



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

我が国における サイバーセキュリティ戦略について

内閣官房 内閣サイバーセキュリティセンター(NISC)

重要インフラグループ 柳島 智

平成28年1月15日

自己紹介

- 1991年 郵政省(現総務省)入省 データ通信課配属
インターネットの商用化に関する検討会 → 1992年に我が国初のISP登場
- 1999年 放送技術政策課
地デジ用及び、アナログ周波数変更対策用の周波数使用計画策定(2001年)
- 2003年 地上放送課受信対策室
アナログ周波数変更対策実行(470万世帯、1800億円)
→ 2003年12月地デジ放送開始、2012年3月アナログ放送終了
- 2007年 データ通信課
IPv6対応、電気通信事業者のエコロジー対応、ICANN、セキュリティ
- 2009年 国際協力課国際展開支援室
地デジ日本方式のアフリカ展開
- 2012年 電波部監視管理室
不法電波の監視
- 2013年 電波部重要無線室
国や地方自治体の無線局免許(デジタル化による電波の有効利用促進)
- 2015年 内閣サイバーセキュリティセンター参事官 重要インフラ担当

目次

- サイバー攻撃の現状
- サイバーセキュリティの推進体制（基本法とNISC）
- サイバーセキュリティ戦略
- 重要インフラに関する施策（第3次行動計画）
- 政府機関、国民への対応
- サイバーセキュリティの将来について考える

• サイバー攻撃の現状

現状を踏まえ、ネットワーク利用者はどう対応すべきか？

- ネットワークの分離 ⇔ 利便性
- ヒューマンエラーを回避するシステム
- 事案への対応体制

国内のサイバーインシデント事例（2015年6月～12月、報道ベース）

➤日本年金機構(6/1)

標的型メールによるウイルス感染により、年金情報125万件が流出

➤富山大学(6/7)

サーバが不正アクセスを受け海外への攻撃の踏み台に

➤石油連盟(6/9)

標的型メール攻撃による情報流出

➤国立情報学研究所(6/9)

サーバが不正アクセスを受け海外への攻撃の踏み台に

➤東京商工会議所(6/10)

標的型メール攻撃による個人情報流出

➤健康保険組合連合会など(6/13)

PCがウイルス感染。情報流出は確認されず

➤独立行政法人国際協力機構(6/16)

標的型メールによるウイルス感染。情報流出は確認されず

➤一般財団法人海外産業人材育成協会(6/17)

標的型攻撃によりウイルス感染

➤中間貯蔵・環境安全事業株式会社(6/17)

サーバに不審なアクセス。情報流出は確認されず

➤全国健康保険協会(6/18)

PCが不審な通信。情報流出は確認されず

➤香川県(6/18)

不正アクセスでメールマガジン登録者3,250名が削除

➤新潟県(6/19)

水飲み場型でのウイルス感染。情報流出は確認されず

➤香川大学附属病院など(6/19)

PCがウイルス感染。情報流出は確認されず

➤五島市(6/21)

Webサイトが改ざんされ、一時閉鎖

➤早稲田大学(6/22)

標的型メール攻撃により個人情報3,300人分が流出

➤徳島大学(6/23)

電子会議システムが不正アクセスされ、踏み台に利用

➤法務省(6/26)

PCが不審な通信、ウイルスに感染した疑い

➤阪神高速道路株式会社(7/4)

Webサイトに不正アクセスを確認し公開を一時中止

➤ホテルグランドヒル市ヶ谷(7/7)

PCがウイルス感染。情報流出をしたおそれ

➤環境省(7/11)

PCがウイルス感染。情報流出は確認されず

➤セブン銀行(7/14)

DDoS攻撃によりインターネットバンキングが利用不可

➤愛媛大・福岡大など(7/14)

攻撃によりメールマガジンの管理アカウント等が流出

➤東京大学(7/16)

標的型メール攻撃により氏名等3.6万件が流出

➤厚生労働省（ハローワーク）(7/18)

事務用PCがウイルス感染。情報流出は確認されず

➤東京都(7/21)

水飲み場攻撃によりウイルス感染。流出は確認されず

➤内閣府(8/4)

メールの管理アカウントが乗っ取られ2万件を送信

➤科学技術振興機構(8/8)

PCがウイルス感染。情報流出のおそれ

➤国土交通省（琵琶湖河川事務所）(8/11)

Webサイトに脆弱性が見つかり、サイトを一時閉鎖

➤関西広域連合(8/18)

Webサイトが改ざん。情報流出は確認されず

➤千趣会(9/15)

不正アクセスで個人情報約13万人分が流出おそれ

➤日本政府観光局、成田国際空港など(10/10)

DDoS攻撃によりWebサイトが閲覧できない状態

➤毎日新聞社(11/4)

DDoS攻撃によりWebサイトが閲覧しにくい状態

➤東京オリンピック・パラリンピック組織委(11/6)

DDoS攻撃によりWebサイトが閲覧できない状態

➤日本経済新聞社(11/12)

DDoS攻撃によりWebサイトが閲覧しにくい状態

➤東京ガス オートサービス(11/14)

不正アクセスにより、顧客情報4,400人分が流出おそれ

➤厚生労働省(11/24)

DDoS攻撃によりWebサイトが閲覧できない状態

➤三菱東京UFJ銀行(12/1)

特定口座に振り込んだ利用者の電話番号が流出

➤町田市(12/8)

PCがランサムウェアに感染。他への影響はなし

➤太地町(12/17)

DDoS攻撃によりWebサイトが閲覧しにくい状態

【凡例】 赤字・・・政府関係機関 青字・・・地方公共団体
日付はいずれも関連報道のあった日

【海外の主要事例】

➤米国 人事管理局(6/5)

攻撃を受け、政府職員や元職員の個人情報約400万人分が流出→後日2,150万人分が流出と修正。身辺調査面談記録なども

➤イタリア ハッキングチーム社(7/8)

攻撃を受け脆弱性情報や取引情報等が流出

海外のサイバー攻撃事案（2014年8月以降、報道ベース）

○ JPモルガン・チェース（2014年8月中旬）

2014年8月、サイバー攻撃が行われ、顧客の名前、住所、電話番号、電子メールアドレス及びユーザー関連の内部情報が流出したことが明らかとなった。サイバー攻撃は、ウクライナをめぐる西側諸国によるロシアへの金融制裁に対する報復としてロシア政府の関与した可能性もあるとのFBI捜査官の見解もある。

○ ソニー・ピクチャーズ・エンターテインメント（2014年11月下旬）

2014年11月、「平和の守護者（Guardians of Peace）」を名乗る組織が、システムに侵入し、同社の数千に及ぶ社内文書や未公開の4作品を含む5作品の同社映画全編の違法コピーがオンライン上に流出。米国政府は、12月19日、当該サイバー攻撃を北朝鮮政府による犯行とし、翌月2日、大統領令を発出し追加的な経済制裁を実施。

○ 保険会社アンセム（2015年2月上旬）

2015年2月、同社に対するサイバー攻撃により、8,000万人分に及ぶ新旧加入者や従業員の個人情報が盗まれた。氏名、生年月日、加入者ID、社会保障番号、住所、電話番号、電子メールアドレス、勤務先情報が漏えいしたが、クレジットカードや医療記録などの情報は流出した形跡はないとしている。なお、攻撃者は米国人事管理局（OPM）（後述）へのサイバー攻撃を行った中国人民解放軍ハッカー部隊であるとの可能性も指摘されている。

○ イラン石油省（2015年3月下旬）

本年5月26日、イラン国营放送は、イラン石油省が同年3月21日から24日の4日間の休日に米国によるサイバー攻撃を受けており、これを撃退したとの発表を報じた。イラン政府は米国政府に対して書簡を送付するとともに、国際司法命令を準備中であるとしている。なお、イラン政府高官は、本年2月イランの科学施設や工業施設に対して複数回のサイバー攻撃が行われていることを明らかにしている。

○ フランスTV5モンド（2015年4月上旬）

2015年4月8～9日、フランス国营テレビTV5モンドは、イスラム国に所属すると主張するグループ「Cybercalophate」によってTVチャンネル、Web、FaceBookが乗っ取られ、イスラム国の犯行を主張するメッセージが表示されていた。4月10日、フランス国防省は、調査の結果、軍の機密情報が漏えいすることはなかったと発表した。

○ ドイツ連邦議会議会（2015年5月上旬）

2015年5月15日、ドイツ連邦議会（下院）のサーバにサイバー攻撃を受け、約2万台のパソコンが外部から自由に操作できる状態となった。メルケル首相の下院事務局のパソコンも感染。情報機関のトップは、手法が極めて巧妙であることからロシアの関与を示唆している。少なくとも5人の議員のパソコンからデータ流出が確認されており、それ以外の情報も流出するおそれがあるとしている。

○ イラン核問題6か国協議会場（2015年5月中旬）

2015年5月12日、スイス当局はイランの核問題をめぐる6か国協議がジュネーブのホテルで行われた際、サイバー攻撃が行われた可能性があり、それに関連するホテルの家宅捜査及びITシステムやソフトウェアの差し押さえを行ったと報道されている。イスラエルの関与が疑われているが、イスラエルは根拠のないものであると否定している。

○ 米国人事管理局（2015年6月上旬）

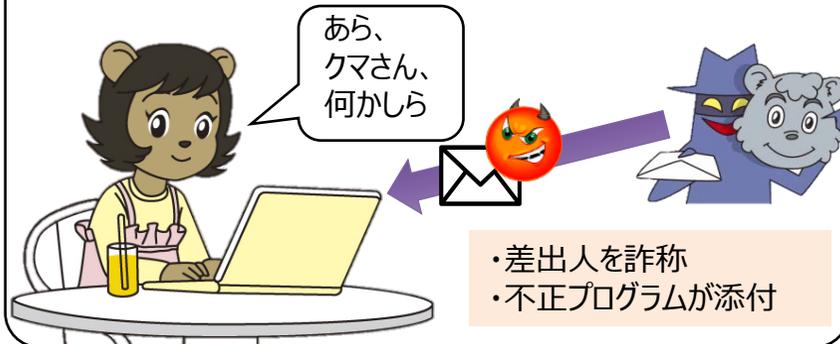
2015年6月4日、米国人事管理局は、システムが侵入され、400万件の職員及び元職員の個人情報が流出したと発表。さらに、7月9日には、2150万人の情報が盗まれていたことを明らかにした専門家の見解では、中国人民解放軍のハッカー部隊である「ディープ・パンダ」と呼ばれる組織が今回の攻撃及び保険会社アンセムへの攻撃を実施したとされている。

様々な標的型攻撃

- 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
- 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

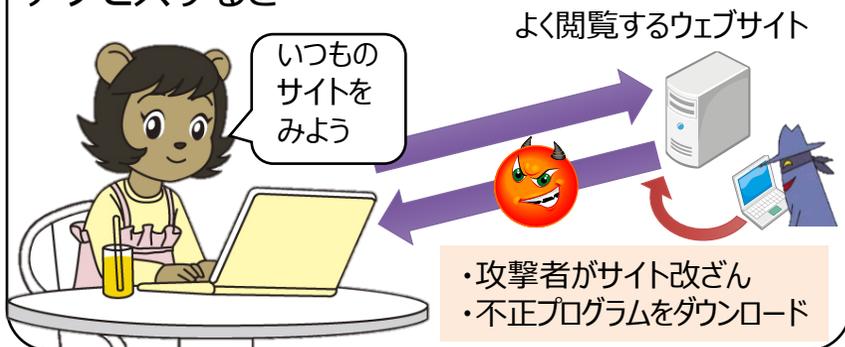
A. メール

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・・・



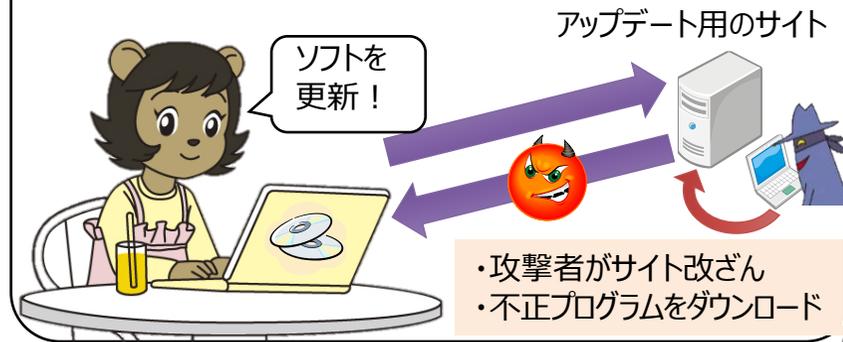
B. ウェブ閲覧（水飲み場型）

いつも閲覧しているウェブサイト
にアクセスすると・・・



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・・・

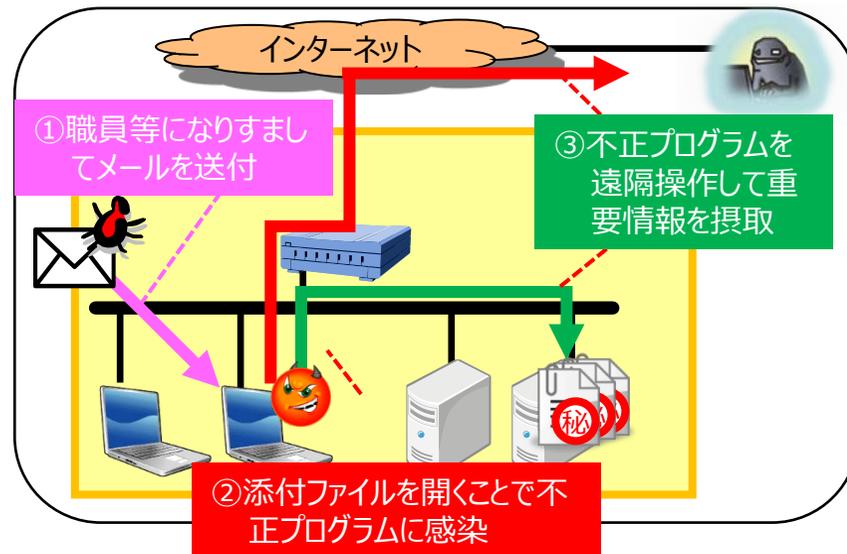


最近の脅威 ① 標的型メール攻撃

脅威の概要

- 特定の組織を狙って職員等になりすましたメールを送付し、添付ファイルやURLを開かせることによって不正プログラムに感染させる。
- 不正プログラムを遠隔操作して内部侵入を繰り返し、重要情報の窃取・破壊等を実施。

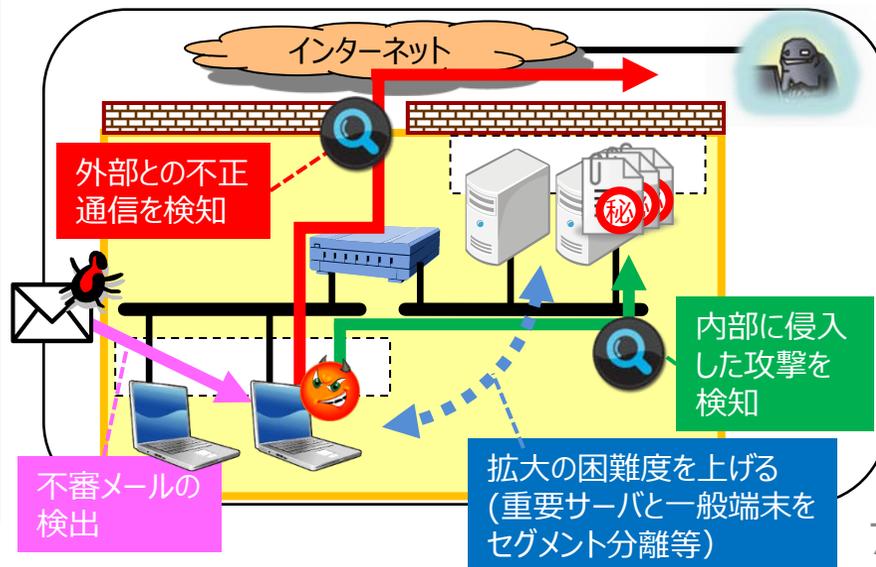
標的型メール攻撃のイメージ



主な対策

- 不審なメールを検出する仕組みの整備、対応能力を向上する（SPFの検証、教育・訓練、等）。
- 感染防止を目的とした入口対策のほか、遠隔操作による攻撃の早期検知等を目的とした内部対策を実施する。

対策の概要(例)



最近の脅威 ②水飲み場型攻撃

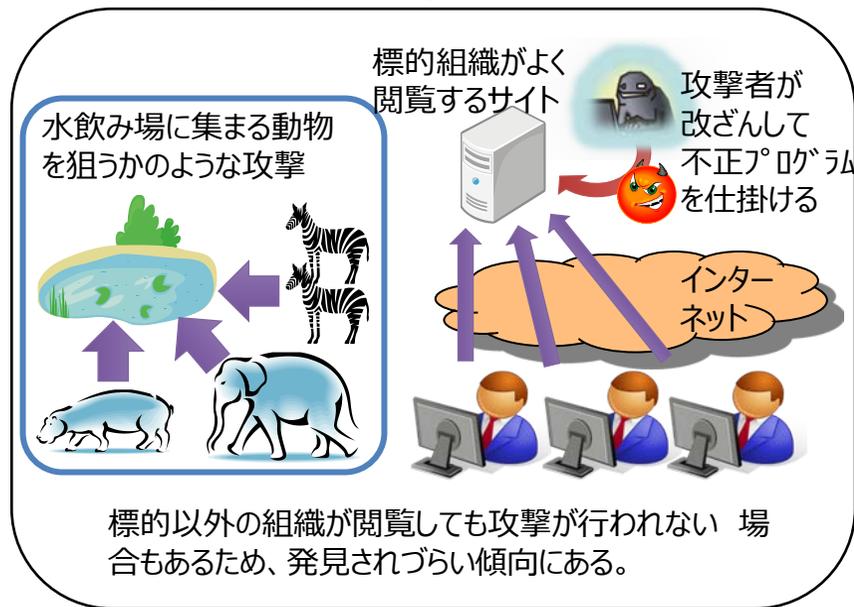
脅威の概要

- 標的組織がよく閲覧するWebサイトを改ざんし、閲覧した端末を不正プログラムに感染させる。
- ブラウザの未知の脆弱性を悪用した攻撃（ゼロデイ攻撃）の場合もあり、未然防止は困難。
- 不正プログラムを遠隔操作して内部侵入を繰り返し、重要情報の窃取・破壊等を実施。

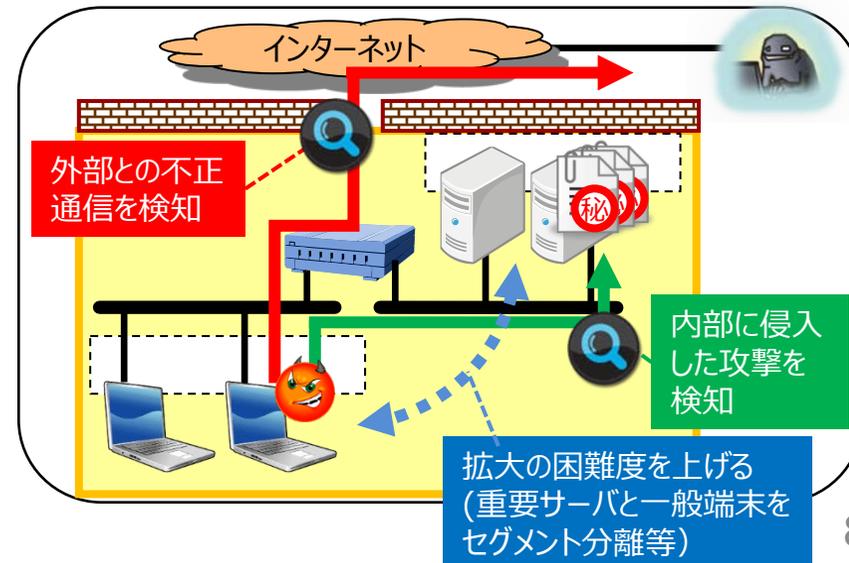
主な対策

- 感染の未然防止は困難であるため、組織内部へ侵入されることを前提に内部対策を実施。
- 内部対策としては、以下が挙げられる。
 - 内部に侵入した攻撃を早期検知して対処
 - 侵入範囲の拡大の困難度を上げる
 - 外部との不正通信を検知して対処

水飲み場型攻撃（イメージ）



対策の概要(例)

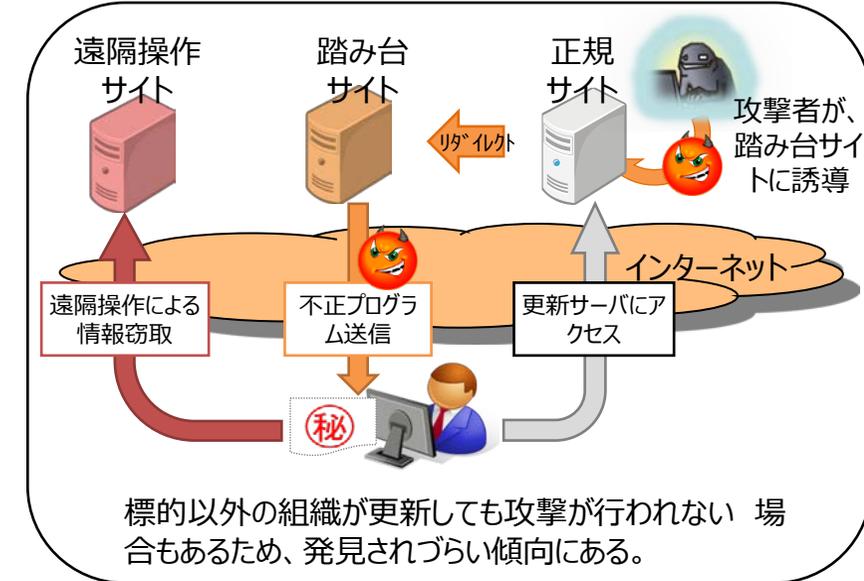


最近の脅威 ③ソフトウェアの更新プログラムを悪用した攻撃

脅威の概要

- 広く利用されているソフトウェアの正規サイトを改ざんし、ソフトウェアの更新を行った端末を不正プログラムに感染させる。
- 不正プログラムを遠隔操作して内部侵入を繰り返し、重要情報の窃取・破壊等を実施。

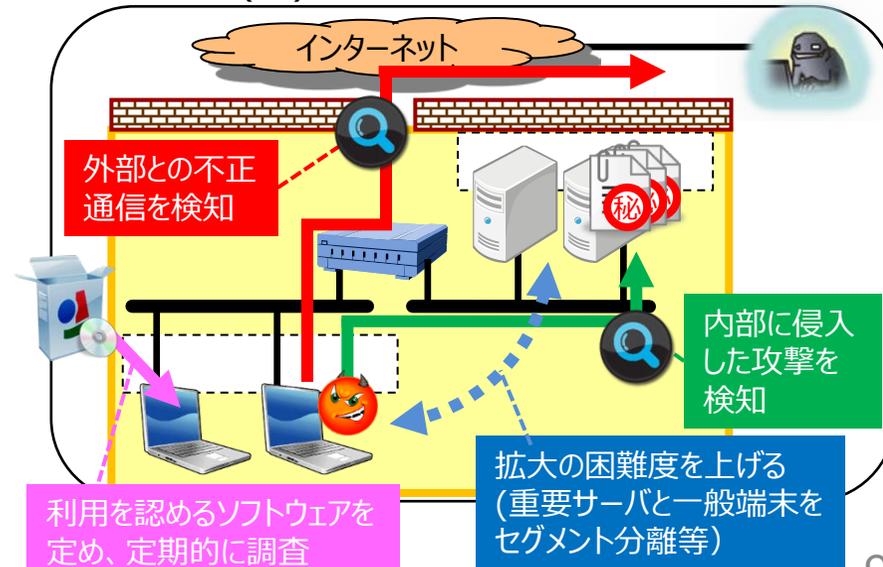
ソフトウェアの更新プログラムを悪用した攻撃（イメージ）



必要な対策

- 端末で利用を認めるソフトウェアを定め、利用されているソフトウェアの状態を定期的に調査する。
- 感染防止を目的とした入口対策のほか、遠隔操作による攻撃の早期検知等を目的とした内部対策を実施する。

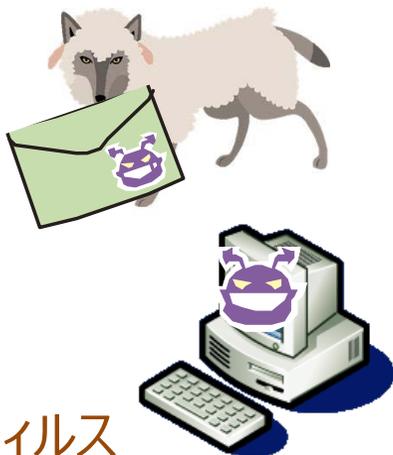
対策の概要(例)



