



高度なデジタルセキュリティ ステンレススチールの耐久性を備えた eCash用トークン

キーリングに適したコンピュータチップベースの
eCashソリューション、10年の寿命を提供

電気・ガスメータ
パーキングメータ
公共交通システム
事務機器

自動販売機
アーケードゲーム機器
オンライン取引
バス・タクシーなどへの燃料補給

MAXIM

eCashのニーズに最適な製品

世界で唯一固有の口座識別子を備えたiButton

最もシンプルなiButtonであるDS1990Aは、固有64ビットROMアドレスのみで構成されています。この唯一のIDはオンラインシステムに使用されているエンボス英数字、バーコード、または磁気帯の口座識別子を持つプラスチックカードのような、耐久性及び信頼性の低い手段を置き換えます。

パスワードで保護されたアクセスを持つiButton

DS1991またはDS1977を使って、口座残高のようなセキュアデータへのアクセスを制限することができます。これらのiButtonは、ホストに読み込みまたは書き込みの動作に、パスワードを要求します。DS1991は3つのサービスデータページを備えており、1個のデバイスで3つの完全に独立したサービスプロバイダに対応することができます。各48バイトサイズのセキュアメモリページは、それぞれ固有の64ビットアクセスパスワードとサービスIDをもっています。さらに、保護されていない64バイトサイズのスクラッチパッドメモリが中間バッファとして動作します。正確なパスワードがあれば、スクラッチパッドから適正なセキュアメモリページにデータをコピーすることは、接続が断続的であっても、非常に信頼性の高い書き込み動作となります。このような信頼性の高い動作は、金額の残高が破損なしで確実に更新され、電子キャッシュの損失が発生しないようにするために不可欠なものです。より大きなメモリが必要であれば、DS1977を使って最大32kBまでのデータを保護することができます。

「チャレンジ・アンド・レスポンス(呼び掛け/応答)」の認証方式を備えたiButton

さらに優れたセキュリティを提供するために、セキュアハッシュアルゴリズム 1 (SHA-1)とよばれるISO/IEC 10118-3標準ハッシュ法アルゴリズムに基づいたチャレンジ・アンド・レスポンス(呼び掛け/応答)方式のセキュアメモリiButtonを提供しています。チャレンジ・アンド・レスポンス方式は2人の当事者間で共通の機密コードを共有することを可能にし、さらに通信中にその機密コードを決して明かさないので、セキュアデータの安全なやりとりを可能にします。内蔵512ビットSHA-1エンジンが、iButtonに保存された情報に基づいて160ビットのメッセージ認証コード(MAC)を演算するために動作させることができます。

チャレンジ・アンド・レスポンス方式iButtonは実証されたアルゴリズムを使い、高度な攻撃を阻止する最高のセキュリティ機能を提供します。これらのデバイスは、コピーアタック、リプレイアタック、盗聴アタック、A-B-Aアタック、及びエミュレーションアタックなどを含む数多くの既知のロジカルセキュリティアタックを阻みます。詳細に関しては japan.maxim-ic.com/AN1201 の白書8：1-Wire SHA-1の概要をご覧ください。

DS1961S—SHA-1エンジン付1kb EEPROM

1kbのアプリケーションメモリを備えたDS1961Sは、SCUへ真正であることを証明するために内蔵SHA-1エンジンと連動して使われる1個の64ビット機密コードを保存します。同様に、SCUはDS1961Sへデータを書き込む前に真正証明を要求されます。このセキュリティの機構は、相互認証と呼ばれ、eCashアプリケーションに最適です。口座の残高は誰でも読むことができますが、認可されたSCUのみがトランザクションを実行し、保存されている値を変更することができます。

DS1963S—SHA-1エンジン付4kb NV RAM

DS1963Sは、4kb NV RAMを装備し、最大7つの異なったアプリケーション、またはサービスプロバイダをサポートし、それぞれ他のサービスプロバイダに明かされることのない64ビットの機密コードを持ちます。このiButtonの中の特殊カウンタは、残高のような過去のまたは現在のデータパターンがデバイスから抽出され、後で不正に再書き込まれないこと保証します。このようにDS1963Sはすべてのデータのインスタンスを一意として扱います。NV RAMテクノロジーは、力づくの物理的な攻撃をほとんど不可能にします。

