不正アクセス事犯の取締り

警察庁生活安全局生活環境課
生活経済対策室　　金澤正和

1

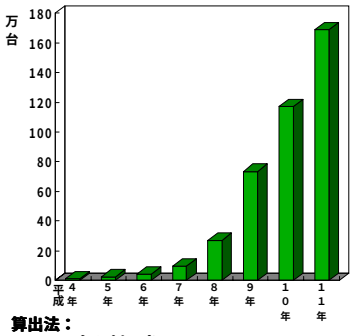
1　不正アクセス禁止法の概要

(1) 制定の背景

2

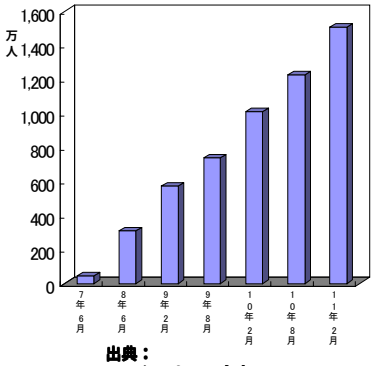
社会のネットワーク化の進展

インターネットに接続されている国内コンピュータ数の推移



算出法：
ドメイン名を割り当てられているＩＰアドレスから算出。
Network Wizards(http://www.nw.com/)による。

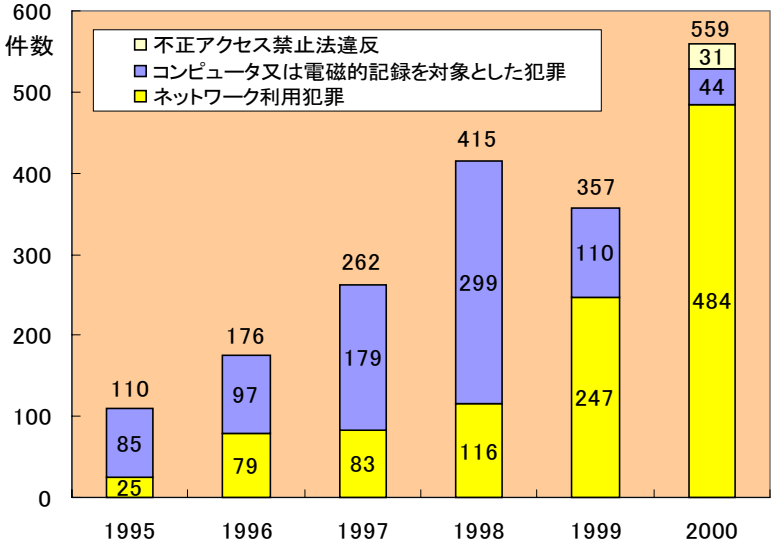
国内インターネット利用者数の推移



出典：
インターネット白書‘９９

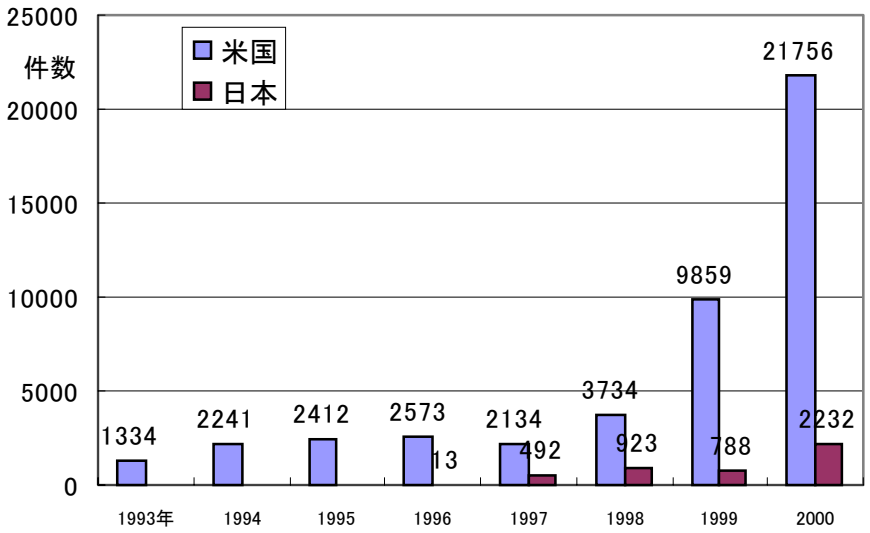
3

ハイテク犯罪の検挙状況の推移



4

日米CERT/CCへの届出インシデント数

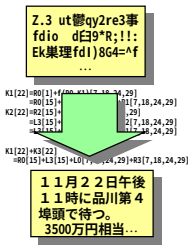


5

ハイテク犯罪対策上の問題点

＜体制上の問題＞

○高度な技術力が必要



データが暗号化され
内容が読めない

高速なコンピュータで
暗号を解読

○国際捜査協力

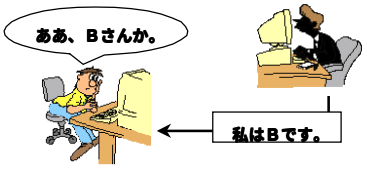
２４時間体制で
国際的な犯罪に対応

インターネットに対する
捜査と主権の調和
（ﾄﾗﾝｽﾎﾞｰﾀﾞｰｻｰﾁ）

＜法制上の問題＞

○不正アクセスが不可罰

「何をやってもばれない」環境が生まれ
犯罪を誘発



○不正アクセスを不可罰としているのは
主要国では我が国のみ

我が国が国際捜査協力の
抜け穴（ループホール）となるおそれ

○物理的痕跡が残らないため、
産業界の協力が不可欠

不正アクセス対策法制の必要性

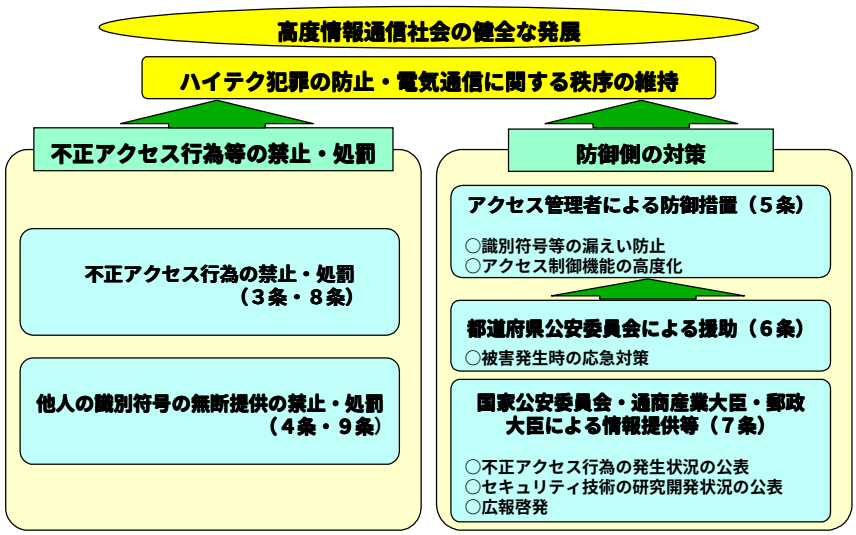
- コンピュータ・ネットワークの発展、普及とハイテク犯罪の増加、被害の深刻化
- コンピュータをネットワークに接続して営まれる社会経済活動の安全を確保しているアクセス制御機能に対する社会的信頼を確保することが必要
- 欧米先進諸国と連携した国際ハイテク犯罪対策の推進

