NUICレター No.2019−3 名古屋大学情報基盤センター

標的型攻撃メール対応訓練とセキュリティ意識向上

Targeted Email Attack Prevention Training and Information Security Awareness Raising

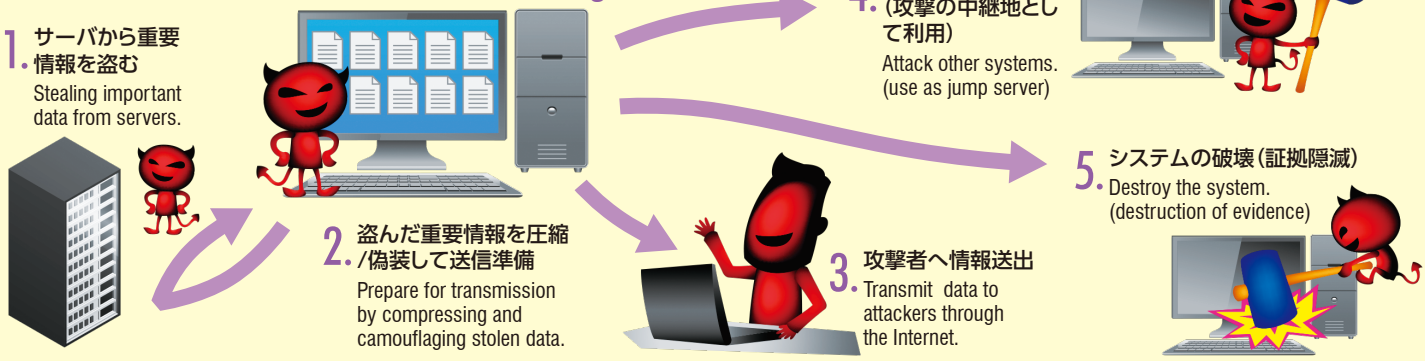
標的型攻撃の脅威に対抗するために必要なこと
How to Defend Against the Threat of Targeted Attacks

標的型攻撃とは What is an Advanced Persistent Threat ?

組織等が持つ重要情報等を窃取するために、あらゆる方法で執拗に行われる攻撃を標的型攻撃（APT: Advanced Persistent Threat)といいます。利用者に攻撃の進行を気づかせない工夫がなされるため、数か月後に被害に気付く例も多く、発見・防止が非常に困難なサイバー攻撃の一つです。
攻撃の初期段階では不審メールが使われる場合が多く、標的にマルウェアを送りつけて感染させたり、フィッシングサイトに誘導して認証情報を窃取したりと、攻撃の足掛かりを作ろうとします。これは、「標的型攻撃メール」と呼ばれ、特段の注意が必要です。
攻撃の初期段階が成功すると、様々な攻撃に発展します。場合によっては、他人への加害者にされてしまう可能性もあります。

Malicious actors may launch persistent, varied attacks in order to steal sensitive information from corporations and other organizations. This is known as an Advanced Persistent Threat (APT). As it is designed to go unnoticed by the system users and maintainers, it often takes months to discover the intrusion and damage caused. In this way, this type of cyberattack is very difficult to detect and prevent.
In many instances, this type of attack starts with a suspicious email, known as a Targeted Email Attack. Targeted email attacks use a variety of methods, such as malware attachments that infect your computer or links to phishing sites that steal authentication information, to create a foothold for further infiltration. For this reason, we must exercise a high degree of caution with emails.
Once this first step has succeeded, the attack can advance in a variety of ways (see diagram). In some cases, the victim may then be used to attack other people.

