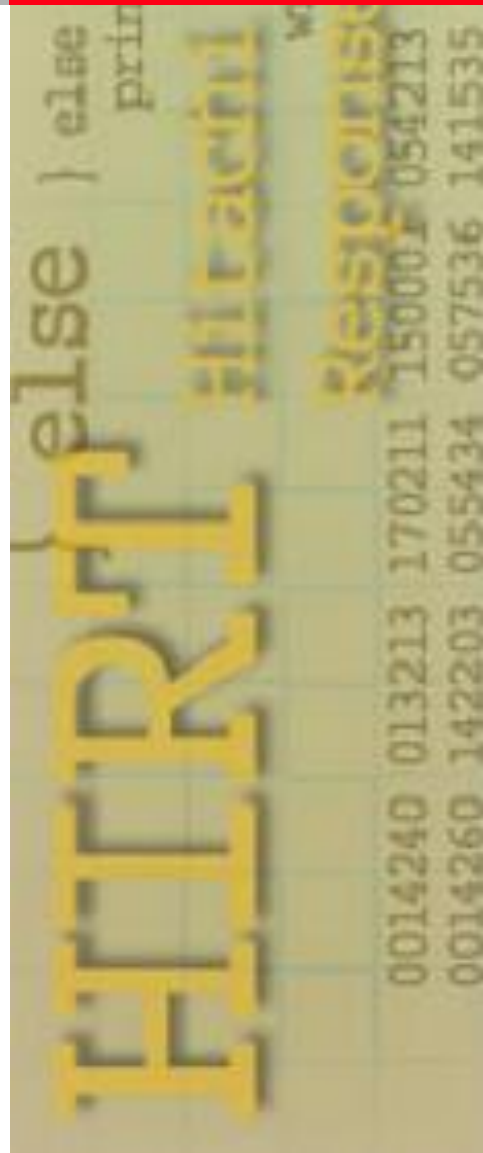
HITACHI
Inspire the Next

セキュリティインシデントから学べること

2016年11月09日

寺田真敏
Hitachi Incident Response Team
http://www.hitachi.co.jp/hirt/

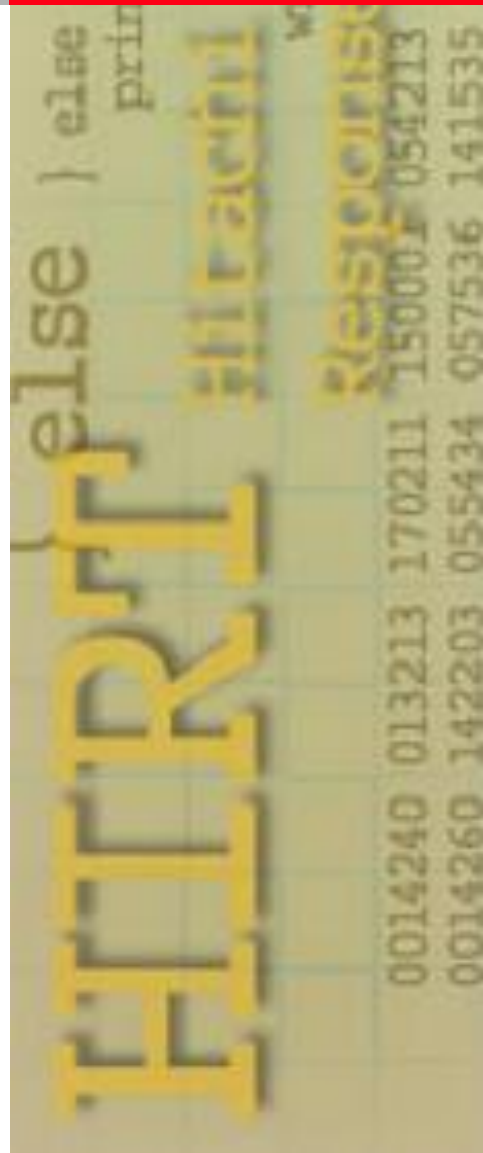


Contents

HITACHI
Inspire the Next

日々、不正アクセス、コンピュータウイルスへの感染など、セキュリティに関係した事件(セキュリティインシデント)が発生しています。
そこで、本講義では、これまでに発生した代表的なセキュリティインシデントを題材に、セキュリティインシデントから学べることを一緒に考えてみたいと思います。

1. インシデントを振り返る
2. 不正アクセスに関する理解を深める
3. シーサート活動



Hitachi Incident Response Team

情報セキュリティ10大脅威 2016

- **2015年に発生し、社会的に影響が大きかったと考えられる情報セキュリティの脅威に関する事故・事件から選出。**

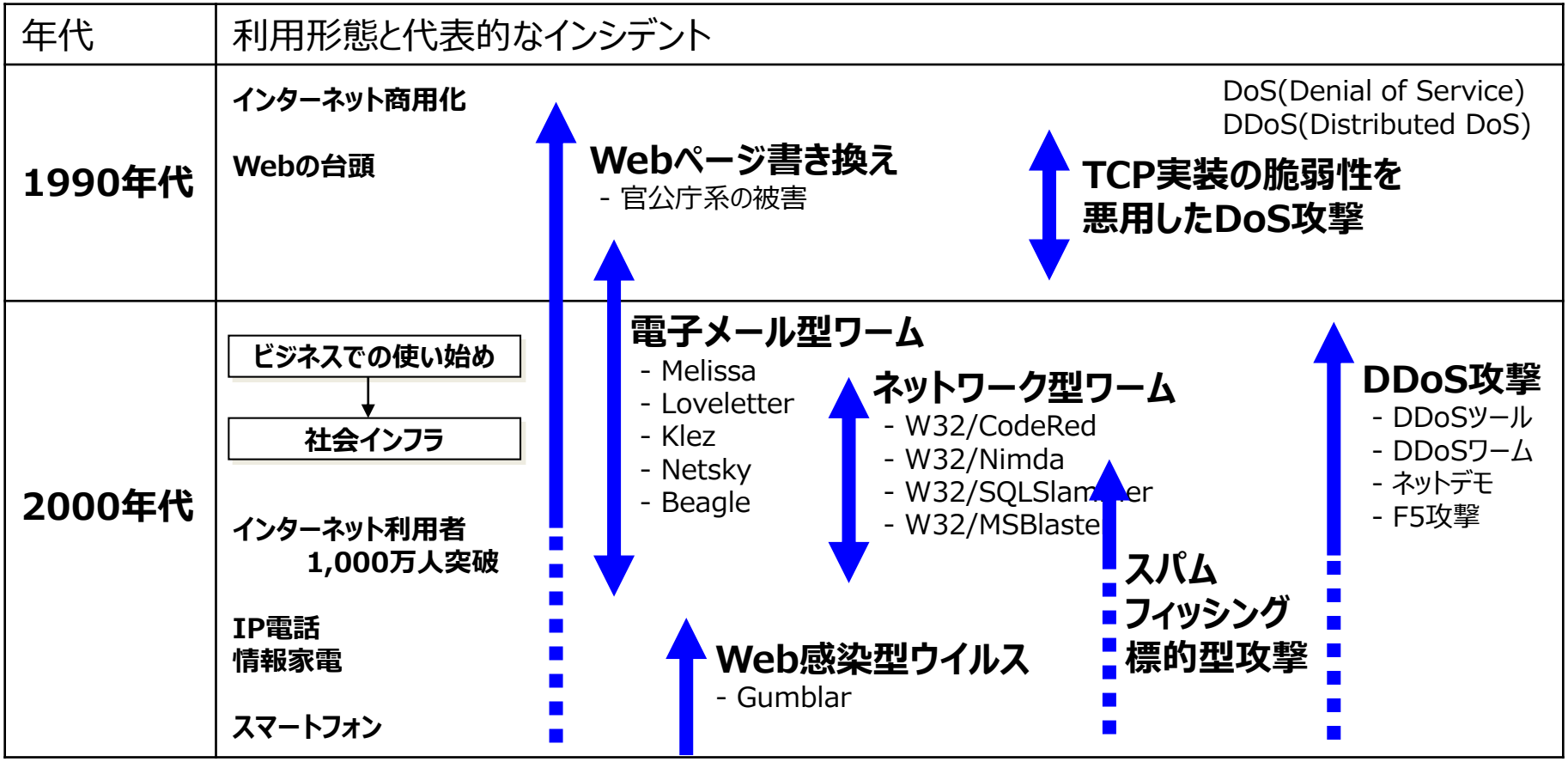
総合順位	脅威	個人	組織
第1位	インターネットバンキングやクレジットカード情報の不正利用	第1位	第8位
第2位	標的型攻撃による情報流出		第1位
第3位	ランサムウエアを使った詐欺・恐喝	第2位	第7位
第4位	ウェブサービスからの個人情報の窃取	第7位	第3位
第5位	ウェブサービスへの不正ログイン	第５位	第9位
第6位	ウェブサイトの改ざん		第５位
第7位	審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ	第3位	
第8位	内部不正による情報漏えい		第2位
第9位	巧妙・悪質化するワンクリック請求	第4位	
第10位	対策情報の公開に伴い公知となる脆弱性の悪用増加		第6位

