

情報セキュリティに関する 普及・啓発活動の調査結果

2011 年 3 月

NTT データ経営研究所

- 目次 -

1.	国内の普及啓発活動.....	1
1.1.	政府中央省庁.....	1
1.2.	地方公共団体.....	10
1.3.	都道府県警察.....	14
1.4.	各種法人・団体.....	19
2.	海外の普及啓発活動.....	29
2.1.	米国における取組み.....	29
2.2.	ドイツにおける取組み.....	31
2.3.	英国における取組み.....	31
2.4.	フランスにおける取組み.....	31
2.5.	オランダにおける取組み.....	31
2.6.	オーストラリアにおける取組み.....	32
2.7.	欧州（EU）における取組み.....	32
2.8.	ITU における取組み.....	32
2.9.	APEC における取組み.....	32

1. 国内の普及啓発活動

1.1. 政府中央省庁

○経済産業省

・CHECK PC¹

一般のインターネット利用者を対象に、セキュリティ対策の実施を啓発するキャンペーンを実施している。コンピュータウイルスの感染、不正アクセス、フィッシング詐欺等の被害を防止することを目的に、セキュリティの基礎知識や対策についての解説、リスク診断、クイズなどのコンテンツをホームページ上で提供している。



図 CHECK PC 特設ホームページ²

・インターネット安全教室³

経済産業省と NPO 日本ネットワークセキュリティ協会が全国各地の関係団体等と協力して実施している。家庭や学校からインターネットにアクセスする一般の利用者を対象に、ネット上でのビデオ教材やリーフレットなどのコンテンツ配信のほか、情報セキュリティに関する基礎知識を学習できる無料セミナーを各地で実施している。

¹ <http://www.checkpc.go.jp/top.html>

² <http://www.checkpc.go.jp/top.html>

³ <http://www.net-anzen.go.jp/>



図 インターネット安全教室 特設ホームページ⁴

・中小企業指導者育成セミナー⁵

中小企業の経営者等の情報セキュリティを指導する立場にある人を対象に、経済産業省とNPO日本ネットワークセキュリティ協会が全国各地の関係団体等と協力してセミナーを実施している。具体的には、ITコーディネータ、中小企業診断士、日商マスター、その他中小企業に対して指導的立場にある方々（各団体指導員、IT関連企業の方等）、団体職員（商工会議所関係者及び商工会関係者、中小企業団体中央会関係者）等を対象としている。各地域で無料セミナーを実施しており、セミナーでは、事例を通じた演習やグループディスカッション等の実践的な方法により行っている。また、参加者には実施報告レポートの提出と引き換えに謝金を提供するなどのインセンティブを用意している。



図 中小企業指導者育成セミナー 特設ホームページ⁶

⁴ <http://www.net-anzen.go.jp/>

⁵ <http://www.jnsa.org/ikusei/seminar/>

○セキュリティ普及促進委員会

「情報セキュリティ月間」を機に、シマンテック、トレンドマイクロ、マカフィーのセキュリティ3社と情報処理推進機構、経済産業省が官民、企業間の壁を超えて連携し、情報セキュリティ対策の普及啓発を実施。「企業の情報セキュリティの課題と在り方」をテーマに、緊急セミナーを開催する。

○総務省

・国民のための情報セキュリティホームページ⁷

インターネットの利用者に対し、ホームページ上で情報セキュリティに関する情報の提供を行っている。初心者向けの「情報セキュリティ三原則」「情報セキュリティ認識度チェック」といったコンテンツや、学習のための「基礎知識」「用語辞典」などのコンテンツ、実際のセキュリティ対策の方法を示した「対策」「実践」といったコンテンツを提供している。

このコンテンツの1つとして、ボットウイルスについての解説⁸を行っている。この中で、子供向けにアニメーションや紙芝居形式で、ボットウイルスについての説明を行うコンテンツを提供している。同じホームページ内に企業ユーザ／システム管理者向けのコンテンツ⁹も併せて用意している。

⁶<http://www.jnsa.org/ikusei/seminar/>

⁷ http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm

⁸ http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kiso/k04_bot.htm

⁹ http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/work10.htm



図 国民のための情報セキュリティホームページ¹⁰

・情報通信の安心安全な利用のための標語¹¹

個人や学校を対象に、情報通信を安心・安全に利用するためのルールやマナー、情報セキュリティの意識を啓発する標語を募集している。初心者を含む情報通信利用者が情報通信を安心・安全に利用するためのルールやマナー、情報セキュリティに関する意識や知識の重要性に気づき、考えるきっかけとすることを目的に、標語を公募し、受賞作を用いた啓発活動を行うことを趣旨としている。

¹⁰ http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm

¹¹ <http://www.fmcc.or.jp/hyogo/>

受賞標語	
【 総務大臣賞 】	
学校部門	ネットはね 一緒に心も つなぐんだ 宇城市立三角中学校(熊本県)
個人部門	送信に そっと マナーを添付する 中出 博之 さん(三重県)
【 協議会長賞 】	
児童部門	気をつけよう 安易なクリック せまるワナ 大山 藍 さん(茨城県)
生徒部門	Eメール 相手を思って いいメール 田畑 晃希 さん(岩手県)
一般部門	子供には 親のルールが セキュリティ 藤部 光春 さん(宮城県)
【 佳 作 】	
	書きちゃダメ 面と向かって言えぬこと 賀曾利 拓実 さん(千葉県)
	危険の芽 気づく親の目 子をガード 加茂 佐和子 さん(神奈川県)
	危機意識 まずは自分に スイッチON 坂井 泰法 さん(新潟県)
	ケータイは 時間を決めて 場所決めて 杉浦 達 さん(東京都)
	どっちやねん! ハンドル持つんか? ケータイか? 久住 英明 さん(大阪府)
	子供のネットマナー 顔けた親を写すミラー 古谷 正伸 さん(東京都)

図 平成 22 年度受賞標語¹²

・情報セキュリティサポーター

JNSA 等の地域 NPO 法人等と連携して、情報セキュリティ対策をサポートする人材の育成や体制整備を支援している。¹³また、文部科学省と連携して、保護者及び教職員を対象に、子供たちのインターネットの安全・安心な利用へ向けた啓発を目的とした講座を開講している。

○文部科学省

・情報の漏えい等の防止についての関連情報

Web ページ学校におけるファイル共有ソフトウェアからの個人情報の漏洩を防止するための注意喚起と防止対策の情報を提供している。¹⁴

¹² <http://www.fmnc.or.jp/hyogo/>

¹³ <http://www.jnsa.org/seminar/2009/100215/data/S1-1.pdf>

¹⁴ http://www.mext.go.jp/b_menu/koukai/kojin/info.htm

・文部科学省が主催する「情報セキュリティセミナー」の配信¹⁵

大学等において情報セキュリティを統括する業務に携わる教職員や実務担当者を対象に、実施したセミナー¹⁶の資料のダウンロードや講義のストリーミング配信などを行っている。

