KAINSにおけるセキュリティ対策

～ 2010年のセキュリティインシデントと今後の対策 ～

総合メディア基盤センター　北口　善明

1　はじめに

ネットワークが欠かせない存在になってきている今日においては，その運用に置いてセキュリティ対策の重要性も増しています．金沢大学のKAINS（金沢大学学術統合ネットワーク）においても，セキュリティに対する様々な取り組みを行っています．代表的なものとしては，ウィルス対策ソフトの配布やファイアウォール機器でのアクセスログ収集，P2Pファイル共有通信の監視などがあります．

本稿では，本学で2010年に発生したセキュリティインシデントを中心に，その攻撃による影響と本学におけるセキュリティに対する取り組みについて報告します．

2　SPAMメールの不正中継攻撃

2010年8月，本学内に設置されていたメールサーバ（SMTPサーバ）が学外からのSPAMメールの踏み台とされ，金沢大学内部から外部に対して大量のSPAMメールを送信するメール不正中継攻撃[1]が発生しました．（図1）．このインシデントが発生したのは夏季一斉休暇の直前辺りからで，本学の送信用メールサーバにおける処理負荷も高まり，メール配信に遅延が生じる結果となりました．

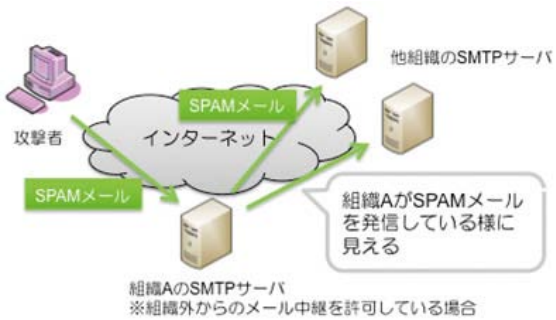

図1　メール不正中継攻撃

ただ，本件の原因究明に至ったのが休暇明けであったため，約一週間に渡ってSPAM攻撃者として金沢大学が外部から認知される結果となってしまいました．この結果，学外ドメイン（yahoo.comやhotmail.comなど）からのSMTP接続が拒否されることとなり，送信用メールサーバにおいてメールが大量に蓄積され，学内全体のメール遅延に繋がりました．

本件の対策として，次の三点の作業を実施しました．まず，踏み台となったサーバへの外部からの接続をファイアウォール機器において切断し，SPAM送信を停止させました．次に，送信用メールサーバを新たに設置し，キューに溜まったSPAMメールの削除とメールの再配送を実施しました．最後に，今回の件で送信用メールサーバがSPAM配信のブラックリストに載ってしまいましたので，ブラックリスト管理者およびメール受信を拒否しているドメインに対して問題点が改善された旨の報告を実施し，ようやく正常な運用に戻すことができました．

このように，SPAMメールの踏み台となると，外部組織に対して多大な迷惑をかけるとともに，組織としての信頼を落としかねません．メールサーバを運用する際には，メール転送設定を学内からのみ許可するといった対策が最低限必要と言えます．

3　附属学園におけるウェブページ改竄

2010年9月，本学の附属校園のウェブページにて不審なファイルが公開されていることが発覚しました．このインシデントが発生した段階で，直ちに該当サーバをネットワークから隔離し，HDD内に残されたアクセスログ解析を行いました．

調査の結果，該当サーバで利用されていたCMSにおけるファイルアップロードの仕組みに脆弱性があることが判明しました．具体的には，学内で利用されていたファイルアップロードの仕組みが外部からも利用可能になっていた点が問題で，この仕組を攻撃者に利用されることとなりました．幸いにも管理者権限を奪取される結果とはならず，不正なファイルが置かれただけで済みましたが，万全を期すためにサーバは新規に構築してコード修正した状態で復旧しました．

公開用ウェブサーバは不特定多数からのアクセスを受け入れる必要があるため，ファイアウォール機器などによるアクセ

1. メール不正中継攻撃：攻撃者が第三者のSMTPサーバを解してメールを送信する攻撃．

ス制限は難しいものになります．そのため，各サーバにて利用するウェブアプリケーションにおいて，個々にアクセス制限を設定するなど，慎重な対策が求められます．

4 金沢大学トップページへの DDoS 攻撃

2010 年 9 月下旬，ウェブページ改竄騒動に引き続き，本学のメインウェブサーバが DDoS 攻撃[2]を受けました．この攻撃により，一時的に本学サイトの閲覧がしにくくなる状況に陥りました（図 2）．

