KPAX

Security Notes

株式会社 COSY　　2025 年 06 月日

Revision History

Date	Version	Description	Author
2023/12/19	<1.0>	KPAX 1.0	Azam
2025/06/12	<2.0>	KPAX 2.0	Azam

目次

1 ソフトウェア概要

1.1 ソフトウェアの概要

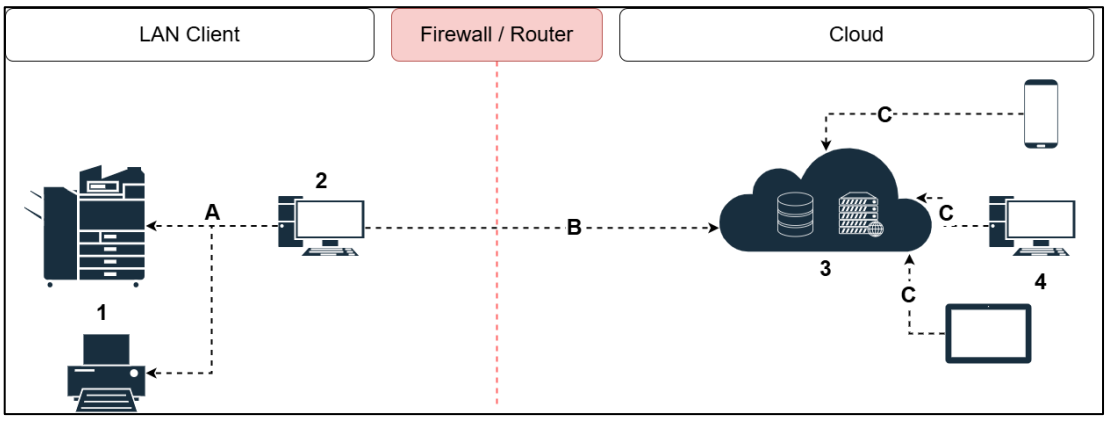
KPAX は、組織内に点在する複数ベンダー製のプリントデバイスを一元的に監視するクラウドベースのシステムです。KPAX は多階層の管理システムをサポートしており、これにより本部組織が支部組織を管理できるようになっています。支部は自組織およびその下位の組織のみを管理できます。

本システムは任意のウェブブラウザからアクセス可能です。システムへのアクセスには、サインインのためのアカウントが必要です。アカウント登録は、既存の登録ユーザーからのメールによる招待を通じてのみ行うことが可能です。各ユーザーには、KPAX の機能や管理可能な組織・オフィスに対するアクセス権限レベルが設定されています。

システムはプリントデバイスに関する情報のみを収集・表示します。たとえば、機器の識別情報（IPアドレス、シリアル番号、MACアドレス）、機器の稼働状況メーター（印刷、コピー、FAX、スキャン）、消耗品および保守部品（インク、ドラム、転写ベルト、定着ユニット）、および機器からのアラートメッセージなどです。

これらのデバイス情報は、「データ収集エージェント」と呼ばれるソフトウェアによって収集されます。これは、プリンティングデバイスにアクセス可能なサーバーや端末にインストールされます。
データ収集エージェントは、機器のメモリ内に情報が存在するまでは何も収集できません。印刷ジョブの内容やユーザー情報などは一切収集されません。

1.2 技術アーキテクチャ図



図表 1. KPAX ネットワークアーキテクチャ図

1. ネットワークプリントデバイス

要件:

-SNMP V1, V2, または V3 がプリンタデバイスにて有効であること

-データ収集エージェントがインストールされた端末からアクセス可能であること

A. データ収集エージェントとネットワークプリントデバイス間の通信

- Port 161 , 162 | SNMP | UDP | データ収集

- Port 80 | HTTP | TCP | デバイスの Web ページへの問い合わせ（SNMP では不十分な場合）

- Port 443 | HTTPS | TCP | デバイスの Web ページへの問い合わせ（SNMP では不十分な場合）

- Port 47545 SNMP | UDP | Canon デバイス向けの追加ポート

- Port 範囲 40000 ~ 60000 | UDP | ポート 47545 への問い合わせに対する応答用

2. KPAX データ収集エージェント

要件:

-対応 OS：Windows Server 2012、2016、2019、2022、Windows 10 バージョン 1607（Enterprise）、または Windows 11

- .Net framework 4.6.2 および.Net 8 Installed (必要に応じてインストーラーが自動インストール)

- インストール時に管理者権限のアカウントが必要

- ネットワーク接続が必要

B. KPAX エージェントとクラウドサーバー間の安全な通信

- Port 443 | HTTPS

3. KPAX サーバー

KPAX サーバーは Microsoft Azure クラウド上にホストされています。デフォルトのホスティング地域はフランスですが、管理するデバイスの規模に応じて、フランス以外の地域でもホスティングが可能です。現在、以下の地域にもホスティングされています：イギリス、アメリカ、カナダ、南アフリカ、インド。

C. KPAX サーバーとクライアントデバイス間の安全な通信

- Port 443 | HTTPS

2　データ収集エージェントのセキュリティに関する注意事項

2.1 データ収集エージェントの概要

KPAX が提供するデータ収集エージェントは、印刷システムに到達可能な Windows 環境（推奨：サーバーまたはユーザーのワークステーション）にインストールされるソフトウェアです。このエージェントは Windows®サービスとして実行され、ユーザーがログインしていなくても、24 時間 365 日動作可能です。定期的かつ設定された間隔で、サービスは印刷状態（IP アドレス範囲、固定 IP、ホスト名によって定義）をスキャンし、一般情報、カウンター、インク残量、消耗部品、アラート/LCD パネルメッセージなどを収集します。

