JAMA・JAPIA

自工会/部工会・サイバーセキュリティガイドライン
工場領域版

自動車産業における工場領域の
サイバーセキュリティ対策の一層の進展のために

0.9 版

2025 年 10 月 17 日

Japan Automobile Manufacturers Association, Inc.

一般社団法人　日本自動車工業会
総合政策委員会
ICT 部会
サイバーセキュリティ分科会

Japan Auto Parts Industries Association

一般社団法人　日本自動車部品工業会
総合技術委員会
DX 対応委員会
サイバーセキュリティ部会

改訂履歴

版数	発行日	改訂内容
第 0.9 版	2025 年 10 月 17 日	初版発行

目次

1. 背景 3
2. 目的と主な活用方法 4
3. 本ガイドラインの対象 5
4. ガイドラインの構成 7
5. その他の活用方法 8
6. 要求事項と達成条件 9
7. 用語集 ２６
あとがき ３０

1. 背景

自動車産業においても増加しているサイバー攻撃の脅威に対応することを目的に、エンタープライズ領域（会社全体のＯＡ環境）を対象とした「自工会/部工会・サイバーセキュリティガイドライン」（エンタープライズ版）を作成した。近年 OA 環境に加えて、工場内の製造設備をはじめとする一部特有の要件を考慮する必要がある OT[1] 環境におけるサイバーセキュリティリスクも高まっている。

自動車は、部品・ソフトウェア等の様々な構成要素を組み合わせて製造されるため、自動車メーカーだけでなく、サプライチェーンを構成する各社の工場に対するサイバー攻撃も懸念される。

このような OT 環境におけるサイバーセキュリティリスクの変化に対応するため、制御システムのセキュリティに関する国際基準である「IEC 62443」などが整理されている。また、経済産業省は「工場システムにおけるサイバー・フィジカル・セキュリティガイドライン」を公表し、工場システムのセキュリティ向上を図っている。

これらの背景を踏まえ、自動車産業における製造設備特有の要件を考慮し、製造設備に対するパッチ適用やインシデント対応体制など、エンタープライズ版とは異なる対策が必要な OT 環境を対象とした業界共通の自己評価基準を明示することで、自動車産業全体の OT 環境のサイバーセキュリティ対策のレベルアップや対策状況の効率的な点検を推進することを目的に、本ガイドライン（工場領域版）を作成した。

[1] OT(Operational Technology)とは、工場などに使われる物理的なシステムや設備を最適に動かすための制御・運用技術の総称。

2. 目的と主な活用方法

本ガイドラインの目的は、自動車産業のサプライチェーンを支えるすべての企業の安全な生産を維持するために、OT 環境のセキュリティ対策を強化することである。

そのため、**本ガイドラインとチェックシートを活用して工場におけるセキュリティ対応部門などが自社の OT 環境のセキュリティ対策状況を自己評価いただくことを主に想定している**。自己評価を通じて、OT 環境において実施すべき基本的なセキュリティ対策に抜け漏れがないかを定期的に確認いただきたい。自己評価は、各社の状況に応じて工場単位もしくはライン単位で実施いただくことを想定している。このような定期的（年 1 回以上）な自己評価を通して、自社の OT 環境のセキュリティ対策の強化に役立てていただきたい。

また、本ガイドラインのチェックシートは自己評価を目的としており、評価基準を以下のとおりに設定している。本チェックシートでは、各評価項目に関して社内・工場内などにおいて検討しているかが確認ポイントとなる。自己評価を通して自社でのセキュリティ対策の検討状況を整理・把握いただきたい。

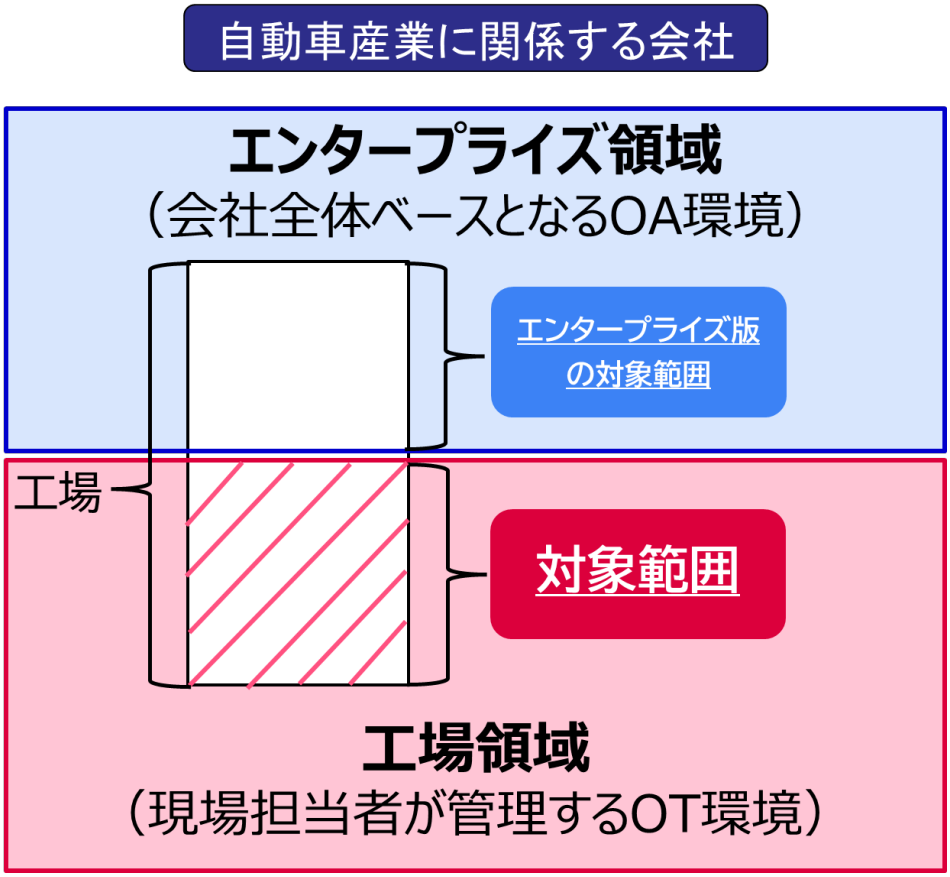
本目的を踏まえて、具体的には以下の通りに評価基準を設定している。「□」、「△」、「×」に関してはリスクが残存する項目になるため、定期的（年 1 回以上）な自己評価の際に見直しを行っていただきたい。「□」の項目については、見直しの際に見送りの理由がその時点でもなお妥当であるか、実施準備がどの程度進捗しているかなどを確認していただきたい。「△」、「×」については、見直しの際に項目に関する社内での検討状況を確認いただきたい。

