

社外で活用するノートPCの情報漏洩防止と 資産管理の効率化を支援する 「Dell System Track」

ノートPCの紛失・盗難は、情報漏洩をはじめ企業における重大なセキュリティリスクとなっている。
この課題に対応するため、デルは紛失・盗難にあったノートPCの所在を特定し、企業データを保護する
パブリック・クラウドのサービス「Dell System Track」(※2011年8月よりサービス名称等変更)を提供している。
同サービスは資産管理ソリューションとしても活用可能であり、
企業におけるモバイル環境の拡大をシンプルな形でサポートするものだ。

デル株式会社
公共・法人マーケティング本部サービス & ソリューションマーケティング
シニア マネージャー
土肥明彦

パブリック・クラウドによる オンデマンドなIT管理サービスを提供

デルは、クラウド・コンピューティングに様々な形で取り組んできた。例えば、パブリック・クラウドのサービスプロバイダに対してはクラウド特化型インフラを、プライベート・クラウドを導入するユーザ企業に対しては仮想化ソリューションを提供している。

そして現在、あらゆる規模の企業に対してオンデマンドでIT管理サービスを提供するパブリック・クラウドのビジネスにデル自身が踏み出した。従来のオンサイト・ソリューションでのオペレーションの煩雑さを解消し、シンプルで効果的なIT管理の実現を目的とする「デルITマネジメントSaaS」である。クライアント統合管理やエンタープライズ統合管理をはじめ、インパクトの大きいIT課題に対応するサービス・メニューを用意しており、すでにワールドワイドでは1万5,000社以上の企業、数百万人のユーザがデルITマネジメントSaaSのサービスを利用している。

同サービスの多岐にわたるメニューの中で、今回フォーカスするのが「Dell System Track」だ。現在、ある調査会社の報告によれば、米国の空港における年間のノートPCの紛失・盗難数は62万4,000台に達しており、そのうち回収された割合はわずか3%にすぎないという。こうした頻発するノートPCの紛失・盗難が、情報漏洩など企業にとっての重大なリスクをもたらしていることは言うまでもない。Dell System Trackは、紛失・盗難

にあったノートPCの所在を特定し、そのノートPC上にある企業データを保護するもの。さらに、各地域の警察と協力し、盗難にあったノートPCの回収に努めるというサービスを提供し、セキュリティリスクの低減をサポートする。

紛失・盗難にあったノートPCを リアルタイムで追跡してデータを保護

具体的にDell System Trackでは、下記のような機能を組み合わせることで、紛失・盗難にあったノートPCの追跡、そしてデータ保護を行う(図1)。

•System Identification/Connectivity

データ保護対策を実行するために紛失・盗難にあったノートPCに接続し、レポートの生成に利用するハードウェアとソフトウェアの基本情報を収集する。

•Geotechnology

GPSベースのトラッキングとWi-Fi三角測量により、カスタマーポータル地図上でノートPCの所在を可視化し、リアルタイムで追跡する。

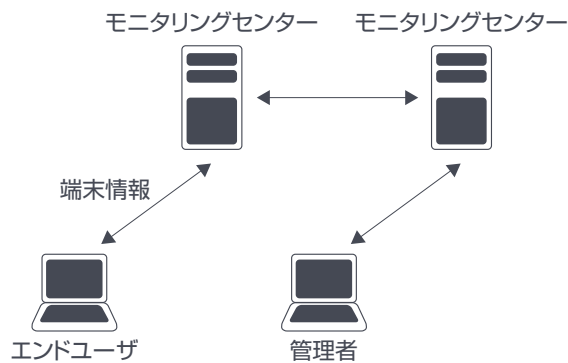
•Data Security

追跡対象の端末がインターネットもしくは無線ブロードバンドに接続された時点で、端末から機密データを削除する。また、重要ファイルの緊急抽出を実施することも可能。

図1 Dell System Trackの機能とメリット

System Trackの機能	メリット
検索対象システムのリアルタイム追跡 (Geotechnology機能の選択が必要)	・別の場所に持ち運ばれ紛失した端末の位置を特定 ・予め設定したエリアから離れた際にアラート ・リースまたはレンタルされた端末も確実に回収
SystemTrackエージェントにより、あらゆるシステムから遠隔操作で一元的にデータを削除	・重要データを不正アクセスから保護 ・重要データを削除した状態でリースまたは配置換えされた端末を回収
リモート緊急ファイル抽出	・端末を紛失しても、重要なデータは確実に保護
SystemTrackエージェントをBIOSに搭載 ※BIOSが対応していることが条件	・BIOSはセキュリティが保たれており、フォーマットやハードドライブ更新を行っても設定を保持
毎日一度は監視センターへ接続	・資産情報の変更の監視が容易に可能 ・違反事項に関わる問題を迅速に識別
盗難時リカバリ対応チーム	・貴重なハードウェアの回収確率に大きく貢献