2.2 情報の収集および送信方法

データ収集エージェントは、SNMP、ICMP、HTTP、HTTPS の各プロトコルを使用して印刷システムから情報を収集します。収集されたデータは HTTPS（ポート 443）を通じて KPAX クラウドサーバーへ送信されます。クラウドサーバーで使用される SSL 証明書は、4096 ビットの RSA 鍵を使用し、証明書の有効期間は最大 90 日間で、60 日ごとに自動更新されます。

エージェントは、プリントデバイスの管理に有用かつ必要な情報のみを収集します。デバイスのメモリに情報が存在するまで、収集は行われません。**印刷ジョブに関する情報やユーザーデータは一切収集されません。**より安全な接続のために、SNMP コミュニティ名の変更または SNMP バージョン 3 の使用が推奨されます。

2.3 収集される情報

- デバイスの識別情報:
  - メーカー
  - モデル
  - シリアル番号
  - IP アドレス
  - ネットワーク名
- デバイスのハードウェア機能情報:
  - Typology (複合機、プリンターなど)
  - Technology (レーザー、インクジェットなど)
  - カラー対応 (カラー/モノクロ)
  - 両面印刷対応
  - 設置日付
  - ファームウェア

- 消耗品および保守部品(トナー、ドラム、ベルトなど)

- デバイスのカウンター情報:
  - メインカウンター (総印刷枚数、カラー、モノクロ)
  - 高度なカウンター(印刷、コピー、スキャン、FAX、A3、A4、両面など)
  - メーカー独自のカウンター
- デバイスの技術的ステータス:
  - LCD モニターの状態(印刷準備完了、スリープなど).
  - アラートメッセージ(用紙切れ、トナー残量低下、紙詰まりなど).

2.4 オプションのリモートアップデート

データ収集エージェントには、オプションの自動アップデート機能があります。この機能は、定期的に新しいバージョンのソフトウェアがあるかをチェックします。

2.5 ネットワークトラフィック

KPAX エージェントによって発生するネットワークトラフィックは非常に少量であり、ネットワーク上で分析される IP アドレスの数によって変動します。以下の表は、一般的な Web ページ（例：google.com）の読み込みと比較した場合のおおよその通信量を示しています。

Event	Size (Approximate Value)
標準的な **Web** ページの読み込み（例：**google.com**）	約 35 ko(kb)
スキャンは実行されたが、**IP** アドレスが分析されなかった場合	約 1 ko(kb)
フルスキャン（**8** 台のデバイス）	約 4 ko(kb)
カウンタースキャン（**8** 台のデバイス）	約 3 ko(kb)
消耗品スキャン（**8** 台のデバイス）	約 1 ko(kb)
メンテナンス部品スキャン（**8** 台のデバイス）	約 2 ko ~ 4 ko
アラートスキャン（**8** 台のデバイス）	約 2 ko(kb)

3 セキュリティ関連のよくある質問

3.1 KPAX セキュリティ概要

--ソフトウェア: すべての KPAX アプリケーションはデジタル署名されており、VirusTotal でスキャンされています。

--Web Stack: 脆弱性情報（CVE）は社内ツールで毎日確認されています。

--ネットワーク: すべての通信は TLS 1.2 で暗号化されています。

--クラウドサーバー: KPAX は Microsoft Azure 上でホストされています。Azure のデータセンターは ISO/IEC 27001、SOC 1、SOC 2、SOC 3 の認証を取得しています。

3.2 KPAX 製品のセキュリティ監査プロセス

KPAX は、製品とシステムのセキュリティ確保のため、専門のサイバーセキュリティ企業と緊密に連携しています。この企業は以下のような主要な対応を実施しています：

- **Penetration Testing (侵入テスト):** KPAX ソフトウェア（データ収集エージェント）に対して、脆弱性を特定・修正するための詳細な侵入テストが実施されています。
- **インフラセキュリティ監査:** ネットワークインフラ、サーバー、ワークステーションを対象とした、包括的な IT インフラ監査が行われました。
- **脆弱性スキャン:** 自動化ツールを用いて KPAX ソフトウェアの脆弱性を定期的にスキャンしており、CVE データベースで毎日更新されています。
- **Training & Support:** KPAX チームは、フィッシングなどのサイバー攻撃やセキュリティ対策のベストプラクティスについて、サイバーセキュリティ企業から定期的にトレーニングを受けています。

この連携により、KPAX はサイバー脅威に対する防御を継続的に強化し、高いセキュリティレベルを維持しています。

3.3 KPAX の情報セキュリティプロセスに関連する証明書

現時点では、KPAX 自体は ISO や SOC 認証を取得していません。代わりに、ホスティングプロバイダーである Microsoft Azure のセキュリティ保証に依存しています。Microsoft Azure は、ISO 27001、SOC 1、SOC 2、SOC 3 の認証を取得しており、これによりデータ保護、ネットワークセキュリティ、アクセス制御において、業界標準のセキュリティ管理が確保されています。