

# 堅牢な暗号鍵管理による セキュアで高速なアプリケーション配信

## Entrust nShield HSMとA10 ThunderのSSL/TLS アクセラレーションの連携

A10 NetworksとEntrust社は、SSL/TLS暗号化通信のセキュリティ強化に関して連携ソリューションを提供しています。A10 Thunder CFW/ADC シリーズがアプリケーションサーバーのSSL/TLS アクセラレーションを行う際に利用する暗号鍵の管理と保護、および暗号化処理をEntrust nShield HSMのハードウェア上で行うことで、高度なセキュリティを確保すると同時に、高いパフォーマンスでの処理を実現します。このソリューションにより、FIPS140-2 Level 3などの高度なセキュリティ基準を満たしたセキュアで高速なアプリケーション配信を実現できます。

### SSL/TLS通信の増大と暗号鍵管理の脆弱性

セキュリティとプライバシーの懸念により多くのアプリケーションでSSL/TLS通信の適用が進んでおり、高度なセキュリティを要求されるオンライン取引において利用されるだけでなく、今日では多くのWebサイトにおいて全てのWebリクエストとレスポンスがHTTPSで暗号化されています。アプリケーションのパフォーマンスを落とさずにSSL/TLS通信の増大に伴って増加する暗号処理に対応するには多くの演算リソースが必要となるため、アプリケーションサーバーを多数配置してのアプリケーショントラフィック処理が必要になりますが、暗号鍵が多数のサーバーに配置されることで暗号鍵の管理は煩雑化します。

また、ソフトウェアによる暗号処理は、高品質な乱数を発生できないために暗号の解読に繋がる可能性があります。また、アプリケーションサーバー上への暗号鍵の保管は、サーバーへの攻撃や暗号鍵をメモリ上に展開する際の盗聴などにより漏えいする危険性があります。暗号鍵が漏えいするとSSL/TLS通信が解読されてしまうため、機密情報の流出やクレジットカードの偽造などに繋がります。このような事態を防ぐためには、安全な環境での暗号鍵の保護が重要になります。

### Entrust nShield HSMによるハードウェアベースでの 暗号鍵管理・保護とA10 Thunder ADC/CFWの連携

Entrust社が提供するHardware Security Module (HSM)であるnShield HSMを利用することで、SSL/TLS通信の暗号処理や鍵管理を耐タンパ性の高いハードウェア上で行うことができます。これにより、アプリケーション配信基盤で利用する暗号鍵の安全管理・保護が可能になると共に、暗号化処理や署名処理のオフロードも可能になります。Entrust nShield HSMはマルチクライアント接続・高可用性を意識した製品設計になっており、多様な暗号アルゴリズムに対応しています。また、FIPSやCC(Common Criteria)などの政府機関が要求するセキュリティ認定を取得しています。暗号鍵へのアクセスログ等により、監査や追跡調査の負担も軽減します。

A10 ネットワークスのThunder CFW/ADC シリーズはアプリケーション配信の高速化機能として、HTTP/HTTPSやFIXを含む多様なプロトコルに対応したサーバー負荷分散機能に加え、サーバーのSSL/TLS通信に関わる処理をオフロードするSSL/TLSアクセラレーションの機能を持っています。暗号化処理をA10 Thunderで行うことで、アプリケーションサーバーの暗号処理にかかるCPU負荷を大きく軽減するとともに、暗号鍵の管理を一元的に行うことで運用負荷も軽減されます。

### 課題：

SSL/TLS通信のトラフィックが増加しアプリケーションの暗号処理が増加する一方で、ソフトウェア上で処理される暗号鍵は暗号解読や攻撃により情報が漏えいする危険性があり、アプリケーション配信のパフォーマンスやコンプライアンス維持へのインパクトなく、安全管理を行う必要がある

### 解決策：

SSL/TLS通信の暗号処理・鍵管理を耐タンパ性の高いハードウェア上で行うHardware Security Module (HSM)であるEntrust nShield HSMとA10 Thunder CFW/ADCの連携により、アプリケーションのSSL/TLSアクセラレーション処理で利用される暗号鍵の堅牢な管理と保護、および高速なSSL/TLS処理を実現

### メリット：

- セキュアで高速なアプリケーション配信の実現
- SSL/TLS暗号鍵の保護と管理コストの低減
- FIPS140-2 Level 3などの基準を満たす高度なセキュリティの確保
- 高パフォーマンスでの暗号化処理
- Entrust nShield HSMの負荷分散による高可用性と拡張性

