資料4－1

総務省
MIC Ministry of Internal Affairs and Communications

政府における情報セキュリティ政策の取組について

平成26年1月15日
事　　務　　局

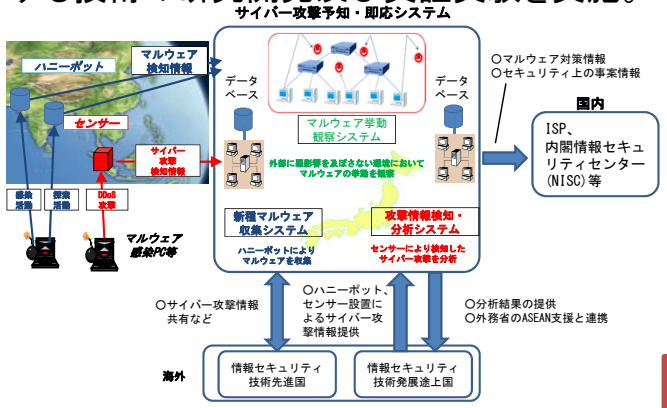
総務省情報セキュリティ関係の平成26年度予算案

予算

分散型サービス妨害（DDoS）攻撃

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を実施。



◇　平成24年３月に、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**。

◇　平成24年４月に**モルディブ**、５月に**インドネシア**との間で情報共有を開始。平成25年２月に**タイ**、3月に**マレーシア**と連携について合意。

◇　平成25年9月、「**日・ASEANサイバーセキュリティ協力に関する閣僚政策会議**」の結果、技術協力プロジェクト**JASPER**の一部として展開することを決定。

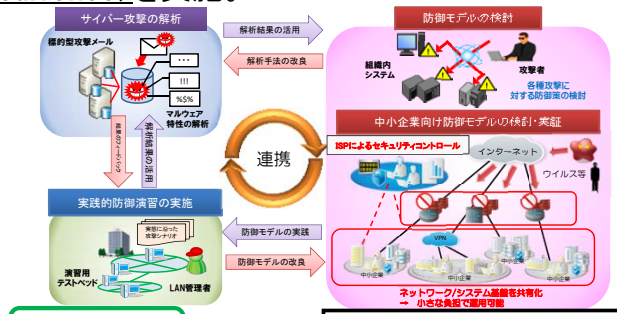
◇　現在、欧州諸国、シンガポール等と連携に向けて協議中。

23年度	6.3 億円
23年度補正	5.6 億円
25年度	5.8 億円
26年度（案）	**3.0 億円**

標的型攻撃

サイバー攻撃複合防御モデル・実践演習

標的型攻撃の解析による実態把握、中小企業も対象とした防御モデルの検討、官民参加型の実践的な防御演習（CYDER: CYber Defense Exercise with Recurrence）を実施。

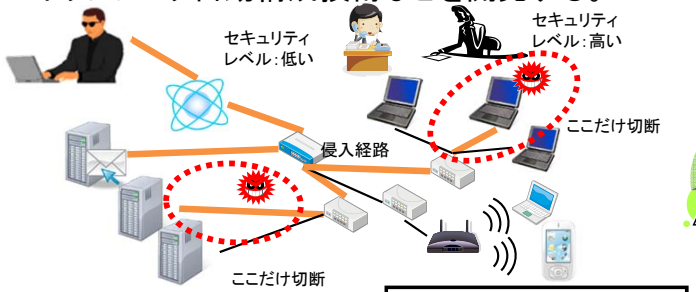


CYDER

24年度補正	15.2億円
26年度（案）	**4.5億円**

サイバー攻撃の解析・検知に関する研究開発

利用者の行動特性等に基づいた不正な意図、被害の程度などの検知技術、被害拡大の防止のための ネットワーク自動構成技術などを開発する。



25年度	5.5億円
26年度（案）	**3.1億円**

個人のマルウェア感染等

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。平成25年11月から開始。

25年度	4.8億円
26年度（案）	**3.5億円**

電波の能率的かつ安全な利用に関するリテラシー向上

スマートフォン利用者の安心・安全な無線LAN（Wi-Fi）の利用に向けて、利用者及びアクセスポイント設置者の情報セキュリティ対策に関するリテラシーを向上するために、テキストの作成やセミナーなどを実施。

