山下塾第４弾

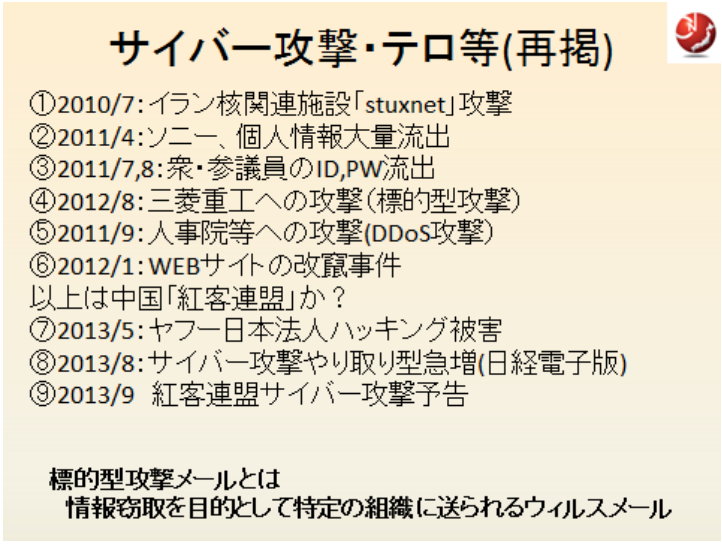
山下 輝男

第７回　我が国のテロ対策の現状と課題

第７回　講座

始めに
　今最も懸念されているサイバー攻撃・テロについてみてみましょう。

１　サイバー攻撃・テロ概観
　サイバー攻撃に関する最近の状況を確認します。



２　サイバー攻撃対処等
　サイバーテロについて、警察白書では、「コンピューター・ネットワークを通じて各国の国防・治安等をはじめとする各種分野のコンピューター・システムに侵入し、、データを破壊、改竄する等の手段で国家または社会の重要な基盤を機能不全に陥れるテロ行為」と規定している。
　先ず、政府の体制等についてみてみましょう。サイバー攻撃により、我が国の安全保障上の防衛や我が国の重要インフラの防護そして、経済的な基礎である重要な情報の防護のために政府としても重視して取り組んでいます。その状況を説明します。

サイバー攻撃・テロ

1　標的型サイバー攻撃
　対策ソフト機能せず(日経電子版25/8/22)
　特定IP標的ウィルス被害(読売25/10/9　次VG)
2　政府の対処態勢、情報収集・共有体制
　内閣官房に「情報セキュリティセンター(NISC)」
3　リアルタイム検知ネットワークシステムの24時間運用等　(警察庁)
4　重要インフラ10分野:情報通信、金融、航空、鉄道、ガス、政府・行政サービス、医療、水道、物流
5　県警:サイバー攻撃特別捜査隊(サイバーフォース)、サイバー攻撃対策官&分析センター
6　重要インフラ事業者等との連携強化


官庁や大企業 被害
特定IP 標的ウイルス
サイト閲覧で感染
「日本狙う新たな手口」

3　サイバーセキュリティ戦略の変遷

　サイバー空間における対処については、当初は情報セキュリティ基本計画として、次いで、情報セキュリティ戦略として策定されましたが、今年６月にサイバーセキュリティ戦略として策定されました。これはサイバー空間における脅威の増大に伴いより対応を強化しようというものです。

サイバーセキュリティ

1　経緯
　情報セキュリティ基本計画(Ⅰ，Ⅱ)
　↓
　情報セキュリティ戦略(2010/5)
　↓
　サイバーセキュリティ戦略

2　サイバーセキュリティ戦略策定の背景
　サイバーリスクの甚大化、拡散、グローバル化
　国家や重要インフラへのサイバー攻撃の現実化
　従来施策からの次元を超えた取り組みの実施

4　サイバーセキュリティ戦略策定に至る経緯の概要

　2005年、情報セキュリティ政策会議が設置され、以来一次二次の情報セキュリテイ基本計画、国民を守る情報セキュリティ戦略が策定されてきたが、この推移を表で示せば次のスライドの通りである。

情報セキュリティ政策の推移(参考)

5　サイバーセキュリティ戦略の概要

今年6月に策定されたサイバーセキュリティ戦略の概要は次のスライドの通りです。

サイバーセキュリティ戦略の概要

1　策定2013/6　対象期間　～2015年

2　リスクの深刻化、甚大化、拡散、グローバル化

3　基本的考え

①サイバーセキュリティ立国を目指す

②・情報の自由な流通の確保

・深刻化するリスクへの新たな対応→多層的な取組

・リスクベースによる対応の強化

・社会的責務を踏まえた行動と共助

③国、重要インフラ事業者、企業・教育機関等の役割や方向性を明示

サイバーセキュリティ戦略の概要(2)

④取組分野

・強靭なサイバー空間の構築

政府横断的な対策強化、GSOCの抜本的強化

サイバー空間犯罪対策強化

武力攻撃一環のサイバー攻撃対処

：サイバー防衛隊(仮称)

