



データセキュリティ コンプライアンスを実現する 8つのステップ

規制強化に対応するための
機密情報資産のプライバシーを守る、
ステップバイステップガイド

データセキュリティコンプライアンスを実現する 8つのステップ

規制強化に対応するための 機密情報資産のプライバシーを守る、 ステップバイステップガイド

目次

機密データを保護し、コンプライアンスを実証するために、セキュリティおよびコンプライアンス部門が把握すべきポイント	3
ステップ 1 リスクの量的把握と質的把握	3
ステップ 2 プライバシーや規制コンプライアンスに対応したポリシーの設定	4
ステップ 3 リスクの管理と統制	5
ステップ 4 パートナー、サプライヤ、およびサービスプロバイダーの監視	6
ステップ 5 従業員教育と認知度の向上	6
ステップ 6 適正評価と監査のサポート	7
ステップ 7 役員および経営陣へのレポート	7
ステップ 8 リスク低減のための継続的な監視とレポート	8
まとめ	9
Vontu について	9

機密データを保護し、コンプライアンスを実証するために、セキュリティおよびコンプライアンス部門が把握すべきポイント

この 1 年でデータセキュリティや企業情報の機密保持に関する問題が急増し、「ネットワークセキュリティが十分でない」と企業の経営者に警鐘を鳴らしています。企業は、金銭的な損失やブランドの失墜を避けるためだけでなく、規制遵守を実証する上でも、データ自体を保護する必要があります。GLB(グラムリーチビリー)法、HIPAA、クレジットカード業界のセキュリティ基準(PCIDSS)、EU データ指令など、いくつかの国際基準や米国連邦政府のデータプライバシーに関する規制や 35 を超える米国州法では、企業に機密情報である顧客データや内部データの保護を義務づけています。Vontu ソリューションを導入すれば、官公庁は FISMA(連邦情報セキュリティマネジメント法)、NIPP(国家インフラストラクチャ防護計画)、およびホワイトハウス OMB(行政管理予算局)と NIST(米国標準技術局)の PII(プロフェッショナル賠償保険)などの規制も遵守できます。コンプライアンス違反のリスクを軽減するために、セキュリティ担当部門は、データ漏えいインシデントの頻度や重大度を低減するプロセスやテクノロジーを導入する必要があります。

情報漏えい対策(DLP)ソリューションのリーダーである Vontu は、Charles Schwab、Equifax、Raymond James Financial などの企業をはじめ、米国連邦政府機関や、エネルギーおよび公益事業、金融サービス、保険、ハイテク、小売、通信、製造、メディア娯楽、医薬品、ヘルスケアなどさまざまな業界のユーザー企業が、外部規制ならびに内部データのセキュリティポリシーの遵守を実証するために役立っています。機密情報の漏えいリスクを軽減し、規制遵守の証明を支援するため、本ガイドは作成されています。本ガイドは、各組織のデータセキュリティのプロセス、ポリシー、およびテクノロジーを評価および強化するための具体的なステップについてまとめたものです。

ステップ 1 リスクの量的把握と質的把握

顧客データや従業員データなどの機密情報を保護し、コンプライアンスを実証する第一のステップは、リスクを把握することです。最新の統計によると、電子メールの 400 件に 1 件、ネットワークファイルの 50 個に 1 個に機密情報が含まれていることがわかりました。しかし、これらのデータを明確に把握できている企業はごくわずかです。ほとんどの企業では、機密データがどこに保存され、どこで使用されているか、また、検出したデータはどのように処理すればよいか把握できていません。リスクを定量化するために、セキュリティ担当部門は、リスクにさらされている機密データについて、より詳細に知る必要があります。顧客アカウント、患者の医療情報、財務記録など、どのデータがリスクにさらされているか？ 機密データはファイルサーバー、データベース、ノートPC、デスクトップ、その他のデータ保存場所のどこに保存されているか？ 電子メール、インスタントメッセージ、FTP などを使用して、どれくらいの量の機密データがどのようなルートで社外に転送されているか？ どのような極秘情報がローカルドライブにダウンロードされたり、CD/DVD にコピーされたり、あるいは USB ドライブやその他のリムーバブルディスクにコピーされているか？ また

データセキュリティコンプライアンスを実現する 8 つのステップ

それらの責任の所在はどこにあるか？ インシデントの重大度はどれくらいのものか？ このような質問への回答を得ることによって、セキュリティ担当部門はリスクを量的、質的に把握し、プロアクティブなプロセスとテクノロジーを導入する次のステップへ進むことができます。

