CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

# 国家サイバーセキュリティ・ガバナンス - ウクライナ

**アンドレイ・ダヴィディウク**

**NATO サイバー防衛センター・オブ・エクセレンス**

**オレクサンドル・ポティ**

**ウクライナ特別通信・情報保護局**

国家サイバーセキュリティ・ガバナンス・シリーズ

タリン 2024

## 著者について

**Andrii Davydiuk**:サイバーセキュリティの博士号取得者であり、NATO CCDCOE の技術研究者、ウクライナ特別通信情報保護局国家サイバー保護センター副支部長、ウクライナ科学アカデミー国立エネルギー工学モデリング研究所（G.E. Pukhov Institute for Modelling in Energy Engineering）の上級科学研究員。

**Oleksandr Potii :** ウクライナ特別通信・情報保護局副局長、技術科学博士、教授。

## この研究について

本書は、国別のサイバーセキュリティ・ガバナンスの包括的な概要を提供する一連の国別報告書の一部である。その目的は、さまざまな国のサイバーセキュリティ管理に対する認識を向上させ、各国が国内のサイバーセキュリティ・ガバナンスを強化するのを支援し、ベストプラクティスの普及を促し、省庁間および国際協力の発展に貢献することである。

主に NATO 協力サイバー防衛センター・オブ・エクセレンス（NATO CCDCOE）のスポンサー国である NATO 加盟国に焦点を当て、各国報告書は機関間のサイバーセキュリティの役割と責任の分担を概説し、それぞれの任務、タスク、能力、また機関間の調整について記述している。特に、政治的・戦略的管理、サイバーセキュリティの運用能力、サイバーインシデント管理、軍事的サイバー防衛、危機予防のサイバー的側面などの任務を取り上げている。また、特定の国の組織的アプローチの背景を明確にするために、その国の広範なデジタルエコシステムを紹介し、国のサイバーセキュリティ戦略の目標を概説している。

## CCDCOE

NATO 協力サイバー防衛センター・オブ・エクセレンス（CCDCOE）は、サイバー防衛における最も関連性の高い問題に対する独自の学際的アプローチを提供する NATO 公認の知識ハブである。CCDCOE の中心は軍、政府、学界、産業界からの多様な国際専門家グループであり、現在 39 カ国を代表している。

CCDCOE は、国際的に認知されたサイバー防衛のハブとしての地位を維持し、サイバー防衛の戦略的、法的、運用的、技術的側面における主要な専門知識源であり、基本的なリソースである。当センターは、サイバー防衛のあらゆる側面の最先端でソートリーダーシップを発揮し、この分野を 360 度見渡すことができる。当センターは、技術、戦略、作戦、法律という密接に関連した重点分野の中で、サイバーセキュリティを NATO と国家のガバナンスと能力の主流にするプロセスを奨励し、支援している。

CCDCOE の招きで作成された「タリン・マニュアル」は、国家間や非国家主体との間で行われるサイバー作戦に国際法がどのように適用されるかについて、政策アドバイザーや法律の専門家のための最も包括的な手引書である。2010 年以来、同センターは、世界最大かつ最も複雑な技術的実戦的サイバー防衛チャレンジである「Locked Shields」を開催している。毎年、Locked Shields はサイバーセキュリティの専門家に、リアルタイムの攻撃下で国家の IT システムや重要インフラを防衛するスキルを高める機会を与えている。その焦点は、現実的なシナリオ、最先端技術、そして戦略的意思決定や法律・コミュニケーション面を含む、大規模なサイバーインシデントの複雑さ全体をシミュレートすることにある。

CCDCOE は、世界のサイバー防衛コミュニティから主要な専門家や意思決定者を集め、タリンで毎年開催されるユニークなイベント「サイバー紛争に関する国際会議（CyCon）」を主催している。2009 年からタリンで開催されているこの会議には、毎年春に 600 人以上の参加者が集まる。

CCDCOE は同盟国全体のすべての NATO 機関のためにサイバー防衛活動の分野における教育訓練ソリューションを特定し調整する責任を負っている。NATO の認定を受けたセンター・オブ・エクセレンスは NATO 司令部の一部ではない。

www.ccdcoe.org publications@ccdcoe.org

**免責事項**

本書は NATO CCDCOE の成果物である。必ずしもセンター、NATO、加盟国の政策や意見を反映するものではない。当センターは、本出版物に含まれる情報の使用から生じるいかなる損失や損害についても責任を負わず、また本出版物で参照されている外部ウェブサイトを含む外部情報源の内容についても責任を負わない。

本出版物のデジタルコピーまたはハードコピーは、NATO 内部で使用する場合、および非営利かつ非商業的な目的で個人的または教育的に使用する場合に限り、完全な引用を付すことを条件に作成することができる。

# 目次

**1. デジタル社会とサイバーセキュリティ評価 ..... 5**

1.1 デジタル・インフラの利用可能性と利用率 ..... 5

1.2 デジタル公共サービス ..... 6

1.3 ビジネスにおけるデジタル化 ..... 14

1.4 サイバー脅威の状況とサイバーセキュリティ評価 ..... 15

**2. 国家サイバーセキュリティ戦略と法的枠組み ..... 20**

2.1 国家サイバーセキュリティ戦略文書 ..... 20

2.2 国家サイバーセキュリティ戦略 ..... 25

2.3 サイバーセキュリティ法 ..... 26

**3. 国家サイバーセキュリティ・ガバナンス ..... 37**

3.1 戦略的リーダーシップと政策調整 ..... 37

3.2 サイバーセキュリティの権限とサイバーインシデントへの対応 ..... 37

3.3 サイバー危機管理 ..... 39

3.4 軍事サイバー防衛 ..... 39

3.5 民間セクターとの関わり ..... 41

**4. 参考文献 ..... 43**

4.1 方針 ..... 43

4.2 法律 ..... 43

4.3 その他 ..... 47

**5. 略語 ..... 50**

# 1. デジタル社会とサイバーセキュリティ評価

## 1.1 デジタル・インフラの利用可能性と利用率

### ウクライナの国別指標（2023 年）

| | |
|---|---|
| **人口** | 37,289,000[1] （2019 年） |
| **インターネット利用者（人口比）** | 83.47%[2] (2020) |
| **面積（km2）** | 603,700 [3] |
| **一人当たり GDP（米ドル）** | 4,534[4] (2022) |

### 国際ランキング

| 国連統計 [5] | |
|---|---|
| **電子政府発展指数 2022** | 0.80290 （2022 年） 193 カ国中 46 位 |
| **オンライン・サービス・インデックス（OSI）** | 0.8148 (2022) |
| **電気通信インフラ指数（TII）** | 0.7270 (2022) |
| **人的資本指数（HCI）** | 0.8669 (2022) |

[1] "Results of Assessment of Existing Population of Ukraine Have Been Published" *(*www.kmu.gov.ua) <www.kmu.gov.ua/news/oprilyudneno-rezultati-ocinki-chiselnosti-nayavnogo-naselennya-ukrayini>, accessed on .08.2023.

[2] "2020 年 1 月 1 日現在の地域別インターネット加入者数" (ukrstat.*gov.ua*)<https://ukrstat.gov.ua/operativ/operativ2019/zv/zv_reg/kaI_reg/kaI_reg0419_u.htm>は 2023 年 6 月 8 日にアクセスされた。

[3] "National Atlas of Ukraine" (*World Data Centre* | *WORLD DATA CENTRE*) <http://wdc.org.ua/atlas/1060000.html> accessed on 06.08.2023.

[4] "GDP Per Capita (Current US$) - Ukraine" (*data.worldbank.org*) <https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=UA> accessed on 06.08.2023.

[5]"E-Government Development Index" <https://publicadministration.un.org/egovkb/en-us/Data/Country Information/id/180-Ukraine> accessed on 06.08.2023.

| EU 統計 [6] | |
|---|---|
| **グローバル・サイバーセキュリティ指数** | 66 % (2021) |
| **全米サイバーセキュリティ指数** | 80.83 % (2024) |

ウクライナ・グローバル・**サイバーインデックス・ランキング**（2023 年）

| | |
|---|---|
| **ICT 開発指数（IDI）（2017 年）** [7] | IDI ランク 79 |
| **全米サイバーパワー指数（NCPI）（2022 年）** [8] | NCPI ランク 13 |
| **ネットワーク・レディネス指数（NRI）（2022 年）** [9] | NRI ランク 43 |
| **核セキュリティ指数（NSI）（2023 年）** [10] | NSI ランク 24 |

## 1.2 デジタル公共サービス

ウクライナでは、国家をデジタル化し、デジタルサービスを実施するために、ウクライナデジタル変革省（MODT）が設立された。 [11] MODT は中央執行機関であり、その活動はウクライナ閣僚会議（CMU）によって指示・調整される。

国防省は、中央行政当局のシステムの中で、以下の分野における国家政策の形成と実施を保証する主要機関である：

デジタル化、デジタル開発、デジタル経済、デジタル革新と技術、電子統治と電子民主主義、情報社会の発展、情報化；

---

[6] 「NCSI：：ウクライナ" (*Index*) <https://ncsi.ega.ee/country/ua/210/> accessed on 06.06.2024.

[7] "ITU | 2017 Global ICT Development Index" (*ITU: Committed to connecting world*) <www.itu.int/net4/ITU D/idi/2017/index.html> accessed on 06.06.2024.

[8] "National Cyber Power Index 2022" (*Belfer Centre for Science and International Affairs*) <www.belfercentre.org/publication/national-cyber-power-index-2022> accessed on 06.06.2024.

[9] "Ukraine - Network Readiness Index" (*Network Readiness Index - Benchmarking Future of Network Economy*) <https://networkreadinessindex.org/country/ukraine/> accessed on 06.06.2024.

[10] "The 2023 NTI Nuclear Security Index" (*The Nuclear Threat Initiative*) <www.nti.org/analysis/articles/the-2023-nti nuclear-security-index/> accessed on 06.06.2024

[11] "About Us Ministry of Digital Transformation of Ukraine" (ウクライナデジタル変革省) <https://thedigital.gov.ua/ministry> accessed on 06.06.2024.

電子文書管理の実施、市民のデジタル・スキルとデジタル権の開発の分野；

オープンデータ、公的電子登録、国家電子情報資源の開発と相互運用性、ブロードバンド・インターネットアクセス・インフラの開発、e コマースと e ビジネス；

電子サービスおよび管理サービス、電子信託サービス、電子身分証明書の提供；

IT 産業の発展、ディア市の法体系の整備と運用の分野。

その活動において、MODT は MODT 規則（[12] ）に従っている。

MODT は命令によってその権限を実施する。2021 年 2 月 17 日付ウクライナ閣僚会議（Cab. of Ministers of Ukraine）第 365-r 号[13] および 2019 年 1 月 30 日付ウクライナ閣僚会議（Decree of the Cabinet of Ministers of Ukraine）第 56 号[14] .

同時に、CMU は「社会領域のデジタル変革戦略」[15] 、2025 年までの「デジタル開発、デジタル変革、国家財政管理システムのデジタル化実施戦略」[16] 。

ウクライナの各省庁、その他の中央行政機関、地方軍政機関では、2020 年 3 月 3 日付 CMU 決議第 194 号（[17] ）により、デジタル開発関連機関の副責任者であるチーフ・デジタルトランスフォーメーション・オフィサー（CDTO）の役職が導入された。

ウクライナにおけるデジタル化のペースと範囲を拡大するため、デジタル問題省は電子サービスの統一ウェブポータル「Dia」を創設した。[18]

---

[12] デジタル変革省の課題 2019 年 9 月 18 日付ウクライナ閣僚会議決議 第 856 号：2024 年 1 月 13 日現在 <https://zakon.rada.gov.ua/laws/show/856-2019-п#Text> accessed on .06.2024

[13] デジタルトランスフォーメーションの課題：命令 2021 年 2 月 17 日付ウクライナ閣僚会議第 365-r 号：5 月 4 日現在 <https://zakon.rada.gov.ua/laws/show/365-2021-p#Text> 2024 年 6 月 6 日アクセス。

[14] デジタル開発の問題 2019 年 1 月 30 日付ウクライナ閣僚会議決議第 56 号：2023 年 6 月 30 日現在 <https://zakon.rada.gov.ua/laws/show/56-2019-п#Text> 2024.06.06 にアクセスした。

[15]社会領域のデジタル変革戦略の承認について：命令。Cab. of the Ministers of Ukraine dated October 28, 2020 No. 1353-r <https://zakon.rada.gov.ua/laws/show/1353-2020-p#Text> accessed on 06.06.2024.

[16]2025 年までの期間における国家財政管理システムの デジタル開発、デジタル変革、デジタル化の実施戦略の承認と、その実施に向けた措置計画の承認に関する：命令 2021 年 11 月 17 日付ウクライナ閣僚会議第 1467-r 号：2023 年 4 月 11 日現在 <https://zakon.rada.gov.ua/laws/show/1467-2021-p#Text> 2024 年 6 月 6 日アクセス。

[17]中央・地方行政機関の デジタル開発、デジタル変革、デジタル化の問題に関するユニット、中央行政機関の副首長、地方行政機関、キエフ市、セヴァストポリ市のデジタル開発、デジタル変革、デジタル化の問題に関する活動の課題：Decree of the Cabinet of Ministers of Ukraine dated 03.03.2020 No. 194<https://zakon.rada.gov.ua/laws/show/194-2020-п#Text> accessed on 06.06.2024.

[18]"電子サービス DIIA の統一国家ウェブポータル｜国家企業「DIIA」" (State Enterprise "DIIA")<https://se.diia.gov.ua/unified-state-web-portal-of-electronic-services-diia> accessed on 06.06.2024.

2019 年 12 月 4 日の CMU 決議 No.1137 によって承認された「電子サービスの統一国家ウェブポータルに関する規則」。1137、[19] 、Dia ポータルは、行政その他の公共サービスに関する電子サービスや情報へのアクセス、行政当局、その他の国家機関、地方自治機関、企業、機関、組織への不服申し立て（ウクライナ法「市民の不服申し立てについて」によるものを含む）、[20] 、サービスの提供に必要な国家電子情報資源からの情報取得、ならびに本規則で規定された場合におけるサービスの質の監視および評価を行う、すべての人の権利を実施することを意図していると決定した。"

一般的に、デジタル省は「Dia」、「Dia.デジタル教育」、「Dia.ビジネス」、「インターネット上の子供の安全」、「電子居住」、「Dia.City」、「欧州統合」、「すべての教師にノートパソコンを」、「仮想資産」、「Dia.センター」 [21]

「Dia」モバイル・アプリケーションのおかげで、ウクライナの市民はスマートフォンから電子文書を利用できる。

デジタル文書の法的効力は、以下の法律で定められている：

- e-パスポートと TIN：2021 年 8 月 18 日付 CMU 決議第 911 号、[22] 。

- e-出生証明書 2020 年 9 月 23 日付 CMU 決議第 911 号; [23]

- 電子証明書：2014 年 10 月 1 日付 CMU 決議 第 509 号[24] ；

- e-student カード：2019 年 12 月 18 日付 CMU 決議第 1051 号[25] .

---

[19] 電子サービスの統一国家ウェブポータルと行政サービスの統一国家ポータルの発行：2019.12.04 付け閣僚閣僚決議第 1137 号：2024 年 4 月 2 日現在<https://zakon.rada.gov.ua/laws/show/1137-2019-п#Text> 2024.06.06 にアクセスした。

[20] 市民の上訴について 1996 年 10 月 2 日付ウクライナ法第 393/96-VR 号：2023 年 12 月 31 日現在 <https://zakon.rada.gov.ua/laws/show/393/96-вр#Text> 2024 年 6 月 6 日アクセス。

[21] About Us ウクライナデジタル変革省（Ministry of *Digital*Transformation of Ukraine） <https://thedigital.gov.ua/ministry> accessed on 06.06.2024.

