資料３

「サイバー攻撃解析協議会」開催について（案）

１．開催の趣旨・目的

本年4月26日の第29回情報セキュリティ政策会議において、総務大臣及び経済産業大臣より、近年、攻撃手法がますます巧妙化・複合化するサイバー攻撃を高度解析する枠組みについて、両省で連携して構築していくことを発表（P4,5）。さらに、７月４日の第30回情報セキュリティ政策会議において、これらのサイバー攻撃からの防御に必要な高度解析を実施するため、総務省及び経済産業省並びに(独)情報通信研究機構、(独)情報処理推進機構、テレコム・アイザック推進会議及びJPCERTコーディネーションセンターの４団体からなる「サイバー攻撃解析協議会」（以下「協議会」という。）を発足することについて、両大臣より発表した（P8,9）。

これを踏まえ、今般、両省において「サイバー攻撃解析協議会」を発足する。本協議会の活動によりサイバー攻撃の実態を把握し、その結果を関係省庁や重要インフラ事業者等に提供していく。

２．活動内容・スケジュール

各団体が保有するマルウェア解析結果、攻撃元情報、攻撃の予兆を示すネットワーク関連情報等のうち共有可能なものを結集し、高度解析を実施することにより、業界横断的又は長期間執拗に行われるサイバー攻撃の特徴や攻撃手法等、サイバー攻撃の実態等を把握する。

この活動を円滑に実施するため、今夏を目途に、協議会の下に関係団体から成るWGを設置。WGにおいて、収集情報、提供情報、情報提供先の要件等の検討・整理を行い、その結果は、年度末までに協議会に報告する。

３．構成・オブザーバ

協議会は、総務省及び経済産業省並びに(独)情報通信研究機構、(独)情報処理推進機構、テレコム・アイザック推進会議及びJPCERTコーディネーションセンターの４団体により構成し、内閣官房情報セキュリティセンターをオブザーバとする。

活動内容に応じて、構成等は変更可能とする。

４．庶務

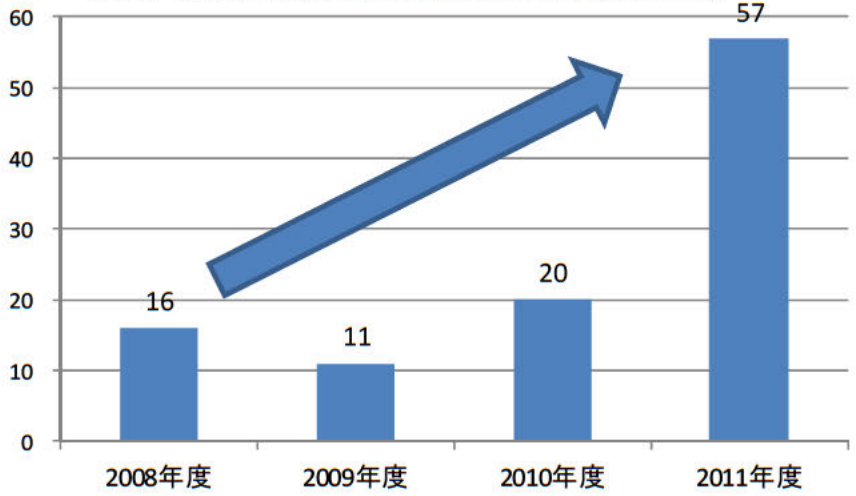
協議会の庶務は、総務省情報流通行政局情報セキュリティ対策室及び経済産業省商務情報政策局情報セキュリティ政策室において処理する。

