資料2

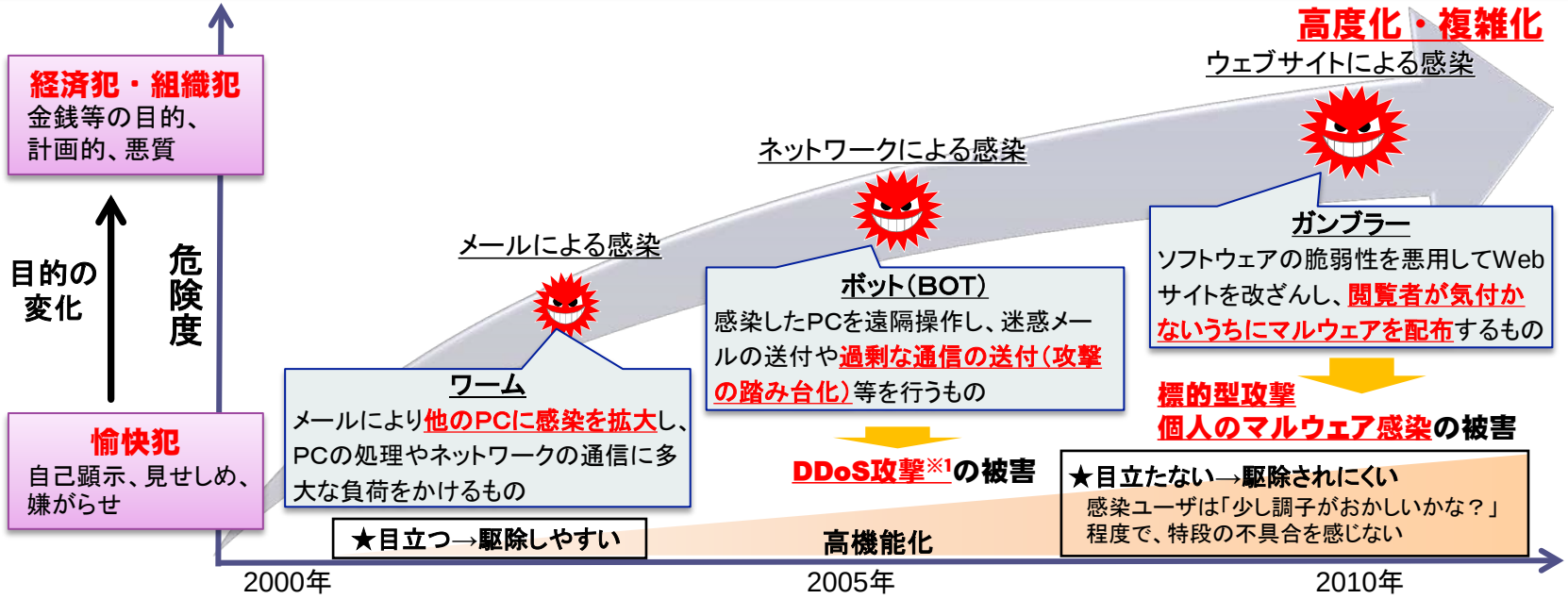
総務省
MIC Ministry of Internal Affairs and Communications

「電気通信事業におけるサイバー攻撃への適正な対処に関する研究会」について

平成25年11月29日
事　　務　　局

情報セキュリティ上の脅威の増大

インターネット等の情報通信技術は社会経済活動の基盤であると同時に我が国の成長力の鍵であるが、昨今、情報セキュリティ上の脅威の多様化・悪質化により、その被害が深刻化。



マルウェア※2の悪質化による脅威の増大

※1：DDoS攻撃：分散型サービス妨害攻撃（Distributed Denial of Service）のこと。多数のコンピュータから一斉に大量のデータを特定宛先に送りつけることにより、当該宛先のネットワークやサーバを動作不能にする攻撃。

