SCIENCEPARK

文章番号：SP1802-S01

NonCopy2による
教育セキュリティガイドラインへの
対応のご提案

サイエンスパーク株式会社

1．ガイドラインの背景

SCIENCEPARK

文科省が教育の情報化を進める中、取り組みを阻害しかねないインシデントが発生。以下の緊急提言が発せられ、セキュリティガイドラインの整備へつながった。

教育情報セキュリティのための緊急提言

1．情報セキュリティを確保するため、校務系システムと学習系システムは論 理的又は物理的に分離し、児童生徒側から校務用データが見えないようにす ることを徹底すること。

2．児童生徒が利用することが前提とされている学習系システムには、個人情 報を含む情報の格納は原則禁止とし、個人情報をやむを得ず格納する場合に は、暗号化等の保護措置を講じること。

3．各学校において情報セキュリティの専門家を配置することが困難な現状を 踏まえれば、重要な個人情報を扱う校務系システムは、教育委員会が管理も しくは委託するセキュリティ要件を満たしたデータセンター（クラウド利用 を含む）で一元的に管理すること。

4．校務系ならびに学習系システムにおいても、教職員や児童生徒の負担増に ならないよう配慮しつつ、二要素認証の導入など認証の強化を図ること。

5．セキュリティチェックの徹底の観点から、システム構築時及び定期的な監 査を実施すること。

6．セキュリティポリシーについて、実効的な内容及び運用となっているか検 証を行うこと。その際、アクセスログの 6 か月以上保存、デフォルトパスワ ードの変更等について確認すること。

7．教職員の情報セキュリティ意識の向上を図るため、全学校・全教職員に対 する実践的な研修を実施すること。

8．情報セキュリティの強化の観点から、教育委員会事務局への情報システム を専門とする課・係の設置や首長部局の情報システム担当との連携強化等、 教育委員会事務局の体制を強化すること。

２．要はなんなのか

緊急提言やガイドラインの目的は、

機微情報を外に出さないこと

3．学校におけるインシデント

SCIENCEPARK

学校における情報セキュリティインシデント

4

不適切なネットワーク接続、ID・パスワード管理が原因の事案

○佐賀県における教育情報システムからの情報流出

平成２８年１月、佐賀県において、教育情報システム（校内システム及び教育委員会が管理する教育情報システム）に対する不正アクセスにより、公立中学校・高等学校の生徒ら１万人超（全９校）の個人情報（氏名・住所・成績情報・指導記録等）が外部に流出。校務用サーバと学習用サーバをつなぐネットワークのID・パスワードの管理が不適切であった。

○中学校で生徒が学内ネットワークに不正アクセス

中学校において、生徒が学内のパソコンネットワークに不正にアクセスし、同級生ら約２００人の名前や成績、住所などの個人情報を入手。生徒は学内のパソコンから校務用サーバーに、校長の名前をパスワードに使って侵入できることに気付き、データを取得。

○工業高校における個人情報流出問題

工業高校において、進路指導部内のパソコンに保存されていた卒業生304人の氏名や成績、進路先、他校の卒業生3人の調査書の内容がインターネット上に流出。

進路指導部内のパソコンは教職員が使うパソコンとＬＡＮで接続されていたほか、生徒が使う教育用パソコンともLANで結ばれており、自習中の男子生徒が自分のホームページに情報を転送。

