

「教育情報セキュリティポリシーに関するガイドライン」の目的

◆ 目的

- ✓ 児童生徒や外部の者等による不正アクセス防止等の十分な情報セキュリティ対策を講じることは、教師及び児童生徒が、安心して学校においてICTを活用できるようにするために必要不可欠。
- ✓ このことを踏まえ、各教育委員会・学校が情報セキュリティポリシーの作成や見直しを行う際の参考とするものとして、『教育情報セキュリティポリシーに関するガイドライン』を策定した。
(平成29年10月)
- ✓ ICT環境が常に進歩を遂げていることから、本ガイドラインについても、他機関の動向、技術的な進展等を踏まえつつ、随時見直しを行う。



文部科学省HPにて公表

http://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm



地方公共団体における 教育情報セキュリティの基本的な考え方

- ① **組織体制を確立すること**
 - ・ 情報セキュリティの責任体制の明確化
 - ・ 首長部局の情報政策担当部局との連携
- ② **児童生徒による機微情報へのアクセスリスクへの対応を行うこと**
 - ・ 情報の機微の度合いごとに、取扱ルールを決定
- ③ **インターネット経由による標的型攻撃等のリスクへの対応を行うこと**
 - ・ 教員が使用する校務系ネットワークと児童生徒が使用する学習系ネットワークの論理的な分離、インターネットリスクの高いシステムと機微な情報の論理的な分離 等
- ④ **教育現場の実態を踏まえた情報セキュリティ対策を確立させること**
 - ・ 教員が個人情報を外部に持ち出す際のルールの明確化
 - ・ 情報システムを教員が扱う際の、順守すべきルールの整理
- ⑤ **教職員の情報セキュリティに関する意識の醸成を図ること**
 - ・ 研修等の実施
- ⑥ **教職員の業務負担軽減及びICTを活用した多様な学習の実現を図ること**
 - ・ 教育委員会が情報セキュリティの確保を主導することによる教員の業務負担の軽減
 - ・ システムの種類に応じた異なるセキュリティ対策による、ICTを活用した学習活動への配慮

※ 情報セキュリティポリシーとは
「組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書」のこと。

「教育情報セキュリティポリシーに関するガイドライン」の改訂について

- ✓ Society5.0時代において社会構造や雇用環境が大きく変化することが考えられており、そのような社会において求められる能力や子供たち自身の多様化を踏まえた学習環境の構築、その実現に向けた教員の働き方改革など、教育現場の改善が急務
- ✓ クラウドを適切に活用することで、より安全に、柔軟かつ効率的にICT環境整備を進めることができ、教育現場の改善に向けた有力な解決策となる

⇒ 教育現場においてもクラウドの活用が促進されるよう、「教育情報セキュリティポリシーに関するガイドライン」を改訂

(参考：クラウド活用に関する政府の方向性)

■ クラウド・バイ・デフォルトの原則

- クラウドサービスは、正しい選択を行えば、コスト削減に加えて、情報システムの迅速な整備、柔軟なリソースの増減、自動化された運用による高度な信頼性、災害対策、テレワーク環境の実現等に寄与する可能性が大きいことから、政府情報システムの導入においても、クラウドサービスの利用を第一候補として検討を行うこととしている。
※ 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」
(2018年6月7日 各府省情報化統括責任者 (CIO) 連絡会議決定)

■ 総務省「教育現場におけるクラウド活用の推進に関する有識者会合」における検討

- 教育現場におけるクラウド活用のメリットを明らかにするとともに、学校現場、教育システムのクラウド化に向けた課題と、国が取り組むべき事項を整理し、提言として公表
<「教育情報セキュリティポリシーに関するガイドライン」の改訂に関連する提言>
 1. 教育現場におけるシステム導入を検討する際には、まずはクラウドから検討を始めること (クラウド・バイ・デフォルト)
 2. クラウドサービスの調達時には、安全性評価の観点から、第三者評価を求めること
 3. 教育ネットワーク構築の在り方について、より柔軟なセキュリティ確保モデルを提示すること
 4. 情報資産分類について、例示の在り方も含めて検討すること

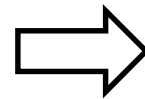
■ 経済産業省・総務省「クラウドサービスの安全性評価に関する検討会」における検討

- ISO27017や政府統一基準、米国FedRAMP等を参考としつつ、政府機関がクラウドサービスを利用する際の安全性評価を行うための認証制度の構築に向けた議論を実施
※ 公表後、必要に応じて「教育情報セキュリティポリシーに関するガイドライン」に内容を反映

ガイドライン改訂の方向性について

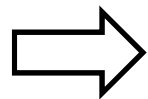
■ 改訂の経緯・課題と方向性

- ▲ 現行のガイドラインは、教職員の情報セキュリティに関する意識を向上させた一方で、ガイドラインに記載された具体的な対策例を一言一句遵守することが目的化してしまったため、急速な技術進展、中でもクラウドサービスの活用に対応できず、教育情報の活用が硬直性が生じるという弊害が各地で生じている。



