推奨プラクティス：
工業用制御システムにおける
サイバーセキュリティインシデント
対応能力の開発

制御システムセキュリティプログラム

National Cyber Security Division：
米国国土安全保障省
国家サイバーセキュリティ部門

2009年10月

邦訳：
一般社団法人 JPCERT コーディネーションセンター

本翻訳文書は、一般社団法人JPCERT コーディネーションセンターが、原書の著作権を保有する アメリカ国土安全保障省（U.S. Department of Homeland Security : DHS）の許諾を得て翻訳したものです。

日本語版の内容について、原書に沿ってできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありませんので、必要に応じて CSSP (Control Systems Security Program) のホームページより原書 "Developing an Industrial Control Systems Cybersecurity Incident Response Capability" をご参照ください。

また、翻訳監修主体は本文書に記載されている情報により生じる損失または損害に対し、いかなる人物あるいは団体にも責任を負うものではありません。

なお、当文書に関わる最新情報は以下の CSSP のホームページをご参照ください。

http://www.us-cert.gov/control_systems/

要旨

この国の力、成長、繁栄は、主要なリソースと健全に機能するインフラによって維持されている。こうしたインフラの多くは、さまざまな工業用制御システムによって支えられている。工業用制御システムという言葉は、監視制御とデータ取得、プロセス制御、分散制御、及び国の重要なインフラの制御、監視、管理を行うその他のシステムを指す。重要なインフラと主要リソースは、農業・食料、銀行及び金融、化学、商用施設、通信、重要な製造業、ダム、防衛産業基盤、救急サービス、エネルギー、政府施設、保健公衆衛生、情報技術、国定記念物・建築物、原子炉、資材・廃棄物、郵便・運送、輸送システム・水の18の分野からなる。簡単に言えば、制御システムは情報を収集し、決められたパラメータと受け取った情報に基づいて機能を実行するものである。

工業用制御システムは、従来のビジネス情報システムと同様、悪意のあるさまざまな攻撃元から攻撃を受ける可能性が増している。こうした攻撃は、注目されることを目的とするハッカーから、設備や施設に損害をもたらす、高度な国家レベルの狙いまでさまざまである。攻撃元は、不満を持つ従業員、競合相手、そして不注意でサイトをマルウェアに感染させてしまう友好的な相手の場合もある。

本文書は、制御システムを利用する施設が、攻撃元を問わずサイバーインシデントに備え、対応するのに役立つ推奨事項を示す。そして、インシデントから得た教訓を活かし、潜在的攻撃に備えてシステムを強化する方法も提案する。本文書には、従来の情報技術において認められている手段や方法も含まれているが、主に工業用制御システム固有の側面に焦点を当てている。

エグゼクティブサマリ

本文書は、施設内または組織内の工業用制御システム（ICS：Industrial Control Systems）の保護に関心のある者を対象とした推奨事項を示す。そして、ICSに脅威を与えたり、損害をもたらしたりするサイバー関連インシデントへの備えと対応に重点を置いている。すなわち、インシデントに対する備えや防止方法だけでなく、インシデントが発生した場合の対応、分析、復旧の方法についても取り上げる。

インシデント対応の概念は、ほとんどの人にとっては、自然災害による緊急事態への対応という文脈でなじみがある。基本原則は、防止、準備、計画、インシデント管理、復旧、緩和、是正、インシデント後分析、教訓など、サイバーインシデント対応の原則と同様である。サイバーインシデント向けの対応では、特にコンピュータ及び関連テクノロジを利用する、悪意のある当事者が引き起こした、負の影響をもたらす事象が対象となる。本文書では、たとえば物理的セキュリティの問題及びサイバー関連以外の問題は取り上げない。

本文書の推奨プラクティスは、特にICSを対象としたサイバーインシデントに絞って示されている。従来の情報技術（IT）のインシデント対応は、何年にもわたって定義されてきた。しかし、ICS固有の特徴に対応する関連の情報と技術はようやく登場し始めたばかりだ。ICSには、その独自の環境に複雑性を加える制約が存在する。たとえば、多くのシステムは10年以上経過し、セキュリティで保護されていないプロトコルとアーキテクチャを使用しているという事実に関係なく、主要なシステムすべてを稼動させ続けなければならない必要性や、標準に基づかないインタフェースやプロトコルをサポートする必要性、そしてベンダサポートが得られない可能性のある機器を維持するという課題が存在する。こうした制約によって、ICSへのサイバーインシデント防止と発生時におけるインシデント対応が共に複雑になる。

本文書は、ICSに対するインシデント対応を管理しなければならない担当者向けの一般的推奨事項を示す。インシデント対応に関連するすべての活動を詳細に取り上げることが目的ではないが、本文書は、個々の関連領域に関する詳細を提供する参照文献の明示を心がけている。本文書は、従来のIT関連文書に記されている一般的な手法を解説するものではないが、ICS環境に固有の領域については重点的に取り上げている。

本文書は、4つの主なセクションに分かれている。1つめのセクションは、サイバーインシデントに関する計画の作成に焦点を合わせ、サイバーインシデント対応チームの設立や適切な要員、方針、手続きを定めた対応計画の作成について解説している。2つめのセクションでは、インシデントの防止を取り上げる。インシデントの防止は、サイバーインシデントの影響の重大度を軽減できるため非常に重要である。3つめのセクションはインシデント管理を取り上げ、（1）潜在的問題または実際の問題の検出、（2）事象の封じ込め（特にサーバにインストールされたマルウェアに関連する場合）、（3）マルウェアの根絶を含む是正、そして（4）事象からの回復とシステム機能の完全復旧について説明する。最後の4つめのセクションは、インシデント後分析を取り上げている。インシデントをよりよく理解するために必要な原因、アクセス経路、脆弱性、及びその他の情報を調べることに加え、サイバーフォレンジックやデータ保存を含め、将来のインシデント防止方法についても解説する。

本文書は、対応能力の確立に関心のある者を含め、ICS固有のサイバーインシデント対応の必要性を認識する資産所有者による使用を念頭においている。さらに、既存のサイバー対応能力を本文書の考え方に照らし合わせて確認したいものにとっても有用である。

本文書は、一般の推奨事項を取り上げる範囲が限定されているため、サイバーセキュリティのベストプラクティス文書を含め、参考文献リストを本文書の末尾に掲載している。サイバーセキュリティ及びインシデント対応に関連する推奨Webサイトも掲載している。

本文書が示す、サイバーセキュリティインシデント対応のための推奨プラクティスは、アメリカ合衆国の重要なインフラ及び主要リソース分野において、不可欠なプロセスを現在サポートしているICSのセキュリティ強化に利用できる数多くの推奨プラクティスの1つである。

目次

図

表

略語

AGA	American Gas Association（米国ガス協会）
API	American Petroleum Institute（米国石油協会）
CC	Coordinating Center（コーディネーションセンター）
CERT	Computer Emergency Response Team（コンピュータ緊急対応チーム）
ChemITC	Chemical Information Technology Council（化学情報技術審議会）
CIAC	US DOE Computer Incident Advisory Capability（DOE-CIRCに置き換わった）
CIDX	Chemical Industry Data Exchange
CIO	Chief Information Officer（最高情報責任者）
CIP	Critical Infrastructure Protection（重要インフラ保護）
CIRC	Cyber Incident Response Capability（サイバーインシデント対応能力）
CPNI	Centre for the Protection of National Infrastructure（英国国家インフラストラクチャ保護局）
CSET	Cyber Security Evaluation Tool（サイバーセキュリティ評価ツール）
CSIRT	Computer Security Incident Response Team（コンピュータセキュリティインシデント対応チーム）
CSSP	Control System Security Program（制御システムセキュリティプログラム）
DHS	Department of Homeland Security（国土安全保障省）
DOE	U.S.Department of Energy（米国エネルギー省）
ENISA	European Network and Information Security Agency（欧州ネットワーク・情報セキュリティ庁）
FIPS	Federal Information Processing Standards（連邦情報処理規格）
FIRST	Forum of Incident Response and Security Teams
GFIRST	Global Forum of Incident Response and Security Teams
ICS	Industrial Control System(s)（工業用制御システム）
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDS	Intrusion Detection System（侵入検知システム）
IEC	International Electrotechnical Commission（国際電気標準会議）
IEEE	Institute of Electrical and Electronics Engineers（電気電子学会）
IP	Internet Protocol（インターネットプロトコル）

IPS	Intrusion Prevention System（侵入防御システム）
IPsec	Internet Protocol Security
ISA	International Society of Automation（旧The Instrumentation, Systems and Automation Society：国際計測制御学会）
ISAC	Information Sharing and Analysis Center（情報共有・分析センター。特定分野に対応するものが存在する）
ISO	International Standards Organization（国際標準化機構）
IT	Information Technology（情報技術）
IT-ISAC	Information Technology – Information Sharing and Analysis Center
NCSD	National Cyber Security Division（国家サイバーセキュリティ部門）
NERC	North American Electric Reliability Corporation（北米電力信頼度協会）
NIAC	National Infrastructure Advisory Council（国家インフラ諮問委員会）
NIDS	Networks Intrusion Detection Systems（ネットワークベースの侵入検知システム）
NIST	National Institute of Standards and Technology（国立標準技術研究所）
NVD	National Vulnerability Database（国家脆弱性データベース）
PIDS	Protocol-based Intrusion Detection System（プロトコルベースの侵入検知システム）
RTOS	Real Time Operating System（リアルタイムオペレーティングシステム）
SCADA	Supervisory Control and Data Acquisition（監視制御データ収集システム）
SP	Special Publication
U.S.	United States（アメリカ合衆国）
US-CERT	United States Computer Emergency Readiness Team（米国コンピュータ緊急即応チーム）

キーワード

工業用制御システム、サイバーインシデント対応、サイバーセキュリティ、フォレンジック、インシデント管理、インシデントレポート、侵入検知、侵入防御

推奨プラクティス

工業用制御システムにおけるサイバーセキュリティ

インシデント対応能力の開発

1. 序文

インシデント対応という概念は、ICS（Industrial Control System:工業用制御システム）やコンピュータよりもはるか以前に存在していた。この考え方は、事業または組織に影響を及ぼす可能性がある、予期しない、負の影響をもたらす事象に対する備えと対応策に基づいている。インシデントの原因は、故意でない場合（嵐や洪水などの場合）と故意の場合（施設に侵入し、設備や備品を盗んだり、損壊したりする侵入者や破壊者などの場合）がある。原因によらず、組織に影響を及ぼすマイナス事象に対して備え、適切に対応することは、常に良い事例を提供してきた。工業界では、何年にもわたって重要な設備や業務に負の影響をもたらす出来事に対し、緊急時対応計画を作成してきた。たとえば、資産所有者のほとんどが、予防的保守プログラム、緊急用バックアップ電源、予備の設備を用意している。しかし、ごく最近では、資産所有者は、ICSに対するサイバー脅威に直接関係するインシデントに直面している。

サイバーインシデント対応及びサイバーセキュリティは、従来の情報技術（IT）組織にとっては目新しい問題ではないが、これらは今、ICSベンダ及び資産所有者の関心を集めている。ICSは従来、外部の多くの影響から分離されたスタンドアロンのシステムで構成されていた。技術、性能、コスト低下といった要因が重なった結果、かつては分離されていたシステムは、共通の通信プロトコルとアクセスポイントを持つネットワークを介して接続された、より新しい統合システムに置き換えられたり、アップグレードされたりすることが多い。こうした状況は、工業用制御システムを直接的または間接的にインターネットからのアクセスに対して開放し、ITに損害をもたらしてきたものと同じセキュリティ上の脆弱性にさらす可能性を有している。こうした脅威の拡大にもかかわらず、ICSの領域では、セキュリティ意識、そして効果的な方針及び行動の面で遅れている。皮肉なことに、サイバーセキュリティインシデントに対する迅速で効果的な対応の必要性は、従来のIT事業環境よりもICS環境の方が高いと考えられ、対応が有効であるためには、これまでとは異なる点を重視し行動をとる必要がある。

IT業務システムで展開される標準的なサイバーインシデント是正措置は、ICSサイバーインシデントにそのまま適用しても、稼働中のICS固有の事柄について事前に検討し計画しなければ、効果がないどころか大損害をもたらす可能性がある。ICSサイバーインシデントへの対応に必要となる迅速性と効果的な行動は、そのインシデントに先立ってどれだけ検討を行い、計画を立てるかによって直接決まる。サイバーインシデント対応チームは、インシデントの事前に確立し、周到な訓練を行う、関連するセキュリティ計画、方針、手順について周到な準備が求められる。

本文書は、従来のIT環境で適用されてきた実績のあるプラクティスを活用して、どのようなインシデント対応を、どのようにICS環境に適用するかを従来のIT環境との相違点を明らかにしながら検討する。本文書は、サイバーセキュリティ及びサイバーインシデント対応管理を扱う上でプロセスエンジニアが直面する特有の課題に対し、推奨される対処方法を示す。

1.1 対象読者および範囲

本推奨プラクティスは、サイバー攻撃からICS環境を守ること中心としたコンピュータサイバーインシデント対応能力の開発を担当するチームを対象に作成された。具体的には、オペレーションマネージャ、プラントマネージャ、プロセスエンジニア、セキュリティ専門家、ネットワーク管理者、及び法務や物理的セキュリティの専門家、その他のIT専門家が対象である。対象者は、関与する人がさまざまな責任を負うような小規模組織では少数にとどまる場合もあれば、業務内容がサイバーセキュリティの特定の面に限定される専門家が集まった大規模グループの場合もある。

本文書は、ICSに関連する、特化されたサイバーインシデント対応能力の開発方法に関する俯瞰的な手引を提供するとともに、より詳細な情報を知るための参考文献や関連文書を紹介する。本文書は、ITにおけるインシデント対応プログラム作成について提供されている文書を書き直したり、整理したりしたものではない。数多くの優れた文書がすでに存在し、容易に入手できる。本推奨プラクティスは、背景情報、ベストプラクティスを提供するのに加え、ICSサイバーセキュリティチームが直面する特有の問題に適用するために、実績のあるインシデント対応プログラムから参考にすべき検討事項を示す。内容は技術的なものではないが、読者にはICS環境についてはもちろん、ITのアーキテクチャ及びプラクティスの基本を理解していることが期待される。本文書におけるICSの定義には、プロセス制御システム、SCADA（Supervisory Control

and Data Acquisition : 監視制御データ収集システム）、組み込みシステム、及びDCS（Distributed Control System : 分散制御システム）が含まれる。他の規制手引書では、IACS（Industrial Automation and Control Systems : 工業自動化及び制御システム）に言及するものもあるが、本章ではすべてICSと呼ぶ。

本文書は、サイバーインシデント対応に関連する、特定分野の標準、指針、要求事項を置き換えるものではない。一部の分野では、関連する規制を遵守するために、非常に具体的で詳細なインシデント対応計画が要求されるが、それ以外の分野や業種では要求されない可能性がある。どちらの場合であっても、サイバーインシデント対応能力を確立して施行し、リスクに対する具体的取り組み及び計画の実施を資産所有者に委ねる必要がある。本文書は、インシデント対応能力を開発しようとする者に助言と手引を提供する。

1.2 背景

サイバーインシデント対応とは、ICS所有者の資産またはICS所有者の運営能力に影響を与える可能性のある、認識されたサイバー関連インシデントに対し、組織がどのように対応するかを指す。対応を誤ると、無秩序で逆の影響をもたらす、効果のない行動をとったり、損害を拡大させたりする恐れがある。いかなる組織でも、会社の業務に与える影響を最小限に抑えながら、計画に基づいた円滑な対応に努めるべきである。これを達成するには、サイバーインシデントが発生する前に、計画と手順を整えてテストしておく必要がある。

サイバーセキュリティの対象となる、ICSを含む環境では、インシデントはコンピュータネットワーク及び設備への不正なアクセスと、資産所有者に何らかの負の影響をもたらす行動を伴うのが一般的である。損害には、データの盗難、個人または会社に関わる機密情報の暴露、主要サービスの中断、生産業務の停止、物理設備や環境の損傷、公開Webサイトの改ざんなどが挙げられる。侵害による経済的及び社会的影響は、マイナスの評判、顧客からの信用喪失、訴訟の可能性、生産業務中断や設備の交換、及び修復による財政上の直接的損失を考慮すると、きわめて重大なものとなる恐れがある。

ICSを含め、組織のコンピュータネットワークへの侵入に成功される可能性は、組織の業務システムまたはインターネットのいずれかに、直接、間接を問わず接続されているシステムすべてにおいて高いといえる。注目度の高い会社や政府機関の多くが、日に数千回もアクセスの試みがあると報告している。攻撃者は、偵察、ボットネット、バックドア、ソーシャルエンジ

