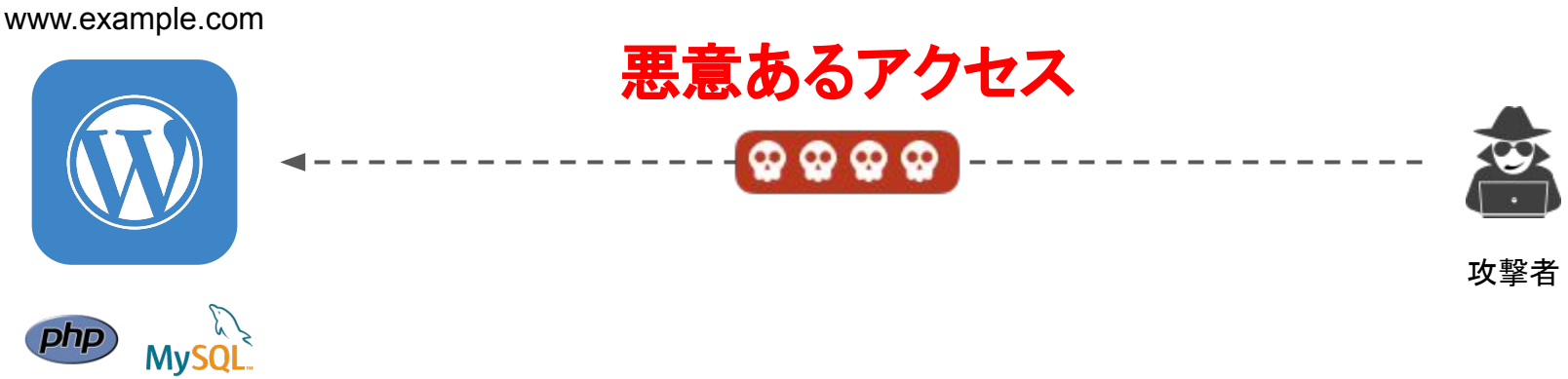
静的化によるセキュリティ確保について

rev. 201909

espar導入前（静的化実施前）



サーバをインターネットにさらしている状態
www.example.com を知ってさえいれば**誰でも**アクセスできることが最大の問題

WordPressサイトの４大ウィークポイント

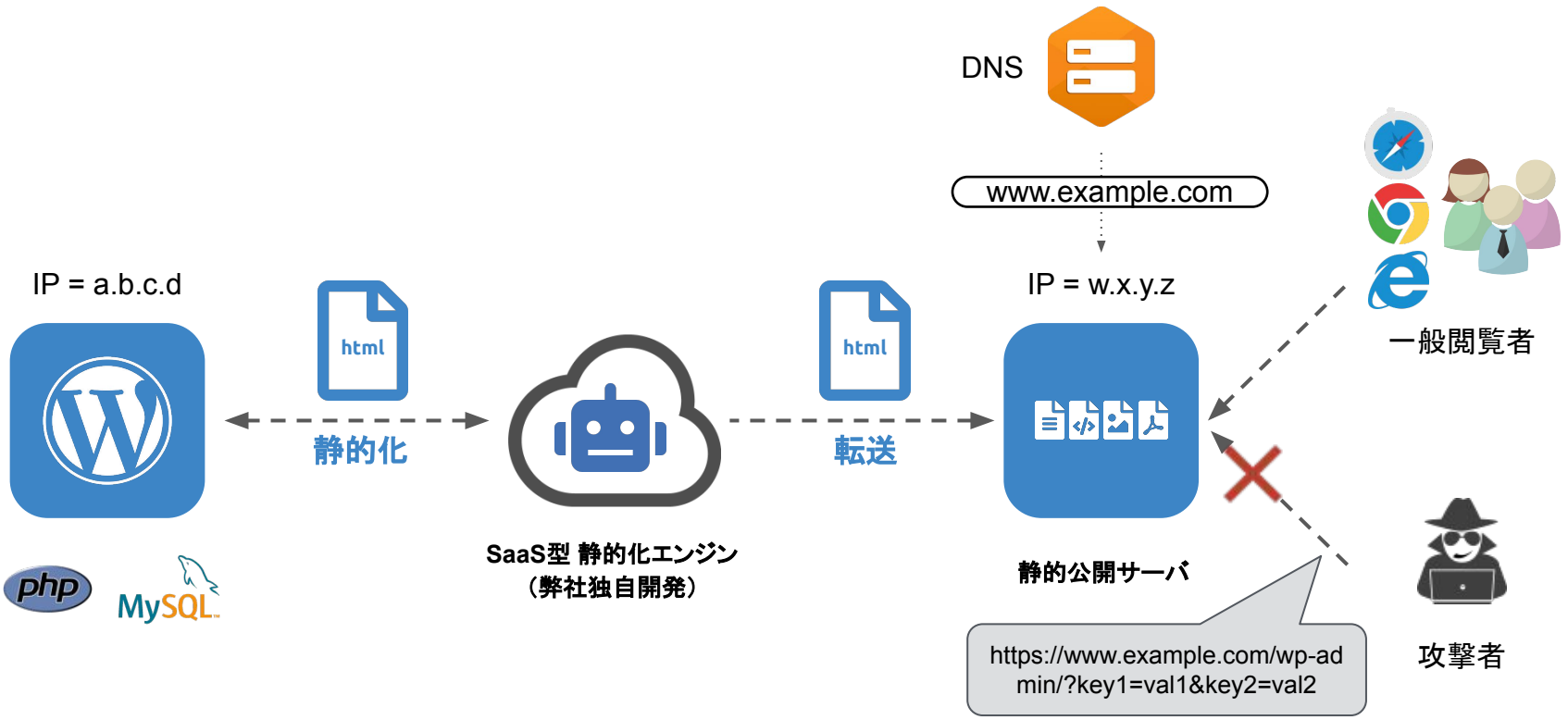
