agenda

NIFTY Cloud
ニフティクラウド

1 **submission 踏み台問題とは？**

加瀬　正樹（ニフティ株式会社）

2 **ISPの対応事例～BIGLOBE編～**

加藤　理人（NECビッグローブ株式会社）

3 **スパムメール×マルウェアの実態**

上村　理（トレンドマイクロ株式会社）

4 **Submission踏み台問題への対策**

西島　正憲（株式会社シマンテック）

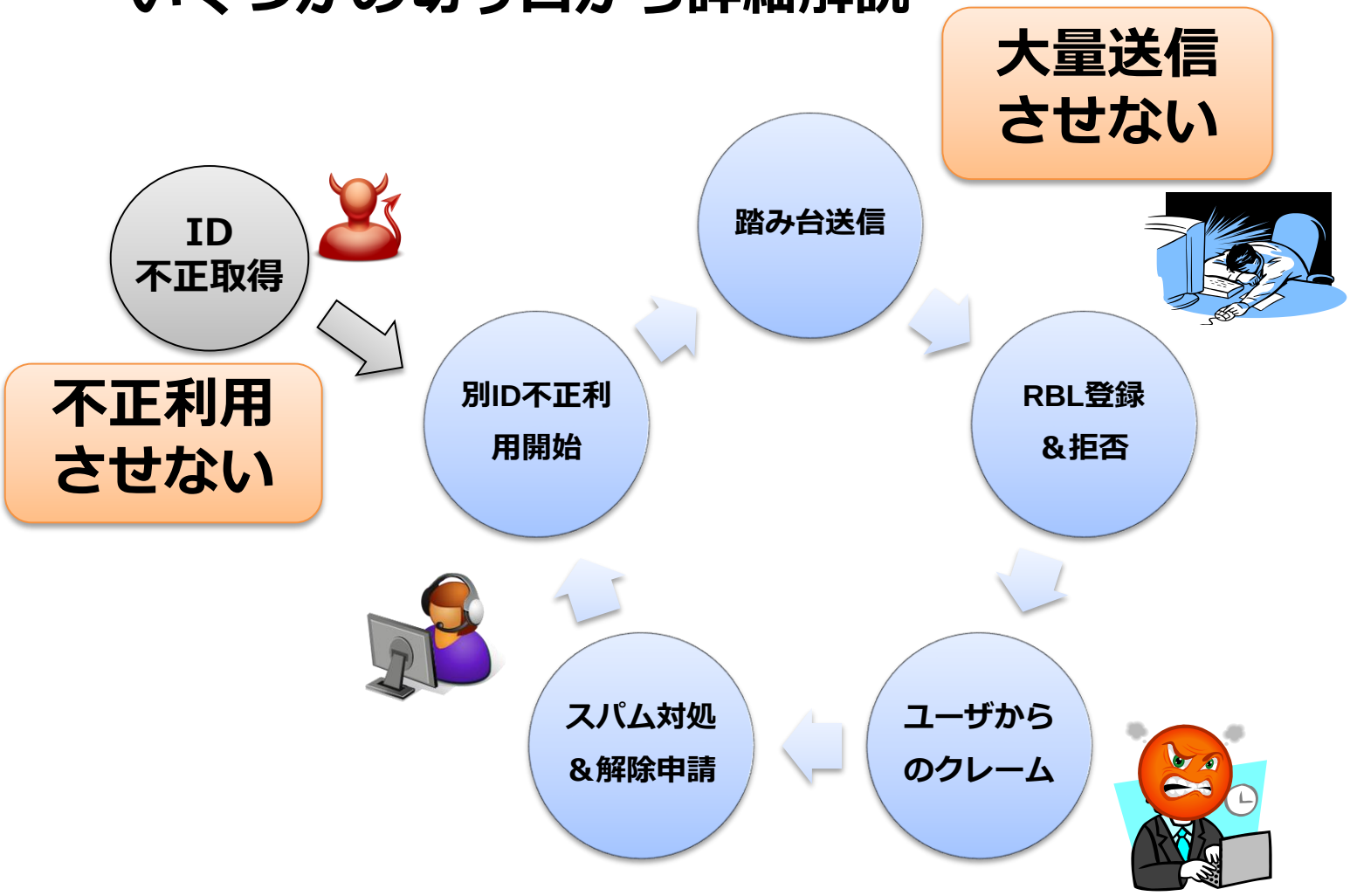
5 **対策の実際と将来的な解決は？**

加瀬　正樹（ニフティ株式会社）

実際の対策

NIFTY Cloud
ニフティクラウド

いくつかの切り口から詳細解説



不正利用させない（マルウェア対策）

NIFTY Cloud
ニフティクラウド

Spammer はどうやってID/PWを入手している？

1. **マルウェア感染**
2. オンライン攻撃
3. 危殆化システム

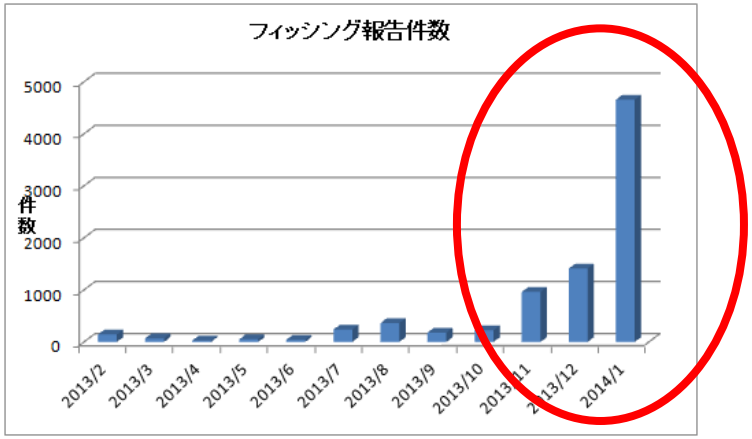


図. フィッシング対策協議会に寄せられたフィッシング報告件数(海外含む)

