資　料　編

コンピュータウイルスの現状及びその対策と今後の予測について

村上　智(Satoshi Murakami)
株式会社シマンテック　セールスエンジニアリング本部

2013年セキュリティ　5大予測

ソーシャルネットワークの収益化に伴う脅威

・SNSが利益を追求する一環としてメンバー間でギフトを購入してプレゼントできる機能の提供を開始する中、SNSを通じてユーザーの決済情報を盗んだり、ユーザーをだまして決済情報や個人情報を入力させたりする攻撃が増加する。

サイバー上の対立図式が一般化

・国家間、組織間、個人間のサイバースパイ、サイバー攻撃、示威行為などがさらに横行する。

※2012/10 Symantec Blogより出展

ランサムウェアが新たな脅威に

・一時猛威を振るった偽ウイルス対策ウェアは影を潜め、ユーザーの情報を人質にして金銭を脅し取るランサムウェアが浮上。Symantecのランサムウェアに関する報告書によれば、現時点で被害額は少なく見積もっても年間500万ドルを超えており、今後さらに増えることが予想される。

モバイルを狙ったアドウェアの横行

・携帯端末から情報を抜き取ったり、迷惑な広告を表示させたりするモバイルアドウェア「マッドウェア」は過去9カ月で210%の激増となり、今後も増え続ける見通し。無料アプリを利用したマッドウェアはさらに攻撃的になり、悪質性が強まる恐れもある。

モバイルとクラウドへの移行は攻撃者も同様

・モバイルプラットフォームとクラウドサービスが標的として狙われるようになる。それを裏付ける現実として、Androidを狙うマルウェアは2012年に急増した。管理されていないモバイル端末で会社のネットワークにアクセスしたり、そこから取得したデータがクラウドに保存されたりする中で、情報流出や標的型攻撃の危険性が高まる。

新たな脅威：ランサムウェア

ランサムウェア ロック画面の例

ランサムウェアとは

何らかの方法でコンピュータの機能を無効にし、正常状態への復元の引き換えに金銭を不正に要求する悪質なソフトウェア

当初は単純に画面をロック、コンピュータへのアクセス復元のために金銭と要求するだけの単純なものが多かった

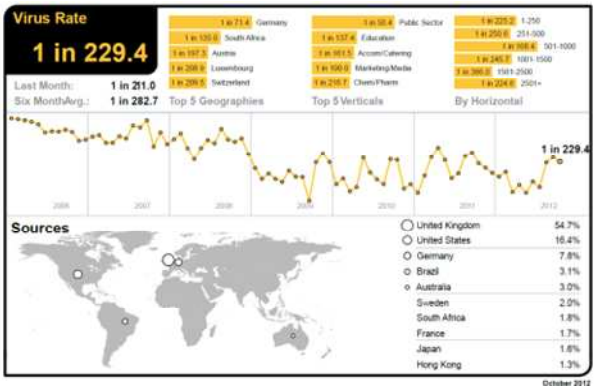
2009年の登場以降、進化／巧妙化

- 世界的な広がり
  - ⇒ ユーザーの国に合わせてローカライズ
- 法執行機関を称するものの増加
  - ⇒ 左の例はFBI
- 背後の犯罪者の強力な金銭的動機
  - ⇒ より創造的になっている

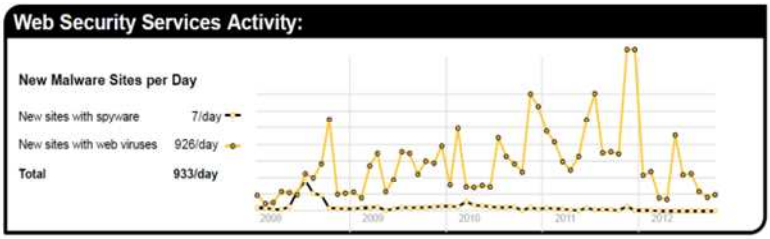
悪質な攻撃 – マルウェア メール及びWebによる脅威

全体的に減少傾向にあるものの、引き続き、主流な経路になっている

※シマンテックが調査 2012/10 1カ月分の調査から要約



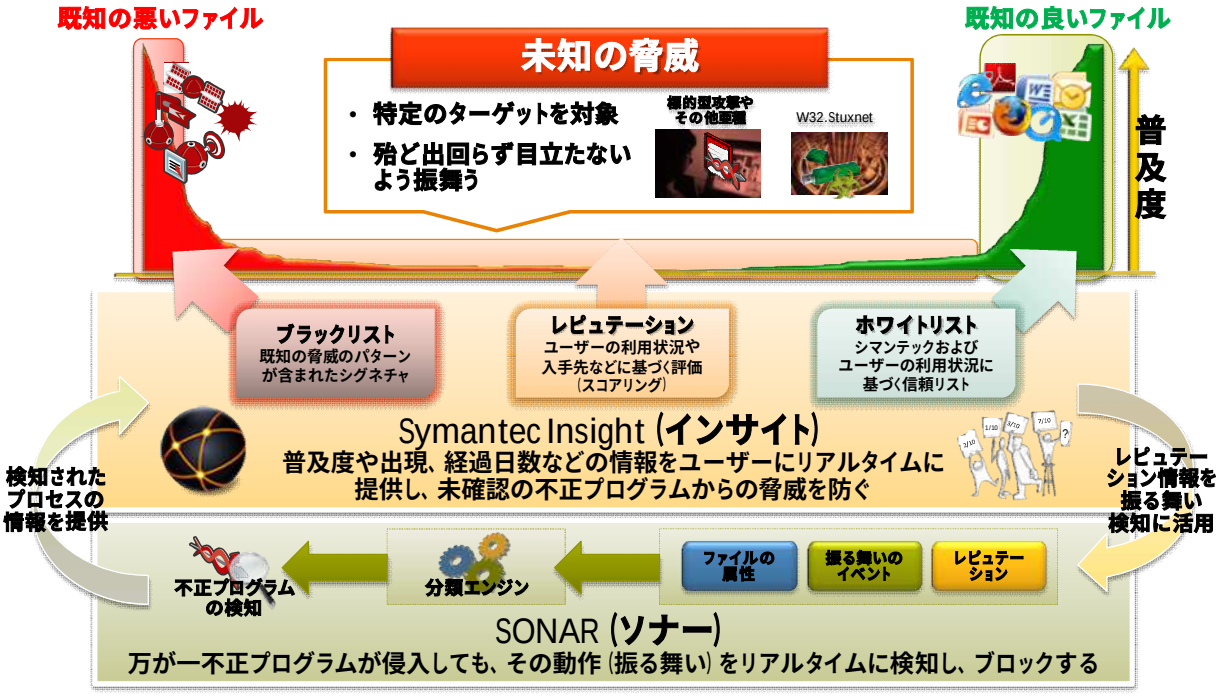
- 229.4通に1通がメール感染型ウィルス（日本は約1300通に1通）
- 悪質なWebサイトへのリンクが張られたメール感染型マルウェア全体の23.5%



- マルウェアサイト1日に933件を特定

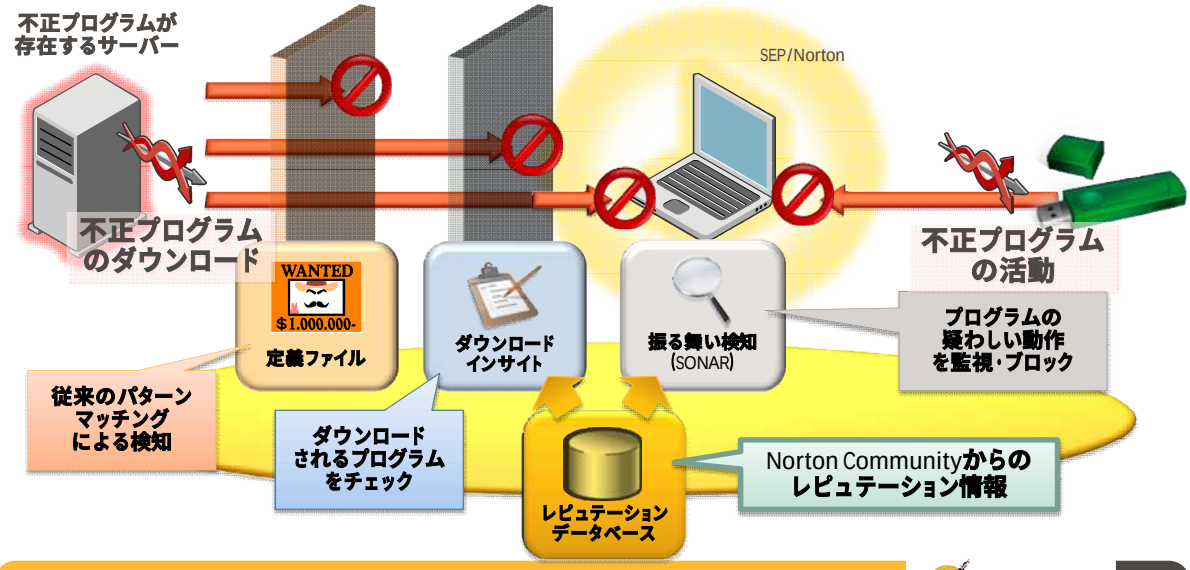
出典元:http://www.symantec.com/connect/blogs/2012-10

定義ファイルの限界：未知の脅威に対する振る舞い検知とレピュテーション



レピュテーション技術による未知の脅威からの保護

- レピュテーション情報を活用することで、定義ファイルでは検知できない、新しい不正プログラムにも迅速に対応



基本行動の大切さ： 継続した普及活動

疑わしいリンクや添付ファイル、Web サイト上の不審なリンクはクリックしない！！

OSやインストールされている各ソフトウェアについては常に最新の状態であることを保つ

不明なソースからソフトウェアをダウンロードする際には十分注意する

⇒ 振る舞い検知、レピュテーション技術等の積極活用を促進

マルウェア感染等を防ぐ確実な一歩

Symantec.

Thank you!

