DPRK サイバー脅威勧告

発表日: **2020 年 4 月 15 日**

題目: **北朝鮮サイバー脅威に関するガイドライン**

米国国務省、財務省、国土安全保障省、および連邦捜査局は、国際社会、ネットワーク防衛担当者、ならびに一般市民のために北朝鮮サイバー脅威に関する包括的な資料として本勧告を公表する。本勧告は、正式名朝鮮民主主義人民共和国(DPRK)である北朝鮮によるサイバー脅威を強調し、かつ、この脅威を低減するための推薦される措置を提供する。特に、添付書類1ではDPRKのサイバー脅威に関連する米国政府の資料を列挙し、添付書類2は国連1718制裁委員会（DPRK）専門家パネルの諸報告書へのリンクを含めている。

DPRKの悪意あるサイバー活動は米国やより広い国際社会に脅威を及ぼし、とりわけ国際金融制度の完全性と安定性に対する重大な脅威となる。強固な米国および国連制裁の圧力の下で、DPRKは大量破壊兵器と弾道ミサイルのプログラムのための収入を生み出すために、サイバー犯罪を含む不法活動にますます依存するようになってきている。米国はとりわけ、米国政府が「隠されたコブラ」と呼んでいる北朝鮮の悪意あるサイバー活動に、深い懸念を抱いている。DPRK は、米国の重要なインフラに影響を及ぼす攪乱的あるいは破壊的なサイバー活動を行う能力を有している。さらにDPRKは、金融機関から盗むためにサイバー能力を使用しており、何がサイバー空間での国家の責任ある行動であるかに関して醸成されつつある国際的なコンセンサスに全く反する攪乱的で有害なサイバー活動のパターンを示してきた。

米国は、同じ考え方をもつ諸国と緊密に協力して、DPRK の攪乱的、破壊的、あるいはその他のサイバー空間を不安定化させる行動に注意を払いかつこれを非難する。例えば、2017年12月には、オーストラリア、カナダ、ニュージーランド、米国、および英国は、 WannaCry 2.0 というランサムウェア攻撃がDPRKの仕業であることを公にし、DPRKの有害で無責任なサイバー活動を非難した。デンマークと日本は、2017年5月に世界中の何十万台ものコンピュータに害をもたらした攪乱的なWannaCry 2.0ランサムウェア攻撃に対する共同非難を支持する声明を公表した。

国際社会、ネットワーク防衛担当者、および一般市民は、北朝鮮がもたらすサイバー脅威を低減するために警戒を怠らず協力することが大切である。

金融セクターを標的とするDPRKの悪意あるサイバー活動

DPRKのサイバー活動者の多くは、朝鮮人民軍総参謀部偵察局のような国連や米国に指定された機関に従属している。DPRKの国家支援によるサイバー活動者は、ハッカー、暗号に精通したデコーダー、ソフトウェア開発者から主に構成され、彼らはスパイ活動、金融機関や仮想通貨交換所を標的とするサイバー窃盗、および外国メディア企業に対する政治的な動機による操作などを行う。彼らはこれらの活動を可能にするために世界中で広範囲のマルウェア・ツールを開発し、設置し、ますます巧妙になってきている。DPRKの国家支援を受けたサイバー活動者による不法収入を獲得するためのよくある戦術には以下のような活動が含まれるが、これに限られるものではない。

サイバーによる金融窃盗やマネーロンダリング。 国連安保理1718委員会専門家パネルの2019年中間報告書 (2019年 POE中間報告書) は、国連安保理の制裁にも拘わらず、DPRKがますます高度になっているツールや戦術を通じて金融機関から盗むための悪意あるサイバー活動の活用によって、ますます収入を生み出せるようになってきていると述べている。2019年 POE 中間報告書は、ある場合には、こうした悪意あるサイバー活動が複数の法域を通過するマネーロンダリングにも拡大されていると指摘している。2019年 POE中間報告書は、十数件のDPRKによるサイバー強盗疑惑を捜査しており、DPRKは2019年末の時点で、こうした不法サイバー活動により20億ドルもの金の窃盗を試みたと指摘している。2020 年3月の司法省の没収申し立てにおける主張はPOEの調査結果の部分と一致している。特に、没収申し立ては、北朝鮮のサイバー活動者が仮想通貨交換所をハッキングしたり、何億ドルものデジタル通貨を盗んだり、資金をロンダリングしたりする陰謀の推進のために北朝鮮のインフラをどのように使ったかを述べている。

