重要インフラ防護に関する
諸国の枠組み等に関する調査報告書

２０１５年３月

内閣官房　内閣サイバーセキュリティセンター(NISC)

※本調査報告はNISCの委託により、株式会社情報通信総合研究所が実施したものです。

概　要

◆調査目的

重要インフラ防護（情報セキュリティ対策）の向上及び今後の国際連携の強化に資するよう、米欧の各種政策／施策等と日本の施策比較

◆調査内容

重要インフラ防護に関する諸国の枠組み等に関する調査
(1) 諸国の重要インフラ防護に係る枠組みの比較
(2) 情報セキュリティの国際標準・関連規定の洗い出し

◆調査対象

I.　米国
II.　欧州連合

◆調査範囲

(1) 枠組み：文献(公開済)情報、現地ヒヤリング
(2) 国際標準、関連規定：文献(公開済)情報(ISO,IEC,ITU等)

1-1. 米国の重要インフラ防護サマリ

◆NCCIC(DHS)が調整役として、各政府機関および重要インフラ事業者等のとりまとめ

◆官民間の情報共有体制

・重要インフラパートナーシップ助言協議会(CIPAC)
・サイバー統合連携グループ(Cyber UCG)

→ **定期的な情報共有の仕組みを構築**

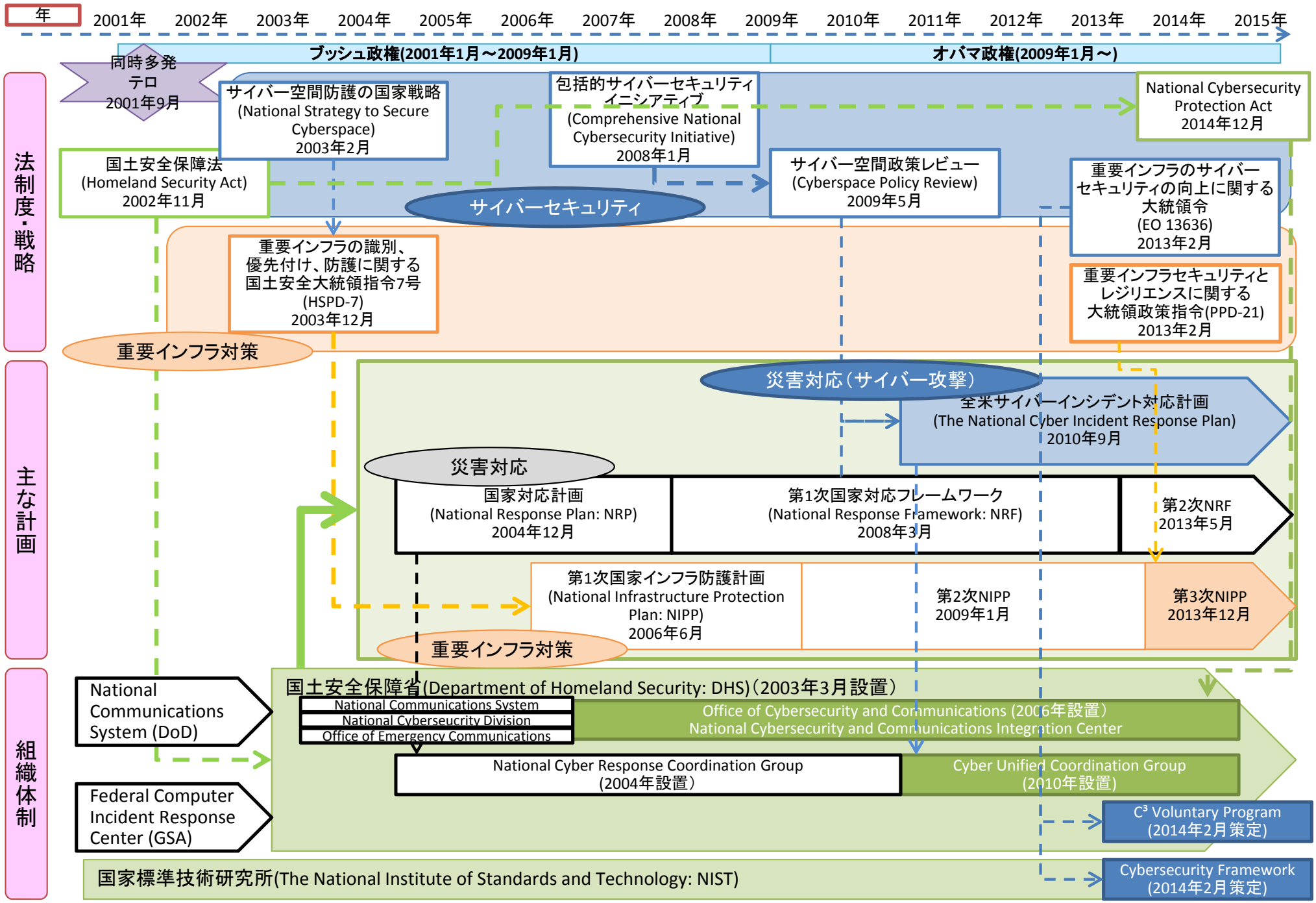
◆法施策等

包括的サイバーセキュリティ・イニシアティブ(CNCI)
サイバー空間政策レビュー(CPR)
重要インフラのサイバーセキュリティの向上に関する大統領令(E.O.)

