SCS 9001概要
Supply Chain Security 9001

SCS 9001って何、どう使うの？

2023年12月11日TL 9000セミナーテキストより抜粋

SCS 9001:グローバルサイバーセキュリティ標準

- SCS 9001 は、高度なサプライ チェーン サイバー攻撃が増加しているため、グローバル サプライ チェーン セキュリティのための情報通信技術 (ICT) 固有の標準に対する緊急のニーズに対応するため作成されたものである。
- SCS 9001 は単なる標準ではなく、企業、政府、消費者向けの信頼できる ICT プロバイダーおよびサプライヤーを検証する完全なサイバーセキュリティおよびサプライ チェーン セキュリティ管理システムをめざしたものである。

  - 安全なソフトウェア開発
  - ソフトウェアIDとソースのトレーサビリティを確保するための検証方法
  - 製品セキュリティ
  - 内部統制の原産地と透明性に関する政府の要件

SCS 9001を使う理由

- セキュリティは製品ではなく、プロセスでコントロールするべき。
- SCS 9001 は、品質マネジメント システム (QMS) の上に構築されたプロセスベースの規格である。
- SCS 9001 認定サプライヤを使用することで、すべての製品とサービスにわたって一貫したセキュリティを確保できる。

- SCS 9001の現状
  - SCS9001を取込んでの通信全体での活動までは進んでいない。
    - トライアル的な状況にある。
  - R2.0が発行され、AB,CBの教育が行われている。
  - TL 9000と同様、AB,CBのによる認証認定が行われる。

- 将来サプライヤーからの認証登録を求められる可能性もある。

SCS 9001を実装するメリット

- ユーザーへのサービスの継続的な改善
- 組織とその顧客との間の強化された関係
- サプライチェーンのセキュリティ管理システム要件の標準化
- 外部監査とサイト訪問の効率的な管理
- 均一な測定
- 全体的なコスト削減と競争力の向上
- 強化された管理と改善された組織のパフォーマンス

