# SQAT®
# 情報セキュリティ瓦版

2019 年 10 月号

株式会社ブロードバンドセキュリティ
セキュリティサービス本部
東京都新宿区西新宿 8-5-1 野村不動産西新宿共同ビル 4F
TEL：03-5338-7417 FAX：03-5338-7435
https://www.bbsec.co.jp/

# クラウド環境における セキュリティの重要性

## ー 利便性＋αで求められるセキュリティ意識 ー

その利便性の高さからクラウドが広く普及しています。いまや既存システムのクラウド環境への移転、リニューアル化は時代の潮流といって良いでしょう。一方で、サーバ運用においてインシデントが発生してしまった場合、なりすましや DDoS 攻撃などによって様々な面で大きな被害を受ける恐れがあります。現実にサーバ運用のトレンドになっているクラウド環境では、その利便性に潜む罠によって、近年いくつもインシデントが発生しています。クラウド環境を利用するために重要な「リスクの可視化」についてお伝えいたします。

### アメリカ金融大手で 1 億人を超える情報漏洩

2019 年 7 月、米金融大手 Capital One は、外部の第三者から不正アクセスを受け、1 億件を超える大規模な個人情報漏洩があったことを公表しました。[*1] ただし、流出した個人情報（右記、表 1 参照）を悪用した事例は、9 月時点で確認されていないとのことです。

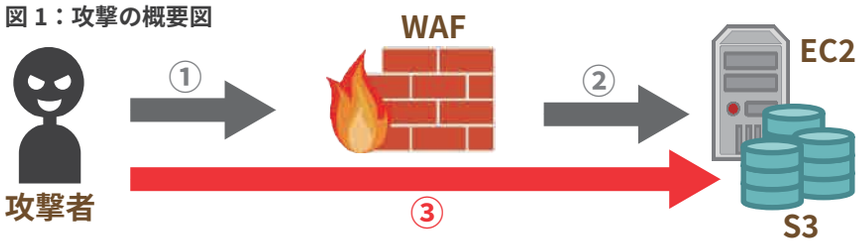
今回のインシデントは AWS（Amazon Web Services）環境下で発生しましたが、そこで同社は以下の点を主張しています。

■基盤システムへの侵害はない
■クラウド特有の脆弱性ではない
■対応の早さはクラウド利用の恩恵

**表 1：インシデントにより漏洩した情報**

| | |
|---|---|
| アメリカ 約 1 億人分！<br>カナダ 約 600 万人分！ | クレジットスコア（信用偏差値）、与信限度額、貸方残高、支払履歴、連絡先 |
| | 2016 ～ 18 年における取引データの一部（計 23 日分） |
| | クレジットカード顧客の社会保障番号約 114 万件 |
| | 銀行口座番号約 8 万件 |

**図 1：攻撃の概要図**




① クラウドサーバ上にあるファイアウォール（Capital One が独自に運用していた WAF）の設定不備を突く
② Amazon EC2 インスタンス（仮想サーバ）のメタデータサービスにアクセスし、AWS S3（シンプルストレージサービス）の認証情報を取得
③ AWS S3 に格納されている Capital One の重要情報を盗取

**表 2：AWS が提供するツール**

| | |
|---|---|
| AWS IAM アクセスアドバイザー | アクセス許可のガードレールを実装 |
| Amazon GuardDuty | 悪意のある操作や不正な動作を継続的にモニタリング |
| AWS WAF | SSRF を含む一般的なサイバー攻撃を防御 |
| Amazon Macie | 機密データを自動的に検出、分類、保護 |

### インシデントから浮上した問題点

Capital One のシステム環境における問題点は、WAF の運用上の設定ミスにより、SSRF 攻撃※（上記、図 1 参照）を検知できなかったこと、サーバ上のデータに対するアクセス制御が不十分だったこと、データ奪取に気づけるモニタリングを実施していなかったことが主に挙げられます。AWS はリスク軽減策としてツールを提供しており（上記、表 2 参照）、これを活用していれば、インシデントに繋がらなかった可能性も考えられます。