25年度	30百万円
26年度（案）	**31百万円**

税制

① 中小企業投資促進税制の延長・拡充

✓　中小企業による設備投資（ソフトウェア含む）に対して特別償却や税額控除を行う措置について、適用期限を**3年間延長**。

② 中小企業等の少額減価償却資産の取得価額の損金算入の特例の延長

✓　取得価額30万円未満の全ての減価償却資産（ソフトウェア含む）を対象に、全額即時損金参入を認める措置について、適用期限を**2年間延長**。

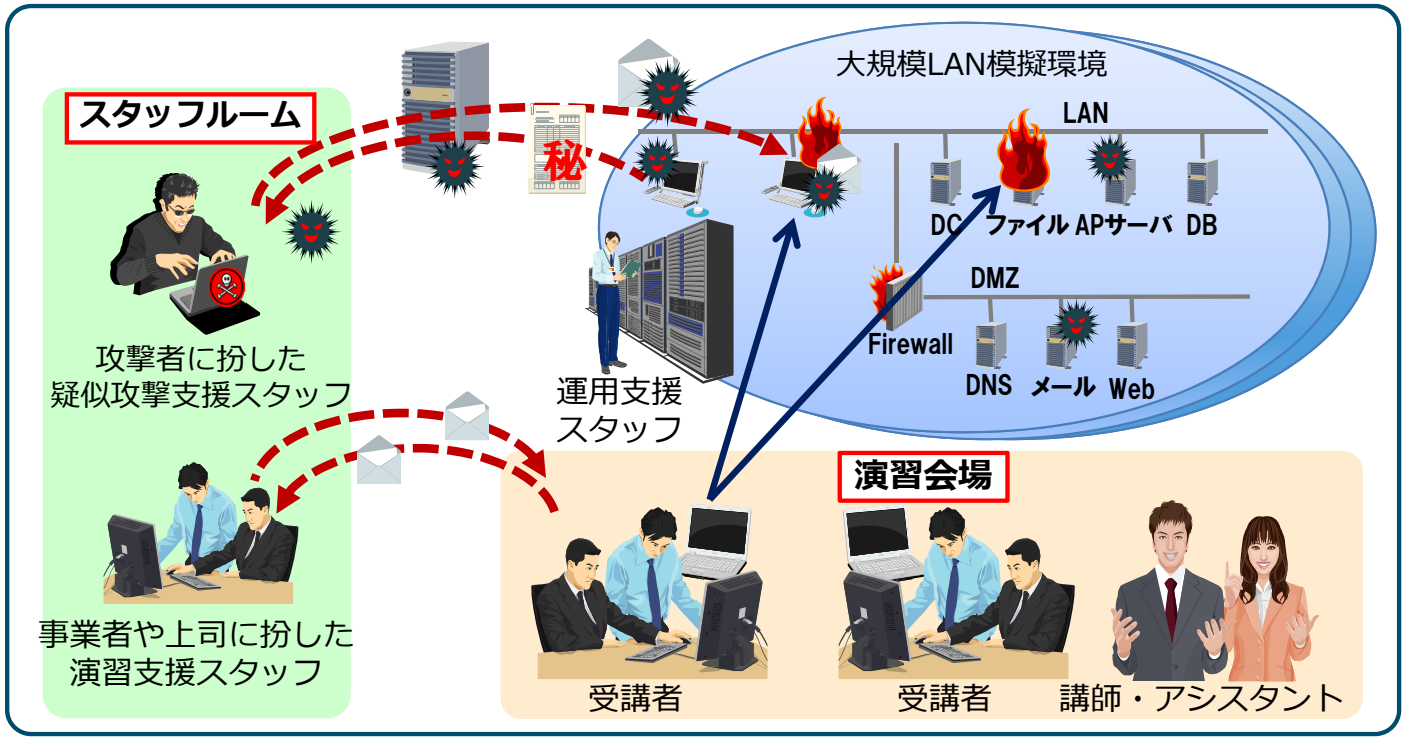
✓　**WindowsXPのサポート期限が切れることに伴う中小企業のパソコン、ソフトウェア等の入替えニーズにも対応可能。**