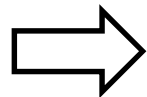
- ◆ ガイドラインの位置付け・構成の見直し

- ▲ 現行ガイドラインの大部分が、オンプレミスによる環境構築を想定した内容であり、クラウドサービスの利用を前提とした記載がなく、教育現場におけるクラウドサービスの利用に関する方向性が不明確であった。



- ◆ クラウド・バイ・デフォルトの原則を本文に追記
- ◆ クラウドサービスの利用に関する例文等を参考資料に追加

- ▲ クラウドサービスの利用の際の、クラウドサービス提供事業者における情報の取扱いが必ずしも明らかではない。
(同意のない目的外利用や第三者提供等が行われないか 等)



- クラウドサービス提供事業者が留意すべきプライバシーに関する事項を追加

ガイドラインの改訂内容

◆ ガイドラインの位置付け・構成の見直し

- ✓ 本書の目的や基本理念を示した従来の第1章を『**本文**』に、教育委員会・学校が対策基準を検討・策定する際の考え方や例文を記載した従来の第2章を『**参考資料**』という位置付けとする

※ 教育委員会においては、『本文』の理念を踏まえつつ、実現したい学習・校務の環境、費用・運用コスト、現在の環境整備の状況（ネットワーク等）を踏まえ、教育委員会自らが判断してセキュリティポリシーの策定・改訂を実施

【従来のガイドライン】

- 第1章 総則
 - 1.1 本ガイドラインの目的
 - 1.2 本ガイドライン制定の背景
 - 1.3 地方公共団体における教育情報セキュリティの考え方
 - 1.4 教育情報セキュリティポリシーの構成と学校を対象とした「対策基準」の必要性
- 第2章 情報セキュリティ対策基準
 - 2.1 対象範囲及び用語説明
 - 2.2 組織体制
 - 2.3 情報資産の分類と管理方法
 - ...

【今後のガイドライン】

- 第1章 ガイドラインの目的
- 第2章 ガイドライン制定の背景
- 第3章 地方公共団体における情報セキュリティの基本理念
- 第4章 教育情報セキュリティポリシーの構成と学校を対象とした「対策基準」の必要性
- 第5章 クラウド・バイ・デフォルトの原則
- (参考資料)
 - 1.1 対象範囲及び用語説明
 - 1.2 組織体制
 - 1.3 情報資産の分類と管理方法
 - ...
 - 1.9 クラウドサービスの利用について
 - ...

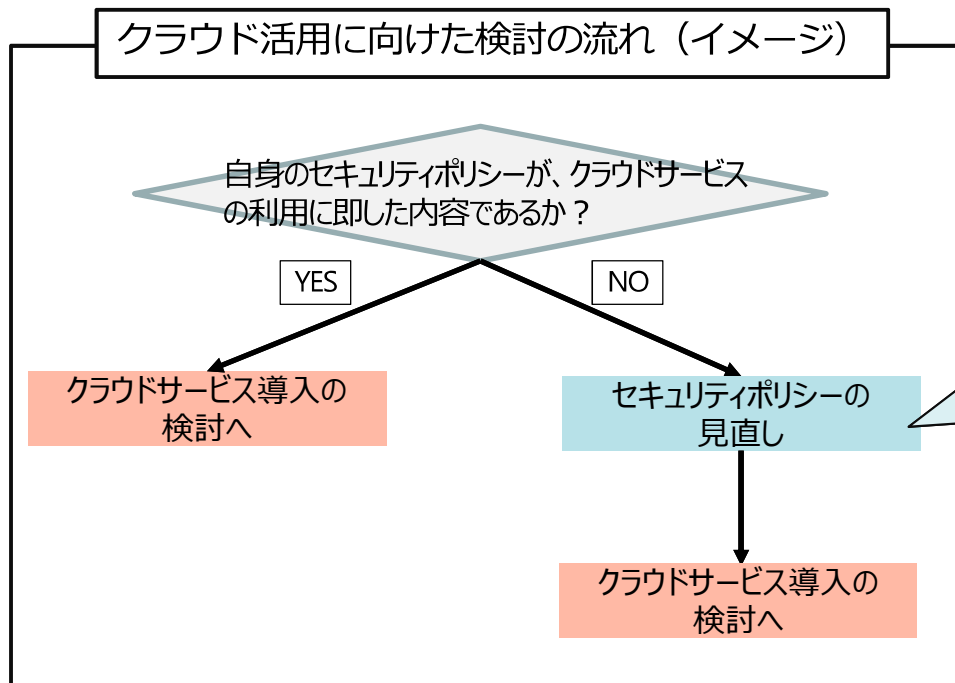
本文

参考資料

ガイドラインの改訂内容

◆ クラウドサービスの利用に関する記述の追加

- ✓ 本文に、「クラウド・バイ・デフォルト」の原則を踏まえた内容を追記するとともに、参考資料として、クラウドサービスのメリット・留意点のほか、クラウドサービスの利用におけるセキュリティ対策の項目例を記載
- ✓ これらの記載を参考に、各教育委員会は必要に応じて、自らの教育情報セキュリティポリシーを、クラウドサービスの利用に即した内容に修正することが必要



