アメリカにおける K-12 Cybersecurity Learning Standards の内容構成

Construction of K-12 Cybersecurity Learning Standards in the US

荊木　拓*　世良啓太**　宅間聖一*
IBARAKI Hiroshi　SERA Keita　TAKUMA Seiichi

市位　真*　山下義史***　森山　潤****
ICHII Shin　YAMASHITA Yoshifumi　MORIYAMA Jun

本研究では，我が国の初等中等教育におけるサイバーセキュリティ教育の推進に向け，まず，サイバーセキュリティを取り巻く現状と，日本および海外のセキュリティ教育に関わる取り組みを整理した。次に，アメリカの行政府等が連携して作成したスタンダードである K-12 Cybersecurity Learning Standards で取り扱われている内容を整理した。その結果，本スタンダードは，「コンピューティングシステム」，「デジタルシティズンシップ」，「セキュリティ」という 3 つのコアコンセプトのもと，「通信・ネットワーク」，「オンラインセーフティ」，「情報セキュリティ」など計 9 つのサブコンセプトが設定され，幼稚園から高等学校までの各発達段階に応じ，学習するトピックが設定されていた。これらの内容構成から本スタンダードは，すべての市民に必要なリテラシーレベルから，専門教育へと架橋する人材育成の視点まで体系的に包含されていると考えられた。

キーワード：サイバーセキュリティ，セキュリティ教育，初等中等教育，K-12 Cybersecurity Learning Standards，アメリカ
Key words : cybersecurity，security education，elementary and secondary education，K-12 Cybersecurity Learning Standards，the United States

1．はじめに

本研究の目的は，初等中等教育におけるサイバーセキュリティ教育の推進に向け，基礎的知見を得るために，日本および海外におけるセキュリティ教育に関わる取り組みをまとめた上で，特に，アメリカにおけるサイバーセキュリティスタンダードの K-12 Cybersecurity Learning Standards で取り扱われている内容を整理することである。

近年，サイバー空間の利用が加速している。2016 年に閣議決定された第 5 期科学技術基本計画で示されている，未来の日本社会のあるべき姿（Society 5.0）とは，サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより経済発展と社会的課題の解決を両立する，人間中心の社会（Society）であり [1]，サイバー空間の利用は加速すると予想される。

一方で，セキュリティインシデントも近年，急増している。独立行政法人情報処理推進機構（IPA）は 2022 年 7 月，「情報セキュリティ白書 2022」をまとめた [2]。同白書によると，2021 年のセキュリティインシデントの種類別報道件数が，2020 年と比較して 43.2%，増加したことを報告している。特に多かったのは不正アクセスに関する報道で，全体の約 4 割を占めていた。また，法務省がまとめた「令和 4 年版 犯罪白書」によると，不正アクセスをはじめとする，いわゆるサイバー犯罪が年々増加し，2021 年には 12209 件にのぼった [3]。このような，サイバー犯罪の増加は，世界的に見ても特に日本で顕著である。アメリカの Zscaler 社が行った調査によると，2022 年に日本へ行われたサイバー攻撃は，2021 年と比較して，613.1%となった [4]。また，トレンドマイクロ株式会社の調査によると，小学校 6 年生～中学校 3 年生のうち，17.2%がサイバー犯罪に関するトラブルを経験した事がある [5]。このように，サイバー犯罪やサイバー攻撃は年々増加しており，その標的は一般人や子供達にも及びつつある。

これに対し，政府は様々な対策を行っている。2014 年に施行されたサイバーセキュリティ基本法（平成二十六年法律第百四号）はそのひとつである [6]。同法第一章第一条では「情報通信技術の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化に伴い，情報の自由な流通を確保しつつ，サイバーセキュリティの確保を図ることが喫緊の課題となっている状況に鑑み，（中略）経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに，国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。」と掲げられている。

＊兵庫教育大学大学院（修士課程）人間発達教育専攻生活・健康・情報系教育コース
＊＊奈良教育大学
＊＊＊兵庫教育大学先端教職課程カリキュラム開発センター
＊＊＊＊兵庫教育大学大学院学校教育研究科人間発達教育専攻生活・健康・情報系教育コース 教授

令和５年７月10日受理

ここから，同法がサイバー犯罪の深刻化等を受けて策定されたものであること，そしてこの法律が持続的発展，国民が安心して暮らせること，安全の確保等を目的として策定されたものであることが分かる。また，2021年9月28日には，サイバーセキュリティ戦略が閣議決定された[7]。この閣議決定は，サイバー空間を「自由，公正かつ安全な空間」とし，サイバーセキュリティ基本法に掲げた目標を達成するべく，基本的な方向性を定めたものである。この戦略の中では，「実空間との融合が進み，あらゆる国民，セクター，地域等において，サイバーセキュリティの確保が必要とされる時代が到来」したため，「今後，サイバー空間とは繋がりのなかった主体も含め，あらゆる主体がサイバー空間に参画することとなる」と述べた上で，誰一人取り残さないサイバーセキュリティの確保を掲げ，Cybersecurity for All をコンセプトに施策を推進しようとしている。このサイバーセキュリティ戦略において，横断的・中長期的な視点を取り入れた施策の1つとして，人材の確保，育成，活躍促進が掲げられている。こういった動向を踏まえると，今後，学校現場においてもサイバーセキュリティ人材の育成を見据えた教育が行われると期待される。

前述のとおり，サイバー空間の利用が進むにつれ，サイバーセキュリティの重要性が高まりつつあるが，サイバーセキュリティの定義は一様ではない。そもそも，ISO/IEC 27032:2012では，サイバー空間を「人間，ソフトウェア，およびテクノロジーデバイスやそれに接続するネットワークを用いたインターネット上のサービスのやりとり（interaction）の結果として生じる複雑な環境で，いかなる物理的形態も存在しないもの」と，サイバーセキュリティを「サイバー空間において機密性，完全性，可用性を保持すること」と定義している[8]。また，前述のサイバーセキュリティ基本法ではサイバーセキュリティを「電子的方式，磁気的方式その他人の知覚によっては認識することができない方式により記録され，又は発信され，伝送され，若しくは受信される情報の漏えい，滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ，その状態が適切に維持管理されていること」と定義されている[6]。一方で，総務省が発行している情報通信白書には，サイバーセキュリティが守るべきサイバー空間について，「インターネットの上で多様なサービスのサプライチェーンやコミュニティなどが形成された，いわば一つの新たな社会領域」と定義されている[9]。これは，単に技術的な範囲にとどまらず，社会領域にまで視野を広げており，サイバー空間やサイバーセキュリティを広義に捉えていることが推察される。このように，サイバー空間およびサイバーセキュリティの定義は，一様でないものの，本稿では，ISO/IECが定めた元来の定義に即して，取り扱うこととする。

2．セキュリティ教育に関わる取り組み

2.1 我が国におけるセキュリティ教育

我が国におけるセキュリティ教育は1986年の臨時教育審議会に端を発する。1986年の臨時教育審議会では，初等中等教育における情報教育の重要性及び必要性を指摘した[10]。例えば，情報モラルの確立や情報活用能力の育成，技術科の選択領域として「情報基礎」の設置，小・中・高等学校を通じた体系的なコンピュータ等教育機器の活用などが提唱されている。臨時教育審議会の提唱を受け，情報教育に関する多様なプロジェクトが初等中等教育において立ち上がっている。1994年，文部省・通産省による「100校プロジェクト（ネットワーク利用環境提供事業）」は，草創期におけるパイロットプロジェクトであり，インターネットの教育利用に先導的な役割を果たしている[11]。このプロジェクトでは，学校における情報環境の整備に加え，ネットワークを用いて，国内外の学校・生徒間を繋いだ能動的な学習など，従来の枠を越えた試みやカリキュラムが数多く報告された。

こうした情報化への対応が進む中，次第に情報モラルや情報倫理に関する懸念が強まるようになった。1996年に中央教育審議会が公表した「21世紀を展望した我が国の教育の在り方について（1次答申）」では「『ハッカー』等は許されないといったコンピュータセキュリティーの必要性に対する理解等の情報モラルを，各人が身に付けることが必要であり，子供たちの発達段階に応じて，適切な指導を進める必要がある」と示された[12]。つまり，セキュリティに関わる内容は，前出の臨時教育審議会に端を持つ情報モラルの一部として捉えられていた。これを受け1998年および1999年告示の学習指導要領では，中学校 技術･家庭科 技術分野（以下，技術科）や高等学校 情報科などにおいて情報モラルに関する記載がなされた[13][14]。特に，情報科の科目「情報C」においては，セキュリティに関わる内容も学習指導要領に記載されており，個人認証，暗号化，情報通信ネットワークの保守・管理等の重要性を取り扱うこととされた。

2000年代に入ると，インターネットの急速な発達に伴い，ネットワーク上において，子供に関するトラブルが多発した[15]。これに対し，文部科学省は，「情報モラル等指導サポート事業」を実施し，情報モラル教育を推進した[16]。この事業では，情報モラルの効果的な指導手法の調査研究が行われたり，情報モラルの指導を普及するフォーラムが開催されたりした。そうした成果の1つとして2007年に「情報モラル指導モデルカリキュラム」が公表され，情報モラルが「情報社会の倫理」「法の理解と遵守」「安全への知恵」「情報セキュリティ」「公共的なネットワーク社会の構築」の5つに細分化された[17][18]。これによってセキュリティに関わる内容が情報モラルの1つであると明示された。

