資料4

「サイバークリーンセンター（CCC）」における ボットウイルス対策について

平成23年1月25日

政策統括官（情報通信担当）
情報セキュリティ対策室

サイバー攻撃

「サイバー攻撃」の手法

※インターネットを介したものが主だがマルウェア感染手法としてUSBなど可搬型メディアを使う場合あり

◆不正アクセス

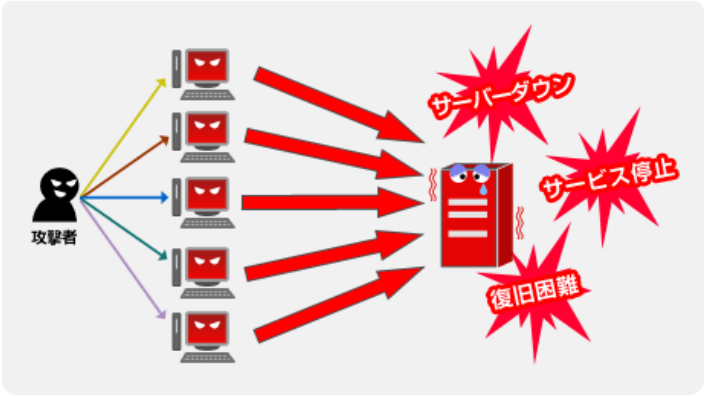
・不正に入手したパスワードを用いたり、脆弱性を突く等して、情報システムにアクセスする

