



RSA

White Paper

**認証トークンの信頼性と耐久性が
セキュリティ対策を成功へと導く**

認証トークンの信頼性と耐久性は、企業のセキュリティにとって極めて重要な要素です。ハードウェア・ベースの認証トークンは、認証時にユーザーが本物かどうかを確認する重大な責任があります。また、ユーザーが製品を簡単に問題なく利用できることも重要視されます。有効期間中は認証用に常時活用されるトークンですが、正しく扱われないことや、過酷な環境で利用されることも少なくありません。

RSA セキュリティは最も信頼性の高い認証トークンの開発に注力し続けています。本書では、RSA が実施している厳格な信頼性テストについて概説します。このテストは、企業のさまざまなユーザーが認証 トークンを利用するときに想定した極めて厳しい条件を RSA SecurID が満たしていることを確認するためのものです。

セキュリティ対策成功の鍵 ～トークンの高信頼性～

二要素認証を採用している企業では、認証のための便利で使いやすいトークンをユーザーに提供し、社内情報やアプリケーションへのアクセスに活用して、企業リソースを安全に利用させることが可能です。ハードウェア・トークンはキーホルダーに簡単に付けられるサイズに設計されており、大半のトークンは使用期間が3年から5年間あります。最も厳しい条件下であっても、継続的に使用できる設計を施している必要があります。

トークンに障害が発生した場合、ユーザーの生産性が低下するだけではありません。ヘルプ・デスクのコストが増加し、予備のトークンを大量に在庫する必要があり、さらに配布するという負担が発生します。つまり、効果的かつ生産的にセキュリティ対策を実施する上で、トークンの信頼性は重要な鍵です。また、トークンの信頼性の高さは、セキュリティ対策にかかる総所有コスト(TCO)の削減にも不可欠な要素です。

トークンは、一時的にでも過酷な状況下で使用される場合があります。その結果、トークンが破損してしまうと、ユーザーは社内情報や他のリソースにアクセスできなくなります。過酷な条件のほとんどは予測が可能です。業界最高レベルの信頼性を保証するため、RSA は予測される環境下でトークンをテストしています。

例えば、極端な温度や湿度環境にさらされたり、航空機の貨物室で気圧の変化を受けたりすることが考えられます。あるいは、極端に振動や衝撃の強い状況に置かれたり、窓や机から落下したりする可能性もあります。ESD

(静電放電)もトークンの信頼性を脅かす問題の1つです。多忙なユーザーが毎日持ち歩いた場合に避けようのない衝突や傷、へこみに耐えられるような耐久性も非常に重要となります。

実生活で予測し得る不慮の誤用には、衣服のポケットにトークンを入れたまま洗濯機さらには乾燥機に投入してしまうユーザーもいるでしょう。車でひいたり、洗面台に落ちたり、ハード・ドライブの上に放置する可能性もあります。信頼性は設計の副産物ではなく、設計の目標です。

RSA セキュリティは、企業がセキュリティ・インフラとリソースの管理を簡素化できるよう、トークンの信頼性向上に重点を置いた投資を行い、結果として業界最高レベルの信頼性を実現しています。また、考え得る最悪の状況にも耐えられるよう設計されています。

RSA SecurID 認証トークンを採用した企業は、業界で最も信頼性の高いトークンを配布でき、社員の生産性を高められます。交換用トークンの配布にかかる負荷を削減でき、エンドユーザーに一貫性のある簡便な認証方法を提供しながら、セキュリティの確保にかかる全体的なコストを削減できるのです。

避けることができない過酷な使用条件

セキュリティ要員やITスタッフがどのような対策を講じても、利用者は厳しい環境下で認証トークンを使用してしまうでしょう。トークンは洗濯乾燥機にかけられたり、自動車のタイヤに轢かれたり、空港のセキュリティ・チェックで X 線を当てられたり、何日も何時間もキーホルダーにぶら下げられたり、凍えるほどの寒さやうだるような暑さの車内に放置される可能性があります。