- ✓ 2013年11月度から報告件数が**急増**
- ✓ 2014年1月度の報告件数(**4,656件**)は昨年の年間件数(**3,803件**)超え

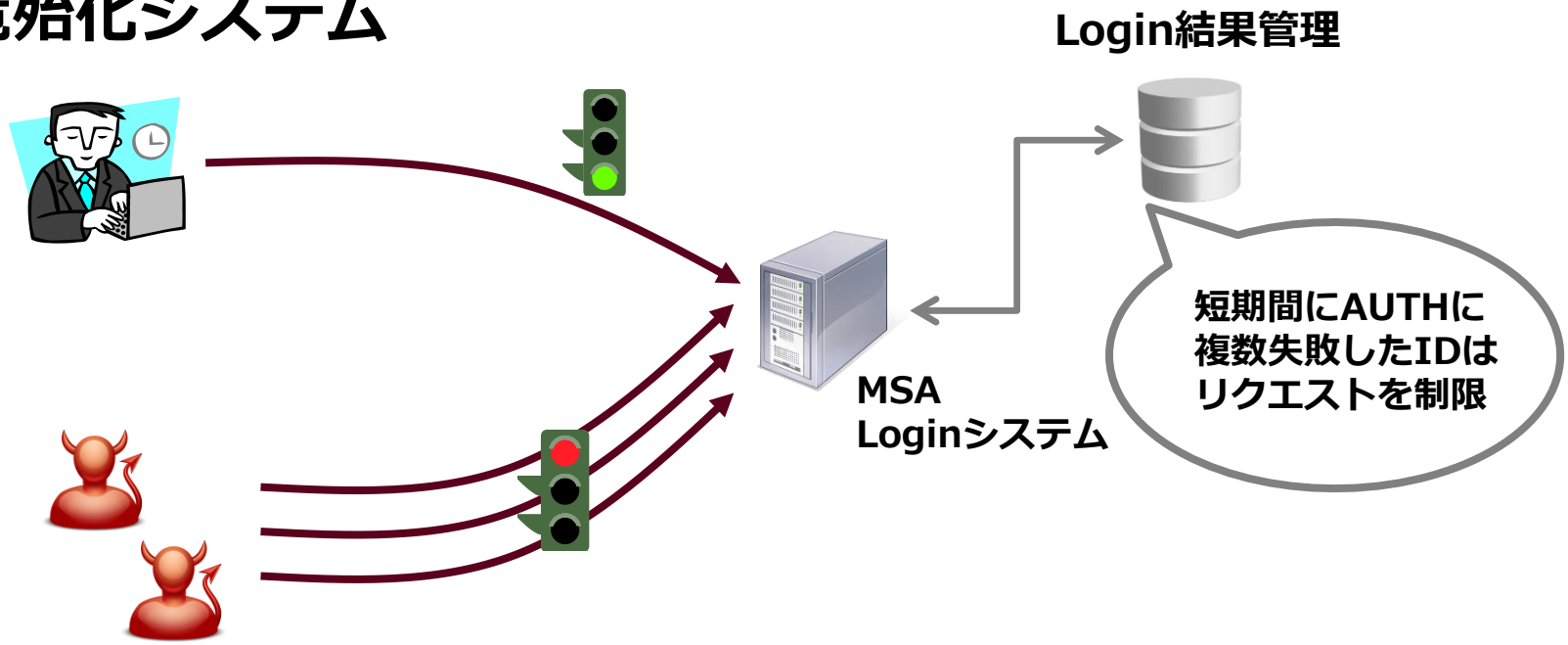
運用者としてできることには限りがある

不正利用させない（オンライン攻撃）

NIFTY Cloud
ニフティクラウド

Spammer はどうやってID/PWを入手している？

1. マルウェア感染
2. オンライン攻撃
3. 危殆化システム



