平成25年10月26日
情報セキュリティマネージャー
ISACAカンファレンス2013

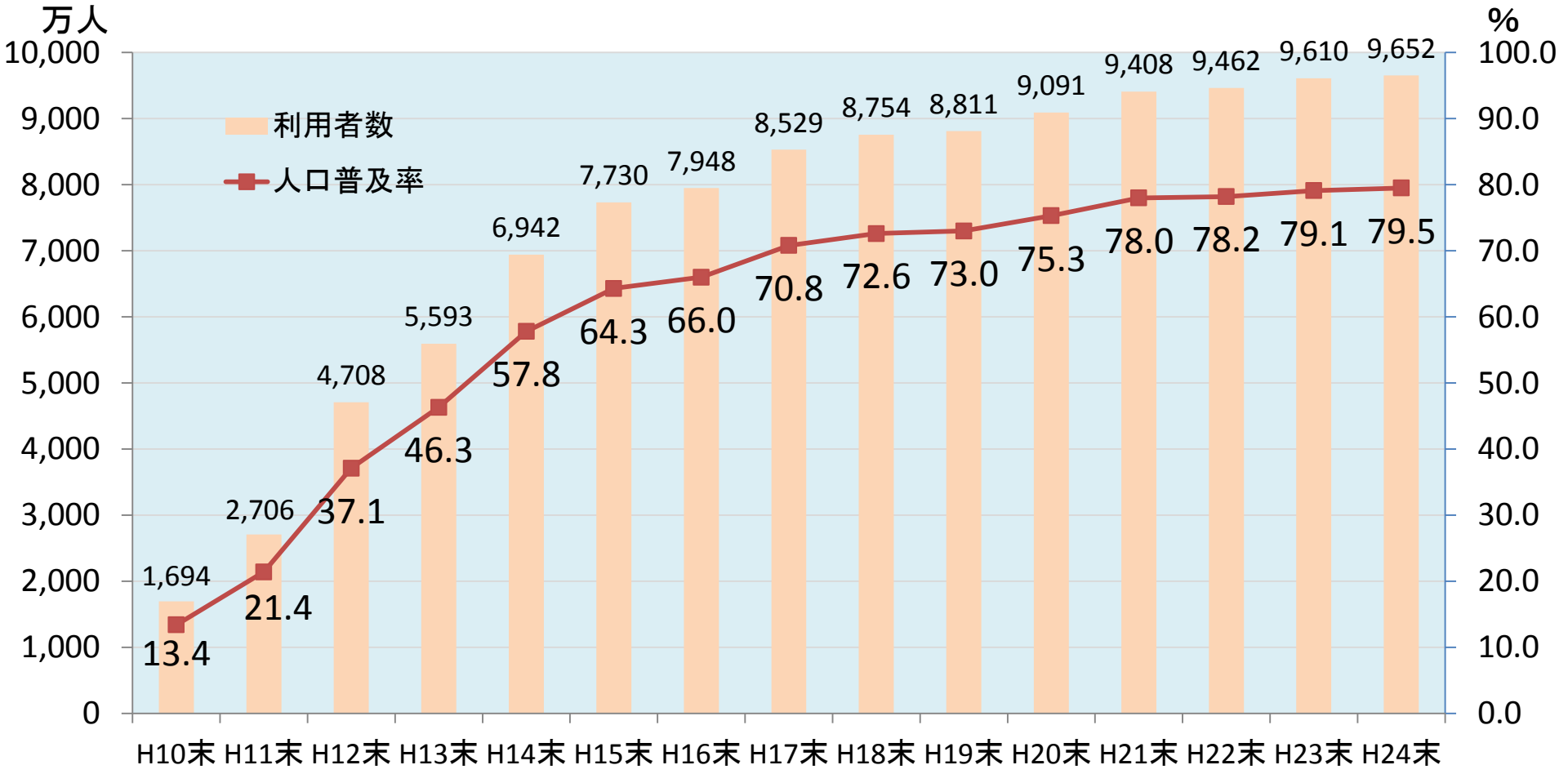
サイバー犯罪の現状と対策

警察庁生活安全局情報技術犯罪対策課
課長補佐　間仁田　裕美

サイバー犯罪情勢

インターネットの普及状況

○ 平成24年末で国民の8割がインターネットを利用している。
○ 13～49歳までの年齢階層では利用率は9割を超えている。60歳以上も増加傾向。
○ 個人のインターネット利用率は大都市のある都府県を中心に高い。



出典:平成24年通信利用動向調査(総務省)

