

Epson Cloud Solution PORT

セキュリティー ガイドライン

目次

セキュリティへの取り組み.....3

セキュリティ方針.....	3
セキュリティの取り組み	4
データセンター	4
お客様データの保護.....	4

Epson Cloud Solution PORT.....5

概要と用語.....	5
------------	---

データ収集.....6

ネットワークプロトコル.....	6
収集・送信データ.....	6
セキュリティ	6

データ送信.....7

ネットワークプロトコル.....	7
データフォーマット	7
セキュリティ	7

リモート操作.....8

ネットワークプロトコル.....	8
リモート操作の種類.....	8
対象のデバイス	8
セキュリティ	9

ユーザー管理.....10

ネットワークプロトコル.....	10
------------------	----

ユーザー情報.....	10
セキュリティ	10

データストレージ.....11

セキュリティ	11
--------------	----

付録.....12

送信データ	12
ネットワークプロトコルと使用ポート	13
SSL.....	14
商標	14

セキュリティへの取り組み

セキュリティ方針

エプソンは、「経営理念」に基づく「企業行動原則」にのっとり、情報セキュリティの基本姿勢と遵守すべき内容を「情報セキュリティ基本方針」として定めました。グループを構成する一人一人が情報セキュリティの重要性を認識し、実践できるガバナンスと企業風土を造り上げて、社会やお客様、ビジネスパートナー様から信頼される企業であり続けます。

1. エプソンは、企業活動に活用する全ての情報^(*)を重要な経営資源と認識し、情報セキュリティの取り組みを経営の重要な活動の一つに位置付けます。
(*)お客様の個人情報、営業、製品、技術、生産、ノウハウ等の営業秘密情報を対象にします。また、こうした情報を保管、活用する情報システムも含みます。
2. エプソンは、グローバルで共通の情報セキュリティポリシーを定めて、情報セキュリティの責任体制と推進体制を明確にし、情報資産を適正に保護、管理できるマネージメントシステムを構築します。
3. エプソンは、お客様を始めとするステークホルダーの皆様の信頼に応えるため、企業活動にかかわる情報セキュリティのリスクを的確に把握、管理し、事業の継続性確保に努めます。
4. エプソンは、役員を始めとする全ての従業員に対し、継続的な教育や啓発を行い、情報セキュリティをグループ全員に定着させます。
5. エプソンは、情報セキュリティに関する法令、契約、その他関連法規の遵守のためにコンプライアンスプログラムを整備し、その徹底を図ります。
6. エプソンは、経営の責任として、情報セキュリティのマネージメントシステムを評価し、継続的に改善します。

セキュリティの取り組み

エプソンでは、お客様に製品やサービスを安全に安心してお使いいただくために、以下のセキュリティを確保する取り組みをしています。

1. 製品やサービスのセキュリティの確保を品質の根幹と捉えています。
 - ・商品のライフサイクル（企画からお客様のご利用終了まで）において、セキュリティの確保を考慮した製品やサービスづくりを行っています。
2. お客様に対して、セキュリティに関する情報提供や啓発を積極的に行っています。
3. ぜい弱性への対応を継続して行っています。
 - ・業界標準ツールによるぜい弱性試験を実施し、ぜい弱性のない製品やサービスを提供することに努めています。
 - ・未知のぜい弱性が見つかった場合は、速やかに分析を行って情報や対策を提供します。

データセンター

エプソンでは、世界的なセキュリティ基準や標準を満たしているサービスプロバイダーを利用しています。Epson Cloud Solution PORT では Amazon Web Services（アマゾン ウェブ サービス、以下 AWS）を利用しています。

