脆弱性体験学習ツール「AppGoat」を用いた
集合教育実施の手引き

独立行政法人情報処理推進機構
セキュリティセンター

目次

はじめに

本書は、脆弱性体験学習ツール「AppGoat」のウェブアプリケーション用学習ツールを用いて集合教育を行う際の効果的な教育方法や段取り、注意点についてまとめた手引書です。

本書の想定する読者
・脆弱性体験学習ツール「AppGoat」のウェブアプリケーション用学習ツール（集合学習モード）を用いて集合教育を行う組織内の教育担当者(人事部)、学校の先生(教授)。

用語一覧

用語	説明
AppGoat	脆弱性体験学習ツール。学習教材と演習環境をセットにし、ウェブアプリケーションの脆弱性の検証手法から原理、影響、対策を学習することができます。
管理者	集合教育を計画し、集合教育のための準備を行う人。例えば、講師や教師を想定しています。
学習者	集合教育を受講する人。従業員や生徒、セミナー参加者を想定しています。
集合学習モード	管理者 PC に AppGoat をインストールして学習するモード。
個人学習モード	管理者および学習者 PC に AppGoat をインストールして学習するモード。

1.AppGoat とは

脆弱性体験学習ツール「AppGoat」（以降、AppGoat）は、脆弱性の概要や対策方法等の脆弱性に関する基礎的な知識を実習形式で体系的に学べるツールです。学習者は、学習テーマ毎に用意された演習問題に対して、埋め込まれた脆弱性の発見、プログラミング上の問題点の把握、対策手法の学習を対話的に実施できます。

AppGoat には、以下の 3 種があります。

・ウェブアプリケーション用学習ツール（集合学習モード）
・ウェブアプリケーション用学習ツール（個人学習モード）
・サーバ・デスクトップアプリケーション用学習ツール

本書ではこれら 3 種の内、「ウェブアプリケーション用学習ツール（集合学習モード）」（以降、集合学習モード）に焦点を当て、これを用いた集合教育の実施方法について説明します。

集合学習モードは、**官公庁、ソフトウェア開発企業、教育機関（大学や高等専門学校など）でご利用頂いております。**

なお、個人学習モードを用いた集合教育も可能です。集合学習モードおよび個人学習モードの教育のイメージおよび違いについて以下に示します。また、個人学習モードを使って集合教育を行う場合の考慮点については別紙 1 で紹介します。

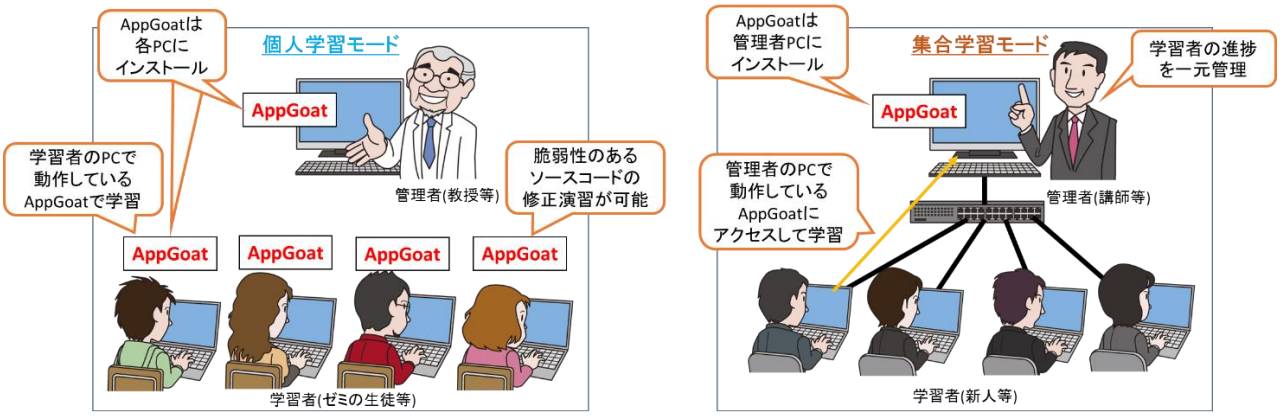

図 1.1：各モードの教育のイメージ

表 1.1：各モードの違い

	個人学習モード	集合学習モード
AppGoat のインストール対象	管理者 PC・学習者 PC	管理者 PC※
学習可能人数	制限無し	40 名程度
ネットワーク環境の整備	不要	必要
ソースコード修正演習	演習可能	演習不可
学習者の学習状況の進捗管理	不可	可能
オススメの集合教育シーン	・不定期に集合教育を実施 ・学習者自身が PC を持ち込む 例：大学のゼミ 小規模な勉強会	・定期的に集合教育を実施 ・専用の教室がある 例：会社の新人教育 高校や専門学校の授業

※演習等で利用するツール(Fiddler 等)は学習者 PC にインストールが必要です。

2.集合教育の環境および AppGoat の入手

2.1. ネットワーク環境および動作環境

・ネットワーク環境の準備

集合教育は、外部から隔離されたネットワーク内で行う必要があります。以下の図のように、管理者 PC にインストールした AppGoat へアクセスできるのは、管理者および同一ネットワーク内の学習者 PC からのみになるように集合教育のネットワーク環境を準備します。

