

V-Campus 6th 更新

－ p3.ネットワークセキュリティ －

1. 概要

p3. ネットワークセキュリティでは、V-Campus 5th にて構築したネットワークセキュリティに対し、さらなる強化を要求した。また新たに、クラウド PROXY の導入による Web アクセス対策の強化と、SOC (Security Operation Center:以降、SOC と表記) サービスによる分析を可能とした。

今回の更新では、7社の提案があったが、SOC サービスを要件とすると費用が跳ね上がる事となり厳しい状況であったが、選定ベンダーに於いては柔軟な対応が可能との事で採用した。

2. 更新のポイント

(1). 基本対策の見直し・強化

- ① Firewall ポリシー見直し
- ② IPS (Intrusion Prevention System) による不正通信の検知・遮断
- ③ 多重構成による検知率向上
- ④ WEB アクセス制御
- ⑤ SSL 通信での複合化 (暗号化された不正な通信を遮断)

(2). 強化対策

- ① 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)
- ② 相関分析による不正通信の検知
- ③ SOC 導入 (専門家による分析)

3. p3. ネットワークセキュリティのまとめ

今回の更新では、セキュリティ強化を念頭に構築を進めてきた。しかしながら、世間一般では情報漏洩問題が騒がれ後を絶たない。V-Campus 6th Stage においても、セキュリティ面の課題がまだ残るものの、V-Campus 5th に比べてかなりの強化を行っている。セキュリティについては、今後も引き続き検討を実施していく。

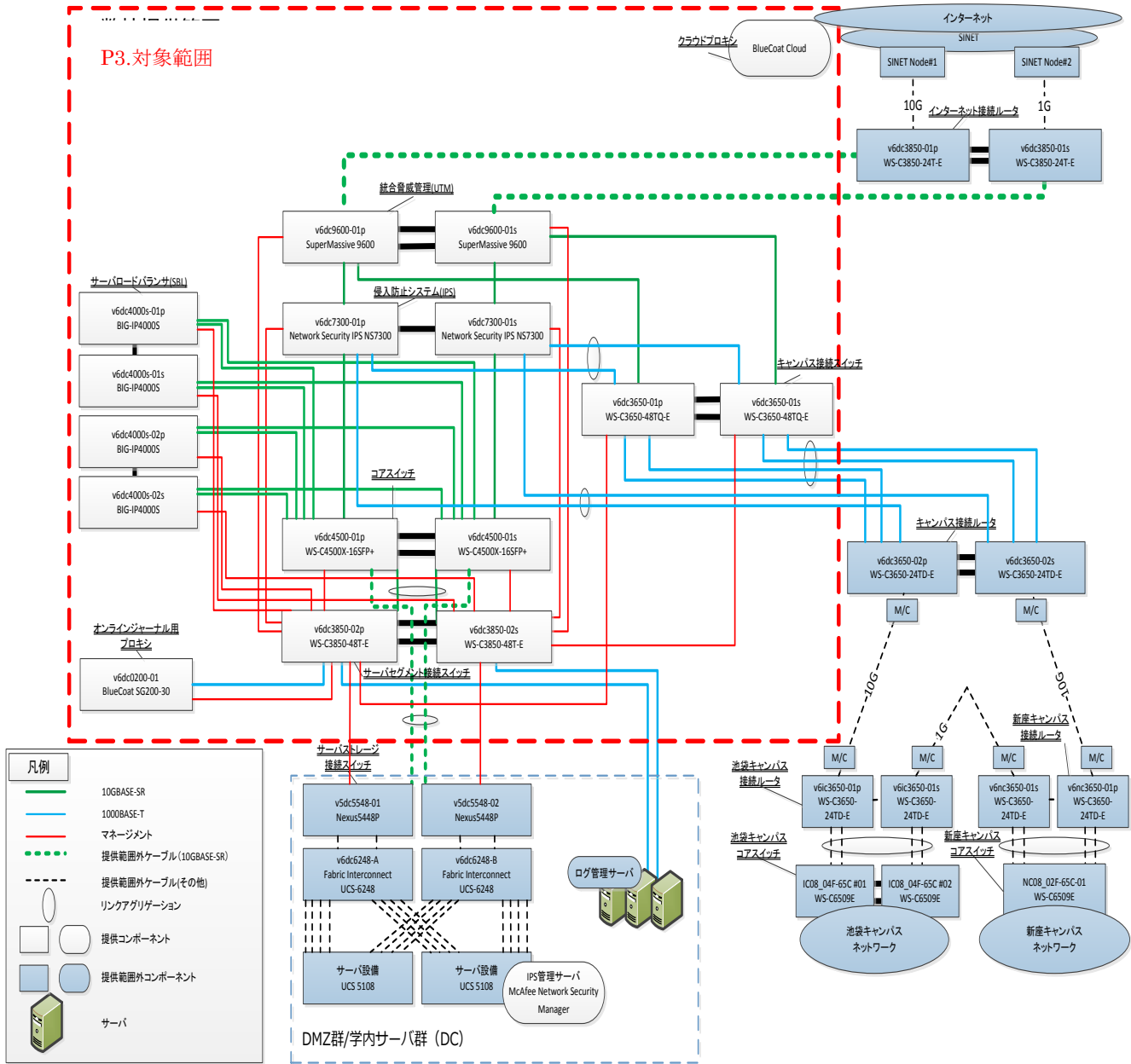


図 1: ネットワーク 概要図