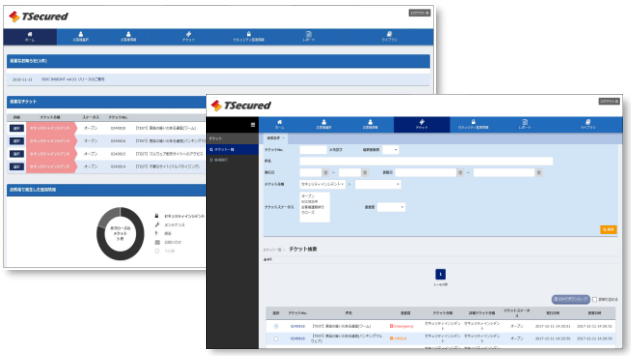
提供サービス内容

標準サービス	
ログの収集と分析	●お客様環境にあるサービス対象機器から、オールトヨタイントラネット（ATI）内にあるセキュリティ分析システムに収集されたログを、セキュリティアナリストが分析 ●収集されたログの保管期間と過去ログ検索期間は3ヵ月 ※ログの転送には、ログ収集サーバまたはサービス対象機器にログ転送プログラムの導入が必要 ※「セキュリティ共通基盤」などトヨタシステムズが提供する一部のサービスをご利用の場合は、お客様側での導入作業は不要
インシデントの判定と通知	●24時間365日のセキュリティ監視を行い、インシデント発生時はセキュリティアナリストが以下の5段階に分類 ［Emergency（緊急）］［Critical（重要）］［Warning（警告）］［Informational（情報）］［False Positive（誤検知）］ ●重要セキュリティインシデント（Emergency、Critical）は、判定から15分以内を目標に、電話およびメールでお客様担当者へ連絡 ※通知メールにはWebポータルへのリンクを記載 ●重要度の低いセキュリティインシデント（Warning、Information）は、Webポータルへの情報登録のみ実施 ●インシデントの詳細情報はWebポータルより確認可能
セキュリティ情報の提供	●独自入手情報および公開情報から収集した最新の脅威情報を、セキュリティアナリストが独自に精査。更新への追従を行い、セキュリティ分析ルールを随時更新 ●月次レポートをお客様に提出
オプションサービス	
データ送付	収集されたログ1ヵ月分をまとめてメディアに保存し、送付

Webポータル

- インシデントの詳細情報の確認や問い合わせ対応が可能
- Webポータルのログイン認証に必要となるソフトウェアトークンアカウントは、ユーザごとにご用意します。



参照できる情報	
お客様情報	お客様の連絡先情報、監視対象ネットワーク情報を参照することが可能
チケット情報	サービスイン後、すべてのチケットを参照することが可能
セキュリティ監視情報	過去2年間（731日）に発生したインシデントおよびイベントを参照することが可能
インシデント情報	次の各項目の詳細を確認することが可能 ・重要度　・検知内容　・想定される攻撃の内容　・不審な通信先情報　・推奨する対策　・参考情報
レポート	月次レポート、JSOC INSIGHTを参照することが可能 （サービスイン後、すべてのレポートを参照可能）
ライブラリ	Webポータル説明書などを参照することが可能

月次レポート（サンプル）

- インシデント発生状況／統計情報
- SOC Advanced内他社との比較情報
- チケット発行状況
- 世間でのセキュリティ動向トピック

記載されている会社名、製品名およびサービス名称は各会社の商標または登録商標です。
記載内容は2022年８月現在のものです。記載された仕様は予告なく変更する場合があります。

TOYOTA SYSTEMS

株式会社トヨタシステムズ
TEL：050-3142-7889　　Mail：helpdesk01@tns.toyotasystems.com
URL：https://www.toyotasystems.com