資料１

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（案）

資料１－１　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（案）（概要）

資料１－２　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（案）

資料１－１

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（案）（概要）

平成２７年８月２０日

サイバーセキュリティ戦略本部

1. 原因究明調査結果の構成

2. 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)

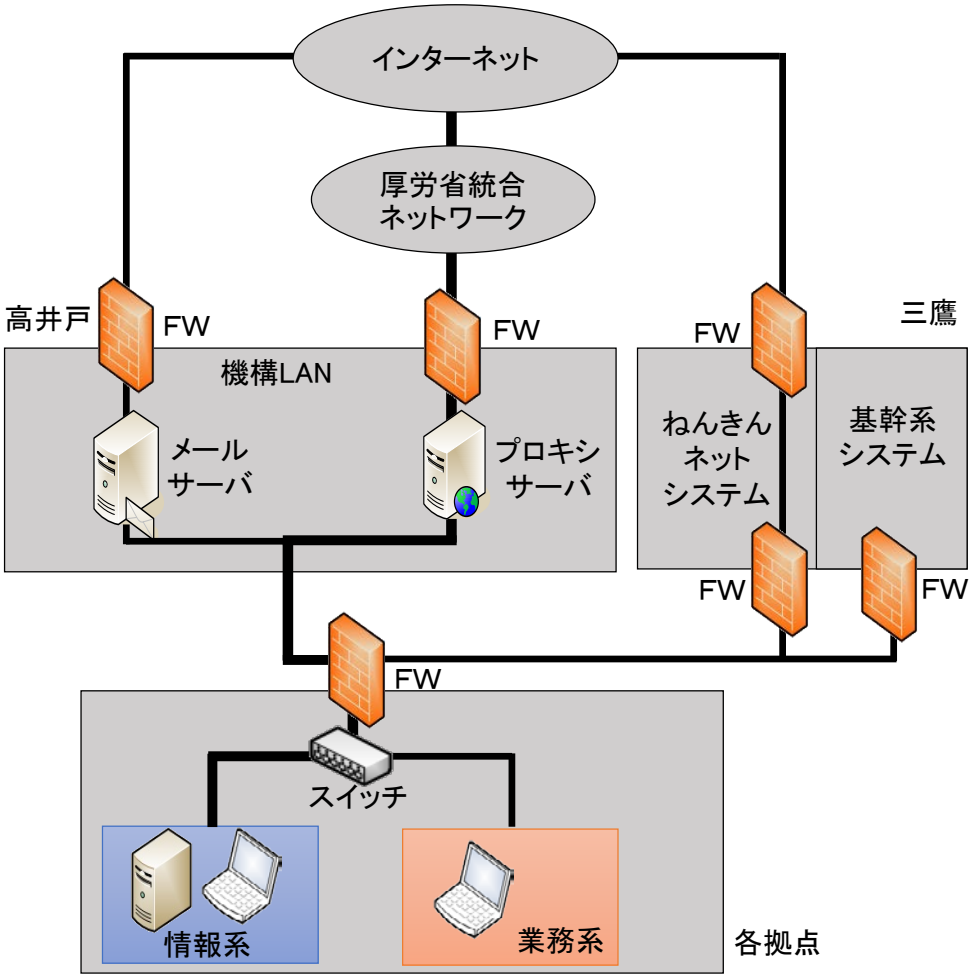
3. 事案に関する技術的検討(その1)

□ 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。



3. 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。

4. 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）

5. 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。

6. 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。

資料１－２

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
（案）

平成２７年８月２０日

サイバーセキュリティ戦略本部

目次

はじめに

平成 27 年 6 月 1 日、日本年金機構(以下「機構」という。）は、外部から送付された不審メールに起因する不正アクセスにより、機構が保有している個人情報の一部 （約 125 万件）が外部に流出したことが 5 月 28 日に判明したとして、報道発表を行った。

特定の政府機関、企業を狙ったいわゆる「標的型攻撃」が我が国において広く社会的に問題化したのは平成 23 年の衆議院事務局、三菱重工業等に対する標的型攻撃に端を発しており、年々増加の傾向にある。そして、今般の機構事案は、個人情報が大量に流出したことが現実に確認された初めてのものである。

我が国のサイバーセキュリティの確保に関しては、サイバーセキュリティ基本法の全面施行に伴い、平成 27 年 1 月、サイバーセキュリティ戦略本部(以下「本部」という。）及び内閣官房内閣サイバーセキュリティセンター（以下「NISC」という。）がサイバーセキュリティに関する政策及び事案対応の司令塔機能を担うべく発足したところである。本部は、政府機関におけるサイバーセキュリティ対策のための統一基準を定め、各府省庁は、統一基準を参考としながら、当該府省庁の特性を踏まえたセキュリティポリシーを策定・運用するとともに、セキュリティ対策を実施するための組織・体制の整備等を行い、セキュリティ対策を総合的に推進することとされている。

本文書は、政府機関のサイバーセキュリティ確保体制において、なぜ今回のように大量の個人情報が流出する結果となったのかについて調査を行い、本事案に係るデータを解析した結果を基に、本部及び NISC がこれまで行ってきた政府機関に対するサイバーセキュリティ対策上の課題を明らかにするとともに、その課題を踏まえ、政府として速やかに所要の改善措置を講じることにより、政府機関全体のサイバーセキュリティの向上を図ることを目的とする。あわせて、調査を通じて得られた教訓を明らかにすることにより、政府機関のみならず、我が国の企業や個人における標的型攻撃対策の強化等、サイバーセキュリティの更なる能力向上のための参考に供することを企図しているものである。

なお、本文書は、サイバーセキュリティ基本法第 25 条第 1 項第 3 号に規定された「国の行政機関で発生したサイバーセキュリティに関する重大な事象に対する施策の評価(原因究明のための調査を含む。)」に基づくものである。また、本文書には、NISC の対処能力を推知しうる情報が含まれるが、今般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。

1. 事案の状況と本部及びNISCの対応

最初に、今回の事案に関する本部及びNISCの対応を時系列で示す。

○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「厚労省情参室」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。)

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[1]を受領したが、メール本文中のリンク先である商用オンラインストレージ[2]から不正プログラムは削除されていた。

○5月15日(金)(解析結果提供A)

NISCは、厚労省情参室から不審メール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。

---

[1] 不審メールI～Ⅳの概要については、「表 1 不審メールの整理」(7ページ)参照。

[2] 顧客に対し、インターネット上のサーバの領域をデータ保管用に提供するサービスをいう。

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」[3]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[4]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。

また、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[5]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[6]。

さらに、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。

---

[3] 「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 10 日 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。

[4] 情報セキュリティ緊急支援チーム(通称 CYMAT: CYber incident Mobile Assistance Team)

[5] 関係行政機関の長は、本部長の求めに応じて、本部に対し、本部の所掌事務の遂行に必要なサイバーセキュリティに関する資料又は情報の提供及び説明その他必要な協力を行わなければならない。

