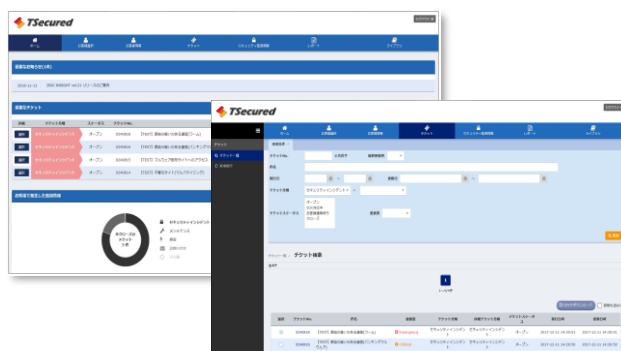


## 提供サービス内容

標準サービス	
ログの収集と分析	<ul style="list-style-type: none"> <li>●お客様環境にあるサービス対象機器から、オールドヨタイムトラネット（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</li> <li>●収集されたログの保管期間と過去ログ検索期間は3か月</li> <li>※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</li> <li>※「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</li> </ul>
インシデントの判定と通知	<ul style="list-style-type: none"> <li>●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）]</li> <li>●重要セキュリティインシデント（Emergency, Warning, 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</li> <li>※通知メールにはWebポータルへのリンクを記載</li> <li>●重要度の低いセキュリティインシデント（Warning, Informational）は、Webポータルへの情報登録のみ実施</li> <li>●インシデントの詳細情報はWebポータルより確認可能</li> </ul>
セキュリティ情報の提供	<ul style="list-style-type: none"> <li>●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</li> <li>●月次レポートをお客様に提出</li> </ul>
オプションサービス	
ログ拡張	ログ保管期間と過去ログ検索期間を12か月に延長
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
RSA SecurID追加・再発行	Webポータルのログイン認証に使用するRSA SecurIDを追加発行
オンサイト報告会	セキュリティアナリストがお客様訪問し、セキュリティ監視状況をご報告

### 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なRSA SecurIDトークンを1個提供

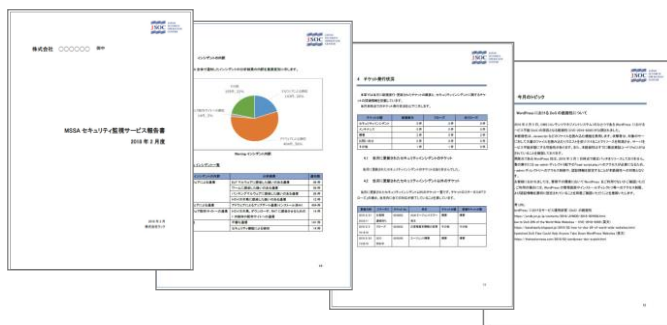


### 参照できる情報

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2020年11月現在のものです。記載された仕様は予告なく変更場合があります。



株式会社トヨタシステムズ

TEL : 050-3142-7889 Mail : [helpdesk01@tns.toyotasystems.com](mailto:helpdesk01@tns.toyotasystems.com)

URL : <https://www.toyotasystems.com>



2022年第1版