民間での脆弱性コーディネーションの最前線

～バグ報奨金制度の現状と展望～

株式会社スプラウト

BugBounty.jpチーム　小西 明紀

Introduction

Cyber Security Labs sprout ＝ サイバーセキュリティ 技術×情報

スプラウトは、通称ホワイトハッカーと呼ばれるセキュリティエンジニアを中心に、情報通信分野に精通したコンサルタントやリサーチャーらで構成されるサイバーセキュリティの専門家集団です。

世界トップクラスの「Cyber Security & Intelligence Company」を目指して、調査・研究・開発に取り組んでいます。

Introduction

日本初のバグ報奨金プログラムのプラットフォーム

BugBounty.jp powered by sprout

参加企業は、自社のウェブサービスやアプリケーションにバグや脆弱性が潜んでいないかどうかの調査を、世界中のホワイトハッカーに依頼することができます。

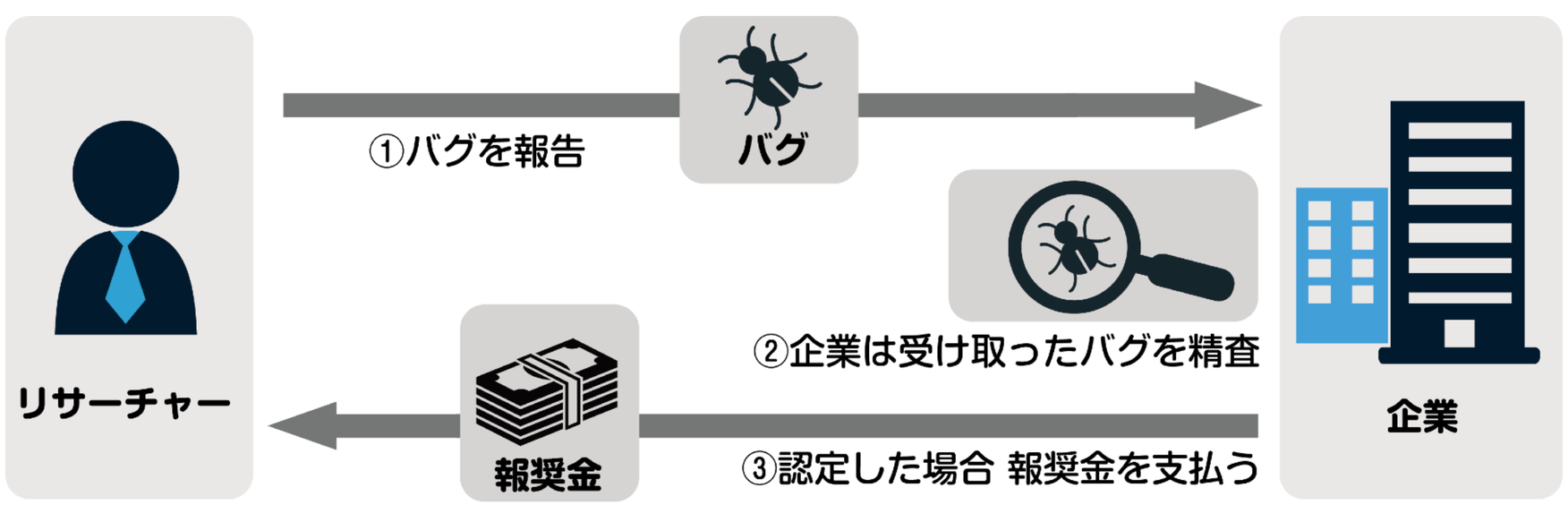
本当の“悪意あるサイバー攻撃”を受ける前に、是非セキュリティ対策の一つとしてご活用ください。

