NRI SECURE

Internet Week 2018

D2-3 知れば組織が強くなる！ペネトレーションテスト
で分かったセキュリティ対策の抜け穴

丸ごとわかるペネトレーションテストの今

2018年11月28日

NRIセキュアテクノロジーズ株式会社
サイバーセキュリティーサービス事業本部
サイバーセキュリティーサービス一部

セキュリティコンサルタント
石川　朝久, Ph.D., CISSP, CSSLP, CISA, CISM, CFE, PMP

はじめに：講演者紹介

石川　朝久（ISHIKAWA, Tomohisa）

- **所属　：ＮＲＩセキュアテクノロジーズ株式会社**
- **役職　：セキュリティコンサルタント**
- **専門　：攻撃技術・不正アクセス技術（= Red Team）**
  - セキュリティ診断・侵入テスト・インシデント対応など、攻撃技術を軸にした技術コンサルタント
- **資格　：博士（工学）, CISSP, CSSLP, CISA, CISM, CFE, PMP**
  GIACs（GSEC, GSNA, GPEN, GWAPT, GXPN, GREM, GCIH, GCFA, GWEB）
- **主担当プロジェクト**
  - **情報サービスA社**　**AKB48選抜総選挙投票システムへのセキュリティ診断**
  - 金融B社　グループ共通セキュリティ診断スキームの構築・実行支援
  - 金融C社　セキュリティ戦略・CSIRT運用・実行支援
- **対外活動（抜粋）**
  - ASEAN諸国　政府官僚向けセキュリティ管理研修講師（2010）
  - DEFCON 24 SE Village Speaker (2016)
  - **IPA 情報処理技術者試験委員・情報処理安全確保支援士試験委員（2018~）**
  - **オライリー社『インテリジェンス駆動型インシデントレスポンス』翻訳・監訳（12/26発売予定！）**

O'REILLY®
オライリー・ジャパン

インテリジェンス駆動型インシデントレスポンス

攻撃者を出し抜くサイバー脅威インテリジェンスの実践的活用法

Scott J. Roberts
Rebekah Brown 著

石川 朝久 訳

D2-3 知れば組織が強くなる！ペネトレーションテストで分かったセキュリティ対策の抜け穴

1）丸ごと分かるペネトレーションテストの今

- 時間：16:15 – 17:10
- 講演者：石川　朝久（NRIセキュアテクノロジーズ株式会社）

⇒ **ペネトレーションテストの概要と、国内外の動向について把握する。**

2）Sansanがペネトレーションテストを受けてきた3年間の記録

- 時間：17:10 – 17:45
- 講演者：河村 辰也氏（Sansan株式会社）

⇒ **ペネトレーションテストを受ける立場から、実践的な経験談を聞く。**

3）ペネトレーションテスト実務者座談会

- 時間：17:50 – 18:45
- 講演者：小河氏、北原氏、大塚氏、ルスラン氏、中津留氏

⇒ **ペネトレーションテストを実施する立場から、組織として気を付ける対策を聞く。**

はじめに：

本日のテーマとお話したいこと

- 1. そもそもペネトレーションテストとは？
- 2. 具体的なシナリオから考察
- 3. 国外の動向
- 4. まとめ

1. そもそもペネトレーションテストとは？

ペネトレーションテストとは？

Gartnerによれば…

- **実際の攻撃テクニックで、事前に設定した目標を達成可能か検証し、組織のセキュリティレベルをチェックすること！！**

- ３種類の要素を定義することが大事
  - 目標（Test Objective）
  - スコープ（Scope）
  - 実施条件（Rule of Engagement）

Gartner：*“Using Penetration Testing and Red Teams to Assess and Improve Security”* (2017.04.17)