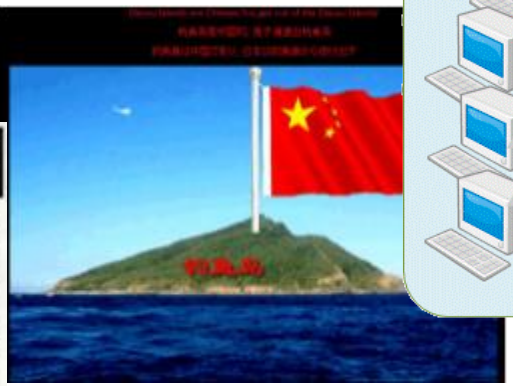
サイバー空間の脅威

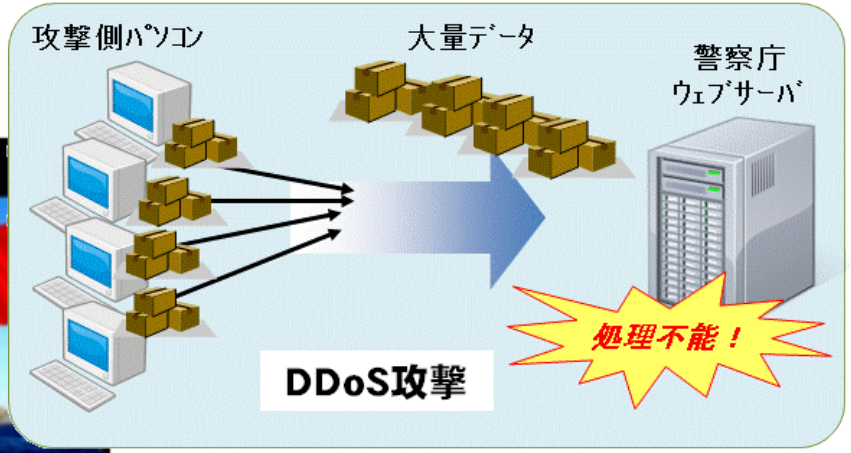
国民生活を脅かすサイバー犯罪

- 不正アクセス禁止法違反
- コンピュータ・電磁的記録対象犯罪等
- ネットワーク利用犯罪

国の重要な情報やシステムを標的としたサイバー攻撃

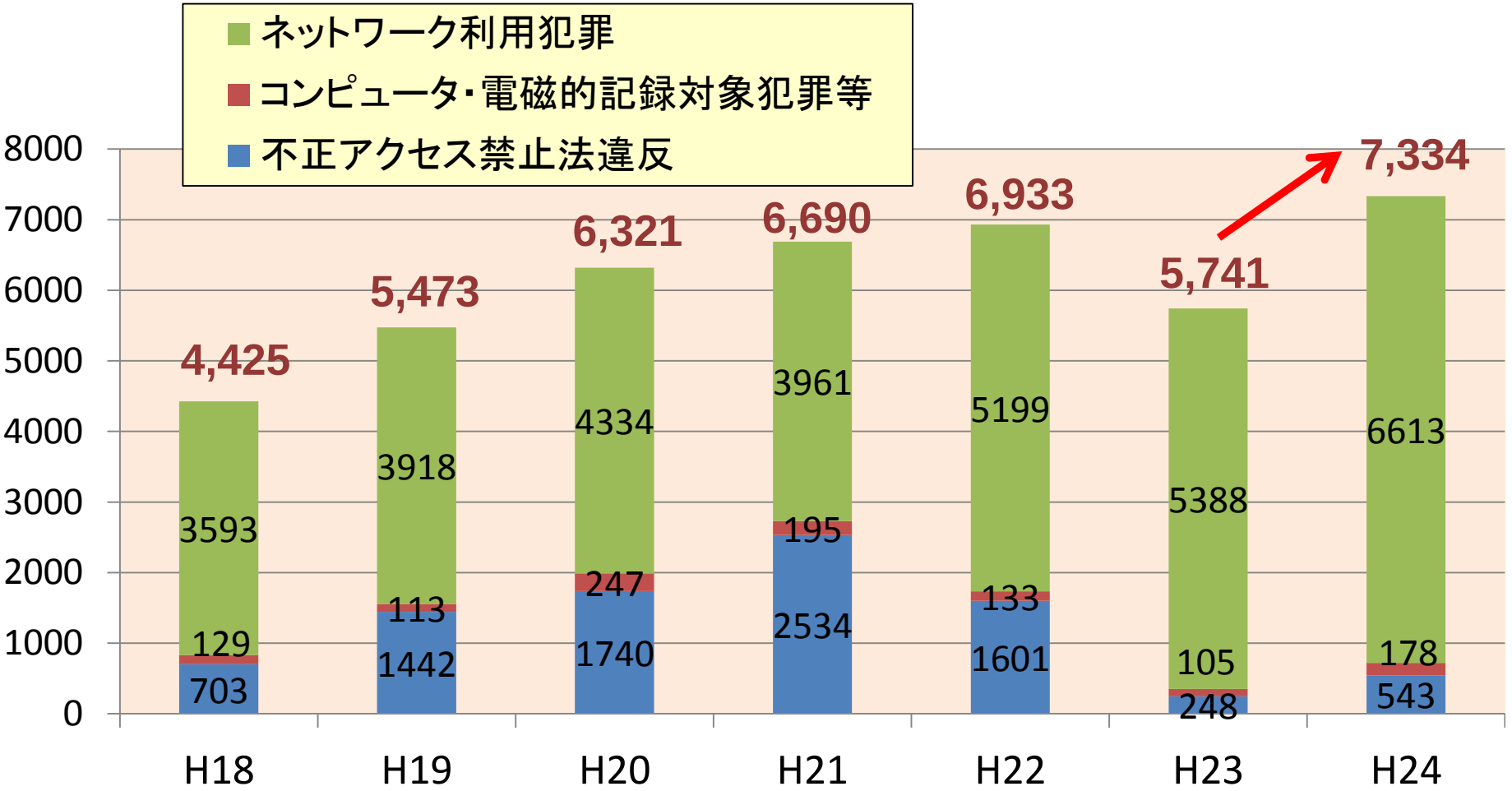
- サイバーテロ
- サイバーインテリジェンス





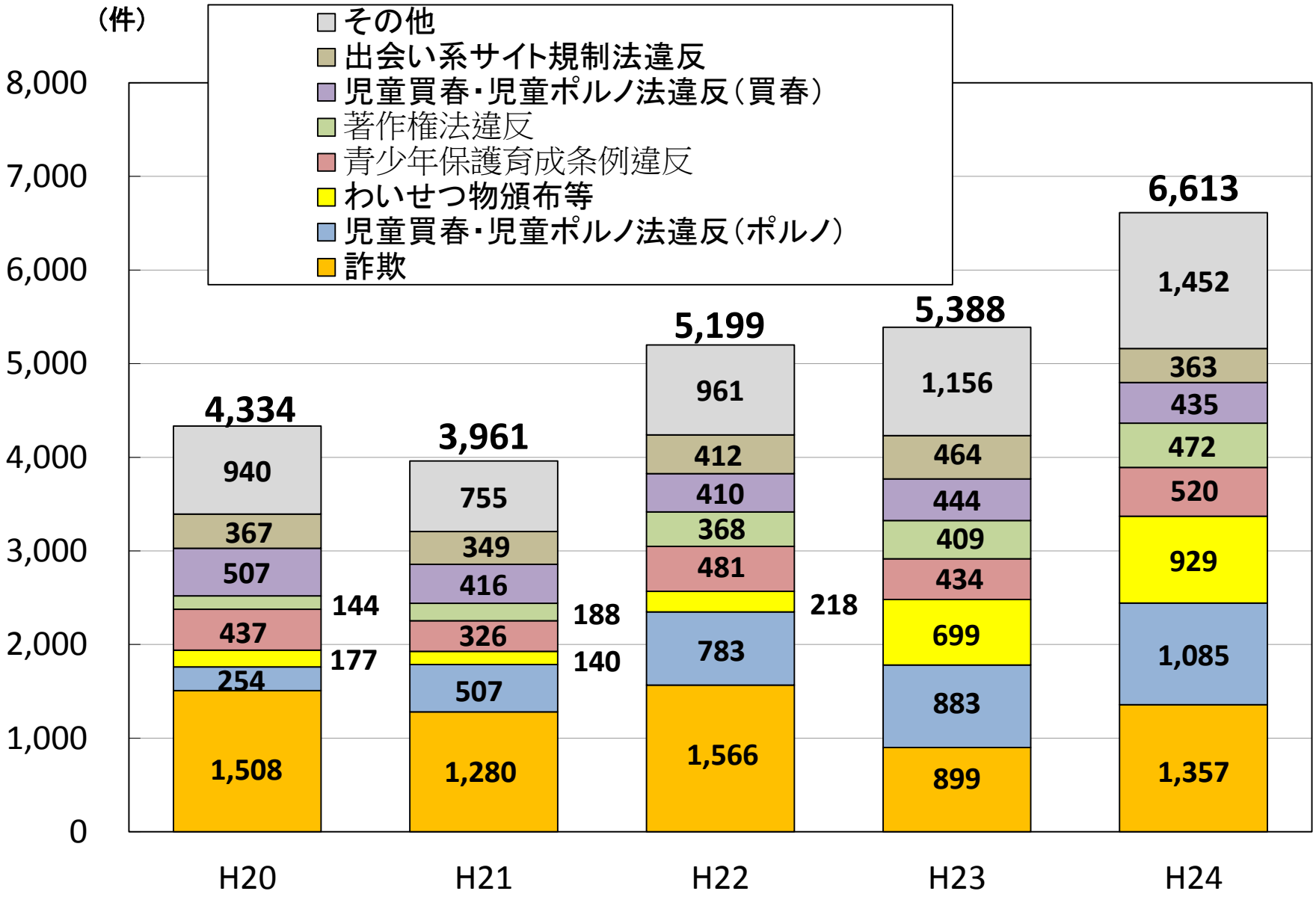
サイバー犯罪の検挙状況

- ○ 平成24年中のサイバー犯罪の検挙件数は7,334件。
- ○ ネットワーク利用犯罪検挙件数は過去最高を記録。
- ○ 不正指令電磁的記録に関する罪は41件（コンピュータ・電磁的記録対象犯罪等に計上）。
- ○ 不正アクセス禁止法違反では、検挙人員が法施行以降最多に。