- ○：項目の対策を検討した結果、実施済み（代替策の実施も含む）
- □：項目の対策を検討した結果、実施見送り・実施準備中
  （対策未実施のリスクの許容なども含む）
- △：項目の対策の実施有無を検討中
- ×：項目の対策の実施有無を未検討
- ー：項目の対策の対象となる設備・機器・サービス等がない

また、**本ガイドラインとエンタープライズ版は対象領域が違うため、本ガイドラインのチェックシートは、エンタープライズ版のチェックシートの結果に影響することはない。**

3. 本ガイドラインの対象

本ガイドラインは、エンタープライズ版が対象としている会社全体ベースとなるOA環境と異なり、工場などの現場担当者が管理するOT環境を対象としている。以下に工場領域のチェックシートの範囲を示す。また、エンタープライズ版と工場領域版の違いを表で示す。

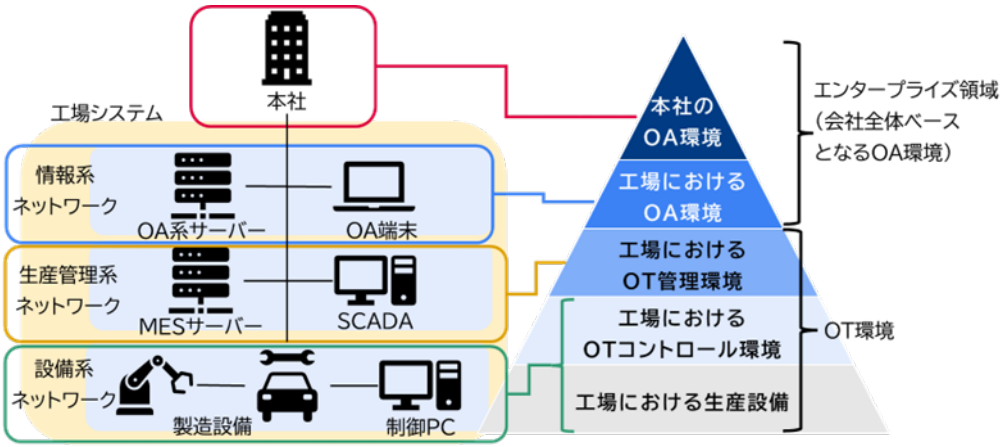


＜図:「自工会/部工会・サイバーセキュリティガイドライン 工場領域版」の対象領域＞

＜表：エンタープライズ版・工場領域版の対象範囲の違い＞

場所 / 環境	工場以外	工場
OA環境	エンタープライズ版	エンタープライズ版
OT環境	―	工場領域版

一般的な OT 環境の対象範囲の一例を以下に示す。これはあくまでも一例であり、各社は自社の OT 環境の定義に基づいて対象範囲を明確にする必要がある。



＜図：OT 環境の一例＞

上記定義を踏まえ、本ガイドラインの想定読者は、製造設備を持つ自動車産業に関係する企業を対象とし、各社における OT 環境のセキュリティ業務関与者としている。

- CISO （最高情報セキュリティ責任者）
- リスク管理部門
- 監査部門
- 工場におけるセキュリティ対応部門
- 工場の情報システムの開発/運用部門
- 工場の制御システムの開発/運用部門
- 工場におけるデータマネジメント部門
- 工場におけるサプライチェーンの管理責任を負う購買や調達部門
- その他のセキュリティに関わる部門（人事・法務・総務）

4. ガイドラインの構成

本ガイドラインは、自動車産業のサプライチェーンにおける OT 環境のセキュリティ向上を優先課題と捉え、企業の規模に関わらず中小企業を含めたすべての企業が活用できるよう OT 環境で実施すべき重要項目を整理した。

また、達成状況の確認に使用するチェックシートを付録として添付している。

・ガイドライン（本紙）
ガイドライン制定の背景と目的を明らかにし、ガイドラインの対象範囲、構成、活用方法、要求事項・達成条件、用語集を記載

・付録：チェックシート
要求事項・達成条件の確認に使用するチェックシート

5. その他の活用方法

2章にも記載した通り本ガイドラインにより、**自動車産業のサプライチェーンを支えるすべての企業において、OT環境において実施すべき基本的なセキュリティ対策に抜け漏れがないか定期的（年1回以上を推奨）または必要に応じて確認し、自社のセキュリティ向上のために活用することを、業界全体で推進していきたい。**

上記の主な活用方法以外にも以下のような活用方法を想定している。

＜想定活用方法＞

(1) 企業におけるOT環境でのセキュリティポリシー策定及び対策実装
添付チェックシートにおいて示された要求事項及び達成基準を参考にして、自社のOT環境に関するセキュリティポリシー策定及びセキュリティ対策の実装に取組むことができる。

(2) 企業におけるセキュリティ教育・訓練・啓発活動への活用
本ガイドラインを通じ、自社のOT環境のセキュリティに関する教育・訓練、啓発活動に活用することができる。

＜担当領域情報の追加＞

自社内で自己評価を担当する方が不明確な場合に、担当者を決めるための参考情報として、担当領域名(機能)を対策項目毎に追加した。評価者を決定される際に参考とていただきたい。

