A2／AD 環境下における サイバー空間の攻撃及び防御技術の動向 ③

木村　初夫

株式会社 NTT データ　公共システム事業本部
第一公共システム事業部　第三システム統括部　嘱託

5．サイバー空間の防御技術の動向

5.1　現状のサイバー攻撃対処プロセス

第 2 章において、「A2／AD 環境下におけるサイバー空間の脅威」としては、APT 攻撃、インサイダー攻撃、サプライチェーン攻撃、ネットワークアクセス阻止攻撃及び制御システムの脆弱性攻撃に集約・整理されることを示した。これらの脅威に対する現状のサイバー攻撃対処プロセスとしては、CJCSM 6510.01B、NIST SP 800-83 Rev.1 及び ISO／IEC 27035：2011 のインシデント対処プロセス標準に基づき、図 5.1-1に示す防護（予防）、検知・分析、対応、復旧及びインシデント後処理のライフサイクルがある。これらの対処プロセスでは、サイバー脅威のリアルタイムな状況認識に基づくインシデント対応が中心であり、資産の脆弱性及びセキュリティ管理策の脆弱性の状況認識については、静的な定期的情報セキュリティ監査に基づいており適時性に欠けるという問題がある。

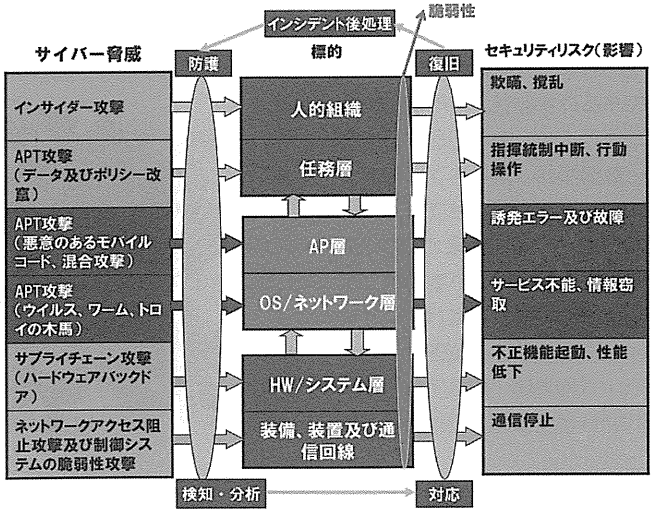

図5.1-1　現状のサイバー攻撃対処プロセス

5.2　情報セキュリティリスク管理に基づくサイバー攻撃対処プロセス

APT 攻撃出現前の従来の防御方式では、防護及び外部センサによるサイバー脅威の検知中心の縦深防御対策並びに静的な定期的情報セキュリティ監査による資産及びセキュリティ管理策の脆弱性検知が行われてきた。しかし、ゼロデイ及び未パッチの脆弱性並びにセキュリティ管理策の脆弱性を狙ったネットワーク速度の APT 攻撃に対しては、そのような脆弱性検知速度では実効性がないため完全に防御することは不可能である。また、APT 攻撃の場合、サイバー脅威が使用する資産の脆弱性及びセキュリティ管理策の脆弱性が情報システムに存在しなければ、情報セキュリティリスクは生起しない。このような資産の脆弱性及びセキュリティ管理策の脆弱性を狙ったサイバー脅威の概念を図5.2-1に示す。

APT 攻撃のようなサイバー脅威に対応するためには、「ISO／IEC 27005：2011情報セキュリティリスク管理」に基づき、サイバー脅威並びに資産の脆弱性及びセキュリティ管理策の脆弱性を継続的に監視しリスクアセスメント（リスク特定、リスク分析及びリスク評価）を行い情報セキュリティリスクに対応する「情報セキュリティリスク管理プロセス」を適用した新たなサイバー攻撃対処プロセスの導入が必要である。この情報セキュリティリスク管理プロセスは、動的なリスクに対応するための「ISO 31000：2009リスク管理」で規定されたリスク管理プロセスに準拠したものであり、図5.2-2に示すとおりである[1]。また、情報セキュリティリスクは、リスク要因である資産、脅威及び脆弱性から次式のように表現できる。

情報セキュリティリスク＝f（資産価値、脅威の起こりやすさ、資産の脆弱性、セキュリティ管理策の脆弱性）

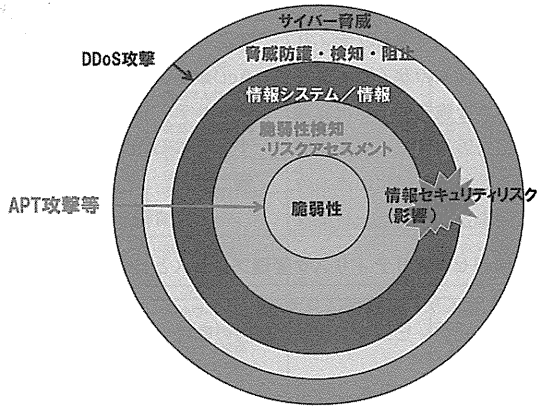

図5.2-1　脆弱性を狙ったサイバー脅威の概念

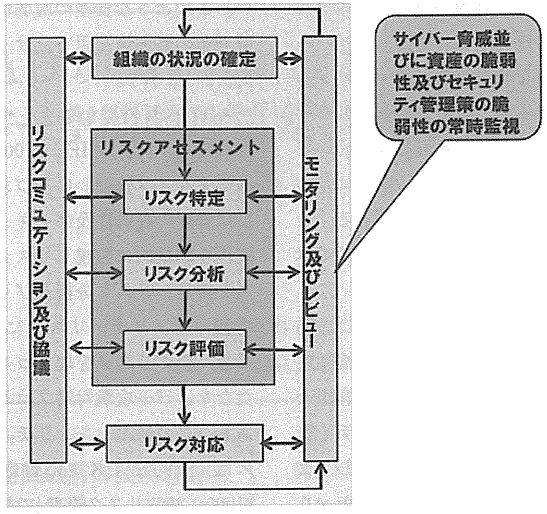

図5.2-2　情報セキュリティリスク管理プロセス
出典：ISO／IEC 27005：2011、ISO、2011

さらに、任務及び業務レベルリスクは、任務／業務、資産価値及び情報セキュリティリスクから次式のように表現できる。このためには、任務／業務と資産価値の関係定義が必要である。

任務及び業務レベルリスク＝f（任務／業務、資産価値、情報セキュリティリスク）

動的なサイバー脅威であるAPT攻撃のようなサイバー攻撃対処には、情報セキュリティリスク管理を実現するための従来のサイバー脅威の状況認識にリアルタイムな脆弱性の状況認識を加えたセキュリティ常時監視能力の整備並びに情報セキュリティリスク対応及び復旧能力の向上が必要である。このようなサイバー脅威及び脆弱性の状況認識によって任務及び業務レベルのリスクをリアルタイムに評価し、意思決定者を支援することができる。これは、国防総省が推進している能動サイバー防衛（Active Cyber Defense）と同様なサイバー防御概念である。また、このようなネットワーク速度のサイバー空間の防御にも、動的な指揮統制モデルであるOODA（Observe, Orient, Decide and Act）サイクルが適用できる。すなわち、情報セキュリティリスク管理プロセスは、表5.2-1に示すようにOODAサイクルに対応するものと理解できる。

一方、情報セキュリティリスク管理プロセス

表5.2-1　情報セキュリティリスク管理プロセスとOODAサイクルの対応

【情報セキュリティリスク管理プロセス】	【OODAサイクル】
・モニタリング及びレビュー：リスク要因の監視	・Observe（監視）
・組織の状況の確定	・Orient（状況認識）
・リスクアセスメント：リスク特定・分析・評価	・Decide（意思決定）
・リスク対応：リスク修正・保有・回避・共有	・Act（対応）

のモニタリングに相当するセキュリティ常時監視については、「NIST SP 800-137情報セキュリティ常時監視（2011年9月）」によって「組織的なリスク管理意思決定をサポートするために情報セキュリティ、脆弱性及び脅威の継続的な状況認識を維持すること」と定義されている[2)]。

5.3　サイバー防御技術の現状及び将来

サイバー防御技術については、表5.3-1に示すとおり現状のサイバー攻撃対処プロセス及びサイバー脅威別に既存技術、開発中及び統合化技術、革新技術について識別・整理している。

既存技術は、防護、外部センサによる検知及び状況認識を中心に開発・整備されてきたが、現在の最大のサイバー脅威であるAPT攻撃を完全に防御することはできない。APT攻撃に実効性のある対応をするためには、既存のサイバー脅威の状況認識に加えて、従来、定期的な情報セキュリティ監査により行われていた脆弱性の把握をセキュリティ常時監視によりリアルタイムな脆弱性の状況認識に変える必要がある。このためにはセキュリティ自動化技術の導入により脆弱性管理、パッチ管理、構成管理、資産管理等を統合化する必要がある。また、任務レベル及び業務レベルのサイバー空間の状況認識のためのリスク評価については、新たな開発が必要である。制御システムの防御についても、APT攻撃に実効性のある対応をするためにセキュリティ常時監視が必要である。

さらに、APT攻撃及びサプライチェーン攻撃の防護能力の向上のために革新技術としての移動目標、テーラー化信頼空間及び集積回路安全化の研究開発並びにサプライチェーンリスク管理の標準化が行われている。また、インシデントの迅速な対応及び復旧能力の向上のためにインシデント対応自動化及びサイバーセキュリティ情報交換の標準化並びにサイバー耐性の向上がある。

次節以降では、今後の主要なサイバー防御技術として、セキュリティ常時監視、防護能力向上、サイバー耐性向上、サイバーセキュリティ情報交換の標準化及び制御システムの防御について述べる。