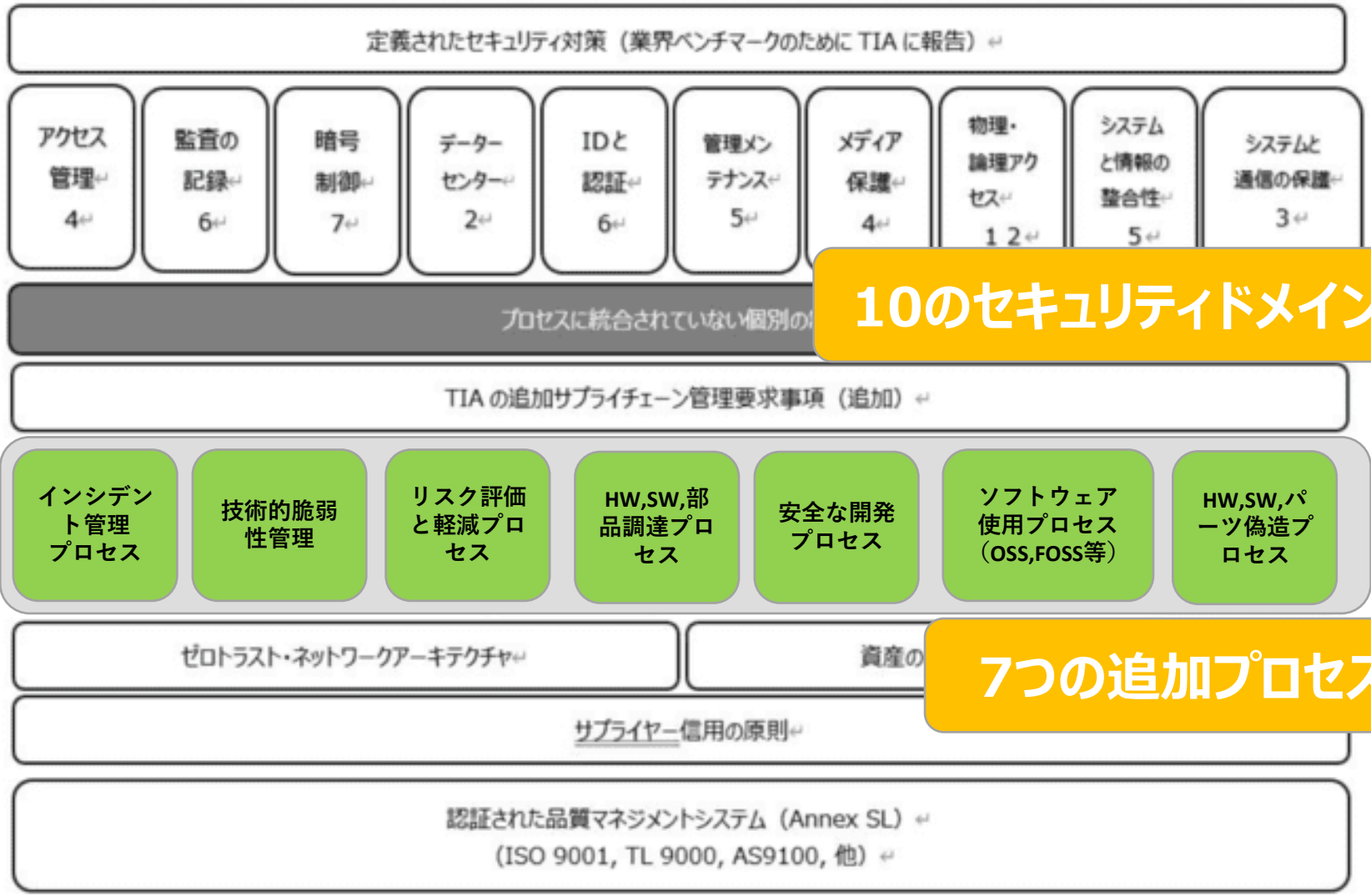
将来的には、

- SCS 9001 測定の業界ベンチマーク
- 組織のサプライ チェーンにおける脆弱性の発見と適切な措置

SCS 9001 Handbook R2.0の概要

- 基本的にISO 9001の章立て・内容・構成をベースに作成されている
- 要求事項の大項目・中項目はISO 9001と同一。
  - サプライチェーンセキュリティに関する要求事項については x.x.SC.xという形でそれぞれの章に追加されている。
- TL 9000と同様にセキュリティに関する測定法が規定されている。
  - SCS 9001では、要求事項と測定法が一つにバンドルされている。
- 要求事項
  - 全98項目。
  - ISO 9001のように組織における製品やサービスの開発、製造、出荷、保守といったライフサイクルにおけるサプライチェーンを含んだセキュティマネジメントに対する要求事項が規定されている。

SCS 9001のアーキテクチャモデル



SCS 9001 R1.0ハンドブックの構成

要求事項

セクション1	はじめに
セクション2	構造
セクション3	SCS 9001の管理
セクション4	組織の状況
セクション5	リーダーシップ
セクション6	計画
セクション7	支援
セクション8	運用
セクション9	パフォーマンス評価
セクション10	改善
附属書A	規制の目的及び規制
附属書B	必要な測定法
附属書C	開発モデル
附属書D	用語集
附属書E	参考文献

セクション1～3および
本文であるセクション4～10は
ISO 9001:2015 と同じ構造
：ハイレベルストラクチャー (HLS)

測定法

- B1 測定の使用方法と範囲
- B2 測定処理、使用及び職責要件
- B3 測定使用の原則
- B4 責任
- B5 情報及びリソース
- B6 一般測定要件
- B7 測定定義、計数ルールと計算
  - B7.1 脆弱性制御 (VC)
  - B7.2 更新の適時性 (UT)
  - B7.3 サプライヤセキュリティコンプライアンス (SSC)
  - B7.4 サプライヤの再検証 (SR)
  - B7.5 フィッシング攻撃成功 (PAS)
  - B7.6 未認可エントリ率 (UER)
  - B7.7 不正アクセス (UA)

