産総研の情報システムに対する
不正なアクセスに関する報告

2018 年 7 月 20 日

国立研究開発法人 産業技術総合研究所

要　約

産総研の情報システムに対する不正なアクセス に関する報告（要約）

2018 年 7 月 20 日
国立研究開発法人 産業技術総合研究所

1. はじめに

本報告書は、2018 年 2 月 6 日に明らかになった、国立研究開発法人 産業技術総合研究所（以下「産総研」という。）の情報システムに対する外部からの不正なアクセスについて、被害状況、原因等について整理するとともに、今後講じるべき情報セキュリティ対策を取りまとめたものである。

本報告書の作成に当たっては、外部有識者を中心とする「情報システムに対する不正なアクセスに関する調査委員会」を設置し、産総研が調査・整理した事実関係を基に同委員会の議論・審議を経て取りまとめられた。

2. 事案の概要

2.1. 不正なアクセスの概要

産総研の主たる情報システムである

① クラウドサービスを利用するメールシステム
② 独自に構築する内部システム

の双方に順次不正なアクセスが行われ、

① 職員のログイン ID の窃取
② パスワード試行攻撃によるパスワード探知
③ 職員のログイン ID・パスワードを用いた、内部システムへの不正侵入
④ 内部システムのサーバの「踏み台」化
⑤ メールシステム及び内部システムの複数のサーバに保管したファイルの窃取又は閲覧

といった一連の不正行為が行われた。

2.2. 事案への対応

事案の発見後、直ちに、業務システムの停止とインターネット接続の遮断を行い、重要業務システムの復旧を優先させた上で、被害状況の調査と原因分析を実施した。

2.3. 情報漏えいの状況

不正なアクセスにより、

① 未公表の研究情報 120 件
② 共同研究契約等に関する情報 約 200 件
③ 個人情報を含む文書 約 4700 件
④ 全職員の氏名・所属
⑤ 143 アカウント分の電子メール及び添付文書

等が、外部へ漏えい又は閲覧された可能性がある。ただし、これらには機密性３情報（秘密保全の必要性が高く、その漏えいが国の安全又は利益に損害を与えるおそれがあるもの、研究所の業務及び利益に重大な損害を与えるおそれがあるもの等）は含まれていない。

情報漏えいに関係する外部機関等へは、本事案の経緯を説明し謝罪した。

3. 不正なアクセスの手口

3.1. 侵入者の特徴

不正なアクセスの接続元は、

① その多くが海外の IP アドレス

② 活動の時間帯は、月曜から金曜の 16 時半頃から深夜 2 時頃

であり、同一者（又はグループ）によるものと推定している。

3.2. メールシステムへの不正なアクセス

侵入者は、以下の 2 回の攻撃を通じて、ID・パスワードを入手するとともに、メール及びその添付ファイルを窃取又は閲覧した。

○ 第 1 次攻撃

実施時期 ： 2017 年 10 月 27 日～ 12 月末

特　　徴 ： 初期は ID が不明のまま ID とパスワードの両方を探索
11 月以降は職員の ID を特定した上でパスワード試行攻撃

○ 第 2 次攻撃

実施時期 ： 2018 年 1 月 23 日以降

特　　徴 ： 職員の認証用データベース（LDAP サーバ）への不正検索

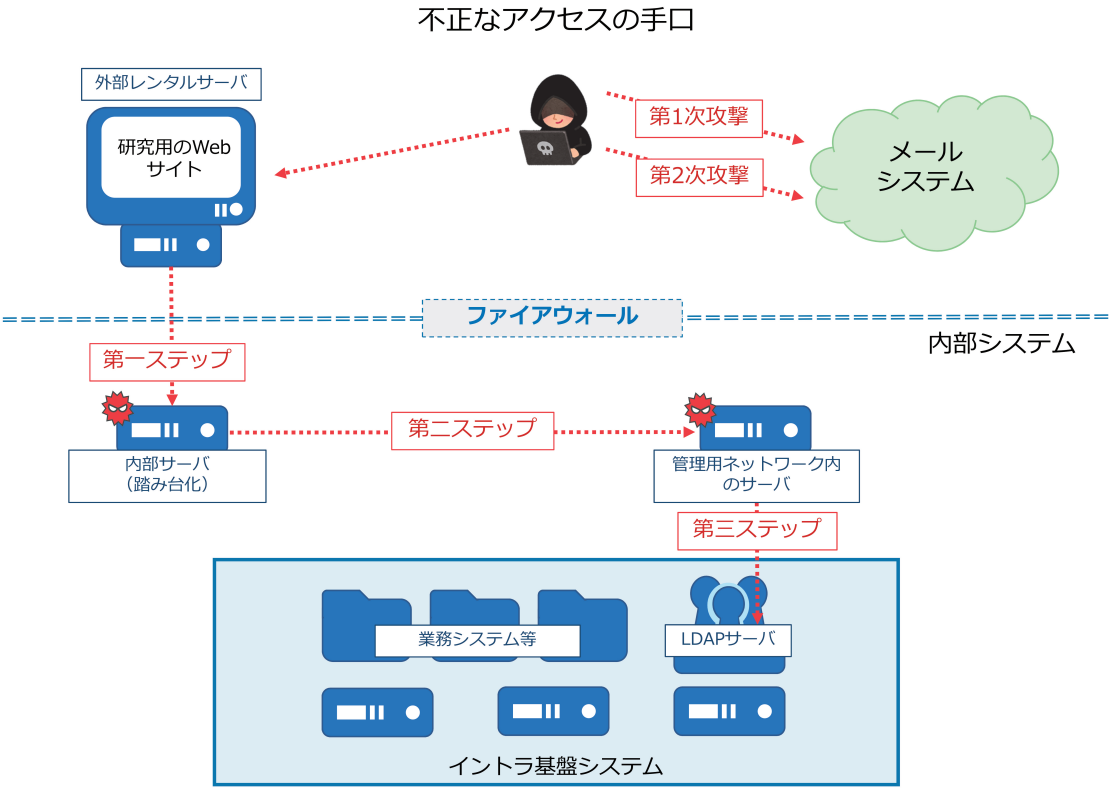
3.3. 内部システムへの不正なアクセス

侵入者は、以下のステップを踏みながら、管理者権限を窃取し、サーバ内のデータを窃取又は閲覧した。

第一ステップ：外部のレンタルサーバ上に設置していた研究用の Web サイトを通じて、内部の OS を遠隔操作。マルウェアを内部サーバに置き、このサーバを踏み台化。

第二ステップ：この踏み台サーバを介して、管理用ネットワーク内のサーバに接続し、外部から遠隔操作。

第三ステップ：管理用ネットワーク内にあった他のサーバより職員のアカウント情報を窃取。



4. 被害を発生・拡大させた要因

主な要因は以下のとおり。

① システム・機器の問題
- メールシステムのログイン方法
- 内部サーバと連携していた外部サイト
- 広域でフラットな内部ネットワーク
- 内部ネットワークの不十分な監視
- アクセス制限のなかった管理用ネットワークのサーバの存在
- 情報機器の脆弱性

② パスワード・暗号鍵の管理と強度の問題

③ 外部委託業者の管理の問題

④ マネジメントの課題

5. 再発防止のために今後取り組む対策

上記要因を踏まえ、既に応急的対策は実施したが、今後更に以下のとおり再発防止策を講じる。

○ 多要素認証の導入

メールシステム及び内部システムのログインに、多要素認証を導入する。

○ 内部ネットワークの分離と監視強化

研究用ネットワークと業務用ネットワークを分離するとともに、内部通信の監視を強化する。

○ パスワードの設定方法等の運用ルールの見直し

有効なパスワードの設定方法や、重要情報の管理、情報端末の管理等について、運用ルールを見直し、職員に周知徹底する。

○ 外部委託の運用改善

最低価格落札方式から総合評価落札方式へ切り替え、より能力の高い業者を選定するとともに、一括契約によって外部委託事業者の数を減らす。

○ 組織体制の見直し

CISO（Chief Information Security Officer：最高情報セキュリティ責任者）の下に、情報セキュリティ対策部署を明確に位置づけて、不正なアクセスへの対策を強化するとともに、各研究部門にセキュリティチームを設置し CSIRT（Computer Security Incident Response Team）との連携によって情報セキュリティリスクの低減を図る。

○ 事業継続計画の見直し

情報セキュリティインシデントの深刻度に応じた事業継続計画及び緊急時対応計画を立案する。

本　文

目　次

1. はじめに

本報告は、2018 年 2 月 6 日に明らかになった国立研究開発法人 産業技術総合研究所（以下「産総研」という。）の情報システムに対する外部からの不正なアクセスについて、事案発生からの経緯、判明した被害の状況及び侵入経路等と被害の原因等について整理するとともに、今後、産総研が講じるべき情報セキュリティ対策を記載したものである。

あわせて、調査を通じて得られた内容及び教訓を明らかにすることにより、我が国の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。

本報告書の作成に当たっては、外部有識者を中心とする「情報システムに対する不正なアクセスに関する調査委員会」（以下「調査委員会」という。）を設置した。産総研が調査･整理した事実関係を基に、同委員会での議論･審議を経て、本報告書は取りまとめられた。

2. 事案の概要

本事案は、2017 年 10 月 27 日から 2018 年 2 月 10 日の間、産総研の情報システムが、継続的に外部から不正なアクセスを受け、クラウドサービスを利用するメールシステム及び独自に構築する内部システムの双方に順次侵入されたものである。産総研が本事案を認知したのが同年 2 月 6 日であったため、その時までに広範にわたる被害が生じていた。

主な被害、侵入者による不正行為は以下のとおりである。

- 143 名の職員アカウントの窃取（電子メール及び添付文書等の外部へ漏えい又は閲覧された可能性を含む）
- パスワード試行攻撃によるパスワード探知
- 職員の ID・パスワードを用いた内部システムへの不正侵入
- 内部サーバの踏み台化

これらによって侵入者に窃取又は閲覧された可能性のあるデータには機密性 3 情報（産総研情報セキュリティ規程（29 規程第 13 号。以下「情報セキュリティ規程」という。）に定める、秘密保全の必要性が高く、その漏えいが国の安全又は利益に損害を与えるおそれがあるもの、研究所の業務及び利益に重大な損害を与えるおそれがあるもの等）は含まれていなかった。

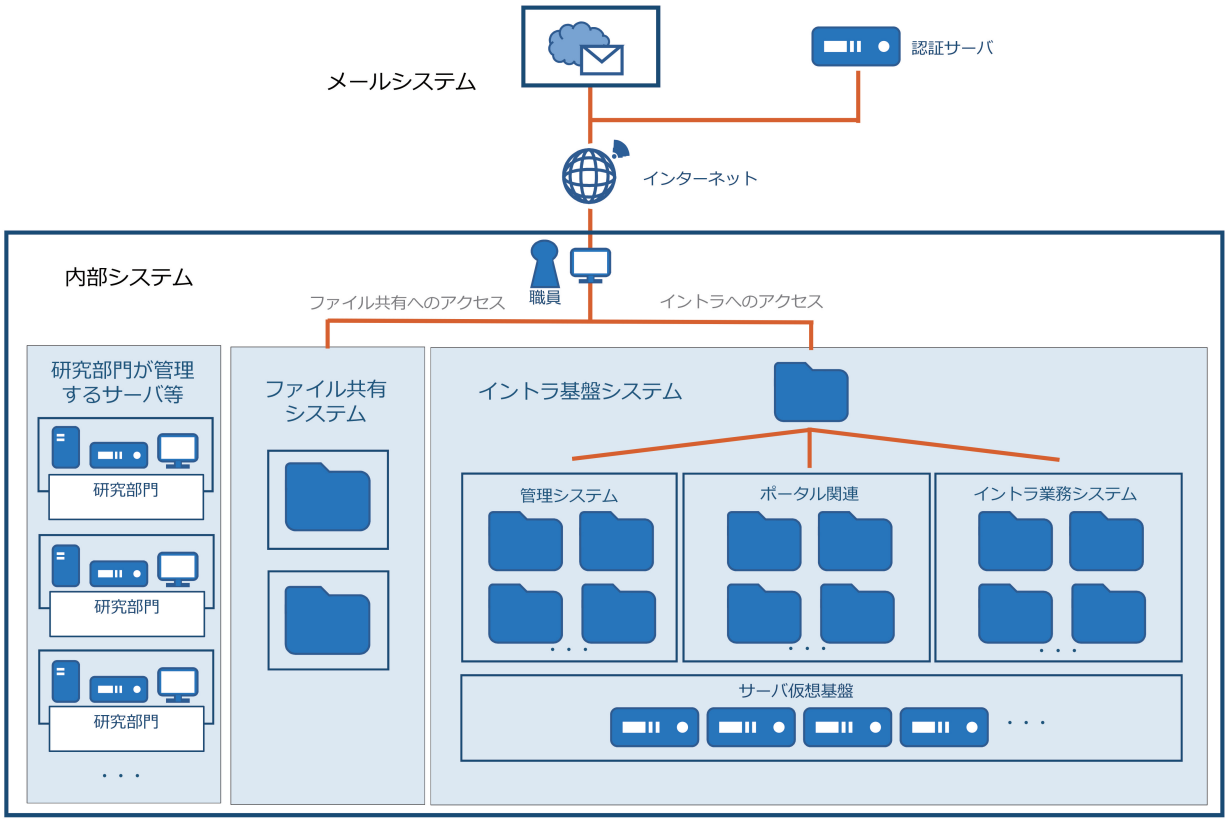
また、情報漏えいに関係する外部機関等には、本事案の経緯を説明の上、謝罪した。

本事案への対処として、被害拡大の防止のため、一時、ほぼ全ての業務システムを停止させ、外部へのインターネット接続を遮断した。業務を継続するために、業務システムのうち重要なものから順に復旧作業を進めることを優先しつつ、被害状況の調査と分析を実施してきた。主要な業務システムは 2018 年 3 月 28 日までに、インターネット接続は同年 4 月 1 日までに再開した。

3. 産総研の情報システム及び情報セキュリティ管理体制の概要

3.1. 全体構成

情報システムの全体概要（2018 年 1 月末現在）を下図に示す。



情報システムの主な特徴は以下のとおりである。

- ○ 産総研の情報システムは、メールシステムと内部システムの２つから構成される。
- ○ 内部システムは、イントラ基盤システム、ファイル共有システム、研究部門が管理するサーバ等で構成される。
- ○ イントラ基盤システムの中のイントラ業務システムは、知財管理や財務会計等の、研究所の運営・管理に必要な数十種類の独立したシステムであり、管理システム等とともに、一つのサーバ仮想基盤上で稼働している。また、イントラ基盤システムを管理するネットワークとして、研究用ネットワークや業務用ネットワークとは別に管理用ネットワークを有している。
- ○ 研究実施に必要なサーバ等は、各研究部門が管理している。所全体で数千台のサーバ等を保有しており、うち、数百台が共同研究や知財等の重要な研究情報を含むサーバである。

3.2. メールシステムの概要

- ○ メールシステムは外部のクラウドサービスを利用している。
- ○ 同システムには個人用のファイル保存フォルダがあり、アクセス許可設定を追加すれば、別アカウントからもフォルダ内のファイルを閲覧することができる。また、同システムには共有フォルダのサービスも付随している。
- ○ 同システムのユーザ認証は、外部に構築した認証サーバ経由で行っており、当該認証サーバは内部システムの認証システムと常に同期させている。

3.3. 内部システムの概要

- ○ イントラ業務システム及びファイル共有システムは、内部システムに構築した認証システムにより、メー

ルシステムと同一の ID・パスワードで利用できる環境となっている。

○ ファイル共有システムは、所属する部署のフォルダのみ利用可能なようにアクセス制限しているが、アクセス許可の設定を追加すれば、部署をまたいでのフォルダの共有も可能である。

○ 内部システムは原則として所内での利用を目的としているため、所外で利用するには、別途支給されるセキュリティトークン（ワンタイムパスワード生成器）を使用した二要素認証による VPN 接続を経由する必要がある。