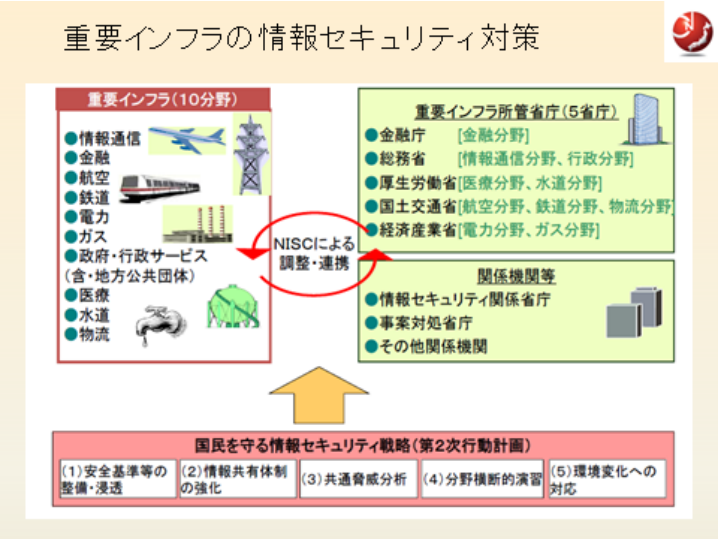
・活力ある、世界を率先するサイバー空間構築

⑤・NISCの「サイバーセキュリティセンター」への改組

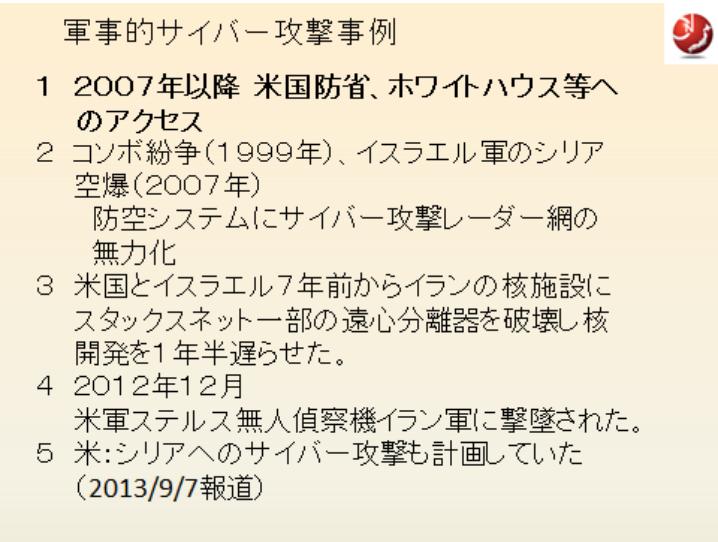
・日本版NCFTA(サイバー犯罪対策のための産官学連合)の創設等

6　重要インフラの情報セキュリティ対策について

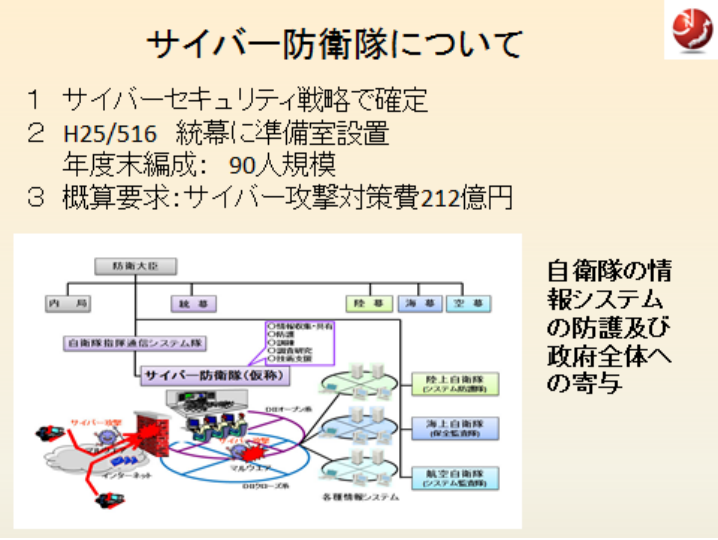
サイバーセキュリティ戦略において、現行「重要インフラの情報セキュリティ対策に係る第二次行動計画」を見直すこととしているが、現行第二次行動計画の概要は以下の通りである。



7軍事施設がサイバー攻撃を受けた事例
　最も安全に気を使うべき軍事施設も軍事的サイバー攻撃を受けております。



8　サイバー防衛隊について
　サイバーセキュリティ戦略で規定されている自衛隊のサイバー防衛隊の概要は以下の通りです。我が国のサイバー防衛の先導役になって貰いたいものですが、少々規模が小さ過ぎはしないかとの懸念を感じるのは小生のみでしょうか？一騎当千のサイバー戦士になって欲しいものです。