6. 要求事項と達成条件

ラベル	目的	要求事項	No.	達成条件	達成基準
1 体制 (平時)	情報/OT セキュリティに関する体制及び役割を明確化し、 保護すべきデータの漏洩・サイバーセキュリティ対策の徹底、強化を図る	平時の情報/OT セキュリティリスクを管理する体制を整備し、事故発生に至らないよう、情報収集と共有を行うこと	1	工場や生産技術内の情報/OT セキュリティ部門責任者を含む、平時の体制と責任と役割を部や課レベルまで明確化している	【規則】 ・情報/OT セキュリティリスクは、経営に重大な影響を及ぼすことを理解し、組織的に経営判断できる体制を設置していること
			2	定期的、または必要に応じて、平時の体制を工場や生産技術の部や課レベルまで見直ししている	【頻度】 ・1 回／年、もしくは、重大な情報/OT セキュリティ事件・事故が発生した場合 ・または、社内組織改正等にて、お客様情報をはじめとした各種情報の保護・管理部署や責任者に変更が生じた時
			3	製造設備・機器やそのネットワークに関するサイバー攻撃や情報漏えいの新たな手口を知り、対策を工場や生産技術の部署へ共有している	【規則】 ・平時の体制に則り、情報/OT セキュリティ事件・事故事例やその対応策を社内部署へ共有していること 【対象】 ・役員、工場長以下管理者、従業員、社外要員（派遣社員等） 【頻度】 ・1 回／年、もしくは、社内外で重大な情報/OT セキュリティ事件・事故が発生した時

ラベル	目的	要求事項	No.	達成条件	達成基準
2 体制(事故時)	情報/OT セキュリティに関する体制及び役割を明確化し、事件・事故の発生時に、被害を限定的なものに抑えて最小化し、できるだけ速やかに元の状態へと復旧する	情報/OT セキュリティ事件・事故発生時の対応体制とその責任者を明確にしていること	4	情報/OT セキュリティ事件・事故発生時の対応体制と責任と役割を工場や生産技術の部や課レベルまで明確化している	【規則】 ・情報/OT セキュリティを統括する役員（CISO、工場長等)や情報/OT セキュリティ担当部署の役割・責任が明確化されていること ・情報/OT セキュリティ事件・事故の基準や社内外組織との連絡先、ルートが明確化されていること
			5	工場や生産技術で発生した発生した情報/OT セキュリティ事件・事故対応が実施され、事故の概要や影響および対応内容の記録がある	【規則】 ・情報/OT セキュリティ事件・事故の報告フォーマットが整備されていること
			6	定期的、または必要に応じて、事故時の体制を工場や生産技術の部や課レベルまで見直ししている	【頻度】 ・1 回／年、もしくは、重大な情報/OT セキュリティ事件・事故が発生した場合等
3 事故時の手順	同上	情報/OT セキュリティ事件・事故発生後に早期に対処する手順が明確になっていること	7	工場や生産技術で発生した情報/OT セキュリティ事件・事故時の対応手順(初動、システム復旧等)を定めている	【規則】 ・対応手順には組織の必要に応じて下記の手順を含んでいること ①発見報告、　②初動(ネットワークからの切り離し等の被害抑制の対応を含む)、③調査・対応、④復旧、⑤真因追及、⑥最終報告 工場領域においては、生産中の製品の存在及び安全や環境を考慮した上で、上記を定めること

ラベル	目的	要求事項	No.	達成条件	達成基準
4 日常の教育	マルウェアや機密情報についてリスクや正しい取り扱いを理解させ、情報/OT セキュリティ事件・事故を予防する	従業員として注意することを教育していること	8	工場や生産技術の各部署の情報/OT セキュリティ管理者に対して、組織内での対策とマネジメント手法に関する教育を実施している	【規則】 ・組織内での対策とマネジメント手法に関する教育を実施すること ・教育内容を振返り、次回の教育内容を改善すること 【対象】 ・各部署の情報/OT セキュリティ管理者または推進者 ※情報/OT セキュリティ管理者が任命されてない場合は部門長 【頻度】 ・1 回以上／年
			9	工場や生産技術の管理者が情報/OT セキュリティに関する役割と責任を理解するための機会を設けている	【規則】 ・経営層が役割と責任を理解するための説明の場を設けている ・説明内容を振返り、次回の説明内容を改善すること 【対象】 ・工場長以下管理者 【頻度】 ・1 回以上／年 LV2 では対象範囲を役員クラスまで広げる
			10	工場や生産技術独自に啓発活動を実施している	【規則】 ・工場固有の情報/OT セキュリティの重要性を再認識する機会を設けること 【対象】 ・工場長以下管理者、従業員、社外要員（派遣社員等） 【頻度】 ・1 回以上／年
			11	工場や生産技術で特に重要なリスクやルールについて啓発活動を実施している	【規則】 ・各社が定める活動単位（部・室など）で特に重要なルールやリスクについてリマインドすること ・啓発内容を振返り、次回の啓発内容を改善すること ・工場領域版のガイドライン・チェックシートを活用する 【対象】 ・職場特有のリスクの理解、ルールの遵守が重要な従業員、社外要員（派遣社員等） 【頻度】 ・1 回以上／1 年

ラベル	目的	要求事項	No.	達成条件	達成基準
	情報/OT セキュリティ事件・事故に迅速かつ適切に対応できるように事前に備え、事故発生時の被害拡大の防止・迅速な復旧を図る	自組織内あるいは組織を跨いで影響する情報/OT セキュリティ事件・事故の発生と影響を抑制する教育・訓練を行っていること	12	工場や生産技術で発生した情報/OT セキュリティ事件・事故発生時の対応について教育・訓練を実施している	【規則】 ・情報/OT セキュリティ事件・事故発生時の対応について、教育資料配布・掲示、e ラーニング、集合教育等による教育や訓練を実施すること 【対象】 ・役員、工場長以下管理者、従業員、社外要員（派遣社員等） 【頻度】 ・新規受け入れ時、かつ、1 回／年以上
			13	工場や生産技術独自に教育・訓練の内容を必要に応じて見直ししている	【頻度】 ・教育・訓練実施前後、もしくは 1 回／年以上