「2020年代に向けた教育情報化に関する懇談会」スマート・スクール構想WG第三回山崎委員発表資料

2017年10月19日教育委員会対象セミナー in 大阪
文部科学省生涯学習政策局情報教育課 松本課長補佐講演資料

大規模インシデントはネットワークから流出している

４．なにをすべきか

標的型攻撃、ランサムウェア、内部犯行、いたずら

漏えいの原因は様々ですが、情報の流出経路は

デバイス　or　ネットワーク

のどちらかです

これらの経路に対していかに適切に対処するかが
情報漏洩対策の要点となります

5．NonCopy2による課題解決

NonCopy2で対応可能な項目

①ファイルの持ち出し管理
（デバイス制御）

②機微情報の保護（暗号化）

③ネットワーク分離

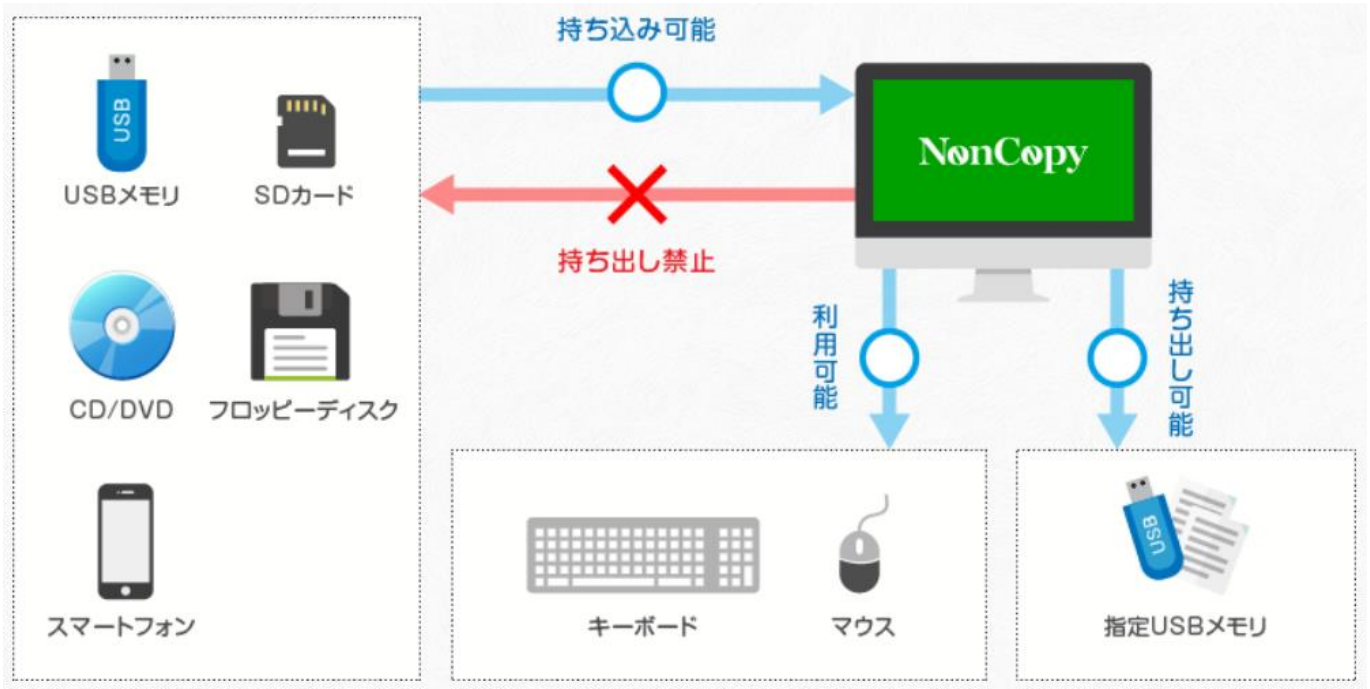
◎メリット
・**1つのソフトで複数の課題**に対応
・導入製品を減らすことで、
コストと運用負担を軽減