7

(2) 法の概要

8

法の基本構成



9

法の目的（第1条）

本法は、**不正アクセス行為の禁止等**により、**電気通信回線を通じて行われる電子計算機に係る犯罪の防止**及びアクセス制御機能により実現される電気通信に関する秩序の維持を図り、もって高度情報通信社会の健全な発展に寄与することを目的としている。

10

定義－1　アクセス管理者（第2条第1項）

電気通信回線に接続している電子計算機（特定電子計算機）の電気通信回線を通じた利用（特定利用）につき当該特定電子計算機の動作を管理する者

11

定義－2　識別符号（第2条第2項）

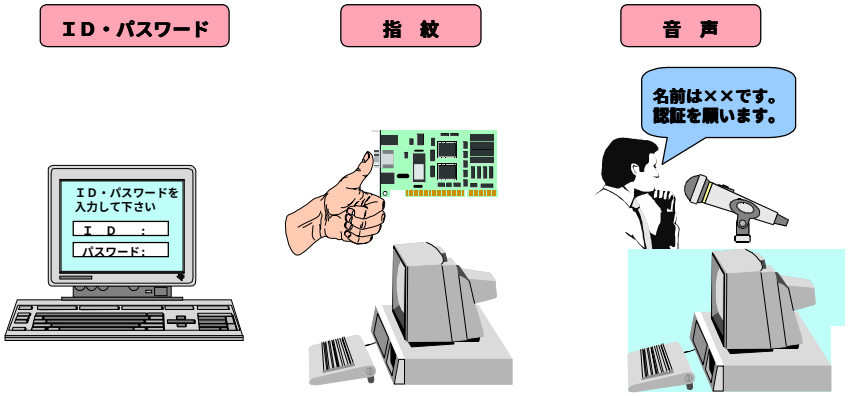
利用権者ごとに定められている符号で、**アクセス管理者が他の利用権者と区別して識別するために用いられるもの**。次のいずれかに該当する符号又は次のいずれかに該当する符号とその他の符号を組み合わせたもの。

1　アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号
2　利用権者の身体の全部若しくは一部の影像又は音声を用いてアクセス管理者が定める方法により作成される符号
3　利用権者の署名を用いてアクセス管理者が定める方法により作成される符号

（注）利用権者：特定電子計算機の特定利用をすることについてアクセス管理者の許諾を得た者

12

識別符号の例



13

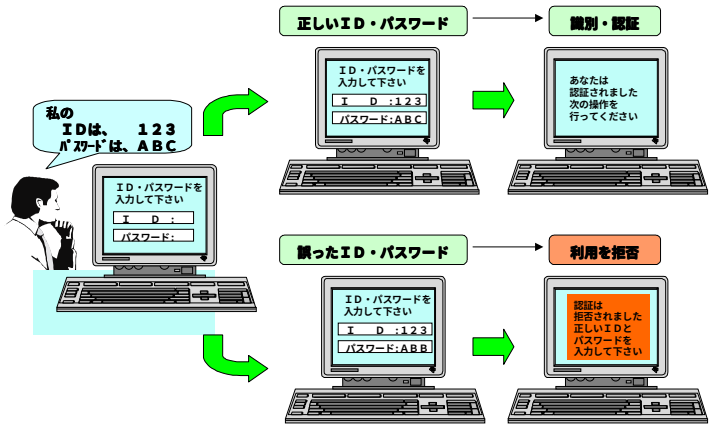
定義－３　アクセス制御機能（第２条第３項）

正規の利用権者以外の者による特定電子計算機の特定利用を制限するために、当該特定電子計算機の特定利用をしようとする者に識別符号（注）を入力させ、**正しい識別符号が入力された場合にのみ利用制限を自動的に解除する当該特定電子計算機等に付加されている機能**

（注）識別符号を用いてアクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号を含む。

14

アクセス制御機能の概要

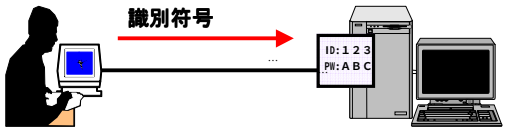


15

アクセス制御機能を付加されている特定電子計算機

特定利用に係る特定電子計算機に付加されている場合

特定利用に係る特定電子計算機

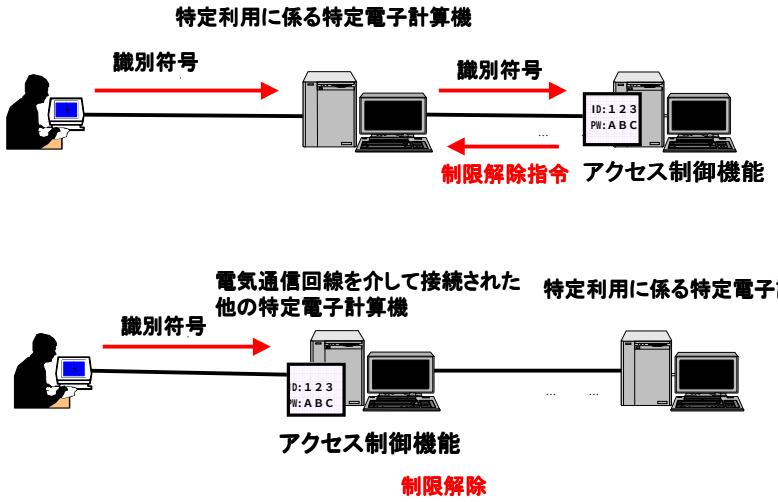


アクセス制御機能

利用制限解除

16

電気通信回線を介して接続された他の特定電子計算機に付加されている場合



17

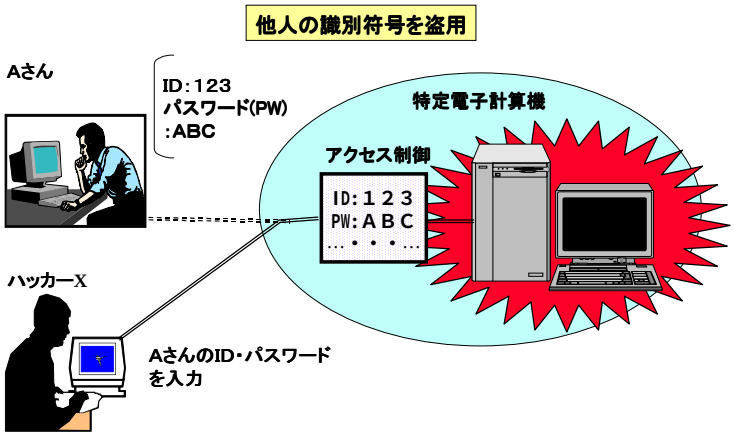
不正アクセス行為の禁止、処罰（第3条、第8条）

アクセス制御機能による利用制限を免れて特定電子計算機の特定利用をできるようにする行為を不正アクセス行為として禁止。違反者には、1年以下の懲役又は50万円以下の罰金。

