日本電機工業会技術資料

JEM-TR249

監視制御用計算機システムにおける セキュリティ対策のガイドライン （追補１）

Guide to information security for
supervisory control and data acquisition systems
(Amendment 1)

2011年(平成23年) 7月 12日 制定
2017年(平成29年) 7月 日 改正

一般社団法人日本電機工業会

白　　紙

目　次

ページ

まえがき

この追補は，監視制御用計算機システムWG，電力技術委員会及び標準化委員会の審議を経て，総合技術政策委員会が改正したもので，これによって，JEM-TR249：2011は改正され，一部は置き換えられた。

この追補は，著作権法で保護対象となっている著作物である。

この追補の一部が，特許権，出願公開後の特許出願，実用新案権，又は出願公開後の実用新案登録出願に抵触する可能性があることに注意を喚起する。一般社団法人日本電機工業会は，このような特許権，出願公開後の特許出願，実用新案権，又は出願公開後の実用新案登録出願にかかわる確認について，責任をもたない。

日本電機工業会技術資料は，少なくとも5 年を経過する日までに総合技術政策委員会の審議に付され，速やかに，確認，改正又は廃止されます。

日本電機工業会技術資料　　JEM-TR 249：2017

監視制御用計算機システムにおける セキュリティ対策のガイドライン （追補１）

Guide to information security for supervisory control and data acquisition systems (Amendment 1)

この追補は，JEM-TR249：2011(監視制御用計算機システムにおけるセキュリティ対策のガイドライン)(以下　技術資料という)を次のように改正する。

序文の末尾に，“また，2016年に制定された**「JESC Z0004(2016)電力制御システムセキュリティガイドライン」**とこの技術資料との関係を**附属書C**に示す。”を追加する。

箇条2(引用規格)に，次に掲げる規格を追加する。

JESC Z0004(2016)　**電力制御システムセキュリティガイドライン**

参考文献に，次に掲げる報告書を追加する。

電気協同研究　第73巻　第1号　電力系統監視制御システムの実態と展望

附属書Bの次に**附属書C**を追加する。

附属書C
（参考）
電力制御システムセキュリティガイドラインとこの技術資料との対応

JESC Z0004(2016) 電力制御システムセキュリティガイドライン(以下 ガイドラインという)の項目を，主な対応内容と関連付ける。主な対応内容には，セキュリティ技術を適用して対応する内容（技術），電気事業者が運用で対応する内容（運用），電気事業者が組織の役割を明確化することで対応する内容（組織）があり，その関連性を**表C.1**に示す。

表C.1—ガイドラインの項目と主な対応内容との関連性

ガイドライン項目	主な対応内容		
	技術	運用	組織
第1章 総則	—	—	○
第2章 組織	—	—	○
第3章 文書化	—	—	○
第4章 セキュリティ管理	—	—	○
第5章 設備・システムのセキュリティ	—	—	—
第5-1条 外部ネットワークとの分離	—	○	—
第5-2条 他ネットワークとの接続	○	○	—
第5-3条 通信のセキュリティ	○	—	—
第5-4条 機器のマルウェア対策	○	—	—
第5-5条 不正処理防止策	○	—	—
第5-6条 アクセス制御	○	—	—
第5-7,5-8条 ログの取得	○	○	—
第6章 運用・管理のセキュリティ	—	—	—
第6-1条 セキュリティ仕様の確認	—	○	—
第6-2条 機器・外部記憶媒体及びデータの管理	—	○	—
第6-3条 外部記憶媒体等のマルウェア対策	○	○	—
第6-4条 管理者権限の適切な割当	—	○	—
第6-5条 セキュリティパッチの適用	—	○	—
第6-6,6-7条 入退管理	—	○	—
第7章 セキュリティ事故の対応	—	○	○

この附属書は，ガイドラインの第5章，第6章の対策について記載するものであり，ガイドラインとこの技術資料との対応表を**表C.2**に示す。

表C.2—ガイドラインの項目とこの技術資料との対応表

ガイドライン項目			この技術資料	
項目	セキュリティ要件	対策	項目	対策
第5-1条	・外部ネットワークとの分離	外部ネットワークとの分離	7.5 c)	Demilitarized Zone(DMZ)による外部ネットワークとの分離を行う。
第5-2条	1.接続点の最小化	他ネットワークとの接続点の最小化	7.5 a)	セキュリティレベルに応じてセグメントを分けて構成する。
	2.接続点の防御	他ネットワークとの接続点に防御措置	7.3.3 7.4.2 7.5 c) 7.5 e) B.1.2 B.3	接続点にファイアウォール，Intrusion Detection System (IDS)を設置する。 DMZによる外部ネットワークとの分離を行う。
第5-3条	1.暗号化	必要に応じてデータを暗号化	7.4.4 B.5.1	必要に応じてデータを暗号化する。 ただし，処理遅延への注意及び暗号鍵の管理・更新を厳密に行う。
	2.通信プロトコル	適切な通信プロトコルの選択	7.5 b) B.5.2 B.5.3	通信路の保護及び特殊プロトコルによってセキュリティ対策を施す。
第5-4条	・機器のマルウェア対策	機器へのウィルス対策ソフトの実装	7.3.3 B.1.1	不正ソフトウェア対策ソフトを導入する。
第5-5条	1.不正プログラム防止	予め定められたプログラムだけが実行されるようにする(ホワイトリスト)	（現在は記載なし）[a)]	
	2.不正処理防止	誤ったコマンドが発行されない仕組み コマンド発行者の権限の最小化	7.5 f)	正しい操作者及び装置の識別・認証，ユーザの入退室管理によって実施する。ただし，入退室管理はこの技術資料の対象外。
第5-6条	1.接続制御	予め許可された機器以外の接続を許可しない	7.4.2	不必要なポートのブロック，ファイアウォールによって通信するプロトコル種別を最小にする。
	2.認証	通信相手が予め許可された機器であることを確認する仕組み	7.5 f)	正しい操作者及び装置の識別・認証，ユーザの入退室管理によって実施する。
	3.ネットワーク分割	利用目的などに応じてネットワークを分割	7.5 a)	セキュリティレベルに応じてセグメントを分けて構成する。

