１０１－１０６４
平成２２年　５月２１日

本庁各課（室）長
各出先機関の長
各県立学校長　殿
学校以外の教育機関の長

教　育　長

職員の情報セキュリティ意識の徹底について（通知）

情報セキュリティ対策の徹底については、日頃から厳しく指導及び管理いただいているところですが、昨年度から今年度にかけて、本県において、業務用パソコンやＵＳＢメモリが紛失する事案等が発生しております。

今のところ、個人情報等のデータが流出したということは聞いておりませんが、私たち県職員は、これらの事実を重く受け止め、個人情報の持つ重要性を再度認識するとともに、その取扱いについては今まで以上に細心の注意を払うことが求められます。

また、行政機関からの個人情報の流出は、県民の信頼を損ねるとともに、個人の権利利益の害等を引き起こすなど不測の事態を生じかねません。

つきましては、今後再びこのような事案等が発生することのないよう、下記により、再度、各所属にて情報セキュリティ意識の徹底について、職員への周知徹底をお願いします。

なお、各市町村教育委員会教育長へは、県教育長より参考までに通知文書を送付しましたので申し添えます。

記

１　パソコン及びＵＳＢメモリなどの記録媒体は、原則、庁外（学校等含む。）持ち出し禁止とする。
ただし、業務上必要な場合に限り、所属長の許可により持ち出しすることは可能とし、情報は必要最低限のものとする。

２　保有個人情報の送信や送付に当たっては、所属長の指示に従い、安全な送信・送付手段を選択するとともに、あて先等の十分な確認を行うこと。
なお、ファックスによる個人情報の送信は、原則、禁止とする。ただし、業務上必要な場合に限り、所属長の許可により送信することは可能とする。

※　上記１及び２の所属長の許可により持ち出し及び送信が可能なものについては、各所属においてルールを定める必要があるため、【別紙１】の参考例により、情報資産の持ち出し及び送付に関する規程を定めること。

３　持ち出す電子ファイルにはパスワードを設定すること。
電子ファイルのパスワードの方法は、「サイボウズ（Ｒ）ガルーン―ファイル管理(全庁)―情報政策課―パスワード設定・暗号化」を参照(別紙２～５)。

※　ＵＳＢメモリのセキュリティツール等、Ｗｅｂサイトからのダウンロード方法については、「(別紙６)【参考】各メーカーのＷｅｂサイトよりダウンロードできるセキュリティツール・ソフトウェア等」を参照ください。

４　その他
別添リーフレット「今、教育現場での情報リスク管理が問われています」を参照に添付しておりますので、職員への周知徹底を図る際等にご利用ください。

（文書取扱　教育庁総務課）

担当：総務担当　金丸(内線3228)
電　話：０９８５(２６)７２３３
ＦＡＸ：０９８５(２６)７３０６

【別紙１】

（参考例）情報資産の執務室外持ち出し及び送付に関する規程

平成２２年４月１日
○　○　○　○課

１　総則

宮崎県情報セキュリティ対策基準に規定される情報分類Ⅰ（個人情報）及びⅡ（公開することを予定していない情報及び行政事務の執行等に重要な影響を及ぼす情報）の情報資産（以下「重要情報資産」という。）は、原則として執務室外への持ち出しが禁止されている。

本規程は、○○○○課における重要情報資産の持ち出し及び送付の取扱いを定めたものである。

２　重要情報資産の持ち出し

重要情報資産の持ち出しは、原則禁止とする。

但し、職員が業務上重要情報資産を持ち出す必要がある場合は、別紙様式により必ず持ち出し申請を行い、情報セキュリティ管理者（以下「○○長」という。）の許可を受けなければならない。

また、持ち出した重要情報資産を返却する際は、必要な確認作業を実施しなければならない。

３　重要情報資産の送付

重要情報資産の送付は、原則禁止とする。

但し、職員がこれらの重要情報資産を郵送、ファクシミリ、電子メール等の手段により送付する場合は、起案の決裁等により○○長の許可を受けなければならない。

また、送付後には到着確認を行わなければならない。

４　安全対策

（１）持ち出しについて

職員が重要情報資産の持ち出しを行う際には、盗難・紛失等に注意し、施錠、電子データの暗号化等、必要な対策を実施しなければならない。

また、職員は持ち帰ったパソコンや記録媒体を使用する前に、ウィルス対策ソフトを使用してコンピュータウィルス等を持ち込まないようにしなければならない。

（２）送付について

職員が重要情報資産を送付する際にはなるべく安全な方法を選択し、特に電子メールは誤送信等の危険性を考慮して添付ファイルを暗号化する等の対策を実施しなければならない。

