NISC

National center of Incident readiness and Strategy for Cybersecurity

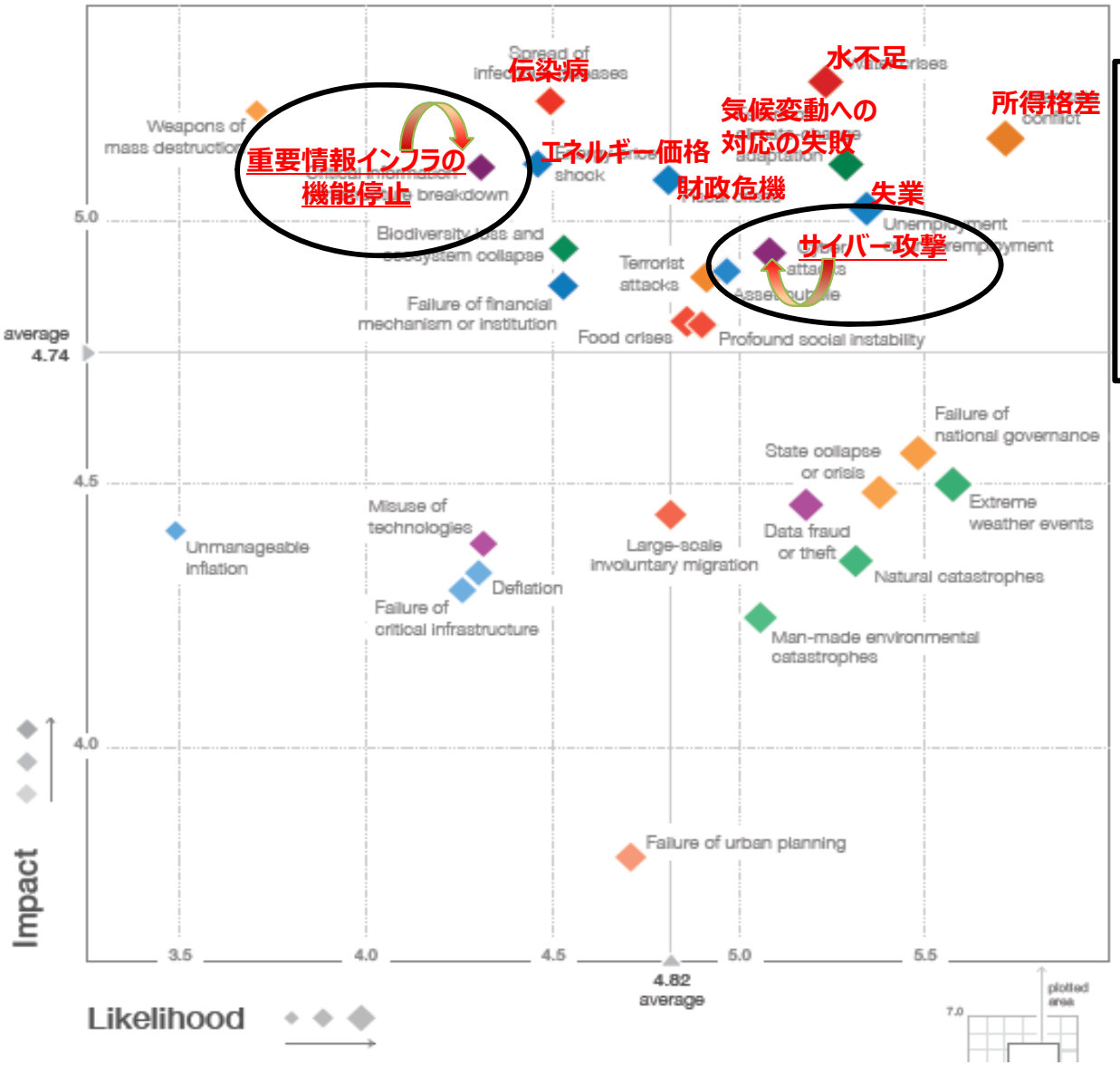
我が国のサイバーセキュリティ戦略

２０１５年２月２６日

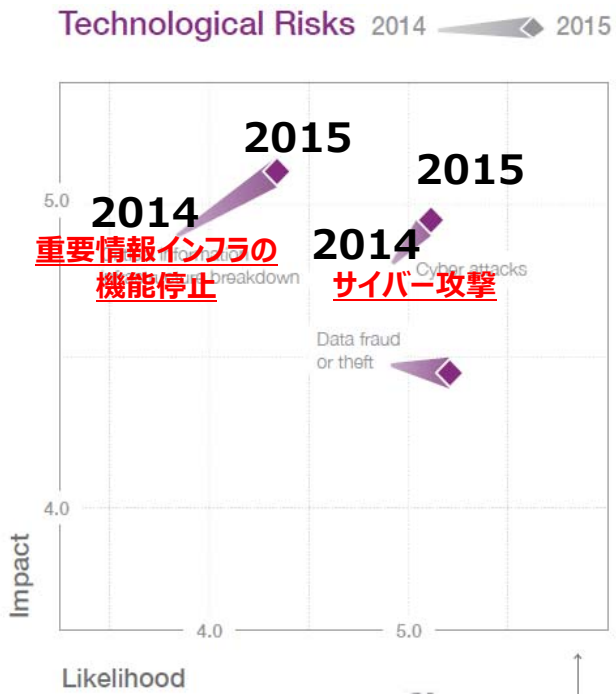
内閣サイバーセキュリティセンター（NISC）副センター長
内閣審議官　谷脇　康彦

http://www.nisc.go.jp/

世界が直面するグローバルリスク



"大規模サイバー攻撃のリスクは、発生確率、発生時の影響度のいずれの側面からみても平均的リスクを上回る。これはサイバー攻撃がますます洗練化されていることに加え、インターネットに接続されるモノが急増し、企業によってクラウドにより多くの機微性を有するパーソナルデータた蓄積されるようになってきていることによるものである。"



備考:全世界及び全産業界に対して重大な悪影響を及ぼす可能性のあるものとして抽出した28のリスクに関する今後10年間の展望について、世界各地の約900名の専門家に対する調査結果をとりまとめたもの。

(Source)World Economic Forum "Global Risks 2015 : 10th edition"

国家安全保障戦略（13年１２月閣議決定）

Ⅲ　我が国を取り巻く安全保障環境と国家安全保障上の課題

１　グローバルな安全保障環境と課題

(4)国際公共財(グローバル・コモンズ)に関するリスク

近年、海洋、宇宙空間、サイバー空間といった国際公共財(グローバル・コモンズ)に対する自由なアクセス及びその活用を妨げるリスクが拡散し、深刻化している。

（中　　略）

情報システムや情報通信ネットワーク等により構成されるグローバルな空間であるサイバー空間は、社会活動、経済活動、軍事活動等のあらゆる活動が依拠する場となっている。

一方、国家の秘密情報の窃取、基幹的な社会インフラシステムの破壊、軍事システムの妨害を意図したサイバー攻撃等によるリスクが深刻化しつつある。

我が国においても、社会システムを始め、あらゆるものがネットワーク化されつつある。このため、情報の自由な流通による経済成長やイノベーションを推進するために必要な場であるサイバー空間の防護は、我が国の安全保障を万全とする観点から、不可欠である。

サイバー空間と国際法の適用関係

“International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.”

(Source) UN General Assembly, Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security (June 2013)

「サイバーセキュリティ戦略」（平成25年6月情報セキュリティ政策会議）

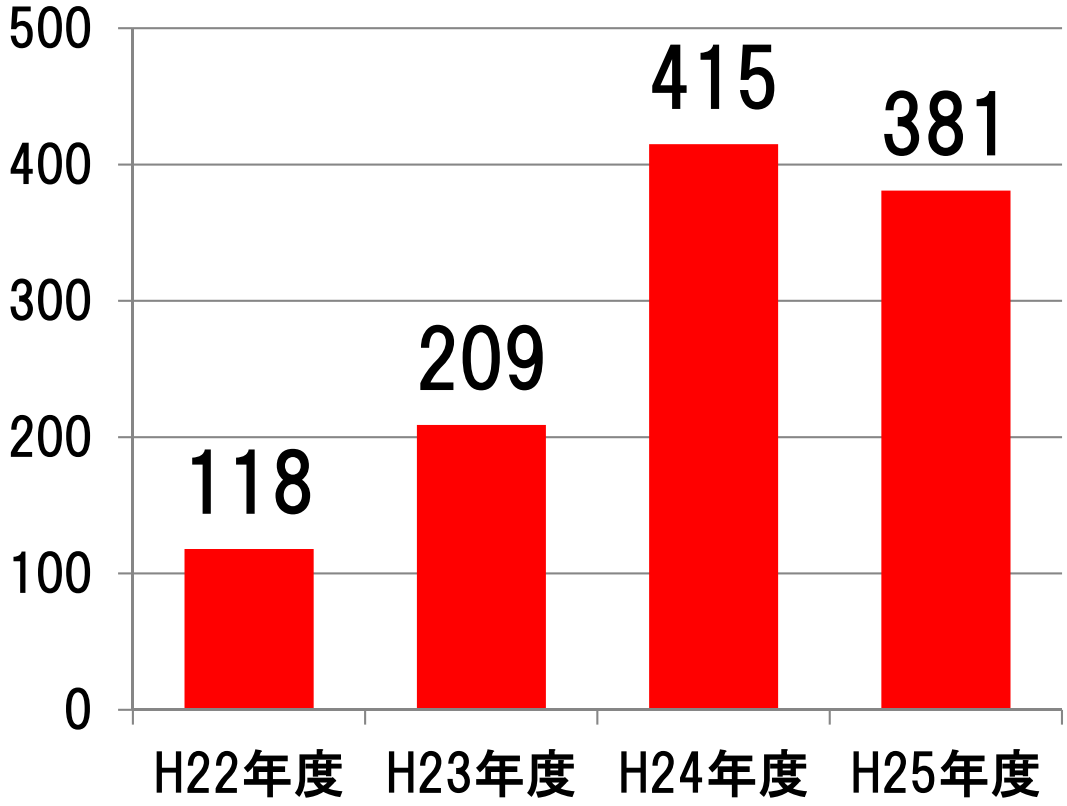
NISC

	政府機関・独立行政法人等	重要インフラ事業者	企業・一般個人
「強靱な」サイバー空間（守り強化）	① ●機微情報を守るためのリスク評価手法の確立【2014年6月】・統一基準の見直し【同年5月】 ●GSOCの強化、CYMAT・CSIRTとの連携による 的確・迅速な対応 ●対処訓練の実施（3・18（サイバー）の日）、警察・自衛隊等の関係機関の役割整理 ●SNS・グループメールを含む新サービスに伴う新たな脅威への対応【2014年5月】	② ●重要インフラの範囲拡大や安全基準見直し等行動計画の見直し【2014年5月】 ●政府機関やシステムベンダー等との情報共有の強化 ●事業継続確保のための分野横断的な演習 ●重要インフラで利用される制御機器等を国際標準に則って評価・認証するための基盤構築	●スマートフォン不正アプリへの対応 ●情報セキュリティ月間・「サイバーセキュリティの日」創設【毎年2月】 ●普及啓発プログラム（2011年情報セキュリティ政策会議）の改訂【2014年7月】 ●税制など中小企業のセキュリティ投資の促進 ●ISP等による個人への感染に関する注意喚起などIT 関係事業者の取組 ●ログ保存の在り方検討などサイバー犯罪の事後追跡可能性の確保
「活力ある」サイバー空間（基礎体力）	③ ●人材育成プログラム（2011年情報セキュリティ政策会議）の改訂【2014年5月】 ④ ●研究開発戦略（2011年情報セキュリティ政策会議）の見直し【2014年7月】		
「世界を率先する」サイバー空間（国際戦略） ●国際戦略の策定【2013年10月】	⑤ ●日ASEAN【2009年～：日ASEAN政策会議注1（2014年10月・東京）】等 ●日米【2013年～：日米サイバー対話（2014年4月・ワシントンDC）】等 ●日英【2012年～：日英サイバー協議】 ●日印【2012年～：日印サイバー協議】 ●日EU、日仏、日イスラエル、日エストニア、日豪、日露… ●サイバー空間の国際規範づくり等に関する会議【2011年～：次回（2015年4月・オランダ・ハーグ）】 ●IWWN注2（2014年5月・東京） ●MERIDIAN注3（2014年11月・東京）		〈注１〉 日・ASEAN情報セキュリティ政策会議。各国局長級が参加。 〈注２〉 サイバー空間の脆弱性、脅威、攻撃に関する国際的取組の促進。米・独・英・日等の政府機関、CERTが参加。 〈注３〉 重要インフラ防護等のベストプラクティス共有や国際連携等に関する意見交換。米・英・独・日等の政府機関が参加。 ●共同意識啓発活動【毎年10月】
組織体制	⑥ ●NISCの機能強化（サイバーセキュリティセンター（仮称）への改組：2015年）		

