くらしの中に
総務省

平成26年1月21日より
総務省キャッチフレーズが変わりました!

総務省における情報セキュリティ政策の最新動向

情報流通行政局
情報セキュリティ対策室
本田　知之

情報セキュリティ上の事案

分散型サービス妨害(DDoS)攻撃

2009年7月・・・韓国、米国の金融機関や政府機関等のシステムが攻撃を受け、数日間に亘りウェブサイトへのアクセス不能な状態に陥ったことに加え、推定で27～41億円の経済的な被害が発生。

2010年9月・・・中国のハッカー組織が、日本政府機関のウェブサイトを攻撃すると表明した後、防衛省及び警察庁等のウェブサイトが攻撃を受け、3日間に亘りアクセスしづらい状態が継続。

2012年6月・・・国際ハッカー集団アノニマスが、ネット上の違法ダウンロード行為に刑事罰を導入する改正著作権法の成立に反発し、日本政府等に攻撃予告。**財務省、国交省**のウェブサイトが改ざんされたほか、最高裁、自民党、民主党のウェブサイトが一時アクセスしづらい状態が発生。

2012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改ざん。

2013年3月・・・欧州において、スパム対策組織やインターネットセキュリティ会社へのDDoS攻撃**(DNSAmp攻撃)**が発生、同年夏には国内通信事業者においても被害が発生。

不正アクセス

2011年4月・・・ソニーの子会社(ソニー・コンピュータエンタテイメント及び米国法人)のシステムに対する不正アクセスにより、個人情報(氏名・住所、電子メールアドレス、クレジットカード番号等)約1億人分が窃取。

2012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から、当該PCの所有者が誤認逮捕。

2012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。

2013年4月・・・NTTレゾナントが運営するポータルサイト「goo」が不正アクセスを受け、約3万人のアカウントに不正ログインがあったとの報道。

2013年夏以降・・インターネットサービスを提供する各社において、**「リスト型攻撃」**によるものと思われる不正アクセス被害が急増。

標的型攻撃

2010年9月・・・イランの原子力発電所の制御システムにおいて、USB経由でスタックスネットと呼ばれるマルウェア感染が確認されたとの報道。

2011年8月・・・三菱重工業の社内サーバやパソコン約80台が情報収集型のウイルスに感染し、コンピュータのシステム情報が流出したおそれ。

2011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。

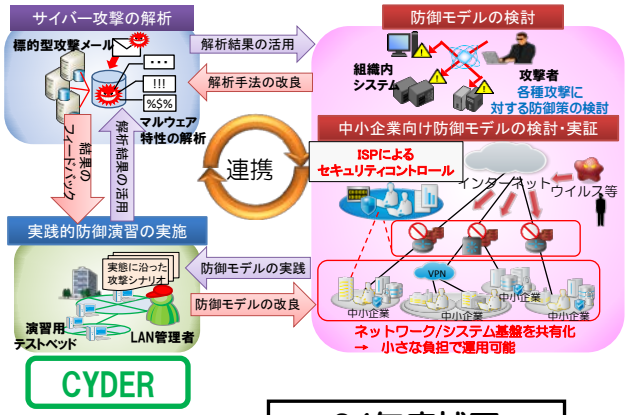
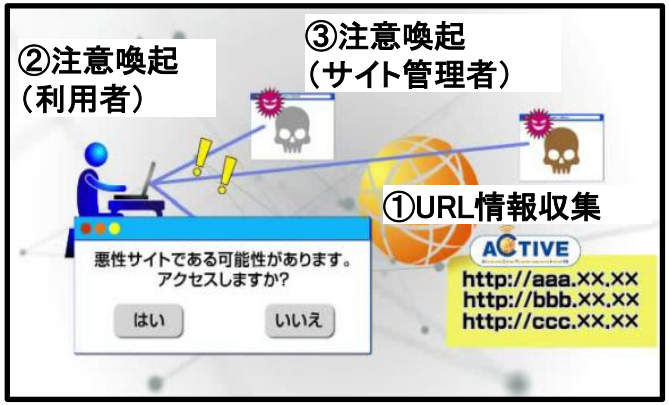
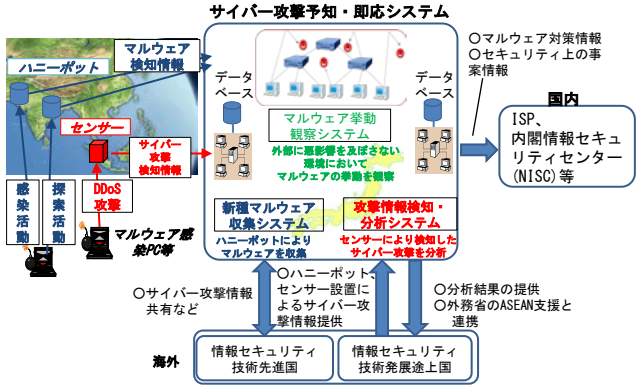
2011年11月・・**総務省**のパソコン23台が情報収集型のウイルスに感染していたことが判明、個人情報、業務上の情報が流出したおそれ。