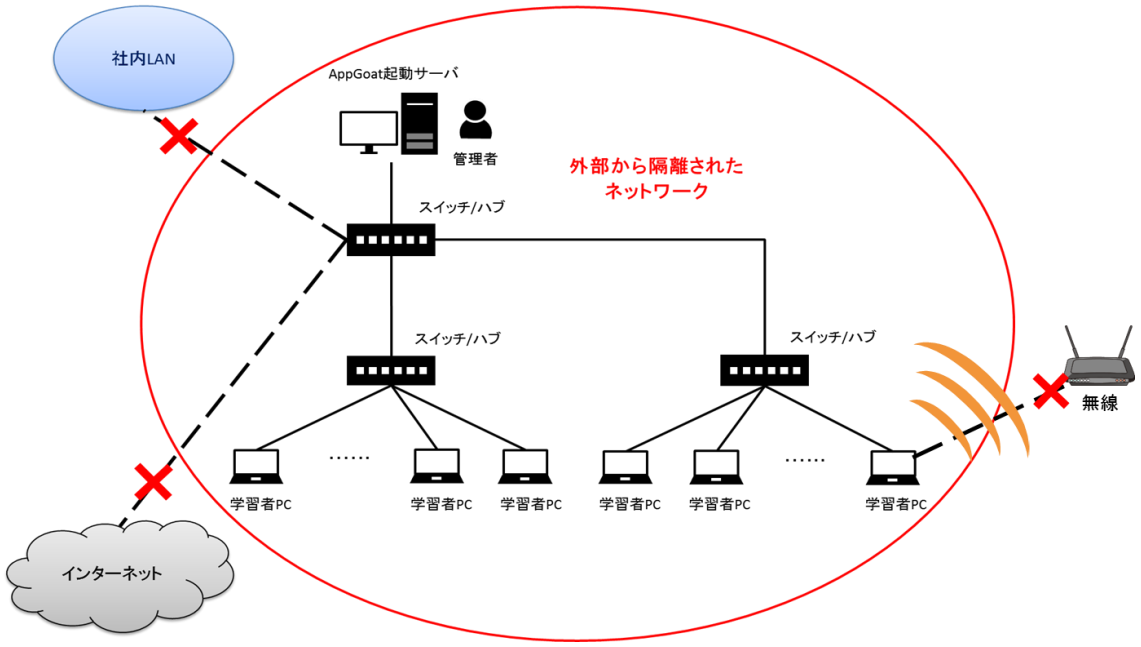

図 2.1：ネットワーク環境のイメージ

【注意】

AppGoat は、脆弱性の概要や対策方法等の脆弱性に関する基礎的な知識を実習形式で体系的に学べるツールであり、**学習用の脆弱性を意図的に作り込んであります。**このため、ご利用環境によっては、**外部の攻撃者に学習用の脆弱性を悪用され、利用者や利用組織に被害が発生する可能性があります。**

集合教育は、必ず**外部から隔離されたネットワーク内**で行ってください。また、集合教育のネットワークを誤ってインターネットに繋げるリスクを考慮して、集合教育のネットワークで**グローバル IP アドレスは使わない**ようにしてください。(*1)

(*1) 誤ってインターネットに繋いでしまった場合、外部のインターネット利用者から集合教育ネットワークに接続している PC が見えるようになります。この結果、悪意ある人から学習者 PC に対して不正アクセスが行われる可能性があります。不正アクセスされると、PC 内のファイルの窃取や改ざん、PC へのウィルスのインストールなどの恐れがあります。

・動作環境

管理者および学習者の動作環境を以下に記載します。

表 2.1：動作環境

項目	内容
OS	下記のいずれかの 32bit/64bit OS Microsoft Windows 8.1 Microsoft Windows 10
CPU	Intel Core プロセッサファミリー 相当以上推奨
メモリ	4GB 以上
ネットワーク帯域	100Mbps 以上
HDD	1GB 以上の空き容量
モニタ	解像度 1,024×768 ピクセル以上
ブラウザ	Google Chrome Mozilla Firefox Microsoft Internet Explorer ※ Microsoft Edge ※ ※本ブラウザを使用する場合、一部実施できない演習があります。
その他	Adobe Reader 11 以上がインストールされていること

【注意】

集合教育中の管理者 PC は、複数の学習者からアクセスされ、AppGoat に意図的に作り込んでいる脆弱性に対して攻撃が行われます。学習者が意図せず、または悪意ある学習者が意図的に、脆弱性を攻撃して、AppGoat が稼働する環境(OS 等)に影響を与える可能性があります。

そのため、AppGoat を動作させる環境は、可能であれば、VMware Player 等の仮想環境を実現するソフトウェアを利用し、仮想環境上での実行を推奨します。仮想環境を実現するソフトウェアの持つスナップショット機能等により、容易に AppGoat を動作させる前の環境に戻すことができるため、繰り返し集合教育を行う場合に有効です。

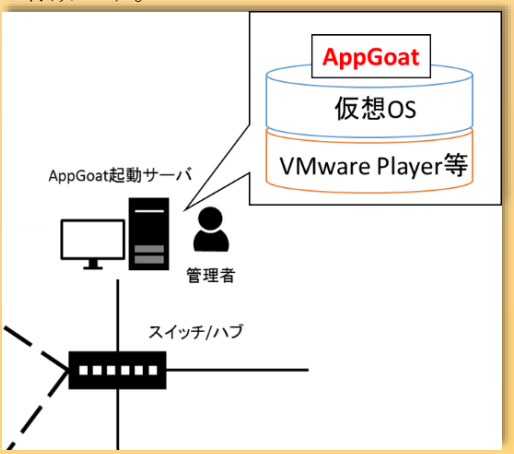

図 2.2：仮想環境のイメージ

2.2. AppGoat の利用申請とダウンロード

AppGoat をダウンロードするためには、IPA への利用申請が必要です。また、集合学習モードでは「有効期限設定ファイル」の反映も必要です。

以下の手順に沿って実施してください。

① AppGoat の利用申請を行う

AppGoat のダウンロードには事前にメールによる利用申請が必要です。

下記 URL の手順に従って、IPA に申請してください。

■集合学習モード

https://www.ipa.go.jp/security/vuln/appgoat/classroom.html

② AppGoat をダウンロードする

利用申請を行うと IPA からメールでダウンロード URL の連絡があります。

上記 URL の手順に従って AppGoat をダウンロードします。

AppGoat はファイルサイズが大きい(V3.0.3 は約 810MB)ため、ご利用のネットワーク環境によってはダウンロードに時間がかかることがあります。また、ダウンロード先のハードディスクに十分な空き容量があることをご確認の上、ダウンロードするようご注意ください。