○ 内部と外部との通信はファイアウォールにより常時監視している。

3.4. 情報システムの運用・保守・管理

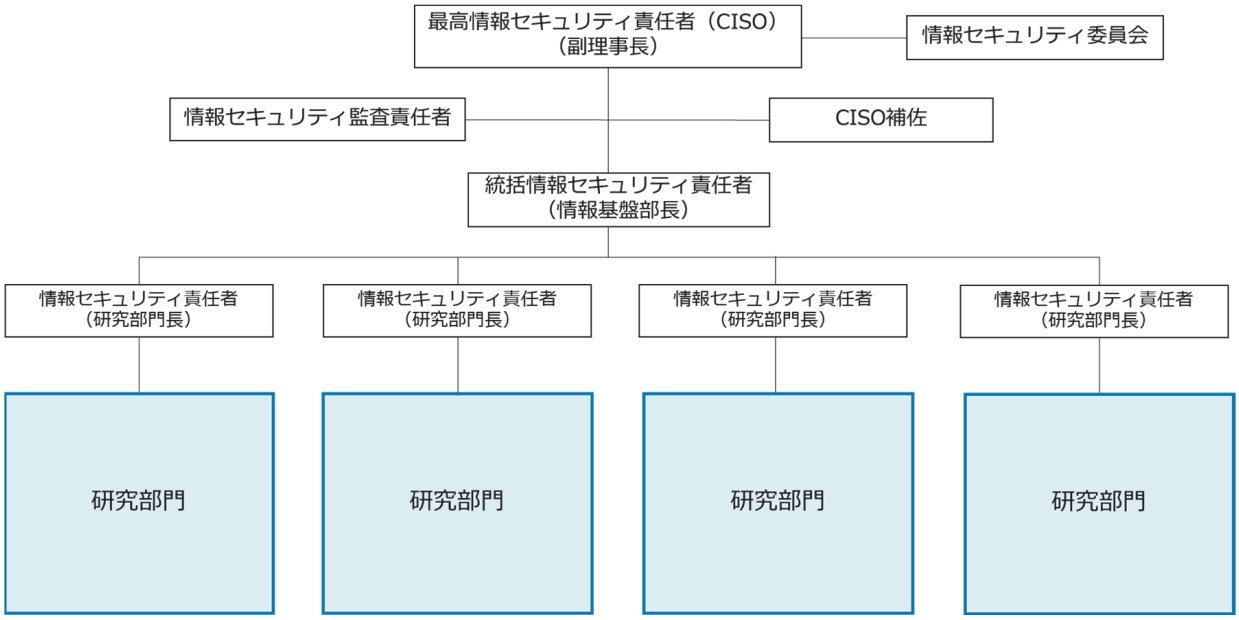
○ 研究部門が管理するサーバ等を除き、情報システムの運用・保守・管理の大部分は複数の外部業者へ委託しており、これらの業者が産総研のサーバ等を利用して実施している。

○ 主な委託業務は以下のとおり。

- 統合ネットワーク監視
- ネットワークの運用・保守
- ファイル共有システムの運用・保守
- サーバ仮想基盤の運用・保守
- イントラ業務システムの運用・保守
- 認証サーバの運用・保守

3.5. 情報セキュリティ管理体制

情報セキュリティ管理体制（2018 年 1 月末現在）は下図に示す。



3.5.1 マネジメント体制

産総研では、本部（情報基盤部）と現場（研究部門：約 50）が、情報セキュリティマネジメントを分担する、いわゆる分権型のガバナンス構造を有している。分担の考え方は、各研究部門の長が責任をもって自らの技術情報を守るための情報セキュリティ体制を推進するとともに、これら研究部門を支えるために情報基盤部にて一元的な情報セキュリティマネジメントを行っている。

○ 本部（情報基盤部）

「最高情報セキュリティ責任者（CISO：Chief Information Security Officer：副理事長）」の指揮・監督の下、「統括情報セキュリティ責任者（情報基盤部長）」が産総研の情報セキュリティ全体を統括管理する。主な役割は以下のとおり。

- 政府統一基準に基づく情報セキュリティ規程・実施要領・ガイド等の策定

- セキュリティ情報の所内周知
- ファイアウォールの通信監視
- 情報セキュリティインシデントへの対処
- 研究部門の外部ネットワーク接続の事前確認
- 固定 IP アドレスの発行
- 情報セキュリティ監査及び情報セキュリティ委員会の事務局等

○ 現場（各研究部門）

「情報セキュリティ責任者（研究部門長）」が各研究部門内の情報セキュリティに関する全ての監督と責任を負う。主な役割は以下のとおり。

- 職員の情報機器の調達・管理
- PC 端末の持ち込み・持ち出し承認
- OS のバージョン更新
- メール誤送信の防止
- 情報の保管
- 外部ネットワーク接続サーバ等のセキュリティ対策・運用管理等

○ 情報セキュリティ委員会

CISO を長とし、外部有識者を加えた委員会を設置し、産総研の情報セキュリティ対策に係る方針やルール、情報セキュリティ監査の内容等について審議・決定する。年 3、4 回程度開催する。

3.5.2 非常時の体制

○ 連絡体制

研究部門において情報セキュリティインシデントが発生した際には、情報セキュリティ責任者（研究部門長）から統括情報セキュリティ責任者（情報基盤部長）へ報告し、統括情報セキュリティ責任者が必要な措置を研究部門へ指示・伝達する。

○ CSIRT（Computer Security Incident Response Team）

統括情報セキュリティ責任者を長とし、情報セキュリティインシデントに速やかに対処する体制（CSIRT）を整備している。情報セキュリティに関する専門的な知識又は適性を有する職員等で構成され、NISC、JPCERT/CC 等の外部機関と密に連携している。

○ 情報セキュリティ対策本部

統括情報セキュリティ責任者を長とし、重大な情報インシデントの発生時に組織する。CSIRT メンバーに加え、関係省庁との連絡調整及びプレス対応のため、企画本部の職員を招集する。

3.5.3 情報セキュリティ監査

情報基盤部が監査室とともに情報セキュリティ対策に関する専門の業者に委託して、研究部門等に対して実施する。監査計画は実施前に情報セキュリティ委員会で承認を得ることとしている。監査結果は研究部門へ伝達され、速やかに必要な措置を講じるよう求めるとともに理事会へ報告している。

○ マネジメント監査

- 情報セキュリティ責任者（研究部門長）に対して隔年で実施。
- 情報資産についての台帳整備等の管理状況、教育・自己点検等の実施状況、情報システムのセキュリティ対策の実施状況等を確認。

○ セキュリティ診断

- 外部ネットワークへ接続している全てのサーバ等に対して毎年実施。
- ポートスキャン、脆弱性攻撃診断、セキュリティパッチの適用確認等を実施。

4. 事案の経過

以下に事案発見以降の主な経過を記載する。

4.1. 発見から初動対応まで

【2018 年 2 月 6 日（火)】

○ 産総研の情報システム管理を担当する職員（SE）が、自身のメールシステムに対し自身が通常使用しない地点の IP アドレス（国内の特定大学）からログイン履歴があることを偶然発見。さらに、当該 IP アドレスと国外の IP アドレスから、メールシステムへ不正なアクセスが複数（41 アカウント）あることを発見した。

○ 直ちに CSIRT から理事長、最高情報セキュリティ責任者（CISO：副理事長)、産総研幹部へ緊急連絡し、さらに経済産業省へ連絡を行った。

○ 当日、以下の緊急対応を実施した。

- 上記 SE のアカウントを含め、不正ログインされていた 41 アカウントについて、パスワードを強制的に変更。
- 内部ネットワーク以外からのメールシステムへのアクセスを遮断。
- 外部委託業者、外部機関（JPCERT/CC（8.2 参照）等）へ連絡。

4.2. 情報セキュリティ対策本部の設置

【2 月 7 日（水)】

○ 本事案に全所的に対応するため、「情報セキュリティ対策本部」を設置（添付 1：情報セキュリティ対策本部体制図)。第 1 回「情報セキュリティ対策本部会議」を開催し、以下の方針を決定した。（なお、対策本部会議は合計 32 回開催。）

- 本事案に関して事実関係の把握と整理を行う。
- 被害範囲を推定するとともにその影響について評価する。
- 外部機関（経済産業省等）への報告について、内容・方法等を検討し実行する。

4.3. 情報セキュリティ対策本部設置後の対応

【2 月 8 日（木)・9 日（金)】

○ 内部システム（イントラ業務システム、ファイル共有システム）への不正なアクセスが確認された。

○ 以下の緊急対応を実施。

- 全職員の内部システム用ログインパスワードを強制変更。
- イントラ業務システム及びメールシステムの大半の機能を停止。

○ 外部機関（NISC（8.1 参照)、警視庁等）と連携し、被害の範囲、侵入経路等について分析を開始した。

【2 月 13 日（火)】

○ 被害の拡大防止のため、外部へのインターネット接続を遮断した。

○ 産総研 HP にて本事案を公表した。

【2 月 23 日（金)、24 日（土)】

○ 全ての内部システムのネットワーク機器の初期化を完了した。

○ 安全が確認できたネットワーク機器及び端末を利用して、優先度、緊急度の高いイントラ業務システム（財務会計システム、出勤簿システム）を再開した。

【2 月 28 日（水）～ 3 月 9 日（金)】

○ 外部接続している研究部門（X 研究センター）のサーバに、不正な通信中継の痕跡があったことを確認した。これが、内部システムへの不正なアクセスの足掛かりとなった可能性が浮上した。

○ メールシステムの 143 アカウントへ不正ログインがあったこと、個人用フォルダ / 共有フォルダからファイルがダウンロードされていたことが判明した。

【3 月 28 日（水）】

○　ファイアウォールの監視強化のため、現行の外部委託業者に加え、別の業者による監視を追加した。

○　インターネット接続を日中のみ再開した。

○　主要なイントラ業務システム（全体の約 8 割）を再開した。

【4 月 1 日（日）】

○　夜間についても、インターネット接続を再開した。

【4 月 6 日（金）】

○　警視庁へ被害届を提出した。

【4 月 10 日（火）】

○　外部有識者による調査委員会を設置した。

【4 月 25 日（水）、5 月 9 日（水）、5 月 18 日（金）、5 月 29 日（火）、6 月 14 日（木）】

○　調査委員会を以下のとおり 5 回開催。（添付 2：調査委員会委員一覧）

【第 1 回調査委員会】　4 月 25 日（水）

(1)　本件事案の経過説明

(2)　不正なアクセスの原因の推定に関する審議

(3)　本件に関する被害の経過報告

(4)　再発防止のための抜本的対策に関する検討、審議

(5)　報告書（案）の構成に関する検討

【第 2 回調査委員会】　5 月 9 日（水）

(1)　不正なアクセスに関する被害調査の報告

(2)　不正なアクセスの原因の推定に関する審議

(3)　再発防止のための抜本的対策に関する審議

(4)　報告書（案）に関する審議

【第 3 回調査委員会】　5 月 18 日（金）

報告書（案）に関する審議

【第 4 回調査委員会】　5 月 29 日（火）

報告書（案）に関する審議

【第 5 回調査委員会】　6 月 14 日（木）

報告書（案）の承認（書面審議）

5. 被害の状況

5.1. 不正なアクセスの概要

本事案は、2017 年 10 月 27 日から 2018 年 2 月 10 日の長期にわたり、継続的に外部から不正なアクセスを受けたものであり、概要は以下のとおりである。

○　侵入者は、複数のメールアカウントに不正ログインする一方、X 研究センターが管理するサーバを踏み台化し、以下のことを行った。

- 内部システムへの侵入
- ファイル共有システムへの不正ログイン
- 研究部門が管理するサーバへの侵入
- イントラ基盤システムのサーバ仮想基盤等への侵入

- LDAP サーバ（職員の認証用データベース）の不正検索による全職員のアカウント情報の窃取。これを用いたメールアカウントへの不正ログイン

○ 本事案では、いわゆる標的型メール攻撃により端末をマルウェア感染させる手口ではなく、「ID･パスワードを用いて、外部から直接、あるいは内部システムの踏み台を通じて不正ログインする」という方法が用いられた。脆弱性を突く攻撃も一部はあったものの、主にパスワードを次々と入手又は推定・復元する手法にて内部システムの奥へと侵入した。

○ 本事案によって、侵入者は 143 名の職員が過去にやり取りしたメールを窃取又は閲覧したと推定される。また、メールシステムの個人用フォルダ / 共有フォルダ及び内部システムに置かれていたファイルを不正ダウンロードした。

5.2. 不正なアクセスの経過

○ 侵入者は、何らかの手法により 2017 年 10 月 27 日に 1 名、30 日、31 日に 8 名の職員のアカウントへ不正ログインした。

○ その直後、全職員のログイン ID を窃取し、全ログイン ID に対してパスワード試行する攻撃を開始し、11 月 1 日に 48 名、翌 2 日に 45 名、11 月 8 日に 87 名のアカウントに不正ログインした。

○ さらに 12 月末までに、新たに 7 名のアカウントに不正ログインした。この時点までに、合計 100 名のアカウントに不正ログインした。

○ パスワードを試行する攻撃は 12 月 13 日まで続き、認証サーバに不具合が発生した。この間 2 回、外部委託業者から「産総研にブルートフォース攻撃（パスワード試行攻撃の一種）が行われている。ただし、攻撃は全て失敗している。」旨の報告があった。

○ 10 月 28 日から 11 月 2 日にかけて、産総研が保有する IP アドレスの全域に対してポートスキャンがあり、これにより、外部からの所内システムの利用の際に用いる VPN の接続口を発見され、11 月 1 日から 3 日にかけてメールシステムのアカウントの一部を用いて不正接続が試みられていた。しかし、VPN サーバではワンタイムパスワード生成トークンによる二要素認証を実施していたことにより、侵入に失敗していた。その他には基本的に外部から接続できる IP アドレスは存在しないため、外部から直接侵入する方法はなかった。

○ 12 月 15 日、侵入者は X 研究センターが外部レンタルサーバと連携している内部サーバを踏み台化し、これを通じて内部システムへ侵入した。

○ 12 月 20 日から 1 月 26 日にかけて、X 研究センターの内部サーバを踏み台に、さらにイントラ業務システムに不正ログインした。イントラ業務システムの不正ログインには、メールシステムへの不正ログインに使用した ID・パスワードを利用した。また、12 月 26 日から 27 日にかけて、当該サーバからファイル共有システムへ不正ログインした。

○ 1 月 16 日、使用電力量モニタサーバに不正ログインすることで、内部システムの管理用ネットワークへ侵入した。さらに、これを踏み台として、外部委託業者のサーバへ侵入し、このサーバに置かれていた、内部システムの各種機器のパスワードを窃取し、システムの奥へと侵入が可能となった。使用電力量モニタサーバへの不正ログインには、別に不正ログインしたメールから ID･パスワードを窃取した（推定）。

○ 1 月 23 日、職員のアカウント情報を検索できる LDAP サーバを不正に検索し、職員のアカウント情報を窃取し、一部のアカウントのパスワードを復元した（推定）。1 月 23 日から 2 月 5 日にかけて、43 名のメールアカウントへ不正ログインがあった。これには上記 LDAP サーバから窃取された情報が利用された（推定）。

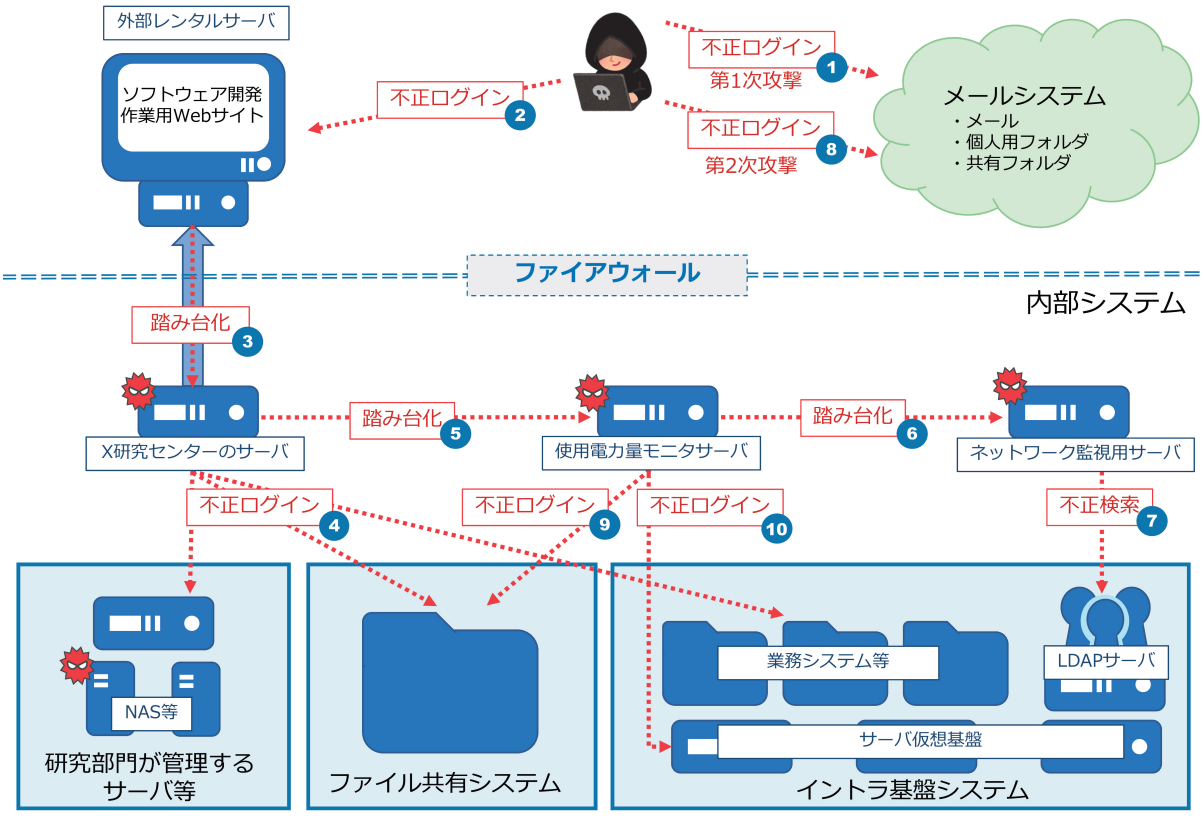
○ 1 月 26 日から 2 月 5 日にかけて、使用電力量モニタサーバからファイル共有システムへ不正ログインした。

