レビュー、変更実施の承認/非承認、監査を要求するものです。本要件の主な責務は組織側であり、組織はシステム変更(e.g. OS バージョン変更)する際に変更内容をレビューし、承認フローを経たうえで、変更を実施する必要があります。組織側の対応をサポートする機能として、本機のファームウェアのアップデートにより追加された機能や変更内容の情報を公開しています。(ユーザーズガイド (機能追加のお知らせ))	N/A	-	ユーザーは本機のシステムの変更に際して、変更内容をレビューし、承認フローを経たうえで、変更を実施してください。 システムの変更には構成ベースラインの変更、構成設定の変更、スケジュールされていない未承認の変更、および脆弱性を修正するための変更が含まれます。 例えば、ファームウェア更新についてのレビューを行う場合、ユーザーズガイド (機能追加のお知らせ)からファームウェアに関する変更内容を確認できます。 ユーザーは変更内容を確認し、承認後にファームウェアの更新を行い、構成ベースラインに変更内容を反映させます。 更新には承認された自動ファームウェア更新機能を利用することができますが、更新時の変更内容は追跡し、構成ベースラインに反映する必要があります。

NIST SP 800-171 rev2 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンター側の対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.4 構成管理 Derived (派生セキュリティー要件)	3.4.4	Analyze the security impact of changes prior to implementation.	本要件は、組織のシステム変更前に、セキュリティーに関する影響分析を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。	N/A	-	ユーザーは機器のシステムの変更に際して、変更内容をレビューし、承認フローを経たうえで、変更を実施してください。 システムの変更には構成ベースラインの変更、構成設定の変更、スケジュールされていない未承認の変更、および脆弱性を修正するための変更が含まれます。
	3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	本要件は、組織のシステム変更(e.g. ハードウェア構成変更、アップデート)を行う人物の定義及びアクセス制限の文書化、実施を要求するものです。本要件の主な責務は組織側であり、組織はハードウェア、ソフトウェアにアクセスし、物理的および論理的な構成変更を行う権限を与えられた担当者を定義、特定、およびアクセス制限に関する制約事項を文書化する必要があります。アクセス制限方法としては、入室管理、パスワードによるユーザー認証、更新自動化などが適用可能です。本機は組織側の対応をサポートする機能としてユーザーのロールごとにアクセス制限を課す機能を具備しています。	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。 **ACCESS MANAGEMENT SYSTEM** 権限レベル（ロール）ごとに使用できる機能を割り当てたり、新しいロールを作成したりすることができます。	＜ユーザー管理＞を設定する ＜ACCESS MANAGEMENT SYSTEMを使用＞を有効にする	ユーザーはハードウェア、ソフトウェアにアクセスし、物理的および論理的な構成変更を行う権限を与えられた担当者を定義、特定、およびアクセス制限に関する制約事項を文書化してください。 アクセス制限の例としては、入室管理やパスワードによるユーザー認証があります。あるいはシステム更新を自動化することによりユーザーが更新機能にアクセスすることを制限することができます。 例えば、組織は機器の管理者を決め、機器の管理者アカウント発行します。機器の設定に対して、管理者以外のユーザーによる変更を制限することで、組織が規定した管理者のみが機器の構成を変更することができるようにします。
	3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	本要件は、組織のシステムが基本機能のみを具備すること(最小機能の原則)を要求しています。本要件の主な責務は組織側であり、組織は検討・定義した構成ベースライン及びセキュリティーポリシーにのっとり、組織内のシステムの構成及び機能を統制する必要があります。ここで定義する構成ベースラインおよびセキュリティーポリシーでは、不要なハードウェア、ソフトウェアの搭載や、不要な機能を有効化しないよう、最小機能の原則に基づき定義する必要があります。本機は組織側の対応をサポートする機能として、組織が定義したセキュリティーポリシーを簡便に本機に反映させるためのインポート／エクスポートによる一括設定機能を具備しています。	**セキュリティーポリシー** 本機のセキュリティーポリシーを設定することで、情報セキュリティーに関わる本機の設定を一括して適用／管理することができます。 セキュリティポリシー設定により、[USBポリシー]や[ポートの利用ポリシー]、[印刷のポリシー]などを設定することで、不要な機能は有効化しないよう設定することができます。 本機のセキュリティーポリシー設定は、インポート／エクスポートすることができます。複数の機器に同じポリシーを適用することで、組織全体の機器を同一の設定状態で管理することができます。	＜セキュリティーポリシー設定＞を設定する	ユーザーは構成ベースラインやセキュリティーポリシーに従い、機器の運用に不要な機能を特定し、それら機能を制限・無効化してください。 制限・無効化する対象の機能としてはデフォルトで有効となっているアプリケーションやプロトコル、ポートが含まれます。 本機ではセキュリティーポリシー設定機能を利用することにより情報セキュリティーに関わる本機の機能を一括して制限することができます。例えば、使用しない印刷プロトコル用ポート（e.g. LPD：ポート番号515、FTP：ポート番号21）を本機能により制限することができます。
	3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	本要件は、組織のシステムで用いられる非基本プログラム、機能、ポート、プロトコル、及びサービスの使用を制限、無効化、及び防止することを要求しています。本要件の主な責務は組織側であり、組織は検討・定義したセキュリティーポリシー(利用が許可されるポート、プロトコル、サービス等の定義)にのっとり、組織内のシステムを統制する必要があります。本機は組織側の対応をサポートする機能として、組織が定義したセキュリティーポリシーにのっとり、本機の機能を制限する機能としてセキュリティーポリシー機能が利用可能です。	**セキュリティーポリシー** 本機のセキュリティーポリシーを設定することで、情報セキュリティーに関わる本機の設定を一括して適用／管理することができます。 セキュリティポリシー設定により、[USBポリシー]や[ポートの利用ポリシー]、[印刷のポリシー]などを設定することで、不要な機能は有効化しないよう設定することができます。 本機のセキュリティーポリシー設定は、インポート／エクスポートすることができます。複数の機器に同じポリシーを適用することで、組織全体の機器を同一の設定状態で管理することができます。	＜セキュリティーポリシー設定＞を設定する	ユーザーは構成ベースラインやセキュリティーポリシーに従い、機器の運用に不要あるいはセキュアでない機能を特定し、それら機能を制限・無効化してください。 本機ではセキュリティーポリシー設定機能を利用することにより情報セキュリティーに関わる本機の機能を一括して制限することができます。例えば、使用しない印刷プロトコル用ポート（e.g. LPD：ポート番号515、FTP：ポート番号21）を本機能により制限することができます。
	3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	本要件は、組織のシステム内で使用されるソフトウェアを、ブラックリストもしくはホワイトリスト方式で制限することを要求しています。本機はホワイトリスト方式のソフトウェア実行制限機能として、起動時・稼働時のシステム検証機能、ファームウェアやアプリケーションインストール時の署名検証機能を具備しています。	**起動時のシステム検証** 本機に組み込んであるファームウェア、システムやMEAPアプリケーションの完全性を、起動時に検証します。 **ランタイムシステム保護** 本機の稼働中に、ランタイムシステム保護機能を使ってプログラムの不正な改変と不正なプログラムの実行を防止し、システムの信頼性を向上できます。	＜起動時のシステム検証＞を有効にする ＜ランタイムシステム保護＞を有効にする	ユーザーは組織のシステム内で使用されるソフトウェアを、ブラックリストもしくはホワイトリスト方式で制限してください。 本機は起動時のシステム検証機能およびランタイムシステム保護機能を設定することで本機で使用されるシステムを制限することができます。
	3.4.9	Control and monitor user-installed software.	本要件は、組織のシステム内に新たにインストールされるソフトウェアの管理・監視を要求しています。本機は「通信」、「認証」、「出力」といったさまざまな機能を、拡張／最適化するための仕組みとして、MEAP（Multifunctional Embedded Application Platform）を提供しています。リモートUIからSMS（Service Management Service）によりMEAPアプリケーションのインストールや使用状況の確認が可能です。また、ユーザー認証機能によりアプリケーションを管理できるユーザーを制限したり、監査ログ機能によりインストールイベントを記録・監視することができます。	**MEAPアプリケーションの管理** リモートUIのSMSを表示してアプリケーションを管理することができます。 **監査ログ機能** 本機がどのように使用されているかを確認／分析したいときは、ログを活用することができます。ログには操作日時、ユーザー名、操作の種類、機能の種類、操作結果などの情報が記録されます。	リモートUIの［Service Management Service］によりアプリケーションを管理する 監査ログ機能を有効にする	ユーザーは構成ベースラインに定められたソフトウェアコンポーネント以外にインストールされるアプリに関するポリシーを規定し、ポリシーが順守されていることを確認してください。 ポリシーには、アプリの配布元の限定やインストールに際する承認などが含まれます。 リモートUIのSMSを表示してアプリケーションを管理することができます。 インストールイベントは監査ログに記録され、ユーザーは監査ログをモニタリングすることでインストールアプリに関するポリシーの遵守を確認することができます。

NIST SP 800-171 rev2 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンター側の対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.5 識別と認証 Basic (基本セキュリティー要件)	3.5.1	Identify system users, processes acting on behalf of users, and devices.	本要件は、組織のシステムへのアクセス時のユーザーやデバイスの識別を要求しています。組織はユーザー・デバイスを一意に識別できるような識別子を割り当てる必要があります。本機は操作パネルやリモートUIへのアクセス時のユーザー認証や、通信プロトコルレベルのアクセス制御、アドバンスドボックス利用時のアクセス制御など種々の認証機能を具備しています。また、IEEE802.1X認証により本機にネットワーク経由でアクセスするデバイスを認証サーバーで識別・認証することも可能です。	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。 **ネットワークの認証管理** 本機は通信プロトコル(e.g. IPP, SNMP)について認証機能を設定することができます。 **アドバンスドボックスの認証管理** アドバンスドボックスを公開する際に認証設定を行うことで不正アクセスを防止できます。 **IEEE 802.1X対応** 本機はIEEE 802.1X認証を導入したネットワークにクライアントとして接続することができます。	＜ユーザー管理＞を設定する ＜IPP印刷の設定＞の＜認証を使用＞を有効にする ＜SNMP設定＞の＜SNMPv1を使用＞を無効にする ＜SNMPv3を使用＞を設定する ＜アドバンスドボックス設定＞の＜認証管理＞を設定	ユーザーはシステムにアクセスするユーザーやデバイスを一意に識別できるようにしてください。例えば、ユーザーの識別方法としてはユーザーIDの割り当て、デバイスの識別方法としてはMACアドレスやIPアドレスなどを利用することができます。 本機では、本機にアクセスする際の認証時に要求されるユーザアカウントやICカードを利用することでユーザーを識別することができます。 デバイスの識別については、IEEE802.1X認証を導入することで認証サーバーに識別・認証されたクライアント機器にのみネットワーク接続を許可することが可能です。また、監査ログに記録されている本機にアクセスしたデバイスのIPアドレスなどを確認することでもデバイスを識別することができます。
	3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	本要件は、組織のシステムへのアクセス時の認証を要求しています。本機は操作パネル、リモートUIへのアクセス時のユーザー認証や、通信プロトコルレベルのアクセス制御、アドバンスドボックス利用時のアクセス制御など種々のユーザー認証機能を具備しています。本機のユーザー認証では、ユーザーを識別するためのパスワード認証が利用可能であり、デフォルトパスワードの変更を要求するように設定することもできます。また、IEEE802.1X認証により本機にネットワーク経由でアクセスするデバイスを認証サーバーで識別・認証することも可能です。	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。 お買い上げ時の管理者パスワードを変更していない場合は、新しいパスワードに変更するようメッセージが表示されます。 **ネットワークの認証管理** 本機は通信プロトコル(e.g. IPP, SNMP)について認証機能を設定することができます。 **アドバンスドボックスの認証管理** アドバンスドボックスを公開する際に認証設定を行うことで不正アクセスを防止できます。 **IEEE 802.1X対応** 本機はIEEE 802.1X認証を導入したネットワークにクライアントとして接続することができます。	＜ユーザー管理＞を設定する ＜IPP印刷の設定＞の＜認証を使用＞を有効にする ＜SNMP設定＞の＜SNMPv1を使用＞を無効にする ＜SNMPv3を使用＞を設定する ＜アドバンスドボックス設定＞の＜認証管理＞を設定する ＜IEEE 802.1X設定＞	ユーザーは組織のシステムにアクセスするユーザーやデバイスに対する認証を行ってください。 本機はユーザーが操作パネルやリモートUIを介して本機にアクセスする際の認証に加えて、認証機能を有するプロトコル（e.g. IPP、SNMP）については認証機能を設定することができます。 また、IEEE802.1X認証を導入することで認証サーバーに識別・認証されたクライアント機器にのみネットワーク接続を許可することが可能です。
3.5 識別と認証 Derived (派生セキュリティー要件)	3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	本要件は、組織のシステムへのネットワークアクセス時、もしくは特権アカウントへのローカルアクセス時に多要素認証を要求しています。本機は、操作パネルへのアクセス時にICカード認証と暗証番号を併用することで多要素認証を要求するように設定できます。	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。 ICカード認証により多要素認証を設定することができます。	＜ユーザー管理＞を設定する	ユーザーは組織システムへのアクセスに多要素認証を設定してください。 本機のユーザー管理設定で管理者に対してICカード認証及び暗証番号を利用するよう設定してください。 また、組織システムで情報端末に対する多要素認証を実施し、その構成に合わせて本機の認証先のドメインを設定してください。本機は認証サーバーとしてActive DirectoryまたはLDAPサーバーを設定可能です。
	3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	本要件は、組織のシステムへのネットワークアクセス時にリプレイ攻撃耐性のある認証メカニズムの導入を要求しています。本機は、リモートUIへのアクセス時の通信路保護機能として、TLS通信が利用可能であり、これにより認証時にリプレイ攻撃耐性を持たせることができます。	**TLS暗号化通信** TLS暗号通信はリプレイ攻撃に耐性がある認証方式を採用しています。したがって、パソコンなどの機器から本機にアクセスしてデータをやりとりする際に、TLS暗号化通信を利用してリプレイ攻撃への耐性を持たせることができます。	＜TLS設定＞を設定する各機能/アプリケーションの設定で＜TLSを使用＞を有効にする。また、環境に応じてサーバー証明書の検証を実施するよう設定する。	ユーザーはネットワークアクセス時にはリプレイ攻撃に耐性のあるメカニズムを採用してください. リモートUIから本機にアクセスする際には、本機のTLS機能を有効にすることでリプレイ攻撃に対する耐性を持たせることができます。 TLSを利用するために、暗号化に必要な「鍵と証明書」（サーバー証明書）を指定する必要があります。
	3.5.5	Prevent reuse of identifiers for a defined period.	本要件は、組織のシステムへのログインアカウントに関して、特定期間の再利用禁止を要求するものです。組織は、アカウント管理ガイドラインを策定・運用することで、ガイドラインで規定した期間中に識別子が再利用されないよう、従業員に周知徹底する必要があります。	N/A	-	ユーザーはアカウント管理ガイドラインを策定・管理し、アカウントの再利用を禁止する期間を規定してください。 アカウント管理ガイドラインに従い、指定した期間アカウントの再利用を禁止してください。 例えば、アカウントにユーザーの名前を使用している場合などに、離職などにより無効になったユーザーのアカウント名と新規ユーザーのアカウント名が同一になることがありますが、このケースはアカウントの再利用にあたるため、ポリシーに定められた期間内の場合、再利用を禁止してください。
	3.5.6	Disable identifiers after a defined period of inactivity.	本要件は、組織のシステムへのログインアカウントに関して、特定期間非アクティブなアカウントが存在する場合、当該アカウントの無効化を要求するものです。本機は、一定期間ログインしていないユーザーのアカウントを自動で削除する機能を具備しています。	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。 本機は一定期間ログインしていないユーザーのアカウントを自動で削除することができます。	リモートUIで［認証管理］の［一定期間ログインしていないユーザーを削除する］を設定する	ユーザーはアカウント管理ガイドラインを策定・管理し、アカウントが自動削除されるまでの非アクティブな期間について規定してください。 規定した期間が経過したアカウントについては、当該アカウントを削除してください。 本機は一定期間ログインしていないユーザーのアカウントを自動で削除する機能を有しており、当該機能を有効にすることでアカウントの自動削除を実施することができます。

