JAMA・JAPIA

自工会/部工会・サイバーセキュリティガイドライン

自動車産業における
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

2020 年 3 月 31 日

Japan Automobile Manufacturers Association, Inc.

Japan Auto Parts Industries Association

一般社団法人　日本自動車工業会
電子情報委員会
サイバーセキュリティ部会

一般社団法人　日本自動車部品工業会
IT 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	2020 年 3 月 31 日	初版発行

目次

1. 背景と目的

自動車産業はCASE(Connected、Autonomous、Shared & Services、Electric)に代表されるように100年に一度の技術的大変革期を迎えており、業界全体がモビリティ社会の実現に向けてITの利活用を推進している。一方で、ITインフラ環境や工場等の制御システムをはじめとして企業が管理するより多くの情報システムがインターネットにつながることで、社内環境に対するインターネットからのサイバー攻撃の脅威が増していることに加え、昨今は標的の企業を狙うためにセキュリティ対策を強化中の関係企業や取引先等のネットワークを攻撃したり、標的企業が利用するソフトウェアや製品に不正なプログラムを埋め込んだりするようなサプライチェーンを狙ったサイバー攻撃も懸念されることから、自動車産業を取り巻くサイバーセキュリティリスクは深刻化している状況にあると言える。

このようにサイバーセキュリティリスクが増加する環境の中で安全・安心で豊かなモビリティ社会と自動車産業の持続可能な発展を実現するためには、業界を取り巻くサイバーセキュリティリスクを正確に理解しながら業界全体でサイバーセキュリティリスクに適切な対処を行うことが必要不可欠である。

また、こうしたサイバーセキュリティリスクの変動にあわせて、国土交通省からはサイバーセキュリティ認証制度（UN WP29、CS/SU認証）により業界として統一したサイバーセキュリティ対応を行うことが要求されており、また経済産業省からはサプライチェーンのセキュリティレベルの向上に向け「サイバー・フィジカル・セキュリティ対策フレームワーク」が提示され、情報システム分野における業界標準のガイドラインを作成することが求められている。

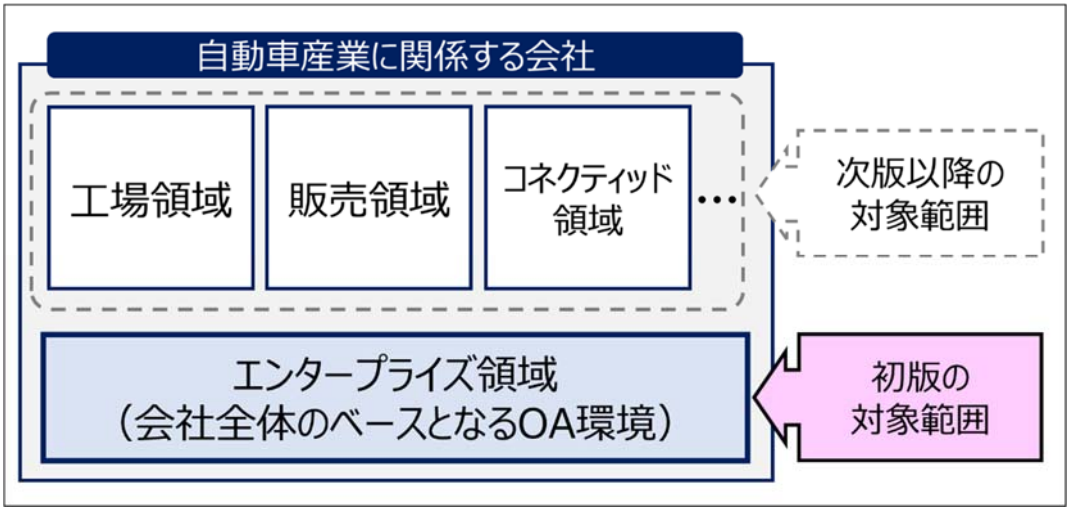
前述の背景をふまえ、自動車メーカーやサプライチェーンを構成する各社に求められる自動車産業固有のサイバーセキュリティリスクを考慮した対策フレームワークや業界共通の自己評価基準を明示することで、自動車産業全体のサイバーセキュリティ対策のレベルアップや対策レベルの効率的な点検を推進することを目的として本ガイドラインを作成した。