世界の国々の防衛状況を評価

- **世界初の「サイバー防衛報告書」を発表**
- 本年1月、McAfee社とベルギーのシンクタンクSDA (Security & Defence Agenda) は、サイバー防衛に関する世界の専門家の意識調査結果
- 27か国の主要な政策立案者と政府、企業、学界におけるサイバーセキュリティの専門家約80人に綿密なインタビュー調査を実施するとともに、35か国の世界的なリーダー250人に匿名で調査を行う
- この評価は、Robert Lentz 元米国防次官補代理 (サイバー情報保障担当) のモデルを採用。攻撃からの耐性を 5 段階で表し、サイバー防衛の取り組みの現状とサイバー攻撃の阻止能力を評価

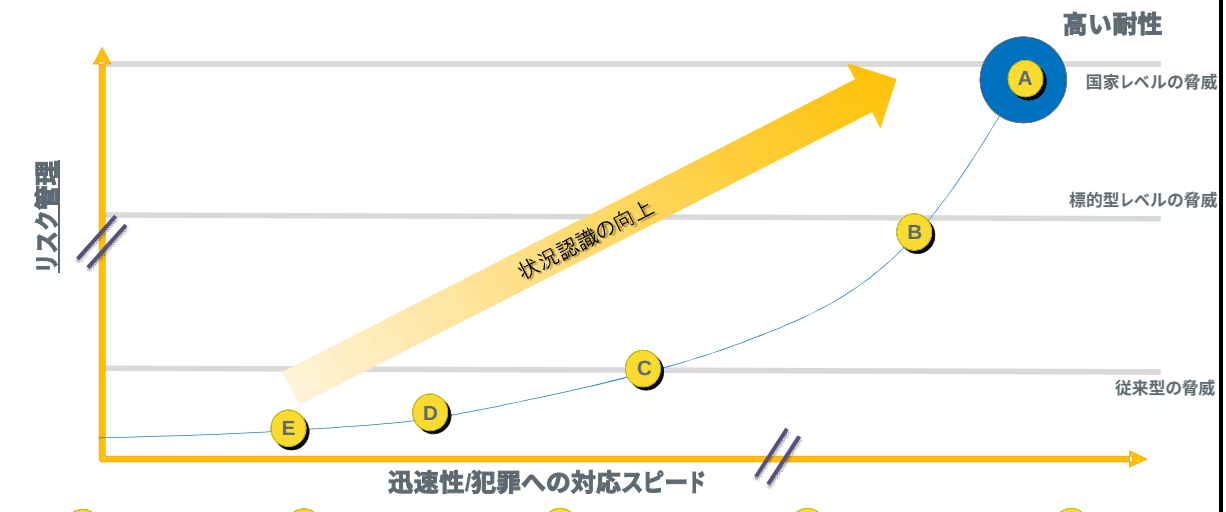
2

サイバー上の難題 (抜粋)

- 「サイバー犯罪は儲かるだけでなく、リスクが低く、匿名で実行することが可能です。核の脅威やそれ以前の脅威と異なり、サイバー上の脅威は知らないうちに襲ってきます」
- 「サイバー犯罪者は動きが迅速で、資金も豊富にある。情報共有に対する法的な制限もなく、非常に組織的な攻撃を実行することも可能だ」
- 「サイバー攻撃では、攻撃対象はほぼ無制限です。核の時代に入ってから軍縮が推進されるまで20 年から30 年ほどかかりましたが、サイバー空間において国際的な法体系が整備されるまでに同程度の時間が必要になるでしょう。」
- 「我々は未知の領域に足を踏み入れている。サイバー環境の変化は非常に激しい。コンテンツだけでなく、次々と新たな使い方が出てくる。ビジネス モデルも多岐にわたる。実際に何が起きていて、我々が何をすべきか誰も把握していない」