※2マルウェア：コンピュータウイルスのような有害なソフトウェアの総称

サイバー攻撃による被害の例

11年10～11月・・・衆参両院のサーバやパソコンが情報収集型のウイルスに感染していたことが報道、ID・パスワードが流出したおそれ。（標的型攻撃）

12年6月・・・国際ハッカー集団「アノニマス」により、財務省、国土交通省のウェブサイトが一時アクセスしづらい状態が発生。（DDoS攻撃）

12年9月・・・中国からのサイバー攻撃により、最高裁判所、文化庁等のウェブサイトが一時アクセスしづらい状態が発生。（DDoS攻撃）

12年9月・・・ウイルスに感染したPCが第三者により遠隔操作され、掲示板に違法な書込みが行われたことでPCの所有者が誤認逮捕。（個人のマルウェア感染）

12年10月・・・ウイルス感染により、ネットバンキングにログインした利用者のPCの画面に偽画面が表示され、ID・パスワードが窃取。これにより、数百万円の不正送金が発生。（個人のマルウェア感染）

13年1月・・・農林水産省のPCが遠隔操作型のウイルスに感染し、TPPに関する機密文書が窃取されたおそれがあることが報道。（標的型攻撃）

情報セキュリティに関する総務省の主な予算施策（H24補正及びH25当初）

課題

標的型攻撃

標的型攻撃等の巧妙化するサイバー攻撃により、政府機関、民間企業等において機密情報漏えい等の被害が発生する事態が頻発。

個人のマルウェア感染

個人利用者においても、ウェブサイト等からのマルウェア感染により、ネットバンキングの不正送金などの実被害が発生。

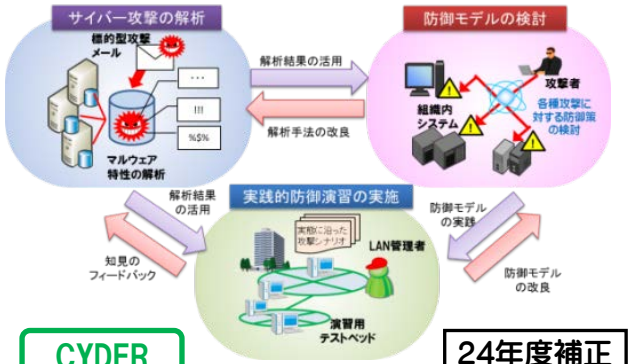
分散型サービス妨害攻撃（DDoS攻撃）

海外を主な発信源とするDDoS攻撃等により、政府機関等のウェブサイトのアクセス障害や改ざん等が頻発。

実証実験

サイバー攻撃解析・防御モデル実践演習

標的型攻撃等の新たなサイバー攻撃の解析による実態把握、防御モデルの検討、官民参加型の実践的な防御演習による人材育成を実施。

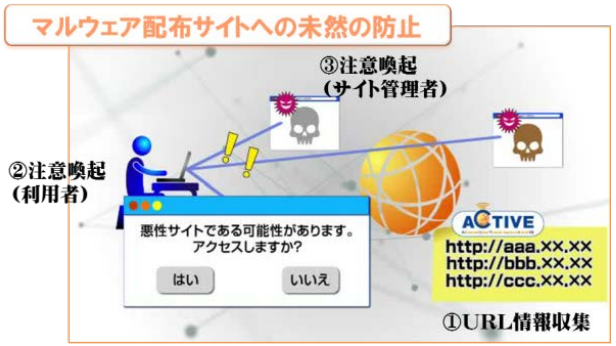


CYDER

24年度補正
15.2億円

ACTIVE（Advanced Cyber Threats response InitiatiVE）官民連携による国民のマルウェア感染対策

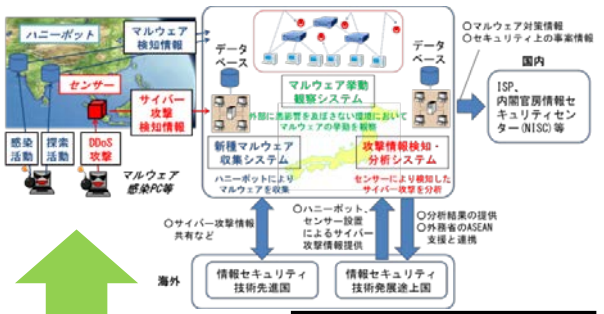
ISP等と連携し、インターネット利用者を対象に、マルウェア配布サイトへのアクセスの未然防止など総合的なマルウェア感染対策を行うプロジェクト。



25年度
4.8億円

PRACTICE（Proactive Response Against Cyber-attacks Through International Collaborative Exchange）