以上

サイバー攻撃の現状について

■ 特定の組織の機密情報の窃取を目的とした標的型サイバー攻撃に関する相談は、3年で約4倍に増加。

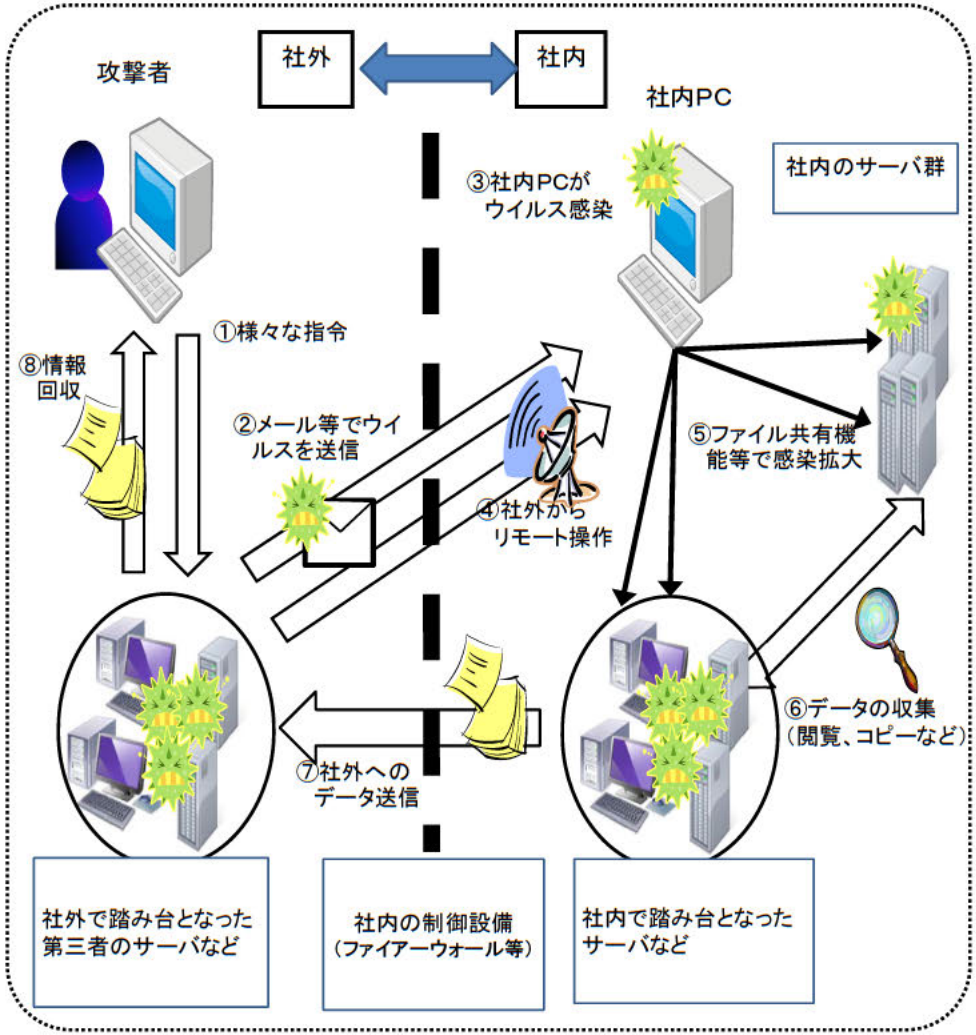
【(独)情報処理推進機構相談窓口での受付件数】



＜サイバー攻撃の事例＞

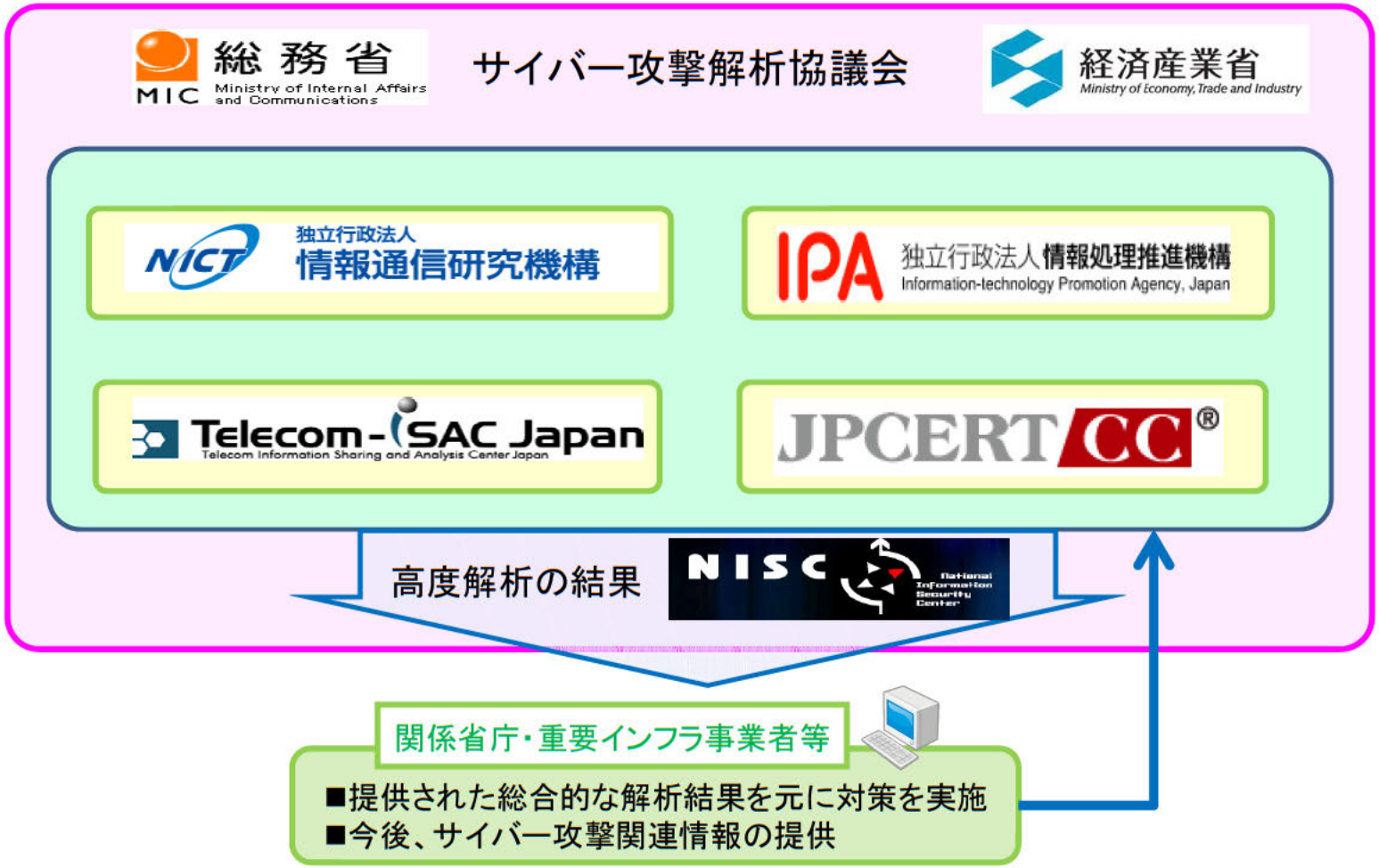
年	事例
平成23年4月	ソニーへのサイバー攻撃により、約1億件の個人情報が漏えい
平成23年7、8月	衆・参議院議員のPCがサイバー攻撃を受け、議員のID・パスワードが流出
平成23年8月	三菱重工業へのサイバー攻撃により、一部情報が漏えい
平成24年5月	(独)原子力安全基盤機構がマルウェア感染
平成24年6月	アノニマスによる政府機関等へのサイバー攻撃