不正アクセス行為の類型
- 他人の識別符号を無断で入力する行為（第3条第2項第1号）
- 識別符号以外の情報又は指令を入力する行為（同項第2号、第3号）

18

他人の識別符号を無断で入力する行為（第3条第2項第1号）



19

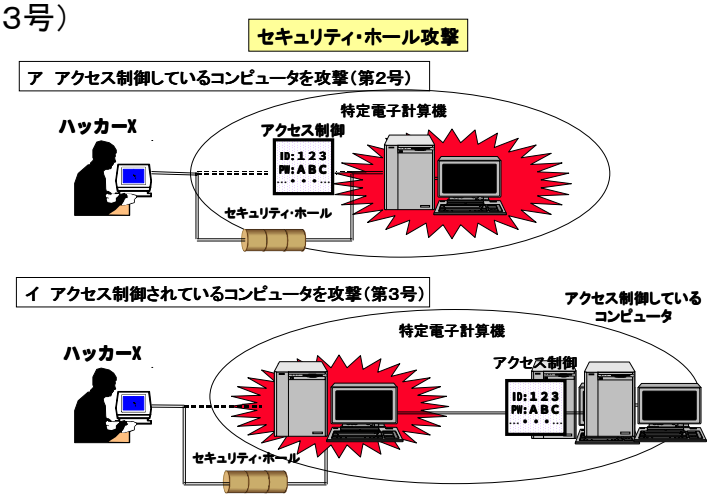
○ 他人名義でプロバイダ等と契約して識別符号を入手した者が当該識別符号を入力した場合には、「他人の」識別符号を入力したことにはならないので、不正アクセス行為には該当しない。

※ 他人名義で識別符号を入手する過程において、私文書偽造・同行使に該当する行為を行っていると考えられる。

○ **アクセス管理者が行う場合**及び**アクセス管理者又は利用権者の承諾を得て行う場合**は、禁止の対象から除外されている。

20

アクセス制御機能による**特定利用の制限を免れることができる情報又は指令を入力**する行為（第3条第2項第2号、第3号）



21

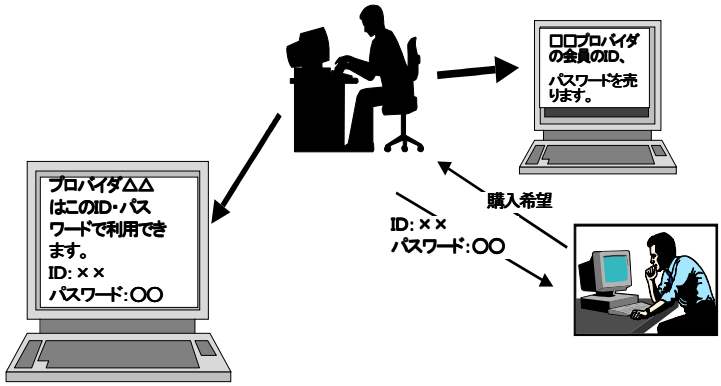
○ アクセス制御機能による特定利用の制限を免れることができる「情報又は指令」には、例のような特殊なコマンド（指令）だけでなく、アクセス管理者に無断で追加されたID・パスワード（利用権者に付されたものではないので、識別符号には該当しない。）のようなものも含まれる。

○ **アクセス管理者又はその承諾を得た者が行う場合**は、禁止の対象から除外されている。

22

不正アクセス行為を助長する行為の禁止、処罰（第4条、第9条）

他人の識別符号を無断で提供する行為を禁止。違反者には、30万円以下の罰金。



23

○ 他人名義、架空名義でプロバイダと契約する等して識別符号を入手した者が当該識別符号を販売していた場合には、「他人の識別符号」ではないので、第4条違反には該当しない。

※ 他人又は架空名義で識別符号を入手する過程において、私文書偽造・同行使に該当する行為を行っていると考えられる。

○ アクセス管理者が行う場合又はアクセス管理者又は利用権者の承諾を得て行う場合は、禁止の対象から除外されている。

24

アクセス管理者による防御措置（第5条）

アクセス管理者は、特定電子計算機を不正アクセス行為から防御するため必要な措置を講ずるよう努めるものとする。

25

具体的な防御措置

- ●識別符号の適正な管理
- ●アクセス制御機能の有効性の検証
- ●アクセス制御機能の高度化
- ●ログの有効活用
- ●ネットワーク・セキュリティ責任者の設置

26

都道府県公安委員会による援助等（第6条）

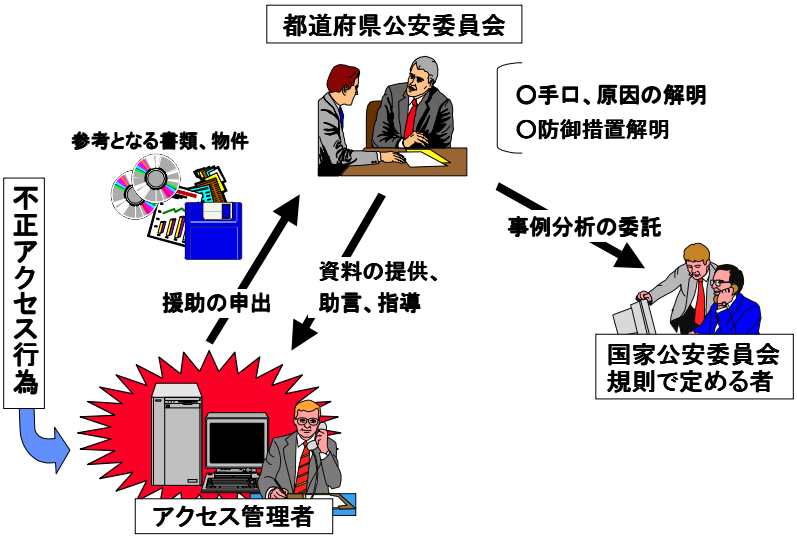
•都道府県公安委員会は、不正アクセス行為に係るアクセス管理者からの申出に応じ、特定電子計算機を不正アクセス行為から防御するため必要な応急の措置が的確に講じられるよう、必要な援助を行うものとする。

