V-Campus 7th 更新
ー p3.ネットワークセキュリティ ー

1. 概要

p３.ネットワークセキュリティでは、多様化するセキュリティ脅威への強化と合わせて、多要素認証やVPNからのアクセス制御が対応可能な提案を募集した。

また授業内での動画配信サービスやGoogleやOffice365のクラウド通信による通信帯域増加にも対応できることやｐ７.監視との親和性も評価条件とした。

2. システム更新のポイント

(1).基本対策の見直し・強化

① IPsec VPNの導入
② IPS（Intrusion Prevention System） による不正通信の検知・遮断
③ WEBアクセス制御
④ SSL通信の複合検査
⑤ 統合LOG保全（ネットワーク機器、サーバ機器すべてのログを保管）
⑥ 相関分析による不正通信の検知

(2).強化対策

① 多要素認証との連携
② 利用者ごとのVPNアクセス制御
③ 新座キャンパスのプライベートIP化

3. ｐ３.ネットワークセキュリティまとめ

今回の更新では、最新のセキュリティ脅威への対策をとりつつ、プライベートIP化など本学での長期の課題にも対応した。

ただ、日進月歩で変化する脅威に対して、今後も継続した情報収集を図りながら将来を見据えた対策を講じていく。