恐喝キャンペーン。DPRK のサイバー活動者はさらに、第三国機関に対してその機関のネットワークに不正侵入し、身代金を払わなければそれを閉鎖するという恐喝キャンペーンも行った。ある場合には、DPRKのサイバー活動者は、将来そのような悪意あるサイバー活動がないことを保証するための長期的なコンサルティング取り決めを装って、被害者から支払いを要求した。DPRKのサイバー活動者はさらに、第三者クライアントのために、ウェブサイトのハッキングや標的の恐喝を行うことを請け負って支払いを得ている。

クリプトジャッキング。 2019年 POE中間報告書は、POEがDPRKのクリプトジャッキングの活用を捜査しているとも述べているが、これは被害者の装置に不正侵入し、デジタル通貨をマイニングするコンピュータ資源を盗むスキームである。POEは、クリプトジャッキングのマルウェアに汚染されたコンピュータが、マイニングされた資産ーその多くは匿名性が強化されたデジタル通貨（時には「プライバシーコイン」ともいわれる）を、平壌にある金日成総合大学を含めて、DPRKにあるサーバーに 送ったといういくつかの事例を特定した。

こうした活動は、制裁の影響を低減する一方で収入を生み出すために DPRKがサイバー手段の活用を行っていることを強調するものであり、いかなる国もDPRKによる被害を受け、利用さ

れうることを示している。 2019 年POE中間報告書によると、POEはまた、DPRKに対する国連安全保障理事会の制裁違反の試みとして、これらの活動を捜査中である。

米国政府がDPRKの仕業として公にしたサイバー活動

DPRKは、データを盗み、攪乱的および破壊的なサイバー活動を行うために、米国やその他の政府と軍事ネットワーク、ならびに民間機関や重要なインフラに関連するネットワークを繰り返し標的としてきた。現在までに、米国政府は以下のサイバー事件を DPRK の国家支援によるサイバー活動者や共謀者の仕業であると公にしてきた。

- ***ソニーピクチャーズ。*** 2014年11月に、DPRKの国家支援によるサイバー活動者は、ソニーピクチャーズエンターテインメント (SPE) に対して、2014年の映画『インタビュー』への報復としてサイバー攻撃を行ったとされている。DPRKのサイバー活動者は、極秘データを盗むためにSPEネットワークをハッキングし、SPEの幹部や従業員を脅迫し、何千台ものコンピュータに損害を与えた。

    - ソニー捜査に関するFBIの最新情報 (2014年12月19日) https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation
    - 北朝鮮政権が支援するプログラマーに関する司法省の刑事訴状 (2018年9月6日) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- ***バングラデシュ銀行強盗。*** 2016年2月、DPRKの国家支援によるサイバー活動者は、世界中の金融機関から少なくとも10億ドルを盗もうとしたとされ、国際銀行間通信協会（SWIFT）ネットワークの不正取引を通じてバングラデシュ銀行から8100万ドルを盗んだとされている。訴状によると、DPRKのサイバー活動者は銀行の従業員を標的にするスピアフィッシングの電子メールを通じて銀行のコンピュータネットワークに不正侵入した後、SWIFTネットワークとインターフェイスするバングラデシュ銀行のコンピュータ端末にアクセスした。それからDPRKサイバー活動者は、不正に証明されたSWIFTのメッセージを ニューヨークの連邦準備銀行に送り、バングラデシュ銀行の連邦準備銀行口座から共謀者が管理する口座へと資金を移転するよう指示した。

    - 北朝鮮政権支援のプログラマーに関する司法省の刑事訴状 (2018年9月6日) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- ***WannaCry 2.0***. DPRKの国家支援によるサイバー活動者は、WannaCry 2.0といわれるランサムウェア、およびその以前のランサムウェア2バージョンを開発した。2017年5月に、WannaCry 2.0 ランサムウェアは150カ国以上の病院、学校、企業、および家庭の何十万台というコンピュータをウィルス感染させた。WannaCry 2.0ラン