出典　情報セキュリティ10大脅威 2016
http://www.ipa.go.jp/security/vuln/10threats2016.html

インシデント(セキュリティインシデント)とは・・・

セキュリティ上の問題事象

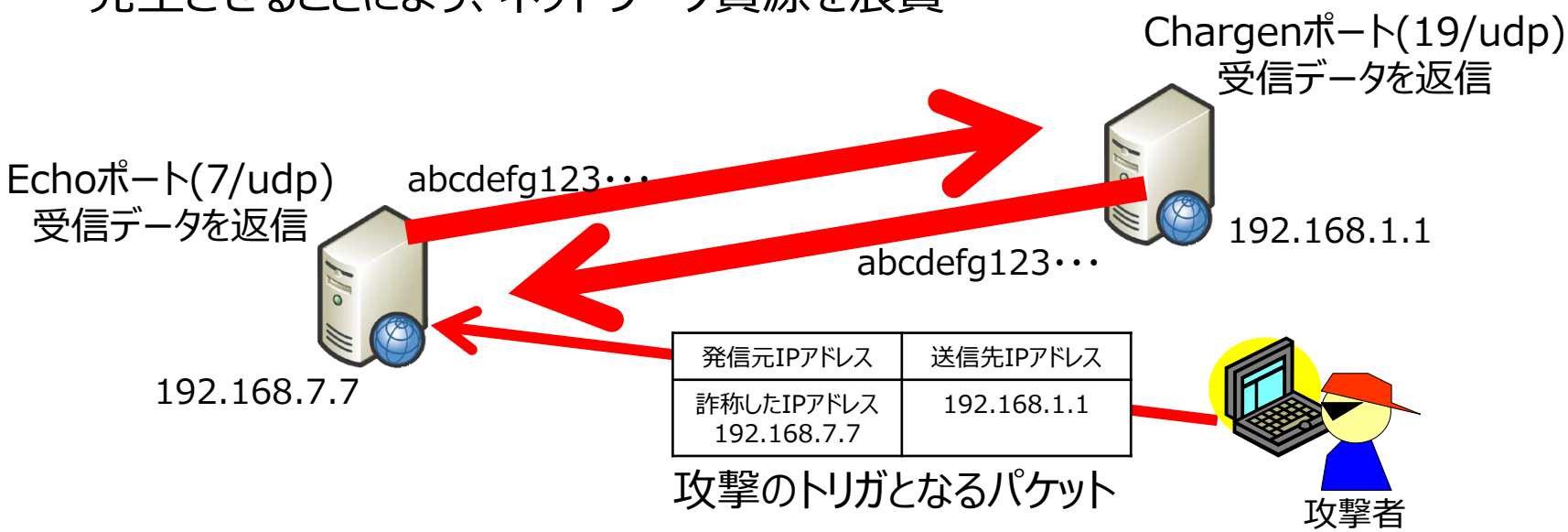
- システムを運用している際に発生するセキュリティ上の問題事象のこと



DoS(Denial of Service)攻撃

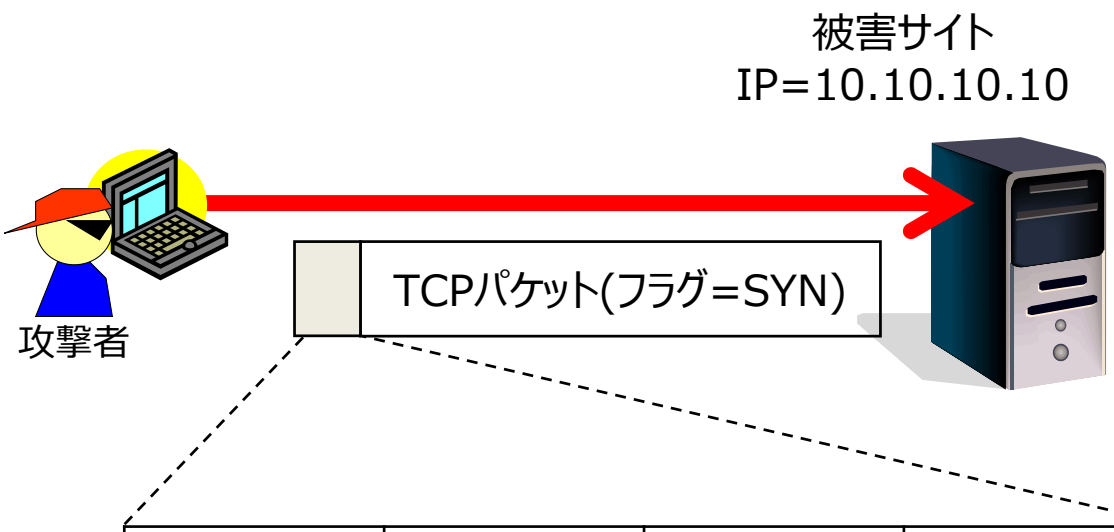
サービス停止や運用妨害を目的とした攻撃：多種多様

- **電子メール爆弾(電子メールの大量送付など)**
  サーバ資源の浪費
- **ブラウザDoS**
  クライアント資源の浪費
- **UDP Echo Flooding 【 パケットレベルのDoS攻撃 】**
  UDPのEcho(7)とChargen(19)を使って通信の無限ループを発生させることにより、ネットワーク資源を浪費



サービス停止や運用妨害を目的とした攻撃：脆弱性悪用

- **LAND 【 パケットレベルのDoS攻撃 】**
  発信元IPアドレス／ポート番号と送信先IPアドレス／ポート番号とを同じに設定したTCP SYNパケットを送信



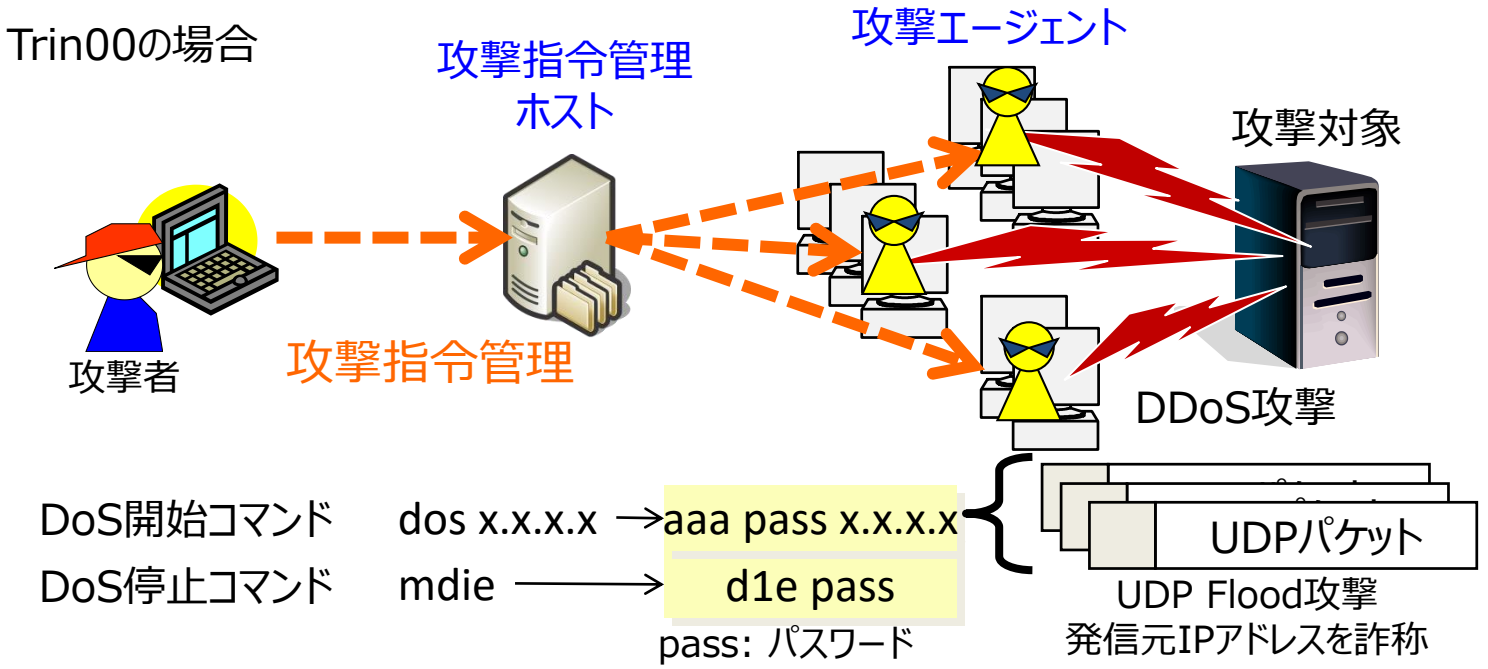
発信元IPアドレス	送信先IPアドレス	発信元ポート番号	送信先ポート番号
10.10.10.10	10.10.10.10	80	80

「発信元IP＝送信先IP」、「発信元ポート番号＝送信先ポート番号」を設定したTCPパケットを用いることで、LAND攻撃未対策のシステムの場合には、通信不能状態に陥れることができる。

DoS(Denial of Service)攻撃

サービス停止や運用妨害を目的とした攻撃： n倍化

- **DDoSツール**
  - 多数サイトに攻撃エージェントを手動で配備し、攻撃エージェントを制御しながらDoS攻撃を実施する。
  - Trinoo(Trin00)、TFN(Tribe Flood Network)、TFN2K(TFN2000)など



Hitachi Incident Response Team

実験室から実システムへ

1986年01月　Brain (IBM PC互換機で発見された最初のコンピュータウイルス)
1986年　PC-Write (最初のトロイの木馬)
1986年12月　Virdem (最初のファイル感染型ウイルス)
1987年10月　Cascade (暗号化された最初のウイルス)
1987年12月　Christmas Tree (自己伝搬による脅威が表面化した最初のワーム)
1988年11月　Morris Worm (インターネットを震撼させた大規模ネットワーク型ワーム)
⇒バッファオーバーフロー攻撃などサーバプログラムの脆弱性を利用
1989年12月　AIDS (最初のランサムウェア)

コンピュータウイルスという名前は、1984年にFred Cohenが発表した論文「Computer Viruses - Theory and Experiments」に由来する。この論文の中で、コンピュータウイルスとは、他のプログラムに寄生して広がっていくプログラムとして定義された。また、ワームという名前は、1975年John BrunnerのSF小説「The Shockwave Rider」の中で登場する自己増殖型のプログラムtapewormに由来すると言われている。1986年になると実社会に被害を与えるコンピュータウイルスが出現し始めた。

1. 1990年代前半

学術系サイトでのインシデント発生

1990年	1260 (最初に確認されたポリモーフィック型ウイルス)
1991年04月	Tequila (感染拡大の発生した最初のポリモーフィック型ウイルス)
1991年	Michelangelo (ウイルスの存在自身が社会的な問題となったウイルス)
1994年02月	パスワード大量盗難事件 ⇒パケットモニタリングによる認証情報の盗聴
1994年12月	Good Times (最初のHOAXウイルス)
1995年01月	ケビン・ミトニック事件 ⇒IPアドレス偽装によるコネクションハイジャック
1995年07月	Concept (初めて発見されたマクロウイルス)

1990年にブルガリアでオンラインのウイルス交換掲示板 (VX: Virus eXchange BBS)が立ち上がり、ウイルスのコードやアイデアの交換が始まった。翌年の1991年にはブルガリアのDark AvengerがThe Mutation Engine(MtE)と名付けたミューテーション型ウイルス作成キットを開発した。1992年になると、ウイルス作成キットVirus Creation Laboratory(VCL)、The Phalcon/Skism Mass Produced Code Generator(PM-MPC)が登場し、コンピュータシステムを使えるユーザであれば、誰でもウイルスを作れるようになった。

1. 1990年代後半

商用系サイトでのインシデント発生

1996年07月　Laroux (Excelファイルを感染対象とする最初のマクロウイルス)
1996年08月　米国司法省Webサイトの書き換え
⇒Webの普及に伴う脆弱性の顕在化
1996年09月　米国の大手プロバイダPANIXへのDoS攻撃
⇒パケットレベルのDoS攻撃の出現
1997年08月　Web cgi-binプログラムへの攻撃
⇒脆弱性探査ツールの高度化

脆弱性発見に伴うインシデントが日本で多発するまでに時差あり

1999年01月　W32/Ska (電子メールを利用して感染を広げる先駆け的なウイルス)
1999年02月　W97M/Melissa (電子メールで自己伝搬する最初のワーム型マクロウイルス)

1998年末から、電子メールを介して流布するトロイの木馬、ワームが出現し始めた。トロイの木馬によっては、感染したコンピュータをリモートからインターネット経由で自由にアクセスできる状態にしてしまうなど、不正アクセスによって発生する被害と同様な被害を伴うようになった。特に、1999年に入るとユーザ名やパスワード情報を盗み出す、電子メールに自分自身を添付し送信し自己伝搬するなど、「トロイの木馬」「ワーム」に該当するウイルスの数は激増した。

W97M/Melissaウイルス出現後から時差なしの世代へ

2000年01月	国内官公庁関連Webサイトの書き換え事件
2000年02月	米国有名サイトへのDDoS攻撃事件 ⇒DDoS攻撃の出現
2000年05月	VBS/Loveletter
2001年02月	国内複数Webサイトの書き換え事件
2001年05月	Solaris/Sadmind ⇒サーバプログラムの脆弱性を攻撃
2001年07～08月	W32/CodeRed I/II
2001年07月	W32/Sircum (情報漏えいを伴うウイルスの先駆け)
2001年09月	W32/Nimda ⇒サーバ/クライアントプログラムの脆弱性を攻撃

ウイルス世代へ
時差なし世代へ

電子メール型ワームが台頭し、2000年だけでも電子メールを介して自己伝搬する数十種類のワームが発見された。特に、大きな変化は、サーバプログラムの脆弱性を攻撃するネットワーク型ワームの流布であり、人手の介入を必要としない自己伝搬の方法が主流となり始めた。