諸外国と連携してサイバー攻撃に関する情報を収集するネットワークを構築し、サイバー攻撃の発生を予知し即応を可能とする技術の研究開発及び実証実験。



PRACTICEの
基盤技術として支える

23年度　6.3 億円
23年度補正　5.6 億円
25年度　5.8 億円

NICT研究開発

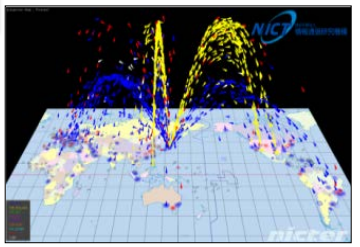
NICT施設整備補助金

潜在型マルウェアの検知技術等、革新的な情報セキュリティ技術の研究開発・実証実験施設をNICTに整備。

24年度補正
100億円

NICTER（Network Incident analysis Center for Tactical Emergency Response）リアルタイムネットワーク観測・分析

NICTにおいて、サイバー攻撃観測・分析網により、サイバー攻撃の状況をリアルタイムで把握し、分析するシステムを構築。



NICTER

ISPとの官民連携によるサイバー攻撃対応方策の変遷

マルウェアの変遷

ボット

インターネットにつないだだけで、インターネット利用者の知らない間に感染するボットが主流。

Drive-by-download

Webを見ただけで感染するWeb感染型マルウェアが台頭。

より高度で多様なマルウェア

より高度で多様なマルウェアが次々と出現。

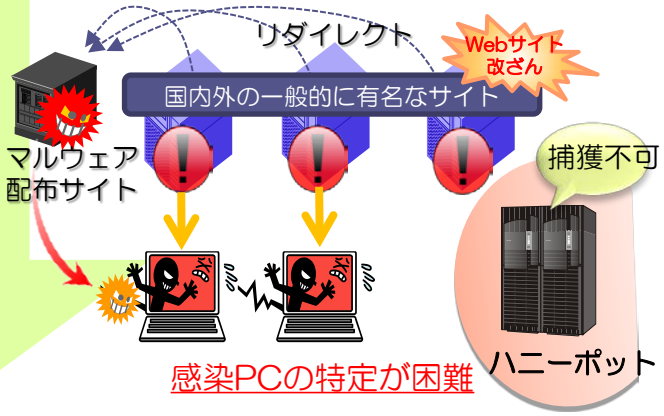
ネットワーク感染型マルウェア

ネットワーク経由で感染するマルウェア。ハニーポットにて捕獲可能。

感染PCの特定が可能

Web感染型マルウェア

Webサイトへのアクセスにより感染するマルウェア。ハニーポットでの捕獲ができないため対策が必要。



感染PCの特定が困難

対応方策の変遷

Cyber Clean Center

2006～2010

ボット対策プロジェクト

Advanced Cyber Threats response InitiatiVE

2013～2017

マルウェア感染防止・駆除の取組

サイバー攻撃への対処における通信の秘密との関係について

- サイバー攻撃への対策を実施するにあたっては、攻撃に係る通信に関する情報の取得・利用が必要となる場合があり、「通信の秘密」について留意することが必要。
- 「通信の秘密」の保護は、個人の私生活の自由を保護し、個人生活の安寧を保障する（プライバシーの保護）とともに、通信が人間の社会生活にとって必要不可欠なコミュニケーション手段であることから、憲法上の基本的人権の一つとして、憲法第21条 第2項において保障されているもの。
- 日本国憲法の規定を受け、電気通信事業法において、罰則をもって「通信の秘密」を保護する規定が定められており、電気通信事業法上「通信の秘密」は厳格に保護されている。