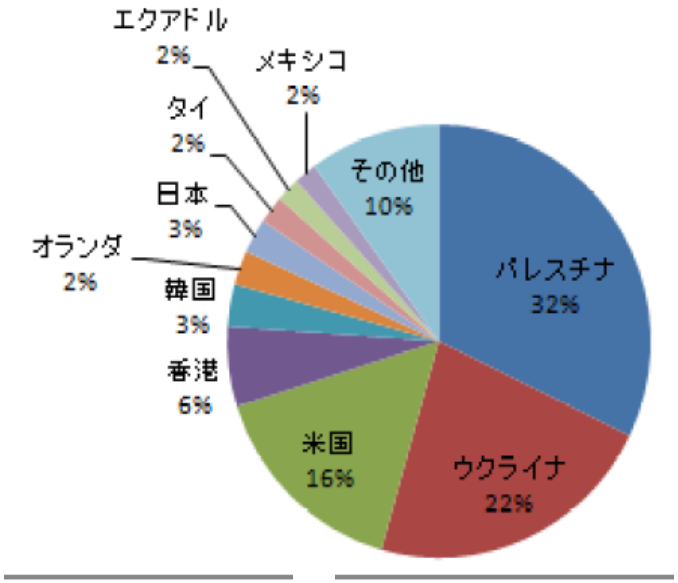
増加する標的型メール攻撃

○機密情報などの窃取を目的としたサイバー攻撃
○年々増加し、手口も巧妙化（組織的な攻撃の可能性）
○感染後の通信の接続先は、ほとんどが海外。

政府機関等への標的型メールに関する
注意喚起の件数の推移



H25年中の標的型メール攻撃に使用された
不正プログラム等の接続先



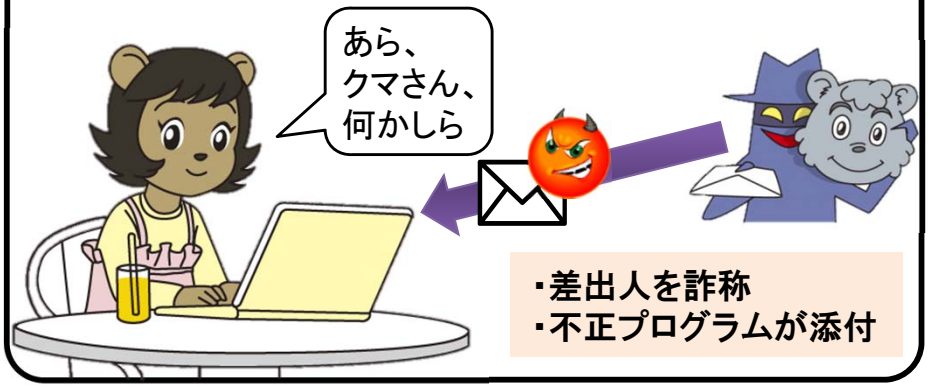
出典：警察庁（H26年2月）

様々な標的型攻撃

〇標的型攻撃は、初期潜入し、遠隔操作により侵入範囲を拡大し、情報窃取等を行うもの
〇初期潜入段階において、端末を不正プログラムに感染させるために種々の手口が使われている

A. メール

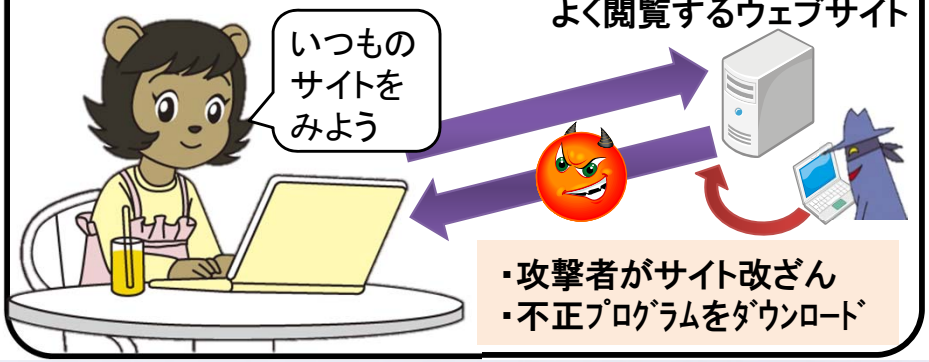
よく知っている人からのメールだと思って添付ファイルを開いてしまうと・・・



・差出人を詐称
・不正プログラムが添付

B. ウェブ閲覧（水飲み場型）

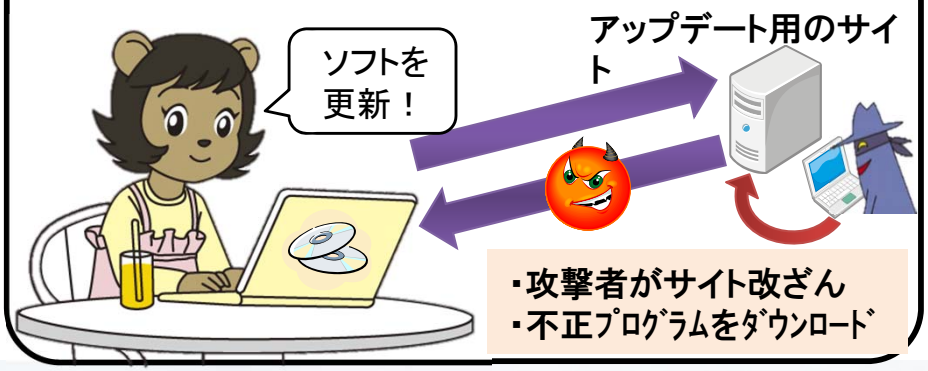
いつも閲覧しているウェブサイトにアクセスすると・・・



・攻撃者がサイト改ざん
・不正ﾌﾟﾛｸﾞﾗﾑをﾀﾞｳﾝﾛｰﾄﾞ

C. ソフトウェアアップデートを悪用

ソフトウェアのアップデート機能を使用すると・・・



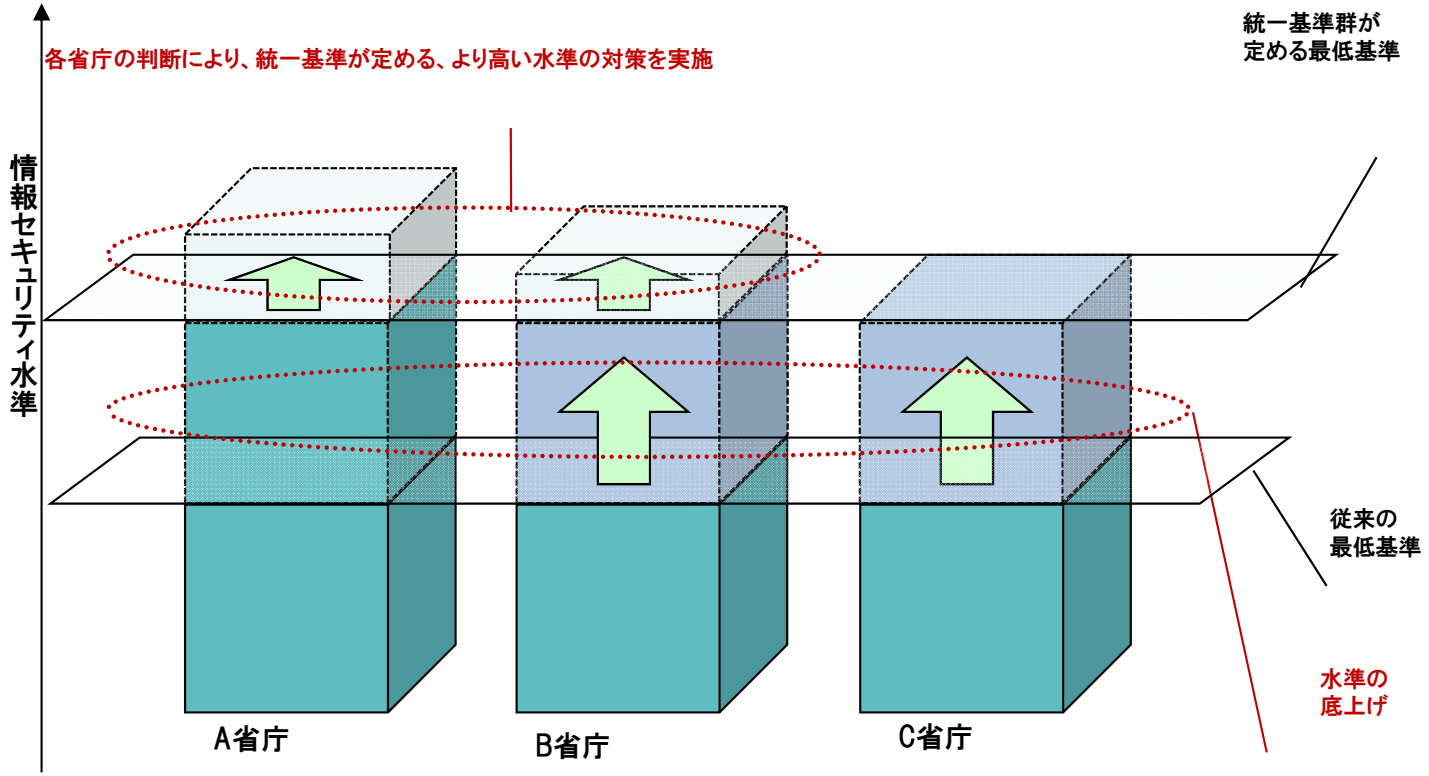
・攻撃者がサイト改ざん
・不正ﾌﾟﾛｸﾞﾗﾑをﾀﾞｳﾝﾛｰﾄﾞ

統一基準群（政府機関セキュリティポリシーのベースライン）

○政府機関が実施すべき対策の統一的な枠組みを構築

○政府機関全体の情報セキュリティ水準の底上げに寄与

＜統一基準群の効果（イメージ）＞



統一基準群の改定（14年5月、情報セキュリティ政策会議決定）

◆ 標的型攻撃への対策

➢ 標的型攻撃から守るべき重点業務等を特定し、関係する情報システムについて、内部侵入を早期発見し、活動を困難化するための対策を計画的に講ずる。

標的型攻撃のイメージ

・特定の組織の情報に狙い
・従来の外壁防護を無効化

内部対策の強化が重要

◆ サプライチェーンリスクへの対策

➢ 情報システムの構築等の外部委託の際、委託先における不正機能の混入防止のため、厳正な管理を要求。

高度サイバー攻撃対処のための取組等（14年6月、CISO等連絡会議決定）

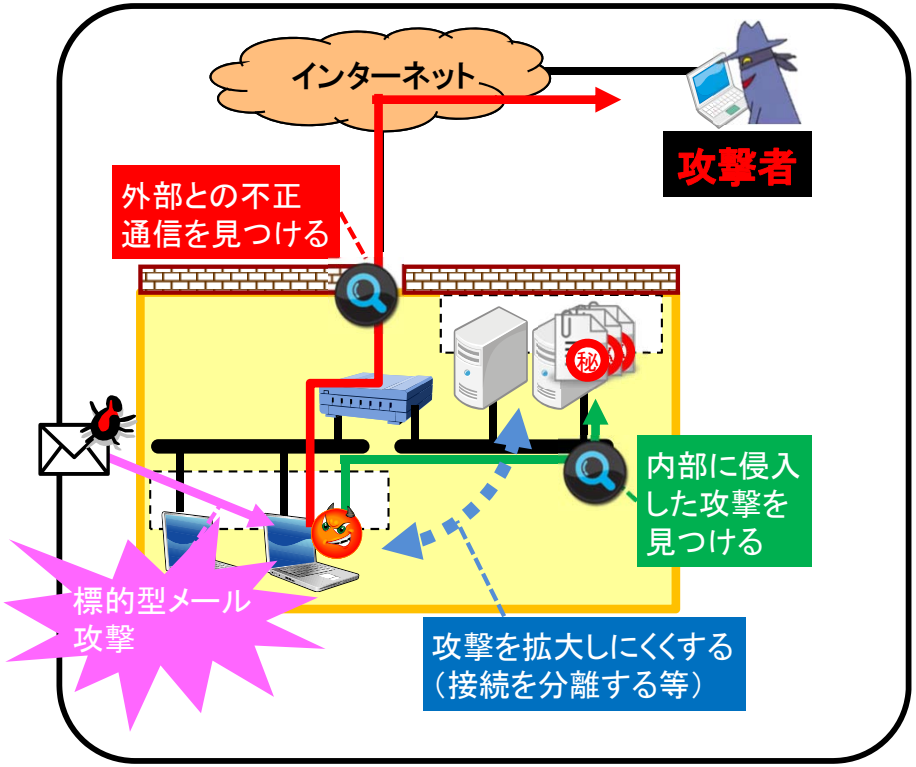
高度サイバー攻撃対処のための取組

◆ 取組の概要

- 高度サイバー攻撃の脅威から重要な業務・情報を取り扱う情報システムを守るため、それらを特定し、対象となる情報システム内部に侵入した攻撃の発見・遮断を目的とした対策を、計画的・重点的に実施する取組を今年度から本格的に実施する。

（平成26年6月25日　情報セキュリティ対策推進会議）

情報セキュリティ対策の概要(例)



独立行政法人における情報セキュリティ対策の推進

◆ 独立行政法人におけるセキュリティ対策の推進

- 独立行政法人がサイバー攻撃の標的となっている事例が複数判明
- 独立行政法人においても、政府の重要な情報を扱う場合は、政府機関と同等の情報セキュリティ対策を講ずることを決定