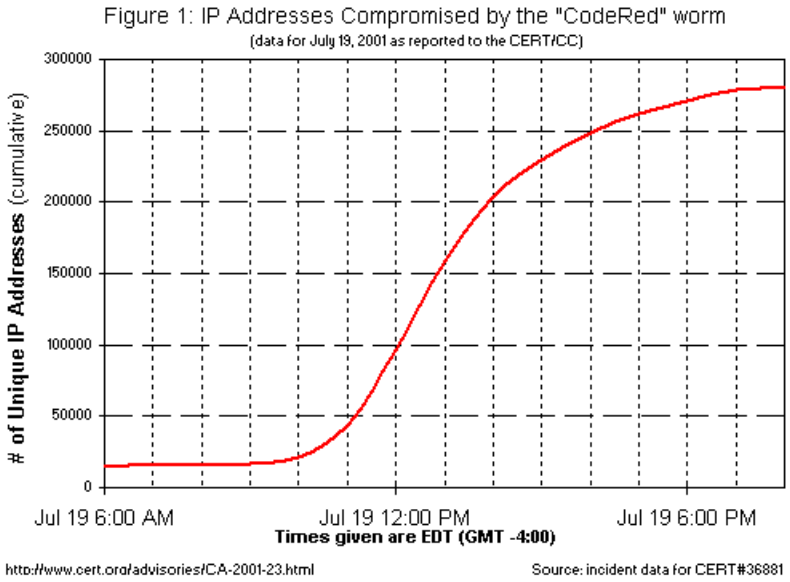
ネットワーク型ワーム W32/CodeRed I/II

- **数時間のうちに20万台以上の計算機が感染した。**

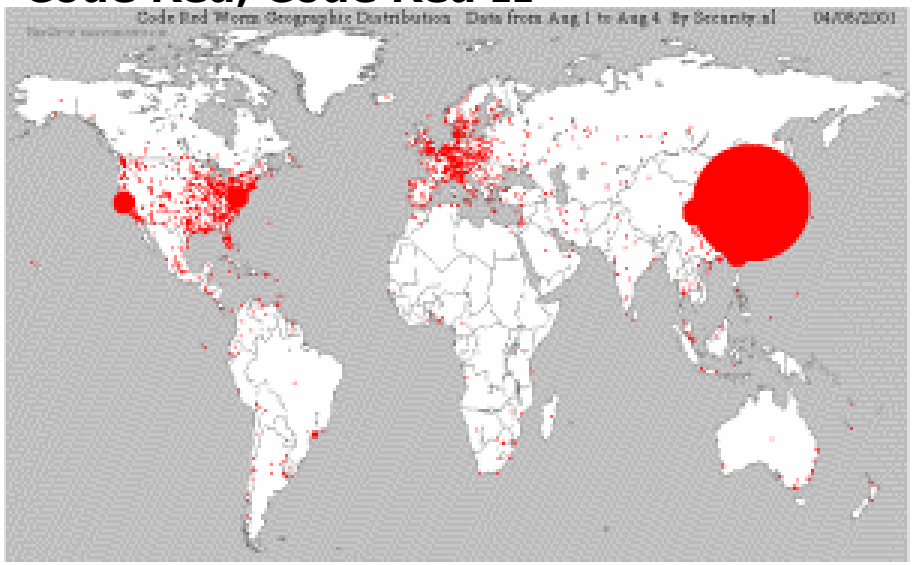
2001年6月18日　「MS01-033: Index Server ISAPI エクステンションの未チェックのバッファによりWebサーバが攻撃される」を公表

2001年7月18日　W32/CodeRed I 発生

2001年8月6日　W32/CodeRed II 発生



Code Red, Code Red II



出典　CERT Advisory CA-2001-23 Continued Threat of the "Code Red" Worm
http://www.cert.org/advisories/CA-2001-23.html

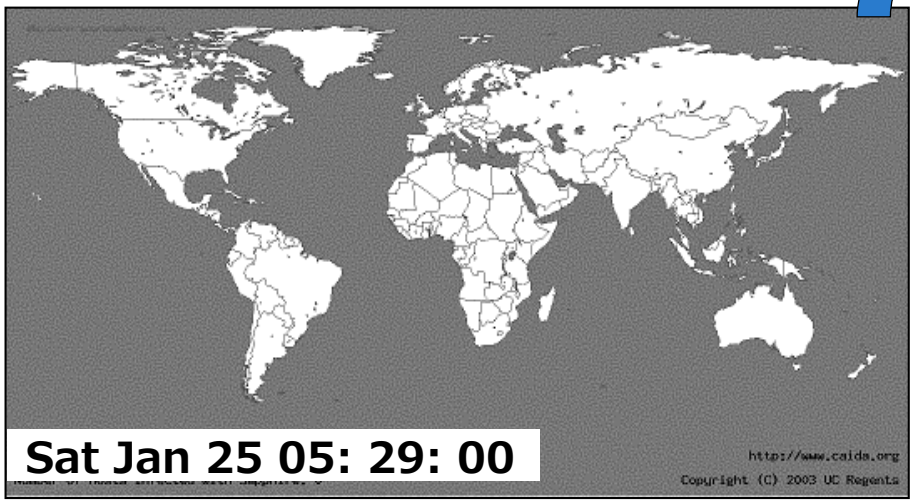
ネットワーク型ワーム W32/SQLSlammer

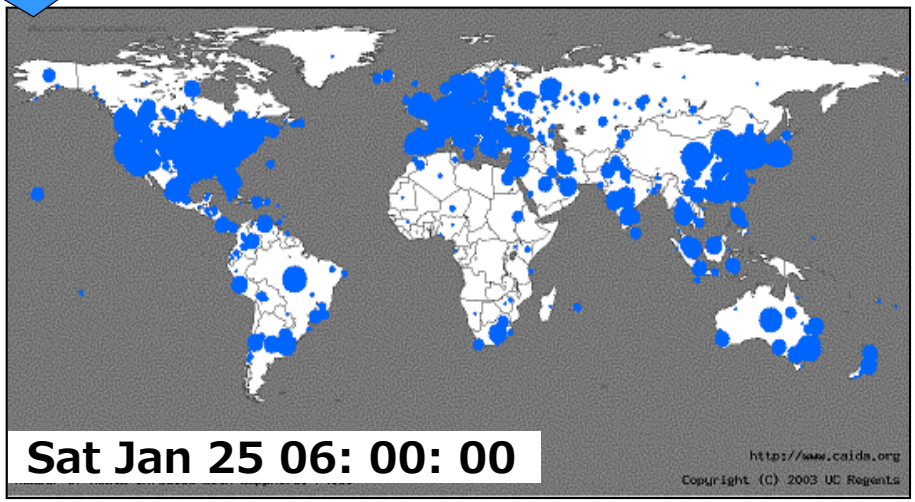
- **感染動作自体がインターネットをDoS状態に陥れる。**

2002年7月25日　「MS02-039: SQL Server 2000 解決サービスの
バッファのオーバーランにより、コードが実行される」を公表

2003年1月25日　W32/SQLSlammer 発生

僅か30分　**10分間のうちに脆弱性のあるホストのうち90%が感染したといわれている**





出典　Cooperative Association for Internet Data Analysis
http://www.caida.org/

2005年～2006年

Hitachi Incident Response Team

新たなインシデント形態へ

- **大規模感染型ネットワーク型ワームは影を潜め、2005年6月頃から、特定の組織のみを狙った標的型攻撃(Targeted Attack)の存在が報告され始めた。**

2003年1月	W32/SQLSlammer	ネットワーク型ワーム全盛期 (均一的かつ広範囲に渡る被害)
2003年8月	W32/MSBlaster	
2004年5月	W32/Sasser	
2005年8月	W32/Zotob	
2005年	SQLインジェクション攻撃によるWebサイト侵害	
	Winny、Shareによる情報流出	金銭を目的とした犯罪活動 (類似した局所的な被害)
	フィッシング	
	スパイウェア	
2006年	ワンクリック不正請求	
	偽セキュリティソフトの押し売り	
	文書ソフト(Word、Excel等)の脆弱性を用いたウイルス感染	
	標的型フィッシング	スパイ型犯罪活動 (局所的な被害)
	標的型メール	

活動基点が怪しいから普通(怪しくない)に移行

- **攻撃対象もOS/アプリケーションからユーザへ**

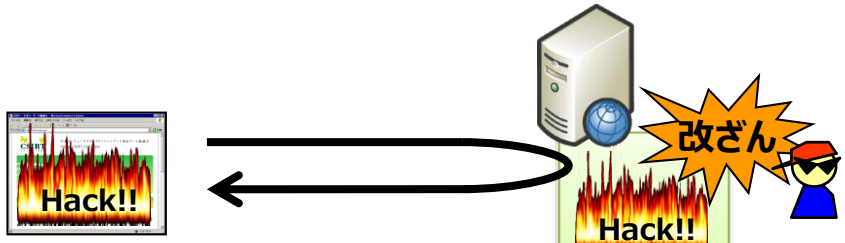
2007年　**iframeなどのサイト誘導を用いたウイルス感染**
⇒活動基点となる誘導元Webサイトは、
怪しいWebサイトから普通のWebサイトに移行

