2012/05/24

我が国情報セキュリティ戦略についての一考察

損 保 ジ ャ パ ン　顧 問
（前　内閣官房情報セキュリティセンター長）
西 川　徹 矢

私とIT･情報セキュリティとの関わり

昭和22.6大阪府生、同41.3府立高卒、同41.4大学工学部入学、同43.4法学部に転学部、同47.3法学部卒

昭和47.4警察庁入庁（愛知県警中署見習(同47)、青森県警捜二課長(同50)、警視庁捜二課長代理(同52、同)神田署長(同54)、同第三機動隊長(同55)、在マニラ大使館一等書記官(同58)、警察庁捜一･会計課理事官(同61)、警視庁捜二課長(平元)、同刑事部･防犯部参事官(同3)、和歌山県警本部長(同5)、警察庁情報通信企画課長(同7)、新潟県警本部長(同10)

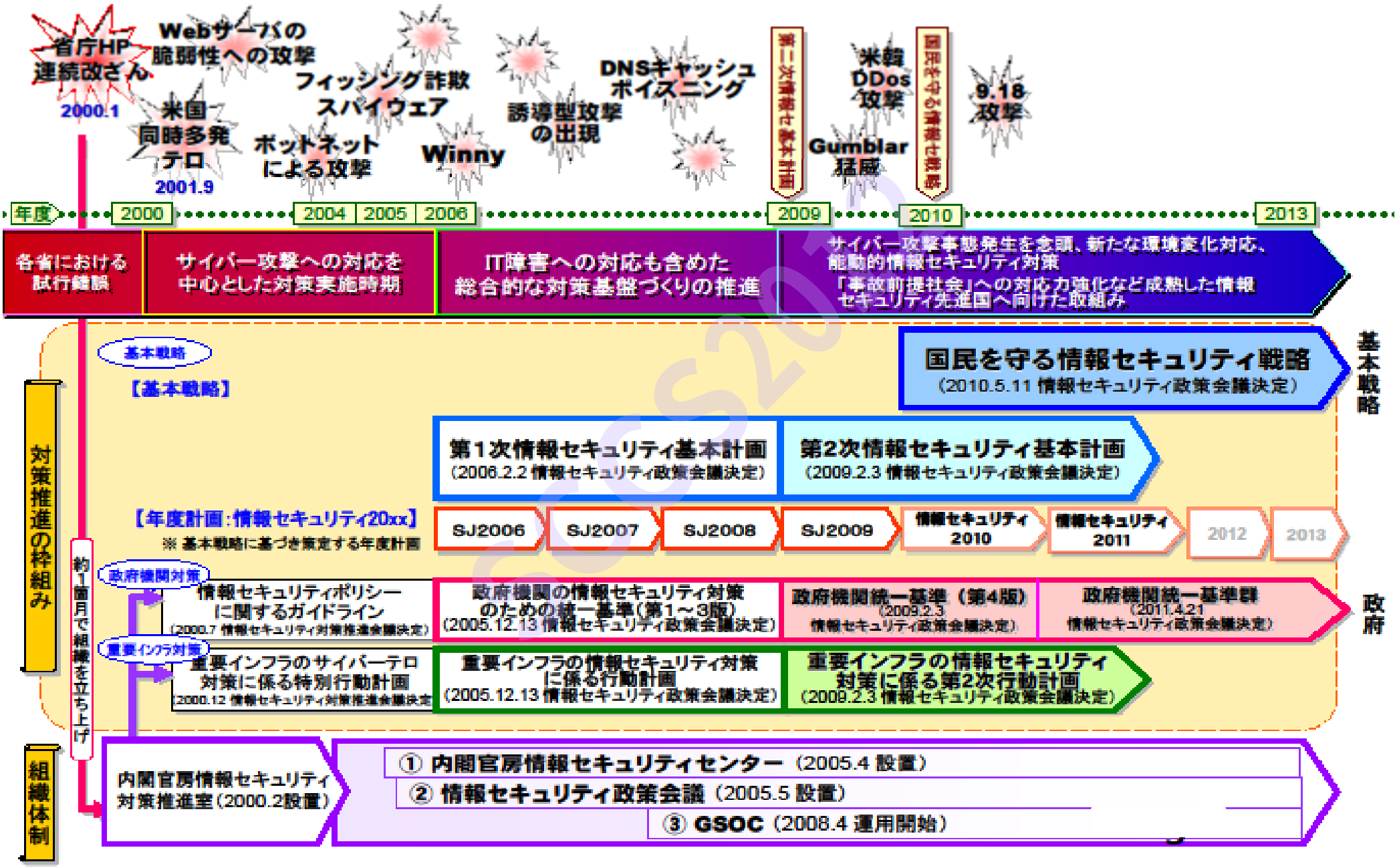
平成11.5防衛庁(省)勤務（防衛審議官(運用局担当)(同11)、防衛参事官(IT、施設、環境担当)(同12)、運用局長(同14)、人事教育局長(同16)、官房長(同17)、退官(同19)

平成19.12生保顧問(同19)、弁護士登録(同21)、内閣官房副長官補(安全保障･危機管理担当)(兼NISC長)(同21)、損保顧問(同23)

その他活動　南紀白浜(平8)、越後湯沢(同10)ITセキュリティ関連事業立上以来参画等

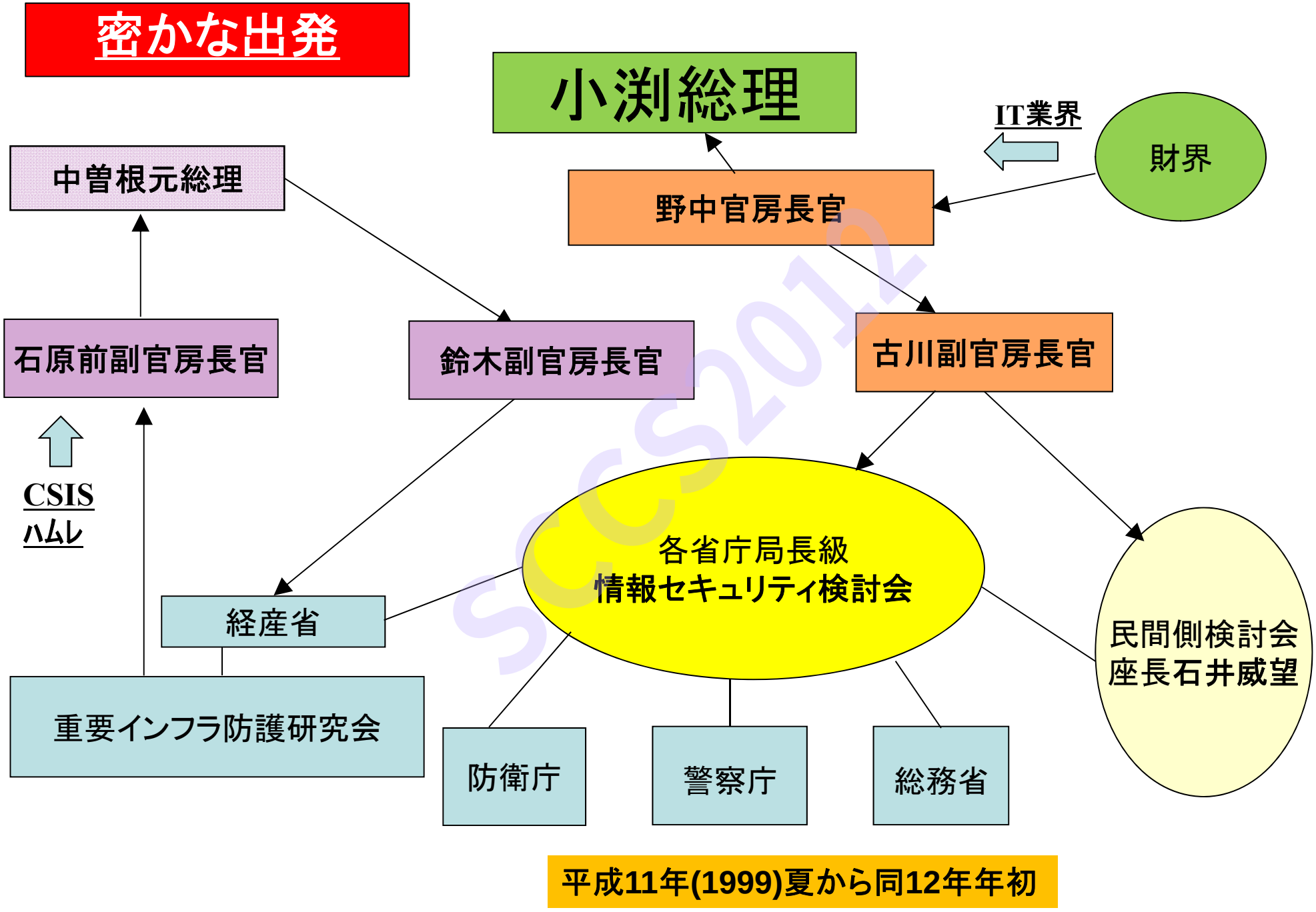
青字のポストは傍系担当職として、赤字のポストは直系担当職として関与
いずれも技術者ではない形(管理)で情報セキュリティに関与
その出発点は捜査情報管理（愛知県警中署見習(昭和47)時代）から

我が国における情報セキュリティの始まりと変遷



我が国の危機管理法制定に至る背景

198911	H元	東独、西側への自由出国を許可(ベルリンの壁の実質的崩壊)
199010	H02	東西ドイツ統一
199207	H04	米、国外の地上、海上配備戦術核の国内への撤去完了
199302	H05	北朝鮮、寧辺周辺の核施設に対する特別査察拒否
199303		北朝鮮、NPT脱退を宣言
199305		北朝鮮、日本海に向け弾道弾ミサイル発射(ノドン)
199308		細川内閣発足
199402	H06	日米首脳会談
199402		大綱見直しに向け、防衛問題懇談会が議論を開始
199406		北朝鮮、IAEAからの脱退を米国に通知
199406		カーター元米大統領訪朝、金日成主席と会談
199408		防衛問題懇談会、報告書提出(→周辺事態関連の記述なし)
199410		米朝「枠組み文書」に署名
199501	H07	阪神淡路大震災(17日)
199502		大規模災害で緊急参集チーム招集制度設立
199503		地下鉄サリン事件(20日)
199506		全日空機乗取り事件
199511	H07	新「防衛計画の大綱」策定(→周辺事態について初めて記述)
199604	H08	官邸危機管理センター発足
199604	H08	日米安保共同宣言(→周辺事態における日米協力に言及)
199605		内閣情報集約センター発足
199701	H09	ロシアタンカーナホトカ号海難・油流出事故
199709	H09	新「日米防衛協力の指針」(ｶﾞｲﾄﾞﾗｲﾝ)、2+2で了承(周辺事態への対応を明記)
199804	H10	内閣法一部改正により内閣危機管理監設置を決定
199905	H11	「周辺事態安全確保法」成立(船舶検査活動部分は法律から削除)
200101	H13	内閣副長官補(危機管理・安全保障担当)
200101	H13	内閣危機管理監設置
200103	H13	「船舶検査活動法」施行


