制御システム向けセキュリティ監視技術

Security Monitoring Technologies for Control Systems

小島　健司　　外山　春彦
■KOJIMA Kenji　■TOYAMA Haruhiko

社会インフラなどに広く用いられている制御システムは，これまで機器ベンダー独自のオペレーティングシステム（OS）やプロトコルを用いて，独立したネットワークで運用されることが多かったため，セキュリティは十分に考慮されていなかった。昨今，標準的なOSやプロトコルの採用，及び外部システムへの接続が増えたことで，制御システムがサイバー攻撃の標的となるリスクが増え，事故事例も報告されている。一方，情報システムでは，標的型攻撃の台頭に伴い，新たなセキュリティ対策のアプローチであるセキュリティ監視技術が注目されている。

東芝及び東芝ソリューション（株）では，セキュリティ監視技術を制御システムへ適用し，安全・安心な社会インフラシステムを実現するための研究開発を進めている。

Conventional control systems in the field of social infrastructure systems have been designed with a dedicated operating system and protocol, and connected to the related components via a local network. Security threats from external networks have consequently not been a strong focus of concern. Recently, however, security risks have been increasing and cyberattacks on such control systems have been reported, because versatile operating systems and protocols are being used to reduce costs and systems are being connected to other systems via the Internet to improve operating efficiency. At the same time, with the increase of targeted attacks in the field of information systems, security monitoring technologies have been attracting considerable attention as a new approach to the implementation of security countermeasures.

With the aim of realizing safe and secure social infrastructure systems, Toshiba and Toshiba Solutions Corporation are engaged in the development of security monitoring technologies for control systems.

1　まえがき

海外の核燃料施設の遠心分離機が，スタックスネットと呼ばれるコンピュータウイルスを用いたサイバー攻撃を受ける事件が，2010年に発生した。これに代表される，発電所や，プラント，工場，ビルなどの制御システムを狙ったサイバー攻撃の報告が増えつつある。これら社会インフラを支える制御システムにセキュリティ事故が発生すると，人命に影響が及ぶなど社会的な影響が大きいため，セキュリティを確保し安定的な運用を目指すことが非常に重要である。

従来，制御システムは機器ベンダー独自のOSやプロトコルを用い，外部ネットワークに接続されない独立したネットワークで運用されており，サイバー攻撃を受ける可能性は低かった。しかし，生産性や効率を向上させるために外部の情報システムと接続し，また，コストを削減するために標準的なOSやプロトコルを利用することが増えて，サイバー攻撃を受ける可能性が飛躍的に高まっており，セキュリティ対策が重要になっている。東芝グループが注力事業の一つとして取り組んでいるスマートコミュニティにおいても，社会インフラを制御する様々な制御システムを情報システムに接続することでエネルギー利用効率の最適化などの目的を実現しており，セキュリティ確保が重要な課題である。

一方，情報システム分野では特定の企業や官公庁を狙った標的型攻撃が相次いでおり，社会的な問題になっている。標的型攻撃では未知のセキュリティホールを利用して攻撃対象の組織に合わせた攻撃が行われるため，ファイアウォールや，認証，アクセス制御などのようなシステムの出入口を保護する従来のセキュリティ対策だけでは不十分になっている。

このようななか，情報システム分野ではセキュリティ監視技術が注目を浴びている。セキュリティ監視技術は，システム内の多数のサーバや，ネットワーク機器，ファイアウォール，IDS/IPS（Intrusion Detection System/Intrusion Prevention System）などのセキュリティ機器から集めたログを分析することで，システムへの攻撃や侵入といったセキュリティインシデント及びその兆候を早期に検出し，被害が発生する前に対処することを目的としている。この分析を高度化する，SIEM（Security Information and Event Management）と呼ばれるセキュリティ監視製品がいくつかのベンダーから提供されている。また，セキュリティ監視技術を活用し，セキュリティ監視を外部組織に対してサービスとして提供する企業も存在する。このようなサービスをSOC（Security Operation Center）サービスと呼ぶ。

ここでは，安全・安心な社会インフラシステムの実現を目指して東芝と東芝ソリューション（株）が研究開発を進めている，制御システムに適したセキュリティ監視技術の概要について述べる。

2　セキュリティ監視技術の概要

情報システム向けのセキュリティ監視製品は，一般に収集，正規化，蓄積，及び分析の機能で構成される。ここでは，これらの機能を提供する基盤をセキュリティ監視基盤と呼ぶ。それぞれの内容について以下に述べる。

