制御システム環境における サイバーセキュリティ文化の支援を目的とした 運用セキュリティ（OPSEC）の使用

第 1.0 版 推奨プラクティス草案

執筆：Mark Fabro（Lofty Perch Inc.）、Vincent Maio（INL）
協力 : Rita Wells、David Kuipers、Trent Nelson、Heather Rohrbaugh
INL Critical Infrastructure Protection Center
（重要基盤構造保護センター）
Idaho Falls, Idaho 83415

作成：米国アイダホ国立研究所
（INL：Idaho National Laboratory）

2007 年 2 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 ″ Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Systems Environments Version 1.0 Draft Recommended Practice″ 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/

目次

キーワード

制御システム、運用セキュリティ、OPSEC、セキュリティ文化、サイバーセキュリティ、産業ネットワーク

はじめに

数多くの公共・民間分野にわたる情報インフラには、IT の配備とデータ通信に関していくつかの共通の特性がある。制御システム領域においては、特にそれが顕著である。大部分の組織は堅牢なアーキテクチャを採用し、外部ネットワーク、業務ネットワーク、制御システムネットワークの統合を推し進めることで業務の強化とコスト削減を図っている。データに対するセキュリティは、多くの場合、用途に特化した技術を使用して配備され、ポリシー、ガイダンス、運用上の要件に基づくサイバーセキュリティ「文化」の形成によって支えられる。セキュリティ文化は、運用セキュリティ（OPSEC）の手法を使用することで、手続きとガイドラインを日常の運用に浸透させ、それにより経営側にも利用者側にもサイバーセキュリティの維持・強化の取り組みを促進することができる。

しかし、事業領域の保護に必要なサイバーセキュリティ計画や、セキュリティプログラムを支えるために形成されたセキュリティ文化を、制御システムの領域に簡単に持ち込むことはできない。隔離された運用、旧来型のネットワーク手法、職務活動における硬直的な役割分担などといった諸々の要因は、高度なサイバーセキュリティに関する能力、機能性、あるいはモチベーションを作り出す上で有用とは言い切れない。このため、組織の運用セキュリティを活用し、制御システムアーキテクチャ内の情報資産の保護に役立つ効果的かつ自立的なセキュリティ文化を確立するには、その施策の方針を示すガイダンスが必要である。

本書では、制御システムおよび産業ネットワークのサイバーセキュリティにとって非常に重要ないくつかの要素を示し、サイバーセキュリティ意識の高い文化の形成がそれらの要素によってどのように促進されうるかを概観する。また、運用セキュリティ計画の策定のための次の指針・方針を示す。

- 制御システムに適したサイバーOPSEC 計画の策定について
- サイバーセキュリティを運用ライフサイクルに組み入れる方法について
- 技術的および非技術的なセキュリティ問題緩和策の策定について

対象読者と適用範囲

本書の対象読者は、制御システム領域におけるサイバーセキュリティの開発、配備、改善を担当する管理者およびセキュリティ専門家である。システムオペレータやエンジニアが参照し、利用できるような柔軟な構成にもなっているが、制御システム環境に対するサイバーセキュリティプログラムの配備およびセキュリティ意識の高い文化の形成を担当する人員に読まれることを意図している。本書は、特定の分野に固有のサイバーセキュリティプログラムを策定する手法に取って代わるものではなく、一般的であるが特段の注

意を要するいくつかの領域について、関心を持つ者に指針を示すものである。とりわけ、現代的な IT（情報技術）領域でのサイバーセキュリティプログラムの配備経験者や、産業用制御アーキテクチャ向けにサイバーセキュリティ計画を配備する上での諸問題に取り組み始めた読者に最適であると考えられる。本書の内容は、高度な技術知識を要するものではなく、本書を新しい情報リソースの保護策を作成する際や、すでに実施されている保護計画を強化する際の土台として使用できる。

煩雑になるのを避けるため、読者全般にはある程度ITセキュリティの知識があるものと想定して、サイバーセキュリティのいくつか一般的な標準についてのみ言及する。本書は、セキュリティ意識の高い文化の発展に役立つサイバーOPSEC計画を策定する際に直面するいくつかの大きな問題に対処することを目的としている。読者には、本書で取り上げる基本的な標準から着手して、特定の分野により適したほかの資料や手引書も調べることを推奨する。さらに、自組織のITセキュリティフレームワークを土台にして制御システム分野におけるOPSECを作成していく中で、分野に固有のその他の堅牢なサイバーセキュリティの取り組みを取り入れてベストプラクティスの強化を図れることに注目する [1]。世界中で 40 を超える標準化機関が、制御システムのセキュリティに直接的または間接的な効果をもたらす指針の作成を行っている。さまざまな取り組みの成果を参考にしながら、本書を基礎として組織独自のOPSECプログラムを策定するとよい [2]。

背景

最近、テロリスト、国家、ハッカー、内部の脅威による、制御ネットワークへのサイバー攻撃の可能性に関する文献が増えてきた [3]。数十年前の古い技術で構築された基幹システムと、業務ネットワークやインターネットとの接続や相互接続が急速に進められているが、これによるセキュリティへの影響は明白であり、懸念を呈し、賢明な措置を求める相応の理由がある [4]。しかし、こうした情勢にある多くの業界で、実際にサイバーセキュリティが最優先事項として扱われているとは言えない。その理由は、サイバーセキュリティに投入するリソースがないこと、効果的なサイバーセキュリティ機能を配備する能力がないこと、脅威の存在を示す有力な証拠がないことなどさまざまである。また、制御システムのサイバーセキュリティを担当する人員に十分な知識がなく、制御ネットワークに最適の製品や対応策を判断できない場合や、効率よくサイバーリスクを低減する方法がわからない場合もある。また、主要な制御システムを保護するために必要な技術を配備した後も、運用レベルで防御戦略の維持、支援、継続に必要なセキュリティ文化が自然に発展していくとは限らない。

---

[1] ISA SP99、NIST、NERC、CIDX による具体的なサイバーセキュリティ関連資料など、公開されている分野別のガイダンスを確認することを推奨する。詳細については http://www.us-cert.gov/control_systems/csdocuments.html を参照のこと。

[2] ISA Intech Magazine 2006 年 12 月号 57 ページ「Power to Security Standards」（Joseph M. Weiss 著）

[3] http://www.us-cert.gov/control_systems/csthreats.html

[4] http://www.us-cert.gov/control_systems/index.html

重要インフラとして認識されている業界[5]（エネルギー、水道、交通、薬品製造など）では、制御システムや産業ネットワークのサイバーセキュリティに関して「しっかりした管理」と「しっかりした調査」（デューケア、デューディリジェンス）が必要である。必要な水準のセキュリティを保ちつつ、目的、効果、使い勝手、規制上の要件への順守、コストの制約などの問題とバランスよく対処するための適切な手順を実施していくことは、細心の注意を要する作業であり、容易に行えるものではない。

運用のサイバーセキュリティを適正なレベルに維持するには、制御システムに関連する各種要素（制御室の人員、ソフトウエアプリケーション、装置、ネットワーク環境全体など）のセキュリティを適正に確保しなければならないため、制御システムのライフサイクルの中で継続的な取り組みと統制が必要である。「しっかりした管理」では、経営管理層、制御システム管理者、制御システムおよびITシステムセキュリティ監督責任者が適正な手順を実施し、制御システムネットワークを保護するとともに、従業員と社会を確実に保護する必要がある。「しっかりした調査」では、「しっかりした管理」と同じ人員が予防型のプログラムに取り組み、サイバー脅威を特定し、サイバー空間における脆弱性の問題および制御システムとそれに関連する産業ネットワークへのサイバーセキュリティリスクの低減に関するその他の問題を理解・管理することが求められる。

事業領域において、または事業自体の中核を支える業界環境において、会社資産を保護するには、堅牢なセキュリティ技術や事業計画の構想を展開することに加え、サイバーセキュリティ文化を形成し増進していくことが重要である。セキュリティ文化を形成できる環境作りは、運用セキュリティの構成要素を開発することによって行うことができる。このOPSEC計画は、エンタープライズネットワークおよびITネットワーク用にあらゆる場所で実施されているプログラムと大きく異なるものではない。

事業領域で実績のあるサイバーセキュリティプログラムを単に改良して制御領域に移行するのは、必ずしももっとも効果的な解決策ではない。制御システムアーキテクチャにある領域特有の問題の一部に対応した新しいOPSEC計画を策定にあたっては注意が必要である。下の表 1 は、サイバーOPSEC計画に含まれると考えられる一般的なITセキュリティ要素を表に示し、制御システムにおける要件と異なるいくつかの点を明らかにしたものである[6]。

表 1　制御システムの要件

セキュリティ項目	IT	制御システム
ウイルス対策/ モバイルコード対策機能	一般的、広く普及	一般的でない、 配備が難しい
サポート技術の寿命	3～5 年	最大 20 年
外部委託	一般的、広く普及	ほとんど使われない
パッチの適用	定期的/計画的	遅い（ベンダ固有）
変更管理	定期的/計画的	旧来の方法 – 現代の

[5] http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html
[6] PA Knowledge Limited（2002 年）