2008年　**電子メールを利用したウイルス埋め込みPDFの配布**
⇒ウイルスの添付された電子メールは、
怪しい電子メールから普通の電子メールに移行

USBメモリ型ウイルスの流布
⇒フロッピーディスクを介した流布の再来
⇒USBメモリの自動再生／自動実行を利用した
ソーシャルエンジニアリング攻撃

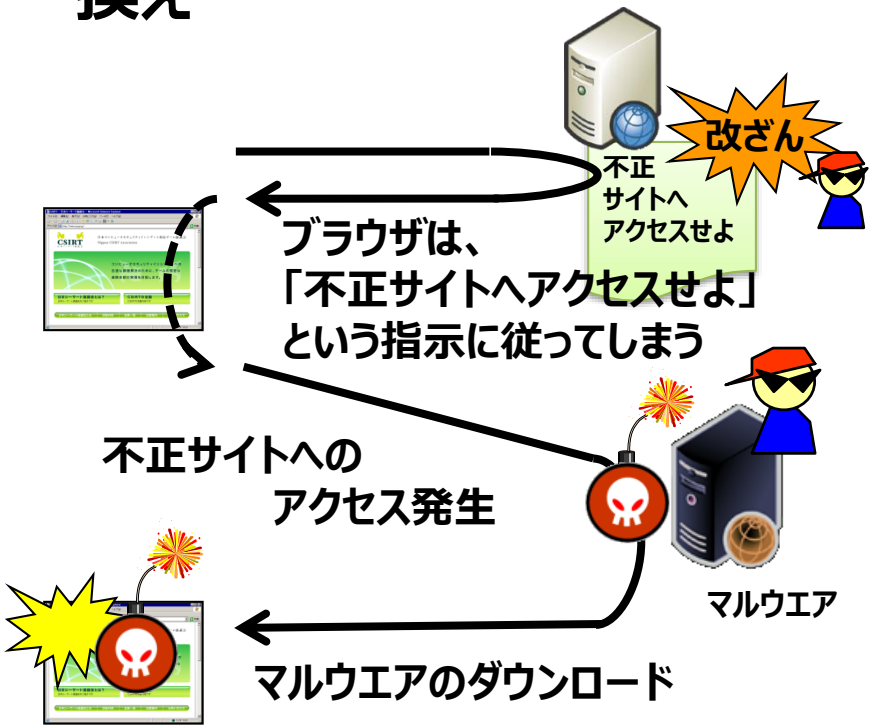
単純なページ書き換え vs 不正なサイトへの誘導

- 単純なページ書き換え



改ざんサイトにアクセスすると
改ざんされた画像が表示される

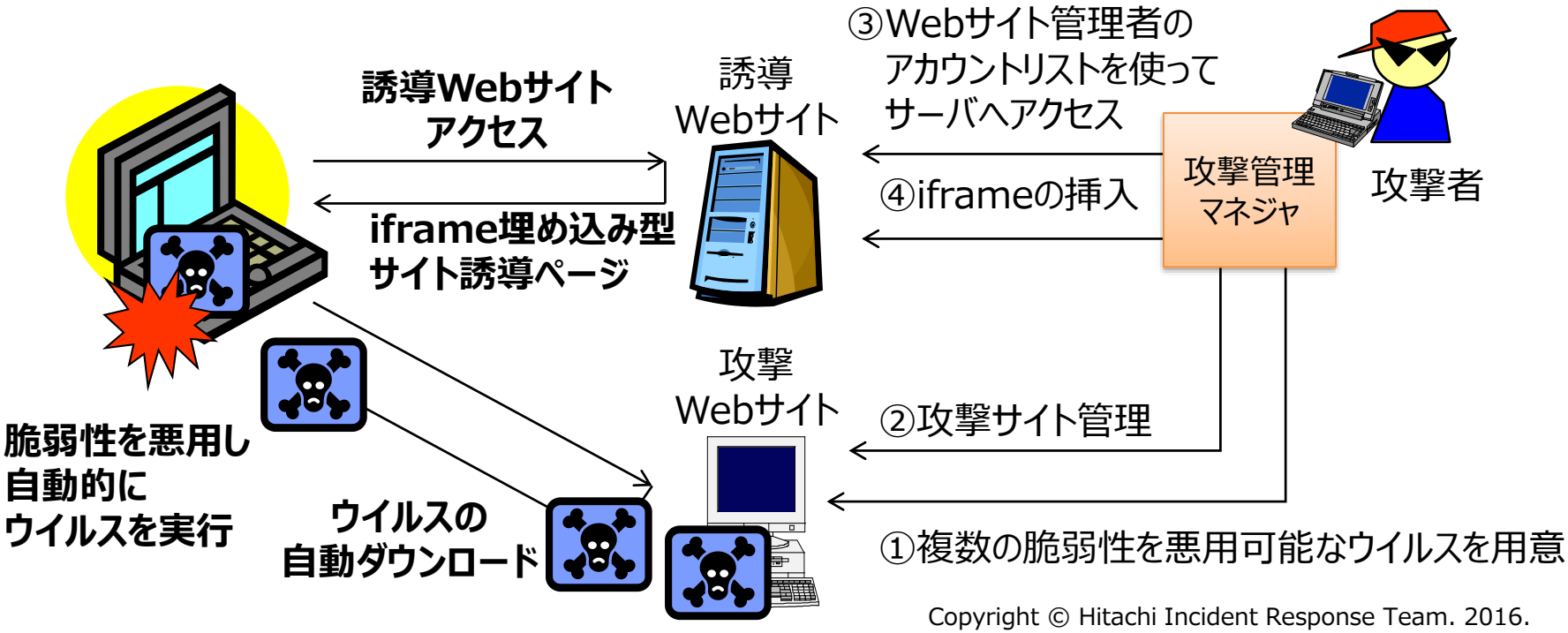
- 不正なサイトに誘導する書き換え



改ざんサイトにアクセスすると
不正サイトに誘導され、
パソコンがマルウエアに感染する場合がある

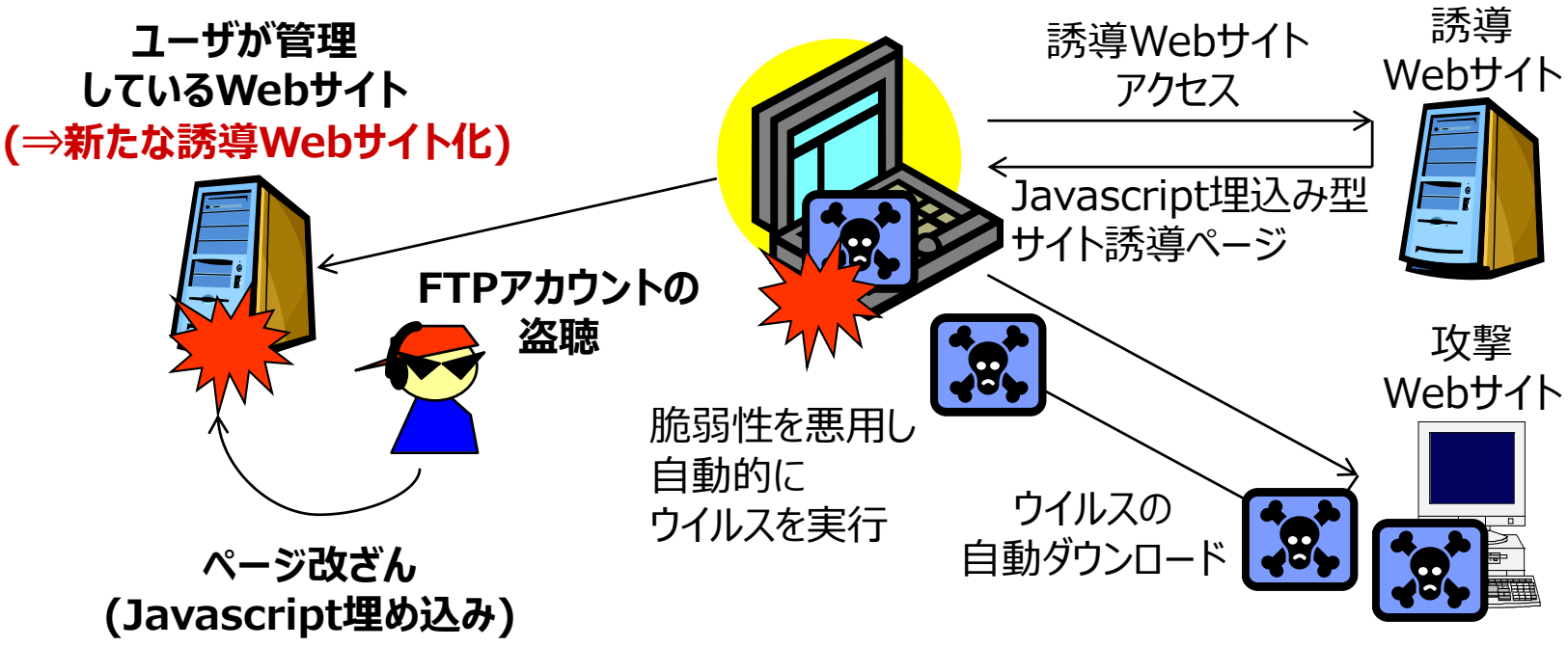
iframeなどのサイト誘導を用いたウイルス感染

- **ページ改ざんの新たな悪用形態**
  Webサイトのページを改ざんして、サイト訪問者をウイルスサイトへ誘導する細工を仕掛ける。改ざんされたWebサイトを閲覧したサイト訪問者は、自動的にウイルスサイトに誘導される。結果として、不正なプログラムをダウンロードしたり、情報を盗み出したりするウイルスに感染する恐れがある。



サイト誘導を用いたウイルス感染活動のシステム化

- **Gumblar：アカウント盗聴による感染拡大サイクルの実現**
  Webサイトのページを改ざんして、サイト訪問者を攻撃Webサイトへ誘導する細工を仕掛ける。 誘導Webサイトを閲覧したサイト訪問者は、自動的に攻撃Webサイトに誘導され、ウイルスに感染してしまう。さらに、盗聴したFTPアカウントを用いて新たな誘導Webサイト化を試みる。



2010年 Advanced Persistent Threat

攻撃対象を狙い撃ちした高度な潜伏型攻撃

- **特定組織を対象とし(標的型)、組織内ネットワークを活動基点とした(潜伏型)侵害活動**

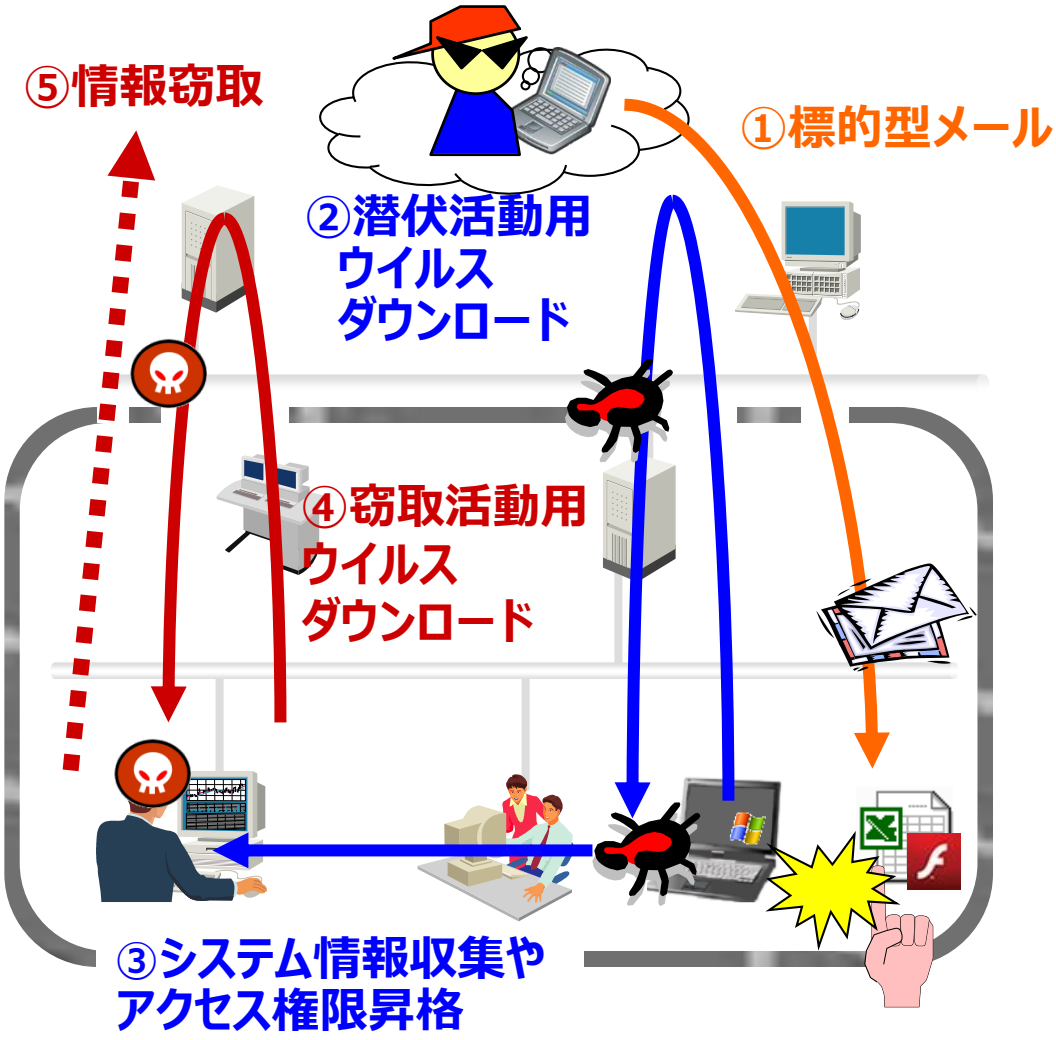
A	**Step1(侵入)：ソーシャルエンジニアリングを用いた攻撃** ● 標的型メール ● 悪意あるWebサイトへの誘導(⇒ウイルス: Gumblar) ● USB経由(⇒ウイルス: Conficker)
P	**Step2(潜伏)：潜伏中は外部との通信環境を維持** ● 攻撃指令管理ホストとの接続 ● 新たな機能や自身の更新のためファイルダウンロード
T	**Step3(窃取や妨害)：最終目標(脅威)に合わせて変更** ● ソフトウエア構成管理システムへの攻撃(⇒オーロラ攻撃) ● 機密情報の窃取(⇒ナイトドラゴン) ● 制御システムの動作妨害(⇒スタクスネット)