•都道府県公安委員会は、援助を行うため必要な事例分析の実施の事務を国家公安委員会規則で定める者に委託することができる。

•委託に係る事例分析の従事者に秘密保持義務を課する。違反者は、1年以下の懲役又は50万円以下の罰金に処する（第8条第2号）

27

都道府県公安委員会による援助の概要



28

国による援助（第7条）

•国家公安委員会、通商産業大臣及び郵政大臣は、毎年少なくとも1回、不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況を公表するものとする。

•国は、不正アクセス行為からの防御に関する啓発及び知識の普及に努めなければならない。

29

２　不正アクセス事犯の取締り状況

30

(1) 不正アクセス行為の発生状況
（平成12年中）

- 認知件数　106件
- 海外からのアクセス　25件
- **ホームページの改ざん、消去を伴うもの　３３件**
- **DDoS用攻撃ツールを仕掛けられていたもの　２件**

31

不正アクセス行為に係る特徴

		認知件数
被害に係る特定電子計算機のアクセス管理者別	プロバイダ	59
	大　学	8
	情報通信企業	6
	その他	33
	計	106

		認知件数
認知の端緒別	アクセス管理者からの届出	30
	利用権者からの届出	23
	発見者からの通報	7
	被疑者の取調べ	35
	その他	11
	計	106

32

不正アクセス対策に関するアンケート結果

- 19．3%の団体が過去1年間に不正アクセス等の被害
- 大学の被害は5割を超える
  - 主な被害は、ウィルス感染55．0%、メールの不正中継45．0%、踏み台27．5%
  - 23．5%の団体が届出。警察への届出5．3%
  - 未届出の理由は、大した被害がなかったから46．7%、社内で対応できたから35．0%、問題解決にならないから21．7%

33

(2) 平成12年中の検挙状況

事 犯 別	検挙事件数	検挙件数	検挙人員
不正アクセス行為	30	62	34人
不正アクセス助長行為	4	5	5人
計	31 （重複3）	67	37人 （重複2人）

●パスワード管理の甘さに付け込んだ事案が多い（12事件、14件）
●ID・パスワード入手等にクラッキング・ツールを利用した事案が多い（8事件、14件）

34

検挙事例1

- **違法薬物販売目的の他人の識別符号を使用した不正アクセス禁止法違反等事件**

　無職の男(34)が、クラッキング・ツール等を利用して入手した他人のＩＤ・パスワードを使用して不正にインターネットに接続し、ホームページを開設した上、薬物販売の広告を掲示し、薬物の購入希望者とメールのやり取り等をするとともに、同ホームページで販売する目的で医薬品や向精神薬を自宅に所持していた。１２年３月、不正アクセス禁止法違反、薬事法違反及び麻薬及び向精神薬取締法違反で検挙した（千葉）。

35

検挙事例2

- **音楽配信会社のメールサーバに対する不正アクセス禁止法違反事件**

　音楽配信会社の元役員(32)が、役員当時知り得た社長等のＩＤ・パスワードを使用して同社のメールサーバに侵入し、電子メールの内容を盗み見た。１２年６月、不正アクセス禁止法違反で検挙した（警視庁）。

36

検挙事例3

- **解雇された会社の識別符号を窃用した不正アクセス禁止法違反等事件**

　情報通信関連会社の元社員(25)が、同社を解雇されたことに立腹し、同社に金銭的損害を与える目的で、在職中に知り得た同社のＩＤ・パスワードを使用して不正にインターネットに接続するとともに、同社に高額のインターネット接続料が請求されるように契約内容を変更する旨の虚偽の情報をプロバイダのサーバに送信して事実証明に関する電磁的記録を不正に作出したほか、ホームページ上で前記ＩＤ等を公開した。１２年１０月、不正アクセス禁止法違反及び電磁的記録不正作出罪で検挙した（警視庁）。

37

検挙事例4

- **広域にわたるハッカー・グループによる不正アクセス禁止法違反事件**

　ハッカー・グループの主犯格の男(30)が、クラッキング・ツール等を利用して入手した他人のＩＤ・パスワードを使用して不正に国立大学、観光協会及びプロバイダの各サーバに侵入するとともに、自己の運営する掲示板において、前記国立大学のサーバに係る同ＩＤ等の掲示、観光協会及びプロバイダに対する不正アクセス手法の教示等を行った。また、同教示を受けた同グループのメンバーである主婦(42)、大学生(23)が、それぞれクラッキング・ツールの利用等教示を受けた手法により入手した他人のＩＤ・パスワードを使用して不正に国立大学又は観光協会のサーバに侵入した。１２年１１月、不正アクセス禁止法違反で主犯格のほかハッカー・グループのメンバー２人を検挙した（愛知、秋田、宮城、警視庁、広島）。

38

検挙事例5

- **大学生が他の大学生の識別符号を窃用した不正アクセス禁止法違反等事件**

　大学生(22)が、自己が好意を寄せる大学生がこれに気付かないことに立腹し、推知した同人のＩＤ・パスワードを使用して不正に大学の認証サーバに侵入し、同人になりすまして同人の名誉を毀損する内容の電子メールを送信するとともに、ホームページの掲示板に同内容を書き込み・掲示し、不特定多数の者に閲覧させた。１２年８月、不正アクセス禁止法違反及び名誉毀損罪で検挙した（埼玉）。

39

検挙事例6

- **ｉモード電話機用のウェブ・サーバに対する不正アクセス禁止法違反事件**

　無職の男(23)が、ｉモード電話機用の掲示板から入手した他人のＩＤ・パスワードを同電話機のメール・サービスを利用してハッカー仲間である会社員(25)に提供、さらに、同会社員が、同ＩＤ等をハッカー仲間である大学生(25)に提供し、同大学生が、同ＩＤ等を使用して不正にｉモード電話機用のウェブ・サーバに侵入し、掲示板の内容を書き換えるなどした。１２年１０月、不正アクセス禁止法違反で無職の男ら３人を検挙した（警視庁）。

40

３　警察における対応

41

(1)　政府における取組

42

政府及び大手企業に対する攻撃の現状

海外での事案

平成11年３月　ＮＡＴＯ（北大西洋条約機構）のサイトにユーゴスラビアのハッカー侵入。
５月　ＦＢＩのサイトがＤｏＳ（サービス拒否）攻撃の被害。サイトを一時閉鎖。
５月　米ホワイトハウスのサイトにハッカー侵入。在ユーゴスラビア中国大使館誤爆事件に抗議。
９月　米株式市場のサイトにハッカーが書き込み。
平成12年２月　米有力ネット企業のサイトがＤｏＳ攻撃による集中アクセスで相次ぎパンク。
５月　「Ｉ　ＬＯＶＥ　ＹＯＵ」と題した電子メールで届く新種のコンピュータ・ウイルスが世界的規模で拡散。
13年１月　米国マイクロソフトのサイトがDoS攻撃による集中アクセスにより障害

