JPCERT-PR-2011-0001
発行日 : 2011-01-12

JPCERT/CC 活動概要 [2010 年 10 月 1 日 ～ 2010 年 12 月 31 日]

【活動概要トピックス】

—トピック 1 —
Web アクセス解析サービス基盤を悪用した新しいタイプの攻撃に関する注意喚起

JPCERT/CC では、インシデント報告の受付業務や脆弱性等の脅威情報収集活動において観察される脅威の動向の中で特に警戒を要すると思われるものについて注意喚起を行っています。10 月には、Web アクセス解析サービス基盤を悪用した攻撃が確認され、これに対する注意喚起を行いました。

一般的にアクセス解析サービスを利用する Web サイトは、サイトへのアクセスを解析するためにコンテンツ（html ファイル）内にアクセス情報収集サーバのプログラムを呼び出すスクリプトを含んでいます。アクセス解析サービスを経由した攻撃では、アクセス解析サーバ上のプログラムを改ざんすることにより、当該アクセス解析サービスを委託しているすべての Web サイトをマルウエアに感染させるサイトに作り変えます。

この攻撃に対する直接的な対策を取るべきはアクセス解析サービス事業者ですが、一義的な被害者は、サービス契約をしている Web サイトに訪問した利用者であり、その間に Web サイト運営者が介在するため、責任の所在が不明確になるなど、注意を要するサービスを特定するための情報の提供方法に難しさが生じました。

JPCERT/CC においては、本来は、具体的な対策をとることができる情報を注意喚起として発行するのが原則ですが、一般利用者に広く被害が及ぶ可能性がある事案については、必ずしも十分な具体性を有する情報を公開することができない場合であっても、アクセス解析サービス事業者の対策を促すとともに、一般のウェブ利用者の基本的なマルウエア耐性の向上策が講じられることを期待して、可能な範囲の情報を公開して注意喚起を行うことで被害の拡大防止に努めています。

アクセス解析サービスを使用した Web サイト経由での攻撃に関する注意喚起
https://www.jpcert.or.jp/at/2010/at100028.txt

―トピック 2 ―

アジア各地でセキュアコーディングセミナーを開催

JPCERT/CC は、10 月にインド(デリー、バンガロール)、11 月にベトナム（ハノイ）、12 月にフィリピン（マニラ）において、各国の National-CSIRT の協力を得て、現地のエンジニアをターゲットとした C/C++セキュアコーディングセミナーを開催しました。ベトナムは昨年度に続き 2 回目の開催であり、昨年度同様のセミナーを開催したタイとインドネシアを加えると、日本企業のオフショア開発先となっている主な国々を、中国を除き、概ね一巡したことになります。オフショア開発の相手国として、またこれからの発展が期待される新興国市場としても重要度が高まるアジア地域で、ソフトウエアセキュリティに関するノウハウを提供することは、日本の情報産業市場にとっても意義のある活動であると認識しています。
セミナーは演習やコードレビューなどを取り入れた実践的なものであり、「多くの新しい学びがあった」等の感想に象徴されるように、事後アンケートでも高い評価を得ました。第二ラウンドとも言える次年度以降については、より広い技術普及をめざして工夫を加えた形での活動の継続を検討していきたいと考えています。

セキュアコーディング
https://www.jpcert.or.jp/securecoding.html

―トピック 3 ―

アフリカ諸国向け CSIRT トレーニングを実施―AfriNIC-13

JPCERT/CC は、11 月に開催されたアフリカ地域のインターネット関係者による国際会議 AfriNIC-13 に参加するとともに、3 日間にわたるアフリカ諸国向けの CSIRT トレーニングや、経営層や政府の政策担当者向けのワークショップの講師を務めました。AfriNIC-13 は、アフリカ地域におけるインターネット関連の事業者が、国際的なベストプラクティスや技術動向を議論するイベントで、今回は、南アフリカのヨハネスブルグで開催されました。CSIRT トレーニングは、その一環として、アジア地域との連携を促進する AAF（Africa Asia Forum on Network Research & Engineering）が主催したプログラムです。JPCERT/CC は、トレーニングの講師として参加するだけでなく、アフリカ各国の政府関係者、セキュリティ対策機関、ISP らと CSIRT 業務の連携方法の確認、意見交換など協力体制の構築につながる活動に努めました。
今後、急速にモバイル端末を含めたネットワーク利用の拡大が予想される一方で、ほとんどの国に CSIRT が存在しないアフリカ地域は、世界のサイバーインシデントの発生源となることが懸念される地域です。この地域のサイバーセキュリティが著しく悪化すれば、日本も、それと無縁ではいられないと考えられます。JPCERT/CC では、日本に関連したインシデントがアフリカ地域で発生した場合のインシデントレスポンスを円滑に進めるための連携体制の強化に向けての基盤作りにも努めています。

JPCERT CC®

—活動概要—

目次

本活動は、経済産業省より委託を受け、「平成２２年度コンピュータセキュリティ早期警戒体制の整備（不正アクセス行為等対策業務）」事業として実施したものです。
ただし、「平成２２年度コンピュータセキュリティ早期警戒体制の整備（フィッシング対策協議会運営）」事業として経済産業省から受託して実施した「**5.フィッシング対策協議会事務局の運営**」に記載の活動については、この限りではありません。
また、「**7.講演活動一覧**」及び「**8.執筆・執筆記事一覧**」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。

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 2374 件、インシデント件数ベースでは 2638 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ます。ただし、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は 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 731 件でした。前四半期の 701 件と比較して約 4%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などに対し、現状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、国際的な調整・支援が必要となるインシデントにおいて、日本の窓口組織として、国内や国外 (海外の CSIRT など) の関係機関と調整活動を行っています。この活動を通じて、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しています。

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/2011/IR_Report20110112.pdf

1-1-1. インシデントの傾向

本四半期は、10 月に多くの「フィッシングサイト」の報告をいただきました。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、538 件で、前四半期の 487 件から約 10%増加しました。また、前年度同四半期（336 件）との比較では、約 60%の増加となっています。
本四半期のフィッシングサイトが装っていたブランドの国内・国外別の内訳を[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	10 月	11 月	12 月	国内外別合計（割合）
国内ブランド	177	88	19	284 (53%)
国外ブランド	58	91	53	202 (37%)
国内外の別不明	17	19	16	52 (10%)
月別合計	252	198	88	538(100%)

本四半期は、グローバルにサービスを提供しているクレジットカード会社を装ったフィッシングサイトを数多く報告いただいたため、国外ブランドを装ったフィッシングサイトの件数が 202 件と、前四半期の 123 件から 64 % 増加しました。なお、国内のブランドを装ったフィッシングサイトの件数も、284 件と、前四半期の 278 件から微増しています。

本四半期のフィッシングサイトの調整先は、国内が 53%、国外が 47%でした。前四半期の割合（国内 62%、国外 38%）と比較して、本四半期は国外との調整が増えました。これは、前述のグローバルにサービスを提供しているクレジットカード会社を装ったフィッシングサイトの多くが国外に設置されていたためです。

本四半期に報告が寄せられた Web サイト改ざんの件数は、199 件でした。前四半期の 353 件から約 44%減少しています。これは、いわゆる Gumblar による Web サイト改ざんに関する報告が、11 月頃から減少したためです。いわゆる Gumblar の減少については、一部の亜種の攻撃がおさまってきており、世間での注目度が下がっていることも一因になっています。一方で 11 月ころから報告いただいている Web サイト改ざんでは、Internet Explorer の未修正の脆弱性を悪用した攻撃や、Java の脆弱性を悪用する、より脅威度の高い攻撃が確認されています。JPCERT/CC では、これらの攻撃の分析を行い、攻撃において中核となっていたサイトを停止させる対応を行っています。

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元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及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を対象としたコンピュータウイルス、Web 改ざんなどのサイバー攻撃に関する情報を収集、分析しています。これらの様々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なども併せて行いながら、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」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」など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 のホームページ、RSS、約 25,000 名の登録者を擁するメーリングリストなどを通じて、本四半期においては、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などに関する次のような情報を提供しました。

発行件数：11 件　https://www.jpcert.or.jp/at/

2010-10-01　攻撃用ツールキットを使用した Web サイト経由での攻撃に関する注意喚起
2010-10-06　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起
2010-10-13　2010 年 10 月 Microsoft セキュリティ情報 (緊急 4 件含) に関する注意喚起
2010-10-27　アクセス解析サービスを使用した Web サイト経由での攻撃に関する注意喚起
2010-10-27　アクセス解析サービスを使用した Web サイト経由での攻撃に関する注意喚起 (更新)
2010-11-05　Adobe Flash Player の脆弱性に関する注意喚起
2010-11-10　2010 年 11 月 Microsoft セキュリティ情報 (緊急 1 件含) に関する注意喚起
2010-11-17　Adobe Reader 及び Acrobat の脆弱性に関する注意喚起
2010-12-09　不適切な設定で Asterisk を利用した場合に発生し得る不正利用に関する注意喚起
2010-12-15　不適切な設定で Asterisk を利用した場合に発生し得る不正利用に関する注意喚起 (更新)
2010-12-15　2010 年 12 月 Microsoft セキュリティ情報 (緊急 2 件含) に関する注意喚起

1-2-1-2. Weekly Report

JPCERT/CC が得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）**に発行しています。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/

JPCERT/CC レポート内で扱った情報セキュリティ関連情報の項目数は、合計 86 件、「今週のひとくちメモ」のコーナーで紹介した情報は以下の 12 件でした。

2010-10-06　National Cyber Security Awareness Month 2010
2010-10-14　PostgreSQL のサポートポリシー
2010-10-20　JP ゾーンの DNSSEC 署名開始
2010-10-27　マイクロソフトセキュリティインテリジェンスレポート 第 9 版
2010-11-04　導入済みソフトウエアのアップデートに注意
2010-11-10　夏時間 (Daylight Saving Time)
2010-11-17　踏み台にされる Web サイト～いわゆる Gumblar の攻撃手法の分析調査～
2010-11-25　Adobe Reader のサポート期間に注意
2010-12-01　Microsoft EMET
2010-12-08　Exchange Server 2000 と SQL Server 7.0 のサポート期間に注意
2010-12-15　担当者が選ぶ 2010 年の重大ニュース
2010-12-22　最新版ブラウザのセキュリティ

