検　証　報　告　書

要 約 版

平成 27 年 8 月 21 日

日本年金機構における

不正アクセスによる情報流出事案検証委員会

日本年金機構における不正アクセスによる情報流出事案検証委員会

名　簿

委員長	甲斐中　辰夫	弁護士（卓照綜合法律事務所）、元最高裁判所判事、元東京高等検察庁検事長
委員	青嶋　信仁	株式会社ディアイティ　取締役　セキュリティサービス事業部長
	大谷　義雄	全国社会保険労務士会連合会副会長
	齋藤　洋平	フューチャーアーキテクト株式会社　テクノロジーイノベーショングループ　バイスプレジデント
	藤井　眞理子	東京大学先端科学技術研究センター教授
	増田　宏一	公認会計士、元日本公認会計士協会会長
事務局長	野村　修也	中央大学法科大学院教授、弁護士（森・濱田松本法律事務所）、厚生労働省顧問
参与	金子　桂輔	弁護士（黄櫨綜合法律事務所）
	齊藤　貴一	弁護士（卓照綜合法律事務所）
	佐々木　宏幸	株式会社ディアイティ　セキュリティサービス事業部、情報処理技術者試験委員、CISSP
	芝　昭彦	弁護士（芝経営法律事務所）
	鈴木　ひろみ	社会保険労務士（鈴木社会保険労務士事務所）
	永宮　直史	特定非営利活動法人日本セキュリティ監査協会事務局長、情報セキュリティ主席監査人
	西田　恵	株式会社 IHI　情報システム部　技師長
	福田　舞	弁護士（卓照綜合法律事務所）
	松崎　祥三	有限責任あずさ監査法人／KPMG　IT 監査部マネジャー
	松本　卓也	弁護士（阿部・井窪・片山法律事務所）
	山口　達也	有限責任あずさ監査法人／KPMG　IT 監査部パートナー
	山﨑　千春	有限責任あずさ監査法人／KPMG 金融事業部マネージングディレクター

（注）委員及び参与の表記は五十音順。

目　次

第１　検証の概要

１　本委員会設置の経緯

平成 27 年５月８日、厚生労働省（以下「厚労省」という。）及び日本年金機構（以下「機構」という。）は、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。）から、機構のネットワークシステムと外部との間で不審な通信が行われている旨の情報を受領した。これを受け、機構は、当該ネットワークシステムに係る保守運用等の委託先会社（以下「運用委託会社」という。）と連携して、関係端末の LAN ケーブルの抜線、セキュリティソフトへの最新の定義ファイルの適用等の対応を行った。しかし、その後も、機構のネットワークシステムに対しては、外部からの不審なメールが波状的に送られるなど、標的型攻撃の兆候が継続してみられた。さらに、同月 28 日には、警視庁の捜査により、上記標的型攻撃によって流出したとみられるデータが機構外部のサーバで発見されるに至り、機構による調査の結果、上記データには、機構の保有する極めて多数の個人情報が含まれていることが判明した。

これらの事態を受け、厚生労働大臣は、厚労省及び機構から独立した第三者からなる検証委員会を早急に立ち上げ、これらの一連の事案についての原因究明と再発防止策を検討させることとし、同年６月４日、「日本年金機構不正アクセス事案検証委員会」（同年７月 17 日付で「日本年金機構における不正アクセスによる情報流出事案検証委員会」と名称変更。以下「本委員会」という。）を設置する旨を決定した。

２　委嘱事項

厚生労働大臣は、平成 27 年６月８日、本委員会委員長に対し、機構に対する不正アクセス事案（以下「本事案」という。）により損なわれた厚労省及び機構に対する国民の信頼を回復できるよう、本事案に関し、機構及び厚労省の組織並びに初動及び事後の対応について検証し、原因の究明を行うとともに効果的な再発防止策について検討し、報告を行うことを委嘱した。

３　本委員会による検証の目的

本委員会による検証の目的は、上記２の委嘱に基づき、本事案の発生に至るまでの機構及び厚労省の組織における問題点並びに本事案発生後の機構及び厚労省の初動及び事後の対応における問題点を検証し、それらを踏まえ、本事案

の原因を究明するとともに、再発防止策を提言することである。

本委員会は、あくまでも機構及び厚労省のいずれからも独立した中立公正な立場から、上記目的のために調査検証を実施するものであり、本事案に関する機構、厚労省その他の組織団体又はその役職員の民事上、刑事上その他の責任の有無を確定し、これを追及することを目的とするものではない。

4　検証方法の概要

本委員会は、上記３の目的を果たすため、平成27年６月８日以降、関係資料の検証分析、関係者のヒアリング等の調査を実施し、その上で、入手した情報について随時必要に応じて委員及び参与の合議により総合分析を行い、同年８月19日（以下「本報告基準日」という。）までに入手した情報に基づき、本検証報告書をとりまとめた。

具体的な検証方法の概要は、以下のとおりである。

（１）関係資料の検証分析

本委員会は、厚労省及び機構に対し、関係資料（関係諸内部規程、決裁文書類、関係諸会議体の議事録及び同会議体における資料、運用委託会社との間の関係契約書類、関係ネットワークシステムの構造、運用状況等に関する資料、フォレンジック調査報告書、厚労省及び機構の役職員間等で発受信された電子メール、連絡文書その他の資料等）の開示を要請し、厚労省及び機構から開示を受けたこれら関係資料の検証分析を行った。

また、本委員会は、運用委託会社及び機構のネットワークシステムに導入されたセキュリティソフトの提供会社（以下「セキュリティソフト会社」という。）からも、必要に応じて関係資料の開示を受け、その検証分析を行った。

（２）関係者のヒアリング

本委員会は、厚労省及び機構の役職員をはじめ、必要に応じて運用委託会社及びセキュリティソフト会社の関係者等に対しヒアリングを実施した。ヒアリングに際しては、上記３の本委員会の検証の目的にのみ利用することを説明し、その承諾を得た。本報告基準日までのヒアリング対象者は、合計延べ78名である。

5　本委員会による検証及びその結果の前提

本委員会は、強制的な調査検証の権限を有するものではなく、その調査検証

は厚労省及び機構の役職員その他の関係者の任意の協力を前提としている。また、本委員会と検証の性質上、限られた日時と人員により調査検証せざるを得ず、これらのことから、本委員会による検証及びその結果が一定の制約を免れ得るものではない。なお、本委員会による検証により明らかになった事実等には、公にすることによって攻撃者を利するおそれがあるものが含まれることから、これに該当すると本委員会が認めた事実等については、本報告書の記述から除外していることも付言する。

