

本当にもう脆弱性はない？

～ハッカーの力を借りるバグバウンティとは？～

はじめに（国内外で認知度が高まりつつあるバグバウンティ）

近年、バグバウンティやバグ報奨金制度という言葉をよく耳にするようになった。バグバウンティ（バグ報奨金制度）とは、企業が自社の製品やサービスに対する調査案件を公開し、世界中のホワイトハッカー（以降、ハッカーと呼ぶ）が、製品やサービスの脆弱性（バグ）を発見・報告することで、企業がハッカーに対して報奨金を支払う仕組みのことである。

バグバウンティの仕組み自体は、2000 年頃から存在していたが、ここ数年で、企業とハッカーが連携して脆弱性の発見に取り組むことに対する認知度が高まり、海外の IT 企業を中心に、バグバウンティを導入する企業が増えてきた。また、IoT やコネクテッドカー等の普及に伴い、自動車を含む製造業においても導入する企業が登場している。一方、日本国内では、IT 企業を中心に広まってきているものの、まだ認知度が低く、導入する企業が限られている状況である。

このように、国内外の企業がバグバウンティの導入を検討している中、ある企業のセキュリティ担当役員から、このような言葉が聞こえてくる。



セキュリティ
担当役員 A 氏

当社の製品は、リリース前に社内の脆弱性診断や外部の専門企業によるペネトレーションテスト等のセキュリティ検証活動によって十分に脆弱性を潰しているので、バグバウンティなど不要だろう。

そもそも、外部のハッカーに調査を依頼するなんて、当社の情報を公開するようなものだ。かえって悪用されるリスクがあるのでは？

A 氏の発言は、一見正しいように聞こえるが、ネットワークやシステムが複雑化するとともに、サイバー攻撃も日々高度化、巧妙化している昨今の状況において、開発工程の中でしっかりとセキュリティ検証を行ったからといって、「もう脆弱性は残っていない」と断言できるのだろうか。

本稿では、セキュリティ検証活動におけるバグバウンティの位置付けや仕組みを述べるとともに、バグバウンティプラットフォームを活用したバグバウンティの導入について紹介する。

バグバウンティのメリット

一般的なセキュリティ検証活動を整理すると、図 1 のように、テスト実施者に提供される情報量の少ない方から順に Black Box、Gray Box、White Box の 3 つに分類できる。Black Box では、活用情報は主に公開情報となり、内部的な設計情報が無い状態で行う攻撃者視点でのテストとなる。入手した情報を基に、攻撃シナリオを作成し、実際に攻撃を仕掛けて侵入につながる脆弱性や問題点の有無を確認する。一方の White Box では、仕様書・設計書等を基に、製品の内部構造を理解

した上で行う設計者視点でのテストである。例えば、設計者によるセキュリティ機能テストや、ソースコードレビューをはじめ、自動化ツールを用いたファジングテストや脆弱性診断等がある。最後に Gray Box であるが、Black Box と White Box の中間に位置し、第三者的な客観視点でのテストとしながらも、最低限の設計情報を提供することで、テストの効率性を高めることを可能とするものである。

テスト・検証活動の分類		視点	活用 情報	実施者数	主な活動	
少 テスト実施者に提供される情報量 多	Black Box	最低限の製品情報を踏まえて、製品の外側から見える機能を基に動作状況を確認	攻撃者	公開情報	多数	バグバウンティ
	Gray Box	Black／Whiteが混在	設計者	非公開情報	少数	ペネトレーションテスト／レッドチーム演習
	White Box	仕様書・設計書を基に内部構造を理解した上で、プログラムのロジックや制御の流れを確認				社内レビュー／各種テスト※ ※：ソースコードセキュリティ検査、 ファジング検査、 システムセキュリティ検査、 ウェブアプリケーション検査 等

図 1：既存のセキュリティ検証活動とバグバウンティの関係

バグバウンティは、このうち Black Box テストに位置する。攻撃者視点で対象のシステムに対して実際にサイバー攻撃を仕掛ける点はペネトレーションテストやレッドチーム演習と同様だが、セキュリティ人材と経済性の観点でメリットがある。

まずセキュリティ人材の観点では、ペネトレーションテスト等の担当者には高度なセキュリティの知識やスキルが求められることから人材の確保が難しく、仮に、組織内で人材が確保できたとしても、限られた視点での検証となるため、継続的な運用において属人化の問題が生じ、テスト品質が担当者に依存する場合がある。これに対してバグバウンティは、世界中の多数のハッカーが調査を実施することから、より多角的な視点での脆弱性の発見が期待できる。

