SPF レコードダングリング問題について



株式会社TwoFive

会社概要

TwoFiveは、メールから新時代のメッセージングまで
コミュニケーションのセキュリティ課題に挑むリーディングカンパニーです。

社名	株式会社TwoFive（TwoFive,Inc.）
設立	2014年5月
代表者	末政 延浩
事業内容	● メッセージングテクノロジー ● ITセキュリティ ● モバイルテクノロジー
所在地	本社　〒104-0061 東京都中央区銀座3-10-7　ヒューリック銀座三丁目ビル3F ベトナム支社　TT01-37 Mon City, Ham Nghi, My Dinh 2, Nam Tu Liem, Hanoi, Vietnam
販売パートナー	● 株式会社日立ソリューションズ ● NECソリューションイノベータ株式会社 ● 東芝デジタルソリューションズ 株式会社 ● 株式会社ブロードバンドセキュリティ ● 株式会社インターネットイニシアティブ ● SB C&S株式会社 ● スターネット株式会社 ● 株式会社QTnet ● 株式会社セキュアイノベーション
主要取引銀行	三井住友銀行（プロパー）

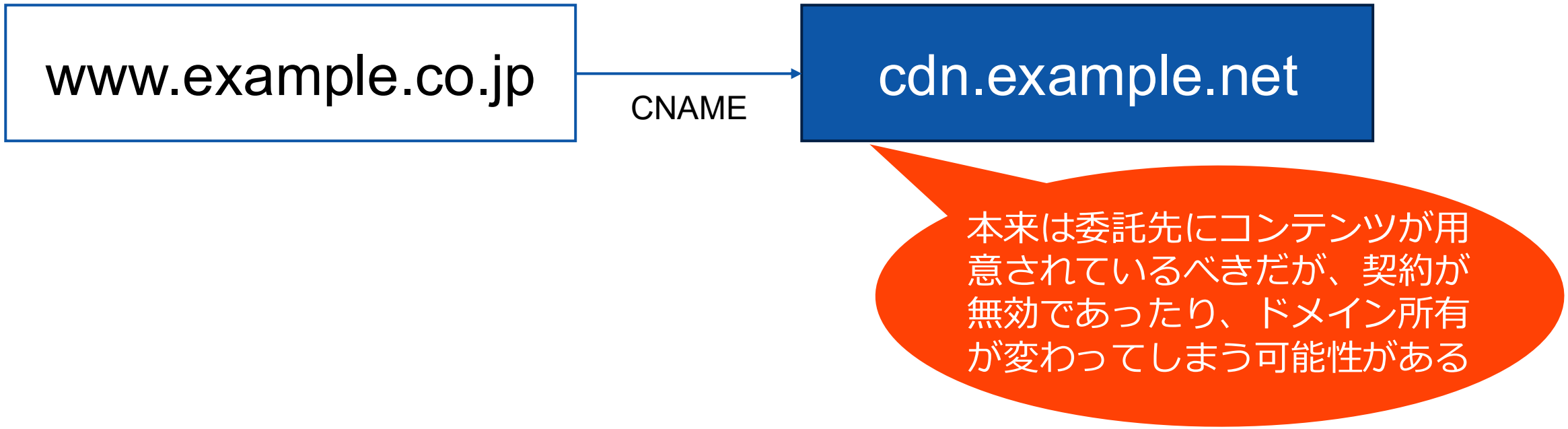
© TWOFIVE ALL RIGHTS RESERVED.

ダングリングレコード



ーダングリングレコード(dangling record)

ダングリングレコードとは（中略）指定された名前の実体が無効になっている
リソースレコードを示す用語として使われることがあります（図1）。
danglingは「宙ぶらりんの」を意味しています。