Java駆動の暗号法を備えたiButton

当社では、最高レベルのセキュリティニーズを満たすために、DS1955B Java™駆動暗号法のiButtonを提供しています。Java Card 2.0適合の仮想マシン、6kBのNV RAMメモリを持ち、FIPS PUB 140-1適合としてNISTの検証済みです。セキュリティレベルが非常に高いため、このデバイスを使ってインターネットを介して郵便切手をダウンロードしたり、汎用プリンタを使って郵便切手を印刷することを米国政府は認可しています。お札を印刷するのと同じことです！さらに、PKIチャレンジ・アンド・レスポンス認証方式を使い、ホームページ情報へのアクセス権限を与えることができます。他の人たちが書類の作成元を確認できるように書類に署名して承認することも可能です。

JavaはSun Microsystemsの商標です。



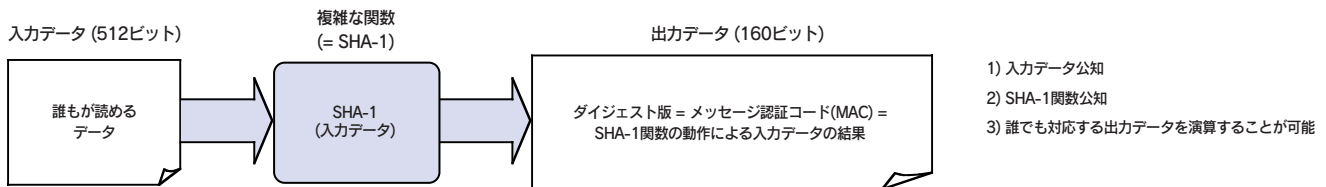
SHA-1 iButtonで優れたeCashシステムが実現できる理由

eCashのトークンは現金と同等

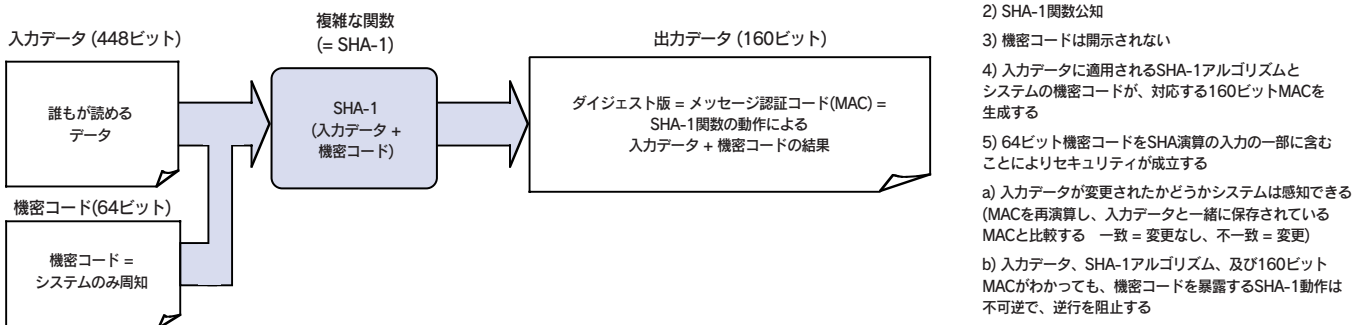
必要条件	現金	eCash iButton
真正証明の提供	一般周知の外観、材質の感触、印刷の質	複雑で不可逆的な数学アルゴリズムと64ビット機密コードを使って電子的に認証
変更、偽造が困難であること	粗雑な変更は明白にわかる; 高度な印刷工程、材料の入手が困難、法的な制裁などの理由で偽造することは困難/危険である	複雑なアルゴリズムと64ビット機密コードにより、データの変更、またはデバイスが複製/模造されたものでないことを証明
暗号化 対 デジタル署名	現金の価値を直接視認して、一般的に真正の判断をすることが可能。貨幣の価値を「暗号化」する必要なし(例えば価値を機密コードにする)	誰でもeCashトークンの価値を直接読取ることが可能。現金と同じように、変更を加えることを不可能にするのが大切で、価値を暗号化する必要なし