この場合、パスワードは別の方法で受取人に伝達しなければならない。

５　緊急時対応

職員は、重要情報資産の紛失・盗難等、重要情報資産の流出に気づいた場合は、別に定める緊急時対応手順(※)に従って、○○長に報告しなければならない。

６　附則

この規程は、平成○○年○月○日から施行する。

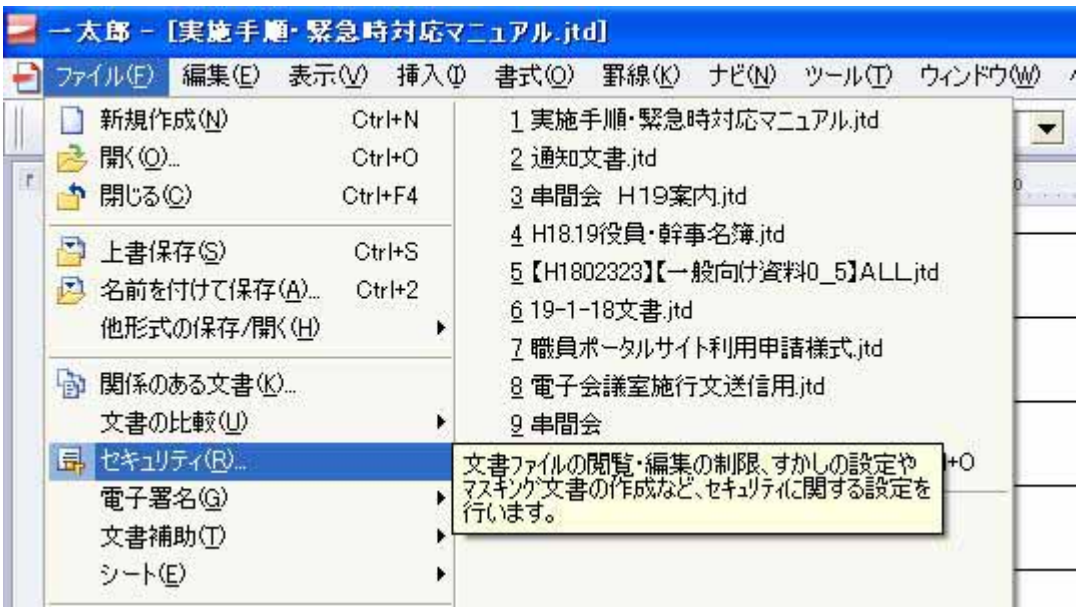
※　別記参照。

なお、サイボウズ（R）ガルーン上は、「全庁ファイル管理―情報政策課―規程・要領等―一般業務用ＰＣ管理要領―緊急対応手順．ｐｄｆ」に掲載。

一太郎パスワード設定手順 1／5

1　既存のファイルにパスワードを設定する

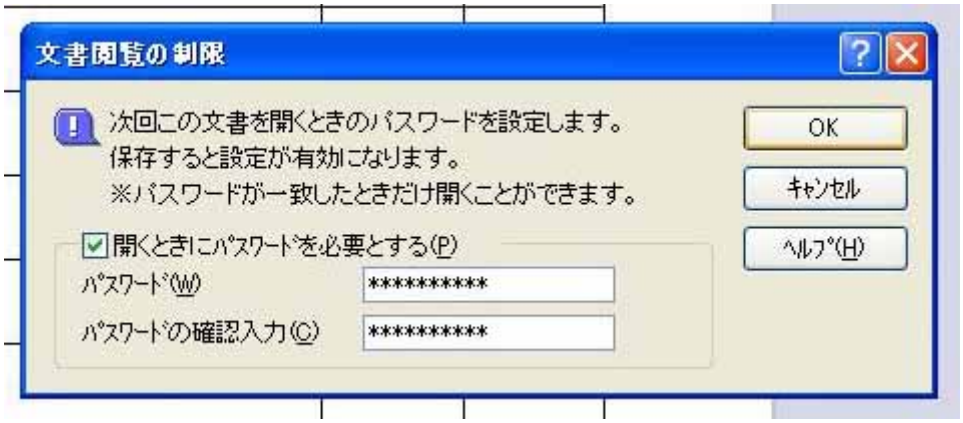
1－①「ファイル＞セキュリティ」を実行します。



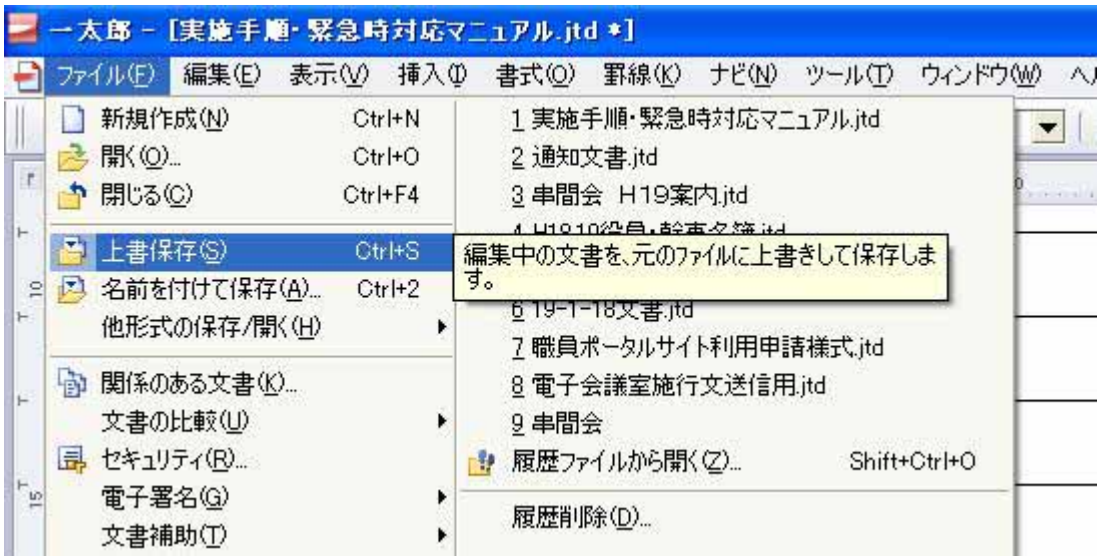
1－②「文書閲覧制限」のを「設定」ボタンをクリックします。

1－③「開くときにパスワードを必要とする」にチェックを入れてパスワードを設定します。上下とも同じパスワードを入力してください。

◆ 注意事項 ◆
※パスワードはアルファベットの大文字と小文字が区別されます。
※パスワードを紛失したり、忘れたりした場合、ファイルを開くことはできなくなります。

