サイエンティフィック・システム研究会
2006 年度システム技術分科会第 2 回会合　　2007 年 1 月 31 日

コーディネーションセンターから見た情報セキュリティの最新動向と対応体制のベストプラクティスについて

JPCERT コーディネーションセンター
早期警戒グループ　リーダ／情報セキュリティアナリスト
名和 利男

(1) JPCERT/CC とは

JPCERT コーディネーションセンター(JPCERT/CC)は、世界規模に進化するセキュリティインシデントに対応するため、我が国を代表する CSIRT[1](Computer Security Incident Response Team)として、国際連携(FIRST[2]、APCERT[3])、予防・対策・対処、モニタリングを行い、我が国の CSIRT 活動の推進を支援している。

JPCERT/CC の沿革については、1992 年にボランティアベースの活動から始まり、1996 年に任意団体として正式に発足し、2003 年法人格を取得後は、インターネット定点観測事業や脆弱性情報流通調整機関としての活動をしている。

(2) 最近のセキュリティトピック

ア トピック１ – Botnet

Botnet とは、Bot と呼ばれるウィルスの一種に感染したコンピュータが構成するネットワークの総称であり、数百～数万台の規模で構成されている。（最近は、規模縮小化の傾向にある）

また、攻撃者である Herder[4]は、脆弱性等を狙った感染攻撃、PC 内の機密情報の搾取、迷惑メールなど送信及び中継などの命令を Bot に出すことが確認されている。これは、マルウェア[5]作者の目的が、以前のウィルスやワームなどにみられた愉快犯的なものから、明らかな金銭目的へと変化していることを意味している。

イ トピック２ – Phishing

2006 年、世界的に Phishing の被害が急速に拡大した。特に、犯罪組織化及び高機能の Phishing 作成ツールの出現などが特徴的であり、”Phishing”という言葉自体がオクスフォード英語辞書に載るほど認知度が上がっている。また、様々な Phishing 対策に対抗する手段も洗練化されており、有効な対策手段の確立が難しい。

2005 年 12 月のインディアナ大学の Phishing に関する調査より、Phishing サイトが立ち上がってから１日程度で、ID 及びパスワード取得などの目的達成が 70%以上になることが分析できる。このため、Phishing サイトを発見した場合は、迅速に報告することが重要である。しかし、残念なことに、その報

---

1 CSIRT：コンピュータセキュリティインシデントの報告を受け付け、適切な対応及び関係部署と他の組織やチームと連携を図ることによって、被害の局限化と迅速な解決の支援するチームを意味する。

2 FIRST : Forum of Incident Response and Security Teams

3 APCERT:Asia Pacific Computer Emergency Response Team(アジア太平洋コンピュータ緊急対応チーム)

4 Herder : bot(botnet)を操る攻撃者を指す。herder とは英語で羊飼いのこと。

5 マルウェア(malware)： 一般に不正プログラム全般を指す。　(脚注文責 :SS 研事務局)

告先(消費者保護団体、警察機関、CSIRT など)があまり周知されていないのが現状である。

ウ 用語から見るセキュリティ動向

Phishing に関係して、以下のキーワードが顕著に見られる。

Spear Phishing[6]、クリック詐欺、Vishing[7]、Piggy Back[8]、Crimeware[9]、Dump[10]、Carding[11]、Screen logger[12]、Money Mule[13]

特に、”Vishing” については、電話で銀行のアカウントの ID とパスワードを確認させるような自動応答メッセージなどを聞かせる手法で、アカウント情報を不正に入手するということを意味する。

エ 最近の事象を５W１Hで整理

- WHEN(いつ発生?) ： 脆弱性が公表される前の攻撃が増加
- HOW(どんな手法?) ： 大規模に広がるワーム等はもう見られなく、ソーシャルエンジニアリング[14]、高性能なアプリケーションの機能を利用した攻撃にシフトしている。
- WHAT(どんな被害?) ： 金銭目的
- WHERE(どこが対象?) ： 攻撃対象の局所化
- WHO(いったい誰が?) ： やはり不明だが、最近は組織化されていることが確認されている。
- WHY(なぜ行う?) ： 情報が取得しやすい環境にあるから。

※「犯罪化」の傾向が強くなってきている。

オ とらなければならない対策

- 犯罪者のリスクを底上げする。
- 脆弱性の数を減らす。
- 国境のないインターネットに必要な協調

特に、すべての政府レイヤー、警察レイヤー、技術レイヤーを繋ぐコーディネーターとして CSIRT の活動を活発化させる必要がある。

(3) 対応対策のベストプラクティス：CSIRT

ア CSIRT とは

CSIRT は 1988 年モリスワームによる被害にかかる対応体制の不備が大きな原因であったことに対する対策として、コンピュータの緊急事態に適切に対応する組織(CERT/CC)を構築したのがきっかけである。その組織モデルのことを CSIRT という。また、単独の CSIRT のみで、すべての業種や組織体に対して対応をとることが難しいため、様々な分野や国で CSIRT の設立が始まり、その連携を図るためにコ

---

6 Spear phishing : 特定の人物を狙い、偽のメールを送ったりウイルスを仕込んだりしてパスワードや個人情報などを搾取する詐欺。

7 Vishing(VoIP Phishing) : IP 電話経由で大量の電話番号へ録音されたメッセージを送り、偽造された発信者番号で安心させた上でクレジットカード番号を聞き出す詐欺。

8 Piggy back : 正規のものの同伴者を装い侵入する行為。

9 Crimeware : ユーザの個人情報を盗み、オンライン銀行から金銭を不正に引き出したりといった犯罪行為を行なう目的で作られた悪意のあるソフトウェア。

10 Dump : クレジット情報のこと。

11 Carding : カード不正利用ツールやクレジットカード情報(Dump)、さまざまな個人情報は、Carding と呼ばれる site で売買されている。

12 Screen logger : ユーザ名やパスワードなど、画面に表示されていた個人情報等の機密情報詐取プログラム。

13 Money Mule : phising や個人情報窃盗は世界中で盗まれたお金を洗浄するための悪意にうっかり荷担してしまった人(mule:麻薬の運び屋の意)。mule はメールで送られてくる求人募集に応募することで、不透明な商売や取引に巻き込まれるケースが多い。

14 Social Engineering : id/password を入手するため、メールに仕掛けられた攻撃を実行するリンクをクリックさせたりする等、心理的な弱点をついて、人を騙すハッキングの一種。 (脚注文責 SS 研事務局)

ミュニティーの活動が活発になっている。

イ CSIRT の活用

CSIRT を組織内に設けると、①情報セキュリティのガバナンスとして、②対外的から統一された窓口(Point of Contact)として、そして、③インシデント対応に必要な外部との信頼関係の構築に役立つ。

ウ 万が一のインシデント発生時に必要なこと

インシデントが発生した場合は、①迅速かつ確実に適切なところに発生情報を伝達し、②現場は、誰が、何を、どこまで、どのような判断で実施しなければならないかを迅速に決定し、行動することが必要である。③想定外のインシデントについて、信頼できるところに助けを求めることが必要であり、日ごろからの情報蓄積と様々な組織との関係構築をしておく必要がある。

(4) 連絡先

CSIRT 構築に関するご相談は、office@jpcert.or.jp まで。

また、インシデント報告に関しては、info@jpcert.or.jp となっており、専用の報告様式については、http://www.jpcert.or.jp/form/ にある。

以 上