		セキュリティには不適
時間に厳しい処理	遅延は 許容される場合が多い	安全のために 時間に対する要求は厳しい
可用性	遅延は 許容される場合が多い	24 時間 365 日（連続稼働）
セキュリティ意識	民間・公共分野ともに高い	サイバーセキュリティに 関しては低い
セキュリティテスト/監査	計画的、義務	停止に備えたテストを 時折実施
物理的セキュリティ	安全	良好だが 遠隔・無人の場合が多い

OPSEC 計画に必要とされるセキュリティ項目に、IT 領域と制御システム領域の要件それぞれが影響を及ぼすことは、上の表から明らかである。影響を適正に分析することなく IT 中心の既存計画を制御システム領域に適用すると、マイナスの結果を生じかねない。そこで、こうした違いに対応するサイバーOPSEC 計画を策定するための基礎となる重要な事項を準備する必要がある。制御システムのサイバーOPSEC 計画を策定するにあたっては、主として次のような事項が検討対象になると考えられる。

リアルタイムデータの必要性がセキュリティ技術の配備方法にどう影響するか。セキュリティ技術配備（暗号化など）の副作用として遅延が発生することが許容されるか。

オペレータのコミュニティとそれに関連する専門的な職能は OPSEC 活動にどう影響するか。

遠隔施設の物理的セキュリティは、ソフトウエアやファームウエアのアップグレードを目的とした、コンポーネントへのアクセスにどう影響するか。復旧やインシデント対応の所要時間についてはどうか。

テスト設備やステージング設備がない場合、セキュリティソフトウエア（ウイルス対策など）のアップグレード版を本番環境にインストールする前にどのような方法で評価するか。

本書では、制御システムの OPSEC プログラムにとって、ひいてはサイバーセキュリティ文化の形成にとって本質的な重要性の高い、いくつかのサイバーセキュリティ活動について述べる。それらの活動は、通常の事業運営とのバランスを考慮して行われなくてはならない。また、それらの活動は基本的に定型化された性質を備え、産業ネットワークや、コンピュータを利用した個別の制御システムが信頼性とセキュリティを保って稼働し続けることを可能にするものでなくてはならない。本書は、次のとおり大きく 3 つのセクションに分かれている。いずれのセクションも、OPSEC の主要な理念に取り組んで制御システムのサイバーセキュリティ文化を形成することに主眼を置く内容である。

セクション 1：OPSEC プログラムの策定：経営管理層から利用者へ

セクション 2：サイバーセキュリティ文化の持続：運用ライフサイクルへのセキュリティの組み入れ

セクション 3：技術的および非技術的解決策

セクション 1 では、運営管理、実施責任、効果的なサイバーOPSEC プログラムを策定するために管理者が実施する手順について述べる。ここで扱う内容は、OPSEC による統制を構成する中核的な要素の確認、OPSEC プログラム作成に関する問題へのそれら要素の適用、制御システムを考慮したプログラム内容の策定、管理の責任分界点の確立、また、実施期間を通じたプログラムの拡充である。

セクション 2 では、サイバーセキュリティを開発と運用のライフサイクルに組み入れる方法について述べ、制御システムおよび産業ネットワークにおける主要なセキュリティ目標を満たすための仕組みを示す。これにより組織は、管理者、オペレータ、その他の者に適用可能な、制御システム領域に適した自立的なサイバーセキュリティ機能の形成と維持のための能力を備えることができる。ここでは、たとえば「SPOF（Single Point of Failure：単一障害点）」などの問題と、クラスタリングやバックアップの使用に関する伝統的な IT 概念を取り上げる。

セクション 3 では、問題や被害の緩和策についての考え方を、技術的および非技術的見地の両面から説明する。OPSECの基本についてこれまでに論じた内容とあわせ、このような形でサイバーセキュリティ手法を示すことにより、ユーザはサイバーセキュリティに関して手持ちの駒を全般的に増やすことができ、セキュリティ文化を支えられるようにそれらの駒をどのように使うかを判断できるようになる。このセクションの内容は、制御領域におけるセキュリティ問題の緩和策のための技術的な取り組み、トレーニングおよび意識向上活動、およびサイバーOPSECプログラムの拡充に関する提案事項である。ここでは攻撃と対策については触れないが、読者には、サイバー攻撃と制御システムに関するUS-CERTの既存資料を確認することを推奨する[7]。

1. サイバーOPSECプログラムの策定：経営管理層から利用者へ

堅牢なサイバーセキュリティポリシーを実施するだけでなく、効果的なサイバーセキュリティプログラムの策定、支援、維持を経営管理層が行うことが、総合的に健全なサイバーセキュリティ体制をとる上で不可欠である。IT エンタープライズシステムと自動制御ネットワークを使う産業が考慮すべきサイバーセキュリティ上の問題は数多くある。たとえば、極秘の製品データの漏えい、制御データの破損、サービスの中断、自動制御下にある資産の物理的破壊などがある（最後の項目は、IT ネットワークと比較して制御システムや産業ネットワークに特有である）。経営的視点から見ると、制御システム分野におけるサイバーOPSEC プログラムの作成と維持は、従来の IT 分野の場合と非常によく似ている。しかし、ある種のニュアンスや文化の違いによってサイバーセキュリティプログラムの管理に困難が生じる可能性がある。それゆえ制御システム環境においては、IT 分野からいかにして適切な OPSEC の原理を再利用するかが課題になる。

[7] http://www.us-cert.gov/control_systems

こうした問題を緩和するために、経営管理者は産業分野に従事するユーザやオペレータの特有の要求、能力、運用上の要件を考慮したプログラムを根付かせることができなくてはならない。そのようなプログラムは多くの場合、次のように馴染みのある重要要素を含んでいる。

制御システムユーザ向けのサイバーOPSEC プログラムの作成

経営管理層の責任および文化的な考慮事項の定義

制御システムに対応した OPSEC の責任分界点の定義

制御システム向けのサイバーセキュリティ OPSEC ポリシーの作成

セキュリティ文化の形成に制御システムオペレータ/ユーザの意見を反映する体制の確保

制御システム OPSEC プログラムの施行と監視

1.1 プログラムの策定

制御システム領域に属する組織の多くは、より大きな企業や事業部門による何らかの運営の監督を受ける立場にある。現代的な事業体のほとんどが最新の IT 通信インフラを使用していることから、そうした事業体は（少なくとも何らかの水準の）サイバーセキュリティプログラムおよびポリシーを持っていると考えてよい。これは必ずしもプログラムが堅牢であることを意味せず、単に何らかのサイバーセキュリティが何らかの水準で実施されていることを示すに過ぎない。その実体はウイルス対策ソフトウエア、ファイアウォール、ユーザ認証といったものであり、いずれも、ほとんどの商用 IT ソリューションで見られる標準的なセキュリティ対策である。大規模な組織は、各種サイバーOPSEC 要素をあらゆる側面から監督する専門のサイバーセキュリティ機能を擁している場合もある。

従来の IT 領域のためのサイバーOPSEC プログラムがあれば（あるのが一般的である）、制御領域のためのサイバーOPSEC 構想を構築する作業ははるかに容易である。OPSEC 計画の構成要素は、それを運用する領域を問わず総じて非常によく似ている。このため、経営管理層にとってはすでに実績のある計画を制御環境に「移行」するほうが容易である。また、事業領域向けに実施されている計画がすでにある場合、制御領域の運営者がその計画にある程度（限定的であっても）関与している可能性も十分にある。このため、基本的に、サイバーOPSEC 計画の作成において上層部の賛同を得やすくなり、計画に説得力を持たせることも容易になる。

1.2 プログラムの要素

OPSECの要素は組織の要件に応じた独特の構成になる可能性がある。重要な構成要素をサイバーセキュリティプログラムの本質的な内容として確実に盛り込むための指針

として、ISO 27002（旧 17799）[8]などの規格が参考になる。プログラムの要素となる事項は次のようなものである。

1.2.1 リスク評価とリスク対策

この活動は、組織的視点から行われる全体的および統合的なリスク評価であり、制御システム領域のしっかりとした分析作業が含まれる。いずれにせよ、リスクを（資産価値としてではなく）もたらされる結果の関数として捉えると、制御システム環境に適した計算が容易になる場合がある。この計算には、制御領域に特有の要素である人命喪失、平均復旧時間、環境への影響などを考慮すべき場合がある。

1.2.2 制御領域のための情報セキュリティポリシー

この活動には、組織の事業目標、事業目標を達成する制御システムの役割、情報（サイバー）セキュリティへの全体的な依存性を完全に理解することが含まれる。また、この活動は実際のユーザやオペレータの要求を反映し、分かりやすく、当該制御領域に適用可能であり、使用する人々によって実施されるものである必要がある。

1.2.3 情報セキュリティの組織（内部、外部）

セキュリティガバナンス体制を創設、運営、監視するための経営管理体制を確立することが必要である。セキュリティプログラムには上層部の承認と支持が必要であり、セキュリティ機能は制御環境内のほかの IT 機能に可能な限り盛り込まれる必要がある。ほかの IT 機能には外部の組織も含まれる。また、サードパーティやほかのベンダに関係するセキュリティ問題および活動にも対応が必要である。

1.2.4 資産の管理、分類、制御

組織は自身の産業制御システム環境内にある情報資産を把握しておく必要があり、サイバーOPSEC 計画は、そうしたリソースを適切に保護できる形をとる必要がある。資産を所有者に割り当て、セキュリティ機能の適用をその所有権に割り当てれば、資産の分類および責任という 2 つの問題に対応できる。制御領域の情報資産は、保護の度合いを示す形で分類される必要がある。分類の結果として情報が適切にラベル付けされ、ユーザ、オペレータ、プロセスに割り当てられなくてはならない。