[6] 日本年金機構が平成 27 年 6 月 1 日付けで公表した情報流出事案に関し、厚生労働省が同機構に対して行った、サイバーセキュリティに関する監督に関する資料又は情報の提供(閣サ第 386 号、平成 27 年 6 月 1 日)

2. 事案に関する技術的検討

本事案に対して NISC で実施した原因究明調査のうち、技術的調査により判明した事項について述べる。

2.1. ネットワーク構成の確認等

2.1.1 ネットワーク構成の確認

技術的調査に当たり、関係資料等により機構のネットワーク構成について確認した結果を「図 1 日本年金機構のネットワーク構成(概要)」に示す。

インターネットへの Web アクセス(以下「外部通信」という。) を行う情報系と、個人情報を管理している基幹系システムと接続され外部通信を行わない業務系が存在する。また、インターネットと接続するための回線として、厚労省統合ネットワーク経由の回線のほか、メール送受信専用外部回線及びねんきんネットシステム専用外部回線が存在する。

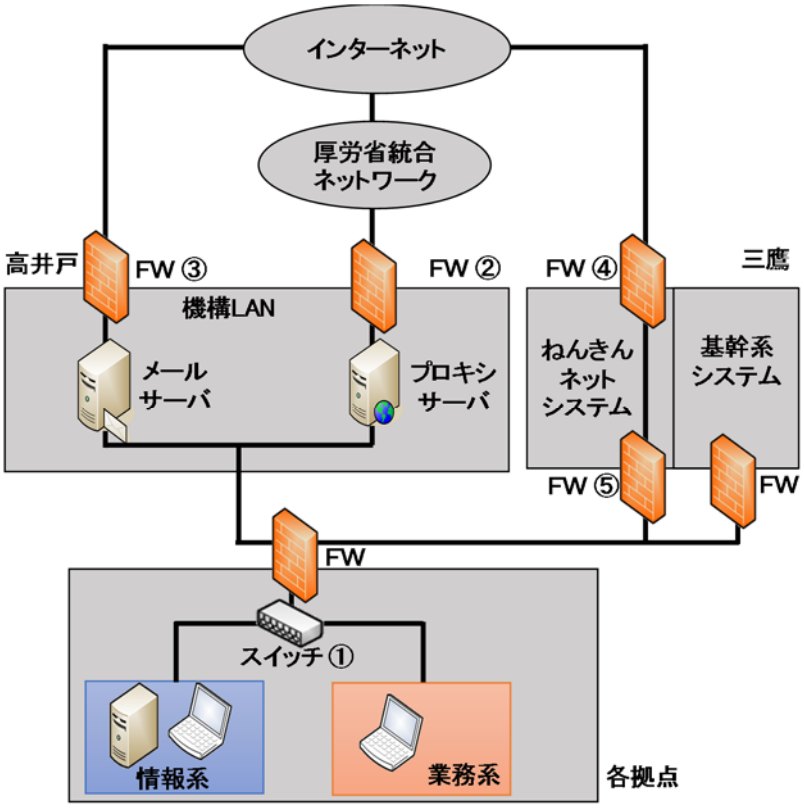


図 1 日本年金機構のネットワーク構成(概要)

2.1.2 外部通信に関する設定の確認

機構からの外部通信は、情報系からプロキシサーバを経由して行われるのが通常であるが、それ以外の外部通信が攻撃者によって行われた可能性も考えられる。このため、ネットワーク設定の確認を行い、その結果、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ことを確認した。

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と考えられる。

ネットワーク設定については、システム運用業者の説明及び資料により確認するとともに、NISC 職員が現地において直接確認した。その詳細は、以下のとおりである。

⑴ 業務系からのプロキシサーバ経由の外部通信

業務系からのプロキシサーバ経由の外部通信については、各拠点のスイッチ(①)及び厚労省統合ネットワークのファイアウォール(②)において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及び資料並びに NISC 職員の現地調査により確認した。

なお、プロキシサーバには業務系端末からの外部通信に関する履歴はなかった。

⑵ メール送受信専用外部回線経由の外部通信

情報系からのメール送受信専用外部回線経由の外部通信については、機構 LAN のファイアウォール(③)において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及び資料並びに NISC 職員の現地調査により確認した。

業務系からのメール送受信専用外部回線経由の外部通信については、各拠点のスイッチ(①)及び機構 LAN のファイアウォール(③)において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及び資料並びに NISC 職員の現地調査により確認した。

⑶ ねんきんネットシステム専用外部回線経由の外部通信

情報系からのねんきんネットシステム専用外部回線経由の外部通信については、各拠点のスイッチ(①)及びねんきんネットシステムのファイアウォール(④及び⑤)において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及び資料並びに NISC 職員の現地調査により確認した。

業務系からのねんきんネットシステム専用外部回線経由の外部通信については、ねんきんネットシステムのファイアウォール(④及び⑤)において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及び資料並びに NISC 職員の現地調査により確認した。

2.2. プロキシログの解析等

2.2.1 プロキシログの解析

一般に、サイバー攻撃によって情報が流出する場合、不正プログラムに感染した端末が外部の指令サーバに接続し、攻撃者からの指令の受け取り、別の不正プログラム

や攻撃ツールのダウンロード、集めた情報の送出等を行うため、当該指令サーバとの間で各種の不審な通信を行う。

そこで、不正プログラムへの感染による不審な通信を抽出するため、機構からプロキシサーバのログ(以下「プロキシログ」という。) を入手し解析を行った。

(1) 解析対象

5 月 8 日 00:00～6 月 4 日 20:32 のプロキシログ(ただし、5 月 10 日 20:01～23:58 のプロキシログは欠損[7])

(2) 解析結果

プロキシログに記録された全ての通信について、不審な通信の特徴の有無を調べ、23 件の不審な通信先(以下「接続先」という。) を抽出した。また、不正プログラムへの感染により不審な通信を行ったと考えられる端末(以下「感染端末」という。) 31 台[8]を特定した。

次に、感染端末と接続先との通信について、プロキシログに記録された各端末からの通信の履歴を接続先ごとに集計し 1 時間単位でグラフ化した(図　2　感染端末と不審な通信(9 ページ))。通信成功の履歴が記録されていた時間帯は接続先に応じて色分けして表し、通信失敗のみの履歴が記録されていた時間帯は灰色で表している。

なお、通信時間は必ずしも通信量と比例せず、不審な通信は必ずしも情報流出を意味しないことに留意が必要である。

2.2.2 不審メールとの突合等

(1) 不審メールの整理

機構から入手した不審メールを受信日、件名等をもとにⅠ～Ⅳに整理した結果を「表 1 不審メールの整理」に示す。

[7] 機構において 5 月 10 日にプロキシログの確認をした際に 5 月 10 日 20:00 までのログを保存し、その後、5 月 22 日に再度プロキシログの確認をした際に 5 月 10 日 23:58 以降のログを保存した結果、5 月 10 日 20:01～23:58 の欠損が発生した。

[8] 31 台のうち 6 台は不審な通信が全て失敗している。

表 1 不審メールの整理

不審メールの番号	受信日	不審メールの概要
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
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
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)
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

