最近のサイバー攻撃の動向

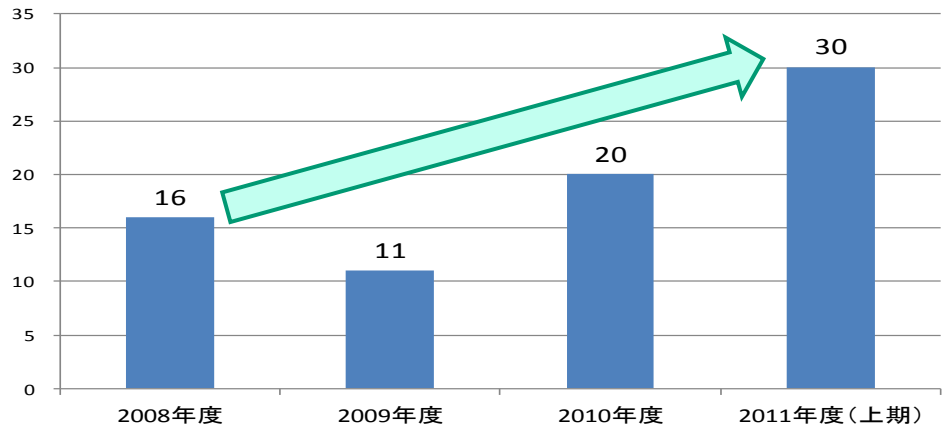
経済産業省 Ministry of Economy, Trade and Industry

資料1

標的型サイバー攻撃の増加

■ 特定の組織の機密情報等の詐取を目的とした標的型サイバー攻撃に関する相談は、2年半で2倍に増加。

【(独)情報処理推進機構(IPA)相談窓口での受付件数】



(経済産業省への標的型サイバー攻撃事例)

- 平成22年11月、経済産業省の職員を装い、情報流出の機能があるウイルスが添付されたメールを省内職員宛に送付。
- 約20人の職員が開封し、ファイルを実行したが、ウイルスは機能せず、情報流出は無し。

(標的型攻撃メールのイメージ)

From: ●●●@●●●.go.jp
To: ●●
Subject:【最新資料送付・取扱注意】【表敬時間変更】【暫定版送付】11月25日(木)16:00～16:30大畠大臣×ムハメジャノフ・カザフスタン共和国下院議長について