ニアリング、隠れたマルウェアなど、さまざまな技法を駆使して、サイバーセキュリティの脆弱性を試す。攻撃の多くは、正しく設定されたファイアウォール、従業員に対するサイバーセキュリティ意識向上訓練、ドアの施錠など、基本的なセキュリティ対策を実施することで容易に阻止できる。しかし、非常に経験の豊富なハッカーや侵入者からの保護は非常に困難な場合がある。それほど能力のないハッカーであっても、新たなExploitが紹介されてから、その攻撃に悪用される脆弱性を修正するパッチをベンダが配布するまでの間に、システムへの侵入を許してしまう（ゼロデイ攻撃）。ベンダがパッチをリリースしてからICS所有者がパッチを適用するまでの間も、能力の高くない攻撃者に対して、さらなる攻撃の機会を与えることになる。

ICS環境では、パッチの適用は重要度及び業務に影響を与える可能性が高く、適用の前に徹底した互換性テストが必要となる場合があるため、パッチのリリースから適用までの期間がより大きな問題となる恐れがある。こうしたパッチは、製品が依然サポートされている場合でもベンダがすぐに開発しない場合があったり、テスト要件が特殊である、需要が限定的であるという理由から数か月遅れる可能性もあったりする。

何らかのインシデント発生の可能性を、組織に及ぶ影響と併せて考慮すると、こうしたICS固有の問題に対応するインシデント対応能力が必要であることがわかる。

サイバーインシデント対応能力は、インシデントを予防する事前対策的な要素、またインシデント発生後に組織による対応を改善するための要素がいくつか含まれなければならない。これらの要素には、計画立案、インシデント予防、インシデント後分析/フォレンジックがあり、図1に緑色で示した。それ以外の要素は、インシデント発生後のインシデントの検知と管理を中心とする。これらは性質上、事後対応的な要素であり、通常、厳しい時間的な制約と高い可視性の下で実行される。これらの要素は、検知、封じ込め、是正、回復と復旧であり、図1に赤色で示す。

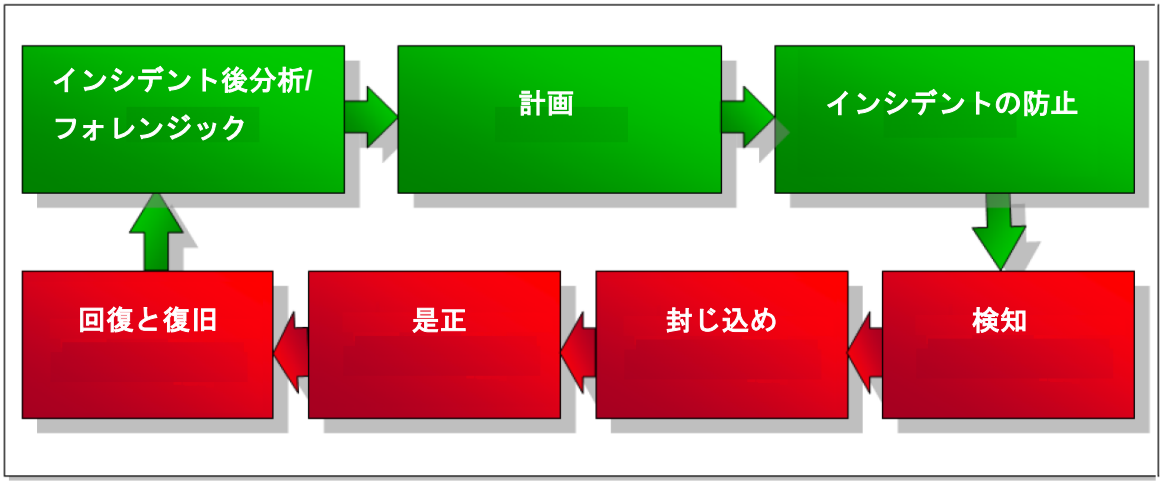

図1 インシデント対応の主要要素

効果的なインシデント対応能力の開発を支援するために、権威の確立されたインシデント対応組織が提供する既存の手引書を入手し、精査するべきである。これらの文書を評価し、インシデントに対応する組織の具体的な任務または趣旨に適合する内容を決定できる。コンピュータインシデント対応チームを開発する方法については、多くの情報を入手できる。分野固有の文書（ガス、石油、エネルギー、核、化学など）はもちろん、米国、英国、欧州連合が提供する手引書も、無料またはわずかな費用で容易に入手できる。本文書の最後及び出典Webサイトにある参考文献セクションには具体例の一覧を示す。以下では、CERT基準能力の確立に役立つ可能性のある、よく知られた他のCERTプログラムを出典とする情報を示す。

アメリカ国土安全保障省（U.S. Department of Homeland Security:以下DHS）のCSSP（Control Systems Security Program）は、ICS-CERT（Industrial Control Systems-Cyber Emergency Response Team）を開発したプログラムである。このチームの設立の趣旨は、重要なインフラ分野すべてにおいて制御システムのサイバーセキュリティリスクを低減することである。このプログラムは、DHSと連携し、ICSに焦点を置いたサイバーセキュリティに関するUS-CERT（United States Computer Emergency Readiness Team）を作成した。ICS-CERTを支えているのは、脆弱性、侵入の方法とツール、そしてICSインシデントを防止または軽減する方法について習熟している専門スタッフである。これらのスタッフはサイバー攻撃手法及び予防対策技術に関する最新情報に精通している。さらに、CSSPは、ICS資産所有者にとってのセキュリティリスクを低減する製

品とサービスを提供している。その他の製品及びサービスとしては、推奨プラクティス、自己評価ツール、ICSセキュリティ文書、調達に関する推奨事項、標準規格への対応が挙げられる。

CSSPの情報は http://www.us-cert.gov/control_systems/index.html から入手できる。

US-CERTは2003年の創設以来、連邦行政府機関へのサイバー攻撃に対する対応の支援と防御、そして州及び各地域の政府機関、業界、海外のパートナとの情報共有と連携を提供することを任務としている。

DOE（U.S. Department of Energy）は1989年、Morris Wormが登場してしばらく後に、CIAC（Computer Incident Advisory Capability）を作った。この組織の任務は、DOE従業員及び請負業者に対し、さまざまなコンピュータセキュリティサービスを無料で提供することであった（“Assessing the CIAC Computer Security Archive,” CIAC-2302 R.1を参照）。この任務は現在、新たに設立されたDOE-CIRC（DOE-Cyber Incident Response Capability）に移行され、DOEに対しインシデント対応、報告、追跡のサービスを提供する責任を負っている。この情報は、DOE以外も利用が可能である。

US-CERT及びDOE-CIRCは、GFIRST（Government Forum of Incident Response and Security Teams）およびFIRST（Forum of Incident Response and Security Teams）のメンバーである。GFIRSTは、政府のITシステムのセキュリティを確保する責任を負うセキュリティ対応チームからの技術専門家と戦術専門家からなるグループである。

CPNI（Centre for the Protection of National Infrastructure）は、旧National Infrastructure Security Co-ordination Centreを吸収した組織で、英国向けにサイバーセキュリティ関連の手引書を発行している。CPNIは、EUの機関であるENISA（European Network and Information Security Agency）と連携している。ENISAは、EU加盟国の専門家センターであり、ネットワークと情報のセキュリティ分野におけるEUの機関である。ENISAは、EU加盟国や民間企業、産業部門を対象としたベストプラクティスに関する専門的なアドバイスや推奨事項の提供を担当する。これら組織におけるCSIRT（Computer Security Incident Response Teams）設立のベストプラクティスについては、本文書の参考文献セクションに示す。

NIST（National Institute of Standards and Technology）は、サイバーセキュリティ全般を取り上げたガイドや刊行物に加え、特にインシデント対応を取り上げたガイドや刊行物を作成している。本文書末に示した参考文献では、全般的ガイドと特別刊行物を紹介している。その他、インシデントの取扱や対応に関する具体的な文書として次のものがある。

- NIST SP 800-40, “Creating a Patch and Vulnerability Management Program（パッチ及び脆弱性管理プログラムの策定）”
- NIST SP 800-61, “Computer Security Incident Handling Guide（コンピュータセキュリティインシデント対応ガイド）”
- NIST SP 800-83, “Guide to Malware Incident Prevention and Handling（マルウェアによるインシデントの防止と対応のためのガイド）”
- NIST SP 800-86, “Guide to Integrating Forensic Techniques into Incident Response（インシデント対応へのフォレンジック技法の統合に関するガイド）”
- NIST SP 800-92, “Guide to Computer Security Log Management（コンピュータセキュリティログ管理ガイド）”

これらの文書は従来のITを対象としているが、ICSインシデント対応の方針と手順を実施するための手引も提供している。

政府が提供する情報のほか、民間の専門家によるインシデント対応の情報が数多く提供されている。たとえば、大学や専門学校、ハードウェアやソフトウェアのベンダ、民間の組織や機関、コンサルティング会社の専門家や個人の専門家の情報を入手できる。Carnegie Mellon Software Engineering Instituteの専門家によるIT向けの例として、「*Handbook for Computer Security Incident Response Teams (CSIRTs)（コンピュータセキュリティインシデント対応チーム(CSIRT)のためのハンドブック）*」（Carnegie Mellon University発行）が挙げられる。

2. サイバーインシデント対応計画

サイバーインシデント対応能力を開発する第一段階は、計画及び準備である。可能であればインシデントを予防し、インシデントが発生した場合でも対応できる準備をするために、あらゆる要素を集約する。この後のセクションでは、計画及び準備の段階（図2参照）について説明する。

サイバーインシデント対応能力は、対応チームの編成、組織の方針と手続きの確立、対応計画自体の作成、チーム内外への報告と連絡の方法決定、計画が想定通り機能するかの検証、事象発生時におけるチームを支援する状態/状況レポートの有効化、といった要素で構成されている。

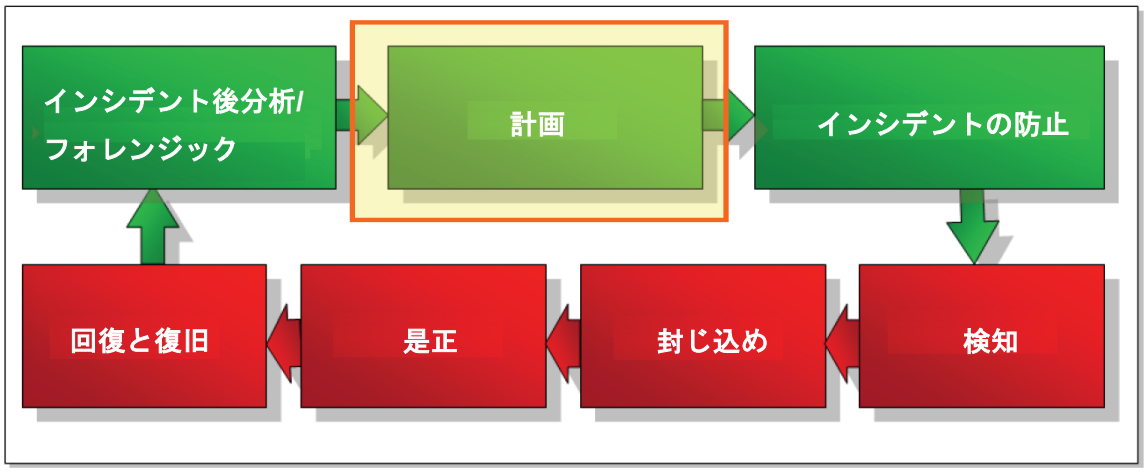

図2 計画および準備の段階

2.1 チームの編成

インシデント対応能力を開発する最初の段階は、チームの編成である。ほとんどのグループは、通常CSIRTと呼ばれるチームとして編成される。CSIRTは、インシデント対応専従の専門家で構成される場合と、別に日常的な責任を担っている兼務のスタッフで構成される場合がある。本文書では、CSIRTはICSを直接サポートする、内部の対応チームを指すものとする。その他の外部対応チームは、特定の技術領域、地理的または組織的区分に基づいて組織される。

2.1.1 チームの責任

CSIRTの責任は、資産所有者の組織規模と構造によって異なる。そして、従来ICSセキュリティチームに支援を提供していなかった、異なる部門間で責任が共有される場合もある。第三者の参加は、設備ベンダまたはコンサルタントや他の専門家との間でベンダサービス品質保証契約を通じて求めることができる。この選択肢は、リソースが限定されている資産所有者にとって必要となる場合がある。

サイバーインシデント対応チームの責任には以下が含まれる。

- サイバーセキュリティの脅威及び脆弱性に関する専門的リソースとして行動する
- インシデントの予防、情報、分析に関する情報センターとして機能する
- インシデント対応に関する、組織の方針と手続きを作成する
- ICSの保護手段を理解する
- インシデント発生時に組織に及ぶ運営上の影響を特定する
- インシデント対応計画の作成とテストを行う
- 内部で報告されるインシデント及び疑わしいインシデントすべてを扱う、一元化された連絡先として行動する
- インシデント発生時に対応する
- インシデント後、主要な利害関係者及び外部機関（ICS-CERTや警察など）に報告する
- 分析及び法的措置を支援するフォレンジック情報を収集する
- インシデントの再発を防止する保護手段を実現する
- インシデント後、ICSを是正する

2.1.2 チームの編成

CSIRTの編成についてはさまざまなモデル[a]が示されている。ICS環境に最も適用しやすいCSIRTモデルは、集約された対応チームか、分散された対応チームかのどちらかである。一元

[a] CSIRT モデルに関する詳細については、『Organizational Models for Computer Security Incident Response Teams (CSIRTs)』（2003 年 12 月；Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle, Mark Zajicek）というタイトルの Carnegie Mellon University ハンドブックを参照。

化されたサイバーインシデント対応チームは、さまざまな規模の組織にみられ、さまざまな背景を持つ個人で構成される。一元化チームで際立っている特徴は、ICSに地理的に近接している点である。一元化チームの場合、サーバ、ネットワーク、監視設備、エンジニアリングワークステーション、及び物理的設備に接続される制御装置は、通常すべて1カ所の施設に存在する。一元化チームは現場で作業し、あらゆるインシデント対応活動を実行する。このモデルは、可能であれば推奨される手法である。なぜなら、複数チーム間のやりとりに関連して生じるオーバーヘッドが削減され、現場でのアクセス、制御、分析に余裕をもたせることが可能だからである。分散対応チームには、中心となるCSIRTが含まれる場合もあるが、組織の場所が物理的に離れているため、複数チームが存在するか、または複数チームが必要となる。このモデルは、施設が複数の州（または国）に分散して存在し、1つのチームが何らかのインシデントにタイミングよく対応することができない場合に適用される。さらにこのモデルは、地理的に分散した大規模な組織においても必要となる。その場合、遠隔地のチームには、請負契約を結んだ専門家やパートタイムのスタッフが含まれることもある。この手法は、チーム間の連絡と連携をより重視する必要があるが、インシデント発生源である現場に遠隔地のチームがいることが可能になる。分散した組織では、強力な中心となるCSIRTに加え、遠隔地には自己完結した個別のCSIRTを配置することが推奨される。計画、予防、分析、フォレンジックは、規模の効率性を考慮し、すべて中心グループから提供することができる。ただし、インシデント対応は、現地のCSIRTがインシデント発生時に先頭に立ち、組織の中央のスタッフの支援を受けながら、現場で直接行われなければならない。

本文書は、スタッフ配置については取り上げていないが、スタッフ配置について詳細に述べた優れた刊行物が入手できる[b]。もっとも、対応チームの編成にあたっては、ICSに関連する以下の2つの課題に取り組まなければならない。

- IT環境は、ネットワーク構成、オペレーティングシステム、設備のどれもが動的に変化している。一方、ICS環境は構成が固定されていることが多く、一般的に現場や業務に固有の構成を持つ、独特で、場合によっては旧式の装置で構成される。一般的なICS設備を扱う場合でも、その使用方法と、障害時に生じる影響は、必ずといっていいほど対象組織固有である。残念ながら、環境にかかわるこうした知識を持っているのは多くの場合、ごく少数の主要な制御システムエンジニアに限られている。これは、限られた人的資源で継続的な

[b] スタッフ配置に関する詳細については、NIST Special Publication 800-61, “Computer Security Incident Handling Guide,”（20041 月、pp. 2.82.16）を参照のこと。
その他に、CSIRT に関する前出脚注（a）で示した CMU のハンドブックも参照のこと。

対応を提供するという問題をさらに深刻なものにする。継続できた場合でも、従業員が疲弊したり、離職率が上昇したりする恐れがある。これらのシステムを保守、運用するためには特別な知識が必要であるため、どちらの場合も悪影響が生じる。チームの編成では、割り当てについて考慮しなければならず、できる限り多くの作業や責任を主要でないスタッフや請負業者に委任することも検討する必要がある。

