平成18年2月22日
平成17年度第6回情報ネットワーク部会資料より

クラッキング被害発生時の対処ルール

1.電源を入れたままネットワークからはずし,生きている状態でセンター職員が事実の確認と可能な限りの証拠を集める.

2.証拠を集めたら電源を切り,該当マシンのDiskをすべて外す.そのDiskのインタフェース部にはセンターの封印シールを貼り,証拠保全のために再利用できないこととする.

3.該当するネットワークには,今後の防止のため,センター側で監視機材を設置し,ネットワークの監視を強化することとする.

Q.被害箇所の監視期間,内容,開始時期は?
A.監視期間は被害内容と攻撃相手の出方によるが,長期的になります.
ディスクの保管期間は2年間とします.
開始時期は,必要に応じてすぐに行います.

Q.被害にあったサーバディスクが退官された教員のディスクの場合はどうするのか?
A.センターで引き取ります. それ以外は該当教員が保管します.

Q.残しておくべきログを周知すべき.
A.telnet,ssh,mail,WWW ,その他の公開サービス(学内向けおよび学外向け)を行っているサーバ類のログは取っておくべき.