定期的に導入セミナーを開催中！
https://bugbounty.jp/

バグ報奨金制度とは

バグ報奨金制度とは

バグ報奨金制度とは、セキュリティ上問題となる欠陥（脆弱性）発見を世界中のハッカーに依頼し、発見されたバグの重要度に応じて、報奨金を支払う仕組み



バグ報奨金制度の歴史

mixi　LINE

cybozu　BugBounty.jp powered by sprout

1995 → 2004 → 2010 → 2012 → 2014 → 2016

Netscape　mozilla FOUNDATION　Google　hackerone　GitHub

iDEFENSE　ZERO DAY INITIATIVE　facebook　Microsoft　UNITED

PWN2OWN　bugcrowd　Dropbox

バグ報奨金制度の運営形態

自社運営

自社で企画・運営を行う

LINE　Microsoft　Google　facebook

クラウド利用（バグ報奨金プラットフォーム）

バグ報奨金制度の運営をサポートするクラウドサービス
を利用する

BugBounty.jp powered by sprout　hackerone　bugcrowd

スポンサー運営（クラウド利用あり）

インターネット上で影響力の大きい製品に対して、
スポンサーが資金・プラットフォームを拠出し運営を行う

対象プログラム

Apache httpd
php
OpenSSL

スポンサー

Microsoft
facebook

バグ報奨金制度の特徴

- 一般的なセキュリティ診断とバグ報奨金制度の差を比較すると、両者の目的は同じだが、多くの面で異なっている

- 診断が苦手とする部分をバグ報奨金制度は、補完することが可能

一般的なセキュリティ診断		バグ報奨金制度
成果にかかわらず一定	コスト	成果報酬制
コストの観点から難しい	継続性	成果報酬のため継続しやすい
担当の診断員に依存しがち	属人性	世界中のハッカーが実施
高	網羅性	不透明
監査証明として有効	監査性	監査証明としては弱い

