@police

インターネット治安情勢
～インターネット観測結果から

警察庁
情報通信局情報技術解析課
サイバーテロ対策技術室
牧野　浩之

@police

講演内容

- 情報セキュリティマネジメントシステム
- インターネット観測結果
- 事例紹介
- 対策

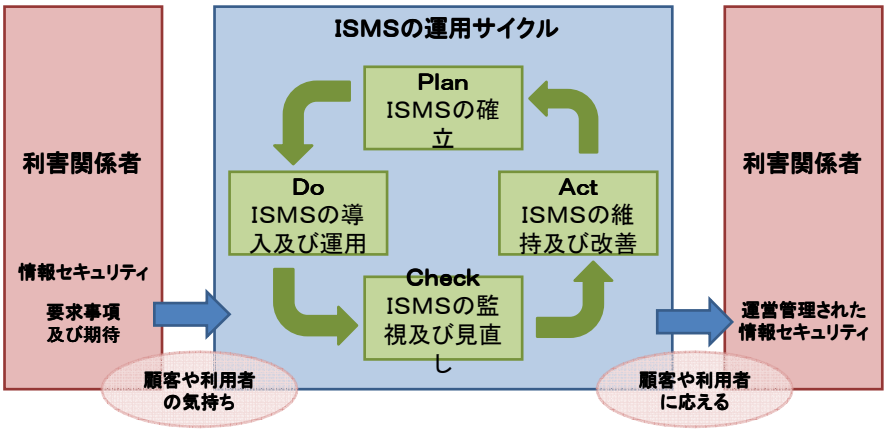
@police

情報セキュリティマネジメントシステム

@police

情報セキュリティマネジメントシステム

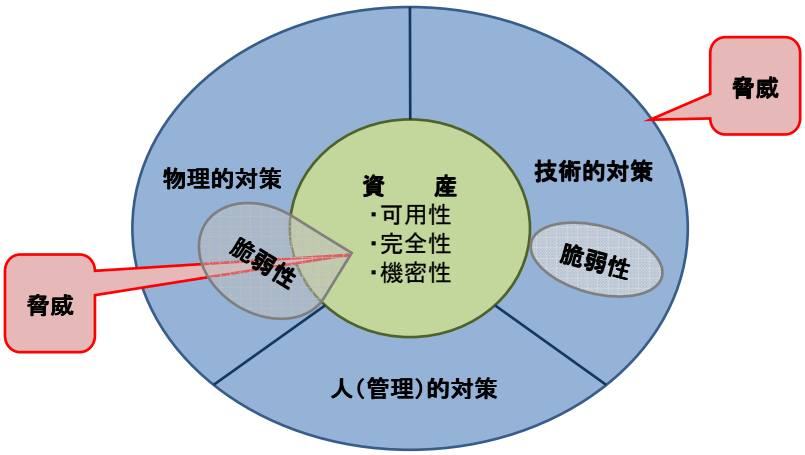
- 情報セキュリティを維持するために方針を確立し、その目的を達成するシステム（しくみ）