お客様データの保護

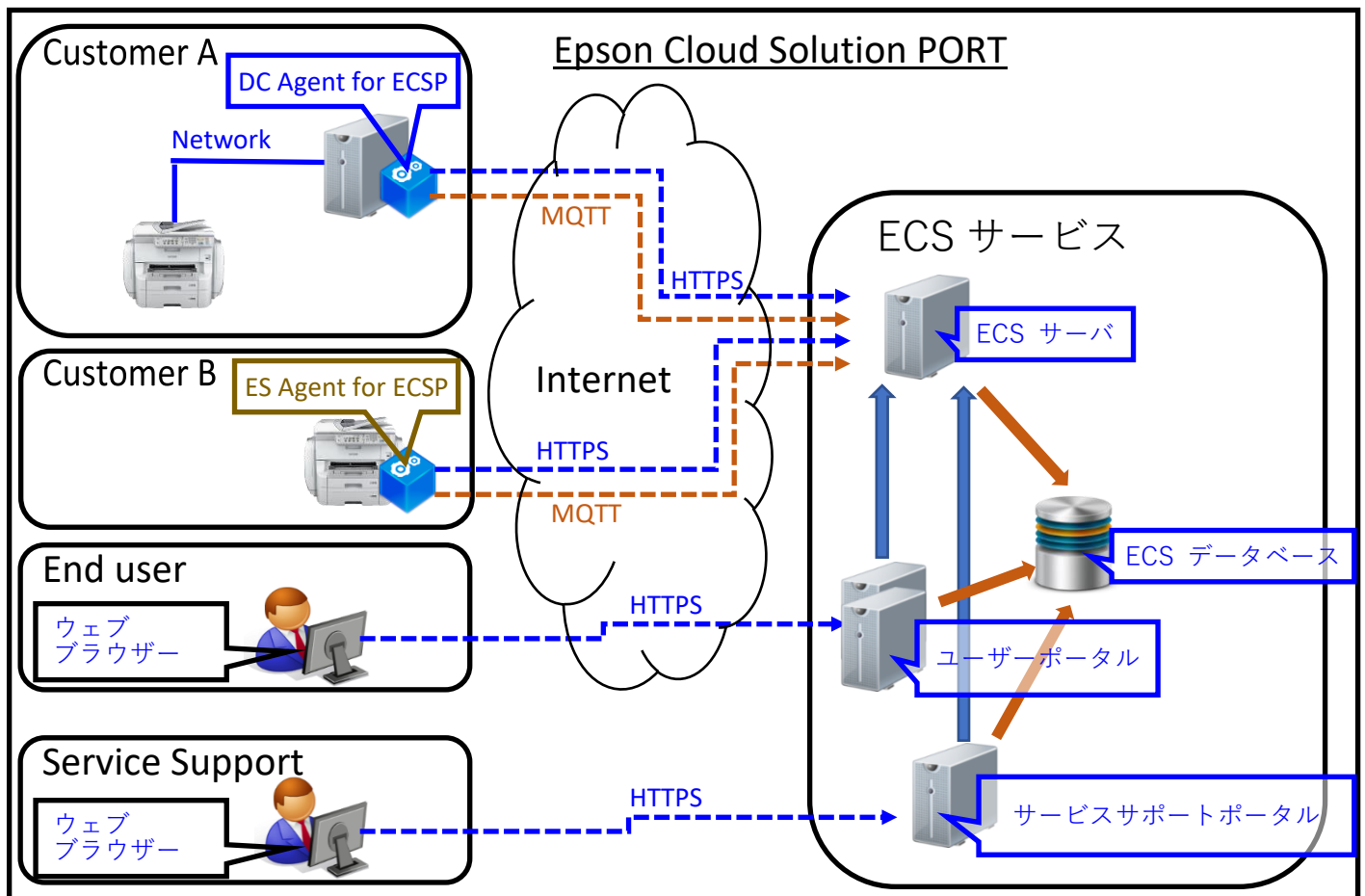
エプソンでは、以下の取り組みによってお客様からの情報のセキュリティを確保しています。

1. デバイスやパソコンとサーバー間の通信は暗号化されています。第三者によるデータの盗聴やデータの改ざんからお客様のデータを守ります。
2. お客様のデータを以下の組み合わせで運用しています。これによってデータを不正アクセスから守ります。
 - ・プライベートなクラウド環境（Virtual Private Cloud）で扱う
3. サーバーへの不正なアクセスを常に監視しています。脅威に対し即座に対応を行います。
4. プライバシースタートメントにより個人情報保護の方針を定めています。
「収集する情報」、「利用の目的と範囲」、「情報の管理方法」などを明確にしており、お客様本人の同意がなければ個人情報を第三者に提供しません。
5. お客様のデータへアクセスできるのは、特別な権限をもつ限られた者であり、かつデータへのアクセスは全て記録させます。また、このアクセス権は定期的に棚卸を実施し、適切な状態を維持しています。

Epson Cloud Solution PORT

概要と用語

Epson Cloud Solution PORT（エプソンクラウドソリューションポート、以下 ECS）は、エプソン製デバイスを管理し、さまざまなサービスを提供します。ECS は、Epson DC Agent for ECSP（エプソンデーシーエージェントフォーエプソンクラウドソリューションポート、以下 DC Agent for ECSP）、Epson ES Agent for ECSP（エプソンプリンターエージェントフォーエプソンクラウドソリューションポート、以下 ES Agent for ECSP）、ECS サーバー、ウェブサイト（ユーザーポータル、サービスサポート）、および ECS データベースで構成されています。詳細は以下をご覧ください。なお、このドキュメントでは、ECS のセキュリティーに関する情報を提供します。



DC Agent for ECSP は、指定されたネットワーク接続デバイスからデバイスデータを収集し、ECS サーバーに送信する Windows クライアントのアプリケーションです。

ES Agent for ECSP はデバイスのファームウェアです。自らデバイスデータを収集して ECS サーバーに送信し

ます。

ECS サーバーは、DC Agent for ECSP や ES Agent for ECSP が送信したデータを受信し、ECS データベースにデータを保存します。