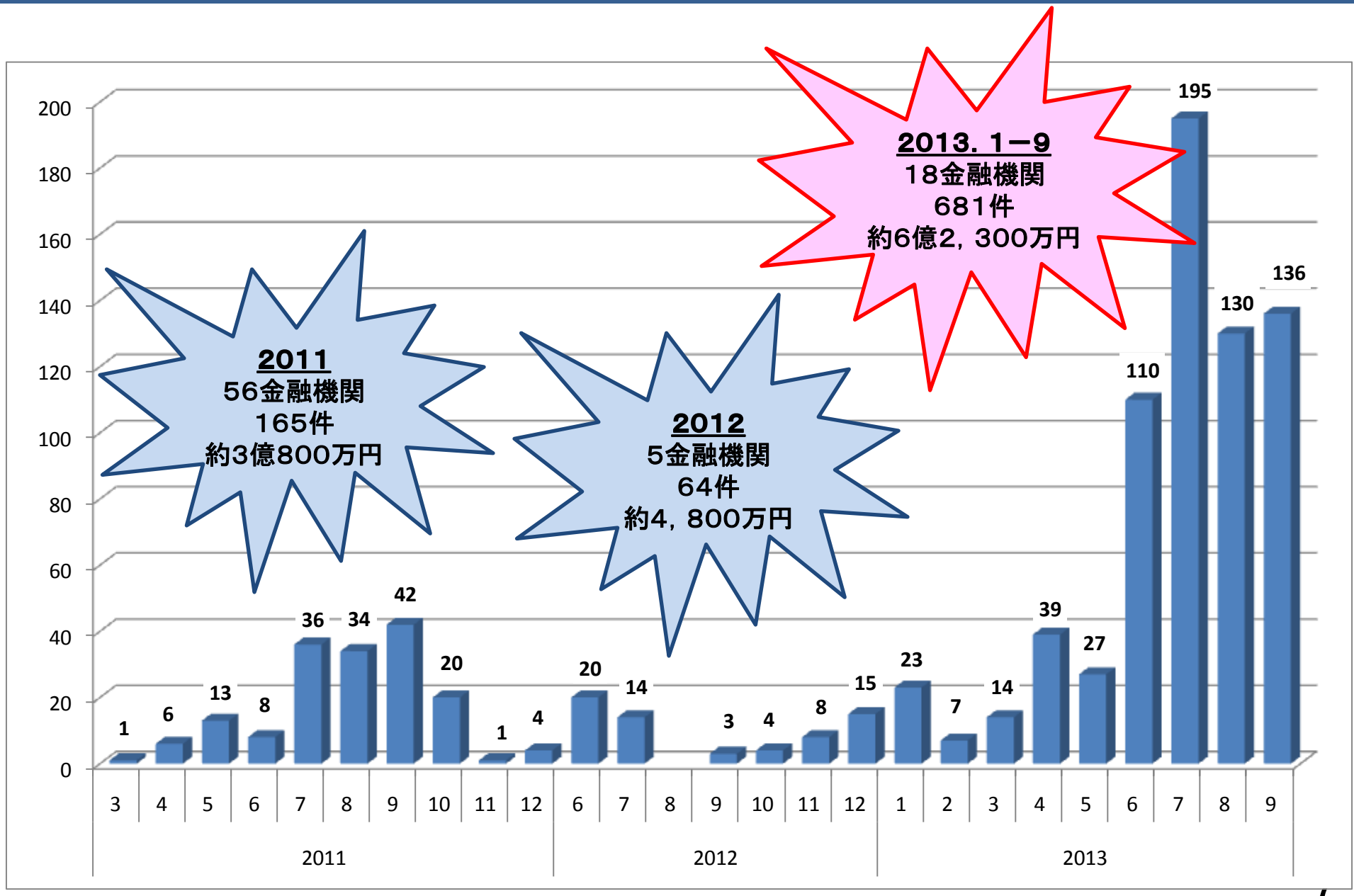


サイバー犯罪の検挙状況

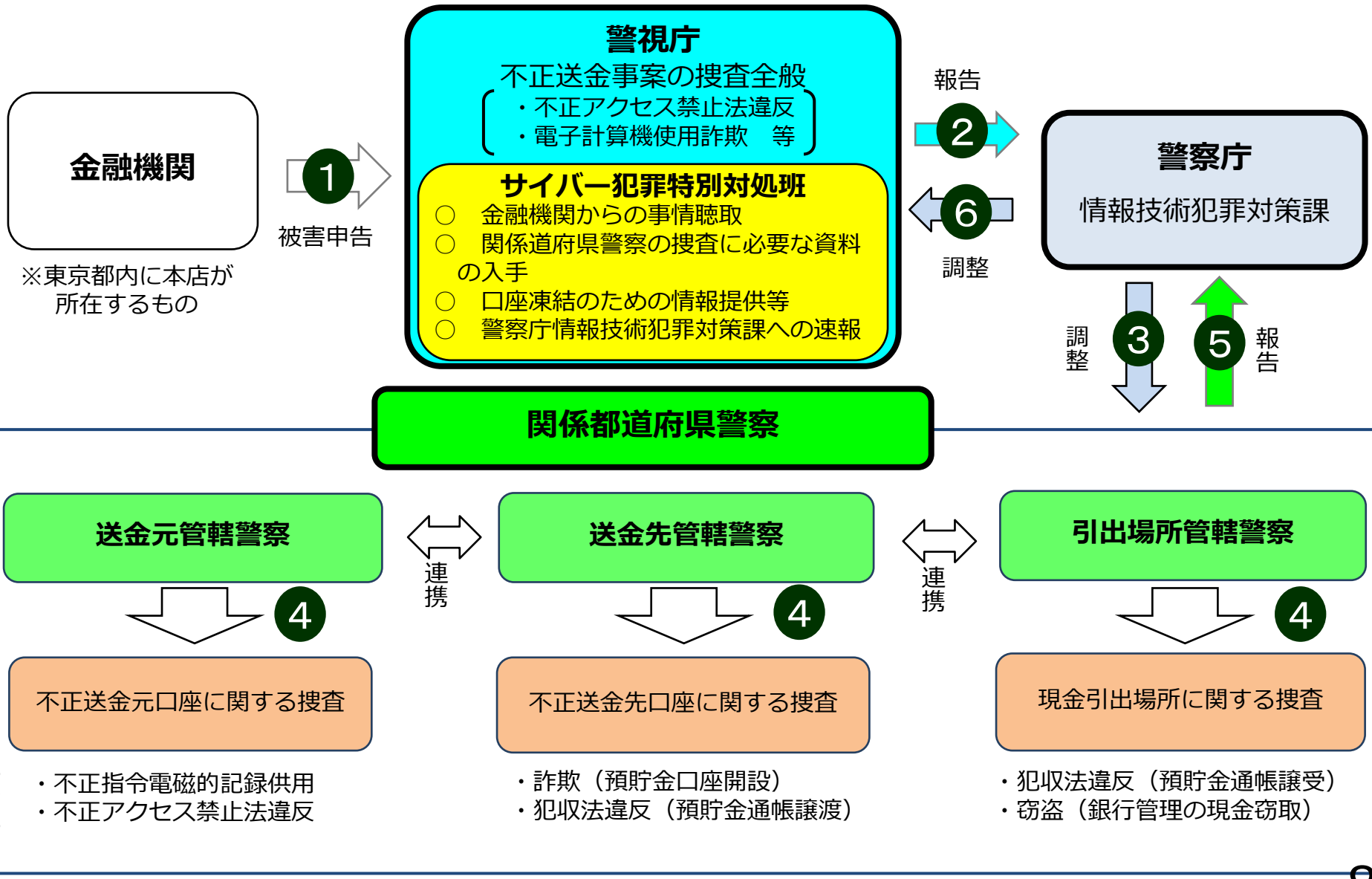
ネットワーク利用犯罪の内訳



インターネットバンキングに係る不正送金事案

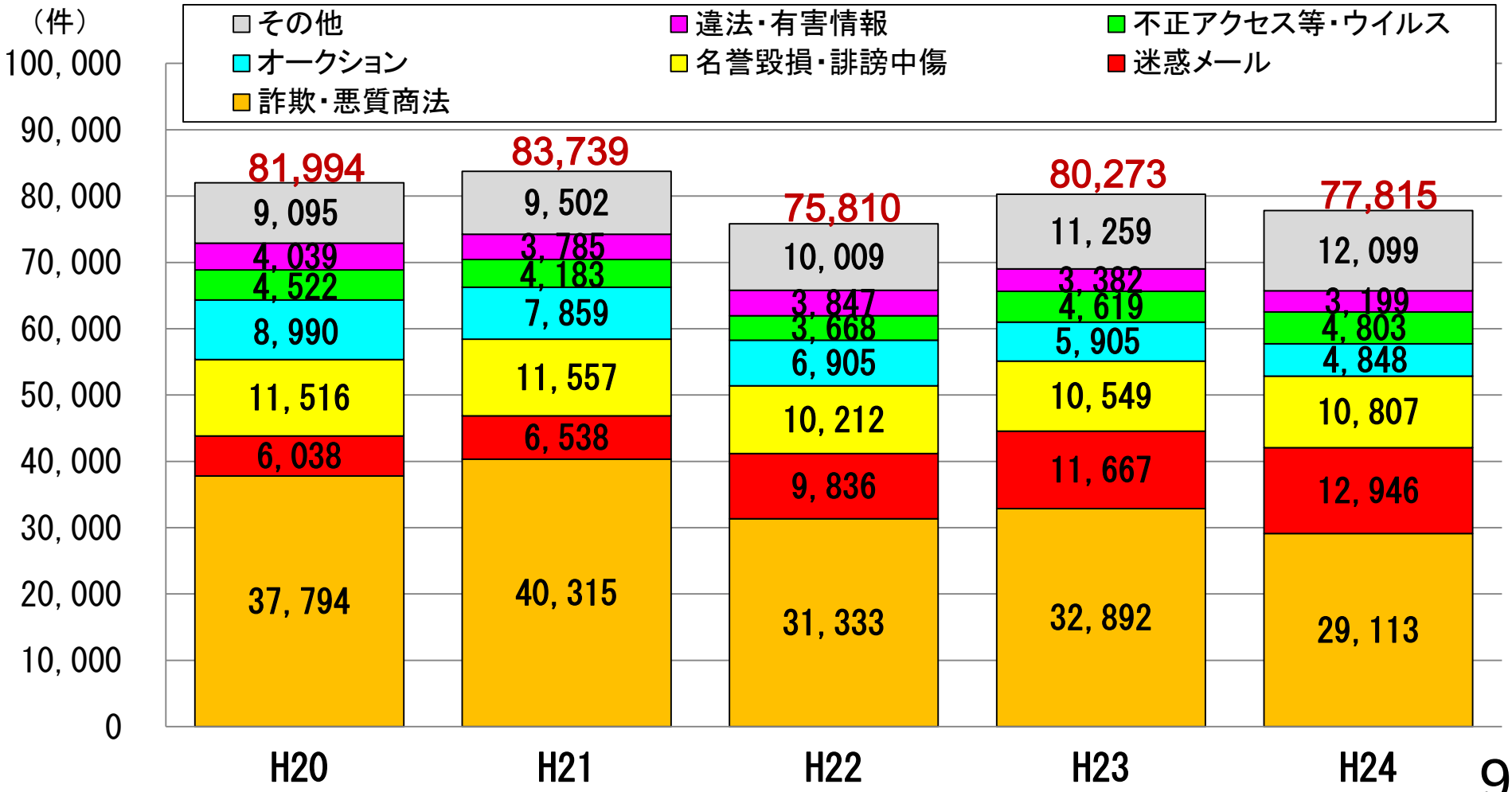


サイバー犯罪特別対処班



サイバー犯罪等に関する相談状況

○ 平成24年中に都道府県警察の相談窓口で受理したサイバー犯罪等に関する相談件数は77,815件。
○ 詐欺・悪質商法に関する相談が最も多いが、迷惑メールに関する相談が増加傾向。