[22] e-パスポートおよび海外渡航用 e-パスポート、それらの電子コピーの作成・検証手続きの承認に関する：2021 年 8 月 18 日付閣議令第 911 号：2022 年 11 月 17 日現在 <https://zakon.rada.gov.ua/laws/show/911-2021-п#Text> 2024 年 6 月 6 日アクセス。

[23] 出生証明書に記載された情報および本籍地に関する情報を電子的に表示する実験的プロジェクトの実施について。移住サービス 2020 年 9 月 23 日付ウクライナ閣僚会議令第 911 号：3 月 14 日現在。2022 <https://zakon.rada.gov.ua/laws/show/911-2020-п#Text> accessed on 06.06.2024.

[24] 国内避難民の会計について：Decree of the Cabinet of Ministers. of Ukraine dated October 1, 2014 No. 509: as of November 24 2023 <https://zakon.rada.gov.ua/laws/show/509-2014-п#Text> accessed on 06.06.2024.

[25] 電子学生（生徒）チケットの使用に関する実験的プロジェクトの実施について：Decree of the Cabinet of Ministers. of Ukraine dated 18.12.2019 No. 1051: as of February 1 2022 <https://zakon.rada.gov.ua/laws/show/1051-2019-п#Text> accessed on 06.06.2024.

デジタル・トランスフォーメーションに関するウクライナ・ヴェルホヴナ・ラーダ委員会は、ウクライナでも機能しており、2019 年 8 月 29 日に第 9 回召集のウクライナ・ヴェルホヴナ・ラーダに設置された-[26] 。

委員会の主題は以下の通りである：

- ウクライナにおけるデジタル化とデジタル社会の立法原則；

- 国家および州の情報化プログラム；

- EU のプログラム「デジタル単一市場」（Digital Single Market、EU4Digital）およびその他のデジタル協力プログラム；

- デジタル・アントレプレナーシップの分野における革新、スタートアップ・エコシステムの開発；

- デジタル技術分野の研究センター；

- デジタル産業と電気通信；

- 電子統治と公共電子サービス

- 電子民主主義；

- 電子信託サービスとデジタル ID；

- 国家情報と分析システム、電子文書フロー；

- 州の情報資源、電子登録簿、データベース；

- e コマース（電子商取引、e ビジネス）；

- 仮想資産、ブロックチェーン、トークン化；

- スマートインフラ（都市、コミュニティなど）；

- オープンデータ」分野の発展；

- 無線周波数資源；

- 軌道経済の発展

[26] 第 9 回召集のウクライナ・ヴェルホヴナ・ラーダの委員会のリスト、量的構成、テーマについて：2019 年 8 月 29 日付ウクライナ議会の決議 Verkhov.第 19-IX 号：2023 年 2 月 23 日現在<https://zakon.rada.gov.ua/laws/show/19-20#Text> 2024.06.06 にアクセス。

- ウクライナにおけるインターネットの管理、機能、利用に関する立法原則；

- 重要インフラの分野を含むサイバーセキュリティとサイバー保護 - 情報の技術的・暗号的保護

- デジタル・コンピテンシーとデジタル・ライツの育成。

またウクライナでは、2021 年 2 月 8 日付 CMU 決議第 94 号（[27] ）により、国家機関のニーズに対応するため、国家情報資源保存ナショナルセンターが設置された。

国家情報資源確保国家センター（以下、国家センター）は、国家情報資源の信頼性と中断のない運用、サイバー保護、国家電子情報資源の保管、国家機関、軍事組織（軍隊と国防省の主要情報総局を除く）、企業、機関、組織の国家電子情報資源の情報とバックアップを確保するために設立された組織体である。国家センターの機能を確保する任務は、ウクライナ特別通信情報保護局（SSSCIP）に課せられている。国家情報資源保護国家センターの運営メカニズムは、CMU の決議（2023 年 7 月 4 日付）第 311 号で定められている。[28]また、2022 年 3 月 3 日付 CMU 決議第 522 号は、国家情報資源予約ナショナルセンターへのサービス提供手順を定めている。[29]特に以下のサービスが提供される：

1. 電子通信キャビネットまたはその一部を共用ホールに設置すること。
2. 遮蔽されたホール内の電子通信キャビネットに機器を設置すること。
3. 独立したスクリーンホールの電子通信キャビネットに機器を設置すること。
4. 共用ホールにある情報保存の技術的手段のためのディスクスペースを提供する。
5. 情報保存の技術的手段のためにディスクスペースを提供する。
6. 情報保管の技術的手段のためのディスクスペースを提供する。
7. 共用ホールにコンピューティングリソースを提供する。
8. スクリーンのあるホールでコンピューティングリソースを利用できる。
9. 独立したスクリーンホールにコンピューティングリソースを提供する。
10. 物理サーバーを別途レンタルする。

---

[27] 国家情報資源保存国立センターの機能に関する実験的プロジェクトの実施について：2021 年 2 月 8 日付閣議令第 94 号：2023 年 4 月 11 日現在 <https://zakon.rada.gov.ua/laws/show/94-2021-п#Text> 2024 年 6 月 6 日アクセス。

[28] 国家情報資源保存国立センターの機能に関する問題：ウクライナ閣僚会議決議（2023 年 7 月 4 日付）第 311 号 <https://zakon.rada.gov.ua/laws/show/311-2023-п#Text>（2024 年 6 月 6 日閲覧）。

[29] 国家情報資源保存国立センターのサービス提供手続きの承認について：2022 年 5 月 3 日付ウクライナ閣僚会議決議第 522 号：2023 年 4 月 11 日現在<https://zakon.rada.gov.ua/laws/show/522-2022-п#Text> 2024 年 6 月 6 日アクセス。

11. 使用する仮想サーバーを提供する。

12. 動的に割り当てられたディスクリソースの使用を提供する。

13. 国の電子情報資源の処理（保存）に使用されるコンピュータ資源のバックアップ。

14. 国家電子情報資源の処理（保存）に使用される国家電子情報資源のバックアップ。

15. コンピューティングリソースを利用したソフトウェアの利用を提供する。

16. 国の電子情報資源を配置する。

17. 国の電子情報資源を管理する。

18. 国の電子情報資源を保管する。

19. 国の電子情報資源を処理・保存するシステムのインターネットへのアクセスは、保護されたノードに接続する。

20. 国の電子情報資源へのアクセスを組織するための安全な通信手段を提供する。

21. 国の電子情報資源を管理するための安全な通信手段を提供する。

22. 国の情報資源への安全なモバイルアクセスを提供する。

23. 災害後の国家電子情報資源の復旧。 {項目 23 は、2023 年 7 月 4 日の閣議決定第 311 号により変更されたものである。}

24. 国の電子情報資源のバックアップコピーを保存する。

25. 国の電子情報資源のデータアーカイブを保存する。

26. サイバー攻撃（DDoS 攻撃など）の検知と防御。

27. サイバー防衛施設のコンピューティングリソースのシミュレーションを展開する。

28. ユーザー・ドメイン名システムにおける情報の保護。

29. ユーザー機器へのサイバーインシデントやサイバー攻撃を検知する。

30. データ伝送ネットワークへの不正アクセスを検知・防止する。

31. ネットワーク画面の技術的能力を利用して情報資源を保護する。

32. 外部のサイバー脅威から電子メールを保護する。

33. セキュリティ・ポリシーによってデータ伝送ネットワークへのアクセスを管理する。

34. 特権ユーザーアカウントの管理。

35. コンピューターシステムやネットワークがサイバー攻撃に対して脆弱であるかどうかをテストする。

36. コンピュータプログラムのセキュリティ研究のために、安全で隔離された仮想環境を提供する。

37. サイバー事件やサイバー攻撃からウェブサイトを守る。

38. 仮想セキュアデータ伝送ネットワークを提供する。

さらに、国家機関と重要インフラ施設のサイバー保護のため、SSSCIP は、2020 年 12 月 16 日付の CMU 決議第 1358 号によって機能する全国電気通信ネットワークの実施を保証している。[30] 。

全国的な電気通信ネットワークは、以下を目的としている：

国家情報資源の流通（送信、受信、作成、処理、保存）と保護、安全な電子通信の提供；

平時、緊急時、特別時の国家管理のために、国家電気通信網（NTN）のサービスを提供し、利用者にサイバー保護サービスを提供する。

NTN のサービス一覧は、2021 年 8 月 17 日付ウクライナ国家特別通信・情報保護庁命令第 502 号により決定されている[31]特に、以下のサービスグループが利用できる：

- NTN の輸送電子通信サービス；
- 特別通信サービス；
- NTN のマルチメディアサービス；
- 情報資源へのアクセスサービス - サイバー保護サービス

これとは別に、政府機関にインターネットへの安全なアクセスを提供している国家サイバー保護センター（[32] ）の、国家機関のインターネットへの保護アクセス・システムも注目に値する。

---

[30] 全国電気通信ネットワークの機能に関する問題：2020 年 12 月 16 日付ウクライナ閣僚会議決議第 1358 号（2022 年 8 月 20 日付）<https://zakon.rada.gov.ua/laws/show/1358-2020-п#Text> 2024 年 6 月 6 日閲覧。

[31] 全国電気通信ネットワークのサービスリストの承認について：2021 年 8 月 17 日付のウクライナ政府通信・情報特別業務省令第 502 号。Govt. Special Services Communication and of Information of Ukraine, August 17, 2021 No. 502: as of April 12 2023. <https://zakon.rada.gov.ua/laws/show/z1288-21#Text> accessed on 06.06.2024.

[32] 重要インフラ対象物のサイバー保護に関する一般要件の承認について：2019 年 6 月 19 日付ウクライナ閣僚会議決議第 518 号：9 月 7 日現在。2022. <https://zakon.rada.gov.ua/laws/show/518-2019-п#Text> accessed on 06.06.2024.

SSSCIP はまた、ウクライナ CERT-UA（[33] ）のウクライナ・コンピューター緊急対応チーム（Computer Emergency Response Team of Ukraine）の機能も確保している。同チームは、サイバーインシデントについて市民から寄せられた情報を処理している。

ウクライナの国家機関がデジタル・サービスを提供する際の情報保護とその実施を規定する主な規制文書は以下の通りである：

- ウクライナ法「情報通信システムにおける情報保護について」；[34]
- CMU 決議「情報通信および情報通信システムにおける情報保護の確保に関する規則の承認について」；[35]
- CMU の決議「重要インフラ対象物のサイバー保護に関する一般要件の承認について」；[36]
- ウクライナ法「個人データの保護について」；[37]
- ウクライナ法「電子身分証明書および電子信託サービス」;"[38]
- CMU 決議「情報・電子通信システムにおける国家情報資源の保護問題に関する行政当局の相互作用のための手続きの承認について」；[39]

[33] 「CERT-UA" (*cert.gov.ua*) <https://cert.gov.ua/about-us> 06.06.2024 にアクセスした。

[34] 情報通信システムにおける情報の保護に関する：1994 年 5 月 7 日付ウクライナ法/94-VR 号：2024 年 4 月 4 日現在 <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text> 2024 年 6 月 6 日アクセス。

[35] 情報、電気通信、情報通信システムにおける情報保護を確保するための規則の承認について：2006 年 3 月 29 日付ウクライナ閣僚会議決議第 373 号：2022 年 10 月 21 日現在<https://zakon.rada.gov.ua/laws/show/373-2006-п#Text> 2024 年 6 月 6 日アクセス。

[36] 重要インフラ対象物のサイバー保護に関する一般要件の承認について：2019 年 6 月 19 日付ウクライナ閣僚会議決議第 518 号：9 月 7 日現在。2022. <https://zakon.rada.gov.ua/laws/show/518-2019-п#Text> accessed on 06.06.2024.

[37] 個人情報の保護について：2010 年 6 月 1 日付ウクライナ法第 2297-VI 号：2024 年 4 月 27 日現在 <https://zakon.rada.gov.ua/laws/show/2297-17#Text> 2024 年 6 月 6 日アクセス。

[38] 電子信託サービスについて：2017 年 10 月 5 日付ウクライナ法第 2155-VIII 号：2024 年 1 月 1 日現在。 <https://zakon.rada.gov.ua/laws/show/2155-19#Text> 2024.06.06 にアクセス。

[39] 情報通信システムにおける国家情報資源の保護に関する行政当局の相互作用のための手続きの承認に関する：2002 年 11 月 16 日付ウクライナ閣僚会議決議第 1772 号：9 月 7 日現在。2022 <https://zakon.rada.gov.ua/laws/show/1772-2002-п#Text> accessed on .06.2024.

- 行政当局、およびその管理領域に属する企業、機関、組織の情報、電子通信、情報通信システムの登録に関する規則（2005 年 8 月 3 日より第 688 号）；[40]

- 情報化ツールの設計、導入、運用における必須作業段階リスト（1998 年 2 月 4 日第 121 号より）；[41]

- 情報通信システム（ICS）登録簿（2007 年 4 月 24 日 No.72 より）の情報基金の形成および使用に関する手続き。[42] 。

## 1.3 ビジネスにおけるデジタル化

ビジネスを拡大し、官僚的な手続きを簡素化するために、デジタル省は Dia.Business プロジェクトを開発した。[43]

これは、国土開発省が 2020 年 2 月に開始した起業家精神と輸出発展のための大規模な国家プロジェクトである。2021 年 5 月からは、国土開発省がウクライナの国内外市場における起業家精神の開発・支援を担当する国家機関である起業家精神・輸出開発事務所とともにプロジェクトを実施する。プロジェクトのウェブポータルは、すでに起業に携わっている、あるいはこれから起業を計画しているウクライナ人に情報を提供する：

- 起業の準備をどうするか；

- どこで勉強し、どこで相談を受けるか；

- 国や国際的なプログラムから、ビジネスのための資金援助を受けることができる；

- 投資家やパートナーを見つける方法

- 女性起業家支援プログラムについての詳細はこちら；

- 様々な業種向けの銀行支援プログラム

---

[40] 行政当局、およびその管理領域に属する企業、機関、組織の情報、電気通信、情報通信システムの登録に関する規則の承認に関する：2005 年 8 月 3 日付ウクライナ閣僚会議決議第 688 号：9 月 7 日現在。2022 <https://zakon.rada.gov.ua/laws/show/688-2005-п#Text> accessed on 06.06.2024.

[41]情報化施設の 設計、実施、運用における必須作業段階リストの承認に関する：1998 年 2 月 4 日付ウクライナ閣僚政令第 121 号：9 月 3 日現在。2011 <https://zakon.rada.gov.ua/laws/show/121-98-п#Text> accessed on 06.06.2024.

[42] 行政当局、およびその管理範囲に属する企業、機関、組織の情報、電気通信、情報通信システム登録簿の情報基金の形成および使用手続きの承認に関する：命令管理者 Govt. special services communication and of Information of Ukraine date April 24, 2007 No. 72: as of January 10 2023. <https://zakon.rada.gov.ua/laws/show/z0500-07#Text> accessed on 06.06.2024.

[43] "National project Diia.business" (Diia.business - Main page) <https://business.diia.gov.ua/about-project> accessed on .06.2024.