（平成26年6月25日　情報セキュリティ対策推進会議）

独法及び主務省庁が一体となって対策を推進

1. 業務計画の中で情報セキュリティ対策を位置付け
   - ・統一基準群を踏まえた情報セキュリティ対策を独法にも適用
2. 連絡体制構築により、迅速な情報連絡・共有
   - ・経営管理層への情報展開、判断による迅速な対応
3. 業務評価の際にフォローアップし、対策を着実に推進
   - ・対策の実効性確保のための推進力

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

（2014年5月、情報セキュリティ政策会議決定）

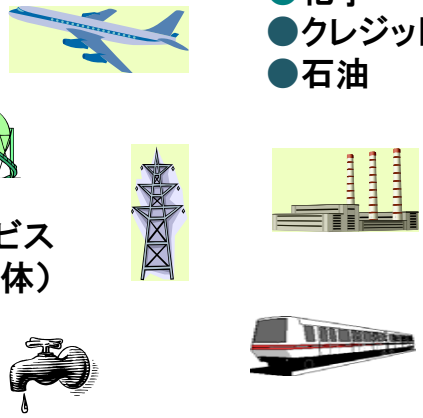
NISC

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
- 化学
- クレジット
- 石油

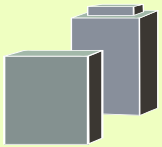


NISCによる調整・連携

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］
- 経済産業省［電力、ガス、化学、クレジット、石油］
- 国土交通省［航空、鉄道、物流］

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・演習・訓練間の連携による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

重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定指針

指針策定の背景

目指す方向

重要インフラにおけるサービスの持続的な提供

課題

IT障害の極小化／IT障害の迅速な復旧と再発防止

一義的には重要インフラ事業者等による適切かつ継続的な実施・改善が必要

課題解決に向けて

～自らの情報セキュリティ対策の水準や不足を知るために、照らす規範等（安全基準等）が必要～

国の施策として、情報セキュリティ対策の水準の維持・向上に資するガイドラインの提示

～分野ガイドラインや事業者等の内規等の策定・改訂に資する指針の提示～

＊第3次行動計画を受けた指針（改訂版）を2015年度に提示

指針（改訂版）の概要

指針の体系（以下3冊にて構成）

記載内容

指針_本編（概念）
＊改訂

Ⅰ．目的及び位置付け
Ⅱ．「安全基準等」で規定が望まれる項目

「策定の目的」、「対象範囲」、「対象とする原因」、「役割」、「公開」、「対策項目（PDCAベース）」に係る解説

具体的に何をすればよいか

指針_対策編（具現化例）
＊改訂

Ⅰ．対策編の位置付け
Ⅱ．具体的な情報セキュリティ対策項目の例示

対策項目（PDCAベース）毎の取組や成果等の例示

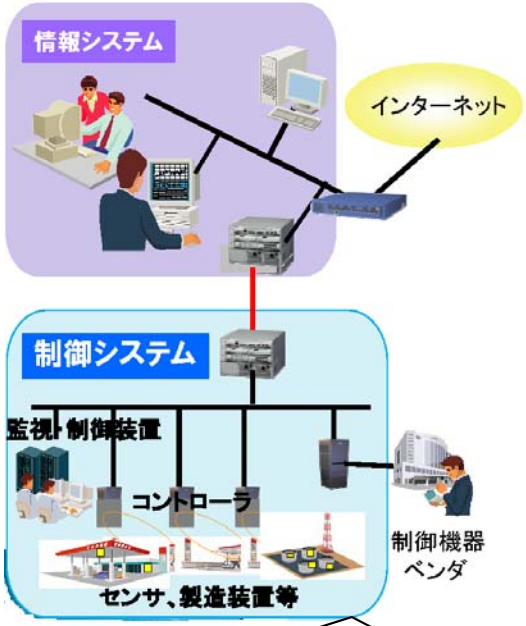
どの対策から行うか

指針_手引書（優先順位付け等の考え方）
＊新設

Ⅰ．目的及び位置付け
Ⅱ．情報セキュリティ対策の優先順位付け及び対応策決定のプロセス

各プロセスを解説しつつ、「どのような対策をどの程度で行うか」を各事業者等が自ら定めることを推奨

制御システムの普及



従来

制御システムは事業者毎に固有の仕様部分が多く、詳細な内部仕様等を把握できない限り、外部からの攻撃は難しいものであった。

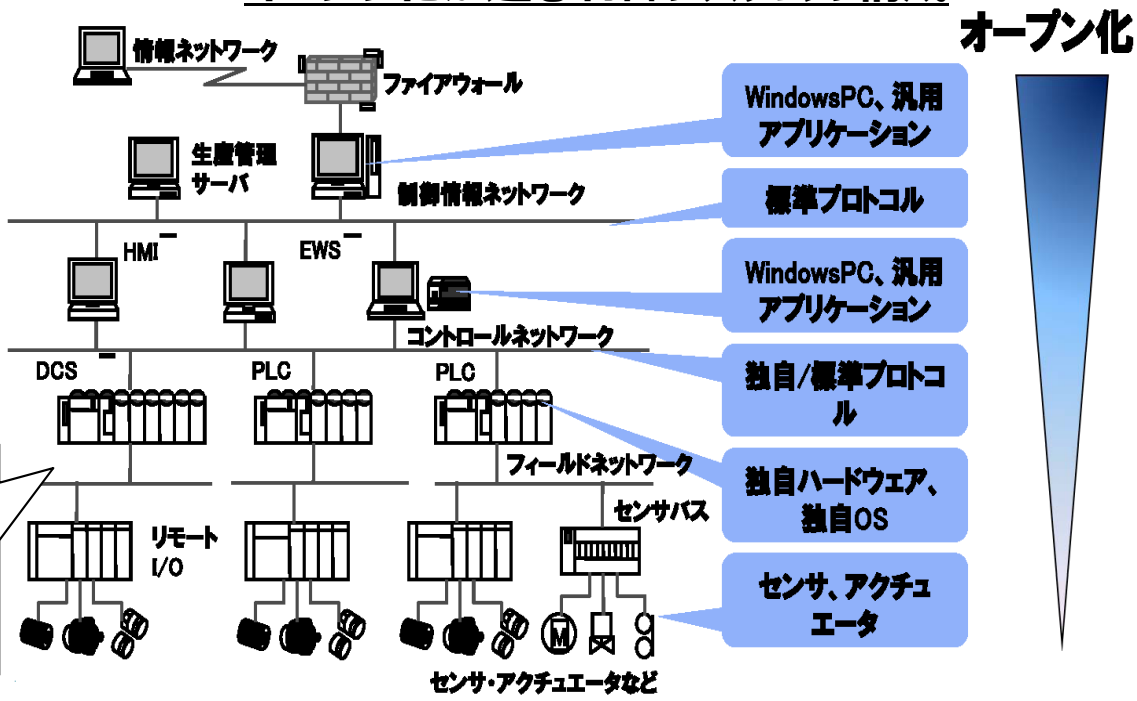
最近の状況

○ 標準プロトコルや汎用製品が仕様に採用され、汎用化が進んでいる。
○ 外部ネットワークにも接続されるようになっている。
○ このような状況から事業者及びシステム開発企業の利便性が向上してきている反面、攻撃対象になりやすいという特徴が現れてきている。

○ 生産の自動化や、フィードバック制御による入力値の自動制御等、様々な用途で工数の軽減や正確性の向上を目的に利用。
○ 最近は、一般的な情報システムが接続するオフィスネットワークから、制御情報系ネットワーク、制御ネットワークを介して、制御システムのコントローラやセンサーまでを間接的に接続するような構成が多い。

○ アプリケーション等が動作する上層のレイヤではWindowsのパソコン等のクライアント端末や汎用アプリケーション、標準プロトコルを利用。
○ 実際の制御に関わる下層部分は独自のプロトコルやハードウェア、OSが利用される割合が高く、固有の仕様により構成。
○ オープン化が上層部から徐々に進行。

オープン化が進む制御システムの構成



【出典：独立行政法人情報処理推進機構「制御システムセキュリティ国際標準の現状と日本の取組み」（2011年11月18日）http://www.ipa.go.jp/files/000025094.pdf】

重要インフラ分野横断的演習

	2012年度	2013年度	2014年度
参加機関	42組織 (21事業者等)	61組織 (38事業者等)	94組織 (70事業者等)
参加者	148名	212名	348名

演習の模様

意見交換会の模様

新・情報セキュリティ人材育成プログラム（１４年５月、情報セキュリティ政策会議決定）

NISC

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するためには、
○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

IT人材106万人（SE80万人） *IPA調べ

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

【需要】経営層の意識改革

○**組織の経営層**
・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。**

○**実務者層のリーダー層**
・**経営戦略の視点から情報セキュリティの課題や方向性を考え、経営層と実務者層の橋渡しができる能力を育成。**

【供給】人材の「量的拡大」と「質的向上」

○**IT技術者等**に、情報セキュリティを必須能力として位置付け、訓練・演習教材等の作成や能力評価基準・資格のあり方の検討を進める。

○**高度な専門性及び突出した能力を有する人材**の発掘・育成を推進するとともに、実社会での活躍を促進。

○**グローバル水準の人材**の育成に向け、国際的な体験や情報共有を通じて人材が研鑽を積む環境を構築。

○**政府機関**は自ら率先して、情報セキュリティ上のリスクに対応できる職員の採用・育成や研修・訓練等を強化。

○**教育機関**（初等中等教育機関含む）の実践的なIT教育を充実させるとともに、情報セキュリティに関する教員養成を推進。

企業等における情報漏えいインシデントの動向

○企業等における情報漏えいインシデントについて、全体の件数自体は減少しているが、**不正アクセスを原因とする大規模な被害**が急増。

2013年個人情報漏えいインシデント

	2013年データ	2012年データ
漏えい人数	925万2305人	972万65人
漏えい件数	1388件	2357件
想定損害賠償総額	1438億7184億円	2132億6405万円
一件当たりの漏えい人数	7031人	4245人
一件当たり平均想定損害賠償額	1億926万円	9313万円
一人当たり平均想定損害賠償額	2万7701円	4万4628円

件数は減少

被害が大規模化

インシデントの規模トップ10

No.	漏えい人数	業種	原因
1	400万人	情報通信業	不正アクセス
2	169万2496人	情報通信業	不正アクセス
3	47万人	卸売業，小売業	不正アクセス
4	42万6000人	公務（他に分類されるものを除く）	紛失・置忘れ
5	24万3266人	情報通信業	不正アクセス
6	17万5297人	情報通信業	設定ミス
7	15万0165人	卸売業，小売業	不正アクセス
8	12万0616人	金融業，保険業	管理ミス
9	10万9112人	情報通信業	不正アクセス
10	9万7438人	情報通信業	不正アクセス