情報モラルは道徳との関係性も高く，2008年7月に示された中学校学習指導要領解説 道徳編では「情報モラルの問題に留意した指導」として「情報モラルにかかわる題材を生かして話合いを深めたり，コンピュータ

による疑似体験を授業の一部に取り入れたり，生徒の生活体験の中の情報モラルにかかわる体験を想起させたりする工夫などが考えられる」と記載された[19]。一方で，同解説 技術・家庭編では，技術科の内容「D情報に関する技術」の「(1) イ 情報通信ネットワークにおける基本的な情報利用の仕組みを知ること。」において，「情報セキュリティの確保のために対策・対応がとれるよう，D (1) のウと関連させて指導するよう配慮する。」と記載された[20]。ここで内容「D (1) のウ」は，「著作権や発信した情報に対する責任を知り，情報モラルについて考えること。」であるため，情報セキュリティが情報モラルと関連しつつも独立したものとして考えられるようになったと推察される。加えて，その翌年に示された高等学校学習指導要領においては，情報科が「社会と情報」「情報の科学」の2科目となったものの，いずれの科目においても学習指導要領に情報セキュリティの指導が示された[21]。

2017年3月告示の中学校学習指導要領においては，技術科で，情報モラルに加えて情報セキュリティの技術の仕組み等の取り扱いが示されたほか，「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」とされ，情報 / サイバーセキュリティが義務教育段階で取り扱われることとなった[22]。また本改訂では，問題解決学習を重視した教育課程の展開が強調されている。つまり，技術科における各内容（A）-（D）は，大きく分けて，「生活や社会を支える技術」「技術による問題の解決」「社会の発展と技術」の3要素に区分され，生活や社会を支える技術の原理・法則を理解し，問題解決学習を展開し，そしてこれからの技術の発展を考えていくといった学習過程が示された。特に内容「D情報の技術」では，問題解決学習が他内容と違い2項目が設定されており，より時間数が割かれて指導されるものと予想される。一方，2017年7月に公開された中学校学習指導要領解説　特別の教科　道徳編において，情報モラルの内容は「情報社会の倫理，法の理解と遵守，安全への知恵，情報セキュリティ，公共的なネットワークがあるが，道徳科においては，（中略）特に，情報社会の倫理，法の理解と遵守といった内容を中心に取り扱うことが考えられる。」と述べられ，セキュリティに関わる内容は，道徳科であまり扱われないこととなった[23]。

2018年に示された高等学校学習指導要領では，情報Ⅰにおいて「(1) 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。」と，「(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。」が示された[24]。加えて，同解説 情報編においては，小規模な情報ネットワークを構築したり不具合を解決したりすることが示された[25]。これは，開発者や管理者など，サイバーセキュリティ人材育成へと繋がる内容であるといえる。

以上を俯瞰してみると，我が国におけるセキュリティ教育は情報モラルの一部として捉えられてきたが，近年になり情報モラルとは独立したものと考えられるようになってきたことが分かる。また，セキュリティ教育を中心的に担うと想定される技術科および情報科では，今後，科学的な原理・法則に基づいた，サイバーセキュリティ人材育成へと繋がる内容が展開されると分かる。これらを踏まえ，情報モラルは「情報モラル指導モデルカリキュラム」のような独立した体系的なモデルカリキュラムが存在するものの，セキュリティに関しては，独立した体系的で科学的理解に基づいたモデルカリキュラムは管見の限り見当たらなかった。初等中等教育におけるサイバーセキュリティ教育を推進する上では，そのようなカリキュラムやスタンダードが必要となってくると考えられる。

2.2 海外におけるセキュリティ教育

サイバーセキュリティに対する関心は海外においても高く，国家戦略として様々な取り組みを行っているだけでなく，セキュリティ教育にも力を入れて取り組まれている。例えば，イギリス政府は，National Cyber Security Strategy 2022を公開し，2030年まで民主的サイバー大国としての地位を保ち，サイバー空間を通じて国益を保護・増進することを目標として掲げた[26]。そのためにサイバーセキュリティ人材を育成するための学習プログラムや低年齢向けのイベント等を政府主導で開催する他，サイバーセキュリティについての相談ができるような「サイバーレジリエンスセンター」をイギリス全土に設置するとしている。

また，アメリカでは2016年に第44代大統領であるバラク・オバマが発表したサイバーセキュリティ・ナショナル・アクション・プランにおいて，190億ドルの予算を確保し，サイバーセキュリティ関連の人材確保や脆弱性のあるシステムの置き換え，サイバーセキュリティ分野での官民の連携等を行うとした[27]。このプランに基づき，National Institute of Standards and Technology（以下NIST）は2018年にCybersecurity Frameworkと呼ばれる，企業や組織がサイバーセキュリティを強化するための指針を作成・公開した[28]。

Association for Computing Machineryの下部組織Computer Science Teachers Associationは2012年にCSTA K-12 Computer Science Standardsを公開した[29]。このCSTA K-12 Computer Science Standardsは，幼稚園から高等学校までのすべての子供に向けた，コンピュータサイエンスに特化したカリキュラムであるものの，「ネットワークとインターネット」の中に「サイバーセキュリティ」という項目が設けられるなど，サイバーセキュリティに関する内容も散見されるスタンダードとなっている。

これに対し，非営利組織Cyber Innovation Center（以下，CIC）は，アメリカの行政府と協力の上，2021年にサイバーセキュリティ教育に特化したK-12

Cybersecurity Learning Standards を公開した[30]。この K-12 Cybersecurity Learning Standards は，幼稚園から高等学校までのすべての子供に，科学的理解に基づいたサイバーセキュリティ教育を行うことを目的として作られた体系的なスタンダードである。加えて，サイバーセキュリティに関わる基礎的な内容が網羅されているスタンダードであるため，サイバーセキュリティ人材を育成する高等教育機関等ともシームレスに接続することが出来る。こうした特徴を持つ K-12 Cybersecurity Learning Standards であるが，その内容を整理した例は国内では見当たらなかった。そこで，本稿では K-12 Cybersecurity Learning Standards を取り上げ，その内容を整理することとした。

3．K-12 Cybersecurity Learning Standards の内容整理

3.1 K-12 Cybersecurity Learning Standards の概要と位置づけ

K-12 Cybersecurity Learning Standards（以下，本スタンダード）は，CIC が立ち上げた CYBER.ORG（the National Integrated Cyber Education Research Center）によって 2021 年 8 月に公開された。本スタンダードは幼稚園児から 12 年生までを対象とした，アメリカ 50 州で統一された，サイバーセキュリティに特化したスタンダードである。

本スタンダードの開発は 2020 年 9 月に遡るが，将来的に，世界中で 180 万人のサイバーセキュリティ人材が将来的に不足し，現在や将来を生きるすべての子供が，巧妙化しつつあるサイバー攻撃の猛威に直面すると予測されていた。そのため，すべての子供達が「サイバー空間で安全かつ倫理的に生活し，遊び，良きデジタル市民として成長すること」および将来のサイバーセキュリティ人材の育成を見据えた教育を行うことは，喫緊の課題となっていた。一方で，アメリカの教育においては，前述したコンピュータサイエンスに特化したカリキュラムや，一般向けのサイバーセキュリティに関わるガイドラインは存在したものの，サイバーセキュリティ教育に特化した子供向けのスタンダードは無かった。そこで，前述の課題の解決に向け，アメリカ 50 州で統一された国家的な学習基準を作成し，サイバーセキュリティ教育を推進していくことを目標として，アメリカの行政機関である Cybersecurity and Infrastructure Security Agency（以下，CISA）や NIST が運営・主導するパートナーシップである National Initiative for Cybersecurity Education などの省庁や関係機関等が連携しながらプロジェクトが開始された。その約 1 年後の 2021 年 8 月，省庁や関係機関等のステークホルダーら計 65 名の手によって本スタンダードは完成した。

なお，本スタンダードは教師だけでなく教育委員会関係者やインフォーマル教育における教育者等，様々なレベルで利用することを想定されており，クリエイティブコモンズライセンスの下で提供されている。

3.2 K-12 Cybersecurity Learning Standards の体系表

本スタンダードでは，「3 つのコアコンセプトを中心に，サイバーセキュリティ教育における重要な基礎となる要素を全て備えている」と述べられているように，中心となる「コンピューティングシステム」，「デジタルシティズンシップ」，「セキュリティ」の 3 つのコアコンセプトを定めている。さらに，各コアコンセプトに 3 つずつのサブコンセプトを，各サブコンセプトに 2 ～ 5 つの，合計で 29 のトピックを定めている。各トピックでは，幼稚園から高等学校までの，各発達段階（K-2, 3-5, 6-8, 9-12）に応じて学ぶべき内容とその目標を体系的に整理している。和訳したコアコンセプトとサブコンセプト，トピックの一覧を表 1 に示す。

本スタンダードでは，サイバーセキュリティ教育を「接続された電子機器がデジタル時代にどう作用していくのか，情報資産を脆弱性からどう保護していくのか，について理解させるとともに，我々の社会で利用される技術を取り巻く道徳的・倫理的な問題を理解させること。」と説明した上で，コアコンセプトについて「サイバーセキュリティ教育における主要な，概念または目的」を表していると述べている。また，例えばデジタルシティズンシップについては，2020 年に欧州評議会が内容を 3 分野 10 領域に分け体系的に整理した[31]ものの，

