要旨

① 研究テーマ 「クラウドサービスでの攻撃」

② 背景

昨今、企業のみならずプライベートにおいても、身近なところで“クラウド”という言葉が浸透してきている。クラウドの最大の魅力は、データを自社で保管しクローズドな環境で運用するのではなく、インターネット上に保管することで、PC やスマートデバイス等からいつでもどこでも利用可能な環境を、私たちに提供してくれることである。

こういったメリットを謳い文句に、クラウドは急速に広がってきている一方で、今までオンプレ環境を利用してきたユーザの中にはクラウドの利用に対してセキュリティ面での不安を抱えている。

そこで私たちは攻撃者の視点に立ち、クラウドのセキュリティが十分なものであるのか調査する。

③ 研究の目的

クラウド上に構築したシステムに脆弱性があった場合、クラウドのサービス機能でその脆弱性を補完可能であるか、また脆弱性に対する対策は何かを調査し提案する。

「クラウドはセキュリティが十分でない」という先入観を減らし、クラウドの普及に貢献する。

④ 研究の方針

クラウドを運用するにあたり、クラウド特有のセキュリティリスクの調査を行う。
併せて、クラウドサービスが提供する機能でセキュリティホールを補完可能か調査する。

⑤ 仮説

構築されたアプリケーションに脆弱性が見つかっても、クラウドによって提供されているサービス機能次第で補完することができるのではないか。

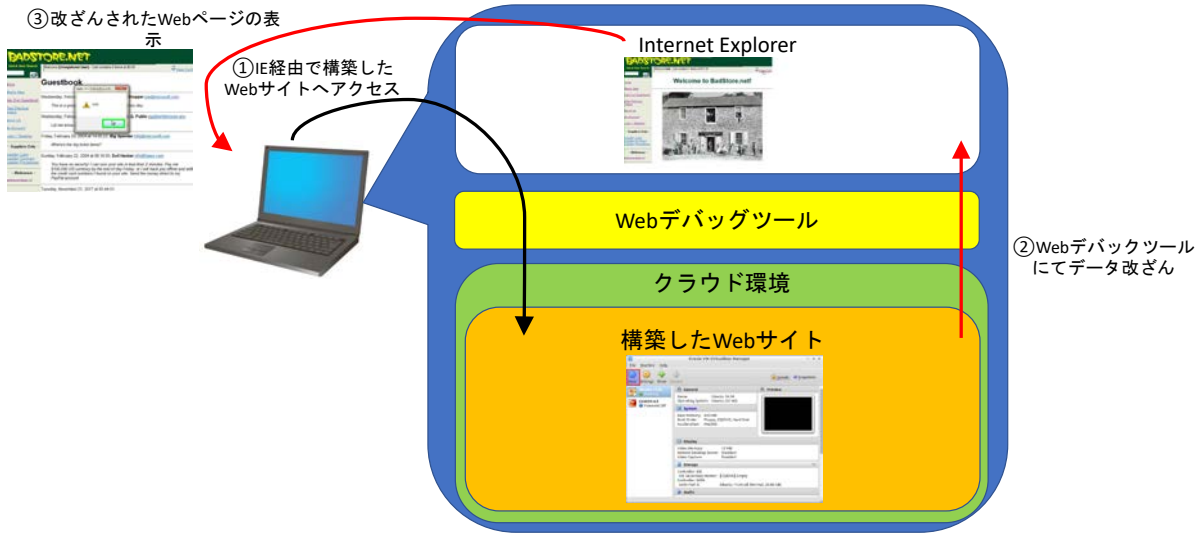
⑥ 研究内容

⇒以下シナリオにて、研究を実施する。

・クラウド(AWS)上にて脆弱性を作り込んだ Web サイトを構築する。
・構築した Web サイトに対して攻撃を行う。
・クラウド上で提供されている Web サイト防御サービス（WAF）の有り無しで結果を比較する。

※WAF：Web Application Firewall

要旨



◆クラウドを導入するに当たり、最大の懸念事項は情報漏洩だと考えられる。

そこでクラウド上に構築された脆弱性のあるアプリケーション(Web サイト)に対して、SQL インジェクション、ブルートフォース等の攻撃を行い、アプリケーションの内部情報を不正に取得することを試みる。クラウド上で提供されている Web サイト防御サービス（WAF）の有り・無しにより、どのような結果が得られるか検証する。

※AWS と限定した理由：
他のクラウドサービスと比較した結果、あまり差がみられない為、メジャーな AWS を採用した。

⑦ 今後の方向性

「クラウドはセキュリティが十分でない」という思い込みを減らすことを第一に考え、上記①～⑥項の内容について研究を進めていく。

研究した結果を見て頂くことで、クラウドに対する不安を持つ人が一人でも減ると幸いです。

以上