

『ネットワークセキュリティ対策技術研修』
不正アクセスの最新動向
～インシデント事例から考えるネットワークセキュリティ～

一般社団法人

JPCERTコーディネーションセンター

2009年11月13日（東京）

27日（大阪）

椎木 孝斉

真鍋 敬士

- インシデントの傾向
- インシデント事例の紹介
 - マルウェア添付メール
 - 改ざんされたWebからの誘導
 - 侵入、遠隔操作
- 取り組み
 - ボット対策推進事業
 - ITセキュリティ予防接種
 - 脆弱性情報ハンドリング

JPCERT/CCをご存知ですか？

■ JPCERT/CC

■ Japan Computer Emergency Response Team Coordination Center

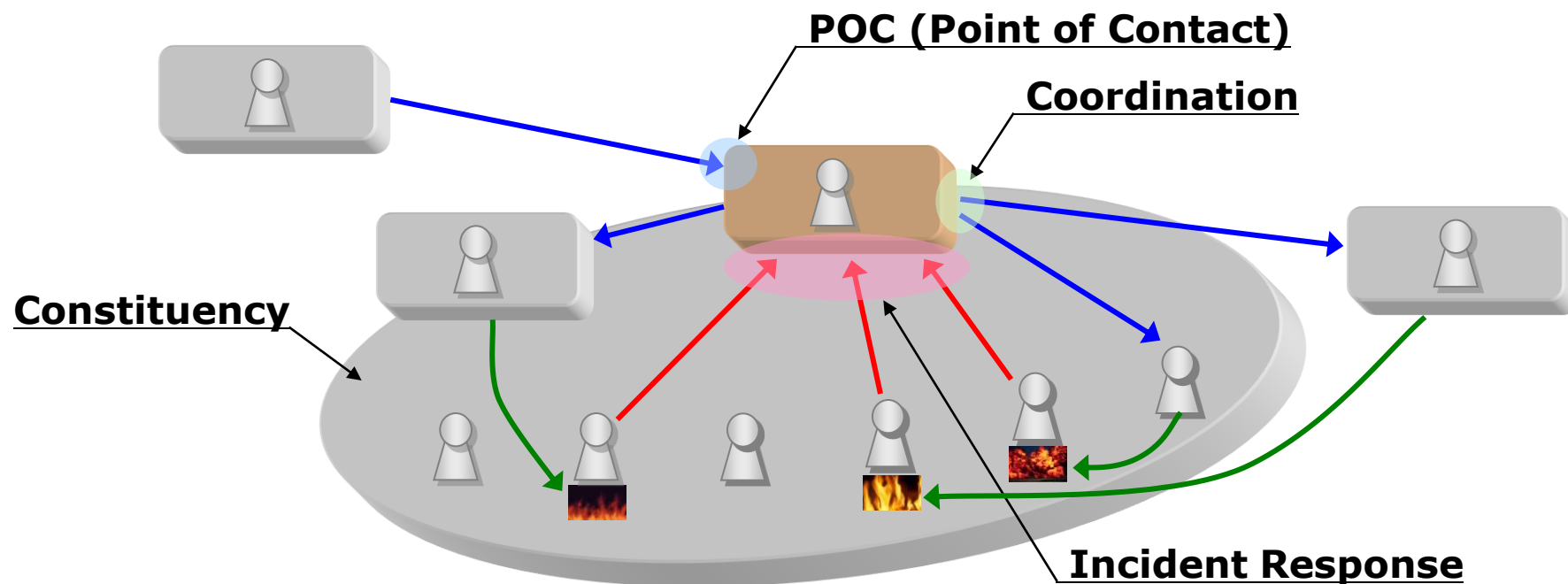
ジェーピーサート・コーディネーションセンター

- コンピュータセキュリティインシデントに関する調整・連携などの活動
- 国内組織や海外組織との連携活動
- 情報収集・分析・発信活動
- 「コーディネーションセンター」としての役割
- CSIRT(Computer Security Incident Response Team)のひとつ

コンピュータセキュリティインシデント:

- ✓コンピュータセキュリティに関係する人為的事象
- ✓意図的および偶発的なもの(その疑いがある場合)

- Computer Security Incident Response Team
- 米国CERT/CC: 1988年に設立された世界初のCSIRT
- インシデントハンドリングを主な活動とする組織体の一般名称



-JPCERT/CCをご存知ですか?-
JPCERT/CCの沿革

インシデントハンドリング

1996

Japan Computer Emergency Response Center

1998

FIRST membership

2003

Corporate status acquired

インターネット定点観測
システム(ISDAS)

2004

脆弱性情報ハンドリング

FIRST SC member

2005

早期警戒情報提供

Anti-Bot project
(10th anniversary)

2006

アーティファクト分析

Early Warning Partnership
Vulnerability Coordination Center

–JPCERT/CCをご存知ですか?–
JPCERT/CCの活動

JPCERT/CC®

インシデント予防

脆弱性情報ハンドリング

- 未公開の脆弱性関連情報を製品開発者へ提供し対応依頼
- 国際的に情報公開日を調整



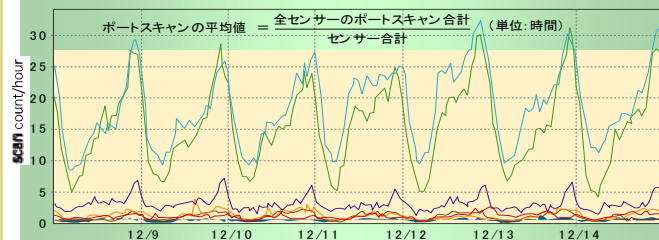
JVN Japan Vulnerability Notes

インシデントの予測と捕捉

情報収集・分析・発信

定点観測 (ISDAS)

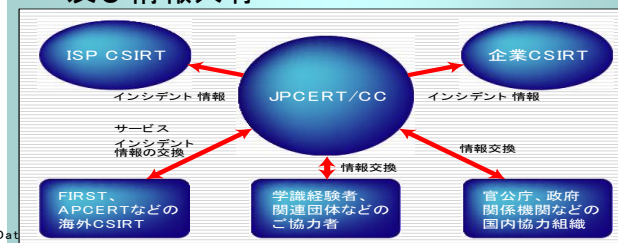
- ネットワークトラフィック情報の収集分析
- 定期的なセキュリティ予防情報の提供



発生したインシデントへの対応

インシデントハンドリング

- インシデントレスポンスの時間短縮による被害最小化
- 再発防止に向けた関係各関の情報交換及び情報共有



早期警戒情報

重要インフラ事業者等の特定組織向け情報発信

CSIRT構築支援

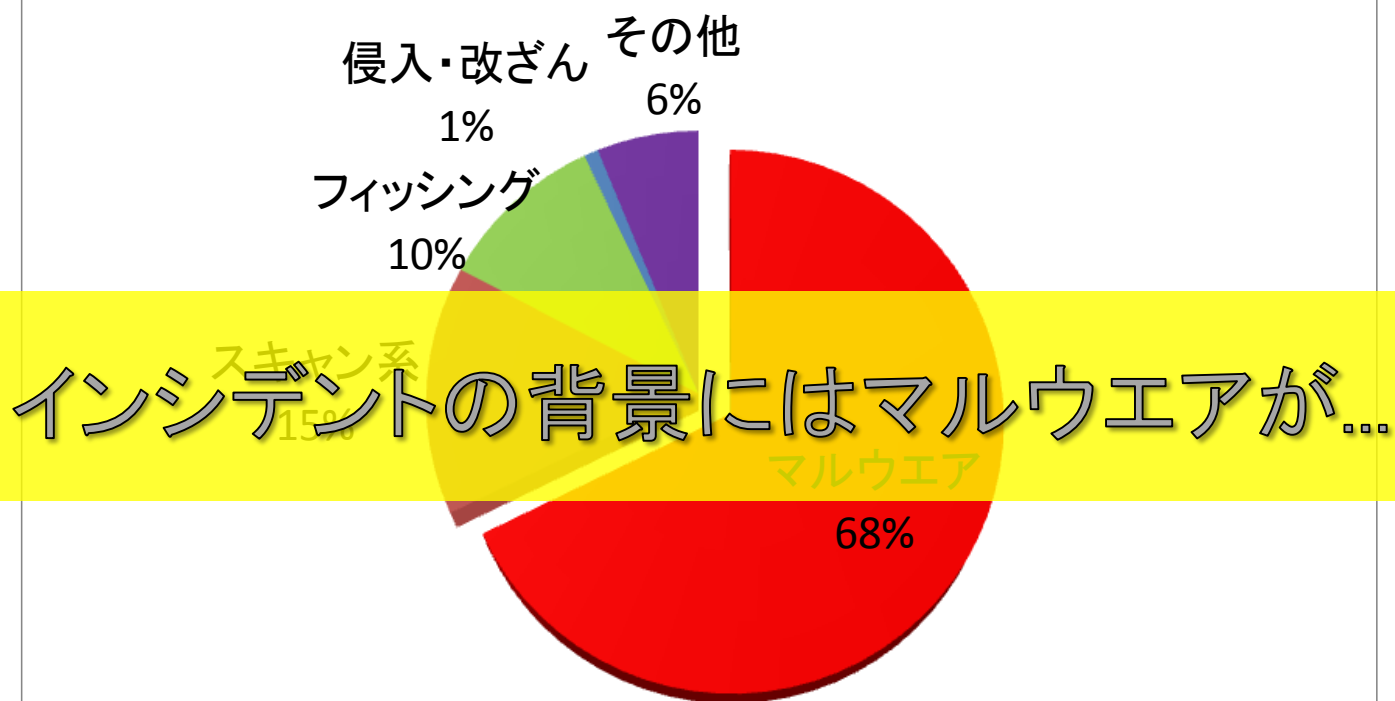
企業内のセキュリティ対応組織の構築支援

アーティファクト分析

マルウェア(不正プログラム)等の攻撃手法の分析、解析

- ① 国際インシデント対応演習への参加、人気セミナーの海外展開、アジア諸国のNational CSIRT 構築支援活動などによる国際貢献、連携強化
- ② FIRST Annual Conference Kyoto 2009:世界のセキュリティチームによる国際会議の日本開催が成功裏に終了
- ③ Web フォームによるインシデント報告の受付、注意喚起及び脆弱性情報の英語による発信等、利用者の利便性向上のための機能を追加
- ④ 「JPCERT/CC 脆弱性関連情報取扱いガイドライン」の改定
- ⑤ 文部科学省の先導的IT スペシャリスト育成推進プログラムによる高度セキュリティ人材育成活動に協力
- ⑥ ボット対策事業の平成20 年度活動報告を公開
- ⑦ 制御システムのセキュリティに関する提供情報を拡充

