SafeNet のトランスペアレントなトークン化により PCI コンプライアンスのコストと労力を削減

WHITE PAPER

トークン化は、さまざまな組織や業界でますます採用が進んでいます。PCI データを事実上除外することで、トークン化は多くの利益をもたらし、組織はセキュリティを強化しつつ PCI コンプライアンスの労力とコストを削減できるようになります。本書では、トークン化について詳細な情報を提供するほか、潜在的利益を最大限まで達成できるようにトークン化の採用を成功させる実践的なガイドラインを提供します。

序論 : コンプライアンスの課題

「十分である」というのは、どのくらいのことなのでしょうか？ ことセキュリティに関しては、この問題はあらゆる組織にとって頭痛のタネであり続けています。Payment Card Industry Data Security Standard（PCIDSS）によって規制される企業にとっては、監査を無事に完了した後でさえこの問題が残り続けます。監査の翌日に新しいシステムがインストールされ、新たな脅威が発見され、新たなユーザーが追加され、新しいパッチが公開されるかもしれません。監査を通過したのに違反が発生したら、その影響はやはり壊滅的なものになる可能性があります。

IT インフラ、セキュリティソリューション、脅威、規制、そしてそれらの解釈は進化し続けています。セキュリティに関しては、組織は多層防御アプローチを取る必要があり、そのためこの仕事には終わりがありません。これは、ほぼすべての業界の組織に当てはまります。企業は、従業員の個人情報を安全に保護するために警戒し続ける必要があります。Sarbanes-Oxley、Health Insurance Portability and Accountability Act（HIPAA）、HITECH、EU Data Privacy Directive、またはその他の規制に縛られる組織にとって、センシティブなデータを安全に保護することは基本要件です。

ビジネスおよびセキュリティリーダーはこの状況の中で、予算配分、スタッフ配属、新規投資、継続的なコストと、セキュリティ目標とのバランスを常に熟考して見いだすように努力しなければなりません。それを考えると、セキュリティを最大にしつつ効率を最大にするためにアプローチを精緻化することは、セキュリティチームの義務です。そのため、多くの組織がトークン化に期待しているのです。

本書ではトークン化について、またそれが組織の PCI コンプライアンスの取り組みをどのようにサポートできるかについて、詳細に説明します。特定の導入シナリオに対しどの最適なアプローチを選ぶために考慮すべき要因を含め、トークン化を暗号化やその他のアプローチと比較します。また SafeNet のトランスペアレントなトークン化のアプローチについても説明し、このソリューションがセンシティブなデータを保護することを目指している組織に効果的かつ効率的な方法で提供する利点と利益を明らかにします。

トークン化の代替手段についての考察：暗号化、データマスキングなどのアプローチ

今日のセキュリティを取り巻く状況下では、最適なセキュリティを確保し、コンプライアンスの維持を試みるための多くの選択肢が組織にはあります。以下はトークン化を補完するか、その代替手段となりうるアプローチの概要です。

「暗号化されたデータをコンプライアンスの範囲外と見なせるのは、暗号化されたカード会員データを保持する機関がそのデータを解読する手段を持っていない場合で、唯一その場合だけに限られます」
—PCI SSC Issues Statement on Scope of Encrypted Data via FAQ 10359、2009/10/11 発行

暗号化

PCI によって規制されるほとんどの組織で、カード会員データはある時点で暗号化されていない状態で取り出される必要があります。それを考慮すると暗号化は基本要件であり、確実に権限のあるユーザーのみが承認目的のためにセンシティブな決済情報にアクセスできるようにする必要があります。ただしセキュリティ戦略を立てるときは、暗号化が組織の PCI コンプライアンスの取り組み範囲に与える影響の程度を考慮に入れることが重要です。

PCI Security Standards Council が明らかにしているように、暗号化されたデータは依然としてそのデータを解読するメカニズムを持つ組織の範囲内にあります。言い換えると、マーチャントがオフサイトの保管設備を利用しており、決済データをオフサイトに送る前に暗号化していたら、決済データを解読する機能が保管設備内にない限り、その設備の運用はコンプライアンスの範囲外となります。

このように暗号化は、コンプライアンスの範囲を縮小させるのに役立ちます。しかし、暗号化メカニズムを採用している組織内にはデータを解読する機能があるため、暗号化されたデータを保管またはアクセスするシステムの存在を最小限に抑えるよう注意を払う必要があります。これには、以下のようないくつかの理由があります。