2. 本ガイドラインの対象

本ガイドラインは、自動車産業に関係する全ての会社を対象とし、各社においてセキュリティ業務に関与している以下に例示される部門の責任者及び担当者を想定読者としている。

- 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
- セキュリティ対応部門
- 情報システムや制御系システムの開発/運用部門
- データマネジメント部門
- サプライチェーンの管理責任を負う購買や調達部門

なお、本ガイドラインの初版では、特定の業務領域によらず全体の業務に共通するエンタープライズ領域（業務基盤となる OA 環境）を対象範囲とする。



＜図:自動車産業 CS ガイドライン初版の対象領域＞

3. ガイドラインの構成

自動車産業サプライチェーン全体のセキュリティの向上を優先課題ととらえており、中小企業を含めた全ての企業が本ガイドラインを活用できるよう、企業の規模によらず自動車産業全体が優先して実施すべき重要項目に絞り込んだ構成とした。

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

本ガイドラインは、「経済産業省 サイバー・フィジカル・セキュリティ対策フレームワーク」を中核に、「NIST Cybersecurity Framework v1.1」、「ISO 27001」、「AIAG Cyber Security 3rd Party Information Security 1st Edition」、「IPA 中小企業の情報セキュリティ対策ガイドライン」をベンチマークし作成した。

4. ガイドラインの活用方法

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、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、業界をあげて推し進めて行きたい。

また、共通のガイドラインに基づくセキュリティの実装及びその評価により、自社の取引関係におけるセキュリティ信頼チェーン構築に関わる評価プロセスを簡素化し効果的な利用を期待する。

(1) 企業におけるセキュリティポリシーの策定及び対策の実装
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、自社におけ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) 自動車産業における信頼のチェーン構築への活用

本ガイドラインを通じ、共通のセキュリティチェックシートによりセキュリティ対策の実装状況を確認することで、多岐複雑な自動車産業の企業間の取引におけるセキュリティ信頼チェーンの構築に活用することができる。

(3) 企業におけるセキュリティの教育・訓練・啓発活動への活用

本ガイドラインを通じ、自社のセキュリティ状況を把握し、セキュリティに関する各企業での教育・訓練、啓発活動に活用することができる。

5. 要求事項と達成条件

分類	ラベル	要求事項	No.	達成条件
共通	方針	自社のセキュリティ対応方針を自組織内に周知しており、方針に基づく運用を行っていること	1	自社のセキュリティ対応方針(ポリシー)を策定している
			2	セキュリティ対応方針(ポリシー)を社内に周知している
	ルール	従業員への社内機密情報のセキュリティ社内ルールを規定していること	3	従業員に守秘義務を理解させ、守らせている
			4	業務で利用する情報機器の利用ルールを周知している
	法令順守	情報セキュリティに関する法令を考慮し、社内ルールを策定すること(法令例：個人情報保護法、不正競争防止法)	5	情報セキュリティに関する法令を考慮し、ルールを策定、教育・周知している
			6	法令の変更に伴い、ルールを適宜見直ししている
	体制(平時)	平時のセキュリティ対応体制を整備し、事故発生に至らない情報収集と共有を行うこと	7	セキュリティ責任者を含む、体制と責任と役割を明確化している
			8	定期的、または必要に応じて、平時の体制を見直ししている

			9	新たな行為や攻撃の手口を知り、対策を社内部署へ共有している
	体制 (事故時)	セキュリティ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	10	体制と責任と役割を明確化している(社内外組織の連絡先を含む)
			11	発生したセキュリティ事故の概要や影響およびその後の対策が実施され、その記録がある
			12	定期的、または必要に応じて、事故時の体制を見直ししている
	事故時の手順	セキュリティ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	13	セキュリティ事故時の対応手順(初動、システム復旧等)を定めている
			14	特に、ウイルス感染時の対応手順を定めている
	日常の教育	従業員として注意することを教育していること	15	電子メールのウイルス感染に関する従業員への教育を行っている
			16	インターネットへの接続に関する従業員への教育を行っている
			17	機密区分に応じた情報の取り扱いに関する従業員へ教育を行っている
	セキュリティ事故対応の教育・訓練	セキュリティ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	18	教育・訓練を定期的に実施し、その記録がある
			19	教育・訓練の内容を必要に応じて見直ししている
守る対象を明確にし、リスクを特定する(特定)	他社とのセキュリティ要件	サプライチェーン上で発生するセキュリティ要件が明確になっていること	20	他社との間で、機密情報の取り扱い方法が明確になっている
			21	セキュリティ事故時の他社との役割と責任が明確になっている
	アクセス権	アクセス権(入室権限やシステムのアクセス権)を適切に	22	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