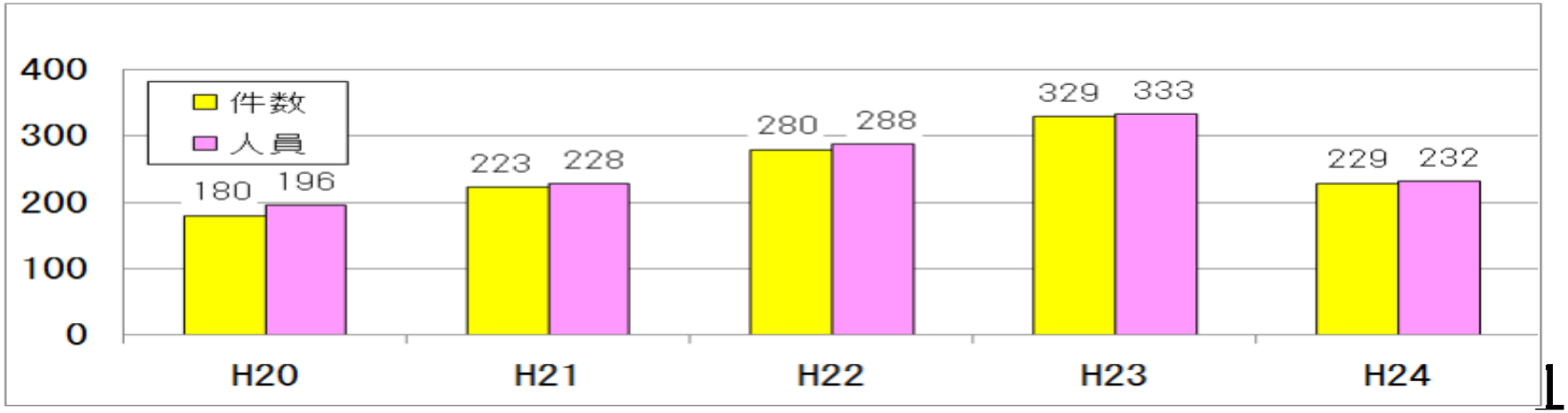
インターネット上の自殺予告事案

オンラインゲームのメール機能を利用した自殺予告事案へ対応した例

○　A警察は、知人がオンラインゲームのメール機能を利用して自殺をほのめかす内容を送信しているとの通報を受け、ゲームの運営会社に対する緊急照会を実施。
○　メールの発信場所としてインターネットカフェを特定したため、カフェの協力を得て張込みを実施し、来店した発信者を保護した。

書込者を山中において保護した例

○　B警察は、電子掲示板に自殺をほのめかす書き込みがあるとの通報を受け、電子掲示板の管理者等に対する緊急照会を実施。
○　判明した契約者情報からC警察管内の書込者を特定し、C警察に書込者の保護を依頼。
○　保護依頼を受けたC警察は、書込者がいると想定された山中を探索した結果、書込者を発見し保護した。



政府における情報セキュリティ対策

情報セキュリティ対策のための政府の体制

内閣官房情報セキュリティセンター（NISC）

2005.4.25設置

①情報セキュリティ政策に関する基本戦略の立案

②政府機関の総合対策促進

③政府機関の事案対処支援

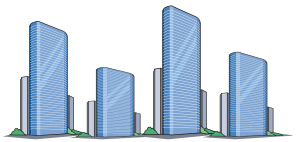
④重要インフラの情報セキュリティ対策

重要インフラ所管省庁

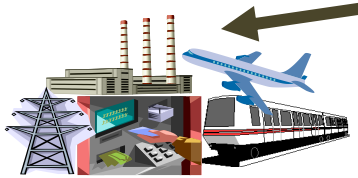
- 金融庁
- 総務省
- 国土交通省
- 経済産業省

情報セキュリティ関係省庁

- 警察庁
- 防衛庁
- 総務省
- 経済産業省



政府機関
（各省庁）



重要インフラ

企業

個人

政府のサイバーセキュリティ戦略

IT総合戦略本部

決定

設置根拠：IT基本法（H12年11月）
本部長：内閣総理大臣
副本部長：情報通信技術（IT）政策担当大臣、内閣官房長官、総務大臣、経済産業大臣
本部員：国家公安委員長その他の国務大臣及び有識者10名

「世界最先端IT国家創造」宣言

（平成25年５月24日IT総合戦略本部決定）

○ 閉塞を打破し、再生する日本へ向け、また、世界最高水準のIT利活用社会の実現と成果の国際展開を目標とする第二次安倍内閣の「新たなIT戦略」

Ⅳ. 利活用の裾野拡大を推進するための基盤の強化
3.　サイバーセキュリティ
サイバーセキュリティの強化は、国家の安全保障のみならず、IT・データ利活用の促進等を通じた我が国の産業競争力強化等のためにも不可欠なものである。
「サイバーセキュリティ戦略」に基づき、具体的な施策を推進することを通じて、世界を率先する強靭で活力あるサイバー空間を構築することにより「サイバーセキュリティ立国」を実現する。

情報セキュリティ政策会議

決定

設置根拠：IT戦略本部決定（H17年５月）
議長：内閣官房長官
議長代理：情報通信技術（IT）政策担当大臣
構成員：国家公安委員長、総務大臣、経済産業大臣、防衛大臣及び有識者６名

サイバーセキュリティ戦略

（平成25年６月10日情報セキュリティ政策会議決定）

○ 政府の中期的な情報セキュリティ戦略

サイバーセキュリティ2013

○ 政府の情報セキュリティ政策に係る　年度計画

（平成25年６月27日情報セキュリティ政策会議決定）

サイバー犯罪の特徴

【サイバー犯罪の特徴】

- **犯罪の実行者の特定が困難**

  犯罪の実行者は、第三者のコンピュータを「踏み台」にして犯罪を敢行することが可能。

- **被害が潜在化する傾向**

  不正アクセス行為を受けたり、コンピュータ・ウイルスに感染したりしている事実を被害者自らが把握できず、違法行為による被害が潜在化する傾向にある。

- **国境を容易に越えて実行が可能**

  コンピュータとインターネットへのアクセスさえ確保できれば、容易に国境を越えてサイバー犯罪を敢行することが可能。

官民が一体となって社会全体で取り組むべき課題

警察におけるサイバーセキュリティ対策の推進体制

警察庁・管区警察局

次長を庁とするサイバー空間の脅威に対する総合対策委員会

長官官房審議官（サイバーセキュリティ戦略担当）

警察のサイバーセキュリティ戦略を統括

重点的に検討・推進する施策

- ○ 国民生活を脅かすサイバー犯罪への対処能力の向上
- ○ 国の重要な情報やシステムを標的としたサイバー攻撃への対処能力の向上
- ○ 国際連携の強化
- ○ 情報通信技術の高度化や法改正を踏まえた解析体制・執行力の確保

生活安全部門	警備部門	情報通信部門
情報技術犯罪対策課	警備企画課 （サイバー攻撃対策官 サイバー攻撃分析センター）	情報技術解析課 （サイバーフォース 技術センター 不正プログラム解析センター）

↔ ↔

捜査の指導・調整　等

都道府県警察

サイバー犯罪・サイバー攻撃対策プロジェクト

（部門横断的な対策の枠組み）

犯罪捜査　被害の未然防止・拡大防止　事案発生時の緊急対処　平素からの情報収集・分析

サイバー空間の脅威に対する総合対策

～サイバー空間の脅威に対する社会全体の対処能力の強化～

基本方針

- ○ 社会全体でサイバー空間の脅威に立ち向かう気運の醸成
- ○ 警察における態勢の強化及び捜査環境の整備
- ○ 外国捜査機関等との連携による国際連携の強化

サイバー犯罪対策

- ☆ 抑止対策と捜査活動の連動
- ☆ 新しい手口、国境越えて発生するサイバー犯罪の取締りの強化
- ☆ サイバー犯罪を抑止するための環境整備

不正アクセス

- ○ 不正アクセス防止対策に関する官民意見集約委員会（官民ボード）の設置
- ○ 「不正アクセス行為の防止対策に関する行動計画」の策定
- ○ 不正アクセス禁止法の法定刑引き上げ・フィッシングの禁止・処罰等の不正アクセス禁止法改正の検討

違法・有害情報対策

- ○ インターネット・ホットラインセンター（ＩＨＣ）の運用
- ○ ＩＨＣからの通報に係る「全国協働捜査方式」の実施
- ○ 警察庁等による環境整備等を踏まえた、一部のＩＳＰによる自主的なインターネット上の児童ポルノブロッキングの開始
- ○ コミュニティサイトの利用に起因する犯罪から子どもを守るための緊急対策の実施

サイバーテロ・サイバーインテリジェンス対策

- ☆ 総合的な対策を推進するための態勢の確保
- ☆ 未然防止のための官民連携の推進
- ☆ サイバー攻撃事案の実態解明の推進

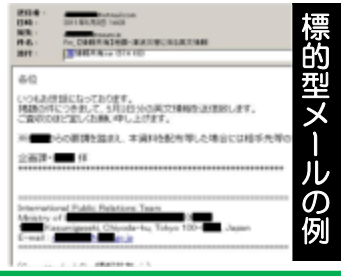
サイバーテロ

- ○ 重要インフラ事業者等への個別訪問
- ○ サイバーテロ対策協議会を通じた重要インフラ事業者等への情報提供
- ○ サイバー攻撃の発生を想定した官民共同訓練の実施
- ○ 内閣官房等関係省庁との連携

サイバーテロ対策協議会

サイバーインテリジェンス

- ○ 先端技術を有する全国約４８００の事業者と「サイバーインテリジェンス情報共有ネットワーク」を確立し、標的型メール等に関する情報を集約分析、注意喚起



標的型メールの例

サイバー犯罪対処能力の強化等に向けた緊急プログラム

趣旨

一連の遠隔捜査ウイルス等による犯行予告事案により明らかとなった警察の捜査力の不足を踏まえ、サイバー空間において今後起こり得る様々な事態にも対処できるよう、サイバー犯罪対処能力の強化等に向けて当面緊急に推進すべき施策を取りまとめたもの。