2013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。

2013年3月・・・韓国において、主要放送局や金融機関のコンピュータが一斉にダウンするというサイバー攻撃が発生。

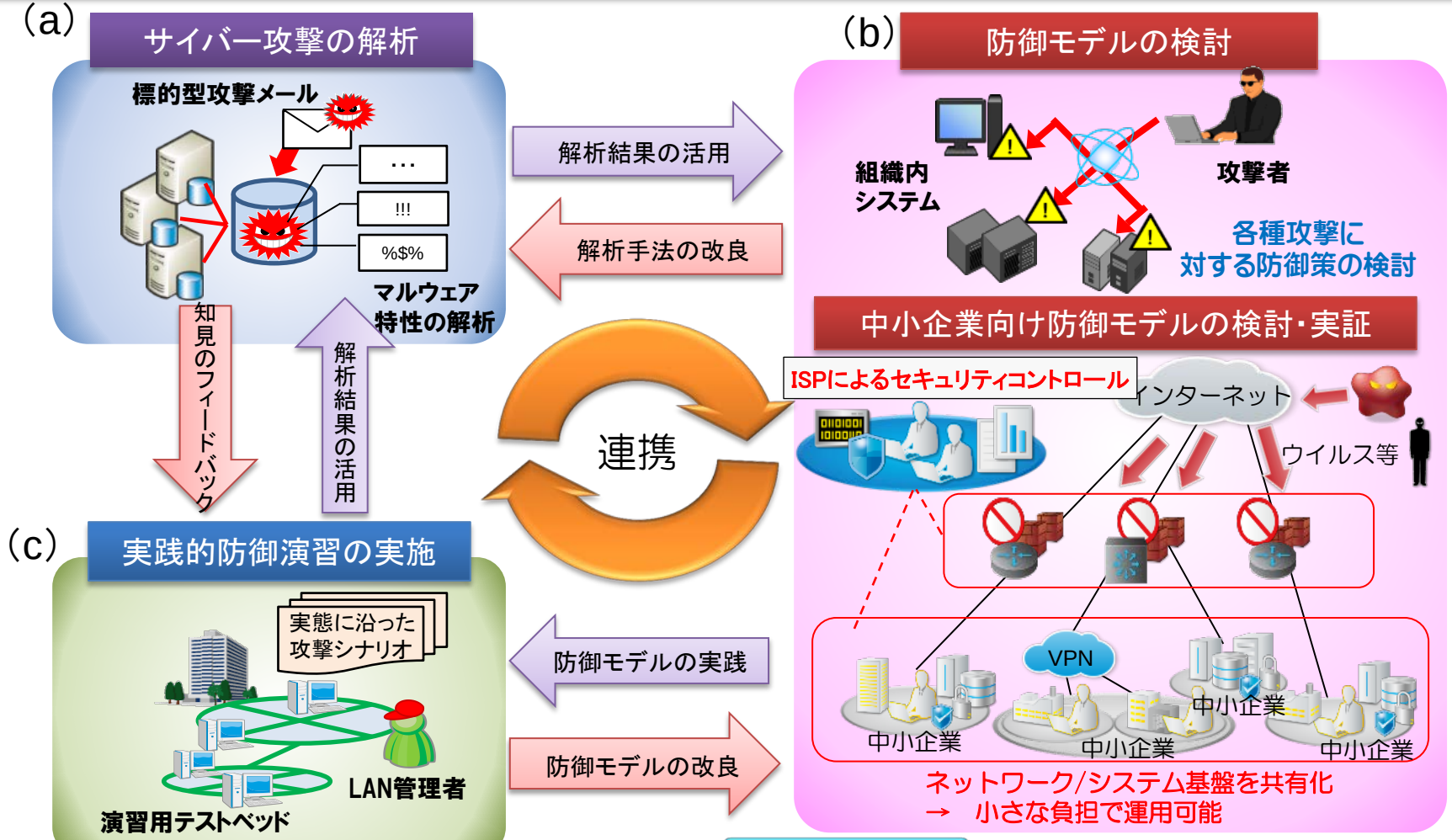
2013年8月・・・複数の新聞社で運営される有料ニュースサイトが改ざんされ、サイトを通じてマルウェアの感染が拡大。**(ゼロデイ攻撃・水飲み場攻撃)**

