産業用制御システム セキュリティガイドを読むために

NIST（アメリカ国立標準情報技術研究所）SP 800-82 Ver.2 ：産業用制御システム（ICS：Industrial Control Systems） セキュリティガイドへの導入

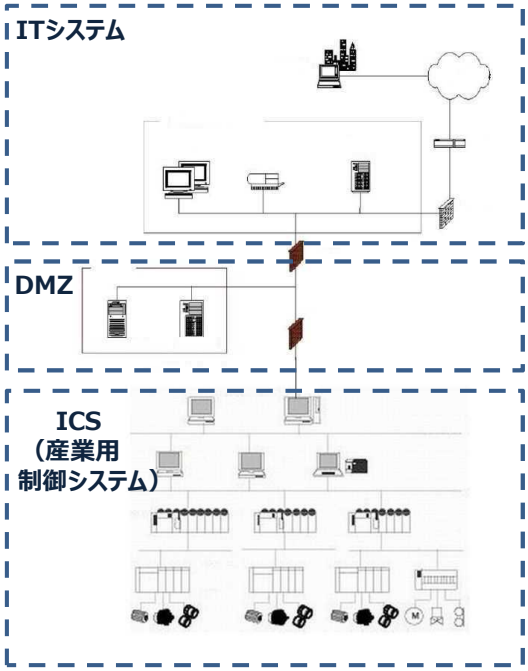
2018年12月25日
（一社）日本電機工業会　技術部

（注）本文書は、NIST　SP 800-82 Ver.2*（和英併記版）を読むために、その背景と概要について、筆者の理解の範囲内でまとめたものです。正確な内容及び完全な内容について調べる場合は、Web上に掲載された原本を参照ください。NISTSP 800-82は，米国国立標準技術研究所（NIST）の著作権物です。
＊原文　http://dx.doi.org/10.6028/NIST.SP.800-82r2
和訳(JPCERT/CCのWebページ) https://www.jpcert.or.jp/ics/information02.html

