



静的化によるセキュリティ確保について

rev. 202504

espar vault 導入前（静的化実施前）

www.example.com



悪意あるアクセス



攻撃者

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



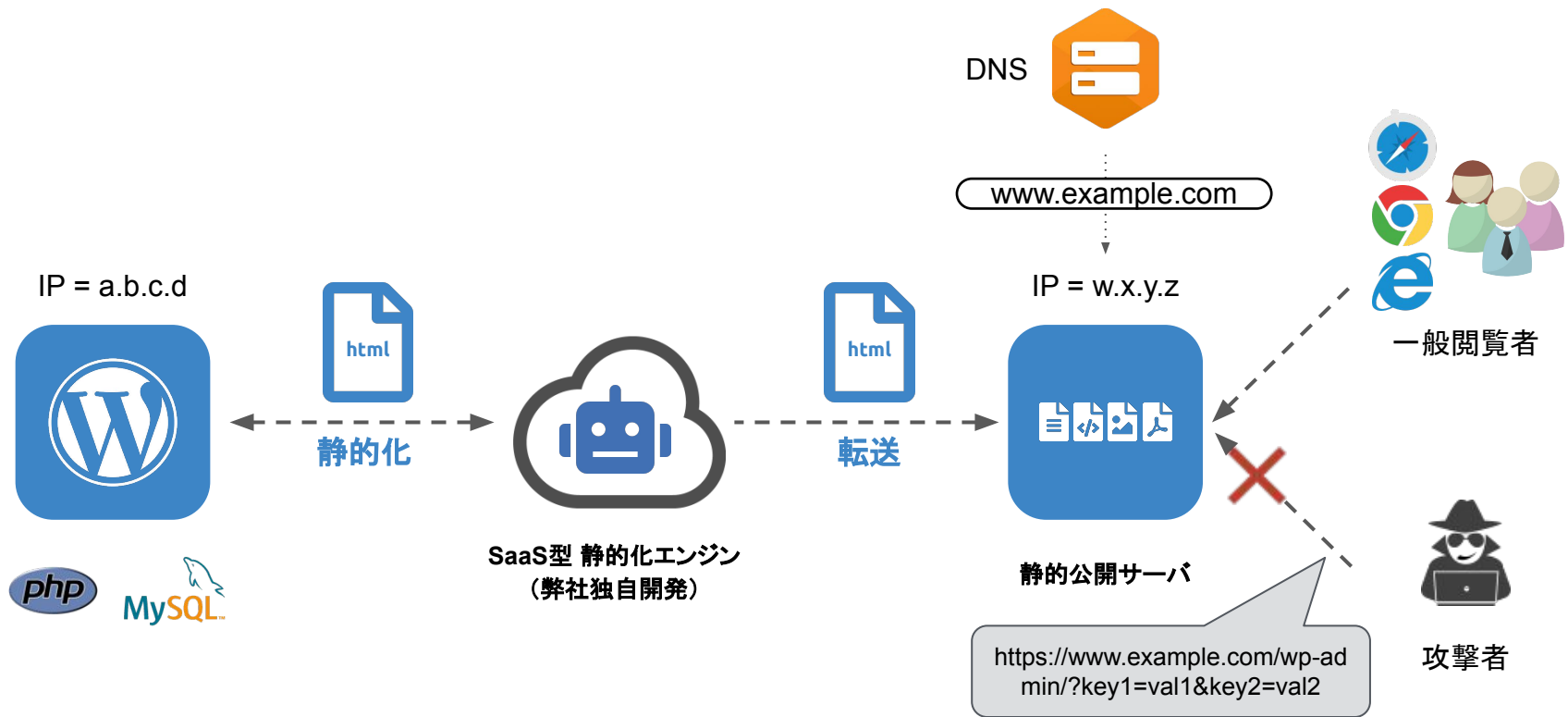
1. FTP/SSHへの不正ログイン
2. 管理画面への不正ログイン
3. 脆弱性へのアクセス
4. 大量同時アクセス (DoS/DDoS)



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(IP=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

(弊社の生体認証付き専用端末を使って弊社 IPから弊社担当のみが公開鍵鍵認証方式でのみ SSH可)

