JP AAWG Japan Anti-Abuse Working Group

M3AAWG ドキュメント解説 ~ DNS Abuse ~

株式会社TwoFive

加瀬 正樹

参照ドキュメント

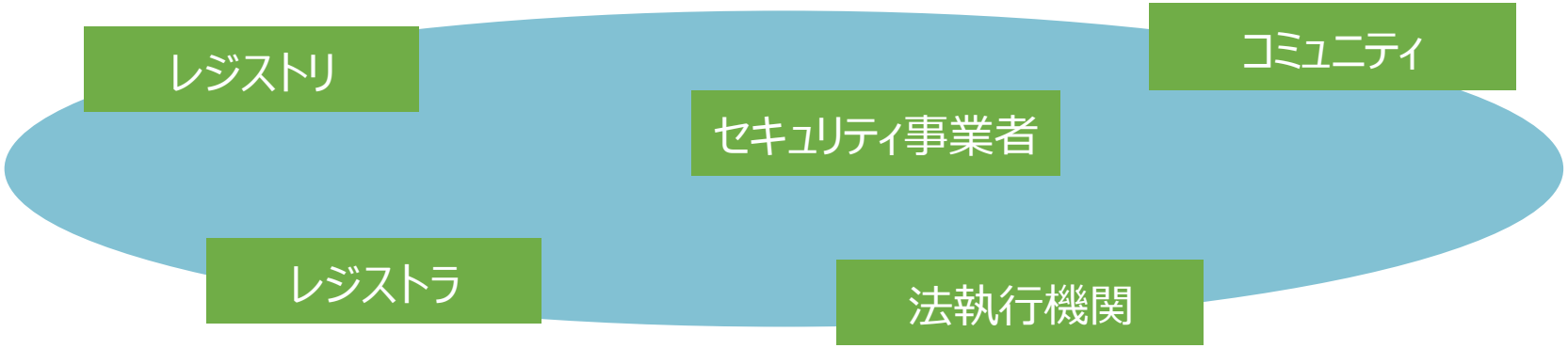
- https://www.m3aawg.org/sites/default/files/doc_files/dns_abuse_prevention_remediation_and_mitigation_practices_for_registrars_and_registries.pdf

- 2024年1月に公開したもので、レジストリやレジストラが DNS Abuse（ドメイン名を悪用した攻撃）に対してどのように予防・緩和・是正を行うべきかをまとめたベストプラクティス集です

- 公開後の ICANN での情報が反映されていない場合があります

DNS Abuse とは

- ICANN 定義は4つ
  - Malware: マルウェア配布
  - Botnet: C&C やボットネット
  - Phishing: フィッシング
  - Pharming: DNS 改竄による誘導
  - （Spam も場合によっては含まれる）
- DNS Abuse への対応は「ドメイン停止ありき」ではない
- 十分な証拠を確認し、被害とのバランスを取った上での適切な対策



Prevention (予防)

- 攻撃者がアカウント作成すること
- 攻撃者がドメインを登録すること
- 攻撃者がドメインを乗っ取ること

Prevention (予防)

- 攻撃者がアカウント作成すること
  - 名前、メールアドレス、電話番号、住所を検証する
  - 構文検証、実在確認、本人確認（通報や法執行には重要！）
- 攻撃者がドメインを登録すること
- 攻撃者がドメインを乗っ取ること

Prevention (予防)

