本資料について

本資料は下記論文を基にして作成されたものです．文書の内容の正確さは保障できないため，正確な知識を求める方は原文を参照してください．

著者， M. Danley　D. Mulligan　J. Morris　J. Peterson
論文名， Threat Analysis of the geopriv Protocol draft-ietf-geopriv-threat-analysis-00
出展， IETF Internet Drafts
発表日， 2003**年**5**月**18**日**

geoprivの脅威

渡邊研究室

00J139　**柳沢信成**

要約

- このドキュメントでは、geopriv構造に対して脅威の分析をする
- この脅威とは、データの記憶から構造の実態による結果、およびgeoprivによってもたらされた情報の乱用である

geoprivについて

- Geographic Location/Privacy
- **地理情報（緯度経度や高度など）をオブジェクト・データ化して、HTTPやHTMLで表現したり検索できる仕組みを目指している**
- **利用者のプライバシーを保護するための匿名性の仕組みも考慮 しなければならない**

用語集

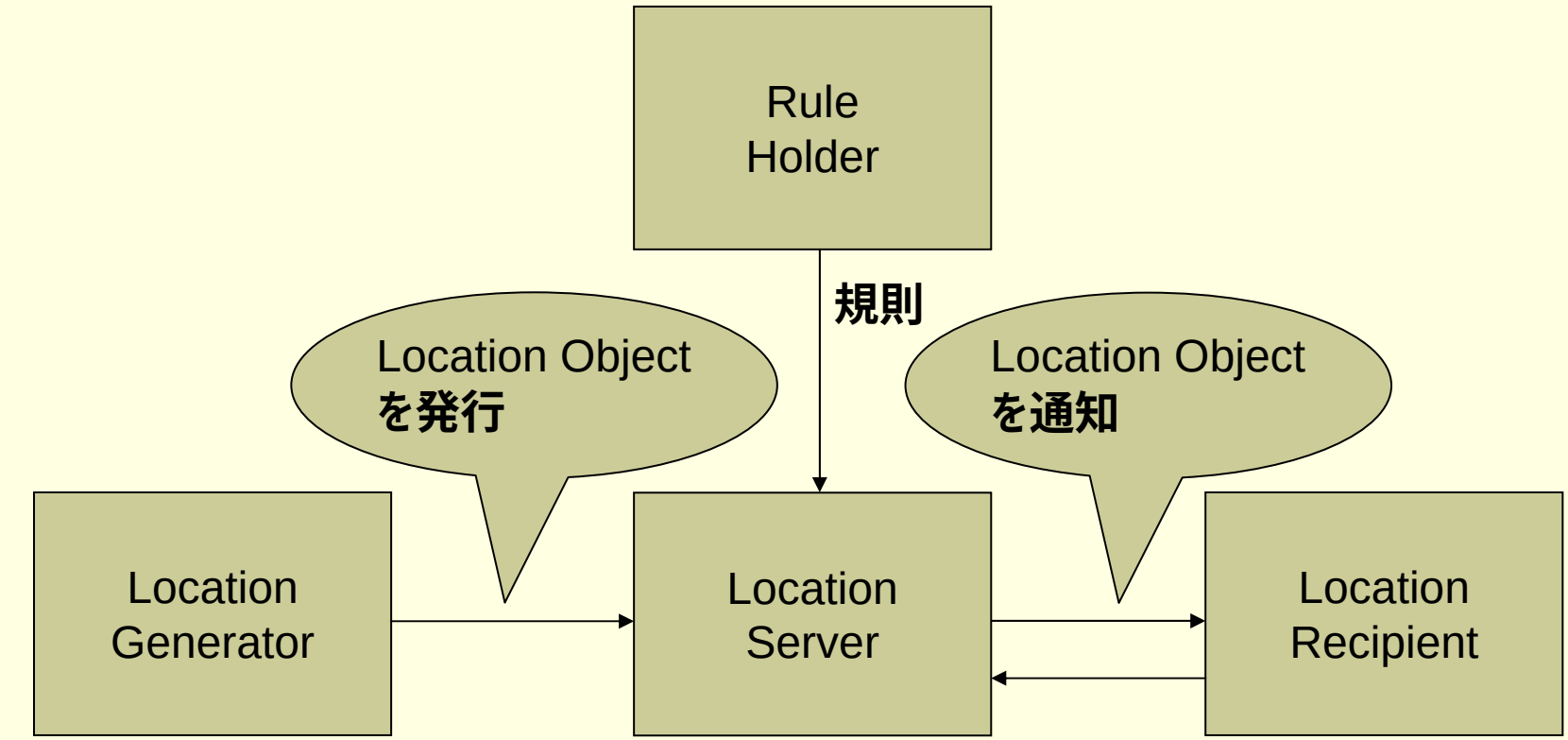
- Location Information (LI)
  - **位置情報**
- Rule Maker
  - Target**の位置情報の規則（内容）を決めるもの**
  - **どれだけの情報を、誰に知らせるかなど**
  - Target**自身がきめる**
- Rule Holder
  - **規則を保持するもの**