次に、経済性の観点では、ペネトレーションテスト等は外部の専門企業に依頼することが多く、その場合、料金体系が人月ベースの工数となる。そのため、組織によっては、予算との兼ね合いで、限られた時間内に対象の細部まで検証することが困難となり、結果として対象範囲やテスト項目が制限され、限定的な検証となる場合もある。

一方、バグバウンティは、その期間内で受けた報告のうち、技術的な裏付けを確認できた報告のみに対する成果報酬である。そのため、当初想定した以上の脆弱性が見つかることで、計画以上の報酬を支払うことになるリスクはあるものの、成果の有無に関わらず一定額のコストが固定費として発生する方法（例：ハッキングのエキスパートの雇用や外部委託等）よりも効率的であり、運用上も継続しやすい。

このようなことから、既存の社内テストやペネトレーションテスト等だけでなく、これらを補完する手法としてバグバウンティを活用することで、想定もしなかった脆弱性の発見が期待できる。

バグバウンティ導入のハードルを下げるバグバウンティプラットフォーム

では、実際にバグバウンティを導入するにあたって、何をすべきだろうか。バグバウンティの導入には、全て自社で導入する方法と、バグバウンティプラットフォームを利用する方法の 2 つがある。全て自社で導入する場合、全ての企業で導入可能という訳ではなく、一般的に想定される予算の確保や社内各部署との調整等に加え、図 2 に挙げるような課題が導入のハードルとなる。

- 3/8

課題 1

報告者とのやりとりを行う窓口の構築
- Ω

課題 2

報告内容の検証、選別を行うセキュリティ人材の確保
- 📄

課題 3

各種規約（参加条件、制限・禁止事項、報奨金額、等）の整備

図 2：バグバウンティ導入における課題

図 2 の全ての課題について、自社内で対応する人材を確保した上で体制を構築するには相当の労力を要すると考えられる。ただし、近年、脆弱性を発見したい企業とハッカーをマッチングさせるバグ Bounty プラットフォームと呼ばれるサービスが登場し、上記課題への対応を代行している。バグ Bounty プラットフォームの仕組みについて図 3 に示す。

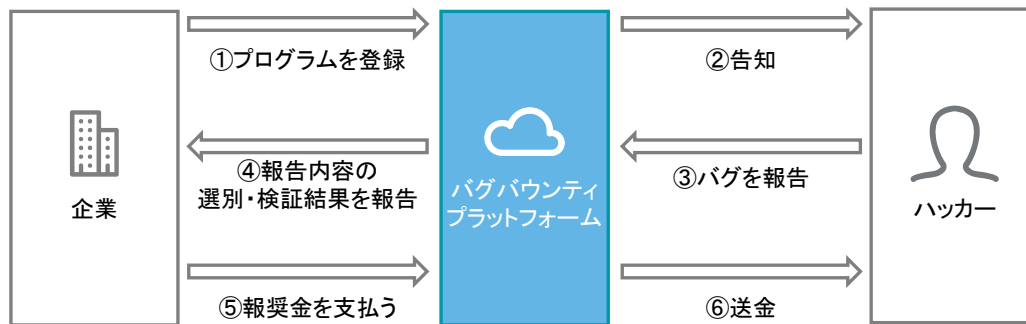


図 3：バグ Bounty プラットフォームの仕組み

バグ Bounty を自社で導入するかどうかは、社内のセキュリティ人材や予算との兼ね合いとなることが多いが、バグ Bounty プラットフォームを活用することで、上記の課題への対応の代行を依頼できるため、バグ Bounty 導入のハードルを下げるができる。

例えば、課題 1 において、企業は、報告者とのやりとりを行う窓口の構築が必要となるが、バグ Bounty プラットフォームは世界中のハッカーからの報告を一手に引き受ける（図 3 内の③）。また、バグ Bounty の参加者の多くは海外のハッカーであるため、それらの報告に対応するためには英語が必須となるが、国内向けのバグ Bounty プラットフォームも立ち上がり、言語の面での不安も払拭されつつある。

次に課題 2 について、脆弱性を発見したハッカーからバグ Bounty プラットフォームに対して報告が寄せられるが、バグ Bounty では、調査対象外となるシステムの脆弱性に関する報告や、不正確な内容の報告が寄せられることもある。