www.example.com

1. FTP/SSHへの不正ログイン
2. 管理画面への不正ログイン
3. 脆弱性へのアクセス
4. 大量同時アクセス（DoS/DDoS）

攻撃者

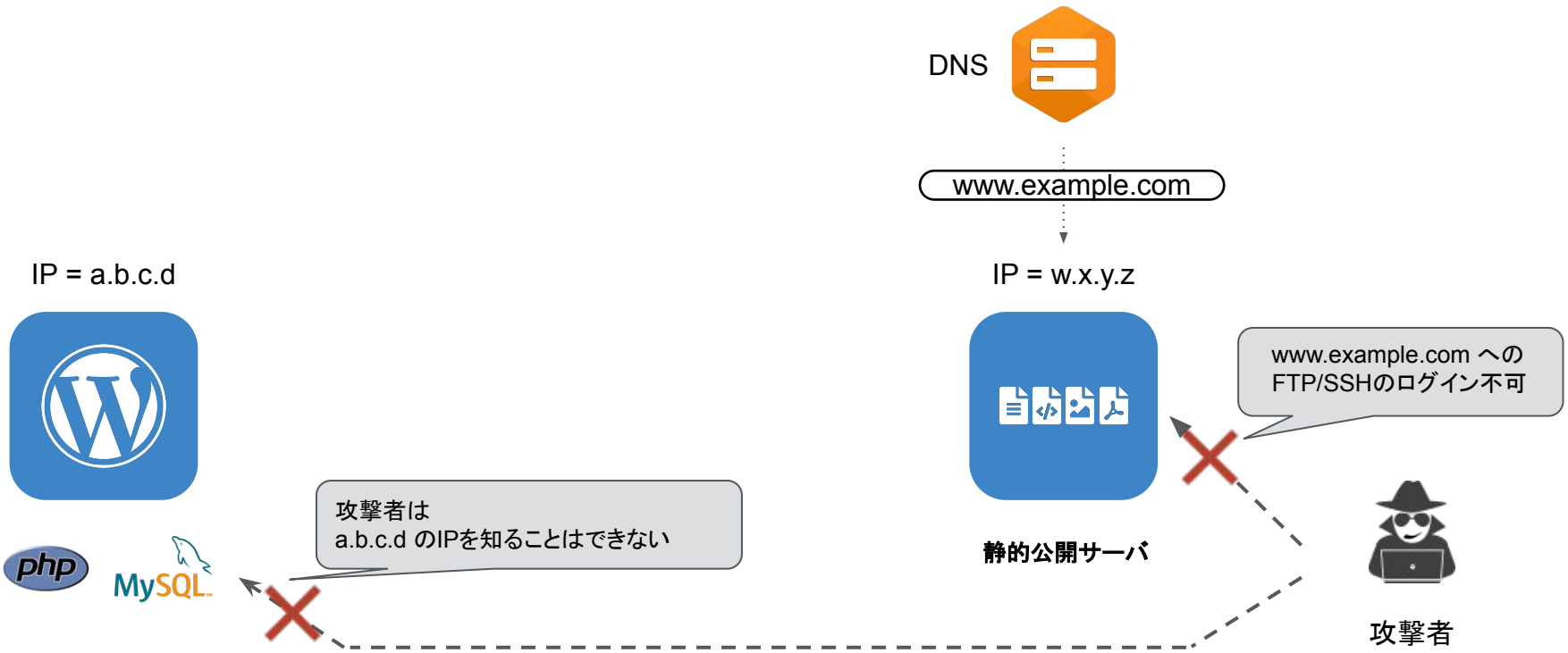
攻撃者がWordPressサーバに**直接アクセスできる状態**なので、
ウィークポイントを突かれ、事故が起こる

