指導の流れ：中学校「PHP の修正が公開された夜、社会はどう動いたか」

スライド：`php-20261021-junior-high.pptx`（15 枚、ノートに台本）／`php-20261021-junior-high.pdf` ワークシート：`worksheet-junior-high.pdf`（A4、1 枚。手がかりカードは刷らず、スライド10を映す。直すときは `.pptx`） 出典：Data is CITY（teleport.jp/dataiscity/）、CC BY 4.0

ねらい

- 2026年10月21日の出来事を、「脆弱性 → 修正の公開（＝弱点の公開）→ 予防のための一時停止と更新」のつながりで説明できる。
- 社会のサイバーセキュリティが、研究者・開発者・国の機関・会社の担当者・利用者の連携で守られていることに気付き、自分の行動を一つ決める。

学習指導要領のどこに当たるか

技術・家庭（技術分野）の授業として行う。道徳・学級活動は「関連」にとどめる（この1時間を道徳の時数には数えない）。

区分	当たる所	この授業での扱い
技術分野 2 内容 D(1)ア	「…情報のデジタル化や処理の自動化、システム化、情報セキュリティ等に関わる基礎的な技術の仕組み及び情報モラルの必要性について理解すること」	サーバーとクライアント（スライド5）、脆弱性と修正（6〜8）
技術分野 3 内容の取扱い (4)ア（D の取扱い）	「…社会におけるサイバーセキュリティが重要であることについても扱うこと」	連携の図（スライド12）
技術分野 2 内容 D(4)イ	「技術を評価し、適切な選択と管理・運用の在り方…について考えること」	「止める？止めない？」の判断（10〜11）、更新の管理・運用（13〜14）
総則	第1章 第2の2(1) 情報活用能力（情報モラルを含む）	全体
道徳（関連）	第3の2(6) 情報モラルに関する指導の充実。内容 C［遵法精神、公徳心］とも関わる	うわさや漏れた情報を広めない（14）。道徳の時間で扱うなら、内容項目に沿って主題を立て直す
学級活動（関連）	日常の生活の安全	端末の使い方の約束と結びつけるとき

ことばの決まり（現場の先生の助言を受けて）

- 「当てる」（パッチを当てる）は使わない。「修正版に更新する」「更新する」で統一する。スライド8にだけ「ニュースなどでは『パッチを当てる』とも言う」と注を付けた。

- 「約7割」は「ウェブサイトの約7割（69.2%）が PHP を使っている」と言い、スライドに「※サーバー側の言語が分かるサイトの中で数えた割合」と小さく残す（W3Techs の条件）。
- 「脆弱性」は 5 の終わりで「今回の問題は、この PHP に脆弱性が見つかったこと」と出し、6 で「脆弱性とは？」と説明する。
- IPA（アイ・ピー・エー／情報処理推進機構。情報セキュリティの注意を呼びかける国の機関）、AWS（Amazon のサーバー貸し出しサービス）、CISA（アメリカ政府のサイバーセキュリティを担当する役所）は、出てきた所で一言添える。
- 「リテラシー」は「情報や技術を正しく理解して使いこなす力」（スライド11）。

情報モラル指導モデルカリキュラム（「教育の情報化に関する手引」追補版 第2章第4節）では、中学校の段階で「情報セキュリティに関する基礎的・基本的な知識」を身に付け、「情報セキュリティの確保のために、対策・対応がとれる」ことが求められている。

時間配分

50 分（出欠・配布の 2 分を含む）

生徒が口を開くのは、2（30秒）、7（近くの人と30秒、必ずやる）、9（話し合い）、14（書く）。

時間	スライド	活動	問い
0〜2分	—	出欠・ワークシート配布	—
2〜6分	1〜2	導入：同じ夜に一斉に「メンテナンス中」	「何が起きていたと思う？」（近くの人と30秒）
6〜10分	3〜4	時系列：PHP の開発チームは修正版を10月22日に公開する予定だったが、21日未明〈日本時間〉に弱点の番号などが漏れたので、1日早めて21日23時に公開／止まったもの（短く）：壊れて止まったのではなく、各社が予防のために自分で判断して止めた。国の案内は命令ではない	—
10〜16分	5〜6	PHP はサーバー側（ウェブサイトの約7割＝69.2%。※言語が分かるサイトの中で）。サーバーの仕事は、届いたお願いに合わせて答え（ページ）を作って返すこと。だから直すのはサーバーを動かす会社／「今回の問題は PHP に脆弱性があったこと」→ 脆弱性とは？（2件とも 9.2）	—
16〜20分	7	なぜその夜のうちに急いだか：直した版を公開すると、見比べて「どこが弱かったか」も知られる（修正の公開は弱点の公開でもある）	**近くの人と30秒（必ず）** 「それなら、修正を公開しなければいい？」
20〜22分	8	答え合わせ：公開しないと守る側が直せない。だから公開して、すぐ更新する。今回は公開前に漏れ、試みも見つかっていた。会社は予防のために止めた	—

