アプリケーションノート

WaveLogic Encryptionソリューション

すべての転送中データを常時プロテクト

セキュリティは、役員会議で取り上げられる議題になっています。2020 Thales Data Threat Report[1]の調査では、設立以降にデータ漏洩の被害に遭った経験のある企業の割合が49%であることが明らかになりました。ヘルスケア、金融、官公庁、教育など、攻撃を受けやすい業界のデータ漏洩の件数は平均を大きく上回っています。

データ漏えいは、顧客情報を危険にさらすだけでなく、組織の収益にも影響を与えます。Ponemonのグローバル調査によると[2]、1回のデータ漏えいで約2万5,500件の記録が流出し、数百万ドルのコストが発生するのに加え、顧客からの信頼の低下など、計り知れない損失が生じます。この調査では、2019年に米国で起きたデータ漏洩の合計コストが平均819万ドルであったことも判明しました。この数字でも業界による違いが見られます。ヘルスケア業界の1レコードあたりの損失は、ほぼ2倍です。

しかし、データ漏洩の脅威が増しているにもかかわらず、ネットワークを流れるトラフィック・フローは増えています。帯域需要の増加が続くなかで、運用の複雑さを軽減しながら、容量を段階的に拡張できるネットワークが必要とされています。また、データ漏えいの手口は巧妙化し、攻撃頻度は高まっています。機密情報や個人情報を収集しようと常に狙いを定める悪意ある攻撃から影響を受けずに済む組織はありません。現在の大容量ネットワークは、広帯域よりはるかに高いレベルで、保管中と転送中のすべての重要データをプロテクトするセキュリティ戦略を必要としています。なぜなら、データがメトロからリージョナル、長距離、さらに海底ネットワークへと世界中を転送されているからです。

現在の大容量ネットワークのセキュリティ保護を目的としたCienaのWaveLogic™ Encryptionは、広く導入されている6500 Packet-Optical Platformで、プロトコルに依存しないスケーラブルな超低遅延の暗号化ソリューションを費用対効果の高い方法で達成します。このソリューションは、モジュール式のコンパクトな大容量トランスポート機器であるCienaのWaveserver®ファミリーまで拡張され、安全で費用対効果の高いデータセンター相互接続（DCI）アプリケーションを実現します。この常時稼働の暗号化は、運用と管理の容易さを兼ね備え、実装しやすいデータ・プロテクション戦略を可能にします。この戦略では、Cienaの業界最先端のWaveLogicコヒーレント技術を利用し、比類ない柔軟性やパフォーマンスとともに、業界初のコヒーレント100G～400Gワイヤースピードの暗号化ソリューションを実現します。

メリット

- 超低遅延のFIPS準拠の暗号化ソリューションを提供し、非常に安全で透過的なエンドツーエンド通信を実現
- プログラマブルなWaveLogicコヒーレント技術を用いたスケーリングにより、柔軟な100G～400Gワイヤースピードの暗号化を実現
- プロトコルに依存しない暗号化機能を搭載し、多様なサービスをサポートする柔軟性を提供
- 認証とデータ暗号化の2つの独立したキーセットの使用や、秒単位の高速な暗号化キー・ローテーションなど、強化されたセキュリティ機能を活用
- X.509証明書ベースの認証を使用している企業の既存の公開鍵インフラストラクチャー（PKI）にシームレスに統合
- エンドユーザーが統合管理ツールを使用して、サービスとしての暗号化機能を安全に管理
- 世界中の金融、法律、ヘルスケア、軍、公益事業、官公庁のネットワークに広く導入されている実績のある暗号化ソリューション

1 https://cpl.thalesgroup.com/sites/default/files/2020-04/2020-data-threat-report-global-edition-infographics.pdf
2 Ponemon、IBM調査「Cost of a Data Breach 2020」 https://www.ibm.com/security/data-breach

暗号化テクノロジー

暗号化は、アルゴリズムを使用して情報を変換し、暗号化技術で「キー」と呼ばれる特別な情報を持つ人以外がその情報を判読できないようにするプロセスとして定義されています。基本的に、このプロセスではデータを暗号化し、データを取り出そうとする侵入者またはメッセージ解読用の適切なキーを持たない人に対してデータを完全に使用不可能にすることで、ネットワークを使用できないようにします。

