

平成22年度 学校・教育機関の個人情報漏えい事故の 発生状況・教員の意識に関する調査

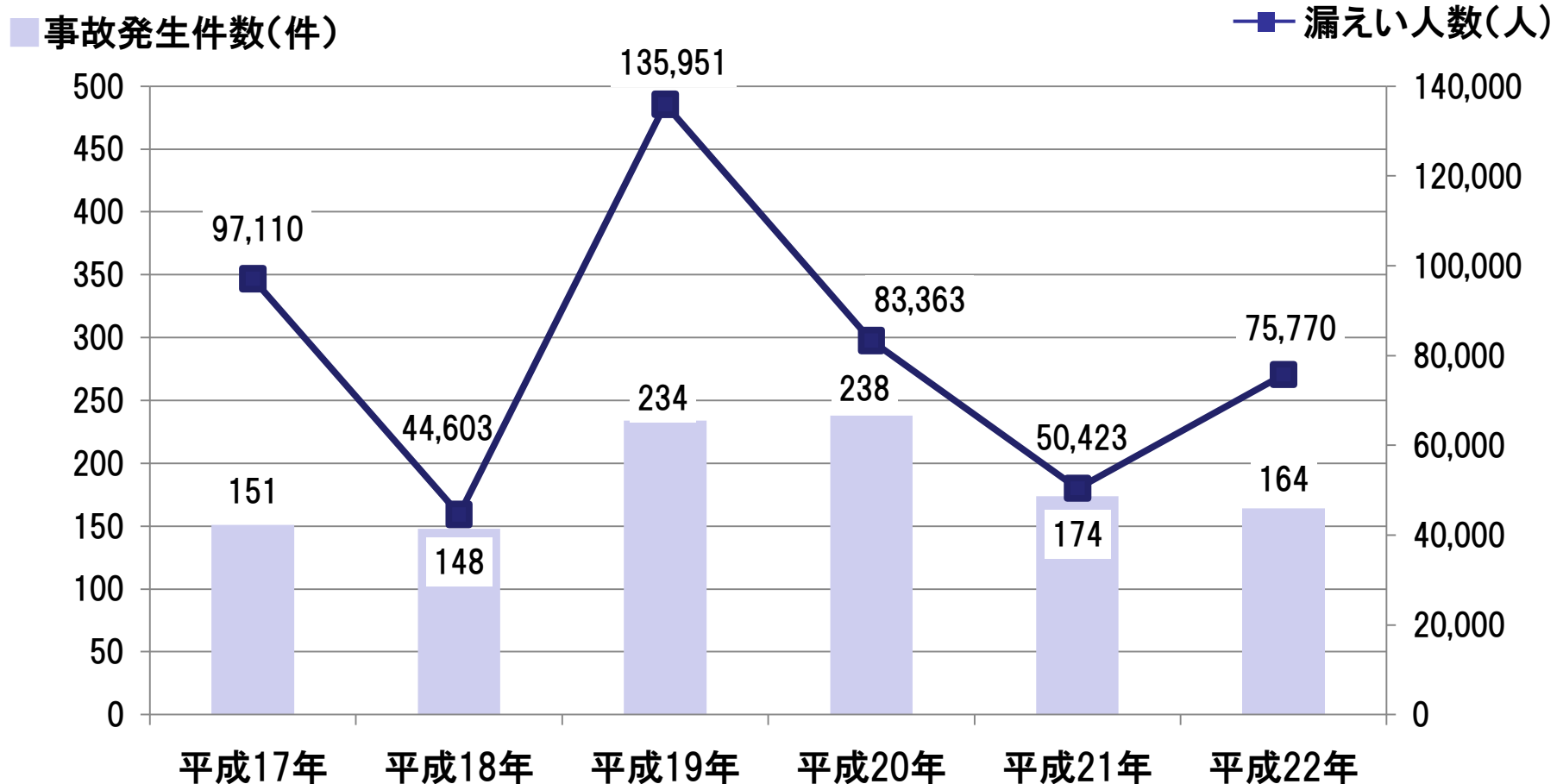


本資料について

- ◆ 本資料は、平成22年度に学校、教育機関、関連組織で発生した、児童・生徒・教員などの個人情報を含む情報の漏えい事故についての公開情報を集計したものです。
- ◆ 学校や自治体が発表・公開した情報を集計しています。発生したすべての情報漏えい事故を網羅したものではありません。