3

リスク/迅速性成熟度モデル



E 事後対応
- 手作業での対応が多い
- 最低限のツール (アンチ・ウイルス)
- 事故が発生した後に対応と対策

D ツールベース
- 断片的にツールが導入
- 外部コンプライアンスの適合を目指すシステム

C 統合ピクチャ
- ツールが面として導入されシステムとして統合され防御 (初期)
- 状況認識の向上
- 各種ログによる相関分析を実施

B 動的な防御
- 高い予測機能
- リアルタイムでリスク分析を実施
- 攻撃を検知し防御可能な迅速な対応が可能なシステム

A 高い耐性
- 高い予測機能
- 各種攻撃を受けている場合でも、通常のシステム運用が可能
- サプライチェーンと重要インフラの保護

4

状況認識の向上とは？

McAfee An Intel Company

送信元情報

敵の規模

攻撃の意図

攻撃の種類

既に侵入？　　不審な動き？

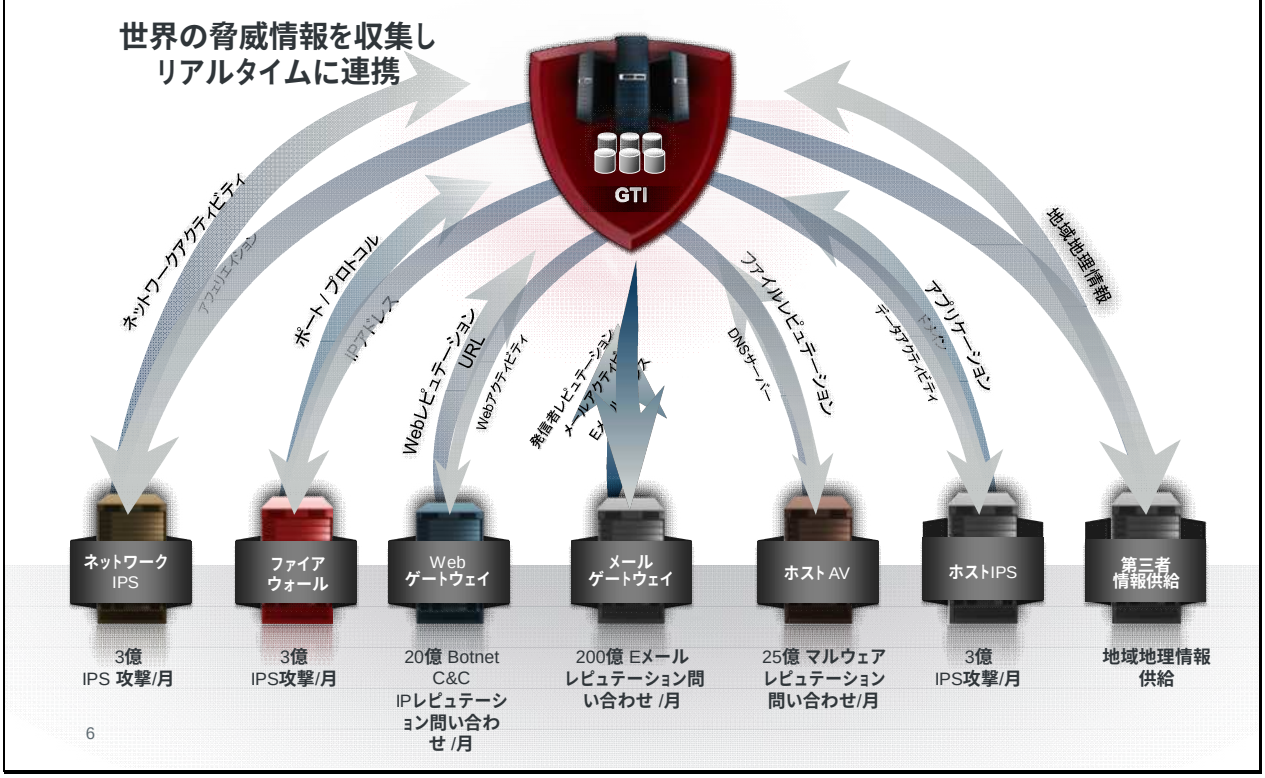
弱点･脆弱な部分は？

迅速な対処措置？

5

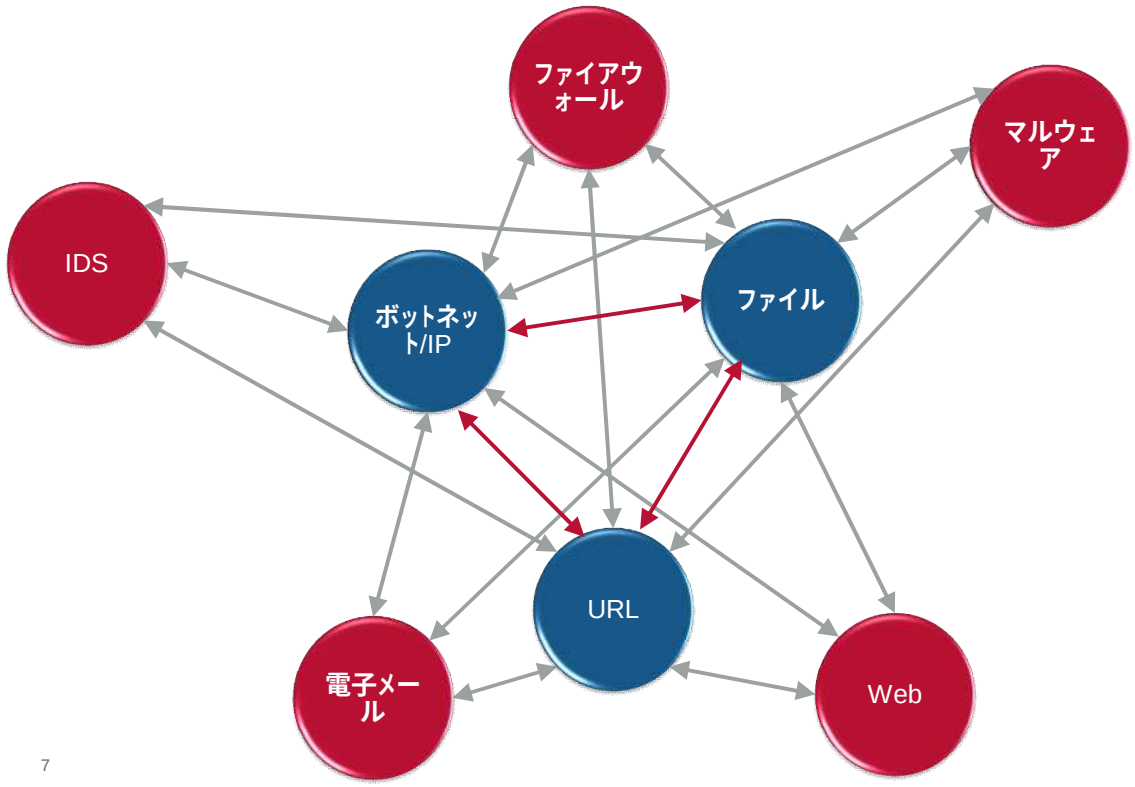
McAfee Global Threat Intelligence

McAfee An Intel Company



6

情報の相関分析

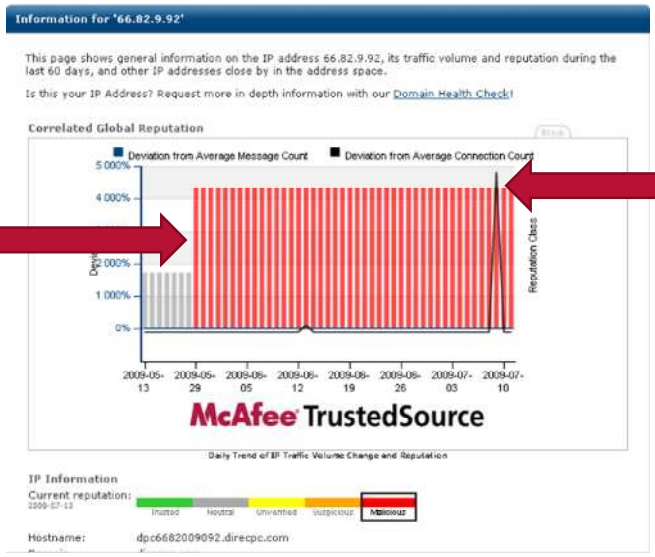


7

脅威の相関分析の例：「点と線を結ぶ」

- 2009年7月4日：韓国の200,000ゾンビーボットネットが、米国および韓国政府のサイトに対してDDoS攻撃を開始
- GTI脅威情報が攻撃トラフィックの80%以上を検知しブロック

5月29日　グローバルな複数脅威の関連付けにより、不正なレピュテーションの可能性を察知



7月4日のDDoS

8

McAfee Strategy to Fight Cybercrime

1. Legal Frameworks & Law Enforcement
2. Education & Awareness
3. Technology & Innovation

McAfee Initiative to Fight Cybercrime
http://www.mcafee.com/us/campaigns/fight_cybercrime/index.html

9

ご清聴大変有難う御座いました。

Tor（The onion router）の悪用事例等

平成２３年度総合セキュリティ対策会議検討結果

- **インターネット上の高度匿名化技術（Ｔｏｒ）**
  将来的な悪用に備えた調査研究のため、次の取組が必要
  - 国内外における高度匿名化技術の利用状況等の実態把握
  - 国際会議等を通じて各国の捜査機関等と連携し、将来的な対策を検討

日本における悪用の事例

- **インターネット掲示板を利用した脅迫事案**
  （平成２４年、検挙）
  - 被疑者は、Ｔｏｒを悪用してインターネット掲示板に殺害予告等の書き込みを多数行ったが、各種捜査の結果、書き込まれていた者とトラブルになっていた被疑者が浮上し、検挙に至ったもの
- **インターネットバンキングに対する不正アクセス事案**
  （平成２２年、未検挙）
  - 被疑者は、Ｔｏｒを悪用してインターネットバンキングに不正アクセスしたもの
- **出会い系サイトの掲示板を利用した禁止誘因行為事案**
  （平成２２年、未検挙）
  - 被疑者は、Ｔｏｒを悪用して出会い系サイトの掲示板に、児童を異性交際の相手方となるように誘引する書き込みを行ったもの

海外における悪用の事例

- **Ｔｏｒが犯罪に用いられた事案は多数発生**
  - Ｔｏｒはサイバー犯罪者の間で、匿名性を確保するための基本的なツールとなっている。

警察による情報セキュリティ等に関する広報啓発の現状

情報セキュリティ等に関する広報啓発の基本方針

サイバー空間の脅威に対する総合対策推進要綱（平成23年10月制定）

- 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の促進のため、警察庁において制定。
- 広報啓発については、「社会全体でサイバー空間の脅威に立ち向かう気運を醸成する」との基本方針を掲げ、具体的には以下の事項等を推進することが定められている。

- サイバー空間の脅威の実態を踏まえ、**一般のインターネット利用者、一般企業、IT関連企業等の対象の違いに応じた広報啓発活動**の推進
- 児童の犯罪被害を防止するため、**児童、保護者、携帯電話事業者等に対し、フィルタリングの導入等による携帯電話及びインターネットの適切な利用についての周知徹底**
- 同種手口による**被害拡大を防ぐための事件広報**

不正アクセス防止対策に関する行動計画（平成23年12月策定）

- 官民が一体となった不正アクセス行為に関する実態情報の共有等のため、官民意見集約委員会（※）が策定。
- 広報啓発については、「斉一的な普及啓発活動のための基盤整備」、「タイムリーな情報提供の推進」等を掲げ、具体的には以下の事項等を推進することが定められている。

- **ポータルサイトの充実**
  - ・利用者が必要としている情報を保有しているポータルサイトに簡単に到達できるサイト構築
  - ・IPAを中心に、政府機関を初めとした既存のポータルサイトを統括するサイト構築
- **生徒・学生・保護者・教育機関を対象とした普及啓発**
  - ・情報セキュリティ講習の推進、情報通信技術関連イベント等の活用等
- **一般利用者（高齢者等を含む。）を対象とした普及啓発**
  - ・インターネットを利用する際に、最低限必要となる対策の定義（OSのアップデート等）
  - ・最低限必要となる対策方法についての標語の作成・周知
- **官公庁・地方公共団体を対象とした普及啓発**
  - ・政府機関に対する脆弱性情報等に関する注意喚起の発出等
- **不正アクセス行為の被害に遭った場合の対応方法等の周知活動**
  - ・不正アクセス行為に関する相談・届け出のホームページにおける必要な情報の掲載等
  - ・情報セキュリティに関する講習等の場を通じた各相談・届け出窓口等の周知等
- **最新の技術動向を踏まえた的確な情報提供**
  - ・新しい技術等の利用における情報セキュリティ対策の必要性の啓発
  - ・各種端末、サービスを利用する幅広いユーザに対する各種リスク等の啓発

※官民意見集約委員会・・ 平成22年度総合セキュリティ対策会議の提言を受け、警察庁、総務省及び経済産業省が、社会全体としての不正アクセス防止対策の推進に当たって必要となる施策に関して、現状の課題や改善方策について意見を集約するため、平成23年に設置したもの。

具体的な取組内容

警察では、前記の方針等に沿って、下記の取組等を実施している。

各種講習等を通じた広報啓発

生徒・学生・保護者・教育機関に対する講習等

・入学説明会等の機会を利用し、フィルタリングの導入やID・パスワードの管理の重要性等インターネットを利用する上で遵守すべき事項等に関する広報啓発を行っている。

一般利用者に対する講習等

・フィッシング等に関する注意喚起、OSのアップデートの適切な実施等インターネットを利用する際に最低限必要となる対策方法に関する広報啓発を行っている。
・高齢者に対しては、振り込め詐欺に関する防犯活動の場や、地域の会合等も活用している。

企業・官公庁に対する講習等

・標的型メール等、サイバー攻撃の現状等に関する広報啓発を行っている。

【講習会の例】

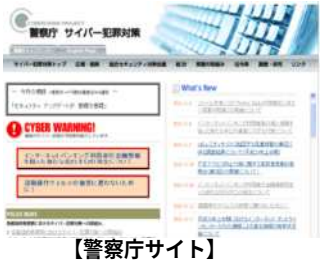
【参考：平成23年中の情報セキュリティに関する講習の実施状況】
学　生：7,691回、1,800,378人に対して実施
一般人：3,971回、　344,531人に対して実施
企業等：　974回、　29,941人に対して実施

ウェブサイトにおける広報啓発

警察庁ウェブサイトにおいて、事件広報、新たな手口に関する注意喚起、被害に遭った際の対応要領の紹介、都道府県警察の窓口案内、各種資料の掲載、標語の紹介等を行っている。

都道府県警察においても、サイバー犯罪に関するウェブサイトを開設し、広報啓発に努めている。

IPAが管理する情報セキュリティ・ポータルサイトに対して、コンテンツの提供を行っている。



【警察庁サイト】

【IPA管理サイト】

【資料の例】

一連の犯行予告事案等を受けた取組内容

インターネット掲示板等への犯行予告事案を受けた取組内容

警察庁ウェブサイトにおける広報啓発

・「遠隔操作ウイルスの被害に遭わないために！」と題した資料を掲載し、ウイルス対策ソフトの導入や、信頼のおけないプログラムをダウンロードしないこと等につき、広報啓発を行った。

※ IPAが管理する情報セキュリティ・ポータルサイトにも上記資料の内容等が掲載されるよう措置した。

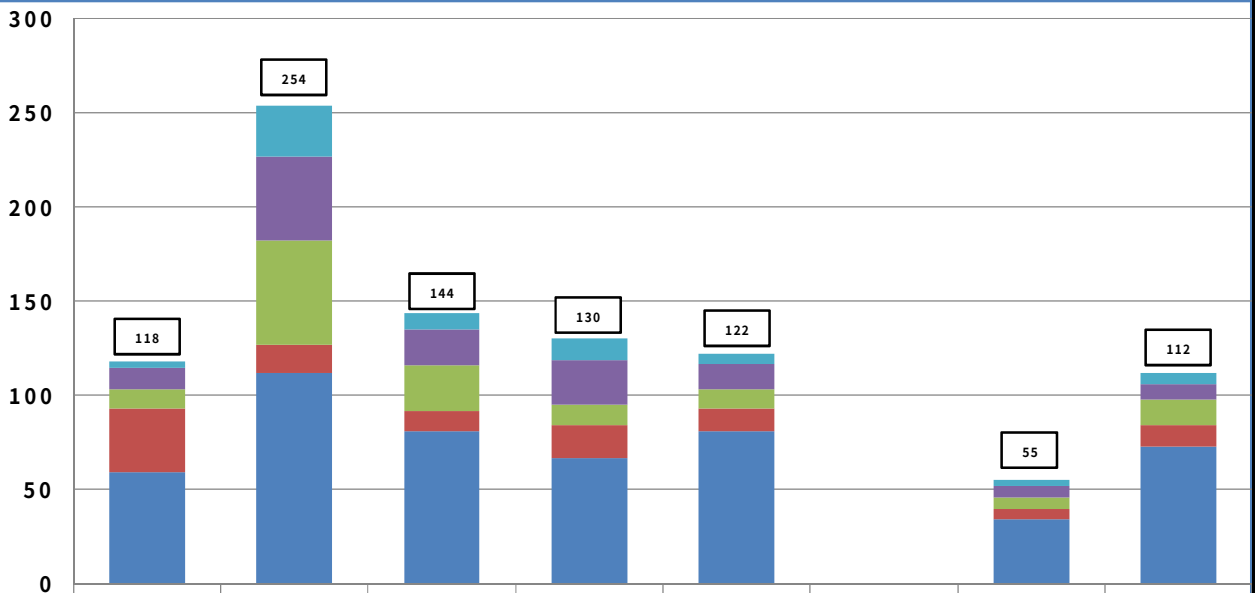
インターネットバンキング利用者等の個人情報を狙った新たな手口の事案を受けた取組内容

