資料3

NISC

National center of Incident readiness and Strategy for Cybersecurity

サイバーセキュリティ協議会について

サイバーセキュリティ分野における
従来の枠を超えた
情報共有・連携体制の構築

（検討中の案）

内閣官房 内閣サイバーセキュリティセンター
基本戦略第２グループ
平成31年１月17日

サイバーセキュリティに関する情報共有の効果とその重要性（単独で行う対策の限界）

- サイバーセキュリティの確保は、本来、各組織が自主的に取り組むべきもの
- しかし、サイバー攻撃の複雑化、巧妙化により、被害組織（被害組織から相談を受けるセキュリティベンダ・専門機関等を含む）が単独で有効な分析を行い、確証をもって効果的な対策を迅速に講じることに限界が生じてきている
- また、被害組織等から他の組織へ迅速な情報共有が行われなければ、攻撃手口や対策手法等を他組織が知ることができず、同様の手口によるサイバー攻撃の被害がいたずらに拡大するおそれ

個社単独での対策の限界

情報共有の効果

（参考）　既存の情報共有体制の具体例

○現在、NISCをはじめとする政府機関や民間において、以下のような情報共有体制が活動している（代表的なものを紹介）。

- 早期警戒情報の提供システム「CISTA」（JPCERT/CC）

  ※CISTA：Collective Intelligence Station for Trusted Advocates

- 「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づく情報共有体制（NISC)
- サイバー情報共有イニシアティブ「J-CSIP」（IPA)

  ※J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan

- 日本サイバー犯罪対策センター（JC3）による情報共有
- ICT-ISAC、金融ISAC、電力ISAC 等（民間事業者）

  ※ISAC：Information Sharing and Analysis Center

（参考）　ランサムウェア「WannaCry」（ワナクライ）事案

事案の概要

平成29年５月、政府機関や病院、銀行、大手企業等のコンピュータが、マイクロソフト製品の脆弱性を悪用したランサムウェア（身代金要求型の不正プログラム）「WannaCry」（ワナクライ）に感染

海外：約**150カ国**以上で感染。英国の病院では**診療・手術の中止**等、業務に支障を及ぼす被害が発生

日本：**自治体、鉄道、病院といった重要な機関**を含む幅広い分野において被害が発生

H29.3月 ≫ H29.4月 ≫ H29.5月

3/15
Microsoft製品の脆弱性修正プログラム公開

5/12(金)
Ａ社
システム異常発生

5/13(土)
Ａ社 対策チーム立ち上げ、状況把握開始

5/15(月)
Ａ社がサイバー攻撃を受けた旨報道

5/15 (月)
B市、C市、D社にて感染確認

5/16 (火)
E社感染確認

5/17 (水)
Ａ社 復旧・ニュースリリース

当時、被害拡大を防ぐために迅速な共有が必要であった情報は何か

◆修正プログラム未適用のPCは、起動した瞬間にネットワーク経由で感染し、ロックされるおそれ
→各職員は出勤後、不用意にPCを起動してはならない。

この旨を、国内の各組織に、（職員出勤時刻までに）一刻も早く周知する必要があった。

しかし、

当時の被害企業にとっての情報提供リスク

- 個社単独では自らの分析内容に確証が持てない状況
- 情報提供先の他組織で秘密の保持が十分に担保されていない

⇒ 情報提供の結果、誤った情報が世間に漏れることで、
- **責任追及を受けるリスク**
- **風評被害を受けるリスク**

情報共有体制に関する課題とその解決方法
➡「デメリットの除去」と「メリットの増加」が重要

事業者等が直面する課題

- 信頼できる者以外には情報を出せない
- 提供した情報が適切に取り扱われず、提供者名等が漏れてしまうおそれ
- 機微な情報を法的根拠なく提供すると、他法に抵触するおそれ

デメリットの除去

- **共有相手を選択**できるしくみ
- 罰則により担保された **守秘義務（法律事項）**
- 法律に規定された **情報提供義務（法律事項）**

P5

事業者等が直面する課題

- 情報を提供しても、それに対するフィードバックがない
- こちらから情報を出すばかりでは不公平である

メリットの増加

- 提供した情報に対する **フィードバックを得られる**仕組み
- 「ただ乗り」を防止し、**ギブアンドテイク**の情報共有

P6

デメリットの除去について
～（法律事項）サイバーセキュリティ基本法の一部を改正する法律～

（平成30年法律第91号）

趣旨

・サイバーセキュリティに対する脅威が一層深刻化する中、官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策の推進に係る協議を行うための**協議会を創設。**
・**構成員に対して守秘義務及び情報提供義務を適用する**等の措置を講ずる。