第2　本委員会が認定した事実

1　サイバー攻撃とその対応

「サイバー攻撃」とは、特定の組織のコンピュータシステムやネットワークに不正に侵入する等の方法で、情報・データの窃取・改ざん・破壊やシステムの機能阻害等の損害を与える行為である。本事案におけるサイバー攻撃は、攻撃対象を事前に入念に調査した上で、対象組織の役職員に対し、マルウェアが含まれるファイルを添付したり、アクセスするとマルウェアがダウンロードされるよう仕組まれたサイトへのリンクを記載したりしたメールを送りつける代表的な「標的型攻撃」であったと考えられる。

端末に感染したマルウェアは、その後、バックドアの開設、他のマルウェアのダウンロード、端末への認証情報やネットワーク環境に関する情報収集等、その後の攻撃の基盤構築活動を展開する。その上で、攻撃者は、他の端末やサーバの認証情報を窃取してそれらに攻撃範囲を拡大させる等して、システム内の情報の広汎な窃取、システムの機能阻害といった自らの攻撃目的の完遂を図る。

標的型攻撃への対応策として、NISC や独立行政法人情報処理推進機構等が公開しているガイドライン等においては、

①「システム設計」：企画・設計の段階から、業務内容やシステム環境の特性等を踏まえたリスク評価に応じた適切なシステム設計を行うこと

②「運用管理」：最新の情報に基づくセキュリティ教育及び実践的訓練の継続的実施、情報セキュリティインシデント（以下「インシデント」という。）対応部署への専門家の配置、脆弱性管理やセキュリティの最新の定義ファイルの導入等の「入口対策」、攻撃者にシステムへの侵入に成功された場合に被害範囲の最小化を図るための「内部対策」、攻撃者によるシステム内部の情報の外部流出を阻止するための「出口対策」を組み合わせて行う（「多層防御」）こと

③「インシデント対応」：CSIRT（Computer Security Incident Response Team）

を中心とする緊急対応体制をあらかじめ整備し、継続的な訓練等により迅速な初動や組織横断的な対応等の能力向上に努めること
が要求されている。

2　日本年金機構のネットワークシステムの概要

機構が業務において使用しているネットワークシステムには、政府管掌年金事業に関し政府から根幹業務を提供する「社会保険オンラインシステム」（「基幹系システム」とも呼ばれる。）と、それ以外の業務に関するサービスを提供するシステム（「情報系システム」とも呼ばれる。）がある。前者は厚労省の所有で機構にその運用を委託しており、後者は機構が自ら所有し運用している。

情報系システムの中心をなしているのが、本件標的型攻撃の対象となった「機構 LAN システム」である。同システムは機構の役職員の日常業務において用いるイントラネットであり、インターネット接続や電子メールのサービスも提供している。また、ファイル共有を行うためのファイルサーバも設置されており、機構内で「共有フォルダ」と呼ばれている。情報系システムは、厚労省統合ネットワーク等を経由してインターネットに接続されている。なお、基幹系システムと情報系システムは、ネットワーク上で物理的に接続されているものの、ネットワーク機器等によって論理的に分離された状態にある。

3　日本年金機構における情報システムの設計と運用

機構においては、機構 LAN システムでは個人情報に関する処理を行わないことをシステム構成の前提としていた。しかしながら、業務の必要を理由に個人情報が機構 LAN 上の共有フォルダに保管されるようになり、共有フォルダに個人情報が置かれるという上記前提に反する運用が行われていた。

また、機構においては、機構 LAN に内在し標的型攻撃を引き起こす可能性のある種々の脆弱性には注意が払われておらず、監視（モニタリング）が常時行われていなかったなど、機構 LAN については標的型攻撃を想定したシステムの設計や運用がなされていなかった。

4　日本年金機構における情報セキュリティの問題

機構においては、①CSIRT 制度が設けられておらず、本件のような事象を想定した厚労省との緊急連絡体制も定められていなかった、②リスクに備えた人員配置が行われていなかった、③運用委託会社との間でインシデント発生時における緊急対応の内容につき明確な合意がなかった、④情報セキュリティに関する研修内容は不十分で、標的型攻撃を含むサイバー攻撃に関する訓練は行われていなかったなど、情報セキュリティ体制は脆弱であった。

機構における個人情報は、原則として基幹系システムに保管され、一定の条件の下で機構 LAN に接続する共有フォルダで保管されていた。共有フォルダへの保管に際しては、アクセス権を制限するか、パスワードを設定するルールとなっていたが、暗号化等も行われておらずそもそも極めてリスクの高い運用であったほか、そうしたルールですら厳守が徹底されていなかった。しかも、ルールの遵守状況を実効的に確認できる仕組みは設けられていなかった。このように、機構においては個人情報保護に関する認識が不足していた。

機構では、情報セキュリティや個人情報保護に関する自己点検が毎月実施されていたが、各職員が個々で改善施策を検討することとされているなど実効性が不十分であった。また、外部からの攻撃を想定した情報セキュリティ対策は監査対象とされていなかった。

機構本部からの全国の拠点に対する指示は、年間数千件に及ぶ上、過去のものと重畳的なものもみられたなど、現場に相当な負荷がかかっている。また、機構本部が現場におけるルールの遵守状況等について把握できる枠組みとなっていなかった。このように機構の現場に対するガバナンスは不十分であった。

5　日本年金機構の情報セキュリティに対する厚生労働省の監督体制

厚労省においては、機構の監督を所掌する年金局及び省全体の情報セキュリティ対策を担当する政策統括官付情報政策担当参事官室（以下「情参室」という。）のいずれの部署においても、機構 LAN システムについての責任部局であるとの認識が希薄であり、適切な監督が行われなかった。

厚労省自体の情報セキュリティ体制も脆弱であった。厚労省に配置されていた CIO 補佐官が最高情報セキュリティアドバイザーとされていたが、情報セキュリティ担当部門との連携は不十分であり、本事案についての情報連絡も遅延した。

厚労省には CSIRT 体制が定められていたものの、技術力を持った実働要員が充てられていないなど実効性に乏しく、厚労省と関連組織全体の連携もなされていなかった。

6　本件標的型攻撃とこれに対する対応

本事案においては、標的型メールを送付する手口によって機構 LAN システムが三段階にわたる標的型攻撃を受けた結果、共有フォルダに保管されていた大量の個人情報等が外部に流出した。

（1）本件標的型攻撃に先立つ平成 27 年 4 月 22 日の攻撃

機構に対する本件標的型攻撃に先立つ平成 27 年 4 月 22 日、厚労省に対して

類似の手口による攻撃が行われていた。同日、厚労省年金局等を対象とする標的型メールによる攻撃が行われ、受信した職員が添付ファイルを開封したことから端末が感染し、C&C サーバに対する不正な通信が発生したが、NISC からの通知を受けた厚労省において URL ブロックを行ったことにより、発生の約２時間後に通信が遮断された。当該不正通信のアクセスログによれば、各アクセスは、GET メソッドといわれる、外部から情報を取得する命令文による HTTP 通信であり、不明な文字列が付加されていた。