https://jprs.jp/glossary/index.php?ID=0274

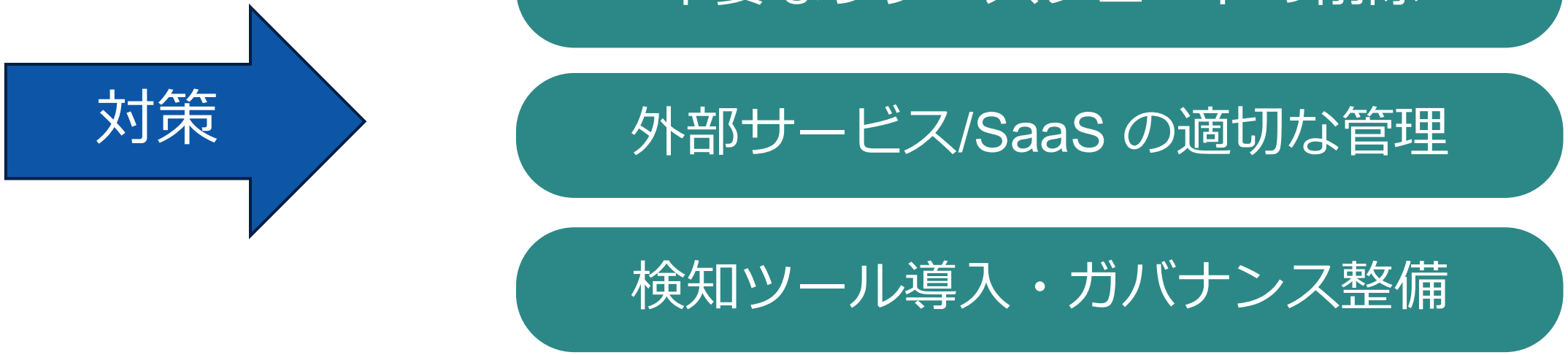
© TWOFIVE ALL RIGHTS RESERVED.

ーダングリングレコード(dangling record)のリスクと対策

代表的なダングリングレコードのリスクとしては、

- **サブドメインの乗っ取り（Subdomain Takeover）**
- **悪意あるコンテンツの配信**

が考えられる。



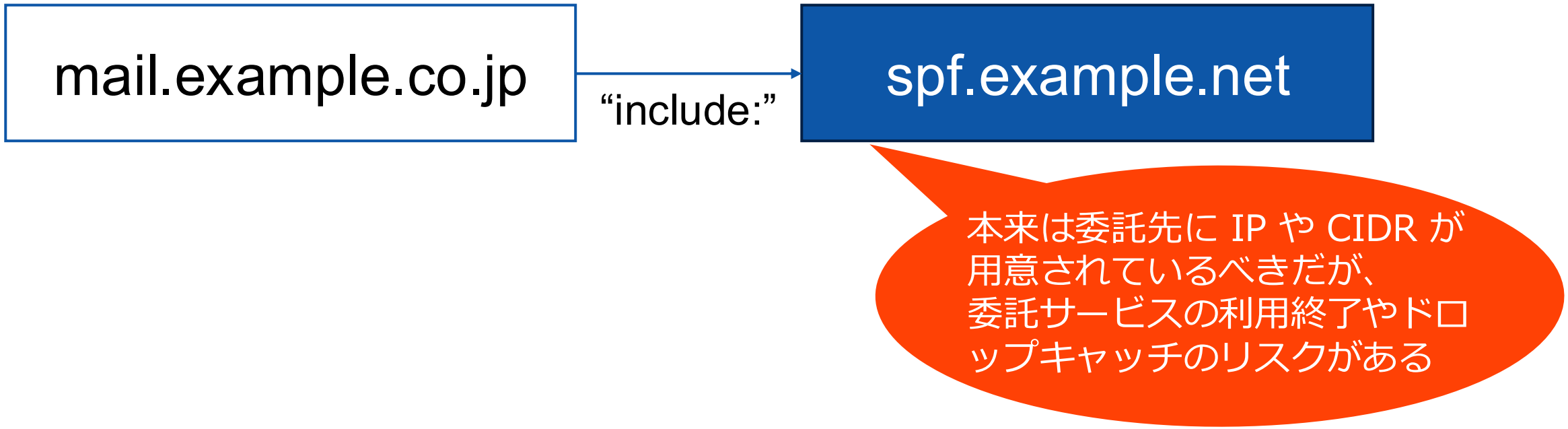
© TWOFIVE ALL RIGHTS RESERVED.