1.2.5 人的セキュリティ

アクセスと割り当てに関しては、組織の監督が常時必要である。新規採用者/在籍者/離職者の区別に基づいて人事部門に要件の割り当てを行わせると、制御システム業務としては、制御システム資産を使用している間の、ユーザや従業員の状況を持続的に把握できる。このモデルでは、ユーザの雇用前、雇用中、および組織からの離職後における資産保護に、セキュリティおよび適切な配慮を施すことができる。また、制御システム資産の構成、監視、運用のさまざまな役割の管理上の責任と実施責任を複数の人員で分担できるように、職務リソースを階層化すべきである。

---

[8] ISO Code of Practice for Information Security Management（ISO 17799、27002）
http://www.27000.org/

1.2.6 物理的セキュリティと環境セキュリティ

多くの制御システム領域には、物理セキュリティを効果的に確保する装置がすでに導入されている。そうした要素は、IT 機能が配備される前の段階で制御システム環境に導入されていることが多く、新しいセキュリティ技術に対応するために更新が必要な場合がある。その見直し作業においては、物理的な立入り制限、事務所、部屋、施設のセキュリティ確保、物理的アクセス管理策の提供、および火災、電磁波、破壊工作のリスクを最小限に抑えるための保護策の提供などが確認の対象となる。重要な制御領域においては、さらに対象を拡大して、何らかの活動のために電源供給とデータケーブルの十分な保護まで含めることがある。

アクセス管理と物理的アクセスには、遠隔施設のシステム中枢に関するメディア（ソフトウエア/ファームウエアのアップグレード版など）のインストールと管理も検討事項に入れる必要がある。多くのシステムアーキテクチャにおいて、保守作業を必要とする制御装置の設置場所が地理的に遠く離れていることはよくあり、適切な物理セキュリティが確保されていない可能性がある。しかし、そのような場所には作業者が出入りするため、現行の技術に対してアップグレードや修正を行うことができる。その際、システムに対してメディアの挿入、取り出しが行われることから、サイバー活動と物理的アクセスとの相関させることが有用であると認められる場合がある。多くの場合、遠隔施設はマスタ制御ネットワークへの有効な接続ポイントとなるからである。このため、物理的アクセスに関する活動のログとサイバー活動を相互に参照すると、システムへのアクセス状況全体をより確実に把握できる可能性がある（1.2.8 を参照）。

1.2.7 通信管理と運用管理

制御システム領域におけるあらゆる情報処理リソースの管理と運用の手順を示した正確な文書を定めるべきである。通信管理・運用管理の下位要素としては次のようなものがある。

- 運用手順
  - 変更管理
  - 職務分掌
  - 開発環境へのアクセス
- バックアップおよびデータ保管活動
- 悪意のあるソフトウエア（マルウエア）および攻撃からの保護
- サードパーティによるサービス提供
- システム計画および受入れ
- ネットワークセキュリティおよび監視
  - セキュアなネットワーク管理
  - ネットワークセキュリティ技術
  - ファイアウォール、ルータ、侵入検知

特に注目すべきはネットワーク管理の要素である。制御システム領域のサイバーセキュリティ要件としては、一般的なITネットワークに見られるものとは異なる内容の対応策が要求される。このような環境では、多層防御などの対策によって全体的なセキュリティ

体制を大幅に改善できる可能性がある[9]。制御システムのコンピュータネットワークにおいてセキュリティを実現・維持するには、接続された公衆ネットワークを通るデータの機密性と完全性を守るために特別な管理策を確立すべきである。また、ネットワークサービスの可用性を維持するための特別な管理策も必要とされる。

1.2.8 アクセス制御

多くの制御領域に見られる特有の信頼と権限のため、アクセス制御は単なる運用環境のユーザだけでなく、それ以外にも適用する必要がある。相互接続という制御システムの性質と、多くの制御装置が本来備えている特有の機能を考慮に入れるために、サイバーOPSEC 計画のアクセス制御機能を開発する際には多くの構成要素を検討する必要がある。堅牢なアクセス制御を定義するために検討する必要がある要素は次のようなものである。

- ユーザアクセスおよびユーザ責任の管理
- アクセス制御に関する業務要件の管理（企業領域における要件とは大きく異なる可能性がある）
- オペレーティングシステムのアクセス制御の監視
- 装置のアクセス制御の指揮
- モバイルコンピューティングの統制（遠隔地での活動、メディアのインストールを含む）

1.2.9 システムの調達、開発、保守

制御システムアーキテクチャ内で稼働する重要システムに堅牢なセキュリティが確実に適用されるために、セキュリティ機能は制御技術の本質的な機能として備わっているべきである。言うまでもなく、その実現は多くの組織にとって困難だと考えられる。表 1 のとおり、平均的なサポートの継続期間は 20 年程度の長期にわたるため、ユーザは所定のベンダの技術に「拘束」されることになる場合が多い。セキュリティはシステムに当初から組み込まれていることが理想であるが、現在運用されている重要システムは、堅牢なネットワークやサイバーセキュリティ（ベンダの設定した単純なパスワード以上のセキュリティ）が要求されなかった時期の設計によるものが多い。

情報セキュリティは、制御システムの仕様策定、構築/調達、テスト、実装に関するプロセスにおいて考慮される必要がある。セキュリティ要件、正当なデータ処理、ファイルの保護、および暗号化による管理策[10]は、すべて（ほかの要素と）組み合わされ、重要要件に関する 1 つの基本水準を形成するものである。さらに、ベンダとのやり取りに関するほかの側面（コーディング作法、不具合修正方法など）も含まれるべきである[11]。

---

[9] http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf

[10] http://www.gtiservices.org/security/AGA12Draft3r6.pdf

[11] http://www.msisac.org/scada/

変更を追跡管理しやすくするために、厳格な変更管理手続き（セクション 3 を参照）を実施すべきである。OS やソフトウエアパッケージに生じた変更は厳しく管理され、サイバーOPSEC 計画に反映されるべきである。

1.2.10　インシデント管理

制御システム領域でサイバーセキュリティインシデントが発生した場合に備え、しっかりとした報告活動が実施されている必要がある。インシデント報告に関しては既存のテンプレートやフレームワークが多数あり、また、伝統的なIT領域の報告に使用されているテンプレートも使用できる。しかし、制御システム領域におけるインシデントの管理および対応方法を策定、配備するにあたっては注意が必要である [12]。たとえば、多くのインシデント対応計画は、システムのシャットダウン、撤去、フォレンジック分析を必要とする。制御システムにおける産業アプリケーションの多くが本質的に極めて重要な性格を有することを考えると、こうした活動は不可能または著しく困難といえる。このため、インシデント処理とフォレンジック分析については、制御システムに特化したセキュリティマネージャ向けの指示や対応行動をまとめた独特の最終結果が得られるような、新しい戦略を模索する必要がある。

1.2.11　事業継続管理

事業領域の場合と同様、制御システム環境においても、運用継続性管理プロセスの設計、実装、定期的なテストを行うべきである。制御システムアーキテクチャを有する組織の多くが、物理的インシデントやその他の非サイバーインシデントによる中断の後、運用再開のために事業継続管理（BCM：Business Continuity Management）計画を実施しているのはもっともなことである。しかし、制御システム環境においてサイバー空間における運用の支援に必要な BCM 活動が検討され始めたのは最近のことである。その初期においては、既存の事業領域の BCM 計画を制御システム領域に転換するといった作業も行われてきた。事業領域の場合と同様に、こうした計画については、状況、運用能力、全体的な制御システムアーキテクチャの変化を踏まえ、定期的なテスト、保守、見直し作業が必要となる。読者には、この分野で行われてきた特有の作業を調べ（ISA、NERC など）、自組織の環境への適用可能性を確認することを推奨する。

1.2.12　コンプライアンス

多くの分野において、標準、規制ガイダンス、関連法規の条項に厳密に従うことは必要不可欠である。最近はさまざまな制御システム領域のサイバーセキュリティに関するベストプラクティスが多数策定されており、今後いっそうの増加が見込まれる [13]。また、IT 分野の場合と同様、OPSECを順調に実践し続けるためには、法律、取引契約、知的所有権、ベンダライセンスを遵守することが肝要である。

---

[12] https://forms.us-cert.gov/report/

[13] http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

2. サイバーセキュリティ文化の持続：セキュリティを運用ライフサイクルに組み入れる

制御システム環境における運用ライフサイクルは容易に確立されるものではなく、オペレータの活動、業務要件、技術のアップグレード、ベンダのサポート、安全性に関する継続的なトレーニングおよび意識向上活動など、数多くの関連機能を統合する必要がある。その上で、こうした機能（その他多数の機能）が連携して動作することにより、徹底したセキュリティが要求される精巧で複雑な環境が作られる。セキュリティ文化は制御領域に属する物理的資産の保護にも関係するため、ほとんどの組織には何らかのセキュリティ文化があるといえる。しかし、隔離されていたシステムを企業体、業務パートナー、提携先サイトと接続するプラクティスの広がりとともに、そうしたセキュリティ文化をサイバーセキュリティにまで拡大することが必要になった。

