2011 年 6 月 13 日

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

【報道資料】

日本企業の 73%が 2010 年にデータ漏洩を経験

課題は、データ・セキュリティ、コンプライアンス、ユーザの意識向上

チェック・ポイントと Ponemon Institute のセキュリティ調査結果 第 2 報

ゲートウェイからエンドポイントまでの包括的セキュリティを提供するチェック・ポイント・ソフトウェア・テクノロジーズ株式会社（本社：東京都新宿区、代表：代表取締役社長　藤岡健）と大手調査会社Ponemon Instituteは本日、各国のITセキュリティ管理者を対象に実施された調査「Understanding Security Complexity in 21st Century IT Environments (21世紀のIT環境におけるセキュリティの複雑性に関する調査)」の結果を公表し、2010年にデータ漏洩問題を経験した日本企業は国内調査対象企業の73パーセントに上ることが調査レポートから明らかになったと発表しました。同レポートによれば、漏洩した情報内容は、「消費者の個人情報」（52パーセント）、「顧客情報」（50パーセント）、「社員情報」（34パーセント）、「知的財産」（28パーセント）、「事業計画」（22パーセント）の順となっており、多くの企業が複数のデータ漏洩問題を経験しています。また漏洩した情報の特定ができない日本企業は全体の38パーセントに達し、調査を実施した欧米4ヶ国との比較で最も高い数値を示しました。Web 2.0アプリケーションの普及やネットワーク接続されたモバイル・デバイスの増加に伴い、データ・セキュリティの強化やITにおけるGRC （ガバナンス、リスク管理、コンプライアンス）要件への対応が企業にとって大きな課題になっていることがうかがえます。

日本では、350人以上のITセキュリティ管理者を対象に実施されたこの調査によると、日本企業におけるデータ漏洩の原因は「デバイスの紛失や盗難」が最も多く、次いで「セキュリティが不十分なモバイル・デバイス」、「ネットワークへの攻撃」、「Web 2.0アプリケーションやファイル共有アプリケーション」、「電子メールの誤送信」という結果になっています。また回答者の32パーセントは、「社員はデータのセキュリティやコンプライアンス、ポリシーに対する意識が非常に低い、または全く意識していない」と答えています。多くの場合、ユーザがセキュリティ脅威に対する第一の「防護壁」になることを考えると、データ保護戦略にユーザ教育を盛り込むことはもはや不可欠と言えます。

チェック・ポイントのネットワーク・セキュリティ製品担当バイスプレジデントであるオーデッド・ゴンダ（Oded Gonda）は、「データのセキュリティとコンプライアンスが最高情報セキュリティ責任者 (CISO) にとっての最重要課題であることはすでによく知られています。しかし、データ漏洩の原因から明らかなように、大半の事例はユーザの不注意によって発生しており、データ漏洩を検知するだけでなく防止するためには、ユーザ教育のための施策をデータ漏洩対策に盛り込み、情報資産の可視化と管理性を高める適切な仕組みおよび手続きを確立する必要があります」と述べています。

Ponemon Instituteの会長兼創立者であるラリー・ポネモン（Larry Ponemon）博士は、「表面化するしないにかかわらず、毎年非常に多くのデータ漏洩事件が発生している今日では、ガバナンスやリスク管理、コンプライアンスに関する問題に注目が集まるのも当然です。しかし、現代におけるデータ・セキュリティとは、単にテクノロジーを次々に導入して、これらの課題を克服すれば済む問題ではありません。データ漏洩の原因は、社員の意識の低さにもあり、企業は、自社のセキュリティ・ポリシーについてしっかりとしたユーザ教育を実行することも求められています」と述べています。

DLP（データ損失防止）が情報セキュリティ上の最重要課題として浮上する中、企業には、データ漏洩を引き起こす主な原因を理解し、データ侵害を防止するためのベスト・プラクティスについて、以下のような実践を

取り上げています。

- **自社のデータ・セキュリティ要件を理解する**：自社が保有する機密データの種類を明確に把握、記録すると共に、法規制や業界基準に基づくコンプライアンスの対象となるデータの種類を理解する
- **機密データを分類する**：自社が保有のする機密データの種類をリストにまとめ、機密レベルを指定する。データを「公開」、「部外秘」、「極秘」などに分類するための文書テンプレートを作成し、データ・ポリシーや機密情報の成立要件をエンドユーザに周知する
- **ビジネス・ニーズに即したセキュリティ・ポリシーを策定する**：セキュリティ戦略は、エンドユーザの業務を妨げることなく情報資産を保護できることが求められるため、まず、個々の社員やグループ、部門のビジネス・ニーズに合わせて、分かりやすいビジネス用語でセキュリティ・ポリシーを定義する。また、アイデンティティ認識ソリューションを利用することで、ユーザや IT 環境をより明確に把握したうえで、適切にセキュリティ・ポリシーの実施が可能となる
- **ライフサイクル全体にわたってデータを保護する**：ユーザやデータ・タイプ、プロセスの相関分析結果に基づき、さまざまな形式の機密データをライフサイクル全体（保存中、転送中、使用中）にわたって保護できるデータ・セキュリティ・ソリューションの導入を検討する
- **コンプライアンス上の負担を軽減する**：法規制や業界基準に基づくコンプライアンス要件を評価し、自社のセキュリティやビジネス・フローに与える影響を分析する。ソリューションを導入する場合は、HIPAA や PCI DSS、SOX 法など特定の基準に合わせてベスト・プラクティス・ポリシーをカスタマイズできるシステムを選択することにより、短期間で稼働が開始でき、最低限保護が必要なデータ以外についても予防型の対策を実施する余裕が期待できる
- **ユーザをプロセスに関与させ、意識の向上を図る**：ユーザをセキュリティの意思決定プロセスに関与させる。専用のソリューションを利用すれば、セキュリティ・ポリシーについてユーザ教育を行い、ユーザ自身がリアルタイムでセキュリティ・インシデントに対処できる態勢が整備する。ソリューションによるデータの漏洩防止とユーザ教育を組み合わせて、ユーザに自己学習の機会を与えることにより、リスクの高い行動をユーザ自身が判断可能となる

