

2018 年 7 月 9 日

CA Technologies の調査で、既存の企業文化が DevSecOps 導入の障害になっていることが明らかに

～ただし IT リーダーは DevSecOps の重要性を認識しており、調査回答者の 3 分の 2 がセキュリティを
ソフトウェア開発のライフサイクルに統合することが不可欠であると回答～

CA Technologies（東京都千代田区、社長：反町 浩一郎）は本日、セキュアなソフトウェア開発に関する世界的調査における日本の結果を発表しました。これによれば、日本の多くの企業が現在の企業文化がソフトウェア開発ライフサイクルへのセキュリティの統合（DevSecOps）の採用を妨げていることが明らかになりました。また、日本の回答者のうち、現在の企業文化と慣行が開発、運用、セキュリティの連携にとって必要な事であると認識しているのは 14%にすぎませんでした。

IT 業界調査会社 [Freeform Dynamics](#) によって実施された「[Integrating Security into the DNA of Your Software Lifecycle](#)（ソフトウェア・ライフサイクルの DNA にセキュリティを統合する）」と題されるこの新調査の目的は、DevOps にセキュリティを統合することがなぜ新たな原則となったのかを示す深い考察を示すことにあります。この調査では、日本の回答者、78 人を含む 15 の市場の 1,200 人以上の IT リーダーが調査対象となりました。

ソフトウェアがデジタル・エコノミーにおけるビジネスの成功にとってその重要性を増すにつれて、セキュリティへの懸念が急激に高まっています。実際に、日本の回答者のうち 62%が、ソフトウェアとコードの問題によるセキュリティ上の脅威がますます懸念されていることに同意しています。

しかし、回答者の 58%は、ソフトウェア開発プロセスにセキュリティのテストと評価を組み込む上で既存の企業文化がハードルとなっていると回答しています。同様に、製品の市場投入時間短縮を成功させるためにセキュリティを犠牲にしないことの重要性を上級管理職は理解していると回答したのは、全体の 17%にすぎませんでした。

日本でのデジタル・エコノミーにとって不可欠なセキュリティに対する DevSecOps のアプローチ

今回の調査から判明した事実、セキュリティをソフトウェア開発において不可欠な要素にしようとする組織の努力を妨げている原因が企業の組織文化の格差であることを示しています。

CA technologies セキュリティ・ソリューション事業部 事業部長 四宮 康典

今日のデジタル化への急速な変化の世界では、増え続ける顧客の要求から、多くの組織がソフトウェア・アプリケーションとそのアップデートをほぼ継続的にリリースするようになっています。アプリケーション・セキュリティについては、開発ライフサイクルの最終工程あるいは本番稼働後に置かれているままでは、アプリケーションを早く市場に投入しなければならないというプレッシャーに屈してセキュリティ脆弱性を残したままリリースしてしまいます。製品/サービスのデリバリー・サイクルが短くなれば、セキュリティをソフトウェア・ライフサイクルの全ステップに統合することが欠かせなくなります。これが DevSecOps の背後にある基本原則であり、ソフトウェア開発ライフサイクルに関わる誰もがセキュリティの責任を負うことになります。

日本では、調査対象の IT リーダーの 58%が、セキュリティをソフトウェア開発ライフサイクルに統合することが重要であると認識しています。DevSecOps を採用することで、企業は、セキュリティの脆弱性や、それに関連する生産停止時間、データ漏洩、消費者からの信頼の喪失、ブランド・イメージの悪化といったことで生じる高いコストを回避することができます。

また、DevSecOps は、企業がセキュアなソフトウェアの提供をサポートし、それによって、今日のデジタル・エコノミーの推進力であるアプリケーションやデジタル・サービスに対するユーザの信頼性を高めることに貢献します。調査によると、日本の回答者の大多数が、ソフトウェア開発が成長と拡大を支え（97%）、企業の競争力を強化し（87%）、デジタル・トランスフォーメーションを促進する（80%）ことに同意しています。