◆マルウェア感染 （ウィルス等の悪意あるソフトウェア）

・メールにウィルスを添付したり、ネットワークを介して、ウィルスのパソコンへの送り込み等を行う

◆業務妨害攻撃（DDoS攻撃）Distributed Denial of Service

・マルウェア（ボット）に感染した多数のパソコン等を踏み台として、大量のデータを情報システムに送信する



マルウェア感染PC

攻撃者に操られる

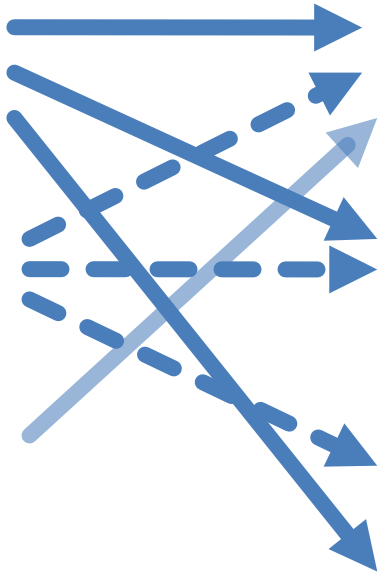
各種サービスサーバー

-ホームページ提供

-電子商取引（ネットショップ）

-掲示板等

情報システムの被害



➢機能不全

・情報システムが機能しなくなる（例：サーバのダウンによりウェブサイトが閲覧できなくなる）

➢改ざん

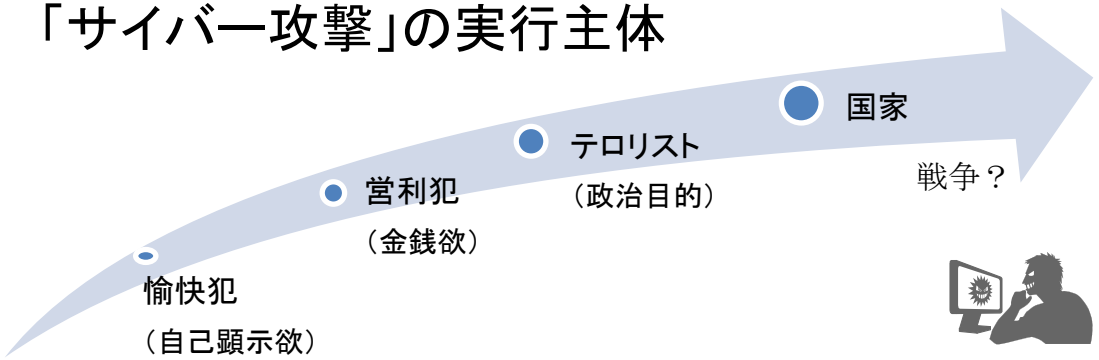
・ウェブサイトに本来の画像とは異なる画像が埋め込まれる

・人間が視認できないリンク（悪性サイトへつながる）が貼られる

➢情報窃取

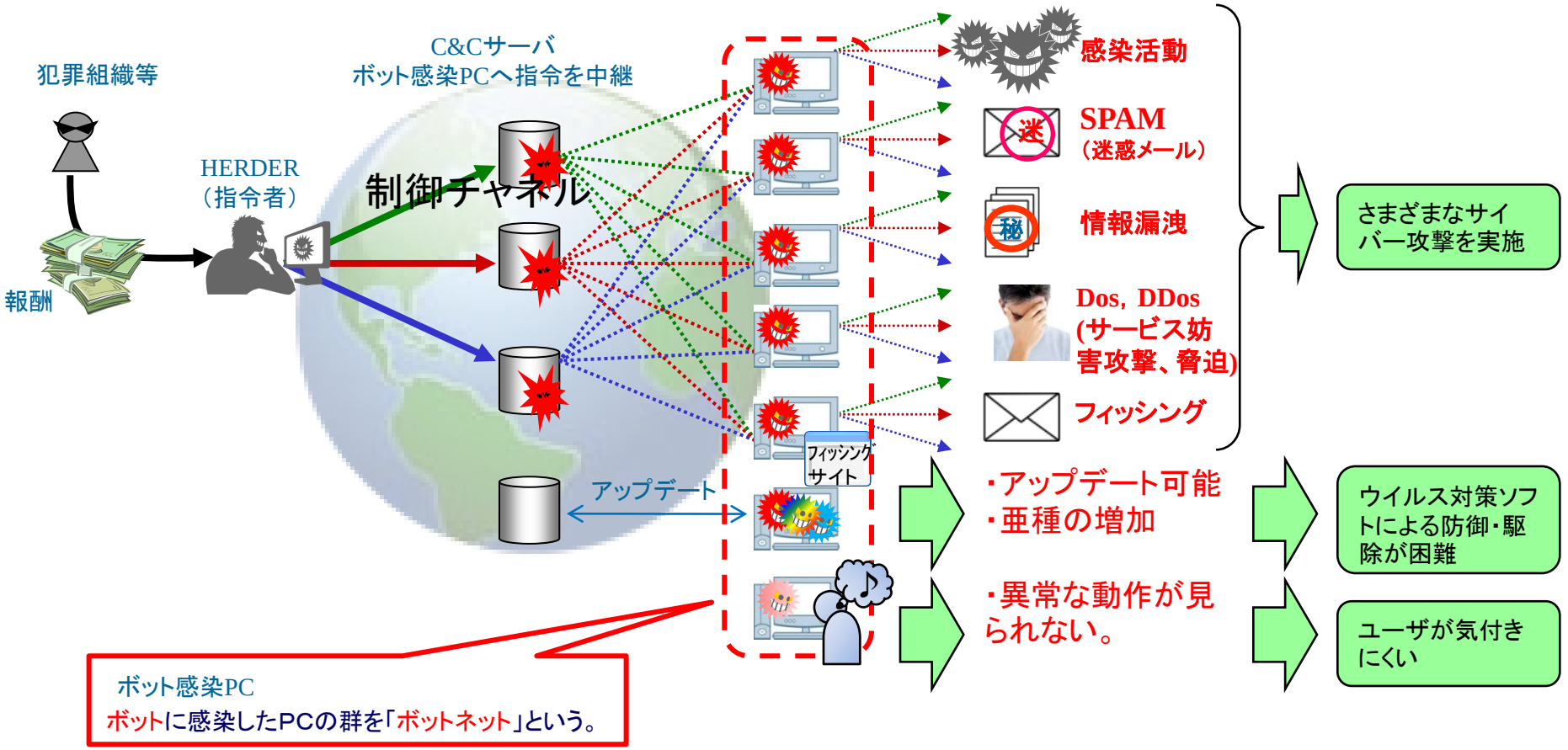
・情報システム内に蔵置されているデータが盗み取られる

「サイバー攻撃」の実行主体