表5.3-1　サイバー攻撃対処プロセス別防御技術の現状及び将来

脅威	防護	検知・分析	対応	復旧	インシデント後処理
インサイダー攻撃	**・特権アクセス管理**	インサイダー監視	・インシデント対応自動化	・サイバー耐性向上	**・知識管理**
APT攻撃	**・ファイアウォール（ACL）** **・ネットワーク型IPS** **・プロキシフィルタ** **・識別・認証（パスワード強化）** **・暗号化** ・パッチ管理（※） **・移動目標** **・テーラー化信頼空間** ・サイバー耐性向上	**・ネットワーク型IDS** **・ホスト型IDS** **・Web分析** **・既知マルウェア検知** ・未知マルウェア検知 **・脅威の状況認識** ・脆弱性管理（※） ・構成管理（※） ・資産管理（※） ・サイバー耐性向上	・インシデント対応自動化 ・サイバーセキュリティ情報交換の標準化	・サイバー耐性向上	**・知識管理** ・サイバーセキュリティ情報交換の標準化
サプライチェーン攻撃	**・集積回路安全化** ・セキュアブート ・SCRMの標準化	・SCRMの標準化		・サイバー耐性向上	**・知識管理**
ネットワーク阻止攻撃及び制御システムの脆弱性攻撃	**・耐EMP/HEMP** **・対TEMPEST** **・冗長化** ・制御システムのパッチ管理 ・サイバー耐性向上	**・ネットワーク管理** ・制御システムのセキュリティ常時監視 ・サイバー耐性向上	・インシデント対応自動化	・サイバー耐性向上	**・知識管理**

現状の防護技術及び外部センサ検知技術よる脅威（後）の状況認識だけでは、APT攻撃を完全に防御できないため、情報セキュリティリスク発生時の円滑な対応を行うために脆弱性（後）の状況認識を加えたセキュリティ常時監視能力の整備が必要である。（サイバー空間における孫子の兵法）

凡例：既存技術：黒字、開発中及び統合化技術：青字、革新技術：赤字

5.4 セキュリティ常時監視

(1) 米国におけるセキュリティ常時監視

米国連邦政府の情報セキュリティは、2001年9月11日の同時多発テロ以降、連邦情報セキュリティ管理法（Federal Information Security Management Act：FISMA）が制定され、各省庁は年に一度、情報セキュリティを見直し、行政管理予算局（OMB）にセキュリティ報告書を提出することが義務付けられた。また、連邦情報システムの運用認可のための国立標準技術研究所（NIST）のセキュリティ標準に基づくセキュリティ評価認証（C&A）制度が整備され、大量の紙ベースのセキュリティ評価認証が3年毎に実施されてきた。

OMBは、2009年FISMA議会報告書において、「過去15年間に亘る国家サイバーセキュリティ対策は、増大するサイバー脅威に対応できなかった。」と述べている[3]。APT攻撃が出現する前のセキュリティ管理策の技術対策としては、新しいサイバー攻撃技術の出現とともに縦深防御戦略に基づく防護能力及び検知能力の向上が行われたが、ソフトウェアの脆弱性をゼロにすることは不可能であるため、それら対策は対処療法であり実効性の高いものではなかった。

OMBは、ゼロデイ脆弱性を含むAPT攻撃の完全防御は不可能であるとの認識に基づき、連邦政府情報システムへのサイバー攻撃に対する危機管理を円滑に実施できるように継続的な情報システムのセキュリティ健全性の状況認識の可視化、すなわち常時監視（Continuous Monitoring）を行うために、2010年4月にFISMAに関する新たなガイドライン（M-10-15）を公表した。これにより、これまで各連邦政府機関で静的及び紙ベースで行われていたFISMAの準拠状況の年次報告は、国土安全保障省（DHS）が整備した常時監視自動化ツールであるCyberScopeを用いて同年10月以降オンラインで行われることになった[4]。2012年6月のDHSの報告によると、成功事例である国務省（DoS）事例におけるサーバ及びパーソナルコンピュータのリスクは、このセキュリティ常時監視の導入により12ヶ月で89%減少している。また、重要度の高い平均パッチ実施率は、1週間で84%及び1ヶ月で93%になっている。技術的なセキュリティ管理策のデータ有効性は、3年毎ではなく2～15日毎になるとともに、セキュリティ評価認証コストも56～62%削減している[5]。

DHSは、2012年6月に次期セキュリティ常時監視である常時診断緩和（Continuous Diagnostic and Mitigation：CDM）及び調達コスト削減及び高度セキュリティ人材不足の解決のためのクラウドサービスによるCMaaS（Continuous Monitoring as a Service）の計画を発表している。CDMは、既存常時監視能力の向上及び自動化、セキュリティ関連情報の相関・分析、及びリスクベース意思決定の高度化を目的として、次に示す15ツール及び11サービスを提供する[6]。

① ツール
- ハードウェア資産管理
- ソフトウェア資産管理
- 構成管理
- 脆弱性管理
- ネットワークアクセス制御管理
- アクセスの保証された利用者の信頼管理
- セキュリティ関連行動管理
- 資格認定及び認証の管理
- アカウントアクセス管理
- 緊急事態及びインシデントのための準備
- 要求ポリシーの設計及び構築並びに計画策定
- 品質の設計及び構築
- 監査情報管理
- 運用セキュリティ管理

② サービス
- タスク指示管理サポート
- CDM指示計画立案
- CDMダッシュボードサポート
- ツール及びセンサの設備仕様化
- ツール及びセンサの構成及びカスタマイズ化
- CDMツール及びセンサのデータ及び所要状態の維持
- CDMツール及びセンサの運用
- CDMツールと省庁レガシーアプリケーション／データとの間の相互運用性の統合及び維持
- インストールされたダッシュボードとのデータ供給の運用
- CDM統制における訓練及びコンサルティング
- 独立検査及び妥当性検証（IV&V）及びシステム運用認可サポート

一方、国防総省は、2011年1月に国防権限法（NDAA：H.R.6523）の制定によりDoD情報システムへのセキュリティ常時監視の導入を義務付けた[7]。

(2) セキュリティ常時監視及びセキュリティ自動化の標準化

ア セキュリティ評価認証制度の統合化

従来、米国においては、情報システムの運用認可判断を行うためのセキュリティ評価認証制度は、情報コミュニティ（IC：Intelligence Community）、国防総省（DoD）及び連邦政府（民間部門）別に評価認証プロセス及び情報保証管理策／セキュリティ管理策が策定及び運用されてきた。国家安全保障システムに対するサイバー攻撃脅威の現実化に対応するために、国家情報局（ODNI）、DoD、NIST及びOMBが参加する情報保証評価認証変革コミュニティフォーラムが2006年6月に発足し、共通標準及び用語の欠如、相互主義の欠如、文書過多及び評価認証プロセスが長すぎるとの共通課題認識に基づき、2007年1月にポリシーベースの大量文書に基づく情報保証からセキュリティリスク管理ベースの情報保証への変革のための「7つの情報保証評価認証変革目標」を発表した[8]。

① 相互主義のための共通信頼レベルの定義（CNSSI 1191）
② 他組織の情報システムの再利用のための相互主義の適用（CNSSI 1260）
③ 共通セキュリティ管理策の定義（NIST SP 800-53、CNSSI 1253）
④ 共通用語の定義（CNSSI 4009）
⑤ エンタープライズリスク管理の実装（NIST SP 800-37）
⑥ IC及びDoDにわたるエンタープライズ運用環境内での設計及び運用
⑦ IC及びDoDの共通評価認証プロセスの制定

これらの変革目標に基づき、IC及びDoDの国家安全保障システムのセキュリティ評価認証制度は、図5.4-1に示すNISTの統合情報セキュリティフレームワーク（Unified Information Security Framework）をベースに変革が進んでいる。その基盤となる情報セキュリティ共通標準を次に示す[9]。

① NIST SP 800-39 情報セキュリティリスク管理
② NIST SP 800-30 リスクアセスメント実施指針
③ NIST SP 800-37 リスク管理フレームワーク

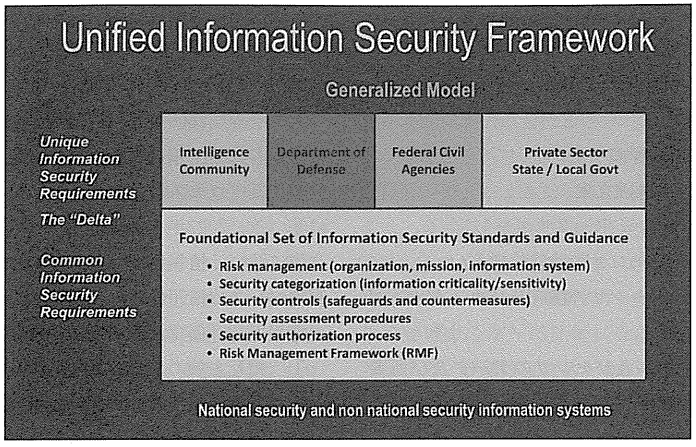

図5.4-1　統合情報セキュリティフレームワーク

出典：Mapping Supply Chain Risk Using NIST Standards and Guidelines, Dr. Ron Ross, NIST, Oct. 15, 2012

④　NIST SP 800-53　セキュリティ管理策

⑤　NIST SP 800-53A　セキュリティ管理策評価指針

ODNIは、情報コミュニティ指示ICD503を2008年9月15日に交付し、7つの変革目標の実現、DCID 6／3（Director of Central Intelligence Directive 6／3-Protecting Sensitive Compartmented Information Within Information Systems）及びDCID 6／3マニュアルの廃止並びにICD503への置換、DCID 6／5実装マニュアルの廃止、及びDCID 6／3マニュアル付録E（インテリジェンス情報システムへの外国政府によるアクセス）の継続適用の基本的考え方に基づき、情報保証評価認証プロセス及び情報保証管理策をそれぞれCNSSP　22及びCNSSI 1253に移行している[10]。