※ 表中の括弧内の数字はメールの件数を表す。

(2) 不審メールとの突合

プロキシログの解析結果と「表 1 不審メールの整理」で整理した不審メールとの突合作業を行い、各不審メールにより発生した不審な通信を確認した。

①不審メールⅠ

5 月 8 日、不審メールⅠの受信直後、端末 1 台から不審な通信が発生している。これは、不審メールⅠの本文中にあるリンク先に係る不正プログラムに感染したことが原因と考えられる。

また、不審な通信が発生してから約 4 時間後には、接続先への通信が止まっている。これは、NISC において不審な通信を検知した旨を厚労省情参室に通知後、機構において当該端末の LAN ケーブルを抜線したためと考えられる。

なお、不審メールⅠの受信から不審メールⅡの受信までの約 10 日間、この端末以外からの不審な通信は発生していない。

②不審メールⅡ

不審メールⅡの受信直後、端末 3 台から不審な通信が発生している。これは、不審メールⅡの添付ファイルに係る不正プログラムに感染したことが原因と考えられる

が、接続先への通信は失敗している[9]。

③不審メールⅢ

不審な通信は発生しておらず、不正プログラムに感染していないと考えられる。

④不審メールⅣ

5 月 20 日午後、不審メールⅣの受信直後、端末 1 台から不審な通信が発生している。これは、不審メールⅣの添付ファイルに係る不正プログラムに感染したことが原因と考えられる。また、不審メールⅣの受信後、数時間以内に、他の 6 台の端末からも不審な通信が発生している。

その後、5 月 21 日から 5 月 23 日にかけて、上記 7 台の感染端末のうち 2 台を含む計 21 台の端末から国内のサーバ(接続先 X)への多数の通信が発生しているが、警察庁からの情報提供により、接続先 X への通信は、約 125 万件の個人情報の流出に関する通信であったことが判明している。

なお、5 月 24 日以降、不審な通信は発生していない。

2.2.3 備考

(1) 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。

(2) 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) 警察庁からの情報提供により、不審な通信が成功している 3 つの接続先について、年金機構からの個人情報の流出が認められなかったことが判明している。なお、その他の接続先の中には、サーバの特定ができなくなっているものや、サーバが海外に所在するものが含まれている。

[9] 不審メールⅡの受信後不審メールⅢの受信までの間に、不審メールⅠと同じ件名のメールが非公開メールアドレスにおいて 1 件受信されているが、不審な通信は発生していない。

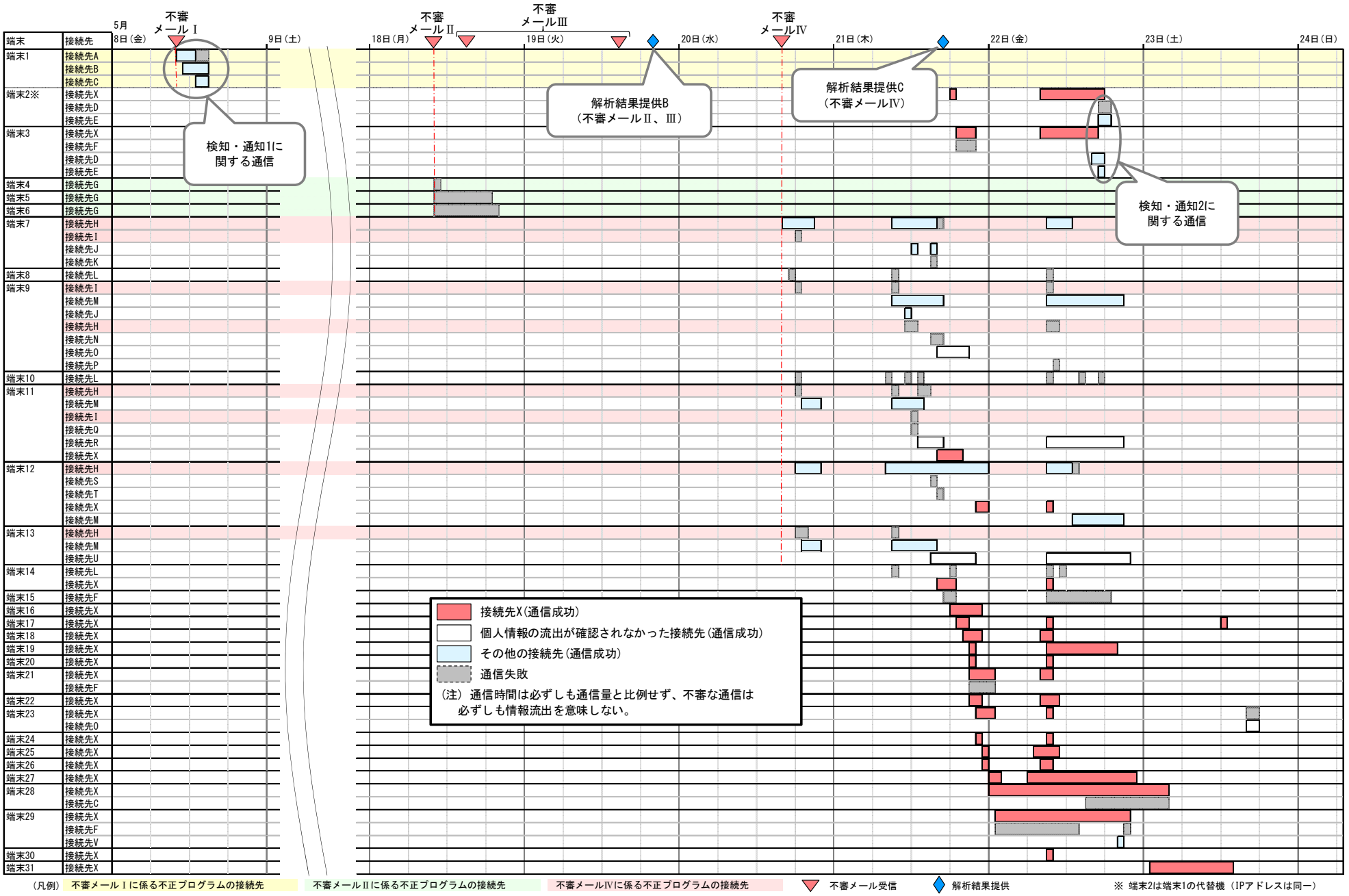


図 2 感染端末と不審な通信

2.3. 認証サーバの調査

認証サーバ[10]に対する攻撃の有無を調査するため、認証サーバのイベントログ(5 月 7 日 23:54～29 日 23:54)を入手し解析したが、イベントログには、認証サーバが攻撃されたか否かを判断するのに十分な情報が残っていなかった。

他方、感染端末に対するフォレンジック調査[11]により、5 月 22 日午後、1 台の感染端末でドメイン管理者権限[12]を奪取する不正プログラムが実行されていたことが判明した。当該不正プログラムは認証サーバの脆弱性を攻撃するものであり、脆弱性への対策が不十分であったことから攻撃が成功し、ドメイン管理者権限が奪取されたと認められる。しかし、この時点では、接続先 X との通信をした 21 台の感染端末のうち、20 台が既に接続先 X との通信を行っていることから、ドメイン管理者権限の奪取と約 125 万件の個人情報流出との関連性は薄いと考えられる。

