資料１

【機密性2情報】

東京オリンピック・パラリンピック競技大会等の大規模国際イベントにおけるサイバーセキュリティの確保に向けた取組の今後の活用方策に関する有識者会議
第２回会合

事務局説明資料

(参考)国内外の政府機関等におけるサイバーセキュリティ施策

2021年３月

内閣官房　内閣サイバーセキュリティセンター

国内外の政府機関等におけるサイバーセキュリティ対策

1　London2012大会後の英国の施策とその成果

2　米国のサイバーセキュリティに関する情報共有体制

3　東京大会に向けて国内関係省庁が推進するサイバーセキュリティ対策（抜粋）

4　「英国の施策」と「米国の情報共有体制」を参考にした議論の方向性について（例）

1　London2012大会後の英国の施策とその成果

本件に係る内容は、NISCの委託を受けたエヌ・ティ・ティ・コミュニケーションズ株式会社が調査しているものとなります

1　London2012大会後の英国の施策 –NCSC設立–(1/2)

英国のセキュリティ機能集約が必要な背景としては、大会以前から次のような問題が発生。大会の4年後、このCERT-UKやその他の重複する機能を持つ組織が乱立していた状況「Alphabet Soup問題」はNational Cyber Security Centre (NCSC) への機能統合により解消。

解決した課題：

・「国家サイバーセキュリティ戦略 2016-2021」が出される前の2016年4月、中央政府内に少なくとも12のサイバーセキュリティに関連する組織・チームが存在

・　各々の組織が相互の調整なしに指針を出すため重複や矛盾も生じ、産業界からも政府のどの部署に助言を求めればよいのかわからないと不満が募っていた。

解決策：

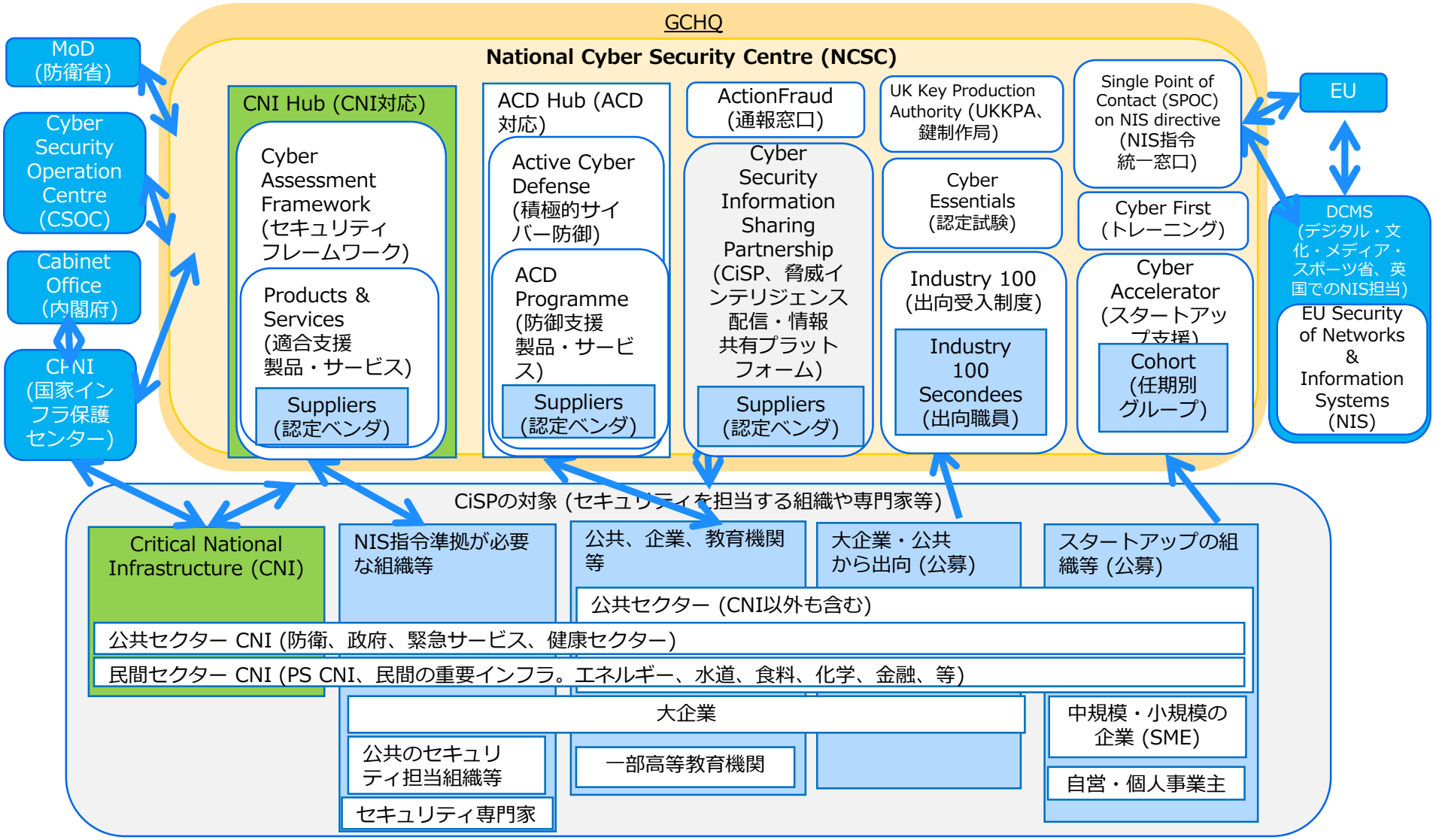
・　民間や諸外国と対外的な活動を行う部署の機能を1つに集めて窓口一本化
(CESG-GCHQ の情報セキュリティ部門、CCA、CERT-UK、CPNIのサイバー関連部門の 4 組織 -> NCSC)