静的化 ＝ 攻撃者をWordPressサーバに到達できなくなるする技術



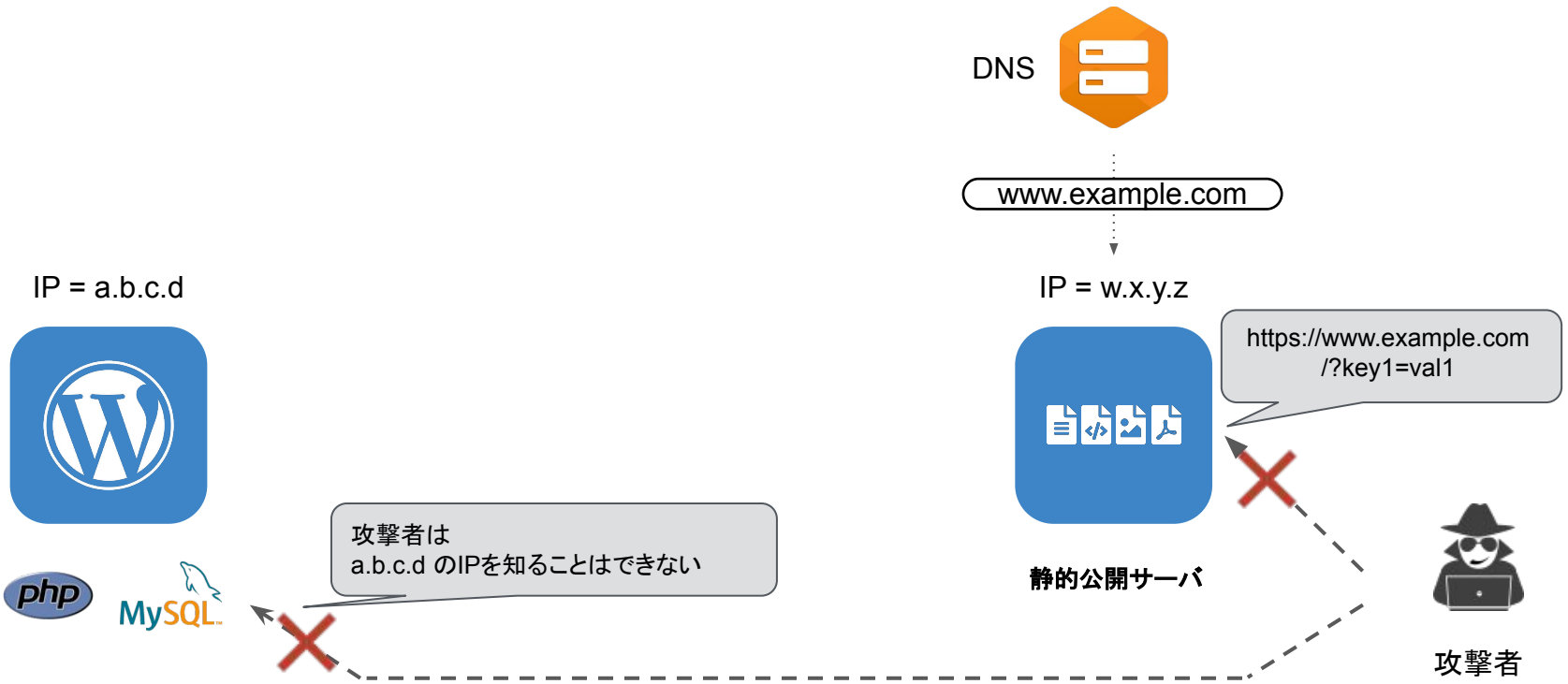
静的化・別サーバホスティング・DNS変更により、
WordPressサーバには原則アクセスさせないようにする
(サーバにアクセスできないのだから攻撃もしようがない)

