

サイバー空間における脅威ニュース【情報を盗み取る手口】

(ニュースの内容は、各種報道、インターネット等で公表されている情報に基づくものです。)

○ 米国大手ホテルのPOSシステム^{*1}から情報漏えい

IT mediaニュースは、平成27年11月24日、米国ホテルチェーン大手のStarwood Hotels & Resortsが、系列の一部ホテルのPOS端末がマルウェア^{*2}に感染し、利用客の決済カード情報が流出した可能性があることを発表したと報じた。

マルウェアが見つかったのはカナダや米国、ハワイにあるシェラトンやウェスティン等の系列ホテル。平成26年11月から平成27年3月頃にかけて、レストランやギフトショップ等のPOSシステムで相次いで感染した。宿泊予約システムへの感染は、現時点では見つかっていないという。

同マルウェアは、利用客が使ったクレジットカード等の決済カード番号や所有者の氏名、セキュリティコード、有効期限等の情報を盗む仕様になっていた。捜査当局や専門家と連携して各ホテルで対策を講じ、マルウェアの除去を済ませたと説明している。

同ホテルはカード情報が流出した可能性のある利用客に連絡を取り、不正使用監視等のサービスを提供するという。

また、米国ホテル大手のヒルトン・ワールドワイドも、平成27年11月24日、グループで運営するホテルのPOSシステムが不正アクセスを受け、クレジットカード等の顧客情報が流出したと発表した。

情報流出の件数については公表していないが、グループのホテルで平成26年11月から12月の間と、平成27年4月から7月の間にカードを利用した顧客が被害を受けた可能性があり、対象者にカードの使用履歴の確認を求めている。



顧客の信頼を損なわないために！

POSシステムを狙う脅威への対策として、次のような対策を行きましょう。

- 組織内通信であってもファイアウォール^{*3}で不要な通信を制限する。
- POSレジ本体のOS^{*4}にセキュリティ対策ソフトを導入する。
- すでに暗号化されたデータを暗号通信プロトコルSSL^{*5}で送信するなど、二重に暗号化を施す。
- ネットワーク内の不審な挙動や通常業務と異なる動きがないかを調べるなど、セキュリティ情報やイベント管理^{*6}を徹底する。

お困りの
ときは！

京都中小企業情報セキュリティ支援ネットワーク (Ksisnet)
IT 相談窓口 (公益財団法人京都産業21 お客様相談室)

相談内容：情報セキュリティ対策、情報漏えい・流出事案等
※毎週月曜日～金曜日の9:00～17:00 (祝日を除く)

TEL 075-315-8660 メールアドレス okyaku@ki21.jp

公益財団法人京都産業21 お客様相談室 (〒600-8813 京都市下京区中堂寺南町134 京都府産業支援センター内)



※1 POSシステム

POSとは、販売時点情報管理（Point of sale）の略称。物品販売の売り上げ実績を単品単位で集計すること。その機能を有するシステムをPOSシステムと呼び、別名、パソコンPOS、POSレジ、POSレジスタと呼ばれることもある。

POSの導入における最大の利点は、商品名や価格、数量、日時などの販売実績情報を収集するため、「いつ・どの商品が・どんな価格で・いくつ売れたか」を経営者側が把握しやすく、売れ行き動向を観察できる点にある。

POSシステムは、主に、スーパーマーケットやコンビニエンスストア、ドラッグストア（薬局）、アパレルショップ、各種専門店、外食産業、ガソリンスタンド、ホテルなどのチェーンストア等で導入され、年々その機能が進化しているが、近年はその簡易版が一般商店などにも普及している。

※2 マルウェア

ウイルスのみならず、不正にパソコンを操作するバックドアなどのスパイウェア、強制的に広告を表示するアドウェア、嘘の情報で購入を促す偽セキュリティ対策ソフトなど、コンピュータの利用者が意図しない動作をする不正なプログラムの総称

※3 ファイアウォール

ファイアウォールとは、あるコンピュータやネットワークと外部ネットワークの境界に設置され、内外の通信を中継・監視し、外部の攻撃から内部を保護するためのソフトウェアや機器、システムなどのこと。原義は「防火壁（firewall）」であり、外部のネットワークからの攻撃に対する防御を、火事の炎を遮断して延焼を防ぐことになぞらえている。

※4 OS（オペレーティングシステム/基本ソフト）

OSとは、Operating Systemのソフトウェアの種類の一つで、機器の基本的な管理や制御のための機能や、多くのソフトウェアが共通して利用する基本的な機能などを実装した、システム全体を管理するソフトウェア。

パソコン向けのOSとして広く利用されているものには、Microsoft社のWindowsシリーズやApple社のMac OS Xなどがあり、企業などが使うサーバ向けのOSとしてはLinuxなどUNIX系OSや、Microsoft社のWindows Serverシリーズなどがよく使われる。スマートフォンやタブレットなどではGoogle社のAndroid OSやApple社のiOSが用いられることが多い。

※5 暗号通信プロトコルSSL

SSL（Secure Socket Layer）は、インターネット上でやりとりされるデータを暗号化して送受信するプロトコル（通信手順）の一つ。データを送受信する一対の機器間で通信を暗号化し、中継装置などネットワーク上の他の機器によるなりすましやデータの盗み見、改ざんなどを防ぐことができる。

※6 イベント管理

ここでいうイベントとは、モニタリングに使用する監視ツールなどから通知されるITサービスに影響ある事象、システムの状況変化に関する通知のこと。ITインフラストラクチャ（情報システムを稼働させる基盤となる施設や設備、機材、配線などの組み合わせのこと）全体で発生するすべてのイベントをモニタリングし、管理することによって通常どおりに運用されていることを監視することができ障害などの例外状況を検出した場合には、他の管理プロセスへ引き継ぎを行う。