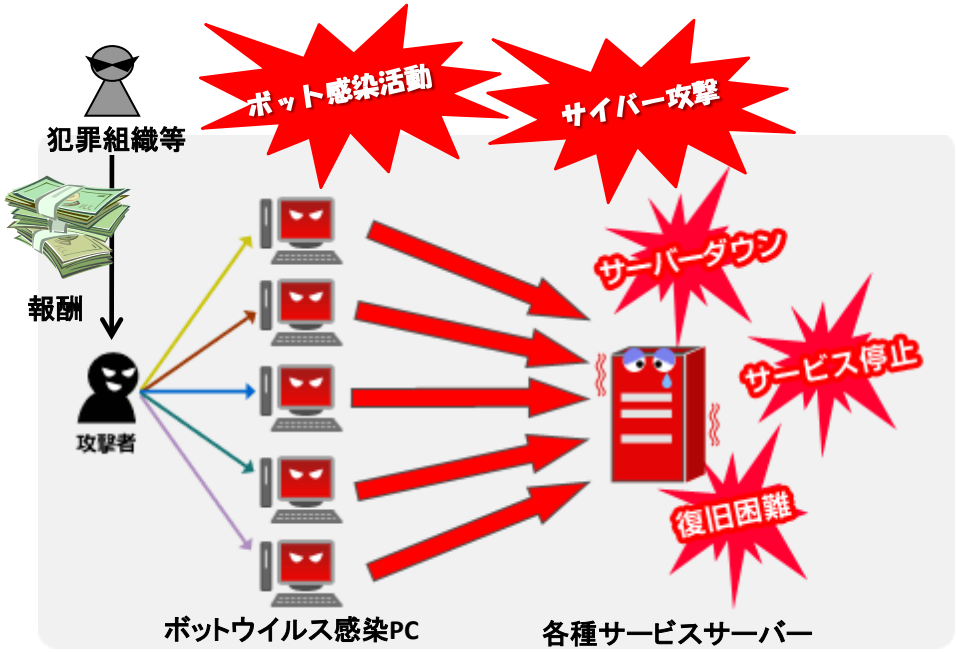
ボットとは

■ボットネットを構築し、悪意の管理者からの命令により、様々なサイバー攻撃を協調して実施。
■命令に従いアップデート（新しいボットプログラムの導入）する機能や、数多くの亜種が存在。
■感染したPCは異常な動作をしているようには見えない。



ボットウイルス感染PCの問題点

◆ボットウイルス感染PCは、他のPCに感染活動を行い感染被害を拡大。
◆多数のボットウイルス感染PCで形成されるネットワーク(ボットネット)を操り、サイバー攻撃に利用。
◆ブラックマーケットが存在し、ビジネス化。



◆大規模サイバー攻撃による被害例

2007年 4月	エストニアの政府機関やメディアなどの Web サイトが サービス停止に追い込まれた。
2008年 8月	グルジアの政府機関などのWebサイトがDDoS攻撃を受け、アクセス不能な状態に陥った。
2009年 7月	米韓の政府主要サイトが一斉に攻撃を受け、韓国では数日にわたりサイトへのアクセスが不能になった。


電脳攻撃 見えぬ敵
米韓 政府サイトなど被害
ウイルス感染2万台
北朝鮮説 証

朝日新聞(2009/7/11)