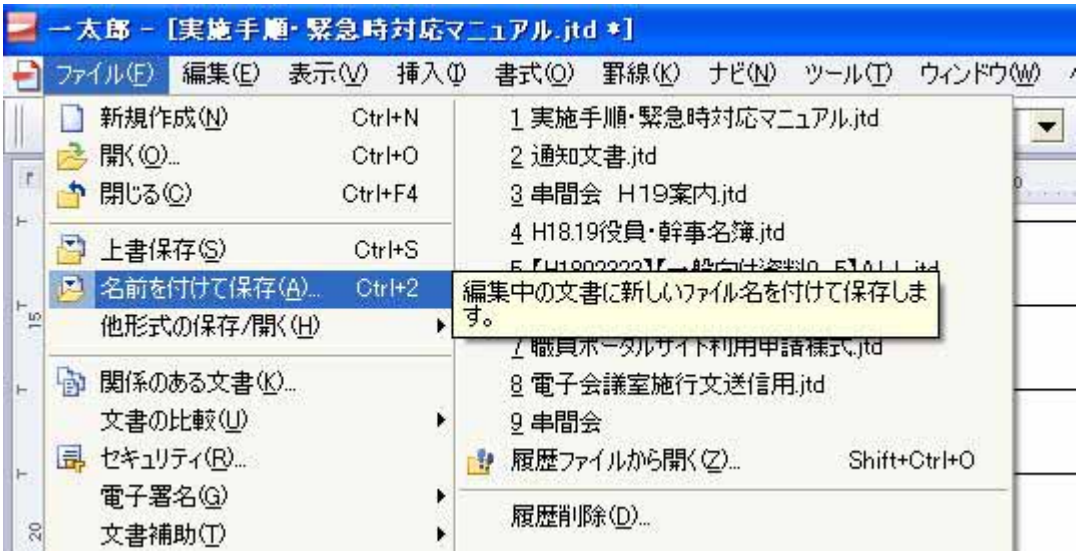


1－④ファイルを保存すると設定が有効になります。

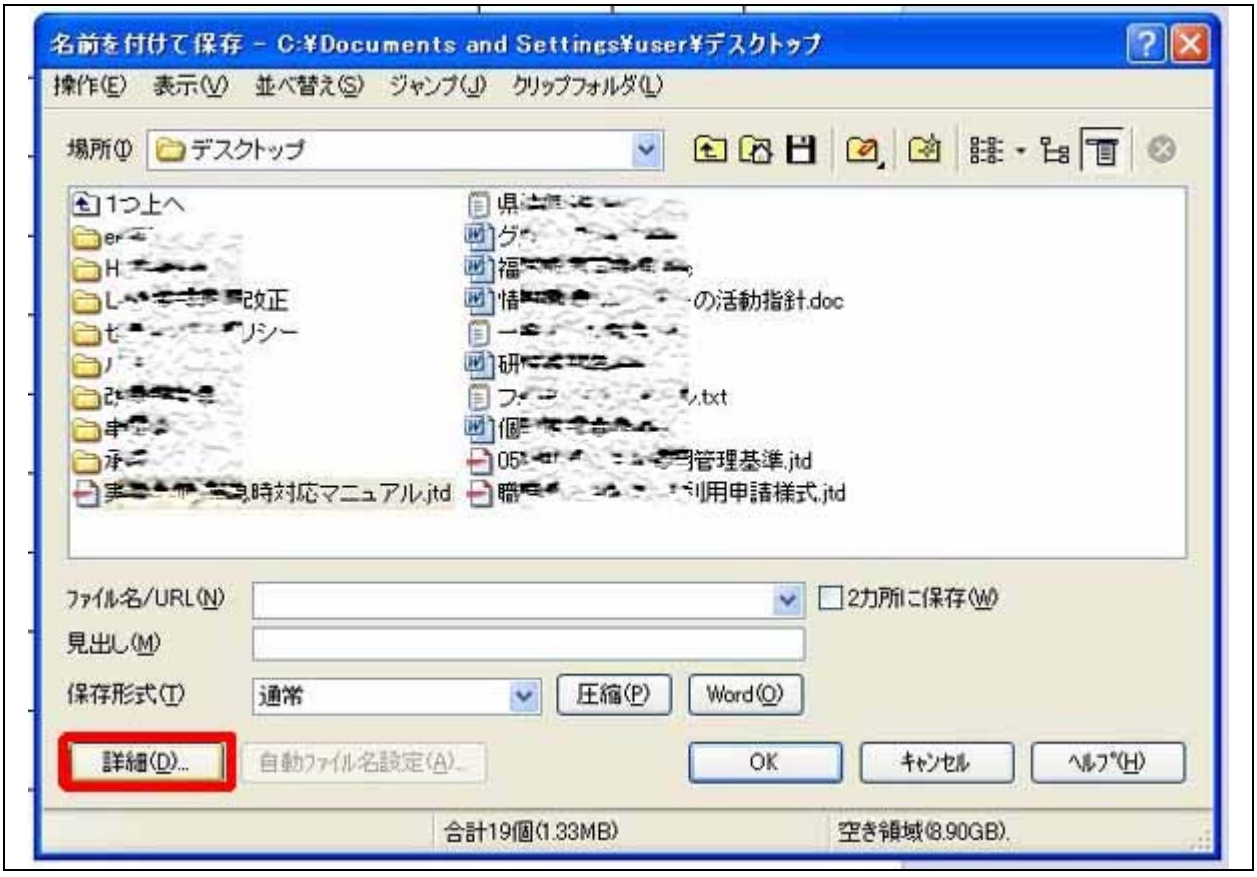


2　新規作成した文書にパスワードを設定する。

２－①「ファイル＞名前をつけて保存」を実行します。

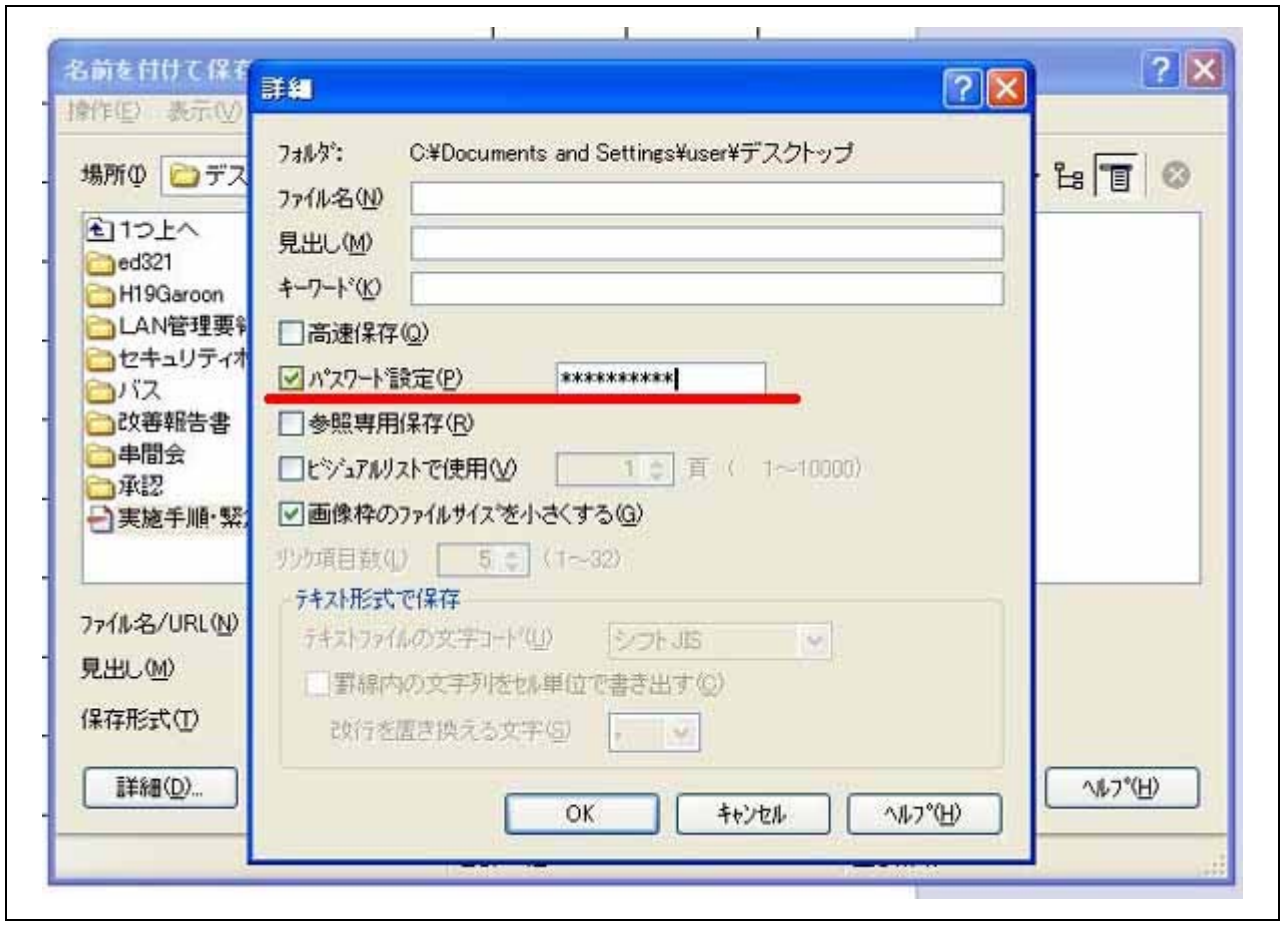


２－②「詳細」ボタンをクリックします。

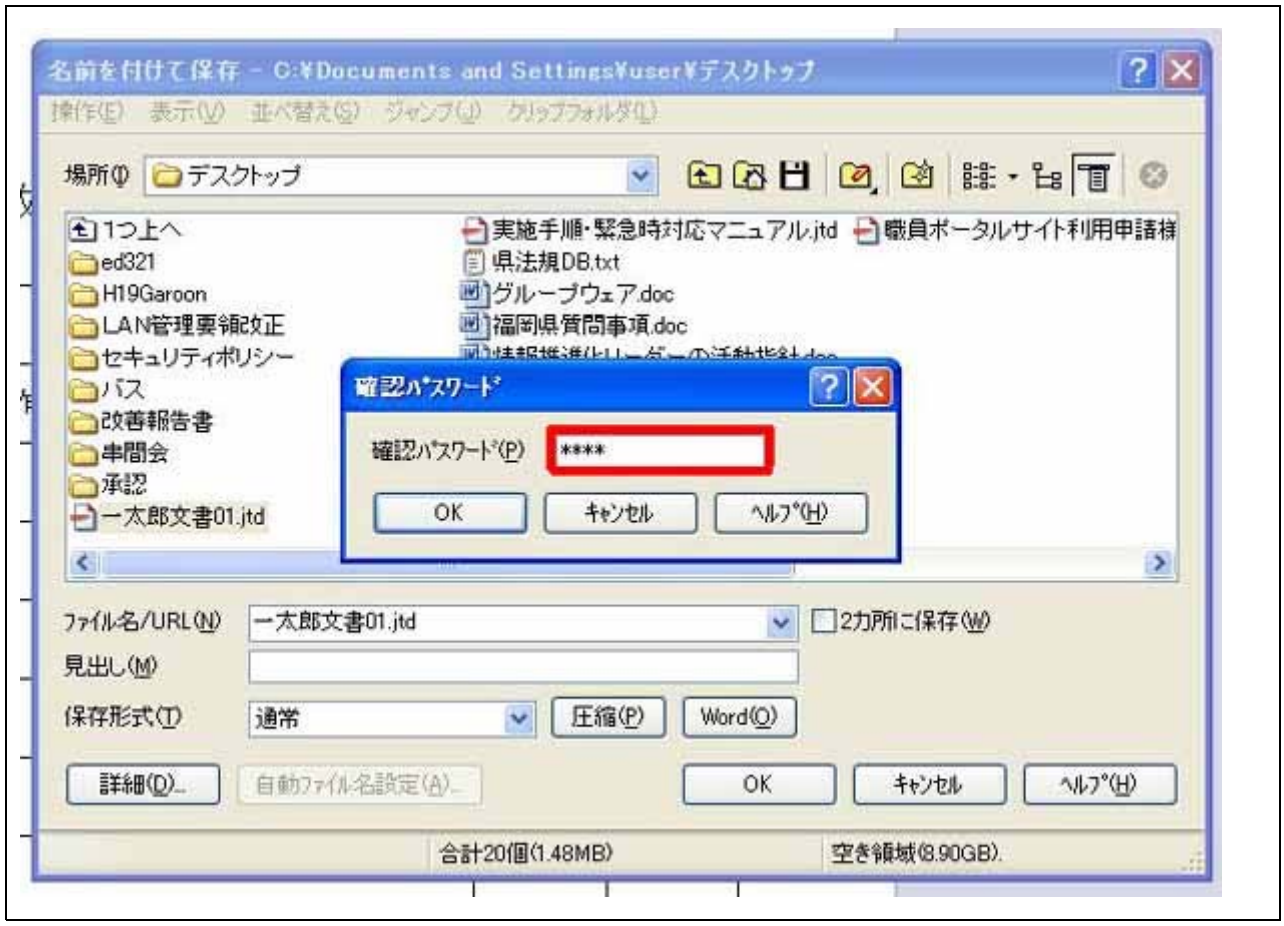


２－③「パスワード設定」にチェックを入れて、パスワードを入力します。

◆ 注意事項 ◆
※パスワードはアルファベットの大文字と小文字が区別されます。
※パスワードを紛失したり、忘れたりした場合、ファイルを開くことはできなくなります。

