ケーススタディ：SymantecとNapatechは企業の情報漏洩リスクの理解を支援します

Symantecについて

ガートナーのマジッククアドラントによると、Symantecは企業の情報漏洩防止 (DLP) における ソリューションリーダーです。DLPはデータ漏洩の件数が増加するにつれてセキュリティ上の大きな懸念として浮上しました。この問題を解決するには時間とコストが発生するだけでなく、ブランドイメージの低下につながります。情報漏洩箇所を特定するため、Symantec情報漏洩防止 (DLP) ネットワークモニタは、機密データが社内ITネットワークから送信される前に、ビジネスコミュニケーションを継続的に調査します。

課題：情報漏洩リスクの範囲を理解する

今日、企業は生成・収集されるデータの量が指数関数的に増加するにつれて、セキュリティの必要性を認識しています。競争力を維持するための知的財産 (IP) と顧客情報を保護する必要性は、IT企業の役員の間では最優先ではないにしても重大な優先事項となっています。電子メールプロバイダ、ソーシャルネットワーキング、製造業、医療、教育、政府、ソフトウェア、小売業など、あらゆる業界で2016年の1年間だけで発生したデータ漏洩の件数を考えてみても、もはや誰も安全ではないのです。

IT部門の管理対象外のデバイスやネットワーク、特にモバイルデバイスやクラウドを使用すると、企業の情報漏洩リスクは劇的に高まります。データの潜在的な領域数が増すだけでなく、監視対象のデータの量も劇的に増加します。情報漏洩を精査するために必要なすべてのデータを収集することがますます困難になっています。

ソリューション：Napatechアクセラレーションによるネットワークモニタ

Symantecのネットワークモニタを使用すれば企業はデータの紛失箇所を精査できます。このソリューションは、ネットワークを通過するデータを受動的に監視しつつ、日々の運用には影響を与えません。そして、セキュリティホールが特定されれば、顧客は将来そのような情報漏洩を抑止する方法を正確に定義することができます。

ネットワークモニタが情報漏洩の程度を正確に表示するために、Napatechアクセラレータは常に完全なデータパケットキャプチャを可能にします。Napatechを使用することで、ネットワークモニタはこれまでITネットワークの外部に送信されたすべてのデータを完全に認識します。

課題

IT部門の管理対象外のデバイスやネットワークを使用すると、情報漏洩のリスクは劇的に高まります。一方で、情報漏洩を精査するために必要なすべてのデータを収集することがますます困難になっています。

ソリューション

NapatechアクセラレータとSymantec DLPネットワークモニタを活用すれば、社内ITネットワーク外に送信される機密データをゼロパケットロスで検知できます。

利点

NapatechアクセラレータとSymantec DLPネットワークモニタを活用すれば、すべてのビジネスコミュニケーションを完全に把握できるため、機密情報を誤って処理し、企業を情報漏洩のリスクにさらす危険性の高いユーザを特定できます。

DN-1037 Rev. 1-JA

利点

Napatechアクセラレータは、社内ネットワークを往来するすべてのパケットを確実にキャプチャします。その後、Symantecネットワークモニタがキャプチャされたすべての関連データを検査することで、企業は情報漏洩リスクの全体図を描くことができます。送信されるデータの量と種類が増え続けると、リスクを完全に評価することが重要になります。

このソリューションのメリットはさまざまな業界に適用できます。

ケース 1：

電子医療記録 (EHR) の出現に伴い、患者の機密性を確保することは、米国の医療における最重要課題となっています。EHRは医療従事者が患者に総合的かつ合理化されたサービスを提供するのを支援しますが（医療施設が人の病歴に素早くアクセスできるようになる）、こうした記録に含まれる個人健康情報 (PHI) は医療保険の携行性と責任に関する法律 (HIPAA) で機密情報と定められています。

PHIへの不正アクセスが起こると、識別情報（生年月日、社会保障番号）が漏洩するだけでなく、法的に医者と患者の間でのみ共有できる診断情報も漏洩します。例えば、保険会社は、患者の填補を検証するために医療提供者に情報を要求することができます。その際、医療提供者は手続きを迅速化するために暗号化されていない患者のファイルを送信することがあります。ネットワークモニタを設置すると、この通信は自動的にリアルタイムで非適正のフラグが立てられ、提供者は即座に対応することができます。

ケース 2：

企業は競争力を維持するために知的財産 (IP) を保護する必要があるので、小売業界における情報漏洩のリスクが収益の損失につながることは想像に難くありません。世界中の顧客にサービスを提供する今日の大手小売業者は、数多くの現地の流通業者とIPを共有する必要があります。競合他社がその恩恵を受ける可能性のある情報漏洩（例えば、盗難）を最小限に抑えるために、通信は安全でなければなりません。

小売業では最新の価格を提供することが重要です。場合によっては、小売業者は、流通業者がアクセスするために中央の文書リポジトリを提供します。顧客との会議で新しい価格設定を知る必要があっても、現場でリポジトリにアクセスできない場合、流通業者は小売業者に情報を直接送信するよう要求するでしょう。

しかし、小売業者が電子メールやftpなどの手段で価格情報を流通業者に直接送信することはできません。Napatechは、ネットワークモニタがこれらの違反の事例をキャプチャできるようにすることで、知的財産 (IP) の盗難に対する脆弱性を排除します。

ケース 3：

大学も情報漏洩に配慮する必要があります。こうした高等教育機関は、政府機関と民間の両方が主催する研究を通じて知的財産 (IP) を生み出しています。しかし、大学は厳しい予算で処理する状況が続いていることが知られており、包括的なDLPソリューションを実装するための時間やリソースがない場合があります。

Napatechアクセラレータを使用すると、ネットワークモニタは比較的短時間で実際のDLPリスクを評価できます。効率的なパケットキャプチャにより、組織は情報漏洩リスクの範囲を完全に把握することができます。これにより、大学はDLPのアーキテクチャを実装するためのビジネスケースを作り、短期的および長期的に問題に取り組む現実的な計画を策定することができます。

Symantec 情報漏洩防止 (DLP) の詳細については、以下のウェブサイトを参照してください。
go.symantec.com/dlp

Napatechアクセラレータの詳細については、以下のウェブサイトを参照してください。
www.napatech.com/products/accelerators

さらにユーザ事例を見る：
www.napatech.com/resources/case-studies

ヨーロッパ・中東・アフリカ
Napatech A/S
デンマーク コペンハーゲン

Tel. +45 4596 1500
info@napatech.com
www.napatech.com

北米
Napatech Inc.
マサチューセッツ州 ボストン
カリフォルニア州ロスアルトス
ワシントンD.C.

Tel. +1 888 318 8288
info@napatech.com
www.napatech.com

アジア太平洋
Napatech China/South Asia
台湾 台北
Tel. +886 2 28164533 Ext. 319

ナパテックジャパン株式会社
日本 東京
Tel. +81 3 5326 3374
ntjapansales@napatech.com

Napatech Korea
韓国 ソウル
Tel. +82 2 6001 3545

ntapacsales@napatech.com
www.napatech.com