- 州のオンライン・サービスを利用してビジネスを行う方法。

Dia.Business は Diya エコシステムのサブブランドである。

Dia はデジタル国家のブランドであり、プロジェクトのエコシステムである：Diya ポータル、Diya モバイル・アプリケーション、Dia.Digital 教育、Dia.Business、Dia City 国家プロジェクトである。

## 1.4 サイバー脅威の状況とサイバーセキュリティ評価

サイバーセキュリティの確保は国家安全保障に必要な要素である。[44]ウクライナのサイバーセキュリティ戦略の第 3 章「安全なサイバースペース」には、国のサイバースペースに対する課題とサイバー脅威が記載されており、国の成功発展の鍵を構成している。[45]これらには以下が含まれる：

- 国際競争においてサイバー手段を積極的に活用する；

- 情報通信技術、特にクラウドや量子コンピューティング、5G ネットワーク、ビッグデータ、モノのインターネット（IoT）、人工知能（AI）などが急速に進歩している状況下で、サイバーセキュリティ・ツールの開発には競争原理が働いている；

- サイバースペースの軍事化とサイバー兵器の開発は、サイバースペースにおける敵対行為や情報破壊活動を支援するためのサイバー攻撃を秘密裏に実行することを可能にする；

- COVID-19 の大流行が経済活動や社会行動に与えた影響であり、電子サービスや ICS の広範な利用によって、遠隔地における社会関係のかなりの部分が急速に変化し、再編成された；

- 新しい技術、デジタルサービス、市民と国家間の電子的相互作用の仕組みの導入が、サイバーセキュリティ対策の面で体系的でなく、適切なリスク評価なしに行われている。

ウクライナのサイバーセキュリティに対する脅威には次のようなものがある：

サイバースペースにおけるロシア連邦のウクライナに対するハイブリッド攻撃。侵略国家は、攻撃的なサイバー兵器の武器を絶えず拡大しており、その使用は、回復不能かつ不可逆的な破壊的結果をもたらす可能性がある。ロシア連邦のサイバー攻撃は、何よりもまず、ウクライナの国家機関の ICS や重要な情報インフラの対象物を無力化し（サイバー破壊工作）、秘密裏にアクセス・支配を獲得し、諜報活動や情報破壊活動を行うことを目的としている。サイバー攻撃はまた、侵略国家が特殊な情報作戦の要素として積極的に利用し、住民に操作的な影響を与え、選挙プロセスを妨害し、ウクライナの国家としての信用を失墜させている；

---

[44] ウクライナの国家安全保障について 2018 年 6 月 21 日付ウクライナ法第 2469-VIII 号：3 月 31 日現在。2023 <https://zakon.rada.gov.ua/laws/show/2469-19#Text> accessed on 06.06.2024.

[45]2021 年 5 月 14 日付ウクライナ 国家安全保障・防衛評議会決定「ウクライナのサイバーセキュリティ戦略について」：2021 年 8 月 26 日付ウクライナ大統領令 第 447/2021 号 <https://zakon.rada.gov.ua/laws/show/447/2021#Text> 2024 年 6 月 6 日閲覧。

サイバー犯罪は、情報資源、社会プロセス、市民個人に損害を与え、情報技術に対する国民の信頼を低下させ、重大な物質的損失をもたらす。ウクライナの国家安全保障の基盤に対する犯罪、犯罪収益の合法化に関連する犯罪、人身売買、武器・弾薬・爆発物の違法な取り扱いにサイバースペースを利用すること；他国政府によって組織・支援された、麻薬、向精神薬、その類似品や前駆物質（広まりつつある）、その他人々の生命や健康を脅かす対象物や物質の違法流通、政治・経済・軍事目的の機密情報の窃取に関連するサイバー攻撃（すなわち、ウクライナの国家安全保障の基盤、犯罪収益の合法化に関連する犯罪）。e.,諜報活動や破壊活動の実施などである。このようなサイバー攻撃の特徴は、その期間、複雑さ、隠れた性質であるため、防止、検知、無力化が困難であること、テロ組織がサイバー空間を利用して、サイバーテロ行為、金融犯罪、テロ活動を支援するその他の不法行為を行うことである。

ウクライナがサイバースペースで直面している課題や脅威を考慮すると、国家のデジタル変革のプロセスにおけるサイバーセキュリティの役割は極めて重要になっている。

脅威を形成する前提条件と要因：

ウクライナは、情報通信技術製品の海外メーカーへの技術依存度が高く、そうした製品のセキュリティ要件への適合性を評価するシステムがないため、未申告の機能による情報インフラの脆弱性の度合いが高まり、サイバー脅威への対抗能力が低下している；

サイバーセキュリティの分野における規制と法的枠組みの不完全さ、情報保護の分野における陳腐化、欧州法の規定の遅々たる実施、犯罪捜査のデジタル要素に関する不十分な規制、この分野における法律の要件に違反した場合の法的責任の低さなどである；

国家機関の大部分において、サイバー保護に関連する構造的な下部組織、必要な人員配置、適切な管理体制が欠如していることに加え、サイバー保護事業の残余ベースでの資金調達が不十分である；

行政の全領域と国家の生活活動がダイナミックにデジタル化されている状況において、情報セキュリティの独立監査制度と、脆弱性に関する情報を開示する仕組みが欠如している；

サイバーセキュリティとサイバー保護の専門家の訓練レベルと高度な訓練に関する最新の要件に準拠していないこと、特に、公共部門で働く意欲を高める仕組みが効果的でない；

ウクライナの重要インフラとその保護に関する法律がないため、こうしたインフラのサイバー保護システムの形成が著しく複雑になっている；

現代の脅威、サイバー空間における課題、サイバーセキュリティ産業の発展における世界的動向に対応するサイバー保護の組織的・技術的モデル（OTM）を実施するための対策が不完全である；

市民のデジタル・リテラシーを向上させ、サイバースペースで安全に行動する文化を醸成するためのシステムが欠如しており、サイバー脅威やサイバー保護に対する市民の意識が低いことがそれに拍車をかけている；

サイバーセキュリティに関する効果的な情報・分析支援システムが欠如している；

国家の情報資源や重要な情報インフラの対象へのサイバー攻撃に対する防御が不十分である；

アクセスが制限された情報の大部分が処理されている国家機関や経済団体の ICS 保護状態に関する法律の要件に準拠していない。

ウクライナ国家安全保障防衛会議（NSDC）[46] は、国家のサイバーセキュリティに対する脅威を無力化するための緊急措置を決定した。

州は、州の情報資源が処理される情報、電子通信、ICS の構成における脆弱性や欠陥を特定するための手順を有している。[47] 脆弱性の検出と、そのようなサイバー事件やサイバー攻撃への対応。[48] 情報（自動化された）、電子通信、ICS、電子通信ネットワークのオープンな脆弱性の検索と検出[49] ；情報、電子通信、ICS における国家情報資源のセキュリティ状態の評価、 [50] インターネットに掲載された政府情報資源の脆弱性のスキャン、[51] 重要情報インフラ、国家情報資源、情報のサイバー保護状態のレビュー、および法

[46] 国家のサイバーセキュリティに対する脅威とそれを無力化するための緊急措置について：2016 年 12 月 29 日付ウクライナ安全保障・防衛国家評議会決定：2017 年 2 月 16 日現在 <https://zakon.rada.gov.ua/laws/show/n0015525-16#Text> 06.06.2024 にアクセス。

[47]国家情報資源が処理される情報・通信・情報通信システムの構成における脆弱性や欠陥を特定するための、 一連の組織的・技術的措置の導入に関する実験的プロジェクトの実施について：2020 年 12 月 23 日付ウクライナ閣僚会議決議第 1363 号：9 月 7 日現在。2022 <https://zakon.rada.gov.ua/laws/show/1363-2020 п#本文> 2024 年 6 月 6 日にアクセスされた。

[48] 脆弱性を検知し、サイバーインシデントやサイバー攻撃に対応するシステムの機能を確保する上での問題点：2020 年 12 月 23 日付ウクライナ閣僚会議決議第 1295 号：9 月 7 日現在。2022 <https://zakon.rada.gov.ua/laws/show/1295-2020-п#Text> accessed on 06.06.2024.

[49] 情報（自動化）、電子通信、情報通信システム、電子通信ネットワークの潜在的脆弱性を検索・特定するための手順の承認について：Decree of the Cabinet of the Ministers of Ukraine dated May 16, 2023 No. 497 <https://zakon.rada.gov.ua/laws/show/497-2023 п#Text> accessed on 06.06.2024.

[50]情報・電気通信・情報通信システムにおける国家情報資源のセキュリティ状態の評価手順の承認に関する：2014 年 12 月 2 日付のウクライナ政府通信情報特別局の命令である。Govt. Special Services Communication and of Information of Ukraine dated 02.12.2014 No. 660: as of January 10 2023. <https://zakon.rada.gov.ua/laws/show/z0090-15#Text> accessed on 06.06.2024.

[51]インターネットに掲載されている国家情報資源の脆弱性をスキャンする手順の承認について：2016 年 1 月 15 日付のウクライナの行政当局の命令である。Govt. special services communication and of Information of Ukraine dated January 15, 2016 No. 20: as of January 10 2023 <https://zakon.rada.gov.ua/laws/show/z0196-16#Text> accessed on 06.06.2024.

律で定められた保護要件。[5253] 特に、脆弱性を検知し、サイバー事件やサイバー攻撃に対応するシステムの運用を確保するため、ICS のテレメトリー収集サブシステム（アクティブセンサー）の機器一式[54] 。

サイバー保護の状況に関する包括的なレビューは、SSSCIP の関連する定期報告書、特に「重要情報インフ ラ、国家情報資源、法律で保護要件が定められている情報のサイバー保護状況に関するレビュー 報告書」で入手できる、[55]「ICS における国家電子情報資源の保護状況に関する情報および分析資料」、[56] 「2023 年上半期のウクライナのサイバーセキュリティ戦略計画の実施に関する分析報告書」、[57] 「2022 年における国家のサイバーセキュリティ確保に関連するタスクのウクライナ国家特別通信情報保護局による実施に関する報告書」、[58]脅威調査の結果に基づく SSSCIP の分析報告書」、[59] 「サイバーインシデントおよびサイバー攻撃に対する脆弱性の検出と対応のシステムに関する報告書」、[60] 「デジタル変革に関するウクライナ・ヴェルホヴナ・ラーダ委員会」、特に「国家サイバーセキュリティの主要主体の活動に関する独立監査の結果に関する年次報告書の提出とさらなる評価に関する報告書」、[61]ウクライナ法「ウクライナにおけるサイバーセキュリティの主要原則について」の実施状況の監視に関する予備的分析報告書」、[62] 「ウクライナのサイバーセキュリティおよび重要インフラの対象に関する法律のプロジェクトで実施されなければ

---

[52] 重要情報インフラ、国家情報資源、情報のサイバー保護状態のレビューの実施手順の承認について：2020 年 11 月 11 日付ウクライナ閣僚会議決議第 1176 号 <https://zakon.rada.gov.ua/laws/show/1176-2020-п#Text> 2024 年 6 月 6 日アクセス。

[53] 重要情報インフラ、国家情報資源、および法律で保護が義務付けられている情報のサイバー保護状況の見直しに関する省庁間ワーキンググループの結成について：政府通信・特殊業務省令 Govt. Special Services Communication and of Information of Ukraine, September 10, 2021 No. 550: as of November 2 2023 <https://zakon.rada.gov.ua/laws/show/z1264-21#Text> accessed on 06.06.2024.

[54] 情報通信システム（アクティブセンサー）のテレメトリー収集サブシステム、脆弱性を検出し、サイバーインシデントやサイバー攻撃に対応するシステムの機器一式をサイバー保護対象に譲渡する手続きの承認について：管理者の命令である。2022 年 6 月 24 日付ウクライナ特別通信・情報保護国家サービス第 284 号 <https://zakon.rada.gov.ua/laws/show/z0758-22#Text> 2024 年 6 月 6 日アクセス。

[55]法律（SSSCIP 2023）で保護が義務付けられている、重要情報インフラ、国家情報資源、情報のサイバー保護状況の見直しに関する報告書。

[56]*ICS*(SSSCIP2023)における国家電子情報資源の保護状況に関する情報提供および分析資料。

[57]*2023* 年上半期のウクライナのサイバーセキュリティ戦略計画（SSSCIP 2023）の実施に関する分析報告書。

[58]*2022* 年におけるウクライナ国家特殊通信情報保護局による国家のサイバーセキュリティ確保に関する任務の実施に関する報告書（SSSCIP 2023）。

[59]脅威の調査結果に基づく *SSSCIP* の分析レポート（SSSCIP 2023）。
<https://cip.gov.ua/services/cm/api/attachment/download?id=60201>。

[60]サイバーインシデント及びサイバー攻撃に対する脆弱性検知・対応体制に関する報告書
<https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf>.

[61]国家サイバーセキュリティの主な対象者の活動に関する独立監査の結果に関する年次報告書の提出とさらなる評価に関する報告書（デジタルトランスフォーメーションに関する委員会）
<www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_01.pdf>。

[62]ウクライナ法「ウクライナにおけるサイバーセキュリティ確保の基本原則について」の実施監視に関する予備報告書（デジタルトランスフォーメーション委員会）
<www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_02.pdf>.

ならない欧州連合の法律の規範に関する分析報告書」、「サイバーセキュリティ管理のベストプラクティス」などがある[63]

サイバー空間におけるサイバー攻撃や脅威に関する分析・統計データの公表は、政府の対応チームである CERT-UA と NSDC の National Cybersecurity Coordination Centre が行っている。[64]

[63]サイバーセキュリティ管理のベストプラクティス（デジタルトランスフォーメーション委員会）<www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_04.pdf>.

[64] "National Cybersecurity Centre" (国家サイバーセキュリティセンター) <www.ncscc.gov.ua/> accessed on 06.06.2024.

# 2. 国家サイバーセキュリティ戦略と法的枠組み

## 2.1 国家サイバーセキュリティ戦略文書

ウクライナの最初のサイバーセキュリティ戦略は、2016 年 3 月 15 日のウクライナ大統領令第 96 号によって承認された。その実施期間中、国家サイバーセキュリティシステムの確立と発展に努めた。その制度化の重要な段階は、ウクライナ法「ウクライナのサイバーセキュリティ確保の基本原則について」の採択であった。この法律は、人間と市民、社会と国家の重要な利益、サイバー空間におけるウクライナの国益を保護するための法的・組織的基盤、サイバーセキュリティ分野における国家政策の主な目標、方向性、原則、この分野における国家機関、企業、機関、組織、個人、市民の権限、サイバーセキュリティを確保するための活動の調整の主な原則を定義している。

重要情報インフラ対象物のサイバー保護に対する規制支援が改善され、その定義の手順とサイバー保護の一般要件が採用された。

ウクライナ国家特殊通信・情報保護局、ウクライナ安全保障局（SSU）、ウクライナ国立銀行、ウクライナインフラストラクチャー省、ウクライナ国防省、ウクライナ国軍には、サイバーセキュリティやサイバー保護を確保するためのセンター（ユニット）が設置されている。

NTN が整備され、国家情報資源保護センターが設立され、脆弱性を検出してサイ バー事件やサイバー攻撃に対応するシステムが機能し、ウクライナのコンピュータ緊急 事態に対する政府対応チーム CERT-UA が運用されている。サイバーセキュリティを提供する安全保障・防衛部門の各主体の活動の調整を改善するため、NSDC の作業組織である国家サイバーセキュリティ調整センター（NCSCC）が設立され、そのソリューションはこの分野における最も複雑な問題の解決に貢献している。

海外のパートナーとのサイバーセキュリティ分野での協力は積極的に発展しており（アメリカ合衆国、グレートブリテン及び北アイルランド連合王国、ドイツ連邦共和国、オランダ王国、日本など）、EU や NATO との協力も深まっており、他の国や国際機関の参加を得てサイバー訓練が実施されている。

毎年恒例のサイバーセキュリティ月間イベントが始まった。

2021 年 5 月 14 日付ウクライナ大統領令第 447/2021 号「ウクライナのサイバーセキュリティ戦略に関するウクライナ国家安全保障・防衛評議会の決定について」 安全なサイバー空間は国の成功発展の鍵であるとして、ウクライナの新たなサイバーセキュリティ戦略が採択された。[65] .