- コンプライアンスの範囲とコスト。暗号化を管理するシステムや暗号化されたデータの保護と伝送は、PCI の範囲に非常にたくさんあります。マルウェア対策、多要素認証、そしておそらく最も重要な厳密な鍵保護メカニズムを含む PCI 規制の範囲は、忠実に守られる必要があります。さらにこれらの各システムが PCI 監査の範囲内にあり、監査されるシステムが多ければ多いほど、全体の監査費用は高くなります。
- アプリケーション統合。通常、暗号化されたデータへのアクセスが必要なアプリケーションはすべて、暗号テキストの非常に長いフィールドサイズに対応するために、プレーンテキストとバイナリデータからの移動に伴うデータ型とフィールド長の変化に対応できるよう変更が必要になります。これらの変更は関連するアプリケーションの数とタイプによって膨大な時間と費用が必要になる恐れがあります。

形式を維持した暗号化

形式を維持した暗号化（Format Preserving Encryption）は、関連アプリケーションへの暗号化の影響を最小限に抑えることが可能なため、ここ数年いくつかのベンダーによって紹介されてきました。しかし本書の公開時点では、PCI Security Standards Council は、形式を維持した暗号化に関する公式の方針を公表しておらず、これらの手法がコンプライアンスの指針を満たしているかどうか、またどれが許容できるかについて保留のままにしています。また多くのアルゴリズムとモードは、米国国立標準技術研究所（NIST）などの標準化団体によって承認されていない可能性があります。形式を維持した暗号化は、強力な暗号化アルゴリズムで通常作成されるよりも短い値を返す必要があるため、実証済みのアルゴリズムをベースにしたトランスペアレントなトークン化と比べると、暗号テキストの強度は低下します。さらに悪質な攻撃によって形式を維持した暗号化とその関連アルゴリズムに使用される鍵が奪われた場合、暗号化されていないテキストが取り出される恐れがあります。トークンは、トークン化されたデータをやりとりするシステムによって取り出しができません。そのため、これらのシステムは監査の範囲外になります。

比較	トランスペアレントなトークン化	形式を保存した暗号化
監査範囲の縮小	✔	⃠
解読に対する脆弱性の低さ	✔	⃠
高いセキュリティ強度	✔	⃠
実証済みのアルゴリズム	✔	⃠

データマスキング

データマスキングは、多くの企業のセキュリティおよびコンプライアンス目標に関して言うなら、考慮すべきもう 1 つのアプローチです。データマスキングはテストおよび開発環境で一般的に使われているアプローチであり、アプリケーション開発をアウトソーシングする場合に特に役立ちます。データマスキングは、実際の顧客データのセキュリティを、アプリケーション開発環境が侵害しないように使用します。データマスキングでは、センシティブデータは現実的ではあるものの実際のものではないデータに置き換えられます。データマスキングは有用な手法かもしれませんが、開発組織は参照整合性などの側面が対処されるようにし、データマスキングに使われるメカニズムが、実データを発見する可能性のあるリバースエンジニアリング手法の影響を受けないようにする必要があります。

上記の代替手段の特性と考慮すべき事項を考えると、トークン化が市場で受け入れられつつあることが理解できます。次のセクションでは、最も効果的にトークン化を採用するためのさまざまな洞察と考慮すべき事項について説明します。

トークン化成功への鍵

近年、トークン化はますます PCI コンプライアンスに不可欠なアプローチとなっています。トークン化は決済データのセキュリティを強化しつつ、セキュリティと PCI 監査にかかる全体的なコストを削減できるよう組織をサポートしています。

トークン化は、オンラインでのクレジットカード取引やその他のセンシティブなデータの伝送のために採用され、センシティブデータをオリジナルデータの特性を保持するトークンに置き換えることによって機能します。セキュリティチームはトークン化により、データベース、アプリケーション、ユーザーがセンシティブなデータに直接アクセスせずに、そのセンシティブなデータのプレースホルダとしかやりとりできないようにすることが可能です。トークン化システムは、センシティブデータをオリジナルデータと同じ形式の暗号化されたトークンに変換するため、関連するアプリケーションはシームレスに動作し続けることができます。マスキング機能は、データの一部を認証用に利用可能にする必要がある場合も維持できます。