ペネトレーションテストとは？

目標（Test Objective）

- 例）情報漏洩の潜在的影響を確認したい！！
- 例）脆弱性管理などの有効性を検証したい！！
- 例）監視・MSSサービスの実力を評価したい！！

スコープ（Scope）

- ネットワーク、Webアプリ、標的型攻撃、無線LAN…

実施条件（Rule of Engagement）

- 実施時間、連絡先、禁止事項、データの取り扱い…

Gartner：*“Using Penetration Testing and Red Teams to Assess and Improve Security”* (2017.04.17)

言葉の定義：「脆弱性診断」と何が違うのか？

- 脆弱性診断（Vulnerability Assessment）のポイントは**網羅性**！！
- ペネトレーションテストのポイントは、**目的達成の検証有無**！！

	脆弱性診断	ペネトレーションテスト
目的	脆弱性を**網羅的に洗い出す**こと	**目的を達成するために**、必要な脆弱性を発見・評価・悪用すること。
アプローチ	ギャップ分析アプローチ	リスクベースアプローチ
方法	**静的**な方法論 → ツール重視	**動的**な方法論 → マニュアル重視
脆弱性の悪用	控えることが多い	実際に悪用する
報告書	個別の脆弱性リスト	シナリオベース
実施時間	**数日**	**数日～数週間**
頻度	毎日～毎年	１年間に１回ぐらい
費用	$ ~ $$	$$ ~ $$$$

国内の動向：TLPT

- **日本：高いセキュリティが要求される金融業を中心にTLPTというキーワードが登場**
  - **TLPT**（**T**hreat-**L**ead **P**enetration **T**est）：脅威ベースのペネトレーションテスト

金融庁：平成29事務年度　金融行政方針

大規模な金融機関については、そのサイバーセキュリティ対応能力をもう一段引き上げるため、より高度な評価手法[14]の活用を促す。また、金融機関に対し金融ISAC[15]等を通じた情報共有の一層の推進を促す。

加えて、「G7サイバーエキスパートグループ」[16]をはじめ、様々な国際会議でサイバーセキュリティの議論が行われており、各国当局とともに具体的な方針の策定に貢献していく。

---

[13] 同方針では、（ｉ）サイバーセキュリティに係る金融機関との建設的な対話と一斉把握、（ii）金融機関同士の情報共有の枠組みの実効性向上、（iii）業界横断的演習の継続的な実施、（iv）金融分野のサイバーセキュリティ強化に向けた人材育成、（ｖ）金融庁としての態勢構築、の５項目を柱としている。

[14] 例えば、金融機関（外部ベンダー等の利用を含む）による脅威ベースのペネトレーションテスト（テスト対象企業ごとに脅威の分析を行い、個別にカスタマイズしたシナリオに基づく実践的な侵入テスト）。

Source：https://www.fsa.go.jp/common/about/research/20180516/TLPT.pdf
Source：https://www.fsa.go.jp/news/29/2017StrategicDirection.pdf

国内の動向：TLPT – 脅威ベースのペネトレーションテスト

キーワード１：脅威

- 脅威：**敵対的意図　× 機会　× 能力**
  - **敵対的意図**
    - （攻撃者の）動機　×　組織的資産　×　組織的特徴
  - **機会**
    - 攻撃するポイントがあるか？（外部環境　×　**内部環境**）
    - **内部環境が、防御側が唯一コントロールできるパラメータ**
  - **能力**
    - 具体的な攻撃テクニック・技術

国内の動向：TLPT – 脅威ベースのペネトレーションテスト

キーワード２：実施する上での特徴

Continuous Operation（継続的な実施）

- 攻撃側（**Red Team**）が継続的に新しい攻撃テクニックを試行し、防御側（**Blue Team**）の技術・プロセス面で弱い部分を常に探し続けること。

Iterative Collaboration（反復的なコラボレーション）

- テスト終了後に攻撃側・防御側が議論し合い、課題の改善を行っていくPDCAを行う。（**Purple Teaming**）
- これにより、組織のセキュリティを強化する！！