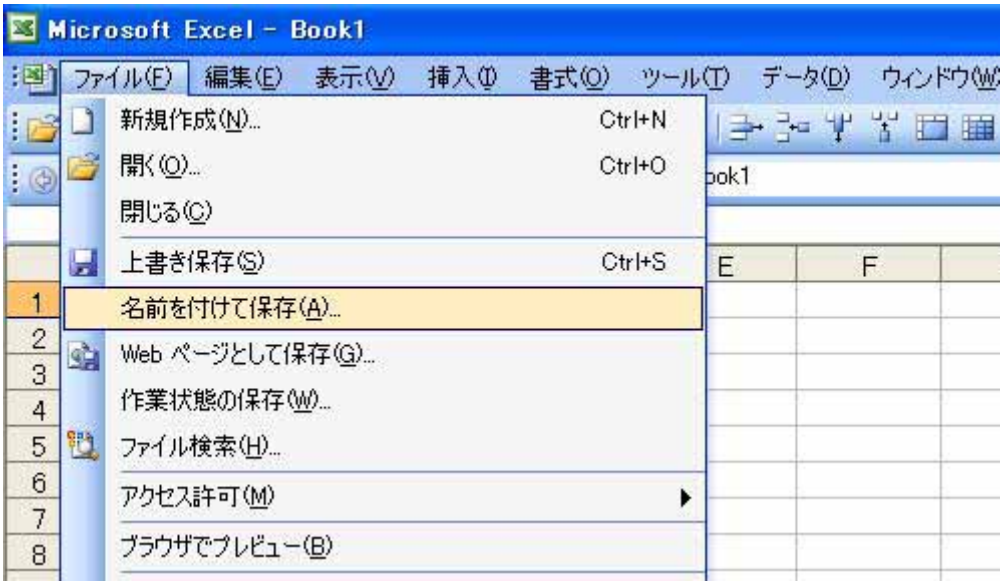


２－④パスワードの確認画面が表示されるので、２－③で設定したパスワードを入力してください。
ファイル名を入力して「OK」ボタンをクリックします。

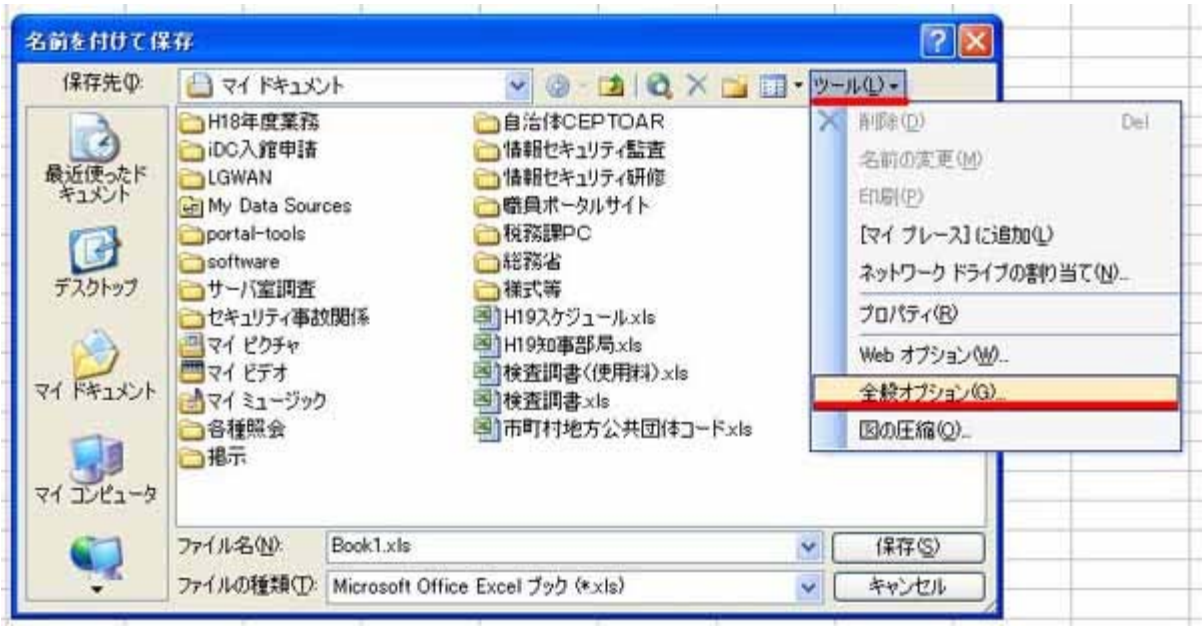


Microsoft Excel パスワード設定手順

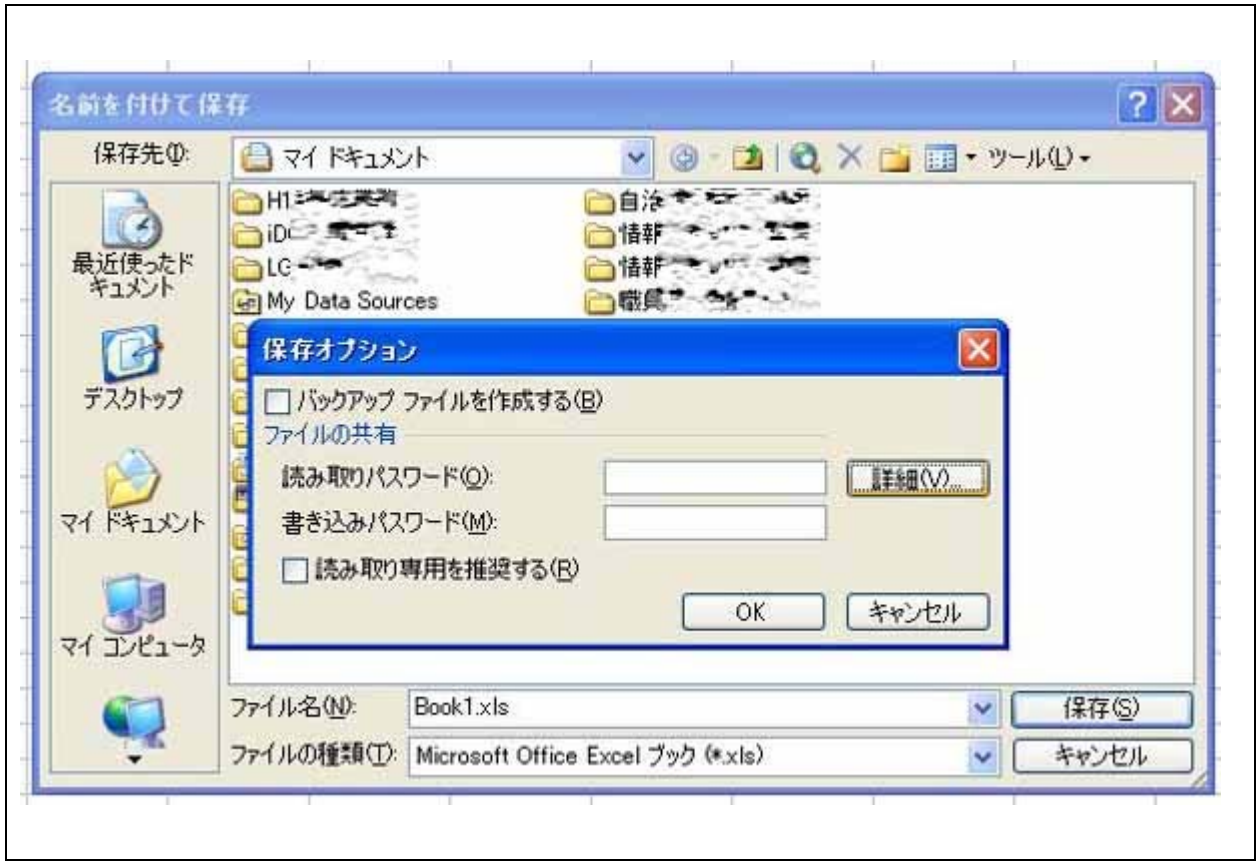
①「ファイル＞名前をつけて保存」を実行します。



②「ツール＞全般オプション」を選択します。



③「詳細」ボタンをクリックします。