- スタッフ配置の決定は、権限の区分に対応していなければならない。ITでは、決定は通常、CIO（Chief Information Officer）、IT担当重役、または同等の役職に委ねられる。ICS運用の責任は、プロセスの中断に細心の注意を払っているプラントマネージャが担うことが多い。プラントマネージャも従来のエンジニアリング分野の出身である場合があり、サイバーセキュリティの問題に対する意識が十分でない可能性がある。経営陣は、いかなる業務も停止しないようプラントマネージャにプレッシャーをかけることも考えられる。権限に対する同意を得た上で、インシデント発生前にCSIRT、運営部門、エンジニアリング部門、及びIT管理部門との間で理解が確立されていなければならない。こうした組織はそれぞれ、重要な知識やスキルをチームにもたらすことができるが、CSIRTは始めから適切なレベルの権限を持っていなければならない。でなければ、プラントの運営が危険にさらされている間、権限の決定に貴重な時間を費やすことになる。

2.1.3 役割の分担

すべての組織が各ポジションにスタッフを直接配置できるわけではないが、個々の役割を明確にし、割り当てる必要がある。スタッフが複数の役割を兼務したり、ICSインテグレータやICSのベンダやメーカーからの要員であったりしても同様である。需要の大きい大組織や、冗長性を確保したい場合、1つの役割に複数の人を割り当てることもできる。これは特に、特有の知識や経験を持つプロセスエンジニアやオペレーションエンジニアの場合にあてはまる。CSIRTの各役割は下記のとおりである。

- **CSIRTチームマネージャ**　チームが統率され、目標を達成することを確認する責任を担う人を1名割り当てる必要がある。CSIRTチームマネージャは、自身が技術面の指導的立場に立つか、または別にCSIRT内の誰かを技術面の指導に当たらせる。チームマネージャは、会社の利益を最優先に考えて行動するための権限を経営陣から与えてもらう必要がある。CSIRTの機能を外部に委託する場合も、チームマネージャが請負業者の行動、作業、契約内容を監督しなければならない。チームマネージャは、コンピュータインシデントの緩和、

封じ込め、解決を適切なタイミングで成功させるための主要リソースを集める上で重要である。

- **プロセス/制御システムエンジニア**　プロセス/制御システムエンジニアは、対象制御システムアーキテクチャの専門家であるべきで、ICSが生産またはサポートするシステム構成要素及び製品を把握し、理解している必要がある。この人物は、正常時と異常時における設備の機能と機能サイクルだけでなく、ICS内の構成要素がサービスから取り除かれたときに生じる可能性のある影響に関する重要情報も提供する。プロセスエンジニアは、設備障害の解決法や回避策、必要に応じて業務を再開する方法をCSIRTが理解する上で重要な役割を果たす。

- **ネットワーク管理者**　ネットワーク管理者は、インシデントがコンピュータネットワークを発生源とするサイバー攻撃に関係する場合、CSIRTにおいて重要な役割を果たすことができる。この人物は一般に、セキュリティ上の脆弱性、パッチ適用、侵入検知、システム監視など、ネットワークアクセスについて精通している必要がある。サイバー関連の事象の事前、最中、事後における、ネットワークスイッチ、ルータ、ファイアウォールの活動ログに関する知識と入手可能性は、インシデントの範囲と複雑さを知る上で重要であり、発見された脆弱性を解決、是正する方法に関する手がかりを与える。ほとんどのサイバー関連インシデントはネットワークが関係しており、ネットワークに精通したネットワーク管理者がインシデントを発見し解決する鍵を握る。

- **システム管理者**　システム管理者は、本来、制御システム管理者であるが、現代の組織では高度な統合がなされているため、IT管理もその職務に含まれる場合がある。システム管理者は、影響のあるサーバにおけるアクセス権及びシステム運用ログについて精通している必要がある。システム管理者は、プロセス制御操作及び業務サイクルについて精通している場合もある。さらに、個々のシステムの現在の状況を把握し、潜在的な脆弱性を認識しておく必要がある。システム管理者は、ベンダやサプライヤとの窓口となる場合もある。

- **プラントマネージャ（ICS/制御センターマネージャを含む）**　プラントマネージャは、インシデント対応計画の詳細の大部分には関与しない可能性があるが、インシデントが特定された場合のリスク評価プロセスの一部として、業務中断の権限の割り当てに関与しなければならず、CSIRT業務の財源を確保したり、経営陣や外部（報道関係を含む）との連絡係として活動したりしなければならない。

- **IT担当重役、CIO、チーフエンジニア**　この役割は、責任という点ではプラントマネージャに似ている。IT担当重役とプラントマネージャという2つの管理監督の職位は不可欠であり、権限の委譲やインシデントに適用するリソースについて連絡を取り合い、調整しなければならない。最新の制御システムは通常、既存のITネットワークや業務システム、通信設備と統合されている。

- **セキュリティ専門家**　セキュリティの専門知識には、物理的セキュリティと法の施行が含まれるが、本文書では主に、サイバーセキュリティの専門知識を取り上げる。セキュリティ専門家は2つの役割を果たす場合があるが、脆弱性、Exploit、予防技術に関する深い知識を持ち、特にインシデント予防法及びインシデント発生時の回復方法を理解している人材を準備しておく必要がある。セキュリティ専門家は、場合によっては、犯罪活動の特定や起訴手続きの支援にあたることもある。

- **法律の専門家**　法律の専門家は、1）国内、国際、連邦、州におけるあらゆる法律と規制に対するコンプライアンス確保、2）提訴時に認められる証拠の説明、3）証拠収集の方法の明示、4）第三者による保守の場合の責任範囲、5）プライバシーの侵害など、避けるべき落とし穴をチームが理解するための支援、といった領域で必要となる。法律の専門家は、チームによるインシデント計画作成時、状態/状況レポートを有効化するとき、及びフォレンジックやデータ収集時に非常に有用な存在である。大規模な組織では、社内に法務部門を抱えている場合がある。小規模組織では、法律面の支援を外部に求める場合があるが、このような場合は、インシデント対応に具体的な経験のある法律事務所に連絡を取るべきである。

- **広報スペシャリスト**　広報スペシャリストは必要に応じて参加させる。この人物は、インシデントがサービスを大きく中断させたり、組織の製品提供能力に悪影響を及ぼしたりした場合に重要な役割を果たす。発電や下水処理など、組織が一般の人々に対して直接サービスを提供している場合に特に重要となる。広報スペシャリストは、報道媒体を通じ適切な情報とメッセージが確実に一般の人々に送られるようにする責任を担う。

- **人事スペシャリスト**　人事スペシャリストは、インシデントが組織内部の人間によって試みられるか、実行された場合に、CSIRTの活動に参加する。法律に関連する事項、方針、手続き、処罰行為は通常、この人物が扱う。

- **ベンダサポートエンジニア**　ベンダの技術スタッフは専門的で重要な知識を持っているため、インシデントに関係する設備とシステムについて資産所有者に技術的な支援を提供できる、ベンダ側の人物を明らかにしておく必要がある。ベンダサポートエンジニアは、CSIRTでは見つからない情報や見解を提供することができる。たとえば、彼らの持つ専門知識は、資産の復旧に役立つだけでなく、必要な場合にはカスタムパッチの作成にも役立つ。
- **その他の支援スタッフ**　その他の専門知識が必要な場合は、支援要員をCSIRTに追加できる。追加する支援要員としては、必要に応じて弁護士や警察関係者、コンピュータフォレンジックスペシャリスト、リスクマネジメントスペシャリスト、データベース管理者、アプリケーション開発者、プラットフォームスペシャリスト、政府機関などが挙げられる。組織のサポートとスケジュール管理または方針や手続きの用意といった日常業務については、秘書やテクニカルライター要員が有用である。

CSIRTモデルが分散型の場合、上記に示したうちできるだけ多くの役割を中央の事務所に配置し、遠隔地にはそれぞれ一定の技術スタッフを配置するべきである。少なくとも、プロセスエンジニアリング、システム管理、及びネットワークに関する経験者を、分散している遠隔地それぞれに配置すべきである。インシデント自体が通常の通信経路を妨げる可能性があるという認識のもと、通信はインシデント発生時にも有効かつ信頼できるものでなければならない。

ロジスティック要素は詳しく取り上げないが、チームに推奨されるインフラとして、恒久的または一時的な「作戦室」、モバイル通信機器、ラップトップ、及び利用可能な文書（方針、計画、手続き、電話番号リストなど）が挙げられる。これらはすべて、インシデントの影響が及ぶ可能性の少ない場所に用意する。

CSIRTの第一の目的は、サイバー関連インシデントに対処することであるが、対応チームは、ICSやSCADAシステムの停止、設備の壊滅的障害、洪水や台風などの自然災害といった、サイバー関連でない出来事にも活用できる。

2.2　方針及び手続きの設定

方針及び手続きを決めておくことはほとんどのビジネス機能において重要であるが、生産停止や多額の金銭的コストを伴うプレッシャーの下、そして多くの場合、非常に不都合なタイミングで、また、権限を持つ人がすぐに対処できない可能性のある状況において決断が下され

るため、インシデント対応も重要である。チームメンバーが重圧にさらされない状況で手続きと支援方針を作成することが非常に重要である。作成時において、チームメンバーは選択肢の比較検討、方法のテスト、影響と代替策の分析、経営陣の指示や承認の獲得を行うことができる。一般的なサイバーセキュリティ方針[c]の多くは、IT保護と制御システム保護の両方に役立つ。本文書においては、インシデント対応関連の方針は、ICS組織内で確立し、公開するべきである。

インシデント対応方針を実行するために、明確かつ詳細な運用手続きを作成すべきである。インシデント対応計画に含まれる手続きは、サイバー緊急事態以外における手続きと似ており、事象の発生前にテストすべきである。手続きの構造、正確さ、適時性に存在する問題は、実際の対応時ではなく、調整が可能な開発段階に見つけ出しておくべきである。

初期インシデント対応方針は、CSIRTの設立を方向付け、インシデント対応計画の基礎となるべきである。インシデント対応計画は、CSIRTの権限を定義するものである。方針は、インシデント対応計画内で定義される手続きと行動の根幹となる。その他に検討すべきセキュリティ関連の方針が数多く存在するが、ICSとの関連性が高いものは次のとおりである。

- **人的資源**　組織内の誰かがインシデントの原因の場合に、従業員や請負業者に対してとる行動を踏まえた方針を定めるべきである。この方針は、インシデント検出時の当面の対応と行動、調査の実施方法、及び関連の懲罰方針に適用される。
- **情報開示**　情報開示に関する組織の立場、及び情報漏洩時に組織がとる行動に関する方針を定義しなければならない。方針には、連絡先及び報告時の時間的制約も含めるべきである。インシデント対応計画は、盗難される恐れがあり、機密である可能性のある情報に対応するものでなければならない。具体的には、セキュリティ分類レベル、個人情報、ビジネスまたはエンジニアリングのプロセス情報、制御デバイスに存在するベンダ独自のデータまたはコードといった情報が考えられる。
- **コミュニケーション**　インシデントが発生したら、メディア対応とコミュニケーションに関する方針を適用する。方針には、組織を代表して話をする人物を定義する。必要に応じて、ベンダと顧客に対応する担当者も定義する。

---

[c] 一般的なセキュリティ方針の例としては、許容される使用目的、パスワード、バックアップ、リモートアクセス、ワイヤレスアクセス、ゲストアクセス、暗号化、データ分類、保持、VPN ポリシーなどが挙げられる。

- **権限の割り当て**　前述したとおり、制御システム環境では、組織の責任が二重になる傾向がある。プラントマネージャは運営に責任を持ち、CIOは主にICSに接続、またはICSで使用されるネットワークとコンピュータ関連機器の責任を担当する。方針は、エスカレーションリストと権限の区分に加え、特定のマネージャが対応できない場合の委譲（バックアップを含む）について定める必要がある。

2.3　サイバーインシデント対応計画の作成

サイバーインシデント対応計画は、ICSに関するインシデント対応方針を実装する手続きと行動を確立し、文書化するものである。そして、サイバーインシデント対応計画では、セキュリティインシデントを定義し、インシデントに対応して組織の損害を軽減する手順の概略を示す。IT関連のインシデント対応計画のテンプレートや実例は各種入手可能であり、一部は参考文献として示してある。これらのテンプレートや実例は、計画作成に着手するよい手がかりとなる。インシデント対応計画を作成するときは、以下のセクションについて検討する。

1. **概要、目的、目標**　計画内のこのセクションは、達成する内容を定義する。このセクションでは、インシデントに対する対応の選択肢に照らして、ビジネスの全体目標に関する方向性や指針を示すことができる。

2. **インシデントの説明**　ITタイプのインシデントの多くは、かなり容易に分類できる。たとえば、サービス運用妨害攻撃、ネットワークへの不正アクセス、保護されたプライベート情報へのアクセス、Webページの改ざん、サービスの悪用などが挙げられる。

   ICS環境の場合、できる限りセキュリティインシデントの明確な定義を決定し、伝達しなければならない。これは特に、設備の障害や予期しないソフトウェアのふるまいが、サイバーセキュリティインシデント、摩耗による機械的故障、環境条件、またはその他のセキュリティ関連以外の要素によるものかを検討するときに重要である。サイバーセキュリティインシデントとそれ以外のインシデントを理解し、区別することが重要である。設備またはソフトウェアの障害が独立して存在する場合は、交換によって問題が解決する場合がある。障害の原因が脆弱性の悪用、破損したパッチやテスト未実施のパッチの適用による場合、またはマルウェアがシステムやネットワーク上に残存している場合、元の設備や他の同様の設備が危険にさらされている可能性がある。ハードウェアまたはソフトウェアの設定内容がインシデントの根本原因である場合、ハードウェアまたはソフトウェアを交換しても

問題は解決せず、再感染を防止できない。インシデントを正確に説明することも、CSIRTの無駄な発動を防止する。

ICSの場合、サイバーベースのインシデントとそれ以外の原因で生じたインシデントを区別することが重要となる。たとえば、不満を抱える従業員がバールで損害を与えた設備への対応は、未知の攻撃者が同じ設備を不正に操作して損害を加えた設備への対応は大幅に異なる。独自の状況に対し適切な対応をとることができるよう、各インシデントタイプを特定し、定義することが重要である。

3. **インシデントの検出**　これは、インシデントの「発見」とも呼ばれ、インシデントを特定し、報告する方法を含む。明白なインシデントがごくまれに存在するが（ICSネットワークにログオンした状態の侵入者が見つかったり、Webサイトが改ざんされたりするなど）、ほとんどのインシデントは、自動分析ツール、システムの動作パターン、オペレータ、スーパバイザ及びその他スタッフが何に注意しておくべきかを意識することが検出には必要となる。オペレータ及びプロセスエンジニアは、異常な操作を検出する上で非常に重要であり、システム動作の違いに最初に気付く。この違いは、ICSに起きている状況を理解する鍵となる。インシデント対応計画は、自動システム、疑わしい活動が検出された場合にスタッフ、請負業者、パートナに期待すること、及びヘルプデスクとコールセンターのスタッフがとる手続きについて定めていなければならない。

4. **インシデントの通知**　異常な事象が識別されたら、優先的に原因の特定と、小さなシステム事象であるかどうか、または即時のエスカレーションが必要かどうかの判断をする必要がある。インシデント対応計画内のこのセクションでは、インシデント報告に関する連絡先情報を明確にしておく必要がある。このセクションには、内部スタッフ（システム管理者、ネットワーク管理者を含む）の勤務先電話番号、携帯電話番号、電子メールアドレス、インスタントメッセージなどを示す。以下の状況に対応できる情報も明確にしておく。

- 勤務時間外の緊急連絡方法
- オフサイトの連絡番号
- 顧客及びパートナの連絡先
- バックアップスタッフの緊急連絡方法
- 管理監督者の連絡先及びエスカレーションのルール
- 誤ったインシデント認定を除外する基準

- 関連する規制当局の連絡先
- ICS-CERT/US-CERTの連絡番号と情報
- ベンダ/インテグレータの責任内容と連絡先情報

この連絡先情報は、潜在的インシデントを検出する可能性のある者すべてに公表すべきである。運営担当に週単位および月単位で発行される当直連絡先リストは、サイバーインシデント発生時に誰に支援を求められるかをすべての従業員が把握するのに役立つ場合がある。外部機関は他のサイトの事象に基づいて潜在的インシデントを報告する可能性があるため、必要なすべての外部組織にも連絡先情報を提供すべきである。

5. **インシデント分析**　インシデント対応計画内の手続きは、報告されたインシデントを評価、分析する方法を示す。インシデントは、内部のまたは外部の情報源から報告される可能性があり、いつ報告があるかは決まっていない。インシデント管理のこの段階では、報告を受け取る側は以下を判断しなければならない。

   - 当該事象によってもたらされる恐れがある危険、または施設や施設の要員の安全に及ぶ影響
   - 報告されたインシデントが本物か、または誤ってインシデントと判断されたものか
   - インシデントがどの段階にあるか（始まり、発生中、発生後）
   - 組織に及ぶ可能性のある影響
   - インシデントの具体的な種類
   - インシデントに影響を受けた、または受ける可能性のあるシステムと設備
   - システムが、利用可能な予備システムにフェイルオーバー（障害時切替え）したかどうか
   - インシデントが他のネットワーク、または外部のパートナや顧客にまで及ぶ可能性があるかどうか
   - どの組織が影響を受けるか、誰が対応を担当するか

