NISC National center of Incident readiness and Strategy for Cybersecurity

日本年金機構における個人情報流出事案に関する原因究明調査結果（概要）

平成２７年８月２０日

サイバーセキュリティ戦略本部

原因究明調査結果の構成

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って、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って、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)

2. 事案に関する技術的検討(その1)

□ 原因究明調査により判明した事項①(ネットワーク構成の確認等)

◆ 機構のネットワークは、情報系からプロキシサーバを経由しての外部通信以外の外部通信が遮断される設定。したがって、攻撃者による外部との不審な通信については、プロキシサーバにその履歴が残る(プロキシログの解析結果は次頁参照)。

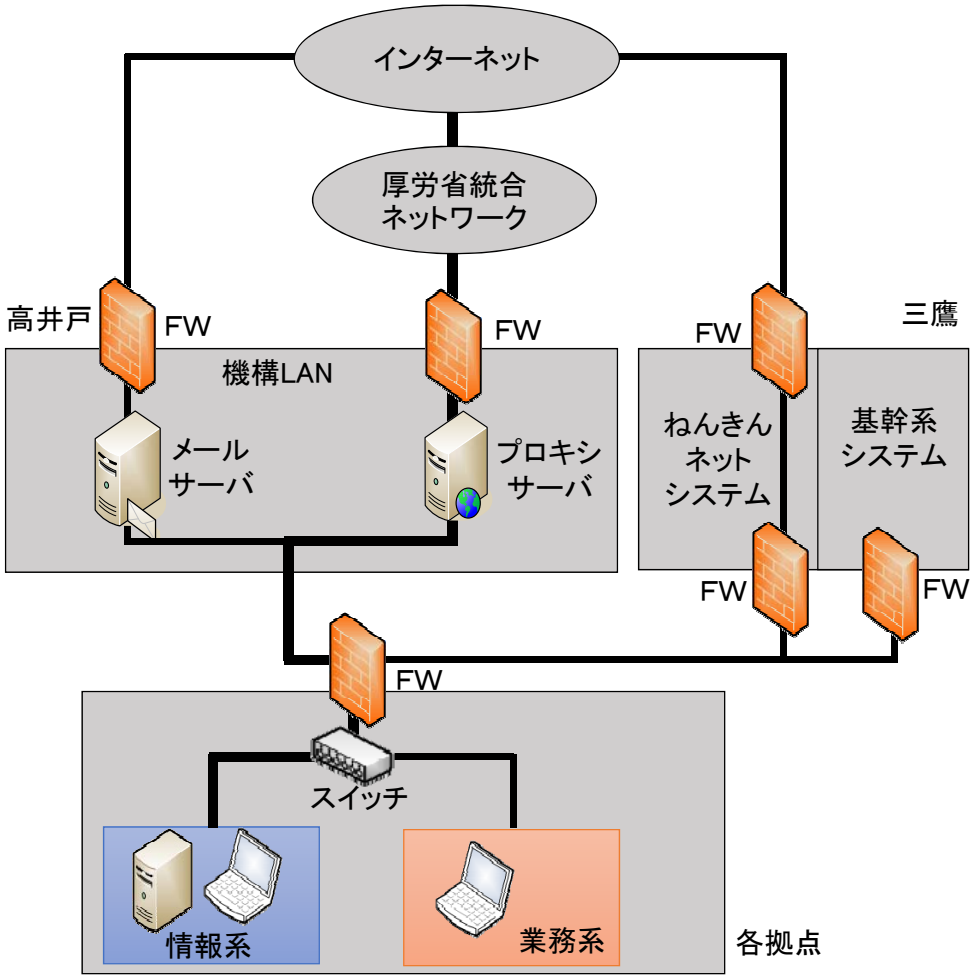
・業務系端末からの外部通信について

業務系端末から厚労省統合ネットワーク経由の外部通信は、スイッチ及びファイアウォールにより遮断される設定となっていることをシステム運用業者の説明と資料により確認。また、現地において、NISC職員が説明どおりの設定となっていることを直接確認。

プロキシサーバに、業務系端末からの外部通信に関する履歴なし。

・メール用回線等を通じた外部通信について

メール用回線及びねんきんネットシステム経由のWebアクセスは、スイッチ及びファイアウォールにより遮断される設定となっていることをシステム運用業者の説明と資料により確認。また、現地において、NISC職員が説明どおりの設定となっていることを直接確認。



2. 事案に関する技術的検討(その2)

□ 原因究明調査により判明した事項②(プロキシログの解析、不審メールとの突合等)

