特集論文

原子力計装制御システムのサイバーセキュリティ対策の現状と展望

稲葉隆太*
町田慎弥*

Present and Future of Cyber Security Measures for Instrumentation and Control Systems of Nuclear Plant

Ryuta Inaba, Shinya Machida

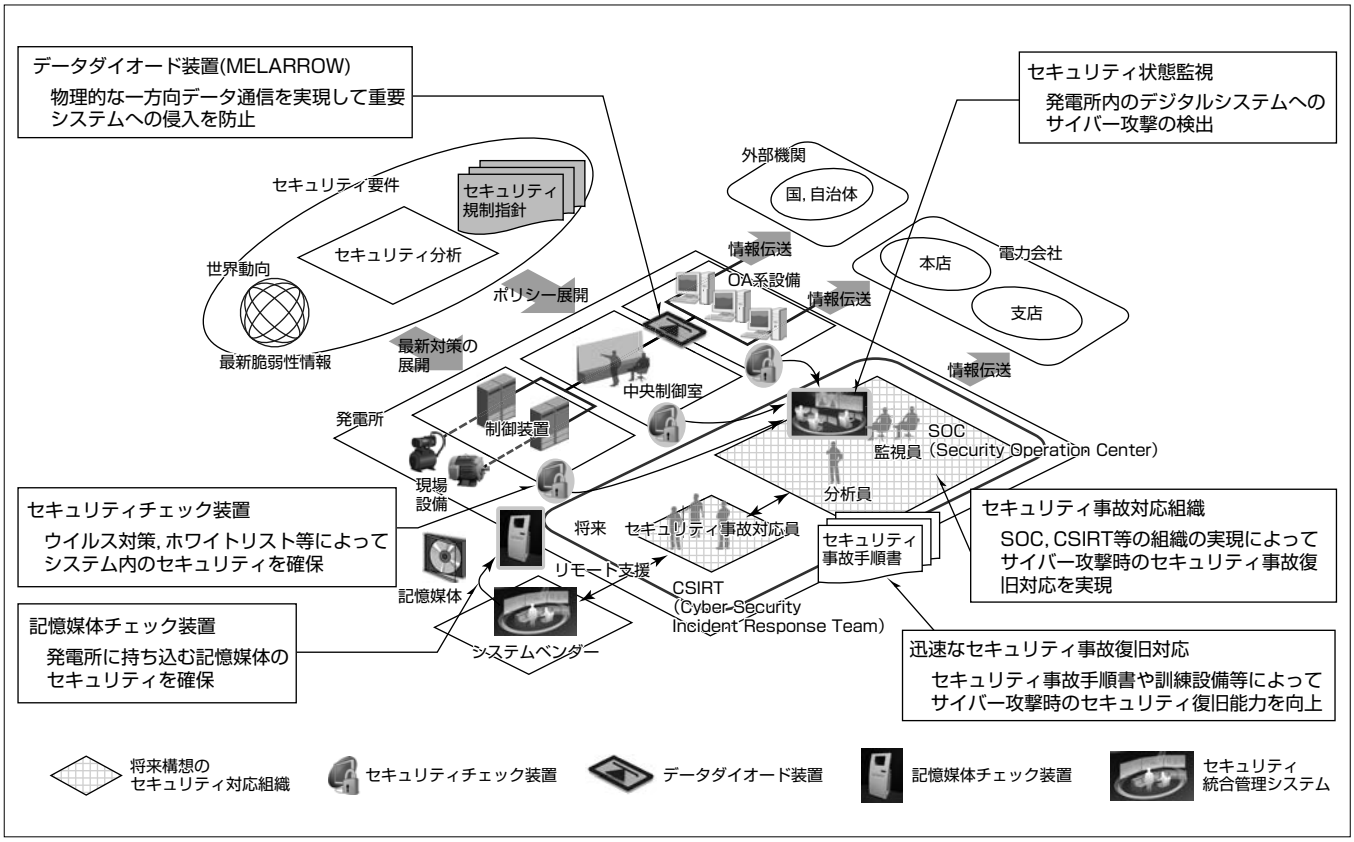
要　旨

サイバー攻撃の増加を背景に，国内では，サイバーセキュリティ基本法が制定され，重要インフラ(国民生活と社会経済活動が大きく依存する，電力，金融，航空などの13分野)の事業者に自主的，かつ積極的なサイバーセキュリティの確保を要求している。また，経済産業省は電力制御システムのサイバーセキュリティ確保を目的に，電力制御システムセキュリティガイドラインを2016年度内に制定する計画である。いずれも，技術面(アクセス管理，マルウェア(注1)対策等)，運用面(事故対応組織，手順書の整備など)の対策の実施，PDCA(Plan Do Check Action)によるセキュリティ対策の向上を要求している。今後，重要インフラ事業者はこれら要件を満足したサイバーセキュリティ対策を実現していく必要がある。