サムウェアは感染したコンピュータのデータを暗号化し、ビットコインのデジタル通貨での身代金支払いをサイバー活動者が要求できるようにした。財務省は、北朝鮮のコンピュータプログラマーの一人をWannaCry 2.0 の共同謀議とソニーピクチャーズサイバーへの攻撃とバングラデシュ銀行強盗において役割を果たしたとして指定し、さらに、本人が働いていた組織を指定した。

- CISAのテクニカル警報: WannaCry ランサムウェアに関連する指標 (2017年5月12日) https://www.us-cert.gov/ncas/alerts/TA17-132A
- WannaCryランサムウェアの出元についてのホワイトハウス・プレスブリーフィング (2017年12月19日) https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/
- 北朝鮮政権が支援するプログラマーに関する司法省の刑事訴状(2018年9月6日) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and
- 複数のサイバー攻撃について財務省は北朝鮮を標的とする (2018 年 9 月 6 日) https://home.treasury.gov/news/press-releases/sm473

- ***FASTCash キャンペーン。*** DPRKの国家支援によるサイバー活動者は、2016年末以降、アジアやアフリカのATMから何千万ドルも盗むために『FASTCash』と呼ばれるATM現金引き出しスキームを駆使している。FASTCashスキームは、詐欺的取引を促進するために銀行内の支払い変更のアプリケーションサーバーに遠隔地から不正侵入する。2017年のある事件では、DPRKのサイバー活動者は30カ国以上の国にあるATMから同時に現金を引き出すことを可能にした。2018年の別の事件では、DPRKのサイバー活動者は23ヵ国のATMから同時に現金が引き出せるようにした。

  - FASTCashキャンペーンに関するCISAの警報 (Oct. 2, 2018) https://www.us-cert.gov/ncas/alerts/TA18-275A
  - CISAのマルウェア分析報告書: FASTCash関連のマルウェア (2018年10月2日) https://www.us-cert.gov/ncas/analysis-reports/AR18-275A

- ***仮想通貨交換所ハッキング。*** 2018年4月の司法省による対物没収の申し立てに述べられた主張に詳細が記載されているように、DPRKの国家支援によるサイバー活動者は仮想通貨交換所をハッキングし、デジタル通貨ほぼ2億5千万ドル相当を盗んだ。申し立てにおいてはさらに、法執行機関が資産の出所を突き止めるのを防止する試みとして資金源を見えにくくするために、盗まれた資産が何百回もの自動仮想通貨取引を通じてどのようにロンダリングされたかを述べている。その後、2人の中国市民が北朝鮮グループを代理して資産ロンダリングを行い、DPRK管理の口座から約9100万ドルと、別の通貨交換所のハッキングからの追加の950万ドルを受け取ったと、申し立ての中で主張されている。2020年3月には、財務省はサイバーおよびDPRK制裁権限の下でその2個人を指定し、同時に司法省は当該個人が

マネーロンダリングと無認可の送金の容疑で以前に告発されており、113のデジタル通貨口座が没収の対象であるとの発表した。

- ラザルスグループのために暗号通貨をロンダリングした個人に対する財務省の制裁（2020年3月2日) https://home.treasury.gov/news/press-releases/sm924
- 通貨交換所ハッキングからの暗号通貨のロンドリング容疑での２人の中国市民の司法省起訴と民事没収申し立て (2020年3月2日) https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack

DPRK のサイバー脅威への対抗措置

北朝鮮は、大量破壊兵器プログラムを含めて、政権の優先課題のために収入を生み出すべく全世界のサイバー可動インフラを標的としている。各国政府、産業、市民団体、および各個人に対して、DPRK のサイバー脅威から身を守り、対抗するために以下のような関連措置を全て行うように強く要請する。

- **DPRK のサイバー脅威への意識を高める。**DPRK が行った悪意あるサイバー活動の重要性、範囲かつその多様性を強調することは、脅威への官民セクターの一般的な意識を高め、適切な予防とリスク低減措置の採択と実施を促進する。

- **DPRK のサイバー脅威の技術情報を共有する。**DPRK のサイバー脅威を探知・防護するための国内・国際両レベルでの情報共有は、ネットワークとシステムの強化されたサイバーセキュリティを可能にする。ベストプラクティスは各国政府間で、かつ民間セクターで共有すべきである。2015 年サイバーセキュリティ情報共有法 (6 U.S.C. §§ 1501–1510)の条項の下では、非連邦機関は、連邦および非連邦機関と「隠されたコブラ」関連のサイバー脅威指標や防護手段を共有することができる。