このような無効あるいは誤情報等の「ノイズ」となる報告を除外し、対処すべき脆弱性の報告を選別するには、単に労力を要するだけでなく、高度なセキュリティ知識を有する人材を確保する必要がある。バグ Bounty プラットフォームは、寄せられた報告からの有益な情報の選別や脆弱性の検証、それらを基にした助言等もサービスとして提供する（図 3 内の④）。

また、課題 3 のような各種規約についても定める必要があるが、実態としてハッカーに読まれないケースも多いため、特別のこだわりがない場合は、バグ Bounty プラットフォームにおいて共通化された規定を利用することで、独自に規定する労力を軽減することができる。

まずはプライベート形式の検討を

ここまで、バグ Bounty の導入におけるバグ Bounty プラットフォームの活用について述べたが、実際に、ハッカーに対して依頼するとなると、冒頭の A 氏の二つ目の発言のように、自社の製品やサービスに係る情報を不特定多数のハッカーに公開することになる等、心理的な抵抗がある。

そこでバグ Bounty プラットフォームは、企業からの依頼形式として、パブリック形式とプライベート形式の 2 つの形式を用意している。パブリック形式は、上述の不特定多数のハッカーに対して依頼する形式であるのに対し、プライベート形式は、プラットフォームに登録されているハッカーから、一定以上の評価を得ているハッカーだけを招待、または参加申込を経て受け付けられた人のみが参加できるものである。プライベート形式では、あらゆる側面が参加者以外に対して非公開となる。

多くの組織は、まずはプライベート形式のバグ Bounty から始め、バグ Bounty プラットフォームの使い勝手や、報告された脆弱性への社内の対応プロセスが有効に働くかを確認する。その上で、報奨金予算の予測や、社内調整を行い、パブリック形式へと移行する傾向がある。

以上を踏まえ、冒頭のセキュリティ担当役員 A 氏には次のような発言を期待したい。



セキュリティ
担当役員 A 氏

開発工程では、脆弱性診断等のセキュリティ検証を実施しているが、サイバー攻撃は日々進化するため、リリース後に新たなリスクにさらされることも十分考えられる。よって今後は、既存の検証だけでなく、念のため、バグバウンティも導入しよう。

社内リソースを踏まえると、バグバウンティプラットフォームを利用した方が良さそうだが、経験のない状況下で、不特定多数のハッカーに依頼するパブリック形式は情報統制の観点でリスクが高い。まずは実績のあるハッカーに依頼するプライベート形式を試してみよう。

IoT やコネクティッドカー等の普及に伴い、ネットワークやシステムが複雑化する中、サイバー攻撃も日々高度化、巧妙化しているため、新たな脅威や攻撃手法が登場し、いつ新たなリスクにさらされてもおかしくはない。そうしたリスクを一つでも減らすためにも、これからは企業自らハッカーと積極的に連携し、また、そうした姿勢が社会から評価されるようになることを望む。

デロイト・トーマツサイバー合同会社

Mail ra_info@tohatsu.co.jp
URL www.deloitte.com/jp/dtcy

【国内ネットワーク】 東京・名古屋・福岡

※貴社および貴社の関係会社とデロイト・トーマツグループの関係において監査人としての独立性が要求される場合、本サービス内容がご提供できない可能性があります。詳細はお問合せください。

デロイト・トーマツグループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト・トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト・トーマツ コンサルティング合同会社、デロイト・トーマツ ファイナンシャルアドバイザリー合同会社、デロイト・トーマツ 税理士法人、DT 弁護士法人およびデロイト・トーマツ コーポレート ソリューション合同会社を含む）の総称です。デロイト・トーマツグループは、日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約 30 都市以上に 1 万人を超える専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト・トーマツグループ Web サイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ・トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人のひとつまたは複数指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよびそれらの関係法人はそれぞれ法的に独立した別個の組織体です。DTTL はクライアントへのサービス提供を行いません。詳細は www.deloitte.com/jp/about をご覧ください。デロイト アジア パシフィック リミテッドは DTTL のメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける 100 を超える都市（オークランド、バンコク、北京、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務およびこれらに関連するプロフェッショナルサービスの分野で世界最大級の規模を有し、150 を超える国・地域にわたるメンバーファームや関係法人のグローバルネットワーク（総称して“デロイトネットワーク”）を通じ Fortune Global 500® の 8 割の企業に対してサービスを提供しています。“Making an impact that matters”を自らの使命とするデロイトの約 312,000 名の専門家については、（www.deloitte.com）をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。

Member of
Deloitte Touche Tohmatsu Limited

© 2020. For information, contact Deloitte Tohmatsu Cyber LLC.