インシデントの傾向



インシデント報告件数割合(2009年7月～9月)

<http://www.jpcert.or.jp/ir/report.html>より

■ ボットネット

ー 攻撃インフラ

- フィッシング, サービス妨害, 迷惑メール, ...
- アンダーグラウンドビジネス: 分業・連携

➤ CCC: ボット対策推進プロジェクト(2006年～)

- ボット対策活動を国の事業として実施

■ 標的型攻撃

ー ソーシャルエンジニアリング的手法

- 時事ネタ、個人情報、機密情報による誘引

ー 未修正の脆弱性の悪用

- JPCERT/CC内でのマルウェア分析から脆弱性情報ハンドリングを行ったケースも

➤ ITセキュリティ予防接種調査

- <http://www.jpcert.or.jp/research/#inoculation>

■ 潜行化

～分析ツールや環境がなければ専門家でも判定困難～

— 様々な隠蔽能力

- 既存のプログラムに似せた名前
- 既存プロセスへのインジェクション

— 派手に動かない性質

■ ツール化

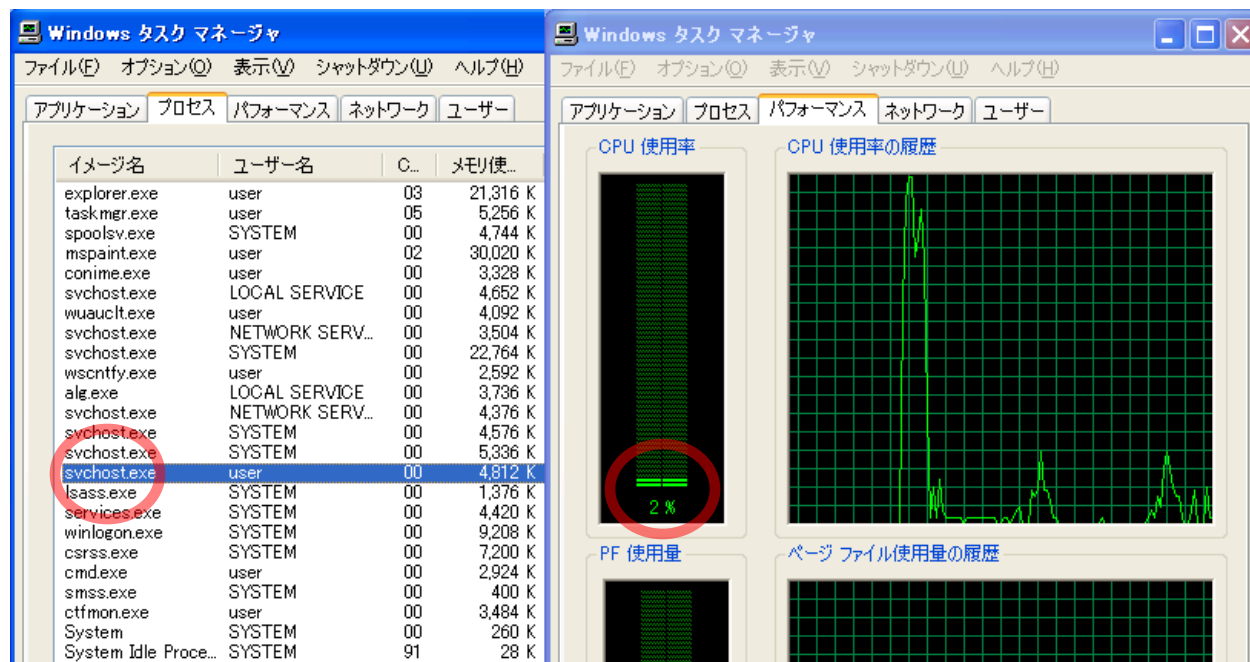
～専門知識不要～

— GUIにより簡単にできる

- カスタムマルウェア作成
- 感染PCの管理
- フィッシュキット

— 有償サポート

- アンチウイルス検知回避



インシデント事例

インシデント事例①マルウェア添付メール

差出人: [redacted] 宛先: [redacted]
件名: Thank you for setting the order No.475456 日時: Mon, 5 Oct 2009 11:23:50 -0500

Dear Customer!

Thank you for ordering at our online store.
Your order: Sony VAIO A1133651A, was sent at your address.
The tracking number of your postal parcel is indicated in the document attached to this letter.
Please, print out the postal label for receiving the parcel.

Internet Store.

install.zip

差出人: [redacted] 宛先: [redacted]
件名: Microsoft Outlook Notification for the mailer-daemon@list.jpccert.or.jp 日時: Sat, 17 Oct 2009 10:18:41 -0600

You have (5) New Message from Outlook Microsoft

- Please re-configure your Microsoft Outlook Again.
- Download attached setup file and install.

install.zip

差出人: [redacted] 宛先: [redacted]
件名: Conflicker.B Infection Alert 日時: Mon, 19 Oct 2009 21:27:05 -0300

Dear Microsoft Customer,

Starting 18/10/2009 the Conflicker.B worm began infecting Microsoft customers unusually rapidly. <
Microsoft has been advised by your Internet provider that your network is infected.

To counteract further spread we advise removing the infection using an antispayware program. We <
are supplying all effected Windows Users with a free system scan in order to clean any files <
infected by the virus.

Please install attached file to start the scan. The process takes under a minute and will prevent <
your files from being compromised. We appreciate your prompt cooperation.

Regards,
Microsoft Windows Agent #2 (Hollis)
Microsoft Windows Computer Safety Division

install.zip

- 実行した場合、感染しているというメッセージを表示
- 外部へ接続し偽アンチウイルスの本体となる 実行ファイルをダウンロードして実行



※ 感染している旨のメッセージと install.exe のアイコン



※ Antivirus Pro 2010 のインストール画面とダウンロードした exe のアイコン

JPCERT/CCに届いたマルウェア添付メール

■ 公開アドレス宛にマルウェア添付メール

■ 日 時: 2009年2月26日22時22分ころ

■ 送信先: info@jpcert.or.jp

■ 送信元: 国内ドメインを詐称したアドレス

送信サーバのIPアドレスは国外割当IPアドレス

日	月	火	水	木	金	土
22	23	24	25	26	27	28
1	2	3	4	5	6	7

■ JPCERT/CCにおける対応

■ 分析結果

■ 種 類: gh0st RATの一種

■ 通信先: 国外ドメイン(国外割当IPアドレス)
→ 標的型攻撃メールとの関連性が疑われる

■ 検体の通信先に対してコーディネーションを実施

■ 3月2日16時30分ころに通信先IPアドレスを管轄するCSIRTに情報提供

■ 3月3日14時46分の時点でDNSのAレコードが削除されていることを確認

RAT(Remote Access Trojan/Administration Tool)

■ PCの遠隔操作を可能にするツール

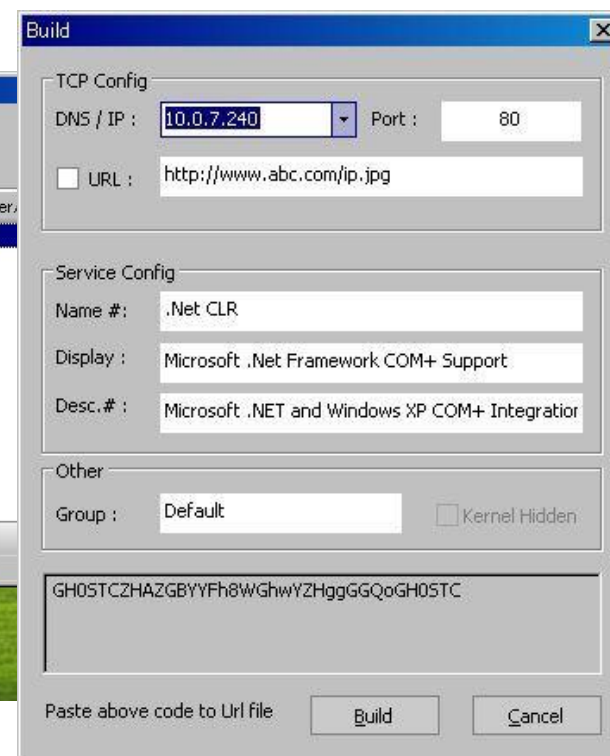
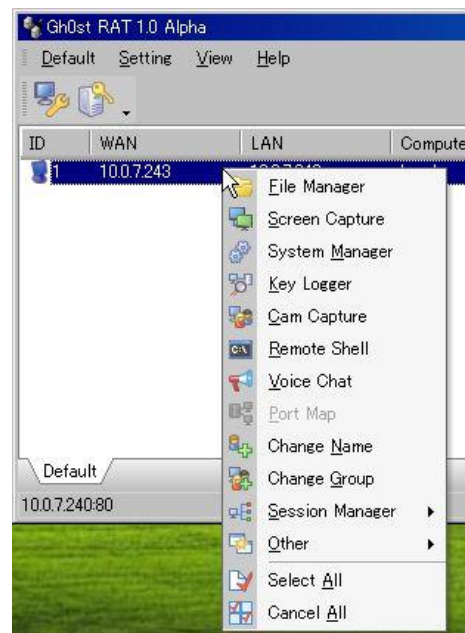
- GUIによりマルウェアの作成やクライアントの管理が可能