○ 1 月 30 日、イントラ基盤システムのサーバ仮想基盤の管理コンソールへ不正ログインした。

○ 2 月 9 日、ファイル共有サーバ 3 台のうちの 1 台に、管理者アカウントで接続した。

○ 同日、管理用ネットワークの踏み台としていた使用電力量モニタサーバ上の痕跡を削除した。（同サーバ上にコピーしたファイルやイベントログを削除。）

不正なアクセスの侵入経路概略図



5.3. 侵入経路と被害の原因

5.3.1 侵入者の活動の特徴

○ 不正なアクセスの接続元として、最初に発覚したのは国内の特定大学の IP アドレスである。それ以外は、いずれも海外の IP アドレスであり、その総数は 155 個に及んでいる。

○ 侵入者がどの国又は地域から攻撃を行っていたかは定かでないが、その活動パターンに明確な特徴が見られ、侵害イベントの発生時刻は、日本時間の月曜から金曜の 16 時半頃から深夜 2 時頃までに収まっている。

○ また、Web ブラウザによる不正なアクセスでは、特定の種類のブラウザを継続して使用しており、同時に複数の Web ブラウザが用いられることはなく、多くの場合一つ又は二つの Web ブラウザを同時に使用していた。

○ これらのことから、一連の侵害イベントは同一者によるものである可能性が高く、実行者は 1 名か数名程度と推定できる。

5.3.2 メールシステムへの不正なアクセス

被害アカウントの特定は、約 8 か月分のログイン履歴から目視確認を含めて集計する方法で行った。

○ 被害アカウントは、パスワード試行攻撃等が原因と考えられる第 1 次攻撃（100 名分、2017 年 10 月 27 日～ 12 月末）と、LDAP サーバへの不正検索が原因と考えられる第 2 次攻撃（43 名分、2018 年 1 月 23 日以降）によるものに大きく分けられる。（初動対応で発見した 41 アカウントは、全て第 2 次攻撃によるものであった。）

○ 第 1 次攻撃の被害アカウントの利用者に聞き取り調査を行ったところ、設定されていたパスワードは、キーボード配列をなぞっただけの安易なものが大半を占めていた。

5.3.3 内部ネットワークへの侵入

○ X 研究センターが、外部のレンタルサーバに設置していた「ソフトウェア開発作業用 Web サイト（以下「J サイト」という。）」に対して、12 月 15 日に不正ログインがあった。（J サイトは、内部ネットワークに置かれたソフトウェア開発用の複数の OS を遠隔操作する機能をもっており、OS 上の任意のコマンドを実行できる仕組みを有していた。）

○ 侵入者は、何らかの手法で J サイトの ID・パスワードを特定し、研究の作業用に設定していたアカウントに、1 月 30 日まで継続的に不正ログインした。

○ 侵入者は、J サイトに不正ログインし、内部ネットワークの 2 台の仮想マシン（内部サーバ）を遠隔操作した。

○ X 研究センターの 4 台の仮想マシンにマルウェアが置かれ、そのうち 2 台が、内部システムへの侵入の踏み台に使われた。

5.3.4 内部システムへの不正ログイン

① ファイル共有システム

○ ファイル共有システムは、メールシステムと共通の ID・パスワードで利用できたため、メールシステムへの不正ログインがあったアカウントのうち一部が、ファイル共有システムへの不正ログインにも利用された。

○ メールシステムへの第 1 次攻撃 100 名のうち 3 名のアカウントと第 2 次攻撃 43 名のうち 4 名のアカウントを用いて、X 研究センターの仮想マシン及び使用電力量モニタサーバを踏み台に、不正なアクセスを行った。

○ ファイル共有システムの所在は、それまでに閲覧されていたメールの内容から特定された（推定）。

② 使用電力量モニタサーバ

○ イントラ業務システムの管理用ネットワーク内のサーバ等は、アクセスコントロールリストにより個別にアクセス元 IP アドレスを制限しており、管理用ネットワーク外からは直接アクセスできないよう設計されていた。

○ 管理用ネットワーク内の使用電力量モニタサーバでは、このアクセス制限が施されていなかったため、これが踏み台となり、管理用ネットワーク内の各種サーバに、管理 ID・パスワードを用いて不正なアクセスが行われた（X 研究センターの仮想マシンを介して侵入したものと推定）。

○ 接続にはリモートデスクトップ（遠隔操作するための Windows の機能）が用いられた（推定）。

○ 侵入者は、第 1 次攻撃 100 名のうち 1 名のアカウントからメールを検索して、使用電力量モニタサーバの管理 ID・パスワードを窃取した（推定）。

③ 外部委託業者のサーバ

○ 1 月 16 日から 2 月 8 日にかけて、外部委託業者が構築・運用していたネットワーク監視用サーバが不正侵入された。4 台に侵入され、うち 2 台にマルウェアが置かれて、遠隔操作による他への攻撃の踏み台となった。また、当該サーバはアクセス制限されていなかった。

○ 当該サーバには、同社が運用している多数のネットワークスイッチ等の管理パスワード、及び LDAP サーバの検索用 ID・パスワードが、暗号化されずに保管されていた（それらが閲覧された可能性がある）。

④ LDAP サーバでの不正検索

○ 1 月 22 日から 2 月 8 日にかけて、上記、外部委託業者のサーバで閲覧したと考えられる ID・パスワードを用いて、管理用ネットワーク内の LDAP サーバへの検索が行われ、職員のアカウントの記録（レコード）が盗み出された。

○ LDAP サーバのレコードには、氏名、所属等の情報がある他、認証サーバのログイン ID と、暗号化され

たパスワードとハッシュ化されたパスワードが含まれており、これらを侵入者が入手した。

○ 侵入者は、オフライン攻撃によってパスワードを復元し、復元したパスワードで、第2次攻撃43名のメールアカウントへ不正ログインした（推定）。

○ 被害アカウントのほとんどは情報基盤部職員のものであった（情報システムに関する情報を更に閲覧しようと試みたと推測される）。

⑤ サーバ仮想基盤の管理コンソール

○ 1月30日、踏み台となった使用電力量モニタサーバから、イントラ基盤システムのサーバ仮想基盤の管理コンソールへ不正ログインがあった。

○ 管理コンソールからは仮想マシンの起動・停止や、ネットワークの構成変更等が可能であるが、管理コンソールから閲覧できる情報には、漏えいが問題となるような情報がなく、また、ログには不正な操作を行った痕跡はなかった。

5.3.5 NASへのマルウェア感染

○ 複数の研究部門に設置されていたネットワーク接続ハードディスク装置（以下「NAS」という。）のうち数台に、マルウェアの存在又は感染の形跡があった。これらのNASには脆弱性があることが以前から報告されており、その脆弱性を突いて内部ネットワーク経由でマルウェアに感染したものと推定される。

○ これらのNASのうち、少なくとも1台は、使用電力量モニタサーバを遠隔操作するための踏み台として利用された。

（添付3：被害範囲の特定と原因の究明に関する分析結果）

5.4. 漏えい情報の調査

以下のシステムを対象にして、漏えい情報の内容について調査を実施した。

○ メールシステム
- 不正ログインされたメールシステムのアカウント

○ 内部システム
- ファイル共有システム
- 「踏み台」となったサーバ
- 不正なアクセスを受けたサーバ及びNAS

調査方法は以下のとおりである。

○ メールシステムについては、不正ログインされた職員のアカウントを対象に、送受信していたメールや添付ファイルの内容を、未公表の研究情報、個人情報等に大別した上で、漏えい情報を集計した。

○ 内部システムについては、サーバのログ情報やファイアウォールの通信記録から漏えい情報を特定し、メールシステムと同様に集計した。

調査の結果、本事案によって、外部へ漏えい又は外部から閲覧された可能性のある情報は下表のとおりであることが判明した。

機密性	分類		詳細分類	電子メール本体及び添付ファイル※1		内部システムにあったファイル		合計
				漏えいした件数	閲覧された可能性のある件数	漏えいした件数	閲覧された可能性のある件数	
機密性2	共同研究契約等に関する情報			200	8	0	0	208
	未公表の研究情報	1	企業・他機関との共同研究等の情報	82	22	12	1	117
		2	上記に含まれない未公表の研究情報	1	0	0	2	3
	個人情報	1	採用関係書類（応募書類、履歴書）	181	18	5	0	204
		2	学会・イベント等の参加者名簿	125	10	15	15	165
		3	所内業務用の連絡先等	158	1,447	71	2,661	4,337
		4	メールアカウント	※2 83	※2 60	0	0	143

※1 個人用フォルダ／共有フォルダを含む。
※2 当該アカウントの電子メールが漏えい又は閲覧された可能性がある。
※3 上記の表以外に情報システムに関する情報及び全職員の氏名・所属等が漏えい又は閲覧された可能性がある。

○ 漏えい又は閲覧された可能性のある情報については、更に内容を精査し、未公表の研究情報については以下を確認した。

- 漏えい又は閲覧された可能性のある情報は全て機密性２であり、機密性３情報※は含まれていない。

  ※機密性３情報とは、情報セキュリティ規程において情報の機密性の観点から最高度の格付のものとして区分される情報。具体的には、産総研文書管理・決裁規程（29 規程第 43 号）において秘密文書として定める極秘文書（秘密保全の必要性が高く，その漏えいが国の安全又は利益に損害を与えるおそれがあるもの若しくは研究所外から極秘文書として提供されたもの）及び秘文書（極秘文書に次ぐ程度の秘密であって，研究所の業務及び利益に重大な損害を与えるおそれがあるもの若しくは関係者以外には知らされてはならない情報を含む極秘文書以外のもの又は研究所外から秘文書として提供されたもの）に相当する情報。
- 知的財産権の獲得に影響する情報は含まれていない。
- 企業・他機関との共同研究等の情報については、第三者が転用できない又は転用の可能性が低い情報等、いずれも今後の研究に支障のない情報のみである。

○ 共同研究契約等に関する情報等、メールで送受信したファイルは暗号化されていたが、直後のメールでパスワードを送付していた。

○ 共同研究契約等に関する情報 208 件のうち 185 件は、1 名の共同研究契約担当職員のアカウントから漏えいしたものである。

○ 所内業務用連絡先の個人情報 4337 件のうち 2653 件は、3 名の職員アカウントから漏えい又は閲覧された可能性があるものである。

○ 未公表の研究情報については、技術的な観点からは転用できない情報等のみであったこと等を確認した。

○ しかし、外部から提供された情報や個人情報が漏えいするという事態については、非常に重く受け止めている。

○ 関係する企業・外部機関、個人等へは本事案に係る経緯を説明の上、謝罪を行った。

6. 被害を発生・拡大させた要因

6.1. システム・機器の問題

6.1.1 メールシステムのログイン方法

- ○ メールシステムへのログインが外部から可能で、かつ、ID・パスワードのみで可能な設計としていたことは、被害を発生させた一つの大きな要因である。
- ○ ID・パスワードを探り当てようとするパスワード試行攻撃の兆候があったが、それを察知した際に有効な対策が打てなかった（侵入者はパスワード試行攻撃等により、10 月 27 日から 12 月末までの第 1 次攻撃で 100 名の職員アカウントに不正ログインしたと推測される）。
- ○ クラウドサービスの導入時、VPN によるアクセス制限を解除して利便性を向上させたが、十分なリスク評価を実施しなかったため、本事案のメールシステムへの不正ログインを防止できなかった。

6.1.2 内部サーバと連携していた外部サイト

- ○ X 研究センターがファイアウォールの外に設置した J サイトには、内部サーバと連携して、外部から容易に内部サーバ上の OS をコントロールできる機能（外部からの遠隔操作）があった。
- ○ J サイトのこの機能が内部ネットワークへの侵入口を開ける原因になってしまった（侵入者は外部サーバに不正ログインし、内部サーバを遠隔操作するとともに、これを内部システムの侵入の踏み台として利用したと推定される）。
- ○ この機能の危険性について、X 研究センターの認識が不足していた。

6.1.3 広域でフラットな内部ネットワーク

- ○ 内部ネットワークが広域でフラットな構成であり、研究用ネットワークと、業務用ネットワークとが切り離されていなかった。
- ○ このため、内部ネットワーク内であれば、どのサーバへも到達可能な状態にあった（侵入者は内部ネットワークへ侵入後、イントラ業務システムや複数の研究部門の NAS 等の情報機器に侵入した）。

6.1.4 内部ネットワークの不十分な監視

- ○ 統合ネットワーク監視を外部委託業者に委託し、ファイアウォールその他のログを自動検知ルールにより監視していたものの、内部システムへ侵入された後のポートスキャンを検知することができなかった。

6.1.5 アクセス制限のなかった管理用ネットワークのサーバの存在

- ○ イントラ業務システムの管理用ネットワーク内の全てのサーバは、管理機能に直接アクセスできないよう、個別のアクセスコントロールリストによるアクセス元 IP アドレス制限を行うルールになっていた。
- ○ しかし、使用電力量モニタサーバ及び外部委託業者のネットワーク監視用サーバはアクセス制限が施されておらず、踏み台として利用された。

6.1.6 情報機器の脆弱性

- ○ 情報機器のセキュリティ対策は、原則として各研究部門の責任において実施することとなっている。
- ○ 以前より脆弱性の懸念が指摘されていた NAS が、安価であること等を理由に、十分なリスク評価をせずに多くの研究部門で使用されていた。
- ○ また、一部の外部委託業者は、保守サポート期限が切れたサーバを使用していた。

6.2. パスワード・暗号鍵の管理と強度の問題

- ○ 産総研では、要機密情報については暗号化を行い、パスワードや暗号鍵は別経路で送信することとしている。
- ○ しかし、送信方法についての具体的なルールはなく、多くの場合、パスワードをメールで送信していた（侵

入者に、メール内に書かれていた管理者パスワードや、暗号鍵を窃取され、それを用いてメールの添付ファイルの閲覧や、サーバへの侵入等が行われた)。

○ 職員に対するパスワードの設定ルールは定めていたものの、キーボード配列をなぞっただけの安易なパスワードを設定していた例があった（このため、100 アカウントのパスワードを特定され、メールシステム等に侵入された)。また、管理者パスワードについても安易な設定が少なからずあった。

○ 2017 年 11 月に新たなパスワードの設定ルールを設けるとともにパスワードの強度チェッカーを導入したが、キーボード配列をなぞっただけのようなパスワードを排除するようなものではなかった。

○ LDAP サーバの検索用 ID・パスワードを含む、多数の管理者パスワードが、外部委託業者のネットワーク監視用サーバに暗号化されずに保管されていた（侵入者は、同サーバにも侵入したためこれらが閲覧され、窃用された)。

○ また、管理者パスワードその他の管理情報を暗号化するための鍵に、極めて簡単な文字列を用いており、暗号化の強度を満たしていなかった。

6.3. 外部委託業者の管理の問題

○ 外部委託業者に対しては、産総研の情報セキュリティポリシーを遵守するよう、契約における仕様書で定めている。しかし、一部の外部委託業者のサーバについては、十分なセキュリティ対策が講じられていなかった。

○ 産総研情報セキュリティ実施要領（29 要領第 15 号）では、外部委託業者の情報セキュリティ対策の履行状況を定期的に確認することとなっていたが、本事案で問題となった一部の外部委託業者については未実施であった。

○ 外部委託業者に対する監査は行っておらず、また監査の必要性についても検討していなかった。

○ 一部の業務については同一業者との契約が継続していたことから、程度や判断基準が契約書や仕様書で必ずしも明らかになっていない業務については、慣行的な運用になっていた。

○ 委託先の選定においては、最低落札価格方式の競争入札を行っているため、委託先の情報セキュリティ対策や能力等を十分に評価できるものになっていなかった。

○ 外部委託業者の数が多く（約 40 社)、管理が行き届いていなかった。

6.4. マネジメントの課題

2016 年度からは副理事長が CISO を務め、情報・人間工学領域長と環境安全本部長（情報化統括責任者を兼ねる）が CISO 補佐として CISO をサポートする体制とし、その体制の下で統括情報セキュリティ責任者である情報基盤部長を中心に情報セキュリティマネジメントを行ってきたが、今般の事案を未然に防止するには十分でなかった。