情報漏えい事故 発生件数・漏えい人数5年分推移

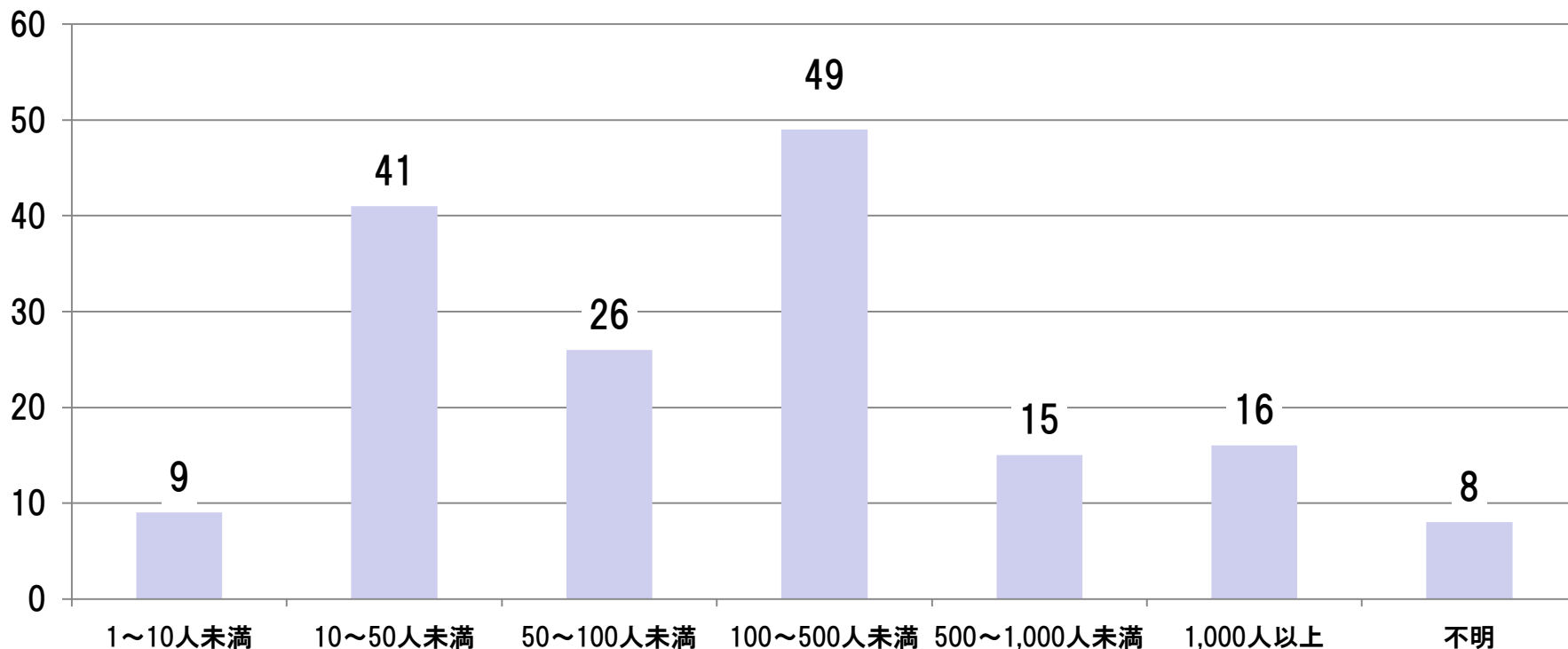
- ◆ 毎年、多くの個人情報漏えいしています。平成22年度の場合、事故1件あたりの漏えい人数は、462人となっています。



