日立ソリューションズ・クリエイト

HITACHI
Inspire the Next

既知・未知の脅威を検知し、長期的に稼働するIoTデバイスを守る

IoTデバイス向け セキュリティソリューション

IoTの利用拡大の裏で、IoTデバイスを狙ったサイバー攻撃は日々巧妙化しています。
しかし、IoTデバイスを導入時のセキュリティ対策のまま使用し続けているケースが多く、
導入後も継続してセキュリティ状態を更新・管理することが非常に大切です。

IoTデバイスへのサイバー攻撃事例

海外鉄道システム	攻撃者が鉄道システムの電子掲示板に列車の遅延や運休が生じたという偽のメッセージを掲載し、大混乱に。
世界各国の監視カメラ	世界各国で数万箇所、国内でも5千箇所以上の監視カメラ映像が流出し、Webサイトで誰でも確認できる事態に。

? 課題

IoTデバイスのセキュリティの対策が不十分

IoTデバイスの管理運用ができていない

! 対策

- IoTデバイスへの負荷が少ないセキュリティ対策
- 新たに検出された攻撃や脅威をAIが学習
- 既知・未知の脅威を検知・防御

- IoTデバイスを常時モニタリング
- 稼働状況・セキュリティリスクを報告
- インシデント発生時の調査支援

「IoTデバイス向けセキュリティソリューション」導入によるメリット

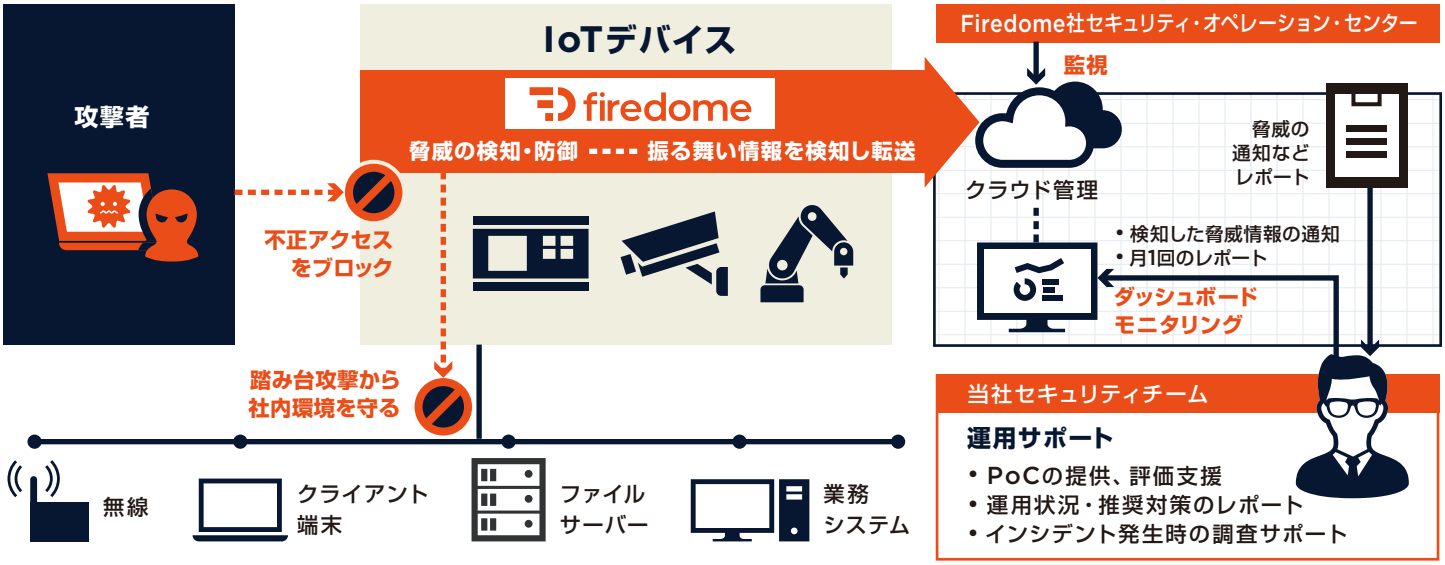
IoTデバイスメーカーの企業価値向上

セキュリティ対策により提供するIoTデバイスの信頼性を確保

IoTデバイス利用者の事業継続性向上

監視サービス・運用支援により利用者の負担を抑え、安全な運用を実現

「IoTデバイス向けセキュリティソリューション」の概要



Firedomeによる脅威の検知・防御

脅威インテリジェンスによりサイバーキルチェーンに即した「進化し続ける」多層防御を実現

サイバーキルチェーン			
偵察	ポートスキャンによる攻撃対象の調査	入口対策	ポート監視
武器化			
配送	DOS攻撃／脆弱性を悪用した外部からの不正アクセス		FW機能
攻撃	攻撃コードの実行によるマルウェアダウンロード／情報搾取	内部対策	プロセス動作検知
	既知・未知のマルウェア実行		定義ファイルでの保護
インストール	AIによる機械学習で振る舞い検知		機械学習
遠隔制御	マルウェアに感染したIoTデバイスがC&Cサーバー(攻撃者の指令サーバー)に接続	出口対策	ホワイトリスト型接続制御
目的達成			

スマートデバイスで二次元バーコードを読み取っていただくか、
URLをブラウザーのアドレスバーに入力してアクセスしてください

URL | www.hitachi-solutions-create.co.jp/solution/iot_security/

※ 本ソリューションはFiredomeを活用しています。　※ Firedomeのロゴ及び製品名は米国法人Firedome, Inc.の米国における登録商標、または商標です。

商品・サービスに関するお問い合わせ・ご相談受付

Webによる受付

www.hitachi-solutions-create.co.jp/inq.html

お問い合わせページより、商品・サービスをお選びください。

メールによる受付

hsc-contact@mlc.hitachi-solutions.com

*ご相談・ご依頼いただいた内容は回答などのため、当社の関連会社（日立ソリューションズグループ会社）および株式会社日立製作所に提供（共同利用含む）することがあります。
取り扱いには十分注意し、お客さまの許可なく他の目的に使用することはありません。

HSC202203

株式会社 日立ソリューションズ・クリエイト

www.hitachi-solutions-create.co.jp/