・　NCSC (国家サイバーセキュリティ・センター) は GCHQ （政府通信本部) 傘下
-GCHQ の情報やスキル・経験を活用できる。
※　敵対国による大規模なサイバー攻撃かサイバー犯罪から防御することも NCSCの役目であるが、相手国をサイバー攻撃するような「戦争行為」は国防省（MoD:Minitry of Defence）及び軍のサイバー部隊の仕事と位置づけられている。

https://www.jetro.go.jp/ext_images/_Reports/01/427a23803575001d/20170120.pdf

1　London2012大会後の英国の施策 –NCSC設立–(2/2)

NCSCは各管轄省庁等と連携しての国家中枢防衛、重要インフラや公共・民間組織に対しての情報提供、実運用の有償・無償サポートを含む包括的な支援を提供



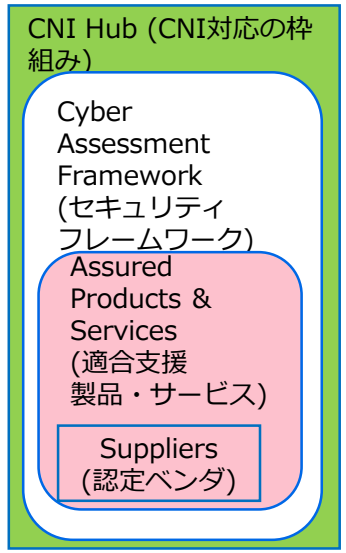
CiSP ：　英国全体で官民連携でのリアルタイムでの脅威情報共有を推進する取組（ Cyber Security Information Sharing Partnership の略）

1　London2012大会後の英国の主な施策 –ｾｷｭﾘﾃｨ運用面の支援– (1/2)

NCSCはCNI (重要な国家インフラ、政府および民間組織) を次の方法でサポート。
ロンドン大会後の動向、例えばペネトレーションテスト等、セキュリティ対策の実運用に対しても認定製品やサービス等で積極的な支援を開始（CNI以外の組織も購入可）。