ユーザーポータル、サービスサポートポータルは、「Epson Cloud Solution PORT 会員サービス」「Epson Remote Monitoring System」で提供されるウェブサイトで、承認されたユーザーがログインできます。ユーザーポータルでは ECS データベースに保存されたデータを表示できます。また、サービスサポートポータルでは、ECS サーバーを利用してデバイスをリモート操作できます。それぞれのユーザー情報は、ECS データベースに保存されます。

データ収集

ネットワークプロトコル

DC Agent for ECSP は以下のネットワークプロトコルとポートでデバイスデータを収集します。

DC Agent for ECSP が使用する全てのネットワークプロトコルとポートについては、付録をご覧ください。

DC Agent for ECSP

プロトコル	ポート	IN/OUT	説明
SNMP(UDP)	161	OUT	ネットワーク接続されたデバイスからデータを収集します
ENPC(UDP)	3289	OUT	エプソン独自のプリンター制御プロトコルです。

※プリンタードライバが使用するポートは記載していません。

収集・送信データ

DC Agent for ECSP と ES Agent for ECSP は、製品名、製造番号、ステータス情報、インク残量、ジョブ履歴などのデバイスデータを収集して ECS サーバーに送信します。

DC Agent for ECSP と ES Agent for ECSP が送信するデバイスデータの詳細については、「付録」をご覧ください。

セキュリティ

DC Agent for ECSP は、指定されたデバイスからデバイスデータを収集します。ターゲットデバイスは、DC Agent for ECSP が管理するデバイスリストによって識別されます。指定されていないデバイスやパソコンからデータを収集することはありません。DC Agent for ECSP や ES Agent for ECSP は、印刷データを収集しません。

データ送信

ネットワークプロトコル

DC Agent for ECSP や ES Agent for ECSP は、以下のネットワークプロトコルとポートでデバイスデータを ECS サーバーに送信します。

DC Agent for ECSP と ES Agent for ECSP が使用するネットワークプロトコルとポートについては、付録をご覧ください。

DC Agent for ECSP

プロトコル	ポート	IN/OUT	説明
HTTPS(TCP)	443	OUT	ECS サーバーにデバイスデータを送ります

※プリンタードライバーが使用するポートは記載していません。

ES Agent for ECSP

プロトコル	ポート	IN/OUT	説明
HTTPS(TCP)	443	OUT	ECS サーバーにデバイスデータを送ります

データフォーマット

DC Agent for ECSP と ES Agent for ECSP は、業界標準のデータ交換形式である JSON でデバイスデータを送信します。

セキュリティ

クライアント（DC Agent for ECSP または ES Agent for ECSP）とサーバー（ECS サーバー）間のインターネットを介したデータ伝送は、HTTPS 通信により保護されています。

HTTPS の詳細については、「付録」の“SSL セクション”をご覧ください

リモート操作

ネットワークプロトコル

DC Agent for ECSP や ES Agent for ECSP は、以下のネットワークプロトコルとポートを使用してリモート操作をします。

DC Agent for ECSP と ES Agent for ECSP が使用するネットワークプロトコルとポートのリストについては、付録をご覧ください。

DC Agent for ECSP /ES Agent for ECSP

プロトコル	ポート	IN/OUT	説明
HTTPS(TCP)	443	OUT	ECS サーバーの SSL 証明書をダウンロードします。
MQTT over SSL (TCP)	443	OUT	ECS サーバーのリモート操作コマンドを受け付けます。

※プリンタードライバーが使用するポートは記載していません。

リモート操作の種類

サービスサポート担当者は、以下のリモート操作ができます。

- ・デバイスの状態情報、累積稼働情報の取得
- ・ヘッドクリーニングの実行
- ・故障診断の実行（故障診断機能があるプリンターのみ）

対象のデバイス

指定されたデバイスがリモート操作の対象です。指定されていないデバイスは、リモート操作できません。

セキュリティー

指定されたデバイスにリモート操作コマンドを送信できるのは、ECS サービスのアカウントを持っているサービスサポートユーザーです。他の人はどの種類のリモート操作も実行できません。ユーザーは、自身が管理するデバイスのリモート操作を実行できます。他のデバイスのリモート操作やアクセスはできません。

リモート操作の流れは以下の通りです。

- (1) サービスサポート担当者は、ECS サービスでデバイスとリモート操作の種類を選択します。
- (2) ECS サービスは、データセンター内部のセキュアネットワークを介して ECS サーバーにリクエストを送信します。
- (3) ECS サーバーは、DC Agent for ECSP または ES Agent for ECSP に MQTT over SSL を使用してリモート操作コマンドを送信します。