情報セキュリティに関する総務省の主な予算施策

	標的型攻撃	個人のマルウェア感染	分散型サービス妨害攻撃（DDoS攻撃）
課題	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。	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	**サイバー攻撃複合防御モデル・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。	**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。	**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。
			
	24年度補正 15.2億円 26年度当初 4. 5億円	25年度当初 4.8億円 26年度当初 3.5億円	23年度当初 6.3 億円 23年度補正 5.6 億円 25年度当初 5.8 億円 26年度当初 3.0 億円

サイバー攻撃複合防御モデル・実践演習

新たなサイバー攻撃に対応可能な環境を実現するため、攻撃の解析及び防御モデルの検討を行い、官民参加型のサイバー攻撃に対する実践的な防御演習等を実施する。



計画年数

4か年計画（平成26年度～29年度）

所要経費

平成26年度当初予算　4．5億円

（平成24年度補正予算額15億円）

（1） サイバー攻撃解析について

■ 標的型攻撃等のサイバー空間上の新たな脅威に対して、攻撃手法を迅速かつ効果的に解明するため、サイバー攻撃に関する情報収集・解析手法を確立する。

具体的内容

■ 大規模LAN環境を用いてサイバー攻撃に関する情報収集・解析等の調査・実証を実施。

① 攻撃の解析

＜解析例＞

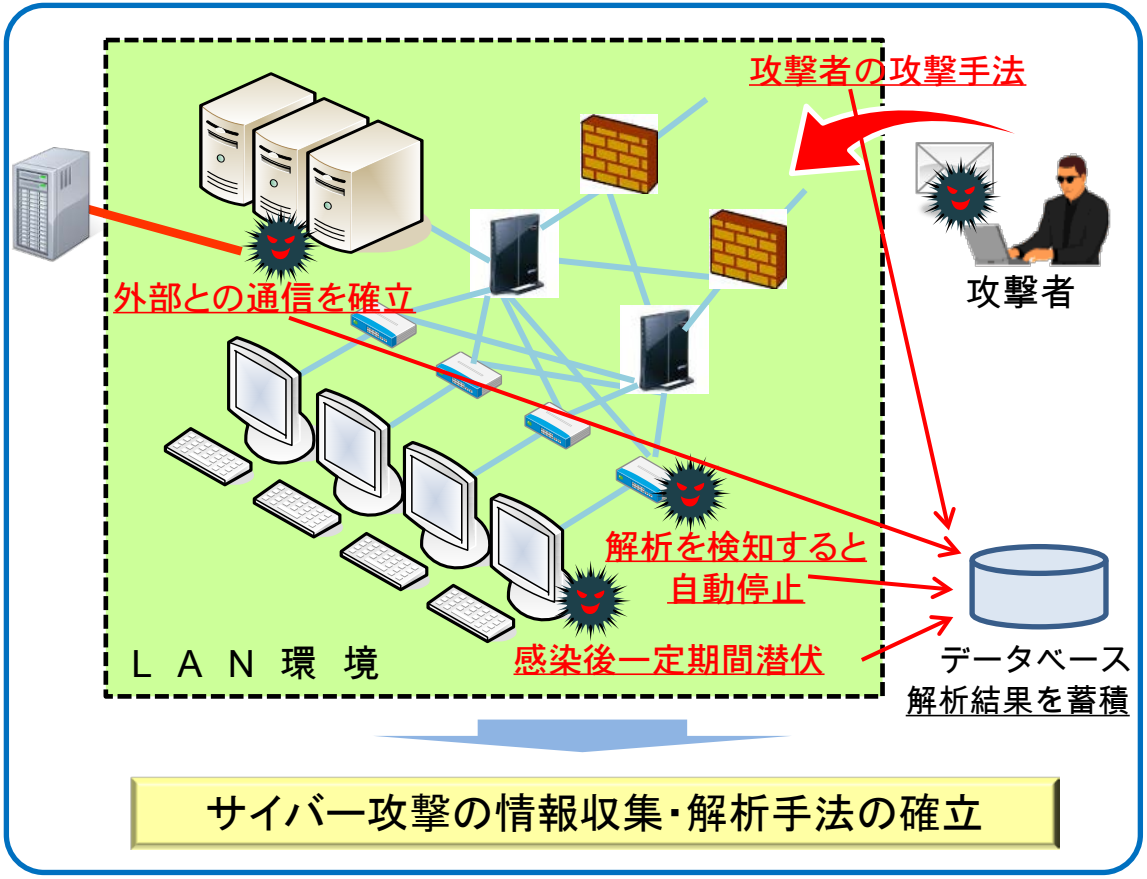
○ 攻撃者の攻撃手法

○ マルウェアの振る舞い
（耐解析機能や外部との通信の有無等）

② 解析結果のデータベース化

■ 上記の取組を通じてサイバー攻撃の情報収集・解析手法の確立を図る。

概要図



サイバー攻撃の情報収集・解析手法の確立

（2） サイバー攻撃防御モデルについて

■ サイバー攻撃が発生した際に、迅速かつ的確なインシデントレスポンスを実施できるようにするため、被害状況分析・特定手法、推奨レスポンス等のサイバー攻撃防御モデルを確立する。

具体的内容

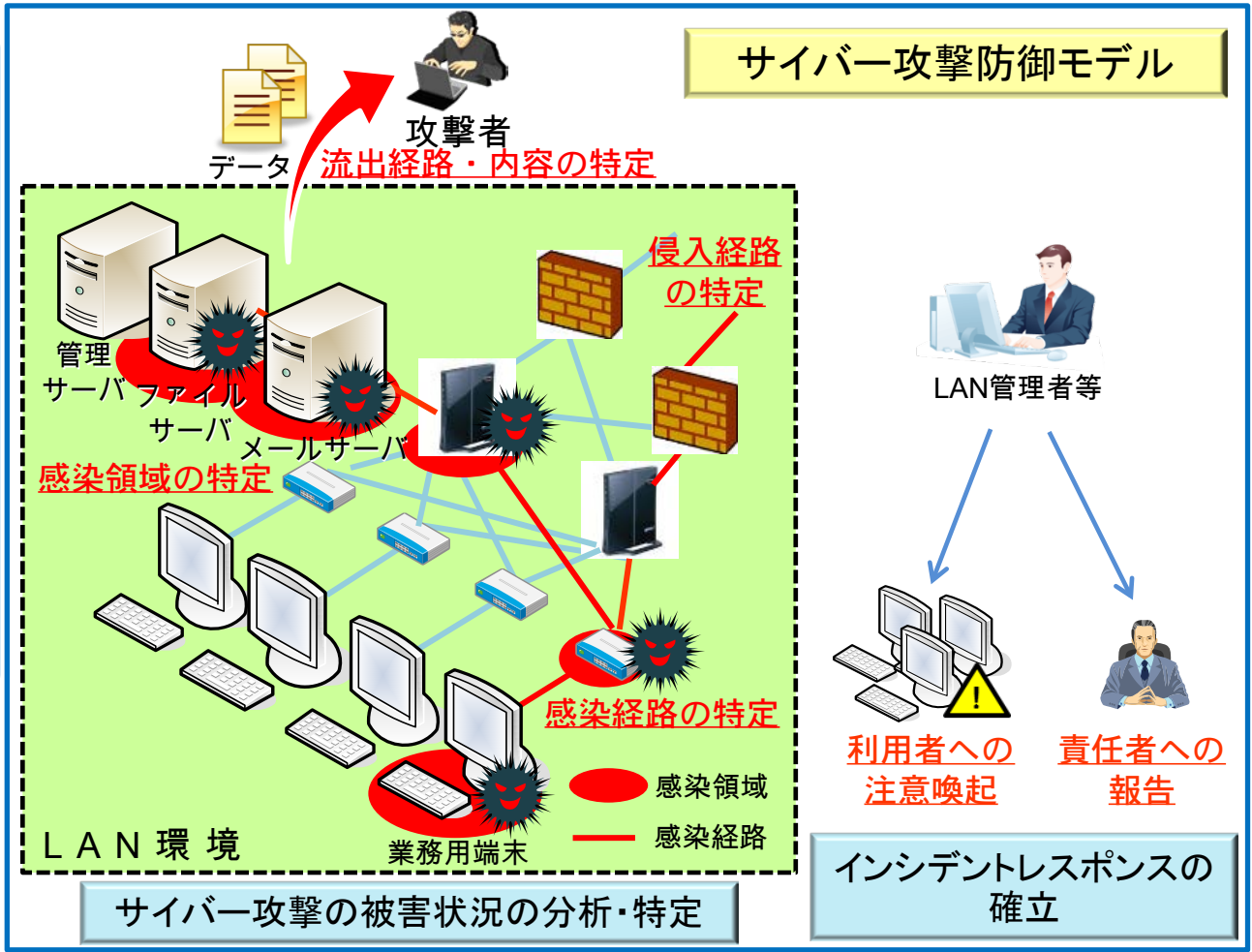
■ 大規模LAN環境を用いて、サイバー攻撃が発生した際の被害状況の分析・特定、インシデントレスポンス等に関する調査・実証を実施。