		管理していること	23	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
			24	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
	情報資産の管理(情報)	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	25	機密区分に応じた情報の管理ルールを定めている
			26	高い機密区分の情報資産(情報)は一覧表を作成している
			27	情報資産(情報)は機密区分に応じた管理ルールに沿って管理している
	情報資産の管理(機器)	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	28	重要度に応じた情報機器、OS、ソフトウェアの管理ルールを定めている
			29	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
			30	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
	リスク対応	自組織内(自組織の業務:業務委託も含めて)のセキュリティリスクに対する対策を行っていること	31	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(影響範囲、発生頻度等)を特定できている
			32	必要に応じて経営層へリスク及び対策を報告し、 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
			33	情報資産のリスクは管理ルールに沿って管理している

	取引内容・手段の把握	取引先を明確にし、取引に利用している手段を把握していること	34	会社毎に取引内容・取引手段(受発注の手段等、情報のやり取り)を明確にしている
	外部への接続状況の把握	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、接続状況が適切に管理されていること	35	自組織の資産が接続している外部情報システムの利用ルールを定めている
			36	利用している外部情報システムの一覧がある
			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
	社内接続ルール	社外から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	業務で利用する情報機器の自社ネットワークへの接続ルールを定めている
攻撃を防ぐ対策を実施(防御)	物理セキュリティ	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	サーバー等の設置エリアは、入場可能な人を定めている
			40	サーバー等の設置エリアは、施錠等で入場を制限している
	認証・認可	不正利用防止のため、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	41	ユーザーID を個人毎に割り当てている
			42	ユーザーとシステム管理者の権限を分離している
			43	パスワード設定に関するルールを定めている
			44	ユーザーID は定期的、または必要に応じて棚卸しを行い、不要な ID を削除している

	パッチやアップデート適用	公開されている脆弱性について、対策を行っていること	45	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
攻撃されたことを迅速に知るために(検知)	ウイルス対策ソフト	セキュリティ上の異常を素早く検知する ウイルス対策を行っていること	46	パソコン、サーバーには、ウイルス感染を検知・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
			47	ウイルス対策ソフトのパターンファイルは常に最新にしている
検知被害の対応と修復(対応・復旧)	バックアップ・復元(リストア)	サイバー攻撃に対して重要情報の被害を最小限に留める対策を行っていること	48	適切なタイミングでバックアップを取得している
			49	復元(リストア)手順を整備している
			50	システムが停止した際も業務が遂行できる代替手段を用意している

6. 用語集

No	用語	説明
1	BYOD	従業員が個人保有の携帯用機器を使って、業務に使用すること。(BYOD :Bring your own device)
2	CASE	自動車業界のトレンドを示す造語。クルマとデータセンターをつないで情報を分析しサービス提供を行うコネクティッド、自動的に目的地まで導く自動化、ライドシェアサービスを意味するシェアリング、100%電気を動力源とする電気自動車の普及を目指す電動化の４つを意味する。
3	CS/SU 規制	UN WP29 において導入が検討されている Cyber Security (CS) ならびに Software Updates (SU) に関する規制。2019 年 9 月に改定案が公開され、採択に向けた作業が進められている。
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	JVN	日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供する組織。 Japan Vulnerability Notes の略称。
6	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。
7	OEM	自動車メーカー。 Original Equipment Manufacturer の略称。
8	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。
9	UN WP29	自動車基準調和世界フォーラムの 29 番目の作業部会。世界で唯一の自動車基準の調和組織として、基準案の検討などの活動を行っている。
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	暗号化方式	第三者が情報を見てもわからないように変換する手法を暗号化といい、暗号化を行うために様々な方式がある。無線 LAN の例では、WEP、WPA、WPA2 などがあり、安全な暗号化方式を選んで利用する必要がある。
13	ウイルス	セキュリティ上の被害を及ぼす悪意を持ったプログラムを指す総称。ウイルス以外に、スパイウエア、ボットなどもある。
14	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。
15	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。
16	完全性	情報が全て揃っていて欠損や不整合がないこと。
17	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。
18	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。
19	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。
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、期待されていた IT システムや制御システム等の機能が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	一般的には、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	情報機器	情報を処理したり、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。