### クラウド環境の利点と危険性

クラウドサービスは、高い利便性ゆえに増加を続けています。米 Cisco はホワイトペーパー[*2] の中で、2016 年には 1 年あたり 6.0 ゼタバイト[1)] だったトラフィック量が、2021 年には 19.5 ゼタバイトまで増加し、全データセンターのトラフィックに占めるクラウドデータセンターのトラフィック比率は、88%から 95%へ増加すると予想しています。こうした増加の理由は、クラウド環境が自社設備内で情報システムを管理・運用するオンプレミス環境と比べて、コスト面、

運用面での利点があるためと考えられます。一方で利点に対して危険性があることも理解しなければなりません。

1. 自社内にオンプレミス環境を用意する必要がない
→外部委託することにより、他社環境に依存することになる
2. 仮想化されたリソースの配分自由度が高い
→従量課金のため、使いすぎると高コストになる
3. 構成するソフトウェアの独自開発が不要
→構成するソフトウェアがオープンソースのため、攻撃者に解析されやすい

一度攻撃を許してしまえば、情報漏洩、DDoS 攻撃によって、莫大な費用損失が発生し、企業のビジネス破綻を招く可能性があります。クラウドサービスの利用には、利便性と引き換えにある攻撃の可能性にも目を向ける必要があります。そもそも、基本的にクラウド環境は公開ネットワークからアクセスが可能なため、セキュリティ設定の実施は必須なのです。

では、実際にどのようにセキュリティを強化していくのか。対策の一つとして各クラウドベンダが提供しているクラウド環境上のセキュリティ関連の汎用モジュールを利用することを推奨します。例えば、AWS の場合では、インターネットセキュリティの標準化団体である CIS（Center for Internet Security）が公表している『CIS Amazon Web Service Foundations Benchmark』[*3] というガイドラインや、第三者による評価（当社では「AWS セキュリティ設定診断」として提供）を活用し、システム環境の設定状況を把握することが望ましいでしょう。

## 独自性カスタマイズのリスク

クラウド環境は各ベンダの提供している汎用モジュールが充実していますが、実際の提供サービスの機能と合致しないことがあり、その場合、独自のカスタマイズや実装が必要になります。前述の Capital One のインシデントでは、このカスタマイズこそがあだとなりました。実際の運用環境では、ポリシーや他との互換性を考慮して様々なカスタマイズが行われますが、その際に設定ミスが発生することで、セキュリティホールとなる可能性があることを認識し、十分に注意しなければなりません。また、カスタマイズされたモジュールそのものに問題がなかったとしても、汎用モジュールとの連携が原因で問題が発生することもあるでしょう。クラウド環境上で Web サービスを提供する場合には、各種設定がベストプラクティス（最善策）に適合しているかを把握し、さらに第三者の目から見た診断によって分析を行い、リスクを可視化することが重要です。

## クラウドの時代

今後、世の中はますます利便性の高いクラウドへと傾倒し、既存システムのクラウド環境への移転、リニューアル化がもはや時代の潮流となるでしょう。それゆえに、攻撃者の格好のターゲットとならないよう、隙を与えないための定期的な診断によるリスク把握は、クラウドを用いたビジネスにおいて必要不可欠なのです。

**※SSRF 攻撃**
**（Server Side Request Forgery）**

公開サーバに攻撃コマンドを送信することで、サーバ権限を利用し、非公開の内部サーバに攻撃が実行可能になる。
クラウド環境の内部サーバに対して、メタデータ取得 API を実行させ、ユーザの認証情報（ID・パスワード）を盗み取れる。

注：
[1] 6.0 ゼタバイト＝$6.0\times10^{21}$

参考情報：
[*1]https://www.capitalone.com/about/newsroom/capital-one-announces-data-security-incident/
[*2]https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html
[*3]https://www.cisecurity.org/?s=amazon+web+service+foundations+benchmark

# 既知の脆弱性こそ<br>十分なセキュリティ対策を！

**サイバー攻撃が経年とともに進化を遂げていることにもはや疑う余地はありません。しかし、我々ユーザ側はどうでしょうか。「複雑さはセキュリティの敵」といわれる中、ますます複雑化する IT 環境において求められている対策も多様化しています。日々様々な脆弱性が報告されていますが、三大脆弱性は「無知」「怠慢」「過信」であると考えます。「知る」「動く」そして「疑う」ことで、見えざる敵から情報資産を守りましょう。**