✓ クラウドサービス事業者の情報セキュリティ対策の全容を、教育委員会・学校自らが、個別かつ詳細に把握し、検証することは困難

⇒ 安全性の確認には第三者認証の取得・準拠状況や監査報告書等を活用する等、自身のセキュリティポリシーをクラウドサービスの利用に即した内容となるように改訂することが重要

例えば・・・

「データセンターを（目視で）確認すること」という文言は、クラウドサービスではなじまない。
（セキュリティ対策として、データセンターの所在を秘匿しているため）

ガイドラインの改訂内容

◆ クラウドサービス提供事業者が留意すべきプライバシーに関する事項の追加

- ✓ クラウドサービス等を利用する場合、事業者における個人情報の適切な管理が行われていることが必須であり、個人情報の収集・利用の範囲等について、サービス提供定款や契約書面等で確認することが必要

【確認項目例】

<p>(1) 個人情報の利用範囲</p> <ul style="list-style-type: none"> 教育・学校の目的に必要な情報、または児童生徒・保護者の許可した情報を超えて個人情報の収集、維持、使用、共有をしないこと。 	<p>(7) 個人情報の利用目的</p> <ul style="list-style-type: none"> 個人情報を収集、使用、共有、および保持するのは、教育機関、教師、または利用者によって承認された目的に限ること。
<p>(2) 個人情報の売買禁止</p> <ul style="list-style-type: none"> クラウドサービスの導入によって知り得た個人情報について、売買も含め、無断提供をしないこと。 	<p>(8) 個人情報の取扱いについての情報開示</p> <ul style="list-style-type: none"> 個人情報の取扱いについて、契約またはプライバシーポリシーで明確に示すこと。
<p>(3) 個人情報を利用した利用者に対する広告活動等の無断使用の禁止</p> <ul style="list-style-type: none"> 教育・学校の目的を達成すること以外に、個人情報について児童生徒・保護者に対する行動ターゲティング広告をはじめとする、広告活動その他無断使用をしないこと。 	<p>(9) 利用者による個人情報管理</p> <ul style="list-style-type: none"> 個人情報の登録、変更、削除に関するサービスを利用者に提供すること。
<p>(4) 不必要な個人プロフィール作成禁止</p> <ul style="list-style-type: none"> 教育・学校の目的を達成するため、または児童生徒・保護者によって許可された場合を除き、不必要な個人プロフィールを作成しないこと。 	<p>(10) 個人情報の適正管理</p> <ul style="list-style-type: none"> 個人情報に対する不正アクセス又は個人情報の紛失、破壊、改ざん、漏洩、盗難等のリスクに対し、適切な安全対策を講じること。また、個人情報を正確かつ最新の状態で管理すること。
<p>(5) 不適切なポリシー等の変更の禁止</p> <ul style="list-style-type: none"> クラウドサービスの運用等において、利用者に対する明確な通知・相談等の対応もなく、利用者のプライバシーポリシーに重大な影響を与えるような変更を行わないこと。 	<p>(11) 再委託</p> <ul style="list-style-type: none"> サービス提供の全部又は一部を第三者に再委託又は代行実施させる場合には、個人情報保護法制等を遵守し、当該再委託先又は代行実施先について、同等の義務を課し、管理するものとする。
<p>(6) 個人情報の保持期間定義</p> <ul style="list-style-type: none"> サービス提供期間（利用者と合意した期間）を超えて個人を特定する情報を保持しないこと。 	<p>(12) 合併/買収</p> <ul style="list-style-type: none"> 合併または他社による買収を伴う場合、後継企業が以前に収集した個人情報について同様の義務を負うことを条件に、個人情報を継続して管理するものとする。

※ USの「Future of Privacy Forum」(研究機関)及び「Software&Information Industry Association」(規格標準化推進団体)が運営する「生徒児童のプライバシーを保護するサービスプロバイダーの誓約」を元に整理

その他の改訂について

◆ クラウド関連以外の主な修正点

➤ ネットワーク分離等に関する文言の適正化

「児童生徒からの機微情報に対するアクセスリスクへの対応」、「外部からの機微情報に対するアクセスリスクへの対応」が目的である一方、校務系と学習系ネットワークの分離そのものが目的となっているケースが存在。本来の目的を明確化するとともに、技術革新も踏まえた柔軟な対応を行うことができるよう、文言を適正化。

➤ 教育委員会における学習系・校務系ネットワークの一元管理に関する文言の適正化

セキュリティ対策の観点から、教育委員会のデータセンター等でネットワークを集約することが想定される一方で、局所的にネットワークの負荷が増大し、安定的な稼働に支障をきたす可能性もあることから、用途・目的に応じて柔軟に対応できるよう、文言を適正化。

➤ 情報資産分類の整理に関する文言の適正化

様々なツール（デジタルドリル、ポートフォリオ等）が普及してきた現状を踏まえ、学校・教育委員会が実現したい環境と情報セキュリティのバランスを考慮しつつ、柔軟に対処することができるよう、文言を適正化