講ずべき対策等に関する広報啓発

・事案を認知後、警察庁において「不正にポップアップ画面が表示される」など手口の概要等に関する広報啓発を実施した。
・その後、利用者の方のパソコンから、不正な入力画面を表示する動作をすると見られるウイルスが検知されたことを受け、必要なプログラムをダウンロードしないこと等講ずべき対策等に関する広報啓発を実施した。

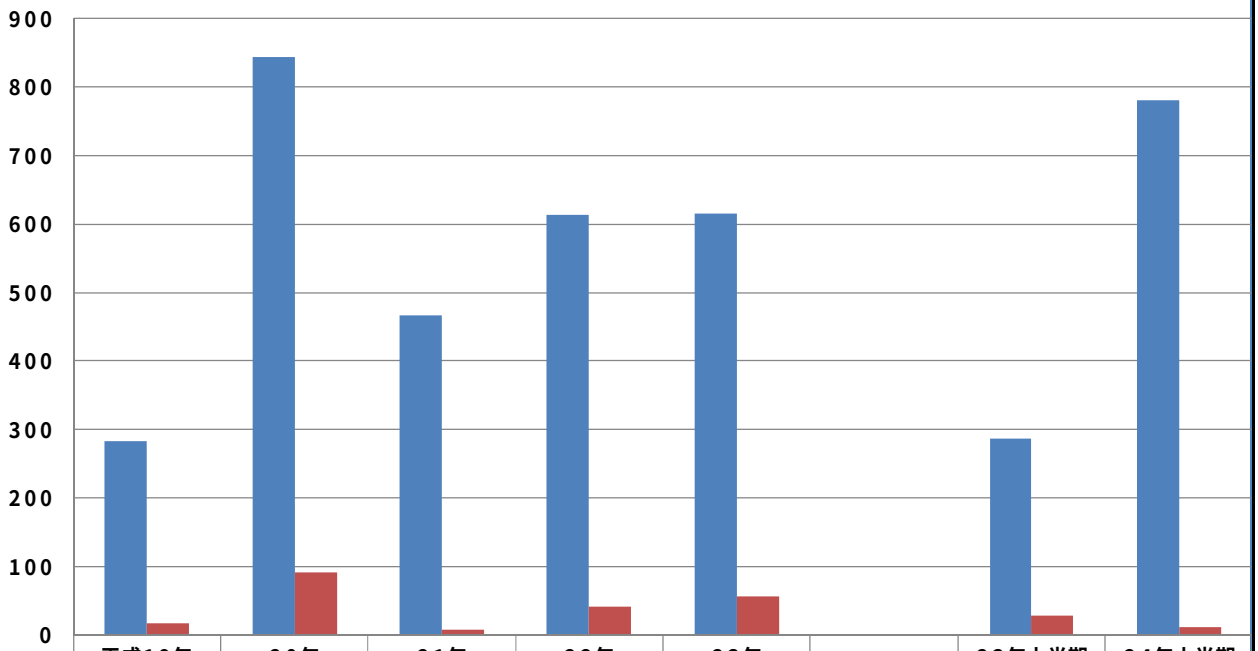
※上記内容については、警察庁ウェブサイトにも掲載して広く広報啓発に努めた。

インターネットを利用した殺害予告等の検挙状況



	平成19年	20年	21年	22年	23年		23年上半期	24年上半期
軽犯罪法違反	3	27	9	11	5		3	6
偽計業務妨害 信用毀損	12	45	19	24	14		6	8
威力業務妨害	10	55	24	11	10		6	14
恐喝	34	15	11	17	12		6	11
脅迫	59	112	81	67	81		34	73

インターネットを利用した殺害予告等のインターネットホットラインセンターへの通報状況等



	平成19年	20年	21年	22年	23年		23年上半期	24年上半期
殺害予告等	283	844	466	614	615		287	780
うち警察への情報提供	17	92	8	41	56		29	11

注：平成19年の警察への情報提供件数には自殺予告が含まれる。

インターネットを利用した犯行予告・ウイルス供用事件に係る誤認逮捕事案の検証結果等について

主な反省教訓事項

- 遠隔操作等の可能性に対する認識不足
- 部門間の連携不足
- 逮捕判断時における検討不足
- 供述に対する吟味不足等

全国警察に以下の徹底を指示

サイバー犯罪に対する意識改革

- サイバー犯罪捜査に係る知識の底上げ
- 部門間の連携強化
- 官民の連携推進

捜査指揮の徹底

- 証拠の総合的な評価
- 供述内容の多角的な吟味
- 取調べ指揮

サイバー犯罪捜査上の具体的留意事項等

- 証拠の解析・分析の徹底
- ログの迅速な確保
- 捜査力・解析力の向上

警察と民間事業者等におけるウイルスに係る情報の共有について

趣旨

警察と民間事業者等との間で、既存の枠組みを活用しつつ、ウイルスに係る情報の共有を行うことにより、当該ウイルスによる被害の拡大防止を図るもの

ウイルスを民間事業者等に提供した最近の実績

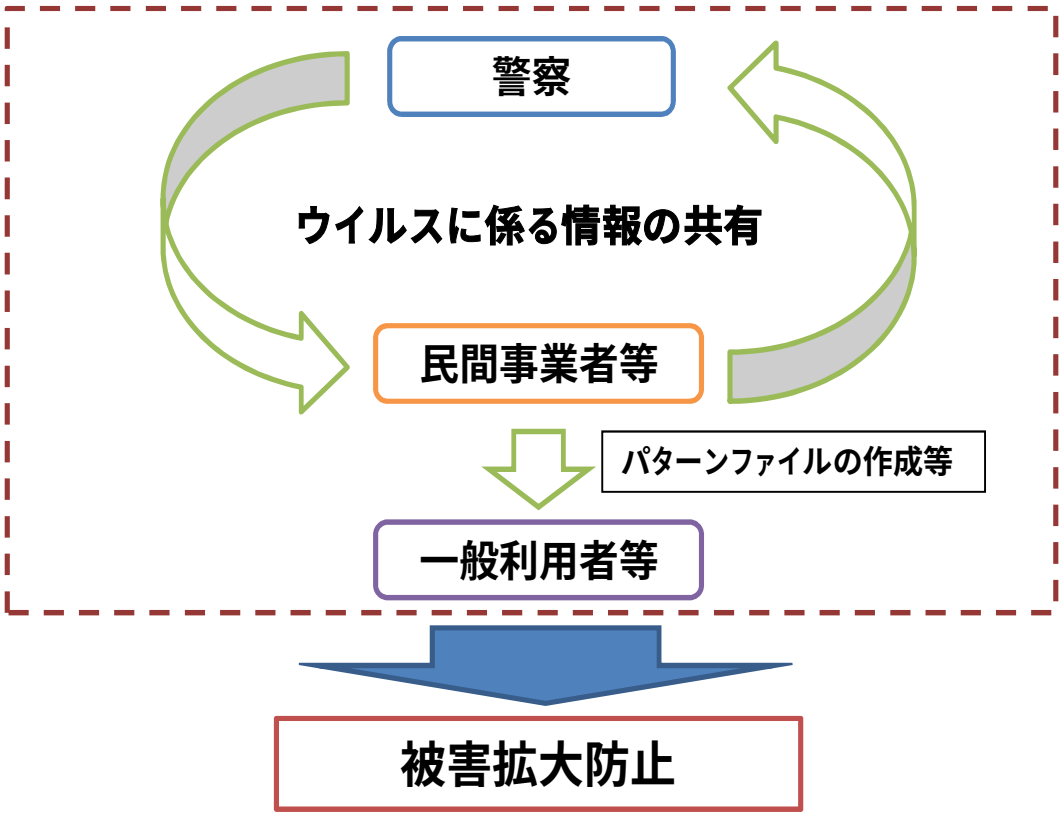
インターネットを利用した犯行予告･ウイルス供用事件

第三者からの遠隔操作を可能とする新種のウイルスを、既存の枠組みを通じて民間事業者等に提供し、民間事業者等においてパターンファイルの作成等を実施し、被害拡大の防止を図った。

インターネットバンキング利用者等の個人情報を狙った新たな手口による事案

利用者が金融機関の正規のインターネットバンキングのページからログインすると不正なポップアップ画面を表示させるウイルスを、既存の枠組みを通じて民間事業者等に提供し、民間事業者等においてパターンファイルの作成等を実施し、被害拡大の防止を図った。

ウイルスに係る情報の共有スキーム（案）



サイバー社会浸透と現実を見据えた御提案

匿名化システム、不正アプリ等への対抗

2013年1月31日
株式会社ラック
セキュリティ事業統括 事業推進部 西本 逸郎

本書は、西本逸郎個人の意見であり、株式会社ラックや、所属・関係している団体等の意見を代表したものでは、一切ありません。

また、内容も社会一般に対するものではなく、趣旨と背景をご理解頂いている範囲でのお取扱を、お願いいたします。

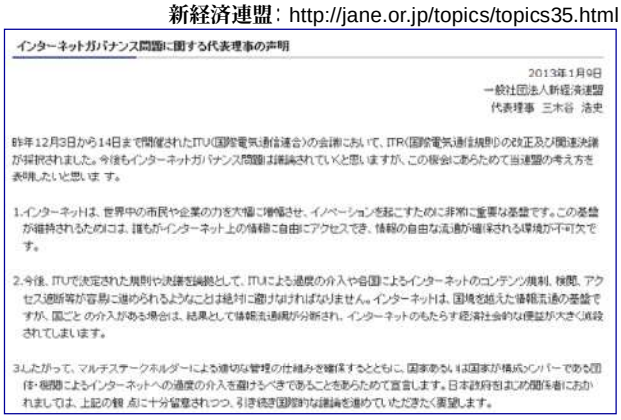
1. 匿名化システムに関して

インターネット(サイバー)社会に関し、
以下の二点がポイントであろうかと
考えます。

1) インターネットの安易で過度な
監視や検閲に関する拒否。

2) インターネットにおける、
匿名化システムを乱用した
犯罪の温床化への対抗

新経済連盟: http://jane.or.jp/topics/topics35.html



インターネットガバナンス問題に関する代表理事の声明

2013年1月9日
一般社団法人新経済連盟
代表理事 三木谷 浩史

昨年12月3日から14日まで開催されたITU(国際電気通信連合)の会議において、ITR(国際電気通信規則)の改正及び関連決議が採択されました。今後もインターネットガバナンス問題は議論されていくと思いますが、この機会にあらためて当連盟の考え方を表明したいと思います。