用語集

- Location Object (LO)
  - **位置情報を伝えるもの**
- Location Generator (LG)
  - Target**の位置を決定し、**LO**を作成するもの**
- Location Recipient (LR)
  - **位置情報を受け取るもの**
- Location Server (LS)
  - **規則を適用し、**LR**に位置情報を発行するもの**

基本的な構造

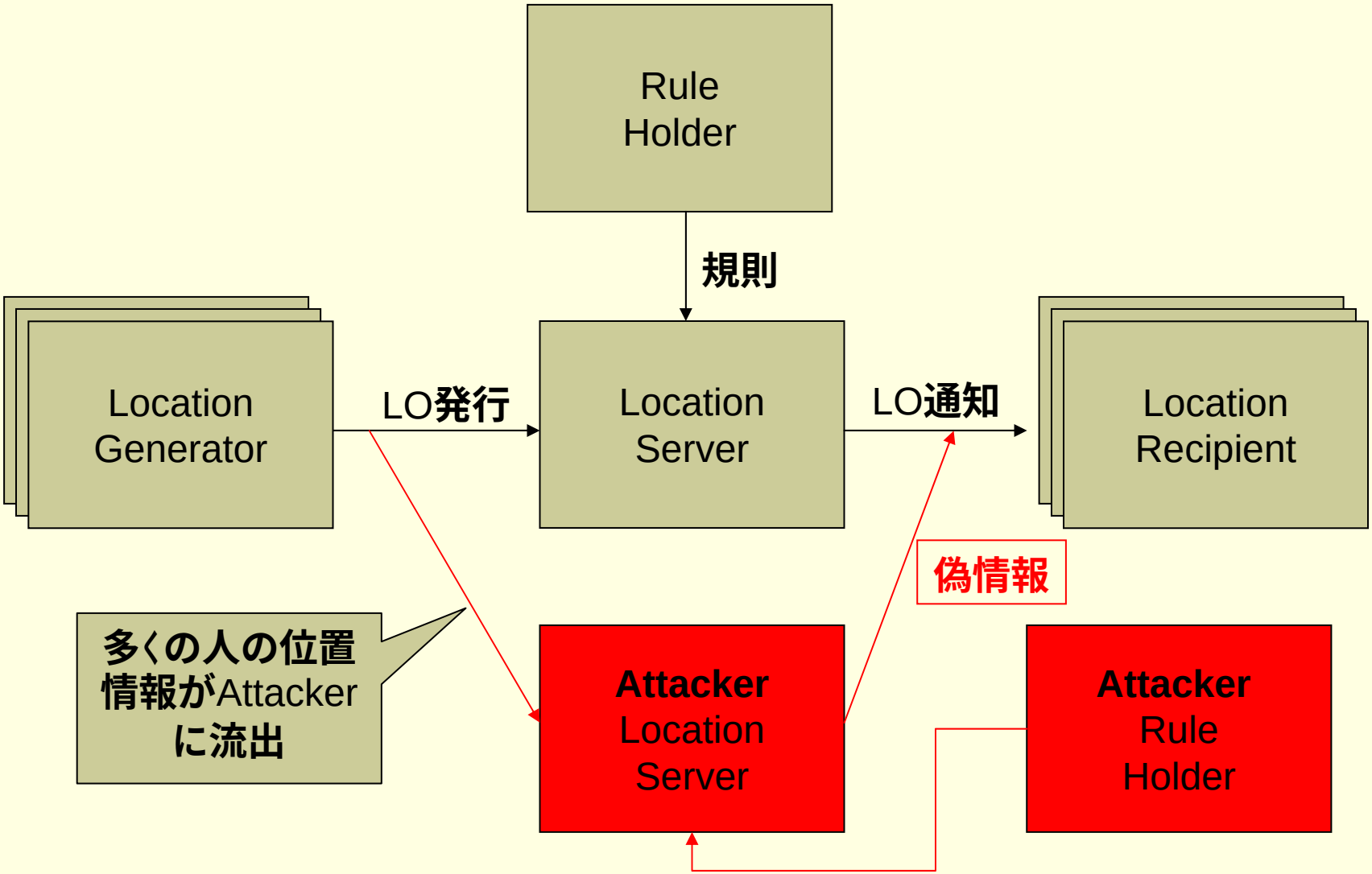
draft-ietf-geopriv-reqs-03.txt より



geoprivへの攻撃