2.4. 感染端末に対するフォレンジック調査

感染端末に対しシステム運用業者が行ったフォレンジック調査の結果について入手し、その内容を確認した。

一般に、フォレンジック調査によって知ることのできる内容には限界があるが、感染端末に対するフォレンジック調査により、不審メールに係る不正プログラムが実行された形跡のほか、権限昇格を行うものなど各種の不正プログラムが実行された形跡、ファイル圧縮等の情報収集活動の形跡、ローカル管理者権限[13]による不審な活動の形跡等が確認された。

2.5. 攻撃の全体像

不審メール、不審な通信及び感染端末に対するフォレンジック調査の結果を基に、本事案において攻撃者が行った攻撃の全体像について述べる。

2.5.1 不審メールⅠ～Ⅳによる攻撃の共通性

不審メールⅠ～Ⅳについて分析を行ったところ、以下のとおり共通点があることが判明した(図 3 不審メールの共通点(11 ページ))。このことから、不審メールⅠ～Ⅳによる攻撃は、同一の攻撃者による一連のものと考えられる。

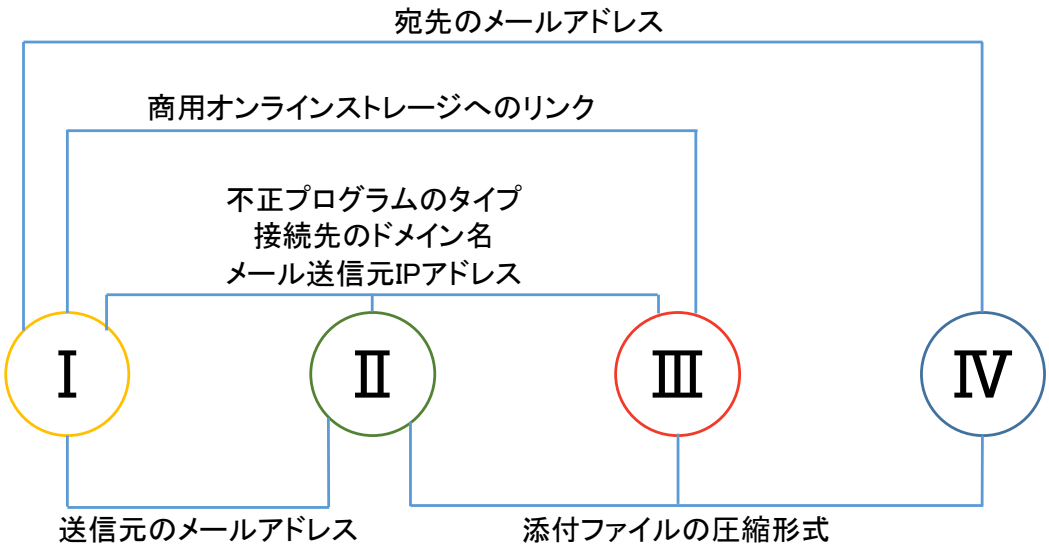
---

[10] ネットワークにおいてユーザ認証等のユーザ管理を行うサーバをいう。

[11] 端末等に残された電磁的記録の保全、分析等を行う調査をいう。

[12] ネットワーク全体に対して設定される権限で、同権限を持つユーザは、ネットワークに参加している全ての端末、サーバを管理する権限を持っている。

[13] 端末、サーバごとに設定される権限で、同権限を持つユーザは、その端末等を管理する権限を持っている。



※　線のつながりは共通点があることを示している。

図 3 不審メールの共通点

2.5.2 攻撃の概要[14]

(1) 不審メールⅠによる攻撃

機構が使用しているメールアドレスの中には、その使用目的の性格上、ウェブサイトで公開されているものがある。攻撃者は、このような機構の公開メールアドレスを入手するとともに、「「厚生年金基金制度の見直しについて(試案)に関する意見」」という件名で、年金業務に関連があるように偽装したメールを準備、不正プログラムを蔵置した商用オンラインストレージへのリンクを本文中に張った上で、5 月 8 日、機構の 2 つの公開メールアドレスに対してメールを送信したと認められる。この結果、1 台の端末を不正プログラムに感染させた。

感染端末が指令サーバに接続した後、攻撃者は、遠隔操作によりこの端末上で権限昇格を行う不正プログラムを実行し、情報収集活動を行った形跡が認められるが、他の端末を不正プログラムに感染させることはなく、約 4 時間後、感染端末の LAN ケーブルの抜線により活動が中断されたと認められる。

(2) 不審メールⅡによる攻撃

不審メールⅡ及びⅢによる攻撃を行うに当たり、攻撃者は、ウェブサイト等で公開されていない機構職員のメールアドレス及び氏名(漢字表記のフルネーム)を 100 以上用意している。これら非公開メールアドレス等の入手方法は不明であるが、不審メールⅠに

[14]「表 1 不審メールの整理」(7 ページ)及び「図 2 感染端末と不審な通信」(9 ページ)参照

よる攻撃で入手した可能性も排除されない。

攻撃者は、「給付研究委員会オープンセミナーのご案内」という件名で、年金業務に関連があるように偽装したメールを準備、本文中に送信相手の氏名を明記し、不正プログラムを圧縮して添付した上で、5 月 18 日、機構職員 98 人の非公開メールアドレスに対してメールを送信したと認められる。この結果、3 台の端末を不正プログラムに感染させた。

しかし、3 台の感染端末とも指令サーバへの通信が失敗し、攻撃者は端末を遠隔操作下に置くことができなかった。

⑶ 不審メールⅢによる攻撃

攻撃者は、「厚生年金徴収関係研修資料」という件名で、年金業務に関連があるように偽装したメールを準備、不正プログラムを圧縮して添付した上で、5 月 18 日、不審メールⅡを送信した数時間後、機構職員 16 人の非公開メールアドレスに対してメールを送信したと認められる。

更に、攻撃者は、同じ件名で添付ファイルがなく、不正プログラムを蔵置した商用オンラインストレージへのリンクを本文中に張ったメールを準備、5 月 18 日から 19 日にかけて、機構職員 4 人の非公開メールアドレスに対して送信したと認められる。

これらの攻撃の結果、端末が感染した形跡はなく、攻撃者は端末を遠隔操作下に置くことができなかった。

⑷ 不審メールⅣによる攻撃

攻撃者は、「【医療費通知】」という件名で、医療費の通知を偽装するメールを準備、不正プログラムを圧縮して添付した上で、5 月 20 日、機構の 3 つの公開メールアドレスに対して送信したと認められる。

医療費の通知を偽装するメールは、昨年秋から広く出回っており、複数のセキュリティベンダから関連情報が公開されている。このメールは、短い本文で医療費の通知を淡々と伝えるものであり、攻撃先に特化した作り込みがなされていないものであるが、長期にわたり使い回されていると考えられる。