表 1: K-12 Cybersecurity Learning Standards のコアコンセプトとサブコンセプトとトピック

コアコンセプト	サブコンセプト	トピック
コンピューティングシステム	通信・ネットワーク	ネットワーク通信，ネットワーク機器，クラウドコンピューティング，プロトコル，データ損失
	ハードウェア	接続機器，IoT，オペレーティングシステム
	ソフトウェア	ソフトウェアアップデート，プログラミングとスクリプト
デジタルシティズンシップ	オンラインセーフティ	ネットいじめ，デジタル足跡，個人情報
	エシックス	脅威アクター，倫理的誠実さ
	政策・法的問題	規則・法律・規則，知的財産，利用規約・ユーザー規約
セキュリティ	情報セキュリティ	CIAトライアド，アクセス制御，データセキュリティ，脅威と脆弱性，暗号化
	ネットワークセキュリティ	認証，ネットワーク機器の保護，脅威と脆弱性
	物理的セキュリティ	脅威と脆弱性，セキュリティ制御

その内容は多岐に渡り，本スタンダードの「デジタルシティズンシップ」で取り扱われている内容よりも広い。つまり「コンピューティングシステム」,「デジタルシティズンシップ」,「セキュリティ」それぞれの分野から，サイバーセキュリティ教育に関わりの深い内容のみを取り上げていると考えられる。

そもそも本スタンダードでは，各コアコンセプトについて，「コンピューティングシステムには，目的を達成するため，相互に関連するハードウェアとソフトウェアが含まれる。サイバーセキュリティの専門家は，攻撃者がコンピューティングシステムの弱点を突いて機密性・完全性・可用性を破壊することを防ぐ。」,「デジタルシティズンシップには，組織や個人に影響を与える規範・通例・法律・政策など，社会において責任ある適切な技術の利用に関することを含んでいる。」,「セキュリティの特徴として，コンピュータネットワークへのアクセスの保護，全ての物理的な装置への安全なアクセス，個人情報および組織のデータを保護するための説明責任などが挙げられる。」と説明している。加えて，サイバーセキュリティに関わる用語については，表2のように定義されており，こういった定義に基づいてスタンダードが構成されていると分かる。以下に各コアコンセプトにおける具体的な目標の例と特徴を示す。

(1) コンピューティングシステム

コアコンセプト「コンピューティングシステム」の各トピックにおける，学年ごとの目標とその内容を和訳したものを資料1～3に示す。「コンピューティングシステム」には,「通信・ネットワーク」,「ハードウェア」,「ソフトウェア」の3つのサブコンセプトが設定されており,「通信･ネットワーク」には5つの,「ハードウェア」と「ソフトウェア」には3つのトピックが設定されている。例えば「ハードウェア」に設定されているトピック「オペレーティングシステム」において，幼稚園児から2年生段階（K-2）では,「オペレーティングシステムの役割を説明できる」という目標が，3年生から5年生段階（3-5）では,「様々なオペレーティングシステムの役割を区別することができる」という目標が掲げられている。また，6年生から8年生段階（6-8）では,「時代遅れのオペレーティングシステムのリスクについて議論できる」という目標が，9年生から12年生段階（9-12）では,「オペレーティングシステムを堅牢にするための計画を立てることができる」という目標が掲げられている。このようにコアコンセプト「コンピューティングシステム」では，サイバーセキュリティに深く関わるコンピュータの仕組みや機能等について取り扱われている。

(2) デジタルシティズンシップ

コアコンセプト「デジタルシティズンシップ」の各トピックにおける，学年ごとの目標とその内容を和訳したものを資料4～6に示す。「デジタルシティズンシップ」には,「オンラインセーフティ」,「エシックス」,「政策･法的問題」の3つのサブコンセプトが設定されており,「オンラインセーフティ」および「政策・法的問題」には3つの,「エシックス」には2つのトピックが設定されている。例えば「オンラインセーフティ」に設定されているトピック「デジタル足跡」において，幼稚園児から2年生段階では,「ネット上でのいい行動と悪い行動を区別することができる」という目標が，3年生から5年生段階では,「デジタル足跡の概念を説明する」という目標が掲げられている。また，6年生から8年生段階では,「デジタル足跡を構成する多くのデータソースがあることを認識する」および「デジタル足跡の永続性を認識する」という2つの目標が，9年生から12年生段階では,「デジタル足跡について，プラスとマイナスの両面から意味を検討する」という目標が掲げられている。このようにコアコンセプト「デジタルシティズンシップ」では，サイバーセキュリティに関わる倫理的・法的な技術の取り扱い等について，目標が定められている。

(3) セキュリティ

コアコンセプト「セキュリティ」の各トピックにおける，学年ごとの目標とその内容を和訳したものを資料7～9に示す。「セキュリティ」には,「情報セキュリティ」,「ネットワークセキュリティ」,「物理的セキュリティ」の3つのサブコンセプトが設定されており,「情報セキュリティ」には5つの,「ネットワークセキュリティ」には3つの,「物理的セキュリティ」には2つのトピックスが設定されている。例えば「ネットワークセキュリティ」に設定されているトピック「脅威と脆弱性」において，幼稚園児から2年生段階では,「情報交換の方法と，なぜその方法が保護されなければならないかを理解できる」という目標が，3年生から5年生段階では,「情報交換のためのオープンな手法の脆弱性について議論できる」という目標が掲げられている。また，6年生から8年生段階では,「悪意のある行為がネットワークセキュリティを脅かすことを説明できる」という目標が，9年生から12年生段階では,「ネットワークセキュリティに影響を与える様々な種類の攻撃を分析できる」という目標が掲げられている。このようにコアコンセプト「セキュリティ」では,物理的な保護を含む,コンピューティングシステムを保護する方法について，サイバーセキュリティに関わる基本的な内容が取り扱われている。

それぞれのトピックでは，発達段階が上がるにつれて，より高度かつ開発者やサイバーセキュリティ人材を意識した内容が展開されている。例えばコアコンセプト「コンピューティングシステム」のサブコンセプト「通信・ネットワーク」のトピック「クラウドコンピューティング」では，幼稚園児から2年生段階において「クラウドコンピューティングを利用した，情報の保存と共有についての利点を述べられる」と述べられており，単に利点を述べられることを目標としているが，9年生から12年生段階では「クラウドコンピューティングの