■ 主な機能

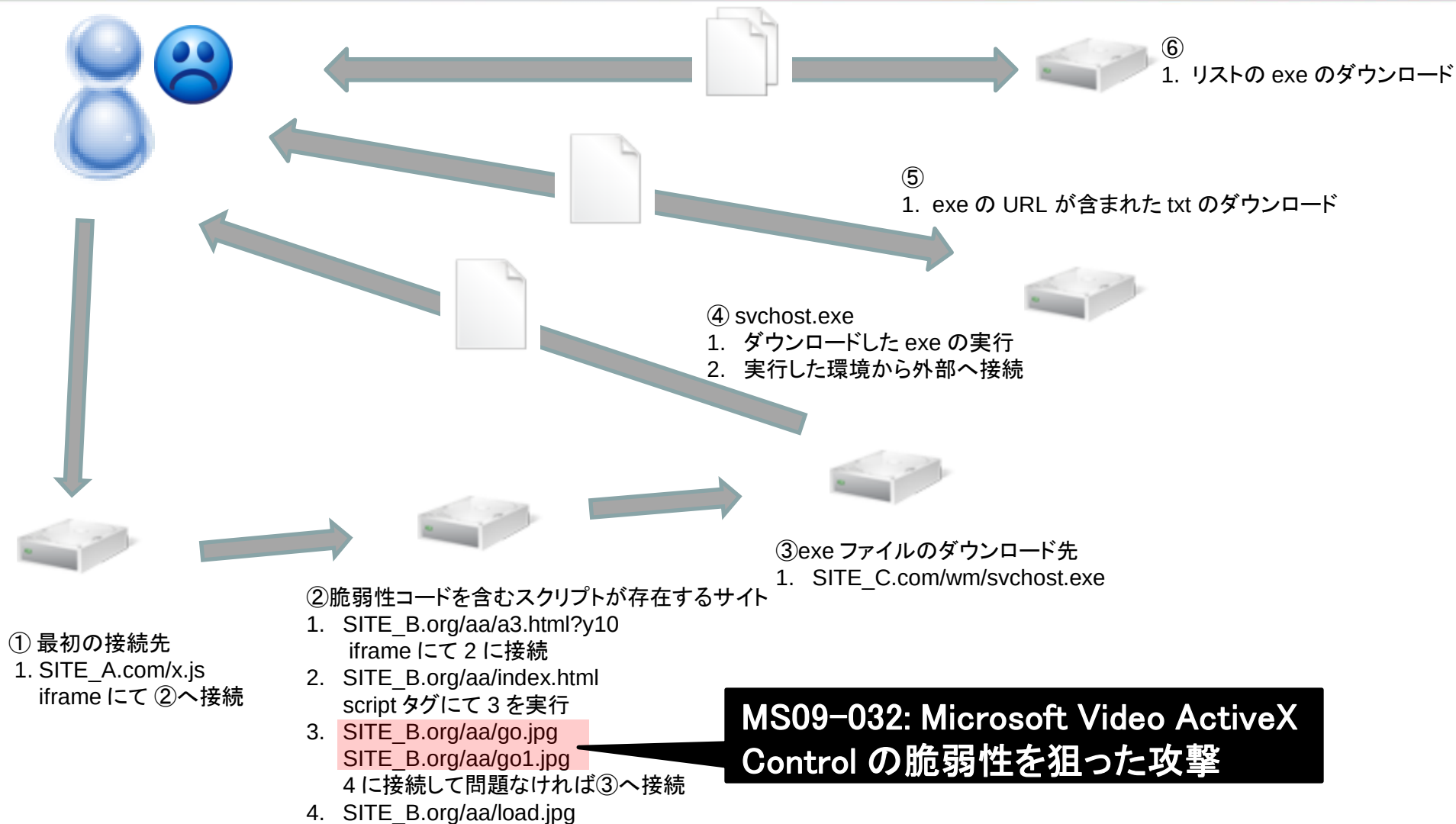
- プロセス情報の取得
- 特定プロセスの停止
- 特定のウイルス対策ソフトのバイパス
- マシンのシャットダウン、リモート
- リモートからのデスクトップ操作
- 任意のプログラムの実行
- スクリーンショットの取得
- Webカメラの操作
- 音声の録音
- キーロガー

■ 関連記事

- フォーティネットが総括: 上半期のセキュリティ動向
<http://www.itmedia.co.jp/enterprise/articles/0907/30/news073.html>
- Tracking GhostNet: Investigating a Cyber Espionage Network
<http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network>
- 「15万台が感染、国内でも被害多数」、ウイルスツール「Zeus」の脅威
<http://itpro.nikkeibp.co.jp/article/NEWS/20090827/336060/>



インシデント事例②改ざんされたWebからの誘導



■ 共通的な挙動

- ① Web改ざん
 - マルウェアホスティングサイトへ誘導するJavaScriptの埋め込み
- ② ダウンローダ実行
 - 脆弱性を悪用して動作し、別のマルウェアをダウンロード
- ③ マルウェア感染
 - アカウント情報盗聴等を行う

■ 問題を大きくする要因

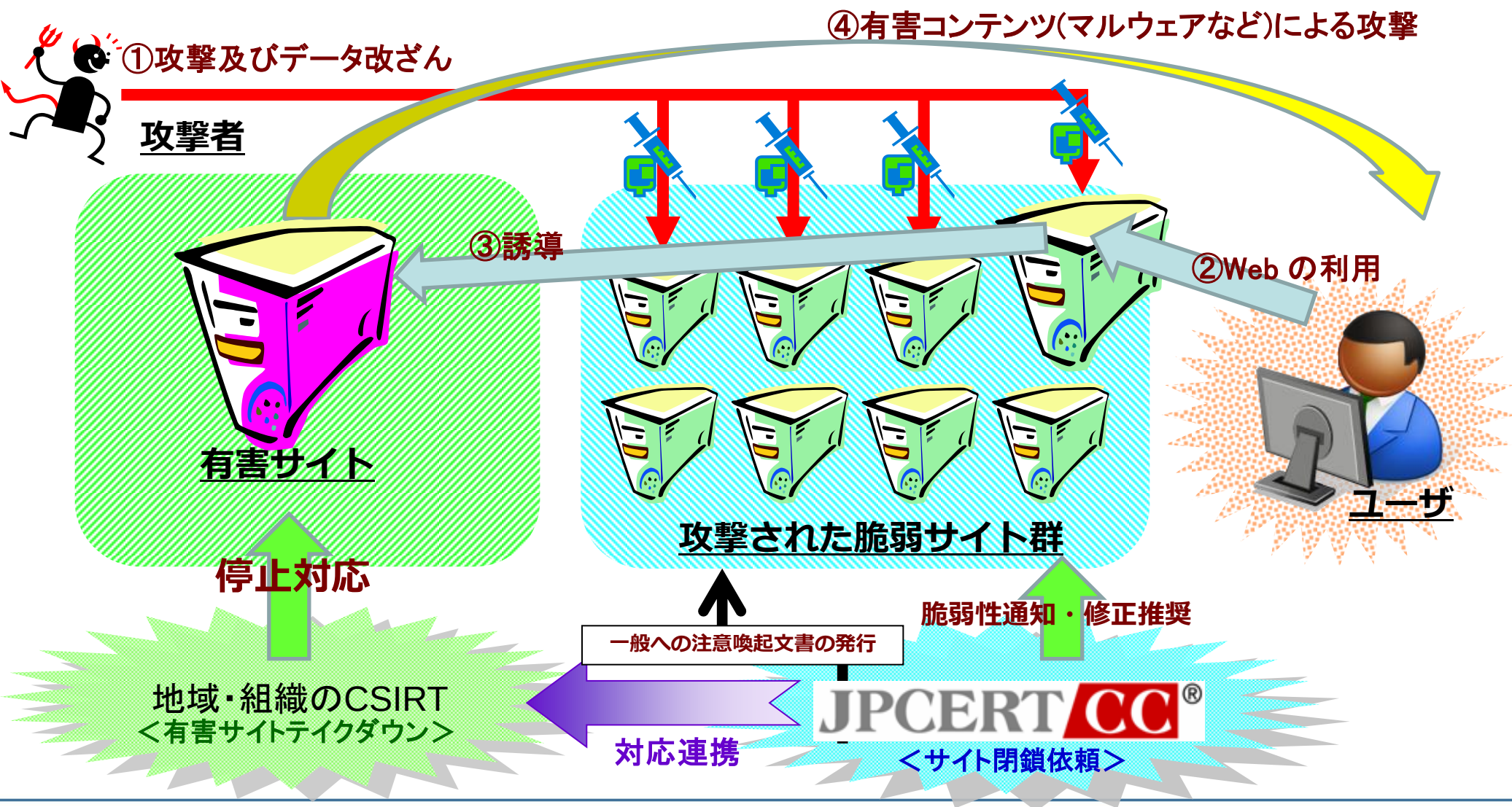
ー 技術的な難しさ

- JavaScriptの難読化
- マルウェアの多様性
 - パターンだけでは検知困難
- 無数のマルウェアホスティングサイト
- アクセス制限
 - 複数グループ

ー 事業者側での対応の限界

- 不正なFTPアクセスの制限
- 『改ざん』の判断
- 繰り返される改ざん
 - 本質的な対策がなされていない

-インシデント事例②改ざんされたWebからの誘導-
SQLインジェクション



■ Adobe Reader/Acrobat 関連

- util.printf (影響バージョン: 8.1.2 以下)
- Collab.collectEmailInfo (影響バージョン: 8.1.1 以下)
- app.doc.Collab.getIcon (影響バージョン: 8.1.2 以下および 9.0 以下)