@police

情報セキュリティ

- 資産、対策、脆弱性、脅威の関係



@police

脅威の分類例

- 人的脅威

  意図的脅威（Deliberate）

  DoS攻撃、なりすまし、改ざん、侵入、盗難

  偶発的脅威（Accidental）

  停電、断水、人的リソース（スタッフ）不足

- 環境的脅威

  環境的脅威（Environmental）

  落雷、地震、台風

@police

脅威の分類例

- 人的脅威

  意図的脅威（Deliberate）

  DoS攻撃、なりすまし、改ざん、侵入、盗難

  偶発的脅威（Accidental）

  停電、断水、人的リソース（スタッフ）不足

- 環境的脅威

  環境的脅威（Environmental）

  落雷、地震、台風

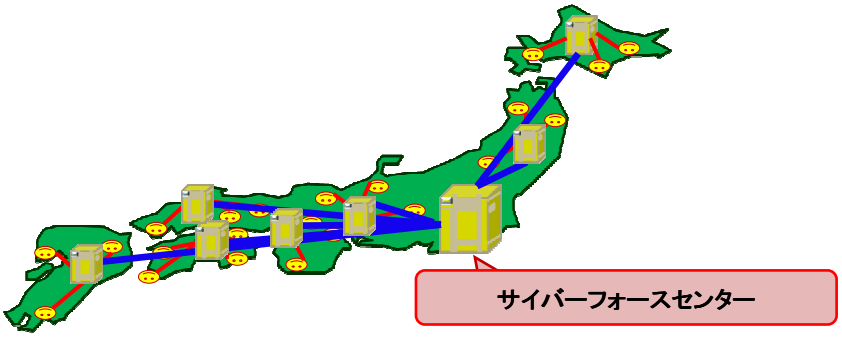
@police

H22年インターネット観測結果

@police

検知ネットワークシステム

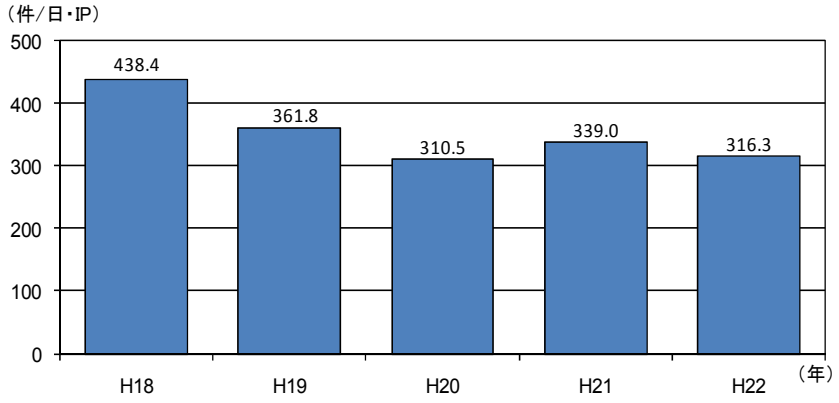
- 全国の警察施設にセンサーを設置、無差別に行われる攻撃の予兆等を定点観測により把握



@police

センサーに対するアクセス

- H22年は、1日に1IPアドレス当たり316．3件のアクセスを観測（4分34秒に1回）



@police

宛先ポート別検知件数上位

- ウイルスや悪意のあるツールによるものと思われるアクセスが上位を占める

順位	ポート	件　数 (1日・1IP当たり)	備　考
1位	445/TCP	152．8件	Windows共有ネットワーク（RPC）等
2位	1433/TCP	20．9件	Microsoft SQL Server等
3位	135/TCP	19．8件	Windows共有ネットワーク（RPC）等
4位	8/ICMP	19．6件	Ping等
5位	22/TCP	10．9件	SSHサービス等
その他		92．3件	

@police

国別検知件数上位

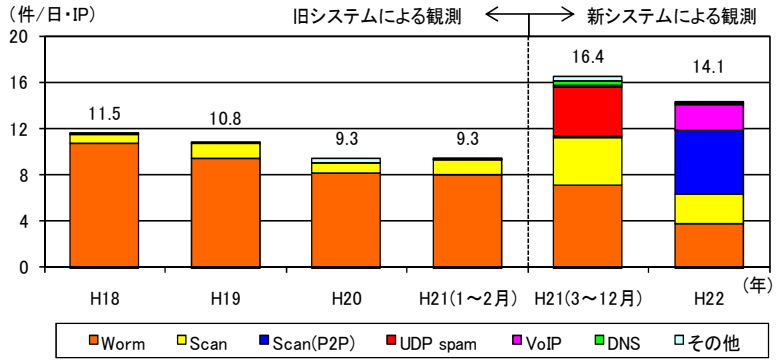
- Conficker ワームによるものと思われるアクセスが多くの国で活発

順位	国・地域	件　数 (1日・1IP当たり)	備　考
1位	中国	64．1件	攻撃ツールによるスキャン行為
2位	日本	52．3件	Conficker ワーム
3位	米国	29．7件	BitTorrent探索
4位	ロシア	16．6件	
5位	台湾	16．5件	オープンリレーメールサーバ探索
その他		137．1件	

