



## コンプライアンス対策ソリューション

*Know the **Unknown**™*

**NIKSUN**®

[www.niksun.com](http://www.niksun.com)

WHITEPAPER

カリフォルニア州法 SB1386 は個人情報の秘密に関する規制を定め、暗号化されていない個人情報が権限のない人物によって入手された場合は、本人へ通知するよう要求しています。

顧客データが個人情報漏洩もしくは盗難に遭った場合や、集団訴訟が起きた場合に結果として生じる罰金は、一部の企業組織にとっては壊滅的な打撃となります。

## 論 点

規制による要求は、企業ネットワークにおいて情報がどのように受領、処理、操作、送信、アクセス、保管されるべきかを定める上でのガイドラインとなってきました。企業はデータがどのように扱われるべきかを定めた規制と内部ポリシーに従うために、かなりの投資をしてきました。しかしながら、ネットワーク監視ソリューションがデータを管理する方法へのこれらのポリシーの適用においてはしばしば見落としが発生します。

ネットワーク監視と分析のソリューションは、ネットワーク上にある企業の事業資産の健全性を示す上で必須の要素です。結果として、これらのツールはしばしば慎重に扱うべき情報へのアクセスを伴いますが、そのアクセスは内部ポリシーまたは規制のポリシーにより、定められた方法で管理されなければなりません。そうしたネットワーク監視ツール上の慎重に扱うべき情報の収集、処理、保管、アクセスは、完全に定めを順守するために、ネットワークキングの他の側面においてと同等に効率的にコントロールされなければなりません。

NIKSUN のネットワーク監視ソリューションは、データ管理について指示するポリシーの意義を考慮しています。NIKSUN アプライアンスは強化されたオペレーション・システムや、厳格なセキュリティ規則、アクセス制御を備え、同時にすべてのユーザ・アクティビティを監査する機能を持ち、安全でコンプライアンスに備えたソリューションであると証明されています。

## 序 論

サーベンス・オクスリー法 (2002 年)、グラム・リーチ・ブライリー法 (1999 年)、連邦情報セキュリティ管理法 (FISMA、2002 年)、データ保護法 (1998 年)、医療保険の相互運用性と説明責任に関する法律 (HIPAA、1996 年) は、データ管理に対する企業の注意について、法的な要求を強化してきました。これらの法による指示は、企業の説明責任、統合性、財産管理、リスク管理、およびデータの受領や送信、取扱い、保管の統一化について、包括的な枠組みを示してきました。これらのポリシーを順守できなければ、法律上、あるいは会計上の深刻な事態を招く可能性があります。

SOX や HIPAA のような規制ポリシーの厳格な要求を満たすため、企業は既存のネットワークインフラをその要求に適合させたり、新しいインフラを導入したりということに、大きな投資をしてきましたが、監査プロセスにおける失敗の可能性が潜んでいる基幹システムの正確な分類は、高い費用がかかる課題です。そのようなポリシーの管轄下にあるネットワーク・コンポーネントを分離するには、計画性の高い資産管理システムや棚卸資産開示システム、時間、またもっとも重要なこととして、ネットワークを法令に準拠した状態に保つための変更管理の論理的計画に対し、大幅な投資が必要です。

さらに、コンプライアンス管理対策を導入するためにサードパーティ・ベンダーのソリューションに依存すると、100 パーセントのコンプライアンスを目指す一連の対策へ新たな脆弱性のある関連性がもたらされます。コンプライアンス関連の法律がどのようにソリューションの使用に影響をおよぼすかをベンダーが認識し、コンプライアンス不履行のリスクを克服するためにパッチをタイムリーに、かつ頻繁に供給することは、極めて重要です。また、パッチや関連する文書を供給する頻度は、すでに重い負担が掛けられている IT や IT リソースに対し大きな運用上の影響を与え、それゆえに費用対効果の高いコンプライアンス管理という目標達成にはさらに負担が掛かります。



