学校情報セキュリティマニュアル

沖縄県はなさき支援学校（R4.7.11）

I. 情報セキュリティ対策の実施目的

（1）校務の円滑な運用のため、ＩＣＴの活用がスムーズにできるようにする。
（2）情報漏洩を防止する。
（3）本校の社会的信用の維持及び向上させる。

II. 情報セキュリティ対策の基本方針

（1）トラブルの未然防止（リスク・マネージメント）として、情報機器活用や ICT セキュリティ関連の情報提供や ICT 研修、ウィルス対策などに務める。
（2）トラブル発生時、被害を最小限にとどめる処置（クライシス・マネジメント）を講じる。校内で解決が見込まれない場合は関連部署と保守担当業者へ報告し、処置する。
（3）トラブル発生後、速やかに教育機能の回復と校務継続を図り、本校の社会的責任を果たす。

III. 情報資産

情報資産とは、資産として価値のある情報のことである。本校における情報資産は大きく分けて３つである。それは生徒に関すること、職員に関すること、学校に関することが挙げられる。デジタルデータと紙媒体ともに情報セキュリティにおける脅威から守らなければならない。

＜＜本校が管理する重要な情報資産＞＞

・生徒の個人情報：住所、連絡先、家族構成、生活環境、障がいに関する資料、支援計画に関する資料、勤怠、成績 等
・生徒指導情報：指導内容、指導歴、配慮事項 等
・高校入試：受検生を特定する資料（住所、連絡先、出身中、内申、成績 等） 入試問題、判定会議資料等
・職員の個人情報（住所、連絡先、家族構成、収入 等）
・校内ＬＡＮ接続端末やプリンタ等のＩＰアドレス
・教育支援システムや TimeNets、各サーバー、各端末のＩＤとパスワード な

IV. 情報セキュリティにおける脅威

「情報セキュリティ」における脅威とは、情報資産が利用できなくなる直接の原因となるモノである。

脅威の分類		例　　示	
人為的脅威	意図的脅威	・生徒 ・職員 ・外部	１．技術的な脅威 （1）不正侵入（不正アクセス）となりすまし。 （2）SNS 等で他人を誹謗中傷する情報や虚偽 の情報を打ち込む。 （3）ウィルス製造とその拡散。 （4）Web ページや情報資産の改ざん。 （5）情報資産の漏洩と流失や削除。 （6）各システムを乗っ取る。 など ２．物理的な脅威 （1）サーバーや通信機器・情報端末などを破壊や、電源を抜く。 （2）情報機器を無用に叩いたり、投げたり、落としたり、水没させたりする。 （3）情報機器を窃盗する。 など

脅威の分類		例　　示	
人為的脅威	偶発的脅威	・生徒 ・職員	1．技術的な脅威 （1）操作ミスによるデータの移動。 （2）操作ミスによるデータ削除。 （3）操作ミスによるデータの書き換え。 （4）操作ミスによる設定変更。 など 2．物理的な脅威 （1）情報機器や可搬記録媒体（ＵＳＢメモリや 外付けHDD ハードディスク など）を置き忘れる。 （2）情報機器や可搬記録媒体（ＵＳＢメモリや 外付けHDD ハードディスク など）を落として破壊する。 など
環境的脅威		自然災害事故など	地震、洪水、台風、落雷、火事、津波、 停電、瞬時停電(瞬断、瞬電) など

Ⅴ. 校内ＬＡＮ利用上での禁止事項

Ⅳ であげた脅威から校内ＬＡＮを守るため、沖縄県教育情報ネットワーク管理運用規程等に基づき、以下のことを禁ずる。

（1）人権の侵害、個人情報の漏洩、第三者を誹謗中傷する行為
（2）著作権等の知的財産権及び肖像権を侵害する行為
（3）公序良俗に反する行為
（4）虚偽の情報を発信する行為
（5）他者の名誉・信用を傷つける行為 、及び プライバシーを侵害する行為
（6）営利目的の行為、及び法令に違反する行為
（7）生徒用セグメント及び無線ＬＡＮセグメントで個人情報等を扱う行為
（8）個人所有のコンピュータ、無線情報端末、教育用コンピュータ等を教師用セ グメントで利用する行為
（9）ネットワーク機器及び各種サービスへのログインＩＤ・パスワード、設定条件 等を第三者へ他言する行為
（10）ネットワーク通信を阻害する行為
（11）ファイル共有ソフトなど、ネットワーク全体を脅かす恐れのあるアプリケー ションソフトのインストール及びそれらを利用する行為
（12）ネットワーク運用に支障を来す恐れのあるアプリケーションソフトのインス トールやサイトへのアクセス
（13）沖縄県教育情報ネットワークのコンテンツフィルタリングを回避する行為
（14）県立総合教育センターの許可なく、ネットワークに無線通信機器を接続し、 無線通信が可能となる環境を構築する行為
（15）沖縄県教育情報ネットワークに県立総合教育センターが指定する機種以外の アクセスポイントを設置し、ネットワークに接続する行為
（16）無線情報端末に設けられた制限を解除し、製造者や管理責任者の意図しない 状態でネットワークに接続する行為
（17）前各号に掲げるもののほか、法令及び社会慣行に反する行為
（18）管理者および情報視聴覚部以外の職員が、サーバー室に立ち入る行為
（19）サーバー室に私物や教材等の荷物を保管する行為
（20）USB メモリ等の可搬記憶媒体を使用する行為
（21）私物パソコン等を校内の教師用セグメントのネットワークに接続行為