密かな出発
小渕総理
IT業界
財界
中曽根元総理
野中官房長官
石原前副官房長官
鈴木副官房長官
古川副官房長官
CSIS
ハムレ
各省庁局長級
情報セキュリティ検討会
経産省
民間側検討会
座長石井威望
重要インフラ防護研究会
防衛庁
警察庁
総務省
平成11年(1999)夏から同12年年初

近年の情報セキュリティに係る脅威の動向

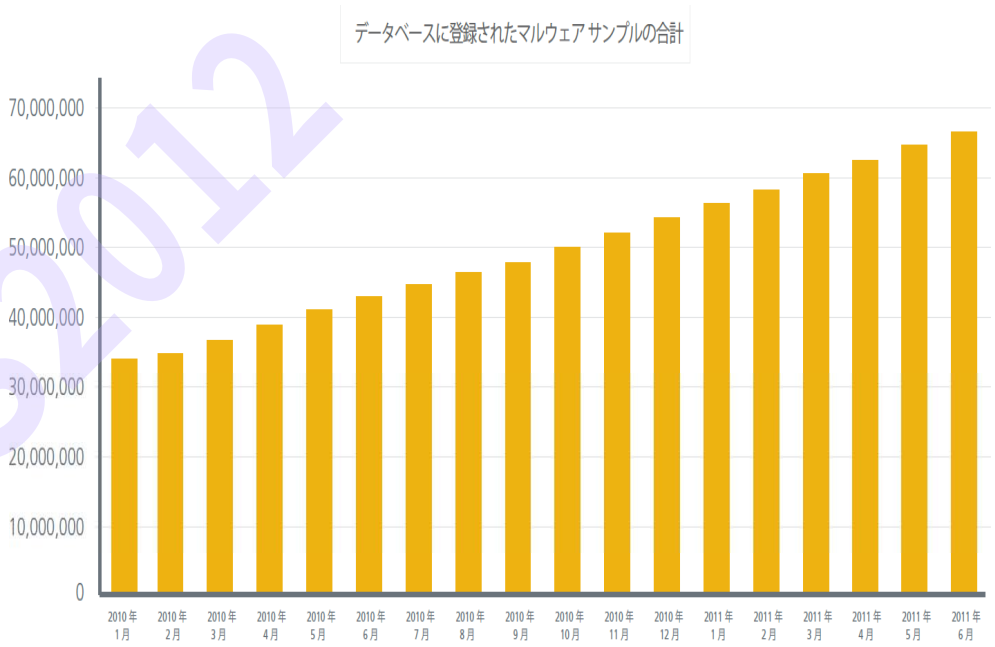
最近の情報セキュリティに係る脅威は、ますます大規模化・高度化・複雑化
政府機関や民間企業に対するサイバー攻撃の脅威も現実化

最近の事例

2007.4	エストニア政府機関等へのDDoS攻撃（注1）
2007.10	鉄道業A社の自動改札システムで障害　首都圏約660駅で計4400台の改札機が使用不能に　260万人に影響
2008.5	金融業B社でシステム障害　約2万件が取引不能
2008.8	グルジア政府機関へのDDoS攻撃
2008.9	航空業C社でシステム障害　53便欠航、276便に遅れ
2009.2	D県HPへ大量アクセス　一時閲覧しにくい状態に
2009.4	E省のHP改ざん
2009.4	F省地方支分部局の非公開HPの改ざん
2009.7	韓国、米国政府機関等への大規模なDDoS攻撃
2009末	「ガンブラー攻撃」（注2）によるウェブサイト改ざん被害等が増加
2010.9	我が国政府機関等へのサイバー攻撃事案
2011.3	韓国政府機関等への大規模なDDoS攻撃
2011.3	金融業F社でシステム障害。送金処理の遅延等が発生
2011.4	G社米国子会社のネットワークへの不正侵入　最大で7700万人分の顧客情報が流出
2011.9	H社等への標的型攻撃によるウィルス感染が発覚
2011.9	J社等への標的型攻撃によるウィルス感染が発覚

ウイルス種類の増加状況

【出典】米マカフィー社

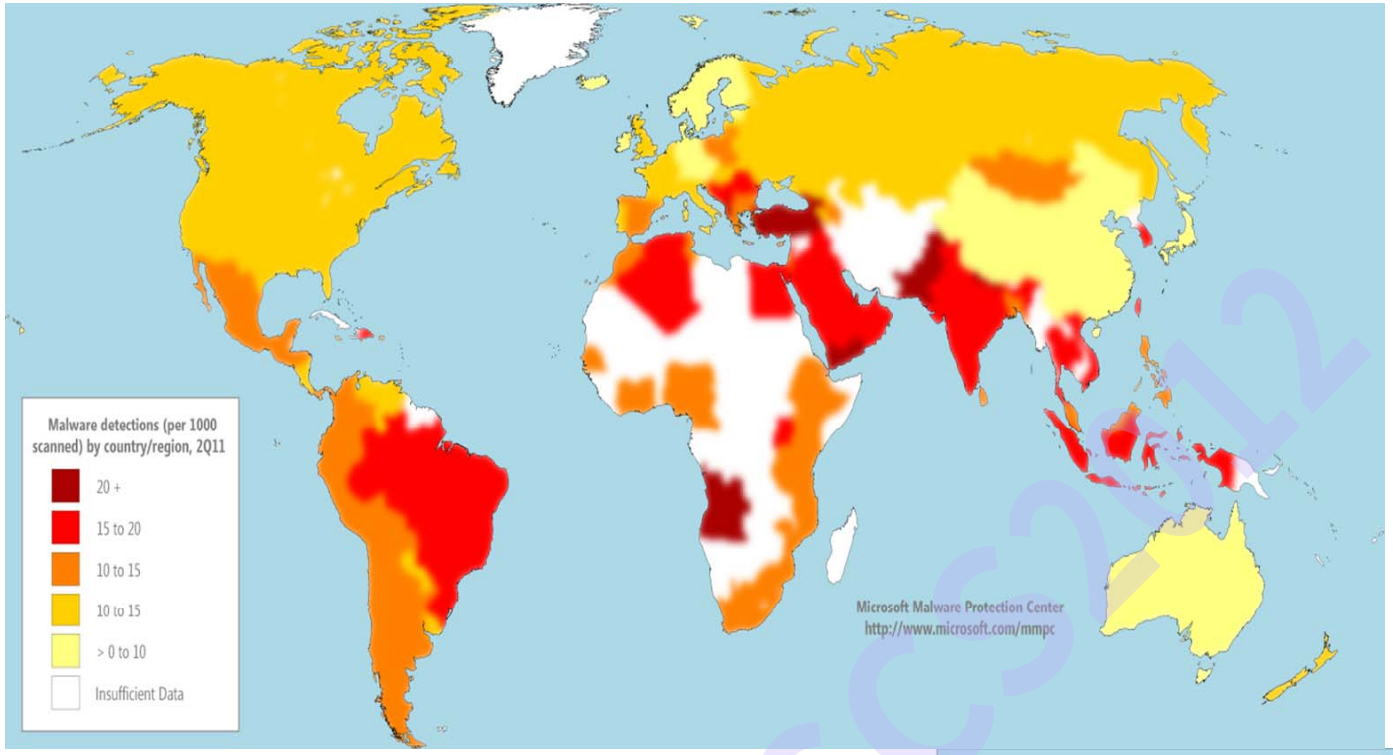


（注1）Distributed Denial of Service（分散サービス妨害）

（注2）コンピュータウイルスによる攻撃の一種であり、一般企業のホームページに潜り込むことで、利用者に感染を広めていく攻撃手段を特徴とする。

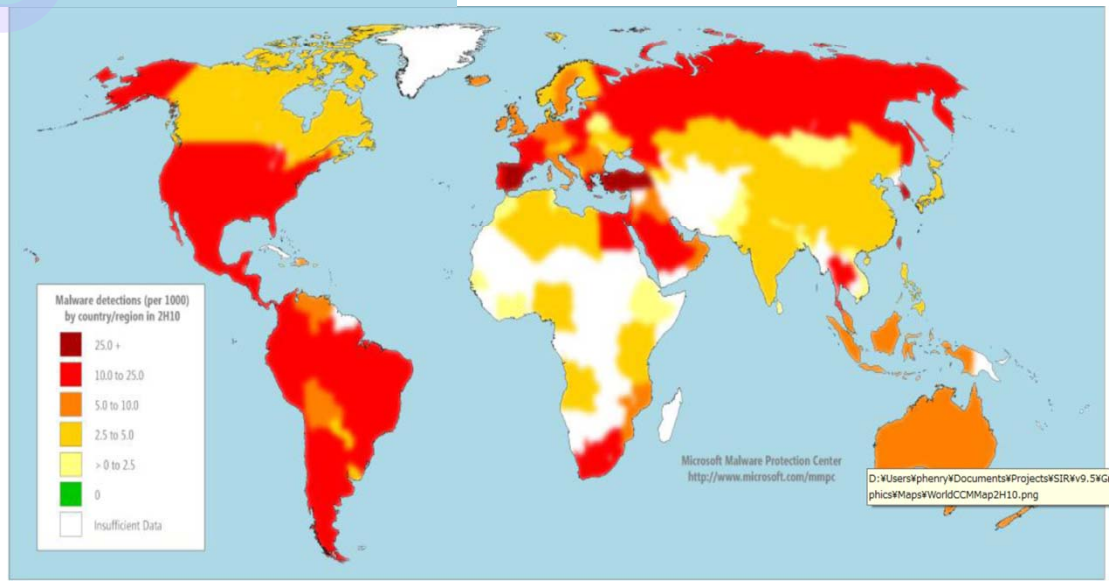
※　本資料は報道ベースで作成

世界のマルウェア感染率の推移



2011年4～6月

我が国のマルウェア感染率（0.21%）は世界平均（0.98%）を大きく下回る。



2010年7～12月

出典：Microsoft Security Intelligence Report Volume 11

すべての国民が情報通信技術を安全・安心に利用できる環境の実現

世界最先端の「情報セキュリティ先進国」の実現

官民連携・国際連携

サイバー空間上の我が国の安全保障・危機管理の確保

◆ 大規模サイバー攻撃事態への対処

情報通信技術の利活用を促進し我が国の経済成長に寄与

◆ 情報セキュリティ上のリスクの増大等新たな環境変化に対応した情報セキュリティ政策

- 情報セキュリティ基盤の強化
- 国民・利用者保護

日本の情報コミュニティ

内閣総理大臣

官房長官

内閣官房

官房副長官（政務）

官房副長官（事務）

内閣危機管理監

内閣情報官

内閣情報調査室

官房副長官補（3）

安全保障会議

法務省

内閣府

外務省

国交省

経産省

財務省

総務省

防衛省

その他

公安庁

警察庁

海保庁

：情報コミュニティ構成省庁

情報セキュリティ政策の枠組みと推進体制

内閣官房を中心に関係省庁も含め横断的な体制を整備

高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）

本部長　内閣総理大臣
副本部長　内閣特命担当大臣（科学技術政策）
内閣官房長官
総務大臣
経済産業大臣
本部員　本部長及び副本部長以外のすべての国務大臣
民間有識者（10人）