骨子

対処能力の向上

➢ 捜査力及び解析力の強化

- 官民人事交流
- 民間企業への講義委託等による効果的な教育・訓練の実施
- ハッカーからの協力の確保
- Tor等高度匿名化技術に係る調査・研究　等

➢ 体制の整備

- サイバー犯罪捜査員・解析担当職員等の増員
- 警察庁の体制の在り方の検討
- 不正プログラム解析センターの拡充　等

➢ 資機材の整備

- 新種のウイルスを検知するためのシステムの高機能化　等

国際連携の推進

- 外国捜査機関等との情報共有の強化
- サイバー犯罪に係るリエゾン派遣　等

民間事業者等の知見の活用

➢ 情報共有枠組みの構築

- アンチウイルスベンダーとの情報共有枠組みの構築　等

➢ 官民一体となったサイバー犯罪抑止対策の推進

- 通信履歴の保存に係る民間事業者等の取組を促進
- 悪質なサイト管理者の管理責任の明確化
- スマートフォン用アプリに係る被害防止対策　等

➢ 民間の知見の捜査等への活用

- 民間事業者等への手口分析等の嘱託
- 解析対象となる電子機器等の技術情報に関する協力強化

広報啓発

- 「情報セキュリティ月間」（毎年２月）、民間事業者との会議、ウェブサイト等あらゆる機会・手段を通じた広報啓発活動の推進

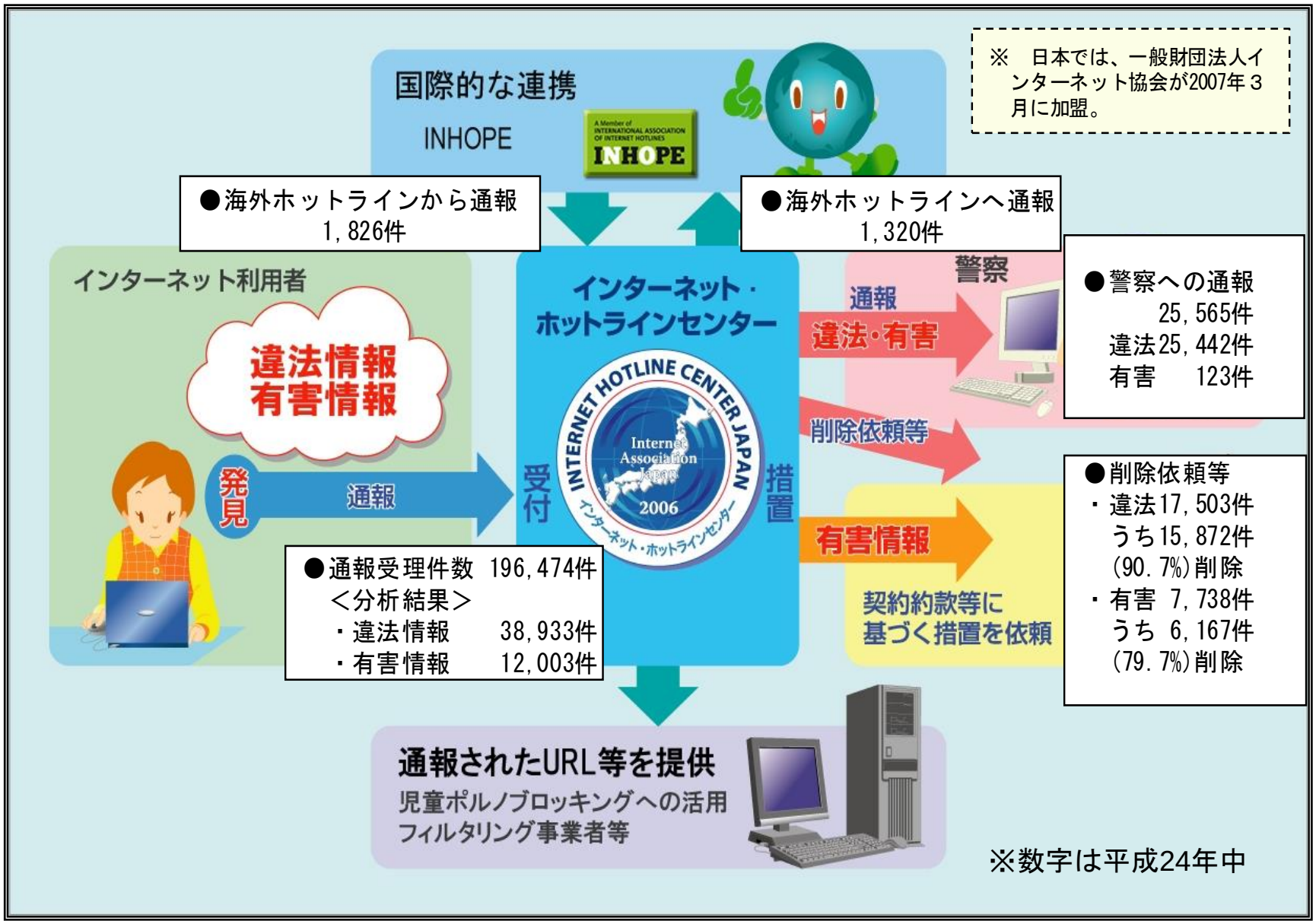
違法有害情報への対策

インターネット・ホットラインセンター（IHC）

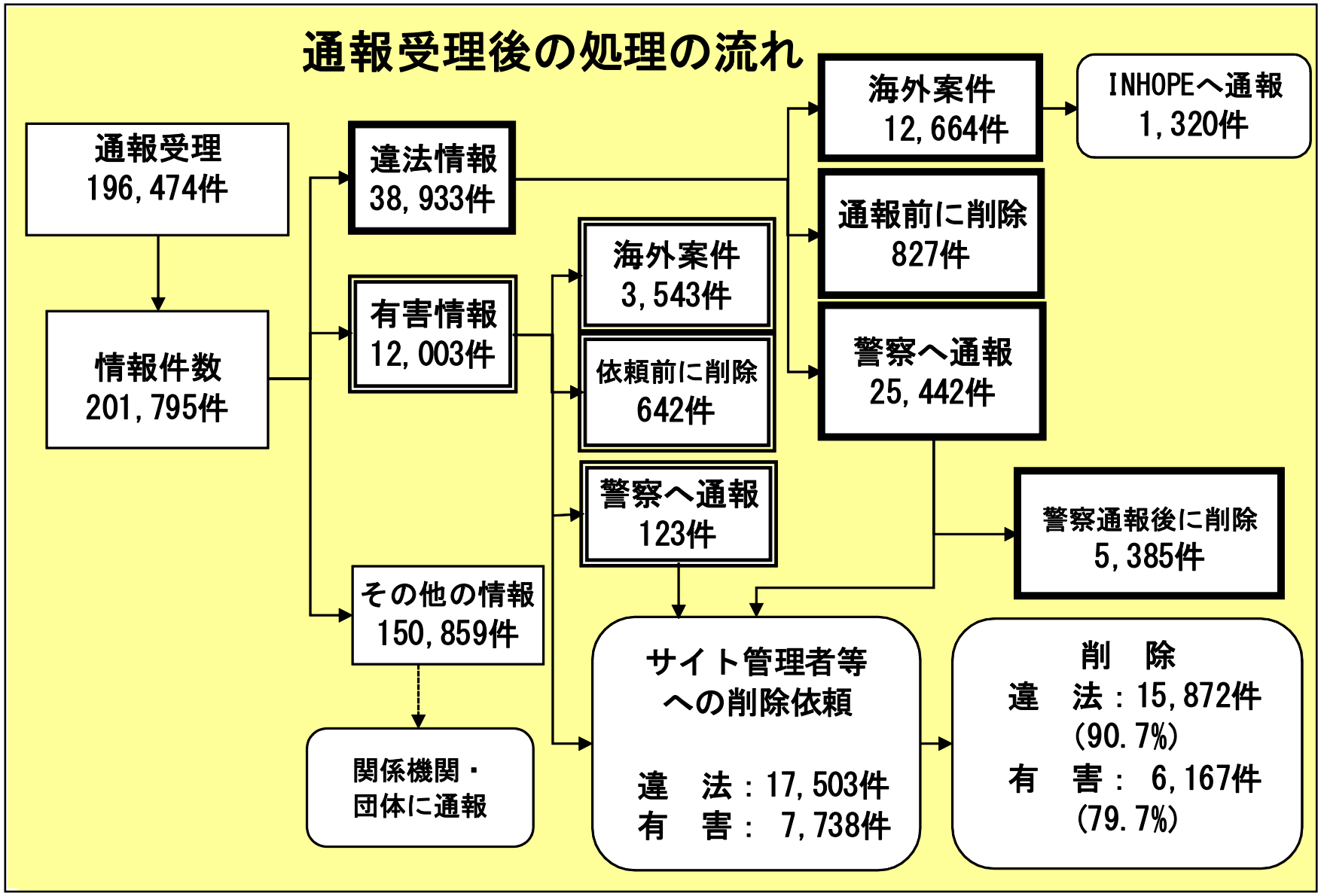
○　インターネット利用者から違法・有害情報に関する情報を受け付け、警察への情報提供、電子掲示板の管理者等への削除依頼等を実施。

http://www.internethotline.jp

IHCの運用状況


国際的な連携
INHOPE
※　日本では、一般財団法人インターネット協会が2007年３月に加盟。
●海外ホットラインから通報
1,826件
●海外ホットラインへ通報
1,320件
インターネット利用者
違法情報
有害情報
発見
通報
インターネット・
ホットラインセンター
受付
措置
INTERNET HOTLINE CENTER JAPAN
Internet Association Japan
2006
インターネット・ホットラインセンター
通報
違法・有害
警察
●警察への通報
25,565件
違法25,442件
有害　123件
削除依頼等
●削除依頼等
・違法17,503件
うち15,872件
(90.7%)削除
・有害 7,738件
うち 6,167件
(79.7%)削除
有害情報
契約約款等に
基づく措置を依頼
●通報受理件数　196,474件
＜分析結果＞
・違法情報　38,933件
・有害情報　12,003件
通報されたURL等を提供
児童ポルノブロッキングへの活用
フィルタリング事業者等
※数字は平成24年中