NIST SP 800-171 rev2 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンター側の対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.5 識別と認証 Derived (派生セキュリティー要件)	3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	本要件は、組織のシステムへのログインアカウントに関して、新たにパスワードを設定・変更する際に、組織が定めたポリシーに従い最小パスワード文字数、複雑性の強制を要求するものです。本機は、パスワードの信頼性向上機能として、パスワード最小文字数の設定、パスワード複雑さ(※1)の設定が可能です。 ※1 パスワードに、数字、英小文字・大文字、記号を必ず使用するように設定可能	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。 本機はパスワードの登録に必要な最小文字数、パスワードに含める文字・数字・記号について設定することができます。	<パスワード設定> <最小文字数の設定> <英大文字を1字以上必ず使用> <英小文字を1字以上必ず使用> <数字を1字以上必ず使用> <記号を1字以上必ず使用> を設定する	ユーザーはパスワード設定時のポリシーを規定してください。 ポリシーにはパスワードの最小文字数、パスワードの複雑性(数字・文字・記号の組み合わせ）についての指定が含まれます。 ユーザーは、システムの利用者がポリシーに従ったパスワードを設定するように管理してください。 本機はパスワードのポリシーを設定する機能を有しており、当該機能を有効にすることでシステムの利用者にパスワードポリシーを強制できます。
	3.5.8	Prohibit password reuse for a specified number of generations.	本要件は、組織のシステムへのログインアカウントに関して、既定されたパスワード生成回数の間、パスワードの再利用禁止を要求するものです。組織側のパスワード管理ガイドラインに「既定の生成回数の間、パスワード再利用を禁止する」ように記載し、組織側の運用として、従業員にパスワードの再利用禁止を周知徹底してください。	N/A	-	ユーザーはパスワード管理ガイドラインを策定・管理し、パスワードの再利用頻度とパスワード生成の最小回数を規定してください。 規定した回数に満たない時点でのパスワードの再利用を禁止してください。 例えば、パスワード生成の最小回数を３回とした場合、パスワードの再設定をするときに3個前までのパスワードと同じパスワードの利用を禁止します。5回目の変更時は1回目のパスワードであれば再利用可能です。
	3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	本要件は、組織のシステムへのログインアカウントに関して、デフォルトパスワードからの変更を要求するものです。本機は、管理者の初回ログイン時にパスワードを変更させる機能を具備しています。	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。 お買い上げ時の管理者パスワードを変更していない場合は、新しいパスワードに変更するようメッセージが表示されます。	<ユーザー管理>を設定する	ユーザーは初回ログイン時に使用したデフォルトパスワードの変更を実施してください。 本機は管理者の初回ログイン時にパスワードの変更を促す警告を表示することができます。
	3.5.10	Store and transmit only cryptographically-protected passwords.	本要件は、組織のシステムへのログインアカウントに関して、取り扱うパスワードを保護することを要求しています。本機は、ユーザー認証に用いるユーザーパスワードは、ハッシュ化または暗号化して本機内に保存しています。また、ストレージ暗号化や、TLSによる通信路暗号化機能も具備しています。	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。 本機はユーザー認証に用いるパスワードをハッシュ化または暗号化して保存しています。 **ストレージデータの暗号化** 本機のストレージには、アドバンスドボックスやユーザーボックス内のファイル、アドレス帳の登録情報、残存するジョブデータ、パスワード情報などが保存されています。これらのデータを暗号化することにより、情報を不正に読み取られることを防いでいます。 **TLS暗号化通信** パソコンなどの機器から本機にアクセスしてデータをやりとりする際に、盗聴、改ざん、なりすましなどを防ぐために、TLS暗号化通信を利用することができます。	<ユーザー管理>を設定する <TLS設定>を設定する各機能/アプリケーションの設定で <TLSを使用>を有効にする。また、環境に応じてサーバー証明書の検証を実施するよう設定する。	ユーザーは組織のシステムへのログインアカウントに関して、取り扱うパスワードを暗号化により保護してください。 本機のパスワードはハッシュ化または暗号化して保存されています。 リモートUIからログイン操作を行う場合はTLSを有効にすることで通信路におけるパスワードの保護を実現できます。
	3.5.11	Obscure feedback of authentication information.	本要件は、組織のシステムへのログインアカウントに関して、パスワード入力時のショルダーハックを防止するため、アスタリスク等でパスワードを隠蔽することを要求していいます。本機は、パスワード入力時に、入力文字を伏字にする機能を具備しており、他者から覗き見られることを防止できます。	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。 本機はパスワード入力時に、入力文字を伏字にして表示します。	N/A	ユーザーはパスワード入力時のパスワード伏字化などの認証情報を隠蔽するための対策を行ってください。ただし、本機は設定不要です。
3.6 インシデント対応 Basic (基本セキュリティー要件)	3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	本要件は、組織にインシデントレスポンス体制の確立を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織はCSIRT(Computer Security Incident Response Team)などのインシデントレスポンスチームを立ち上げる必要があります。	N/A	-	ユーザーはインシデントレスポンス体制を定め、確立してください。
	3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	本要件は、インシデントレスポンスに関するものであり、特にインシデント発生時の原因追跡、文書化、報告(組織内・外)を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。CSIRTによるインシデントの調査・対応、及びその結果を、組織は文書化する必要があります。また、組織は、組織内・外に調査結果を報告する必要があります。	N/A	-	ユーザーはインシデントレスポンスのプロセス、特にインシデント発生時の原因追跡、文書化、報告(組織内・外)のプロセスを定め、確立してください。
3.6 インシデント対応 Derived (派生セキュリティー要件)	3.6.3	Test the organizational incident response capability.	本要件は、インシデントレスポンスに関するものであり、特に組織のインシデントレスポンス能力のテストを要求するものです。本要件の主な責務は組織側であり、本機は対象外です。	N/A	-	ユーザーはインシデント対応トレーニングのテストを実施してください。

NIST SP 800-171 rev2 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンター側の対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.7 メンテナンス Basic (基本セキュリティー要件)	3.7.1	Perform maintenance on organizational systems.	本要件は、組織のシステムに対してメンテナンスの実施を要求するものです。本要件の主な責務は組織側であり、組織は保守計画にのっとり、組織内のシステムのメンテナンスを実施する必要があります。本機は、組織の対応をサポートする機能として、ストレージ交換時にデータをバックアップし、レストアする機能を具備しています。	**データのバックアップ／リストア** 本機に保存されているデータを、外付けのストレージまたはSMBサーバーにバックアップすることができます。事前にバックアップしておくことで、万一のときにも復元することが可能です。	リモートUIの[データ管理]によりバックアップ/リストアを実行する	ユーザーは保守計画に則り、機器のメンテナンスを実施してください。 メンテナンスには定期的な計画保守、不定期保守、必要に応じた再構成、および破損修理が含まれます。 本機はストレージ交換時のデータバックアップ機能を有しており、ユーザーはメンテナンス時にバックアップを取り、メンテナンス終了後にデータをリストアすることができます。
	3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	本要件は、組織のシステムに対するメンテナンスにおいて、メンテナンス用ツール等の管理・保護を要求するものです。本要件の主な責務は組織側ですが、本機の保守は担当サービスが行うため、メンテナンスツールに対する管理と保護を実施する必要があります。キヤノンではメンテナンスに用いるツールの管理とメンテナンス時における教育を実施しています。	N/A	-	ユーザーはメンテナンス要員の監督とメンテナンスツールに対する管理・保護を実施してください。
3.7 メンテナンス Derived (派生セキュリティー要件)	3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI（Controlled Unclassified Information）.	本要件は、組織のシステムに対するオフサイトメンテナンスにおいて、システム内の CUI（Controlled Unclassified Information） をサニタイズ(無効化・削除)することを要求するものです。組織は、システムを外部組織にメンテナンスに出す際に、システム内のCUIを盗み見られないようにデータ削除したり、ストレージを取り外すなどすることで、CUIをサニタイズする必要があります。本機は、組織の対応をサポートする機能として、機器内のデータを完全に消去する機能を提供しています。	**すべてのデータ／設定を初期化** 本機のすべての設定値をお買い上げ時の状態に戻します。ストレージ内に残されたデータは「0」や他の値で上書きして完全に消去されるため、ストレージの交換や廃棄時に機密データが外部に流失するのを防ぐことができます。	<全データ/設定の初期化>を実行する	ユーザーは機器を第三者によってメンテナンスさせる場合はストレージ内のCUI（Controlled Unclassified Information）に対するサニタイズを実施してください。 サニタイズの手段として、ストレージ内のデータを完全に消去することがあげられます。 データの消去の際には本機のデータ/設定初期化機能を利用することができます。
	3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	本要件は、組織のシステムに対するメンテナンスにおいて、可搬メディアを利用する場合、可搬メディアのウイルスチェックを要求するものです。本要件の主な責務は組織側ですが、本機の保守は担当サービスが行います。担当サービスは組織のセキュリティーポリシーに従い、対応を行います。(例えば、ウィルスチェックを実施したUSBメディアの利用など)	N/A	-	ユーザーはメンテナンスに使用する可搬メディアに対してウィルスチェックを実施してください。
	3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	本要件は、組織のシステムに対するメンテナンスにおいて、ネットワークを介したリモートメンテナンスを実行する場合に、多要素認証によるアクセス制御、及びリモートメンテナンス完了時に直ちにセッションを終了することを要求するものです。本機には、リモートメンテナンス機能はないため、当該要件は対象外となります。	N/A	-	ユーザーはネットワークを介したリモートメンテナンスを行う際には、多要素認証によるアクセス制御を実施してください。 リモートメンテナンス完了後には、直ちにセッションを終了してください。
	3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	本要件は、組織のシステムに対するメンテナンスにおいて、メンテナンス作業員の活動を監督することを要求するものです。本要件の主な責務は組織側であり、組織はオンサイトで作業するメンテナンス作業員が不正行為を働かないように監督する必要があります。外部組織のメンテナンス作業員に一時的に入室許可などのアカウントを提供する場合は、そのアカウント管理も組織側の責務となります。	N/A	-	ユーザーは機器のメンテナンス実施時には、作業員に対して機器にアクセスするための認可を行ってください。 ユーザーは機器のメンテナンスの監督を実施してください。

NIST SP 800-171 rev2 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンター側の対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.8 記憶媒体の保護 Basic (基本セキュリティー要件)	3.8.1	Protect (i.e., physically control and securely store) system media containing CUI（Controlled Unclassified Information）, both paper and digital.	本要件は、組織が取り扱う CUI（Controlled Unclassified Information） を含む媒体(紙・デジタルデータを含む可搬メディア)の保護を要求するものです。本要件の主な責務は組織側であり、組織は自組織が取り扱うCUIを含む可搬メディアや紙媒体を入室管理がされた場所に格納するなどし、保護する必要があります。本機は、組織側の対応をサポートする機能として、CUIを含む印刷物が第三者に不正に持ち去られないように、強制留め置き印刷機能や可搬メディアの使用を制限する機能を具備しています。	**留め置き印刷** 「印刷物放置による持ち去り」や「意図しない情報開示」、「ミスプリント防止」などの目的で、管理者によって強制的にいったん印刷する文書を本機内に留めることができます。 **メモリーメディアの使用の制限** USBメモリーなどのメモリーメディアは手軽で便利な反面、適切に管理されていない環境下では逆に情報漏えいの要因となる恐れがあります。モリーメディアの使用を禁止して、スキャン文書をメモリーメディアに保存できなくしたり、メモリーメディア内のデータを印刷できないようにしたりします。	＜強制留め置き＞を有効にする ＜メモリーメディア設定＞＜スキャン機能を使用＞または＜プリント機能を使用＞で＜OFF＞を選択	ユーザーは自組織が取り扱うCUI（Controlled Unclassified Information）を含む可搬メディアや紙媒体を保護してください。 例えば、CUIの記載されている印刷物について入室管理などによりアクセス制限が課されている場所に設置する、あるいは鍵のかかった収納に保存することで保護してください。 本機には、CUIの保護をサポートする機能として留め置き印刷機能やメモリーメディアの使用制限機能があります。 強制留め置き印刷を設定することで、第三者が印刷物を持ち去ることを防止することができます。可搬メディアの使用を制限する際は、メモリーメディア設定を設定してください。
	3.8.2	Limit access to CUI （Controlled Unclassified Information） on system media to authorized users	本要件は、組織が取り扱う CUI（Controlled Unclassified Information） を含む媒体(紙・デジタルデータを含む可搬メディア)へのアクセス制御を要求するものです。本要件の主な責務は組織側であり、組織は自組織が取り扱うCUIを含む媒体を許可された利用者のみがアクセスできる場所に保管する必要があります。また、台帳などで媒体の持ち出し履歴を記録する必要があります。	N/A	-	ユーザーは自組織が取り扱うCUI（Controlled Unclassified Information）を含む可搬メディアや紙媒体に対するアクセスを制限してください。 例えば、ユーザーは機器を入室管理などによりアクセス制限が課されている場所に設置する、あるいは機器のストレージを鍵のかかった収納に保存し、限られたユーザーのみがアクセスできるようにしてください。 メディアへのアクセスの際にはチェックアウトと返却のプロセスを実施し、メディアへのアクセスを記録してください。
	3.8.3	Sanitize or destroy system media containing CUI （Controlled Unclassified Information） before disposal or release for reuse.	本要件は、組織が取り扱う CUI（Controlled Unclassified Information） を含む媒体(紙・デジタルデータを含む可搬メディア)、及びシステムデバイスに内蔵された記録媒体(内蔵ストレージ)を手放す際に、適切にサニタイズ・破壊することを要求するものです。本機は、内蔵ストレージ内のデータを完全消去する機能を具備しており、本機を廃却したり、リユースに出す前に本機能により、サニタイズできます。	**すべてのデータ／設定を初期化** 本機のすべての設定値をお買い上げ時の状態に戻します。ストレージ内に残されたデータは「0」や他の値で上書きして完全に消去されるため、ストレージの交換や廃棄時に機密データが外部に流失するのを防ぐことができます。	＜全データ/設定の初期化＞を実行する	ユーザーは機器を廃却あるいはリユースする際に、内蔵ストレージの情報を消去してください。 消去の際には本機の全データ/設定の初期化機能を利用することができます。
3.8 記憶媒体の保護 Derived (派生セキュリティー要件)	3.8.4	Mark media with necessary CUI（Controlled Unclassified Information） markings and distribution limitations.	本要件は、組織が取り扱う CUI（Controlled Unclassified Information） を含む媒体(紙・デジタルデータを含む可搬メディア)に対し、CUIを含む媒体であることをマーク表示等で明示し、注意喚起することを要求するものです。本要件の主な責務は組織側であり、本機は対象外です。本機は、組織側の対応をサポートする機能として、CUIを含む印刷物であること示すスタンプの印字や地紋印字機能を具備しています。	**スタンプ** 印刷／コピーするときに、「社外秘」などのスタンプを付けることが可能です。 **地紋印字** 印刷／コピーするときに、「コピー禁止」や「社外秘」などの見えない文字を出力紙の背景に常に埋め込むようにすることができます。出力紙を複製しようとすると、埋め込まれた文字が用紙全面に浮かび上がって出力されるので、無断複製や情報の流出についてユーザーに注意を促すことができます。	＜スタンプ＞または＜地紋印字の設定＞を設定する	ユーザーは機器で取り扱う情報(e.g. 印刷物)にCUI（Controlled Unclassified Information）が含まれる場合、その旨を表示してください。 例えば、印刷物に機密レベルを表示することにより、閲覧可能なユーザーを明示してください。 本機のスタンプまたは地紋印字機能を利用することで、CUI を含む印刷物であることを示す文字(e.g. 機密レベル)をスタンプとして出力紙に印字したり、地紋として埋め込むことができます。
	3.8.5	Control access to media containing CUI（Controlled Unclassified Information） and maintain accountability for media during transport outside of controlled areas.	本要件は、組織が取り扱う CUI（Controlled Unclassified Information） を含む媒体(紙・デジタルデータを含む可搬メディア)に対し、アクセス制御、及び外部持ち出し時の説明責任維持を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。なお、外部持ち出し時の説明責任維持方法としては、例えば、メディア内データの暗号化・改ざん検知があります。また、他にもメディアの輸送活動を許可された担当者に制限し、メディアの輸送経路を追跡して明確な記録を取得し、紛失、破壊、改ざんを防止および検出することでも実現できます。	N/A	-	機器や機器の内蔵ストレージを設置・保管場所から持ち出す場合はCUI（Controlled Unclassified Information）の完全性と機密性を保護してください。 完全性・機密性の保護は、メディアの暗号化、メディアの輸送活動を行う担当者の制限と輸送経路の追跡と記録などにより実現できます。
	3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI （Controlled Unclassified Information） stored on digital media during transport unless otherwise protected by alternative physical safeguards	本要件は、組織が取り扱う CUI（Controlled Unclassified Information） を含む媒体(デジタルデータを含む可搬メディア)に対し、持ち出し中の機密性確保を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織はCUIを含む可搬メディアを持ち出す際は、データを暗号化した上で持ち出すように運用する必要があります。	N/A	-	機器や可搬メディアを設置・保管場所から持ち出す場合はCUI（Controlled Unclassified Information）の完全性と機密性を保護してください。