データを暗号化する方法は数多くあります。様々な標準が、関連製品とキーに関する暗号化の要件を規定し、ネットワーク装置の認定プロセスを定めています。多様なキーサイズ（56ビット、128ビット、256ビット）を持つ、米国標準技術局（NIST）が制定したAdvanced Encryption Standard（AES）など、いくつかの標準ベースの暗号化アルゴリズムがあります。これらの標準は、米国の連邦情報処理標準（FIPS）Publicationとして発行されています。たとえば、AES-256暗号化アルゴリズムは、FIPS 197として公表されました。FIPS 197などのアルゴリズムに固有のPublicationに加え、NISTはFIPS 140-2において、ハードウェアとソフトウェアの両方のコンポーネントを含む暗号化モジュールの要件を調整する標準を公表しています。

ほかにも暗号化ソリューションを認定する同様のフレームワークがあります。コンピューター・セキュリティ認証のための国際規格（ISO/IEC 15408）である、Common Criteria for Information Technology Security Evaluation（情報技術セキュリティ評価のためのコモンクライテリア）も重要な標準です。Common Criteriaは、光ネットワーク内のネットワーク・エレメントなど、ネットワーク機器の仕様、実装、評価プロセスを厳格で標準的な方式で確実に実施する方法を規定します。ドイツでは、ドイツ連邦政府の情報セキュリティ庁であるBSIが、Common Criteriaに対する認証を含むセキュリティ認証を発行しています。Common Criteriaに基づくBSI認証は、多くの場合にローカル認証の基礎として使用され、認証プロセスにかかる時間と費用を節約します。この一連の標準と認証プロセスは、サービス・プロバイダーとエンドユーザーに、暗号化ソリューションが標準によって義務付けられている厳格なラボテストと審査に合格し、規定要件への準拠が実証されているという安心感を提供します。

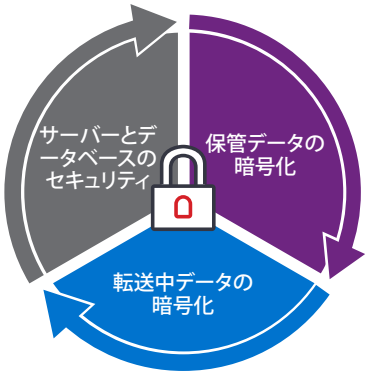

図1：転送中データの暗号化は総合的なセキュリティ戦略の一環

今日のネットワークのセキュリティ保護

保管中と転送中のデータをセキュリティ保護するために、現在、暗号化が広く使用されています。暗号化の傾向について調査したPonemonレポートによると、調査対象のグローバル組織のうち、暗号化戦略を持たないと回答した組織はたった13%でした。[3] 全業界の小規模から大規模までのすべての組織が、データセンターに保存されている情報を不正アクセスからプロテクトするためにあらゆる対策を講じる必要があります。データ漏えいの影響とコストは無視できないレベルに達しており、評判の低下、刑事訴訟の恐れ、規制違反による高額な罰金、顧客解約率の上昇など、組織が被る影響はますます大きくなっています。

現在、サーバー、データベース、ルーター、スイッチに保管されているデータについては、ユーザーアクセスと認証情報に基づいてデータをプロテクトする様々な技法が広く使用されています。一方、今日のWebスケール・ネットワークでは、広帯域通信がデータセンターの壁を越えてより大規模に、場合によっては世界規模のネットワークを横断して行われるので、大量の重要データが転送中の状態に置かれています。その結果、図1に示すように、包括的なITセキュリティ・アプローチに、総合的なセキュリティ戦略の一環として転送中のデータをプロテクトする堅牢な暗号化ソリューションを組み込む必要が生じています。事業者はプライベート・クラウドから送出されるデータを暗号化することで、転送中のデータが様々なセキュリティ・レベルのネットワークを経由して、宛先に到着するまでの間に不正傍受されないように防御できます。