産総研は研究者約 2300 人を抱える巨大な研究所であり、約 50 の研究部門に分かれて研究を実施している。これら研究部門に、それぞれ情報セキュリティ体制を構築し、各研究部門長が情報セキュリティ責任者となって、部門内の情報セキュリティマネジメントを行っている。情報技術研究部門のように情報セキュリティ自体を研究対象としている部門も存在するが、大部分は材料やエネルギー、エレクトロニクス、生命工学、計量標準、地質等を研究対象とする部門であり、必ずしも情報セキュリティに関する知見や問題意識が高いとは言えない。また、研究部門で情報セキュリティ体制を担っているのは研究者自身であり、予算その他の制約から情報セキュリティの専門人材を各研究部門に配置することは困難である。各研究部門における研究の自由度を十分に確保する必要もある中で、可能な限り情報セキュリティマネジメントを検討し推進してきたところである。

しかし、産総研の情報セキュリティマネジメントに関して、具体的には、以下の５点で課題が存在していたものと考えられる。

＜組織・体制上の課題＞

○ 統括部署である情報基盤部に、情報技術に関する専門家の人数が不足しており、研究部門へのサポートが十分にできていなかった。

○ CISO は副理事長であり、統括情報セキュリティ責任者は情報基盤部長であるが、組織上、情報基盤部は環境安全本部の中にあり、CISO と情報セキュリティ責任者間での意思疎通の迅速性に欠けることがあった。

○ 情報基盤部の中で、情報セキュリティの担当部署が明確に分かれておらず、情報セキュリティ対策に組織的に取り組めていなかった。

○ 研究部門のセキュリティ対策において、情報セキュリティ責任者（研究部門長）のガバナンスが十分に機能していなかった。

○ 規程上、本部と各研究部門の責任分担は明確化されていたが、情報機器の調達・管理、調達した機器のネットワークへの接続承認といった具体的な行為について、連携が十分取られておらず、必要なリスクを評価できていなかった。

＜研究部門内での情報セキュリティの徹底＞

○ 情報機器の外部ネットワークへの接続に関するリスクについて、研究部門が十分に認識をしていなかった。日常的な情報機器のリスクチェック、インシデントに関する監視とその報告等が適切に行われないケースもあり、また、リスクに関する啓発・啓蒙も十分ではなかった。

＜重要情報の管理についてのポリシーと体制＞

○ 重要情報の管理についてルールはあるが、分権型ガバナンスの下、どのように管理されているかチェックが行われていなかった。パスワードの生成、管理についても、職員への指導、チェックが十分ではなかった。

＜研究部門への情報セキュリティ監査＞

○ 情報セキュリティ責任者（研究部門長）へのマネジメント監査と、外部接続サーバのセキュリティ診断を定期的に実施していたが、形式的なヒアリングや一般的な脆弱性診断に留まっており、十分ではなかった。

＜重大なインシデント事案が発生した際の体制＞

○ 日常的なインシデント対応は行われていたが、本事案のように重大なインシデントが生じた際に参照すべき事業継続計画が用意されていなかった。

7. 再発防止のための対策

「6. 被害を発生・拡大させた要因」の分析・考察を踏まえ、以下に再発防止のための対策を整理する。現時点での応急的対策に加え、優先順位を考慮しつつ、抜本的な対策を速やかに講じる。

7.1. 現時点で措置済の対策（応急的対策）

① メールシステムへのログイン【6.1.1 への対策】

メールシステムへのログインについては、外部からは VPN 接続を必須とする運用とし、さらに、内部ネットワークからログインする場合でも、一定期間ごとに二段階認証を求めるよう認証方式を強化した。

② ファイアウォール内から外部へ接続するサーバ【6.1.2】

用途と通信先を精査し、必要性と安全が確認できないサーバ等は全て遮断した。

③ 管理者パスワードの作成及び保管方法、並びにファイル暗号化時の鍵の作成方法及び保管方法【6.2】

有効なパスワードの設定方法、管理方法を検討し、情報基盤部で運用開始するとともに、外部委託業者に周知・徹底した。

④ 外部委託業者の老朽化したサーバ【6.3】

老朽サーバは廃止し、最新の OS を載せた新規のサーバに交換した。

⑤ 脆弱性が指摘された NAS【6.1.6】

使用を中止し、研究部門から回収した。

⑥ 統合ネットワーク監視【6.1.4】

既に導入していた統合ネットワーク監視における SIEM の自動検知ルールを見直し、不正な通信が内部で発生した場合にもすぐに検知できるよう、内部通信の監視を強化した。

⑦ 管理用ネットワーク内のサーバのアクセス制限【6.1.3】【6.1.5】

全てのサーバにアクセス権限を設定するとともに、分離用のネットワーク機器を新たに追加し、これによって業務用ネットワークを研究用ネットワークから切り離した。

7.2. 今後取り組む抜本的対策

7.2.1 システムの強化策

新システム（クラウドサービス等）の導入の際の十分なリスク評価、通信のセグメント間での管理・制御・検知について、最新の技術動向を常に調査し、必要に応じて速やかに以下のようなシステム強化を行う必要がある。

- ○ 多要素認証等の強固な認証技術を、内部システムのうちイントラ基盤システム等の重要なシステムにも導入し、破られにくく、かつ攻撃が検知可能な認証システムを導入する。【6.1.3】
- ○ 研究用ネットワークをセグメント分離できるネットワークを構築する。さらに、セグメント間の通信を制御できるようネットワーク構成を抜本的に見直す。【6.1.3】
- ○ 侵入や拡散の即時検知のため、内外を通過するファイアウォールの監視、セグメント間の内部通信監視を導入する。【6.1.4】
- ○ 重要システムにおいては、必要十分なログを蓄積し、不正なアクセスの分析・解析ができるシステムを導入する。また、侵入時にログ等の証跡が消去されないよう、ログの冗長化や遠隔保存等の仕組みを導入する。【6.1.4】

7.2.2 運用の見直し強化

安易なパスワードの不使用・送付方法の見直し、ファイアウォール外へのサーバ等の接続の審査強化、エンドポイントセキュリティ導入困難機器等の十分なリスク評価・管理、サーバの設定状況の確認に関して、以下のような運用の見直し強化を行う必要がある。

- ○ 有効なパスワードの設定方法、管理方法について改めて検討し、産総研の情報セキュリティ実施要領及び情報セキュリティ実施ガイドに反映させるとともに、職員、外部委託業者に周知・徹底する。【6.2】
- ○ 外部接続に際しては、ネットワーク構成、管理者の知識・能力、管理体制等について専門家による厳格な審査を行い、十分なセキュリティ対策が講じられていることを確認する。【6.1.2】
- ○ エンドポイント監視が効果を上げない機器（研究用の Linux 機器、NAS 等）については、機器の選定方法のガイドライン、監視方法を見直す。【6.1.6】
- ○ 情報機器の脆弱性情報の所内徹底を図るとともに、固定 IP の運用ルールの見直しを行う。【6.1.6】
- ○ 研究活動の実態を踏まえつつ、研究用サーバ管理ルール、重要情報の管理ルールの見直しを行う。【6.4】
- ○ 全体システムについて、より実効性・継続性のある情報セキュリティ監査を行う。また、ISMS（情報セキュリティマネジメントシステム）の認証取得を検討する。【6.4】

7.2.3 外部委託の運用改善【6.3】

外部委託業者の情報セキュリティ対策に関する契約履行状況の把握、従来慣行を前提とした業務の内容解釈の排除に向けて、以下のような外部委託の運用改善を図る必要がある。

- ○ つくばセンターの契約における作業員の常駐義務が、応札業者を限定し、同一業者による長期的・慣行的運用の一因となった可能性があることから、外部委託業者の選定条件を見直す（一例としては、遠隔監視・運用の活用）。
- ○ 重要な情報を扱う外部委託については、外部委託業者から情報漏えい等のリスクが生じないよう、業者選定に当たっての一般競争入札について、最低価格落札方式から総合評価落札方式への切り替えを検討し、情報セキュリティの取組についてより能力の高い業者を選定できるよう、契約・選定方法を見直す。
- ○ 関連業務は極力まとめ、一括して競争入札するよう改め、管理監督する外部委託業者の数を減らす。
- ○ 委託先の選定基準マニュアルと、外部委託業者向けの情報セキュリティ対策チェックリストを作成し、情報セキュリティ対策の履行状況の確認等を定期的に行う。
- ○ 外部委託業者に対して、情報セキュリティ監査を行うことを検討する。

7.2.4 組織体制の見直し【6.4】

マネジメントの課題に示したとおり、産総研では本部（情報基盤部）と約 50 の現場（研究部門）が情報セキュリティマネジメントを分担する、いわゆる分権型のガバナンス構造を有し、各研究部門の長が責任を持って自らの技術情報を守るための情報セキュリティ体制を推進するとともに、これら研究部門を支えるため管理部門である情報基盤部が研究部門を含めた一元的な情報セキュリティマネジメントを行っている。

国立研究開発法人の特徴を踏まえたサイバーセキュリティの在り方については、「サイバーセキュリティ戦略中間レビュー」（平成 29 年 7 月 13 日サイバーセキュリティ対策本部決定）においても、「各研究部門の長によるガバナンスの下で対策を推進する体制を構築し、研究者に対する教育・訓練を充実することに加え、研究開発を行いやすい環境と情報セキュリティの確保の両立を図るべく、ユーザに依存しない対策を強化することが効果的と考えられる。また、組織内での情報セキュリティマネジメントの運用に際しては、研究部門と管理部門を通じた一元的な運用を強化することが重要である」といった方向性が示されており、これを参考としつつ産総研の実態に即して制度設計していく必要がある。

しかし、改めてその実態を振り返ると、CISO と 2 名の CISO 補佐の下で統括情報セキュリティ責任者を担う情報基盤部長が中心となる体制を構築したものの、情報基盤部に研究部門を十分に支援するだけの要員が確保できていなかったこと、情報セキュリティの担当職員が情報化推進担当も兼務せざるを得ず情報セキュリティ対策に組織的に取り組めていなかったこと、研究部門自らが管理するネットワークや情報機器におけるリスクを十分に把握できなかったこと等により、事案の発生を防ぐことができなかった。

組織体制については産総研の特徴を踏まえつつ、今後とも試行錯誤を繰り返しながら見直し・更新を続けていく必要があるが、今回の事案を踏まえれば、さらに、情報セキュリティ委員会の格上げ、司令塔としての CISO の役割と機能性の強化、情報セキュリティ対策部署の明確化、組織全体のリテラシー向上に向けた所内関連部署（情報基盤部、情報技術研究部門等）の緊密な連携等を進めることが必要であり、具体的には以下を講じる。

- ○ CISO を長とし、情報セキュリティのリスク認識に基づく情報セキュリティマネジメントシステムを構築し、PDCA サイクルを回すとともに、必要に応じてマネジメント体制の見直しを行う。
- ○ 情報セキュリティ委員会の位置づけを理事長の直下に格上げし、当該委員会を通して、情報セキュリティ対策に関する理事長のトップマネジメントがより強く働くよう体制を見直す。
- ○ 所外の情報セキュリティの専門家を、最高情報セキュリティアドバイザーとして委嘱することを検討する。
- ○ CISO の下に、情報セキュリティ対策部署を明確に位置づけ、不正なアクセスへの対策の強化を図るとともに、インシデントに対する機動性を確保する。
- ○ 情報セキュリティ対策部署には、所内の状況把握が可能となるよう、システムの調達・管理、情報セキュリティ対策に関する十分な知見を有する者を配置する。情報セキュリティ対策部署の責任者には、所内

の各部門長との十分な調整ができるよう、必要な権限を付与することとし、必要に応じて体制を強化する。

○ 情報セキュリティ対策部署は、外部の情報セキュリティ機関との連携を一層深め、常に最新の情報を交換するとともに、それらの情報を適時適切に関連部門に提供する。

○ 所内関連部署（情報基盤部、情報技術研究部門等）の専門家からなる「情報セキュリティ対策会議（仮称）」を設置し、情報セキュリティ対策についての連携を強化する。

○ 研究部門の情報セキュリティ対策状況を、定期的に情報セキュリティ対策部署へ報告する仕組みを導入する。

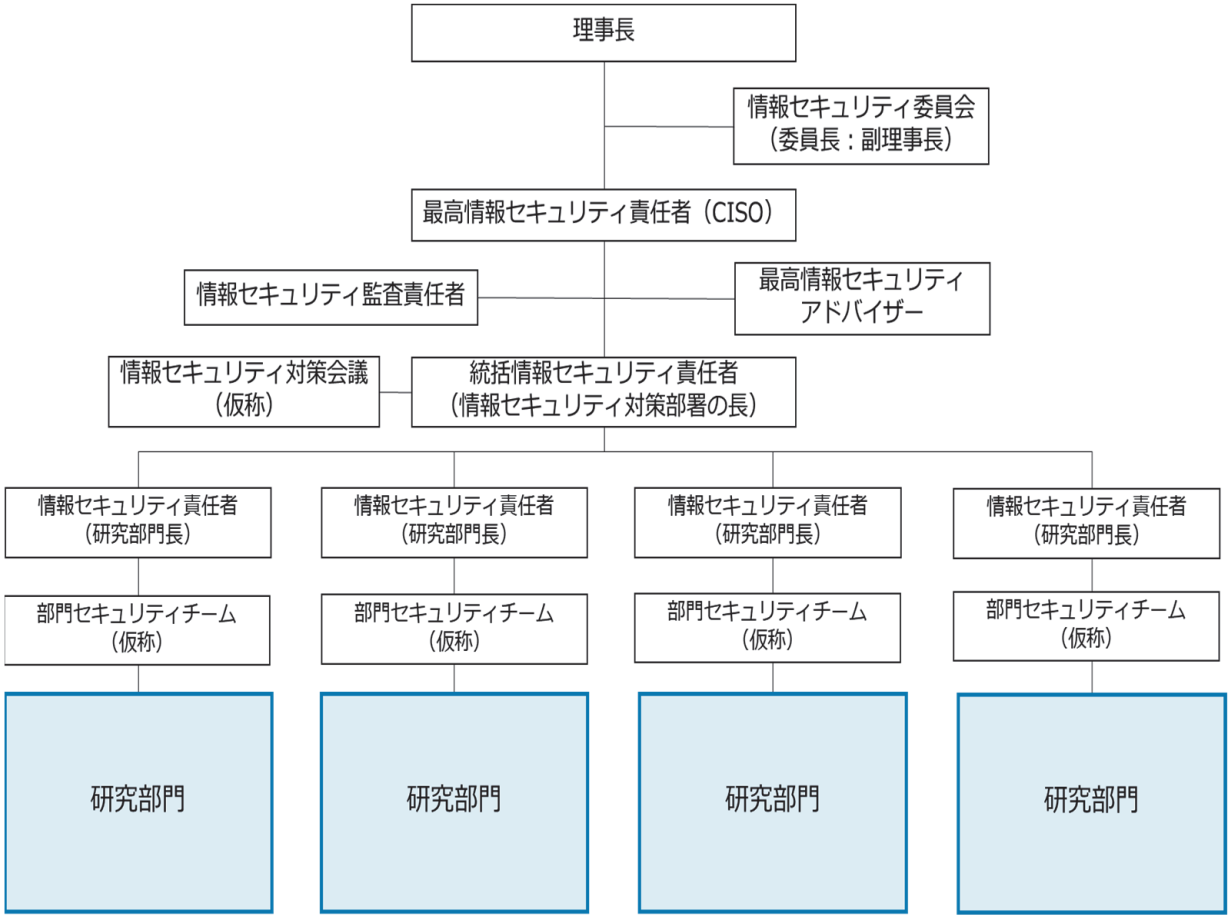
○ 研究部門長の情報セキュリティ責任者としてのマネジメント向上のため、研究部門長研修（毎年実施）に、情報セキュリティに関する項目を追加する。

○ 各研究部門に、情報セキュリティ責任者（研究部門長）をサポートする「部門セキュリティチーム（仮称）」を設置する。部門セキュリティチームは副研究部門長（又はそれに相当する者）を長とし、部門内の 2、3 名の職員で構成する。

○ 部門セキュリティチームは、情報セキュリティ対策部署及び CSIRT と連携し、セキュリティ対策に関する最新の情報交換等を行うことによって、部門内のセキュリティリスクの低減を図る。

