News Release

2016 年 1 月 13 日
SCSK株式会社

標的型攻撃監視・防御サービスを提供開始
～次世代サンドボックスを活用し、情報漏えいをリアルタイムに防御～

SCSK株式会社（本社：東京都江東区、代表取締役社長：大澤　善雄、以下SCSK）は、標的型攻撃を検知する「標的型攻撃監視サービス」、および標的型攻撃に起因する情報漏えい被害を防ぐ「標的型攻撃防御サービス」の提供を本日から開始します。SCSKがシステム開発や運用で培ったノウハウとセキュリティー分野での専門性を活用し、各企業に特有の経営リスクや機密情報に合った、お客様ごとのセキュリティー対策を提供します。

1. 背景

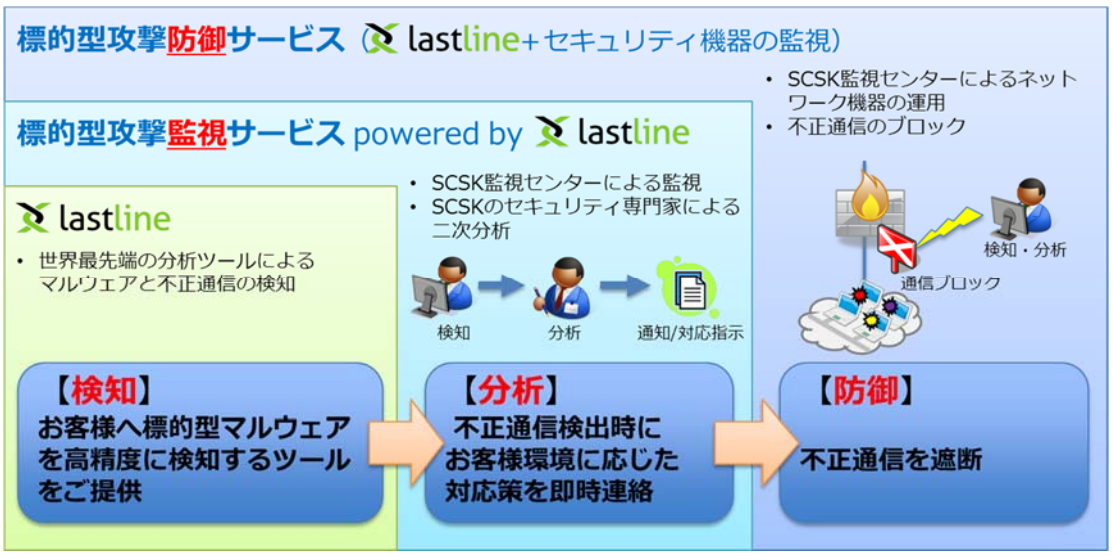
昨今、セキュリティー事故が企業や組織の存続に与える影響は大きくなっています。最近の高度なサイバー攻撃は、アンチウイルスやファイアウォールといった、攻撃を防ぐことを目的にした従来型の対策では攻撃者に回避され、検知することが難しい状況です。また、情報漏えいによる被害を未然に防ぐためには、このような高度な攻撃を検知した上で、リアルタイムに迅速な対応が必要になります。

2. サービスの概要

お客様環境に最先端のサンドボックスシステム※「Lastline（ラストライン）」を導入することで、既知の攻撃を防ぐだけではなく、未知の脅威も高精度に検出します。その検出状況をSCSK監視センターによって 24 時間監視し、お客様の環境に合った二次分析を行います。情報漏えいなどの事象を防ぐための対応が必要な際には、対応策を即時にお客様へ連絡します。

また、SCSK監視センターによる、ファイアウォールや不正侵入検知・防御装置のセキュリティー対策機器の監視サービスと併用することで、即座に不正通信を遮断し、標的型攻撃に起因する情報漏えいを高精度かつ迅速に防御することも可能です。

※サンドボックスシステム　…　プログラムを隔離された領域の中だけで動作させ、その他のシステムに影響を与えない環境で分析する仕組み



3. 価格

1,000 ユーザーでご契約の場合、年間 15,000 円（税別）/1 ユーザー
※価格はユーザー数によって変動します

4. 提供目標

サービス提供開始後 1 年間で、10 社へのサービス提供を目指します。

「Lastline」について

「Lastline」は従来型のセキュリティー対策では防御できない高度な攻撃を検知し、外部との不正な通信をブロックします。標的型攻撃に使われる高度なマルウェアを最先端の手法と独自のナレッジによって分析し、その挙動を高精度に把握することができます。導入形態はクラウド型、オンプレミス型から選択でき、企業のシステム環境やセキュリティー要件に応じた構成が可能です。

詳細はこちらの URL をご覧ください。 http://www.scsk.jp/sp/sys/products/lastline/

SCSKセキュリティー監視センター「SCSK SOC」について

ICT 環境のセキュリティーレベルを維持するためには、セキュリティー製品やソリューションを導入するだけではなく、安全な状態が保たれているかどうかを監視し続け、万一インシデントが発生した場合には迅速な対処が必要です。「SCSK SOC」は 24 時間 365 日、お客様ネットワークの状況を監視し、外部からの攻撃と内部からの情報漏えいを検知することで被害を未然に防ぐ、被害を最小限に留めるために必要な機能をご提供します。

詳細はこちらの URL をご覧ください。 http://www.scsk.jp/sp/sys/service/soc-csirt/

SOC: Security Operation Center

本件に関するお問い合わせ先

【製品・サービスに関するお問い合わせ先】
SCSK株式会社
netX データセンター事業本部　セキュリティサービス部　松村
TEL：03-5166-2815
E-mail： lastline-staff@ml.scsk.jp

【報道関係お問い合わせ先】
SCSK株式会社
広報部　　栗岡
TEL：03-5166-1150