また、同日感染した端末が通信を行った C&C サーバのドメインは、５月８日に機構で感染した端末が通信を行った C&C サーバと同一であり、サブドメインのみが異なるものであった。仮に４月 22 日の段階で厚労省統合ネットワークにおいてドメイン単位での URL ブロックを実施していれば、５月８日に発生した同一ドメインの C&C サーバに対する不正な通信は防げたが、現実には４月 22 日の時点で厚労省において実施した URL ブロックはサブドメイン単位のもので、ドメイン単位での URL ブロックを実施したのは５月８日に至ってからであった。

（２）第一段階

ア　攻撃の態様

平成 27 年５月８日午前、機構の２つの公開メールアドレス宛てに同一のアドレスから不審メール２通が送信された。受信した職員の一人がこれを開封し、メール本文に記載されていた外部のオンラインストレージサービスへの URL のリンクをクリックしたことでその端末に不正プログラムがダウンロードされ、外部との不正な通信が発生した。当該不正通信は、当該端末から LAN ケーブルを抜線し LAN から遮断するまでの約４時間継続し、極めて大量の Web アクセスが行われていた。各アクセスは、４月 22 日に発生した不正な通信と同様、GET メソッドの命令文に不明な文字列が付加されているなどの特徴を有していた。

イ　機構の対応

５月８日、NISC は、厚労省統合ネットワークを通じて発信されている不審な通信を検知し、厚労省に通報した。厚労省は、不審な通信の発信元を機構 LAN システムと特定し、機構の同システム担当部署に NISC の通報内容を伝達した。

機構は、不審な通信の発信元端末を特定した後、直ちに当該端末の LAN ケーブルを抜線した。機構 LAN の運用委託会社は、当該端末を回収し、セキュリティソフト会社に解析を依頼するとともに、NISC から通知された情報に基づき、不審な通信先とされる URL について、機構 LAN における URL ブロックを実施した。

なお、翌９日未明に、運用委託会社から機構に対して、アクセスログを解析

した結果、情報漏えいの可能性は極めて低いと考えている旨の報告がなされた。

機構は、５月９日に、運用委託会社を通じて、先に解析を依頼した検体から新種ウィルス（マルウェア）が検出されたとの結果を受領した。12 日には、当該新種ウィルスは「トロイの木馬」タイプで、特定のサイトにファイルを取得しにいくものであり感染端末から情報を発信することはない、との報告を運用委託会社から受領した。また、15 日にも、運用委託会社より、あらためて、当該新種ウィルスの挙動は従前の報告のとおりである旨の報告がなされた。

機構との協議に基づき、運用委託会社は、他の端末への感染拡大の有無を確認するため、NISC から通報のあった URL へのアクセスログの監視を５月８日から 13 日まで行ったが、同 URL に対するアクセスは検知されなかった。

機構は、５月８日、全職員に対して注意喚起文書を発した。ただし、同日受信した実際の標的型メールの送信元アドレスや件名などを引用した具体的な例示はなされず、標的型メールに対する一般的な注意喚起にとどまった。

機構は感染の拡大を懸念していたが、その対応は特定の URL に対する通信の監視のみにとどまった。しかし、この対応では、当該 URL に対する通信が発生しない限り機構 LAN 内部における端末の感染拡大を直ちに認知できないため、不十分な対応であった。また、不審な通信が約４時間にもわたって継続していたことなどを考慮すれば、GET メソッドの HTTP 通信であっても、様々な不正プログラムが当該端末に取り込まれている可能性や、不明な文字列によって情報が外部に送信されていた可能性をも想定し、ただちに感染した端末のフォレンジック調査及びディレクトリサーバなどの主要サーバの調査に着手すべきであったと考えられる。

仮に、この段階で感染端末のフォレンジック調査を行っていれば、当該端末内に残された攻撃者の痕跡などがより早い段階で確認できたと考えられ、第二段階以降の機構の対応が異なるものとなっていた可能性がある。

なお、機構の担当者の中には、標的型攻撃の可能性があり、さらなる攻撃が行われる可能性もあるとの危機感をもって情報発信を行った者もいたが、危機意識は組織的に共有されず、適切な対応には至らなかった。

また、機構は、５月８日に受信した標的型攻撃メールの送信元メールアドレスの受信拒否設定を行わなかったため、18 日に同一のメールアドレスから大量の標的型攻撃メールが送信されるに至った。

ウ　厚労省の対応

厚労省においては、情参室の情報セキュリティ対策係が NISC からの通報を受領後、厚労省統合ネットワークの運用保守を担当している統計情報部に不審な通信の発信元の特定を依頼し、その回答を年金局を通じて機構の機構 LAN シス

テム担当部署に連絡した。NISC による通報が機構の担当部署に到達するまでの間に、およそ２時間半が経過している。また、情参室においても年金局においても、上長に対して本件についての報告は上がらなかった。

厚労省は、機構に対し、感染端末の特定と抜線等の対応を求めたが、それ以上の具体的な指示をすることはなかった。また、厚労省は、４月 22 日に本事案と類似の手口による標的型攻撃を受け、その際の攻撃に用いられたマルウェアに感染した場合には被害が大きくなる可能性があるとの情報をNISCから得ていた。しかし、５月８日の段階で、厚労省は機構に何ら情報提供を行わなかった。そのため、機構においても、本件が厚労省やその関係機関を狙った一連の標的型攻撃の一環であるとの着想に至らなかった。

ただし、厚労省統合ネットワークの運用管理者側では、４月 22 日に発生した不審な通信の通信先のドメインと５月８日に発生した不審な通信の通信先のドメインが同一であったことから、５月８日、同ネットワークにおいてドメイン単位でのURLブロックを実施した。

（３）第二段階

ア　攻撃の態様

５月 18 日午前、機構職員 101 の個人メールアドレス宛てに計 101 通の標的型メールが送信された。これらのメールの送信元アドレスは、上記第一段階のメールと同一であった。機構は、同アドレスにつき受信拒否設定を行ったが、同日午後から翌 19 日午前にかけて新たに異なるアドレスから合計 19 通の標的型メールが送信されたため、この送信元アドレスについても受信拒否設定を行ったところ、同日午後、さらに異なるアドレスから職員の個人アドレス宛てに１通の標的型メールが送信された。

以上の一連の攻撃の中で、５月 18 日の段階で、端末３台が感染し、不正な通信が発生した。これらの感染端末が通信を試みた C&C サーバについては、５月８日に厚労省統合ネットワークにおいて URL ブロックが実施されていたため、結果としてアクセスは成功しなかった。

なお、フォレンジック調査の結果によれば、第一段階の攻撃において、職員のメールアドレスが外部に漏えいされ、第二段階の攻撃に用いられた可能性が高いことが判明した。

イ　機構の対応

機構は、５月 18 日午前に全国の複数の職員から不審メール受信の報告を受けたため、運用委託会社に対し不審メールの件数を確認したところ、既に 100 件ものメールが送られてきていたことが判明し、標的型攻撃を受けていることを