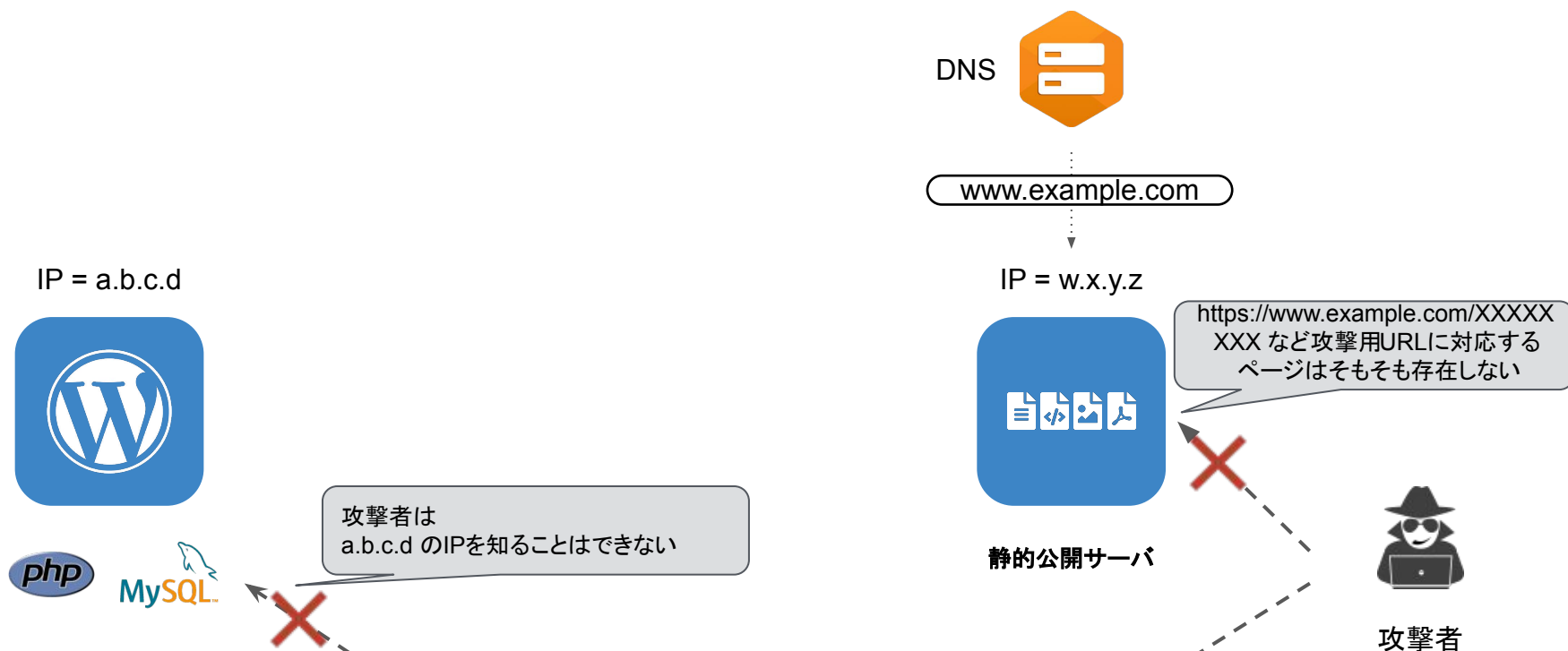
②管理画面の不正ログイン対策



公開サーバ側にはWordPressは存在しない

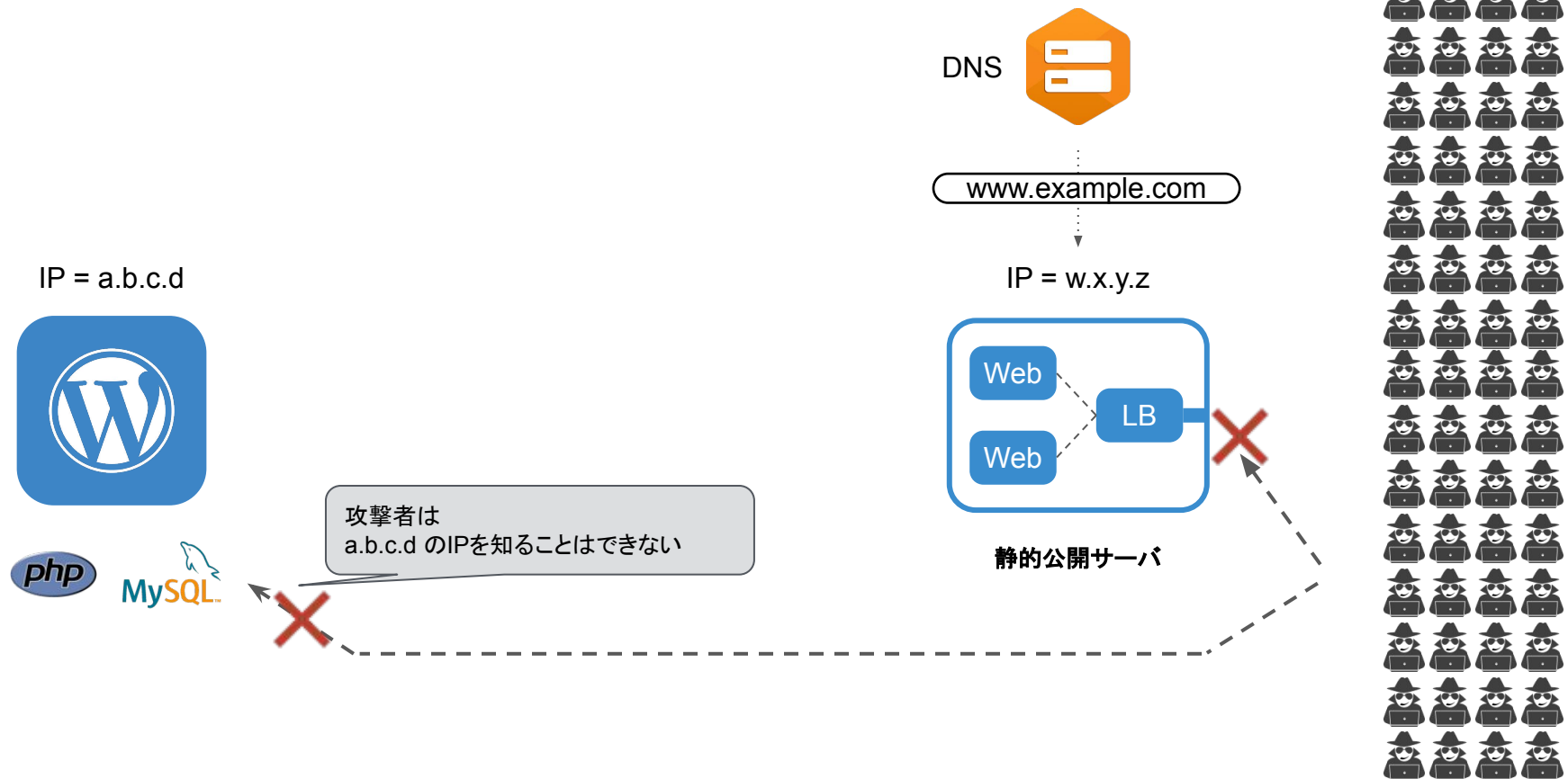
→ たとえ攻撃者が /wp-admin/ にアクセスしても 404 not found を返すだけ

③脆弱性へのアクセス対策



公開サーバ側には、DBもPHPもいかなるサーバサイドプログラムも存在しない
→ たとえ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

