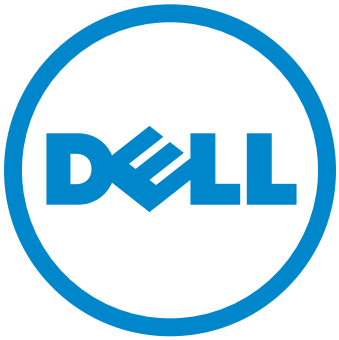
ネットワークのコンプライアンス

ホワイトペーパー



このホワイトペーパーは情報提供のみを目的として作成されたものであり、誤字脱字や不正確な技術情報が含まれている場合があります。本書の内容は現状のまま提供され、その内容について明示または黙示にかかわらずデルはいかなる責任も負いません。

© 2011 Dell Inc. All rights reserved. Dell Inc.の書面による許可なく、文書を無断で複写、複製、転載することを禁じます。詳細については、デルにお問い合わせください。

Dell、デル、*デル*のロゴ、*デル*のバッジ、および*PowerConnect*はDell Inc.の商標です。本書では、上記以外の商標や会社名が、その商標や会社名を使用する権利を有する団体またはその製品を示す目的で使用される場合があります。他社の商標および会社名は、一切デルに帰属するものではありません。

2011年11月

目次

今日のコンプライアンス

はじめに

情報技術（IT）は、規模、スピード、および範囲の面で、ビジネスの手法を根本から変えるまでになりました。ITの進歩は、ほんの20年前には想像もできなかった新しいサービスや機能を生み出し、医療機関や金融機関の運営方法から企業を組織する手段に至るまで、事実上すべてのものに影響を与えています。現在の消費者による情報へのアクセスは目を見張るものがありますが、その一方で、各組織は、運営のさらなる透明化に懸命に取り組んでいます。

また、IT分野のイノベーションはネットワーク関連の新しい需要も生み出し、企業や消費者の情報に対する新たな脅威ベクトルも出現しています。その結果、国際規制、連邦規制、州条例、地方条例、業界の規制など、データやリソースのセキュリティおよびプライバシーを確保するためのさまざまな規制が制定されました。ほとんどの組織では複数の規制や規則に基づいて業務を行っていますが、それらを取りまとめるための手段は、ほぼネットワークのみに頼っています。企業がコンプライアンスに取り組み始めた当初は、業界に適用される規制のみを考慮する、あるいはデバイスまたはネットワークセグメントに対象を絞る、というアプローチを採用していました。しかし、このようなアプローチは、現在ではほぼ有効性を失っています。今日におけるコンプライアンスを実現するには、ネットワーク全体を包括的に監視する以外に手段がありません。

しかし、ネットワークがさまざまな場所や拠点にまで及んでいる可能性を考慮すると、ネットワークを包括的に監視することは極めて難しいと言えます。さまざまな規制の多くが、自社のインフラストラクチャに対してだけでなく、ビジネスパートナーのインフラストラクチャに対してもコンプライアンスを求めています。さらに、ITの能力の変化や向上に伴って規則も変更および改善され、現時点で規制に準拠しているテクノロジーがすぐに時代遅れになってしまうことも考慮すべき問題です。

コンプライアンスにおいて必要な鳥瞰図を描く上で大きな問題になるのは、ネットワークそのものです。今日のネットワークのほとんどは当面の需要に対応するために構築されたため、共通点のないデバイスで構成された、非効率的な「寄せ集め」になっていることがほとんどです。ネットワークでトラフィックを送ることは可能ですが、デバイスはコミュニケーションを行うために作られたものではありません。こうした状況が、一貫性のある情報を集めにくくしているのです。

このホワイトペーパーでは、今日求められているコンプライアンスの主なタイプについて広く概説します。また、全体として、特定のデバイスや分野ではなく、ネットワークを中心としたコンプライアンスに対するアプローチについて検討します。最後に、デルのネットワーキングソリューションがどのようにネットワークの最適化、機敏性、オープン性に関する指針に基づいて構築されているかを示します。デルのネットワーキングソリューションを利用すると、既存のインフラストラクチャを活用できるだけでなく、ネットワークの設計コストを低く抑えつつ、ビジネスおよび法令順守の要件を満たすことができます。

コンプライアンスを取り巻く状況

以下の表で、今日の主なコンプライアンス要件のいくつかについて簡単に説明します。この表は、国際規制について説明しようとするものでも、任意の規定について詳細に調査するためのものでもありません。この表の目的は、どのようにすれば任意の組織が複数の規制に同時に準拠できるかを示すことにあります。