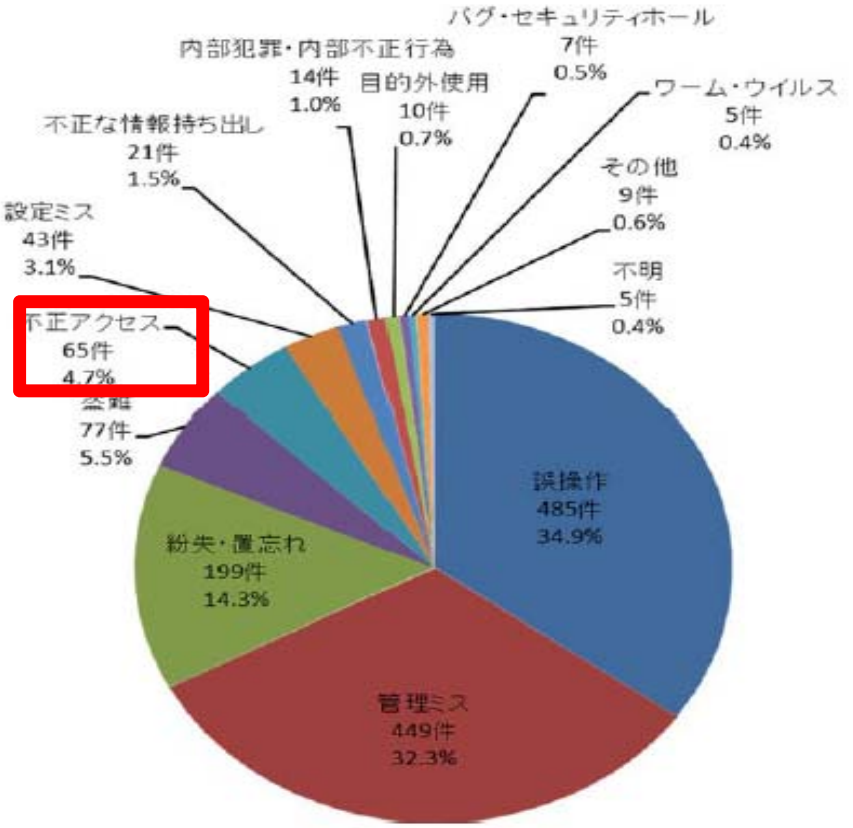
情報通信業が多い

2013年は不正アクセスが急増！

100万人以上！

大規模な漏えいの上位を占める不正アクセス

2013年原因別インシデント数



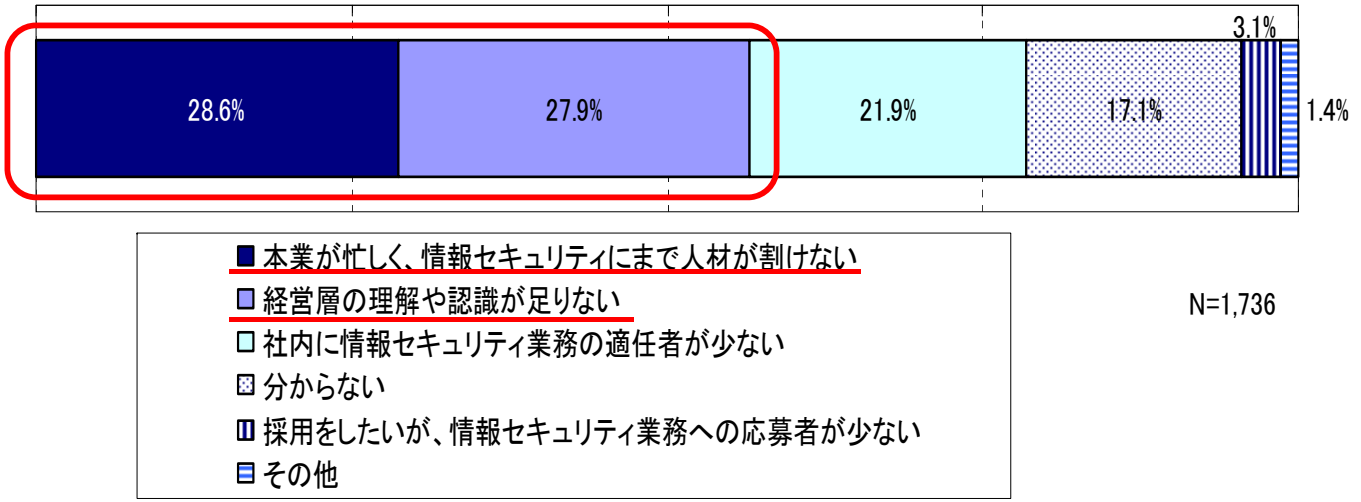
出典：2013年度 情報セキュリティインシデントに関する調査報告～情報漏えい編～（日本ネットワークセキュリティ協会（JNSA））

2013年1月1日～12月31日の1年間にインターネットニュース等で報道されたインシデントの記事、組織から公表されたインシデントのプレスリリース等をもとに集計。想定損害賠償額については、JNSAが開発したモデルを用いて推定。

企業等における情報セキュリティ対策の現状

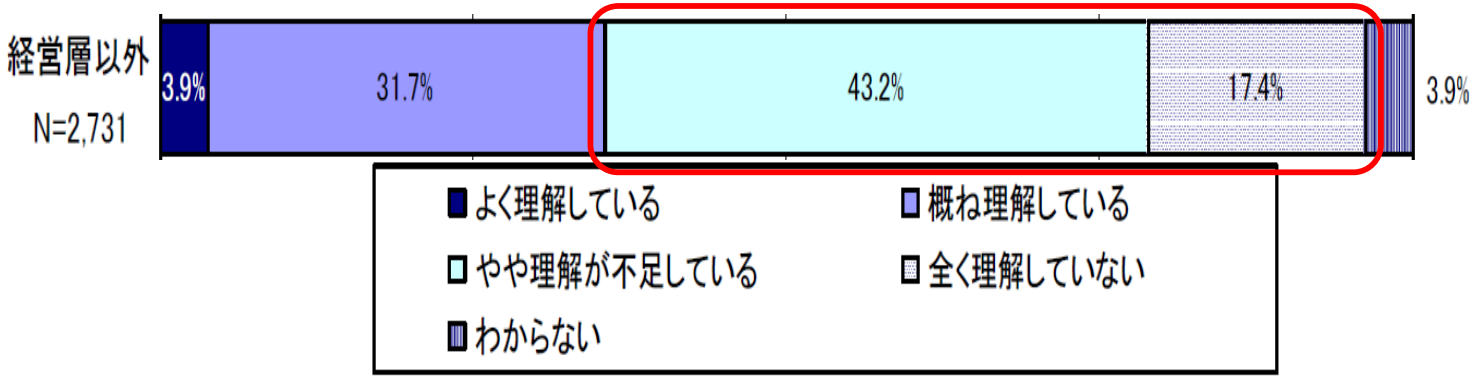
○企業では<u>情報セキュリティに関する業務に従事する人員が不足</u>。その原因として、「情報セキュリティにまで人材が割けない」「経営層の理解や認識が足りない」が半数を超えている。
○経営層のセキュリティに対する理解度として「やや理解が不足」「全く理解していない」が6割程度。

人材不足の原因（社内向け業務）



企業経営層の情報セキュリティに対する理解度

（経営層以外からの回答）



出典：独立行政法人情報処理推進機構「情報セキュリティ人材の育成に関する基礎調査」2012年4月

米証券取引委員会(SEC)「企業財務部門開示ガイダンス」

「CF Disclosure Guidance」とは

- サイバーセキュリティ・リスク及びサイバーインシデントに関わる開示義務に関する、SEC企業財務部門の見解の記述をガイドする文書。
- サイバーセキュリティが、当該企業の事業に重要な影響を与える場合に、財務リスクなどと同様に開示を要求し得る、新たなビジネスリスクとして識別している。
  - ただし、企業に法的義務を課すSECのルールや規則とは異なり、企業に新たな開示義務を課すものではない。
  - また、SECはガイダンスの内容について、承認／非承認のいずれも行っていない。

右記の6項目に関して、サイバーセキュリティ・リスクやインシデントに関する、開示概要を示している

リスクファクター
- 企業のサイバーインシデントに関するリスクが、当該企業への投資を、投機的或いは危険なものにし得るファクターの中で最も重要なリスクファクターである場合に、その開示をする必要がある。

MD&A*1
- サイバーセキュリティ・リスク及びサイバーインシデントに関わる費用やその他の影響が、企業経営、資産流動性、財務状況等に重大な影響を与えると考えられる場合には、それらについてMD＆Aの中で開示する必要がある。

事業内容
- サイバーインシデントが、企業の製品、サービス、顧客や取引先との関係や競合状況に重大な影響を与える場合には、当該企業の「事業内容」の中でそれについて開示する必要がある。

法的手続
- 企業或いはその子会社が、サイバーインシデントに関わる法的手続を保留されている場合には、その訴訟に関わる情報を、当該企業の「法的手続に関する情報開示」の中で開示する必要がある。

財務諸表の開示
- 潜在的或いは実際のインシデントの性質や大きさにより、サイバーセキュリティ・リスクやサイバーインシデントは当該企業の財務諸表に広範な影響を与える可能性があることを開示する必要がある。

サイバーインシデントの発生前段階及び発生事後段階
- 企業が取り組んだインシデント回避対策コスト（発生前段階）や顧客とのビジネス関係を維持するために顧客に提供した費用または損失等（発生事後段階）を考慮する。

開示規制及び手続き
- 企業は、開示規制及び手続きの有効性に関する結論を開示する必要がある。

*1 Management's Discussion and Analysis of Financial Condition and Results of Operations：経営者による財政状態及び経営成績の検討と分析。米国では、SECが投資家への情報提供の一環として企業に開示を要求している。

（出所）ＮＴＴデータ

情報セキュリティ研究開発戦略（改定版）（14年７月、情報セキュリティ政策会議決定）

サイバーセキュリティ戦略（2013年6月策定）において示された
- ○ サイバー攻撃の検知・防御能力の向上
- ○ 制御システム、ICチップなど社会システム等を保護するためのセキュリティ技術の確立
- ○ ビッグデータ（パーソナルデータ等）利活用等の新サービスのための技術開発　等

を推進する観点から、**「情報セキュリティ研究開発戦略」を改定**

情報セキュリティ研究開発の推進方針

1. サイバー攻撃の検知・防御能力の向上
- ・分散しているサイバー攻撃情報等の共有のための組織等の連携強化
- ・研究者等へ政府の有するサイバー攻撃の検体等の提供等を検討

2. 社会システム等を防護するためのセキュリティ技術の強化
- ・制御システム等のセキュリティ技術の国際標準化・認証制度等を推進

3. 産業活性化につながる新サービス等におけるセキュリティ研究開発
- ・今後発展が期待されるICT利用分野で上流工程からセキュリティ品質の組込を推進

4. 情報セキュリティのコア技術の保持
- ・暗号等のコア技術の保持は、我が国の新規産業創出や安全保障等の観点から重要であり維持・強化

5. 国際連携による研究開発の強化
- ・各国が「強み」を有する技術を組合せ発展させるため、研究者受入等国際連携を推進

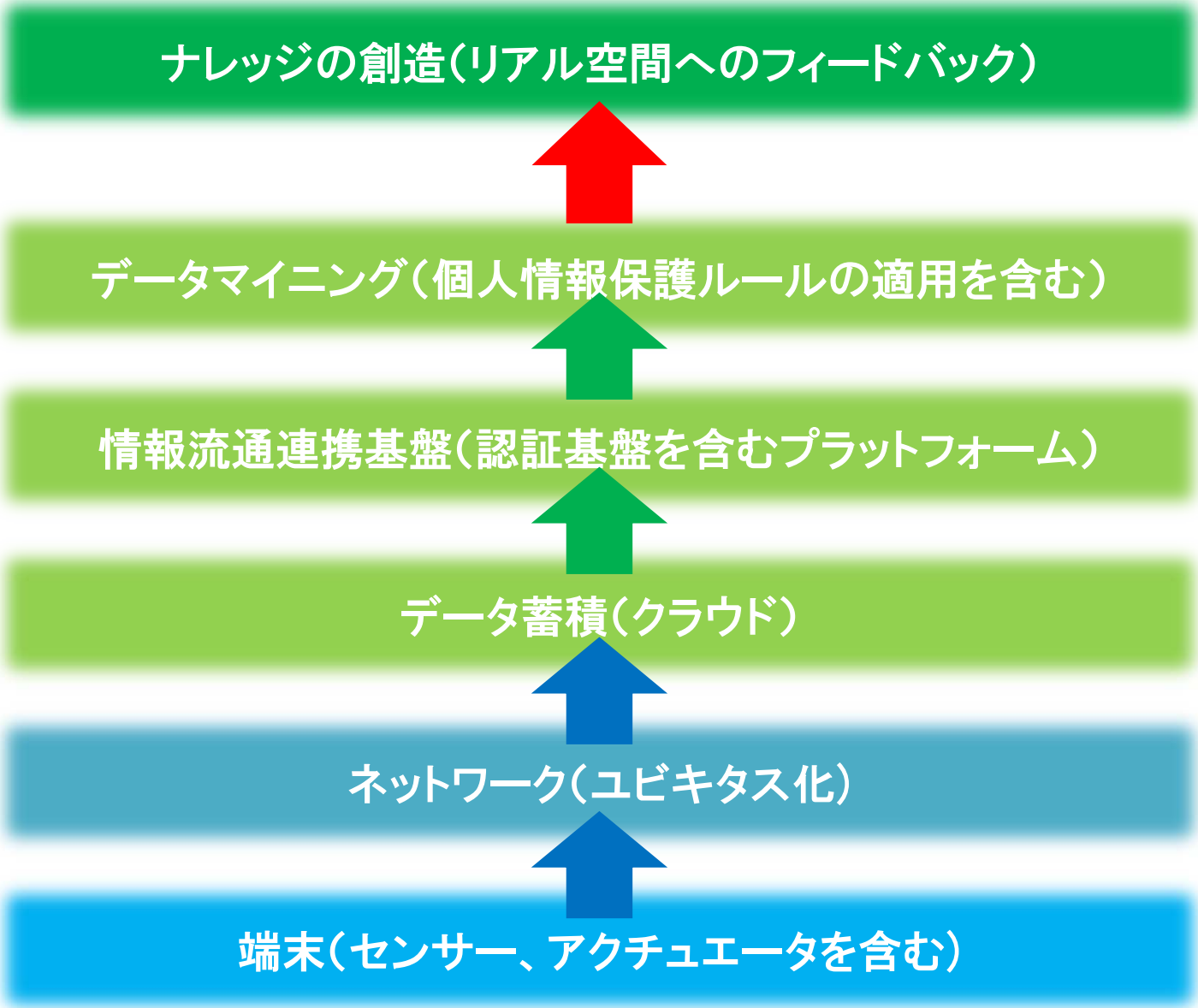
研究開発の効果・成果を高めるための方策等

1. 研究成果の社会還元の推進
2. 必要な研究開発リソースの確保と柔軟性確保
3. 情報セキュリティ技術と社会科学など他分野との融合

情報セキュリティ研究開発における重要分野
（※　左記の観点を踏まえ、重要分野を整理）

(1)情報通信システム全体のセキュリティの向上
サイバー攻撃の検知、認証、次世代ネットワーク　等
(2)ハード・ソフトウェアセキュリティの向上
制御システム、デバイス、ソフトウェアの安全性確保　等
(3)個人情報等の安全性の高い管理の実現
プライバシー保護、パーソナルデータ利活用　等
(4)研究開発の促進基盤の確立と理論の体系化
理論体系化、調査研究、標準化、評価、暗号技術　等
(5)発展分野でのセキュリティ研究開発
医療健康、農業、次世代インフラ、ビッグデータ、自動車のネットワーク接続　等