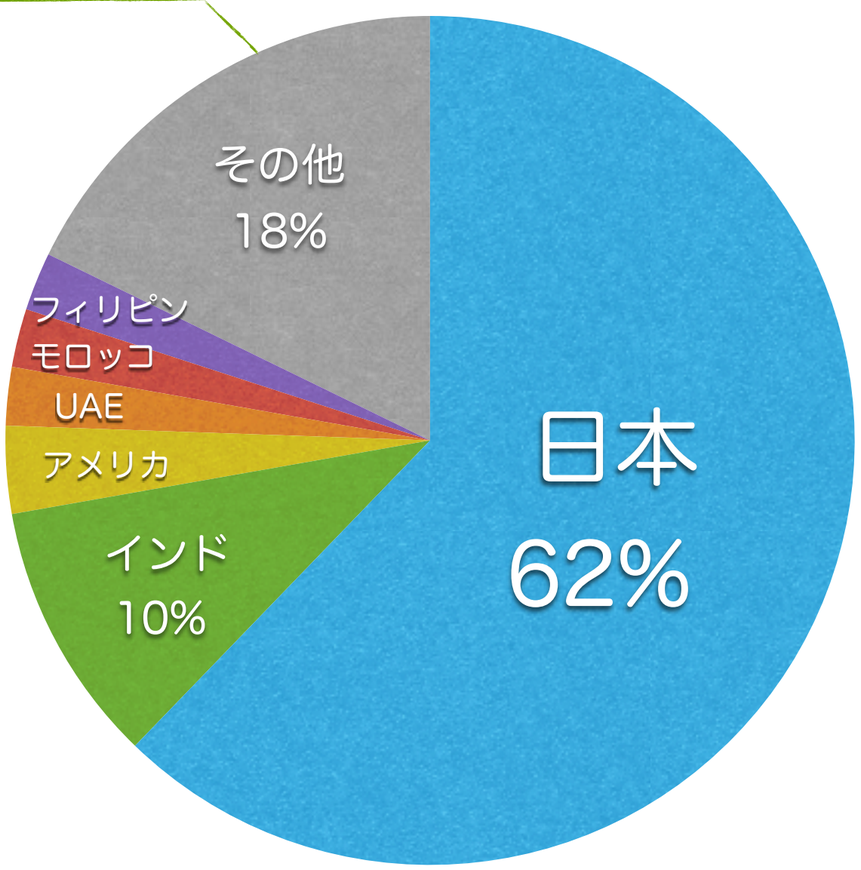
バグ報奨金制度の最前線

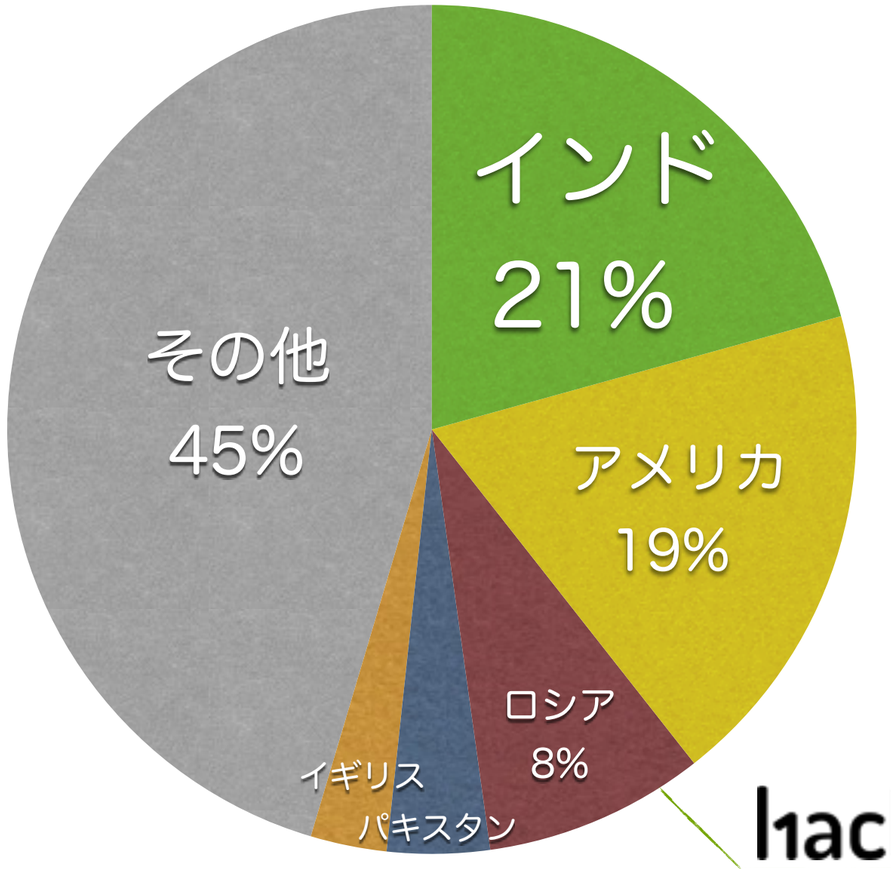
バグ報奨金制度の最前線

- ✓ 品質
- ✓ 実績
- ✓ コスト
- ✓ 脆弱性流通
- ✓ 運用手法

品質 ～リサーチャーの国別割合～

BugBounty.jp powered by sprout





hackerone