情報窃取の攻撃シナリオ

Step1：侵入活動・・・①
ウイルス添付メールによるパソコンへの感染

Step2：潜伏活動・・・②③
システム情報収集やアクセス権限昇格

Step3：窃取活動・・・④⑤
機密情報の窃取

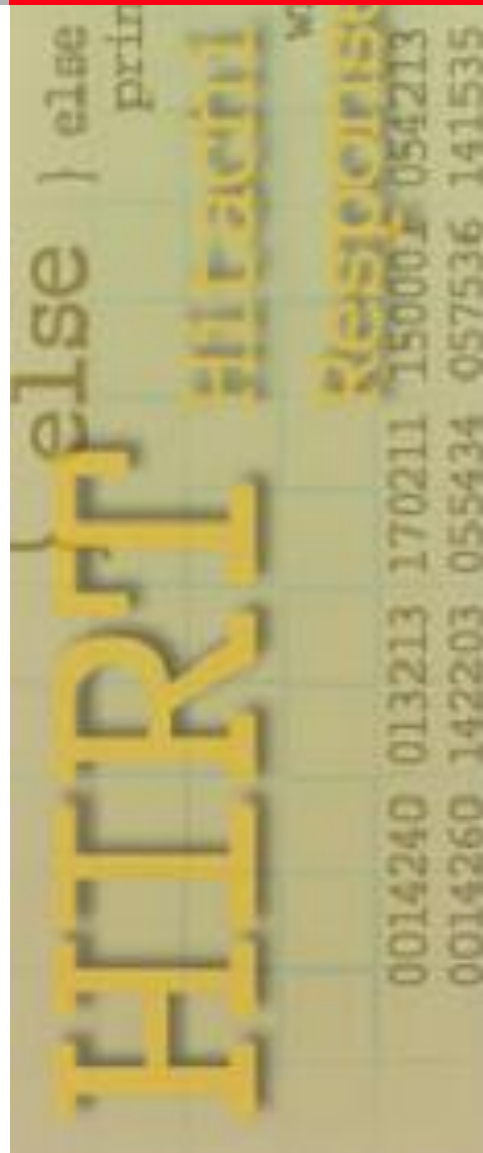


Contents

HITACHI
Inspire the Next

日々、不正アクセス、コンピュータウイルスへの感染など、セキュリティに関係した事件(セキュリティインシデント)が発生しています。
そこで、本講義では、これまでに発生した代表的なセキュリティインシデントを題材に、セキュリティインシデントから学べることを一緒に考えてみたいと思います。

1. インシデントを振り返る
2. 不正アクセスに関する理解を深める
3. シーサート活動



不正アクセスとは

- **システムの脆弱性を探査ならびに検証し、そして攻撃するための技術**

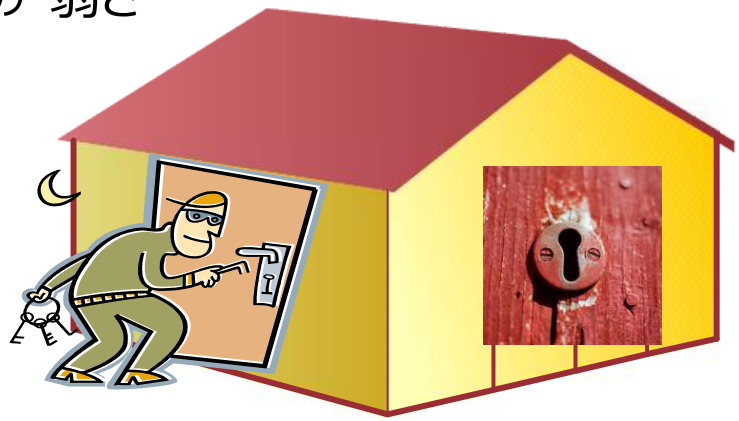
- 不正アクセスの特徴、脅威や対処方法を把握するには、TCP/IPの通信層、アプリケーションプログラム、データやユーザなどの攻撃対象毎に分類したり、情報収集段階、攻撃段階、占領段階のように侵入活動のフェーズ毎に分類したり、コンピュータに侵入することを必要とする攻撃活動か否かの攻撃形態毎に分類するなどさまざまな観点から分類していくと良い。
  - **攻撃対象別：TCP/IP、アプリケーション、データ、ユーザなど**
  - **攻撃段階別：3段階の分類(情報収集、攻撃、占領)など**
  - **攻撃形態別：ローカル/リモート、内部型/外部型、能動型/受動型**

2. 不正アクセスに関する理解を深める

脆弱性(ぜいじゃくせい)とは・・・

- **OSやソフトウエアなどのセキュリティ上の欠陥**
  家に例えると、ドアの鍵穴の劣化、鍵そのものの”弱さ”

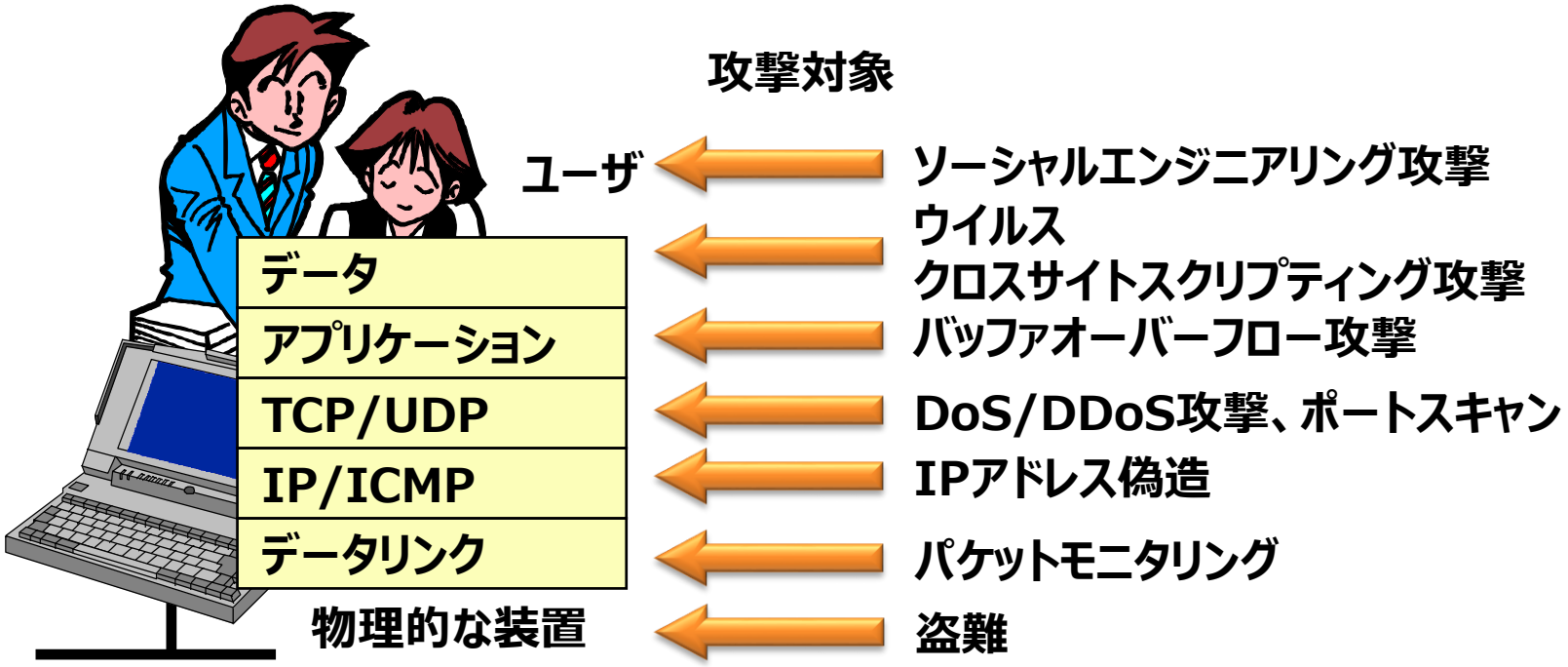
  脆弱性があると(鍵が付いていない、鍵をかけていないのと同じこと)・・・侵入者(攻撃者)によって家(PC・サーバ)に容易に入られてしまうことに。



- **ウイルス対策と脆弱性対策は、同じではない。**
  - **脆弱性対策**
    劣化した鍵穴を修繕したり、鍵そのものを防犯性の高いものに交換すること。
  - **ウイルス対策**
    警備員を雇う(ウイルス対策ソフトを導入)こと。ただし、警備員がよそ見するなどの隙(ウイルス定義ファイルの未更新など)を利用されると、脆弱性を悪用されて侵入されてしまう可能性がある。

攻撃対象別：攻撃対象にあわせて攻撃手法を選択

- 攻撃対象別の場合、攻撃対象は物理的な装置、TCP/IP、アプリケーション、データ、ユーザと多岐に渡る。



ソーシャルエンジニアリング攻撃

- **社会工学的な観点から発生する脆弱性(人間の心理的な隙や行動上の隙)を利用した攻撃方法**
  - 人間の心理的な隙を利用する事例
    - コンピュータ管理者になりすまして、「(システム管理上)あなたのパスワードを送ってほしい」というメールを送り、パスワードを聞き出す
    - 電話や、面と向かって個人情報を盗み出そうと働きかける
  - 人間の行動上の隙を利用する事例
    - ゴミ箱に廃棄された紙ゴミから重要情報を読み取る
    - 肩越しに画面や利用者の手の動きからパスワードを盗み見る

ソーシャルエンジニアリング攻撃

メッセージにより誘導する

- **【電子メール】**
  1991年4月、米国のコンピュータ緊急対応チームCERT/CCから「CA-1991-03：Unauthorized Password Change Requests Via Mail Messages」という注意喚起が発行された。

SAMPLE MAIL MESSAGE as received by the CERT (including spelling errors, etc.)
:
{mail header which may or may not be local}
:
This is the system administration:
Because of security faults, we request that you change your password to "systest001". This change is MANDATORY and should be done IMMEDIATLY. You can make this change by typing "passwd" at the shell prompt. Then, follow the directions from there on.

Again, this change should be done IMMEDIATLY. We will inform you when to change your password back to normal, which should not be longer than ten minutes.

Thank you for your cooperation,

The system administration (root)

END OF SAMPLE MAIL MESSAGE

報告された攻撃は、システム管理者を装って「パスワードを変更して欲しい！」という電子メールを送りつけるという手法であった。

出典　CERT Advisory CA-1991-03 Unauthorized Password Change Requests Via Mail Messages
http://www.cert.org/advisories/CA-1991-03.html

添付ファイルを開きたくなるメッセージを利用する

- **【電子メール型ワーム】**
  電子メールにウイルスファイルを添付して自己伝搬していく、いわゆる電子メール型ウイルスにも利用されている。

1999年頃に流布したウイルスが利用した件名／本文である。いずれの場合も、思わず添付ファイルを開きたくなるメッセージとなっている。

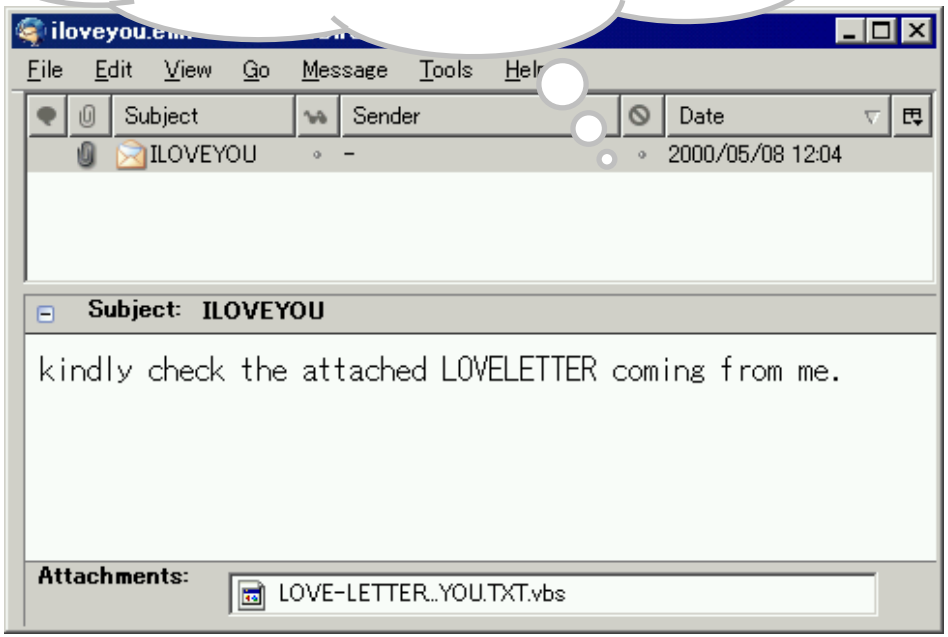
名称	利用されたメッセージ
W97M/Melissa 【1999年2月】	件名：Important Message From “ユーザ名” 本文：Here is that document you asked for ... don't show anyone else ;-) 頼まれていたドキュメントです。誰にも見せないように;-)
VBS/Loveletter (ラブレター) 【2000年5月】	件名：ILOVEYOU. 本文：kindly check the attached LOVELETTER coming from me. 私からのラブレターです。どうぞ読んでみて下さい。
VBS/OnTheFly 【2000年8月】	件名："Here you have, ;o)" 本文：Hi: Check This! 添付："AnnaKournikova.jpg.vbs"

