SQAT® Security Report

2024年 春夏号

基幹システムまで進むクラウド化、セキュリティで確認すべき要点とは？

知る・守る 続ける

BBSecは内閣サイバーセキュリティセンターの「サイバーセキュリティ普及啓発」に賛同しています

便利で安全なネットワーク社会を創造する
株式会社ブロードバンドセキュリティ

ごあいさつ

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 本部長　齊藤 義人

2023年はAIにはじまりAIに終わる年となりました。毎日のようにメディアやソーシャル・サービスでAIが取り上げられ、さまざまな形でAIを活用したサービスが登場し、人々が簡単にAIに触れられるようになりました。世間と同様に、サイバーセキュリティに関する分野でも、AIに注目が集まりました、それも攻防ともに。サイバー攻撃者は生成AIを利用したマルウェア開発やフィッシングメール生成、そのほかAIの悪用に乗り出しています。悪用の事例としては、昨年11月の臨時国会会期中に、生成AIを用いて岸田総理大臣の声を再現したとみられる偽の動画がSNSで拡散されたことが挙げられます。一方で、サイバーセキュリティに関連する組織や専門家も、AIを利用したさまざまなセキュリティサービスを展開して、これに対抗しています。AIを用いて攻撃確度を割り出すサイバー指標であるEPSSや、イスラエルがサイバー攻撃に備えるために生成AIを用いた「サイバードーム防衛作戦」を展開するとしていることなどが、そうした潮流から生まれ出たものと言えるでしょう。

そして、2024年はいよいよもってDXが進んでいく年になると予想されます。物流業界を取り巻く「2024年問題」もそうですが、少子高齢化の日本社会において、DXによる生産性向上は必要不可欠です。2024年はAIとDXが強く結びついていく年になることでしょう。そうした中、サイバー攻撃は激化し、サイバーセキュリティの重要性は益々高まってくることが予想されます。

本レポートは、株式会社ブロードバンドセキュリティ（以下、BBSec）の脆弱性診断サービス「SQAT®」における2023年下半期（7月～12月）の診断結果からデータを抽出し、集約したものを弊社のエンジニアらの感性も交えてアウトプットしたものです。今号は「基幹システムまで進むクラウド化、セキュリティで確認すべき要点とは？」と題して、クラウド環境においてのセキュリティの懸念点、そしてクラウド環境のセキュリティ設定の重要性についてひもとく企画や、セキュリティ分野からの地方創生を考える弊社の「東北セキュリティ診断センター」を紹介する記事などが掲載されております。

本レポートが読者の皆様のセキュリティ対策における有益な情報としてご活用していただけることを願ってやみません。それこそが「便利で安全なネットワーク社会を創造する」をモットーに掲げるBBSecの使命であると考えております。

CONTENTS

SQAT.jp

※本レポートは、弊社セキュリティサービス本部のホームページ
「SQAT®.jp（URL：https://www.sqat.jp/）」
https://www.sqat.jp/sqat-securityreport/からダウンロード可能です。

巻頭企画

基幹システムまで進むクラウド化、セキュリティで確認すべき要点とは

DX推進や働き方の変化などにより、システムをクラウド化する組織は増える一方だ。中には基幹システムをクラウド化する組織も存在し、普及が進んでいる。身近な存在となったクラウドだが、同時にクラウド環境の設定ミスによる情報漏洩といったインシデントが後を絶たない。ここでは今一度クラウド環境においてのセキュリティの懸念点、そしてクラウド環境のセキュリティ設定の重要性について確認していく。

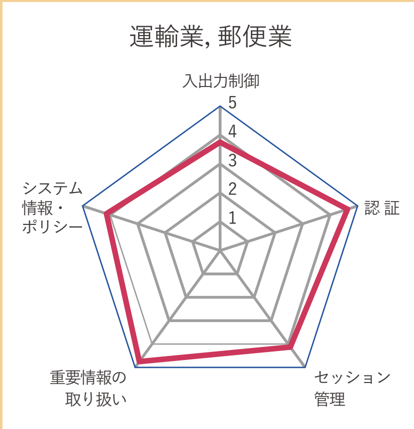
SQAT® Security Report 編集部

増加し続けるクラウドシステムとその範囲

DX推進や、感染症対策による働き方の変化などが相まって、システムをクラウド化する組織は増加し続けている。その動きは一般企業にとどまらず、例えば昨今「医療クラウド」と呼ばれる病院の電子カルテのクラウド化や、「ガバメントクラウド」と呼ばれる地方公共団体の基幹業務のクラウド化なども行われている。特にガバメントクラウドについては、日本政府が令和3年度から段階的な移行を経て、令和7年度末には、原則すべての地方公共団体の基幹業務システムをクラウド化する計画であり、規模としてもかなり大きいものである。

DX推進が活発な運輸業界の弊社脆弱性診断結果

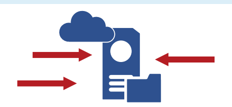
今DX推進が活発な業界の一つとして話題に挙がるのが運輸業界である。2024年4月から自動車運転業務の残業規制が始まり、トラックドライバーなどで常態化していた長時間労働が制限されるようになるため、それに伴う利益の減少などの諸問題（「2024年問題」と呼ばれる）をシステム化によって対応するといったDX推進の動きが強まっている。
実際、運輸業界における2023年7月～12月の弊社脆弱性診断は8割以上がクラウド上にあるシステムを対象に行われた。結果を平均したものが右図である。認証や重要情報の取り扱いといったカテゴリではセキュリティレベルが高い状態となっているが、入出力制御ではいくらかリスクの重大性が高い脆弱性が検出されている。2024年問題のように期限が決められていたり、早急な対応が求められたりという環境下でのシステム導入はセキュリティに穴が生まれやすい。DX推進を行う際は、必ずセキュリティが問題ないかのチェックも実施することを推奨する。