法令	説明	適用範囲
EUデータ保護条令	個人データの処理に関する個人の保護、および当該データの自由な移動について規定した条例です。この条例は、欧州連合（EU）内での個人データの処理について規定するものであり、EUのプライバシーおよび人権保護法の重要な構成要素です。	個人データを収集または配布するほぼすべての組織に適用される包括的なデータ保護法。
連邦情報セキュリティ管理法（FISMA）	連邦政府によって規制された情報を保管する場合に適用される、セキュリティ管理に関する要件について規定した法令です。この法令は、連邦機関全体に及ぶ計画を策定、文書化、および実施する上で、各連邦機関に対して、その業務および資産を支える情報および情報システムのセキュリティを確保することを求めるものです。	情報（別の機関、請負業者、または他の供給者によって提供または管理される情報を含む）の作成、使用、保管、または伝送を行う機関。
グラム・リーチ・ブライリー法（GLBA）	金融機関が保管する個人の財務情報の守秘義務と完全性について規定した法令です。 この法令の主な規則に、金融機関による顧客個人の財務情報の収集と開示について定めた「金融プライバシー規則」があります。 この規則は、金融機関であるかどうかにかかわらず、このような情報を受け取る企業にも適用されます。「セーフガード規則」は、すべての金融機関に対して、顧客情報を保護するための予防策を策定、実施、および維持することを求めるものです。	顧客の個人的な財務情報を受け取る金融機関またはその他の企業（信用調査機関、不動産鑑定士、住宅ローンブローカーなど）。
国際標準化機構（ISO）	さまざまな国際標準組織の代表者で構成された、国際的な標準設定団体です。ISOは、ISO/IEC TR 17799:2000（情報セキュリティマネジメントの実践のための規範）や、組織において情報セキュリティマネジメントを開始、実装、維持、改善するためのガイドラインと一般原則について定めたISO/IEC 27002:2005など、各種の標準およびレポートを作成しています。	細目ごとに異なります。詳細については、http://www.iso.orgをご覧ください。
医療保険の相互運用性と説明責任に関する法律（HIPAA）	特定可能な患者の医療情報のプライバシーとセキュリティに関する要件などについて規定した法令です。プライバシーについては、紙または電子ファイルにかかわらず、すべての記録が対象になります。セキュリティについては、電子情報が対象になります。	患者の医療記録の作成、使用、保管、伝送を行うすべての部署（ビジネスパートナーの部署や離れた場所にある診療所を含む）。

ペイメントカード業界データセキュリティ基準（PCI DSS）	カード払いの処理を行う組織が、クレジットカード詐欺、ハッキング、およびその他のセキュリティに関する各種の問題を防止できるようにするための指針として、主要なクレジットカード会社が策定した基準です。クレジットカード情報の処理や保管を行う企業、またはクレジットカードによる支払いを処理できなくなるリスクのある企業。売買業者やサービスプロバイダは、PCI DSS Qualified Security Assessor（QSA）を有する企業による監査を受け、コンプライアンスに関する検証を行う必要があります。	クレジットカードによる支払いサービスを処理するすべての組織または部署。この基準は、垂直業界すべてに適用されます。
サーベンス・オクスリー法（SOX法）	米国の2人の 連邦議会議員（ポール・サーベンス上院議員とマイケル・オクスリー下院議員）が提出し、2002年に成立。報告された財務諸表の正確性に関する企業経営陣の個人的な責任を重視および厳格化した、株式公開企業の財務データのプライバシーと完全性を保証するための法律です。	すべての株式公開企業。
Control Objectives for Information and related Technology（COBIT）	COBITは規制ではありません。ITガバナンスや情報技術（IT）の管理に関する一連の実践規範（フレームワーク）です。	
国立標準技術研究所（NIST）	NISTは規制ではありません。NISTは、コンプライアンスを構築するための基盤となるベストプラクティスの標準を策定しています。	
CFR（連邦規則集）17巻240条17項a-4または17項b-4	データ保持およびストレージメディアの要件に関する種類と期間について規定されています。	ブローカー/売買業者、金融サービス。
CFR（連邦規則集）21巻II章	FDAのセキュリティ、法令順守、監査能力について規定されています。	製薬メーカーおよび医療機器メーカー。
家族教育権とプライバシー法（FERPA）、1974年	FERPAは、中等教育を修了した学生が教育の記録について詳細に調べる権利について規定し、それらの記録を第三者に開示する際の条件を定めたものです。	高等教育機関および従業員を雇用している企業。