Real Threat Based Scenarios（現実の脅威に基づくシナリオ）

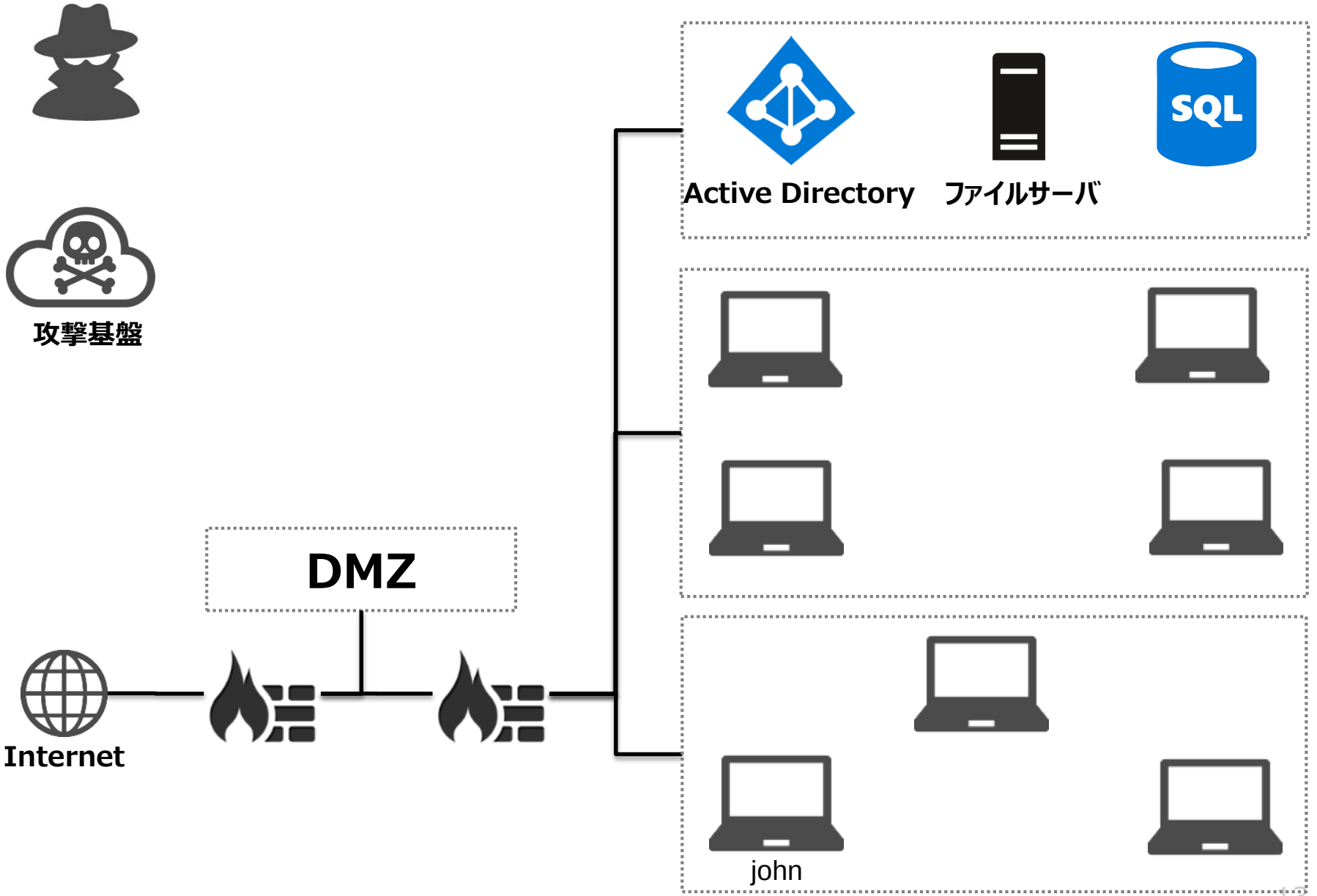
- 実際の脅威動向をもとに、シナリオを組み立てていく。
- 想定する脅威次第では、24時間いつでも実施することもある。

