NA4Sec
Network Analytics for Security

ホスティングサービスの危険な同居人

NTT docomo Business

2026年1月23日
NTTドコモビジネス株式会社

スピーカー紹介

TLP:CLEAR
つなごう。驚きを。幸せを。

NA4Sec Network Analytics for Security

NTT docomo Business

NTTセキュリティ・ジャパン

戸祭 隆行　プロフェッショナルサービス部　インシデントレスポンスチーム

セキュリティ技術研究・開発（攻撃インフラの脅威分析）
インシデントレスポンスに従事

NTTドコモビジネス

冨樫 良介　イノベーションセンター

セキュリティ技術研究・開発（攻撃インフラの脅威分析）

本講演の狙い

TLP:CLEAR

つなごう。驚きを。幸せを。

NA4Sec Network Analytics for Security

docomo Business

レンタルサーバサービスは、物理的なリソース準備の手間がかからず、手軽に利用できることから、多くの企業や個人がウェブサイトやメール運用に使っています。

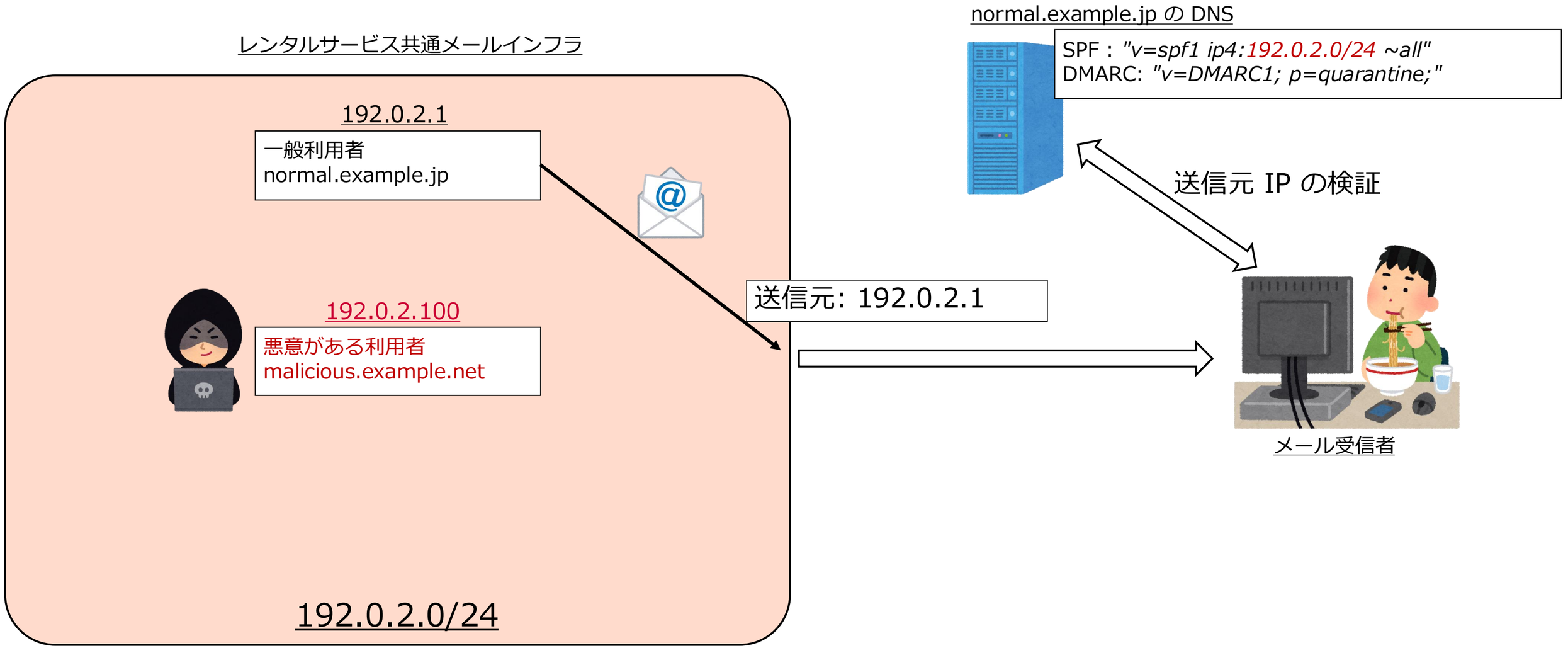
一方で、多数の利用者がリソースを共有するためセキュリティの担保が難しくなる場合も存在します。