IHCに通報される違法・有害情報の流れ



違法情報・有害情報の類型

IHCに通報される違法情報

① **わいせつ物公然陳列**（刑法第１７５条第１項）
② **児童ポルノ公然陳列**（児童ポルノ法第７条第４項）
③ **売春目的等の誘引**（売春防止法第５条第３号及び第６条第２項第３号）
④ **出会い系サイト規制法違反の禁止誘引行為**（同法第６条）
⑤ **薬物犯罪等の実行又は規制薬物**（覚せい剤、麻薬、向精神薬、大麻、あへん及びけしがら）**の濫用を、公然、あおり、又は唆す行為**（麻薬特例法第９条）
⑥ **規制薬物の広告**（覚せい剤取締法第２０条の２、麻薬及び向精神薬取締法第２９条の２及び第５０条の１８、大麻取締法第４条第１項第４号）
⑦ **預貯金通帳等の譲渡等の勧誘・誘引**（犯罪収益移転防止法第２７条第４項）
⑧ **携帯電話等の無断有償譲渡等の勧誘・誘引**（携帯電話不正利用防止法第２３条）
⑨ **識別符号の入力を不正に要求する行為**（不正アクセス禁止法第７条第１号）
⑩ **不正アクセス行為を助長する行為**（不正アクセス禁止法第５条）

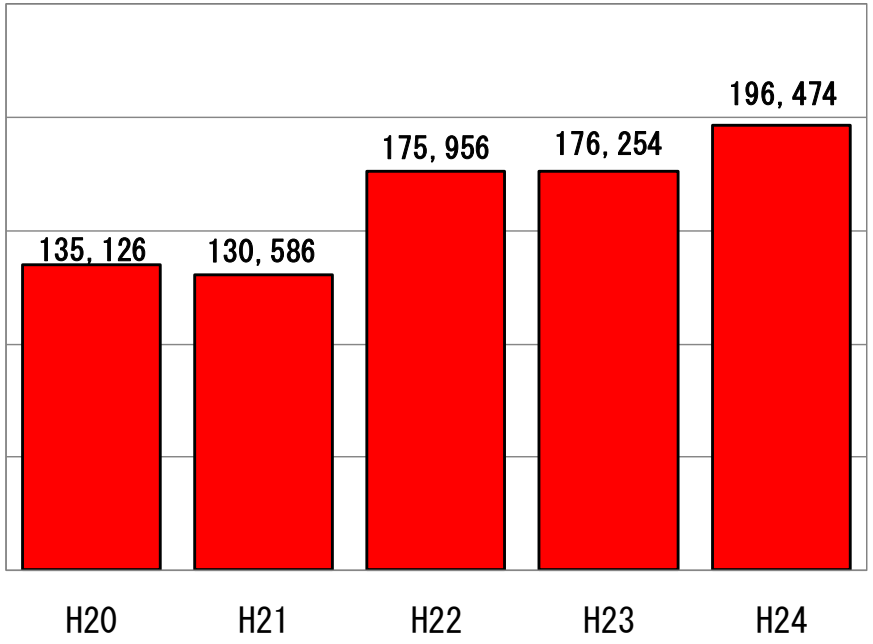
IHCに通報される有害情報

① **情報自体から、違法行為**（けん銃等の譲渡等、爆発物の製造、児童ポルノの提供、公文書偽造、殺人、脅迫等）**を直接的かつ明示的に請負・仲介・誘引等する情報**
② **列挙する違法情報について、違法情報該当性が明らかであると判断することは困難であるが、その疑いが相当程度認められる情報**
③ **人を自殺に誘引・勧誘する情報**

