JPCERT-PR-2015-02
発行日：2015-04-16

JPCERT/CC 活動概要 [2015 年 1 月 1 日 ～ 2015 年 3 月 31 日]

活動概要トピックス

ートピック1ー　内閣官房内閣サイバーセキュリティセンターと国際連携活動及び情報共有等に関するパートナーシップを締結

2 月 10 日に、我が国のサイバーセキュリティ対策の効果的な推進に資することを目的として、内閣官房内閣サイバーセキュリティセンター(以下「NISC」といいます。)との間で、国際連携活動及び情報共有等に関するパートナーシップを締結しました。

JPCERT/CC は、サイバーセキュリティ基本法(平成 26 年法律第 104 号)第 31 条第 1 項が定める「サイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整を行う関係機関」として、また、「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針」(平成 26 年 11 月 25 日決定) 3 (2)④に記述される「サイバーセキュリティに係る緊急時対応関係機関」として、パートナーシップの目的を達することができるよう、NISC への協力体制を強化して参ります。
なお、JPCERT/CC に対するインシデント対応の調整依頼、関係情報の提供、JPCERT/CC からの各種連絡等に関する情報の取扱いは、従前と同様で、パートナーシップの締結によって取扱いが変わることはありません。

(プレスリリース)
JPCERT/CC、内閣官房内閣サイバーセキュリティセンターと国際連携活動及び情報共有等に関するパートナーシップを締結
https://www.jpcert.or.jp/pr/2015/pr150001.html

※JPCERT/CC にお寄せいただいた各種情報の取り扱い方針につきましては次の URL をご参照ください。

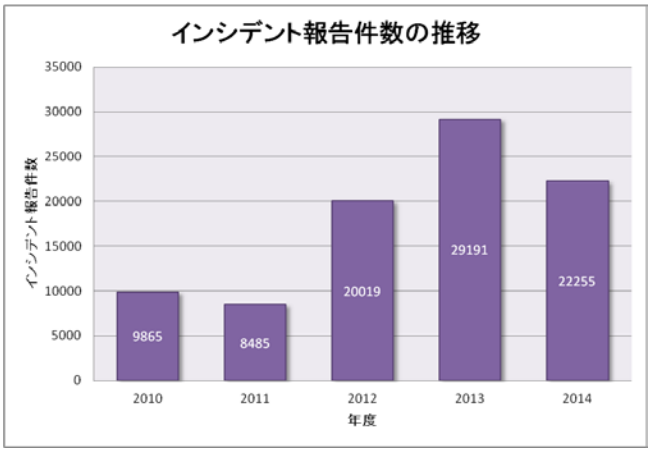
- インシデント報告：https://www.jpcert.or.jp/form/index.html#1
- 制御システムインシデントの報告：https://www.jpcert.or.jp/ics/ics-form.html#1
- 脆弱性関連情報取扱いガイドライン：:https://www.jpcert.or.jp/vh/partnership_guide2014.pdf
- プライバシーポリシー：https://www.jpcert.or.jp/privacy.html

ートピック2ー　2014 年度のインシデントの報告件数は前年度より 24%減るも、調整件数は 9,684 件と 10%の増加

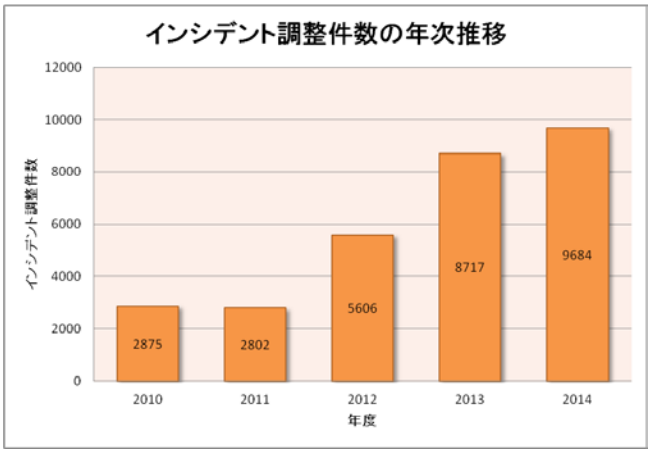
本四半期のインシデントの報告件数は 6,869 件、調整件数(※)は 3,088 件で、前四半期と比較して、報告件数は 10%増加し、調整件数は 32%増加しました。また、前年同期と比較すると、総報告数で 40%増加し、調整件数は 55%増加しました。
本四半期に報告を受けたインシデントの分類としては、システムの弱点を探索するインシデントが 54.3%、Web サイト改ざんに分類されるインシデントが 14.4%を占めています。

システムの弱点を探索するインシデントに関しては、DNS の通信の送信元として、オープンリゾルバになっている国内ホストを数多く確認しています。オープンリゾルバは DDoS 攻撃に使用される可能性があるため、ホストを管理する組織やユーザに対して、サーバやルータ等の機器の設定を見直していただくよう、連絡を行っています。

2014 年度(2014 年 4 月から 2015 年 3 月)に受け付けたインシデント報告の件数は 22,255 件で、前年度の 29,191 件と比較して 24%減少していますが、調整件数は、前年度の 8,718 件から 10%増の 9,684 件と増加しています。これは、大量発生型の Web 改ざんの報告数が減少したことと、1 件のインシデント報告について複数の調整が必要とされる案件が増加したことによると考えられます。



[図 1 インシデント報告件数の推移(年度比較)



[図 2 インシデント調整件数の推移]

※「調整件数」とは、インシデントの拡大防止のため、サイトの管理者等に対し、現状の調査と問題解決のための対応を依頼した件数を示します。

JPCERT/CC インシデント報告対応レポート[2015 年 1 月 1 日 ～ 2015 年 3 月 31 日]
https://www.jpcert.or.jp/pr/2015/IR_Report20150416.pdf

ートピック3ー　制御システムセキュリティ啓発活動　～制御システムセキュリティカンファレンス 2015 と 4 箇所のセキュリティセミナーを開催

2 月 12 日に、制御システムセキュリティカンファレンス 2015 を東京で開催し、264 名の方にご来場いただきました。今回で 7 回目となる本カンファレンスでは、「現状を理解し、将来に備える」をテーマに制御システムセキュリティへの取組について講演いただくなど、今後のセキュリティ改善活動に繋がるような情報交換に役立つプログラムを目指しました。
また、2014 年 12 月から 2015 年 2 月にかけて、岡山、福岡、名古屋、東京において制御システムセキュリティセミナーを開催しました。本セミナーでは、制御システム環境におけるセキュリティ対策の必要性が叫ばれる中、どのように取り組んでいくべきなのかに関して弊センターが実施した情報収集や調査の結果を用いて、今後の制御システムセキュリティ対策を考える上で考慮すべき点を紹介しました。

制御システムセキュリティカンファレンス 2015
https://www.jpcert.or.jp/event/ics-conference2015.html

ートピック4ー　第 11 回　APCERT 合同サイバー演習

APCERT(Asia Pacific Computer Emergency Response Team)は、3 月 18 日、サイバー攻撃への即時対応能力を確認するため、合同サイバー演習を実施しました。本演習は、アジア太平洋地域で発生し、国境を越えて広範囲に影響を及ぼすインシデントへの対応における各経済地域 CSIRT 間の連携の強化を目的として、毎年実施されています。
11 回目となる今回の合同サイバー演習のテーマは、「家庭用のネットワーク機器を悪用した攻撃への対処」でした。APCERT の加盟チームのみならず、イスラム諸国のコンピュータ緊急対応チームである OIC-CERT(The Organisation of The Islamic Cooperation – Computer Emergency Response Teams)からエジプト、チュニジア、モロッコも加わって、22 の経済地域から計 28 チームが参加しました。
JPCERT/CC は、この演習にプレーヤー(演習者)として参画するとともに、ExCon と呼ばれる演習の進行調整役も務め、スムーズな演習の実施を支えました。

(APCERT MEDIA RELEASE)
APCERT EMBARKS ON CYBER ATTACKS BEYOND TRADITIONAL SOURCES
http://www.apcert.org/documents/pdf/APCERTDrill2015PressRelease_Final.pdf

本活動は、経済産業省より委託を受け、「平成２６年度サイバー攻撃等国際連携対応調整事業」として実施したものです。
ただし、「7.フィッシング対策協議会の会員組織向け活動」に記載の活動については、この限りではありません。また、「4.国際連携活動関連」、「9.主な講演活動一覧」、「10.主な執筆一覧」、「12.協力、後援一覧」には、受託事業以外の自主活動に関する記載が一部含まれています。

目次

1. 早期警戒

1.1. インシデント対応支援

JPCERT/CC が本四半期に受け付けたコンピュータセキュリティインシデント(以下「インシデント」といいます。)に関する報告は、報告件数ベースで 6869 件、インシデント件数ベースでは 5485 件でした(注 1)。

(注 1)「報告件数」は、報告者から寄せられた Web フォーム、メール、FAX による報告の総数を示します。また、「インシデント件数」は、各報告に含まれるインシデントの件数の合計を示し、1 つのインシデントに関して複数の報告が寄せられた場合にも 1 件のインシデントとして扱います。

JPCERT/CC が国内外のインシデントに関連するサイトとの調整を行った件数は 3088 件でした。前四半期の 2337 件と比較して 32%増加しています。「調整」とは、フィッシングサイトが設置されているサイトや、改ざんにより JavaScript が埋め込まれているサイト、ウイルス等のマルウエアが設置されたサイト、「scan」のアクセス元等の管理者等に対し、状況の調査や問題解決のための対応を依頼する活動です。

JPCERT/CC は、インターネット利用組織におけるインシデントの認知と対処、インシデントによる被害拡大の抑止に貢献することを目的として活動しています。国際的な調整・支援が必要となるインシデントについては、日本における窓口組織として、国内や国外(海外の CSIRT 等)の関係機関との調整活動を行なっています。

インシデント報告対応活動の詳細については、別紙「JPCERT/CC インシデント報告対応レポート」をご参照ください。

JPCERT/CC インシデント報告対応レポート
https://www.jpcert.or.jp/pr/2015/IR_Report20150416.pdf

1.1.1. インシデントの傾向

1.1.1.1. フィッシングサイト

本四半期に報告をいただいたフィッシングサイトの件数は 466 件で、前四半期の 406 件から 15%増加しました。また、前年度同期(557 件)との比較では、16%の減少となりました。

本四半期のフィッシングサイトの報告件数を、装っていたブランドが国内か国外かで分けた内訳を添えて[表 1-1]に示します。

[表 1-1 フィッシングサイトの国内・国外ブランド別の件数]

フィッシングサイト	1 月	2 月	3 月	国内外別合計(割合)
国内ブランド	22	18	14	54(12%)
国外ブランド	136	52	93	281(60%)
ブランド不明	67	36	28	131(28%)
月別合計	225	106	135	466(100%)

(注 2)「ブランド不明」は、報告されたフィッシングサイトが停止していた等の理由により、JPCERT/CC がブランドを確認することができなかったサイトの件数を示します。

前四半期の 11 月から確認されていなかった国内金融機関を装ったフィッシングサイトが、1 月の後半に短期間ながら確認されました。最初に確認した時点でのフィッシングサイトの IP アドレスは、以前にも使用されていた国内 ISP のネットワークのものでしたが、その後複数回にわたり別の国内 ISP のものに変化し、最終的に香港の IP アドレスになった後でサイトが停止しました。複数の国内 ISP の IP アドレスに切り替わったことから、フィッシングサイトとして使用されたホストは、攻撃者の管理下にあるボットまたはプロキシであると考えられます。

また、前四半期に引き続き、国内オンラインゲームサービスを装ったフィッシングサイトについての報告が継続的に寄せられています。オンラインゲームサービスを装ったフィッシングサイトでは、ランダムに付与されたと考えられるアルファベット 5 文字の.com ドメインの URL が大量に確認されていますが、ドメインが異なるサイトでも IP アドレスは共通しており、ホストとしては単一であると見られます。また、複数の異なるゲームのフィッシングサイトが同一の IP アドレスを使用していた例も確認しており、同一の攻撃者が複数ブランドのフィッシングを行っている可能性があります。

フィッシングサイトの調整先の割合は、国内が 73%、国外が 27%であり、前四半期(国内 70%、国外 30%)に比べ、国内への調整が増加しています。

1.1.1.2. Web サイト改ざん

本四半期に報告が寄せられた Web サイト改ざんの件数は、792 件でした。前四半期の 781 件から 1%増加しています。

本四半期は、Web の検索エンジンでブランド製品の名称などを検索すると、検索結果に大量の不審なショッピングサイトが表示されるという報告を複数受領しました。これらの Web サイトは、検索結果の表示では日本語のショッピングサイトのように見えますが、Web サイトのトップディレクトリにアクセスするとショッピングサイトとは無関係な Web サイトであり、外部から不正にコンテンツを設置された可能性があります。

それらの Web サイトには、大量のブランド製品名などの文字列や難読化された JavaScript が埋め込まれており、JavaScript の難読化を解除すると、不審なショッピングサイトを参照する iframe や、アクセス解析に使用する JavaScript を確認できました。このような改ざんの目的は、検索結果を不正に操作することにあると推測されます。

1.1.1.3. その他

本四半期においては、スキャンに分類される、オープンリゾルバとなっている国内ホストを非常に多く確認し、ホストを管理する組織やユーザに対して、サーバやルータ等の機器の設定を見直していただくよう連絡を行いました。