時 間	講 演 内 容 ・ 講 演 者	資 料 (PDF)	Streaming 配 信
13:00	開会の挨拶 (文部科学省)		streaming
13:05-14:00	基調講演 「グローバル情報社会における日本の情報セキュリティ」 講師:村井 純 慶應義塾大学 環境情報学部長 教授 情報セキュリティ政策会議有識者委員		streaming
14:00-14:10	休憩		
14:10-15:20	講 演 「教育・研究機関等のためのセキュリティ知識 -インシデントに学ぶ-」 講師:高橋 郁夫 弁護士、IT法律事務所主宰、 ITリサーチ・アート社代表取締役		streaming
15:20-15:30	休憩		
15:30-16:25	講 演 「実務者からみた情報セキュリティマネジメント事例 -組織における効果的な情報セキュリティマネジメントとは?-」 講師:角熊 登 国立大学法人 広島大学 社会連携・情報政策室 情報化推進グループ主査 (ITコーディネーター)		streaming
16:25-16:35	休憩		
16:35-17:30	講 演 「PDCAサイクルの中での「C」(評価)の果たす役割」 講師:石井 秀明 有限責任監査法人トーマツ エンタープライズリスクサービス シニアマネジャー		streaming
17:30	閉会の挨拶 (国立情報学研究所)		streaming

図 情報セキュリティセミナーの内容¹⁷

○厚生労働省

医療機関向けに「医療情報システムの安全管理に関するガイドライン」¹⁸を策定している。

○総務省・経済産業省連携プロジェクト

・サイバークリーンセンター (CCC)

プロジェクト参加 ISP の協力を得て、メールと Web を組み合わせた手法により、感染元ユーザに対し注意喚起を行う事後的な対応活動を行っている。具体的には、「おとりマシン」(Honeypot)を設置し、意図的に感染させることで、感染者の IP アドレスを取得し、感染者には、メールでボットウイルス駆除手順を案内する「対策サイト」の URL を記載し

¹⁵ <http://www.nii.ac.jp/csi/secsem/2010/>

¹⁶ http://www.nii.ac.jp/hrd/ja/security/h16sec_seminar.html

¹⁷ <http://www.nii.ac.jp/csi/secsem/2010/>

¹⁸ <http://www.mhlw.go.jp/shingi/2009/03/s0301-4.html>

感染を知らせるとともに、「対策サイト」に案内することで、感染者にボットウイルスの危険性、駆除手順をわかりやすく説明している。¹⁹

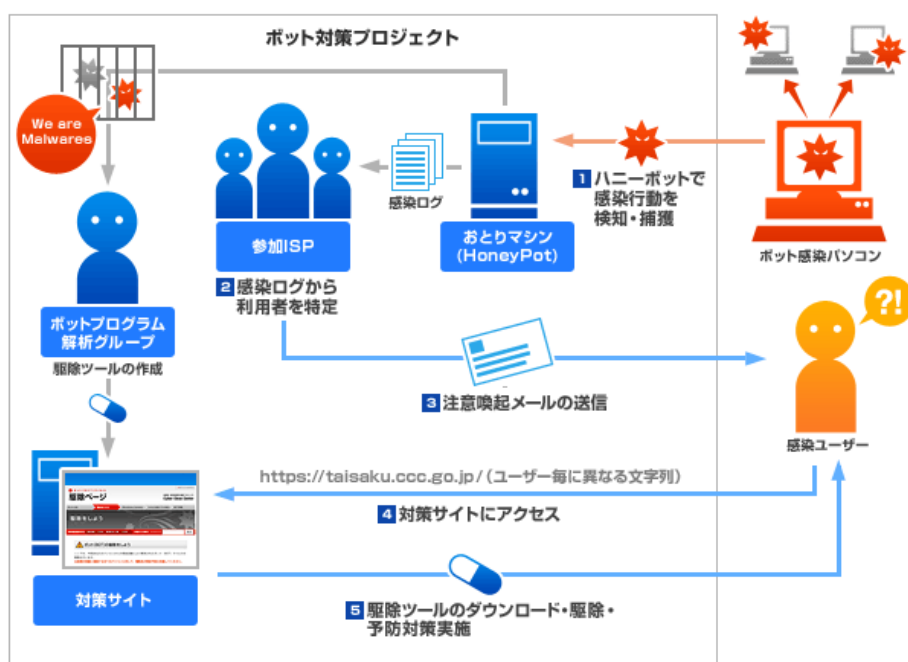


図 注意喚起の概要²⁰

○総務省・文部科学省連携プロジェクト

・e-ネットキャラバン²¹

子ども、保護者、教職員等に対してインターネットの安心・安全利用に関する啓発活動として、講座の実施をしている

○内閣府

・情報セキュリティ月間

政府では、情報セキュリティに関する普及啓発強化のため、2月を「情報セキュリティ月間」と定め、内閣官房(NISC)、警察庁、総務省、文部科学省及び経済産業省が協力し、情報セキュリティに関する普及啓発活動を官民連携の下に推進している。具体的には、官房長官から情報セキュリティの重要性を訴えるメッセージの発信(首相官邸ホームページに掲載)や関係省庁、企業等による情報セキュリティに関するセミナー等の行事を全国で

¹⁹ <https://www.ccc.go.jp/activity/index.html>

²⁰ <https://www.ccc.go.jp/activity/index.html>

²¹ <http://www.e-netcaravan.jp/index.html>

開催するほか、NISC ホームページにおいて情報提供を推進している。²²

○警察庁


・@police²⁴

ハイテク犯罪・サイバーテロの未然防止及び被害の拡大防止のため、ネットワークセキュリティに関する様々な情報を、パソコンユーザ向け、システム／ネットワーク管理者向け、キッズ向けにホームページ上で情報提供している。

・サイバーセキュリティ・カレッジ²⁵

サイバーセキュリティ・カレッジ

○ サイバーセキュリティ・カレッジとは、
情報セキュリティに関する国民の知識及び意識の向上を図るため、警察やプロバイダ連絡協議会が主催する研修会、学校関係者等からの依頼による講演会、地域の各種セミナー、情報通信技術関連イベント等の機会を活用して、手口の実演を交えるなどして、サイバー犯罪の現状、対策等に周知を図るもの。



サイバーセキュリティカレッジ(H20.7 群馬)

○ 広報強化月間中のサイバーセキュリティ・カレッジ実施状況

	H18年(4~5月)	H19年(5月)	H20年(2月)
実施回数	約2,600回	約2,500回	約2,200回
受講者数	約361,000人	約360,000人	約336,000人

図 サイバーセキュリティ・カレッジの概要²⁶

・警察庁サイバー犯罪対策 ホームページ

サイバー犯罪情報の提供（CYBER WARNING）や、情報セキュリティ対策についてのパンフレットの配布²⁷やドラマ仕立ての動画配信（情報セキュリティ対策ビデオ）、インターネットでの相談窓口（インターネット安心・安全相談）²⁸などを行っている。

²² http://www.nisc.go.jp/press/pdf/sm10event_press.pdf

²³ <http://www.nisc.go.jp/index.html>

²⁴ <http://www.npa.go.jp/cyberpolice/>

²⁵ <http://www.nisc.go.jp/conference/seisaku/kihon/dai11/pdf/11siryou02.pdf>

²⁶ <http://www.nisc.go.jp/conference/seisaku/kihon/dai11/pdf/11siryou02.pdf>

²⁷ <http://www.nisc.go.jp/conference/seisaku/kihon/dai11/pdf/11siryou02.pdf>

²⁸ <http://www.npa.go.jp/cybersafety/>

○中小企業庁

中小企業庁は、「安心して個人情報を取り扱うためには」²⁹ というパンフレットにより、インターネットにおける個人情報保護に関する啓発活動を行っている。

○消費者庁

・情報セキュリティに関する検討会³⁰

偽造・盗難キャッシュカード及びインターネットバンキングにおける不正取引に関して、金融庁監督局内に「情報セキュリティに関する検討会」を設置し、ATM システム（利用時の対策、情報管理態勢、被害発生時の対応）と、インターネットバンキング（利用時の対策、基本設計その他）について検討している。