SPFレコードダングリング



ー SPF レコードダングリング

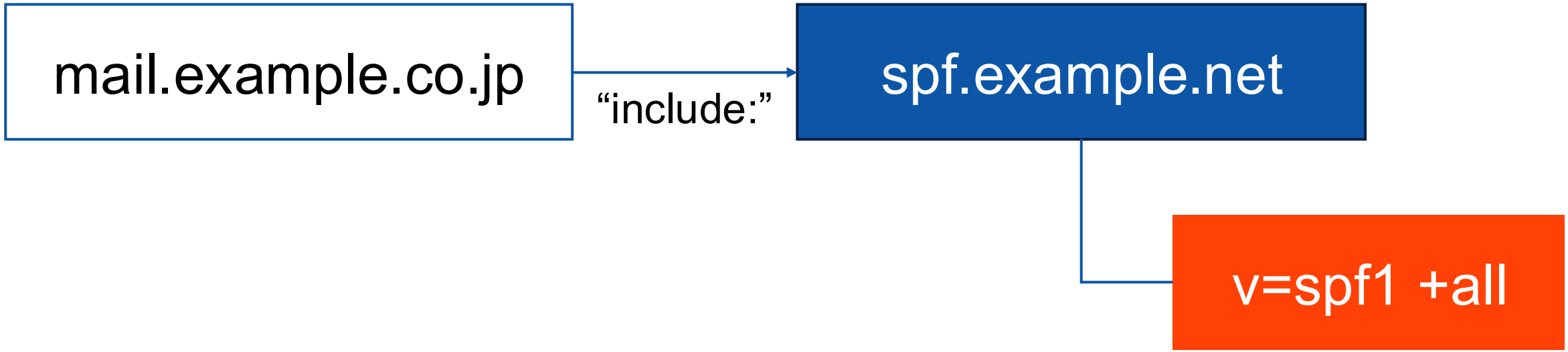
メール送信を外部委託/SaaS利用している場合、”include:” や “redirect=“ を使って、送信許可設定を DNS TXT レコードに記述していますが、指定された名前の実態が無効・乗っ取られるリスクがある。



© TWOFIVE ALL RIGHTS RESERVED.

ー SPF レコードダングリング

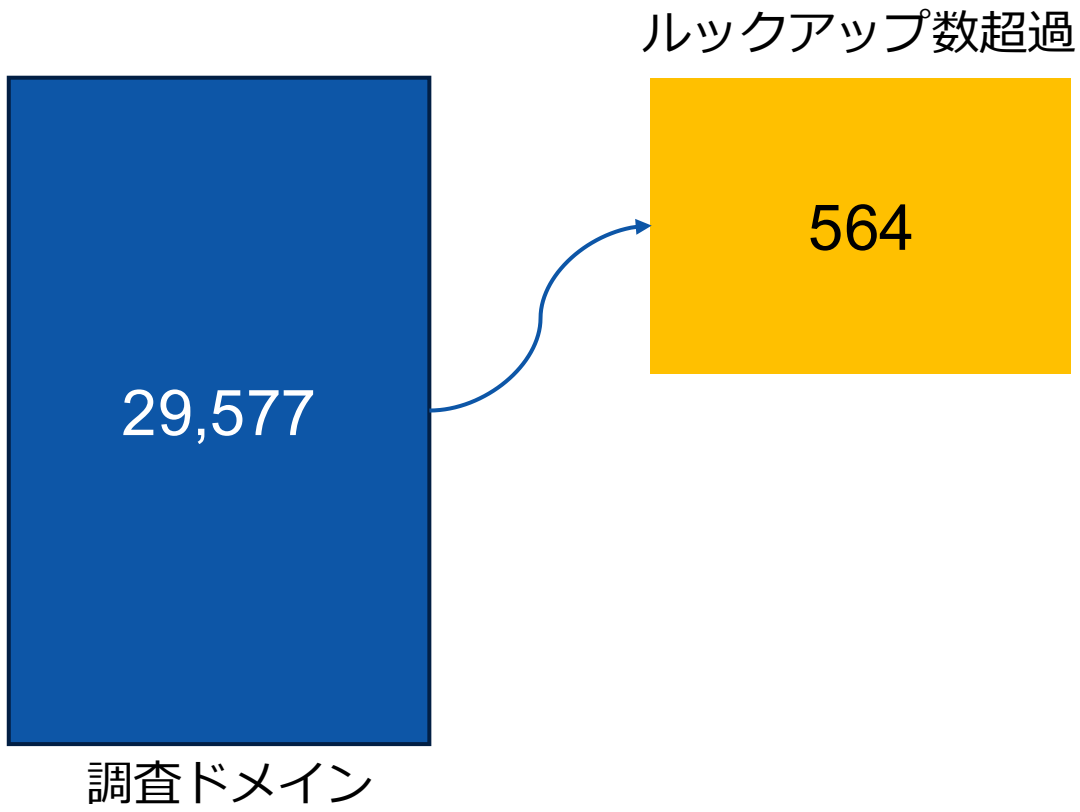
メール送信を外部委託/SaaS利用している場合、”include:” や “redirect=“ を使って、送信許可設定を DNS TXT レコードに記述していますが、指定された名前の実態が無効・乗っ取られるリスクがある。