一方、DoDは、現在の情報保証評価認証プロセスであるDIACAP（DOD Information Assurance Certification and Accreditation Process）及び情報保証管理策をそれぞれNIST SP 800-37 Rev. 1（2010年2月）／CNSSP 22（2009年2月）及びNIST SP 800-53 Rev. 4（2013年4月）／CNSSI 1253 Rev.に移行するために、NISTのリスク管理、セキュリティ管理策及びセキュリティ常時監視を反映したDoDD 8500.1及びDoDI 8500.2の改訂並びにNISTのリスク管理フレームワーク、リスクアセスメント、セキュリティ管理策評価指針及びセキュリティ常時監視を反映したリスク管理フレームワーク実装指針としてのDoDI 8510.01の再策定が2013年第2四半期目途に進められている。NIST SP 800-53 Rev. 4における主要変更点は、APT、サプライチェーンリスク、インサイダー脅威、アプリケーションセキュリティ、モバイルセキュリティ、クラウドセキュリティ等に対応する新しいセキュリティ管理策の追加及び向上である。DoDのセキュリティ評価認証制度の統合化状況を図5.4-2に示す[11]。

イ　セキュリティ常時監視及びセキュリティ自動化の標準化

セキュリティ常時監視については、「NIST SP　800-39　情報セキュリティリスク管理

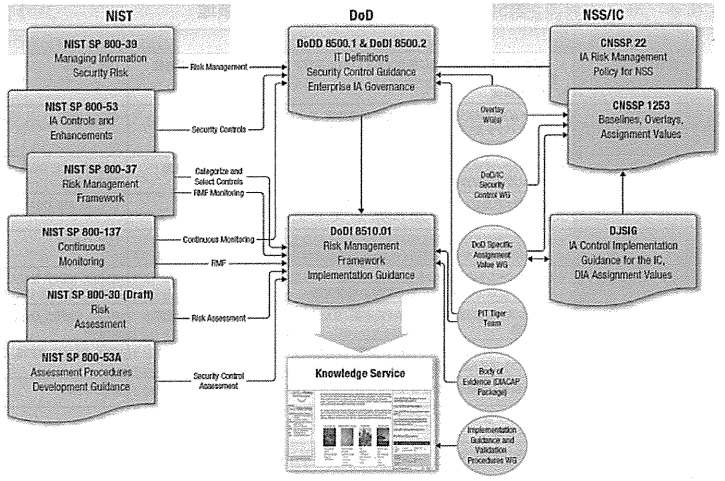

図5.4-2　DoDのセキュリティ評価認証制度の統合化状況

出典：Cyber 101, Dominic Cussatt, DoD, AFCEA West 2013, Jan. 29, 2013

（2011年3月）」において、3つの主要な情報セキュリティ常時監視（ISCM）活動として、有効性の監視、システム及び運用環境に対する変更の監視、及びコンプライアンスの監視を挙げている[12]。「NIST SP 800-37　リスク管理フレームワーク」では、リスク管理フレームワーク（RMF）に基づく監視プロセスにおけるシステムレベルでのセキュリティ管理策の監視を記述している[13]。「NIST SP 800-137　情報セキュリティ常時監視（2011年9月）」は、NIST SP 800-39及びNIST SP 800-37において要求されるリスク管理フレームワーク（RMF）の監視プロセスの常時監視要件の実現のためにセキュリティ常時監視の定義、オンラインシステム運用認可、ライフサイクル等を標準化している[14]。当面のセキュリティ常時監視領域は、脆弱性の状況認識のための脆弱性管理、パッチ管理、構成管理及び資産管理の4つの領域であり、その自動化をSCAP（Security Content Automation Protocol）V1.2がサポートしている。さらに、サイバー脅威の状況認識のためのイベント管理、インシデント管理、マルウェア検知等への適用領域拡大に向けて新しいセキュリティ自動化標準が開発されている。

また、セキュリティ常時監視アーキテクチャについては、DHSの連邦ネットワークセキュリティCAESARS（Continuous Asset Evaluation, Situational Awareness, and Risk Scoring）フレームワークを拡張したエンタープライズ常時監視参照アーキテクチャ、常時監視参照モデル技術仕様、常時監視技術参照モデル適用を標準化している。これらは、常時監視の調達及び実装指針の青写真の提供、常時監視の機能分解、相互運用性の推進等をねらいとしたものである。さらに、構成管理については、NISTセキュリティ管理策の構成管理要件を満足する「NIST SP 800-128　セキュリティ構成管理指針（2011年8月）」を標準化している[15]。セキュリティ常時監視のあるべき姿の例としてのエンタープライズ常時監視参照アーキテクチャを図

表5.4-1　セキュリティ常時監視領域

区分	常時監視領域	概　要	セキュリティ自動化標準
現行SCAP適用領域（SCAP V1.2）	脆弱性管理	・ホスト及びネットワーク上に使用されているOS及びアプリケーションの既知脆弱性識別 ・脆弱性評価	CVE, CVSS
	パッチ管理	・システム及びシステム構成要素の脆弱性走査 ・必要なパッチ及び影響のあるデバイスのソフトウェア更新に関する情報提供 ・パッチ実施プロセスの意思決定支援	CVSS, OVAL
	構成管理	・セキュリティ設定の構成、設定変更の監視、設定状態の収集、及び設定の復元 ・セキュリティ設定評価	XCCDF, CCE, OVAL, OCIL,CCSS
	資産管理	・ソフトウェア及びハードウェア資産の登録簿の維持管理	CPE, AI, ARF,OVAL
SCAP適用領域拡大	イベント管理	・ネットワークまたはシステム内の可観測事象の監視及び必要に応じた対応 ・既知攻撃シグネチャに基づくイベント検知及び攻撃を示す行動に基づく異常検知	CEE, CybOX
	インシデント管理	・複数のイベントによるインシデント発生通知 ・サイバー攻撃の検知、対応及び影響の極限支援	CYBEX, IODEF, MAEC, CAPEC, CybOX, CVE, CWE
	マルウェア検知	・標的システム上のウイルス、トロイの木馬、またはその他不正コードの存在の識別及び報告	MAEC, CAPEC, OVAL , CybOX
	ソフトウェア保証	・ソフトウェアのプロセス及び製品の要求、標準及び手順への適合性を保証する計画的かつシステム的活動	CWE, CAPEC, CWSS, CWRAF
	ネットワーク管理	・ホスト検知、登録簿、変更管理、性能監視及び他のネットワーク機器管理	CVE, OVAL
	ライセンス管理	・ソフトウェア資産のライセンスコンプライアンスの追跡、使用状態の監視及びライフサイクル管理	
	情報管理	・組織内の情報のセキュリティ確保のためにその場所と転送の管理	

出典：NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, NIST, Sept. 2011

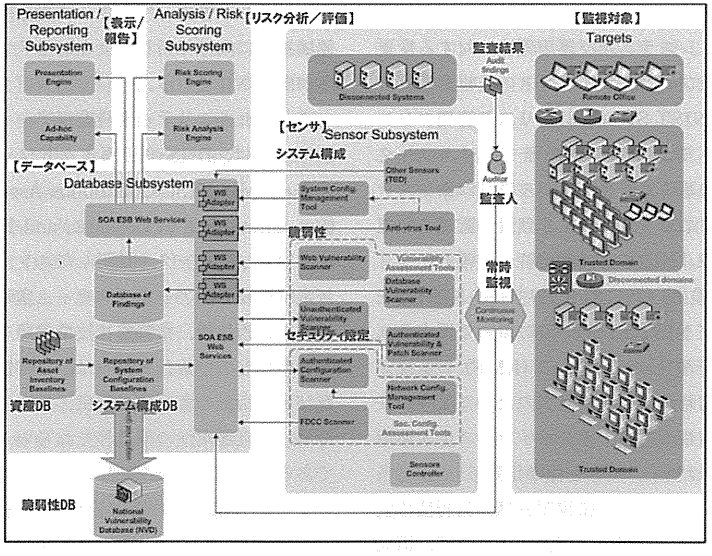

図5.4-3　セキュリティ常時監視システムのあるべき姿の例：エンタープライズ常時監視参照アーキテクチャ

出典：CAESARS Framework Extension: An Enterprise Continuous Monitoring Reference Model (Second Draft), NIST IR 7756, Jan. 2012

5.4-3に示す[16]。

あるべき姿としてのセキュリティ常時監視システムは、センサ、データベース、リスク分析／評価及び表示／報告サブシステムから構成される。センサは、ソフトウェア、Web及びデータベースに関する脆弱性センサ、セキュリティ設定に関するセンサ及びシステム構成に関するセンサから構成される。データベースは、資産、システム構成及び脆弱性並びに常時監視による監視データに関するデータベースから構成され

表5.4-2　セキュリティ常時監視の標準化状況

標準番号	概要	発行年月
NIST SP 800-137	情報セキュリティ常時監視	2011.09
NIST SP 800-30 Rev.1	リスク評価実施指針	2012.09
NIST SP 800-37 Rev.1	リスク管理フレームワーク(RMF)適用指針	2010.02
NIST SP 800-39	情報セキュリティリスク管理	2011.03
NIST SP 800-40 Rev.3	パッチ管理技術指針(案)	2012.09
NIST SP 800-41 Rev.1	FW及びFWポリシー指針	2009.09
NIST SP 800-53 Rev.4	セキュリティ管理策	2013.04
NIST SP 800-53A Rev.1	セキュリティ管理策評価指針	2010.06
NIST SP 800-61 Rev.2	セキュリティインシデント処理指針	2012.08
NIST SP 800-70 Rev.2	セキュリティチェックリスト指針	2011.02
NIST SP 800-82	制御システムセキュリティ指針	2011.06
NIST SP 800-83 Rev.1	マルウェアインシデント防止・処理指針	2013.07
NIST SP 800-86	フォレンジック技術のレスポンス対応統合指針	2006.08
NIST SP 800-94 Rev.1	IPDS指針(案)	2012.07
NIST SP 800-128	セキュリティ構成管理指針	2011.08
NIST IR 7756	CAESARSフレームワーク拡張参照モデル(案)	2012.01
NIST IR 7799	常時監視参照モデル技術使仕様(案)	2012.01
NIST IR 7800	常時監視技術参照モデル適用(案) (資産、構成及び脆弱性管理領域)	2012.01