Vontu は、ユーザーの組織がデータセキュリティのコンプライアンスを実証し、情報資産への脅威と潜在的なコンプライアンス違反を特定するのに役立ちます。さらに、ネットワーク上に保存されているデータ、転送中のデータ、また、ノートPCにダウンロードされたり、USB ドライブやその他のリムーバブルメディアにコピーされるデータについて、リスクにさらされている特定の機密データをピンポイントで発見し、セキュリティ違反による潜在的影響の頻度と重要性を定量化できるようにします。Vontu の導入により、セキュリティ担当部門は、ハイリスク分野について次の情報を完全に把握できます。

- ファイルサーバー、データベース、Microsoft® SharePoint®、Lotus Notes®、Documentum®、LiveLink®、Web サーバー、Microsoft® Exchange、エンドユーザーのノートPC やデスクトップ、その他のデータ保存場所に格納されている機密データの場所と露出の度合い
- ネットワークから外部に出る機密データ（顧客情報、財務情報、知的財産など）の量と種類
- ポリシーに違反する可能性のある機密情報漏えいの頻度と重大度
- 機密データが組織外に転送される手法
- ローカルドライブにダウンロードまたは USB ドライブ、CD/DVD、iPods® などのストレージデバイスにコピーされる機密データの種類
- 機密データ違反について責任を負う当事者とその重大度
- 違反している可能性があるコンプライアンスの規制

Vontu Risk Assessment を使用してリスクの定量化を行った後、データセキュリティポリシーを設定し、保護のためのテクノロジーを導入し、さらに、コンプライアンスを実証するために予防措置を講じることができます。

ステップ 2 プライバシーや規制コンプライアンスに対応したポリシーの設定

政府規制や従業員プライバシー法は、組織内でデータ保護ポリシーを構築し導入する上で重要な役割を果たします。組織のグローバル化が進むにつれ、ポリシーや人材監視に関する国際法が及ぼす影響も拡大しています。プライバシー法や規制は国ごとに異なりますが、組織がコンプライアンスを実証できるようなポリシー作成のガイドラインとなる要件が多数あります。

- データ自体のセキュリティを保護する
- 規制遵守を実証する
- 従業員のプライバシーを保護する

データセキュリティコンプライアンスを実現する 8 つのステップ

Vontu のポリシーに基づいたデータ検出、保護状況の監視、防止機能を使用することにより、これらの要件を満たすことができます。事前に定義したポリシーテンプレートを使用して、データの保存場所や使用場所に関係なく、GLBA、HIPAA、PCIDSS、FISMA、OMB、NIPP、PIPEDA などをはじめとする、50 以上のデータプライバシー規制の国際法、連邦法および州法の潜在的違反がないかを調査できます。ポリシーテンプレートは、組織に固有のデータ保護要件やオペレーションの管轄に合わせて柔軟に調整することも可能です。このような柔軟性により、規制変更の際にポリシーを対応させ、継続的なコンプライアンスを実証することができます。

ステップ 3 リスクの管理と統制

セキュリティ担当部門とコンプライアンス担当部門は組織内のリスクと重要性を特定した後、情報漏えい対策(DLP)ソリューションを導入することによって、リスクを低減し、コンプライアンスを実証することができます。この段階では、(保存場所や使用場所に関係なく)データの保護、検出精度、規制遵守に対応したポリシー、全社規模への拡張性、その他の要件が意思決定プロセスにおける重要な要因になります。効果的な情報漏えい対策ソリューションでは次のことができます。

- 露出を軽減し、コンプライアンスを保証するために、正確に脅威を検出する
- 照準を絞ったポリシーベースの監視によって、従業員プライバシーの違反を防ぐ
- 保存されている機密データへの未承認のアクセス、改ざん、使用を防止する
- ネットワークまたはエンドポイント上の機密データが社外に流出するのを防ぐ
- エンドポイントに保存されている機密データを監視し、データの不適切な使用、送信、また、USB ドライブ、CD/DVD、iPods® などのストレージデバイスへのコピーを防ぐ
- ファイルサーバー、データベース、Microsoft® SharePoint®、Lotus Notes®、Documentum®、LiveLink®、Web サーバー、Microsoft® Exchange、エンドユーザーのノートPC やデスクトップ、その他のデータ保存場所上で露出される機密データを検出して保護する
- 暗号化ポリシーを自動的に施行する
- レポーティングおよびポリシー施行を自動化して、規制遵守を実証し、システムおよびインシデント対応、通知、ワークフロー、コンプライアンスレポーティングを一元化する

Vontu を導入することで、組織内で機密データ違反のリスクを低減できます。保存場所や使用場所に関係なく、コンプライアンス要件に合わせて固有に設定したポリシーに従ってデータが継続的に検査されます。潜在的な違反が検出された場合、Vontu では従業員への通知とエスカレーションによって矯正を自動的に実施し、従業員の行動を変更したり、既存のビジネスプロセスにおけるコンプライアンスの不備をピンポイントで特定することができます。また、保護すべきデータで暗号化されていないものを見つけ出し、送信される前に暗号化サーバーに自動的に転送させます。最後に、集中レポーティングおよび分析を使用して、セキュリティ担当部門がコンプライアンスを実証し、より迅速かつ確信を持って監査に対応できます。