セキュリティの投資は抑えて、本来やるべき教育ICT化に
予算を向けていただく

6．ファイルの持ち出し管理

6．ファイルの持ち出し管理

外部記憶媒体へのコピーを禁止



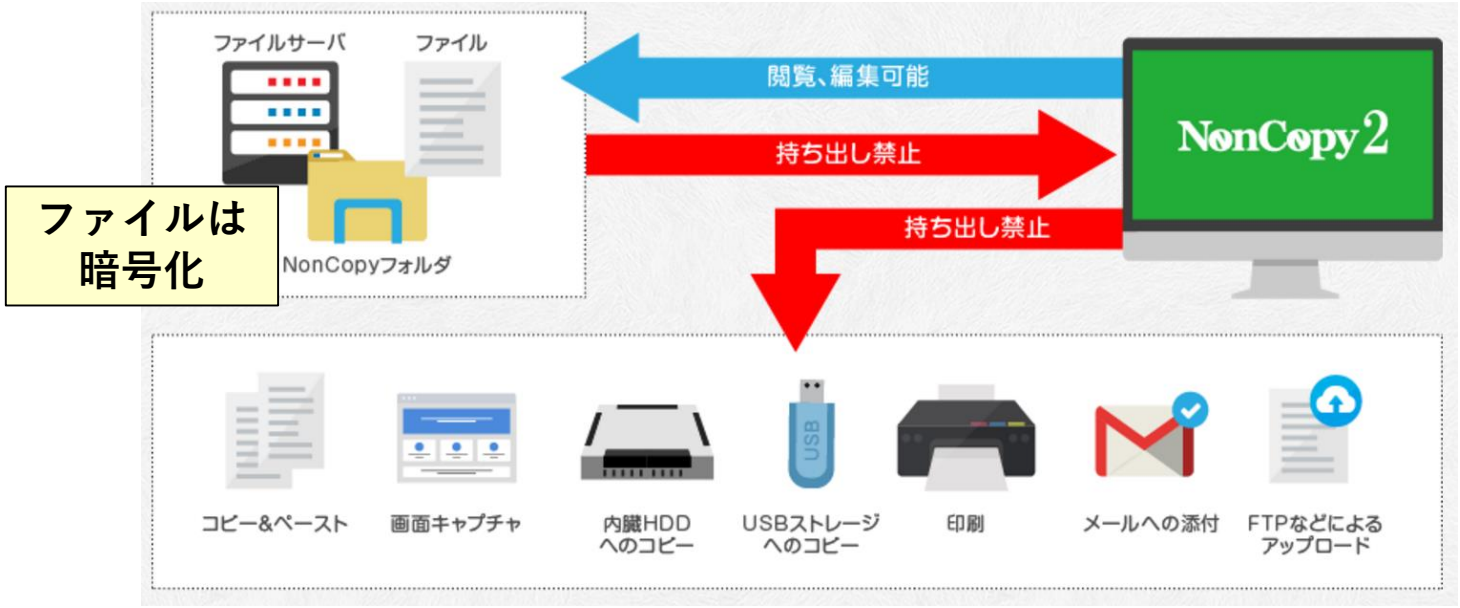
■特長
・ワークフローによる持ち出し管理
・許可デバイス/許可WiFiの登録

・持出しのログ
・持出ファイルのシャドウィング
・分離したNW間のデータ移動

７．機微情報の保護（暗号化＋α）

7．機微情報の保護（暗号化＋α）

保護フォルダに保存したファイルは暗号化され、NonCopyフォルダからデバイスやネットワークへの持ち出しを禁止します。暗号化されているため、不正アクセスを受けてもデータを見られる心配はありません。