③ ダウンロードした ZIP ファイルを展開（解凍）する

ZIP ファイルを展開すると「IPATool」というフォルダが作成されます。

「IPATool」フォルダは、AppGoat の演習で使用するため(*1)、**OS のインストールドライブ(*2)の配下に配置**してください。また、**全角文字、半角スペース、半角記号をフォルダのパスに含まない**ようにしてください。これらの文字が 1 つでもパスに含まれていると AppGoat が起動できません。

*1　「ディレクトリ・トラバーサル」の演習で「Windows¥win.ini」を参照します。
他のドライブを使用した場合、当該脆弱性の演習が正しく行えなくなります。

*2　AppGoat が動作する OS である Windows は、通常、C ドライブにインストールされています。

④ 「有効期限設定ファイル」を反映（保存）する

「集合学習モード」の利用申請を行うと、IPA からダウンロード URL と共に「有効期限設定ファイル」（AppGoatSetting.key）が送付されてきます。このファイルを集合教育時に利用する管理者 PC の「IPATool」フォルダ内に保存します。

有効期限内であれば、何度でも「集合学習モード」で AppGoat を利用できます。

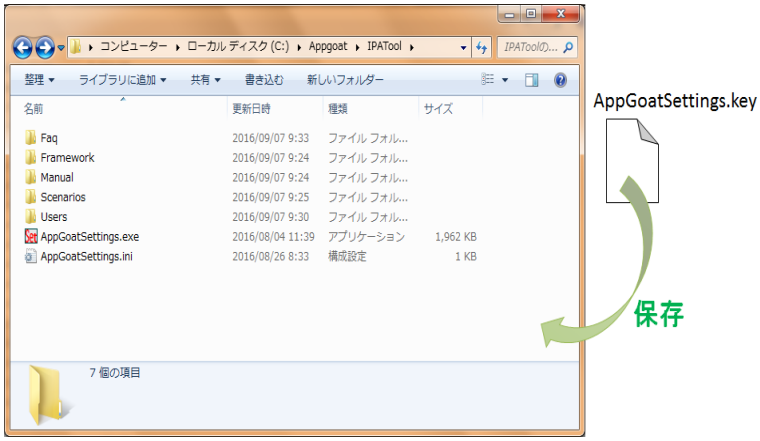

図 2.3：有効期限設定ファイルの保存のイメージ

3.集合教育の準備及び集合教育の実施

AppGoat を利用して集合教育を行う上で事前に検討・準備するべき事項は下図のとおりです。これらについて、以降の節で具体的に記載します。

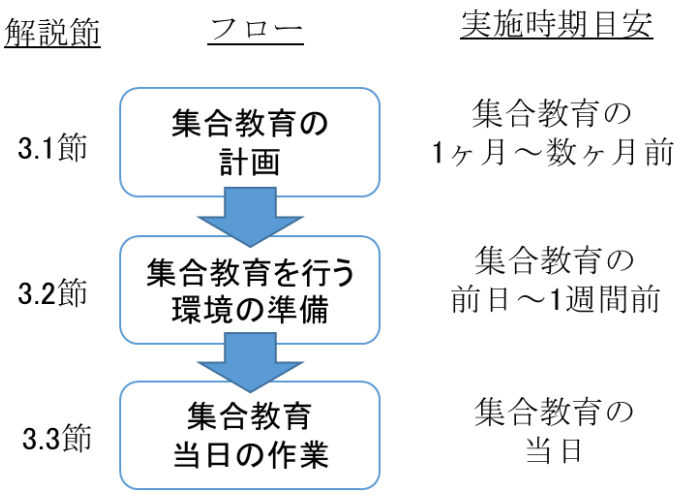

図 3.1：集合教育の実施フロー

3.1. 集合教育の計画

集合教育を行う上で事前に学習者の人数や学習させる内容等について検討する必要があります。実施時期の目安は１ヶ月～数ヶ月前です。
例えば以下の要素を検討する必要があります。

・学習者のスキルの考慮

AppGoat は、学習する上で最低限必要なスキルとして、基本情報技術者試験の合格者、または同等の知識を持つことを想定しています。そのため、学習者のスキルがそれに満たない場合、その差を埋めるため、管理者側で AppGoat とは別に補足資料を準備することを推奨します。集合教育に参加する学習者のスキルに合わせて適宜準備が必要です。