⑴　収集　　システム内のサーバ機器や，ネットワーク機器，セキュリティ機器などからセキュリティ監視に利用するログや通信データをセキュリティ監視基盤に集約する。

⑵　正規化　　各機器から収集したログや通信データを分析しやすいように，あらかじめ決められた正規化ルールにより解釈する。ログの出力形式は使用している機器やソフトウェアにより異なるため，正規化することで統一して扱えるようにする。

例えば，機器へのログインに失敗したログを，ある機器では“FAILED LOGIN”と出力するのに対して，別の機器では“LOGIN FAILURE”と出力する場合があるが，これらを同じログイン失敗の事象として解釈できるようにする。別の例としては，ログや通信データ中に含まれるIP（Internet Protocol）アドレスを“送信元IPアドレス”として解釈する。このような正規化を行うことで，効率的に分析できる。セキュリティ監視製品では多種多様な機器のログを取り込むための正規化ルールを提供している。

⑶　蓄積　　セキュリティ監視基盤では，セキュリティインシデントを分析するために大量のログや通信データを収集し蓄積する。高度な分析を行うためには大量のデータを効率よく分析できる必要があり，セキュリティ監視製品では独自のデータベースを持つなどの工夫がなされている。また，フォレンジックと呼ばれる，不正アクセスや機密情報漏えいの原因究明のためにも使用されることを想定して，蓄積されたデータの完全性を保証している製品もある。

⑷　分析　　収集，正規化，及び蓄積されたログや通信データをあらかじめ設定された検出ルールに基づき分析をすることで，セキュリティインシデントの可能性を検出する。また，分析者がセキュリティインシデントの真偽や原因を特定するために必要な支援機能も提供される。

3　制御システムにおけるセキュリティ対策の特徴

3.1　情報システムとの違い

情報システムと制御システムとでは，セキュリティ対策を考えるうえで考慮すべき特徴に大きな違いがある。その概要を**表1**に示し，詳細について以下に述べる。

表1．情報システムと制御システムのセキュリティを考えるうえでの特徴
Differences in characteristics of security measures for information and control systems

項　目	情報システム	制御システム
機器設置場所	保護すべき機器がデータセンターに集約	保護すべき機器がフィールドに分散配置
優先されるセキュリティ特性	機密性	可用性と完全性

3.1.1　機器設置場所　　情報システムでは，サーバなど重要な機器はデータセンターなど物理的にも論理的にも安全性の確保された領域に設置され，利用者はそこにアクセスして利用する。また，昨今ではクラウドコンピューティング技術により，システムとしての集約率がいっそう高まっている。このようにシステムが集約して設置されることには，セキュリティ確保のための管理や対策が容易になるという利点がある。

これに対して制御システムでは保護すべき重要な機器が物理的に分散して配置される。例えば，ビル管理システムでは，ビルの各所に機器を直接制御するコントローラが多数設置され，それら一つ一つが攻撃の対象になりえる。制御システムのセキュリティ対策ではこれら分散配置される機器をいかに保護していくかが課題となる。

3.1.2　優先されるセキュリティ特性　　情報セキュリティは情報の機密性（Confidentiality），完全性（Integrity），及び可用性（Availability）を維持することであると定義され[1]，これら三つの特性を一般に情報セキュリティの3要素と呼ぶ。情報システムではこの中で特に機密性が重視される。スマートコミュニティでも多数の個人情報や計測データを扱い，この保護は重要な課題である。例えば，HEMS（Home Energy Management System）では，個人の電力消費量情報などから生活パターンを読み取ることができるため，この情報を保護する必要がある。

これに対して，制御システムでは完全性や可用性が重視される。完全性はシステムが正しく動作することであり，これが損なわれるとシステムの異常動作につながる。可用性はシステムが動作し続けることであり，これが損なわれるとシステムの停止につながる。例えば，電力システムの異常動作や停止は住民の社会生活に直接影響を及ぼすだけでなく，重大な事故や損失につながる可能性がある。

3.2　制御システムにおけるセキュリティ対策

3.1節で述べたように，情報システムと制御システムとでは求められるセキュリティ上の要求や状況が異なる。したがって，セキュリティ対策を実施するうえでは，これらの特徴を考慮した対策を検討していく必要がある。

情報システムでは日々新しい攻撃手法が発見されるなかで，

それに追随する形で新しいセキュリティ対策技術が提案されてきた。これに対して制御システムでは，これまで攻撃の標的となる可能性が低くセキュリティがあまり重視されてこなかった。そのため，情報システム向け対策技術の流用が中心で，制御システム向けの技術は未成熟であった。しかし，制御システムを狙った攻撃が増加することが予想されるなかで，今後は制御システムの特徴を利用した攻撃に対処できる技術が必要になる。