平成22年度 漏えい人数の分布別 事故件数

◆ 情報漏えい事故1件あたりの漏えい人数は、1人から1万3,000人まで大きく幅があります。

■ 事故発生件数(件)



傾向

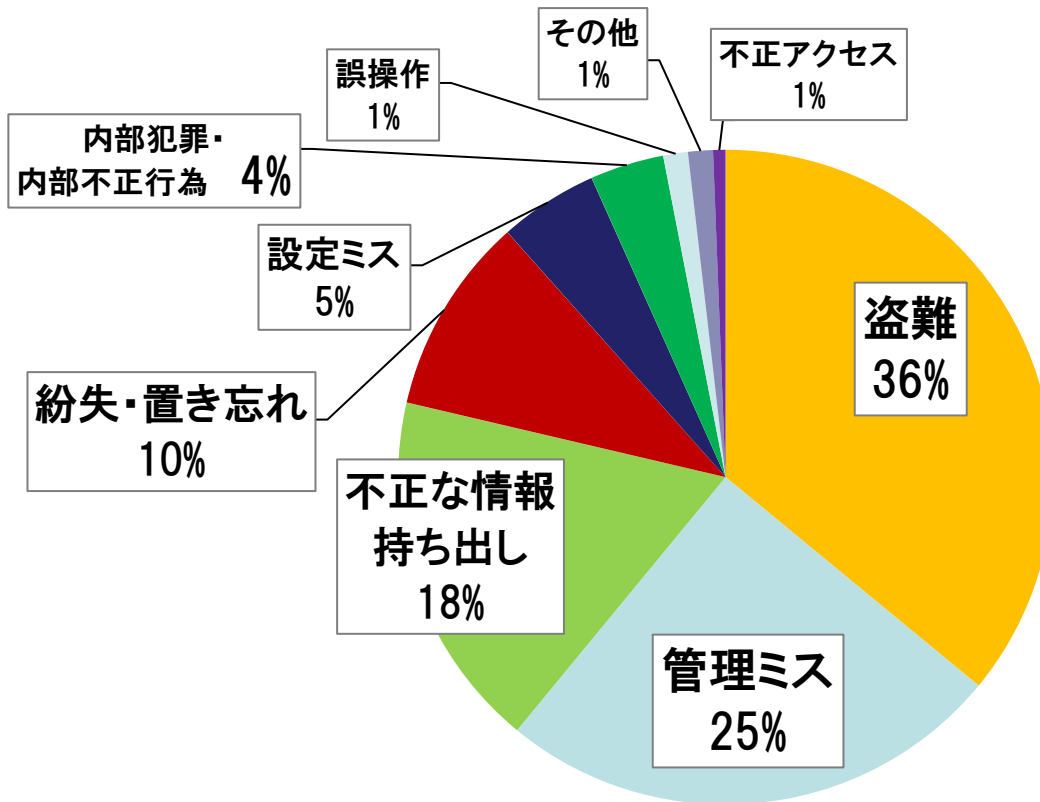
クラス単位の事故が多い(小学校に多い)

学年単位の事故が多い(中学・高校に多い)

