レピュテーションの観点から IPアドレスをクリーニングする

シスコシステムズ合同会社

コンサルティングシステムズエンジニア

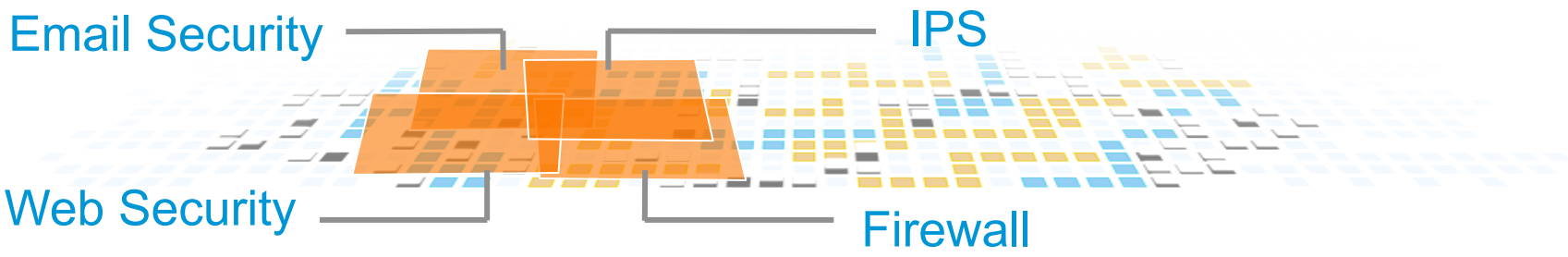
小林 秀行

アジェンダ

1. IPレピュテーション
2. 汚れたIPアドレスの課題