表 2: K-12 Cybersecurity Learning Standards に記載されている用語集

用語	定義
AAA	AAAフレームワークは，組織が情報セキュリティをどのように保護するのかを説明する上で，CIAトライアドを補足するものである。AAAフレームワークは，Authentication（認証），Authorization（認可），Accounting（アカウンティング）から成る。
アクセス制御	アクセス制御は，個人が表示・利用の許可されている情報へアクセスするため，認証・承認を行う。アクセス制御は，ユーザー本人であること，およびデータへの適切なアクセス権を持っていると保証する方法である。
利用規約（AUP）	プライベートネットワーク上で許可される活動を定義した，書面による合意のこと。
アカウンティング	アカウンティングでは，どのユーザーがシステムにアクセスし，どのリソースを利用しているのか追跡する方法を提供する。具体的には，通常業務を規定するためのリスト（ベースライン），潜在的不正アクセスを発見するためにユーザーの行動を監査する能力（フォレンジック）が含まれる。
AI，バーチャルアシスタント	いわゆる「スマート」なデバイスには，デジタルパーソナルアシスタントが含まれている。具体的には，Google，Alexa（Amazon），Siri（Apple）などがある。
アナログネットワーク	アナログ信号によって論理的にデータを伝送する手段のこと（つまり，伝送される信号は全てアナログ波形である）。
認証	認証は，ユーザーを識別するための方法を提供する。認証プロセスでは通常，有効なユーザーの認証情報を必要とし，知識情報，所持情報，生体情報，位置情報，行動情報によって確認される。
認可	認可はセキュリティ管理において定義された，認証ユーザーの権限に基づき，リソースや情報へのアクセスを提供する。認可の概念では，ユーザーがアクセスできるもの，できないものを制御する。
セルラー方式ネットワーク	モバイル機器にネットワーク接続を提供するための，タワーとアクセスポイントから成る無線ネットワーク。各タワーが担当するエリアを「セル」と呼ぶため，セルラーと呼ばれる。モバイル機器の位置がセルから次のセルに移動すると，機器の接続は，次のセルに転送される。
認証局（CA）	デジタル署名された，組織の素性を認証するための証明書を提供する，信頼された者。
証明書	公開鍵基盤（PKI）を構成する要素の1つで，多くは，通信を暗号化するための公開鍵を提供し，信頼できる認証局（CA）を通じて組織の素性を確認するために利用される。
CIAトライアド	組織内の情報セキュリティに関するポリシーの基準として設計された3つの部分から成るモデル。ここでは，機密性とは，情報へのアクセスを制限する一連の規則であり，完全性とは，情報が信頼でき正確であると保証することであり，可用性とは，権限を与えられた人々の情報へのアクセスを保証することである。
暗号	不正なアクセスを防ぐ目的で，メッセージを見えなくするため使用される可逆的な方法やアルゴリズムのこと。
クラウドコンピューティング	ネットワーク上で共有されるコンピュータのリソースのことで，内部構造がエンドユーザーから抽象化されている。
通信チャンネル	情報を交換するための手段や媒体のこと。
著作権	著作物または出版物の複製物を一定期間，所有者が独占的に作成する権利（特許に似ている）。
サイバーセキュリティ	ネットワークやデバイス，データを不正な利用から守ること。
多層防御	複数の防衛手段が連動してセキュリティを確保する方法のことで，レイヤー防御と呼ばれることもある。
ダイジェスト	ハッシュアルゴリズムによる最終結果または出力のこと。
デジタルシティズンシップ	社会とのかかわりを持つため，コンピュータ技術を，責任をもって適切に使用すること。
デジタル足跡	インターネット上で利用できる，現実や仮想の個性を構成する，公的および私的な情報。
デジタルネットワーク	デジタル信号によってデータを論理的に伝送する手段（つまり，伝送される信号は全てアナログ波形である）。
任意アクセス制御（DAC）	情報へのアクセスは，データを作成または保存しているユーザーによって制御される。
暗号化	不正なアクセスを防ぐ目的で，メッセージを見えなくする可逆的なプロセスのこと。逆は，復号と呼ばれる。
フェアユース	適切な帰属情報が提供される場合に，法律によって認められる，著作物の限定的な使用のこと。
ファイヤーウォール	特定の基準に基づき，許可されたネットワークトラフィックと，許可されていないネットワークトラフィックをフィルタリングするネットワーク機器。
ハッキング	システムに対して不正にアクセスする行為。
ハードウェア	電気回路が連携して，ソフトウェアを実行し，演算を行うもの。
ハッシュ衝突	ハッシュアルゴリズムにおいて，2つの別々な入力が同じ出力（ダイジェスト）を生成すること。
ハッシュ化	一方通行で不可逆的なプロセス・アルゴリズムのことであり，与えられた入力に対して，それぞれ固有のダイジェストまたは文字と数字の固定長文字列を生成する。同じダイジェストは2つとない。
知的財産権	個人または組織が所有するプロセス，アイデア，デザインなどの無体（物理的でない）創造物を指す。
インターネットプロトコル（IP）	インターネットを構成する主要なプロトコル。この形式のデータはパケットに分割され，ネットワークアドレスに基づいて，送信元から送信先までルーティングされる。IPパケットは，TCPまたはUDPパケットにフォーマットされる。
モノのインターネット（IoT）	インターネットに接続され，日常生活の中で何らかの機能を自動的に実行する機器（例，サーモスタット・ドアベル）。
ローカルエリアネットワーク（LAN）	小さな単一の地理的領域内に含まれる，プライベートネットワーク（多くの場合，10.x.x.xや192.168.x.xなどのプライベートネットワークアドレスが使用され，識別される）。
強制アクセス制御	情報へのアクセスは，データが保管されているまたはアクセスするコンピュータのオペレーティングシステムによって制御される。
MAC（Media Access Control）アドレス	ネットワーク通信を確立する際に，ネットワークインターフェースと他のネットワークインターフェースを区別するために使用される固有の識別子。このアドレスは製造者によって設定され変更できないが，ソフトウェアによって別の値を機器に伝達できる。
ネットワーク機器	ネットワークに接続されている，またはネットワークを構成する機器（ハードウェア）。
ネットワーク中立性（ネット中立性）	ネット中立性とは，すべてのインターネットサービスプロバイダー（ISP）が，すべてのインターネット通信を差別なく平等に扱わなければならないとする原則のこと。基本的にネット中立性は，ISPが意図的にオンラインコンテンツへのアクセスをブロックしたり，速度を落としたり，課金制にしたりしないようにしている。
ネットワーク構成	ネットワークの概念的な組織や構造。
否認防止	アイテムの所有権や著作権について，争うことが出来ないこと。
パッチ	プログラムのセキュリティ上の脆弱性や致命的なエラーなど，予測しない動作を抑制するためのソフトウェアアップデート。
特許	ある製品を生産したり独自の生産プロセスを一定期間，権利者が独占的に使用する権利（著作権に似ている）
永続性	オンラインのデジタルコンテンツを，確実に削除出来ないこと。
個人情報	特定の個人を識別することができるデータ。
プロトコル	情報交換の際に利用される構造およびフォーマットからなる通信規格であることが多い。
公開鍵暗号	公開鍵を使用してデータを暗号化し，一致する秘密鍵を持つユーザーによってのみ，簡単に復号化することができる。
公開鍵基盤（PKI）	公開鍵暗号に必要な証明書に署名し，保護する信頼システムを構成するプロセスと技術。
ロールベースアクセス制御	情報へのアクセスは，組織内での個人の役割に依存します。
ソフトウェア	コンピュータ機器がオペレーションを実行するため，コードで書かれた一連のステップのこと。
利用規約（ToS）	エンドユーザーに提供するサービスの種類と，エンドユーザーおよびそのデータに関する組織の運営方法を説明する，組織との合意書のこと。
データの3つの状態	データの3つの状態とは「使用中のデータ」（現在アクセス中），「停止中のデータ」（アクセスを待っている），「移動中のデータ」（ある場所から別の場所に移動している）を指す。
商標	ブランドや組織を識別するために使用される，固有の図形，シンボル，またはロゴのこと。
伝送制御プロトコル（TCP）	TCPのデータのパケットは，信頼性が高く（確実に届く），連続性があり，送信エラーがないことを目的としている。TCPパケットには，パケットの正常な受信を確認するための情報，パケットを送信した順序，データがそのまま到着したことを確認するためのチェックサムが含まれている。TCPの利点は配信の保証にある。
ユーザーデータグラムプロトコル（UDP）	UDPのデータのパケットは，確認なしに送信され，順番通りに到着しない場合がある。またUDPパケットは，全く到着しないこともある。遅れて到着したUDPパケットや，順番に到着しないUDPパケットは，単に無視される。UDPの利点は，ネットワークのオーバーヘッドが少ないことにある。
ワイドエリアネットワーク（WAN）	広い地域に張り巡らされたネットワーク。
ワイヤレスローカルエリアネットワーク（WLAN）	ネットワーク上の機器同士の接続に無線リンクを利用するネットワークで，多くの場合，有線ネットワーク上のリソースにアクセスするため，無線アクセスポイント（WAP）を利用する。

リスクと利点を評価する」とされており，開発者や管理者を想定した，かつ技術を評価し社会創造しようとする視点を含んだ目標であると言える。

このように本スタンダードでは，1 人の利用者を想定した内容から開始し，学年が上がるにつれて開発者やサイバーセキュリティ人材育成へと繋がる内容が展開されていることが分かる。

4．まとめと今後の課題

本稿では初等中等教育におけるサイバーセキュリティ教育の推進に向け，近年のサイバー空間およびサイバーセキュリティに関する動向をまとめた上で，国内外におけるセキュリティ教育に対する取り組みを整理した。また，2021 年に CYBER.ORG や CISA などによって作成された K-12 Cybersecurity Learning Standards について整理した。

その結果，本スタンダードは 3 つのコアコンセプト，9 つのサブコンセプト，29 のトピックから構成されており，各トピックでは K-2，3-5，6-8，9-12 の各年齢において取り扱う内容が定められていた。そして，学年が上がるにつれて開発者やサイバーセキュリティ人材育成へと繋がる内容が展開されていた。

今後，学校現場においてもサイバーセキュリティ人材の育成を見据えた教育が期待されることを踏まえると，K-12 Cybersecurity Learning Standards のような海外の枠組みを適用した学習内容の展開が考えられる。ただしその際には，これまで我が国の情報 / サイバーセキュリティ教育で行われてきた学習内容が，海外のスタンダードにおいて，どの部分に位置づけられるのか分析を行う必要があるが，これについては今後の課題とする。また，他のスタンダードやサイバーセキュリティ人材に求められる力などと比較し，本スタンダードが適切であるか検討することも，今後の課題として挙げられる。

参考文献

1） 内閣府：Society 5.0，https://www8.cao.go.jp/cstp/society5_0/（2023.06.14 最終閲覧）

2）独立行政法人情報処理推進機構：情報セキュリティ白書 2022，独立行政法人情報処理推進機構（2022）

3）法務省法務総合研究所：令和 4 年版犯罪白書，日経印刷（2022）

4）ThreatLabz：The State of Encrypted Attacks，https://info.zscaler.com/resources-industry-reports-the-state-of-encrypted-attacks-2022（2023.06.14 最終閲覧）

5）トレンドマイクロ株式会社：子どもと保護者のスマートフォン利用に関する実態調査 2020，https://www.trendmicro.com/ja_jp/about/press-release/2020/pr-20200310-01.html（2023.06.14 最終閲覧）

6）デジタル庁：e-Gov 法令検索　サイバーセキュリティ基本法（平成二十六年法律第百四号），https://elaws.e-gov.go.jp/document?lawid=426AC1000000104（2023.06.14 最終閲覧）

7）内閣サイバーセキュリティセンター：サイバーセキュリティ戦略（閣議決定），（2021）

8）ISO：ISO/IEC 27032:2012（Information technology—Security techniques—Guide lines for cybersecurity），（2018）

9）総務省：平成 24 年度版 情報通信白書，ぎょうせい（2012）

10）臨時教育審議会：二十一世紀に向けての教育の基本的な在り方（第二次答申），（1986）

11）中村圭一：100 校プロジェクトにおけるネットワークの教育利用，電子情報通信学会技術研究報告，Vol.96（579），pp.15-22（1997）

12）中央教育審議会：21 世紀を展望した我が国の教育の在り方について（1 次答申），（1996）

13）文部省：中学校学習指導要領，文部省（1998）

14）大蔵省印刷局編：高等学校学習指導要領 : 文部省告示，大蔵省印刷局（1999）

15）石原一彦：情報モラル教育の変遷と情報モラル教材，岐阜聖徳学園大学紀要，Vol.50，pp.101-116（2011）

16）一般財団法人 コンピュータ教育推進センター：情報モラル等指導サポート事業，http://www.cec.or.jp/monbu/17jmoral.html（2023.06.14 最終閲覧）