6. **対応行動**　このセクションは、検出されるインシデントの種類ごとに、従うべき手続きを定義しているため、インシデント対応計画にとって不可欠である。インシデントは一般に、もっとも起きて欲しくないときに発生する。スタッフに対するストレスや重圧が高まり、選択肢を試す時間がほとんどなく、すべての行動が管理監督者や利害関係者、場合により

一般の人々によって監視され、評価される。行動を考え抜いて定義し、インシデント発生前にテストすることが重要である。対応行動を定義するときは、以下を考慮する。

- 対応は、インシデントの種類に直接関連づけなければならない。1つの方法がすべての状況に適合することはなく、定期的に新たな攻撃ベクトルについて検討すべきである。
- インシデント対応計画は、夜間、週末、休日、スタッフ不在時、通信機器の不作動時など、万が一の事態に細かく対応するものでなければならない。計画的または予期しない停電など、計画に影響する外的要因にも対処すべきである。
- 計画内で示された行動には、問題の封じ込め、機能する状態への運用の復旧、及び再発の防止をカバーする包括的な対応が含まれなければならない。上述のとおり、行動はインシデントの種類とその重大度によって異なる。
- 対応手続きは、見過ごした要素、誤解されている要素、不完全な要素、不正確な要素を判断できるよう、可能な限り現実に近い状況でテストを行うべきである。すべての懸案事項に対処するまで、修正を行い、再テストする。
- 対応活動は、計画段階の間にビジネスへの影響に照らして比較検討し、承認を取り付けなければならない。是正措置が、インシデント自体よりもビジネスに悪影響を及ぼす場合もある。
- 計画の作成では、ありとあらゆる観点を考慮するべきである。たとえば、技術、法律、コミュニケーション、経営、業務、エンジニアリング、人事といった観点を考慮する。
- 対応行動は、あらゆるフォレンジック要件を考慮しなければならない。フォレンジックは必ずしもすべての事例で必要となるわけではないが、インシデントの種類によっては、犯罪の可能性やその他の法的措置のために情報を特定、保全する必要性を含む手続きが求められる。

7. **コミュニケーション**　コミュニケーションの要素は、対応活動に含めることはできるが、インシデント対応計画内の独立したセクションで取り上げてもよい要素である。コミュニケーションのセクションには以下の内容を含める。

- メディア、緊急対応サービス、国家機関、地域組織や国際組織といった、必要なすべての連絡先を掲載する
- インシデント発生時の連絡窓口と、組織を代表して話す用意ができている、代替要員を含む1名以上の担当者

- 当面の対応に使用できるよう用意し、精査しておいた声明及びプレスリリース情報。これは特に、一般の人々が依存している製品またはサービスを組織が提供している場合に重要である。
- 内部、外部両方から組織への報告系統
- ICS全体に含まれる重要なシステムと構成要素の主要ベンダに所属する、関係するスキルセットを有する担当者名の最新リスト
- 電話回線、携帯電話網、インターネットを通じ、不完全な通信経路に対処する代替の物理的手段の説明。これには、いずれか、またはすべての通信手段が機能しない事態の説明も含まれる。

8. **フォレンジック**　サイバーフォレンジックは、インシデントに関連するデータの収集、調査、分析に加え、犯罪の疑いがある者に対する法的措置で使用する、犯罪を証明する証拠の保全に重点が置かれる。対象データは、入手可能なログ（ネットワーク、サーバ、ワークステーション）、物理的構成要素（可能であれば、影響を受けたRTOS（Real Time Operating System）のハードディスクとビットマップイメージ）、電子メール、ボイスメール、テキスト、通話記録に存在する可能性がある。情報収集はインシデントの理解及びさらなる活動の防止に役立つが、この手法には、データの完全性と保全に関する、インシデントの把握だけにとどまらない特別な意味合いが含まれる。ICSに関連するサイバーフォレンジックに特化した推奨プラクティス[d]が入手可能である。この推奨プラクティスは、インシデント対応計画のフォレンジックのセクションを作成するときに参照すること。

9. **その他のセクション**　上記の領域は、インシデント対応計画における不可欠の要素である。インシデント対応計画は、さらに詳細なトピックに分割できる。そして、インシデントの追跡や報告など、必要に応じて他のセクションを追加することもできる。

2.4　計画の実施

インシデント対応演習を計画し、実施し、その結果を評価することは、通常業務に影響し、阻害する可能性はあるが、かかわっている利害を考慮すれば、これは必須である。最良の対応

[d] 参考文献：“Recommended Practice: Creating Cyber Forensics Plans for Control Systems（推奨プラクティス：制御システムに対するサイバーフォレンジック計画の作成）”2008 年 8 月 25 日、Control Systems Security Program (CSSP), Department of Homeland Security（US-CERT の Web サイトを参照）

計画であっても、実際のインシデント発生時に直面するすべての障害を予想できるわけではないし、予期しない状況に人がどう反応するかはどんな場合でも予想できない。対応にあたって一定の役割を果たすことが期待される人の所在がつかめないことはよくある。事前に訓練を受けた人が、新しい人に変わっている可能性がある。分析の時間がほとんど、または全くない状況で決断を求められるときに、予期しない事象の生じる可能性がある。

実際のインシデントで起こる問題の多くは、テストや演習に含まれている。このことは、大損害をもたらす決断や生産停止の影響を被ることなく、手続きを確認、分析、変更する機会が得られることを意味する。ただし、これは実運用システムを忠実に再現する環境で計画をテストした場合にのみあてはまる。

インシデント対応計画の部分テストを実施することも、予期しない振る舞いを評価する上で生産的である。こうした部分テストにより、完全テストに先立って計画を調整し、計画をより効果的かつ効率的なものにすることができる。部分テストは、完全テストに伴うコストや中断の負担を負わずに、CIRT（Computer Incident Response Team）の新しいメンバーを訓練するよい機会となる。

以下は、インシデント対応シミュレーションの準備において検討する項目である。

- インシデント対応計画の一部の側面は、すべての種類のインシデントで類似しているが、それ以外の側面は大幅に異なる。インシデントが異なれば、要求される対応レベルが異なる可能性がある。たとえば、侵入者がICSネットワークをスキャンするものの設備の設定は改変しない場合は、有毒化学物質の処理を制御するポンプやバルブをロックする保護手段を無効にする場合と比較して、要求される対応レベルが低い。演習は、できるだけ多くの種類の重大シナリオを取り上げ、シナリオに応じて演習の性質を調整する。
- インシデント対応計画の練習では、インシデント対応計画に存在する弱点を発見するために、できるだけ実践的となるよう現実の条件に近づける必要がある。演習が実際の運用環境の状況に近ければ近いほど、実際の実証の発生前により多くの問題が見つけて解決できる。インシデント対応計画がどう遂行されるかの見通しを正確に立てるために、可能であれば実際の設備を使用する。これは、演習用に一時的な設備を用意するようにベンダと連携することも含む。
- 演習は、最悪の場合の条件をシミュレートすべきである。できる限り大きな損害を与えようとする侵入者、または世間の注目を広く集めようとする者は、できるだけ都合の悪いタ

イミングを意図的に狙う可能性がある。希望する成果にもよるが、現場に人が最も多い、営業日のピーク時、または主要な技術スタッフや管理監督者が不在の週末や休日の深夜に行われることが考えられる。

- 演習は、インシデントへの対応や軽減に関与するすべての人物が参加する必要がある。一部の人間に訓練を行っても、インシデントに実際に直面する従業員が何をすべきかよくわかっていなければ、そのシフト中に事象が発生しても役に立たない。
- 演習は、スタッフの変更、施設や設備の変更、及び過去の演習や実際の事象から得た新情報を反映するために、定期的に行うべきである。
- 演習時の状況は、スタッフが通常でない状況について深く考えるよう計画する。これにより、意志決定プロセスの弱点、及び意図しないなだれ現象とその結果を浮かび上がらせることができる。
- CSIRTは、可能であれば、演習と潜在的インシデントの準備において、他の施設の経験を活かすべきである。この情報は、ICS-CERTのスタッフやCSSPの専門家との共同作業によって得ることができる。

2.5　システムの状態/状況レポート

システムの状態/状況レポートの有効化とは、異常な動作、侵入の試み、またはインシデントの検出、影響の把握、解決策の迅速な支援に有用なデータを含む、システムに関する情報を報告する自動化された仕組みをハードウェアまたはソフトウェアに関連づけることを指す。たとえば、ネットワークのログ記録やデータベース監査、特定のネットワークや設備向けに組織内で開発されたカスタムアプリケーション、提供された設備に組み込まれているベンダ開発の機能などが該当する。

プログラマが状態/状況レポート機能をソフトウェアアプリケーションに適用する（または使用目的に関係ない状態/状況レポートを提供するためだけにプログラムにコードを組み込む）場合、必ずといっていいほどプログラムのデバッグか、問題が報告された場合のサポート情報提供に役立てることを目的としている。このシステムを有効にするためにリソースを使用する正当な理由を考えるなら、ソフトウェアのデバッグ、これから起ころうとしている設備障害の

検出、作業プロセスの効率改善を含め、あらゆる種類のシステム問題の解決に役立てることが可能と考えることができる。

状態/状況情報をレポートするコードの追加は、インシデント発生後のフォレンジックを支援する上で非常に有用である。ただし、その主たる重要な目的はフォレンジックではなく、インシデントの検出と解決である。

ICSに関する状態情報の有効化には実際に利点が存在する一方、課題も存在する。ICSの性質上、多くのデバイスが揮発性メモリを搭載する設計となっており、ベースコードへのアクセスが困難となる可能性がある。ベンダは、コストやリスクという理由から、新たなコードの追加には消極的な場合がある。さらに、生成され、入手可能な状態のデータは、実用的な形でログデータを書き込んだり、保存したりできないほど速やかに置き換えられることが少なくない。ネットワークトラフィックの負荷は、ログ記録の追加によって、通常の運用に変化をもたらすか、悪影響をもたらすレベルにまで影響を及ぼすおそれがある。

有用な情報を収集するためにシステム構成要素を自動化する方法には、さまざまなものがある。主な種類は次のとおりである。

- **NIDS (Networks Intrusion Detection Systems:ネットワーク侵入検知システム)** このアプリケーションは、ハードウェア機器とソフトウェアソリューションの両方が該当し、ネットワーク上に配置され、ネットワークへのアクセスの試みを検出するのに有用である。ITにおける何年にも渡る実績があり、同様にICS環境にも有用である。NIDSは、侵入の試みをネットワーク管理者に警告し、ネットワーク管理者が設定したパラメータに従って、すべての警告情報を記録する。
- **PIDS (Protocol-based Intrusion Detection System：プロトコルベースの侵入検知システム)** PIDSは、ネットワークよりむしろ、構成要素に関連している。通常、PIDSはサーバと、サーバに接続されている機器との間に配置され、両者間の通信プロトコルを分析する。PIDSの派生形として、APIDS（Application Protocol-based Intrusion Detection System:アプリケーションプロトコルベースの侵入検知システム）がある。これは、アプリケーション固有のプロトコルで通信を行う複数のサーバの間に配置される。
- **HIDS (Host-based Intrusion Detection System:ホストベースの侵入検知システム)** HIDSはホストシステム上に存在し、ホスト上のアプリケーション固有のデータを分析する。ログファイル、ファイルシステム、データベースの変更の分析などが行われる。

- **IPS（Intrusion Prevention System：侵入防止システム）** IPSテクノロジは未成熟であり、ICSの障害の原因となるリスクが高いため、このシステムは現時点ではICS環境には推奨されない。IPSについては、利用可能なテクノロジ、およびそのテクノロジが統合業務システムにおいて果たす役割の可能性に関して全般的な理解を深めるため言及する。IPSは、侵入検知システム（IDS）に似ているが、悪意のある行動に対して能動的に反応し、可能であればその活動を遮断または防止する点がIDSと異なる。ICS環境に実装する場合、NIDSおよびIPSはともに、サーバタイプの構成要素への適用は限定的ながらも、ネットワークに密接に関連づけられる。侵入防止システム（IPS）および侵入検知システム（IDS）のタイプの製品に関する詳細情報は、インターネット上で容易に入手できる。ICSとの互換性を確保するために、システム導入前に徹底した準備テストを実施することを強く推奨する。侵入防止システム（IPS）のような能動的なシステムは、正当な活動を防止する可能性があるため、このシステムを使用する前に、認められる活動を確立しておかなければならない。
- **ネットワークと機器のログ記録** 上記の侵入検知システム(IDS)タイプのものを含め、ネットワークのログを記録する製品は、成熟したものが市販されている。しかし、使用されている各種の制御システム機器に関して言えば、状況は必ずしも同じではない。機器のログ記録は、発売時期、ベンダ、機器のタイプ、使用できる設定によって異なる。管理者は、機能が利用可能な場合、及び業務を中断しない状況においては、必ず監査とログ記録の機能を有効にするべきである。ベンダも自己監視機能を新製品に搭載したり、既存ハードウェアのアップグレードで対応したりすることが推奨される。
- **データジェネレータの設定** 市販のシステムを利用してデータの正常な収集を行うためには、検討すべきいくつかの要素がある。すべての設定項目について把握、理解し、機器を正しく設定して、警告通知を定期的に監視することが重要である。完璧に機能する検出システムであっても、警告が送られて、それを受け取る人がいなかったり、気付かなかったりすれば無意味である。これは、当直が割り当てられておらず、多くの誤認定インシデントが通知され、実際のインシデントが見過ごされやすい場合が該当する。カスタマイズされたログ記録と監視機能の場合、有用な設定をすれば機器の価値が高まる。たとえば、平常運用時の屋外機器の状態を測定し、定期的にサーバに報告する場合が該当する。サーバは、規定外の条件や異常なトラフィックについて常に検査し、そのような条件やトラフィックは電子メールや緊急連絡手段、警報などで報告される。関連する特定の機器を分析し、ベンダが提供するか、または独自に用意した監視機能を機器に適用することが重要である。

独自に用意した監視機能を使用する場合、特に旧式の機器や専用ソフトウェアを搭載する機器の場合、当該機器に直接アクセスする手段が存在しない場合がある。このような状況では、機器内部を監視することはできないが、機器に送られる、または機器から送られる信号は検査できる可能性がある。構成要素の状態/状況を外部から正確に検証する方法が存在する場合もある。ICSと業務システムとの間には、ネットワークトラフィックに関して違いがある。ICSのトラフィックは、業務システムの場合と比較して限定的で、内容が一定しているため、ベースライン取得後に範囲外、または異常な内容に基づいて特徴的パターンを作成することができる。

一部のシステムやアプリケーションは運用上の問題を起こす可能性があるため、ICSにおいて状態/状況レポートを有効化するときは注意が必要である。[e]たとえば、一部の古い制御システムに対して、侵入検知システム（IDS）やウィルス対策ツールによっては非常に干渉の度合いが高く、システムを無効にしたり、シャットダウンしたりする恐れがある。適切に設定されていない侵入検知システム（IDS）やウィルス対策ツールは、ICSが機能しないレベルになるまで、重要なデータ通信の速度を低下させてしまう。これらツールを配備する計画は、ICSベンダに確認し、ICS及びシステム、並びにそれらのシステム上で共存する支援アプリケーションについて互換性をテストしなければならない。最新のソフトウェアのなかには、既存の支援ソフトウェアと間で互換性のない場合がある（例：Javaの各バージョン）。

このような種類のシステムについては以下の点を確認しておく必要がある。

- ログファイルはどこに保存されるか
- ログファイルの保存期間はどれくらいか
- 古いログファイルは削除されるのか、アーカイブとして保存されるのか
- 調査するパラメータは何か（ポート、ログイン/ログアウト時間、異常トラフィックの発生サイクルや時間など）

[e] CSSP は、本文書に記載されるすべての方法は、実際に運用する前に徹底的にテストを行うことを強く推奨している。

3.　インシデント防止

サイバーインシデントの防止は、インシデントへの対応よりも望ましいが、ICS環境ではまったく新たな次元の話となる。これは、通常のITと比較して、ネットワークから先の部分がはるかに少なく、場合によっては、システム機器に検出機能がないからである。さらに、機能を果たす構成要素には修正されない脆弱性が存在する可能性があり、厳しい攻撃を受けた結果として、負傷や死亡、財政面における重大な損失が考えられる。相対的な脆弱性とその影響の重大性の度合いがどちらも高いため、施設にはインシデント防止のための十分なリソースを配置すべきある。