1．NIST SP800-82とは

NIST SP800-82とは、アメリカ政府機関に産業用制御システム（ICS）を納入する際に、納入業者が守るべきセキュリティポリシーを示した文書

民間向けでも参照される



ITシステムとICSの関係図

NIST SP800-82

セキュリティポリシーのリスト
（NIST SP800-82
第2版ICSオーバーレイ）

～

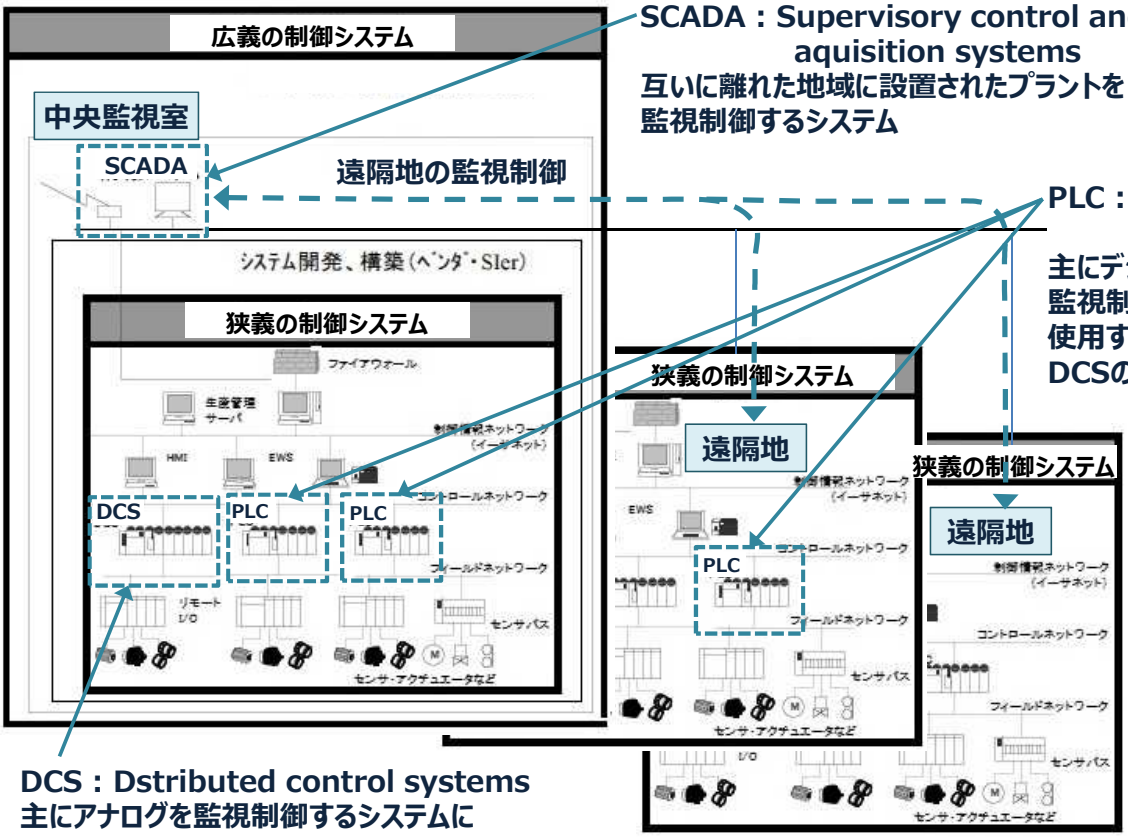
連邦情報強化法と
大統領命令に従うための
セキュリティポリシー

ICS
（産業用制御システム）
を納入

セキュリティポリシーを
反映した上で
政府機関へ納入

アメリカ
政府機関

2.産業用制御システム の中核「SCADA」「DCS」「PLC」とは



SCADA：Supervisory control and data aquisition systems
互いに離れた地域に設置されたプラントを１カ所から監視制御するシステム

PLC：Programmable logic controllers
主にデジタル・離散系を監視制御するシステムに使用するコントローラ。
DCSの子局としても使用。

DCS：Dstributed control systems
主にアナログを監視制御するシステムに使用するコントローラ。PLCの親局としても使用。

NIST SP800-82：SCADA、DCS、PLCの設定について記載あり。

3.米国政府組織内のNISTの位置付け

米国政府機関

- エネルギー省(DOE)
  - 配電・エネルギー信頼性局(OE)
  - 国立研究所
    - パシフィックノースウエスト(PNNL)
    - アイダホ(INL)
    - サンディア(SNL)
    - アルゴン(ANL)
    - オークリッジ(ORNL)
- 国土安全保障省(DHS)
  - サイバーセキュリティについて所管
  - 国家サイバーセキュリティ部門(NCSD)
  - 科学技術局(S&T)
  - US-CERT
- 商務省(DOC)
  - 国立標準技術研究所(NIST)
    - 政府の調達システムの仕様を規定
- 環境保護庁(EPA)
- 国立科学財団(NSF)

出典：
IoT関連のNIST発行文書の分野
2015年11月
IPA/SEC
ソフトウェアG
資料より

表. NISTが発行している幅広い分野の文書

国	団体		発行済みの文書が記述する範囲 IoT	CPS	Industorie 4.0	Ecosystems	Smartcities	Clean Production	Industry Technologies	Business Solutions	Marketing	Systems Engineering	Security by Design
EU	IERC	3	○			○	○				○		
	EC	6	○			○	○	○	○				○
DE	acatech	2	○	○	○								○
	Agenct FR(	1			○								
	Fraunhofer	3	○	○	○	○						○	○
	DIN/VDE	1			○								○
US	NIST	10	○	○		○			○			○	○
	IIC	4	○	○		○			○		○		○
	SEI	2											○
	PCAST	2										○	
	INCOSE(N:	3										○	○
	IEEE	1	○	○					○			○	
	GE	3	○	○		○			○				○
	IBM	2	○			○	○			○			○

4. 米国の主な制御システムセキュリティガイドラインとの関連

米国の主な制御システムセキュリティガイドライン
（出典：IPA発行 「重要インフラの制御システムセキュリティとITサービス」

- **NIST SP800-82** ←本規格
  - ・産業用制御システム（ICS）のセキュリティガイド。SCADA、DCS、PLCその他のシステム設定
- **NIST SP800-53**
  - ・連邦政府向け情報システムのセキュリティコントロールを選択するためのガイドライン
- **ANSI/ISA 99.00.01：ANSI（米国国家規格協会）、ISA（the International Society of Automation）発行**
  - ・用語、概念とモデル
- **NERC Cyber Security Standards：NERC（北米電力信頼度協議会）発行**
  - ・電力分野の事業者向けガイドライン