○ 具体的には、CSIRT が対処したインシデント事例を適宜、部門セキュリティチームへ展開し、インシデントの原因やその対処内容、脆弱性情報等を共有するとともに、インシデント発生時の対応訓練を実施することによって情報セキュリティに関する研究部門のリテラシーの底上げを図る。

見直し後の情報セキュリティ管理体制を下図に示す。



7.2.5 事業継続計画（BCP）の見直し【6.4】

今回のような事案に適切に対応するため、重大なインシデントの際の事業継続計画、外部委託業者への要請事項（侵害の状況確認、影響範囲の特定、ログの調査等）を明らかにしておくことが重要であり、以下の対策を講じる必要がある。

- ○ 情報セキュリティインシデントの深刻度に応じた事業継続計画（Business Continuity Plan）及び緊急時対応計画（Business Contingency Plan）の立案をする。
- ○ インシデント発生時に十分な対応を行えるように外部委託業者等との契約を見直す。また、常日頃より、委託業者との協力に関する十分な情報交換を行う。
- ○ 重要なシステムへのサイバー攻撃に対する、継続性（Continuity）と危機対応（Contingency）のための訓練を実施する。

（添付 4：被害を発生・拡大させた要因と再発防止のための対策）

8. 他機関との連携状況

産総研では、事案の発生直後より、以下のとおり、各関係機関との密接な連携を図ってきた。

8.1. NISC（National center of Incident readiness and Strategy for Cybersecurity、内閣サイバーセキュリティセンター）

不正なアクセスを行った IP アドレスの情報及び踏み台となったサーバのログの提供について NISC から依頼を受け、これらの情報を提供した。

以降、提供した情報に関する詳細な質問への対応や、発見されたマルウェアの検体を NISC へ順次提出した。

8.2. JPCERT/CC（JPCERT コーディネーションセンター）

本事案判明直後、専門的知見を有する中立機関である JPCERT/CC へ助言を求めた。

以降、提供した情報に関する詳細な質問への対応や、発見されたマルウェアの検体を、JPCERT/CC へ順次提出した。

8.3. 警視庁

警視庁・サイバー攻撃対策センターに対しては、本事案判明直後より情報提供を行うとともに、捜査について相談を行った。

その後、4 月 6 日に正式に捜査を依頼した。

以後、提供した情報に関する詳細な質問への対応や、発見されたマルウェアの検体を、警視庁へ順次提出した。

9. おわりに

本報告書では、産総研が受けた大規模なサイバー攻撃について、事案の経過と攻撃の手口、被害を拡大させた要因、再発防止策等を記述した。

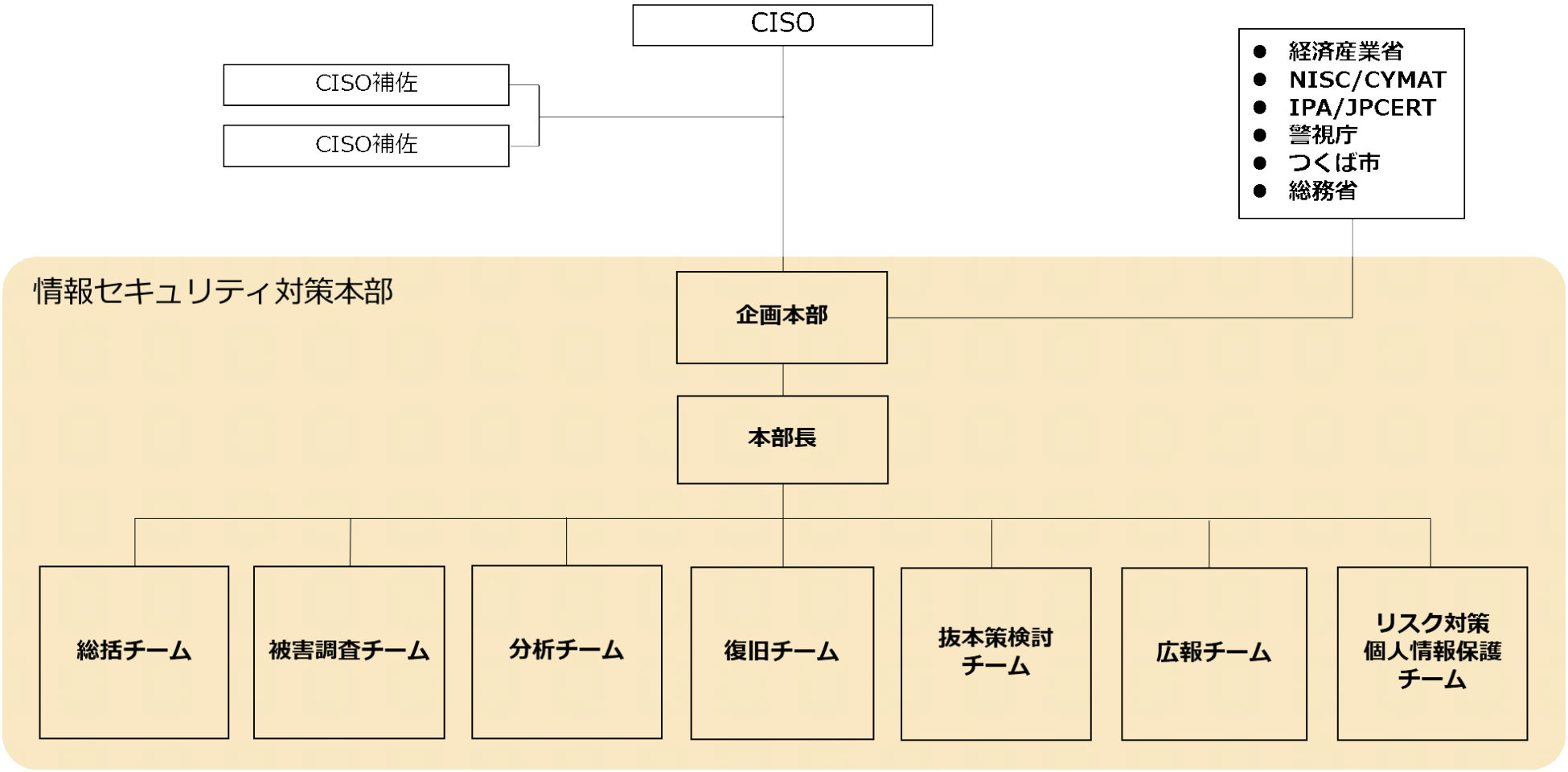
攻撃の期間が長期にわたり、また、不正なアクセスを受けた範囲が広範にわたったため、復旧、被害調査、分析に相当の時間を要した。

今回の事案を教訓として、産総研の職員一人ひとりが、情報セキュリティに対する意識を一層高めることが求められる。

また、ハード・ソフトの両面で、再発防止策を速やかかつ着実に実行することにより、再びこのような情報セキュリティインシデントが発生しないよう努める所存である。

添　付

情報セキュリティ対策本部体制図



添付１

添付２

「情報システムに対する不正なアクセスに関する調査委員会」

委員長

土　居　範　久	慶應義塾大学 名誉教授 特定非営利活動法人 日本セキュリティ監査協会 会長

委員

齋　藤　　隆	弁護士（ひかり総合法律事務所）
板　倉　陽一郎	弁護士（ひかり総合法律事務所）
長　尾　慎一郎	長尾公認会計士事務所 日本セキュリティ・マネジメント学会 監事 特定非営利活動法人 日本セキュリティ監査協会 副会長
島　田　広　道	国立研究開発法人 産業技術総合研究所 理事
関　口　智　嗣	国立研究開発法人 産業技術総合研究所 理事

事務局

情報セキュリティ対策本部

添付３

被害範囲の特定と原因の究明に関する分析結果

以下は、本事案における被害範囲を特定し、原因を究明することを目的に、外部業者に委託して行ったフォレンジック調査（電子機器に残された証拠の保全と分析調査）及び、ログ解析、職員からの聞取り調査の結果を踏まえ、その分析結果を取りまとめたものである。

目　次

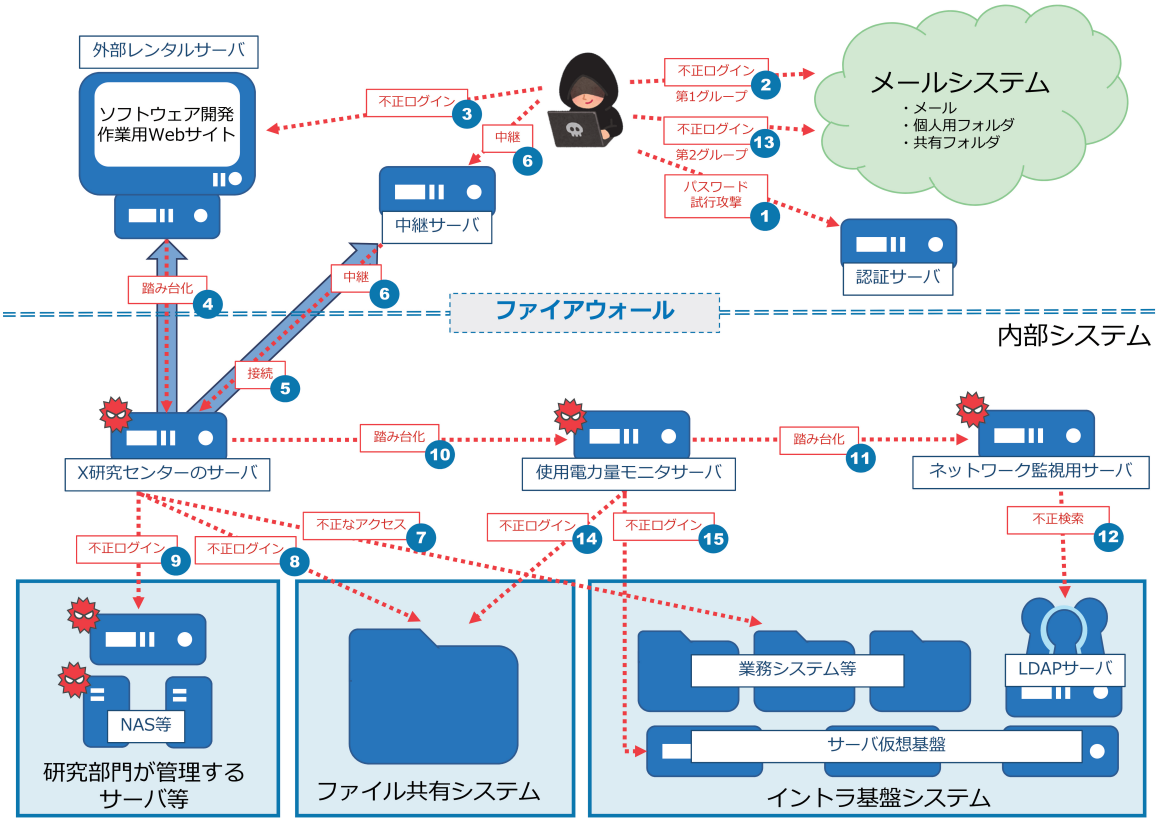


図 1　侵入経路とその順序（丸数字が順序を表す）

1. 職員アカウントへの不正ログイン

1.1. 侵入者の活動の特徴

不正なアクセスの接続元は、最初に発覚した国内の特定大学の IP アドレスの他は、ほとんどが海外の IP アドレスであり、その総数は 155 個に及び、その内訳は以下の通りであった。

- ○ メールシステムへのアクセス手段として匿名通信システム「Tor」が用いられ、Tor の出口として 120 個のアドレスを確認。
- ○ 匿名通信の用途で特定の事業者の VPN サービスが用いられ、出口として 7 個のアドレスを確認。
- ○ 後述する踏み台との中継の用途、bot が通信する C&C サーバの用途、パスワード試行攻撃の用途等で、複数のレンタルサーバが用いられており、その IP アドレスとしてアメリカ 5 個、ドイツ 5 個、シンガポール 3 個、フランス 2 個、オランダ 2 個、スイス 2 個、中国 2 個、香港 2 個、日本 1 個、カナダ 1 個、スウェーデン 1 個、リトアニア 1 個、ラトビア 1 個の計 28 個を確認。

被害の範囲を確実に特定するためには、これらが同一者による一連の活動であるのか、それとも独立した複数の侵入者らによる多数の活動であるのか、それを見極めることが必要であった。

匿名通信が駆使されているため、侵入者がどの国又は地域から攻撃を行っていたかは定かでないが、その活動時刻に明確な特徴が見られた。侵入者の手動による操作と考えられる侵害事象の発生時刻が、日々同じ時間帯にあり、日本時間の月曜から金曜の夕方 16 時半頃から深夜 2 時頃であった。(24 時をまたぐ活動であるため、以下、便宜的に日時は 24 時をまたがないようにして示している。)

さらに、Web ブラウザによる不正なアクセスでは、特定の種類の Web ブラウザが継続して用いられており、同時に多数の Web ブラウザが用いられることはなく、ほとんどで 1 つ又は 2 つの Web ブラウザが同時に使用されていた。

これらのことから、一連の侵害イベントは同一者による活動である可能性が高く、組織による活動であり、1 名か、数名程度によるものと推定できる。

1.2. メールシステムへの不正なアクセス

初動対応で発見されたメールシステムへの不正ログインでは、国内の特定大学と香港の 2 箇所の IP アドレスからのアクセスによる 41 アカウントの被害が見つかったが、他にも被害がないかを確認する必要があった。

メールシステムの異常検知機能を用いて調べると、それら 2 箇所の IP アドレスから以外にも、不正ログインと疑われるアクセスが数多く存在し、その発生期間も数か月に及ぶことが判明した。

そこで、被害アカウントの特定作業においては、取得することができた約 8 か月分のログイン履歴から、慎重を期すため目視確認を含めて集計する方法[1]で行った。その結果、2017 年 10 月 27 日から 2018 年 2 月 6 日にかけて不正ログインがあり、被害アカウントの数は 143 名分であったと結論付けた。

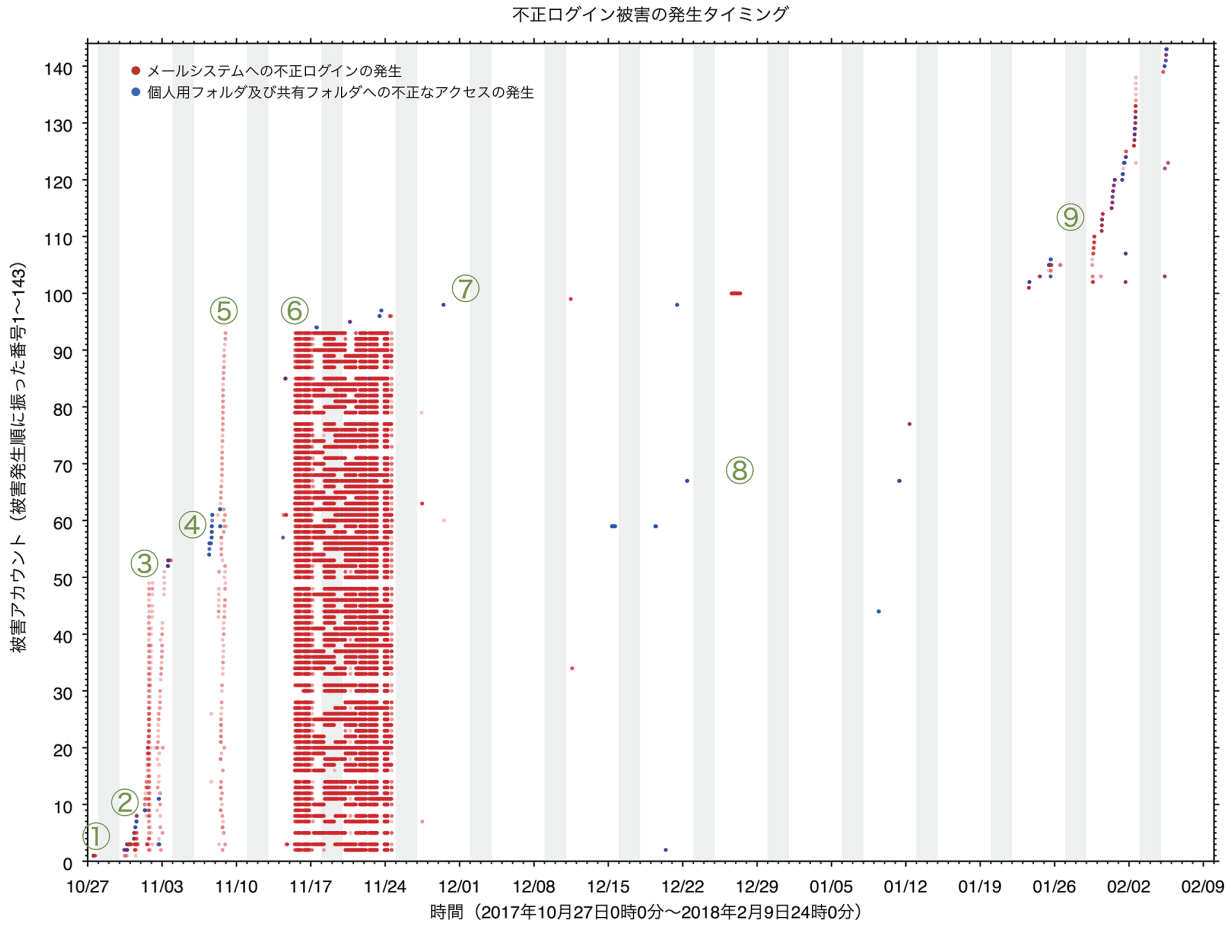


図２　メールシステムへの不正ログイン被害の発生タイミング

被害の発生タイミングを図 2 に示す。横軸は時間であり、縦軸は被害アカウントを表しており、被害発生順に振った番号（1 ～ 143）を縦軸としてプロットしている。赤の点はメールシステムへの不正ログインの発生を示し、青の点は、個人用フォルダ及び共有フォルダへの不正なアクセスの発生を示している。縦の灰色のバーは、土曜及び日曜日を表している。