1.インターネットは、世界中の市民や企業の力を大幅に増幅させ、イノベーションを起こすために非常に重要な基盤です。この基盤が維持されるためには、誰もがインターネット上の情報に自由にアクセスでき、情報の自由な流通が確保される環境が不可欠です。

2.今後、ITUで決定された規則や決議を端緒として、ITUによる過度の介入や各国によるインターネットのコンテンツ規制、検閲、アクセス遮断等が容易に進められるようなことは絶対に避けなければなりません。インターネットは、国境を越えた情報流通の基盤ですが、国ごとの介入がある場合は、結果として情報流通網が分断され、インターネットのもたらす経済社会的な便益が大きく損なわれてしまいます。

3.したがって、マルチステークホルダーによる適切な管理の仕組みを確保するとともに、国家あるいは国家が構成メンバーである団体・機関によるインターネットへの過度の介入を避けるべきであることをあらためて宣言します。日本政府当おじめ関係者におかれましては、上記の観点に十分留意されつつ、引き続き国際的な議論を進めていただきたく要望します。

この、<u>相対する命題</u>に応えなければならない。
→ そのためには、残念ながら、完全に守られた世界の実現は不可能であることを認識し、<u>事故前提の対応力強化を図る</u>ことが肝要と考えます。

1. 匿名化システムに関して

3) 関係者への対応要請

① 利用者
匿名化システムの適切利用へ、リテラシーとモラル教育の実施と過剰利用抑制策

② 組織
企業や団体内部での匿名化システム利用に係るポリシーの制定要請とその実施依頼
→ モニターや遮断方法。

③ サービス提供者
→ 匿名化システム利用者への利用ポリシーの制定要請とその実施依頼
※ 同時に、CSRFへも同時に考慮要請できるとよい。
(1) 利用を遠慮いただくサービス
(2) 詳細な記録を取得し許可するサービス
(3) 全く、考慮しないサービス

※ 利用の見極め方法などは例を提示できるとよい。ノードリストのDB化、
スクリプトによる利用回避 等

1. 匿名化システムに関して

4) 万一への備え

国を揺るがすような事件、社会的に影響が大きな事件などが匿名化システムによってなされた可能性が高いと判断された場合、ある決められたルールにのっとり捜査が可能となるよう準備をしておくことが、重要と考える。また、匿名化システム自身に係る研究も重要である。

① 万一のためのログ取得要請

インターネット接続プロバイダーに対して、匿名化システム利用のログ保持を要請する。

「契約者・接続先IPアドレス・時刻」の保持ができれば、後日判明する、匿名化システム利用時刻（利用された側のアクセスログから知ることができる）と突き合わせることにより、絞り込める可能性がある。また、犯罪への悪用抑制も見込む。

② 匿名化システムの解析・研究

システムの持つ脆弱性や実際の動作から、調査可能な中継ノードへの捜査能力の向上を図る。

2. 不正アプリに関して

1) ウイルスの変化

	従来	最近
プログラム	如何にもウイルス	普通のプログラム
感染方法	Exploit	人間系への騙し
目的	データ窃取系	遠隔操作系
作成者	プロ・海外	普通のプログラマ・国内
判別	明快	難しい
出回り範囲	広範囲	特定場所

※ もちろん、目的により高度で組織化されたところが仕掛けているものも存在するが、其のレベルへの対応に関しては多く述べられているのでここでは対象としない。むしろ、一般化しているところに、注意を払う必要がある。

2. 不正アプリに関して

2) 不正指令電磁的記録の作成や供用罪の回避

「はなから、そのつもり」の犯人が、利用者を騙すために、利用規定などで、プログラムの説明を偽り①、若しくは、利用者が騙されることを見越して「正直」に取得を宣言②して、プログラムを配布するケースが出てきているようだ。

実際に、配布者を信頼してよいかどうかは、現実には、その後、決まるものである。
また、そのときは全うに考えていても、後で気が変わるかもしれない。

こういう輩への対抗（所謂、入り口対策）はきっちりやっていただきたいが、本来、防ぐべき、情報流通拡散の防止（所謂、出口対策）の考慮も、必要と考える。

特に、本人の意図しないプライバシー情報等の「善意の第三者」による拡散は、なんらか考慮する必要があると考える。
（ある面、忘れられる権利と同等なのかもしれない。）

2. 不正アプリに関して

3) 万一への備え

ウイルス対策ソフトの導入は、一般社会においても相当な啓発が図られてきていると考えるが、ここにきて「ウイルス対策ソフトでは防ぐことが出来ない」という理解から、脱落も懸念されるところである。

一案であるが、万一の場合、自身の無実を証明できるための「ボイスレコーダ」のような機能を、市販のウイルス対策ソフトに持っていただいたらどうだろうか。

望ましいフォーマット、暗号化方法等を取り決め合理性と真正性を確保し、各社に理解頂き導入していただく。万一の場合は、「ボイスレコーダ」を捜査機関などに提出いただき、プライバシーを確保しつつ、犯人の行為・手口（遠隔操作）をあぶりだし、冤罪を防止するとともに、合理的な捜査を後押しすることが可能となる。

2. 不正アプリに関して

4) 技術解析能力

二つの能力に関する「規模」が求められている。

① フォレンジック

サイバー犯罪でなくとも、サイバー捜査能力の向上が、カギを握っている時代である。そのためには広大なサイバー空間で発生する事件を見越した、体制の規模が必要になる。

② 不正プログラム解析

恐らくは、立件において実際に「手を下した」プログラムの解析が求められる。この解析は、従来の「ウイルス対策=発見と駆除」に必要な、解析とは別物である。

捜査機関において、本技術の習得と研鑽に関しては随分と進んでいるものと推測するが、その、規模が課題となってくる。

3. 官民連携の摸索

1) 前述の規模への対応

フォレンジックと不正プログラム分析

2) 情報連携

① WikiProfile.jp (作成中)
閉鎖的な匿名掲示板

② ワークショップの開催
関係者の人脈交流には大きな意味があると考えます。
今後も、随時開催しますが、ご要望などありましたら、遠慮なくご相談ください。

ありがとうございました。

Any question ?

平成２４年度総合セキュリティ対策会議　第3回　資料

ウイルス感染による匿名P2Pへの情報漏えいの顛末

～漏えい情報を悪用し企業脅迫を迫る犯人逮捕までの実例～

2013年1月31日
株式会社シンプレクス･コンサルティング
CISO
徳田　敏文（元日本IBM情報セキュリティ担当）

内容

- 事件経緯
  - IPアドレスの特定からそのIPアドレス利用者へリーチするまで
  - 匿名について
- 課題と提言

※本件は、情報管理の問題、プロバイダーの対応の問題、匿名の個人の問題、法律の不備、法的な問題等様々な事例を含んでいますが、今回はIPアドレスとその利用者特定という点に焦点を絞ってご説明いたします。

事件経緯 （1） ー 発覚

発覚

- 2008年6月、業務用PCでWinnyを使用していた日本IBMの委託先社員がコンピュータウイルス（暴露型ウイルス）に感染
  - ハードディスク上のファイルがWinnyに広がる。一部業務データが含まれていた。
  - 問題の人物（以下「I 氏」）がそのファイルを発見し取り込み、内容を分析し公開した。
- 2008年9月、インターネット上の掲示板（2ちゃんねる）に、日本IBMが請け負った業務に係る資料4点の画像が投稿される ※5ページ目参考
  - プロジェクト体制図、プログラムコード、マニュアル、個人情報の入った本番データも含まれていた
- 同時に別のP2Pファイル共有ソフトである Share にファイルおよびファイル名を加工して意図的に流出させていることが発覚

事件経緯 （2） ー 調査

調査

- 「I 氏」は、2ちゃんねるに日本IBMの著作物と個人情報約１１万人分のうち、1,500人分のファイルを公開し、ファイルのダウンロードに必要な情報など書き込みをしていた
  - この時点で、ウイルスが共有させるWinny以外の別P2Pファイル共有ソフト Share への公開を明らかにしている。
- Shareアプリの情報流通原理を調査し、当時約20万台の総当り調査（クローリング）を実施してファイル公開者のIPアドレス特定に成功
- 2ちゃんねるの書き込みにあるアップロード画像や、委託先社員の会社のWEBアクセスログなど複数の方法からIPアドレスを特定
- クローリングで得たIPアドレスと一致した

事件経緯 （3） ー 対応

対応

- ファイルの送信停止･削除などを求める警告書を作成し、プロバイダー経由で「I 氏」と2ちゃんねるのやじ馬に送付
  - 匿名が破れたと思ったやじ馬から、書面に書かれている連絡先に問い合わせが入り始め、データの送信者は激減する
  - ※6ページ参考
- 「I 氏」は、2ちゃんねるへ投稿を続け、読者に情報の拡散を続けるように呼びかけつつ、個人情報を段階的に公開し始める
  - こちらから送付した警告書文面など本人にしか届かない内容、知りえない内容も掲載するようになった。
  - 特定したIPアドレスが、「I 氏」が使用している
- 「I 氏」に対する発信者情報開示の請求を行ったが、「I 氏」は情報開示に不同意のため、プロバイダーは、「I 氏」に関する情報の開示はできないとの結論に至った。
- ダウンロードを阻止（難しく）する技術開発に成功･適用
  - 公開されるファイルに対してダウンロード阻止の方策をとり、それでも「I 氏」のアップロードが続く。