1. アドバイス、サポート、ガイドの提供
2. 信頼できるグループ内でフォーラムやイベント開催
3. 支援サービス提供 (CAF準拠支援、インシデントレスポンス)
4. 産業内コラボレーション推進 (Industry 100での出向制度)
5. 政府でのCNI向けセキュリティ政策検討時のアドバイスや支援
6. 脅威インテリジェンスの提供 (CiSP経由、または対象組織への直接提供)
7. 政府での新しいICT環境向けセキュリティ政策検討時のアドバイスや支援
8. MSPなどのCNIに重要なサービスを提供する組織に対しての支援

（実運用に対しての積極的な支援）
セキュリティ運用支援の各種製品・サービスやベンダーにつき、基準に基づいた検証・認定の上で、公式に有償提供を仲介。CAF適合支援の枠組みで提供される製品・サービス数は200以上に上り、ペネトレーションテスト (47件)、業務向け製品セキュリティ (43件)、セキュリティコンサル (28件)、インシデントレスポンス (9件)、トレーニング (2件) 等が含まれる。



https://www.ncsc.gov.uk/section/private-sector-cni/cni#section_5
https://www.ncsc.gov.uk/section/products-services/all-products-services-categories

1　London2012大会後の英国の主な施策 –ｾｷｭﾘﾃｨ運用面の支援– (2/2)

CNI以外の非重要インフラに対しても、大会後の「国家サイバーセキュリティ戦略2016-2021」からの英国全体でセキュリティを飛躍的に向上させるための取組として、Active Cyber Defense (積極的サイバー防御) の枠組みが存在。フィッシング、メールフィルタリング等の多くの攻撃により発生する大部分の弊害から保護することを目的に、基本的な対策を実施するもの。次のサービスが認定ベンダまたはNCSCにより提供されている。

1.Protective Domain Name Service (DNSフィルタリング、公共セクター向け)
2.Web Check　(Webチェック、公共セクター・大学以上の高等教育機関向け)
3.Mail Check　(メールチェック、公共セクター・大学以上の高等教育機関向け)
4.Host Based Capability (エージェントセキュリティ、中央政府向け)
5.Logging Made Easy (ログイン管理製品、Windows向け、対象不問)
6.Vulnerability Disclosure
　-Vulnerability Reporting Service (脆弱性通報システム、対象不問)
　-Vulnerability Disclosure Pilot (脆弱性検出・トリアージ、中央政府向け)
　-Vulnerability Disclosure Toolkit (脆弱性検出・報告用ツール、対象不問)
7.Exercise in a Box (インシデント対応シナリオによる訓練、対象不問)
8.Suspicious Email Reporting Service (不審メール報告、対象不問)
9.The NCSC Takedown Service (NCSCによるテイクダウン、公共向け)

https://www.ncsc.gov.uk/section/products-services/active-cyber-defence
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

1　London2012大会以後の英国の主な施策 –官民連携の情報共有 CiSP–

Cyber Security Information Sharing Partnership (CiSP) は、大会後の2013年から運用を開始。英国全体で官民連携でのリアルタイムでの脅威情報共有を推進。

2015年以降NCSCの管轄に移行され、通信手段等で一定の基準を満たした組織及び所属する個人がCiSPに登録可能で、次の機能を提供。

- 政府や産業界のカウンターパートと、安全な環境で繋がることができる。
- 脅威情報を随時取得可能
- CiSPのフォーラム上で組織間での情報交換や質問などが可能
- 登録組織向けにカスタマイズされたネットワーク監視レポート無償購読

CiSPのサイバー脅威インテリジェンス (Cyber Threat Intelligence) にはOpen Source Intelligence (OSINT) によるレポートや、政府や産業界によるレポートが含まれ、CiSPに所属する組織がインテリジェンスを利用した脅威分析の初歩として、攻撃者、その攻撃手法等を自ら分析し監視や対策に役立てることが可能

CiSPについては、過去に次の数字の発表あり。

・22のセクターから10,569名登録、20,270点のコンテンツ (2018年時点)
・22のセクターから約5,500組織が加入、15,571名登録 (2019年時点)

https://www.ncsc.gov.uk/section/keep-up-to-date/cisp#section_4
https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf

1　London2012大会以後の英国NCSCの活動成果、年推移–

NCSCの直近3年のCiSP、ACD、CNI等各枠組みを総合した対応の規模や推移は次のとおり。資格認定数、CiSP加入者数、インシデント対応数が増加しており、指針発行から事故対応までを把握しつつ統括する機関として実績を重ねている。

種別	2018年	2019年	2020年	成長率 (Growth)
対応したインシデント数	557	658	723	130%
対応した被害組織数	N/A	約900	約1200	133%
対応した脅威の件数	214	154	414	193%
閉鎖したフィッシングサイトの数	138,398	177,335 (62.4%は24h以内に閉鎖)	166,710 (65.3%は24h以内に閉鎖)	120%
CiSP新規加入者数	2,361	5,000	2,953	125%
暗号鍵の提供数 (NCSC内 UK Key Production Authority (UKKPA)経由)	145,000 (クライアント数 200)	108,411 (クライアント数 170)	101,747 (クライアント数 140)	70%
ホームページ訪問数	190万	280万	270万	142%
ガイダンスとブログの発行数	ガイダンス134、ブログ95	ガイダンス34、ブログ69	ガイダンス30、ブログ60	39%
Cyber Essentialsの認定数	8900以上	14,234	17,100	192%
CyberFirst courseの受講者数 (学生)	1,968	2,614	1,770	90%
Cyber Security Awareness等の無償セッションの提供数	1,000以上	2,700以上 (トレーニングイベントを含む)	100以上 (ワークショップ、ポッドキャスト、ウェビナー等)	10%
海外訪問 (受け入れ) 数	54	56	20以上	37%
イベント開催数 (参加者数)	80	197 (参加者数9,000名以上)	101 (参加者数4,602名以上)	126%

https://www.ncsc.gov.uk/annual-review/2018/ncsc/docs/ncsc_2018-annual-review.pdf
https://www.ncsc.gov.uk/annual-review/2019/ncsc/docs/ncsc_2019-annual-review.pdf
https://www.ncsc.gov.uk/files/Annual-Review-2020.pdf
https://www.cbronline.com/feature/punched-tape-ukkpa

1　London2012大会以後の英国NCSCの活動成果、2020年–

　最新の2020年度では次のような取り組みと成果 (数量) が示されている。
リスクの高いベンダーへの対応や、Covid-19関連等といった新しい対象に対しても迅速で柔軟な対応を行い、一年以内に可視化できる成果に繋げている。

新しい脅威への対応：
- 　リスクの高いベンダー対応として米国のHuaweiに対する制裁を迅速にレビューし、英国で必要を政府および実務者視点の両面で検討し、速やかに政府に提案
- 　Covid-19およびリモートワーク関連
  - 　125か国で利用されているトレーニングツール「Exercise in a Box」においてリモートワークに関連したコンテンツを追加、新しいリスクを学びとして提供
  - 　リモートワーク、Covid-19関連攻撃者に関してガイドラインをタイムリーに展開