ラベル	目的	要求事項	No.	達成条件	達成基準
5 アクセス権	アクセス権設定の不備に起因した、機密エリアやシステムへの不正アクセスを防止する	アクセス権(入室権限やシステムのアクセス権)を適切に管理していること	14	人の異動に伴うアクセス権(入室権限やシステムのアクセス権)の管理ルールを定めている	【規則】 ・重要な製造設備・機器については、以下の内容等を含む管理ルールを定めること ・アクセス権の発行・変更・削除は申請・承認制であること ・与える入室許可・アクセス権の範囲は必要な範囲に限定すること ・入室権限やアクセス権の棚卸について定めていること ・与えた入室許可・アクセス権の申請書または台帳を管理していること 【対象】 ・業務で利用するシステムおよびPCログオン時のユーザーID ・機密上の配慮が必要な場所や部屋
			15	人の異動に伴うアクセス権(入室権限やシステムのアクセス権)の管理ルールを定めている	【規則】 ・重要な製造設備・機器については、アクセス権を付与するための条件を明確にする ・アクセス権の設定は、システム管理者の要件および設定手順を明確にし、厳格な管理下で実施する。 ・重要な製造設備・機器については、情報利用者とシステム管理者の権限を分離するなど、個人に権限が集中しない環境とする。 ・重要な製造設備・機器については、その運用／利用状況を監視する。
			16	管理ルールに沿ってアクセス権の発行、変更、無効化、削除を実施している	【規則】 No49／50に定義した管理ルールの遵守状況の点検を行っていること
			17	アクセス権の棚卸を定期的、または必要に応じて実施している	【規則】 No49／50により定めたルールに従い、アクセス権の棚卸を定期的、または必要に応じて実施していること
			18	アクセスログは、安全に保管しアクセス制御された状態で管理されている	【規則】 ・法規制等により要求される事項を満たす事ができるよう、適切な期間のログを保持する。 ・ログを脅威から保護するため、ログを保存するモノ、システムにアクセス制御等を適用すること 【対象】 ・重要な製造設備・機器

ラベル	目的	要求事項	No.	達成条件	達成基準
6 情報資産の管理（情報）	情報資産を適切に管理し、機密情報の漏洩を防止する	情報資産の機密区分を設定・把握し、その機密区分に応じて情報を管理していること	19	機密区分に応じた情報の管理ルールを定めている	【規則】 ・以下の内容等を含む管理ルールを定めること ・機密の特定 ・機密区分のレベル判定と表示 ・区分に応じた取り扱い方法 ・取り扱いエリアの区分及び制限 ・保管期間（エンタープライズと合わせる） 【対象】 ・情報資産（情報） ・有形機密情報（非公表の試作品など）
			20	機密区分に応じた情報の管理ルールを定期的、または必要に応じて見直ししている	【規則】 ・管理ルールの内容を確認し、必要に応じて改善すること 【頻度】 ・1 回以上 ／年
			21	高い機密区分の情報資産(情報)・有形機密情報（非公表の試作品など）を一覧化している	【規則】 一覧には、対象情報・有形機密情報（非公表の試作品など)、管理者名、部署名、保管場所、保管期限、開示先、連絡先などを含むこと 【対象情報】 No.54 で定めた機密区分のうち、高レベルの機密に該当する情報資産・有形機密情報（非公表の試作品など）
			22	高い機密区分の情報資産(情報)・有形機密情報（非公表の試作品など）の一覧化を定期的、または必要に応じて見直ししている	【規則】 ・一覧表の内容を確認し、必要に応じて是正すること 【頻度】 ・1 回以上 ／年
			23	情報資産(情報)・有形機密情報（非公表の試作品など）は機密区分に応じた管理ルールに沿って管理している	【規則】 No.54 に定義した管理ルールの遵守状況の点検を行い、不備・違反があれば是正を行うこと 【頻度】 1 回/年 以上

ラベル	目的	要求事項	No.	達成条件	達成基準
7 情報資産の管理(機器)	IT 資産を適切に管理し、情報/OT セキュリティ事件・事故につながるリスクを減ずるとともに、情報/OT セキュリティ事故発生時の対応を迅速化する	会社が保有する情報機器及び機器を構成する OS やソフトウェアの情報(バージョン情報、管理者、管理部門、設置場所等)を適切に管理していること	24	重要度に応じた製造設備の情報機器、OS、ソフトウェアの管理ルールを定めている	【規則】 製造設備・機器の重要度に応じて、導入、設置、ネットワーク接続、OS、セキュリティパッチ適用、導入設備メーカー等のルールを含む管理ルールを定めていること
			25	重要度に応じた製造設備の情報機器、OS、ソフトウェアの情報(バージョン情報、管理者、管理部門、設置場所等)について、一覧を作成している	【規則】 ・製造設備・機器の重要度に応じて、バージョン情報、管理者、管理部門、設置場所等の管理項目を含む情報機器、OS の一覧を作成すること
			26	重要度に応じた製造設備の情報機器、OS、ソフトウェアの情報(バージョン情報、管理者、管理部門、設置場所等)の一覧を定期的、または必要に応じて、見直ししている	【頻度】 ・1 回/年 以上
			27	重要度に応じた製造設備の情報資産(機器)は重要度に応じた管理ルールに沿って管理している	【規則】 No59＆60 に定義した管理ルールに沿って管理を実施すること。不備・違反があれば是正を行うこと 【頻度】 1 回/年 以上
			28	廃棄時(リース終了時含む)は、記憶媒体のデータを消去している	【規則】 ・情報資産(機器)の廃棄時(リース終了時含む)はデータを復元できないよう消去すること ・情報資産(機器)の記憶領域の消去を実施した記録または業者の廃棄証明書を保管すること ※ディスクのフォーマットは、データを復旧される可能性があるため不可 【対象】 -製造設備・機器の情報資産(機器)のサーバー、PC、外部記憶媒体