実践的サイバー防御演習（CYDER）

CYDER: CYber Defense Exercise with Recurrence

- 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、今年度中に6回実施予定。

演習イメージ



演習スケジュール

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

演習参加者

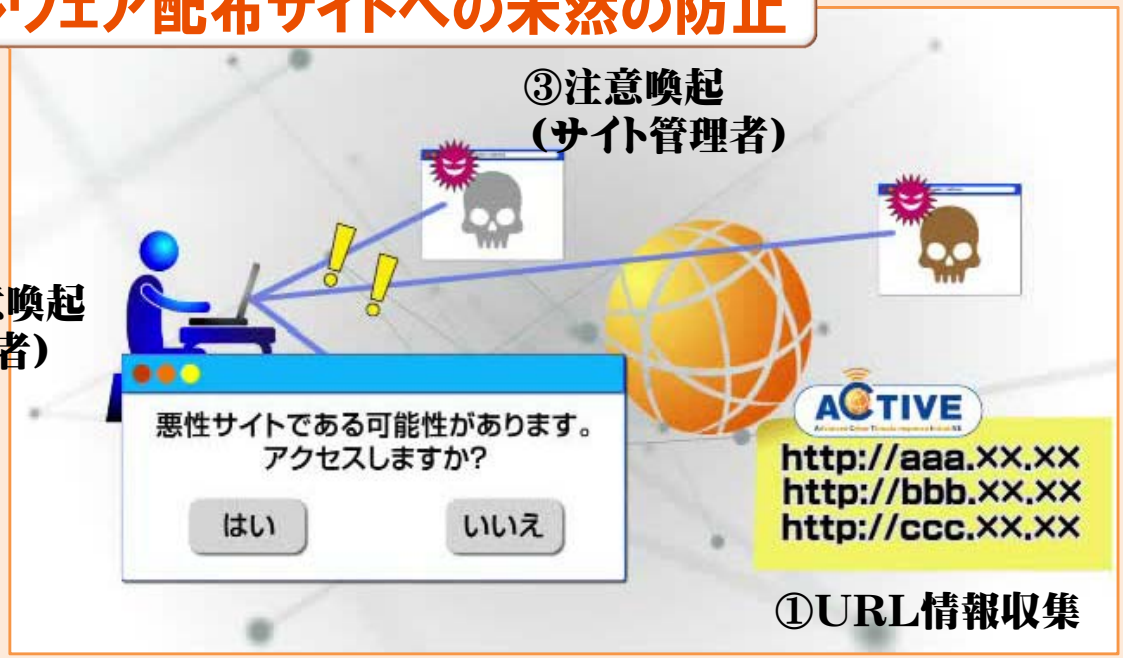
省庁（総務省、法務省、防衛省等）や独立行政法人、民間事業者などから計32組織、174名が参加予定。

ACTIVE（Advanced Cyber Threats response InitiatiVE）

○ ACTIVEは、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。平成25年11月から開始。
○ 総合的なマルウェア感染対策を官民連携により実施するプロジェクトは、世界初。

ACTIVE（Advanced Cyber Threats response InitiatiVE）の取組

マルウェア配布サイトへの未然の防止



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。

上記のほか、マルウェアに既に感染している利用者に対する注意喚起など、総合的なマルウェア感染対策を実施。

日・ASEANサイバーセキュリティ協力に関する閣僚政策会議（開催結果）

平成25年9月12～13日、「日・ASEANサイバーセキュリティ協力に関する閣僚政策会議」を開催。
① サイバー攻撃の予知即応及びマルウェア感染警告について技術協力する
② 政府職員向けの大規模な人材育成を実施する
ことを、共同声明の中で確認。

1. 経緯

「日・ ASEAN友好協力40周年」の記念事業の一つとして、平成24年11月の「日・ ASEAN情報通信大臣級会合」（フィリピン）にて、今年に日本で開催することに合意したもの。

2. 開催概要

日　時: 平成25年9月12日（木）～9月13日（金）　於　ホテルオークラ
参加者: 新藤総務大臣、平経済産業大臣政務官、内閣官房情報セキュリティセンター、及びASEAN加盟国（10カ国）の閣僚級。
開会では安倍総理大臣が挨拶。
内　容: ASEAN各国から、ASEAN域内にてICTの発展段階が異なる現状やセキュリティ上の課題が共有されたほか、我が国からは、総務省、経済産業省、内閣官房情報セキュリティセンターの各々から、技術面や人材育成面での協力内容について提案を実施した。また、安全で活力のあるサイバー空間の構築に向け、サイバー空間は情報の流通を維持し経済的繁栄を促進し続けるものであるべきという原則を確認しつつ、これらの議論内容を共同声明として採択した。