発生タイミングとアクセスパターンの特徴及び推定される侵入者の意図から、被害の段階を 9 段階に分けることができ、図中の丸数字で示す。それぞれの段階の特徴は以下の通りである。

- ○　第 1 段階は、2017 年 10 月 27 日に行われた 1 名のアカウントへの不正ログインである。これが最初の不正ログインとなった。
- ○　第 2 段階は、10 月 30 日と 31 日に行われた計 8 名（第 1 段階の 1 名を含む）のアカウントへの不正ログインである。これらは、次節で示す実在 ID に対するパスワード試行攻撃より前に不正ログインされている。

[1] 被害アカウントの特定作業は次の方法で行った。不審な IP アドレス（Tor の出口や、他の攻撃元の IP アドレス）からログインされたアカウントを抽出し、それらのアカウントにログインした他の IP アドレスを抽出して、そのうち本人による正当なアクセスによるものと考えられる IP アドレスを目視確認によって除く作業を行って、残った不審な IP アドレスからログインされた他のアカウントを抽出し、同様にそれらのアカウントにログインした他の IP アドレスを抽出して、これらを繰り返すことにより、不審 IP アドレスが出尽くした時点で収束したものとした。

○ 第3段階は、11月1日から3日までに行われた計50名への不正ログインである。これらは、この時点までに次節で示す実在IDに対するパスワード試行攻撃により特定されたパスワードを用いて不正ログインされたものと推定できる。

○ 第4段階は、11月3日から8日までに行われた、11名のアカウントに対する個人用フォルダ及び共有フォルダへの不正なアクセスである。このとき、侵入者はどのようなファイルを閲覧できるかを探ったものと推定できる。これらは、継続して行われていたパスワード試行攻撃により新たに特定されたパスワードを用いて不正ログインされたものと推定できる。

○ 第5段階は、11月8日に行われた、この時点までにパスワードを特定されたと推測される87名のアカウントに対する一斉ログインである。ここで、自動化されたログインが試行されたものと推定できる。

○ 第6段階は、11月15日から24日にかけて、第5段階の87名から4名を除いた83名に対して、同時並行的に繰り返し不正ログインが行われている。このとき、全てのメールがダウンロードされたものと推定できる。

○ 第7段階は、11月8日から12月26日にかけて散発的に7名のアカウントが新たに不正ログインされている。これらは、パスワード試行攻撃で後から特定されたパスワードを用いたものと推定できる。

○ 第8段階は、11月27日から1月12日にかけて散発的に、既知のアカウントに対して再び、不正ログインと個人用フォルダ及び共有フォルダへの不正なアクセスが行われている。これらは、侵入者が何らかの目的を持って特定のアカウントのメールの内容を確認したものと推定できる。

○ 最後の第9段階は、2018年1月23日以降に行われた、不正ログインと個人用フォルダ及び共有フォルダへの不正なアクセスである。これらは、後述するLDAPサーバの不正検索の後に行われたものであり、第7段階までとは異なる原因でパスワードを特定されたものと推定できる。

以上の各段階は、パスワード試行攻撃等が原因と考えられる「第1グループ」（第1段階から第8段階まで）と、LDAPサーバの不正検索が原因と考えられる「第2グループ」（第9段階）とに分けられる。第1グループの被害は計100名分（図1の❷）で、第2グループの被害は43名分（図1の⓭）である。初動対応で発見した41名分のアカウントは、全て第2グループに含まれるものであった。

初動対応の際、メールシステムへの不正ログインを発見した41アカウントは、パスワードが比較的強固な強度のものであったことから、単純にパスワードを推測されたとは考えにくく、フィッシング攻撃の被害とも考えにくいものであった。このことから、再発防止のためには、パスワードを特定された原因の究明が急務であった。

被害アカウントの利用者に聞き取り調査を行い、被害当時にどのようなパスワードを設定していたかを確認したところ、以下の通りであった。

【第1グループ】

○ 第1段階の1名は年月日を基にした単純な文字列[2]であった。

○ 第2段階の8名のうち第1段階の1名を除く7名は、それなりの強度（強固とまでは言えないが、数百回程度の試行（次節参照）で破られるとは考えにくい強度）のものであった。

○ 第3～第8段階の92名のうち十数名はパスワードを覚えていなかったが、その他の者についてはほとんどが、キーボード配列をなぞって入力された安易なものであった。

○ 第7段階の遅いタイミングで不正ログインされたアカウントは、キーボード配列ほどには単純ではないものの、簡単なローマ字文字列に数字を加えた程度のものであった。

【第2グループ】

○ 比較的強固な強度のものが設定されていた。

[2] 年月日を数字と英大文字小文字で表現したものである。

第 1 グループの不正ログインの手口は、第 2 段階のみ不明であるが、残りの段階については、次節で示すように、パスワード試行攻撃によるものと推定している。

被害の内容としては、第 6 段階の対象アカウントでは、サーバに残っていた全部のメールを窃取されてしまったと推定できるほかは、どの程度のメールが窃取されたかはログからは不明であり、キーワード検索等により必要なだけのメールが閲覧されたものと推定できる。個人用フォルダ及び共有フォルダへの不正なアクセスについては、どのファイルが閲覧されたかをログにより特定できるため、そのファイルの内容の調査を行った。その調査結果は本報告書本文に示した。

1.3. 認証サーバへの大量のパスワード試行攻撃

メールシステムへのログインと内部システム（イントラ業務システム）へのログインを認証連携させている認証サーバは、外部からアクセス可能なところに置いていたことから、パスワード試行攻撃にさらされていた（図 1 の❶）。

2017 年 11 月 14 日と 12 月 8 日に、認証サーバに対する大量のパスワード試行攻撃の発生を認知していたが、認証サーバの外部委託業者から「攻撃は全て失敗している」旨の説明があったため、それ以上の調査を行わなかった。その理由は、当該認証サーバでは、ログイン ID（以下「ID」という。）を、メールアドレスではなく、職員が独自に決める任意の文字列としていることから、いわゆるリスト型攻撃[3]の影響を受けないと考えたためであった。

しかし、本事案の発覚後に改めて調査を行ったところ、大量のパスワード試行攻撃の結果として不正ログインが成功していたと推定できる結果が得られた。以下、この分析について示す。なお、Web サーバのアクセスログからでは認証の成否を判別できず、認証サーバも認証の成否をログに出力していなかったため、この分析は、当該認証サーバが参照している LDAP サーバのログを集計することにより行った。

図 3 は、認証サーバが参照している LDAP サーバの 1 日当たりの検索数の推移（横軸は時間、縦軸は検索の回数）である。2017 年 10 月末から、赤の線が示す認証失敗の数（存在する ID に対するパスワード誤りの場合）が急増しており（最大値は 140 万回）、明らかに攻撃があったと分かる。また、青の線が示す存在しない ID に対するログイン試行が 6 月 1 日から有意に増大していたことを確認できる。

これらが同一侵入者による一連の攻撃であるか、複数の攻撃者による攻撃かを見極めるために、LDAP サーバに対する ID 毎の認証試行の発生タイミングをプロットしたのが図 4 である。上側に赤でプロットした点は、存在する ID に対する認証失敗の記録であり、下側に青でプロットした点は、存在しない ID に対する認証試行の記録である。縦軸は、ID を表しており、出現順に振った番号（存在する ID は正の整数、存在しない ID は負の整数）を縦軸としてプロットしている。横軸は時間で、残っていた最古のログ 2017 年 1 月 22 日から、認証サーバを新システムへの入替えのために停止させた 2018 年 1 月 6 日までの範囲である。

時間経過に伴って上下とも ID 数が増えていくのは、職員による正規の認証試行においてパスワードを間違えた場合（上側）と ID を間違えた場合（下側）が記録されたものが含まれているから[4]である。

ここで明らかな異常が見られるのは、まず、下側の中央部に位置する濃い青のブロック（図中 (A)）である。これは、2017 年 7 月 15 日から 8 月 25 日までの間に、高速に ID 探索が行われていたことを示している。このほか、6 月 1 日から（図中 (B)）と、2 月上旬から（図中 (C)）にも、量は少ないものの、同様に ID 探索があった[5]ことが分かる。

---

[3]「リスト型攻撃」とは、ネットサイトでログイン ID にメールアドレスを用いているところが多い中、どこか一つのネットサイトが、システムで保管している ID とパスワードの組のリストを流出させる事故を起こした場合に、この流出したリストを入手した攻撃者が、他のサイトでこのリストに記載された ID とパスワードを用いて不正ログインを試みると、不正ログインが比較的高い確率で成功してしまう攻撃のことを言う。2010 年頃からこうした攻撃が頻発するようになったことから、今日では、他のサイトと同じパスワードを使い回さないようにするべきである旨の注意喚起が利用者らに呼びかけられている。ログイン ID にメールアドレスを用いず、独自の文字列としているシステムの場合には、リスト型攻撃は成立しにくくなる。

[4] 青の横向きの線が見られるのは、存在しない ID に繰り返しログイン試行があったものであるが、個別に精査したところ、退職等によって無効になったアカウントに対して、本人がメールクライアントの設定をそのままにしたことにより、繰り返しログイン失敗が起きていたものと考えられるものであった。

[5] これらが横に並んでいるのは、同じ ID に対して繰り返しパスワードを変えたログイン試行が行われたことを示しており、同一攻撃者又は別々の者が同一の ID リストに基づいて攻撃したものと推定できる。特に、試行する ID を増やしながらも、それと同時のタイミングで、過去に試行した ID も繰り返し試行していることから、同一者によるものである可能性が高いといえる。

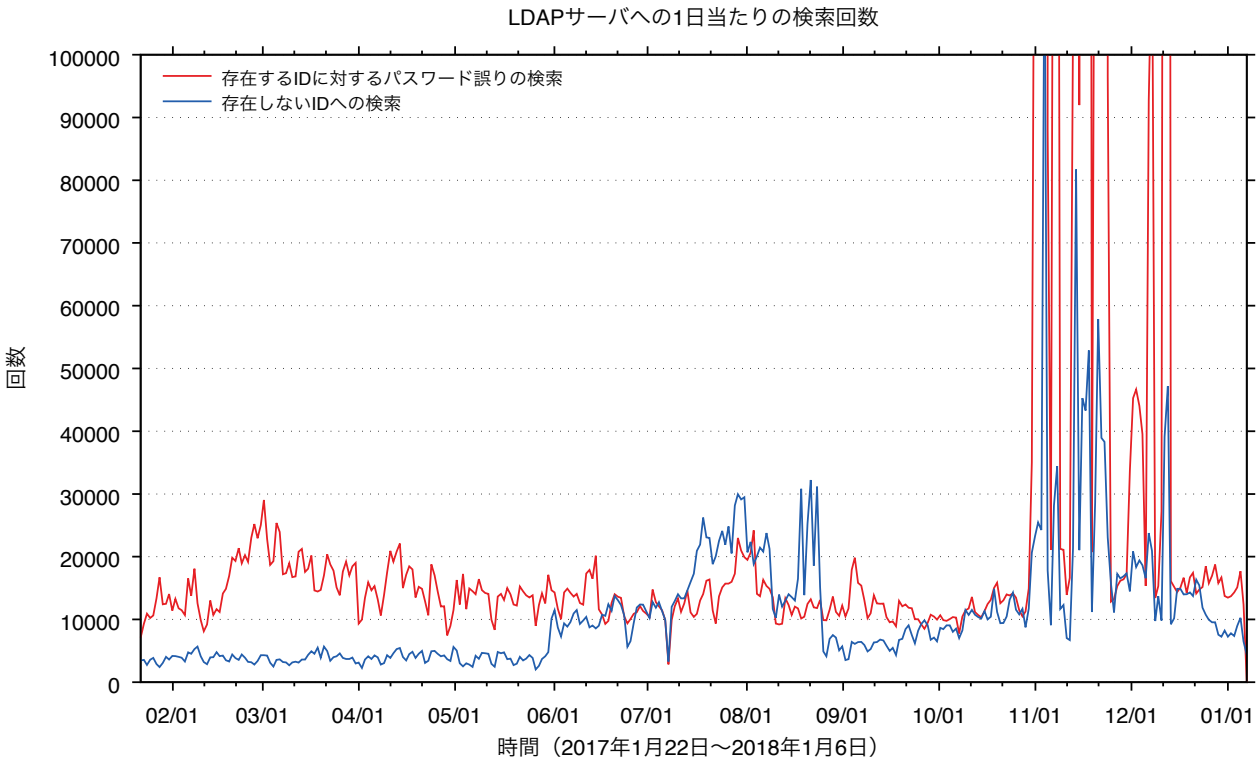


図３　LDAP サーバへの１日当たりの検索回数

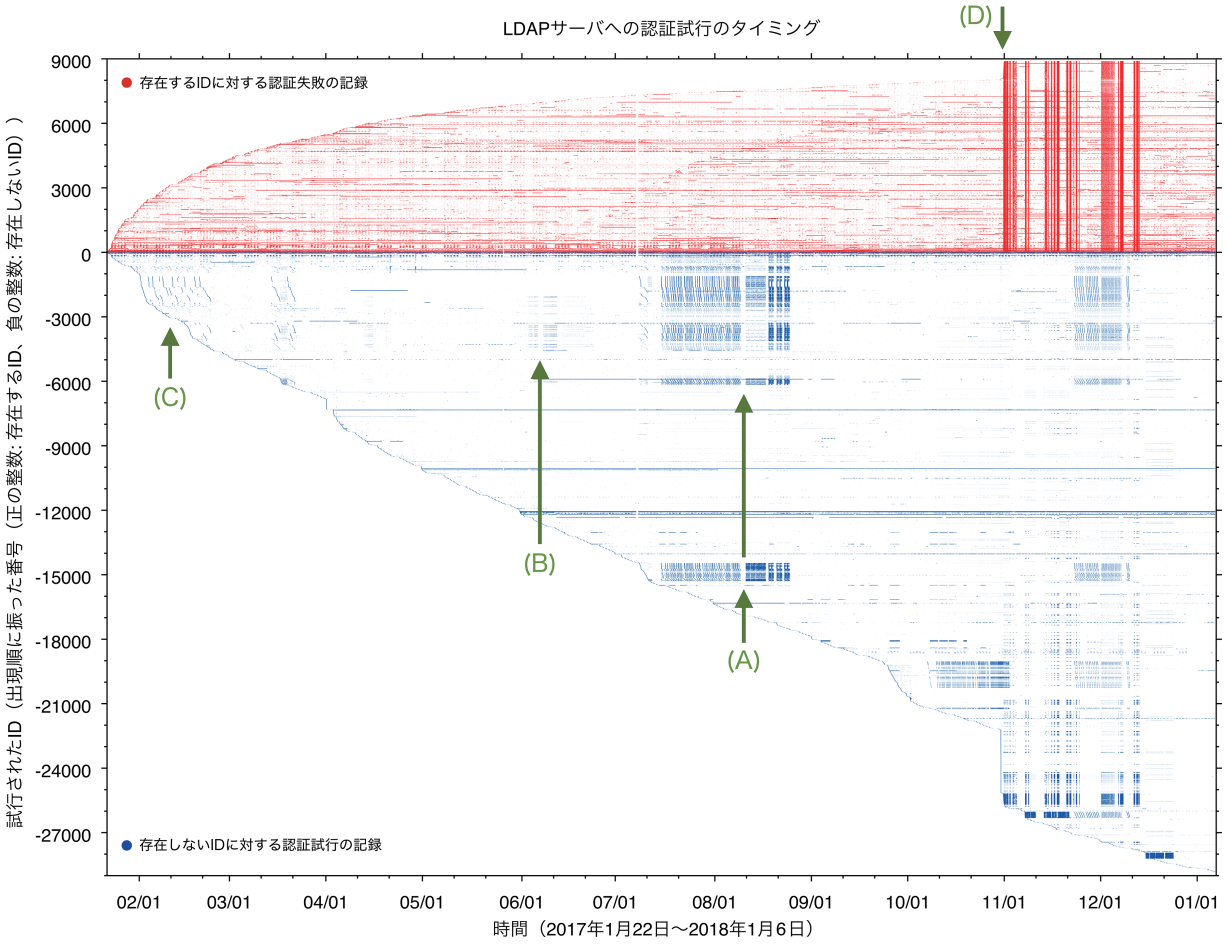


図４　LDAP サーバへの認証試行のタイミング

この認証サーバでは、ログイン画面において、ログインが成功した場合と失敗した場合とで、結果に違いがない画面設計となっていたため、ID だけ先に特定することはできないようになっていた。そのため、図のように、存在しない ID に対して繰り返しパスワード試行が行われていた。