[65]2021 年 5 月 14 日付ウクライナ 国家安全保障・防衛評議会決定「ウクライナのサイバーセキュリティ戦略について」: 2021 年 8 月 26 日付ウクライナ大統領令 第 447/2021 号 <https://zakon.rada.gov.ua/laws/show/447/2021#Text> 2024 年 6 月 6 日閲覧。

ウクライナは、国家サイバーセキュリティ・システムの主要な主体に加えて、企業体、公的団体、ウクライナ市民個人など、より広範な参加者をサイバーセキュリティ分野の課題解決に関与させている。国家サイバーセキュリティ調整センターは、このプロセスにおいて重要な統一・調整の役割を果たす。

サイバーセキュリティ事業体の相互作用は、ウクライナの法律「サイバーセキュリティの基本原則について」([66])によって規制されている。

サイバーセキュリティを確保するための対策を、自らの権限の範囲内で直接実施する科目は以下の通りである：

1) 省庁をはじめとする行政の中枢機関である；

2) 地方と州の行政である；

3) 地方自治団体である；

4) 法執行機関、情報機関、防諜機関、作戦・捜査活動の対象；

5) ウクライナ国軍および法律によって編成されたその他の軍事組織；

6) ウクライナ国立銀行

7) 重要インフラの対象として分類される企業、機関、組織である；

8) 事業体、ウクライナ市民およびその団体、その他、国の情報資源、電子情報サービス、電子取引の実行、電子通信、情報保護、サイバー保護に関連する活動および／またはサービスを提供する者。

国家サイバーセキュリティ・システムの主体は、SSSCIP、ウクライナ国家警察、SSU、ウクライナ国防省とウクライナ軍参謀本部、情報機関、ウクライナ国立銀行であり、これらを通じてウクライナの憲法と法律が定める方法で以下の主な任務を遂行する：

1) SSSCIP は、サイバースペースにおける国家情報資源と情報の保護に関する国家政策の形成と実施、法律に明記された保護の要件、サイバースペースにおける侵略に対する積極的な対策、重要な情報インフラ対象物のサイバー保護、これらの分野における国家管理の実施、サイバー保護に関する他のサイバーセキュリティ機関の活動の調整、全国電気通信ネットワークの構築と機能、OTM の実施を保証する；

サイバーインシデントやサイバー攻撃を予防、検知、対応し、その影響を排除するための組織的・技術的対策を実施する；

[66] ウクライナのサイバーセキュリティ確保の主要原則について：2017 年 10 月 5 日付ウクライナ法第 2163-VIII 号：2024 年 4 月 4 日現在<https://zakon.rada.gov.ua/laws/show/2163-19#Text> 2024.06.06 にアクセス。

重要インフラ施設における情報セキュリティ監査の実施を確保し、情報セキュリティ監査人の要件を定め、その認証（再認証）の手順を決定し、重要インフラ施設の通信・技術システムの脆弱性監査を調整、組織、実施し、サイバー保護国家センター、サイバー空間における攻撃への積極的対抗センター、ウクライナのコンピュータ緊急事態に対する政府対応チーム CERT-UA の機能を確保する。

2) ウクライナ国家警察は、サイバー空間における違法な侵害から、人権と市民の権利と自由、社会と国家の利益を確実に保護し、サイバー犯罪を防止、検出、阻止、解決するための措置を実施し、市民のサイバーセキュリティに対する意識を高めている。

3) SSU は、サイバースペースで行われる人類の平和と安全に反する犯罪の予防、発見、終結、公表を行い、サイバーテロやサイバースパイと闘うことを目的とした防諜・作戦調査対策を実施し、想定されるサイバー攻撃やサイバー事件に対する重要インフラ施設の準備態勢を秘密裏にチェックする；国家の重要な利益を脅かすサイバー犯罪に対抗し、国家の電子情報資源、法律で保護が義務付けられている情報、重要情報インフラに関するサイバー事件やサイバー攻撃を調査し、国家の安全保障分野におけるサイバー事件に対応する。

4) ウクライナ国防省およびウクライナ国軍参謀本部は、その権限により、サイバー空間における軍事的侵略を撃退するための国家準備措置（サイバー防衛）を実施し、サイバー空間の安全保障とサイバー脅威に対する共同防護を確保するために、NATO およびその他の国防圏の主体との軍事協力を実施し、非常事態および戒厳令下で重要な情報インフラの適切なサイバー保護を確保するための措置を実施する。

5) ウクライナの諜報機関は、サイバー空間におけるウクライナの国家安全保障に対する脅威や、サイバーセキュリティ分野に関連するその他の出来事や状況に関する諜報活動を行っている。

6) ウクライナ国立銀行は、銀行、金融サービス市場で活動するその他の者、国家規制およびウクライナ国立銀行によって活動が実施される者の監督、決済システムの運営者および／または決済システムの参加者、決済サービスの技術的運営者によるサイバー保護および情報セキュリティを確保するための手順、要件、対策を決定し、その実施を監督し、ウクライナ国立銀行内にサイバー保護センターを設置し、銀行のサイバー保護システムの機能を確保する；また、銀行、金融サービス市場で活動するその他の者、ウクライナ国立銀行、決済システムの運営者および／または決済システムの参加者、決済サービスの技術的運営者が実施する国家規制および監督における重要インフラ施設のサイバー保護状態の評価および情報セキュリティの監査を提供する。

1. ウクライナの国家安全保障の構成要素としてのサイバーセキュリティ分野における活動の調整は、ウクライナ大統領が NSDC を通じて行っている。

2. 国家サイバーセキュリティ調整センター（National Cybersecurity Coordination Centre）は、NSDC の実務機関として、サイバーセキュリティを確保する安全保障・防衛部門の活動を調整・管理し、ウクライナのサイバーセキュリティ戦略の形成と明確化に関してウクライナ大統領に提案する。

3. CMU は、サイバーセキュリティ、人権および市民の権利と自由の保護、サイバー空間におけるウクライナの国益、サイバー犯罪との闘いの分野における国家政策の形成と実施を保証する。さらに、国家サ

イバーセキュリティシステムを機能させるために必要な力、手段、資源を組織し、提供し、重要インフラ施設（ウクライナの銀行システムにおける重要インフラ施設を除く）における情報セキュリティ監査システムの要件を策定し、その機能を保証する。

ウクライナのサイバーセキュリティ・システムの開発は、OTM に基づいて行われている。[67]OTM は、国家特殊通信局の専門家によって、現行法の規範と規定を適用する 5 年間の実践、国家サイバーセキュリティ・システム構築の経験、他国のサイバーセキュリティ・モデルの長所と短所の分析、この分野での作業編成の実践、サイバーセキュリティの他のテーマとの相互作用に基づいて開発された。OTM は、サイバー攻撃やその他のサイバーインシデントへの迅速な（危機的）対応、および通信システムの脆弱性を最小限に抑えることを目的とした対策の実施を目的とした、サイバー保護のための措置、力、手段のセットである。

OTM に関する規則は、モデル自体、その使命、構成と構造、機能メカニズム、目標を定義している。今回初めて、サイバー保護の力と手段、コンピュータ緊急事態への対応チーム、サイバー衛生の定義が定義された。OTM はマルチレベルのアーキテクチャを想定しており、3 つのインフラからなる構造化されたシステムである。

上位レベル - 組織・管理インフラ - サイバーセキュリティ分野の国家政策を形成および／または実施するサイバーセキュリティ主体の集合、中位レベル - 技術インフラ - サイバー保護の力・手段とその提供の集合、基本レベル - 基本インフラ - 重要情報インフラ対象物およびその重要資産、経済主体、ウクライナ国民およびその各種団体、その他活動および／または関連サービスを提供する者の集合である。

OTM に関する規則は、サイバー攻撃やサイバーインシデントへの迅速な（危機）対応、対策の実施、通信システムの脆弱性の最小化を目的として、その実施を明記している。

OTM に関する規則は、一つの考え方によって統一された、首尾一貫した、矛盾のない、構造化されたシステムの概要、その中での国のサイバーセキュリティシステムの各主体の位置づけ、他の主体とのつながりの性質、モデルの一つまたは他のレベルの様々な主体間の相互作用の形態、情報交換の方向性、サイバーインシデント管理の主な段階、予防、検知、識別の基本的なメカニズム、サイバーインシデントやサイバー攻撃への対応とそこからの回復について述べている。OTM に関する規則は、サイバーセキュリティのエコシステムを明確に定式化した。このエコシステムでは、すべての参加者が互いに密接に関係し、互いの活動を補完し合っている。

OTM は、サイバー保護の組織的、管理的、技術的、基本的なインフラから構成され、国家サイバーセキュリティシステムの機能を確保するために実施される。

サイバー防衛の組織・管理基盤は、以下の部門から構成される：

部門別には、中央行政機関、1 つまたは複数の分野における国家政策の形成および／または実施を確保し、またはその権限によってサイバーセキュリティを確保するための措置を直接実施するその他の国家機

[67]サイバー保護の組織的・技術的モデルに関する 規則の承認について：ウクライナ閣僚会議決議（12/29/2021）No.1426 <https://zakon.rada.gov.ua/laws/show/1426-2021-п#Text> 2024 年 6 月 6 日アクセス。

関、および所有形態に関係なく重要インフラの対象が含まれる；地域（地方）：情報保護およびサイバー保護の分野の活動に従事する地方行政機関、地方自治機関、企業、機関および組織を含み、所有形態は問わない；

これには、研究機関、情報保護とサイバーセキュリティ分野の高等教育機関、および専門人材の訓練、アップグレード、再教育に携わる教育・科学機関が含まれる；

民間には、非国有企業、情報保護やサイバー保護に従事する組織や機関（重要インフラ施設を除く）が含まれる。公共には、公的組織、組合、協会、サイバーセキュリティ分野の専門家、サイバーセキュリティ分野で活動を行う国際機関や政府間機関が含まれる。

サイバー防衛の基本インフラは、サイバー空間における個人と市民、社会と国家の重要な利益、そして国益の保護を確保するために機能する。

国家のサイバーセキュリティシステムの有効性を向上させることは、現在、サイバースペースにおける国家の重要な情報インフラの安定的で安全な機能を確保するための主要な課題であり、OTM はその解決策として実施されている。その規範的定義は、国家の重要な情報インフラのサイバー回復力のレベルを向上させるという課題を解決するために、サイバーセキュリティ事業体の努力を統一するための条件を作り出すことである。この重要な情報インフラには、重要なインフラ対象物、通信、情報、その他のシステムの両方が含まれ、その機能の安定性と信頼性は、国家機関、企業、あらゆる所有形態の機関や組織、市民団体の機能にとって決定的に重要である。[68]

同戦略の実施は、2021 年 12 月 30 日付のウクライナ国家安全保障・防衛会議の決定「ウクライナのサイバーセキュリティ戦略の実施計画について」によって実施され、2022 年 2 月 1 日付のウクライナ大統領令第 37 号によって発効し、2022 年 2 月 23 日の CMU 会議で承認された（議定書第 17 号）。[69]この文書により、国家特殊通信管理局は、ウクライナのサイバーセキュリティ戦略の実施計画の実施に必要な法律の草案を作成し、政府に提出すること、および 6 カ月ごとに CMU と NSDC 機関にウクライナのサイバーセキュリティ戦略の実施計画の実施状況に関する情報を提供することを任務としている。

ウクライナのサイバーセキュリティ戦略の実施計画の一環として、94 のタスクのうち 90 が積極的に実施されており、そのうち 2023 年上半期の「非常に限定的な進捗」の段階は 5%（2022 年より 5%少ない）、「初期的な進捗」の段階は 13%（2022 年より 2%少ない）、「進捗の加速」の段階は 36%（2022 年より 2%少ない）、「計画された結果の段階的な達成」の段階は 42%（2022 年より 12%多い）であった。2023 年通年では、全般的に、戦略の課題の実施率は 17%増加した。

---

[68]2021 年 12 月 29 日付ウクライナ閣僚会議決議第 1426 号で承認されたサイバー保護の組織的・技術的モデルに関する規定の科学的・実践的解説」（*https://cip.go*v.ua、2022 年 2 月 11 日）<https://cip.gov.ua/ua/news/naukovo-praktichnii-komentar-do-polozhennya-pro-organizaciino tekhnichnu-model-kiberzakhistu-zatverdzhenogo-postanovoyu-kabinetu-ministriv-ukrayini-vid-29-grudnya-2021-r-1426> 2024 年 6 月 6 日にアクセス。

[69]2021 年 12 月 30 日付ウクライナ国家安全保障・防衛評議会決定「ウクライナのサイバーセキュリティ戦略の実施計画について」について 2022 年 2 月 1 日付ウクライナ大統領令第 37/2022 号 <https://zakon.rada.gov.ua/laws/show/37/2022#Text>

## 2.2 国家サイバーセキュリティ戦略

ウクライナのサイバーセキュリティ確保の優先順位と戦略目標ウクライナのサイバーセキュリティ確保の優先順位は以下の通りである：

国家主権の保護と社会の発展のためにサイバースペースを確保する；

サイバースペースにおけるウクライナ国民の権利、自由、正当な利益を保護する、

サイバーセキュリティ分野における欧州と大西洋の統合。

国家サイバーセキュリティシステムの新たな質を形成するには、この戦略の実施期間中に達成すべき戦略目標を明確かつ分かりやすく定義する必要がある。**抑止力（C）**の形成のためには、以下の戦略目標を達成する必要がある：

**目標 C.1.**：効果的なサイバー防衛 - ウクライナは、サイバー空間における武力紛争を遂行する権限を持つ部隊を創設し、その開発（人員と技術を含む）を確保し、その機能と適用に関する適切な法的、組織的、技術的モデルを形成する。サイバー防衛活動中、国家サイバーセキュリティシステムの主要な主体と防衛部隊の効果的な相互作用、適切な訓練、そうした組織への財政的支援を確保する。組織的なサイバー訓練、部隊の能力と効果の評価、部隊の活動を評価する指標の開発と実施を行う。

**目標 C.2.**：サイバースペースにおける諜報活動や破壊活動、サイバーテロに効果的に対抗する - ウクライナは、国家、社会、個々の市民の利益を確保するために、外国の諜報活動や破壊活動、サイバースパイ行為、サイバーテロを検知、防止、阻止し、その要因となる状況を排除するための諜報対策を継続的に実施する。

**目標 C.3.**：サイバー犯罪に対する効果的な対策 - ウクライナは、法執行機関及び法執行機能を有する特別国家機関が、サイバー犯罪の脅威を最小化する能力を獲得し、予防措置を実施し、サイバー犯罪を捜査するための技術的及び人的資源を強化することを確保する。

**目標 C.4.**：非対称的抑止手段の開発 - ウクライナは、経済、外交、諜報の各手段を駆使するとともに、民間セクターの潜在力を活用することにより、ウクライナに対するサイバー空間での攻撃的行為の抑止を確保するために必要な条件を整備する。

**サイバー・レジリエンス（K）**を獲得するためには、以下の戦略目標を達成する必要がある：

**目標 K.1.**：ウクライナは、経済的安寧を確保し、ウクライナ国民一人ひとりの権利と自由を守るという利益のために、すべての利害関係者のために、国家的サイバー即応態勢のための明確で理解しやすい措置を導入し、実施する。ウクライナはサイバー即応態勢を強化する。サイバー即応態勢とは、すべての利害関係者（主に安全保障・防衛分野の主体）がサイバー攻撃にタイムリーかつ効果的に対応し、現実のサイバー脅威および潜在的なサイバー脅威に対する常時準備態勢を確保し、その発生の前提条件を特定・排除する能