しかし、企業がセキュリティ・インフラへの投資を最大限に活用するつもりであるならば、認証トークンはどのような条件においても正常に機能し続けなければなりません。

本ホワイトペーパーは、2 種類のハードウェア・トークンの信頼性テストについて、詳しく説明します。

RSA SecurID SID700

RSA SecurID SID700 は、小さなキー・フォブ型であらゆるキーホルダーに簡単に取り付けられるため、エンドユーザーにとって非常に携帯性が高い製品です。あらかじめ設定された使用期間の間 RSA SecurID アルゴリズムが 60 秒ごとに一意のコードを生成し、表示します。



RSA SecurID SID800

RSA SecurID SID800 は、業界が認めた SID700 の機能と SUN® Java®テクノロジー・ベースのスマート・チップを一体化した、USB 接続が可能な多機能デバイスです。

この認証トークンはあらゆる USB デバイスに差し込むことができ、いつでもどこでもアクセスが可能になります。また、デジタル署名とファイル暗号化証明書もサポートしています。パスワード情報が安全に保管されるので、多様なシステムやアプリケーションが存在し、さまざまな顧客ニーズが存在する環境に最適です。



トークンの信頼性・耐久性への投資

生活上の過酷な利用であっても製品の最大限の信頼性を保証するため、RSA は数百万ドルをかけて最高の設備を有する試験用研究所を設立しました。同研究所にはトレーニングを積んだ多くの信頼性テストの技術者が配置されています。研究所の一部の試験設備は、実社会の厳しい使用状況を再現するために作られています。

RSA では新たな認証トークンの開発にあたり、そのトークンが、RSA が求める信頼性・耐久性の要件を満たしていることを確認するためのテスト計画を策定しています。新製品はそのライフサイクルを通して、十分に検証された厳密な手順でテストされます。数的指標が入念に設定さ

認証トークンの高いセキュリティ強度

RSA SecurID の二要素認証ソリューションは、ユーザーが知っていること（Something You Know）、すなわちパスワードや PIN（暗証番号）による認証、そしてユーザーが持っているもの（Something You Have）、つまり、常に異なるコードを生成する認証トークンによる認証に基づいています。ユーザーは自分の PIN と RSA SecurID 認証トークンで生成された 6 桁または 8 桁の数字を組み合わせるだけで、RSA SecurID の技術で保護されるリソースにアクセスできます。

米国特許を取得している時間同期技術を基盤とする RSA SecurID 認証トークンは、ワンタイム（使い捨て）の認証コードを生成します。この認証コードは 60 秒ごとに変化します。使い捨てパスコードを使用することで、確実にユーザーを特定または認証できます。認証トークンのトークン・コードは、認証サーバーである RSA Authentication Manager と同期しています。PIN とトークン・コードを組み合わせで作られたパスコードが RSA Authentication Manager で認証された場合のみ、保護されているリソースへのアクセス権がユーザーに付与されます。

誤った PIN やパスコードが入力された場合は、アクセス拒否されます。この使いやすいセキュリティ・ソリューションは最新の認証技術を基盤にしており、高い信頼性があります。ユーザーは自分の Windows コンピュータから Web サーバーに至るまで、あらゆる対象にアクセスするときに認証トークンが必要となります。認証トークンを使用することで、社内ネットワークにリモートから安全にアクセスでき、企業のアプリケーションや情報にも無線で安全に接続できるようになります。RSA ではソフトウェア・ベースとハードウェア・ベースの 2 つの認証トークンを提供しており、広範な認証オプションを提供しています。

れ、すべてのテスト条件において追跡されます。また、軍用のサンプリング・レベルよりも厳しいテストが信頼性テスト全体で実施されます。軍用サンプリングとは米国防総省が購入予定のシステムの信頼性を確認するのに用いる方法で、サンプリングすべき量を提示するものです。