図2 Dell System Trackによる資産管理

**構成情報を毎日自動送信**

エンドユーザのPCから毎日構成情報を自動送信

レポート機能

- ・ハードウェア構成情報
- ・ソフトウェア構成情報
- ・周辺機器情報
- ・ハードディスク容量情報
- ・変更情報
- ・OSの更新情報
- ・無許可のソフトウェア情報
- ・ウィルス駆除情報
- ・モデムの追加情報
- など

リース期限管理

・リース期間を管理し、リース切れを防止

・Device Security

遠隔操作によりシステムをOSレベルで強制終了する。

・Theft Recovery

各地域の警察と協力することで、盗難の被害に遭ったノートPCを回収。（追加料金対象。また、地域事情により対応不可の場合もあり）

これらの機能を実行するソフトウェア・モジュール（System Trackエージェント）は、ノートPCのBIOSとOS上にあらかじめインストールされた状態で納品されるため、簡単にセットアップし、運用を開始することが可能だ。いったん起動した後は、System TrackエージェントがデルのSystem Track監視センターと毎日コンタクトを行い、IT管理者は各ノートPCの管理・保護を行うための一連の操作をリモートで実施できるようになる。その際にIT管理者が社内ネットワークにアクセスする必要はない。

また、盗難にあったノートPCが犯人によってOSの再インストールやSystem Trackエージェントの削除が行われた場合でも問題はない。先に述べたようにSystem TrackはBIOS上にもインストールされているため、自動的にOS上にふたたび展開し、ノートPCの保護を継続するのである。

煩雑だった資産管理の作業を リモートから実行することで効率化

現在、多くの企業では、災害や計画停電時の対応を念頭に置いた在宅勤務体制の導入を進めている。一方、昨今のビジネス環境の変化の中で、従来のようなオフィスに依存しない、より柔軟かつ機動的な業務体制を確立することも求められている。組

織運営のコスト削減、社員一人ひとりの生産性向上、ワーク・ライフ・バランスの最適化といったトータルな視点から、多様なモバイル環境の整備が求められている。

こうした時代の流れの中で、モバイル環境に不慣れなエンドユーザが社外でノートPCを使い始めるケースは、今後ますます増えていくと予想される。その意味でもDell System Trackは非常に重要な役割を担うことになる。

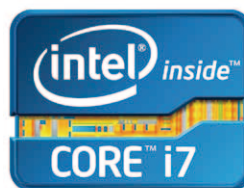
さらにDell System Trackで特筆すべきは、ノートPCが紛失・盗難にあった際のセキュリティリスクの低減のみならず、これまで高まる一方だったIT/総務部門における資産管理作業の負荷軽減にも大きく貢献するという点である。各エンドユーザに配布したノートPCから日々自動的に送信されてくるハードウェア構成情報、ソフトウェア構成情報、位置情報などをもとに、嚴重な資産管理をリモートから一括して行うことが可能となるのである。

例えば、ノートPCのHDD容量に空きがなくなった場合、システムに何らかの変更が行われた場合、許可されていないソフトウェアがインストールされた場合、ウィルスの定義ファイルを一定期間更新していない場合、指定された場所を離れてノートPCが持ち出された場合など、いずれかのノートPCがポリシーに違反した際にアラートを発して即座に対処することができる。

もちろん、管理したい資産情報を個別に設定することも可能だ。例えば、リース/レンタル期限を設定しておけば、返却期限が近づいたノートPCを一覧表示するといったことも簡単に行える。さらにデルでは、電源OFF状態のノートPCに対してもリモートからロックをかけられる新機能の提供や、Android OSへの対応といったDell System Trackのエンハンスも計画している。日本企業の課題にマッチした、より有益なパブリック・クラウドのソリューションとしてサービスの拡充を図っていく考えだ。

インテル® アンチセフト・テクノロジー^{*1}で さらにセキュリティを強化

トップレベルの第2世代インテル® Core™ i7 vPro™ プロセッサをはじめとするインテル® Core™ プロセッサファミリー搭載のデルのノートPCでは、紛失や盗難といった情報漏洩のリスクを最小化するための、インテル® アンチセフト・テクノロジーを利用することが可能だ。このハードウェアによるスマートなセキュリティ機能は、盗難の可能性を検知し、自動的にノートブックPCを無効化することができ、重要なデータを確実に保護する。ノートブックPCが正式なユーザーの手元に戻ったら、シンプルで迅速な低コストの方法によって、PCやデータに損害を与えることなく、フル機能状態に復帰させることを可能としている。



*1: すべての条件下で絶対的なセキュリティを提供できるシステムはありません。インテル® アンチセフト・テクノロジーを利用するには、同テクノロジーに対応したチップセット、BIOS、ファームウェア、ソフトウェアを搭載したシステムと、同テクノロジーに対応したサービス・プロバイダーのサービスへの加入が必要です。対応状況と機能については、各システムメーカーとサービス・プロバイダーにお問い合わせください。データやシステムの紛失や盗難など、サービス利用の結果生じたいかなる損害に対してもインテルは責任を負いません。詳細については、<http://www.intel.com/go/anti-theft/>（英語）を参照してください。