© TWOFIVE ALL RIGHTS RESERVED.

ー SPF レコードダングリング実態調査

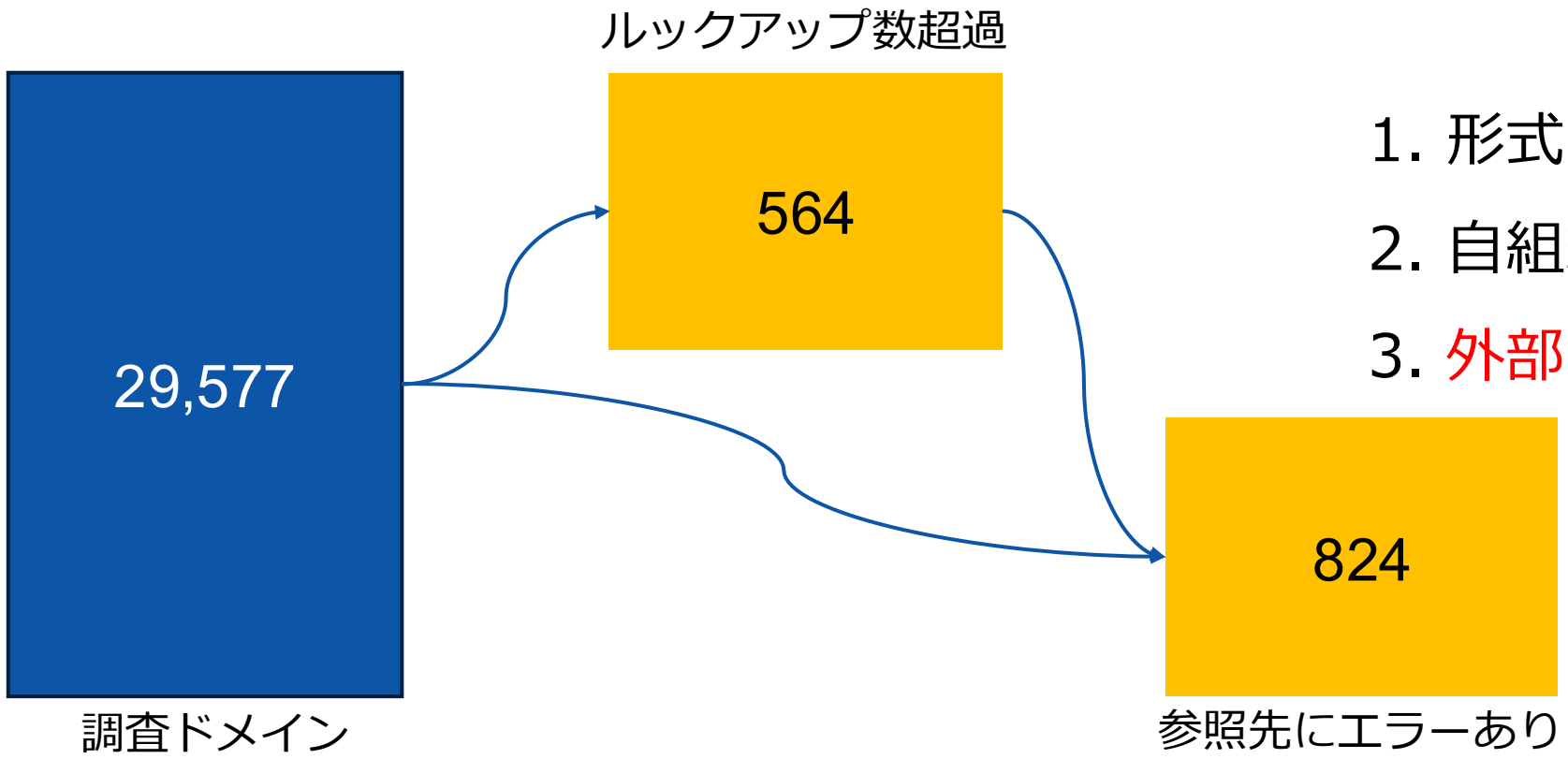
TwoFive が実際にメールドメインとして把握している 29,577 ドメインについて調査。ルックアップ数超過は 564 ドメイン（1.9 %）。



