SANS

アプリケーションセキュリティ調達基準

はじめに

一般に、ほとんどのセキュリティ事件・事故（悪意あるユーザが、他人のコンピュータを乗っ取るような事象）の根幹にある原因は、設定の問題と不適切なコンピュータコードという 2 つの問題のいずれかである。特に、不適切なコードの重大性が増している。2000 年 2 月、ホワイトハウスで行われたクリントン大統領とインターネットおよびソフトウェア専門家との会談において、Mudge と名乗るハッカーは大統領に次のように述べている—「ソフトウェアがずさんに開発されている。発売前に、ソフトウェアの誤りを検出するための検査すら行われていない」。それから約 9 年が経過したが、犯罪者や国家によるバグの多いソフトウェアへの攻撃が増す一方である以外、ほとんど変化は見られない。

本資料は、他の 2 つの構想と併せて、ソフトウェアの購入者とユーザがこうした状況に対処するための第一歩となるべきものである。本資料の活用により、カスタムソフトウェアの購入者は、ソフトウェア納入前にコードの検査とセキュリティ上の弱点の修正をコード作成者の責任で行うよう求めることができる。2 番目のプロジェクト「CWE/SANS Top 25」では、最も深刻なセキュリティ問題の原因となるプログラミングエラーに順位を付けて発表している（http://cwe.mitre.org/top25/）。3 番目のプロジェクトである GSSP アセスメントでは、プログラマに安全なコードを作成できる知識があるか雇用者が確認できる（www.sans.org/gssp）。

本資料は、必要に応じて改訂される。本資料の内容の改善および最新情報の反映に関するご意見は、procurement@sans.org までお送りいただきたい。

第一著者 / 寄稿者

Will Pelgrin, CSO New York State
Jim Routh, CISO, Depository Trust and Clearing Corporation
Jeff Williams, Aspect Security

この調達ガイドライン案には、『OWASP Secure Software Contract Annex』の大部分の基準が盛り込まれている点にご注意いただきたい。OWASP 基準は、次のサイトより無償で入手できる。

https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

質問 / コメント

質問やコメントがある場合、またはベストプラクティスや実際の契約を共有する意向がある場合は、spa@sans.org までご連絡いただきたい。

2009 年 1 月

アプリケーションセキュリティ調達基準

I. 概要

ベンダーは、本契約の有効期間中のソフトウェア開発において、以下の契約条件を含む一般的な業界標準に準拠して最大限の安全管理を行うことに同意する。

本契約は、第三者の請負業者とその下請け業者、およびベンダーにより雇用されたその他の事業体を含む、ソフトウェア開発に関わるあらゆる当事者のセキュリティ関連の権利および義務を明確にするものである。

ベンダーは、本契約の条項がベンダーの従業員、およびベンダーにより本契約のために雇用される第三者の請負業者とその下請け業者にも適用されることに、書面にて同意するものとする。

ベンダーは、購入者が運用するソフトウェアの脆弱性が露呈する可能性を抑制するため、セキュリティ上の問題および関連文書に関する情報の保護に必要なあらゆる措置を実施するものである。

ベンダーは、本契約の条項に準拠し、セキュリティ上の重大な問題を可能な限り迅速に解決するため、完全に安全なソフトウェア開発に向けた適用可能な最高の業界標準を採用するものである。「適用可能な最高の業界標準」とは、「対象となる分野において技術的な専門知識を有した、業務に従事する堅実な従業員が、業務において適切に注意を払うことによって、技量や効率を遺憾なく発揮する環境」とすることができる。

作業者

ベンダーは、本契約期間におけるアプリケーションの開発、管理、および更新のプロセス全体のセキュリティの責任担当者を書面にて指名する。指名される担当者は、上級テクニカルセキュリティ専門家 1 名であり、プロジェクトのセキュリティリーダーと呼ばれる。セキュリティリーダーは、各成果物のセキュリティを書面にて保証する。

セキュリティトレーニング

ベンダーは、開発チームのメンバー全員がセキュアプログラミング技術のトレーニングを適切に受けていることを確証する責任を負う。

契約締結前に、ベンダーは、アプリケーション開発者がアプリケーション開発に先立って受講したトレーニングコースを含むプロセスを文書化する。

契約締結前に、ベンダーは購入者に対し、本契約に関わるすべてのアプリケーション開発者が、セキュアアプリケーション開発における適切なレベルのトレーニングを正式に受け、アプリケーションセキュリティの能力認定試験に合格していることを保証する。