- 他人の位置情報を知ることは、プライバシーの侵害となる
- geopriv全体のシステムの停止をもくろむ攻撃者もいるかもしれない

Serverへのものまね

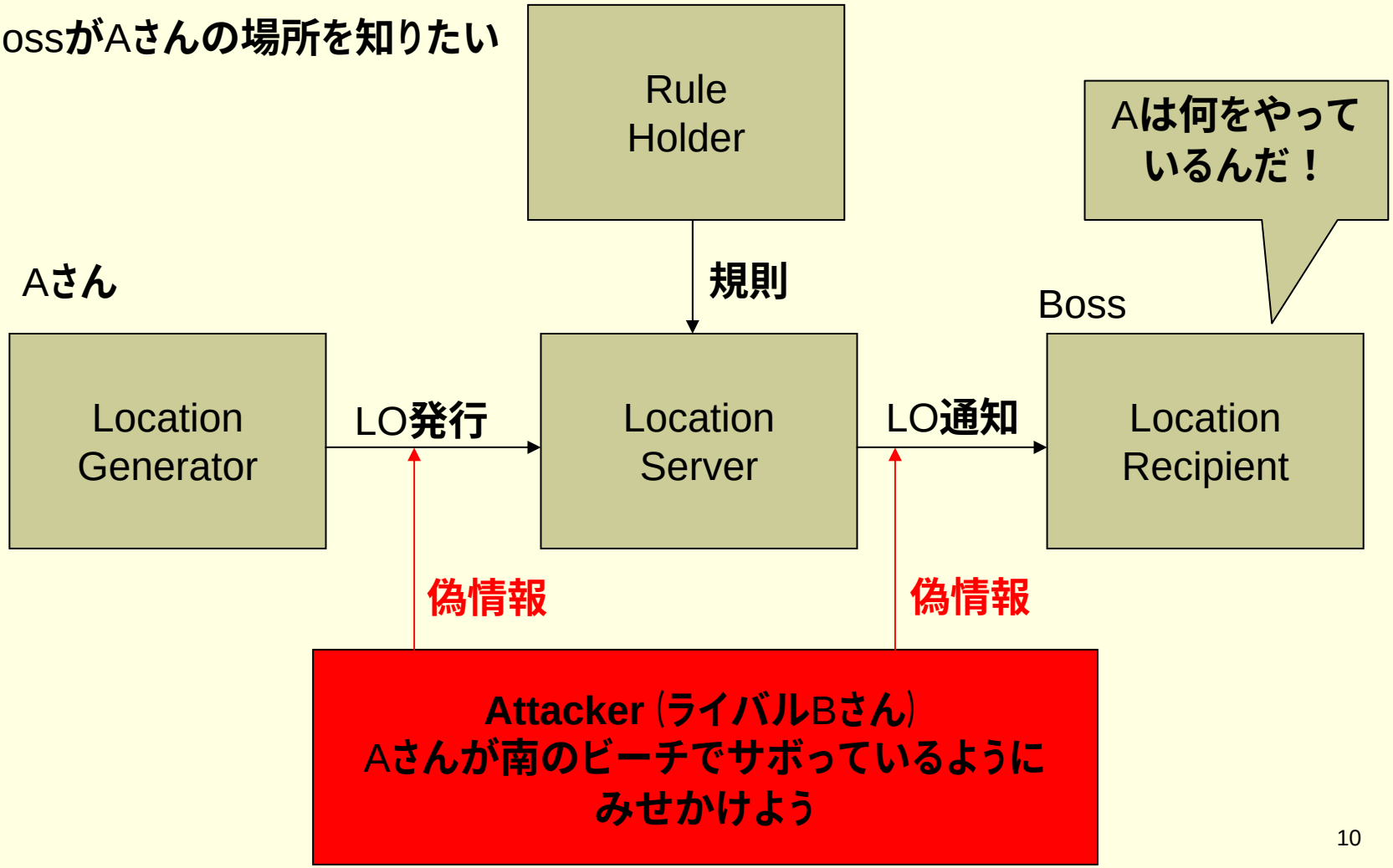


Serverへのものまね

- 秘密性がLGとLSとの接続、LSとLRとの接続の両方が必要である
- ものまねを防ぐために、LSはLRを認証できなければならない
- 同様に、LGはものまねを防ぐためにLSを認証することができなければならない
- 最終的に、LSはRule Makerを認証して、権限のないパーティーが規則を変えることを絶対にできないようにしなければならない