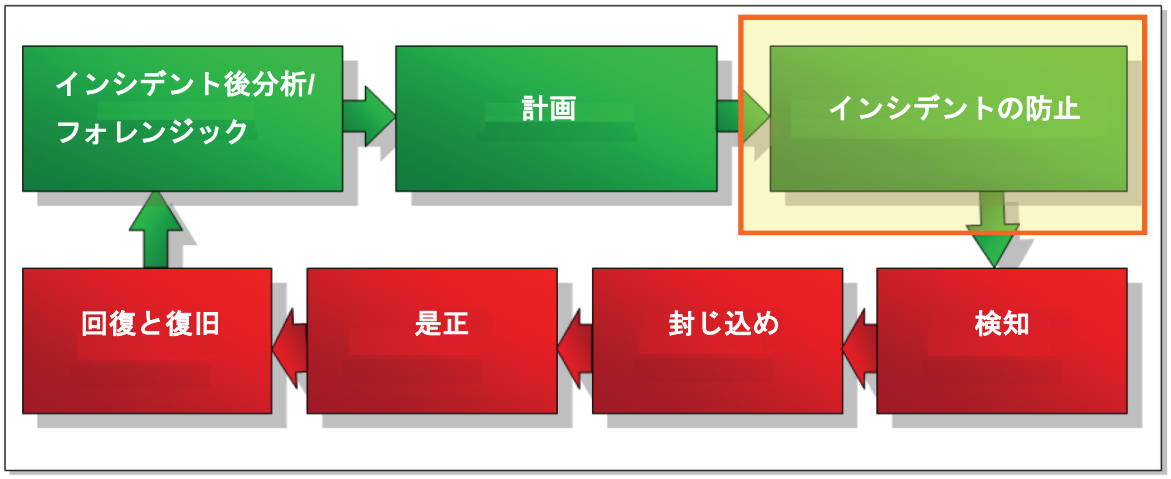

図3 インシデント防止段階

3.1　ツール及び指針

この推奨プラクティスは、サイバー攻撃からのICS保護に役立てるため作成された数多くの標準、ガイド、白書、アプリケーション、ソフトウェアツールの1つである。

NISTは、制御システムネットワークに対するサイバー攻撃防止に役立つ、2つの標準を作成した。SP 800-53, “Recommended Security Controls for Federal Information Systems － Information Security（連邦政府情報システムにおける推奨セキュリティ管理策－情報セキュリティ）”は、情報システム全般向けに作成され、完全なセキュリティ計画の作成に効果的である。最近までICSは、独自のソフトウェアと制御プロトコルを実行する独立したシステムであったという点で、

従来の情報システムと似ている点がほとんどなかった。しかし、これらのシステムが、接続性、効率性、リモートアクセス機能を向上させるために、組織の中心的な情報システムに統合されるようになったため、従来の情報システムと類似する点が増え始めている。こうした状況に対応するため、NISTは、公共分野及び民間のICSコミュニティと協同し、SP800-53 for ICS、付録Iにセキュリティ管理策の適用に関する具体的な手引を作成した。

NISTは、特に制御システム環境向けにSP 800-82, “Guide to Industrial Control Systems (ICS) Security（工業用制御システムのセキュリティのためのガイド）”を作成した。この文書は、本文書発行時点において、最終公開草案の段階にあった。それ以外にも、ICSの特定の形態を使用する特定分野に関する標準とガイドが作成されている。

「*Catalog of Control Systems Security: Recommendations for Standards Developers*[f]（制御システムのセキュリティカタログ：標準作成者のための推奨事項）」のAppendix Aにはその他の標準が示されている（表1参照）。表に示す標準は、該当するものがあれば、出典のカタログに掲載されるものより新しいバージョンに更新されており、カタログにない標準も追加してある。

表1 ICSセキュリティ標準

共通ラベル	説明
AGA 12-1	American Gas Association (AGA) Report 12、『Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan』、2006年3月
AGA 12-2	AGA Report 12、『Cryptographic Protection of SCADA Communications Part 2: Retrofit Link Encryption for Asynchronous Serial Communications』、2006年3月
ANSI/ISA-99.00.01-2007	International Society of Automation (ISA)、『Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models,』、2007年12月
FIPS 140-2	Federal Information Processing Standards (FIPS) Publication 140-2、『Security Requirements for Cryptographic Modules』、2001年5月25日
Draft FIPS 140-3	FIPS Publication 140-3, 『Security Requirements for Cryptographic Modules』。FIPS PUB 140-2（2001年5月25日発行、2007年7月13日ドラフト版発行、2009年10月現在もドラフト）の後継規格
API 1164	American Petroleum Institute (API) STD 1164、『Pipeline SCADA Security』、2004年9月1日。API 1164は現在APIによって更新中であり、内部審査に入っている。この標準は2009年半ばには一般利用のために公開される見通し
CIDX	（この文書は2006年にCIDX(Chemical Industry Data Exchange)から米国化学工業協会（ACC）に移行された）『Guidance for Addressing Cyber Security in the Chemical Industry』Ver. .0、2006年5月。この標準はISA 99の『Manufacturing and Control System Security, Part 2: Establishing a Manufacturing and Control System Security Program』に置き換わる予定である。
ISO 27001	International Standards Organization (ISO) Publication 27001:2005、『Information Technology – Security techniques – Information security management systems – Requirements,』、First edition、2005年10月15日

[f] *Catalog of Control Systems Security: Recommendations for Standards Developers（制御システムのセキュリティカタログ：標準作成者のための推奨事項）*、2008 年 1 月、Appendix A、National Cyber Security Division, Control Systems Security Program, Department of Homeland Security.

共通ラベル	説明
ISO 27002	ISO Publication 27002:2005（旧ISO 17799）、『Information technology – Security techniques – Code of Practice for Information Security Management』、2007年番号変更
IEC 62351	The International Electrotechnical Commission (IEC) publication IDC/TS 62351, Parts 1-6、『Power systems management and associated information exchange – Data and communications security』、2007年5月15日
IEEE 1402	Institute of Electrical and Electronics Engineers (IEEE), Document IEEE 1402, 『Guide for Electric Power Substation Physical and Electronic Security』、2000年1月30日
ISA 99.00.01-2007	ISA、『ANSI/ ISA 99.00.01-2007, Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models』、2007年10月29日
ISA 99.00.02-2007	ISA、『ANSI/ ISA 99.00.02-2007, Security for Industrial Automation and Control Part 2: Establishing n Industrial Automation and Control System Security Program』、2007年10月29日
ISA 99.00.03-2007	ISA 、『ANSI/ ISA 99.00.03-2007, Security for Industrial Automation and Control Part 3: Operating an Industrial Automation and Control System Security Program』、2007年10月29日
ISA 99.02.01-2009	ISA 、『ANSI/ ISA 99.02.01-2009, Establishing an Industrial Automation and Control Systems Security Program』、2009年2月
NERC CIP	North America Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards、 CIP-002 – CIP 009、standards on security topics、2006年5月2日
NIST SP 800-40 R2	NIST SP 800-40、Rev.2、『Creating a Patch and Vulnerability Management Program』
NIST SP 800-53	NIST SP 800-53、Rev.3、『Recommended Security Controls for Federal Information Systems – Information Security』、2009年7月
NIST SP 800-61	NIST SP 800-61, Rev. 1、『Computer Security Incident Handling Guide』、2008年3月
NIST SP 800-82	NIST SP 800-82、『Guide to Industrial Control Systems (ICS) Security』、Final Public Draft、2009年
NIST SP 800-83	NIST SP 800-83、『Guide to Malware Incident Prevention and Handling』、2005年11月
NIST SP 800-86	NIST SP 800-86、『Guide to Integrating Forensic Techniques into Incident Response』、2006年8月
NIST SP 800-92	NIST SP 800-92、『Guide to Computer Security Log Management』、2006年9月

表1に示す標準は、制御システムへの関連性に基づいて選択され、ICSに適用可能な最も広い範囲の分野と標準をカバーする、全般的なサイバーセキュリティ指針のセットである。インターネットを検索すれば、学術機関、民間企業、民間コンサルタント、政府機関が公開する何百ものガイド文書が見つかる。

組織が自身のICS環境のセキュリティ状態を評価するのに役立つ自動化ツールが提供されている。これらのツールは、民間ベンダが提供するスタンドアロンのソフトウェアプログラムの形態の場合と、コンサルティング会社が提供する評価サービスと併せて提供される製品の場合がある。さらに、オープンソース製品も役に立つ場合がある。

CSSPを通じ、DHSの指示の下で開発された有用な自己評価ツールに、CSET（Cyber Security Evaluation Tool）がある。この評価ツールは、一般のIT分野及びICSの特定業界分野における業界標準に基づいている。CSETは、標準に基づいて作成された一連の質問に対する回答に基づき、サイトのセキュリティ状態を評価する。そして、ICSの図を入力し、図内の各構成要素に対応する質問を表示する手段を提供する。このツールは、施設で改善される可能性のある部分及び最初に対処すべき部分を示すレポートを作成する。図4はCSETの起動時の画面である。

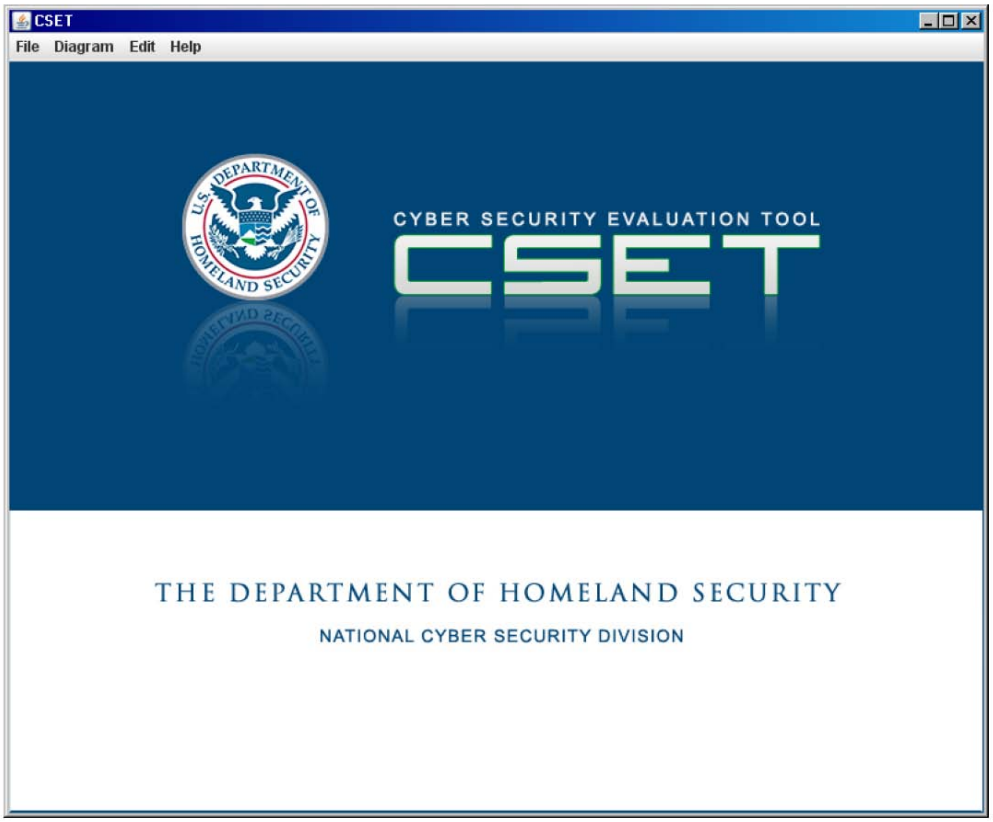

図4 CSETの起動時の画面

3.2　パッチ管理

パッチ管理は、効果的なサイバーセキュリティプログラムにおいて考慮すべき数多くの領域の1つでしかない。パッチ管理及びベンダとの連携は、ICSに関連して独自の要求事項があるため本文書では特に強調している。パッチ管理はインシデント対応にとって2つの点で重要である。まず何よりも重要なのは、パッチ管理が、インシデントの発生を防ぐ基本的な手段であるということである。次に重要なのは、パッチの適用が、脆弱性に対応して、Exploitの再発を防止する手段であることである。パッチを適用しなければ、システムはインシデント発生前と変わらず、脆弱な状態におかれたままとなる。

ICSのパッチ管理[g]については、以下の問題について検討しなければならない。

[g] 参照文献：“Recommended Practice for Patch Management of Control Systems（制御システムのパッチ管理における推奨プラクティス）” DHS Control System Security Program (CSSP)（2008 年 12 月）

- パッチを適用するための保守時間帯のスケジュールを実運用システムにおいて設定する難しさ
- サポートが終了し、パッチを入手できない設備
- 本来のベンダまたはサプライヤではなく、サードパーティが発行したパッチ
- 特に設備の独自性が高く高価な場合に、実運用システムへの適用前に実運用以外の環境で実施するパッチのテスト
- テストベッドまたはシミュレーション環境の作成
- 直近の既知の良好な設定を展開する必要のある場合に備えて、正常稼動しているシステムの障害復旧ポイントとしてのシステム設定の有効なバックアップの作成
- パッチがICSの正常な運用を妨げることが判明した場合のパッチのロールバック手続きの開発
- ICS内の隣接するアプリケーションに問題を起こすパッチ
- 適切なタイミングでのベンダからのパッチ受領
- 単体テスト及びシステム結合テストの両方を含む、ベンダが使用するテストプロセスの容認
- パッチが実運用システムを停止させたり、悪影響を与えてしまったりするリスクの想定
- パッチの適用に要する時間の把握、（必要に応じた）パッチの削除に要する時間の把握
- ICS構成要素に組み込まれているパッチ適用ソフトウェアの使用

本文書では、制御システムのパッチ管理についてこれ以上は取り上げないが、DHS CSSPプログラムの下で作成された「Recommended Practice for Patch Management of Control Systems（制御システムのパッチ管理における推奨プラクティス）」[h]（2008年12月）には、制御システムのパッチ管理に関する詳細情報が記載されている。CSIRTのスタッフは、パッチ管理の推奨プラクティスのほか、IT及びICSに対するパッチ適用のガイドを参照し、全般的情報やガイド情報を確認することが推奨される。

[h] 本文書は、特に制御システムのパッチ管理に関する問題に対処するため、作成された。本文書はUS-CERTのウェブサイトで入手できる。

3.3　ベンダとの連携

ソフトウェアの独自性、サイバーセキュリティに対する業界の未成熟さ、ベンダの顧客ベースが限られているという理由から、ICS環境においては、サイバーセキュリティに関してベンダと連携することが重要となる。

ビジネスITモデルでは、ごく限られた数のオペレーティングシステムと（ネットワーキング）ベンダに対し、文字通り何百万ものユーザが存在する。これは、LinuxやWindowsといった単一の製品に含まれる脆弱性が顧客ベースのほぼ全体に影響を及ぼすことを意味する。パッチ適用プロセスは成熟度が高く、しっかり確立されており、ベンダによる対応が期待されており、それが当たり前とさえ認識されている。さらに、ある製品またはその特定のバージョンに対するサポートは、顧客が新しいバージョンにアップブレードすることを期待して、やめることができる。これは、IT環境では容認されている慣行であり、顧客ベースに新たな機能を提供するために望ましい場合が多い。

ICSモデルの場合、1つのベンダが数多くの製品を販売しており、これら製品の多くのバージョンが現場で積極的に利用されている。これら製品の耐用年数は20年以上に及ぶ。さらに、IT環境の製品と比較すると、顧客の数が相対的に少ない。製品、発売時期、製品の独自性によって異なるが、数十、数百の顧客しか存在しない場合もある。ベンダには複数の製品及び製品の複数バージョンをサポートする負担があり、修正プログラムを要求する顧客数が少ないため、パッチ、状態/状況レポート、修正プログラムを適切なタイミングで提供することを保証できず、まったく提供できない場合もある。

防止と対応の両方をできるだけ高い水準で確保するためには、顧客とベンダの技術スタッフとの間で対象を絞った連携が重要である。すべての顧客が声を揃えれば、ベンダに対し、必要なパッチの提供でセキュリティ問題に対処するようプレッシャーをかけられる。継続的なパッチと関連サポートを確保するには、ベンダとサービス品質保証契約を締結しなければならない。この契約は失効させてはならない。失効させてしまうと法的影響力が失われる。

顧客は、優先順位や顧客のニーズに関して方向性を示すこともできる。これについては、製品ユーザの観点から、ユーザグループが関与し、ベンダの技術スタッフと営業スタッフに継続してフィードバックを提供する。

インシデントに対応する場合、ベンダ側の技術スタッフまたはサポートスタッフの関係が重要である。ICSの構成要素の重要性にもよるが、ベンダの技術スタッフをCSIRTの拡張スタッフまたはチームメンバーとして参加させる必要が生じることもある。これは、氏名、専門分野、連絡先情報を管理しておく必要があることを意味する。ベンダ側のスタッフは、緊急事態の発生時には支援のため呼び出される可能性があることを認識しておく必要がある。こうした手配には、期待してよい支援の内容と、そうした支援の費用を定めたサービス品質保証契約の締結が必要となる可能性がある。インシデントが発生してからでは、ベンダと新たに契約を結ぼうとしても遅すぎる。契約にパッチまたは修正プログラム提供までのターンアラウンドタイムを含めることは、必ずしもすべての場合で効果的ではないが、可能であればそうしておくことが推奨される。