添付ファイルを安全なファイルであると勘違いさせる

- **【二重拡張子】**
  VBS/Loveletter(2000年5月)、Win32/Bugbear(2002年10月)

2000年代には、メッセージだけではなく、見た目を騙す手法が出始めた。2000年5月に出現したラブレターウイルス(VBS/Loveletter)は、「I Love You」という題名と共に、添付ファイルをテキストファイルと勘違いさせるために、「.TXT」という文字列を入れた「LOVE-LETTER-FOR-YOU.TXT.vbs」という添付ファイル名を使用した。

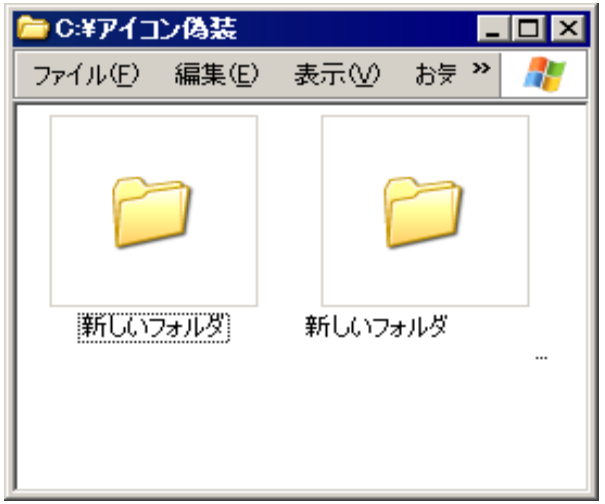
添付ファイルは、拡張子がvbsであるが、その前に「TXT」が付いていたために、テキストファイルと勘違いして多くのユーザが開いてしまったと言われている。

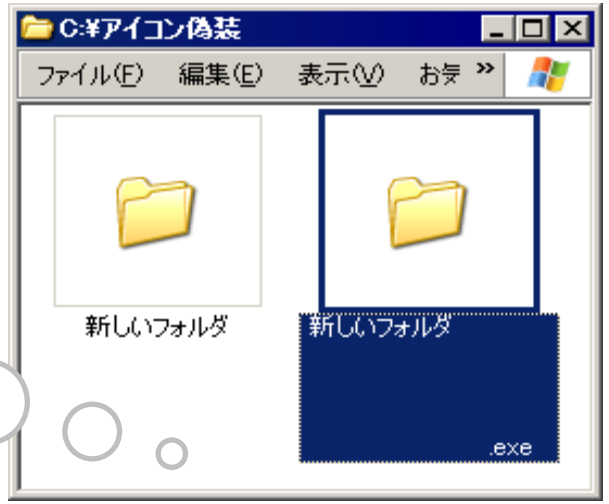


問題のない操作であると勘違いさせる(1)

- **【アイコン偽装＋ファイル名偽装】**
  Anntinny(2003年)

  情報漏えいウイルスとも呼ばれ、Winnyでの情報漏えい被害を発生させ続けているアンティニィ(Antinny)は、実行可能ファイル(＝ウイルス本体)をアイコン偽装していた。





**右側のアイコンは一見フォルダに見えるが、
実はフォルダと同じアイコンを表示する、
非常に長いファイル名
(コピー～新しいフォルダ2･･･空白文字･･･　.exe)
を使って偽装された実行可能ファイル
(＝ウイルス本体)である。**

問題のない操作であると勘違いさせる(2)

- **【 USBメモリ型ウイルス(USBメモリの自動再生／自動実行)】**
  Conficker(2008年11月)

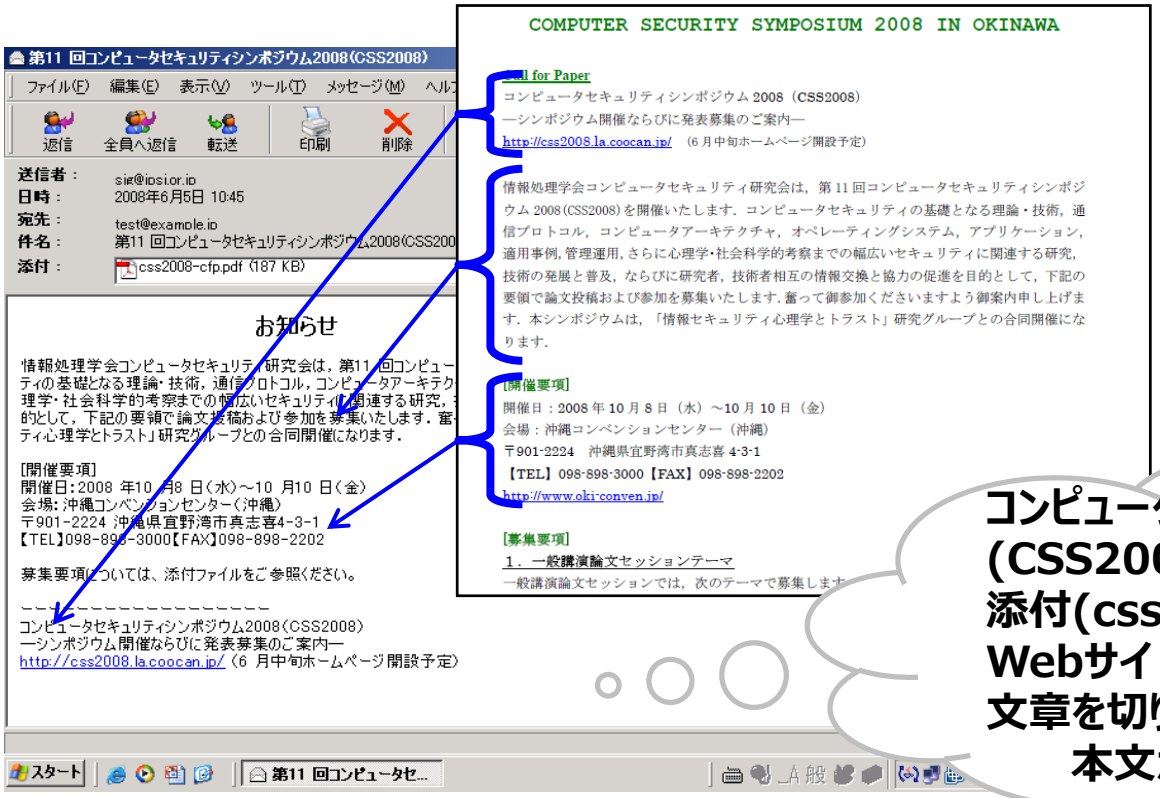
2008年11月頃から出現したコンフィッカー(Conficker)には、2008年12月に入ってから、USBメモリの自動再生／自動実行を利用した感染機能が追加された。

USBメモリの自動再生／自動実行を利用して騙す手法を再現したものである。この事例の場合、ダイアログの「OK」ボタンを押すと、上段にある「USBメモリを開く」が選択され、USBメモリに格納された実行可能ファイル(＝ウイルス本体)が起動することになる。

Windows XPパソコンにUSBメモリを接続した直後の状態

本物を活用する(1)

- **【再利用：カット&ペースト】**
  標的型攻撃メール(欧米2005年～、国内2005年～)

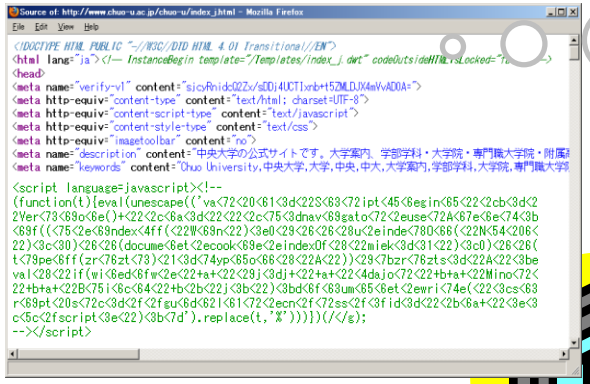


2008年あたりから、「怪しいメールには気をつけなさい」という注意喚起では通用しなくなる事例が出始めた。この頃から、サイバー攻撃の活動基点が「怪しい」から「怪しくない(怪しさを感じさせない)」に切り替わり始めた。

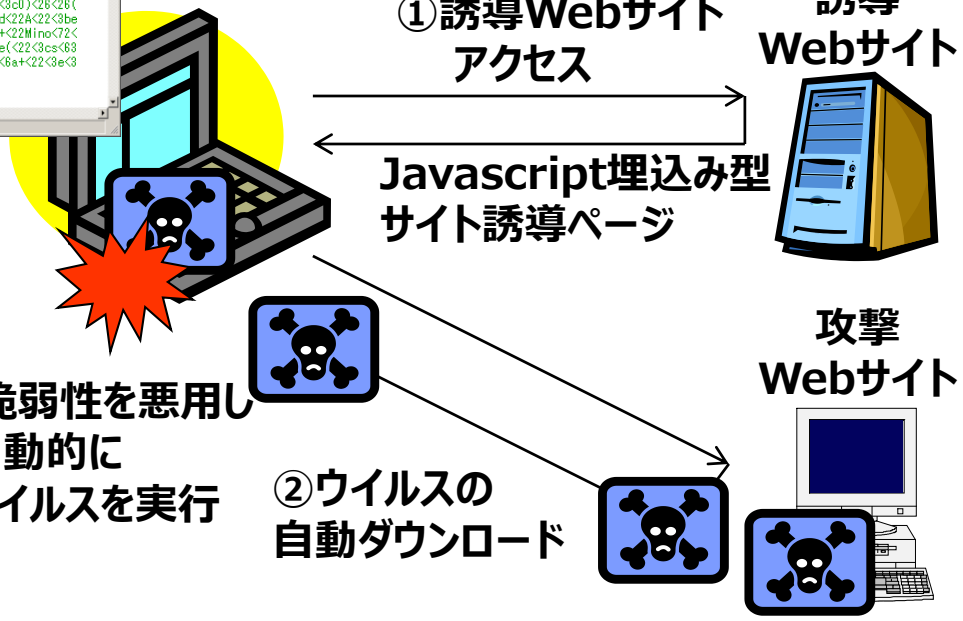
コンピュータセキュリティシンポジウム2008(CSS2008)の募集要項を装ったウイルス添付(css2008-cfp.pdf)メールである。Webサイトに掲載されているPDFから文章を切り貼りして電子メールの本文が作成されている。

本物から誘導する(1)

- **【サイト誘導を用いたウイルス感染活動】**
  Gumblar(2009年5月)