三菱電機は，計装制御システムへの技術面の対策としてセキュリティチェック装置，データダイオード装置，記憶媒体チェック装置などのセキュリティデバイスの開発を実施し，原子力発電所への納入を実現した。

現在は，運用面の対策実現に向け，セキュリティ状態監視，セキュリティ事故対応組織，迅速なセキュリティ事故復旧対応などの基本方針の策定に向けた取組みを推進している。

(注1)　悪意のあるソフトウェア。ウイルス，トロイの木馬など。



計装制御システムにおけるサイバーセキュリティ対策の全体構成

発電所のサイバーセキュリティ確保のため，中央計装や計装制御に用いられるデジタル設備に対するセキュリティ対策を講じるとともに，万が一のサイバー攻撃に備え，セキュリティ状態を監視するSOCや，セキュリティ事故時の復旧対応を行うCSIRTなどを配置し，セキュリティ統合管理システム，セキュリティ事故手順書などを整備することで迅速な対応を実現する。

*電力システム製作所

1. まえがき

近年，デジタルシステムに対するサイバー攻撃は増加の傾向にあり，その攻撃対象は制御システムにまで及んでいる。2015年末にウクライナで発生して20万人以上に影響を与えた大規模な停電もサイバー攻撃が原因とされており，システムの停止だけではなく，サービスの停止にまで至った。

従来，原子力分野では発電所の安全への取組み(安全設計)を継続して行ってきた(プラントの深層防護，誤操作防止，設備多重化など)。セキュリティ対策に関しても，安全機能を持つ設備には，直接的な外部ネットワークへの接続禁止，独自装置・プロトコルなどを採用してきた。

一方で，高度化するサイバー攻撃への対応，内部脅威対応，最新の規制指針対応など，新たな観点でのサイバーセキュリティ対策が求められている。

本稿では，原子力計装制御システムのセキュリティ要件，セキュリティ技術対策及びセキュリティ運用対策について述べる。

2. 計装制御システムでのセキュリティ要件

セキュリティ対策には一般的に，技術面の対策(ウイルス対策，アクセス管理など)と，運用面の対策(セキュリティ事故時体制，手順書，パッチ管理など)が必要である。対策の要件はセキュリティ分析の結果や，各事業分野の規制指針・ガイドラインから抽出できる。

2.1 セキュリティ分析からの要件

セキュリティ対策を検討する際，セキュリティ分析によって，現状の問題点を正確に抽出して対策を講じることが重要である。セキュリティ分析手法には，米国国立標準技術研究所(NIST)によって策定されたセキュリティ分析のガイドラインNIST SP800-30[1]や，ISO/IEC27001に記載のセキュリティリスク軽減を図るためのガイドラインISMS(Information Security Management System)[2]などの手法が存在する。いずれも対象システムを体系的に分析し，セキュリティの脅威をリスク値として数値化(定量化)することで，適切な対策を講じることを可能とする。

NIST SP800-30に基づき，セキュリティ分析を行った結果，抽出される脅威と対策例を**表1**に示す。

表1．NIST SP800-30に基づいて抽出された脅威と対策例

対象	脅威例	対策例
装置	装置内情報への不正アクセス	・アクセス管理 ・暗号化
	装置を悪用したサービス妨害	・ホワイトリスト
	装置に感染したマルウェアによるサービス妨害	・ウイルス対策 ・ホワイトリスト
	記憶媒体(USBメモリ等)によるマルウェア感染	・ウイルス対策 ・記憶媒体チェック装置
通信路	通信データの盗聴，改ざん	・暗号化 ・ログ監視

2.2 セキュリティ規制指針からの要件

原子力分野のサイバーセキュリティ規制指針として，国際原子力機関(IAEA)発行のNuclear Securityシリーズ[3](注2)，米国原子力規制委員会(NRC)発行のRG5.71[4](注3)などが存在する。これら規制指針には，次の技術面，運用面の要件があり，対策を講じる必要がある。