トークン化を効果的に実装すると、組織のセキュリティと PCI コンプライアンスにかかるコストが大幅に削減できます。アプリケーションがトークン化にアクセスできても、トークン化を逆行させて暗号化されていない状態のカード会員データにアクセスする手段を持たない場合、それらのアプリケーションは PCI の範囲外であると見なされます。そのため、組織はこれらのシステムに対して PCI に義務付けられたセキュリティ対策を採用する必要はありません。また、これらのアプローチは継続的な PCI 監査のコストを削減します。Illumis のディレクターであるサイモン・シャープ氏は次のように話しています。「監査役はトークン化を確実に機能させるため、カード会員データがないように、特に個人アカウント番号（PAN; Personal Account Number）があった場所には存在しないように、全システムをサンプリングして点検します。システムを範囲から除外できるように、トークン化された値と PAN を分けることが重要です」。

以下に、新しいトークン化の実装を計画する際に考慮すべき重要な事項と戦略を示します。

「トランスペアレントなトークン化は、センシティブデータをデータベースシステムから除外するためにセンシティブではない同じ形式のデータに置き換える、非常に便利な手法です」

「これは、データベーススキーマの変更がまったく不要であることを意味しますが、トークン化ソリューションと適切に統合するために、関連システムに変更が必要なケースは依然として存在します。またシステムが新しいトークンデータを、たとえばビジネスインテリジェンスソリューションの基盤として使用するなど、誤って解釈しないように細心の注意を払う必要があります。ほとんどの操作は置き換え前の実際のデータに対して実行する必要があることを理解しておくことが重要です」

アレキサンドレ・ピント氏、シニアテクニカルマネージャー兼 PCI QSA、暗号セキュリティ

「私たちが提供できる価値の中で特筆すべきは、システムとプロセスを統合整理することによる監査範囲の縮小であり、確実に業務上の正当な理由があるシステムまたはプロセスに対してのみ、センシティブな決済データをアクセス可能な状態に保ちます」と、Accuvant の PCI プログラムマネージャー、CISSP、QSA、ISO ISMS 主任審査員であるブライアン・セラ氏は話します。「実際、監査の範囲から除外されたすべてのシステムについて、企業は監査時間を約 2 時間節約し、PCI 標準によって要求されるすべてのセキュリティ対策を適用し維持管理するのにかかる多額の費用を節減しています」

削除またはトークン化を通したセンシティブなカード会員データのインスタンスの最小化

組織は、暗号化、トークン化、またはその他のセキュリティ対策を採用する前に、ビジネスに不可欠な場合のみカード会員データの保管とアクセスが可能にすることから始める必要があります。必要性がなければセンシティブデータを完全に除外し、漏洩の可能性を減らすことが、重大な第一歩です。

特定のシステム上に存在するデータを除外したり、暗号化したり、トークン化したりすることによる影響を評価することは重要です。

センシティブなデータが発見されたら、他のシステムの関連付けと相互依存性に関して分析する必要があります。たとえば、ビジネスプロセスがセンシティブなデータにアクセスする必要がある場合、それらのプロセスはそのセンシティブなデータを暗号化またはトークン化することによって影響を受けるでしょうか？説明がつかない場合、それらの関連プロセスに対するトークン化の影響はビジネスに重大な問題を引き起こす可能性があります。

次にセキュリティチームは、どこでどのようにトークン化を採用できるかを決める必要があります。現在、トークン化は一般的に次の 2 つの方法のいずれかで採用されています。

- アウトソーシング。e コマースの場合は、小売業者は自社のシステム内で暗号化されていないカード会員データにアクセスする可能性が決してないように、トークン化を完全にアウトソーシングできます。たとえばオンライン取引が終了した後に、カード情報をトランスペアレントにサービスプロバイダーにリダイレクトできます。その後サービスプロバイダーは、カードデータをトークンに変換して、そのトークンを小売業者に返します。このアプローチの欠点は、トークンおよび決済データの移行の複雑さを考えると、小売業者がサービスプロバイダーを非常に変更しにくくなる場合があるということです。また、このアプローチは複数のカードプロセッサを使用する小売業者にとっては選択肢にならない場合があります。

- 社内。マーチャントは、関連するダウンストリームアプリケーションが暗号化されていないカード会員データにアクセスできないように、カード番号をトークンに変換して管理します。このアプローチは 1 つ目のケースほどコンプライアンスの範囲を縮小しませんが、マーチャントはより柔軟性を持てるため、特定のサービスプロバイダーに固定されてしまうことはありません。