① 被害状況の分析・特定
- 侵入経路
- 感染経路・領域
- 被害の進行度　　等

② インシデントレスポンスの確立
- 利用者への注意喚起
- 責任者への報告　　等

■ 上記の取組を通じてサイバー攻撃の防御モデルの確立を図る。

概要図



（3） 実践的サイバー防御演習（CYDER）について

CYDER: **CY**ber **D**efense **E**xercise with **R**ecurrence

■ 官公庁・大企業等のLAN管理者等のサイバー攻撃対処能力向上のため、大規模LAN環境を模擬した環境による実践的なサイバー防御演習（CYDER）を実施。

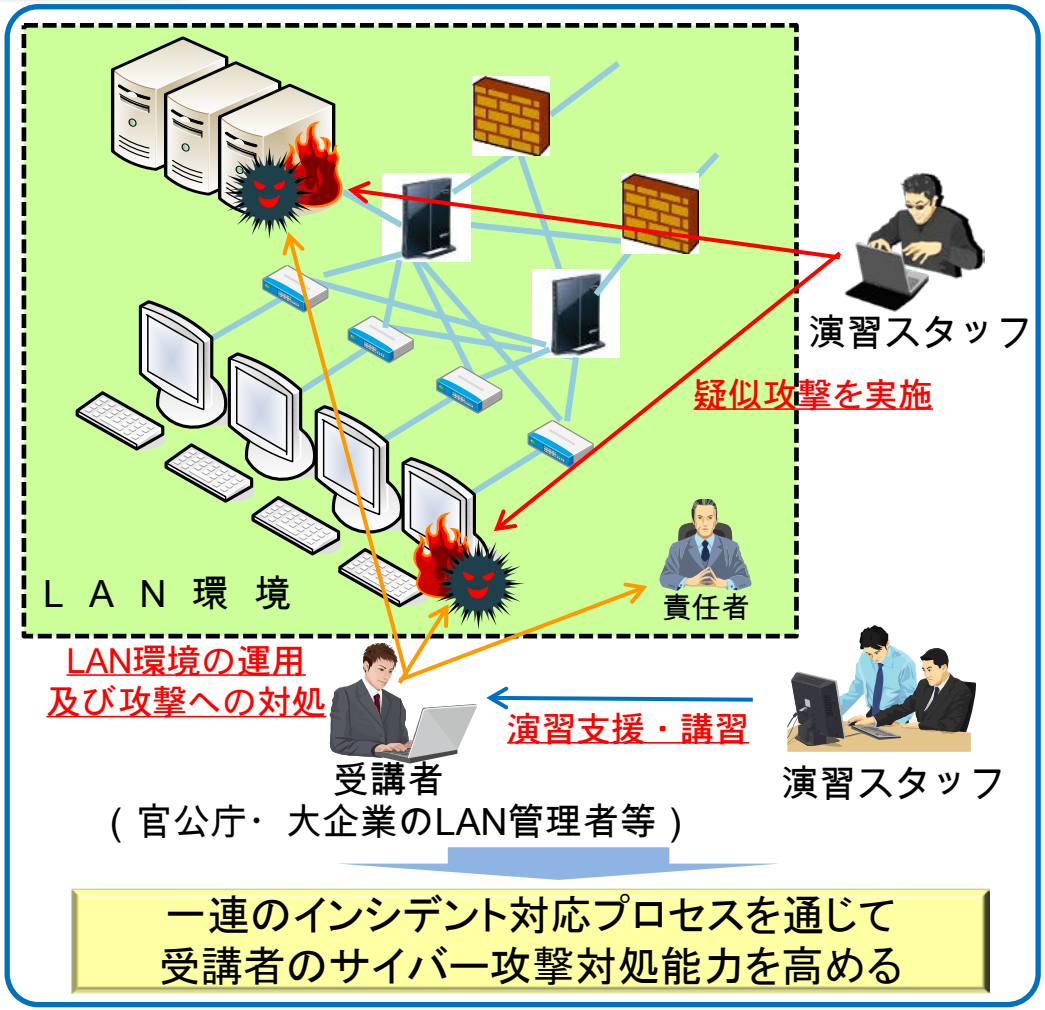
具体的内容

■ （1）及び（2）で確立したサイバー攻撃の解析手法及び防御モデルを活用し、職員数千人規模の組織内ネットワークを模擬した大規模環境による、官公庁・大企業を対象としたサイバー防御演習を実施する。