また、fast-flux(ドメインに対して複数の IP アドレスを割り当て、さらに割り当てる IP アドレスを短期間で切り替えることにより、不正な目的で使用するホストの停止を難しくする攻撃)に関する報告が増加したこともあり、「その他」に分類されるインシデント報告件数が前四半期から 91%増加しました。

1.1.2. インシデントに関する情報提供のお願い

Web サイト改ざん等のインシデントを認知された場合は、JPCERT/CC にご報告ください。JPCERT/CC では、当該案件に関して攻撃に関与してしまう結果となった機器等の管理者への対応依頼等の必要な調整を行うとともに、同様の被害の拡大を抑えるため、攻撃方法の変化や対策を分析し、随時、注意喚起等の情報発信を行います。

インシデントによる被害拡大および再発の防止のため、今後とも JPCERT/CC への情報提供にご協力をお願いいたします。

1.2. 情報収集・分析

JPCERT/CC では、国内の企業ユーザが利用するソフトウエア製品の脆弱性情報、国内インターネットユーザが影響を受ける可能性のあるコンピュータウイルス、Web サイト改ざん等のサイバー攻撃に関する情報を収集し、分析しています。これらのさまざまな脅威情報を多角的に分析し、必要に応じて脆弱性やウイルス検体の検証等も併せて行い、分析結果に応じて、国内の企業、組織のシステム管理者を対象とした「注意喚起」 (一般公開) や、国内の重要インフラ事業者等を対象とした「早期警戒情報」 (限定配付) 等を発信することにより、国内におけるサイバーインシデントの発生・拡大の抑止を目指しています。

1.2.1. 情報提供

JPCERT/CC の Web ページ (https://www.jpcert.or.jp) や RSS、約 25,000 名の登録者を擁するメーリングリスト、早期警戒情報の受信者用のポータルサイト WAISE (Watch and Warning Analysis Information for Security Experts) 等を通じて、本四半期は次のような情報提供を行いました。

1.2.1.1. 注意喚起

深刻かつ影響範囲の広い脆弱性等について、次のような注意喚起情報を発行しました。

発行件数：8 件　https://www.jpcert.or.jp/at/

2015-01-14　2015 年 1 月 Microsoft セキュリティ情報 (緊急 1 件含) に関する注意喚起 (公開)
2015-01-14　Adobe Flash Player の脆弱性 (APSB15-01) に関する注意喚起 (公開)
2015-01-21　2015 年 1 月 Oracle Java SE のクリティカルパッチアップデートに関する注意喚起 (公開)
2015-01-28　Adobe Flash Player の脆弱性 (APSB15-03) に関する注意喚起 (公開)
2015-01-06　Adobe Flash Player の脆弱性 (APSB15-04) に関する注意喚起 (公開)
2015-02-12　2015 年 2 月 Microsoft セキュリティ情報 (緊急 3 件含) に関する注意喚起 (公開)
2015-03-11　2015 年 3 月 Microsoft セキュリティ情報 (緊急 5 件含) に関する注意喚起 (公開)
2015-03-13　Adobe Flash Player の脆弱性 (APSB15-05) に関する注意喚起 (公開)

1.2.1.2. Weekly Report

JPCERT/CC が収集したセキュリティ関連情報のうち重要と判断した情報の抜粋をレポートにまとめ、原則として毎週水曜日 (週の第 3 営業日) に Weekly Report として発行しています。このレポートには、「ひとくちメモ」として、情報セキュリティに関する豆知識情報も掲載しています。

発行件数：12 件　https://www.jpcert.or.jp/wr/

Weekly Report で扱った情報セキュリティ関連情報の項目数は、合計 52 件、「今週のひとくちメモ」のコーナーで紹介した情報は、次の 12 件でした。

2015-01-07　担当者が選ぶ 2014 年重大ニュース
2015-01-15　「脆弱性診断士(Web アプリケーション)スキルマップ」が公開
2015-01-21　IPA が「2014 年度情報セキュリティ事象被害状況調査」報告書を公開
2015-01-28　JANOG NTP 情報交換 WG 成果物へのコメント募集
2015-02-04　サイバーセキュリティ月間
2015-02-12　IPA が「情報セキュリティ 10 大脅威 2015」を発表
2015-02-18　JNSA「2013 年 情報セキュリティインシデントに関する調査報告書」を公開
2015-02-25　「地方公共団体における情報セキュリティポリシーに関するガイドライン(案)」コメント募集
2015-03-04　Ruby 1.9.3 サポート終了
2015-03-11　日本シーサート協議会「SSH サーバセキュリティ設定ガイド Ver 1.0」を公開
2015-03-18　IPA「安全なウェブサイトの作り方 改訂第 7 版」を公開
2015-03-25　EMET 5.2 リリース

1.2.1.3. 早期警戒情報

JPCERT/CC では、国民の生活や社会経済活動を支えるインフラ、サービスおよびプロダクト等を提供している組織の情報セキュリティ関連部署もしくは組織内 CSIRT に向けて、それらの組織やサービス提供先に深刻なセキュリティ上の問題を惹起する可能性のある脅威情報やその分析結果、対策方法に関する情報等を「早期警戒情報」として提供しています。

早期警戒情報の提供について
https://www.jpcert.or.jp/wwinfo/

1.2.2. 情報収集・分析・提供 (早期警戒活動) 事例

本四半期における情報収集・分析・提供 (早期警戒活動) の事例を紹介します。

【glibc の脆弱性】
2015 年 1 月 27 日、glibc の脆弱性に関する情報が公開されました。glibc は、複数の OS 上の様々なアプリケーションで使用されており、また、当該脆弱性が悪用される最悪のケースでは任意のコードの実行が可能であるとしてメディアなどで取り上げられ話題になりました。JPCERT/CC では、本脆弱性に関する調査・検証を行って影響がかなり限定的である点が確認できたことから、週次で発行している Weekly Report で本脆弱性に関する情報を提供しました。

【Oracle Java SE のクリティカルパッチアップデート】
2015 年 1 月 21 日 Oracle Java SE のクリティカルパッチアップデートに関する注意喚起を発行いたしました。Oracle Java SE には複数の脆弱性が悪用された場合、遠隔の第三者は当該脆弱性を使用することで、Java を不正終了させたり、任意のコードを実行させたりする可能性がありました。また Java SE JDK/JRE 7 は 2015 年 4 月のクリティカルパッチアップデートをもって、公式アップデートが終了予定であり、Java SEJDK/JRE 8 への移行を検討することを推奨しています。

1.3. インターネット定点観測

JPCERT/CC では、インターネット上に複数の観測用センサーを分散配置し、不特定多数に向けて発信されるパケットを収集するインターネット定点観測システム TSUBAME を構築し、運用しています。TSUBAME から得られる情報を、既に公開されている脆弱性情報やマルウエア、攻撃ツールの情報などと対比して分析することで、攻撃活動や攻撃の準備活動等の状況を把握することに努めています。

1.3.1. インターネット定点観測システム TSUBAME の運用、および観測データの活用

JPCERT/CC は、さまざまな地域に設置された観測用センサーを含むインターネット定点観測システム TSUBAME を構築運用するとともに、観測されたデータを各地域の CSIRT と共同で分析をするためのプ

ロジェクトである TSUBAME プロジェクトの事務局を担当しています。2015 年 03 月末時点で、観測用センサーはアジア・太平洋地域の 23 地域に設置されています。今後も設置地域を拡大し、より充実したセンサー網の構築と共同分析の高度化を進めるべく関係機関と交渉を続けています。

TSUBAME プロジェクトの目的等詳細については、次の Web ページをご参照ください。

TSUBAME(インターネット定点観測システム)
https://www.jpcert.or.jp/tsubame/index.html

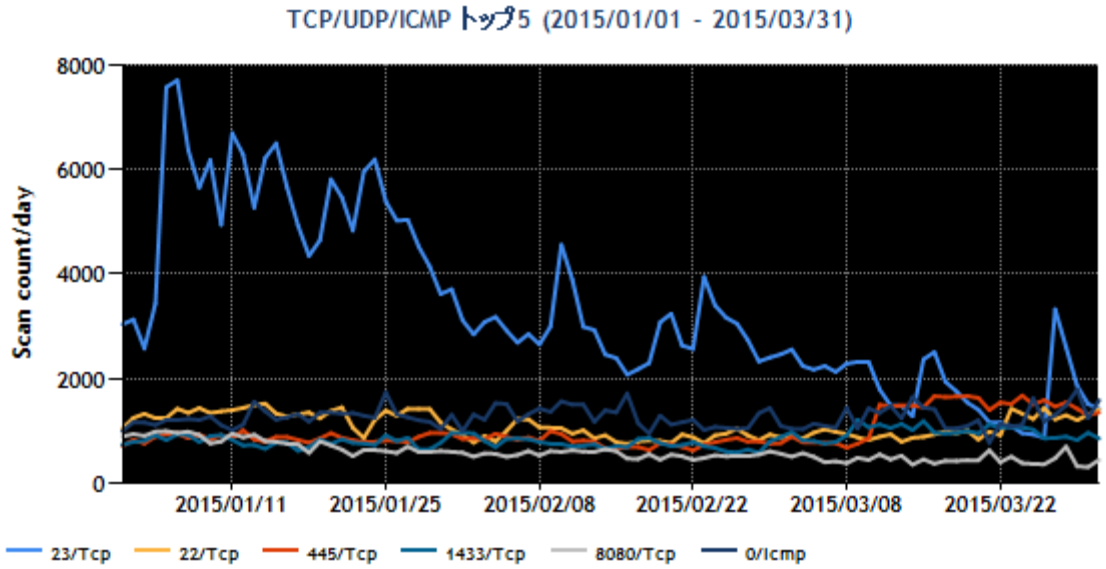
JPCERT/CC は、TSUBAME で収集したデータを宛先ポート番号や送信元地域ごとに分類して統計分析し、既知の脆弱性情報やマルウエア、攻撃ツール等との関連を考察することで、攻撃活動や準備活動の捕捉に努めています。

主に日本企業のシステム管理者等の方々に、自ネットワークに届くパケットの傾向と比較していただけるよう、日本国内のセンサーで受信したパケットを宛先ポート別に集計してグラフ化し、毎週月曜日に JPCERT/CC の Web ページで公開しています。また、四半期ごとに観測傾向や注目される現象を紹介する「インターネット定点観測レポート」を公開しており、2014 年 10 月から 12 月分のレポートを 2015 年 1 月 27 日に公開しました。

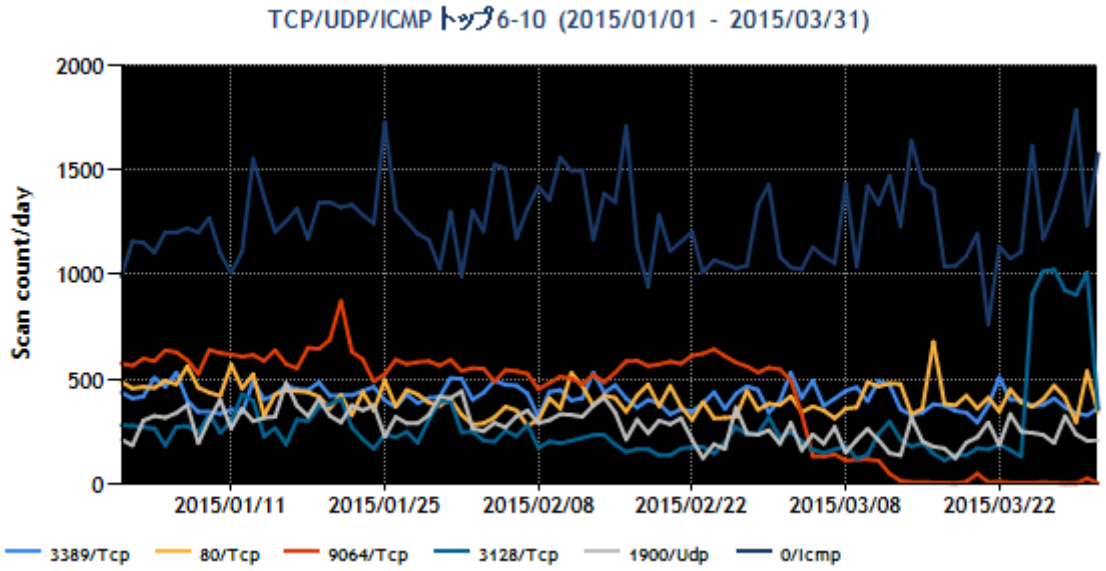
TSUBAME 観測グラフ
https://www.jpcert.or.jp/tsubame/index.html#examples

インターネット定点観測レポート(2014 年 10～12 月)
https://www.jpcert.or.jp/tsubame/report/report201410-12.html