■ ActiveX 関連

- MS09-032

■ FlashPlayer などブラウザの Plugin など

OS だけではなく、ブラウザに Plugin として利用されているサード
パーティー製のアプリケーションなどを狙うものが多くみられる

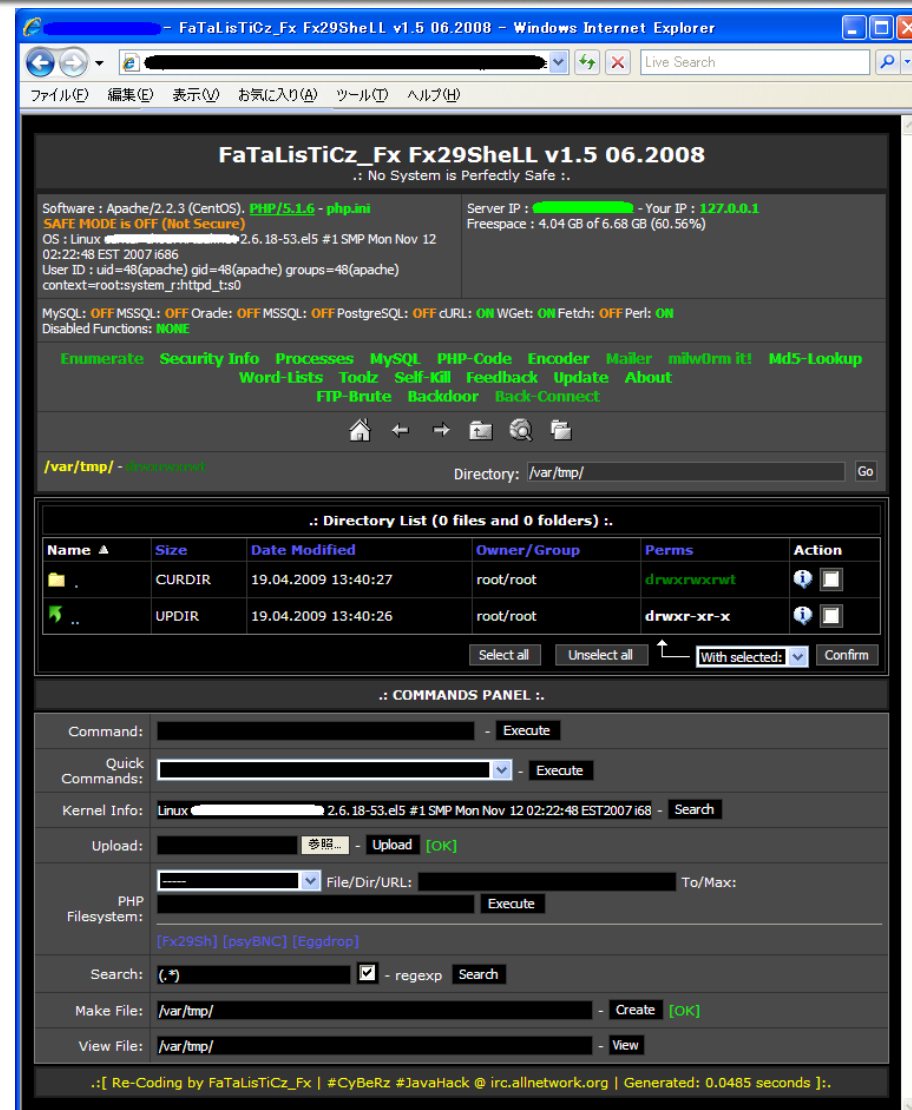
インシデント事例③侵入、遠隔操作

■ Webブラウザ経由での遠隔操作

- ネットワーク透過性
- フィッシングサイトの立ち上げにも

■ PHPでの実装

- 高い移植性
- カスタマイズが容易



■ 一般ユーザ

- OSやアプリケーションのアップデート
- アンチウイルス製品の導入・運用
- 最終ログイン日時等のアカウント情報への関心

■ サイト管理者

- Webコンテンツの定期・不定期の確認
- 定期的なログの確認
- パスワードの適切な運用

■ 関連組織・事業者

- 一般ユーザやサイト管理者への注意喚起
- 組織間での情報共有

取り組み

2009年09月度の注意喚起活動実績

1 収集検体総数

当月: 135,685体 累積: 15,165,119体
「おとりマシン」に対する無数の攻撃の中から収集した、ボットウイルス等の検体数（バイナリファイル）

2 同定検体数

当月: 5,930体 累積: 950,673体
同じ検体が多数収集されるため、検体のサイズや外形的特徴の重複を除いた一意な検体数（バイナリファイル）

3 未知検体数

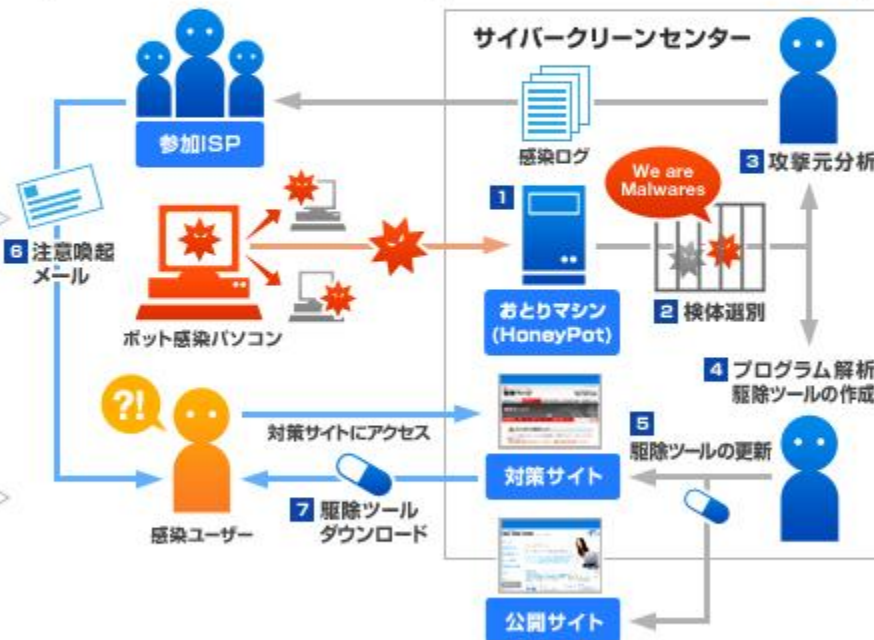
当月: 326体 累積: 26,048体
隔離した検体を市販のウイルス対策ソフトで検査し、検知できなかった検体数

6 注意喚起数

メール通数
当月: 11,314通
累積: 434,454通
対象者数
当月: 5,499人
(内新規1,955人)
累積: 90,439人
参加ISPから感染者に出した注意喚起メール数及び人数

7 被注意喚起者駆除ツールダウンロード率

30% (累積)