通信の秘密について

日本国憲法

第２１条　２　検閲は、これをしてはならない。**通信の秘密はこれを侵してはならない。**

電気通信事業法

（秘密の保護）

第４条　**電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。**

※　「通信の秘密」とは、①個別の通信に係る通信内容のほか、②個別の通信に係る通信の日時、場所、通信当事者の氏名、住所・居所、電話番号などの当事者の識別符号、通信回数等これらの事項を知られることによって通信の意味内容を推知されるような事項すべてを含む。

第１７９条　電気通信事業者の取扱中に係る通信（第１６４条第２項に規定する通信を含む。）の秘密を侵した者は、２年以下の懲役又は１００万円以下の罰金に処する。

２　電気通信事業に従事する者が前項の行為をしたときは、３年以下の懲役又は２００万円以下の罰金に処する。

３　前２項の未遂罪は、罰する。

通信の秘密が侵害されない又は侵害が許容される場合

①通信当事者の「同意」がある場合

②正当防衛、緊急避難、正当業務行為等の違法性阻却事由がある場合

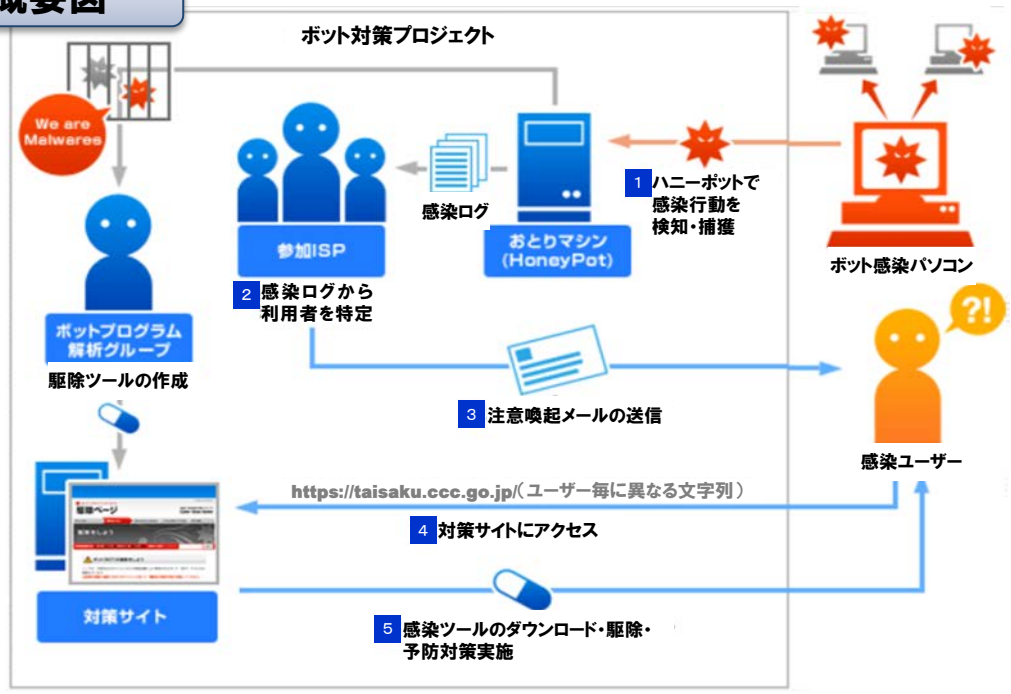
サイバークリーンセンター（CCC）について　－ボットウイルス対策プロジェクト－

○　平成18年12月より経産省との連携の下、情報セキュリティ関係機関のオールジャパン体制として「**サイバークリーンセンター（CCC）**」を組織し、サイバー攻撃の踏み台等となるボットウイルス撲滅に向けた取組を実施。