- **サイバーセキュリティのベストプラクティスを実施・促進する。**サイバーセキュリティ強化のために、技術的・行動的な措置を採択することは、米国や世界のサイバーインフラをさらに安全かつ回復力のあるものにする。マネーサービス事業を含めて金融機関は、悪意ある DPRK のサイバー活動から防護するために独自の措置を講じるべきである。この措置とは、政府や産業界のチャンネルを通じての脅威情報の共有、リスクを最低限に抑えるためのネットワークのセグメント化、データの定期的なバックアップの維持、共通の社会エンジニアリング戦術に関する意識トレーニングへの取り組み、情報共有やネットワークアクセスを司る政策の実施、およびサイバー事件対応計画の作成などが含まれようが、これに限られるものではない。エネルギー省のサイバーセキュリティ能力熟練モデルと米国標準技術研究所のサイバーセキュリティ枠組みは、強固なサイバーセキュリティ実践を開発・実施するためのガイダンスを提供する。添付書類 1 に示されるように、サイバーセキュリティ・インフラストラクチャセキュリティ庁 (CISA) は、ネットワークを防衛する人々が悪意あるサイ

バー活動を確認・低減するために、テクニカル警報やマルウェア分析報告書を含む広範な資源を提供している。

- **法律施行機関に通知する。**ある組織が悪意あるサイバー活動の被害者となったことを疑う場合には、それが DPRK か他から発せられたものであっても、時宜を得た形で法律執行機関に通知することが非常に重要である。このことが捜査を早めるだけではなく、金融犯罪の場合には、盗まれた資産の回収の機会を増すこともできる。

  米国の法律執行機関は、北朝鮮のサイバー活動者によって盗まれた何百万ドルものデジタル通貨を差し押さえてきた。マネーサービスビジネスを含めてあらゆる種類の金融機関は、こうしたサイバー脅威に関する情報を求める米国法執行機関からの要請に従うことにより初期段階で協力し、米国法律執行機関からの要請あるいは米国裁判所の命令を受け取り次第没収可能な資産を確認し、かつ、そのような資産の差し押さえを支援するために米国法執行機関に最終段階で協力することによより、協力を提供するよう奨励されている。

- **反マネーロンダリング (AML)強化 / テロリズム資金調達対抗 (CFT) / 拡散資金調達防止 (CPF) 順守。**各国は AML/CFT/CPF に関する金融措置タスクフォース (FATF) 基準を迅速かつ効果的に実施すべきである。この中には、金融機関とその他対象となる機関が FATF 基準ならびに FATF 公的声明・ガイダンスに沿うリスク低減措置を活用することの保証が含まれる。特に FATF は、DPRK から発する継続的なマネーロンダリング、テロリスト資金調達、および拡散資金調達のリスクから国際金融制度を保護するための対応策を全ての国が適用するよう求めてきた。[1] これには、全金融機関やその他対象となる機関に、DPRK 企業、金融機関、およびその代理で活動している機関を含めて、DPRK とのビジネス関係や取引に特別の注意を払うよう求める勧告が含まれている。国連安保理決議 2270 本文 33 項に沿って、加盟諸国はその領土内にある DPRK 銀行の既存の支店、子会社、および代理事務所を閉鎖し、DPRK 銀行との代理店関係を停止すべきである。

  さらに 2019 年 6 月に、FATF は仮想通貨交換所を含めてデジタル資産サービス提供者を規制・監督し、デジタル通貨取引を行う際にリスクを低減するように、全ての国に義務付けるよう基準を修正した。デジタル資産サービス提供者は、顧客の企業がマネーロンダリング、テロリスト資金調達、および拡散資金調達を促進することに活用される可能性があることから、顧客の活動の変化に警戒を続けるべきである。米国はとりわけ、取引監視、不審活動報告、顧客のデューデリジェンスやその他の義務がない状態で、無記名の支払いや口座サービスの機能性を提供するプラットフォームについて懸念している。

[1] *北朝鮮に関する措置への FATF 呼びかけの全体は以下を参照のこと。* https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html.