事件経緯 （4） ー 顛末

顛末

- 2009年2月 プロバイダーに対するログ保全、IPアドレス使用者の情報開示仮処分命令（東京地裁）
  - プロバイダーからIPアドレス使用者の氏名･住所が開示される
- 2009年3月 「I 氏」に対する情報公開（アップロード）禁止の仮処分命令（東京地裁）
- 2009年6月 「I 氏」を日本IBMの著作権を侵害したとして告訴。翌月逮捕（警視庁）
- 2009年8月 「I 氏」が起訴される（東京地検）
- 2009年9月 刑の決定

2ちゃんねるに投稿された内容

I 氏が2ちゃんねるに書き込んだ内容の実物

215 :[名無し]さん(bin+cue).rar:2008/09/12(金) 19:26:57 ID:Y4Z0cspd0
>>43
[仁義なき] 5Xのドキュメント vol7.zip eOjVW3luCw 157,529,775
[仁義なき] 5Xのドキュメント vol8.zip eOjVW3luCw 317,346,353
[仁義なき] 5Xのドキュメント vol9.zip eOjVW3luCw 233,453,691
[redacted]システム開発に関する資料。今年6月の流出。Vol7のみ完走
本番データらしきもの[redacted]の名前、住所、口座番号がある。[redacted]分(約10万人)あるかも
他に、[redacted]一覧」等テストの過程で出力されたデータ(名前や口座番号)が少々
さてこれは本番データでしょうか。最初日本IBMからの流出かと思ったが、ベトナムオフショア
開発に関する資料があることから[redacted]し(東京都中央区日本橋)からの流出と推定
この件に関しては、ほとぼりがさめるまでこれ以上の活動は自粛
http://up2.viploader.net/upphp/src/vlphp228827.png
http://up2.viploader.net/upphp/src/vlphp228828.png
http://up2.viploader.net/upphp/src/vlphp228829.png
http://up2.viploader.net/upphp/src/vlphp228830.png

※ウイルスが生成する不適切な文字列やファイルの特定情報が含まれる部分は塗りつぶししています。

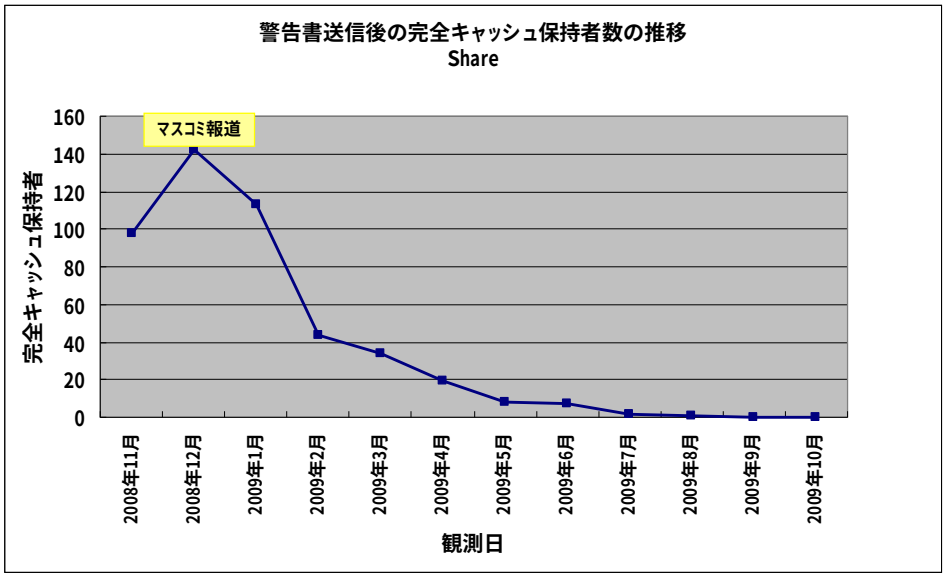
3つの流出ファイル内容の一部と1つのファイル・リストが掲載されていた

①

実データのため読み取りにくくしてあります。

警告書の効果

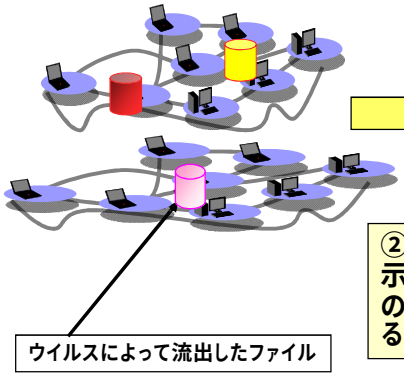
- ファイル公開者と1対1で接続し確実にファイルを保有し発信している人物を特定した。

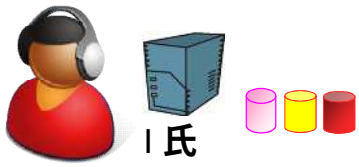


I 氏の日々の行動

Winnyネットワーク

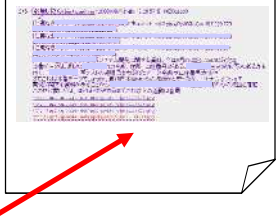
①Winnyに流通している情報を日々収集する





I 氏

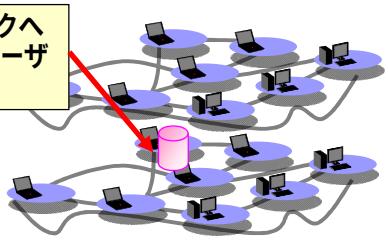
2ちゃんねる



②内容を調べてネタになりそうなものは、掲示板にダウンロードに必要な情報やファイルの内容などを掲示し、情報の拡散を呼びかける

ウイルスによって流出したファイル

③ファイル名を変更してShareネットワークへ意図的にアップロードし不特定多数のユーザーがダウンロード可能な状態にする



Share ネットワーク

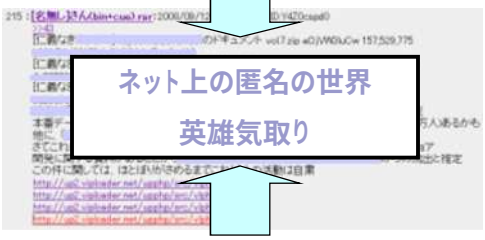
※仙台で観測された同様な行動の人物は、後日新聞の取材に対して、「金銭目的でやっていた。年間1,000万円ぐらいの儲けがあった。」と語っていた。

本当の正体は不明

本性はプロの活動家か？

愉快犯

匿名掲示板



ネット上の匿名の世界

英雄気取り

すごいぞ～

無責任なやじ馬たち

覗き見趣味の「愉快犯」と考えていたが。

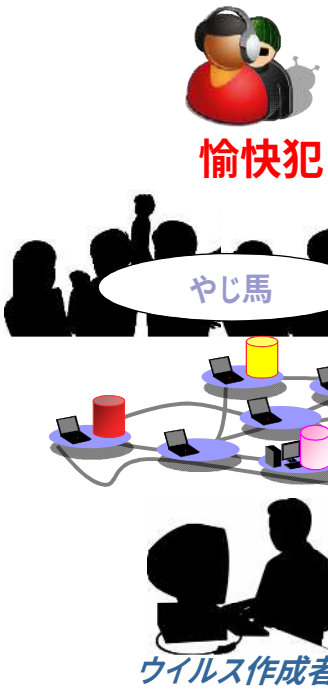
- ネットの住人（匿名掲示板の中では別人格？）
- 掲示板の中では神と呼ばれて英雄気取り
- 匿名でバレなければひどいことを言う
- 世の中が「自分の悪事」で大騒ぎする事を喜ぶ
- 何年たってもおとがめがない（安心している）

この行為は何か危険なのか？

取り締まる法律が無ければなんでも悪用する

自宅から政府や企業を攻撃して潰す事すらできる？

このケースでは、主犯格とやじ馬を分離することで情報拡散を抑止できた



追跡 / 刑事責任の追及
前例を作る。法整備を求める

監視 / 解散
関わりを持たせない

削除 / 拡散防止
技術的に可能なことを示す

ウイルス作成の動機を与えない
ウイルス作成罪
新しい法律ができた

エスカレートすると挑発的な行動に出るが、そこを利用することができた

94 : [名無し]さん(bin+cue).rar : 2008/11/13(木) 23:38:55 ID:+4tycKjX0
本当はこれもUp保留の予定だったのだが
[redacted]が流出を認めないので
テストデータだと思ってUpしたら…全部本物だったのね

↓何のために導入したのやら。運用がザル
http://up2.viploader.net/upphp/src/vlphp236398.png

95 : [名無し]さん(bin+cue).rar : 2008/11/13(木) 23:48:45 ID:ySyowJuB0
馬鹿だなぁ。おまえ捕まるぞ。

仁義なき[redacted]ウイルス情報 Part78

対応状況を公表しないことによって、苛立ちでデータをアップロードしてくる。そこを観測できるように網を張っていた

複数の書き込みとクローラーによる観測の一致で「I 氏」のIPアドレスは確実に特定されていった

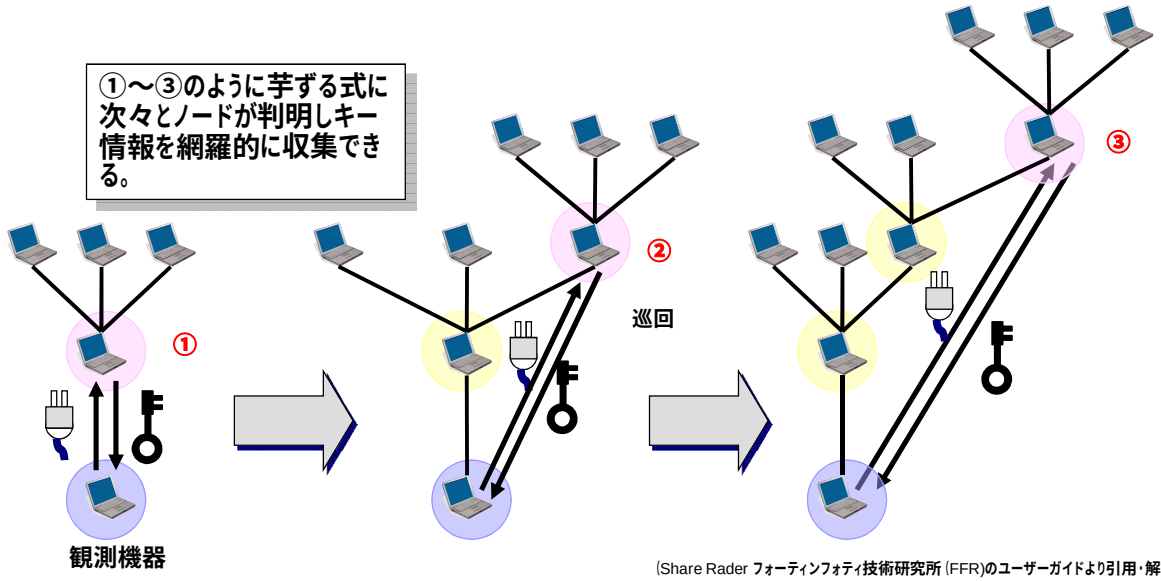
736 : [名無し]さん(bin+cue).rar : 2009/03/07(土) 19:38:26 ID:qkskzih10
日本IBM,やる気みたいね。明日受け取る
黒幕[redacted]らしい
訴状や第1回口頭弁論期日・場所は、追って公開します
http://www2.uploda.org/uporg[redacted]