17）文部科学省：情報モラル指導モデルカリキュラム，https://www.mext.go.jp/a_menu/shotou/zyouhou/1296900.htm（2023.06.14 最終閲覧）

18）小孫康平：情報モラル教育の研究動向と教育方法学における指導方法，皇學館大学紀要，Vol.57，pp.256-237（2019）

19）文部科学省：中学校学習指導要領解説，道徳編，日本文教出版（2008）

20）文部科学省：中学校学習指導要領解説 , 技術・家庭編，教育図書（2008）

21）文部科学省：高等学校学習指導要領，東山書房（2009）

22）文部科学省：中学校学習指導要領（平成 29 年告示），東山書房（2018）

23）文部科学省：中学校学習指導要領（平成 29 年告示）解説 , 特別の教科 道徳編，教育出版（2018）

24）文部科学省：高等学校学習指導要領（平成 30 年告示）：平成 30 年 3 月告示，東山書房（2019）

25）文部科学省：高等学校学習指導要領（平成 30 年告示）解説 , 情報編，開隆堂出版（2018）

26）United Kingdom of Great Britain and Northern Ireland Cabinet Office：National Cyber Strategy 2022，（2022）

27）八山幸司：米国オバマ政権における IT 政策の総括と次期トランプ政権の IT 政策の展望，独立行政法人日本貿易振興機構，（2016）

28）National Institute of Standards and Technology：CYBERSECURITY FRAMEWORK，https://www.nist.gov/cyberframework（2023.06.14 最終閲覧）

29）Computer Science Teachers Association：CSTA K-12 Computer Science Standards，https://csteachers.org/Page/

standards（2023.06.14 最終閲覧）
30）CYBER.ORG：K-12 Cybersecurity Learning Standards，https://cyber.org/standards（2023.06.14 最終閲覧）
31）Council of Europe：DIGITAL CITIZENSHIP EDUCATION Trainers' Pack，https://rm.coe.int/16809efd12（2023.06.14 最終閲覧）

資料１「通信・ネットワーク」の各トピックにおける，学年ごとの目標と内容

		K-2	3-5	6-8	9-12
通信・ネットワーク	ネットワーク通信	**・オンラインの概念を明確化する** ネット接続の例とデバイスを介した接続の利点について、説明する。生徒は、インターネットがグローバルに接続されたネットワークサービスであり、コンピュータの中にないことを理解する必要がある。 **・機器のオンライン利用とローカル利用の違いについて説明できる** すべてがオンラインである訳ではないこと、すべてが接続できる訳ではないこと、ネットワークがデバイス同士を接続していること、インターネットが世界中の何百万ものデバイスを接続していることなど、学年相応の例に焦点を当てる必要がある。	**・ネットワーク通信について説明できる** これまでの学習内容に加え、接続された機器間の情報交換としてのネットワーク通信について、学年相応の例に焦点を当てて取り扱う。	**・ネットワーク構成を比較する** これまでの学習内容に加え、LANやWANの構成の学年相応の例に焦点を当てる必要がある。 **・ネットワークデバイスのMACアドレスとIPアドレスを区別できる** パブリックIPアドレス、プライベートIPアドレスなどのIPアドレス体系を見分けられる。生徒は、MACアドレスとIPアドレスがあることを理解する必要がある。	**・OSI参照モデルの層について説明できる** これまでの学習内容に加え、OSI参照モデルの7つの層に関して、学年相応の例にに焦点を当てる必要がある。また、様々なネットワークの層の役割を説明できる。
	ネットワーク機器	**・ネットワークにアクセスするには機器が必要だと認識する** ネットワーク接続するには、複数の機器が必要だと例を出しながら話す。生徒は、インターネットが1つの機器の中にあるわけではないことを知り、インターネット接続のために様々な機器が必要だと知る。	**・特定のネットワーク機器を見分けられる** これまでの学習内容に加え、アクセスポイント、ハブ、スイッチ、ルーター、ユーザー機器など、様々なネットワーク機器の学年相応の例に焦点を当てる必要がある。	**・接続されたネットワーク機器の役割を見分けられる** これまでの学習内容に加え、アクセスポイント、ハブ、スイッチ、ルーター、ユーザー機器など、様々なネットワーク機器の学年相応の例に焦点を当てる必要がある。	**・適切なネットワーク機器を使用して、ネットワークの図を作成できる** これまでの学習内容に加え、アクセスポイント、ハブ、スイッチ、ルーター、ユーザー機器など、様々なネットワーク機器を含む図を、学年相応の例に焦点を当てながら取り扱う。
	クラウドコンピューティング	**・クラウドコンピューティングを利用した、情報の保存と共有についての利点を述べられる** ネットワーク/インターネットベースのストレージとして定義される、クラウドコンピューティングについて、学年相応の例を中心に取り扱う。	**・クラウドコンピューティングを使用して、情報を保存し共有する方法を示すことができる** これまでの学習内容に加え、接続されたドライブや、Google Docsなど、学年相応の例に焦点を当てる必要がある。 **・安全なクラウドコンピューティングを実践する** これまでの学習内容に加え、ログイン、ログアウトなどの安全なクラウドコンピューティングの実践について、学年相応の例に焦点を当てる必要がある。	**・様々なクラウドコンピューティングモデルの利点と欠点を認識する** これまでの学習内容に加え、パブリッククラウド、コミュニティクラウド、プライベートクラウドなど、クラウドコンピューティングモデルの、学年相応の例に焦点を当てる必要がある。	**・クラウドコンピューティングのリスクと利点を評価する** これまでの学習内容に加え、クラウドコンピューティングの様々なリスクと利点について、学年相応の例に焦点を当てて取り扱う必要がある。クラウドコンピューティングの例としては、IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）、SaaS（Software as a Service）、といった様々な「aaS（as a Service）」などが挙げられる。また、クラウドコンピューティングの利点としては、環境災害によるデータ損失を防ぐ分散ストレージ、遠距離にいるユーザーとの共同作業、利用されないサーバーを購入しないことによるコスト削減（必要な分だけ支払う）など様々な点が挙げられる。クラウドコンピューティングのリスクとしては、クラウド事業者のミスによる不正アクセス、ユーザーへの不正な権限付与、不注意によるデータの公開などが考えられる。
	プロトコル	**・オンラインで利用できる様々なサービスを見分ける** WEB、電子メール、ビデオ、ゲームなどのオンラインサービスについて、学年相応の例を取り扱う必要がある。	**・オンラインで利用できる様々なサービスについて説明できる** これまでの学習内容に加え、WEB、電子メール、ビデオ、ゲーム、Googleドライブ、ネットワークドライブなど、様々なオンラインサービスの学年相応の例に焦点を当てて取り扱う。	**・オンラインで利用できる様々なサービスに使用されるプロトコルを見分ける** これまでの学習内容に加え、WEB、電子メール、ビデオ、ゲーム、TCP（WEBと電子メール）、UDP（ビデオとゲーム）、HTTP、HTTPSなど、様々なオンラインサービスについて、学年相応の例に焦点を当てて取り扱う必要がある。	**・オンラインで利用できる様々なサービスについて、使用されているポートとプロトコルを比較できる** これまでの学習内容に加え、TCPとUDPに関連する様々なプロトコルの学年相応の例に焦点を当てて、取り扱う。TCPの例としては、HTTPやHTTPS（WEB）、IMAPやPOP3（電子メール）などがある。UDPの例としては、音楽/音声、DNS、DHCP、ゲームなどが上げられる。 **・オンラインで利用できる様々なサービスに関するリスクを見分けられる** これまでの学習内容に加え、TCPやUDPがもたらすリスクについて、学年相応の例に焦点を当てて取り扱う必要がある。
	データ損失	**・データの損失とサービス停止について明確化する** 作品を保存するプロセスなど、データの損失を回避するための学年相応の例に焦点を当てる必要がある。	**・バックアップの役割と重要性を説明できる** これまでの学習内容に加え、アプリやクラウドベースのサービスが提供する、自動保存機能がもたらすバックアップについて、学年相応の例に焦点を当てる必要がある。	**・バックアップの役割と重要性を説明できる** これまでの学習内容に加え、冗長なシステムが、データ損失やサービス停止を防ぐ方法について、学年相応の例に焦点を当てる必要がある。	**・冗長性を実装したリスク軽減のための計画を策定する** これまでの学習内容に加え、リスクを軽減する手段としてのバックアップや補助電源などの冗長性の例、および災害が発生した場合のホットサイトとコールドサイトの使用について、学年相応の例を中心に取り扱う。

