自動車産業 セキュリティチェックシート(必須項目)

Ver.0.9
一般社団法人　日本自動車工業会
一般社団法人 日本自動車部品工業会

会社名		評価範囲	▽プルダウンから選択ください
評価者(評価日)		確認者(確認日)	
E-Mailアドレス			
Tel番号			

達成条件評価欄に達成条件毎の実施レベルをご記入ください。また、評価の根拠記入欄に対策状況をご記入ください。

分類	ラベル	要求事項	No.	達成条件	他社事例	評価結果		対応状況			経産省CPSF要求事項に関する対策要件ID
						達成条件評価	評価の根拠記入欄 ■対策完了(2点)：規程名、導入システム/策定・改定・導入年 ■対策中(1点)：現状と完了予定時期 ■未実施(0点)：今後の改善計画 ■該当なし：該当しないと判断した理由	0:未実施	1:対応中	2:対応完了	
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	–	▽プルダウンで評価ください					CPS.BE-2
			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	–	▽プルダウンで評価ください					
	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	・業務上知り得た情報を外部に漏らさない等のルールを守らせている ・個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしている	▽プルダウンで評価ください					CPS.GV-2
			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(個人所有機器(BYOD)含む)	・個人所有のUSBを利用しないルールを周知している	▽プルダウンで評価ください					
	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	–	▽プルダウンで評価ください					CPS.GV-2
			6	法令の変更に伴い、ルールを適宜見直ししている	–	▽プルダウンで評価ください					
	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(社内外組織の連絡先を含む)	・小規模な組織であれば１～２名の体制の場合もある	▽プルダウンで評価ください					CPS.AE-2 CPS.RA-2 CPS.DP-2 CPS.IM-1 CPS.IM-2
			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	–	▽プルダウンで評価ください					
			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	・他社事例や技術動向等の専門的な分析ができない場合は、支援サービスの窓口を把握している ・IPAの情報セキュリティのページからセキュリティ事例を把握している	▽プルダウンで評価ください					
	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)	・小規模な組織であれば１～２名の体制の場合もある	▽プルダウンで評価ください					CPS.AE-2 CPS.RA-2 CPS.DP-2 CPS.IM-1 CPS.IM-2
			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	–	▽プルダウンで評価ください					
			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	・発生したセキュリティ事故の原因や影響範囲等の専門的な分析ができない場合は、支援サービスの窓口を把握している ・過去のセキュリティ事故事例の概要や影響およびその後の対策を検討した記録から見直しをしている	▽プルダウンで評価ください					
	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	・メール送信履歴から、意図しないメール送信がないかを確認している ・感染源を特定している ・感染したサーバーやパソコンに対して駆除が正しく行われたことを確認する手順が決まっている ・社外に影響が発生していないか把握する手順(外部通信のログ確認)が決まっている	▽プルダウンで評価ください					CPS.RP-1
			14	特に、ウイルス感染時の対応手順を定めている	・ウイルスを検知した際のユーザーの取る初動(パソコンのネットワークからの切り離し等)が周知されている	▽プルダウンで評価ください					
	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	・電子メールの添付ファイルや本文中のURLリンクを介したウイルス感染に気を付けている	▽プルダウンで評価ください					CPS.AT-1
			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	・信頼しない公衆無線LANへは接続しない ・安全に使うために、適切な暗号化方式を使った無線LANを利用すること ・インターネットを介したウイルス感染やSNS書き込み等のトラブルへの対策を行っている	▽プルダウンで評価ください					
			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	・紛失や盗難防止のため、重要情報が記載された書類や電子媒体は、机上に放置せず、書庫等に安全に保管している ・重要情報が記載された書類や電子媒体を持ち出すときには、盗難や紛失の対策をしている ・離席時にパソコン画面の覗き見や勝手な操作ができないようにしている ・重要情報が記載された書類や、重要なデータが保存された媒体を破棄する時は、復元できないようにしている。 ・電子メールやFAXの宛先の送付ミスを防ぐ取組みを実施している	▽プルダウンで評価ください					
	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	–	▽プルダウンで評価ください					CPS.AT-1
			19	教育・訓練の内容を必要に応じて見直ししている	–	▽プルダウンで評価ください					
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	・秘密保持契約を締結し、契約終了時に機密情報の返却、消去を行わせている	▽プルダウンで評価ください					CPS.BE-1
			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	–	▽プルダウンで評価ください					