表5.4-3　セキュリティ自動化の標準化状況

標準番号	概要	発行年月
NIST SP 800-126 Rev.2	SCAP V1.2仕様	2011.09
NIST SP 800-117 Rev.1	SCAP V1.2適用指針	2012.01
NIST IR 7511 Rev.3	SCAP V1.2試験要件(案)	2013.01
NIST IR 7275 Rev.4	XCCDF仕様	2011.09
NIST IR 7669	OVAL試験要件(案)	2010.03
NIST IR 7692	OCIL V2.0仕様	2011.04
NIST SP 800-51 Rev.1	CVE/CCE使用指針	2011.02
NIST IR 7695	CPE:命名V2.3	2011.08
NIST IR 7696	CPE:命名整合V2.3	2011.08
NIST IR 7697	CPE:辞書V2.3	2011.08
NIST IR 7698	CPE:適用言語V2.3	2011.08
NIST IR 7435	CVSS及びその適用	2007.08
NIST IR 7502	CCSS	2010.12
NIST IR 7693	AI 1.1仕様	2011.06
NIST IR 7694	ARF 1.1仕様	2011.06
NIST IR 7848	ASR 1.0仕様(案)	2012.05
NIST IR 7802	TASAD V1.0	2011.09
NIST IR 7831	CRE V1.0	2011.12
NIST IR 7864	CMSS	2012.07

る。リスク分析／評価では、監視データに基づき任務及び業務レベルのリスク分析／評価を行う。

また、セキュリティ常時監視の標準化状況を表5.4-2に示す。

セキュリティ常時監視の基盤となるセキュリティ自動化については、現在、SCAP V1.2を標準化している。セキュリティ自動化の標準化状況を表5.4-3に示す。また、SCAP V1.2の概要を表5.4-4に示す[17]。セキュリティ自動化標準技術の実装を図5.4-4に示す[18]。

表5.4-4　SCAP V1.2の概要

区分	項目	概要	維持管理組織
言語	eXtensible Checklist Configuration Description Format (XCCDF) 1.2 セキュリティ設定チェックリスト記述形式	セキュリティ設定チェックリスト仕様言語	NSA及びNIST
	Open Vulnerability and Assessment Language (OVAL) 5.10 セキュリティ検査言語	セキュリティ設定チェックリスト用試験手順仕様言語	MITRE社
	Open Checklist Interactive Language (OCIL) 2.0 チェックリスト会話言語	会話型セキュリテチェック表現言語	MITRE社
一覧	Common Vulnerabilities and Exposures (CVE) 共通脆弱性識別子	ソフトウェア関連欠陥の命名法及び辞書	MITRE社
	Common Configuration Enumeration (CCE) 5 共通セキュリティ設定一覧	システムセキュリティ問題の命名法及び辞書	MITRE社
	Common Platform Enumeration (CPE) 2.3 共通プラットフォーム一覧	製品名及びバージョンの命名法及び辞書	MITRE社
測定及び評価システム	Common Vulnerability Scoring System (CVSS) 2.0 共通脆弱性評価システム	ソフトウェア欠陥脆弱性相対重要度の測定仕様	FIRST
	Common Configuration Scoring System (CCSS) 1.0 共通セキュリティ設定評価システム	ソフトウェアセキュリティ設定問題重要度の測定仕様	NIST
報告形式	Asset Reporting Format (ARF) 1.1 資産報告形式	資産及び資産間関係に関する情報並びに報告の伝達表現データモデル	NIST
	Asset Identification 1.1 資産識別子	既知識別子及び／または資産情報に基づく一意識別	MITRE社及びNIST
完全性	Trust Model for Security Automation Data (TMSAD) 1.0 セキュリティ自動化データ用信頼モデル	SCAP完全性仕様	NIST

注. 青字はSCAP 1.1からの変更及び追加部分である。

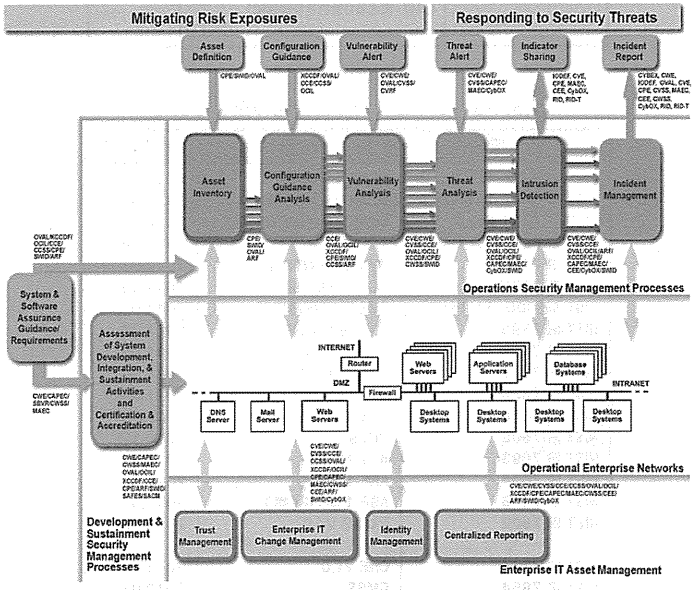

図5.4-4　セキュリティ自動化標準技術の実装

出典：http://makingsecuritymeasurable.mitre.org/about/index.html#config

ウ　米国のセキュリティ設定基準

米国においては、セキュリティ常時監視を実現するために組織及び情報システムのセキュリティ管理策に基づき、連邦政府及びDoDのセキュリティ設定基準であるFDCC（Federal Desktop Core Configuration）／USGCB（United State Government Configuration Baseline）及びSTIG（Security Technical Implementation Guide）が表5.4-5に示すとおり策定されてきた。また、DoDのセキュリティ設定基準であるSTIGのコンテンツ作成イメージを図5.4-5に示す[19]。

(3)　国内のセキュリティ常時監視の課題

国内の政府機関の情報システムのセキュリティ常時監視については、平成25年6月27日に

表5.4-5　米国のセキュリティ設定基準

区　分	セキュリティ設定基準	概　要	備　考
連邦政府	FDCC	米国連邦政府のOMB主導のデスクトップセキュリティ基準 FDCC Major Version 1.2：Windows XP, Windows Vista, XP Firewall, Vista Firewall, Internet Explorer 7.0 Security Check lists	
	USGCB	米国連邦政府のCIO評議会主導のFDCCを発展させたセキュリティ設定基準 USGCB: Windows 7 and Internet Explorer 8, Mac OS X, Red Hat Enterprise Linux	
国防総省	STIG	米国国防総省の定めるセキュリティ設定基準 STIG: OS, AP, CDS, Network	

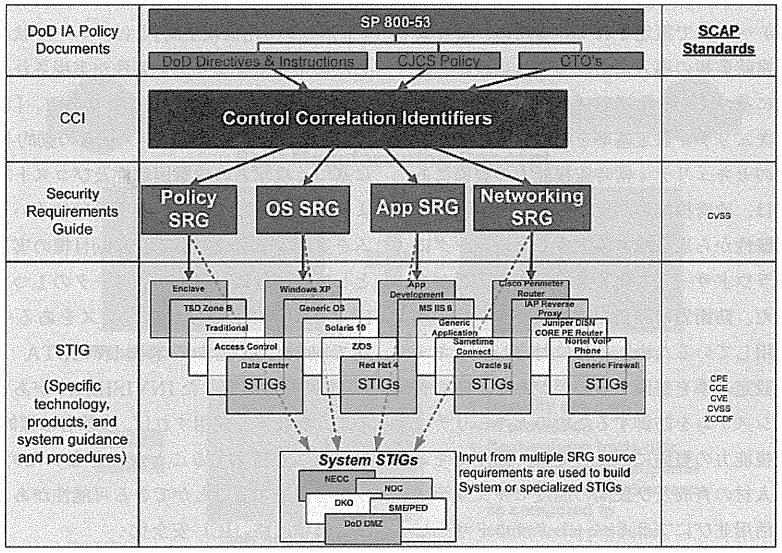

図5.4-5　DoDのSTIGコンテンツ作成イメージ

出典：STIGs, SCAP and Data Metrics, DISA, July 2010

公表された「政府機関における情報セキュリティに係る年次報告（平成24年度）」において、APT攻撃に対する対策としては、「情報システムにおける適正な対策の実施及び監視・運用の強化を伴う計画的で持続可能な情報セキュリティ投資が必要である」と述べられているが、その監視対象は新たな脅威であり資産及びセキュリティ管理策の脆弱性には言及されていない[20]。この年次報告、パブリックコメント等に基づきNISCが策定した「サイバーセキュリティ戦略」では、APT攻撃に対する新たなリスクベースの対応の1つとして「脆弱性への対処」が取り上げられたが、まだ、具体的なセキュリティ常時監視の基本方針まで至っていない[21]。今後、この「脆弱性への対処」の重要性を政治トップ層に啓蒙するとともに概念を具体化する必要がある。

政府機関の情報セキュリティ対策における政府機関統一技術基準はISO／IEC 27001（ISMS）ベースで策定されているため、セキュリティ常時監視の導入にあたっては当該統一技術基準に基づくOS及びアプリケーションに関するセキュリティ設定基準を整備する必要がある。そのセキュリティ常時監視能力の整備にあたっては、政府機関の高度セキュリティ人材確保の困難性から当該能力のアウトソーシングによるクラウドサービス化等を検討する必要がある。また、防衛省は独自の情報セキュリティ基準を適用しているため、それに対応したセキュリティ設定基準を整備する必要がある。防衛省の情報システムを防御するためのセキュリティ常時監視能力の整備にあたっては、高度セキュリティ人材の育成及び民間の高度セキュリティ人材の活用並びにプライベートクラウドサービス化を検討する必要がある。