本四半期に TSUBAME で観測された宛先ポート別パケット数の上位 1 位～5 位および 6 位～10 位を、[図 1-1]と[図 1-2]に示します。

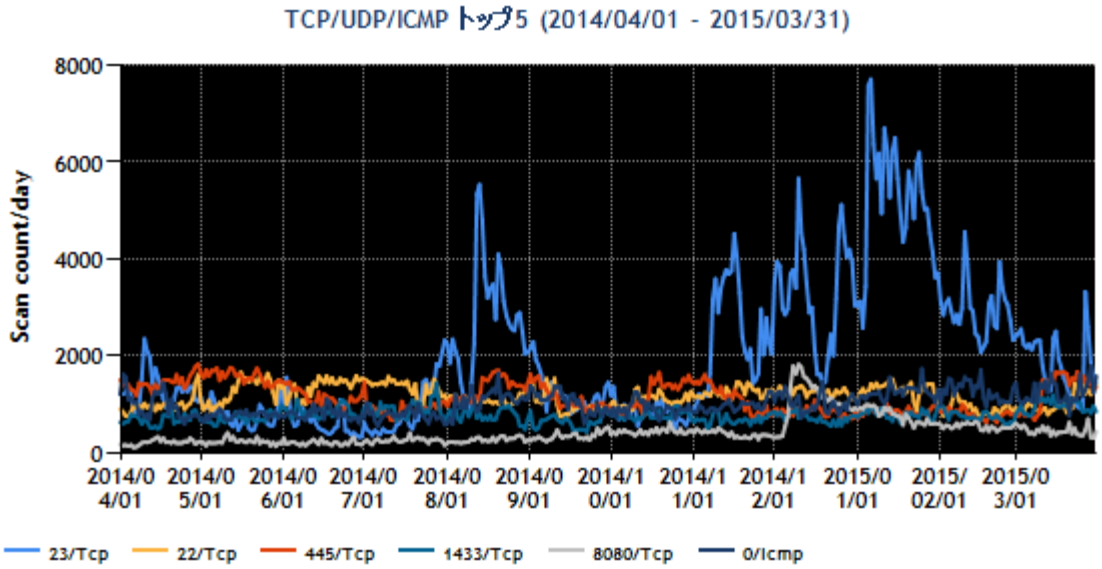


[図 1-1 宛先ポート別グラフ トップ 1-5 (2015 年 1 月 1 日-3 月 31 日)]

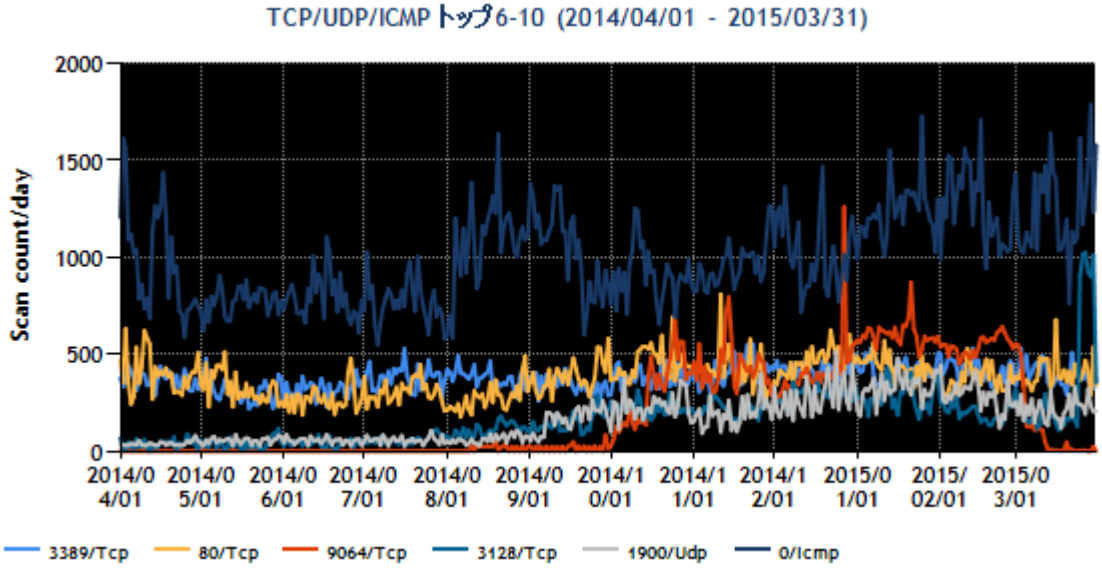


[図 1-2 宛先ポート別グラフ トップ 6-10 (2015 年 1 月 1 日-3 月 31 日)]

また、過去 1 年間(2014 年 4 月 1 日-2015 年 3 月 31 日)における、宛先ポート別パケット数の上位 1 位～5 位および 6 位～10 位を[図 1-3]と[図 1-4]に示します。



[図 1-3 宛先ポート別グラフ トップ 1-5 (2014 年 4 月 1 日-2015 年 3 月 31 日)]



[図 1-4 宛先ポート別グラフ トップ 6-10 (2014 年 4 月 1 日-2015 年 3 月 31 日)]

本四半期は、23/TCP 宛のパケットが 1 月以降減少しました。この減少の原因はわかっていません。23/TCP 宛パケットの多くは送信元が中国でした。なお、前四半期においては、既知の脆弱性(いわゆる Shellshock)をもつ QNAP 社製の Network Attached Storage (以下「NAS」といいます。)製品のマルウエア感染に起因すると思われる、国内を送信元とする 23/TCP 宛のパケットの増加が観測されましたが、本四半期には減少しました。これは、利用者によるマルウエア対策と駆除が進んだ結果であると推測されます。そ

の他、順位に変動はありますが、Windows や Windows 上で動作するソフトウエアへのスキャン活動と見られるパケットや、SSH サーバ等遠隔操作のためにサーバ側が待ち受けているポートのスキャン活動と見られるパケットも、これまでと同様に多く観測されています。

1.3.2. TSUBAME 観測データに基づいたインシデント対応事例

JPCERT/CC では、日々TSUBAME の観測情報を分析し、不審な動きが認められた場合に、必要に応じて送信元 IP アドレスの管理者に連絡する等の対処をしています。

(1) マルウエアに感染した NAS 製品についての対応

本四半期も、前四半期に引き続き、国内の IP アドレスから送信された、23/TCP、8080/TCP 、10000/TCP を探索するパケットが多数観測されました。国外のものを含めて送信元 IP アドレスを調査すると、QNAP 社の NAS 製品の管理画面が確認されました。この NAS 製品には、既知の脆弱性(いわゆる Shellshock)が存在し、利用者がこの脆弱性を修正しないままインターネットからリモートアクセス可能なサービスを有効にしていると、マルウエアに感染してしまう可能性があります。マルウエアに感染した製品は、踏み台となって、さらに他の機器を感染させる活動をしていると推測されます。

インターネット定点観測レポート(2014 年 10～12 月)
2.1 23/TCP, 8080/TCP 宛へのパケットの増加
https://www.jpcert.or.jp/tsubame/report/report201410-12.html#2.1

TCP 8080 番ポートへのスキャンの増加に関する注意喚起
https://www.jpcert.or.jp/at/2014/at140055.html

JPCERT/CC では、TSUBAME で観測した情報から、送信元となっている国内の IP アドレスを調査し、当該 NAS 製品が稼働していることが確認できた先の管理者に対して、該当 IP アドレスで稼働している NAS 製品がマルウエアに感染していないか調査するよう依頼しました。

(2) 攻撃に使用される OpenResolver となっている機器についての対応

本四半期も、前四半期に引き続き、DNS 応答パケットおよび DNS サービスのポート不達を示す ICMP エラーパケットが多数観測されました。国内の送信元 IP アドレスを調査したところ、DNS のリクエストに応答する OpenResolver になっていました。TSUBAME で観測されたパケットは、攻撃者が DNS 権威サーバに過剰な負荷を課そうとする DDoS 攻撃の一部と推測されます。なお、本四半期は、国内でも比較的ユーザ数の多い、複数ドメインを管理している権威 DNS サーバ(以下「共有 DNS サーバ」という。)が、本攻撃の影響を受けたと推測される事象が発生しました。本攻撃を受けたドメインが、共有 DNS サーバで管理されていたことから、同一共有 DNS サーバを利用している別のドメインも影響を受け、ドメインの情報が参照できなくなったものと推測されます。

JPCERT/CC では、TSUBAME で観測した DNS 応答パケットおよび DNS サービスのポート不達を示す ICMP エラーパケットを調査し、その送信元となっている国内の IP アドレスの管理者に対して調査を依頼したところ、多くの管理者から「DNS サーバやネットワーク機器の設定が不適切で OpenResolver になっていたことを確認し、必要な対応を行った」等の回答を得ました。

2. 脆弱性関連情報流通促進活動

JPCERT/CC は、ソフトウエア製品利用者の安全確保を図ることを目的として、発見された脆弱性情報を適切な範囲に適時に開示して製品開発者による対策を促進し、用意された対策情報と脆弱性情報を脆弱性情報ポータル JVN（Japan Vulnerability Notes；独立行政法人情報処理推進機構[IPA]と共同運営）を通じて公表することで広く注意喚起を行う活動を行っています。さらに、脆弱性を作り込まないためのセキュアコーディングの普及や、制御システムの脆弱性の問題にも取り組んでいます。

2.1. 脆弱性関連情報の取扱状況

2.1.1. 受付機関である独立行政法人情報処理推進機構(IPA)との連携

JPCERT/CC は、経済産業省告示「ソフトウエア等脆弱性情報取扱基準」(平成 26 年経済産業省告示第 10 号。以下「本基準」といいます。）に基づいて製品開発者とのコーディネーションを行う「調整機関」に指定されており、本基準を踏まえて取りまとめられた「情報セキュリティ早期警戒パートナーシップガイドライン（以下「パートナーシップガイドライン」といいます。）に従って、対象となる脆弱性に関係する製品開発者の特定、脆弱性関連情報の適切な窓口への連絡、開発者による脆弱性の検証等の対応や脆弱性情報の公表スケジュール等に関する調整を行い、原則として、調整した公表日に JVN を通じて脆弱性情報等を一般に公表しています。**本基準**では、受付機関に IPA が指定されています。JPCERT/CC は IPA が受け付けた届出情報の転送を受けて、製品開発者への情報提供を行い、対策情報公開に至るまでの調整を行っています。最終的には、IPA と共同で、脆弱性情報ポータル JVN において対策情報を公開しています。両組織間においては、脆弱性情報の分析結果や脆弱性情報の取り扱い状況等の情報交換を行う等、緊密な連携を行っています。なお、本基準における IPA の活動および四半期ごとの届出状況については、次の Web ページをご参照ください。

独立行政法人情報処理推進機構(IPA) 脆弱性対策
http://www.ipa.go.jp/security/vuln/

2.1.2. Japan Vulnerability Notes(JVN)において公表した脆弱性情報および対応状況

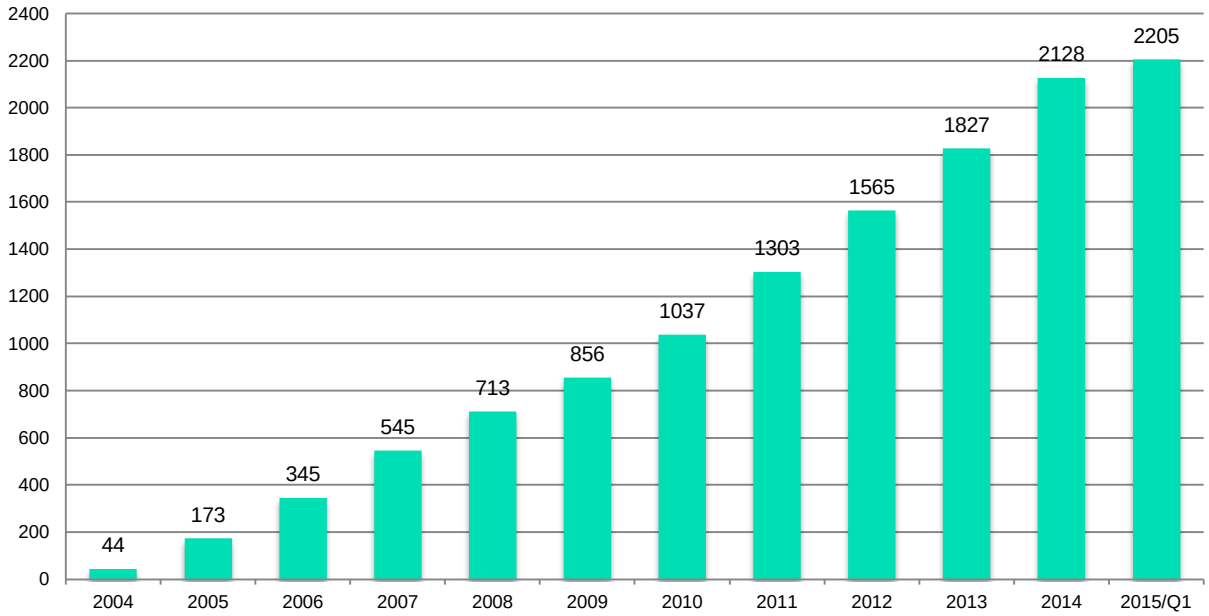
JVN で公表している脆弱性情報は、本基準に従って国内で届け出られた脆弱性に関するもの（「JVN#」に続く 8 桁の数字の形式の識別子[例えば、JVN#12345678 等]を付与。以下「国内取扱脆弱性情報」といいます。）と、それ以外の脆弱性に関するもの（「JVNVU#」に続く 8 桁の数字の形式の識別子[例えば、JVNVU#12345678 等]を付与。以下「国際取扱脆弱性情報」といいます。）の 2 種類に分類されます。国