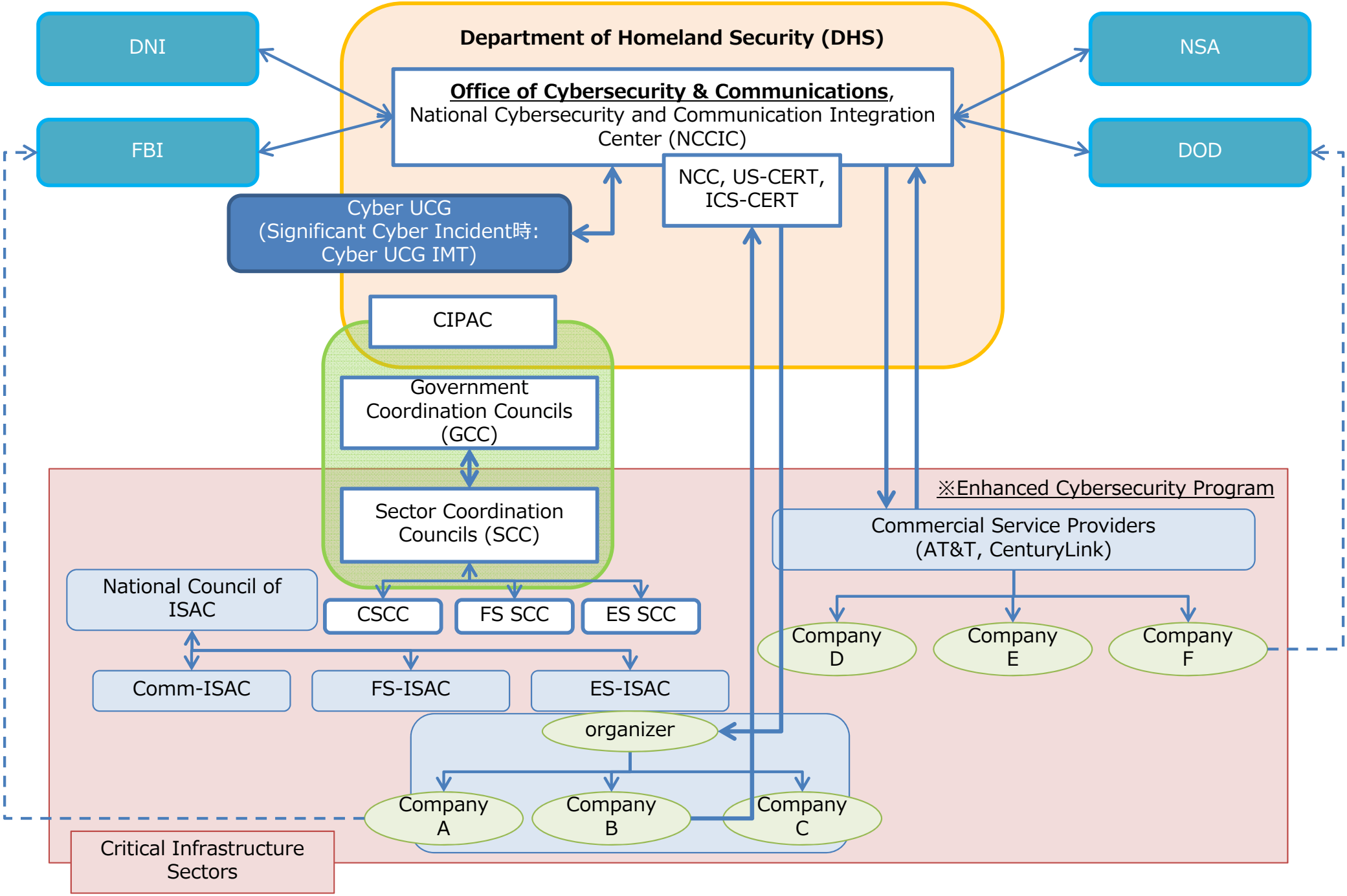
→ **上記を支える様々な計画／運用面の支援プログラムを実施**

NCCIC: National Cybersecurity and Communications Integration Center
DHS: Department of Homeland Security
CIPAC: Critical Infrastructure Partnership Advisory Council
Cyber UCG: Cyber Unified Coordination Group
CNCI: Comprehensive National Cybersecurity Initiative
CPR: Cyberspace Policy Review
E.O.: Executive Order

1-2. 米国の重要インフラ防護政策の変遷



1-3. 米国の重要インフラ防護に関する情報共有体制



1-4. 米国の重要各施策概要 1/2

		項目		概要
全般	法制度	Homeland Security Act (2002) （Critical Infrastructure Information Act of 2002含まれる） National Cybersecurity Protection Act (2014)		2001年9月11日のテロ事件を受け、国土安全保障省(DHS)を設立 重要インフラ防護についても、DHSを中心として施策が策定 サイバーセキュリティは、DHS配下にNCCICが設置され、本部局が中心に対応 2014年末の法律で、NCCICに法的権限付与
	主管省庁	DHS NCCIC		DHSのNCCICを中心に、インシデント情報等についての官民間の情報共有を実施 各重要インフラ所管省庁(Sector Specific Agency: SSA)はNCCICと連携して対応