一方、国内の民間におけるISMS認証取得組織数は、世界の半分以上（世界のISMS認証取得組織数：7,940組織（2012年8月））である4,310組織（2013年6月8日現在）を占めており、静的な紙ベースの情報セキュリティ監査からISO／IEC 27001に基づくセキュリティ常時監視への移行の情報セキュリティ投資の経営判断のために経営層への啓蒙が必要である[22][23]。また、国内の民間のセキュリティ常時監視サービスについては、MSS（Managed Security Service）の一環として提供されるものと予測される。

5.5 防護能力向上

(1) テーラー化信頼空間及び移動目標[24]

米国の大統領管理室国家科学技術委員会は、米国サイバーセキュリティ研究開発戦略のゲームチェンジャー主要テーマとして、表5.5-1に示すとおり防護能力を飛躍的に向上する「テーラー化信頼空間」及び「移動目標」を挙げている。

「テーラー化信頼空間」とは、ユーザ状況に応じた適切なセキュリティ要件が実現される信頼性の高い環境を実現するものである。「移動目標」とは、目標の環境パラメータの動的「変化」に基づく攻撃者の攻撃困難性及びコスト増加によって被攻撃下での悪影響を受けにくいシステムを実現するものである。移動目標の実用化例としては、目標の環境パラメータの1つであるIPアドレス及びMACアドレスをある一定周期で動的に変化する米国INVICTA NETWORK社が開発したINVISILANがある。このような技術を使用すれば、攻撃者は標的のIPアドレスを探索することができないためAPT攻撃を回避することができる可能性がある。

(2) 集積回路（IC）安全化

ハードウェアのサプライチェーン攻撃に対応するために、米国のIARPA及びDARPAはそれぞれ集積回路の製造プロセス革新及び試験法の研究開発を行っている。

IARPAは、「高信頼集積回路（TIC）計画」においてオフショア製造ICの安全性及び知的財産権保護のための分割製造（Split-Manufacturing）プロセス（オフショアでのトランジスタ層FEOL（Front-End-Of-Line）製造プロセスと米国施設での金属化BEOL（Back-End-Of-Line）プロセスとの分割）の確立を目的としている[25]。このIC分割製造概念を図5.5-1に示

表5.5-1 「テーラー化信頼空間」及び「移動目標」の研究開発

テーマ	研究目的	研究目標	備考
テーラー化信頼空間（Tailored Trustworth Space）	ユーザー状況に応じた適切なセキュリティ要件が実現される信頼性の高い環境の実現	・状況に応じたセキュリティ要件の的確な設定 ・特定のセキュリティ属性毎の保証レベルの調整 ・検証可能な情報に基づくシステム間の信頼の確立	
移動目標（Moving Target）	動的「変化」に基づく攻撃困難性及びコストの増加による被攻撃下での悪影響を受けにくいシステムの実現	・耐性システムの設計 ・移動目標メカニズムの開発 ・移動目標メカニズムの有効性の分析 ・彼の行動の観測及び分析能力の強化	移動目標の実用化例：INVICTA NETWORKS社のINVISILAN（IPアドレス及びMACアドレスのホッピング）

出典：Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program, Executive Office of the President, National Science and Technology Council, Dec. 2011

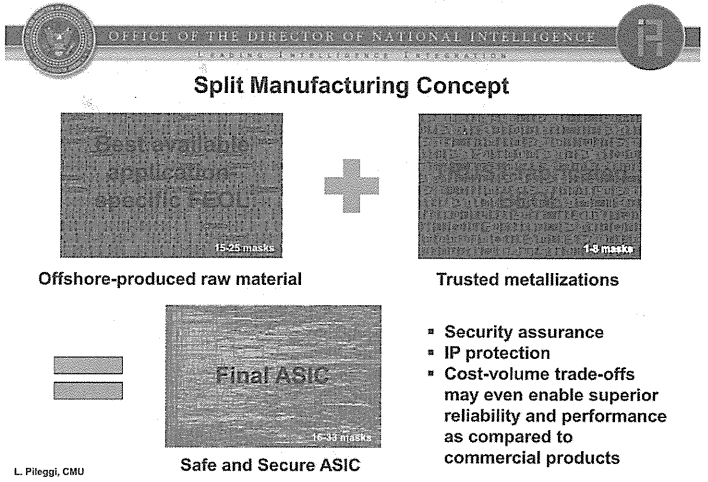

図5.5-1 IC分割製造概念

出典：Trusted Integrated Chips (TIC), ODNI, July 27, 2011

す[26]。一方、DARPAは、「集積回路安全化・高信頼化（IRIS）計画」においてIC機能試験とタンパリング有無確認並びに有効寿命決定のための技術開発を目的としている[27]。

(3) セキュアブート

セキュアブート（Secure Boot）は、コンピュータの起動時にディジタル署名のあるファームウェア、オペレーティングシステム（OS）・ローダー等しか実行できないようにする、システム実装時の防護能力を向上する技術である。本技術は、BIOSに変わるファームウェアのインタフェース仕様である「UEFI（Unified Extensible Firmware Interface）」によって策定されている。現在の最新仕様は、UEFI Specification V.2.3.1（27.1 Secure Boot）（June 27, 2012）である。マイクロソフト社のWindows 8は、UEFI Secure Bootを採用している。セキュアブートの概念を図5.5-2に示す。

(4) サプライチェーンリスク管理の標準化

ICTサプライチェーンリスク管理の標準化については、NISTが2012年10月に「NIST IR 7622 サプライチェーンリスク管理プラックティス改訂版」を公表し、その新標準である「NIST SP 800-161 サプライチェーンリスク管理プラックティス（案）」を2013年8月に出している。また、「NIST SP 800-53 Rev. 4 セキュリティ管理策（2013年4月）」では「SA-12 サプライチェーン防護」管理策の強化を行っている。NIST IR 7622が提示しているサプライチェーンリスク管理プラックティス及びNIST SP 800-53 Rev. 4が提示しているサプライチェーン防護管理策の強化をそれぞれ次に示す。

① NIST IR 7622のサプライチェーンリスク管理プラックティス[28]

- サプライチェーン要素、プロセス及びアクターの識別
- サプライチェーンにおけるアクセス及び露出の制限
- 要素、プロセス、ツール及びデータの源の確立及び維持
- 厳しい制限内での情報共有
- サプライチェーンリスク管理啓蒙訓練の実施
- システム、要素及びプロセスの防御設計の活用
- 継続的インテグレータレビューの実施
- 配送メカニズムの強化
- 維持活動及びプロセスの保証
- システムまたは要素ライフサイクルにおける処分及び最終廃棄活動の管理

② NIST SP 800-53 Rev. 4のサプライチェーン防護管理策の強化[29]

- 調達戦略／ツール／方法論
- 供給者レビュー

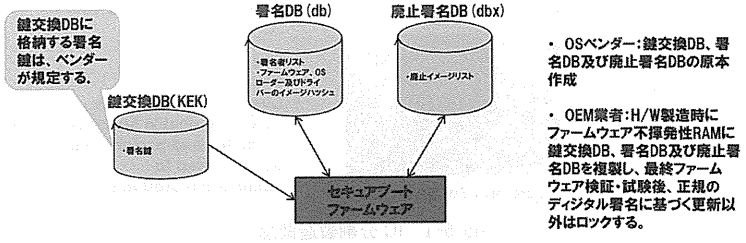

図5.5-2 セキュアブートの概念

・損害の限定
・選定／受領／更新前の評価
・オールソースインテリジェンスの活用（潜在的供給者の分析）
・運用セキュリティ
・本物及び警告されないことの妥当性評価
・サプライチェーン要素、プロセス及びアクターの侵入試験／分析
・組織相互間協定
・重要情報システム構成要素
・情報システム、システム構成要素または情報システムサービスの識別及び追跡性
・サプライチェーン要素の弱点または欠陥対応プロセス

一方、国際標準化機関であるISO／IECは、次に示す「ISO／IEC 27036（供給者関係の情報セキュリティ）」の策定を行っている。

- 第1部：概要及び概念
- 第2部：共通要件
- 第3部：ICTサプライチェーン指針
- 第4部：アウトソーシング・セキュリティ指針

5.6 サイバー耐性向上[30][31]

サイバー攻撃は完全防御できないため、被攻撃下においても情報システムの運用継続を可能とすることを目的として、サイバー耐性（Cyber Resiliency）に関する研究が米国で行われている。

サイバー耐性は、MITRE社によると次のように定義されている。

「国家、組織または任務または業務が機能することが必要なサイバー資源の不利な条件、ストレスまたは攻撃に直面する能力を向上するために予測する、耐える、復旧する、及び進化する能力」

また、サイバー耐性を実現するための方法論として、サイバー耐性工学（Cyber Resiliency Engineering）が次のように定義されている。

「サイバー耐性を向上するために進化する耐性プラックティスを適用できる方法並びにそれらプラックティスの異なる適用戦略に関連するトレードオフを検討する任務保証工学の一研究分野」