力であり、これにより、主に重要情報インフラの対象であるサイバー耐性を確保する。この目的のため、ウクライナは国家インシデント管理システムを構築する。

**目標 K.2.**：ウクライナは、サイバーセキュリティ分野の専門家の訓練と高度な訓練のシステムの抜本的な改革を実施するとともに、サイバーセキュリティ分野の既存の有資格者の潜在能力を維持するための措置を実施する。国内の科学的・技術的潜在力は、主に国家のサイバーセキュリティを確保する課題の解決に関与する。デジタルスキル、現代のサイバー脅威とその対策に関するサイバー意識は、ウクライナ国民一人ひとりの教育に不可欠な要素となる。

**目標 K.3.**：安全なデジタルサービス - ウクライナは、社会、国内市場、国家経済のニーズと、必要なサイバーセキュリティ対策との間のバランスの達成、およびデジタルサービスのライフサイクル全体を通じての信頼性と安全性の確保を確実にする。

**相互作用（B）**を改善するためには、以下の戦略目標を達成する必要がある：

**目標 B.1.**：調整システムの強化 - ウクライナは、国家サイバーセキュリティシステムを構築し機能させる過程において、サイ バーセキュリティ主体が効果的に相互作用するための条件を整備するとともに、サイバー攻撃やサイ バーインシデントの結果を防止、撃退、無力化する際の効果的な共同行動のための条件を整備し、サイ バー空間における緊急事態（危機的状況）を克服するために、すべての関係者の活動を調整する。

**目標 B.2.**：サイバーセキュリティ分野における新たな関係モデルの形成 - ウクライナは、サイバー保護対策に国家が参加するサービスモデルを導入する。このモデルでは、国家は要求の供給源としてではなく、国家サイバーセキュリティシステム開発のパートナーとして認識される。

**目標 B.3.**：実際的な国際協力 - ウクライナは、国際パートナーとの関係を、サイバー攻撃への共同対応やサイバーセキュリティにおける危機の克服のための相互信頼の醸成だけでなく、サイバー攻撃やサイバー事件に関する情報交換、共同サイバー作戦、国際的なサイバー犯罪の捜査、定期的な e ラーニングや訓練、経験やベストプラクティスの交換など、純粋に実際的な協力にも向ける。ウクライナは、サイバースペースにおける行動規範の共同策定や関連規制・法的枠組みの改善に関する国際機関の枠組み内での対話に積極的に参加する。国際的なパートナーとの調整は、ウクライナ外務省が行う。

## 2.3 サイバーセキュリティ法

ウクライナにおけるサイバーセキュリティ確保の法的基盤は、ウクライナ憲法、国家安全保障の基礎に関するウクライナ法、内政・外交政策の原則、電子通信、国家情報資源・情報の保護に関する法律に組み込まれており、これらの保護要件は法律によって定められている。この法律およびウクライナのその他の法律、サイバー犯罪に関する条約、ウクライナのヴェルホヴナ・ラダが拘束力のある同意を与えたその他の国際条約、ウクライナ大統領による政令、CMU の法律、およびウクライナの法律を実施するために採択されたその他の規範的法律行為である。

この分野の基本法は、ウクライナ法「情報について」[70]、ウクライナ法「国家機密について」[71]、ウクライナ法「ウクライナのサイバーセキュリティ確保の基本原則について」である。同法は、サイバー空間における個人と市民、社会と国家、ウクライナの国益の保護を確保するための法的・組織的基盤のほか、サイバーセキュリティ分野における国家政策の主な目標、方向性、原則、この分野における国家機関、企業、機関、組織、個人、市民の権限、サイバーセキュリティを確保するための活動を調整するための主な原則を定めている。

この法律は、サイバーセキュリティとサイバー保護の対象、サイバーセキュリティの対象を定義し、重要インフラ対象のサイバーセキュリティの基礎となる原則、サイバーセキュリティの原則、国家サイバーセキュリティシステム、ウクライナ CERT-UA のコンピュータ緊急事態に対応する政府チームの任務について説明している。また、サイバーセキュリティ分野における官民協力や、ウクライナでサイバーセキュリティを提供する事業体への支援提供の基盤も築かれた。この法律は、サイバーセキュリティ分野の法律違反に対する責任を規定し、サイバーセキュリティ対策への財政支援、サイバーセキュリティ分野での国際協力、ウクライナのサイバーセキュリティを確保するための対策の合法性に対する管理などの問題を考慮している。

情報およびサイバーセキュリティを確保するための要件は、ウクライナの「情報通信システムにおける情報の保護に関する法律」によって定められている。この法律は、情報および電子通信システムの保護分野における関係を規定している。この法律は、システムにおける保護の重要な対象、関係の主体、システムにおける情報へのアクセスの問題、情報の所有者とシステムの所有者との関係、システムの所有者とユーザーとの関係、システムの所有者間の関係、システムにおける情報の条件、システムにおける情報保護の確保プロセス、およびそのようなシステムにおける情報保護の分野における国家機関の権限を定義している。さらに、システムにおける情報保護に関する法律違反の責任と国際協力についても規定されている。

この法律により、国の情報資源または法律で保護要件が定められたアクセス制限のある情報は、包括的な情報保護システムを使用したシステムで処理され、適合性が確認されなければならない。包括的な情報保護システムの適合性の確認は、国家審査の結果に基づいて行われ、その審査は、業界の要求事項および情報セキュリティ規範を考慮し、法律で定められた方法で行われる。

情報の技術的および暗号的保護手段の遵守の確認および国家審査は、法律で定めら れた手続きによって実施される。国家情報資源またはアクセスが制限された情報を保護するための複雑なシステムを構築し、その保護要件が法律で定められている場合、情報の暗号化保護（情報の暗号化保護分野における国家専門家の結果に基づく肯定的な専門家の意見を有する）が実施される。ウクライナの国家認定機関および他国の国家認定機関の両方が国際認定機関または地域認定機関のメンバーであり、かつ／または適合性評価に関して当該機関と相互承認協定を締結している場合、ウクライナの国家認定機関または他国の国家認定機関によっ

[70] 情報について 1992 年 10 月 2 日付ウクライナ法第 2657-XII 号：2023 年 7 月 27 日現在 <https://zakon.rada.gov.ua/laws/show/2657-12#Text> 2024 年 6 月 6 日アクセス。

[71]国家機密について 1994 年 1 月 21 日付ウクライナ法第 3855-XII 号：2024 年 1 月 1 日現在 <https://zakon.rada.gov.ua/laws/show/3855-12#Text>

て認定された適合性評価機関が発行した適合証明書、または技術的情報保護分野における国家検査の結果に基づく肯定的な専門家の意見を有する情報保護の技術的手段を提供する。

国家情報資源およびアクセス制限のある情報は、国家機密、公的情報、国家登録簿および統一登録簿など、その作成および運用が法律で定められているものを除き、以下の条件をすべて満たせば、包括的情報保護システムを使用せずにシステムで処理することができる：

適合性評価機関、ウクライナの認定国家認定機関、または他国の国家認定機関（ウクライナの国家認定機関でもある場合）が実施した、情報セキュリティマネジメントシステムに関するウクライナの国家基準への適合性評価手順の結果に基づく、情報セキュリティマネジメントシステムの適合性の確認；

暗号情報保護分野における国家専門家の結果に基づく肯定的な専門家の意見を持つ暗号情報保護手段によって、システム内の情報保護に使用する；

ウクライナの国家当局が一時的に権限を行使していないウクライナの領土、ウクライナ評議会の最高決議により侵略国として承認された国家の領土、ウクライナの「制裁に関する」法律により制裁が適用された国家の領土、およびそのような国家と関税同盟を結んでいる国家の領土において、システムのいずれの要素も所在を特定できず、そのようなシステムの所有者またはその正式な代表者が、ウクライナの領土で登記された法人（その代表者）であることはできない；

システムの所有者またはその代理人であって、システムの構成要素がウクライナ国外に所在し、システムを使用してサービスを提供する者は、ウクライナで登記された法人であるか、ウクライナに正式な代理人がいなければならない。国家の情報資源またはアクセスが制限された情報のカテゴリーに応じて、システム内の情報の保護を確保するために CMU が定めた特別な要件を満たすこと。

システム所有者は、システムが適切に機能し、そこで処理される情報が以下の方法で保護されることを保証しなければならない：

州の情報資源およびシステムのバックアップ・コピーを作成し、その保護、完全性、および機密性に関する要件に準拠する；

ウクライナの戒厳令の有効期間中、およびその終了または解除から 6 カ月後、ウクライナ国外（特にウクライナの外国外交機関）を含め、法律で定められた手続きにより、国家情報資源およびシステムのバックアップコピーを暗号化された形で個々の物理メディアに作成し、その後、保管のために転送（移動）することを確保する；

ウクライナにおける戒厳令の法体系の期間中、および戒厳令の終了または廃止から 6 カ月後に、ウクライナ国外にあるクラウドリソースおよび／またはデータ処理センターに配置するための国家情報資源およびそのバックアップコピーの移転（移動）を確保すること。

国家機関のインターネットへのアクセスは、安全なインターネット・アクセス・ノードを使用して実施されなければならない。一方、国家機関は、国家機関のインターネットへの安全なアクセスを確保するためのサービスをシステムに提供する。[72]

行政機関におけるコンピュータ・プログラムの使用は、2003 年 9 月 10 日付の CMU 決議第 1433 号によって規制されている。[73]

電子文書管理システムのサイバー保護レベルを向上させるための方法論的勧告が策定された。[74]

ウクライナの国家当局が一時的に権限を行使していないウクライナの領土、ウクライナのヴェルホヴナ・ラーダによって侵略国家と認定された国家の領土、制裁に関するウクライナ法によって制裁が適用されている国家の領土、およびそのような国家と関税同盟や軍事同盟を結んでいる国家の領土に、国家情報資源やシステムのシステムを設置したり、バックアップコピーを保管したりすることは禁止されている。

2021 年 5 月 14 日付のウクライナ国家安全保障・防衛会議の決定「ウクライナのサイバーセキュリティ戦略について」に基づくウクライナ大統領令第 447 号/2021 号によると、サイバー空間における緊急事態（危機）に対する国家対応計画が規定されている。また、2022 年 2 月 1 日付のウクライナ大統領令「2021 年 12 月 30 日付のウクライナ国家安全保障・防衛会議の決定について」および「ウクライナのサイバーセキュリティ戦略の実施計画について」[75]、サイバー空間における緊急事態（危機的状況）に対応するための国家計画の策定が 2023 年後半に予定されている。

ウクライナ国防省とウクライナ国軍参謀本部は、「ウクライナのサイバーセキュリティを確保するための基本原則に関する」ウクライナ法により、その権限において、サイバー空間における軍事的侵略を撃退するための国家準備措置（サイバー防衛）を実施している。

同時に、ウクライナの法律「ウクライナの特殊通信および情報保護に関する国家サービス」[76]、サイバースペースにおける侵略に対する積極的な対抗措置のシステムを構築し、その機能を確保すること、およ

---

[72] 国家機関のインターネットへのアクセス保護システムに関する規則の承認について：2023 年 8 月 30 日付ウクライナ特別通信・情報保護国家庁命令第 771 号 <>2023 年 8 月 30 日付第 771 号<https://zakon.rada.gov.ua/laws/show/z1624-23#Text>（2024 年 6 月 6 日付アクセス）。

[73] 行政当局におけるコンピュータ・プログラムの使用手続き」の承認について：2003 年 9 月 10 日付ウクライナ閣僚会議決議第 1433 号：2024 年 4 月 12 日現在 <https://zakon.rada.gov.ua/laws/show/1433-2003-п#Text> 2024 年 6 月 6 日アクセス。

[74] 電子文書管理システムのサイバー保護レベル向上のための方法論的勧告」の承認について：2023 年 8 月 30 日付ウクライナ行政長官命令第 773 号。<https://zakon.rada.gov.ua/rada/show/v0773519-23#Text>は 2024 年 6 月 6 日にアクセスされた。

[75]2021 年 12 月 30 日付のウクライナ 国家安全保障・防衛評議会の決定「ウクライナのサイバーセキュリティ戦略の実施計画について」による：2022 年 2 月 1 日付ウクライナ大統領令。No. /2022<https://zakon.rada.gov.ua/laws/show/37/2022#Text> accessed on 06.06.2024.

[76] ウクライナの特別通信と情報保護のための国家サービスに関する：2006 年 2 月 23 日付ウクライナ法第 3475-IV 号：2023 年 12 月 31 日現在 <https://zakon.rada.gov.ua/laws/show/3475-15#Text>

びサイバースペースにおける侵略に対する積極的な対抗措置のためのセンターを構築し、その機能を確保することが想定されている。

ウクライナでは、「ウクライナ軍のサイバー部隊に関する」法律も制定されつつある。

2003 年 1 月 28 日付で、欧州評議会の「サイバー犯罪に関する条約」と、コンピューターシステムを通じて行われる人種差別的・排外主義的行為の犯罪化に関する「サイバー犯罪に関する条約の追加議定書」がウクライナで批准された。

サイバー犯罪という用語は、ウクライナの法律「ウクライナのサイバーセキュリティ確保の基本原則について」で定義されている。サイバー犯罪とは、電子計算機（コンピュータ）、自動化されたシステム、コンピュータネットワークまたは電気通信ネットワークの助けを借りてサイバースペースで行われる、社会的に危険な犯罪行為であり、その刑事責任は法律によって規定されている。

- ウクライナ刑法は、サイバー空間における犯罪の刑事責任を規定している。同法は、以下の種類の犯罪を規定している：

- 情報（自動化）、電子通信、ICS、電子通信ネットワークの運営を無許可で妨害する（ウクライナ刑法第 361 条）；

- 悪意のあるソフトウェアやその普及のための技術的手段の違法な使用、配布、販売、およびそれらの配布や販売のための創作（ウクライナ刑法第 361 条）；

- 電子計算機（コンピュータ）、自動化システム、コンピュータネットワーク、またはそのような情報のキャリアに保存されている、アクセスが制限された情報の無許可販売または配布（ウクライナ刑法第 361 条）；

- 電子計算機（コンピュータ）、自動化システム、コンピュータネットワークで処理された情報、またはそのような情報の媒体に保存された情報に対する無許可の行為で、その情報にアクセスする権利を有する者が行ったもの（ウクライナ刑法第 362 条）；

- 電子計算機（コンピュータ）、自動化システム、コンピュータネットワーク、電気通信ネットワークの運用に関する規則、またはそれらで処理される情報の保護に関する命令や規則に違反すること（ウクライナ刑法第 363 条）；

- 電子計算機（コンピュータ）、自動化システム、コンピュータネットワーク、または電気通信メッセージの大量配信のために設計された電気通信ネットワークの運営を妨害する（ウクライナ刑法第 363 条）。

さらに、サイバー犯罪者の活動は、ウクライナ刑法第 200 条「送金文書、支払いカード、銀行口座へのアクセス手段、電子マネー、それらの製造装置による違法行為」、ウクライナ刑法第 3 編 190 条「電子計算機を使用した違法な操作による詐欺」、同第 231 条「商業秘密または銀行秘密を構成する情報の使用

または利用のための違法な収集」に該当する。ウクライナ刑法第 231 条「商業上または銀行上の秘密を構成する情報を使用または利用するための違法な収集」に関するものである。

カーディング（Carding）- カード所有者が承認していないクレジットカード（クレジットカードの詳細）を使った不正取引。これは、クレジットカードの盗難や不正取得、さらなる偽造のためのカード・データのコピー、カード所有者の参加なしにインターネット上で買い物をするためのカード詳細のコピーなどである。いずれにせよ、犯罪者の主な目的は他人の金銭にアクセスすることである。この目的を達成するために、犯罪者は不注意で騙されやすい市民から必要な情報を得る様々な方法を編み出す。そのような方法の一つがフィッシングである。