	政策	国家インフラ防護計画(NIPP)		DHSが策定している重要インフラの防護計画 2013年12月に大統領政策指令(PPD-21)に基づき、第3次計画として改訂
				重要インフラセクタとして16分野を指定 化学、商業施設、通信、重要製造業、ダム、救急サービス、情報技術、原子力、農業・食料、防衛基盤産業、エネルギー、健康＆公衆衛生、金融サービス、水、政府施設、交通システム
	関係主体	全体	重要インフラパートナーシップ助言協議会(CIPAC)	NIPPに基づいて設置 政府の重要インフラ防護プログラムと民間及び地方政府のインフラ防護活動をコーディネートする重要インフラ政策に関し、DHSやSSAに対して助言や提言を行う
		個別	政府調整委員会(GCC)	CIPAC配下に設置された委員会 NIPP等の政府計画等に関する導入、運用、アップデート等についてセクタ毎に検討 各重要インフラ分野毎のGCCが存在し、関係する省庁や州政府機関、自治体レベルが参加
			セクタ調整委員会(SCC)	CIPAC配下に設置された委員会 重要インフラセクタ毎に事業者が自主運営で運営 各事業者のCEO相当の役員がメンバとして参画し、対応するGCCと共同して、NIPP等の計画を導入、運用していくにあたっての検討
	フレームワーク	サイバーセキュリティフレームワーク		NISTが2013年2月の大統領令13636を受け、2014年2月策定・公表 重要インフラに対するサイバーリスクを低減するため、施策の優先順位付けや効率的な対策等についての指針
		重要インフラサイバーコミュニティ（C^3）ボランタリープログラム		サイバーセキュリティフレームワークの導入を支援するためプログラムとして2014年2月に策定 US-CERTが、フレームワークの利用支援、対応窓口、フィードバック等の対応実施

