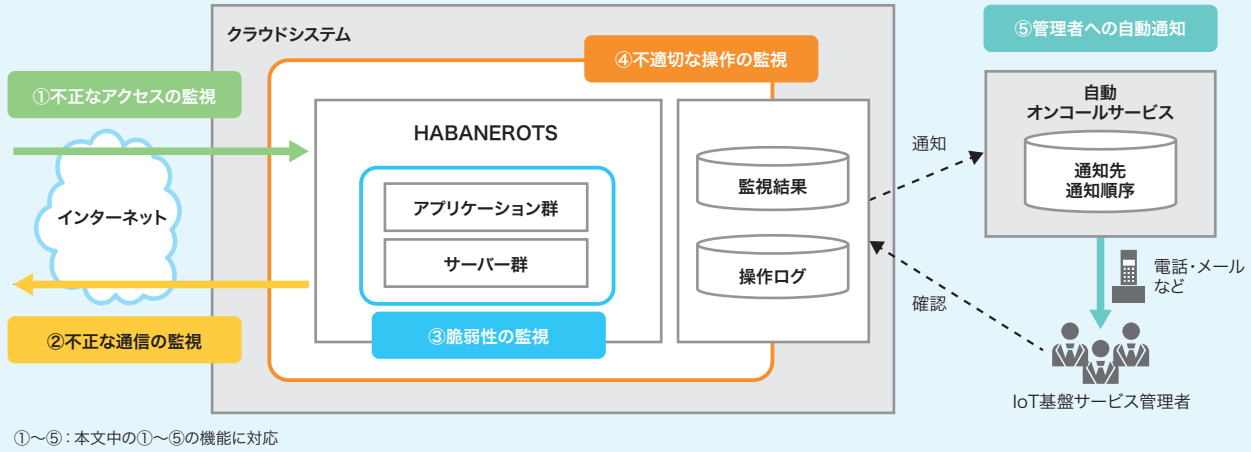
IoT基盤サービスのためのセキュリティー監視の仕組み



HABANEROTSのセキュリティー監視の仕組み
Overview of security monitoring system for HABANEROTS Internet of Things (IoT) platform service

近年，センサーなどのIoT（Internet of Things）機器データを活用するサービスの実現には，クラウド環境が広く利用されている。クラウド環境を利用する際，ハードウェアなどの基盤の品質はクラウド事業者が責任を持つが，クラウド環境に構築するシステム（以下，クラウドシステムと略記）の品質は，全てシステム構築者の責任となる。このため，クラウドシステムの構築とその運用において，セキュリティーの確保は重要な課題である。

大量のIoT機器のデータ収集や遠隔操作といった機能を提供するIoT基盤サービスであるHABANEROTSも，クラウドシステムの一つである。今回，これをセキュアに継続運用するためのセキュリティー監視の仕組みを実現した。

この仕組みは，①ソフトウェアの脆弱性を突いたクラウドシステム外部からの不正なアクセスの監視，②コンピューターウイルス感染などによるクラウドシステム内部からの不正な通信の監視，③クラウドシステム内で稼働するソフトウェアの脆弱性の監視，④ファイアウォール設定ミスなどのクラウドシステムの不適切な操作の監視，といった機能を持つ。