我が国での事案

平成11年６月　毎日新聞社、朝日新聞社のホームページが相次ぎ書き換えられる。
平成12年１月　日本の１０以上の省庁・公的機関でホームページが書き換えられるなどの被害

サイバーテロの脅威の現実化

43

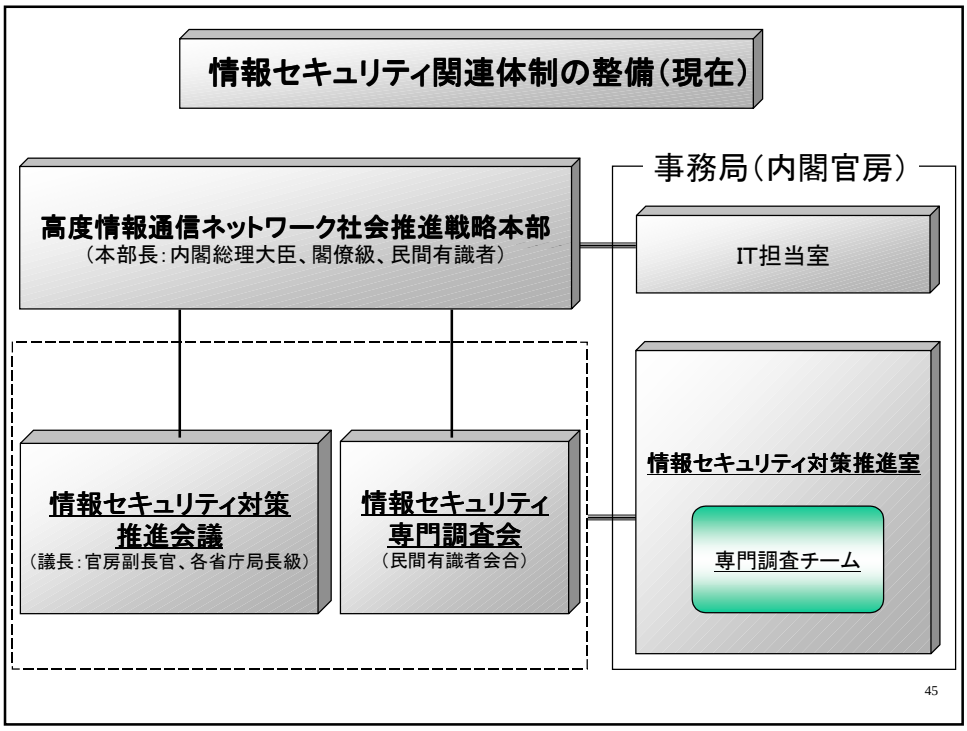
一連のハッカー事案を踏まえ、政府の体制を強化

「情報セキュリティ関係省庁局長等会議」を拡大改組し、
高度情報通信社会推進本部の下に、全ての省庁の
局長級で構成する「情報セキュリティ対策推進会議」
を設置（2000年2月29日 高度情報通信社会推進本部長決定）

高度情報通信社会推進本部の下で、民間有識者からなる
「情報セキュリティ部会」を開催
（2000年2月29日 高度情報通信社会推進本部長決定）

内閣官房に「情報セキュリティ対策推進室」を設置
（2000年2月29日 内閣総理大臣決定）

44



情報セキュリティ確保のための取組

- H12.1　ハッカー対策等の基盤整備に係る行動計画
- H12.7　情報セキュリティポリシーに関するガイドライン
- H12.12　重要インフラのサイバーテロ対策に係る特別行動計画
- H13.1　高度情報通信ネットワーク社会形成基本法
- H13.3　e-Japan重点計画
- H13.6　e-Japan2002プログラム

46

ハッカー対策等の基盤整備に係る行動計画

（平成12年1月 情報セキュリティ関係省庁局長等会議）

情報セキュリティポリシーの策定

各省庁の情報システムに係る情報セキュリティの確保のため、明文化されたポリシーを策定し、情報資産の重要性に応じた安全対策、取扱方法等を定める。

○各省庁共通の「ガイドライン」を作成
（平成12年7月）

○各省庁において、セキュリティポリシーを作成
（平成12年中）

サイバーテロ対策に係る特別行動計画

サイバーテロの対象となる可能性のある重要インフラ分野について、今後講ずべき対策について検討し、行動計画として取りまとめる。

○サイバーテロ対策に係る特別行動計画案の策定
（平成12年11月）

政府調達におけるセキュリティ評価の導入

信頼性の高い政府システムの構築のため、各省庁において十分なセキュリティ水準の製品を利用する。

○「各省庁の調達におけるセキュリティ水準の高い製品等の利用方針」
↓
平成13年度以降運用

47

高度情報通信ネットワーク社会形成基本法

第1条 この法律は、情報通信技術の活用により世界的規模で生じている急激かつ大幅な社会経済構造の変化に的確に対応することの緊要性にかんがみ、高度情報通信ネットワーク社会の形成に関し、基本理念及び施策の策定に係る基本方針を定め、国及び地方公共団体の責務を明らかにし、並びに**高度情報通信ネットワーク社会戦略本部**を設置するとともに、**高度情報通信ネットワークの形成に関する重点計画**の作成について定めることにより、高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進することを目的とする。

第22条 高度情報通信ネットワーク社会の形成に関する施策の策定に当たっては、に必要な措置が**高度情報通信ネットワークの安全性及び信頼性の確保、個人情報の保護その他国民が高度情報通信ネットワークを安心して利用することができるようにするため**講じられなければならない。

第35条第2項 重点計画は、次に掲げる事項について定めるものとする。
一 高度情報通信ネットワーク社会の形成のために政府が迅速かつ重点的に実施すべき施策に関する基本的な方針
二 世界最高水準の高度情報通信ネットワークの形成の促進に関し政府が迅速かつ重点的に講ずべき施策
三 教育及び学習の振興並びに人材の育成に関し政府が迅速かつ重点的に講ずべき施策
四 電子商取引等の促進に関し政府が迅速かつ重点的に講ずべき施策
五 行政の情報化及び公共分野における情報通信技術の活用の推進に関し政府が迅速かつ重点的に講ずべき施策
六 **高度情報通信ネットワークの安全性及び信頼性の確保**に関し政府が迅速かつ重点的に講ずべき施策
七 前各号に定めるもののほか、高度情報通信ネットワーク社会の形成に関する施策を政府が迅速かつ重点的に推進するために必要な事項