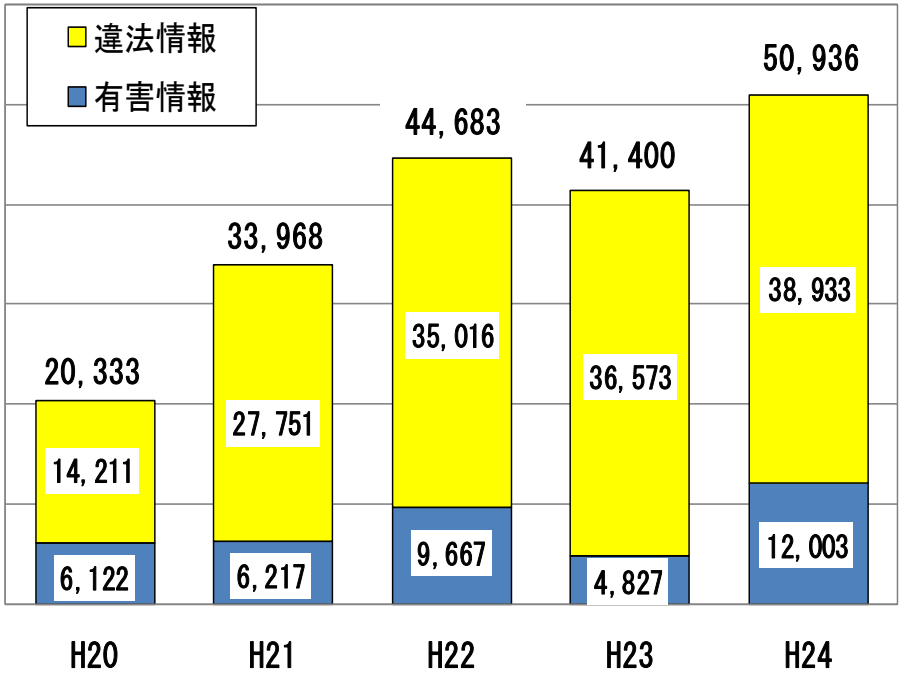
平成24年中の違法・有害情報の現状

○　警察庁では、平成18年6月より、IHCにインターネット上の違法・有害情報の通報等を業務委託。

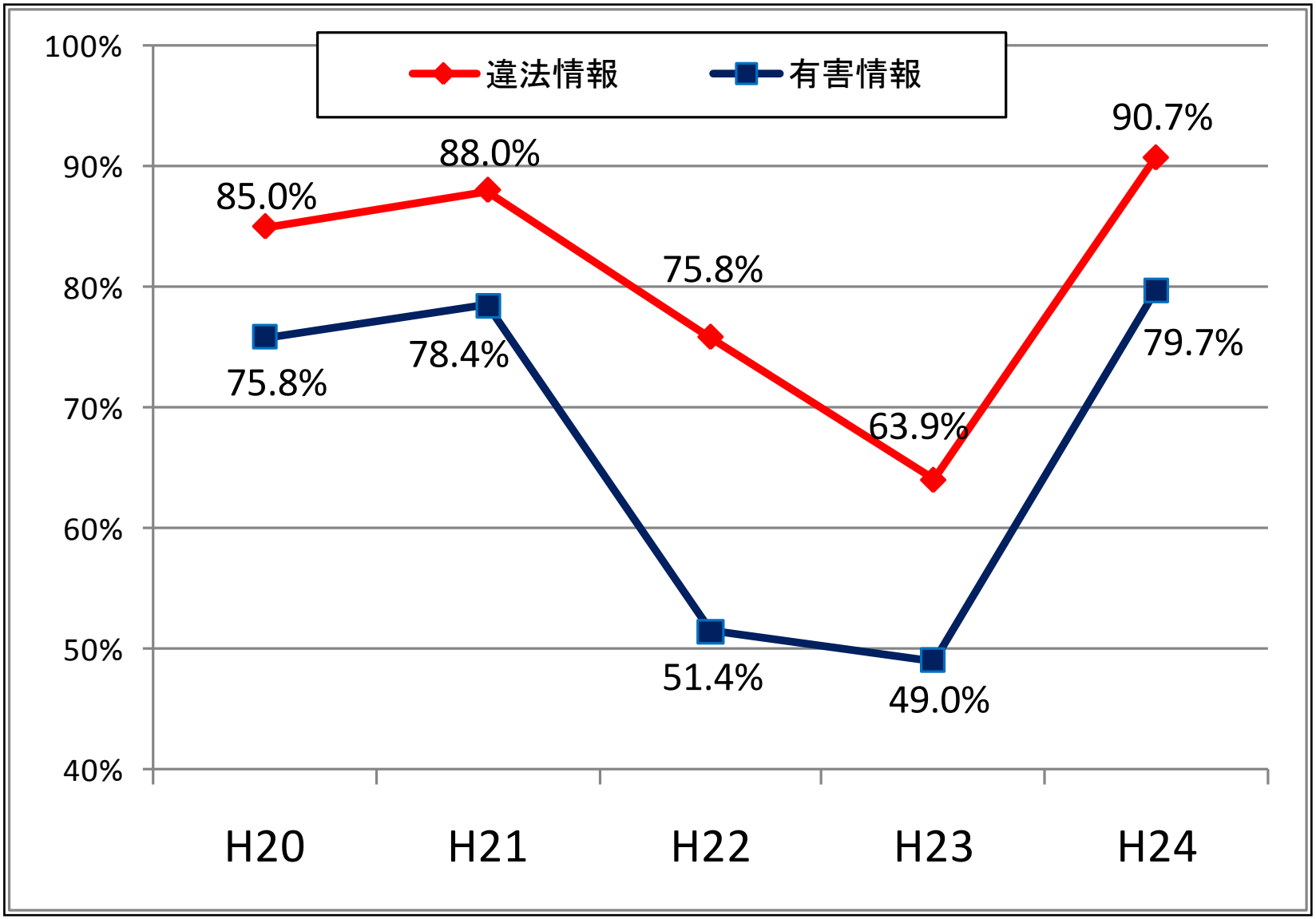
過去5年の通報受理件数の推移



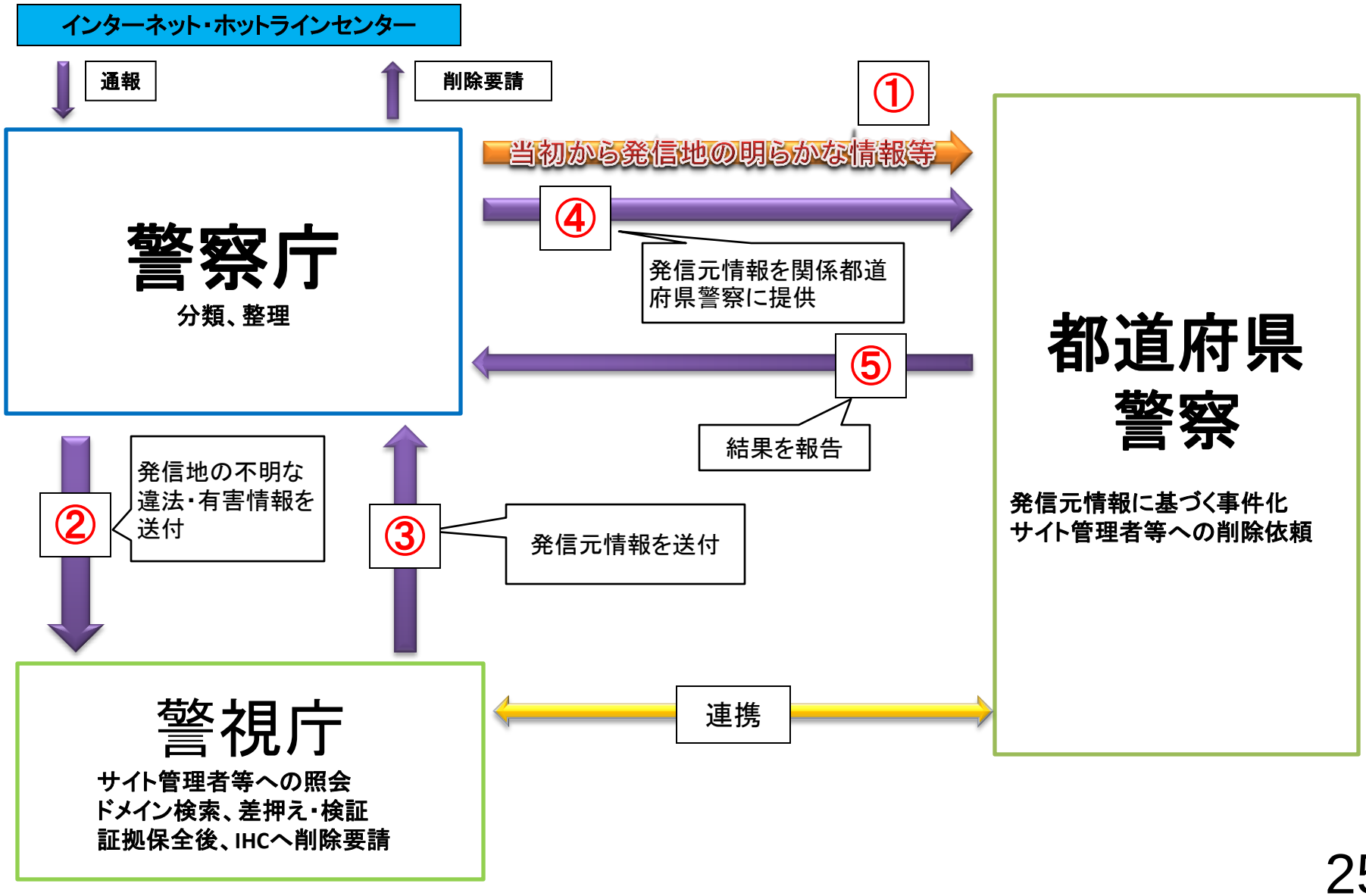
過去5年の違法・有害情報該当件数の推移



IHCによる違法・有害情報の削除依頼状況



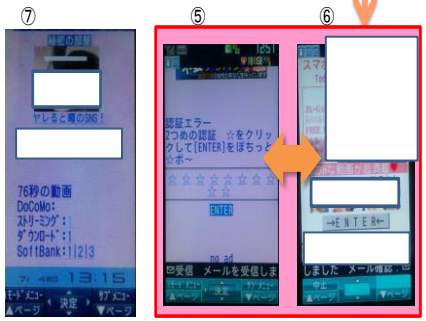
全国協働捜査方式


インターネット・ホットラインセンター
通報
削除要請
①
当初から発信地の明らかな情報等
警察庁
分類、整理
④
発信元情報を関係都道府県警察に提供
⑤
結果を報告
都道府県警察
発信元情報に基づく事件化
サイト管理者等への削除依頼
②
発信地の不明な違法・有害情報を送付
③
発信元情報を送付
警視庁
サイト管理者等への照会
ドメイン検索、差押え・検証
証拠保全後、IHCへ削除要請
連携

サイバーパトロール業務の外部委託

【複雑な認証が必要な例】

18回ミスなしでクリックすることでようやく「認証」の先に進める



通報された⑦の記事を見るためには、②の指示に従ってリンゴマークと18禁動画を順にクリックして、リンク先の③の中から対象項目を探し出してクリックするという作業を(このケースの場合)合計18回行う必要がある。

途中で1回でもクリックミスすると②の始めからやり直しとなる。

また、途中でミスをしていたとしても、最後の④の「認証」を押すまでそれが分からない。たとえ一度も認証に失敗しなかったとしても約30分かかる。

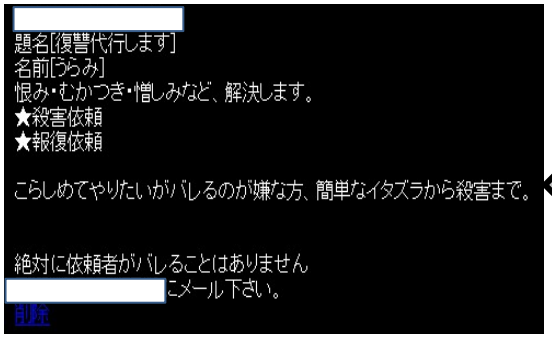
次に⑤の「☆」を左から順にクリックして、リンク先のサイト⑥を表示させ、また⑤に戻って次の☆をクリックしてリンク先サイトを表示するという作業を☆の数だけ行うことで、動画再生ページにたどり着く。

【業務体制】
専従１０名体制
（内訳）
管　理　者　　１名
オペレータ　　８名
連絡・統計　　１名

出会い系サイト
利用の児童

インターネット・
ホットラインセンター

【闇サイトの例】



○委託業務の内容
１　対象とする情報
　○出会い系サイト内の禁止誘引行為
　○登録制サイト内の児童ポルノ情報
　○悪質かつ緊急に対処すべき情報　　等
２　ホットラインセンターへの通報
３　出会い系サイト利用の児童に対する警告メールの送信

一般からの通報が
期待できない
情報を対象

官民連携の推進

関係事業者等との連携による被害防止対策の推進

金融機関との連携

- ○ 各都道府県警察と金融機関との連携による不正送金事案の被害拡大防止
- ○ 被害の発生状況や犯行手口等に係る情報共有
- ○ 迅速な被害の届出の要請

セキュリティ事業者との連携

- ○ アンチウイルスベンダー等を始めとするセキュリティ関連事業者との連携強化によるサイバー犯罪による被害の防止
- ○ ウイルス対策ソフトで検知できない不正プログラムに係る情報の提供