## 増加するデータ漏洩事故

データ漏洩、Web サイト改竄、マルウェア感染、サービス運用妨害（DoS ／ DDoS）等、サイバー攻撃はとどまることを知らず、被害件数は増加する一方です。脆弱性情報やデータ漏洩事故に関する市場調査およびリスク評価などを専門とする Risk Based Security 社の統計によれば、2019 年 1 月から 10 月現在までに発生したデータ漏洩事故は約 5,000 件にも及び、漏洩したデータ件数は約 75.6 億件で、現在もその数は増え続けています。[*1]

同社より発行された最新の統計レポート『Cyber Risk Analytics 2019 MidYear QuickView Data Breach Report』[*2] をみると、2019 年上半期に発生したデータ漏洩事故件数は、過去 8 年間で最も多いことが分かります。（下記、図 2 参照）

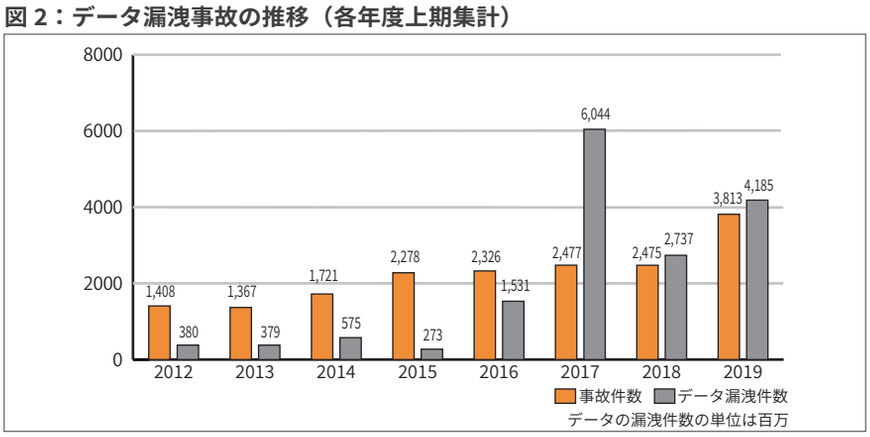
最近では、NoSQL や全文検索システムにおいて立て続けにデータ漏洩事故が発生しています。2019 年 8 月上旬に報道された、国内の企業で起きた従業員に関するデータ漏洩事故が記憶に新しいところかもしれません。2019 年 7 月から 8 月の 2 ヵ月間において、NoSQL サーバである MongoDB、または NoSQL/ 全文検索システムである Elasticsearch を使用している環境で発生した主なデータ漏洩事故・事件の一覧をまとめました。
（次ページ、表 3 参照）

## 設定不備が問題に

ここで誤解しないでいただきたいのは、これらデータ漏洩事故・事件は MongoDB や Elasticsearch 自体に問題があったのではないということです。問題は、NoSQL サーバや全文検索システムをデフォルト設定のまま利用していたことにあります。例えば、MongoDB や ElasticSearch、またシェアの高い Apache Cassandra、Apache Solr では、いずれもデフォルトで認証設定が無効です。これは NoSQL がユーザデータベースのような構造化データを扱うものとは区別され、元来非構造化データを集積する目的で使用されてきたことが背景にあると推測されます。外部から参照される可能性が低いものとして捉えられてきた非構造化データを取り扱うため厳密な認証は不要、というのが NoSQL の開発者の認識だったのではないでしょうか。中でも Elasticsearch は以前、認証機構を別モジュールとして有償販売をしていました。外部からアクセスされることは極めて稀なケースであるという認識だったからこそ、別モジュール扱いにしていたのでしょう。このような背景を考えると、ユーザが「なんとなく」「うっかり」認証設定をしていなかった可能性は十分考えられます。しかし、2019 年 5 月から Elasticsearch が認証を本体の機能として追加したことや様々なデータが格納されるようになったこと等を鑑みると、認証設定を「うっかり忘れた」や「必要だと思わなかった」では済まなくなります。