1-2-2. 脅威の動向について

本四半期も、いわゆる Gumblar をはじめとする、Web サイトやそこで使われる外部コンテンツが汚染され、閲覧した利用者が被害を受ける攻撃活動が報告されました。サイト管理者は、適切にサイトを管理できているか、利用者は閲覧に使っているブラウザやプラグインが適切なバージョンを使っているか、今一度確認することをおすすめします。

10 月には、Web アクセス解析サービス基盤を悪用した攻撃が確認されました。一般的にアクセス解析サービスを利用する Web サイトは、サイトへのアクセスを解析するためにコンテンツ（html ファイル）内にアクセス情報収集サーバのプログラムを呼び出すスクリプトを含んでいます。アクセス解析サービスを経由した攻撃では、アクセス解析サーバ上のプログラムを改ざんすることにより、当該アクセス解析サービスを委託しているすべての Web サイトをマルウエアに感染させるサイトに作り変えます。そのため、当該 Web サイトを閲覧した、脆弱性のある古いソフトエアを使用しているコンピュータがマルウエアに感染する事態となりました。

12 月には、Twitter などで利用される短縮 URL サービスによる URL を使用した攻撃も発生しています。Twitter では、140 文字という文字数制限のため短縮 URL がよく使用されますが、短縮 URL サービスによる URL はアクセスしようとしているサイトのドメイン・アドレスを事前に確認することが困難なため、ツイートの内容とは異なるフィッシングサイトやマルウエアなどを仕込んだサイトなどへの誘導路となっている可能性があります。

また、本四半期には、APEC JAPAN 2010 や中国漁船拿捕に関する動画データの公開、朝鮮半島の情勢悪化など、国際的なイベントの開催や事案の発生により、国内の重要インフラ組織などに対するサイバー攻撃が危惧されました。JPCERT/CC では、これら事案に伴うサイバー攻撃への対応を目的とした情報収集を行い、国内重要インフラ組織などとの情報共有、連携を行うとともに、各国 CSIRT からの情報収集や連携体制の再確認を行いました。

1-3. インターネット定点観測システム(ISDAS)

インターネット定点観測システム (以下「ISDAS」といいます。) では、インターネット上に設置した複数のセンサーから得られるポートスキャン情報を収集しています。これらの観測情報は、公開されている脆弱性情報などとあわせて、インターネット上のインシデントの脅威度などを総合的に評価するために利用しています。また、観測情報の一部は JPCERT/CC Web ページなどでも公開しています。

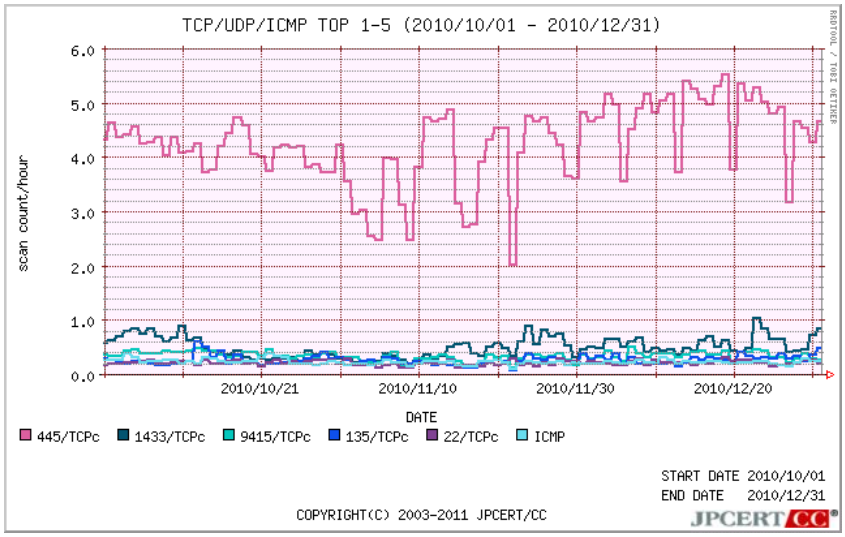
1-3-1. ポートスキャン概況

インターネット定点観測システムの観測結果は、ポートスキャンの頻度や内訳の推移を表すグラフとして JPCERT/CC の Web ページを通じて公開しています。アクセス先ポート別グラフは、各センサーに記録されたアクセス先ポートごとのスキャン件数の平均値を表しています。

JPCERT/CC インターネット定点観測システムの説明
https://www.jpcert.or.jp/isdas/readme.html

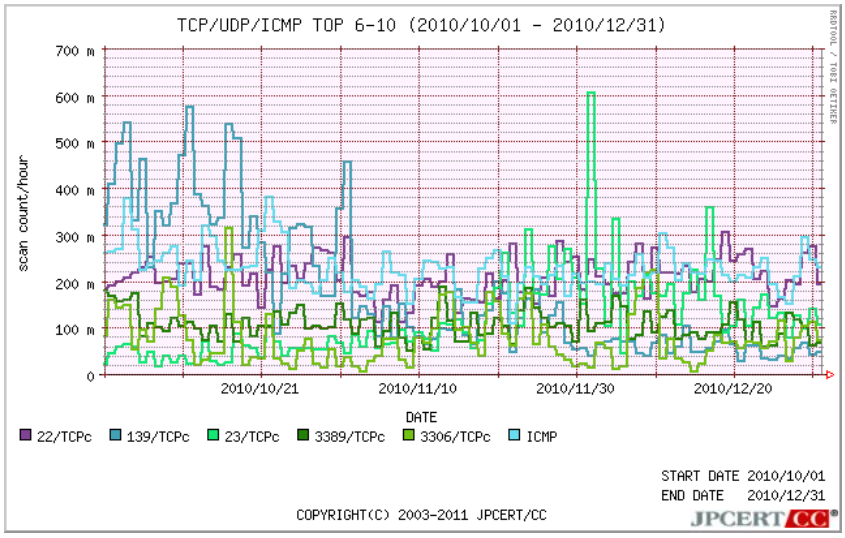
本四半期に ISDAS で観測されたアクセスの宛先ポートの上位 1 位～5 位および 6 位～10 位のそれぞれについて、アクセス数の時間的の推移を[図 1-1]と[図 1-2] に示します。

- アクセス先ポート別グラフ top1-5 (2010 年 10 月 1 日-12 月 31 日)



[図 1-1　アクセス先ポート別グラフ top1-5]

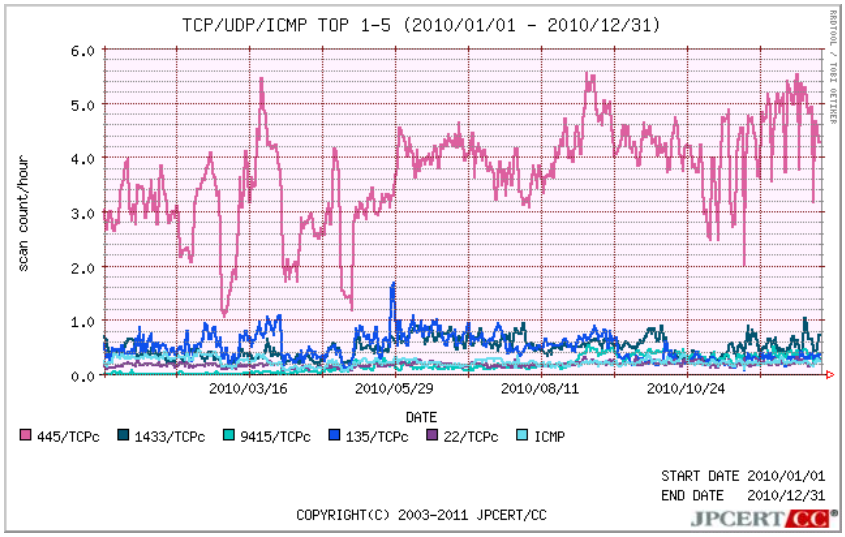
- アクセス先ポート別グラフ top6-10 (2010 年 10 月 1 日-12 月 31 日)



[図 1-2　アクセス先ポート別グラフ top6-10]

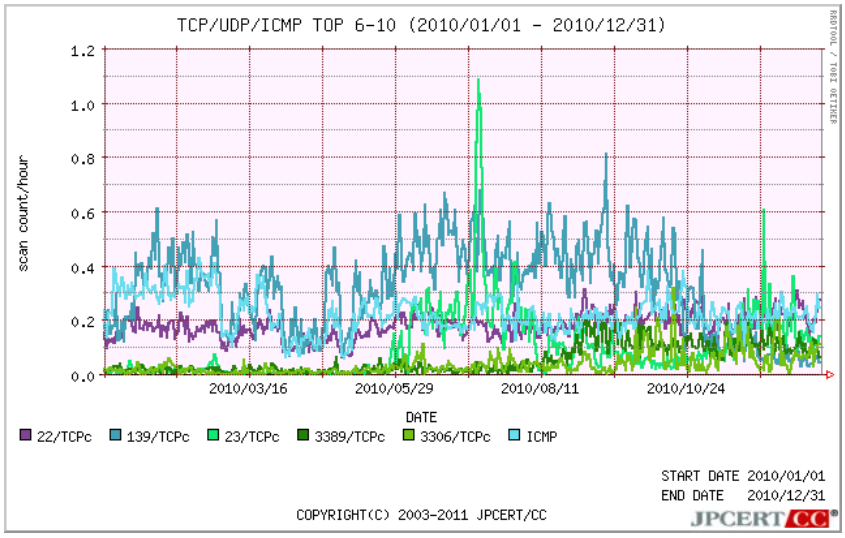
また、より長期間のスキャン推移を見るため、2010 年 1 月 1 日から 2010 年 12 月 31 日までの期間における、アクセスの宛先ポートの上位 1 位～5 位および 6 位～10 位のそれぞれについて、アクセス数の時間的の推移を[図 1-3]と[図 1-4]に示します。

- アクセス先ポート別グラフ top1-5 (2010 年 1 月 1 日-2010 年 12 月 31 日)