標的型メール攻撃の攻撃プロセス

時間をかけて執拗に狙う！

① 初期潜入

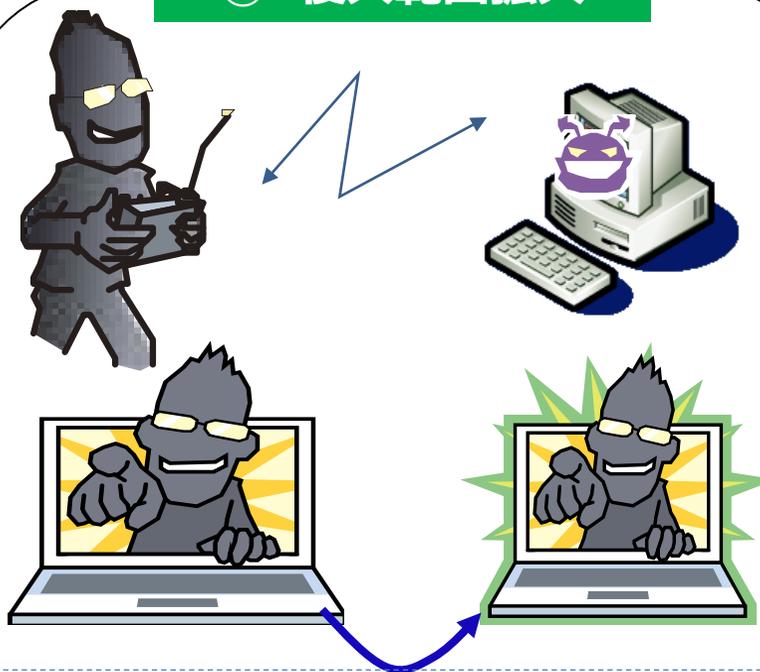


ウィルス
対策ソフトが
検知しない！

最初はメールの
添付ファイルや
リンクを開くだけ

外部（インターネット）

② 侵入範囲拡大



遠隔操作により、
システムの内部に侵入し、
乗っ取りを拡大

組織内ネットワーク

③ 情報窃取



重要情報の窃取や
システム破壊も



標的型攻撃メールの例

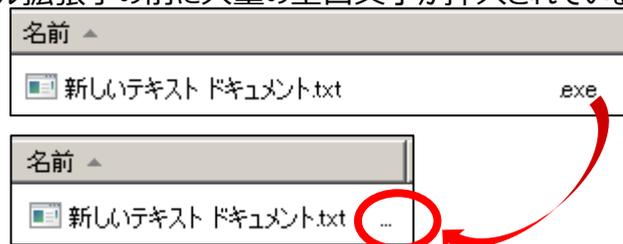
メールのテーマ

- 知らない人からのメールだが、メール本文のURLや添付ファイルを開かざるを得ない内容
 - ✓ 新聞社や出版社からの取材申込や講演依頼
 - ✓ 就職活動に関する問い合わせや履歴書送付
 - ✓ 製品やサービスに関する問い合わせ、クレーム
 - ✓ アンケート調査
- 心当たりのないメールだが、興味をそそられる内容
 - ✓ 議事録、演説原稿などの内部文書送付
 - ✓ VIP 訪問に関する情報
- これまで届いたことがない公的機関からのお知らせ
 - ✓ 情報セキュリティに関する注意喚起
 - ✓ インフルエンザ等の感染症流行情報
 - ✓ 災害情報
- 組織全体への案内
 - ✓ 人事情報
 - ✓ 新年度の事業方針
 - ✓ 資料の再送、差替え
- 心当たりのない、決裁や配送通知 (英文の場合が多い)
 - ✓ 航空券の予約確認
 - ✓ 荷物の配達通知
- IDやパスワードなどの入力を要求するメール
 - ✓ メールボックスの容量オーバーの警告
 - ✓ 銀行からの登録情報確認

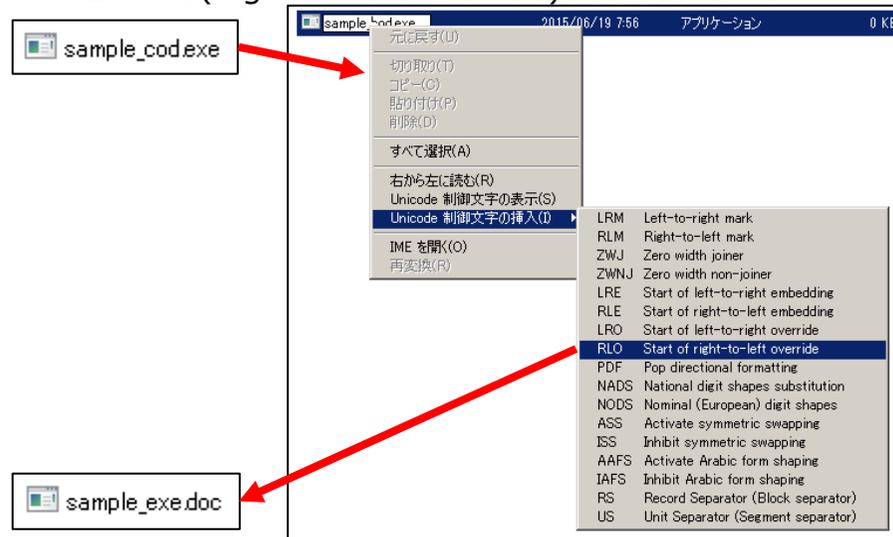
出典: IPA テクニカルウォッチ「標的型攻撃メールの例と見分け方」より

添付ファイルなど

- アイコンが偽装されている
 - ✓ 実行形式ファイルなのに文書ファイルやフォルダのアイコンとなっている
- ファイル拡張子が偽装されている
 - ✓ 二重拡張子となっている
 - ✓ ファイル拡張子の前に大量の空白文字が挿入されている



- ✓ ファイル名にRLO(Right to Left Override)が使用されている



- 表示されているURL (アンカーテキスト) と実際のリンク先のURLが異なる (HTMLメールの場合)

標的型攻撃でのマルウェアがなぜ防ぎにくいのか

非対称性

- 防御側は全てをどんな時でも完全に防ぐ必要 ←→ 攻撃者はいつかどこかで穴を見つけられればよい

アンチウイルスソフトで検知できない

- マルウェア作成や難読化を容易にするソフトウェア → 亜種増大によるパターンマッチの限界（全部は無理）
- 攻撃者は遠隔操作で最新版にアップデート可能 → 複数を常に侵入させ1つでも残っていれば勝利
- 攻撃者は既存のアンチウイルスソフトで検知できないことを確認してから使用

ゼロデイ脆弱性が狙われる

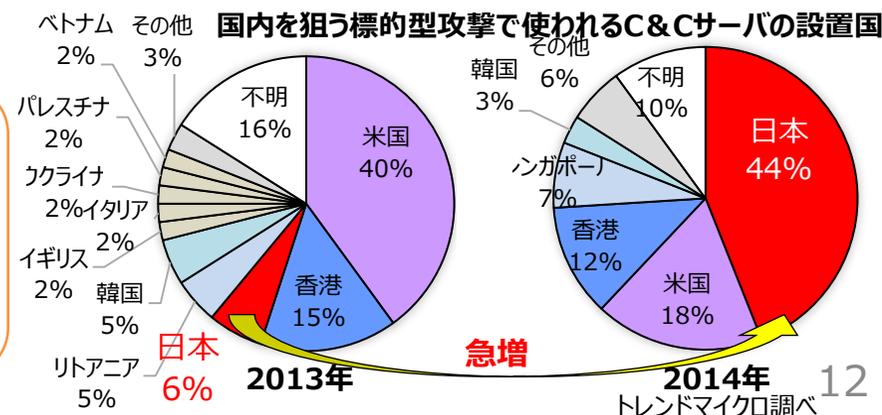
- 闇市場でゼロデイ脆弱性が取引 → バグ発見はよいお金（バグ発見報酬制度の進展が必要。。。）
- 攻撃側の体制変化；単独愉快犯から組織的・経済的行動 → 高い技術力と資金力
- パッチ公開後も短時間(数時間～数日)でマルウェア作成 → 企業のパッチ当ては、検証に数日～数週間

カスタマイズされた攻撃

- 対象を研究してから攻撃 → メールやりとりを把握して返信メールにマルウェアを仕込む等
- 特定業界しか見えないようなWebサイトが改ざんされ、特定IPだけにマルウェア埋め込み → 発見されにくい

正常に見せかけた通信や挙動による検知逃れ

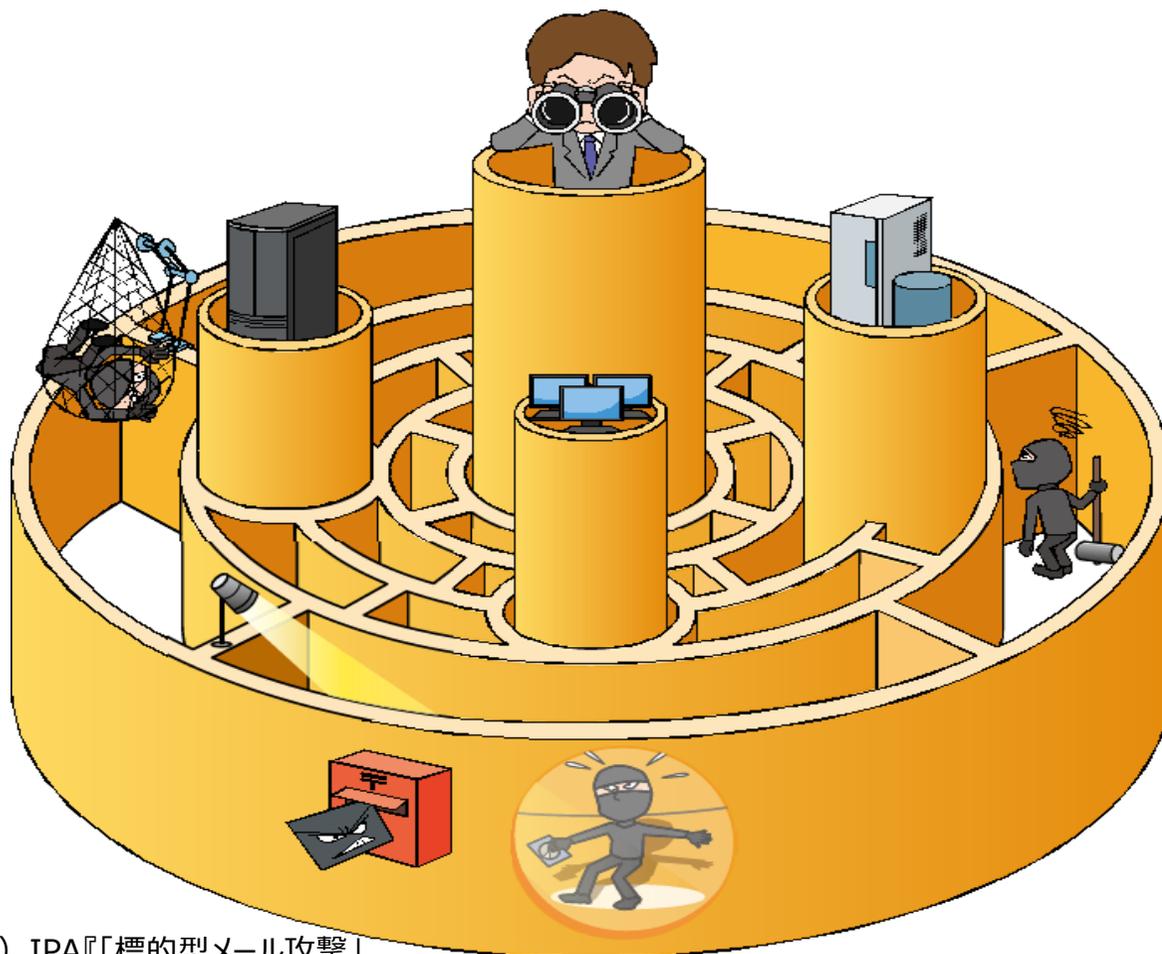
- 通常通信に紛れて遠隔操作 → http(80番)やSSL(443番)
- 攻撃指令(C&C)サーバは国内が主流 → .jpも安心できない
- OS標準コマンドを使用して感染拡大
- 解析環境（サンドボックス等）では反応しないよう細工
- メモリのみ存在するプログラム、自身が残したログの消去



多重防御を備えたシステム構築が重要

- 侵入を100%防ぎ続けることは困難。侵入されても被害を抑える対策実施が重要。
- 単独の対策に頼らない多重防御を備えたシステム構築が重要。

■ 多重防御を備えたシステムのイメージ



重要なものを重点的に守る

第2、第3の壁を作って
攻撃を拡げにくくする

侵入されていないか見張る

インシデント対応体制の整備～意義

- ITシステムの複雑化 →原因特定や復旧がより困難に／IT部門と利用部門の乖離
- ITシステムの汎用化 →被害が広範囲かつ短期に拡大しやすい
- 攻撃の高度化・複雑化 →対策・対応に高い専門性が必要で部門ごとの確保が困難



組織的な対応が必要

求められる機能とは、

組織内の情報共有及び連携

- ✓ インシデント報告を集める窓口の一本化
- ✓ 組織内のインシデントの一元管理と部署間調整

外部組織との調整

- ✓ 外部に起因するインシデント（DDoS、高度サイバー攻撃(APT:Advanced Persistent Threat)による攻撃など）を解決するため、他組織に対する適切な依頼
- ✓ 外部からのインシデント関連情報を受け取る窓口の一本化
- ✓ 組織間連携しなければならないインシデント対応のため、外部組織との強い信頼関係構築

インシデント発生後に、その対応方法を考え始め対応体制をとるのは、被害を拡大させる一因となる

→できるだけ**事前にインシデント対応計画を策定し、対応体制等を整えておく**必要

インシデント対応体制の整備～有用性

組織内CSIRTについて

- ✓ **C**omputer **S**ecurity **I**ncident **R**esponse **T**eam の略、「シーサート」と発音される
- ✓ 組織内でコンピュータセキュリティインシデント対応に関する業務を専門に担当するチーム
- ✓ 組織によっては、他の関連業務と兼務することによって、組織内にCSIRT の機能を実装している場合もある

組織の内部に対する主な機能

- ✓ 組織内で発生したインシデントの報告を受けるための、一本化された窓口を提供する
- ✓ 発生したインシデントに対応する、または、発生したインシデントへの対応に必要な技術的支援やノウハウを提供する
- ✓ インシデント対応における組織としての意思決定を支援する
- ✓ 組織横断的に発生するインシデントにおいて、組織内の調整役として活動する
- ✓ 組織の情報システム管理者、ユーザ、その他の従業員に対し、セキュリティ教育と意識啓発を行う

組織の外部に対する主な機能

- ✓ 外部のインシデント対応組織との連絡調整を行う
- ✓ セキュリティインシデントの事例や動向、インシデント対応手法や技術に関する情報を外部から収集し、組織内に展開する
- ✓ 従業員・メディア・国民へ適切な情報を提供する

日本年金機構における個人情報流出事案：事案概要

- 平成27年5月8日から20日にかけて4種類の不審メールが日本年金機構へ送付され、23日までに**31台の端末がマルウェアに感染**し、23件の不審な通信先への通信が発生
- 6月1日、機構は、外部から送付された不審メールに起因する不正アクセスにより、機構が保有している**個人情報の一部（約125万件）が外部に流出**したことが5月28日に判明したとして、報道発表
- 23件中1件の通信先への通信が約125万件の個人情報の流出に関する通信であったことが警察庁からNISCへの情報提供により判明

- サイバーセキュリティ戦略本部が、サイバーセキュリティ基本法第25条第1項第3号に規定された「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。）」に基づき原因究明調査を実施
- 6月1日、NISCに原因究明調査チームを設置
- 8月20日にNISCにて原因究明調査結果を公表
http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf

日本年金機構における個人情報流出事案：事案の状況と本部及びNISCの対応

● 5月8日(金)(検知・通知1)

- NISCは、厚生労働省(以下「厚労省」という。)ネットワークにおいて不審な通信を検知し、厚労省政策統括官付情報政策担当参事官室(以下「情参室」という。)に対してその旨を通知した。
- NISCは、厚労省情参室から不審な通信をした端末を特定し、LANケーブルの抜線を行った旨の連絡を受け、その後、同日中に不審な通信を検知しなくなったことを確認した。(以降、厚労省情参室に対し、随時、助言等を実施。)

● 5月15日(金)(解析結果提供A)

- NISCは、厚労省情参室から5月8日に受信した不審メールⅠに関する不正プログラムを受領後、解析を実施し、同日中に解析結果を厚労省情参室へ提供した。

● 5月19日(火)(解析結果提供B)

- NISCは、厚労省情参室から5月18日に受信した2種類の不審メール(不審メールⅡ、不審メールⅢ)及び不正プログラムを受領後、解析を実施し、同日中に解析結果を厚労省情参室へ提供した。

● 5月21日(木)(解析結果提供C)

- NISCは、厚労省情参室から5月20日に受信した不審メールⅣ及び不正プログラムを受領後、解析を実施し、同日中に解析結果を厚労省情参室へ提供した。

● 5月22日(金)(検知・通知2)

- NISCは、厚労省ネットワークにおいて不審な通信を検知し、厚労省情参室に対してその旨通知した。
- NISCは、厚労省情参室から、機構において、不審な通信をした端末のLANケーブルの抜線を行った旨の連絡を受け、その後、同日中に不審な通信を検知しなくなったことを確認した。

● 5月29日(金)

- NISCは、厚労省から、5月8日以降の経緯について5月19日に機構が警察へ相談したこと及び機構において情報流出が生じた旨の説明を受け、サイバーセキュリティ戦略本部長(官房長官)(以下「本部長」という。)に報告した。
- 本部長は、NISCから報告を受け、即時に「特定重大事象」^{注1}であるとの判断を行った。
- NISCは、厚労省の要請を受けて、厚労省と機構が行う対応を支援するため、CYMAT^{注2}を派遣した。

● 6月1日(月)

- NISCは、客観的・専門的立場から原因究明を実施するため、原因究明調査チームを設置した。
- 本部長は、サイバーセキュリティ基本法第30条第2項の規定に基づき、機構を監督する立場にある厚生労働大臣に対して、厚労省が機構に対して行ってきたサイバーセキュリティに関する監督に関する資料、情報の提供を要請した。
- 内閣官房副長官(事務)を議長とするサイバーセキュリティ対策推進会議を開催し、全府省庁に対して、システム点検と個人情報の適正管理を指示した。

注1：「サイバーセキュリティ戦略本部重大事象施策評価規則」(平成27年2月サイバーセキュリティ戦略本部決定)において、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し、又は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、又は与えるおそれがあるもの等の事象をいう。

注2：情報セキュリティ緊急支援チーム(通称CYMAT：CYber Incident Mobile Assistance Team)

日本年金機構における個人情報流出事案：事案に関する技術的検討①

□ 原因究明調査により判明した事項①(ネットワーク構成の確認等)

- ◆ 機構のネットワークは、情報系からプロキシサーバを経由しての外部通信以外の外部通信が遮断される設定。したがって、攻撃者による外部との不審な通信については、プロキシサーバにその履歴が残る（プロキシログの解析結果は次頁参照）。

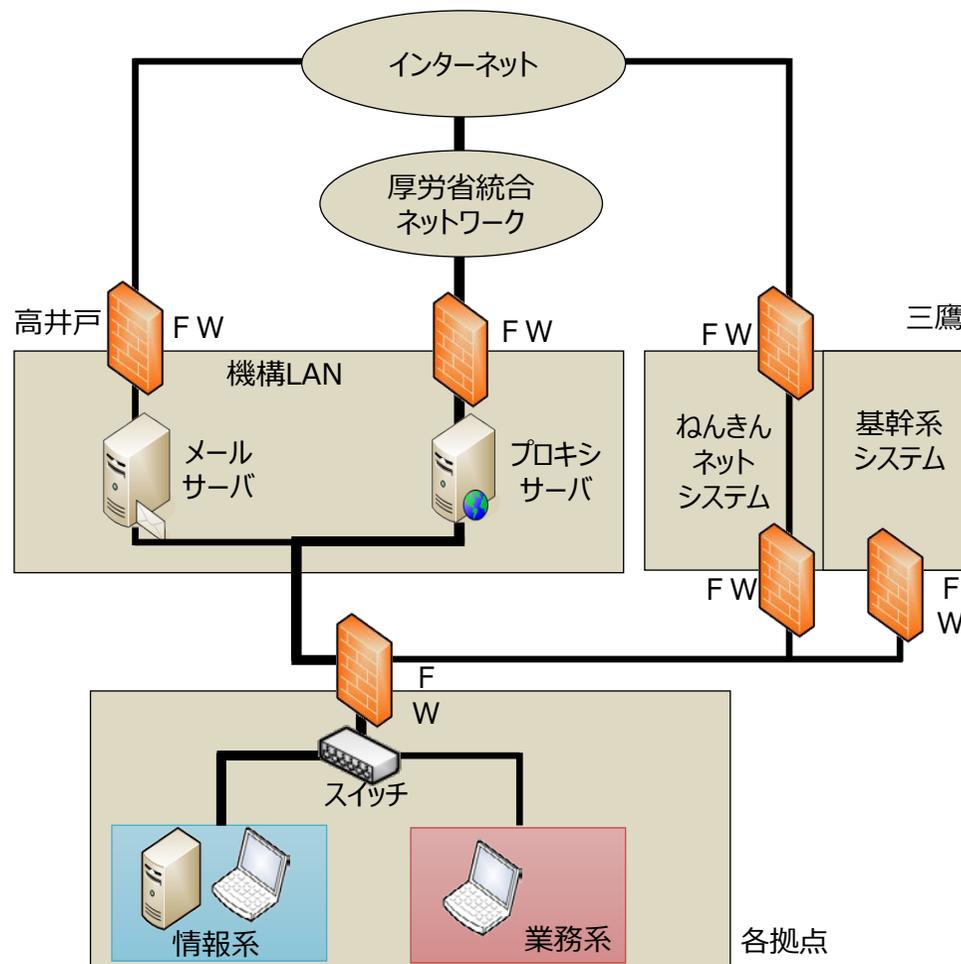
・ 業務系端末からの外部通信について

業務系端末から厚労省統合ネットワーク経由の外部通信は、スイッチ及びファイアウォールにより遮断される設定となっていることをシステム運用業者の説明と資料により確認。また、現地において、N I S C職員が説明どおりの設定となっていることを直接確認。

プロキシサーバに、業務系端末からの外部通信に関する履歴なし。

・ メール用回線等を通じた外部通信について

メール用回線及びねんきんネットシステム経由のWebアクセスは、スイッチ及びファイアウォールにより遮断される設定となっていることをシステム運用業者の説明と資料により確認。また、現地において、N I S C職員が説明どおりの設定となっていることを直接確認。



日本年金機構における個人情報流出事案：事案に関する技術的検討②

□ 原因究明調査により判明した事項②(プロキシログの解析、不審メールとの突合等)

- ◆ プロキシログの解析により、不審な通信先 2 3 件、不審な通信を行った端末 3 1 台を特定、不審メールと突合。

不審メールの番号	受信日	不審メールの概要	発生した不審な通信
I	5月8日(金)	件名：「厚生年金基金制度の見直しについて(試案)に関する意見」 宛先：公開メールアドレス(2) リンク：商用オンラインストレージ	端末 1 台が不正プログラムに感染、不審な通信が発生。約 4 時間後に端末の通信ケーブルを抜線、その後は不審な通信なし。
II	5月18日(月)	件名：給付研究委員会オープンセミナーのご案内 宛先：非公開の個人メールアドレス(98) 添付ファイル：給付研究委員会オープンセミナーのご案内.lzh	端末 3 台が不正プログラムに感染、不審な通信が発生するも接続先への通信は失敗。
III	5月18日(月) ～ 5月19日(火)	件名：厚生年金徴収関係研修資料 宛先：非公開の個人メールアドレス(20) 添付ファイル：厚生年金徴収関係研修資料 (150331厚生年金徴収支援G) .lzh (16) リンク：商用オンラインストレージ(4)	不審な通信は発生せず。
IV	5月20日(水)	件名：【医療費通知】 宛先：公開メールアドレス(3) 添付ファイル：医療費通知のお知らせ.lzh	20日午後、端末 1 台が不正プログラムに感染、不審な通信が発生。数時間以内に、他の6台の端末からも不審な通信が発生。 21日から23日にかけて、合計21台の端末から国内のサーバ(接続先 X)への多数の通信。

- ◆ NISCでは、不審メール II 及び不審メール III に関する解析結果を5月19日夜に、不審メール IV に関する解析結果を5月21日夕刻に、それぞれ厚労省情参室に提供しているが、これらの解析結果には不正プログラムの接続先に関する情報が含まれていた。
- ◆ 5月22日にNISCにおいて不審な通信を検知し厚労省に通知した後、機構による調査の過程で接続先 X への多数の通信が判明した。