NIST、ISA、IECの協力関係（出典：IPA発行 「重要インフラの制御システムセキュリティとITサービス」

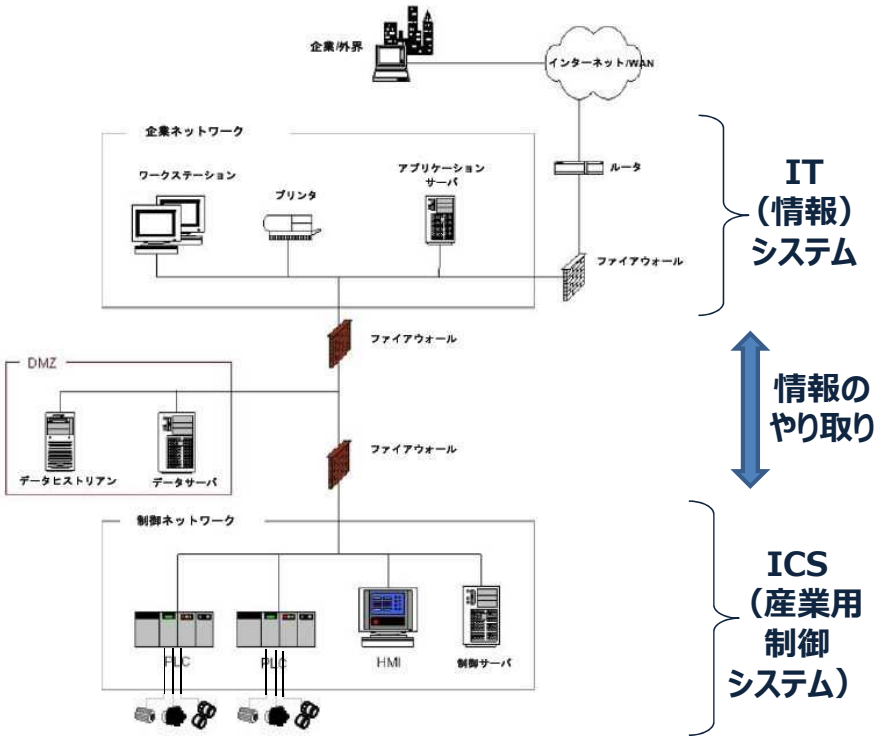
5. NIST SP 800-82 の概要

◆NIST SP 800-82 Ver.2（2015年2月発行）の記載内容

（１）産業用制御システム（ICS）の概要
（２）ITシステムと比較してのICSの特徴、脅威と脆弱性
（３）ICSセキュリティプログラム（準備・対策のプログラム）
（４）ITシステムとICSの接続方法：ネットワークアーキテクチャ
（５）ICSにおけるセキュリティの維持、管理の方法+
（６）付録G：NIST SP800-82 第2版ICSオーバーレイ
アメリカの政府機関に納入するICSシステムのセキュリティに関して実施が必要な項目のリストを「高・中・低の3ランク」に分けて記載 ← NIST SP800-82の中心的な内容

◆ JPCERT/CC（国内のサイバーセキュリティに関する団体）のWebページに和英併記版のNIST SP 800-82 Ver.2が掲載され、ダウンロードが可能。
https://www.jpcert.or.jp/ics/information02.html

6. ITとICSの比較（その１）



ICS（産業用制御システム）の特徴

- ◆物理量を制御する
  安全が優先する
- ◆多数のネットワークが混在している
- ◆コントローラの使用年数が長い
  10～15年
  古いシステムが混在する
- ◆システムを停止するのが困難な場合が多い
- ◆ソフトウェアのアップデートが困難な場合が多い
  ・システムとしての動作確認が必要
  ・システムを停止できないため
- ◆独自のOS、独自の通信方式を持つ機器がある
- ◆ITシステムと情報のやり取りが必要