このメールの送信により、攻撃者は、端末 1 台を不正プログラムに感染させた。

この感染端末が指令サーバに接続した後、攻撃者は、当該端末を遠隔操作し、約 30 分後には当該端末のローカル管理者権限を奪取したと考えられる。その後、攻撃者は、2 時間以内に他の 6 台の端末を順次不正プログラムに感染させ、うち 3 台を遠隔操作下に置くことに成功した。攻撃者は、すべての端末においてローカル管理者権限の ID・パスワードが同一であったことを悪用し、短時間で感染を拡大させたと考えられる。

このように、5 月 20 日のうちに攻撃者は 4 台の端末を遠隔操作下に置いた。

5 月 21 日になり、攻撃者は、更に 1 台の端末を遠隔操作下に置き、計 5 台の端末を遠隔操作できる状態を確保した上で、夕刻から深夜にかけて次々と 17 台の端末を不正プログラムに感染させ、接続先 X への通信を発生させた。急速な感染拡大は、前日同様、ローカル管理者権限の悪用によるものと認められる。深夜は、端末の電源が落とされていることが通常であり、攻撃が中断されることが多いと考えられるが、攻撃者は、電源が落ちていない端末 2 台を不正プログラムに感染させ、端末を遠隔操作できる環境を夜通し確保したと認められる。

5 月 22 日朝の時点で、攻撃者が遠隔操作下に置いた端末は 23 台となり、うち 20 台で接続先 X との通信が成功していた。しかし、攻撃者は、接続先 X との通信を 6 台の端末に限定し、同日昼までにその他の端末からの接続先 X への通信を自ら終了させたと認められる。

同日午後には、攻撃者は、接続先 X との通信を継続しつつ、認証サーバを攻撃してドメイン管理者権限を奪取したと考えられる(「2.3 認証サーバの調査」(10 ページ)参照)ほか、同日夕刻には、5 月 8 日に遠隔操作下においた端末(実際には代替機)を含む 2 台の端末において、5 月 8 日に使った不正プログラムと同じタイプの不正プログラムを動作させ、これが NISC によって検知されることとなった。

攻撃者は、5 月 23 日にも新たに端末 1 台を不正プログラムに感染させ、接続先 X と通信させているが、この端末を含めて同日中に不審な通信を行った端末は 4 台にとどまり、夕刻以降は不審な通信が発生していない。5 月 23 日が土曜日のため多くの端末の電源が落ちていたことに加え、機構において接続先 X への通信を発見し、LAN ケーブルの抜線、拠点単位での外部通信の遮断等の対応を行ったことにより、攻撃の継続が困難な状況になったと考えられる。

以上のように、攻撃者は、不審メールⅠ～Ⅲによる攻撃では、攻撃先の業務への関連を偽装したメールを執拗に送信する悪質性を見せ、不審メールⅣによる攻撃では、遠隔操作下に置いた端末を起点に容赦のない感染拡大活動及び情報窃取活動を行った。

これら悪質極まりないサイバー攻撃の結果、約 125 万件の個人情報が流出したと認められる。

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

3.1. CSIRT の運用に関する検討

政府機関の情報セキュリティインシデント[15](以下「インシデント」という。）に備えた体制は、「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 19 日情報セキュリティ政策会議決定）（以下「政府統一基準」という。）において、情報セキュリティインシデント対応チーム（CSIRT[16]）を整備し、以下の事項を含めて、その役割を明確にすること等を規定している[17] 。

- インシデントを認知した際に、CISO[18]や NISC に報告すること(政府統一基準 2.1.1(6)(c)、2.2.4(2)(b)及び 2.2.4(2)(f))
- 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(政府統一基準 2.2.4(1)(a))
- 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(政府統一基準 2.1.1(6)(b))

厚労省は、政府統一基準に準拠して情報セキュリティポリシーを定める必要があるが、特殊法人である機構は、政府統一基準の適用対象とされていない。ただし、情報セキュリティ対策は、それに関わる全ての行政事務従事者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を整備する必要がある(政府統一基準 2.1.1)。

このような方針に示されるとおり、厚労省としては、機構が厚労省の所掌事務である年金事務について厚労省と一体となって業務を行っていること、また、機構の取り扱う情報が大量の個人情報であることに鑑みれば、可能な限り政府統一基準と同等レベルの情報セキュリティ対策が講じられるべく、機構を適切に監督する立場にある。

こうした背景を踏まえ、両組織における CSIRT の運用等について調査・検討を行った。

---

[15] 情報セキュリティインシデントとは、「望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。」(JIS Q 27000:2014)と定義される。

[16] 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

[17] 詳細は、「1.政府機関の情報セキュリティ対策のための統一基準(抜粋)」(25 ページ)、解説は「2. 府省庁対策基準策定のためのガイドライン(抜粋)」(26 ページ)参照。

[18] Chief Information Security Officer :最高情報セキュリティ責任者

3.1.1 インシデント発生時等の報告・連絡等について

政府統一基準においては、上述のとおり、インシデントに対応するための体制の整備や、インシデントを認知した際の報告・対処手順を整備するよう求めている。

厚労省は、政府統一基準に準拠し、情報セキュリティポリシーを定めており、インシデントを認知した際は、CISO(官房長)及びNISCに報告する旨規定している。また、インシデントが発生した場合の対処及び報告等の手続きについては、インシデント対処の手順書を定めており、統括情報セキュリティ責任者(情報政策担当参事官)は、すべての行政事務従事者に周知することとしている。報告等の手順の概要をまとめると、インシデント発生時等の報告・連絡については、次のようになっている。

(a) 省内外(NISCを含む。) からインシデントの発生の連絡を受け付ける情報セキュリティ担当の窓口は、情参室のサイバーセキュリティ対策専門官及び情報セキュリティ対策係。
(b) 行政事務従事者が、インシデントを認知した場合には、その者が所属する課室長等に報告し、課室長等の指示に従う。
(c) 当該インシデントに係る課室長等は、CSIRTと情報を共有する。
(d) 当該インシデントに係る課室長等は、当該インシデントの発生している当該部局の総括的な課長等に報告し、緊急対応策についての指示をする。
(e) 当該インシデントに係る課室長等はCISOに速やかに報告し、CISOは、当該インシデントの発生している当該部局の総括的な課長等に対して、被害拡大防止等の指示等を行う。

今回のインシデントにおいては、厚労省によれば、セキュリティポリシーに基づく手順書に基づいた必要な措置は一応とられていたが、責任者への報告はなされていなかったとしている(今回のインシデントにおいて、機構において発生したインシデントについては厚労省年金局事業企画課長への報告、GSOC[19]からの通知については情報政策担当参事官への報告が、これに該当すると考えられる。)。

なお、機構のセキュリティポリシーにおいては、インシデント対処体制の必要性を規定し、その具体化はシステム障害対応を主たる目的としたリスク管理一般の規定等に委ねている。そして、リスク管理一般の規定においては、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について、明確化されていない。