(1) セキュリティレベルの異なるセグメント間のデータ通信の物理的な一方向化
(2) 記憶媒体のライフサイクル管理(記憶媒体の輸送から，発電所受入れ，導入，破棄までのセキュリティ管理)
(3) セキュリティ状態監視
(4) セキュリティ事故対応組織の確立
(5) 迅速な復旧対応

(注2) IAEA策定の核セキュリティに関する国際的文書。基本文書，勧告文書，実施指針，技術文書などの幅広い要件。
(注3) 米国原子力規制委員会(NRC)策定のサイバーセキュリティに関する規制指針。

2.3 原子力向けセキュリティ要件

2.1節，2.2節で抽出した“原子力向けセキュリティ要件”を**表2**に示す。

3. 計装制御システムのセキュリティ技術対策

原子力向けセキュリティ要件(**表2**)のうち，技術要件①～③の対策実現に向け，セキュリティチェック装置(技術要件①)，データダイオード装置(技術要件②)，記憶媒体チェック装置(技術要件③)の開発を行った。各装置の特長を次に示す。

3.1 セキュリティチェック装置

デジタル装置に対する一般的なセキュリティ機能(ウイルス対策，ホワイトリスト，アクセス管理など)を搭載し，セキュリティ確保を実現するとともに，複数装置のセキュリティ状態を集約することで，同一ネットワーク上の装置のセキュリティの一元管理を可能とした(**図1**)。

3.2 データダイオード装置

データダイオード装置“MELARROW[5]”データ通信を物理的に一方向化するネットワーク装置(**図2**)である。IEEE802.3ahの単方向通信の技術によってデータの物理的一方向通信機能を実現した。

セキュリティレベルの異なる境界に設置することで，セキュリティレベルの低いネットワークからの不正侵入を遮

表2．原子力向けセキュリティ要件

分類	No.	要件概要
技術要件	①	不正アクセス，マルウェア感染，サービス妨害，データ改ざん等への対策
	②	セキュリティレベルの異なるセグメント間のデータ通信の物理的な一方向化
	③	記憶媒体のライフサイクル管理
運用要件	①	セキュリティ状態監視
	②	セキュリティ事故対応組織の確立
	③	迅速な復旧対応

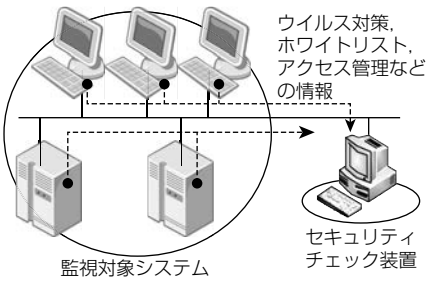


図1．セキュリティチェック装置の概念図

図2．データダイオード装置(MELARROW)

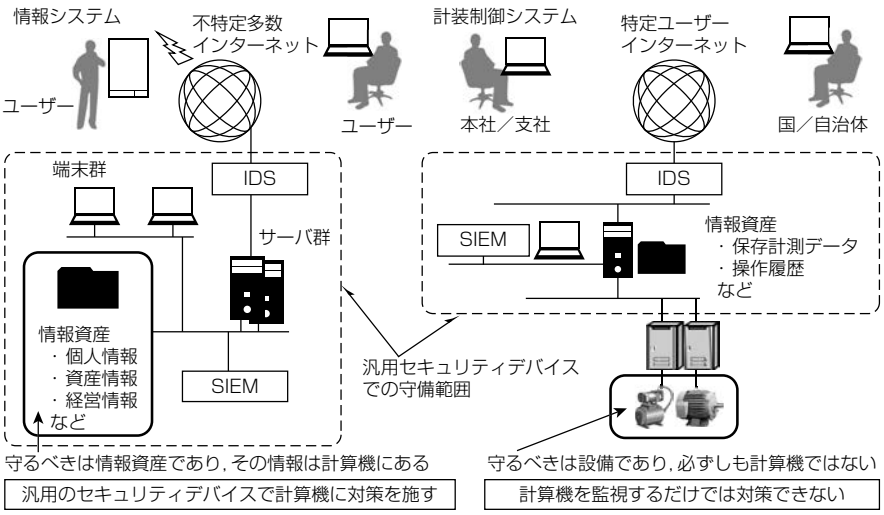


図4．情報システムと計装制御システムのセキュリティ監視の違い

図3．記憶媒体チェック装置

断可能にした。米国の原子力発電所では，この装置の導入が要件となっている。

3.3　記憶媒体チェック装置

プラント設備のソフトウェア改造時などに，発電所へ持ち込む可搬型記憶媒体(DVD，USBなど)のセキュリティを管理することによって，サイバー攻撃から防護する装置である(**図3**)。暗号化，ウイルス対策などの機能によって，改造全フェーズ(メーカー出荷，輸送，受入れ，実機改造)に想定される可搬型記憶媒体へのセキュリティ脅威から防護できるシステムを実現した。