図 4 で次に着目すべき異常な点として、上側の赤のプロットが、2017 年 10 月末から急激に濃くなっている部分（図中 (D)）がある。これは、実在する ID に対する認証失敗の記録であり、赤のプロットが上下に全部が濃くなっていることから、全部のアカウント（約 8,000 個[6]）に対してログイン試行されたことが分かる。この日までに実在する ID の全部を知られたことを意味する。

このタイミング（2017 年 10 月 31 日 図中 (D)）は、前記のメールシステムへの不正ログインの段階のうち、第 2 段階より後で、第 3 段階の直前の時刻である。第 3 段階で、キーボード配列のような弱いパスワードを設定したアカウントが被害に遭ったのは、この不正ログイン試行が開始されてすぐにパスワードを特定されてしまったものと推定できる。

実際にパスワードとしてどのような文字列が試行されたかは、入力文字列をログに残さない仕様であるため確認できないが、フォレンジック調査の結果、一部について、キーボード配列に沿った文字列が入力された痕跡が、削除済みのエラーログから見つかった。これには、シフトキーを併用して入力される記号も含めて試行するものが含まれていた。

ID 当たりの試行されたパスワードの数はさほど多いものではなかった。図 5(a) に、第 1 グループのアカウントについて、ID 毎のパスワード試行の累積回数の推移を示す。試行回数は数十から数百程度であり、キーボード配列を基にした弱いパスワードは、その程度の試行で早々と特定されてしまったものと推定できる。

次に、本当にこれらのパスワード試行攻撃が原因でメールシステムへの不正ログインにつながったのか、その因果関係の有無を推定するため、図 5(b) に、被害のなかったアカウントから無作為抽出した 80 のアカウントについての累積回数の推移を示した。

(a) と (b) を比較して言えることは、第 1 グループの被害アカウントは、途中でパスワード試行の対象から除外された様子があることである。このことは、(b) で累積回数が急増しているタイミングで、(a) では急増していない線が多く見られることから分かる。これは、不正ログインに成功したアカウントを試行対象から除外した、つまり、これらのパスワード試行攻撃の結果としてパスワードが特定されたのであり、それによって第 1 グループのアカウントに対する第 3 段階以降の不正ログインに利用されたのだと推定できる。

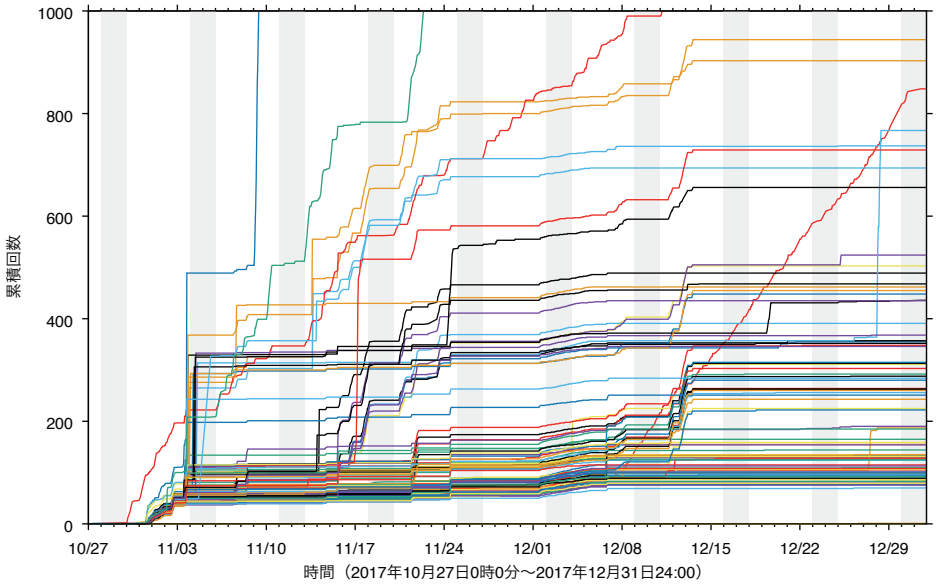
第 2 グループの被害アカウントについての同じ推移を示したグラフを図 5(c) に示す。(b) の被害のなかったアカウントの場合と比較して、同じタイミングで累積回数が急増していることから、この段階ではパスワードを特定されていないと推定できる。なお、この図で、11 月 22 日に一部を対象に大量のパスワード試行が行われているが、これらの ID はいずれも情報基盤部の職員らのアカウントであった。このことから、侵入者は、早い段階から情報基盤部の職員を狙って不正ログインしようとしていたものと推定できる。

その後、12 月 13 日にパスワード試行攻撃がほぼ中止された。これは、同じ方法ではこれ以上のパスワード特定ができなくなったと判断されたのか、後に述べるように内部ネットワークへの侵入手段を発見しパスワード試行攻撃の必要性が薄れたためと推定できる。

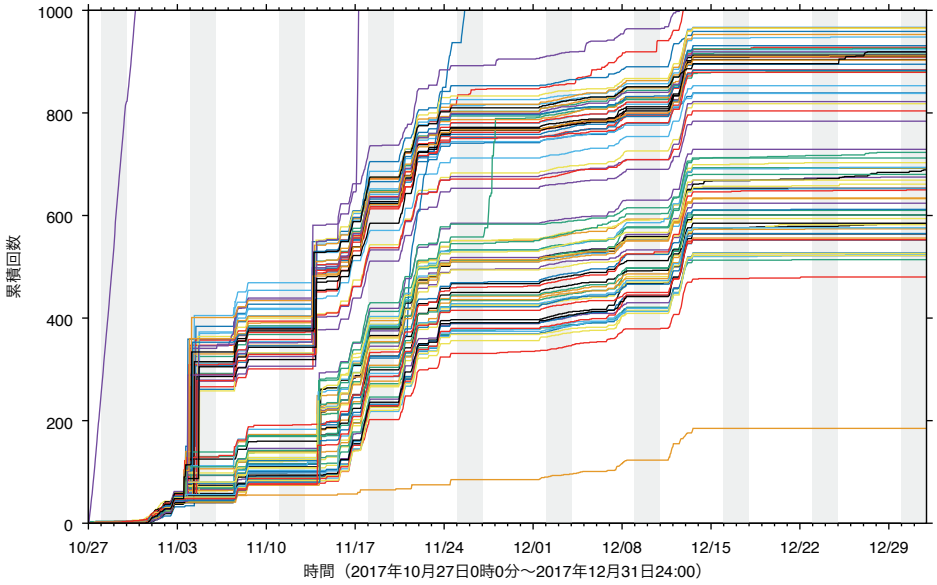
パスワード試行攻撃の兆候がありながら、それを察知して対策を打てなかったことは、被害を拡大させた要因のひとつである。パスワード試行攻撃は、図 4 のように、2017 年 2 月の時点で既に始まっていたが、この段階では緩やかな速度による試行であったため、直ちに気づくことは難しかったかもしれない。しかし、図 3 のように、1 日当たりの認証の失敗回数の変化を観測していれば、2017 年 6 月 1 日からの急増を見つけることはできた可能性がある。

外部業者に委託している統合ネットワーク監視では、標的型メール攻撃等を想定して、エンドポイント監視（マルウェア等による端末の不審な挙動の監視）及び内部から外部への不審な通信の検知に注力していたが、認証サーバは、別の保守委託先業者が管理しており、産総研ネットワークの外に置かれていたため、不審なパスワード試行は統合ネットワーク監視の対象に含まれていなかった。

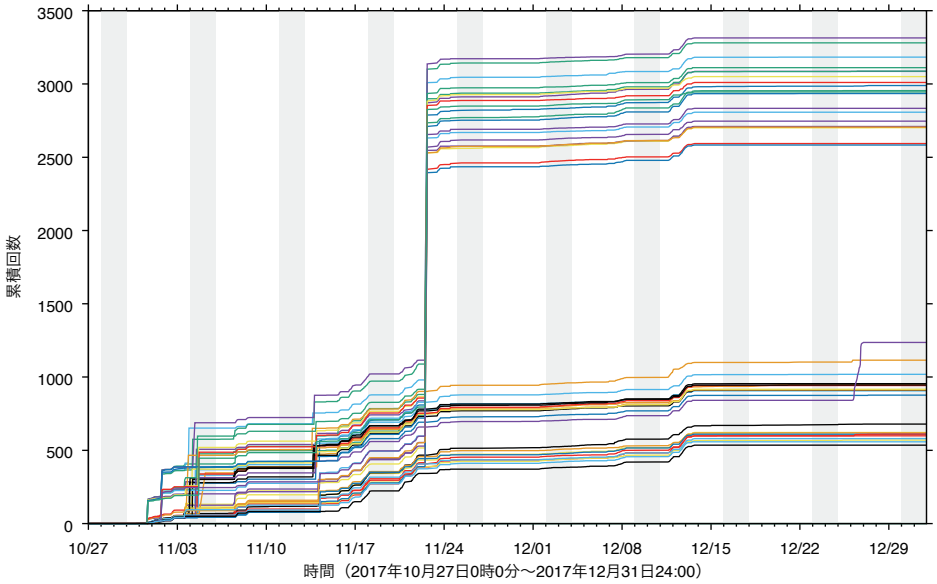
[6] 図 4 のグラフからは 9,000 個弱あるように見えるが、赤の濃いブロックの中にはプロットのない ID が散在しており、実際の数を集計すると約 8,000 個である。



(a) 第 1 グループの被害アカウント



(b) 被害のなかった無作為抽出 80 アカウント



(c) 第 2 グループの被害アカウント

図 5　ID 毎のパスワード試行の累積回数の推移

1.4. パスワードによる利用者認証の限界

職員のパスワード管理については、かねてより、180 日を期限とした定期変更を強制し、非常に弱いパスワードは設定不可とする措置も講じていた。しかし、その方法では、キーボード配列を基にしたパスワードを排除できておらず、上記の安易なパスワードの設定が可能となっていた。

キーボード配列を基にしたパスワードとは、2009 年の U.S. Air Force Academy による論文「Visualizing keyboard pattern passwords」[7] に示されているように、キーボード上を連続的になぞってタイプした文字列のことである。論文が指摘しているように、このようなパスワードは単純なものから複雑で長いものまであり得るが、パターン化し、専用の辞書が作られているため、辞書攻撃によって破られてしまうものである。

前記の聞き取り調査で、十数人の職員が複数のキーボード配列のパスワードを挙げて「このうちのいずれか」と回答した。変更ごとに 1 文字ずつ伸ばしていったとする回答もあった。このことから、パスワードの定期変更を強制しても、こうした弱いパスワードを設定する一部の職員（全体の 1% 程度に当たる）は、定期的に弱いパスワードに変更し続けていたものと推定される。

本事案が発覚する前の 2017 年 5 月、パスワード設定ルールを見直すことを計画し、定期変更の強制を取りやめると同時に、弱いパスワードを設定不可とするために、文字種と文字数に必須要件を設け、かつ、パスワード強度チェッカーを導入して、2017 年 11 月 1 日から実施していた。しかし、そのようなパスワードへの変更が強制されるのは、各アカウントの次の期限切れのときであり、今回のパスワード試行攻撃が、ちょうど同じタイミングで来ていたことから、被害を防ぐには間に合わなかった。

見直し後のルールであっても、キーボード配列を基にしたパスワードを排除できない設定となっていた。キーボード配列をなぞる途中でシフトキーを押したり離したりすることで、記号や大文字を混ぜることができる上に、文字数はいくらでも長くすることができるが、前掲の論文も指摘しているように、シフトキーが併用された文字列も辞書攻撃により破られてしまう。よって、仮に侵入者の攻撃までにこの見直しルールの強制が間に合っていたとしても、被害を防げていたとは限らない。

パスワードの強度を確保するには、文字種による制限ではなく、ランダムにパスワードを作成するなどの他のアプローチが必要であるが、一人も不正ログイン被害を出さないようにするためには、もはや、ID・パスワードによる利用者認証では限界がある。

産総研では、前記のようにログイン用の ID を各職員が独自に決める任意の文字列としたことで、いわば「パスワードが二つある」のに近い設計となっていたことから、いわゆる「リスト型攻撃」に耐えられると想定していた。しかし、本事案では ID を特定されたことで、弱いパスワードを設定している一定の割合の利用者が不正ログインされてしまった。

また、たとえランダムにパスワードを作成する方法を利用者に徹底したとしても、ログイン認証画面を模したフィッシング攻撃を防ぐことはできない。

産総研のメールシステムは、2011 年度までは、外部からの直接のログインはできない設計にしていた。2000 年より、外出先からの利用を必要とする場合には、VPN 接続でセキュリティトークン（ワンタイムパスワード生成器）を用いた二要素認証を必須とする設計としていた。これが、2011 年度以降にメールシステムをクラウド化した際に、クラウドサービスに直接インターネットからアクセス可能であったことから、認証サーバも外部からログインできる設計に変更し、一般職員へのトークンの発行を停止していた。その際、情報セキュリティ委員会において、「この設計はフィッシング攻撃に耐えられない」旨の懸念も指摘されたが、最終的には EV SSL 証明書の導入によって認証サーバのログイン画面の真正性を見分けやすくすることで十分と判断していた。本事案の発覚後、認証サーバを外部からアクセスできないようにするとともに、トークンの一般職員への発行を再開することにより、応急的対策とした。

本事案を受けてメールシステム側に二段階認証を導入する対策も施したが、これは内部からの攻撃を防止するためのものである。二段階認証のみでは、インターネット側からの中間者攻撃手法によるフィッシング攻撃を防止することはできないため、この応急的対策を、当面、維持する必要がある。

---

[7] D. Schweitzer, J. Boleng, C. Hughes, and L. Murphy, “Visualizing keyboard pattern passwords,” In Proceedings of 6th International Workshop on Visualization for Cyber Security (VizSec 2009) (2009), IEEE, pp. 69–73.

