2003－DSM－30　(4)
2003／9／26

大学におけるインシデント対応の一事例

田村直之[1]　鳩野逸生[1]　伴好弘[1]
{tamura,hatono,ban}@kobe-u.ac.jp

最近のインターネットの普及に伴い，情報セキュリティ・インシデントの発生件数も増加の一途をたどっている．

そのようなインシデントを起こさないためには，セキュリティ・ポリシーの策定やそれに基づいた監査・運用体制を確立し，厳格に実行することが必要なのはもちろんであるが，一旦インシデントが起こった後の対応をどのように行うかも非常に重要である．

本稿では，著者らの大学で実際に起こったインシデントとその対応の経緯について，一事例として紹介を行う．

A CASE STUDY OF HANDLING INCIDENT AT A UNIVERSITY

Naoyuki Tamura[2]　Itsuro Hatono[2]　Yoshihiro Ban[2]
{tamura,hatono,ban}@kobe-u.ac.jp

The rapid spread of the Internet also increases the number of security incident.

In order to prevent such incident, important points are, of course, the establishment and strict enforcement of security audit/management system based on a security policy. However, it is also very important to handle the incident properly after it occurred.

In this paper, we report a case study of a security incident and our response happened at the authors' university.

[1] 神戸大学 学術情報基盤センター
[2] Information Science and Technology Center, Kobe University

1　はじめに

最近のインターネットの普及に伴い，情報セキュリティ・インシデントの発生件数も増加の一途をたどっている [1].

そのようなインシデントを起こさないためには，セキュリティ・ポリシーの策定やそれに基づいた監査・運用体制を確立し，厳格に実行することが必要なのはもちろんであるが，一旦インシデントが起こった後の対応をどのように行うかも非常に重要である [2, 3, 4].

本稿では，著者らの大学で実際に起こったインシデントとその対応の経緯について，一事例として紹介を行う．なお，本稿の内容は，実際にインシデント対応に当たった著者らがまとめたものであり，すべての文責は著者らにある．

2　経緯

以下は，実際に起こった経緯について時系列順に並べたものである．

2003 年 6 月 17 日 (火)

(1) 本学で運用していた掲示板システムからのポートスキャンが検出された，とのメールが NASA Ames Research Center から学術情報基盤センター (以下センター) 宛に届いた (午前 00:00).

(2) 5 分以内にスイッチの設定を変更し，掲示板システムと学外との通信遮断を行った.

(3) 掲示板システムの使用している 443 番ポート (https) 以外に，120 番ポートがバックドアとして開いていることを確認し，学外から学内全計算機の 120 番ポートに対する通信を遮断した (30 分以内).

(4) 掲示板システムを設置してあるサーバ室に出向き，ネットワークケーブルを外した (1 時間以内).

(5) 掲示板システムの管理者が不在のため，ログインできず，またリブートすれば実行中のプロセス情報が取り出せないため，これ以上の調査は不可能と判断し，翌朝まで待つことにした.

(6) 早朝より調査を開始し，OS は Linux，Web サービスシステムは Apache 1.3.20, OpenSSL 0.96b で，既知のセキュリティホールのあるバージョンであること，また海外からの不正侵入の痕跡を発見した．さらに，約 25800 名のログイン ID と暗号化されたパスワード (.htpasswd ファイル) が読み出せる状態になっており，それらうち 22721 名のパスワードがセンターのパスワードと同一であることを確認した．また，その他の個人情報等が保存されていないことを確認した.

(7) 午後までに，全パスワードの変更と情報の前面公開を行う方針をセンターとして決断した．また学外からのメール取り込みの制限 (POP3, APOP 接続の制限) を行った．なお，学外からセンターへのログインおよびメール送信 (SMTP) は従来から制限されている.

(8) 並行して，パスワード一括変更までのスケジュールの大枠を作成した．新パスワードの通知書の印刷と送付に時間がかかること，パスワード一括変更処理にかなりの時間がかかると予想されること，したがって授業への影響を最小にするために一括変更作業は土日に行わざるを得ないこと，等からパスワード一括変更作業は 7 月 5, 6 日とし，6 月中に各ユーザでパスワードを変更してもらい，6 月中にパスワード変更しなかったユーザに対してのみ，強制的にパスワード変更を行うことにし，以下のような予定を立てた.

    6 月 18–30 日: 各ユーザによるパスワード変更．パスワード一括変更のための準備.
    7 月 1–4 日: 各ユーザによるパスワード変更停止．新パスワード通知書の印刷および発送準備.
    7 月 5–6 日: パスワード一括変更作業.
    7 月 7 日–: 新パスワード通知書の配布.