NIST SP 800-171 rev2 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンター側の対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.8 記憶媒体の保護 Derived (派生セキュリティー要件)	3.8.7	Control the use of removable media on system components.	本要件は、組織が取り扱う CUI（Controlled Unclassified Information） を含むリムーバブルメディア(e.g. 外付け HDD)の管理を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織は例えば以下のような管理を行う必要があります。 ・リムーバブルメディアを組織内のシステムに接続する際にウイルスチェックを実施 ・リムーバブルメディア数の管理(必要最小限に) ・持ち出し時のトレーサビリティ確保(正しく廃棄・再利用されたことまで要追跡) 本機は、組織側の対応をサポートする機能として、本機での可搬メディアの使用を制限する機能を具備しています。	**メモリーメディアの使用の制限** USBメモリーなどのメモリーメディアは手軽で便利な反面、適切に管理されていない環境下では逆に情報漏えいの要因となる恐れがあります。ここでは、メモリーメディアの使用を禁止して、スキャン文書をメモリーメディアに保存できなくしたり、メモリーメディア内のデータを印刷できないようにしたりします。	<メモリーメディア設定> <スキャン機能を使用>または<プリント機能を使用>で<OFF>を選択	ユーザーはCUI（Controlled Unclassified Information）を含むリムーバブルメディアに対する管理を実施してください。 例えば、組織で扱うリムーバルメディアに対して、使用を制限・あるいは禁止してください。 リムーバルメディアを使用する場合には、メディア内に悪意のあるコードが混入していないことを確認し、持ち出す際にはトレーサビリティを確保し、メディアの廃棄や再利用について追跡してください。 本機で可搬メディアの使用を制限する際は、メモリーメディア設定を設定してください。
	3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	本要件は、組織が取り扱う CUI（Controlled Unclassified Information） を含むポータブルストレージデバイスにおいて、識別可能な所有者がいない場合、使用の禁止を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織は識別可能な所有者(個人、組織、プロジェクトなど)がいないポータブルストレージデバイスは、リスク回避のため、使用を禁止する必要があります。 本機は、組織側の対応をサポートする機能として、本機での可搬メディアの使用を制限する機能を具備しています。	**メモリーメディアの使用の制限** USBメモリーなどのメモリーメディアは手軽で便利な反面、適切に管理されていない環境下では逆に情報漏えいの要因となる恐れがあります。ここでは、メモリーメディアの使用を禁止して、スキャン文書をメモリーメディアに保存できなくしたり、メモリーメディア内のデータを印刷できないようにしたりします。	<メモリーメディア設定> <スキャン機能を使用>または<プリント機能を使用>で<OFF>を選択	ユーザーは識別可能な所有者がいないCUI（Controlled Unclassified Information）を含むポータブルストレージデバイスの使用を禁止してください。 例えば、組織で扱うポータブルストレージデバイスに所有者(個人、組織、グループ）のラベルを張り付けることを義務化し、ラベルのないデバイスの使用を禁止してください。 本機で可搬メディアの使用を制限する際は、メモリーメディア設定を設定してください。
	3.8.9	Protect the confidentiality of backup CUI（Controlled Unclassified Information） at storage locations.	本要件は、組織が保存するバックアップ用の CUI（Controlled Unclassified Information） において、バックアップ CUI に関しても機密性を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織は例えば、CUIを暗号化したうえで、外付けHDDにバックアップとして保存し、かつ当該外付けHDDは物理的なアクセス制御(e.g. 入室制限)などで保護する必要があります。本機は、組織側の対応をサポートする機能として、データバックアップ時にバックアップデータを暗号化することが可能です。	**データのバックアップ／リストア** 本機に保存されているデータを、外付けのストレージまたはSMBサーバーにバックアップすることができます。事前にバックアップしておくことで、万一のときにも復元することが可能です。バックアップの際にパスワードを入力すると、バックアップする保存データを暗号化できます。	リモートUIの[データ管理]によりバックアップ/リストアを実行する ［バックアップデータを暗号化する］を設定する	ユーザーは機器で扱うCUI（Controlled Unclassified Information）のバックアップを取る際には、バックアップの機密性の保護をしてください。 例えば、バックアップデータを保存したHDDを暗号化したうえで入室管理などによりアクセス制限が課されている場所に設置する、あるいは鍵のかかった収納に保存し、限られたユーザーのみがアクセスできるようにしてください。 本機のデータのバックアップ／リストア機能を利用することで、外付けのストレージまたは、SMBサーバーにデータをバックアップすることができます。さらにバックアップデータは暗号化することも可能です。
3.9 要員のセキュリティー Basic (基本セキュリティー要件)	3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI（Controlled Unclassified Information）.	本要件は、CUI（Controlled Unclassified Information） を含む組織のシステムへのアクセス許可を出す際に、個人の審査を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織はスクリーニングにより個人を審査する必要があります。スクリーニングとして、例えば、バックグラウンドチェックや薬物検査を実施したり、各役職に必要なアクセスレベルに応じて、適切な法律、ポリシー、規制、基準を反映したスクリーニングを行う必要があります。	N/A	-	ユーザーは組織でCUI（Controlled Unclassified Information）を取り扱う場合には、CUIを取り扱う個人に対してスクリーニングを実施してください。 スクリーニングには、バックグラウンドチェックや薬物検査などが含まれ、各役職に必要なアクセスレベルに応じて適切な法律、ポリシー、規制、基準を反映したスクリーニングを行う必要があります。
	3.9.2	Ensure that organizational systems containing CUI （Controlled Unclassified Information） are protected during and after personnel actions such as terminations and transfers.	本要件は、離職や配置転換等の人事異動の前後で、CUI（Controlled Unclassified Information）及びCUIを含む組織のシステムが変わらず保護されることを要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織は例えば以下により離職者から CUIを保護する必要があります。 ・全社のIT機器(例えば、ラップトップ、携帯電話、記憶装置)の返却 ・すべてのID/アクセスカードおよび/またはキーの返却 ・退社後もCUIを話さない義務があることを社員に再認識させるための出口面接を実施 加えて組織は以下のような対応を行う必要があります。 ・再使用する前にすべての機器内のデータを消去 ・CUIへのアクセスを許可しているすべてのアカウントへのアクセスを削除 ・従業員アカウントの無効化またはクローズ ・CUIを使用する物理スペースへのアクセスを制限	N/A	-	ユーザーは機器の利用者が人事異動による配置転換あるいは離職した場合に機器のCUI（Controlled Unclassified Information）にアクセスできないよう対策を実施してください。 例えば、配置転換あるいは離職するユーザー本人に対しては、貸し出していたIT機器やIDカードなどの返却を要求し、CUIなどの機密情報に関する制約の確認を行ってください。組織は、返却してもらったIT機器の情報の消去やアカウントの無効化を実施してください。
3.10 物理的保護 Basic (基本セキュリティー要件)	3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	本要件は、組織のシステム、装置等への物理アクセスを許可された個人に限定することを要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織は例えば入室管理などによりシステムに物理アクセス可能な人物を制限する必要があります。	N/A	-	ユーザーは、許可された個人だけが物理的にアクセスできる環境に、機器を設置してください。 許可された個人だけが物理的にアクセスできる環境としては、例えば、施錠やその他の方法により物理的に他と隔離されて、バッジ・IDカード・スマートカード等に含まれる資格情報によりアクセスが制御されている環境が想定されます。機器の設置場所としては部屋が想定されますので、部屋へのアクセス制御、つまり入室管理が主な対策と考えられます。しかし、敷地・建物といったレベルでのアクセス制御の有効性も考慮を要する場合もあります。

NIST SP 800-171 rev2 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンター側の対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.10 物理的保護 Basic (基本セキュリティー要件)	3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	本要件は、組織が具備するシステムインフラ(送電施設、電源ケーブル、ネットワークケーブル等)の保護・監視を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織は例えば入室管理や監視カメラにより、IT設備を保護・監視する必要があります。	N/A	-	ユーザーは、ユーザー組織の物理的なインフラシステムを保護・監視してください。 インフラシステムとしては次のようなものが想定できます。 ・電力インフラをサポートする送電施設、電源ケーブル等。 ・ネットワークインフラをサポートするネットワークケーブル、HUB、ルーター等。 ・設置環境をサポートする入室管理システム、管理カメラ等。
3.10 物理的保護 Derived (派生セキュリティー要件)	3.10.3	Escort visitors and monitor visitor activity.	本要件は、組織への訪問者・来客のエスコート・監視を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織は例えば訪問者バッチや従業員の付き添いにより、訪問者の活動を監視する必要があります。	N/A	-	ユーザーは訪問者を常にエスコートして、ユーザーの施設内での訪問者の行動を監視してください。また、来訪記録等、訪問者の活動を記録してください。 これらを実現するためには、次の事項も検討する必要があります。 ・訪問者のエスコート手順の確立。 ・バッジ・名札等の訪問者識別手段の活用。
	3.10.4	Maintain audit logs of physical access.	本要件は、組織内施設への入室や、システムへの物理アクセスの監査ログ記録を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織は例えばIDカードによる入室時に自動で監査ログに入退室が記録されるようにしたり、受付等で訪問者の施設への出入りを記録する必要があります。	N/A	-	ユーザーは、物理的アクセスに関する監査ログを適切に管理してください。 物理的アクセスに関する監査ログは、敷地・建物・居室といった施設へアクセスに関するログのほかに、来客に関するログもあります。
	3.10.5	Control and manage physical access devices.	本要件は、組織内施設への入室やシステムへの物理アクセスに用いるハードウェアトークン (e.g. IDカード) の管理を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織は例えばIDカードで付与されるアクセス権をIDカードを貸与した個人ごとに管理する必要があります。	N/A	-	ユーザーは、物理的アクセス制御に用いているデバイス (e.g. ハードウェアトークン、IDカード) を適切に管理してください。 適切な管理のためには、次の事項も検討する必要があります。 ・発行から破棄・失効までの一連のライフサイクルを通しての処理フローの確立。 ・紛失時、貸与時などの例外的な処理への対応。
	3.10.6	Enforce safeguarding measures for CUI （Controlled Unclassified Information） at alternate work sites.	本要件は、組織の代替作業サイト (e.g. 在宅勤務、サテライトオフィス) における CUI（Controlled Unclassified Information） の保護を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織は例えばポリシーや組織規定に応じて、以下のような対策を講じる必要があります。 ・持ち出しノートパソコンには、パッチ管理機能、ウイルス対策ソフト導入や、HDD暗号化を実施 ・組織内システムへのアクセスにはVPNなどのセキュアな通信手段の実施	N/A	-	ユーザーは、代替の作業サイト (e.g. テレワークのサイト、サテライトサイト) で物理的なアクセス制御を適切に実施してください。 代替の作業サイトにおいても、通常作業サイトと同等のレベルの対策が必要になります。
3.11 リスク評価 Basic (基本セキュリティー要件)	3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI（Controlled Unclassified Information）.	本要件は、CUI（Controlled Unclassified Information） に関する組織運用、組織資産、及び個人に対するリスクへの定期的なアセスメントを要求するものです。本要件の主な責務は組織側であり、本機は対象外です。なお、ここで述べるリスクアセスメントは一般的なビジネスに対するものであり、3.12 のセキュリティー(脆弱性)アセスメントとは異なります。組織は例えば以下のような重大インシデントにつながる恐れのあるリスクを定期的にアセスメントする必要があります。 ・不十分に設計され実行されたビジネスプロセス ・情報の開示や修正などの不注意による人々の行動 ・内部からの脅迫や詐欺などの意図的な行為 ・システムが意図した通りに機能しないこと ・自然災害、公共インフラ、サプライ・チェーンの障害などの外部イベント	N/A	-	ユーザーは、業務と資産に対して、リスクアセスメント (リスクの評価) を定期的に実施してください。 リスクアセスメントとしては、次の事項も検討する必要があります。 ・情報システムと、その情報システムが処理、保存、または伝送する情報の不正なアクセス、利用、開示、中断／途絶、変更、破壊が発生する可能性と被害の大きさを含めてリスクを判断する。 ・リスクアセスメントの結果を記録するとともに、ステークホルダーとレビュー・結果の共有する。 ・情報システムが稼働する環境に大きな変化があった場合、もしくはセキュリティー状態に影響をあたえる他の状況変化があった場合は、速やかにリスクアセスメントを実施する。
3.11 リスク評価 Derived (派生セキュリティー要件)	3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	本要件は、組織のシステムに対する定期的な脆弱性スキャンを要求するものです。本要件の主な責務は組織側です。組織は例えば、市販の脆弱性スキャナを用い、本機を含めて組織内システムやアプリケーションの脆弱性を定期的に評価する必要があります。	N/A	-	ユーザーは、関連する情報システム・アプリケーションに対して新たな脆弱性が発見された場合、または定期的に、脆弱性のスキャンを実施してください。
	3.11.3	Remediate vulnerabilities in accordance with risk assessments.	本要件は、組織のシステムに見つかった脆弱性への対応を要求するものです。本要件の主な責務は組織側です。組織は例えば、市販の脆弱性スキャナを用い、本機を含めて組織内システムやアプリケーションの脆弱性を検出・評価し、必要に応じて脆弱性を修正するようにパッチを充てるなどする必要があります。	N/A	-	ユーザーは、リスクアセスメントで識別した脆弱性を修正してください。情報システムへ修正パッチを充てる方法もありますし、脆弱性を回避する管理策を規定する修正方法も考えられます。