データ主導型社会を支えるIoT



検討事項（例）

■自律・分散・協調型NW
（インターネット網に類似）
→マルチステークホルダーによる検討が必要。

■Security by Designの徹底

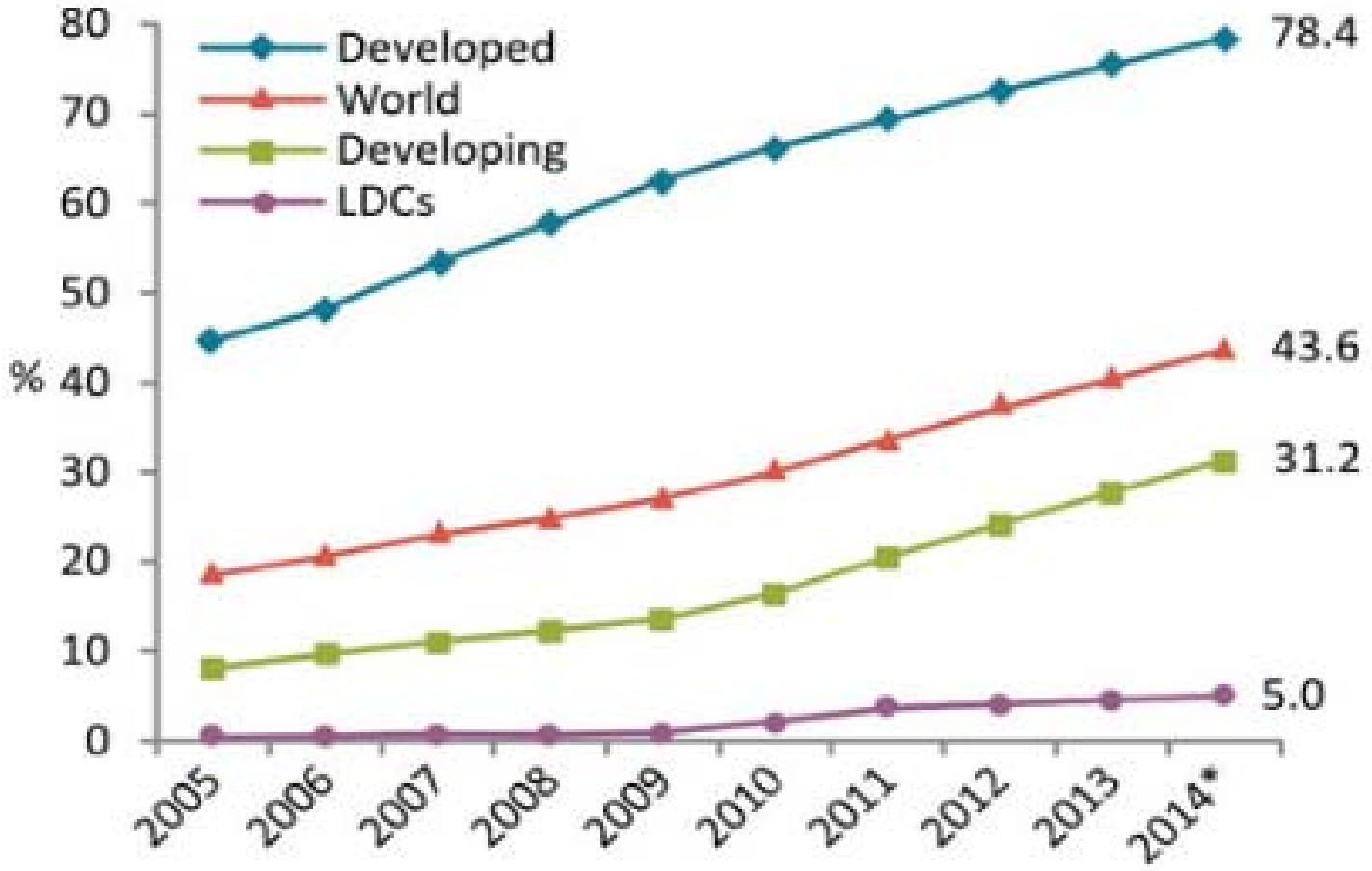
■異NW間の責任分界点とインターフェースの共通化

■インシデント情報の共有体制（連鎖の拡大への対応）

■個人情報保護の仕組み

世界のインターネット世帯普及率の推移

世界約30億人がインターネットを利用（2014年度末、推計値）



(Source) ITU “Measuring the Information Society” (October 2014)

サイバーセキュリティ国際連携取組方針（１３年１０月）

策定方針の決定

日本再興戦略 -JAPAN is BACK-　（平成25 年6月14 日閣議決定）（抄）

4. 世界最高水準の IT 社会の実現　⑤サイバーセキュリティ対策の推進

世界最高水準の IT 社会にふさわしい、強靭で活力あるサイバー空間を構築するため、「サイバーセキュリティ戦略」を踏まえ、政府機関や重要インフラにおけるセキュリティ水準及び対処態勢の充実強化や国際戦略の推進等、サイバーセキュリティ対策を強力に展開する。

〇サイバーセキュリティに関する国際戦略の策定

- 我が国と戦略的に強い結び付きのある国・地域との多角的パートナーシップの強化、我が国が強みを持つセキュリティ技術の国際展開等を政府一体となって加速させるため、**今年度中に、「情報セキュリティ政策会議」において新たにサイバーセキュリティ国際戦略を策定する**とともに、来年度中に制御システム等のセキュリティの国内での評価・認証を開始し、インフラの整備・輸出等を促進する。

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）（抄）

４　推進体制等　（2）評価等

本戦略に基づく各種取組施策の確実な実施及び各施策間の有機的な連携を確保する観点から、サイバーセキュリティ立国の実現に向けた中長期の目標の管理を行うとともに、本戦略に基づき、2013年度から毎年度の年次計画及び**サイバーセキュリティに関する国際戦略を策定する**。

サイバーセキュリティ国際連携取組方針を策定

- サイバーセキュリティ政策で我が国として重視する国際連携に関する方針の明確化
- 我が国として具体的な貢献分野を訴求
- 重点的な取組地域（アジア太平洋、欧米等）を具体的に明示

バイ・マルチの政策対話において日本のスタンスをアピール

Copyright (c) 2013 National Information Security Center (NISC). All Rights Reserved.

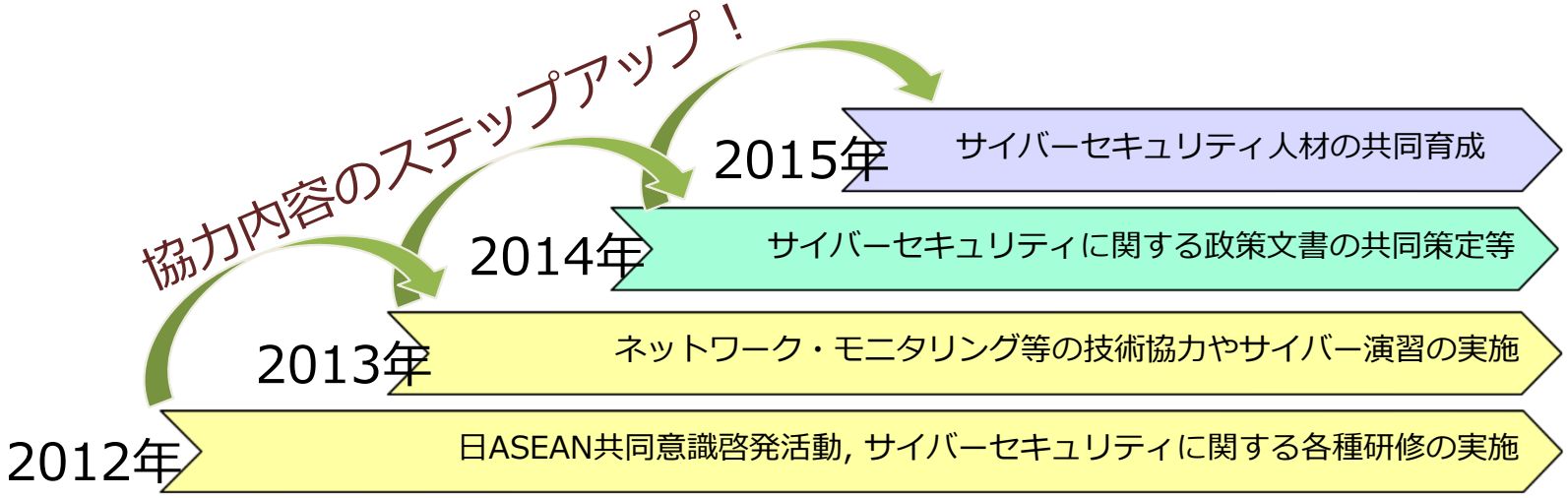
ASEANとの国際連携の成果（2013～2014年）

- ASEAN各国との国際会議*を主催，協力内容をステップアップ

2013年以前からの取組である日ASEAN共同意識啓発活動や各種研修，技術協力、サイバー演習等について、内容を充実・高度化させつつ継続

2014年の重点的取組として，「日ASEANにおける重要インフラ防護に関するガイドライン」を共同策定。また，サイバー犯罪対策対話によって法執行分野の能力構築支援を開始

2015年の重点的取組として，高度なスキルを有するサイバーセキュリティ人材の共同育成に向けた検討を開始



ASEAN・JAPAN

*第7回 日ASEAN情報セキュリティ政策会議(局長級）及び第3回日ASEANシンポジウム（2014年10月7日～9日・東京）
第6回 日ASEAN政府ネットワークセキュリティワークショップ（課長級）(2014年8月27日～28日・シンガポール）
重要インフラ専門家パネル（2014年1月・東京，2月・クアラルンプール，5月・タイ)
第1回 日ASEANサイバー犯罪対策対話（2014年５月・シンガポール）

国際連携に向けた政策対話の推進

EU
●重要インフラ防護や官民の情報共有等の取組の共有、意識啓発や政策動向の意見交換
●第2回日EU・ICTｾｷｭﾘﾃｨﾜｰｸｼｮｯﾌﾟ：２０１３年12月
●第1回日EUサイバー協議：２０１４年10月

英国
●国際規範づくり、安全保障分野での課題、サイバー犯罪への取組、重要インフラ防護、等に関する意見交換
●第２回日英サイバー協議：２０１４年１１月

インド
●安全保障分野での課題、サイバー犯罪への取組、重要インフラ防護等に関する　意見交換
●第1回日印サイバー協議：２０１２年11月

エストニア
○日エストニアサイバー協議(2014年12月)

フランス
○日仏サイバー協議(2014年12月)

イスラエル
○日イスラエルサイバー協議（2014年11月）

ロシア
○日露サイバー協議の立ち上げ予定

基本的な考え方
「情報の自由な流通の確保」という基本的な考え方の下、民主主義、基本的人権の尊重及び法の支配といった価値観を共有する国や地域とのパートナーシップ関係を多角的に構築・強化。

リスクのグローバル化

国際戦略の策定
●多角的なパートナシップの強化や技術の国際展開等の加速化

米国
●脅威認識の共有、国際規範づくり、重要インフラ防護、防衛分野のサイバー課題等に関する意見交換
●第2回日米サイバー対話：２０１４年4月@ワシントン

ASEAN
●意識啓発、人材育成、技術協力、情報共有体制の構築等での連携
●サイバーセキュリティ協力に関する閣僚政策会議：平成25年9月
●共同意識啓発活動の実施：２０１２年10月~

オーストラリア
○日豪サイバー協議：2015年2月

多国間・マルチステークホルダーの取組み

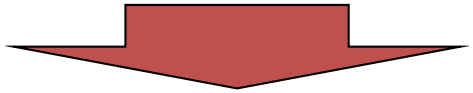
サイバー空間の国際規範づくり等に関する会議
●サイバー空間における自由と安全保障の両立、開放性や透明性、マルチステークホルダーの重要性、サイバー空間における**国際行動規範づくり**，サイバー犯罪条約，キャパシティ・ビルディング、サイバー空間における従来の**国際法や国家間関係を規律する伝統的規範の適用**、信頼醸成措置等に関する対話。
●60ヵ国の政府機関，国際機関，民間セクター，NGO等が参加。　●ハーグ会議：20１５年4月

MERIDIAN
●**重要インフラ防護**等のベストプラクティスの共有や国際連携方策等に関する意見交換。
●米・英・独・日等の重要インフラ防護担当者が参加。

IWWN
●サイバー空間の脆弱性、脅威、攻撃に関する国際的取組の促進。
●米・独・英・日等の政府機関、CERTが参加。

オリンピック・パラリンピック・ロンドン大会(2012)の教訓

GCHQ(政府通信本部)に政府予算を付けて英国全体のセキュリティ対策を実施。



■ロンドンオリンピック公式サイトへの攻撃
- ➢2週間の開催期間に2億1，200万回のサイバー攻撃(公式サイト "London2012.com")。
- ➢全体で23億件のセキュリティイベントが発生。
- ➢1秒間に1万1千件のDDoS攻撃を観測・防御。