すでに述べたとおり、技術の所有権（アクセス権）をオペレータやユーザに割り当てることは、情報資産の戦術的保護と、サイバーセキュリティに関連する文化活動の導入に役立つ。しかし、制御システム領域においてセキュリティ機能の維持と自己継続的なセキュリティ能力の形成を促すには、図 1 のとおり、サイバーセキュリティと OPSEC プログラムをシステムライフサイクルに組み入れる必要がある。そうすれば、サイバーセキュリティを運用のあらゆるレベルに導入し、必要とされる浸透度を達成し、サイバーセキュリティ文化の育成に適した環境を用意することができる。

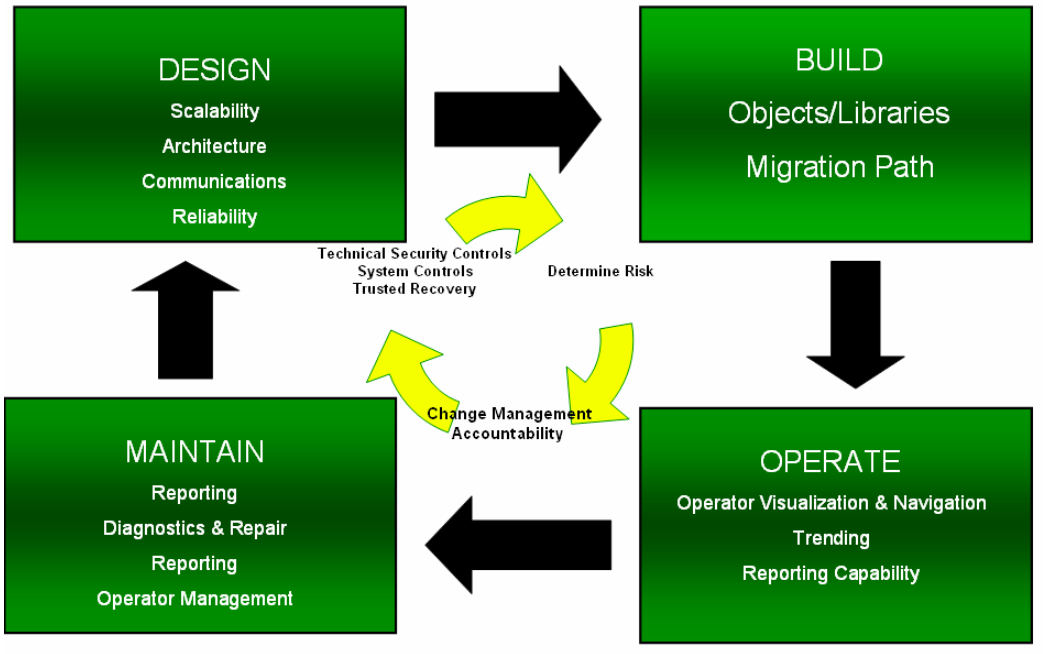

図 1. セキュリティ要素に着目したシステムライフサイクル概念図

DESIGN	設計
Scalability Architecture Communications Reliability	スケーラビリティ アーキテクチャ 通信 信頼性

BUILD	**構築**
Objects/Libraries Migration Path	オブジェクト/ライブラリ 軽減パス
MAINTAIN	**保守**
Reporting Diagnostics & Repair Reporting Operator Management	報告 診断・改修 報告 オペレータ管理
OPERATE	**運用**
Operator Visualization & Navigation Trending Reporting Capability	オペレータ視覚化・誘導 動向把握報告機能
Technical Security Controls System Controls Trusted Recovery	技術的セキュリティ管理策 システム管理策 高信頼リカバリ
Determine Risk	リスクの特定
Change Management Accountability	変更管理 実施責任

図 1 から明らかなように、ライフサイクルにサイバーセキュリティを組み入れる機会はさまざまな箇所にある。その他の主要なライフサイクル要素と同じくセキュリティを共通的な戦略の一部を構成する要素とし、運用文化全体に浸透させることは可能である。セキュリティは一過性の作業で実現できるものではなく、むしろそれ自体がプロセスであることを認識し、ライフサイクルアプローチを使用してサイバーOPSEC 計画を制御システム領域に実装すると、ある程度の柔軟性が確保される。しかし、真に効果的なセキュリティを確保するには、ライフサイクルのできるだけ早い段階において OPSEC プログラムの基礎を確立する必要がある。

制御システム環境では、産業制御システムという領域の性質（ベンダへの特化）と、対応する IT 領域内の標準的要素との微妙な違いから、一部の要素に関して特別の注意が必要となる。このため、一部のフェーズについてはサイバーセキュリティの組み入れが困難になる可能性がある。しかし、サイバーOPSEC に対して事後的なアプローチをとると、かけた労力の度合いにかかわらず時間的にも金銭的にもコストがかさみ、オペレータ、エンジニア、管理者の意見がセキュリティに否定的になる場合が多いことが実証されている。そのような事態はサイバーセキュリティ文化にとってマイナスであり、避けるべきである。実際、運用のあらゆる側面にサイバーセキュリティをあらかじめ盛り込んでおくことは OPSEC ベストプラクティスに含まれる要素の 1 つである。

制御システムのハードウエア、ソフトウエア、サイバーセキュリティ製品が提供する保証水準を評価する際は、複数回の運用面の保証とライフサイクル面の保証を評価プロセスに含める。運用面の保証に関しては、特定の産業制御システムネットワーク製品のアーキテクチャ、備えている機能、および機能性が評価される。これらの項目は、産業顧客がその製品を使用することで必要な水準の保護を享受し続けられるかどうかを評価するものである。評価プロセスにおいて調査される運用面の保証としては、たとえば、アクセス管理メカニズム、特権コードとユーザプログラムコードの分離、監査と監視の機能、隠れ

チャネル分析、および、製品が予期せぬ状況に直面した場合の高信頼リカバリなどがある。現在、セキュリティに対応した制御システムの戦略的調達について所有者/オペレータに指針を示すガイドの策定作業がいくつか進められている[14]。

ライフサイクル面の保証は、制御システム製品がどのように開発されたものであり、その開発中どのようにして品質が維持されたかに関係する。設計フェーズの基礎は、スケーラビリティ、アーキテクチャ、通信、信頼性である。信頼性は、システムが特定の条件下で長期の運用を維持できる能力を実現するものとして、伝統的にもっとも重要な要素と見なされてきた。このためシステムセキュリティに関しては、システムの可用性や、システムの機能実行における信頼性と結びついた文化が発展してきたのである。システム保護の施策はこの立場から行われ、サイバーセキュリティに対する配慮を含んでいないことがよくある。そうした考え方はサイバー空間をほとんど考慮せずに発展してきたため、対象を拡大してサイバーセキュリティを視野に入れさせる必要がある。

当該製品のライフサイクルにおける各段階には、「信頼に足る」との判定を受けるために必要な何らかの標準や期待水準が設定されていることがある。ライフサイクル面の保証に関する標準としては、たとえば設計仕様、クリッピングレベル設定、単体テストおよび統合テスト、構成管理、高信頼配布などがある。優れたセキュリティ水準を達成した製品を提供しようとする制御システムベンダは、これらの各項目の評価とテストを受けることになる。つまりサイバーセキュリティを（全体的なサイバーOPSEC 計画の一部を構成する要素として）確実にシステム設計プロセス内に組み入れるには、ユーザとベンダの間に効果的な関係が成立している必要があることは明白である。

もちろん、サイバーOPSEC 計画の支援と制御システム情報資産の保護に使用できる技術や戦略は商品としても提供されている。しかし、投資収益率の点でもっとも優れているのは予防的な問題緩和活動であることを考えると、サイバーセキュリティを早期に導入することが施策全体を成功に導く条件の 1 つであると考えられる。以降のセクションでは、運用面およびライフサイクル面の保証に関するいくつかの問題を取り上げる。これらは制御システム製品の評価にかかわるだけでなく、製品が実装された後には重要インフラまたは産業の責任にもかかわるためである。サイバーOPSEC を支援する要素は、設計・構築・運用・保守の 4 つのフェーズに分かれたサイクル全体の上に戦略的に配置される。この結果、サイバーセキュリティが微細な末端レベルまで浸透し、サイバー空間に対する高い意識を持ったセキュリティ文化の形成が促される。

2.1 クリッピングレベル

設計フェーズと運用フェーズの両方において、産業システムを使用する組織は、特定のエラーが何回発生したら活動に異常があったと見なすかのしきい値をあらかじめ定めておくことができる。多くの制御領域では、正常な運用活動からの逸脱が発生することはまれである。ほとんどの場合、ネットワーク活動と通信は監視可能であるため通信環境の動作は予測可能である。このため、データトラフィックや活動が平常時のしきい値を超えた場合には異常事態を調査する活動を開始させることができる。「クリッピングレベル」とも呼ばれるこのしきい値に定義したレベルを超えると、警報が発動される。

[14] http://www.msisac.org/scada/

サイバーセキュリティの異常イベントや制御システム領域内の活動について検出と通知を行うことは、要するに履歴上の意味づけ（異常イベント監視）を行うことに似ている。サイバーセキュリティのしきい値は、制御システムにおいて正常と見なされるサイバー関連活動の基準値であり、これを超えると警報が発せられる。正常な運用活動を監視するクリッピングレベルと同じように、サイバーセキュリティのクリッピングレベルは、ユーザおよびサイバー活動に関して異常な活動を検出した場合に警報を発動する。