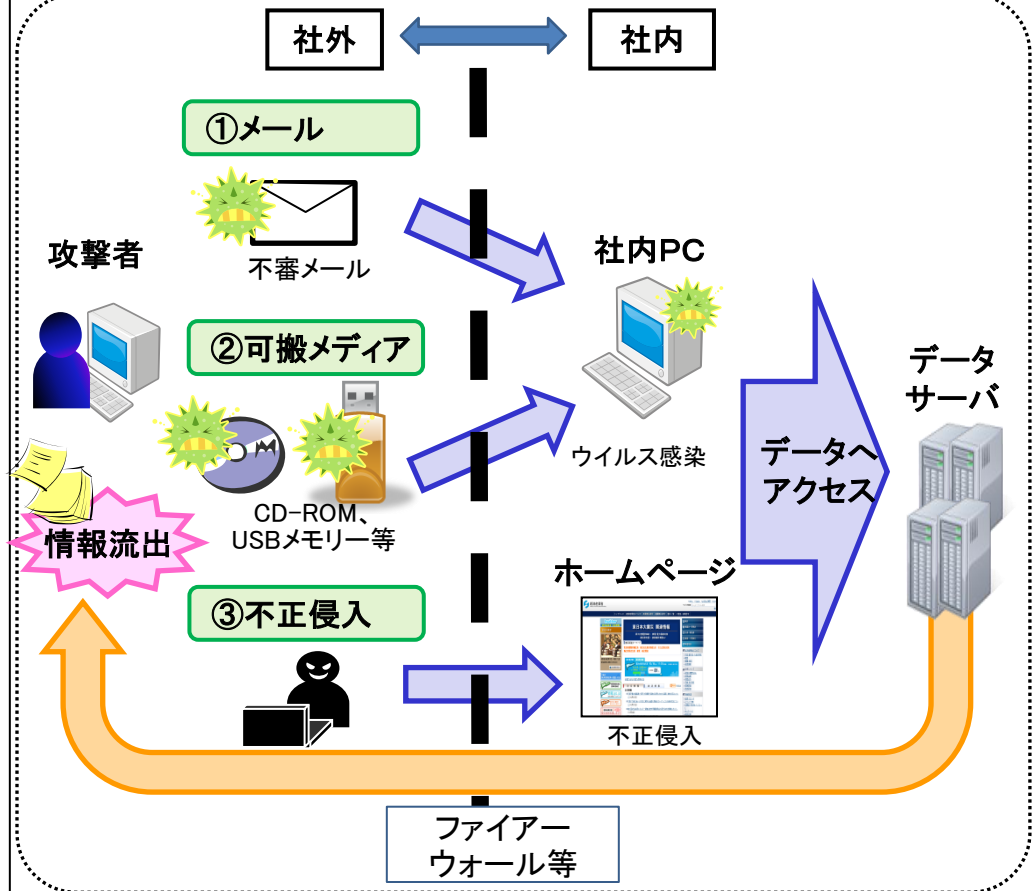
各位 ＞

大変お世話になっております。
本日10:30～10:45、標記表敬に関して●●審議官レクを行いました。
結果、発言応答要領のP6とP7が変更(内容を簡素化)となりましたので共有いたします。

また、以上をもちまして大畠大臣レク用資料セットとなりましたので共有いたします。


meit.lzh

標的型サイバー攻撃のイメージ



年	事例
平成22年9月	イランの核施設へのサイバー攻撃
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8月	三菱重工へのサイバー攻撃により、一部のコンピューターシステム等の情報が漏えいした可能性(調査中)

標的型サイバー攻撃に対するこれまでの対策

経済産業省
Ministry of Economy, Trade and Industry

企業等の実態調査
［以下の調査の内容について、NISCに情報共有］

【防衛・原子力産業】（緊急聞き取り調査）

実施期間：9月20日～10月24日

■ 防衛・原子力産業等8社への標的型サイバー攻撃を踏まえ、（独）情報処理推進機構（IPA）の協力の下、調査を実施。

○三菱重工と類似の事案があるかについて聞いたところ、全ての企業が、最近標的型を含む不審メールを受信。

○このうち、4社の一部端末がウイルスに感染。

ある 4社	確認されていない 4社

○製品・技術に関するデータの一部が、社内サーバー間で意図しない形で移動したことが判明。当該サーバから何らかのデータの一部が社外に流出した可能性があることを確認した社がある。
　ただし、現時点で防衛や原子力に関する保護すべき情報が流出したことは確認されていない。

○その他の社については、製品・技術情報の漏えいは、現在確認されていない。

（調査対象）三菱重工、IHI、川崎重工、富士重工、日立、東芝、三菱電機、日本航空宇宙工業会　（計8社）

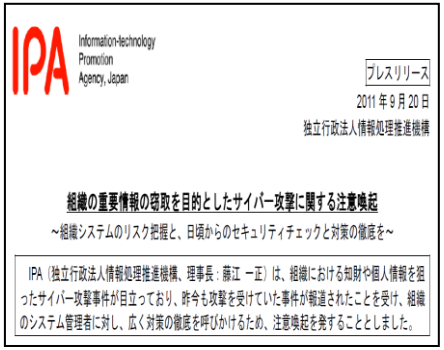
IPAによる対策

■ IPAは、HPにおいて注意喚起を実施するとともに、対策情報を公表。

【1．注意喚起の発出等】

9月20日、29日、10月18日に、標的型サイバー攻撃に対する注意喚起を発出。

合わせて、標的型サイバー攻撃に対応するための対策を改めて紹介。


IPA Information-technology Promotion Agency, Japan
プレスリリース
2011年9月20日
独立行政法人情報処理推進機構
組織の重要情報の窃取を目的としたサイバー攻撃に関する注意喚起
～組織システムのリスク把握と、日頃からのセキュリティチェックと対策の徹底を～
IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、組織における知財や個人情報を狙ったサイバー攻撃事件が目立っており、昨今も攻撃を受けていた事件が報道されたことを受け、組織のシステム管理者に対し、広く対策の徹底を呼びかけるため、注意喚起を発することとしました。