いずれの場合も、これらのアプローチはかなりの利益をもたらします。一方でセキュリティチームは、暗号化されていない決済データにユーザーやアプリケーションがアクセスできるようにする必要がある場合、トークン化を使いたがらないかもしれません。システムやユーザーに、暗号化されていないテキストのカード会員データの使用権限を与える必要がある場合、暗号化がトークン化よりも良い代替手段または補完手段となることがあります。特にスプレッドシートや Word 文書データなど非構造化データがある場合は、暗号化は構造化データに採用されたトークン化を補完するものになります。

「監査の取り組みの焦点となりやすい領域の 1 つは、トークンをオリジナルの PAN と関連付けるルックアップテーブルのセキュリティです」と、Foregenix のディレクターであるベンジー・ホザック氏は言います。「これはソリューションにとって不可欠であり、それ相応に保護されなくてはなりません。そのため、この領域での経験と専門知識を持った評判の良いサプライヤーと協業することが推奨されます」

実証済みのサードパーティソリューションの利用

PCI 監査役が暗号化とトークン化のコンプライアンスについて検証する際にまず尋ねる重要な質問は、利用されているテクノロジーのタイプです。マーチャントや金融機関が暗号化やトークン化の領域の一部にでも社内開発されたシステムを採用していると、監査の範囲は実質的に拡大します。実装の各面、アクセス管理から鍵ローテーションにいたるすべてを調査して検証する必要があります。その結果、社内開発されたシステムによって、先行投資と継続的開発の増加は言うまでもなく、監査コストが大幅に増加する可能性があります。

一方で PCI 監査役によってすでに入念に検査されたコンプライアンス順守の市販ソリューションを採用すると、監査プロセスを単純化でき、監査役はメカニズム自体よりも、セキュリティシステムの実装方法に焦点を合わせることができます。

さらに、一貫した方法でトークン化インフラをとらえて、すべての側面が安全に保護されるようにすることも重要です。

「トークン化、鍵管理、暗号化はハードウェアで可能な限り実行すべきだという考えを大いに支持します。」と、Illumis のサイモン・シャープ氏は話します。

「どれだけマルウェア対策を採用しても、結局ソフトウェアは脆弱なままの可能性があります。インラインキーロガーを使用するハッカーは依然としてアクセス制御を侵害できるかもしれません。ハードウェアベースのソリューションは、こうした重要なシステムに不可欠な追加のセキュリティ層を提供します」

暗号化とトークン化の集中管理

組織は可能な限り、1 つのプラットフォームで暗号化とトークン化の統合機能を提供するシステムを利用すべきです。こうしたシステムは、次のようなさまざまな利点をもたらします。

- **コスト節減**。トークン化ソリューションが暗号化と独立して動作する場合、先行購入、初期統合、継続的保守にかかるコストは通常、非常に高くなります。
- **監査と修復の単純化**。ログとポリシーが様々なポイントソリューションから収集され追跡される場合、コンプライアンスの実証と維持管理はより複雑になります。
- **集中型の鍵管理**。共通のプラットフォームから鍵管理を利用することによって、管理者は暗号化されたデータのベストプラクティスだけでなく、PCI DSS または VISA に従って、トークン化されたデータのベストプラクティスを確立できます。たとえば、PAN の暗号テキスト用の AES256 や関連するハッシュ値またはトークン値を保護するための SHA256 など、Token Vault（トークン保管庫）のコンポーネントに最も強力な暗号鍵を使用する柔軟性を持てます。
- **一貫したポリシー実施**。どんなデータをどちらの方法（トークン化または暗号化）で、どこで保護するかを制御する目的だけでなく、特権ユーザーやシステム権限を管理するため、一元的に保護ポリシーを実施することが重要です。

これらの利点を最適化するために、組織は大量のトランザクションへの対応に必要な拡張性を提供するソリューションを探さなくてはなりません。また業界標準、トークン化、暗号化アプローチに対する最大限に広範なサポートを提供し、さらには初期投資を長期的に最大限に活用できるようなソリューションを採用する必要があります。コンプライアンスは静的なイベントではなく、組織が機微なデータを管理する必要がある限り、継続的な取り組みであることを知ることが特に重要です。

ハードウェアベースのプラットフォームでセキュリティを最適化

組織は可能な限り、センシティブなビジネス資産を保護する重要な層を提供するハードウェアベースのプラットフォームを利用すべきです。堅牢なハードウェアベースの暗号化およびトークン化プラットフォームは、集中型のセキュアなバックアップや、より制限されたアクセスポイントなどの機能を特徴としており、セキュリティ全体を大幅に強化できます。