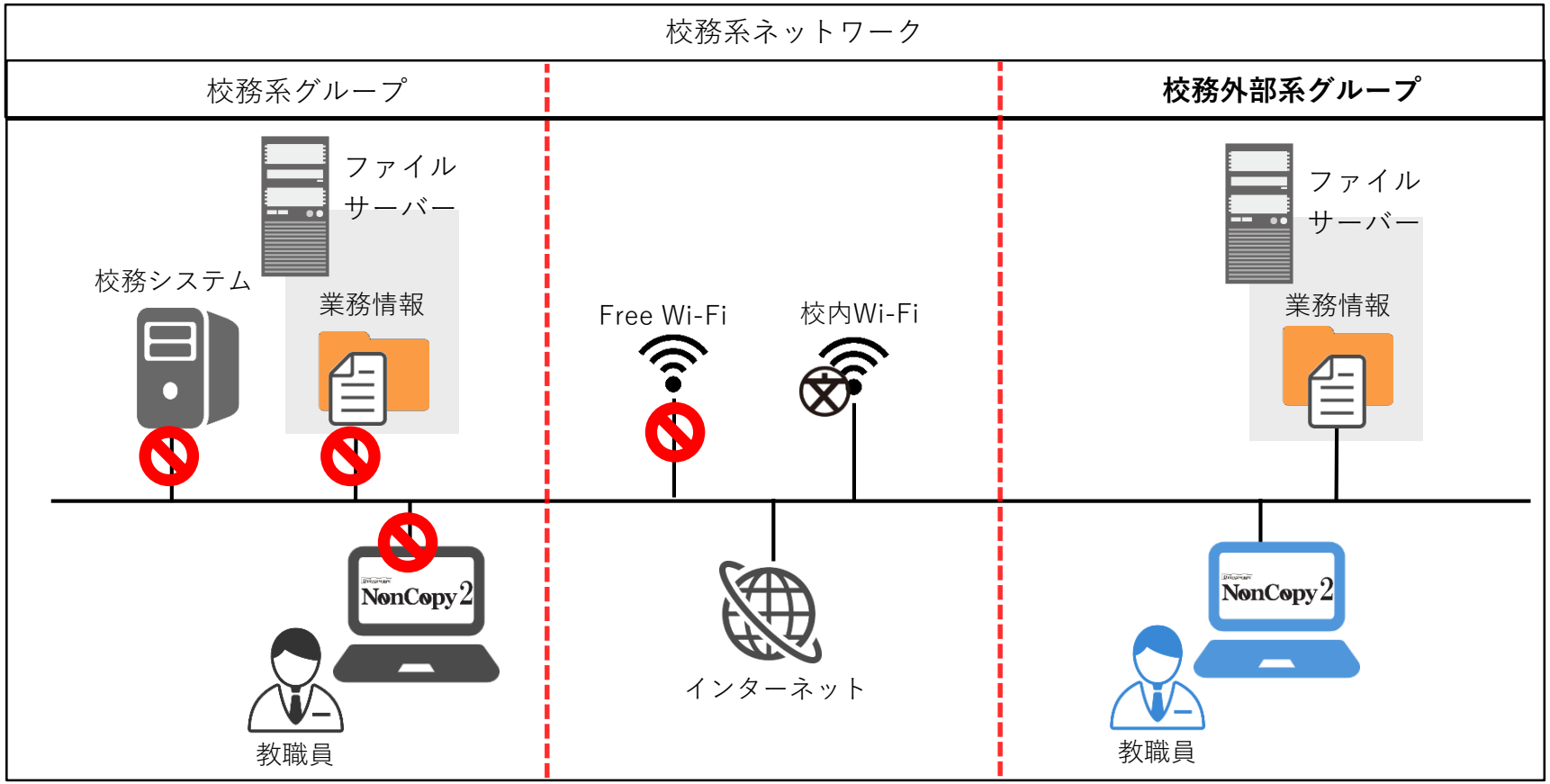
暗号だけでは不十分
人やマルウェアにデータを持って行かせません。

8．ネットワーク分離

8.1　分離案１（PCに余裕がある場合）