ラベル	目的	要求事項	No.	達成条件	達成基準
8 リスク対応	情報資産のセキュリティリスクを特定し、会社として組織的な対策を行うことにより、業務影響を極小化する	自組織内(自組織の業務：業務委託も含めて)の情報/OT セキュリティリスクに対する対策を行っていること	29	情報資産において 「機密性」「完全性」「可用性」の 3 要素が確保できなくなった場合のリスクを特定できている	【規則】 対象の情報資産に情報/OT セキュリティ事件・事故が発生した時の業務影響を影響範囲や発生頻度を踏まえ把握すること 【対象】 No56&60 で特定した情報資産 【観点】 -外部の脅威 -自社の脆弱性 ※必要に応じて、パートナー企業起因の脅威、脆弱性を考慮すること -情報資産の価値 【方法】 -対象の情報、情報システムを定めること -各観点の評価規則、およびそれらを考慮したリスクレベルの規則を定めること -各情報、情報システムについて、各観点の評価からリスクレベルを決定すること 【頻度】 重要な情報資産を見直した時、または、1 回／年 以上
			30	必要に応じて経営層へ業務影響及び対策を報告し、セキュリティ業務に関与している社内部署と共有している	【規則】 №66 で把握した業務影響に対する対策方法及び計画を策定し、報告・共有すること 報告に際し役員からの指示があった場合、これを関係部門へ共有すること 【対象】 情報/OT セキュリティの総括責任者、関係部門 【頻度】 1 回／年 以上
			31	業務影響への対策は策定された計画に沿って管理している	【規則】 №68 で作成された対策及び計画が適切に実施され、業務影響の低減がされていることを確認し、発見された不備の是正などを実施すること 【対象】 情報資産の業務影響 【頻度】 1 回／年 以上

ラベル	目的	要求事項	No.	達成条件	達成基準
9 取引内容・手段の把握	どの取引先とどのような情報資産をどのような手段でやり取りするかを明確にし、取引を通じた情報漏えい等を防止する	取引先毎に、取引で取り交わされる情報資産と、取引に利用している手段を把握していること	32	会社毎に取り交わす情報・手段(受発注の手段等、情報のやり取り)を一覧化している	【規則】 一覧表には取引に伴い授受／使用される 情報資産とその取り扱いを記載し、取引先と相互に把握すること 【対象】 重要な製造設備・機器の情報資産（№54&59 で定められた機密レベルが高い情報資産など）を共有する取引先 【頻度】 取引開始時／取り交わす情報・手段の変更時
10 外部への接続状況の把握	外部情報システム利用における安全性と信頼性の確保、および情報/OT セキュリティ事件・事故発生時の迅速な対応を図る	関係組織（サプライヤー等含む）との関係において、自組織の通信ネットワーク構成を把握し、他組織との連携状態やデータの流れを監視すること	33	工場内のネットワーク図を作成し、現場ですぐに活用できる状態にある	【基準】 ・ネットワーク図を作成すること ［対象範囲］ -工場領域の自社の情報機器が存在するネットワーク ［見直し頻度］ -1 回/年以上 ・現場で活用できるようになっていること
			34	ネットワーク図・データフロー図は、定期的、 または必要に応じて、見直ししている	【頻度】 ・1 回/年以上

ラベル	目的	要求事項	No.	達成条件	達成基準
		外部情報システム(顧客・子会社・関係会社・外部委託先・クラウドサービス・外部情報サービス等)を明確にし、利用状況を適切に管理していること	35	製造設備・機器の情報資産が接続する場合の外部情報システムの利用ルールを定めている（外部情報システムにはリモートメンテも含まれる）	【規則】 ・以下の内容を含む利用ルールを定めること ・外部情報システムとの接続判定可否ルールを含む ・外部情報システムの接続先と守秘義務契約を締結する ・外部の情報サービスを利用する際のセキュリティ要件を定めている ・外部の情報サービスの利用時にセキュリティ要件を満たしているかサービス内容を確認し、承認した証跡を保管している
			36	利用している外部情報システムを一覧化している	【規則】 ・外部情報システムの一覧を作成していること
			37	外部情報システムの一覧を定期的、または必要に応じて見直ししている	【規則】 ・定期的に棚卸を実施するとともに、新規あるいは利用中止するものを一覧に反映すること 【頻度】 ・1回／年以上、かつ、新規開始あるいは利用中止時
11 社内接続ルール	社内ネットワークの利用を適切に管理することにより、情報漏えいやマルウェア感染などの被害を最小化する	社内ネットワークへの接続時には、情報システム・情報機器の不正利用を抑制する対策を行っていること	38	製造設備・機器の情報機器の工場ネットワークへの接続ルールを定めている	製造設備・機器の情報機器（PC、サーバー、等）の接続ルール 【規則】 ・工場ネットワークへの接続に関するルールを定めること 【対象】 ・工場ネットワークに直接接続するすべての機器 ・会社標準機器、社外からの持ち込み機器含む ・社外から工場ネットワークへ接続するための追加ルール 【規則】 ・リモートアクセスを利用する場合のルールを定めること 【対象】 ・社外から公衆インターネット経由あるいは専用線経由で工場社内ネットワークに接続する全ての機器

ラベル	目的	要求事項	No.	達成条件	達成基準
12 物理セキュリティ	サーバー等の重要機器への不正操作による情報漏洩、改ざん、システム停止を防ぐ	サーバー等の設置エリアには、物理的セキュリティ対策を行っていること	39	重要な製造設備・機器設置エリアは、入場可能な人を定めている	【規則】 ・重要な製造設備・機器設置エリアに入場可能な人を定めること
			40	重要な製造設備・機器設置エリアは、施錠等で入場を制限している	【規則】 ・重要な製造設備・機器設置エリアを施錠すること ・施錠が出来ないエリアに重要な製造設備・機器が設置されている場合、重要な製造設備・機器を専用ケースに入れて施錠すること ・管理者を定めて、施錠管理を行うこと
		脆弱性が発見された際の対策対象の把握や外部記憶媒体を用いた情報漏えい等を抑制する対策がおこなえていること	41	設備・機器、生産用 PC の構成・設定ルールを定め、構成・設定ルールに変更がある場合は承認を経て変更している	【規則】 ・設備・機器、生産用 PC の構成(ソフトウェアとバージョン)の変更は承認制にすること ［対象］ -設備・機器、生産用 PC の OS、オフィスソフト、ブラウザ、ウイルス対策ソフト、PLC 等のプログラムやパラメータ
			42	設備・機器、PC で利用を許可または禁止するソフトウェアを定め、ソフトウェアの無断インストールを禁止し、違反がないか定期的に確認している	【規則】 ・社内で利用許可または禁止するソフトウェアの一覧を作成し周知すること ・ソフトウェアの無断インストールを制限すること ・定期的にソフトウェアのインストール状況を確認すること ※システムでインストール制限している場合は確認不要 ［対象］ -設備・機器、クライアント PC ［制限すべきソフトウェアの例］ -情報漏えいにつながるソフトウェア -深刻な脆弱性があるソフトウェア -マルウェア・スパイウェアの疑惑のあるアプリ ［確認頻度］ -1 回/年 ［周知対象］ -役員、従業員、派遣社員、受入出向者