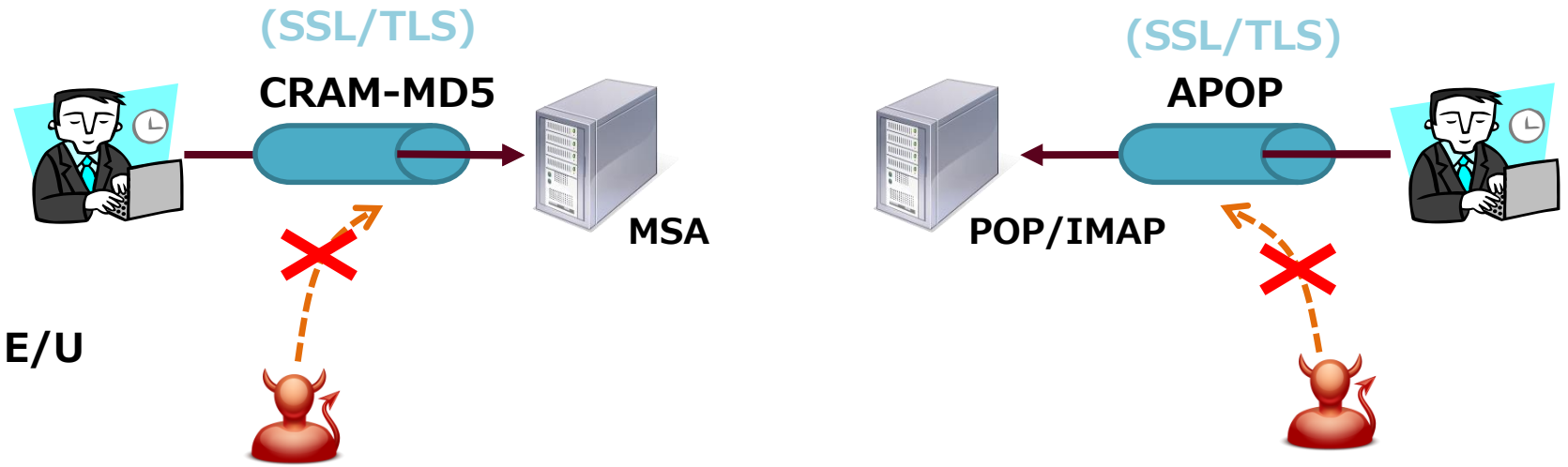
従来対策…最近の傾向では少ない

不正利用させない（危殆化システム）

NIFTY Cloud
ニフティクラウド

Spammer はどうやってID/PWを入手している？

1. マルウェア感染
2. オンライン攻撃
3. **危殆化システム**



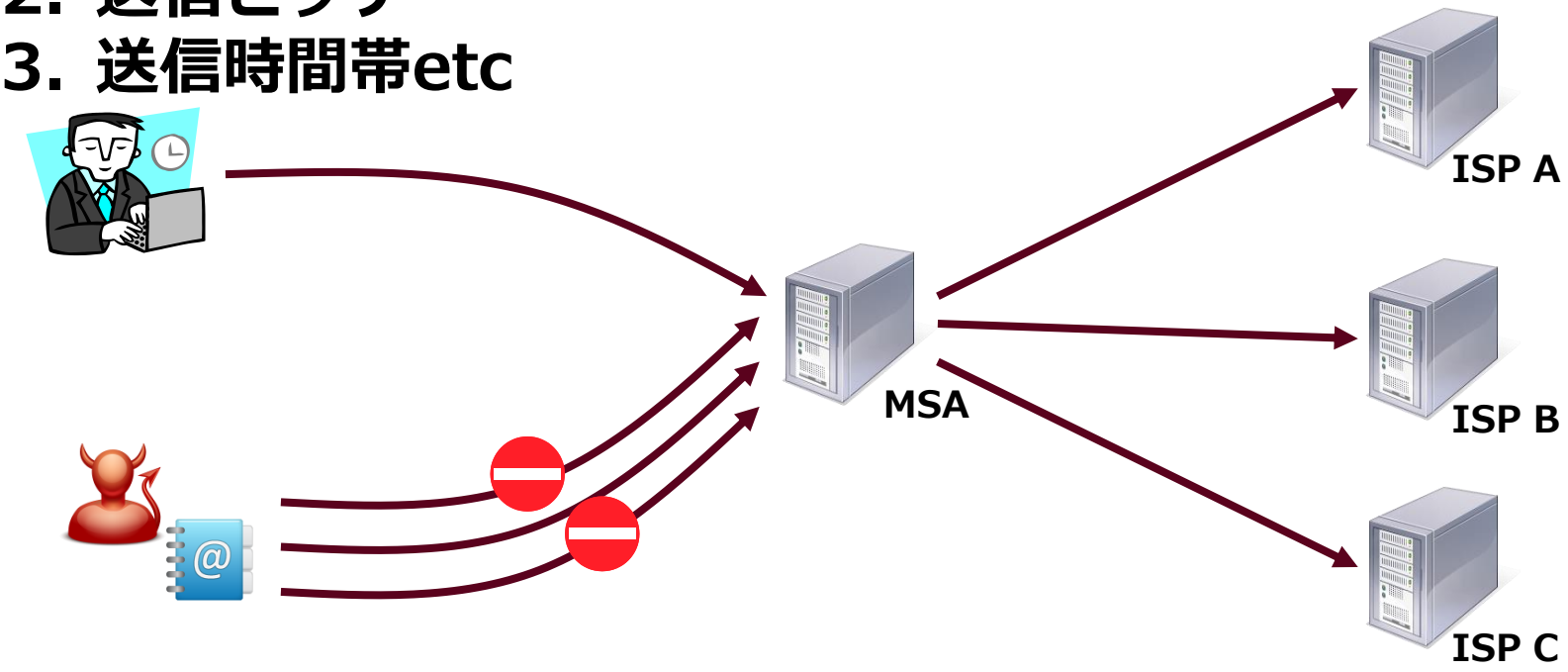
ID/PW盗聴のリスクは極力避けるべき

大量送信させない（発信元制御）

NIFTY Cloud
ニフティクラウド