■開会式での電力インフラ(照明)への攻撃
- ➢オリンピックに備えて考えられる限りの電力インフラへのサイバー攻撃対処訓練を5回実施。本番直前に攻撃情報があり、電力設備を急遽マニュアルで操作。
- ➢わずか30秒の停電で開催国の威信が損なわれる(reputation riskへの対応が重要)。

■教訓
- ➢「ダウンタイム」は許されない。
- ➢品質保証は"Right First Time"と"Fail Fast"が原則。
- ➢本格システム稼働は開催の28か月前。
- ➢英国との協力関係(2014年5月総理訪英、日英協定によるﾉｳﾊｳ移転、日英ｻｲﾊﾞｰ協議(同年11月))

オリンピック・パラリンピック東京大会に向けた政府の検討体制

オリパラ閣僚会議（議長：安倍総理）＝ **TOGC** (Tokyo Olympic Games Council)

オリパラ関係府省庁連絡会議（議長：杉田副長官）

セキュリティ幹事会

座長 － 内閣危機管理監

座長代理 －内閣官房オリパラ室長、内閣官房副長官補（内政）、内閣官房副長官補（事態対処・危機管理）、警察庁次長（シニア・セキュリティ・コマンダー）

構成員 － 内閣官房（内政・事態・ＮＩＳＣ・内調）、内閣府（防災担当）、警察庁、金融庁、総務省、消防庁、法務省、公安調査庁、外務省、財務省、文科省、厚労省、経産省、国交省、海上保安庁、原子力規制庁、防衛省の局長級

オブザーバー － 東京都、組織委、警視庁、東京消防庁の幹部

事務局 － 警察庁、総務省、外務省、経産省、国交省、防衛省の協力を得て内閣官房（内政・事態・NISC）において処理

テロ対策ＷＴ

座長 － 内閣審議官（事態、内政）

座長代理 － 警察庁審議官

※ 構成員等は今後調整

事務局 － 警察庁、国交省、防衛省の協力を得て内閣官房（事態・内政）において処理

サイバーセキュリティＷＴ

座長 －内閣審議官（ＮＩＳＣ副センター長）

座長代理 － 警察庁審議官

※ 構成員等は今後調整

事務局 － 警察庁、総務省、外務省、経産省、防衛省の協力を得て内閣官房（ＮＩＳＣ）において処理

サイバーセキュリティ2014（14年7月、情報セキュリティ政策会議決定）

NISC

▸「サイバーセキュリティ戦略」(2013年6月10日情報セキュリティ政策会議決定、対象期間：2013～2015年度)に基づく年次計画の2期目。

	2013	2014	2015
戦　略	「サイバーセキュリティ戦略」（2013/06/10）		
年次計画	「サイバーセキュリティ2013」（2013/06/27） • 戦略に基づき、各分野で新たな方針／プログラム等を策定	「サイバーセキュリティ2014」（2014/07/10） • 新たな方針／プログラム等を踏まえ、個々の施策をより具体化して推進	
「強靭な」サイバー空間	「政府機関統一基準群」改定（2014/05/19） 「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」策定（2014/05/19） 「情報セキュリティ普及・啓発プログラム」改定（2014/07/10）	【主な施策】 • 政府機関統一基準群の改定を踏まえた情報セキュリティポリシーの見直し（内閣官房及び全府省庁） • 政府機関におけるクラウドコンピューティングの情報セキュリティ対策の強化（内閣官房及び総務省） • 調達時における対策の推進（内閣官房） • GSOCの抜本的強化（内閣官房及び全府省庁） • 重要インフラに関する、安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント、防護基盤の強化（内閣官房、重要インフラ所管省庁、情報セキュリティ関係省庁、事案対処省庁） • 新たな情報セキュリティ普及啓発プログラムの策定・推進（内閣官房及び関係府省庁） • 高度化・巧妙化するマルウェアを検知・除去し、感染を防止するためのフレームワークの構築（総務省） • 日本版NCFTAの創設に向けた検討（警察庁） • 防衛情報通信基盤（DII）の整備（防衛省） • 国家レベルのサイバー攻撃への対応の強化（内閣官房、警察庁、総務省、外務省、経済産業省、防衛省及び関係省庁）	
「活力ある」サイバー空間	「情報セキュリティ研究開発戦略」改定（2014/07/10） 「情報セキュリティ人材育成プログラム」改定（2014/05/19）	【主な施策】 • 情報セキュリティ研究開発戦略の研究開発の推進（内閣官房及び関係府省庁） • 新・情報セキュリティ人材育成プログラムの推進（内閣官房） • サイバー攻撃事前防止・早期対策に向けた取組の推進（総務省） • 情報セキュリティに係る競技会・演習等の実施（総務省及び経済産業省） • 情報処理技術者試験制度に関する在り方についての検討（経済産業省）	
「世界を率先する」サイバー空間	「サイバーセキュリティ国際連携取組方針」策定（2013/10/02）	【主な施策】 • サイバー空間に関する国際的な規範作りへの参画等（内閣官房、総務省、外務省、経済産業省及び関係府省庁） • サイバーセキュリティ政策に関する二国間対話の強化（内閣官房、総務省、外務省、経済産業省及び関係府省庁） • 多国間の枠組み等における国際連携・協力の推進（内閣官房、外務省及び関係府省庁） • サイバー攻撃に関する諸外国関係機関との連携の強化（警察庁及び法務省） • 諸外国とのCSIRT間連携の強化（経済産業省）	
推進体制等	サイバーセキュリティ基本法 「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針」（2014/11/25）	【主な施策】 • NISCの機能強化（内閣官房） • 官民の情報共有の更なる推進（内閣官房及び関係府省庁）	

サイバーセキュリティ基本法の概要

第Ⅰ章．総則

■**目的（第1条）**

■**定義（第2条）**

⇒ 「サイバーセキュリティ」について定義

■**基本理念（第3条）**

⇒ サイバーセキュリティに関する施策の推進にあたっての基本理念について次を規定

① 情報の自由な流通の確保を基本として、官民の連携により積極的に対応

② 国民1人1人の認識を深め、自発的な対応の促進等、強靭な体制の構築

③ 高度情報通信ネットワークの整備及びITの活用による活力ある経済社会の構築

④ 国際的な秩序の形成等のために先導的な役割を担い、国際的協調の下に実施

⑤ IT基本法の基本理念に配慮して実施

⑥ 国民の権利を不当に侵害しないよう留意

■**関係者の責務等（第4条～第9条）**

⇒ 国、地方公共団体、重要社会基盤事業者（重要インフラ事業者）、サイバー関連事業者、教育研究機関等の責務等について規定

■**法制上の措置等（第10条）**

■**行政組織の整備等（第11条）**

第Ⅱ章．サイバーセキュリティ戦略

■**サイバーセキュリティ戦略（第12条）**

⇒ 次の事項を規定

① サイバーセキュリティに関する施策の基本的な方針

② 国の行政機関等におけるサイバーセキュリティの確保

③ 重要インフラ事業者等におけるサイバーセキュリティの確保の促進

④ その他、必要な事項

⇒ その他、総理は、本戦略の案につき閣議決定を求めなければならないこと等を規定

第Ⅲ章．基本的施策

■**国の行政機関等におけるサイバーセキュリティの確保（第13条）**

■**重要インフラ事業者等におけるサイバーセキュリティの確保の促進（第14条）**

■**民間事業者及び教育研究機関等の自発的な取組の促進（第15条）**

■**多様な主体の連携等（第16条）**

■**犯罪の取締り及び被害の拡大の防止（第17条）**

■**我が国の安全に重大な影響を及ぼすおそれのある事象への対応（第18条）**

■**産業の振興及び国際競争力の強化（第19条）**

■**研究開発の推進等（第20条）**

■**人材の確保等（第21条）**

第Ⅲ章．基本的施策（つづき）

■**教育及び学習の振興、普及啓発等（第22条）**

■**国際協力の推進等（第23条）**

第Ⅳ章．サイバーセキュリティ戦略本部

■**設置等（第24条～第35条）**

⇒ 内閣に、サイバーセキュリティ戦略本部を置くこと等について規定

附則

■**施行期日（第1条）**

⇒ 公布の日から施行（ただし、第Ⅱ章及び第Ⅳ章は公布日から起算して1年を超えない範囲で政令で定める日）する旨を規定

■**本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備等（第2条）**

⇒ 情報セキュリティセンター（NISC）の法制化、任期付任用、国の行政機関の情報システムに対する不正な活動の監視・分析、国内外の関係機関との連絡調整に必要な法制上・財政上の措置等の検討等を規定

■**検討（第３条）**

⇒ 緊急事態に相当するサイバーセキュリティ事象等から重要インフラ等を防御する能力の一層の強化を図るための施策の検討を規定

■**IT基本法の一部改正（第４条）**

⇒ IT戦略本部の事務からサイバーセキュリティに関する重要施策の実施推進を除く旨規定

サイバーセキュリティ戦略本部の機能・権限（イメージ）

NISC

内閣

サイバーセキュリティ戦略の案の閣議請議

内閣総理大臣

戦略の案の作成

行政各部の指揮監督に関する意見具申

IT総合戦略本部

① 高度情報通信ネットワーク社会の形成に関する重点計画の作成、同計画の実施推進

② 上記のほか、同社会の形成に関する施策で重要なものの企画に関する審議、同施策の実施推進

※ 上記の実施推進のうち、府省横断的計画・関係行政機関の経費見積り方針・施策の実施に関する指針の作成、施策の評価を政府CIOに委任

本部長　：官房長官
副本部長：国務大臣
本部員　：国家公安委員会委員長、総務大臣、外務大臣、経産大臣、防衛大臣、上記以外の国務大臣のうち本部の事務を遂行するために特に必要があるとして総理が指定する大臣
有識者のうち総理が任命する者

戦略案の意見

重要事項について緊密連携

サイバーセキュリティ戦略本部

①サイバーセキュリティ戦略の案の作成及び同戦略の実施推進

② 国の行政機関及び独法における対策基準の作成及び同基準に基づく施策の評価（監査を含む。）その他の同基準に基づく施策の実施推進

③ 国の行政機関で発生したサイバーセキュリティに関する重大な事象に対する施策の評価（原因究明のための調査を含む。）

④ 上記のほか、次の事務

イ）サイバーセキュリティに関する重要施策の企画に関する調査審議

ロ）同施策に関する府省横断的計画・関係行政機関の経費見積り方針・施策の実施に関する指針の作成、施策の評価その他の実施推進

ハ）同施策の総合調整

本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備等
（情報セキュリティセンター[NISC]の法制化等）

資料等提供義務

勧告

勧告に基づく措置の報告聴取

国家安全保障会議

① 国家安全保障に関する外交政策及び防衛政策に関し、平素から機動的・実質的に審議

② 武力攻撃事態等への対処等の国防に関する重要事項に関し審議

③ 重大緊急事態への対処に関する重要事項に関し、集中して機動的かつ実質的に審議し、必要に応じて、政府がとるべき措置等について建議

戦略案の意見

我が国の安全保障に関する重要事項について緊密連携

資料等必要な協力の求め

情報の提供等の協力の求め

地方公共団体、独立行政法人、国立大学、特殊法人・認可法人であって本部が指定するもの、国内外の関係者との連絡調整を行う関係機関　等

地方公共団体

求めに応じるよう努める

各府省等

我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針

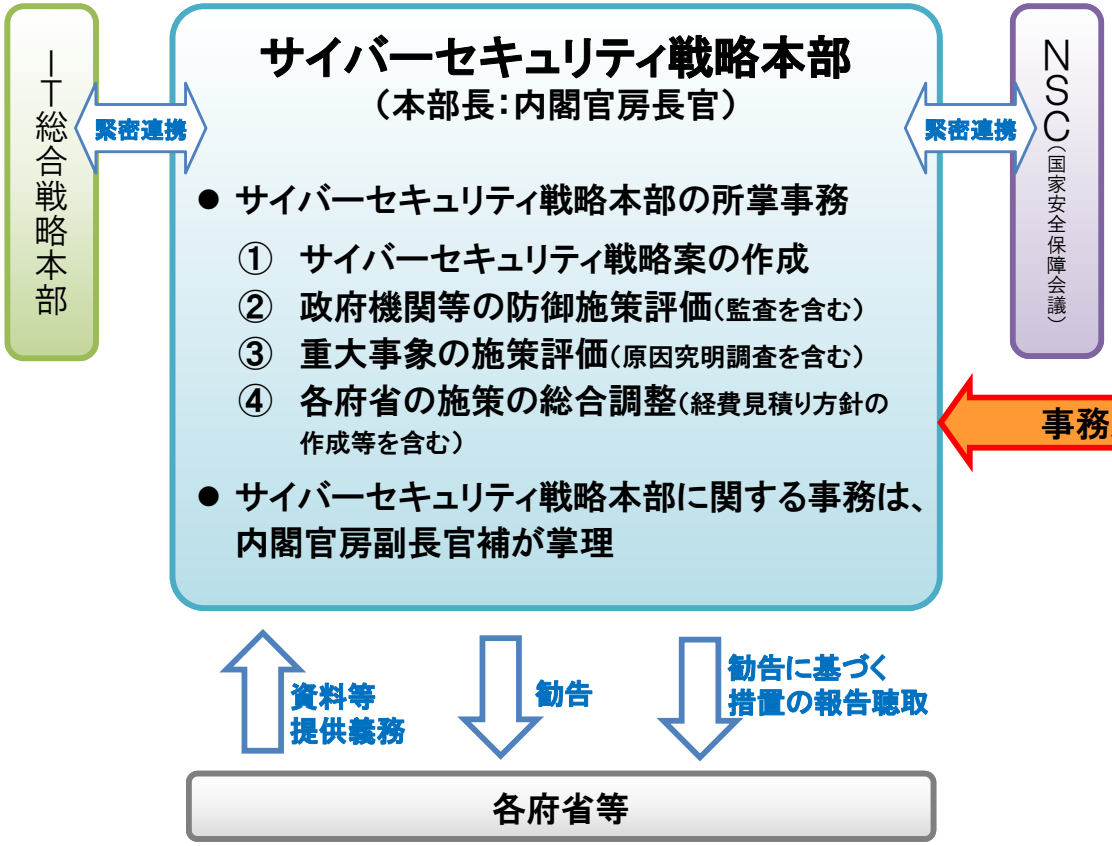
（2014年11月情報セキュリティ政策会議決定）

1　機能強化の必要性

以下の観点から、我が国の「サイバーセキュリティ」強化のための推進体制の機能強化が不可欠

- あらゆる活動のサイバー空間への依存の高まりにより、リスクが深刻化（甚大化・拡散・グローバル化）
- 「世界最高水準のIT利活用社会」の実現が成長戦略の柱の1つ
- 国際的な連携の強化が必要な諸外国においても、積極的な体制強化を実施
- 2020年東京オリンピック・パラリンピックに向けた対策の強化が必要