RSA はこのサンプリング量を上回る量(時には大幅に上回る量)をテストしています。サンプル量を大きくすることで、各ロットの信頼性レベルについてより正確な統計を把握できます。

米連邦政府がすべてのトークンに課している要件を除いて、トークンのテストに関するガイドラインは何も存在しません。RSA はこれまで培ってきた信頼性の高い認証トークンの開発技術・知識を基に、信頼性テストの方法論そして信頼性テストのための設備を継続的に向上させています。

同研究所が目標としているのは、実生活で想定される条件をシミュレーションすることで、予想される使用期間を通じて(さらには使用期間を過ぎても)すべてのロットのトークンが問題なく実環境で使用されるようにすることです。実施されるテストは次のように分類できます。

- 気温、湿度、高度
- 振動、衝撃、落下、転倒
- 静電放電(ESD)
- 耐久性

RSA SecurID SID700 と RSA SecurID SID800 に対して実施される詳細な信頼性テストを理解いただくため、以下のセクションでは最も過酷な条件下で定期的 to 実施される信頼性テストの一部を例に挙げて説明します。

気温、湿度、高度のテスト

RSA の品質保証(QA)テストは、トークンの各ロットを大量にサンプルとしてテストを実施し、極端な温度、湿度、高度の条件下でも機能し続けることを確認します。実際に行われているテストの一部の例を、以下に記します。

信頼性テストは、極端に高い温度条件と低い温度条件という両極端で実施されます。

高温条件の一例が、砂漠で停車した自動車にトークンを置いたままにする場合です。また、ユーザーが冬のアラスカを訪れ、トークンを自動車に置いたままにする場合も考えられます。RSA の信頼性研究所では、トークンの各ロットを気温摂氏 65 度(華氏 149 度)の状態 で 96 時間テストし、極めて高い温度に置かれても正常に機能し続けることを確認しています。

上記のテストで使用されたトークンは、今度は摂氏マイナス 20 度(華氏マイナス 4 度)の状態 で 96 時間テストされ、寒い場所でも正常に機能することが確認されます。

温度差がある条件下もシミュレーションされます。昼間は非常に暑く夜間は非常に寒くなる砂漠地帯など、極端な高温と低温にトークンがさらされる可能性があります。温度衝撃テストでは、極端な高温と極端な低温が短時間に切り替わる状況をシミュレーションします。

このテストでは飛行機による急上昇と急降下もシミュレーションします。RSA はこのような極端な温度差を効率的にシミュレーションするためのテスト用の設備を独自に設計しています。

トークンの信頼性に影響を及ぼす可能性のあるもう 1 つの要素は湿度です。そこで、認証トークンに高湿度テストを実施しています。研究所では気温が摂氏 35 度(華氏 95 度)、湿度が 95%の状態 で連続 96 時間のテストを実施し、その後、温度と湿度を段階的に周囲条件まで下げていきます。このテストは、ハワイやアジア太平洋など湿度の高い地域のユーザーに対して、トークンの信頼性を保証するのに重要なテストです。

認証トークンは、航空機の貨物室で運ばれることもあるため、厳密な高度テストを実施しています。トークンは特別な環境施設内の真空容器に収容されます。

高度約 12,000 メートル(約 40,000 フィート)の状態と同じになるよう気温が周囲温度から摂氏 0 度(華氏 32 度)まで下げられ、12 時間置かれます。次に、摂氏 50 度(華氏 122 度)に上げられて 12 時間置かれます。

このテストでは、航空機による移動で想定される最も過酷な高度条件にトークンが耐えられるかどうかを試します。

振動、衝撃、落下、回転のテスト

RSA SecurID の認証トークンが極めて激しい振動、衝撃、落下、回転にさらされても正常に機能することを確認するため、詳細にカスタマイズされたテストを実施しています。機械的振動はトークンに発生する障害の一番の原因となる可能性があるため、振動テストを実施することで、激しい振動があってもトークンの構造的完全性が損なわれないことを確認します。これらのテストは、出荷や配送でトークンがさらされる条件をシミュレーションしています。