時間	スライド	活動	問い
22〜24分	9	首相の呼びかけ（短く）：相手はサイトの運営者。①PHP を使っているか確かめる ②23時の修正版にすぐ更新できるよう準備する	—
24〜33分	10	話し合い：今の状況を 6 枚の手がかりカード A〜F にした（個人2分→班4分→発表3分、3班まで）	「今夜、お店（サイト）を止める？止めない？どのカードをいちばん重く見た？」
33〜35分	11	まとめ：止めると困ること／止めないと起こりうること。判断に要る情報を、自分のサイトが PHP で動いていると知らない人もいる。ふだんから知っておくこと（リテラシー）も守りの一部（結論は言わない）	—
35〜37分	12	連携で夜を越えた（今回は流れが崩れかけた）。IPA が何かを一言	—
37〜38分	13	自分の端末でも毎週のように。学校の端末は学校が更新する	—
38〜42分	14	4つの行動（2 のパスワードは今回とは別の、ふだんの心がけ）	—
42〜50分	15	ワークシート①（ア〜エの選択）③（②は10で書いた）	—

計 50 分（2+1+3+3+1+3+3+4+2+2+9+2+2+1+4+8）。

45 分版

スライド4（−1分）と9（−2分）を飛ばし、話し合いを 9 分→7 分（発表を2班）にする。計 45 分。首相の呼びかけはスライド3の時系列で触れる。

15 分の短縮版

分	スライド
2	2
2	3
2	5（直すのはサーバー側。ここを飛ばすと「スマホで PHP を更新しなきゃ」という誤解が残る）
2	7（30秒の問いは一人に聞くだけ）
2	8
3	14
2	15（③だけ口頭で）

計 15 分。話し合いは省く。

話し合いの進め方（スライド10・11）

- 手がかりカードは刷らない。スライド10を画面に映すだけで使う。答え（止めると困ること・止めないと起こりうること）は見せない。
- 手がかりカード：A PHP が動くのは注文と会員のページ／B 修正版は23時、更新に約1時間かかる／C 夜9〜11時はいちばん注文が多い／D 会員10万人の名前・住所・注文の記録／E 国家サイバー統括室と首相が「今夜」と呼びかけ（実際の出来事）／F 23時に更新したあと、動作の確認に約30分。A〜D・F は話し合いのための設定。
- はじめに「あなたはネットショップの責任者です。今の状況を 6 枚のカードにしました。今夜お店を止めますか？止めませんか？」と読み上げる（スライド10の 1 行目）。
- 個人2分でカードを読んでワークシート②に書く。
- 発表は3班まで。ほかの班は、ワークシート②を回収して次の時間に紹介する。
- 板書例：左に「止めると困ること」、右に「止めないと起こりうること」、下に「判断に必要な情報（自分のサイトのどこで PHP が動く？ 外から届く？ 誰が決める？）」。
- まとめでは、お店を開いていても自分のサイトが PHP で動いていると知らない人もいること、知らなければその夜に判断できないことを言い、「ふだんから知っておくこと＝リテラシー」につなぐ。
- まとめ（スライド11）：正解は一つではない。どちらを選ぶかは会社の事情による。結論は言わない。事実として、国家サイバー統括室は、すぐ更新するのが難しい場合は一時停止も「リスクを低減させるための有効策の一つと考えられます」と案内し、実際に止めた会社も多く報道された。判断に要る情報を、ふだんから知っておくこと（リテラシー）も守りの一部。

授業の前日に確かめること

- IPA のページで「国内被害の事例を把握していない」（10月27日時点）が変わっていないか。
- スライド4のサービス名は口頭で補う前提。1〜2個でよい。
- スライド9で首相の名前と投稿を映すので、管理職に一言伝えておく。政治的な評価はしない。
- 学校の端末の更新の管理（教育情報セキュリティポリシーに関するガイドラインでは、OS・ブラウザを含むソフトウェアの更新を一元管理することが望ましいとされる）。