■ 大手先端企業へのサイバー攻撃にみられるように、攻撃手法は、ますます巧妙化・複合化している。



サイバー攻撃解析協議会のイメージ

○ （独）情報通信研究機構、（独）情報処理推進機構、テレコム・アイザック推進会議（Telecom-ISAC Japan）及びJPCERT/CCが保有する情報を元に、サイバー攻撃からの防御に必要な高度解析を実施する。
○ その結果を、NISC経由で関係省庁や重要インフラ関係事業者等へ提供し、サイバー攻撃対策に資する。



最近の情報セキュリティ政策

総務省 MIC Ministry of Internal Affairs and Communications

米国（国土安全保障省）とのサイバーセキュリティ連携

2012年3月22～23日、「インターネットエコノミーに関する日米政策協力対話」（第3回局長級会合）において、以下について合意。

- **米国と日本両政府、民間部門及び研究機関が、サイバー攻撃に関する情報を共有し、研究開発の分野での協力関係を加速化**
- **双方は、二国間及び国際的なサイバーセキュリティ協力の強化を確認**

総務省と国土安全保障省が、サイバー攻撃に関する情報を共有するとともに、サイバー攻撃の対策に向けた研究開発を協力して実施。

総務省

国際連携によるサイバー攻撃予知・即応プロジェクト

総務省 MIC Ministry of Internal Affairs and Communications

NICT National Institute of Information and Communications Technology

Telecom-ISAC Japan Telecom Information Sharing and Analysis Center Japan

国土安全保障省

PREDICT（プレディクト）プロジェクト

Homeland Security

PREDICT Protected Repository for the Defense of Infrastructure Against Cyber Threats

サイバー攻撃に関する情報を共有

ASEAN諸国との連携による人材育成

2012年3月22～23日、セキュアなネットワーク運用等を国際的な協力に基づき実施できる人材の育成を目的に、ASEAN各国のインターネット接続事業者（ISP）等による「日ASEAN情報セキュリティ人材育成ワークショップ」を開催。

サイバー攻撃高度解析機能の整備

近年、攻撃手法がますます複合化・複雑化するサイバー攻撃を高度解析する枠組みについて、経済産業省等と連携して構築していく。

経済産業省における「情報セキュリティ2012骨子案」への主な対応

経済産業省 Ministry of Economy, Trade and Industry

官民連携による情報共有

○ 重要インフラ機器製造業者等の間でサイバー攻撃に関する情報共有を行う枠組みとして昨年10月に発足したJ-CSIP（ジェイ シップ）の下、情報共有のルールに合意。（本年3/21）

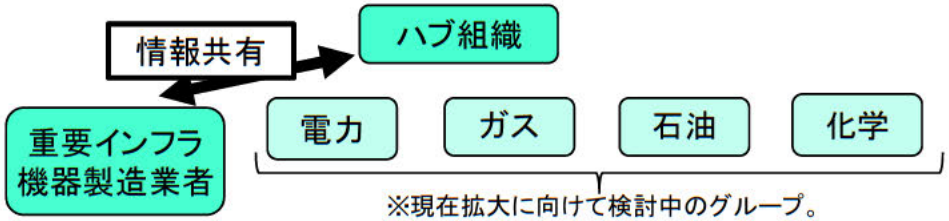
J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan

本年4/2、重要インフラ機器製造業者9社（※）とIPA間で秘密保持契約を締結。ルールに基づく情報共有開始。

※IHI、川崎重工、東芝、NEC、日立、富士重工、富士通、三菱重工、三菱電機

IPA：（独）情報処理推進機構　外部連携先：JPCERT/CC等

○今後、本ルールを踏まえつつ、重要インフラ等の分野にも枠組みを拡大。



サイバー攻撃高度解析機能の整備

近年、攻撃手法がますます複合化・複雑化するサイバー攻撃を高度解析する枠組みについて、総務省等と連携して構築していく。

セキュリティ対策を通じたインフラ輸出強化

○重要インフラ等で活用されている制御システムのセキュリティ強化を図るため、セキュリティ検証施設（テストベッド）を米国の協力を得つつ今年度中に構築。

【テストベッドの構築主体】

技術研究組合制御システムセキュリティセンター

理事長：新誠一（電気通信大学教授）

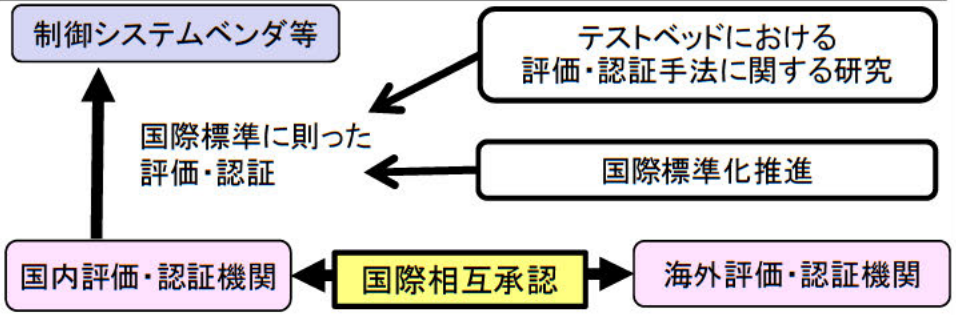
組合員：（独）産業技術総合研究所、IPA、アズビル、東芝、日立製作所、富士電機、三菱重工業、三菱総合研究所、森ビル、横河電機

主たる実施場所：　宮城県多賀城市　みやぎ復興パーク内

※ 米国エネルギー省所管のアイダホ国立研究所では、テストベッドを保有し研究を実施。既に、牧野副大臣と米国エネルギー省チューニング長官との間で新たな研究協力を確認。

○テストベッドにおいて、評価・認証手法に関する研究を行い、競争力強化に資する国際標準化推進（2014年度目途に成立予定）。

○合わせて、評価・認証機関同士の国際相互承認実現に向けた取組を促進。



「情報セキュリティ2012」について

「情報セキュリティ2012」の位置付け

「国民を守る情報セキュリティ戦略」に基づく年度計画

情報セキュリティを取り巻く環境の変化

本格的なサイバー攻撃の発生と深刻化
- 我が国の政府機関における標的型攻撃の顕在化
- 更なる進化が見込まれる標的型攻撃　等

社会経済活動の情報通信技術への依存度の更なる高まりとリスクの表面化
- スマートフォン等の本格的な普及とマルウェア等による脅威の拡大
- 制御システム等に対するリスクの高まり　等

新たな技術革新に伴う新たなリスクの出現
- M2M[※1](Machine To Machine)環境の出現　等

重大な情報通信システム障害のリスク回避に向けた取組の必要性の高まり
- 東日本大震災における電力の喪失や建物の損壊等
- 携帯電話事業者等におけるシステム障害の発生　等

諸外国における取組の強化
- 諸外国における情報セキュリティに対する戦略的な取組の強化
- サイバー空間における国際的規範作りに関する議論の進展　等

基本方針

国や国の安全に関する重要な情報を扱う企業等に対する高度な脅威への対応強化
- 標的型攻撃に係る官民連携の枠組みの構築と情報共有・分析検討の推進
- CSIRT等の機能を有する体制の構築と要員の整備・充実
- 標的型攻撃に効果的な研究開発の推進

スマートフォンの本格的な普及等新たな情報通信技術の広まりに伴うリスクの表面化に対応した安全・安心な利用環境の整備
- スマートフォン利用者への情報セキュリティ対策の周知
- スマートフォン、クラウドコンピューティング、制御システム、M2M等における情報セキュリティの確保