身元をだます

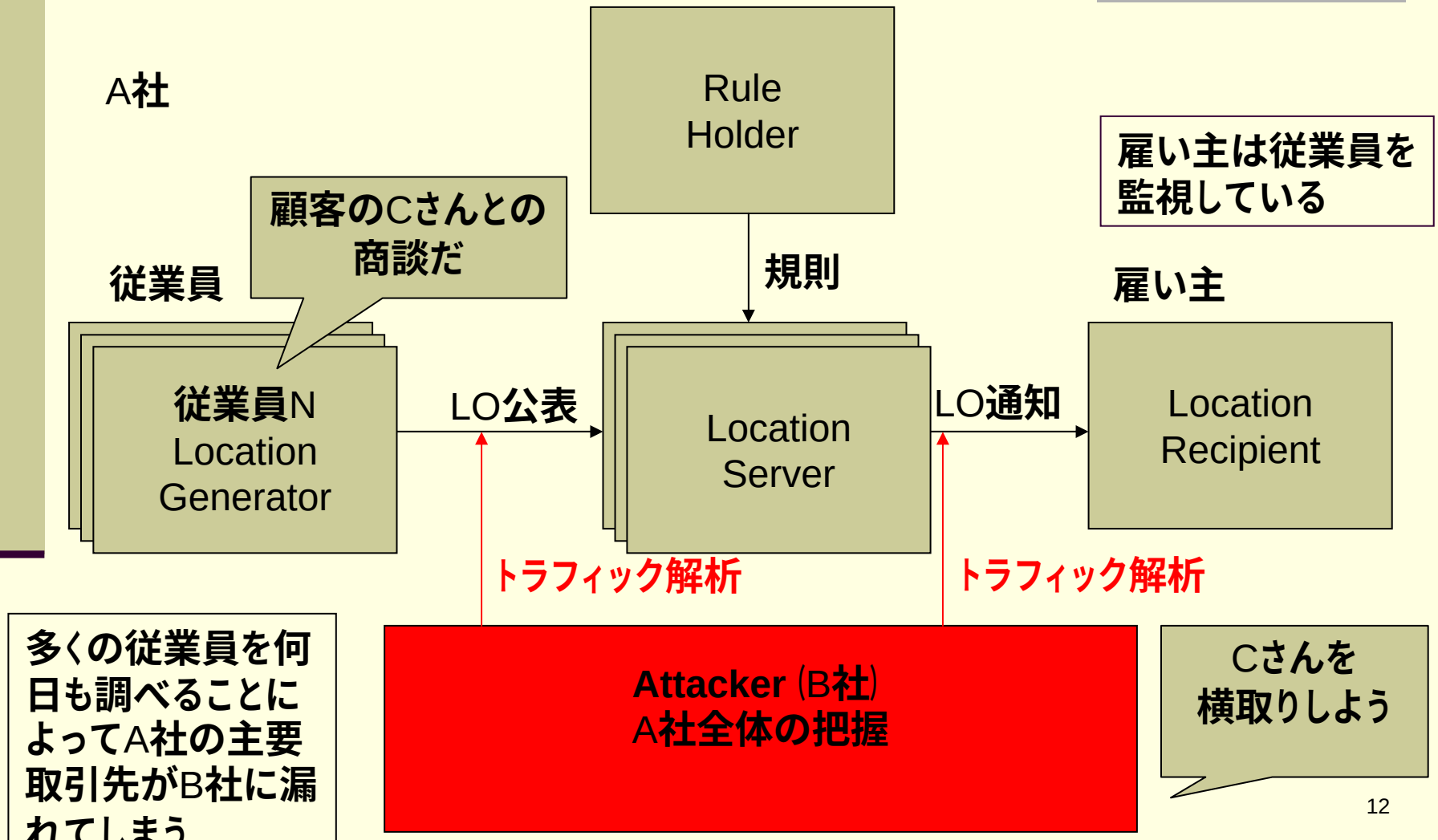
BossがAさんの場所を知りたい



身元をだます

- LSはLGを認証する必要がある
- 同様に、LRはLGを認証する必要がある

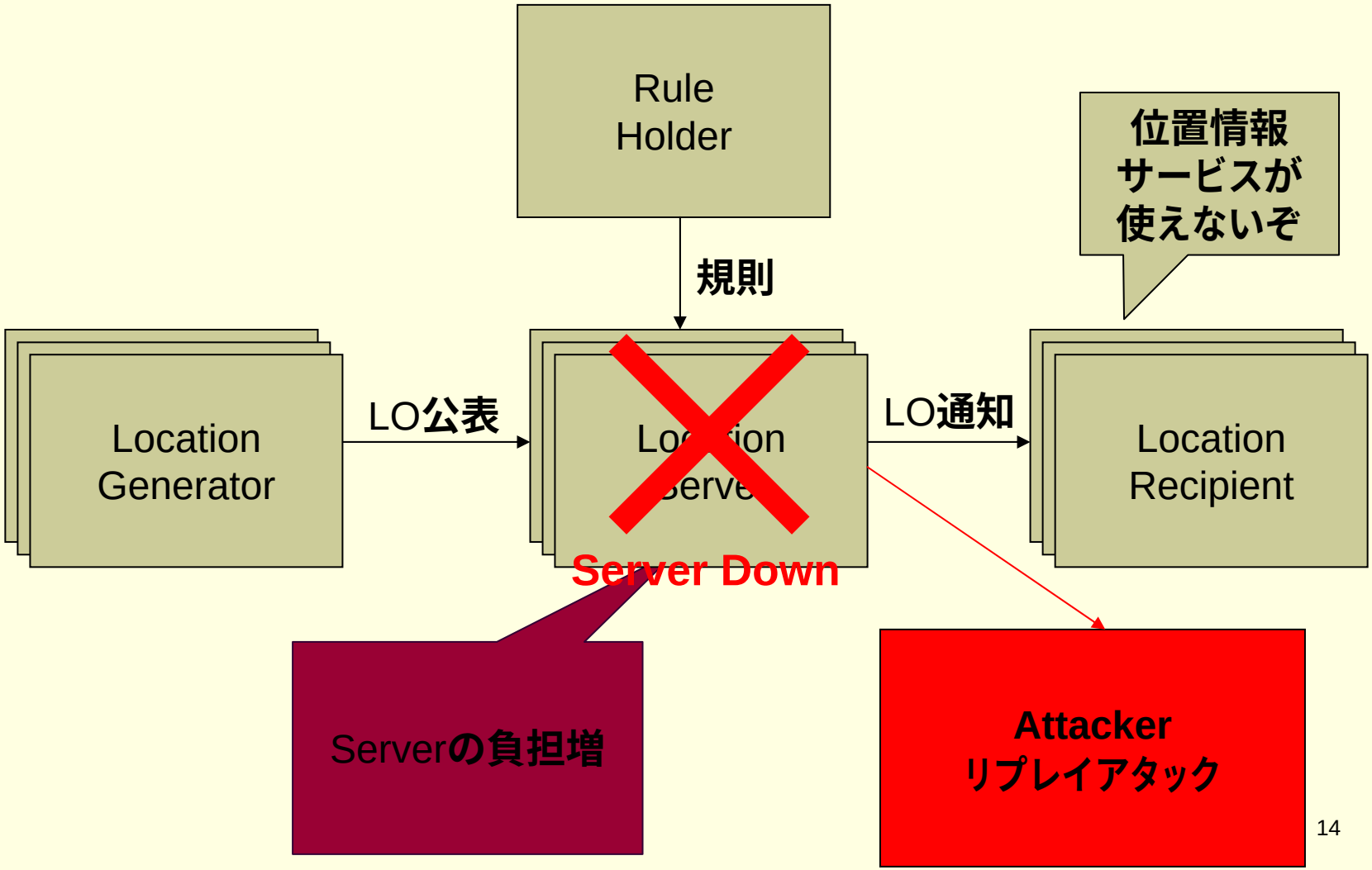
情報収集


A社
Rule Holder
雇い主は従業員を監視している
顧客のCさんとの商談だ
従業員
規則
雇い主
従業員N Location Generator
LO公表
Location Server
LO通知
Location Recipient
トラフィック解析
トラフィック解析
多くの従業員を何日も調べることによってA社の主要取引先がB社に漏れてしまう
Attacker (B社)
A社全体の把握
Cさんを横取りしよう

情報収集

- Rule Makerは、彼らの位置情報の仕様に関して、規則を定義できなければならない
- LSとLRとの接続が、秘密でなければならないのと同様に、LGとLSとの接続も秘密のままでなければならない
- LSは、ものまねを防ぐために、LRを認証することができなければならない
- LSは、権限の無い実体が確実に規則を変えることができないようするために、Rule Makerを認証することができなければならない