資料２ 「ハードウェア」の各トピックにおける，学年ごとの目標と内容

		K-2	3-5	6-8	9-12
ハードウェア	接続機器	**・コンピュータの接続機器またはパーツを見分けられる** ヘッドフォン、スクリーン、プラグ、機器類を接続する場所など、学年相応の、生徒用デバイスの例に焦点を当てる必要がある。	**・接続機器の脆弱性について説明できる** これまでの学習内容に加え、学年相応のBYOD（個人所有デバイスの持ち込み）の例と、ネットワークに接続したり、学校の端末で未知のファイル・ドライブを開いたりすることに対するリスクに焦点を当てる必要がある。	**・ハードウェアの脆弱性に対する認識を高めるための戦略を立てることができる** これまでの学習内容に加え、悪意のあるUSBドライブ、キーロガー、ハッキングされたWEBカメラなどから生じる危険性について、学年相応の例に焦点を当てて取り扱う必要がある。	**・デバイスの接続に関するリスクの軽減方法を、識別できる** これまでの学習内容に加え、ネットワークセキュリティの低下や悪意のある事件によるデータ損失など、学年相応の例に焦点を当てる必要がある。
	IoT	**・IoTを構成するデバイスの例を見分けられる** 生徒は、IoT（インターネットに接続され、データを収集・共有する物理デバイスと定義される）の学年相応の例に焦点を当て、機器の具体例と、そうではない例を分類または選択する。	**・IoTを明確化する** これまでの学習内容に加え、IoTが、現在インターネットに接続されている世界中の何十億もの物理的な機器を指し、すべてのデータが収集・共有されていることを示す学年相応の例に、焦点を当てる必要がある。	**・IoT機器のリスクと利点を評価する** これまでの学習内容に加え、学年相応のIoT機器の例と、それらの機器に関するリスク・利点に焦点を当てる必要がある。	**・IoT機器の脆弱性を分析する** これまでの学習内容に加え、学年相応のIoT機器の例と、それらの機器を使用したり、接続したりすることに関する、脆弱性に焦点を当てる必要がある。
	オペレーティングシステム	**・オペレーティングシステムの役割を説明できる** 携帯電話、コンピュータ、ゲーム機など、学年相応のオペレーティングシステムの例について、取り扱う必要がある。	**・様々なオペレーティングシステムの役割を区別できる** これまでの学習内容に加え、電話機、コンピュータ、ゲームシステムなど、様々なオペレーティングシステムの学年相応の例に焦点を当てる必要がある。	**・時代遅れのオペレーティングシステムのリスクについて議論できる** これまでの学習内容に加え、オペレーティングシステムの更新やパッチの重要性など、学年相応の例に焦点を当てる必要がある。	**・オペレーティングシステムを堅牢にするための計画を立てることができる** これまでの学習内容に加え、不要なサービスの終了やポートの閉鎖、アップデートやパッチのインストール、使用しないプログラムの削除、ユーザー権限の見直しなど、オペレーティングシステムを堅牢にするための方法について、学年相応の例を取り扱う。

資料３ 「ソフトウェア」の各トピックにおける，学年ごとの目標と内容

		K-2	3-5	6-8	9-12
ソフトウェア	ソフトウェアアップデート	**・アプリやデバイスを最新の状態に保つことの必要性を理解する** アプリとデバイスの学年相応の例と、ユーザーが、どのようにそれらをアップデートするように促されるのかについて焦点を当てる必要がある。	**・アプリやデバイスを最新の状態に保つことの必要性を理解する** これまでの学習内容に加え、ファームウェア、アプリケーション、オペレーティングシステムを更新することにより、パッチを適用し、システムを保護する方法について、学年相応の例に焦点を当てて取り扱う必要がある。	**・ソフトウェアに存在する脆弱性の例を特定できる** これまでの学習内容に加え、OS、アプリケーション、デバイスのアップデートをインストールしないことで生じる脆弱性について、学年相応の例に焦点を当てる必要がある。	**・リアルタイムでパッチを適用するシステムの利点と欠点を比較できる** これまでの学習内容に加え、Windows、MacOS、Linux、iOS、Androidを搭載したデバイスに定期的に提供されるような、オペレーティングシステムのパッチについて、学年相応の例に焦点を当てる必要がある。
	プログラミングとスクリプト	**・スクリプトによって、Webページやアプリがユーザーの操作に反応する仕組みについて説明できる** Webページやアプリが、ボタンをクリックしたりテキストボックスに入力したりといったユーザーの行動を解釈するために、どういったコードを用いているか、学年相応の例に焦点を当てる必要がある。	**・Webページやアプリが、コードの簡単な調整によって、どのように変更できるか説明できる** これまでの学習内容に加え、コードを変更することで、Webページやアプリをどのように変更できるのかについて、学年相応の例に焦点を当てる必要がある。例えば、繰り返し（ループ）や条件分岐などの概念を、Webページやアプリが私たちの行動に反応する方法と関連付けることなどが考えられる。	**・サイバー攻撃におけるスクリプトの役割について説明できる** これまでの学習内容に加え、スクリプト（ここには、一連の単純なシステムコマンド、システム構成に使用される高度なスクリプト言語、複雑なタスクを自動化するものなどが含まれます）がサイバー攻撃に関連するイベントになる方法について、学年相応の例に焦点を当てる必要がある。	**・サイバー攻撃とサイバー防御におけるスクリプトの役割について説明できる** これまでの学習内容に加え、サイバー攻撃を広める可能性のあるプログラミング言語やスクリプト言語、およびサイバー攻撃を軽減するために利用できる防御策について、学年相応の例に焦点を当てる必要がある。
	アプリケーション	**・アプリケーションが、コードを含むソフトウェアであることを認識する** 生徒がよく知っているソフトウェアアプリケーションの、学年相応の例に焦点を当てる必要がある。	**・すべてのソフトウェアには脆弱性がある可能性があると説明できる** これまでの学習内容に加え、オペレーティングシステム、アプリケーション、マルウェアの学年相応の例を中心に取り扱う。	**・安全なシステムの保護においてソフトウェアが果たす役割について説明できる** これまでの学習内容に加え、安全なシステムの保護においてソフトウェアが果たす役割について、学年相応の例に焦点を当てる必要がある。	**・様々なプラットフォームに存在するソフトウェアが、それらのプラットフォームからの、情報を監視・収集・分析するために、どのように使用されているか説明する** これまでの学習内容に加え、ファイアウォール、パケットスニファー、パケットアナライザー、ネットワークモニターなど、学年相応の例に焦点を当てる必要がある。またSIEM（セキュリティ情報およびイベント管理）ソフトウェアについても取り扱う必要がある。

資料４ 「オンラインセーフティ」の各トピックにおける，学年ごとの目標と内容

		K-2	3-5	6-8	9-12
オンラインセーフティ	ネットいじめ	**・ネットいじめの例を話し合い、ネットいじめに対する学年相応の対応を模範とする** 学年相応のネットいじめの例、ネット上で意地悪をされた時の対処法、ネット上での模範となるべき行動などを中心に、取り扱う。	**・ネットいじめの例と年齢に応じた介入方法について話し合い、実演する** これまでの学習内容に加え、バイスタンダー（傍観者）とアップスタンダーのような介入方法について、学年相応の例に焦点を当てる必要がある。	**・ネットいじめの意影響、特定と予防の方法について認識を高めるための方法を考えられる** これまでの学習内容に加え、ネットいじめの認識方法、いじめを受けている場合に生徒がとるべき行動、ネットいじめの被害者になりそうな人をサポートするための発言方法について、学年相応の例に焦点を当てる必要がある。	**・ネットいじめの影響についての、意識を高めるための計画を準備する** これまでの学習内容に加え、いじめを減らす、または防ぐために役立つ行動の、学年相応の例に焦点を当てる必要がある。
	デジタル足跡	**・ネット上でのいい行動と悪い行動を区別できる** 学年相応のオンラインでの行動の例（例えば、オンラインで他人に親切にすべきである等）に焦点を当てる必要がある。	**・デジタル足跡の概念を説明する** これまでの学習内容に加え、オンライン上の評判がどのように、人の存在意義を高めたり、傷つけたりするのかについて、学年相応の例に焦点を当てる必要がある。	**・デジタル足跡を構成する多くのデータソースがあることを認識する** これまでの学習内容に加え、ユーザーのテレメトリーを共有する可能性のあるアプリ、ウェアラブル、モバイルデバイスを通じて、第三者がデジタル足跡の作成のため、どのように情報を収集するのか、学年相応の例に焦点を当てる必要がある。 **・デジタル足跡の永続性を認識する** これまでの学習内容に加え、オンラインに投稿された情報が完全に削除または消去されない可能性があることについて、学年相応の例に焦点を当てる必要がある。	**・デジタル足跡について、プラスとマイナスの両面から意味を検討する** 倫理的、社会的、経済的な意味合いについて、学年相応の例に焦点を当てて取り扱う。
	個人情報	**・個人情報と公開情報を区別できる** プライバシーや、自分自身について話してもよいものが、機密性にどう関係しているのかについて、学年相応の例に焦点を当てる必要がある。	**・個人を特定できる情報を明確化する** これまでの学習内容に加え、学年相応の、個人を特定できる情報の例や、個人情報および公的情報を含む個人情報を、オンラインで安全に保つ方法などに焦点を当てる必要がある。	**・個人を特定できる情報を共有することのリスクと利点について話し合う** これまでの学習内容に加え、組織、個人、アプリケーションなどの関係者と、個人を特定できる情報を共有することに対するリスクや利点について、学年相応の例に焦点を当てる必要がある。 **・個人を特定できる情報を検出し、修正し、開示を防止するための技法を検討する** これまでの学習内容に加え、写真や投稿へのタグ付け、ハッシュタグの使用、不適切な投稿などの方法によって、公開される情報（意図的かそうでないか、自分か他人か）について、学年相応の例に焦点を当てる必要がある。	**・社会的アイデンティティの重要性と、個人情報、長期的なキャリアへの影響、デジタルデータの永続性に関する、オンライン活動の意味を説明できる** これまでの学習内容に加え、大学入試、キャンセルカルチャー、キャリア、人間関係などの分野における、個人情報を共有する影響について、学年相応の例に焦点を当てる必要がある。 **・個人データを保管する組織に対する、データ侵害の個々のリスクを説明できる** これまでの学習内容に加え、組織がハッキングされた際、データを盗まれた個人に、損害を与える可能性があることを理解するため、学年相応の例を挙げるべきである。