フィッシング - カードの所有者からカード情報をおびき出すことを目的とした詐欺行為。通常、クレジットカードの所有者自身が自発的に必要な情報を詐欺師に知らせる。

フィッシングにはいくつかの種類がある：

- SMS フィッシングとは、潜在的な詐欺被害者が、クレジットカードが銀行によってブロックされ、そのロックを解除するために詳細を提供する必要があるというメッセージや、カード所有者が懸賞に当選したが、その配送料を支払う必要があるというメッセージを受信することである。SMS メッセージには多くのオプションがあるので、このようなメッセージを受け取った場合は特に注意が必要だ。

- インターネット・フィッシングとは、詐欺師が銀行、決済サービス、オンラインショップなどの公式ページを模倣したフィッシング（偽）ページを作成することである。

ヴィッシングとはサイバー犯罪の一種で、メッセージの中に特定の都市番号に電話をかけるよう要求する内容が含まれており、会話の中でカード所有者の機密データが要求される。

スキミング - 特殊な装置（スキマー）を使ってペイメントカードのデータをコピーすること。通常、ATM でのカード取引中に発生する。データを入手するために、犯罪者はミニカメラや交換可能なキーボードを使用する。

POS スキミングは、現代化されたスキミングの一種である。この場合、詐欺師はカード・リーダーの内側に設置されたほとんど目に見えない装置を使用する。こうして、クレジットカードのデータが気づかれないようにコピーされる。

オンライン詐欺-偽のオンライン・オークション、オンライン・ストア、ウェブサイト、電気通信を含む。

海賊版-インターネット上で知的財産を違法に頒布すること。

マルウェア - ウイルスや悪意のあるソフトウェアの作成と配布。

違法なコンテンツ - 過激主義、テロリズム、薬物中毒、ポルノ、残酷さと暴力のカルトを促進するコンテンツ。

リファイリングは、電話トラフィックの違法な代用品である。

サイバー空間における犯罪に対抗するため、CMU の決議「国家警察の領域組織の設立について」[77]、サイバー警察局が設立された。

[77]国家警察の領域組織の形成について：2015 年 10 月 13 日付ウクライナ閣僚会議決議 No.831 <https://zakon.rada.gov.ua/laws/show/831-2015-п#Text> 06.06.2024 にアクセスした。

**重要インフラ**

重要インフラのサイバー保護の問題は、ウクライナ法「重要インフラについて」、[78] 2019 年 6 月 19 日付 CMU 決議「重要インフラ対象物のサイバー保護に関する一般要件の承認について」第 518 号[79] 、2020 年 10 月 9 日付 CMU 決議「重要インフラ施設のいくつかの問題」第 1109 号[80] 、2020 年 10 月 9 日付 CMU 決議「重要情報インフラ施設のいくつかの問題」第 943 号 、2023 年 8 月 4 日付 CMU 決議「重要インフラ対象物の認証のいくつかの問題」第 818 号 、SSSCIP 管理局命令第 23 号「方法論的対象物の認証の承認について」によって規制されている。943, 2023 年 8 月 4 日付 CMU 決議「重要インフラ対象物の認証に関する若干の問題」第 818 号[81] , SSSCIP 管理局命令第 23 号「重要インフラ対象物の分類に関する方法論的勧告の承認について」,[82] 国家特別通信管理局命令第 601 号「重要情報のサイバー保護レベルの向上に関する方法論的勧告の承認について」。

インフラストラクチャー（修正あり）、[83] SSSCIP 管理局命令第 463 号 方法論の承認について。

自動化されたプロセス管理システムのサイバー保護を確保するための勧告。 [84] 国家レベルの「サイバー攻撃／サイバーインシデント」のプロジェクト脅威に基づく重要インフラ対象物保護計画の策定に関する勧告と、それに対応する重要インフラ対象物保護計画の書式が策定された。重要インフラ対象物の法的地位の取得は、当該対象物に関する情報が重要インフラ国家登録簿に登録されたことを確認した後に行われる。[85]

**クラウドサービス**

---

[78] 重要インフラについて 2021 年 11 月 16 日付ウクライナ法第 1882-IX 号：2024 年 1 月 1 日現在 <https://zakon.rada.gov.ua/laws/show/1882-20#Text> accessed on 06.06.2024.

[79] 重要インフラ対象物のサイバー保護に関する一般要件の承認について：2019 年 6 月 19 日付ウクライナ閣僚会議決議第 518 号：9 月 7 日現在。2022. <https://zakon.rada.gov.ua/laws/show/518-2019-п#Text> accessed on 06.06.2024.

[80] 重要インフラ対象物の問題 2020 年 10 月 9 日付閣議決定第 1109 号：2024 年 1 月 20 日現在 <https://zakon.rada.gov.ua/laws/show/1109-2020-п#Text> 2024 年 6 月 6 日アクセス。

[81]重要インフラ対象物の認証に関する問題：<https://zakon.rada.gov.ua/laws/show/818-2023-п#Text>2024 年 6 月 6 日にアクセスされた。

[82] SSSCIP 管理局命令第 23 号「重要インフラ対象物の分類に関する方法論的勧告の承認について」 <https://zakon.rada.gov.ua/rada/show/v0023519-21#Text> 2024 年 6 月 6 日アクセス。

[83]SSSCIP 管理局命令第 601 号「重要情報インフラのサイバー保護レベル向上のための方法論勧告の承認について（変更あり）」。 <https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06601> accessed on 06.06.2024.

[84] SSSCIP 管理局命令第 463 号「技術プロセスを制御する自動化システムのサイバー保護確保のための方法論的勧告の承認について」<https://zakon.rada.gov.ua/rada/show/v0463519-23#Text> 2024.06.06 にアクセス。

[85] SSSCIP 管理局の命令 No.793 重要情報インフラのオブジェクトの国家登録簿に情報を提出するためのフォームの承認について <https://zakon.rada.gov.ua/rada/show/v0793519-23#Text> 2024.06.06 にアクセスした。

ウクライナにおけるクラウドサービスプロバイダーの活動は、ウクライナの「クラウドサービスに関する法律」によって規制されている。[86]同法は、クラウドサービスの提供において生じる法的関係を定義し、国家当局、クリミア自治共和国当局、地方自治団体、ウクライナの法律により編成された軍事組織、国営企業、権力主体による機関および組織、ならびにそのような権力が委譲されたその他の主体によるクラウドサービスの利用について具体的に定めている。

法第 8 条第 2 部によると、クラウドサービスやデータセンターサービスを公共ユーザーや重要インフラ施設に提供するためには、クラウドサービスやデータセンターサービスのプロバイダーに関する情報をリストに含めなければならない。

同法第 12 条第 1 項により、CMU は、相互運用性と競争維持の原則に基づき、国家情報資源または法律で保護要件が定められている限定的なアクセス権のある情報の処理に関連するクラウドサービスおよび／または情報処理センターサービスを提供する手順を定め、その順序を決定する：

バックアップとバックアップコピーの独立したシステムへの保存が義務付けられている；

クラウド・サービスのユーザーからクラウド・サービスのプロバイダーおよび／またはデータセンター・サービスへのデータ転送は、クラウド・サービスの提供を保証するためであり、クラウド・サービスのプロバイダーからクラウド・サービスのユーザーへのデータ転送でもある；

クラウドサービスおよび／またはデータセンターサービスのプロバイダーから別のプロバイダーへのデータ転送；

クラウドサービスおよび／またはデータセンターサービスのプロバイダーのネットワークおよび情報システムのセキュリティを評価するために必要な情報（文書化されたセキュリティポリシーを含む）を提供すること。

同法第 12 条第 2 部は、クラウドサービスおよび／またはデータセンターサービスの提供手続きに含まれなければならない条項の要件を定めている。このような命令には、以下が含まれるべきである：

- 構造化された形式、一般的に使用されている形式、機械が読み取り可能な形式でデータを伝送するための要件；

- クラウドサービス及び／又はデータセンターサービスの他のプロバイダーへの切り替え、又はクラウドサービスの拒否の場合に適用されるプロセス、技術的要件、条件及び支払いに関する情報の量に関する要件であって、調達手続（簡易調達手続）の勝者を決定するために、明確かつ利用しやすい形でクラウドサービスの利用者に提供されなければならないもの；

[86]クラウドサービスクラウドサービスについて：2022 年 2 月 17 日付ウクライナ法第 2075-IX 号：2024 年 4 月 4 日現在 <https://zakon.rada.gov.ua/laws/show/2075-20#Text> 2024 年 6 月 6 日アクセス。

- 特に、品質管理、情報セキュリティ管理、サービス継続性管理、環境影響評価に関する情報を含む。

ウクライナ法「クラウドサービスに関する法律」（2022 年 2 月 17 日付第 2075-IX 号）第 8 条は、クラウドサービスおよび／またはデータセンターサービスのプロバイダーに対し、いくつかの要件を満たすことを求めている。クラウドサービスおよび／またはデータセンターサービスの提供者は、電子通信ネットワーク、クラウドサービスを提供するために使用される電子通信サービスおよび情報システムのセキュリティに起因するリスクを管理するために、適切かつ相応の技術的・組織的措置を講じなければならない。

このような措置は、クラウドサービスを提供するために使用される電子通信ネットワーク、電子通信サービス、情報システムのセキュリティレベルを、発生したリスクに対応して確保するものでなければならず、次の要素を考慮しなければならない：システムと機器のセキュリティ、インシデントの解決、事業継続管理、監視、監査、テスト、国際基準への準拠。

クラウドサービスおよび／またはデータセンターサービスの提供者は、クラウドサービスおよび／または データセンターサービスの提供に重大な悪影響を及ぼすインシデントが発生した場合、不合理な遅滞な く、通信サービス規制当局および CERT-UA に、通信サービス規制当局が承認した方法で通知しなければならない。

クラウドサービスおよび/またはデータセンターサービスのプロバイダーは、以下を行わなければならない：

- サイバー保護分野における国家政策の形成と実施のために指定された国家機関に、文書化されたセキュリティ方針を含め、電子通信ネットワーク、電子通信サービス、情報システムのセキュリティを評価するために必要な情報を提供する；

- 通信サービス規制当局が承認した要件への不適合を排除する。

2022 年 3 月 12 日付 CMU 決議第 263 号「戒厳令下における ICS、電子通信システム、公的電子登録簿の機能確保に関する諸問題」は、戒厳令期間中、各省庁、その他の中央・地方行政機関、国営・自治体の企業、機関、およびその管理領域に属する組織は、情報、情報通信、電子通信システム、公的電子登録簿の所有者（保有者）および／または管理者として、その適切な機能を確保するとともに、その中で処理されるあらゆる情報の保護を確保しなければならないと規定している。そのために、以下の追加措置を講じることができる：

- ウクライナ国外にあるクラウドリソースおよび／またはデータ処理センターに国家情報資源および公的電子登記簿を配置し、その配置ごとに gov.ua ドメインのドメイン名を登録する；

- 国家情報資源および公的電子登録簿のバックアップ・コピーを追加作成し、そのような資源のために確立された完全性、機密性、可用性の要件に準拠する；

- 情報、情報通信、電子通信システム、公的電子登録の運用を停止し、制限する。

各省庁、その他の中央・地方行政機関、国営・公営企業、機関、およびその管理領域に属する組織は、ウクライナの州境外にあるクラウドリソースおよび／またはデータ処理センターを無償または有償で利用することができる。

各省庁およびその他の中央・地方行政機関は、戒厳令の終了または廃止後 6 ヶ月以内に、上記の措置の実施を停止し、SSSCIP 管理局およびデジタル変革省に上記の措置の終了を直ちに通知するよう指示される。

# 3. 国家サイバーセキュリティ・ガバナンス

## 3.1 戦略的リーダーシップと政策調整

戦略レベルでは、サイバーセキュリティ問題に関する調整は、2016 年 1 月 27 日付のウクライナ国家安全保障・防衛評議会の決定「ウクライナのサイバーセキュリティ戦略について」によって形成され、2016 年 3 月 15 日付のウクライナ大統領令第 96 号によって発効した NSDC の実務機関である NSDC の国家サイバーセキュリティ調整センターによって行われている。

NCSCC は、2016 年 6 月 7 日付ウクライナ大統領令 No.242/2016 によって承認された国家サイバーセキュリティ調整センターに関する規則によって機能している[87]NCCS はサイバーセキュリティの主要な対象のみを調整し、その決定はすべての国家機関による検討は必須だが実施は必須ではない。NCCS は、サイバーインシデント／サイバー攻撃への対応中にサイバーセキュリティ機関が相互作用するための手順を承認した。[88]

NCSCC は技術協定を通じて NATO CCDCOE と交流しているが、これには NATO 諸国や NATO CCDCOE に代表されるパートナー諸国との交流も含まれている。

## 3.2 サイバーセキュリティの権限とサイバーインシデントへの対応

SSSCIP は、国家通信システム、国家機密通信システムの機能と発展、暗号および技術情報保護、サイバー保護、特別目的郵便通信、政府現場サービス通信、サイバー空間における侵略への積極的対策、その他法律で義務付けられた任務の分野における国家政策の形成と実施を確保するために任命された国家機関である。

国家サイバーセキュリティシステムの構成要素としての OTM の実施は、国家機関のインターネット への保護されたアクセスシステムの主要な構成要素の構築と運用、国家情報資源のアンチウ イルス保護システム、情報セキュリティの監査、重要な情報対象インフラのサイバー保護状 態を保証するサイバー保護国家センターによって行われる；サイバー保護対象に関する脆弱性を検出し、サイバー事件やサイバー攻撃に対応するためのシステム、コンピュータ緊急事態に対応するチームの相互作用のためのシステム、サイバーセキュリティの他のテーマと協力して、サイバー脅威に対応するためのシナリオ、そのような脅威に対抗するための対策、サイバー訓練のプログラムや方法を開発する。

---

[87] 国家サイバーセキュリティ調整センターについて：2016 年 06 月 07 日付ウクライナ大統領令 No.242/2016：2021 年 7 月 17 日現在 <https://zakon.rada.gov.ua/laws/show/242/2016#Text> 2024 年 06 月 06 日アクセス。

[88] "National Security and Defence Council of Ukraine" (ウクライナ国家安全保障防衛評議会) <www.rnbo.gov.ua/ua/Diialnist/5765.html> accessed on 06.06.2024.

CERT-UA の任務は以下の通りである：

1) サイバーインシデントに関するデータの蓄積と分析、サイバーインシデントの国家登録の維持；

2) サイバー保護対象物の所有者に対して、これらの対象物に関連するサイバーインシデントの結果の予防、検出、排除に関する実務的な支援を提供する；

3) 国家サイバーセキュリティシステムの対象者およびサイバー保護対象物の所有者を対象に、サイバー保護問題に関する実践的なセミナーを開催する；

4) 最新のタイプのサイバー攻撃やサイバー脅威に対抗するための勧告を作成し、公式ウェブサイトに掲載する；

5) 法執行機関との交流により、サイバー攻撃に関する情報をタイムリーに提供する；

6) 特に、年会費を支払って FIRST Security Incident Response Teams Forum（FIRST セキュリティ・インシデント・レスポンス・チーム・フォーラム）に参加する枠組みの中で、サイバーインシデント対応の問題に関して海外や国際組織と交流する；

7) ウクライナのコンピュータ緊急対応チームや、所有形態に関係なく、サイバースペースの安全確保に関連する活動を行うその他の企業、機関、組織との交流を図る；

8) サイバー保護対象に関するサイバー事件に関して市民から寄せられた情報を処理する；

9) ウクライナの国家機関、地方自治団体、法律によって編成された軍事組織、所有形態に関係なく企業、機関、組織、そしてウクライナの市民が、サイバー保護とサイバー脅威への対抗の問題を解決するための支援を行う。

また、重要な国際交流として、コンピュータセキュリティインシデント対応チーム FIRST と信頼され た導入者のフォーラム（TF-CSIRT）への CERT-UA の参加がある。[89]

サイバーインシデントに関する情報交換は、NSDC の NCSCC 会合で承認された「サイバーインシデントに関する情報交換に関する通則（TLP プロトコル）」によって行われる。

サイバースペースにおける様々な種類の事象に対するサイバーセキュリティ機関の対応は、2023 年 4 月 4 日付 CMU 決議第 299 号「サイバースペースにおける様々な種類の事象に対するサイバーセキュリティ機関の対応に関するいくつかの問題」[90] 、2023 年 7 月 3 日付国家特別通信管理局命令第 570 号によっ

[89] "Trusted Introducer：Directory：CERT-UA" (*Trusted Introducer : Home*) <www.trusted introducer.org/directory/teams/cert-ua.html> accessed on 06.06.2024.

