



夏休みは、いかがお過ごしだったでしょうか？今年の夏は、高知県四万十市で国内観測史上最高の気温41.0度を記録するなど真夏日が続き、体力を消耗する日が多くありました。体調は、いかがでしょうか？先生方には、各種研修への参加や校務、部活動指導等でお忙しい毎日を過ごされて、短い夏だったと思います。また、子ども達は、部活動や様々な体験を通して、ひとまわり成長したことと思います。学校に子ども達の笑顔が帰ってきます。夏休み明けの子ども達一人一人の成長の理解と変化の早期発見をお願いします。

「夏季休業明けの児童・生徒指導について」(平成25年6月13日学教第422号より抜粋)

1 生活態度や生活状況の観察と理解

- ① 教職員の協力体制による情報の共有化
 - ・ 夏季休業明けの児童生徒の生活状況を、担任を中心としながら、全教職員による状況把握と情報の共有化を図ってください。
- ② 児童生徒理解
 - ・ 児童生徒一人一人をしっかりと観察し、夏季休業前との変化を把握してください。
- ③ 不登校の未然防止
 - ・ 夏季休業明けは、生活状況の変化により、不登校になるケースも考えられることから、早期発見、早期対応に努めてください。

2 学校生活への適応への援助

- ・ 児童生徒の中には、夏季休業明けに学校生活に適応できない者が増加する傾向にあることから、家庭やサポートセンターなどとも十分に連携を図りながら、児童生徒の生活のリズムを整えさせてください。

3 配慮を要する児童生徒に対する早期対応

- ・ 児童生徒の心理的な状態等は、日常生活の乱れや態度の変化となって現れやすいことから、これらを早期に発見し、以下の項目に基づいた適切な指導・援助をしてください。

- ① 保護者との情報の共有化及び相談
- ② 面接指導や個別指導の実施
- ③ 関係教職員、スクールカウンセラー、関係機関等と連携した組織的な対応

4 学業指導の充実

- ・ 「学業指導の充実に向けて」(H24.3 県教育委員会)を参考にするなどして、溶け込みやすい雰囲気づくり及び居心地のよい環境づくりなど学級経営の改善を図りつつ、意欲的に学習活動に取り組める学業指導の一層の充実を図ってください。



【9月の予定】

※時間のみ記載の会の場所は石橋庁舎です。

日	月	火	水	木	金	土
1	2 小学校授業再開 中学校授業再開	3 初任研AC S&U 南河中	4	5 初任研BD 市教頭研修会 14:00~	6 下地区中学校新人水泳 大会 S&U 国分寺西小	7
8	9 市道徳教育研修会 国分寺西小 13:45~ 教職・養教・栄養職員2 ~5日目研修 総教センター	10 学習意欲部会 15:30~ S&U 石橋小	11 S&U 古山小 教育委員学校訪問 (祇園小) Jアラート試験放送 11:00、11:30	12	13 S&U 薬師寺小	14 石橋中運動会 国分寺中運動会
15	16 敬老の日 	17	18 要請訪問吉田東小 要請訪問南河内中 要請訪問南河二中 S&U 国分寺小	19 下地区中教研 B	20	21 国分寺東小運動会 市小中学校音楽祭 石橋中 秋の交通安全運動 ~30日
22	23 秋分の日 	24 下地区学校音楽発表会 (小学校) 栃木市文化会館 S&U 吉田西小	25 要請訪問細谷小 市小中校長定例会 9:00~ 学力向上部会(小国) 15:30~	26 教育委員学校訪問 (緑小)	27 下地区中学校新人大会	28 薬師寺小運動会 吉田東小運動会 吉田西小運動会 国分寺西小運動会 下地区中学校新人 大会
29 下地区中学校新 人大会	30 下地区学校音楽発表 会(中学校) 栃木市文化会館 学力向上部会(中教) 15:00~					

～無線 LAN の仕組みについて (その2)～

今月は無線 LAN のセキュリティについてです。許可されたパソコン以外が接続できないように、以下のような仕組みがあります。

(1) セキュリティ方式：無線 LAN 子機の認証を行う方式

セキュリティ方式	暗号化キー管理方式	暗号化方式	改ざん検知領域	改ざん検知アルゴリズム
WEP		WEP	ICV	CRC32
WPA	PSK/EAP	TKIP/AES)	MIC	Michael
WPA2	PSK/EAP	(TKIP/AES	MIC	CCMP

(2) 暗号化キー管理方式：通信内容を暗号化するキーの生成方式

暗号化キー管理方式	認証サーバ(RADIUS 等)	暗号化キー生成	暗号化キー生成元	Key の生成単位
PSK (パーソナルモード)	不要 (暗号化キーはユーザ管理)	固定	パスフレーズ (固定)	実装依存 (アクセスポイン ト単位で共通が多い)
EAP (エンタープライズモード)	必要 (暗号化キーはそのサーバで一括管理)	動的 (セッション毎変更)	乱数	ユーザ (又は端末) ごとに 個別

(3) 暗号化方式 (暗号化プロトコル)：通信内容を暗号化する方式

暗号化方式	暗号化アルゴリズム	暗号化キー長	IV	特徴
WEP	RC4	64bit/128bit	24bit	市販 PC を使用して数秒で解読可能
TKIP	RC4	128bit	48bit	暗号鍵を一定時間毎に自動的に更新する。ソフト ウェア処理のため処理スピードの低下がおこる。
AES	AES(Rijndael)	128/192/256bit	48bit	ハードウェア処理のため、既存の機器の一部では 対応できない

IV(初期値ベクトル)：暗号化キーを生成する乱数列。同じ暗号鍵でストリームを生成しても毎回異なるストリームを生成するのが必要。受信者がその暗号を解読する際に必要なので送信側で渡される。

RC4ストリーム暗号 (平文をビット単位あるいはバイト単位などで逐次、暗号化する暗号)

AESブロック暗号 (平文を128ビットの固定長のブロックに分割して暗号化する)

上記のように、WEP→WPA→WPA2 と安全度は上がり、WEP→TKIP→AES と安全度は上がります。認証サーバを用意できれば PSK より EAP のほうが安全度は上がります。また、MAC アドレスフィルタリングと SSID ステルスは詐称やクラッキングにより抜け道があるので十分な対策ではありませんが、設定したほうが安全です。

無線 LAN はどこでも LAN に接続できて便利な反面、設定が分かると、誰でも校外からでもアクセスできてしまうので、有線接続に比べるとセキュリティに注意する必要があります。

※MAC アドレスフィルタリング、SSID ステルス、改ざん検知領域、改ざん検知アルゴリズムについては紙面の都合上割愛しました。詳しいことは情報教育アドバイザーまでお尋ねください。