日本年金機構における個人情報流出事案：CSIRTの運用等に関する検討

	NISC	厚労省	年金機構
インシデント対処	<ul style="list-style-type: none"> ● 政府統一基準^(注1)では、インシデントを認知したときに、CISO^(注2)やNISCに報告することを定めている。 ● 統一基準では、インシデント発生時に、CISOやNISC等への連絡のため、<u>各府省庁において報告窓口を含む報告・対処手順を整備することとしている。</u> 	<ul style="list-style-type: none"> ● 厚労省の情報セキュリティポリシーでは、インシデントを認知したときに、<u>CISOやNISCに報告する旨定めている。</u> ● 厚労省は、報告・対処手順を整備しているが、今回のインシデントにおいて、GSOC^(注3)から連絡を受けた担当窓口から、厚労省の責任者（CISO、課長等の幹部）に報告が上がっていなかった。 	<ul style="list-style-type: none"> ● 機構のセキュリティポリシーにおいて、<u>インシデント対処の必要性を規定し、その具体化はリスク管理一般の規程等に委ねている。</u> ● 当該規程において、リスクの定義、導入、運用、分析・評価、見直し等の枠組みが規定されているものの、<u>サイバー攻撃を想定した具体的な対応が明確化されていない。</u>
CSIRT ^(注4) 体制	<ul style="list-style-type: none"> ● 政府統一基準では、CSIRTに属する職員については、「<u>専門的な知識又は適性を有すると認められる者を選任すること</u>」と定めている。 ● CSIRTに属する職員の選任は、<u>各府省庁が統一基準の規定に従うこととされている。</u> 	<ul style="list-style-type: none"> ● 厚労省のポリシーでは、CSIRTに属する職員について、「<u>CISO、情報政策担当参事官、当該事案に係る部局の総括的な課長及び担当課室長等、CISOアドバイザーを充てる</u>」と定めている。 ● CSIRTの構成員が課室長等以上であり、<u>実働要員（課長補佐以下の職員）が選任・指名されていない</u>かった。 	<ul style="list-style-type: none"> ● 特殊法人である機構は、<u>政府統一基準の直接の適用対象ではない。</u> ● CSIRT体制は定めておらず、セキュリティポリシーや諸規程にもその定めはない。（機構によると、平成27年7月10日からCSIRT体制の構築の検討を開始。）
個人情報を取り扱うシステムの整備等	<ul style="list-style-type: none"> ● 「ガイドライン」^(注5)において、<u>標的型攻撃に対する多重防御の取組は、外交・安全保障等に加え「個人にもたらされる被害」も対象としている。</u> 	<ul style="list-style-type: none"> ● 厚労省統合ネットワークにおける標的型攻撃に対する多重防御の取組を進めていたが、<u>機構の情報系ネットワークは、「ガイドライン」の取組の対象としておらず、標的型攻撃に対する多重防御の取組が十分でなかった。</u> 	<ul style="list-style-type: none"> ● <u>インターネットに接続していない業務系からインターネットに接続をしている情報系に個人情報を移して取り扱っていた。</u>

(注1)「政府機関の情報セキュリティ対策のための統一基準」(平成26年5月 情報セキュリティ政策会議決定)

(注2) Chief Information Security Officer :最高情報セキュリティ責任者

(注3) Government Security Operation Coordination team:政府機関情報セキュリティ横断監視・即応調整チーム

(注4) Computer Security Incident Response Team:コンピュータシステムやネットワークに保安上の問題に繋がる事象が発生した際に対応する組織

(注5)「高度サイバー攻撃対処のためのリスク評価等のガイドライン」(平成26年6月25日 情報セキュリティ対策推進会議)

日本年金機構における個人情報流出事案：今回のサイバー攻撃の特徴と対策

□ 標的型攻撃の特徴

- 標的型攻撃は巧妙化しており、使われるメールも見分けが困難。
→メール開封を前提とした対策が必要。
- 攻撃者は乗っ取った端末を足掛かりとして、侵入を拡大させる。
→初期段階での認知・対処、侵入範囲を拡大させないためのシステム設計・構築・運用が重要。

□ 標的型攻撃に対する情報システム防御策等の考え方

自組織の情報・システム・業務を守る目的・対策について考え、職務・職責に応じて実施することが求められる。
[検討対策例]

◆ システム防御策

- メールに添付された実行形式のファイルを取り込まない・起動できないようにシステム設定。
- 既知の脆弱性を放置しないようにアップデート等を行う。脆弱性診断を実施。ウェブブラウザの拡張機能の必要最小限の使用。
- 侵入範囲が拡大しにくいように設定・運用。
- 業務・情報の性質等に応じて重要な情報に攻撃が到達しないよう、システム分離。
- システム分離したときに各システムで扱える情報・できない情報につきルール化し、職員に徹底。
- ローカル管理者権限のパスワードを共通とする範囲の最小限化。
- 不要な管理アカウントの確実な消去。
- 内部ネットワークにおける異常を検知する仕組みの整備。等

◆ インシデント対策に係る対策

- 不審メールの受信（不正プログラム動作の可能性）につき攻撃者が繰り返して攻撃を試みるものとして継続的に対応。
- システム構築・運用事業者とは独立した専門性の高い事業者への依頼等、平素からの準備。
- CISO等権限を有する者の下でのインシデント対応。

日本年金機構における個人情報流出事案：本部・NISCがとるべき再発防止対策

□ 各府省庁への情報提供が有効に機能するための対策

- ◆ NISCは、不審な通信検知後、速やかに分析を行い、インシデントの疑いのあるものは当該省庁に対して通知等を行っているが、通知や提供する不正プログラムの解析結果の重要性を当該省庁が理解し、迅速に適切な措置が取られることを前提としている。
- ◆ 今回の事案の教訓を踏まえれば、今後は、平素から各府省庁に対して、標的型攻撃を含むサイバー攻撃の本質と影響、NISCからの検知通知や不審メール等の解析結果の活用方法、対処方法等について研修や演習の機会を提供していく必要がある。
- ◆ 研修や演習の対象は、情報システム部局のみならず、独立行政法人、特殊法人等を所管する部局の幹部も対象として含めねばならない。本部は、その実施状況を年次報告等において評価し国民に説明していくことが重要である。

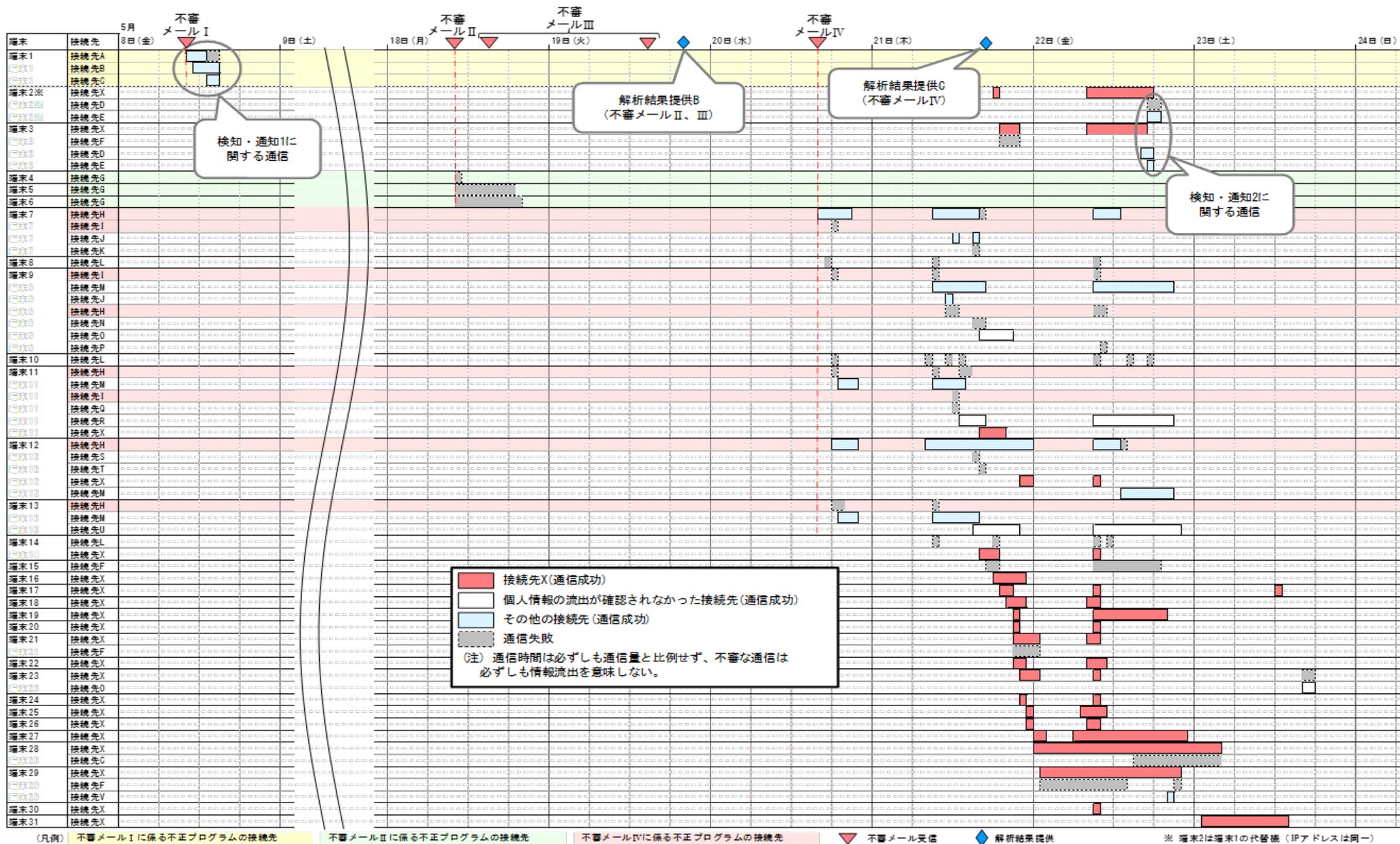
□ インシデントに備えた体制の強化

- ◆ 各府省庁においては、政府統一基準等に従って、CISOの指示の下、専門的な知識又は適正を有すると認められる者を選任したCSIRTを整備し、平素から要員の事案対処能力、経験の向上を図り、実践できるようにしておくことが求められている。
- ◆ NISCは、各府省庁のCSIRTが、事案発生時に実働する体制が整備・強化されるよう、事案の対応についての演習・訓練等の機会を設け、また、本部は、各府省庁において適切に体制整備がされ、実践のための必要な取組がなされているか等についても監査の対象とするなど、PDCAサイクルに基づく着実な取組を確保していく。
- ◆ 本部及びNISCは、政府統一基準等の見直しを行い、サイバーセキュリティ対策の向上を図る。

□ 標的型攻撃のリスクを踏まえたシステムの構築、維持、運用の強化対策

- ◆ 本部及びNISCは、標的型攻撃への対処について、政府統一基準の他、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」を取りまとめ、その実施を推進してきたが、その適用範囲は、国の行政機関としている。
- ◆ 今後は、大量の個人情報を取り扱うリスクの高いシステムにおいても、サイバー攻撃のリスクを踏まえたシステムの構築、維持、運用がなされるよう、各府省庁に対し多重防御の取組を加速化すべく次のような取組を促すよう対策を講じていく。
 - リスクを考慮したシステム構築を行うための基準の改善（適用範囲の拡大を含む。）
 - システムの維持運用を確実にする監査の強化
 - 特に技術的な事項について、外部から起用するCIO補佐官、CISOアドバイザーの積極的な活用
- ◆ 併せて、GSOC機能について、攻撃の手法が時々刻々巧妙化していることを踏まえ、不断の見直しを行っていく必要がある。

年金機構事案：感染端末と不審な通信



(出典) サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査報告」(2015年8月)

• サイバーセキュリティの推進体制（基本法とNISC）

- 事案の発生と政策・推進体制の変遷
- 基本法の制定による体制整備
 - 国、地方自治体、民間事業者の責務
 - 国民の努力

省庁HP連続改ざん(2000年)

中央省庁を対象としたホームページ書き換え (科学技術庁、総務庁他)

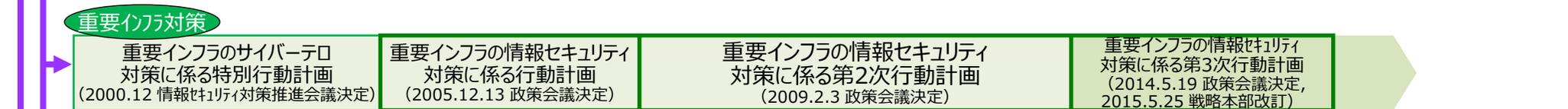
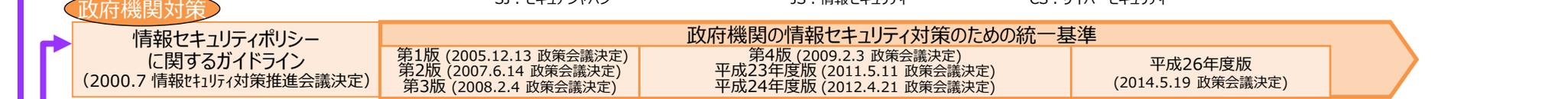
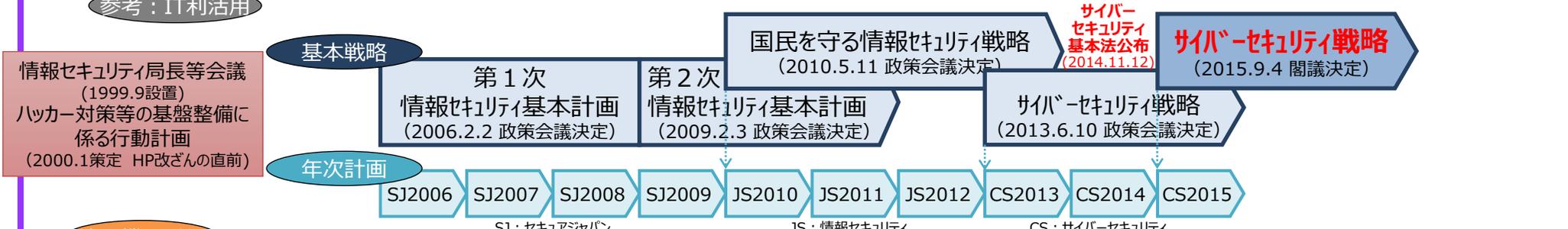
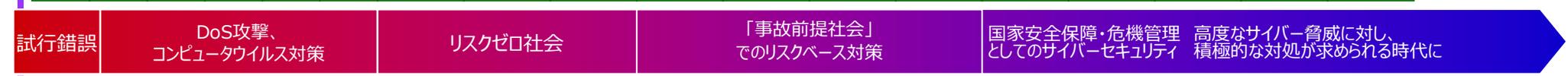
2000年1月から2月にかけて、多数の中央省庁系サイトが不正侵入及び改竄の被害を受けた。多くの場合、ホームページのデータを改竄され中国語や英語で日本やロシアを中傷するメッセージを記入された。科学技術庁、総務庁統計局は短期間に2度の被害を受けた。

- ・1月24日 科学技術庁のホームページが改竄される
- ・1月25日 大蔵省、通商産業省へのアタックが試みられたが、未遂に終わる
- ・1月25日 総務庁統計局のホームページのデータやプログラムが全て消去される
- ・1月26日 科学技術庁のホームページが再び襲われ、内容を書き換えられる
- ・1月26日 総合研究開発機構 (NIRA) のホームページが改竄される
- ・1月26日 文部省、防衛庁へのアタックが試みられたが、未遂に終わる
- ・1月27日 運輸省のホームページが不正侵入を受け、改竄される
- ・1月27日 農林水産省へのアタックが試みられたが、未遂に終わる
- ・1月27日 人事院近畿事務局のホームページが侵入され、ファイル9割が消去される
- ・1月27日 総務庁統計局のホームページが二度目の不正侵入を受け、改竄される
- ・1月28日 日本銀行へのアタックが試みられたが、未遂に終わる
- ・1月29日 政府資料等普及調査会のホームページが改竄される
- ・1月30日 郵政省沖縄管理事務所のホームページが改竄される
- ・1月31日 東京都老人総合研究所の英語ホームページが改竄される
- ・2月1日 参議院ホームページが改竄される
- ・2月2日 科学技術振興事業団のホームページが改竄される
- ・2月2日 基盤技術研究促進センターのホームページが改竄される

サイバーセキュリティ政策の経緯



- 今後の重要な環境変化
- ▶ 伊勢志摩サミット、2020年東京オリンピック・パラリンピック競技大会
 - ▶ 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



サイバー脅威の深刻化

IT依存度の高まり

PC



多くの職場・家庭に普及し、インターネットに接続
(2014年末: PC普及率 78.0%、インターネット普及率 82.8%)
※2015年版情報通信白書(総務省)

スマートフォン



世帯保有率が6.6倍に急増
(2010年末: 9.7%→2014年末: 64.2%)
※2015年版情報通信白書(総務省)

自動車



一台に搭載される車載コンピュータは100個以上、
ソフトウェアの量は約1000万行
※自動車の情報セキュリティへの取組みガイド(2013.8 IPA)

スマートメーター
(次世代電力量計)



電力会社による開発・導入の開始
[主な予定]・東京: 2020年度までに2700万台の導入完了
・関西: 2022年度までに1300万台の導入完了

サイバー攻撃の増加

【政府機関への脅威件数等】



国家関与の疑われる攻撃



韓国 (2013年4月)

重要インフラ(金融・放送等)に
対する大規模サイバー攻撃が発生。
韓国当局は北朝鮮の所業と発表。



米国 (2014年12月)

ソニー・ピクチャーズ・エンタテインメント社に
対するサイバー攻撃が発生。米国
政府は北朝鮮に責任ありとし、国家
安全保障上の問題として対応。

2020年東京オリンピック・パラリンピック 競技大会へ向けた準備

- 世界の注目を集める祭典。「ダウンタイム」は許されない。
- 2012年のロンドン大会では、開催期間中、約2億件のサイバー攻撃が発生。
- 英国政府は、6年前からサイバー攻撃対策を準備。

サイバー脅威に対応し、サイバーセキュリティを強化するため、**サイバーセキュリティ基本法が成立、施行。**

(平成26年11月12日公布。平成27年1月9日全面施行)

サイバーセキュリティ基本法～目的（法第1条）

第一条 この法律は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている状況に鑑み、我が国のサイバーセキュリティに関する施策に関し、基本理念を定め、国及び地方公共団体の責務等を明らかにし、並びにサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定めるとともに、サイバーセキュリティ戦略本部を設置すること等により、高度情報通信ネットワーク社会形成基本法（平成十二年法律第百四十四号）と相まって、サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。

背景

- インターネット等の整備
- ITの活用の進展



世界規模でのサイバーセキュリティに対する脅威の深刻化等内外の諸情勢の変化

喫緊の課題：情報の自由な流通の確保 & サイバーセキュリティの確保

対応：サイバーセキュリティに関する施策を総合的に推進

- 基本理念を定め
- 国・地方公共団体の責務等を明らかにし
- サイバーセキュリティ戦略の策定等施策の基本となる事項を定め
- サイバーセキュリティ戦略本部を設置

&

高度情報通信
ネットワーク社会
形成基本法
(IT基本法)

目的

- 経済社会の活力の向上と持続的発展
- 国民が安心して暮らせる社会の実現
- 国際社会の平和・安定の確保、我が国の安全保障に寄与

サイバーセキュリティ基本法～定義（法第2条）

第二条 この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他の知覚によっては認識することができない方式(以下この条において「電磁的方式」という。)により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置(情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体(以下「電磁的記録媒体」という。)を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。)が講じられ、その状態が適切に維持管理されていることをいう。

「サイバーセキュリティ」

電磁的方式により { 記録され
発信され
伝送され
受信され } る情報の { 漏えい
滅失
毀損 } の防止

例

その他の当該情報の安全管理のために必要な措置

&

{ 情報システム
情報通信ネットワーク } の { 安全性
信頼性 } の確保のために必要な措置

含む

{ 情報通信ネットワーク
電磁的記録媒体 } を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置

が講じられ、
その状態が適切に
維持管理されていること

※電磁的方式…電子的方式、磁気的方式その他の知覚によっては認識することができない方式

サイバーセキュリティ基本法の概要

平成26年11月12日 公布（法律第104号）
平成27年1月9日 全面施行

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、強靱な体制の構築
- 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）

■ 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基本法～国の責務

国の責務

(国の責務)

第四条 国は、前条の基本理念（以下「基本理念」という。）にのっとり、サイバーセキュリティに関する**総合的な施策を策定**し、及び**実施する責務を有する**。

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)

第十三条 国は、国の行政機関、独立行政法人（独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する独立行政法人をいう。以下同じ。）及び特殊法人（法律により直接に設立された法人又は特別の法律により特別の設立行為をもって設立された法人であって、総務省設置法（平成十一年法律第九十一号）第四条第十五号の規定の適用を受けるものをいう。以下同じ。）等におけるサイバーセキュリティに関し、**国の行政機関及び独立行政法人におけるサイバーセキュリティに関する統一的な基準の策定**、**国の行政機関における情報システムの共同化**、**情報通信ネットワーク又は電磁的記録媒体を通じた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及び分析**、**国の行政機関におけるサイバーセキュリティに関する演習及び訓練並びに国内外の関係機関との連携及び連絡調整によるサイバーセキュリティに対する脅威への対応**、**国の行政機関、独立行政法人及び特殊法人等の間におけるサイバーセキュリティに関する情報の共有**その他の必要な施策を講ずるものとする。

サイバーセキュリティ基本法～重要インフラ関係部分

重要インフラの定義

法第3条及び第12条第2項第3号

重要社会基盤事業者

国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者

重要社会基盤事業者等

重要社会基盤事業者及びその組織する団体並びに地方公共団体

重要インフラの責務

(地方公共団体の責務)

第五条 地方公共団体は、基本理念にのっとり、国との適切な役割分担を踏まえて、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する。

(重要社会基盤事業者の責務)

第六条 重要社会基盤事業者は、基本理念にのっとり、そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

施策

(重要社会基盤事業者等におけるサイバーセキュリティの確保の促進)

第十四条 国は、重要社会基盤事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずるものとする。

(サイバー関連事業者その他の事業者の責務)

第七条 **サイバー関連事業者**（インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者をいう。以下同じ。）**その他の事業者**は、基本理念にのっとり、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

(国民の努力)

第九条 国民は、基本理念にのっとり、サイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に必要な注意を払うよう努めるものとする。

サイバーセキュリティ基本法～戦略本部

(設置)

第二十四条 サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、内閣に、**サイバーセキュリティ戦略本部（以下「本部」という。）**を置く。

(所掌事務等)

第二十五条 本部は、次に掲げる事務をつかさどる。

- 一 **サイバーセキュリティ戦略の案の作成及び実施の推進**に関すること。
 - 二 **国の行政機関及び独立行政法人におけるサイバーセキュリティに関する対策の基準の作成**及び当該基準に基づく**施策の評価（監査を含む。）**その他の当該基準に基づく**施策の実施の推進**に関すること。
 - 三 **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。）に関すること。
 - 四 前三号に掲げるもののほか、サイバーセキュリティに関する施策で**重要なものの企画に関する調査審議、府省横断的な計画、関係行政機関の経費の見積り**の方針及び**施策の実施に関する指針の作成並びに施策の評価**その他の**当該施策の実施の推進**並びに**総合調整**に関すること。
- 2 本部は、サイバーセキュリティ戦略の案を作成しようとするときは、あらかじめ、高度情報通信ネットワーク社会推進戦略本部及び国家安全保障会議の意見を聴かなければならない。
- 3 本部は、サイバーセキュリティに関する重要事項について、高度情報通信ネットワーク社会推進戦略本部との緊密な連携を図るものとする。
- 4 本部は、我が国の安全保障に係るサイバーセキュリティに関する重要事項について、国家安全保障会議との緊密な連携を図るものとする。

(組織)

第二十六条 本部は、サイバーセキュリティ戦略本部長、サイバーセキュリティ戦略副本部長及びサイバーセキュリティ戦略本部員をもって組織する。

サイバーセキュリティ基本法～勧告

(サイバーセキュリティ戦略本部長)

第二十七条 本部長は、サイバーセキュリティ戦略本部長（以下「本部長」という。）とし、内閣官房長官をもって充てる。

2 本部長は、本部の事務を総括し、所部の職員を指揮監督する。

3 本部長は、第二十五条第一項第二号から第四号までに規定する評価又は第三十条若しくは第三十一条の規定により提供された資料、情報等に基づき、必要があると認めるときは、**関係行政機関の長に対し、勧告することができる。**

4 本部長は、前項の規定により関係行政機関の長に対し勧告したときは、当該関係行政機関の長に対し、**その勧告に基づいてとった措置について報告を求めることができる。**

5 本部長は、第三項の規定により勧告した事項に関し特に必要があると認めるときは、**内閣総理大臣に対し、当該事項について内閣法（昭和二十二年法律第五号）第六条の規定による措置がとられるよう意見を具申することができる。**

内閣法

第六条 内閣総理大臣は、閣議にかけて決定した方針に基づいて、行政各部を指揮監督する。

サイバーセキュリティ基本法～資料提供

(資料提供等)

第三十条 **関係行政機関の長**は、本部の定めるところにより、本部に対し、サイバーセキュリティに関する**資料又は情報**であって、本部の所掌事務の遂行に資するものを、**適時に提供**しなければならない。