認識した。

機構は、不審メールの受信について職員から情報提供を受ける都度、運用委託会社に依頼して当該不審メールの送信元アドレスからの受信状況を確認するとともに、その受信拒否設定を行った。また、今回は不審メールの内容を具体的に示した上で、全職員に対する注意喚起を行った。しかし、機構は、不審メールの受信者リスト一覧を運用委託会社から受領しながらも、メールを受信した職員らに個別に添付ファイルの開封の有無を確認しなかった。その後の職員による開封を防止し、また、開封の有無が端末の感染の有無を知る端緒ともなるのであるから早期に確認すべきであった。結局、機構は、5月18日の時点で3台の端末が感染していたことを6月1日まで気付かなかった。

機構は、5月 18 日に検体を収集することのできた2通の不審メールにつき、運用委託会社を通じてセキュリティソフト会社へ解析を依頼するとともに、19日には厚労省情参室を通じてNISCへも検体を提出した。

なお、機構は、標的型攻撃を受けているとの認識のもと、19 日に警視庁高井戸警察署に捜査依頼を行った。

機構としては、不審メールの数は 100 通を超えていたこと、8日とは異なり非公開の職員メールアドレス宛に職員の姓名をメール本文に記載する形で送付されていたこと、着信したメールの送信元アドレスを受信拒否設定にする都度異なるアドレスから不審メールが送信されてきていたことなどからすると、5月8日から機構を狙った攻撃者が本格的に大規模かつ執拗な攻撃を仕掛けてきているとの危機意識を持つべきであった。そして、さらなる攻撃による感染拡大を防ぐため、遅くとも19日の段階でインターネットの全面遮断に踏み切るべきであったと考えられる。

ウ　厚労省の対応

厚労省情参室は、5月 18 日及び19日の事象につき、19日に機構から報告を受けた。しかし、当該報告においては上記の異常性に関する情報は提供されなかったため、情参室として危機意識を持つことができず、NISC との間の伝達窓口として機能するにとどまった。

また、機構から、年金局事業企画課庶務係長に対しても、19 日の時点で、18日及び19日の事象について情参室に宛てられたものと同様の報告がなされていたが、同係長においては、情報セキュリティに関する専門知識を有している情参室が直接対応しているとの認識から、自らは危機意識を持つことはなく、上長への報告はなされなかった。

（4）第三段階

ア　攻撃の態様

5月20日、機構の公開メールアドレス宛てに新たな送信元アドレスから標的型メールが合計5通送信された。これらを受信した機構職員のうち一人がメールを開封し添付ファイルを開いたことでその使用端末がマルウェアに感染し、C&Cサーバに対する不正な通信が発生し、当該端末を起点としてさらに少なくとも2拠点にわたる26端末に感染が拡大した。そして、5月20日から23日までの間に、合計27台の端末から多数のC&Cサーバへの不正な通信が発生し、この過程で感染端末からのアクセスによって共有フォルダに保管されていた業務情報や個人情報が収集され、外部に流出した。

かかる攻撃の過程において、機構の端末及びディレクトリサーバの管理者権限が窃取された。フォレンジック調査の結果によれば、端末のOS及びディレクトリサーバの既知の脆弱性が利用されたことが原因であると推定される。

イ　機構の対応

機構は、5月20日、職員から不審メールを受信したとの報告を受けたため、運用委託会社に依頼して当該不審メールの送信元アドレスについて受信拒否設定を行い、併せて、当該不審メールの送信元アドレスからのメールを受信した者を特定した。しかしながら、機構は、職員の一人が標的型メールの添付ファイルを開封していた事実を5月25日まで確認することができなかった。

機構は、5月20日、運用委託会社を通じて不審メールから確保された検体の解析を依頼し、21日、厚労省情参室を通じてNISCにも検体を提出した。

そして、21日、NISCから戻って来た解析結果には、当該不審メールの添付ファイルを開封した場合に通信が発生しうるC&CサーバのURLが記載されており、これらは従前の攻撃で用いられたものとは異なる新たなものであった。しかしながら、機構は、当該解析結果に記載されたC&CサーバのURLブロックや当該C&Cサーバに対する通信の監視といった対策は講じなかった。その結果、5月21日の時点で機構の端末から当該C&Cサーバに対する通信が発生していたにもかかわらず、28日に至るまでその事実を認識することができなかった。

5月22日、機構は再びNISCから不審な通信を検知したとの連絡を受け、当該通信を発している同一拠点（A拠点）にあった2台の端末を特定してLANケーブルを抜線するとともに、A拠点全体の厚労省統合ネットワークを経由したインターネット接続の遮断を実施した。

5月23日には、運用委託会社が行っていたプロキシサーバのログの監視により、別の拠点（B拠点）から、特定のURLに対し大量の不審な通信が断続的に行われていることが判明したため、機構は当該通信を行っている端末2台を特定し、これらのLANケーブルを抜線した。また、当該URLと通信記録がある端末

の有無を確認したところ、B拠点において19台の端末から不審な通信が発生していたことが判明したため、同日、B拠点についても感染端末のある部門からの厚労省統合ネットワークを経由したインターネット接続を遮断した。

さらに、5月25日には、運用委託会社より、上記22日及び23日の事象につき、①22日にNISCから通知された不審な通信については、GETメソッドのみ記録されていることから情報漏えいが発生した可能性は極めて低いこと、他方、②23日に確認された通信についてはPOSTメソッドが記録されていることから、情報漏洩が発生した可能性は否定できない、との報告を受けた。機構幹部は、インターネット全面遮断による業務への影響を重視し、一定数以上の拠点で端末が感染しなければ全面遮断をしないとの基準を打ちたてた。

機構は、以上のような状況にもかかわらず、22日、23日、さらには25日のいずれの時点においても、特定のURLについてブロックを行うとともに、アクセスログの監視を実施し、通信監視体制を強化したものの、インターネット接続の全面遮断に踏み切ることはなかった。

機構は、5月28日、警視庁から「機構から流出したと考えられるデータを発見した」との連絡を受領し、ようやく29日に機構全体の厚労省統合ネットワークを経由したインターネット接続の遮断を実施した。しかしながら、メール送受信専用外部回線については、同回線を通じて外部に情報が漏えいすることはないだろうとの判断に基づき、6月4日に至るまで遮断されなかった。

ウ　厚労省の対応

厚労省情参室は、5月21日、機構より、19日の報告後にも新たに不審メールが送信されていたとの報告を受けたが、同時に、5月8日のウィルスについては情報を外部に漏えいするものではなく、同日の事象に関してこれまでのところ情報漏えいは確認されていないとの報告を受けた。このため、情参室担当者は、5月8日の事象は収束に向かっていると認識し、危機意識を持つことはなかった。