ラベル	目的	要求事項	No.	達成条件	達成基準
		重要情報を格納・利用するシステムにおいて、人為的設定ミスによる被害を最小化する対策を実施していること	43	サーバーや IoT 機器の不要な機能を無効化している デフォルトユーザーID の利用の停止をしている デフォルトパスワードの変更をしている	【規則】 ・不要サービス、デーモンを無効化すること ・デフォルトユーザーID の利用を停止すること ・デフォルトパスワードの変更すること
13 通信制御		サイバー攻撃、内部情報漏えいを防止するため、情報システム・情報機器や不正な Web サイトへの通信制御を行っていること	44	インターネットと社内ネットワークとの境界にファイアウォールを設置し、通信を制限している（ローカルブレイクアウトやリモートメンテナンス環境を含む）	【規則】 ・社内と社外のネットワーク通信を制限する仕組みを導入すること ［導入場所］ -社内外ネットワークの境界（ローカルブレイクアウト、リモート保守） ［制限する項目］ -接続元および接続先の IP アドレス -通信ポート
			45	ファイアウォールのフィルタリング設定(通信の許可・遮断設定)を記録し、不要な設定がないか定期的に確認している	【規則】 ・社内外ネットワーク通信のフィルタリング設定を記録すること ・定期的に不要なフィルタリング設定がないか確認すること ・不要なフィルタリング設定を削除すること 【記録する項目】 ・申請者、接続元および接続先の IP アドレス、通信方向、プロトコル、ポート番号、利用用途、登録日、有効期限 【確認頻度】 ・1 回/年
			46	リモートアクセスの ID を管理し、不要な ID がないか定期的に確認している	【規則】 ・リモートアクセスの ID の発行・変更・削除は申請・承認制にすること ・定期的に不要な ID がないか確認すること ・不要な ID を削除すること 【確認頻度】 ・1 回/年

ラベル	目的	要求事項	No.	達成条件	達成基準
			47	各社のリスク判断に基づき OA、工場ネットワークを分離している。	【規則】 ・業務内容やデータ重要性でシステムを分類し、専用のネットワーク毎に設置すること 【対象】 ・工場ネットワーク／OA ネットワーク等
			48	インターネット経由の通信が盗聴、改ざんされないよう、通信を暗号化している	【規則】 ・社内外ネットワーク通信を暗号化すること 【対象】 ・社外から社内へのリモートアクセス通信 ・ユーザーと社外公開サーバーとの間で認証を伴う通信
			49	端末と無線 LAN アクセスポイントの間の通信を暗号化している	【規則】 ・端末とアクセスポイントの間の通信を暗号化すること ・政府推奨暗号において危殆化している暗号技術は利用しないこと 【対象】 ・社内無線 LAN

ラベル	目的	要求事項	No.	達成条件	達成基準
14 認証・認可	情報システムの不正利用や、情報システムの不正操作・変更を防ぐことで、情報漏洩、改ざんを防ぐとともに、情報システムを安定稼働させる。さらに、情報漏えい、改ざんや情報システム停止の際の原因調査を可能にする	情報システム・情報機器への認証・認可の対策を行っていること	50	ユーザーID を個人毎に割り当てている	【規則】 ・ユーザーID を共有しないこと ・やむを得ず共有 ID が必要な場合は、共有 ID を利用するユーザを限定する、もしくは利用したユーザーを特定できるようにすること ・資産の重要度に応じて、重要度の高い生産システム・生産設備は共有 ID ではなく、個別のユーザ ID を設定すること 【対象】 ・業務で利用するシステムおよびパソコンログオン時のユーザーID
			51	パスワード設定に関するルールを定め、周知している	【規則】 ・桁数・組み合わせ文字・有効期限を定めること ・英字や数字の連続など容易に推測されるものを避けること ・パスワードの漏えいが判明した場合は、パスワードを変更すること ・初回登録時、工場出荷時に設定された初期パスワードを変更すること ・パスワードは強度を確保および機密性を確保すること （資産にメモを張り付ける等をしないこと） 【対象】 ・業務で利用するシステムおよびパソコンログオン時のパスワード 【周知対象】 -役員、従業員、派遣社員、受入出向者
			52	重要システムではセッションタイムアウトを実装している	【規則】 ・重要システムではセッションタイムアウトを実装すること 【対象】 ・社外公開システム、重要な社内システム ※社外公開しているシステムのみ対象とする

ラベル	目的	要求事項	No.	達成条件	達成基準
15 パッチやアップデート適用	不正アクセスやマルウェア感染のリスクを低減する	サポート期限が切れた機器、OS、ソフトウェアを利用しないようにしていること	53	サポート期限が切れた OS、ソフトウェアを利用しないようにしている	【規則】 ・サポートのある OS、ソフトウェアを利用すること ・やむを得ずサポート切れの OS、ソフトウェアを利用する場合は、できる限り脆弱性悪用のリスクを低減すること 【対象】 ・会社支給のパソコンの OS、ブラウザ、Office ソフト ・サーバーの OS、ミドルウェア ・会社支給のスマートデバイスの OS、アプリ ・インターネットとの境界に設置されているネットワーク機器の OS、ファームウェア
		脆弱性を利用した不正アクセスを防止する施策を実施していること	54	情報システム・情報機器、ソフトウェアへセキュリティパッチやアップデート適用を適切に行っている	【規則】 ・セキュリティパッチやアップデート適用を、規則と期限を定め実施すること ・やむを得ず適用できない場合は、適用対象外の理由を記録すること ・セキュリティパッチやアップデート適用に関して、適用できない場合の代替策も含め基準と適用タイミングを定めること 【対象】 ・パソコン、スマホ、タブレット、サーバー、ネットワーク機器、ソフトウェア等 -会社支給のクライアント PC の OS、ブラウザ、Office ソフト -サーバーの OS、ミドルウェア -会社支給のスマートデバイスの OS、アプリ -インターネットとの境界に設置されているネットワーク機器の OS、ファームウェア パソコン（生産設備のメンテナンス PC を含む)、サーバ等
			55	脆弱性の管理体制、管理プロセスを定めている	【規則】 ・脆弱性情報の収集から対応まで担当部署の役割・責任を明確化すること ・脆弱性情報/脅威情報を収集する情報源、ツール、頻度を定めること ・収集した情報の対応要否判断基準・対応手順を定めること ・対応履歴を記録し、月次でチェックすること
			56	外部から受け取ったデータが安全であることを確認している	【規則】 ・ウイルス対策ソフトのリアルタイムスキャンを実行すること ・外部から受け取ったファイルを安全な仮想環境上で安全性を確認するシステムを導入すること