（事務局）
内閣官房IT担当室
室長（官房副長官補（内政））

情報セキュリティ政策会議　（2005年5月30日　IT戦略本部長決定により設置）

議長　内閣官房長官
議長代理　内閣府特命担当大臣（科学技術政策）
構成員　国家公安委員会委員長
総務大臣
経済産業大臣
防衛大臣
民間有識者（６人）

閣僚が参画

- 重要インフラ専門委員会
- 技術戦略専門委員会
- 普及啓発・人材育成専門委員会
- CISO等連絡会議

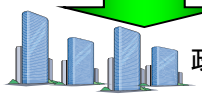
（事務局）
内閣官房情報セキュリティセンター（NISC）
センター長（官房副長官補（安危））
副センター長（内閣審議官）2名
内閣参事官6名
情報セキュリティ補佐官（アドバイザー）3名

協力

協力
4省庁
- 警察庁（サイバー犯罪の取締り）
- 総務省（通信・ネットワーク政策）
- 経済産業省（情報政策）
- 防衛省（国の安全保障）

重要インフラ所管省庁
金融庁（金融機関）
総務省（地方公共団体、情報通信）
厚生労働省（医療、水道）
経済産業省（電力、ガス）
国土交通省（鉄道、航空、物流）
その他の関係省庁　その他
文部科学省（セキュリティ教育）　等

重要インフラ事業者　等



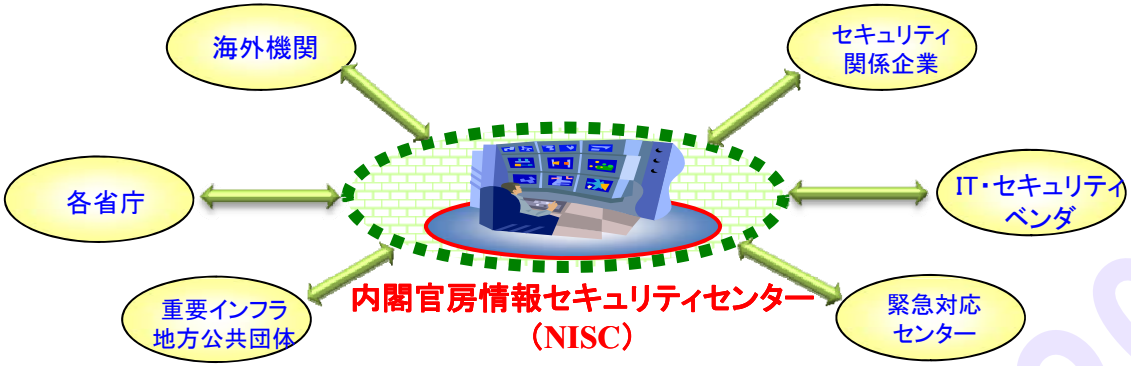
政府機関（各府省庁）

企業

個人

現行の情報セキュリティ政策のフレームワーク

複雑化・高度化する情報セキュリティ対策 ➡ **NISCを中心とした官民連携の取組**



- ◆ NISCを結節点とした官民連携の強化、我が国全体としての対処能力の最大化
- ◆ 統一的・横断的な情報セキュリティ対策の推進による底上げ
- ◆ PDCAサイクルによる持続的改善
- ◆ 国際連携の強化によるイニシアティブの発揮

政府機関・地方公共団体

「政府機関統一基準」等により情報セキュリティを確保

【主な施策】

① サイバー攻撃等への対処

②情報セキュリティ体制の整備
（最高情報セキュリティ責任者（CISO）の設置など）

③政府機関統一基準の策定
（各省庁が守るべき最低限の対策水準を規定）

④政府機関におけるPDCA

⑤政府横断的な情報収集・分析システム（GSOC）の運用

重要インフラ

「重要インフラ行動計画」に基づく官民連携による重要インフラ防護

【主な施策】

① 安全基準等の整備・浸透

② 情報共有体制の強化

③重要インフラ防護対策の向上
（共通脅威分析、演習等）

※重要インフラ（10分野）
- ●情報通信
- ●金融
- ●航空
- ●鉄道
- ●電力
- ●ガス
- ●政府・行政サービス
- ●医療
- ●水道
- ●物流

企業・個人

普及啓発の推進

【主な施策】

①情報セキュリティ普及・啓発プログラムの推進

②「情報セキュリティ月間」の実施

③情報セキュリティガバナンス確立の支援

横断的取組

- ● 情報セキュリティ研究開発戦略の推進
- ● 情報セキュリティ人材育成プログラムの推進
- ● 国際連携・協調の推進
- ● 情報セキュリティ関係の制度整備等

最近の戦略等主要な制定・改正

2010.5.11　「情報セキュリティ基本計画」から「国民を守る情報セキュリティ戦略」に

2011.4.21　「政府機関統一基準」類を「政府機関統一規範」類に

2011.4.21　「政府機関の情報セキュリティ対策のための統一規範」

＊2011.4.21　「政府機関の情報セキュリティ対策における政府機関統一管理基準及び政府機関統一技術基準の策定と運用等に関する指針」

＊2011.4.21　「政府機関の情報セキュリティ対策のための統一管理基準」

＊2011.4.21　「政府機関の情報セキュリティ対策のための統一技術基準」

（＊については、施策の推進等により2012.4.26に一部改正）

2011.7.8　「情報セキュリティ研究開発戦略」の制定

2011.7.8　「情報セキュリティ普及・啓発プログラム」の制定

2011.7.8　「情報セキュリティ人材育成プログラム」の制定

政府機関の情報セキュリティ対策のための統一技術基準の改定について

昨今の政府機関等を対象とした標的型攻撃の顕在化、情報技術や利用環境の変化に対応し、運用の更なる実効性の向上等を図るため、**政府機関統一技術基準を見直し**

○新たな脅威等への対応

標的型攻撃に対する技術的な対策の明確化、災害時の継続的な運用

＊標的型攻撃対策に関する項を設け、侵入及び感染拡大防止に関する遵守事項を追加

＊パスワードを設定する時は、必要なセキュリティ上の強度を持つような機能の設定等の規定を追記

＊可用性を担保するため、通信回線装置の設定情報のバックアップ等に関する規定を追記

○情報技術・利用環境の変化への対応

IPv6技術の導入対策、区域における対策の明確化

＊準拠製品の選択、ﾌｨﾙﾀﾘﾝｸﾞ機能の適切な設定等、IPv6技術の導入に伴う対策を追加

＊情報を取り扱う区域にクラス区分を設け、クラスに応じた対策の実施に関する規定を追加

○基準運用の実効性の向上

リスク分析の実効性を確保

＊従来の「基本遵守事項」（必須）と「強化遵守事項」（必要に応じて実施）の枠組みを廃止し、すべての遵守事項について、各府省庁における確実なリスク分析の実施

「国民を守る情報セキュリティ戦略」の概要（平成22年5月11日情報セキュリティ政策会議決定）

現状の課題

大規模なサイバー攻撃事案等の脅威の増大

✓重要インフラ等、国民生活に直結するサービスの情報通信技術への依存による脅威の増大
✓国境を越えたサイバー攻撃が現実化（米韓大規模サイバー攻撃（2009年7月））
✓ガンブラーウイルス等、年々新たなウイルスが出現。攻撃手法も高度化・多様化

社会経済活動の情報通信技術への依存度の増大

✓情報家電、電子タグなどあらゆる機器がネットワークに接続
✓ 約8割の国民が情報セキュリティに不安感

急速な技術革新の進展

✓ クラウド・コンピューティング技術、IPv6への移行
✓ 暗号の危殆化につながるコンピュータの能力向上

グローバル化の進展

✓ 国境を越えた瞬時の情報流通
✓ 各国の個人情報保護・情報セキュリティ制度の調和

- *重要インフラ等の国民生活に直結するサービスの情報通信技術への依存の高まりにより、脅威（ITリスク）は着実に増大*
- *情報セキュリティ上の攻撃手法が多様化・高度化・複雑化しており、従来の取り組みでは対応が困難*
- *各国でも戦略的な取り組み（＊）を実施*

（＊）米国
・サイバースペース政策レビュー（60日レビュー）
・「サイバーセキュリティ調整官」を設置し、国家的取組みを強化
・「2010 Cybersecurity Enhancement Act 」（2010年2月）

課題に対応する新戦略の必要性

「国民を守る情報セキュリティ戦略」

国民を守る情報セキュリティ戦略（2010～2013）

第2次基本計画（2009～2011）

（＊）第2次情報セキュリティ基本計画を包含し、今後4年間の重点的な取組み

基本的な考え方（取組みの重点化）

① サイバー攻撃の発生を念頭に置いた政策強化・対処体制整備
② 新たな環境変化に対応した政策の確立
③ 受動的な対策から能動的な対策へ

➢ ITリスクを克服し、安全・安心な国民生活を実現
➢サイバー空間の安全保障・危機管理政策の強化と情報通信技術政策の連携
➢安全保障・危機管理及び経済の観点に国民・利用者保護の観点を加えた3軸構造の総合的な政策（特に、国民・利用者の視点を重視した政策の推進）
➢ 国際連携の強化

安全・安心な国民生活を実現

サイバー空間上の我が国の安全保障・危機管理の確保

情報通信技術の利活用を促進し、我が国の経済成長に寄与

実現すべき成果目標

2020年までに、インターネットや情報システム等の情報通信技術を利用者が活用するにあたっての脆弱性を克服し、全ての国民が情報通信技術を安心して利用できる環境 （高品質、高信頼性、安全・安心を兼ね備えた環境）を整備し、世界最先端の「情報セキュリティ先進国」を実現