1-4. 米国の重要各施策概要 2/2

		項目		概要
全般	行動計画	全米サイバーインシデント対応計画(NCIRP)		サイバー攻撃に対する省庁および民間企業やその他関連機関との連携体制の改善を目指して2010年に策定 インシデント発生時（平常時、大規模時）の情報共有体制等について規定
		平常時	NCCICが主導・調整	インシデント情報等について、直接NCCICと情報共有するか、既に確立されている報告枠組みを通じて報告するかの2種類 各省庁や企業から指名された幹部やスタッフから構成されたサイバー統合調整グループ(Cyber UCG)がNCCICをサポート
		大規模サイバーインシデント時	Cyber UCG IMTと連携してNCCICが調整	国家サイバーリスク警戒レベル(NCRAL)がレベル２以上になると大規模インシデント発生時となる Cyber UCGから選ばれた各省庁の政府高官及び民間企業の幹部から構成される Cyber UCG IMTがインシデント対応計画等の策定等を監督し、NCCIC等と連携
情報共有	施策	サイバー情報共有・連携プログラム(CISCP)		官民間の情報共有の会合が毎週開かれ、脆弱性等に関する情報を共有する枠組み DHSは脅威情報に関する①指標速報、②分析速報、③警報速報、④施策提案を作成し、関係主体に共有
		拡大サイバーセキュリティサービス(ECS)プログラム		DHSが主導する情報共有プログラム DHSから任命された商用サービス事業者に対しDHSは機密性の高い情報等を提供し、商用サービス事業者はネットワーク監視等の実施と合わせて、DHSから提供された脅威情報に自社のセキュリティ分析情報等を追加し、契約先の企業に有料で提供
	機密情報の防護	重要インフラ情報防護(PCII)プログラム		重要インフラ情報法(2002)に基づき、重要インフラ情報防護(PCII)プログラムが制定され、国家セキュリティ防護を目的に情報共有した情報はPCIIとして情報公開法や民事訴訟等での利用から保護される
	技術仕様	TAXII(情報共有フレームワーク) STIX（言語体系） CybOX（サイバー攻撃観測記述形式）		DHSのNCCICが主導して、自動化・構造化されたサイバーセキュリティ情報共有技術の導入を推進 DHSスポンサーの下、MITREが開発 マシン間の情報共有を可能とし、リアルタイムでの情報共有を目指す
	判断基準	Traffic Light Protocol (TLP)		当該情報を情報共有すべきかどうかの情報提供にあたっての判断基準 RED（情報提供元のみ）、AMBER（情報を知る必要がある者のみに限定）、GREEN（各層における関係者と共有可能な情報）、WHITE（公共向けの情報）の４種類に情報を分類される

1-5. 米国の最近の動向

- **サイバーセキュリティ関連法の制定**
  - 2014年12月18日に、National Cybersecurity Protection Act of 2014を含む、4本のサイバーセキュリティ関連法が成立
  - National Cybersecurity Protection Act of 2014では、DHSのNCCICの法的権限が明確化

- **官民間の情報共有促進に関する大統領令（2015/02/15）**
  - 民間セクタのサイバーセキュリティ情報共有の促進に関する大統領令
    1. 民間セクタのサイバーセキュリティ連携の促進
       - 情報共有組織の開発を促進する
       - 情報共有組織のための共通のボランタリーな基準を開発する
    2. 官民情報共有の権限付与
       - DHSが情報共有組織(ISAO)と契約締結するための権限を明確化
       - 民間事業者がサイバーセキュリティ脅威情報にアクセスする際の手続きの簡素化
    3. 強力なプライバシー・市民的自由の保護の提供
    4. 将来的な法制化への道筋を作る

- **サイバー脅威情報統合センタ(CTIIC)設立に関する覚書（2015/2/25）**
  - 海外からのサイバー脅威やサイバーインシデントに関する全ての情報を統合・分析センタの設立
  - サイバー脅威情報の情報収集に関する新たな権限が付与されたわけではなく、また直接民間企業と情報共有する組織としては位置づけられていない。DHSのNCCIC等の既存機関の支援組織としての位置づけ

