指導の流れ：高等学校 情報Ⅰ「PHP の脆弱性を直す修正版の公開まで、あと1時間」

スライド：`php-20261021-high.pptx`（本編 13 枚＋付録 2 枚、ノートに台本）／`php-20261021-high.pdf` ワークシート：`worksheet-high.pdf`（A4、1 枚。直すときは `.pptx`） 出典：Data is CITY（teleport.jp/dataiscity/）、CC BY 4.0

題の「あと1時間」は、首相の X 投稿（21時55分ごろ）から、PHP の脆弱性 2 件を直す修正版の公開（23時）までのこと。

ことばの決まり（現場の先生の助言を受けて）

高校1年生が知らない言葉は、出てきた枚で読み方と一言の説明を添える。

- クライアント＝見る側の端末のブラウザ（サイトを見るアプリ）（スライド4）
- AWS（エー・ダブリュー・エス）＝Amazon のサーバー貸し出しサービス。今回の報告はその調査チーム／PoC（ピー・オー・シー）＝悪用できることを確かめるための、お試しのプログラム（6）
- 米 CISA（シーサ）＝アメリカ政府の、サイバーセキュリティを担当する役所／IPA（アイ・ピー・エー）＝情報処理推進機構／NCO＝国家サイバー統括室（7）
- 差分（さぶん）＝直す前と後で、変わった部分。「修正の公開は弱点の公開でもある」の理由なので、①コードは公開されていて誰でも比べられる ②差分＝どこを直したか＝どこが弱かったか ③攻撃する側も読む → 公開したらすぐ更新、の 3 段で話す（8）
- NIST CSF 2.0（ニスト・シー・エス・エフ）＝アメリカの標準化機関 NIST がまとめた、サイバーセキュリティ対策の考え方。統治・識別・防御・検知・対応・復旧の 6 つ（9。訳語は IPA の訳。「識別」を「特定」と訳す資料もある）
- 「約7割」は「ウェブサイトの約7割が PHP を使う」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（W3Techs）」と小さく残す。
- 「当てる」（パッチを当てる）は使わず、「更新する」「適用する」で統一する。

ねらい（評価の観点ごと）

- 知識・技能：脆弱性・修正の公開・攻撃の関係を、時系列と根拠（一次情報）をもって説明できる。
- 思考・判断・表現：サービスを止めるかどうかの判断を、情報セキュリティの観点と、判断に必要な情報（識別・統治）から考察できる。
- 主体的に学習に取り組む態度：運営者と利用者それぞれの役割を踏まえ、情報社会の一員としての自分の行動を決めようとしている。

学習指導要領のどこに当たるか

科目・項目	本文	この授業での扱い
情報Ⅰ 2 内容 (1) ア(イ)	「情報に関する法規や制度、情報セキュリティの重要性、情報社会における個人の責任及び情報モラルについて理解すること。」	責任の分かれ目（スライド11）、自分にできること（12）
同 (1) イ (イ)	「情報に関する法規や制度及びマナーの意義、情報社会において個人の果たす役割や責任、情報モラルなどについて、それらの背景を科学的に捉え、考察すること。」	「なぜ首相まで今夜と言ったか」を、漏れ（前倒し）・公開後の差分からの攻撃・連携の根拠で説明し直す（2→13）
同 (4) ア (ア)	「情報通信ネットワークの仕組みや構成要素、プロトコルの役割及び情報セキュリティを確保するための方法や技術について理解すること。」	クライアントとサーバー（4）、RCE・CVE・CVSS（5）、協調された公開（6）
同 (4) イ (ア)	「目的や状況に応じて、情報通信ネットワークにおける必要な構成要素を選択するとともに、情報セキュリティを確保する方法について考えること。」	NIST CSF の 6 つの機能（9）、止める判断（10）
総則	第1章 第2款の2(1) 情報活用能力（情報モラルを含む）	全体

（本文は高等学校学習指導要領〈平成30年告示〉第2章第10節 情報 第2款 第1 情報Ⅰ から写した。）「公共」の情報化と社会、「総合的な探究の時間」の課題設定（例：自分の学校・部活のサイトはどこで動いているかを、管理する人に聞いて調べる）にも広げられる。

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（予想を書く）、5（近くの人と30秒、必ずやる）、7、9、10（話し合い）、13（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	首相の投稿。予想をワークシート①へ	「なぜ、そこまで急いだのか？」
6〜8分	3	止まったもの（予防のために自ら止めた。BASE は15時50分から）	—
8〜11分	4	PHP の位置（ウェブサイトの約7割＝69.2%。※言語が分かるサイトの中で）。クライアント＝ブラウザ。直すのはサーバー側	—