内閣官房副長官補（安全保障・危機管理担当）の体制

内閣官房副長官補（安全保障・危機管理担当）

内閣審議官×４

情報セキュリティセンター

〇情報セキュリティ基本戦略立案
〇政府機関総合対策促進
〇情報セキュリティ事案対処支援
〇重要インフラ対策
〇情報セキュリティ国際戦略の立案
等

〇安全保障基本政策
〇事態対処専門委員会の運営
〇緊急時連絡・初動体制
〇大規模自然災害
〇危機管理センター運用
〇NBCテロ対策
〇テロ・ゲリラ等陸上事案への対処
〇ハイジャック対処
〇不審船等海上事案への対処
〇航空・鉄道・海上事故対処
〇在外邦人保護
〇日米・国際協力
〇大量避難民対策
〇事態対処法制の企画・総括
〇国民保護法の運用
〇指定公共機関に関する事項
〇特定公共施設利用法の運用
〇米軍行動関連措置法の運用
〇緊急事態基本法制の検討
等

副長官補　×　１
内閣審議官×　４
内閣参事官・内閣事務官

（平成24年1月現在）

計　約100名

出向元：内閣府、警察庁、防衛庁、総務省、消防庁、法務省、公安調査庁、外務省、財務省、厚生労働省、農林水産省、経済産業省、国土交通省、気象庁、海上保安庁　等

政府横断的な情報収集・分析システム（GSOC）

（注）Government Security Operation Coordination team

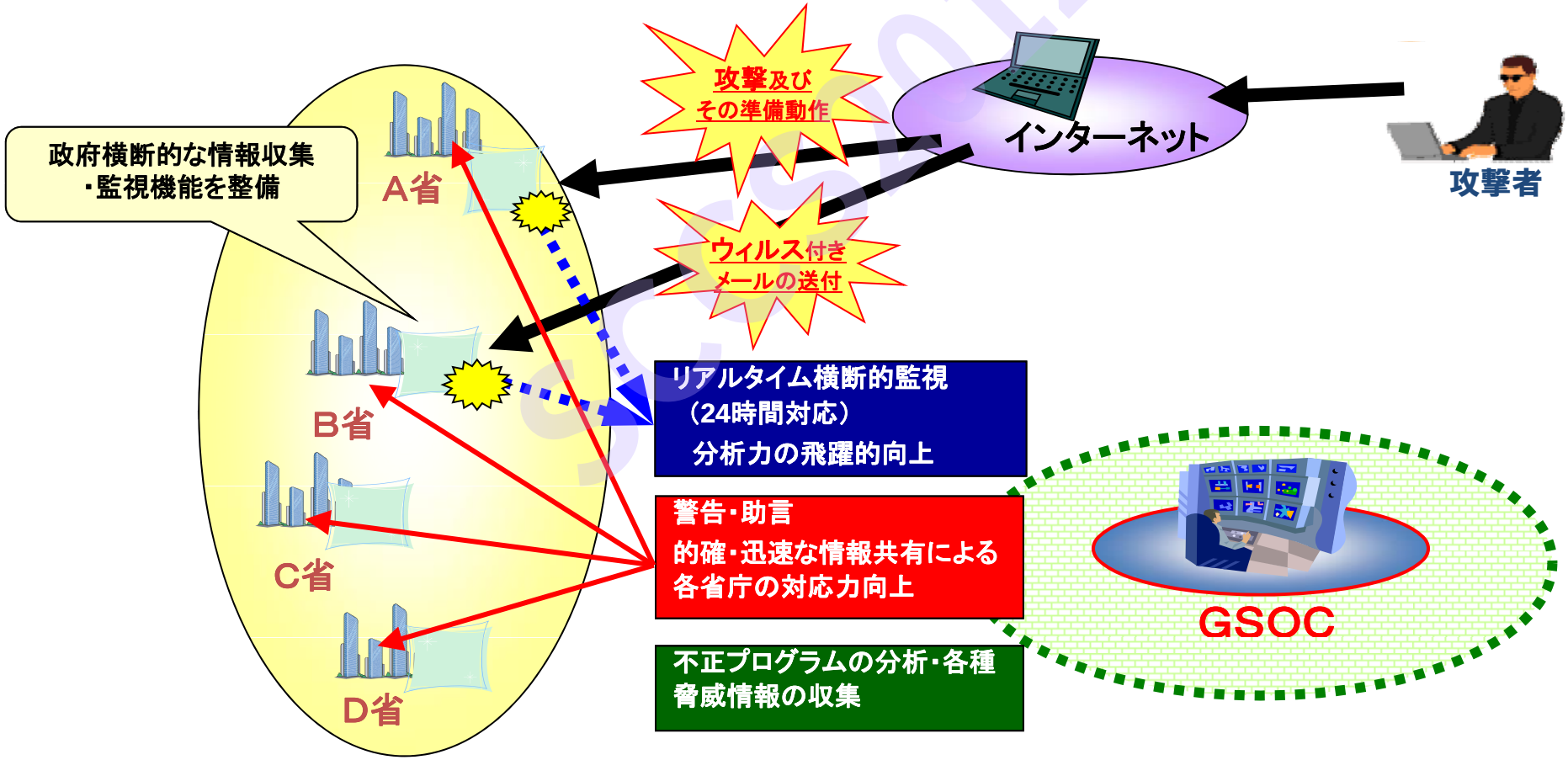
目　的

■ 情報セキュリティ問題（外部からのサイバー攻撃など）に対して、政府機関の緊急対応能力強化を図るために整備・運用

（経緯）

2008年4月～　運用開始

2009年1月～　24時間運用開始　　（注）なお、現時点では、本府省省庁のシステムのみを監視対象としている



大規模サイバー攻撃事態等への対処について

現状認識

【官房長官指示 （情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議（H22.12.27））】

○現代社会は、サイバー攻撃の脅威にさらされており、政府として対処態勢を強化していくことが必要。

○各省庁は、大規模なサイバー攻撃が、我が国の安全保障・危機管理に影響を及ぼしうる重大な脅威であることを十分認識し、これに適切に対処するための取組を強化する必要がある。

過去の事例

○米国・韓国における大規模サイバー攻撃事案（H21.7）　○我が国政府機関HPに対するサイバー攻撃事案（H22.9）

政府におけるサイバー攻撃等への対処態勢の強化について

（H22.12.27 情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議申し合わせ）

対策

事案発生時の対処態勢の構築

○　政府一体となった対処態勢の構築

・「大規模サイバー攻撃事態等への初動対処について（H22.3.19内閣危機管理監決裁）」に基づく具体的な対処体制の構築

○訓練の実施等

・　H23.3、各省庁が連携した訓練を実施。今後も継続して実施予定。

・当該訓練の結果を踏まえ、別途、対処要領等の作成を検討。

情報収集・集約体制の強化

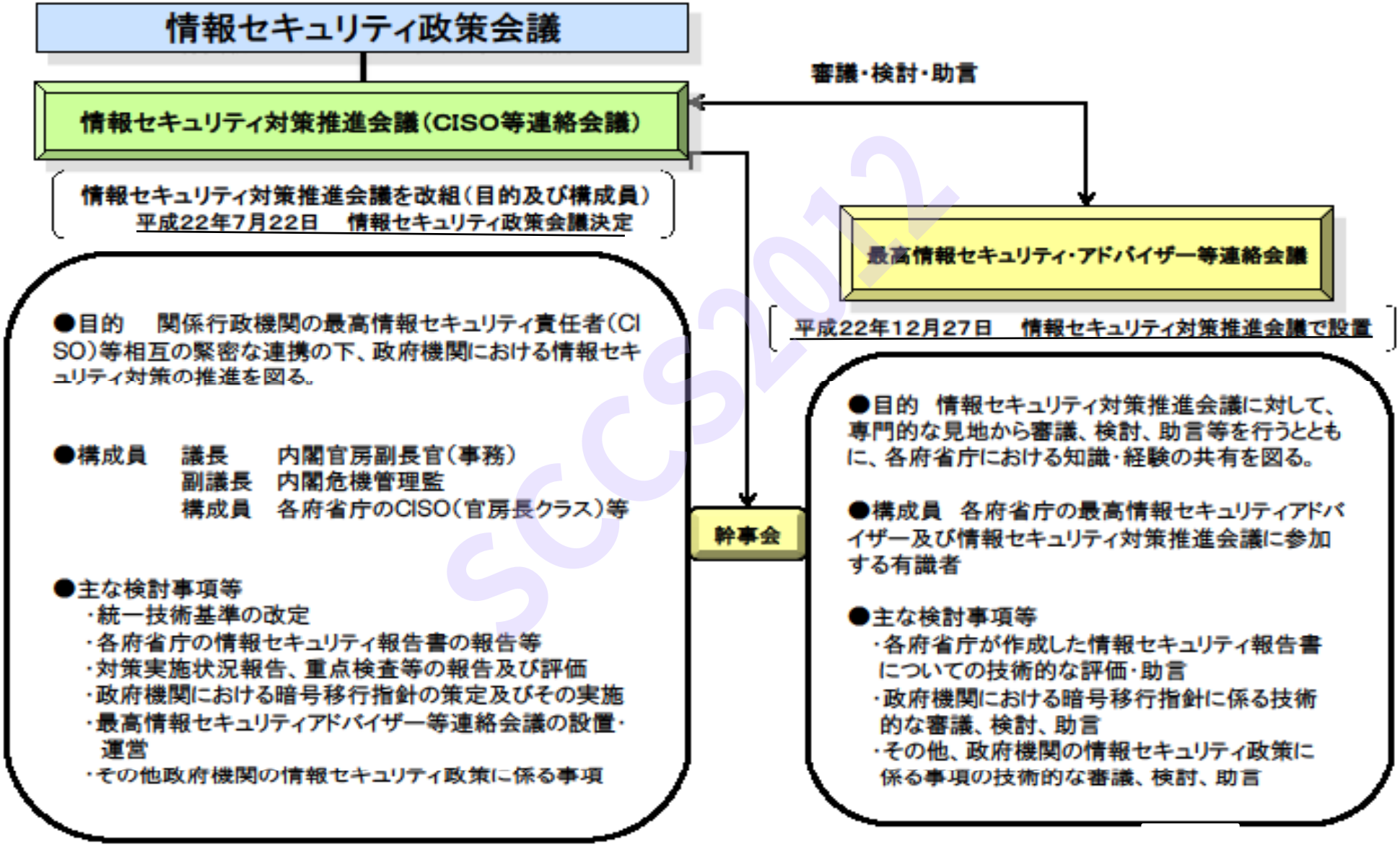
○平素からの情報収集・集約体制

・「我が国におけるサイバー攻撃に係る情報収集・集約体制等の整備について（H22.12.27情報セキュリティ対策推進会議申し合わせ）」に基づき、各省庁から提供される情報を収集・集約・共有