3. 成果

共同声明には、サイバー攻撃の予知即応（PRACTICE）及びマルウェア感染警告（DAEDALUS）からなる技術協力（JASPER）や専門家派遣等を通じて5年間で1000人規模の政府職員向けの研修を実施（日・ASEANサイバーセキュリティ人材育成イニシアティブ）するなどの協力内容が盛り込まれた。

4. フォローアップ状況

平成25年10月の第6回「日・ASEAN情報セキュリティ政策会議」（フィリピン）にて、「JASPER」ではPRACTICEの未連携国へ連携を呼びかけるとともに、年内にASEAN10カ国の参加を目指してDAEDALUSへの参加募集を開始。また、「日・ASEANサイバーセキュリティ人材育成イニシアティブ」では各国からの意見集約の後、年明けの研修開始を確認。平成25年12月の日・ASEAN特別首脳会議にて、これらのサイバーセキュリティ分野の協力を進めていくことが、ビジョン・ステートメント（成果文書）に盛り込まれた。

JASPER（Japan-ASEAN Security PartnERship）

JASPER（ジャスパー）
（Japan-ASEAN Security PartnERship）

○Japan-ASEAN Security PartnERshipの略。
○「日・ASEANサイバーセキュリティ協力に関する閣僚政策会議」の共同閣僚声明にて、ネットワークセキュリティ分野における技術協力を強化するため、日・ASEAN間のプロジェクトとして開始。「サイバー攻撃予知即応プロジェクト（PRACTICE）」及び「感染警告（DAEDALUS）」の総称。

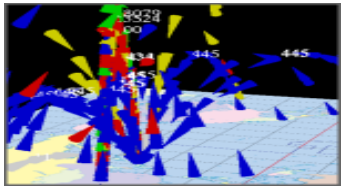
サイバー攻撃予知即応プロジェクト（PRACTICE（プラクティス））

○Proactive Response Against Cyber-attacks Through International Collaborative Exchangeの略。
○サイバー攻撃に関する情報を収集・分析の上、情報共有を行い、サイバー攻撃発生の予知・即応を可能とする技術を確立するためのプロジェクト。総務省予算（H23年度からH27年度）で現在までに15億円で研究開発中。現時点で、ASEANではインドネシア、タイ、マレーシアからサイバー攻撃観測データの提供を受けている。

感染警告（DAEDALUS（ダイダロス））

○Direct Alert Environment for Darknet And Livenet Unified Securityの略。
○独立行政法人情報通信研究機構（NICT）による、マルウェア感染をリアルタイムに警告するサービス。
（2012年6月に国内でサービスを開始）