①FTP/SSHの不正ログイン対策



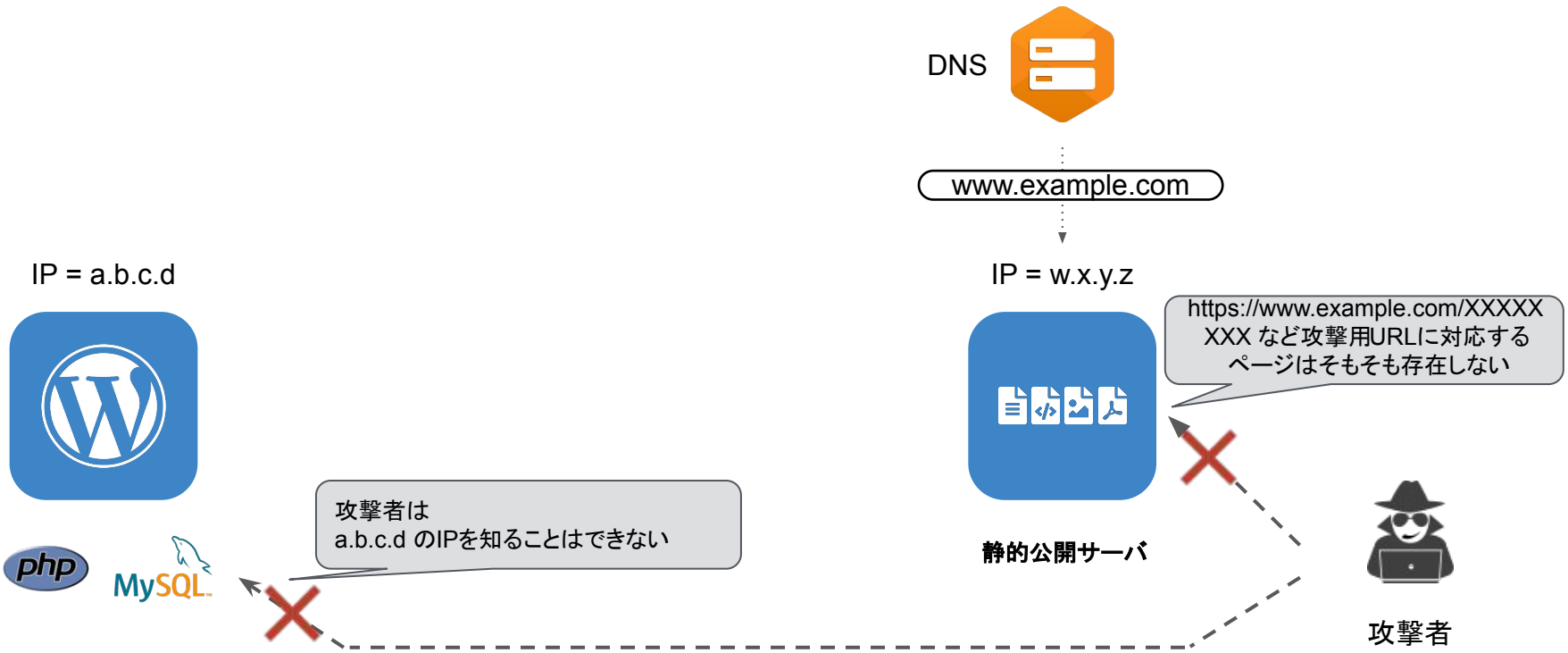
攻撃者はWordPressサーバ(a.b.c.d)にたどり着く事はできない
静的公開サーバ側はFTP/SSHのログイン不可
(当社の生体認証付き専用端末を使って当社 IPから当社担当のみが鍵認証方式でのみアクセス可)