サイバー攻撃 韓国大混乱
危機管理の課題露呈
整ったネット環境 裏目
北の部隊 1000人規模

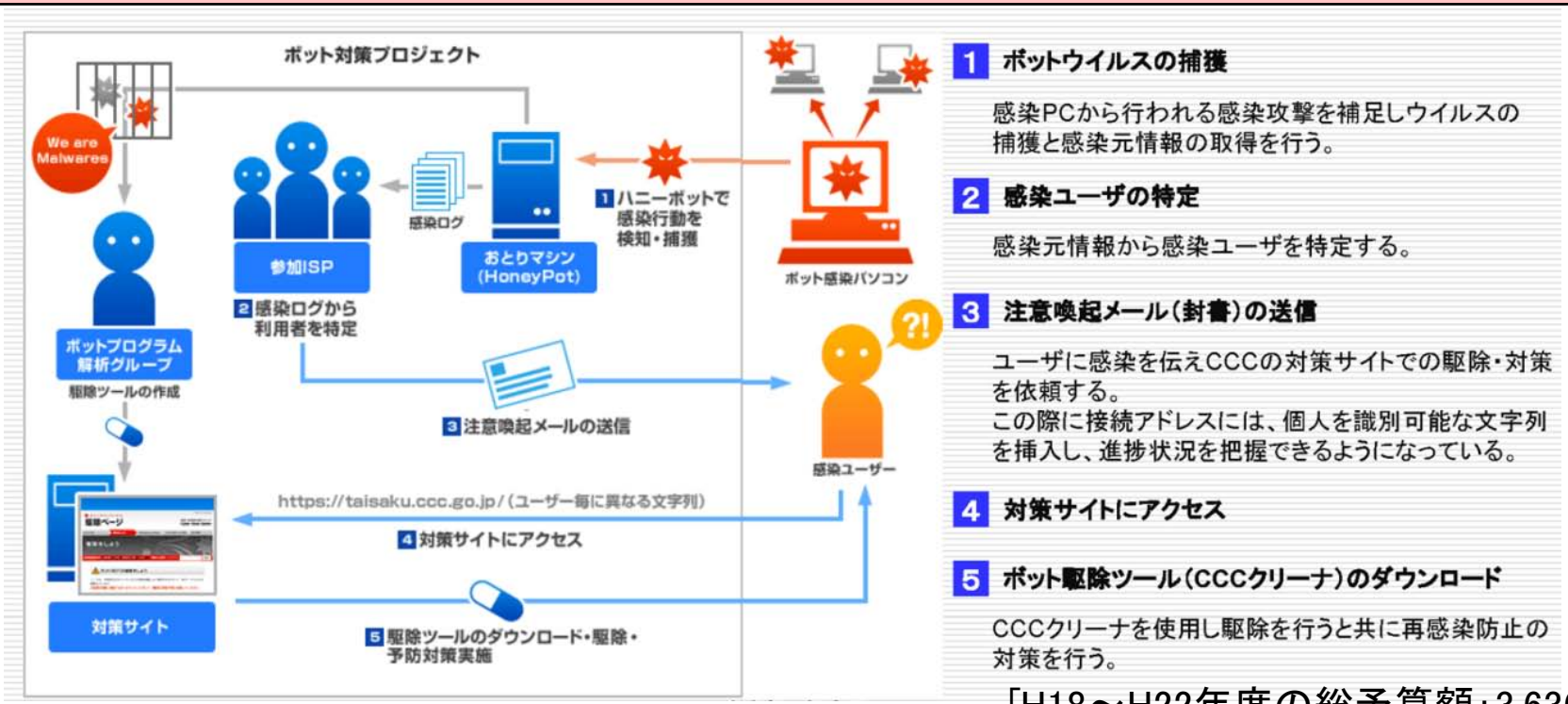
読売新聞(2009/7/11)