際取扱脆弱性情報には、CERT/CC や NCSC-FI といった海外の調整機関に届け出られ国際調整が行われた脆弱性情報、海外の製品開発者から JPCERT/CC に直接届け出られた自社製品の脆弱性情報等が含まれます。なお、国際取扱脆弱性情報には、US-CERT からの脆弱性注意喚起の邦訳を含めていますが、これには「JVNTA」に続く 8 桁数字の形式の識別子（例えば、JVNTA#12345678）を使っています。

本四半期に JVN において公表した脆弱性情報は 77 件（累計 2205 件）で、累計の推移は[図 2-1]に示すとおりです。

本四半期に公表された個々の脆弱性情報に関しては、次の Web ページをご参照ください。

JVN(Japan Vulnerability Notes)
https://jvn.jp/

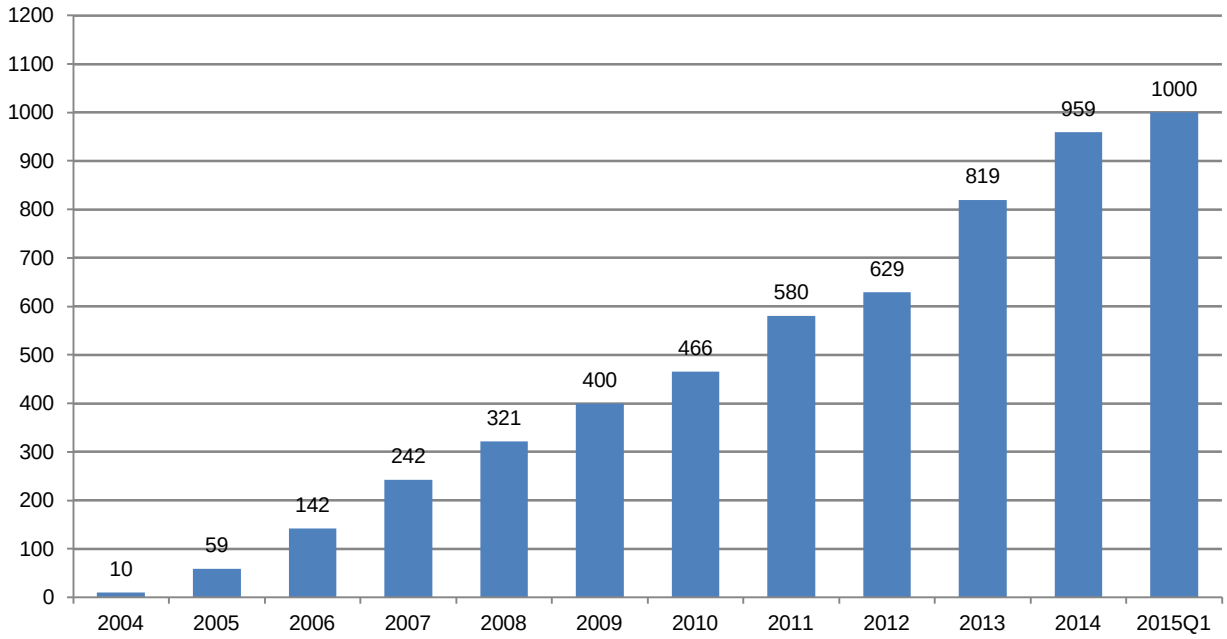


[図 2-1　JVN 公表累積件数]

本四半期において公表に至った脆弱性情報のうち、国内取扱脆弱性情報は 41 件（累計 1000 件）で、累計の推移は[図 2-2]に示すとおりです。41 件のうち、26 件が国内製品開発者の製品、14 件が海外の製品開発者の製品、1 件が国内外の複数の製品開発者の製品のものでした。また、前四半期に引き続き本四半期も、自社製品届出による脆弱性情報を 4 件公表しました。

本四半期に公表した脆弱性情報を、影響を受けた製品のカテゴリで分類すると、ウェブ掲示板に関するものが 7 件、Android 搭載携帯端末や Android アプリに関するものが 6 件、セキュリティソフトウエアが 5 件、フォームメールやメールソフトウエアが 4 件、ルータ等組込系製品が 4 件、CGI に関するものが 3 件、ウェブアルバムが 3 件、それ以外では、グループウエア、ハッシュ値計算 Java 実装、パスワード認証プログラム、ショッピングカート、サーバ関連製品、コンテンツ管理システム（CMS）、仮想化用ソフ

トウエア等がそれぞれ 1 件ずつとなり、多様なカテゴリの製品が混在していました。



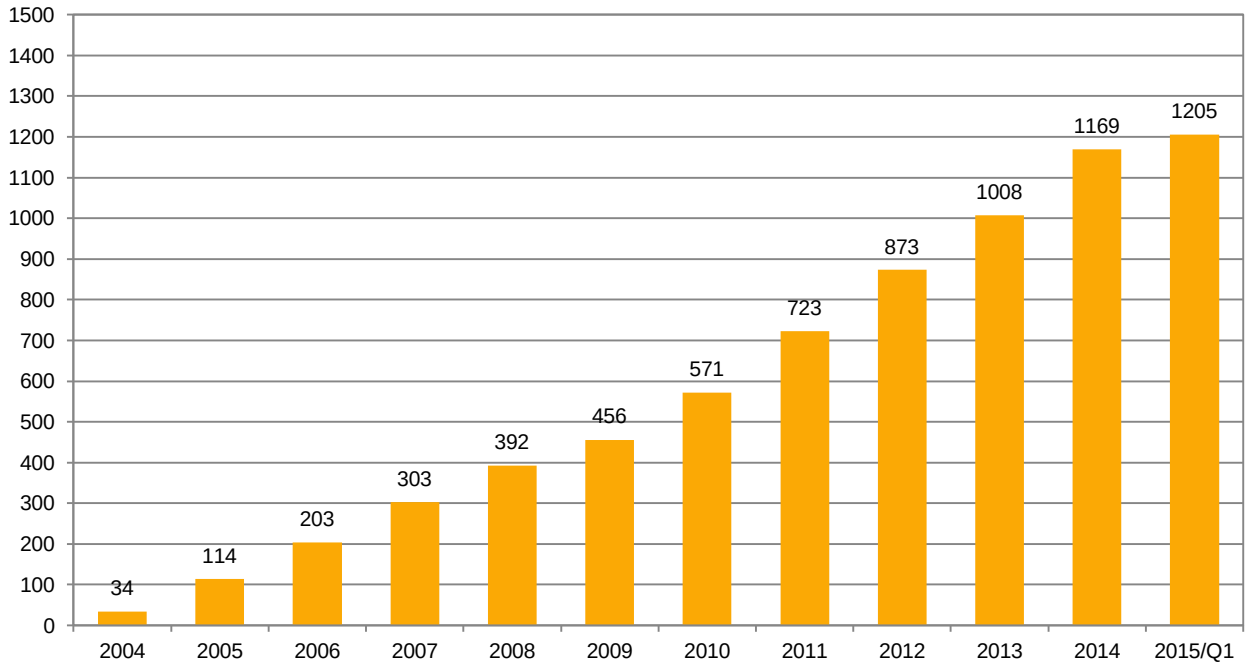
[図 2-2 公表を行った国内取扱脆弱性情報の累積件数]

本四半期に公表した国際取扱脆弱性情報は 36 件（累計 1205 件）で、累計の推移は[図 2-3]に示すとおりです。

本四半期には、暗号化通信プロトコルである SSL に新たな脆弱性が複数指摘されました。昨年（2014 年）4 月にも OpenSSL の「Heartbleed」と呼ばれる脆弱性が公になり、SSL 通信のセキュリティに影響を及ぼす脆弱性として注目を集めましたが、その影響範囲が大きさに鑑み、JPCERT/CC が OpenSSL の脆弱性情報の事前通知を受けられるよう調整していました。その成果もあり、本四半期においては、JVNVU#98974537「OpenSSL に複数の脆弱性」を 2015 年 1 月に、JVNVU#95877131「OpenSSL に複数の脆弱性」を 2015 年 3 月に、開発者である OpenSSL Project Team からの情報公開とほぼ同期して、JVN で公開することができました。また、影響範囲が大きいと考えられたため、日本国内の関連する複数の製品開発者へ情報を展開し、調整を行いました。

本四半期に公表した脆弱性情報の内訳を多いものから挙げると、組込系製品（有線・無線 LAN ルータやドライブレコーダ等）に関するものが 5 件、BIOS に関するものが 4 件、上述の OpenSSL を含むプロトコルに関するものが 3 件、ライブラリに関するものが 2 件、その他としては、通信規格である Bluetooth、サーバ関連製品、コンテンツ管理システム（CMS）、プラグイン、ゲートウェイ等セキュリティ製品、テキストエディタ等といった多様な製品に関するものが混在していました。また自社製品に関する届出は、Apple から 4 件、ISC から 1 件、横河電機から 1 件の計 6 件でした。

本四半期においては、JVN Technical Alert（注意喚起）として、JVNTA#91476059「Superfish がインストールされた Lenovo 製 PC に HTTPS スプーフィングの脆弱性」を、米国 US-CERT Technical Alert TA15-051A “Lenovo Superfish Adware Vulnerable to HTTPS Spoofing "と同期して、JVN で公開しました。



[図 2-3　国際取扱脆弱性情報の公表累積件数]

2.1.3.　連絡不能開発者とそれに対する対応の状況等

本基準に基づいて報告された脆弱性について、製品開発者と連絡が取れない場合には、2011 年度以降、当該製品開発者名を JVN 上で「連絡不能開発者一覧」として公表し、広く連絡の手掛かりを求めています。これまでに 185 件(製品開発者数としては 117 件)を公表し、25 件（製品開発者の数としては 16 件）の調整を再開することができ、脆弱性関連情報の取扱いにおける「滞留」の解消に一定の効果を挙げています。

本四半期は、連絡不能開発者一覧への新規掲載は行いませんでした。一方、既に掲載されていた 3 件（製品開発者数にして 1 件）について調整を再開することができ、JVN で脆弱性情報を公表することができました。本四半期末日時点での「連絡不能開発者一覧」の掲載案件数は 160 件となっており、継続して製品開発者や関係者からの連絡および情報提供を呼びかけています。

こうした呼びかけによっても製品開発者と連絡が取れないケースについて、利用者保護の観点から脆弱性情報を公表する手続きを定めた、本規準およびパートナーシップガイドラインの改正は、昨年5月に完了しており、第一回目となる公表判定委員会が前四半期に開催されました。深刻な脆弱性については、製品開発者と連絡が取れない場合であっても、情報の公表をいつまでも先延ばしにしないための対応を着実に進めています。

2.1.4.　海外 CSIRT との脆弱性情報流通協力体制の構築、国際的な活動

JPCERT/CC は、脆弱性情報の円滑な国際的流通のため、脆弱性情報ハンドリングを行っている、米国

の CERT/CC、英国の CPNI、フィンランドの CERT-FI 等の海外の調整機関と協力関係を結び、それぞれが報告を受けた脆弱性情報の共有、各国の製品開発者への通知および対応状況の集約、脆弱性情報の公表時期の設定等の調整活動を連携して行っています。さらに Android 関連製品や OSS 製品の脆弱性の調整活動の中では、製品開発者が存在するアジア圏の調整機関、特に韓国 KrCERT/CC や中国 CNCERT/CC、台湾 TWNCERT との連携も増えており、国際連携活動の幅が一層広がっています。また、米国 ICS-CERT との連携も、2013 年末より活発化しており、2014 年に 7 件、本四半期においても 1 件と合計 8 件の制御システム用製品の脆弱性情報を公表しました。新たな分野での国際的活動が定着しつつあると言えます。
JPCERT/CC は、日本における脆弱性ハンドリングのコンタクトポイントとして、脆弱性情報ハンドリングにおける国際的活動を引き続き推進してまいります。

JVN 英語版サイト(https://jvn.jp/en)上の脆弱性情報も、日本語版とほぼ同時に公表しており、脆弱性情報の信頼できるソースとして、海外のセキュリティ関連組織等からも注目されています。

また、JPCERT/CC は、CAN（CVE Numbering Authorities）として認定されています。本四半期は、JVN で公表したもののうち、国内で届出られた脆弱性情報 40 件に、JPCERT/CC が CVE 番号を付与しました。2008 年以降においては、MITRE やその他の組織への確認や照合を必要とする特殊なケース（全体の 1 割弱）を除いて、JVN 上で公表する脆弱性のほぼすべてに CVE 番号が付与されています。

CNA および CVE に関する詳細は、次の Web ページをご参照ください。

News & Events　“JPCERT/CC Becomes CVE Numbering Authority”
https://cve.mitre.org/news/archives/2010_news.html#jun232010a
CVE Numbering Authorities
https://cve.mitre.org/cve/cna.html
About CVE
https://cve.mitre.org/about/index.html