開発者の身元調査

ベンダーは、開発チームのメンバー全員に対して適切な身元調査を実施し、本契約およびソフトウェア開発プロセスに関わるすべての個人が身元調査で問題がないことを保証する。

脆弱性、リスク、および脅威

ベンダーは、ソフトウェアライフサイクルにおいて可能な限り早期の時点で脆弱性、リスク、および脅威を割り出すよう努力することを書面にて同意する。ソフトウェアライフサイクルとは、当該アプリケーションの開発、管理、更新からアプリケーションの使用期間の終了までを意味する。

ベンダーは、アプリケーションにより提供される機能や重要な資産における主なリスクを特定する。ベンダーは、添付資料における最も一般的なプログラミングエラー25 項目の分析を実施し、これらのエラーが低減されていることを書面にて記録する。ベンダーはリスク評価を実施し、リスクを判別して優先順位を付け、脆弱性を列挙して特定の攻撃がアプリケーションに及ぼす影響を理解し、当該契約義務、法規定、およびセキュリティのベストプラクティスと標準に準拠していることを保証する。

ベンダーは、アプリケーションの脆弱性、リスク、および脅威が特定された時点で速やかかつ完全に、これらに関するあらゆるセキュリティ関連情報を書面にて購入者と共有する。このようなセキュリティ文書には、セキュリティ設計、リスク分析、または問題を記述する。

アプリケーション開発

契約締結前に、ベンダーは購入者に対し、アプリケーション開発、パッチ管理、および更新のプロセスを詳述した文書を書面にて提出する。この文書では、ソフトウェアを安全に開発、保守、および管理するためにプロセスの各レベルで講じる手段を明確に指定する。

ベンダーは購入者に対し、すべてのセキュリティ関連設定オプションと、これらのオプションがソフトウェアの全体的なセキュリティに及ぼす影響を詳細に記述した、安全な設定に関するガイドラインを書面にて提出する。このガイドラインには、オペレーティングシステム、Web サーバ、およびアプリケーションサーバを含む対応プラットフォームにおける依存関係と、セキュリティを確立するための設定方法を詳述する。ソフトウェアのデフォルト設定は安全(セキュア)でなければならない。

契約締結前に、ベンダーは購入者に対し、準拠する業界セキュリティ標準と対処レベルを書面にて明記する。

契約締結前に、購入者はベンダーに対し、アプリケーションソフトウェアライフサイクルにおいて適用されるその他のセキュリティ標準と対処レベルを書面にて明記する。

ベンダーは、前記の標準と対処レベルに準拠することに書面にて同意する。ベンダーは購入者に対し、各セキュリティ要件の達成に向けた設計を明確に記述した文書を書面にて提出する。ベンダーは安全なコーディングのガイドラインを策定してこれに準拠する。このガイドラインは、コードの形式、構成、およびコメント方法を定めるものである。すべてのセキュリティ関連コードには、詳細なコメントを付けるものとする。一般的なセキュリティの脆弱性を回避するための特定のガイダンスも組み込む。また、コードテストに向けた準備段階として、少なくとも 1 名の開発者がすべてのコードをセキュリティ要件およびコーディングのガイドラインと突き合わせて評価する。

II.開発環境

(a) セキュアコーディング

ベンダーは、セキュアコーディングを促進するためソフトウェア開発環境で使用するツールを公開する。

(b) 設定管理

ベンダーは、チームメンバーを認証すると同時に、ソフトウェアベースラインや関連するすべての構成ファイルおよびビルドファイルの変更を記録するソースコード管理システムを使用する。

(c) ディストリビューション

ベンダーは、ソースから完全な配布ソフトウエアを確実にビルドするビルドプロセスを用いる。このプロセスには、クライアントへ納入するソフトウェアの完全性を検証する手法が含まれる。

(d) 開示

ベンダーは購入者に対し、ソフトウェアに使用したすべてのサードパーティソフトウェアを書面にて文書化する。サードパーティソフトウェアには、商用、無償、オープンソース、およびクローズドソースのすべてのライブラリー、フレームワーク、コンポーネント、およびその他の製品が含まれる。