こうしたコンプライアンスを目指した小さな変化とコンプライアンス目標を達成するためのベンダーへの依存においては、ネットワーク・ベースのパフォーマンス・ツールおよびセキュリティ・ツール(すなわち、ネットワーク監視、パケットのキャプチャおよび分析用ツール、侵入検知システム (IDS)、侵入防御システム (IPS)、ネットワークの動作分析 (NBA) システム)はしばしば見落とされ、コンプライアンス基準へ向かうその産業の主要な動きから除外されてしまいます。これらのツールにあるようなポリシーを順守したデータ管理が欠如していることは、監査の際にのみ露呈します。それでは遅すぎ、あまりに犠牲の大きい手抜きと言えます。

## ITの利用・開発・維持への影響

SOX や HIPAA、その他の類似の法令が発効されると、情報技術の利用や開発、維持の方法に深く長期に渡る影響が生じます。コンプライアンス確保にかかる費用は、基盤システムに脆弱性が生じやすい場合に増加する可能性があります。

世界的に展開された 700 を越すネットワーク・アナライザがネットワーク上にあり、そのすべてが Windows OS とアンチウイルス・ソフトを稼働させていたケースを例にとってみましょう。最初の問題は単なるデバイスの設置でしたが、センターとなる管理システムがなかったことを考えれば決して些細な課題ではありませんでした。アナライザの設置を終えると今度は、最初のバッチリリースとの同時リリースが必然的にできなかった、クライアント PC が承認した OS のアップデートを入手する必要がありました。これにより、最初のバッチリリースで述べられている新たな脆弱性にさらされる時間が長引くという結果を招きました。さらに、アンチウイルス・ソフトを定期的にアップデートし、アナライザに感染がないか毎日スキャンし、トリガとなったアラームを調査する必要がありました。

資産管理や資産の棚卸しの手続きは時間を消費し、費用がかかり、変更の計画および検証、実装には多くの手作業の処理を要します。不安定な状態で現れる法令違反についての法律関連事項に対応するだけでなく、ネットワーク運用におけるコンプライアンスの実践を十分に強固なものとし、ネットワーク全体のセキュリティおよびパフォーマンス、制御を維持することもまた、緊急に対応すべき課題です。

---

<sup>1</sup> This was an actual case of a large financial institute on Wall Street.

## NIKSUNはコンプライアンスの基準に

NIKSUN は、ネットワーク・セキュリティ分析、コンプライアンス監視、パフォーマンス分析ソリューションにおけるトップのソリューション・プロバイダとして、コンプライアンス対策を目指して業界をシフトさせることに自らの役割があると認識しています。NIKSUN は、そのソリューションがお客様によるコンプライアンス上の監査プロセスにおける不成功の原因ではないことを保証するため、ソリューションがネットワーク・データを受信、処理、保存、リリースする方法を鋭く認識し、またいくつかのセキュリティ監査を問題なく経験した厳重な制御システムを実装しています。

その結果、すべての NIKSUN アプライアンスにはデータ・セキュリティおよびデータ制御のための一連の強固な機能が実装されています。データへのアクセスを検証し制御するための確実な機能を備えてお客様の力を高めることにより、NIKSUN 製品はコンプライアンス管理プロセスに対する制御を失う危険からお客様を守り、企業が費やす時間と費用を節約します。NIKSUN アプライアンスが様々なコンプライアンス上のポリシーの基準に備えていることは、極めて容易にお客様に確かめて頂けます。