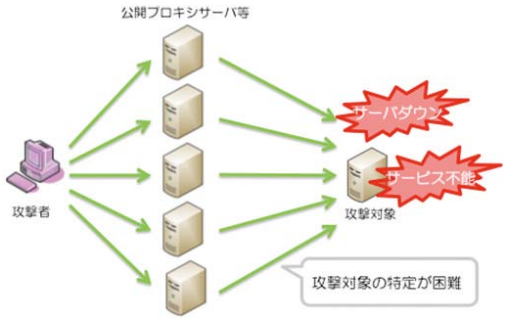

図 2　DDoS 攻撃

今回の DDoS 攻撃の解析を行ったところ，9 月 18 日の 16:11 から 1 回目の攻撃が始まり，16:13 には 1 分間のアクセス数が 19,898 にも達していたことが分かりました．また，2 回目の攻撃は 9 月 19 日の 20:17 から始まり，約一日の期間に渡ってサーバが高負荷な状態となりました．

DDoS 攻撃は，送信元が多数になるためファイアウォール機器における防御が難しい攻撃です．実際に様々な国と地域から 4000 以上の送信元としてアクセスされる攻撃でした．また，送信元に利用される端末の多くは公開プロキシサーバ[3]であり，攻撃者自身の特定も困難となります．

5 金沢大学におけるセキュリティ対策

今回紹介したようなインシデントの発生を受けて，以下のような対策を実施もしくは今後導入予定としています．

■公開サーバに対する脆弱性検査

外部公開を実施しているサーバに対して脆弱性検査を実施しました．この脆弱性検査は今後定期的に実施し，公開サービスにおける脆弱性の早期発見を目指します．また，ウェブアプリケーションにおける脆弱性検証も検討中です．

■外部公開申請サーバ／サービスの見直し

外部公開を行う際にはサーバ管理者による申請作業を必須として運用していましたが，利用期間が曖昧でありました．そこで運用形態を見直し，今後はすべてのサービスを年度末までの利用とし，利用延長の際には簡単な手続きを必要とする運用にする予定です．

■UTM 機器の導入

来年度に予定している基幹ネットワークの更新において，UTM（Unified Threat Management）機器の導入を予定しています．UTM はファイアウォール機能にアンチウィルスや不正侵入検知機能などを統合管理するものです．様々な脅威におけるデータベースを利用することで，DDoS 攻撃なども検知・防御することが期待できます．

■MAC アドレス認証による接続機器管理

今回紹介した外部からの脅威に対するものではありませんが，各部局内に設置されているフロアスイッチにおいて MAC アドレス認証による接続管理を検討しています．学内の全ての機器を一斉に置き換えることは困難でありますので，部局毎に順次導入することにしています．これにより，部外者のネットワーク接続を排除でき，また，接続機器の利用ユーザが明確になることで，内部ネットワークのセキュリティが向上します．

6 おわりに

ネットワークのセキュリティは，ファイアウォール機器などを用いたゲートウェイセキュリティモデルだけでは万全とは言えません．ネットワークを守るためには各端末，特に外部公開しているサーバにおけるセキュリティ対策を十分に実施することが重要です．

総合メディア基盤センターでは，KAINS の運用におけるセキュリティ向上を目指し，今後，先に挙げた様な外部からの攻撃に対する取り組みを強化します．また，併せて内部利用のセキュリティ強度を高める対策も検討しています．ただし，セキュリティの向上のためには利用者の意識改善も必要となります．センターの取組みに対してご理解いただけるように，利用者に対しての啓蒙活動も併せて実施していきたいと考えています．

2. DDoS（Distributed Denial of Service）攻撃：複数の端末から特定のサーバに対して大量の通信を行う攻撃．
3. 公開プロキシサーバ：不特定多数に対して利用を公開している通信の代理サーバ．匿名プロキシとも言う．