図 3.2：学習者のスキルの違いのイメージ

・集合教育で行う教育の内容の検討

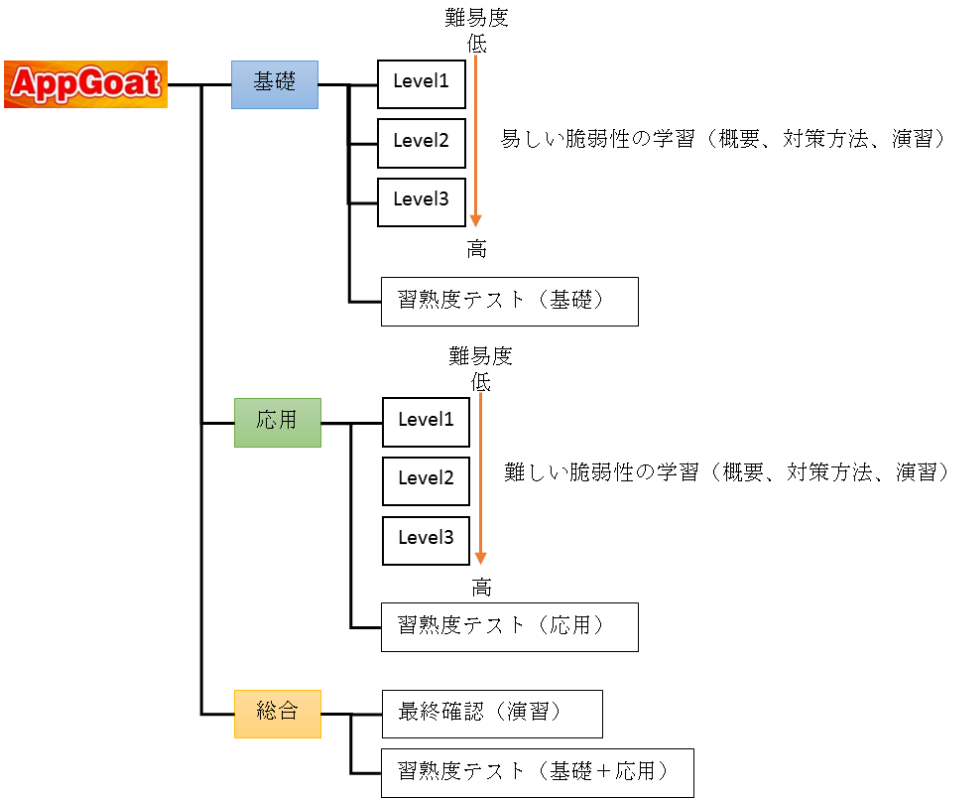

図 3.3：AppGoat の構成の全体像

AppGoat の学習は、「基礎」「応用」「総合」の 3 つから構成されています。

「基礎」→「応用」の順で段階的に学習を進めることで「脆弱性」のイメージを掴みやすくなります。最後に「総合」で演習を行い、理解度を確認します。

表 3.1：.AppGoat の構成

構成	内容
基礎	理解することが比較的容易な脆弱性です。 最初に学ぶべき 6 つの脆弱性について学習できます。
応用	基礎より難易度が高い脆弱性です。 基礎の次に学ぶべき 6 つの脆弱性について学習できます。
総合	学習してきた知識を使ってどこに脆弱性があるかを発見する演習を行えます。 基礎・応用の学習が終わった後の最終確認に適しています。

また、「基礎」と「応用」では演習内容をレベル分けしています。学習の難易度を徐々に上げて行くことで、学習者が脆弱性を無理なく理解できます。

表 3.2：.AppGoat のレベル

レベル	内容
Level1	脆弱性の概要を学べます。また、シンプルなウェブアプリケーションに対して脆弱性を発見する演習を行えます。
Level2	脆弱性の概要や対策方法を学べます。また、Level1 より複雑なウェブアプリケーションに対して脆弱性を発見する演習を行えます。
Level3	脆弱性の概要や対策方法を学べます。また、Level2 より高難度な脆弱性を発見する演習を行えます。

「基礎」「応用」「総合」には習熟度テストを用意してあります。このテスト結果により、理解できている脆弱性と理解が不十分な脆弱性を確認できます。理解が不十分な脆弱性を再度学習させて理解度を高めてください。

表 3.3：.AppGoat の習熟度テスト

習熟度テスト	内容
基礎・応用の習熟度テスト	学習した脆弱性に関する習熟度テストです。出題範囲は、学習中の脆弱性の Level1 および Level2 です。Level3 からは出題されません。
総合の習熟度テスト	すべての脆弱性に関する習熟度テストです。習熟度テストの出題範囲は、全脆弱性の Level1 から Level3 です。

上記を踏まえ、**どの範囲を学習対象とするか、事前検討しておく必要があります**。

【例】

・基礎と応用で脆弱性を一通り教育し、最終確認として総合を実施させよう。
・Level3 は難易度が高いので、Level1 と Level2 を教育させよう。
・力試しにテストは全て(基礎・応用・総合)実施しよう。

図 3.4：集合教育の内容の検討イメージ

・学習者の利用許諾条件合意書内の誓約書への同意および保管方法の検討

管理者は、AppGoat で集合教育を開始する前に、学習者に対して、紙やメール等で利用許諾条件合意書内の誓約書に記載されている条項に合意を得る必要があります。そのため、**事前に学習者に利用許諾合意書内の誓約書の同意を求める方法と同意後の誓約書の保管方法を検討する必要があります。**例えば、集合教育開始前に契約書を配布し、署名後に回収するといった対応の検討が必要です。

なお、利用許諾条件合意書内の誓約書については、AppGoat の、[IPATool¥Manual]内の termsofuseagreement.pdf または、誓約書部分を抜粋した letterofunderstanding.docx を確認してください(本書の付録 2 にも誓約書を記載しています)。必要に応じて、IPA が提出を求める場合があるため、教育終了後 3 年間、誓約書を保管する必要があります。

図 3.5：利用許諾同意のイメージ

・集合教育の参加人数

集合学習モードでは、同時に接続する**最大学習者数は 40 名を想定**しています。

学習者が 40 名を超える場合、AppGoat をインストールするための PC を複数台用意し接続数を分散させる等の運用を検討する必要があります。

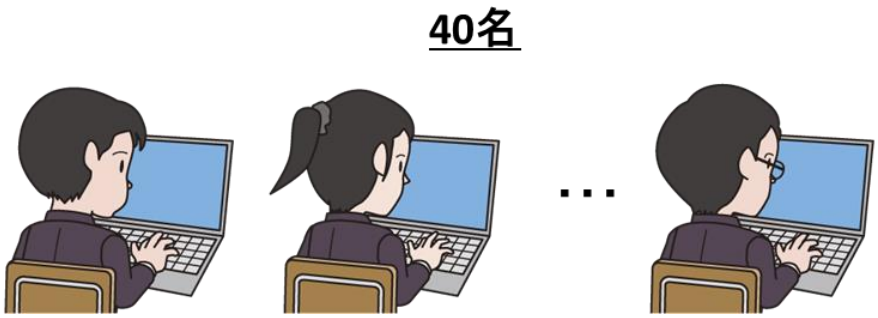

図 3.6：学習者の人数のイメージ

・学習者に関する情報の設定内容の検討

集合学習モードでは、学習者が AppGoat で学習するためには学習者用のアカウントの作成が必要になります。管理者は、学習者用のアカウントを作成するために図 3.7 に示す情報を登録する必要があります。

なお、氏名や所属については仮の名称(user001 等)でもかまいません。どこまで厳密に登録するかは組織の集合教育の方針や管理者の判断に委ねられます。

設定内容		説明
ログイン ID	[必須]	半角英数字 32 文字以内
初期パスワード	[必須]	半角英数字および記号 32 文字以内
氏名	[必須]	32 文字以内
所属	[任意]	32 文字以内