[図 1-3 アクセス先ポート別グラフ top1-5]

- アクセス先ポート別グラフ top6-10 (2010 年 1 月 1 日-2010 年 12 月 31 日)



[図 1-4 アクセス先ポート別グラフ top6-10]

引き続き Windows や Windows 上で動作するソフトウエアへの Scan 活動に加え、Telnet、SSH サーバやターミナルサービスなどコンピュータを遠隔操作で使う場合に、サーバ側が待ち受けているポートへの Scan 活動が増えています。そのほか、アクセス制御が不十分な、OpenProxy サーバや、SIP サーバへの Scan も引き続き観測しています。OS やアプリケーションに脆弱性を修正する修正プログラムを適用しているか、ファイアウォールやウイルス対策ソフトなどが正しく機能しているか、強固な認証方法を使っているか、今一度確認することが重要です。

1-4. 日本シーサート協議会 (NCA) 事務局運営

JPCERT/CC は、国内のシーサート(CSIRT: Computer Security Incident Response Team) 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た日本シーサート協議会（Nippon CSIRT Association: NCA）の事務局として、協議会の問合せ窓口、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の運用、Web ページ、メーリングリストの管理等の活動を行っています。
2010 年 12 月には、日本シーサート協議会主催で国際連携 Workshop を開催しました。海外セキュリティ機関（The Honeynet Project[1]、Shadowserver[2]の 2 組織）の技術者を招聘し、1 日目はハニーポットで収集したデータの分析やマルウエアの実態把握を行う研修が行われました。2 日目は The Honeynet Project、Shadowserver の活動の紹介のほか、JPCERT/CC からは中国におけるインターネット事情について講演しました。

日本シーサート協議会の活動の詳細については、以下の URL をご参照ください。

日本シーサート協議会 Web ページ
http://www.nca.gr.jp/

インシデントの報告方法の詳細
https://www.jpcert.or.jp/form/

インシデントの報告 （Web フォーム）
https://form.jpcert.or.jp/

1 1999 年に設立されたコンピュータセキュリティや情報心理学の専門家などで構成される非営利団体。ハニーポットの開発や運用、情報の分析などを行っている。
The Honeynet Project (http://www.honeynet.org/)

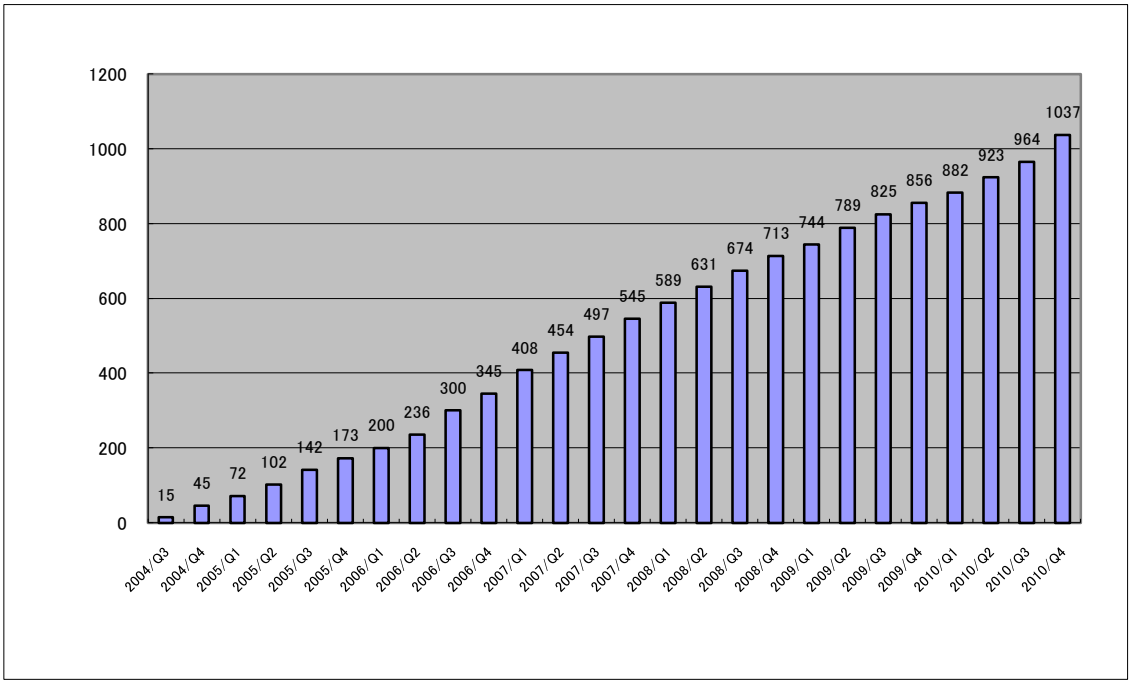
2 2004 年に設立されたセキュリティの専門家などで構成される非営利団体。マルウエアやボットネット活動における情報収集や分析、情報発信を行っている。
Shadowserver (http://www.shadowserver.org/wiki/pmwiki.php/Main/HomePage)

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）との共同運営) に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、脆弱性を作りこ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. Japan Vulnerability Notes (JVN) において公開した脆弱性情報および対応状況

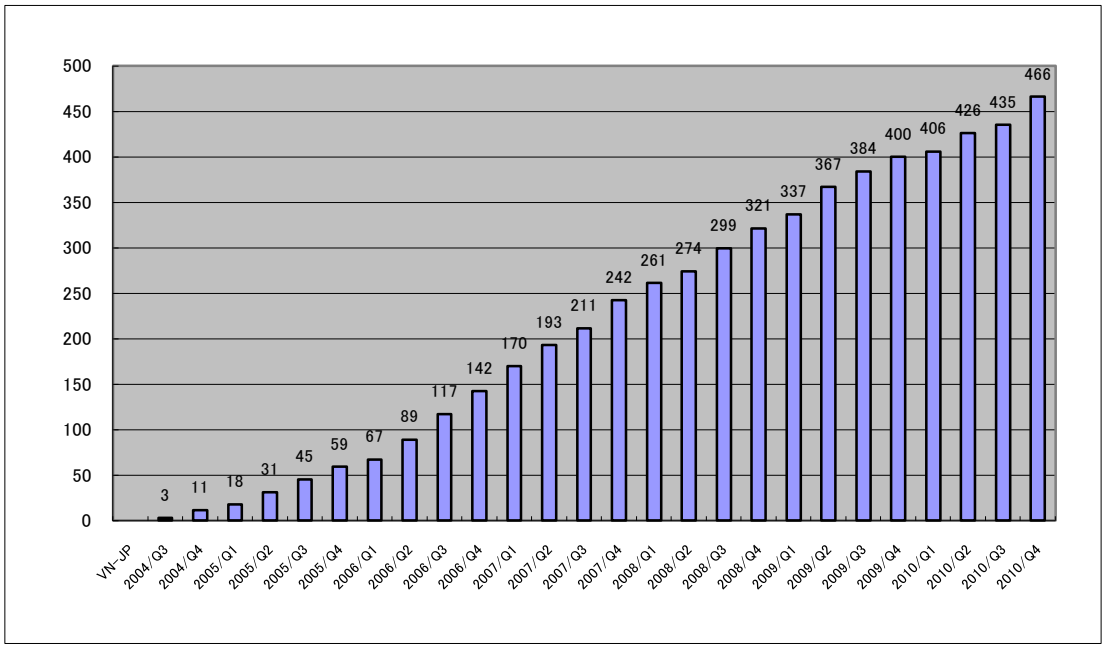
JPCERT/CC は、経済産業省告示「ソフトウエア等脆弱性情報取扱基準」（以下「本基準」といいます。）において、製品開発者とのコーディネーションを行う「調整機関」に指定されており、本基準を踏まえてとりまとめられた「情報セキュリティ早期警戒パートナーシップガイドライン」に詳述された調整機関の役割を担う活動を行っています。
本四半期に JVN において公開した脆弱性情報は 73 件(累計 1037 件) [図 2-1] で、2004 年に JVN で脆弱性情報の公表を開始してから、累計で 1000 件を超えました。本四半期に公開された個々の脆弱性情報に関しては、JVN(http://jvn.jp/)をご覧ください。



[図 2-1　累計 JVN 公開累積件数]

このうち、本基準に従って調整を行い、JVN で公開した脆弱性情報は 31 件(累計 466 件) [図 2-2] でした。これは、前四半期の 9 件と比較して 3 倍強という結果になりました。本四半期の JVN 公開

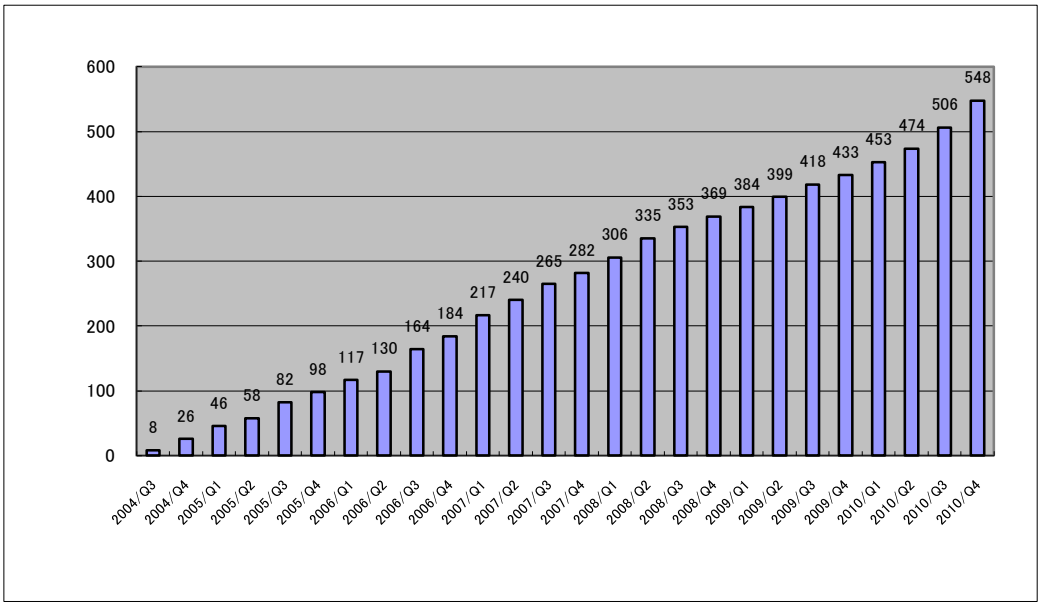
件数増加の背景には、2010 年 8 月 26 日に公開された JVNVU#707943「Windows プログラムの DLL 読み込みに脆弱性」に関連する脆弱性を抱えるソフトウエア製品に対する届出が 16 件あり、届出の通知を受けた各製品開発者が、JPCERT/CC との調整のもと修正対応を行い、その対応状況を JVN 公開したことがあげられます。また、本四半期は、製品開発者自身よる自社製品における脆弱性の届出が 3 件あり、JVN での公開が非常に速やかに行われたことも、本四半期の JVN 公開件数の増加に影響しているといえます。