ユーザは一般的なWebサイトにだけアクセスしていると思い込む。しかし、ブラウザは蔵置された誘導コードにより、ウイルスをダウンロードするサイトにアクセスしてしまう。



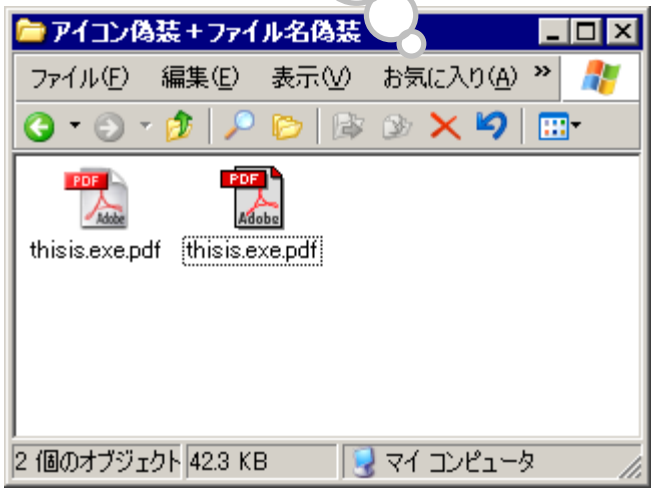
2009年に入ると、Webサイトにおいても、「怪しいWebサイトには気をつけなさい」という注意喚起だけでは通用しなくなった。2009年5月に出現したガンブラー(Gumblar)は、一般的なWebサイトの一部を改ざんして、ブラウザ上には表示されない誘導コードを蔵置する。

問題のない操作であると勘違いさせる(3)

- **【アイコン偽装＋ファイル名偽装】**
  RLTrap(2011年)

左側のファイル名は「thisis.exe.pdf」であり、右側のファイル名は「thisis.」と「fdp.exe」の間にRLO制御文字の入った「thisis. [RLO制御文字] fdp.exe」となっている。

2011年9月に出現したアールエルトラップ(RLTrap)は、Unicode制御文字のRLO(Right-to-Left Override)を利用してファイル名偽装した。RLOは、アラビア文字など右から左に記述する文字のために書字方向を変更するための制御文字である。
このRLOの制御文字をファイル名の途中に挿入することにより、画面に表示されるファイル名の右端に来る文字列をpdfなどの無害な拡張子に見せかけることができてしまう。

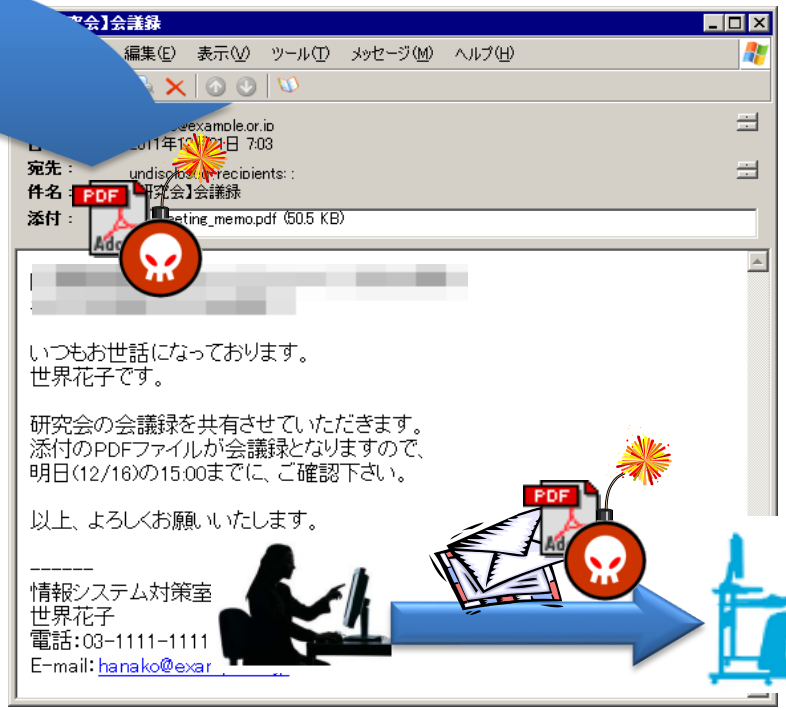


本物を活用する(2)

- **【再利用+再送】**
  標的型攻撃メール(国内2011年～)

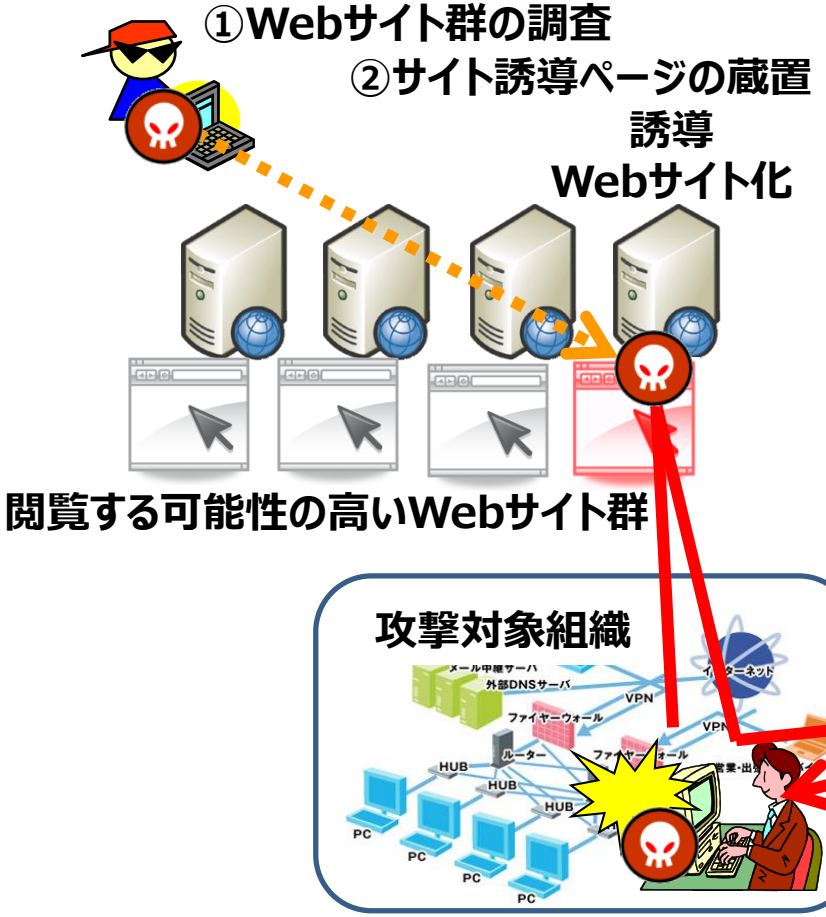
2011年の標的型攻撃の電子メールでは、電子メール(オリジナル)を搾取した後、その電子メールに添付されているファイルをウイルスファイルに入れ換えて再送された。

送付された電子メールを搾取した後、添付ファイルに攻撃コードを埋め込み再送する。



本物から誘導する(2)

- **【Webサイト待ち伏せ型】**
  Watering Hole Attack(水飲み場攻撃)(2012年)



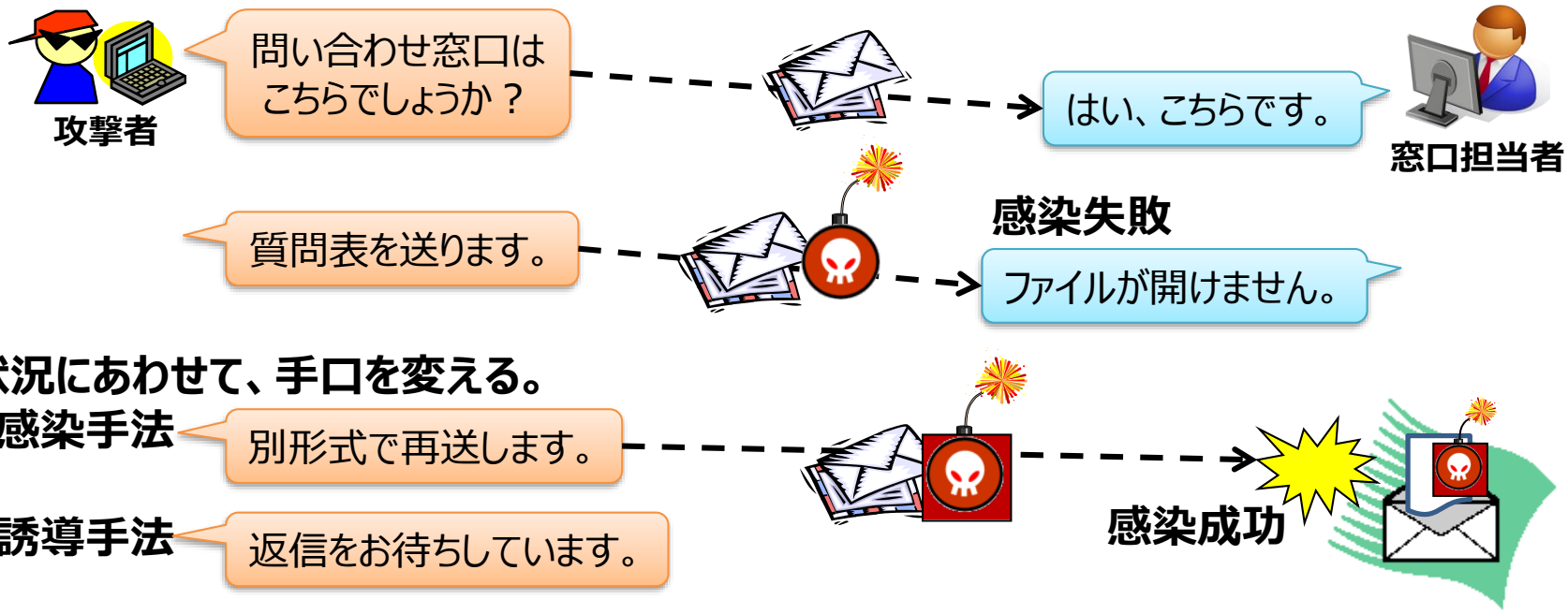
攻撃対象組織が閲覧する可能性の高いWebサイト群を狙う手法
・・・水飲み場で獲物を待ち伏せるライオンのように、攻撃対象組織の利用者が誘導Webサイト(＝攻撃Webサイト)を閲覧するのを待ち受ける

ソーシャルエンジニアリング攻撃

会話により誘導する

- **【やり取り型】**
  標的型攻撃メール(国内2014年～)

一般の問い合わせ等を装った無害な「偵察」メールなど、一連のやりとりの中で、ウイルス付きのメールが送られてくる。



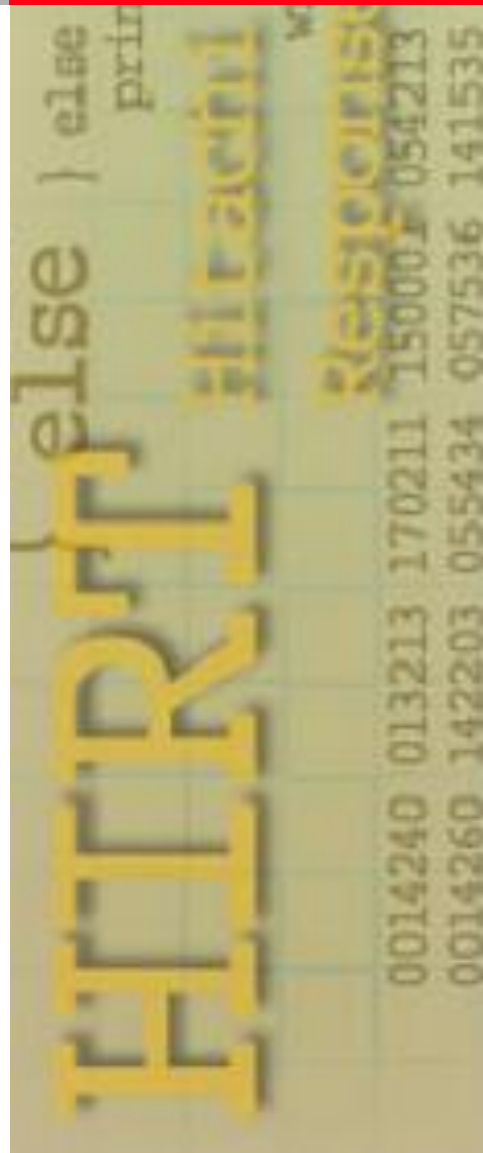
出典　組織外部向け窓口部門の方へ：「やり取り型」攻撃に対する注意喚起 ～ 国内5組織で再び攻撃を確認 ～
https://www.ipa.go.jp/security/topics/alert20141121.html