さらに、加速度を 15 Grms、周波数帯域を 10~2,000 Hz とし、3 つの軸それぞれについて 1 時間振動を加えるテストを実施します。このテストの後、トークンを目視で検査します。

機械的衝撃も、トークンに問題を発生させる原因になり得ます。実際の例としては、トークンが壁に叩きつけられた場合の衝撃を挙げることができます。

突然の衝撃にトークンが耐えられことを検証するために衝撃テストを実施しています。衝撃テストには、パルス時間.5 ms で 3500 Gs の衝撃を与えるテストなどがあります。また、これらのテストはトークンの各軸について実施されます。テスト後のトークンは目視で検査され、ハードウェアに一切の損傷がなく、正常に機能することを確認します。

トークンの扱いで過失がある場合、最も一般的なのは、おそらく落下でしょう。使用期間中にトークンが落されるか否かということは重要ではなく、落される回数や高さに対する耐久性を確認することが重要です。

そこでさまざまな高さからハードウェア・トークンが落される状況をシミュレーションし、詳細な落下衝撃テストを実施しています。各テストでは、トークンの各軸について落下の衝撃を測定します。また、ランダムに落下させるテストも実施します。これは、特定の軸への影響ではなく、落下の結果を測定するためのテストです。デスクから落した場合、ポケットから落した場合、階段から落した場合などをシミュレーションするため、91.44 cm (36 インチ)、121.92 cm (48 インチ)、152.4 cm (60 インチ)の高さからそれぞれトークンを落します。さらに、同じテストを異なる落下面(タイル、絨毯、コンクリート、など)でも実施しています。

トークンは、ポケットやバッグに入れて運ばれたり、加重されたり、収納時に他の物とぶつかったりすることは避けられません。そこで RSA は、厳密な回転テストを実施します。回転テストの目的は、使用上で最も極端な状況をシミュレーションすることにあります。ユーザーがトークンを衣服のポケットに入れたまま、乾燥機にかけてしまう可能性さえあります。

そこで研究所では、このような衝撃をシミュレーションするためにカスタム設計され、小さな衣類乾燥機によく似た回転テスターを使用します。

六角形の回転テスターにトークンを置き、一緒に小銭、トークンと同じキー・リングに付けられる可能性が高い一般的な鍵を複数、投入します。このドラムが回転すると、トークンは小銭や鍵と衝突します。このテストは 1 時間、2 時間、4 時間、6 時間継続されます。小銭や鍵と一緒にドラムで回転したトークンは目で検査され、機械的な損傷がないこと、正しいトークン・コードを表示していることが確認されます。

静電放電(ESD)のテスト

ESD とは、ある物体から別の物体へと電子が移動することで、一般的には「静電気」や「静電気ショック」と呼ばれます。半導体は ESD に対して敏感であるため、小さくて高機能な RSA のトークンをテストして、さまざまなレベルの ESD に耐えられることを確認する必要があります。絨毯の上を歩いたりペットと遊んだりするだけでトークンは、ESD にさらされます。空中放電と表面放電の両方についてトークンをテストします。テスト対象の各トークンは、さまざまな ESD 電圧レベルで 26 箇所を ESD ガン(静電気試験器)で撃たれます。

ESD とは、ある物体から別の物体へと電子が移動することで、一般的には「静電気」や「静電気ショック」と呼ばれます。半導体は ESD に対して敏感であるため、小さくて高機能な RSA のトークンをテストして、さまざまなレベルの ESD に耐えられることを確認する必要があります。絨毯の上を歩いたりペットと遊んだりするだけでトークンは、ESD にさらされます。空中放電と表面放電の両方についてトークンをテストします。テスト対象の各トークンは、さまざまな ESD 電圧レベルで 26 箇所を ESD ガン(静電気試