SafeNet のトランスペアレントなトークン化

SafeNet は組織がセキュリティを強化し、PCI コンプライアンスを確保し、セキュリティコストを削減することを可能にする、堅牢かつ包括的で柔軟なソリューションを提供します。セキュリティチームは SafeNet の利用により、監査の範囲を縮小してセキュリティを強化する際に、トークン化の利点を最大限引き出すのに必要な機能が得られます。SafeNet はトークン化と暗号化の機能を統合することによって、ビジネスにもセキュリティ目標にも最大限の利点をもたらす方法でトークン化および暗号化を適用するのに必要な柔軟性をセキュリティチームに提供します。

利点

- PCIコンプライアンスを確保してセキュリティを強化
- 監査コストの削減
- セキュリティの管理および統合の合理化
- VISAのベストプラクティスとの整合性

利点

SafeNet Tokenization の採用には、さまざまな利点があります。

- **PCI コンプライアンスを確保してセキュリティを強化**。SafeNet の利用により、組織は形式を維持したトークン化によってクレジットカード情報を安全に保護し、PCI 規制に対応できます。またセキュアな鍵保管とバックアップ、粒度の細かい管理制御などを特徴とする強化した DataSecure アプライアンスによって、センシティブなデータのセキュリティを最適化できます。さらに SafeNet は、銀行取引データや個人記録などを含むクレジットカード情報に加え、広範なデータ型を保護できます。

- **監査コストの削減**。SafeNet は、監査の必要があるデバイスの数を制限することによってセキュリティチームが時間とお金を節約できるようにします。PCI コンプライアンスの監査に直面している場合、多くの組織がセンシティブなデータの存在する各サーバについて規制順守を保証しなくてはなりません。SafeNet Tokenization は、データベースとアプリケーション内のセンシティブなデータをトークンに置き換えるため、監査するサーバが少なくてすみます。 監査の範囲を縮小することで、時間とお金を節約できます。

- **セキュリティの管理および統合の合理化**。SafeNet を採用することで、組織はトークン化と暗号化を統合したソリューションでポリシーの管理、ライフサイクル鍵管理、保守、監査を行う中央プラットフォームを利用できます。また完全にアプリケーショントランスペアレントにトークン化を導入できるため、トークン化されたデータに対応するようアプリケーションをカスタマイズする必要がありません。

- **VISA ベストプラクティスとの整合性**。SafeNet のトランスペアレントなトークン化は、トークン生成、トークンマッピング、暗号化を使用したカード会員データリポジトリとしての Data Vault（データ保管庫）の使用、強力な暗号鍵管理に関する最近公開されたトークン化バージョン 1.0 の VISA ベストプラクティスと整合しています。
  (http://usa.visa.com/download/merchants/tokenization_best_practices.pdf)

SafeNet Tokenization は、さまざまな統合オプションを用意しています。お客様の環境に適したセキュリティ手法を選択できるよう柔軟性を提供し、その一方でより多くのデータ型を保護することを可能にします。ビジネスロジック、データベースアーキテクチャ、ストレージシステムなどの重要な企業コンポーネントに影響を与えることはありません。また SafeNet Tokenization は、開発チームがデータを非識別化したりマスク処理したりする必要がなく、環境をテストするために実データを移動または複製することを可能にします。組織は SafeNet Tokenization を採用することで、最適な効率と費用対効果でデータを保護し続けることができます。

機能

- 形式を維持したトークン化
- トークンのバリエーション
- 多くのデータ型をサポート
- 広範なプラットフォームをサポート

機能

SafeNet は、さまざまな重要な機能を提供します。

- **形式を維持したトークン化**。割り当て時に重複のない値やトークンの形式を定義することで、アプリケーションやユーザーとのトランスペアレントなやりとりを確保します。トークン値のデータ形式を維持するため、データとやりとりするアプリケーションをカスタマイズする必要はありません。SafeNet は、一部をマスク処理したデータ（例 ; XXXXX6789）など、さまざまなデータ形式をサポートしています。

- **トークンのバリエーション**。さまざまなトークンのバリエーションを選択できます（ランダムな桁のトークン化、連番のトークン化、最初の 2 桁または 6 桁を維持してのトークン化、最初の 2 桁と最後の 4 桁のトークン化）。