3. IPアドレスのクリーニング

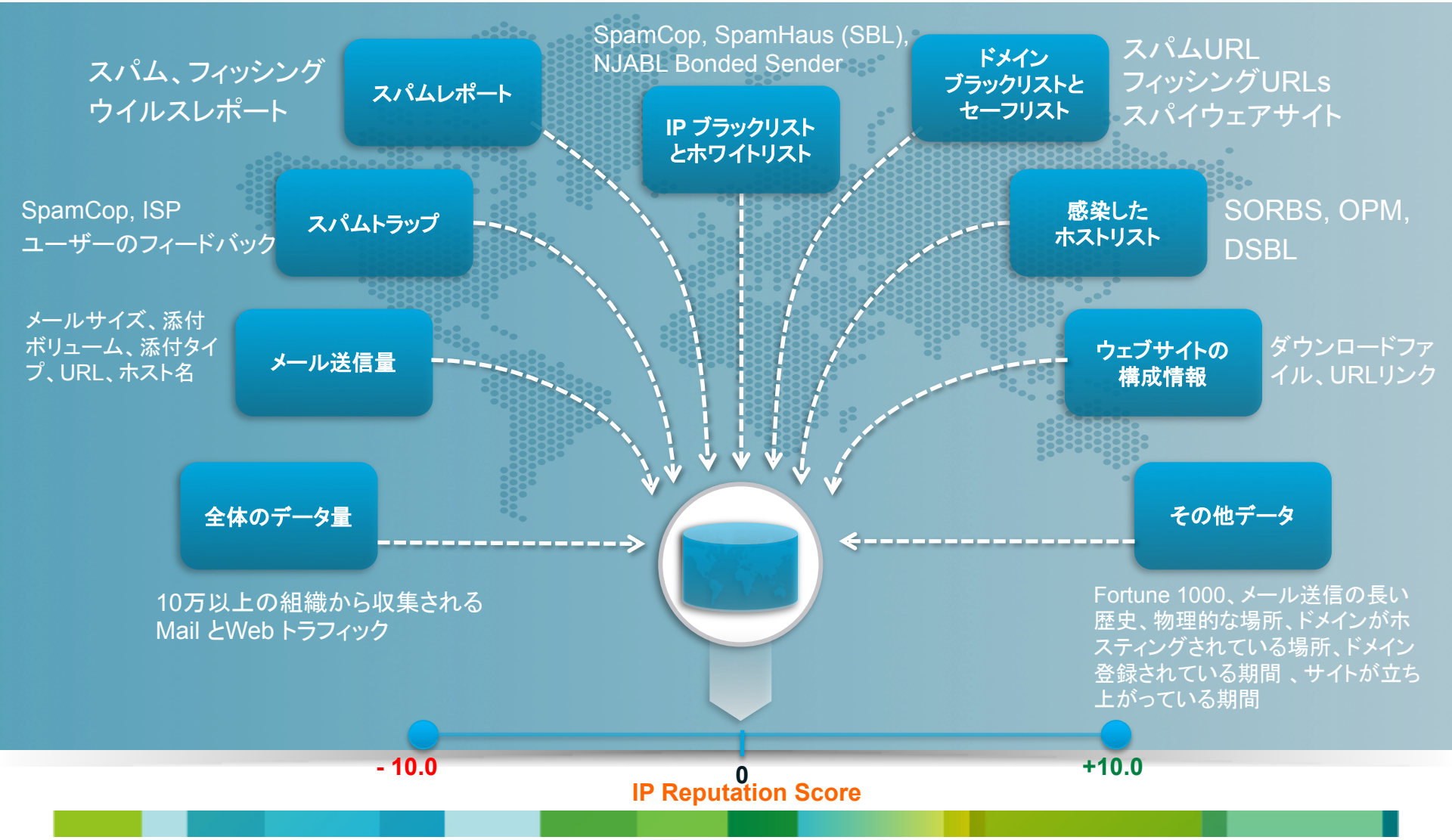
1 IPレピュテーション

IPレピュテーション
レピュテーションはIPアドレスの活動履歴である。

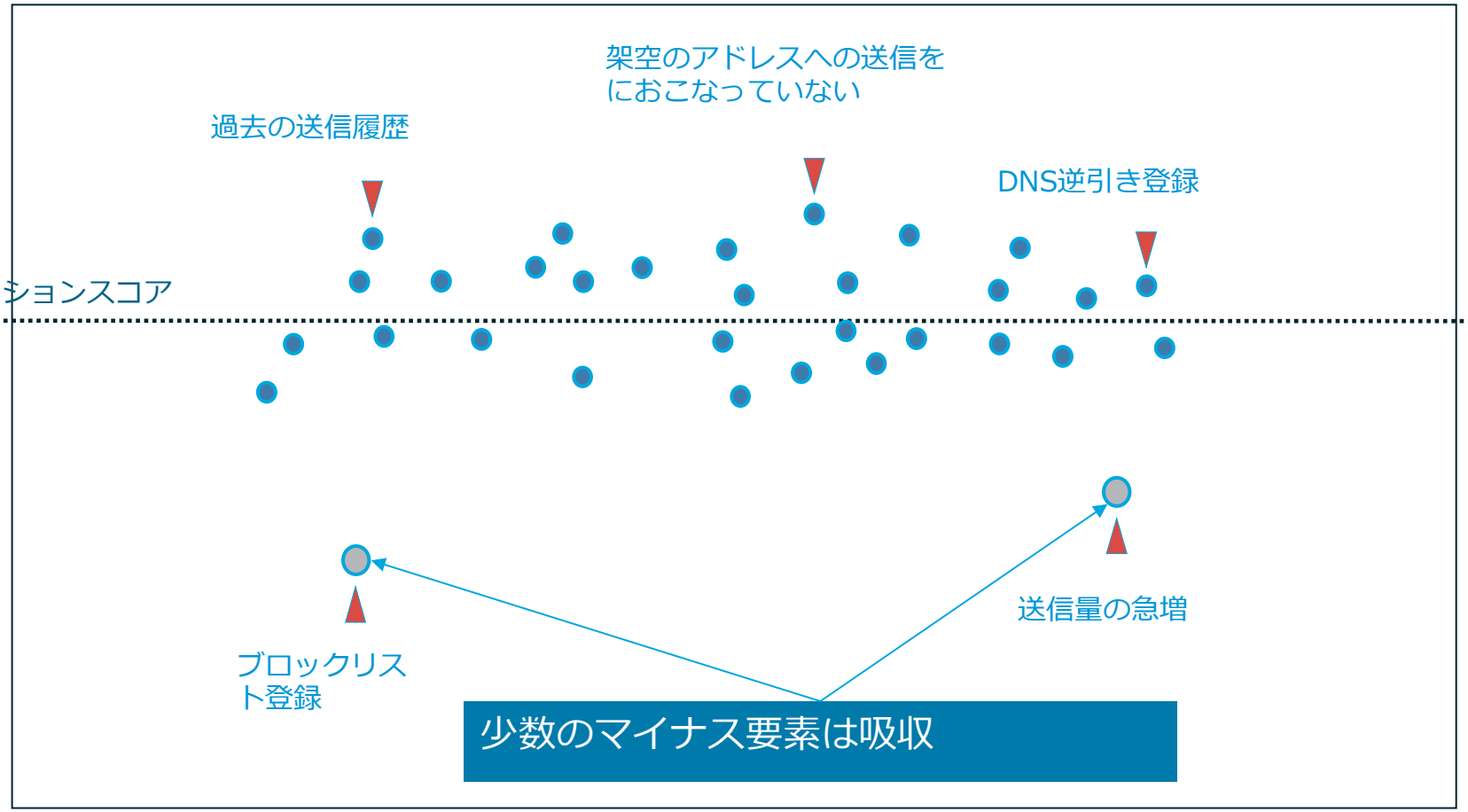


- レピュテーションとはIPアドレス、ネットワーク品質のヒストリーである。
- コンテンツ検査、カテゴライズ、ブラック／ホワイトリストではない。
- 過去の行動履歴やコンテキストに基づいた、統計的なリスク評価である。
- 膨大なデータから複数の要素の組み合わせでスコアを計算する。