SCS 9001測定法

- 測定法
  - 想定対象：組織の内部システムやプロセスにおけるインシデント（組織の製品やサービスそのものが対象ではない）
  - 測定期間：四半期ごと
- 測定項目：7大項目（提出: 13小項目）
  - 脆弱性制御(VC): 時間内に発生した脆弱性の軽減・修復率
  - 更新の適時性(UT): 期間内のデバイスやシステムの更新完了率
  - サプライヤ・セキュリティコンプライアンス(SCCC): 期間内にセキュリティに準拠していないサプライヤの率
  - サプライヤの再検証(SR): 期間内に完了していないサプライヤの再検証数
  - フィッシング攻撃成功(PAS):組織が実施したフィッシングテストにおけるフィッシング攻撃の全体的な成功率
  - 未認可エントリ率(UER): 期間内の不正エントリテストにおけるエントリ率
  - 不正アクセス(UA): 期間内の不正アクセスの検出所要時間/軽減率/修復率

SCS 9001測定法（その1）

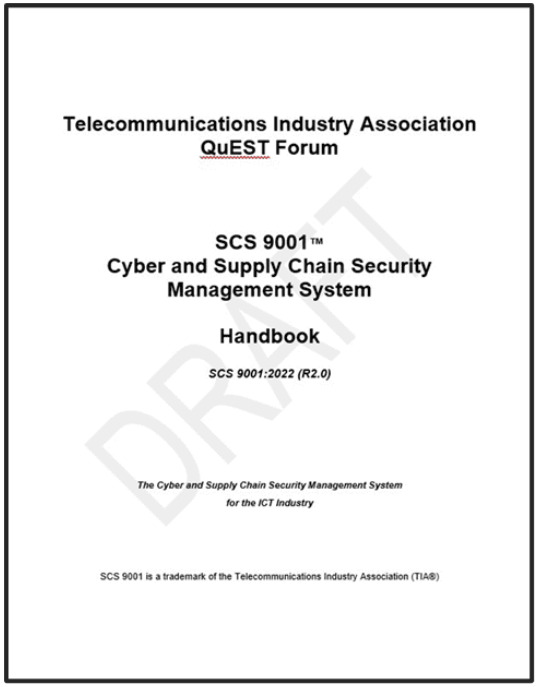
測定項目	データ要素		提出測定値		
B7.1 脆弱性制御 (VC) ・組織の脆弱性の発見と通知の記録 ・組織の脆弱性緩和および修復完了記録	VCMcc VCMdc VCMch VCMdh VCRcc VCRdc VCRch VCRdh	報告期間中に期限が到来し、完了した重大な脆弱性緩和の数 報告期間中に発生した重大な脆弱性緩和の数 報告期間中に完了した高レベルの脆弱性緩和の数 報告期間中に実行される高レベルの脆弱性緩和の数 報告期間中に完了した重要な脆弱性修正の数 報告期間中に行われる重要な脆弱性修正の数 報告期間中に完了した脆弱性の高い修復の数 報告期間中に実行すべき高脆弱性修正の数	VCM1 VCM2 VCR1 VCR2	重大な脆弱性の軽減率 高レベル脆弱性の軽減率 重大な脆弱性の修復率 高レベル脆弱性の修復率	100 x (VCMcc/VCMdc) 100 x (VCMch/VCMdh) 100 x (VCRcc/VCRdc) 100 x (VCRch/VCRdh)
B7.2 更新の適時性 (UT) ・組織の更新通知記録 ・組織の更新完了記録	UTce UTde UTcn UTdn	報告期間中に更新および完了するエンドユーザデバイスの数 報告期間中に更新されるエンド・ユーザー・デバイスの数 報告期間中に更新および完了する予定のネットワーク・エレメント 報告期間中に更新される予定のネットワークエレメントおよびコアシステムの数	UTe UTn	Updated Timeliness: エンドユーザデバイス Updated Timeliness: NEとコアシステム	100 x (UTce/UTde) 100 x (UTcn/UTdn)
B7.3 サプライヤセキュリティ コンプライアンス (SSC) ・データは組織の供給者情報から得る	SSCc SSCd	報告期間内にセキュリティフレームワーク準拠していない重要な仕入先の数 報告期間中の重要な仕入先の合計数	SSC	Supplier Security Compliance	100 x (SSCc/SSCd)
B7.4 サプライヤの再検証 (SR) ・組織のサプライヤ再検証スケジュール ・組織のサプライヤ再検証完了記録	SRc SRd	報告期間中に発生するサプライヤ再検証で完了しなかった件数 報告期間中に発生するサプライヤ再検証の件数	SR	サプライヤの未再検証率	100 x (SRc/SRd)