日本におけるセキュリティに対する姿勢とアプローチは前向き

企業文化の課題や各種の懸念が増えているのにもかかわらず、今回の調査から、日本の IT リーダーが今日のビジネスにおいてセキュリティが果たしている役割についてより重要性を見出していることが明らかになりました。日本の回答者の 67%以上が、セキュリティは新たなビジネス機会をもたらすイネーブラーである点に同意しています。さらに、67%の回答者は、セキュリティ・チームが業務部門からはリーダーとみなされており、決してイノベーションを妨げる存在ではないことに同意しています。

この調査で強調されたもうひとつの要素は、セキュリティを強化するために企業が先進的なテクノロジーを社内で広く採用している点でした。また、70%以上の回答者は、行動分析と機械学習の使用が以下の分野では不可欠であると考えています。

- ユーザー・データを保護しながらユーザー・エクスペリエンスを向上させる（79%）
- 活動のパターンに基づいてデータ侵害の脅威を評価する（70%）
- データ侵害を回避および/またはその影響を緩和するための予防的措置を実施する（78%）
- ユーザが行っていること、およびそれらについて知っていることに基づいてコントロールを認証する（78%）

本レポートでは、ソフトウェア開発ライフサイクルにセキュリティを統合できている企業を「ソフトウェア・セキュリティ・マスター」（日本を含む全回答者の上位 34%）と定義しており、それらの企業の特徴が紹介されています。それらの特徴としては、セキュリティ脆弱性に対する早期および継続的なアプリケーションテストの実施、DevSecOps の採用が含まれます。実際、他の多くの企業と比較して、「ソフトウェア・セキュリティ・マスター」は、セキュリティを新しいビジネス・チャンスの可能性と見なすことに強く同意する可能性が 2 倍以上ありました。

調査方法について

本調査は、CA Technologies の後援により、2017 年 7 月、市場調査会社 Freeform Dynamics 社 Intelligence Unit 部門が世界 15 カ国（米、ブラジル、英、仏、独、西、伊、スイス、豪、日、中、印、香港、シンガポール、韓国）で実施しました。IT 部門と業務部門の管理職以上（エグゼクティブ）1,279 人に対して実施したオンライン調査を、業界幹部への電話インタビューでさらに検証しました。Freeform Dynamics 社については www.freeformdynamics.com を参照ください。調査方法の詳細については、調査報告書『[Integrating Security into the DNA of Your Software Lifecycle](#)（ソフトウェア・ライフサイクルの DNA にセキュリティを統合する）』を参照してください。

本レポートの完全版およびその他のサポート資料は以下からダウンロードしてください：

- レポート：[Integrating Security into the DNA of Your Software Lifecycle](#)（英語）
- ブログ：[The Competitive Edge of DevSecOps](#) Ayman Sayed（英語）

CA Technologies について

CA Technologies (NASDAQ: CA) は、ビジネスの変革を推進するソフトウェアを提供し、アプリケーション・エコノミーにおいて企業がビジネス・チャンスをつかめるよう支援します。ソフトウェアはあらゆる業界であらゆるビジネスの中核を担っています。プランニングから開発、管理、セキュリティまで、CA は世界中の企業と協力し、モバイル、プライベート・クラウドやパブリック・クラウド、分散環境、メインフレーム環境にわたって、人々の生活やビジネス、コミュニケーションの方法に変化をもたらしています。CA Technologies の詳しい情報については、[〈http://www.ca.com/us.html〉](http://www.ca.com/us.html)(米 CA Technologies)、[〈http://www.ca.com/jp〉](http://www.ca.com/jp)(日本)をご覧ください。また、ツイッターについては、https://twitter.com/ca_japan をご覧ください。

***本文中に記載されている会社名、製品名は、各社の登録商標または商標です。**

この件に関する報道機関からのお問い合わせ先：

CA Technologies
〒102-0093 東京都千代田区平河町 2-7-9 JA 共済ビル 9 階
コーポレート・コミュニケーション部
TEL: 03-6272-8110 FAX: 03-6272-8115
e-mail : ca-pr@kyodo-pr.co.jp