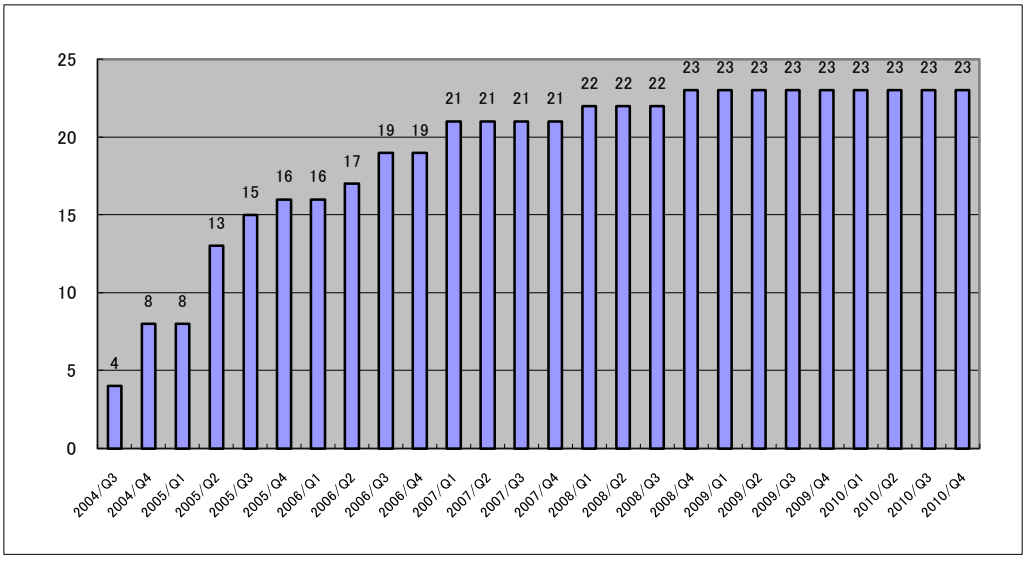
[図 2-2　累計 JVN_JP(JVN#)公開累積件数]

また、CERT/CC とのパートナーシップに基づいて調整を行い、JVN において公開した脆弱性情報は 42 件(累計 548 件) [図 2-3]でした。なおこの 42 件の中には、フィンランド CERT-FI との調整に基づき調整が行われた JVNVU#624959「侵入検知システム (IDS) および侵入防止システム (IPS) の機能を回避可能な問題」も含みます。本四半期中に公開された脆弱性情報の中では、Microsoft 製品に関するものが 8 件、Apple 製品に関するものが 6 件、Adobe 製品に関するものが 3 件、Oracle 製品に関するものが 3 件公開されました。この他、本四半期には、ISC BIND 等といったサーバ製品に関するものが 7 件、ライブラリや言語、プロトコルなどに関するものが 4 件、制御系製品に関するものが 4 件と、多岐多様な製品における脆弱性情報の公開が行われたことが特徴的でした。

なお、英国 CPNI とのパートナーシップに基づいて調整を行い、JVN にて公開した脆弱性情報は 0 件(累計 23 件) [図 2-4] でした。



[図 2-3　VN_CERT/CC(JVNVU#および JVNTA)公開累積件数]



[図 2-4　累計 VN_CPNI(CPNI) 公開累積件数]

2-2.　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、国内のみならず国際的な枠組みにおける脆弱性情報の円滑な流通のため、同じ国際調整機関である米国 CERT/CC、英国 CPNI、フィンランド CERT-FI などの海外 CSIRT 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情報通知、各国製品開発者の対応状況の集約、脆弱性情報の公開時期の設定などの連携した調整活動を行っています。

また、2008 年 5 月 21 日から運用を開始した JVN 英語版サイト(http://jvn.jp/en)へのアクセス数も徐々に増加しており、海外の主要セキュリティ関連組織などからも注目されるようになっていることがうかがえます。昨今は、海外の組織から公開されるアドバイザリの多くが、JVN 英語版サイトへのリンクを掲載しています。

JPCERT/CCは、JVN上で公開する脆弱性情報に対して、2008年8月から個別に米国MITRE社への申請を行ってCVE (Common Vulnerabilities and Exposures) 番号を取得してきましたが、2010年6月23日に、米国MITRE社より、CNA（CVE Numbering Authorities、CVE採番機関）に認定されたことに伴い、自ら、よりタイムリにCVE番号を採番できることになりました。本四半期は、25件の脆弱性情報についてCVEを採番し、JVNに掲載しました。2008年にCVEの採番を開始して以降、約98%の案件に対し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 URL をご参照ください。

News & Events “JPCERT/CC Becomes CVE Numbering Authority”
https://cve.mitre.org/news/index.html#jun232010a

CVE Numbering Authorities
https://cve.mitre.org/cve/cna.html

About CVE
https://cve.mitre.org/about/index.html

2-3. 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 URL 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(改訂版)
https://www.jpcert.or.jp/vh/partnership_guide2009.pdf
JPCERT/CC 脆弱性情報取り扱いガイドライン
https://www.jpcert.or.jp/vh/guideline_2009.pdf

本四半期の主な活動は以下のとおりです。

2-3-1. 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

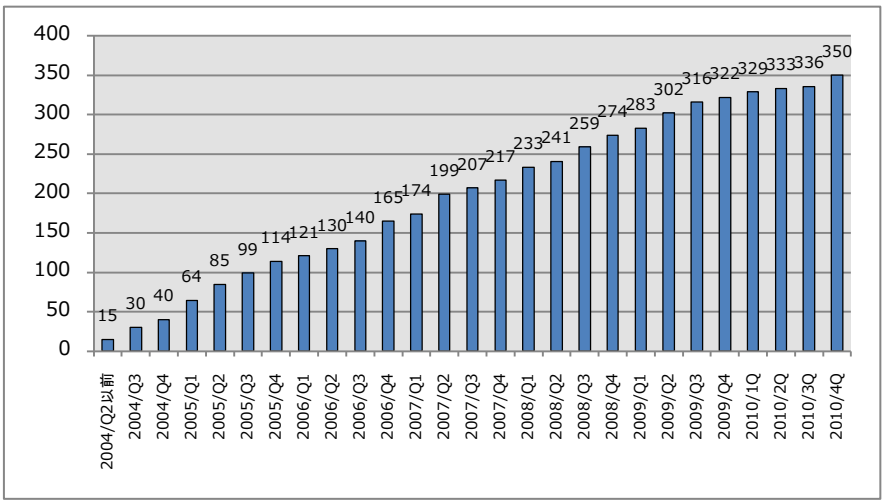
本基準では、受付機関に独立行政法人情報処理推進機構（以下「IPA」といいます。）(http://www.ipa.go.jp/)、調整機関に JPCERT/CC が指定されています。JPCERT/CC は IPA が受け付けた届出情報の転送を受けて、製品開発者への情報提供を行い、対策情報公開に至るまでの調整を行っています。最終的には、 IPA と共同で、脆弱性情報ポータル JVN において対策情報を公開しています。両組織間においては緊密な情報の交換、脆弱性情報の分析等を行っています。なお、本基準における IPA の活動および四半期毎の届出状況については次をご参照ください。

http://www.ipa.go.jp/security/vuln/

2-3-2. 日本国内製品開発者との連携

本基準では、JPCERT/CC が脆弱性情報を提供する先として、日本国内の製品開発者リスト(製品開発者リスト)を作成し、各製品開発者の連絡先情報を整備することが求められています。JPCERT/CC では、製品開発者の皆様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 2-5]に示すとおり、2010 年 12 月 31 日現在で 350 社の製品開発者の皆様にご登録をいただいています。

登録等の詳細については、https://www.jpcert.or.jp/vh/agreement.pdf をご参照ください。



[図 2-5 累計製品開発者登録数]

また、2009 年 7 月 10 日に改定した「JPCERT/CC 脆弱性関連情報取扱いガイドライン」に基づき、脆弱性情報への対応が必要な製品開発者と連絡がとれない等の理由により調整が困難なケー

スへの対応について、IPA が主催する脆弱性研究会にて検討を行うなど、関係機関と協議をしながら具体的な運用手順の整備を進めています。

2-3-3. 「脆弱性情報開示」の国際標準化活動への参加

ISO/IEC JTC-1/SC27 の国際会議(半年ごとに各地を持ち回り開催)が 10 月上旬にベルリンで開かれ、同 SC の WG3 において進められている、脆弱性情報の取扱いおよび開示に関する国際標準の策定作業に引き続き参加しました。

製品開発者による脆弱性関連情報の受取と発信に際して情報をやり取りする方法を示したガイドラインである「脆弱性情報開示」(29147； Vulnerability Disclosure (VD)； 旧称 Responsible Vulnerability Disclosure)は、6 月に参加各国に第 1 次委員会草案(CD: Committee Draft)が送付されており、9 月に参加各国が投票とコメントを寄せた上で会議に臨みました。なお、日本は、この草案に対して 50 項目以上に及ぶコメントを付けた上で、委員会草案として改善すべき点が多数残っているとして次の段階に進むことに反対する投票をしていました。