仁義なき[redacted]ウイルス情報 Part84

赤枠内はすべてIPアドレスが特定でき、今までのIPアドレスと一致した。

暗号通信を使用するアプリでも研究を続けるとよいアイディアが出てくる

クローリングという調査方法は、接続ノードが保持している他のノード情報（IPアドレスやポート番号）を取得するという操作を繰り返していく事で、WinnyやShareが稼動するノードを網羅的に調査する。さらに、接続したノードからファイルの所在情報(キー)を繰り返し集めることで、 WinnyやShareが稼動するノードだけではなく、ファイルの所在情報(キー)も網羅的に収集することが可能。



（Share Rader フォーティンフォティ技術研究所（FFR)のユーザーガイドより引用・解説）

課題と提言

- 民間企業・個人対プロバイダーでは、発信者情報開示などは事実上不可能である（あった）
  - 特定方法が明確で悪質なケースは、民間どうしでも開示できるような仕組みが必要ではないか
- 相手が不明であったり、掲示板が関係している事案の場合は警察に理解してもらうことが難しかった
  - そこに違法行為がないのか、話を聞いてもらいたかった。（2008年当時）
- 匿名を一部でも打ち破ると事態は好転する
  - 特にやじ馬など本気でない人は、一斉に解散する。
- IPアドレスは、論理的なアドレスであり、ある時間にそのIPアドレスを使用していた者の特定には、複数の技術的アプローチによることが好ましい。
- IT犯罪を未然に防ぐ法的整備が今後も必要
  - 何を取り締まるのが効果的なのか専門家で議論してほしい。
  - ウイルス作成罪や改正不正アクセス禁止法などは効果が高いと感じている。

参考（1） 当時のWEBニュース記事

全 国　　ページ更新時間：2009年07月29日（水）12時05分

■ IBM作成データを公開した容疑で逮捕

神奈川県が発注し、日本ＩＢＭが作成したデータを、ファイル共有ソフト「ｓｈａｒｅ」を使ってインターネット上に公開したとして、５０歳の無職の男が警視庁に逮捕されました。

著作権法違反の疑いで逮捕されたのは、東京・八王子市に住む[redacted]容疑者（５０）で、去年１１月、「日本ＩＢＭ」の著作物である「神奈川県立高校授業料徴収システム」などを、ファイル共有ソフトを使ってインターネットに公開した疑いが持たれています。

システムは神奈川県が「日本ＩＢＭ」に作成を依頼したもので、県立高校の生徒の氏名や住所、振り込み口座番号なども入力されていました。

ＩＢＭの下請け会社の社員がパソコンごと自宅に持ち帰ったところ、ウィルスに感染し流出。これを発見した[redacted]容疑者が、ファイル共有ソフト「ｓｈａｒｅ」を使って公開していたということです。警視庁の調べに対し、[redacted]容疑者は容疑を否認しています。（29日11:43）

MBS毎日放送の動画ニュースサイトより引用

2009年7月29日 13時04分

IBMファイル流出容疑で男逮捕 生徒の個人情報も　KYODO NEWS

日本IBMの著作物を含むファイルをインターネット上に流出させたとして、警視庁生活経済課などは29日、著作権法違反の疑いで東京都八王子市館町1097、無職[redacted]容疑者（50）を逮捕した。生活経済課によると、ファイルには、昨年流出が発覚した神奈川県立高校の生徒約2千人分の個人情報が含まれていた。川嶋容疑者は「シェアにアップロードするのが違法と知らなかった」と容疑を否認。

共同ニュースより引用

「シェア」でIBMファイル配布＝著作権法違反容疑で男逮捕－警視庁

ファイル共有ソフト「Share（シェア）」を使い、日本アイ・ビー・エムが著作権を持つプログラミング関係ファイルをインターネット上でダウンロードできる状態にしたとして、警視庁生活経済課などは29日、著作権法違反容疑で、東京都八王子市館町、無職[redacted]容疑者（50）を逮捕した。

同課によると、ファイルをネットで公開したことは認めたが、「著作権法に違反するとは思わなかった」と容疑を否認している。（2009/07/29-12:20）

参考（2） 当時の本件に対する有識者の意見の一部

- 流出データをネット上から削除するにはネット上に公開した本人でないと消去できない。県教委は人物の特定には捜査機関の協力が必要とみているが、県警幹部は「流出データは違法な情報でなく、悪用の事例など被害申告もない。二次被害の抑止を徹底してもらうしかない」と、現状では捜査機関が介入する状況 ではないとしている。
- 「接続業者には通信の秘密があるので現在の法体制では（開示は）非常に難しい」
- 県教委は個人情報保護法の適用を年頭に県警に相談したが、県警は個人による流出のみでの摘発は困難と回答したという。内閣府によると、同法は事業者による個人情報の目的外使用を禁じているが、表現の自由などとの兼ね合いから、個人の行動の制限は想定していない。服部政男・一橋大名誉教授（情報法）も「ネットの進展に法整備が追いついておらず、今回情報を流出させた者の刑事責任を問うのは難しいのではないか」
- 県は関連法として「刑法」「プロバイダ責任制限法」「個人情報保護法」を挙げ、「いずれも個人情報などをインターネット上に意図的に流出させる個人の行為に対し、法的責任を問えるものではない」と指摘。地方公共団体に管理責任がある個人情報などを取得した人物が、インターネットを介して不特定多数の者が入手できる状態に置く行為を禁止し、罰則を規定した法律を早急に制定するよう求めている。
- 日本IBMはこれまで独自に公開者のネット上の識別番号を割り出し、ネット接続業者に公開者の氏名などの公表を要求。しかし、業者側は「本人の同意がなければ開示できない」などと拒否していた。
- 日本IBMは発信者の情報開示を求めて東京地裁に提訴。二月下旬に仮処分が出ると、接続業者は開示に応じたという。日本IBMは特定できた「公開者」に、ネット上から情報の削除し、拡散をやめるよう要請。返答がなかったため、不正競争防止法に基づく営業秘密の保護などを理由に情報再発信の禁止を申し立て、今月六日に仮処分が出たという。同社は「相手の出方次第で、提訴や告訴も引き続き検討する」としている。
- 県教委は今後、公開者本人への直接の働きかけを始めるほか、日本IBMに対し損害賠償請求する方針。仮処分については「裁判所が今回の行為が問題という判断を示したことが大きい。できる範囲の対策でも抑止効果になる」と評価している。
- 個人による漏えいそのものを犯罪として問うことが難しかった点について、ネット犯罪に詳しい紀藤正樹弁護士は「個人情報保護法の不備を露呈させた珍しい事件だ。警視庁はやむを得ず、形式犯の著作権法で逮捕したのではないか」と指摘する。

平成２５年１月
警察庁

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
～いわゆる遠隔操作ウイルス等による犯行予告事案を受けて～

趣旨

一連の遠隔操作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

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

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

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

平成25年1月16日
サイバー空間の脅威に対する
総合対策委員会決定

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
～いわゆる遠隔操作ウイルス等による犯行予告事案を受けて～

一連の遠隔操作ウイルス等による犯行予告事案により、警察のサイバー犯罪捜査に対する信頼が大きく揺らぐとともに、情報通信技術の急速な発達に警察捜査が追いつけていないのではないかとの不安を国民に与える結果となった。これら一連の事案については、関係都府県警察において検証が行われ、サイバー犯罪捜査に関しては、捜査員間での知識レベルの差が大きく、本件捜査においても、第三者による遠隔操作について、知見は有していたものの、その可能性を見いだすことができなかったこと等が示された。

サイバー空間の安全・安心の確保は、警察として最優先で取り組むべき課題の一つであり、これまでも警察庁では「警察庁サイバーセキュリティ重点施策」等により各種施策を推進してきたところであるが、今回の一連の事案を受けて当面緊急に推進すべき施策を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として取りまとめた。今後は、本プログラムを着実に実施し、サイバー空間の安全と安心を確保するよう努めるものとする。

第１　対処能力の向上

今後ますます高度化・複雑化するサイバー犯罪等に対処するため、次の施策により、サイバー犯罪等対処能力の向上を図る。

１　捜査力及び解析力の強化

(1)　専門的知識・能力を有する者の採用等

ア　官民人事交流

民間事業者の知見を活かし、最新の情報技術に対応した各種施策を実施していくため、警察と情報通信企業等との人事交流の実施を検討する。

イ　情報通信職員の採用拡大

インターネットやスマートフォンが普及し、多くの犯罪に悪用され、情報技術解析部門に持ち込まれる電磁的記録の解析業務が質・量共に増大していることから、解析対応力の向上のため、情報通信職員の新規採用の拡大に努める。

(2)　効果的な教育・訓練

ア　民間企業への講義委託等

捜査員一般のサイバー犯罪捜査に係る知識の底上げを図るため、民間企業に講義を委託するほか、捜査員の知識等に応じた効率的な教育の実施に努める。

イ　大学等への派遣

情報通信技術や情報セキュリティ等に関してより高度で専門的な知識を習得させるため、海外を含め、情報セキュリティ等に関する教育を行っている大学等への捜査員、解析担当職員等の派遣を検討する。