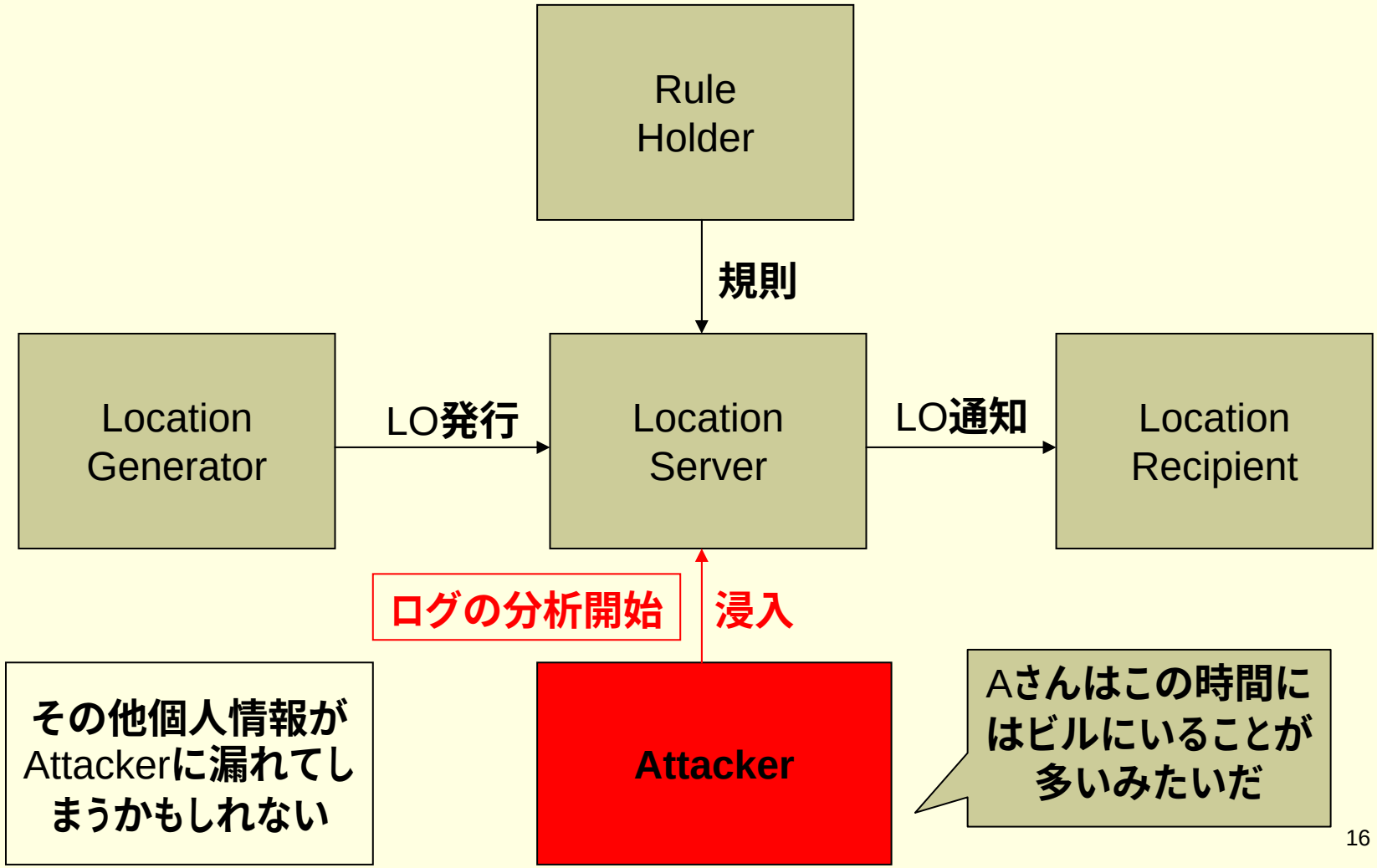
サービスの停止


Rule
Holder
規則
位置情報
サービスが
使えないぞ
Location
Generator
LO公表
LO通知
Location
Recipient
Server Down
Serverの負担増
Attacker
リプレイアタック