図．情報（IT）システム と産業用制御システム（ICS）　出典：SP 800-82 Ver.2

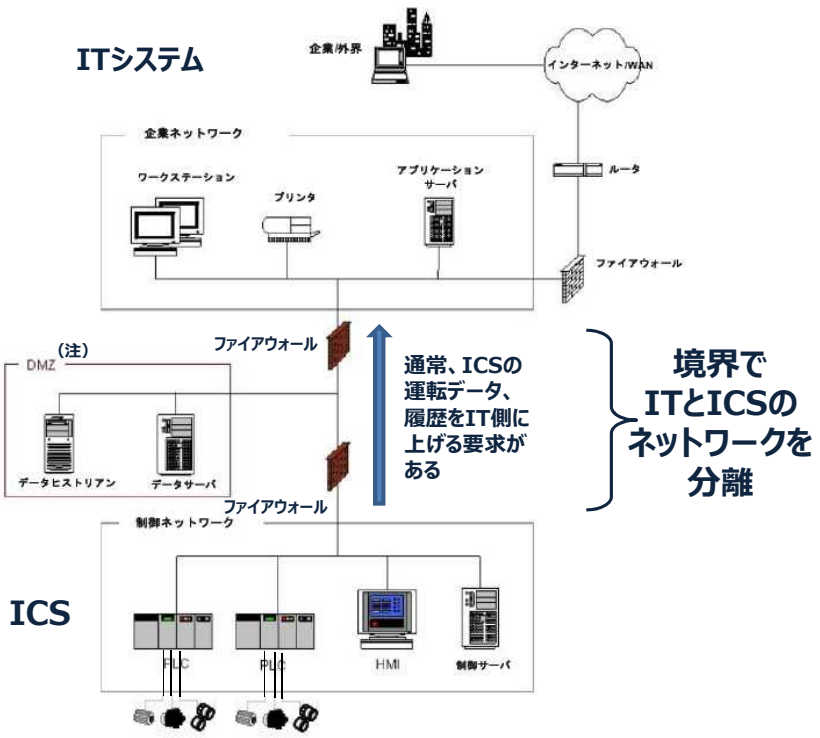
7. ITとICSの比較（その２）

表．情報（IT）システム と産業用制御システム（ICS)の比較　出典：SP 800-82 Ver.2

カテゴリ	情報（IT）システム	産業用制御システム（ICS）
性能要件	リアルタイム不要 応答は一貫していること ハイスループット必須 大きな遅延とジッターは許容 重要な緊急相互作用が少ないこと セキュリティに必要な程度に厳格なアクセス制限を実装できること	リアルタイム 応答は緊急を要する 中程度のスループットで可 大きな遅延やジッターは不可 人その他の緊急相互作用への応答が重要 ICS へのアクセスは厳重に制限されるが、マンマシンインタフェースを阻害・干渉しない
可用性（信頼性）用件	リブート等の応答は可 可用性の欠点はシステムの運用要件に応じて許容されることが多い	プロセスの可用性要件によりリブート等の応答は不可 可用性要件から冗長システムが必要となる場合あり 停止は数日又は数週間前にあらかじめ計画・予定 高可用性要件により徹底的な展開前試験が必要
リスク管理要件	データを管理 データの機密性と保全が肝要 フォールトトレランスはさほど重要でない（瞬時のダウンタイムは重大リスクでない） 重大なリスク影響は業務の遅延	物理世界の制御 人の安全が肝要、プロセスの保護はその次 フォールトトレランスが不可欠、瞬時のダウンタイムも不可 重大なリスク影響は法令不履行、環境への影響、人命・装備品・生産喪失
システム運用	システムは一般的 OS 上で使用 アップグレードは自動展開ツールを利用するので容易	まちまちで専用の OS を使用する場合あり、セキュリティ機能はないことが多い 専用制御アルゴリズムと修正済みハードウエア/ソフトウエアが関係するため、ソフトウエア変更は慎重を要し、通常ベンダーが担当
リソースの制約	システムはセキュリティソリューション等の追加サードパーティアプリケーションに対応する十分なリソースを適用	システムは所期の産業プロセスに対応するようにできており、追加セキュリティ機能に対応する十分なメモリや演算リソースはない

カテゴリ	情報（IT）システム	産業用制御システム（ICS）
通信	標準通信プロトコル プライマリ有線ネットワークで局所的に無線機能あり 一般的 IT ネットワーク規範	多数の専用・標準通信プロトコル 専用有線・無線（無線及びサテライト）を含む数種の通信メディアを利用 ネットワークは複雑で、制御エンジニアの専門知識を必要とすることあり
管理変更	ソフトウエア変更は良好なセキュリティポリシー・手順に従いタイムリーに実施。手順は自動化されていることが多い。	ソフトウエア変更は、システム全体を通じて徹底的に試験・展開し、制御システムが保全されるようにする。ICS 停止の多くは、数日又は数週間前にあらかじめ計画・予定が必要。サポートが終了した OS を使用している場合あり
管理サポート	多様なサポートスタイルあり	サービスサポートは通常 1 業者のみ
コンポーネントの寿命	3 年～5 年	10 年～15 年
コンポーネントの所在場所	通常ローカル所在で、アクセスが容易	コンポーネントは隔絶された遠隔地にあり、アクセスにはかなりの物理的労力が必要