[19] 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

3.1.2 CSIRT 体制について

厚労省の情報セキュリティポリシーでは、CSIRT に属する職員について、CISO(官房長)、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(CIO 補佐官)を充てるとしている。また、CSIRT の庶務は情参室で行い、CISO アドバイザは、専門的な知識及び経験に基づき、緊急時における対応等情報セキュリティ対策全般に対しての助言等を行うこととしている。

今回の事案発生時点においては、CSIRT が機能するための前提となる報告等がなされていなかったが、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点にも留意が必要である。

一方、日本年金機構セキュリティポリシーにおいては、インシデント対処の必要性や、その具体的な規定は複数の規程類で規定している。リスク管理全般については、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は明確となっていない。また、いずれの規程類においても CSIRT 体制についての定めはなかった。

なお、機構によると、平成 27 年 7 月 10 日から CSIRT 体制の構築をはじめとしたセキュリティ体制の整備の検討を開始したとしている。

3.2. システムへの多重防御(標的型攻撃対策)に関する検討

標的型攻撃とは、特定の組織に狙いを絞り、その組織の業務習慣等内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃である。

典型的なものとしては、システム内部に潜入し、侵入範囲を拡大し、重要な情報を窃取し又は破壊する攻撃活動が考えられる。

3.2.1 政府統一基準における対策について

こうした一連の攻撃活動は、未知の脆弱性を悪用する等の手法も用いて実行されるため、完全に検知・防御することは困難であることから、政府統一基準(6.2.4)において、標的型攻撃による組織内部への侵入を低減する入口対策のみならず、内部に侵入した攻撃を早期検知して対処する内部対策、侵入範囲の拡大の困難度を上げる内部対策及び外部との不正通信を検知して対処する内部対策から構成される多重防御の情報セキュリティ対策体系によって、標的型攻撃に備える必要があることが示されている。

具体的な対策を示すものとして、「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)(以下「リスク評価等ガイドライン」という。) があり、その適用範囲は、国の行政機関と記述している。

3.2.2 厚労省等における状況

厚労省においては、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、リスク評価等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。

さらに、標的型攻撃からの有効な遮断機能を有すると考えられる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ため、標的型攻撃を受けるリスクに当該個人情報をさらす結果となった。

4. 今回のサイバー攻撃の特徴と対策

サイバー攻撃の特徴は、攻撃者の存在であり、相手を知って対処することが求められる。

「2.5 攻撃の全体像」(10 ページ)で述べた攻撃者がとったと考えられる行為についての分析を踏まえ、こうした攻撃者の存在を意識した上で、政府としての課題と対策を検討した。

4.1. 標的型攻撃の特徴等

標的型攻撃では、攻撃者は標的とする組織に狙いを定め、精巧な技術と相当程度の資源を投入して、標的とする組織の情報を窃取し、業務を妨害することを狙うとされる。そして、長期間にわたって、目的達成に必要な水準の通信を維持し、繰り返して攻撃をしかけ、目的を着実に遂行するといった特徴がある[20]。

4.1.1 不審メールと標的型攻撃

標的型攻撃の典型的な手法のひとつとして、標的とする組織のアドレスに対して不正プログラムを添付などしたメールを送り付けることに始まる標的型メール攻撃がある。今回の攻撃は、これに該当する。標的型攻撃に使われるメールは一目では見分けがつかないよう巧妙化が進んでいるとともに、緊急性をあおったり職員の不注意を誘ったりする心理的な手法が用いられている。このため、不審メールの開封を完全に防ぐことを目標とする対策は現実的ではなく、メール開封(少なくとも端緒の端末１台は感染すること)を前提とした対策が必要である。

最初の端末への攻撃が成功すると、攻撃者は、その端末を乗っ取り、端末内の情報(端末が接続されているシステムの構成・設定、端末使用者がやり取りしたメールのアドレスや文面、端末使用者が保存したファイル等)及び端末からアクセス可能な情報(サーバに保存され、端末使用者に閲覧権限のあるファイルやデータベース等)を閲覧、窃取等することが可能となる。そして、窃取したメールのアドレスや文面を、次回以降の攻撃のために利用し、標的とする組織内・周辺組織の多数のアドレスに不信感を抱かせないメールを送りつけることが可能となる。

4.1.2 標的型攻撃の展開

攻撃者は乗っ取った端末を足掛かりとして、当該端末に含まれているログイン情報や接続されている機器の情報等を利用して、当該端末を遠隔操作しながら他の機器を攻撃し、侵入を拡大させる。事態の進行の程度に応じて、重要な情報の窃取等致命的な事態を招く可能性が高まるため、早期に攻撃を認知し、当該端末をネットワークから隔離す

[20] National Institute of Standards and Technology (NIST) Special Publication 800-53,Security and Privacy Controls for Federal Information Systems and Organizations,April 2013

ることが基本である。防御する側としては、侵入範囲が拡大すれば、システム全体をインターネットから遮断せざるをえなくなる。

このため、以下の事項を含め、攻撃された端末から侵入範囲を拡大させないための対策や、ネットワークを管理するような重要な機器を攻撃させないためのシステム設計・構築・運用が重要である。

こうした一連の攻撃者の活動においては、いわゆるゼロデイ攻撃[21]など回避が極めて困難な手法を用いることが多い。そして標的とする組織に対して執拗に攻撃が継続されるといった特徴がある。

4.2. 標的型攻撃に対する情報システム防御策等の考え方

IT 環境があらゆる業務に不可欠な現状において、ますます巧妙化しているサイバー攻撃から自組織の情報、システム、業務を守る目的及び対策について考え、理解し、それぞれの職務・職責に応じて実施することが求められる。このため、前述の攻撃者側の手順を理解した上で、標的型攻撃から情報システムを防御するためには、次に例示したような対策が攻撃を発見・阻止する上で有効であると考えられる。

なお、対策については、他から示された画一的な基準を受動的に実施してもうまくいく性質のものではない。組織の業務、取り扱う情報、保有するシステムに応じて、多様な対策の中からどう守りを構築するのか、目的に照らし、業務が円滑に実施できるような対策とは何か、組織として能動的に検討した上で最適な手法を設定し、実施することが肝要である。

4.2.1 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・起動できないシステム設定とする。加えて、通常業務における圧縮ファイルのメール添付の取り扱いにおいても、安全性が確認された標準的な方法に統一し、それ以外の方法を制限する。
- システム運用の基本的な対策として、既知の脆弱性を放置しないようオペレーティングシステムのアップデートや、ソフトウェアへの最新のセキュリティパッチの適用を着実に行う。また、システムにこうした脆弱性がないかを検証するための診断（ペネトレーションテスト等）を行う。
- 脆弱性の発生個所を最小限とするため、ウェブブラウザの「プラグイン」などの拡張機能の使用を必要最小限とし、ゼロデイ攻撃を続発させたソフトウェアの使用を取りやめることを含め、使用を認めるソフトウェアを定期的に見直す。
- ウェブ閲覧の効用は高い反面、ウェブ表示が広く認められることは、システム攻撃への糸口を与えることとなることを認識し、例えば、ウェブ表示において、不必要