○情報共有のデメリット除去のために必要な規定を措置

1　罰則（※）により担保された**守秘義務**　※１年以下の懲役又は50万円以下の罰金

2　法律に規定された**情報提供義務**

◆　施行時期は2019年４月を想定。

◆　運用システムはJPCERT/CCの早期警戒情報提供システム 「CISTA」を活用予定。

メリットの増加について　～「ギブアンドテイク」による情報共有～

背景	法改正による**デメリット除去は不可欠**だが、 それだけでは情報提供を促進する**インセンティブにならない**ため、 情報提供を行う**メリットを増加させることも重要**
解決策	提供者の**モチベーション**と提供される**情報の質**を維持するため、 積極的な情報提供に**能力**と**意欲**を有する者を、一般の構成員と別に、 特別貢献構成員（仮称）としてグループ化
特別貢献構成員（仮称）のメリット	○　提供した未確定の情報に対して**相互にフィードバックを行う**ことで、**提供した情報の確度を高めることができる**。 ○　各主体がフィードバックだけでなく、自らも積極的に情報を提供する**ギブアンドテイクの原則を徹底**することで、**特別貢献構成員のみに共有される情報を得ることができる**。

サイバーセキュリティ協議会

※改正法中、「協議会の組織及び運営に関し必要な事項は協議会が定める」としており、今後、協議会の規約で整備予定。

構成員の役割

特別貢献構成員（仮称）

未確定の情報を
相互にフィードバックを行い、
速やかに対策情報等を作出する
※専門機関、セキュリティベンダ等

対策情報等の情報提供

一般の構成員

基本的に、
作出された対策情報等を受領し、
自らの組織の対策に役立てる
※国の行政機関、地方公共団体、重要社会基盤事業者等

一般の構成員のメリット　守秘義務が強く担保された協議会の枠組みの下で、特別貢献構成員等に対し、安心して相談することができる。

協議会における対策情報等の作出及び共有の流れの全体像

○ 一部の専門機関・セキュリティ事業者からは、守秘義務等が法律で規定されたことに加え、協議会の運営にあたって特別貢献構成員（仮称）同士の未確定情報の相互交換が公正に行われれば、協議会における情報共有活動が更に活発化する、といった期待の声が挙がっているところ。

○ また、一部の重要社会基盤事業者等からは、自社で事案発生の疑いが生じた際に、守秘義務が強く担保された協議会に対しては、ダイレクトに、気兼ねなく安心して連絡、相談することができる、といった期待の声が挙がっているところ。

○ いずれにせよ、具体的な運用の詳細については、引き続き関係者等の意見を踏まえつつ慎重に検討を進める予定。

その他運用における留意事項

1　他の情報共有体制との連携（参加者の事務負担増への配慮）

重要インフラ事業者等、複数の情報共有体制に参加する主体に、重複作業の発生等による事務負担をおかけすることがないよう、他の情報共有体制との間で必要な連携を協議していく予定。

2　リアルタイムでの情報共有の追求

できるだけリアルタイムでの情報共有を実現する観点から、協議会は逐一対面で集まるのではなく、システムを通じて行っていく予定。

3　発足当初は、G20等に万全を期す観点から優先度の高い主体に対し、参加を働きかけ

協議会の発足時点（2019年４月を予定）における構成員については、同年6月のG20等に万全を期す観点から優先度の高い主体に対し働きかけを行うこととし、発足後、協議会の実際の運営状況等を踏まえつつ、2020年東京大会等に万全を期す観点から漸次拡大していくこととする予定。

（理由）

（1）　12月の法案成立後まだ間もないところであり、具体的な運営ルールに関する各関係主体との協議は、各主体から寄せられたご意見等を丁寧に踏まえつつ、今後、十分な時間的余裕をもって慎重かつ誠実に進める必要があること

（2）　協議会の運営について十分な経験の蓄積がない段階で多くの主体が一斉に参加することとなると、各主体が機微な情報を出しづらくなったり、現場が混乱したりするおそれがあること