1-6. 重要インフラ防護に係る日米制度比較 1/2

	日本		米国		
	関係主体	施策	関係主体	施策	概要
法制度／戦略	国会 (参議院／衆議院)	サイバーセキュリティ基本法(2014)	連邦議会 (上院/下院)	国家安全保障法(2003) 国家サイバーセキュリティ防護法(2014)	DHSの制定(2003)と、NCCICの法的位置づけの明確化(2014)
	サイバーセキュリティ戦略本部／内閣サイバーセキュリティセンター(NISC)	サイバーセキュリティ戦略(2013)	White House (ブッシュ)	包括的サイバーセキュリティ戦略:CNCI (2008)	政府、重要インフラに関する12のセキュリティ施策
			White House (オバマ)	サイバー空間政策レビュー:CPR (2009)	CNCIの見直しの政権施策 （短期10、中期14） 官民パートナーシップ強化
				大統領令 (2013,2015)	官民間の情報共有強化に向けた政府施策の策定
計画		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) 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」策定にあたっての指針第3版(2013)	国土安全保障省 (DHS)	第3次国家インフラ防護計画:NIPP (2013)	全体的なリスクマネージメント、情報共有とリスクベース手法の開発と実行の強化
				全米サイバーインシデント対応計:NCIRP (2010)	サイバー攻撃に対する官民の連携体制の改善 連邦、政府、民間企業、NCCICの役割を規定
			国家標準技術研究所(NIST)	重要インフラのサイバーセキュリティを向上させるためのフレームワーク (2013)	サイバーセキュリティリスクを管理するためのリスクベースアプローチを提示
				サイバー脅威の情報共有に関するガイドライン:SP800-150	インシデント対応のライフサイクルの中で情報共有や調整、対応を明記

1-6. 重要インフラ防護に係る日米制度比較 2/2

		日本		米国		
		関係主体	施策（実施主体）	関係主体	施策（実施主体）	概要
運用	政府機関	NISC	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)	DHS	政府調整委員会:GCC	NIPP等の政府計画に関する導入、運用、アップデート等についてセクタ毎に検討。
					NCCIC	情報共有の窓口、調整役として位置 24時間365日監視
	官民	NISC	ー		Cyber UCG	重大なサイバー攻撃の脅威が発生した場合、関係省庁を統括 平常時はNCCICをサポート
			重要インフラ専門調査会		重要インフラパートナーシップ助言協議会:CIPAC	GCC/SCCの親会 重要インフラ施策等のレビュー
			第3次行動計画に基づく官民情報共有		サイバー情報共有・連携プログラム:CISCP	政府・重要インフラ事業者での脆弱性情報共有枠組み
			NISC重要インフラニュースレター		重要インフラサイバーコミュニティ(C^3)ボランタリープログラム	NISTのサイバーセキュリティフレームワークの利用促進・導入支援
			ー		拡大サイバーセキュリティサービス(ECS)プログラム	DHSから認可された商用サービス事業者が、契約先企業に対して脅威情報等を販売 リアルタイムの機械間情報共有を実施。
	民間分野間	セプター	セプターカウンシル総会	重要インフラ事業者	セクタ調整委員会:SCC	各セクタの行動計画の導入、運用、改訂
			セプターカウンシル幹事会			
			情報共有WG		NC-ISAC	セクタ間の関係強化や共通の問題等の意見交換
			情報収集WG			
			相互理解WG			
	民間分野内	セプター	セプター間情報共有		ISAC	サイバー上の脅威や脆弱性やイベント等についての情報共有 (17 ISAC)
			ISAC			

2-1. 欧州連合の重要インフラ防護サマリ

- 欧州連合の枠組みは、「欧州重要インフラ防護プログラム(EPCIP)」2006
- 重要インフラ防護に関する原則等が提示され、EU加盟国は本プログラムに基づき重要インフラ防護施策を制定することが求められている。
- 官民間の情報共有体制