NIST SP 800-171 rev2 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンター側の対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.12 セキュリティー評価 Basic (基本セキュリティー要件)	3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	本要件は、組織のシステムにおけるセキュリティー管理策の定期的なアセスメントを要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織は例えば、以下のような対応によりセキュリティー管理策のアセスメント(セキュリティーアセスメント)を行う必要があります。 ・セキュリティー管理策の定期的な評価、及び文書化 ・提案された新しい管理策、または既存の管理策の更新 ・管理策の修正(改善)計画の立案 ・新たに発見されたセキュリティーリスクの文書化する	N/A	-	ユーザーは、組織のシステムにおけるセキュリティー管理策のアセスメントを定期的に実施してください。
	3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	本要件は、組織のシステムにおける脆弱性対応に関する行動計画の立案及び実施を要求するものです。本要件の主な責務は組織側です。組織は例えば、脆弱性スキャナなどで本機を含む組織内システムに脆弱性が見つかった場合は、すみやかに脆弱性対応を行うための行動計画を立案し、実行する必要があります。行動計画には例えば以下のようなことが含められます。 ・脆弱性対応の責任者 ・対応方法、対応時期の記載 ・対応結果の評価・測定方法の定義	N/A	-	ユーザーは、組織のシステムにおいて、欠陥を修正し、脆弱性を軽減・除去するための行動計画を立案し、実施してください。
	3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	本要件は、組織のシステムにおけるセキュリティー管理策の有効性検証のために、継続的な管理策の確認を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織は例えば、定期的に自組織システム内のハードウェア、ソフトウェア、ファームウェアのインベントリ等を、予め定義したセキュリティー管理策と合致した運用になっているか確認し、必要に応じて改善し、結果を上層部等に報告する必要があります。	N/A	-	ユーザーは、管理策の継続的な有効性を確実にするため、セキュリティー管理策を確認し、必要に応じて改善してください。
	3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	本要件は、組織がセキュリティー要件を実装する方法を概説した文書であるシステムセキュリティー計画の策定を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織は、例えば NIST SP 800-18 を参考にシステムセキュリティー計画の策定する必要があります。	N/A	-	ユーザーは、システムセキュリティー計画を策定し、文書化し、定期的に更新してください。システムセキュリティー計画は、システム境界・システムの運用環境、セキュリティー要件がどのように実装されているか、他のシステムとの関係について示してください。
3.13 システムと通信の保護 Basic (基本セキュリティー要件)	3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	本要件は、組織のシステム境界における通信の監視・制御・保護を要求するものです。本機はファイアウォール機能を具備しており、本機能を用いることで本機の境界を通る通信 (本機が送受信する通信データ) の監視・制御・保護が可能です。さらに、本機はプロキシーサーバーを利用する機能を具備しており、本機能を用いることで組織システムの境界を通る通信をプロキシーサーバーが監視・制御・保護できます。	**ファイアウォール** ファイアウォールとは、外部ネットワークからの不正アクセスを防止し、ローカルエリア内のネットワークへの攻撃や侵入を防ぐシステムです。お使いのネットワーク環境で、特定の外部IPアドレスからの通信を制限することで、危険と思われる外部からのアクセスをあらかじめ遮断できます。 **プロキシー設定** ウェブサイトの閲覧時にプロキシーサーバーを経由して外部に接続します。プロキシーサーバーを使うとより安全にウェブサイトを閲覧することができるため、セキュリティーの向上が期待できます。	<ファイアウォール設定>を設定する <プロキシー設定>を有効にする	ユーザーは組織システムの外部境界、および主要な内部境界において、通信を監視し、管理し、保護してください。第一には、組織システムの外部境界、および主要な内部境界を定義してください。次に、定義した境界において、プロキシーサーバーを設置する等、通信を監視し、管理し、保護してください。 本機はファイアウォール機能、およびプロキシーサーバーを利用する機能を具備しています。 組織のシステムで実施すべきセキュリティー管理方針に従い、本機が実施すべき機能を有効化して、実施してください。
	3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	本要件は、組織の IT インフラ開発において、セキュリティーを考慮したアーキテクチャ設計、ソフトウェア開発手法、及びシステムエンジニアリングの原則を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織は、例えば NIST SP 800-160 (System Security Engineering) を参考に、そこから適用可能な手法を取り入れ、システム開発に取り組む必要があります。	N/A	-	ユーザーは、組織のITシステムの新規開発・アップグレード時において、情報セキュリティーを考慮して、アーキテクチャ設計・ソフトウェア開発手法・システムエンジニアリングの原則を採用してください。

NIST SP 800-171 rev2 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンター側の対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.13 システムと通信の保護 Derived (派生セキュリティー要件)	3.13.3	Separate user functionality from system management functionality.	本要件は、組織のシステムにおいて、ユーザー機能とシステム管理機能とに分離することを要求するものです。本機は、システム管理者向けの機能 (e.g. 設定変更) と、一般ユーザー用の機能 (e.g. プリント、スキャン) とに分離されています。また、ユーザー認証機能により、システム管理者向けの機能を利用可能な特権ユーザー (管理者) と、一般ユーザーとを識別して認証 (アクセス制御) することが可能です。	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。	<ユーザー管理>を設定する	ユーザーは、組織のシステムにおいて、ユーザー機能とシステム管理機能を分離してください。 本機は管理者向けの機能 (e.g. 設定変更) と、ユーザー向け機能 (e.g. プリント、スキャン、センド) とに分離されています。組織のシステムで実施すべきセキュリティー管理方針に従い、本機が実施すべき管理者機能を有効化して、実施してください。
	3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	本要件は、組織のシステムにおいて、ストレージ等の共有システム資源を介した情報漏洩を防止することを要求するものです。 本機は、ストレージ上の不正な情報転送や意図せぬ情報転送を防止する、強制留め置き機能・アドバンスドボックスの認証管理機能を具備しています。	**留め置き印刷** 「印刷物放置による持ち去り」や「意図しない情報開示」、「ミスプリント防止」などの目的で、管理者によって強制的にいったん印刷する文書を本機内に留めることができます。 **アドバンスドボックスの認証管理** アドバンスドボックスを公開する際に認証設定を行うことで不正アクセスを防止できます。	<強制留め置き>を有効にする <アドバンスドボックス設定>の<認証管理>を設定する	ユーザーは、組織のシステムにおいて、ストレージ等の共有システム資源を介した情報漏洩を防止してください。 本機は、強制留め置き機能やアドバンスドボックスの認証管理機能によって、ストレージ等の共有システム資源を介した情報漏洩を防止することが可能です。組織のシステムで実施すべきセキュリティー管理方針に従い、これらの設定を行ってください。
	3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	本要件は、外部公開された組織のシステムのネットワーク分離として、サブネットワークの利用を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織は、例えば、内部ネットワークとインターネットなど外部ネットワークとの間に中立地帯（DMZ）を設ける必要があります。	N/A	-	ユーザーは、内部ネットワークから物理的または論理的に分離されるサブネットワークを構築し、外部公開用システムコンポーネントを構築したサブネットワーク上に配置してください。
	3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	本要件は、組織のシステムのネットワーク制御において、デフォルトで通信トラフィックを拒否し、例外によってのみ許可することを要求するものです (ホワイトリスト方式)。本機は、ファイアウォール機能を具備しており、組織は本機能を利用することで、自社のセキュリティーポリシーに従い全通信を拒否し、必要な通信のみ例外で許可するように設定可能です (ホワイトリスト方式)。	**ファイアウォール** ファイアウォールとは、外部ネットワークからの不正アクセスを防止し、ローカルエリア内のネットワークへの攻撃や侵入を防ぐシステムです。お使いのネットワーク環境で、特定の外部IPアドレスからの通信を制限することで、危険と思われる外部からのアクセスをあらかじめ遮断できます。	<ファイアウォール設定>を設定する	ユーザーは組織システムの外部境界、内部境界におけるファイアウォールの設定において、「デフォルトでネットワーク通信トラフィックを拒否し、例外によってネットワーク通信トラフィックを許可する」の方針で、設定してください。 本機が具備するファイアウォール機能を有効化する場合も、同様の方針で設定してください。
	3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	本要件は、組織が VPN を利用する際にスプリットトンネリングの無効化を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織は、VPNで外部から接続してくるリモートデバイス (ノートパソコン、スマートフォン、タブレットなど) の設定でスプリットトンネリングを無効化したり、リモートデバイスのスプリットトンネリング (またはスプリットトンネリングを許可する設定) を検出し、リモートデバイスがスプリットトンネリングを使用している場合は接続を禁止するように制御する必要があります。	N/A	-	ユーザーは、リモートデバイスが、組織のシステムとの非リモートコネクションの確立と同時に、外部ネットワークの資源への何らかの他のコネクションを介して通信すること (e.g. スプリットトンネリング) を防止してください。
	3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI（Controlled Unclassified Information）during transmission unless otherwise protected by alternative physical safeguards.	本要件は、組織のシステムにおける伝送データの保護 (情報漏洩対策) を要求するものです。本機は、FIPS140認証を取得した暗号モジュールを利用しています。また、FIPS 140-2 に準拠したアルゴリズムを利用し伝送データを暗号化するように設定することもできます。本機は、伝送データ暗号化機能として、TLS 機能や IPsec 機能 を具備しています。	**TLS暗号化通信** パソコンなどの機器から本機にアクセスしてデータをやりとりする際に、盗聴、改ざん、なりすましなどを防ぐために、TLS暗号化通信を利用することができます。 また、設定によりFIPS140-2準拠のアルゴリズムの使用に限定することが可能です。 **IPSec通信** TLS暗号化通信はWebブラウザーや電子メールクライアントなど、特定のアプリケーションで暗号化する技術ですが、IPSec通信はIPプロトコルのレベルで暗号化を行います。そのため、さらに汎用性の高いセキュリティーを実現できます。	<TLS設定>を設定する各機能/アプリケーションの設定で <TLSを使用>を有効にする。また、環境に応じてサーバー証明書の検証を実施するよう設定する。 <IPSecを使用>を有効にする <暗号方式をFIPS 140-2準拠にする>を有効にする	ユーザーは、伝送中にCUI（Controlled Unclassified Information）の不正な開示を防止するために暗号メカニズムを利用してください。 本機は、TLSやIPsecによって伝送データを暗号化することができます。TLSでは暗号アルゴリズムを選択できますので、FIPS140-2準拠の暗号アルゴリズムを選択してください。
	3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	本要件は、組織のシステムにおける通信セッション管理に関し、特にセッション終了時、もしくは所定時間非アクティブな場合、当該ネットワークコネクションを終了することを要求するものです。本機は通信セッション終了時もしくは所定時間非アクティブな場合、ネットワークコネクションを自動で切断する機能を具備しています。	本機は通信セッション終了時もしくは所定時間非アクティブな場合、ネットワークコネクションを自動で切断します。 例えば、リモートUIを一定時間操作しない場合、自動的にセッションを終了します。	N/A	ユーザーは、通信セッション終了時または定義された非アクティブな時間の経過後に、ネットワークコネクションを切断するような設定にしてください。 ただし、本機では、ネットワークセッションのタイムアウトに関する設定は不要です。

