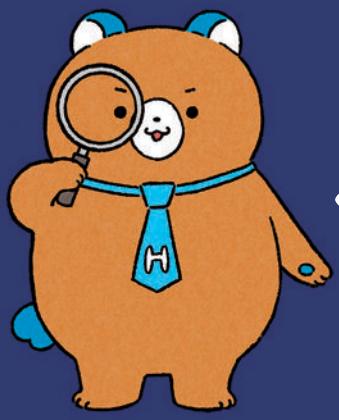
HARPの
ログ点検サービス

ろぐみ～る



組織の内部脅威によるセキュリティインシデント
ログの適切な分析による事前のリスク回避

株式会社HARP

できていますか?ログ分析

内部不正によるセキュリティインシデント実例

故意による内部脅威

不正閲覧

市納税課職員が勤務時間中に業務と関係なく興味本位で市民4名の住所や課税情報を閲覧した

↓

市に情報提供があり発覚

影響

- 市民の情報の漏洩および信頼の失墜

不正持ち出し

職員Aが、権限を持つ職員Bに依頼し全市民の個人情報を送付させた

↓

個人の満足感のために
このデータをUSBメモリに
コピーし無断持ち出し

影響

- 全市民の個人情報の漏洩
- 市は職員Aを住民基本台帳違反容疑で刑事告訴

過失による内部脅威

個人情報の紛失

業務委託先が作業のために必要なデータを記録したUSBメモリを市政情報センターから無断で持ち出し

↓

作業後、データ未削除のまま
飲食店に立ち寄り、帰宅時に紛失

影響

- 全市民の情報が一時紛失

故意・過失を問わず自治体内部の脅威による重大なインシデントが複数発生

不正のいち早い検知や抑止対策がますます重要に

セキュリティ10大脅威

「情報セキュリティ10大脅威」において「内部不正」が毎年ランクイン

内部からの不正アクセス等をはじめとする「内部不正による情報漏洩等の被害」は年々脅威を増しています。
内部の職員は重要情報にアクセスしやすく、アカウントの悪用や不正持ち出し等からインシデントが発生しています。
こういったインシデントはログの定期分析をすることによって早期に検知することが可能です。

また、ログの定期分析は個人情報保護委員会のガイドラインや立入検査で求められており、自治体の対応は行政手続における特定の個人を識別するための番号の利用等に関する法律で定められています。

※独立行政法人情報処理推進機構(IPA)
情報セキュリティ10大脅威2025[組織]

組織向け脅威

1 ランサム攻撃による被害	6 リモートワーク等の環境や仕組みを狙った攻撃
2 サプライチェーンや委託先を狙った攻撃	7 地政学的リスクに起因するサイバー攻撃
3 システムの脆弱性を突いた攻撃	8 分散型サービス妨害攻撃(DDoS攻撃)
4 内部不正による情報漏洩	9 ビジネスメール詐欺
5 機密情報等を狙った標的型攻撃	10 不注意による情報漏えい等

ログ点検サービス「ろぐみ～る」って？

ログの適切な分析により、組織の内部脅威によるセキュリティインシデントを発見、
または未然に防ぐための市町村向けサービスです。
ログをLGWAN上のWebシステムにアップロードすると、システムが自動でログを分析し、
2か月に1度、レポートの形で分析結果を提供します。

サービスの流れ（隔月のサイクルで実施）

LGWAN-ASP等
クラウドサービス

対象ログファイル

- 標準化対象の総合行政システム
- 端末操作が記録できる端末管理アプリ
- 「いつ」「誰が」「どこから」「何を実行」が記載されているログ全般

自治体から
ログを受領

受領ログを
分析

分析レポートを
提出

- 各点検項目の結果を［ABC判定］
- 「いつ」「どの端末が」「なぜ」検出したのか、「リスク」と合わせてレポート
- 第三者からの点検レポートで、客観的な事実確認が可能

自治体個別の運用に最適化

シンプルな点検項目	HARPの点検項目
勤務時間の操作	原課毎の業務傾向
異なる端末の操作	慣例的な運用方法
エラー操作の記録	年間イベントを考慮

ログを定期的に点検することで、
不正持出や不正閲覧、改ざんといった、特定個人情報の
不適切な取り扱いを検知するとともに、
職員のログ点検業務負荷を軽減します

例

人口1万人規模の
自治体について、
当社のセキュリティ業務
担当者が手作業で
作業を行う場合

ログの抽出、分析、レポート作成、レビューまで
1回あたり11人日の稼働がかかる…
（知見のない職員が行う場合はもっとかかる）

ログ点検サービスを利用することで
年間60人日の稼働削減が可能!!