8. ICSセキュリティアーキテクチャ



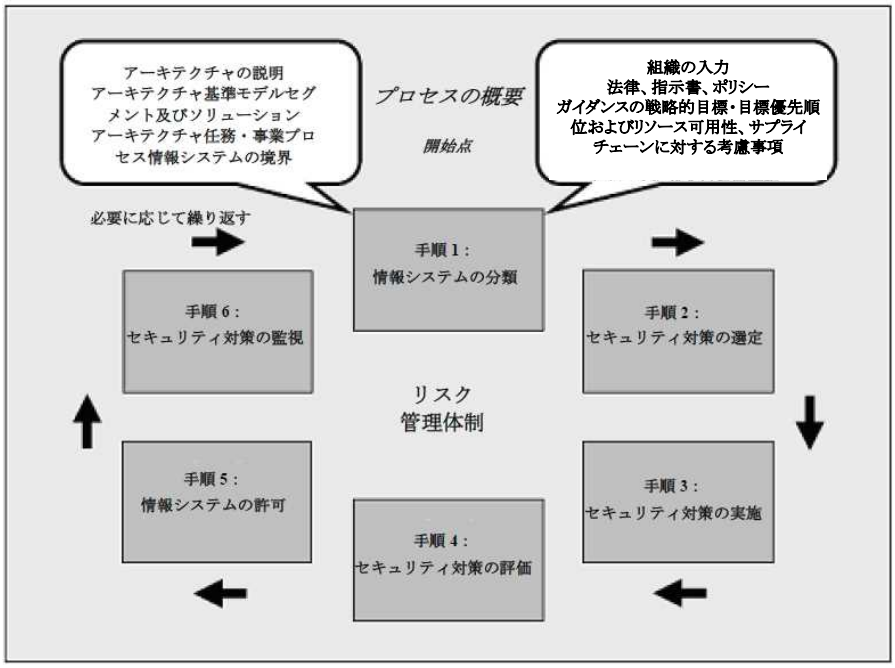
ICSセキュリティアーキテクチャの概要
～ ITとICS間のネットワークの分離～

- ◆境界（ITとICS間）の保護
  - ・DMZ、ファイアウォールの使用
- ◆ファイアウォール
  - ・システムの目的に沿った機能を持つファイアウォール
- ◆論理的なネットワークの分離
  - ・IPネットワークのアドレス構成を区別
- ◆ファイアウォール、DMZ、ルータの組み合わせ及びその機能から、システムの目的の沿った方式をセキュリティを選定
  - ・単独のファイアウォールによる方式
  - ・ファイアウォールとルータによる方式
  - ・ファイアウォールとDMZによる方式
  - ・2台のファイアウォールとDMZによる方式（左図はこの方式の例）

図．ICSセキュリティアーキテクチャ
出典：SP 800-82 Ver.2

（注）DMZ：直訳で「非武装地帯」。ネットワーク間の通信をDMZを経由する通信のみに限る。この方式により、許可されていない通信をカットして、ホワイトリスト（許可されたもののリスト）にある通信に限って、通信ができるようになる。

9. ICSへのセキュリティ対策の実施



図．リスク管理体制業務
出典：SP 800-82 Ver.2

NIST SP800-53の管理策（18分野）
以下の管理策について、システムの要求に合わせてセキュリティのレベルを設定し、管理する。

- ◆アクセス制御（AC）
- ◆意識及び訓練（AT）
- ◆監査及び説明責任（AU）
- ◆セキュリティ評価及び権限付与（CA）
- ◆不測事態計画（CP）
- ◆構成管理（CM）
- ◆識別及び認証（IA）
- ◆インシデント対応（IR）
- ◆保守（MA）
- ◆メディア保護（MP）
- ◆物理境界上の保護（PE）
- ◆プランニング（PL）
- ◆人員のセキュリティ（PS）
- ◆リスク評価（RA）
- ◆システム及びサービスの取得（SA）
- ◆システム及び通信保護（SC）
- ◆システム及び情報の保全（SI）
- ◆プログラム管理（PM）

10. NIST SP 800-82　第2版ICSオーバーレイ（付録G）

◆目的

政府機関業務･資産の情報セキュリティを確保するため、を2014年連邦情報強化法（FISMA）、大統領指示（PPD-21）、大統領命令13636に従い、最低要件を含んだ規格、およびガイドラインをNISTが作成した。

◆NIST SP 800-82　第2版ICSオーバーレイとは

NIST SP800-53 付録F （IT向けのセキュリティ対策のリスト）を元にして、ICSに対応するため、「NIST SP 800-82　第2版　ICSオーバーレイ」として拡張し、ICS特有の事項を記載してまとめたリストである。各項目について、セキュリティレベル（低･中･高）により、実施しなくてはならないかどうかを示す。「選定」と記載された項目は、実施が必要。「空白」で示された項目は実施不要。