NIST SP 800-171 rev2 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンター側の対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.13 システムと通信の保護 Derived (派生セキュリティー要件)	3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	本要件は、組織のシステムにおける暗号鍵の管理を要求するものです。本要件の主な責務は組織側であり、組織は自組織が順守する必要のある法律や、行政命令、ポリシー、指令、規制、および基準にのっとり、CUI（Controlled Unclassified Information） の暗号化に用いる暗号鍵を管理・運用する必要があります。本機が暗号鍵の生成・保護等の鍵管理を行う際は、TPMによる鍵保護を行うことが可能です。	**TPM** 本機に記録されているパスワード、TLS通信用公開鍵ペア、ユーザー証明書などの機密情報を暗号化する暗号鍵（TPM鍵）をTPMチップ内に安全に保管できます。これにより、本機にとって重要な情報の漏えいを抑止できます。	<TPM設定>を設定する	ユーザーは、組織のシステムで実施すべきセキュリティー管理方針に従い、暗号鍵を生成・破棄・管理してください。 本機のTPM設定を有効化して、暗号化鍵を管理してください。
	3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI （Controlled Unclassified Information）.	本要件は、組織のシステムにおいて CUI（Controlled Unclassified Information） を暗号化で保護する際に、FIPS 認証取得済みの製品利用を要求するものです。本機はストレージ暗号化やTLS/IPSecによる暗号化通信において、FIPS認証取得済みの製品を利用しています。	**FIPS140-2準拠アルゴリズム** TLS通信の暗号化方式をFIPS140-2準拠のアルゴリズムに限定することが可能です。 ストレージ暗号化機能及びIPSec機能は、常にFIPS140-2準拠のアルゴリズムで動作するため、設定不要です。	<暗号方式をFIPS 140-2準拠にする>を有効にする	ユーザーは、FIPS認証取得済みの暗号モジュールを利用することを要求されます。 FIPS140-2準拠アルゴリズムが動作するよう本機の設定をしてください。
	3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	本要件は、組織が利用する TV 会議システムなどの協働コンピューティングデバイスにおいて、リモートアクセスによるデバイス活性化の禁止、及びデバイス利用の旨をユーザーに通知することを要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織は、例えば全てのデバイスに関して、リモートでカメラまたはマイクをオンにする機能を無効にしたり、カメラまたはマイクの電源が入ったときにユーザーに警告するツール (使用中に点灯するインジケータライトや、ポップアップ表示) などを利用する必要があります。	N/A	-	ユーザーは、組織が利用する TV 会議システムなどの協働コンピューティングデバイスにおいて、リモートアクセスによるデバイス活性化の禁止、及びデバイス利用の旨をユーザーに通知できるようにしてください。
	3.13.13	Control and monitor the use of mobile code.	本要件は、組織のシステムが利用するモバイルコード (e.g. JavaScript、ActiveX, Flash など) の利用監視を要求するものです。本機は、本機が具備する ウェブブラウザー上で実行されるモバイルコードを制御する機能として、JavaScript設定や、ウェブブラウザー機能そのものの利用を制御する機能を具備しています。	**ウェブブラウザー** ウェブブラウザー機能上で動作するモバイルコードとしてJavascriptが使用可能です。設定によりJavascriptの使用を制御できます。	<ウェブブラウザー> <JavaScriptの使用>を設定にする	ユーザーは、組織のシステムが利用するモバイルコード (e.g. JavaScript、ActiveX, Flash など)の利用監視してください。 本機でウェブブラウザー機能を有効にする場合は、JavaScriptの設定により管理してください。
	3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	本要件は、組織のシステムで利用する VoIP の管理・監視を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。本機は、IPファクス機能においてVoIPゲートウェイを利用することが可能です。	N/A	-	ユーザーは、VoIP を利用管理・監視してください。
	3.13.15	Protect the authenticity of communications sessions.	本要件は、組織のシステムが確立・利用する通信セッションの真正性の保護を要求するものです。本機は、TLS 通信による通信路暗号化で通信セッションを保護しています。 また、セッションIDをランダムに決定することによるセッション固定化攻撃対策などのセッションIDに対する攻撃対策も実施しています。	**TLS暗号化通信** パソコンなどの機器から本機にアクセスしてデータをやりとりする際に、盗聴、改ざん、なりすましなどを防ぐために、TLS暗号化通信を利用することができます。	<TLS設定>を設定する各機能/アプリケーションの設定で<TLSを使用>を有効にする。また、環境に応じてサーバー証明書の検証を実施するよう設定する。	ユーザーは、組織システムの通信セッションにおいて、中間者攻撃、セッションハイジャック、および通信セッションの改ざん等に対する保護を実施してください。 本機のTLS 通信による通信路暗号化によって、これらの攻撃への耐性を上げることができます。したがって、本機のTLS通信を有効にしてください。
	3.13.16	Protect the confidentiality of CUI （Controlled Unclassified Information） at rest.	本要件は、組織のシステム内に保持される CUI（Controlled Unclassified Information）の機密性の保護を要求するものです。本機は、ストレージ暗号化機能を具備しており、本機能により本機内に保存・蓄積されるデータの機密性を保護することができます。	**ストレージデータの暗号化** 本機のストレージには、アドバンスドボックスやユーザーボックス内のファイル、アドレス帳の登録情報、残存するジョブデータ、パスワード情報などが保存されています。これらのデータを暗号化することにより、情報を不正に読み取られることを防いでいます。	N/A	ユーザーは、組織システム内に保持される CUI（Controlled Unclassified Information）の機密性を担保してください。 本機のストレージに格納されるデータはストレージ暗号化機能により自動的に暗号化されます。
3.14 システムと情報の完全性 Basic (基本セキュリティー要件)	3.14.1	Identify, report, and correct system flaws in a timely manner.	本要件は、組織のシステムに関する既知脆弱性の識別・報告・修正を要求するものです。本要件の主な責務は組織側です。組織は組織内のシステムに関する脆弱性情報を収集・識別し、組織内の情報セキュリティー責任者に報告した上で、システムに悪影響を及ぼす脆弱性を速やかに修正する必要があります。機器に関する脆弱性がキヤノンから公表されたときは、速やかに組織内の情報セキュリティー責任者に報告し、必要に応じてファームウェアの更新を行います。また、本機は、手動及び定期的なファームウェアアップデート機能を具備しているため、脆弱性に対応されたファームウェアを本機に適応することが可能です。	N/A	-	ユーザーは、組織システムを構成するデバイス、ソフトウェアの脆弱性情報を収集し、適切に対応してください。 本機は、手動および自動でのファームウェアのアップデート機能を具備しています。これらの機能を利用して、ファームウェアのアップデートを実施してください。また、弊社のホームページに脆弱性情報を掲載していますので、定期的にアクセスして、脆弱性情報をご確認ください。
	3.14.2	Provide protection from malicious code at designated locations within organizational systems.	本要件は、組織のシステムに関して、悪意のあるコード (マルウェア) からの保護を要求するものです。本機は、マルウェアを検知する機能として、起動時・稼働時のシステム検証機能、ファームウェアやアプリケーションインストール時の署名検証機能を具備しています。	**起動時のシステム検証** 本機に組み込んであるファームウェア、システムやMEAPアプリケーションの完全性を、起動時に検証します。 **ランタイムシステム保護** 本機の稼働中に、ランタイムシステム保護機能を使ってプログラムの不正な改変と不正なプログラムの実行を防止し、システムの信頼性を向上できます。	<起動時のシステム検証>を有効にする <ランタイムシステム保護>を有効にする	ユーザーは、組織システムに対して、悪意のあるコードから保護してください。 本機は、MEAPアプリケーションのインストール時、ファームウェアのアップデート時にデジタル署名で検証することで、正規のソフトウェアだけをインストールすることができます。また、本機に組み込まれているソフトウェアを保護するために起動時のシステム検証、ランタイムシステム保護の機能を具備しています。これらの機能を有効化してください。
	3.14.3	Monitor system security alerts and advisories and take action in response.	本要件は、組織のシステムに関して、外部組織からのセキュリティーに関する警告・勧告の監視と適切な対応を要求するものです。本要件の主な責務は組織側であり、本機は対象外です。組織は、例えば社内のCSIRTで適宜 US-CERT などの外部組織からの警告・勧告がないかを監視し、必要に応じて、その警告・勧告に従いシステムに脆弱性パッチを適応します。	N/A	-	ユーザーは、組織システムを構成するデバイス、ソフトウェアの脆弱性情報を外部から受け取り、適切に対応してください。脆弱性情報は、US-CERT、JPCERT等の信頼できる外部組織から受け取る必要があります。

NIST SP 800-171 rev2 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンター側の対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.14 システムと情報の完全性 Derived (派生セキュリティー要件)	3.14.4	Update malicious code protection mechanisms when new releases are available.	本要件は、組織のシステムに関して、マルウェア検知機能の迅速なアップデートを要求するものです。本要件の主な責務は組織側であり、組織は例えば、組織内で利用しているウイルス検知ソフトの定義ファイルや・検知エンジンを自動で更新するように設定する必要があります。本機は、マルウェア検知機能として起動時・稼働時のシステム検証機能を具備しています。	**起動時のシステム検証** 本機に組み込んであるファームウェア、システムやMEAPアプリケーションの完全性を、起動時に検証します。 **ランタイムシステム保護** 本機の稼働中に、ランタイムシステム保護機能を使ってプログラムの不正な改変と不正なプログラムの実行を防止し、システムの信頼性を向上できます。	<起動時のシステム検証>を有効にする <ランタイムシステム保護>を有効にする	ユーザーは、組織システムに対する、悪意のあるコードからの保護メカニズムの更新があった場合、速やかにアップデートしてください。例えば、ウイルス検知ソフトの定義ファイルに更新があった場合、速やかに適応することが求められています。 本機の保護メカニズムではウィルス定義ファイルの更新は必要ありません。ファームウェアを常に最新に保つように更新してください。
	3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	本要件は、組織のシステムやファイルの定期スキャン、リアルタイムスキャンを要求するものです。本要件の主な責務は組織側であり、組織は例えば、ウイルス検知ソフトにより組織のシステムを定期的にスキャンするように設定したり、USBメモリーなどの可搬メディア利用の際は都度ウイルススキャンする必要があります。本機は、マルウェア検知機能として、起動時・稼働時のシステム検証機能を具備しており、ホワイトリスト方式で本機の起動時・稼働時にマルウェアを検知しています。また、ファームウェアやアプリケーションインストール時の署名検証機能により、マルウェアが不正にインストール・実行されるのを防止しています。	**起動時のシステム検証** 本機に組み込んであるファームウェア、システムやMEAPアプリケーションの完全性を、起動時に検証します。 **ランタイムシステム保護** 本機の稼働中に、ランタイムシステム保護機能を使ってプログラムの不正な改変と不正なプログラムの実行を防止し、システムの信頼性を向上できます。	<起動時のシステム検証>を有効にする <ランタイムシステム保護>を有効にする	ユーザーは、組織のシステムの定期的スキャン、およびファイルがダウンロード・オープン・実行されるような、外部情報源 (e.g. USBメモリーなど可搬メディア) からのファイルアクセス時のリアルタイムスキャンを実行してください。 本機は、ソフトウェアのインストール時、起動時、ランタイム時にそれぞれ、デジタル署名検証、起動時のシステム検証、ランタイムシステム保護によってスキャンを行っています。起動時システム検証、ランタイムシステム保護機能については、設定を有効化してください。
	3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	本要件は、組織のシステムに関する攻撃や潜在的な脅威の兆候を検知するために、組織のシステムの監視を要求するものです。本要件の主な責務は組織側であり、組織は、SIEMやIDS（Intrusion Detection System）・IPS（Intrusion Prevention System）などを用い、脅威の予兆を検知・監視し、必要に応じて対策する必要があります。本機は、組織の対応をサポートする機能として、以下の機能を具備しており、これらの機能が異常発見時 (不正通信ブロック、改ざん検知時) に記録する履歴やログを分析することでも、組織は本機に関する攻撃の予兆を検知できます。 ・ファイアウォール設定 ・起動時のシステム検証 ・ランタイムシステム保護 ・ファームウェアやMEAPアプリケーションインストール時の署名検証 ・監査ログ設定	**ファイアウォール** ファイアウォールとは、外部ネットワークからの不正アクセスを防止し、ローカルエリア内のネットワークへの攻撃や侵入を防ぐシステムです。お使いのネットワーク環境で、特定の外部IPアドレスからの通信を制限することで、危険と思われる外部からのアクセスをあらかじめ遮断できます。 ファイアウォールによって遮断された通信履歴は、IPアドレスブロック履歴から最新の100件を確認できます。遮断された通信の履歴は、リモートUIからCSV形式でエクスポートすることができます。 **起動時のシステム検証** 本機に組み込んであるファームウェア、システムやMEAPアプリケーションの完全性を、起動時に検証します。 **ランタイムシステム保護** 本機の稼働中に、ランタイムシステム保護機能を使ってプログラムの不正な改変と不正なプログラムの実行を防止し、システムの信頼性を向上できます。 **監査ログ機能** 本機がどのように使用されているかを確認／分析したいときは、ログを活用することができます。ログには操作日時、ユーザー名、操作の種類、機能の種類、操作結果などの情報が記録されます。また、Syslog送信を利用することで、SIEM（セキュリティー情報・イベント管理）システムにSyslogを送信することが可能です。SIEMシステムとの連携により、リアルタイムのアラート情報からさまざまな情報の分析が一元で管理できるようになります。	<ファイアウォール設定>を設定する <IPアドレスブロック履歴>を確認する <起動時のシステム検証>を有効にする <ランタイムシステム保護>を有効にする 監査ログ機能を有効にする	ユーザーは、攻撃や潜在的な攻撃の兆候を検出するために、ネットワークトラフィックを含んだ組織のシステムを監視してください。 本機は、ファイアウォールによって遮断された通信履歴に加えて、インストール時のデジタル署名検証、起動時のシステム検証、ランタイムシステム保護のログを取得することができます。これらのログを分析することで、攻撃・攻撃の兆候を検出できる可能性があります。
	3.14.7	Identify unauthorized use of organizational systems.	本要件は、組織のシステムの不正利用の識別を要求するものです。本要件の主な責務は組織側であり、組織は例えば、IDS（Intrusion Detection System）・IPS（Intrusion Prevention System）やウイルス検知ソフト、SIEMなどを用い、組織のシステムの利用状況を監視し、不正利用を識別(特定)する必要があります。本機は、組織の対応をサポートする機能として、以下の機能を具備しており、これらの機能が異常発見時 (不正通信ブロック、改ざん検知時) に記録する履歴やログを分析することでも、組織は本機に関する不正利用を識別 (特定) できます。 ・ファイアウォール設定 ・起動時のシステム検証 ・ランタイムシステム保護 ・ファームウェアやMEAPアプリケーションインストール時の署名検証 ・監査ログ設定	**ファイアウォール** ファイアウォールとは、外部ネットワークからの不正アクセスを防止し、ローカルエリア内のネットワークへの攻撃や侵入を防ぐシステムです。お使いのネットワーク環境で、特定の外部IPアドレスからの通信を制限することで、危険と思われる外部からのアクセスをあらかじめ遮断できます。 ファイアウォールによって遮断された通信履歴は、IPアドレスブロック履歴から最新の100件を確認できます。遮断された通信の履歴は、リモートUIからCSV形式でエクスポートすることができます。 **起動時のシステム検証** 本機に組み込んであるファームウェア、システムやMEAPアプリケーションの完全性を、起動時に検証します。 **ランタイムシステム保護** 本機の稼働中に、ランタイムシステム保護機能を使ってプログラムの不正な改変と不正なプログラムの実行を防止し、システムの信頼性を向上できます。 **監査ログ機能** 本機がどのように使用されているかを確認／分析したいときは、ログを活用することができます。ログには操作日時、ユーザー名、操作の種類、機能の種類、操作結果などの情報が記録されます。また、Syslog送信を利用することで、SIEM（セキュリティー情報・イベント管理）システムにSyslogを送信することが可能です。SIEMシステムとの連携により、リアルタイムのアラート情報からさまざまな情報の分析が一元で管理できるようになります。	<ファイアウォール設定>を設定する <IPアドレスブロック履歴>を確認する <起動時のシステム検証>を有効にする <ランタイムシステム保護>を有効にする 監査ログ機能を有効にする	ユーザーは、無許可、不正な組織のシステムの利用を識別してください。 本機は、ファイアウォールによって遮断された通信履歴に加えて、インストール時のデジタル署名検証、起動時のシステム検証、ランタイムシステム保護のログを取得することができます。これらのログを分析することで、不正な組織システムの利用を検出できる可能性があります。