1.5. ID を特定された原因

前記のように、ID は職員により独自に決められた文字列となっていたため、長期のパスワード試行攻撃にも耐えて、被害に至らなかったのであるが、全ての ID に対してパスワード試行が開始されたことで、すぐさま不正ログイン被害が生じた。なぜ全ての ID が突如として特定されたのか、というのが原因究明における疑問点であった。

大量の ID を特定された時期が、メールシステムへの不正ログイン被害の第 1、第 2 段階の後であることから、第 1 段階で 1 人の一般ユーザに不正ログインされた結果、何らかの方法を用いて、全 ID のリストを窃取された可能性が仮説として考えられた。攻撃対象となった ID には、その直前の時期に新規登録されたアカウントの ID が含まれていたことから、過去に漏えいしたデータに基づくものではなく、直前に窃取されたものが直ちに利用されたものと推定できる。

2. 内部ネットワークへの侵入と内部システムへの不正なアクセス

2.1. 内部ネットワークへの侵入

10 月 28 日から 11 月 2 日にかけて、産総研が保有する IP アドレスの全域に対してポートスキャンがあった。ポートスキャンにより、外部からの所内システムの利用の際に用いる VPN の接続口を発見され、11 月 1 日～ 3 日にかけてメールシステムへの不正ログインの第 1、第 2 段階で利用されたアカウントの一部を用いて不正接続が試みられていた。しかし、VPN サーバではワンタイムパスワード生成トークンによる二要素認証を実施していたことにより、侵入に失敗していた。その他には基本的に外部から接続できる IP アドレスは存在しないため、外部から直接侵入する方法はなかった。

その後、内部ネットワークへの侵入の糸口となったのは、所外のレンタルサーバに設置していた研究用の Web サイトであった。X 研究センターが外部のレンタルサーバに設置していたソフトウェア開発作業用 Web サイト（以下「J サイト」という。）に導入していた「継続的インテグレーションツール」に対して、12 月 15 日に不正ログインがあった（図 1 の❸）。

このツールは、ソフトウェア開発用の仮想環境上の複数の仮想マシン（OS）を統合管理してソフトウェア開発の自動化をサポートするものであり、その機能の一つに、管理画面上から管理下の仮想マシンを遠隔操作して任意のコマンドを実行できる機能がある。加えて、この機能には、クラウド環境等での利用を想定して、管理される側の仮想マシンからの常時接続の通信（ポーリング通信）を逆向きに利用して制御するモードがあり、X 研究センターは、開発用の仮想マシンを内部ネットワークに配置するために、このモードを利用していた。

侵入者は、J サイトのアカウントに不正ログインすることで、内部ネットワーク内に設置された 2 台の仮想マシン P と仮想マシン Q を遠隔操作した（図 1 の❹）。

仮想マシン P には、汎用の通信中継用ソフトウェアを設置され、12 月 18 日に SOCKS サーバの機能を仕掛けられていたことが、フォレンジック調査により判明した。この SOCKS サーバは、シンガポールにある中継サーバに接続（図 1 の❺）されており、侵入者は、当該シンガポールの中継サーバを経由して、この仮想マシン P の SOCKS サーバに接続する（図 1 の❻）ことにより、内部ネットワークへの IP 接続が可能になっていたと推定できる。

この直後に仮想マシン P から内部システム（イントラ業務システム）へのアクセスが行われた（図 1 の❼）形跡が、DNS サーバのログにより確認された。このログから、イントラ業務システムのヘルプデスクサイト等が閲覧されたと推定される。イントラシステムの URL は、それまでにメールシステムへの不正ログインで閲覧していた被害アカウントのメールの内容から見つけ出していたものと推定できる。

さらに、後述する他の内部システムへのさらなる侵入（図 1 の❿）のためにも、この仮想マシン P と Q は踏み台として用いられ、1 月 31 日まで継続的に用いられていた。フォレンジック調査の結果、X 研究センターのこの仮想環境の 4 台の仮想マシンにマルウェアが置かれていた。

このような事態を許した原因は、本来ならば、全て内部に設置するか又は全て外部に設置するべきであったものを、内部と外部にまたがって設置したことにある。逆向き接続による制御機能は、セキュリティ目的のファイアウォールをまたがって使うことを想定したものではなかった。また、ソフトウェアを改ざんされるリスクのある開発環境を、公開鍵暗号認証等を用いずに、ID・パスワードによるログインで利用可能にしていたことも、このような事態を許した原因である。

2.2. 内部システムの探索

2017 年 12 月 21 日に、前記の仮想マシン P を踏み台として、内部システムへのポートスキャンが行われた痕跡があった。Web サーバと LDAP サーバのポートに対して行われている。この段階から LDAP サーバへの不正接続を企図していた様子が窺える。

その他にも、12 月 22 日、12 月 27 日、2018 年 1 月 15 日、1 月 19 日、1 月 23 日にもポートスキャンがあった。これらのポートスキャンについて、統合ネットワーク監視による警報は上がらなかった。

2.3. 内部システム（イントラ業務システム）への不正なアクセス

2017 年 12 月 20 日から 2018 年 1 月 26 日にかけて、イントラ業務システムに対し、前記の仮想マシン P と Q を経由した不正なアクセス（図 1 の❼）があったことがログから判明した。前記のメールシステムでの被害アカウントの第 1 グループに属する 3 名のパスワードを用いて、イントラ業務システムに不正ログインされていた。

ログを精査したところ、イントラ業務システムの一部に対して不正に閲覧されたが、重要な業務システム（知的財産管理システム、健康管理システム等）へのアクセスはなく、また、イントラ業務システムからファイルをダウンロードしたという記録はなかった。

2.4. 内部システム（ファイル共有システム）への不正なアクセス

内部ネットワークには、主に本部組織の業務用ファイルの置き場所として、ファイル共有サーバ（以下「FSS」という。）がある。そのログインアカウントは、前記のメールシステムやイントラ業務システムと共通のパスワードで利用できるようになっている。

そのため、前記のメールシステムへの不正ログインのあったアカウントのうちの一部が、FSS への不正ログインにも利用されていた。FSS のログから抽出したところ、前記の第 1 グループの 100 名のうち 3 名のアカウントに対して、第 2 グループの 43 名のうち 4 名のアカウントについて 、前記の踏み台（仮想マシン P 及び Q）と（図 1 の❽）、後述する別の踏み台（使用電力量モニタサーバ）から（図 1 の⓮）の不正接続を受けていた。

これにより一部のファイルを不正にコピーされていた。不正にコピーされたファイルはログから特定できたので、そのファイルの内容の調査を行った。その調査結果は本報告書本文に示した。

3. 管理用ネットワークへの侵入

3.1. 内部システム（使用電力量モニタサーバ）への侵入

産総研の内部ネットワークは、全体としてはフラットなネットワークであったが、業務システムを管理するサーバ等については、独立した管理用ネットワークに置かれており、個別にアクセスコントロールリストによりアクセス元 IP アドレスを制限し、管理機能に直接アクセスできないように設計されていた。ところが、管理用サーバの置かれたネットワーク内に、このアクセス制限を施していなかった使用電力量モニタサーバがあり、これが不正侵入され、踏み台とされた（図 1 の❿）ことにより、管理用ネットワーク内の各種サーバにまで不正なアクセスを許す事態（図 1 の⓫⓯）となっていた。

使用電力量モニタサーバは、使用電力量をイントラ業務システムに表示するために後から設置されたサーバで、その管理は、情報基盤部とは別の組織が管理していたが、アクセス元 IP アドレスを制限する必要性の認識が共有されていなかった。

不正なアクセスには、リモートデスクトップが用いられ、ID・パスワードにより不正ログインされ、遠隔操作された（図 1 の❿）。不正ログインされた原因は以下のように分析している。

使用電力量モニタサーバの管理を担当していた職員が、前記のメールシステムの第 1 グループの被害アカウントに該当していた。当該アカウントの利用者である職員に聞き取り調査を行い、どのようなメールのやり取りがあったかを確認したところ、以下のことが判明した。

2017 年 8 月に、使用電力量モニタサーバで不具合が発生した際、当該職員は、自ら調査をすべく、当該サーバの管理者パスワードを、運用を委託している外部委託業者にメールで教えてほしいと依頼した。この際、当該サーバの IP アドレスと ID を電子メール中に記載した。これに対し、同社は、当該パスワードを記載したテキストファ

イルを暗号化 ZIP ファイルとし、添付ファイルとして電子メールで回答した。

こうしたやり取りの電子メールは、メールシステムにログインして、検索機能を用いて「パスワード」で検索することで、容易に見つけられる状態になっていた。

添付ファイルは暗号化されていたが、その復号用のキーは、当該職員が当該業務に着任して最初に同社と連絡を取り合った際に、同社から、「パスワードルール」として、産総研の略号等にメールの送信日を加えたものとする旨の連絡をメールで受け取っていた。

これらのことから、侵入者は、当該職員のメールシステムアカウントに不正ログインし、「パスワード」でメールを検索することで、管理者パスワードの回答メールと「パスワードルール」のメールを発見して、添付ファイルの ZIP の暗号を復号し、その中にある使用電力量モニタサーバの管理者パスワードを窃取したものと推定できる。

3.2. 内部システム（外部委託業者のサーバ）への侵入

2018 年 1 月 16 日から 2 月 8 日にかけて、ネットワーク管理業務を担当する外部委託業者が構築･運用していた、syslog サーバ（各種ログをネットワーク経由で集約するためのサーバ）及びネットワーク監視用サーバの 4 台が、仮想マシン P と使用電力量モニタサーバから侵入されていた（図 1 の⓫）。

侵入された原因は､第 1 に､アクセスコントロールリストによる接続元 IP アドレスの制限をしていなかったこと、第 2 に、ログイン用のパスワードが安易なものであったこと、第 3 に、古い OS を用いていたことが挙げられる。

ネットワーク監視用サーバの 1 台は脆弱性を突かれて侵入された痕跡があり、他のサーバは ID・パスワードにより不正ログインされていたことが、フォレンジック調査により判明した。

パスワードには、アカウントの ID と同一のものがあったほか、英単語中の「a」を「@」に、「i」を「1」に置き換えただけのものなど、安易なものが使われていた。加えて、担当者の交代があっても、これらのパスワードが 5 年以上にわたって変更されておらず、使われなくなったアカウントも削除されず残っていた。

古い OS については、サーバの一部が、同社との今回の契約以前から使い続けられていたもので、更新されていなかったことに加え、OS 自体がサポート切れであるにもかかわらず更新されていなかった。サポート期限切れの OS は脆弱性修正パッチが未適用になるということであり、セキュリティリスクが極めて大きいが、対処できていなかった。

侵入された 4 台のうちの 2 台にマルウェアを置かれ、遠隔操作による他への攻撃の踏み台とされていた。そのうちの 1 台は、後述する LDAP サーバの不正検索のための踏み台となった。

また、このうちの 1 台である syslog サーバが、同社従業員らにより、作業用のファイルサーバとして目的外に使用されており、同社が運用している多数のネットワーク機器の管理パスワードが暗号化されずに保管されていた。これらのネットワーク機器に不正操作の形跡はなかったが、後述する LDAP サーバの検索用 ID・パスワードも、このサーバに暗号化されずに保管されていたことから、これが閲覧され、窃用された可能性がある。

本事案の発覚後に調査を行うまで、このサーバが管理パスワードの保管場所として利用されていたと把握できておらず、正規の作業用のファイルサーバにて管理されているものと認識していた。

3.3. LDAP サーバでの不正検索

2018 年 1 月 22 日から 2 月 8 日にかけて、IP アドレスでアクセス制限していた LDAP サーバに対して、前記外部委託業者のサーバを踏み台とし、同サーバで閲覧したと考えられる ID・パスワードが窃用され、LDAP 検索が行われていた（図 1 の⓬）。LDAP サーバのログによれば、全職員のアカウントの記録（レコード）を窃取されていた。

この LDAP のレコードには、氏名、所属等の情報がある他、認証サーバでログインに用いる ID 並びに暗号化されたパスワード及びハッシュ化されたパスワード（ソルト付き）が含まれており、これらが 2018 年 1 月 23 日の時点で侵入者の手に渡ったと推定できる。

このタイミングでメールシステムへの第 2 グループへの不正ログインが開始されていることから、ハッシュ化されたパスワードに対してオフライン攻撃[8]によるパスワード復元が試みられ、これにより復元されたパスワード

で、第2グループ43名の被害アカウントへの不正ログインに至ったと推定できる。

3.4. ファイル共有サーバへの管理者権限での接続

踏み台となった使用電力量モニタサーバから、ファイル共有サーバ（FSS）に管理者権限で共有接続していた（図1の⓮）痕跡があった。FSSの管理者パスワードを特定された原因は、以下のように推定する。

第2グループに含まれる被害アカウント（図1の⓭）でFSSに不正ログインされて（図1の❽）コピーされたファイルの中に、FSSの管理者パスワード及びほぼ全てのイントラ基盤システムの管理者パスワードが、簡単な鍵で暗号化された状態で置かれていた。このためこれを即座に復号されて、パスワードを窃取されたものと推定できる。

使用電力量モニタサーバのフォレンジック調査により、FSSから管理者権限でコピーされたファイルのリストは特定できた。

管理者権限でコピーされたこれらのファイルについてファイアウォールの送信ログの分析によれば、外部に直接に送信された形跡があった。

3.5. サーバ仮想基盤の管理コンソールへの不正ログイン

踏み台となった使用電力量モニタサーバから、サーバ仮想基盤の管理コンソールに不正ログインされた（図1の⓯）痕跡が見つかった。

管理コンソールからは仮想マシンの起動・停止や、ネットワークの構成変更等が可能であるが、管理コンソールから閲覧できる情報には、漏えいが問題となるような情報がなく、また、ログには不正な操作を行った痕跡はなかった。

しかし、不正なファイルを設置してログを消去することは可能であることから、万全を期すため、サーバ仮想基盤及びサーバ仮想基盤上で動作する全ての業務システムの再構築を行って対処することとなった。

4. 研究用サーバ等への攻撃

4.1. 研究用サーバMへの不正なアクセス

Y研究センターの研究用サーバの1台に、マルウェアが設置され、踏み台とされていた（図1の❾）が、このサーバを踏み台にした他のサーバへの攻撃は成功していなかった。

このサーバはディスク監視用のサーバであり、重要な情報は置かれていなかった。ファイアウォールの記録から、2018年2月5日にデータが外部へ送信されていたことが判明したが、①このサーバには監視サーバのプログラムと監視データのみが置かれていたこと、②このサーバを踏み台にした他のサーバの情報の窃取に失敗していたこと、③このサーバの削除されたディスク領域からファイルの復元を試みたところ、他のサーバにあったと考えられるファイルが一つも見つからなかったことから、重要な研究情報は外部へ送信されていないと推定できる。

4.2. 複数の研究部門に設置されていたNASへのマルウェア感染

複数の研究部門に設置されていたネットワーク接続ハードディスク装置（以下「NAS」という。）の4台からマルウェアが検出されたほか、他のNAS2台にもマルウェア感染と見られる形跡があった。

これらのNAS製品にはOSコマンドインジェクションを始めとする重大な脆弱性が過去に発覚しており、脆弱性対応がなされていなかったことから、内部ネットワーク経由でマルウェアに感染したものと推定できる。

このうちの少なくとも1台は、使用電力量モニタサーバを遠隔操作するための踏み台として利用され、2018年2月9日の最後の不正事象として、使用電力量モニタサーバのイベントログ消去のために用いられた。

---

[8]「オフライン攻撃」は、ハッシュ化されたパスワードや暗号化されたファイル等を窃取した攻撃者が、攻撃者のコンピュータ上で、辞書攻撃や総当たり攻撃によって推測したパスワードを試行する手法で、攻撃者の利用可能な計算資源により、例えば1秒間に数百万～数千万回といった、高速な試行が可能なものである。対する「オンライン攻撃」は、ネットワークを通じてログイン画面にID・パスワードを入力して試行する手法で、1秒間に数十～数百回程度しか試行できない。この違いから、オンライン攻撃では不正ログインされることのない比較的強固なパスワードでも、オフライン攻撃では復元されてしまう場合がある。

4.3. 他の研究部門の研究用サーバへの侵入試行の痕跡

Z 研究センターのデータサーバ 2 台のファイル共有領域から、サーバ M を踏み台としてデータを窃取しようとしていた痕跡があった。フォレンジック調査を行ったところ、データ窃取に至る侵害の痕跡がなく、また、サーバ M にもデータをコピーできた痕跡が発見されなかった。

共有フォルダの名前は参照できたものの、パスワードの入手に至らず、データのコピーには至らなかったものと推定できる。

その他、全ての研究部門について、研究用データを置いているサーバ数百台について調査を行ったところ、踏み台からアクセスされたログは確認されなかった。また、安価な NAS 製品の一部にはアクセスログを記録していないものや、取得できないものがあったが、これらにおいては、重要なデータが置かれていなかったことが確認された。

被害を発生・拡大させた要因と再発防止のための対策

被害を発生・拡大させた要因		再発防止のための対策	
		応急的対策	抜本的対策
①システム・機器の問題	・メールシステムのログイン方法	・外部からはVPN接続を必須とする運用とし、内部ネットワークからログインする場合でも、一定期間ごとに二段階認証を求めるよう認証方式を強化	・左記と同様
	・内部サーバと連携していた外部サイト	・必要性と安全が確認できないサーバ等は全て遮断	・外部接続には、ネットワーク構成、管理者の知識・能力、管理体制等について厳格な審査を実施
	・広域でフラットな内部ネットワーク	・研究ネットワークと管理用ネットワークを分離	・研究用ネットワークをセグメント分離できるネットワークを構築
	・内部ネットワークの監視	・SIEMの自動検知ルールの見直し	・セグメント間の内部通信監視を導入 ・重要システムのログ冗長化・遠隔保存
	・アクセス制限のなかった管理用ネットワークのサーバ	・管理用ネットワーク内の全てのサーバにアクセス権限を設定	・左記と同様
	・情報機器の脆弱性	・脆弱性が指摘されたNASの使用を中止し、研究部門から回収	・情報機器の脆弱性情報の所内徹底
②パスワード・暗号鍵の管理と強度の問題		・有効なパスワードの設定方法、管理方法を検討し情報基盤部で運用を開始	・有効なパスワードの設定方法、管理方法について改めて検討し、情報セキュリティ実施ガイド等に反映
③外部委託事業者の管理の問題		・老朽化サーバを廃止し、新規サーバへ交換	・関連業務を一括契約し、外部委託業者の数を減らす ・情報セキュリティ対策の履行状況の定期的な確認 ・情報セキュリティ監査の実施
④マネジメントの課題		－	・組織体制の見直し ・事業継続計画（BCP）の見直し