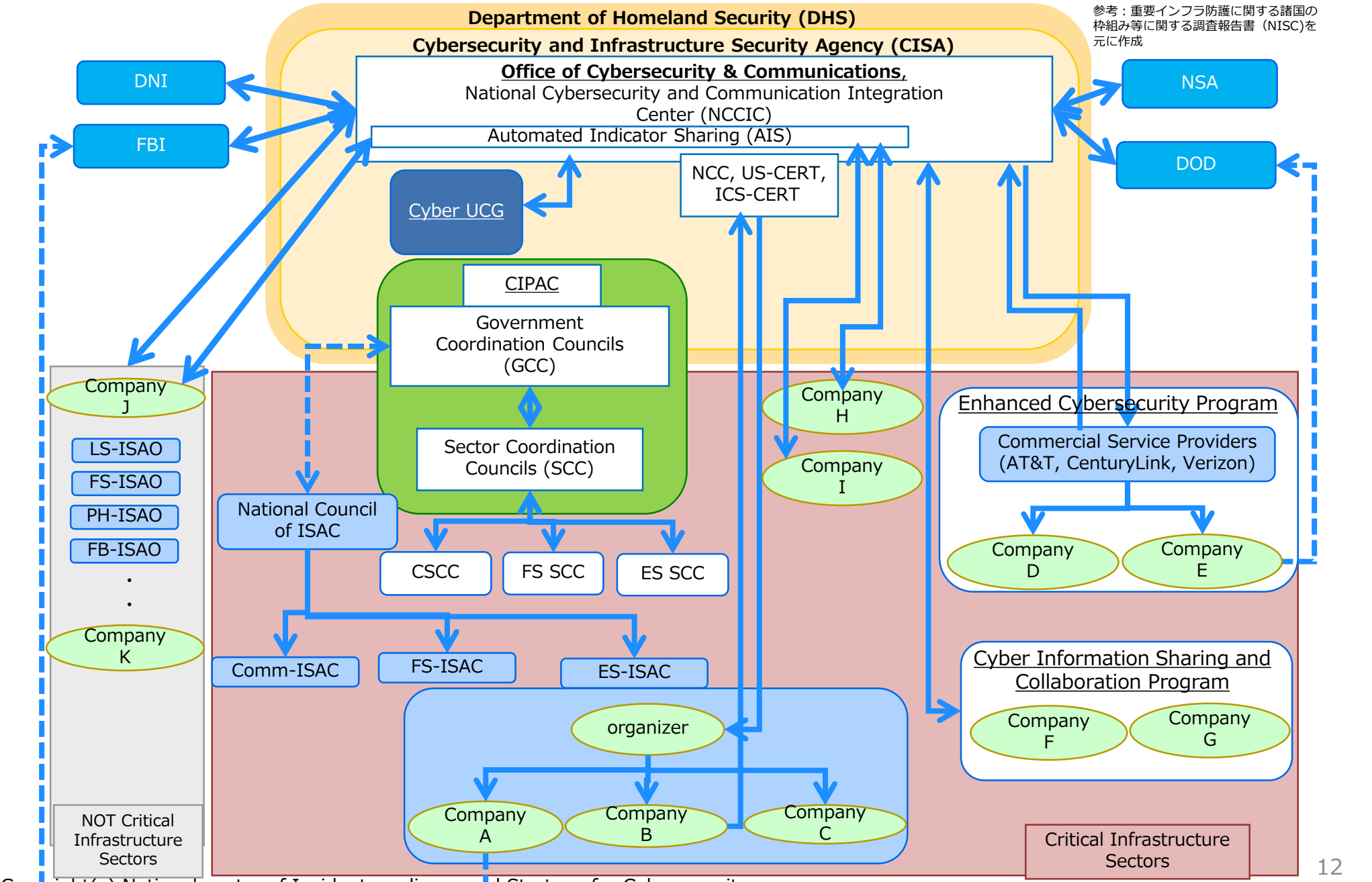
大規模で情勢にも対応した積極的なサイバー防御 (ACD)：
- 　不審メール報告サービスにおいて、2.3億件の不審メールの報告に対応
- 　22000件以上の不正URLをCovid-19に関連した詐欺行為で閉鎖 (テイクダウン)
- 　200件以上のCovid-19に関連したサイバーインシデントに対応
  - 　NHSトラストを含む健康セクターに対して支援を提供
  - 　NHSトラストのIPアドレス1億以上に対して脆弱性スキャンを実施