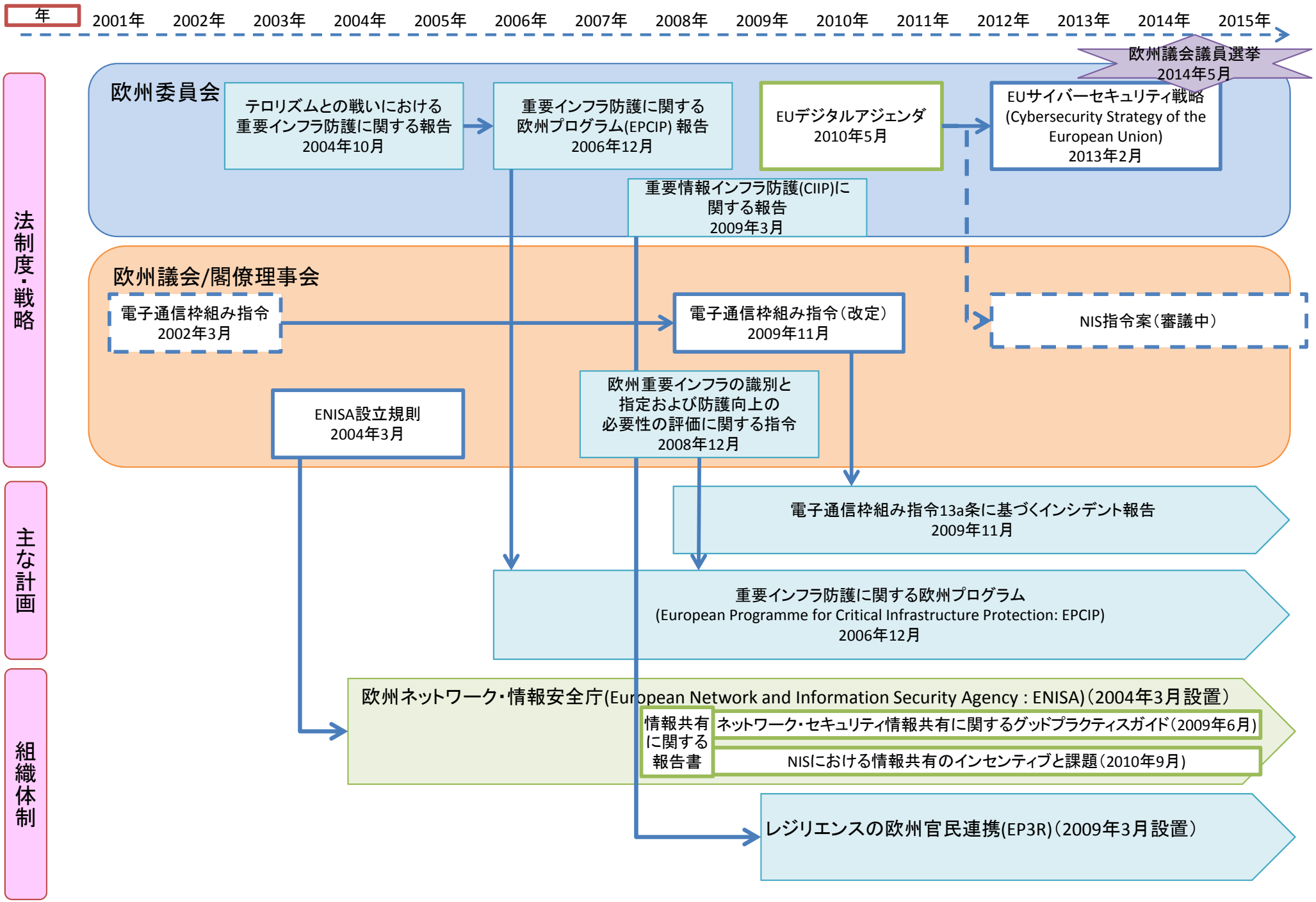
  2009年ENISA配下に「レジリエンスのための欧州官民連携(EP3R)」設立
  EU全体の重要インフラ防護強化に向けた官民連携の組織として位置づけられ、官民の幹部レベル、及び専門家レベルの2レイヤの情報共有体制が構築。

- 2013年2月に提案されたNIS指令案が、2015年中の成立を目指して、2015年３月現在閣僚理事会において審議されている状況。

  重要インフラ事業者に対してインシデント等の報告義務を求める規定が含む報告義務については、電子通信枠組み指令13a条において、通信事業者に対しては報告義務が求められている。

EPCIP:European programme for critical infrastructure protection
ENISA: European Network Information Security Agency
EP3R: the European Public-Private Partnership for Resilience