5月25日になり、機構から、機構の複数台の端末が感染し外部へ通信が発生していること、2拠点においてインターネット接続を停止していることなどが情参室に報告され、担当者はようやく事態の異常さを認識し、上長である参事官に報告するに至った。そして、同日、CIO補佐官への報告・相談がなされ、同補佐官は27日に機構に赴き状況報告を受けたが、初動対応について指示するタイミングとしては時機を逸しており、証拠の保全及び被害拡大の防止についての指示しかできなかった。

5月25日には、機構から年金局の幹部に対しても標的型攻撃を受けている状況について報告がなされ、同日、年金管理審議官まで報告が上がるに至った。

（5）情報流出

機構は、6月1日、本事案により機構保有の約 125 万件の個人情報が外部に流出していることが5月 28 日に判明したことを公表した。

流出が確認された個人情報は、職員が共有フォルダに保管していた情報の一部であり、最大で「基礎年金番号」「氏名」「生年月日」「住所」の4情報の流出が確認された件数が約 5.2 万件、「住所」を除く3情報が約 116.7 万件、「基礎年金番号」「氏名」の2情報が約 3.1 万件の合計約 125.0 万件であり、該当する人数は、受給者約 53 万人、被保険者約 49 万人の合計約 101 万人である。

第3　本件標的型攻撃と情報流出の原因

1　総論

本件は、機構が保有する機構 LAN システムに対して、いわゆる標的型攻撃が行われたことにより、同システムの共有フォルダ内に保存されていた個人情報が大量に外部へ流出した事案である。

本件情報流出をもたらせた標的型攻撃は、被害者が攻撃を認識し一応の防御をしているにもかかわらず、次々と手口を変えて攻撃を継続する極めて執拗かつ組織的なものであった。

これに対し、こうした標的型攻撃を含むサイバー攻撃に対する対応は、機構及びこれを監督する厚労省のいずれにおいても不十分なものであり、高度化する攻撃に対応可能な体制が整備されていなかったことが個人情報の大量流出という深刻な事態につながったと言わざるを得ない。

このような事態となった根本原因は、①機構、厚労省ともに、標的型攻撃の危険性に対する意識が不足しており、事前の人的体制と技術的な対応が不十分であったこと、②インシデント発生後においては、現場と幹部の間、関連する組織間に（例えば、機構と厚労省、同一組織間の各部署、機構と運用委託会社など）、情報や危機感の共有がなく、組織が一体として危機に当たる体制になっておらず、その結果、組織内の専門知識を持つ者の動員ができず、担当者が幹部の明確な指揮を受けることもできないままに場当たり的な対応に終始し、迅速かつ的確な対処ができなかったことにある。

この点は、以下の二つの場面での対応に端的に表れている。

第一に、緊急事態に迅速に対応すべき CSIRT が、機構において組織されていないため、何らの備えもなく 5 月 8 日の第一段階の攻撃を迎え、情報セキュリ

ティの専門知識を有する職員を動員できず、外部の専門家にも協力を得ないままで、担当者と運用委託会社とが、判明した個々の感染端末の特定と抜線に終始し後手に回ったことがあげられる。

第二に、本事案で第二段階の攻撃により標的型メールの一斉発信が行われ、このまま推移すれば、職員のうち誰かがメールの添付ファイルを開封し端末の感染が続発することが容易に予想される事態になったのに、情報の共有に欠け、組織が一体として危機に対処していないために、機構内部はもとより運用委託会社、厚労省からもインターネット接続の全面遮断との意見が出ず、なすべき決断ができないまま情報流出に至ったことである。

本件情報流出をもたらせた個別的な要因をあげれば、人的体制と技術的な観点から以下の通り様々な要因があげられるが、それらは、全て上記の根本的な原因に起因するものである。

2　日本年金機構における要因

（1）サイバー攻撃に対する人的・組織的な準備の不足

機構は、本事案のような外部からのサイバー攻撃による情報流出の可能性について、業務運営上のリスクとして漠然と認識はしていたものの、事務処理誤りや内部者による情報流出等のリスクへの対応を優先し、サイバー攻撃による情報流出の可能性に対しては、認識が乏しく有効な準備を行っていなかった。

とりわけ、標的型攻撃に適切に対応するためには、しかるべき責任者による指揮の下、組織内外の専門的知見を随時活用して組織を挙げた対応を行うことができる人的体制を整備するとともに、具体的な対応に関する手順書等のマニュアルを整備しておくことが不可欠であるが、そのいずれにおいても対応が不十分であった。

ア　人的体制の不備

人的体制の準備の面では、最高情報セキュリティ責任者以下情報セキュリティポリシーに定められた所定の体制は構築されていたものの、ポスト指定的に一般の職位に基づいて定めた体制であったため、実効的なリーダーシップに基づく対応が的確に遂行できなかった。また、内部の専門家を活用する努力も払われず、外部専門家にアドバイスを求める体制もなく、人的体制は質・量ともに不備があったと認められる。

イ　サイバー攻撃への対応体制の不備

組織的な準備の面をみると、機構内では緊急時に必要な CSIRT が設けられて

おらず、そのため現場の担当者が中心となって対応せざるを得なかった。また、標的型攻撃に対する具体的対処が明示されたマニュアルが定められていたとは認められないばかりか、本件のような事態を想定した厚労省との緊急連絡体制も定められていなかった。

さらに、運用委託会社と機構との間の契約によれば、サイバー攻撃等のインシデント発生時の緊急時対応に関する具体的なサービス内容についての明確な合意はなされていなかったため、責任や権限の所在が不明確なまま本件標的型攻撃に対処していた。

ウ　情報共有の不足

本事案を通じて、機構内部、機構と運用委託会社及びセキュリティソフト会社との情報共有ができていなかったことも、本件での不適切な対応につながったと認められる。

機構の担当者は攻撃の当初から標的型攻撃を疑っていたが、その懸念は機構内部にも、また、不正通信を解析する運用委託会社及びセキュリティソフト会社にも共有されていない。機構幹部は、中堅幹部からきちんとした状況の報告や対処の進言を受けることができず、現場の担当者は幹部の明確な指揮を受けられないままに個々の事象の対応に追われていた。

また、運用委託会社は、部分的な情報をもとに５月８日の事象をマルウェアの分析結果に基づき「情報漏えいの可能性は極めて低い」と報告し、機構もその内容を鵜呑みにしてしまった。セキュリティソフト会社も全体の状況が分からないままマルウェア解析の情報提供をするにとどまった。

エ　組織としての一体的な対応の不足

本事案の発生後、本事案への対応にあたった機構の役職員においては、相応の危機感が共有されていたことは認められるが、本事案が深刻な標的型攻撃であり、これによって大規模な情報流出が惹起され、機構全体の業務遂行に重大な支障が生じ得るといった可能性が真剣に検討された形跡はみられない。機構LAN システムの運用を担当する基幹システム開発部の一部の人員を中心に事態の対応にあたるのみで、他の部署や現場を広く巻き込んだ組織横断的な対応体制を構築することができなかった。