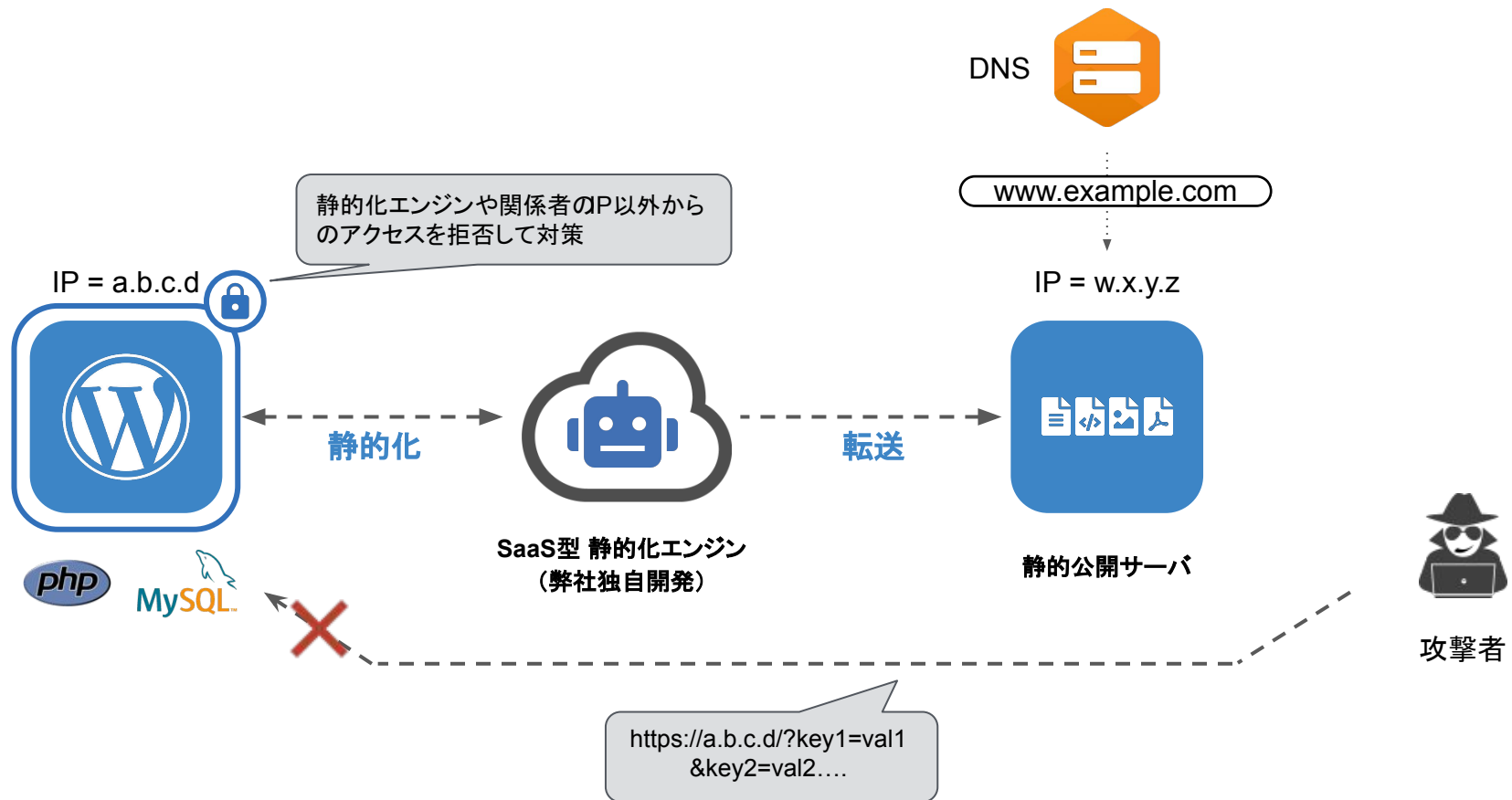


公開サーバ側ではHTMLファイル等のファイルを読んで返すだけ
さらに冗長化した負荷分散により、理論上はこれ以上に速くならない最高スピードで応答

疑問『静的化前にIPがバレていた ら？』

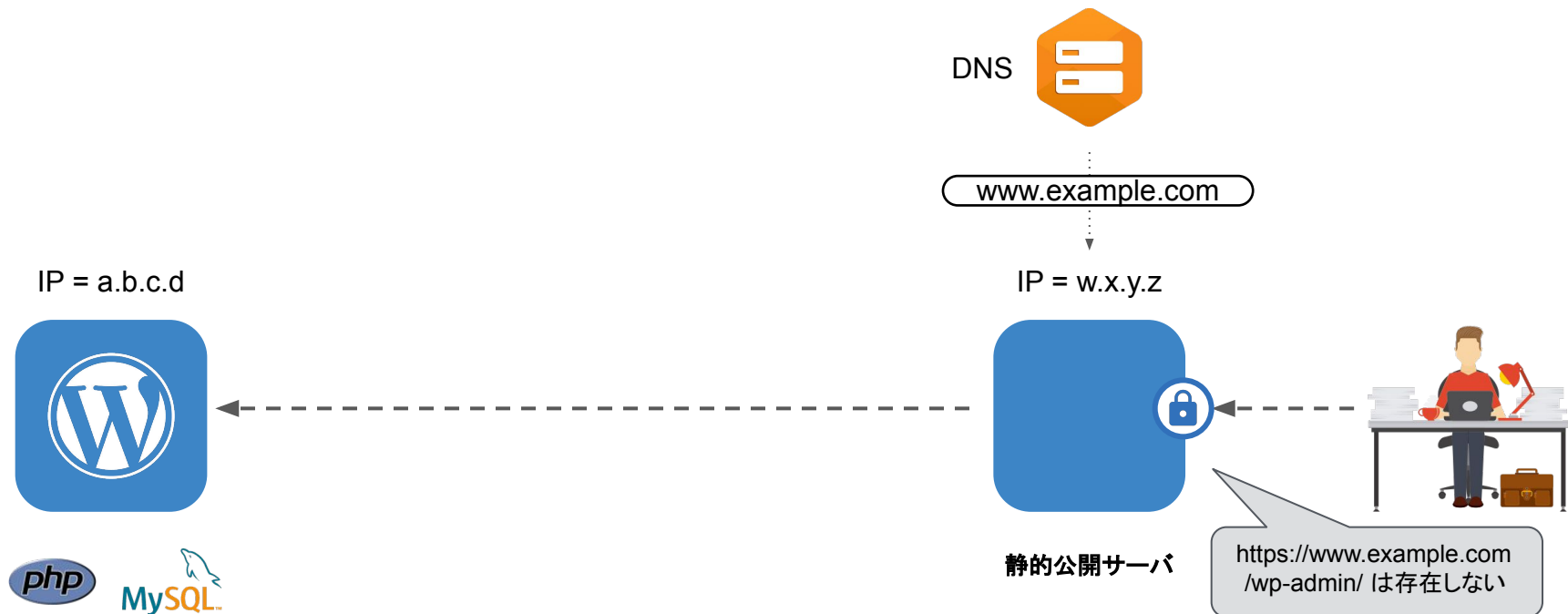


疑問 『静的化前にIPがバレていた ら？』



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。リーバスポキシ)

→ 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サイトを公開することができる。
WordPressサーバの存在を隠す以上に強固なセキュリティはない