2.2. 日本国内の脆弱性情報流通体制の整備

JPCERT/CC では、本基準に従って、日本国内の脆弱性情報流通体制を整備しています。
詳細については、次の Web ページをご参照ください。

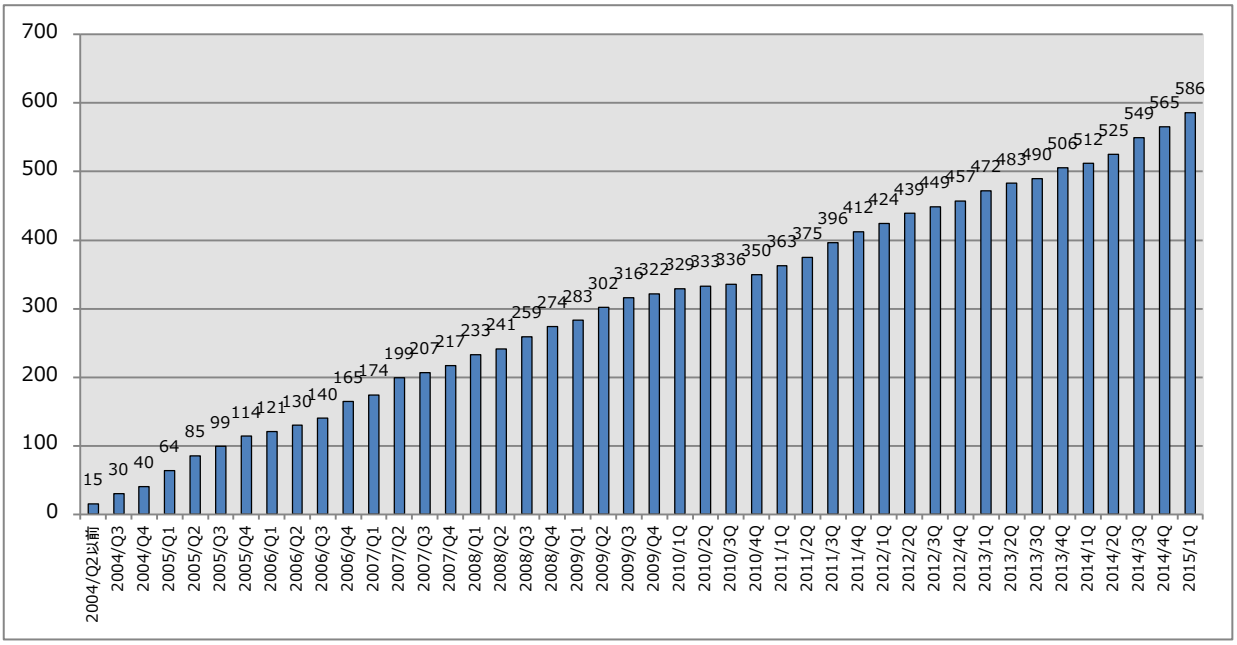
脆弱性情報取扱体制
http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
脆弱性情報コーディネーション概要
https://www.jpcert.or.jp/vh/
「情報セキュリティ早期警戒パートナーシップ」の運用を開始
https://www.jpcert.or.jp/press/2004/0708.txt

情報セキュリティ早期警戒パートナーシップガイドライン(2014 年版)
https://www.jpcert.or.jp/vh/partnership_guide2014.pdf
JPCERT/CC 脆弱性情報取扱いガイドライン
https://www.jpcert.or.jp/vh/vul-guideline2014.pdf

2.2.1. 日本国内製品開発者との連携

本基準では、脆弱性情報を提供する先となる製品開発者のリストを作成し、各製品開発者の連絡先情報を整備することが、調整機関である JPCERT/CC に求められています。JPCERT/CC では、製品開発者の皆さまに製品開発者リストへの登録をお願いしています。製品開発者の登録数は、[図 2-4]に示すとおり、2015 年 3 月 31 日現在で 586 となっています。
登録等の詳細については、次の Web ページをご参照ください。

JPCERT コーディネーションセンター製品開発者リスト登録規約
https://www.jpcert.or.jp/vh/agreement.pdf



[図 2-4 累計製品開発者登録数]

2.2.2. 製品開発者との定期ミーティングの実施

JPCERT/CC では、技術情報やセキュリティ・脆弱性の動向などの情報交換や、脆弱性情報ハンドリング業務に関する製品開発者との意見交換、また製品開発者間の情報交換を目的として、脆弱性情報ハンドリングにご協力いただいている製品開発者の皆さまとのミーティングを定期的に開催しています。

本四半期は 2015 年 3 月 19 日にミーティングを開催し、最近の脆弱性の動向や事例分析、製品開発者に

おける脆弱性診断や脆弱性対応の事例などを紹介するとともに、それらに関する製品開発者との意見交換を行いました。

[図 2-5 製品開発者との定期ミーティングの様子]

2.3. 脆弱性の低減方策の研究・開発および普及啓発

2.3.1. セキュアコーディングに関する講演活動

情報流通対策グループの脆弱性解析チームでは、脆弱なソフトウエアの解析等を通じて得られた脆弱性やその対策方法に関する知見を、広く一般のソフトウエア開発者の方々に伝えるための活動を進めており、その一環として、カンファレンス等での講演を行っています。
本四半期は、ソフトウェア開発者/IT エンジニアの祭典として知られる翔泳社主催のカンファレンス「Developers Summit 2015」において、脆弱性解析チームの熊谷裕志が、Android アプリにおける SSL/TLS サーバ証明書検証に関する発表を行いました。

独自に収集した 5307 件の Android アプリに対して SSL/TLS サーバ証明書検証の実装を簡易調査した結果、1930 件のアプリに脆弱性の可能性があることが判明しています。この調査結果をもとに、問題となっているコードを示しながら脆弱性を解説し、また脆弱性が実際に悪用される可能性があることをデモにより示し、その対策方法について発表しました。

Developers Summit 2015
事例から学ぶ Android アプリのセキュアコーディング

「SSL/TLS 証明書検証の現状と対策」
http://event.shoeisha.jp/devsumi/20150219/session/702/

また、講演の資料はこちらからも閲覧できます。
http://www.slideshare.net/jpcert_securecoding

2.3.2. ハイブリッドアプリフレームワーク「Apache Cordova」における脆弱性の調査

HTML5 や Javascript といったウェブ関連技術を使用してアプリを開発するハイブリッドアプリフレームワークである Apache Cordova について、アプリ開発の際に作りこまれ得る脆弱性に関する調査を行いました。

ハイブリッドアプリフレームワークを使用したアプリ開発では、おもに HTML5 や Javascript といったウェブ関連技術が活用されます。アプリのクロスプラットフォーム展開も容易にできるため、これを利用して開発されるアプリケーションが増えてきており、また、今後一層普及することが予想されます。しかしその一方で、ウェブ関連技術に関するセキュリティ上の問題が開発されるアプリに持ち込まれ、新たな脆弱性となることも懸念されます。そこで、ハイブリッドアプリフレームワークとして最も普及している Apache Cordova に注目し、これを使用した開発の際に作り込まれやすい脆弱性について調査を実施しました。

本調査の結果、Apache Cordova を使用して開発されたアプリでは、ネイティブアプリで指摘されてきた脆弱性に加え、ウェブアプリで指摘される脆弱性や Apache Cordova 固有の脆弱性が作り込まれやすいことが判明しました。今後、本調査結果を開発者向けの資料にまとめて公開する予定です。

2.3.3. CSRF 対策ライブラリに関する調査

既存のソフトウエアに組み込んで CSRF 対策を行うためのライブラリに関する調査を行いました。

ネットワークに接続されたデバイスの web インタフェースや EC サイトなどに CSRF(クロスサイトリクエストフォージェリ)の脆弱性が存在すると、情報漏えいや不正送金などに悪用される可能性があります。その結果、大きな影響を及ぼすインシデントにつながる危険があるため、CSRF 脆弱性が発見された際には迅速に対策を行うことが求められます。近年、既存のソフトウエアに組み込んで CSRF 対策を行うためのライブラリ(以下「CSRF 対策ライブラリ」といいます。)が複数公開されています。まだ CSRF 対策ライブラリの評価は定まっていませんが、これらを適切に活用することで、CSRF 対策が容易になると期待されます。そこで、これらのライブラリがどのようなアプローチで対策を行うものなのか、また、その適用がどの程度現実的なのかを明らかにするための調査を行いました。その結果、注意すべき点はあるものの、CSRF 対策ライブラリは十分に現実的で効果的なアプローチであることが分かりました。今回の調査結果は、開発者向けに解説を加えたうえで啓発資料として公開する予定です。

2.3.4. 「SSH サーバセキュリティ設定ガイド V1.0」の執筆に協力

日本シーサート協議会 (NCA: Nipon CSIRT Association) の SSH サーバセキュリティ設定検討 WG では、SSH サーバをサイバー攻撃から守るためのセキュリティ設定について解説するドキュメントをまとめる活動を行っており、3 月 6 日に設定ガイド Ver1.0 を公開しました。この活動には、JPCERT/CC から脆弱性解析チームの戸田洋三が参加し、SSH を使った通信の仕組みやドキュメント構成に関する議論から執筆まで、活動全般に尽力しました。

SSH サービスはサーバのリモート保守やファイル転送などで利用されていますが、踏み台として悪用され第三者への不正アクセスに加担してしまうなど、サイバー攻撃活動の攻撃対象となる可能性があります。本ガイドでは、CentOS と OpenSSH によるサーバ環境を例として、SSH サーバをサイバー攻撃から守るためのセキュリティ設定について解説しています。

SSH サーバセキュリティ設定ガイド (Ver 1.0)
http://www.nca.gr.jp/imgs/nca_ssh_server_config_v01.pdf

2.3.5. CERT C コーディングスタンダードのルールを更新中

JPCERT/CC では、CMU/SEI のセキュアコーディングプロジェクトが提供する CERT C Coding Standard を邦訳して提供しています。これは C 言語におけるセキュアコーディングを実践するためのルール集で、その内容は日々更新されています。

本四半期に邦訳を更新したルールは次のとおりです。

削除(4 件)

- FLP31-C. 実数値を引数にとる関数を複素数値で呼び出さない
- FLP33-C. 浮動小数点数の演算時には整数を浮動小数点数に変換する
- FLP35-C. 浮動小数点数値を比較する際には精度を考慮する
- MSC36-C. realloc() 関数の呼び出し前にメモリ領域のアラインメントを確認する

移動(2 件)

- INT36-C. ポインタから整数への変換、整数からポインタへの変換 (INT11-C より移動)
- DCL41-C. switch 文のなかでは最初の case 句より前で変数宣言しない (MSC35-C より移動)

新規追加(7 件)

- DCL41-C. switch 文のなかでは最初の case 句より前で変数宣言しない
- FLP06-C. 浮動小数点数の演算時には整数を浮動小数点数に変換する
- FLP07-C. 浮動小数点型を返す関数の返り値はキャストする
- INT35-C. 整数型の精度を正しく求める

- INT36-C. ポインタから整数への変換、整数からポインタへの変換
- POS48-C. 他の POSIX スレッドのミューテックスをアンロックしたり破壊したりしない
- POS49-C. データが複数のスレッドからアクセスされる場合、ミューテックスを使って隣接するデータがアクセスされないよう保護する

内容の更新(27 件)

- FLP30-C. 浮動小数点変数をループカウンタに使用しない
- FLP32-C. 数学関数における定義域エラーおよび値域エラーを防止または検出する
- FLP34-C. 浮動小数点の型変換は変換後の型の範囲に収まるようにする
- FLP36-C. 整数型から浮動小数点型への変換時に精度を確保する
- FLP37-C. 浮動小数点値の比較にオブジェクト表現を使用しない
- INT05-C. 可能性のあるすべての入力を処理できない入力関数を使って文字データを変換しない
- INT06-C. 文字列トークンを整数に変換するには strtol() 系の関数を使う
- INT07-C. 数値には符号の有無を明示した char 型のみを使用する
- INT08-C. すべての整数値が範囲内にあることを確認する
- INT09-C. 列挙定数が一意の値に対応することを保証する
- INT10-C. % 演算子を使用する際、結果の剰余が正であると想定しない
- INT12-C. 式中で使用される単なる int のビットフィールドの型について勝手な想定をしない
- INT13-C. ビット単位の演算子は符号無しオペランドに対してのみ使用する
- INT14-C. 同じデータに対してビット単位の演算と算術演算を行わない
- INT15-C. プログラマ定義の整数型に対する書式付き入出力には、intmax_t もしくは uintmax_t を使用する
- INT16-C. 符号付き整数の表現形式について勝手な想定をしない
- MSC33-C. 無効なデータを asctime() 関数に渡さない
- MSC37-C. 非 void 型関数の制御が関数定義の最終行に到達しないことを保証する
- MSC38-C. マクロとして実装されている可能性のある定義済みの識別子をオブジェクトとして扱わない
- MSC39-C. 値が不定の va_list に対して va_arg() を呼び出さない
- POS30-C. readlink() 関数を適切に使用する
- POS33-C. vfork() を使用しない
- POS34-C. putenv()の引数として自動変数へのポインタを渡さない
- POS38-C. fork およびファイル記述子を使用するときには競合状態に注意する
- POS39-C. システム間でデータを送受信するときは正しいバイトオーダーを使用する
- POS44-C. シグナルを使ってスレッドを終了しない
- POS47-C. 非同期キャンセルが可能なスレッドを使用しない