起こりうる被害 Possible damage



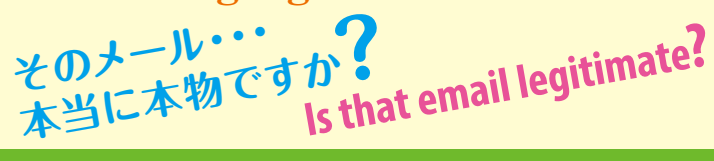
標的型攻撃に対抗するために Defending Against APTs

情報連携統括本部では、「標的型攻撃メール」による被害を防ぎ、万一の時に被害を最小限にとどめるため、毎年、全教職員を対象に「標的型メール攻撃対応訓練」を実施しています。訓練を通じて知ってほしい、標的型攻撃から自身の身を守るためのエッセンスを掲載したので、是非ご覧ください。

In order to prevent damage from such Targeted Email Attacks, or, in a worst-case scenario, to limit the amount of damage caused, Information & Communications holds yearly “Targeted Email Attack Prevention Training” for the entire faculty and staff. Please visit the I&C website to see what training can teach you about the essentials of protecting yourself from targeted attacks.

標的型メール攻撃に対する啓発用コンテンツ
（名古屋大学情報連携統括本部サイト）
http://www.icts.nagoya-u.ac.jp/nu-only/ja/security/Targeted-mail.html

Awareness Raising Materials for Targeted Email Attacks (NU I&C website)
http://www.icts.nagoya-u.ac.jp/nu-only/en/security/Targeted-mail.html



過去の標的型攻撃の事例 Cases of past APT

● 知らない人からのメールだが、開封せざるを得ない内容
Content that prompts you to open even though it's coming from an unknown sender.

1.新聞社等から取材依頼 An interview requests from a newspaper company.
2.就職活動（問合せ、履歴書送付） Inquiry or CV attachment related to a job application.
3.教育、研究、イベント等への問合せ・クレーム Inquiry or complaint related to the education, research, or enents at the University.
4.アンケート調査 Survey
5.学会等からの案内 Communication from an academic society.

● 誤って自分宛に送られたメールのようだが、興味を持たされる内容
Seems be sent erroneously but the content is interesting.

1.議事録等の内部文書送付 Sending an internal document such as minutes.
2.VIP訪問に関する情報 Information related to a VIP visit.

名古屋大学情報連携統括本部の情報サービス
Services Provided by Nagoya University Information & Communications

名古屋大学情報連携統括本部は、教職員・学生に様々な情報サービスを提供しています。
Nagoya University Information & Communications offers a variety of information services to staff, faculty and students.
http://www.icts.nagoya-u.ac.jp/ja/services/ http://www.icts.nagoya-u.ac.jp/en/services/

名古屋大学無線ネットワーク NUWNET
http://www.icts.nagoya-u.ac.jp/ja/services/nuwnet/

Nagoya University Wireless Network (NUWNET)
http://www.icts.nagoya-u.ac.jp/en/services/nuwnet/

学内各所に、名大IDで利用できる無線LAN基地局（SSID:nuwnet）が配置されています。 Wireless LAN Access Points (SSID: nuwnet) have been installed in many locations throughout our campus. You can connect to them using your Nagoya University ID.

全学メール
http://www.icts.nagoya-u.ac.jp/ja/info/mail.html

Nagoya University Mail Service email address
http://www.icts.nagoya-u.ac.jp/en/services/numail/

名大の教職員・学生であれば、どなたでも、情報連携統括本部が発行する「全学メールアドレス」を取得することができます。 Any Nagoya University staff, faculty member, or student can obtain a "Nagoya University Mail Service email address" issued by Information & Communications.

サイトライセンス取得ソフトウェア
http://www.icts.nagoya-u.ac.jp/ja/services/sitelicense/

Site Licensed Software (Limited to the University)
http://www.icts.nagoya-u.ac.jp/ja/services/sitelicense/

Symantec Endpoint Protection, Mathematica9など様々なソフトウェアのサイトライセンスを取得しています。 Nagoya University has several site licenses for software, such as Symantec Endpoint Protection, Mathematica9, etc.