ではなぜ、最近になって頻繁に MongoDB や Elasticsearch のデー

**図 2：データ漏洩事故の推移（各年度上期集計）**




出典：Risk Based Security 社
『Cyber Risk Analytics 2019 MidYear QuickView Data Breach Report』データより当社作成

タ漏洩事故が取り上げられるようになったのでしょうか。一つの要因として、クラウド環境に導入しやすいという点があります。

実際、検索エンジンの「SHODAN」によると、AWS（Amazon Web Services）やDigitalOcean、Microsoft Azure、Google Cloudなどで多くのインスタンスが公開されていることを確認できます。クラウド環境に構築し、そこにオンプレミス環境からデータを移行した際、「うっかり」認証を設定し忘れたなどの理由で第三者にアクセスされる機会を増やしてしまったケースもあるでしょう。また、昨年秋ごろから多くのセキュリティ研究者が認証のないNoSQLや全文検索システムを発見する、一種の“ブーム”が到来していることも原因の一つとなっています。当社の脆弱性診断でも、認証設定のないElasticsearchやApache Solrを何度か検出しています。

## 定期的な対策と設定の見直しを

問題なのは認証設定だけではありません。出荷時／インストール時のデフォルト設定のまま確認もせずに運用することも、セキュリティのベストプラクティス（最善策）として推奨されません。利用可能なセキュリティ設定は適用する、不要なサービスポートは閉じる、悪用されうるサービスポートに対しては強固なアクセス制御を行う、といった基本のセキュリティ対策を講じるべきでしょう。ちなみに、同じ非構造化データを扱うSplunkにおいては、デフォルトでいくつかのセキュリティ設定が有効化されています。オープンソースと商用ソフトウェアで、コスト、運用保守、互換性など様々な面でメリット・デメリットがありますが、いずれにしても言えることは、自組織の資産に対して、オンプレミスかクラウド環境かに関わらず、定期的な棚卸しとアップデート、設定の確認、脆弱性診断などを通じて、不要なものや対処が必要なものがないかを常に把握しておくことが重要です。

NoSQLや全文検索システムに関するデータ漏洩事故について調査し、設定に問題のあるシステムを数多く発見、報告しているセキュリティアナリストのBob Diachenko氏は、とあるインタビューでこの問題について今後の展望を聞かれた際、利用者の意識改革が鍵であると答えています。[*3]

> *“tl;dr – Read the manual and don’t be lazy!”* [1)]

## 色々な顔を持つクリックインターセプション

サイバー攻撃は日々繰り広げられていますが、毎回脆弱性が新たに

**表3：2019年7月～8月に発生したNoSQL環境での主な漏洩事故・事件一覧**

| 業種 | 漏洩規模 | 漏洩した情報 |
|---|---|---|
| ITサービス | 20億レコード | スマートホームデバイスの位置情報・種類・スケジューリング情報・アクセスするアカウント所有者の個人情報・認証情報など |
| 自治体 | 9,000万レコード／26GB | 住民の個人情報・IDカード番号・ビジネスに関する情報など |
| 金融 | 30万レコード | 顧客の個人情報 |
| ITサービス | 80万レコード | ユーザの個人情報・家族の情報 |
| 自動車 | 1億3,400万ドキュメント／40GB | 従業員個人情報・マシンのインベントリ情報 |
| ITサービス | 2,780万レコード／23GB | 自社のサービスを利用する企業の従業員の生体認証情報・個人情報・従業員のアクセス認証情報（平文・非暗号化）など |
| 不明 | 1,400万人の個人情報／3GB | 2017年以降のチリの有権者の個人情報・納税者番号など |
| ホテル | 800万行 | 予約情報・宿泊客の個人情報・宿泊客のライフスタイルに関する情報・支払い条件・苦情・ルームサービスのオーダー・ホテルのadminの認証情報・宿泊客向けシステムのログイン情報・請求書・清掃員が撮影したホテルの部屋の画像など |
| ホテル | 70万レコード | 予約詳細・パスワード・支払いカードの情報<br>※テストデータが大半を占めるとしている |
| 出版 | 210万レコード | 顧客の個人情報・請求書・購買履歴・ショッピングカートのID・アクティベーションコードとトークン・カードの詳細情報 |
| 医療サービス | 3.7万レコード | 治験に参加する患者の個人情報・既往歴など |
| 教育 | 最大70万レコード | 生徒の個人情報・通学する学校名・学年・学区 |

