Microsoft Corporation
Japan Parameter Sheet
Cryptographic Features
Microsoft Global Trade Compliance
Date issued: 13 February 2020

SQL Server Compact

All versions

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

Parameter sheets apply to all versions of declinations of SQL Server Compact Edition:
SQL Server Compact 4.0
SQL Server Compact 3.5 and 3.5 SP1 and SP2
SQL Server Compact 3.1
Previous versions

1. 暗号機能 / Cryptographic Capabilities

暗号機能は認証又はデジタル署名以外の目的を有するか。 The cryptographic capabilities are for purposes other than certification or digital signature	☐ 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 B. 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	☐ NO	☒ YES

[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.

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).		

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

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
SHA-1 3DES AES	160 168 128	Database file encryption.

3. マスマーケット該当性 / 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) 購入に関して何らの制限を受けず、店頭において又は郵便、信書便若しくは公衆電気通信回線に接続した入出力装置（電話を含む。）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の制限なく無償で提供されるもの（外国でのみ販売又は無償で提供されるものについては、当該販売の態様若しくは無償	☐ NO	☒ YES

で提供されることを書面で確認できるものに限る。） 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) through communication devices (including telephones), or available free without restriction;		
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

省令第 21 条第 1 項に該当するか。 Is the software controlled under the Japanese law in light of the results of 1 and 2 above?	☐ 該当 YES	☒ 非該当 NO

（該当と判定された場合 <If yes>）

貿易外取引等省令第 9 条第 2 項第 14 号イ又はロに基づいて取引の許可が不要となるプログラムか。 Can the software be exported without prior government approval under the mass-market exemption in light of 3 above?	☐ 許可必要 NO	☐ 許可不要 YES