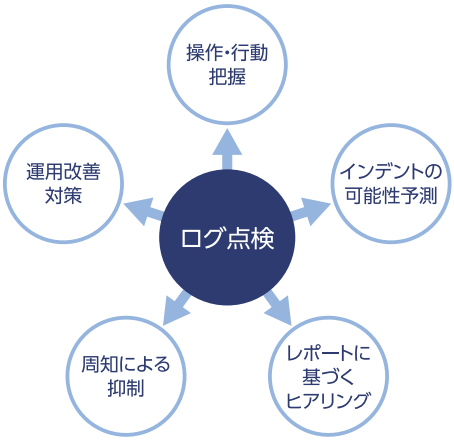
※隔月で年6回の運用を想定

HARPのログ点検サービスの強み

POINT 01

業務運用上のリスクを事前に把握

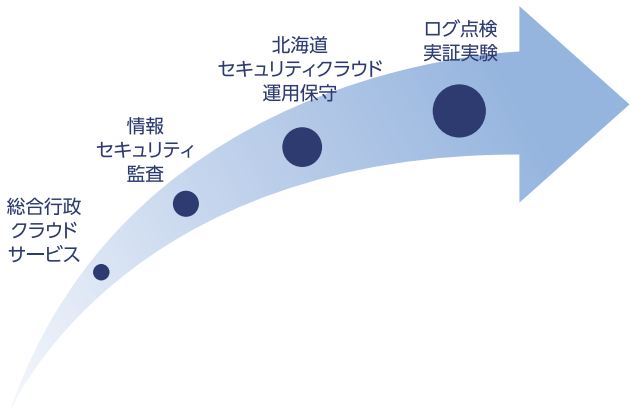
ログ分析のレポートにより操作・行動傾向を把握することができるため、「インシデントが起こってから」の対応ではなく、可能性や予兆から、有効な運用改善対策が取れるようになります。
また、ログ分析を定期的に実施している事実が庁内で周知されることで職員による内部不正に対する抑止効果にもなります。
第三者である弊社が作成したレポートに基づくことで、職員へのヒアリングが行い易くなります。



POINT 02

有識者の分析によるセキュリティガバナンス強化

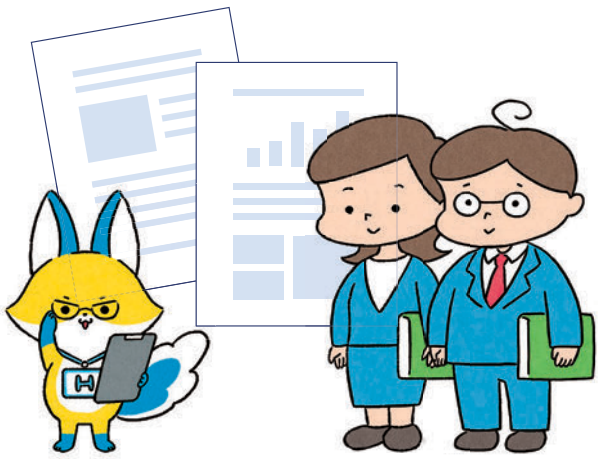
弊社はログ点検業務の実証実験、北海道セキュリティクラウド運用保守、情報セキュリティ監査、総合行政クラウドサービス等の実績から、豊富な知見を有しています。
有識者の徹底的な分析によりセキュリティガバナンス強化に繋がります。



POINT 03

個人情報保護委員会の立入検査を想定

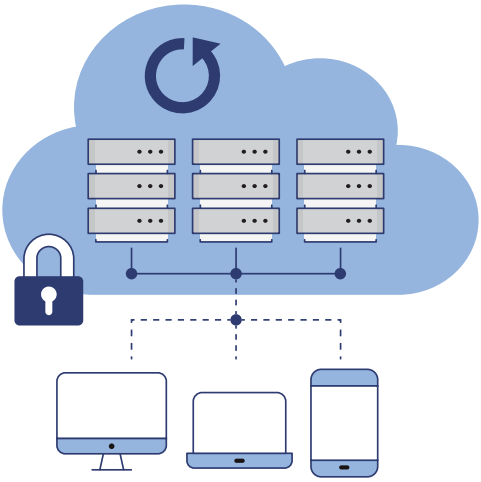
ろぐみ～るは、個人情報保護委員会からログの定期点検について指摘を受けた自治体様のご要望から開発され、複数自治体様と約1年間の実証実験を経てアップデートを重ねています。



POINT 04

LGWAN上で分析可能!

ろぐみ～るは、LGWAN上で提供するWebサービスです。分析対象ログは LGWAN接続系の端末からシステムへアップロードが可能であり、セキュアな環境で情報の受け渡しも安心してご利用いただけます。



点検レポートを納品!
個人情報保護委員会が求める基準を想定

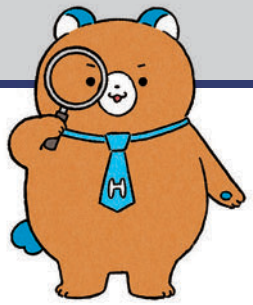
故意による内部脅威の事例
他人のIDで戸籍情報管理システムに不正アクセス

調査結果

- Bさんが他の職員（Aさん）のパスワードを盗用
- 戸籍情報管理システムにアクセス
- 計93回の戸籍情報の閲覧と帳票35部を出力
- 不正者（Bさん）は元市民課戸籍係の前歴あり
- 専用端末に権限のない職員が操作している

「複雑な家系図を作成したかった」職員が
戸籍情報管理システムに
不正アクセスし
停職3カ月の懲戒処分

ログ点検



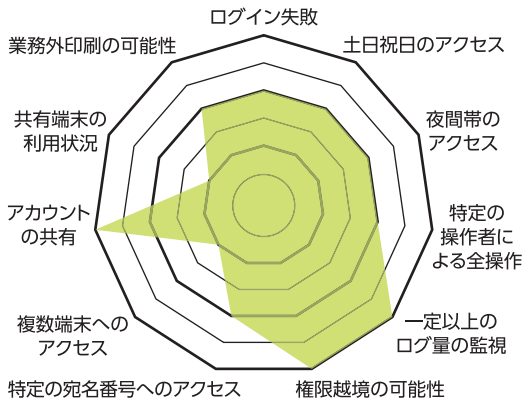
12の観点で分析を行い、予想されるリスクを
A・B・Cの3段階で評価します。
例えば、この不正事例について、ろぐみ～るでは
以下のようにレポートされます。

Ⅰ 点検結果サマリ（レポートイメージ）

判定

B

点検項目



点検結果

【X月X日 ●時▲分頃】

BさんがAさんのアカウントを利用し戸籍情報を出力した可能性があります。
また、時期的には人事異動の時期ではないと推察されますため、アカウント盗用のリスクがあります。

【客観的な証拠】

- Aさんの普段の戸籍情報の業務パターンと異なる
- Aさんが専用端末を普段使わない時間に操作ログが検出
- Aさんのログイン記録が同時刻に別ロケーションで2件発見
- Bさんのアカウントで専用端末のログイン成功を確認
- 専用端末から戸籍情報管理システムのAさんのアカウントでのログイン記録を確認
- Aさんの異常検知した時間帯は、Bさんが操作記録が存在しない
- 異常検知した時間帯に専用端末付近の端末のアクセス記録がない

こんなお悩みを解決します

Before	After
● 人手が足りない	● アウトソーシングで別業務集中
● ログの分析方法が分からない	● 分析済みのレポートを提出
● 何から始めれば良いか分からない	● 有識者によるトータルサポートで安心
● 不正の定義が決められない	● 関連事項に対する諸条件を代理で設定
● 不正疑惑の職員へヒアリングしづらい	● 第三者レポートに基づくヒアリングで客観的に事実確認

導入の流れ

STEP 01 ご契約

スケジュールや対象とするログの確認、進め方について協議・決定

STEP 02 ヒアリングシート記入

ログ種類や点検項目について記入

STEP 03 ログ提出

各タイミングで対象ログを提出

STEP 04 レポート納品

提出いただいたログから点検項目に基づいたレポートを納品

お問い合わせ

TEL 011-206-7970（企画営業部 ダイヤルイン）

MAIL eigyo-harp@e-harp.jp

もっと詳しく知りたい方は

HARPろぐみ～る

HARPではお客様に安心して
ご利用いただけるよう
ISMS認証・Pマークを取得しています

株式会社HARP

〒060-0001
北海道札幌市中央区北1条西6丁目1-2 アーバンネット札幌ビル3F
TEL. 011-221-5800　FAX. 011-212-7082

www.e-harp.jp/logmeel