10月3日には、標的型サイバー攻撃についての技術的な分析結果を公表。

【2．相談窓口による対応】

従来より相談窓口を設置しているところ、改めて周知徹底。（標的型サイバー攻撃を含むサイバー攻撃全般の相談を受付。）

IPA 情報セキュリティ安心相談窓口

（相談件数）

9/11-9/20	9/21-9/30	増加率
516	563	約10%

サイバー攻撃に対する今後の対策

経済産業省
Ministry of Economy, Trade and Industry

経済産業省としては、昨年12月以来、サイバーセキュリティと経済研究会（委員長：村井純慶應義塾大学教授）において、標的型サイバー攻撃対策等について検討。本年8月、中間とりまとめを公表。これを踏まえ、下記の対策を実施。

サイバー情報共有イニシアティブ（J-CSIP）の発足

■ サイバー攻撃による被害拡大防止のため、重工、重電等、重要インフラで利用される機器の製造業者を中心に情報共有の場を構築。

【メンバー】

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、ラック、（独）情報処理推進機構（IPA）、（社）日本情報システム・ユーザー協会、JPCERT/CC、経済産業省

■ 今年度中、情報共有ルール等の整備を実施。（委託調査実施中）。順次、参加企業を拡大。

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

【今後の予定】

本年10月以降

J-CSIPを発足

情報共有ルール等の整備

参加企業拡大

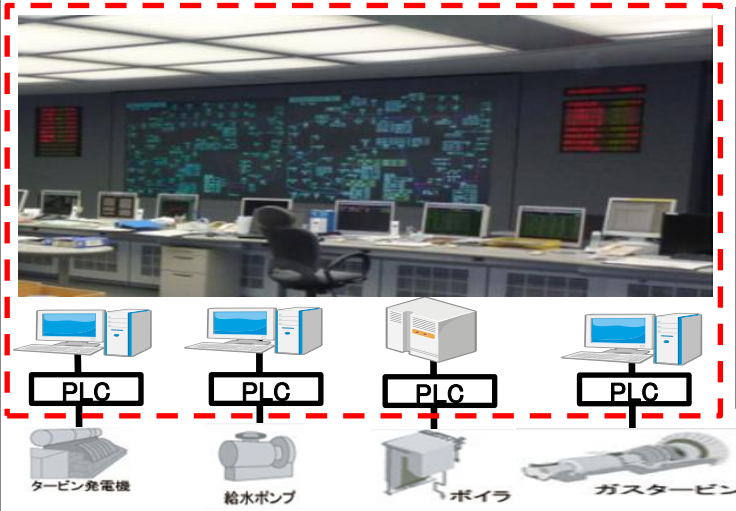
重要インフラ等のセキュリティ強化

■ 重要インフラ等のセキュリティ検証施設を構築、セキュリティ検証に関し日米協力（※）を実施。

※ 米国エネルギー省所管のアイダホ国立研究所では、重要インフラ等の制御システムの実機に対して模擬サイバー攻撃を行うセキュリティ検証施設を保有し、研究を実施。

本年9月、牧野副大臣とチュー米国エネルギー省長官との会談において、新たに研究協力を行うことを確認。

【セキュリティ検証施設内のイメージ】



重要インフラ等の制御システムに対して模擬サイバー攻撃を行い、セキュリティ検証を実施。

■ 重要インフラ等のセキュリティ強化に向けた諸課題（セキュリティ基準、評価手法等）を検討するため、今月、官民によるタスクフォースを設置。来年春を目途に中間報告。