◆オーバーレイ（リスト）に記載の項目

176項目のセキュリティの管理項目のリストになっている（次ページ以降にその項目を示す）。

出典：SP 800-82 Ver.2

11. NIST SP 800-82　オーバーレイ　項目一覧（その１）

表 G-1　セキュリティ対策ベースライン

管理番号	管理名	当初の対策ベースライン 低	中	高
AC-1	アクセス制御ポリシー・手順	AC-1	AC-1	AC-1
AC-2	アカウント管理	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	アクセス施行	AC-3	AC-3	AC-3
AC-4	情報フロー施行	未選択	AC-4	AC-4
AC-5	任務の分割	未選択	AC-5	AC-5
AC-6	最小権限	未選択	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	ログイン失敗	AC-7	AC-7	AC-7
AC-8	システム利用通知	AC-8	AC-8	AC-8
AC-10	現行セッション管理	未選択	未選択	AC-10
AC-11	セッションロック	未選択	AC-11 (1)	AC-11 (1)
AC-12	セッション終了	未選択	AC-12	AC-12
AC-14	識別・認証のない許可済み行為	AC-14	AC-14	AC-14
AC-17	リモートアクセス	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	ワイヤレスアクセス	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	モバイルデバイス用アクセス制御	AC-19	AC-19 (5)	AC-19 (5)
AC-20	外部情報システムの利用	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	連携・情報共有	AC-21	AC-21	AC-21
AC-22	公開コンテンツ	AC-22	AC-22	AC-22
AT-1	セキュリティ意識・訓練ポリシー・手順	AT-1	AT-1	AT-1
AT-2	セキュリティ意識訓練	AT-2	AT-2 (2)	AT-2 (2)
AT-3	役割ベースセキュリティ訓練	AT-3	AT-3	AT-3
AT-4	セキュリティ訓練記録	AT-4	AT-4	AT-4
AU-1	監査・説明責任ポリシー・手順	AU-1	AU-1	AU-1
AU-2	監査事象	AU-2	AU-2 (3)	AU-2 (3)
AU-3	監査記録内容	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	監査ストレージ容量	AU-4 (1)	AU-4 (1)	AU-4 (1)
AU-5	監査処理不備への対応	AU-5	AU-5	AU-5 (1) (2)
AU-6	監査の審査・分析・報告	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)
AU-7	監査削減・報告書作成	未選択	AU-7 (1)	AU-7 (1)
AU-8	タイムスタンプ	AU-8	AU-8 (1)	AU-8 (1)
AU-9	監査情報の保護	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	否認防止	未選択	未選択	AU-10
AU-11	監査記録保留	AU-11	AU-11	AU-11
AU-12	監査作成	AU-12	AU-12	AU-12 (1) (3)
CA-1	セキュリティ評価・権限付与ポリシー・手順	CA-1	CA-1	CA-1
CA-2	セキュリティ評価	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	システム相互連接	CA-3	CA-3 (5)	CA-3 (5)
CA-5	行動・マイルストーン計画書	CA-5	CA-5	CA-5
CA-6	セキュリティ権限	CA-6	CA-6	CA-6
CA-7	継続監視	CA-7	CA-7 (1)	CA-7 (1)
CA-8	ペネトレーション・テスト	未選択	未選択	CA-8
CA-9	内部システム接続	CA-9	CA-9	CA-9
CM-1	設定管理ポリシー・手順	CM-1	CM-1	CM-1
CM-2	ベースライン設定	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	設定変更管理	未選択	CM-3 (2)	CM-3 (1) (2)
CM-4	接続影響分析	CM-4	CM-4	CM-4 (1)
CM-5	変更用アクセス制限	未選択	CM-5	CM-5 (1) (2) (3)
CM-6	構成設定	CM-6	CM-6	CM-6 (1) (2)
CM-7	最低限機能	CM-7 (1)	CM-7 (1) (2) (4) (5)	CM-7 (1) (2) (5)
CM-8	情報システムコンポーネント目録	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	設定管理計画書	未選択	CM-9	CM-9
CM-10	ソフトウエア使用制限	CM-10	CM-10	CM-10
CM-11	ユーザがインストールしたソフトウエア	CM-11	CM-11	CM-11
CP-1	不測事態計画ポリシー・手順	CP-1	CP-1	CP-1
CP-2	緊急時対応計画	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)
CP-3	不測事態訓練	CP-3	CP-3	CP-3 (1)
CP-4	緊急時対応計画訓練	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-6	代替ストレージサイト	未選択	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	代替処理サイト	未選択	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	電気通信サービス	未選択	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	情報システムバックアップ	CP-9	CP-9 (1)	CP-9 (1) (2) (3) (5)
CP-10	情報システムの復旧・再構築	CP-10	CP-10 (2)	CP-10 (2) (4)
CP-12	セーフモード	CP-12	CP-12	CP-12
IA-1	識別・認証ポリシー・手順	IA-1	IA-1	IA-1
IA-2	識別・認証（組織ユーザ）	IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)
IA-3	デバイス識別・認証	IA-3	IA-3 (1) (4)	IA-3 (1) (4)
IA-4	識別子管理	IA-4	IA-4	IA-4
IA-5	認証コード管理	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)