図 3.7：アカウント作成のための情報

・AppGoat の動作検証

AppGoat は様々な機能や学習コンテンツがあるため、集合教育当日にいきなり操作・理解するのは難しいです。AppGoat の操作方法や学習できる内容を事前に確認することを推奨します。「利用マニュアル(集合学習モード 管理者編)」(¥IPATool¥Manual¥admin_ja.pdf)を参照しながら確認を行ってください。

なお、AppGoat のインストールフォルダ(¥IPATool¥)をコピーし、集合教育用とは別に検証用に AppGoat を用意することを推奨します。動作検証をする中でデータの投入等があり、初期状態から変更され、集合教育時になんらかの不都合が発生する可能性があるためです。

3.2. 集合教育を行う環境の準備

集合教育を行う環境を準備します。準備項目について記載します。実施時期の目安は前日～1 週間前です。

(1) ネットワークの構築

2.1 節を参考に、集合教育を行うネットワーク環境や PC の準備を行います。学習者 PC に割り当てた IP アドレスの情報は「(2)管理者 PC のセットアップ」時に利用します。

(2) 管理者 PC のセットアップ

以下のフローに従い管理者 PC のセットアップを行います。「利用マニュアル(集合学習モード 管理者編)」(¥IPATool¥Manual¥admin_ja.pdf)を参照しながら行ってください。

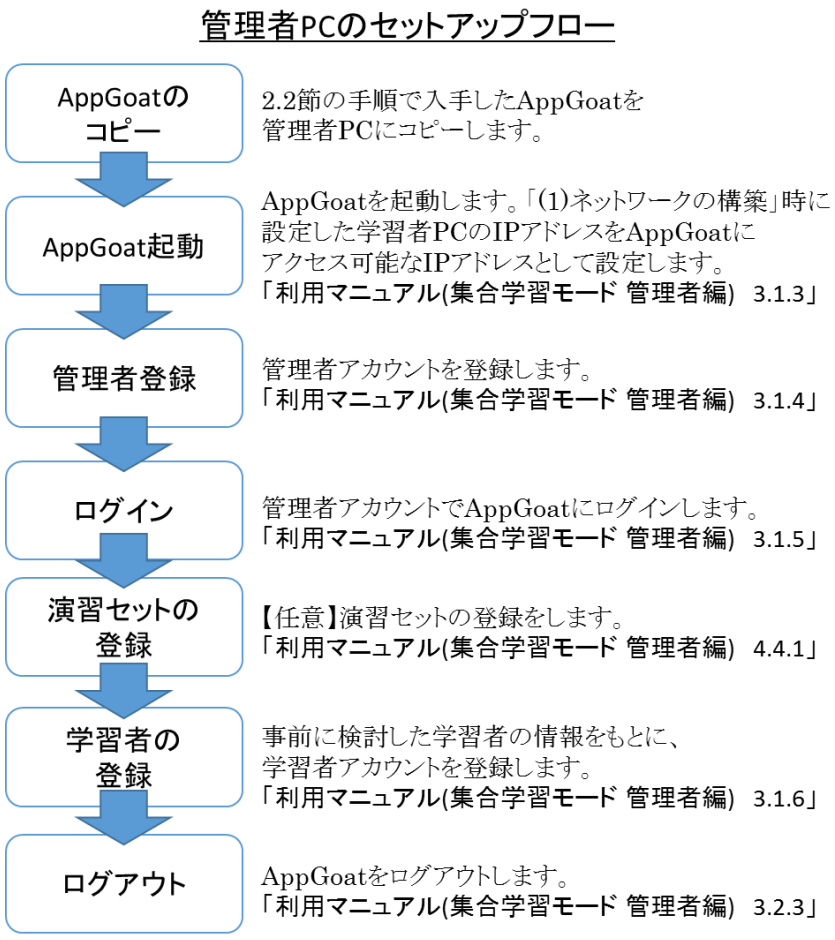

図 3.8：管理者 PC のセットアップフロー

(3) 学習者 PC のセットアップ

・Fiddler のダウンロードおよびインストール

AppGoat には、フリー検査ツール「Fiddler」を用いて検査演習を行うものがあります。この検査演習を行うためには、学習者 PC に Fiddler のインストールが必要です。

インストールは、下記のサイトからダウンロードして行います。

https://www.telerik.com/download/fiddler

なお、Fiddler の使い方については、AppGoat 起動後に総合メニューから「学習環境へ」→「注意事項」→「テーマ一覧-補足-Fiddler の使い方」と移動し、確認することができます。

・AppGoat の接続テスト

管理者 PC で動作している AppGoat への接続テストを行います。ログイン URL(http://管理者 PC の IP アドレス)※にアクセスし、ログイン画面が表示されることを確認します。画面が表示されない場合は、以下の点を確認してください。

・ネットワークの設定が誤っていないか(IP アドレス、ネットマスク等)

・ネットワークに接続されているか

・ブラウザのプロキシが設定されていないか(集合教育用のネットワークでプロキシサーバを利用していない場合)

・AppGoat は起動しているか、

※例：管理者 PC の IP アドレスが 192.168.10.1 で AppGoat を 80 ポート(デフォルト設定)で起動している場合

http://192.168.10.1

なお、AppGoat 起動時の設定によって、別途ポート番号(http://管理者 PC の IP アドレス:ポート番号)が必要です。

例：管理者 PC の IP アドレスが 192.168.10.1 で AppGoat を 81 ポートで起動している場合

http://192.168.10.1:81

(4) AppGoat の停止

「利用マニュアル(集合学習モード 管理者編)　3.2.4」を参照し、AppGoat を停止します。

3.3. 集合教育当日の作業

集合教育当日に最低限必要な作業について記載します。

・管理者 PC および AppGoat の起動

管理者 PC を起動後、AppGoat を起動します。(「利用マニュアル(集合学習モード 管理者編)　3.1.2」)