@police

シグネチャを用いた不正侵入等の検知

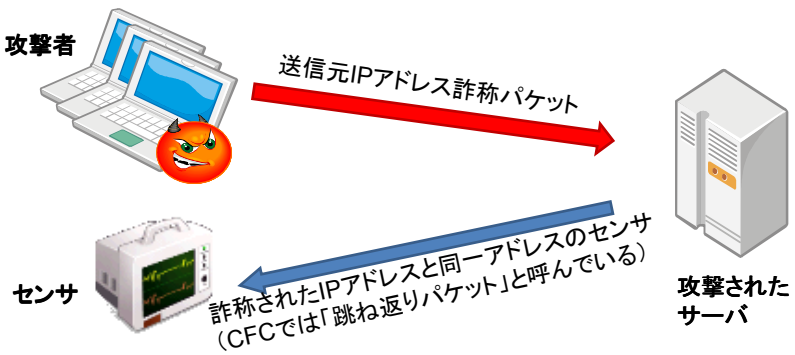
- VoIP/SIP機器の探索と考えられる通信が増加
- スキャンやワームによるものと思われる活動も活発



@police

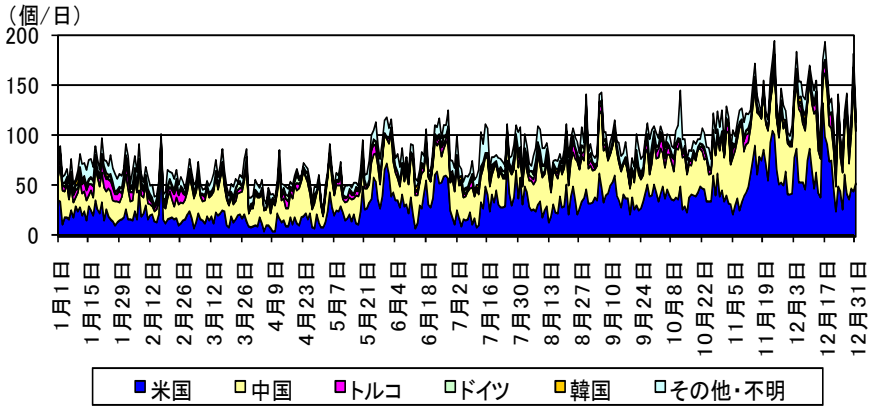
DoS攻撃

- 単一または多数のコンピュータから攻撃対象のコンピュータのサービスを妨害する目的で不正なパケットを送りつける攻撃



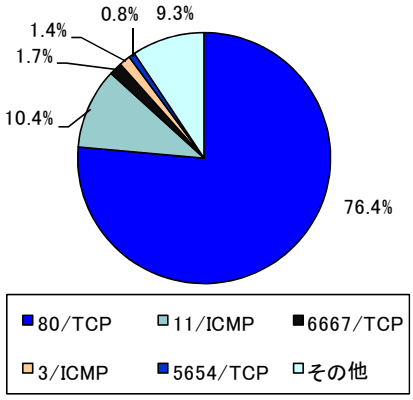
DoS攻撃被害状況

- 発信ポート80/TCPからの跳ね返りパケットの観測からWebサーバへの攻撃状況を把握



日本国内のDoS攻撃被害状況

- 日本国内からのパケット検知件数は、１日当たり１２．２件（１．５IPアドレス）



事例紹介

参　考
　事例の詳細や個々の対策等については、**「情報技術解析平成22年報　～平成22年中のインターネット観測結果等～」**で公開しています。

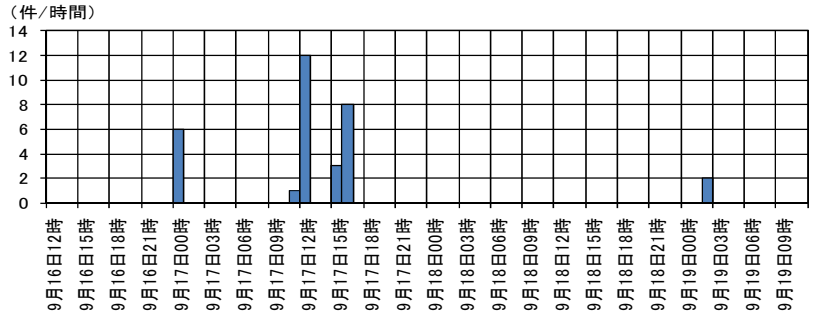
上記報告書は、警察庁セキュリティポータルサイト「＠Police」（URL http://www.npa.go.jp/cyberpolice/index.html ）のインターネット治安情勢のページまたは以下のURLから直接ダウンロードできます。
http://www.npa.go.jp/cyberpolice/detect/pdf/H22_nenpo.pdf