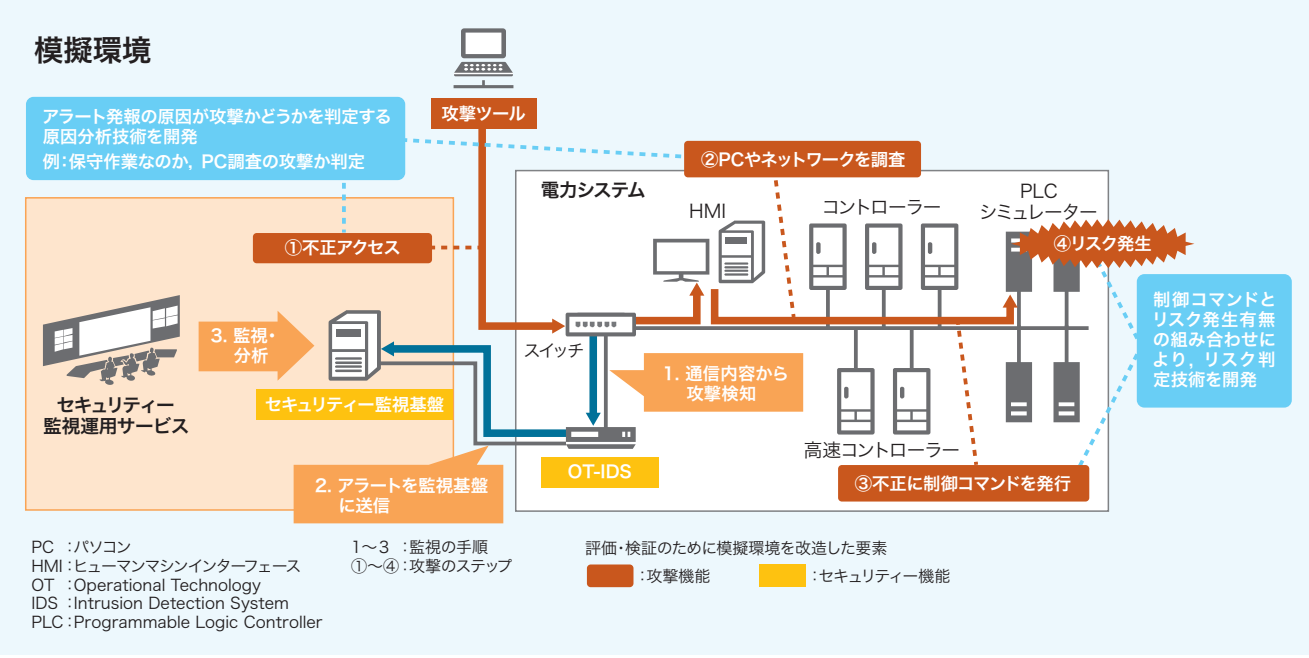
クラウドシステムは，サービス利用者数に応じたサーバー追加や，設定変更，新たに見つかった既存ソフトウェアの脆弱性など，日々状況が変化する。このため，サービス公開時や，その後の一定期間ごとのセキュリティー確認だけでは不十分である。今回実現した仕組みでは，これらの変化を常に監視し，新たなセキュリティー違反を即座に検知する。

特に重大な違反を検知した場合，⑤自動オンコールサービス経由で，電話やメールでIoT基盤サービス管理者に自動通知する機能も持つ。管理者は，監視結果や操作ログから原因を追及し，被害を最小限に抑えることができる。

今回の仕組みは，クラウド事業者が提供する標準的なセキュリティー監視サービスと，一般的なSaaS（Software as a Service）だけで実現した。また，この仕組みを自動構築するIaC（Infrastructure as Code）を社内オープンソースとして公開しているため，東芝グループ内であれば容易に適用が可能である。今後も全社的なクラウドシステムのセキュリティー向上と標準化に貢献していく。

デジタルイノベーションテクノロジーセンター

制御システム向けセキュリティー監視技術の高度化



模擬環境を用いたセキュリティー技術の高度化

Sophistication of cybersecurity technologies for operational technology (OT) systems through utilization of simulated environments

社会インフラや産業システムなどの制御システムは近年，情報システムで用いられてきた汎用のOS（基本ソフトウェア）や，OS以外のソフトウェア，通信プロトコルなどを利用するようになった。また，生産管理システムなどの情報システムとの接続や，クラウドシステムにある製造データを活用するためのインターネットへの接続なども加速している。その結果，これまで情報システムで起こっていたサイバー攻撃の脅威が，制御システムにも及んでいる。

東芝グループは，長年培ってきた制御システムの知見とセキュリティー運用の経験を融合し，制御システムのライフサイクル全体にわたってリスクを低減するソリューションやサービスを提供するセキュリティー技術を開発している。今回，セキュリティー監視技術を高度化するために，異常検知した際にサイバー攻撃か否かを判別する原因分析技術と，サイバー攻撃による安全性への影響を評価するリスク判定技術を開発した。

制御システムでは，保守作業などの非定常的な作業が頻繁に行われるため，異常な通信を検知してアラートが発せられた際に，それが保守作業による意図したものか，サイバー攻撃によるものかを判定する必要がある。そこで，セキュリティー監視基盤上で保守作業の情報とアラートを照合することで，精度の高い原因分析を可能にした。また，制御システムは人命や環境に影響を及ぼさないことが最優先なので，サイバー攻撃が安全性に影響を及ぼすかどうかの判定が最も重要である。そこで，事前に制御コマンドなどが制御システムの安全性に影響を与えるか否か評価を行い，その結果を参照することで，リスク判定精度を向上させた。

自社開発の電力システムなどの模擬環境を活用して実際にサイバー攻撃を実施することで，これらの技術が有効なことを確認した。

これらを活用することで，より高度なセキュリティー監視・運用サービスの提供を目指す。

関係論文：東芝レビュー．2022，77，3，p.11–14.

東芝デジタルソリューションズ（株）