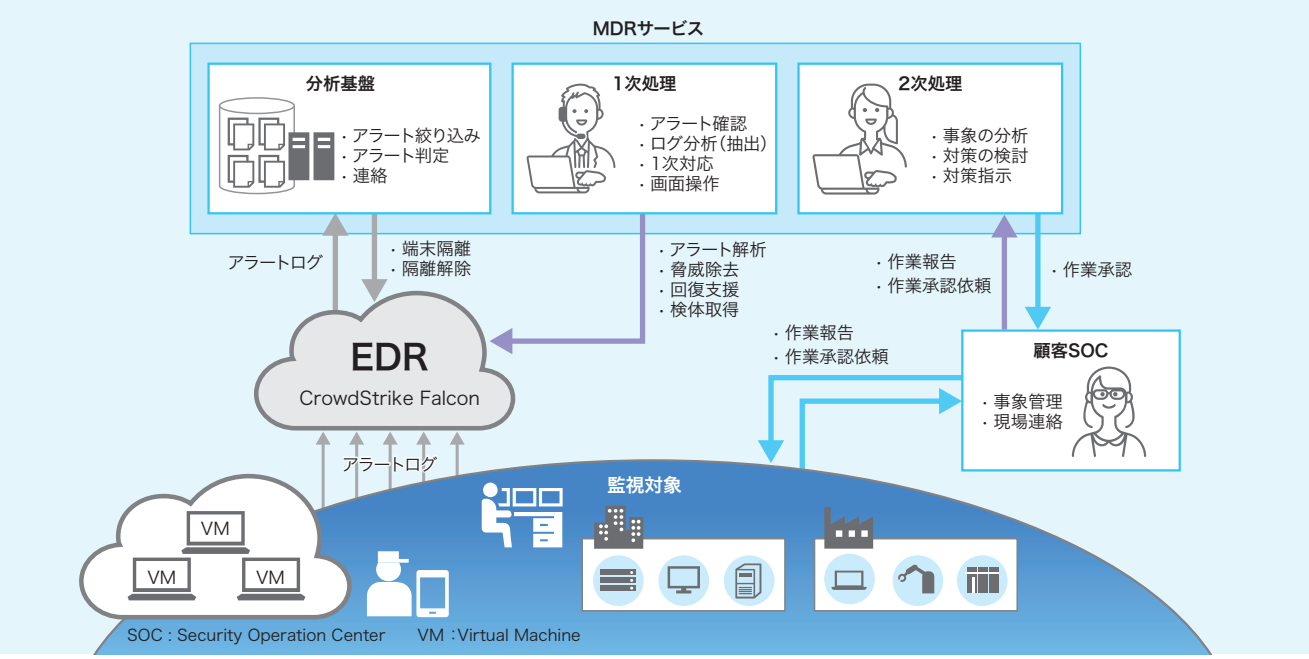
EDR製品とセキュリティー運用サービスの提供開始



CrowdStrike FalconとMDRサービスfor CrowdStrikeの概念図
Concept of CrowdStrike Falcon and managed detection and response (MDR) security operation service

近年，サイバー攻撃の高度化・巧妙化が進んでおり，ウイルス対策ソフトウェアを導入するだけでは，パソコンを代表としたエンドポイントへのマルウェアやランサムウェアなどの感染を防ぐことが困難な状況である。一方，近年のワークスタイルの変化により，在宅勤務や外出先のモバイル環境など，様々な環境で業務が行われるようになった。また，従来の安全な社内ネットワークではなく，ファイアウォールや侵入検知システムによる境界防御型ネットワークを前提としないゼロトラストネットワークの概念が広まりつつある。

このような中，業務で扱う情報の漏洩（ろうえい）防止やマルウェア感染などによる業務停止の回避には，エンドポイントへのセキュリティー対策がますます重要である。エンドポイントへのサイバー攻撃・不正侵入を検知するためには，パソコンなどの端末の振る舞いを常時監視し，不審な動きがあれば直ちに通報・隔離できるEDR（Endpoint Detection & Response）が有効である。

当社は，EDR製品であるCrowdStrike Falcon(注)の取り扱い，及び顧客環境での利用を支援するセキュリティー運用サービス“MDR（Managed Detection and Response）サービス for CrowdStrike”の提供を開始した。これは，CrowdStrike Falconが検知する日々の大量のアラートから過検知や誤検知を排除して処置が必要なアラートを抽出する技術，及び抽出されたアラートを最新の攻撃手法や動向を踏まえて適切に処理する技術に基づくサービスである。東芝グループや官公庁などでの豊富な実績やノウハウを持つ運用員が対応する。

顧客は，CrowdStrike Falconと，これに対応したMDRサービスを合わせて利用することで，高度な専門知識と情報を得て，効率的に運用可能になる。

（注）CrowdStrike, Inc.の製品・サービス。当社はCrowdStrike, Inc.の認定リセラーパートナー。

東芝デジタルソリューションズ（株）