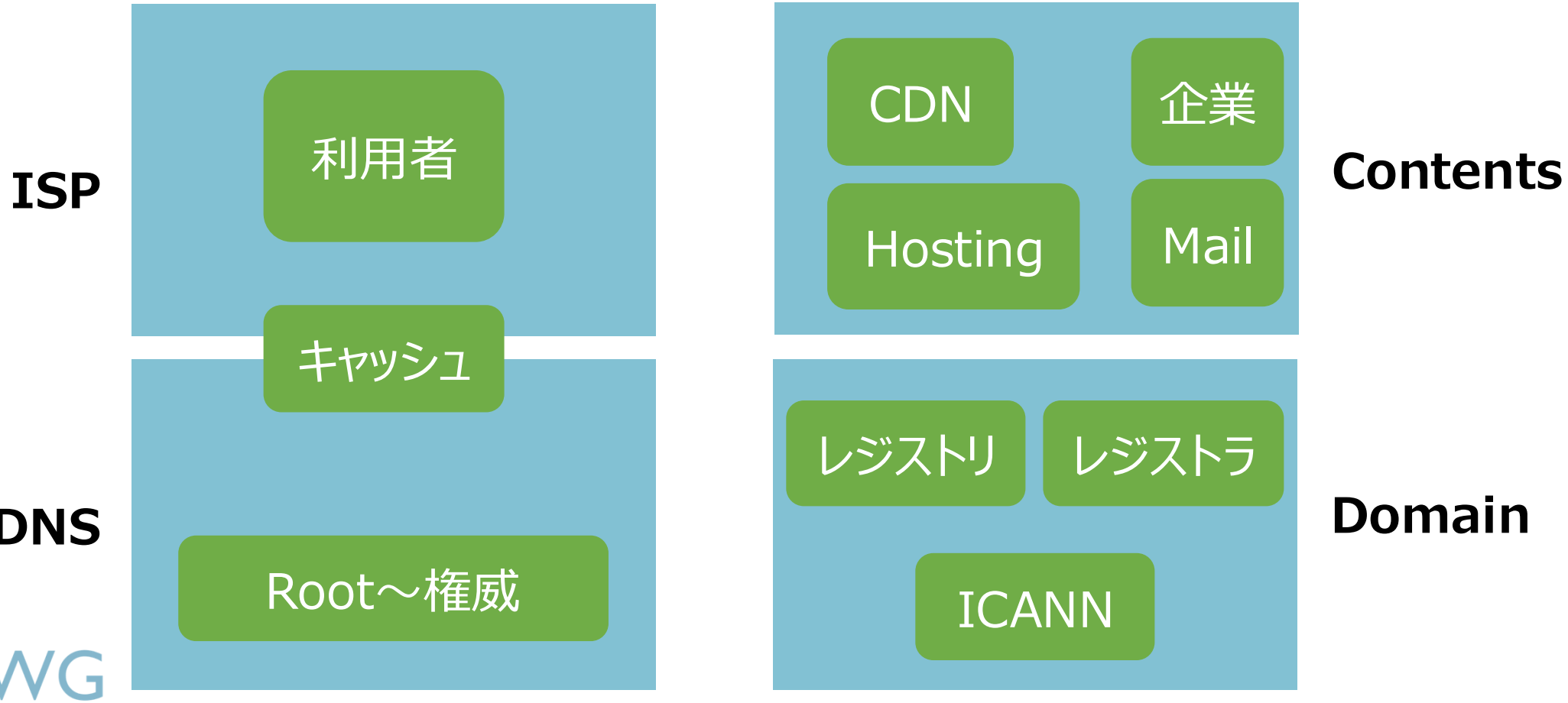
- 攻撃者がアカウント作成すること
- 攻撃者がドメインを登録すること
  - 加えて、ある種のレピュテーションを活用する
  - VPN からの接続か、地理情報が一致するか、大量登録か、etc
  - DGA（ドメイン生成アルゴリズム）への予防策を講じる
- 攻撃者がドメインを乗っ取ること

Prevention (予防)

- 攻撃者がアカウント作成すること
- 攻撃者がドメインを登録すること
- 攻撃者がドメインを乗っ取ること
  - アカウント自体の MFA やアクセスログの監視で予防する
  - 連絡先など設定変更などの通知を有効にする
  - DNS レコードの変化や CTlog を監視する