4　制御システム向けセキュリティ監視技術

4.1　制御システムへ適用する際の対処

3章で述べたとおり，制御システムは情報システムに比べ高い可用性が要求されることから，攻撃の兆候を早期に検出することを目的としたセキュリティ監視技術の有効性が高い。

ここでは，セキュリティ監視技術を制御システムに適用するにあたり，3章で述べた情報システムとの違いに対し，どのように対処したかについて述べる。

4.1.1　機器設置場所　多数のフィールド機器が分散配置される制御システムには，システムへの出入口が多数存在し，攻撃者の侵入経路も多数存在する。したがって，どの経路から侵入した攻撃であっても，その兆候を確実につかむために，収集機能ではシステム内部の各所から通信データやログを集めることとした。更に，分析機能では各所から集めた複数の情報を互いに関連付けて分析するようにした。

4.1.2　優先されるセキュリティ特性　可用性を維持するためには，攻撃の被害が発生する前に早期に攻撃の兆候を検出することが重要である。このために，分析機能では監視対象となる制御システムの特徴に合わせた検出ルールを定義し，正常状態と異なるふるまいを検出することで早期検出を実現している。

4.2　各機能における対応

制御システム向けのセキュリティ監視技術の全体像を**図1**に示し，各機能における制御システム向けの対応について以下に述べる。

4.2.1　収集　制御システムでは，各種機器の制御を行うコントローラなどの制御機器がシステム内に分散配置される。これら制御機器に近い箇所から通信データを収集することで，セキュリティインシデントの検出をより高い精度で行うことが可能になる。制御機器近くからの情報を収集するためには，セキュリティ監視基盤に安全に情報を送信できる情報収集装置が必要である。この装置は，セキュリティ監視基盤に接続されて，制御システムのネットワークからログや通信データをセキュリティ監視基盤に送信する役割を持つ（**図2**）。情報送信にあたっては，通信量を抑えるために，送信する情報を取捨選択して分析に使用する情報だけを送信し，通信の信頼性を確保するために，エンティティ認証や，通信の暗号化，メッセージ認証などを行うといった機能を持つ。

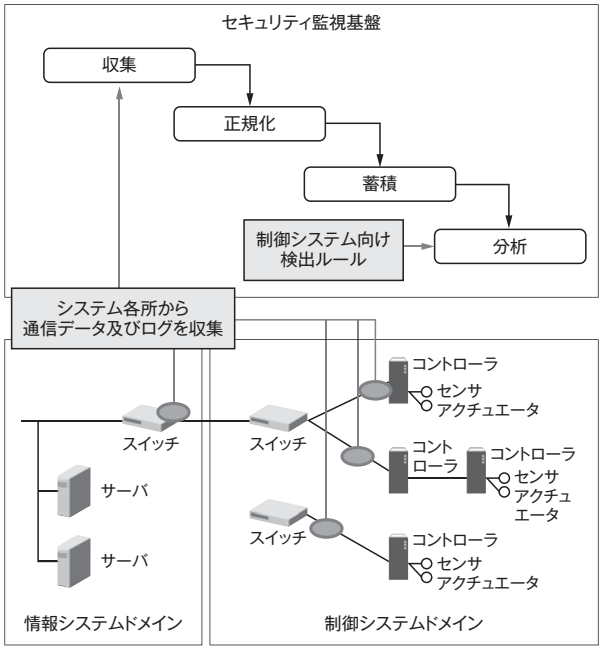

図1．制御システム向けセキュリティ監視技術の概要 ― 制御システムの特性を考慮し，情報システム向けセキュリティ監視を拡張している。
Overview of security monitoring technologies for control system

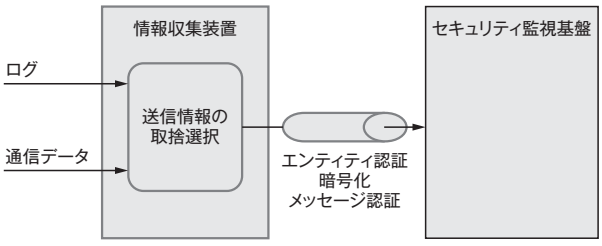

図2．情報収集の概要 ― 機器に近い箇所に情報収集装置を設置することで，精度の高い分析を実現する。
Information collection scheme

制御システムでは一般に機器の利用年数が10 ～ 20年と情報システムに比べ長く，OSのパッチを適用できないなどセキュリティレベルが不十分な機器も数多く稼働している。このような稼働中の既存システムの保護も重要な課題であり，情報収集装置により後付けでセキュリティ監視を提供できるようになる。