時間	スライド	活動	問い
11〜16分	5	PHP に 2 件の脆弱性が見つかった（2件とも 9.2、RCE）。メモリが壊れる仕組みは口で一言	**近くの人と30秒（必ず）**「3つがそろうと、なぜ最悪？」
16〜20分	6	時系列①：8月の報告→10/17 攻撃の試み→漏えい・前倒し→PoC。AWS と PHP 側の見方の割れ。AWS・PoC を一言で	—
20〜23分	7	時系列②：23時公開→26日 CISA の KEV に載る（悪用が始まった日ではない）→IPA。CISA・IPA・NCO を一言で	「被害の事例を把握していない＝被害がない？」
23〜26分	8	一般論：なぜ「修正の公開は弱点の公開でもある」か。差分（直す前と後で変わった部分）を 3 段で（AI の研究は Firefox など。PHP ではない）。急いだ理由は両方：公開前の漏れ（→前倒し）と、公開後に差分から来る攻撃	—
26〜30分	9	NIST CSF 2.0 とは何か（NIST がまとめたサイバーセキュリティ対策の考え方）。6 つは同時に回す、中心に統治	「10月21日の夜、ふだんから準備ができていなかったら困ったのは、6 つのうちどれ？」（一つでなくてよい）
30〜39分	10	話し合い（机の移動と個人1分→班5分→発表3分、3班まで）	「21時、お店のサイトを今夜止める？止めない？ 判断に必要な情報は？」
39〜42分	11	運営者と利用者の役割	—
42〜46分	12	4つの行動（「今回も」と「ふだん」を分ける）	—
46〜49分	13	ワークシート③。④（200字）は宿題でよい。①の予想を一言で言い直す	—
49〜50分	—	予備	—

計 50 分（2+1+3+2+3+5+4+3+3+4+9+3+4+3+1）。机の移動で押したら、スライド7を省く。

45 分版

スライド3（−2分）と7（−3分）を飛ばす。計 45 分（予備 1 分を残す）。KEV と IPA の話はスライド6の台本で一言触れる。

15 分の短縮版

分	スライド
2	2
3	5（30秒の問いを含む）

分	スライド
3	6
2	8
2	9
2	12
1	13（①を言い直すだけ）

計 15 分。

付録（本編に入れない）

- 付録 A（14）：侵入された後、組織の中に広がる速さ（平均29分・最速27秒、2025年の eCrime）。修正を適用する速さとは別の量。「なぜ時間で測るの？」と聞かれたとき用。
- 付録 B（15）：NICTER のダークネット観測、2016年→2025年（9年）で約4.9倍。2025年の約55%は調査目的のスキャンで、すべてが攻撃ではない。

指導の注意

- 首相の投稿は事実として扱い、政治的な評価はしない。首相の名前と投稿を映すので、管理職に一言伝えておく。
- 時刻は日本時間で示す（出典の UTC：修正版公開 14:00 UTC＝23:00 JST、漏えい 10月20日 15:00 UTC ごろ＝21日 0時ごろ、最初の PoC 21日 02:00 UTC ごろ＝11時ごろ）。
- PoC の時期は出典で見方が割れる（スライド6にも表示）。AWS は「公開の約12時間前から複数の PoC」、The PHP Foundation は「公開時点で、機能する攻撃コードは把握していなかった」。誰が、どこから観測したかで読み分ける。
- 26日は CISA の KEV カタログに載った日。悪用が始まった日ではない（攻撃の試みは公開前の17日から見られていた）。
- 前倒しの理由は番号などの漏れ（The PHP Foundation）。AWS が17日に見た攻撃の試みは、前倒しの理由には挙げられていない。
- 急いだ理由は両方：公開前の漏れ（→前倒し）と、公開した後に差分から攻撃が来ること（首相・NCO の「23時の修正をすぐ適用できる準備を」）。どちらが先・大きいとは出典に書いていない。
- スライド3：各社が言っているのは「予防的な措置」まで。攻撃される前だったかどうかは分からない。止めた時刻は会社ごとに違う（BASE は予告より早めて15時50分から。夜8時ごろから多くが続いた）。
- NCO の案内の言葉は原文どおり「…一時的に停止させることも、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」。
- スライド8の「AI で1時間足らず」は、Firefox の JavaScript エンジンと Windows のカーネルを対象に、特定の試作のモデルで行った研究室の条件の研究。PHP の話ではない。

- NIST CSF 2.0 の 6 つの機能は成果の分類で、同時に回すもの。統治はほかの 5 つを貫く中心。順番の正解を決めない。
- 怖がらせて終わらない。数字の続く枚は付録に回し、最後は自分の行動で閉じる。
- 攻撃コードや漏れた情報を「探してみる」課題は出さない。自校のサイトを外から試すこともしない。