ラベル	目的	要求事項	No.	達成条件	達成基準
16 マルウェア対策	マルウェア感染による情報漏洩、改ざん、システム停止を防ぐ	セキュリティ上の異常を素早く検知するマルウェア対策を行っていること	57	パソコン、サーバーには、マルウェア感染を検知・通報するソフトウエア (ウイルス対策ソフト)を導入している	【規則】 ・パソコン、サーバーごとにウイルス対策ソフトを導入すること ・機器に応じた適切なスキャン範囲と頻度を規定し、スキャンを実行すること ・ウイルス対策ソフトのパターンファイルが最新化できない場合、代替となる対応を定め実施すること 【対象】 ・ネットワークに接続している全てのパソコン、サーバー
			58	ウイルス対策ソフトのパターンファイルは常に最新化している	【対象】 №136 の対象のとおり 【パターンファイルの更新頻度】 起動し利用する日ごとに 1 回 以上
		セキュリティ事件・事故が発生した場合に、侵入経路や漏えい経路の調査が行えるよう、ログが取得されていること	59	インシデント発生時の調査のために必要なログを取得している	【規則】 ・下記ログを取得、保管している [取得するログ(保管期間)] -メールの送受信ログ(6 カ月) 取得項目：日時、宛先メールアドレス、送信元メールアドレス -ファイアウォールのログ(6 カ月) 取得項目；日時、送信元 IP アドレス、送信先 IP アドレス -プロキシサーバーのログ(6 カ月) 取得項目：日時、リクエスト元 IP アドレス、URL -リモートアクセスのログ(6 カ月) 取得項目：日時、接続元 IP アドレス、ユーザーID -認証サーバーのログ(6 カ月) 取得項目：日時、接続元 IP アドレス、ユーザーID、成功/失敗 -エンドポイント（パソコン、サーバー）の操作ログ（6 ヶ月） 取得項目：日時、ホスト名、ユーザーID、IP アドレス、操作内容 ※クラウドサービスの利用も対象に含む ※クラウドサービスを利用しており保管期間の規則を満たせない場合は リスクに応じて期間を各社で判断 ※工場領域はエンドポイントの操作ログの取得が難しい場合、 ネットワークログの取得および OS 基本機能のシステムログを取得

ラベル	目的	要求事項	No.	達成条件	達成基準
17 バックアップ・復元(リストア)	システム停止、データ消失による業務影響を極小化するとともに、早期の業務復旧を実現する	サイバー攻撃に対して重要情報の被害やシステム稼働の影響を最小限に留める対策を行っていること	60	適切なタイミングでバックアップを取得している	【規則】 ・取得対象、取得頻度を定めてバックアップを取得すること ・バックアップを取得できない場合は、バックアップに代替する施策を検討すること
			61	復元(リストア)手順を整備している	【規則】 バックアップ対象ごとにリストア手順書を整備すること
			62	重要なデータやシステムについてバックアップの復元(リストア)テストを実施している	【規則】 ・定めた復元手順により、復元ができることを確認すること 【対象】 ・重要なデータ・システム 【頻度】 ・システム構築時、変更時、定期的（リスク応じて判断） ・頻度はシステム構築時、変更時
			63	サーバー等の設置エリアには、設備に災害対策、環境対策を実施している	【規則】 ・火災、水害、停電に対する対策を行うこと ・温湿度管理を行うこと

7. 用語集

No.	用語	説明
1	CISO	企業や組織内において実効力のあるセキュリティ施策を行うために設置される責任者。サイバー攻撃やセキュリティ事件・事故の際の判断や対応を行う。 Chief Information Security Officer の略称。
2	CSIRT	企業や組織等におけるコンピュータセキュリティに関する事件・事故の調査対応にあたる専門チームのこと。 Computer Security Incident Response Team の略称。
3	HTTPS	ホームページがあるサーバーとブラウザがある端末（PC やスマホ等）間の通信規格。従来の HTTP を暗号化してセキュアにしたもの。ホームページアドレスの先頭に記載される。 Hyper Text Transfer Protocol Secure の略称。
4	IPA	コンピュータウイルスやセキュリティに関係する調査・情報提供を行っている独立行政法人。情報処理推進機構。
5	MAC アドレス	製造段階に付与するネットワーク機器や PC・サーバーのネットワークアダプタの固有識別番号。
6	OEM	自動車メーカー。 Original Equipment Manufacturer の略称。
7	OS	Operating System の略。コンピューターの土台を支えている基本ソフトウェアのこと。Windows、Mac、Linux などがある。
8	SOC	ネットワークやデバイスを監視し、サイバー攻撃の検出や分析、対応策のアドバイスを行う組織。 Security Operation Center の略称。
9	VPN	インターネット等の他のネットワーク上に仮想の専用回線を構築し、イントラネット内と同様なセキュア通信を実現する技術。 Virtual Private Network の略称。
10	Windows Update	Windows の脆弱性を修正するためにプログラムを配信する機能。
11	アクセス権	システムの利用者および利用者グループに対して設定される、そのシステムの利用権限のこと。アクセス制御に利用され、設定に応じて利用を許可したり拒否したりする。
12	亜種	既に出まわった不正プログラムやワームなどの一部を改変して作られた派生型マルウェアのこと。