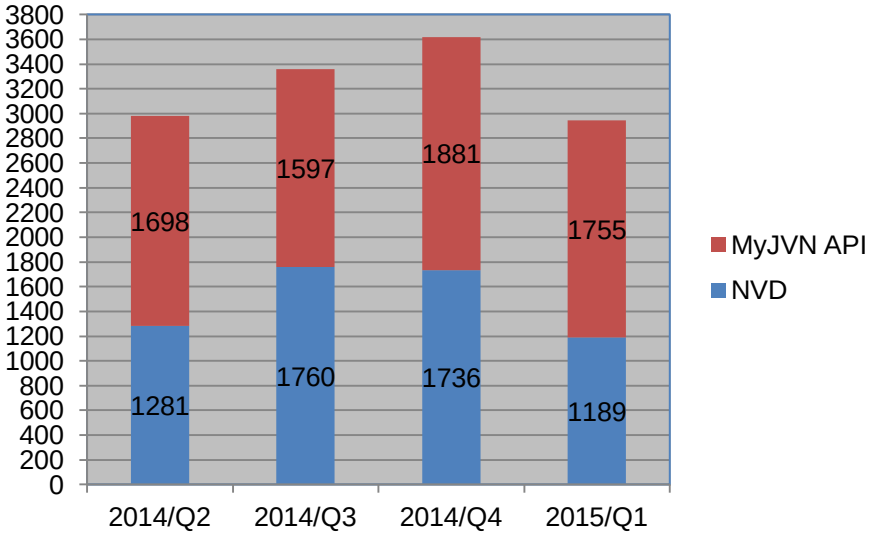
2.4. VRDA フィードによる脆弱性情報の配信

JPCERT/CC は、大規模組織の組織内 CSIRT 等での利用を想定して、KENGINE 等のツールを用いた体

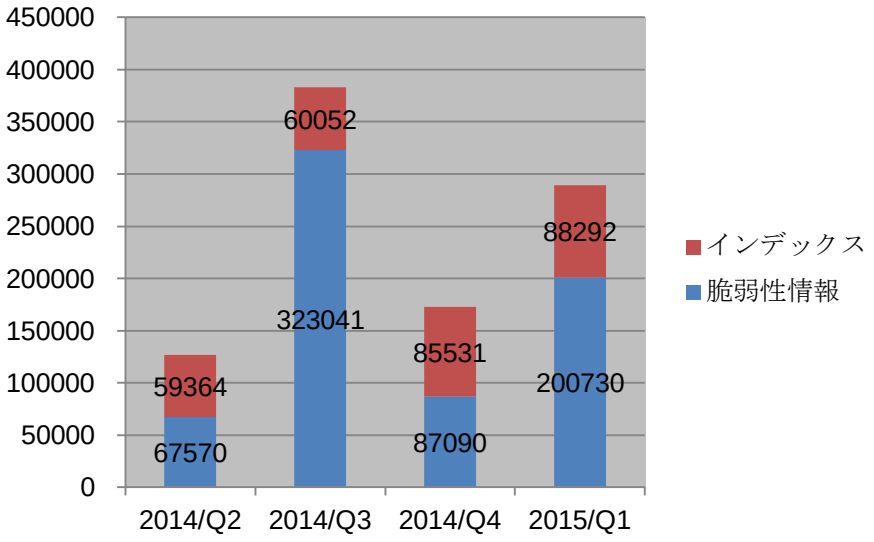
系的な脆弱性対応を可能とするため、IPA が運用する MyJVN API および NIST(National Institute of Standards and Technology)の NVD(National Vulnerability Database)を外部データソースとして利用した、VRDA(Vulnerability Response Decision Assistance)フィードによる脆弱性情報の配信を行っています。VRDA フィードについての詳しい情報は、次の Web ページをご参照ください。

VRDA フィード 脆弱性脅威分析用情報の定型データ配信
https://www.jpcert.or.jp/vrdafeed/index.html

四半期ごとに配信した VRDA フィード配信件数のデータソース別の内訳を[図 2-6]に、VRDA フィードの利用傾向を[図 2-7]と[図 2-8]に示します。[図 2-7]では、VRDA フィードインデックス(Atom フィード)と、脆弱性情報(脆弱性の詳細情報)の利用数を示します。VRDA フィードインデックスは、個別の脆弱性情報のタイトルと脆弱性の影響を受ける製品の識別子(CPE)を含みます。[図 2-8]では、HTML と XML の 2 つのデータ形式で提供している脆弱性情報について、データ形式別の利用割合を示しています。

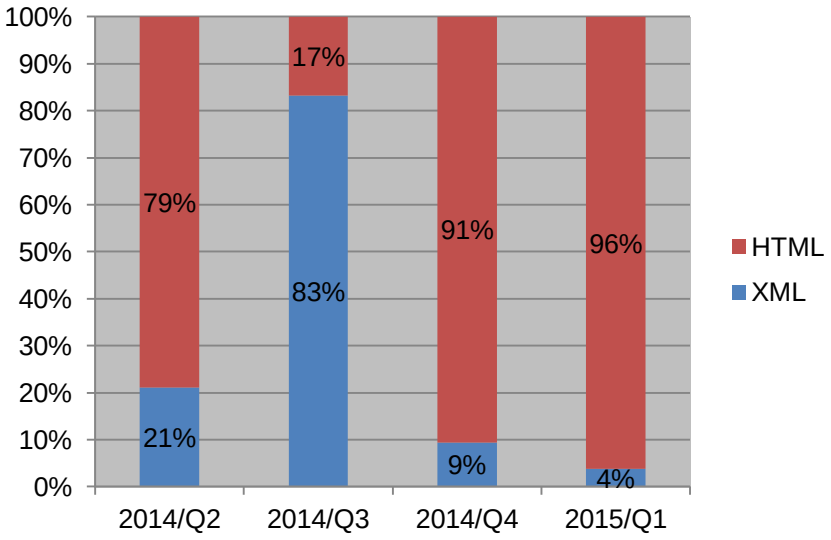


[図 2-6 VRDA フィード配信件数]



[図 2-7 VRDA フィード利用件数]

[図 2-7] に示したように、インデックスの利用数については、前四半期と比較し、大きな変化は見られませんでした。一方、脆弱性情報の利用数については、前四半期と比較し、2 倍以上に増加しました。



[図 2-8 脆弱性情報のデータ形式別利用割合]

[図 2-8] に示したように、本四半期の脆弱性情報のデータ形式別利用傾向については、前四半期と同様に HTML 形式が利用される割合が高い利用傾向が見られました。

3. 制御システムセキュリティ強化に向けた活動

3.1. 情報収集分析

JPCERT/CC では、制御システムにおけるセキュリティインシデントに関わる事例や標準化活動の動向、

その他セキュリティ技術動向に関するニュースや情報等を収集・分析し、必要に応じて国内組織等に情報提供を行っています。本四半期の情報収集分析活動の中で収集し分析した情報は 477 件でした。このうち、国内の制御システム関係者に影響があり、注目しておくべき事案を「参考情報」として、制御システムセキュリティ情報共有コミュニティ(注 1)に提供しました。

(注 1) JPCERT/CC が運営するコミュニティで、制御システム関係者を中心に構成されています。

本四半期は、次の参考情報を発行しました。

発行件数：2 件

2015-01-19 [参考情報] Phoenix Contact Software 社の ProConOs および MultiProg に認証関連の脆弱性に関する情報共有
2015-03-24 JPCERT-ICSAD-2015-0002 [参考情報] DLL ハイジャッキングの脆弱性に関する情報共有

また、海外での事例や、標準化動向などは JPCERT/CC からのお知らせとともに、制御システム関係者向けに月刊ニュースレターとして配信しています。

発行件数：3 件

2015-01-13 制御システムセキュリティセミナー開催のご案内
2015-02-06 制御システムセキュリティ関連情報 2015-0001
2015-03-06 制御システムセキュリティ関連情報 2015-0002

本ニュースレター配信先の制御システムセキュリティ情報共有コミュニティについては、現在 477 名の方にご登録いただいています。今後も内容の充実を図っていく予定です。参加資格や申込み方法については、次の Web ページをご参照ください。

制御システムセキュリティ情報共有コミュニティ
https://www.jpcert.or.jp/ics/ics-community.html

3.2. 制御システム関連のインシデント対応

本四半期における制御システムに関連するインシデントの報告件数は 1 件でした。
また、SHODAN をはじめとするインターネット・ノード検索システムにおいて制御システム機器や関連プロトコルに対応した機能拡張が進んでいて、攻撃されるリスクが高まっていることに対する対策として、「インターネット・ノード検索システム」等のインターネット上の公開情報を分析し、国内の制御システム等で外部から悪用されてしまう危険性のあるシステムの保有組織に対して情報を提供しました。こうした危険性のあるシステムに関する本四半期の情報提供件数は、3 件でした。

3.3. 関連団体との連携

SICE(計測自動制御学会)と JEITA(電子情報技術産業協会)、JEMIMA(日本電気計測器工業会)が定期的に開催している合同セキュリティ検討 WG(ワーキンググループ)に参加し、制御システムのセキュリティに関して専門家の方々と意見交換を行いました。

3.4. 制御システム向けセキュリティ自己評価ツールの配付情報

JPCERT/CC では、制御システムの構築と運用に関するセキュリティ上の問題項目を手軽に抽出し、バランスの良いセキュリティ対策を行っていただくことを目的として、簡便なセキュリティ自己評価ツールである日本版 SSAT(SCADA Self Assessment Tool)や J-CLICS(制御システムセキュリティ自己評価ツール)の配付を行っています。本四半期は、日本版 SSAT に関して 5 件、J-CLICS に関して 10 件の利用申込みがありました。直接配付件数の累計は、日本版 SSAT が 168 件、J-CLICS が 231 件となりました。

3.5. 制御システム用製品開発ベンダにおける脆弱性対応窓口の設置支援

2014 年 8 月に「参考資料：制御システム用製品の開発ベンダにおける脆弱性対応について」を公開したことにあわせて、国内の制御システム用製品の開発ベンダが、脆弱性情報を受け取る窓口を開設する支援活動を行っています。本四半期に、新たに脆弱性情報の窓口を設置し、製品開発者リストへの登録を行った制御システム製品開発ベンダはありませんでした。累計では 9 社となります。

3.6. 制御システムに関するセキュリティセミナーの開催

2014 年 12 月から 2015 年 2 月にかけて岡山、福岡、名古屋、東京で制御システムセキュリティセミナーを開催しました。本セミナーでは、制御システム環境におけるセキュリティ対策の必要性が叫ばれる中、どのように取り組んでいくべきなのかに関して弊センターが実施した情報収集や独自の調査結果を用いて、今後の対策を考える上で考慮すべき点について紹介を行いました。最終的に、本セミナーでは、74 名の方にご参加いただきました。

3.7. 制御システムセキュリティ情報共有ポータルサイトのリニューアル公開

2015 年 1 月 21 日に制御システムセキュリティ情報共有ポータルサイト「ConPaS(Control System Security Partner's Site)」をリニューアルしました。本リニューアルでは、システムのセキュリティ機能強化に加え、これまでの利用状況や利用者からの要望を踏まえて、利用者がコンテンツを活用し易くなるようメニューを再構成するとともに、コンテンツの拡充や解説の追加などを行いました。
これにより、制御システムセキュリティに関する文献等を収集し配列したライブラリとして、より活用し易い構成となりました。

制御システムセキュリティ情報共有ポータルサイトについて
https://www.jpcert.or.jp/ics/conpas/index.html

3.8. 制御システムセキュリティカンファレンス 2015 開催

2月12日(木)に東京(品川)で、制御システムセキュリティカンファレンス 2015を開催し、264名の方にご来場いただきました。今回で7回目となる本カンファレンスでは、「現状を理解し、将来に備える」をテーマに[表3-1]のようなプログラムで講演者の方々から制御システムセキュリティへの取組について講演いただき、今後のセキュリティ改善活動に繋がるような情報交換に役立つプログラム構成としました。プログラム等の詳細については、次のURLをご参照ください。

制御システムセキュリティカンファレンス 2015
https://www.jpcert.or.jp/event/ics-conference2015.html
制御システムセキュリティカンファレンス 2015 においての講演資料
https://www.jpcert.or.jp/present/#year2015

[図 3-1 制御システムセキュリティカンファレンス 2015 講演風景]

[表 3-1 講演内容]

(1) 「制御システムセキュリティの現在と展望 2015～この 1 年間を振り返って～」 JPCERT/CC 顧問 宮地 利雄
(2) 「Crouching Yeti から見る産業システム攻撃・諜報活動の高度化」 株式会社カスペルスキー ビジネスデベロップメントマネージャー 松岡 正人
(3) 「制御システムのセキュリティ確保へ向けて～横河電機グループの取り組み～」 横河電機株式会社 IA プラットフォーム事業本部共通技術開発センター センター長 井上 健

(4) 「セキュリティバリアデバイスのストレージ保護機能とその活用」 独立行政法人産業技術総合研究所 セキュアシステム研究部門制御システムセキュリティ研究グループ 戸田 賢二
(5) 「ユーティリティ制御システムのセキュリティへの対応 ～ICS Cybersecurity Incident Response andTroubleshooting Process～」 トヨタ自動車株式会社 プラント・環境生技部工場計画室 担当部長 高野 正利
(6) 「サイバー演習の有効性 ―レジリエントな組織づくりに向けて―」 国立大学法人名古屋工業大学 青山 友美
(7) 「ネットワークモニタリングシステム NIRVANA による制御システムへの攻撃検知」 独立行政法人情報通信研究機構 ネットワークセキュリティ研究所サイバーセキュリティ研究室 室長 井上 大介