◆ プロキシログの解析により、不審な通信先23件、不審な通信を行った端末31台を特定、不審メールと突合。

不審メールの番号	受信日	不審メールの概要	発生した不審な通信
Ⅰ	5月8日(金)	件名:「厚生年金基金制度の見直しについて(試案)に関する意見」 宛先:公開メールアドレス(2) リンク:商用オンラインストレージ	端末1台が不正プログラムに感染、不審な通信が発生。約4時間後に端末の通信ケーブルを抜線、その後は不審な通信なし。
Ⅱ	5月18日(月)	件名:給付研究委員会オープンセミナーのご案内 宛先:非公開の個人メールアドレス(98) 添付ファイル:給付研究委員会オープンセミナーのご案内.lzh	端末3台が不正プログラムに感染、不審な通信が発生するも接続先への通信は失敗。
Ⅲ	5月18日(月) ～ 5月19日(火)	件名:厚生年金徴収関係研修資料 宛先:非公開の個人メールアドレス(20) 添付ファイル:厚生年金徴収関係研修資料(150331厚生年金徴収支援G).lzh (16) リンク:商用オンラインストレージ(4)	不審な通信は発生せず。
Ⅳ	5月20日(水)	件名:【医療費通知】 宛先:公開メールアドレス(3) 添付ファイル:医療費通知のお知らせ.lzh	20日午後、端末1台が不正プログラムに感染、不審な通信が発生。数時間以内に、他の6台の端末からも不審な通信が発生。 21日から23日にかけて、合計21台の端末から国内のサーバ(接続先X)への多数の通信。

◆ NISCでは、不審メールⅡ及び不審メールⅢに関する解析結果を5月19日夜に、不審メールⅣに関する解析結果を5月21日夕刻に、それぞれ厚労省情参室に提供しているが、これらの解析結果には不正プログラムの接続先に関する情報が含まれていた。

◆ 5月22日にNISCにおいて不審な通信を検知し厚労省に通知した後、機構による調査の過程で接続先Xへの多数の通信が判明した。

3. CSIRT（情報セキュリティインシデント対応チーム）の運用等に関する検討

	NISC	厚労省	年金機構
インシデント対処	● 政府統一基準(注1)では、インシデントを認知したときに、CISO(注2) やNISCに報告することを定めている。 ● 統一基準では、インシデント発生時に、CISOやNISC等への連絡のため、各府省庁において報告窓口を含む報告・対処手順を整備することとしている。	● 厚労省の情報セキュリティポリシーでは、インシデントを認知したときに、CISOやNISCに報告する旨定めている。 ● 厚労省は、報告・対処手順を整備しているが、今回のインシデントにおいて、GSOC(注3)から連絡を受けた担当窓口から、厚労省の責任者（CISO、課長等の幹部）に報告が上がっていなかった。	● 機構のセキュリティポリシーにおいて、インシデント対処の必要性を規定し、その具体化はリスク管理一般の規程等に委ねている。 ● 当該規程において、リスクの定義、導入、運用、分析・評価、見直し等の枠組みが規定されているものの、サイバー攻撃を想定した具体的な対応が明確化されていない。
CSIRT(注4)体制	● 政府統一基準では、CSIRTに属する職員については、「専門的な知識又は適性を有すると認められる者を選任すること」と定めている。 ● CSIRTに属する職員の選任は、各府省庁が統一基準の規定に従うこととされている。	● 厚労省のポリシーでは、CSIRTに属する職員について、「CISO、情報政策担当参事官、当該事案に係る部局の総括的な課長及び担当課室長等、CISOアドバイザを充てる」と定めている。 ● CSIRTの構成員が課室長等以上であり、実働要員（課長補佐以下の職員）が選任・指名されていなかった。	● 特殊法人である機構は、政府統一基準の直接の適用対象ではない。 ● CSIRT体制は定めておらず、セキュリティポリシーや諸規程にもその定めはない。（機構によると、平成27年7月10日からCSIRT体制の構築の検討を開始。）
個人情報を取り扱うシステムの整備等	● 「ガイドライン」(注5)において、標的型攻撃に対する多重防御の取組は、外交・安全保障等に加え「個人にもたらされる被害」も対象としている。	● 厚労省統合ネットワークにおける標的型攻撃に対する多重防御の取組を進めていたが、機構の情報系ネットワークは、「ガイドライン」の取組の対象としておらず、標的型攻撃に対する多重防御の取組が十分でなかった。	● インターネットに接続していない業務系からインターネットに接続をしている情報系に個人情報を移して取り扱っていた。

(注1)「政府機関の情報セキュリティ対策のための統一基準」(平成26年5月　情報セキュリティ政策会議決定)
(注2) Chief Information Security Officer :最高情報セキュリティ責任者
(注3) Government Security Operation Coordination team:政府機関情報セキュリティ横断監視・即応調整チーム
(注4) Computer Security Incident Response Team:コンピュータシステムやネットワークに保安上の問題に繋がる事象が発生した際に対応する組織
(注5)「高度サイバー攻撃対処のためのリスク評価等のガイドライン」（平成26年6月25日　情報セキュリティ対策推進会議）