[90] サイバー空間における様々な種類の事象に対するサイバーセキュリティ事業体の対応に関するいくつかの問題点：ウクライナ閣僚会議決議（2023 年 4 月 4 日）第 299 号<https://zakon.rada.gov.ua/laws/show/299-2023-n#Text>（2024 年 6 月 6 日閲覧）。

て承認された関連する方法論的勧告を考慮して実施される[91]同時に、この問題は、CMU の決議「情報・電子通信システムにおける国家情報資源の保護に関する行政当局の相互作用のための手続きの承認について」([92] ）でも規定されている。

## 3.3 サイバー危機管理

サイバースペースにおける危機を管理するため、ウクライナの主要状況センター「SOTA」内の最新情報分析システムが開発され、ウクライナ NSDC の装置の一部として運用が開始された。[93]SSU のサイバーセキュリティ状況センターが設立され、NCSCC の決定の一つに、特にエネルギー分野におけるサイバーセキュリティ状況センターの建設が盛り込まれている。

現在、ウクライナ国家安全保障防衛会議（NSDC）の専門家は、関係省庁とともに、2021 年 6 月 18 日付ウクライナ大統領令第 260 号（[94] ）により発効した、2021 年 6 月 4 日付ウクライナ国家安全保障防衛会議の決定「状況センターネットワークの改善と国家安全保障・防衛分野のデジタル変革について」の実施に取り組んでいる。

## 3.4 軍事サイバー防衛

ウクライナ国軍の通信・サイバーセキュリティ部隊は、ウクライナ国軍の特殊部隊であり、戦闘統制・警戒システムに加え、通信・情報システムの機能を確保し、平時からその拡充を図る任務を与えられている。非常事態や戒厳令が敷かれるこの特別な期間中、ウクライナ国軍の部隊（軍）の管理を確保し、ウクライナの国家サイバーセキュリティ・システムを機能させるための対策を実施するという任務を解決しなければならない。

ウクライナ軍参謀本部の主要通信・サイバーセキュリティ部門（以下、J6）は、ウクライナ軍参謀本部（以下、ウクライナ軍参謀本部）の構造単位であり、ウクライナ軍の通信システムの管理、その機能の組織化、その拡張・拡大措置の計画、組織化、ウクライナ軍におけるサイバーセキュリティの管理を行う、ウクライナ国軍の通信システム（ウクライナ国軍の ICS）における情報の保護、ウクライナ国軍の ICS のサイバー保護は、平時および戒厳令の特別期間のいずれにおいても行われる、ウクライナ国軍の通信・防衛サイバー作戦の計画（国防軍の防衛サイバー作戦へのウクライナ国軍の参加）ウクライナ国軍、国防軍の他の構

---

[91] SSSCIP 管理局命令第 570 号 サイバー空間における様々な種類の事象に対するサイバーセキュリティ事業体の対応に関する方法論的勧告の承認について<https://zakon.rada.gov.ua/rada/show/v0570519-#Text> 2024.06.06 にアクセス。

[92] 情報通信システムにおける国家情報資源の保護に関する行政当局の相互作用のための手順の承認に関する：2002 年 11 月 16 日付ウクライナ閣僚会議決議第 1772 号：9 月 7 日現在。2022 <https://zakon.rada.gov.ua/laws/show/1772-2002-п#Text> accessed on .06.2024.

[93] "National Security and Defense Council of Ukraine"（ウクライナ国家安全保障防衛評議会）<www.rnbo.gov.ua/ua/Diialnist/5011.html> accessed on 06.06.2024.

[94]Україна, Рада національної безпеки і оборони України.(2021, 4 черв.).Рішення Ради національної безпеки і оборони України, Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони.Дата звернення : 13 серп.2023.[Онлайн].Доступно: https://zakon.rada.gov.ua/laws/show/n0039525-21#Text

成部隊の使用に関する戦略的計画、ウクライナ国軍の通信システムの開発、ウクライナ国軍への装備品・通信資産の提供の計画の過程で行われる。

J-6 は、ウクライナ軍の機密通信の中心機関であり、ウクライナ軍の野戦通信と郵便通信を提供する組織の主要機関である。

J6 の活動は、ウクライナ軍参謀本部副参謀長が権限分掌によって直接指揮、調整、統制している。

J6 の主な任務は以下の通りである：

- ウクライナ国軍の電子通信ネットワーク管理の計画、運営組織化、実施、拡大・拡張の組織化；
- ウクライナ国軍の特殊通信システムの計画、組織化、機能確保（組織状態の監視、特殊（機密）通信の安全確保、任務情報の暗号化保護を含む）；
- ウクライナ国軍の ICS の計画、組織、管理、ウクライナ国軍指導部、軍管理機関、その他ウクライナ国軍の軍事組織機構に対する基本的・機能的サービスの組織；
- ウクライナ軍のサイバーセキュリティの組織と管理、ウクライナ軍の ICS における情報の保護、ウクライナ軍の ICS のサイバー保護、ウクライナ軍の防衛サイバー作戦の組織と準備、ウクライナ軍の防衛サイバー作戦への参加；
- ウクライナ軍内のフィールド・サービスおよび郵便通信システムの運営管理に関する計画、運営組織、実施；
- ウクライナ国軍および国防軍の他の構成部隊の戦略的使用計画におけるコミュニケーション計画；
- ウクライナ国軍の軍政機関、軍部隊、部隊に対する装備品および通信機器（サービス）、ならびに野戦用および郵便用通信機器の提供を計画する；
- ウクライナ軍の通信システムを発展させるための措置を計画し、直接実施する。

ウクライナ軍参謀本部の無線・電子・サイバー戦主管部局（以下、主管部局）は、ウクライナのサイバー防衛計画、無線・電子戦およびサイバー戦の計画と実施、無線周波数帯の管理、関連能力の開発に関する任務の実施を組織することを目的としている。本局の主な任務は以下のとおりである：

- ウクライナ国防軍および国防軍の他の構成部隊の戦略的利用のために、サイバー戦争を計画、組織、準備、実施する；
- ウクライナ、国家当局、安全保障・防衛セクターの各コンポーネントのサイバー防衛行動の計画と調整を行う；

- ウクライナ国軍および国防軍の他の構成部隊の戦略的利用のために、電子戦の計画、準備の組織化、および実施を行う；

- ウクライナの「電子通信に関する」法律により、特別な利用者による無線周波数帯域の利用分野の管理に関する参謀本部の権限が実施される。

J-6 はまた、軍のネットワークのサイバー防衛の組織化にも責任を負っている。

## 3.5 民間セクターとの関わり

サイバーセキュリティ分野における官民の交流は、ウクライナの法律「ウクライナのサイバーセキュリティ確保の基本原則について」によって行われている。

1.サイバーセキュリティ分野における官民協力は、以下のような形で行われている：

1) ボランティア組織の参加を含め、サイバー脅威をタイムリーに検知、予防、無力化するシステムを構築する；

2) 市民のデジタルリテラシーを高め、サイバースペースにおける安全な行動の文化、サイバーセキュリティの目標をサポートするために必要な複合的な知識、技能、能力を向上させる；

3) 重要インフラに対するサイバー脅威、その他のサイバー脅威、サイバー攻撃、サイバー事件に関して、国家機関、民間企業、市民の間で情報交換を行う；

4) コンピュータ緊急対応チームの連携と調整を行う；

5) サイバーセキュリティ分野における主要な産業プロジェクトや規範文書の作成に、専門家ポテンシャル、科学機関、専門家団体、公的機関が関与すること；

6) サイバー攻撃への対応において、助言と実践的支援を提供する；

7) インターネットの安全性を確保するためのイニシアチブの形成と、市民、産業界および企業の代表者のための権威ある相談窓口の設置；

8) サイバーセキュリティを確保するための措置の有効性を公的に管理する仕組みを導入する；

9) 保険会社、監査人、弁護士を含むプロフェッショナル・ビジネス・サービス・プロバイダーとの全国サミットを定期的に開催し、サイバーセキュリティ分野におけるより良いリスク管理の推進における彼らの役割を決定する；

10) 人材育成システムを構築し、サイバーセキュリティ問題に関するさまざまな活動領域の専門家の能力を向上させる；

11)　個人、公共団体、ボランティア団体、IT 企業などと緊密に協力し、サイバー空間におけるサイバー防衛対策を実施する。

2.サイバーセキュリティ分野における官民の相互作用は、特定の対象や種類の活動に関して法律で定めら れている法体系の特殊性を考慮して適用される。

# 4. 参考文献

## 4.1 方針

社会領域のデジタル変革戦略の承認について：命令。Kab. of the Ministers of Ukraine dated October 28, 2020 No. 1353-r <https://zakon.rada.gov.ua/laws/show/1353-2020-p#Text> accessed on 06.06.2024

2025 年までのデジタル発展、デジタル変革、国家財政管理システムのデジタル化の実施戦略の承認と、その実施に向けた措置計画の承認に関する：命令 Kab. of the Ministers of Ukraine dated November 17, 2021 No. 1467-r: as of April 11 2023 <https://zakon.rada.gov.ua/laws/show/1467-2021-p#Text> accessed on 06.06.2024.2021 年 5 月 14 日付ウクライナ国家安全保障・防衛評議会決定「ウクライナのサイバーセキュリティ戦略について」：2021 年 8 月 26 日付ウクライナ大統領令第 447/2021 号 <https://zakon.rada.gov.ua/laws/show/447/2021#Text> 2024 年 6 月 6 日閲覧。

## 4.2 法律

デジタル変革省の課題 2019 年 9 月 18 日付ウクライナ閣僚会議決議第 856 号：2024 年 1 月 13 日現在 <https://zakon.rada.gov.ua/laws/show/856-2019-п#Text> 2024.06.06 にアクセス。

デジタルトランスフォーメーションの課題：命令。Kab. of Ministers of Ukraine dated February 17, 2021 No. 365-r: as of May 4 2023 <https://zakon.rada.gov.ua/laws/show/365-2021-p#Text> accessed on 06.06.2024.

デジタル開発の問題 2019 年 1 月 30 日付ウクライナ閣僚会議決議第 56 号：2023 年 6 月 30 日現在 <https://zakon.rada.gov.ua/laws/show/56-2019-п#Text> 2024.06.06 にアクセス。

中央・地方行政機関のデジタル開発、デジタル変革、デジタル化の問題に関するユニット、中央行政機関の副長、地方行政機関、キエフ市、セヴァストポリ市のデジタル開発、デジタル変革、デジタル化の問題に関する活動の問題点：Decree of the Cabinet of Ministers of Ukraine dated 03.03.2020 No. 194 <https://zakon.rada.gov.ua/laws/show/194-2020 п#Text> accessed on 06.06.2024.

電子サービスの統一国家ウェブポータルと行政サービスの統一国家ポータルの発行：2019.12.04 付ウクライナ閣僚会議決議第 1137 号：2024 年 4 月 2 日現在<https://zakon.rada.gov.ua/laws/show/1137-2019-п#Text> 2024.06.06 にアクセス。

市民の上訴について 1996 年 10 月 2 日付ウクライナ法第 393/96-VR 号：2023 年 12 月 31 日現在 <https://zakon.rada.gov.ua/laws/show/393/96-вр#Text> 2024.06.06 にアクセス。

e-パスポートおよび海外渡航用 e-パスポート、それらの電子コピーの作成・検証手続きの承認について：2021 年 8 月 18 日付 CMU 法令第 911 号：2022 年 11 月 17 日現在 <https://zakon.rada.gov.ua/laws/show/911-2021-п#Text> 2024 年 6 月 6 日アクセス。

出生証明書に記載された情報および登録された居住地に関する情報の電子表示の使用に関する実験的プロジェクトの実施について：2020 年 9 月 23 日付ウクライナ閣僚会議令第 911 号：3 月 14 日現在。2022 <https://zakon.rada.gov.ua/laws/show/911-2020-п#Text> accessed on 06.06.2024.

国内避難民の会計について Decree of Cabinet of Ministers of Ukraine dated October 1, 2014 No. 509: as of November 24 2023 <https://zakon.rada.gov.ua/laws/show/509-2014-п#Text> accessed on 06.06.2024.

電子学生（生徒）チケットの使用に関する実験的プロジェクトの実施について：Decree of the Cabinet of Ministers. of Ukraine dated 18.12.2019 No. 1051: as of February 1 2022 <https://zakon.rada.gov.ua/laws/show/1051-2019-п#Text> accessed on 06.06.2024.

第 9 回召集のウクライナ・ヴェルホヴナ・ラーダの委員会のリスト、量的構成、テーマについて：2019 年 8 月 29 日付ウクライナ議会の決議 Verkhov.第 19-IX 号：2023 年 2 月 23 日現在 <https://zakon.rada.gov.ua/laws/show/19-20#Text> 2024.06.06 にアクセス。

国家情報資源保存国立センターの機能に関する実験的プロジェクトの実施について：2021 年 2 月 8 日付閣議令第 94 号：2023 年 4 月 11 日現在 <https://zakon.rada.gov.ua/laws/show/94-2021-п#Text> 2024 年 6 月 6 日アクセス。

国家情報資源保存国立センターの機能に関する問題：ウクライナ閣僚会議決議（No. 311, 04/07/2023 <https://zakon.rada.gov.ua/laws/show/311-2023-п#Text> accessed on 06.06.2024.

国家情報資源保存国立センターのサービス提供手続きの承認について：2022 年 5 月 3 日付ウクライナ閣僚会議決議第 522 号：2023 年 4 月 11 日現在 <https://zakon.rada.gov.ua/laws/show/522-2022-п#Text> 2024 年 6 月 6 日アクセス。

全国電気通信ネットワークの機能に関する問題：2020 年 12 月 16 日付ウクライナ閣僚会議決議第 1358 号：2022 年 8 月 20 日現在 <https://zakon.rada.gov.ua/laws/show/1358-2020 п#本文> 2024 年 6 月 6 日にアクセスされた。

全国電気通信ネットワークのサービスリストの承認について：2021 年 8 月 17 日付のウクライナ行政府通信・情報特別業務令第 502 号：2023 年 4 月 12 日現在 Govt. special services communication and of Information of Ukraine dated August 17, 2021 No. 502: as of April 12 2023 <https://zakon.rada.gov.ua/laws/show/z1288-21#Text> accessed on 06.06.2024.

重要インフラ対象物のサイバー保護に関する一般要件の承認について：2019 年 6 月 19 日付閣議決議第 518 号：9 月 7 日現在。2022 <https://zakon.rada.gov.ua/laws/show/518-2019-п#Text> > accessed on 06.06.2024.

情報通信システムにおける情報の保護に関する：Law of Ukraine dated 07/05/1994 No. 80/94-VR: as of April 4 2024 <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text> accessed on 06.06.2024.