大学などが多い

事故の種類別 発生割合

- ◆ 書類や、USBメモリ、パソコンなどの「盗難」「管理ミス」「不正な情報持ち出し」「紛失、置き忘れ」が全体の約80%を占めています。



傾向

・学校で発生した情報セキュリティ事故は、公表されないものもありますが、発生した場合、警察などの学校外の機関も関わる「盗難」は公表されることが多いです。

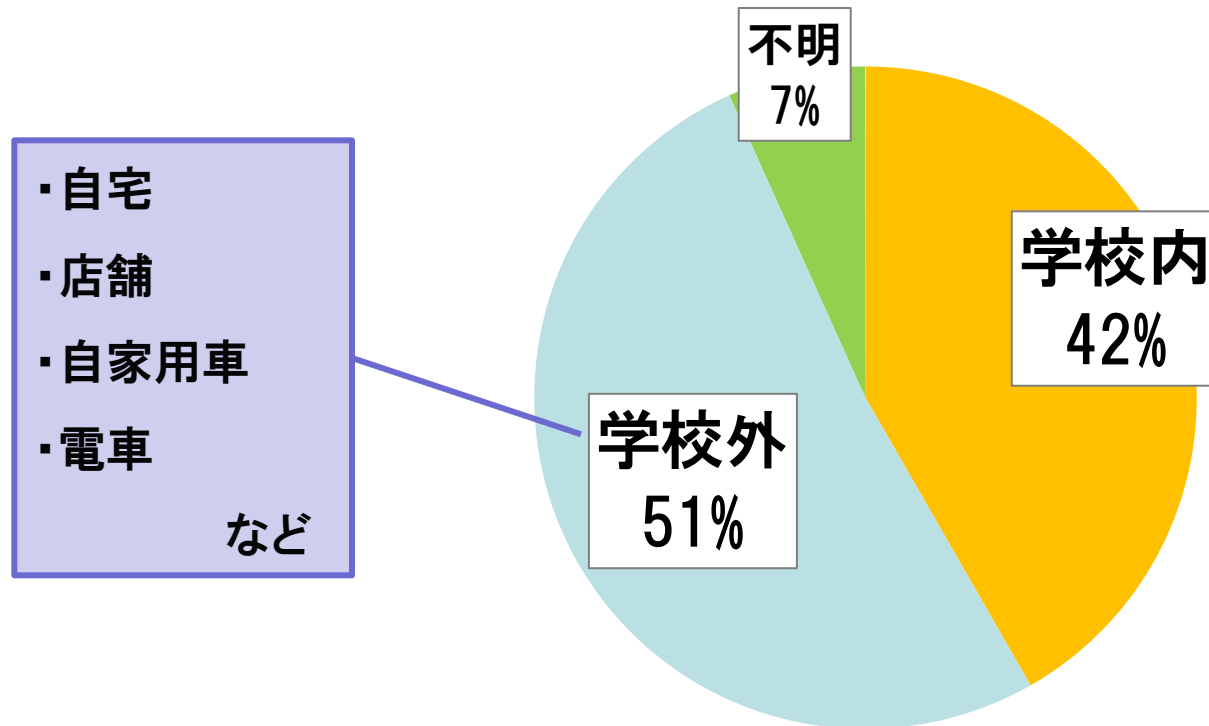
・「盗難」「紛失」には「管理ミス」や「不正な情報持ち出し」に起因するものも多くあります。

（例：ルールを無視して情報を持ち出したら、盗難あった）

発表情報で、「盗難」「紛失」などと発表されているものについても、「管理ミス」や「不正な情報持ち出し」がきっかけとなって起きたことが公表されているものは、それぞれ「管理ミス」「不正な情報持ち出し」として集計しています。