よく出る質問と答え

- 「公開しなければいいのでは？」→ スライド7で近くの人と30秒で考え、スライド8で答え合わせ。公開しないと、世界中でサーバーを動かしている守る側が直せない。だから「公開して、すぐ更新する」。
- 「じゃあ、公開前から攻撃されてたの？」→ AWS のおとりのサーバーで「試み」が見つかった、ということ。どの会社が攻撃されたかは分かっていない。だから多くの会社は予防のために止めて、23時の修正を待った（スライド8）。
- 「伏せておくのは隠ぺい？」→ 隠すためではなく、準備ができた所からみんなが同時に直せるようにするため。今回はその前に漏れた。

- 「動画を誤って公開したのは誰？」→ 脆弱性を報告した側の会社（The PHP Foundation の説明）。スライド12で「報告する」側として出てくる。報告がなければ直せなかったが、同じ側のミスで手順が崩れかけた。人の仕事にはミスがある。だから、漏れても動けるように、ふだんの準備と連携が要る。
- 「パスワードで防げたの？」→ 防げない。今回の弱点は「ログインなしで」攻撃できるもの。パスワードの心がけは別の攻撃への備え（スライド14）。

ワークシート（worksheet-junior-high.pdf）

① 10月21日に何が起きた？　ア〜エから一つ選ぶ（スライド15と同じ）。書けたら「なぜ、その夜のうちに急いだ？」を一言で

- ア 大規模なサイバー攻撃やアクセスの集中で、多くのサイトが壊れて止まった
- **イ PHP に脆弱性が見つかり、多くの会社が予防のため一時停止して、修正版に更新した（正解）**
- ウ PHP に脆弱性が見つかり、利用者が自分のスマホで PHP を更新することになった
- エ 首相の命令で、PHP を使うサイトはすべて止めなければならなくなった
- ア はスライド2でよく出る予想、ウ は「直すのはサーバーの側」（5）の取り違え、エ は「お願い」と「命令」（4・9）の取り違え。どれを選んだかで、どこをもう一度話すかが分かる

- ② 話し合い：止める・止めない・条件つき／いちばん重く見た手がかりカード（画面の A〜F）と理由（スライド10で書く）
- ③ 自分にできること（いつ・何をする？）

評価の目安：① でイを選べている（ア・ウ・エを選んだ生徒には、その取り違えの所を次の時間に短く返す）。一言が書けていれば「修正の公開が弱点の公開でもある（公開されると攻撃する人にも弱点が分かる）」ことに触れているか。② でカードを根拠に理由が書けている。③ が「いつ」を含む具体的な行動になっている。

使った事実と出典（スライドの隅にも記載）

事実	出典
修正版 23 時（14:00 UTC）公開、本来は 10月22日。CVE 番号などの漏えい（10月20日 15:00 UTC ごろ＝日本時間21日 0時ごろ）で1日前倒し、報告した側の会社が攻撃の動画を誤って公開。報告は 8月	The PHP Foundation（2026-10-21）https://thephp.foundation/blog/2026/10/21/todays-php-security-release-and-how-were-strengthening-php-security/
認証なしでのリモートコード実行を許しうる2件、2件とも CVSS v4.0 で 9.2	PHP 公式 https://www.php.net/archive/2026.php
国家サイバー統括室が21日午後に X で注意喚起。一時停止も「リスクを低減させるための有効策の一つと考えられます」	共同通信（熊本日日新聞掲載、2026-10-22）https://kumanichi.com/articles/2049509 ／ INTERNET Watch（2026-10-22）

事実	出典
首相の X 投稿 21時55分ごろ、内容	https://x.com/takaichi_sanae/status/2112890642590564386 ／ INTERNET Watch https://internet.watch.impress.co.jp/docs/news/2150203.html
止まったサービスの例	日本経済新聞・Impress Watch・ITmedia NEWS（2026-10-21）、ギズモード・ジャパン（2026-10-22）https://www.gizmodo.jp/article/php-vulnerability-incident-explained/
サーバー側の言語が分かるサイトの 69.2% が PHP（スライドでは「ウェブサイトの約7割」＋注）	W3Techs https://w3techs.com/technologies/details/pl-php
公開の4日前に攻撃の試み、公開から数時間で攻撃コード	Amazon Threat Intelligence（2026-10-21）
国内被害の事例は把握していない／CISA KEV 掲載（10月26日）	IPA https://www.ipa.go.jp/security/security-alert/2026/alert20261022.html

出典：Data is CITY（teleport.jp/dataiscity/）、CC BY 4.0