サイバーレスキュー隊（J-CRAT） 活動状況
[2015 年度下半期]

2016 年 6 月 29 日
IPA（独立行政法人情報処理推進機構）
技術本部セキュリティセンター

サイバーレスキュー隊（J-CRAT）[i]における、2015 年度下半期(2015 年 10 月～2016 年 3 月)の活動状況を以下に示す。

1 活動結果

2016 年 10 月～2016 年 3 月に、「標的型サイバー攻撃特別相談窓口」に対して寄せられた相談件数と、緊急を要する事案に対してレスキュー支援を行った件数、そのうち当該組織での対応が必要と判断し隊員を派遣したオンサイト支援の件数を、表1に示す。

表 1 J-CRAT 支援件数の推移

項番	項目	2014年			2015年		
		上期	下期	合計	上期	下期	合計
1	相談件数	41 件	66 件	**107 件**	246 件	291 件	**537 件**
2	レスキュー支援数	17 件	21 件	**38 件**	104 件	56 件	**160 件**
3	オンサイト支援数	6 件	5 件	**11 件**	31 件	8 件	**39 件**

※1 1 つの事案に対して複数回のオンサイト対応を要した場合も、1件として集計

「標的型サイバー攻撃特別相談窓口」に対して寄せられた**相談件数**は **291 件**であった。このうち、**レスキュー支援**へ移行したものは **56 件**、**オンサイト支援**を行った事案数は **8 件**であった。

レスキュー支援へ移行した **56 件**の組織ごとの内訳は、独立行政法人 3 件、社団・財団法人 11 件、企業 39 件、その他公共機関等 3 件であった。

2015 年度下半期の支援件数を**昨年の同時期(2014 年 10 月～2015 年 3 月)**と比較すると、**相談件数**がおよそ **4.4 倍**、**レスキュー支援件数**がおよそ **2.6 倍**、**オンサイト支援件数**が **1.6 倍**となった。公的機関の情報漏えい事案のあった **2015 年上期**と比較すると、**相談件数**がおよそ **1.2 倍**、**レスキュー支援件数**がおよそ **0.5 倍**、**オンサイト支援件数**が **0.25 倍**となった。

2 2015 年度下半期の活動を通じてみられた特徴的な事項

(1) 業務で実際に使用したメールを再加工し、詐称メールに利用されるケースがあった。その特徴は以下である。

- 本物のメールを加工しているため、メール文面や添付ファイル名だけで見分けることは困難である。ただし、差出人のメールアドレスや、添付されたファイルの拡張子を確認すれば不審であると見抜くことが可能なケースが大半であった。
- 本物のメールを詐称メールに使われたケースでは、そのメールを閲覧できる人物(送信者、または受信者)のパソコンがウイルスに感染していた例や、メールアカウントの ID/パスワードが不正に利用されていた例も見られた。

(2) 特定の業界を狙ったと思われるキャンペーンが確認された。(詳細については別冊の「サイバーレスキュー隊(J-CRAT)分析レポート 2015」を参照)

3 活動を通じての提言

2015 年下半期に活動を通じて見られた標的型サイバー攻撃を前提に、以下の通り提言する。

(1) 日ごろからシステム全体を把握しておくこと(再掲載)

事前に自組織で使用しているシステム全体を把握していれば、被害の拡大を防げたケースが多く見られた。組織にシステム全体の把握者が不在であれば、職務としての担当者を立てることが望ましい。システムの全体を把握していれば、有事の際の被害範囲の把握や対策の網羅的な確認などが可能になり、ウイルス感染後の被害拡大を抑えることが出来る。インターネット接続状況や装置の場所、ファイルサーバや認証サーバなどの各種サーバ、パソコンの台数、メールやウェブサーバの構成把握がセキュリティの向上と万一のインシデント対応に有効である。

(2) ファイアウォールやプロキシサーバの適切な利活用を図ること(改版)

ファイアウォールやプロキシサーバでのアクセス制御やログの取得をしておらず、被害の拡大や原因究明が困難となるケースが多く見られた。少なくとも、①ファイアウォールの導入、②ファイアウォールでの適切なアクセス制御、③ファイアウォールでのログの取得(イントラネット側からインターネット側への許可ルールに適合する通信を含む)、をすべきである。

さらに、④プロキシサーバの導入、⑤プロキシサーバでの適切なアクセス制御、⑥プロキシサーバでのログの取得、を行うことで、通信制御や、潜伏、侵攻の気付き、原因調査や被害状況の把握の手助けとなりうる。

通信制御の有効な手法としては下記が挙げられる。

- URL ベースでの通信制御(IP アドレスの変動に依存しないフィルタリング)
- プロキシを経由しないウイルス通信(Direct 接続)の検出
- プロキシサーバログ等から通信の流量の把握

また、最近も見られているウイルス通信の傾向把握として以下も有効である

- 名前解決をせずに IP アドレスへ直接行う通信や、ダイナミック DNS への通信、PasS 環境への通信の検知
- 名前解決後の IP アドレスが 127.0.0.1 や 0.0.0.0、またはドメインが存在しない事を示すエラー(NXDOMAIN)が返された、定期的に発生する通信の検知

ログ取得の期間は、扱う情報の種類やシステムの影響度、組織のニーズなど様々な要因が関係するため、ひとえに示すことはできないが、既存で取得できる環境があれば、最低でも 3～6 ヶ月、これから新規の調達を考える場合は、業務の重要度に応じた適切な期間の取得を検討していることが望ましい。

(3) メールアカウントやメールサーバ・サービスの不正利用(踏み台)への対策

自身の利用するメールアカウントが不正に利用されないためにも、適切なパスワード管理や不審な WiFi の利用を避けるなどの注意が必要である。また、自組織の管理するメールサーバや利用するメールサービスで不正中継への対策が取られている事が望まれる。特に、POPbeforeSMTP や SMTP-AUTH などを使い、インターネット上から自身のメールアカウントを利用する際には、自身の認証履歴、送信済み履歴が把握できる事が望ましい。一般的な不正利用対策として、OP25B(Outbound Port 25 Blocking)、やパスワードアタックへの対策、リソース監視・セッション監視等も有効である。

万一、アカウント情報が窃取された際のリスク管理として、日ごろから機微なメールのやりとりはサーバやメーラーに残さずに削除、または暗号化して保管することも検討するべきである。

(4) 実行ファイルの取扱いについて

2015 年下半期に見られた標的型攻撃メールでは、実行ファイル(ウイルス)をパスワード付きの ZIP 形式で圧縮した後、メールに添付して送付するケースがほとんどであった。さらに実行ファイルの拡張子は「.txt.exe」や、「.doc.exe」となっており、テキストアイコンを偽装しているものであった。このためシステム側では添付ファイルの拡張子(パスワード付きの ZIP 形式で圧縮されたものを含む)にてフィルタリングできるメール製品を活用する事が望ましい。またユーザでは不審な実行ファイルの防止を図るため拡張子を表示する設定にするべきである。この設定は Active Directory を活用していればグループポリシーとして配信することも可能である。

以上

[i] IPA が標的型サイバー攻撃の被害拡大防を目的に 2014 年 7 月に発足。相談を受けた組織の被害の低減と攻撃の連鎖の遮断を支援する活動を行っている。
https://www.ipa.go.jp/security/J-CRAT/