コンプライアンスと企業

あなたが勤めている会社は、さまざまな規制に直接または間接的に従っている可能性があります。コンプライアンス責任者から1年または四半期ごとの記録とレポートを提出するよう要求されて、これらの規制の存在を知ることもあります。しかし、場合によっては、会社が規制に従っていることに気付かないことさえあるかもしれません。ペイメントカード業界データセキュリティ基準（PCI DSS）は、このタイプの規制です。PCI DSSは法律ではなく、主要な5つのクレジットカードブランドによってまとめられた、極めて規範的な一連の要件です。PCIは、積極的に違反を探すわけではありません。PCIが行うのは、セキュリティ違反への対処です。医療などの特定の業界は、PCIに準拠することを求められていますが、準拠していないことも珍しくありません。こうした状況は、医療業界向けのHIPAA法にPCIのコンプライアンスも対象として含まれているだろうという誤解から生じる場合があります。しかしHIPAAは、

実際には、PCIのような「規範的」な規定ではなく、「目標指向」の規定の1つです。HIPAAでは、結果が調査されますが、その結果に至る過程はさまざまです。一方、PCIでは、特定のネットワーク要素が特定の場所に必要になります。

コンプライアンスに関する規制やその影響を受ける業種の数は、毎年増え続けています。コンプライアンスに必要な情報をまとめることは、それだけで大規模なイニシアチブになる場合があります。コンプライアンスに関する管理業務や定期的なレポート作成業務は、現在では、コンプライアンス責任者だけではなく、ネットワークを管理しているIT部門やセキュリティの専門スタッフも行っています。これらの各個人が従事することになると思われる現在および将来のイニシアチブには、ネットワークセキュリティ、差別化されたアクセス制御、リアルタイムでのコンプライアンスの修正とレポート作成、インフラストラクチャのコンプライアンスの実施と管理、インフォメーションストアの保管と回復などが含まれるでしょう。

このプロセスでは、ネットワークの各所に設置されたさまざまなIT機器からデータを収集し、そのデータを照合して、必要に応じて対策を講じる必要があります。また、レポートの作成やポリシーの適用を行ったり、コンプライアンス組織から要求された所定の形式でデータをまとめたりする必要もあります。インフラストラクチャおよびセキュリティデバイスの多くは、これらの機能の一部を備えていますが、ネットワーク内の他の要素と相互運用できるように設計されていない場合もあります。この問題は、プロセス全体において人為ミスが発生しやすいという事実により、さらに複雑になっています。

コンプライアンスの実践

何らかの規制に準拠することによる影響は、業界に関係なく、ほぼ確実に生じます。特に、既に目一杯働いているスタッフに必要な時間を考慮すると、業務を通常通り行いながらコンプライアンスを実践する最適な方法について、よく検討する必要があります。デルは、まずネットワークに着手すべきであると考えています。その理由は、すべてのセキュリティ/ITインフラストラクチャが稼働する基盤がネットワークであるためです。ネットワークは、セキュリティやプライバシーに関する要件と同様、組織全体に浸透しているため、コンプライアンス要件を全体的な視点で捉えるためのきっかけとしては、最も合理的な部分であると言えます。

信頼性の高いネットワーキングソリューションベンダーなら、企業活動を萎縮させることなく、規制に準拠するために必要なベストプラクティスを提供できます。ネットワーキングソリューションベンダーについて調査する際に検討すべき具体的な項目を、以下に示します。

ITとコンプライアンスの専門知識の結合

ITは実際に、コンプライアンスイニシアチブが成功するかどうかを左右します。その一方で、ビジネス要件は満たさないが、規制には厳密に準拠したネットワークを構築しても、企業のニーズは満たされません。ビジネス要件の達成とコンプライアンスの両方において高い評価を得ているソリューションベンダーを見つけることが重要です。デルのネットワーキングソリューションは、必要なデバイスを提供するだけではありません。ソリューションに加え、必要な専門知識も提供することができます。デルは、規制に準拠したネットワークを実現するソリューションを提供できるだけでなく、デルの専門スタッフは、セキュリティの評価から、コンセプトの提案、導入、継続的かつ合理的な管理、レポート作成に至るまで、すべてのプロセスをサポートすることができます。