5.2 NIST SP 800-172 要件対応表

ガイドラインの要件に対応するための設定を行う際には、この要件対応表をご活用ください。

NIST SP 800-172 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンターの対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.1 アクセス制御 Enhanced Security Requirements	3.1.1e	Employ dual authorization to execute critical or sensitive system and organizational operations.	本要件は、組織における「重要または機密のシステム」の運用時に二重権限の利用を要求しています。組織は予め「重要または機密のシステム」を識別・定義する必要があります。通常、「重要または機密のシステム」は例えば、銀行の金融システムやインフラの制御システムなどが該当します。組織が定めた「重要または機密のシステム」利用時(特定のコマンド、アクション、または機能実行時)には、本機を含め、二重の権限による承認を要求するように運用する必要があります。例えば、組織は「重要または機密のシステム」のアップデート時に、正管理者・副管理者双方の承認(二重の権限による承認)を得たときのみアップデートを許可するに運用する必要があります。別の例としては、「重要または機密のシステム」の特権コマンド利用時に、二重の権限による承認を要求するように運用する必要があります。	N/A	-	予め「重要(critical)または機密のシステム」を識別・定義してください。「重要または機密のシステム」利用時(特定のコマンド、アクション、または機能実行時)には、二重の権限による承認を要求するように運用する必要があります。そのため、重要もしくは機密のシステムの有無を判断し、存在する場合、当該システムの機能の使用時に二重の権限による認証を実施してください。
	3.1.2e	Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.	本要件は、組織のシステムへのアクセスを、組織が管理するデバイス・システムに限定することを要求しています。本要件の主な責務は、組織側となります。組織は、社内で利用可能なデバイスを管理し、マルウェアに感染したデバイスなどが組織内のシステムに不正にアクセスできないように運用する必要があります。他にも技術的な実現方法として、システムにアクセスするデバイスに対して、デバイス認証を要求するように、デバイス認証機能を実装することでも実現可能です。本機のデバイス認証の方法として、RADIUS認証を用いることができます。	**IEEE 802.1X対応** 本機はIEEE 802.1X認証を導入したネットワークにクライアントとして接続することができます。 IEEE 802.1Xを導入したネットワークに機器を接続して通信を始めようとすると、まずその機器が正しいユーザーであるかどうか確認されます。確認はRADIUSサーバーに問い合わせることで行われ、正しいユーザーであれば認証されます。認証が下りないかぎりLANスイッチ（アクセスポイント）は機器からの通信要求を遮断します。	<IEEE 802.1X設定>を有効にする	本機を含めたシステムへアクセスする主体が組織所有のシステムコンポーネントであることを確認する方法を検討してください。また、本機がシステムへアクセスする場合に組織所有のシステムコンポーネントであることを証明する方法を検討してください。たとえば、デバイス認証を行ったり、機器が持つMACアドレスや、機器に割り当てたIPアドレスで制限を設けたり、RADIUS認証を必須とする方法が考えられます。本機の場合は、RADIUS認証を用いることができます。
	3.1.3e	Employ [Assignment: organization-defined secure information transfer solutions] to control information flows between security domains on connected systems.	本要件は、組織が定義したセキュアな情報転送手段を用い、組織のシステム上のセキュリティードメイン間の情報フローの制御を要求しています。本要件の主な責務は組織側です。組織はまず、本機を含め、 CUI（Controlled Unclassified Information）含むドメインと、CUIを含まないドメインとを識別する必要があります。そして、CUIを含むドメインとCUIを含まないドメインとの間の情報転送に用いる手段も定義します。 例えば、組織は、ファイアウォールを用い CUI を含むドメインと CUI を含まないドメインとに分離します。さらにドメイン間通信として、企業 WAN を介したサイト間 VPN を用い、ドメイン間の情報(CUI)フローを制御します。他にも CUI を保持するファイルサーバーを設け、適切なアクセス制御を行うことでもドメイン分離が可能です。	N/A	-	組織としてセキュアな情報転送手段を定義してください。また、CUIを含むドメインとCUIを含まないドメインを識別してください。CUIドメインから出入りする情報フローをセキュアな情報転送手段によって制御してください。セキュアな情報転送手段としては、VPN、ファイアウォールの使用等が考えられます。
3.2 意識向上と訓練 Enhanced Security Requirements	3.2.1e	Provide awareness training [Assignment: organization-defined frequency] focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training [Assignment: organization-defined frequency] or when there are significant changes to the threat.	本要件は、組織の従業員に対する APT(Advanced Persistent Threat) に関するセキュリティートレーニングの実施を要求しています。本要件の主な責務は組織側です。APT は標的型攻撃の一種であり、より高度で持続的な攻撃でしばしば組織的に行われることがあります。また APT は、通常の標的型攻撃同様、従業員による不審なメール・サイト等の不用意なアクセスが攻撃のきっかけとなる場合が多いです。 例えば、組織は従業員に対し、具体例を交え APT を説明し、さらに APT のきっかけとなりうる不審なメールや不審なサイトを開かないことを本機を含めてすべてのシステムで留意するようにトレーニングをする必要があります。また、APT に関する脅威も日々進化するため、脅威トレンドが変わったり、新たな攻撃手法が出た場合などは、必要に応じてトレーニング内容を更新する必要があります。もしくは、定期的に組織はトレーニング内容を見直し、更新する必要があります。	N/A	-	従業員に対し、APTに対するトレーニングを行って下さい。トレーニングの内容としては、具体例を交えて APT を説明し、APT のきっかけとなりうる不審なメールや不審なサイトを開かないように教育してください。また、脅威トレンドが変わったり、新たな攻撃手法が出た場合、あるいは組織が定めた頻度で定期的にトレーニング内容を見直し、更新してください。トレーニングを行う頻度およびトレーニング内容の見直しを行う頻度を定めてください。
	3.2.2e	Include practical exercises in awareness training for [Assignment: organization-defined roles] that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.	本要件は、組織の従業員に対して、ロール別の実践的な演習を伴うセキュリティートレーニングの実施、及びトレーニング結果に関するフィードバックを従業員及びその上司に提供することを要求しています。本要件の主な責務は組織側です。 例えば、組織は本機を含めたシステムに対するAPTを想定した脅威シナリオを作成し、シナリオに沿って従業員に対して、演習を通じたセキュリティートレーニングを行います。演習では、実際にトレーニング対象となる従業員にメールなどを用いた標的型攻撃を行い、従業員が不審メールを開いてしまった場合の対応等のインシデントレスポンス含め、実体験させることでトレーニングを行います。そして、演習時の各従業員の対応を評価し、フィードバックとして、当該従業員及び上司に共有します。	N/A	-	APTを想定した脅威シナリオを作成し、シナリオに沿って従業員に対し、意識向上のための訓練、例えば、模擬不審メールを従業員に送付する予行演習を行ってください。演習時に各従業員がどう対応したか評価し、結果を従業員とその上司へフィードバックしてください。

NIST SP 800-172 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンターの対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.4 構成管理 Enhanced Security Requirements	3.4.1e	Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.	本要件は、組織が管理するデバイスの構成管理を要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織は、まず組織内のデバイス・システムが具備するコンポーネント(ハードウェア、ソフトウェア、およびファームウェア)のベースライン構成を定義する必要があります。組織内のデバイス・システムの構成を収集し、信頼できるリポジトリ上で管理します。ベースラインの各コンポーネントは、信頼できるソースから取得(ダウンロード)できるように構築する必要があります。 本機は組織側の対応をサポートする機能として、ファームウェア定期アップデート機能を使った自動アップデート機能や、デバイス情報表示機能、インストールしているアプリケーション情報の表示機能を具備しています。	**ファームウェアの定期アップデート** 定期アップデートを設定することにより、本機が定期的に新しいファームウェアをチェックして、自動的にアップデートを行うことができます。 **MEAPアプリケーションの管理** リモートUIのSMSを表示してアプリケーションを管理することができます。	＜定期アップデート設定＞を設定する リモートUIの［Service Management Service］によりアプリケーションを管理する	ユーザーは機器のシステムコンポーネントの情報をもとにベースライン構成を構築し、文書化したうえで管理してください。 ベースライン構成は信頼できるリポジトリで管理する必要があります。 ベースライン構成は定期的にレビューする必要があります。 ベースライン構成に変更が加えられる場合は、変更がセキュリティーに与える影響を分析したうえで、変更の承認が必要となります。 機器のシステムコンポーネントを構築する際には信頼できるソースから取得（ダウンロード）してください。 例えば、本機にファームウェアやアプリケーションをインストールする際には、キヤノン公式のものを使用し、身元が不確かな第三者からのダウンロードは行わないでください。 本機のベースライン構成の構築時には本機のデバイス情報表示機能を用いることによりシステムコンポーネントの情報を得ることができます。
	3.4.2e	Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, [Selection (one or more): remove the components; place the components in a quarantine or remediation network] to facilitate patching, re-configuration, or other mitigations.	本要件は、組織が管理するデバイスの構成管理において、特に定義したベースライン構成と異なるデバイスのコンポーネントの自動修正(是正)を要求しています。例えば、組織は自組織内のデバイス構成を収集・管理するリポジトリ上で、ベースライン構成と異なるデバイス・システムを自動的に検出するようにシステム構築(ツール導入)をします。ベースライン構成と異なるデバイス・システムを検出した場合、手動もしくは自動で、ベースライン構成と一致するように、不要なコンポーネントを削除したり、アップデートパッチを適用したり、設定変更する必要があります。または、ベースライン構成と異なるデバイスによる影響拡大(e.g. マルウェアの感染拡大)を抑制するために、当該デバイスを隔離する必要があります。 本機は不正なコンポーネントを検出した際に自動で当該コンポーネントの動作を停止させる起動時のシステム検証機能およびランタイムシステム保護機能を具備しています。本機能により、組織内の他のシステムに影響を及ぼさないように自動で本機の不正なコンポーネントを隔離(動作停止による切り離し)することができます。	**起動時のシステム検証** 本機に組み込んであるファームウェア、システムやMEAPアプリケーションの完全性を、起動時に検証します。 **ランタイムシステム保護** 本機の稼働中に、ランタイムシステム保護機能を使ってプログラムの不正な改変と不正なプログラムの実行を防止し、システムの信頼性を向上できます。	＜起動時のシステム検証＞を有効にする ＜ランタイムシステム保護＞を有効にする	ユーザーは自動化メカニズムを使用し、誤って構成されたシステム・コンポーネントや不正なシステム・コンポーネントによるベースライン構成からの逸脱を検出してください。 例えば、組織内のデバイス構成を収集・管理するリポジトリ上で、組織内のシステムコンポーネントの情報を自動的に収集・管理するシステムを構築します。収集したデバイスのシステムコンポーネントの情報を組織のリポジトリ内にあるベースライン構成と比較することで、ベースライン構成からの逸脱を検出します。 加えて、ベースライン構成からの逸脱が検出された際のセキュリティーレスポンスを定義する必要があります。 例えば、ベースライン構成にないシステムコンポーネントを検出した際には、不要なシステムコンポーネントを自動的に削除する、あるいは不要なシステムコンポーネントが検出されたことをシステム管理者に通知し、削除を要求するようにレスポンスを定義してください。 ベースライン構成からの逸脱が検出されたデバイスについては、組織内のその他のシステムに影響を及ぼさないよう、デバイスの隔離を実施してください。 本機の起動時のシステム検証機能およびランタイムシステム保護機能を設定することで、本機の不正なコンポーネントの検出と隔離(動作停止による切り離し)を自動で行うことができます。
	3.4.3e	Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components.	本要件は、組織が管理するデバイスの構成管理において、特に自動化された管理ツールを使用し、システムコンポーネントを適切な状態に維持することを要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織は例えば、自動化されたツールを用い、組織が管理するデバイスのコンポーネント情報(e.g. OS バージョン番号)をリポジトリで収集・管理します。利用するコンポーネントに脆弱性が見つかった場合、リポジトリ上のコンポーネント情報を参照し、脆弱性のあるコンポーネントを具備するデバイスに最新パッチを適用するようにスケジューリングします。 本機は組織側の対応をサポートする機能として、ファームウェア定期アップデート機能を使った自動アップデート機能を具備しています。	**ファームウェアの定期アップデート** 定期アップデートを設定することにより、本機が定期的に新しいファームウェアをチェックして、自動的にアップデートを行うことができます。	＜定期アップデート設定＞を設定する	ユーザーは自動化メカニズムを使用し、組織内のシステムコンポーネントの構成を適切な状態に管理してください。 システムコンポーネントは、最新、完全、正確であり、すぐに利用できる状態にある必要があります。 例えば、組織内のデバイス構成を収集・管理するリポジトリ上で、組織内のシステムコンポーネントの情報を自動的に収集・管理するシステムを構築します。 利用するコンポーネントに脆弱性が見つかった場合、リポジトリ上のコンポーネント情報を参照し、脆弱性のあるコンポーネントを備えるデバイスに最新パッチを適用するようにスケジューリングします。 本機のファームウェアに関しては、定期アップデート機能を設定することにより自動的にファームウェアを最新の状態に保つことできます。