大量のイベントが発生する場合に対応するには、侵入検知システム（IDS：Intrusion Detection System）を使用して活動状況や行動パターンを追跡する方法が考えられる。蓄積される膨大な監査ログの監視を続けて特定の活動パターンを正しく識別する作業は、人手で実行すると負担が大きくなりすぎる場合があるからである。クリッピングレベルを使用する目的は、全体的な状況把握の手段を強化し、被害の発生前に管理者に警報を送信できるようにすることと、サイバー関連の攻撃が行われている可能性があるときにその旨を警告できるようにすることである。また、技術的または非技術的な問題緩和戦略を検討する際の参考として観察データを使用する用途や、資産の詳細な動作を調査してシステムに対するリスク状況を正確に把握する用途も考えられる。読者には、制御システム領域のセキュリティ技術に関する詳細な論考を確認することを推奨する[15]。

2.2 構成管理、アクセス管理、変更管理

これらの領域内にある通信ネットワークが接続され、提携先や業務ネットワークなどが制御領域に接続して運用データを収集するようになるにつれ、情報リソースの保護を念頭に入れた戦略を配備する必要が生じている。このような問題に組織が対処し、資産管理や運用管理などの重要分野で指針を提供できるようになることも、サイバーOPSEC 計画に含まれる事項である。

この管理項目の中で注目に値するのは、システムライフサイクルの保守フェーズに関連する変更管理である。産業システムを運用する組織にはほぼ間違いなく、システムライフサイクルの保守フェーズに関連する何らかの変更管理ポリシーがある。しかし、その変更管理プラクティスは実際の自動化プロセスには必ずしも該当しない。このポリシーは通常、通信システム、オペレータインターフェイス、診断ツール、その他システムの信頼性全体に関する要素など、大きなシステム構成要素の変更に適用される。システム間が接続されるようになったため、ネットワークに接続された情報資産や、安全性とプロセス制御にとって非常に重要な情報資産を保護するために、伝統的な変更管理プロセスを拡張する必要が生じた。変更管理の構成要素としては、施設内で変更を実施する方法、制御システムネットワーク内で変更を実施できる人員、変更を承認する方法、変更を文書化してほかの制御システムユーザやほかの従業員に伝達する方法、および、システム復旧をサポートするために変更をバックアップする方法などがある。

これらのポリシーが実施されていなければ、制御システムのユーザによって、ほかのユーザに知られることなく、あるいは承認を受けることなくシステムに変更が加えられる可能性がある。産業レベルでは、変更（フィールド装置のアップグレード、新しい HMI［Human-Machine Interface］装置への交換など）が文書化されずに実施されることはあまりないが、運用直前のサイバーインフラに対する変更などは必要に応じて行われる場合が

[15] http://csrp.inl.gov/

あり、文書化されていないと悪影響が生じる可能性がある。前のセクション 1.2.7 で通信管理および運用管理の要素として述べられている手順的な OPSEC 要素は、セキュリティ文化のサポートに関して非常に重要な役割を担うものである。さらに、変更管理は設計フェーズと運用フェーズの両方と密接な関係があり、産業の実稼働環境に変更を適用する前にはテストと評価の作業が必要だという点には言及しないわけにいかない（後のセクション 2.2.1 を参照）。

厳格な規制の対象となる医薬品やエネルギーなどの産業には、制御システムや産業ネットワークに対して実施してよい作業の具体的な内容と、作業を実施できる厳密なタイミングや条件を定めた厳しいガイドラインがある。そうしたガイドラインは、下流工程にかかわるパートナーやひいては製品のユーザに影響が及ぶことを防ぐ目的で定められている。変更に関する厳密な制限やガイドラインがないと、産業制御システムネットワークに誤って脆弱性が持ち込まれることになりかねない。しかも、変更管理がない場合、実装が済んだ後に行われた変更を監査する作業は非常に煩雑になる。管理者の作業を行いやすくするために、整然とした変更管理プロセスを実施すべきである。このプロセスは、変更管理ポリシーの中で述べられるべきものである。変更の種類は一定でなくても、各種手続きの標準的なリストが用意されていると、プロセスの管理しやすさを保ちやすくなり、また、確実に予測可能・反復可能な方法で変更を実施しやすくなる。

報告にはやりとりが必要であり、組織では変更管理ポリシーから産業領域への対応づけが行われることから、セキュリティ文化を育成する環境を形成する機会が存在する。可能な限り作業部会や支援チームを作り、情報インフラへの変更の報告が効果的かつ適時に行われるようにすべきである。以降のセクションでは、ネットワーク通信、セキュリティ、情報ベースのプロセスに影響する、あらゆる産業システムの変更管理ポリシーに含まれるべき要素の例を示す。

2.2.1 変更実施要求

変更実施要求は、制御システムへの変更の承認責任と制御システム環境内で実施される変更活動の監督責任を持つ人員またはグループへ提出される。

2.2.2 変更承認

変更の要求者は、制御システムに対する変更に正当な理由があることを説明し、適用のメリットおよび発生しうる問題を明示する必要がある。場合によっては、変更の承認前に、要求者が追加調査を実施してさらなる情報を提供するよう求められることもある。

2.2.3 変更の文書化

承認を得た変更は変更ログに入力される。このログは、完了までのプロセスが進むたびに更新される必要がある。

2.2.4 テストの実施および結果提示

制御システムの変更は十分にテストされる必要があり、予期せぬ結果が生じた場合はそれを明らかにする必要がある。変更の重大度によっては、変更内容と適用作業を変更管

理委員会に示すことが必要な場合もある。IT ネットワークの場合と異なり、産業ネットワークやその制御システムへの変更は、単純に 24 時間 365 日いつでもテストできるわけではない。これはほとんどの産業に言えることである。本番環境の制御システムに変更を適用するための運用停止スケジュールを設定する前に、場合によっては、変更を検証するためのテストベッドが必要となる。

2.2.5 適用スケジュール

制御システムの変更についての完全なテストと承認が完了したら、変更適用作業の各段階に関する見通しと必要なマイルストーンの概要を記したスケジュールを策定する。作業手順は完全に文書化され、進捗は監視される。

2.2.6 経営管理層への変更報告

制御システムの変更に関する情報を要約した完全な報告書を経営管理層に提出する。経営管理層に常に最新の情報を提供し、継続的な支持を取り付けられるよう、この報告書は定期的に提出するようにしてもよい。こうした手順は、通常は産業施設で実施される大規模な変更に関して適用される。一般にこの種の変更はコストがかかり、重要な情報インフラや制御システムへの影響が長く続くことがある。しかし、小規模な変更も同じ種類の変更管理プロセスを経るべきである。

制御システムの LAN サーバにパッチを適用する必要がある場合は、前もって本番環境以外のサーバでテストし、制御システム部門の管理者またはネットワーク管理者の承認を得て、さらに、パッチによって悪影響が生じた場合に備えてバックアップおよび「切り戻し計画」を用意しておくことが望ましい。また、システムまたはネットワークに変更を適用する前に、運用部門が承認済みの「切り戻し計画」を作っておくことも重要である。

フィールド機器をアップグレードしてソフトウエアファームウエアを最新バージョンにする作業には、変更管理上の困難が伴う。制御システム領域の効果的なセキュリティ体制を保つ上で非常に重要な問題の 1 つは、主要な装置を常に最新のソフトウエアファームウエアで動作させることである。多くのインストール環境では、アップグレード作業がどのように行われたかの正確な記録を残すことは非常に手間がかかる。アップグレードを必要とする装置の数が多い場合は特にそうである。制御システムおよび産業ネットワークに対する変更は、とりわけ大規模で動的な環境においては、OPSEC プログラムの成功にとって非常に重要な要素である。制御ソフトウエア構成とネットワーク装置に対する変更は、自動化環境で実施できる。以上のすべてについて、詳細を整然と管理し続けることが不可欠である。リビジョン管理、つまり、適正なバージョンのファームウエアやソフトウエアがインストールされた状態を保つことは、効果的で堅牢かつセキュアな運用を維持することの中核をなす要素の 1 つである。

制御システム環境で実施される可能性のある変更には、次のようにさまざまな種類がある。

- 新しい制御ハードウエア、終端装置、サーバ、コンピュータ、もしくは、制御または SCADA LAN へのあらゆる追加ハードウエア（センサ、制御装置など）のインストール

- 新しいアプリケーションおよびOSプラットフォームのインストール
- 異なる構成設定の適用
- パッチや更新プログラムのインストール
- 新しい技術やプロセスの統合
- ポリシー、手順、標準の変更
- 新しい規制や要件の適用
- 有線または無線ネットワークで接続されたシステムへの新しいネットワーク装置（遠隔操作LANアクセス装置の一時または新規追加など）の統合
- コンポーネント、アプリケーション、データへのユーザによるアクセスを可能にする内部または外部データ接続の追加

2.3 システム制御

ITネットワークの場合と同様に、システム制御も産業ネットワーク向けOPSECの一部を構成する要素である。特定の制御システム構成要素の一部（HMIコンピュータ、FEP［Front-End Processor］）に関するOSでは、常に正しいセキュリティコンテキスト内で命令が実行されるようにするために、特定の管理策を実施する必要がある。ほとんどのOSには、特定の種類に属する命令の実行を制限し、制御システム要素のOSが特権状態または管理者状態になっている場合にのみ実行を許可できるメカニズムが備わっている。これを使用すると全体的なセキュリティおよび制御システムの状態が保護され、安定的かつ予測可能な方法でシステムが動作することを保証しやすくなる。