4. インシデント管理

このセクションでは、サイバーセキュリティインシデントの管理に関する、4つの主要な部分について取り上げる。インシデント対応に関する他の文書では、これら主要な活動を拡張または統合している場合もあるが、検出、封じ込め、是正、そして回復と復旧を主要な活動としている（図5参照）。

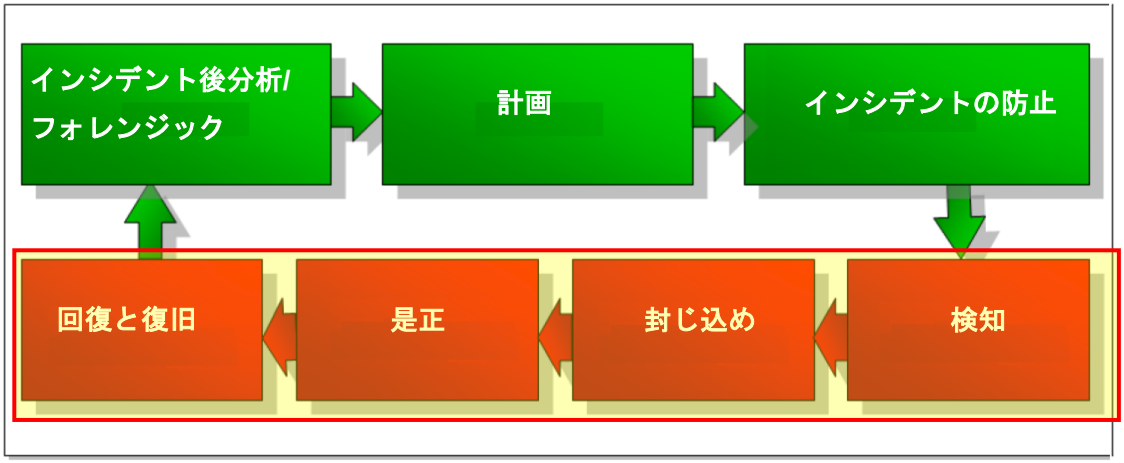

図5 インシデントの管理

4.1 インシデントの検出

インシデントの早期検出は、ICSに加わる損害を限定または防止し、その後の封じ込め、根絶、回復、影響を受けたシステムの復旧という取り組みの負担を軽減するのに役立つ。このセクションはサイバーセキュリティインシデントの検出手段に重点を置き、サイバーセキュリティインシデントが差し迫っていることを示す警戒すべき兆候、サイバーセキュリティインシデントと対応の分類及び優先順位の決定方法、推奨される検出手順について解説する。疑わしいインシデントが発生した場合や検出に関する助力が必要な場合は、ICS-CERTを通じて支援を受けることもできる。

4.1.1 報告及び協調

インシデントが疑われる場合にICS-CERT及びその他の対応組織と連携することで、問題を検出して理解するためのチームの能力を高めることができる。疑わしいインシデント及び既知

のインシデントの両方を報告することで、ICS-CERT[i]及び他の対応組織の専門家はインシデントに対する理解を深め、解決策を見つけ出すことができる。直面している状況が過去に発生したことがあり、検出、防止、回復に関する情報がすぐに入手できる可能性は高い。ICS-CERTを支えるスタッフは、必要であればインシデント管理のあらゆる側面を支援することが可能である。

ICS-CERTのほか、協調や情報に関して役立つ存在としては、IT-ISAC（Information Technology Information Sharing and Analysis Center）、及び以下のセンター[j]を含む、分野固有のISACが挙げられる。

- Communications（通信）
- Electricity Sector（電力）
- Emergency Management and Response（緊急事態管理及び対応）
- Financial Services（金融サービス）
- Highway（高速道路）
- Multi-State（複数州）
- Public Transit（公共輸送）
- Surface Transportation（陸上輸送）
- Supply Chain（サプライチェーン）
- Water（水道）
- Research and Education（研究及び教育）
- Maritime and Research（海事）

IT-ISACの使命に関する声明は、上記組織の目的及び目標の手がかりを示す。Webサイトにもあるように、IT-ISACの使命は以下のとおりである。

---

[i] ICS-CERT は、US-CERT（United States Computer Emergency Readiness Team）の関連組織である。US-CERT は、DHS における NCSD（National Cyber Security Division）の実働部門である。詳細情報を入手、及びインシデントを報告するには、http://www.us-cert.gov にアクセスされたい。

[j] 他の ISAC に関する情報は、ISAC Council の Web サイト（http://www.isaccouncil.org）で入手できる。

- 電子的なインシデント、脅威、攻撃、脆弱性、解決策と対策、セキュリティのベストプラクティス、及びその他の保護手段に関する情報を報告及び交換する
- 上記のような情報を、体系的かつ保護された状態で交換及び調整するための仕組みを確立する
- サイバーセキュリティ及び情報共有の課題に関し、政策立案者に対して考え方の方向性を示す

NRC（Nuclear Regulatory Commission:**米国原子力規制委員会**）など、一部の監督官庁は、分野固有の補足情報を提供したり、特定インシデントに関する報告を要求したりする場合がある。

4.1.2 監視による検出

ICSサイバーセキュリティインシデントは、一般的に2種類の方法で検出できる。1つめは、システムまたは構成要素の異常なふるまいをユーザが観察することによるものである。観察事象は、オペレータ、プロセスエンジニア、システム管理者など、組織のどのメンバーからも報告されうる。2つめは、マルウェア、侵入の試み、ポリシー違反、Exploit、構成要素の障害を検出し、フラグを設定できるネットワークモニタ、ネットワークトラフィック分析アプリケーション、IDS、ウィルス対策プログラムなど、アプリケーションやルーチンによる自動化された検出を用いる方法である。自動化されたこの方法でも、設定、確認、分析、行動のために人間による何らかの関与が必要となる。

ユーザによる観察の方法は、基本的に事後対応の方法であり、いくつかの有害なリスクをもたらす可能性がある。事後対応ということは、侵入およびサイバー攻撃がその時点で行われているか、またはすでに発生してしまったことを意味する。このため、事後対応の方法では、サイバーインシデントに対し、初期の保護能力または防止能力を提供することができない。この方法に伴う悪影響の一部を以下に示す。

- 物理的システムまたは物理的設備に対する損傷
- 制御システムの重要な運用データの採取
- 以降に望まれないシステム動作を引き起こすような、ソフトウェア構成アルゴリズムの改変

- ウィルスやワームなど、システムまたはシステムデータの機密性、完全性、可用性を脅かすマルウェアの注入

システムまたは設備の障害より前に観測可能な、警戒すべき兆候を特定するためにあらゆる努力を行わなければならない。サイバー攻撃以外の手段が、数多くの警戒すべき兆候を誘発しうるが、そうした兆候はそれでもインシデントの前兆として考慮する価値がある。以下は、NIST SP 800-82 “Guide to Industrial Control Systems (ICS) Security (Final Public Draft)（工業用制御システム（ICS）のセキュリティのためのガイド、最終公開草案）”（2008年9月、pp 6–19）から作成した、攻撃の可能性を示すものと考えられる兆候の一覧である。

- 異常に多いネットワークトラフィック
- ディスク容量不足、または空き領域の著しい減少
- 異常に高いCPU利用率
- 新たなユーザアカウントの作成
- 管理者レベルのアカウント使用の試みまたは使用
- アカウントのロックアウト
- ユーザが出勤していないときに使用されているアカウント
- クリアされたログファイル
- 異常に大量のイベントが記録され、容量を使い切ったログファイル
- ウィルス対策プログラムまたはIDSの警告
- ウィルス対策プログラム及びその他のセキュリティ管理策の無効化
- 予期しないパッチによる変更
- 外部のIPアドレスに接続されたマシンまたはインテリジェントフィールドデバイス
- システムに関する情報の要求（ソーシャルエンジニアリングの試み）
- 構成設定に関する予期しない変更
- 予期しないシステムシャットダウン

サイバーインシデントの可能性を示すその他の要素は以下の通りである。

- Webサーバ、データベースサーバ、アプリケーションサーバの停止またはエラーメッセージの表示
- ネットワーク上のホストへの異常に遅いアクセス
- 通常使用されない文字を含むファイル名、新規または予期しないファイルやディレクトリ
- ホストの記録に残されている、監査設定の変更（特に監査機能の無効化）
- 疑わしい内容の大量のバウンスメール
- 通常のネットワークトラフィック量からの異常な逸脱
- ICS設備の異常動作（特に複数の機器が同じふるまいを示す場合）
- 安全システム、バックアップシステム、フェイルオーバーシステムの明らかな無効化
- 運用プロセス自体は安定し、予測可能であるのに対し、一時的に使用率が急増する設備、サーバ、またはネットワークトラフィック
- 社内ネットワーク、または制御システムネットワーク外部の他のネットワークからの未知または異常なトラフィック
- 未知または予期していないファームウェアの書き換え

上のリストは、注意すべき事柄の例を示すものであるが、すべてを網羅しているわけではない。正常な運用状態を理解しておき、可能であれば記録しておくことが推奨される。想定している機能性からの逸脱は警告とみなすことができる。

オペレータの経験が、正常な状態からの逸脱を検出するための最良の情報源である場合もある。なぜなら、設備の動作におけるわずかな違いが、特定することの困難な「何かおかしいと感じる」状況を生み出す可能性があるからである。経験豊富なオペレータは何かが正しく動いていなければそれが分かり、潜在的なサイバー問題だけでなく、セキュリティとは関係のない、設備の摩耗や破損も検出できる。

管理監督者は、システムまたは設備の異常な動作に気付く可能性のある立場にあるオペレータやプラントの他の要員に対し、具体的な連絡先と報告に関する指示を示しておくべきである。連絡先は、オペレータがCSIRTに連絡するための、緊急連絡方法、電子メールの情報を含む。これらの指示には、異常な動作の分析と評価を行うCSIRTを支援するために収集し、報

告する情報のチェックリストも含まれる。連絡先情報とチェックリストの指示は、便利で、簡単に確認できる場所に掲示する。

4.1.3 自動検出手法

インシデント検出を自動化した方法は、ICSに対するExploitを防止する上で非常に有用である。攻撃の性質、試みの回数、及び昼夜を問わず繰り返される試みが生み出す環境は、手作業による監視が不可能でないにしても非常に困難である。ネットワーク化されたICSのほとんどは、その規模にかかわらず、何らかの自動検出機能を備えている。たとえば、ICSネットワークに接続された市販の高度な侵入検知システム（IDS）や、シンプルなファイアウォールログ機能などがある。自動化をアプリケーションにとってバランスよく設定し、意図したとおりに動作させ、適宜、人間による確認と操作を行うことが重要である。

セクション2.5「システムの状態/状況レポート」では、自動化のさまざまな手法を説明している。これらの方法としては、NIDS、PIDS、HIDSなど、各種の侵入検知システム（IDS）がある。ICSの構成要素上に配置され、情報の収集と報告を可能にするアプリケーション（ベンダの開発によるもの、またはカスタムで作成したもの）も取り上げている。

システムの状態/状況レポートの考え方では、状態/状況の情報をシステムの構成要素に報告させる、市販の方法とカスタマイズした方法の両方を利用することを強調している。状態/状況の情報はインシデントの防止に役立つが、インシデント後の分析とフォレンジックにも有用である。

自動検出システムはすべて、適切に機能するために必要な、少なくとも3つの構成要素を備えている。

- **範囲外の事象または限定事象を検出する、プログラムによる方法**：この構成要素には、既知のウィルスシグニチャに一致する文字列、またはサービス運用部外（DoS）攻撃などの一定のネットワーク動作の検出が含まれる場合がある。さらに、制限されている特定のポートへのアクセスの試みを検出したり、既知の不正なIPソースアドレスを検出する場合もある。個々のICS構成要素においては、設備またはソフトウェアの動作が、あらかじめ定めたしきい値を逸脱する場合を検出するカスタムアプリケーションの場合もある。
- **事象または変化を捕捉し、報告する機能**：事象の検出は出発点であるが、有用であるために、アプリケーションは使いやすい形式でデータを整理し、提示しなければならない。よ

り高度なシステムには、フィルタリングと報告の機能を備えるものもある。ログ情報をテキストファイルに書き出すだけの機能を持つシステムもある。有用性を高めるために、機能を特化した構成要素は、何らかの形の監査ファイルやログファイルに変化を書き出したり、記録したりできなければならない。一部のプロセスは、設備の運用に影響を与えずにログデータの一定の流れを連続的に書き出すことができない。このような場合、範囲を設定し、範囲から外れた場合のみ報告するのが理想的である。

- **フラグが付けられた事象のオペレータへの伝達**：侵入防止システム（IPS）のような高度なシステムは、人の関与なしに一部の予防措置を実行できる可能性がある。ただし、侵入防止システム（IPS）は、よく理解されているITアプリケーション向けに設計されており、不用意なシャットダウンが望ましくない結果をもたらす実運用のICSは考慮されていない。より一般的な状況として、誤認インシデントの判別、及び潜在的サイバー攻撃と保守上の問題の切り分けは人が行わなければならない。データへの対処と適切な対応（必要時におけるCSIRTの始動を含む）の開始も人ができなければならない。

自動検出システムの3つの構成要素はそれぞれ正常に機能しなければならず、機能しなければシステムに障害が発生する。最初の2つの構成要素にも一定の制限はあるものの、人による監視と対応に関係する3つめの構成要素の実際面が大きな課題と考えられる。もっとも大きな課題は、人がいること、本物の事象を見分ける訓練、及び本物の事象を発見した時の適切な対応の始動に関連するものである。以下のアドバイスは、ICS担当者を支援する方法に関するものである。

- さまざまなデータソースを集約する、一元化したログ記録を使用して、一貫した形式で1カ所に提示される統合化された情報の集合を管理者が見ることができるようにする。これには、ログファイルまたは監査ファイルに対するインタフェースや、そこからのデータの取得が必要となる場合がある。
- 未加工のログデータのフィルタリングと処理のために必要なアルゴリズムとビジネスルールを作成する（一部の侵入検知システム（IDS）はすでにこれを行う。「ログ絞込み」という）。目的は、ロジックの簡素化と自動化をできるだけ行って、オペレータが常に未加工データを確認しなくても済むようにすることである。
- 自動化された中央のプログラムとスタッフとの間に効果的な通信機能を作成する。これには、電子メールや緊急連絡手段による自動通知、音の出るアラーム（必要な場合）などが

含まれる。通信機能は、通常運用時と、専門家が不在の可能性があるとき（夜間、週末、休日）の両方に配慮して計画する必要がある。

- アナリストによる検出アルゴリズムの定義の効率が向上し、オペレータの訓練によってデータに対する理解が深まるよう、継続的な改善プログラムを準備する。

4.1.4 インシデント対応ツール

セクション2.5で、日常業務の際に潜在的インシデントを検出するさまざまな自動化ツールについて取り上げた。その他に、より具体的で詳細なデータを取得し分析する有用なツールがある。一部の監視ツールは継続的監視及び単一インシデントの検出と解決の両方に使用できるため、重複する部分が存在する。インシデント対応ツールの例として以下のものが挙げられる。

- **ネットフローの取得と分析:** このツールは、受信トラフィックと送信トラフィックを含め、ネットワークを通過するトラフィックの種類を取得し表示する手段を提供する。アプリケーション、カンバセーション、ドメイン、エンドポイント、プロトコルのそれぞれを単位としてデータを分離できる。このツールの多くは、分析とフォレンジックの両方の作業に備えデータの保存も行う。
- **ネットワークパフォーマンスモニタ：** ネットワークパフォーマンスモニタは、ネットワークパフォーマンス把握の手がかりを提供し、異常なパフォーマンスが発生している場所の特定に役立てることができる。このツールは、帯域幅の監視と分析、ネットワークのルーティング分析を行う場合もある。
- **可用性モニタ：** 可用性モニタは、リアルタイムの応答時間の表示など、高度な「ping」機能によってネットワークデバイスが利用可能な状態かどうかの判断を支援する。
- **アプリケーションモニタ:** 不正なアクセスや操作の疑いがある場合、特定のアプリケーションを監視できる。このツールは、全般的なネットワーク監視と比較して、疑わしいアプリケーションをより細かく分析できる。
- **パケット及びトラフィックのリコンストラクタ：** このツールは、ファイルをネットワーク上の本来の形式に再構築し、ネットワーク及び関連トラフィックの固定イメージを取得す