48

(2) 国際的な取組

49

G8とハイテク犯罪対策

１９９５年カナダ・ハリファックス・サミット
国際組織犯罪対策上級専門家会合（通称リヨングループ）を設置。

１９９７年ワシントンＧ８司法・内務閣僚級会合
「ハイテク犯罪と闘うための１０の原則と１０の行動計画」を策定。

１９９８年バーミンガム・サミット
「ハイテク犯罪と闘うための１０の原則と１０の行動計画」を首脳レベルで承認。
・２４時間コンタクトポイント　・法制度のレビュー　・トレーニング会合

１９９９年モスクワ国際組織犯罪対策Ｇ８閣僚会合
「コンピュータに蔵置されたデータの国境を越えたアクセスに関する原則」を策定。

２０００年九州・沖縄サミット
政府と産業界の対話の促進、国際的な協調行動の推進について合意。

２００１年ミラノＧ８司法・内務閣僚会合
・児童ポルノ対策の推進
・欧州評議会コンピュータ犯罪条約案文の確定促進、リヨングループによる作業への期待表明
・児童ポルノ関係データベース構築の可能性追求促進、政府・産業界等の協力の重要性指摘　等

国際的な産業界と政府との対話の推進

- 1997年ワシントンG8司法・内務閣僚会合で合意された「10の原則と10の行動計画」に産業界との共同作業が盛り込まれる。
- 1998年バーミンガムサミットにおいて「10の原則と10の行動計画」の推進が首脳レベルで合意され、産業界との緊密な連携が強調される。
- 2000年5月　パリにおいて、政府・産業界の第1回ハイレベル会合を開催
- 2000年10月　ベルリンにおいて、政府・産業界合同のワークショップ開催。
- 2001年5月　東京において、政府・産業界のハイレベル会合開催。

今後、国際的な協調と併せ、各国において産業界等と政府の対話と連携を深める必要性について合意。また、啓発活動・G8以外の国との協力の必要性を指摘。

51

欧州評議会コンピュータ犯罪対策条約

欧州評議会

発足：1949年8月、現加盟国：41カ国、本部：仏・ストラスブール
評議会は加盟国の外相により構成され、国防安保問題は権限外で、主に経済、社会問題での欧州の統合を加盟各国の政府に勧告する。

条約制定の経緯とスケジュール

コンピュータ犯罪対応のため、「犯罪化すべき行為についてのガイドライン(1989年)」、「刑事手続・国際協力の原則（1995年）」を勧告。

1997年：犯罪問題欧州委員会（加盟国政府局長級会合）の下にコンピュータ犯罪専門家会合を設置、条約起草作業を実施。

評議会加盟国以外も締結可能。コンピュータ犯罪対策分野について初めての多国間条約であることから実質的な世界標準になると考えられる。
日、米、加の3カ国は、オブザーバーとして締約を視野に入れつつ策定作業に参加

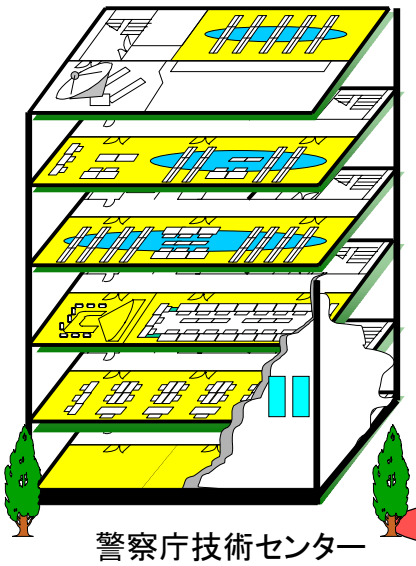
2001年6月18日～22日：刑事問題欧州委員会において最終的な検討。
2001年9月：閣僚級会合で採択。
2001年12月：署名開放。

52

(3) 警察における取組

53

警察の技術対処能力の整備



警察庁技術センター

○ 警察法改正
（平成11年4月）

○ 情報通信局技術対策課
（平成11年4月創設）

○ 警察庁技術センター
（平成11年4月開設）

- 都道府県警察への技術支援
- G8ハイテク犯罪サブグループへの技術面での対応
- ハイテク犯罪に関する技術の調査・分析

充実強化の必要

54

産業界との連携強化

都道府県警察 ← 連絡・調整 ← 警　察　庁

プロバイダ連絡協議会等を通じた産業界との連携

・セキュリティ診断、助言・　指導
・連絡会議の開催、連絡協議会等連携体制の構築
・サイバーテロ発生時の 緊急通報体制の確立

情報セキュリティ・アドバイザーの設置

コンピュータ及びコンピュータネットワーク等に関する専門知識を生かして、ハイテク犯罪の防止のため産業界との連携強化を推進

相談・広報啓発業務

・ネットワーク犯罪等相談窓口、メール等による相談情報
・セキュリティに関するホームページの開設
・各ブロック、警察署等におけるネットワークに関する講演の実施

・犯罪事例、相談事例の分析
・産業界との連携・広報啓発等に係る施策の立案

連携

関係機関・関係団体

サミット等の国際的な取組み

広報啓発・相談・指導・助言

企業、地方公共団体等

ＩＴ基本法案（高度情報通信ネットワーク社会形成基本法）

第21条　高度情報通信ネットワーク社会形成に関する施策の策定に当たっては、高度情報通信ネットワークの安全性及び信頼性の確保、個人情報の保護その他国民が高度情報通信ネットワークを安心して利用することができるようにするために必要な措置を講じなければならない。

国　民

55

都道府県警察における情報セキュリティ対策

都道府県警察本部
ハイテク犯罪対策プロジェクト

防犯：情報セキュリティアドバイザー ⇔ 捜査：ハイテク犯罪捜査官

不正アクセス禁止法に基づく援助

不正アクセス行為からの防御措置が的確に講じられるよう必要な資料の提供、助言、指導等の援助

相談・広報啓発

・ネットワーク犯罪等相談窓口、メール等による相談
・情報セキュリティに関するホームページの開設
・各ブロック、警察署等におけるネットワークに関する講演の実施

産業界との連携強化

・コンピュータ及びコンピュータネットワーク等に関する専門知識を生かして、ハイテク犯罪の防止のためを推進
・サイバーテロ発生時の 緊急通報体制の確立

不正アクセス禁止法違反の事件捜査
法第3条、法第4条違反の検挙

インターネット等のネットワークを利用した犯罪の捜査

インターネットに対するサイバーパトロール

56

情報セキュリティ意識の向上

警 察 庁

・犯罪事例、相談事例の分析
・国民の情報セキュリティ意識の向上のための政策の立案

連絡・調整

情報セキュリティ・アドバイザー

都道府県警察

連携

関係機関・関係団体

プロバイダ連絡協議会における活動

・連絡体制の確立
・意見交換の実施

不正アクセス禁止法に基づく援助措置に関する業務

・法第6条に基づく、不正アクセス行為からの防御措置が的確 に講じられるよう必要な資料の提供、助言、指導等の援助

相談・広報啓発業務

・ネットワーク犯罪等相談窓口、メール等による相談
・情報セキュリティに関するホームページの開設
・情報セキュリティコミュニティセンターにおけるネットワークに関する研修の実施