ソフトウェア資産管理（SAM）
https://sam.icts.nagoya-u.ac.jp/sam/public/auth/loginselect

Software Asset Management System (SAM)
https://sam.icts.nagoya-u.ac.jp/sam/public/auth/loginselect

平成26年4月1日にソフトウェア資産管理規程を施行し、同日から新規購入したハードウェア及びソフトウェアの登録を義務化しました。ソフトウェア資産管理（Software Asset Management System, SAM）を運用し、名大内の組織が保有するハードウェア及びソフトウェア並びにライセンスを適切に管理します。 Nagoya University has implemented the Software Asset Management Rules, which went into effect on April 1, 2014, requiring all hardware and software purchased from that day forward to be registered. By using the Software Asset Management System (SAM), hardware, software, and licenses possessed by organizations within Nagoya University are managed appropriately.

eduroam
http://www.wnet.icts.nagoya-u.ac.jp/manual/eduroam.html

WLAN roaming infrastructure eduroam
http://www.wnet.icts.nagoya-u.ac.jp/manual/eduroam.html

eduroam参加機関の無線LAN基地局を名大IDで利用することができます。 You may access the internet using your Nagoya University ID through the wireless LAN access points of any institutions participating in eduroam.

NUCT
https://ct.nagoya-u.ac.jp

Nagoya University Collaboration and Course Tools (NUCT)
https://ct.nagoya-u.ac.jp

ネットワーク上で講義資料の配付、出席確認、成績確認などができる便利なツールNUCT（Nagoya University Collaborationand Course Tools）があります。 There is a useful tool, the NUCT (Nagoya University Collaboration and Course Tools), that you can use to distribute class materials or check attendance and grades.

情報メディア教育システム
http://www.icts.nagoya-u.ac.jp/ja/media/

Information Media Studies System
http://www.icts.nagoya-u.ac.jp/en/media/

授業や自習のための環境としてコンピュータ室があります。主センターラボ（工学部7号館）の他に、9部局のサテライトラボに分散して配置されています。 The Information Media Studies System provides computer rooms as environments for classes and self-study. These computer rooms include the main center laboratory (School of Engineering Building 7) and a number of satellite laboratories distributed among nine other departments.

ITヘルプデスク
http://www.icts.nagoya-u.ac.jp/ja/helpdesk.html

IT Help Desk
http://www.icts.nagoya-u.ac.jp/en/helpdesk.html

情報サービス全般に関する相談窓口として「ITヘルプデスク」を開設しています。
TEL: 052-747-6389（内線：6389） it-helpdesk@icts.nagoya-u.ac.jp

We have opened the “IT Help Desk” as a one-stop consultation desk for information services.
TEL: 052-747-6389 (direct number to IT Help Desk) (ext. 6389)

HPCI 機関唯一の「京」コンピュータ型スパコン FX100 が利用できる講習会があります。
Workshops are held where you can use the only K-computer-based FX100 supercomputer available among HPCI-registered institutions.

「FX100 システム利用型 MPI 講習会（初級）」（2020 年 2 月 5 日）、「FX100 利用型ライブラリ利用講習会（初級）」（2020 年 3 月 4 日）を開講予定です。
The following workshop sessions are scheduled: “FX100 System-Base MPI Workshop (for beginners)” (February 5, 2020) “FX100-Base Library Use Workshop (for beginners)” (March 4, 2020)

詳しくは／For details, please visit ▶ https://www2.itc.nagoya-u.ac.jp/cgi-bin/kousyu/csview2.cgi

発行・編集：名古屋大学情報連携統括本部広報委員会 〒464-8601 名古屋市千種区不老町 TEL:052-789-4352 FAX:052-789-4385
Issued/Edited by the Public Relations Committee, Information & Communications, Nagoya University
Furo-cho, Chikusa-ku, Nagoya 464-8601, Japan TEL: +81-52-789-4352 FAX: +81-52-789-4385
2020年1月 January.2020