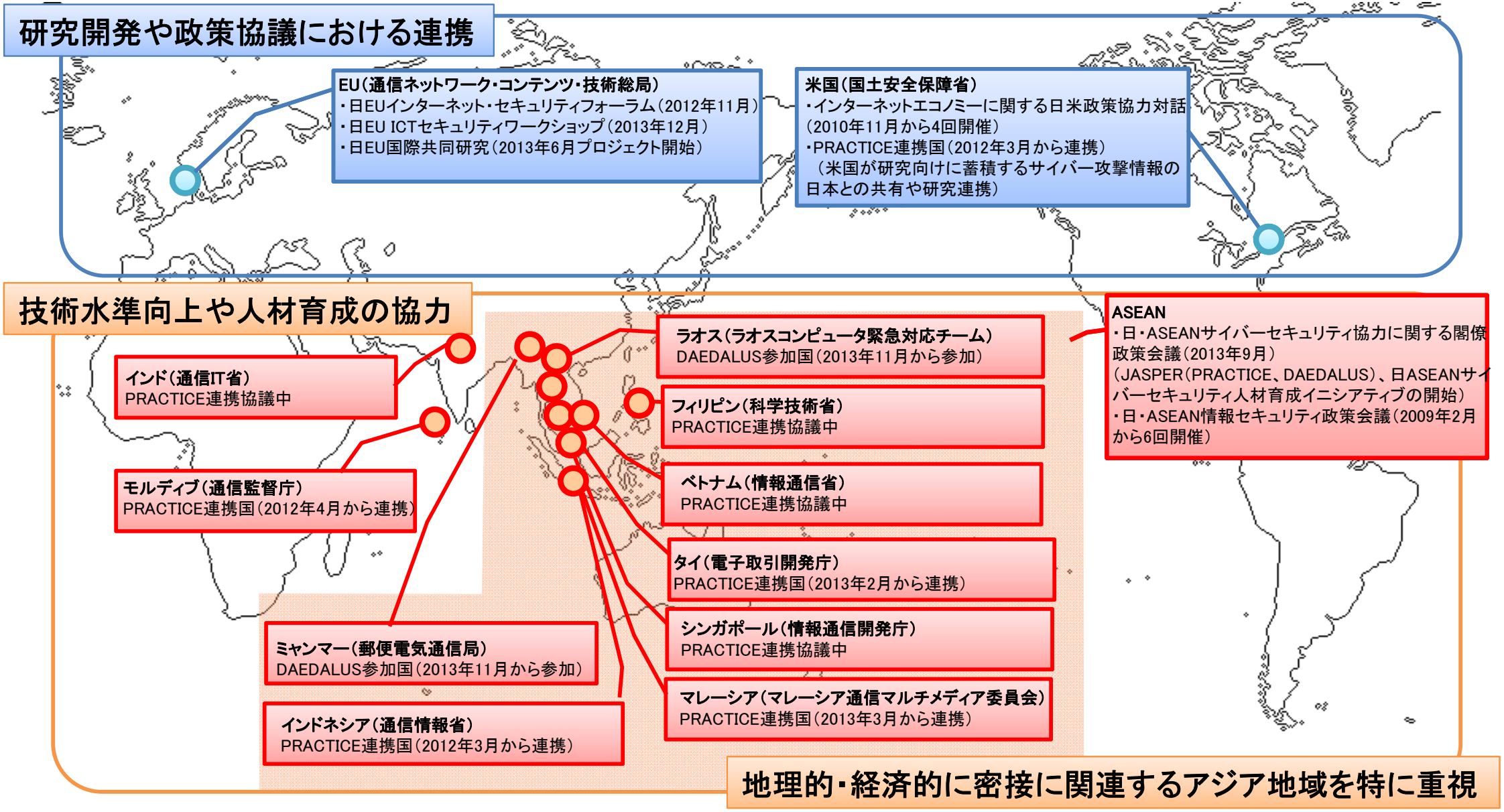
nicter（ニクター）



○Network Incident analysis Center for Tactical Emergency Responseの略。
○独立行政法人情報通信研究機構（NICT）による、ネットワーク上のサイバー攻撃をリアルタイムに観測・分析するシステム。
○nicterによる実証結果を、PRACTICEにおいて新たな技術の確立に反映。
○nicterによる分析結果を活用して、感染警告（DAEDALUS）を実施。

サイバーセキュリティ分野における国際連携の取組

国境を越えたサイバー攻撃に対処するためには国際連携が必要不可欠。総務省は欧米との研究開発や政策協議における連携、及びアジア地域との技術水準向上や人材育成の協力を進めている。



ソウル国際サイバー会議の開催

ソウル国際サイバー会議の概要

（1） 日時・場所： 2013年10月17日（木）及び18日（金） 韓国・ソウル

（2） 主催： 韓国政府

（3） 議題： オープンで安全なサイバー空間を通じた世界の繁栄について

（4） 参加者 ： 約90か国（米国、カナダ、欧州、ロシア、中国、インド、ASEAN、中南米国、アラブ、アフリカ）の政府機関、国際機関、民間企業（インテル、マイクロソフト等）など1,600名程度が参加（昨年の2倍）。

日本からは、外務省の三ツ矢副大臣を団長として総務省など関係省庁が参加。さらに、（一財）日本データ通信協会 テレコム・アイザック推進会議）の飯塚会長が、「経済成長と発展」に関する分科会で、我が国におけるサイバーセキュリティに向けた取組み、特に官民連携による対応の重要性について、基調講演。

会議における主な議論

（1） 4つの全体会合及び6つの分科会が実施。全体会合では10名程度の政府、国際機関の要人から基調講演。分科会は、様々なステークホルダーが参加したパネルディスカッション。