²⁹ http://www.chusho.meti.go.jp/pamflet/sonota/kojin_jyoho.pdf

³⁰ <http://www.fsa.go.jp/news/newsj/17/ginkou/20060310-2.html>

1.2. 地方公共団体

都道府県の情報セキュリティに関する普及啓発活動はサイバークリーンセンター（CCC）へのリンクなどの関連機関のホームページの紹介のほか、ボットウイルスに関する警戒を呼びかけるような内容が多く見られる。

以下、普及活動の例および活動主体を列挙する。

○北海道

- ・NORTH 北海道地域ネットワーク協議会³¹

○秋田県

- ・秋田県ホームページ

「ボットウイルス駆除活動キャンペーン」を県のホームページ内に設けている。³²

○青森県

- ・青森県インターネットプロバイダ防犯連絡協議会³³

○福島県

- ・福島県高度情報化推進協議会³⁴

○宮城県

- ・宮城県高度情報化推進協議会³⁵

○山形県

- ・山形県インターネット防犯連絡協議会³⁶

○茨城県

- ・茨城県情報通信ネットワークセキュリティ協議会³⁷

○栃木県

³¹ <http://www.north.ad.jp/northweb/>

³² <http://www.pref.akita.lg.jp/icity/browser?ActionCode=content&ContentID=1233556375190&SiteID=0>

³³ <http://www.police.pref.aomori.jp/seianbu/hoan/hitech/aipa001.html>

³⁴ <http://www.fukushima-koudo.jp/>

³⁵ <http://www.miyagi-ipa.jp/>

³⁶ <http://www.pref.yamagata.jp/ou/keisatsu/800016/yipa.html>

³⁷ <http://www.sopia.ne.jp/user/pibaraki/netsecure.htm>

- ・栃木県ホームページ
県のホームページ内に、CCC へのリンクを設けている。³⁸

- 千葉県
 - ・千葉県ホームページ
「ボットウイルス駆除活動キャンペーン」を県のホームページ内に設けている。³⁹

 - ・千葉県地域 IT 化推進協議会⁴⁰

 - ・千葉県インターネット防犯連絡協議会⁴¹

 - ・千葉県 IT フロンティア産業支援協議会⁴²

 - ・千葉県電子自治体共同運営協議会⁴³

- 埼玉県
 - ・埼玉県コンピュータ・ネットワーク防犯連絡協議会⁴⁴

- 東京都
 - ・東京都セキュリティ促進協会⁴⁵

- 群馬県
 - ・群馬県情報化推進協議会について⁴⁶

- 北陸地域（石川県）
 - ・北陸無線データ通信協議会⁴⁷

- 新潟県
 - ・IT&ITS 推進協議会⁴⁸

³⁸ <http://www.pref.tochigi.lg.jp/pref/jyouhouka/sekyurithii/sekyurithii-link.html>

³⁹ <http://www.pref.chiba.lg.jp/jousei/event/campaign/sonohoka/bottokujo.html>

⁴⁰ <http://www.it-kyougikai.jp/>

⁴¹ <http://www.lpac.jp/bohan/>

⁴² http://www.pref.chiba.lg.jp/syozoku/f_sanshin/it/frontier.html

⁴³ <http://www.e-chiba.org/>

⁴⁴ <http://www.saitama-cn.gr.jp/>

⁴⁵ <http://www.tosekyo.org/>

⁴⁶ http://www.pref.gunma.jp/cate_list/ct00000871.html

⁴⁷ <http://homepage3.nifty.com/jh9vsf/hwdcc.htm>

○富山県

- ・富山県 SOHO 協議会⁴⁹

○福井県

- ・e マガふくい

福井県で発行している「e マガふくい」の中で、ボットウイルスについての紹介がある⁵⁰。

○長野県

- ・長野県ネットセキュリティ啓発活動推進協議会⁵¹

- ・website 信州

「ボットウイルス駆除活動キャンペーン」を県のホームページ内に設け、CCC へのリンクの掲載及びボットウイルスについての解説を行っている。⁵²

- ・長野県インターネットプロバイダ防犯連絡協議会⁵³

○京都

- ・京都府インターネットカフェ連絡協議会⁵⁴

- ・京都インターネット・セキュリティ対策学校連絡会⁵⁵

○滋賀県

- ・滋賀県情報基盤協議会⁵⁶

○山口県

- ・山口県セキュリティマネージメントフォーラム(Y-Sec)⁵⁷

⁴⁸ <http://www.n-it-its.jp/>

⁴⁹ <http://www.soho-toyama.gr.jp/consult/index.html>

⁵⁰ https://www2.pref.fukui.lg.jp/melma/bnview.php?melma_cod=6bb7d9116788757348&msgseq=msg1192406750db

⁵¹ <http://nasp.cybernetwork.jp/top.html>

⁵² http://www.pref.nagano.lg.jp/kikaku/josei/security/bot/security_bot.htm

⁵³ <http://www.avis.ne.jp/~ipnagano/>

⁵⁴ http://www.pref.kyoto.jp/fukei/anzen/seiki_h/cyber/kir.htm

⁵⁵ http://www.pref.kyoto.jp/fukei/anzen/seiki_h/cyber/isr.htm

⁵⁶ <http://www.it-shiga.jp/>

⁵⁷ http://www.y-sec.jp/y-sec_top.html

○岡山県

- ・Okayama Internet Security Assosication(OISec)⁵⁸

○広島県

- ・Hirosima Internet SEcurirty Consortium(HISEC)⁵⁹

○島根県

- ・島根県サイバーテロ対策協議会⁶⁰

○高知県

- ・高知県ネットワークセキュリティ連絡協議会⁶¹

○愛媛県

- ・愛媛県ネットワーク防犯連絡協議会⁶²

○熊本県

- ・熊本県情報セキュリティ推進協議会⁶³

○佐賀県

- ・佐賀県セキュリティ協議会

○福岡県

- ・福岡県情報セキュリティ連絡協議会

○長崎県

- ・長崎県ネットワーク・セキュリティ連絡協議会

○政令指定都市・中核都市

政令指定都市レベルでの取り組み状況は年によって差が大きい。仙台市は情報セキュリティ研修を開催するなど積極的に取り組んでいる。⁶⁴

⁵⁸ <http://www.oisec.jp/top.htm>

⁵⁹ <http://www.hisec.jp/>

⁶⁰ http://www.pref.shimane.lg.jp/police/shitteimasuka/saiba-tero_20100805/saiba-tero_h22_08_05.html

⁶¹ <http://www2.ocn.ne.jp/~knscc/index2.htm>

⁶² <http://www.iyo.ne.jp/ensa/>

⁶³ <http://www.kmt-ics.co.jp/kuma-security/index.html>

⁶⁴ <http://www.city.sendai.jp/kikaku/jyo-seisaku/joho-sekyu/kensyuu.html>

1.3. 都道府県警察

警察庁および道府県警察本部では、サイバー犯罪を中心とした一般市民に対する啓蒙と警戒の喚起を中心とした普及啓発を実施している。以下に、普及方法の窓口となる活動主体と普及啓発のホームページを列挙する。