■ 一連のインシデント対応プロセスを通じて受講者のサイバー攻撃対処能力を高め、サイバー攻撃に対応可能な人材の育成を図る。

■ 演習を踏まえて演習プログラム及びLAN管理者が習得すべきスキルセットの確立を図る。

概要図

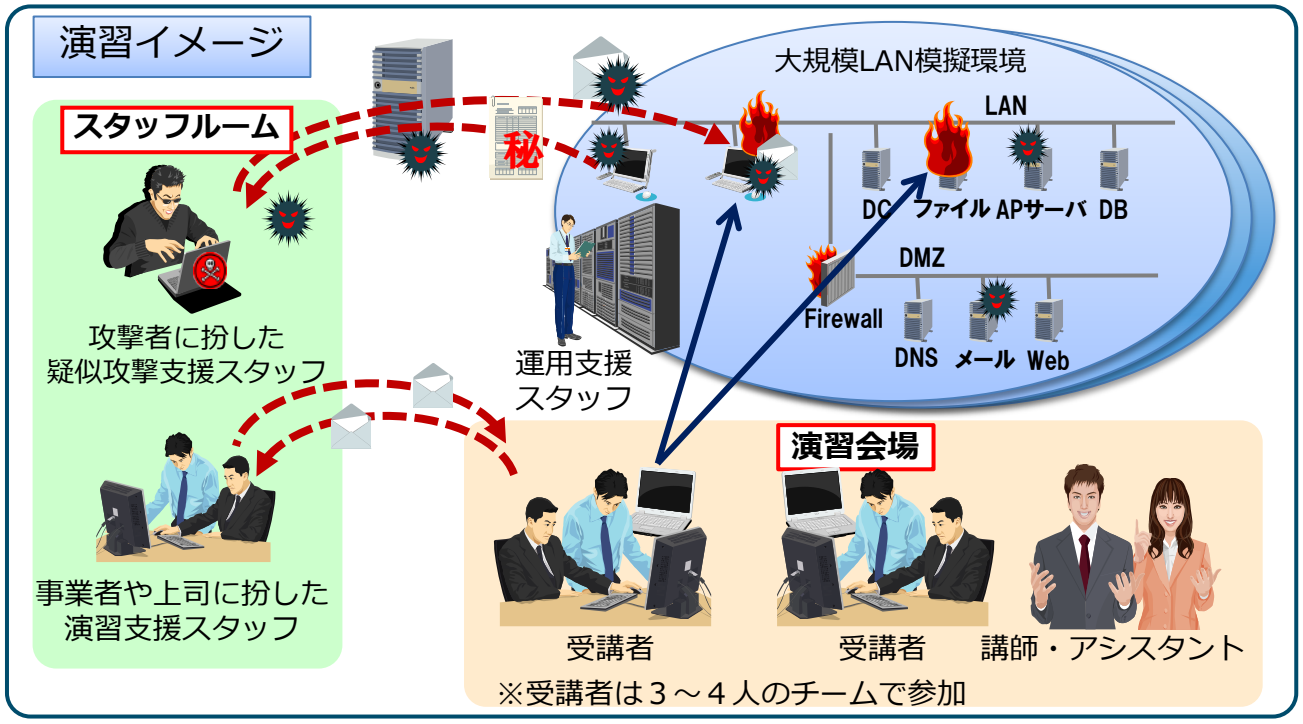


実践的サイバー防御演習（CYDER）

CYDER: CYber Defense Exercise with Recurrence（サイバー 防御 反復演習）

- 官公庁・大企業等のLAN管理者のサイバー攻撃への対応能力向上のため、実践的なサイバー防御演習を実施。
- 職員数千人規模の組織内ネットワークを模擬した大規模環境による、官公庁を対象としたサイバー演習は日本初。
- LAN管理者の能力向上に寄与すると共に、演習で得られた知見を基に防御モデルを確立し広く展開していく予定。
- 「サイバー攻撃解析・防御モデル実践演習」（H24～H29）の一環として実施し、平成25年度中に10回実施。

演習イメージ



演習実績

開催回	開催日
第1回	H25/9/25(水), 26(木)
第2回	H25/10/16(水), 17(木)
第3回	H25/11/13(水), 14(木)
第4回	H25/12/12(木), 13(金)
第5回	H26/1/15(水), 16(木)
第6回	H26/1/29(水), 30(木)
第7回	H26/2/12(水), 13(木)
第8回	H26/2/25(火), 26(水)
第9回	H26/3/3(月), 4(火)
第10回	H26/3/6(木), 7(金)

演習参加者