4.2.2　正規化　制御システムが出力するログや通信データに合わせた正規化ルールが必要である。これにより，制御の内容まで踏み込んだ有効性の高い分析が可能になる。

4.2.3　蓄積　ログや通信データの蓄積に関しては，情報システムの場合と変わりはなく，大量のデータを長期間安全に保存できることが重要である。

4.2.4　分析　制御システム向けの監視では，どのような検出ルールを設定するかという点が従来の情報システム向けの監視ともっとも大きく違う。制御システム向け検出ルールの例として，ここでは**図3**に示す三つの例について述べる。

(1)　宛先　制御システムでは，情報システムに比べ定型的な情報のやり取りが多く，ある機器から発生する通信の宛先を限定するのが容易である。したがって，このルールから逸脱する通信が発生した場合に，それを異常通信の可能性として検出する。

(2)　周期　制御システムでは，機器のステータスを通知するために周期的に流れるメッセージが存在する。この規則性を利用し，この規則から逸脱する通信が許容量以上発生した場合に，それを異常の可能性として検出する。

(3)　内容　制御システム通信の内容に踏み込んだ分析を行う。例えば，コマンド内容を監視し，通常の運用時に発行されないコマンドがないかを監視するというように，制御システムの通信プロトコルならではの特性を利用して，セキュリティインシデントを検出する。

攻撃者はシステムに侵入すると，まず，様々な手法を利用してシステム内の情報を調査し，そこで得た情報を利用して実際に攻撃を行うのが一般的であり，このために多数の不正なコマンドを送信する。例えば，ポートスキャンと呼ばれる手法により，多数の通信を行い次の攻撃対象機器を探索する。これに対して，監視対象のシステムでは通常使用されない通信の宛先や内容を検出することで，攻撃者がシステムに被害を与えるような攻撃に移る前に，その兆候をつかみ早期に対策することが可能になる。

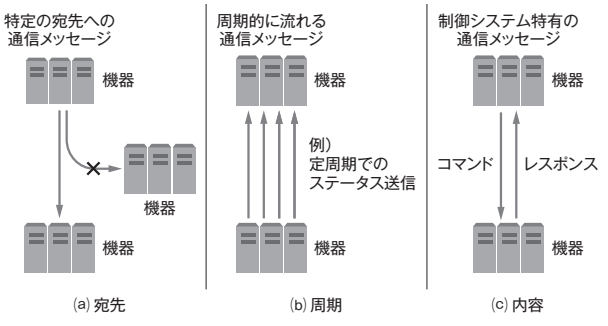

図3．制御システム向けセキュリティ監視の検出ルール例 — 制御システム向けプロトコルの特徴を考慮し検出ルールを作成する。
Examples of security monitoring rules for control system

また，4.2.1項で述べた情報収集装置をシステム内に多数組み込むことで，例えば，システムの入口で取得した通信データとシステムの内部で取得した通信データを関係付け，攻撃の経路を明確にするといった分析が可能である。これにより対策すべき箇所が明確になり速やかに対策することができる。

検出ルールは，対象とする制御システムに合わせてカスタマイズが必要な場合があるが，制御システムでは情報システムに比べればシステム構成や通信内容が単純であり，そこで使用される検出ルールも単純化することができる。したがって，検出ルールの自動学習にも向いていると考えられ，今後，検討していく。

5　あとがき

東芝と東芝ソリューション(株)は，安全・安心な社会インフラシステムの実現に向けて，今後も制御システム向けセキュリティ監視技術の研究開発を行い，その有効性の検証を進めていく。また，セキュリティ監視など運用面でのセキュリティ対策に加え，システムの構築時から脆弱(ぜいじゃく)性を作り込まない取組みも重要であり[2]，システムの構築から運用に至るまで，トータルなセキュリティ技術を開発するとともにサービスを提供していく。

文　献

(1)　JIS Q 27002：2006. 情報技術－セキュリティ技術－情報セキュリティマネジメントの実践のための規範.
(2)　小田原育也　他. スマートコミュニティシステムのためのセキュアシステム構築技術 セキュアSI$_{TM}$. 東芝レビュー. **66**, 11, 2011, p.10－13.

小島　健司　KOJIMA Kenji
東芝ソリューション(株) IT研究開発センター　研究開発部主査。情報セキュリティ技術及び応用システムの研究・開発に従事。
Toshiba Solutions Corp.

外山　春彦　TOYAMA Haruhiko
クラウド＆ソリューション社 ICTクラウドサービス推進部クラウドサービス商品企画・技術部参事。クラウドセキュリティサービスの商品企画に従事。
ICT Cloud Service Div.