DoS攻撃

DoS攻撃事例1

- H22年9月　日本政府機関

日本の政府機関等に対するサイバー攻撃予告
複数の日本政府機関等のウェブサイトへのアクセスが集中

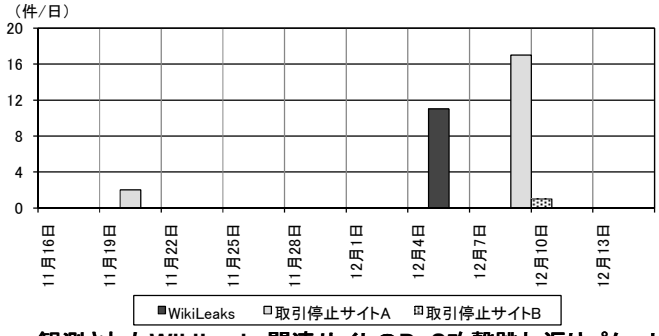


観測された攻撃予告前後のDoS攻撃跳ね返りパケット

DoS攻撃事例2

- H22年12月　内部告発サイト「WikiLeaks」

WikiLeaksの支持グループと支持しないグループとの間で、相互にDoS攻撃が行われたとの報道



観測されたWikiLeaks関連サイトのDoS攻撃跳ね返りパケット

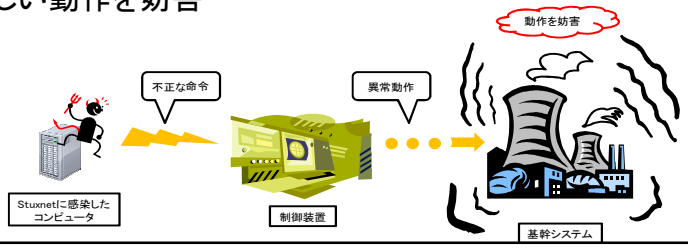
不正プログラムStuxnet

不正プログラムStuxnet

- 標的は、Windowsで動作するドイツのシーメンス社製の監視制御ソフト

  外部記録媒体を経由してコンピュータに感染しネットワーク経由で他のコンピュータに感染

  感染したコンピュータのシーメンス社製の監視制御ソフトを書き換え、制御装置に不正な命令を指示、制御システムの正しい動作を妨害



@police

SIPサーバへの不正接続

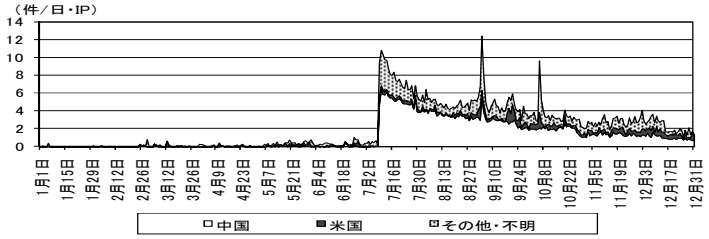
@police

SIPサーバへの不正接続

- H22年7月に、5060/UDPに対するアクセスの急激な増加を検知

  5060/UDPは、IP電話機等のVoIP/SIP機器の通信プロトコルであるSIP（Session Initiation Protocol）で利用

  インターネット上にあるSIPサーバの探索を目的としたものと思われる



5060/UDPに対するアクセスの検知件数

@police

SIPサーバの調査ツール