○事案発生時の情報収集・集約体制

・「緊急事態に対する政府の初動対処体制について（H15.11.21閣議決定）」、「大規模サイバー攻撃事態等への初動対処について」等に基づき、各省庁から提供される情報を収集・集約・共有

情報セキュリティ対策推進会議について



政府におけるサイバー攻撃等への対処態勢の強化について

平成22年12月27日
情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議
申合せ

情報通信技術の発達した現代社会は、いわゆるサイバー攻撃の脅威にさらされており、我が国においても大規模なサイバー攻撃事態が発生する可能性がある。このため、以下の施策を講じることにより、政府におけるサイバー攻撃等への対処の取組をさらに強化していく必要がある。

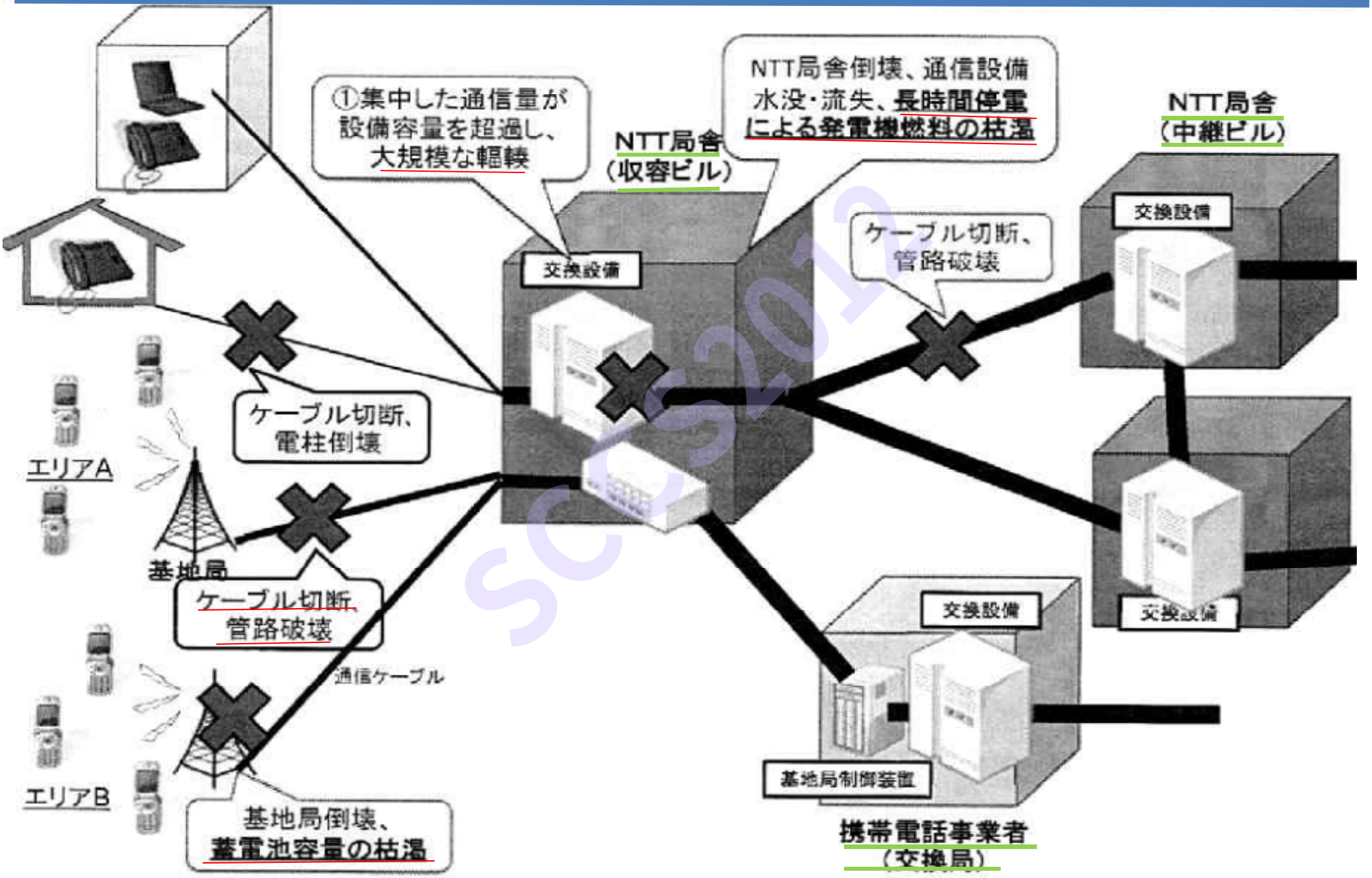
1. 大規模サイバー攻撃事態等における政府の初動対処態勢の整備

○ 内閣官房及び各府省庁は、相互に連携し、初動対処訓練を実施するとともに、 ～（中略）～ 迅速かつ適切な初動対処をとるための態勢を整備する。

2. 平素からの情報収集の強化と情報共有の徹底

○ サイバー攻撃事態に対し、政府として迅速かつ的確に対処するためには、平素から、各府省庁が収集したサイバー攻撃に係る情報が速やかに内閣官房に集約 ～（中略）～ 被害の拡大防止及び再発防止に活用するため、情報連絡を行った府省庁の同意を得た上で、各府省庁に対して積極的な情報提供を行う。

東日本大震災により通信に被害が生じた主な原因



災害に強い通信インフラ

- 発災48時間内の避難所における通信環境の確保(計画と訓練)
- 自衛隊、警察等と連携しての通信施設の応急復旧
- 被災地や支援者からの相談窓口の早期立ち上げ
- 安全確認・避難情報の収集伝達手段の確立
- ICTスキルを持つサポーターの育成と支援確保

インターネットのガバナンス

・ インターネットはもともと核戦争で重要拠点が破壊されても、生き残った拠点間の通信だけは確保できないか、という視点から生まれたもの。
・ その後、大学間での高速コンピュータの共同利用システムに変身し、ヒッピー文化とともに発展(軍用の筈が反戦)
・ 更に、1990年代半ばに、商用に再転換。しかし、中央制御に対する反感は維持。インターネット独立宣言やインターネット自由貿易圏の考え方が根強い。
・ したがって、当初からベスト・エフォートで、セキュリティへの配慮は薄い。①相手の確認もしない。②到達確認もしない。③暗号化しない。④全体の管理者は置かない。⑤自己責任に重きを置いた、分散システムである。

三菱重工業等に対するサイバー攻撃事案について

三菱重工業等に対する攻撃（標的型攻撃によるウィルス感染）

○　防衛装備品や原子力プラントを製造している三菱重工業のコンピュータがウィルスに感染し、情報が抜き取られた痕跡ありと報道（9/19読売新聞）。同社によると、本社、研究所等の約80台のサーバやパソコンが実際に感染し、一部のコンピュータのシステム情報が流出した可能性があるものの、製品や技術に関する情報の流出は確認されていない。

○　IHI、川崎重工業、三菱電機に対しても同様の攻撃があったと報道（9/21新聞各紙）。関係省庁からのヒアリング調査に対し各社は、現時点で重要な情報の漏えいは確認されていない旨回答。

○　政府においては、内閣官房において全府省庁の担当課長等を集め、「政府内の迅速な情報共有」の徹底を指示(9/20)

○　経済産業省及び防衛省において、引き続き情報収集を実施中。また、警察は三菱重工業からの被害届(9/30)を受理し、目下捜査中。

情報セキュリティ政策会議を開催（2011．10．7）

情報セキュリティ政策会議議長（官房長官）からのメッセージ

国の重要な情報を扱い
国の安全に深くかかわる企業

○ 企業の情報セキュリティの一層の強化
○ 政府・民間双方向の情報共有等の官民連携への協力

一般企業等

○ 職員の情報セキュリティ意識の向上
○ 感染時に被害を最小限にとどめる対策の実施

国民全般

○ パソコンやスマートフォン等のセキュリティ関連ソフトウエアを常に最新の状態に

情報セキュリティ対策の強化について

平成２３年１０月７日
情報セキュリティ政策会議議長
内閣官房長官　藤村　修

情報通信技術の発展により、私たちは多大な経済的利益や生活の利便性を享受していますが、その一方で、情報セキュリティ上の脅威も日常のものとなっています。こうした中、国の重要な情報を扱う企業がサイバー攻撃の対象となり、不正なプログラムに感染するという事態が発生しました。

サイバー攻撃は、被害によっては国の安全や国民生活に深刻な事態をもたらす可能性があります。政府及び重要インフラ関連組織においては、これまで進めてきた情報セキュリティ対策を更に高めてまいります。国の重要な情報を扱い国の安全に深く係わる企業の皆様におかれても、今回の事態を契機に、企業の情報セキュリティの一層の強化に努めてください。

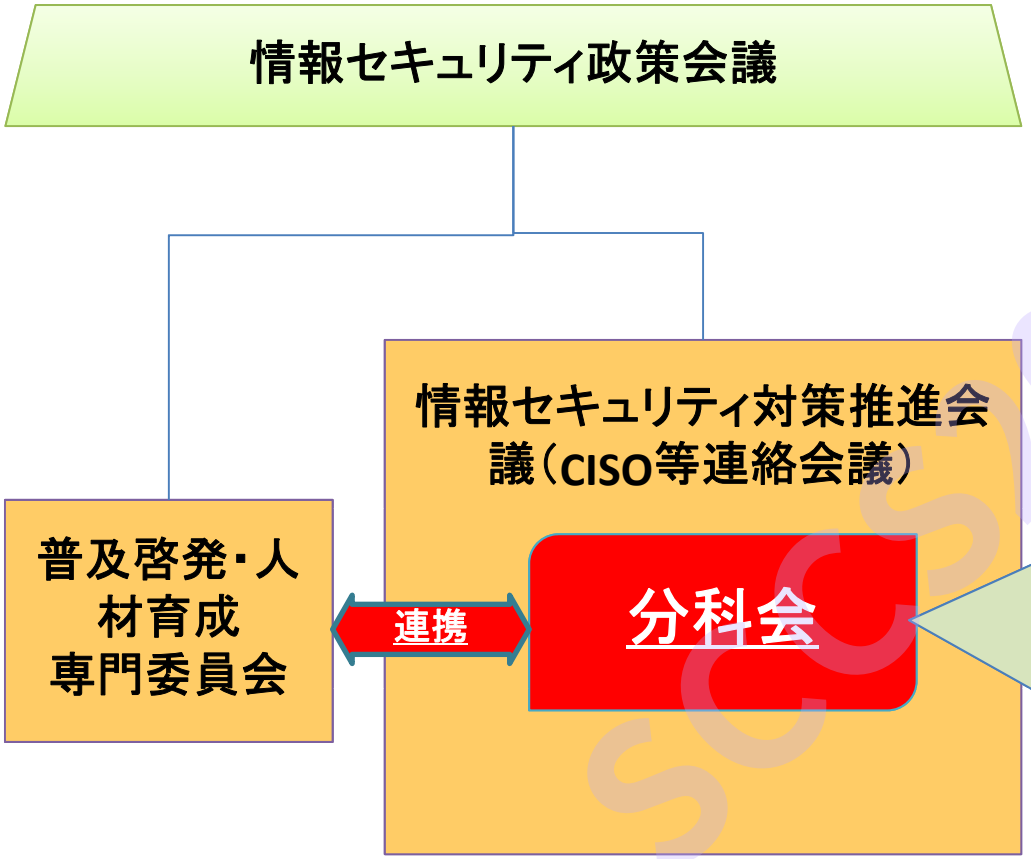
情報セキュリティの確保においては、とりわけ早期の情報共有が重要です。その観点に立ち、政府は今後、政府・民間双方向の情報共有等を通じた官民連携の強化を進めてまいりますので、関係する皆様のご理解とご協力をお願いいたします。