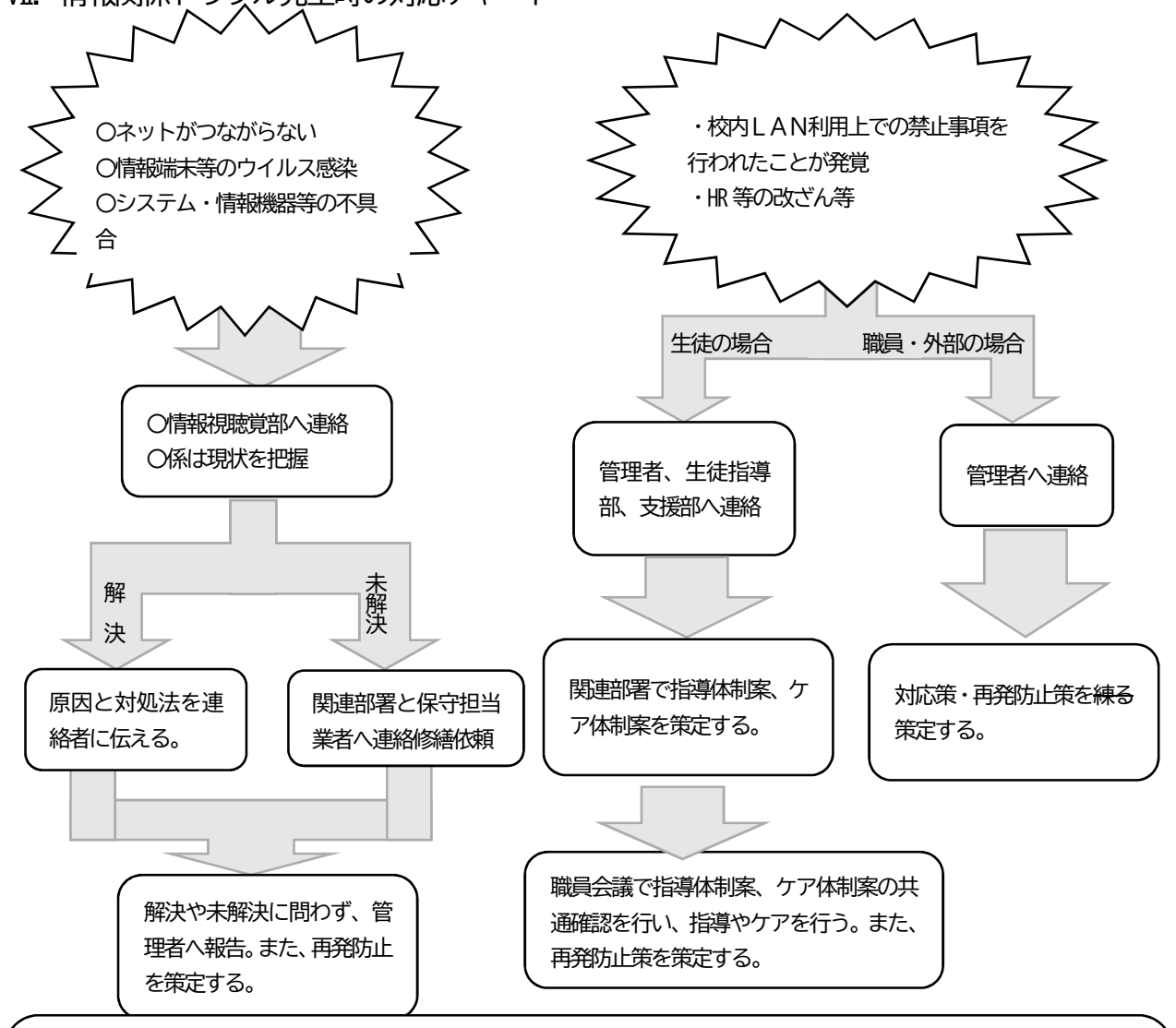
Ⅵ. 情報セキュリティでトラブル発生時の対応

1．以下の場合、各学部の情報視聴覚部に連絡する。情報視聴覚部は状況を確認して改善を図る。改善できない場合は管理者へ報告し、係情報視聴覚部は保守担当業者や各関連部署へ問い合わせをする。

(1) インターネットや校内ネットワークに接続ができなかった場合
(2) 教育支援システムなどでのトラブル発生の場合
(3) ウイルス感染の場合。(感染した情報端末を校内ＬＡＮから抜いてから情報係へ連絡する。)
(4) 情報端末（PC・iPad など）やプリンタの不具合が発生した場合

２．１以外の場合について
(1) 本校生徒でＶの禁止事項が発覚した場合、教頭と生徒指導部・支援部へ連絡し、人権・いじめ防止対策委員会などの関連する委員会を開き、該当者の指導やフォロー及び被害者対応について話し合う。その後、職員会議で指導提案をして承認されてから本校の指導をする
(2) 本校職員でＶの禁止事項が行われたことが発覚した場合、教頭管理者へ連絡する。
(3) 不正アクセスや Web ページ改ざんなどがあった場合上記２の(1)(2)の禁止事項の行為によって情報機器（PC・iPad・プリンタ・ハブ・スイッチングハブ・サーバーなど）やシステムの復元が必要な場合は各情報係へ連絡し、１のような対応をする。
※ 各トラブル解決後、再発防止策を練り策定し、それを全職員に周知する。

Ⅶ. 情報関係トラブル発生時の対応チャート



令和６年度関連部署と保守担当業者
インターネット・ウイルス関連：沖縄総合教育センター　ＩＴ教育班
校内ＬＡＮ：沖縄総合教育センター　ＩＴ教育班、教育庁教育支援課、国建システム　教育支援システム：沖縄総合教育センター
ＩＴ教育班ヘルプデスク　各情報機器(コンピュータ、タブレット、プリンタ等)：各機器の保守担当業者