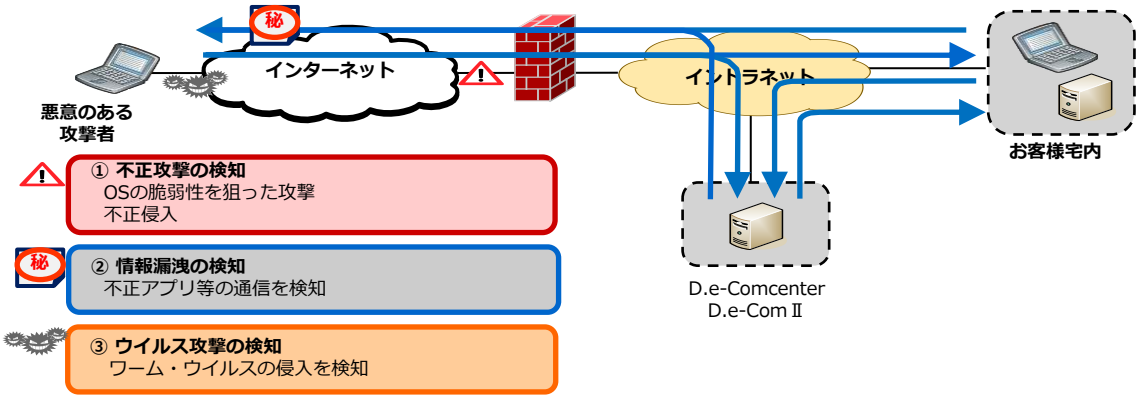
検知可能な脅威と対処



サービス内容

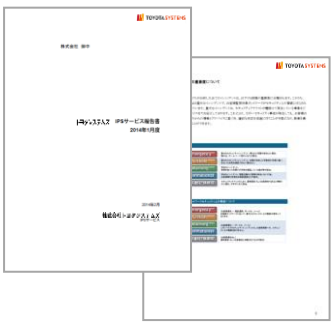
脅威の自動遮断	脅威（不正アプリ、ウィルス・ワーム、不正攻撃）をIPS機器にて検知・自動遮断を実施。
アナリスト解析/検知連絡	IPS機器から取得したログをアナリストにて解析実施。自動遮断では発見できなかった脅威に対して、 お客様窓口へ連絡(電話・E-mail)をし、遮断の実施要否を確認。
暫定処置の実施	お客様からの依頼に基づき、遮断を実施

Webポータル

- インシデント情報の確認、検知ログのダウンロード
- レポートのダウンロード
- インシデント検知時の連絡先変更

月次レポート（サンプル）

- セキュリティイベントの発生件数
- 重要なセキュリティイベントの内容説明
- チケット発行状況
- 「インターネットからの攻撃」のトレンド



検知可能な脅威一覧

①不正攻撃の検知 OSの脆弱性を狙った 攻撃・不正侵入	インターネットから不正ツール等を利用した攻撃を検知します。 検知可能な攻撃手法は以下のとおりです。 ・バッファオーバーフロー系攻撃（Dos攻撃など） ・設備の不備を悪用する攻撃 ・Webアプリケーションの不備を悪用する攻撃（アプリケーション固有のものは検知不可） ・調査活動（ポートスキャンなど）
②情報漏洩の検知 不正アプリ等の通信を 検知』	P2Pソフトウェアによる通信を検知します。 検知可能なソフトウェアは以下の代表的なソフトウェアの他に、 数十種類ものソフトウェアによる通信を検知します。 ・Winny　・WinMX　・Share　・BitTorrent　・eDonkey ・Gnutella　・LimeWire　・Shareaza　・SoftEther（※） 他、数十種類 ※SoftEther はプログラム規定ポート（TCP443：HTTP）使用時のみ検知可能です
③ウイルス攻撃の検知 ワーム・ウイルスの 侵入を検知』	お客様ネットワークからインターネットへワーム・ウィルスの感染活動を検知します。

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

2022年第1版