資料５ 「エシックス」の各トピックにおける，学年ごとの目標と内容

		K-2	3-5	6-8	9-12
エシックス	脅威アクター	**・デジタル機器の良い使い方と悪い使い方を説明できる** 不要な写真の撮影、意図しない情報の共有、パスワードやログインの共有など、機器が善意と悪意を持ってどのように使用されるかについて、学年往々の例に焦点を当てて取り扱う必要がある。	**・ネット上でのいい行動、悪い行動に影響を与える様々な動機を、認識できる** これまでの学習内容に加え、許可なく写真を共有したりタグ付けしたり、パスワードやアカウントを共有するなど、善意と悪意を持って機器を使用する方法について、学年相応の例に焦点を当てる必要がある。	**・様々なタイプの脅威アクターを説明する** これまでの学習内容に加え、国家、サイバーテロ集団、組織的犯罪、ハクティビスト（政治的ハッカー）など、様々な脅威の要因について、学年相応の例に焦点を当てる必要がある。	**・脅威アクターの動機について分析する** これまでの学習内容に加え、金融、政治、イデオロギー、単純な悪意など、脅威となる者の動機に関する学年相応の例に焦点を当てる必要がある。この分析は、シナリオや事例を時事問題から取り出すなど、様々な形で行うことができる。
	倫理的誠実さ	**・安全でないコンテンツを特定する** ポップアップや悪意のあるリンクなど、安全でないコンテンツの学年相応の例に焦点を当てて取り扱う必要がある。	**・サイバー攻撃の例について話し合うことができる** これまでの学習内容に加え、企業、小売業者、ゲーマーなどに影響を与えるような、サイバー攻撃に関する時事問題から、学年相応の例を取り上げ、焦点を当てる必要がある。	**・倫理的なハッキングと悪意のあるハッキングを区別する** これまでの学習内容に加え、様々なタイプの、ハッカーや職業や信条に関して、学年相応の例に焦点を当てる必要がある。	**・サイバー倫理が現在の社会で果たしている役割について議論する** これまでの学習内容に加え、オンラインで行われる行動によって、誠実さや評判が、どのように影響を受けるかについて、学年相応の例に焦点を当てる必要がある。

資料６ 「政策・法的問題」の各トピックにおける，学年ごとの目標と内容

		K-2	3-5	6-8	9-12
政策・法的問題	規則・法律・規制	**・オンライン上の行動が現実世界にどのような影響を及ぼすか、また法律や規則がオンライン上でも適用される場合があることを説明できる** ネット上で誰かに意地悪をすると、現実世界でもその人の気持ちが傷つくなど、ネットと現実の関係について、学年相応の例を中心に取り扱う。	**・オンラインでの交流を生み出すために、特定のポリシーや法律がどのように作られているか説明できる** これまでの学習内容に加え、年齢制限のあるアプリケーションやオンライン上での行動が、法的な責任をもたらす可能性があることなど、デジタルポリシーや法律を通じ安全がどのように守られているかについて、学年相応の例に焦点を当てる必要がある。	**・サイバーセキュリティとプライバシーに関する特定の連邦法、州法、地方法を分析する** これまでの学習内容に加え、コンピュータ不正使用防止法、電子プライバシー法、デジタルミレニアム著作権法などの連邦法、州法、地方法の学年相応の例を取り扱う。デジタルミレニアム著作権法、愛国者法（包括的テロ対策法）、児童インターネット保護法のほかに、ネット中立性の原則についても同様である。	**・個人と企業のための地域、州、連邦、国際的なサイバー法および規制を比較する** これまでの学習内容に加え、地域、州、連邦、国際的なサイバー法および規制、さらには児童オンラインプライバシー保護規則、一般データ保護規則について、学年相応の例に焦点を当てる必要がある。
	知的財産	**・著作権の概念について話し合うことができる** 著作権が、所有権などの考え方と同一視されていることについて、学年相応の例に焦点を当てる必要がある。「誰が文書を書いたのか」「私が作った、世界で新しいものは、全て私のもの」「私が作ったのではないコンテンツには謝意を示す必要がある」などである。	**・著作権とフェアユースの関係について説明できる** これまでの学習内容に加え、公正利用がアイデアの共有を促進しながら、著作権やクリエーターの権利を保護するのに役立つという、学年相応の例に焦点を当てる必要がある。	**・知的財産権と著作権がフェアユースとどのように関係するかを説明できる** これまでの学習内容に加え、利用可能なクリエイティブコモンズライセンスの種類、著作権・商標・特許・登録商標・その他知的財産権の種類の違い、フェアユースがアイデアの共有を促進しながら著者やクリエーターの権利を保護するのに役立つ方法について、学年相応の例を中心に取り扱う必要がある。	**・知的財産法の重要性について議論する** これまでの学習内容に加え、譲渡可能なグッズを含むビデオゲームのコンテンツは誰のものか、コンテンツがリミックスやパロディされた場合の著作権、フェアユースがアイデアの共有を促進しながら著者やクリエーターの権利を保護するのに役立つか、といったアイデアをテーマに、学年相応の例を挙げて行われる。
	利用規約・ユーザー規約	**・利用者を保護するため、利用規約がどのように設計されているかを説明する** 特定の技術を使用することは、利用規約などのポリシーに同意することであり、そういったポリシーはユーザーを保護するためにあることを、「教室のルール」に例えながら、学年相応の例に焦点を当てて取り扱う必要がある。	**・様々な契約について説明し、その目的を説明できる** これまでの学習内容に加え、利用規約（AUPやTOS）、エンドユーザーライセンス契約（EULA）などの様々な契約について、学年相応の例に焦点を当てて取り扱う。	**・様々な契約が、ある技術の利用者と所有者を、どのように保護するかを理解する** これまでの学習内容に加え、AUP、TOS、EULAなどの様々な契約について、学年相応の例に焦点を当てて取り扱う。	**・デジタル環境において、個人と組織を保護するための様々な契約を、見分けることができる** これまでの学習内容に加え、AUP、TOS、EULA、セキュリティポリシーなど、公開されている文書の学年相応の例に焦点を当てて取り扱う。ある文書において、組織よりも個人を有利にしているか、もしくは個人よりも組織を有利にしているか、といったことを扱う。