験器)で撃たれます。

また、トークンが通常保管されるのは放射電磁波耐性がある物質の近く(ハード・ドライブの上やノート PC の上など)です。研究所では、トークンを振幅変調の高周波磁場に置き、放射電磁波耐性についてこれらのトークンをテストします。このテストでは、電磁環境に対するトークンの耐性を確認します。また、空港のセキュリティ監視システムを想定した X 線電磁界でもトークンをテストします(なお、シミュレーションでは空港に設置されているものよりもはるかに強力な X 線電磁界を使用しています)。

耐久性のチェック

RSA では、トークンが日常の使用だけでなく誤用にも耐え得ることを確認するため、詳細な耐久性テストを実施しています。認証トークンは、キー・リングに付けられて持ち運ばれる可能性が高いため、テストではトークンを数年間持ち運んだ場合の状況をシミュレーションします。キー・リングで遊ぶユーザーも少なくありません。その場合、トークンは何度も回転されたり、叩きつけられたり、放り投げられたりします。

キー・リングを引っ張るテストでは、行き過ぎた誤用があってもキー・リングが壊れないかどうかを検証します。このテストはカスタマイズされたプル・テスター・プラットフォームで実施され、キー・リングからキー・フォブまたは接続されている USB 認証トークンが外れるまで力を加えていきます。最終的にキー・リングを壊す力が、RSA の設定している値をはるかに超過していることを保証するための測定が行われます。

また、キー・リングの回転摩耗テストを実施して、20,000 回転しても問題が発生しないことを保証しています。このテストは、使用期間を 5 年間として毎日 10 回以上回転する条件をシミュレーションするものです。さらに、取り付けられている鍵の重さをシミュレーションするために、回転中に力を加えます。

定期的実施しているテストで最も過酷なものは、おそらく自動車で轢くテスト「ラン・オーバー・テスト」です。ラン・オーバー・テストでは、自動車で轢かれてもトークンに問題がないかを検証します。トークンを舗道に置き、自動車

のタイヤで轢きます。その後、目で検査をして物理的損傷がないこと、および正しいトークン・コードが正確に表示されることを確認します。

トークンが直面することの多い耐久性のもう 1 つの問題は水没です。そこで、RSA では浸水テストを実施しています。浸水テストでは水中にトークンを落とし、水が染み込むことなく耐えられるかどうかを確認します。このテストでシミュレーションしているのは、衣類のポケットに忘れられたトークンが洗濯機・乾燥機にかけられるシナリオ、トークンをポケットに入れたままユーザーが泳いでしまうシナリオ、トークンを飲み物の中に落してしまうシナリオです。