したがって、制御システムや制御システムリソースの適正な運用を定めた運用手順を策定する必要がある。これには、システムの起動およびシャットダウン手順、エラー処理、既知のソースや信頼できるソースからの復元などがある。特定の制御プログラムからフィールドのハードウエア装置へ命令を送信する必要がある場合、その要求は通常、より高い権限のプロセスに引き渡される。これはOSのアーキテクチャに組み込まれた機能であり、どのプロセスが特定種類の命令を送信できるかはOS内の制御テーブルに基づいて決定される。入出力命令の多くは特権命令として定義され、OS自体による実行以外は許可されない。ユーザプログラムで入出力情報を送信するには、そのプログラムからシステムの中核部分に通知を送る必要がある。普通、中核部分には、システムの内部リングとして機能する特権プロセスがある。そうしたプロセスはシステムサービスと呼ばれ、ユーザプログラムのプロセスによるアクション実行を（一時的に高い権限を付与することによって）承認するか、ユーザプログラムの代理となるシステムのプロセスを使用して要求を完了させる。

2.4 高信頼リカバリ

制御システム環境内のOSまたはアプリケーション（HMI、FEPなど）にクラッシュまたは障害が発生した場合、そのことで制御システムが何らかのセキュアでない状態に置

かれる事態は避けるべきである。標準的な開発と設定フェーズにおいては、制御システムは一般に障害への「耐性」を備えたシステム、つまりシステムに被害をもたらさないものとして設計される。しかし、新しいシステムやより堅牢なシステムが制御システム領域に導入されると、完全性を備えたシステム復旧手段が必要となる。現代的サイバー攻撃の傾向をいくつか見てみると、攻撃内容の主要な要素の 1 つは、侵害したシステムの障害や再起動を強制的に発生させ、悪意のあるコードによって情報リソースの機能を阻害することである。そこで、システムの故障と復旧（場合によっては複数の構成要素にわたる）に対処するサイバーOPSEC 計画の構成要素として、復旧に関する安全策を設計フェーズと保守フェーズに組み入れる。

一般に、ある種の障害に対して制御システム構成要素の OS がどのように反応するかは、ユーザ/オペレータにとって有用であると考えられ、障害が持つ意味を理解しておくことは、制御システム領域のサイバーセキュリティをよりよく理解する上で役立つ可能性がある。また、トレーニング、対応、管理のプラクティスを盛り込んだ効果的なサイバーOPSEC 計画が適用されると、システム停止時間を短縮し、全体的なセキュリティ体制を改善できる。

システム障害は次のように分類できる。

- システムの再起動
- 緊急時のシステム再スタート
- システムのコールドスタート

システムの再起動は、システム自体が適切な方法でシャットダウンした（または強制シャットダウンされた）後に、TCB（トラステッドコンピューティングベース）障害への対応として実行される。また、システムの環境内に一貫性のないオブジェクトデータ構造が見つかった場合や、重要な作業に不可欠のテーブルに十分な空き領域がない場合にも、システムの再起動が実行されることがある。再起動すると、多くの場合はリソースが解放され、制御システム構成要素はより安定して安全な状態に戻る。

緊急時のシステム再起動は、システムが障害により不適切な方法で停止した後に実施されることが多い。考えられる原因は、システムの中核的な操作が機能しなかったことや、権限レベルの低いユーザプロセスがアクセス制限されたメモリセグメントへのアクセスを試みたことなどさまざまである。原因となった事象がセキュリティ上問題のある活動と見なされ、状態を回復するために再起動せざるを得ないとシステムに判断された可能性がある。これが実行されるとシステムは保守モードに入り、実行されたアクションから復旧した後、一貫性と安定性が確保された状態でオンラインに復帰する。

システムのコールドスタートは、予期せぬ活動が発生し、通常の復旧手順ではシステムを一貫した状態に戻せない場合に実行される。制御システムは復旧を試みるが、システムおよびユーザオブジェクトは一貫性のない状態のままになる可能性がある。場合によっては、制御システムのユーザまたは管理者が介入してシステムを復元することが必要になる。

OPSEC の観点から言えば、必要なファイル構造を監視して完全性や機能性を確認できる能力があると有利である。また、継続稼働が期待されるシステムの場合、予定外の再起動は深刻なセキュリティ問題につながる可能性がある。サイバーOPSEC 計画には、インシデントを観察して報告する方法についての説明とガイダンスを盛り込むべきである。そうすれば、運用報告の新しい標準として、あるいはオペレータによる既存の報告の仕方を補強するものとしてサイバーOPSEC 計画を配備できる。いずれにせよ、伝統的な復旧作業にサイバーセキュリティを適用できると、積極的なサイバーセキュリティ文化の形成に役立つ可能性があり、制御システム情報アーキテクチャの全体的な信頼性をサポートすることになる。あらゆる障害や再起動の場合と同様に、こうした事象においては即時の対処が必要なセキュリティ問題が発生している可能性があるため、原因を調査すべきである。

現代的な制御システム領域には、あらゆる壊滅的な障害に対応できるよう、待機系ネットワークおよびミラーリングされた主要リソースによる冗長性が備わっている。ネットワークインフラでは、ただちに実稼働可能な「ホットスタンバイ」と呼ばれるオンライン情報・制御システム資産を常時待機させていることが多い。主系システムに障害が発生した場合はこの待機系システムがオンラインに切り替わる。運用（およびサイバーセキュリティ）にとって肝要なのは、待機系システムが最新の構成設定に完全に準拠しており、必要が生じたときには主系システムとまったく同じ構成およびシステムアップグレード状態で実稼働を開始できるということである。そうすれば、冗長系システムへの切り換えが必要になった場合にも、主系システムが稼働し続けている場合と同様の運用を維持可能であり、実際そのような運用が行われることになる。ところが、多くの組織では、重要な待機系システムに対して主系と同じサイバーセキュリティ標準に基づくアップグレードや構成設定を適用していない。実際、待機系システムが脆弱性を抱えていた事例も確認されている[16]。

OPSEC 計画を実施し、このような問題の管理と報告の方法をユーザに指示することで、有効な文化的影響をもたらすだけでなく、保守や設計などライフサイクルの重要フェーズに役立つ情報を得ることができる。また、サイバーリスクおよびリスク緩和活動についての理解を深めさせる目的で観察と報告を使用することもできる。

3. 技術的および非技術的解決策

情報および情報資産を保護するために策定されたプログラムは、サイバーセキュリティの「3 本柱」、すなわち機密性・完全性・可用性（C-I-A：Confidentiality-Integrity-Availability）をモデルとしているものが多い。このモデルでは可用性が基盤的要素の 1 つとされているが、制御システムに適用される場合、可用性は最優先の扱いを受けることがほとんどである。それが適切かどうかはさておき、こうした扱いは、サイバー的な観点を含まない従来のセキュリティ文化においてシステムの連続稼働が運用活動の最重要事項と見なされてきたことの結果にほかならない。これらのシステムにおいては、オープンなネットワークとの融合やサイバーリソースを利用した効率向上が進み、機密性と完全性の優先度も可用性と同様に高まるものと考えられる。

[16] http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2003/in200314.pdf （2007 年 1 月 26 日）

単にサイバーセキュリティの C-I-A モデルが確実に実装されるようにするだけでは、現代の環境に適した保証を提供するために十分とは言えない。技術的および非技術的活動の両方の副産物として効果的なサイバーセキュリティ文化を形成することの必要性はすでに明らかである。環境内の全体的なサイバーセキュリティリスクを低減する作業は、技術とポリシーだけで行えるものではない。伝統的な文化によって物理的資産の保護と運用センターのアクセス制限が実現されてきたのと同様に、制御システムのための現在的なセキュリティ文化にもサイバーセキュリティが組み込まれる必要がある。ネットワークとリソースの可用性は、実際にそれらが失われるまで十分に評価されることがない。制御システムの運用に関しては特にそうである。

既存の堅牢な IT セキュリティプログラムによって提供される能力には、組織の制御システム領域において再利用可能なものがあり、制御システム環境におけるサイバー OPSEC 構想の強化に使うことができる。多くの場合、そうした能力はライフサイクル機能の外側に存在する複数の技術的および非技術的解決策を組み合わせたものであり、補助的なサイバーセキュリティ文化を育成するために進行中のサイバーセキュリティ OPSEC プロセスに貢献するものである。全体として、サイバーOPSEC 構想の支えとなり得る主要な問題緩和戦略はいくつか存在するが、それらは同時に、充実したサイバーセキュリティ文化の形成に大きな影響を及ぼす場合がある。このような要素としては、管理作業、ユーザの実施責任、SPOF 対策、セキュリティ意識向上トレーニングなどがある。

3.1 管理作業

3.1.1 職務分掌

管理的マネジメントは重要であるが、制御システムやそれに関連する産業ネットワークにおける OPSEC プログラムの観点では見落とされることが多い。管理的マネジメントには、制御領域が本質的に抱えている脅威（信頼された内部者など）の緩和という 1 つの側面がある。