国際連携の強化
- ハイレベルによる戦略的な情報発信
- 情報セキュリティ政策に関する基本方針に基づく、サイバー空間に関する国際的枠組み作りへの参画

※1　ネットワークに繋がれた機械同士が人間を介在せずに相互に情報交換し、自動的に最適な制御が行われるシステムを指す。

「情報セキュリティ2012」の主要な施策

1　標的型攻撃に対する官民連携の強化等

○ 官民の情報共有の更なる推進（内閣官房、関係府省庁）
○ CSIRT等の体制の整備及び連携の強化（内閣官房、全府省庁）
○ サイバー攻撃高度解析機能の整備（総務省、経済産業省）

2　大規模サイバー攻撃事態に対する対処態勢の整備等

○ 大規模サイバー攻撃事態等発生時の初動対処に係る訓練の実施等（内閣官房、関係府省庁）
○ サイバー防護分析装置の機能強化（防衛省）
○ 悪質・巧妙化するサイバー犯罪の取締りのための態勢の強化（警察庁）

3　政府機関等の基盤強化

○ 情報セキュリティ緊急支援チーム(CYMAT)の設置（内閣官房、全府省庁）
○ 情報セキュリティガバナンスの高度化に向けた取組（内閣官房、全府省庁）

4　重要インフラの基盤強化

○ 共有脅威分析の実施（内閣官房）
○ 分野横断的演習の実施（内閣官房、重要インフラ所管省庁）
○ 制御システムに関する情報セキュリティの確保（経済産業省）

5　情報通信技術の高度化・多様化への対応

○ 官民連携・国際連携によるスマートフォン等の情報セキュリティ確保の推進（総務省、経済産業省）
○ 社会基盤としてのクラウドコンピューティングの情報セキュリティ確保の推進（総務省、経済産業省）
○ M2Mにおける情報セキュリティの在り方の検討及び研究開発の推進（内閣官房、総務省、経済産業省）

6　研究開発、産業振興の推進

○ 「情報セキュリティ研究開発戦略」の研究開発の推進（内閣官房、関係府省庁）
○ 情報セキュリティ産業の振興（内閣官房、総務省、経済産業省）

7　情報セキュリティ人材の育成

○ 情報セキュリティに係る競技会等の実施（総務省、経済産業省）
○ 情報セキュリティに関する教育における産学連携の促進（文部科学省、経済産業省）

8　情報セキュリティリテラシーの向上等

○ 「情報セキュリティ普及・啓発プログラム」の推進（内閣官房、関係府省庁）
○ 国際連携を活用した普及・啓発活動の実施（内閣官房、関係府省庁）

9　制度整備

○ サイバー刑法の円滑な施行（法務省）
○ 改正不正アクセス禁止法の適正な運用を始めとした不正アクセス防止対策の推進（警察庁、総務省、経済産業省）

10　国際連携の強化

○ ハイレベルによる戦略的な取組の強化（内閣官房、外務省、関係府省庁）
○ サイバー空間に関する国際規範作りへの参画等（内閣官房、外務省、関係府省庁）

最近の情報セキュリティ対策

総務省 MIC Ministry of Internal Affairs and Communications

サイバー攻撃高度解析機能の整備

○近年、攻撃手法がますます巧妙化・複雑化するサイバー攻撃に対応するため、サイバー攻撃解析協議会を発足予定（平成24年7月12日）。

○協議会の参加機関が保有する情報を元に、サイバー攻撃からの防御に必要な高度解析を実施。

○その結果を、NISC経由で関係省庁や重要インフラ関係事業者等へ提供し、サイバー攻撃対策に資する。

総務省 MIC Ministry of Internal Affairs and Communications　サイバー攻撃解析協議会　経済産業省 Ministry of Economy, Trade and Industry

- 独立行政法人 情報通信研究機構 NICT
- 独立行政法人 情報処理推進機構 IPA Information-technology Promotion Agency, Japan
- Telecom-SAC Japan Telecom Information Sharing and Analysis Center Japan
- JPCERT CC®