サイバークリーンセンター（CCC）による取組み（H18～H22）

◆ハニーポットを用いて、1日平均25種の新種ボットウイルスを発見し、ウイルス対策ソフトに反映。

◆1日平均438人の感染者を発見し、参加ISP（76社）が感染者にウイルス駆除、WindowsUpdate等の対策実施を勧奨。

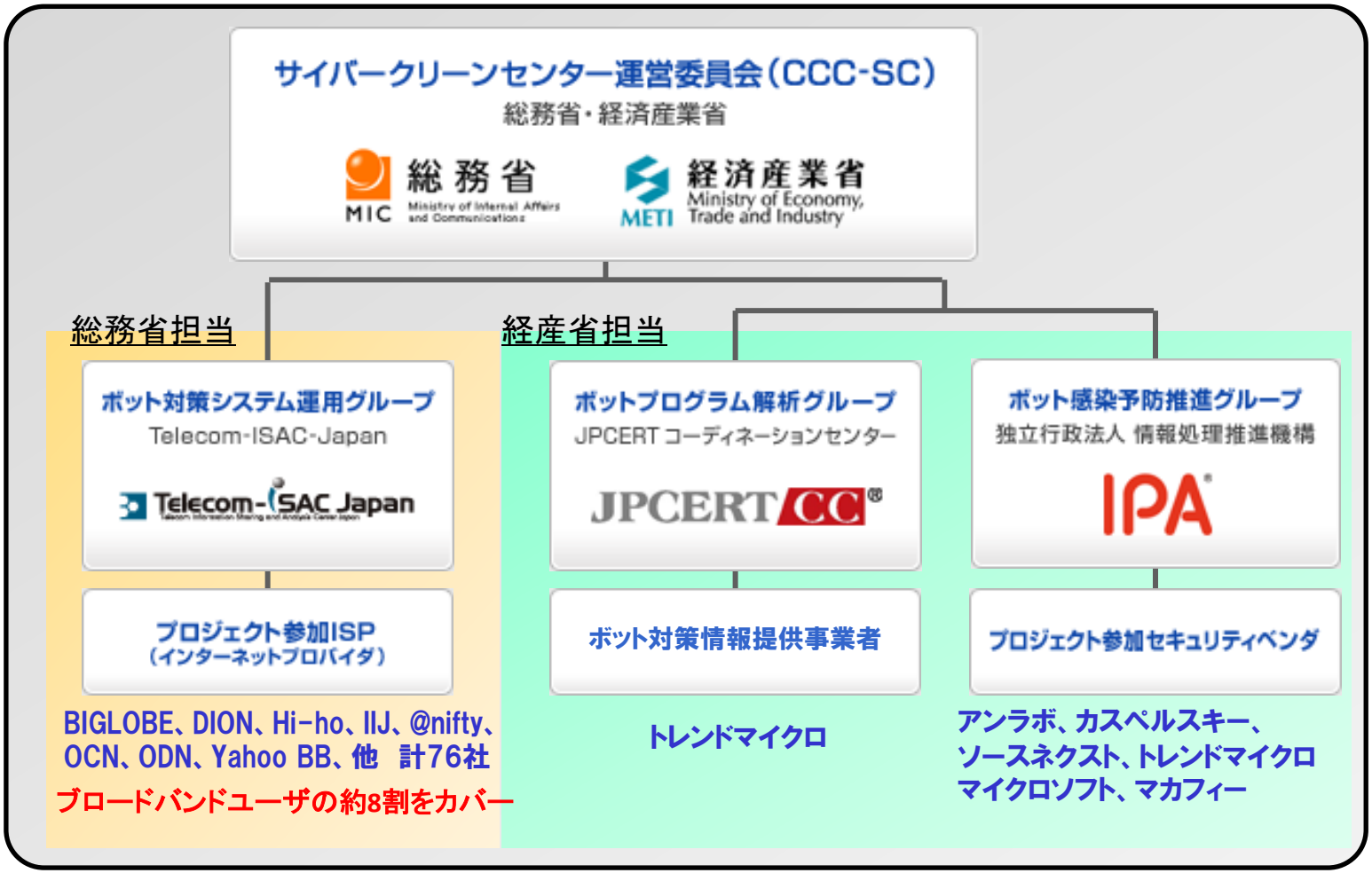
◆ウイルス駆除ツールをウェブサイトで提供し、インターネット利用者の自発的なウイルス駆除等の実施をサポート。
（CCCのホームページの1日平均アクセス数：12,722件、駆除ツールの1日平均ダウンロード回数 ：1,110回）



［H18～H22年度の総予算額：3,636百万円］

サイバークリーンセンターの運営体制

◆総務省、経済産業省の共同プロジェクト。
◆国内ブロードバンドユーザの約8割をカバーする76社のISPが参加。



CCCの成果、国内外での評価・報道

◆ボットウイルス感染率が、5年間で、2～2.5%⇒0.6%に軽減。
◆郵送による注意喚起の導入等により、注意喚起ユーザの各種対処行動の実施率が向上

年度		2005		2007	2008	2009	2010
ボットウイルス感染率		2-2.5% (2000万人中 40-50万人)		ー	1% (3000万人中 30万人)	ー	0.6% (3170万人中 19万人)
注意喚起ユーザの対処行動	CCCサイトアクセス率	ー		36%	49%	59%	71%
	駆除ツールダウンロード率	ー		30%	30%	35%	45%
駆除ツールダウンロード数	単年度	ー		7,895	10,439	5,630	1,092 (7月時点)
	累計	ー		7,895	18,334	23,964	25,056 (7月時点)

◆ホームページにて情報公開
・毎月の検体収集数等の活動実績報告(日本語、英語)
・毎年度の活動報告書(日本語、英語)

◆在日米国商工会議所(ACCJ)
・「インターネット・エコノミー白書2009年」にて、CCCの取り組みにより日本のコンピュータによるサイバー攻撃が激減していることを指摘。