米国でビジネス全体やその相当部分を行っている外国所在のデジタル資産サービス提供者を含めて、米国の金融機関やその他対象となる企業や個人は、銀行秘密法（31CFR の X 章にある財務省の金融犯罪執行ネットワーク（FinCEN）規制を通じて実施されているように）の下での規制義務を順守していることを保証すべきである。金融機関にとっては、こうした義務には、マネーサービスビジネスがマネーロンダリングやテロリスト活動の資金調達に使われることを防止するために妥当に設定された効果的な反マネーロンダリングプログラムの開発と維持、ならびに、FinCEN への不審活動報告においてデジタル資産が関与するサイバーイベントや不法融資によって実施され、影響され、あるいは促進された取引を含む不審取引の確認・報告が含まれる。

国際協力。 DPRKの悪意あるサイバー活動に対抗するために、米国は外交、軍事、法律執行、司法、およびネットワーク防衛やその他のチャンネルを通じての情報や証拠の共有により、DPRKサイバー脅威の意識を高めるべく世界中の国々と定期的に関与している。サイバー手段を通じて資金を盗もうとする DPRKの努力を阻止し、DPRKの悪意あるサイバー活動から防衛するために、米国は、ネットワーク防衛の強化、第三国におけるDPRKとの合弁事業の停止、適用可能な国際法に一致する方法での外国所在の北朝鮮情報技術（IT）労働者の追放などを行うよう各国に要請している。2017年国連安保理決議は、全加盟国に対して、2019年12月22日までにIT労働者を含む、海外で収入を得ているDPRK市民の送還を義務付けた。さらに米国は、DPRKのサイバー脅威を理解、識別、防御、捜査、訴追、対応し、サイバー空間の安定性の保証を助ける国際努力に参加するように、外国政府と民間セクターの能力の強化も求めている。

禁止行為あるいは制裁対象行為に関与することの結果

関連金融取引の処理を含めて、DPRK のサイバー関連活動に関与したり、支援したりする個人や機関は、禁止行為あるいは制裁対象行為に関与することの結果として起こりうることを意識すべきである。

財務省の外国資産管理室 (OFAC) は、他にもあるとはいえ、以下のような行為に関与したと判断されるあらゆる個人に制裁を課する権限を有している。

- 北朝鮮政府や朝鮮労働者党を代理して、サイバーセキュリティを弱体化させる重大な活動に関与した
- 北朝鮮で情報技術 (IT) 産業で活動した
- 他の悪意あるサイバーにより可能となる特定活動に関与した、あるいは
- 物品、サービスあるいは技術の北朝鮮からの重大な輸入や同国への重大な輸出に少なくとも一度関与した。

さらに、財務長官が、国務長官と協議の上、外国金融機関が故意に北朝鮮と重大な貿易を実施または促進した、あるいは、北朝鮮関連の大統領命令や大統領命令 13382（大量破壊兵器

拡散者とその支援者）の下で指定された人のために、北朝鮮関連の活動目的で、重大な取引を故意に実施または促進したと判断する場合には、当該機関は、その他の制約を受ける可能性もあるものの、米国での代理店あるいは口座経由支払いを維持する能力を失う可能性がある。

OFAC は、添付書類 A 経済制裁執行ガイドライン 31 C.F.R. パート 501 に概略説明されているように、明らかな制裁規則違反を捜査し、法執行権限を行使 する。北朝鮮制裁規制 31C.F.R. パート 510 に違反する人は、適用可能な法律で定められた最大限の罰則あるいはその元になった取引額の倍額のいずれかより大きな額を上限とする民事罰金に直面する可能性がある。

2019 年 POE 中間報告書は、銀行や仮想通貨交換所から資金を盗むためにサイバーにより可能となる手段の DPRK による活用したあるいは活用の試みは、複数の国連安保理決議 (UNSCRs) (例えば、UNSCR 1718 本文項 (OP) 8(d); UNSCR 2094, OPs 8 および 11; ならびに UNSCR 2270, OP 32) の違反であり得る、と指摘している。さらに、DPRK 関連の UNSCRs は、国連が課す DPRK 関連制裁への順守を奨励するさまざまなメカニズムも提供する。例えば、国連安保理 1718 委員会は、国連指定の機関とのビジネス取引や制裁回避に関与する個人や機関に標的を絞った制裁 (例えば、資産凍結、および個人の場合は旅行禁止) を課すこともできる。