設備に影響を及ぼす事象が発生した場合に
Spammer の特徴を把握してSMTPでrejectする

1. **接続元IPアドレス**
2. **送信ピッチ**
3. **送信時間帯etc**

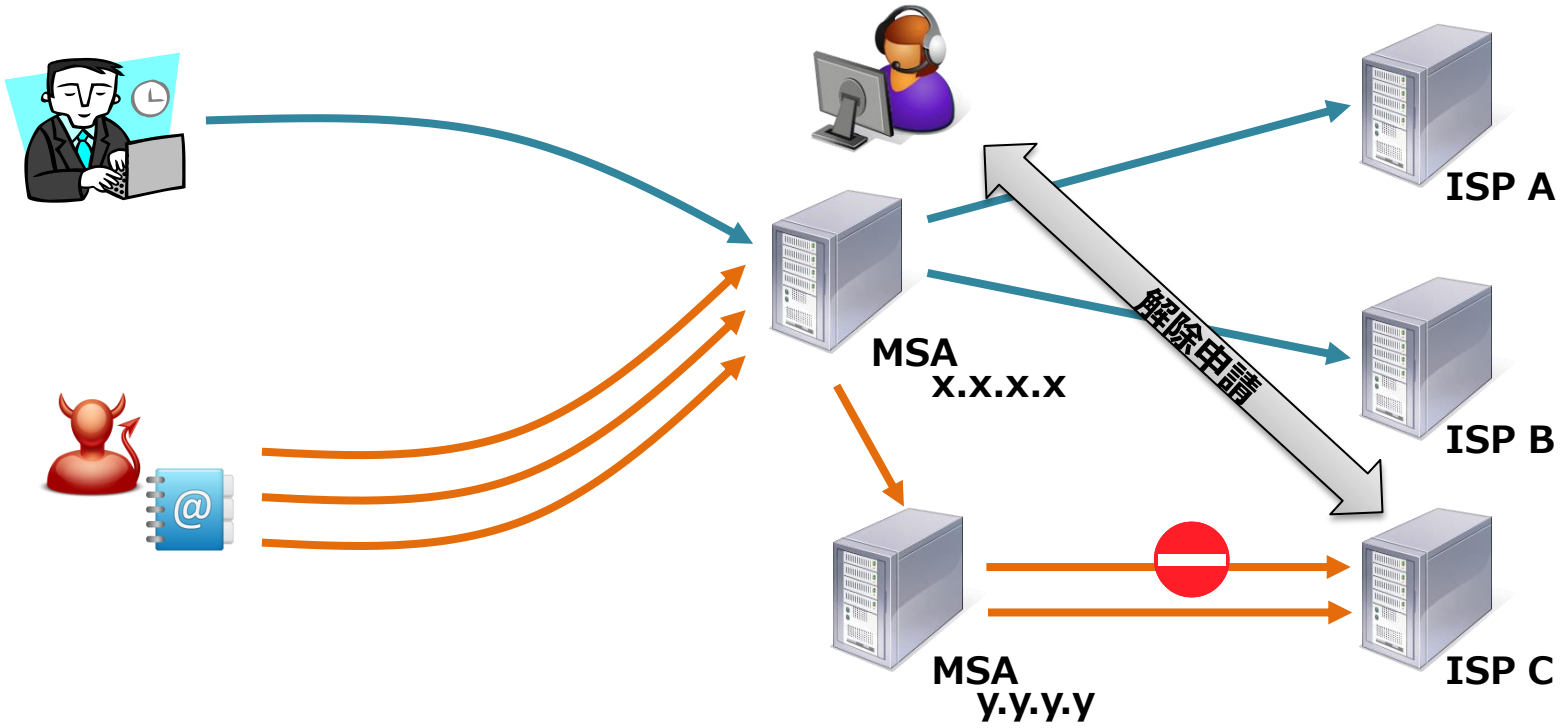


従来対策…基本的にはいたちごっこ

大量送信させない（出口分離）

NIFTY Cloud
ニフティクラウド

宛先によってISP出口サーバ(IPアドレス)を分離する。
ISP発のスパムを出口専用Bulkサーバに集約して、
「お隣さん問題」「RBL解除コスト」を削減する