○警視庁

- ・情報セキュリティ広場⁶⁵

○北海道警察本部

- ・サイバー犯罪の防止について⁶⁶

○青森県警察本部

- ・青森県警察サイバー犯罪対策室 ホームページ⁶⁷

○岩手県警察本部

- ・岩手県警察サイバー犯罪対策室 ホームページ⁶⁸

○宮城県警察本部

- ・宮城県警察サイバー犯罪対策室 ホームページ⁶⁹

○秋田県警察本部

- ・秋田県警察本部生活環境課サイバー犯罪対策室 ホームページ⁷⁰

○山形県警察本部

- ・山形県警察サイバー犯罪対策室 ホームページ⁷¹

○福島県警察本部

- ・福島県警サイバー犯罪対策コーナー⁷²

⁶⁵ <http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku409.htm>

⁶⁶ <http://www.police.pref.hokkaido.jp/info/seian/hitec/kouhou.html>

⁶⁷ <http://www.police.pref.aomori.jp/seianbu/hoan/hitech/index.htm>

⁶⁸ <http://www.iwate-kenkei.morioka.iwate.jp/>

⁶⁹ http://www.police.pref.miyagi.jp/hp/cyber/cyber_index.html

⁷⁰ <http://www.police.pref.akita.jp/kenkei/soudan/25.html>

⁷¹ <http://www.pref.yamagata.jp/ou/keisatsu/800016/cyber/hightec.html>

⁷² <http://www.police.pref.fukushima.jp/onegai/jyouhou/hightech2/hightech.index.html>

○茨城県警察本部

- ・生活安全部生活環境課サイバー犯罪対策室 ホームページ⁷³

○栃木県警察本部

- ・サイバー犯罪対策⁷⁴

○群馬県警察本部

- ・サイバー犯罪対策⁷⁵

○埼玉県警察本部

- ・サイバー犯罪対策(サイバー犯罪対策センター ホームページ)⁷⁶

○千葉県警察本部

- ・サイバー犯罪⁷⁷

○神奈川県警察本部

- ・サイバー犯罪対策センター⁷⁸

- ・ユビキタス社会に対応する情報セキュリティの啓発活動

ユビキタス社会に対応する情報セキュリティの啓発活動を推進するため、マイクロソフト社、県内の u-Kanagawa 推進協議会、NPO 情報セキュリティフォーラムなど情報セキュリティを積極的に推進している民間団体と連携し、企業に対して情報セキュリティを普及啓発するセミナーを開催している。⁷⁹