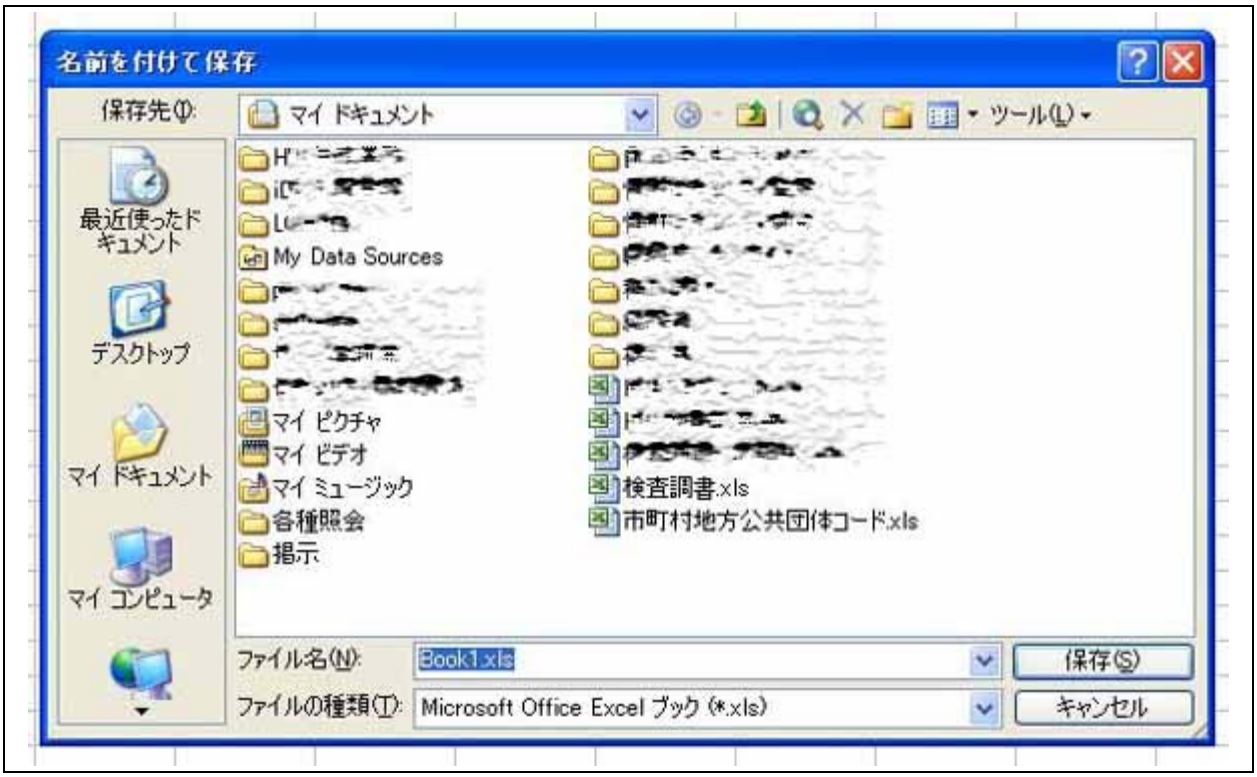


④「暗号化の種類」を選択します。「キーの長さ」が長いほど解読されにくいので、なるべく「128」を選んでください。選んだら「OK」ボタンをクリックします。

⑤「読み取りパスワード」を設定します。入力したら「OK」ボタンを押します。
（書き込みパスワードは、ファイルを変更させたくないときにのみ使用します。）

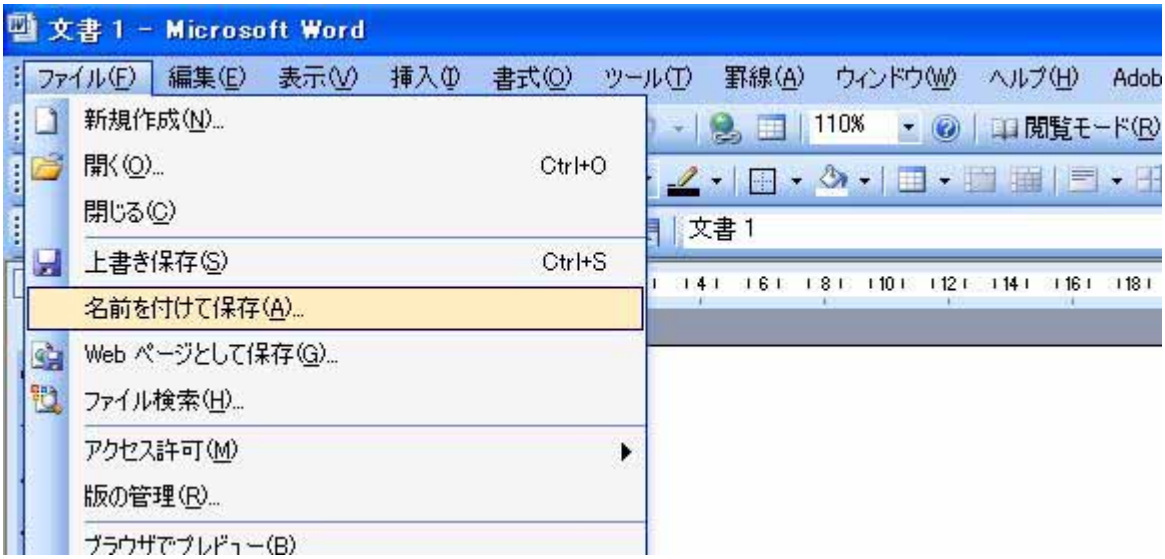
◆ 注意事項 ◆
※パスワードはアルファベットの大文字と小文字が区別されます。
※パスワードを紛失したり、忘れたりした場合、ファイルを開くことはできなくなります。