NIKSUN が提供するコンプライアンス制御とアクセス・コントロールの機能は、下記のように分類できます。

- ◎ 実装制御：このソリューションは、内部ポリシーおよび該当法に基づいてネットワーク全体を流れる一部あるいは全部のデータを監視するために実装可能です。加えて、このソリューションによれば、アプライアンスの分散の状況に応じ、異なる事業分野や地理的に異なる場所においてもデータを監視できます。
- ◎ メンテナンス制御：大規模な分散された環境では、リモートアクセスとセキュリティ・ツールやネットワーク・ツールの管理の容易性は必須です。ロールベース・アクセス・コントロール (RBAC) やロールベース・セキュリティがアプライアンスへのアクセスのために実装されており、またこのソリューションでは機能の作成、修正、有効化、無効化が考慮されています。
- ◎ レポーティング：IT 管理者は、どのユーザがどの程度詳細な情報へのアクセス権を持つかを厳密に定義するアカウント・ポリシーを設定できます。あるレポートにはある人々がアクセス可能で、他のレポートには違うグループの人々がアクセス可能といった設定ができます。

次のセクションで、すべての NIKSUN アプライアンスに共通な独特のセキュリティ機能について概要を示します。



## 実装されているアクセス制御

### 認証とアクセスポリシーを管理

ユーザおよびグループのアカウント認証はローカルでの認証と外部サーバによる認証の異なる2つの形で実装されています。

ローカルでの認証には独特のユーザネームとパスワードが必要で、さらにパスワードには長さが指定され、特定の文字が使われている必要があります。アプライアンスの管理者とアカウント管理者だけがユーザを新規作成でき、またパスワードが事前に定義された期限の後に失効するよう設定できます。ユーザは自分のパスワードを変更することもできます。パスワード・エージングもまた実装されています。

外部サーバによる認証にはお客様が既にお持ちの Active Directory、TACACS、RADIUS、LDAP サーバを用い、ユーザは外部サーバ上で既に設定されている認証ポリシーに則り NIKSUN アプライアンスにログインできます。外部認証を用いることにより、多数のアプライアンスにおいてユーザおよびグループの認証とアクセスポリシーを管理することが容易になります。

多くのネットワーキング・ツールはそれが組み込まれているネットワーク全体を考慮しておらず、従来のプロトコルに対応する機能を備えた中央集約型のユーザ管理は可能ではありません。上述の 700 以上のアナライザが世界的に展開されているお客様の例では、アナライザへのアクセス権を持つ全ユーザが管理者権限を持っていました。前からあるネットワークの認証アーキテクチャに統合されることで、NIKSUN のソリューションは企業によって定義されたアクセス制御を一箇所で忠実に守ります。そのため、NIKSUN のソリューションはシングルサインオンのワークフローの一部となり、分析担当者やオペレータが安全とコンプライアンスを保った上で迅速に仕事をすることが可能になります。

ローカルでの認証および認可と外部認証および認可の両方を提供することにより、NIKSUN は可用性を確保した上での統合の利便性をもたらします。すなわち、ネットワークの機能停止やマルウェアによる攻撃で外部サーバへの接続が途切れたとしても、ユーザは NIKSUN アプライアンスにアクセスできるのです。

### グループ・ポリシーと認可の管理

ロールベース・アクセス・コントロール (RBAC) やロールベース・セキュリティはアプライアンスとソリューションの機能に実装されています。IT 管理者は、どのユーザがどの程度詳しい情報にアクセスできるかを厳密に定義するアカウント・ポリシーを設定できます。RBAC はポリシーの変動の影響を受けないので、お客様は制限が掛けられたデータの強固な管理を考慮に入れた上で、アクセスレベルをカスタマイズして定義できます。役割は、特定の職務権限のために新規に作成でき、それらの役割に特化した操作や機能を設定することができます。このことにより、ユーザは直接に許可を与えられるのではなく、自分に与えられた役割によって許可を引き継ぐため、ユーザの追加や削除のような共通の操作は大幅に簡略化されます。RBAC は例えば、分析担当者には NIKSUN Network Knowledge Warehouse に保存されたメタデータに基づいたレポート作成だけを許可し、一方で、スーパー・ユーザや管理者にはパケットの詳細へのアクセス権を持たせることができます。また、パフォーマンス関連のレポートをアプリケーション・チームやネットワーク・チームにのみ提示する一方で、インシデントやイベントのレポートに対するアクセス権はセキュリティ・チームに与えるようにできます。