2 前項に定めるもののほか、**関係行政機関の長**は、本部長の求めに応じて、本部に対し、本部の所掌事務の遂行に必要なサイバーセキュリティに関する**資料又は情報の提供及び説明**その他**必要な協力**を行わなければならない。

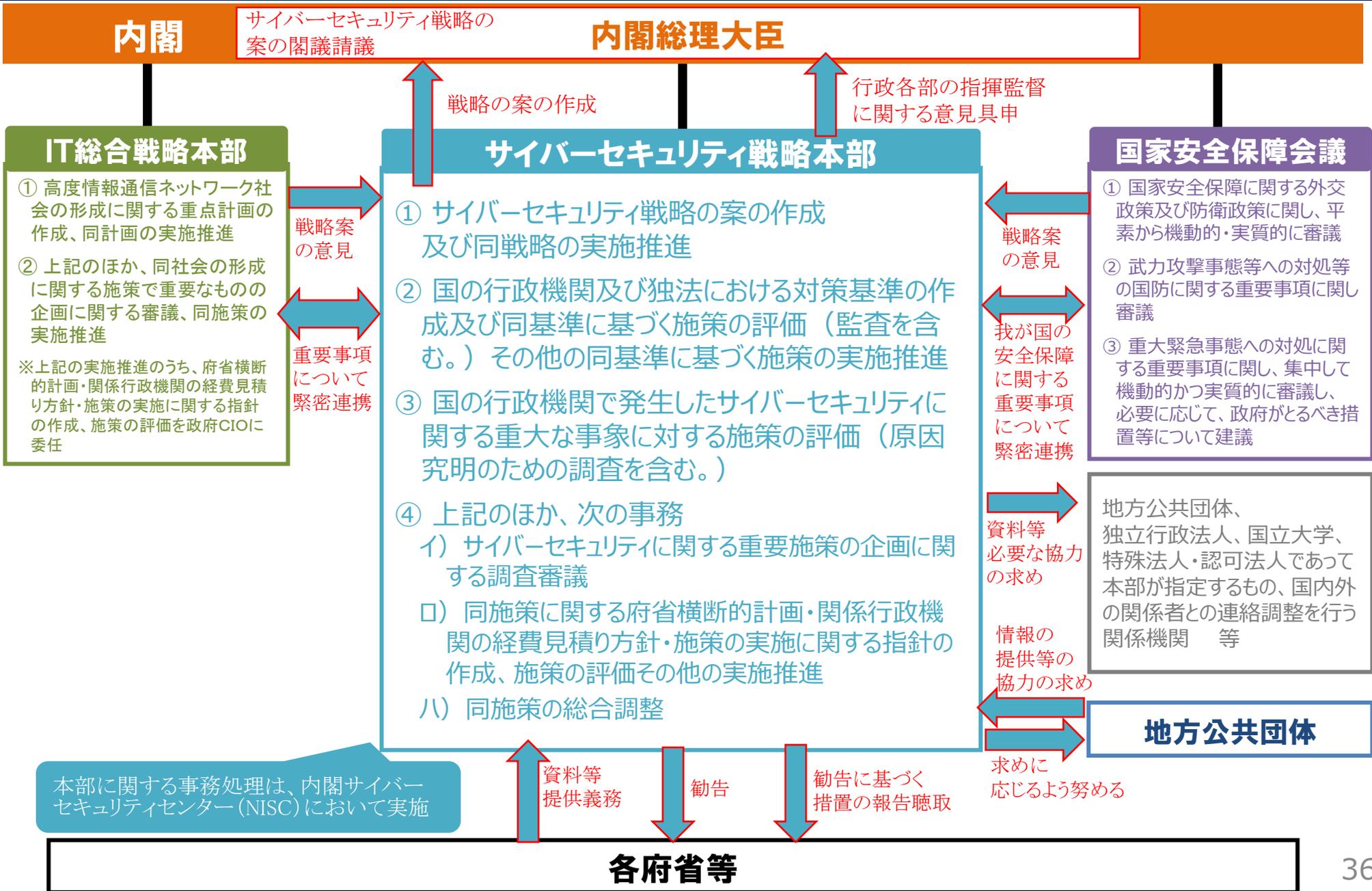
(資料の提出その他の協力)

第三十一条 本部は、その所掌事務を遂行するため必要があると認めるときは、**地方公共団体及び独立行政法人の長**、**国立大学法人**（国立大学法人法（平成十五年法律第百十二号）第二条第一項に規定する国立大学法人をいう。）の**学長**、**大学共同利用機関法人**（同条第三項に規定する大学共同利用機関法人をいう。）の**機構長**、**日本司法支援センター**（綜合法律支援法（平成十六年法律第七十四号）第十三条に規定する日本司法支援センターをいう。）の**理事長**、**特殊法人及び認可法人**（特別の法律により設立され、かつ、その設立等に関し行政官庁の認可を要する法人をいう。）であって本部が指定するものの**代表者並びにサイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整を行う関係機関の代表者**に対して、**資料の提出、意見の開陳、説明**その他**必要な協力を求めることができる。**

2 本部は、その所掌事務を遂行するため**特に必要があると認めるときは**、前項に**規定する者以外の者**に対しても、**必要な協力を依頼**することができる。

地方公共団体以外の
重要インフラ事業者等もこちら

サイバーセキュリティ戦略本部の機能・権限（イメージ）



我が国におけるサイバーセキュリティ政策推進体制（法施行後 H27.1.9～）

内閣

内閣総理大臣

高度情報通信ネットワーク社会推進戦略本部 (IT総合戦略本部)

高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進

緊密連携

サイバーセキュリティ戦略本部 (2015.1.9 サイバーセキュリティ基本法により設置)

本部長 内閣官房長官
 副本部長 東京オリンピック競技大会・パラリンピック競技大会担当大臣
 本部員 国家公安委員会委員長
 総務大臣
 外務大臣
 経済産業大臣
 防衛大臣
 情報通信技術(IT)政策担当大臣
 有識者 (7名; 10名以下)

閣僚が参画

遠藤 信博 日本電気株式会社代表取締役執行役員社長
 小野寺 正 KDDI株式会社取締役会長
 中谷 和弘 東京大学大学院法学政治学研究所教授
 野原佐和子 株式会社イブシ・マーケティング研究所代表取締役社長
 林 紘一郎 情報セキュリティ大学院大学教授
 前田 雅英 日本大学大学院法務研究科教授
 村井 純 慶應義塾大学教授

国家安全保障会議 (NSC)

我が国の安全保障に関する重要事項を審議

緊密連携



重要インフラ
専門調査会

研究開発戦略
専門調査会

普及啓発・人材
育成専門調査会

サイバーセキュリティ
対策推進会議
(CISO等連絡会議)

(事務局)

<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、化学、クレジット、石油)
 国土交通省 (鉄道、航空、物流)

協力

<その他関係省庁>

文部科学省 (セキュリティ教育) 等

内閣官房 内閣サイバーセキュリティセンター
 (2015.1.9 内閣官房組織令により設置)

内閣サイバーセキュリティセンター長
 (内閣官房副長官補(事態対処・危機管理)が兼務)
 副センター長 (内閣審議官)
 サイバーセキュリティ補佐官

政府機関・情報セキュリティ
横断監視・即応調整チーム
(G SOC)

情報セキュリティ
緊急支援チーム
(CYMAT)

協力

閣僚
本部長
5省庁

警察庁 (サイバー犯罪・攻撃の取締り)
 総務省 (通信・ネットワーク政策)
 外務省 (外交・安全保障)
 経済産業省 (情報政策)
 防衛省 (国の防衛)



内閣サイバーセキュリティセンター（NISC）の組織体制



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

センター長
(内閣官房副長官補)

副センター長
(内閣審議官)

副センター長
(内閣審議官)

サイバーセキュリティ補佐官

基本戦略

- 全体戦略及び年度計画の策定
- 研究開発・技術開発戦略の立案
- 普及啓発・人材育成に関する施策の推進 等

国際戦略

- 情報セキュリティに関する我が国の国際戦略の立案
- 諸外国の関係機関等との緊密な連携 等

政府機関総合対策

- 政府統一的な「対策基準」の策定
- 政府機関における情報セキュリティ対策の「評価」
- 政府機関の情報セキュリティ対策の向上に資する施策の推進 等

情報統括

- サイバー攻撃に関する情報の収集・集約
- 政府機関情報セキュリティ横断監視・即応調整チーム(GSOC)の運用 等

重要インフラ

- 重要インフラに関する情報セキュリティ対策の企画・立案
- 重要インフラの分野横断的な演習の実施及び脅威の分析
- 重要インフラの情報セキュリティに関する情報の収集・分析及び提供 等

事案対処分析

- サイバー攻撃事案の対処調整及び訓練
- GSOCの運用のうち、不正プログラムの分析 等

NISCと関係機関との協力（パートナーシップ）について

サイバーセキュリティ対策を推進するため、NISCは関係機関との協力関係を強化。

一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）

【協力内容】 国際連携活動及び情報共有等に関するパートナーシップを新たに締結。（参考：「サイバーセキュリティ基本法」（平成26年法律第104号）による、インシデント発生時に国内外の連絡調整を行う関係機関への協力要請。）

独立行政法人情報処理推進機構（IPA）

【協力内容】 脆弱性対応、民間事業者や独立行政法人等との情報共有、政府機関のシステム調達等に関するセキュリティ認証、国民・企業等に対する普及啓発等の幅広い分野でのパートナーシップを新たに締結。

国立研究開発法人情報通信研究機構（NICT）

【協力内容】 情報通信関連のセキュリティ技術情報の共有、研究開発戦略の推進に関する協力、2020年オリンピック・パラリンピック東京大会等に向けたサイバーセキュリティ技術に関する協力等に関するパートナーシップを締結。

国立研究開発法人産業技術総合研究所（AIST）

【協力内容】 脆弱性等に関する情報共有、研究開発の推進等に関する協力、ITやサイバーセキュリティに関する科学技術的な専門的知見の共有、プライバシー保護に関する専門的知見の共有、サイバーセキュリティに関する企業等との橋渡しに関する協力等に関するパートナーシップを締結。

• サイバーセキュリティ戦略

- 今後の取組方針
- 年金機構事案による拡充

新たな「サイバーセキュリティ戦略」について（全体構成）

1 サイバー空間に係る認識

- サイバー空間は、「無限の価値を産むフロンティア」である人工空間であり、人々の経済社会の活動基盤
- あらゆるモノがネットワークに接続され、実空間とサイバー空間との融合が高度に深化した「**接続融合情報社会（連融情報社会）**」が到来同時に、サイバー攻撃の被害規模や社会的影響が年々拡大、脅威の更なる深刻化が予想

2 目的

- 「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって「**経済社会の活力の向上及び持続的発展**」、「**国民が安全で安心して暮らせる社会の実現**」、「**国際社会の平和・安定及び我が国の安全保障**」に寄与する。

3 基本原則

- ① 情報の自由な流通の確保 ② 法の支配 ③ 開放性 ④ 自律性 ⑤ 多様な主体の連携

4 目的達成のための施策

①後手から**先手**へ / ②受動から**主導**へ / ③サイバー空間から**融合空間**へ

経済社会の活力の向上及び持続的発展

～ 費用から投資へ ～

- **安全なIoTシステムの創出**
安全なIoT活用による新産業創出
- **セキュリティマインドを持った企業経営の推進**
経営層の意識改革、組織内体制の整備
- **セキュリティに係るビジネス環境の整備**
ファンドによるセキュリティ産業の振興

国民が安全で安心して暮らせる社会の実現

～ 2020年・その後に向けた基盤形成 ～

- **国民・社会を守るための取組**
事業者の取組促進、普及啓発、サイバー犯罪対策
- **重要インフラを守るための取組**
防護対象の継続的見直し、情報共有の活性化
- **政府機関を守るための取組**
攻撃を前提とした防御力強化、監査を通じた徹底

国際社会の平和・安定 及び 我が国の安全保障

～ サイバー空間における積極的平和主義 ～

- **我が国の安全の確保**
警察・自衛隊等のサイバー対処能力強化
- **国際社会の平和・安定**
国際的な「法の支配」確立、信頼醸成推進
- **世界各国との協力・連携**
米国・ASEANを始めとする諸国との協力・連携

横断的 施策

■ 研究開発の推進

攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発

■ 人材の育成・確保

ハイブリッド型人材の育成、実践的演習、突出人材の発掘・確保、キャリアパス構築

5 推進体制

- 官民及び関係省庁間の連携強化、東京オリンピック・パラリンピック競技大会等に向けた対応

新たな「サイバーセキュリティ戦略」について（総論）

1.サイバー空間に係る認識 2.目的 3.基本原則

- 本戦略は、2020年東京オリンピック・パラリンピック競技大会の開催、そしてその先の2020年代初頭までの将来を見据えつつ、今後3年程度の基本的な施策の方向性を示すもの。

1 サイバー空間に係る認識

- サイバー空間は「国境を意識することなく自由にアイデアを議論でき、そこで生まれた知的創造物やイノベーションにより、無限の価値を産むフロンティア」である人工の空間で、経済社会の活動基盤である。
- 実空間のモノやヒトが、サイバー空間により物理的制約を超えて接続することで、実空間とサイバー空間の融合が高度に深化した「接続融合情報社会(連融情報社会)」が到来しつつある。
- 一方、国民生活・経済社会活動への重大な被害や我が国の安全保障に対するサイバー脅威も高まっている。今後、こうした脅威が更に深刻化することが予想される。

2 目的

- 「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安定及び我が国の安全保障」に寄与する。

3 基本原則

本戦略の目的達成のための施策の立案及び実施に当たり、以下に示す基本原則に従う。

- ① 情報の自由な流通の確保：サイバー空間発展の基盤として、情報の自由な流通が保証された空間を維持
- ② 法の支配：実空間と同様にサイバー空間に対しても「ルールや規範」の適用を徹底
- ③ 開放性：常に参加を求める者に開かれ、新たな価値を生み出す空間として保持
- ④ 自律性：各者の主体的な行動により、悪意ある行動を抑止する自律的メカニズムを推進
- ⑤ 多様な主体の連携：様々な主体の適切な連携関係構築とダイナミックな対処策実現

我が国は、上記の5つの基本原則に従うとともに、国民の安全・権利の保障のため、政治・経済・技術・法律・外交その他の採り得る全ての有効な手段を選択肢として保持する。

新たな「サイバーセキュリティ戦略」について（各論①）

4.目的達成のための施策

経済社会の活力の向上及び持続的発展

～費用から投資へ～

■ 安全なIoTシステムの創出

- 企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザイン(SBD)の考え方に基づき、安全なIoT(モノのインターネット)システムを活用した事業を振興
- IoTシステムに係る大規模な事業について、サイバーセキュリティ戦略本部による総合調整等により、必要な対策を統合的に実施するための体制等を整備
- エネルギー分野、自動車分野、医療分野等におけるIoTシステムのセキュリティに係る総合的なガイドライン等を整備
- IoTシステムの特徴(長いライフサイクル、処理能力の制限等)、ハードウェア真正性の重要性等を考慮した技術開発・実証事業の実施

■ セキュリティマインドを持った企業経営の推進

- 企業におけるセキュリティに係る取組が市場等から正当に評価される仕組みの構築(経営ガイドライン等の発信含む)
- 経営層と実務者層との間のコミュニケーション支援を行う橋渡し人材層の育成
- 民間・官民間における脅威・インシデント情報の共有網の拡充

■ セキュリティに係るビジネス環境の整備

- 政府系ファンドの活用等により、サイバーセキュリティ関連産業を振興(ベンチャー企業の育成等を含む)
- 中小企業等のクラウドサービス活用に有効なセキュリティ監査の普及促進
- サイバーセキュリティ産業の振興に向けた制度の見直し(リバースエンジニアリング等)
- IoTシステムのセキュリティに係る国際的な標準規格や相互承認枠組み作りの国際的議論を主導
- 知財漏えい防止強化など、公正なビジネス環境を整備



▲自動運転車の実証実験

新たな「サイバーセキュリティ戦略」について（各論②）

4.目的達成のための施策

国民が安全で安心して暮らせる社会の実現

～ 2020年・その後に向けた基盤形成 ～

■ 国民・社会を守るための取組

- ソフトウェア等の脆弱性関連情報の収集やインターネット上の各種のサイバー攻撃等観測システムの連携・強化の推進
- 攻撃を受けた端末の利用者に対する注意喚起等の推進
- 整備が進む公衆無線LAN等のセキュリティ確保のための対策検討
- 地域における普及啓発活動の促進、中小企業や地方公共団体への啓発・支援
- サイバー犯罪への対処能力・捜査能力の向上に向けた取組の強化
(通信履歴の保存の在り方についての関係事業者における適切な取組の推進を含む)



▲ 双方向型の普及啓発セミナー（サイバーセキュリティカフェ）

■ 重要インフラを守るための取組

- 重要インフラ分野の範囲及び各分野内での「重要インフラ事業者」の範囲の継続的な見直し
- より効果的かつ迅速な官民の情報共有、政府機関内での必要な連携、訓練・演習の実施の推進
- マイナンバー制度の円滑な運用確保のため地方公共団体に必要な政策を実施し、国・地方の全体を俯瞰した監視・検知体制や、専門的・技術的知見を有する監視・監督体制を整備
- スマートメーター等の制御系について、国際標準に即した第三者認証制度の活用等を推進



▲ サイバー攻撃等に対する対応能力向上のための演習
(重要インフラ分野横断的演習)

■ 政府機関を守るための取組

- ペネトレーションテスト等を通じたセキュリティ対策を徹底、サプライチェーン・リスクへの対応、政府機関情報セキュリティ横断監視・即応調整チーム(GSOC)による検知・解析機能強化、標的型攻撃に対する多重防御の取組加速等による防御力の強化
- マネジメント監査等を通じた組織の体制・制度の検証・改善、リスク評価に基づく組織的な対策・管理等による組織的対応能力の強化
- 新たなIT製品・サービスの特性を踏まえた政府統一的なセキュリティ対策の策定・推進
- 独立行政法人や、府省庁と一体となり公的業務を行う特殊法人等への監視・監査・原因究明調査の実施等による総合的な対策強化

新たな「サイバーセキュリティ戦略」について（各論③）

4. 目的達成のための施策

国際社会の平和・安定及び我が国の安全保障 ～サイバー空間における積極的平和主義～

■ 我が国の安全の確保

- 警察や自衛隊を始めとする対処機関の能力の質的・量的な向上
- 安全保障上重要な先端技術(宇宙関連技術、原子力関連技術、セキュリティ技術、防衛装備品に関する技術等)に係るサイバーセキュリティの確保
- 政府機関や重要インフラ事業者等によるサービスの持続的提供のための情報の共有・分析・対応に向けた官民連携の一層の強化

■ 国際社会の平和・安定

- 国連等におけるサイバー空間に係る国際的なルール等の形成に向けた積極的な貢献
- サイバー空間を悪用する国際テロ組織に対する国際社会と連携した対処
- 各国の能力構築(キャパシティビルディング)への積極的な協力の推進

■ 世界各国との協力・連携

- アジア大洋州 : 日・ASEAN間の協力関係の更なる深化・拡大並びに地域の戦略的パートナーとの協力・連携の強化
- 北米 : 同盟国たる米国とあらゆるレベルでの緊密な連携・対応(日米サイバー対話、インターネットエコミーに関する日米政策協力対話、日米サイバー防衛政策ワーキンググループ等)
- 欧州・中南米・中東アフリカ : 基本的価値観を共有する国々とのパートナーシップの構築・強化



▲日ASEAN情報セキュリティ政策会議



▲我が国で開催したサイバーセキュリティに関する国際カンファレンス (Meridian Conference 2014)

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プ：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(2015年3月)

リスクの
グローバル化

国際連携取組方針

(13年10月)

- 多角的なパートナーシップの強化
や技術の国際展開等の加速化

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

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。

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
- 第3回日米サイバー対話：2015年7月@東京

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カ国の政府機関、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。

新たな「サイバーセキュリティ戦略」について（各論④・推進体制）

4.目的達成のための施策

5.推進体制

横断的施策

■ 研究開発の推進

- 関係者間の情報・データの共有等によるサイバー攻撃の検知・防御能力の一層の向上
- 融合領域の研究促進、及び安全保障のためのコア技術(暗号技術等)の保持
- 各国が強みを有する技術を有機的に組み合わせた国際連携による研究開発の推進

■ 人材の育成・確保

- 他分野の知識も併せ持つハイブリッド型人材の育成促進
- 高等教育等における産学官連携の推進・実践的演習の充実
- 初等中等教育段階からの教育の充実
(論理的思考力やモノの基礎的動作原理の理解促進、教員の指導力向上に向けた研修等の改善・充実)
- サイバー演習環境のクラウド環境における整備、産学官共同による教材開発の支援
- 国際的競技イベント等を通じたグローバル水準の高度人材の発掘・確保
- 実践的能力を評価する資格制度の創設、標準的なスキルの基準の整備等の推進



▲ 合宿形式で知識・技能を学ぶセキュリティキャンプ



▲ 58ヶ国が参加したセキュリティコンテスト(2014年度)

- NISC対処能力の一層の強化や産学官及び関係省庁間の連携強化によるサイバー攻撃の検知・分析・判断・対処の機能強化
- ### 5 推進体制
- 国家の関与が疑われる高度な攻撃に対し、戦略本部とNSC(安全保障)・重大テロ対策本部(危機管理)と緊密に連携
 - 東京オリンピック・パラリンピック競技大会等に向け、リスクの明確化、組織・施設・協力関係の構築・維持、十分な訓練を実施

- 戦略本部は、各年度の年次計画及び年次報告を作成するとともに、経費見積り方針を策定する。

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IT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

SIP新課題:重要インフラ等におけるサイバーセキュリティの確保

H27(2015)年度~H31(2019)年度(予定)、H27年度予算:5億円

経緯

6月18日(第10回CSTI)
8月6日
9月15日~10月5日
10月15日
11月10日(第12回CSTI:持ち回り)実施方針の決定

新課題候補「重要インフラ等におけるサイバーセキュリティの確保」の承認
情報セキュリティ大学院大学・後藤厚宏教授の内閣府政策参与への任命
研究開発計画案パブリックコメントの実施
ガバニングボードでの事前評価

PD



情報セキュリティ
大学院大学教授
後藤 厚宏

達成目標

- 悪意のある機能を“持ち込ませない”、悪意のある動作を“いち早く発見する”システムの実現
 - 国産セキュリティ技術確立。重要インフラ産業の競争力強化、安全な社会基盤実現に貢献
- ⇒ 2020年五輪大会の安心安全な開催

研究開発計画案概要

古い機器、セキュリティが弱い機器は「信頼」できる機器で囲いこんで防御



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）

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

I T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**」の好循環を形成する。

【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」

- I T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I T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。

政府機関等のサイバーセキュリティ対策の抜本的強化①

日本年金機構の情報流出事案等を踏まえ、政府機関等のサイバーセキュリティ対策について、所要の法改正を含め、抜本的な強化を図る。

(注)「日本再興戦略」改訂2015（平成27年6月30日閣議決定）に盛り込まれた施策を含む追加的施策を新たなサイバーセキュリティ戦略に盛り込み、積極的かつ総合的に推進する。

1. NISCの機能強化

■ GSOCの大幅な機能強化

- 政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）システムの検知・解析機能及び運用体制の強化

■ 業務対象の拡大等

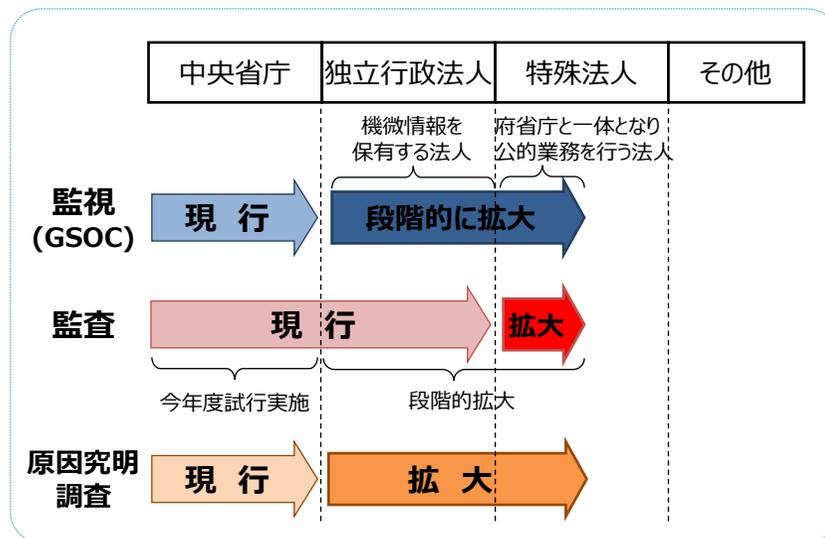
- 監視・監査・原因究明調査業務の対象について、政府機関（中央省庁）に加え、独立行政法人、政府機関と一体となって公的業務を行う特殊法人等に段階的に拡大（所要の法改正について速やかに検討）