情報漏えい事故の発生場所

◆ 学校外での事故が半数以上を占めています。

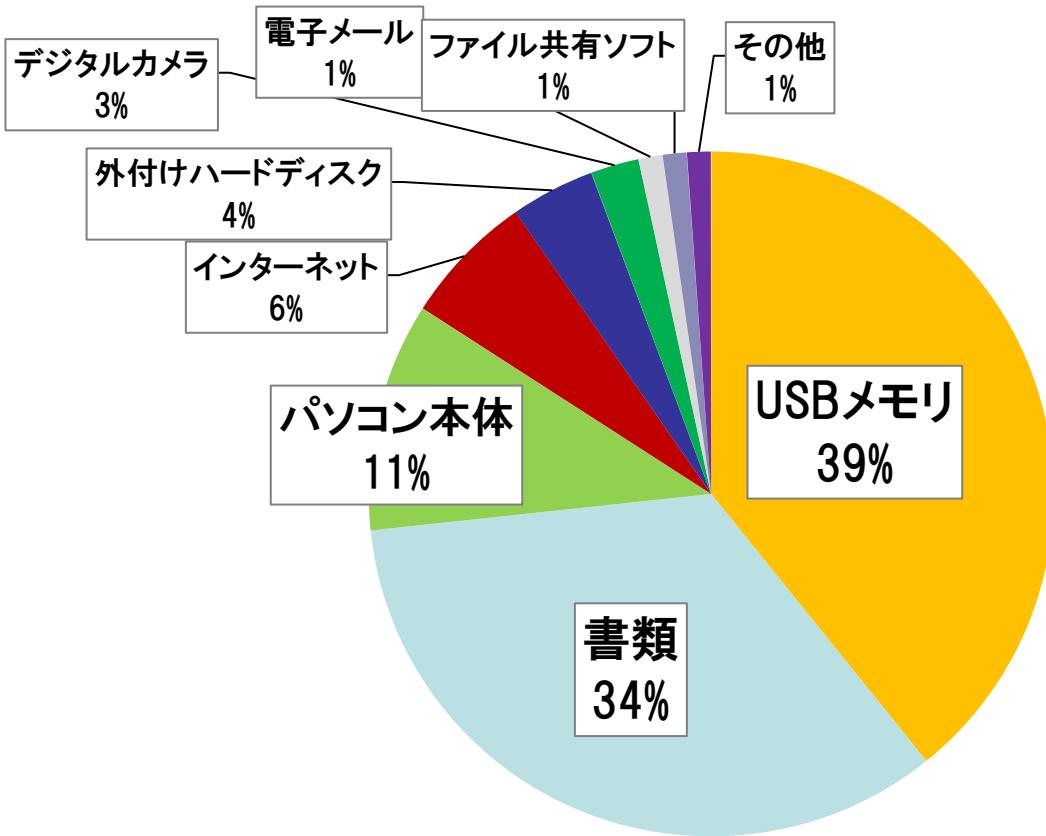


傾向

先生方は、学校外で仕事を行うことも多く、やむをえず情報を持ち出した結果、事故にあってしまうケースが多くなっていると思われます。

漏えい媒体別事故件数

◆ ICT機器(USBメモリ・パソコン・外付けハードディスク・デジタルカメラ)の事故が全体の半数以上を占めます。



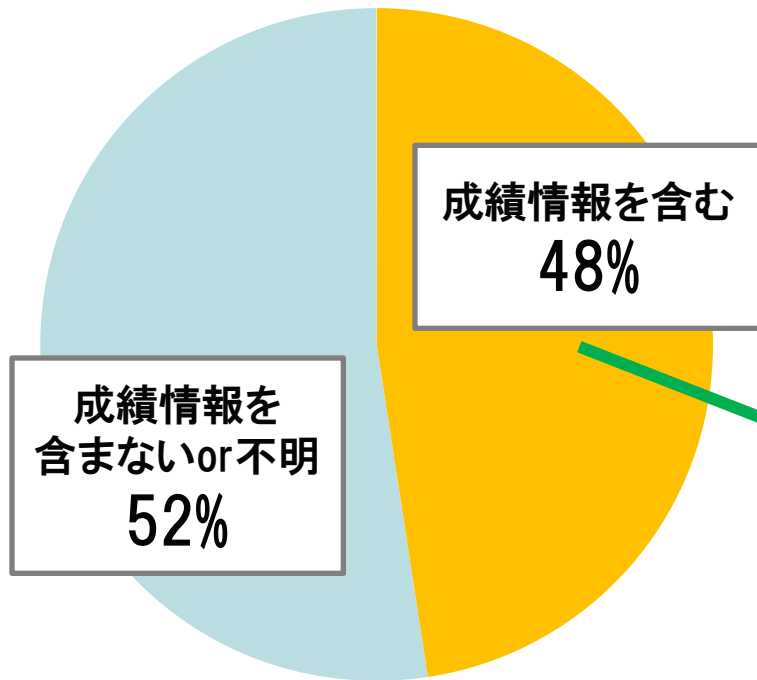
• 一般企業と比較すると、書類の事故が多いことも特徴であるといえます。

⇒テスト、プリントなどの授業で使うものには紙が多いこと、名簿など校務で使う書類も多いことが理由として考えられます。

