ソースコード漏洩事案について

～組織のDXを止めないために～

一般社団法人コンピュータソフトウェア協会

Software ISAC

2021年2月

何が起きたのか？

- 発生事象
  - 金融機関のシステムに関連するソースコードが「GitHub」上に公開されていた。
  - 委託先企業のエンジニアからの情報流出。
  - 「転職の準備のために現在あるコードを全てアップした」というTwitterでの発言。
  - 自身の年収を予測するために、ソースコードを解析させ診断しようとしていた。
  - 一時公開されていたソースコード群からは、他の企業や公的機関に関連する情報も確認された。

（参考）GitHubとは

- ソフトウェア開発プロジェクトに用いられる、ソースコード管理サービスで、ソースコードの閲覧やバク管理、タスク管理、メモやコミュニケーションなどを行うにあたって欠かすことのできないクラウドサービスです。

本事案を適切に理解するための背景

- 日本の産業構造の象徴ともいえるのが「多重下請け構造」（≒サプライチェーン）であり、委託や再委託を行わないとソフトウェア開発は行えない現実。
- DXを推進することは、ソフトウェアを開発・活用することでもあり、ソフトウェア開発はDXの根幹とも言える。
- 「クラウドバイデフォルト」とも政府も含めて発信をしているように、クラウドサービスは様々な環境（開発環境含む）においても使用することが前提となっている。
- 「クラウド」環境は言わば「場」（公園のようなもの）であり、その使い方は利用者の使い方、すなわち設定やリテラシーなどに依存する。
- GitHubはソースコードを共有し合うサービスであり、ソフトウェア開発に求められるスピードや質の観点からも欠かすことのできないサービスである。（いわば、複雑なプラモデルのパーツが公開、共有され、それを共に組み上げていくイメージ。すなわち、このようなプラットフォームが使えないのであれば、その「パーツ自体も自分たちで作り、連携せずに完成させよ」と言っているのに近しい。）
- いつの時代も道具は使い方次第で、便利にもなれば、悪用されることもある。

「GitHubを使うな」≒「開発するな」「DXを止めろ」

組織はどのように向き合うべきか？

- 経営者は、DXを積極的に推進するとともに、DXの根幹にはソフトウェア開発があることや、その開発の環境やプロセスなどの現状を理解する。
- 組織は、サプライチェーンをできる限り把握するとともに、委託元も委託先も相互に協力して、ソフトウェア開発の安全性に努める。
- 組織は、クラウドサービスなどを利用するにあたっては、規約や設定などを理解し、対応を検討、実施した上で用いる。（特に情報公開や共有等に関する設定には注意する。）
- 組織として、リスクを回避（クラウドサービスなどを使用しないと）するだけではなく、低減、移転、そして特に受容についてステークホルダーで議論、理解し、共通認識を持つようにする。
- 道具（ツールやサービス等）を利用することは「人」であることを理解し、常にリテラシーの向上や教育を実施し、「人」に起因するセキュリティ事故をなくす（最小限にする）ようにする。
- セキュリティ事故が発生することを想定し、迅速かつ的確に対応できる体制を確保する。
- 組織内外の開発エンジニアへの敬意を示すとともに、働き方（環境、待遇、ワークバランス等）の改善に継続して努める。

社会全体として考えるべき課題

- クラウド前提社会の活用方法の理解
  - クラウドサービスの規約を理解した上で、インシデントを想定した利用が出来ているか
  - クラウドサービス利用にあたっての、組織としてのポリシーや利用する人のリテラシーなど、組織としての対応が行えているか。

- デジタル社会の根幹になるソフトウェアの安全性の確保
  - 開発する環境（プラットフォームなどの環境）の安全性
  - 開発する人材の安全性（リテラシーやモラル）
  - 開発するソフトウェアそのものの安全性（OSSの利用等）

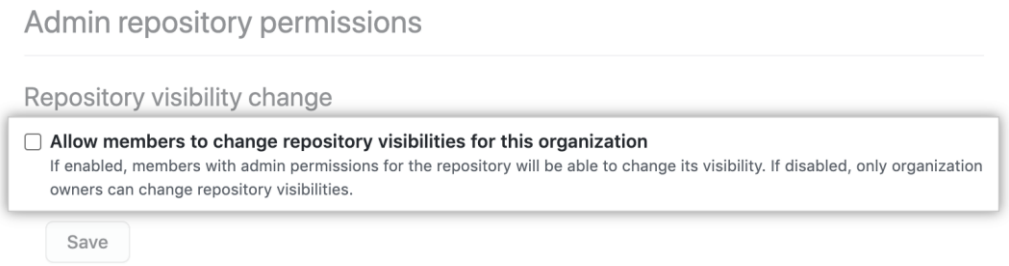
- ソフトウェア開発を行う人材の「量」と「質」の確保
  - エンジニアの確保
  - エンジニアのリテラシー向上
  - エンジニアの継続的なスキルアップ

今回の事案に対する対策について①

- GitHubの設定を確認する。（次スライド）
  - 設定変更を行える人を限定する。
    （委託先には権限を付与しないことなどを検討する。）
  - 自由に作成できないように設定する。
- メンバーを管理する（削除や復帰等、定期的に見直す）。
- 定期的に公開設定状況を確認する。
- 万が一、情報漏洩が発生した場合に備えて、対処できる体制（PSIRT）等を整備する。
- なお、このようなツールを使う場合は、事前に協議し、遵守事項として契約することが望まれる。

今回の事案に対する対策について②

- Organization内のリポジトリの可視性設定の確認
  - リポジトリの可視性変更の権限を設定する



- Organization 内でリポジトリを作成するための権限を設定
  - メンバーのリポジトリ作成可否を設定する