[21] 修正プログラムなどが公開される前の脆弱性を悪用する攻撃。

な埋め込みコンテンツを自動的に取り込まないように設定する。システムは、攻撃を検知しやすく侵入範囲が拡大しにくいように設計・構築し、運用する。特に、業務や取り扱う情報の性質・量に応じて、重要な情報に攻撃が到達しないよう、セグメント[22]を分割し、また、システムの分離を確実に行う。同時に、システムの分離の意義を損なうことのないよう、各システムで扱うことができる情報・できない情報についてルール化し、職員に徹底する。

- 端末のローカル管理者権限の ID・パスワードが端末間で共通で、かつファイル共有が可能であると、これを攻撃者が悪用して侵入範囲の拡大を容易に図ることが可能であるため、ローカル管理者権限のパスワードを共通とする範囲を最小限とする。
- システム管理者の権限が乗っ取られた場合の被害の大きさに鑑み、不要な管理アカウントは確実に消去する、管理端末を独立のセグメントに置く等、その設定にも細心の注意を払う。
- ファイルサーバのアクセスログ、プロキシログ等のログについて平均値からの大幅な逸脱をモニタリングする、内部ネットワークに不正通信の検知システムを導入するなど、内部ネットワークにおける異常を検知する仕組みを整備する。

4.2.2 インシデント対応に係る対策

- 不審メールの受信（特に、不正プログラムが動作したと考えられる場合）については、標的型攻撃の端緒の可能性があり、攻撃者が繰り返して攻撃を試みるものと想定して継続的に対応する。
- インシデントへの対応は、サイバー攻撃による被害状況の調査、手口解明、不正プログラムの除去と復旧・再発防止の一連の対応の実施が必要となり、政府機関職員だけでは対応できない場合があるので、専門性の高い第三者の事業者（システムの構築・運用事業者とは独立した第三者の事業者）に依頼し、客観的で一括した対応も行えるように、平素から調達の準備をする。
- インシデントへの対応には、組織のリソースを迅速に投入し、場合によってはシステムや業務を止める判断が求められることもあるため、CISO 等の権限を持った者の下で行う。

[22] ローカルエリアネットワークを構成する範囲の単位で、スイッチや VLAN を用いて区切られる範囲。

5. 本部及びNISCがとるべき再発防止対策

一連の調査結果を踏まえ、「4.2 標的型攻撃に対する情報システム防御策等の考え方」(19ページ)に示した事項を適切に実施するべく、本部及びNISCがとるべき再発防止対策を次に示す。

(1) 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府省庁に対して通知するとともに、その後も必要の都度情報提供を行っている。また、不審メールや不正プログラムの疑いがあるものについてNISCに提出されれば、速やかに解析を行い、不正プログラムがあると判断したときには、その結果を当該府省庁に提供し、また、当該事案を匿名化した状態で各府省庁に提供している。

こうした一連のNISCからの通知、不審メールや不正プログラムの解析結果の提供・注意喚起が有効に機能するためには、当該省庁においてその重要性を理解し、迅速かつ適切な措置がとられる状態となっていることが前提となっている。

しかし、今回の事案の教訓を踏まえれば、こうした前提とは異なる状態にある府省庁においても、NISCの情報等が確実に活用されるための取組が必要である。そのためには事案に迅速に対処できるよう当該府省庁自らの態勢強化が不可欠であり、また、近年、検知や不審メール等の注意喚起件数が急激に増大していることを踏まえれば、具体的な事案の発生時点から現場レベルで NISC が丁寧に指導し行動を促すということは現実的ではない。

このため、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、必要な知見のレベルを明確化するとともに、研修や演習等の機会を計画的かつ体系的に提供し、事案に関するNISCからの情報提供に対して、各府省庁において適切に措置されるための教育・訓練等の充実を図ることが必要である。また、研修や演習等の対象は、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なければならない。

本部としても、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。

(2) インシデントに備えた体制の強化

インシデントに備えた体制(各府省庁の CSIRT)の整備については政府統一基準に規定され、具体的な整備の方法や内容については政府統一基準のガイドラインに定められている。各府省庁においては、これらの基準等に従いCISOの指示の下、専門的な知識又は適性を有すると認められる者を選任し、実働するよう、適切に事案への対応体制を整備

すること、また、平素から各府省庁のCSIRT要員が事案対処に必要な知識・能力、経験を高め、必要な時にはいつでも実践できるようにしておくことが求められている。

今回の事案を踏まえれば、今後NISCは、各府省庁のCSIRTが、事案発生時に実働する体制整備が図られるよう十分に情報提供等を行うとともに、各府省庁におけるCSIRT体制の強化が図られるよう、滞りのない事案の対応についての演習や訓練等の機会を設けるなどの取組を行っていく必要がある。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[23]に基づく着実な取組を確保していくものとする。

政府統一基準については、行政機関及び独立行政法人についてはその対象としている。しかし、その他の機関については、府省庁と一体となり公的業務を行う特殊法人も含めて、必要な助言や指導をするかどうかについて、「行政事務従事者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うする」ことなどの一般的な考え方以外は示されていなかった。これは、多様な業務や組織、情報、システムを所管する各機関において、自ら具体的な方針について検討した上でセキュリティ対策を進めるべきことを示したものであったが、NISCとしては、こうした考え方が理解されない可能性があることも認識した上で、今後、統一基準の各機関における具体化の状況にも留意しつつ、上述の演習や監査等を推進していく必要がある。

また、今後、本部及びNISCは、今回発生した事案における課題及びサイバーセキュリティ基本法を基に、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こととする。

なお、CSIRT構築の際、CSIRTの責任者(及び実質的な専門家)は、情報システム管理運用者から独立した立場で対処していくことが適切である。しかし、人材不足などの諸事情により、CSIRT の責任者が情報システムを管理運用(又は所管)せざるを得ない組織においては、情報システム管理運用者とは別の者が CISO に報告するなど役割分担を明確に定めることが必要であることをCISOは認識しておく必要がある。(府省庁対策基準策定のためのガイドライン2.1.1(6)(c))

(3) 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

標的型攻撃への対処については、本部及びNISCは、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。しかしながら、このリスク評価等のガイドラインの適用範囲は、国の行政機関と記述している。このため、NISCは、標的型攻撃対策としてシステム上の有益な対応策が示されているにもかかわらず、必要な機関において、その実施がなされないことがある

[23] Plan(計画)、Do(実施)、Check(評価)、Act(改善)を繰り返すことによって、継続的改善を行い、組織の活動の質を高めていく取組。

ことを認識する必要がある。

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、本部及びNISCは、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ものとする。

- 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アドバイザの積極的な活用

併せて NISC においては、政府機関のネットワークを常に監視し、不審な通信を検知し、対処する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。

おわりに

ここ 10 年で、政府機関の業務遂行に対する IT への依存度が急速に高まってきている。こうした状況においては、もはや IT 専門職だけではなく、一般職員においてもサイバーセキュリティに関する所要の知識と行動が要求されるようになった。しかし、IT 依存度の高まりに対して、IT 専門職、一般職員とも、十分に対応できていない面が今回の調査を通じて明らかとなった。