Contents

HITACHI
Inspire the Next

日々、不正アクセス、コンピュータウイルスへの感染など、セキュリティに関係した事件(セキュリティインシデント)が発生しています。
そこで、本講義では、これまでに発生した代表的なセキュリティインシデントを題材に、セキュリティインシデントから学べることを一緒に考えてみたいと思います。

1. インシデントを振り返る
2. 不正アクセスに関する理解を深める
3. シーサート活動



3. CSIRT(シーサート)とは

Computer Security Incident Response/Readiness Teamの略

- **コンピュータセキュリティにかかるインシデントに対処するための組織の総称(機能)**
- **インシデント関連情報、脆弱性情報、攻撃予兆情報を収集、分析し、対応方針や手順の策定などの活動**

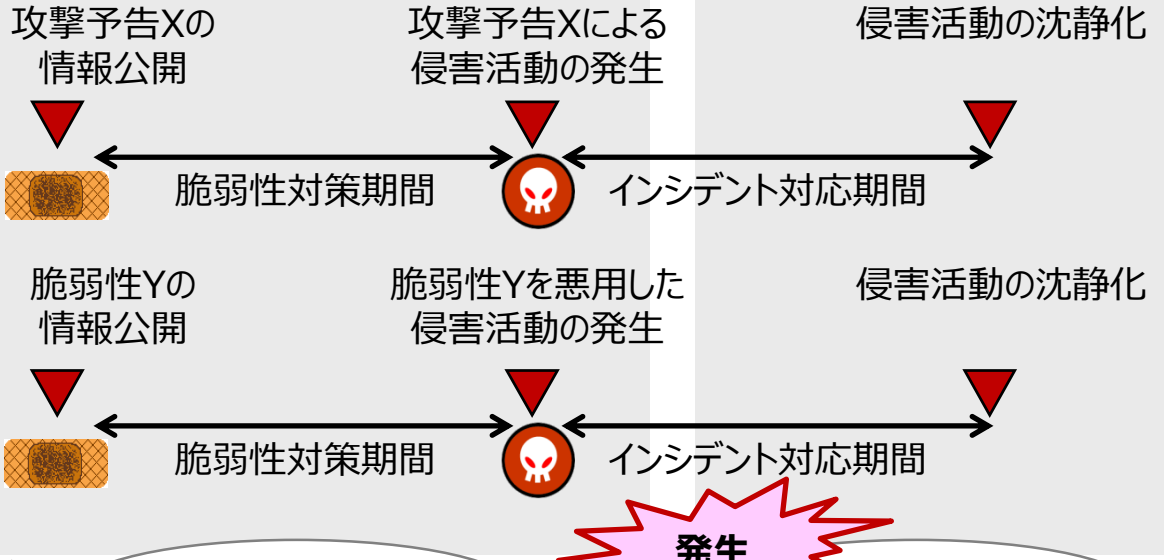
- シーサートの目的、立場(組織内での位置付け)、活動範囲、法的規制などの違いからそれぞれ各チームがそれぞれの組織において独自の活動している。

  ⇒ CSIRTに規格はなく、各組織の実態に即したCSIRTを実装
  ⇒ 1つとして同じCSIRTは存在しない

注：Cyber Security Incident Readiness Teamと呼ぶ場合もある。

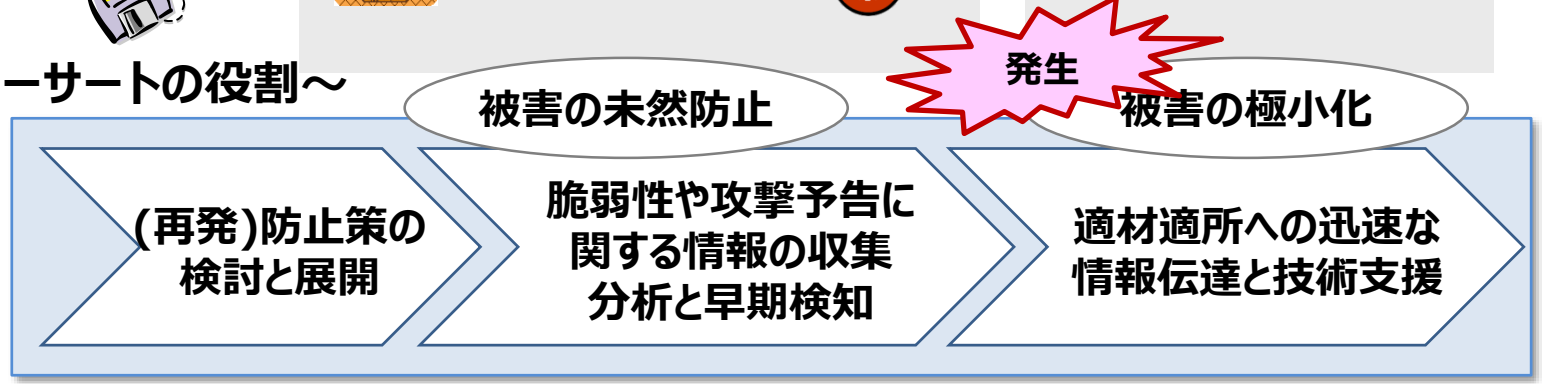
一般的に認識されているシーサートの役割

攻撃予告Xによる侵害活動が発生した場合



公開された脆弱性Yを悪用した侵害活動が発生した場合

～シーサートの役割～



シーサートは多種多様

- **活動範囲の視点からの分類**
  組織シーサート、国際連携シーサート、コーディネーションセンター、分析センター、製品対応チーム、インシデントレスポンスプロバイダなどに分類されることもある。

- **対象範囲、内容、体制などの違いによって、多種多様なシーサートが構成されている。**
  - 対象範囲：国、自組織、顧客
  - 内容(フェーズ)：事前対処、事後対処
  - 内容(機能)：脆弱性ハンドリング、インシデントハンドリング、動向分析、リスク分析など
  - 体制：集約型／分散型、専任型／兼務型

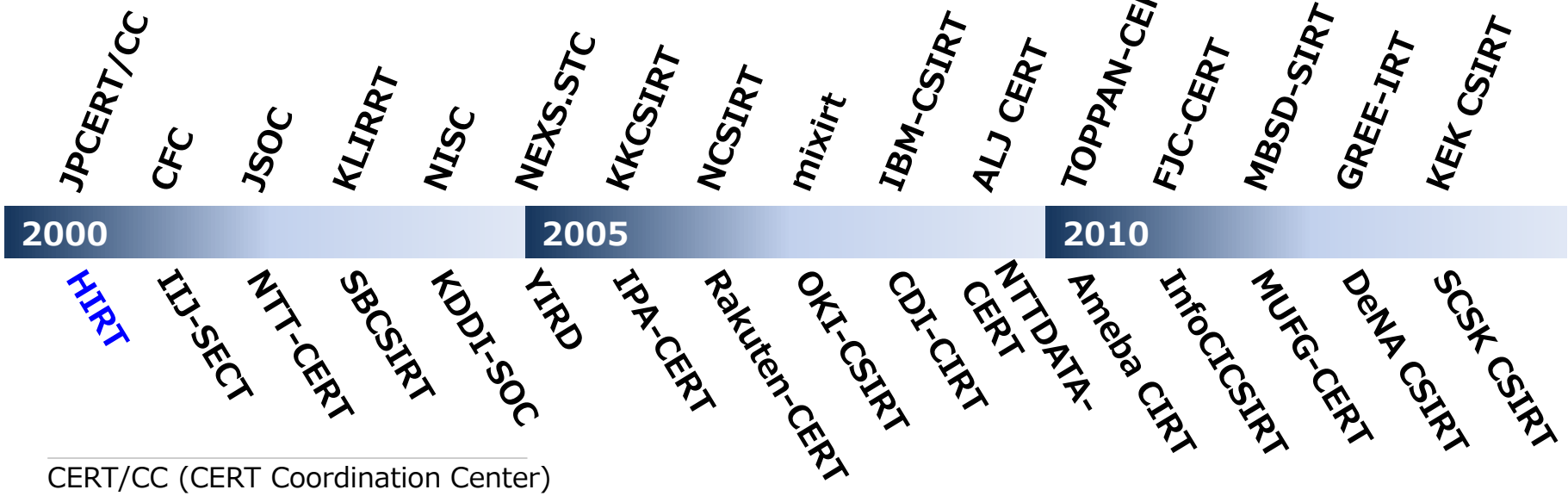
組織シーサート
自組織に関係したインシデントに対応するシーサートのこと。

製品／サービス対応シーサート
提供する製品やサービスのインシデントに対応するシーサートのこと。

3. CSIRT(シーサート)とは：歴史

1988年、インターネットワームを契機に米CERT/CC設立

- 1988年　インターネットワームの出現を契機に、米CERT/CC 設立
- 1990年　Wankワームの出現を契機に、 FIRST 組織化
- 1996年　国内初のシーサート組織、JPCERT/CCが活動開始
- 1998年　HIRT(Hitachi Incident Response Team)プロジェクト開始
- 2007年　国内シーサートの組織間連携のため、日本シーサート協議会 設立



CERT/CC (CERT Coordination Center)
JPCERT/CC(Japan Computer Emergency Response Team/Coordination Center)
FIRST (Forum of Incident Response and Security Teams)

3. CSIRT(シーサート)とは：歴史

よりインテリジェンスな機能を求められてきている

年代	特徴	被害の模式図
2000年 ～2001年	**均一的かつ広範囲に渡る単発被害** Webサイトのページ書き換え	
2000年 ～2005年	**均一的かつ広範囲に渡る連鎖型被害** ウイルス添付型メールの流布 ネットワーク型ワームの流布	
2005年～	**類似した局所的な被害** SQLインジェクションによるWebサイト侵害 Winny、Shareによる情報流出 フィッシング、スパイウェア、ボットなど	
2006年～	**すべてが異なる局所的な被害** **標的型攻撃** **攻撃組織基盤化** **2009年～ 攻撃組織間連携**	

異なる組織のシーサート同士がつながり、手段を共有することで問題解決を図る

異なる組織のシーサート同士がつながり、侵害活動を鳥瞰することで問題解決を図る

組織におけるシーサートの役割

- **シーサート活動から導かれる組織におけるシーサートの役割**
  - 対外的な連絡窓口であること
  - 技術的な問合せに関して対応が可能であること
  - インシデントレスポンス(事後対処)だけではなく、インシデントレスポンスなどの実践的な活動経験を元に、インシデントレディネス(事前対処)を進めていること
  - 部署間を横断した組織体制をとっていること

出典：日本シーサート協議会 第1回連携ワークショップ
ワークショップ開催の趣旨説明 ～ シーサート PoC の重要性 ～
http://www.nca.gr.jp/activity/publication.html

HITACHI
Inspire the Next

END

セキュリティインシデントから
学べること