サイバー耐性の目標、ねらい及び技法を体系

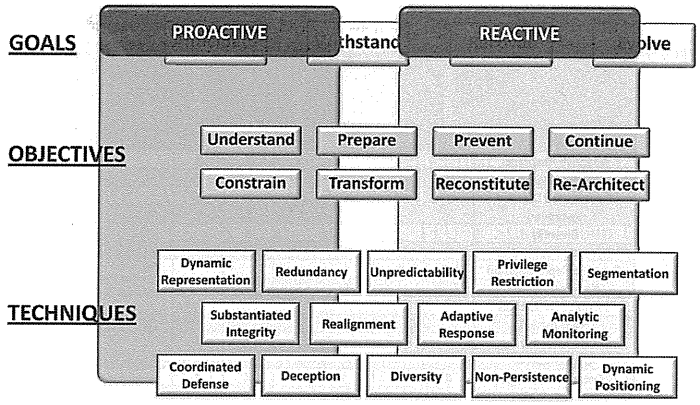

図5.6-1 サイバー耐性のアーキテクチャ

出典：Resiliency in Context, Harriet Goldman, Mitre, May 31, 2012

化したアーキテクチャを図5.6-1に示す。

サイバー耐性の「目標(Goal)」は、Anticipate(予測する)、Withstand(耐える)、Recover(復旧する)及びEvolve(進化する)である。また、これらの目標を達成するための「ねらい(Objective)」として、次に示すものにブレークダウンされている。

① Understand(理解する)

敵、任務またはサイバー資源に関する業務機能依存性並びに敵の活動に関するそれら資源の状態の表示を維持する。

② Prepare(準備する)

予測したサイバー攻撃に対応する実際のサイバー実施方針を維持する。

③ Prevent(予防する)

成功するサイバー攻撃実施を不可能にする。

④ Continue(継続する)

被攻撃下の不可欠な任務/業務機能の期間及び実行可能性を最大化する。

⑤ Constrain(制限する)

敵の攻撃からの被害を限定する。

⑥ Reconstitute(復旧する)

成功した攻撃の結果に対してできる限り任務/業務機能を完全に提供するためにサイバー資源を再運用する。

⑦ Transform(転換する)

過去、現在または未来のサイバー攻撃対応における組織的行動を変える。

⑧ Re-architect(再アーキテクチャ化する)

サイバー耐性技法をより有効に適用するためにアーキテクチャを修正する。

さらに、これらの「ねらい」を実現するために次に示す技法が挙げられている。これらの「ねらい」と「技法」の相関関係を表5.6-1に示す。

① Adaptive Response(適応対応)

攻撃が実行中である表示に対応するアクションを攻撃特性に基づき行う。

② Analytic Monitoring(分析的監視)

潜在的脆弱性、敵の行動及び我の損害を識別するためにリアルタイム及び調整された方法でデータを収集及び分析する。

③ Coordinated Defense(調整防御)

敵の行動に対して重要資源を防御するために複数の明確なメカニズムを適応的及び調整された方法で管理する。

④ Deception(欺瞞)

敵を混乱させるために混乱及び偽命令(例えば、偽情報)を使用する。

⑤ Diversity(多様性)

攻撃の影響の最小化及び敵に対する複数の異なるタイプの技術への攻撃の強制を行うために異質な技術を使用する。

⑥ Dynamic Positioning(動的配置)

分散処理並びに重要アセット及びセンサの動的再配置を用いる。

⑦ Dynamic Representation(動的表示)

構成要素、システム、サービス、任務依存性、敵の活動及び代替サイバー実施方針の効果の表示及び維持を行う。

⑧ Non-Persistence(非一貫性)

情報、サービス及び限定された時間の接続を維持し、脆弱性の攻撃及び一貫した足掛かりの確保のための敵の機会を削減する。

⑨ Privilege Restriction(特権制限)

サイバー資源を使用するために必要な特権並びに重要性と信頼の形式及び程度に基づき利用者及びサイバーエンティティに割り当てられた特権を制限する。

⑩ Realignment(再配置)

中核の任務/業務機能のサイバー資源を調整し、攻撃面を削減する。

⑪ Redundancy(冗長化)

重要資源(情報及びサービス)の複数の防護されたインスタンスを維持する。

⑫ Segmentation(分割)

起源及び/または重要度に基づき構成要素を分割し、成功する攻撃の拡散または損害を限定する。

⑬ Substantiated Integrity(確認された完全性)

重要なサービス、情報、情報の流れ及び構成要素が敵によって改竄されてないことを保証する。

⑭ Unpredictability(予測不可能化)

敵によるアクションの対応ではなくて、頻繁及びランダムに変更する。

表5.6-1 サイバー耐性の「ねらい」と「技法」の相関関係

	Understand	Prepare	Prevent	Constrain	Continue	Reconstitute	Transform	Re-Architect
Adaptive Response				X	X	X		
Analytic Monitoring	X	X		X		X		
Coordinated Defense		X	X	X	X	X		
Deception	X		X		X			
Diversity			X		X			X
Dynamic Positioning	X		X		X			X
Dynamic Representation	X	X					X	
Non-Persistence			X	X	X			X
Privilege Restriction			X	X				
Realignment				X			X	
Redundancy					X	X		
Segmentation			X	X				
Substantiated Integrity	X			X	X	X		
Unpredictability	X		X		X			

出典:Cyber Resiliency Engineering Framework, Deborah J. Bodeau, Mitre, Sept. 2011

5.7 サイバーセキュリティ情報交換の標準化

インシデント対応及びサイバー脅威の情報共有の向上のためにサイバーセキュリティ情報交換の標準化がIETF(Internet Engineering Task Group)、ITU-T Study Group 17 Security及び米国MITRE社において行われている。

(1) IETFの標準化[32)33)]

IETFは、カーネギメロン大学(CMU)のCERT-CCが開発したセキュリティインシデントを記述する標準様式をRFC 5070 IODEF(Incident Object Description and Exchange Format)として2007年12月に策定している。また、IETFは、IODEFデータモデルの新しい拡張(データ保護、構造化されたサイバーセキュリティ情報の統合等)及びRID(Real-time Inter-network Defense)メッセージの一般化を行うMILE(Managed Incident Lightweight Exchange)を開発中である。その拡張要素としては、AttackPattern、Platform、Vulunerability、Scoring、Weakness、Eventreport、Verification及びRemidiationの8つのクラスがある。

(2) ITU-T Study Group 17の標準化[34)]

ITU-T Study Group 17は、既存の各種標準技術を組み合わせたCYBEXというサイバーセキュリティ情報交換フレームワーク(Cyber Security Information Exchange Framework)を規定するITU-T勧告X.1500を2011年4月に制定している。CYBEXは、情報交換に焦点

を絞り、情報を構造化し、その情報をセキュアに交換するためのフレームワークを規定している。その情報表現は、「弱点・脆弱性及び状態の記述」、「イベント・インシデント及びヒューリスティックの記述」及び「情報交換ポリシーの記述」という3つの技術群（クラスタ）に分けて規定されている。「弱点・脆弱性及び状態の記述」クラスタの標準は、CVE、CVSS、CWE、CWSS、OVAL、XCCDF、CPE、CCE及びARFから構成される。また、「イベント・インシデント及びヒューリスティックの記述」クラスタの標準は、CEE、IODEF、CAPEC及びMAECから構成される。

(3) 米国MITRE社の標準化[35)]

米国MITRE社は、サイバー脅威情報共有のために、サイバー脅威の情報表現標準化を次に示すとおり行ってきた。

- CVE (Common Vulnerabilities and Exposures)：共通脆弱性識別子
- CWE (Common Weakness Enumeration)：共通ソフトウェア弱点一覧
- CAPEC (Common Attack Pattern Enumeration and Classification)：共通攻撃パターン及び分類
- MAEC (Malware Attribute Enumeration and Characterization)：マルウェア属性一覧及び特性
- CybOX (Cyber Observales eXpression)：サイバー観測値表現

現在、MITRE社は、高度なサイバー脅威インテリジェンスに対応するために、サイバー脅威情報を表現する構造化言語であるSTIX (Structured Threat Information eXpression)を開発している。STIX言語は、フルレンジの潜在的なサイバー脅威情報の伝達並びに十分な表現性、柔軟性、拡張性、自動化及び可能な限りの人間可読性を目指している。STIXの用途には、サイバー脅威分析、サイバー脅威の表示パターンの具体化、サイバー脅威防止・対応活動管理及びサイバー脅威情報共有がある。STIXは、サイバー脅威インテリジェンスを提供するために次に示す多様なサイバー脅威情報を統合化する図5.7-1に示すアーキテクチャを提供する。

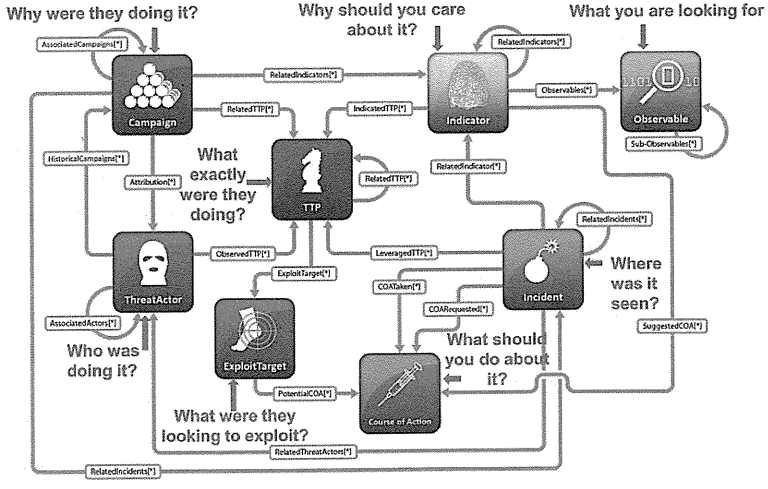

図5.7-1 STIXアーキテクチャ

出典：Cyberattack Analysis and Information Sharing in the U.S., Sean Barnum, MITRE, Feb. 22, 2013

