被害報告一元化の方針

サイバーセキュリティ戦略本部第43回会合　資料

侵害発生 ― 原因究明

DDoS攻撃・ランサムウェア事案

サイバー攻撃であることは最初から明白

インフラ機能等の停止
情報窃取

- ✓ **サイバー新法**
- ✓ **インフラ業法**
- ✓ **個人情報保護法**
- ✓ **警察への相談**

- **様式の統一を先行実施**
- 新法の報告義務施行後、システム整備により共通様式の**窓口を一元化**

初動対応中の報告となり、件数も多いことから、被害組織の負担が極めて大きい

潜伏型サイバー攻撃

※インフラ機能等の停止を伴う場合

（潜伏型攻撃）

インフラ機能等の停止

- ✓ **インフラ業法**

一定の調査後、サイバー攻撃であることが判明

- ✓ **サイバー新法（NISC）**
- ✓ **サイバー新法（所管省庁）**
- ✓ **警察への相談**

※情報窃取を伴う場合

（潜伏型攻撃）

（情報窃取）

一定の事案調査が行われた上での報告であり、比較的、時間的余裕はある状態

システム監視や調査等により、サイバー攻撃と情報窃取を認知

- ✓ **サイバー新法**
- ✓ **個人情報保護法**
- ✓ **警察への相談**

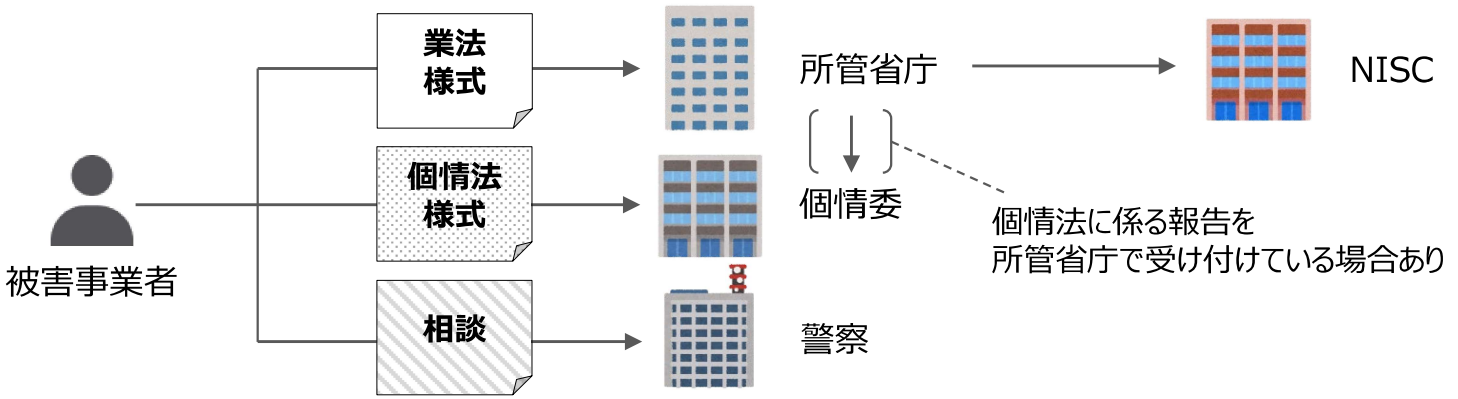
- システム整備により、新法の報告窓口を一本化。関係省庁への共有も可能に。

※報告を踏まえ、関係省庁は、業法等に基づく調査等を実施。

被害報告一元化の実現に向けたタイムライン

現状

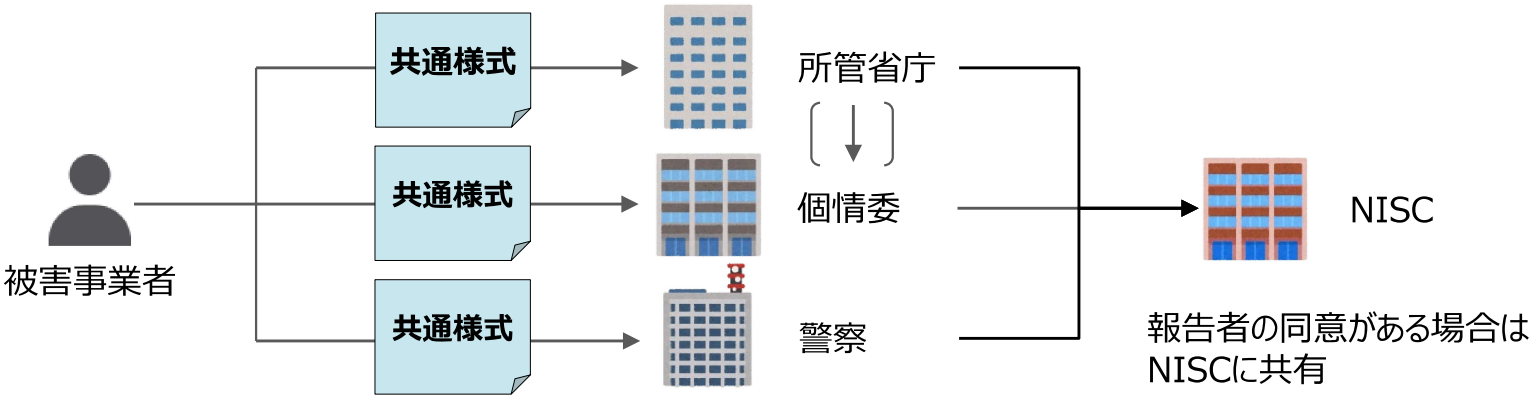
関係政府機関に対して、
個別の様式で
それぞれ報告等を行う必要



DDoS攻撃・ランサムウェア
報告様式の統一

（周知期間等を経て
本年10月1日から実施）

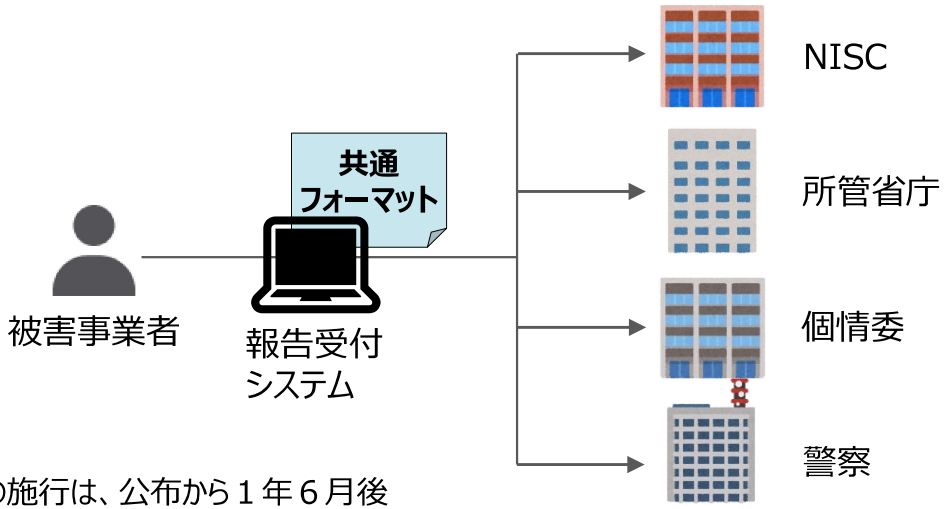
DDoS攻撃・ランサム事案発生時の
関係省庁への**報告様式を統一**



報告窓口の一元化

（システム整備を進め
新法の報告義務施行に併せ実施）

システムを活用し、
新法の報告窓口を一本化。
関係省庁への共有も可能に。



※　報告義務の施行は、公布から１年６月後