○新潟県警察本部

- ・新潟県警察本部ハイテク犯罪対策室 ホームページ⁸⁰

○長野県警察本部

- ・長野県警察本部サイバー犯罪対策室 ホームページ⁸¹

⁷³ http://www.pref.ibaraki.jp/kenkei/01_anzen/07_cyber/index.html

⁷⁴ <http://www.pref.tochigi.lg.jp/keisatu/seikatu/nethanzai.html>

⁷⁵ http://www.police.pref.gunma.jp/seianbu/01seiki/haiteku/index_hai.htm

⁷⁶ <http://www.police.pref.saitama.lg.jp/kenkei/hanzai/mi/cyber/cyber.html>

⁷⁷ http://www.police.pref.chiba.jp/safe_life/cyber_crime/

⁷⁸ <http://www.police.pref.kanagawa.jp/mes/mesd0015.htm>

⁷⁹ <http://www.pref.kanagawa.jp/osirase/sangyo/ms/>

⁸⁰ <http://www.police.pref.niigata.jp/osirase/hightech/>

⁸¹ <http://www.pref.nagano.jp/police/seian/hightech/index.htm>

- 静岡県警察本部
 - ・静岡県警察サイバー犯罪対策室からのお知らせ⁸²

- 富山県警察本部
 - ・富山県警察サイバー犯罪対策室 ホームページ⁸³

- 石川県警察本部
 - ・石川県警察サイバー犯罪対策プロジェクト⁸⁴

- 福井県警察本部
 - ・福井県警察におけるサイバー犯罪対策⁸⁵

- 岐阜県警察本部
 - ・岐阜県警察サイバー犯罪対策室⁸⁶

- 愛知県警察本部
 - ・サイバー犯罪対策⁸⁷

- 三重県警察本部
 - ・サイバー犯罪について⁸⁸

- 滋賀県警察本部
 - ・サイバー犯罪対策⁸⁹

- 京都府警察本部
 - ・サイバー犯罪対策⁹⁰

- 大阪府警察本部
 - ・サイバー犯罪対策⁹¹

⁸² <http://www.police.pref.shizuoka.jp/bouhan/cyber/index.htm>

⁸³ <http://police.pref.toyama.jp/sections/6110/high-tech/index.html>

⁸⁴ http://honbu.police.pref.ishikawa.lg.jp/seian_bu/seiankikaku/cyber/index.htm

⁸⁵ <http://www.pref.fukui.jp/kenkei/seanbu/seikan/cyber/index.html>

⁸⁶ <http://www.pref.gifu.lg.jp/police/kurashi-anzen/hanzai-kenkyo/cyber-hanzai/>

⁸⁷ <http://www.pref.aichi.jp/police/safety/high-tech/index.html>

⁸⁸ http://www.police.pref.mie.jp/info/saftyinfo/06_cyber/index.html

⁸⁹ <http://www.pref.shiga.jp/police/seikatu/seikatsukankyoku/index.html>

⁹⁰ http://www.pref.kyoto.jp/fukei/anzen/seiki_h/cyber/index.html

⁹¹ http://www.police.pref.osaka.jp/05bouhan/high_tech/index.html

- 兵庫県警察本部
 - ・兵庫県警察サイバー犯罪対策室 ホームページ⁹²

- 和歌山県警察本部
 - ・和歌山県警察本部サイバー犯罪対策室⁹³

- 鳥取県警察本部
 - ・サイバー犯罪防犯広報パンフレット・DVD⁹⁴

 - ・サイバー犯罪情報⁹⁵

- 島根県警察本部
 - ・島根県警察サイバー犯罪対策係 ホームページ⁹⁶

- 岡山県警察本部
 - ・岡山県警察本部サイバー犯罪対策室 ホームページ⁹⁷

- 広島県警察本部
 - ・広島県警察サイバー犯罪対策室 ホームページ⁹⁸

- 山口県警察本部
 - ・山口県警察サイバー犯罪対策室 ホームページ⁹⁹

- 徳島県警察本部
 - ・徳島県警察サイバー犯罪対策室 ホームページ¹⁰⁰

- 香川県警察本部
 - ・香川県警察本部サイバー犯罪対策室 ホームページ¹⁰¹

⁹² <http://www.police.pref.hyogo.jp/seikatu/syber/index.htm>

⁹³ <http://www.police.pref.wakayama.lg.jp/cyber/cyber-main.html>

⁹⁴ <http://www.pref.tottori.lg.jp/dd.aspx?menuid=122532>

⁹⁵ <http://www.pref.tottori.lg.jp/dd.aspx?menuid=35002>

⁹⁶ <http://www.pref.shimane.lg.jp/police/hanzai/cyber/index.html>

⁹⁷ <http://www.pref.okayama.jp/kenkei/seian/seiki/cyber/index.html>

⁹⁸ <http://www.police.pref.hiroshima.lg.jp/041/hightech/index.html>

⁹⁹ <http://www.police.pref.yamaguchi.jp/0210/hitec/hitec.htm>

¹⁰⁰ <http://www.police.pref.tokushima.jp/menu09.html>

¹⁰¹ <http://www.pref.kagawa.jp/police/soudan/hightec/index.htm>

- 愛媛県警察本部
 - ・愛媛県警察サイバー犯罪対策室 ホームページ¹⁰²

- 高知県警察本部
 - ・サイバー犯罪相談窓口¹⁰³

- 福岡県警察本部
 - ・サイバー犯罪¹⁰⁴

 - ・情報セキュリティ対策ビデオの紹介¹⁰⁵

- 佐賀県警察本部
 - ・サイバー犯罪対策¹⁰⁶

- 長崎県警察本部
 - ・インターネットトラブルにご用心（《サイバー犯罪対策室メインページ》）¹⁰⁷

- 熊本県警察本部
 - ・サイバー対策関係¹⁰⁸

- 宮崎県警察本部
 - ・宮崎県警察本部サイバー犯罪対策室 ホームページ¹⁰⁹

- 鹿児島県警察本部
 - ・サイバー犯罪のいろいろ¹¹⁰

- 沖縄県警察本部
 - ・サイバー犯罪の対策について¹¹¹

¹⁰² <http://www.police.pref.ehime.jp/cyber/index.htm>

¹⁰³ http://www.police.pref.kochi.lg.jp/seian/seikan/cyber_crime.html

¹⁰⁴ <http://www.police.pref.fukuoka.jp/bohan-info/04.html>

¹⁰⁵ <http://www.police.pref.fukuoka.jp/seian/seikei/028.html>

¹⁰⁶ <http://www.police.pref.saga.jp/kenkei/cyber/index.htm>

¹⁰⁷ <http://www.police.pref.nagasaki.jp/a21seian/b07cyber/HP/cyberindex.htm>

¹⁰⁸ <http://www.police.pref.kumamoto.jp/index.do>

¹⁰⁹ <http://www.pref.miyazaki.lg.jp/police/high-tech/index.htm>

¹¹⁰ <http://www.pref.kagoshima.jp/police/network/index.html>

¹¹¹ <http://www.police.pref.okinawa.jp/anzenkurashi/hanzaihigai/cybercrime/index.html>

1.4. 各種法人・団体

○独立行政法人情報通信研究機構（NICT）

・情報通信セキュリティシンポジウム

大学、研究機関、企業等の情報通信分野の研究開発・運用等に携わる人および一般人を対象に、情報通信セキュリティの専門家による講演及びパネルディスカッションを通じて、情報通信セキュリティの最新動向や、最新テーマについての普及・啓発を行っている。¹¹²

○NP0 日本ネットワークセキュリティ協会（JNSA）

・情報セキュリティ理解度チェック¹¹³

組織の管理者に向けた、社員の情報セキュリティのリテラシーチェックをするためのホームページ。組織の管理者が自組織の社員・職員をユーザ登録し、受講させることで、1人ひとりの情報セキュリティ知識レベルを確認したり、自組織の情報セキュリティ知識レベルの客観的な把握が可能になる。

・理解度セルフチェック¹¹⁴

2007年度に経済産業省の委託でJNSAが作成し、管理・運用を行っているホームページ。オフィスにおける情報セキュリティについて、電子メールやインターネット、PCの利用における注意点やウイルスの知識、オフィスにおけるセキュリティやルール・規則などについての知識の確認ができる。

・情報セキュリティ人材育成シンポジウム¹¹⁵

総務省の委託事業のひとつ。JNSAが運営主体となり、情報セキュリティ教育事業者連絡会（ISEPA）、セキュリティ対策推進協議会（SPREAD）の連携の下、講演及びディスカッションをメインとした無料のシンポジウムを開催している。インターネット利用者、個人の情報セキュリティ対策をサポートする者、情報セキュリティ資格保有者を対象としており、「永遠のビギナー」の知識・技術の底上げおよび適切な情報セキュリティ対策の実現を目的に情報セキュリティ人材の育成・確保に取り組む有識者を招いた講演を行っている。

・中小企業向け指導者育成セミナー

中小企業における情報セキュリティ対策の促進を図るために、中小企業の経営者等に対して、情報セキュリティに対する適切なアドバイスを行なう地域の指導者を育成するた

¹¹² <http://www2.nict.go.jp/pub/whatsnew/press/h20/090210/090210-1.html>

¹¹³ <http://slb.jnsa.org/eslb/>

¹¹⁴ <http://slb.jnsa.org/slbn/>

¹¹⁵ <http://www.jnsa.org/seminar/2009/100215/index.html>

め、各地の商工会議所と連携して全国で指導者育成セミナーを開催している¹¹⁶。

○情報処理推進機構セキュリティーセンター（IPA/ISEC）

・情報セキュリティポータルホームページ

IPAでは、「2010年版 10大脅威 あぶり出される組織の弱点！」を公開している。¹¹⁷

・情報セキュリティ安心相談窓口¹¹⁸

IPAでは、IPAでは不審メール110番(情報セキュリティ安心相談窓口に統合)を設けているほか、窓口寄せられた相談をもとに注意喚起を行っている。

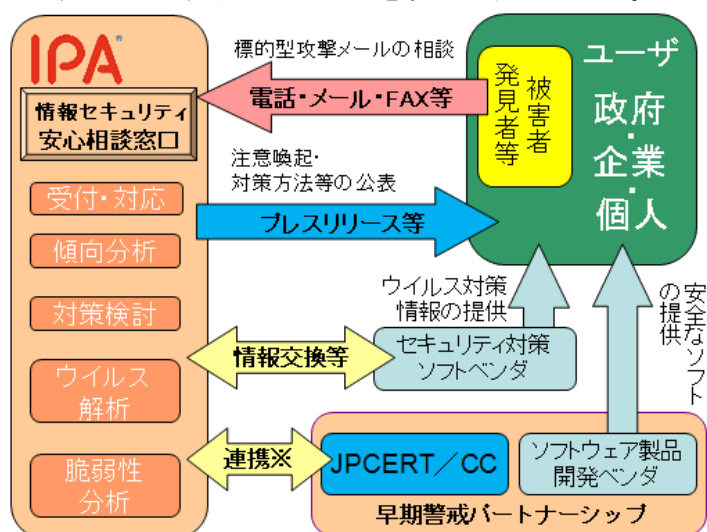


図 情報セキュリティ安心相談窓口¹¹⁹

・IPA しおりシリーズ¹²⁰

「ウイルス対策のしおり」、「スパイウェア対策のしおり」、「ボット対策のしおり」、「不正アクセス対策のしおり」、「情報漏えい対策のしおり」、「インターネット利用時の危険対策のしおり」、「電子メール利用時の危険対策のしおり」を提供している。

・中小企業のためのセキュリティツールライブラリ

IPAでは中小企業向けの情報セキュリティ対策に役立つツールを提供している。このガイドラインに含まれる「5分でできる自社診断シート」を用いて、中小企業の対策

¹¹⁶ <http://www.jnsa.org/ikusei/seminar/>

¹¹⁷ <http://www.ipa.go.jp/security/index.html>

¹¹⁸ <http://www.ipa.go.jp/security/virus/fushin110.html>

¹¹⁹ <http://www.ipa.go.jp/security/virus/fushin110.html>

¹²⁰ <http://www.ipa.go.jp/security/antivirus/shiori.html>

状況を調査した結果、調査対象企業の情報セキュリティ対策状況を確認したところ、66社中 43 社（65%）の点数が合格基準として設定した 70 点に満たなかったとされている。

121

・情報セキュリティ対策¹²²

ウイルス対策、ボットウイルス対策、不正アクセス対策、脆弱性関対策、対策実践情報等の情報セキュリティに関する情報の提供を行っている。

・情報セキュリティ標語・ポスターコンクール

情報セキュリティに関連する様々な被害（コンピュータウイルスの感染、コンピュータへの不正な侵入、ワンクリック不正請求等）に遭わないよう、特に若年層の情報セキュリティ対策への意識を喚起・向上させるため、毎年、小・中・高校生を対象にポスターの募集を行っている。¹²³