Gartner：*“Using Penetration Testing and Red Teams to Assess and Improve Security”* (2017.04.17)

2. 具体的なシナリオから考察

～仮想企業E-Corpを例に～

OA環境をターゲットとした標的型攻撃を想定する場合



OA環境をターゲットとした標的型攻撃を想定する場合

E-Corpのプロファイル

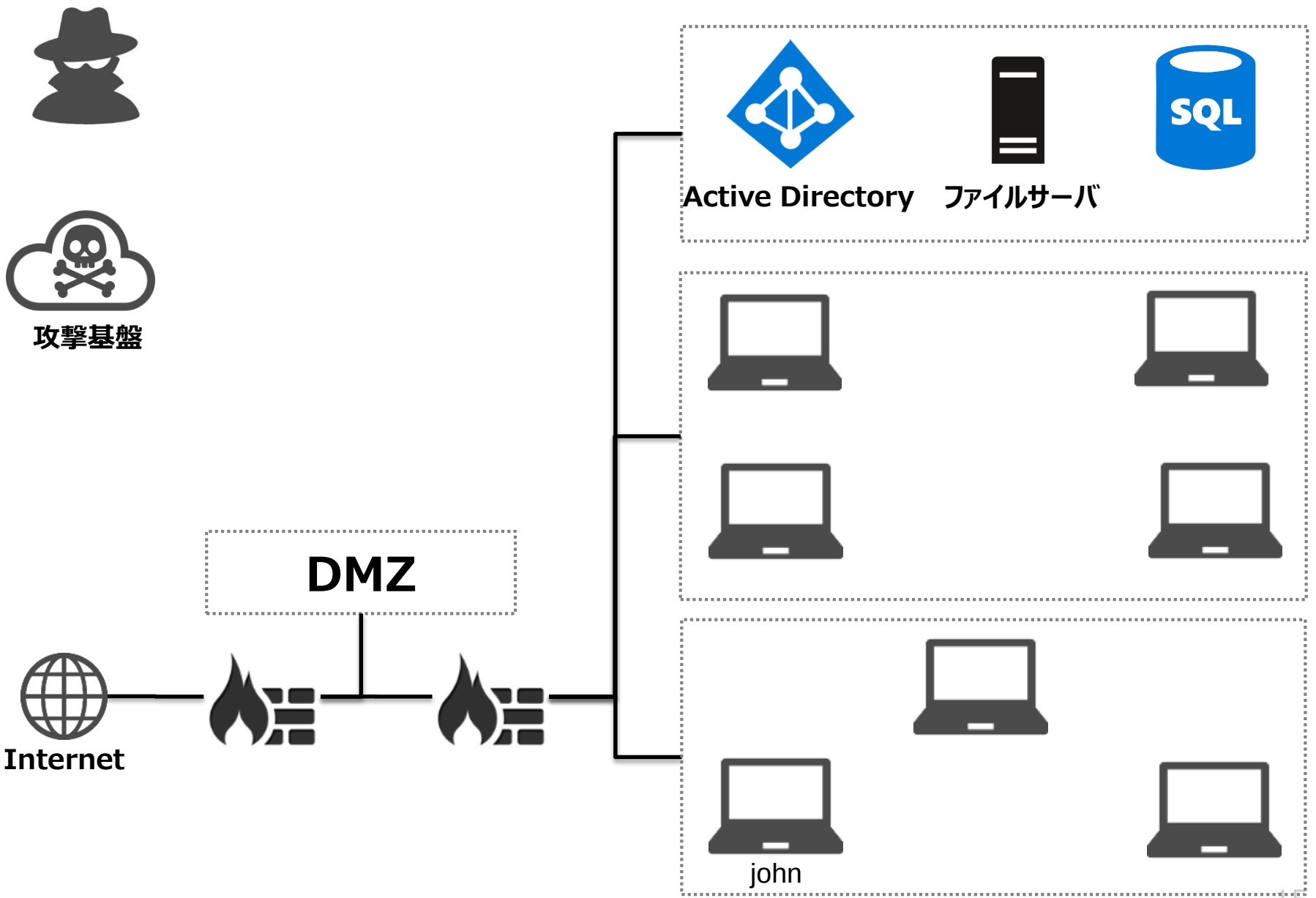
- **脅威**：**敵対的意図　× 機会　× 能力**
  - 動機　　：社内の多くの機密情報・知的財産を窃取したい
  - 組織的資産　　：多くの重要情報・知的財産を保有
  - 組織的特徴　　：B2B企業（Webからの情報窃取は望みが薄い）

