Microsoft Corporation
Japan Parameter Sheet
Cryptographic Features
Microsoft Global Trade Compliance
Date issued: 14 February 2020

Visual Studio 2015

暗号関連パラメータシート（日本）
マイクロソフト・グローバル・トレード・コンプライアンス

This parameter sheet applies to all versions and editions of Visual Studio 2015 and Visual Studio Express 2015 and all previous versions and editions of Visual Studio and Visual Studio Express.

Current editions of Visual Studio are:

- Visual Studio 2015 Community
- Visual Studio 2015 Professional
- Visual Studio 2015 Enterprise
- Visual Studio 2015 Test Professional
- Visual Studio 2015 Team Foundation Server

Editions of Visual Studio Express are:

- Visual Studio Express 2015 for Web
- Visual Studio Express 2015 for Windows
- Visual Studio Express 2015 for Desktop
- Visual Studio Team Foundation Server Express 2015

This parameter sheet covers for all additional software and tools related to or included with Visual Studio such as ASP .Net Development Server, Team Explorer, Team Explorer Everywhere for TFS, all versions of .Net Framework, Intellitrace, Remote tools, Visual C++ redistributables, and various SDKs and DDKs, including third party tools that are part of Visual Studio such as InstallShield and Crystal Reports.

1. 暗号機能 / Cryptographic Capabilities

暗号機能は認証、デジタル署名又は複製することを防止されたプログラムの実行以外の目的を有するか。 The cryptographic capabilities are for purposes other than certification, digital signature, or execution of a copy-protected program.	☐ NO	☒ YES

暗号機能は本製品に搭載されているものか。[1] The cryptographic capabilities are self-contained in the product	☒ NO	☐ YES
暗号機能は次のいずれかに該当するものか。 The cryptographic strength exceeds the following: A. 対称アルゴリズムを用いたものであって、アルゴリズムの鍵の長さが 56 ビットを超えるもの Symmetric algorithms with key length exceeding 56 bit A. 非対称アルゴリズムを用いたものであって、 (a) 512 ビットを超える整数の素因数分解（RSA 等）に基づくもの、 Asymmetric algorithms based on factorization of integers in excess of 512 bits (e.g. RSA), or (b) 有限体の乗法群における 512 ビットを超える離散対数の計算（Diffie-Hellman 等）に基づくもの、 Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g. Diffie-Hellman), or (c) 上記に規定するもの以外の群における 112 ビットを超える離散対数の計算（楕円曲線上の Diffie-Hellman 等）に基づくもの Discrete logarithms in a group other than (B.b) in excess of 112 bits (Diffie-Hellman over Elliptic Curve), or (d) 格子に関連する最短ベクトル又は最近接ベクトル問題（NewHope、Frodo、NTRUEncrypt、Kyber、Titanium 方式を含む。）に基づくもの Shortest vector or closest vector problems associated with lattices (e.g., NewHope, Frodo, NTRUEncrypt, Kyber, Titanium), or (e) 超特異楕円曲線の同種写像の探索（超特異同種写像鍵カプセルを含む。）に基づくもの Finding isogenies between Supersingular elliptic curves (e.g., Supersingular isogeny Key Encapsulation), or (f) ランダムな符号の復号（McEliece、Niederreiter 方式を含む。）に基づくもの Decoding random codes (e.g., McEliece, Niederreiter).	☐ NO	☒ YES

2. アルゴリズム及び鍵長 / Algorithms and Key Lengths

[1] API を通じて OS から提供される場合は除く。/As opposed to that provided by the Operating System through API.

アルゴリズム/ Algorithm	鍵長/ Key Length	プロトコル/アプリケーション/コメント Protocol/Application/Comment
RC2, RC4	40-128	Visual Studio does not contain implementation for those algorithms but it is a tool that allows developers to develop applications that may use cryptography from the operating system or the .NET Framework or non Microsoft libraries. Those listed algorithms are those from the Windows operating system and the .NET Framework crypto classes (as per Windows 10 and .NET Framework 4.6). Recent versions of Visual Studio ship with the .NET Framework and the cryptography classes, and SQL Server Compact and Mobile editions which support encryption of the database file with AES-128. Additionally the product may use SSL/TLS when communicating with servers through secure channels, and Windows DPAPI to protect passwords used in authentication.
DES, 3DES	56, 168	
AES	128, 192, 256	
MD2, MD4, MD5	128	
SHA-1, SHA-2	160, 256, 384, 512	
RSA	512-16384	
DH	1024-4096	
HMAC-SHA1, HMAC-SHA2	160, 256, 384, 512	
DSA_SIGN	1024	
ECDH	NIST P-256, P-384, P-521 curves, CryptoAPI/CNG	
ECDSA	NIST P-256, P-384, P-521 curves, CryptoAPI/CNG	

3. 市販暗号プログラム該当性 / Mass Market Consideration

製品が以下の要件を満たすものかどうか。(The product satisfies the following requirements):

1) 購入に際して何らの制限を受けず、(i) 店頭において(ii) 又は郵便、信書便(iii) 若しくは電気通信の送信による注文により、販売店の在庫から販売されるもの又は使用者に対し何ら制限なく無償で提供されるもの Generally available to the public by being sold, without restriction, from stock at retail selling points by means of (i) over-the-counter transactions, (ii) mail order transactions, (iii) telecommunication transactions, or available free without restriction;	☐ NO	☒ YES
2) 暗号機能が使用者によって変更できないもの The cryptographic functionality cannot easily be changed by the user ;	☐ NO	☒ YES
3) 使用に際して供給者又は販売店の技術支援が不要であるように設計されているもの Designed for use without technical support by the supplier or the distributor	☐ NO	☒ YES

4. 該非判定 / Conclusion

上記 3.に照らして、市販暗号プログラムと判断される結果、適用法上、規制非該当となるプログラムか。 In light of 3 above, is the software a mass-market crypt program that is not controlled under applicable law?	☐該当 NO	☒非該当 YES