多くの組織が、転送中のデータを暗号化する機能をセキュリティ戦略に加えていますが、これまでは転送中のデータをレイヤー2以上のレイヤーで暗号化することに重点が置かれていました。この方法は、データ処理量が少ない、または遅延が許されるなどの低速のITアプリケーションには適した方法となりますが、多くの場合、IPアプリケーションのデータのみをエンタープライズ規模で暗号化するアプリケーションには適しません。この暗号化ソリューションの導入をサポートする運用モデルは、図2に示すように、非常に煩雑でコストがかかります。多くの場合に、プロトコルごとにスタンドアロンの暗号化装置が必要になり、大量の遅延を発生させ、アプリケーションのスループットに影響を及ぼすため、帯域の利用効率が低下します。さらに、複数の独立した装置にわたって

3 Ponemon、Thales e-Security研究レポート「2018 Global Encryption Trends Study」2018年4月
https://go.ncipher.com/rs/104-QOX-775/images/2018-nCipher-Ponemon-Global-Encryption-Trends-Study-ar.pdf

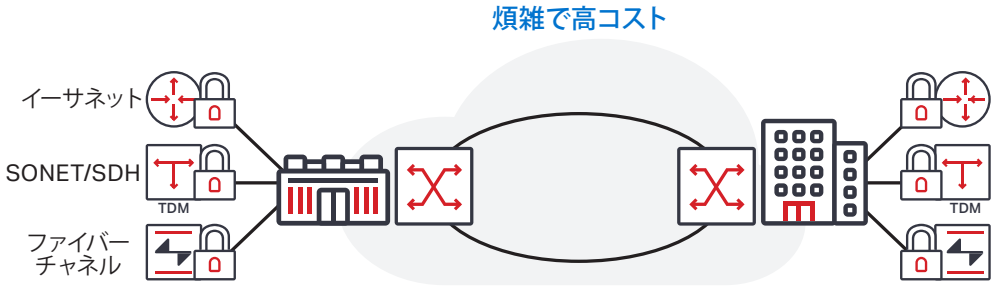

図2：マルチサービス・ネットワークに導入されている従来のプロトコル固有の暗号化

暗号化キーを管理して認証を行う必要があるため、運用が複雑になり、手間がかかります。また、様々な個別の装置にわたってエンドツーエンドでネットワークのトラブルシューティングを行うことによっても複雑さが増大します。また、このアプローチは、組織の転送中データ・プロテクション戦略に思わぬつまずきをもたらします。従来、組織のセキュリティ戦略では光ファイバーケーブルに対する侵入リスクは考慮されてきませんでしたが、光ファイバーケーブルに侵入して伝送中のデータにアクセスする脅威は実在します。光ファイバーは多くの場合、アクセスが非常に容易で、防御もされていません。しかるべきツールさえあれば、誰でも簡単に光ファイバーケーブルにタップを付けて、数日、数ヶ月、または数年にわたって見つかることなく、データを収集し続けることができます。トランスポート・レイヤーの暗号化ソリューションを導入することで、すべての転送中データを常時プロテクトできます。

Data Security with Optical Encryption
図解を今すぐダウンロード

WaveLogic Encryption

ネットワーク・データの機密性、完全性、可用性を保証するCienaのマルチレイヤー・セキュリティ・アプローチの一環として、CienaのWaveLogic Encryptionは、世界規模のインストール・ベースを持つプラットフォームに導入されている実証された暗号化テクノロジーと、世界中の600社を超える事業者に導入されている市場トップクラスの6500 Packet-Optical Platformの実証された信頼性を兼ね備えています。さらに、CienaのWaveLogic Encryption機能はCienaのスタッカブル相互接続システムのWaveserverとWaveserver Aiまで拡張されるため、フルラック搭載可能なスタッカブル構成のシンプルなDCIアプリケーション向けに、1RUの筐体で最大1.2Tbワイヤースピードの暗号化容量を実現します。

導入が容易

WaveLogic Encryptionでは、トランスポート・ネットワーク内のネットワーク・エレメントに暗号化機能が直接的に統合されているので、暗号化ソリューションの導入が非常に簡単です。このアプローチでは、図3に示すように、ネットワークの複雑さが軽減され、アプリケーションごとに異なる暗号化ソリューションを管理する必要がなくなります。このような運用の単純化は、認証とキー管理の専用ツール、企業の既存のPKIへの容易な統合など、暗号化ソリューションの管理にまで拡張されています。