情報セキュリティ上のリスクは、被害者となる恐れがあることはもちろんのこと、不正なプログラムに感染することで意図せずに加害者になってしまうこともあります。情報セキュリティ対策を講じることは、今や社会的な責務ともいえるものになっています。

企業等におかれては、攻撃に強いシステムの導入と、職場一人一人の情報セキュリティ意識の向上等に努めるとともに、感染してしまった場合であっても、被害を最小限にとどめる対策の実施が必要です。国民の皆様におかれては、自分のパソコンやスマートフォン等について、そのセキュリティ関連ソフトウェアを常に最新の状態に維持するなどの対策に努めてください。

情報セキュリティの確保は、安全で安心な国民生活の実現と国際競争の中での継続的な発展に不可欠なものとなっています。官民の連携により世界最先端の情報セキュリティの実現に努めてまいります。

官民連携の強化のための分科会の設置



2011年

10月　7日　情報セキュリティ政策会議において設置方針の決定

10月14日　CISO等連絡会議において分科会を設置

官民連携等を通じて企業等の情報セキュリティ対策を強化するため、以下検討を行う。

(i)　政府としてとるべき方策、特に政府調達等に際して調達先企業に求める情報セキュリティ要件

(ii)　政府と企業等との連絡・連携のあり方

(iii)　産業界の取り組みに対する政府の協力、情報提供のあり方

(iv)　企業等におけるセキュリティ文化の啓発、セキュリティ企業体質の涵養等

○　CISO等連絡会議幹事会構成員等からなる分科会を設置

* CISO: Chief Information Security Officer（最高情報セキュリティ責任者）

官民連携の強化のための分科会における検討結果の概要

2012年1月19日　CISO等連絡会議に報告
1月24日　情報セキュリティ政策会議に報告・公表

経　緯

昨年10月14日以降、3回分科会を開催し、情報セキュリティ対策における官民連携の強化策について検討。この間、企業等におけるセキュリティ対策、セキュリティオペレーション事業者等との意見交換を実施。

報告事項

○国の安全に関する重要な情報を扱う**契約に情報セキュリティ条項**を定める。

○各府省庁がCSIRT(*)の機能を保有するよう求め、**政府CISO (**)を設置**する。

○**企業等においてもCSIRTの機能**を保有する取組を促進する。

○官民のネットワーク関係者間の**情報共有をNISCにおいて実施**する。

○情報セキュリティ人材を育成していく機運を醸成するため、**啓発活動を実施**する。

＊　CSIRT: Computer Security Incident Response Team ：
情報セキュリティインシデントに対処するための組織の総称

＊＊　CISO: Chief Information Security Officer

標的型不審メール攻撃訓練及び公開ウェブサーバ脆弱性検査の結果

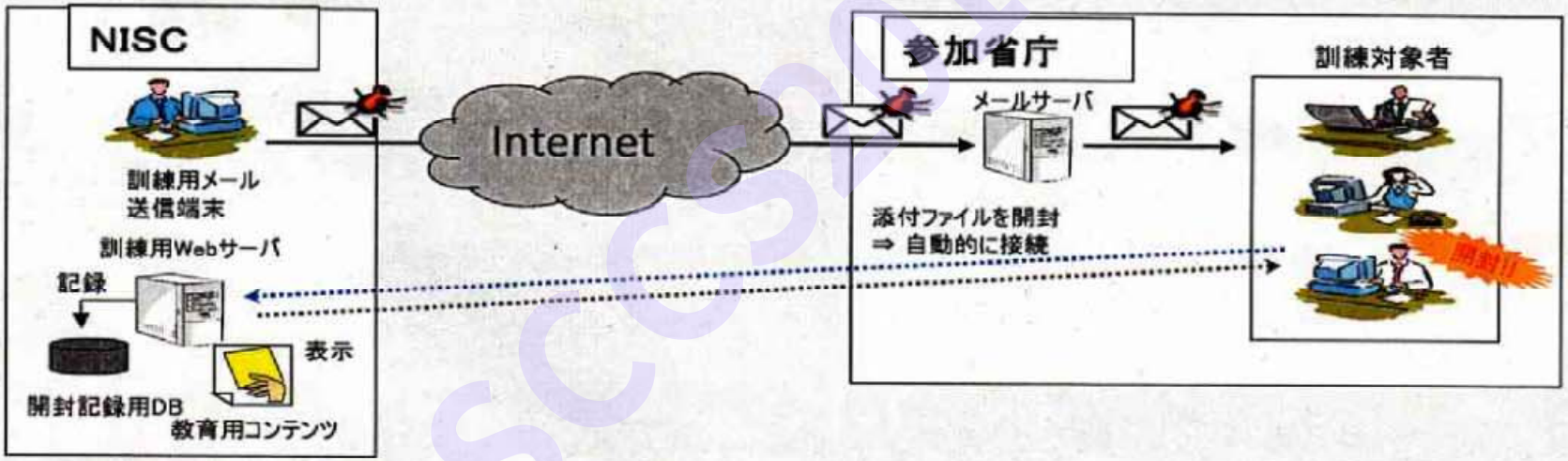
標的型不審メール攻撃訓練結果

訓練・検査期間：平成２３年９月～１２月

訓練対象：内閣官房等１２の政府機関約６万名

訓練結果：今回の訓練における不審メールの開封率は以下のとおり。

- ◆１回目（添付メール）　１０．１%（１．１%～２３．８%）
- ◆２回目（リンクメール）　３．１%（０．４%～　６．１%）



公開ウェブサーバ脆弱性検査結果

検査対象：政府機関のウェブページ（11省庁、約330画面）

検査方法：NISCの委託業者による模擬的な攻撃を実施

検査結果：情報流出につながる弱点が14か所（8省庁）検出され、対処

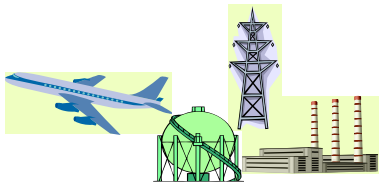
重要インフラの情報セキュリティ対策

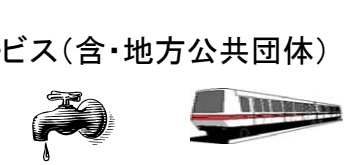
官民連携による重要インフラ防護の推進

重要インフラにおけるIT障害が国民生活、社会活動に重大な影響を及ぼさないことを目指す
①予防的な対策と再発防止対策の両側から対処（具体的には、安全基準の整備、情報共有体制の強化など。）
②重要インフラ事業者等における情報セキュリティ対策の浸透状況や急速な技術進展等を踏まえたPDCAの促進

重要インフラ（10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



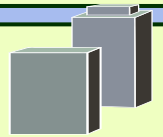


NISCによる
調整・連携

重要インフラ所管省庁（5省庁）

- 金融庁 [金融分野]
- 総務省 [情報通信分野、行政分野]
- 厚生労働省 [医療分野、水道分野]
- 国土交通省 [航空分野、鉄道分野、物流分野]
- 経済産業省 [電力分野、ガス分野]