- **多くのデータ型をサポート**。クレジットカード番号や会員 ID から、社会保障番号や運転免許証ナンバーまで、すべてのデータを保護します。

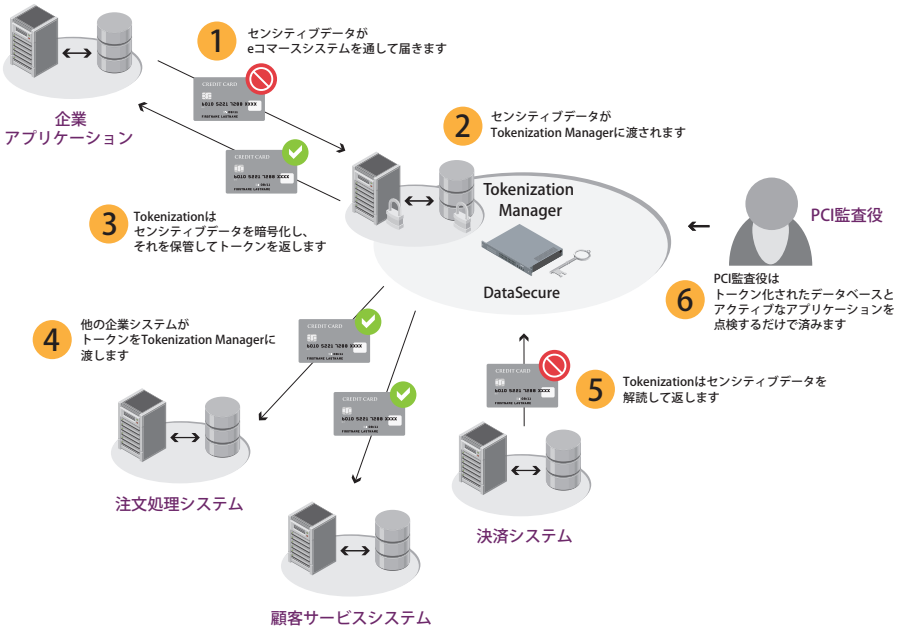
- **広範なプラットフォームをサポート**。Oracle、IBM、BEA、J2EE、Apache、Sun ONE、JBoss など、SafeNet は広範なアプリケーションや Web サービスをサポートしているため、柔軟に導入が可能です。また SafeNet は、Oracle および Microsoft SQL Server 向けのデータとトークンの保管を提供しています。

SafeNet のトランスペアレントなトークン化の導入

以下は、トークン化プロセスのしくみの概要です。

1. センシティブデータが e コマースシステムを通して届きます。
2. センシティブデータが Tokenization Manager に渡されます。
3. Tokenization はセンシティブデータを暗号化し、それを保管してトークンを返します。
4. 他の企業システムはトークンをトランスペアレントに渡されます。
5. PCI 監査役は、適切なトークン化技術であることを保証するために、トークン化されたデータベースか、または Data Vault（データ保管庫）とアクティブなアプリケーションをサンプリングして点検するだけで済みます。他のシステムは範囲から除外されます。

トークン化のしくみ



最後に

PCI コンプライアンスを確保する責務を負う組織にとって、闘いに終わりはありません。この闘いにおいてトークン化はますます一般的なアプローチになりつつあります。これにより PCI データを規制範囲から除外できるため、セキュリティを強化しコンプライアンスコストを削減できます。現在 SafeNet は、組織がトークン化の利点を最大限に引き出せるようにする、トランスペアレントなトークン化ソリューションを提供しています。

SafeNet について

SafeNet は、1983 年に設立された、情報セキュリティ業界における世界的なリーダー企業です。SafeNet は、お客様の貴重な資産である ID や、トランザクション、通信、データ、ソフトウェアライセンスを IT セキュリティの視点から、情報ライフサイクル全般にわたり保護しています。SafeNet のお客様は、100 カ国以上、2 万 5 千を超える企業や政府機関に及び、その情報セキュリティの保護を SafeNet に委ねています。

日本セーフネットについて

日本セーフネット株式会社（http://jp.safenet-inc.com 代表取締役社長：酒匂 潔、本社：東京都港区）は、米国 SafeNet, Inc. の日本法人で、2001 年の設立以来、ネットワークやアプリケーションのセキュリティ製品の日本国内での販売、マーケティング、サポートを提供しています。

本ホワイトペーパーの内容、製品・ソリューションについてのお問合せは下記までお願いいたします。

日本セーフネット株式会社

エンタープライズセキュリティ事業部
東京都港区新橋 6-17-17
御成門センタービル 8F
Tel: 03-5776-2751
Email: jp-info@safenet-inc.com