## デバイスのセキュリティ管理

NIKSUN アプライアンスは、強化された UNIX の OS 上で設計および開発されています。不要なファイルやディレクトリの削除、使わないサービスの無効化、厳しいファイルへのアクセス制限がなされ、開いているポートの数は最小限に抑えられています。違うレベルのアクセス制御の追加は組み込まれたファイアウォールによってなされ、そのファイアウォールは定義された通信ポートや、特定の IP アドレスやサブネット・アドレスからのアクセスのみ許可するように設定できます。

NIKSUN アプライアンスの監視用インターフェースは、パッシブでプロミキヤスモードのため、トラフィック監視は透過的で、いかなるネットワーク・ユーザやスキャンング・ツールも認識することができません。

管理者には、内部のセキュリティ・ポリシーに基づいてアクセス権の設定を制御し構成するための柔軟性が与えられます。様々なアプリケーションのためのウェブベースのユーザ・インターフェースは、安全な HTTP(HTTPS)による使用のみに制限されています。telnet および FTP でのアクセスは、デフォルトで無効となっています。コマンドラインへのアクセスはセキュアシェルに限られ、希望があればアクセスを完全に無効化することができます。

## デバイス設定の管理

大規模な分散された環境では、リモートアクセスとセキュリティ・ツールやネットワーク・ツールの管理の容易性は必須です。NIKSUN は、Central Manger(CM) という名前の安全で中央集約型の管理ツールを NIKSUN アプライアンスの管理用に提供しています。加えて、CM はアプライアンスの状態を監視する機能を提供します。NIKSUN のソリューションは、IBM Tivoli や HP Overview などの企業管理ソリューションとも連動します。Central Manager は、安全なプロトコルを使い厳しい認証基準に従ってアプライアンスと通信しており、既存のアプライアンスの管理ポリシーや機能を増補するために用いることができます。ファイアウォール、SSH、HTTPS、DNS、管理用 IP アドレスのような設定はすべて、リモートで安全に設定することができます。CM はまた、リモートによる一箇所からのソフトウェアの更新、バッチ管理、IDS のシグネチャ更新、アプライアンスの可用性管理などの目的で使用することができます。

## 移送される規制されたデータの保護

規制の掛かっているデータが安全にネットワーク上で送られるよう保証することはベンダーにとって非常に重要です。NIKSUN のソリューションは、ネットワーク上のデータ伝送のための安全で強固な企業のフレームワークを提供します。加えて、データが人事部門や法務部門に送られる必要がある場合には、送られるデータのシグネチャのダイジェストを様々な形式で発行可能という便利さを持っており、データの完全性を保証することができます。

## 静止しているデータの保護

キャプチャされたデータは専用の場所に保存され、未公開のデータは複数のディスクにまたがる構造を作り、分割されます。もしひとつ以上の物理ドライブに障害が起きれば、NIKSUN アプライアンスと特定のファームウェアがなければ絶対にデータにアクセスできず、その特定のアプライアンス上にあるディスクのサブシステムの設定は有効なライセンスキーによるものでなければなりません。

## アクセス・コントロールの報告

NIKSUN のアプライアンスは、すべてのユーザ・アクティビティを追跡し、詳細な監査レポートを作成できます。ログイン中のユーザ、ログインの失敗や未遂、その他のアプライアンス上でなされるすべてのユーザ・アクティビティが記録されます。ユーザがアプライアンスにログインする前には、特定のチケット番号と目的の記述が必須となります。規制が掛かっているデータに誰が、いつアクセスし、その人物がデータを用いて何をしたのかを示す詳細なレポートを作成することができます。