¹²¹ <http://www.ipa.go.jp/security/manager/known/tool/index.html>

¹²² <http://www.ipa.go.jp/security/measures/index.html>

¹²³ <http://www.ipa.go.jp/about/press/20091020.html>

・情報セキュリティセミナー

商工会議所を始めとする各種団体の協力の下、中小企業等を対象とした情報セキュリティセミナーを全国各地で開催している（2009年6月開催）。企業や組織の経営者・部門長、セキュリティ担当者、システム管理者、ホームページ運営者、ウェブアプリケーション開発者を主対象に、情報セキュリティの管理面・技術面からの対策に関する普及啓発を実施している。¹²⁴

【試験の体系図】

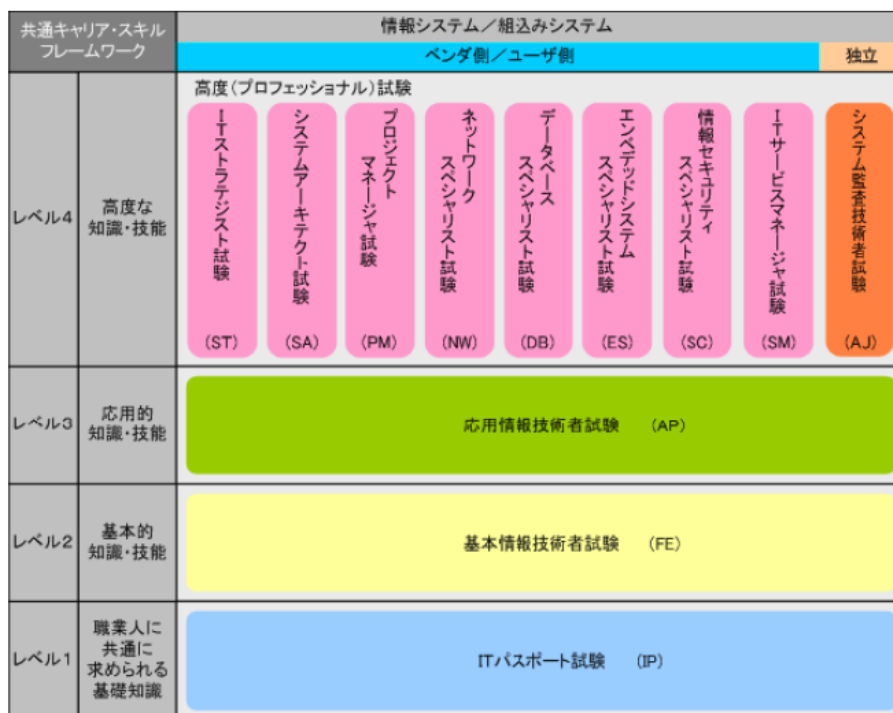


図 情報処理技術者試験における情報セキュリティスペシャリスト試験の位置づけ

○JPCERT コーディネーションセンター (JPCERT/CC)

・IT セキュリティ予防接種調査

JPCERT では、「IT セキュリティ予防接種調査」と題し、標的型攻撃に対する耐性を付けるための仕組みの実証実験を行っている。基本的な予防接種実施手順を踏襲した上で、より幅広い業種と企業規模を対象に、2600人に予防接種を実施している。この調査は、標的型攻撃の特徴のあるメールを被験者に送信し、どれくらいの確率でもそのメールを開いてしまうかを調査するものである。1回目の送信の後に、種明かしメールを送付し、注意を促すことによって、開封率の低下が望めるかを確認するものである。

この調査では、1回目の開封率が、2回目は14.0%となっていることから、ほとんどの場合において2回目の開封率が初回と比較して大幅に減少することが確認されている。

¹²⁴ <http://www.ipa.go.jp/security/event/2009/isec-semi/index.html>

○財団法人ハイパーネットワーク社会研究所、各地方公共団体、中小企業庁、経済産業局

・情報モラル啓発セミナー

企業の経営者、管理者、実務担当者、企業でインターネットを活用する人を対象にしたセミナーを実施している。



図 情報モラル啓発セミナー（佐賀）¹²⁵

○フィッシング対策協議会

・フクロウ先生のフィッシング警告ページ¹²⁶

急増しているフィッシングによる被害の抑止、ユーザの保護、フィッシング対策の普及を目的に、米国 Anti-Phishing Working Group (APWG) が展開する教育プログラムである、Phishing Education Landing Page Program 「フクロウ先生のフィッシング警告ページ」を日本で展開している。フィッシングを目的とするホームページの跡ページにフィッシングに関する警告ページを表示させることで、訪れたホームページがフィッシングを目的としていることや、フィッシングメールに誘導されてしまったことをユーザに認識させる。

・フィッシング フィル¹²⁷

フィッシング フィルは、ゲーム感覚でフィッシングを目的としたホームページの見分け方を学ぶコンテンツである。そこでは、魚のフィルと一緒にフィッシング詐欺にだまされない「URLの見分け方」を覚えるゲームが提供されている。

¹²⁵ <http://www.hyper.or.jp/staticpages/index.php/moral2009saga>

¹²⁶ <http://www.antiphishing.jp/enterprise/landingpage.html>

¹²⁷ <http://www.antiphishing.jp/phil/>

- C/C++ セキュアコーディングセミナー¹²⁸

プログラム開発者を対象に、セキュリティへの十分な配慮が必要な C/C++ 言語で脆弱性を含まない安全なプログラムをコーディングする具体的なテクニックとノウハウを提供するセミナーを開催している。

- フィッシング対策セミナー（経済産業省の委託事業）¹²⁹

フィッシングの危険性や対策について広く周知するためのセミナーを実施している。

○日本ネットワークインフォメーションセンター（JPNIC）

- Internet Week 2010¹³⁰

インターネットに関する技術の研究・開発、構築・運用・サービスに関わる人々が一堂に会し、主にインターネットの基盤技術の基礎知識や最新動向を学び、議論し、理解と交流を深めるためのイベント。インターネットの普及・促進・発展を目的とする、テーマのひとつとして、情報セキュリティに関するプログラムも提供している。

○セキュリティ対策推進協議会（SPREAD）

- SPREAD サポーター

情報セキュリティ人材育成のため、検定試験と養成講座を実施している。公式テキスト「SPREAD 情報セキュリティサポーター標準テキスト改訂版」と「Windows7 追補版」で学習し、検定試験を受け合格した後、SPREAD にサポーター登録を行うことで「SPREAD サポーター」となり認定証が発行される。サポーター養成講座は2009年4月から、日本各地で開催し、2010年9月時点でのサポーター数は280人となっている。¹³¹

○日本ネットワークセキュリティ協会（CSAJ）

総務省からの委託で情報セキュリティ人材育成シンポジウムを開催している。一般利用者の身近で情報セキュリティ対策をサポートする者や情報セキュリティ対策の要となる情報セキュリティ資格保有者等情報セキュリティ人材の育成・確保を目的とする。¹³²