今回は、レンタルサーバのメールサービスにスポットを当てて、そこに潜むセキュリティリスクとレンタルサーバならではの悩ましい事情との関係性について紹介します。

レンタルサーバの共通インフラ

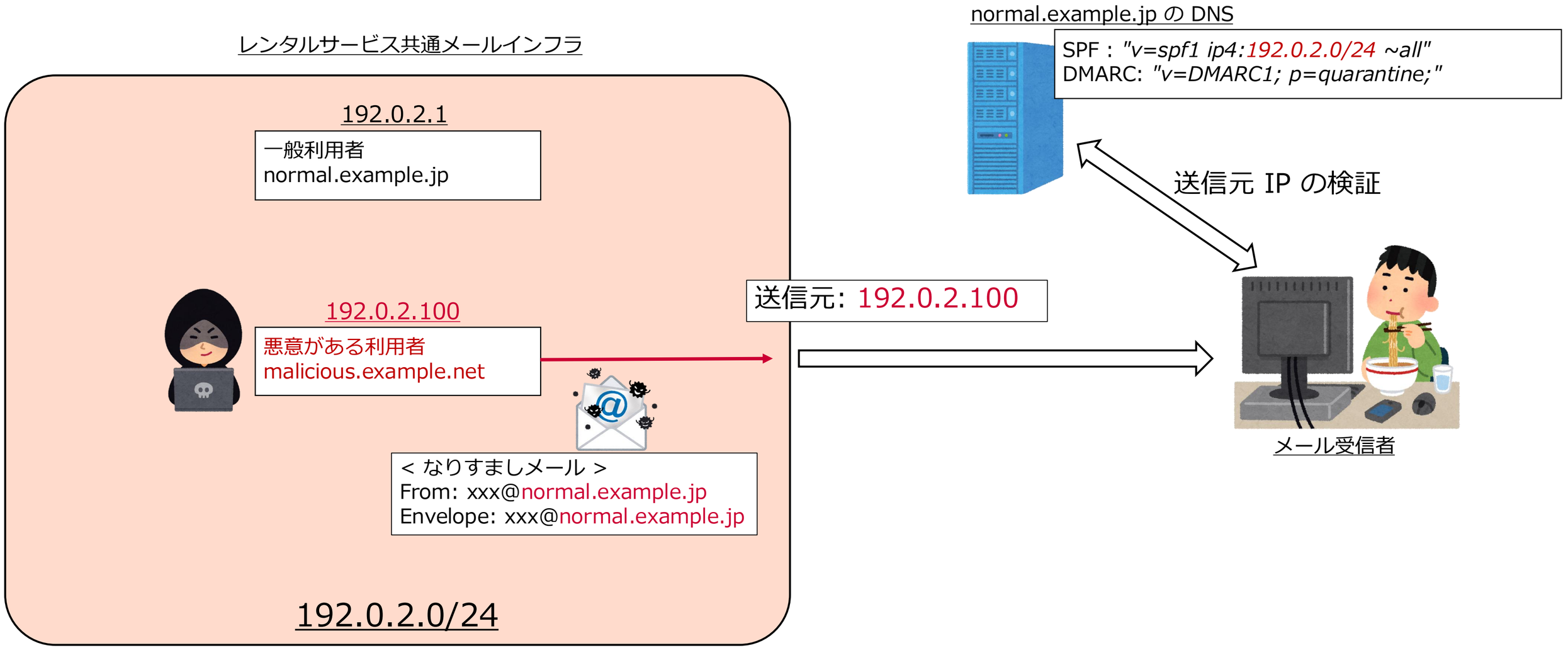
TLP:CLEAR

- レンタルサーバはその性質上、IPアドレスが利用者間で共有される
- IPアドレスが共有されるため、送信元IPアドレスを認証するSPFとは相性が悪い



レンタルサーバの共通インフラ

- レンタルサーバはその性質上、IPアドレスが利用者間で共有される
- IPアドレスが共有されるため、送信元IPアドレスを認証するSPFとは相性が悪い



レンタルサーバの共通インフラ

TLP:CLEAR

つなごう。驚きを。幸せを。

- レンタルサーバはその性質上、IPアドレスが利用者間で共有される
- IPアドレスが共有されるため、送信元IPアドレスを認証するSPFとは相性が悪い

レンタルサービス共通メールインフラ

192.0.2.1

一般利用者
normal.example.jp

192.0.2.100

悪意がある利用者
malicious.example.net

< なりすましメール >
From: xxx@normal.example.jp
Envelope: xxx@normal.example.jp

192.0.2.0/24

送信元: 192.0.2.100

normal.example.jp の DNS

SPF : *"v=spf1 ip4:192.0.2.0/24 ~all"*