■ 連携推進体制の強化

- 独立行政法人情報処理推進機構（IPA）及び国立研究開発法人情報通信研究機構（NICT）をはじめ、大規模なサイバー攻撃への対処等に対する知見を有する者との積極的な連携（所要の法改正について速やかに検討）

■ NISCの要員強化

- 高度セキュリティ人材の民間登用等による対処能力の一層の強化



2. 政府全体の取組強化

■ 政府機関における体制強化

- 政府機関等におけるインシデント対応チーム（CSIRT）体制の強化
- 初動対応に向けた組織的対応体制（幹部を含む。）の構築や政府全体の実践的訓練の実施等による危機管理体制の強化

■ 攻撃リスク低減のための対策強化（対策強化のための方針を早急に策定）

- インターネット接続口の更なる集約化
- 標的型攻撃に対する多重防御の取組の加速化
- 大量の個人情報等の重要情報を取り扱う情報システムのインターネットからの分離
- 政府機関における全面的なクラウドサービスへの移行を見据えた対策の強化

■ 人材・予算の確保

- 行政機関におけるセキュリティ人材の育成促進
- 所要の予算について行政効率化等により節減した費用等をサイバーセキュリティ対策へ振り向け（「サイバーセキュリティ関係施策に関する平成28年度予算重点化方針」に基づき、IoTセキュリティの確保、政府機関の対策強化、人材育成等に重点）

政府機関等のサイバーセキュリティ対策の抜本的強化③

3. その他の重要課題への取組強化

■ 重要インフラに関する取組強化

- 社会環境の変化や既存の知見の集積等を踏まえ、重要インフラの対象範囲を見直し（継続実施）
- 情報共有環境の構築と体制の整備、及び演習・訓練の実施による継続的改善

■ セキュリティ人材の育成のための演習環境の整備（本年度中に人材育成総合強化方針(仮称)を策定）

- クラウド環境の実践的な演習環境の整備等（国立研究開発法人情報通信研究機構（NICT）との積極的な連携）

■ 即応予備チームの体制整備

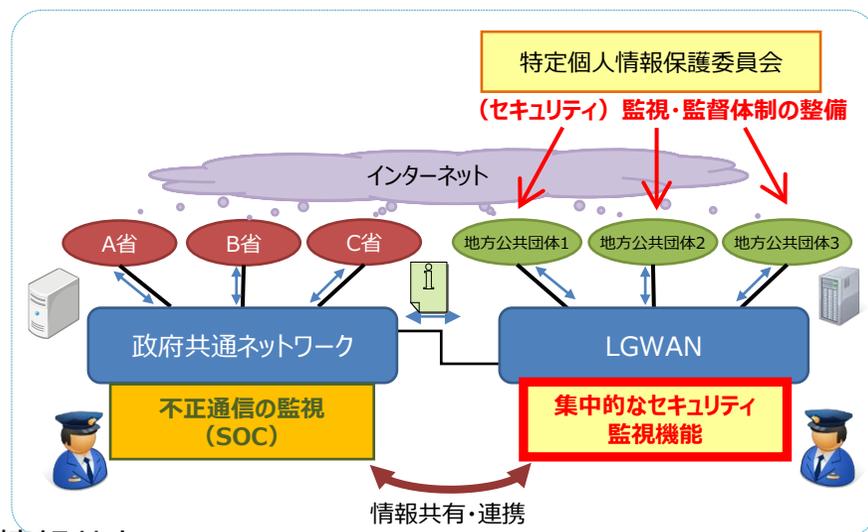
- 政府機関、独立行政法人、民間企業等から緊急時の対処チームへの参加等を可能とする体制の整備（法改正について速やかに検討）

■ マイナンバー制度の円滑な導入に向けた対策の強化

- 特定個人情報保護委員会において、関係機関と連携して監視・監督体制を整備（本年度中を目標）
- 総合行政ネットワーク（LGWAN）について集中監視機能を設ける等、GSOCとの連携による国・地方を俯瞰した監視・検知体制を整備
- 官民連携を実現する認証連携のための枠組みの取組方針を策定

■ 事案対処に関する取組強化

- サイバー攻撃を組織的に行う集団等の動向分析と捜査機関等との情報共有
- 対処機関における能力の質的・量的向上



- **重要インフラに関する施策（第3次行動計画）**

- 民間での取組の考え方
- 政府の対応

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

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 I T 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、
I T 障害の発生を可能な限り減らすとともに I T 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 [総務省、経済産業省等]
- 事案対処省庁 [警察庁、防衛省等]
- 防災関係府省庁 [内閣府、各省庁等]
- 情報セキュリティ関係機関 [NICT、IPA、JPCERT等]
- サイバー空間関連事業者 [各種ベンダー等]

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

H26.5.19 情報セキュリティ政策会議 策定
H27.5.25 サイバーセキュリティ戦略本部改訂

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



I T 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 I T 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

第3次行動計画の基本的考え方・要点

「重要インフラ防護」の目的

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 I T 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、I T 障害の発生を**可能な限り減らす**とともに I T 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。

「基本的な考え方」

情報セキュリティ対策は、**一義的には重要インフラ事業者等が自らの責任において実施**するものである。また、重要インフラ防護における官民が一丸となった取組を通じて国民の安心感の醸成を目指す。

- 重要インフラ事業者等は事業主体として、また社会的責任を負う立場としてそれぞれに対策を講じ、また継続的な改善に取り組む。
- **政府機関は**、重要インフラ事業者等の情報セキュリティ対策に関する取組に対して**必要な支援を行う**。
- 取組に当たっては、個々の重要インフラ事業者等が単独で取り組む情報セキュリティ対策のみでは多様な脅威への対応に限界があることから、**他の関係主体との連携をも充実させる**。

～ 行動計画推進に当たって期待する関係主体、更には事業者等の経営層に期待すること ～

各関係主体（重要インフラ事業者等、政府機関、情報セキュリティ関係機関等）の在り方

- **自らの状況を正しく認識**し、**活動目標を主体的に策定**するとともに、各々必要な取組の中で定期的に自らの対策・施策の進捗状況を確認する。また、他の関係主体の活動状況を把握し、**相互に自主的に協力**する。
- I T 障害の規模に応じて、情報に基づく対応の 5 W 1 H を理解しており、I T 障害の予兆及び発生に対し冷静に対処ができる。多様な関係主体間でのコミュニケーションが充実し、自主的な対応に加え、他の関係主体との連携、統制の取れた対応ができる。

重要インフラ事業者等の経営層の在り方

経営層は、上記の在り方に加え、以下の項目の必要性を認識し、実施できていること。

- 上記の目的達成に当たっての情報セキュリティを中心とする**リスク源の認識**。
- 上記のリスク源の評価及びそれに基づく**優先順位を含む方針の策定**。
- システムの構築・運用及び当該方針の実行に必要な計画の策定、並びに予算・体制・人材等の経営**資源の継続的な確保**。
- システムの運用状況の把握等を通じた当該方針の**実行の有無の検証**。
- 演習・訓練等を通じた他関係主体との情報共有を含む障害対応体制の**検証及び改善策の有無の検証**。

第3次行動計画 施策①：安全基準等の整備及び浸透

重要インフラ防護能力の維持・向上を目的に、PDCAサイクルの下、「指針」及び「安全基準等」の相互的・継続的改善を目指す。

※安全基準等…業法、業界標準／ガイドライン、内規等の総称

※指針……安全基準等の策定・改訂に資するため、分野横断的に必要度の高い対策項目を収録したもの

行動計画期間当初の課題

- 優先順位付けされた指針の提示要望（事業者等から）
- 事業者等のPDCAサイクルに沿った指針の見直し

行動計画期間中の施策

（1）指針の継続的改善

- 指針本編・対策編のPDCAサイクルに沿った見直し
- セキュリティ対策の優先順位付け等（成長モデル）の考え方の例示

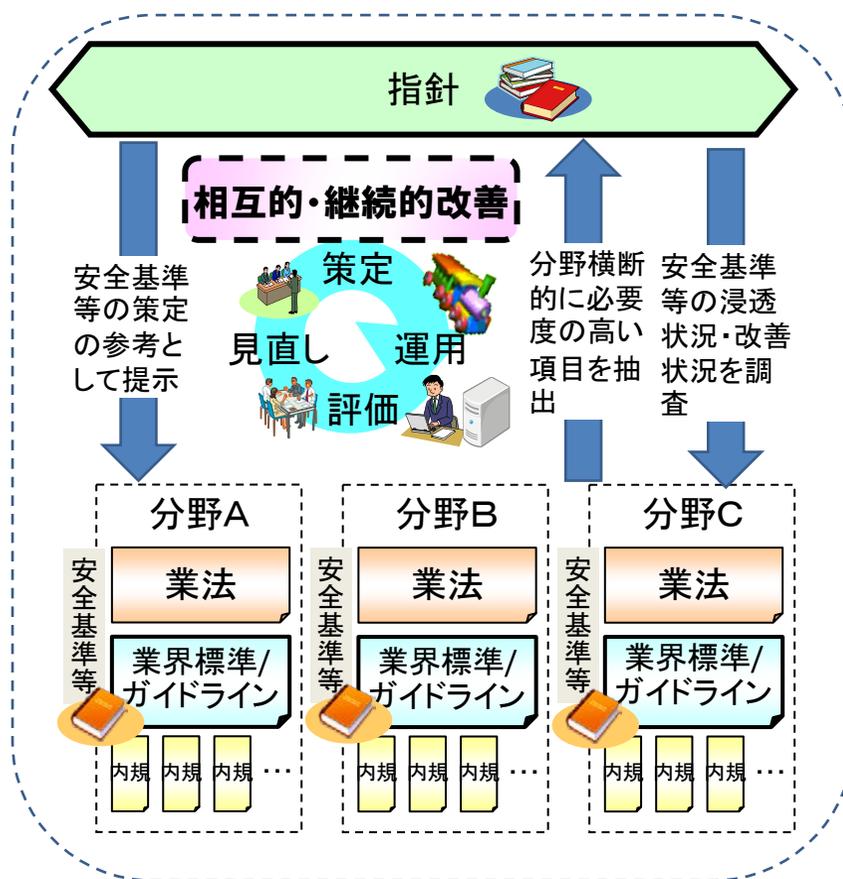
（2）安全基準等の継続的改善

- 各分野の安全基準等を対策等から得た知見を基に改善

（3）安全基準等の浸透

- 毎年の調査（重要インフラ事業者等への往訪を含む）により、対策状況を客観的に把握
- 中小規模事業者等調査対象の拡大と対策プロセスに沿った項目整理により、強化対象等を明確化

第3次行動計画に基づく取組



『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』について

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

～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～

課題解決に向けて

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(第4版)を2015年度に提示

指針(第4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)

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

※(解説例):「情報セキュリティ対策(技術)に係る設計・実装・保守」
情報セキュリティ要件に応じて情報システムへの情報セキュリティ対策を実装する。その際、情報セキュリティ対策機能の実装が業務要件にて要するシステム性能を損なわないよう留意が必要である。また、ノウハウの蓄積を考慮し、情報セキュリティ対策の実装に係る設計資料を作成する。

具体的に何をすればよいか

指針_対策編
(具現化例)

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

※(対策項目例):「情報セキュリティ対策(技術)に係る設計・実装・保守」
○セキュリティ要件の実装に付随するネットワークに係る対応
- 外部ネットワークとの接続制限(プロキシ経由等)
- 内部と外部のネットワークの分離
- 不要なポートの閉塞
- 公開するサーバー上に保存する情報の制限
- ルーターによるDoS攻撃対策 等

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)

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

第3次行動計画 施策②：情報共有体制の強化

多様な脅威に対応するため、個々の重要インフラ事業者等が単独で取り組む情報セキュリティ対策に加え、分野内、分野間あるいは官民間の情報共有を一層強化する。

行動計画期間当初の課題

- 情報共有頻度の分野間格差の解消
- 「脅威の種類」の細分化
- 大規模IT障害対応時の情報共有体制の構築
- 新たな関係主体との連携の在り方の整理 等

行動計画期間中の施策

(1) 情報共有体制の発展

- 新たな関係主体※の追加
※防災関係府省庁、サイバー空間関連事業者
- 平時とその延長線上の大規模IT障害対応体制の構築

(2) 情報共有の更なる促進

- 迅速・正確な状況把握のための情報連絡・提供時の詳細項目の見直し
- セプターカウンシルを始めとするセプター間の情報共有の更なる充実

(3) 関係主体の役割の明確化

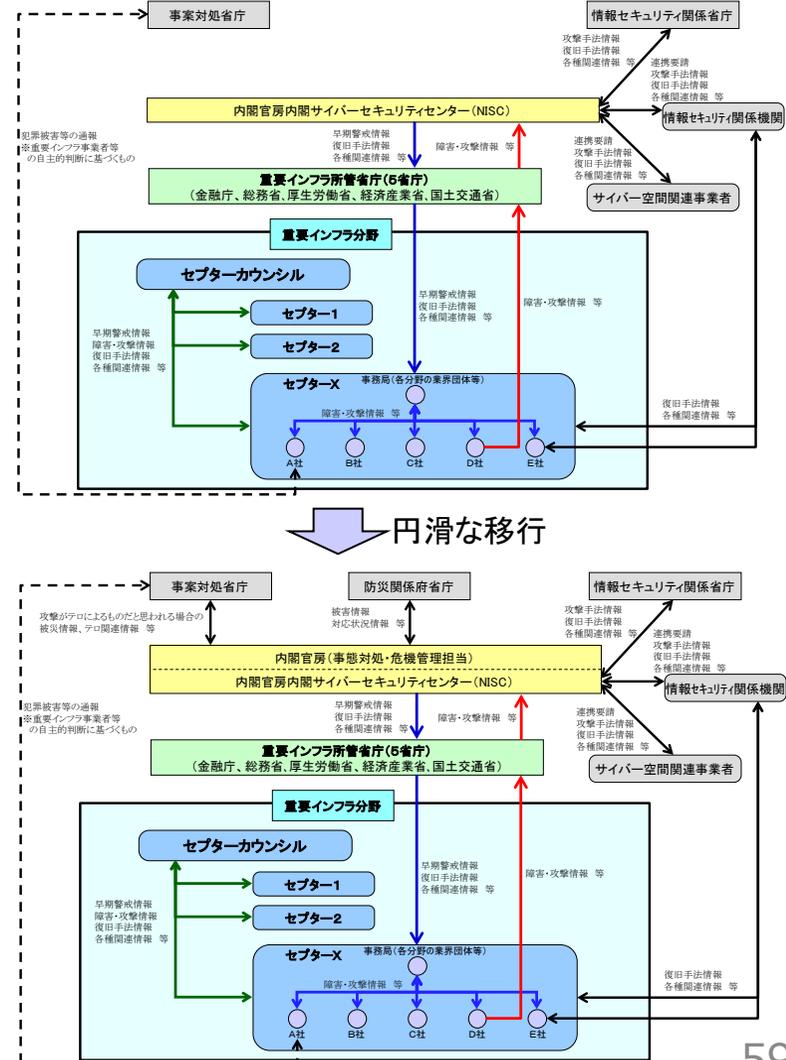
- 多様な関係主体の役割を平時・大規模IT障害発生時に分類して明確化

第3次行動計画に基づく取組

平時

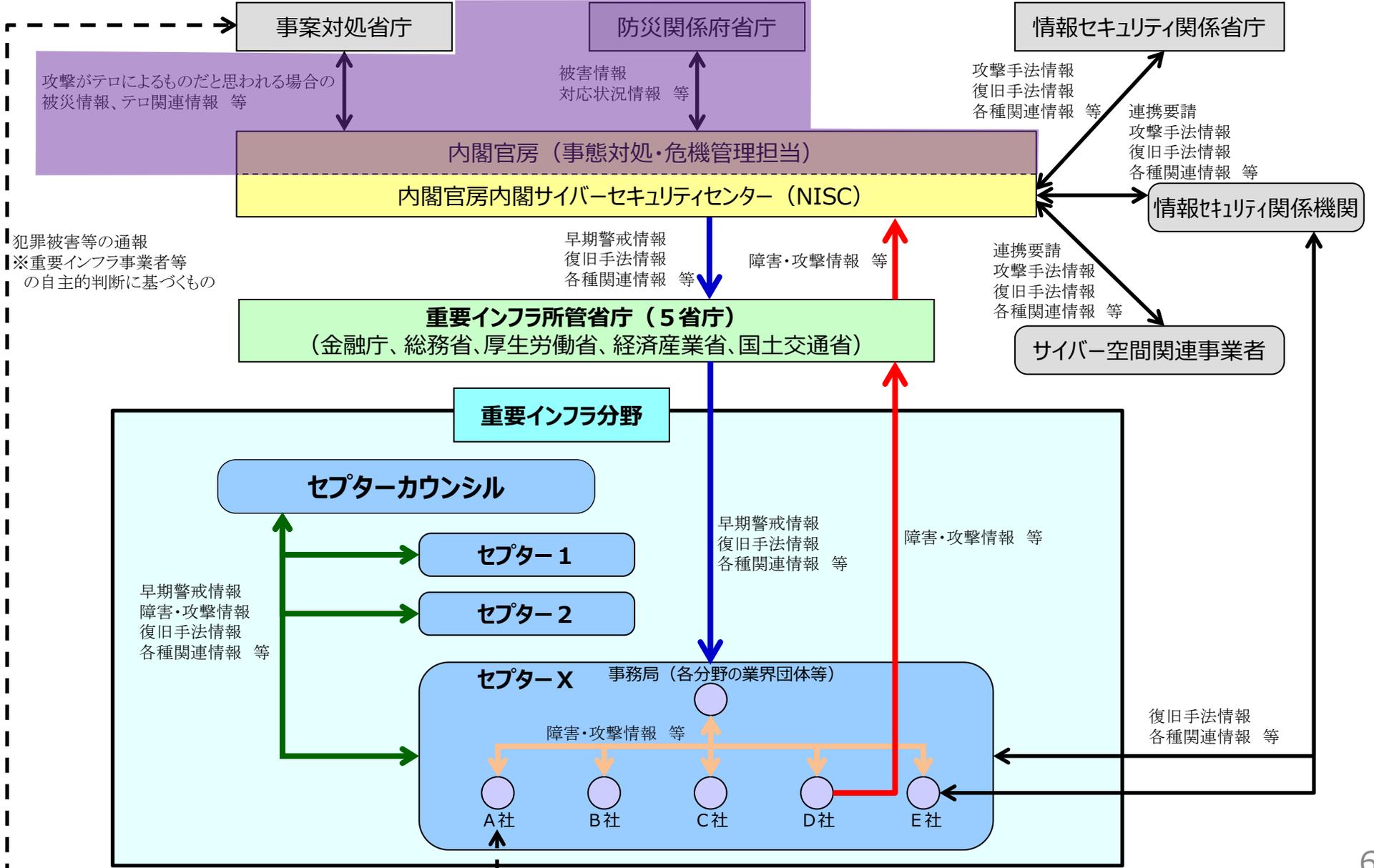
平時の延長線上の体制

大規模IT障害発生時



(参考) 情報共有体制

この部分は大規模IT障害発生時のみ



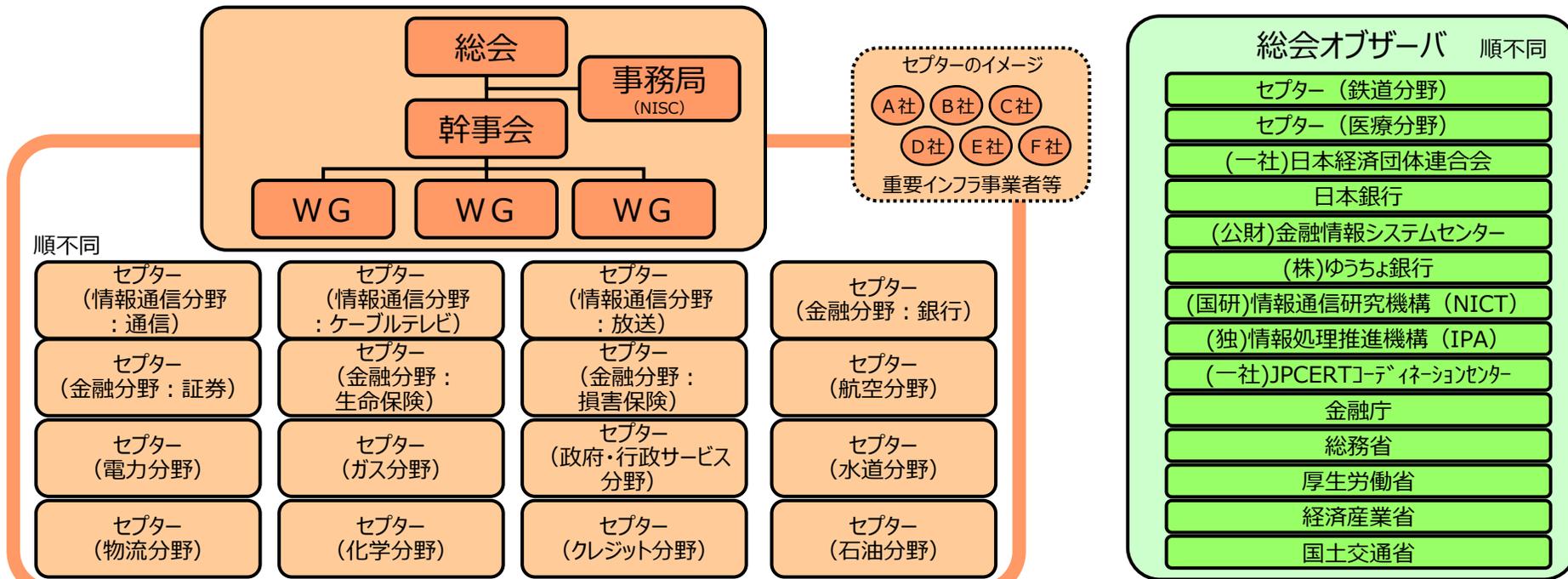
(参考) セプターとセプターカウンシル

セプター (CEPTOAR) Capability for Engineering of Protection, Technical Operation, Analysis and Response

- 重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。
- IT障害の未然防止、発生時の被害拡大防止・迅速な復旧および再発防止のため、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係者間で情報を共有。これによって、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資する活動を目指す。

セプターカウンシル

- 各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
- 分野横断的な情報共有の推進を目的として、2009年2月26日に創設。