⑥ファイル名をつけて保存します。

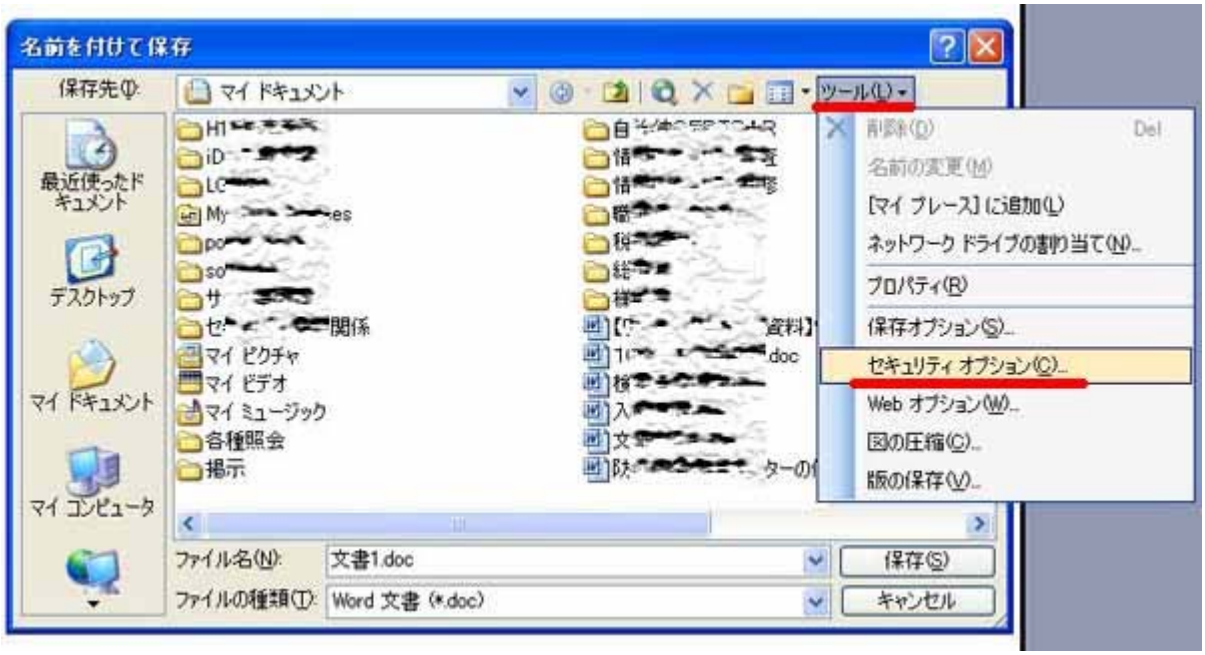


Microsoft Word パスワード設定手順

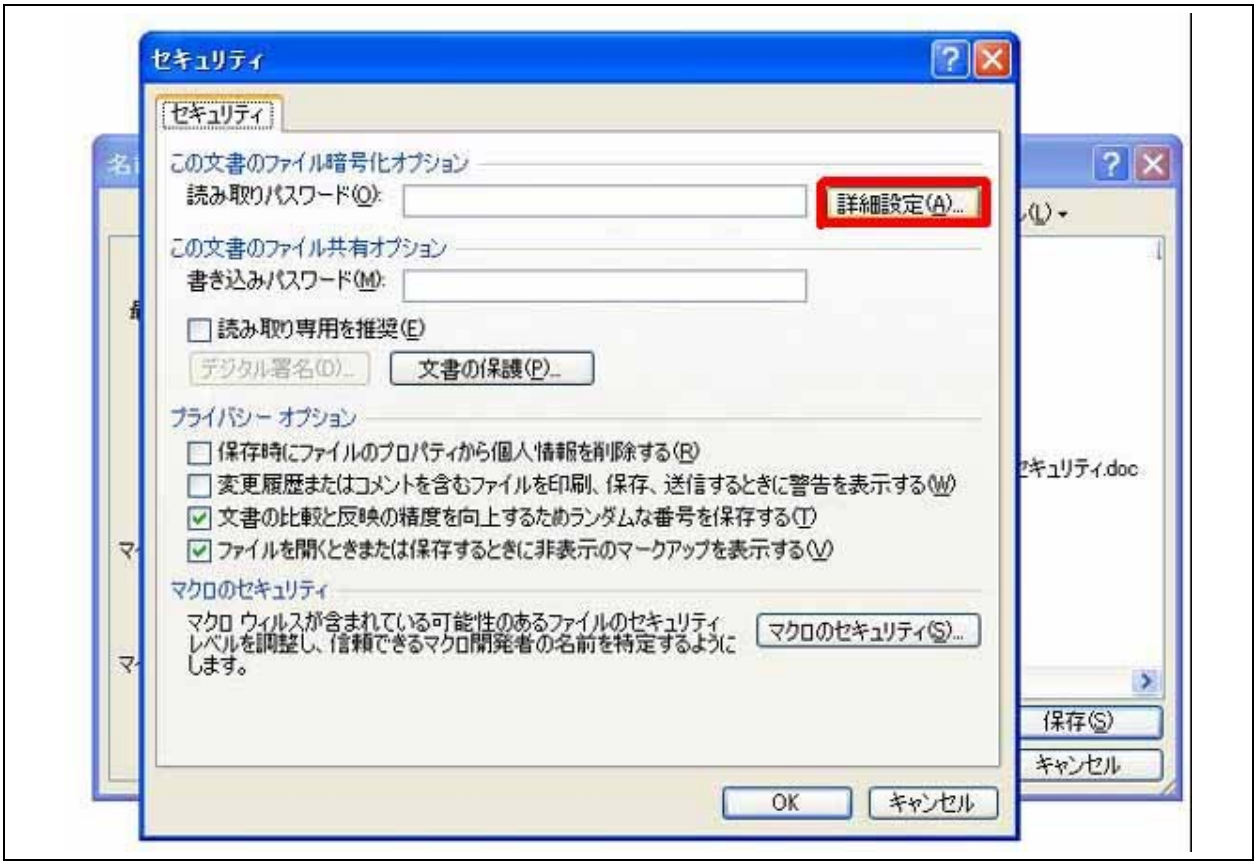
①「ファイル＞名前をつけて保存」を実行します。



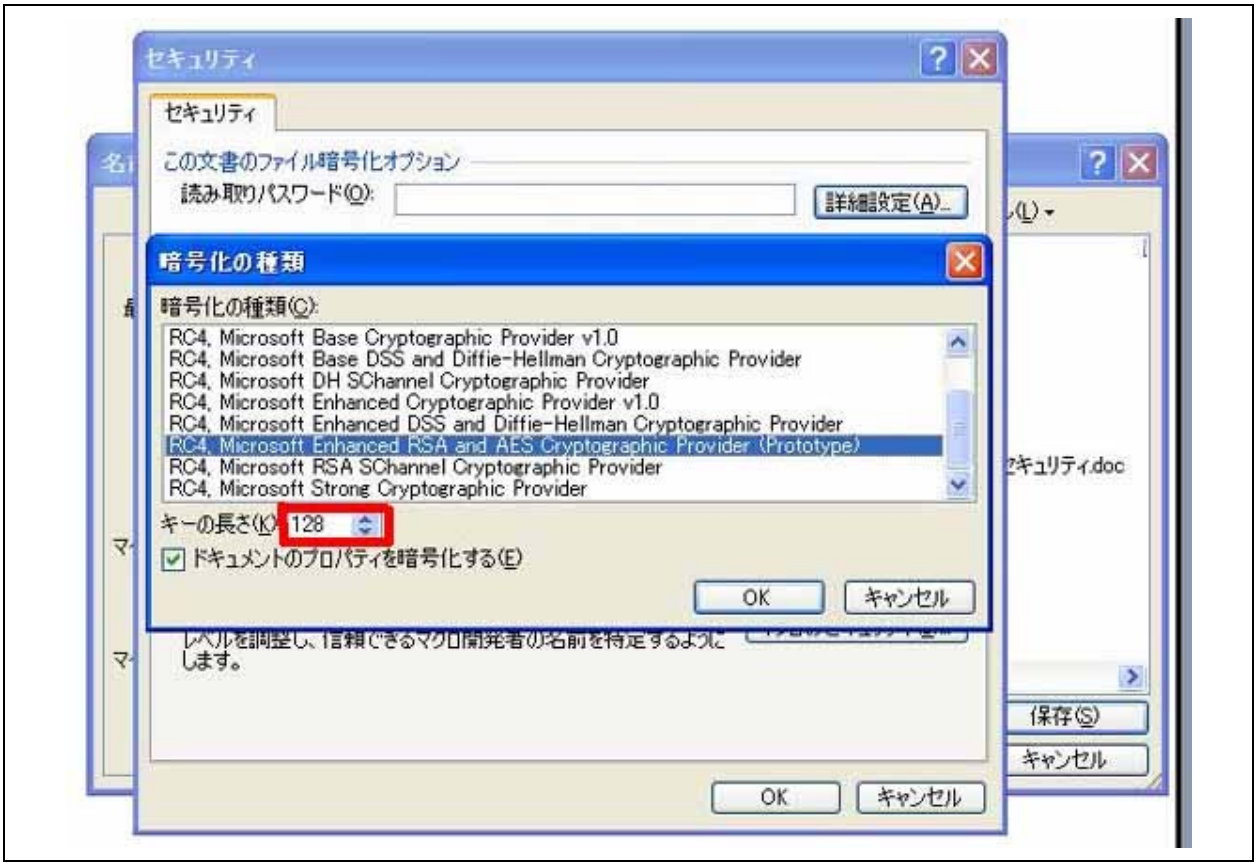
②「ツール＞セキュリティオプション」を選択します。



③「詳細設定」ボタンをクリックします。

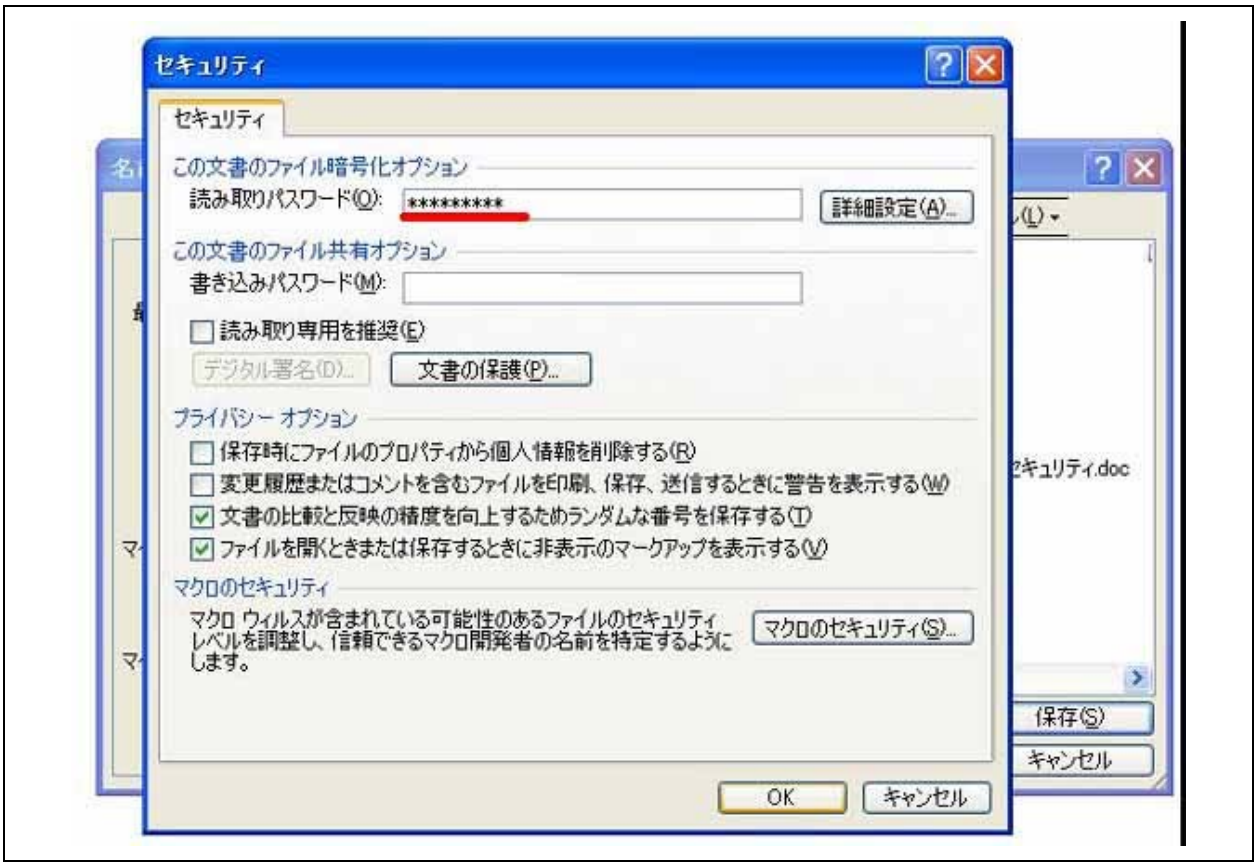


④「暗号化の種類」を選択します。「キーの長さ」が長いほど解読されにくいので、なるべく「128」を選んでください。選んだら「OK」ボタンをクリックします。



⑤「読み取りパスワード」を設定します。入力したら「OK」ボタンを押します。
（書き込みパスワードは、ファイルを変更させたくないときにのみ使用します。）

◆ 注意事項 ◆
※パスワードはアルファベットの大文字と小文字が区別されます。
※パスワードを紛失したり、忘れたりした場合、ファイルを開くことはできなくなります。