発見されているとは限りません。以前からある脆弱性を利用して、手口だけを進化させているケースも多々あります。先般、「クリックインターセプション」に関するホワイトペーパーが公開されました。これは、2019 年 8 月中旬に米国カリフォルニア州で開催された、大学の研究者などが研究成果を発表するアカデミックカンファレンス「USENIX Security '19」において、香港中文大学、ソウル国立大学、Microsoft Research、ペンシルバニア州立大学の研究者らによって共同研究されたクリックインターセプションに関する研究・調査結果をまとめたものです。[*4]

もしかすると「クリックインターセプション」という言葉には耳慣れないかもしれません。これはサイバー攻撃の一種で、Web サイト内のリンクやボタンなどをクリックして遷移する先が第三者のページになるよう URL を差し替える攻撃です。これまでユーザのクリック操作を利用した攻撃については、Web ページの透過表示機能などを悪用した視覚的な騙しの技法が「クリックジャッキング」という名称で広く取り上げられてきました。しかし、ユーザのクリック操作を利用した攻撃はそれ以外にも様々なものがあり、悪質な第三者の JavaScript によって引き起こされる、あらゆる種類のクリックインターセプションを取り上げたのが今回の研究です。この言葉自体は新しいものではなく、大きく分けて以下の 3 つのタイプがあります。

① ハイパーリンクを利用したクリックインターセプション
② イベントハンドラ [2] を利用したクリックインターセプション
③ 視覚的な騙しを利用したクリックインターセプション

いずれの場合も、Web サイトの利用者が何らかのクリック操作を行うことで、第三者の用意した悪意のあるページに遷移させられ（視覚的に判断できるかできないかは別として）、機密情報を奪取されたり、マルウェアに感染させられたり、あるいはアドフラウド（広告詐欺）に加担させられたりといった様々な被害を受けます。

今回の研究で、研究者らは「Observer」と名付けた Web サイトにおけるクリックに関する挙動を確認するツールを作成し、Alexa アクセス数ランキングの上位 250,000 の Web サイトの TOP ページを調査しました。その結果、613 の Web サイトにおいてクリックインターセプションに該当する事象が確認されています。また、①を実行する新たな手口として、巨大なハイパーリンク [3] を埋め込み、Web サイトを訪問した利用者がクリックを余儀なくされるように仕込んだものが発見されたとのことです。

前述のとおり、クリックインターセプションは金銭的利益を得る目的で利用されることもあります。特に最近では、クリックインターセプションがアドフラウドの新たな手口の一つになりつつあります。アドフラウドは広告業界にとって深刻な問題であり、広告主は多大な金銭的被害を受ける恐れがあります。2019 年 8 月初旬、Facebook が、同社の広告プラットフォームを利用して不正な広告収入を得たとしてアプリの開発者を告訴した事件が報道されました。これもクリックインターセプション攻撃の一種で、Google Play ストアからアプリがダウンロードされる際に端末をマルウェアに感染させ、ユーザに気づかせずにアプリ内の広告のクリックを発生させる仕組みになっていたとのことです。これにより、あたかもユーザが自身の意思で表示される広告をクリックしているように見せかけ、不正に広告収入を得ていたと Facebook は説明しています。[*5]

## 十分なセキュリティ対策を

本稿で取り上げた脆弱性は、どれも新しいものではありません。攻撃手法は進化していますが、その元となる問題は十数年前から存在するものです。しかし、未だ対策されていないシステムが多く存在しているのが実情です。当社の脆弱性診断では、こうした既知のセキュリティ上の問題を検出し、それに対するリスク分析と問題を解消するための対策案をご提示いたします。自組織の資産のセキュリティ状況の把握、定期保守などを目的に、各種法令や基準に則って、脆弱性診断を継続的に活用されることをおすすめいたします。

