

# スロットマシンを一括管理するIoTソリューション

## 概要

- 何千台もの接続デバイスで構成されるネットワークにおいて、手動でのパスワード変更は、コストがかかる上に非効率的であり、ヒューマンエラーも発生しやすくなります。そこで、当社はこのパスワード変更プロセスを効率化する、簡単な方法をご提供しております。
- 当社の「RMS (リモート・マネジメント・システム、IoTプラットフォーム)」という効率化されたパスワード管理機能を使用すると、数千台に及ぶデバイスのパスワード変更を数秒で行うことができます。
- RMSにはデバイスの監視、パフォーマンス分析、アップデートや設定の完全制御などの追加機能があり、これによってヒューマンエラーのリスクを減らし、作業時間とコストの削減を達成することが可能です。

## 課題 - サイバー攻撃リスクの軽視は命取りに

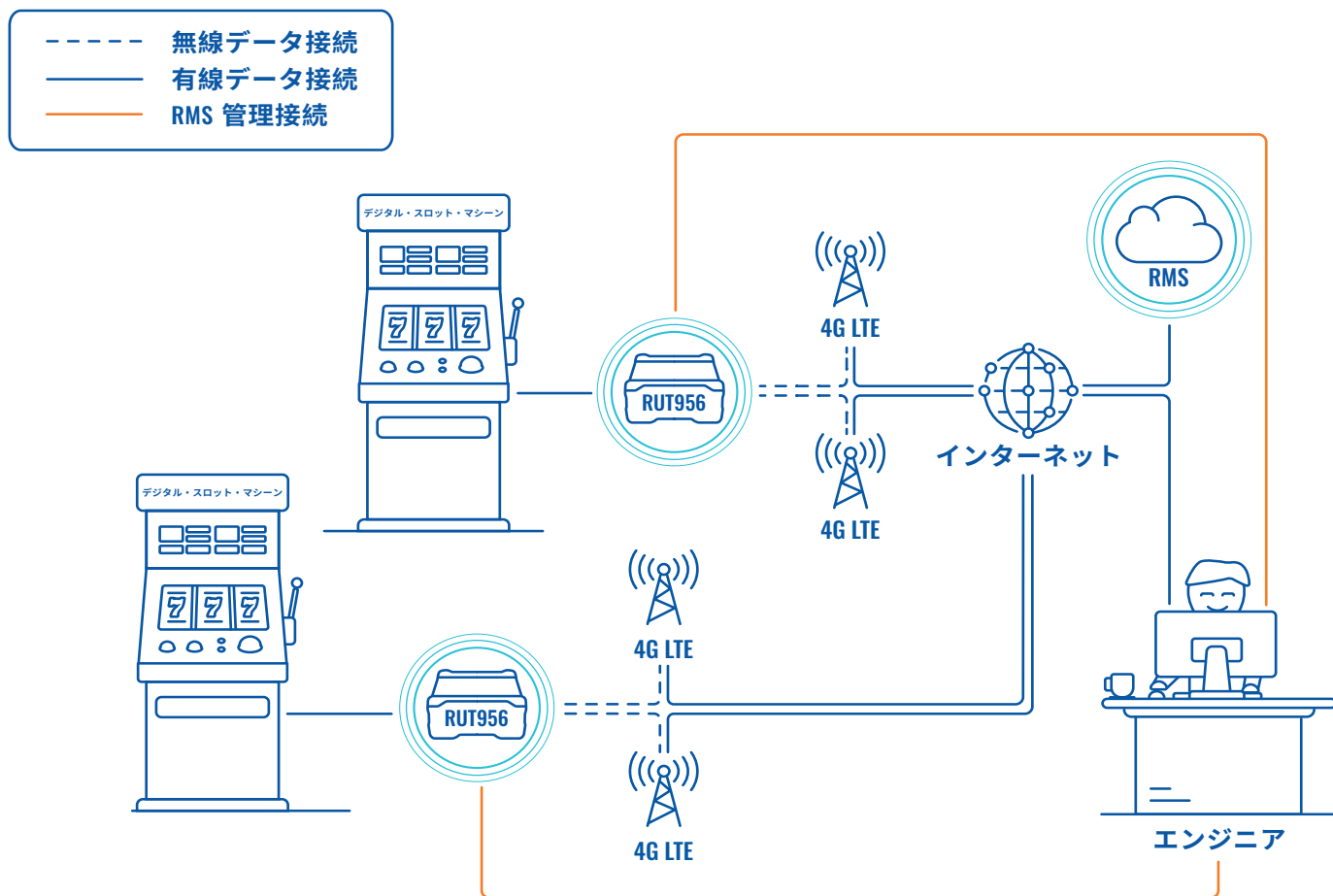
今日、サイバー攻撃に対する予防措置は必須事項となっています。しかし、それによって起こりうる脅威の数が減るわけではなく、実際はその逆で増え続けているのです。ハッカーはさらに卑劣になり、企業の大切なデータを乗っ取るようとする試みは、より狡猾になってきています。個人情報の流出や盗難が起きてしまった後後悔する前に、特別なセキュリティ対策を講じることが賢明だといえるでしょう。しかし、十分な対策ができていない企業はまだ多くないようです。

サイバーセキュリティ対策の方法は数多くあります。当社が最も重要だと考えるのは、ネットワーク接続プロセスの一番手前側にあるネットワーク・デバイスから始めることです。特にデバイスは1つでも乗っ取られてしまうと、コスト的にも風評的にも大きな打撃を受ける可能性があるため、企業の接続ソリューションはすべて、安全でサイバー攻撃から保護されている必要があります。

デバイスのセキュリティを確保するためのベストな方法は、ソリューション内の全デバイスのシステムパスワードを定期的に変更することです。しかしその場合、何千台ものデバイスが同じタスクを要求するにもかかわらず、暗号化されていないインターネット接続トンネルを使用することはできないのです。そう考えるとこの作業を完了するのが簡単ではないのが、おわかりいただけるかと思います。

パスワードを手動で変更するには、通常SMSサービスと高度な技術を持つエンジニアが必要となります。この方法ではコストがかかりますし、ヒューマンエラーのリスクも高まるでしょう。もっと迅速に、リソース効率の良く作業できる方法はないのでしょうか？

## トポロジー



## ソリューション - 複数の課題を一度に解決する“自動化”

最小のコストや時間でサイバー攻撃を回避するには、当社のRMS (リモート・マネジメント・システム、IoTプラットフォーム) で管理を自動化するのが最適なソリューションです。

RMSを使用することで、全体のシステムパスワードを用意に管理し、各デバイスに独自のランダムなパスワードを自動的に割り当てることができます。退屈で飽き飽きするようなプロセスを、セキュリティがしっかりと担保された、非常に迅速かつシンプルな方法に変えることができるわけです。

RMSで本来なら長時間かかる作業を簡単にし、お客様の時間とコストを削減できるわけですが、RMSのよさはそれだけではありません。このシステムは、ネットワークデバイスの制御管理に関してまったく新しい世界を切り開いています。何千ものデバイスを一度に監視し、パフォーマンスを分析し、ファームウェアを更新したり再設定をすることができるのです。

当社のRMSは、お客様の製品に関してパスワードの変更プロセスをはやめ、それに関連するコストと人的ミスリスクを軽減します。複数の課題を一度に解決するソリューションとなっているのです。