NIST SP 800-172 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンターの対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機はキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.5 識別と認証 Enhanced Security Requirements	3.5.1e	Identify and authenticate [Assignment: organization-defined systems and system components] before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant.	本要件は、組織が定義したシステムに対して、ネットワーク接続時にリプレイ耐性のある双方向認証を用い、識別認証することを要求しています。組織は予め本要件を適用するシステムを定義する必要があります。定義したシステムに対して、ネットワーク接続時にTLSによるサーバー・クライアント認証のようなリプレイ攻撃耐性のある認証方法を用い、認証を行う必要があります。また、認証に用いる暗号鍵をTPM(Trusted Platform Module)やTEE(Trusted Execution Environment)などのセキュアな方法を用い、管理する必要があります。組織が本機を本要件の適用システムとして定義した場合、本機のIEEE802.1X 認証を用いることでリプレイ攻撃耐性のある双方向認証で認証された場合にのみ、本機がネットワークに接続できるように制御可能です。また、本機はTPMを具備しており、認証に用いる情報を安全に管理できます。	**IEEE 802.1X対応** 本機はIEEE 802.1X認証を導入したネットワークにクライアントとして接続することができます。 **TPM** 本機に記録されているパスワード、TLS通信用公開鍵ペア、ユーザー証明書などの機密情報を暗号化する暗号鍵（TPM鍵）をTPMチップ内に安全に保管できます。これにより、本機にとって重要な情報の漏えいを抑止できます。	<IEEE 802.1X設定> を有効にする <TPM設定>を設定する	ユーザーは、組織が定義したシステム及びシステムコンポーネントに対して、ネットワーク接続時にリプレイ攻撃に耐性のある双方向認証を採用してください。リプレイ攻撃に耐性のある双方向認証としては、例えばTLSを利用することができます。また、認証に用いる暗号鍵はセキュアなストレージで保護する必要があります。 本機のIEEE802.1X認証機能を設定することで、本機が双方向認証された場合にのみ組織のネットワークに接続できるように設定可能です。本機能を利用する際は、IEEE802.1Xに対応した認証ネットワークの構築が必要です。 また、本機のTPM機能を設定することで、IEEE802.1X認証に用いられる情報を安全に管理できます。
	3.5.2e	Employ automated mechanisms for the generation, protection, rotation, and management of passwords for systems and system components that do not support multifactor authentication or complex account management.	本要件は、多要素認証や複雑なアカウント管理(ユーザーごとに個別のシステムアカウントやログなど)が利用可能でない場合に、パスワードマネージャなどによる自動化されたパスワード管理を要求しています。例えば、パスワードマネージャを用いることで、ユーザーおよびデバイスアカウント用の強力で異なるパスワードが自動的に生成、ローテーション、管理、および格納することができます。ルーターには1人の管理者アカウントがありますが、組織には通常、複数のネットワーク管理者がいます。したがって、複数管理者によりアカウント(パスワード)が使いまわされるため、アクセス管理とアカウンタビリティに問題があります。パスワードマネージャは、自動パスワードローテーション(この例では、ルータのパスワード)などの技術を使用して、一時パスワードをチェックアウトし、そのパスワードを再度チェックインしてアクセスを終了することで、特定のユーザーがデバイスに一時的にアクセスできるようにします。また、パスワードマネージャは同時にこれらの処理をログとして記録します。また、パスワードマネージャは管理するパスワードを強固に保護します。 なお、本機には、多要素認証やユーザー別のアカウント管理・アクセス制御機能が搭載されているため、パスワードマネージャなどのツールを別途使う必要はありません。また、本機にログインしたユーザー毎に本機上での操作をログとしても記録します。	**個人認証管理** 本機を使用するユーザーを認証アプリケーション（ログインサービス）で管理することにより、より高いセキュリティーレベルを保ち、効率的な本機の運用が可能です。	<ユーザー管理>を設定する	ユーザーは組織内のシステムにおいて、ユーザーごとの認証機能といった複雑なアカウント管理や多要素認証が使用できない場合は、以下の機能を満たしたパスワードマネージャなどによる自動化されたパスワード管理を実施してください。 ・ユーザーおよびデバイスアカウント用の強力で異なるパスワードの自動生成、ローテーション、管理、および格納 ・管理するパスワードの強固な保護 本機には多要素認証やユーザー別のアカウント管理・アクセス制御機能が搭載されているため、本機とは別にパスワードマネージャ等を導入する必要ありません。
	3.5.3e	Employ automated or manual/procedural mechanisms to prohibit system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state, or in a trust profile.	本要件は、組織のシステムに接続するシステムコンポーネントに対して、コンポーネントが既知、認証済み、適切な構成、または信頼プロファイル内のいずれでもない場合、システムへの接続を手動もしくは自動で禁止する必要があります。 本機は、 IEEE802.1X に対応しているため、IEEE802.1X 認証を用いることで本機が認証された場合にのみネットワークに接続できるように制御可能です。加えて、 IEEE802.1X により、ネットワーク経由で本機に接続するデバイスに対しても認証されたデバイスのみが本機に接続できるように制御可能です。 また、本機のシステムコンポーネントが適切に構成されているかを検証する機能として、起動時のシステム検証機能およびランタイムシステム保護機能を具備しています。	**IEEE 802.1X対応** 本機はIEEE 802.1X認証を導入したネットワークにクライアントとして接続することができます。 **起動時のシステム検証** 本機に組み込んであるファームウェア、システムやMEAPアプリケーションの完全性を、起動時に検証します。 **ランタイムシステム保護** 本機の稼働中に、ランタイムシステム保護機能を使ってプログラムの不正な改変と不正なプログラムの実行を防止し、システムの信頼性を向上できます。	<IEEE 802.1X設定> を有効にする <起動時のシステム検証>を有効にする <ランタイムシステム保護>を有効にする	ユーザーは組織内のシステムに接続するシステムコンポーネントが既知、認証済み、適切な構成、または信頼プロファイル内のいずれでもない場合、接続を手動あるいは自動で禁止してください。 本機では IEEE802.1X 認証機能を設定することで本機が認証済みの場合にのみ組織のネットワークに接続できるよう設定できます。また IEEE802.1X により、認証されたデバイスのみがネットワーク経由で本機に接続できるように設定できます。 IEEE802.1X認証機能を有効にする際には、IEEE802.1X対応の認証ネットワークの構築が必要です。 ユーザーは、本機を含め組織が管理するデバイスの定義と組織の管理下にあるデバイスのみがネットワークにアクセス可能となるよう認証サーバー（RADIUSサーバー）を設定する必要があります。 また、本機の起動時のシステム検証機能およびランタイムシステム保護を設定することで、本機のシステムコンポーネントが適切に構成されているかを検証することができます。
3.6 インシデント対応 Enhanced Security Requirements	3.6.1e	Establish and maintain a security operations center capability that operates [Assignment: organization-defined time period].	本要件は、セキュリティーオペレーションセンター(SOC)を確立し、組織が定義した期間、SOCを維持・運用することを要求しています。本要件の主な責務は組織側です。組織は本機を含む組織内のシステムやネットワークを(組織が定義した期間中)継続的に監視する SOC を運用する必要があります。SOCは、組織内のセキュリティーインシデントの予兆を検出するために、例えば、組織内のシステムやネットワークのログを継続的に監視・分析します。また、インシデント発生時は、CSIRTを支援するために、ログ分析なども行います。独自のSOCを自組織内に持つ場合もあれば、外部ベンダーのSOCサービスを利用することもあります。	N/A	-	組織内のシステムやネットワークを(組織が定義した期間、例えば24時間365日)継続的に監視し、インシデントの検知を行うセキュリティーオペレーションセンター(SOC)を設置してください。SOCは、組織内のシステムやネットワークのログを継続的に監視・分析します。また、インシデント発生時は、サイバーセキュリティインシデントレスポンスチーム(CSIRT)を支援するために、ログ分析なども行います。
	3.6.2e	Establish and maintain a cyber incident response team that can be deployed by the organization within [Assignment: organization-defined time period].	本要件は、組織が定義した期間内に配備可能なサイバーセキュリティーインシデントレスポンスチーム(CSIRT)の立ち上げ・維持を要求しています。本要件の主な責務は組織側です。組織は常設もしくは定義した期間内に立ち上げ可能なCSIRT体制を確立する必要があります。CSIRTは、組織内のセキュリティーインシデントの評価、文書化、および対応を行う専門家のチームで、本機を含む組織のシステムをインシデントから迅速に回復し、また将来のインシデントを回避するために必要な対応も行う場合があります。	N/A	-	組織が定義した期間内に配備可能な、インシデント対応を行うサイバーセキュリティインシデントレスポンスチーム（CSIRT）を設置してください。CSIRTは、組織内のセキュリティーインシデントの評価、文書化、および対応を行う専門家のチームで、組織のシステムをインシデントから迅速に回復し、また将来のインシデントを回避するために必要な対応も行う場合があります。

NIST SP 800-172 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンターの対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.9 人的セキュリティー Enhanced Security Requirements	3.9.1e	Conduct [Assignment: organization-defined enhanced personnel screening] for individuals and reassess individual positions and access to CUI [Assignment: organization-defined frequency].	本要件は、CUIを含む組織内システムにアクセスする従業員に対する組織定義の強化された人事スクリーニング(審査)、及び組織が定めた頻度での継続的な再審査を要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織は例えば通常の人事審査に加え、CUIセキュリティー保護目的で、追加で(組織で定義した)バックグラウンド審査を行います。人事審査及び再審査では例えば、適用される法律、行政命令、指令、方針、規則、および従業員のCUIアクセスレベルに応じた基準を反映させます。	N/A	-	CUIを含む組織内システムにアクセスする従業員に対して組織定義の強化された人事スクリーニングを実施してください。 一度人事スクリーニングを受けた従業員に対しても組織が定めた頻度で再審査を行い、従業員が必要な人事スクリーニング基準を満たしていることを確認してください。 人事スクリーニングには、例えば、セキュリティー保護を目的として通常の人事審査に加えて追加のバックグラウンド審査が含まれます。 また、人事審査及び再審査時には適用される法律、行政命令、指令、方針、規則、および割り当てられた職階に必要なアクセスのレベルに対して設定された特定の基準を反映させます。
	3.9.2e	Ensure that organizational systems are protected if adverse information develops or is obtained about individuals with access to CUI.	本要件は、CUIにアクセスできる従業員に関して有害な情報がある場合、当該従業員からCUI を保護することを要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織は例えば、CUIを含むシステムに継続的にアクセスする必要があるかどうかが疑問視される従業員に関して有害な情報が発生または得られた場合、有害な情報が解決されるまでの間、CUIを保護するための措置をに直ちにとる必要があります。	N/A		CUIにアクセスできる従業員に関して有害な情報がある場合、当該従業員から CUI を保護してください。 例えば、CUIを含むシステムに継続的にアクセスする必要があるかどうかが疑問視される従業員に関して有害な情報が発生または得られた場合、有害な情報が解決されるまでの間、当該従業員のアクセス権を停止するなどしてCUIを保護してください。
3.11 リスクアセスメント Enhanced Security Requirements	3.11.1e	Employ [Assignment: organization-defined sources of threat intelligence] as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.	本要件は、組織のリスクアセスメントの一部として、脅威インテリジェンスの活用を要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織はリスクアセスメントとして利用する脅威インテリジェンスを検討し、採用する必要があります。	N/A	-	脅威インテリジェンスを入手するために脅威インテリジェンスサービスの利用を検討してください。入手した脅威インテリジェンスに基づいて、システムセキュリティー要件の定義、システムおよびセキュリティーアーキテクチャの開発、セキュリティーソリューションの選択、監視(脅威探索を含む)、および修復作業に活用する仕組みを構築してください。
	3.11.2e	Conduct cyber threat hunting activities [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined event]] to search for indicators of compromise in [Assignment: organization-defined systems] and detect, track, and disrupt threats that evade existing controls.	本要件は、組織が定義したシステムに対する脅威ハンティングの実施を要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織は例えば、組織が定義した頻度、組織が定義したシステムに対して、監査ログを分析したり、脅威インテリジェンスの活用やハニーポットを利用することで、積極的かつ能動的に脅威を検出し、追跡・対策をします。	N/A	-	組織が定義したシステムに対して、侵害の痕跡がないかを確認するサイバー脅威ハンティング活動を実施してください。具体的には、監査ログを分析したり、脅威インテリジェンスの活用やハニーポットを利用することで、積極的かつ能動的に脅威を検出し、追跡・対策をして下さい。サイバー脅威ハンティング活動を行うきっかけになる事象、もしくは実施の頻度を定めてください。
	3.11.3e	Employ advanced automation and analytics capabilities in support of analysts to predict and identify risks to organizations, systems, and system components.	本要件は、組織内のCSIRT・SOCにおけるリスク予測・特定に関して、高度な自動化機能及び分析機能の利用を要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織は例えば、CSIRTやSOCでの膨大なシステムログ・ネットワークログの解析に、外部ベンダーのAI解析ツールを活用することで、効率的に組織のシステムに対するリスク予測・特定が可能となります。	N/A	-	本機を含むシステムのリスクを特定し予測するために高度な自動化機能と分析機能を利用して下さい。例えば、Automated Workflow Operations、Automated Threat Discovery and Response などのソリューションを導入してください。
	3.11.4e	Document or reference in the system security plan the security solution selected, the rationale for the security solution, and the risk determination.	本要件は、組織が選択したセキュリティーソリューション、セキュリティーソリューションの根拠、及びリスク判断について、システムセキュリティー計画に記載または参照することを要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織は例えば、NIST SP 800-18 を参照し、セキュリティーソリューションの説明、根拠、リスク判断を含む形でシステムセキュリティー計画を策定する必要があります。	N/A	-	選択したセキュリティーソリューションとその根拠、及びリスク判断を文書化し、システムセキュリティー計画に含めてください。例えば、セキュリティーソリューションの導入時の契約、システム構成、脅威分析結果、リスクの判断結果を文書化し、システムセキュリティー計画から参照できるようにしてください。

NIST SP 800-172 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンターの対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.11 リスクアセスメント Enhanced Security Requirements	3.11.5e	Assess the effectiveness of security solutions [Assignment: organization-defined frequency] to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.	本要件は、脅威インテリジェンスに基づき、組織が定義した頻度、組織のシステムに対し発生しうるリスクに対抗するためのセキュリティーソリューションの有効性評価を要求しています。本要件の主な責務は組織側です。組織は、例えば、組織のシステムを保護するセキュリティーソリューションを脅威インテリジェンスに基づき定期的に評価し、必要に応じてセキュリティーソリューションを変更する必要があります。	N/A	-	導入したセキュリティーソリューションの効果を測定してください。時間の経過に伴って、新しい攻撃手法や脆弱性が発見される可能性があるため、この測定は頻度を定めて定期的に行ってください。
	3.11.6e	Assess, respond to, and monitor supply chain risks associated with organizational systems and system components.	本要件は、組織のシステム及びそのコンポーネントに関連するサプライチェーンに関して、リスク評価、対応、監視を要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織は、例えば、NIST SP 800-161 を参照し、サプライチェーンリスクを管理する必要があります。	N/A	-	サプライチェーンリスクを特定し、監視してください。サプライチェーンに変更がある場合はリスク評価をやり直してください。
	3.11.7e	Develop a plan for managing supply chain risks associated with organizational systems and system components; update the plan [Assignment: organization-defined frequency].	本要件は、組織のシステム及びそのコンポーネントに関連するサプライチェーンのリスクに関して、リスク管理計画の作成及び更新を要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織は、例えば、NIST SP 800-161 を参照し、サプライチェーンリスクを管理するための計画を策定し、組織が定めたタイミングで更新する必要があります。	N/A	-	サプライチェーンリスクを管理するための計画を更新する頻度を定め、維持管理してください。
3.12 セキュリティーアセスメント Enhanced Security Requirements	3.12.1e	Conduct penetration testing [Assignment: organization-defined frequency], leveraging automated scanning tools and ad hoc tests using human experts.	本要件は、組織が定めた頻度で、組織のシステムやソリューションに対するペネトレーションテスト(侵入テスト)の実施を要求しています。本要件の主な責務は組織側です。組織は、例えば、自動化された脆弱性スキャナや社内外のセキュリティーエキスパート(ペンテスター)によるペネトレーションテストを行い、組織が定めた頻度で本機を含む組織のシステム・ソリューションの脆弱性を評価します。	N/A	-	組織のシステムに対して組織が定めた頻度でペネトレーションテストを実施してください。 ペネトレーションテストでは、組織のシステムの脆弱性の特定や弱点を発見することで、組織のセキュリティー戦略の改善に役立てることができます。 ペネトレーションテストには、自動化された脆弱性スキャンツールのほかに社内のセキュリティーエキスパート（ペンテスター）あるいは信頼できる第三者組織を利用することができます。
3.13 システムと通信の保護 Enhanced Security Requirements	3.13.1e	Create diversity in [Assignment: organization-defined system components] to reduce the extent of malicious code propagation.	本要件は、組織が定めたシステムコンポーネントに対して、多様性を持たせ、悪意のあるコードの伝搬を低減することを要求しています。組織は最初に、本要件の対象となるシステムコンポーネントを定める必要があります。また、多様性を持たせる方法としては、例えば、複数ベンダーのウイルス検知ソフトを利用したり、複数OSの採用、ASLRによるアドレス空間のランダム化などが挙げられます。 本機は、悪意のあるコードの伝搬を低減するためにASLRによるアドレス空間ランダム化機能を具備しているため、本機を本要件の対象システムに定めた場合でも、要件を満たすことが可能です。加えて、複数OS搭載による多様性も備えています。	**ASLR** アドレス空間ランダム化機能	N/A	悪意のあるコードの伝播を防ぐために、組織が定義したシステムコンポーネントを多様化してください。 システムコンポーネントを多様化することにより、特定のシステムコンポーネントに対して成功した攻撃が、他のシステムコンポーネントに対しても同様に成功する可能性を低減させることができます。 例えば、複数のベンダのセキュリティー製品（ウィルス検知ソフトなど）を組織内のシステムに導入することでシステムコンポーネントの多様化が可能です。これにより、あるベンダのセキュリティー製品の脆弱性を利用した攻撃が成功しても、攻撃の影響範囲は当該ベンダの製品が防御している範囲にとどまり、他のベンダの製品が防御しているシステムコンポーネントに影響が出る可能性を低減することができます。 本機は、多様性を持たせる手段としてASLRによるアドレス空間のランダム化機能を備えており、特定のシステムコンポーネントに対する攻撃が成功したとしても、その攻撃が他にシステムコンポーネントに対して同様に成功する可能性を低減させています。 加えて本機は複数OS搭載による多様性も備えています。
	3.13.2e	Implement the following changes to organizational systems and system components to introduce a degree of unpredictability into operations: [Assignment: organization-defined changes and frequency of changes by system and system component].	本要件は、組織のシステムとシステムコンポーネントに対する攻撃インターフェイス(attack surface)のランダム化を要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織は、攻撃者による継続的な攻撃を困難にするために、例えば、外部公開しているシステムのIPアドレス、DNS名をランダムなタイミングで変更します。	N/A	-	ユーザーは攻撃のインターフェースとなりうるシステムに対して組織定義のランダムな要素を取り入れてください。 ランダムな要素を取り入れることで攻撃者がシステムを攻撃する際に、攻撃インターフェースに対する予測を立てることを妨害し、攻撃の計画と実行に対して影響を与えることができます。 例えば、時刻要素をランダム化する要素とした場合、本機のIPアドレスやDNS名をランダムなタイミング(時刻)で変更したり、クレデンシャルの有効期間をランダムに短縮します。また、利用するブラウザーや検索エンジンをランダムなタイミングで変更したり、組織の職員の役割を交換することも有効です。
	3.13.3e	Employ [Assignment: organization-defined technical and procedural means] to confuse and mislead adversaries.	本要件は、技術的・手続き的な手段を用い、攻撃者を混乱・誤解させることを要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織は、例えば、ハニーポットを用い、攻撃者に偽の攻撃ターゲット(おとり)を与えたり、意図的に偽の情報を取得させることで、攻撃者を混乱・誤解させます。	N/A	-	ユーザーは組織内のシステムに対して、攻撃者を混乱・誤解させるための組織が定義した技術的・手続き的要素を導入してください。 このような要素を導入することで、攻撃の遅延や攻撃の影響範囲の低下、あるいは情報漏洩に対する対策を行うことができます。 例えば、組織内のシステム内にハニーポットを設置することで攻撃者を偽のターゲットへ誘導する、組織内で扱うデータに対して意図時に偽の情報を埋め込むといった対策を実施します。