(9) 13:30 大学執行部に経過報告し，上記方針の了承を受けた．同時に，ユーザへの「パスワード変更のお願い」，学外への公開文書等の原案を作成した.

(10) 14:45 学内の全計算機の管理者に，経過報告と注意喚起およびパスワード変更の呼びかけのメールを送信した．
(11) 16:00 文部科学省および IPA(情報処理振興事業協会) へ報告を行った．
(12) 17:30 NASA Ames Research Center にお詫びのメールを送信した．
(13) 19:00 「パスワード変更のお願い」の最終案および英語版を作成した．
(14) 21:00 センター Web ページにパスワード変更のお願いを掲載した．

2003 年 6 月 18 日 (水)

(15) 「パスワード変更のお願い」の各学部での掲示を依頼し，神戸大学のトップページへの掲載を決定した．
(16) 学外からメールが読めないとの苦情が増える．
(17) 学外からのパスワード変更，メール転送設定，APOP 設定を可能にする認証 Proxy システムの構築を開始した．これらは従来は学内からのみ利用可能だった．

2003 年 6 月 19 日 (木)

(18) 学長への経過報告を行った．
(19) パスワード一括変更作業スケジュールの第一案を作成した．
(20) 侵入元と思われる海外の計算機のネットワーク管理者にメールで調査を依頼した．

2003 年 6 月 20 日 (金)

(21) パスワード一元管理システムを開発した業者 (以下業者 A) の担当者とパスワード一括変更作業スケジュールについて打ち合せを行った (注: 業者 A は今回のインシデント発生原因の当事者ではない)．
(22) 学外からのパスワード変更，メール転送設定，APOP 設定を可能にする認証 Proxy システムの運用を開始した．
(23) 神戸大学の学生新聞からの取材があった．
(24) パスワード一括変更プログラムの作成を開始した．

2003 年 6 月 23 日 (月)

(25) パスワード一括変更作業スケジュールをセンター Web ページに掲示した．
(26) パスワード一括変更プログラムの第一版が完成した．
(27) 通知書送付先リストの作成を開始した．
(28) 各新聞社等からの取材があった．

2003 年 6 月 24 日 (火)

(29) パスワード一括変更作業について，業者 A 担当者との打ち合せを行った．
(30) パスワード一括変更作業スケジュールを全ユーザへメール送信した．
(31) 削除対象ユーザ (4726 名) の削除処理を実行した．最終的に対象となるユーザ数が 17995 名 (学生ユーザ 16904 名，研究ユーザ 1091 名) となることを確認した．
(32) NHK からの取材があった．

2003 年 6 月 25 日 (水)

(33) 掲示板システム開発業者からの経過報告があった．

2003 年 6 月 26 日 (木)

(34) 業者 A 担当者立ち合いの元，パスワード一括変更作業の一回目のテストを実施し，テスト結果に基づいてプログラム変更を行った．

2003 年 6 月 30 日 (月)

(35) ユーザ窓口担当者との打ち合せを行った．ユーザによるパスワード変更を停止することによる問い合わせ増加に備えるためのマニュアルを作成した．基本的には，メール転送設定を変更してもらうことで対処するようにした．
(36) 通知書送付先リストの作成が終了した．

2003 年 7 月 1 日 (火)

(37) 午前 9 時にユーザによるパスワード変更を停止した．それまでの間にパスワード変更が正しく行われたユーザは 5181 名だった．一部のサーバのデーモンが停止していたためパスワード変更が正しく行われなかったユーザは 68 名，パスワード変更を行っていないユーザは 12746 名だった．
(38) 通知書 (17995 名) の印刷を開始した (同日中に終了)．
(39) パスワードデータベースのバックアップを行った．

2003 年 7 月 2 日 (水)

(40) 通知書の発送準備を開始した．

2003 年 7 月 3 日 (木)

(41) 念のため全ユーザのホームディレクトリのバックアップを取った．
(42) パスワード一括変更作業について，業者 A 担当者との打ち合せを行った．

2003 年 7 月 4 日 (金)

(43) 7 月 7 日以降のユーザ対応マニュアルを作成した．
(44) 7/5, 7/7, 7/8 の計算機演習履修者のパスワード一覧を作成した．
(45) 18:00 業者 A 担当者立ち合いの元，テストユーザ，研究ユーザ，学生ユーザ 1，学生ユーザ 2 の 4 グループに分けて，パスワード一括変更作業を開始した．また，変更作業が終了したグループに対して，動作テストを行った．
(46) 全ユーザに対する APOP 対応処理を行った．
(47) 学外からの POP3, APOP 接続を許可した．