4. 計装制御システムのセキュリティ運用対策

原子力向けセキュリティ要件(**表2**)のうち，運用要件の対策実現に向け，セキュリティ状態監視(運用要件①)，セキュリティ事故対応組織の確立(運用要件②)，迅速な復旧対応(運用要件③)の基本方針策定に向けた取組みを推進している。次に運用要件の実現に向けた課題とその対策方針について述べる。

4.1　セキュリティ状態監視

計装制御システム向けセキュリティ状態監視は，情報システムで導入されている汎用セキュリティデバイス(侵入検知システム(Intrusion Detection System：IDS(注4))，ファイアウォール，セキュリティ情報イベント管理システム(Security Information Event Management：SIEM(注5)))での監視の仕組みに計装制御システムの特質を踏まえて実現する。

情報システムのセキュリティ監視対象は主にシステム内のデータ(個人情報，資産情報など)であり，その情報がサーバ内に格納されているため，汎用セキュリティデバイスによるセキュリティ監視が効果的である。

一方，計装制御システムのセキュリティ監視対象には，システム内のデータに加えてプラント設備，及び制御装置がある。これらは，汎用セキュリティデバイスでは監視をサポートしているケースが少なく，情報システムのセキュリティ監視の仕組みだけでは実現できない(**図4**)。

計装制御システム向けのセキュリティ監視では，汎用セキュリティデバイスでの監視の仕組みに加え，プラント設備のパラメータ情報や，プラント運転情報の異常からセキュリティ事故を検知・分析するセキュリティ統合管理システムを実現する。将来的には，入退室情報などの物理セキュリティ情報とサイバーセキュリティ情報を組み合わせ，システム操作の妥当性(承認された人が承認された設備を用いて適切な操作をしているか)を判断することで，より高度な監視を実現する。

(注4)　ネットワーク上の不正アクセスを検知し，管理者に通報するシステム。
(注5)　機器やソフトウェアのログを一元的に管理し，セキュリティ上の脅威となる事象を検知・分析するセキュリティソフトウェア。

4.2　セキュリティ事故対応組織の確立

一般的に，セキュリティ事故対応を行う組織として，セキュリティ監視に当たるSOCやセキュリティ事故が発生した際に緊急対応に当たるCSIRTといった部門を構築し，セキュリティ事故対応に備える。

サイバー攻撃は犯罪であるため，これらの部門以外に，法務部門，広報部門，IT部門などとの連携が発生し，外部機関では，警察，国など，幅広い部門との連携が発生する。

発電所には，プラント運転状態を監視する中央制御室や，不正侵入，施設への入退室などの物理セキュリティを監視する詰所などの既存の監視組織が存在する。計装制御システム向けのSOC，CSIRTを構築する際は，これら既存組織との連携(業務統合・分担)を考慮した組織を策定する必要がある。