レピュテーションデータベース
様々なデータ・ソースから情報を収集する。



レピュテーションスコア
スコアは複数の要素を組み合わせて判定する。

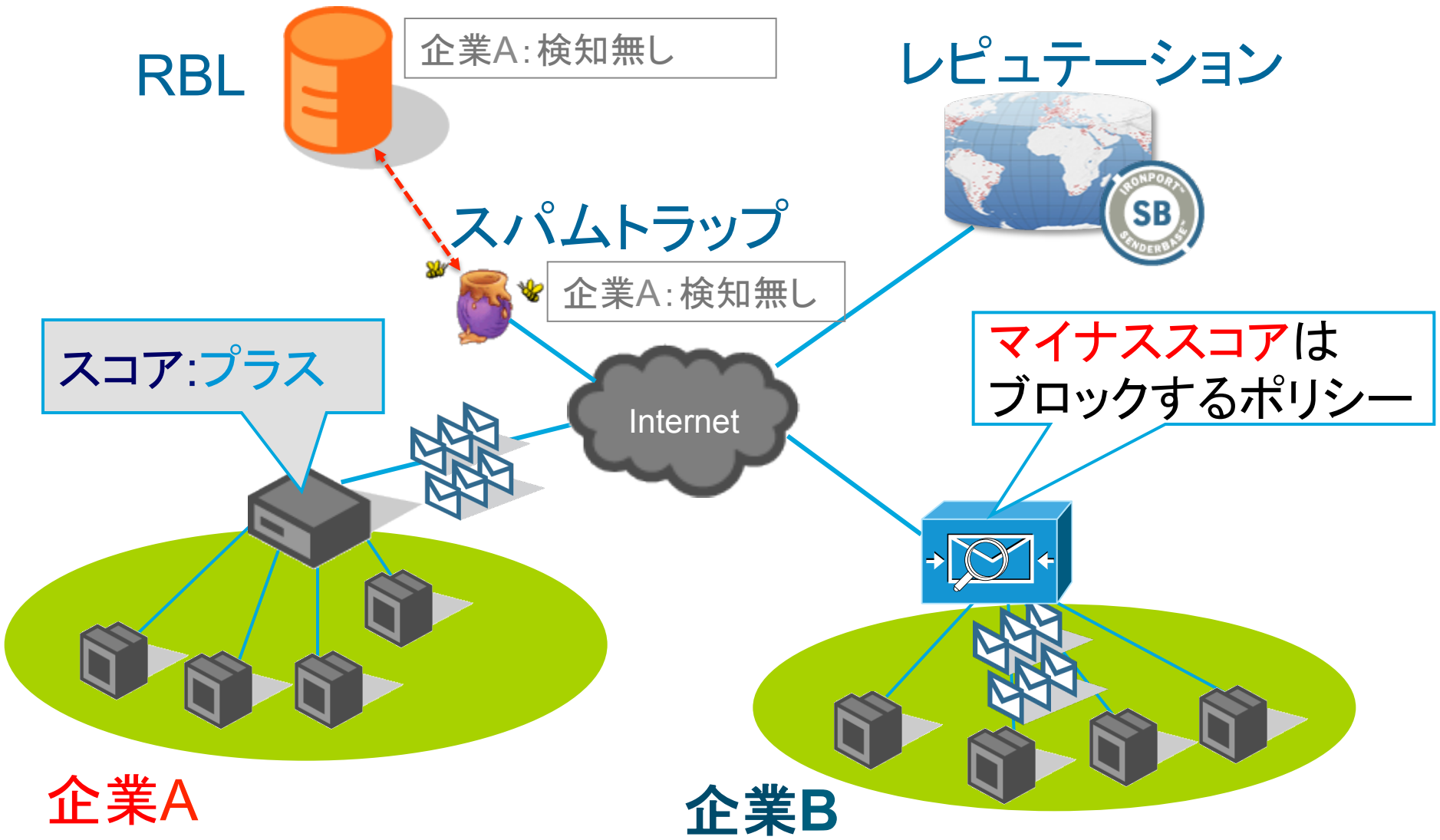


Senderbaseデモ

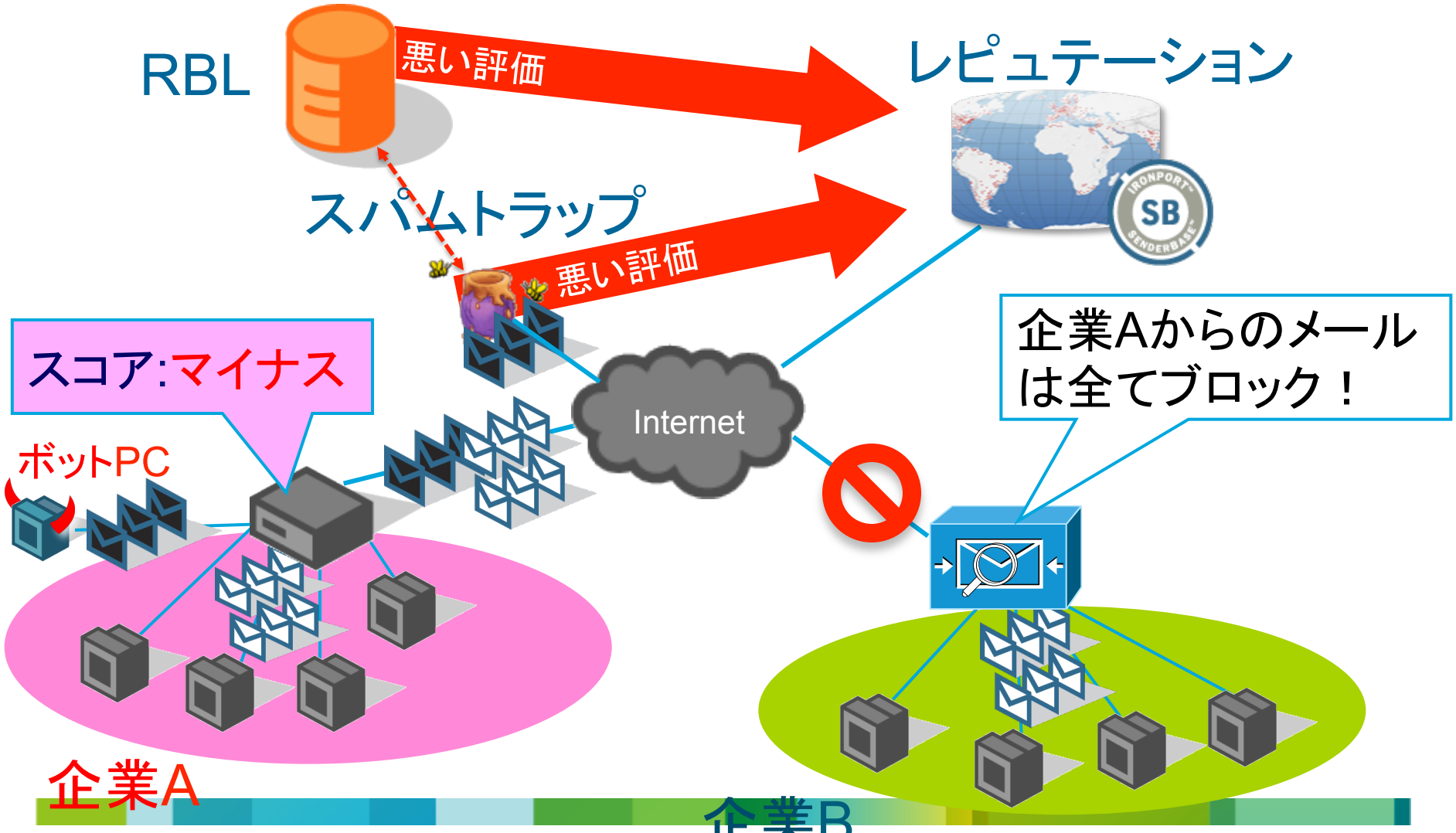
2

汚れたIPアドレスの課題

送信元が汚れていないIPアドレスの場合
企業Aから企業Bにメール送信が完了する。



送信元が汚れてしまったIPアドレスの場合
企業Aから企業Bにメール送信ができない！！！



汚れたIPアドレスの課題
如何にハズレを引かないようにするかが重要！！

1. 前所有者のアクティビティによって、新しく取得したIPアドレスのレピュテーション評価がすでに低い可能性がある。
2. 結果何も悪いことしてないのにレピュテーションフィルタでブロックされサービス利用出来ないこともある。
3. DMZ系（メール、ウェブ）や外部向けサービスとして利用されていたIPアドレスは汚れている可能性が非常に高い。
4. 一度スコアが汚れてしまう（マイナスの評価）と、一般的に元に戻すのには時間がかかる。
5. レピュテーションスコアの再評価はユーザーからの申告が非常に重要。

3

IPアドレスのクリーニング

汚れたIPアドレスクリーニングのヒント
レピュテーションの評価を上げていくには？？

1. インフラ系のアドレスは綺麗（スコアリングされていないIP）
   - インフラ系のアドレスをサービス系に利用する。
2. IPアドレスの移転は根本解決にはならない。
   - 取得前に前所有者のアクティビティを確認するのが重要。
3. 定期的で安定したメール流通量が大事。
   - レピュテーションはメール量もアルゴリズムの一要素としている。
4. 突発的なメール流量を検知し抑える（レートリミット）。
   - 突発的なメール量はスパムとみなされやすいので注意。
5. 各ベンダーにレピュテーションスコアの再評価を依頼する。
   - サービス系で利用されたIPアドレスは利用しないとスコアは徐々に下がっていく。
   - 一度下がったスコアは上がりにくい。
     トラフィックボリュームが少ないので定期的な再評価の対象から外れる。

Thank you.