「職務分掌」概念などの伝統的な原則は、重要インフラや産業のセキュリティが 1 人の人員の単独行動により制御システムを介して侵害されることを防ぐためのものである。つまり、誰も単独で攻撃を実行することはできず同僚の協力が必要となるようにする。こうしたプラクティスは、現に多くの組織で内部の脅威を緩和するために導入されている。運用領域に対する悪意のある行動が内部から発生するのを抑止する施策としては一般的である。しかし、サイバーセキュリティに関しては、リスクが外部の攻撃者にまで拡大されることに注意する必要がある。また、信頼できる内部者が外部の攻撃者に協力するリスク（情報やアクセス手段を提供するなど）や、攻撃者が信頼できる内部者になって外部からのアクセスを利用した攻撃を行うリスクもある。

歴史的に、そして通常は物理的領域から発生する攻撃に対応するものとして、職務分掌は、攻撃の実行と成功のために 1 人の人間が費やす全体的な労力を増大させる。運用上は、自動制御下の重要資産（基幹的な変電所、使用頻度の高い鉄道線路の分岐器、廃水処理施設の塩素タンクなど）に関係するリスクの高い活動は複数に分割され、異なる人員や部門に振り分けられる。

しかし、現代的な制御環境の場合、こうした中核的な活動を取り仕切るのはコンピュータシステムであり、そのプログラムやプロセスを監督するのは 1 人の人員であることが多い。また、そのコンピュータシステム上のコンピューティングリソースを悪意ある者が単独で変更、更新、使用できる場合もよくある。このため、物理的領域における重要な運用の保護には以前から有効であった職務分掌の考え方も、サイバーリソースにまで拡大する必要がある。とはいえ、サイバーOPSEC 計画に含まれるほかの側面と同様、自動制御機能の実行効率が職務分掌によって損なわれることがあってはならず、セキュリティとビジネス機能のバランスを入念に調整することが必要である。

制御システムオペレータ各員の役割については、職務内容を完全かつ整然と定義する必要がある。サイバーセキュリティ担当者は、それらの職務内容に基づいて制御システムに対するアクセス権や具体的な制御システム操作の許可を割り当てる。このためには、組織にサイバーセキュリティ管理専門のチームを設ける必要が生じる可能性がある。このようなチームは中小規模の事業体には存在しないことも多いため、ぜいたくな要求ではある。また、運用環境の管理作業を管理サービス業者や提携先サイトに委託している場合など、職務分掌の概念そのものを適用することが現実的でない状況もありうる。そのような場合も、相応の努力によって、作業の実施に必要な制御ネットワークリソースへのアクセスだけがオペレータに許可されるようにすべきである。たとえば、OPSEC パラメータの定義や文化的要素の浸透に関しては、構成設定や関連するプログラムコードを作成した制御システム構成専門家やエンジニアが自分の作業を自分だけでテストしないようにする。当該コードによって自動化される制御システムや資産に詳しく、異なる職務内容や行動指針を持った別の人員に、元のエンジニアの作成した構成設定に対して機能性と完全性のテストを実施させる。これを行うのは、元の構成を作成したプログラマが、制御プログラムの達成する目的に関して偏見を持っていたり視野狭窄に陥っていたりすると、機能や入力値のテストを限られた条件でのみ実施する可能性があるからである。

3.1.2 ユーザの実施責任

制御システムユーザによるリソースへのアクセスについては、制限と適切な管理を適用し、情報資産に損害を与えかねない必要以上の権限が付与されることを防ぐ必要がある。ユーザが特定の制御システムリソースを使用しているときに試みるアクセスの内容については、監視、監査、およびログの記録を適切に行う必要がある。個人の実施責任を特定できるようにするために、監査ログには個人のユーザ ID を含める必要がある。制御システムおよび産業ネットワークリソースを使用し、また、アクションの実行について承認を得るにあたり、ユーザ各員は自分の責任を把握しておくべきである。ユーザ活動の記録とレビューを行わないと、制御システムユーザに必要以上の権限が付与される事態や未承認のアクセスが発生したかどうかを判断することは困難になる。

監査ログや機能ログには、人力で解釈しなくてはならない解読困難な情報が多量に含まれていることが多い。このため、制御システムハードウエアに特有のログを解析して重要な発見内容を報告する製品が提供されている。疑わしい活動や、本来の水準から乖離しつつある産業ネットワーク環境を発見するために、ログに対しては手作業または自動で監視とレビューを実行する。これにより、制御システムセキュリティ管理者はセキュリティインシデントが発生する前に問題の警告を受けることができる。監視の際、制御システムネットワーク管理者は、制御システムのユーザ、ユーザのアクション、ユーザに現在認め

られているアクセスのレベルに関する事項をいくつか質問する必要がある。考えられる質問内容は、たとえば次のようなものである。

ユーザがアクセスする制御データ情報や、実行する制御システム関連作業は、自分の職務にとって不必要なものか。これに対する回答内容は、ユーザの権限やアクセス許可の再評価（場合によっては変更）が必要かどうかを示している。

ユーザのミスが繰り返し発生しているかどうか。これに対する回答内容は、制御システムユーザに対する追加トレーニング、またはシステム機能性の修正が必要かどうかを示していると考えられる。

取り扱いに注意を要する制限付きの制御データやリソースへのアクセス権が、あまりにも多くのユーザに付与されていないか。これに対する回答内容は、制御システムおよび産業ネットワークのデータやリソースに対するアクセス権の再評価が必要かどうか、これらにアクセスする人員の数を減らす必要があるかどうか、また、付与するアクセス権の範囲を変更する必要があるかどうかを示していると考えられる。データへのユーザのアクセス権は、不要になった時点ですみやかに削除すべきである。

3.2 SPOF対策

現代的な制御環境では、制御技術とオープンなネットワーキングおよびコンピューティングサービスとの融合によって、業務処理の迅速化や産業アーキテクチャに対するより精密な制御が実現されていることが多い。しかし、迅速化の要件によって、または経営管理層、提携先機関、あるいは産業技術を提供するベンダに特有の要求によって、こうした活動の中に SPOF（単一障害点）が発生する場合がある。SPOF は、制御ネットワークにとって大きな潜在リスクとなることが多い。1 つの装置に故障が発生しただけで、産業ネットワークの大部分または全体に悪影響が生じる。SPOF になりうる装置としては、ファイアウォール、ルータ、ネットワークアクセスサーバ、T1 回線、スイッチ、ブリッジ、ハブ、各種の制御システムコンピュータ、および認証サーバなどがある。SPOF に対して脆弱性が生じることを防ぐ最良の対策は、適切な保守を行うこと、定期的にバックアップを作成すること、冗長性を確保することである。

ルータの機能が停止した場合に備えて、ルータ間には複数の経路を確保すべきである。また、ネットワークに変更が生じた際にはその情報がすべてのルータに伝達されるよう、動的ルーティングプロトコルを使用すべきである。さらに、UPS（無停電電源）、RAID など、冗長性による耐故障バックアップ手段を導入し、適切に構成しておくべきである。UPS を使用すると、制御ネットワーク上で重要性の高いシステムリソースに良質かつ安定した電力を供給できる。RAID には、ハードディスクの故障対策とシステムのパフォーマンス向上効果がある。データが分割されて複数のディスクに書き込まれるため、要求した情報を読み出す際にはそれらのディスクのヘッドが並列に使用され、冗長化と高速化が実現される。また、制御データは各ディスク上に展開されるため（パリティ）、1 台のディスクが故障してもほかのディスクが連携して動作し続け、重要な制御データや構成データが復元される。

3.2.1 耐故障性とクラスタリング

クラスタリングは IT ネットワークにおいて広く使われている耐故障サーバ技術であり、冗長サーバに似ているが、要求されるサービスの処理に各サーバが関与する点が異なる。サーバクラスタは、ユーザからは論理的には 1 台のサーバとして見えるサーバ群であり、エンタープライズネットワークでの使用と、制御または SCADA LAN での使用に関しては、単一の論理システムとして管理可能である。クラスタリングは可用性とスケーラビリティの確保に役立つ。物理的に異なる複数のシステムをグループ化して論理的に結合することで、障害を防ぎ、パフォーマンスを向上する技術である。

クラスタを構成するシステムのうち 1 台が故障した場合は、ほかのシステムがその分の負荷を引き受け、処理が継続される。この特長は、主系サーバの故障に備えて待機系の制御システムデータ履歴サーバを温存しておく手法よりも魅力的である。クラスタリングでは、すべてのシステムが要求の処理に使用されるため、故障が発生するまで有休状態のまま保持されるシステムはない。

3.2.2 バックアップ

制御システムソフトウエアのバックアップを作成することと、産業ネットワークのバックアップ（予備）ハードウエア装置を用意することは、制御システムおよび産業ネットワークの可用性を確保するための主要な手段である。組織には、さまざまに異なる状況下で（ハードディスク故障、コンピュータリソース障害、物理的災害発生、その他のソフトウエア的な損傷による使用中データの利用不能化など）重要な制御データを復元できる手段が必要である。バックアップの対象とするデータ、バックアップの実行頻度、バックアッププロセスを開始させる事由を定めた包括的なセキュリティポリシー（OPSEC の要素で使用するもの）を策定すべきである。このプラクティスと、これに対応する OPSEC 計画内の具体的要素には、既存の（実績のある）ポリシーや指針を流用してよい。ただし、プラクティスの内容については、ほかのサイバーOPSEC 要素の場合と同じく、制御システム領域の事情や要件に応じて調整するか新たに作成することが必要である。