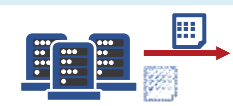
経済産業省が「2025年の崖」と表現しているように、組織内で横断的にデータを活用できなかったり、システムが複雑化・ブラックボックス化したままになっていたりといった課題や、それに並行して業務の見直しがなされない状態となっていたならば、2025年以降毎年最大12兆円もの経済損失が生じる可能性があると言われている。
今後もDX推進は行われていくことが想定され、その中で組織のシステムをクラウド化することもあるだろう。クラウド化すれば、物理的な場所をとらず、容量拡張などが容易で、インターネット環境があればどこからでもアクセスできるなどと利便性が高くなる。そういった利点から基幹システムまでもクラウド化している組織も存在する。

基幹システムとは「基幹」という名のとおり、企業にとって業務を行う上で必要不可欠なシステムのことを指す。そこにはサービス提供や業務運用上に必要な情報が多く含まれており、もしシステムの停止などが引き起こされれば業務継続ができなくなる。

クラウド化によるセキュリティ上の懸念事項として下記が挙げられる。



外部環境にシステムを構築することによる不正アクセスの可能性



データセンターからの情報漏洩、データ消失の可能性

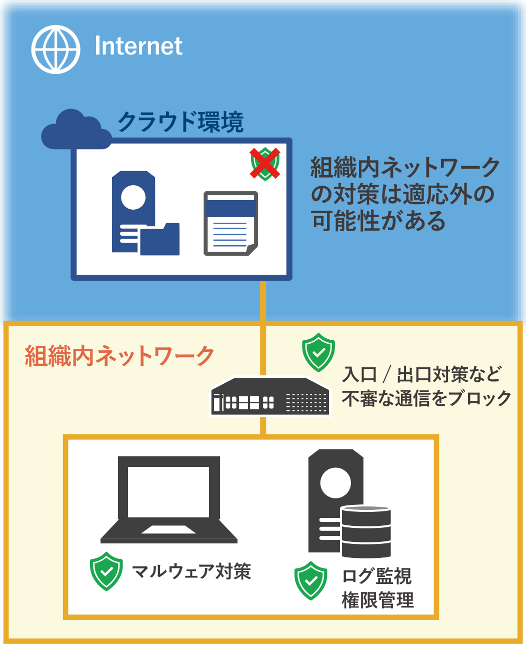
クラウド提供事業者に一部セキュリティを任せざるを得ないため、双方の責任範囲が不明瞭となり、対策の見落としが発生する可能性

そんな中で「クラウドにしておけばクラウド事業者が何とかしてくれるから大丈夫」と、なんとなくの安心感を持ってしまっていたら要注意である。
基幹システムのような重大なシステムをもクラウド環境に移行する流れがある今、セキュリティにおいて何に注意を払うべきなのだろうか？

クラウド化に伴う脅威

クラウドという外部環境にシステムを構築するということは、パブリッククラウドであれば外部のインターネットからその環境にアクセス可能であること、そして自組織内で展開しているセキュリティ対策は外部環境には適応されないため、別途対応が必要であることを認識しなければならない。

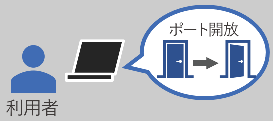
具体的なインシデントの例を挙げる。



<脅威の例１　気づかぬうちに行われたクラウド環境の利用者によるポート開放>

クラウドシステムの構築者からは「構築時ポートは開いていない設定にしている」と連絡を受けていたが、実際に調査するとポートが開いていた。

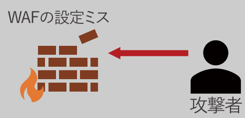
詳しく調査した結果、構築後にクラウド環境の利用者側でポートを開けてしまっていたことがわかった。



ポートが開放されたままということは外部からの通信を受け入れられる状態であるため、攻撃の足掛かりとされる可能性があり、脆弱となる。
このように専門家が実施したセキュアな設定を、利用者が使用しているうちに意図せず脆弱な設定に変更してしまうことが起こりうる。

<脅威の例2　WAFの設定ミスによる情報漏洩>

クラウド環境上のWAF（Web　Application　Firewall）に設定ミスがあり、攻撃者のSSRF（Server Side Request Forgery）攻撃を受けた。



SSRF攻撃によりクラウド環境の内部の仮想サーバに不正アクセスを受け、情報が漏洩してしまった。

SSRF攻撃とは、公開サーバを経由して直接アクセスできないサーバに攻撃を仕掛ける手法である。今回のようにWAFの設定に問題があるとそこを経由して他のサーバが被害を受けてしまう可能性がある。
これにより大規模な情報漏洩などが引き起こされた事例も存在する。

これらの事例からもわかるとおり、クラウド環境のセキュリティ設定に見落としがあったことがインシデントの引き金になっている。ではクラウド環境のセキュリティ設定を見直すうえで、特に優先して見るべき設定は何なのか。

セキュリティの標準化を取り組んでいるアメリカの団体Center for Internet Securityは、CIS Benchmarksというセキュリティのベストプラクティスをまとめたガイドラインを策定している。そのCIS Benchmarksのクラウド環境向けの内容から考えると、とくにリスクの重大性が高い脅威に関連する右記の項目が見えてくる。

これらの項目から考えると、クラウド環境のセキュリティ設定における「アクセス制御・ユーザ認証の強化」と「データの暗号化」が重要であると考えられる。

- rootアカウントでの認証
- 管理用ポートへのアクセス許可
- パブリックアクセスを許可
- ストレージの保管時の暗号化

対策の鍵は…
クラウド設定の
●アクセス制御･ユーザ認証の強化
●データの暗号化