・学習者の利用許諾条件合意書内の誓約書への同意および保管

集合教育開始前に学習者から誓約書への同意を取ります。誓約書を紙に印刷し、学習者に配り同意(署名)を取り、誓約書の回収を行います。誓約書については、AppGoat の、[IPATool¥Manual]内の termsofuseagreement.pdf または、誓約書部分を抜粋した letterofunderstanding.docx を確認してください。本書の別紙 2 にも誓約書を添付しています。

なお、反社会的行為への関与が指摘される、または疑われる場合に、事実確認等のために必要に応じて IPA から提出を求めることがあります。

管理者は、集合教育終了後、誓約書を 3 年間保管してください。

・ログイン ID・PW およびアクセス方法の連絡

AppGoat にログインするための URL やログイン ID、パスワードを学習者に連絡します。

・学習者の進捗管理

AppGoat(集合学習モード)では、学習者の進捗状況を確認できます。管理者でログイン後、総合メニューから「学習者の管理」をクリックし、進捗を管理したい学習者を選択します。

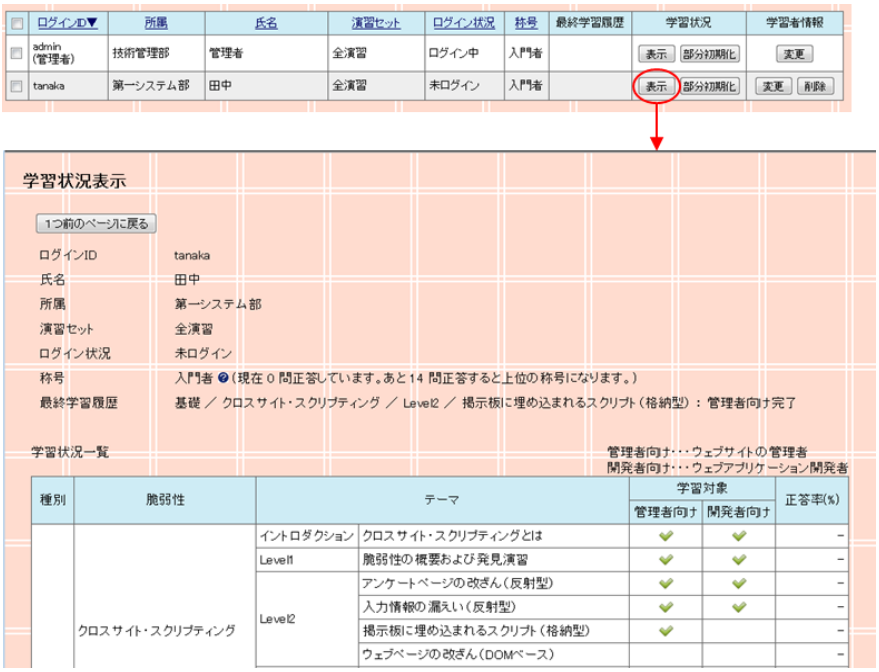

図 3.9 : 学習者の進捗管理

・ログの保管

集合教育で管理者 PC に蓄積した AppGoat に関連するログは、反社会的行為への関与が指摘される、または疑われる場合に、事実確認等のために必要に応じて IPA から提出を求めることがあります。

管理者は、集合教育終了後、管理者 PC 内にある以下のログを 1 年間保管してください。

表 3.4：保管対象のログ

ログファイルの種類	ログファイルの説明	ログファイルの保存場所
AppGoat エラーログ	AppGoat のエラーログを確認することができます。	¥IPATool¥Framework¥Log¥errorlog.txt
Apache アクセスログ	Apache のリクエストのログを確認することができます。	¥IPATool¥Framework¥Apache24¥logs¥access.log
Apache エラーログ	Apache のエラーログを確認することができます。	¥IPATool¥Framework¥Apache24¥logs¥error.log

4.集合教育開始までの作業フロー

3 章では、AppGoat に関わる部分で実施が必要なことを記載しました。実際に集合教育を行う場合、組織のルールや目的によって追加で実施しなければ行けない作業もあります。本章では、会社や学校で集合教育を行う上で想定される作業フローについて記載します。

※本作業フローはあくまで代表例を参考として記載しているものです。
集合教育を行う際には、各組織（企業、学校等）の環境や状況に応じて、適宜、調整してください。

4.1. 学校での集合教育

学校の授業(講義)として、AppGoat を用いて学生への教育を行うことを想定した作業フローです。

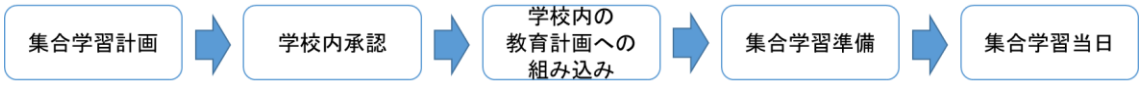

図 4.1：学校での集合教育の想定作業フロー

1. 集合教育の計画

・教育内容の検討

本書 3.1 節で記載している事前検討項目を参考に、集合教育の内容を検討します。

・事前動作検証

AppGoat を事前にダウンロードし、正常に動作するかを検証します。

2. 学校内承認

学校内のルールに従い、AppGoat を使った教育について実施許可を得ます。

3. 学校内の教育計画(シラバス等)への組み込み

学校内のルールに従い、教育計画に組み込みます。

4. 集合学習準備

・集合教育用資料の作成

AppGoat 内で記載している内容は、セキュリティやネットワークに関する用語等をある程度知っているレベル(基本情報処理試験取得レベル)の学習者を想定しています。そのため、それに満たない学習者をターゲットに教育を行う場合には、別途補助資料を用意して AppGoat を補完する形で教育を行うことが効果的です。

IPA では以下の資料を公開しています。
補助資料作成の参考にしてください。

■AppGoat を利用した集合教育補助資料
https://www.ipa.go.jp/security/vuln/appgoat/classroom.html
■安全なウェブサイトの作り方
https://www.ipa.go.jp/security/vuln/websecurity.html