4 駆除ツール作成検体数

当月: 685体
累積: 21,383体

危険度が高く、感染者の多い検体について駆除ツールを作成した検体数

5 駆除ツール

累積更新回数: 139回
駆除ツールは毎週更新

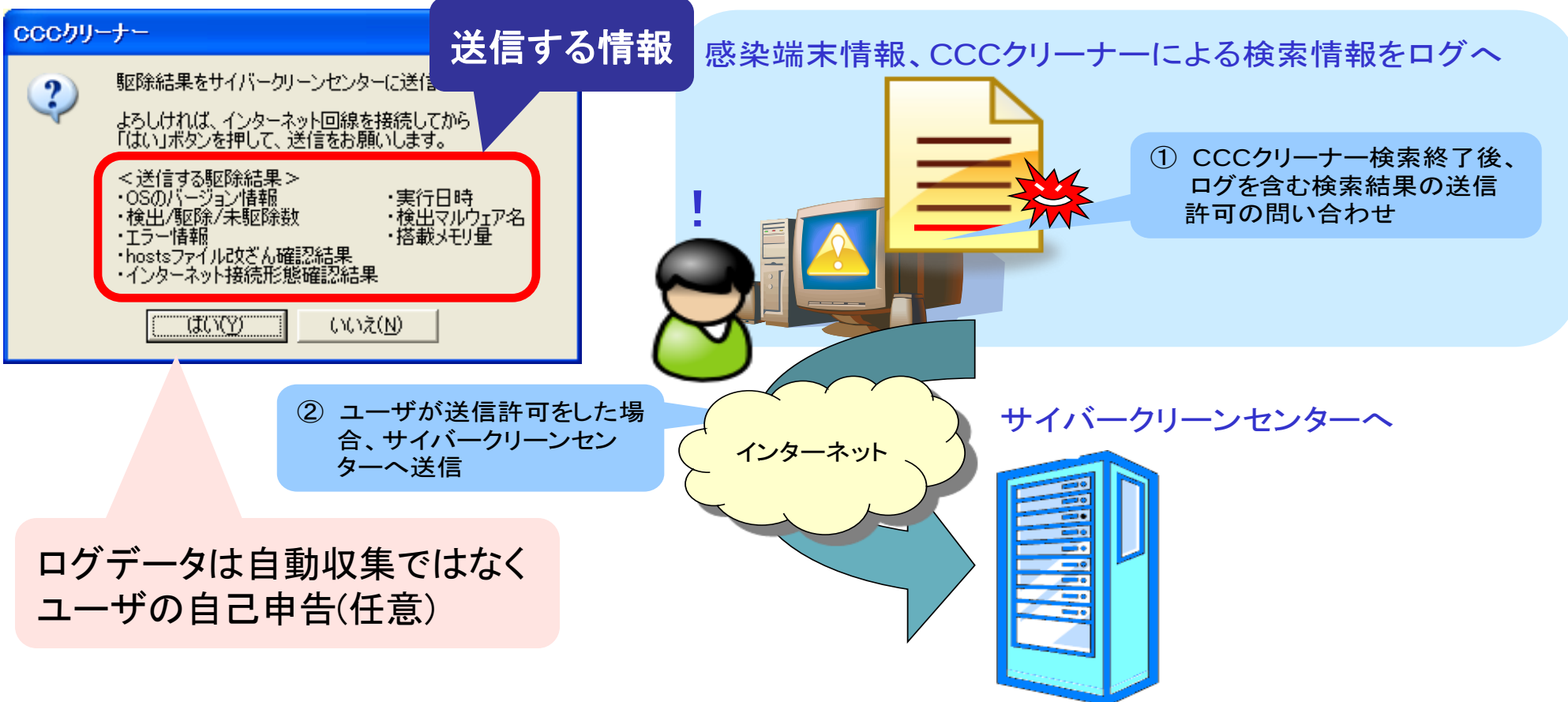
一般公開サイト駆除ツールダウンロード総数

※ 同時時間帯に複数回ダウンロードされたものは除いた数字

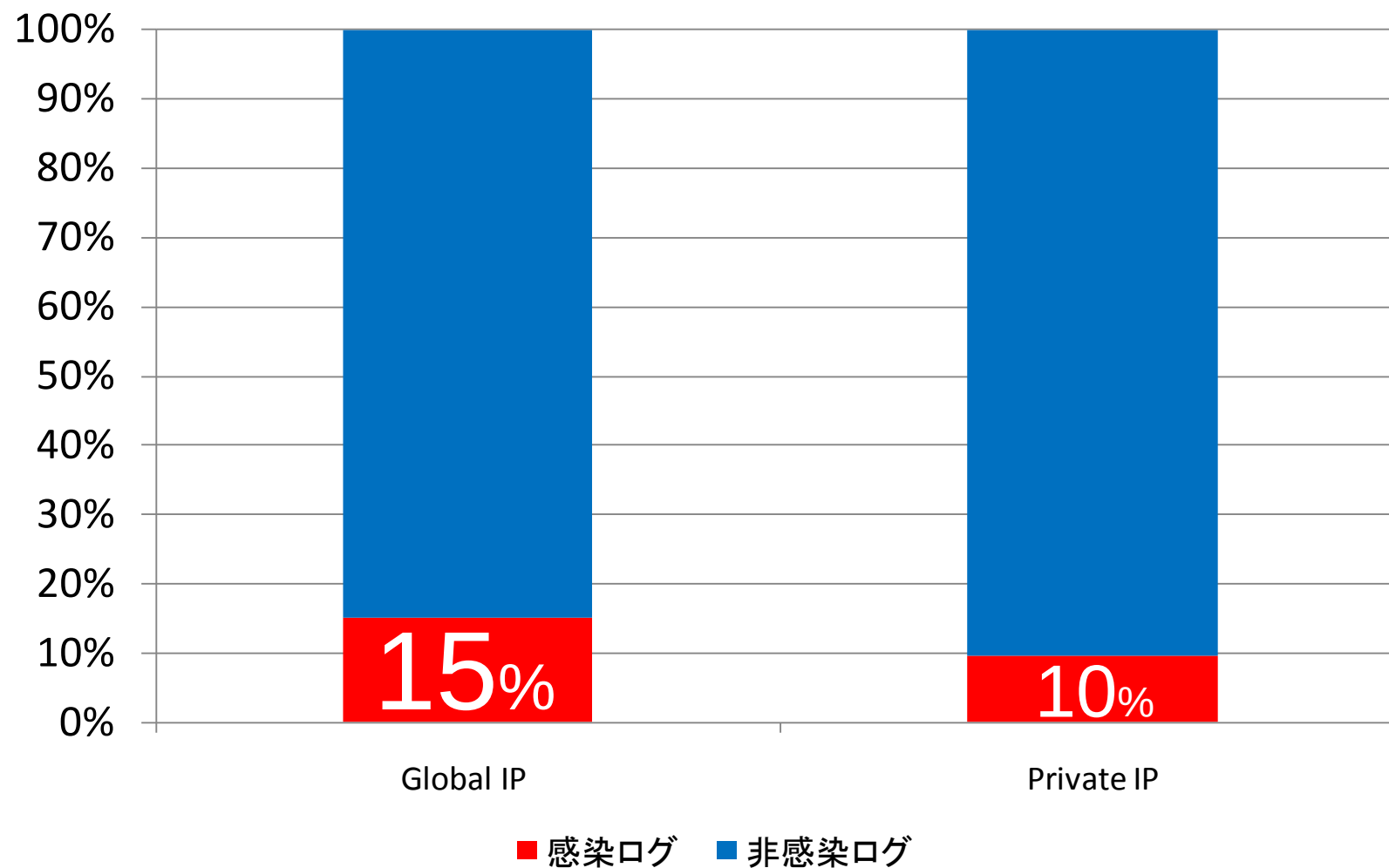
当月: 47,997回 累積: 1,016,373回

目的

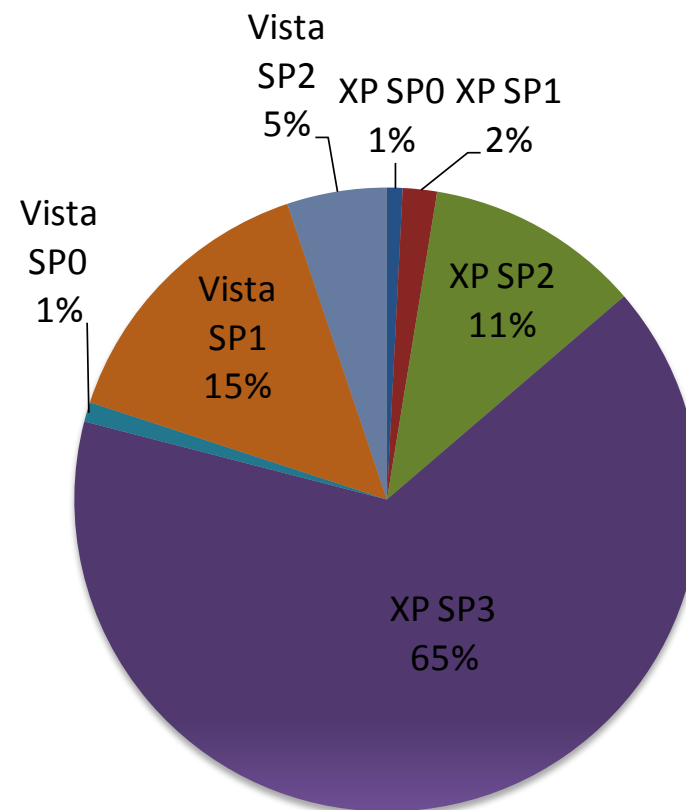
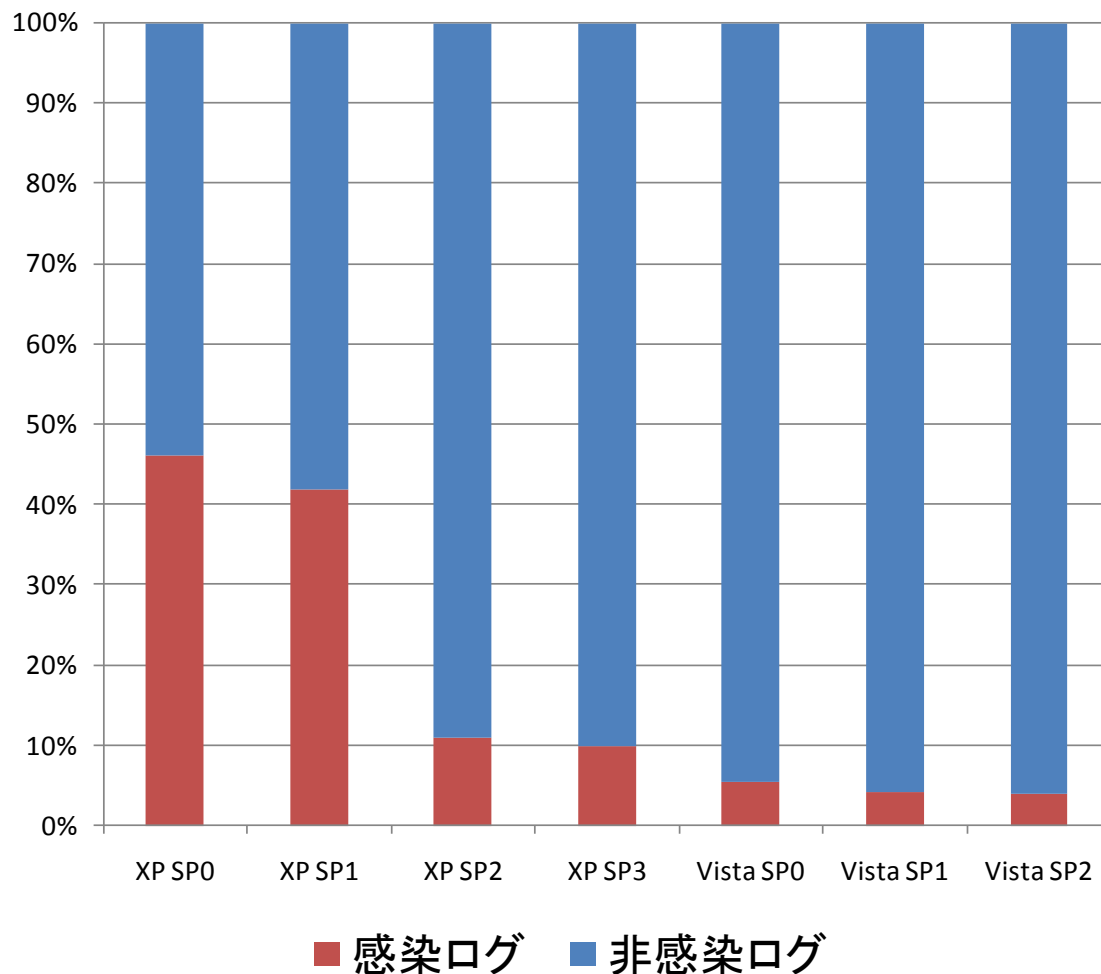
駆除ツールの検出状況送信機能で報告されるユーザの感染状況、ユーザのPC利用環境報告を集計することにより、感染者PCの実態を把握する。