2016

https://hackerone.com/blog/bug-bounty-hacker-report-2016 を参照

品質 ～リサーチャーの質～

有効レポート率

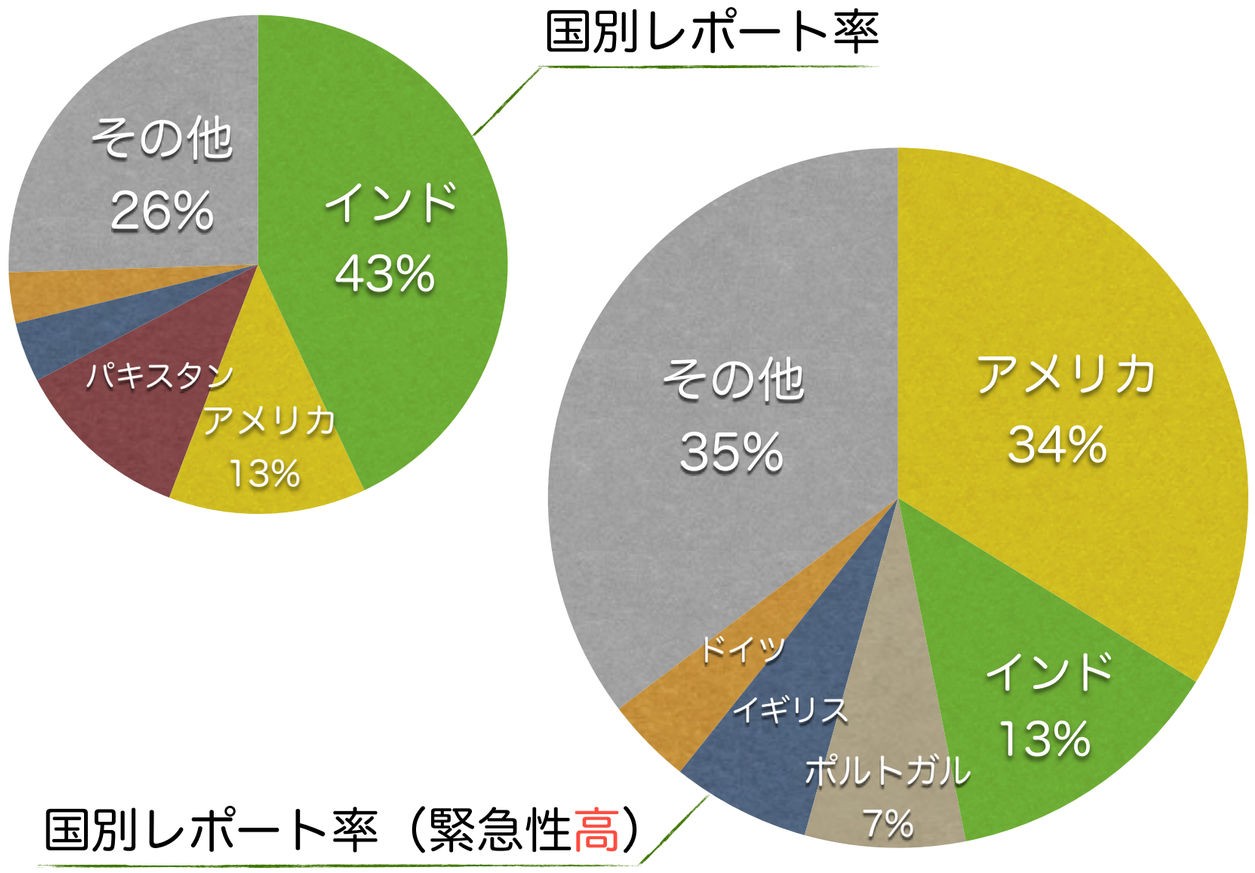
BugBounty.jp powered by sprout　45%

Cyber Security Labs sprout　30%

A社　44%