優秀な数学上の特性を備えたISO標準SHA-1アルゴリズム

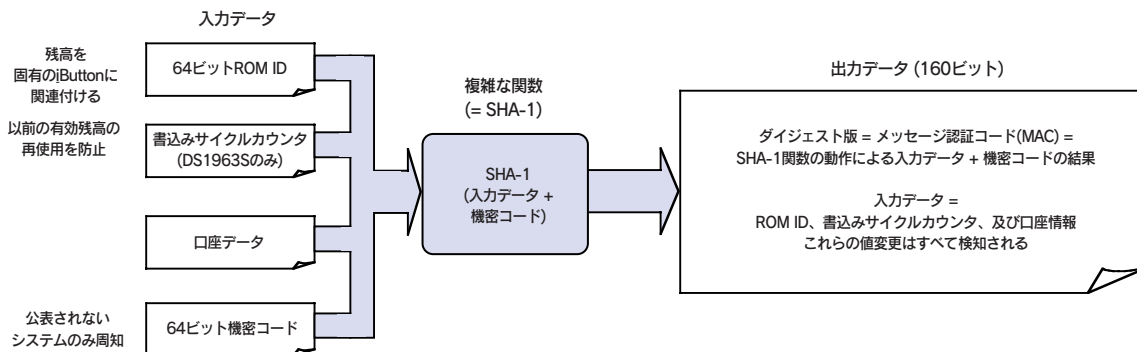
一般例



特殊(セキュア)な例



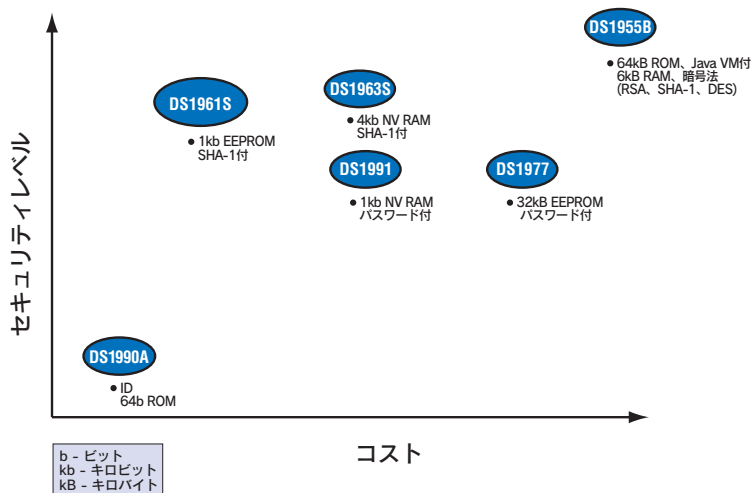
SHA-1 iButton



iButton eCash製品の選択ガイド

**iButton製品の
様々な
セキュリティ
レベル**

iButtonは、広範囲なセキュリティのレベルを装備しているため、各アプリケーションに最適な保護を提供します。



必要条件	適用する品名	備考
固有のIDのみ必要	DS1990A	実行が最も容易; クレジットカードシステムのように独自の口座番号を必要とするだけの簡単なシステムに最適
ユーザアクセス認証用のパスワード保護付メモリが必要	DS1991L DS1977	良好のセキュリティを提供し、実行が容易。顧客によっては、デバイスIDを暗号入力パラメータの1つとして、サービスデータをさらに暗号化する。DS1991Lは3つの独立したサービスのサポートが可能
チャレンジ・アンド・レスポンス(呼び掛け/応答)方式の認証が必要。妨害に対して機密コードの安全を保護したい	DS1961S DS1963S	静的パスワードのアプローチよりも高度なセキュリティを提供。DS1961Sは同じアクセス機密コードを共有する4つのサービスをサポート。DS1963Sは別個の機密コードを持った7つの独立したサービスをサポート
強化された暗号化のサポートが必要(1024ビットキー)。PKIのサポートが必要。	DS1955B	最高レベルのセキュリティを利用可能 FIPS PUB 140-1適合
iButtonを使ったeCashシステムを知るためのスターターキット	DSECASH	このキットでSHA-1ベースのiButtonとなるDS1961SおよびDS1963Sのスピード、信頼性、およびセキュリティのデモを行うことができます。デビット/クレジットを行い、完全なeCashシステムを構築する上で必要なすべてのハードウェアとソフトウェアが含まれます。

ターンキーシステム利用可能

当社の公認ソリューションデベロッパ(ASD)は、多くのeCashアプリケーションに使えるターンキーiButtonをすでに開発しています。さらに、これらのデベロッパはカスタム化されたiButtonソフト/ハードウェアソリューションを設計することもできます。当社のパートナー及び製品に関してはjapan.maxim-ic.com/ibutton/solutions (英文)をご覧ください。