ステップ 4 パートナー、サプライヤ、およびサービスプロバイダーの監視

包括的なコンプライアンス戦略には、組織の中だけではなく、ビジネスパートナー、サプライヤ、その他外部のサービスプロバイダーのための規定も含める必要があります。

複数のパートナー間でデータを共有する組織のために、Vontu は機密情報を保護し、コンプライアンス義務に対処するための専用機能を提供します。その 1 つが、複数のネットワークのエントリポイントを網羅し、パートナーのサイトを含めた、Vontu の集中ポリシー管理機能です。この機能を使用すると、アウトソーシングパートナーのデータセンターに監視機能を導入し、集中的に管理できるようになります。セキュリティ担当部門は、統合されたダッシュボードから潜在的なデータ違反を特定し、違反者に警告を送信し、直ちにプロセスを修正することができます。最後に、アウトソーシングによってデータが海外の組織に使用されるケースが多いことから、Vontu には、グローバルなコンプライアンス要件に対応した機能が組み込まれています。ポリシー管理およびレポーティングを一元化することで、EU データ指令などのグローバルな従業員監視およびプライバシー規制に対応させながら、組織のデータ保護のニーズも維持したポリシー調整が可能になります。

ステップ 5 従業員教育と認知度の向上

大手調査会社Gartnerによれば、データ漏えいが発生したセキュリティインシデントの 70% は、従業員、請負業者、機密情報にアクセスできるその他の作業者を含むインサイダーによるものと報告しています。さらに、ほとんどのインシデントは、悪意を持って行われたのではなく、不注意によるミスやポリシーの理解不足の結果生じたものです。このようなインサイダーによる脅威を削減するために、組織内での認知度の向上や教育活動を通じて、従業員の行動を変える必要があります。

Vontu を使用すると、従業員の行動を変え、日常的にデータ漏えいが発生している業務プロセスを是正することができます。たとえば、インシデントが検出されるとすぐに、Vontu の送信者通知機能によって従業員にメッセージが自動送信されます。これは従業員にインシデントの発生を知らせ、組織内のポリシーを確認させるためのカスタムメッセージです。インシデントの重大度が高い場合は、問題が自動的に管理部門に報告されるように Vontu を設定することができます。リアルタイムの従業員教育とエスカレーションは、組織内のデータ漏えいリスクを低減し、規制コンプライアンスを実証するために役立ちます。

ステップ 6 適正評価と監査のサポート

セキュリティ担当部門とプライバシー担当部門は、外部規制や内部ポリシーのコンプライアンスを証明する必要があります。コンプライアンスの証明には、機密情報の検出、管理、制御などのプロセスおよびコントロールの詳細な説明と、従業員プライバシー規制の遵守が含まれます。外部規制については、罰金が科せられたり公的な信頼を失墜する不安から、もっとも重視されることがありますが、内部ポリシー監査も対応に要する時間とリソースを考えると重要な問題です。外部監査と異なり、内部監査は必ずしもインシデントの発生によって実施されるものではなく、多くの場合、外部監査よりも厳格に実施されます。

Vontu は、セキュリティ担当部門が内部監査と外部監査の両方により徹底的に、かつ、最小限のリソースと時間で対応できるようにします。Vontu のソリューションでは、違反が疑われるすべてのケースについてインシデントのスナップショットを作成し、調査や監査をサポートします。さらに、幅広いコンプライアンスレポートを提供して、リスク領域をピンポイントで特定し、長期的なリスク削減を実証するためにトレンド分析を提供します。これらの分析情報をもとにセキュリティ担当部門はコンプライアンスを実証し、監査の信頼性を高め、規制要件に対応したプロセスとテクノロジーの導入を示すことができます。

ステップ 7 役員および経営陣へのレポート

コンプライアンス違反がおきた組織は社会的な評判が低下し、ブランドが損なわれます。こういったケースが増えてきたために、経営者の間で情報漏えい対策への認識が高まっています。セキュリティ担当部門にとって経営者へのレポートは、コンプライアンス要件に対処し、継続的なリスク低減を示すための重要なステップです。経営者が求める基本的な分析情報には次のものが含まれます。

- **定量化した現在のリスク。** データ漏えい対策リスクの詳細情報が得られ、組織内の他のリスク領域と関係が認められる場合があります。
- **組織分野別のリスク。** リスクが最も大きい分野を明確に把握することで、特定分野のオペレーションに絞り込んでコンプライアンス対策を強化することができます。
- **潜在的な規制リスク。** この情報を得るには、国際法、連邦法、州法のプライバシー規制に関する組織の責任を明確にする必要があります。
- **継続的なリスク低減。** この情報は、責任軽減のためにとられたプロアクティブな対策の証拠となるため、最も重要な情報と捉えられます。