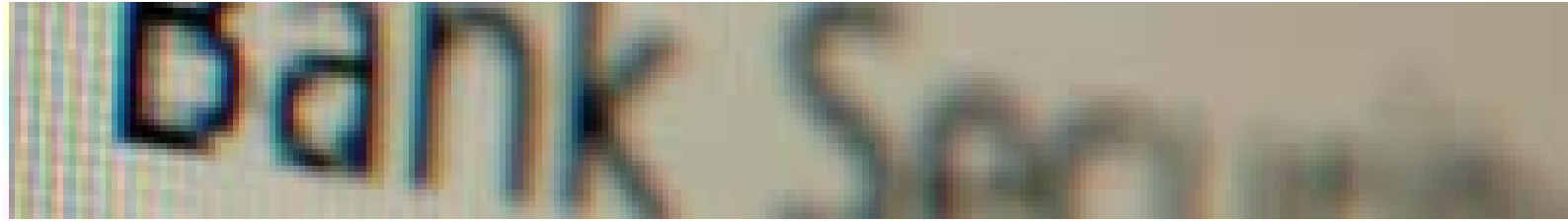
要求の最も厳しい測定基準の設定

研究所が設定する測定基準のすべてがそうであるように、この数値も極端な使われ方をされるトークンの信頼性を測るために設定されました。

このテストでは、朝オフィスに出勤してきたユーザーが接続済みのトークンを差し込み、昼食時に取り出し、昼食後に再び差し込み、終業時間に取り出す、という状況を仮定しています。つまり、このユーザーは 1 日に計 4 回トークンを挿入/取り出すことになります。年に 250 日出勤する場合、挿入/取り出しの回数は 1,000 回に及びます。トークンの有効期間は 5 年であるため、最終的には 5,000 回挿入されると推定できます。研究所では確実にトークンを継続的に利用できるように、この数字を 2 倍にしてトークンを 10,000 回、挿入し取り出すテストをしています。

また、当初は公式ではなかったもので、今では正式となったテストも多数実施しています。たとえば、RSA の営業部門の幹部はトークンを手に持ち、デスクに叩きつけるように置いてトークンの耐久性を証明することがよくあります。このデモンストレーションは以前から顧客のオフィスで行っているもので、顧客に他のメーカーのトークンでも同じことを試してみるよう勧めます。現在では正式なテストとなったこの「テーブル・スラム・チェック」では、表を上にしてトークンを手のひらに置き、その手をデスクに叩きつけて各ロットのサンプルの耐久性を確認します。

USB 型の RSA SecurID SID800 に対しては、SID700 に



適用される上記のテスト以外にも実施します。例えば、USBポートへの差し込みに関する耐久性テストです。すべてのトークンは、USBポートへの挿入と取り外しに10,000回、耐えられることをテストします。RSA SecurID SID800にはUSBコネクタ保護用のキャップついているため、このキャップについても取り外し後にRSA SecurID SID800にしっかりとハマるかどうかがテストします。

結論

トークンをさまざまなユーザーに配布して情報やアプリケーションへのアクセスを保護しようとしている企業にとって、トークンの信頼性は大きな関心事です。RSA セキュリティは20年近くにわたり、ハードウェア・トークンを設計し、業界最高レベルの信頼性を確保し続けています。

その証拠となる事例をいくつ挙げても(有用ではあるかもしれませんが)、RSA セキュリティがトークンの信頼性においてトップの座を維持し続けていることを保証することにはなりません。そのため、トークンの各ロットについて大量のサンプルを使った詳細なテストを実施し、RSA SecurID 認証トークンの信頼性レベルを証明しています。RSA セキュリティでは同じ方法論を用いて競合他社のトークンもテストしているため、自信を持って「RSA SecurID トークンは業界最高レベルの信頼性を確保している」と言えるのです。

信頼性を示す証拠を希望する場合には、上記の方法あるいは独自に開発した方法でテストを実施してください。例えば、複数のベンダーのトークンを評価する場合には、各ベンダーのトークンを自動車で轢いたり、水の入ったグラスやコーヒーの入ったカップに落したりしてみます。あるいはRSA SecurID と他社のトークンを、砂漠地帯あるいはツンドラ地帯に停車した自動車のトランクに放置してみてください。

RSA セキュリティがこのような詳細なテストに投資し、実施している理由は1つです。それは、RSA SecurID ソリューションを選択したお客様が、費用対効果に最も優れた管理方法と、期待通りのエンドユーザー体験を実現してくれる信頼性の高いトークンを、確信を持って導入できるようにすることです。RSA SecurID は信頼性が高く、最も厳しいエンドユーザーの要求にも応えられることが分かっているため、企業は安心して採用していただけます。



EMC ジャパン株式会社

RSA 事業本部

TEL 03-6830-3341

info-j@rsa.com

<http://japan.rsa.com>

EMC2、EMC、EMCのロゴ、RSAおよびSecurIDは、米国およびその他の国におけるEMC Corporationの登録商標または商標です。
© Copyright 2013 EMC Corporation. All rights reserved.

SIDRE SB 0902-J