DMARC: *"v=DMARC1; p=quarantine;"*

**送信元ドメイン名を偽装されると、
「なりすましメール」もSPFの許可IPレンジに
含まれるためSPF/DMARCでは見分けがつかない**

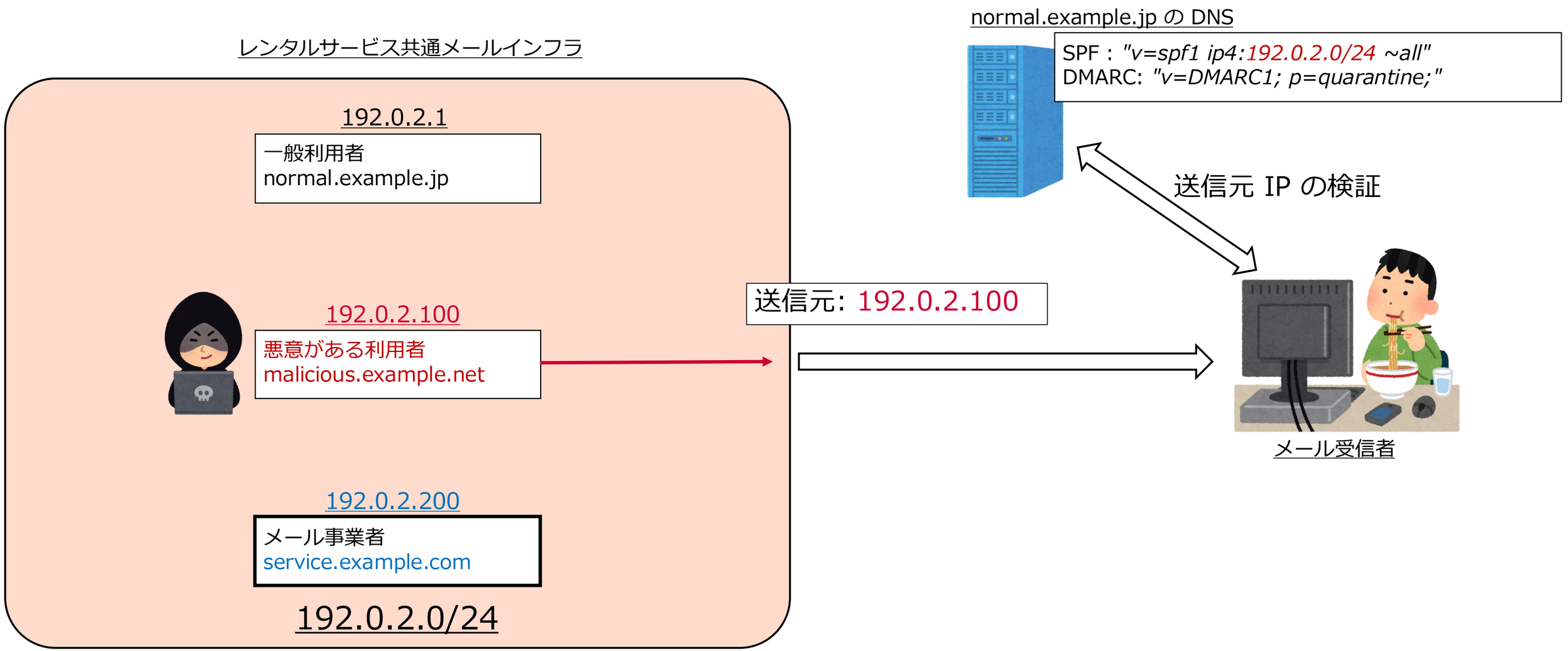
メール受信者

レンタルサーバの共通インフラ

TLP:CLEAR

つなごう。驚きを。幸せを。

- コスト面の観点などから、事業者は必ずしもメールインフラを利用者と分割できない

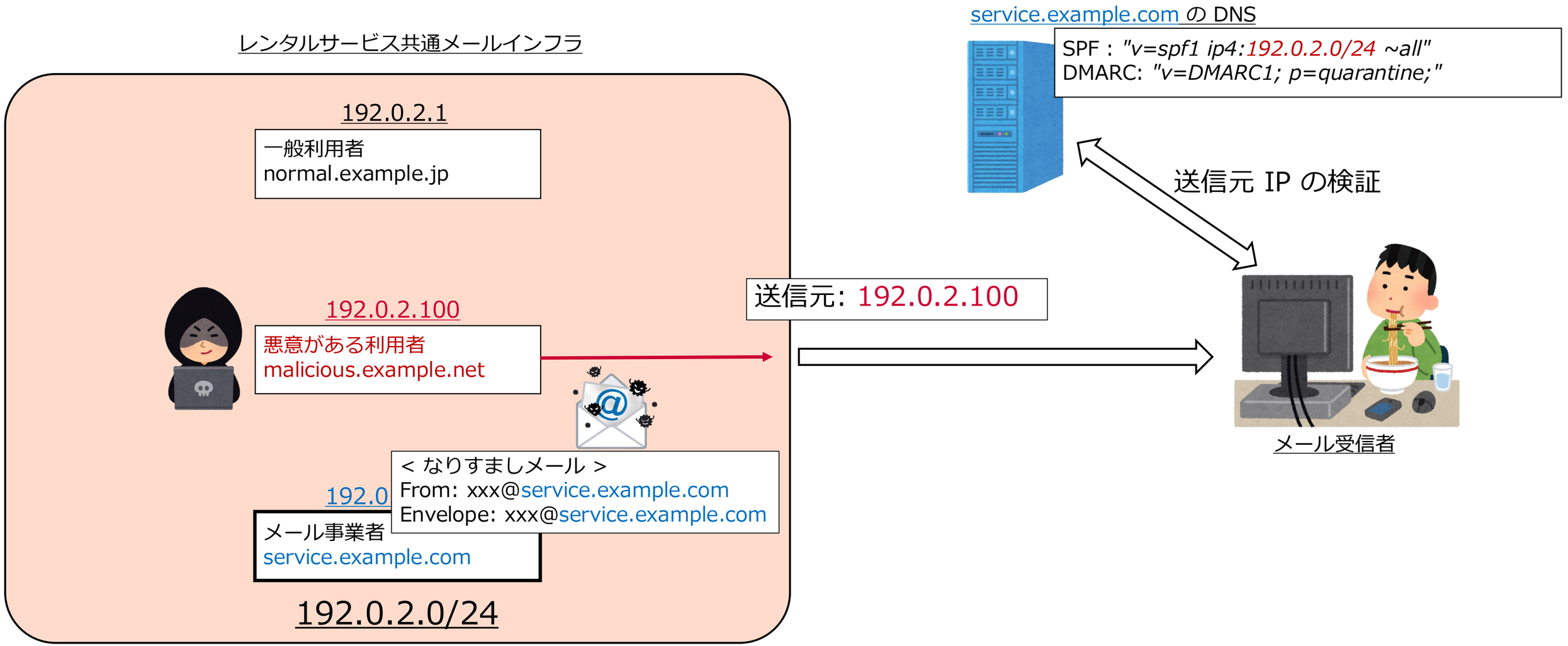


レンタルサーバの共通インフラ

TLP:CLEAR

つなごう。驚きを。幸せを。

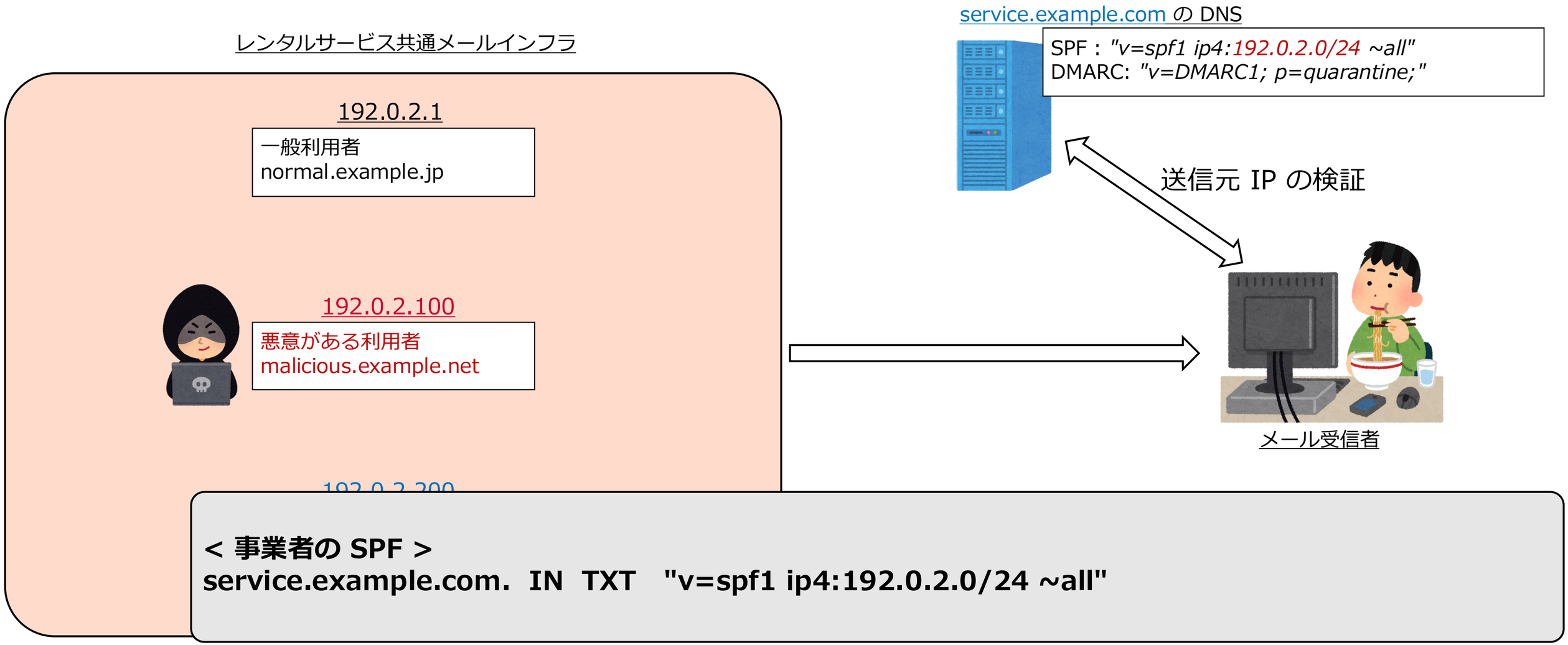
- 事業者と攻撃者のメールインフラが共通の場合、攻撃者は事業者を騙る可能性



利用者と事業者のSPFレコードを比較

TLP:CLEAR

- レンタルサービスのインフラを外部から把握することは難しい
- しかし、利用者と事業者のメールドメインのSPFを比較することは有効



利用者と事業者のSPFレコードを比較

TLP:CLEAR

- 利用者のSPFレコードを確認することで、送信元に使用される可能性があるIPアドレスを確認できる
- 事業者と重複がある場合、本件のリスクに該当するといえる

service.example.com の DNS

SPF：*"v=spf1 ip4:192.0.2.0/24 ~all"*
