

標準サービス

ログの収集と分析

- 分析対象機器より出力される、監視対象端末が外部（インターネット/イントラネット）と通信を行った際の通信記録をセキュリティ分析システムに集約し、複雑・巧妙化する高度なサイバー攻撃の動向、不正IPの履歴などさまざまな要因をもとに相関分析を行います。
- 分析対象機器から、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します。
- 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
- ※分析対象機器がトヨタシステムズ提供サービスの場合、お客様側での導入作業は不要です。
- ※分析対象機器がお客様宅内の場合、ログ転送はお客様にてログ収集サーバまたはサービス対象機器へログ転送プログラムの導入が必要です。

インシデントの判定と通知

- 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段階に分類します。  
[Emergency（緊急）] [Critical（重要）] [Warning（警告）] [Informational（情報）] [False Positive（誤検知）]
- セキュリティ監視・予防遮断は、24時間365日（JST）でご提供いたします。
- 重要セキュリティインシデント（Emergency、Critical）の通知・緊急遮断・問い合わせ対応は、8時～17時365日（JST）電話およびメールでご提供します。
- 重要度の低いセキュリティインシデント（Warning、Information）は、レポートにてお知らせします。

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

Webポータル

- お客様の対策レベルアップに役立つ最新セキュリティ情報を発信
- 対策結果の共有機能で改善状況を見える化



月次レポート（サンプル）

- 世間やトヨタ関連会社の事故事例から「学び」を横展
- 自社の安全度や攻撃等の発生傾向をわかりやすく表示
- 実施するべき対策を簡潔明瞭に提示



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2023年4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。



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>



2019年第1版