DC Agent for ECSP や ES Agent for ECSP と ECS サーバー間のインターネットを介したデータ通信は、HTTPS や MQTT over SSL によって暗号化されるので安全です。

HTTPS や MQTT over SSL の詳細については、「付録」の“SSL セクション”をご覧ください。

ユーザー管理

ネットワークプロトコル

ウェブブラウザは、以下のネットワークプロトコルとポートを使用して ECS サービスにアクセスします。

Web Browser

プロトコル	ポート	IN/OUT	説明
HTTPS(TCP)	443	OUT	ECS サービスのウェブサービスにアクセスします

ユーザー情報

ECS サービスにアクセス権があるユーザーの情報は、全て暗号化されてデータベースに安全に保存されます。

セキュリティ

登録したユーザーが ECS サーバーにログインできます。ログインしたユーザーは、アクセス権を持つ全てのデバイスの情報を参照できます。アクセス権を持たないデバイスの情報は参照できません。

また、サービスサポート担当者は、管理担当のデバイスをリモートで操作できます。アクセス権を持たないデバイスは操作できません。

クライアント（ウェブブラウザ）とサーバー（ECS サーバー）間のインターネットを介したデータ通信は、HTTPS で暗号化されるので安全です。HTTPS の詳細については、「付録」の“SSL セクション”をご覧ください。

データストレージ

セキュリティ

ECS サーバーは、DC Agent for ECSP や ES Agent for ECSP が送信したデータを受信します。 ECS サービスは、ユーザー名やパスワードなどのユーザー情報、パートナー情報、およびクライアント情報を受け取ります。全てのデータは、エプソンのプライバシーポリシーとデータセキュリティポリシーに基づいて、AWS 内のデータベースに安全に保存されます。

付録

送信データ

DC Agent for ECSP や ES Agent for ECSP から ECS サーバーに HTTPS 経由で送信されるデバイスデータには以下が含まれます。

ECS サーバーに収集、または送信されるデバイスデータの種類の、モデル、アクセサリー、構成、エージェントの種類、および使用状況によって異なります。

カテゴリー	データ
Agent	Agent ID
	Agent type
	Agent version
	Collection type
	Sent date
	OS
	OS Version
	OS product type
Device	Manufacturer name
	Model name
	Serial number
	Region code
	Country code
	Time
	Acquired date
	Firmware version

カテゴリー	データ
Device	Printer Status
	Error/warning code
	Status/Error/Warning history
	Operation panel setting
	Printer setting
	Maintenance setting
	Media setting
	Network setting
	Consumable parts information
	Cleaning history
	Maintenance history
	Cumulative ink usage
	Cumulative printing time
	Cumulative printing area
	Job history

ネットワークプロトコルと使用ポート

DC Agent for ECSP と ES Agent for ECSP が使用するネットワークプロトコルとポートは以下の通りです。

■ DC Agent for ECSP

プロトコル	ポート	IN/OUT	説明
SNMP(UDP)	161	OUT	ネットワーク接続されたデバイスからデータを収集します。 ECS サーバーの SSL 証明書をダウンロードします。
HTTPS(TCP)	443	OUT	ECS サーバーにデバイスデータを送ります。
MQTT over SSL (TCP)	443	OUT	ECS サーバーからのリモート操作コマンドを待ちます。
ENPC(UDP)	3289	OUT	エプソン独自のプリンター制御プロトコルです。

■ ES Agent for ECSP

プロトコル	ポート	IN/OUT	説明
HTTPS(TCP)	443	OUT	デバイスデータを ECS サーバーへ送信します。 ECS サーバーの SSL 証明書をダウンロードします。
MQTT over SSL (TCP)	443	OUT	ECS サーバーからのリモート操作コマンドを待ちます。

SSL

インターネットを介した ECS のデータ送信は、全て HTTPS や MQTT over SSL プロトコルだけを使用します。HTTPS の末尾の「S」は「セキュア」の略です。HTTPS は、多くの場合、オンラインバンキングやオンラインショッピングなどで機密情報を保護するために使用されています。MQTT over SSL と HTTPS は SSL（Secure Socket Layer）を使用します。SSL は、クライアントとサーバーの間に暗号化されたリンクを確立するための標準的なセキュリティ技術です。ECS では、クライアントは、DC Agent for ECSP や ES Agent for ECSP、ウェブブラウザ、サーバーは、ECS サーバーや ECS サービスが当てはまります。

SSL を介した HTTPS や MQTT を使用したデータ送信は、全て安全に保護され、適切な宛先に確実に送信されます。

商標

- EPSON および EXCEED YOUR VISION は、セイコーエプソン株式会社の登録商標です。
- Microsoft および Windows は、Microsoft Corporation の米国およびその他の国における登録商標です。
- その他の製品名は、それぞれの所有者の商標または登録商標です。

© Seiko Epson Corporation 2020