インターネット接続形態による感染比率



集計期間: 2008年7月 - 2009年7月



集計期間: 2008年10月 – 2009年10月



Aさん



CCC 実行



CCC 実行(11日後)



CCC 実行(23日後)

[環境]

OS: Windows XP SP0
MEM: 386 MB
NETWORK: Global IP

2種類駆除

TROJ_MEREDROP.KM
TROJ_DLOADER.ETK

2種類駆除

TROJ_INJECT.AKH
BAT_DLOAD.XT

[環境]

OS: Windows XP SP0
MEM: 386 MB
NETWORK: Global IP

ログの送信が
ないため不明

[環境]

OS: Windows XP SP0
MEM: 1024 MB
NETWORK: Global IP

スキャンなし

感染なし

[環境]

OS: **Windows XP SP1**
MEM: 1024 MB
NETWORK: Global IP

3種類検出

Cryp_Virut-4
PE_VIRUT.D-2
PE_VIRUT.D-4



Bさん



CCC 実行



CCC 実行(1日後)



CCC 実行(10日後)

[環境]

OS: Windows XP SP1
MEM: 256 MB
NETWORK: Global IP

4種類駆除

TROJ_AGENT.VW
TROJ_DLOAD.XT
他 2件

6種類駆除

TROJ_AGENT.VW
TROJ_DLOAD.XT
他 4件

[環境]

OS: **Windows XP SP3**
MEM: 256 MB
NETWORK: Global IP

3種類駆除

WORM_ALLAPPLE.IK
BAT_DLOAD.XT
Mal_Allapple

■ ITセキュリティ予防接種(以後予防接種)とは

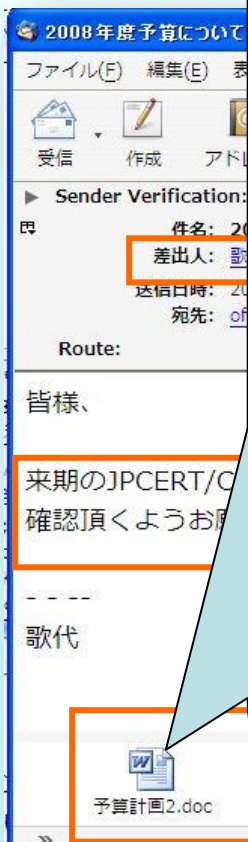
- 電子メールを用いた受動型攻撃に対するエンドユーザのセキュリティ意識の向上を目的とする調査・訓練の手法で、対象者に不審メールを模した無害なメールを送付し、適切な取扱いを行えるかを試すものである。

■ プロジェクトの目的

- 標的型攻撃対策としての予防接種の有効性を確認する。
- 予防接種を安全に実施するための手法を確立する。
- 被験者に対して以下をアンケートし、リスクグループを特定する。

- 年齢、性別、勤続年数、役職、雇用形態、ITリテラシー、使用しているメーカー、セキュリティ教育受講経験

-ITセキュリティ予防接種- 予防接種のコンセプト



本件に関するお問い合わせ先: ●●部 ●●、●●部 ●●

ご注意! このような怪しいメールの添付ファイルを不用意に開封すると
あなたを狙うウイルス等に感染する恐れがあります
(このメールは統計調査のためのものです)

本添付ファイルを届けたメールは、調査のために不審メールを模したもので、本文・件名に記載された内容は架空のものです。

調査結果は有限責任中間法人 JPCERT コーディネーションセンター(JPCERT/CC)に提供し、同様のメールによる脅威への予防活動に活用されます。結果は統計数値として取り扱われますので個人名等が公表されることは一切ありません。

調査精度を上げるため、各位に事前説明を行わずに送付しております。事後のお願いとなりますが、実施にご協力をいただけますよう、何卒よろしくお願い申し上げます。

本添付ファイルに危険性はありませぬ。ウイルス/ワームとしての機能はありません。

添付ファイルを開いた際にインターネット上の訓練用ウェブサイトに置かれた画像を読み込んで表示することで、添付ファイルのオープン状況の確認を行っています。

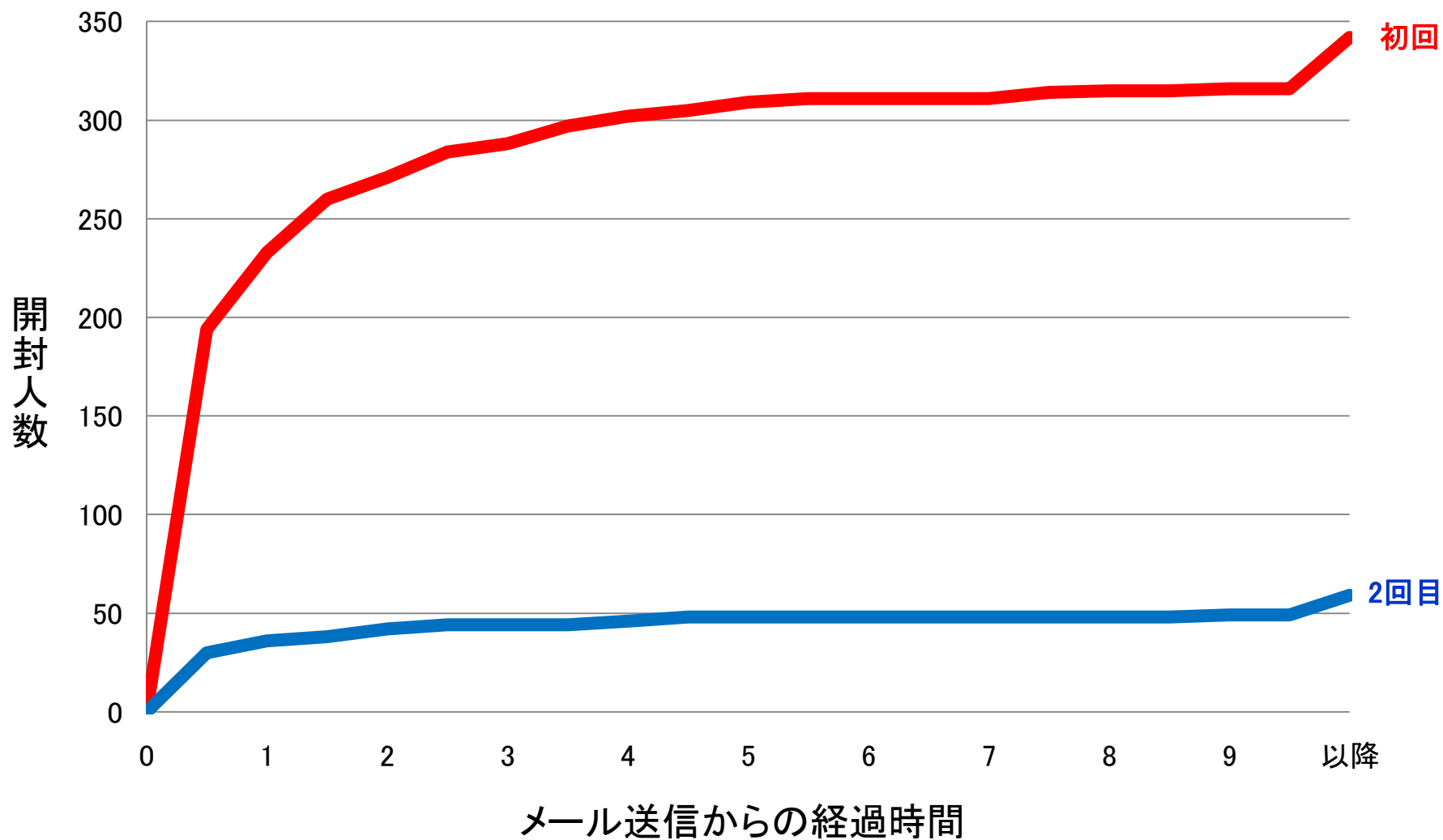
○不審なメールと添付ファイルがもたらす脅威(標的型攻撃):

近年、特定の組織・職員を狙う「不審なメールに添付ファイル(標的型攻撃)」が増加する傾向にあります。標的型攻撃の偽メールは、従来のウイルス対策ソフトでは検出されず、メールボックスまで直接届きます。もともと見えない画像ファイルへのリンクを埋め込むことで、ウイルス等への感染や情報漏洩被害を避けるためには、各自が不審なメールを見つけた際に、必ずしも開封せず、報告を行うことが重要です。

見えない画像ファイルへのリンクを埋め込む

<http://targeted.example.co.jp/user1.jpg>

—ITセキュリティ予防接種—
予防接種の効果

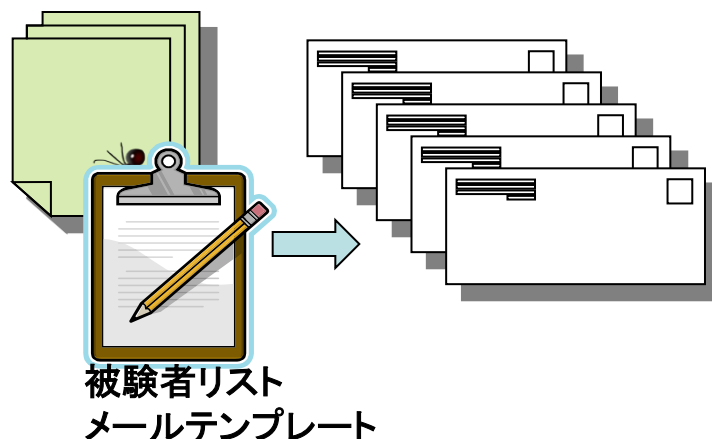
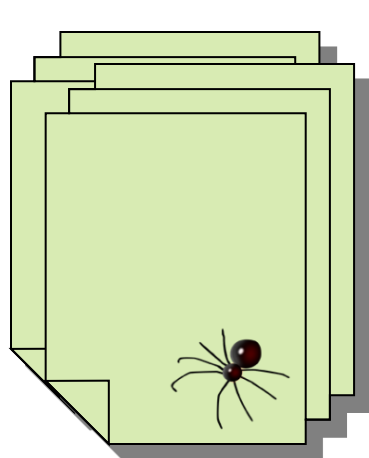