ベルリン会議では、この標準化の適用範囲が「製品開発者による情報のやり取りの方法」と定義されていたにも関わらず、脆弱性情報の取扱い手順についての言及が増していることが問題として取り上げられ、議論の末、この標準化作業と並行して、取扱い手順(Vulnerability Handling Process)を対象とした新たな標準の策定作業を開始することを提案することになりました。この動きは米国の強い意向を反映したもので、米国はエディタ候補を立てて臨んでいます．この提案は、11 月に正式の提案書(New Work Item Proposal)として参加各国に送付され、2011 年 2 月上旬を締切とする投票にかけられています。

「脆弱性情報開示」の第 1 次委員会草案に対しては、他の参加国からも多数のコメント(オーストラリア:2 件，ベルギー:4 件，カナダ:4 件，フィンランド:4 件，ドイツ:7 件，韓国:6 件，南アフリカ:3 件，英国:127 件(うち 124 件は FIRST 由来)，米国:169 件)が寄せられており、これらの取扱いがベルリンの会議で審議されました。コメントの指摘は文書全般に渡っていましたが、特に多数のコメントがあったのは、脆弱性の取扱い手順への言及に関する指摘と、1 次委員会草案になる時点で南アフリカが起草して挿入された概念を解説した章の内容に関する指摘でした。前者は、新しい標準化作業の開始を提案することで合意が得られたことより解決がはかられました。後者については、抜本的な構成の見直しの方向性について合意を得た上で、日本が持ち帰って起草し直すことになり、帰国後に草案を作成して 11 月にエディタに提出しました。その後、審議結果に基づいてエディタが改訂した第 2 次委員会草案(2nd CD)が SC27 事務局から 12 月上旬に送付され、これに対する投票およびコメントが 3 月上旬を締切として参加各国に要請されています。

新たな標準化作業項目提案が登場して戦線拡大の感がありますが、JPCERT/CC では、SC27 国際会議への参加ならびに日本の標準化組織である情報規格調査会を通じて、引き続き、この国際標

準が我が国の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に整合したものとなるよう努めていく所存です。

2-4. セキュアコーディング啓発活動

2-4-1. インド、ベトナム、フィリピンで「C/C++セキュアコーディングセミナー」を開催

前四半期に大阪、名古屋で開催した C/C++セキュアコーディングセミナーと同等の内容のセミナーを、以下の日程でインド、ベトナム、フィリピンの 3 カ国にて実施しました(講義資料と講義は英語で提供)。

・10 月 26 日、27 日 デリー、インド
・10 月 28 日、29 日 バンガロール、インド
・11 月 2 日、3 日 ハノイ、ベトナム
・12 月 1 日、2 日 マニラ、フィリピン

日本のソフトウエア産業の主要オフショア先であるインド、ベトナム、フィリピンの三カ国において、現地のソフトウエア開発者を対象に C/C++セキュアコーディングに関するノウハウを提供することは、現地のセキュリティ啓発に資するのみならず、日本のソフトウェアセキュリティ向上にも資するとの期待を込めて、これら 3 カ国においてセミナーを実施しました。

講義は、「part1. セキュアコーディング概論・文字列」と「part2. 整数・コードレビュー」の 2 つのコースを 2 日間で実施しました。
「part1. セキュアコーディング概論・文字列」では、受講者にセキュアコーディングの必要性や重要性の理解を促す「セキュアコーディング概論」にはじまり、C/C++言語における「文字列」の脆弱性に関する講義、その講義内容について受講者の理解を深めるための「演習」という構成で実施しました。「part2. 整数・コードレビュー」では、C/C++言語における「整数」の脆弱性に関する講義とその内容に関する「演習」、最後にこれらのセミナーで学んだ知識を総動員し、脆弱性を抱えたサンプルコードを受講者自らがレビューして修正方法を考える「セキュリティコードレビュー」という構成で実施しました。

セミナーは、現地の CERT 組織と協力して企画、開催し、受講者から高い評価を得るとともに、JPCERT と各国 CERT 組織との一層の連携強化に資するものとなりました。

受講者アンケートでは継続して開催を望む声を多くいただきました。今後、次年度以降の継続開催を検討してまいります。

2-4-2. C/C++セキュアコーディングセミナー@東京、好評開催中

脆弱性を作り込まないプログラミング手法に関する連続セミナー「C/C++セキュアコーディングセミナー@東京」を 8 月から開始しています。10 月 13 日は「CERTC 文セキュアコーディングスタンダード」に関するセミナーを、11 月 10 日は「動的メモリ管理」、12 月 15 日は「書式指定文字列」の脆弱性に関して講義と演習をセットにした形式のセミナーを実施しました。この後の予定としては、2011 年 2 月に、オープンソースのコンパイラフレームワーク ROSE を使用した CERT C セキュアコーディングスタンダードのルール実装に関する実機を使ったハンズオンを開催する予定です。C/C++言語でのソフトウエア開発に携わる方や静的解析ツールに興味のある方のご参加をお待ちしております。セミナーの募集要項、詳しいスケジュールは下記のイベント情報 URL をご参照ください。

イベント情報：https://www.jpcert.or.jp/event/

2-4-3. C/C++セキュアコーディング 出張セミナー

JPCERT/CC では、C/C++言語を使用した開発を行う企業・組織を対象に、C/C++セキュアコーディングに関する出張セミナー(有償)のご要望を承っています。マネジメント層へのセキュリティ啓発や新人研修のメニュー等としてもご利用いただいています。本四半期は、国内大手メーカ 1 社向けに出張セミナーを実施しました。
出張セミナーのご依頼、お問合わせは、secure-coding@jpcert.or.jp までご連絡下さい。

2-4-4. 開発者向けウェブマガジン CodeZine に好評連載中

翔泳社の開発者向けウェブマガジン CodeZine に「実例で学ぶ脆弱性対策コーディング」と題したシリーズで C/C++セキュアコーディングの解説記事を連載しています。この四半期には次の 1 回分が掲載されました。

第 8 回 Windows の DLL だけが危ないのか？DLL hijacking vulnerability 概説（後編）(10 月 5 日)

CodeZine (コードジン)
http://codezine.jp/

2-5. 制御システムセキュリティに関する啓発活動

2-5-1. 調査活動

2-5-1-1 セキュリティ・アセスメント・ツールの調査

前四半期に引き続き、制御システム用セキュリティ・アセスメント・ツールを関係者に提供するための活動を進めました。SICE/JEITA/JEMIMA 合同 WG に参加し、評価対象とする仮想的な制御システムを設定して考察する手法により、英国 CPNI が開発した SSAT の JPCERT/CC による邦訳版の試用と意見交換を行いました。
合同 WG の成果は、2010 年 9 月に開催された「計測展 2010」において発表され、モデルとして想定した制御システムにおいて、SSAT の利用によってそのセキュリティがどのように改善するかが示されました。JPCERT/CC は、このモデル版の試用を通じて SSAT の適用に係る知見を得るとともに、翻訳ミスその他の問題点について SSAT の改善を行ないました。併せて合同 WG 参加者の意見、要望を SSAT に反映した改良を進めています。本年度末には「合同 WG・JPCERT/CC 監修版 SSAT」(仮称)として公開する予定です。

2-5-1-2 制御システムを攻撃対象としたマルウエアの調査

2010 年 7 月に制御システムをターゲットとした最初のマルウエアとされる Stuxnet の存在が報じられ注目を集めました。半年を経過した現在に至っても関連記事がほぼ毎週のようにセキュリティベンダーのブログやニュースサイトに掲載され、その関心の高さやインパクトの大きさを物語っています。JPCERT/CC では 2 月に開催予定の「制御システムセキュリティカンファレンス 2011」において、このマルウエアに関する多方面の情報を集約してわかりやすく提示するとともに、こうした新たな脅威にどのように立ち向かうべきかを参加者の皆様とともに議論する予定です

2-5-2. 制御システムベンダーセキュリティ情報共有タスクフォースへの情報発信

制御システム開発関係者にセキュリティ関係の情報を提供するニュースレターを隔月で配信しています。今四半期は 11 月 26 日に配信しました。タスクフォースメンバー向けに、セキュリティインシデントに係る事例や関係する標準の動向、技術情報に関するニュースなどを収集して掲載しています。
今後とも、タスクフォースメンバーの要望等を収集し、内容の充実を図っていく予定です。
このニュースレターは、制御システムベンダーセキュリティ情報共有タスクフォースのメンバーであれば、どなたでも受信できます。タスクフォースへの参加資格や申込方法については、次の URL をご参照ください。

制御システムベンダーセキュリティ情報共有タスクフォース
https://www.jpcert.or.jp/ics/taskforce.html

また、2010 年 11 月 17 日～19 日の 3 日間、東京国際展示場で開催された「ものづくり NEXT↑2010」製造業セキュリティ対策特集コーナーにパネル出展し、お立ち寄りいただいた方々に、タスクフォース、「制御システムセキュリティカンファレンス 2011」、JPCERT/CC の活動等の説明・紹介を行いました。

2-5-3. 関連学界活動

ほぼ毎月開かれている SICE (計測自動制御学会)、JEMIMA (日本電気計測工業会) などによる合同セキュリティ検討 WG の活動に参加し、制御システムのセキュリティに関し、制御システムの専門の方々と意見交換を行いました。JPCERT/CC の今期以降のアクションプランのひとつである「ユーザ企業のために対策が必要な脆弱性情報抽出方法の検討」を推進するため、WG メンバーと意見交換しました。なお、この WG では、前述のセキュリティ・アセスメント・ツールの普及活動も進めました。

また、2010 年 11 月 9 日に東京工業大学で開催された「2010 年度産業応用部門大会」（SICE 産業応用部門主催）の、計測・制御ネットワークシンポジウムにおいて、「制御システムのための脆弱性ハンドリングに関する考察」と題する講演を行いました。

2-5-4. 制御システム・セキュリティカンファレンス準備

昨年度に続き、制御システムセキュリティカンファレンスの開催に向けた準備を進めました。今年度は、2011 年 2 月 10 日（木）に東京（品川）で会場を用意し、「現実化した脅威とその対策課題」をテーマに、組織的・体制的領域、技術的領域、および運用上の領域に潜む多くの課題について、「改善」「防御」「回復」の各視点から国内のユーザ、開発者、ベンダの皆様による講演、パネルディスカッションを通じて大いに論じていただく予定です。