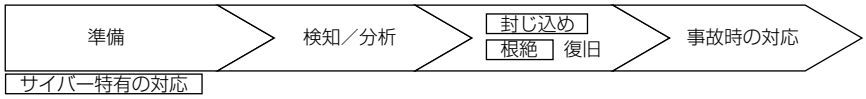


図5．セキュリティ事故発生時の復旧対応フロー

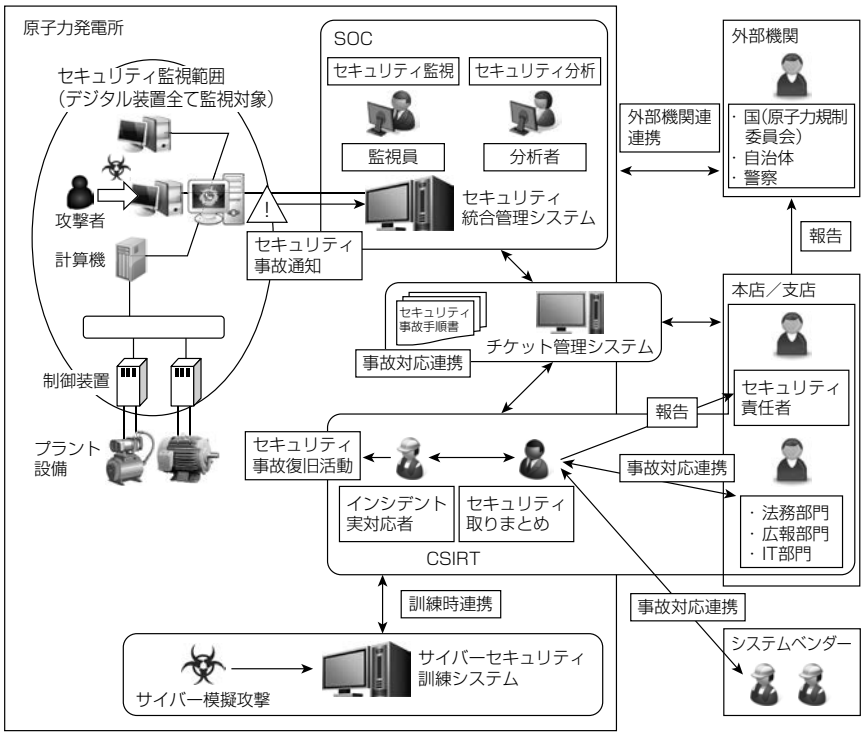


図6．セキュリティ運用の全体像

また，関連組織が幅広く存在するため，セキュリティ事故発生時の情報共有が困難となる。米国政府向けの技術支援，研究開発を行う非営利組織であるMITRE社が発行している“Ten Strategies of a World-Class Cybersecurity Operations Center[6]”では，セキュリティ事故の情報や対応状況をチケット(Ticket)として管理し，関係部門間でチケットを共有するシステム(Ticketing System)の必要性を提示している。計装制御システム向けにもSOC，CSIRT，関連組織にこのチケット管理システムを適用し，関連組織間での情報共有を実現していく。

4.3　迅速な復旧対応

セキュリティ事故発生時は被害が拡大する前に一刻も早い復旧が求められる。緊迫した状況下でミスなく対応するために，**図5**の対応フローに沿った手順書を整備し，発電所の作業員で対応可能な警報表示方針で実現する。

4.1節で述べたとおり，情報システムはシステム内の個人情報，資産情報などの情報資産の機密性を保持する必要がある。そのため，セキュリティ事故と判断されるとシステムを停止して情報資産の機密性を保持した状態で復旧対応に当たる手順書を準備することが多い。

一方，計装制御システムは，プラント運転の継続，つまり，可用性を保持する必要がある。そのため，プラント運転への影響(停止判断)に着目したセキュリティ事故通知方針，手順書の策定が必要である。

また，サイバー攻撃特有の作業(封じ込め，根絶)は，従来の設備故障などによるプラント事故対応では実施しない作業となる。新しい作業に対しての習熟性を向上させるためには，日常的なセキュリティ事故対応の教育・訓練が重要である。サイバー攻撃を模擬発生させ，事故対応の訓練を実現するシステムを現在開発中である。

4.4　運用要件を実現した発電所セキュリティ運用の全体像

4.1節から**4.3節**の実現によって発電所のセキュリティ運用全体像は**図6**のようになる。

5. むすび

3章の活動を通して，原子力計装制御システムに必要となるセキュリティデバイスを開発し，原子力発電所に段階的に納入してきた。今後は，**4章**の運用面に関する課題解決をSOC，CSIRT，セキュリティ統合管理システムなどによって実現し，原子力発電所の更なる安全性の実現に貢献していく。

また，サイバーセキュリティ対策には専門的な技術が不可欠であることから，当社の研究所とも連携して活動を継続していく。

参考文献

(1) Guide for Conducting Risk Assessments, NIST Special Publication 800-30, (2012)
(2) ISO/IEC 27001:2013 Information technology-Security techniques-Information security management systems-Requirements
(3) Nuclear Security Series Publications http://www-ns.iaea.org/security/nss-publications.asp
(4) Regulatory Guide 5.71：Cyber security programs for nuclear facilities, U.S.Nuclear Regulatory Commission (2010)
(5) サイバーセキュリティ装置“MELARROW”，三菱電機技報，**90**，No.1，11 (2016)
(6) Zimmerman, C.,：Ten Strategies of a World-Class Cybersecurity Operations Center, The MITRE Corp. (2014)