https://www.ncsc.gov.uk/files/Annual-Review-2020.pdf

2　米国のサイバーセキュリティに関する情報共有体制

本件に係る内容は、NISCの委託を受けたエヌ・ティ・ティ・コミュニケーションズ株式会社が調査しているものとなります

2　米国のサイバーセキュリティに関する情報共有体制

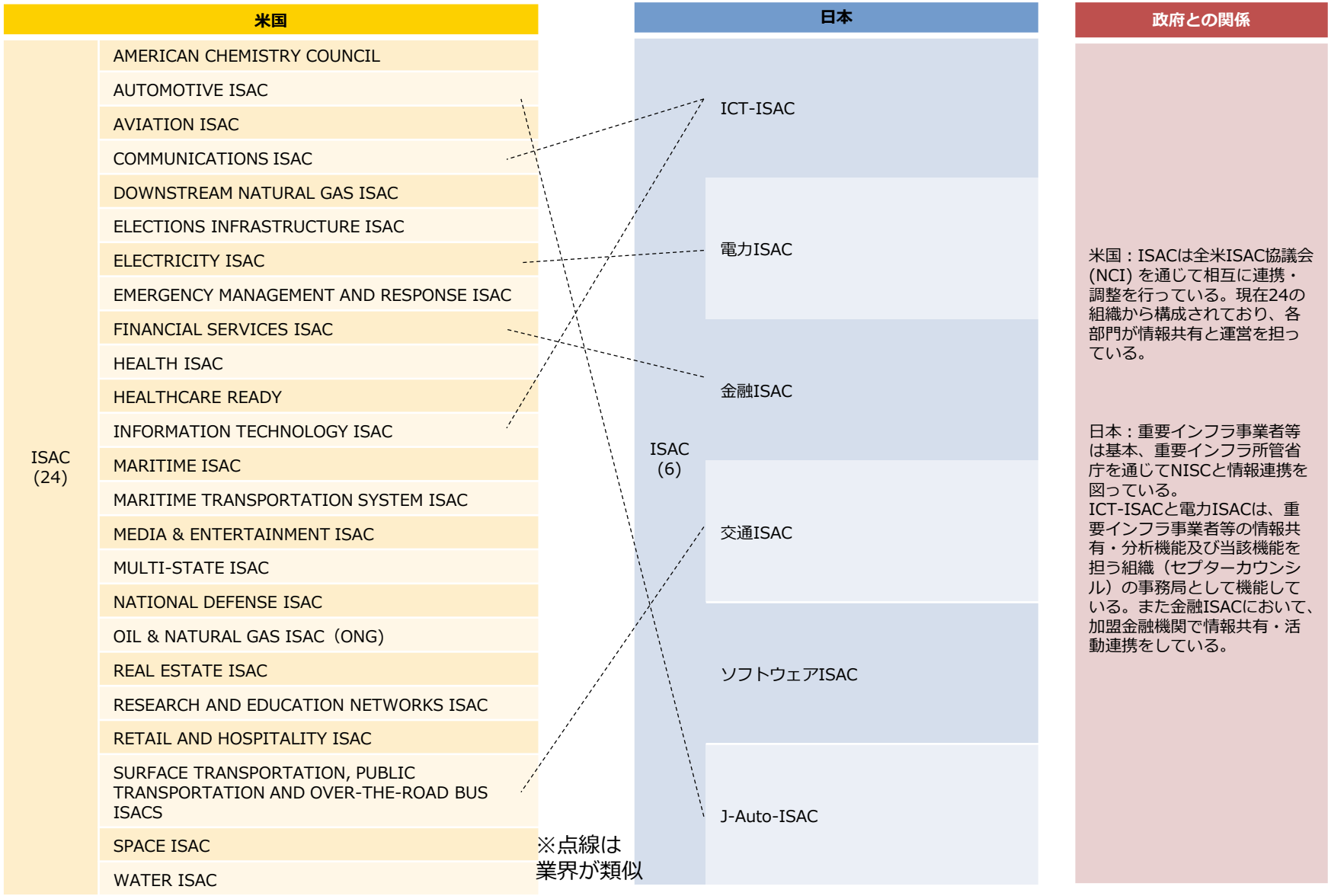


2　米国の施策等概要

米国		
関係主体	施策（実施主体）	概要
CISA	政府調整委員会:GCC	国家インフラ防護計画(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
	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
	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。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。
	インディケータ自動共有(AIS)	連邦政府および民間組織のシステム間で脅威指標共有や随時配信を行う。共有・配信にはSTIXおよびTAXIIの仕様を利用
重要インフラ分野	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
	全米ISAC協議会 (NCI)	セクタ間の関係強化や共通の問題等の意見交換
	ISAC	重要インフラを構成する民間の同じ業界の事業者同士で、サイバーセキュリティに関する情報を共有し、サイバー攻撃への防御力を高めることを目指して活動する民間組織 (24 ISAC)
重要インフラ分野以外	ISAO	ISAOはISACと同様にサイバー脅威に関する情報共有と分析を行う組織であるが、ISACが組織されていない分野やISACのメンバーでない民間企業など幅広い分野を対象として情報共有を可能とすることを目的としている