企 業 等

広報啓発・相談・指導・助言

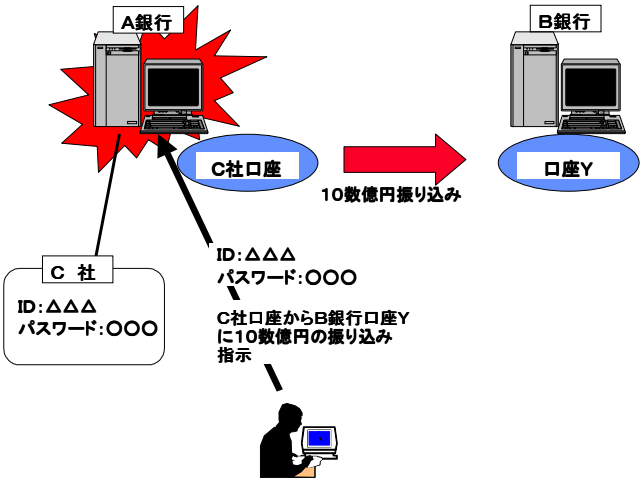
国 民

57

不正アクセス行為を手段としたハイテク犯罪事例

事例1

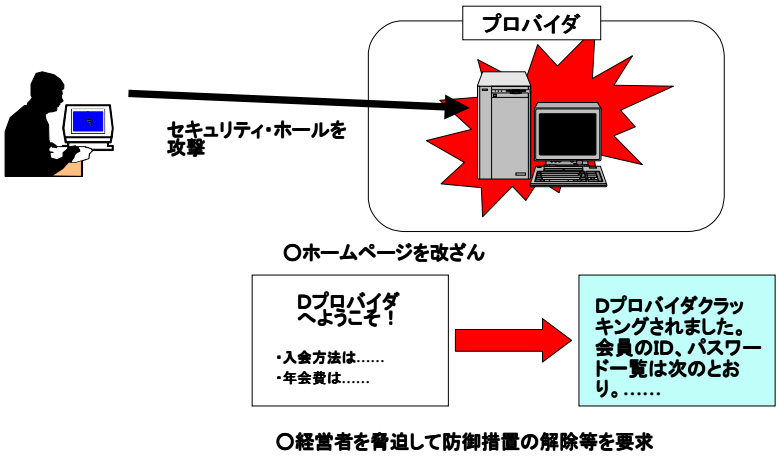
他人のID・パスワードを盗用して都市銀行のコンピュータに不正アクセス行為をし、他行の口座に十数億円の振込をする旨の虚偽の情報を入力し、不法に資金移動を行った。(電子計算機使用詐欺、平成7年2月検挙、愛知)



58

事例2

セキュリティ・ホールを攻撃してプロバイダのコンピュータに不正アクセス行為をし、そのホームページを改ざんして業務を妨害するとともに、同プロバイダ経営者を脅迫して防御措置の解除等を要求した。（電子計算機損壊等業務妨害、強要未遂、平成１０年２月検挙、警視庁）