2-2. 欧州連合の重要インフラ防護政策



2-3. 欧州連合の重要各施策概要

		項目	概要
全般	法制度	電子通信枠組み指令(2002制定、2009改訂) 欧州重要インフラの識別と指定および防護向上の必要性の評価に関する指令(2008) NIS指令案(審議中)	■ 電子通信枠組み指令において、通信事業者に対しインシデント時の報告義務を規定 ■ 現在審議中のNIS指令案では、報告義務を重要インフラ事業者に対象を拡大する規定が盛り込まれている ■ EU各国に対し、自国における重要インフラセクタの指定とその対策に関する施策を実施するよう規定
	支援組織	ENISA	■ 2004年のRegulation (EC) No 460/2004 に基づき設立 ■ EU各国が情報セキュリティ対策を実施するための支援や、ベストプラクティス等の各種情報を各国に共有するための支援活動が中心
	政策	電子通信枠組み指令13a条に基づく報告義務	■ 通信事業者に対するセキュリティ管理義務や、インシデント時の国内監督官庁及びENISAに対する提出義務が求められる
		重要インフラ防護に関する欧州プログラム（EPCIP)	■ EU全体の重要インフラ防護プログラムとして2006年12月より開始 ■ EPCIPのベースとなる2004年の「テロリズムとの戦いにおける重要インフラ防護報告書」において、重要インフラ分野として9分野（エネルギー、情報通信、金融、ヘルスケア、食料、水、運輸、放射物質等の危険物、政府施設）を指定 ■ これらを参考に、EU加盟国は自国の重要インフラセクタを指定
	関係主体	レジリエンスのための欧州官民連携(EP3R)	■ EU全体の重要情報インフラ防護に関する情報共有フレームワーク。各国のセキュリティ監督官庁の幹部と専門技術者の２レイヤによる情報共有体制が構築される ■ EP3Rにおける情報共有は強制化されているものではなく、各国ボランタリーに情報共有するためのプラットフォームとして位置づけられている

3. 重要インフラ防護における情報セキュリティの国際標準・関連規定等

情報セキュリティの国際標準、関連規定や、報告書等を以下10組織の発行文書より抽出。
また、重要インフラ防護にキーワードにより関連が深いと思われるものについては、カテゴリー分類を実施

重要インフラ防護における情報セキュリティの国際標準・関連規定等関係団体抽出文書数一覧

組織名	組織概要	文書数
ISO	国際標準化機構(International Organization for Standardization) 各国の代表的標準化機関からなる国際標準化機関。電気・通信及び電子技術分野を除く全産業分野（鉱工業、農業、医薬品等）に関する国際規格の作成を行う。https://www.jisc.go.jp/international/isoiec.html	ISOのみ：27 IECのみ：24 ISO/IEC：190
IEC	国際電気標準会議(International Electro technical Commission) 各国の代表的標準化機関からなる国際標準化機関。電気及び電子技術分野の国際規格の作成を行う。 https://www.jisc.go.jp/international/isoiec.html	
ITU	国際電気通信連合(International Telecommunication Union) 国際連合の専門機関の一つ。電気通信の改善と合理的利用のため国際協力を増進し、電気通信業務の能率増進、利用増大と普及のため、技術的手段の発達と能率的運用の促進を目的とする。https://www.ituaj.jp/?page_id=158	117
JISC	日本工業標準調査会(Japanese Industrial Standards Committee) 工業標準化法に基づいて経済産業省に設置されている審議会。工業標準化全般に関する調査・審議を行う。http://www.jisc.go.jp/	33
BSI	英国規格協会(British Standards Institution) 英国における、世界最古の国家規格協会。http://www.bsigroup.com/ja-JP/about-bsi/	27
ISACA	旧情報システムコントロール協会(formerly the Information Systems Audit and Control Association) 情報システム、情報セキュリティ、ITガバナンス、リスク管理、情報システム監査、情報セキュリティ監査等、情報通信技術専門家の国際的団体。http://www.isaca.gr.jp/	6
NIST	米国国立標準技術研究所 (National Institute of Standards and Technology) 米国における、技術や産業、工業などに関する規格標準化を行っている政府機関。http://www.sophia-it.com/content/NIST	72
ENISA	欧州 ネットワーク情報セキュリティ庁(European Network and Information Security Agency) EUの専門機関の一つ。ネットワークセキュリティ及び情報セキュリティに関する予防・対応能力を促進することを任務とし、EU加盟国および欧州諸機関へ、アドバイスや提言を提供すると共に、欧州諸機関、EU加盟国ならびに民間企業・産業関係者との連携を促進している。 http://www.ipa.go.jp/security/publications/enisa/	63
IPA	情報処理推進機構(Information-technology Promotion Agency , Japan) 経済産業省所管の独立行政法人。情報セキュリティ、ソフトウェア高信頼化、IT人材育成等の施策を行う。http://www.ipa.go.jp/	228
OECD	経済開発協力機構(Organisation for Economic Co-operation and Development) アメリカ、ヨーロッパ等の先進国によって、国際経済全般について協議することを目的とした国際機関。 情報・コンピュータ・通信政策委員会（ICCP）の下の情報セキュリティ・プライバシー作業部会（WPISP）において、セキュリティ、プライバシー問題について検討している。http://www.oecd.org/sti/whatistheoecdworkingpartyoninformationsecurityandprivacywpisp.htm	9