- Cyber Observables：サイバー観測値（例. ファイル関連情報、レジストリキー値、開始サービス、HTTPリクエスト等）
- Indicators：意味及びコンテキストを持つ潜在的な観測値
- Incidents：具体的な敵行動のインスタンス
- Adversary Tactics, Techniques and Procedures (TTP)：敵の戦術、技法及び手順
- Exploit Targets：エクスプロイト標的（例. 脆弱性、弱点または構成）
- Course of Action：対処方針
- Cyber Attack Campaign：敵のサイバー攻撃意図
- Cyber Threat Actors：敵の識別及び／または類別

また、MITRE社は、サイバー脅威情報をセキュアかつ自動的方法で共有するためにSTIX言語で表現されたサイバー脅威情報のトランスポート層としてTAXII (Trusted Automated eXchange of Indicator Information)の開発を進めている。

5.8 制御システムの防御

重要インフラにおいて主に使用されている制御システムのサイバー防御技術の国内及び米欧の動向について述べる。

(1) 制御システムのサイバー防御技術の国内の動向

我が国における制御システムの脆弱性攻撃対応については、経済産業省が中心となって制御システムのセキュリティ強化及び海外への輸出の促進に向けた諸課題を検討するため、2011年10月に官民による検討タスクフォースを設置している。この組織では、産業用制御システム(IACS)セキュリティ標準としてのIEC (International Electrotechnical Commission) 62443国際標準化の推進、技術研究組合制御システムセキュリティセンター（2012年3月6日）によるサイバーセキュリティテストベッドの構築、IEC 62443に基づくISCI (ISA Security Compliance Institute)との相互認証フレームワークの将来構想、インシデントハンドリング対処手順ガイドライン策定、米国国土安全保障省とのインシデント対応及び脆弱性対応の連携による日本版ICS-CERTの早期立ち上げ準備が行われている。

ア 制御システムのセキュリティ標準・基準

制御システムのセキュリティ標準・基準は、対象範囲、対象事業分野によって異なっており、その全体像を図5.8-1に示す。米国では、ISA (The International Society of Automation)が制御システムセキュリティとして、ISA 99を制定している。IEC 62443は、それに基づき定められている[36)]。

また、欧州のESCoRTSプロジェクトが提示した既存標準の管理策と利用者分野における位置づけを図5.8-2に示す。この図中のISA 99は、IEC 62443を指している。この図からISA 99 (IEC 62443)が、対象範囲、業種分野及び利用者分野に対して包括的な標準であり、情報システムのセキュリティ管理策の米国標準であるNIST SP 800-53及び国際標準であるIEC／ISO 27001を含むことがわかる[37)]。

このような背景に基づき、我が国は制御システムのセキュリティ標準として、IEC 62443を選択し、国際標準化の推進を行っている。IEC

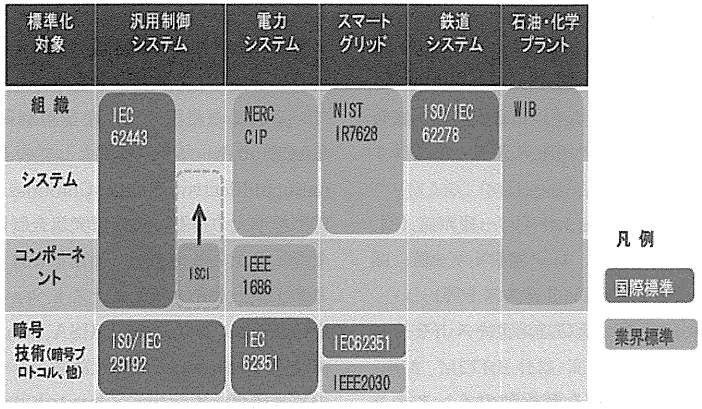

図5.8-1　制御システムに係るセキュリティ標準・基準の全体像

出典：制御システムセキュリティ検討タスクフォース報告書中間とりまとめ、経済産業省、2012年６月１日

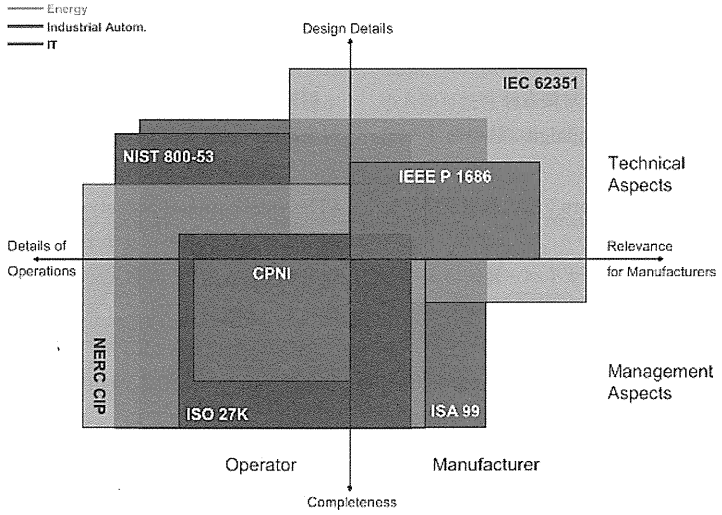

図5.8-2　ESCoRTS プロジェクトにおける既存標準の位置づけ

出典：ESCoRTS：R&D and standardization Road Map, preliminary Deliverable 3.1 Rev. ESCoRTS Consortium

62443の標準一覧及び最新の策定状況を図5.8-3に示す[38]。IEC 62443国際標準化の状況については、最も重要である「制御システムセキュリティ管理システム(CSMS)－要件(IEC 62443-2-1)」が我が国の情報システムのセキュリティ管理策ベストプラクティスであるISO／IEC 27001(ISMS)ベースで作成が進められている。IPAが行ったIEC 62443-2-1とISO／IEC 27001のセキュリティ管理策の比較結果では、それぞれの共通要件の割合は100／126及び73／100で大部分を占めている。IEC 62443-2-1の固有要件26件の内訳は、リスク評価・管理(４件)、セキュリティ組織・訓練(３件)、物理セキュリティ(２件)、権限分離（２件)、アクセス制御（７件)、インシデント対応（２件）等である[39]。さらに、2012年のIEC 62443国際標準化の新しい動向としては、次に示す３点が挙げられる。

・「制御システムセキュリティ・ライフサイクル及び利用事例（IEC／TR 62443 1-4 IACS security lifecycle and use-case)」の追加

・「制御システムセキュリティ管理システム(CSMS)－要件(IEC 62443-2-1)」のStuxnetに対抗するためのセキュリティ管理策の１／３（33項目）の見直し勧告(ISA-TR 62443-0-3、D1E9、June 21、2012)[40]

・「制御システムセキュリティ計画の運用(IEC 62443 2-2 Operating an IACS security program)」の中止及び「制御システムセキュリティ管理システム－実現指針(IEC／TR 62443 2-2 IACS security management system-implementation guide)」に置換

我が国では、ISMS認証を受けた企業が世界の半分程度を占めており、ISMS認証済み企業であれば、CSMS認証も容易に取得できる能力を保有しているものと考えられる。しかし、我が国においては、ISMS認証済み防衛関連企業でもAPT攻撃を受けており、制御システムについても、このような静的認証に基づく対策だけでは十分でなく、情報システムと同様にセキュリティ常時監視の導入が必要である。

イ　サイバーセキュリティテストベッド[41][42]

サイバーセキュリティテストベッドは、多賀

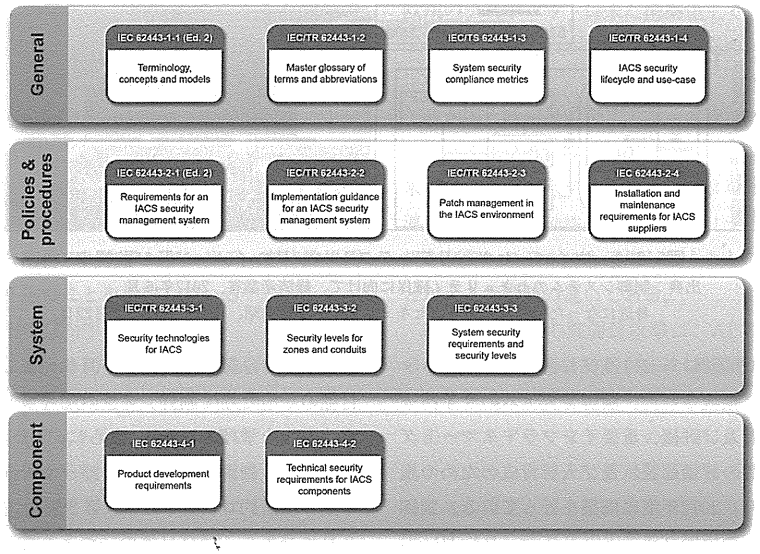

図5.8-3　IEC 62443の最新の策定状況

出典：Eric Cosman, ISA 99 Co-Chair

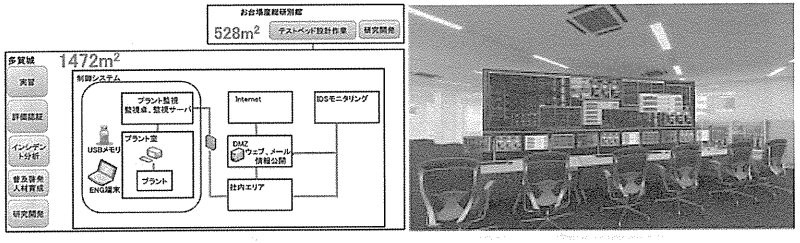

図5.8-4　サイバーセキュリティテストベッドのイメージ及び監視卓

出典：制御システムのセキュリティ確保に向けて、経済産業省、2012年6月
身近になった制御システムのセキュリティ、小林偉昭、IPA、2013年2月22日

城(みやぎ復興パーク)及びお台場に分散しネットワーク接続された、制御システムのサイバー攻撃演習及び評価、重要インフラ・スマートグリッド等の評価認証、及び人材育成のための施設であり、2012年度に構築を行っている。制御システムの模擬プラントとしては、PA（Process Automation)、FA（Factory Automation)、BA（Building Automation)、発電・変電及びガスが設置予定である。サイバーセキュリティテストベッドのイメージ及び監視卓を図5.8-4に示す。