「チェック・ポイントでは、データ漏洩の防止は技術ではなく戦略の問題であるという考えの下、データ侵害を未然に防ぐためのツールや保護機能の開発に取り組んでいます」とゴンダは最後に述べています。

本調査「Understanding Security Complexity in 21st Century IT Environments」は2011年2月にPonemon Instituteによって実施されました。米国、イギリス、フランス、ドイツ、日本から、2,400人を超える（日本は350人以上）ITセキュリティ管理者を対象とした独立した調査です。回答者は、金融や工業、防衛、小売、医療、教育など14の分野にわたる、大小さまざまな規模の組織に属しています。

欧米4カ国における同一調査結果を含む本調査のレポート全文（英語）は http://www.checkpoint.com/products/downloads/whitepapers/ponemon_white_paper.pdf をご参照ください。

また、2011年4月6日に発表した「Ponemon Instituteのセキュリティ調査結果」については、http://www.checkpoint.co.jp/pr/2011/20110406PonemonSurvey_Japan.html をご覧ください。

チェック・ポイントの Software Blade アーキテクチャ™に基づく DLP ソリューション、Check Point DLP

Software Bladeは、技術とプロセスを兼ね備え、情報漏洩の検知と未然の防止を同時に実現する革新的なDLP（Data Loss Prevention： データ損失防止）ソリューションです。画期的なデータ分類技術 MultiSpect™ により、ユーザ、コンテンツ、およびプロセスを総合的に分析してポリシー違反かどうかを正確に判断し、新技術 UserCheck™ により、ユーザ自身が問題をリアルタイムに是正できるようにします。ネットワーク・ベースの DLP ソリューションである DLP Software Blade は、データの取り扱いポリシーについてのユーザ教育を自動的に行って IT セキュリティ担当者が問題処理にかかる工数を削減し、不正な意図の有無にかかわらず企業の機密情報の漏洩を防ぎます。

Software Bladeアーキテクチャ™の詳細については、
http://www.checkpoint.co.jp/products/softwareblades/architecture/index.html をご覧ください。
Check Point DLP Software Bladeの詳細については、
http://www.checkpoint.co.jp/products/dlp/index.html をご覧ください。

Ponemon Institute について

Ponemon Institute© (http://www.ponemon.org/index.php) は企業や政府機関における信頼性に優れた情報およびプライバシー管理の慣習の促進に努めています。目標達成に向けて、同研究所は独立した調査を実施し、官民のセクターからのリーダーを教育して、さまざまな業界の組織のプライバシーとデータ保護の慣習を検証しています。

Check Point Software Technologies Ltd.について

チェック・ポイント・ソフトウェア・テクノロジーズ・リミテッド（www.checkpoint.com）は、インターネット・セキュリティにおけるトップ企業として、セキュリティの複雑さと総所有コスト（TCO）を低減しつつ、あらゆるタイプの脅威からお客様のネットワーク環境を確実に保護するための妥協のないセキュリティ機能を実現しています。チェック・ポイントは、FireWall-1 と特許技術のステートフル・インスペクションを開発した業界のパイオニアです。チェック・ポイントは、革新的セキュリティ技術である Software Blade アーキテクチャをベースとした一層の技術革新に努めています。Software Blade アーキテクチャは、導入先に合わせカスタマイズすることで、あらゆる組織のセキュリティ・ニーズにも的確に対応できる、柔軟でシンプルなソリューションの構築を可能にします。チェック・ポイントは、技術偏重から脱却してセキュリティをビジネス・プロセスの一環として定義する唯一のベンダーです。チェック・ポイント独自のビジョン 3D Security は、ポリシー、ユーザ、実施という 3 つの要素を統合して情報資産の保護を強化し、導入環境のニーズに合わせて高度なセキュリティを確保できるようにします。チェック・ポイントは、Fortune 100 社および Global 100 企業の全社を含む、何万ものあらゆる規模の企業や組織を顧客としています。数々の受賞歴のあるチェック・ポイントの ZoneAlarm ソリューションは、世界中で何百万にも及ぶお客様の PC をハッカー、スパイウェア、および情報窃盗から未然に保護しています。

チェック・ポイント・ソフトウェア・テクノロジーズの全額出資日本法人、チェック・ポイント・ソフトウェア・テクノロジーズ株式会社は、1997 年 10 月 1 日設立、東京都新宿区に拠点を置いています。

####

《本件に関するお問い合わせ先》

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
担当 マーケティング 溝口
Tel: 03-5367-2500 / Fax: 03-5367-2501
Email: info_jp@checkpoint.com

広報代行 株式会社プラップジャパン
担当 矢畑
Tel: 03-4570-3191/ Fax: 03-4570-3189