(e) 評価

ベンダーは、サードパーティソフトウェアが本契約のすべての条項に対応しており、本契約に従って開発されるカスタム開発コードと同様に安全であることを保証するため、合理的な努力を行うものとする。

III.テスト

(a) 概要

ベンダーは、テスト手法または各セキュリティ要件に対応していることを証明する手法を規定したセキュリティテストプランを提出し、このプランに従って作業を進めるものとする。このテストプロセスの厳密度をプランで詳述する。ベンダーはセキュリティテストプランを実施し、テスト結果を書面にてクライアントに提出する。

(b) ソースコード

ベンダーは購入者に対し、アプリケーション開発ライフサイクルプロセスにおいてソースコードの評価を行い、セキュリティ標準、ポリシー、およびベストプラクティスを含む本契約の要件に従っていることを書面にて保障することに同意する。ベンダーは、コード評価実施の手順とフレームワークを適切に文書化する。

(c) 脆弱性および侵入テスト

ベンダーは、本稼働前にアプリケーションに対し脆弱性および侵入テストを実施することに書面にて同意する。

本稼働後に、ベンダーはテスト段階でシステムのセキュリティが侵害されていないことを検証するため、契約に基づいて合意されたセキュリティスキャンを（最新のシグネチャファイルを用いて）実施する。

ベンダーは購入者に対し、スキャンおよびテストの結果と、緩和プランを記述した文書を書面にて提出する。

ベンダーは、事前交渉にて定められた期間内にこれらの脆弱性を緩和することに書面にて同意する。

パッチおよび更新

ベンダーは、ソフトウェアライフサイクルを通じたパッチ管理プロセスでの識別に従い、事前交渉にて定められた期間内にセキュリティに影響するパッチおよび更新を通知する。

ベンダーは、配布前アプリケーションのテストバージョンで、適切なパッチ、更新、および回避策を適用、テスト、検証する。

ベンダーは、すべての更新がテストされ、本稼働前にインストールされていることを検証し、文書化し書面にて提出する。

ベンダーは、事前交渉で定められた手順に基づき、パッチ更新完了時にアプリケーションの機能を検証し、検証結果を文書化して提出する。

セキュリティ問題の追跡

ベンダーは、ソフトウェアライフサイクル全体において判明したすべてのセキュリティ問題(要件、設計、実装、テスト、配備、運用の問題を含む)を追跡する。セキュリティ問題の検出後、可能な限り迅速に各問題に伴うリスクを評価して文書化し、購入者に報告する。

IV.セキュアアプリケーションの納入

ベンダーは、開発プロセスにおいて作成されたセキュリティ文書で構成される「保障パッケージ」を提出する。このパッケージにより、セキュリティに関する要件、設計、実装、およびテスト結果がすべて適切に履行されており、セキュリティ問題がすべて適切に解決されていることが立証される。

ベンダーは、納入前に判明したセキュリティ問題をすべて解決するものとする。納入後に判明したセキュリティ問題は、本契約に定められているその他のバグおよび問題と同様の方法で処理されるものとする。

自身による記載内容の確認

セキュリティリーダーは購入者に対し、ソフトウェアがセキュリティ要件を満たしており、すべてのセキュリティ活動が実施され、判明したセキュリティ問題がすべて文書化され解決されていることを書面にて証明する。証明する状況に関する例外はすべて文書に詳述し、納入時に提出するものとする。

有害コードが含まれていないことの保証

開発者は、ソフトウェア要件に対応しておらず、アプリケーションのセキュリティを侵害するコード(コンピュータウィルス、ワーム、ロジックボム、バックドア、トロイの木馬、イースターエッグ、およびその他のあらゆる形態の有害コード)が含まれていないことを保証する。

V. セキュリティの受け入れおよび保守

受け入れ

ベンダーの保障パッケージが完成し、セキュリティ上のすべての問題を解決した時点で、ソフトウェアが受け入れられる。

セキュリティ問題の調査

受け入れ後にセキュリティ問題が検出、または合理的に疑われる場合、ベンダーは問題の性質を判別するための調査において購入者を支援するものとする。

日本語訳:NRI セキュアテクノロジーズ株式会社