(2)　制御システムのサイバー防御技術の米国及び欧州の動向

ア　米国の動向

米国における制御システムの脆弱性攻撃対応については、前述したISA、国立技術標準局(NIST)、エネルギー省（DoE)、国土安全保障省（DHS）及びICS-CERTが行っている。NISTは、「NIST SP 800-82 Rev.1　制御システムセキュリティ指針」を2013年5月に発表し、情報システムのセキュリティ管理策であるNIST SP 800-53をベースとした制御システムのセキュリティ管理策を策定している。また、これは制御システムのセキュリティ管理策の常時監視を要件として挙げている[43]。DoEは、「エネルギー供給システムサイバーセキュリティ実現ロードマップ」を2011年9月に発表し、その目標の一つとして制御システムセキュリティの常時監視を挙げている[44]。さらに、DHSのICS-JWGは、「制御システムサイバーセキュリティの業界横断的ロードマップ（第3版)」を2011年9月に発表し、開発目標の一つとしてセキュリティ管理策の常時監視の段階的開発を示している[45]。DHSと共同でDoE配下のアイダホ国立研究所(INL)は、サイバーセキュリティ事業として、テストベッドであるNTSB（National SCADA Test Bed）による制御システムの脆弱性検証及び人材育成のためのサイバー演習を行っている。また、INLは、検証結果を基にした制御システムセキュリティ標準化活動の支援として、「制御システムに関する推奨セキュリティの要件規格」を発行している[46]。ICS-CERTは、制御システムのマルウェア解析、インシデント対応、脆弱性ハンドリング、ガイドラインや評価ツールの作成等を行っている。

重要インフラのサイバーセキュリティを向上するために、重要インフラのセキュリティレベル及びサイバー耐性の向上、有効かつ効率的な官民サイバー脅威情報交換の促進と支援、及びサイバー脅威とインシデントに関連するデータ分析フレームワークの開発をねらいとする「重要インフラのサイバーセキュリティフレームワーク」の策定をNISTに指示する大統領令(EO 13636)が2013年2月12日に出された[47]。また、それと同時に重要インフラの物理及びサイバーに関する脅威及び脆弱性の状況認識能力デモ開発を含む大統領決定（PPD-21）が出された[48]。さらに、DoDは、この大統領令に基づき、重要インフラサービス調達において制御システムの防御のためのセキュリティ常時監視要件を盛り込むことを検討している[49]。

イ　欧州の動向[50]

欧州における制御システムの脆弱性攻撃対応については、欧州連合（EU）の欧州ネットワーク・情報セキュリティ庁（ENISA）が、情報システムの側から制御システムのセキュリティ課題をアプローチし、2011年12月に「制御システムの防御勧告」を発表し、制御システムセキュリティ戦略立案、ベストプラックティス活用による制御システムセキュリティ基準の策定、テストベッドの構築、評価認証フレームワークの策定、ICS-CERTの立ち上げ等を挙げている。欧州のテストベットは未だ構築途上である。

(3)　制御システムの脆弱性攻撃対応のあり方及び課題

我が国と欧州は、テストベッド及びセキュリティ評価認証を重視したアプローチであるが、米国は、情報システムのAPT攻撃対策として導入している実効性のあるセキュリティ常時監視を制御システムにも適用しようとしていることが大きな戦略の違いである。

制御システムの脆弱性攻撃は、APT攻撃そのものであるため、その対応には情報システムに対するAPT攻撃対策と同様に、情報システムのベストプラックティスの活用による制御システムのセキュリティ管理策及びリスク管理プロセスの策定とともに、当該セキュリティ管理策に基づく防護及び検知対策に加えて、最終的には米国と同様に我が国においても制御システムのセキュリティ常時監視の段階的開発が必要である。

参考文献

1）ISO：ISO／IEC 27005：2011, Information technology-Security techniques－Information security risk management, 2011
2）NIST：NIST SP 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations, NIST, Sept. 2011
3）OMB：Fiscal Year 2009 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002
4）OMB：M-10-15, MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES, 21 April 2010
5）DHS：Continuous Monitoring and Cloud Boundary Defense, Federal Network Security Agency and Industry Day, 25 June 2012
6）DHS：Drafts Solicitation for Cyber Security Tools and Services, 20 August 2012
7）H.R.6523－198, Subtitle D－Cyber Warfare, Cyber Security, and Related Matters, Jan. 2011
8）Eustace D. King：Transforming IA Certification and Accreditation Across the National Security Community, DoD, CrossTalk, July 2008
9）Dr. Ron Ross：Mapping Supply Chain Risk Using NIST Standards and Guidelines, NIST, 15 Oct. 2012

10) DNI : ICD503 Intelligence Community Information Technology Systems Security : Risk Management, Certification and Accreditation, 15 Sept. 2008
11) DoD : Cyber 101, Dominic Cussatt, AFCEA West 2013, 29 Jan. 2013
12) NIST : NIST SP 800-39 Managing Information Security Risk : Organization, Mission, and Information System View, NIST, March 2011
13) NIST : NIST SP 800-37 Guide for Applying the Risk Management Framework to Information Systems : A Security Life Cycle Approach, Rev.1, Feb. 2010
14) NIST : NIST SP 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations, NIST, Sept. 2011
15) NIST : NIST SP 800-128 Guide for Security-Focused Configuration Management of Information Systems, August 2011
16) NIST : NIST IR 7756 CAESARS Framework Extension : An Enterprise Continuous Monitoring Reference Model (Second Draft), Jan. 2012
17) NIST : NIST SP 800-126 The Technical Specification for the Security Content Automation Protocol (SCAP) : SCAP Version 1.2, Sept. 2011
18) MITRE : Making Security Measurable
http://makingsecuritymeasurable.mitre.org/about/index.html#config、2013年２月１日アクセス
19) Roger S. Greenwell : STIGs, SCAP and Data Metrics, DISA, July 2010
20) 情報セキュリティ対策推進会議：政府機関における情報セキュリティに係る年次報告（平成24年度）、NISC、平成25年６月19日
21) 情報セキュリティ政策会議：サイバーセキュリティ戦略、NISC、平成25年６月10日
22) ISMS International User Group : International Register of ISMS Certificates, Aug. 2012
http://www.iso27001certificates.com/、2013年７月３日アクセス
23) JIPDEC：ISMS 認証取得組織数推移、2013年６月28日
http://www.isms.jipdec.or.jp/lst/ind/suii.html、平成25年７月３日アクセス
24) Executive Office of the President, National Science and Technology Council : Trustworthy Cyberspace : Strategic Plan for the Federal Cybersecurity Research and Development Program, Dec. 2011
25) IARPA : Trusted Integrated Chips (TIC) Program, 26 Oct. 2011
26) IARPA : Trusted Integrated Chips (TIC), 27 July 2011
27) DARPA : Integrity and Reliability of Integrated Circuits, 15 Sept. 2010
28) NIST : NIST IR 7622 Notional Supply Chain Risk Management Practices for Federal Information Systems, Oct. 2012
29) NIST : NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations Rev.4, April, 2013
30) Deborah J. Bodeau & Richard Graubart : Cyber Resiliency Engineering Framework, MITRE, Sept. 2011
31) Harriet Goldman : Resiliency in Context, MITRE, May 31, 2012
32) IETF : RFC 5070 IODEF : The Incident Object Description Exchange Format, Dec. 2007
33) IETF : IODEF-extension to support structured cybersecurity information, Draft, 12 Feb. 2013
34) 高橋健志：ITU-T 勧告 X.1500：サイバーセキュリティ情報交換フレームワーク、NICT、ITU ジャーナル　Vol. 42　No. 2、2012年２月
35) Sean Barnum : Cyberattack Analysis and Information Sharing in the U.S., MITRE, 22 Feb. 2013
36) 経済産業省：制御システムセキュリティ検討タスクフォース報告書中間とりまとめ、2012年６月１日
37) ESCoRTS Consortium : R&D and standardization Road Map, Preliminary Deliverable 3.1 Rev.
38) ISA 99 Committee : Work Product List
http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx、2013年２月１日アクセス
39) IPA：制御システムにおけるセキュリティマネジメントシステムの構築に向けて、2012年10月10日
40) ISA 99 Committee : ISA-TR 62443-0-3 Security for industrial automation and control systems : Gap assessment of ANSI／ISA-99.02.01-2009, Draft 1, Edit 9, 21 June 2012
41) 経済産業省：制御システムセキュリティ検討タスクフォース報告書中間とりまとめ、2012年６月１日
42) 小林偉昭：身近になった制御システムのセキュリティ、IPA、IPA 重要インフラ情報セキュリティシンポジウム2013、2013年２月22日
43) Keith Stouffer, Joe Falco and Karen Scarfone : NIST SP 800-82 Rev.1 Guide to Industrial Control Systems (ICS) Security, NIST, May 2013
44) Energy Sector Control Systems Working Group : Roadmap to Achieve Energy Deliver Systems Cybersecurity, Sept. 2011
45) ICSJWG : Cross-Sector Roadmap for Cybersecurity of Control Systems, 30 Sept. 2011
46) DHS : Catalog of Control Systems Security : Recommendations for Standards Developers, Sept. 2009
47) The White House : Executive Order : Improving Critical Infrastructure Cybersecurity, 12 Feb. 2013
48) The White House : Presidential Policy Directive (PPD-21) Critical Infrastructure Security and Resilience, 12 Feb. 2013
49) Aliya Sternstein : Pentagon will require security standards for critical infrastructure networks, 15 Feb. 2013
50) ENISIA : Protecting Industrial Control Systems : Recommendations for Europe and Member States, 9 Dec. 2011