制御システムユーザが自分のワークステーション上に重要な情報を保存している場合、運用部門は、ユーザワークステーション上にある特定ディレクトリのバックアップ方法、または、シフト交代の前に重要な制御データをサーバ上へ移動してバックアップの対象となるようにする方法を策定する必要がある。バックアップの実行間隔には、制御対象資産の重要度と変化しやすさに応じて、1 週間に 2 回、1 日に 1 回、1 時間に 1 回などといった頻度を設定する。この作業は組織としての裁量によって実行するものである。部門に特有のガイダンスがある場合はその内容を確認することを推奨する。一般論として、バックアップの頻度を高くすれば、それだけバックアッププロセスに必要な時間も増加する。バックアップのコストと、重要な制御データを失う可能性に関する実際のリスクとを比較してバランスを決定することが必要である。サポート要員に余裕がない場合や、セキュリティとデータ復旧管理の機能を完全に外部委託している場合など、組織の実情に応じて検討しなくてはならない課題が多数あるため、ここでもやはり、サイバーOPSEC 手続きの内容は組織に特有のものとなる。

ハードウエア、ソフトウエア、または施設の不具合に起因する損失が発生した後で制御システムの一部または全体を復旧するプロセスには、バックアップの文書化、データ保

管用メディア、バックアップメディアと運用システムとの物理的隔離に関するニーズが本質的に含まれている。システムを損失発生前と同じ状態へと確実に復旧できるように、復元のプロセスと手順については、OPSEC 計画で定義された要件に従ってシステムを復旧するために必要とされる程度に文書化しておくべきである。

3.3 トレーニングと意識向上

サイバーOPSEC 計画は、セキュリティトレーニングとセキュリティ意識向上の活動を行わずに完成することはできない。実効性のある OPSEC 計画を構築する作業の中でも、これは困難な部分と見なされることが多い。しかし、文化のためにもプログラムの自己継続的な性質を実現するためにも、ユーザやオペレータへの効果的な普及促進プログラムを作成し、維持することは極めて重要である。ユーザとオペレータでは、旧来の物理的セキュリティと新しいサイバーセキュリティの問題に対する姿勢が異なる。この違いを超えやすくするために、制御システム領域におけるサイバーセキュリティトレーニングでは重点となる項目を明確にする必要がある。これは当初こそ取り組みにくい作業のように見えるが、部門に特化した実績あるトレーニング方法を利用すれば、堅牢、正確かつタイムリーな普及促進コンテンツを作成できる。

トレーニングコンテンツは標準的なフレームワークを使用して作成できるが、ベストプラクティスによると、通常は対象者が一切の情報リソースにアクセスする前にトレーニングを実施する必要がある。現在では、多くのオペレータやユーザが情報領域へのアクセス手段を持っている。このため制御システムのトレーニングは、サイバーセキュリティ要素も含め、既存の運用やプラクティスに合わせた内容で実施する必要がある。ユーザとオペレータを対象としたサイバーセキュリティトレーニングは、次の点に留意して行うべきである。

- 上層部の決定として履修を義務付ける
- 雇用の条件とする。また、割り当てられる一切のシステムにアクセスする前に履修することを必須要件とする
- 内容更新と実施を少なくとも年に 1 回は行う。OPSEC 計画の規定に該当する新たな人員すべてにサイバーセキュリティトレーニングを受けさせる
- 対象を従業員に限定せず、提携先のユーザや契約社員など、職務を遂行する際に制御システム情報リソースにアクセスするすべての人員に提供する
- 内部にセキュリティ作業部会を組織して、ニュースレター、同報電子メール、メモなどを通じて普及を促進し、内容を充実しながら継続する
- サイバーOPSEC 計画に関連する次の内容を盛り込む（これに限定する必要はない）
    - サイバーセキュリティポリシー（業務および制御システムに特化した内容をともに含む）
    - 物理的セキュリティの見直し

- アクセス制御、管理作業、運用上の安全策
- セキュリティとシステム調達（調達を可能にし、設計フェーズにフィードバックする）
- インシデントの報告、対応、運用継続性計画
- データ保護、データ保管、データ取り扱いの安全性

多くの場合、組織のセキュリティ要員は限られており、サイバーセキュリティトレーニングプログラムの作成、管理、実施に充てられるリソースにも限りがあることはわかっている。このため、制御システム領域の運用を担う組織では、特定システムのトレーニングは実施するがサイバーセキュリティのトレーニングはサードパーティに委託するのが一般的である。これに該当するとしても、組織のトレーニングコンテンツは、運用の具体的な詳細と（該当する場合）システムに特化したセキュリティの両方に適用可能かつ整合した内容であることが望ましい。適切な水準のコンテンツを適切な方法で提供するのが最良のトレーニングであるから（対象がオペレータの場合と管理者の場合では適したコンテンツが異なる）、オペレータのためのサイバーセキュリティトレーニングを外部委託する場合は、提供トレーニング内容に関する参考情報を事前に収集することを推奨する。

トレーニングコンテンツには次の事項が含まれている必要がある。

- 制御システム環境におけるコンピュータ、通信、ネットワークの基本的な背景知識
- 制御システムのサイバーセキュリティリスクに関する基礎（適切な例を含む）
- 運用時に全体的なサイバーセキュリティ水準を低下させる可能性がある、脅威、一般的な脆弱性、アーキテクチャ不備についての簡潔な説明
- 制御システムで使用できる現代的な IT セキュリティ技術およびプラクティス（および適正な配備のための方法論）に関するトレーニング
- 業界に特化したサイバーセキュリティガイドラインと、組織に特化したガイドライン
- ベンダに特化したセキュリティガイドラインに関するトレーニング
- 制御システムのサイバーセキュリティ技術、問題緩和活動、ベストプラクティスの取り扱いを詳細に体験できる実践トレーニング

4. 結論

サイバーセキュリティは一種のプロセスとして定義されることが多い。重要なのは、企業システムおよび制御システムの管理者がサイバーセキュリティ文化の形成に向けたプロセスに着手する必要があるという点である。この文化の確立と維持に必要な問題意識を高める上で、OPSEC プログラムを策定することは非常によい契機となる。

業務の根幹が制御システムに関係している組織では、以前から、物理的なセキュリティについては非常に周到な対策が行われてきた。近年では、隔離されていたシステム間の相互接続や業務ネットワークとの接続が進行したことで融合の問題が生じ、システムおよび関連する情報リソースをサイバー攻撃から保護する能力が新たに要求されている。堅牢な運用セキュリティ（OPSEC）計画は、堅牢なサイバーセキュリティプログラムを策定する上で重要な役割を担う可能性がある。このプログラムは、サイバー攻撃の脅威に立ち向かい、脅威を緩和し、組織への全体的なリスクを低減して、サイバーセキュリティ体制を強化するために使用できる。サイバーOPSEC 計画を作成し、組織に特有の内容や情報を選択的に盛り込むことで、運用手順、システムライフサイクル、およびユーザの全体的な知識の強化を図ることができる。この計画を実施することで、制御システム領域におけるサイバーセキュリティの重要性に関する理解が促され、情報および運用リソースの保護を持続できるサイバーセキュリティ文化が形成される。

5. 参考文献

DHS Control Systems Security Program http://www.us-cert.gov/control_systems/, October 2006

Instrumentation, Systems, and Automation Society http://www.isa.org/community/SP99, November 2006

National Association of Regulatory Utility Commissioners http://www.naruc.org/, November 2006

North American Electric Reliability Council (NERC) http://www.nerc.com/, November 2006

Electric Power Research Institute http://www.epri.com/, November 2006

AGA-12: Cryptographic Protection of SCADA Communications General Recommendations http://www.aga.org/NR/rdonlyres/B797B50B-616B-46A4-9E0F-5DC877563A0F/0/0603AGAREPORT12.PDF, March 2006

Sandia National Labs Center for SCADA Security
http://www.sandia.gov/scada/history.htm, November 2006

21 Steps to Improve Cyber Security of SCADA Networks http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf, January 2007

Common Vulnerabilities in Critical Infrastructure Control Systems http://www.oe.netl.doe.gov/docs/prepare/vulnerabilities.pdf, January 2007

Process Control Systems Forum (PCSF) http://www.us-cert.gov/control_systems/icsjwg/index.html

TSWG SCADA Security Website http://www.tswg.gov/, November 2006
NIST PCSRF http://www.isd.mel.nist.gov/projects/processcontrol/, November 2006

Infragard http://www.infragard.net/, November 2006

Information System Security Association http://www.issa.org/, November 2006

Partnership for Critical Infrastructure Security http://www.pcis.org/, November 2006

Information Systems Audit and Control Association http://www.isaca.org/, November 2006

Presidential Directive on Critical Infrastructure: Identification, Prioritization, and Protection - HSPD-7 http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm, November 2006

Executive Order 13231: Critical Infrastructure Protection http://www.fas.org/irp/offdocs/eo/eo-13231.htm, November 2006

Presidential Decision Directive 63: Critical Infrastructure Protection http://www.fas.org/irp/offdocs/pdd-63.htm, November 2006

The National Strategy to Secure Cyberspace
http://www.dhs.gov/files/publications/editorial_0329.shtm, November 2006

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets http://www.dhs.gov/files/publications/publication_0017.shtm, November 2006