(参考) 各分野のセプター一覧

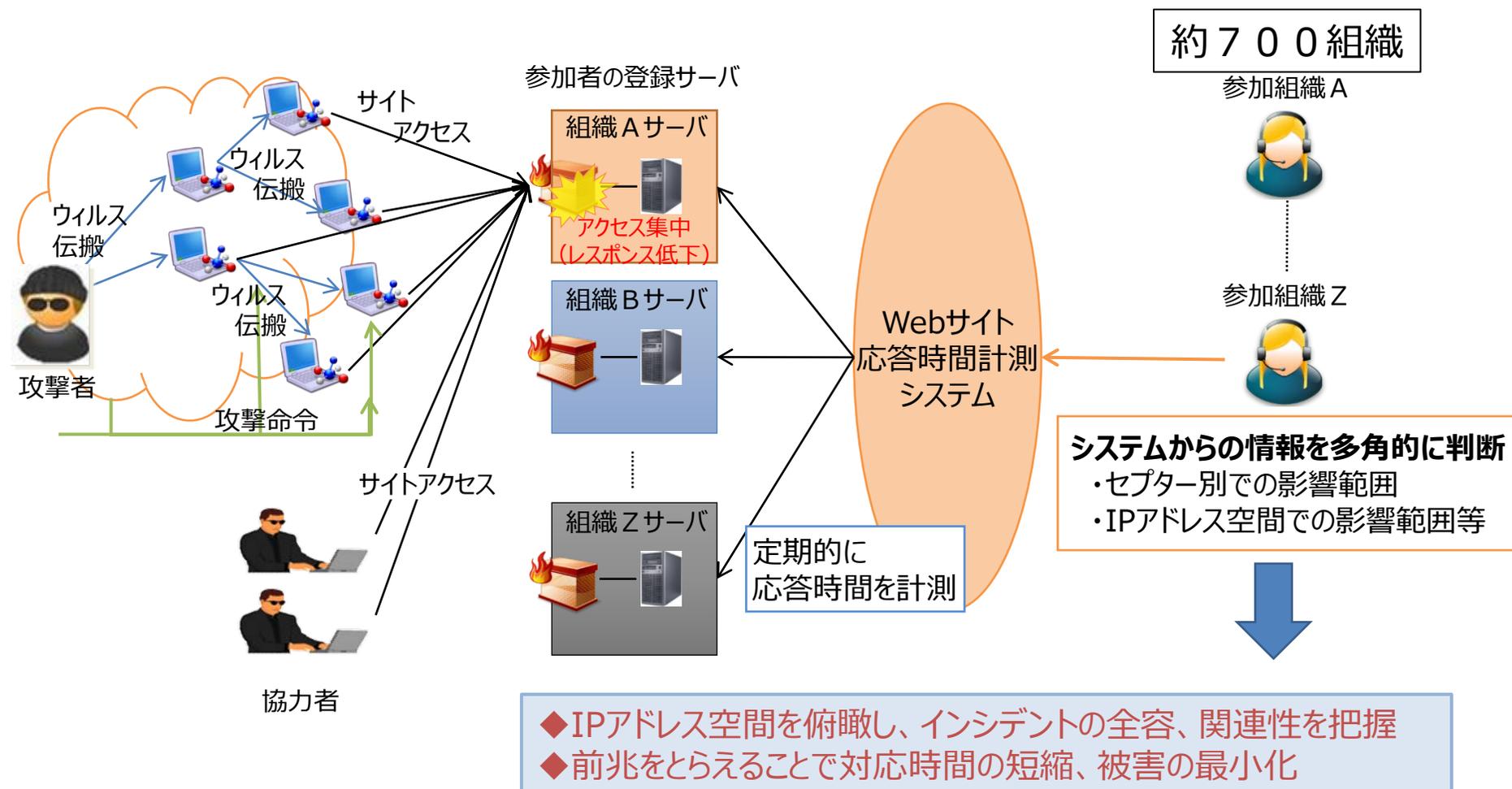
2015年3月末現在

重要インフラ分野	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	化学	クレジット	石油
事業の範囲	電気通信		放送	銀行等	証券	生命保険	損害保険	航空	鉄道	電力	ガス	政府公共団体	医療	水道	物流	化学	クレジット	石油
名称	T-CEPTOAR	ケーブルテレビCEPTOAR	放送CEPTOAR	金融CEPTOAR連絡協議会				航空分野におけるCEPTOAR	鉄道CEPTAOR	電力CEPTOAR	GAS CEPTOAR	自治体CEPTOAR	医療CEPTOAR	水道CEPTOAR	物流CEPTOAR	化学CEPTOAR	クレジットCEPTOAR	石油CEPTOAR
				銀行等CEPTOAR	証券CEPTOAR	生命保険CEPTOAR	損害保険CEPTOAR											
事務局	(一財)日本データ通信協会 テレコム・アイザック推進会議	(一社)日本ケーブルテレビ連盟	(一社)日本民間放送連盟	(一社)全国銀行協会 事務システム部	日本証券業協会 IT統括部	(一社)生命保険協会 総務部組織法務グループ	(一社)日本損害保険協会 IT推進部 共同システム開発室	国土交通省 航空局 安全企画課	国土交通省 鉄道局 総務課 危機管理室	電気事業連合会 情報通信部	(一社)日本ガス協会 技術部	地方公共団体情報システム機構 情報化支援戦略部	厚生労働省 医政局 研究開発振興課 医療技術情報推進室	(公社)日本水道協会 総務部総務課	(一社)日本物流団体連合会	石油化学工業協会	(一社)日本クレジット協会	石油連盟
構成員(内訳)	26社・団体 (固定系の初トランクを有する電気通信事業者、アクセス系の電気通信事業者、ISP事業者、携帯電話事業者等)	310社 (一社)日本ケーブルテレビ連盟の正会員ケーブルテレビ事業者(一社)日本民間放送連盟)	194社・団体 (日本放送協会、地上系民間基幹放送事業者、(一社)日本民間放送連盟)	1,487社 (銀行、信用金庫、信用組合、労働組合、農協等)	254社 7機関 (証券会社、取引所等証券関係機関)	42社 (一社)生命保険協会の定款に定める社員および特別会員)	29社 (オブザーバ3社含む) (一社)日本損害保険協会 情報システム委員会参加会社)	2グループ 3機関 (航空運送事業者、定期航空協会、官庁〔航空局、気象庁〕)	22社 1団体 1機関 (鉄道事業者22社、1団体、官庁〔鉄道局〕)	12社 2機関 (一般電気事業者、日本原電(株)、電源開発(株)、電気事業連合会、電力中央研究所)	10社 (主要な一般ガス事業者10社)	47都道府県 1,741市区町村 (医療機関、(公社)日本医師会、四病院団体協議会(一社)日本医療法人協会、(公社)日本精神科病院協会、(一社)日本病院会、(公社)全日本病院協会、保健医療福祉情報システム工業会)	1グループ 6機関 (医療機関、(公社)日本水道事業者のうち会長都市並びに地方支部長都市) [補足]障害の内容によって、構成員を通じ、全国の日本水道協会の会員水道事業者(1,356事業者)へ情報を提供	8水道事業者 (日本物流団体連合会、日本船主協会、日本内航海運組合総連合会、日本港運協会、日本倉庫協会、全日本トラック協会及び主要な物流事業者16社)	6団体 16社	8社 (主要な石油化学事業者)	18社 (主要なクレジットカード会社等)	15社・グループ (主要な石油精製・元売会社)
緊急窓口	2007年4月運用開始	2012年12月運用開始	2007年4月運用開始										2008年4月運用開始			2015年1月運用開始	2014年4月運用開始	2014年12月運用開始
情報の取扱い	2007年1月制定	2012年11月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2006年9月制定	2007年3月制定	2007年3月制定	2008年3月制定	2008年3月制定	2008年3月制定	2014年12月制定	2014年4月制定	2014年12月制定
情報と連絡手段	障害事例情報等 メール、電話	障害事例情報等 メール、電話	障害事例情報等 メール、電話、FAX、WEB	障害事例情報等 メール、電話、WEB	障害事例情報等 メール、電話、FAX、WEB	障害事例情報等 メール、電話、携帯	障害事例情報等 メール、電話	障害事例情報等 メール、電話	障害事例情報等 メール、電話	脆弱性に関する情報等 メール、電話、携帯、FAX、電子会議室、TV会議、会議体	障害事例情報等 メール、電話、携帯、AX	障害事例情報等 メール、電話、WEB	障害事例情報等 メール、電話、携帯、衛星電話、FAX	障害事例情報等 メール、電話、携帯、衛星電話、FAX	障害事例情報等 メール、電話	障害事例情報等 メール、電話、携帯電話	障害事例情報等 メール、電話	障害事例情報等 メール、電話

(注) 本マップは、各セプターの自主的な整備状況を把握し、マップとして取り纏めたもの。

(参考) Webサイト応答時間計測システム

重要インフラ事業者が登録するWebサイトの応答時間を定期的に計測することで、サイトの動作状況を統計的に監視し、動作異常や外部からの大量のトラフィック等を検知し、複数の観測を複合的に見ることで、異常の早期発見・事実の確認、原因推測をより正確に行い、重要インフラサービス等の被害軽減、サービスの維持、早期復旧を容易にすることを目指す取り組み

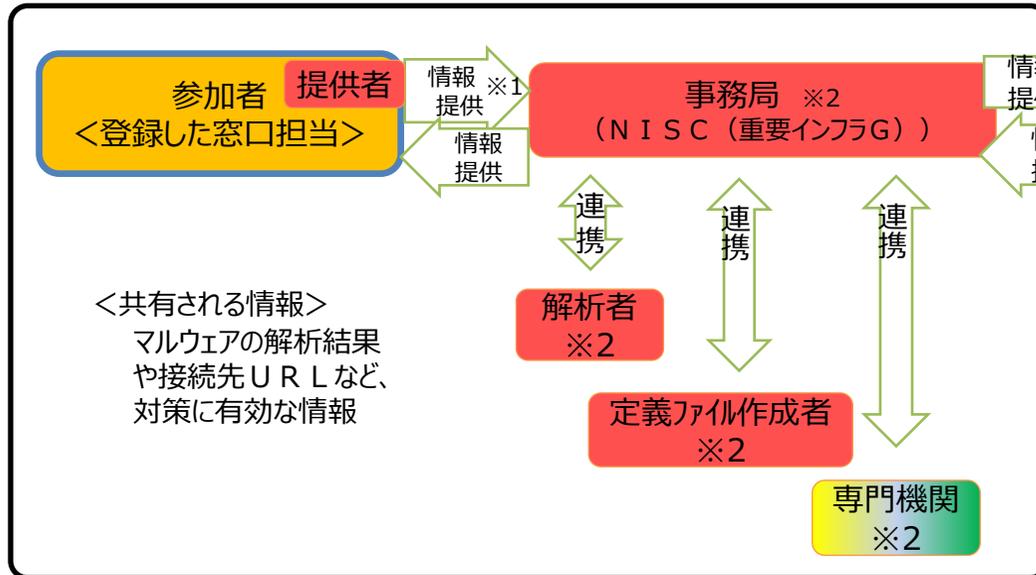


(参考) 標的型攻撃に関する情報共有体制 (C⁴TAP)

C⁴TAP: Ceptoar Councils Capability for Cyber Targeted Attack Protection

重要インフラ事業者において、標的型攻撃が疑われるメールについての一定情報を共有することで、より多くの標的型攻撃に関する情報を収集・共有し、重要インフラサービスへの標的型攻撃の未然防止、もしくは被害軽減、サービスの維持、早期復旧を容易にすることを目指す取組み

<情報共有体制図>



- ※1 情報を扱う者（参加者、解析者等）は、本体制の運用規程を合意し、登録された者
- ※2 情報提供者が、上記類型から、情報の種類毎に、情報共有範囲を指定

<情報共有範囲の類型>

共有範囲のイメージ

Red	情報提供者、事務局及び解析者限り	Red
Amber	Red + 参加者（セブターカウンシル構成員）	Amber
Yellow	Amber + 規程に合意し遵守することを表明したオブザーバ等	Yellow
Green	Yellow + 未参加のカウンシル関係者等	Green
White	公開可能	White

運用規程に合意し遵守することを表明した他の情報共有体制

参加者：約350組織（運用開始時）

第3次行動計画 施策③：障害対応体制の強化

分野横断的演習の更なる充実に加え、IT障害対応に関する他の演習・訓練との連携・役割分担を行うことで、重要インフラ事業者等のIT障害対応能力を高める。

行動計画期間当初の課題

- ▶ 横断的演習の成果の重要インフラ全体への普及・浸透
- ▶ IT障害発生時の対応を踏まえた関係主体の在り方
- ▶ 重要インフラ所管省庁等による演習・訓練との連携等

行動計画期間中の施策

(1) 分野横断的演習の改善

- ▶ 他施策等との連携強化による横断的演習自身の改善
 - ※他施策で得られた知見、最新動向のシナリオへの反映
 - ※演習成果の他施策への反映
- ▶ 成果の浸透
- ▶ 参加対象の裾野拡大

(2) 関係演習・訓練との連携による相乗効果

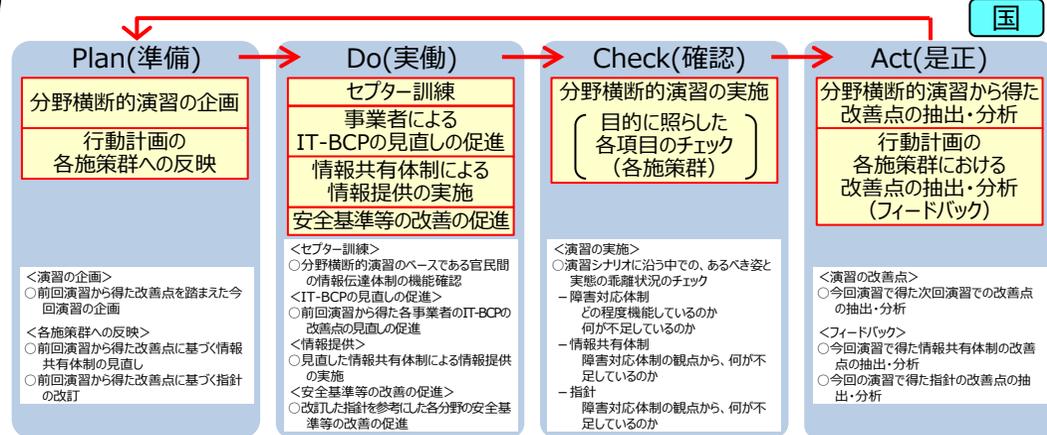
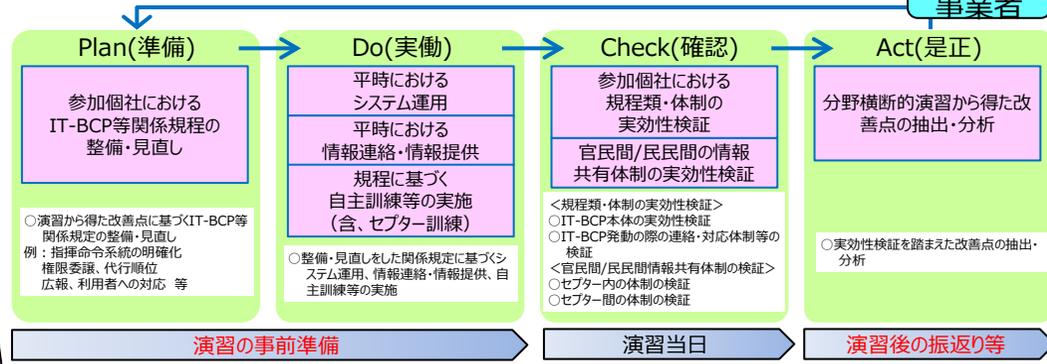
- ▶ セプター訓練・重要インフラ所管省庁による他演習・訓練と相互に連携・補完

第3次行動計画に基づく取組

分野横断的演習の参加者拡大



P D C Aによる改善プロセス例



(参考) 2015年度分野横断的演習 開催概要 ~2006年度より実施~

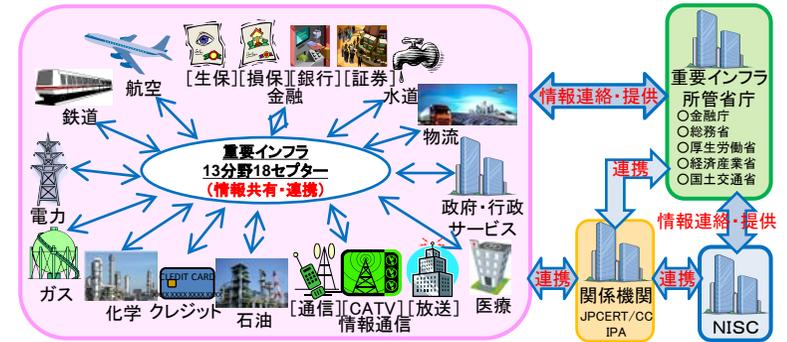
<事前説明会>

- 日時：2015年10月23日(金) 14:00~16:00 他
内容：①NISC各施策の概要説明(第3次行動計画・情報共有体制)
②分野横断的演習の事前説明 等

規程類の事前確認、個別検証課題の確認・調整

<演習当日>

- 日時：2015年12月7日(月) 12:15~18:15
場所：東京会場、大阪会場、自職場
参加者：302組織1168名(内66組織149名が大阪会場、
36組織315名が自職場より参加)
【重要インフラ事業者等：13分野 合計277機関】
【セプター：13分野18セプター】
【関係機関、分野横断的演習検討会有識者、政府機関】



演習内容：2部構成で実施(検証課題に対する参加事業者等の理解を深める効果を狙ったもの)

- 第1部 各分野においてサービスへの影響が小さいIT障害が発生したことを想定し、分野間・官民間での連携を図ることによる情報共有体制の実効性を検証。
- 第2部 サービスへ影響が生じるIT障害が発生し、事業継続が脅かされる事態を想定し、事業継続計画の発動方法や、その手順を確認するなど、事態への対処を検証。

演習を通じた内規・体制等の課題抽出



<意見交換会>

- 日時：2016年1月22日(金) 午後を予定
内容：①分野をまたいだ事業者等間での情報共有(グループディスカッション)
②分野横断的演習の中間報告

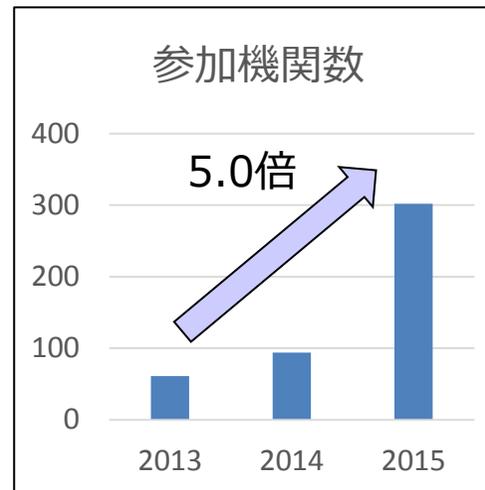
他事業者等との情報共有を通じた改善の促進



(参考) 分野横断的演習の参加実績

2006年度より実施、今年度が10回目

	参加機関数	参加者数
2013年度実績	61組織 (38事業者等)	212名
2014年度実績	94組織 (70事業者等)	348名
2015年度実績	302組織 (277事業者等)	1,168名



※277事業者中、208事業者が初参加



演習の様様(遠藤大臣による視察)



全体振り返りの様様

(参考) 分野横断的演習 シナリオの流れ

【第1部】標的型攻撃

ポイント：情報共有体制、インシデントの初動対応

12:45

(JPCERT/CCによる早期警戒情報)

マルウェア感染と思われる不審な通信の検知

(影響範囲・原因等の初期調査)

マルウェア感染の原因と思われる不審な電子メールの受信実績を把握

(一部事業者等によるNISCへの情報連絡)

(一部事業者等による情報開示)

13:45

NISCからの情報提供

(復旧方法や対策の継続的な対応)

14:15

【第2部】DDoS攻撃／OS脆弱性／制御システム

ポイント：障害対応体制、内部的な判断、意志決定、インシデントの本格対応

15:00

2-a)
DDoS攻撃による重要インフラサービス障害発生

2-b)
OS等における脆弱性を突いた攻撃による重要インフラサービス障害発生

2-c)
制御システムのマルウェア感染による重要インフラサービス運用トラブル発生

(システム監視状況／影響調査／復旧方法の検討／体制構築)

(IT-BCP等発動等の判断時に発動権限者と連絡が取れない状況の発生)

(一部事業者等によるNISCへの情報連絡)

15:45

NISCからの情報提供

(復旧方法や対策の継続的な対応)

16:30

第3次行動計画 施策④：リスクマネジメント

重要インフラ事業者等がその事業目的であるサービスの持続的提供を実現するために実施するリスクマネジメントを支援する。

行動計画期間当初の課題

- ▶ 重要インフラ事業者等において、事業目標達成に向け必要なリスクマネジメントの訴求
- ▶ 環境変化等に応じて生じ得るリスク源、多大な影響が生じうる環境変化の中長期的な調査

行動計画期間中の施策

(1) リスクマネジメントの標準的な考え方

- ▶ リスクマネジメントは自らの状況把握をし、各重要インフラ事業者等がそれぞれにおいて主体的に実施
- ▶ 防護基盤強化のため作成する手引書等の利活用
※国際標準への準拠を求めるものではなく、自組織のリスクマネジメントの更なる最適化等が目的。