4. 国際連携活動関連

4.1. 海外 CSIRT 構築支援および運用支援活動

海外の National CSIRT(Computer Security Incident Response Team)等のインシデント対応調整能力の向上を図るため、トレーニングやイベントでの講演等を通じた CSIRT の構築・運用支援を行っています。

4.1.1. ミャンマーCSIRT 構築支援等(2015 年 3 月 10 日-12 日)

JPCERT/CC は、ミャンマーの National CSIRT である mmCERT/CC のスタッフに対して、同組織の機能強化を目的としたトレーニングを、ミャンマーの旧首都ヤンゴンで計 3 日間に亘って行いました。mmCERT/CC のスタッフ等計 10 名が受講した本トレーニングでは、インシデントデータの収集や管理、分析に関するトレーニングや、Web サーバのログ解析のハンズオン研修を行いました。

[図 4-1 トレーニングの様子]

4.2. 国際 CSIRT 間連携

インシデント対応に関する海外の National CSIRT との間の連携の枠組みの強化、および各国のインターネット環境の整備や情報セキュリティ関連活動への取組の実施状況等に関する情報収集を目的として、国際連携活動等を行っています。また、APCERT や FIRST に参加し、主導的な役割を担う等、多国間の CSIRT 連携の取組にも積極的に参画しています。

4.2.1. APCERT(Asia Pacific Computer Emergency Response Team)

JPCERT/CC は、2003 年 2 月の APCERT 発足時から継続して Steering Committee(運営委員)のメンバに選出されており、また、事務局を担当しています。2011 年 3 月からは、議長チーム(現在 4 期目)としてさまざまな活動をリードしています。JPCERT/CC の APCERT における役割および APCERT の詳細については、次の Web ページをご参照ください。

JPCERT/CC within APCERT
https://www.jpcert.or.jp/english/apcert/

4.2.1.1. APCERT Steering Committee 会議の実施

Steering Committee は、1 月 28 日に電話会議を、また 3 月 2～3 日には APRICOT 2015 の開催にあわせ福岡にて会議を行い、今後の APCERT の運営方針等について議論しました。JPCERT/CC は議長チームおよび事務局として、これらの会議の主導およびサポートを行いました。

4.2.1.2. APCERT を代表しての会議出席

JPCERT/CC は 2 月 24 日から 3 月 6 日に開催された APRICOT 2015(以下「APRICOT」といいます。) に参加し、4 日に行われた APCERT による特別セッション枠" APCERT Security Day"において、「サイバースペースのリスク削減アプローチ」について講演しました。APRICOT についての詳細は、次の URL をご参照ください。

APRICOT 2015
https://2015.apricot.net/

4.2.1.3. APCERT 合同サイバー演習 (APCERT Drill 2015) に参加 (2015 年 3 月 18 日)

APCERT は、サイバー攻撃への即時対応能力を確認するため、合同サイバー演習を実施しました。本演習は、アジア太平洋地域で発生し、国境を越えて広範囲に影響を及ぼすインシデントへの対応における各経済地域 CSIRT 間の連携の強化を目的として、毎年実施されています。

11 回目となる今回の合同サイバー演習のテーマは、「家庭用のネットワーク機器を悪用した攻撃への対処」でした。APCERT の加盟チームのみならず、イスラム諸国のコンピュータ緊急対応チームである OIC-CERT からエジプト、チュニジア、モロッコも加わって、22 の経済地域から計 28 チームが参加しました。

JPCERT/CC は、この演習にプレーヤー(演習者)として参画するとともに、ExCon と呼ばれる演習の進行調整役も務め、スムーズな演習の実施を支えました。

4.2.2. FIRST (Forum of Incident Response and Security Teams)

JPCERT/CC は 1998 年の FIRST 加盟以来、積極的に活動に参加しています。現在は JPCERT/CC の国際部シニアアナリスト 小宮山功一朗が FIRST の Board of Directors のメンバを務めており、1 月 26 日-29 日にスペインのラスパルマスで開催された Board of Directors 会合に出席しました。FIRST および Board of Directors の詳細については、次の Web ページをご参照ください。

FIRST
http://www.first.org/

FIRST.Org,Inc., Board of Directors
http://www.first.org/about/organization/directors

4.2.3. Pacific Telecommunications Council 年次会合への参加(2015 年 1 月 18 日-21 日)

JPCERT/CC は 1 月 18 日から 21 日に米国のハワイで開催された、アジア太平洋地域の通信に関わる政府系・非政府系組織の集まりである Pacific Telecommunications Council の年次会合に参加しました。JPCERT/CC は、19 日の”Executive Insight Roundtable 4 - Managing Cyber Threats in East Asia”というセッションでパネリストとして登壇し、「サイバースペースのリスク削減アプローチ」について意見を述べました。

4.2.4. JICA 東京国際センターIT 研修生による実地見学の受入れ(2015 年 2 月 5 日)

JICA 東京国際センターで「情報セキュリティ政策能力向上コース」を受講中の研修生 12 名(カンボジア、ミャンマー、タイ、ラオス、ベトナム、インドネシア、フィリピンの政府系組織の IT 担当者等)が来訪しました。CSIRT の役割や JPCERT/CC の事業紹介、最近のインシデント動向、重要インフラ防護に向けた JPCERT/CC の取組み等を JPCERT/CC から説明した後、活発な意見交換が行われ、日本および各国におけるインターネットセキュリティ対策の状況が共有されました。

4.2.5. 豪 CERT Australia への訪問 (2015 年 2 月 12 日)

JPCERT/CC は、2 月 12 日、オーストラリアの CERT Australia のキャンベラオフィスを訪問し、今後の両者の連携について意見交換を行いました。会合では、CERT Australia、JPCERT/CC それぞれの活動状況を紹介し、また国際 CSIRT コミュニティにおける連携等について協議し、今後も密な連携を維持することを確認しました。

4.3. その他の活動ブログや Twitter を通した情報発信

英語ブログ(http://blog.jpcert.or.jp/)や Twitter(@jpcert_en)を利用し、日本やアジア太平洋地域の情報セキ

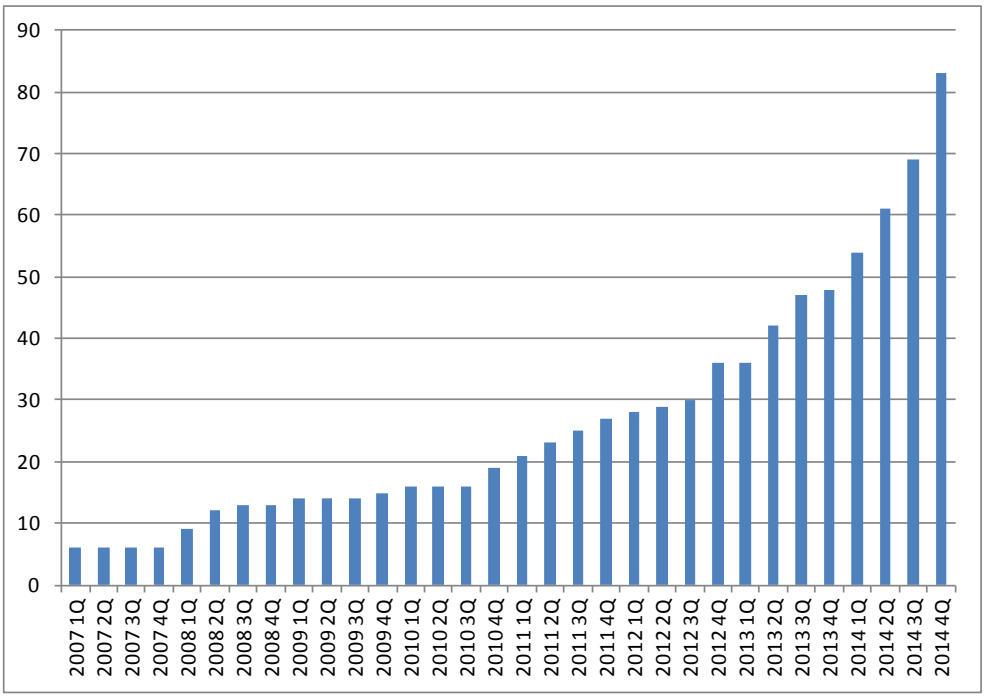
ュリティに関する状況や JPCERT/CC の活動等について継続的に情報発信を行っています。本四半期は次の記事をブログに掲載しました。

AfricaCERT Workshop and Training in Mauritius (2015 年 1 月 15 日)
http://blog.jpcert.or.jp/2015/01/africacert-workshop-and-training-in-mauritius.html
Analysis of a Recent PlugX Variant - “P2P PlugX” (2015 年 1 月 29 日)
http://blog.jpcert.or.jp/2015/01/analysis-of-a-r-ff05.html
A New UAC Bypass Method that Dridex Uses (2015 年 2 月 13 日)
http://blog.jpcert.or.jp/2015/02/a-new-uac-bypass-method-that-dridex-uses.html
Control System Security Conference 2015 (2015 年 3 月 30 日)
http://blog.jpcert.or.jp/2015/03/control-system-security-conference-2015.html

5. 日本シーサート協議会(NCA)事務局運営

日本シーサート協議会(NCA：Nippon CSIRT Association)は、国内のシーサート(CSIRT：Computer Security Incident Response Team)組織が互いに協調し、連携して共通の問題を解決する場として設立されました。その事務局として、JPCERT/CC は、NCA の Web サイトの管理や更新を通じた広報活動、協議会の問合せ窓口やメーリングリストを含む会員情報の管理、加盟のためのガイダンスの実施および手続きの運用を担当するとともに、自らも会員として協議会の活動に参加しています。

本四半期においては、ダイハツ工業株式会社 (D-SIRT)、キーウェアサービス株式会社(KEYWARE-CSIRT)、日本電気株式会社 (NEC-CSIRT)、国立情報学研究所 (NII CSIRT)、キヤノン株式会社 (Canon-CSIRT)、株式会社ジェーシービー (JCB-CSIRT)、スルガ銀行株式会社 (SURUGA CSIRT)、住友生命保険相互会社(SUMISEI-CSIRT)、森ビル株式会社(MB-SIRT)、TDC ソフトウェアエンジニアリング株式会社(TDC-CSIRT)、株式会社京都銀行(KB-CSIRT)、株式会社 KADOKAWA(KADOKAWA-CSIRT)西日本電信電話株式会社(NTT WEST-CIRT)、損保ジャパン日本興亜ホールディングス株式会社(SOMPO HD CSIRT)、明治安田生命保険相互会社(MY-SIRT)、日本ユニシス株式会社(UCSIRT)の 9 組織が新規に加盟しました。本四半期末時点で 83 の組織が加盟しています。これまでの参加組織数の推移は[図 5-1]のとおりです。



[図 5-1　日本シーサート協議会 加盟組織数の推移]

3 月に「第 9 回臨時総会＆第 15 回ワーキンググループ会」を開催いたしました。

2015 年 3 月 6 日 (金) 14:00-17:30
会場：富士ゼロックス株式会社会場
参加人数：186 名

協議会運営規約の一部改定を第 9 回臨時総会に諮り、可決されました。また、第 15 回ワーキンググループ会を臨時総会直後に開催し、各ワーキンググループの活動報告や、新規に加盟した 14 組織からのチーム紹介が行われました。本四半期末現在 83 組織が加盟していますが、来年度には 100 組織を超えると予想され、各 WG でも登録者が増えて活発な活動が行われることになりそうです。今後の課題として、会員数の増加に伴って増加する事務局業務の効率化を検討する必要があります。

日本シーサート協議会の活動の詳細については、次の Web ページをご参照ください。

日本シーサート協議会
http://www.nca.gr.jp/

6. フィッシング対策協議会事務局の運営

JPCERT/CC は、フィッシング対策協議会(以下「協議会」といいます。)の事務局を担当しており、経済産業省からの委託により、協議会における各ワーキンググループ活動の運営や、協議会名での一般消費者