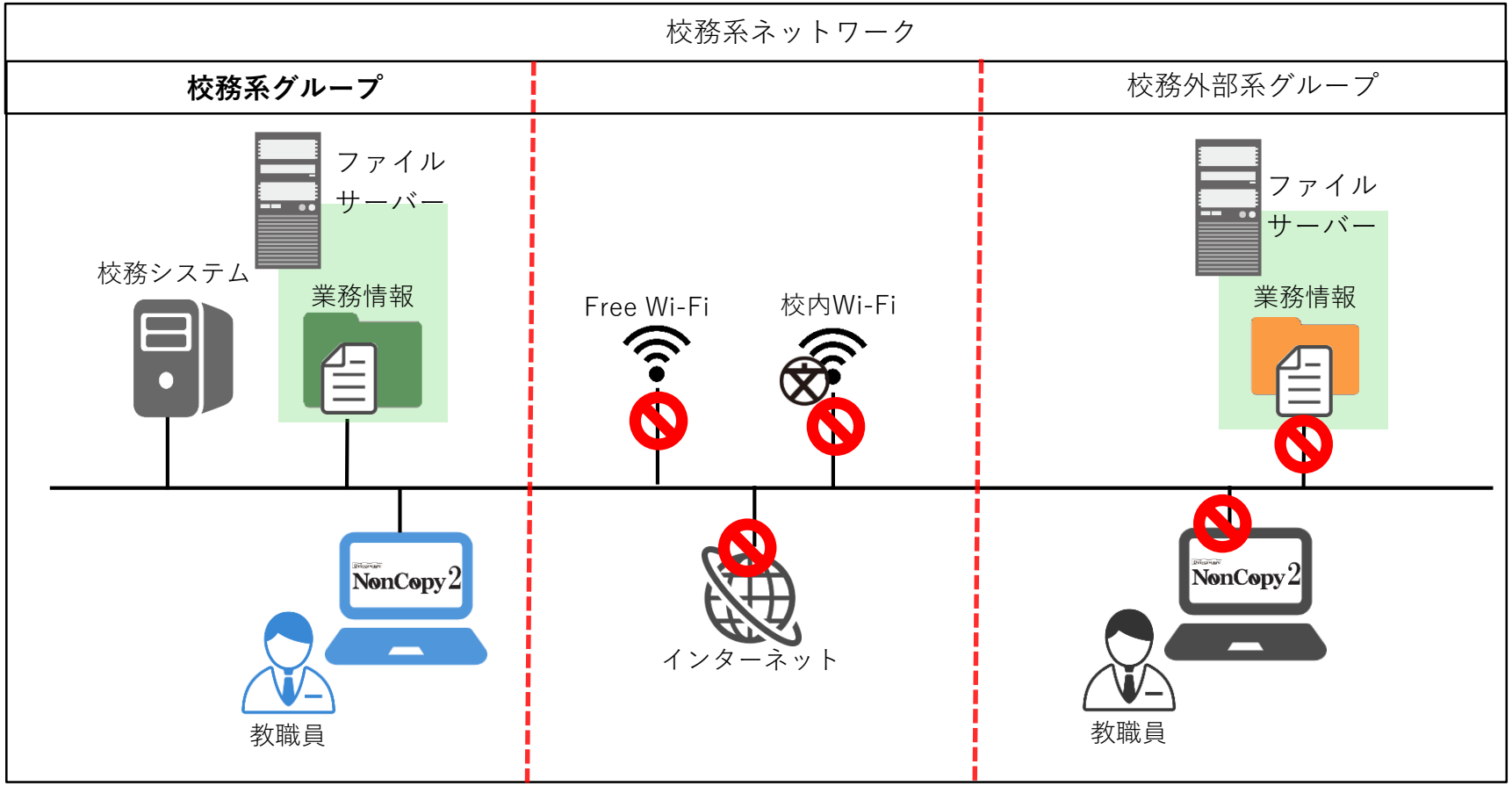
PCやファイルサーバーをグループ分けし、NonCopy 2のネットワーク接続ホワイトリスト機能により、相手グループへのネットワーク接続を禁止する。