インタフェースはシンプルで低コスト

ワンタッチインタフェース

どうやってjButtonと通信するのでしょうか？jButtonはあらゆる電子機器へのインタフェースが簡単です。一瞬の接触で、jButtonとPC、PDA、またはマイクロコントローラの間を最大142kbpsで情報が伝送されます。ただ単にjButtonをポートアダプタに接続されているBlue Dot™レセプタまたはプローブに接触させるだけです。当社では、USB、シリアル、およびパラレルポート用に低コストアダプタを提供しています。



標準的なjButtonプローブは簡単で、堅牢です。また不正確な位置あわせや電気抵抗にも対応できます。カードベースのシステムは、カードスロットが荒い取扱いで容易に破損してしまう複雑な電子/メカ式リーダを必要とし、数多くの電気接続が常に完全にクリーンな状態で保持されなければならず、また正確な位置あわせを必要とするので、保守が難しく、定期的が必要となります。

jButtonは、断続的な接続を想定して設計されています。心配なくいつでもSCUからjButtonを取り外せます。jButtonが再度プローブポイントに接触すると、中断されていたトランザクションは問題なく回復され、データのロスまたは破損が起こることなく、トランザクションが終了します。

jButtonのシステムは、非接触型のカードベースシステムとよく比較されます。非接触型システムのリーダは、接触型カードベースのリーダと比べかなり複雑にできています。これは、コストがかかる上に、異なった周波数または使用される変調方法によって相互操作の問題が発生する可能性があります。

無償のソフトウェア開発ツール

様々なプラットフォームと言語選択プログラミングに対応するjButtonおよび他の1-Wireソフトウェアの開発キットは、ウェブサイトから無料でダウンロードすることができます。多数のアプリケーションノートや白書を参考することによって、開発の負担を減らし、失敗のない開発を行うことができます。

プラットフォーム	リソース	説明
Windows® 32ビット (95、98、NT、2K、ME、XP)	1-Wire SDK	プログラミング言語独立ライブラリは、従来型API* (TMEX)及びウィンドウズCOMインタフェースの1-Wireアダプタの全種類をサポート
Cコンパイラ付のあらゆるプラットフォーム	1-Wire パブリックドメインキット	携帯Cライブラリ。シリアルポートとDS2480Bブリッジ、またはカスタム1-Wireインタフェースをサポート
あらゆるJavaプラットフォーム	Java用1-Wire API	携帯Javaライブラリ。シリアルポートとDS2480Bブリッジ、またはカスタム1-Wireインタフェースをサポート
マイクロプロセッサ	<ul style="list-style-type: none">アプリケーションノート 126* (1-Wire用I/Oポートピン)アプリケーションノート 192* (1-Wire用シリアルポート + DS2480Bのブリッジ)1-Wireパブリックドメイン(PD)キットのI/Oポート組み立て例を参照	マイクロプロセッサに1-Wireポートを加えるための書類。組み立て例もいくつか提供。マイクロプロセッサにCコンパイラがある場合、1-Wireパブリックドメインコードの使用が可能

*入手可能な全APIの概要については、アプリケーションノート155：「1-Wireソフトウェアリソースガイド」を参照してください。すべてのjButton及び1-Wireソフトウェアキットに関してはjapan.maxim-ic.com/ibutton (英文)をご覧ください。

Blue DotはDallas Semiconductor Corp.の商標です。
WindowsはMicrosoft Corporationの登録商標です。













iButton—eCashトークンだけにとどまらない製品群

iButtonの製品群には、eCash、アクセス制御、ガードツアーモニタ、データ管理の保守と検査、デバイス及びソフトウェアの認証、温度データのロギングなど、アプリケーションのすべてのニーズを満たす20以上の異なる製品があります。

製品一覧

	品名	説明		
アドレス番号のみ	DS1990A	64ビットROM ID		
NV RAMメモリ	DS1992/3/5/6L	1kb/4kb/16kb/64kb NV RAM		
EEPROMメモリ	DS1971/3/7	256ビット/4kb/32kB EEPROM		
EPROMメモリ	DS1982/5/6	1kb/16kb/64kb EPROM		
パスワード保護付セキュアメモリ	DS1991L/DS1977	3個の384ビットパーティションNV RAM/1個の32kBパーティションEEPROM		
チャレンジ・アンド・レスポンス式セキュアメモリ	DS1961S	SHA-1付1kb EEPROM		
	DS1963S	SHA-1及びカウンタ付4kb NV RAM		
リアルタイムクロック	DS1904/DS1994L	RTC/4kb NV RAM付RTC		
温度センサ	DS1920-F5	リーダとの接触で現在の温度収集が可能。 デジタル温度計、精度±0.5°C (-55°C~+100°C)		
温度データロガー	品名	温度範囲	最高精度	データログサイズ
	DS1921G-F5	-40°C~+85°C	±1°C (-30°C/+70°C)	2kポイント
	DS1921H-F5	+15°C~+46°C	±1°C	2kポイント
	DS1921Z-F5	-5°C~+26°C	±1°C	2kポイント
	DS1922L-F5	-40°C~+85°C	±0.5°C (-10°C/+65°C)	4k/8kポイント
	DS1922T-F5	0°C~+125°C	±0.5°C (+20°C/+100°C)	4k/8kポイント
温度/湿度データロガー	DS1923L-F5	-20°C~+85°C	±0.5°C、5% RH	4k/8kポイント