¹²⁸ <https://www.jpcert.or.jp/event/securecoding-TK0-seminar.html>

¹²⁹ http://www.antiphishing.jp/news/event/post_34.html

¹³⁰ <https://internetweek.jp/program/>

¹³¹ <http://www.spread-j.org/supporter/index.html>

¹³² http://www.csa-j.jp/government/other/2010/100215_jnsa.html

○財団法人 日本情報処理開発協会（JIPDEC）

EC サービスに関する情報セキュリティ対策についてのガイドラインが策定されている。検討には JIPDEC が関わり、発行元は、電子商取引推進協議会である。

○インシデント情報共有・分析センター（Telecom-ISAC Japan）

ISP を中心として設立した組織。現在は財団法人日本データ通信協会に編入。情報セキュリティに関する情報を業界内で共有・分析している。

○インターネットホットラインセンター¹³³

インターネットホットラインの国際ネットワークである INHOPE の正会員として、日本におけるインターネット上の違法・有害情報の通報受付窓口を運営している。

○金融情報システムセンター（FISC）

金融機関、保険会社、証券会社、コンピュータメーカー、情報処理会社等の出捐によって設立された機関で、重要な社会インフラである金融情報システムの安全性確保のための自主基準の策定や普及啓発活動を行うとともに、金融機関における情報システムの活用や安全性を巡る諸問題について調査・研究を行っている組織である。金融機関等の会員に向けて、セキュリティーポリシー策定の手引き、安全対策基準、設備基準など各種の資料を発刊している。マルウェア、不正アクセス等の情報セキュリティ対策に関するセミナーや安全対策の運用基準・技術基準などのセミナーを実施している。

○医療情報システム開発センター（MEDIS）

厚生労働省、経済産業省、日本病院会の後援のもと、医療情報セキュリティにかかわる人を対象に医療情報システムのセキュリティを考えるセミナー「MEDIS 講演会～医療情報セキュリティを考える～」を実施している。セミナーにおける資料は有料で提供している。¹³⁴

¹³³ <http://www.internethotline.jp/>

¹³⁴ <http://www.medis.or.jp/0709seminar/sem0920a.html>

○Yahoo

利用者がログイン履歴を確認できる不正アクセス対策のための機能や、フィッシング対策のための機能など、利用者が安全に自社のホームページを使えるような機能を提供している。その他、インターネット犯罪やその対策について普及・啓発するためのコンテンツを提供するなどしている。

・Yahoo!あんしんねっと

有害ホームページのフィルタリングソフトの無料配布している。

・インターネットホットラインセンター¹³⁵

インターネットホットラインの国際ネットワークである INHOPE の正会員として、日本におけるインターネット上の違法・有害情報の通報受付窓口を運営している。

・「C.I.A ～サイバー・インテリジェント・エンジェルズ～」¹³⁶

ヤフーが TBS と実施している共同活動。中高生を対象とした情報セキュリティの啓発キャンペーンを実施している。中高生に人気のモデルを起用し、動画やイベントを通じてインターネットの安全な使い方や便利な使い方を啓発している。3社が共同で企画した映像コンテンツをインターネット経由で提供し、中高生向けに情報セキュリティ対策のリテラシーの向上と PC やインターネットの利用法を各社のホームページにおいて啓発している。

○goo

・キッズ goo¹³⁷

「キッズ goo」では、「goo」と同じ大容量の検索データベースを用いながらも、独自のフィルタリング機能を取り入れることで、多くの検索結果のなかから安全と思われるページのみを表示する、子どもにとって安全かつ実用的な検索サービスを提供。小学校のインターネット授業で、広く活用されている。

また、子どもが安全・安心にインターネットを利用するためのルールとマナーを、ウェブ絵本で紹介している。マウスを使ってページをめくりながら楽しく知識を身につけられる。家庭でインターネットを利用する際のルールを決めるためのツールも用意されている。

2009年度の主な取り組みとしては、3月に「家庭と学校を授業でつなぐ 情報モラル教育研究会」を(株)ジャストシステムとの共同プロジェクトとして発足するとともに、「先生のページ」をスタートした。子どもの情報モラルに対する意識向上に貢献するとともに、

¹³⁵ <http://www.internethotline.jp/>

¹³⁶ <http://www.tbs.co.jp/kids/cia/>

¹³⁷ <http://kids.goo.ne.jp/index.html>

小学校教員の授業づくりや校務をサポートしている。¹³⁸

○NTT ドコモ¹³⁹

小学校・中学校・高等学校および地域コミュニティなどの団体に講師を派遣し、携帯電話を使用する上でのマナーやルール、トラブルへの対処方法を啓発する「ケータイ安全教室」の実施や、サポートツールとして映像教材（DVD/VHS）を学校・団体に無償提供。シニア向けの講師派遣型の教室および映像教材の提供も行っている。¹⁴⁰

○KDDI

・安心・安全講座¹⁴¹

小学生、中高生、教員、保護者を対象に携帯電話を安全に使用するためのルールやマナー、注意点についての講義を実施している。

・見つめてみよう、子どものケータイ¹⁴²

子どもに携帯を持たせる保護者を対象に、子どもの携帯電話の利用に関するルール作りや注意を喚起するためのホームページである。

・JUNIOR net¹⁴³

小学校高学年～中学生を主な対象としてインターネットや携帯電話の安全な利用方法やルール・マナーに関する情報など、楽しみながら学んでいただける学習コンテンツを掲載したホームページである。

○ディズニー

・サイバーネチケットコミック¹⁴⁴

アニメーションやクイズを用いて、チャットの注意点やウイルス、チェーンレターなどネットワーク・エチケットについてコミックで掲載している。

¹³⁸ <http://kids.goo.ne.jp/teacher/>

¹³⁹ <http://www.nttdocomo.co.jp/corporate/csr/social/educational/safety/index.html>

¹⁴⁰ http://www.nttdocomo.co.jp/binary/pdf/info/news_release/report/090713.pdf

¹⁴¹ <http://www.kddi.com/corporate/csr/activity/anshin/kyoshitsu/gaiyo/index.html>

¹⁴² <http://www.kddi.com/anshin/>

¹⁴³ <http://www.kddi.com/junior/>

¹⁴⁴ <http://www.disney.co.jp/cybernetiquette/>

○マイクロソフト

・情報セキュリティ啓発絵本¹⁴⁵

子供向けおよび子供を教える立場の親を対象とした活動である。

¹⁴⁵ http://www.microsoft.com/japan/opinionleaders/education_ict/100611_01.msp

2. 海外の普及啓発活動

2.1. 米国における取組み

○連邦政府

・National Science Foundation (NSF)

アメリカ政府や企業がスポンサーになっている情報セキュリティの普及・啓発をするための官民が連携した共同体組織である。NSFは、2007年の情報セキュリティ啓発月間のスポンサーになった際に、「Stay Safe Online. org」という啓発を目的とするホームページを立ち上げた¹⁴⁶。

また、「K12」というオンラインでの学校教育を提供するサービスを活用して、学校・家庭と協力しながら、若年者向けに情報セキュリティ教育のツールを提供している。その他、情報セキュリティ教材のコンテンツをNCSAに参加する民間企業が無償で提供している。

参加企業の例 (抜粋) ¹⁴⁷	提供コンテンツ
Microsoft	Microsoft Online Safety Resources
Business Software Alliance	Play It CyberSafe
Center for Safe and Responsible Internet Use	Cyberbullying Resources for Parents, Teachers, and Students
Cisco	<ul style="list-style-type: none">● Tween Cyber Safety● Teen Cyber Safety● The Realm - Cartoon Series● Cyberspace Action for Education Campaign
Consortium for School Networking (CoSN)	Cyber Security for the Digital District
Department of Justice	Lesson Plan for Elementary and Middle School Children
Federal Trade Commission	<ul style="list-style-type: none">● Net Cetera● OnGuard Online● YouAreHere
McAfee	<ul style="list-style-type: none">● Family Internet Safety Plan● A Parent's Guide to Social Networking Sites
Seattle Public Schools	<ul style="list-style-type: none">● Cyberbullying Curriculum
Symantec	<ul style="list-style-type: none">● Family Resources● Family Safety Blog● OnlineFamily.Norton