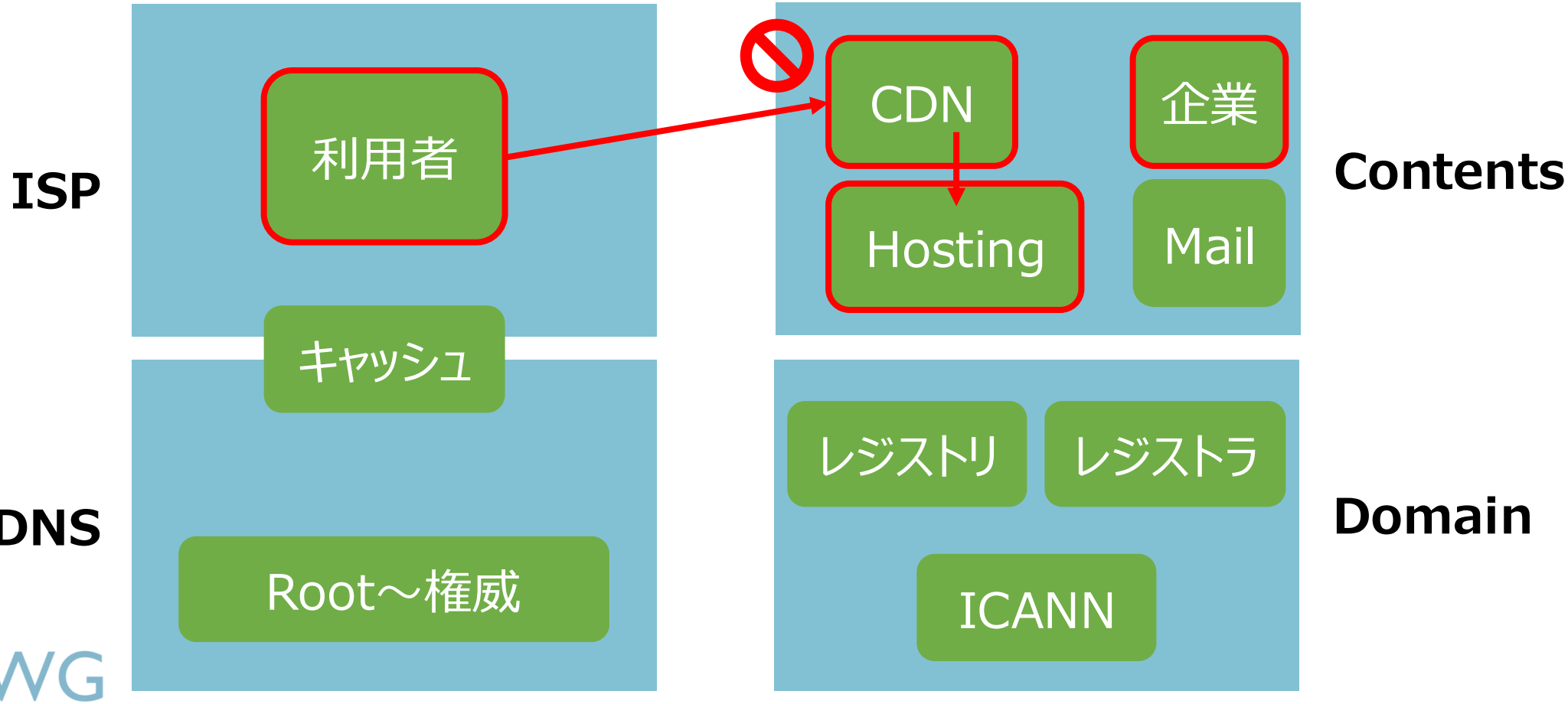
Mitigation (被害軽減)