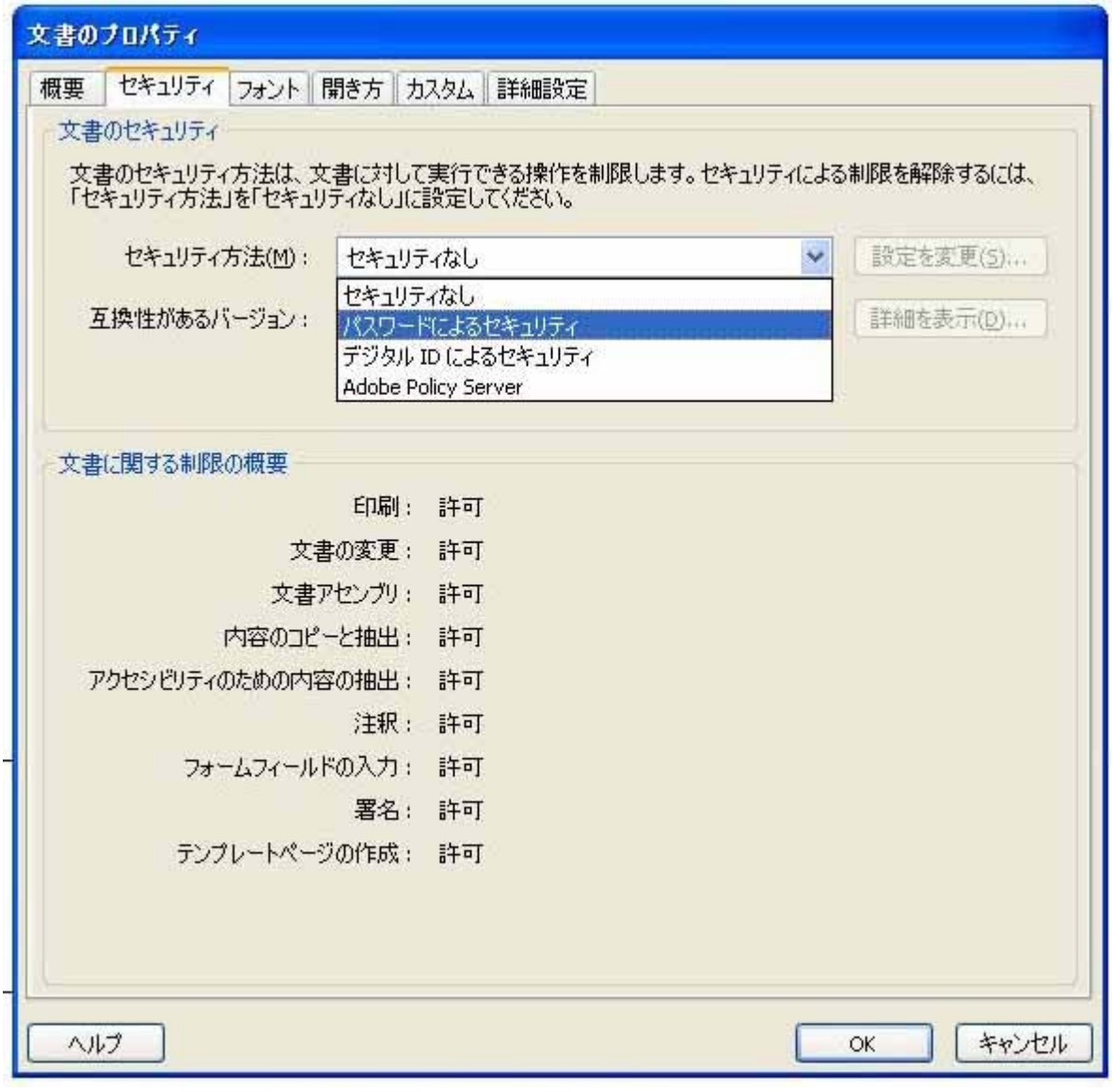


⑥ファイル名をつけて保存します。

Adobe Acrobat パスワード設定手順 1／4

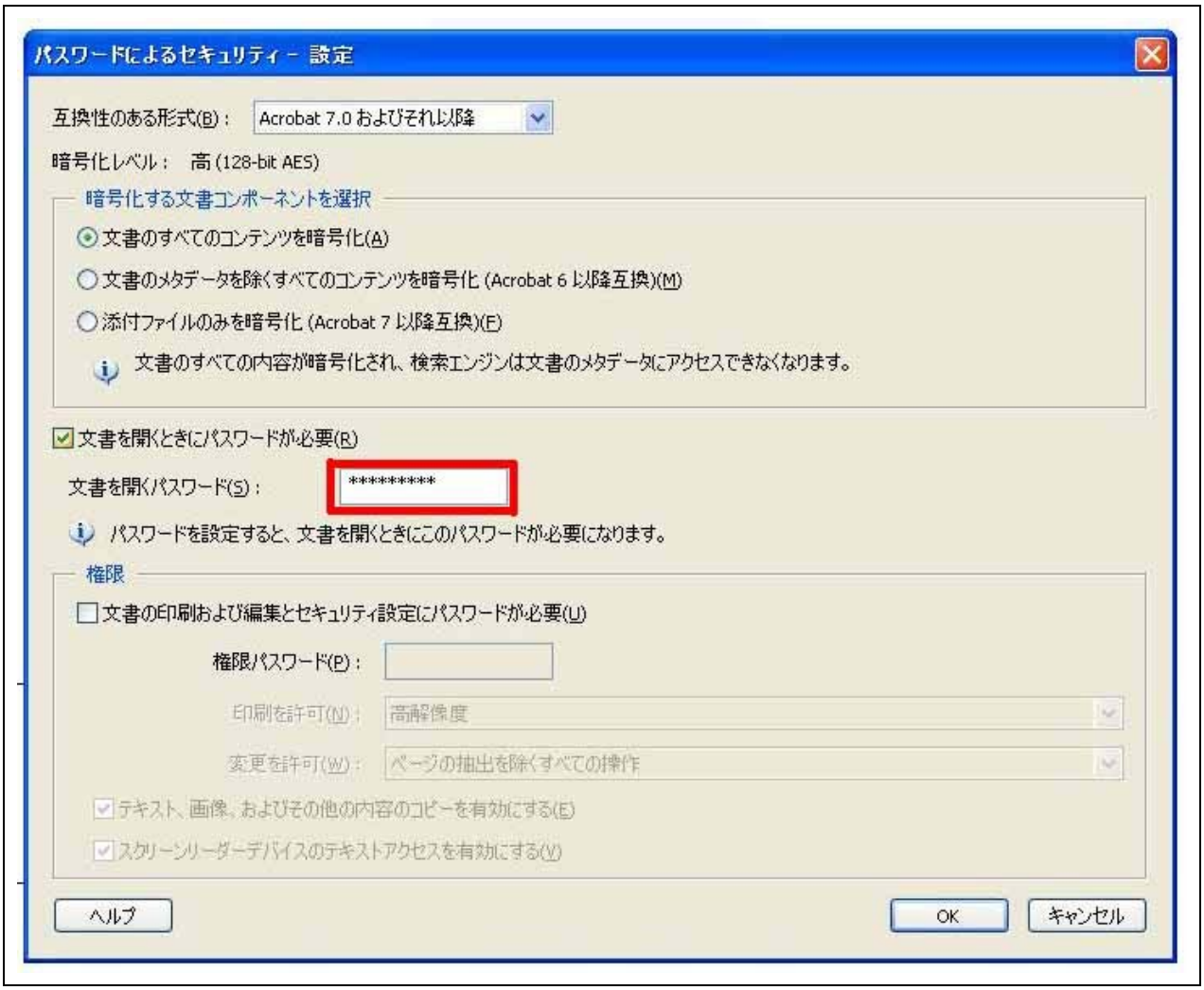
①「文書＞セキュリティ＞文書のセキュリティ設定を表示」を実行します。

②「セキュリティ方法」から、「パスワードによるセキュリティ」を選択します。

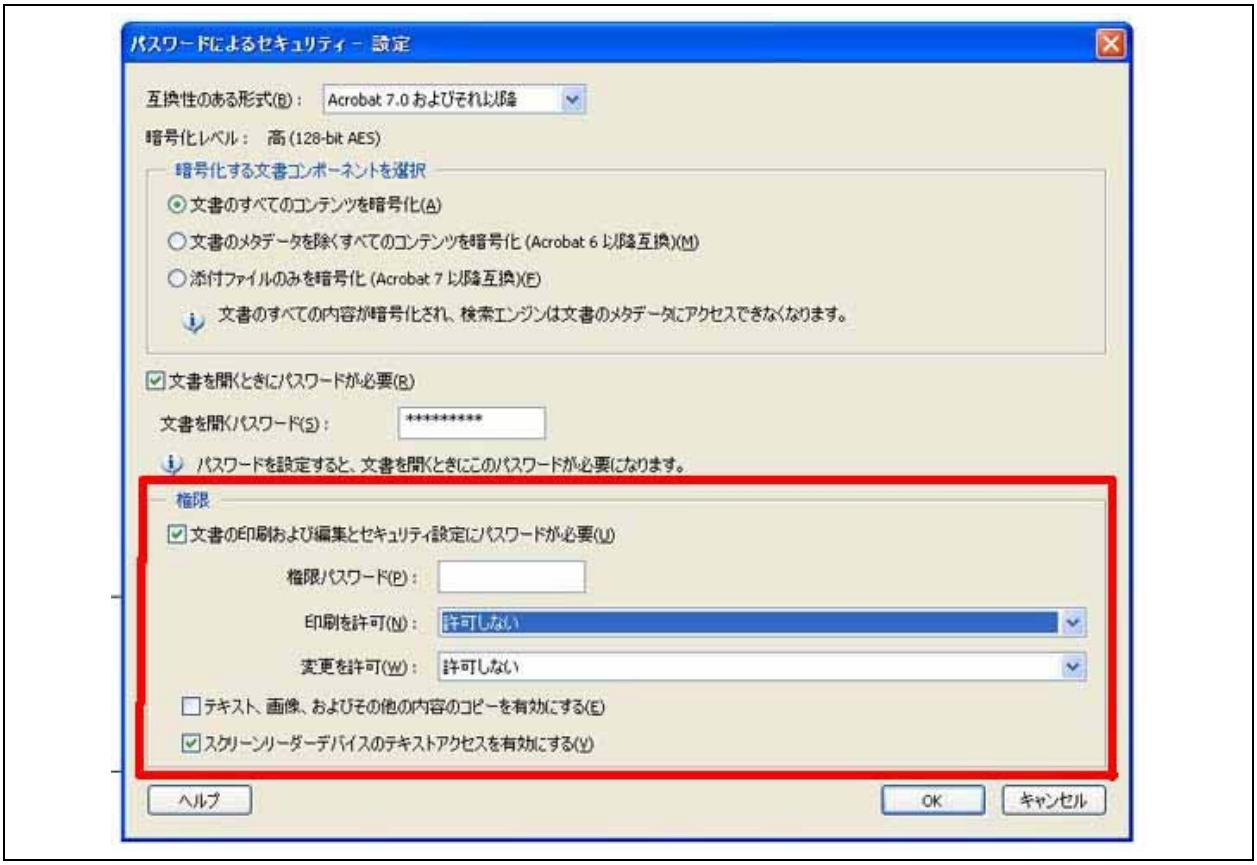


③「文書を開くときにパスワードが必要」にチェックを入れ、パスワードを入力します。

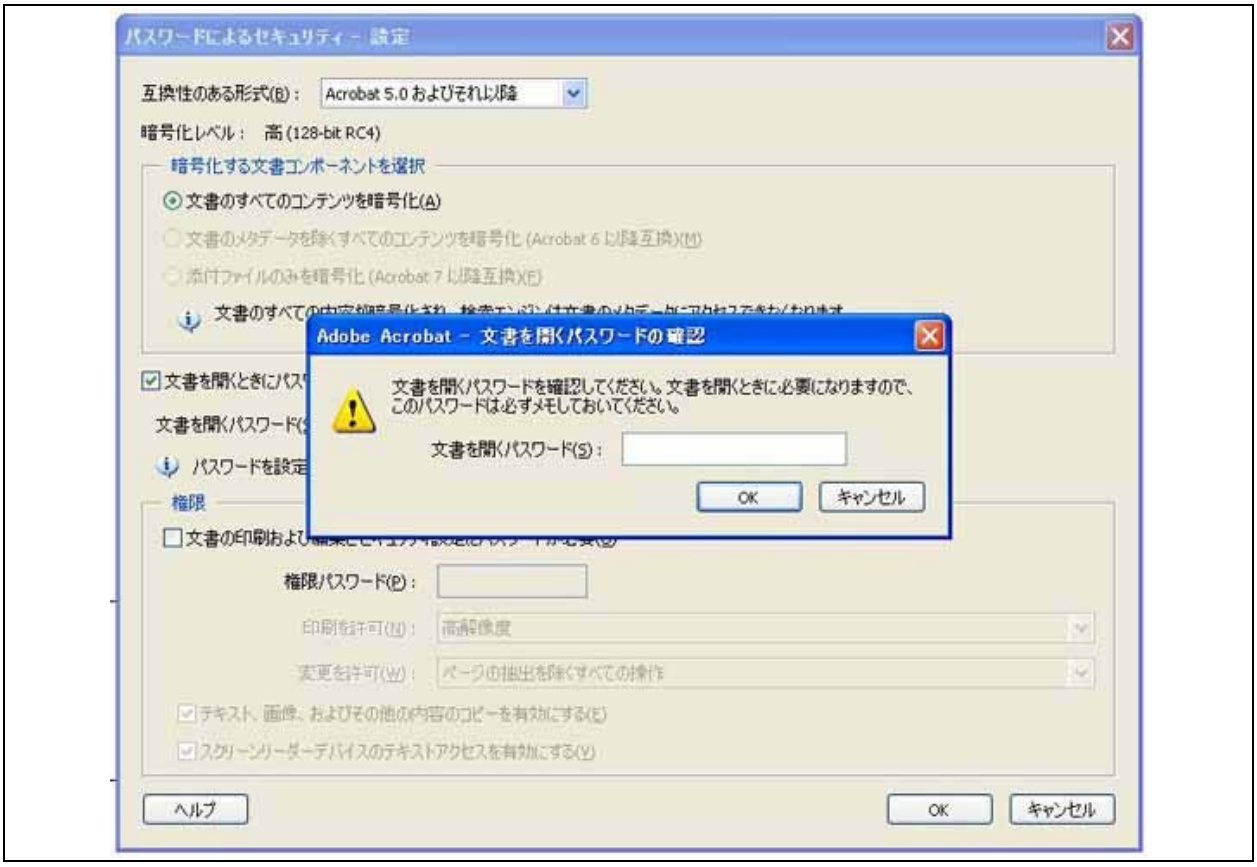
◆ 注意事項 ◆
※パスワードはアルファベットの大文字と小文字が区別されます。
※パスワードを紛失したり、忘れたりした場合、ファイルを開くことはできなくなります。



④アクロバットでは印刷の可否、ファイルの変更の可否についても設定することができます。



⑤「OK」ボタンをクリックすると、パスワード確認画面が表示されるので、④で設定したパスワードを入力します。



⑥ファイルを保存するとパスワード保護が有効になります。

別紙6

【参考】各メーカーのWebサイトよりダウンロードできるセキュリティツール・ソフトウェア等

メーカー：シリコンパワー

シリコンパワー　ユーティリティ　←　Web ページ検索キーワード

- ◆ シリコンパワー Silicon-Power ダウンロードサービスへ
  - ■ SmartKit はシリコンパワー製 USB フラッシュメモリ製品専用のソフトウェア。
  - ■ SmartKit のソフトウェアにより、次の機能を利用することができる。
  - ■ セキュリティ機能
    - ✧ USB フラッシュのメモリ領域を共有エリアとセキュリティエリアに分割することで保存したデータのアクセスをパスワードにより保護する機能。
  - ■ シークレット・ジップ機能
    - ✧ USB フラッシュ内に保存したデータの、圧縮／解凍／パスワードによるファイルの保護を簡単に出来る機能。
    - ✧

メーカー：グリーンハウス

グリーンハウス　ドライバ　←　Web ページ検索キーワード

- ◆ サポート情報 GREEN HOUSE グリーンハウスへ
- ◆ ダウンロードドライバ→USB フラッシュメモリ→Pico Boost 型番 製品詳細 へ
  - ■ GH-UFD＊GBS　USB フラッシュメモリ「Pico Boost」 ＊GB
  - ■ GH-UFD**BS シリーズ対応のパスワードロックソフト
    ※ windows 2000(SP4),XP(SP2),Vista(32bit)のみ対応

メーカー：Transcend

Transcend　技術サポート　←　Web ページ検索キーワード

- ◆ トランセンドジャパン － 技術サポート → ダウンロードセンターへ
- ◆ JetFlash® elite V2.0 を選択
  （JetFlash® elite V2.0 はトランセンドの JetFlash® USB メモリ専用に開発されたソフトウェア）
  - ■ Seclet-zip
    - ✧ 優れたセキュリティと圧縮機能でデータを安全に保存
    - ✧ メモリ容量を有効活用できる保存ファイルの圧縮機能に加え、安全にデータを保存できる。
      ※ JetFlash elite V2.0 は Windows 2000/XP/Vista/7 のみに対応

メーカー：バッファロー

バッファロー　Secure Lock Mobile for USB メモリー　←　Web ページ検索キーワード