¹⁴⁶ <http://www.staysafeonline.org/>

¹⁴⁷ <http://staysafeonline.mediaroom.com/index.php?s=67&item=56>

・ OnGuard Online

米国では、OnGuard Online - Stop・Think・Click¹⁴⁸という啓発活動が行われている。そのなかで、ボットウイルスに対する警告¹⁴⁹も行われている。

また、ボットウイルスを構成する Spyware について学習するための FLASH ゲームの配布を行っている¹⁵⁰。

○Wisconsin 州

Wisconsin 州では州政府が、ボットウイルスについての啓発活動を WebSite で行っている。¹⁵¹

○Virginia 州

Virginia 州政府の WebSite において、Botnet の紹介を行っている¹⁵²。

○U. S. ISAC

U. S. ISAC 内に設けられた REN-ISAC (Research and Education Networking Information Sharing and Analysis Center)¹⁵³では、アラートの中で標的型攻撃についての注意喚起を行っている。この注意喚起では、技術者向けと CIO 向けの 2 つのバージョンが用意されている。その中で、取るべきアクション等が示されている。標的型攻撃に利用される可能性がある脆弱性の発見や標的型攻撃が確認された場合に、都度、このような警戒情報を発信する。

¹⁴⁸ <http://www.onguardonline.gov/default.aspx>

¹⁴⁹ <http://www.onguardonline.gov/topics/botnets-hackers-spam.aspx>

¹⁵⁰ <http://www.onguardonline.gov/games/beware-spyware.aspx>

¹⁵¹ <http://itsecurity.wi.gov/subcategory.asp?linksubcatid=2740&linkcatid=2908&linkid=1499&locid=89>

¹⁵² <http://www.vita.virginia.gov/communications/publications/informationSecurityTips/default.aspx?>

¹⁵³ http://www.ren-isac.net/alerts/banking-attacks_technical_201001.html

2.2. ドイツにおける取組み

ドイツでは、国内の情報セキュリティに関してイニシアティブとする連邦情報セキュリティ庁(BSI¹⁵⁴)が、Anti-Botnet-Beratungszentrum というホームページ¹⁵⁵を立ち上げている。情報提供のほか、ボットウイルスの検知・クリーナーや推奨される Windows の設定、推奨対策製品を個人ユーザ、企業ユーザ毎に情報提供する等のボットウイルス対策支援活動が行われている。

2.3. 英国における取組み

英国では、Businesslink.gov.uk¹⁵⁶が E-Commerce 企業向けに Botnet についての簡単な情報提供を行っている¹⁵⁷。

また、nidirect online service¹⁵⁸が提供するホームページにて Be secure online¹⁵⁹というコンテンツがあり、Spyware や Bot についての紹介がある。

普及啓発として大きな活動としては、makitsecure.org¹⁶⁰がある。この中で、Spyware¹⁶¹についての解説や予防策を紹介している。

同様に Direct gov の WebSite の中に、Be Secure Online¹⁶²というページがあり、ボットウイルスに感染しないためのガイドラインを紹介している。¹⁶³

2.4. フランスにおける取組み

フランスの政府が運営するセキュリティポータルホームページ¹⁶⁴において、ボットウイルスに関する簡単な情報提供を行っている。ボットウイルスの発見方法等の紹介も行っている。¹⁶⁵

2.5. オランダにおける取組み

オランダでは、GOVCERT¹⁶⁶がボットウイルスに関するビデオを作成して、配布¹⁶⁷を行っ

¹⁵⁴ https://www.bsi.bund.de/cIn_183/DE/Home/home_node.html

¹⁵⁵ <https://www.botfrei.de/Anti-Botnet-Beratungszentrum>

¹⁵⁶ <http://www.businesslink.gov.uk/bdotg/action/aboutus?page=AboutUs>

¹⁵⁷ <http://www.businesslink.gov.uk/bdotg/action/detail?itemId=1075385962&type=RESOURCES>

¹⁵⁸ <http://www.nidirect.gov.uk/index.htm>

¹⁵⁹ <http://www.nidirect.gov.uk/index/information-and-services/leisure-home-and-community/technology-and-online-services/computers-and-the-internet/be-secure-online.htm>

¹⁶⁰ <http://www.makeitsecure.org/en/index.html>

¹⁶¹ <http://www.makeitsecure.org/en/securityBasics.html>

¹⁶² http://www.direct.gov.uk/en/HomeAndCommunity/TechnologyInYourHome/InternetTechnologies/DG_10038607

¹⁶³ http://www.getsafeonline.org/nqcontent.cfm?a_id=1044

¹⁶⁴ <http://www.securite-informatique.gouv.fr/>

¹⁶⁵ http://www.securite-informatique.gouv.fr/gp_article636.html

¹⁶⁶ <http://www.govcert.nl/>

ている。

2.6. オーストラリアにおける取組み

オーストラリアでは、CCC と類似の仕組みによって、ISP 側でボットウイルスのトラフィックを遮断する試み¹⁶⁸が行われている。

2.7. 欧州 (EU) における取組み

EU では、7th Framework の 1 つのプロジェクトに VIKING プロジェクト があり、その中で SCADA 向けのセキュリティを研究している。その中で、標的型攻撃に対する対策が研究 されている。また、ICT-FORWARD Project という取組みが立ちあがっており、その中 でも標的型攻撃を重大な脅威 として位置付けて取扱っている。ENISA 等のレポートでも標 的型攻撃への備えについての記載があるほか、European Information Sharing and Alert System (EISAS) という取組みを運用している。この取組みは、中小企業と一般市民をタ ーゲットとして、脅威や脆弱性、攻撃についての情報委を共有し、警戒を促す事を目的と している。その理由として、ENISA のエクゼクティブディレクターである Mr. Andrea Pirotti は、「中小企業及び一般市民は標的型攻撃の対象に最もなり易いが、彼らは往々に して、その規模ゆえに、情報資産を守るためのセキュリティの専門家を雇用することがで きない。その結果、攻撃の被害者に容易になりえると考えている」と述べている。

2.8. ITU における取組み

ITU では、Australian Internet Security Initiative (AISI) が開発したツールを基に、 ITU Botnet Mitigation Toolkit¹⁶⁹を加盟各国に配布することが検討されている。ボット ウイルスへの対応は国際的な枠組みで行う必要がある。そのため、各国間でボットウイル スに対する認識を高めるために、このツールキットが開発されている。

2.9. APEC における取組み

2010 年 10 月 30 日～31 日に沖縄県名護市で開催された APEC 電気通信・情報産業大臣会 合において、「APEC サイバーセキュリティ意識啓発の日」イベントを毎年実施し、APEC 域

¹⁶⁷ <http://www.govcert.nl/render.html?it=147>

¹⁶⁸ http://www.dbcde.gov.au/online_safety_and_security/cybersafety_plan/internet_service_provider_isp_filtering

¹⁶⁹ <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit.pdf> ITU Botnet Mitigation Project: Background & Approach

内における意識啓発を推進していくことが確認されている。

2010年は、「APEC サイバーセキュリティ意識啓発の日」に係わる行事として、APEC 加盟エコノミーにより採択された共通のロゴや、一般ユーザがインターネットを安心・安全に利用する上で推奨される情報セキュリティ対策（サイバーセキュリティトップティップス）を公開した。また、併せてエコノミー毎に独自の取り組みも実施され、APEC 電気通信・情報産業大臣会合においては「APEC サイバーセキュリティ意識啓発ポスター展示イベント」が日韓共催で実施された。¹⁷⁰

¹⁷⁰ http://www.soumu.go.jp/menu_news/s-news/02ryutsu03_02000012.html