司法省は、国際緊急経済権限法 50 U.S.C. §§ 1701 以下参照など、適用可能な制裁諸法の故意による違反を刑事訴追する。このような諸法に故意的に違反した人は、20 年までの禁固、100 万ドルあるいは総利益の計 2 倍のいずれかより大きな額を上限とする罰金、およびそのような取引に関わる全資金の没収に直面しうる。司法省はさらに、銀行秘密法 (BSA)、31 U.S.C. §§ 5318 と 5322 の故意の違反を刑事訴追するが、この法律は金融機関は他のこともあるものの、効果的な反マネーロンダリングプログラムの維持と、特定の報告書の FinCEN への提出を義務付けている。BSA 違反者は、5 年までの禁固、25 万ドルまでの罰金、および違反に関係する物件の没収に直面しうる。司法省はさらに、適切な場合には、こうした法律違反の企業や他機関を刑事訴追する。司法省はまた、外国パートナーと協力して、互いの刑事捜査や訴追を支援する証拠を共有する。

財務長官または司法長官は、米国法典 31 章 § 5318(k)に則り、米国に代理店銀行口座を保持する外国金融機関を外国に保管している記録のために、証人喚問できる。財務長官または司法長官が、外国金融機関は証人喚問に応じなかったことを米国金融機関に書面通知した場合には、米国金融機関は営業日 10 日間以内に代理店銀行業務を停止する必要がある。これができなかった場合には、米国金融機関は毎日民事罰金の対象となり得る。

正義のための DPRK 褒賞

過去や現在進行中の活動を含めて、サイバー空間での DPRK の不法活動について情報を持っている場合に、正義のための国務省褒賞プログラムを通じてのそのような情報提供は、500

万ドルまでの賞金を受け取る資格を得ることができる可能性がある。詳細情報は、
www.rewardsforjustice.net. を参照のこと。

添付書類 I: DPRK サイバー脅威への USG 公開情報と資料

国家情報長官室の米国諜報機関の全世界脅威年次評価。2019年、米国諜報機関は、DPRKが金融機関に対する重大なサイバー脅威になっており、サイバー スパイ脅威であり続け、かつ攪乱的なサイバー攻撃を行う能力を保持していると査定した。DPRKは、収入を生み出すために金融機関から盗むサイバー能力の活用を続けている。平壌のサイバー犯罪活動には、バングラデシュ銀行から推定8100万ドルのサイバー強盗に成功したことを含め、世界中の金融機関から11億ドル以上を盗もうとする試みが含まれている。報告書は、以下を参照のこと。https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

サイバーセキュリティおよびインフラストラクチャセキュリティ庁 (CISA) 技術報告書。米国政府は、DPRKによる悪意あるサイバー活動を「隠されたコブラ」と呼んでいる。「隠されたコブラ」報告書では、DPRKのサイバー活動者が使ったツールとインフラの技術的詳細が記載されている。こうした報告書は、DPRKの悪意あるサイバー活動をネットワーク防衛者が確認し、そのエクスポージャーを低減することを可能にする。CISAのウェブサイトには、これらの持続的な脅威に対する最新情報が記載されている: https://www.us-cert.gov/northkorea.

さらに CISA は、利害関係者にサイバーセキュリティおよびインフラセキュリティの広範な知識と実践を提供し、よりよいリスク管理を可能にするために知識を共有し、国家の重要な機能を保護するためにそれを実践する。以下は CISAの資料へのリンクである。

- 重要なインフラの保護: https://www.cisa.gov/protecting-critical-infrastructure
- サイバー安全性: https://www.cisa.gov/cyber-safety
- 探知と予防: https://www.cisa.gov/detection-and-prevention
- 情報共有: https://www.cisa.gov/information-sharing-and-awareness
- CISA の洞察: https://www.cisa.gov/insights
- サイバー犯罪との闘い: https://www.cisa.gov/combating-cyber-crime
- サイバーエッセンシャル: https://www.cisa.gov/cyber-essentials
- ヒント: https://www.us-cert.gov/ncas/tips
- 国家サイバー意識システム: https://www.us-cert.gov/ncas
- 産業管理システム助言: https://www.us-cert.gov/ics
- 事件、フィッシング、マルウェア、脆弱性の報告: https://www.us-cert.gov/report