- ◆ ドライバーダウンロード Secure Lock Mobile for USB メモリへ
  - ■ USB フラッシュメモリを暗号化できるツール

メーカー：エレコム

エレコム　USB メモリ　セキュリティソフト　PASS　←　検索キーワード

- ◆ USB フラッシュメモリ用セキュリティソフト　「PASS（Password Authentication Security System） X AES」
  - ■ エレコム社 USB フラッシュメモリ（一部除く）用セキュリティソフト
    「PASS（Password Authentication Security System）X AES」
    - ✧ 「PASS（Password Authentication Security System）X AES」にあらかじめ登録された 3 台までのパソコンについては、USB フラッシュメモリをパソコンに接続するだけで自動的に認証する。
    - ✧ 保存データを「AES 256bit」で暗号化する機能が加わり、セキュリティフォルダ上に保存されるデータはすべて、自動的に「AES 256bit」で暗号化される。これにより、認証セキュリティを回避するために、USB メモリ本体を分解して直接データを取り出しても、データが暗号化されているので、解読しない限り内容を閲覧できなくなる。

メーカー：SONY

SONY USB メモリ　ソフトウェア　←　Web ページ検索キーワード

- ◆ ソフトウェア ｜USB メモリー POCKET BIT“ポケットビット”へ
  - ■ ファイル暗号化ソフト「キチッと秘密ファイルロック」
    - ✧ 「キチッと秘密ファイルロック」をご使用になると、ドラッグ＆ドロップで簡単にファイルに暗号をかけて保存することができる。
      ※対応 OS は、Windows 7,Windows Vista および Windows XP（SP2 以降）

（別添）

今、教育現場での情報リスク管理が問われています

情報リスクとは、
情報を扱う中で、危険に遭う可能性や損をする可能性のこと。
その中で、

怖いのは、やはり**個人情報の漏洩！**

■　万が一情報漏洩が起こったら

民事賠償　**刑事罰**　**信用失墜**

本県における過去の事例

- ■個人情報FAX誤送信
- ■県職員PC盗難
- ■ウィニー通じ名簿流出
- ■児童情報WEB掲載
- ■通知票盗難
- ■ネット地図に個人名
- ■USBメモリ紛失

これらに共通する原因は、
情報資産の持ち出し、外部へ送信、ネットに発信する際の危機感の欠如、責任感不足

～特に注意！便利かつ大容量のUSBメモリ～


リスク1：USBワーム

〇ウイルスに感染したUSBメモリを使用することで、コンピュータに感染する。
感染したコンピュータに別のUSBメモリが接続されると、ウィルス自身をUSBメモリにコピーして、USBメモリを介して次々に感染を広げる。
〇ウイルスの中には、Webページから別のウイルスをダウンロードする活動を行うものもある。
結果として、コンピュータがインターネットからの脅威にさらされることになる。

リスク2：媒体紛失

＜個人情報の紛失・盗難の防止＞
県立学校における生徒等に関する電子個人情報の適切な取扱いガイドライン(H17.1.27)より
(7)個人情報を保存した記録媒体は、外部へ持ち出しを禁止すること。

対策

◆◆紛失する、盗難に遭うという前提の元、そのリスク管理を行う事が大事◆◆
〇パスワードによるロックが可能なUSBメモリ
〇USBメモリにデータを書き込むとすぐに暗号化して保存するUSBメモリ
〇指紋認証機能を搭載したUSBメモリ　等が最低限必要
※セキュリティ機能が無いUSBに機能を付ける場合は、別紙「セキュリティ追加」参照

宮崎県教育委員会