- 5060/UDPの通信内容の特徴から、複数のグループに分類、グループの一つは、インターネット上で配布されている、SIPサーバを調査するツールと特徴が一致

SIPサーバ調査ツールの機能
指定した範囲内のIPアドレスに対する、SIPサーバの有無の調査
対象のSIPサーバに対し、指定した範囲のユーザ名の有効/無効の調査
対象のSIPサーバ、ユーザ名に対し、パスワードの総当たり攻撃及び辞書攻撃によるパスワードの調査

@police

標的型メール攻撃

@police

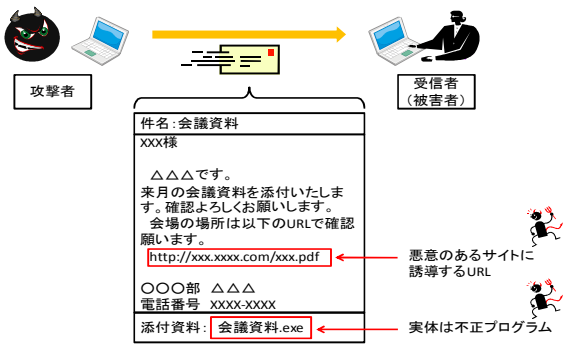
標的型メール攻撃

- 標的型メール攻撃とは、特定の組織や個人に標的を絞って、電子メールを送信する手法による攻撃
- メールに不正なプログラムを添付、不正プログラムを感染させるような悪意のあるサイトへ誘導するリンクが記載されている等
- スピア（槍）のように、標的を絞って攻撃することから、「スピアメール攻撃」とも呼ばれている

@police

標的型メール攻撃の目的

- 目的は、政府関係者や企業関係者のコンピュータに不正プログラムを感染させて、政府機関や企業の機密情報、個人情報等を盗み出すことであると考えられる



@police

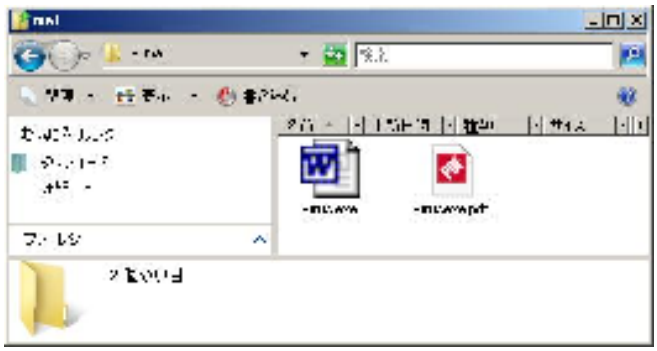
標的型メール攻撃の手口

- 受信者の業務に関連する情報や関心を示すような政治的なニュースや国際的なニュース等がタイトルに用いられる(「東日本大震災~」「福島原発~」等)
- メールの本文に「添付ファイルを確認してください」のように、受信者に添付ファイルを開かせ、不正プログラムを実行させるように仕向けた手法が多く用いられている
- 実行ファイルやPDFファイルが多く、その他にも様々なファイル形式が用いられている
- ゼロデイ攻撃を用いたものがありこれらは、ウイルス対策ソフトで検知されない