© TWOFIVE ALL RIGHTS RESERVED.

ー SPF レコードダングリング実態調査

TwoFive が実際にメールドメインとして把握している 29,577 ドメインについて調査。参照先エラーありは 824 ドメイン（2.8 %）。

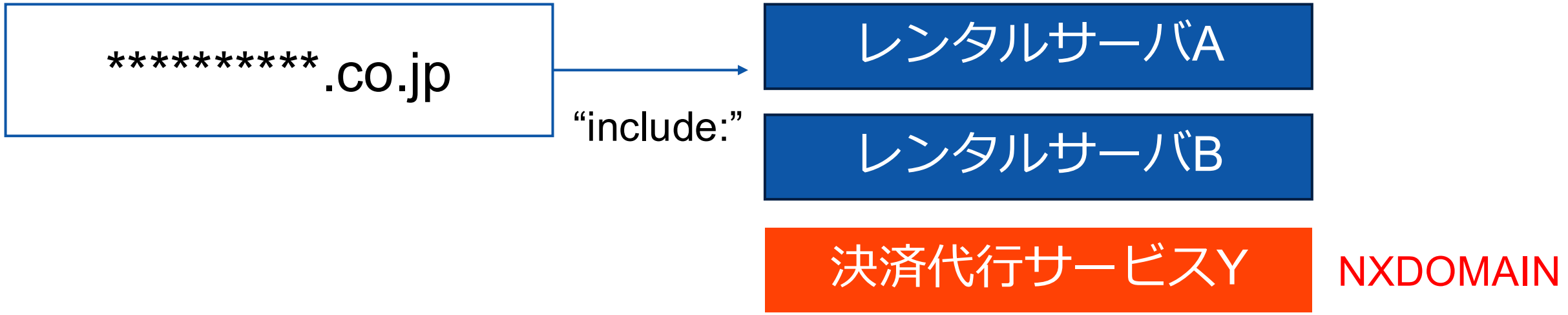


1. 形式エラー
2. 自組織ドメイン NXDOMAIN
3. 外部ドメイン NXDOMAIN

© TWOFIVE ALL RIGHTS RESERVED.