6500プラットフォームが備える柔軟性により、お客様はサイトごとの容量、スペース、電源の要件に最適なシェルフサイズを選択し、費用対効果の高い方法で暗号化サービスを伝送することができます。このソリューションのもう1つの重要なメリットは、イーサネット、SONET/SDH、ファイバーチャネル、OTNなどのプロトコルへの依存性が全くないことです。そのため、柔軟なクライアントを幅広くサポートし、セキュリティ意識の高いお客様の複数のアプリケーションに対応できます。

24時間365日稼働する暗号化による差別化

CienaのWaveLogic Encryptionソリューションでは暗号化が常に有効になっており、すべてのネットワーク・トラフィックが必ず暗号化されるため、最高レベルのセキュリティを確保できます。暗号

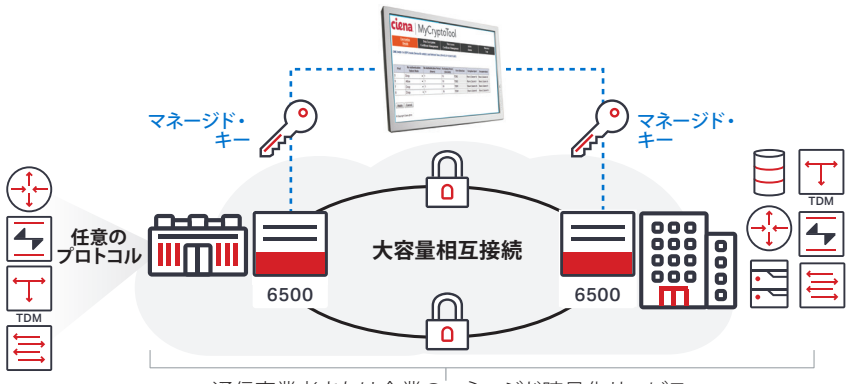

図3：Cienaの6500 WaveLogic Encryptionソリューション

化の有効化と無効化を切り替える機能があれば、柔軟性が向上すると考えるユーザーもいるかもしれませんが、単純な人的エラーが原因で、機密性の高いトラフィックが暗号化されていないネットワークを転送される可能性があります。事業者は、自社のネットワークがメトロ、リージョナル、長距離、海底を越えてグローバルに広がったときに、転送中のすべてのデータが常にプロテクトされる、差別化されたインフラを活用できます。さらに、超低遅延接続と経路/装置プロテクションの複数のオプションを提供する暗号化サービスを活用して、差別化されたSLA（サービス・レベル・アグリーメント）を迅速に提供することで、収益性と顧客定着率を向上させることもできます。

堅固な暗号化

CienaのWaveLogic Encryptionは、中立的な第三者機関により、Common CriteriaやFIPS認定などの業界標準のアルゴリズムと高度なセキュリティ機能で実装されていることが検証および認定されています。WaveLogic Encryptionは、標準ベースの認証メカニズム（X.509証明書など）を備えたFIPS認定のAES-256暗号化エンジンを提供し、企業の既存のPKIへのシームレスな統合を実現します。それに加えて、ハードウェアの6500とソフトウェア・コンポーネントの暗号化モジュールは、FIPS 140-2とCommon Criteria for Information Technology Security Evaluationの完全なBSI認証に準拠しています。これにより、サービス・プロバイダーとエンドユーザーは、暗号化ソリューションが暗号化アルゴリズム、キー交換メカニズム、ユーザー認証など、総合的な評価対象のすべてに準拠しているという安心感を得ることができます。

データ・プロテクションを向上させるために、認証とデータ暗号化の機能に2つの別々のキーセットが使用され、暗号化キー・ローテーションは分単位ではなく秒単位の間隔で高速に実行されます。AES-256データ暗号化セッション・キーは、トラフィックやスループットに影響することなく各回線ポートにおいて、ユーザーが介入することなく自律的にネゴシエーションされ、1秒ごとにローテーションされます。事業者は、楕円曲線暗号（ECC）をサポートする次世代の公開鍵暗号アルゴリズムを導入し、第1世代の公開鍵暗号システムと比べて大幅に安全性が向上した戦略を推進できます。