上記の情報共有の不足とともにこうした対応に終始した背景には、かねてから指摘されている機構のガバナンスの在り方が関係しているものとみられる。

このことは、共有フォルダへの個人情報保管の問題に端的に表れている。誰もが共有フォルダに重要な情報を大量に保管してはいけないと知りつつ、現場は仕事の都合を優先し、幹部は、現場を知らないまま形式的な対応に終始して

長期間を経過し、いつの間にか膨大な個人情報がインターネットの影響下に積み上げられ、今回の情報流出の重要な要因となっている。官民を問わず他の組織では考えられない対応である。

およそ、危機に際しての組織としての一体的な対応は、平素の組織の在り方がそのまま表れる。組織としての一体感のなさが、今回の事案を契機にそのまま表れたものということができる。

オ　個人情報保護に関する認識の不足

すでにみてきたとおり、平時のシステムの運用に関しては、共有フォルダ上に重要な情報を暗号化等せずに保管していたことが大きな要因と考えられる。規定上定められていたアクセス権の設定、あるいはパスワードによる保護は標的型攻撃への対処としては役立たないものであった。

長期間にわたり個人情報がインターネットの影響下でのリスクに晒された状況にあったこと自体が、国民の重要な個人情報を大量に扱う組織としてはあるまじきことである。

そもそも外部からのサイバー攻撃による潜在的な情報流出のリスクを組織として把握している部署がなかった。その結果、リスク回避のためのアクセス制限やパスワード設定などの規定が遵守されず、そうした状況が監査においても点検・改善される仕組みになかったことなど、およそ組織全体として個人情報保護に関する意識が低かったと認められ、これが、今回の情報流出事案につながった大きな要因と指摘せざるを得ない。

カ　情報セキュリティリスク評価の不備

適切なセキュリティ対策を講じるには、まず、網羅的な情報資産の評価が不可欠である。しかしながら、機構においては、個人情報に限っても、機構内に散在する情報の所在の把握と、それらの情報に対するリスクの把握に必要なリスク・アセスメントが実施されておらず、リスクに基づいた有効な情報セキュリティ対策が講じられていなかった。

（2）技術的要因

ア　脆弱性対応の不徹底

標的型攻撃への内部対策の一つとして、ソフトウェアベンダーから提供される脆弱性情報を定常的にチェックし、重大な脆弱性に対応するセキュリティパッチの適用を速やかに行う必要があるが、適用作業に伴うシステム停止等の影響等の懸念から、機構においてはその実施が先延ばしにされていた。

本事案では、第三段階の攻撃において、既知の脆弱性を突かれたことにより

機構 LAN システムのディレクトリサーバの管理者権限が窃取されている。この脆弱性は昨年以来指摘されていたものであり、重要な脆弱性に対するセキュリティパッチの適用の遅れがこのような結果を招いた。

また、機構 LAN システムの端末における管理者 ID とパスワードが全て同一であったことにより、短時間に広範囲の端末へ感染が拡大した。管理者権限の適切な管理が不十分であったと考えられる。

イ　システム監視の不十分性

機構 LAN システムにおけるシステム監視は標的型攻撃に対して不十分なものであった。機構 LAN システムにおいては、メール及びインターネットアクセスのログの採取は実施していたが、監視（モニタリング）は常時行われていたわけではなかった。また、取得されていたログ情報の項目も、攻撃の詳細を把握するには不十分なものであった。

さらに、管理者権限によるシステムの操作履歴や各種サーバの挙動も監視されていなかった。

これらのシステム監視が十分になされなかった結果、攻撃の各段階において状況を把握するために相当の時間を要することとなった。

ウ　インシデント発生時の感染機器のフォレンジック調査の未実施

機構は、５月８日に標的型攻撃を４時間にわたって受けた際、感染端末等に対するフォレンジック調査を行っていなかった。このため、次の攻撃を予測し対策を講ずることができなかった。

インシデント発生時にフォレンジック調査を行うことで、マルウェアを用いて攻撃者が機器を操作した状況が明らかになり、サーバまたは他の端末への感染の拡大の有無や窃取された情報などを推定することが可能になる。この調査結果に基づき、感染拡大のリスクに最大限の注意を払って事象の全容を把握する必要があるが、本件対応においてはこうした視点が欠落していたといわざるを得ない。

３　厚生労働省における要因

（１）情報セキュリティ体制の脆弱性

情報セキュリティ事案に対処する政府の体制は、NISC－厚労省－各部局－年金機構などの特殊法人等、という情報連絡の流れを想定して構築されている。この流れにおいて、連絡のハブの役割を果たす情参室は、情報政策等の業務に加えて情報セキュリティを担当する所掌となっている。

ところが、情参室のセキュリティ担当の係は、通常の人事ローテーションの中で勤務する職員で構成されていた。同係はサイバー攻撃に対するルール整備や研修・訓練の実施も担っていたものの、実質わずか１名の限られた体制の中でマイナンバー制度の施行等多岐にわたる業務を抱えていたこともあり、専門的知見や人員数などの面でみると、その情報システムの規模との比において、到底十分といえる体制とは言い難かった。

厚労省内における専門家としては、CIO補佐官５名が配置されていたが、いずれの者も非常勤であり、かつ、システム刷新業務や調達業務などに加えて情報セキュリティを助言するという状況であったため、インシデントの報告が事後的になるケースが多かったなど、情報セキュリティに関して情参室の担当者等と緊密な連携はとれていなかった。

CSIRT体制も定められているが、その構成員は課室長以上となっており、技術力を持った実働要員が充てられていたわけではない。さらに、厚労省と関連組織との CSIRT 連携はなされていなかった。こうしたこともあり、NISC－厚労省－機構間の情報連携及びインシデント対応に遅れを生じることとなった。

（２）機構LANシステムに対する監督体制の欠落

厚労省には、情参室、年金局事業企画課、年金局事業管理課の各課室があるが、厚生労働大臣の監督下にあるはずである機構 LAN について、どれがその監督権限があるかが不明確であり、どの課室も自らに監督権限があるとの意識がない。これでは、機構 LAN で何らかの危機的事態があったとしても適切な指揮監督ができないのはやむを得ない。

（３）情報連絡の遅延

厚労省においては、情参室に省内及び傘下の特殊法人等のサイバー攻撃に関する情報が報告されることになっている。しかし、その報告は、インシデントが収まってから書面でなされることが多く、肝心な場合には後手に回り適時適切な対応をすることができない。そのため、配置されていた CIO 補佐官の知識を十分に生かすことができなかった。今回の標的型攻撃での対応はその典型例である。