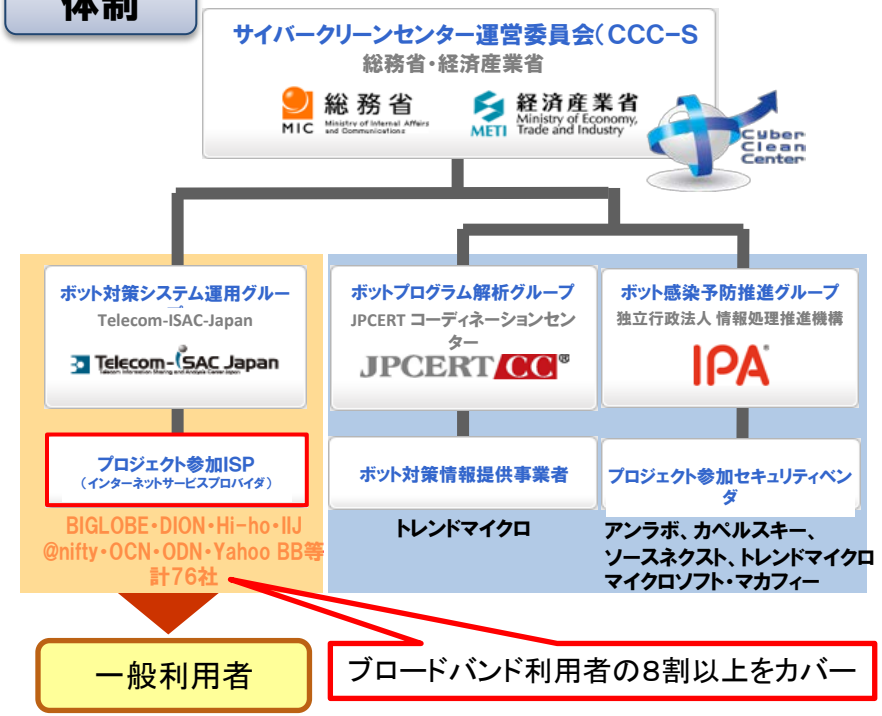
○　ボットウイルス感染者に対して参加ISP（76社）が注意喚起を実施し、ウイルス駆除、Windows Update等の対策実施を勧奨。

○　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。

概要図



体制



通信の秘密との関係

①　CCCの事務局が、ボットウイルス感染パソコンからハニーポットに来た通信における送信元IPアドレス（ダイナミックIPアドレス）を参加ISP（当該IPアドレスの割当てを行っているISP）に提供すること

⇒CCCの事務局はボットウイルス感染パソコンからの**通信を受信する一方当事者であり、通信の秘密の侵害にあたらない**と考えられる。

②　参加ISPが、当該IPアドレスをどの契約者に割り当てたか顧客情報と突合し、該当契約者を割り出すこと

⇒**ボットウイルス感染パソコンに対する現在の危難を避けるための緊急避難として、通信の秘密の侵害に係る違法性は阻却される**と考えられる。

ACTIVE（Advanced Cyber Threats response InitiatiVE）について

■ 平成25年11月からインターネットサービスプロバイダ（ISP）等との協力により、インターネット利用者を対象に、マルウェア配布サイトへのアクセスを未然に防止する等の実証実験を行う官民連携プロジェクト（ACTIVE）を開始。

（１）マルウェア感染防止の取組

① マルウェア配布サイトのURL情報をリスト化。
② マルウェア配布サイトにアクセスしようとする利用者に注意喚起。
③ マルウェア配布サイトの管理者に対しても適切な対策を取るよう注意喚起。