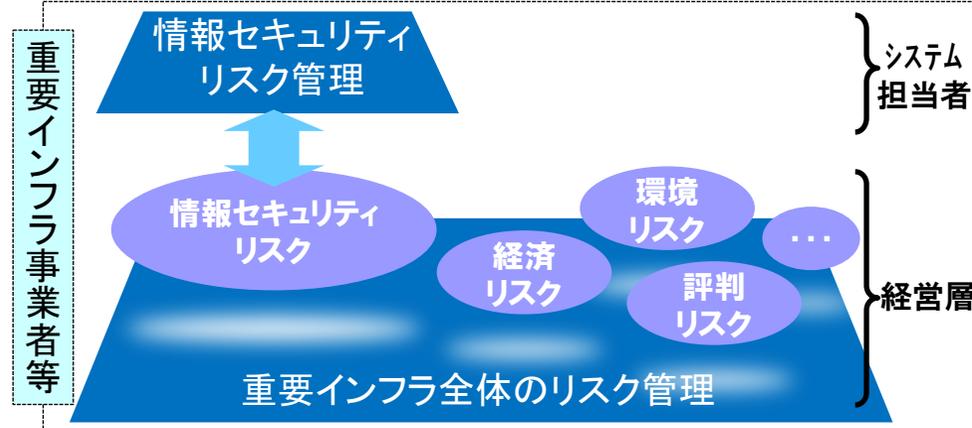
(2) リスクマネジメントの内閣官房による支援

- ▶ リスクアセスメントの支援
 - ・環境変化調査
 - ・相互依存性解析（IT依存度調査含む）
- ▶ リスクコミュニケーション及び協議の支援

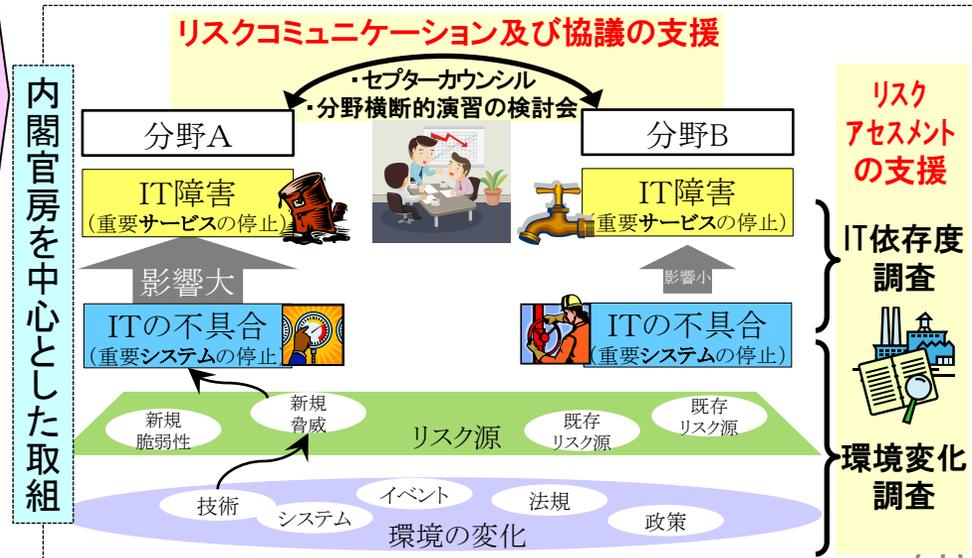
(3) 他施策との相互反映プロセスの確立

- ▶ 環境変化調査、相互依存性解析の結果 ⇒ 他施策
- ▶ 他施策で顕在化したリスク等 ⇒ 調査・解析対象

第3次行動計画に基づく取組



支援

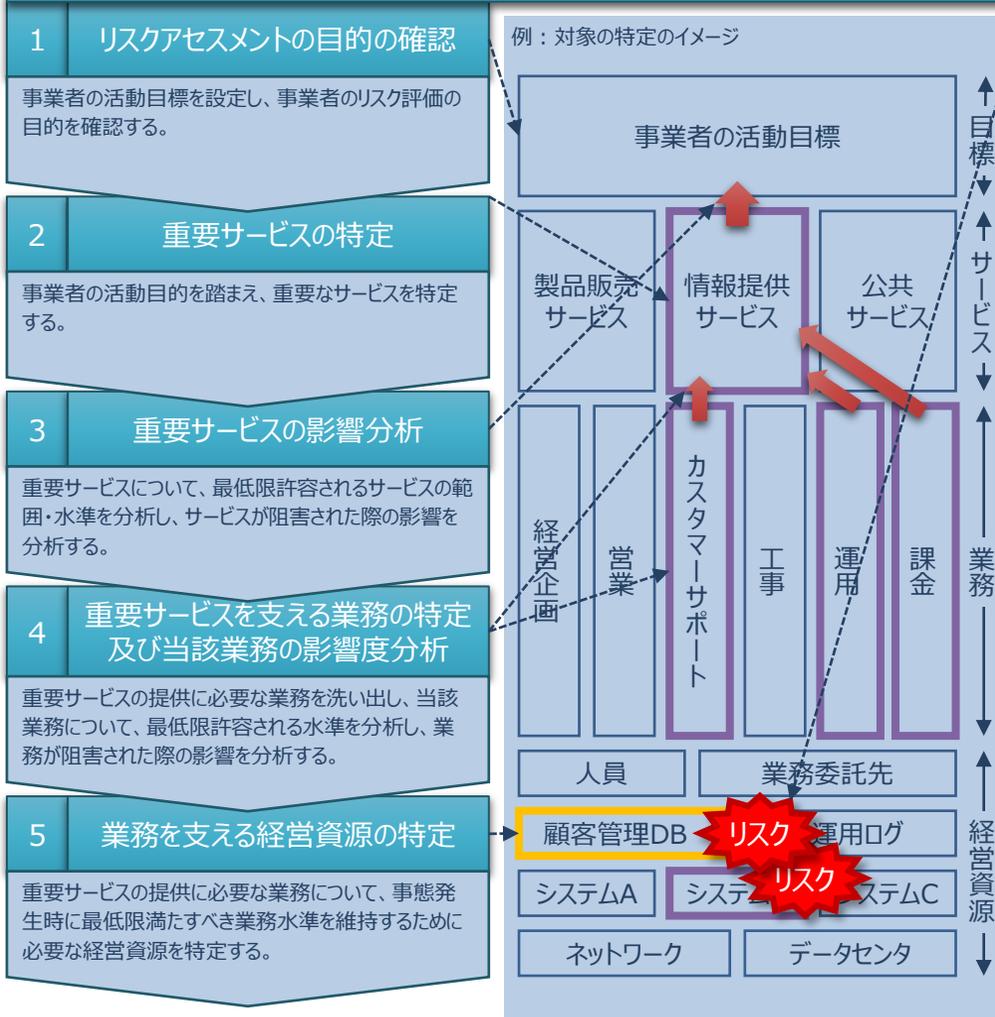


リスク評価手順の全体像（検討中）

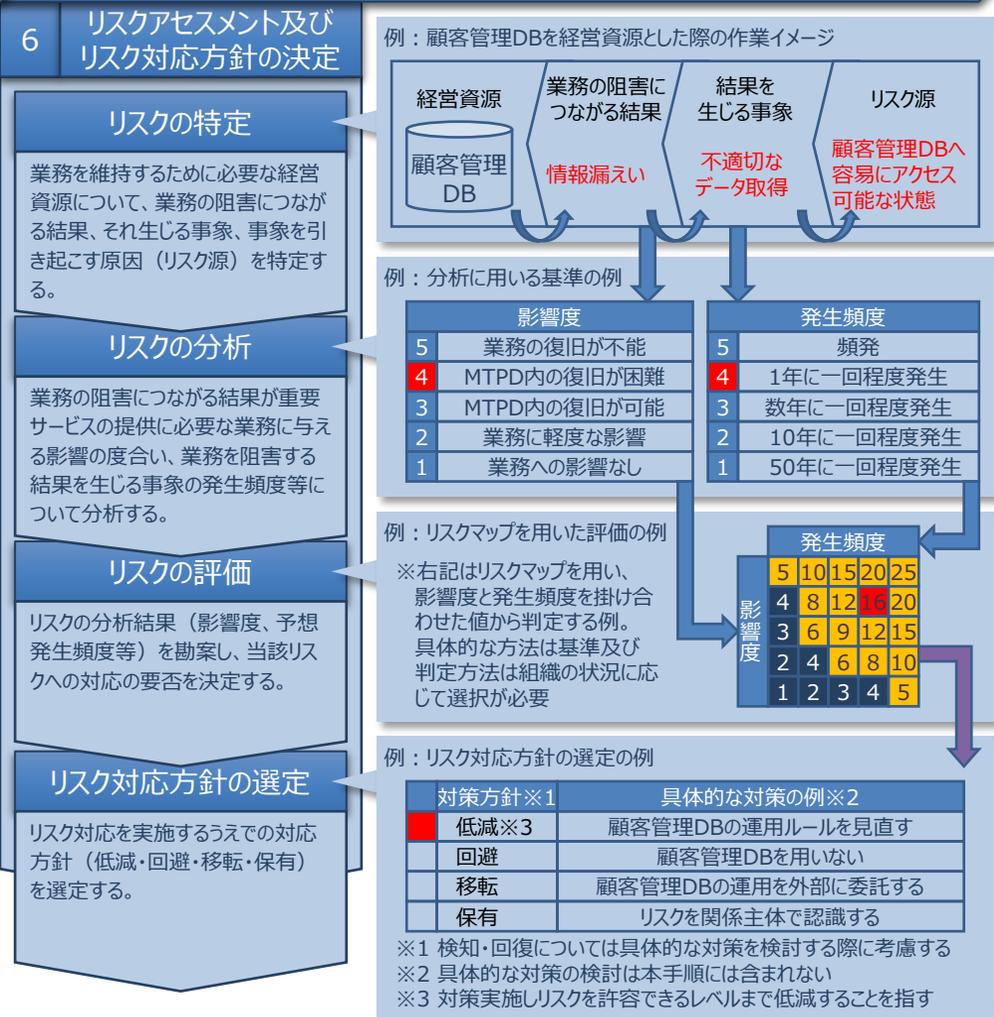
コンセプト

- 事業者の活動目標を阻害しうる不確かさの影響をリスクと捉える。
- 活動目標に照らして守るべき対象を特定し、防ぐべき結果からリスクを特定・分析・評価する。

リスクアセスメントの対象を特定するフェーズ



リスクアセスメントを実施するフェーズ



第3次行動計画 施策⑤：防護基盤の強化

広報公聴、国際連携、関係規程類、国際基準等の手引書作成等、重要インフラ防護の全体を支える共通基盤的な取組を強化する。

行動計画期間当初の課題

- 広報公聴の一層の充実
- 二国間、地域間、多国間の枠組みの積極的な活用を通じた国際連携の強化
- 参照すべき規程類の整備・活用 等

行動計画期間中の施策

(1) 広報公聴

- 行動計画及びその取組について、広く認識・理解を得るための公報広聴活動の充実

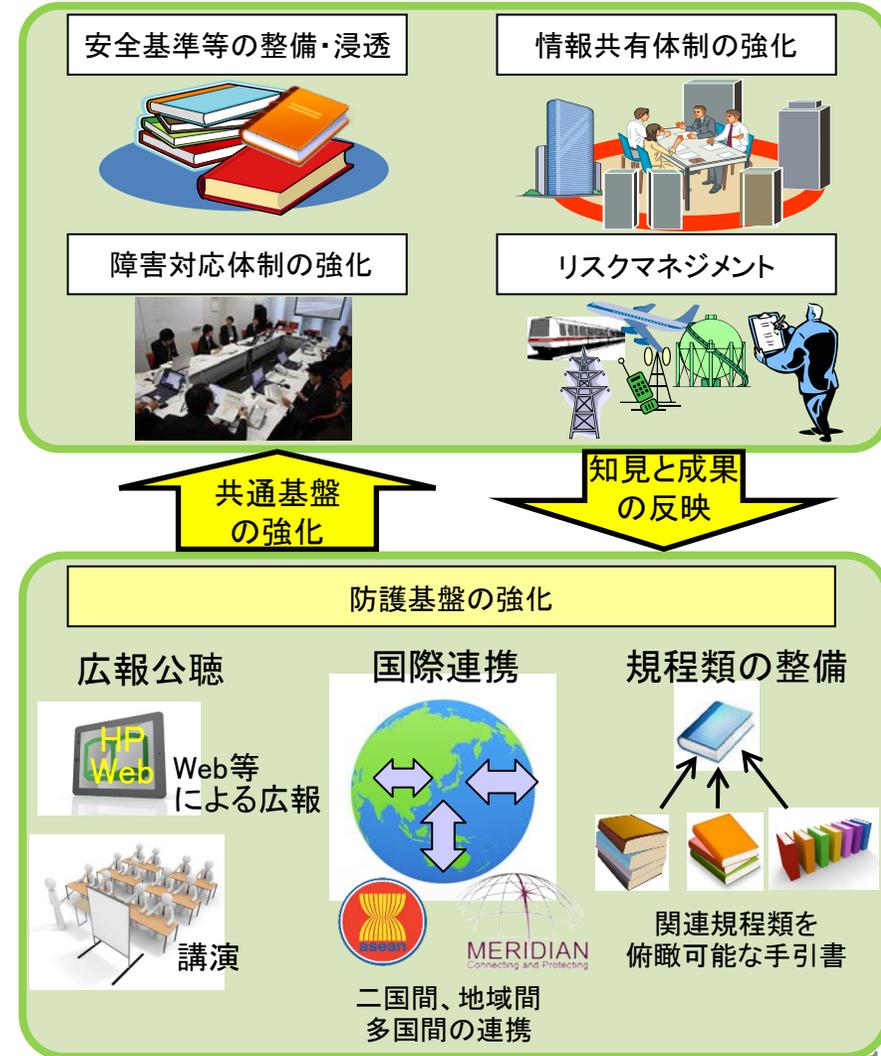
(2) 国際連携

- 欧米、A S E A N、Meridian等二国間、地域間、多国間の枠組みの積極的な活用を通じた国際連携

(3) 規程類の整備

- 重要インフラ防護に係る関連規程集の発行
- 国際基準等の適用の際の手引書等の整備
- 情報セキュリティに関する評価・認証制度の拡充の支援

第3次行動計画に基づく取組



サイバーセキュリティ経営ガイドライン

- サイバー攻撃対策は、IT を利活用する限り避けて通れない経営課題。
- 企業経営者を対象に、対策を推進するためのリーダーシップのとり方について、ガイドラインを策定。
(平成27年12月)

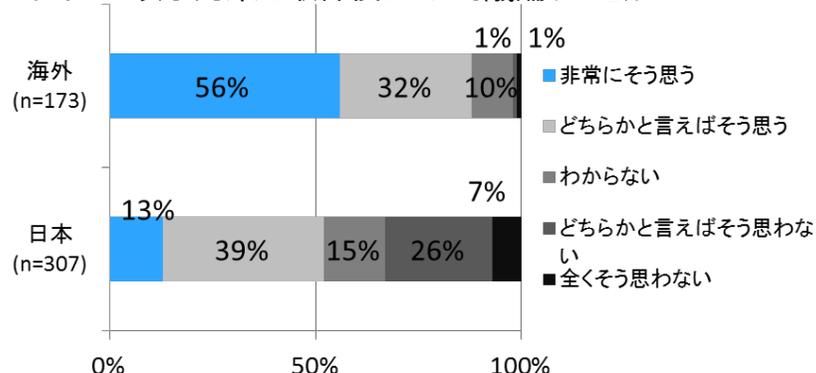
【サイバー攻撃リスクは経営課題】

- Web サーバーに対する不正アクセスにより個人情報が流出した懸念が発生。
- 結果として4 半期純利益を大幅に下方修正した事例あり。

【サイバー攻撃対策が経営問題として考えられていない】

- 海外の企業と比べ、サイバー攻撃対策について取締役レベルの問題と考える我が国企業は少ない

サイバー攻撃対策は取締役レベルで議論すべきか



(出典) KPMGジャパン「KPMG Insight 日本におけるサイバー攻撃の状況と課題 -セキュリティサーベイ2013から-」より経済産業省作成

【サイバーセキュリティ経営ガイドラインの概要】

1. サイバーセキュリティ経営の3原則

- 経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
- 自社のみならず、ビジネスパートナーを含めた対策が必要
- 平時及び緊急時のいずれにおいても、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

2. サイバーセキュリティ経営の重要10項目の概要

- リーダーシップの表明と体制の構築**
(サイバーセキュリティリスクを認識し、体制構築を指示)
- サイバーセキュリティリスク管理の枠組み決定**
(P D C Aの仕組みを作らせ、経営者も適時状況を把握)
- リスクを踏まえた攻撃を防ぐための事前対策**
(対策に必要な資源(予算、人材等)の確保)
- サイバー攻撃を受けた場合に備えた準備**
(緊急時の対応体制の整備と演習の実施、経営者の説明準備)

サイバーセキュリティ経営ガイドライン

<http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html>

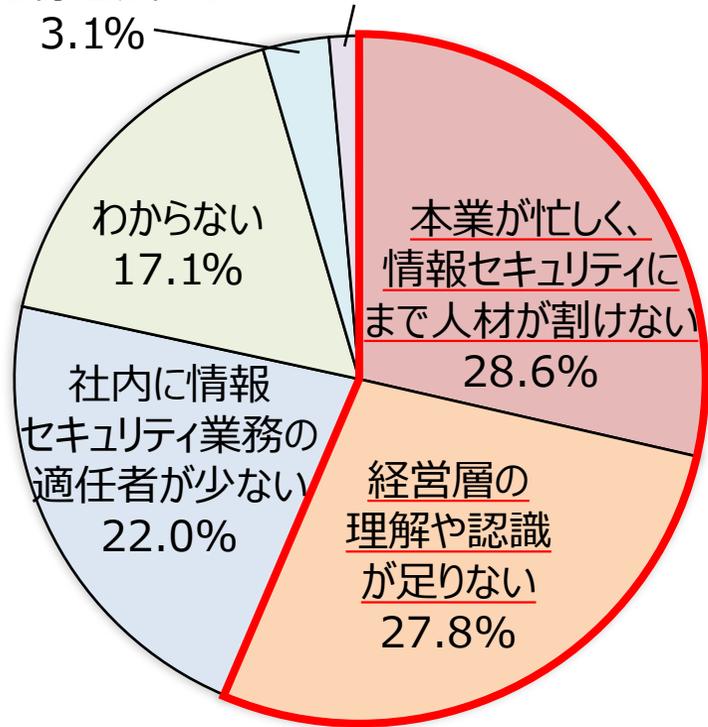
企業等における情報セキュリティ対策の現状

- 企業では情報セキュリティに関する業務に従事する人員が不足。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。

人員不足の原因（社内向け業務）

N=1,736

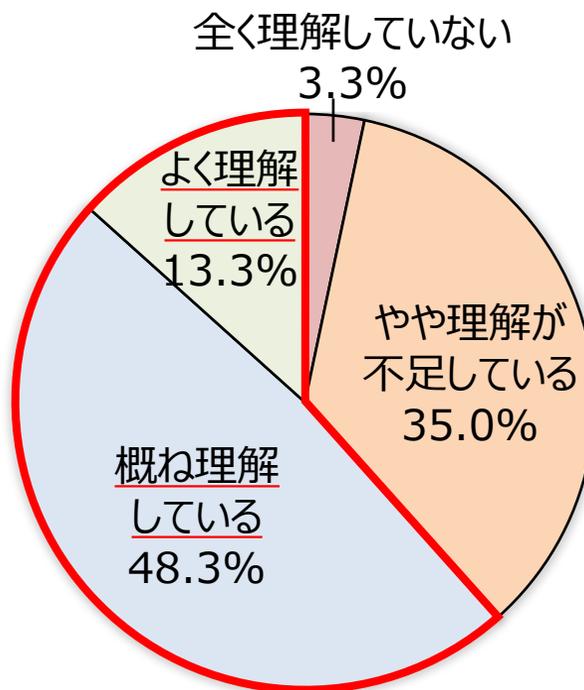
採用をしたいが、
情報セキュリティ業務 への応募者が少ない
その他



経営層の認識・理解度

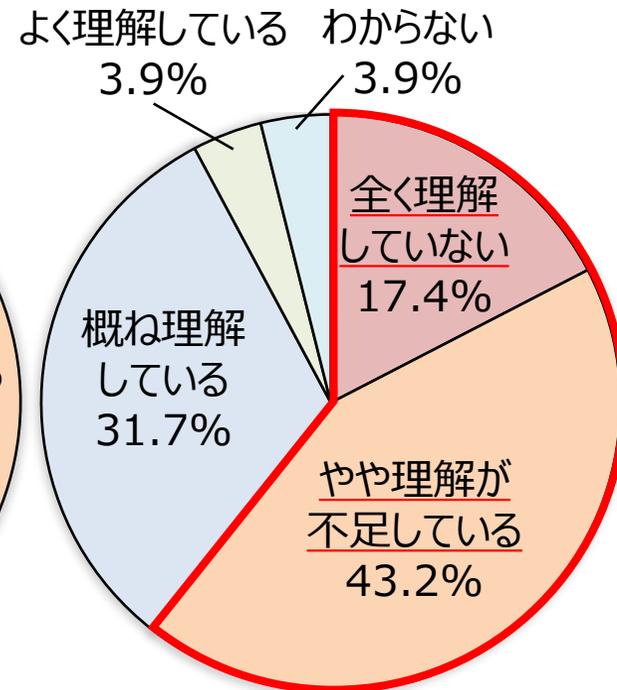
経営層自身 N=180

(6割が理解していると回答)



経営層以外 N=2,731

(6割が理解していないと回答)



サイバーセキュリティに関するリスク開示（有価証券報告書）

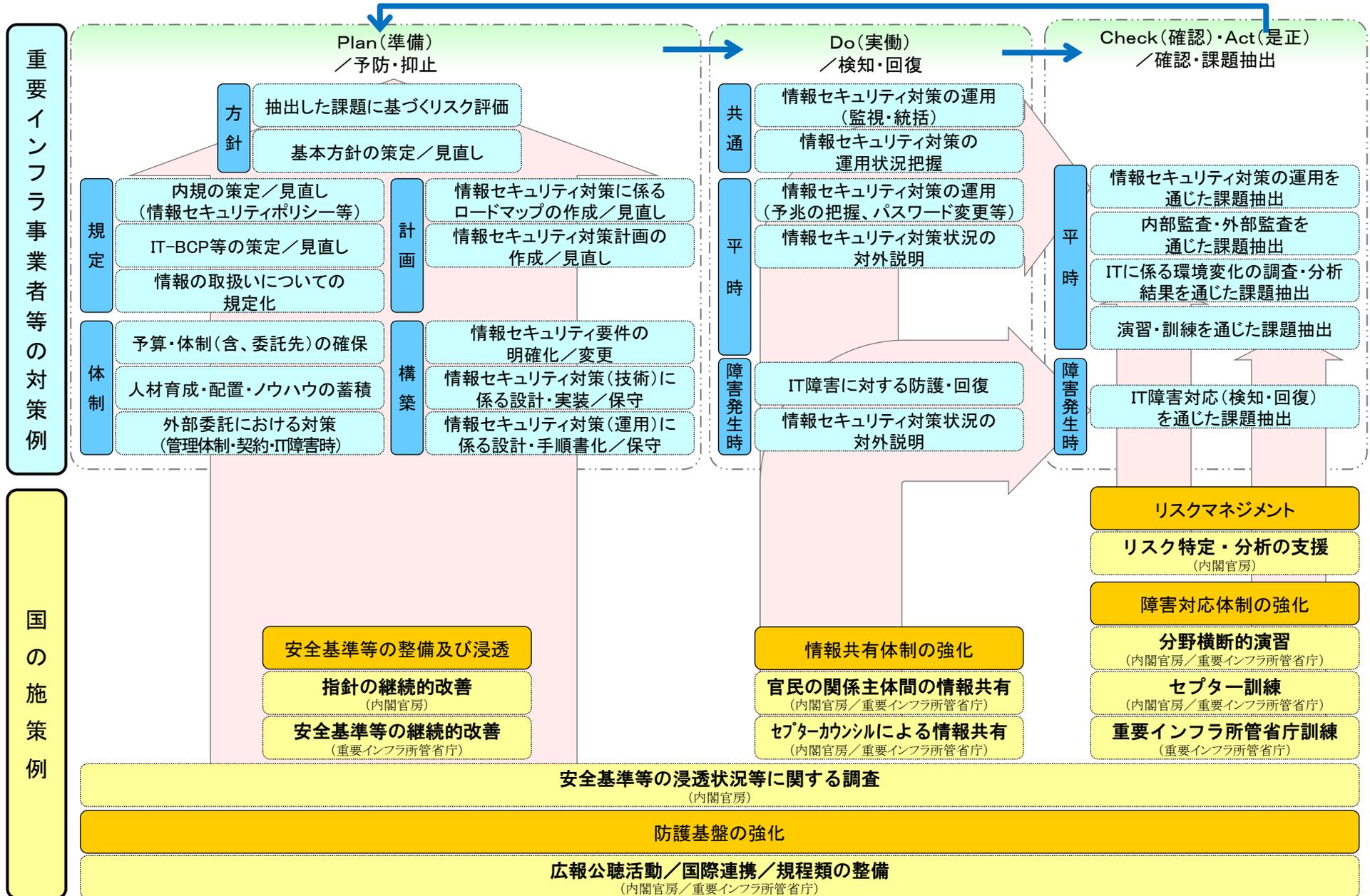
上場企業225社（日経225）の平成21～25年度の5年間を対象「事業等のリスク」へのサイバーセキュリティリスクの記載状況の調査・分析

- 開示企業数は、平成21年度の52%（116社）から**平成25年度の60%（136社）**へと増加。
- 業種別では、通信、銀行、証券、保険、小売業、石油、造船、電力、ガス等の**14業種が100%（合計51社）**。
- 繊維、パルプ・紙、鉄鋼等の**4業種は0%（合計14社）**。
- 素材産業全体（64社）では開示割合が32.8%と低く、**原材料費や為替の影響等のリスクと比べ、サイバーセキュリティリスクの認識が相対的に低い**と考えられる。
- サイバーセキュリティリスクの**記載文書が5年間同一の企業（65社）**には、その記載の仕方が包括的で意味が広く捉えられる（想定インシデント・被害が具体的な）ものが多かった。
- 自社で発生したサイバーセキュリティインシデントを記載している企業は**調査対象企業中4社**と少なかった。

平成25年度 日経225社-業種別サイバーセキュリティ情報開示状況

大分野	日経業種分類		開示企業数	開示企業%		
	(社数)	中分野 (社数)		中分類	大分類	
A 技術	57	01 医薬品	8	2	25.0%	61.4%
		02 電気機器	29	20	69.0%	
		03 自動車	9	4	44.4%	
		04 精密機器	5	3	60.0%	
		05 通信	6	6	100.0%	
B 金融	21	06 銀行	11	11	100.0%	100.0%
		07 その他金融	1	1	100.0%	
		08 証券	3	3	100.0%	
		09 保険	6	6	100.0%	
C 消費	28	10 水産	2	1	50.0%	85.7%
		11 食品	11	10	90.9%	
		12 小売業	8	8	100.0%	
		13 サービス	7	5	71.4%	
D 素材	64	14 鋳業	1	0	0.0%	32.8%
		15 繊維	5	0	0.0%	
		16 パルプ・紙	3	0	0.0%	
		17 化学	18	5	27.8%	
		18 石油	2	2	100.0%	
		19 ゴム	2	1	50.0%	
		20 窯業	9	3	33.3%	
		21 鉄鋼	5	0	0.0%	
		22 非鉄・金属	12	5	41.7%	
		23 商社	7	5	71.4%	
E 資本財・その他	35	24 建設	8	4	50.0%	51.4%
		25 機械	16	8	50.0%	
		26 造船	2	2	100.0%	
		27 その他製造	3	3	100.0%	
		28 不動産	6	1	16.7%	
F 運輸・公共	20	29 鉄道・バス	8	7	87.5%	85.0%
		30 陸運	2	2	100.0%	
		31 海運	3	1	33.3%	
		32 空運	1	1	100.0%	
		33 倉庫	1	1	100.0%	
		34 電力	3	3	100.0%	
		35 ガス	2	2	100.0%	
合計	225		225	136		