ウ　捜査員のための各種マニュアルの作成等

捜査員がサイバー犯罪に利用される情報通信技術の基礎を習得できるよう、情報通信技術に係る基礎的なマニュアルを作成するほか、デジタルフォレンジックによる犯罪捜査への技術支援を促進するため、捜査員及び捜査幹部向けのガイドブックを充実強化する。また、インターネット上の殺人予告等の事案に効果的に対応するため、これまでに発生した犯行予告事案の分析を踏まえた同種事案への対応マニュアルを作成し、捜査員に対する教育・訓練の実施に努める。

エ　高度かつ実戦的な訓練

サイバー空間の脅威への対処能力の向上や高度な技術・知識の習得のための情勢に対応した訓練環境を整備し、第一線で活動する警察職員に対し、高度な解析手法の習得等を目的とした実戦的な訓練の実施に努める。

(3)　捜査手法等

ア　捜査特別報奨金制度の効果的活用

匿名性が高く犯人に結びつく情報の収集が困難であるサイバー犯罪に関する警察への情報提供を促す手法の一つとして、一定の要件を満たしたこの種の事件等を捜査特別報奨金の対象事件として指定することができるよう、捜査特別報奨金取扱要綱を改正したところであり、同制度の効果的な活用を図る。

イ　おとり捜査の積極的活用等

サイバー犯罪捜査においては、事後的な犯人の追跡に困難を伴うケースが多

々あることから、買受け捜査を積極的に活用するとともに、新たな捜査手法について検討する。

ウ　ハッカーからの協力の確保

いわゆるハッカーは、ハッカーフォーラム等の場において、様々な情報交換を行っていることから、こうしたハッカーコミュニティーに積極的に警察職員が参加するなどしてハッカーとの関係を構築し、必要な情報収集を行う。

(4)　新技術に関する研究等

ア　Ｔｏｒ等高度匿名化技術に係る調査・研究

Ｔｏｒ(Ｔｈｅ　Ｏｎｉｏｎ　Ｒｏｕｔｅｒ)等のインターネット上の高度匿名化技術の最新の状況について調査・研究を推進する。また、Ｔｏｒ等高度匿名化技術を利用した通信からのアクセス制限等を含め、高度匿名化技術を用いた犯罪に対する効果的な対策について検討する。

イ　諸外国の捜査手法に関する調査・研究

サイバー犯罪はその特性から容易に国境を越えて行われ、他国で用いられた手口が我が国において利用されることがしばしばあることから、外国捜査機関におけるサイバー犯罪捜査手法の調査・研究を推進する。

2　体制の整備

(1)　サイバー犯罪捜査員及び解析担当職員の増員

サイバー犯罪の高度化・複雑化に対応するため、サイバー犯罪捜査員及び解析担当職員の増員に努めるとともに、都道府県警察からの派遣要請に機動的に対応すべく各管区警察局等に設置されている都道府県(方面)情報通信部情報技術解析課への「機動解析班」の設置等により、サイバー空間の脅威に対処するための体制の充実を図る。

(2)　「全国協働捜査方式」の拡充

サイバー犯罪捜査を効果的・効率的に推進するための、いわゆる「全国協働捜査方式」について、警視庁に設置されている情報追跡班の体制を強化するなどして同方式の拡充を図る。

(3)　サイバー攻撃対策の強化

サイバー攻撃対策について、警察庁の情報収集・分析機能、都道府県警察に対する司令塔機能等を強化するため、「サイバー攻撃対策官」の設置に努めるほか、情報通信部門との連携の下、サイバー攻撃の被害防止及び初動捜査に従事すべく、主要都道府県警察への「サイバー攻撃対策隊」の設置に努めるなどしてサイバー攻撃対策の強化を図る。

(4)　サイバー犯罪に対処するための体制の在り方の検討

サイバー犯罪の形態が多様化している最近の情勢やサイバー犯罪に対する国民の不安感の増大等を踏まえ、高度化・複雑化するサイバー犯罪に対してより効果的な対処を可能とするための警察庁の体制の在り方を検討する。

(5)　「不正プログラム解析センター」の拡充等

不正プログラムの解析体制を充実するため、平成24年11月１日に設置した「不正プログラム解析センター」の体制強化、不正プログラム解析に係るデータベー

スの拡充、不正プログラム解析に関する外国関係機関との情報共有等を推進する。

3　資機材の整備

(1)　新種のウイルスを検知するためのシステムの高機能化

最新のパターンファイルを適用したウイルス対策ソフトであっても検知できない新種のウイルスの検知をより確実なものとするためのシステムの強化に努める。

(2)　解析用資機材の高機能化

情報通信技術や電子機器を利用した犯罪が巧妙化・複雑化している中で、新たな情報通信技術や電子機器が用いられた犯罪にも対応できるよう解析用資機材の更新・強化に努める。

(3)　インターネット観測用システムの高機能化

ＤｏＳ攻撃による被害観測やボットネット観測、Ｐ２Ｐ観測等の各種観測機能を高度化することにより、サイバー犯罪・サイバー攻撃手法の巧妙化・複雑化に対応する技術力を強化するため、現在運用中のリアルタイム検知ネットワークシステムの更新・強化に努める。

第２　民間事業者等の知見の活用

サイバー空間の脅威に対処するためには、警察による取締りのみならず、民間事業者等の知見を活用した取組が必要である。そこで、次の施策により、民間との協力の強化、各種抑止対策等を推進する。

１　情報共有枠組みの構築

(1)　アンチウイルスベンダーとの情報共有等

新種のウイルスに対して早急な対策を講じることができるよう、警察が把握した新種ウイルスに係る情報や、アンチウイルスベンダーが把握した新種ウイルスに係る情報を相互に交換するため、既存の枠組みを活用しつつ、新たな情報共有の枠組みの構築や、民間との協力によるウイルスに係るデータベースの構築を検討する。

(2)　各種情報共有枠組みの活用

「サイバーインテリジェンス対策のための不正通信防止協議会」、「サイバー犯罪に対する警察と民間事業者の共同対処に関する指針」を受けた関係企業との協力体制等の既存の枠組みを活用して、民間との協力による情報共有の取組の強化を図る。

２　官民一体となったサイバー犯罪抑止対策の推進

(1)　通信履歴(ログ)の保存

サイバー犯罪捜査では、通信履歴が必要不可欠であるが、通信履歴が保存されていないために犯人の特定に支障が来す例が少なくないところ、サイバー犯罪抑止等の観点から通信履歴が一定期間保存されるよう、民間事業者等の取組の促進を図る。

(2)　インターネット・ホットラインセンターの拡充

インターネット上に氾濫する違法情報・有害情報に対処するため、サイバー犯罪をめぐる情勢の変化を踏まえて、違法情報・有害情報類型の見直しを図るとと

もに、インターネット・ホットラインセンターの体制の拡充に努める。

(3) サイト管理者の管理責任の明確化

インターネット上には、インターネット・ホットラインセンターからの違法情報・有害情報の削除依頼にも応じない悪質なサイト管理者等が存在しているところ、違法情報・有害情報の書き込みに関するサイト管理者の管理責任を明確化するとともに、当該責任を果たしていない場合の措置を検討する。

(4) サイバーパトロール強化

一般のインターネット利用者からの通報が期待されない、登録サイト内等の違法情報・有害情報やウイルスに関する情報を把握するため、サイバーパトロールを強化する。

(5) スマートフォン用アプリに係る被害防止対策

スマートフォン利用者が悪意のアプリ(プログラム)のダウンロードにより個人情報流出等の被害に遭うケースが多発していることから、事業者等と協力して、スマートフォン用アプリに係る被害防止対策を推進する。

(6) データ通信カード契約時における本人確認徹底要請等

事業者に対して、データ通信カード契約時における公的書類による本人確認の実施やインターネットカフェ利用者の本人確認の徹底等を要請する。

3 民間の知見の捜査等への活用

(1) 手口分析等の嘱託

民間の極めて高度かつ特殊な知見や技術を活用することが必要とされる事案について、守秘義務等に関する措置を講じた上で、民間事業者等に手口分析等を嘱託することを検討する。

(2) 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

効率的な解析の実施のため、解析対象となる携帯電話等の各種電子機器やソフトウェアの仕様等の技術情報の共有に関し、民間有識者、民間事業者、業界団体等との協力を強化する。

第３ 国際連携の推進

地理的・時間的制約が少なく容易に国境を越えて敢行されるサイバー犯罪に効果的に対処するべく、次の施策により、国際連携を推進する。

1 外国捜査機関等との情報共有の強化

常時、外国捜査機関等とのサイバー犯罪に関する情報の交換に努めるほか、サイバー犯罪に対する最新の捜査手法を学び、外国捜査機関との連携を強化するため、米国ＮＣＦＴＡ（National Cyber-Forensics & Training Alliance）の捜査実習への職員の派遣等に努める。また、外国関係機関の解析技術部門への職員の派遣を検討する。

2 国際捜査の推進

サイバー犯罪は容易に国境を越えて敢行されることから、証拠の収集等のため外国捜査機関からの協力を得る必要がある事案については、外国の捜査機関に対して積極的に捜査共助を要請し、的確に国際捜査を推進する。

３　サイバー犯罪に係るリエゾンの派遣

主要国にサイバー犯罪捜査に係る連絡調整を任務とするリエゾンの派遣を検討する。

第４　広報啓発

インターネット空間の自由と開放性を背景に、サイバー犯罪の手口は日々変化し、高度化・複雑化しているところ、このような情勢を踏まえ、被害の未然防止等の観点から次の施策により広報啓発を推進する。

１　総合的な広報啓発

政府により毎年２月に実施される「情報セキュリティ月間」や毎年10月に実施される全国地域安全運動等の機会を捉え、不正アクセス防止対策に関する官民意見集約委員会やサイバー防犯ボランティアの活用を図るなどして国民各層の幅広い参加を得た取組を集中的に推進する。

２　民間事業者との会議等の開催

民間事業者との会議や各種講習会、都道府県警察のウェブサイト等のあらゆる機会・手段を通じ、一般のインターネット利用者、民間企業等対象の違いに応じた広報啓発活動を推進していく。

３　警察庁ウェブサイトの活用等

警察庁ウェブサイトを活用し、事件広報、新たな手口の注意喚起、被害に遭った際の対応要領等の紹介を行うほか、民間団体が管理するウェブサイトに対して、各種コンテンツの提供を行うなどの取組を推進する。