サービスの停止

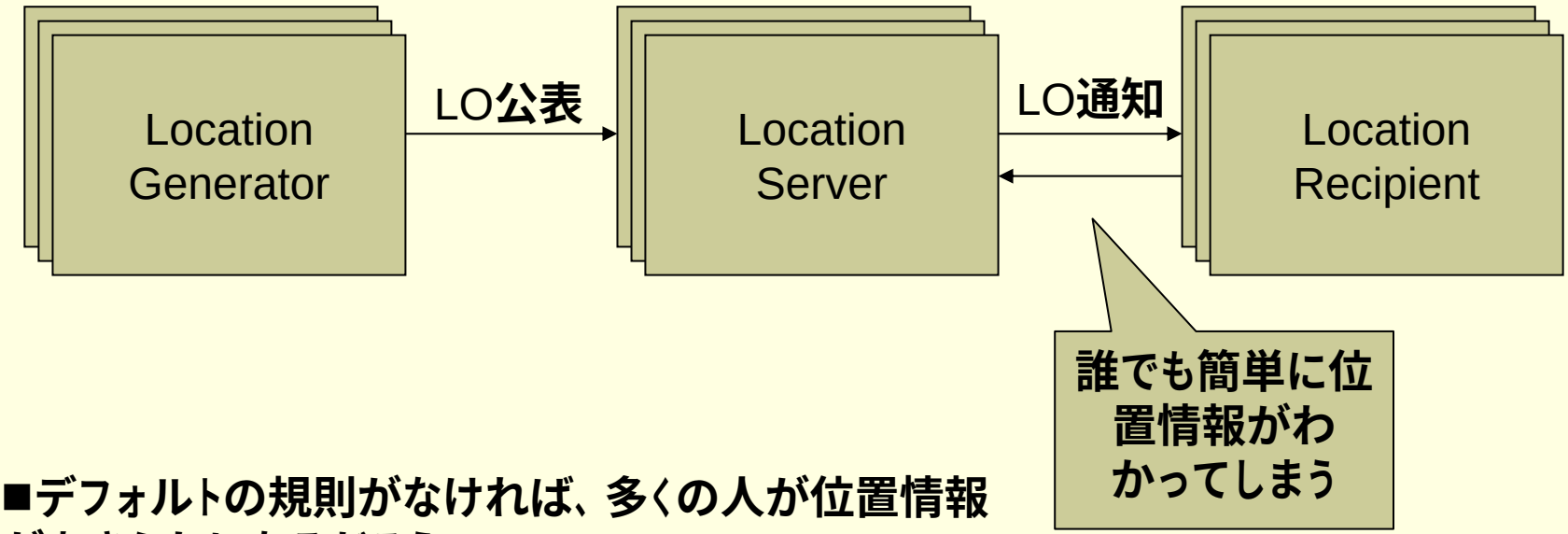
- LSは、認証挑戦と認証試みが不必要にシステム資源を消費しないように、測定をしなければならない
- Rule Makerは位置情報がリプレイアタックを防ぐため、送られてくる情報の割合を制限しなければならない

サーバーへの浸入


Rule Holder
規則
Location Generator
LO発行
Location Server
LO通知
Location Recipient
ログの分析開始
浸入
その他個人情報がAttackerに漏れてしまうかもしれない
Attacker
Aさんはこの時間にはビルにいることが多いみたいだ

規則がなかった場合

Rule Holderに
規則が無かった場合



■デフォルトの規則がなければ、多くの人が位置情報があきらかになるだろう

■プライバシー規則は、位置情報の収集、使用、公開、および保有を制御すべきである

対策(1)

- 正しい情報習慣として7つの主な原則がある
- 1.開放性
  - 位置情報がどのような目的、用途で使われたか個人に知らせるべきである
- 2.個々の参加
  - 個々が、彼らについて集められた全ての情報を見て、不正確な情報は修正するか、取り除かなくてはならない
- 3.収集制限
  - データ収集は取引をするのに必要最低限にすべきである

対策 (2)

- 4.データの品質
  - 個人情報は正確で、完全で、タイムリーでなければならない