ワンクリックで作成可能な監査レポートにより、監査担当者にはセキュリティ監査を完了するために必要なすべての情報を容易に見る方法が提供されます。監査レポートは、パスワードで保護することができ、特定の人々のみが適切なアクセス権をもって入手できるように設定することが可能です。レポートにはシステムの構成設定やセキュリティ・ポリシー、ユーザおよびグループへの許可、外部認証の設定についての情報が含まれています。

## 要 約

規制による要求は、情報セキュリティ対策を中心となって動かすものとして浮かび上がってきました。様々な規制に対するコンプライアンスの維持は IT 部門に莫大な負担を与えます。規制の掛かっているデータを保管するデバイスは安全性が保たれなければならない、そのデータへのアクセスは厳重に管理される必要があります。

NIKSUN が提供するネットワーク監視のソリューションは、強化された UNIX の OS 上で設計・開発され、安全かつ中央で管理されるソリューションとなっています。コンプライアンスは NIKSUN のソリューション(およびアプライアンス、事業)における基準となっており、規制が IT スタッフに与える負担を軽減します。規制が掛かっているデータは静止しているときも移送されるときも保護され、またロールベース・アクセス・コントロールが実装されています。

## **NIKSUN**

### **Corporate Headquarters**

100 Nassau Park Blvd  
Princeton NJ 08540  
t: +1.609.936.9999  
toll free: +1.888.504.3336  
f: +1.609.419.4260  
info@niksun.com

### **NJ - Monmouth Junction**

1100 Cornwall Road  
Monmouth Junction NJ 08852  
t: +1.732.821.5000  
f: +1.732.821.6000

### **Massachusetts**

14 Summer Street, Suite 402  
Malden MA 02148  
t: +1.781.333.3200  
f: +1.270.964.0394

### **California**

4633 Old Ironside Drive  
Santa Clara CA 95054  
t: +1.408.855.9900

### **Europe**

Second Floor, South Park House  
Kidwells Park Drive  
Maidenhead, Berkshire  
SL6 8AQ  
t: +44. (0)162.876.3010  
sales\_europe@niksun.com

### **India**

SCO-16, Sector-14  
Gurgaon  
Haryana 122 001, India  
t: +91.124.231.6013  
sales\_india@niksun.com

### **Japan**

〒103-0023 東京都中央区  
日本橋本町3-3-6 ワカ末ビル7階  
電話：03-6202-7454  
E-Mail: sales\_japan@niksun.com

### **Middle East**

sales\_middle\_east@niksun.com

### **APAC**

sales\_apac@niksun.com



**NIKSUN について** : NIKSUN は特許取得済みのマルチタイムスケールなネットワーク監視およびセキュリティ監視、またリアルタイムな分析ソリューションを提供する代表的なプロバイダーであり、我々のソリューションは、パフォーマンスやセキュリティ、コンプライアンスに関するアプリケーションやサービスへ影響を与えるインシデントについて、識別、アラート、分析、レポートの機能を提供します。NIKSUN の NetOmni Suite は今日利用可能な唯一のテクノロジーであり、大規模な組織の全体図をユーザの責任に準じて世界中に広まるハイスピードな集中型ネットワークへと統合することを可能にします。NIKSUN は組織の迅速で正確な意思決定を可能にし、それによって確実にネットワーク・パフォーマンス、セキュリティおよびコンプライアンス上の目標が達成され、データの整合性が守られます。

NIKSUN、NIKSUNのロゴ、NetDetector、NetVCR、NetVoiceは米国およびその他の国における NIKSUN、Inc. の商標または登録商標です。本文書に記載されている上記以外の製品名および社名は、各社の商標場合があります。NIKSUN、Inc. はこの情報の使用によって生じたいかなる種類の損害についても責任を負わないものとします。情報は予告なく変更されることがあり、また誤植、矛盾、脱漏等を含む可能性があります。

Copyright © 2010 NIKSUN, Inc. All rights reserved. NK-DS-CM01.10