資料７ 「情報セキュリティ」の各トピックにおける，学年ごとの目標と内容

		K-2	3-5	6-8	9-12
情報セキュリティ	CIAトライアド	**・CIAトライアドに含まれる機密性、完全性、可用性の概念を見分けられる** 安全なパスワードや信頼関係など、CIAの概念に関する学年相応の例に焦点を当てるべきである。	**・CIAトライアドの概念が、情報保護のためにどのように機能するか説明できる** これまでの学習内容に加え、安全なパスワードや、個人情報の共有が適切な場合など、CIAの概念に関する学年相応の例に焦点を当てる必要がある。	**・CIAの三位一体が破られた場合の影響を説明できる** これまでの学習内容に加え、可能な限り本物の参考文献を使用した、学年相応のCIAが破られた例に焦点を当てる必要がある。事例をもとに、CIAの3要素のうち、どの部分が悪かったのかを特定できる。	**・CIAトライアドとデータの3つの状態の間の様々な相互作用を説明できる** これまでの学習内容に加え、学年相応の相互作用の例や、人・プロセス・技術がどのようにその相互作用をサポートしているかに焦点を当てる必要がある。データの3つの状態とは「使用中のデータ」（現在アクセス中）、「停止中のデータ」（アクセスを待っている）、「移動中のデータ」（ある場所から別の場所に移動している）を指す。
	アクセス制御	**・個人情報へのアクセスについて明確化する** 個人情報に関して、特権情報（特定の誰かのみが知ることのできる情報）の、学年相応の例に焦点を当てて、取り扱う必要がある。	**・個人情報への適切なアクセスについて説明できる** これまでの学習内容に加え、個人情報へのアクセスについて学年相応の例に焦点を当てる必要がある。生徒は、自宅の住所や親の電話番号などの個人情報（特権情報）を共有する可能性のある、校長や警察官などの権力者の例を挙げられる。	**・アクセス制御の概念と、アクセスを許可されたユーザーを制限する方法を説明できる** これまでの学習内容に加え、ユーザープラットフォーム間でアクセス制御が必要な理由、および認定ユーザーの構成について、学年相応の例に焦点を当てて取り扱う必要がある。	**・アクセス制御の原則、アクセス制御モジュール、最小権限の原則が示す概念を比較できる** これまでの学習内容に加え、アクセス制御の原則としての識別、認証、認可の概念、およびアクセス制御モジュールとしてのMAC（強制アクセス制御）、RBAC（ロールベースアクセス制御）、DAC（任意アクセス制御）の学年相応の例に焦点を当てて取り扱う必要がある。
	データセキュリティ	**・情報が偶然に変更される場合と意図的に変更される場合の違いを見分けられる** 情報の誤りや意図的な改ざんの可能性について、学年相応の例に焦点を当てる必要がある。	**・データが偶発的または意図的に変更される可能性がある場合と、その方法を識別する** これまでの学習内容に加え、生徒は、データがいつどのように、偶然または意図的に変更・破壊されるのかについて、学年相応の例に焦点を当てる必要がある。	**・データを3つの状態に分け、それぞれの状態に対する潜在的脅威を説明する** これまでの学習内容に加え、データの3つの状態（使用中のデータ、停止中のデータ、移動中のデータ）について、学年相応の例に焦点を当てて取り扱う。	**・データを保護するためのセキュリティ対策を、3つの状態、すべてに適用する計画を立てる** これまでの学習内容に加え、データの3つの状態（使用中のデータ、停止中のデータ、移動中のデータ）すべてを保護する、学年相応の例に焦点を当てて取り扱う。
	脅威と脆弱性	**・保護する必要のある情報の例を挙げる** ポップアップ、テキストや電子メール内のリンク、パスワード忘れなどのデジタルな脅威からどのように情報を保護できるか、また、これらの疑わしい脅威や不快な脅威にどのように対応できるかについて、学年相応の例に焦点を当てて取り扱う必要がある。	**・脅威と脆弱性に関する事象を明確化する** これまでの学習内容に加え、マルウェアやなりすましメールなど、学年相応の事象、活動、または行動の例や、これらの疑わしい脅威や不快な脅威に生徒がどのように対応できるかに焦点を当てる必要がある。	**・個人や組織の情報セキュリティに対する脅威と脆弱性を分析できる** これまでの学習内容に加え、マルウェア、なりすましメール、ハッキングなど、脅威や脆弱性に関する学年相応の実例だけでなく、これまでの標準規格にも焦点を当てた議論を行う必要がある。	**・個人や組織の情報セキュリティに影響を与える、様々な種類の攻撃を区別できる** これまでの学習内容に加え、マルウェア、悪意のあるユーザー、ハッキング、セキュリティポリシーの不備など、これまでの基準に加え、学年相応の本格的な事例を中心に取り扱う。
	暗号化	**・暗号化によって情報が保護されていることを認識する** ここでは、暗号が情報を保護する「秘密のコード」と呼ばれることについて、学年相応の例に焦点を当てる必要がある。また、2進数（base-2）、10進数（base-10）、16進数（base-16）といったデータのエンコード方式が、暗号化にどのような効果をもたらすかについても、適宜議論することができる。（注、すべてのエンコード方式がすべての学年に適しているわけではない。）	**・情報や通信システムを暗号化する理由と方法について説明できる** これまでの学習内容に加え、シーザー暗号、スキュタレー暗号、ビッグペン暗号、ROT13などの情報を保護できる簡単な暗号化手法の例に焦点を当てて取り扱う必要がある。2進数（base-2）、10進数（base-10）、16進数（base-16）といったデータのエンコード方式が、暗号化にどのような効果をもたらすかについても、適宜議論することができる。（注、すべてのエンコード方式がすべての学年に適しているわけではない。）	**・httpとhttpsの違いなど、情報をやり取りする際の暗号化の方法と必要性について議論する** これまでの学習内容に加え、学年相応の、より複雑な暗号化手法の例（ヴィジェネレ暗号、ベーコンの暗号、エニグマ暗号など）に焦点を当てて議論する必要がある。2進数（base-2）、10進数（base-10）、16進数（base-16）といったデータのエンコード方式が、暗号化にどのような効果をもたらすかについても、適宜議論することができる。（注、すべてのエンコード方式がすべての学年に適しているわけではない。）	**・コンピュータの進歩が暗号化にどのような影響を与えたかを分析できる** これまでの学習内容に加え、対称型と非対称型、公開鍵と秘密鍵、暗号化アルゴリズムなど、暗号化における現代の進歩に関する学年相応の例に焦点を当てて取り扱う必要がある。2進数（base-2）、10進数（base-10）、16進数（base-16）といったデータのエンコード方式が、暗号化にどのような効果をもたらすかについても、適宜議論することができる。（注、すべてのエンコード方式がすべての学年に適しているわけではない。）

資料８ 「ネットワークセキュリティ」の各トピックにおける，学年ごとの目標と内容

		K-2	3-5	6-8	9-12
ネットワークセキュリティ	認証	**・良いパスワードの概念とその重要性を説明できる** パスワードの概念について、一般的な単語をパスワードとして使用しない、パスフレーズの方がパスワードよりも安全である、文字、数字、記号を組み合わせた方がパスフレーズよりも安全であるなど、学年相応の例に焦点を当てて取り扱う必要がある。	**・認証と認可の役割について説明できる** これまでの学習内容に加え、パスワードを含まない認証と承認の概念、例えば遊園地での指紋認証や、年齢証明をしたり、携帯電話にアクセスしたりするためのクレジットカードによる二要素認証など、学年相応の例に焦点を当てて取り扱う必要がある。	**・認証・認可されたユーザーを保護する方法について説明できる** これまでの学習内容に加え、生徒は二要素、多要素、生体認証など、より高度な認証・認可の方法について、学年相応の例に焦点を当てる必要がある。	**・認証・認可の方法と失敗した場合のリスクを評価できる** これまでの学習内容に加え、証明書、トークン、二要素、多要素、生体認証などの認証・認可の方法について、学年相応の例に焦点を当てて取り扱う必要がある。
	ネットワーク機器の保護	**・多層防御により、様々なセキュリティ機器がどのように連携して動作するのか理解する** 複数の鍵や、数が限られた鍵など、家の安全を守るための層に例えて、どのようにセキュリティを重ねられるのか、学年相応の例に焦点を当てる必要がある。	**・ネットワークと機器を保護するために使用できる多層防御の技術を見分けられる** これまでの学習内容に加え、Wi-Fi設定、家庭用ネットワークと公共ネットワーク、ファイアウォール、ペアレンタルコントロールなどで利用できる、多層防御の技術に焦点を当てる必要がある。	**・シンプルなネットワークを保護するための「多層防御」戦略を説明できる** これまでの学習内容に加え、ファイアウォール、許可リストとブロックリスト、デフォルトパスワードの変更、アクセスポイントなどの、層に分かれた戦略について、学年相応の例に焦点を当てる必要がある。	**・シンプルなネットワークを保護するための「多層防御」戦略を評価する** これまでの学習内容に加え、ファイアウォール、許可リストとブロックリスト、デフォルトパスワードの変更、アクセスポイント、ネットワークセグメンテーションなどの階層的な戦略について、学年相応の例に焦点を当てて取り扱う必要がある。
	脅威と脆弱性	**・情報交換の方法と、なぜその方法が保護されなければならないかを理解できる** ソーシャルメディアのフィード（例、YouTube）やオンラインゲームのプラットフォーム（例、Minecraft）など、情報交換のためのさまざまな方法について、学年相応の例に焦点を当てて取り扱う必要がある。	**・情報交換のためのオープンな手法の脆弱性について議論できる** これまでの学習内容に加え、ソーシャルメディアのフィード（例、YouTube）やオンラインゲームのプラットフォーム（例、Minecraft）など、情報を交換するさまざまな方法における脆弱性について、学年相応の例に焦点を当てて議論する必要がある。	**・悪意のある行為がネットワークセキュリティを脅かすことを説明できる** これまでの学習内容に加え、ソーシャルエンジニアリング、マルウェア、ハッキングなどの悪意のある行為の、学年相応の例に焦点を当てて取り扱う必要がある。	**・ネットワークセキュリティに影響を与える様々な種類の攻撃を分析できる** マルウェア、ハッキング、悪意のあるユーザー、セキュリティポリシーの不備など、これまでの学習内容や、学年相応の攻撃事例を中心に取り扱う。なお、攻撃の監視と記録に関する内容に、リスク分析と管理に関する内容を含めることができる。

資料９ 「物理的セキュリティ」の各トピックにおける，学年ごとの目標と内容

		K-2	3-5	6-8	9-12
物理的セキュリティ	脅威と脆弱性	**・サイバーセキュリティに関連する物理的なセキュリティを明確化する** フロントオフィスでのチェックイン、建物の入り口での警備員、チケットのない人の通行を防ぐ改札口など、物理的セキュリティに関する親しみやすい、学年相応の例に焦点を当て、取り扱う。	**・悪意から人や場所を保護する必要性を説明できる** これまでの学習内容に加え、有名人・政治家・ランドマーク・場所・歴史的文書など、保護が必要な人・場所・物、および悪意がもたらす脅威について、学年相応の例に焦点を当てる必要がある。	**・悪意のある行為が物理的セキュリティをどのように脅かすか説明できる** これまでの学習内容に加え、ソーシャルエンジニアリングやセキュリティポリシーの不備など、様々な悪意のある行為について、学年相応の例に焦点を当てて取り扱う。	**・物理的セキュリティに影響を与える様々な種類の攻撃を分析できる** これまでの学習内容に加え、ソーシャルエンジニアリングやセキュリティポリシーの不備、悪意のある者など、物理的セキュリティを攻撃する例に焦点を当てて取り扱う必要がある。
	セキュリティ制御	**・身元保証のための「信頼せよ、しかし検証せよ」の方針を明確化する** すべての警察官がバッジを所持していることを認識するなど、身元保証のための学年相応の例に焦点を当てて取り扱う必要がある。	**・日常生活で見られる物理的なアクセス制御を区別できる** これまでの学習内容に加え、ドアロック、ID カード、PINコード、杭、照明、フェンス、カメラ、警備員など、本物の物理的なアクセス制御の学年相応の例に焦点を当てる必要がある。	**・多層防御と物理的アクセス制御がどのように連動するか、説明する** これまでの学習内容に加え、ドアロック、ID カード、PINコード、杭、照明、フェンス、カメラ、警備員など、本物の物理的アクセス制御とデジタルなアクセス制御の例に焦点を当てて取り扱う必要がある。	**・多層防御の使用と物理的アクセス制御の必要性を説明できる** これまでの学習内容に加え、近接型ICカード、PINコード、マントラップ方式など、さまざまな物理的アクセス制御の学年相応の例に焦点を当てて取り扱う必要がある。