資料38－１

サイバーセキュリティを巡る最近の動向

令和４年５月

サイバーセキュリティタスクフォース事務局

サイバーセキュリティ対策の強化についての注意喚起

○ 現下の情勢を踏まえ、サイバー攻撃事案のリスクは高まっていると考えられることから、総務省では、関係省庁と連携して、電気通信事業者、放送事業者及び地方公共団体等に対して、サイバーセキュリティ対策の強化について、令和4年2月23日、3月1日、3月24日に続き、4月25日にも注意喚起を実施。

「春の大型連休に向けて実施いただきたい対策について（注意喚起）」

（令和4年4月25日　経済産業省、総務省、警察庁、内閣官房内閣サイバーセキュリティセンター）

昨今においてはサイバー攻撃被害のリスクが高まっており、こうした情勢を踏まえ、今年3月には、関係府省庁の連名にて「現下の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）」等の注意喚起を発出しましたが、その後も、ランサムウェアによるサイバー攻撃被害が国内外の様々な企業・団体等で続いています。また、エモテットと呼ばれるマルウェアへの感染を狙う攻撃メールについては、知り合いのメールアドレスをそのまま使うなどにより知り合いからのメールであると信じ込ませたり、本文が業務上開封してしまいそうな正規のメールの返信を装うなど巧妙化が進み、国内の企業・団体等へ広く感染の被害が広がっていると考えられます。さらに、ブロードバンドルータ、無線 LAN ルータ、監視カメラ用機器類、コピー機をはじめとするネットワークに接続された機器・装置類がマルウェアに感染したことに起因する攻撃通信が、増加傾向にあります。

このように依然として厳しい情勢の下での春の大型連休においては、連休の間隙を突いたセキュリティインシデント発生の懸念が高まるとともに、連休明けに電子メールの確認の量が増えることで偽装のチェックなどがおろそかになるといった感染リスクの高まりが予想されます。さらに、大型連休中は、通常と異なる体制等により、予期しない事象が生じることが懸念されます。

こうした春の大型連休における長期休暇期間がサイバーセキュリティに与えるリスクに鑑み、政府機関や重要インフラ事業者をはじめとする各企業・団体等は、適切な管理策によるサイバーセキュリティの確保について、別紙の対策を講じるようお願いいたします。

あわせて、不審な動き等を検知した場合は、早期対処のために速やかに所管省庁、セキュリティ関係機関に対して連絡していただくとともに、警察にもご相談ください。

（別紙の抜粋）

＜セキュリティ対策の実施に関する責任者における実施事項＞

1. **長期休暇前の対策**
   - ✓ **長期休暇期間中のセキュリティインシデントを認知した際の対処手順及び連絡体制の確認**
   - ✓ **利用機器・外部サービスに関する対策** 例）ファームウェアアップデート
   - ✓ **ソフトウェアに関する脆弱性対策の実施** 例）セキュリティパッチ適用
   - ✓ **バックアップ対策の実施**
   - ✓ **アクセス制御に関する対策**
   - ✓ **職員等への注意喚起の実施**
2. **長期休暇明けの対策**
   - ✓ **サーバ等における各種ログの確認**
   - ✓ **ソフトウェアに関する脆弱性対策の実施**
   - ✓ **不正プログラム感染の確認**
   - ✓ **長期休暇期間中に電源を落としていた機器に関する対策**

＜情報システムを利用する職員等における実施事項＞

1. **長期休暇前の対策**
   - ✓ **利用機器に関する対策** 例）長期休暇中に使用しない機器の電源を落とす
   - ✓ **機器やデータの持ち出しルールの確認と遵守** 例）端末持ち出し内規の遵守
2. **長期休暇明けの対策**