省庁（総務省、防衛省等）や独立行政法人、民間事業者などから計33組織、292名が参加。

CYDERの演習プログラム

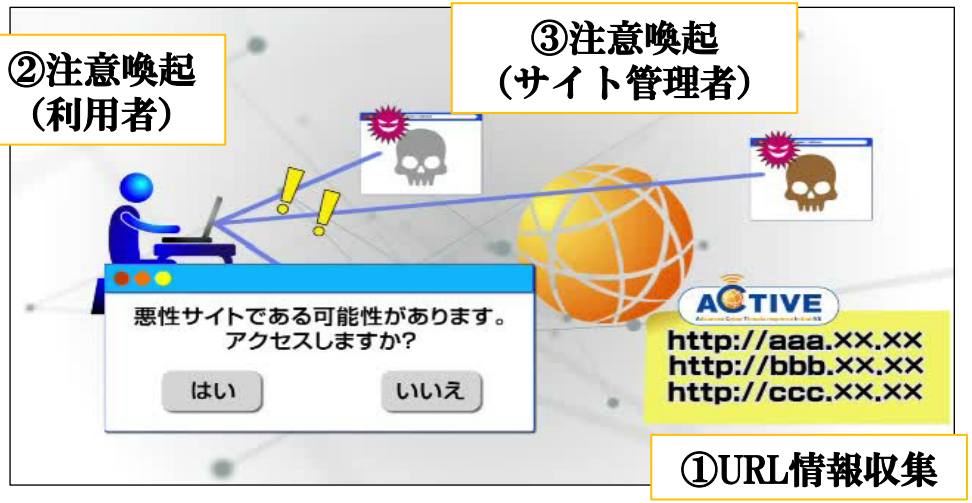
演習プログラム（2日間）

	演習初日	演習２日目
午前	■演習前スキルチェックテスト ■講義 － 最近のサイバー攻撃事例の紹介 － 演習環境・ツールの解説　等	（演習スタッフによる評価作業　等）
午後	■演習 － 監視・分析業務 － 報告書作成　等	■講評 － 各チーム報告書の発表 － 質疑応答／講師講評　等 ■演習後スキルチェックテスト

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。

(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。

計画年数

5か年計画(平成25年度～29年度)

所要経費

平成25年度予算額　4．8億円
平成26年度予算額　3．5億円

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。

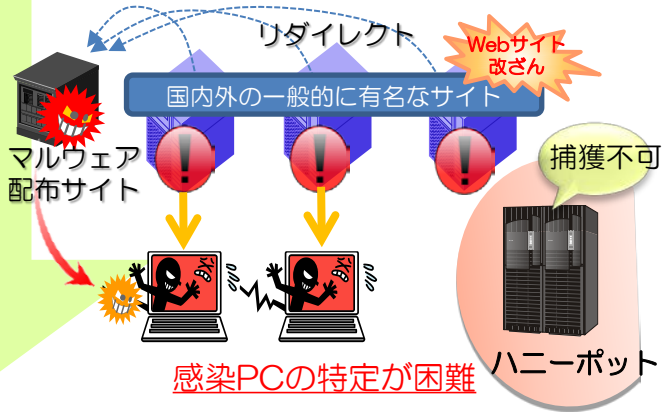
ネットワーク感染型マルウェア

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

国際連携によるサイバー攻撃予知・即応技術の研究開発

1 背景

プロジェクト略称：PRACTICE： Proactive Response Against Cyber-attacks Through International Collaborative Exchange