4. 今回のサイバー攻撃の特徴と対策

□ 標的型攻撃の特徴

- 標的型攻撃は巧妙化しており、使われるメールも見分けが困難。
  →メール開封を前提とした対策が必要。
- 攻撃者は乗っ取った端末を足掛かりとして、侵入を拡大させる。
  →初期段階での認知・対処、侵入範囲を拡大させないためのシステム設計・構築・運用が重要。

□ 標的型攻撃に対する情報システム防御策等の考え方

自組織の情報・システム・業務を守る目的・対策について考え、職務・職責に応じて実施することが求められる。

［検討対策例］

◆ システム防御策

- メールに添付された実行形式のファイルを取り込まない・起動できないようにシステム設定。
- 既知の脆弱性を放置しないようにアップデート等を行う。脆弱性診断を実施。ウェブラウザの拡張機能の必要最小限の使用。
- 侵入範囲が拡大しにくいように設定・運用。
- 業務・情報の性質等に応じて重要な情報に攻撃が到達しないよう、システム分離。
- システム分離したときに各システムで扱える情報・できない情報につきルール化し、職員に徹底。
- ローカル管理者権限のパスワードを共通とする範囲の最小限化。
- 不要な管理アカウントの確実な消去。
- 内部ネットワークにおける異常を検知する仕組みの整備。　　等

◆ インシデント対策に係る対策

- 不審メールの受信（不正プログラム動作の可能性）につき攻撃者が繰り返して攻撃を試みるものとして継続的に対応。
- システム構築・運用事業者とは独立した専門性の高い事業者への依頼等、平素からの準備。
- CISO等権限を有する者の下でのインシデント対応。

5. 本部及びNISCがとるべき再発防止対策

各府省庁への情報提供が有効に機能するための対策

- NISCは、不審な通信検知後、速やかに分析を行い、インシデントの疑いのあるものは当該省庁に対して通知等を行っているが、通知や提供する不正プログラムの解析結果の重要性を当該省庁が理解し、迅速に適切な措置が取られることを前提としている。
- 今回の事案の教訓を踏まえれば、今後は、平素から各府省庁に対して、標的型攻撃を含むサイバー攻撃の本質と影響、NISCからの検知通知や不審メール等の解析結果の活用方法、対処方法等について研修や演習の機会を提供していく必要がある。
- 研修や演習の対象は、情報システム部局のみならず、独立行政法人、特殊法人等を所管する部局の幹部も対象として含めねばならない。本部は、その実施状況を年次報告等において評価し国民に説明していくことが重要である。

インシデントに備えた体制の強化

- 各府省庁においては、政府統一基準等に従って、CISOの指示の下、専門的な知識又は適正を有すると認められる者を選任したCSIRTを整備し、平素から要員の事案対処能力、経験の向上を図り、実践できるようにしておくことが求められている。
- NISCは、各府省庁のCSIRTが、事案発生時に実働する体制が整備・強化されるよう、事案の対応についての演習・訓練等の機会を設け、また、本部は、各府省庁において適切に体制整備がされ、実践のための必要な取組がなされているか等についても監査の対象とするなど、PDCAサイクルに基づく着実な取組を確保していく。
- 本部及びNISCは、政府統一基準等の見直しを行い、サイバーセキュリティ対策の向上を図る。

標的型攻撃のリスクを踏まえたシステムの構築、維持、運用の強化対策

- 本部及びNISCは、標的型攻撃への対処について、政府統一基準の他、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」を取りまとめ、その実施を推進してきたが、その適用範囲は、国の行政機関としている。
- 今後は、大量の個人情報を取り扱うリスクの高いシステムにおいても、サイバー攻撃のリスクを踏まえたシステムの構築、維持、運用がなされるよう、各府省庁に対し多重防御の取組を加速化すべく次のような取組を促すよう対策を講じていく。
  - リスクを考慮したシステム構築を行うための基準の改善（適用範囲の拡大を含む。）
  - システムの維持運用を確実にする監査の強化
  - 特に技術的な事項について、外部から起用するCIO補佐官、CISOアドバイザーの積極的な活用
- 併せて、GSOC機能について、攻撃の手法が時々刻々巧妙化していることを踏まえ、不断の見直しを行っていく必要がある。

本文書は、NISCの対処能力を推知しうる情報が含まれるが、発生した事案の重大性に鑑み、可能な限り実態解明のための情報開示を行い、説明責任を果たす観点から取りまとめたものである。