   例）電子メール確認前の不正プログラム対策ソフトウェア等の定義ファイルの更新実施

https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000475.html

サイバー・レジリエンスに関するG7デジタル大臣による共同宣言

○ 令和4年5月10日から11日に、G7デジタル大臣会合が開催された（※）。

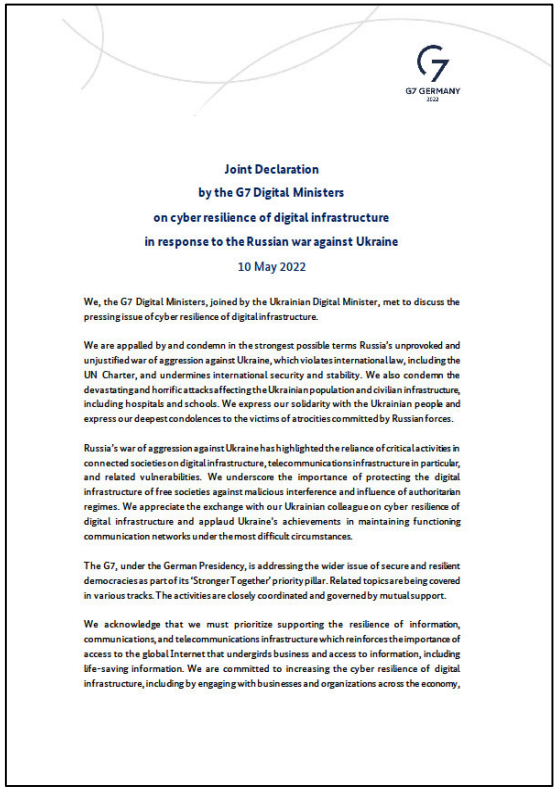
○ 「ともに更に強く（Stronger Together）」をテーマに、偽情報、違法・有害コンテンツ等に関するオンラインの安全性及び信頼性のある自由なデータ流通（DFFT）など、デジタル経済に関する議題について大臣間で議論するとともに、ウクライナの現状について、サイバーレジリエンスに関する観点から議論が行われた。

○ 最終的に、「ウクライナに対するロシアの戦争への対応におけるデジタルインフラのサイバー・レジリエンスに関するG7デジタル大臣共同宣言」及び「G7デジタル大臣会合宣言」が採択された。

※出席：G7構成国（日本からは牧島デジタル大臣、佐々木総務審議官等）、EU、ウクライナ（招待国）、OECD事務次長

「ウクライナに対するロシアの戦争への対応における デジタルインフラのサイバー・レジリエンスに関するG7デジタル大臣による共同宣言」

（令和4年5月10日）



G7 GERMANY 2022

Joint Declaration
by the G7 Digital Ministers
on cyber resilience of digital infrastructure
in response to the Russian war against Ukraine

10 May 2022

We, the G7 Digital Ministers, joined by the Ukrainian Digital Minister, met to discuss the pressing issue of cyber resilience of digital infrastructure.

We are appalled by and condemn in the strongest possible terms Russia's unprovoked and unjustified war of aggression against Ukraine, which violates international law, including the UN Charter, and undermines international security and stability. We also condemn the devastating and horrific attacks affecting the Ukrainian population and civilian infrastructure, including hospitals and schools. We express our solidarity with the Ukrainian people and express our deepest condolences to the victims of atrocities committed by Russian forces.

Russia's war of aggression against Ukraine has highlighted the reliance of critical activities in connected societies on digital infrastructure, telecommunications infrastructure in particular, and related vulnerabilities. We underscore the importance of protecting the digital infrastructure of free societies against malicious interference and influence of authoritarian regimes. We appreciate the exchange with our Ukrainian colleague on cyber resilience of digital infrastructure and applaud Ukraine's achievements in maintaining functioning communication networks under the most difficult circumstances.

The G7, under the German Presidency, is addressing the wider issue of secure and resilient democracies as part of its 'Stronger Together' priority pillar. Related topics are being covered in various tracks. The activities are closely coordinated and governed by mutual support.

We acknowledge that we must prioritize supporting the resilience of information, communications, and telecommunications infrastructure which reinforces the importance of access to the global Internet that undergirds business and access to information, including life-saving information. We are committed to increasing the cyber resilience of digital infrastructure, including by engaging with businesses and organizations across the economy,

（概要）

- ロシアのウクライナ侵攻に対する非難及びウクライナ大臣に対する情報交換への感謝、戦時下のウクライナの通信ネットワーク機能の維持への賞賛
- 情報、通信及び電気通信インフラの強靱性の支援を優先しなければならないことを認識
- 既存のサイバーセキュリティ及び国家安全保障の枠組みに沿った協調的なサイバー対応の強化へのコミットメント
- 2022年3月24日のG7首脳声明に沿って、ウクライナがサイバーインシデントに対し、そのネットワークを守ることを支援する取組を継続することへのコミットメント