・学習環境
集合教育を行う前に学習者および管理者の学習環境の準備を行う必要があります。本書 3.2 節を参考に準備を行います。

5. 集合学習当日

本書 3.3 節および 5 章を参考に集合学習を進めます。

4.2. 会社での集合教育

社内研修等において、AppGoat を用いて、新人や若手に教育を行うことを想定した作業フローです。

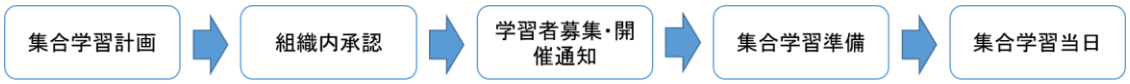

図 4.2：学校での集合教育の想定作業フロー

1. 集合教育の計画

・教育内容の検討

本書 3.1 節で記載している事前検討項目を参考に、集合教育の内容を検討します。

・事前動作検証

AppGoat を事前にダウンロードし、正常に動作するかを検証します。

・集合教育の実施日の決定

集合教育の実施日を決定します。

2. 組織内承認

組織内のルールに従い、集合教育の実施許可を得ます。

3. 学習者募集・開催通知

集合学習に参加する学習者の募集を行います。例えば、メールやウェブページ等で案内することで会社内の参加者を募集します。新人研修等で既に学習者が決まっている場合は、学習者に開催通知の連絡を行います。

4. 集合教育の準備

・集合教育用資料の作成

AppGoat 内で記載している内容は、セキュリティやネットワークに関する用語等をある程度知っているレベル(基本情報処理試験取得レベル)の学習者を想定しています。そのため、それに満たない学習者をターゲットに教育を行う場合には、別途補助資料を用意して AppGoat を補完する形で教育を行うことが効果的です。

IPA では以下の資料を公開しています。
補助資料作成の参考にしてください。

■AppGoat を利用した集合教育補助資料
https://www.ipa.go.jp/security/vuln/appgoat/classroom.html
■安全なウェブサイトの作り方
https://www.ipa.go.jp/security/vuln/websecurity.html

・学習環境
集合教育を行う前に学習者および管理者の学習環境の準備を行う必要があります。本書 3.3 節を参考に準備を行います。

5. 集合教育当日

本書 3.3 節および 5 章を参考に集合学習を進めます。

5.集合教育当日の進め方例

集合教育当日の進め方の例を 3 つ紹介します。集合教育の流れは基本的に管理者が決定しますが、段取りの検討の参考にしてください。

【進め方 1】AppGoat をメインに利用する学習(自習)

初めに管理者（講師）が脆弱性について簡単な解説を行い、その後、学習者が AppGoat を使い、できるだけ独力で学習を進めていきます。

管理者は学習者からの質問に答えるなどして学習者をサポートします。また、管理者は AppGoat の管理画面から学習者の進捗状況を確認できるので、進捗が芳しくない学習者がいれば、解決のヒントを与えることで前進させていきます。

学習者の IT スキルが高い場合に適した進め方です。

【進め方 2】AppGoat の演習機能を利用する学習

管理者（講師）が脆弱性について解説を行い、その後、学習者に AppGoat で演習を行わせ、脆弱性を発見する体験をさせます。AppGoat の演習はレベル分けされているため、それぞれの学習者のレベルにあった演習をさせることができます。

学習者の IT スキルが統一されていない場合に適した進め方です。

【進め方 3】複数回に分けての集合教育

進め方 1 を使って、複数回に分けて AppGoat による集合教育を行います。

企業や学校などで、AppGoat の全ての脆弱性を教育する場合に適した進め方です。

【進め方 1】AppGoat をメインに利用する学習(自習)

1. 集合教育開始前の学習者への連絡・周知

集合教育を始める前に、下記について学習者へ周知します。

・誓約書の配布

・学習者の誓約書への同意

・誓約書の回収・保管

・ログイン用の ID/PW の周知

・AppGoat へのアクセス方法(URL)の周知

・自習対象の脆弱性の説明(AppGoat 内のどの脆弱性を学習するのかを指示)

・自習対象の脆弱性の補足情報

(学習者にとって AppGoat 内の記載では難しいと思う脆弱性についての補足説明等)

2. 自習開始

学習者に自習を開始するよう指示します。

※管理者は AppGoat の管理画面より進捗状況を確認することができます。

※進捗が芳しくない学習者を適宜フォローします。

3. 集合教育の終了

学習者に周知し集合教育を終了します。

4. AppGoat の停止

AppGoat の停止を行います。

5. AppGoat ログの保管

AppGoat 内のログを取得し、保管します。

【進め方 2】AppGoat の演習機能を利用する学習

1. 集合教育開始前の学習者への連絡・周知

集合教育を始める前に以下の内容について学習者に対して行います。

・誓約書の配布

・学習者の誓約書への同意

・誓約書の回収・保管

・ログイン用の ID/PW の周知

・AppGoat へのアクセス方法(URL)の周知

2. 脆弱性を理解する上で必要な知識の学習

脆弱性を学ぶ上で事前に知っておくべき用語の解説を行います。

例：SQL インジェクションであれば、SQL 文の解説を行います。

3. 脆弱性の仕組みの解説

脆弱性の概要やどのように悪用されるのか、脆弱性の確認・攻撃方法について解説を行います。

4. 脆弱性の発見演習

AppGoat を利用して脆弱性のあるアプリケーションに対して攻撃を行う演習を行うように学習者に指示します。学習者の演習状況を確認し、次の手順に進みます。

※管理者は AppGoat の管理画面より学習者の攻撃の成功状況を確認することができます。

5. 脆弱性の影響の解説

脆弱性を悪用された際の影響について解説します。

6. 集合教育の継続

学習させたい脆弱性の数分 2～5 の手順を繰り返します。

7. 集合教育の終了

学習者に周知し集合教育を終了します。

8. AppGoat の停止

AppGoat の停止を行います。

9. AppGoat ログの保管

AppGoat 内のログを取得し、保管します。

【進め方 3】複数日に分けての集合教育

2 日間に分けて集合教育を実施する例を紹介します。

■初日

1. 集合教育開始前の学習者への連絡・周知

集合教育を始める前に以下の内容について学習者に対して行います。

・誓約書の配布
・学習者の誓約書への同意
・誓約書の回収・保管
・ログイン用の ID/PW の周知
・AppGoat へのアクセス方法(URL)の周知

2. 脆弱性を理解する上で必要な知識の学習

脆弱性を学ぶ上で事前に知っておくべき用語の解説を行います。
例：SQL インジェクションであれば、SQL 文の解説を行います。

3. 脆弱性の仕組みの解説

脆弱性の概要やどのように悪用されるのか、脆弱性の確認・攻撃方法について解説を行います。

4. 脆弱性の発見演習

AppGoat を利用して脆弱性のあるアプリケーションに対して攻撃を行う演習を行うように学習者に指示します。学習者の演習状況を確認し、次の手順に進みます。
※管理者は AppGoat の管理画面より学習者の攻撃の成功状況を確認することができます。