プログラマブルな100G～400Gワイヤースピードの暗号化

今日の大容量通信のニーズに対応するために、CienaのWaveLogic Encryptionは業界最先端のWaveLogicコヒーレント技術を活用し、柔軟で大容量のカスタマイズ可能な暗号化ソリューションを実現します。WaveLogic 3の機能をベースにするWaveLogic 3 Extremeは、追加の変調を使用して、より高度な方法で線形と非線形の両方の劣化を緩和することで、すべてのコヒーレント・ネットワーキング・アプリケーションに最高のパフォーマンスを提供します。この最先端ソリューションはソフトウェア・プログラマブルな変調を提供し、PSK変調方式による100Gワイヤースピードの暗号化、8QAM変調方式による150Gワイヤースピードの暗号化、16QAM変調方式による200Gワイヤースピードの暗号化を実現します。WaveLogic Aiは、WaveLogic 3のクラス最高のパフォーマンスをベースにして、400Gに最適化された高度なエンジンを使用することで、トランスポートの経済性を大幅に高めます。チャネル当たりの容量が2倍、同じ容量での伝送距離が3倍、サービス密度が4倍向上します。

事業者は、WaveLogic 3 Extremeライン・モジュールを6500上で各種クライアント・インターフェイスのいずれかと統合することで、10G、40G、または100Gサービス伝送などのトラフィック・ニーズに合わせてカスタマイズしたソリューションを柔軟に導入することができます。需要が増大した時には、この成長に合わせて拡張できるモジュールにより、クライアント・カードを追加するだけで、同じライン・モジュールをプログラムして200Gの暗号化トラフィックを伝送することができます。さらに、大容量の暗号化サービスをネットワーク全体に導入し、6500の大容量のパケット/OTNハイブリッド・ファブリックを活用することで、ネットワーク・リソース効率を最大限に向上させることができます。

Waveserver上では、事業者はわずか1RUの筐体で最大400Gb/sワイヤースピードのFIPS認定のAES-256暗号化回線容量を利用し、同じ装置で10GE、40GE、100GEクライアントの混成をサポートする柔軟性を得られます。プログラマブルな変調方式により、Waveserverは各アプリケーション/ニーズに合わせてワイヤースピードの暗号化回線容量を最適化して、2つの100Gb/s波長、150Gb/s波長、または200Gb/s波長を実現できます。事業者は安全性の高い超大容量の相互接続アプリケーションに対応するために、3つのトラフィック・モジュール（モジュールあたり最大400Gb/sの暗号化容量を提供）のサポート機能を使ってWaveserver Aiを導入し、1RUで最大1.2 Tb/sの暗号化容量を実現できます。WaveserverとWaveserver Aiは、メトロ、リージョナル、または長距離にわたって、非常に安全な超低遅延の転送中データのプロテクションを提供します。

6500の10Gワイヤースピード暗号化

事業者は、暗号化モジュール付き4x10G光トランスポンダーを利用して、費用対効果の高い方法で10G暗号化サービスを提供できます。このシングルスロットのモジュールは、プロトコルに依存しない暗号化された4つの10G回線ポートを介して40Gワイヤースピードの暗号化サービス容量を提供します。つまり、6500の全タイプのシャーシに暗号化機能を統合できるため、ネットワーク設計を単純化することができます。また、このモジュールは、FIPS 140-2 Level 3準拠の設計による強化されたセキュリティを実現し、ゼロ化機能の実装を通じて物理的なカード改ざんに対するプロテクションを提供します。これにより、たとえカードがシェルフに差し込まれていなくても、暗号化モジュールに対する物理的な改ざんが検出されると、直ちにすべてのデータがゼロに設定されて、機密性の高い重要な全データが確実に消去されます。

