調査・監視／ログ保管サービス

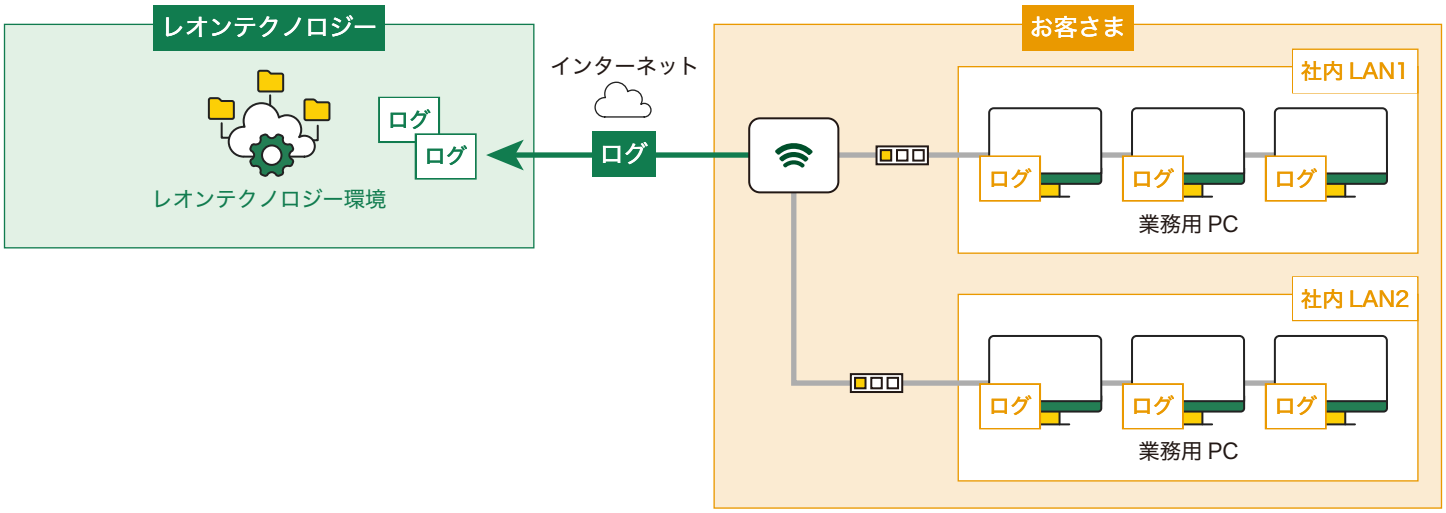
LeonLogCollect(L2C)

株式会社レオンテクノロジー

デジタル社会に「安心」「安全」「安定」を

LeonLogCollect(L2C)について

Windowsイベントログを集約し保管します。Windowsイベントログを保管することで、セキュリティインシデント発生時のフォレンジック調査に活用できます。
弊社製エージェントを導入することで、ログの収集と外部保管が自動化されます。これにより、お客様は手動でログファイルを収集し、保存する手間を省きます。エージェントは定期的に最新のログを取得し、外部の安全なストレージに転送します。



集約可能なログ種類の例

- ☑ Windowsイベントログ
- ☑ コマンド実行履歴
- ☑ Powershell実行履歴
- ☑ RDP接続履歴
- ☑ ログオン履歴

LeonLogCollect(L2C)の特長

1

ログ保管・集約用インスタンスをクラウド上に構築

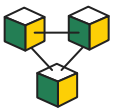
ログ活用基盤をクラウド上で構築する専門知識と経験を提供しています。AWS(Amazon Web Services)を活用し、堅牢でスケーラブルなログ活用基盤を構築いたします。

2

ログ収集用エージェントを提供

弊社が提供するログ収集用エージェントをログ収集対象の端末に導入いただき、対象から取得可能なログを全量、インターネットを介してログ保管・集約用インスタンスに保管いたします。

3



フォレンジック調査を可能にするログの長期保管

弊社の L2Cは、インシデント発生時に貴重な支援を提供します。弊社では、保管したログデータを活用し、フォレンジック調査を迅速かつ効果的に実施できるようお手伝いいたします。

4

サイバー攻撃によるログ操作の防止

インシデント発生時に調査対象となるログを改ざん、削除されないよう保全。万が一、端末内のログを改ざんされてしまった場合でも保全されたログを用いてフォレンジック調査が実施可能です。

ポイント

ログ調査の運用効率化し、社内でイベントログを保管する手間を省略

セキュリティに関わるトラブルが発生した際に、当社サービスにログが集約されているため、有事の際のログ調査にてオペレーションを簡易化できます。端末内で発生したログを弊社管理のサーバーで保管するため、自社内でイベントログを別途、保管・管理する手間を省けます。

弊社が提供する LeonLogCollect(L2C)の強み

こんな課題ありませんか

リスク

- ⚠ ログの不足による詳細な調査が行えない
- ⚠ ログが不足していることで、攻撃経路や被害の特定が困難になる場合があります。

迅速な調査がカギ！ →

レオンテクノロジーなら！

原因特定が早い

- ☑ 集約可能なログが多く、インシデント発生後 対応が迅速
- ☑ 有事の際のログ調査の簡素化が可能です。

こんなお悩みありませんか

リソース

- ⚠ 下請け・外注
- ⚠ その分高くなったり、柔軟性の低下が気になる

お任せください！ →

レオンテクノロジーなら！

迅速かつ丁寧な対応

- ☑ セキュリティベンダーで培った知見
- ☑ 問題解決の豊富な経験があります。迅速なインシデントの原因調査も得意としています。

実施フロー

1 ヒアリング

Windows のバージョンや導入予定台数などをヒアリングさせていただきます。

2 ご提案

ヒアリングさせていただいた内容を基に、費用などをご提案させていただきます。

3 お申し込み

弊社からログ収集用のエージェントアプリケーションを配布します。

4 インストール

お客様側で導入予定の端末にエージェントをインストールしていただきます。

5 運用

インストールが成功した後は、定期的に自動でイベントログをアップロードします。

※製品の仕様は、予告なく変更する場合があります。なお、ご不明な場合は、当社担当営業にお問い合わせください。
※本カタログ中の情報は、カタログ作成時点のものです。

当サービスについて詳しい内容・お問い合わせはこちらまで

LEON TECHNOLOGY

株式会社レオンテクノロジー
TEL 03-5957-1960
営業時間　平日 10:00～19:00

https://www.leon-tec.co.jp/
本カタログのサービスの詳細情報
https://www.leon-tec.co.jp/service/