情報、電気通信、情報通信システムにおける情報保護のための規則の承認について：2006 年 3 月 29 日付ウクライナ閣僚会議決議第 373 号：2022 年 10 月 21 日現在 <https://zakon.rada.gov.ua/laws/show/373-2006-п#Text> 2024 年 6 月 6 日アクセス。

個人情報の保護について 2010 年 6 月 1 日付ウクライナ法第 2297-VI 号：2024 年 4 月 27 日現在 <https://zakon.rada.gov.ua/laws/show/2297-17#Text> 2024 年 6 月 6 日アクセス。

電子信託サービスについて 2017 年 10 月 5 日付ウクライナ法第 2155-VIII 号：2024 年 1 月 1 日現在 <https://zakon.rada.gov.ua/laws/show/2155-19#Text> 2024.06.06 にアクセス。

情報通信システムにおける国家情報資源の保護に関する行政当局の相互作用のための手続きの承認に関する：2002 年 11 月 16 日付ウクライナ閣僚会議決議第 1772 号：9 月 7 日現在。2022 <https://zakon.rada.gov.ua/laws/show/1772-2002-п#Text> accessed on 06.06.2024.

行政当局、およびその管理領域に属する企業、機関、組織の情報、通信、情報通信システムの登録に関する規則の承認について：2005 年 8 月 3 日付ウクライナ閣僚会議決議第 688 号：9 月 7 日現在。2022 <https://zakon.rada.gov.ua/laws/show/688-2005-п#Text> accessed on 06.06.2024.

情報化施設の設計、実施、運用における必須作業段階リストの承認に関する：1998 年 2 月 4 日付ウクライナ閣僚政令第 121 号：9 月 3 日現在。2011 <https://zakon.rada.gov.ua/laws/show/121-98-п#Text> accessed on 06.06.2024.

ウクライナの国家安全保障について 2018 年 6 月 21 日付ウクライナ法第 2469-VIII 号：3 月 31 日現在。2023 <https://zakon.rada.gov.ua/laws/show/2469-19#Text> accessed on 06.06.2024.

国家のサイバーセキュリティに対する脅威とそれを無力化するための緊急措置について：2016 年 12 月 29 日付ウクライナ安全保障・防衛国家評議会決定：2017 年 2 月 16 日現在 <https://zakon.rada.gov.ua/laws/show/n0015525-16#Text> 06.06.2024 にアクセス。

国家情報資源が処理される情報・通信・情報通信システムの構成における脆弱性や欠陥を特定するための組織的・技術的対策一式の導入に関する実験的プロジェクトの実施について：2020 年 12 月 23 日付ウクライナ閣僚会議決議第 1363 号：9 月 7 日現在。2022 <https://zakon.rada.gov.ua/laws/show/1363-2020-п#Text> accessed on 06.06.2024.

脆弱性を検知し、サイバーインシデントやサイバー攻撃に対応するシステムの機能確保に関する問題：2020 年 12 月 23 日付ウクライナ閣僚会議決議第 1295 号：9 月 7 日現在。2022 <https://zakon.rada.gov.ua/laws/show/1295-2020-п#Text> accessed on 06.06.2024.

情報（自動化された）、電子通信、情報通信システム、電子通信ネットワークの潜在的脆弱性を検索・特定する手順の承認について：Decree of the Kab. of the Ministers of Ukraine dated May 16, 2023 No. 497 <https://zakon.rada.gov.ua/laws/show/497-2023-п#Text> accessed on 06.06.2024.

情報、電気通信、情報通信システムにおける国家情報資源のセキュリティ状態を評価する手続きの承認に関する：2014 年 12 月 2 日付のウクライナ政府通信情報特別庁の命令である。Govt. special services communication and of Information of Ukraine dated 02.12.2014 No. 660: as of January 10 2023 <https://zakon.rada.gov.ua/laws/show/z0090-15#Text> accessed on 06.06.2024.

インターネットに掲載されている国家情報資源の脆弱性をスキャンする手順の承認に関する：2016 年 1 月 15 日付のウクライナの行政当局の命令である。Govt. special services communication and of Information of Ukraine dated January 15, 2016 No. 20: as of January 10 2023 <https://zakon.rada.gov.ua/laws/show/z0196-16#Text> accessed on 06.06.2024.

重要情報インフラ、国家情報資源および情報のサイバー保護状態のレビューの実施手順の承認について：2020 年 11 月 11 日付ウクライナ閣僚会議決議第 1176 号 <https://zakon.rada.gov.ua/laws/show/1176-2020-п#Text> 2024 年 6 月 6 日アクセス。

情報通信システムの遠隔測定収集サブシステム（アクティブセンサー）、脆弱性を検出し、サイバーインシデントやサイバー攻撃に対応するシステムの機器一式をサイバー保護対象に譲渡する手続きの承認について：管理者の命令である。2022 年 6 月 24 日付ウクライナ特別通信・情報保護国家サービス第 284 号 <https://zakon.rada.gov.ua/laws/show/z0758-22#Text> 2024 年 6 月 6 日アクセス。

2021 年 5 月 14 日付ウクライナ国家安全保障・防衛評議会決定「ウクライナのサイバーセキュリティ戦略について」：2021 年 8 月 26 日付ウクライナ大統領令第 447/2021 号 <https://zakon.rada.gov.ua/laws/show/447/2021#Text> 2024 年 6 月 6 日閲覧。

サイバー保護の組織的・技術的モデルに関する規則の承認について：ウクライナ閣僚会議決議（12/29/2021）第 1426 号 <https://zakon.rada.gov.ua/laws/show/1426-2021 п#本文> 2024 年 6 月 6 日にアクセスされた。

2021 年 12 月 30 日付ウクライナ国家安全保障・防衛評議会決定「ウクライナのサイバーセキュリティ戦略の実施計画について」：2022 年 2 月 1 日付ウクライナ大統領令第 37/2022 号 <https://zakon.rada.gov.ua/laws/show/37/2022#Text> 2024.06.06 にアクセス。情報について 1992 年 10 月 2 日付ウクライナ法第 2657-XII 号：2023 年 7 月 27 日現在 <https://zakon.rada.gov.ua/laws/show/2657-12#Text> 2024.06.06 にアクセス。

国家機密について 1994 年 1 月 21 日付ウクライナ法第 3855-XII 号：2024 年 1 月 1 日現在 <https://zakon.rada.gov.ua/laws/show/3855-12#Text> 2024.06.06 にアクセス。

国家機関のインターネットへのアクセス保護システムに関する規則の承認について：2023 年 8 月 30 日付ウクライナ特別通信・情報保護国家庁命令第 771 号 <>2023 年 8 月 30 日付第 771 号 <https://zakon.rada.gov.ua/laws/show/z1624-23#Text>（2024 年 6 月 6 日付アクセス）。

行政当局におけるコンピュータ・プログラムの使用手続きの承認について：2003 年 9 月 10 日付ウクライナ閣僚会議決議第 1433 号：2024 年 4 月 12 日現在 <https://zakon.rada.gov.ua/laws/show/1433-2003-п#Text> 2024 年 6 月 6 日アクセス。

電子文書管理システムのサイバー保護レベル向上のための方法論的勧告の承認について：2023 年 8 月 30 日付ウクライナ SSSCIP 指令第 773 号<>。SSSCIP of Ukraine, August 30, 2023 No. 773 <https://zakon.rada.gov.ua/rada/show/v0773519-23#Text> accessed on 06.06.2024.

ウクライナの特別通信および情報保護のための国家サービスに関する：Law of Ukraine dated 23.02.2006 No. 3475-IV: as of December 31 2023<https://zakon.rada.gov.ua/laws/show/3475-15#Text> accessed on 06.06.2024.

国家サイバーセキュリティ調整センターについて：Decree of President of Ukraine dated 07.06.2016 No. 242/2016: as of July 17 2021 <https://zakon.rada.gov.ua/laws/show/242/2016#Text> accessed on 06.06.2024.

サイバー空間における様々な種類の事象に対するサイバーセキュリティ事業体の対応に関する方法論的勧告の承認に関する SSSCIP 管理局の命令第 570 号<https://zakon.rada.gov.ua/rada/show/v0570519-23#Text> 2024 年 6 月 6 日にアクセスされた。

サイバー空間における様々な種類の出来事に対するサイバーセキュリティ機関の対応に関するいくつかの問題点：ウクライナ閣僚会議決議（2023 年 4 月 4 日付）第 299 号 <https://zakon.rada.gov.ua/laws/show/299-2023-п#Text> 2024 年 6 月 6 日閲覧。

## 4.3 その他

"Results of Assessment of Existing Population of Ukraine Have Published" *(*www.kmu.gov.ua) <www.kmu.gov.ua/news/oprilyudneno-rezultati-ocinki-chiselnosti-nayavnogo-naselennya-ukrayini> Date accessed 5 Aug 2024.

2020 年 1 月 1 日現在の地域別インターネット加入者数」（ukrstat.gov.ua） <https://ukrstat.gov.ua/operativ/operativ2019/zv/zv_reg/kaI_reg/kaI_reg0419_u.htm> 2023 年 6 月 8 日にアクセス。

"National Atlas of Ukraine" (World Data Centre | WORLD DATA CENTRE) <http://wdc.org.ua/atlas/1060000.html> accessed on 06.08.2023.

"GDP Per Capita (Current US$) - Ukraine" (*data.worldbank.org*).<https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=UA> accessed on 06.08.2023.

「NCSI：：ウクライナ" (*Index*) <https://ncsi.ega.ee/country/ua/210/> accessed on 06.06.2024.

"ITU | 2017 Global ICT Development Index" (*ITU: Committed to connecting world*). <www.itu.int/net4/ITU D/idi/2017/index.html> accessed on 06.06.2024.

"National Cyber Power Index 2022" (*Belfer Centre for Science and International Affairs*) <www.belfercentre.org/publication/national-cyber-power-index-2022> accessed on 06.06.2024.

"Ukraine - Network Readiness Index" (*Network Readiness Index - Benchmarking Future of Network Economy*) <https://networkreadinessindex.org/country/ukraine/> accessed on 06.06.2024.

"The 2023 NTI Nuclear Security Index" (*The Nuclear Threat Initiative*) <www.nti.org/analysis/articles/the-2023 nti-nuclear-security-index/> accessed on 06.06.2024.

About Us Ministry of Digital Transformation of Ukraine" (ウクライナデジタル変革省) <https://thedigital.gov.ua/ministry> accessed on 06.06.2024.

"電子サービス DIIA の統一国家ウェブポータル｜国家企業「DIIA」（State Enterprise "DIIA"） <https://se.diia.gov.ua/unified-state-web-portal-of-electronic-services-diia> 2024.06.06 にアクセスした。

「CERT-UA" (*cert.gov.ua*) <https://cert.gov.ua/about-us> 06.06.2024 にアクセスした。

"National project Diia.business" (Diia.business - Main page) <https://business.diia.gov.ua/about-project> accessed on 06.06.2024.

重要情報インフラ、国家情報資源、法律で保護要件が定められている情報のサイバー保護状態のレビューに関する報告書（SSSCIP 2023）。*ICS* における国家電子情報資源の保護状況に関する情報および分析資料（SSSCIP 2023）。

*2023* 年上半期のウクライナのサイバーセキュリティ戦略計画（SSSCIP 2023）の実施に関する分析報告書。

*2022* 年におけるウクライナ国家特殊通信情報保護局による国家のサイバーセキュリティ確保に関する任務の実施に関する報告書（SSSCIP 2023）。

脅威の調査結果に基づく *SSSCIP* の分析レポート（SSSCIP2023）
<https://cip.gov.ua/services/cm/api/attachment/download?id=60201>。

サイバーインシデント及びサイバー攻撃に対する脆弱性検知・対応体制に関する報告書
<https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf>.

国家サイバーセキュリティの主な対象者の活動に関する独立監査の結果に関する年次報告書の提出とさらなる評価に関する報告書（デジタルトランスフォーメーションに関する委員会）
<www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_01.pdf>。

ウクライナ法「ウクライナにおけるサイバーセキュリティ確保の基本原則について」の実施監視に関する予備報告書（デジタルトランスフォーメーション委員会）
<www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_02.pdf>.

サイバーセキュリティ管理のベストプラクティス（デジタルトランスフォーメーション委員会）
<www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_04.pdf>.

"National Cybersecurity Centre" (国家サイバーセキュリティセンター) <www.ncscc.gov.ua/> 2024.06.06 にアクセスした。"Scientific and practical commentary on the provision on the organizational and technical model of cyber protection, approved by the resolution of the Cabinet of Ministers of 12.29.2021 No. 1426" *(*https://cip.gov.ua, 11 Feb. 2022) <https://cip.gov.ua/ua/news/naukovo-praktichnii-komentar-do-polozhennya pro-organizaciino-tekhnichnu-model-kiberzakhistu-zatverdzhenogo-postanovoyu-kabinetu-ministriv-ukrayini vid-29-grudnya-2021-r-1426> accessed on 06.06.2024.

"National Security and Defence Council of Ukraine" (ウクライナ国家安全保障防衛評議会) <www.rnbo.gov.ua/ua/Diialnist/5765.html> accessed on 06.06.2024

「信頼できる紹介者ディレクトリ：CERT-UA" (*Trusted Introducer: Home*) <www.trusted introducer.org/directory/teams/cert-ua.html> accessed on 06.06.2024.

"E-Government Development Index" <https://publicadministration.un.org/egovkb/en-us/Data/Country Information/id/180-Ukraine> accessed on 06.08.2023.

ウクライナ国家安全保障防衛会議」（National Security and Defense Council of Ukraine）
<www.rnbo.gov.ua/ua/Diialnist/5011.html>は 2024 年 6 月 6 日にアクセスした。

# 5. 略語

| | | |
|---|---|---|
| CCDCOE | Cooperative Cyber Defence Centre of Excellence | 協力的なサイバー防衛センター・オブ・エクセレンス |
| CDTO | Chief Digital Transformation Officer | チーフ・デジタルトランスフォーメーション・オフィサー |
| CERT-UA | The Computer Emergency Response Team of Ukraine | ウクライナのコンピュータ緊急対応チーム |
| CMU | Cabinet of Ministers of Ukraine | ウクライナ閣僚会議 |
| CSIRT | Computer Security Incident Response Team | コンピュータ・セキュリティ・インシデント対応チーム |
| EU | European Union | 欧州連合 |
| GDP | Gross Domestic Product | 国内総生産 |
| IAS | Information and Analytical System | 情報分析システム |
| ICS | Information and Communication Systems | 情報通信システム |
| ICT | Information and Communication Technology | 情報通信技術 |
| IT | Information Technology | 情報技術 |
| ITU | International Telecommunication Union | 国際電気通信連合 |
| MODT | Ministry of Digital Transformation of Ukraine | ウクライナ・デジタル変革省 |
| NATO | North Atlantic Treaty Organisation | 北大西洋条約機構 |
| NCSCC | The National Cyber Security Coordination Centre | 国家サイバーセキュリティ調整センター |
| NCSI | National Cyber Security Index | 全米サイバーセキュリティ指数 |
| NSDC | The National Security and Defence Council of Ukraine | ウクライナ国家安全保障防衛会議 |
| NTI | Nuclear Threat Initiative | 核の脅威イニシアティブ |
| NTN | National Telecommunication Network | 全国通信ネットワーク |
| OTM | The Organisational and Technical Model of Cyber Protection | サイバー保護の組織的・技術的モデル |
| SMS | Short Message Service | ショートメッセージサービス |
| SSSCIP | State Service of Special Communications and Information Protection of Ukraine | ウクライナ特別通信・情報保護局 |
| SSU | Security Service of Ukraine | ウクライナ保安庁 |

| | | |
|---|---|---|
| TIN | Tax Identification Number | 納税者番号 |
| TLP | Traffic Light Protocol | トラフィック・ライト・プロトコル |
| US | United States | 米国 |