関係機関等



- 情報セキュリティ関係省庁
- 事案対処省庁
- その他関係機関

国民を守る情報セキュリティ戦略（第2次行動計画）

（1）安全基準等の整備・浸透

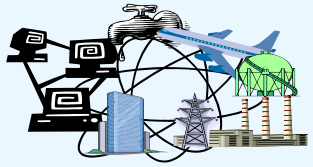
重要インフラ各分野に横断的な「指針」に基づいて、「安全基準」等の浸透を図る

（2）情報共有体制の強化

情報の共有により、個々の主体による孤立した対応から、社会全体としての対応を促進

（3）重要インフラ防護対策の向上

①共通脅威分析

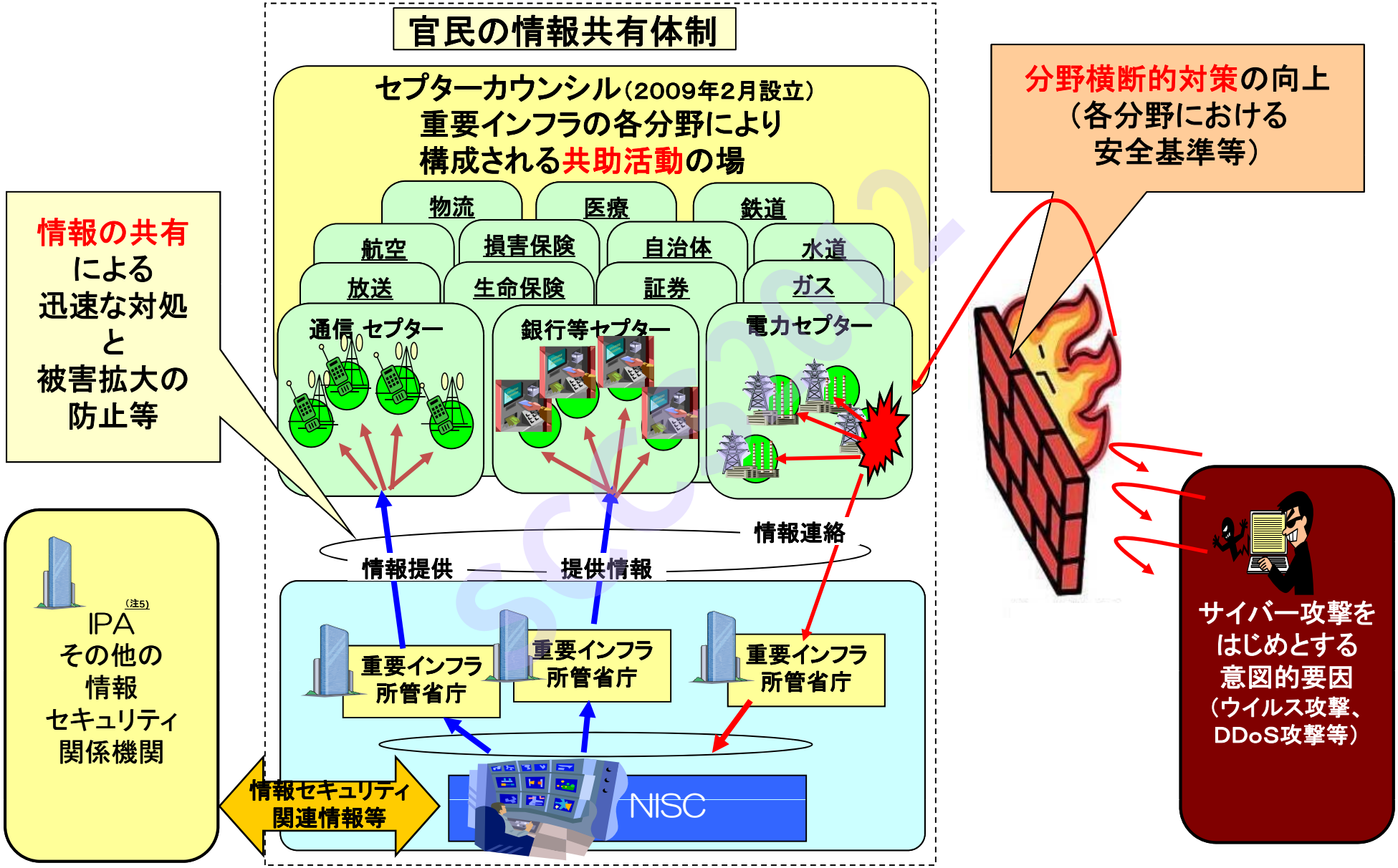


複数分野に共通する潜在的な脅威の分析

②分野横断的演習

防護対策向上のための課題抽出

分野横断的対策（安全基準等）と官民における情報共有の推進



（注5）独立行政法人　情報処理推進機構　(Information-technology Promotion Agency)

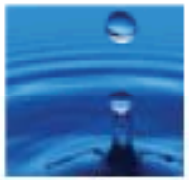
＜参考＞米国における重要インフラ

重要インフラの定義

物理的か仮想上かに関わらず、米国にとって重要なシステム及び資産であり、そのようなシステム及び資産の無力化又は破壊により、国家の安全、経済安全、公衆衛生、安心、又はそれらの組み合わせを低下させる影響を有するもの


農業・食糧


健康・公衆衛生


水


エネルギー


銀行・金融


国定記念物・建築物


救急サービス


政府施設


重要製造業


情報技術


通信


ダム


原子力


商業施設


郵便・物流


交通システム


化学


防衛産業基盤

国家インフラ保護計画（National Infrastructure Protection Plan）を策定し、重要インフラの定義にしたがい、それぞれのセクターに分けて、セクター毎の対応計画を策定

（参考）重要インフラの情報セキュリティ政策に関する日米比較

日本（NISC）	米国（DHS）
■「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」（2009年2月　情報セキュリティ政策会議決定）に基づき対処	■NIPP*（国家重要インフラ防護計画）（2009年2月国土安全保障省改訂（2006年6月策定））に基づき対処（情報セキュリティは重要インフラ防護の一側面） *National Infrastructure Protection Plan
■重要インフラの対象分野（情報セキュリティ） 情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流の10分野	■重要インフラの対象分野（防護全般） 農業・食糧、防衛産業基盤、エネルギー、健康・公衆衛生、国定記念物・建築物、銀行・金融、水、化学、商業施設、重要製造産業、ダム、救急サービス、原子力、情報技術（IT）、通信、郵便・物流、交通システム、政府施設の18分野
■NISCが中心となって重要インフラ所管省庁と情報共有を推進するとともに、重要インフラ分野ごとのセプター（情報共有・分析機能）やセプターの集まりであるセプターカウンシルを構成し、官民の情報共有体制を構築	■GCC（Government Coordinating Council）やSCC（Sector Coordinating Council）といった政府関係者、重要インフラ事業者の集まりを整備し、官民の情報共有体制を構築
■分野毎の安全基準等の継続的な改善を促進することにより、情報セキュリティ対策等の向上を図る	■分野毎に安全対策に関する評価・見直しを行う枠組を構築し、情報セキュリティ対策等を含め継続的な向上を図る
■IT障害上の脅威を原因事象とした分野横断的演習を実施（毎年開催）	■大規模サイバー演習（サイバーストーム）を実施（2年に1回開催）

重要インフラ防護の為の
情報セキュリティの取り組み強化ついて

重要インフラ専門委員会において、「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」を点検し、早急に必要な見直しに着手、年度内を目途にとりまとめ。

重要インフラ防護のための情報セキュリティ対策について、早急に取組を強化・補強すべき点を洗い出し、行動計画に反映する。

（強化・補強すべき点（例））

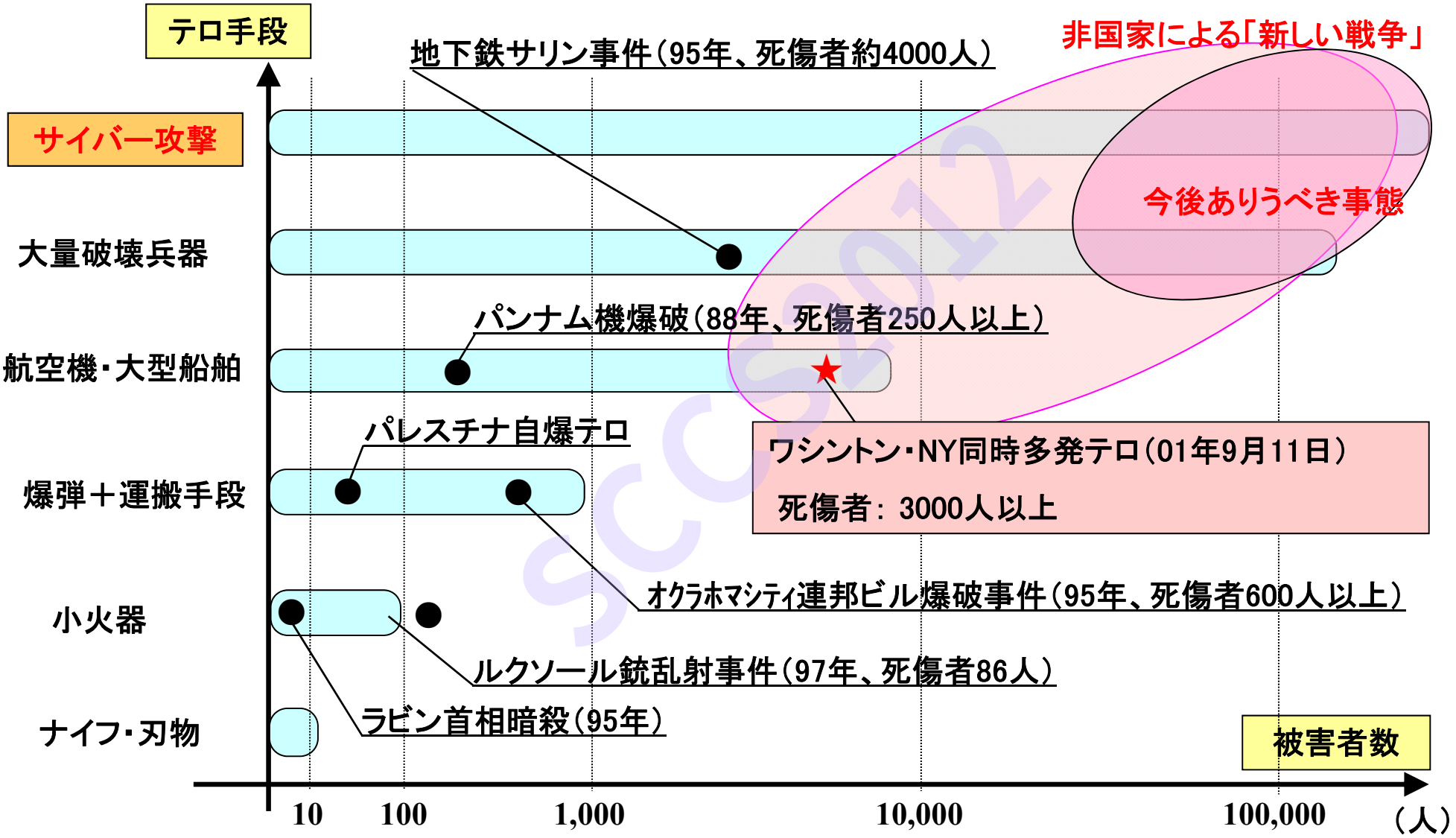
（1） 事業継続計画（BCP：Business Continuation Plan）等の充実
東日本大震災における教訓を踏まえた、安全基準等の策定に当たっての指針（特にBCP）の一層の充実