内閣官房においては、平成 12 年 2 月に内閣官房情報セキュリティ対策推進室が設置され、平成 17 年に内閣官房情報セキュリティセンターに改組され、政府機関のサイバーセキュリティに関して「予防」、「検知」、「対処」の側面から指針を示す等の取組を行ってきた。しかし、今回発生した事案を踏まえれば、これまでの取組を一層加速・強化することが必要である。

本部及び NISC は、本年 1 月のサイバーセキュリティ基本法の全面施行によって、政府機関のサイバーセキュリティ確保に係る権限及び権能を有する機関として改組されたところである。サイバーセキュリティ基本法に基づく我が国のサイバーセキュリティの司令塔として十分に機能させていくためには、今回発生した事案から得られた教訓を踏まえ、再発防止に活かしていくことが求められる。このため、「4 今回のサイバー攻撃の特徴と対策」(18 ページ)に示す再発防止対策について、着実に取り組んでいく必要があるが、その際には、IT を取り巻く環境変化を十分認識し、適切な人事、予算、インフラ整備の側面からの対応も忘れてはならない。

今回の調査は、サイバーセキュリティ基本法に基づく初めての原因究明調査であったが、捜査に当たっている警察から十分な協力を得て調査を進めることができた。また、今回の原因究明調査において、警察庁及び防衛省から NISC の勤務経験を持つ専門家の迅速な派遣が得られたことが実態解明に大きく貢献した。

こうした原因究明調査を通じて得られたグッドプラクティスは、事案対処省庁をはじめ、関係省庁との緊密な連携が、我が国のサイバーセキュリティの強靭化には不可欠であることを示すものである。

サイバーセキュリティを取り巻く環境は年々高度化していることを踏まえ、府省庁間の緊密な連携を通じて、政府全体としてのサイバーセキュリティの強靭化の取組について、継続的かつ機敏に推進していく必要がある。

参考資料

1.政府機関の情報セキュリティ対策のための統一基準(抜粋)

(平成 26 年 5 月 19 日　情報セキュリティ政策会議)

2.1.1　組織・体制の整備

目的・趣旨

情報セキュリティ対策は、それに係る全ての行政事務従事者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を整備する必要がある。特に最高情報セキュリティ責任者は、情報セキュリティ対策を着実に進めるために、自らが組織内を統括し、組織全体として計画的に対策が実施されるよう推進しなければならない。

なお、最高情報セキュリティ責任者は、その権限に属する事務の一部を統一基準に定める各責任者に委任することができる。

遵守事項

(6)情報セキュリティインシデントに備えた体制の整備

(a)　最高情報セキュリティ責任者は、CSIRT を整備し、その役割を明確化すること。

(b)　最高情報セキュリティ責任者は、行政事務従事者のうちから CSIRT に属する職員として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。そのうち、府省庁における情報セキュリティインシデントに対処するための責任者として CSIRT 責任者を置くこと。

(c)　最高情報セキュリティ責任者は、情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制を整備すること。

2.2.4　情報セキュリティインシデントへの対処

目的・趣旨

情報セキュリティインシデントを認知した場合には、最高情報セキュリティ責任者に早急にその状況を報告するとともに、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。また、情報セキュリティインシデントの対処が完了した段階においては、原因について調査するなどにより、情報セキュリティインシデントの経験から今後に生かすべき教訓を導き出し、再発防止や対処手順、体制等の見直しにつなげることが重要である。

遵守事項

(1)情報セキュリティインシデントに備えた事前準備

(a)　統括情報セキュリティ責任者は、情報セキュリティインシデントを認知した際の報告窓口を含む府省庁関係者への報告手順を整備し、行政事務従事者に周知すること。

(b)　統括情報セキュリティ責任者は、情報セキュリティインシデントを認知した際の府省庁外との情報共有を含む対処手順を整備すること。

(2)情報セキュリティインシデントの認知時における報告・対処

(a)　行政事務従事者は、情報セキュリティインシデントを認知した場合には、府省庁の報告窓口に報告し、指示に従うこと。

(b)　CSIRT 責任者は、情報セキュリティインシデントを認知した場合にはその状況を確認し、情報セキュリティインシデントについて最高情報セキュリティ責任者に速やかに報告すること。

(f)　CSIRT は、府省庁の情報システムについて、情報セキュリティインシデントを認知した場合には、当該事象について速やかに、内閣官房情報セキュリティセンターに連絡すること。また、認知した情報セキュリティインシデントがサイバー攻撃又はそのおそれのあるものである場合には、当該情報セキュリティインシデントの内容に応じ、警察への通報・連絡等を行うこと。さらに、国民の生活、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのある大規模サイバー攻撃事態等においては、「大規模サイバー攻撃等への初動対処について(平成 22 年 3 月 19 日内閣危機管理監決裁)」に基づく報告も行うこと。

6.2.4　標的型攻撃対策

目的・趣旨

標的型攻撃とは、特定の組織に狙いを絞り、その組織の業務習慣等内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃である。典型的なものとしては、組織内部に潜入し、侵入範囲を拡大し、重要な情報を窃取又は破壊する攻撃活動が考えられる。これら一連の攻撃活動は、未知の手段も用いて実行されるため、完全に検知及び防御することは困難である。

したがって、標的型攻撃による組織内部への侵入を低減する対策(入口対策)、並びに内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策(内部対策)からなる、多重防御の情報セキュリティ対策体系によって、標的型攻撃に備える必要がある。

遵守事項

(1)標的型攻撃対策の実施

(a)　情報システムセキュリティ責任者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策(入口対策)を講ずること。

(b)　情報システムセキュリティ責任者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策(内部対策)を講ずること。

2. 府省庁対策基準策定のためのガイドライン(抜粋)

(平成 26 年 5 月 19 日　内閣官房情報セキュリティセンター)

2.1.1　組織・体制の整備

【解説】

遵守事項 2.1.1(6)(a)「CSIRT」について

府省庁の情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、当該府省庁が、発生した事案を正確に把握し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とするための機能を有する体制を整備することが必要である。

一般的に、情報セキュリティインシデントの認知時の対処においては、不完全で断片的な情報しかない状況で判断を下し、指示を出して、調査等により状況の解明を進めることとなる。CSIRT は、時々刻々と明らかになる情報を基に、状況を整理し、事態の収束に向けてさらに必要な対応を行い、適切な頻度で幹部に状況を報告する。

遵守事項 2.1.1(6)(c)「情報セキュリティインシデントが発生した際、直ちに自らへの報告が行われる体制」について

CSIRT 責任者が情報システムを所管している場合、当該情報システムの情報セキュリティインシデントを認知した際、二つの役職が利害相反関係にあることから、最高情報セキュリティ責任者等の幹部に報告を上げない、事実関係の一部しか報告しない、報告を遅らせるなど、管理責任に影響を及ぼすおそれがある。

これを避けるため、例えば、CSIRT 責任者には情報セキュリティ責任者以外の者を充てる、最高情報セキュリティ責任者等の幹部に情報セキュリティインシデントについて報告する役割を別途 CSIRT 責任者以外の者に与えるなどにより、迅速かつ適切な報告経路を確保することが必要である。