@police

標的型メール攻撃の関連技術1

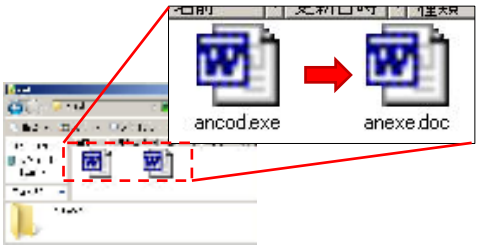
- ファイル種別の偽装
  添付ファイルのアイコンや拡張子を、Wordファイルやファイルに偽装



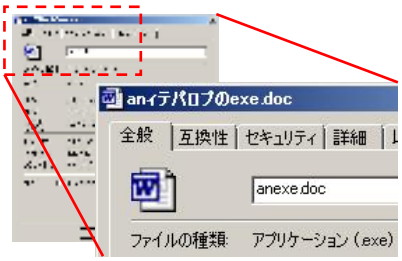
標的型メール攻撃の関連技術２

- 「RLO（Right-to-Left Override）」

  文章を右読みから左読みに変える機能を利用しファイル名「fdp.exe」を「exe.pdf」と表示させ実行ファイルをPDFファイルのように偽装



ファイル名の途中からも可能
「ancod. exe」を「 anexe.doc 」と表示



ファイルのプロパティ表示に矛盾

標的型メール攻撃の関連技術３

- 代替データストリーム

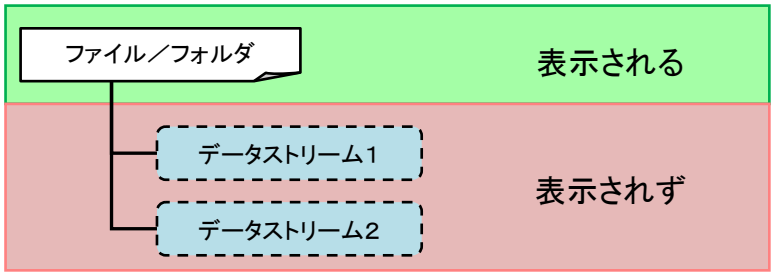
（ADS：Alternate　Data　Streams）

一つのファイルやフォルダが複数のストリームを持つことができるWindowsの機能の一つ

代替データストリームを使用したファイルやフォルダは、Windowsのバージョンによってはエクスプローラやタスクマネージャに表示されず、発見や駆除が非常に困難

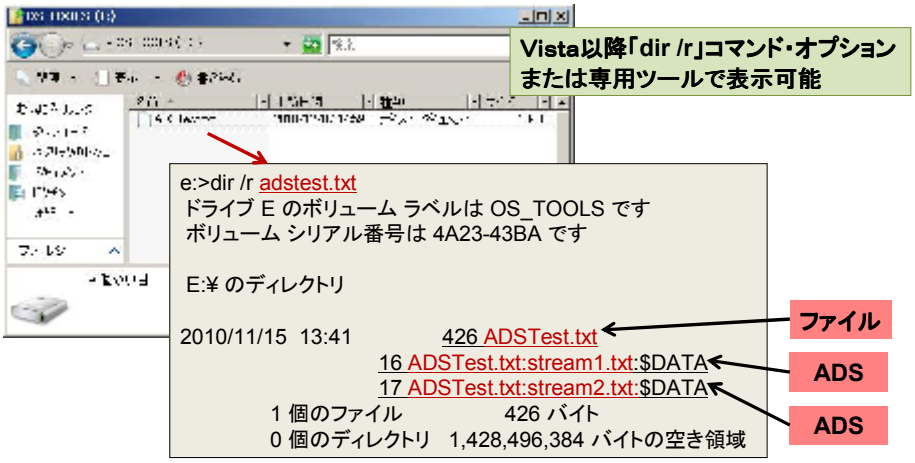
代替データストリーム
ADS：Alternate　Data　Streams

- NTFSの機能の一つ
- ファイルやフォルダにテキストやバイナリデータをストリームとして個別に保存できる機能
- 「ファイル名：データストリーム名」で記述



代替データストリーム（ADS ）

- Windowsのエクスプローラでは表示されない



@police

標的型メール攻撃の関連技術4

- ヒープスプレー（heap spray）

  Windowsが持っている不正プログラムの実行防止機能を回避し、攻撃成功率を高めるための手法

  ヒープと呼ばれるメモリ領域に対して不正なプログラムをスプレーで塗りつぶすように大量に書き込み不正プログラムが実行される可能性を高めるもの

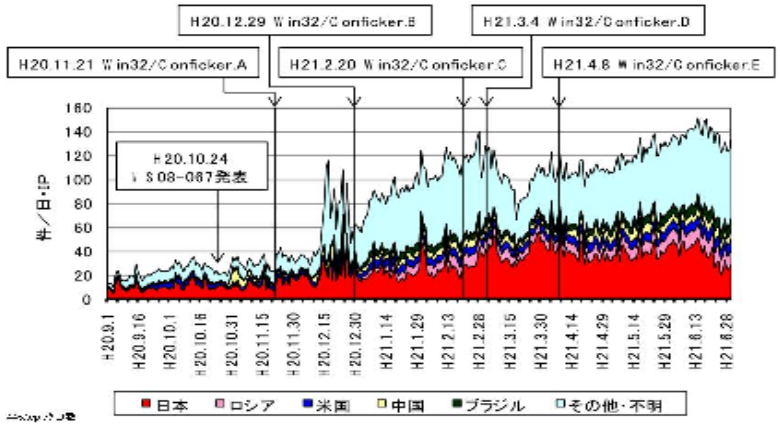
@police