第４　再発防止策の提言

本事案は、システムの脆弱性を突いた執拗かつ組織的な標的型攻撃であり、これを防御するには、以下に述べる組織的、技術的な多層防御体制を構築して

備えなければならない。

この組織的、技術的な多層防御を行うには、一部の者だけではなく組織が一体となった体制、運用が必要である。

したがって、再発防止の具体的な方策を提言する前提として、まず、機構等の役職員全員が標的型攻撃に対する危機意識を持つことが必要である。今回の情報流出事件のもたらした結果の重大性と標的型攻撃の危険性を一部の職員だけではなく、機構全ての役職員が自分達のこととして今後も認識し続けなければならない。

次に、標的型攻撃に際しては、組織が全体となってこれに対応する必要がある。それぞれの役職員が、これは自分の仕事ではないとか、自分の担当範囲でも従来通りのパターンを繰り返して漫然と対応するような姿勢ではなく、平素から困難に際し協力し合って逃げずに対処する組織づくりを心がけるべきである。普段からまとまりを欠いた組織では、危機に対し一体となって対処することなどできるはずがない。

以下、このことを前提に、個別的な再発防止策を提言する。

1　人的体制の整備

（1）セキュリティ対策本部の設立

機構には、副理事長をトップとする形だけの情報セキュリティ体制があるが機能していなかった。早急に、十分な判断力のある最高情報セキュリティ責任者の下にセキュリティ対策本部を設立し、役職員の役割・責任・権限を明確にし、各自が自らのなすべきことを熟知し、その責務を果たせるようにするべきである。そして、専門機関などと連携し最新の情報を入手すると共に、有事の際に共同して対処できる関係を構築しておくべきである。

（2）CSIRT の設立

機構は、膨大な個人情報を取り扱っていながら、緊急時に対応すべき CSIRT を設けていない。機構内の的確な判断力を有する幹部から適任者をトップに選び、外部専門家の支援を受ける体制の CSIRT を設立すべきである。その場合、現場で作業するメンバーをも含めた機動的に動ける体制にすべきである。

（3）共有フォルダなどの個人情報の一元的管理と整理

機構の共有フォルダには、膨大な個人情報等が漫然と積み上げられ、これを一元的に管理していなかったことから、共有フォルダに保管されていた情報の調査に長時間を要し、いまだにその全容が明らかになっていない。

個人情報は、インターネットの影響から遮断し、やむを得ないものは分割して厳格に管理すべきである。その際、現場の実情を理解し守れる規則を作るとともに、作った規則は必ず職員に守らせることが必要である。

（4）教育訓練の徹底

サイバー攻撃の端緒を把握するのは、PC 端末を扱う者全てにその機会があるから、そのポストを問わず教育訓練の実施が必要である。特に幹部には、リスク管理や危機管理の在り方などのセキュリティマネジメントの教育研修を、その他の職員には疑似メールなどによる実践的な訓練が必要である。

（5）外部監査の実施

独立した専門家による情報セキュリティ監査を行う必要がある。内部の監査機能が不十分である以上、外部の目で問題点を発見するのは民間では当然のことである。また、一連の再発防止策を講じた段階で保証型セキュリティ監査を受けることが望ましい。

（6）明確な情報セキュリティポリシーなどの策定

機構の情報セキュリティポリシーや手順書は、標的型攻撃を予測したものではなかった。このことが今回の攻撃に対し、適切な対応ができなかった一因でもある。速やかに標的型攻撃に備えた明確で活用しやすい情報セキュリティポリシーや手順書を策定すべきである。

2　厚生労働省の監督体制の整備

（1）厚労省の情報セキュリティ体制の整備

厚労省の情報セキュリティの中心となるべき情参室が弱体であることは、既に指摘したが、充て職で形式的な現在の情報セキュリティ体制を専門家をアドバイザーとして加えた機能し得る体制に改めること、セキュリティ情報が集中する情参室を質量ともに充実すること、CIO 補佐官との連携を図ること、CSIRT も技術力を持った実用的なものに改めることなどは着実に実行すべきである。

（2）機構 LAN システムに対する監督部署の明確化

今回標的型攻撃を受けた機構 LAN システムについて、厚労省内部で担当部署が不明確であることは、監督省庁としてあり得ないことである。速やかに担当の課室を明確にし、責任を持って対応に当たらせるべきである。

（3）情報連絡の迅速化

今回に限らず、省内及び傘下の特殊法人等からのインシデント発生後の連絡が遅延しているが、標的型攻撃に対しては迅速な対応が必須である。インシデント発生後直ちに情参室に第一報が入り、それが速やかに最高情報セキュリティアドバイザー等の専門家に通報され、指導を受けるように改めるべきである。

3　技術的観点からの提言

（1）業務の実態とリスクに基づいたシステムの整備

実効性のある技術的対策を行うには、まず業務の実態に基づいて情報セキュリティ上のリスクを的確に把握することが必要である。標的型メールを受けるおそれのある業務、大量の個人情報を取り扱う業務、一般事務など、きめ細かな視点でリスクを評価する必要がある。

その上で、このリスク評価の結果に基づき、リスクに応じたネットワークの区画分割を行い、それぞれの業務内容に応じた対策を講じるべきである。その場合、少なくとも個人情報をインターネットに接続した区画に置くことは避けるべきであり、区画をまたがる通信に関しては不正を検知または阻止できる仕組みの導入が必要である。

また、インシデント対応や保守に伴うシステム停止が他の業務に大きな影響を与えないよう、システム設計の段階から配慮がなされるべきである。特に、単一障害点の存在は、それ自身が大きなリスクを抱えるばかりでなく、サイバー攻撃への対応が困難になることから、設計段階から単一障害点を設けないように注意すべきである。

サイバー攻撃は日々高度化していくことから、定期的にリスクの見直しを行い、セキュリティ対策の継続的な改善を図っていくべきである。

（2）防御力を高めるための運用管理の徹底

技術的対策を実効性のあるものにするためには、システム整備と共に防御力を高めるための運用管理を徹底することが不可欠である。新たな攻撃手法に関する情報を常に収集し、運用における技術的な対応をより迅速に行えるようにすべきである。

機構 LAN システムの運用管理においては、脆弱性管理の不備とシステム監視の不十分さにより、被害の深刻化を招いた。脆弱性管理においては、管理者権限を適切に管理するとともに、機構 LAN システムに係わる脆弱性情報の適時適切な収集を行い、重要な脆弱性が確認された場合には、速やかに対応の必要性を判断し、セキュリティパッチを適用することが可能な運用体制を構築すべき

である。また、サイバー攻撃による外部からの侵入を想定した監視内容や監視方法を定め、異常を即座に検知するための監視体制の構築が必要である。

4　日本年金機構の意識改革

前段でも指摘したように、これらの再発防止策は、機構の役職員が今回の事件に正面から向き合って危機意識を持ち、組織が一体となって対応することが前提である。

しかしながら、今回の検証を通じて見た限りにおいて、残念ながらまとまりと自覚を欠いた姿が目に付いた。これだけの情報を流出して国民に多大の心配をかけていながら、検証委員会の調査を受けるに際し、その後改まったとはいえ、一部の者が重要な資料を出し渋り、墨塗りをするなどの態度は論外である。