※1件の事故で複数の媒体から漏えいした場合は、漏えいしたすべての媒体の件数を加えています。

成績情報が含まれていた事故の割合

- ◆ 情報漏えい事故のうち、成績情報を含むものが半数近くでした。



◆参考:情報の価値◆

1人分の成績情報=3万3,000円

(JNSA2010年 情報セキュリティインシデントに関する調査報告書の想定損害賠償額算定式より)

平成22年度の
成績情報漏えい数 29,399 件

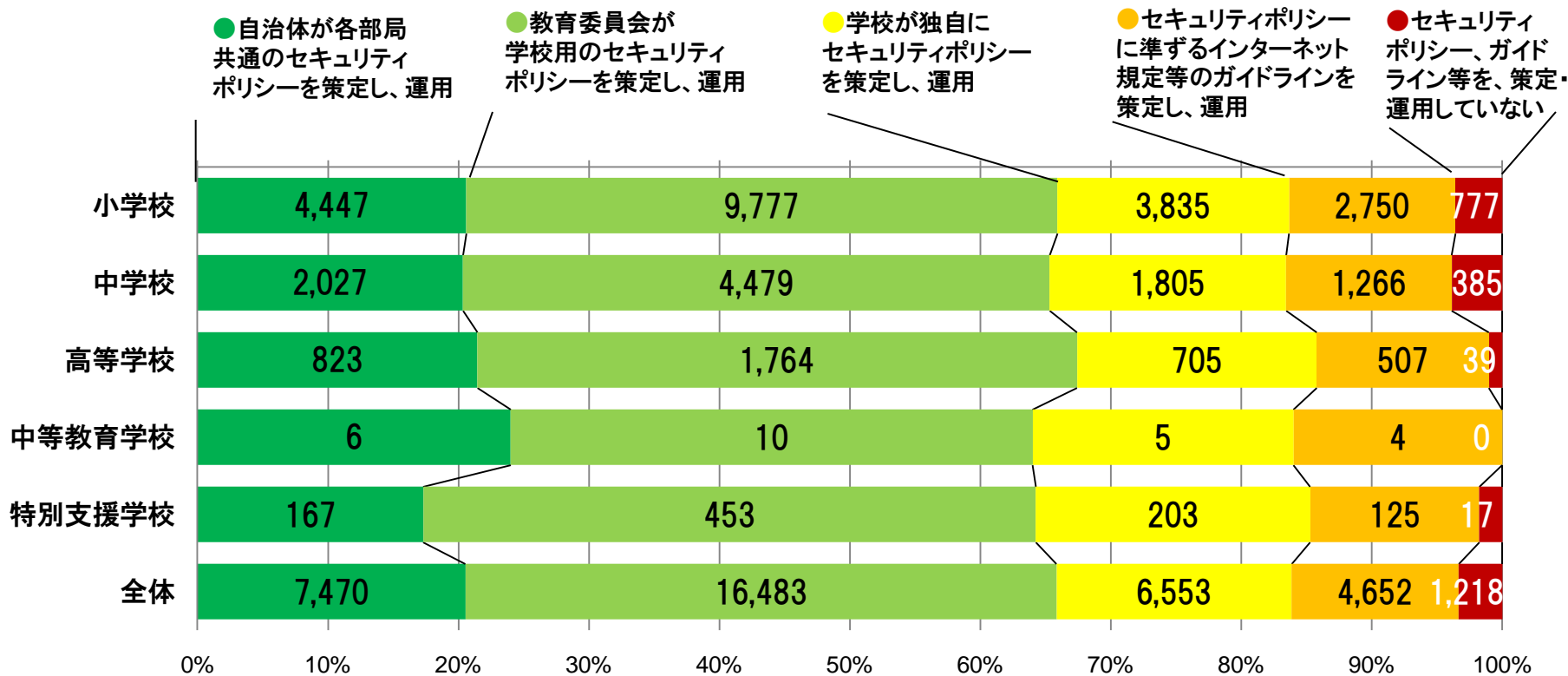
賠償額に
換算すると 約 9億7,000万円

傾向

成績の情報は非常にデリケートな情報であり、漏えいが発生した場合に児童・生徒、保護者に与えてしまう影響は多大なものとなります。先生が校務作業で取り扱う機会も多いため、より注意する必要があります。