出典：SP 800-82 Ver.2

11. NIST SP 800-82 オーバーレイ 項目一覧（その2）

IA-6	認証フィードバック	IA-6	IA-6	IA-6
IA-7	暗号化モジュール認証	IA-7	IA-7	IA-7
IA-8	識別・認証（組織外ユーザ）	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)
IR-1	インシデント対応ポリシー・手順	IR-1	IR-1	IR-1
IR-2	インシデント対応訓練	IR-2	IR-2	IR-2 (1) (2)
IR-3	インシデント対応試験	未選択	IR-3 (2)	IR-3 (2)
IR-4	インシデント処理	IR-4	IR-4 (1)	IR-4 (1) (4)
IR-5	インシデント監視	IR-5	IR-5	IR-5 (1)
IR-6	インシデント報告	IR-6	IR-6 (1)	IR-6 (1)
IR-7	インシデント対応支援	IR-7	IR-7 (1)	IR-7 (1)
IR-8	インシデント対応計画書	IR-8	IR-8	IR-8
MA-1	システム保守ポリシー・手順	MA-1	MA-1	MA-1
MA-2	管理保守	MA-2	MA-2	MA-2 (2)
MA-3	保守ツール	未選択	MA-3 (1) (2)	MA-3 (1) (2) (3)
MA-4	ローカル以外の保守	MA-4	MA-4 (2)	MA-4 (2) (3)
MA-5	保守要員	MA-5	MA-5	MA-5 (1)
MA-6	適時的保守	未選択	MA-6	MA-6
MP-1	メディア保護ポリシー・手順	MP-1	MP-1	MP-1
MP-2	メディアアクセス	MP-2	MP-2	MP-2
MP-3	メディアマーキング	未選択	MP-3	MP-3
MP-4	メディアストレージ	未選択	MP-4	MP-4
MP-5	メディア転送	未選択	MP-5 (4)	MP-5 (4)
MP-6	メディアサニタイズ	MP-6	MP-6	MP-6 (1) (2) (3)
MP-7	メディア利用	MP-7	MP-7 (1)	MP-7 (1)
PE-1	物理環境保護ポリシー・手順	PE-1	PE-1	PE-1
PE-2	物理的アクセス権限	PE-2	PE-2	PE-2
PE-3	物理的アクセス制御	PE-3	PE-3	PE-3 (1)
PE-4	通信メディアのアクセス制御	未選択	PE-4	PE-4
PE-5	出力デバイスのアクセス制御	未選択	PE-5	PE-5
PE-6	物理的アクセス監視	PE-6	PE-6 (1) (4)	PE-6 (1) (4)
PE-8	来訪者立入記録	PE-8	PE-8	PE-8 (1)
PE-9	電気装置及び配線	未選択	PE-9 (1)	PE-9 (1)
PE-10	緊急遮断	未選択	PE-10	PE-10
PE-11	緊急電源	PE-11 (1)	PE-11 (1)	PE-11 (1) (2)
PE-12	緊急照明	PE-12	PE-12	PE-12
PE-13	防火	PE-13	PE-13 (3)	PE-13 (1) (2) (3)
PE-14	温度・湿度制御	PE-14	PE-14	PE-14
PE-15	水害防護	PE-15	PE-15	PE-15 (1)
PE-16	配送・撤去	PE-16	PE-16	PE-16
PE-17	代替作業場	未選択	PE-17	PE-17
PE-18	情報システムコンポーネントの場所	未選択	未選択	PE-18
PL-1	セキュリティ計画ポリシー・手順	PL-1	PL-1	PL-1
PL-2	システムセキュリティ計画書	PL-2 (3)	PL-2 (3)	PL-2 (3)
PL-4	行動規則	PL-4	PL-4 (1)	PL-4 (1)
PL-7	運用セキュリティ概念		PL-7	PL-7
PL-8	情報セキュリティアーキテクチャ	未選択	PL-8	PL-8
PS-1	人員のセキュリティポリシー・手順	PS-1	PS-1	PS-1
PS-2	配置リスク指定	PS-2	PS-2	PS-2
PS-3	人選	PS-3	PS-3	PS-3
PS-4	退職	PS-4	PS-4	PS-4 (2)
PS-5	転勤	PS-5	PS-5	PS-5
PS-6	アクセス同意	PS-6	PS-6	PS-6
PS-7	サードパーティ社員セキュリティ	PS-7	PS-7	PS-7
PS-8	懲戒	PS-8	PS-8	PS-8
RA-1	リスク評価ポリシー・手順	RA-1	RA-1	RA-1
RA-2	セキュリティ分類	RA-2	RA-2	RA-2
RA-3	リスク評価	RA-3	RA-3	RA-3
RA-5	脆弱性検索	RA-5	RA-5 (1) (2) (5)	RA-5 (1) (2) (4) (5)
SA-1	システム及びサービス取得ポリシー・手順	SA-1	SA-1	SA-1
SA-2	リソース割当	SA-2	SA-2	SA-2
SA-3	システム開発ライフサイクル	SA-3	SA-3	SA-3
SA-4	取得プロセス	SA-4 (10)	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (9) (10)
SA-5	情報システム文書化	SA-5	SA-5	SA-5
SA-8	セキュリティエンジニアリング原則	未選択	SA-8	SA-8
SA-9	外部情報システムサービス	SA-9	SA-9 (2)	SA-9 (2)
SA-10	開発者設定管理	未選択	SA-10	SA-10
SA-11	開発者セキュリティ試験評価	未選択	SA-11	SA-11
SA-12	サプライチェーン保護	未選択	未選択	SA-12
SA-15	開発プロセス・規格・ツール	未選択	未選択	SA-15
SA-16	開発者による訓練	未選択	未選択	SA-16
SA-17	開発者セキュリティアーキテクチャ・設計	未選択	未選択	SA-17
SC-1	システム通信保護ポリシー・手順	SC-1	SC-1	SC-1
SC-2	アプリケーション分割	未選択	SC-2	SC-2
SC-3	セキュリティ機能隔絶	未選択	未選択	SC-3
SC-4	共有リソース内情報	未選択	SC-4	SC-4
SC-5	サービス保護妨害	SC-5	SC-5	SC-5
SC-7	境界の保護	SC-7	SC-7 (3) (4) (5) (7) (18)	SC-7 (3) (4) (5) (7) (8) (18) (21)
SC-8	通信機密性・完全性	未選択	SC-8 (1)	SC-8 (1)
SC-10	ネットワーク切断	未選択	SC-10	SC-10
SC-12	暗号鍵設定管理	SC-12	SC-12	SC-12 (1)
SC-13	暗号保護	SC-13	SC-13	SC-13
SC-15	共同コンピューティングデバイス	SC-15	SC-15	SC-15
SC-17	PKI証明書	未選択	SC-17	SC-17
SC-18	モバイルコード	未選択	SC-18	SC-18
SC-19	VoIP	未選択	SC-19	SC-19
SC-20	セキュアな名前/アドレス解決サービス（権限ソース）	SC-20	SC-20	SC-20