59

被害現場での証拠保全

証拠保全の必要性

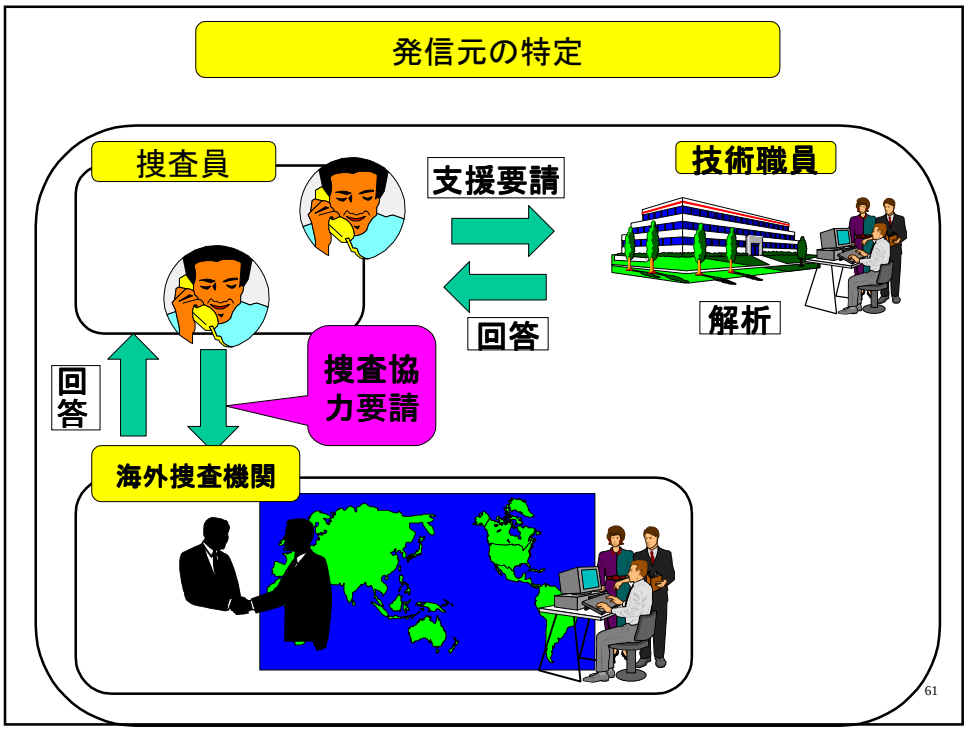
- ログからの発信元・手口の解析
- 消去されたログの復元

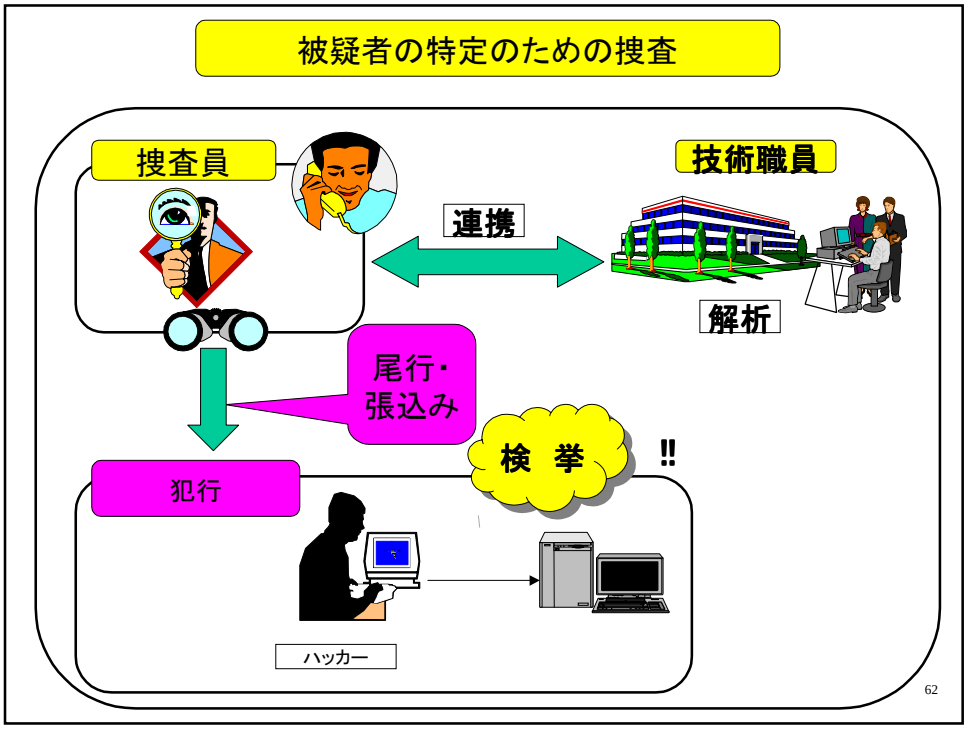
被害者の負担

- 迅速な被害回復の必要性
- 個人のプライバシーの保護の必要性

- ログがない又は消去されている場合
  →ハードディスクの物理コピー
- ログがある場合
  →必要な部分の入手

60


発信元の特定
捜査員
支援要請
技術職員
回答
解析
捜査協力要請
回答
海外捜査機関
61


被疑者の特定のための捜査
捜査員
技術職員
連携
解析
尾行・張込み
検 挙
!!
犯行
ハッカー
62

官庁等ホームページ改ざん事件

１　事案の概要
　平成12年１月から２月にかけて、科学技術庁や総務庁など１１省庁等のホームページが改ざんされるという事件が発生。
　１月２４日に科学技術庁のホームページが改ざんされたのを発端として、ホームページが中国語、英語等の内容に改ざんされたり、データが消去される等連続して発生。

２　対応状況
・警視庁等が電子計算機損壊等業務妨害（刑法第２３４条の２）等の容疑で捜査。
・発信元又は経由地とみられる中国及び米国の捜査機関に対しては、関連情報の提供を依頼。
・捜査に当たっては、被害を受けたコンピュータのハードディスクについて電磁解析を実施。
・被疑者がログを削除したとみられるものや当初からログが存されていないものがあり、解析に大きな困難。

３　解析結果

○　バッファーオーバーフロー攻撃により裏口が作られたもの	８件
○　パスワードを解析し、侵入したもの	２件
○　裏口が複数あり、どれが犯行に使われたかが不明なもの	３件
○　ログがほとんどないため手口が不明なもの	３件

　捜査状況を踏まえて、全省庁に対して防御措置に関する情報を提供。

63

連続発生への対応

・中国人ハッカーによるホームページ書換え事案
（平成13年2月～3月）
・Sadmind/iisワームによるホームページ書換え事案
（平成13年5月）

警察における対応

○　発生の未然防止
○　被害拡大の防止
○　犯人の迅速な追跡

犯罪捜査・援助等
○　迅速な証拠保全
○　犯行手口・接続元の迅速かつ的確な解析
○　犯人の特定のための捜査・国際捜査共助
○　被害の未然防止・拡大防止のための情報提供・広報

被害の未然防止・拡大防止のための情報提供

○ホームページ書き換えプログラムによる事案

- 平成１３年５月１７日：販売企業１８社に対する要請
- 平成１３年５月１０日：事案の概要と注意喚起

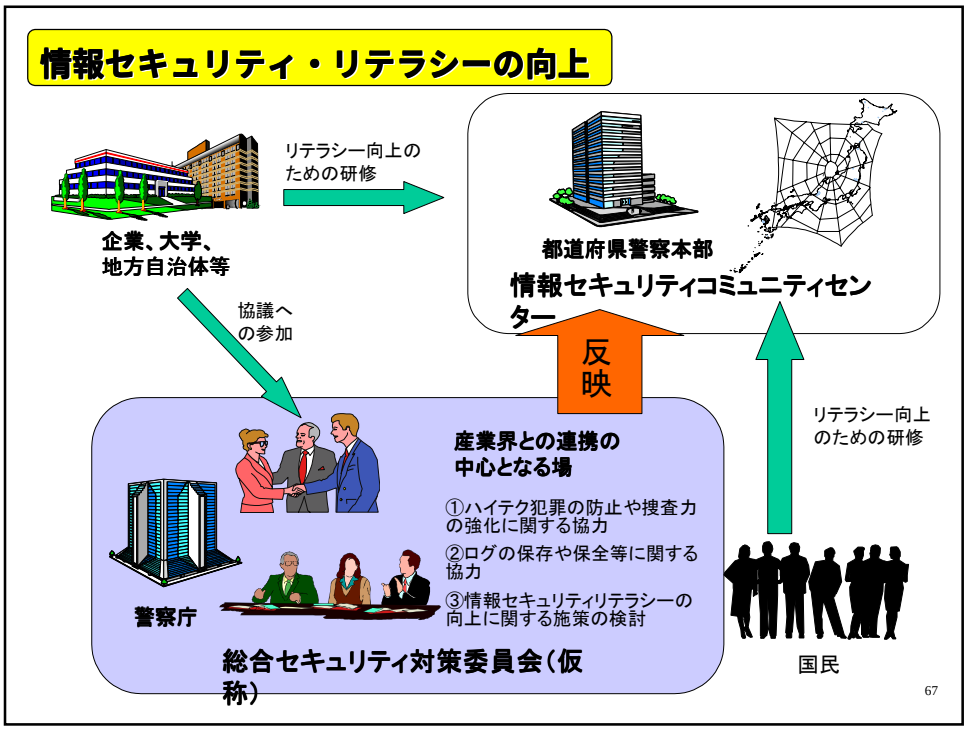
○日本企業等に対するホームページ書き換え事案

- 平成１３年３月　８日：具体的な情報セキュリティ対策に関する情報提供
- 平成１３年２月２３日：事案の概要と注意喚起

65

(4) 警察における今後の取組

66


情報セキュリティ・リテラシーの向上
リテラシー向上のための研修
企業、大学、地方自治体等
都道府県警察本部
情報セキュリティコミュニティセンター
協議への参加
反映
リテラシー向上のための研修
産業界との連携の中心となる場
①ハイテク犯罪の防止や捜査力の強化に関する協力
②ログの保存や保全等に関する協力
③情報セキュリティリテラシーの向上に関する施策の検討
警察庁
総合セキュリティ対策委員会（仮称）
国民
67