報道各位

2000 年 12 月 18 日

インターネット高速暗号処理ボード「CryptoSwift 」が 128 ビットSSL 対応 セキュアサーバのパフォーマンスを向上

-ハードウェア機器による高速暗号処理装置と「ベリサイン・グローバル・サーバID 」が、オンライン・トレーディングのセキュリティを実現

※日本ベリサインからも配布を行っています。

株式会社 大和総研
日本ベリサイン株式会社

大和総研が販売を行う高速暗号処理ボード「CryptoSwift（クリプトスイフト）」と「ベリサイン・グローバル・サーバ ID [*1]」が大和証券のオンライン・トレードに採用され、128 ビット SSL 暗号化による高度なセキュリティとウェブサーバの負荷軽減を同時に実現しました。この実績を踏まえ、大和総研と日本ベリサインは、セキュアサイト構築関連の両社製品のマーケティング、顧客へのソリューション提案を協調して推進する計画です。

株式会社 大和総研（以下 大和総研 所在地: 江東区 社長 田中　榮=たなかさかえ）

日本ベリサイン株式会社（以下 日本ベリサイン 本社:川崎市幸区 社長:児玉皓次＝こだまこうじ）

１．セキュリティ強化による課題

SSL の公開鍵暗号処理は、安全性の高い e コマースサイト運用に欠かせない機能となってきました。128 ビット SSL 暗号化通信は、標準的な 40 ビット SSL と比較して、データの暗号化の強度が２の 88 乗倍（約 3×10^{26} 倍）まで高まるため、大和総研では、オンライン・トレード・システムのセキュリティ向上のためデータ暗号化を 40 ビット SSL から 128 ビット SSL に変更しテスト環境で検証を行ったところ、40 ビット SSL の場合に比べて暗号トランザクションによるウェブサーバへの負荷が４倍になることがあり（大和総研比）CPU への過負荷は、サーバの業務処理速度を著しく低下させ、顧客サービスに影響を与えることがわかりました。

２．解決策

この問題に対するソリューションとなったのが、「CryptoSwift」 でした。「CryptoSwift」は 公開鍵暗号化方式などのセキュリティ機能を加速し、1024bit の RSA トランザクションを 1 件あたり 5 ミリ秒以下で処理できます。レスポンスタイムは最高で 10 倍に早まり、セキュリティ処理に使用されていたサーバのリソースも、他の処理のため

に開放できます。
「CryptSwift」の製造元である Rainbow Technologies 社では、
「CryptSwift をベリサイン・グローバル・サーバ ID を導入した 128bitSSL のサーバに装着すると、暗号処理件数が 秒間 30 件から秒間 1000 件と 30 倍以上に高まり、かつレスポンス・タイムも 15 秒から 2 秒以下に短縮するなど、信頼性が高く軽快なアクセスのできるサイトを低コストで構築することができました。」と公表しています。

3．インターネット高速暗号処理ボードの特徴

オンラインショッピングから 企業間取引までさまざまなアプリケーションを対象とする「CryptoSwift」はセキュアなウェブサーバのパフォーマンスを向上させ、サーバへの投資コストを最大限に活かすことができます。
ボードタイプの CryptoSwift ボードはサーバの PCI スロットに容易に装着でき、ドライバーのインストールも簡単です。また主要なセキュリティプロトコルに対応し、代表的な Web サーバやＯＳの多くともシームレスに動作します。
詳細情報は http://www.dir.co.jp/Reception/ipd/rainbow/index.html をご覧ください。

4．「ベリサイン・グローバル・サーバＩＤ」* 1

ベリサインは、グローバル・サーバ ID の発行にあたって、申請企業の実在性、同企業が当該ドメイン名の正当な利用権者であること、そして、申請者がたしかに同企業を代表して申請していることを厳密な手続にしたがって確認します。これらの手続は、ベリサイン社の業界をリードする認証局運用規程（ CPS: Certificate Practice Statement) に則った形で運用されます。
ベリサイン・グローバル・サーバ ID は http://digitalid.verisign.co.jp/server/index.html から 120,000 円（一件一年間有効 消費税相当額除く）でご申請いただけます。

大和総研について

大和総研は、大和証券グループの総合シンクタンクとして、マクロ・ミクロ経済分野の調査から、コンサルティング、先端技術の研究、システムの企画・開発、システムインテグレーションサービス、教育事業に至るまで、幅広いサービスを提供しています。中でも、金融・資本市場分野を中心に、グローバルな情報・通信ネットワークを活用した調査研究・システム開発に特徴を有しております。
常に地球規模の視点に立ちながら、リサーチ機能、システム機能を有機的に統合した総合研究機関として、多様化するニーズに応えております。
http://www.dir.co.jp

日本ベリサインについて

VeriSign,Inc （NASDAQ：VRSN）の日本法人である日本ベリサインは、ウェブサイト、

企業、EC サービスプロバイダーなどが IP ネットワークを用いた安全な電子商取引／通信環境を実現するために必要とされる、認証、検証、そして決済などのインターネット・トラスト・サービスに関する主要なプロバイダーです。
ウェブサイト、ソフトウェア開発会社そして個人を対象とするベリサインのトラスト・サービスは www.verisign.co.jp および各種 ISP、サービス・プロバイダーから提供されています。パートナープログラムの詳細情報は セキュアサイトパートナーセンター http://digitalid.verisign.co.jp/partner/ をご覧ください。

SSL (Secure Sockets Layer: セキュア・ソケット・レイヤー) * 2

SSL は、ネットスケープ社によって開発された暗号通信プロトコルで、現在インターネット上のセキュリティ・プロトコルとして最も普及しています。秘話性を欠き匿名性が高いインターネットに、盗聴不能で安全な通信チャネルの確立と、ウェブ・サーバとウェブ・ブラウザ相互の認証処理を可能にします。この SSL 暗号化プロトコルを利用するためには、ベリサイン等の CA(Certificate Authority:第三者認証機関)から提供されるデジタル証明書が必要になります。ネットスケープ・コミュニケータおよびマイクロソフト・インターネット・エクスプローラは、このグローバル・サーバ ID をインストールしたウェブ・サーバと通信する際に、最高強度の暗号化テクノロジである 128 ビット SSL 暗号化通信を利用することが可能になります。

以上

＜お問い合わせ＞
日本ベリサイン株式会社
マーケティング・コミュニケーションズ
直木景子
Tel: 044-520-6141 Email: pr@verisign.co.jp

株式会社大和総研
ｅビジネス事業室
営業・マーケティング担当
石田 隆男
Tel: 03-5620-5543 Email: ta.ishida@dir.co.jp