B社　49%

国別有効レポート率（Bugcrowd）



https://blog.bugcrowd.com/bugcrowds-second-annual-state-of-bug-bounty-report を参照

バグ報奨金制度の最前線

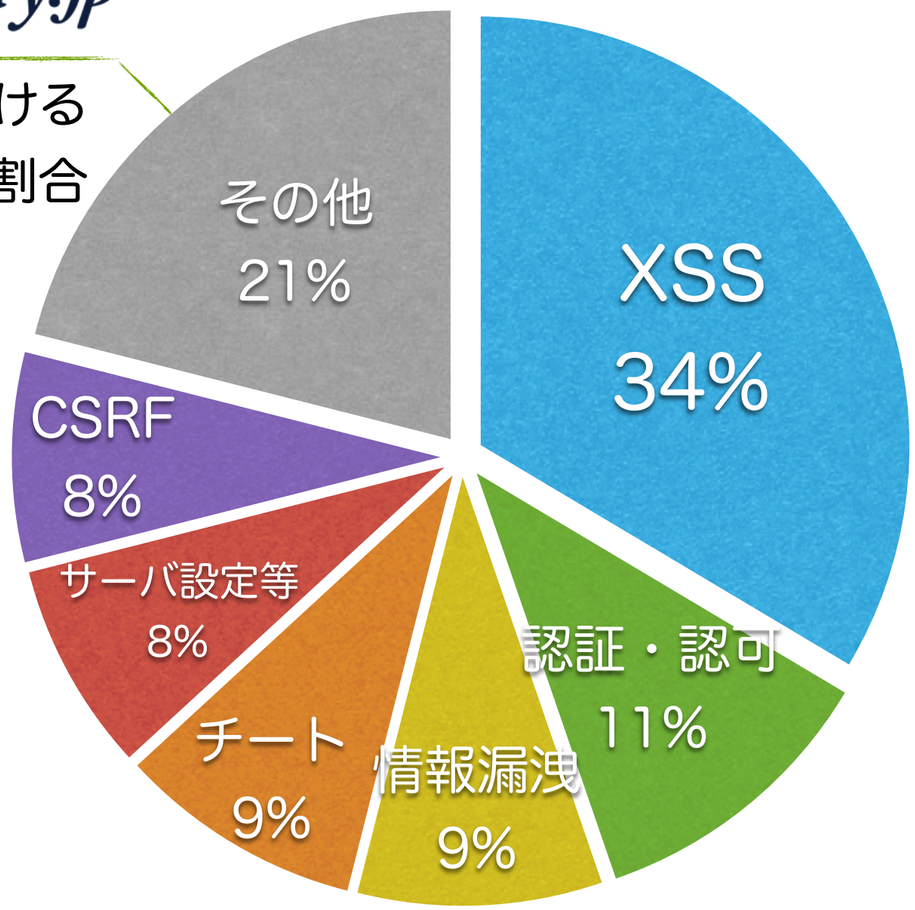
- ✓ 品質
- ✓ 実績
- ✓ コスト
- ✓ 脆弱性流通
- ✓ 運用手法