ー SPF レコードダングリング実態調査 – 例1

国内メールドメインで決済代行サービス（稼働中）を利用しているが、SPF レコードの FQDN タイポになっている。

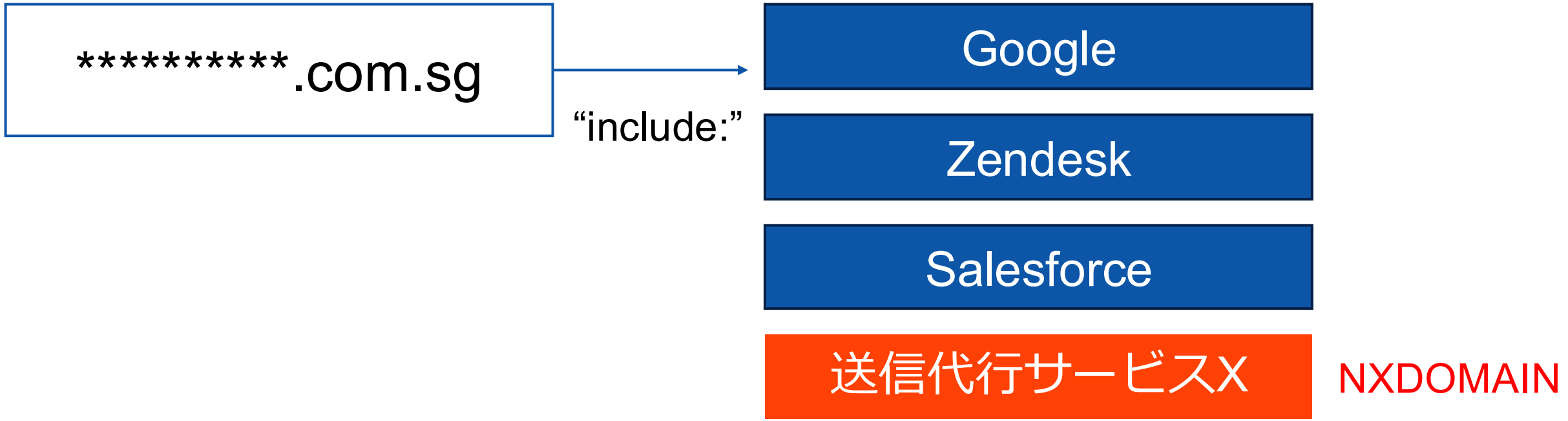


※おそらくは “spf.ドメインY” を “_spf.ドメインY” で誤って指定

© TWOFIVE ALL RIGHTS RESERVED.

ー SPF レコードダングリング実態調査 – 例2

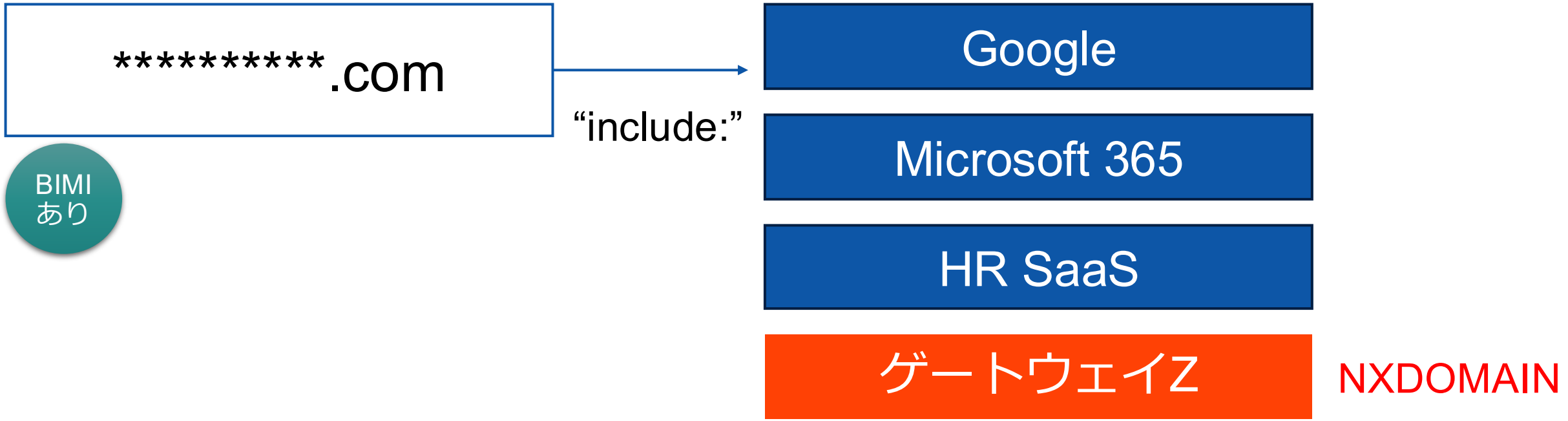
海外メールドメインで送信代行サービス（稼働中）を利用しているが、SPF レコードの FQDN が古くて NXDOMAIN になっている。



© TWOFIVE ALL RIGHTS RESERVED.