アクセサリ一覧

通信ポートアダプタ		
	DS9490R	1-Wire USBアダプタ：1-WireからUSBへのインタフェース。RJ-11インタフェースですべてのリーダ/プローブに接続。
	DS9490B	USB iButtonホルダ/ドングル：1-WireからUSBへのインタフェース。iButtonをデバイスへ挿入。
	DS9097U-S09/009/E25	ユニバーサル1-Wire COMポートアダプタ：1-WireからRS-232 COMポートへのインタフェース(DB9)。RJ-11インタフェースですべてのリーダ/プローブに接続。009バージョンにはID用のDS2502があり、E25バージョンにはEPROM iButton書き込み用12V電源ポートを備え、DB25パッケージで提供。
	DS1410E-001	1-Wireパラレルポートアダプタ：1-Wireからパラレルポートへのインタフェース。iButtonを直接挿入または、DS1402D-DB8もしくはDS1402BP8と併用。
プローブ/レセプタ(リーダ/ライタインタフェース)		
	DS1402D-DR8/DB8	Blue Dot レセプタケーブル：iButtonリーダ/ライタインタフェース。iButtonは瞬間的な接触でBlue Dotインタフェースを介して通信、または連続接続用にBlue Dotへのはめ込みが可能。DR8はRJ-11インタフェースを持ち、DB8はボタンインタフェースを持つ。
	DS1402RP8/BP8	iButtonタッチ&ホールドプローブケーブル：iButtonリーダ/ライタインタフェース。iButtonは瞬間的な接触でプローブを介して通信、または連続接続用にプローブへのはめ込みが可能。DR8はRJ-11インタフェースを持ち、BP8はボタンインタフェースを持つ。
	DS9092GT	iButtonハンドヘルドワンド。iButtonと自己位置合わせが可能に形作られたiButtonプローブ内蔵のプラスチック製ワンド。触覚フィードバックを提供。ワンドは10cmのハンドルと終端にRJ-11ジャック付の1mのケーブル。
	DS9092T/L	パネル取付け用プローブ。Tバージョンは触覚フィードバック、LバージョンはLEDを装備し、野外用途に向く。
	DS1402D-041	組込みタッチ&ホールドアプリケーション向けBlue Dotプローブコンポーネント。
iButtonマウント		
	DS9093Ax/F/N	キーフob：iButtonをキーチェーンにつけて便利に持ち運び可能。3バージョン、5色有り。
	DS9093S/P	ウォールマウント：ほとんどの表面にiButtonを安全に装着することが可能。2種類のバージョンで提供。
	DS9096P	iButton接着パッド：iButtonを何にでも簡単に装着することが可能。

iButton®
Touch the Future!



WHAT'S NEW?

Overview

- What is an iButton?
- Applications
- Brochures
- Videos

iButtons

- ID Only
- Memory
- Real-Time Clock
- Secure
- Temperature

Accessories

- Readers & Adapters
- Mounting Options
- Starter Kits

Sales

- Direct
- Buy Online
- Partners
- Distributors
- Samples
- Trade Shows

Solution Partners

- Solutions Search
- Become a Partner

Contact Us

- Contacts and Support
- Sales Information

Technical Support

- Software Developer's Tools
- Data Sheets
- Application Notes
- Support
 - FAQs
 - Discussion Groups
 - E-mail Updates
- Photo Library

Translations

- Chinese 简体中文
- Japanese 日本語

iButtonに関する最新情報は
japan.maxim-ic.com/ibutton (英文)
をご覧ください。



マキシム・ジャパン株式会社
〒169-0051
東京都新宿区西早稲田3-30-16
ホリゾン1ビル
TEL : 0120-231690
FAX : 0120-231691

まずはiButton
スターターキットの
DSECASHから
始めましょう。