FBI PIN と FLASH 報告書。FBIの民間産業通知 (PIN) は、民間セクターの潜在的なサイバー脅威についての意識を強化する最新情報を提供する。FBI 連絡警戒システム (FLASH) 報告書には、特定の民間セクターパートナーが活用するために、FBI が収集した非常に重要な情報が含まれている。それらは、サイバーセキュリティの専門家やシステム管理者がサイバー犯罪者の持続的な悪意ある活動に対しての防護を助ける行動可能な諜報を受領者に提供することを意図している。企業内での不審活動に気付いたり、関連情報を有する場合には、すぐにFBI CYWATCHに連絡すること。DPRK関連のサイバー脅威 PIN や FLASH 報告書については、cywatch@fbi.gov. に連絡すること。

- FBI サイバー部門: https://www.fbi.gov/investigate/cyber

- FBI 大使館付法務担当員プログラム: FBIの大使館付法務担当員の中核となる使命は、指定された諸外国の主要な法執行機関とセキュリティサービスの連絡を設置・維持することである。 https://www.fbi.gov/contact-us/legal-attache-offices

米国サイバー司令部マルウェア情報公開。 国防総省のサイバー部隊は、金融機関を利用し、スパイ活動を行い、米国やそのパートナーに対する悪意あるサイバー活動を可能にするDPRK マルウェアを含め、DPRK の悪意あるサイバー活動を活発に追及している。米国サイバー司令部は、産業や政府が DPRK の不法活動に対してインフラやネットワークを守るために脆弱性を確認して、マルウェア情報を定期的に公表している。サイバーセキュリティを強化するためのマルウェア情報は次のツイッターアカウントで見つけることができる: @US_CYBERCOM and @CNMF_VirusAlert.

米国財務省制裁情報・不法金融助言。
外国資産管理室 (OFAC's) のオンライン資料センターは、DPRKに関連する制裁助言、関連法令、大統領命令、規則およびサイバー関連制裁を含めて、DPRK制裁ならびに悪意あるサイバー活動に関する制裁について豊富な情報を提供する。OFAC はさらに、DPRK制裁、サイバー関連制裁、およびデジタル通貨についてよく出されるいくつかの質問 (FAQs) への回答も公表した。OFAC 制裁規制や要件に関する質問や懸念については、OFACの順守ホットライン宛に電話 1-800-540-6322 あるいは 電子メールOFAC_Feedback@treasury.gov. に連絡のこと。

- DPRK 制裁
  - https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx
  - よく出される質問 - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#nk
- 悪意あるサイバー活動制裁
  - https://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx
  - よく出される質問 - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#cyber
  - デジタル通貨に関するよく出される質問 - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs

金融犯罪執行ネットワーク(FinCEN) は、国際金融システム (https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a008) の北朝鮮による使用に関して助言を発表している。 FinCEN はさらに、不審活動報告義務をもつ金融機関に対して、サイバー犯罪やデジタル通貨関連の犯罪活動をいつどのように報告するかに関してガイダンスを提供する具体的助言も発表した。

- サイバー犯罪
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005
- 不法なデジタル通貨活動
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a003
- ビジネス電子メールの不正侵入
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a005

- https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003

連邦金融機関検査審議会 (FFIEC) は、金融機関がリスクを確認しサイバーセキュリティへの準備状況を判断するのを助けるためのサイバーセキュリティ査定ツールを開発した。査定ツールは以下を閲覧のこと https://www.ffiec.gov/cyberassessmenttool.htm.

添付書類 II: DPRK サイバー脅威に関する国連専門家パネルの報告書

国連 1718 制裁委員会 (DPRK) 専門家パネルの報告書。DPRKに関する国連安保理 1718 制裁委員会 は、専門家パネルに支援されており、これら専門家は北朝鮮に対する国連安保理決議に概略が述べられた措置の実施に関して、国連加盟国、関連する国連諸機関、および他の当事者からの「情報の収集、検査、分析」を行う。さらにパネルは、1718 委員会に対して中間、最終報告書の両方を提供することによって、制裁実施を改善する方法についての勧告も行う。これらの報告書は以下を参照のこと。
https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports.