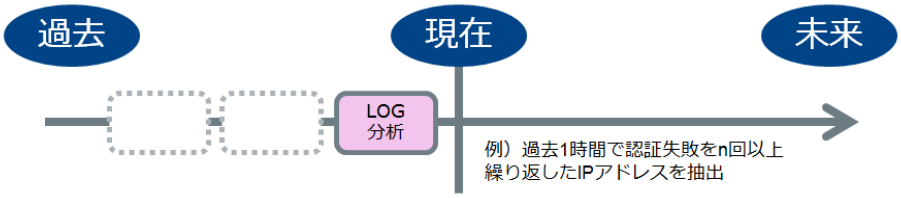
【別紙 4】 ３種類の時系列分析の概要

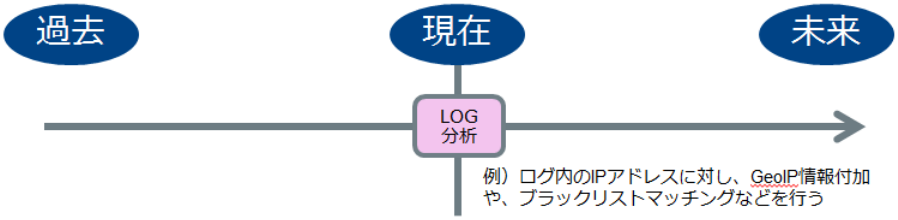
時間軸を踏まえた複数の時系列分析により様々な攻撃の検知に対応します。

①バッチ処理：定期的に過去のログを分析処理



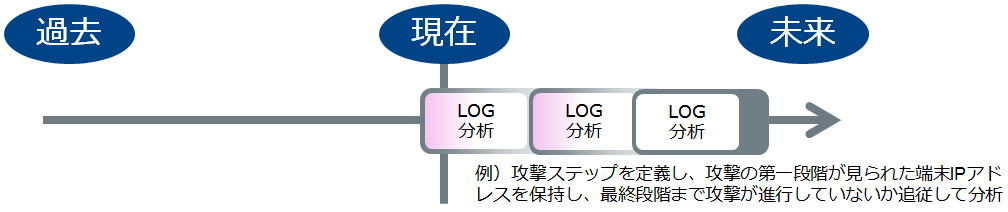
バッチ分析エンジンは，一定期間のログデータを取込み，時系列の中で攻撃もしくは攻撃の予兆と思われるものを検知します。例えば，一定時間内に特定国との接続を繰り返しているパターン，一定のデータ量通信を繰り返しているパターン等を自動検知しています。これにより，ある「過去」時点でのリアルタイム検知をかいくぐった，時間をおいて「未来」に活動するタイプの攻撃を検出します。

②リアルタイム処理：複数装置からのログに対し相関性を分析処理



リアルタイム分析エンジンは，機器のログデータをリアルタイムで取込み，独自に開発したシグネチャならびにルール(ロジック)を適用することにより「現在」発生している脅威を検知します。例えば，データ転送のないコネクション，ブラックリスト登録先への TCP/UDP コネクション等の検出や，オフィス時間外のサーバログイン，複数回のログイン試行等を自動検知しています。これはセキュリティ機器の検知を非セキュリティ機器のログ及び独自の知見により補完し，リスクアナリストによる検証を支援します。

③スライディングウィンドウ処理：特定ログをトリガーに分析を開始/追従



スライディングウィンドウ分析エンジンは、典型的な攻撃パターンの一部が見られたログを基に、特定 PC やサーバーの動作を継続的に追跡調査し、攻撃の進展を検知します。