（2） 環境変化を踏まえた安全基準の改善
標的型攻撃など最近の環境変化を踏まえて、制御システム等についての安全基準の検証を行い、必要に応じて改定

（3） 情報共有体制の強化
平素からの情報収集・情報共有体制の充実

サイバーテロの位置付けと被害の事例

やや特異な位置付け



「情報セキュリティ研究開発戦略」の概要（平成23年7月）

（参考1）

背景

情報通信技術の変革
・クラウド　・ユビキタス化等

新たな脅威の増大

東日本大震災の発生

情報セキュリティ研究開発予算

	2007年	2010年	増減
日本	77.1億円	48.6億円	▲37%
米国	192億円	366億円	＋91%

（日米では、3年間でGDP比で3倍の格差）

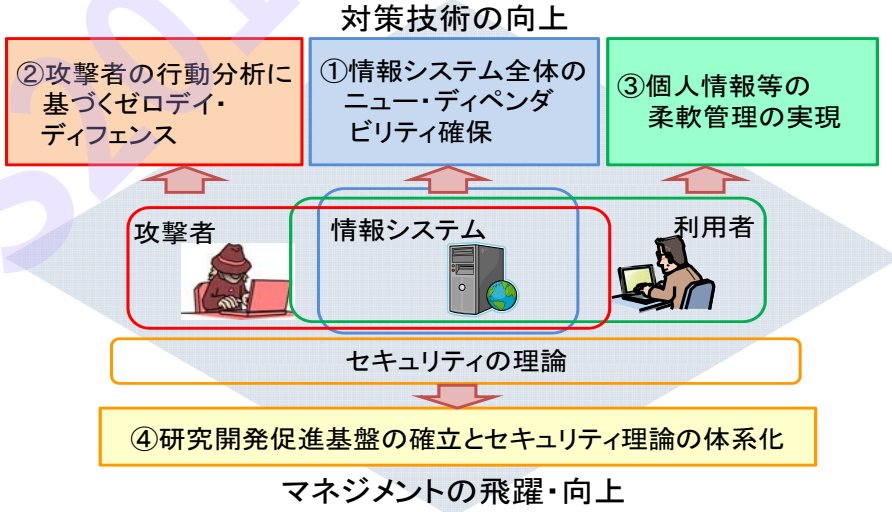
研究開発戦略のコンセプト

（2011年度～2015年度の5か年計画）

攻撃側優位を転換し、防御側優位を目指す「攻めの情報セキュリティ」の実現のための研究開発の促進を図る。
－能動的で信頼性の高い情報セキュリティ（「ニュー・ディペンダビリティ」※）－

（参考）『科学技術に関する基本政策について』に対する答申」（平成22年12月総合科学技術会議決定）

- 4つのコンセプトに基づく、12の重点分野を選定



※　従来の「ディペンダブル」の概念を拡張するとともに、サイバー攻撃を無効化するなど「能動的」な情報セキュリティの要素を追加したものを「ニュー・ディペンダビリティ」という。

- 短期、中長期の投資タイプを設定し、ロードマップを作成。今後5年で特に必要な研究開発分野を明確化
- 震災の発生を受け、耐災害性の高い情報通信システムの構築技術、リスク・マネジメント等を重点化分野に選定

基本的な考え方

- サイバー攻撃を無効化する能動的研究等の革新的取組の推進
- 耐災害性に強い情報通信システムの構築やリスク・マネジメント等の研究の推進
- 社会的イノベーションを支える研究開発との連携強化
- 情報セキュリティ産業のグローバル展開への貢献
- 官民連携・国際連携の推進　等

「情報セキュリティ普及・啓発プログラム」概要（平成23年7月）

（参考2）

（2011年度～2013年度の3か年計画）

背景・課題

●情報セキュリティの確保に関して、約8割の国民や企業が不安
●自ら対策を講じていても、日本人は情報セキュリティに対して漠然とした不安を抱えている（国際比較）

利用環境の変化

・スマートフォン等モバイル環境の高度化
・*SNS等新たなメディアの台頭*
・クラウドコンピューティングの利用拡大

利用者層の変化

・*高齢者層のインターネット利用の増加*
・*SNS等新たなサービスを利活用する若年層の増加*

情報セキュリティ脅威の高度化・多様化

・*悪質なウイルスやボットの多目的化*
・*従来では考えられなかった攻撃の出現*

基本的な考え方

情報セキュリティ文化の定着

情報セキュリティに係る取組を、特殊なものとしてではなく、一般常識、マナー、あるいは社会的習慣として広く国民全体に定着させる。

※）「情報セキュリティ文化」6原則：「認識」、「責任」、「対応」、「協調」、「倫理」、「再評価」をいう。

●恒常的な取組の定着化
- 「情報セキュリティ月間」期間中のみならず、年間を通じた継続的な取組の定着化を図る

●利用実態を踏まえた対策の推進
- 高齢者や若年層等、利用主体の属性に着目したきめ細やかな対策の推進

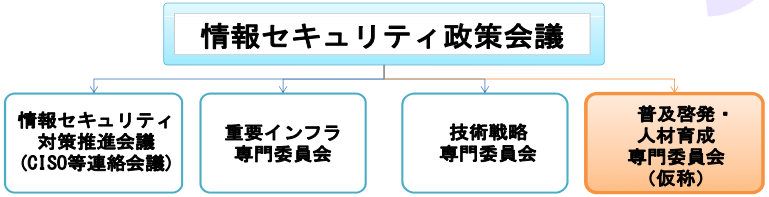
●無関心層への対策の推進
- 一部の利用者が情報セキュリティ対策を講じていなければ、結果的にセキュリティの向上につながらないということを認識する

●官民連携・国際連携の強化

具体的な取組

「普及啓発・人材育成専門委員会」の新設

情報セキュリティの普及啓発及び人材育成を専任とする司令塔機能を明確化するため、「情報セキュリティ政策会議」の下に「普及啓発・人材育成専門委員会」を新たに設置する。



普及啓発コンテンツの充実

- 「国民を守る情報セキュリティサイト」の充実
- 自己診断チェックリストの作成
- 高齢者向け資料の作成

「情報セキュリティ月間」の充実

- 「情報セキュリティ月間」の更なる周知
- 「情報セキュリティ月間」10月開催の検討

各種取組の推進

- 企業に対する普及・啓発の推進（企業のトップの意識改革、中小企業に対する対策）
- 普及・啓発を促進するためのインセンティブ措置の検討
- 情報セキュリティに関する教育及び学習機会の提供（教育機関）
- サイバー犯罪抑止のための広報啓発の推進

国際連携の強化

- 「国民を守る情報セキュリティサイト」（英語版）の充実
- 日・ASEAN関係の強化
- 欧米諸国やAPECとの連携強化

「情報セキュリティ人材育成プログラム」の概要（平成23年7月）

（参考3）

（2011年度～2013年度の3か年計画）

背景

「人材育成・資格制度体系化専門委員会報告書」（2007年）

我が国の情報セキュリティ対策レベルの向上を図るため、
当面、早期に着手・実行すべき課題を集中的な検討を実施、提言。
また、情報セキュリティ関係の資格の整理を実施。

⇒

「情報セキュリティ人材育成プログラム」（2011年）

情報セキュリティ人材の今後の方向性について検討し、
未だ不十分な領域について重点化を図る。

基本的な考え方

1. 「ハイブリッド型人材」、「問題発見・解決型人材」の育成・確保
2. 情報セキュリティ人材育成環境の整備
   - 企業のトップの意識改革：「係長セキュリティ」から「社長セキュリティ」へ
   - 情報セキュリティ人材の価値や効果の可視化
3. 産学連携の強化
   教育機関及び産業界がそれぞれ求める人材像のギャップの解消
4. 先導的研究開発、情報セキュリティ産業の活性化を通じた人材の育成
5. グローバル化に対応できる人材の育成

具体的な取組

政府機関における人材育成

- 「政府機関の情報セキュリティ対策のための統一規範」等に基づく取組（政府職員への情報セキュリティ研修　等）

教育機関における人材育成

- 産学連携や大学間連携等を通じた大学院教育の充実
- 大学教育における情報セキュリティ教育の奨励
- 実務経験学習等実践的な教育の充実（企業人講師の活用　等）
- 発達段階に応じた情報セキュリティに関する教育の充実（初等中等教育）
- 教員への情報セキュリティ研修の充実

企業における人材育成

- 企業経営者の意識改革
- 人材育成環境の整備（求められる人材像の明確化、資格制度・教育プログラム、キャリアパス、処遇や評価体系　等）
- CIO、CISOの任命や情報セキュリティ保険の活用
- セミナー等を通じた重要インフラ事業者、中小企業者向けの人材育成

産学連携・国際連携を通じた人材育成

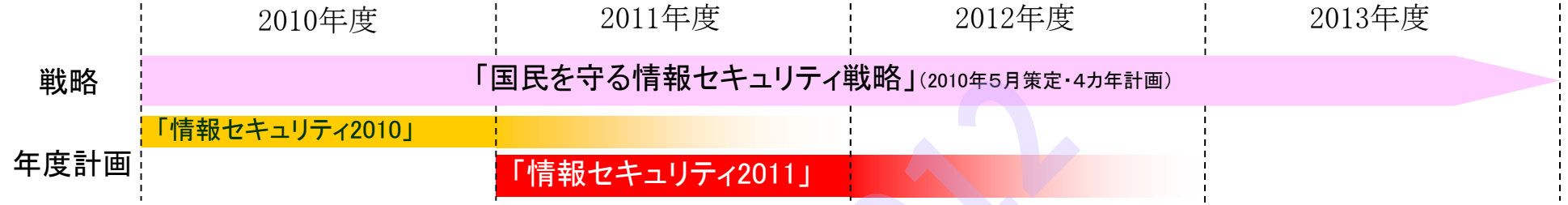
- 産学連携のマッチングの促進（ミスマッチの解消）
- 実践的な教育体制の確立への協力促進
- 情報セキュリティ・コンテスト等の活用
- 政府機関における就業経験機会の推進
- ASEAN諸国等との国際連携の強化

「情報セキュリティ2011」の概要（平成23年7月8日情報セキュリティ政策会議決定）

（参考4）

「情報セキュリティ2011」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への対応

大規模なサイバー攻撃等の脅威の高度化・多様化

- 我が国政府機関へのサイバー攻撃
- 標的型メール攻撃の巧妙化、新たな脅威の出現
- 大規模な個人情報漏えい
- IPv6、クラウド等に関する情報セキュリティ上の課題

新たな技術革新への対応

- ユビキタス化、実空間とサイバー空間の融合化　等

社会経済活動の情報通信技術への依存度の増大

- SNS、スマートフォンの急速な普及　　等

東日本大震災の発生

グローバル化

情報セキュリティの脅威の高度化・多様化に対応した能動的な対応

- 攻撃側と防御側の非対称性を解消する「ゲーム・チェンジ」のための取組の強化
- 能動的で信頼性の高い（ディペンダブルな）情報セキュリティ（「ニュー・ディペンダビリティ」）の確保
- 官民連携、国際連携の推進
- 大規模サイバー攻撃に対応するため、政府横断的な情報収集・分析システム（GSOC）の充実・強化
- スマートフォン、制御システム、IPv6、クラウドコンピューティング、SNS等の情報セキュリティ上の課題への対応

東日本大震災を踏まえた情報セキュリティ分野における対応

- 耐災害性の高い情報システムの検討、再構築
- 情報のバックアップや分散化等に対応した事業継続計画（BCP）の見直し
- 「リスク・マネジメント」「リスク・コミュニケーション」の確立

「オープンで相互運用可能で、セキュアで、信頼性の高いサイバー空間」の構築（G8ドービル・サミット首脳宣言）