- 5.最終的な状態
  - データは、支持された目的だけで使われるべきで、別の目的で使われてはならない
- 6.セキュリティ
  - 個人データは、損失、権限の無いアクセス、破壊、使用、変更、または公開のようなリスクから保護しなければならない
- 7.責任
  - 記録保持者は責任があるべきである

geoprivプロトコルのセキュリティ特性 (1)

- **対策としての規則**
  - Rule Makerでは、収集制限と最終的な状態を定義しなければならない
  - geoprivはデフォルトの規則 (位置情報の公開と制限) を含むべきである。そして、Rule Makerは個々のプライバシーを守るため、自由に自己の規則を変えることができなければならない
  - 収集制限を守るため、LRは全ての規則に気づいているべきではない
  - 位置情報のログの編集を防ぐため、規則はLOに適用されているべきである

geoprivプロトコルのセキュリティ特性 (2)

- **データの伝達の間のセキュリティ**
  - Rule Maker**は、ある特定期間内の情報要求の数を設定すべきである**
  - LS**と**LR**との接続、**LS**と**LR**との接続では、**LO**の秘密性が非常に重要である**
  - LS**はLRと**Rule Maker**、**LG**はLSを認証しなければならない**

geoprivプロトコルのセキュリティ特性 (2)

- データの伝達の間のセキュリティ