・カメラ付きの通信装置が、人の顔などを撮ってその特徴をベクトル情報として取得する
　→ 具体的には、顔画像や全身画像からAIなどを使って特徴量（例：目の位置、輪郭、姿勢など）を数値データ（ベクトル）として抽出します。これは生体情報の一種です。

・そのベクトル情報を「個人情報に戻せない形」に変換する（元に戻せない＝非可逆変換）
　→ 個人情報保護のため、ベクトル情報をそのままサーバに送るのではなく、復元できない形に加工します。これにより、誰かを特定されるリスクを減らします。

・この変換には、似た情報から似た結果が出るような方法（LSH＝類似性ハッシュなど）を使う
　→ 似ている人物のベクトル情報からは、似たビット列（変換情報）が生成される仕組みです。これにより、異なるカメラで同じ人を似たデータとして認識できます。

・変換された情報と、カメラ内での人の位置情報を一緒にサーバに送る
　→ 「この人は今カメラのどこに映っているか」という位置情報と、加工済みの個人情報を同時に送信します。位置情報は、追跡のために重要な要素です。

・サーバは各カメラから送られてきたデータを受け取り、保存する
　→ サーバ側では、通信装置ごとに送られたビット列と位置情報を記録し、あとで追跡処理に使えるようにします。

・複数カメラからの情報を使って、同じ人を追いかける（追跡する）ことができる
　→ 一つのカメラから出て別のカメラに映ったとしても、似た変換情報が得られるので、「同じ人だな」と判断して継続的に追いかけることができます。

・個人が誰かは特定できないが、「同じ人っぽい」ということは分かる
　→ 完全な識別ではなく、「たぶんこの人とこの人は同じ人物」と推定できるようにしています。これにより、法律的に「個人情報」ではないとみなされます。

・この技術を使えば、カメラの映像が重なっていなくても、人の移動経路（動線）を追える
　→ 例えば、Aカメラの視野から消えた人が、数秒後に離れたBカメラに映ったときも、「同じ変換情報」が得られれば追跡が成立します。

・つまり、プライバシーを守りながら人の動きを追跡できる仕組み
　→ 法的に個人情報にあたらない情報を使って、人の流れを分析できるので、ショッピングモールや駅、イベント会場などでの人流管理に役立つ可能性があります。