DMARC: *"v=DMARC1; p=quarantine;"*

レンタルサービス共通メールインフラ

192.0.2.1

一般利用者
normal.example.jp

送信元 IP の検証

< 利用者の SPF >
malicious.example.net. IN TXT "v=spf1 +a:spf.example.com +a:malicious.example.net ~all
malicious.example.net. IN A 192.0.2.100

→ 利用者の送信元 IP (候補) が事業者のSPFに許可されている

メール受信者

192.0.2.200

< 事業者の SPF >
service.example.com. IN TXT "v=spf1 ip4:192.0.2.0/24 ~all"

SPFレコード比較事例

TLP:CLEAR

つなごう。驚きを。幸せを。

NA4Sec Network Analytics for Security

NTT docomo Business

- 複数のレンタルサーバ事業者の SPF レコードを突合

< 事業者 A >
example.jp. IN TXT "v=spf1 ip4:192.0.2.0/24 include:mail-publisher.example.org ~all"

< 事業者 A 利用者 >
customer.example.net. IN TXT "v=spf1 ip4:192.0.2.0/24 ~all"

- **利用者は事業者側と完全に一致した 192.0.2.0/24 からメールを送信すると思われ、これは事業者側の SPF で許可されているためなりすましできる可能性がある**

< 事業者 B >
example.jp. IN TXT "v=spf1 ip4:192.0.2.0/24 ip4:198.51.100.0/24 ~all"

< 事業者 B 利用者 >
customer.example.net. IN TXT "v=spf1 a:customer.example.net ~all"
customer.example.net. IN A 203.0.113.1

- **利用者は自身の A レコードに紐づく IP アドレスからのメール送信しか許可されておらず、これは事業者の SPF と完全に分離されているため、なりすましはできないと思われる**

今後の展望

TLP:CLEAR
つなごう。驚きを。幸せを。

NA4Sec Network Analytics for Security

docomo Business

- ツールによる大規模な実態調査を計画中
  - 事業者の SPF レコードに紐づく IP アドレスを探索し、顧客が利用している IP アドレスが存在するか確認
  - 存在した場合、顧客の SPF レコードと事業者の SPF レコードを突合させて、今回紹介したなりすましが可能か判定

- SPF の認証をパスできたとしても、実際には Postfix の身元詐称防止機能などで防止できるのか検証
- 状態を精査に確認したのち、可能なら事業者と情報共有