5. 脆弱性の影響の解説

脆弱性を悪用された際の影響について解説します。

6. 集合教育の継続

学習させたい脆弱性の数分 2～5 の手順を繰り返します。

7. 初日の集合教育の終了

学習者に周知し、初日の集合教育を終了します。

8. AppGoat の停止

AppGoat の停止を行います。

■2 日目

9. AppGoat の起動

AppGoat を起動します。管理者 PC 内の AppGoat を起動します。

※前日の AppGoat の停止時に正常に停止できていなかった場合、AppGoat の起動時に「pid ファイル[インストールフォルダ名]¥IPATool¥Framework¥Apache24¥logs¥httpd.pid が存在しています。ファイルを削除してやり直してください。」のメッセージが表示され起動できない場合があります。その場合は、メッセージの内容に従い、httpd.pid ファイルを削除してから再度 AppGoat を起動してください。

10. 集合教育開始

前日の続きから集合教育を開始します。

11. 集合教育の終了

学習者に周知し集合教育を終了します。

12. AppGoat の停止

AppGoat の停止を行います。

13. AppGoat ログの保管

AppGoat 内のログを取得し、保管します。

別紙１ 「個人学習モード」を用いた集合教育

AppGoat には「集合学習モード」以外に、「個人学習モード」が存在します。「個人学習モード」を利用して、集合教育を行うことも可能です。

「個人学習モード」を利用した集合教育は、「集合学習モード」を利用した集合教育と違い、以下の点の考慮が必要です。

(1)集合教育するための環境の違い

・関連ツール(Fiddler 等)に加えて AppGoat を学習者の全ての PC にセットアップする必要があります。
・管理者 PC にアクセスするためのネットワーク環境の準備は不要です。
・ログイン認証がないため集合教育開始時に学習者への ID/PW の通知は不要です。
・AppGoat の起動・停止は学習者 PC 全てに行う必要があります。

(2)「集合学習モード」との機能の違い

・脆弱性の発見演習だけではなく、脆弱性の修正演習(ソースコードの修正)も体験できます。そのため、集合教育時に修正演習も学習者に行わせることが可能です。
・学習者の学習の進捗状況を確認できません。管理者が学習者の操作状況を見て進捗を把握する必要があります。

別紙 2　誓約書

(次ページ)

（様式）

誓　約　書

私は、この度、貴職／貴法人が「脆弱性体験学習ツール AppGoat」を用いて実施する集合教育を受講者の一人として受講するに当たり、講師等から受ける注意事項等を誠実に遵守するとともに、下記各項を誓約します。

記

1. 上記集合教育において上記学習ツール AppGoat (以下「AppGoat」といいます)を利用する場合、講師から明示的に使用の許可を受けた機能及び情報、又は AppGoat が明示的に受講者に提示する機能及び情報のみを使用することとし、その他の機能等については、それらを探索せず、また、何らかの事情でそれらを知り得たとしても、それらを決して使用せず、また他の受講者を含めて決して他人に開示・漏洩しません。
2. 上記集合教育における AppGoat の利用によって知り得た他の受講者や貴職／貴法人に関する情報は、上記集合教育の実施目標実現のための、かつ当該集合教育の現場限りにおける利用のみに限ることとし、決して他の目的に利用せず、また他人に開示・漏洩しません。
3. AppGoat の利用によって学んだ知識や情報は、上記集合教育の終了後であっても、私の正当な業務の遂行のためにのみ利用することとし、その他の目的への利用(正当な業務以外で、他人のコンピュータシステムに侵入したり、同システム内で情報を閲覧・書き換え・消去・外部送信等したり、ウィルスへの感染その他その正常な動作に支障を生ぜしめたり、又はそれらを試みる行為を含みます)は決して行いません。
4. 上記各項に違反する行為は犯罪となる可能性が高く、従って刑事訴追を受ける可能性があることを十分に承知するとともに、私又は他の受講者に上記各項違反の嫌疑がかかった場合、事実関係の解明・立証等のために、上記集合教育に関して貴職／貴法人が保有するログ情報等のうち、私に関する部分の全てを、公表し又は関係各機関等に提出することに異存ありません。
5. 前項の場合、私は、前項所定の“私に関する部分の全て”について、それらが正当かつ適法に取り扱われる限り、個人情報保護法上の、またプライバシー保護その他の観点からの権利等を、いずれも主張しません。
6. 私又は他の受講者に上記第１項乃至第３項違反の嫌疑がかかった場合、貴職／貴法人が本誓約書を公表し又は関係各機関等に提出することに異存ありません。私は、本誓約書について、それが正当かつ適法に取り扱われる限り、個人情報保護法上の、またプライバシー保護その他の観点からの権利等を、いずれも主張しません。
7. 私が本誓約書に違反した場合、貴職／貴法人その他全ての関係者が被る各損害の全てを、私が賠償しなければならない責任を負うことを、十分に理解します。
8. 本誓約書は日本国の法律によって解釈され、本誓約書に関して裁判になる場合は東京地方裁判所での裁判手続きのみに服することに同意します。

上記各項の内容を十分に理解の上、上記誓約の証として本書面に署名押印して提出します。

年　　月　　日

(住所)

(氏名)　　㊞

○○○ 御中