よく出る質問と答え

- 「mod_php とは？」→ Apache というウェブサーバーの中に PHP を組み込んで動かす方式。PHP 公式は、mod_php の環境では、アプリのコードが動く前の段階で、認証なしのリクエストから攻撃が届くことを示し、リスクが最も高いとした。ほかの環境についてはそこまで言っていない。
- 「なぜメモリ不足から乗っ取りになるの？」→ 処理の途中で止まると、メモリが中途半端な状態で残る。一般に、壊れたメモリを攻撃者が自分のデータで埋められると、プログラムの流れを乗っ取って好きなコードを動かせる。109619 は、前のリクエストで解放されたメモリを指す状態が残る「解放後使用」（The PHP Foundation）。
- 「うちの学校のサイトは大丈夫？」→ どこで動いているか（教育委員会のサーバー、委託先、レンタルサーバー）による。答えるのは管理する側。情報担当の先生や教育委員会に聞く。
- 「パスワードで防げたの？」→ 防げない。今回の弱点は認証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12で「ふだん」と表示）。

授業の前日に確かめること

- IPA のページの更新（国内被害の書きぶり、KEV の記述）。事実はまだ動いている（例：約束の日時より前に修正入りのイメージを出した会社〈Chainguard〉があった、と The PHP Foundation は書いている）。
- ワークシートの印刷（A4、1 人 1 枚）。

ワークシート（worksheet-high.pdf）

- ① 授業のはじめの予想：なぜ首相まで「今夜」と言ったのか（一言）　← スライド2
- ② 話し合い：お店のサイトを今夜止める・止めない・条件つき、理由／判断に必要な情報 2 つ・利用者に何をいつ伝えるか　← スライド10
- ③ 自分がとる行動を一つ（いつ・何を・どう確かめる）　← スライド13
- ④ 10月21日に何が起きたか（200字、「脆弱性」「修正の公開」「一時停止」を使う。宿題でよい）

評価の目安：知識・技能は ④ で「番号の漏れ → 1日前倒し」と「修正の公開＝弱点の公開（公開後すぐ攻撃が来る）→ 今夜すぐ更新する・止める」の二つの因果が、取り違えずに書けているか（17日の攻撃の試みを前倒しの理由にしていないか）。思考・判断・表現は ② で「識別（どこで動いているか）」「統治（誰が決めるか）」に当たる情報が挙がっているか。主体的に学習に取り組む態度は ③ が「いつ」「どう確かめる」まで具体的か。

使った事実と出典（スライドの隅にも記載）

事実	出典
CVE-2026-109618／109619、2件とも CVSS v4.0 9.2、認証なしの RCE、mod_php のリスクが最も高い、修正版 8.5.12・8.4.27・8.3.36・8.2.35、「完全な回避策はなく更新だけが安全」	PHP 公式 https://www.php.net/archive/2026.php
2 件の仕組み（OOM で中途半端なデータ／解放後使用）、8月11日・24日の報告、本来 10月22日の予定、CVE 番号の漏えいで前倒し、動画の誤公開、23時（14:00 UTC）公開、公開時点で機能する攻撃コードは把握せず、Chainguard の早出し	The PHP Foundation（2026-10-21）
10月17日に攻撃の試みを観測、最初の PoC は公開の約12時間前、公開後数時間で PoC、「7日・30日ではなく時間で測る」	Amazon Threat Intelligence（2026-10-21）https://aws.amazon.com/blogs/security/amazon-threat-intelligence-identifies-php2shell-exploitation-prior-to-public-disclosure-in-madpot/
NCO が21日午後に注意喚起（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」）、首相投稿 21時55分ごろ	共同通信（2026-10-22）https://kumanichi.com/articles/2049509 ／ INTERNET Watch https://internet.watch.impress.co.jp/docs/news/2150203.html
IPA の注意喚起（10月22日）、CISA KEV 掲載（10月26日）、国内被害の事例は把握せず（10月27日更新）	IPA https://www.ipa.go.jp/security/security-alert/2026/alert20261022.html
サーバー側の言語が分かるサイトの 69.2% が PHP	W3Techs https://w3techs.com/technologies/details/pl-php
AI で差分から1時間足らずで攻撃コード（Firefox・Windows、試作のモデル、研究室の条件）	Anthropic Frontier Red Team（2026-06-08）https://www.anthropic.com/research/n-days
侵入から横への広がり 平均29分・最速27秒（2025年、eCrime）〔付録 A〕	CrowdStrike 2026 Global Threat Report https://crowdstrike.com/en-us/press-releases/2026-crowdstrike-global-threat-report
ダークネット観測 2016年 約1,440億 → 2025年 約7,010億パケット（9年で約4.9倍）、2025年の約55.0%は調査目的のスキャン〔付録 B〕	NICT「NICTER 観測レポート 2025」https://csl.nict.go.jp/report/NICTER_report_2025.pdf
守りの 6 機能（統治・識別・防御・検知・対応・復旧）	NIST CSF 2.0 日本語訳（IPA）https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf
止まったサービスの例、BASE は予告より早めて15時50分から停止し、のちに予防的な措置と説明	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）、ロケットボーイズの記事（BASE の案内による）https://rocket-boys.co.jp/security-measures-lab/base_emergency_database_maintenance_2026102/

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