出典：SP 800-82 Ver.2

11. NIST SP 800-82 オーバーレイ 項目一覧（その3）

SC-21	セキュアな名前/アドレス解決サービス（再帰又はキャッシングリゾルバ）	SC-21	SC-21	SC-21
SC-22	名前/アドレス解決サービス用アーキテクチャープロビジョニング	SC-22	SC-22	SC-22
SC-23	セッション信頼性	未選択	SC-23	SC-23
SC-24	既知状態の失敗	未選択	SC-24	SC-24
SC-28	休眠情報の保護	未選択	SC-28	SC-28
SC-39	プロセス隔離	SC-39	SC-39	SC-39
SC-41	ポート及びI/Oデバイスアクセス	SC-41	SC-41	SC-41
SI-1	システム情報完全性ポリシー・手順	SI-1	SI-1	SI-1
SI-2	欠陥修正	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	悪意あるコード保護	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	情報システム監視	SI-4	SI-4 (2) (4) (5)	SI-4 (2) (4) (5)
SI-5	セキュリティ警報・勧告・指示	SI-5	SI-5	SI-5 (1)
SI-6	セキュリティ機能検証	未選択	未選択	SI-6
SI-7	ソフトウエア・ファームウエア・情報の完全性	未選択	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)
SI-8	スパム保護	未選択	SI-8 (1) (2)	SI-8 (1) (2)
SI-10	情報入力検証	未選択	SI-10	SI-10
SI-11	エラー処理	未選択	SI-11	SI-11
SI-12	情報処理保留	SI-12	SI-12	SI-12
SI-13	予想される故障の防止	未選択	未選択	SI-13
SI-14	非執拗性	未選択	未選択	未選択
SI-15	情報出力フィルタリング	未選択	未選択	未選択
SI-16	メモリ保護	未選択	SI-16	SI-16
SI-17	フェールセーフ手順	SI-17	SI-17	SI-17

◆それぞれの項目に詳細の記述がある。以下は、AC-1の例

AC-1（アクセス制御ポリシー・手順）の詳細記述の例

セキュリティのレベル（低・中・高）いずれも「選定」となっており、本項目を満足する必要がある。

AC-1　アクセス制御ポリシー・手順

管理番号	管理名 *管理拡張名*	管理ベースライン 低	中	高
AC-1	アクセス制御ポリシー・手順	選定	選定	選定

ICS 補足ガイダンス：ポリシーは特に ICS の固有の特性・要件及び ICS 以外のシステムとの関係を取り上げる。ベンダー及び保守要員による ICS へのアクセスは、機械・電気室、天井、床、変電設備、スイッチ・バルブ室、ポンプ室等、広範な施設及び地域や監視下にない空間にまたがっている。

ICSに特有な内容を記載

出典：SP 800-82 Ver.2