安全な、最適化されたネットワーク

複雑なネットワークの管理、セキュリティ保護、制御、運用は、骨の折れる作業です。ほとんどのネットワークは、最初から複雑であったり、安全でなかったりしたわけではありません。しかし、時間と共に複雑さが増し、安全性が低下することもあり得るのです。そして、特有の複雑さが原因で、ネットワークが次のような状況になる場合があります。

- 意図せず、潜在的にセキュリティ侵害が発生しやすくなっている（PCI、HIPAA、チャイニーズウォール）
- 管理不能になり、新しいポリシーの規則セットの導入がほぼ不可能になる
- リアルタイム/履歴レポートの作成がサポートされておらず、その結果、記録の保管、コンプライアンスレポートの作成、または回復が困難になり、政府機関に対してコンプライアンスを実証できない

デルのネットワーキングソリューションでは、インフラストラクチャ、セキュリティ、およびストレージの観点から、複雑で非効率的なネットワークを合理化し、コンプライアンスを実践しやすいネットワークへと変えることができます。このアプローチは、特定の要件に基づいて、ネットワークアーキテクチャに組み込まれています。デルは、現在のネットワーキングのニーズを満たすソリューションを提供するだけでなく、将来、ビジネスやコンプライアンスに関する要件が変更されたときにも対応可能な、上位互換性を備えたネットワークを構築します。

オープンスタンダード

コンプライアンスについて検討するとき、紙の上では、単一ベンダーのソリューションが魅力的に見えることもあります。単一ベンダーの製品を利用すれば、シンプルで最適化された、規制に完全に準拠したネットワークを簡単に構築できると考えるかもしれません。しかし残念ながら、そのようなことはほとんどありません。「総合ショップ」を謳っているベンダーのほとんどは、他社製の機器との相互運用ができない独自のテクノロジーへの囲い込みを行います。これはベンダーにとっては好都合ですが、顧客は独自の戦略を選択したり計画したりすることができなくなります。オープンなエコシステムとアーキテクチャを利用すると、ネットワークの複雑さ、ベンダーロックイン、非効率的なネットワークから解放され、それと同時に、独自の戦略を維持できるようになります。また、デルのネットワーキングソリューションのオープンで標準ベースのアプローチを利用することにより、監視およびレポート作成をシンプル化できる、相互運用性、拡張性、柔軟性に優れた仮想化アーキテクチャを導入することができます。これにより、コンプライアンスの実践に伴う負担を軽減できる上、思い通りにビジネスを行えるようになります。

将来のビジネスに対応した計画

ビジネス環境も、企業が準拠する必要があるコンプライアンス関連の規制も、常に変化するものです。重要なことは、今選択したソリューションが、上位互換性を備え、機敏性と柔軟性に優れた戦略的なプラットフォーム（大規模な中断やテクノロジーの転換を生じさせずに、将来のITおよびコンプライアンスに関する規制に対応できるプラットフォーム）として稼働するということです。 デルのネットワーキングソリューションは、今日のダイナミックなビジネス環境に必要な柔軟性と機敏性を提供します。デルは、お客様のネットワークが将来のビジネスに対応できるようにするための「方程式」を変更するお手伝いをします。さらに、将来直面する可能性があるコンプライアンス関連の規制に準拠するために、「前向きな姿勢」を保ち続けます。

まとめ

ネットワークのコンプライアンスへの対応方法を長期的かつ厳密に調査しなければ、今日のコンプライアンスを取り巻く状況について検討することはできません。主要な規制は一部重複する場合があるため、ネットワークが複雑になると、分散型のインフラストラクチャ全体に渡って、コンプライアンス関連のすべての規制に常に準拠することが難しくなります。コンプライアンスの実施とレポート作成は、貴重なスタッフの時間を奪う可能性があり、要件の正確性や履行を妨げることもよくあります。それでも、ネットワークの稼働状態を保ち、ビジネス競争力を維持しながらプロセス全体を進めなければならないのは言うまでもありません。

デルのネットワーキングソリューションでは、お客様が必要とする専門知識を提供します。デルが行うアプローチにはすべて、オープン性、機敏性、最適化、柔軟性といった要素が含まれており、いずれもお客様の目標達成には不可欠なものばかりです。デルのコンプライアンスに対するアプローチも同様です。デルは、完全なソリューションとお客様が必要とする専門知識を提供し、企業に影響を及ぼす今日の各種の規制に準拠できるようにします。さらに、お客様のビジネスを将来に向けて前進させるために、さまざまな機会を利用できるよう準備しています。

デルは、ネットワークを最大限に活用し、お客様の可能性を最大限に引き出します。