9　サイバー攻撃が安全保障上の重要な脅威であることは論を俟たないが、幾つか整理すべき点があると考えられる。
　日米サイバー協議が新設され、情報の共有、対応訓練、専門家育成、民間企業との連携強化などに取り組むこととされており、大いなる前進が期待できる。

安全保障の観点から:新たな課題提起

1　サイバー攻撃は安全保障上の脅威だが、
　我が国に対する武力攻撃事態と認定できるか？
　　どの時点で認定できる？
　自衛権の発動要件との関係は？
　（外国からの組織的･計画的武力行使か？）

2　防衛
　○　防衛の対象は自衛隊のみで良いのか？
　○　装備機材は、国家的対応･連携は？
＊サイバー防衛隊の編成と能力は十分か？

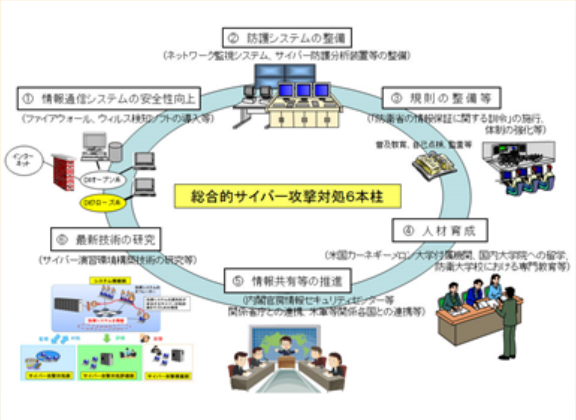
安全保障の観点から:新たな課題提起（2）

3　対抗策は、
　○　カウンター攻撃が出来るか
　　*米国は通常兵器での報復も可としているが・・
　　（米国の「サイバー戦略」）
　○　攻撃者を特定し得るか、民間であった場合
　　対応できるのか？

4　日米共同連携
　日米サイバー防衛協議を新設（9/24Y紙報道）
　サイバー防衛をガイドラインに(9/30Y紙報道)

尚、参考までに防衛省のサイバー攻撃対処について説明します。

サイバー攻撃対処（防衛省HP）



防衛省の取組（報道ベース）

○防衛省：サイバーディフェンス連携協議会（CDC） 7/12
防衛省と防衛産業の間
情報共有、共同訓練、対処能力向上
官民情報共有システムの導入

○H26予算要求 関連経費＝240億円。
- サイバー情報収集装置の整備：27億円
- 次期サイバー防護分析装置のシステム設計等：19億円
- サイバー防護分析装置の整備：4億円
- 防衛情報通信基盤（DII）の整備：135億円
- ネットワークサイバー攻撃対処技術の研究：8億円

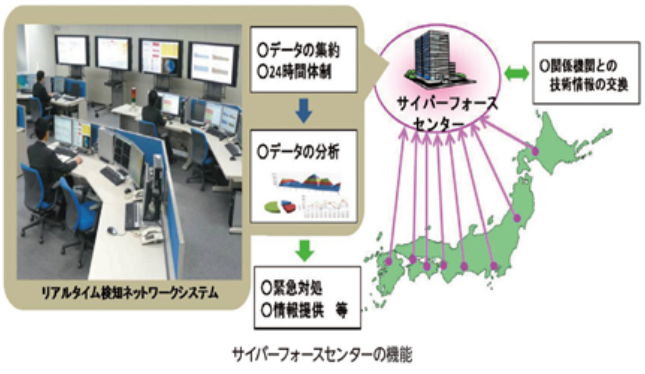
日米サイバー防衛


サイバー防衛 日米指針に
中国をけん制 再改定協議へ


日米サイバー防衛協議
来月上旬合意へ 中国念頭に対策

１０　サイバー攻撃への対処態勢の充実・強化
　政府機関におけるサイバー攻撃認知・解析能力等の向上、インシデント発生時の対処態勢の充実・強化が必要である。
　政府は司令塔としてのＮＩＳＣの強化、ＧＳＯＣ（政府機関・情報セキュリティ横断監視・即応調整チーム）の抜本的強化等を行うこととなっています。サイバー対処の実動対処の任にある警察においてはスライドのような態勢をとっています。

サイバーフォースセンター



サイバーフォースセンターの機能

警視庁サイバー犯罪対策課 200人から260人に増員
（来年秋までに）（9/20報道）

以上で、第７回講座を終了します。
次回は、大量輸送機関等のテロ対策等について検討しましょう。

お勧め記事：　防衛駐在官と危機管理

キーワード アルジェリア人質拘束事件・ サイバー攻撃・ テロ・ テロ対策・ 地下鉄サリン事件

INDEXへ戻る

次の記事　山下塾第4弾 第８回 我が国のテロ対策の現状と課題

前の記事　山下塾第4弾 第６回 我が国のテロ対策の現状と課題

ページの先頭へ

関連サイト　防衛省　統合幕僚監部　陸上自衛隊　海上自衛隊　航空自衛隊