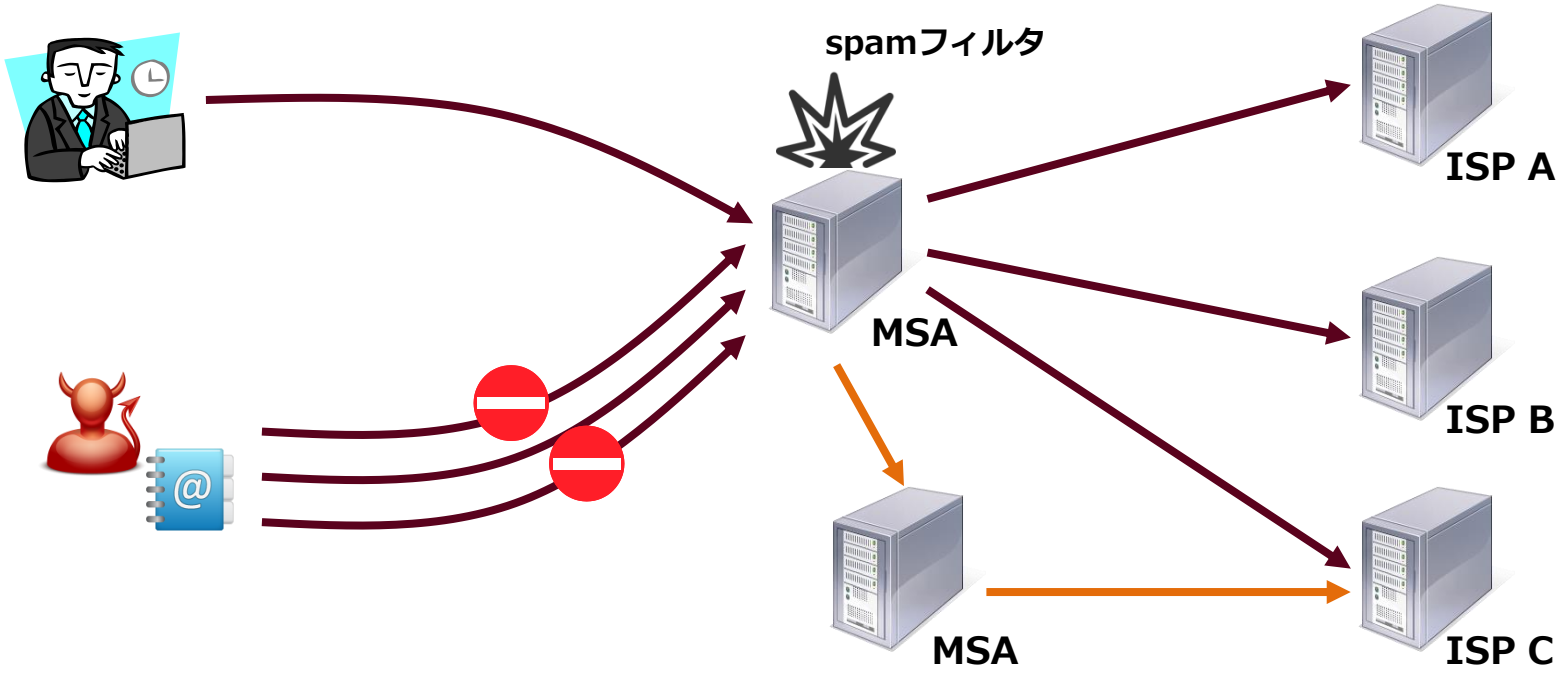


一定の効果があるが、一部ユーザに影響あり

大量送信させない（OutBound Filter）

NIFTY Cloud
ニフティクラウド

(ユーザ同意が前提で)コンテンツフィルタリング実施
reject であったり出口専用Bulkサーバを経由させる



将来的にはrejectに一本化させるべき
SMTP上では解決できない

その他の対策は？

- ワンタイムパスワード／2要素認証
  - 携帯端末での認証
  - クライアント証明書
  - etc
- 原則送信禁止（オプトイン）
  - 海外からの送信禁止（申告制）
  - 少しだけ送信遅延（スマホから承認）

法律面を含めて、業界内で協働していくべき

本セッションのまとめ

NIFTY Cloud
ニフティクラウド

- 今、submission 踏み台問題が悩みの種
- 国内ISPにとって共有課題
- ID/PW入手経路のひとつ「マルウェア感染」
- 送信側対策の一手「OutBound Filter」
- 対策は「不正利用」「大量送信」の観点で検討

ご清聴ありがとうございました