サイバーレスキュー隊（J-CRAT） 活動状況
[2015 年度上半期]

2015 年 10 月 26 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 年度上半期(2015 年 4 月～9 月)の活動状況を以下に示す。

1 活動結果

2015 年 4 月～9 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	**件数（2015 年 4 月～9 月）**	（2014 年 10 月～2015 年 3 月）	（2014 年 4 月～9 月）
1	相談件数	**246 件**	（66 件）	（41 件）
2	レスキュー支援数	**104 件**	（21 件）	（17 件）
3	オンサイト支援数	**31 件**※1	（5 件）	（6 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 **246 件**であった。このうち、**レスキュー支援**へ移行したものは **104 件**、**オンサイト支援**を行った事案数は **31 件**であった。

レスキュー支援へ移行した **104 件**の組織ごとの内訳は、独立行政法人 16 件、社団・財団法人 41 件、企業 19 件、その他公共機関等 28 件であった。

2 特記事項

2015 年度上半期の支援件数を**昨年の同時期(2014 年 4 月～9 月)**と比較すると、**相談件数**、**レスキュー支援件数**がおよそ **6 倍**と、**オンサイト支援件数**もおよそ **5 倍**となった。特に、公的機関の情報漏えい事案のあった 6 月以降は大幅な増加が見られた。

2.1 ウイルス感染被害に関する報道発表(6 月 1 日)による影響について

6 月以降、社会や産業に対して影響のある組織での、標的型サイバー攻撃の被害相談やセキュリティ対策方針に関する相談が増加した。これを受け、ウイルス感染の早期発見、被害の低減を目的に、具体的な発見方法を示した、管理者向け、利用者向けの注意喚起を 3 回実施した(表 2 参照)。

表 2 2015 年 6 月に実施した注意喚起

日時	注意喚起の表題とリンク	概要
6 月 2 日	【注意喚起】ウイルス感染を想定したセキュリティ対策と運用管理を https://www.ipa.go.jp/security/ciadr/vul/20150602-secop.html	多層防御を考慮したセキュリティ対策と運用管理方法
6 月 10 日	【注意喚起】組織のウイルス感染の早期発見と対応を https://www.ipa.go.jp/security/ciadr/vul/20150610-checklog.html	ウイルス活動の確認ポイント（ファイアウォールやプロキシサーバ、Active Directory のログ確認）
6 月 29 日	【注意喚起】潜伏しているかもしれないウイルスの感染検査を今すぐ！ https://www.ipa.go.jp/security/ciadr/vul/20150629-checkpc.html	ウイルス活動の確認ポイント(PC(端末)における不審なファイルや通信有無の確認)

2.2 2015 年度上半期の活動を通じて見られた特徴的な事項

(1) 標的型サイバー攻撃を受けている組織を分析すると、その組織とやりとりをする個人で所有するメールアドレスを経由して攻撃を受けているケースがみられた。これは、かつての高い立場や重要なポストから、組織や職責を離れてもその組織とのやりとりがあり、その個人のパソコンのウイルス感染を介した攻撃となっていた。標的型サイバー攻撃の連鎖は組織間だけでなく、組織と個人の間でも確認された。

(2) 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。

3 活動を通じての提言

(1) 日ごろからシステム全体を把握しておくこと

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

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当該する通信を含む)、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、URL ベースでの通信制御や、プロキシを経由しないウイルス(Direct 接続)の検出、またプロキシサーバログ等から通信の流量を見ることで、情報漏洩の気付きや原因調査の手助けとなりうる。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。

以上

[i] IPA が標的型サイバー攻撃の被害拡大防止を目的に 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/