【自動車産業サイバーセキュリティガイドライン v2.3】レベル1 優先20項目 セルフチェックシート

点検日：[　　]年[　　]月[　　]日 ／ 事業所・部署名：＿＿＿＿＿＿＿＿＿＿ ／ 点検者：＿＿＿＿＿＿＿＿

判定基準：[2点：対策完了]　[1点：対応中・改善中]　[0点：未実施・未検討]

--【柱1：セキュリティ事故発生に備えた構え（8項目）】----------

[区分]	No.	[チェック項目]	自社判定	改善計画・メモ
緊急体制	No.18	事故時の責任者・連絡体制・報告ルートが決まっているか	2 / 1 / 0	
	No.19	事故内容を記録するフォーマット（報告シート）があるか	2 / 1 / 0	
	No.20	緊急連絡先リストや対応体制を定期的に見直しているか	2 / 1 / 0	
	No.24	不審な挙動時の初動対応手順（LAN抜去・Wi-Fi切断）があるか	2 / 1 / 0	
	No.26	ウイルス感染時の専用対応手順（隔離・復旧）が整備されているか	2 / 1 / 0	
バックアップ	No.148	重要データのバックアップを定期的に取得しているか	2 / 1 / 0	
	No.149	バックアップはネットから切り離した安全な場所にあるか	2 / 1 / 0	
業務継続	No.150	システム停止時も紙やFAX等で業務継続できる手順があるか	2 / 1 / 0	

---【柱2：侵入・拡散させない基本対策（12項目）】----------

[区分]	No.	[チェック項目]	自社判定	改善計画・メモ
情報収集	No.16	最新のサイバー攻撃手法や他社事例情報を集めているか	2 / 1 / 0	
OS・ソフト	No.124	OSやソフトウェアにセキュリティパッチを期日適用しているか	2 / 1 / 0	
ウイルス対策	No.136	すべてのPC・サーバーにウイルス対策ソフトを入れているか	2 / 1 / 0	
	No.137	ウイルス定義ファイル（パターン）は毎日最新化されているか	2 / 1 / 0	
アカウント・アクセス管理	No.115	パスワードは「長く・複雑に・使い回さない」ルールか	2 / 1 / 0	
	No.49	情報の重要度（機密性）に応じた分類ルールがあるか	2 / 1 / 0	
	No.51	重要データへのアクセス権限を必要な人だけに絞っているか	2 / 1 / 0	
	No.52	不要なアカウントや権限が残っていないか定期点検しているか	2 / 1 / 0	
接続管理	No.79	持ち込みPC等の社内ネットワーク接続ルールが定められ、システム的に制御・強制されているか	2 / 1 / 0	
外部システム管理	No.76	利用しているクラウドや外部システムを台帳化しているか	2 / 1 / 0	
	No.77	外部システムの利用台帳を定期的に更新しているか	2 / 1 / 0	
	No.78	外部システムの共有設定ミスや不要な権限がないか見直したか	2 / 1 / 0	

【総合スコア：[　　]／40点】　次回点検予定日：　　年[　]月[　]日