シスコ

偽造電子部品検出および防止システム

シスコは、グローバルサプライチェーン全体に包括的なセキュリティ機能を導入して維持しており、不正操作、スパイ行為、中断などの重要な脅威領域に焦点を当てています。シスコは以下のような脅威から生じる問題に対し、多層型のアプローチを取っています。

- 汚染
- 偽造
- 知的財産の不正使用

シスコの偽造電子部品検出および防止システムには、偽造に対する保護、偽造が存在するときの検出、および偽造原材料（例：DFARS 252.246-7007 (a)（2014 年 5 月）で定義された電子部品）と偽造シスコ完成部品の両方を軽減するための継続的なイノベーションへの取り組みが含まれています。

このセキュリティへの取り組みには、以下の作成と導入が含まれます。

A. **意識向上キャンペーン（ベストプラクティス トレーニングと脆弱性および偽造トレンド）：**
シスコの従業員、請負業者の従業員、サプライヤ向けの意識向上キャンペーン。これらのキャンペーンでは、シスコの知的財産を構成する要素やシスコのサプライチェーンまたはサプライヤのサプライチェーンへの偽造品の挿入を回避できる可能性があるプラクティスのタイプなどを取り上げて問題に対処します。この多層型のアプローチでは、以下を提供するシスコのサプライチェーンのメンバーが対象に含まれます。

- 電子コンポーネント
- プリント基板アセンブリ（PCBA）
- 関連するソフトウェア、ファームウェア、セキュリティプログラミング

意識向上キャンペーンには、以下のような手法が含まれます。

- 知的財産保護に関するビデオトレーニング
- 偽造の「しるし」に関する特別なテクニカルサポートおよび修理センターチームのトレーニング：トレンドの変化に応じて更新される
- サプライヤの行動規範トレーニング
- アクセス制御（物理的なアクセスと情報へのアクセスの両方）
- 廃棄管理

- 偽造情報および通信技術の潜在的なソースを特定するように設計された、内密のテスト購入プログラム
- 真正性の証を明確にし、商用マーケットプレイスにリリースする前に水際で偽造を特定するための政府/自治体機関との連携

B. **コンポーネントおよび PCBA 検査、テストとトレーサビリティ**：

シスコは、以下のような品質と真正性への体系的なアプローチも導入しています。

- シスコ製品またはソリューションに使用する、電子コンポーネントなどの原材料を提供するサプライヤを承認する際の厳格な制限
- 電子部品、電子アセンブリ、シスコの完成品すべての真正性やパフォーマンスおよび受け入れ基準に対応する、全サプライヤとの契約上の義務
- シスコ製品の製造元が、電子コンポーネントの承認済みサプライヤからの原材料のみを利用するように義務づける。具体的には、シスコによるテストおよび事前認定を受けた部品のみが対象
- セキュリティテクノロジー、フィジカルセキュリティ、論理的なセキュリティのプロセスを活用する、シスコ向けに管理される電子部品「ハブ」を利用して、シスコの知的財産の汚染、偽造、悪用を最小化
- 以下にシスコのプロセスフローの概要を示します

- 以下による、すべての PCBA 上の全コンポーネントを関連付ける独自のインサーキット テスト プロセス全体の電子部品のリンクを介したトレーサビリティ
    - 日付コード
    - ロットコード
    - 製造番号（MPN）
    - テストプロセスの実行
    - テストおよび品質の結果
    - 材料内容
    - 不変 ID の証明書（該当する場合）のさらなるトレーサビリティの確保
    - ラベル付けとシリアル番号の相関関係のシステムを介し、すべての電子部品を特定の PCBA にリンクし、各 PCBA をシスコの完成品 ID にリンクするさらなるトレーサビリティ

C. **カスタマイズされたシスコの偽造防止技術のセキュアな開発および導入**：

偽造電子部品防止および検出の目標をさらに強化するために、シスコは一連のプラクティス、技術、サードパーティの認定を活用しています。例として以下のものがあります。

- シスコのセキュアな開発ライフサイクル（たとえば、設定管理、バージョン管理、ソースコードアクセス保護、セキュリティベースのリリース基準など、偽造コードを回避する重要な要素に対応）
- オープンソースソフトウェアの出自と導入の監視
- 独自の偽造防止シリコン技術
- 独自のセキュアブートおよびハードウェア トラストアンカー テクノロジーの活用
- 米国の C-TPAT（および OCONUS が提案するもの）、FIPS、コモンクライテリア、IPv6、DCE、USG v6 などの認定や認証
- 上述したシスコの「意識向上キャンペーン」の取り組みにより特定された偽造トレンドに基づく、製品の継続的な強化

D. サポート終了および廃棄プロセス：

シスコは、包括的な一連の物理および論理的なセキュリティのプロセスを導入し、以下の方法で、余剰、旧式、またはサポート終了と見なされる電子部品を確認します。

- 選択した一連のサプライヤによる電子部品の制御および監視
- 偽造品作成のための転用を最小限に抑える方法で電子部品を収集、分解、破壊
- 電子部品の不注意による損失または意図的な除去を回避するための調整プロセスを適用

E.　セキュリティインシデントの通信およびアラート：

シスコは、セキュリティの脆弱性と、お客様、サプライヤ、チャネルパートナー、流通パートナーによる偽造品の疑いに関する報告を促す取り組みを長年にわたって行ってきました。公開されているすべての脆弱性を確認するだけでなく、専任のグローバルチームがセキュリティの脆弱性のアラートと修正を調査し、タイムリーに公開します。シスコ セキュリティアドバイザリ センターを参照してください。

シスコの偽造電子部品検出および防止システムは、この包括的な階層型のアプローチで構成されています。さらにシスコは、ICT 業界全体の偽造電子機器部品の削減に力を入れている多くの国際規格に貢献しています（例：ISO 27036、オープングループの信頼できる技術パートナー規格（Open Group Trusted Technology Partner Standard）– ISO 20243）。