情報セキュリティポリシー・ルールがある学校の割合

◆コンピュータをインターネットに接続している学校で、セキュリティポリシーやルールを策定している学校の数と割合（文部科学省 学校における教育の情報化の実態等に関する調査結果(平成21年度)より）



◆ルールがある学校が全体の96.6%ですが、管理ミスなどの事故が多いことから、ルールがうまく機能していないケースがあると考えられます。

参考情報：平成21年度 個人情報の不適切な取り扱いに係る処分について(文部科学省)

◆ 処分人数・処分内容の内訳

処分を受けた教育職員数 合計424人

訓告等を含めた懲戒処分等286人(前年度比9人増)

懲戒処分48人(前年度比27人減)

減給
13人



- ・全体の三割が、漏えいした本人だけでなく、監督責任による処分を受けています。対策を組織全体を行っていく必要があります。

◆ 処分の理由



補足：事故の種類 分類名の解説(1)

- ◆ 本資料では、情報セキュリティ事故の種類を次のように分類しています。

事故の種類	どのような事故か
不正な情報持ち出し	<p>業務上の必要性などからルールを逸脱して情報を持ち出した結果、情報漏えいした場合。</p> <p>※ルールを逸脱して持ち帰った結果、盗難にあったり、ファイル交換ソフトで漏えいした場合も、不正な情報持ち出しに分類する。</p>
管理ミス	<p>学校内・組織内での取り扱いが不適切だったため、紛失や行方不明となった場合。作業手順の誤りや、情報の公開、管理ルールが明確化されていなかったために業務上において漏えいした事故。原因が学校・組織の管理体制にある。</p> <p>※管理ミスによって盗難が発生した場合は盗難に分類する。 ※校内において、管理が行き届かずに誤って廃棄した場合も含む。</p>
盗難	<p>第三者によって情報記録媒体(USBメモリ、パソコンなど)と共に情報が盗まれた場合。車上荒らし、学校侵入による窃盗など。</p> <p>※保存された情報のみを盗難された場合は、不正アクセスに分類する。</p>
紛失・置き忘れ	<p>持ち出し許可を得た情報を、持ち出し先や移動中に置き忘れたり、紛失した場合。個人の管理ミスによって発生した場合。</p> <p>※校内で管理すべき情報を紛失した場合は、管理ミスに分類する。</p>

補足：事故の種類 分類名の解説(2)

事故の種類	どのような事故か
設定ミス	ユーザがWebサーバやファイルのアクセス権などの 設定を誤ったこと によって情報漏えいした場合。
誤操作	あて先を間違えたり、操作ボタンを間違えて押したりするなどの、 人間の作業・行動によって 情報漏えいした場合。
不正アクセス	外部の第三者が 、主にネットワークを経由して不正にアクセスを行い、情報漏えいした場合。 ※内部の人間の不正アクセスの場合は、内部犯罪・内部不正行為に分類する。
内部犯罪・ 内部不正行為	内部の人間が 、不正アクセス、その他不正な行為によって情報を持ち出し、悪用した場合。
ワーム・ウィルス	ウィルス・ワームによって、情報が漏えいした場合。
バグ・ セキュリティホール	OSやアプリケーション等の既存のソフトウェア上のバグ・セキュリティホールが原因で情報が漏えいした場合。
目的外使用	個人情報を当初の目的以外の用途に使用した場合。開示範囲外を超えて公開した場合。
その他	上記のいずれにも該当しないもの。
不明	原因が不明のもの。