2-6 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 などでの利用を想定して、KENIGINE など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、2010 年 6 月より行っています。

VRDA フィードについての詳しい情報は、以下の URL を参照下さい。
https://www.jpcert.or.jp/vrdafeed/index.html

本四半期に配信した VRDA フィード配信件数のデータソース別の内訳、言語別の VRDA フィードの利用傾向をそれぞれ[表 2-1]と[表 2-2]に示します。[表 2-2]では、言語別に VRDA フィードインデックス（Atom フィード）と脆弱性情報（詳細情報）の利用割合を示し、脆弱性情報については配信データ形式別の利用割合を示しています。

[表 2-1　VRDA フィード配信件数]

2010 年 10 月～12 月			年度累計
MyJVN API	NVD	計	
579 件	1116 件	1695 件	3890 件

[表 2-2　言語別 VRDA フィード利用傾向]

言語	VRDA フィードインデックス	脆弱性情報	（データ形式別）	
			HTML	XML
日本語版	95%	52%	97%	3%
英語版	5%	48%	93%	7%

[表 2-2]に示したように、VRDA フィードインデックスの利用割合以外は、日本語版、英語版ともに脆弱性情報の利用については似通った傾向です。両言語版ともに HTML 形式の利用が圧倒的に多く、フィードリーダと Web ブラウザの組み合わせでの利用がほとんどで、XML 形式で表現された脆弱性情報を機械処理しているケースは非常に少ないようです。言語別で利用傾向がはっきりと異なる点として、VRDA フィードインデックスの利用割合が上げられますが、英語版と日本語版の脆弱性情報の利用割合に大きな差異は無いことから、英語版の一利用者あたりの脆弱性情報の利用の割合が日本語版に比べ非常に高いと言えそうです。

3. ボット対策事業

JPCERT/CC は、総務省・経済産業省連携プロジェクトであるボット対策プロジェクトにボットプログラム解析グループとして参加し、収集されたボット検体の特徴や技術の解析、および駆除ツールの作成を担当しています。また、効率的なボット解析手法の検討や、さらには駆除ツール開発事業者と連携して対策技術の開発なども行っています。

駆除ツールについては、サイバークリーンセンターの一般公開サイトでの CCC クリーナーの提供が 12 月 22 日をもって終了しました。以降、同サイトにおいては、CCC クリーナーに替わって、株式会社 Kaspersky Labs Japan 様に駆除ツールを提供いただいています。なお、ボットに感染

した利用者が個別に案内される注意喚起のサイトにおいては、引き続き CCC クリーナーが提供されています。

このプロジェクトでは毎月の活動実績として「サイバークリーンセンター活動実績」が公開されていますので、ご参照ください。また、前四半期に公開した「ボットの脅威との戦い～サイバークリーンセンター(CCC)活動レポート～」の英語版も公開されております。

サイバークリーンセンター
https://www.ccc.go.jp/

2010 年 11 月度 サイバークリーンセンター活動実績
https://www.ccc.go.jp/report/201011/1011monthly.html

The Fight Against the Threat from Botnets Report on the activities of the Cyber Clean Center(CCC)
https://www.ccc.go.jp/en_report/Report_on_the_activities_of_the_Cyber_Clean_Center.pdf

3-1.「マルウエア対策研究人材育成ワークショップ 2010(MWS 2010)」への参画

「マルウエア対策研究人材育成ワークショップ 2010(MWS 2010)」(ボット対策プロジェクト運営委員会および情報処理学会が共催)が 10 月 19 日から 3 日間の日程で岡山コンベンションセンターにて開催されました。MWS は、ボット対策プロジェクトで収集しているボット観測データから抽出した「研究用データセット」を大学や研究機関等の参加組織に提供し、参加者が同じデータセットを活用して次の 3 つの分野に関する研究発表を行うワークショップです。

(1) 検体解析技術の研究
(2) 感染手法の検知ならびに解析技術の研究
(3) ボットの活動傾向把握技術の研究

JPCERT/CC は、MWS 2010 の実行委員としてワークショップの企画・運営に参加し、ボット対策プロジェクトにおいてマルウエア解析や解析技術の効率化の調査研究を担当している立場から、研究用データセットを構成するマルウエア検体の選定を行いました。

この取り組みは、ボットやマルウエアに関する専門的な知識を持つ研究者/実務者の育成や、対策技術の高度化につながるものであることから、来年度以降の継続開催に期待が寄せられています。

マルウエア対策研究人材育成ワークショップ 2010(MWS 2010)
http://www.iwsec.org/mws/2010/

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) 等に対し、トレーニングやイベントでの講演等を通して CSIRT の構築・運用支援活動を行い、各国のインシデント対応調整能力の向上と、各国 National CSIRT 等と JPCERT/CC との間の相互信頼と連携の強化を図っています。

4-1-1. アジア太平洋地域における活動

4-1-1-1. ベトナム VNCERT の分析技術者に対する受け入れ研修の実施（2010 年 10 月 4 日 - 12 月 17 日）

ベトナム VNCERT で進められているマルウエア等の分析体制の整備計画への協力の一環として、VNCERT の分析技術者２名を受け入れ、JPCERT/CC 内においてマルウエア分析トレーニング研修を行いました。CSIRT でのマルウエア分析においては、個々のチームの技術力だけではなくチーム間の協力関係も重要です。このような研修を実施することにより、より深いレベルでの協力関係を醸成し、国際的なインシデント対応や情報収集をスムーズに実施することができるようになります。

4-1-1-2. JICA 沖縄国際センターIT 研修生による実地見学の受け入れ(2010 年 10 月 13 日)

JICA 国際沖縄センターで「電子政府推進のためのセキュリティ強化コース」を受講中の開発途上国の IT 担当者 8 名の来訪を受け、JPCERT/CC の業務の紹介や意見交換を行いました。研修生は、エジプト、カメルーン、カンボジア、サウジアラビア、タイ、フィリピン、ブータン、ベトナムの 8 ヶ国の省庁、情報関連センターおよび発電公社等の IT 担当者で、それぞれ各国の IT 分野において重要な役割を担っています。National CSIRT が存在する国の研修生にも意外に知られていない National CSIRT の機能および国際連携の重要性、さらには日本の情報セキュリティの動向と関連技術について、理解を深めていただく良い機会となりました。

4-1-2. その他地域における活動

4-1-2-1. アフリカ諸国向け CSIRT トレーニング実施(2010 年 11 月 20 日-23 日)

AfriNIC-13 は、アフリカ地域におけるインターネット業界の主要関係者が集い、国際的なベストプラクティスの最新動向等について協議し、アフリカ地域における活用を推進するための様々な会合を開催するイベントで、今回は、南アフリカのヨハネスブルグにて開催されました。

JPCERT/CC は、AfriNIC-13 に参加し、アフリカ地域とアジア地域の IT 分野における連携を促進するフォーラムである AAF (Africa Asia Forum on Network Research & Engineering) が主催した CSIRT トレーニングおよびワークショップで講師を務めました。この AAF によるアフリカ地域での CSIRT 構築および運営支援活動は、3 年間のプロジェクトとして計画されているもので、今回のトレーニングは、2010 年 5 月にルワンダのキガリで開催された Internet Summit of Africa の場でのトレーニングに続く 2 回目の実施にあたるものです。

CSIRT トレーニングは、11 月 20 日-22 日の 3 日間にわたり、アフリカ各国の技術者約 25 名に向けて実施されました。初日は、CSIRT の基礎、運用および技術、情報セキュリティの技術的概観、OS とプログラミングについて、2 日目は、インシデント分析の基礎（システムログ、ネットワークトラフィック、技術運用）について実践演習を含めた講義をそれぞれ行いました、最終日には、CSIRT 活動における文化の相違や、情報収集および分析、技術文書の公開のノウハウ、ウェブおよびマルウエア分析に関する高度トレーニング、インシデント対応演習の実施手法について講義をしました。

また、11 月 23 日には、アフリカ各国のマネジメント層や政策立案者に向けた CSIRT ワークショップが開催され、JPCERT/CC および APCERT の活動から得た知見を参加者と共有し、意見交換を行いました。その他、アフリカのインターネットセキュリティの実情に関する情報を収集するとともに、今後のアフリカ各国の CSIRT との連携に備えて関係者と意見交換を行ったり、相互の連絡先や連絡方法を確認したりしました。

次回のアフリカ地域での CSIRT 構築および運営支援活動に関するトレーニングは、2011 年 5 月にタンザニアにて開催される予定です。アフリカ各国の情報セキュリティ担当者が一堂に集うため、アフリカ全体に対する地域支援に効果的な機会であり、今後とも JPCERT/CC が培った知見を共有し、日本に関連したインシデントがアフリカ地域で発生した場合等に必要となる連携体制の強化に務めていきます。

本トレーニングの模様について、JPCERT/CC の英語ブログで公開しています。

CSIRT Training for Africa
http://blog.jpcert.or.jp/2010/11/csirt-training.html

4-2. 国際 CSIRT 間連携

海外の National CSIRT との間のインシデント対応に関する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り組みの実施状況等に関する情報収集を目的とした国際連携活動等を行っています。さらに、CSIRT が構成する団体についても、アジア太平洋地域における APCERT (Asia Pacific Computer Emergency Response Team)や、世界的な FIRST (Forum of Incident Response and Security Teams) に参加し、その枠組みに則った

活動をしています。

4-2-1. アジア太平洋地域における活動

4-2-1-1. ベトナム情報通信省(MIC: Ministry of Information and Communications)関係者来訪 (2010 年 10 月 12 日)

ベトナムの National CSIRT である VNCERT (Vietnam Computer Emergency Response Team) が設置されているベトナム情報通信省を始めとする同国代表団の来訪を受け、主に JPCERT/CC と VNCERT の連携分野について協議しました。具体的には、両組織の活動について最新状況を共有するとともに、現在 VNCERT で進められているマルウエア等の分析体制の整備計画に協力することを目的として、JPCERT/CC が有する分析技術や分析環境に関する情報を提供し、上記 4-1-1-1 記載の VNCERT の分析技術者 2 名に対する研修の状況を紹介しました。その他、先方の関心の強い制御システムセキュリティについて JPCERT/CC における取り組みを紹介し、意見交換を行いました。