「重要インフラ事業者等による対策例」と各対策に関連する「国の施策例」

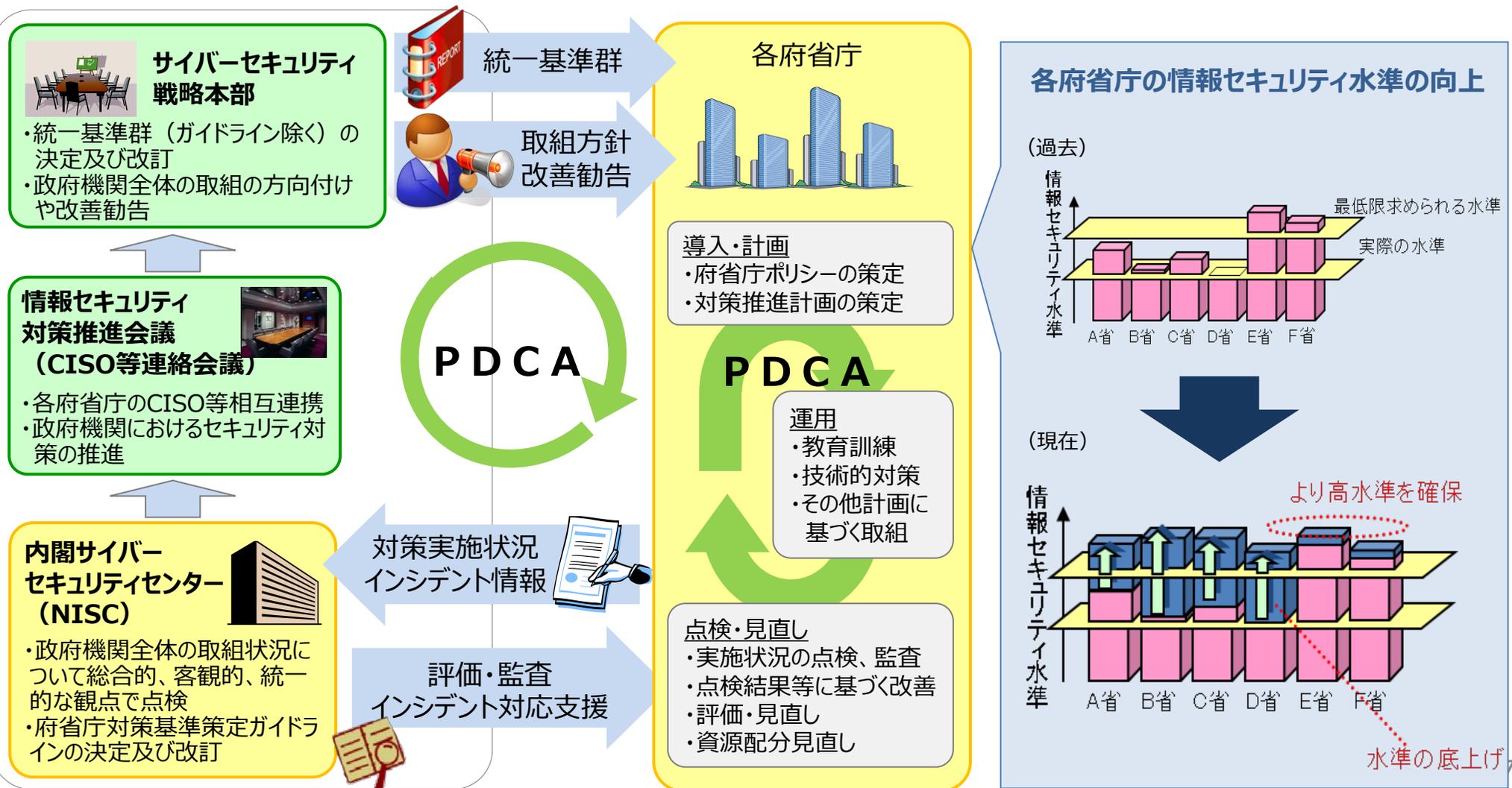


• **政府機関、国民への対応**

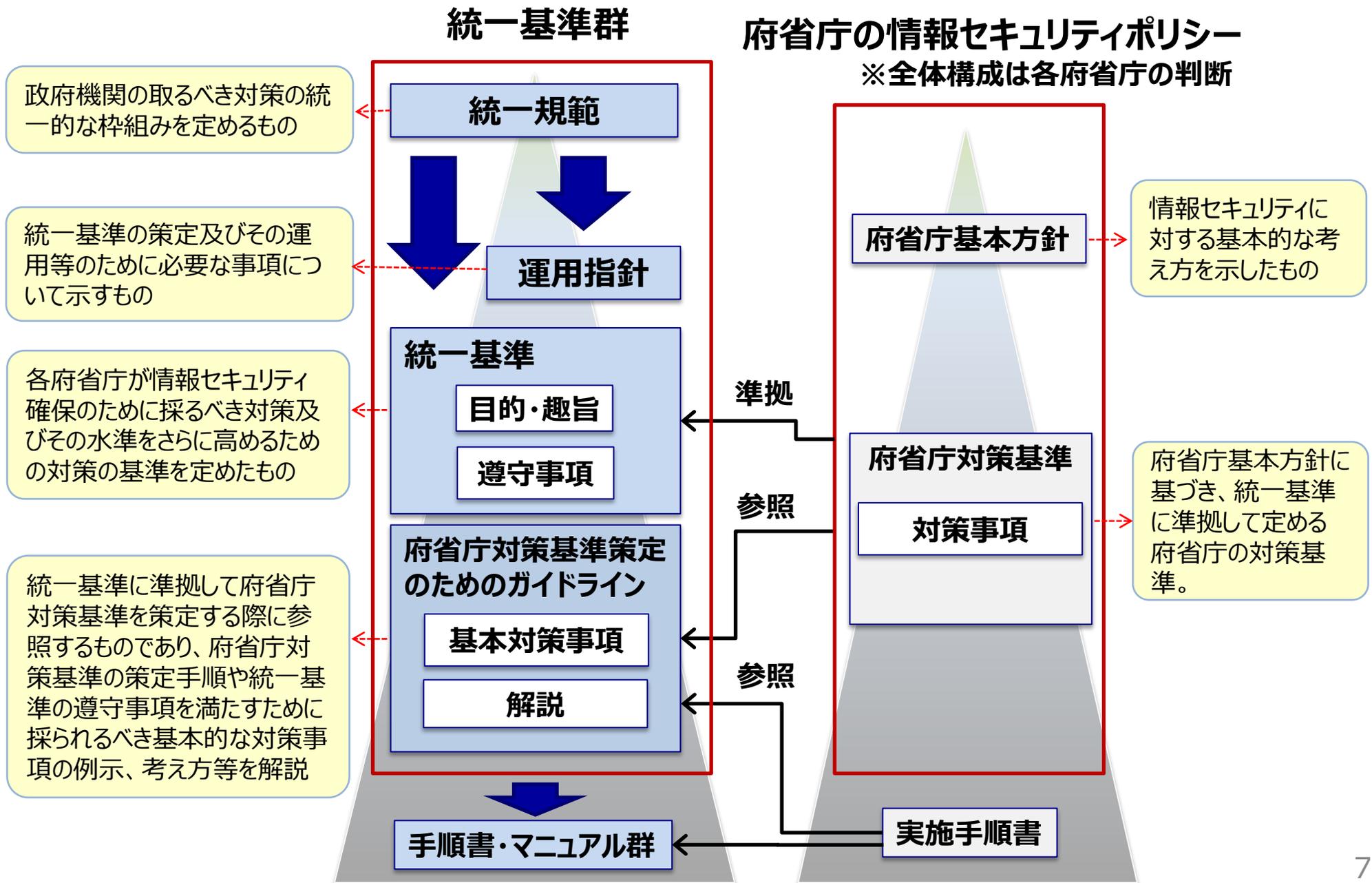
- 政府自身のセキュリティへの取組
- 国民全体への取組
- 2020年に向けた取組

政府機関の情報セキュリティ対策のための統一基準群

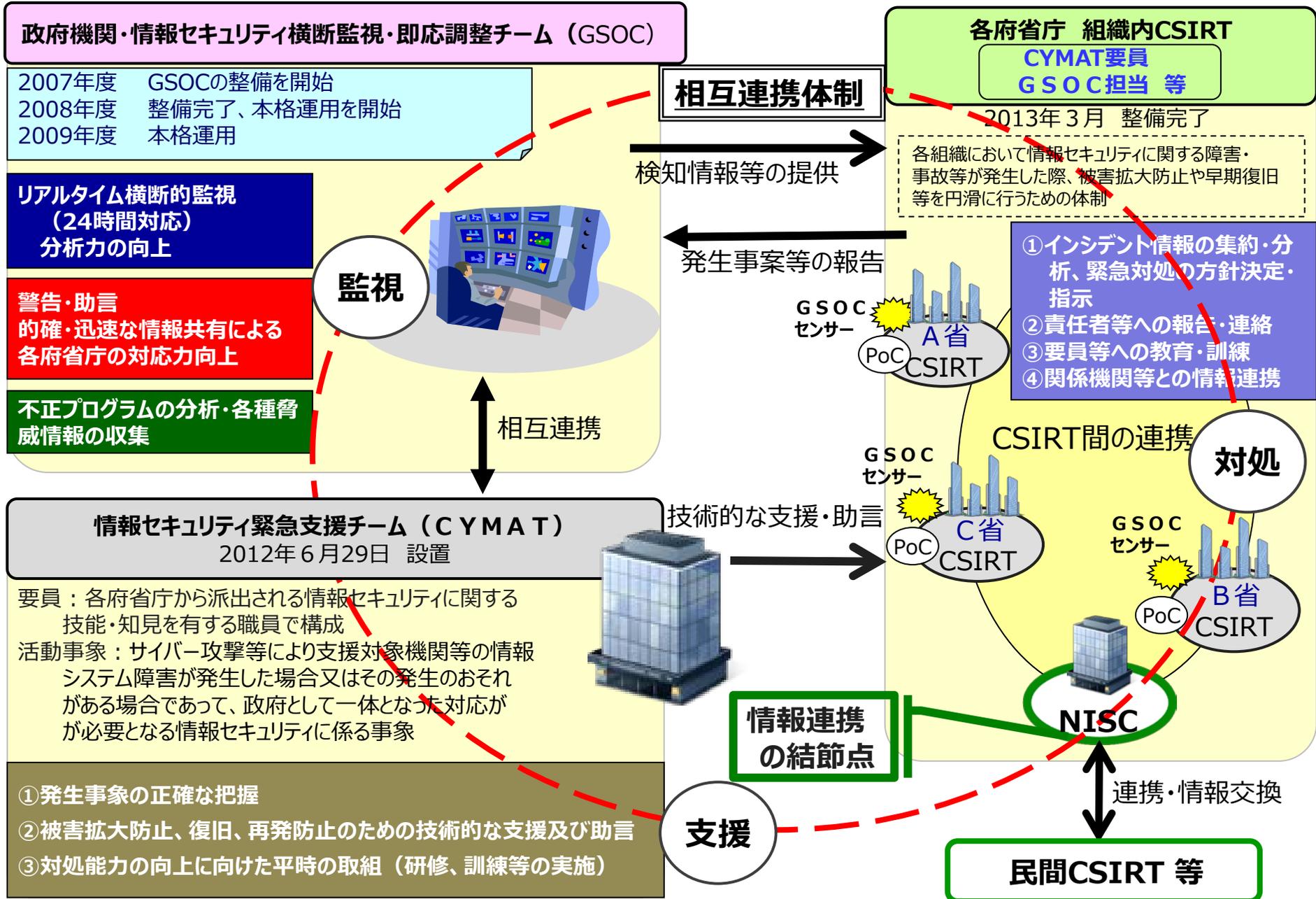
- 「政府機関の情報セキュリティ対策のための統一基準群」（以下、「統一基準群」という。）は、政府全体の情報セキュリティ水準を向上させるための統一的な枠組み。
- 各府省庁は、統一基準に準拠した情報セキュリティポリシー及び、対策推進計画を策定し、対策を実施する。



統一基準群と府省庁のセキュリティポリシー



政府機関等における体制



サイバーセキュリティ対策を強化するための監査に係る基本方針

1 監査の目的

サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、対策強化のための自律的かつ継続的な改善機構であるP D C Aサイクルが継続的かつ有効に機能するよう助言し、対策の効果的な強化を図る。

2 監査の対象

国の行政機関 ※独立行政法人については、当面、特に必要があると認める場合に監査の対象とする。

3 監査の基本的な方向性

(1) 助言型監査

- 有益な助言を行う。
- グッドプラクティスを共有。

(2) 第三者的視点からの監査

- 内部監査とは独立した監査を実施。

(3) 各機関の状況を踏まえた監査

- 実施状況、体制の整備状況等を踏まえ、監査を実施。
- 発展段階に応じて、監査の内容も段階的に発展。

(4) サイバーセキュリティに関する情勢を踏まえた監査テーマの選定

- 重要性・緊急性・リスクの高いものから監査テーマを適切に選定。

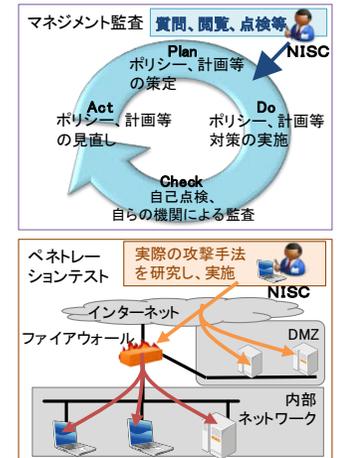
4 監査の実施内容

(1) マネジメント監査

- 国際規格において基本的な考え方である組織全体としてのP D C Aサイクルが有効に機能しているかとの観点から検証する。
- 対策を強化するための体制等の整備状況を検証し、改善のために必要な助言等を行う。

(2) ペネトレーションテスト

- 疑似的な攻撃を実施することによって、サイバーセキュリティ対策の状況を検証し、改善のために必要な助言等を行う。



5 監査の進め方 ※監査事務については、内閣サイバーセキュリティセンターが実施する。

(1) 監査方針の策定

- 年度ごとの監査の基本的な考え方を含む年度監査方針を、年次計画の一部として策定。

(2) 監査の実施

- 必要に応じて外部専門家が協力。
- 過年度の監査実施結果のうち重要な事項については、改善状況を継続的にフォローアップ。

(3) 個別の監査実施結果の通知

- 監査実施結果を、各機関の最高情報セキュリティ責任者（C I S O）へ通知。
- 各機関は、速やかに必要な改善を実施又は改善計画を策定し、改善結果又は計画を報告。

(4) 監査実施結果の取りまとめ・報告

- サイバーセキュリティの特性を踏まえ、攻撃者を利することのないよう配慮しつつ、当該年度に実施した監査の結果を取りまとめ。
- サイバーセキュリティ戦略本部に報告。

サイバーセキュリティ月間（2月1日～3月18日） 2015年分

- 国民のサイバーセキュリティに関する意識を向上させるため、行事の開催や広報等の普及啓発活動を集中実施。
- 新しい取組として**サイバーセキュリティ・カフェ**や**競技形式の訓練**、検索ポータルサイトと連携した意識調査などを実施。また、前年に定評のあった**日替わりコラムの掲載**を実施。

イベントの開催

●キックオフ・シンポジウム（2月2日）

月間のキックオフイベントとして、サイバーセキュリティの現状と対策等に関するシンポジウムを開催



●サイバーセキュリティ・カフェ（月間期間中に実施予定）

コーヒーを片手にサイバーセキュリティについて耳を傾け学んでもらう、市民参加型イベント。ネットでの動画配信も実施。



●サイバーセキュリティ訓練（総務省との共催）

「現場」における実効的なインシデント・ハンドリング能力向上に向け、府省庁対抗による、競技形式の事案対処訓練を実施。

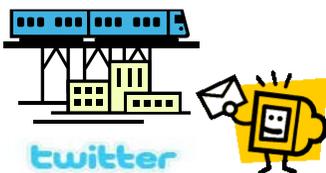
トップメッセージ発信

月間に関するメッセージを
発信。記者会見、HP等を
活用し周知。



各種媒体の活用

マスメディア、電車広告、
メールマガジン、Twitter、
政府広報等を通じ各種情
報を提供



専用HPの更新

「国民を守る情報セキュリ
ティサイト」月間用ページ
コラム「サイバーセキュリティ
ひとこと言いたい！」掲載

（多様な業種・職種の皆様（50
名程度）がコラムを執筆）

その他官民による関連行事

様々な関連行事を集中的に開催

- サイバーセキュリティに関する講習等（都道府県警察）**
小中高校等を対象に、サイバー犯罪の現状、検挙事例等を説明
- e-ネット安心講座（総務省、文部科学省等）**
保護者等を対象とした子供たちをネットトラブルから守るための講座
- インターネット安全教室（経済産業省等）**
家庭や学校におけるネット利用の基礎知識を学習

その他、産学官民の様々な主体により関連行事を開催

周知用素材の作成・配布

ポスター、シール

リーフレット



ロゴマークの活用



Yahoo!ニュース 意識調査への設問提供



官民連携の推進

イベントの共催、講師派遣等

月間バナーと企業等バナーを
相互のウェブサイトに掲載

情報セキュリティ普及啓発ロゴマーク



情報セキュリティ普及啓発ロゴマークは、産官学民連携した情報セキュリティ普及啓発を一層推進するため、有識者等の御意見を賜り、定められた。

本ロゴマークについては、政府機関だけでなく、広く関係機関・団体、企業等にも、長期間、様々なイベントに使用していただき、効果的なPR活動に役立たせ、誰もが安心して情報通信技術の恩恵を享受し、国民一人ひとりが情報セキュリティについての関心を高めてほしいという願いが込められている。

- 中央の球体は国際社会（地球）をイメージし、白い線は情報通信技術のグローバル化と国際社会にいる世界中の人々のネットワーク（繋がり）との両方の意味を持つ。
- 地球を包む3つのオブジェクトは、情報セキュリティ普及啓発のキャッチフレーズ「知る・守る・続ける」そのものであり、
 - ・「知る」(青色)は、ITリスクなどの情報を冷静に理解し知る
 - ・「守る」(緑色)は、安全・安心にインターネットを利用し、情報セキュリティ上の脅威から、身を守る
 - ・「続ける」(赤色)は、情報セキュリティ対策を情熱を持って続けることをそれぞれ意味する。

内閣サイバーセキュリティセンターの予算・体制

内閣サイバーセキュリティセンター予算

サイバーセキュリティ戦略
(平成27年9月4日 閣議決定)

平成28年度
予算案 17.3億円

(参考) 平成27年度
当初予算 16.5億円

(平成27年度 補正予算案 68.1億円)

➤ 政府機関情報セキュリティ横断監視・即応調整チーム(GSOC)による検知・解析機能の強化

○政府機関情報セキュリティ横断監視・即応調整チーム(GSOC)の運用 6.5億円

○政府機関情報セキュリティ横断監視・即応調整チーム(GSOC)の運用 6.5億円

○次期システム構築 66.8億円
(27年度補正予算案)

➤ ペネトレーションテスト等を通じたセキュリティ対策の徹底
➤ マネジメント監査等を通じた組織の体制・制度の検証・改善、リスク評価に基づく組織的な対策・管理等による組織的対応能力の強化

○各府省庁ネットワークに接続されているコンピュータシステムに対する侵入実験及び監査 3.0億円

○各府省庁ネットワークに接続されているコンピュータシステムに対する侵入実験及び監査 3.1億円

○コンピュータシステムに対する侵入実験及び監査 1.3億円 (27年度補正予算案)

➤ サイバーセキュリティに関する情報の収集・分析機能の強化

○脅威予測等総合分析の実施 2.0億円

○脅威予測等総合分析の実施 0.8億円

➤ 政府機関で重大なインシデントが発生した場合等における原因究明調査のための取組強化

○サイバーセキュリティインシデントに係る事後調査 1.0億円

○サイバーセキュリティインシデントに係る事後調査 1.1億円

➤ NISCの体制強化

定員増 22人

定員増 20人

※平成28年度予算案については、上記のほか、サイバーセキュリティ戦略本部の運営経費やサイバーセキュリティ関連施策の実施に必要な経費等(483百万円)を計上

政府のサイバーセキュリティに関する予算

平成28年度予算概算要求額

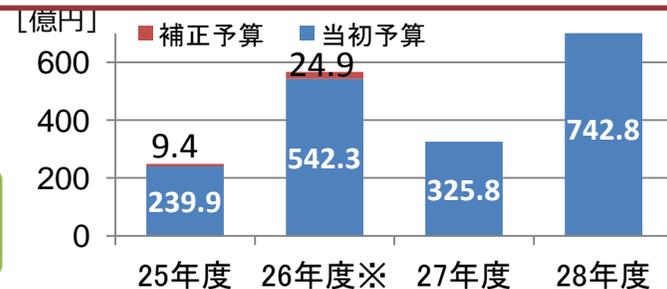
742.8億円

サイバーセキュリティに関する予算として切り分けられない場合には計上していない。

施策例及び平成28年度予算概算要求額

(括弧内は平成27年度当初予算額)

【内閣官房】	内閣サイバーセキュリティセンター予算	
【警察庁】	日本版NCFTAへの参画に伴う経費	
【警察庁】	サイバー犯罪等の対処能力強化のための実践的実習環境の整備等	0.8億円 (0.6億円)
【総務省】	未来志向型ネットワークセキュリティ基盤構築事業	13.0億円 (新規)
【総務省】	サイバー攻撃複合防御モデル・実践演習	6.0億円+事項要求 (4.0億円)
【総務省】	自治体情報セキュリティ対策の抜本的強化	4.4億円+事項要求 (新規)
【外務省】	情報セキュリティ対策の強化	4.8億円 (4.3億円)
【外務省】	サイバー空間における外交及び国際連携	0.1億円 (0.1億円)
【経済産業省】	重要インフラのセキュリティ対策促進・IT製品の評価・認証等 (独立行政法人情報処理推進機構(IPA)交付金)	53.2億円 (36.1億円)
【経済産業省】	サイバーセキュリティ経済基盤構築事業	23.6億円 (17.7億円)
【防衛省】	情報収集機能や調査分析機能強化	42.0億円 (8.4億円)
【防衛省】	ネットワーク監視器材の整備	61.0億円 (29.8億円)
【特定保護委】	特定個人情報に係るセキュリティ確保のための監視・監督体制整備 (マイナンバー関連)	3.2億円+事項要求 (0.6億円)
【厚生労働省】	本省及び日本年金機構等の関係機関における情報セキュリティ対策の強化	62.1億円 (新規)



83.0億円+事項要求 (16.5億円)

1.2億円 (1.1億円)

0.8億円 (0.6億円)

13.0億円 (新規)

6.0億円+事項要求 (4.0億円)

4.4億円+事項要求 (新規)

4.8億円 (4.3億円)

0.1億円 (0.1億円)

53.2億円 (36.1億円)

23.6億円 (17.7億円)

42.0億円 (8.4億円)

61.0億円 (29.8億円)

3.2億円+事項要求 (0.6億円)

62.1億円 (新規)

平成27年度予算額

325.8億円

サイバーセキュリティに関する予算として切り分けられない場合には計上していない。

* 26年度の数値は防衛情報通信基盤(DII)の整備(器材の整備)(クローズ系)(防衛省)、社会保障と税に関わる番号制度の導入に伴うシステム開発(内閣官房)を含む。

オリンピック・パラリンピックにおけるサイバーセキュリティの重要性について

サイバーセキュリティの現状

IT依存度の高まり

PC 多くの職場・家庭に普及
インターネットに接続

スマホ 携帯電話の50%以上が
スマホに置き換わり

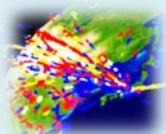
スマートカー 1台に100個以上の
コンピュータを搭載

スマートメーター 2020年までに2700万台
が普及（東電管内）

標的型攻撃の脅威の深刻化



以前にも増して政府機関に大量の不審メール、不正プログラムが送付されており、標的型メールによる脅威が一層深刻化。



日本に向けたサイバー攻撃は世界中から飛来化。

重要インフラに対する脅威の深刻化

- 金融・交通・情報通信など重要インフラへのサイバー攻撃も増加
- オリンピック・パラリンピックの運営に重要インフラの防護が必要



東京大会における要検討事項

- サイバー攻撃は近年急激に増加し、対象が重要インフラ全体にも拡大
- 大会期間中に障害が発生すれば、日本の威信が損なわれる懸念
- ロンドン大会の経験を踏まえ、物理（テロ）面とともに、サイバー面からも、十分な準備期間をかけた慎重な対策が必要
- 新たな施設整備に当たっては当初からサイバーセキュリティの考慮が必要

ロンドン大会でのサイバーセキュリティとサイバー攻撃

<構築システム>

- 約47億回のホームページ閲覧、約1億回のオンライン動画リクエスト数に耐えるシステム
- メイン会場に観客向けの公衆無線LANアクセスポイントを約1,500箇所設置

<事前準備>

- テスト・リハーサルを繰り返し実施

<体制構築>

- 組織委の技術チームがテクノロジー・オペレーション・センターを設置
- 技術スタッフ約600名が24時間稼働（セキュリティ関連スタッフを含む）
- 政府側のセキュリティ体制・関係機関とも緊密な連携

<発生したサイバーセキュリティ事案>

- 組織委NWに係るセキュリティに関する警告：約2.3億件
- 公式HPに対する悪意ある接続要求（不正アクセス）：約2億件
- 開会式直前にスタジアムの電力供給制御システムへの攻撃情報を入手 → 手動切替体制を急遽確保
切替時間の30秒（= 停電）で開催国の威信が損なわれる（Reputation Riskへの対応も必要）

セキュリティ対策検討体制の設置

【概要】

○閣僚会議においてセキュリティ対策の進捗管理を行うことをIOCに対して明確化するとともに、関係府省庁によるセキュリティ幹事会、テロ対策WT及びサイバーセキュリティWTを平成26年10月に設置。今後の課題や緊密な連携についての確認とあわせ、計画・運営段階において関係機関を主導するシニア・セキュリティ・コマンダーとして警察庁次長を登録。

【体制】

オリパラ推進本部（本部長：安倍総理）

←IOCが設置を求める
TOGC（Tokyo Olympic Games Council）に相当

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 - 内閣官房オリパラ事務局長、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・オリパラ事務局・事態・内調・NISC）、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 - 内閣審議官（オリパラ事務局）、警察庁審議官
- 構成員 - 関係省庁の課長級
- オブザーバー - 関係機関の幹部
- 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 - 内閣審議官（オリパラ事務局）、警察庁審議官
- 構成員 - 関係省庁の課長級
- オブザーバー - 関係機関の幹部
- 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

2020年東京オリンピック・パラリンピック競技大会における
サイバーセキュリティ体制に関する検討会

東京オリンピック・パラリンピック競技大会のサイバーセキュリティ確保に向けた取組

サイバーセキュリティ戦略（平成27年9月4日閣議決定）

- 大会の開催、そしてその先の2020年代初頭までの将来を見据えつつ、今後3年程度の基本的な施策の方向性を示す。
- 「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安定及び我が国の安全保障」に寄与することを目的とする。
- 大会に向け、リスクの明確化、実践的対処体制の構築、十分な演習・訓練を実施。

東京オリンピック・パラリンピック競技大会に向けた取組

- 大会の開催・運営に影響を与える重要なサービスを提供する事業者を選定。
- サイバーセキュリティ上のリスクを特定・分析・評価するための手順をとりまとめ、選定された事業者を中心としてリスクマネジメントの実施を促進。



- 関係組織に対して対処のための的確な情報共有を担う中核的組織としてのオリンピック・パラリンピックCSIRTを整備。
- 整備にあたっては、2020年東京オリンピック・パラリンピック競技大会におけるサイバーセキュリティ体制に関する体制検討会を通じ、政府/関連組織の役割を整理し、具体的な体制を検討。

各取組を並行して実施し、補完し合いながら推進

• サイバーセキュリティの将来について考える

- 国民一人一人が対応できるか
- IoT、自動運転等新たなシステムの普及に対応できるか
- 技術革新で打開できるか
- 実現しているものから想像してみる
 - (センサー) 火災報知器
 - (資格) 運転免許、自転車運転者講習
 - (体制) 消防団、避難所
 - (規制) 耐震基準、自動車検査登録
 - (補償) 自動車損害賠償責任保険