ー SPF レコードダングリング実態調査 – 例3

海外メールドメインで、ゲートウェイサービスの指定 SPF レコードが含まれているが、契約終了のため SPF レコードは NXDOMAIN になっている。

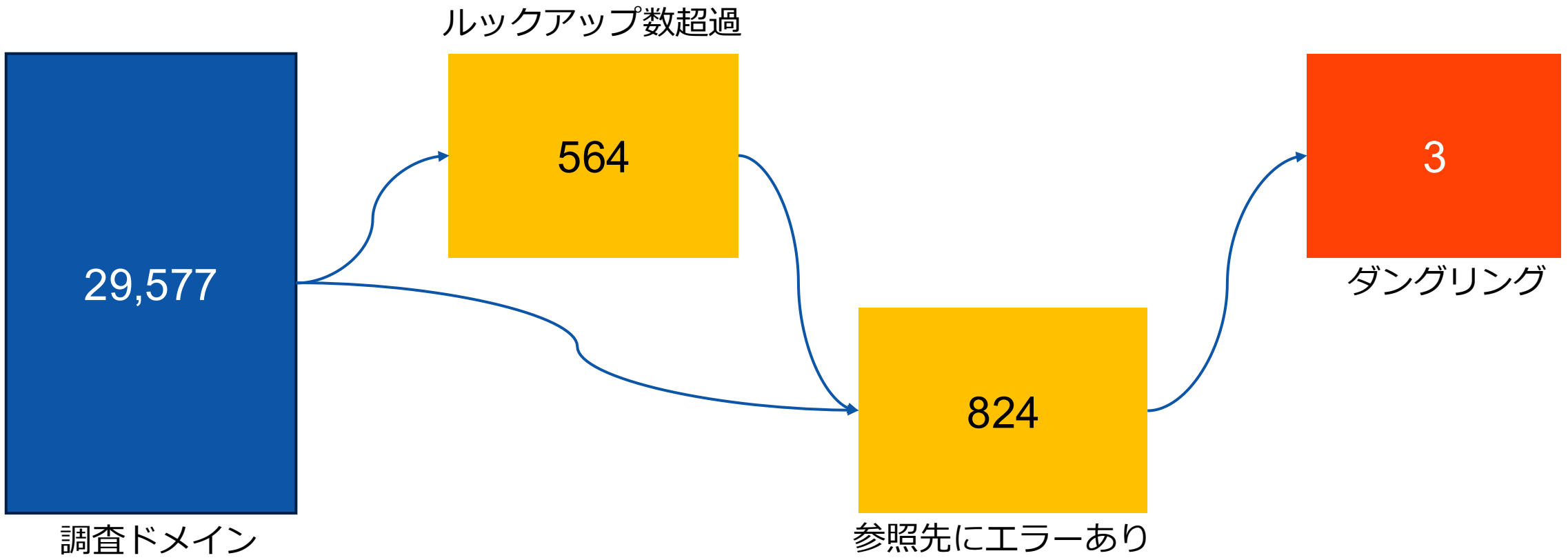


※ ゲートウェイZ は顧客ユニークな SPF レコードを提供している

© TWOFIVE ALL RIGHTS RESERVED.

ー SPF レコードダングリング実態調査

TwoFive が実際にメールドメインとして把握している 29,577 ドメインについて調査。「+all」がどこかに含まれるケースは 3 ドメイン（0.01 %）。



© TWOFIVE ALL RIGHTS RESERVED.

ー SPF レコードダングリングの対策

SPF レコードに外部ドメインを include: や redirect= している場合は、外部要因によってなりすましの顕在化が考えられ、普段から注意が必要です。
以下のような対策を検討してみてください。

対策

- メール送信の委託先の適切な管理
- SPF レコードの定期チェック
- 自社ドメインのドロップキャッチ対策

© TWOFIVE ALL RIGHTS RESERVED.

サービスに関するご相談や
ご不明点がございましたら、
お気軽にお問い合わせください。

当社HP	https://www.twofive25.com/
お問い合わせフォーム	https://www.twofive25.com/contact/