（2） 昨年に比較すると、参加者数が大幅に増大。特にアジア、アフリカ等の途上国、市民団体が増加。

（3） また、昨年は、先進国からの参加者と、新興国からの参加者の間で、明確な意見の対立が見られたが、今回会合では、それが緩和。サイバー空間の課題解決のためには、①マルチステークホルダーの参加が基本であること、②国際協力・連携が必要であること、③キャパシティ・ビルディングが重要であることについて、見解が一致。

（4） 会議の成果文書として、主要な国際会議及び国際機関で作成された成果文書、報告書等からの抜粋による「オープンで安全なサイバー空間に向けたソウル・フレームワーク及びコミットメント」が公表。

（5） 次回会合は、2015年にオランダのハーグにて開催されることが決定。

ソウル国際サイバー会議の概要

（参考）会議の構成

全体会合 1： サイバー空間のビジョン （10月17日）

全体会合 2： グローバルな繁栄に向けたデジタル・ディバイド解消 （10月17日）

全体会合 3： 国境を越えた協力の強化 （10月17日）

パラレルセッション 1 （10月17日） *パネルディスカッション
① **経済成長と発展** → Telecom-ISAC Japan 飯塚会長が、スピーカーとして参加。
② サイバーセキュリティ → サイバー空間における規範・規制、セキュリティ確保等を議論。

パラレルセッション 2 （10月18日） *パネルディスカッション
③ 社会的・文化的恩恵 → サイバー空間から享受する社会的・文化的恩恵につき議論。
④ サイバー犯罪 → サイバー犯罪への対応等につき議論。

パラレルセッション 3 （10月18日） *パネルディスカッション
⑤ 国際安全保障 → サイバー空間での国家安全保障上の問題への対応等につき議論。
⑥ 能力構築支援 → サイバー空間の恩恵を享受するための持続可能な能力開発の方策等を議論。

全体会合 4： パネルディスカッションの取りまとめ会合 （10月18日）

「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アクセスに関する注意喚起**
→ 通信の秘密保護の観点から、**本人（攻撃対象）の同意がある場合**に限り実施
→ マルウェア感染からの利用者保護の観点から、本取組みの普及に向けた**「有効な同意」の解釈の可能性**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。

「重要インフラの情報セキュリティ対策に係る第3次行動計画（案）」の検討状況について

これまでの取組み

重要インフラ

「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもの※」との定義　※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）より抜粋

環境の変化

- IT依存度の高まり → システム障害時の影響の広範囲化・対応の困難化
- 複雑化・巧妙化するサイバー攻撃

行動計画の意義

重要インフラ防護に責任を有する政府と自主的な取組を進める重要インフラ事業者等との共通の行動計画(注)　（参考）第1次行動計画（平成17年12月13日 情報セキュリティ政策会議決定）
第2次行動計画（平成21年2月3日　情報セキュリティ政策会議決定）

（注）日本再興戦略-JAPAN is BACK-（平成25年6月14日閣議決定）及びサイバーセキュリティ戦略において今年度内に新たな行動計画を策定する方針を決定

重要インフラの情報セキュリティ対策に係る第2次行動計画

主な施策

1. 安全基準等の整備及び浸透
2. 情報共有体制の強化
3. 共通脅威分析
4. 分野横断的演習　等

主な課題

社会・技術面での環境変化を踏まえた改善・補強が必要な箇所が存在

1. 重要インフラ事業者等のPDCAサイクルとの整合に基づく指針の見直し
2. 大規模IT障害発生時の対応体制の明確化
3. 演習・訓練に係る関係主体の連携の在り方の模索
4. 環境変化・脅威に適切に対応するための取組
5. 広報公聴、国際連携の強化に追加すべき基盤強化に資する取組　等

**第2次行動計画の基本的な骨格を維持しつつ、
第2次行動計画の課題等を踏まえた修正・補強**

重要インフラの情報セキュリティ対策に係る第3次行動計画（案）

施策群の構成と主要なポイント

1．安全基準等の整備及び浸透	対策途上や中小規模の重要インフラ事業者等への情報セキュリティ対策の「成長モデル」の訴求
2．情報共有体制の強化	平時の体制の延長線上にある大規模IT障害対応時の情報共有体制の明確化
3．障害対応体制の強化	関係主体が実施する演習・訓練の全体像把握と相互連携による障害対応体制の総合的な強化
4．リスクマネジメント	重要インフラ事業者等におけるリスクに対する評価を含む包括的なマネジメントの支援
5．防護基盤の強化	関連国際標準・規格や参照すべき規程類の整理・活用・国際展開　等