	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)を適切に管理していること	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	–	▽プルダウンで評価ください					CPS.IP-9
			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	–	▽プルダウンで評価ください					
			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	–	▽プルダウンで評価ください					
	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	・情報資産の機密区分の設定ができない場合は、供給元に確認している	▽プルダウンで評価ください					CPS.GV-3
			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	–	▽プルダウンで評価ください					
			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	–	▽プルダウンで評価ください					
	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	–	▽プルダウンで評価ください					CPS.AM-1
			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	–	▽プルダウンで評価ください					
			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	・一覧を定期的、または必要に応じて見直ししている	▽プルダウンで評価ください					
	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	＜セキュリティリスクの洗い出し方法例＞ ・脅威、脆弱性から発生頻度、影響範囲を明確化 ・機密区分の高い情報資産の一覧作成 ・機密区分の決定 ・機密区分に応じた対策 ・定期的、または必要に応じて上記を行っている	▽プルダウンで評価ください					CPS.BE-2 CPS.RM-1
			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	–	▽プルダウンで評価ください					
			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	–	▽プルダウンで評価ください					
	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	–	▽プルダウンで評価ください					CPS.BE-3
	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、接続状況を適切に管理していること	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	・クラウド利用時の利用ルールを定めている	▽プルダウンで評価ください					CPS.AM-5
			36	利用している外部情報システムの一覧がある	–	▽プルダウンで評価ください					
			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	–	▽プルダウンで評価ください					
	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	・業務利用端末においてMACアドレスによる認証を行っている	▽プルダウンで評価ください					CPS.AC-1 CPS.AC-3 CPS.AC-4
攻撃を防ぐ対策実施(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	–	▽プルダウンで評価ください					CPS.AC-2 CPS.IP-5
			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	・サーバー設置場所に社員証による入退場認証システムを設置している ・部屋が無い場合は、サーバラックに施錠保管、あるいは施錠可能な部屋やエリアに設置している	▽プルダウンで評価ください					
	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	–	▽プルダウンで評価ください					CPS.AC-1 CPS.AC-5 CPS.AC-6 CPS.AC-9 CPS.GV-3
			42	ユーザーとシステム管理者の権限を分離している	–	▽プルダウンで評価ください					
			43	パスワード設定に関するルールを定めている	・パスワードは英数字記号を含めて10文字以上にしている ・パスワードは複数のシステムで使い回さない ・ログオン試行(失敗)回数を設定し一時的にログオンが出来ないようにしている ・パスワードの有効期限を設定している	▽プルダウンで評価ください					
			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	–	▽プルダウンで評価ください					
	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	・IPA／JVN等のウェブサイトやメールマガジンで最新の脆弱性情報を把握している ・脆弱性対応のソフトウエアアップデートを行っている ・Windows Updateを実施している	▽プルダウンで評価ください					CPS.RA-2 CPS.MA-1
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	・ウイルス対策ソフトを導入し、外部セキュリティー監視サービス会社と連携して対応している	▽プルダウンで評価ください					CPS.RP-1
			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	–	▽プルダウンで評価ください					
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	・定期的に重要情報のバックアップを取り、サプライチェーンに影響を及ぼすものに対しては、復元(リストア)訓練を行っている	▽プルダウンで評価ください					CPS.DS-6 CPS.DS-7
			49	復元(リストア)手順を整備している	–	▽プルダウンで評価ください					
			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	–	▽プルダウンで評価ください					
						0 / 100点					