SCS 9001測定項目（その2）

測定項目	データ要素		提出測定値		
B7.5 フィッシング攻撃成功 (PAS) ・組織のフィッシングテスト記録	PASs PASe	報告期間内で成功したフィッシング攻撃の数 報告期間内の各フィッシングテストの対象となった従業員数	PAS	フィッシング攻撃成功率	100 x (PASs/PASe)
B7.6 未認可エントリ率 (UER) ・組織のエントリー・ポイント数 ・組織の不正侵入テスト記録	UERc UERp	報告期間中のテスト中の不正エントリ数 報告期間中にテストされた可能性のあるエントリポイントの数	UER	未認可エントリ率	UERc/UERp
B7.7 不正アクセス (UA) ・組織の不正アクセスの検出と通知の記録 ・組織の不正アクセス発生の開始、軽減および修復の記録	UATo UATd UATdt UATs UAMc UAMd UARc UARd	報告期間中の不正アクセスの最初の発生日時 報告期間中に検出された、または組織に報告された日時 報告期間中の発生から検出/報告までの日時: Σ(UATo-UATd) 報告期間中に検出された不正アクセスの合計数 報告期間に期限が到来し、期限通りに完了した緩和策の数 報告期間中に期限が到来した緩和措置の件数 報告期間中に期限が切れ、期限どおりに完了した是正の数 報告期間中に支払うべき是正措置の数	UAT UAM UAR	不正アクセス平均検出時間 不正アクセス緩和率 不正アクセス是正率	UATdt/UATs 100 x (UAMc/UAMd) 100 x (UARc/UARd)

SCS 9001 R2.0　R1.0からの主な変更点

- ISO 9001からの切り離し
  - QMSを必要としない場合など、組織の柔軟性に対応
  - ISO規格の認証をすでに持っているなど
- 政府要件への対応（サポート）の改善
  - 英国電気通信セキュリティ法
- パイロットで行った試行から得た全般的な改善



SCS 9001 の現在

- R2の承認は定足数に達し、承認発行（2023/9）
- 今後のサポート
    - AB/CBのトレーニング
    - 最終的な価格設定　⇒　＄395（PDF）
- IoT業界への適用を検討するチームを立ち上げる
  （Amazonの参加？など）
- UL,CTA*とIoT標準化について打合せ中
- アメリカ国務省及び商務省と協力し、コスタリカの5G国家標準としてSCS 9001の採用
    - ネットワーク構築に認定を義務付ける予定

*CTA: Consumer Technology Association

SCS 9001R2.0　まとめ

- SCS 9001の購入
  - PDF版　シングルユーザー　＄395
  - 印刷版　＄395 (在庫あり)
  - PDF+印刷　＄632 (在庫あり)　（20%割引）
- 他公的機関の採用状況
  - ANSI　未採用
  - 国防総省　未採用
- 現在の認定機関
  - ANAB:ANSI National Accreditation Body
- 認証機関
  - DNV　DQS　Schellman　TUV

- IoT業界（Amazon？？）を取込む、ULなどとの標準化を検討