②管理画面の不正ログイン対策



静的公開サーバにはWordPressは存在しない
→ 攻撃者が /wp-admin/ にアクセスしても 404 not found を返すだけ

③脆弱性へのアクセス対策

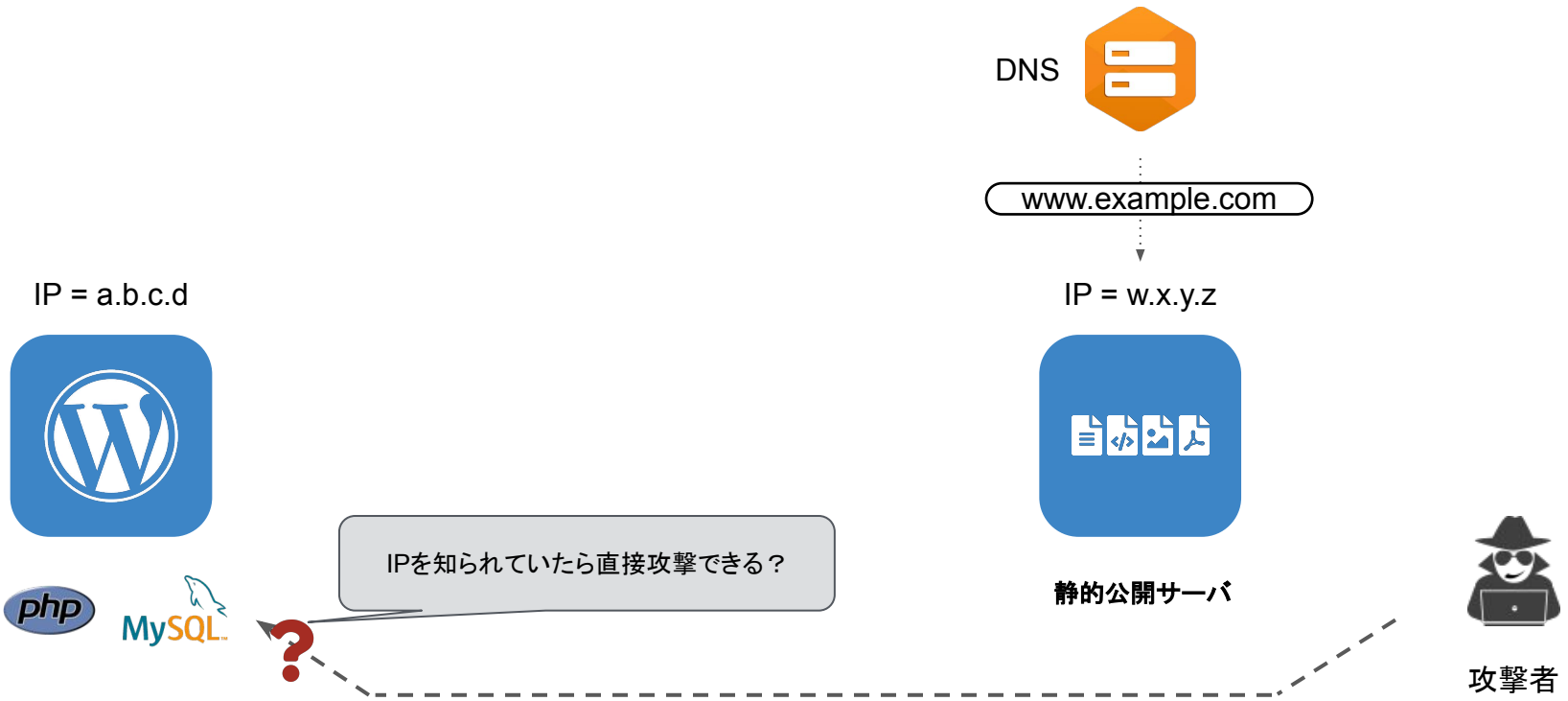


静的公開サーバにはPHPもDBもWordPressもプラグインも何も存在しない
→ 脆弱性を突くアクセスをしても 404 not found を返すだけ

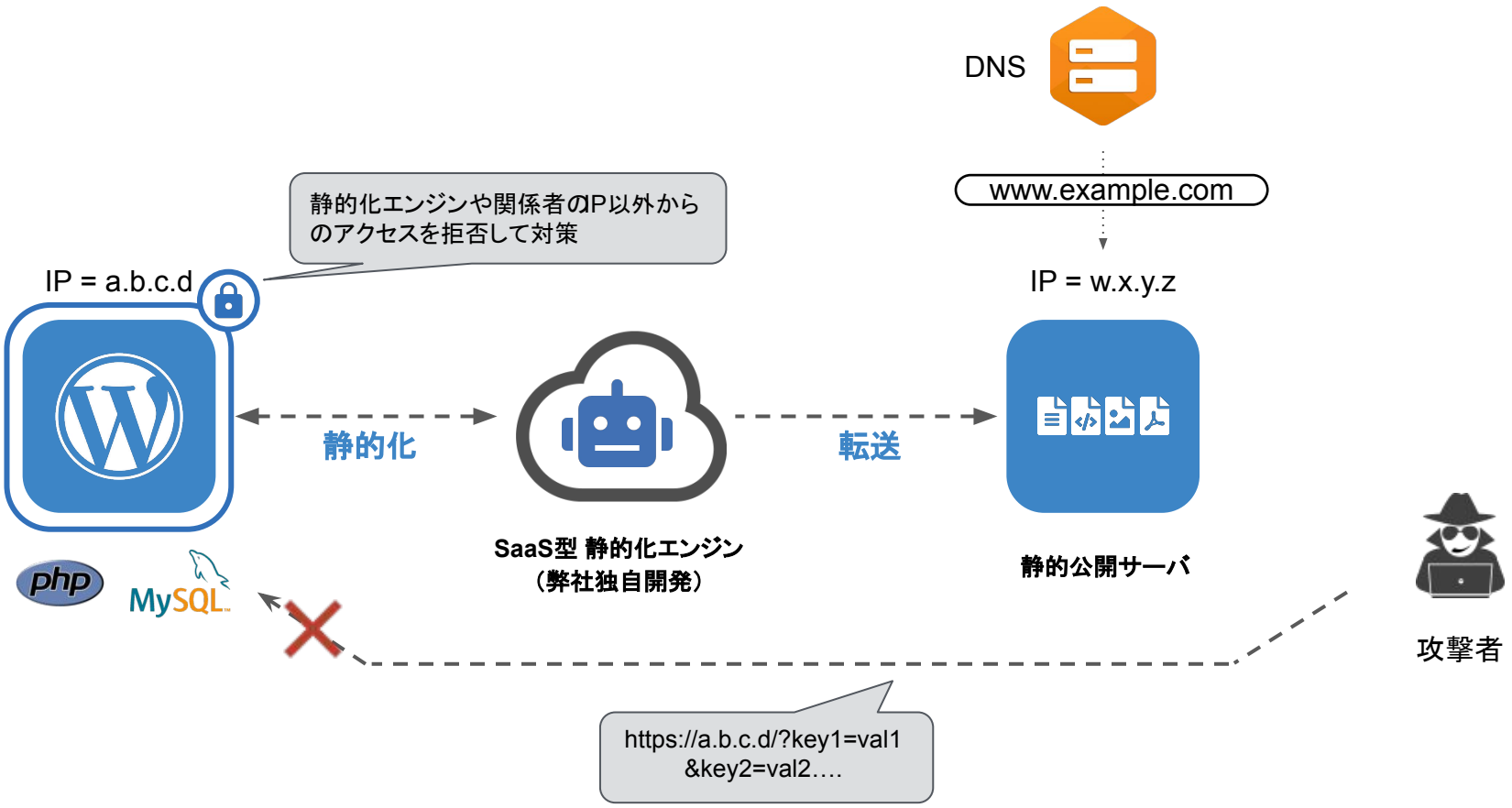