るものであり、ネットワークトラフィックモニタと関連づけられたり、その一部としてバンドルされたりすることが多い。

- **プロトコルアナライザ：**上記の他のツールと同様、このツールは、フォレンジック分析の可能性に備え、パケット情報（統合された統計情報を含む）を取得し保存する機能を備える。
- **tracerouteツール及びwhoisツール：**これらは、侵入者を侵入元のコンピュータまで追跡するのに役立てることができる。関連する機能では、IPアドレスのブロックや報告を行うことができる

4.1.5 インシデントの分類

インシデントであることが確認されたら、サイバー攻撃を分類し、その分類に基づいて対応の優先順位を決める。分類は、インシデントの種類と、ICSに与える可能性のある損害に基づくべきである。インシデントの種類によって、適切な対応レベルが決まる。インシデント対応計画には、インシデントの種類ごとの対応レベル（及び努力レベル）を詳細にまとめる必要がある。前述のとおり、インシデント対応計画の作成は、事象が実際に発生する充分前に行う。

対応の優先順位は、発生時とその後にICSに及ぶ影響、及び影響を受ける設備とシステムの、会社の運営からみた重要性に基づいて決めるべきである。

以下の質問は、分類と優先順位の基準の決定に役立てることができる。

- Exploitはどのように発生し、再び発生する可能性があるか。どれくらいの時間で再発するか。
- インシデントは組織の内部か、または外部か。
- システムに置かれた攻撃ツールがある場合、それはどのような種類か。
- 攻撃ベクトルによって影響を受けるネットワークとシステムはどれか。問題は他のサイトや顧客に広がる可能性はあるか。
- 攻撃によって、法律上または安全上の問題は生じるか。
- インシデントが数時間または数日以内に封じ込められないと、影響はどれくらい拡大するか。

- システムは安全にフェイルオーバーできるか。引き続き稼働できるか。
- 影響を受けた構成要素はICSにとって、及び運営全般にとってどれくらい重要か。

以下は、分類と優先順位を決定するための推奨される手順である。

1. 各インシデントの特定と緩和の責任を負う、調査の主担当者を割り当てる。
2. インシデントが悪意によるものか、そうでないものか確認する。インシデントが悪意によるものでない場合、完全なCSIRTは不要である。ただし、一部のリソースを問題の解決に使用する可能性がある。
3. 証拠を詳細に確認、評価し、証拠へのアクセスを管理しながら、正確な記録をづける。
4. 稼働している業務部門のネットワークサービスを、影響を受けたシステムに提供する特定の担当者と調整を行う。

組織固有の具体的な手順を含めるべきである。手順はインシデント対応計画内で明確に定義し、インシデントを分類し、優先順位を決定するときのCSIRTの行動を導くものであること。

4.2　封じ込め

封じ込めはマルウェアの拡大と影響の防止に重点が置かれるが、マルウェア以外のインシデントのなかには封じ込めに関連して別の行動が要求される。たとえば、ある従業員が別の人物のユーザアカウントとパスワードを使用し、アクセス権限のない情報にアクセスする場合があてはまる。この状況を封じ込めるには、この従業員を情報へのアクセスから除外し、必要に応じて懲罰措置を講じる。システム上にマルウェアを残さなかったがICS構成要素に直接アクセスしていた攻撃者の場合は、封じ込めでは侵入者の遮断、設備が影響を受けていればその復旧、及びセクション3「インシデント防止」で概説した保護手順を実行する。

封じ込めが行われる第一の事例は、ICS上に何らかの形態のマルウェアが残されている場合である。このセクションは、侵入者用のアクセス経路を作ったり、自律的に動作してICSに損害をもたらしたりする、サーバまたは他の構成要素上に置かれたソフトウェアに関連する封じ込めの問題を中心に取り上げる。その他の情報は、2005年11月発行のNIST SP 800-83 “Guide to Malware Incident Prevention and Handling（マルウェアによるインシデントの防止と対応のためのガイド）”を参照のこと。

マルウェアの封じ込めには2つの主要な目的がある。1つめの目的はシステムの他の部分への拡大を止めること。2つめは、ICSに引き続き損害が加わるのを防止することである。ICS内または施設全体の他の構成要素やネットワークへの拡大からマルウェアを隔離している場合であっても、隔離したセグメントの中で引き続き損害を与える可能性がある。

マルウェアの封じ込めは、各組織で標準的な手法に従うわけではない。封じ込めの手法は、マルウェアの種類、影響を受けるシステムの重要性、受容できるリスクレベルによって異なる。このため、どの組織もそれぞれに固有のシステム要件に基づいた適切な封じ込め措置を決定しなければならない。封じ込めの基準は、適切に文書化し、組織とCSIRTのメンバーが理解しておく必要がある。

マルウェアの封じ込めにはいくつかの方法がある。1つめは、ウィルス駆除プログラムなど、問題を排除し、システムの機能を復旧する自動化されたテクノロジを使用する方法である。2つめは、インシデントを処理している間、サービスを停止する方法、3つめは、フィルタリングプロセスを用いて特定種類のネットワーク接続を遮断する方法である。

自動化されたテクノロジを使用すると、検出と対応が即座に実行される（ユーザがそのように処理するようアプリケーションをプログラムした場合）。この方法は既知のマルウェアに対してのみ対応でき、ゼロデイ攻撃の脆弱性を是正できない。ゼロデイ攻撃は、まだパッチが提供されていない脆弱性を狙う。自動化テクノロジのツールは、フィルタリングプロセスまたは初期防御として機能することでサイバー攻撃の脅威を大幅に低減でき、組織のリソースの節約とシステムのダウンタイム短縮を可能にする。制御システムエンジニアにとっての課題の1つが、独特のICSコンポーネント、特に旧式または固有のプロトコルを利用する構成要素を扱える自動アプリケーションを見つけることである。

サービスの一時的な停止は、混乱を生じる可能性のある思い切った手段であり、通常、サービスの無効化など、アプリケーションレベルで実行される。この方法は、サービスに関連するIPアドレスまたはポートを遮断するファイアウォールを使用するなど、サーバ上、またはネットワークレベルで実行される。影響を受ける特定のサービスを停止することで、影響を受けていない構成要素の運用を維持してサービスが完全に失われないようにしながら、感染の急速な拡大を阻止し、防ぐ。求められている結果は、失われる機能性を最小限にとどめながらインシデントを効果的に封じ込めることである。サービス停止に効果的に備えるため、組織は、使用されているネットワークと構成要素のサービスの一覧を、対応するTCP（Transmission Control Protocol）ポートとUDP（User Datagram Protocol）ポートの情報とともに維持しなければならない。

接続の無効化による封じ込めを使用することは、外部システムとの間の接続確立を試みる、感染システムへのネットワーク接続を一時的に制限する、効果的かつ迅速な手段である。これにより、マルウェアによるダウンロードを防止し、そのシステムの感染が内部のその他のネットワークシステムに拡大するのを防げる。狙いは、ネットワーク通信ポイントを取り除き、重要な制御システムをネットワークから隔離して、隔離した部分を他の重要なサービスを中断せずにテストし検証することにある。重要なICSネットワーク構成要素の接続を解除するこの方法は、インシデントに対する計画と準備の段階で手順を明確にし、テストしておくべきである[k]。

[k] サービスの停止は、業務に重大な影響を与える可能性がある。CSSP では、これらの措置は、細心の注意を払い、実運用システム以外のシステムで徹底的にテストを実施した後のみ実行することを推奨している。

4.3　是正

完全なシステム回復の前に、問題の原因を直すための是正を実行すべきである。是正では、システム上に残されたマルウェアの根絶、脆弱な設備の取り外しまたは交換、設備またはソフトウェアの再設定とパッチ適用、特定人物のアクセス件の取り消しなどを行う。

インシデントが不正アクセスを伴っていた場合、アクセス経路を閉鎖する。アクセス経路の閉鎖では、全パスワードと特定のユーザ名を変更したり、不正アクセスが確認されたIPアドレスからのアクセスの遮断、ファイアウォールにおけるポート設定の変更を行ったりする。

ICSに対して注意深く分析を行い、侵入者がたどった経路を検証する。この作業は、実際の弱点を明らかにするだけでなく、目を向けなければならない可能性のある同様の領域も明らかにすることができる。たとえば、特定のダイアルアップ機器が問題の原因であった場合、同じように脆弱な類似機器がICS全体に点在している可能性がある。

インシデントに、システムに残されたマルウェアが関与している場合、その削除または根絶が必要である。施設の運用中断を最小限に抑えながら、根絶によってマルウェアを削除するのが理想である。マルウェアの種類、感染の危険度、使用する封じ込め方法によって異なるが、マルウェア削除のプロセスを成功させるにはある程度時間を要する。

感染したシステムからマルウェアを削除する技術は多数存在する。もっとも一般的な方法は、ウィルス対策ソフトウェア、スパイウェア検出/削除ユーティリティ、パッチ管理ソフトウェアなど、自動化された根絶ツールを使用することである。その他には、システムを感染前のある時点まで復旧したり、主要なシステムファイルを際ロードしたりする方法がある。根絶ツールは、感染が検出されていれば、マルウェアを素早く見つけ出し、削除することができる。残念ながら、ウィルス対策型プログラムほとんどは、代表的なITシステムを対象としており、より特化された制御システム上のマルウェアは検出しない。さらに、こうしたプログラムは問題のないシステムファイルやデータファイルを削除したり、変更したりする危険がある。このような状況では、ベンダの協力を得ながら手作業による削除が必要になったり、対象システムでテスト済みの削除ソフトウェアをベンダ自身が提供できたりする可能性がある。

マルウェア感染の程度がより重大な場合、再構築が必要な場合がある。再構築では、オペレーティングシステムとアプリケーションの再インストールとセキュリティ保護に加え、バックアップファイルからのデータの復旧を行う。

システムに以下の特徴が見られる場合は、完全な再構築を検討する必要がある。

- 侵入者が、システムに対するrootレベルまたは管理者レベルのアクセス権を取得した。
- 確実に確認されていない、バックドア型のアクセスが許可された。これは、バックドアが1つ見つかっても別のバックドアが見つからないままである危険がある。
- システムファイルがマルウェアによって、または侵入者によって直接置き換えられた。
- ウィルス対策ソフトウェア、スパイウェア検出/削除ユーティリティ、またはマルウェアを根絶する他のプログラムや技術を使用した後、システムが安定しない、または正常に機能しない。これは、マルウェアが完全に根絶されていないか、またはマルウェアによって重要なシステムファイルやアプリケーションファイル、設定が損傷していることを示す。

根絶が完了したら、ICSが意図どおりに動作することを確認するテストを行うことが強く推奨される。テストでは、監視可能な動作だけでなく、インシデント検出情報を精査し、不正なコードが残存する兆候を探す。[1]

4.4 回復と復旧

ICS環境には、回復と復旧に関して、通常のITシステムでは見られない複雑さが存在する。ただし、従来のITとの共通点として、マルウェアの削除、バックアップデータのデータベースへの復元、一時的封じ込め措置の体系的な解除、運用システムとアプリケーションすべての再起動が挙げられる。

ICSにおいて複雑性が増す要因は、インシデント対応の一部としてシステムを管理しなければならない方法に関連する。施設が提供するサービスの多くはインシデント対応時に停止できないため、別の方法をとる必要がある。たとえば、フェイルオーバーシステムへの制御機能の切り替え、一時的または限定的な機能をもつ予備機器への移行、ネットワークアクセスからのシステム構成要素の隔離といった方法がある。これらの方法を使用する場合、重要な機器やプロセスは稼動を続けるが、統合が限定され、場合によっては機能が制約される、暫定運用の状態になる。

[1] 基本的なシステムファイルが変更されたり、削除されたりしたすべての場合、CSSPは、実運用システムに変更を加える前にツールと手順を徹底的にテストすることを推奨する。

運用の継続性が要求されるため、この一時的な運用状態は企業にとって高い危険性がある。ほとんどの重要な状況では、冗長システムを用意しておくことが期待される。ただし、高コストとアーキテクチャの複雑性から三重の冗長性は(理想的ではあるが)必ずしも可能ではない。そのため、予備システムに障害が発生すると、生産が停止し、CSIRT及び業務スタッフはできるだけ早く運用を復旧しようと、大きなプレッシャーに見舞われる。

従来のIT構成要素の復旧に関する情報は、NIST SP 800-61 “Computer Security Incident Handling guide（コンピュータセキュリティインシデント対応ガイド）”（2004年1月発行）などのコンピュータセキュリティ文書や本文書の最後に示す参考文献リストから得られる。ICSに関する具体的な推奨事項は以下のとおりである。

- インシデント前に、利用可能な機器（必要な場合はポータブル機器も含む）を使用した緊急時対応計画を作成しておく。これにより、主要なシステムの復旧に取り組んでいる間に運用を継続できる。
- すべての予備システムを、主システムと同じ水準までパッチを適用し、保守しておく。
- 計画に定めた時間に、計画に基づくテストを定期的に実施し、フェイルオーバーシステムを稼働させたときに正常に機能することを確認する。
- インシデント前に、ICSのセグメントを個別の稼動させる計画を作成しておく。この計画により、エンジニアは構成要素間の相互依存関係の現実的状況を把握でき、必要な場合は切り離しを決断できる。
- 最悪の事態のシナリオにおける現実的な時間制約でバックアップ機器をテストする。たとえば、予備電源は設備の状況にもよるが、数時間ではなく数日単位でシステムへの電力供給が必要となる場合がある。
- システムがインシデント前の状態に確実に復旧したことを確認できるように、受け入れテストと手続きを定め、実施する。テストには、自動テストと手動テストの両方が含まれる。
- 受け入れ手続きをインシデント対応計画の一部として定義し、適切な権限を持つ担当者がテストを承認し、ICSの完全な稼働を宣言できるようにする。

セクション5で説明するように、回復の最終段階はシステムを元の状態に復旧することだけではなく、より良好で安全な状態にすることである。復旧後のシステムは元の稼働能力を備えるだけでなく、インシデントの発端となったExploitからも保護されていなければならない。

5. インシデント後分析及びフォレンジック

インシデント後分析及びフォレンジックは、3つの領域で構成されている。1つめの領域は、インシデント、対応、影響を分析し、何を変えれば対応を改善できたかを明らかにして文書化する作業となる、教訓の学習である。2つめの領域は再発の防止、つまり類似インシデントの防止を含め、サイバーセキュリティプログラムの中に発見された弱点を是正するために、教訓を実際に活かすことである。3つめの領域はフォレンジックで、これには法的措置の可能性を踏まえ、証拠としてのデータを取得し、保護することが含まれる。

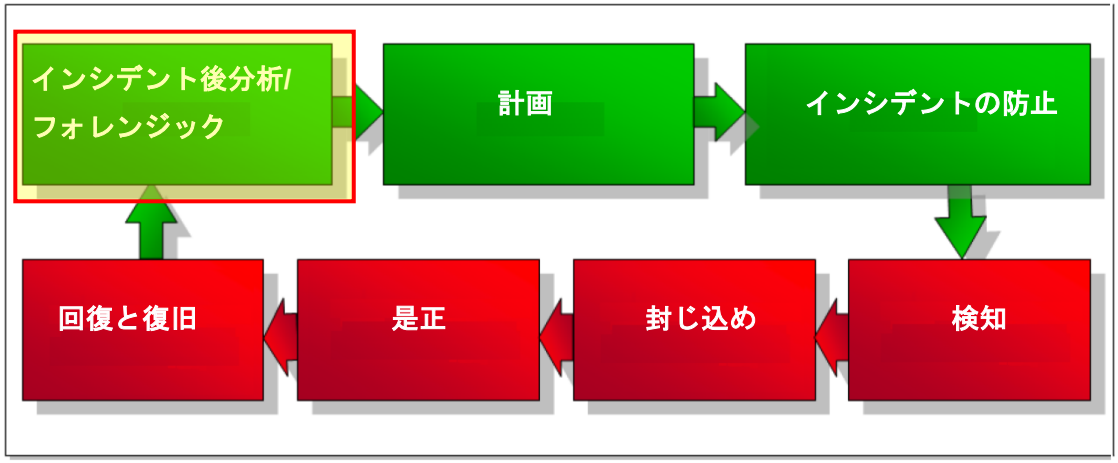

図6 インシデント後分析及びフォレンジック

5.1 教訓の学習

残念ながら、サイバー攻撃はダイナミックなものであり、攻撃者は自身の成功から素早く学ぶと同時に、失敗に終わった防御や不完全な防御につけ込んでくる。サイバー攻撃事象はどれも、制御システムのセキュリティ状態に潜む弱点を明確に知る機会を与えてくれる。そして、組織の対応のあり方に含まれる弱点も明らかになる。教訓の学習を実施することは、弱点を特定し、誤りを繰り返さぬようにするために重要である。

インシデントは、成功か失敗かに関係なく、ICSのセキュリティを高める追加情報を得る機会として利用すべきである。たとえば、至近弾のように、外部からの偵察が検出されたが弱点を悪用されるには至らない事例は、貴重な情報をもたらしてくれる可能性がある。ファイアウォール、ルータ、スイッチ、サーバ、ワークステーションのログを徹底的に精査することで、