注：

[1] 訳：tl;dr –マニュアルを読みなさい、そして面倒がらずに行動しなさい！（※「tl;dr」が何か分からない場合は検索してみてください。「知る」「動く」「疑う」を実践しましょう。）

[2] JavaScript で記述された、マウスの動きなどの操作に対して特定の処理を与える命令のこと

[3] 例として、ページの広い範囲を埋めつくすようなバナーなど

参考情報：

[*1] https://www.cyberriskanalytics.com/#statistics

[*2] https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

[*3] https://dzone.com/articles/exploring-elasticsearch-vulnerabilities

[*4] https://www.usenix.org/system/files/sec19fall_zhang_prepub.pdf

[*5] https://newsroom.fb.com/news/2019/08/enforcing-against-click-injection-fraud/

Column
～コラム～

# CVSS バージョン 3.1 リリース

CVSS（共通脆弱性評価システム：Common Vulnerability Scoring System）は、セキュリティ脆弱性の深刻度を、汎用的に、同一基準で、定量的に評価する手法です。

仕様検討と普及を推進している非営利団体 FIRST (Forum of Incident Response and Security Teams) が、CVSS のバージョンを 3.1 に更新し、2019 年 6 月に公開しました。主な変更点は下記、表 4 のとおりです。

米国立標準技術研究所（NIST）の脆弱性情報データベース NVD（National Vulnerability Database）で は、2019 年 9 月 11 日付で CVSS バージョン 3.1 の採用を開始しています。その他セキュリティに関する主な機関となる IPA や JPCERT/CC では、コメントを発表しておらず、今後の動向が注目されています。（2019 年 10 月中旬時点）また、クレジットカード情報および取引情報を保護するための PCI DSS (Payment Card Industry Data Security Standard) は、早ければ 2020 年後半にも公開が予定される「PCI DSS バージョン 4.0」でどの CVSS バージョンを採用するのかにも注視する必要がありそうです。

参考情報：
https://www.first.org/cvss/specification-document
https://www.helpnetsecurity.com/2019/07/15/cvss-3-1/

**表 4：CVSS バージョン 3.0 から 3.1 への主な変更点**

| 要点 | 概要 |
|---|---|
| 隣接ネットワークの定義 | ・攻撃元区分の隣接ネットワークの定義に、VPN などのセキュアな経路を通った接続や論理的な隣接ネットワークを追加 |
| インターネットから隔離された環境 | ・インターネットから隔離された環境に対する評価は、攻撃元区分（AV）を N から A と評価変更するのではなく、環境評価値（MAV）を A として評価 |
| 単一の脆弱性に対する複数の CVSS の許容 | ・同一の脆弱性に対して、製品バージョン、プラットフォーム、OS 等の違いによって異なる CVSS 基本値を設定することが可能 |
| 攻撃難易度（AC）の前提 | ・基本値の算定にあたり、攻撃者は一般的な設定や防御機構（F/W）の初期値を含む対象システムの弱点を知っている前提でスコアリング<br>・特定の攻撃対象に関する攻撃防御策・緩和策に関する条件は環境評価値で考慮 |
| 影響度<br>（C：機密性　I：完全性　A：可用性）<br>に関する追記 | ・攻撃の結果もたらされるアクセスの増大、権限昇格など負の影響は脆弱性の影響度（CIA）で考慮される<br>・CIA のスコアリングでは攻撃者が攻撃前に得ている権限と攻撃後に得た権限を比較し、権限における変化によって最大限もたらされる影響度を評価することが求められる |

**SQAT®（Software Quality Analysis Team）とは**
**～スペシャリスト集団が組織の脆弱性対策をトータルに支援～**

「SQAT®」は、BBSec がご提供する脆弱性診断サービスです。エンジニア、コンサルタント、ホワイトハッカー等から編成された精鋭チームが、あらゆる側面から網羅的な診断を実施。スペシャリストのノウハウを結集して組織の情報システム強化をお手伝いします。お客様は金融機関・インターネット事業者などの民間企業から、官公庁をはじめとする公共機関まで幅広く、これまでに延べ 4,300 組織、22,300 を超えるシステムで利用されています。



**株式会社ブロードバンドセキュリティ　お問合せ電話番号　03-5338-7417**