

1. 事案の状況と本部及びNISCの対応



□ 5月8日(金)(検知・通知1)

- ◇ NISCは、厚生労働省(以下「厚労省」という。)ネットワークにおいて不審な通信を検知し、厚労省政策統括官付情報政策担当参事官室(以下「情参室」という。)に対してその旨を通知した。
- ◇ NISCは、厚労省情参室から不審な通信をした端末を特定し、LANケーブルの抜線を行った旨の連絡を受け、その後、同日中に不審な通信を検知しなくなったことを確認した。(以降、厚労省情参室に対し、随時、助言等を実施。)

□ 5月15日(金)(解析結果提供A)

- ◇ NISCは、厚労省情参室から5月8日に受信した不審メールⅠに関する不正プログラムを受領後、解析を実施し、同日中に解析結果を厚労省情参室へ提供した。

□ 5月19日(火)(解析結果提供B)

- ◇ NISCは、厚労省情参室から5月18日に受信した2種類の不審メール(不審メールⅡ、不審メールⅢ)及び不正プログラムを受領後、解析を実施し、同日中に解析結果を厚労省情参室へ提供した。

□ 5月21日(木)(解析結果提供C)

- ◇ NISCは、厚労省情参室から5月20日に受信した不審メールⅣ及び不正プログラムを受領後、解析を実施し、同日中に解析結果を厚労省情参室へ提供した。

□ 5月22日(金)(検知・通知2)

- ◇ NISCは、厚労省ネットワークにおいて不審な通信を検知し、厚労省情参室に対してその旨通知した。
- ◇ NISCは、厚労省情参室から、機構において、不審な通信をした端末のLANケーブルの抜線を行った旨の連絡を受け、その後、同日中に不審な通信を検知しなくなったことを確認した。

□ 5月29日(金)

- ◇ NISCは、厚労省から、5月8日以降の経緯について5月19日に機構が警察へ相談したこと及び機構において情報流出が生じた旨の説明を受け、サイバーセキュリティ戦略本部長(官房長官)(以下「本部長」という。)に報告した。
- ◇ 本部長は、NISCから報告を受け、即時に「特定重大事象」^{注1}であるとの判断を行った。
- ◇ NISCは、厚労省の要請を受けて、厚労省と機構が行う対応を支援するため、CYMAT^{注2}を派遣した。

□ 6月1日(月)

- ◇ NISCは、客観的・専門的立場から原因究明を実施するため、原因究明調査チームを設置した。
- ◇ 本部長は、サイバーセキュリティ基本法第30条第2項の規定に基づき、機構を監督する立場にある厚生労働大臣に対して、厚労省が機構に対して行ってきたサイバーセキュリティに関する監督に関する資料、情報の提供を要請した。
- ◇ 内閣官房副長官(事務)を議長とするサイバーセキュリティ対策推進会議を開催し、全府省庁に対して、システム点検と個人情報の適正管理を指示した。

注1:「サイバーセキュリティ戦略本部重大事象施策評価規則」(平成27年2月サイバーセキュリティ戦略本部決定)において、①国の行政機関が運用する情報システムにおける障害を伴う事象であつて、行政事務の遂行に著しい支障を及ぼし、又は及ぼすおそれがあるもの、②情報の漏えいを伴う事象であつて、国民生活又は社会経済に重大な影響を与え、又は与えるおそれがあるもの等の事象をいう。

注2:情報セキュリティ緊急支援チーム(通称CYMAT:CYber Incident Mobile Assistance Team)