No.	用語	説明
13	外部情報サービス	自組織内で情報機器を保有しない形態の情報サービス。 インターネット上で提供されたり、関連のある他組織で提供されたりする。
14	可用性	必要な人が必要な時に、情報を使える状態であること。
15	完全性	情報が全て揃っていて欠損や不整合がないこと。
16	機密区分	機密情報を分類する区分。例として「極秘」「社外秘」など。
17	機密情報	企業が保有している情報のうち外部への開示が予定されない情報。開示されれば企業に損失が生じる恐れがある。
18	機密性	許可されていない情報を、使用させない、また開示しないこと。
19	危殆化	何らかの状況変化で危険な状態になる事。用例:コンピューター演算能力の飛躍的向上により解読技術が進化し、暗号が危殆化する。
20	クラウドサービス	自組織内で情報機器を保有しない形態の情報サービス。 主にインターネット上で提供される。(外部情報サービスの一部)
21	サイバー・フィジカル・セキュリティ対策フレームワーク	経済産業省が 2019 年 4 月に策定した、産業界全般に求められるセキュリティ対策の全体像を整理したフレームワーク。
22	サイバーセキュリティリスク	サイバー攻撃により、電子データの漏えい・改ざん等や、IT システムや制御システム等の機能が期待通りに果たされないといった不具合が生じるリスク。
23	サプライチェーン	製品の原材料・部品の調達から、製造、在庫管理、 配送、販売、消費までの一連の流れ。供給連鎖。
24	重要な製造設備・機器	各社のリスク判定基準に応じて重要と判断された設備・機器。 リスク判定基準としては以下のような観点がある。 ・部品・製品供給に影響を及ぼす可能性のある設備・機器 ・部品・製品の品質に影響を及ぼす可能性のある設備・機器 ・地域住民・工場従事者の安全に影響を及ぼす可能性のある設備・機器　等

No.	用語	説明
25	情報機器	情報を処理・伝達・加工するための機器。パソコン・サーバー・スマートフォンなどとその周辺機器。
26	情報資産	企業が保有している守るべき重要な情報と重要な情報を 取り扱う機器。 例）情報資産（情報）：機密情報や個人情報等 情報資産（機器）：サーバー、パソコン、ネットワーク機器、OS、 ソフトウェア等
27	情報/OTセキュリティ事件・事故	情報資産や製造設備に内在した脆弱性が突かれ情報資産や製造設備を取り巻く様々な脅威により、顕在化したもの。 セキュリティインシデントとも呼ばれる。
28	初動	情報/OTセキュリティ事件・事故等が発生した際に、最初に起こす行動や動作。
29	スナップショット	ある時点でのソースコードや、ファイル、ディレクトリ、データベースファイルなどの状態を抜き出したもののこと。
30	スパイウェア	ユーザーに関する情報をユーザーが意図しない形で収集し、それを自動的に送信するマルウェア
31	制御システム	製品の製造、出荷、生産、および販売などの産業プロセスを制御するのに使用される情報システム。 制御システムには、地理的に分散している資産を管理するのに使用される監視制御データ収集システム（SCADA）、分散制御システム（DCS）、およびローカルなプロセスを プログラマブル論理制御装置（PLC）の利用を通じて制御するシステムなどがある。
32	生産技術	製品を効率的かつ高品質に生産するために生産ラインの設計や管理を行う技術。
33	脆弱性	プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のこと。
34	セキュリティパッチ	ソフトウェアで発見された問題点や脆弱性に対し、これらの不具合を解決するためのプログラム。
35	セキュリティポリシー	トップマネジメントによって正式に表明された組織のセキュリティに係る意図や方向付け及び、そのような意図や方向付けに基づいてセキュリティ対策を行うために組織が定めた規定。
36	ソフトウェア	情報システムを動かすために利用されるプログラムのこと。 特定の作業を行うために使用されるアプリケーションを指すことが多い。
37	ディープラーニング	人工知能技術の中の機械学習技術の一つ。人間の手を使わず、コンピューターが自動的に大量のデータの中から希望する特徴を発見する技術を指す。

No.	用語	説明
38	デーモン	UNIX, Linux, Mac OS X などUnix 系のオペレーティングシステムにおいて動作するプログラムで、主にバックグラウンドで動作するプログラムを指す。
39	認証	相手が名乗った通りの本人であると何らかの手段により確かめること。
40	パケット フィルタリング	通信が正しく行われるように特定のルールに基づいて検査、あるいは通信セッションの前後関係の整合性を検査し、不正だと判断した場合パケットを破棄するフィルタリング手法である。
41	ファームウェア	コンピューター等の電子機器に組み込まれた、ハードウェアを制御するためのソフトウェア。
42	復元(リストア)	障害発生時に、予め取得しておいたバックアップデータから、正常稼働状態にデータを戻すこと。
43	マルウェア	不正かつ有害に動作させる意図で作成された悪意のあるソフトウェアや悪質なコードの総称。コンピュータウイルスやワーム、スパイウェアなどが含まれる。
44	無線 LAN	物理ケーブルを使わない、無線技術を利用したネットワーク。 Wi-Fi とも呼ばれる。
45	ランサムウエア	「ランサム（Ransom＝身代金)」と「ウェア（Software)」を繋げた造語で、ソフトウェアを悪用し、データの身代金を要求するマルウェアのこと。
46	ローカルブレイクアウト	企業の本社やデータセンターを経由せずに、各拠点から直接インターネットに接続するネットワーク構成。

あとがき

自動車産業は、様々な部品・ソフトウェア等の構成要素を組み合わせて製造しているため、自動車を製造している工場だけでなく、部品・ソフトウェアを製造している工場に対するサイバー攻撃も懸念されます。

自動車産業における製造設備特有の要件を考慮した上で、製造設備に対するパッチ適用、インシデント対応体制整備など、エンタープライズ版と異なる対策が必要となる OT 環境を対象とした業界共通の自己評価基準の明示により、自動車産業全体の OT 環境のサイバーセキュリティ対策のレベルアップや対策状況の効率的な点検を推進することを目的として本ガイドライン（工場領域版）を策定しました。

本ガイドラインが、自動車産業における OT 環境のサイバーセキュリティ対策のレベルアップに役立つことを期待しています。

連絡先:一般社団法人　日本自動車工業会　安全・環境領域

〒105-0012　東京都港区芝大門一丁目 1 番 30 号　日本自動車会館
TEL:03-5405-6125　　FAX:03-5405-6136