High-capacity Wire-speed Encryption Modules
データシートを今すぐダウンロード

シンプルになった暗号化管理

クラス最高のトランスポート・レイヤー・セキュリティ・ソリューションであっても、使いやすい統合された暗号化管理アプローチを利用できなければ、完璧なソリューションとは言えません。トランスポート管理から暗号化管理を分離することで、事業者または企業が保守するインフラストラクチャーの柔軟性を高めることができます。いずれの場合も、データの「所有者」であるエンドユーザーが、重要なデータに関連付けられた暗号化セキュリティ・パラメーターのフルコントロールを維持し、自社のセキュリティ・ポリシーによって義務付けられているとおりに新しいキーまたは証明書を発行し、同時にエンドツーエンドでセキュリティ・アラームやログに常に注意を払うことが重要です。

Cienaの6500 WaveLogic Encryptionソリューションには、ネットワークの分散管理のために設計された専用の暗号化管理インターフェイスであるMyCryptoToolが含まれています。エンドユーザー/セキュリティ責任者は、MyCryptoToolを使用して、通信事業者または企業のマネージド・ネットワークのセキュリティ・パラメーターとアラームを個別に管理することができます。使いやすいインターフェイスが特長のMyCryptoToolは、暗号化モジュールに安全に接続して相互認証を提供し、権限のあるセキュリティ担当者のみにアクセスを制限します。サービス・プロバイダーから暗号化サービスを購入する場合、他のすべてのサービスと同様に、サービス・プロバイダーがリンク、プロビジョニング、管理、パフォーマンス・モニタリングを管理しますが、サービス・プロバイダーが暗号化パラメーターに対するコントロールと表示機能を持つことはありません。同じ企業または官公庁で2つの異なるグループが暗号化ソリューションを導入して管理している場合にも、このアプローチが有効です。

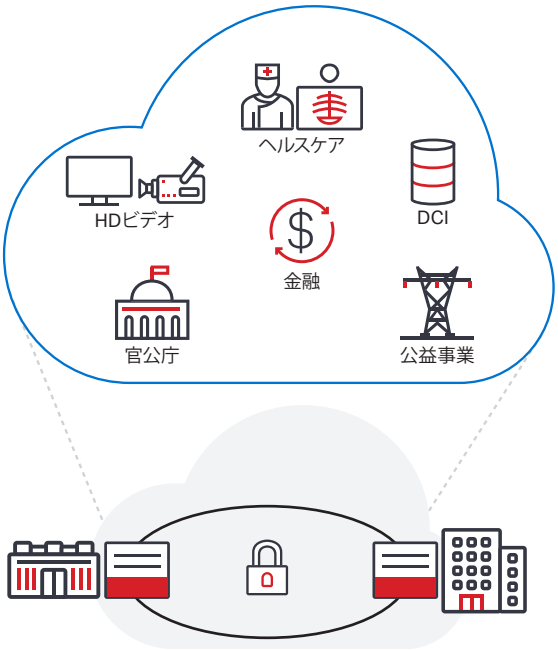

図4：*WaveLogic Encryption*の主要アプリケーションの例

主要アプリケーション

CienaのWaveLogic Encryptionソリューションは、現在のすべての大容量アプリケーションで重要な転送中データをプロテクトするように設計されています。これらのソリューションのメリットを活かせる主要なアプリケーションには、次のようなものがあります。

- 大容量ストレージと暗号化データ伝送を実現するエンタープライズDCI
- 異なるロケーション間で安全かつ高速な認証された通信を確立する必要がある官公庁
- 医療関係者同士で安全かつ効率的にタイムリーに連携するための高品質および低遅延の要件に対応するヘルスケア・アプリケーション
- マネージド・サービス・アプリケーション
- 高解像度ビデオや高速トレーディングなど、安全性と超低遅延伝送ソリューションを必要とする遅延が許されないアプリケーション
- 極めて重要な通信インフラをプロテクトする必要がある公益事業者

まとめ

光ファイバー・ネットワーク経由で配信される機密情報が増えるにつれ、今日の大容量通信は、サーバーのセキュリティと保管データの暗号化だけでなく、転送中データを暗号化する堅牢なソリューションを組み込んだITセキュリティ・アプローチを採用する必要があります。高い柔軟性とセキュリティに加え、運用と管理の容易さを兼ね備えたCienaのWaveLogic Encryptionは、費用対効果の高いスケーラブルなワイヤースピードの暗号化ソリューションを実現することで、街角、都市、国境、さらに海を越えて伝送されるすべての転送中データを常時プロテクトします。