- **重要インフラ分野を現行の10分野から13分野に拡大（化学、クレジット及び石油の各分野を追加）**
- **行動計画の要点として、「経営層に期待する在り方」等を示すとともに、PDCAサイクルに基づく事業者等の対策例とこれに関連する国の施策を一覧化**
- **客観的な評価指標の提示とこれに基づく定期的な評価・改善の実施**

第3次行動計画の全体像

官民連携による重要インフラ防護の推進

重要インフラにおけるサービスの持続的な提供を行い、自然災害やサイバー攻撃等に起因するIT障害が国民生活や社会経済活動に重大な影響を及ぼさないよう、IT障害の発生を可能な限り減らすとともにIT障害発生時の迅速な復旧を図ることで重要インフラを防護する

重要インフラ（13分野）

- 情報通信
- 金融
- 航空
- 鉄道
- 電力
- ガス
- 政府・行政サービス（含・地方公共団体）
- 医療
- 水道
- 物流
- クレジット
- 石油
- 化学





NISCによる
調整・連携

重要インフラ所管省庁（5省庁）

- 金融庁［金融］
- 総務省［情報通信、行政］
- 厚生労働省［医療、水道］
- 国土交通省［航空、鉄道、物流］
- 経済産業省［電力、ガス、クレジット、石油、化学］

関係機関等

- 情報セキュリティ関係省庁
- 事案対処省庁
- 防災関係府省庁
- 情報セキュリティ関係機関
- サイバー空間関連事業者

重要インフラの情報セキュリティに係る第３次行動計画

安全基準等の整備・浸透

重要インフラ各分野に横断的な対策の策定とそれに基づく、各分野の「安全基準」等の整備・浸透の促進

情報共有体制の強化

IT障害関係情報の共有による、官民の関係者全体での平時・大規模IT障害発生時における連携・対応体制の強化

障害対応体制の強化

官民が連携して行う演習等の実施によるIT障害対応体制の総合的な強化

リスクマネジメント

重要インフラ事業者等におけるリスク評価を含む包括的なマネジメントの支援

防護基盤の強化

広報公聴活動、国際連携の強化、規格・標準及び参照すべき規程類の整理・活用・国際展開

新・情報セキュリティ人材育成プログラム（仮称）について

サイバーセキュリティ戦略で示された課題

情報セキュリティに係るリスクの深刻化に対応し、情報セキュリティ水準の向上を図るためには、

○人材の量的不足の解消に向け 積極的な取組が必要であるとともに、教育だけでは得られない突出した能力を有する人材の確保も大きな課題。

○そのためには、社会全体で育成し活用するための仕組みが必要。

人材の量的・質的不足

情報セキュリティ従事者 約26.5万人

うち質的不足 約16万人

さらに量的不足 約8万人

⇒これら人材の雇用の受け皿も不可欠

取組の方針

我が国の情報セキュリティの水準を高めるため、人材の「需要」と「供給」の好循環を形成する。

【需要】経営層の意識改革

○経営層の意識改革を促し、情報セキュリティを経営戦略として認識させるための取組を推進。
○製品・サービス調達における情報セキュリティの要件化等を通じ、投資意欲を喚起して、人材の需要を創出。

【供給】人材の「量的拡大」と「質的向上」

○実務を担うボリュームゾーンに当たる既存のIT技術者に、情報セキュリティを必須能力として位置付ける。
- ①技術者に情報セキュリティを意識させるための取組
- ②情報セキュリティ能力の評価基準・資格等の整備
- ③情報セキュリティの実践的スキル向上のための取組

○グローバル化する脅威に対応できる、高度な人材や突出した能力を有する人材を育成・発掘。
- ①高度な専門性を持った情報セキュリティ人材育成のための高等教育の強化
- ②最先端の分野で活躍する突出した人材の発掘及び更なる能力向上

○とりわけ、政府機関等においては、訓練・演習等による内部人材の育成、優秀な外部人材の登用に率先して取り組む。
さらに、調達における情報セキュリティの要件化等を通じ、我が国のセキュリティ水準の向上、人材の需要喚起につなげる。