2　米国と日本のISACの比較

Information Sharing and Analysis Center（ISAC) は、重要インフラを構成する民間の同じ業界の事業者同士で、サイバーセキュリティに関する情報を共有し、サイバー攻撃への防御力を高めることを目指して活動する民間組織である。



2　米国ISAOの活動状況

Information Sharing and Analysis Organizations（ISAO）は、2013年2月12の大統領令に基づきDHSに設置促進が指示されたものである。

ISAOはISAC と同様にサイバー脅威に関する情報共有と分析を行う組織であるが、ISACが組織されていない分野やISACのメンバーでない民間企業など幅広い分野を対象として情報共有を可能とすることを目的としている。従って、ISACとは異なり、産業分野毎で関連付けられているものではなく、広く産官学の分野や地域等において団体が組織されている。

米国		政府との関係
カテゴリー	代表的なISAO	
地域ISAO (17) 産業・セクターISAO (46) 特定テーマISAO (7) その他ISAO (9)	・Cyber USA 各州に作られた官民パートナーシップ体制の集合体 2016 年10 月に7 組織で結成され、オバマ政権下でサイバーセキュリティ顧問を務めた Howard A.Schmidt 氏らが設立した財団により運営している ・Advanced Cyber Security Center 米国New England の大学・企業・政府機関等21 団体が参加する非営利ISAO（Facebook, RSA, Harvard University, MIT など） 情報共有により、最先端のセキュリティ研究や教育プログラムの作成、セキュリティ政策の作成を遂行する ・The National Cybersecurity Society 社員数499人以下の中小企業を対象とした非営利ISAO これまでISAC の枠組みに入れなかった中小企業に対し、セキュリティ情報の提供や教育を実施している ・Accountability Group 広告代理店の他、広告主や出版社、セキュリティベンダー、政府機関などが業種を超えてデジタル広告の不正排除、マルウェア防止などに取組む ・Global Resilience Federation FS-ISAC（金融）、Energy Analytic Security Exchange（エネルギー）、Legal services ISAO（法務）の3 組織を運営する ISAC・ISAO を束ねるISAO であるという点で特徴的 ・Information Association of Certified ISAOs 情報共有組織の立ち上げ・活動支援を行っている団体 国土安全保障省でISAO の枠組み作成に携わった者が設立したISAO ・The Trustworthy デジタル広告のセキュリティ向上を目的としたISAO 出典:サイバー攻撃に対するセキュリティ情報共有組織(ISAC)の構築に関する調査研究 https://www.jttri.or.jp/pdf/H29cyber_ISAC-houkoku.pdf	CISAの官民連携による情報共有分析組織であるNCCIC（国家サイバーセキュリティ通信統合センター）を通じて、ISAOとの継続的なコラボレーションを推進し、包括的な調整を行う