セキュリティ更新プログラム公開

@police

セキュリティ更新プログラム公開

- セキュリティ更新プログラム公開直後から悪意のある活動が発生



@police

対　策

@police

悪意のある攻撃に対する配意

- 扱っている情報（資産）の価値の認識
- インターネット上の脅威の認識
- 被害発生防止対策に加えて、被害拡大防止対策の実施
- たとえクラウドが対象となっても基本的な防御姿勢は変わらない

@police

被害拡大防止対策

- 被害発生防止対策に加えて、被害拡大防止対策の実施

  被害発生の原因やメカニズムの分析結果が広く知られるにつれ、被害発生を完全に押さえることは不可能ということが認識されてきた

  被害が発生したときにその被害規模や深刻度があまりに大きいものが多くみられた

  リスク管理の問題として捉えられるようになってきている。最近では、事業継続性についても考慮されるようになっている

@police

最低限実施すべき対策

- OSやアプリケーションの更新プログラムの適切な適用
- ウイルス対策ソフトやファイアウォールソフト等の適切な運用
- メールに添付されたファイルや、メール中のリンク先を不用意に閲覧しない

@police

コンピュータの利用状況によって有効な対策

- パソコンやユーザ・アカウント等の使い分け
- 使用していないパソコン等のシャットダウン
- 不要な機能を導入しない、又は使用不可にする
- パスワード等の秘密データを安易にパソコン等へ保存しない
- セキュリティ更新プログラムが提供されなくなったソフトウェアの適切な更新

企業等の情報セキュリティ担当者が考慮すべき対策例

- パソコン、ウェブサーバ等の機器の適正な設定
- データベースを運用している場合は、外部からのデータベースへの不正な命令を遮断するといった、データベースを不正に操作されないような対策についての検証
- ログ等の定期的な確認による、異常の早期発見と必要な措置
- 対策の実施前に不具合の発生等を検証するため、各種ソフトウェアやコンピュータ機器の販売元等から提供されているセキュリティ情報の確認やシステムの不具合等が発生しないことを確認する等配意が必要

おわり

警察庁
情報通信局情報技術解析課
サイバーテロ対策技術室
牧野　浩之