■制御イメージ：**校務外部系グループ**のネットワークポリシー



8.1　分離案１（PCに余裕がある場合）

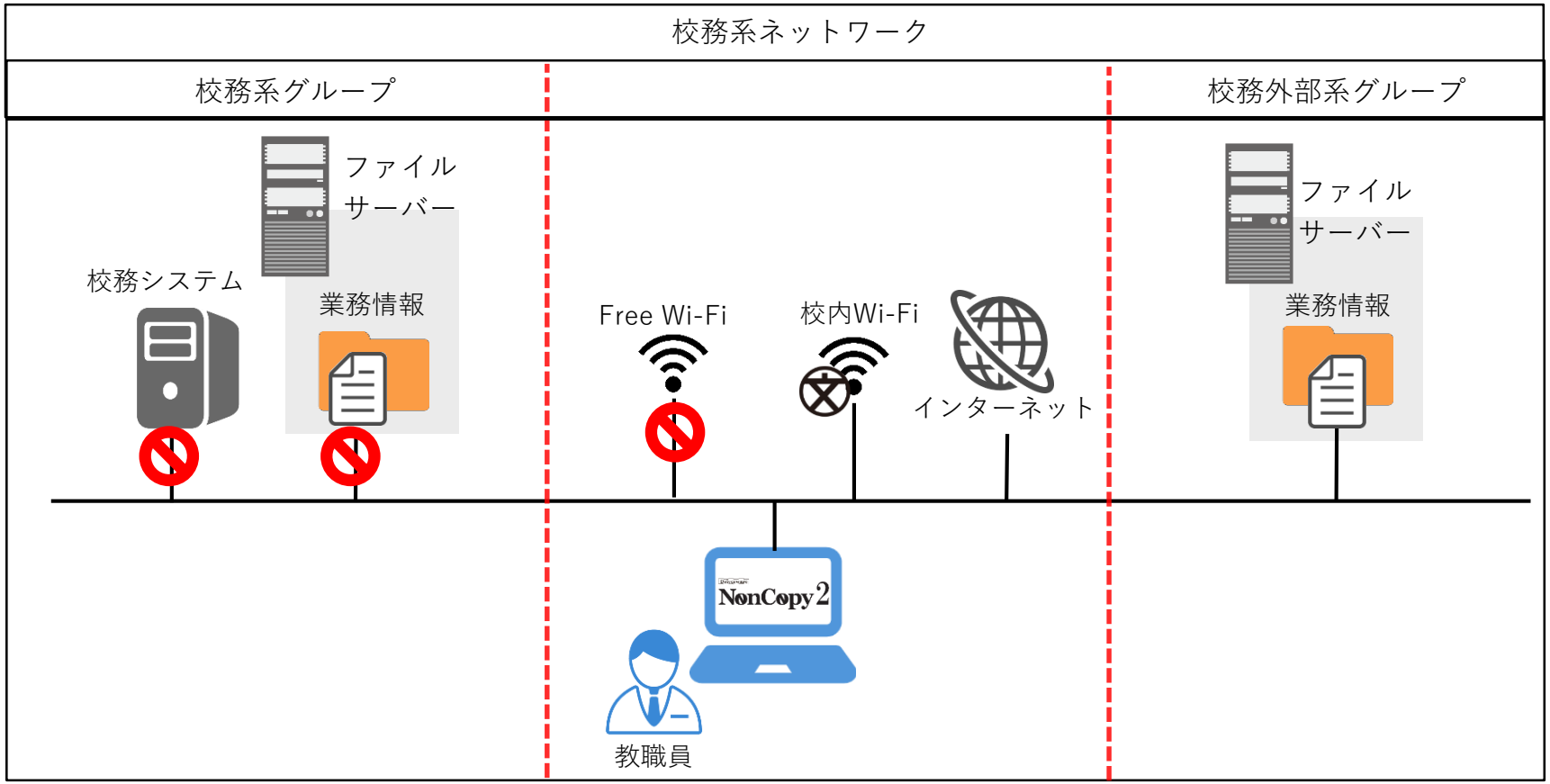
■制御例：**校務系グループ**のネットワークポリシー



8.2　分離案２（PCに余裕がない場合）

NonCopy 2は機密情報にアクセスする際、セキュリティモードへ切り替えを行います。通常時、セキュリティモード時それぞれにネットワーク接続先をホワイトリスト登録することで、機密情報アクセス時のインターネット遮断を行います。

■制御イメージ：**通常時**のネットワークポリシー



8.2　分離案２（PCに余裕がない場合）

■制御イメージ：**セキュリティモード時**のネットワークポリシー