■ 政府機関、民間企業等の情報通信システムが大規模なサイバー攻撃を受け、サービス停止、情報漏えい等の被害が発生しており、サイバー攻撃の発信元の多くは海外であることから、国際連携による攻撃への対処が必要。

■ 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）においても「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等に関する研究開発プロジェクトを実施」することとされている。

2 施策の概要

○ サイバー攻撃情報を分析し、サイバー攻撃を予知する技術及びサイバー攻撃情報を収集するセンサーの運用・管理技術等のサイバー攻撃情報収集・共有技術の開発

○ 欧州及びASEAN諸国との協力関係を構築し、開発した技術を活用したサイバー攻撃の情報収集の実証

3 計画年数

5か年計画（平成23年度～27年度）

4 所要経費

平成23年度当初予算額	6．3億円
平成23年度補正予算額（第4号）	5．6億円
平成25年度予算額	5．8億円
平成26年度予算額	3．0億円

5 国際連携の状況

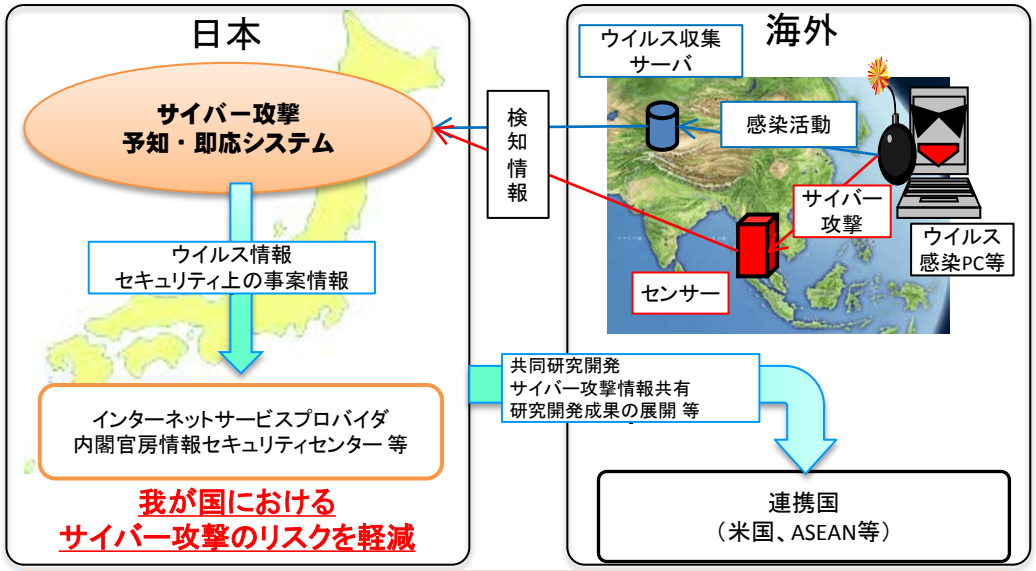
○ 平成23年11月、「第4回日・ASEAN情報セキュリティ政策会議」において、ASEAN各国に連携を呼びかけ。

○ 平成24年3月には、サイバー攻撃の予知のための研究開発の協力について、**米国と合意**。6月に研究者中心の日米会合を実施。

○ そのほか、平成24年3月に**インドネシア**、4月に**モルディブ**、平成25年2月に**タイ**、3月に**マレーシア**、平成26年3月に**シンガポール**との間で合意。

○ 現在、欧州諸国、その他のASEAN諸国等と連携に向けて協議中。

〔事業イメージ〕



サイバー攻撃は国境を越えて発生することから、情報収集ネットワークを国際的に構築し、サイバー攻撃に対応

その他にも・・・

○　無線ＬＡＮの情報セキュリティに関する普及啓発

平成２６年５月７日に公表しました！

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/wi-fi.html

○　総務省ホームページを通じた普及啓発

平成２５年４月にリニューアル！

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html