高度解析の結果　NISC National Information Security Center

関係省庁、重要インフラ事業者、その他関係企業等

スマートフォンの情報セキュリティ対策

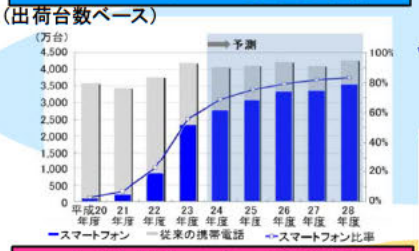
○平成23年10月、「スマートフォン・クラウドセキュリティ研究会」（座長：山口英　奈良先端科学技術大学院大学教授）を設置。同年12月に中間報告、平成24年6月29日に最終報告をとりまとめ。

○事業者・政府等における対策及び利用者への普及啓発方策を提言。

背景

スマートフォンの急速な普及

（出荷台数ベース）



マルウェアの種類の増加

対策

事業者等における対策

○マルウェアを含むアプリケーションの作成・流通・インストール防止対策

○アプリケーション提供サイトの運営方針開示等、利用者が自衛できる環境の構築

○OSのぜい弱性対策

○無線LANの情報セキュリティ対策

利用者への普及啓発

スマートフォン
情報セキュリティ３か条

1．ＯＳ（基本ソフト）を更新
2．ウイルス対策ソフトの利用を確認
3．アプリケーションの入手に注意

政府における対策

○事業者等と連携しアプリケーションの性質の可視化の枠組みを整備

○利用者保護のための技術の研究開発

○利用者への総合的な普及啓発の実施

○国際連携の推進

＊今後、事業者・政府等の取組を定期的にフォローアップし公表

経済産業省における「情報セキュリティ2012案」への主な対応

経済産業省 Ministry of Economy, Trade and Industry

官民連携による情報共有

○サイバー攻撃に関する情報共有を行う枠組みとして昨年10月に発足したJ-CSIP（ジェイ・シップ）について、**新たに4グループ、14組織が参加を表明**。

○今後、更なる参加企業の拡大を検討。

J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan

J-CSIP（ジェイ・シップ）

ハブ組織（IPA）

新たに参加を表明

重要インフラ機器製造事業者	IHI、川崎重工、東芝、NEC、日立、富士重工、富士通、三菱重工、三菱電機
電力	電気事業連合会（6月29日参加）
ガス	日本ガス協会
石油	石油連盟、JX、出光興産、昭和シェル石油、富士石油
化学	宇部興産、昭和電工、住友化学、電気化学工業、トクヤマ、三井化学、三菱化学

サイバー攻撃高度解析機能の整備

○近年、攻撃手法がますます巧妙化・複雑化するサイバー攻撃に対応するため、**サイバー攻撃解析協議会を発足予定（7月12日）**。

○協議会の参加機関が保有する情報を元に、サイバー攻撃からの防御に必要な高度解析を実施。

○その結果を、NISC経由で関係省庁や重要インフラ関係事業者等へ提供し、サイバー攻撃対策に資する。

総務省 MIC Ministry of Internal Affairs and Communications　**サイバー攻撃解析協議会**　経済産業省

- NICT 独立行政法人 情報通信研究機構
- IPA 独立行政法人 情報処理推進機構 Information-technology Promotion Agency, Japan
- Telecom-ISAC Japan
- JPCERT CC®

高度解析の結果　NISC

関係省庁、重要インフラ事業者、その他関係企業（J-CSIP参加企業）等

制御システム等のセキュリティ確保

○制御システムを含めた総合的なサイバー演習を**電力、ガス、データセンター分野**において実施。

○制御システムのセキュリティを確保するため、日米連携によるシンポジウムを7月13日に開催。

高度情報セキュリティ人材の育成

○若手向けセキュリティキャンプの実施（8月）。

○セキュリティコンテスト全国大会の実施（年度内）。

○情報セキュリティ人材の能力・知識の体系化。