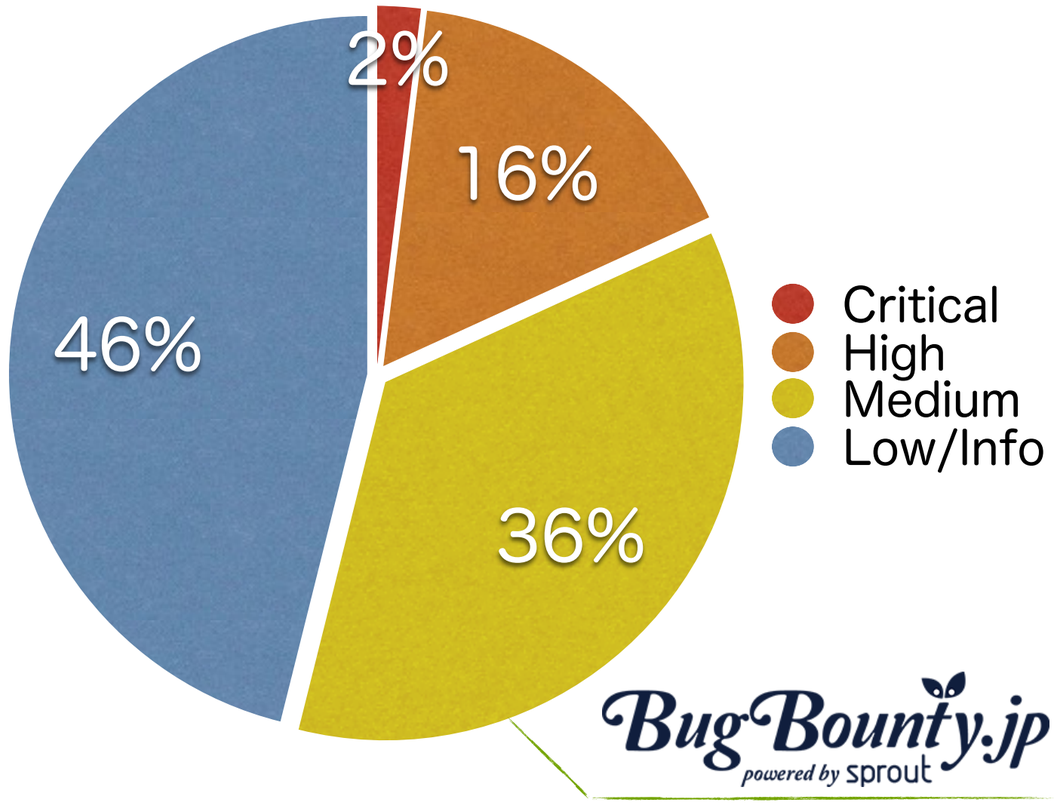
Cyber Security Labs sprout

実績 ～どんな脆弱性が報告されるか～

BugBounty.jp powered by sprout

有効報告数における
脆弱性タイプの割合





BugBounty.jp powered by sprout

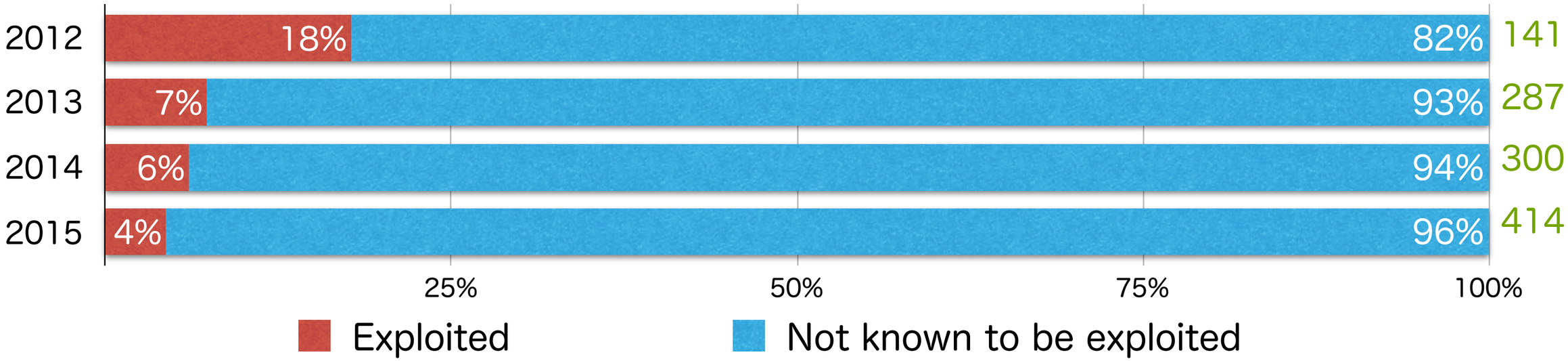
有効報告数における
危険度の割合

2016

実績 ～どれだけリスクが軽減されているのか～

脆弱性が利用された場合のリスクを算出することで、数値化することは可能
しかし、悪用されなければリスクが顕在化しないという現実もあり不透明

クリティカルな脆弱性全体における悪用された割合（Microsoft）



https://pacsec.jp/psj16/PSJ2016_Akila_Srinivasan-Microsoft_bug_bounty-publish.pdf を参照

成果を数値化するのは難しいが、悪用されうる脆弱性は確かに減っている

バグ報奨金制度の最前線

- ✓ 品質
- ✓ 実績
- ✓ コスト
- ✓ 脆弱性流通
- ✓ 運用手法

Cyber Security Labs sprout

コスト ～報奨金額～

	Google	UBER on hackerone	LINE	Cyber Security Labs sprout on BugBounty.jp powered by sprout
XSS	$7,500	$5,000	$500	$500
Authentication Bypass	$10,000	$10,000	$5,000	$2,000
SQL injection	$10,000	$10,000	$3,000	$2,000
Remote code 実行	$20,000	$10,000	$10,000	$5,000

実施側の裁量で決定してよいが、報奨金額がリサーチャーへの訴求力となる

コスト ～支払額～

BugBounty.jp powered by sprout

104 万円

23 万円

31 万円

B社

A社

Cyber Security Labs sprout

cybozu

2016

447 万円

730 万円

2015

2015

150 万ドル↑

200 万ドル↑

Google

2016

https://security.googleblog.com/2016/01/google-security-rewards-2015-year-in.html 、 https://security.googleblog.com/2015/01/security-reward-programs-year-in-review.html
http://blog.cybozu.io/entry/2016/04/22/080000 を参照