多くの有用なデータを発見することができる。こうしたデータによりアナリストは、通常の活動のベースライン、及び不正アクセスの方法や成功の過程を判断することができる。インシデントは、システムに対する物理的な攻撃に必ずしも限定されない。アクセス権を得ようとする試みには、ソーシャルエンジニアリングなどサイバー関連以外の活動や、電子メールを使用して受信者にデータやパスワード、アカウント設定情報を開示するように働きかけるフィッシングの試みなどもある。

教訓の学習は、インシデントが確認されるごとに行うべきである。そうすることでインシデントを精査し、システムセキュリティに存在するアクセス経路を特定して閉じることができる。問題が見つからず修正されない場合、攻撃は、より簡単かつ頻繁に繰り返される恐れがある。

施設のインシデント以外のインシデントも精査することを強く推奨する。これは、実際のインシデントによる損害を被ることなく、ICSのセキュリティ状態を継続して改善する理想的な機会である。ほとんどの組織はセキュリティインシデントの詳細を公表することに積極的ではないため、被害を受けた組織から得たインシデント情報と教訓を確認するために、CSSPとICS-CERT、及び他のCSIRTと緊密に連携する必要がある。大規模な組織は類似の設備を複数所有している場合があるため、得られた教訓は組織内のすべてのサイトで共有することが重要である。

教訓の学習は、インシデント後できるだけ早く行う。通常は、回復と復旧の後に続けて行う。教訓の学習が遅れると、さらなる類似のExploitに対してICSを脆弱な状態に置いたままになる。教訓学習のガイドラインは以下のとおりである。

- 内部CSIRTのメンバーはなるべく全員が参加すること。異なる観点と経験から価値のある見方が生まれる。
- CSIRTのチームマネージャは、教訓学習実施のために召集をかけて開催する責任を負うものとする。議論とアクションアイテムの両方に注意を払う。
- 情報は、ベンダ、インテグレータ、及びICS-CERTを含む、国や専門的活動を行うインシデント対応チームなど、外部の情報源から探すべきである。こうして得た情報から、Exploitに関する詳細や他の人が脆弱性を是正した方法を知ることができる。
- 答えられなければならない主な質問は以下のとおりである。
    - 影響を受けた構成要素はどれか。種類、メーカーは何か。
    - 被害を受けたオペレーティングシステム（組み込みシステムも含む）は何か。
    - どのようにしてアクセス権を取得されたか。
    - 受けた損害は何か。受ける可能性のある損害は何か。
    - ICSへのアクセスを許したネットワーク脆弱性（存在する場合）は何か。
    - インシデントを防止した可能性のある標準及び技術ソリューションは何か。
    - インシデントを防止した可能性のある手続き及び方針は何か。
    - さらなるExploitの防止に必要な訓練は何か。
    - インシデントはどのように検出されたか。もっと早く検出、または防止できなかったか。

- まだ脆弱性は残っているか。どれくらいの時間残ったままか。
- ベンダはパッチまたはその他のソリューションを提供したか。提供があった場合、それらは適切なタイミングでICSに実装されたか。
- 機器、コミュニケーション、権限の範囲、ベンダとの連携、分析、意志決定、回復など、インシデント対応の構成はどのようなものであったか。
- 改善しプロセスを変更すべき領域はどこか。
- この情報は信頼できるパートナと共有してよいか、
- この情報は、適切な政府機関（対応チームを含む）と共有してよいか。

- 各弱点の識別情報に基づいて具体的に作業を参加者に割り当てて、それぞれの弱点に体系的に対処できるようにする。CSIRTチームマネージャは、さらなるExploitを防止するためのすべての活動が適切なタイミングで完了していることを確認する責任を負う。

5.2 再発の防止

脆弱性が発見されても、防止対策をとるまでその脆弱性は開いたままの扉である。教訓学習の主要な目的の1つが、インシデントを分析し、Exploitの再発を防止する行動を開始することである。インシデント防止の全体的な精査が有用である（セクション3「インシデント防止」参照）。

セクション3に示す推奨事項に加え、インシデントに対し、施設側で以下のうち1つ以上を実行することができる。

- **アクセス手段の特定**：アクセス手段の特定は、インシデントによって容易な場合と困難な場合がある。従業員または請負業者によるインシデント、または内部からのアクセスによるインシデントは特定が容易であるが、正当なアクセス権は提供しなければならないため解決が困難である。防止措置としては、人物背景調査のさらなる徹底、訓練の充実、情報を知る必要性と組織内における役割責任に基づくアクセス制御などが挙げられる。インシデントには、サーバ上に置かれたマルウェアが関与する場合がある。解決策としては、マルウェアの削除に続き、追加のウィルス対策支援や、ソーシャルエンジニアリングと防止技法に関するより詳細なユーザ訓練を行う。アクセス手段の発見が難しい場合のように、さらに困難な状況では、高い技術を持つ侵入者がネットワークログを消去したり、タイム

スタンプを偽装したり、ICSに対する必要なアクセス権や管理者権限が設定された、不正入手したアカウントを使用したりしている可能性がある。内部CSIRTによってアクセス手段を発見できない場合は、その手段を発見するため専門家による支援を要請する必要があることもある。アクセス経路が見つからない場合、最後の手段として、可能性のあるすべてのアクセス経路のセキュリティ強化を設備側で体系的に取り組む必要がある。

- **侵入者の動機の理解：**ICSのあらゆる面にリソースを割り当てることは困難なため、特定の対象領域のセキュリティを強化することが現実的である。たとえば、情報の窃盗が動機の場合、データベースがターゲットの可能性がもっとも高く、主要なデータベースサーバと管理システムのセキュリティ保護が当座の優先事項となる。世間の混乱、危害、世間の注目が侵入者の求める結果の場合、ICSの特定の構成要素に注目する必要があるかもしれない。動機が金銭的損害を会社に与えることであれば、生産プロセスがターゲットの可能性がある。動機を理解することで、ICS環境の特定の側面に、より迅速かつ絞り込んで注意を払うことができる。

- **特定のICS構成要素の評価及び強化：**アクセス手段は通常ネットワークが関係しているが、インシデントは、構成要素の特定のモデルやタイプに関連する脆弱性を露見させる可能性がある。ICS構成要素の評価では、パッチ未適用の構成要素、旧式の機器、または構成要素間の無防備な通信が露呈する可能性がある。解決策としては、機器の交換、パッチの適用、ICS内の構成要素周辺の境界の強化（構成要素の交換が容易にできない場合）が挙げられる。この分析により、古いシステム構成要素の交換に対するコスト面の正当な理由が得られる場合がある。

- **検出方法の精査：**通常、施設内でインシデントが発生した場合、運用されている検出方法が早い段階でその試みを検出できるだけの能力がなかったことを意味する。たとえば、実際のExploitに先立って、偵察活動が数日または数週間にわたって行われていた可能性がある。解決策としては、より強力な侵入検知手段とソフトウェアアプリケーション、またはログの精査と分析の必要性拡大が挙げられる。

5.3　フォレンジック及び法的問題

コンピュータフォレンジックというと、ほとんどの場合、インシデントを引き起こした人物または組織に対する法的措置で使用する情報及び証拠の収集と保全が連想される。ただし、

本文書の推奨プラクティスという観点からすると、フォレンジックは、インシデントの理解と分析に役立つ情報の収集にとどまらない。教訓の学習によって、将来の攻撃からICSを保護する方法につながる脆弱性が特定され、分析される。正規のサイバーフォレンジックのように情報収集に重点が置かれるが、見つかったデータの保全と保護に関してはそれほど厳しい要件があるわけではない。ここで定義した非正規のフォレンジックは、正式な手続きで見つかった証拠の取扱に関する要件も無視する。したがって、非正規のデータ収集と分析の目的は、ICSを強化することにある。正規のフォレンジックの目的は、刑事訴訟手続きの裏付けとなる、許容される法的証拠を収集することである。

非正規および正規のフォレンジック活動の両方で、困難の生じる可能性がある。たとえば、制御システム構成要素内のRTOSの多くは実行中にメモリを使用している。電源を切ると破損したカーネルが消去され、電源の再投入時には、最初に設定されていたパラメータで基本カーネルが再ロードされる。サイバー攻撃の間にカーネルが改ざんされた場合、攻撃時点のRTOSカーネルの状態を記録し、保全する簡単な方法は現在提供されていない。問題のある構成要素をネットワークから切断することで隔離し、電源を入れたままにしておけば、隔離したコンポーネントのカーネルのスナップショットを記録して、後の分析に使用することは可能である。

インシデントのほとんどの事例では、システム管理者またはプロセスエンジニアの優先事項は、できる限り早く通常の運用を再開することであり、被害を受けた機器を再起動することでそれを実行することが少なくない。再起動をこのような形で実行すると、証拠が破壊される可能性がある。再起動が必要な場合は、情報を取得するその他のフォレンジック手段を利用できる可能性がある。こうした手段には、サーバのシステムログ、ファイアウォールの双方向のログ、スイッチのログなどがある。これらの選択肢は、ログを保存する設定が不適切であったり、ログを保全する能力がなかったりという理由で利用できない可能性がある。

その対極では、ログに記録されるデータが多すぎれば、有用な情報が上書きされたり、破壊されたりする恐れがある。これはほとんどのIT要素にあてはまる。ログ記録の有効化を阻害する主要な要素には、ログの精査による異常な活動の検出、古いログの消去、アーカイブ保存、特定ログの保全など、管理上の作業も含まれる。これらのログは適切に保全されれば、発生した活動、発生した日時、発生の状況を知る上で不可欠なものとなる。しかし、ログの記録が不適切な場合、大量のデータと活動が記録され、フォレンジック調査にとっての価値が限られてしまう。

本文書は、ICSのフォレンジックの詳細についてはこれ以上言及しない。制御システムにおける正規及び非正規のフォレンジックとデータ収集の両方の詳細については、CSSPの下で作成されたもう1つの推奨プラクティスも参照のこと。当該文書は、“Recommended Practice: Creating Cyber Forensics Plans for Control Systems（推奨プラクティス：制御システムに対するサイバーフォレンジック計画の作成）”（2008年8月、DHS Control Systems Security Program作成）である。

ICSにおけるフォレンジックに関する参照情報として、NIST SP 800-61 “Computer Security Incident Handling Guide（コンピュータセキュリティインシデント対応ガイド）”やNIST SP 800-86 “Guide to Integrating Forensic Techniques into Incident Response（インシデント対応へのフォレンジック技法の統合に関するガイド）”、CSSPの“Creating Cyber Forensics Plans for Control Systems（制御システムにおけるサイバーフォレンジック計画の作成）”などのガイド文書もある。

6. 結論

本文書に示す手順は、ICSのユーザに対し、ICS環境の分析と理解、防止装置、インシデント発生時の対応方法と管理方法などのインシデント対応能力を確立する基本を示すものである。

以下の3つの行動が重要である。

- 組織の内外を問わず、過去のインシデントの経験から学ぶ。
- 考え抜かれた方針と手続きを含む、効果的な対応計画によってインシデントに備える。
- ICS内の脆弱性を評価し、システムを守る保護手段を実装する。

サイバーインシデントが実際に発生した場合に備えてさらなる対応活動を検討する。対応活動には、インシデントの検出、インシデントの影響の封じ込め、ICSからの脅威の排除、通常運用へのシステムの復旧などがある。

より高度で意欲的な当事者による脅威が増加し、企業ネットワークやインターネットへのICSの統合が拡大するなか、本文書及び他のインシデント対応文書に登場する関係者は、重要な設備の計画と手続きに組み込む必要がある。そうすることで、多くの問題の発生を防止し、施設による対応の必要が生じた場合、成果をもたらす効果的な形で対応することができる。

6.1 推奨参考文献

“Guide to Industrial Control Systems (ICS) Security（工業用制御システム（ICS）のためのセキュリティのためのガイド）” National Institute of Standards and Technology (NIST) Special Publication 800-82（最終公開草案）2008年9月、Keith Stouffer、Joe Falco、Karen Scarfone

“Computer Security Incident Handling Guide（コンピュータセキュリティインシデント対応ガイド）” NIST Special Publication 800-61、2004年1月、Tim Grance、Karen Kent、Brian Kim

“Guide to Malware Incident Preventions and Handling（マルウェアによるインシデントの防止と対応のためのガイド）” NIST Special Publication 800-83、2005年11月、Peter Mell、Karen Kent、Joseph Nusbaum

Handbook for Computer Security Incident Response Teams (CSIRTs)（CSIRTのためのハンドブック）, Carnegie Mellon Software Engineering Institute, 2nd Edition、2003年4月、Moira J. West-Brown、Don Stikvoort、Laus-Peter Kossakowski、Georgia Killcrece、Robin Ruefle、Mark Zajicek

“Recommended Security Controls for Federal Information Systems（連邦政府情報システムにおける推奨セキュリティ管理策）” NIST Special Publication 800-53, Rev. 2、2007年12月、Ron Ross、Stu Katzke、Arnold Johnson、Marianne Swanson、Gary Stoneburner、George Rogers

Security Guidelines for the Petroleum Industry（石油業界セキュリティガイドライン）third Edition、2005年4月、copyright 2005, American Petroleum Institute.

Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries（石油業界および石油化学業界におけるセキュリティ脆弱性の評価方法）2004年10月、American Petroleum Institute.

“Recommended Practice for Patch Management of Control Systems（制御システムのパッチ管理における推奨プラクティス）” DHS Control System Security Program (CSSP)（2008年12月）

“Technical Article: Security Incidents and Trends in SCADA and Process Industries（技術文書：SCADA及びプロセス産業におけるセキュリティインシデントと傾向）”2007年5月、Eric Byres、David Leversage、Nate Kube

ガイド文書“Guidance for Addressing Cyber Security in the Chemical Industry（化学産業におけるサイバーセキュリティ対応ガイド）” American Chemical Council and ChemITC, Version 3.0、2006年5月

“Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations（犯罪調査におけるコンピュータの捜索と押収及び電子的証拠の入手）”、2002年7月、Computer Crime and Intellectual Property Section – Criminal Division – United States Department of Justice.

“Creating Cyber Forensics Plans for Control Systems（制御システムにおけるサイバーフォレンジック計画の作成）” DHS Control System Security Program (CSSP)、2008年8月

6.2 Webサイト

http://www.kb.cert.org/vuls/

http://csrp.inl.gov/Documents/Forensics_RP.pdf

http://www.cpni.gov.uk/Docs/Guide_3_Establish_Response_Capabilities.pdf

http://www.cpni.gov.uk/

http://www.cpni.gov.uk/Products/bestpractice/3692.aspx

http://www.doecirc.energy.gov/index.html

http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf – Creating a Patch and Vulnerability Management Program

http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf – Information Security

http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf – Computer Security Incident Handling Guide

http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf – Guide to Malware Incident Prevention

http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf – Guide to Integrating Forensic Techniques into Incident Response

http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf – Guide to Computer Security Log Management

http://www.americanchemistry.com/s_chemitc/sec.asp?CID=1641&DID-6201

http://www.first.org/

http://www.enisa.europa.eu/act/cert

http://nvd.nist.gov/home.cfm

http://www.isa.org/

http://www.americanchemistry.com/s_acc/index.asp

http://www.americanchemistry.com/s_chemITC

http://www.usdoj.gov/criminal/cybercrime/

http://www.us-cert.gov/control_systems/csdocuments.html

7. 用語集

*CERT/CC（Computer Emergency Response Team Coordination Center）。*CERT/CCは1988年12月に、米国防省の一部である国防高等研究計画局（Defense Advanced Research Projects Agency）によって創設された。CERT/CCの目的は、インターネットセキュリティにおける脆弱性の研究、攻撃を受けたWebサイトに対するサービスの提供、セキュリティ警告の発表であった。CERT/CCは現在、Carnegie Mellon UniversityのSoftware Engineering Instituteに置かれている。

*NIAC（National Infrastructure Advisory Council）。*NIACは、国土安全保障省長官を通じ米大統領に、経済の18の領域を支える重要なインフラの、物理面及びサイバー面の両方のセキュリティについてアドバイスを行う。NIACは、保険社会福祉省、運輸省、エネルギー省など、他の機関の長に対し直接助言を行う権限を持つ。NIACは、重要インフラのセキュリティを確保するために公共部門と民間部門の間の連携と協力関係を強化し、リスク管理、情報管理、情報共有、保護戦略、及び公共/民間部門間の役割と責任の明確化に関する方針と戦略について助言を行う。

*NVD（National Vulnerability Database）Version 2.2。*SCAP（Security Content Automation Protocol）を利用して提示された脆弱性管理データに基づく標準を集めた、米国政府のデータベース。このデータベースは、セキュリティチェックリスト、セキュリティ関連ソフトウェアの欠陥、誤設定、製品名、影響に関する測定基準に関するデータベースで構成されている。NVDは、ISAP（Information Security Automation Program）を支援するデータベースである。