表C.2—ガイドラインの項目とこの技術資料との対応表（続き）

ガイドライン			この技術資料	
項目	セキュリティ要件	対策	項目	対策
第5-7条 第5-8条	・ログの取得	不正侵入や内部不正を把握するためのログを取得	7.3.5 7.4.3 7.5 h) B.4	ログ管理及びインシデント監視を実施する。
第6-1条	1.セキュリティ仕様	システムの調達時にセキュリティ仕様を明確にする	（技術資料対象外）[b)]	
	2.準拠性の確認	システムがセキュリティ仕様通りに設計、製造されていることを確認する	（技術資料対象外）[b)]	
	3.仕様変更	セキュリティに影響を与える可能性がある変更を管理する	7.3.2	ソフトウェア，並びに各種パラメータに関する全ての変更及び更新は，正式な手順で実行し，記録する。
第6-2条	1.機器・外部記憶媒体の管理	機器・外部記憶媒体の構成情報・利用状況の管理	7.3.4 7.5 g)	可搬形メディアについては，USBポートを使用不可に設定するか，又は安全なメディアを識別して，管理を行う。
	2.データの管理	制御に関連するデータを管理し、保護する	7.4.1 7.4.2 7.4.3 7.4.4 7.5 b) B.4 c)	識別・認証，アクセス制御，データの暗号化，通信路の保護を行う。ログ管理及びインシデント監視を実施する。
第6-3条	・外部記憶媒体等の取扱い	接続する外部記憶媒体についてウィルスチェックを行う	7.3.4	安全なメディアを識別し管理を行う。

表C.2—ガイドラインの項目とこの技術資料との対応表（続き）

ガイドライン			この技術資料	
項目	セキュリティ要件	対策	項目	対策
第6-4条	・管理者権限の適切な割当て	a)誰がその管理者権限を利用して業務を遂行したかを確認及び記録する仕組み	7.3.5 7.4.3 7.5 h) B.4	ログ管理及びインシデント監視を実施する。
		b)管理者権限を悪用した不正行為がないことを確認する仕組み		
		c)管理者権限の割当て状況を定期的に確認	（技術資料対象外）[c]	
第6-5条	・セキュリティパッチの適用	セキュリティパッチを適用するか、代替策を適用する	7.3 7.3.3	パッチを適用する場合には，可能な限り最新のものを適用する。パッチの適用によるその他のソフトウェアへの影響を適切に評価・検証する。
第6-6条 第6-7条	1.セキュリティ区画	物理的なセキュリティ区画を設定する	（技術資料対象外）[c]	
	2.アクセス管理	セキュリティ区画には許可されたものだけがアクセスできるようにする	（技術資料対象外）[c]	

注[a] 運転人員は教育又は審査を受けて選任されているため，悪意（内部犯行など）・誤操作はないものとしている。また，外部からの侵入対策に対しては，多層防御によって防ぐことを前提としている。

注[b] 発注・検収処理等のユーザ側の管理に関する事項は，対象外としている。

注[c] 建屋を含めたアクセス管理の問題，人事管理の問題，教育の問題などの使用者側の管理に関する事項は，対象外としている。

JEM-TR249：2017

監視制御用計算機システムにおける セキュリティ対策のガイドライン（追補１）

解説

この解説は，本体及び附属書に規定・記載した事柄，並びにこれらに関連した事柄を説明するもので，規格の一部ではない。

1　主な改正点

主な改正点は，次のとおりである。

2016年に制定された「JESC Z0004(2016) 電力制御セキュリティガイドライン」とこの技術資料との関係を附属書Cに示した。

2　懸案事項

今回の改正に当たって懸案事項として残された事項を，次に記す。

・JESC Z0004(2016)に記載があり，技術資料に記載がない項目を検討し追記する。
・セキュリティ認証基準（IEC 62443）における技術資料が目指すレベルを明確化する。
・技術資料では入口を防御することに主眼を置いているが，マルウェアがシステムに侵入された後の対策を記載する。
・最新の標準化動向，技術動向を調査し，附属書A，Bを見直す。