2　サイバーセキュリティ基本法の制定



3　我が国の推進体制の機能強化に向けた取組

（1）情報セキュリティ政策会議の担ってきた機能は、サイバーセキュリティ戦略本部が担うこととなる。

（2）内閣官房情報セキュリティセンター（NISC）を以下の組織に法制化（内閣官房組織令）する。

内閣サイバーセキュリティセンター（注）

- 内閣サイバーセキュリティセンターの所掌事務
  - ①GSOCに関する事務
  - ②原因究明調査に関する事務
  - ③監査等に関する事務
  - ④サイバーセキュリティに関する企画・立案、総合調整
- センター長には、内閣官房副長官補をもって充てる

（3）今後、戦略本部の事務の稼働状況、オリンピック・パラリンピック東京大会開催に向けた準備、サイバー空間における脅威の増大等の諸情勢を踏まえつつ、法制の追加的な整備等について引き続き検討。

（注）英名称：National center of Incident readiness and Strategy for Cybersecurity

内閣サイバーセキュリティセンター発足（2015年1月9日）

サイバーセキュリティ戦略本部（2015年2月9日）

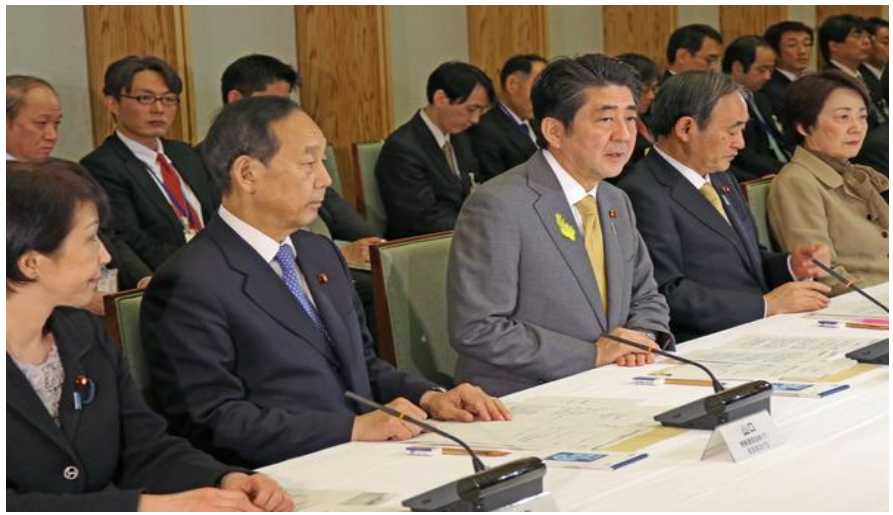
安倍総理

●サイバー空間は、経済成長やイノベーションを推進するために必要な場。サイバーセキュリティは**成長戦略を実現するためにも必要不可欠**な基盤。

●他方、サイバー空間における脅威はますます深刻化。サイバー攻撃への対応は、まさに**国家の安全保障・危機管理上の重要な課題**。

●**サイバーセキュリティ戦略本部は、名実ともに、我が国のサイバーセキュリティ分野の司令塔**となるべき存在。まずは、**サイバーセキュリティ施策の基本的方針について、新たな「サイバーセキュリティ戦略を策定**。

●**オリンピック・パラリンピック東京大会の成功にはサイバーセキュリティの確保が必要不可欠**。こうした点も見据え、我が国のサイバーセキュリティに万全を期して参りたい。



新・サイバーセキュリティ戦略の策定に向けて

○今後の重要な環境変化
- オリンピック・パラリンピック東京大会
- マイナンバー利用開始
- IoTの広がり　等
  （スマートメーター、自動走行システム等）

試行錯誤	DoS攻撃、コンピュータウイルス対策	リスクゼロ社会	「事故前提社会」でのリスクベース対策	国家安全保障・危機管理としてのサイバーセキュリティ	高度なサイバー脅威に対し、積極的な対処が求められる時代に

情報セキュリティ・サイバーセキュリティ

- 第１次 情報セキュリティ基本計画（2006.2.2）情報セキュリティ政策会議決定
- 第２次 情報セキュリティ基本計画（2009.2.3）情報セキュリティ政策会議決定
- 国民を守る情報セキュリティ戦略（2010.5.11）情報セキュリティ政策会議決定
- サイバーセキュリティ戦略（2013.6.10）情報セキュリティ政策会議決定
- サイバーセキュリティ基本法公布（2014.11.12）
- **新・サイバーセキュリティ戦略**（2015.X.XX）サイバーセキュリティ戦略本部決定 閣議決定

IT利活用

- e-Japan戦略（2001.1）
- e-Japan戦略Ⅱ（2003.7）
- IT新改革戦略（2006.1）
- i-Japan戦略2015（2009.7）
- 新たな情報通信技術戦略（2010.5）
- 世界最先端ＩＴ国家創造宣言（2013.6.14 IT総合戦略本部決定・閣議決定, 2014.6.24 改訂）