4-2-1-2. 日中韓の CSIRT による国際シンポジウムへの参加(2010 年 11 月 19 日)

日中韓の CSIRT(JPCERT/CC, CNCERT/CC, KrCERT/CC)が一堂に会する初の公開シンポジウムが沖縄で開催されました。本シンポジウムは、講演とパネルディスカッションを通して、日中韓各国および本シンポジウムの開催地となった沖縄のサイバーセキュリティの現状、3 国間の情報共有の現状、人材育成の重要性、およびクラウドコンピューティングにおける情報セキュリティの考え方、日中韓それぞれの首都圏から等距離にある沖縄が 3 国間の連携に果たすべき役割等に関して、その問題意識を、開催地の沖縄県を中心とした県内外の関係者で共有することを目的に開催されたものです（主催：一般財団法人　国際開発センター、社団法人　沖縄県情報産業協会／共催：JPCERT/CC、CNCERT/CC、KrCERT/CC、特定非営利活動法人　フロム沖縄推進機構／後援：沖縄県、内閣府沖縄総合事務局、経済産業省、JICA 沖縄、財団法人　沖縄県産業振興公社（順不同）、協力企業：合同会社　スタークロス沖縄）。

日中韓の専門家が集い、サイバーセキュリティにおける現状と課題を共有した本シンポジウムは、サイバーセキュリティの強化を一国の課題として捉えるのではなく、脅威の国際化傾向に対応するための国際連携強化の重要性、つまり地域規模および世界規模の課題として捉えることの必要性を沖縄県内外の関係者に伝える有意義な機会となりました。

本シンポジウムの模様は、地元の新聞でも取り上げられました。

情報保護へ国際連携　日・中・韓代表者がシンポ
http://www.okinawatimes.co.jp/article/2010-11-20_12171/

4-2-2. その他の地域における活動

4-2-2-1. 「情報セキュリティインシデントマネジメント」の国際標準化活動への参加(2010 年 10 月 6 日-8 日)

情報セキュリティインシデントマネジメントのためのガイドラインである ISO/IEC 27035 “Information security incident management”の標準化が ISO/IEC JTC 1/SC 27 WG4 において検討されており、10 月にドイツのベルリンにて開催された SC 27 の国際会議において、最終委員会草案(FCD: Final Committee Draft)に対する各国からのコメントの取扱いが審議されました。

本規格は、組織が情報セキュリティに関するインシデントマネジメントを遂行するためのガイダンスとなる情報を提供するもので、今回の会議を経て、最終国際規格案(FDIS: Final Draft International Standard)に進むことが決定しました。次回の会議は、2011 年 4 月にシンガポールにて開催予定です。

4-2-2-2. GOVCERT.NL シンポジウム 2010 等への参加(2010 年 11 月 15 日-16 日)

オランダのロッテルダムで開催された GOVCERT.NL シンポジウム 2010 に参加し、講演やパネルディスカッションを通して、最新のトピックスや動向（ボットネット軽減における制御点としての ISP、SSH ブルートフォース攻撃に関する攻撃行動、標的型攻撃の検知方法、Stuxnet と SCADA システムへの攻撃、オランダ警察庁によるサイバー犯罪への取り組みの現状、安全なソフトウエア開発の向上に向けたセキュリティ問題への事前対策の取組み等）に関する情報を収集しました。また、欧州各国の CSIRT 等との円滑な連携の継続のため、各チームと近況等に関する情報交換を行いました。

さらに、11 月 16 日には同じくオランダのロッテルダムで National CSIRT 間のコード共有化のワークショップが開催され、JPCERT/CC が議長を務めました。本ワークショップでは、各国の National CSIRT が開発した運用支援ツール（ソフトウエア）を National CSIRT 間で広く共有し、当該ツールを用いたプロジェクトを推進すること等を目的に、コード共有化に向けた技術的方法およびそれに伴う課題について協議しました。今回の参加者は、日本、アメリカ、オーストラリア、オーストリア、オランダ、スイス、スウェーデン、ハンガリー、フィンランド、ブラジル、ポーランド等の主要 CSIRT メンバーで、今後は、CERT/CC が主催する National CSIRT Meeting 等の場を通して協議が進められます。

4-2-2-3. 米国 US-CERT、ICS-CERT 訪問および CIP-Forum への参加(2010 年 12 月 1 日-3 日)

米国の US-CERT を訪問し、JPCERT/CC と US-CERT 間の連携活動（日米におけるインシデント動向の共有、米国内における情報共有強化の取組みの紹介、ツールやマテリアルの共有の検討

等）について協議を深めました。また、ICS-CERT(Industrial Control Systems Cyber Emergency Response Team)を訪問し、JPCERT/CC の制御系システム活動に関する最新状況を共有すると共に、情報連携の強化等について協議しました。さらに、CIP-Forum に参加し、重要インフラ保護および制御系システム分野における情報を収集し、関係者との関係構築に努めると共に、JPCERT/CC からサプライチェーンセキュリティに関する講演を行いました。

4-3. APCERT 事務局運営

JPCERT/CC は、アジア太平洋地域の CSIRT のコミュニティである、APCERT の事務局を担当しています。APCERT についての詳細は、次の URL をご参照ください。

APCERT
https://www.jpcert.or.jp/english/apcert/

4-4. FIRST Steering Committee への参画

FIRST Steering Committee のメンバとして、JPCERT/CC の職員が FIRST の組織運営に関与しています。

FIRST Steering Committee
http://www.first.org/about/organization/sc.html

5. フィッシング対策協議会事務局の運営

JPCERT/CC では、経済産業省からの委託により、フィッシング対策協議会（以下、本章において「協議会」といいます。）の事務局として、協議会の総会や各ワーキンググループの運営、Web ページの管理、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、JPCERT/CC のインシデント対応チームに対するフィッシングサイトの停止調整の依頼、国内外関連組織との共同研究などの活動を行っています。

5-1. 情報収集/発信の実績

本四半期、協議会では、協議会 Web ページや会員向け ML により、フィッシングに関するニュースや緊急情報を 11 件発信しました。また、フィッシングの動向や新対策技術に関する有識者インタビュー記事を協議会 Web ページに 3 件掲載したほか、会員向けにフィッシングに関するトピックの提供などを実施しました。

5-2. フィッシングサイト URL 情報を提供する対象会員（対策サービス事業者）の拡大

協議会では、協議会会員のうちのフィッシング対策ツールバーなどを提供している事業者やウイルス対策ソフトベンダに対し、協議会に報告されるフィッシングサイトの URL のリストを、日に数回提供しています。提供した URL 情報をブラックリストに追加していただく等、ユーザ保護に向けた取組みに活用していただくことを目的としています。本四半期は、新たにマカフィー(2010 年 11 月)、アンラボ(2010 年 12 月)の 2 社に提供を開始しました。これにより協議会が情報を提供している事業者は合計で 9 社となりました。現在も複数の事業者との間で情報提供に関する協議を行っており、提供先を順次拡大していく予定です。

5-3. Web サイトのリニューアル

2010 年 10 月に消費者やサービス事業者のアクセシビリティを考慮した Web デザインの改善を行いました。各種情報を利用者に分かりやすく周知できるよう、消費者向けとサービス事業者向けに分け、コンテンツの内容を拡充しました。

[図 5-1：フィッシング対策協議会 HP https://www.antiphishing.jp/]

5-4. フィッシング対策セミナーの開催

11 月 17,18,19 日に、より広範にフィッシング対策の重要性を訴えるため、海外からの講演者も

交えた本格的なフィッシング対策セミナーを、東京（参加者：136 名）、大阪（参加者：28 名）に加えて今年は新たに福岡（参加者：27 名）の 3 会場で開催しました。セミナーのプログラムは次のとおりです。

基調講演（同時通訳）13:35-14:35　「中国におけるフィッシング対策の状況-アンチフィッシングアライアンスチャイナのご紹介」 Anti-phishing Alliance of China(APAC) 副事務局長 China Internet Network Information Center (CNNIC) 管理部副主任 Xiao Bohan 氏
講演 1 14:40-15:20 東京会場： 「マイクロソフトにおけるフィッシング対策への取り組」 マイクロソフト株式会社 チーフセキュリティアドバイザー 高橋正和氏 大阪会場、福岡（博多）会場： 「フィッシング対策技術の動向について」 株式会社セキュアブレイン 執行役員マーケティングディレクター 中田太氏
講演 2 15:35-16:15「楽天でのセキュリティ体制 ～楽天からみるインターネットセキュリティの脅威と、その対策～」 楽天株式会社 軍司祐介氏
報告 16:20-17:00「増加するフィッシング詐欺 今、何が出来るのか」 フィッシング対策協議会／JPCERT コーディネーションセンター 【東京会場】 小宮山功一朗 【大阪会場】 瀬古敏智 【福岡会場】 山本健太郎

注) 講演 1 については東京会場と大阪/福岡会場で講演者が異なる。

5-5. 普及啓発コンテンツの公開

2009 年度の協議会のワーキンググループ活動などで作成した資料を公開しました。
公開した資料の概要は次のとおりです。

1) フィッシングレポート 2010
概要:2009 年度におけるフィッシングの被害状況や攻撃技術・手法の変化などを取りまとめ、さらにはフィッシングの範疇にとどまらないフィッシングの手口に発展する脅威とその対策、法制度に関する検討を行い、その結果をまとめました。

フィッシングレポート 2010
https://www.antiphishing.jp/report/pdf/phishing_report_2010.pdf

5-6. 講演活動

本四半期に協議会として以下の講演を行いました。

1) 小宮山 功一朗「増加するフィッシング詐欺　今、何ができるのか」
千葉県クレジットカード犯罪対策連絡協議会 第 20 回定例会,2010 年 12 月 14 日
2) 小宮山 功一朗「パネルディスカッション 相手認証の必要性と考え方、現状動向」
SecurityDay 2010, 2010 年 12 月 22 日