データセキュリティコンプライアンスを実現する 8 つのステップ

Vontu のレポートによって、セキュリティ担当部門は最も重要な問題にプロアクティブに対処できます。Vontu のお客様は、エグゼクティブダッシュボード、分析、監査記録を使用して、組織内のリスクを定量化し、規制上の責任を管理者に通知し、長期的なリスク削減を明示するための重要なエグゼクティブレベルの指標を提示することができます。Vontu エグゼクティブレポートには、例として次のものが含まれます。

- 事業部別リスクレポート
- コンプライアンス規制違反の可能性
- 事業部別違反の可能性
- アウトソーシングパートナー別の違反の可能性

ステップ 8 リスク低減のための継続的な監視とレポート

コンプライアンスの観点から、規制担当者と組織内外の監査機関は、組織がプロアクティブかつ継続的なリスク緩和を図っているという証拠を求めることがよくあります。コンプライアンス目標を実現するには、組織が潜在的な違反を特定し、明白な傾向を明らかにし、崩壊した業務プロセスを是正するために、継続的にデータ保護ポリシーの有効性を評価する必要があります。

Vontu を導入することで、組織はデータ漏えいリスクを継続的に低減することができます。Vontu をインストールした後、お客様はリスクのベースラインを設定し、違反が発生する可能性のあるすべての分野でコンプライアンスを推進するためにポリシーの絞り込みを開始します。システムが稼働すると、通知機能、メッセージ選択ブロック、ポリシーベースの暗号化などの機能によって違反が回避されます。また、Vontu の履歴レポートとトレンド分析を使用して、セキュリティ担当部門は監査要求に対処し、リスク削減とコンプライアンスの向上を実証することができます。

まとめ

グラムリーチビリー法、HIPAA、FISMA、OMB などの規制と 35 以上の州法データプライバシーポリシーによって、グローバルに展開する企業や官公庁は、不注意または悪意によってプライベートなデータが漏えいしないように保護する義務があります。この規制管理は、組織が包括的な情報漏えい対策の一環として取り入れなければならない、新たな取り組みの一面を意味しています。しかし、規制条項を知ることはその第一歩に過ぎません。リスクの緩和は、現在の露出の度合いを明確にし、データ保護のプロセスとテクノロジーを導入し、継続的な改善のための継続的な分析と評価を実施する必要がある、持続的なプロセスなのです。

データ漏えい対策ソリューションのリーダーである Vontu は、組織がデータを漏えいするインシデントの発生頻度と重大度を低減してブランドと評判を守り、顧客データや知的財産を保護し、コンプライアンスを実証することを可能にします。Vontu Data Loss Prevention 8 は、エンドポイントとネットワークベースのソフトウェアの両方を組み合わせた初めての統合ソリューションで、保存場所や使用場所を問わず、機密データを正確に検出して自動的に保護します。Vontu の多層化アーキテクチャでは、データがネットワーク上と未接続のエンドポイントのどちらに保存されていても、悪意または不注意によるデータ漏えいを防止できます。また、ネットワークゲートウェイやエンドポイントからのデータ漏えいも阻止します。

Vontu について

Vontuは、2007年にシマンテックが買収した、エンドポイント技術とネットワーク技術を組み合わせ、機密データを保管場所や使用方法にかかわらず正確に検出し、自動的に保護する情報漏えい対策(DLP)ソリューションで業界リードするプロバイダーです。データ漏えいリスクを減らすことにより、Vontu社は組織が世間の信頼を高め、コンプライアンスを示し、競争力を維持できるように支援します。データを最重要視する世界最大規模の企業や政府機関が Vontu 社の顧客となっています。Vontu 社は IDG の InfoWorld 2007 Technology of the Year Award「Best Data Leak Prevention」や SC Magazine による 2006 U.S. Excellence Award「Best Enterprise Security Solution」、および Global Award「Best New Security Solution」をはじめとする数々の賞を獲得しています。製品の詳細情報はwww.vontu.comをご覧ください。



Copyright ©2008 Symantec Corporation. All rights reserved. SymantecとSymantecロゴは、米国におけるSymantec社およびその関連会社の登録商標です。その他の会社名、製品名は各社の登録商標または商標です。
製品の仕様・価格は、都合により予告なしに変更することがあります。本カタログの記載内容は、2008年7月現在のものです。

株式会社シマンテック

〒107-0052 東京都港区赤坂1-11-44 赤坂インターシティ

www.symantec.com/jp/vontu

E0807WP0-IN-DLP8STEP