**ENTRUST**

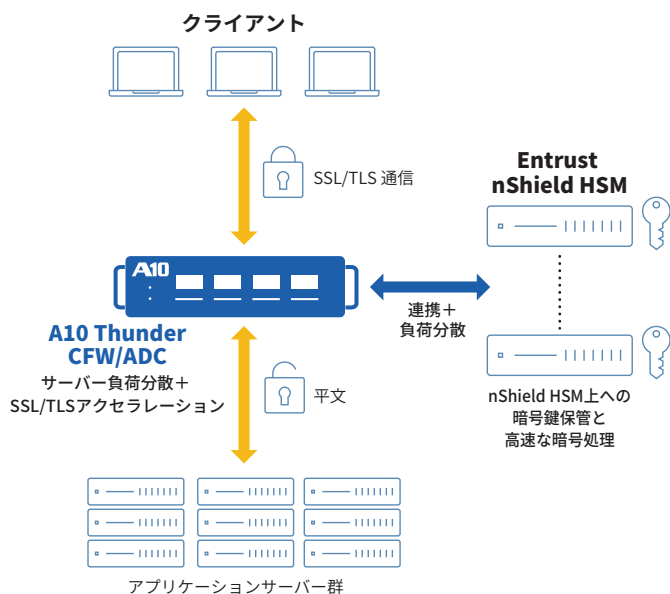


図1：Entrust nShield HSMとA10 Thunder CFW/ADCの連携によるセキュアで高速なアプリケーション配信基盤

A10 ThunderのSSL/TLSアクセラレーションで利用される暗号鍵の堅牢な管理と保護、および暗号処理の高速化を実現するために、図1に示すようなEntrust nShield HSMとの連携が可能です。この連携では、暗号鍵はEntrust nShield HSMのハードウェア内に保管されており、暗号化処理や署名処理がHSM上で実施されます。

Entrust nShield HSMとA10 Thunder CFW/ADCとの連携には、以下の特長とメリットがあります。

- **セキュリティ強化の実現**：HSM利用により暗号鍵をA10 Thunderから物理的に分離して管理
- **セキュリティ基準への準拠**：FIPS140-2 Level 3などの基準を満たす高度なセキュリティの確保により、公的機関や金融サービス、エンタープライズ向けの法規制に対する対応が可能に
- **高パフォーマンス暗号化処理**：Entrust nShield HSMとA10 Thunderが連携したSSL/TLSアクセラレーションにより高いパフォーマンスでの暗号化処理を実現
- **高可用性と拡張性**：Entrust nShield HSMをA10 Thunder CFW/ADCで負荷分散することにより高い可用性と拡張性を実現

また、A10 Thunder CFW/ADCをアプリケーションサーバーの負荷分散に用いることで、TCPコネクションリユースやRAMキャッシングなどのアプリケーション配信高速化機能、DDoSに対する防御やWeb Application Firewall (WAF)、L4ステートフルファイアウォールやL7ファイアウォールなどによるセキュリティ機能、NAT機能、グローバル負荷分散などの機能を併せて利用することができ、セキュアで高速、かつ可用性の高いアプリケーション配信が実現できます。

## まとめ

オンライン取引などの高いセキュリティが求められるアプリケーションにおいてはSSL/TLS通信で利用する暗号鍵の堅牢な管理と暗号処理の高速化が重要な課題となります。A10 Thunder CFW/ADCとEntrust nShield HSMの連携により、暗号鍵を堅牢に管理・保護することによるセキュリティの強化と、SSL/TLSアクセラレーションによる暗号化処理の高速化、サーバー負荷分散によるアプリケーション配信高速化と可用性の向上を併せて実現できます。これにより、FIPSなどの高度なセキュリティ基準を満たした、セキュアで高速なアプリケーション配信が実現されます。

## Entrust 社について

Entrust は信頼できる認証、支払い、データ保護を実現することにより、動き続ける世界をセキュアにしています。今日、支払いや国際取引、オフィスや企業ネットワークへのアクセスにおいて世界中でより安全で円滑なユーザ体験が求められています。私たちは他に類を見ない幅広いデジタルセキュリティとID発行ソリューションを通じ、世界で最も信頼されている組織から信頼されています。

[entrust.com/ja/HSM](http://entrust.com/ja/HSM)

## A10 Networks / A10 ネットワークス株式会社について

A10 Networks (NYSE: ATEN) は、サービス事業者やクラウド事業者および企業で利用される5Gネットワークやマルチクラウドアプリケーションのセキュリティを確保します。高度な分析や機械学習、インテリジェントな自動化機能により、ミッションクリティカルなアプリケーションを保護し、信頼性と可用性を担保します。A10 Networksは2004年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界117か国のお客様にサービスを提供しています。

A10 ネットワークス株式会社はA10 Networksの日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションをご提供することを使命としています。

[www.a10networks.co.jp/](http://www.a10networks.co.jp/)

Facebook : <http://www.facebook.com/A10networksjapan>

## Learn More

About A10 Networks

お問い合わせ

[a10networks.co.jp/contact](http://a10networks.co.jp/contact)

## A10 ネットワークス株式会社

[www.a10networks.co.jp](http://www.a10networks.co.jp)

[a10networks.co.jp/contact](http://a10networks.co.jp/contact)

©2020 A10 Networks, Inc. All rights reserved. A10 ロゴ、A10 Networksは米国およびその他の各国におけるA10 Networks, Inc. の商標または登録商標です。その他上記の全ての商品およびサービスの名称はそれら各社の商標です。A10 Networks は本書の誤りに関して責任を負いません。A10 Networks は、予告なく本書を変更、修正、譲渡、および改訂する権利を留保します。製品の仕様や機能は、変更する場合がございますので、ご注意ください。商標について詳しくはホームページをご覧ください。[www.a10networks.com/a10-trademarks](http://www.a10networks.com/a10-trademarks)

Part Number: A10\_SB\_Entrust\_and\_A10 Nov 2020