からのフィッシングに関する報告・問合せの受付、報告に基づくフィッシングサイトに関する注意喚起等の活動を行っています。

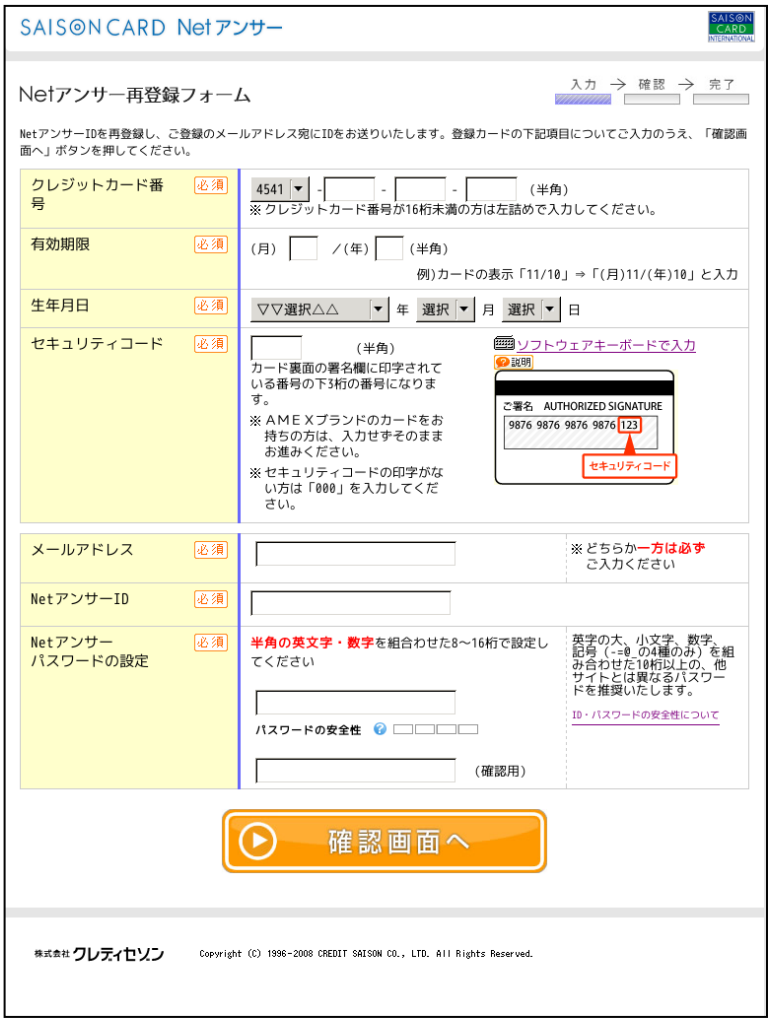
6.1. 情報収集/発信の実績

本四半期は、協議会 Web サイトや会員向け ML を通じて、フィッシングに関するニュースや緊急情報を 21 件発信しました。

本四半期も、金融機関をかたるフィッシングや通信事業者をかたるフィッシングのサイトが新たに見つかったとの報告を受けました。特にオンラインゲーム事業者をかたるフィッシングについては、本四半期に数千件の報告を受けました。協議会では、名前をかたられた事業者に、メール本文やサイトの URL 等の関連情報を提供しました。また、金融機関をかたるフィッシングに関しては[図 6-1]の「[2015 年 1 月 23 日新規] 三菱東京 UFJ 銀行をかたるフィッシング」の 1 件、クレジットカード会社をかたるフィッシングに関しては[図 6-2]の「[2015 年 3 月 23 日新規] セゾン Net アンサーをかたるフィッシング」など 2 件、オンラインゲーム事業者をかたるフィッシングに関しては[図 6-3]の「[2015 年 3 月 20 日新規] ハンゲームをかたるフィッシング」など 3 件、合計 6 件の緊急情報を協議会の Web 上で公開し、広く注意を喚起しました。

[図 6-1 [新規] 三菱東京 UFJ 銀行をかたるフィッシング(2015/01/23)
https://www.antiphishing.jp/news/alert/ufj20150123.html]

さらに、これらフィッシングに使用されたサイトを停止するための調整を、JPCERT/CC のインシデント対応支援活動を通じて行い、すべてについて停止を確認しました。



[図 6-2 [新規] セゾン Net アンサーをかたるフィッシング (2015/03/23)
https://www.antiphishing.jp/news/alert/saison20150323.html]

[図 6-3　[新規] ハンゲームをかたるフィッシング (2015/03/20)
https://www.antiphishing.jp/news/alert/hangame20150320.html]

6.2. 講演活動

協議会では、フィッシングに関する現状を紹介し、効果的な対策を呼び掛けるための講演活動を行っています。本四半期は次の講演を行いました。

(1)駒場一民：
「最新のフィッシング動向と対策について」
神奈川県クレジットカード犯罪対策連絡協議会, 2015 年 2 月 25 日
(2)小宮山功一朗：
「金融機関ウェブサイトのフィッシング被害軽減にむけた研究報告会」
日欧 ICT 国際共同研究プロジェクト NECOMA,2015 年 3 月 19 日

6.3. フィッシング対策協議会の活動実績の公開

協議会の Web サイトにおいて、報告されたフィッシングサイト数を含む、毎月の活動報告等を公開しています。詳細については、次の Web ページをご参照ください。

フィッシング対策協議会 Web ページ
https://www.antiphishing.jp/
フィッシング対策協議会 2015 年 1 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201501.html
フィッシング対策協議会 2015 年 2 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201502.html
フィッシング対策協議会 2015 年 3 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201503.html

7. フィッシング対策協議会の会員組織向け活動

フィッシング対策協議会では、経済産業省から委託された活動以外に、会費による会員組織向けの活動を、運営委員会の決定に基づいて行っています。

7.1. 運営委員会開催

本四半期においては、フィッシング対策協議会の活動の企画・運営方針の決定等を行う運営委員会を次のとおり開催しました。

(1) フィッシング対策協議会 第 22 回運営委員会
日時：2015 年 1 月 16 日 16:00 - 18:00
場所：トッパン・フォームズ株式会社

(2) フィッシング対策協議会 第 23 回運営委員会
日時：2015 年 2 月 13 日 16:00 - 18:00
場所：日立システムズ株式会社

(3) フィッシング対策協議会 第 24 回運営委員会
日時：2015 年 3 月 13 日 16:00 - 18:00
場所：ネットスター株式会社

8. 公開資料

JPCERT/CC が本四半期に公開した調査・研究の報告書や論文、セミナー資料は次のとおりです。

8.1. 分析センターだより

JPCERT/CC では、インシデントに関連して報告いただいた情報や収集した情報を調査し、インシデントをもたらした攻撃の手法やその影響を把握するアーティファクト分析という活動を行っています。分析技術者が日々のアーティファクト分析業務の中で感じたこと、発見したことを中心に執筆した「分析センターだより」として新たに 3 つの話題を公開しました。

(1) 縮小表示プレビューに偽装したアイコンをもつマルウエア (2015/03/19)
アイコン偽装はユーザによるマルウエアの実行を誘う古典的な手法ですが、最近の OS に実装されている縮小表示プレビュー機能を模倣するアイコン偽装についてまとめました。

縮小表示プレビューに偽装したアイコンをもつマルウエア (2015/03/19)
https://www.jpcert.or.jp/magazine/acreport-thumbnailicon.html

(2) Dridex が用いる新たな UAC 回避手法 (2015/02/09)
攻撃者がより高い権限を掌握する手段の一つとして、ユーザーアカウント制御(UAC)の回避があります。マルウエアが使う 2 種類の UAC 回避手法について紹介しました。

Dridex が用いる新たな UAC 回避手法(2015/02/09)
https://www.jpcert.or.jp/magazine/acreport.html

(3) マルウエア PlugX の新機能 (2015/01/29)
標的型攻撃で使われる代表的なマルウエアのひとつである PlugX について、最近報告されている検体の特徴をまとめました。

マルウエア PlugX の新機能(2015-01-22)
https://www.jpcert.or.jp/magazine/acreport-plugx.html

8.2. 脆弱性関連情報に関する活動報告レポート

IPA と JPCERT/CC は、ソフトウエア等脆弱性関連情報取扱基準(現行版は平成 26 年経済産業省告示 第 10 号)に基づき、2004 年 7 月から受付機関(IPA)や調整機関(JPCERT/CC)として脆弱性関連情報流通制度の一端を担っています。
本レポートは、2015 年 10 月 1 日から 2014 年 12 月 31 日までの活動実績と、本四半期に届出ないし公表された脆弱性に関する注目すべき動向についてまとめたものです。

ソフトウェア等の脆弱性関連情報に関する活動報告レポート[2014 年第 4 四半期(10 月～12 月)]
(2015 年 01 月 28 日)
https://www.jpcert.or.jp/press/2015/vulnREPORT_2014q4.pdf

8.3. インターネット定点観測レポート

JPCERT/CC では、インターネット上に複数のセンサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類して分析するインターネット定点観測を継続的に実施しています。これを、脆弱性情報、マルウエアや攻撃ツールの情報などを参考に分析することで、攻撃活動や準備活動の捕捉に努めています。
本レポートは、インターネット定点観測の結果を四半期ごとにまとめたものです。

インターネット定点観測レポート 2014 年 10 月～12 月
(2015 年 01 月 28 日)
https://www.jpcert.or.jp/tsubame/report/report201410-12.html

8.4. IPv6 セキュリティテスト手順書および検証済み製品リスト(2015/01/15)

「IPv6 セキュリティテスト手順書」に従って IPv6 対応機器ベンダが検証した結果をリスト化した「IPv6 セキュリティテスト検証済み製品リスト(2014/08/01)」を公開しました。これは、IPv6 対応機器の購入を検討されている企業や組織のシステム担当者の方に、機器選定時の参考資料としてご利用いただくことを目的としています。本四半期は、新たに 2 製品の検証結果を追加して改版し、1 月 15 日に公開しました。

IPv6 セキュリティテスト検証済み製品リスト
(2015 年 01 月 15 日公開)
https://www.jpcert.or.jp/research/ipv6product_list.html

9. 主な講演活動一覧

(1) 真鍋 敬士(理事・分析センター長)：
「サイバー攻撃の傾向と対応への課題」
NTT コミュニケーションズ株式会社　情報セキュリティ研修,2015 年 03 月 27 日

(2) 早貸 淳子(専務理事)：
「2020 年に向けた我が国の情報課題と 企業・生活者の対応策～サイバーセキュリティ、 個人情報保護、マイナンバー等～」
公益財団法人 日本生産性本部 情報化推進国民会議　情報化シンポジウム・イン・東京,2015 年 03 月 17 日

(3) 小林 裕士(インシデントハンドリンググループ 情報セキュリティアナリスト)
「最新のサイバーインシデント情勢とログ設定について」
サイバー空間の脅威に対する新潟県産学官民合同対策プロジェクト推進協議会
人材育成・対処能力向上分科会及びサイバー攻撃対策分科会合同分科会,2015 年 02 月 27 日

(4) 村上 晃(経営企画室 兼 エンタープライズサポートグループ部門長):
「未知の脅威とインシデント事後対応の重要性 ～ 転ばぬ先の杖から転んだ後の杖～」
日経 BP 社 ITpro Active 製品選択支援セミナー「未知の脅威」への対策】,2015 年 02 月 27 日

(5) 山内 徹(主席研究員)
「サイバーセキュリティー高度化・複雑化するサイバー攻撃への対応ー」
独立行政法人製品評価技術基盤機構,2015 年 02 月 19 日

(6) 竹田 春樹(分析センター リーダ)
「セキュリティ担当者が知っておくべきサイバー攻撃の脅威」
一般社団法人日本クレジット協会 平成２６年度 第６回 カードセキュリティ研究部会,
2015 年 2 月 13 日

(7) 村上 晃(経営企画室 兼 エンタープライズサポートグループ部門長):
「CSIRT 構築の事例と勘所を知る ～“百社百様”ひとつとして同じものはない～」
ITmedia エグゼクティブ勉強会,2015 年 01 月 22 日

10. 主な執筆一覧

(1) 重森 友行(執筆当時：早期警戒グループ 情報セキュリティアナリスト):
「第 1 回 メールや Web 経由で侵入、端末の乗っ取りを図る」
「第 2 回 ドメイン管理者の認証情報が狙われる」
「第 3 回 ポイントは「アカウント管理」と「早期検知」」
「第 4 回 イベントログを精査、攻撃の痕跡を見つける」
日経 BP 社 ITpro 特集記事 「Active Directory が危ない！標的型攻撃から守れ」,2015 年 03 月 23 日～26 日

(2) 松本 悦宜 (執筆当時：早期警戒グループ 情報セキュリティアナリスト):
「2014 年の情報セキュリティ動向」
Impree R&D「インターネット白書 2015」,2015 年 02 月 03 日

11. 開催セミナー等一覧

(1) 制御システムセキュリティカンファレンス2015
制御システムにおける脅威の現状を紹介しつつ、今できる対策、将来に向けて研究が進められている対策技術について紹介し、制御システムセキュリティ向上に向けた行動を具体的に検討するための情報を共有することを目的にカンファレンスを開催しました。

・主 催：経済産業省
一般社団法人JPCERT コーディネーションセンター
・開催日時：2015年2月12日(木) 10:00～17:00
・参加人数：264名

詳細については、次のWebページ をご参照ください。
制御システムセキュリティカンファレンス2015
https://www.jpcert.or.jp/event/ics-conference2015.html

12. 協力、後援一覧

本四半期は、次の行事の開催に協力または後援をしました。

(1) Security Days 2015
主 催：株式会社ナノオプト・メディア
開催日：2015年3月5日(木)～3月6日(金)
(2) JSSEC スマートフォン セキュリティ・シンポジウム2015
主 催：一般社団法人日本スマートフォンセキュリティ協会(JSSEC)
開催日：2015年2月26日(木)

■インシデントの対応依頼、情報のご提供
info@jpcert.or.jp
https://www.jpcert.or.jp/form/
PGP Fingerprint ： FC89 53BB DC65 BD97 4BDA D1BD 317D 97A4 69EC E048
■制御システムに関するインシデントの対応依頼、情報のご提供
icsr-ir@jpcert.or.jp
https://www.jpcert.or.jp/ics/ics-form.html
PGP Fingerprint ： B3C2 A91C AE92 50A9 BBB2 24FF B313 E0E1 0DDE 98C1
■脆弱性情報ハンドリングに関するお問い合わせ ：vultures@jpcert.or.jp
■制御システムセキュリティに関するお問い合わせ ：icsr@jpcert.or.jp
■セキュアコーディングセミナーのお問い合わせ ：seminar-secure@jpcert.or.jp
■公開資料、講演依頼、資料使用、その他のお問い合わせ：office@jpcert.or.jp