予防接種メール作成ツール

配送ツール

Webバグ挿入

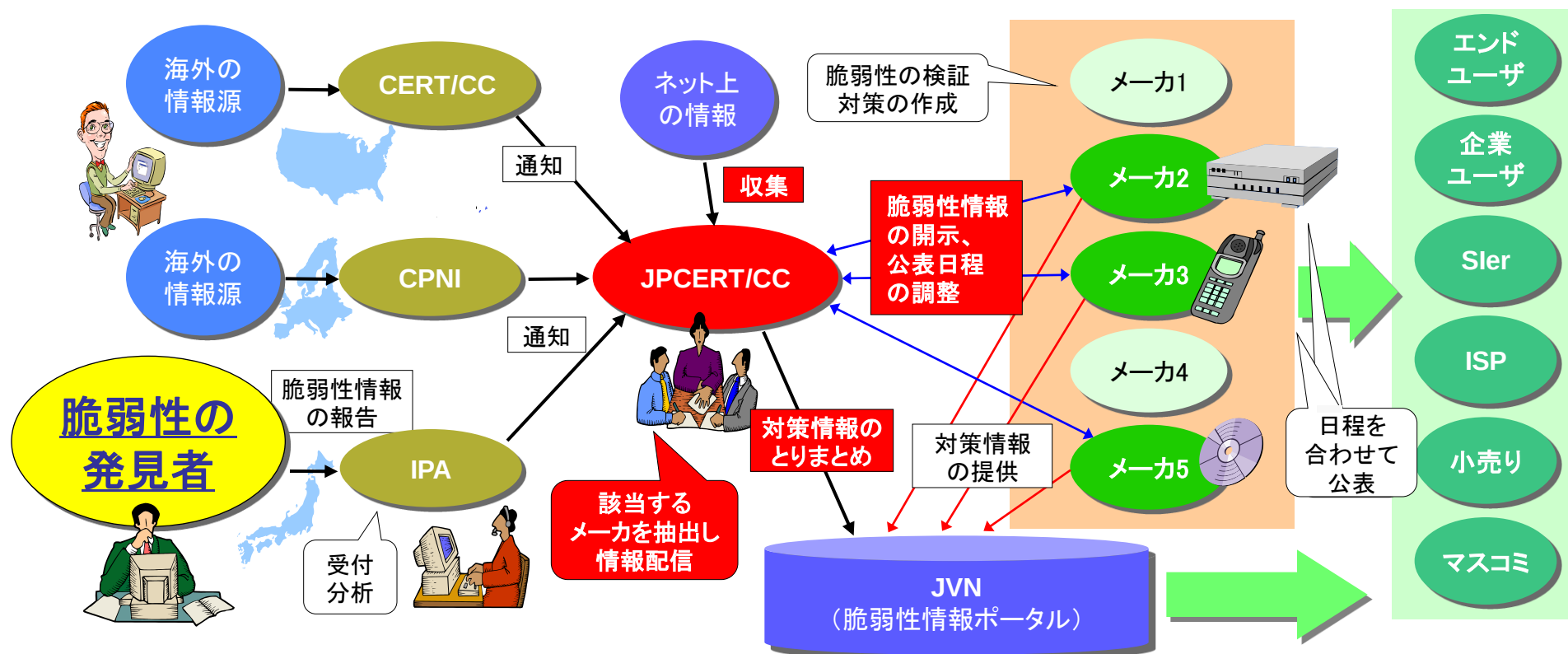
メール作成



無償、但しサポートは不可
お問い合わせは: office@jpcert.or.jpまで

- 脆弱性関連情報を、適切な関係者へ事前に開示し、被害を最小限に食い止めるためのプロセス
 - 未公開脆弱性情報の受付 ⇒ 検証 ⇒ 製品開発者に開示
 - 国外の関係機関(CERT/CC, CPNI等)と連携し、国内外の製品開発者へ情報展開
 - 関係するすべての製品開発者が同時に情報公開するよう調整
 - 脆弱性情報ポータルサイト(JVN)を運営し、脆弱性情報と各社の対応を公開

- 経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」に基づく活動
 - JPCERT/CCが調整機関として指定されている
 - JEITA, JNSA, JISA, CSAJ, IPA, JPCERT/CCが協同で「情報セキュリティ早期警戒パートナーシップ」ガイドラインを策定



Japan Vulnerability Notes - Windows Internet Explorer

https://jvn.jp/ Japan Computer Emergency Re... Google

お気に入り おすすめサイト Web スライス ギャラ...

Japan Vulnerability Notes

最終更新日: 2009/11/05 English

JVN Japan Vulnerability Notes

過去のお知らせ

新着リスト

JNVU#943857: 複数の TCP の実装におけるサービス運用妨害 (DoS) の脆弱性 [2009/11/05 15:07] (更新)

JVN#72974205: Roundcube Webmail におけるクロスサイトリクエストフォージェリの脆弱性 [2009/11/04 15:16]

JVN#75694913: Roundcube Webmail におけるクロスサイトリクエストフォージェリの脆弱性 [2009/11/04 15:00]

JVNTA09-294A: 緊急 Oracle 製品 における複数の脆弱性に対するアップデート [2009/10/29 17:24]

JVN#13011682: SEIL/X シリーズおよび SEIL/B1 におけるサービス運用妨害 (DoS) の脆弱性 [2009/10/28 15:00]

JVN#06362164: SEIL/X シリーズおよび SEIL/B1 におけるバッファオーバーフローの脆弱性 [2009/10/28 15:00]

JVN#75368899: IPv6 を実装した複数の製品にサービス運用妨害 (DoS) の脆弱性 [2009/10/27 13:17]

JVN#33822756: キヤノンITソリューションズ製 ACCESSGUARDIAN におけるクロスサイトスクリプティングの脆弱性 [2009/10/20 15:00]

JVN#23108985: 複数のサイボウズ製品におけるクロスサイトスクリプティングの脆弱性 [2009/10/15 15:00]

JVNTA09-286A: 緊急 Microsoft 製品 における複数の脆弱性に対するアップデート [2009/10/15 14:36]

JVNTA09-286B: 緊急 Adobe Reader および Acrobat における複数の脆弱性に対するアップデート [2009/10/15 14:36]

JNVU#257117: Adobe Reader および Acrobat の複数の JavaScript メソッドに脆弱性 [2009/10/14 16:20]

JNVU#276653: Microsoft Internet Information Services FTP サーバにおけるバッファオーバーフローの脆弱性 [2009/10/14 16:16]

JNVU#135940: 緊急 Windows SMB version 2 に脆弱性 [2009/10/14 16:16]

JNVU#676492: Wireshark の erf ファイル処理に脆弱性 [2009/10/07 16:30]