3　東京大会に向けて国内関係省庁が推進するサイバーセキュリティ対策（抜粋）

3　東京大会に向けて国内関係省庁が推進するサイバーセキュリティ対策（抜粋）

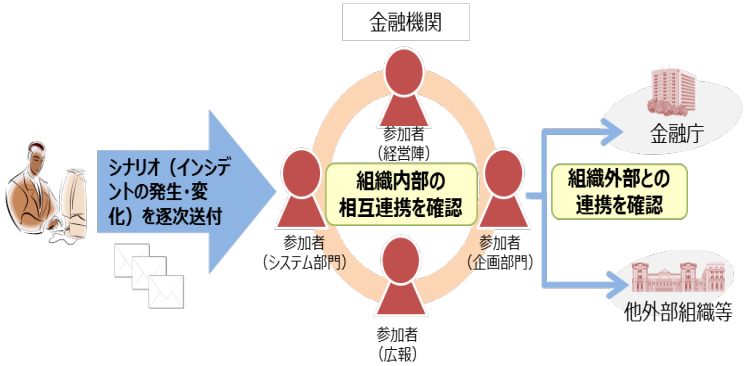
◘ 金融業界横断的なサイバーセキュリティ演習（Delta Wall）（金融庁）

- ✓　サイバー攻撃の脅威が金融システムの安定に影響を及ぼしかねない大きなリスクとなっている中、金融業界全体のインシデント対応能力を底上げするべく、「金融業界横断的なサイバーセキュリティ演習（Delta Wall（注））」を平成28年10月から毎年実施

（注）Delta Wall：サイバーセキュリティ対策のカギとなる「自助」、「共助」、「公助」の３つの視点（Delta）＋防御（Wall）

- ✓　預金取扱金融機関・証券会社のみでなく、資金移動業者や暗号資産交換業者等、各金融業態から広く参加を呼びかけており、例年100社以上が参加
- ✓　令和元年度の演習においては、2020年東京大会の開催時におけるリスク等を想定したシナリオとし、大規模インシデント発生時の金融機関内外の情報連携に係る対応体制や手順を検証・確認

演習スキーム



◘ 2020年東京大会に向けた実践的サイバー演習（サイバーコロッセオ）（総務省）

- ✓　近年さらに高度化・多様化するサイバー攻撃に備え、東京大会の適切な運営を確保することを目的として、大会関連組織のセキュリティ担当者等を対象とした、高度な攻撃にも対処可能な人材の育成を行う実践的サイバー演習「サイバーコロッセオ」を平成30年２月から本格的に実施
- ✓ 大規模演習環境を用いて、東京大会の公式サイト、大会運営システム等ネットワーク環境を模擬した、仮想のネットワーク環境を構築し、大会時に想定されるサイバー攻撃を疑似的に発生させ、攻撃者側の視点をも踏まえたハイレベルな防御手法の検証・訓練を行う演習を実施

サイバーコロッセオのイメージ

４　「英国の施策」と「米国の情報共有体制」を参考にした議論の方向性について（例）

「英国の施策」と「米国の情報共有体制」を参考にした議論の方向性について（例）

◘ サイバーセキュリティに関する対外的な窓口のワンストップ化の検討（特に対民間等）

- 英国では、中央政府内にサイバーセキュリティに関連する組織・チームが数多く存在し、各々の組織が相互の調整なしに指針を出すため重複や矛盾も生じ、産業界からも政府のどの部署に助言を求めればよいのかわからないと不満が募っていた。
- CESG-GCHQ の情報セキュリティ部門、CCA、CERT-UK、CPNIのサイバー関連部門等 -> NCSC

◘ サイバーセキュリティに関する情報共有プラットフォームの提供と集約の検討

- NCSCは、CiSP(※)を用いて、対民間との情報共有を実施している。政府や産業界のカウンターパートと、安全な環境で繋がることができ、監視や対策に役立てることが可能。
- JISP構築時に参考にした情報共有体制とそのプラットフォーム。

※Cyber Security Information Sharing Partnership

◘ 情報コミュニティの設立、活性化及びその連携の支援のための施策の検討

- 米国では、重要インフラ事業者によるISACだけでなく、ISACが組織されていない分野やISACのメンバーでない民間企業など幅広い分野を対象としてサイバー脅威に関する情報共有と分析を行う様々なISAOが、活発に活動している。

◘ サイバーセキュリティに関して政府が連携する範囲の拡大の検討（特に対民間）

- 重要インフラ事業者、公共セクターだけでなく、ベンダー、大企業、中小企業、教育機関などまで、広く連携対象にしている。

◘ サイバーセキュリティ対策のための政府による積極的な施策の検討

- “Active Cyber Defense”の概念の下、英国全体でセキュリティを飛躍的に向上させるための取組として、フィッシング、メールフィルタリング等の攻撃により発生する弊害から保護するための対策を提供。
- 英国では、大規模な詐欺行為に関連して大量の不正ドメインを閉鎖（テイクダウン）。