25	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、PC、ネットワーク機器、OS、ソフトウェア等
26	初動	セキュリティ事故等が発生した際に、最初に起こす行動や動作。
27	制御システム	製造、製品の出荷、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）、および前二者より小規模ながら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。
28	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。
29	セキュリティ事故	情報資産に内在した脆弱性が情報資産を取り巻く様々な脅威により突かれ、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。
30	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。
31	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。
32	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。
33	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。
34	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。
35	復元(リストア)	障害発生時に、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。

あとがき

昨今のサイバー攻撃は、自社内環境だけでなくサプライチェーンを狙った攻撃が増加しており、自動車産業を取り巻くサイバーセキュリティリスクは深刻化しています。

このような環境の中で安全・安心で豊かなモビリティ社会と自動車産業の持続可能な発展を実現するためには、業界を取り巻くサイバーセキュリティリスクを正確に理解しながら業界全体でサイバーセキュリティリスクに適切な対処を行うことが必要不可欠です。

そのため、自動車メーカーやサプライチェーンを構成する各社に求められる自動車産業固有のサイバーセキュリティリスクを考慮した対策フレームワークや業界共通の自己評価基準を明示することで、自動車産業全体のサイバーセキュリティ対策のレベルアップや対策レベルの効率的な点検を推進することを目的として、日本自動車工業会（ＪAMA)、日本自動車部品工業会（ＪＡＰＩＡ）が共同でセキュリティガイドライン(対策項目、基準)を策定しました。

本ガイドラインが、自動車産業全体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。

執筆委員(会社名　五十音順)

一般社団法人　日本自動車工業会

電子情報委員会 サイバーセキュリティ部会 CS ガイドライン検討タスク

役割	会社名	氏名
リーダー	トヨタ自動車株式会社	坂　季也
サブリーダー	日産自動車株式会社	鳥居　俊太郎
サブリーダー	本田技研工業株式会社	久保　充
委員	スズキ株式会社	鈴木　秀明
委員	株式会社SUBARU	大内　良博
委員	ダイハツ工業株式会社	阪田　信行
委員	株式会社トヨタシステムズ	岩下　満夫
委員	株式会社トヨタシステムズ	谷口　昇
委員	マツダ株式会社	市本　秀則
委員	三菱自動車工業株式会社	宇津井　祐介

一般社団法人　日本自動車部品工業会

IT 対応委員会 サイバーセキュリティ部会

役割	会社名	氏名
部会長	株式会社デンソー	後藤　俊二郎
副部会長	日立オートモティブシステムズ株式会社	中尾　考行
副部会長	日立オートモティブシステムズ株式会社	岸　友和
副部会長	マレリ株式会社	鈴木　健一
委員	愛三工業株式会社	新名　健治
委員	アイシン精機株式会社	大西　裕之
委員	ＮＯＫ株式会社	本沢　翼
委員	ＫＹＢ株式会社	川野　次郎
委員	ＫＹＢ株式会社	須郷　英知
委員	株式会社小糸製作所	野寄　靖史
委員	株式会社ショーワ	遠嶋　成樹
委員	スタンレー電気株式会社	田中　知明
委員	株式会社デンソー	原　浩司
委員	株式会社デンソー	野田　智文
委員	株式会社東海理化	増田　直樹
委員	豊田合成株式会社	松井　幸吉
委員	トヨタ紡織株式会社	大迫　光弘
委員	日本特殊陶業株式会社	加藤　宏明
委員	日本発条株式会社	鈴木　孝司
委員	株式会社ミツバ	尾形　永
委員	株式会社ミツバ	入江　祐介
委員	矢崎総業株式会社	植松　克則

連絡先:一般社団法人　日本自動車工業会　技術統括部

〒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