脆弱性レポート一覧

JVN

HOME

JVNとは

脆弱性レポートの読み方

脆弱性レポート一覧

VN-JP

VN-CERT/CC

VN-CPNI

TRnotes

JVN iPeDia

脆弱性対策情報データベース

JVNJS/RSS

ベンダ情報一覧

脆弱性情報の届出

お問合せ先

サイト運営組織

JPCERT/CC

JPCERTコーディネーションセンター

IPA/ISEC

情報処理推進機構セキュリティセンター

早期警戒パートナー

JEITA

社団法人電子情報技術産業協会

JISA

社団法人情報サービス産業協会

CSAJ

社団法人コンピュータソフトウェア協会

JNSA

NPO日本ネットワークセキュリティ協会

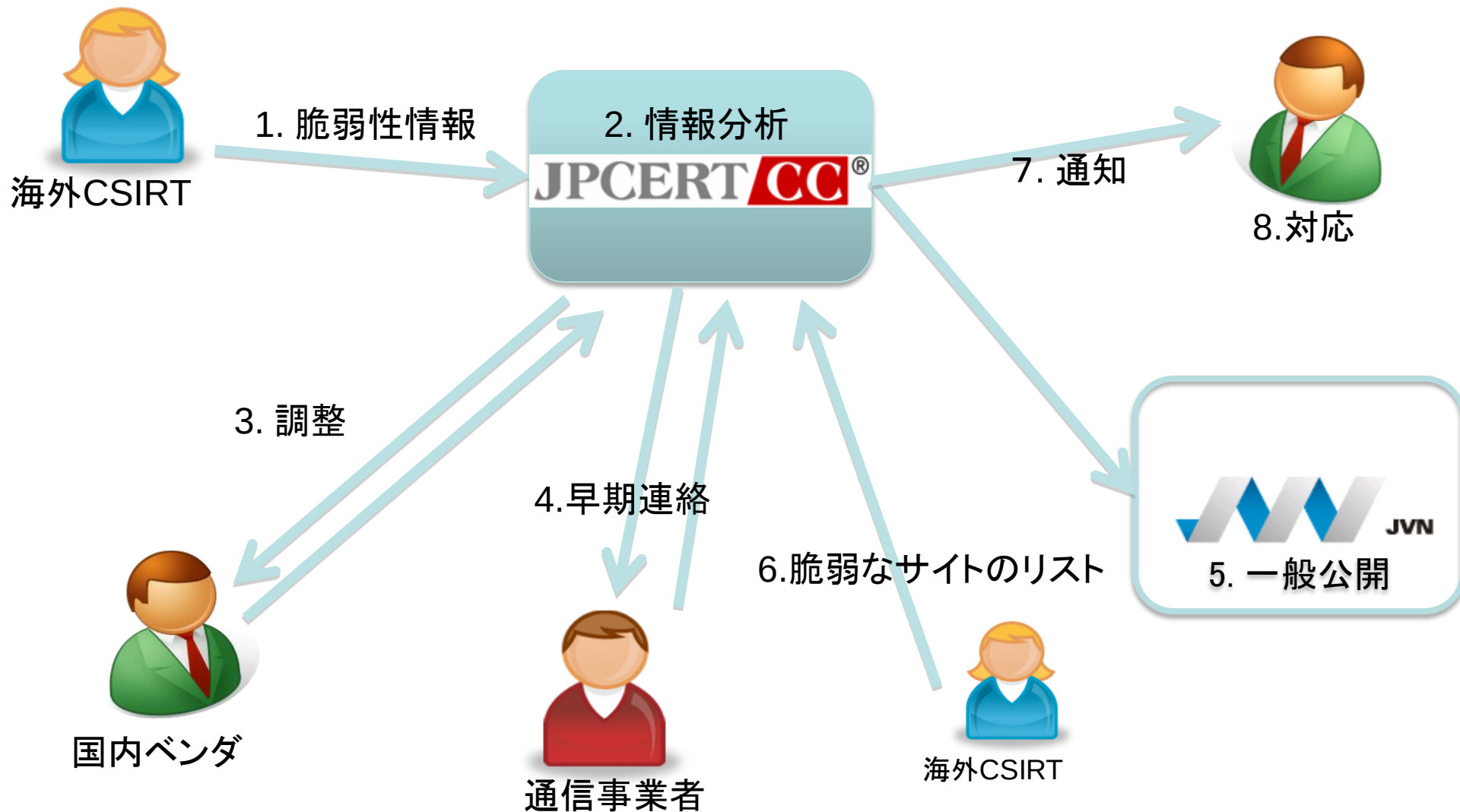
関連組織

CERT/CC

インターネット | 保護モード: 有効

- 隠しておくのは得策ではない
 - 情報公開により、脆弱性をユーザに周知し、対策の適用を促す
 - いずれ悪意の第三者が脆弱性を発見し、攻撃に利用される可能性
- 「公表日一致の原則」の遵守
 - 脆弱性情報と、対策情報を同時に公開する
 - 脆弱性の影響を受けるすべての製品開発者が同時に情報公開する
- すべての関係者が同時に情報公開するよう日程調整
 - 脆弱性の影響を受ける製品を開発するすべてのベンダ
 - 海外の調整機関や製品開発者を含む
 - 発見者の要望が影響する場合もある

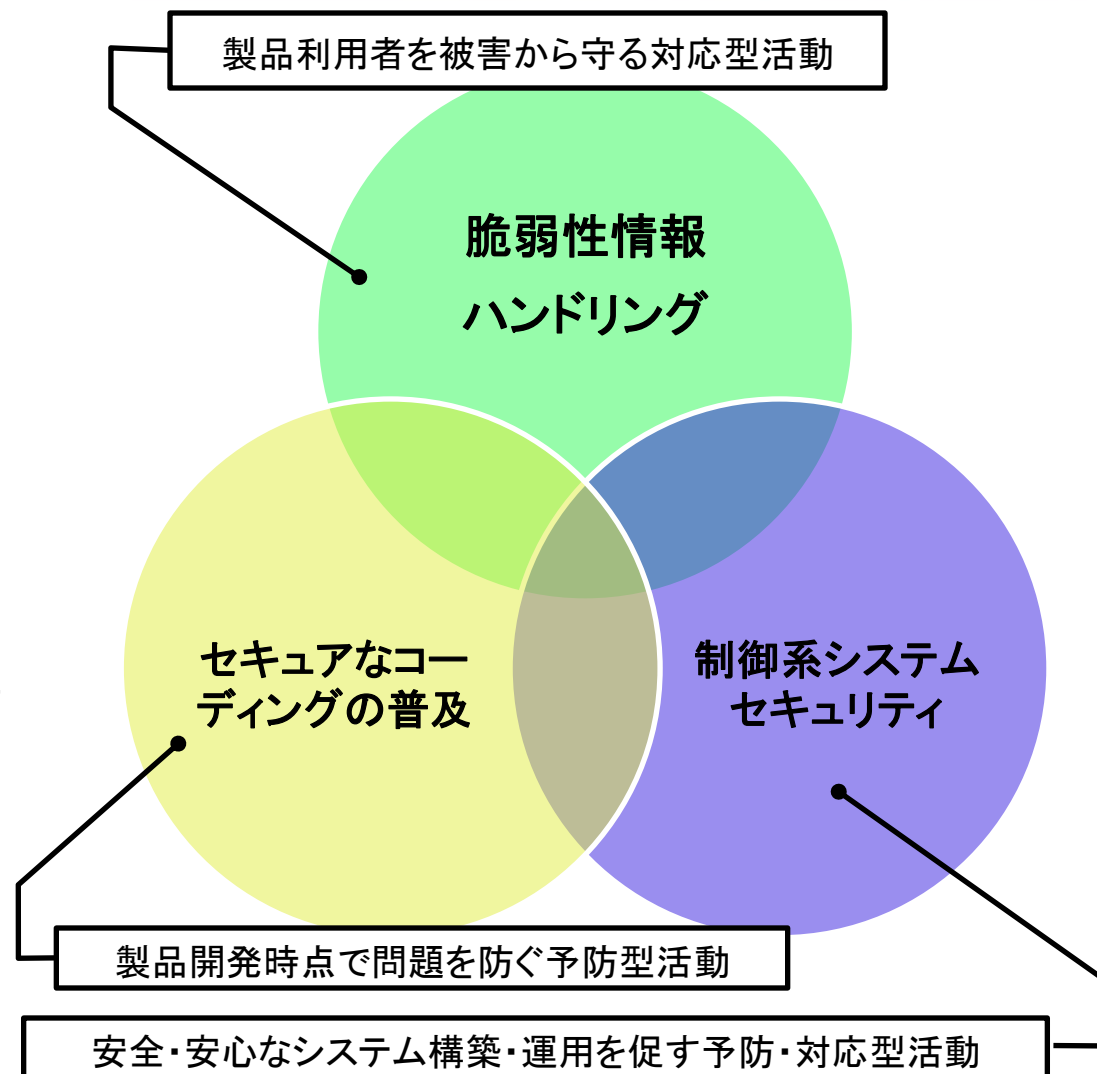
DNSキャッシュポイズニングの脆弱性



ソフトウェア等の脆弱性への取り組み

- 高度な情報処理を実現するICT環境に潜む脆弱性によって脅かされる、全ての利用者の安全を守る為に3つの観点から活動を行っています。

- ゼロデイの脅威から製品利用者を守る
⇒脆弱性情報ハンドリング
発見された製品や規格の脆弱性が、対策も取られないまま公になる前に、拡大する被害を未然に防ぐための活動
- 正しいコーディング方法を広め、安全な製品開発を促す
⇒C/C++セキュアコーディング
不十分な理解によりコーディングされた脆弱なソフトウェア製品がもたらす脅威を未然に防ぐための活動
- 安全・安心なシステムの開発・運用を促す
⇒制御系システムセキュリティ
汎用IT製品が導入された事によって、その脅威にさらされ始めた制御系システムにおいて、安全・安心な環境を維持する為の開発・運用を促す活動



ま と め

■ 今日の流れは今後も

ー 対策側: 分断・孤立

- ソーシャルエンジニアリング的手法

- 役割を持った多段化

ー 攻撃側: 分業・連携

- ツールによる簡易化

- 合わせ技: 量(弱い対象)と質(強い対象), コンピュータ以外のメディア

■ 非技術的な問題

ー ガラパゴス化

- フィッシングや標的型攻撃

ー 過度の社会的制裁、個人情報過敏症

- 行き過ぎると恰好の餌食に

お問い合わせ、インシデント対応のご依頼は

JPCERT **CC**®

JPCERT **CC®**
Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター

安全・安心なIT社会のための、国内・国際連携を支援する

▶ お問い合わせ ▶ サイトマップ ▶ English

Home

サイト内検索

検索

トップページ

情報提供

- ・ 注意喚起
- ・ 早期警戒
- ・ 脆弱性対策情報
- ・ Weekly Report

各種届出・申込

制御システムセキュリティ

ラーニング

公開資料

- ・ 四半期レポート
- ・ 研究・調査レポート
- ・ CSIRTマテリアル

イベント

プレスリリース

JPCERT/CC

関連組織



JPCERT/CCはFIRSTのチームメンバーです。またJPCERT/CCスタッフがSteering CommitteeメンバーとしてFIRSTの運営に協力しています。



JPCERT/CCはAPCERTの事務局です。

注意喚起

深刻に影響範囲の広い、情報セキュリティ上の脅威など最新のセキュリティ情報を配信しています。

JPCERTコーディネーションセンター

— Email: office@jpcert.or.jp

— Tel: 03-3518-4600

— Web: <http://www.jpcert.or.jp/>

過去の注意喚起

脆弱性関連情報

ソフトウェアなどの脆弱性と対策情報をJVNより提供しています。

インシデント報告

— Email: info@jpcert.or.jp

— Web: <http://www.jpcert.or.jp/form/>

詳しく見る

Weekly Report

2009-06-17日

HTTPS RSS



発生元への「調整」を依頼したいインシデントを「報告」したい

ISDAS
[インターネット定点観測]



インターネット上に設置したセンサーにより、セキュリティ上の脅威となるトラフィックを観測しています。

お薦めページ



教育担当者が使える、新入社員などが身につけておくべきセキュリティ知識などを紹介しています。

イベント

・第21回 FIRST Annual Conference 京都 参加申し込み受付中

・O/C++ セキュアコーディング ハーフデイキャンプ参加申し込み