5-7. 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、毎月の活動報告として「フィッシング対策協議会への報告件数」などを公開しています。詳細については次の URL 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 2010 年 10 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201010.html
フィッシング対策協議会 2010 年 11 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201011.html
フィッシング対策協議会 2010 年 12 月 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201012.html

6. 公開資料

JPCERT/CC の各業務において実施した情報セキュリティに関する調査・研究の報告書や論文、セミナー資料を公開しました。

6-1. 研究調査レポート「踏み台にされる Web サイト～いわゆる Gumblar の攻撃手法の分析調査～」の公開

2009 年 4 月以降、JPCERT/CC のインシデント対応窓口では、いわゆる Gumblar の攻撃による Web サイトの改ざんの報告を多く受けてきました。この攻撃の特徴は、改ざんされた Web にアクセスさせることでマルウエア感染を引き起こし、そのマルウエアに感染した PC から収集したアカウント情報を利用して、さらなる Web 改ざんを再生産する循環により影響範囲を拡大する点にあり、また、こうした一定の枠組みの中で時とともに異なるマルウエアが登場して世代交代をしつつ進化を遂げていった点も注目されました。JPCERT/CC では、受け取った報告から Web 改

ざんの実態把握や統計情報の収集を行うだけでなく、必要に応じて関連マルウエアを分析し、その結果に基づいて、改ざんされたサイトの管理者や、実行されるマルウエアの配布先などへコーディネーションを行っていますが、こうした JPCERT/CC の活動を通して得られた情報を元に、Gumblar の攻撃手法の流れ、感染するマルウエアの動作などを公開用にとりまとめました。

現在では、いわゆる Gumblar といわれる攻撃は陰を潜めつつありますが、この攻撃の目的は、後の攻撃のためのインフラ整備を行っていたとも考えられます。また、前回の攻撃によって仕込まれたマルウエアの今後の影響も忘れてはいけません。未だ予断を許さない Web 改ざんの攻撃手法の実態を理解し、今後の対策の検討の参考にしていただけるよう公開しました。

「踏み台にされる Web サイト-いわゆる Gumblar の攻撃手法の分析調査」
(2010 年 11 月 15 日)
https://www.jpcert.or.jp/research/2010/webdefacement-20101115.pdf

6-2. セキュリティ対策講座「電子メールソフトのセキュリティ設定について」の改訂

2010 年 3 月に公開した「電子メールソフトのセキュリティ設定について」に、メーラーの種類として Web メール 2 種(Gmail、Yahoo!メール)を追加し、HTML メールの取り扱いや添付ファイルの取扱いに関する記述も追加した改訂版を作成し、公開しました。

「電子メールソフトのセキュリティ設定について」(2010 年 12 月 6 日)
https://www.jpcert.or.jp/magazine/security/mail/index.html

7. 講演活動一覧

(1) 歌代 和正(代表理事):
「インターネット時代のセキュリティ管理」
奈良先端科学技術大学院大学 先端領域特論 B,2010 年 11 月 4 日
(2) 小熊 信孝(情報流通対策グループ 制御システムセキュリティ):
「制御システムのための脆弱性ハンドリングに関する考察」
SICE 2010 年度産業応用部門大会　計測・制御ネットワークシンポジウム,2010 年 11 月 9 日
(3) 小宮山 功一朗(国際部マネージャ,早期警戒グループ リーダ 情報セキュリティアナリスト):
「増加するフィッシング詐欺 今、何が出来るのか」
フィッシング対策セミナー@東京,2010 年 11 月 16 日
(4) 瀬古 敏智(早期警戒グループ 情報セキュリティアナリスト):

「増加するフィッシング詐欺 今、何が出来るのか」
フィッシング対策セミナー@大阪,2010 年 11 月 17 日

(5) 山本 健太郎(早期警戒グループ 情報セキュリティアナリスト):
「増加するフィッシング詐欺 今、何が出来るのか」
フィッシング対策セミナー@福岡,2010 年 11 月 18 日

(6) Jack YS Lin(早期警戒グループ 情報セキュリティアナリスト):
「Internet Security Trends in Japan」
Internet Security Trends in Japan,2010 年 11 月 18 日

(7) 早貸 淳子(常務理事)
「日本におけるサイバーセキュリティの現状」
日中韓、国際シンポジウム～東アジアの情報セキュリティを考える,2010 年 11 月 19 日

(8) 宮地 利雄 (理事):
「Panel discussion MOF2010」
MOF2010 パネルディスカッション,2010 年 11 月 19 日

(9) 山口 英(理事), 小宮山 功一朗(国際部マネージャ, 早期警戒グループ リーダ 情報セキュリティアナリスト):
「CSIRT Training for Engineer」
Afrinic CERT Training@南アフリカ,2010 年 11 月 20 日～22 日

(10) 山口 英(理事), 小宮山 功一朗(国際部マネージャ, 早期警戒グループ リーダ 情報セキュリティアナリスト):
「APCERT activity update」
Afrinic CERT Workshop@南アフリカ,2010 年 11 月 23 日

(11) 水野 哲也(早期警戒グループ リーダ 情報セキュリティアナリスト)
「インシデント発生時における外部組織との対応事例」
InternetWeek2010 ,2010 年 11 月 25 日

(12) 中谷 昌幸 (早期警戒グループマネージャ 情報セキュリティアナリスト):
「情報セキュリティインシデントの最新動向とその対策」
NEC キャピタルソリューション マネジメントサロン講演会,2010 年 11 月 25 日

(13) 小宮山 功一朗(国際部マネージャ, 早期警戒グループ リーダ 情報セキュリティアナリスト):
「2010 年セキュリティ事件簿」
InternetWeek2010 ,2010 年 11 月 26 日

(14) Jack YS Lin(早期警戒グループ 情報セキュリティアナリスト):
「インターネットセキュリティの現状」
電子応用懇話会平成 22 年 12 月月例会,2010 年 12 月 1 日

(15) Jack YS Lin(早期警戒グループ 情報セキュリティアナリスト):
「中国における最新のインターネット事情の講演」

NCA2010 国際連携ワークショップ,2010 年 12 月 3 日

8. 執筆・取材記事一覧

(1) 中尾 真二(事業推進基盤グループ 広報):
「Fast-flux は減少し、トラディショナルなフィッシングが増加―APWG」
フィッシング対策協議会 インタビュー,2010 年 10 月 4 日

(2) 久保 正樹(情報流通対策グループ 脆弱性アナリスト)、戸田 洋三(情報流通対策グループ リードアナリスト):
「Windows の DLL だけが危ないのか？ DLL hijacking vulnerability 概説（後編）」
翔泳社 CodeZine,2010 年 10 月 5 日

(3) 中尾 真二(事業推進基盤グループ 広報):
「サクラを使ったメール詐欺が増加している―国民生活センター」
フィッシング対策協議会 インタビュー,2010 年 11 月 8 日

(4) 中尾 真二(事業推進基盤グループ 広報):
「Gumblar の目的は攻撃インフラ構築だった?-JPCERT/CC、サイト改ざん攻撃の分析調査を発表」
RBB TODAY,2010 年 11 月 19 日

(5) 中尾 真二(事業推進基盤グループ 広報):
「ヨーロッパでは 64 ビット版 Windows 7、ボットネット対策が 2011 年の課題―Eddy Willems, G Data セキュリティラボ」
フィッシング対策協議会 インタビュー,2010 年 12 月 9 日

9. 開催セミナー等一覧

(1) C/C++ セキュアコーディングセミナー@Delhi
(2) C/C++ セキュアコーディングセミナー@Bangalore
(3) C/C++ セキュアコーディングセミナー@Hanoi
※(1)-(3)のセミナーの詳細は、「2-4-1」をご参照ください。
(4) C/C++ セキュアコーディングセミナー2010@東京
※本セミナーの詳細は、「2-4-2」をご参照ください。
(5) フィッシング対策セミナー@東京
(6) フィッシング対策セミナー@大阪
(7) フィッシング対策セミナー@福岡
※(2)-(4)のセミナーの詳細は、「5-4」をご参照ください。
(8) ものづくりNEXT2010 製造業セキュリティ対策特集コーナーへの出展
近年、制御システムに対するセキュリティの関心が高まる中、制御監視系プロトコルの脆弱性調査の実施、セキュリティカンファレンスの開催、メールニュースの配信など、

注意喚起体制や情報共有体制を維持・拡大するとともに、関係者の意識を高める活動に取り組んでいます。
そのひとつの活動して、本コーナーへ出展し、制御システムに関わるユーザ、ベンダ、システムインテグレータの方々に、問題提起と解決のための資料等のご案内をしました。

・主　　催　社団法人日本能率協会
・開催時期　2010年11月17日～19日
・展示会入場者累計　39,363名

(9) SecurityDay2010

近年インターネットは、さまざまな社会経済活動の中で広く利用されるようになりその依存性が高まる一方で、インターネットを通じたコンピュータセキュリティインシデントが頻発し、ますます増大する傾向にあります。これら脅威は社会的なリスクであり、それらを低減させるひとつの方法として、プロフェッショナルや専門家の情報共有と議論の場が必要ではないかと考え、共催5社が、情報セキュリティに関わるユーザ、運用、管理といった立場の方を対 象に、参加者とともに考え議論、問題提起をするセミナーを開催しました。

・主　　催　日本インターネットプロバイダ協会(JAIPA)、日本ネットワークセキュリティ協会(JNSA)、日本データ通信協会(Telecom-ISAC-Japan) 、日本電子認証協議会(JCAF)、JPCERT/CC
・開催時期　2010年12月22日
・集客人数　90名

詳細については、以下のURLをご参照ください。
Securityday 2010
http://securityday.jp/

10. 後援・協力一覧

(1) Email Security Expo& Conference 2010
2010 年 10 月 6 日～7 日
(2) InternetWeek2010
2010 年 11 月 24 日～26 日
(3) 第 7 回デジタル・フォレンジック・コミュニティ 2010 in TOKYO
2010 年 12 月 13 日～14 日

■ 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

■ 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：cs-security-staff@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、その他のお問い合わせ：office@jpcert.or.jp