通信の秘密との関係

ISP等が、利用者がアクセスしようとするサイトのURLの情報を知得し、注意喚起を行うことについては、利用者の同意に基づいて行われており、通信の秘密の侵害にあたらない。

（２）マルウェア駆除の取組

① マルウェアに感染した利用者のPCを特定。
② 利用者に適切な対策を取るよう注意喚起。
③ 注意喚起の内容に従いPCからマルウェアを駆除。

通信の秘密との関係

① ACTIVE事務局が、マルウェア感染パソコンからハニーポットに来た通信における送信元IPアドレスを、当該IPアドレスの割当てを行っているISPに提供することは、ACTIVE事務局は当該通信を受信する一方当事者であり、通信の秘密の侵害にあたらないと考えられる。

② 上記ISPが、当該IPアドレスをどの契約者に割り当てたか顧客情報と突合し、該当契約者を割り出す行為は、マルウェア感染パソコンに対する現在の危難を避けるための緊急避難として、通信の秘密の侵害に係る違法性は阻却されると考えられる。

「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」の開催

現状

■ 情報通信技術の発展に伴い、サイバー攻撃の手法が巧妙化・複雑化。これにより、以下の被害が発生。
① システムの破壊・停止、データの改ざん　② 情報窃取・漏洩　③ 更なる攻撃の踏み台化

■ 主なサイバー攻撃に対するプロバイダによる対策は次のとおり。

・ **マルウェア配布サイトへのアクセスによるマルウェア感染の拡大**
→ 利用者からの同意に基づき、マルウェア配布サイトへアクセスする通信を検知し、**攻撃対象に注意喚起・遮断**【ACTIVEで推進中】

・ **DDoS攻撃等**
→ **事業者設備に対する大量通信**の送信を検知し、遮断することは**正当防衛又は緊急避難**として実施

課題

■ **マルウェア配布サイトへの注意喚起**
→ 現状では、通信の秘密の観点から、**本人（攻撃対象）の同意がある場合**に限り実施
→ 利用者保護の観点から、**「有効な同意」の解釈の緩和の可能性**について要検討

■ **DDoS攻撃等**
→ 現状では通信の秘密の観点から、事業者設備に対する大量通信の検知・遮断については**正当防衛又は緊急避難として対応可能と整理**
→ **必ずしも事業者設備に影響を与えるとは限らないサイバー攻撃の事案への対策の可能性について要検討**

スケジュール

平成26年3月を目途に一定の取りまとめを行う予定。

サイバーセキュリティに関する政府戦略について

【サイバーセキュリティ戦略（平成２５年６月１０日情報セキュリティ政策会議決定）抜粋】

３．取組分野

（１）「強靱な」サイバー空間の構築

④サイバー空間の衛生

潜在型のマルウェアの挙動等について、高度かつ迅速に検知するための技術開発等を行うとともに、サイバー攻撃の複雑・巧妙化などサイバー空間を取り巻くリスクの深刻化の状況等を踏まえ、**情報セキュリティを目的とした通信解析の可能性等、通信の秘密等に配慮した、関連制度の柔軟な運用の在り方について検討**する。

【サイバーセキュリティ２０１３（平成２５年６月２７日情報セキュリティ政策会議決定）抜粋】

Ⅱ 具体的な取組

１「強靱な」サイバー空間の構築

④サイバー空間の衛生

（ノ）情報セキュリティ目的の通信解析の可能性等関連制度の柔軟な運用の在り方の検討（総務省）

総務省において、**情報セキュリティを目的とした通信解析の可能性等、通信の秘密等に配慮した、関連制度の柔軟な運用の在り方について、**可能な範囲で速やかに**一定の結論を得る**よう、サイバー攻撃の実態、これに対する現行の取組状況等の実態把握に努めるとともに、情報セキュリティを目的とした通信解析における課題の洗い出し等を行う。