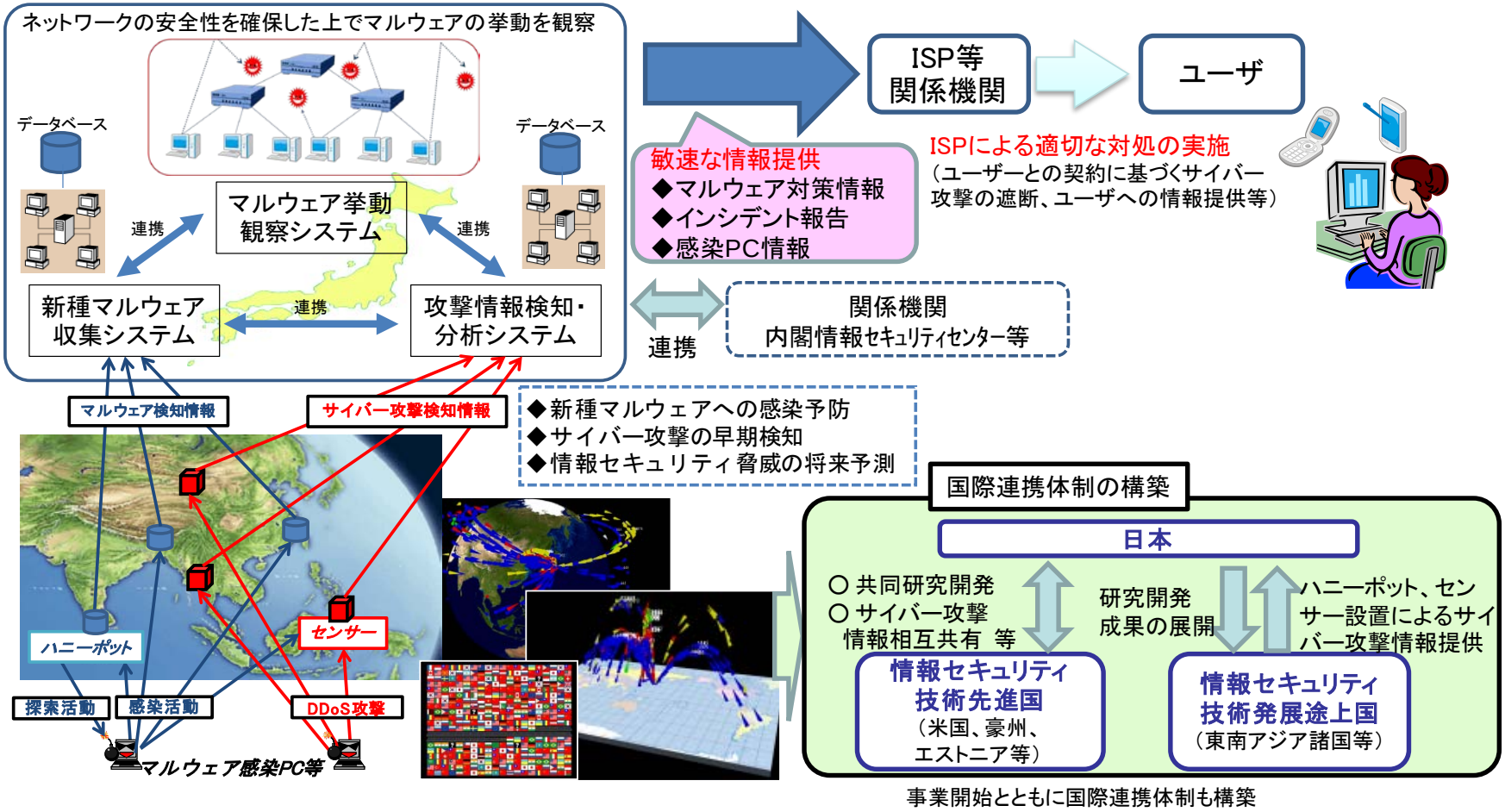
◆マイクロソフト社
・「Microsoft Security Intelligence Report Volume7(2009年)」にて、日本のウイルス感染率が他国に比べ低い理由としてCCCの取組みを指摘

◆国内TV報道で紹介
・NHK総合「クローズアップ現代」
・NHK教育「ITホワイト・ボックス」
・TV東京「ワールド・ビジネス・サテライト」
・フジテレビ「めざましTV」等

H23年度実施するCCCの後継施策

国際連携によるサイバー攻撃予知・即応技術の研究開発（H23年度予算額：629百万円）

◆サイバー攻撃に関する情報収集ネットワークを国際的に構築し、米国、豪州、APEC諸国をはじめとする諸外国と協力して、サイバー攻撃に対抗するための研究開発を実施し、日本におけるサイバー攻撃等のリスクを軽減。



事業開始とともに国際連携体制も構築