サイバーセキュリティ立国」の実現が急務

安全保障

- 国家安全保障戦略（2013.12.17 閣議決定）

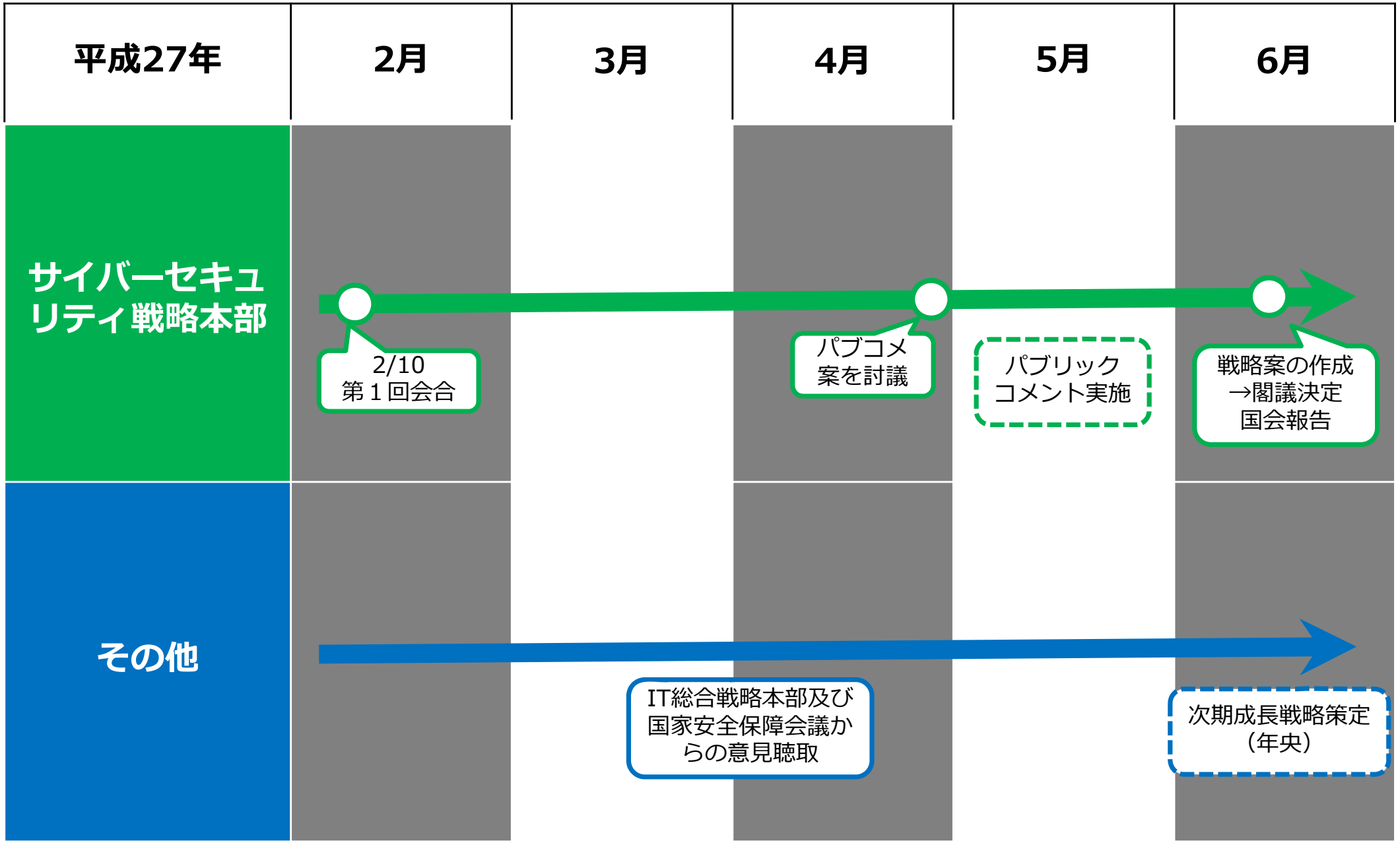
サイバー空間の防護は、我が国の安全保障を万全とするとの観点から、不可欠

成長戦略

- 日本再興戦略（2013.6.10 閣議決定, 2014.6.24　改訂）

「サイバーセキュリティ推進体制等の強化」が項目の一つ

新・サイバーセキュリティ戦略の策定スケジュール（案）



新・サイバーセキュリティ戦略における主な検討課題（例）

【全般的事項】

・今後、「サイバー空間」はどのような性質の空間として発展していくと考えるか。

・サイバー空間における多様な主体間の役割分担をどのように考えていくべきか。

・サイバーセキュリティ政策を推進する上で、我が国はどのような基本原則に基づくべきか。

【政策分野別事項】

・サイバー空間を通じて我が国の経済・社会の持続的な発展を実現するためには、サイバーセキュリティが果たす役割や必要とされる政策をどのように考えるか。

・国民が、サイバー空間上で安全に、安心して豊かな経済社会活動を行うためにはどのような対策が必要か。

・サイバー空間に係る我が国の安全保障を確保し、国際社会の平和に貢献するためには、どのような政策を追求すべきか。

【基盤的事項】

・社会全体のセキュリティ意識を高め、更にその能力を高めるためには、どのような取組が考えられるか。

・日本におけるセキュリティ人材を充実させるためには、どのような政策を推進すべきか。

・社会や技術が変化していく中、サイバーセキュリティに関する研究開発等はどのようなあり方が適切か。

重大インシデントに係る原因究明等のプロセス

～重大事象施策評価規則（2015年2月、サイバーセキュリティ戦略本部決定）～

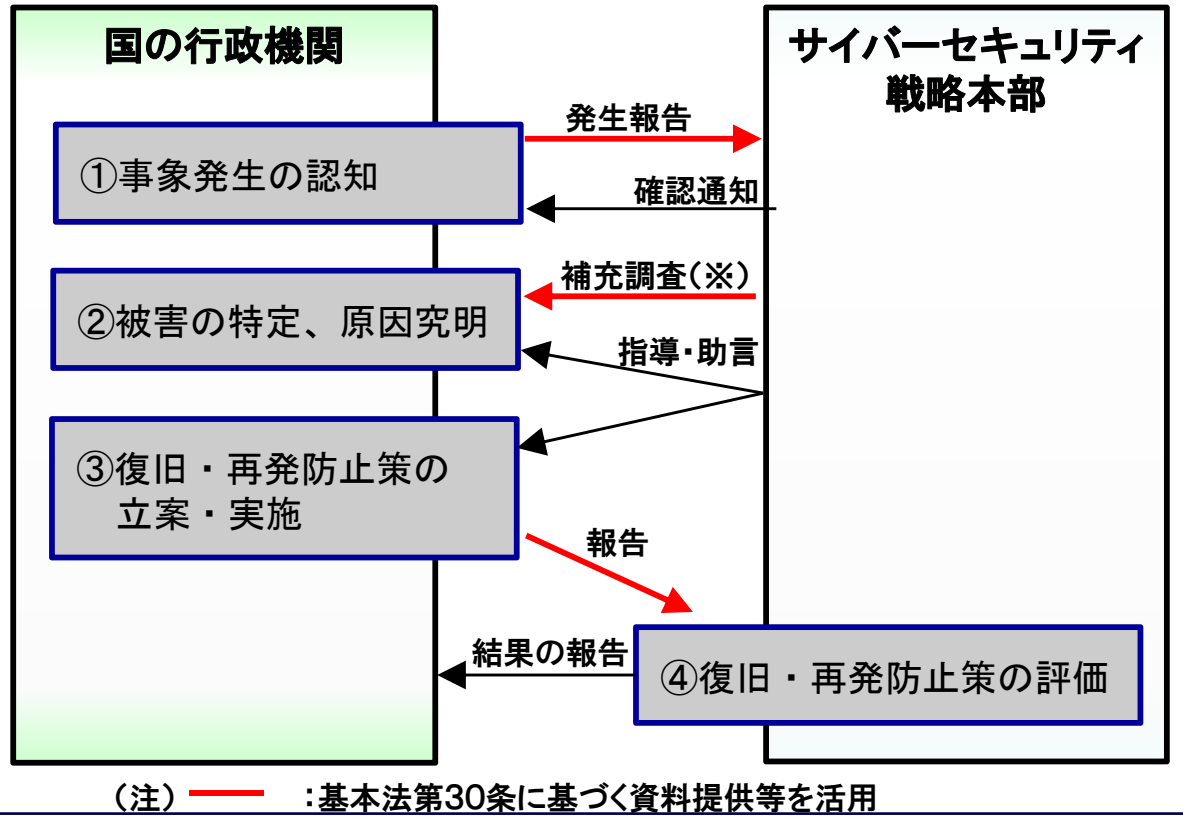
対象とする事象（特定重大事象）

1. 国の行政機関が運用する情報システムにおける障害を伴う事象であって、行政事務の遂行に著しい支障を及ぼす（おそれがある）もの

2. 情報の漏えいを伴う事象であって、国民生活又は社会経済に重大な影響を与える（おそれがある）もの

3. 我が国のサイバーセキュリティに対する国内外の信用を著しく失墜させる（おそれがある）事象（例：我が国の行政機関のサーバー等が、他国へのサイバー攻撃の踏み台とされるケース）

事務処理の概要



（注）——　：基本法第30条に基づく資料提供等を活用

（※） デジタルデータの保全・分析といったフォレンジック調査。

補足事項

- 関係行政機関と本部は、緊密な連携を図るとともに、秘密保持に留意する。
- 本部は、評価等を踏まえ、必要に応じて勧告や政府機関統一基準群の改定等知見のフィードバックを行う。
- 迅速・柔軟な対応のため、上記の本部事務（原則として④の評価を除く）は、内閣サイバーセキュリティセンターにおいて処理。

サイバーセキュリティ戦略本部による監査の実施

目的：国の行政機関におけるサイバーセキュリティ対策の強化を図ること

サイバーセキュリティ戦略本部

事務委任

報告等

NISC

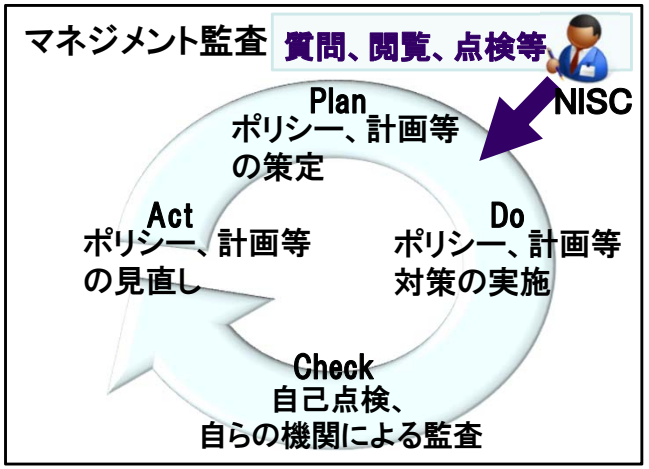
①②の二本立てで監査を実施

①セキュリティ向上のための体制・制度が機能しているかの検証による評価（監査）（以下「マネジメント監査」という。）

統一基準群に基づく施策の取組状況について、主に組織全体としての**対策強化を続ける仕組みが有効に機能しているかどうかの観点**から関係者への質問、資料の閲覧、情報システムの点検等により**検証**し、**改善のための必要な助言等を行う**。

マネジメント監査の着眼点

P（計画立案）、D（実行）、C（点検）、A（見直し）の実施状況を確認するとともに、セキュリティ対策のための体制等についても確認



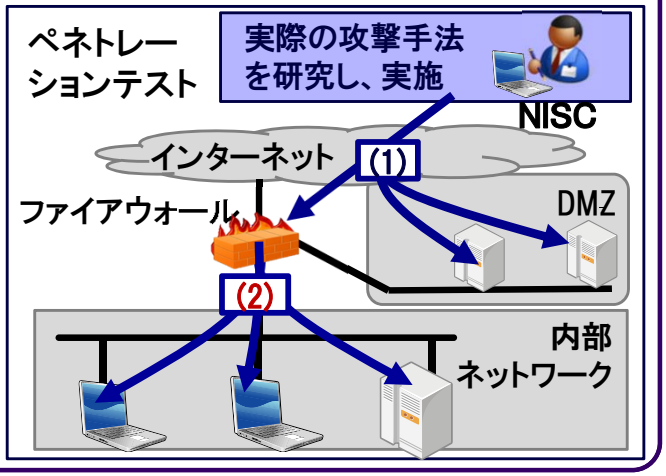
②情報システムに対する疑似的攻撃による評価（監査）（以下「ペネトレーションテスト」という。）

情報システムに対して、攻撃者が用いる手法で**実際に侵入できるかどうかの観点**から防御策の状況を**検証**し、**改善のための必要な助言等を行う**。

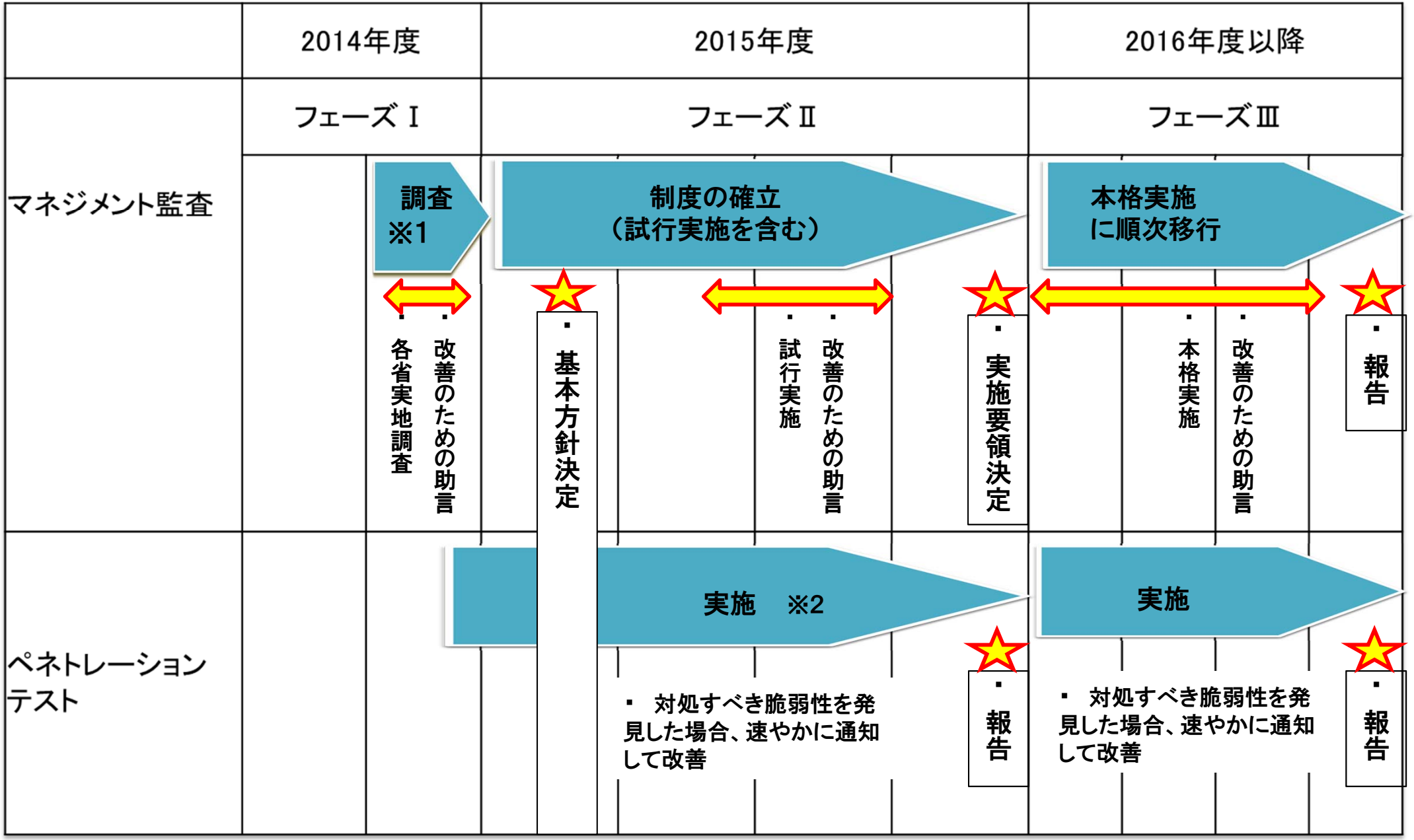
ペネトレーションテストの着眼点

(1)インターネット経由での不正アクセスを想定し、問題点の有無を検証

(2)インターネットとの境界を突破できた場合、内部ネットワークについても、問題点の有無を検証



監査実施に向けたスケジュール



※1　サイバーセキュリティ基本法の施行により、基本方針決定に向け各機関の施策の取組状況についてヒアリング等の実地調査等を実施。

※2　平成26年度補正予算及び平成27年度予算（予定）により実施。

米サイバーセキュリティ対策強化関連法(2014年12月)

■Federal Information Security Modernization Act 2014
- 2002年制定のFISMA法(各省にITシステムセキュリティの年次監査・報告を義務付け)の強化
- DHSに政府機関のサイバーセキュリティ対策(軍・インテリジェンスコミュニティ関連を除く)の監督権限を付与。

■National Cybersecurity Protection Act of 2014
- DHSのNCCIC(国家サイバーセキュリティ・通信統合センター)を常設(法的権限の付与)
- NCCICにおいてサイバー脅威に関する官民情報を共有。

■Cybersecurity Workforce Assessment Act of 2014
- DHSにおいて省内のサイバーセキュリティ人材の能力評価(3年ごと)を義務付け。同評価を基に人材強化。

■The Border Patrol Agent Pay Reform Act of 2014
- DHSにおけるサイバーセキュリティ人材に係る給与水準等の設定権限を付与。

■Cybersecurity Enhancement Act of 2014
- NIST(国立標準技術研究所)について、産業界主導のセキュリティ対策等の促進・支援を行う組織として位置づけ。
- OSTP(大統領府科学技術政策局)について、連邦政府のサイバーセキュリティ研究開発計画の策定・改定する組織として位置づけ。

米国サイバーセキュリティ対策強化(2015年1月13日)

オバマ米大統領演説@国土安全保障省
☞サイバーセキュリティに関する立法提案


(Source)White House HP

✔**情報共有の促進**
- ・官民・民間部門内での情報共有の促進
- ・民間主導の情報共有・分析機関の組織化の推進
- ・情報共有に際してのプライバシーに係る制限の義務付け

■民間部門の情報共有分析組織（ISAOｓ：Information Sharing and Analysis Organizations)の設立促進。
■ISAOｓ設立促進のため、情報共有の在り方等の運用に関する任意基準策定のためのNPO組織創設を支援。
■DHS内のNCCICとISAOｓの連携強化。 等

(注)Executive Order on Promoting Private Sector Cybersecurity Information Sharing (Feb 13, 2015)

■国家情報長官の下に新たにサイバー脅威情報統合センター（CTIIC：Cyber Threat Information Integration Center)を設置。
■CTIICはサイバー脅威に関するインテリジェンス情報の分析・統合機能を持つ。

(注)モナコ大統領補佐官(国土安全保障及びテロ対策担当)(2015年2月10日)

✔**サイバー犯罪に取り組む法執行機関の近代化**
- ・ボットネットの売買に対する訴追の可能化
- ・窃取された米国民の金融情報の海外への売買の処罰化
- ・スパイウェアの売買を防止するための法執行機関の権限の拡大

✔**情報漏えいに関する報告**
- ・顧客データ漏えいに関する企業の顧客に対する報告義務の連邦法への統一(現在46の州法)

内閣サイバーセキュリティセンター

National center of Incident readiness and Strategy for Cybersecurity