IoTのセキュリティ保護に関するBSAの原則

BSA会員企業は、世界のソフトウェア業界で信頼されるリーダーとして、IoT（モノのインターネット）セキュリティの進歩を含めIoTイノベーションの最前線に立っています。BSAは、責任あるリスクベースのアプローチを含む、IoTの信頼構築のための以下の原則を支持します。

1. **IoTエコシステムの多様性と複雑さに対応する。**IoTエコシステムの複雑さと多様性を総合的に考慮し、システムの各部分が果たす役割と、それらの部分がどのように相互作用するかを認識し、そのような複雑さに対応できて技術的中立性を保った柔軟な政策を策定する。

2. **重要な概念と要件を明確に定義する。**「IoT」や「IoTデバイス」など、IoTセキュリティに関連する主要な概念と要件を明確に定義する。

3. **デバイスだけでなく、IoTエコシステム全体を保護する。**IoTテクノロジー全体に導入されたソフトウェア、ファームウェア、ハードウェアなどを考慮し、高度なネットワークベースのセキュリティ対策の開発と適用を妨げるデバイス中心の政策を回避することで、信頼と安全に対するリスクベースのアプローチを推進する。

4. **コンシューマー向けIoTと産業用IoT（IIoT）を区別する。**すべてに適合する単一のアプローチを追求するのではなく、コンシューマー向けIoTおよびIIoTテクノロジーによってもたらされるさまざまなリスクに対処する。コンシューマーデバイスの政策では、デバイス内でのセキュリティの構築を優先的に行う必要があり、産業用ユーザーには、独自の複雑な運用環境に合わせてセキュリティ対策を調整できる柔軟性が必要である。

5. **業界のベストプラクティスに基づいて構築される。**業界を率いるリーダーたちの専門知識を取り入れ、広く受け入れられかつ業界で開発されたリスクベースのIoTセキュリティのベストプラクティスを取り入れることで、IoT市場全体のセキュリティを強化する必要がある。

6. **IoTライフサイクル全体を通じたセキュリティを奨励する。**IoTライフサイクル全体を通じたセキュリティを促進するために、脆弱性開示（CVD）プロセスとエンドオブライフ（EOL）・ポリシーを自発的に確立するよう企業を奨励する。

7. **マルチステークホルダー・プロセスを採用する。**複数の利害関係者によるプロセスを活用して業界と協力し、既存の、合意に基づくガイドラインをもとに、IoTセキュリティのベストプラクティスを開発する。

8. **国家および国際的な政策の調和を図る。**IoTセキュリティ政策を、可能な限り、世界中で進行中の他の同様の取り組みに沿うよう調整する。

9. **国際的に認められたIoT標準の開発と使用をサポートする。**IoTセキュリティ政策はそれが存在する場所にかかわらず、世界的、自発的、そして合意に基づく基準と一致したものでなければならず、国際的に認知された新しいIoTセキュリティ標準の開発をサポートする。

10. **必要に応じて適切にベースラインセキュリティ要件を設定する。**必要に応じて、コアセキュリティ機能を広く受け入れられている国際標準に準拠させる。これら国際標準は、最新のテクノロジーとセキュリティプラクティスに対応するべく定期的に更新される。

11. **セキュリティをIoTの取得に統合する。**調達プロセスの部門や機関を奨励し、業界主導の、自発的な、合意に基づく国際ガイドラインに基づいて、安全で相互運用性が高く、拡張性に優れた資産向けIoTソリューションを優先させる。

12. **IoTをインシデント対応に含める。**IoTの考慮事項をインシデント対応計画に統合する。これには、IoTのインシデントや緊急対応の政策が含まれる。