2003 年 7 月 5 日 (土)

(48) 05:00 パスワード一括変更の全作業が終了した．
(49) 15:00 土曜日開講の計算機演習への立ち合いを行った．

2003 年 7 月 7 日 (月)

(50) 通知書の配布を開始した．

3　インシデント対応策

今回の事例だけを元に一般的な対応策をまとめるのは難しいが，文献 [2, 3, 4] なども参考にして，インシデント対応 (特に，緊急的対応) の一方法をまとめてみる．

(1) **落ち着く**: 落ち着いて対処することが重要である．間違った決断をすると後で困ることになる．

(2) **対策チームの編成**: 対策チームを作る．対策チームは，以下に述べる事項を行う．これらは，組織全体に大きな影響を及ぼす可能性があるため，組織の上層部との連携も重要である．上層部が的確な判断をできるように，適宜状況をわかりやすく上層部に説明し，具体的な処置の実行について権限の委譲を受けておく．

(3) **状況の正確な把握**: 技術的に綿密な調査をし，何が起こった/起こっている/今から起こりえるのかをできるだけ正確に把握する．

(4) **影響および被害の予想**: どのような影響あるいは被害がどのような範囲に起こった/起こっている/今から起こりえるのかを予想する．起こりえるものについては，最悪のケースを想定することも必要である．大規模なインシデントの場合は，社会的な影響も考慮する．

(5) **対策プランの作成**: 影響および被害をできるだけ小さくするための対策プランを作成する．技術的な対策だけでなく，ユーザへの連絡手順，マスコミ対応等，影響および被害の範囲に応じたプランを作成する．

ユーザへの連絡については，的確かつわかりやすい情報が，確実に伝わるようにしなければならない．ユーザに伝えるべき内容が刻々と変化する可能性も高いので，Web ページ等による情報伝達も利用する．

大規模なインシデントの場合は，広報担当部署と協力して，マスコミ等への広報プランを作成する．広報担当部署だけで応対できるように，想定問答集なども作成しておくと良い．なお，マスコミ等は情報を歪めて伝達する傾向があるので注意する．

(6) **関係方面への連絡**: 組織内および IPA 等の外部組織への報告，侵入先や侵入元への連絡を行う．

(7) **対策プランの実行**: 作成した対策プランを実行する．ユーザからの多数の問い合わせが予想される場合は，ユーザ対応マニュアルを作成する．ただし，すべての問い合わせを機械的に処理しようとしてはならない．ユーザからの問い合わせには，重要な問題点が含まれていることがある．常に状況を把握し，場合によっては対策プランそのものを見直す．

4　おわりに

今回のインシデントについて，発生の原因となった計算機は，センターで運用していたものではないが，恥ずかしい限りであり，反省すべき点は多数ある．

しかしながら，インシデント対応については，必要なことを行い，影響を最小限に抑えることができた (少なくとも現時点では) と考えている．あえてこのような一事例を紹介することで，読者の方々の参考になれば幸いである．

最後に，今回のインシデントについて，センターユーザならびに大学内外関係者に多大な迷惑をおかけした点をお詫びいたします．

また，神戸大学学長を始めとする大学上層部の迅速かつ的確な決断，および学術情報基盤センターや学内の各部署の御協力がなければ，今回のインシデントへの対応をこのように行うことはできませんでした．この場を借りて深く感謝致します．

参考文献

[1] 情報処理振興事業協会 セキュリティセンター. 情報セキュリティインシデントに関わる調査 調査報告書. IPA/ISEC, 2002. (http://www.ipa.go.jp/security/fy13/report/incident_survey/incident_survey.pdf)

[2] 情報処理振興事業協会 セキュリティセンター. インシデントマネジメント. IPA/ISEC 情報セキュリティセミナー, 2001. (http://www.ipa.go.jp/security/awareness/administrator/incident.pdf)

[3] JPCERT/CC. 技術メモ—コンピュータセキュリティインシデントへの対応. JPCERT-ED-2002-0002, 2002. (http://www.jpcert.or.jp/ed/2002/ed020002.txt)

[4] 小島 肇: ありがちなインシデントとその対応, 滋賀大学 セキュリティー対策第 3 回講習会, 2003. (http://www.st.ryukoku.ac.jp/~kjm/security/)