NIST SP 800-172 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンターの対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.13 システムと通信の保護 Enhanced Security Requirements	3.13.4e	Employ [Selection: (one or more): [Assignment: organization-defined physical isolation techniques]; [Assignment: organization-defined logical isolation techniques]] in organizational systems and system components.	本要件は、1つもしくは複数の「組織が定義した物理的な隔離技術」または/かつ「組織が定義した論理的な隔離技術」により、組織のシステム及びシステムコンポーネント内のCUIを保護することを要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織はシステムを保護するための物理的もしくは/かつ論理的な隔離方法を定義する必要があります。論理的な隔離方法の例としては、例えば、CUIデータへのタグ付け、DRM、VLAN などがあります。物理的な隔離方法の例としては、例えば、入室管理された部屋への CUI データサーバー(ネットワーク非接続)の配置などがあります。	N/A	-	ユーザーは組織内のシステムあるいはシステムコンポーネントに対して組織が定義した物理的・論理的分離技術を採用することで、CUIを含む情報を保護してください。 分離技術を採用することで、CUIを扱うシステムコンポーネントに対する追加のセキュリティー対策の実施やCUIの情報フローを制限することができます。 論理的な分離技術として、例えば、CUIデータへのタグ付け、DRMによるCUIの監視とフローの制限や仮想マシン・VLANによるホスト上でのCUIの分離などがあります。 物理的な分離技術として、例えば、入室管理された部屋への CUI データサーバー(ネットワーク非接続)の配置などがあります。
	3.13.5e	Distribute and relocate the following system functions or resources [Assignment: organization-defined frequency]: [Assignment: organization-defined system functions or resources].	本要件は、組織が定義したシステム機能やリソースについて、処理の分散や定期的な再配置を要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織は例えば、IPアドレス、DNS名、ネットワークトポロジーの定期的な変更やフラグメンテーションを実施します。	N/A	-	ユーザーは組織が定義したシステム機能やリソースについて、処理の分散や組織が定義した頻度での再配置を実施してください。 処理の分散やリソースの再配置により、攻撃者が攻撃目標を設定することを困難にしたり、データ侵害を局所化することができます。 例えば、IPアドレス、DNS名あるいはネットワークトポロジーを定期的に変更することで攻撃者の攻撃目標設定を阻害する、フラグメンテーションを行うことでデータ処理を分散させ、データ全体が侵害されることを防ぐことができます。
3.14 システムと情報の完全性 Enhanced Security Requirements	3.14.1e	Verify the integrity of [Assignment: organization-defined security critical or essential software] using root of trust mechanisms or cryptographic signatures.	本要件は、Root of Trust(RoT) またはデジタル署名を用い、組織が定義したセキュリティー上重要または必須のソフトウェアの完全性検証を要求しています。組織は、最初にセキュリティー上重要又は必須のソフトウェアを定める必要があります。セキュリティー上重要又は必須のソフトウェアの完全性を検証する方法としては、例えば、セキュアブートがあります。 本機は、起動時に、Root of Trust に基づくデジタル署名検証によってファームウェアおよびアプリケーションの完全性を検証する起動時システム検証機能を具備しています。また、本機は、稼働中に、Root of Trustに基づくソフトウェアによってプログラムの不正な改変と不正なプログラムの実行を防止する稼働時システム保護機能を具備しています。さらには、本機は、ファームウェアやアプリケーションインストール時にデジタル署名検証することによって、正規のソフトウェアのみインストールするよう制限しています。	**起動時のシステム検証** 本機に組み込んであるファームウェア、システムやMEAPアプリケーションの完全性を、起動時に検証します。 **ランタイムシステム保護** 本機の稼働中に、ランタイムシステム保護機能を使ってプログラムの不正な改変と不正なプログラムの実行を防止し、システムの信頼性を向上できます。	＜起動時のシステム検証＞を有効にする ＜ランタイムシステム保護＞を有効にする	ユーザーは、Root of Trustに基づく信頼メカニズムまたはデジタル署名を利用して、組織が定義したセキュリティー上重要または必須のソフトウェアの完全性を検証してください。そのためには、まず、組織内システムの中で、セキュリティー上重要なソフトウェアを定義する必要があります。次に、定義したソフトウェアごとに、完全性を検証する方法を検討する必要があります。 本機は、MEAPアプリケーションのインストール時、ファームウェアのアップデート時にデジタル署名で検証することで、正規のソフトウェアだけをインストールすることができます。また、本機に組み込まれているソフトウェアを保護するために、起動時のシステム検証、ランタイムシステム保護の機能を具備しています。これらの機能を有効化してください。
	3.14.2e	Monitor organizational systems and system components on an ongoing basis for anomalous or suspicious behavior.	本要件は、組織のシステム及びシステムコンポーネントに関して、異常または疑わしい振る舞いを継続的に監視することを要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織は、例えば、市販のUEBA(User and Entity Behavior Analytics)ツールを使い、AI・機械学習により組織のシステム内の異常または疑わしい振る舞いを監視します。	N/A	-	ユーザーは、組織のシステム及びシステムコンポーネントに関して、異常または疑わしい振る舞いを継続的に監視してください。そのためには、まず、組織内システムの中で、監視対象とすべきシステムおよびシステムコンポーネントを識別する必要があります。次に、識別した対象ごとに、ふるまいを監視する方法を検討する必要があります。
	3.14.3e	Ensure that [Assignment: organization-defined systems and system components] are included in the scope of the specified enhanced security requirements or are segregated in purpose-specific networks.	本要件は、組織が定義したシステム及びシステムコンポーネントが、指定の強化されたセキュリティー要件の範囲に含まれているか、または目的に特化したネットワークに分離されていることの確認を要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織は、例えば、組織のシステムが具備する機能や設定が NIST SP 800-172 の強化されたセキュリティー要件を満たしているか確認します。NIST SP 800-172 の要件を満たさないシステムに対しては、インターネット非接続などのネットワーク分離・隔離により攻撃を受けにくい環境となっているかを確認します。	N/A	-	ユーザーは、組織が定義したシステム及びシステムコンポーネントが、指定の強化されたセキュリティー要件の範囲に含まれているか、または目的に特化したネットワークに分離されていることを確認してください。暗号化、認証、アクセス制御等による隔離によってスコープを定義することができ、この定義したスコープで考察できます。
	3.14.4e	Refresh [Assignment: organization-defined systems and system components] from a known, trusted state [Assignment: organization-defined frequency].	本要件は、組織が定義した頻度で、組織が定義したシステム及びシステムコンポーネントを既知の信頼された状態にリフレッシュすることを要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織は、最初に本要件の適用対象とするシステム及びシステムコンポーネントの定義、及びリフレッシュする頻度を定義する必要があります。組織は、例えば、リポジトリなどに保持してあるシステム及びシステムコンポーネントの正常なイメージを用い、組織が定義した頻度で、対象システム及びシステムコンポーネントをリフレッシュする(更新、元に戻す)必要があります。リポジトリ側の信頼性、完全性も定期的に検証する必要があります。これにより、APTによる攻撃の影響や拡散を抑制することができます。 本機は組織側の対応をサポートする機能として、ファームウェア定期アップデート機能を使った自動アップデート機能を具備しています。	**ファームウェアの定期アップデート** 定期アップデートを設定することにより、本機が定期的に新しいファームウェアをチェックして、自動的にアップデートを行うことができます。	＜定期アップデート設定＞を設定する	ユーザーは、組織が定義した頻度で、組織が定義したシステム及びシステムコンポーネントを既知の信頼された状態にリフレッシュしてください。そのためには、まず、組織内システムの中で、対象とすべきシステムおよびシステムコンポーネントを識別する必要があります。次に、それぞれに対応したリフレッシュの頻度を決定する必要があります。 本機はファームウェア定期アップデート機能を具備しており、ファームウェア更新を自動化することができます。
	3.14.5e	Conduct reviews of persistent organizational storage locations [Assignment: organization-defined frequency] and remove CUI that is no longer needed.	本要件は、組織が定義した頻度で組織内の永続的な保存場所(ストレージ)を確認し、不要となったCUIの削除を要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織は、最初に永続的なストレージを確認する頻度を定義する必要があります。組織は、例えば、HDDなどの永続的なストレージに保持してある CUI を組織が定義した頻度で確認し、不要で利用しない CUI は削除します。現在は使わないが、将来使う可能性のあるもしくは保持する必要のある CUI は、オフラインのストレージで保管するようにすることで、オンラインでの不正アクセスの脅威から保護します。	N/A	-	ユーザーは、組織が定義した頻度で組織内の永続的な保存場所(ストレージ)を確認し、不要となったCUIを削除してください。そのためには、対象とすべき保存場所ごとに、確認する頻度を決定する必要があります。

NIST SP 800-172 要件			キヤノン複合機/プリンターと要件の関連について	キヤノン複合機/プリンターの対応		組織(ユーザー)側の対応
ファミリー	ID	要件	要件の概要と、対応する複合機/プリンターの機能を記載しています。本機とはキヤノン複合機/プリンターを示します。本機が要件に直接関連しない場合でも、本機の機能がお客様の組織側で必要な対応をサポート可能であればその機能を記載しています。	関連する機能 要件に関連するキヤノン複合機/プリンターの機能を記載しています。組織の対応をサポートする機能を含みます。 複合機/プリンターが関連しない要件の場合、「N/A」と記載しています。	対応する設定 関連機能を利用するために必要な設定を記載しています。	要件を満たすためにお客様の組織側で必要な対応を記載しています。本機とはキヤノン複合機/プリンターを示します。ここで記載の内容は対応例であり、これに限るものではありません。
3.14 システムと情報の完全性 Enhanced Security Requirements	3.14.6e	Use threat indicator information and effective mitigations obtained from [Assignment: organization-defined external organizations] to guide and inform intrusion detection and threat hunting.	本要件は、侵入検知及び脅威ハンティングを行う際に、組織が定義した外部組織から得られた脅威インディケーター情報と効果的な緩和策の利用を要求しています。本要件の主な責務は組織側であり、本機は対象外です。組織はまず、脅威情報(脅威の詳細や、対策・緩和策含む)の情報ソースとなる外部組織(e.g. JPCERT, US-CERT, CERT/CC)を定義する必要があります。組織は、例えば、JPCERT から脅威に関する情報を取得し、SOC(セキュリティーオペレーションセンター) による組織内システムに対する侵入検知・脅威ハンティングに活用します。	N/A	-	ユーザーは、侵入検知及び脅威ハンティングを行う際に、組織が定義した外部組織から得られた脅威インディケーター情報と効果的な緩和策の利用してください。
	3.14.7e	Verify the correctness of [Assignment: organization-defined security critical or essential software, firmware, and hardware components] using [Assignment: organization-defined verification methods or techniques].	本要件は、組織が定義した検証方法または手法を使用して、組織が定義したセキュリティー上重要または必須のソフトウェアが正しいことを検証することを要求しています。組織は、最初にセキュリティー上重要または必須のソフトウェアの定義、及び定義したソフトウェアが正しいことを検証するための方法を定義する必要があります。定義したセキュリティー上重要又は必須のソフトウェアが内製の場合は、組織側で定義した検証方法を用い内製ソフトウェアが正しいことを検証する必要があります。外製の場合は、外部ベンダーに本要件が課せられます。ただし、NIST SP 800-172 の Discussion に記載の通り、ソフトウェアの正しさの検証は一般に時間がかかり、ほとんどの商用オペレーティングシステムおよびアプリケーションでは採用されていません。したがって、暗号プロトコルの検証など、非常に限られた用途にしか適用されない可能性があります。 本機は、セキュリティー上重要な暗号モジュールとして、FIPS140 認証を取得した暗号モジュールを利用しています。これらの暗号モジュールは、暗号アルゴリズムの実装の正しさ等を第三者試験機関でテストされ、FIPS140 認証されています。また、本機は、複合機・プリンターのセキュリティー標準である IEEE 2600 に準拠したセキュリティー機能に対して第三者機関で評価され、ISO/IEC 15408 (Common Criteria) 認証を取得しています。	**FIPS140-2準拠** 本機は、TLS暗闇化通信やIPSec通信、ストレージデータ暗号化機能で用いる暗号技術は、米国連邦政府が策定した情報処理標準規格FIPS140-2 Level2準拠の暗号アルゴリズムを利用することが可能です。 **ISO/IEC 15408 (Common Criteria) 認証** 本機は複合機やプリンターの情報セキュリティーに関する国際的な規格「IEEE Std 2600TM-2008（IEEE 2600）」に準拠しています。また、IEEE 2600 に準拠したセキュリティー機能に対して第三者機関で評価され、ISO/IEC 15408 (Common Criteria) 認証を取得しています。	N/A	ユーザーは、組織が定義した検証方法または手法を使用して、組織が定義したセキュリティー上重要または必須のソフトウェアが正しいことを検証してください。本機の場合、内蔵している暗号モジュールに対する FIPS140 認証、および本機に対する ISO/IEC 15408 (Common Criteria) 認証の利用が想定されます。 本機は FIPS140 認証済みの暗号モジュールを利用しており、本体においても、IEEE 2600 に準拠した ISO/IEC 15408 (Common Criteria) 認証を取得しています。

免責事項

- 本ドキュメントに記載されている情報は、作成時に入手可能な最新の情報に基づいています。
- キヤノン株式会社は、ここに定める場合を除き、市場性、商品性、特定使用目的の適合性、または特許権の非侵害性に対する保証を含め、明示的または暗示的にかかわらず本書に関していかなる種類の保証を負うものではありません。キヤノン株式会社は、直接的、間接的、または結果的に生じたいかなる自然の損害、あるいは本書をご利用になったことにより生じたいかなる損害または費用についても、責任を負うものではありません。
- 本ドキュメントの内容は予告なく変更することがありますのでご了承ください。

規制に関する免責事項

- 本ドキュメントの内容は、キヤノンの見解であり、お客様またはキヤノンのパートナーに対する法的アドバイスではありません。キヤノンは、法律顧問やコンプライアンスコンサルタントの提供を行っていないからです。お客様は、規制および法令の遵守に対する特定のソリューションの適合性を判断するために、それぞれ有資格の弁護士に依頼する必要があります。

商標

- 「MEAP」は、キヤノンの複合機ならびにプリンターに搭載された「アプリケーションプラットフォーム」についてのキヤノン株式会社の商標です。