プロバイダ連絡協議会

- ○ 各都道府県警察におけるプロバイダや消費者団体等との連携の枠組みの構築
- ○ サイバー犯罪の情勢や手口、サイバー犯罪被害防止等に関する情報交換

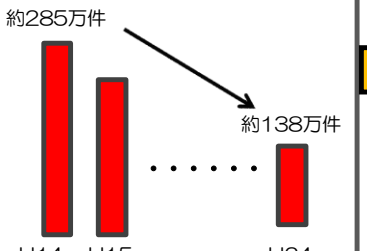
インターネットカフェ連絡協議会

- ○ 各都道府県警察におけるインターネットカフェ提供事業者との連携の枠組みの構築
- ○ 本人確認の徹底等による匿名性の排除の要請

サイバー防犯ボランティアの育成・支援の推進

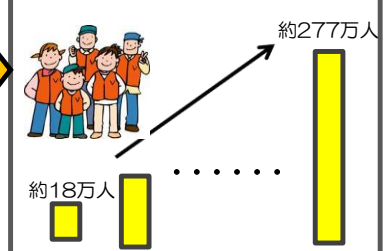
刑法犯認知件数の推移

10年連続で減少



背景

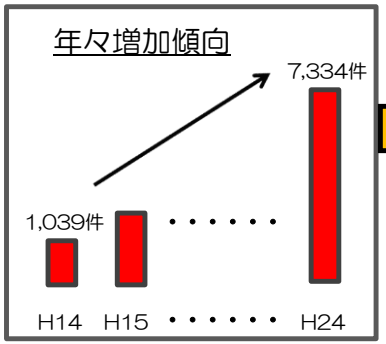
防犯ボランティア急増



防犯ボランティアによる
自主的な防犯活動の促進

サイバー犯罪の検挙推移

年々増加傾向



背景

サイバー空間における
防犯ボランティア

育成低調

サイバー防犯ボランティアの育成の必要性

～平成22年度総合セキュリティ対策会議報告書～

○問題の所在

サイバー空間が有する匿名性等の理由から、

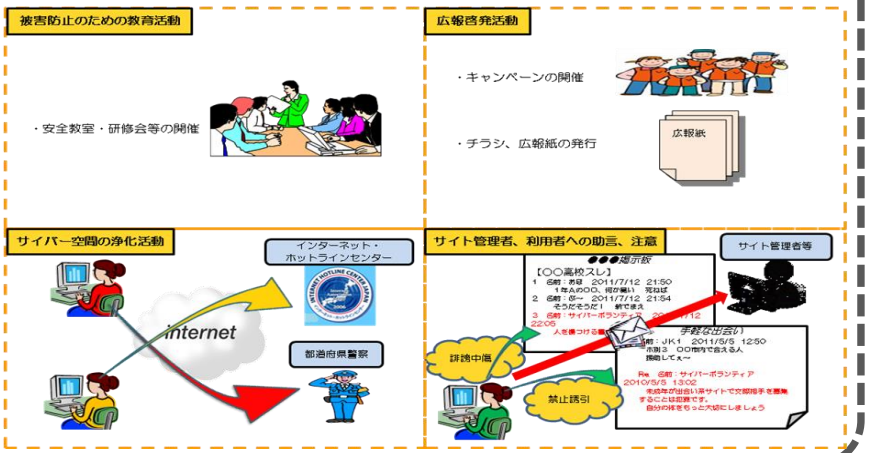
○違法・有害情報の氾濫

○無責任な中傷等の書き込みを安易に敢行

その背景には、

○サイバー空間における規範意識の低下

○サイバー防犯ボランティアに期待される役割



育成・支援上の課題

○地域住民に係る防犯ボランティア活動への意識調査※では、
- 参加意欲→ぜひ参加、機会があれば参加 63.0%
  （会社員等 64.1%　自営業等 70.0%　主婦 62.8%）
- どうすれば参加しやすいか→活動の具体的ノウハウ 53.4%

○防犯ボランティア団体の代表者へのアンケート※では、
- 継続・発展への課題→活動のマンネリ化 35.5%
- マンネリ化等への必要な支援→新たな活動ノウハウ 34.9%

※「地域安全安心ステーション」推進事業に関する意識調査2010

実施した施策と今後の推進内容

○サイバー防犯ボランティア育成・支援の在り方に関する調査研究（平成24年度）

サイバー防犯ボランティア活動の試行実施を通じて、実践的な調査研究を進め、課題や改善点、活動上の具体的留意事項、関係機関・団体との連携・支援が望まれる事項等を抽出・整理

→「活動マニュアル」、「育成カリキュラム」の作成

・個別の活動に応じた具体的な活動要領　・活動上の安全・安心を確保するための方策

○サイバー防犯ボランティアの育成・支援（平成25年度以降）

- 新たなボランティア活動層へのアプローチ
- 既存の防犯ボランティア団体の活動領域の拡大

関係事業者等との連携による被害防止対策の推進

情報セキュリティ月間等における広報啓発活動

○　2月と10月の情報セキュリティ月間における広報啓発活動を実施

研修会等における情報セキュリティアドバイザーによる講演

○　非行防止教室や情報セキュリティ講座等における講演の実施

広報啓発用パンフレット等の配布

○　出会い系サイトやスマートフォンに起因した被害の防止対策のためのリーフレット等を配布

警察庁ウェブサイトの活用

○　警察庁サイバー犯罪対策ウェブサイトを活用した情報提供

警察庁サイバー犯罪対策ウェブサイト

http://www.npa.go.jp/cyber/

不正アクセス防止対策に関する官民意見集約委員会

概要

平成22年度総合セキュリティ対策会議での提言を受け、社会全体として不正アクセス防止対策を推進するに当たり、現状の課題と改善方策に係る官民の幅広い意見を集約するため、平成23年6月、官民意見集約委員会（官民ボード）が設置された。

構成員

（構成員）　サーバ・コンピュータ製造事業者、OSソフト製造事業者、ウイルス対策ソフト開発事業者、コンピュータ・セキュリティ監査事業者、コンピュータ・セキュリティ関連団体、通信事業者関連団体、研究所等から27人
（事務局）　警察庁、総務省及び経済産業省
（オブザーバ）　内閣官房情報セキュリティセンター

ワーキング・グループの設置

- ○ 不正アクセス防止対策に関する行動計画
- ○ 不正アクセス行為の実態解明に資する方策
- ○ 不正アクセス行為からの防御に関する知識の普及等の方策
- ○ 既存の対策では対応が困難な手口等について、不正アクセス行為に至る前の段階での対応を可能とする方策

平成23年中の成果

平成23年12月、「不正アクセス防止対策に関する行動計画」を策定

官民連携した広報啓発活動の推進

平成25年度総合セキュリティ対策会議

概要

総合セキュリティ対策会議は、情報通信ネットワークの安全性・信頼性を確保するためには、産業界等との連携が不可欠であることから、情報セキュリティに関する産業界等と政府機関との連携の在り方、特に警察との連携の在り方について検討を行うため、平成13年度に設置された生活安全局長主催の私的懇談会。

経緯

- サイバー空間の脅威に対処する産学官の情報共有と協力の促進の枠組みである米国のNCFTAは、法執行機関への情報提供等により犯罪捜査への貢献に実績。
- 「サイバーセキュリティ戦略」（平成25年6月10日第35回情報セキュリティ政策会議決定）等において「日本版NCFTAの創設」について提言。

本年度テーマ

サイバー空間の脅威に対処するための産学官連携の在り方
～日本版NCFTAの創設に向けて～

検討項目

- **サイバー空間の脅威に関する産学官の保有する情報の集約・分析の在り方**
  → 金融機関を標的とした不正プログラムやボットネット等の情報の収集・分析体制等
- **サイバー空間の脅威に関する産学官の連携による研究開発の在り方**
  → サイバー犯罪捜査やサイバー攻撃対処に資する技術・ツール等の研究・開発
- **捜査機関等の職員に対するトレーニングの提供の在り方**
  → 警察・政府機関・アジア地域のサイバー犯罪捜査官等に対するトレーニング
- **海外の関係機関等との連携の在り方**
  → 米加NCFTAやユーロポールのEC3との連携やIGCIに対する支援等による国際的なサイバー犯罪捜査のオペレーションへの参加・協力

米国NCFTAについて
（National Cyber-Forensics & Training Alliance）

NCFTA

民間企業

法執行機関

学術団体

情報共有
（データベース）

情報の集約・分析

- ○ 金融、マルウェア等に関する被害情報の集約
- ○ 被疑者関連情報の抽出
- ○ 法執行機関・民間企業への情報提供

トレーニングの提供

- ○ ボットネット等の捜査実習（被疑者の特定等）
- ○ 効果的な捜査手法に関する議論
- ○ 最新の脅威に関する講義

サイバー犯罪の脅威の深化

法執行機関・民間企業・学術団体の連携による効果的対応の必要性

NCFTAの設立

設立

1997年設立
（米国ピッツバーグ）

組織

法執行機関・民間企業・学術団体を構成員とする非営利団体

目的

産学官における情報共有と協力の促進によるサイバー空間の脅威の効率的な特定及び軽減

機能

- ・ サイバー犯罪に係る情報の集約と分析
- ・ トレーニングの提供
  （諸外国の捜査機関の捜査員が参加）　等

サイバー空間の脅威への対処に向け

警察活動に御協力をお願いします。

ご清聴ありがとうございました。