- 多くの仲介者がいることを念頭に置く
- 不正の種類、深刻度、有効性、速さ、精度、比例性、コストで判断



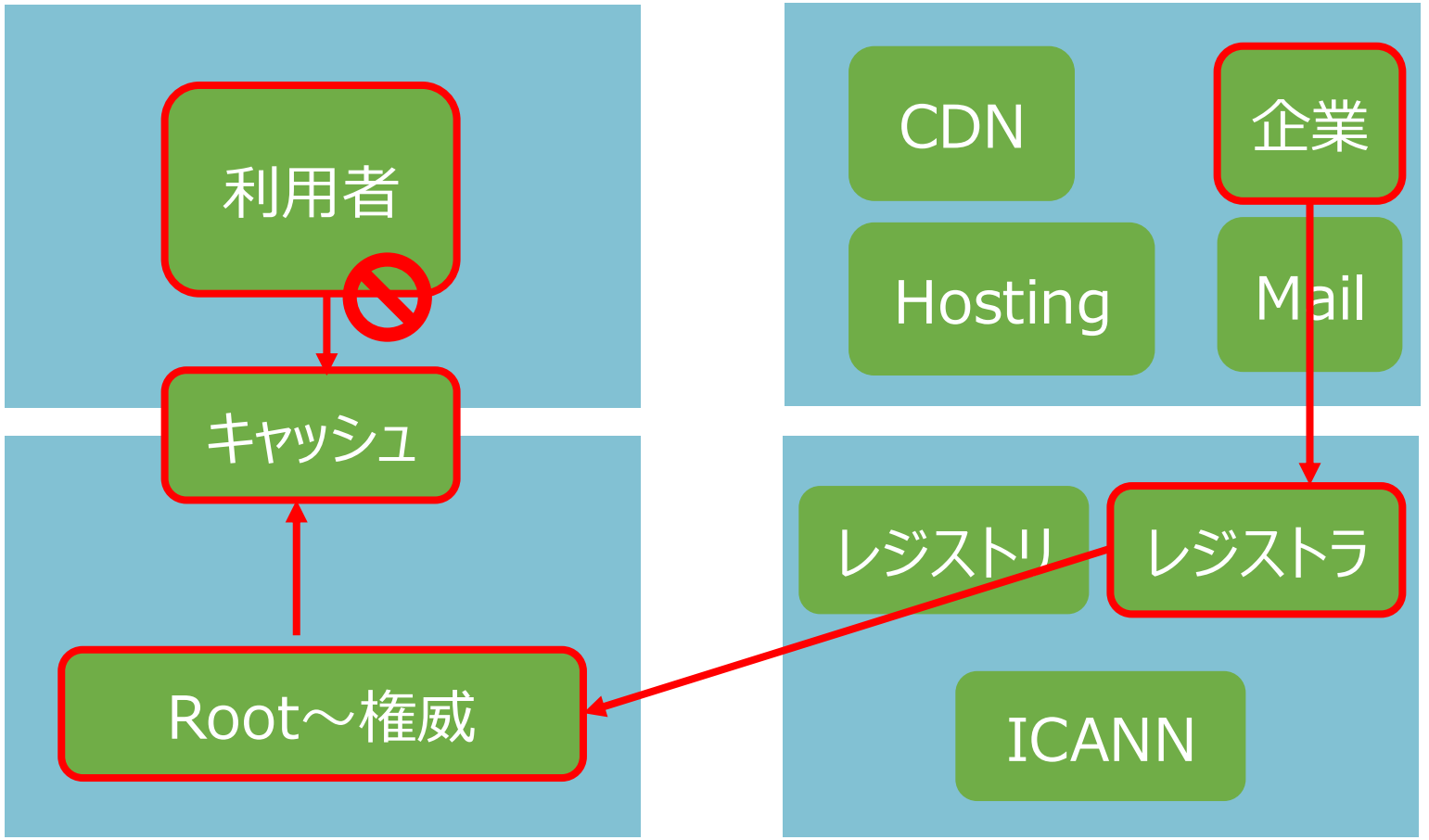
Mitigation (被害軽減)

- シナリオ: ウェブサイトが攻撃者に改竄された
- WebホスティングまたはCDNで当該コンテンツだけを削除



Mitigation (被害軽減)

- シナリオ: 攻撃者によってフィッシングサイトが作成された
- レジストラによるhold、DNS レベルでアクセス無効化



Remediation (是正)

- 不正登録のケース
- 侵害のケース

	不正登録	侵害
パターン	攻撃者自身のアカウントでドメインを登録する	自身のドメインの DNS やコンテンツが侵害される
被害者	第三者	登録者+第三者
是正措置	• アカウントロック • シンクホール誘導 • 再登録の防止	• 証拠収集と法執行機関への共有 • 停止と復旧の時期と方法の手順化 • 登録者への通知
注意点	正当なアカウントの回復方法	ドメイン停止が妥当なのか

まとめ

- DNS Abuse を考える場合は当事者だけでなく仲介者が多い
- バランスのよい対策を心がけて「巻き添え」を起こさない
- 証拠・証跡に基づいた行動や回復方法を準備する