年金制度に対する国民の信頼を回復するためにも、これを機会に徹底的な意識改革が必要であると考える。

第5　終わりに

今回の機構に対する標的型攻撃は、まれにみる組織的かつ執拗な攻撃であったが、これに対する機構と厚労省の備えは極めて脆弱であり、結果として大規模な情報流出をもたらし国民の信頼を失墜した。しかし、現在のIT時代において、標的型攻撃を含むサイバー攻撃があるからといって今さら紙媒体の時代に戻ることはありえず、この種攻撃を防御するために攻撃者の偵察・侵入・情報収集・情報窃取など各段階において、体制的かつ技術的な多層防御によりこれに備える必要がある。

標的型攻撃を含むサイバー攻撃は、このところ極めて組織的かつ巧妙化している。今回の事例は、単に機構だけの特殊な問題として捉えるのではなく、官民を問わず全ての組織が、この種の攻撃に対しあらかじめどのような備えができているか、攻撃があった場合に具体的にどう対応するかを真剣に考える契機として生かすことができれば幸いである。

参考　IT用語の解説

英	C&Cサーバ（Command and Controlサーバ）	あらかじめ乗っ取ったコンピュータに対し、サイバー攻撃等に関する命令を送信してこれを制御する、乗っ取ったコンピュータから得た情報を受信する等の役割を果たしている外部のサーバ。C2サーバともいう。
	CIO（Chief Information Officer）	組織全体における情報システムや情報流通に関する事項を統括する最高責任者。
	CSIRT（Computer Security Incident Response Team）	セキュリティインシデントに対応するための組織。平時はインシデント情報等の収集・分析とそれに基づく対応方針・手順の策定にあたり、インシデント発生時には緊急対応を担う。
	GETメソッド	HTTP通信又はHTTPS通信（いずれも、Webブラウザ等のクライアントとサーバの間で行われる通信の仕組み。）において、クライアントがサーバに送信する命令文の種類の一つ。一般的にはサーバから情報を取得する目的で用いられるが、サーバに対し情報を送信する目的で利用することも可能である。
	LAN（Local Area Network）	同一施設内にあるコンピュータや通信機器、プリンタ等の機器を接続し、情報をやり取りするネットワーク。
	OS（Operating System）	機器の制御機能や他のソフトウェアが共通して利用する機能等を備えた、システム全体の基本となるソフトウェア。
	POSTメソッド	HTTP通信又はHTTPS通信において、Webブラウザ等のクライアントがサーバに送信する命令文の種類の一つ。一般的にはサーバに対し情報を送信する目的で用いられる。
	URLブロック	URL（インターネット上の情報の位置を特定するための書式）に特定の文字列を含む通信先との間の通信を遮断する措置。
あ	インシデント	情報セキュリティインシデントのこと。コンピュータシステムのセキュリティに脅威を及ぼし、又はその可能性のある事象。
	ウィルス	マルウェアの一種で、自己伝染機能（他のシステムやプログラムに伝染する）、潜伏機能（時間、起動回数等の条件が揃うまで症状を出さない）、発病機能（情報の送信や破壊等の被害を生じさせる）のいずれかの機能を持つもの。広義ではマルウェア全般をウィルスと呼ぶこともある。
	オンラインストレージサービス	インターネット上でファイル共有のための領域を提供するサービス。
か	クライアント	コンピュータネットワークにおいて、他のコンピュータ（サーバ）に対して情報処理サービスの提供を求め、その提供を受けるコンピュータ・ソフトウェア。
さ	サーバ	コンピュータネットワークにおいて、他のコンピュータ（クライアント）からの求めに応じて何らかの情報処理サービス（ファイルの提供等）を行うコンピュータ・ソフトウェア。

	脆弱性	ソフトウェア等に存在するセキュリティ上の欠陥。サイバー攻撃に際し悪用される危険がある。
	セキュリティソフト	マルウェアの検出・駆除その他の情報セキュリティに関する機能を提供するソフトウェア。
	セキュリティパッチ	完成したソフトウェアにおける、既知の脆弱性への対応等の変更点を収録したファイル。
た	単一障害点	コンピュータシステムにおいて、その箇所が毀損した場合にシステム全体の機能が損なわれることとなる箇所。
	定義ファイル	マルウェアに関する情報を収録したファイル。セキュリティソフトがマルウェアを検出するために用いる。パターンファイルとも呼ばれる。
	ディレクトリサーバ	コンピュータネットワークにおいて、ID、パスワード、メールアドレス等の個々のユーザーに関する情報や、ユーザーごとのアクセス権限の設定等を一元管理するサーバ。コンピュータネットワーク内の機器（コンピュータやプリンタ等）に対してプログラムを自動的に導入する機能も持つ。
	ドメイン	インターネット上の個々のネットワーク等を識別する名前。同一ドメイン内のより小さな単位を識別する名前をサブドメインと呼ぶ。
	トロイの木馬	マルウェアの一種で、正体を偽ってコンピュータへ侵入し、データの消去・流出、他のコンピュータへの攻撃等の不正な命令を実行するもの。ウィルスと異なり、自己増殖はしない。
は	バックドア	コンピュータやサーバ、コンピュータネットワークの内部に、ID・パスワードによる認証等の正規の手続を踏むことなく侵入することができる「裏口」のこと。マルウェア（特にトロイの木馬）によって設置されることがある。
	抜線	ケーブルを抜き取る等の物理的な方法で、機器とコンピュータネットワークとの間の接続を完全に遮断すること。
	ファイルサーバ	コンピュータネットワークにおいて、ファイルを共有するためのサーバ。
	フォレンジック	デジタルフォレンジックのこと。コンピュータやネットワークシステムに残されたデータ等を詳細に解析・復元し、過去に行われた情報処理や通信等に関する事実を究明する作業。
	プロキシサーバ	コンピュータネットワーク内部のコンピュータがインターネットに接続する際に、間に入って通信を中継するサーバ。プロキシサーバを経由することによって、コンピュータネットワーク内部の個々のコンピュータに関する情報を外部に知られることなく通信を行うことができ、コンピュータネットワーク内部への不正アクセス等のリスクを減少させることができる。
ま	マルウェア	不正・有害な動作を行う意図で作成された、悪意のあるソフトウェアの総称。何らかの不正な命令を実行したり、外部への通信を行ったりする。サイバー攻撃の主要な手段。

ら	ログ	コンピュータやソフトウェアが、その起動や停止、設定変更、処理した情報や通信に関する内容、処理結果、エラーの有無内容等を自動的に時系列で記録したもの。