④大量同時アクセス（DoS/DDoS）対策

静的公開サーバ内で十分な負荷分散と帯域確保
また静的応答であるため理論上最高速の応答
（LB：負荷分散装置 Load Balancer）

疑問 『静的化前にIPがバレていたら？』

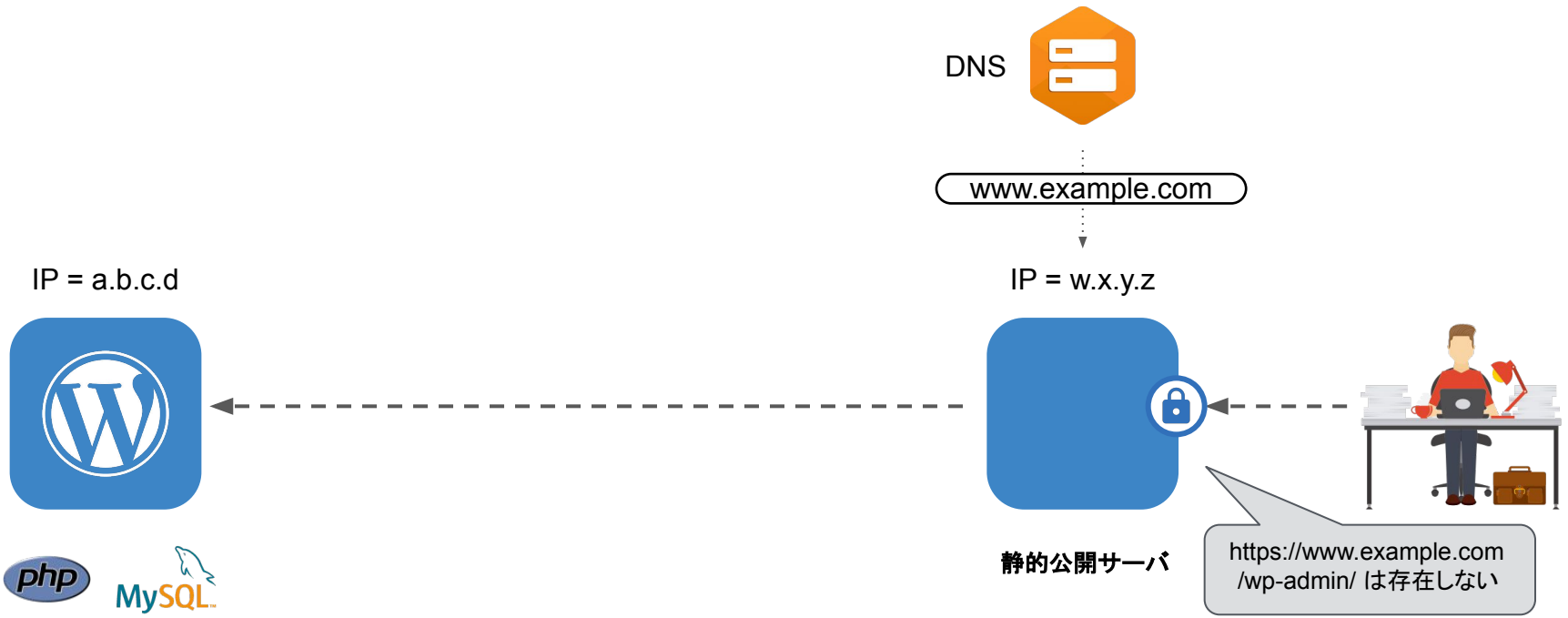


疑問 『静的化前にIPがバレていたら？』



WordPress側サーバは当該IPを知るべき関係者からのみのアクセスに制限
Basic認証も併用することでより強固に
→ IPが攻撃者にバレていてもWordPressにアクセスはされない状態に

疑問 『管理画面は？』



管理者であると識別できる場合（IP制限・Basic認証)に限り、/wp-admin/が存在するかのように振る舞う（WordPress 側に代理応答。プロキシ技術）

→ 悪意ある第三者にはアクセスさせず、関係者にのみアクセスさせることができる

最強のセキュリティ

守りたいモノの存在を攻撃者に知らせない（隠す）こと

静的化＆別サーバ公開

静的化によって、
WordPress**サーバ**の存在を非公開にしつつ、
WordPress**サイト**を公開する