バグ報奨金制度の最前線

- ✓ 品質
- ✓ 実績
- ✓ コスト
- ✓ **脆弱性流通**
- ✓ 運用手法

脆弱性流通 ～発見した脆弱性をどこへ？～

脆弱性流通形態

公的コーディネーター … 国家・公的な機関に運営される脆弱性コーディネーション組織へ報告する。報告者の貢献は示される

各企業の窓口 … 当事者が設置した窓口へ報告。無報酬または報奨金という形で買い取られる

即時公開 … 通告・警告の有無に関わらず、パッチ前に即時公開する

高額売買 … 民間の買取業社、またはダークウェブなどを通じて売却する

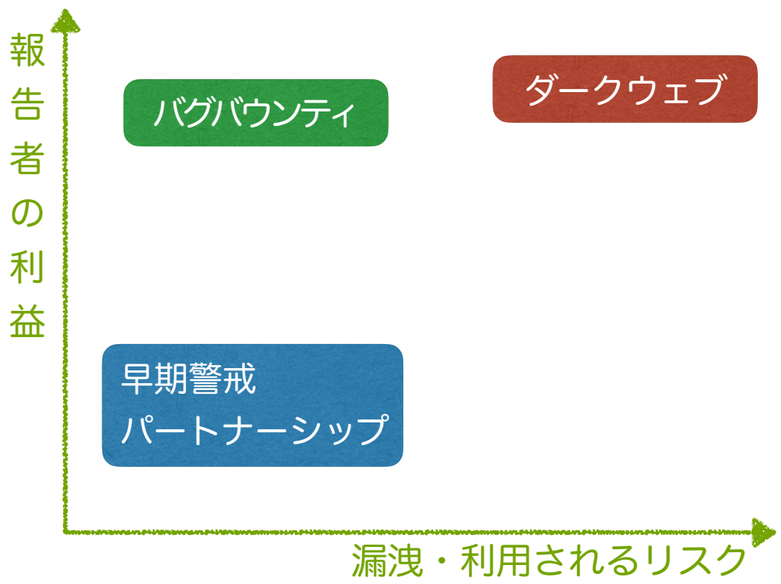
公開しない … 公開せず、発見者が保持。適宜利用することも想定される

脆弱性流通 ～どこに流すのがいいのか～

早期警戒
パートナーシップ … IPAおよびJPCERT/CCによって運用される、脆弱性報告窓口へ報告

バグバウンティ … 自社に窓口を設け、脆弱性を適切な価格で買取る

ダークウェブ … ダークウェブ内のサイトで売買



企業の窓口を設けて、脆弱性を買取る

脆弱性を報告する側の立場

リスクなく調査できる ＆ 報奨を得られる

脆弱性を報告される側の立場

漏洩リスク減 ＆ 公開しなくてもよい

脆弱性流通 ～脆弱性を公開する意義～

全体

脆弱性を報告する側の立場

- 広く危険性を警告したい
- 自らの正当性を問いたい
  # 企業との立場に違いがある場合
- 活躍を示したい

脆弱性を報告される側の立場

- 基本的に公開したくない
- 製品利用者（顧客）への警告義務
- リサーチャーとの関係を良好に維持したい

- インターネット上のリサーチャー＆開発者、双方の教育資産となる
- 脆弱性情報が広く告知されることで、利用者のリスクも低減される

脆弱性公開は、大きな目でみると、リスクを低減する方向に働く

バグ報奨金制度の最前線

- ✓ 品質
- ✓ 実績
- ✓ コスト
- ✓ 脆弱性流通
- ✓ 運用手法

Cyber Security Labs sprout

運用手法 ～PublicとPrivate～

バグ報奨金制度の実施形態

Public … 制限を設けず、世界中のリサーチャーに広く調査を依頼

Private … 特定のリサーチャーだけに調査を依頼

PublicとPrivateの併用

運用初期の安全性向上＆ノイズの低減によって、デメリットを補う

運用手法 ～ソリューションハイブリッド～

様々なセキュリティソリューション＆サービス

- Vulnerability Scanner
- Pen-Testing with security company
- Crowdsourced Pen-Testing

× Bugbounty

Crowdsourced Pen-TestingとBugbountyの併用

Crowdsourced Pen-Testing → Private / Public

バグバウンティのリサーチャーへ依頼
高度なスキルを持つハッカーによる網羅的な診断
大規模な更新時には必ず実施

継続的に実施
細かいシステム更新による脆弱性をハンドリング

Bugbountyリソースを利用した診断で網羅性・継続性を確保

バグ報奨金制度の向かう先

今後の展望

- 脆弱性の市場は拡大し続ける
- 無視するか、倫理観に頼るか、買い取るか
- バグ報奨金制度の実施はもはやデファクト
- 訴求力のあるバウンティプログラムを
- すべての企業が導入できるわけではない
- 導入を促し、支援する取り組みも必要

ご静聴ありがとうございました！

BugBounty.jpに関するお問い合わせ

bugbounty@sproutgroup.co.jp