- **機会**（外部環境　×　**内部環境**）
  - 外部：E Corpの利用環境において、様々な脆弱性が発見されている
  - 内部：パッチ管理など基本的な活動はやっている。不備がないか不安。

- **能力**
  - 日々攻撃を受けているが、洗練された攻撃者に過去やられた経験があり、同じような攻撃者が狙ってくると考えている。
  - 特に知的財産を狙う攻撃者は多い。

OA環境をターゲットとした標的型攻撃を想定する場合

偵察・武器化
配送
攻撃
インストール
遠隔操作
侵入拡大
目的実行



ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-Stage Channels
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy

Source : https://attack.mitre.org/

PIVOTS X PAYLOADS

SIMULATE A FULL-SCALE HIGH-VALUE PENETRATION TEST

GAME PIECES


X-Ray Specs


Ono Sendai Cyberspace 7


The Hero's Slingshot


King Arthur's Rabbit


Code Injector


Cyber Web Crawler of Cybor


My First Burner Phone


Mr. Rogue AP


The Clipboard of Authority


Light Sword of Holding


Black Magic Wand of SEC760


SANS Netwars Energy Drink

GAME MODIFIERS

Build a Home Pen Test Lab — BONUS TURN www.sans.org/webcasts/building-super-duper-home-lab-105640	Play SANS Holiday Hack Challenge — Go Forward 2 Spaces www.holidayhackchallenge.com
Read SANS Pen Test Blogs — Opponent Loses Turn https://pen-testing.sans.org/blog	Watch SANS Pen Test Webcasts — Advance to Next Phase www.youtube.com/sanspentesttraining
Take SANS Pen Test Training — BONUS TURN www.sans.org/pentest	Listen to Internet Storm Center Daily Podcast — All Opponents Lose a Turn https://isc.sans.edu/podcast.html
Attend an InfoSec Conference — Go Forward 3 Spaces https://infosec-conferences.com/	Participate in SANS Netwars — Advance to Next Phase www.sans.org/netwars

SANS Download a PDF version of the Pivots & Payloads poster, additional game pieces, and game modifiers at www.sans.org/boardgame

SANS The Most Trusted Source for Information Security Training, Certification, and Research

PIVOTS X PAYLOADS

SIMULATE A FULL-SCALE HIGH-VALUE PENETRATION TEST

Reporting

Use your packet capture to help show network trust relationships	You realize you didn't take enough screenshots: *PANIC!* **ROLL DICE, SKIP THAT MANY TURNS**	You took screenshots the entire time! Good job	Your notes were well written and easy to follow	Your proofreader has the week off, **SKIP NEXT TURN** while you find a replacement	You add the target organization's alerts to show they have detection capabilities	Target organization likes draft report! Gives feedback in a timely manner	Target organization wants you to present the findings to the board of directors **SKIP NEXT TURN TO PREPARE**

Post-Exploitation

Host Blue Team catches you **SKIP NEXT TURN**	DLP is only looking at email, so you can exfil data with ease	You find SQL injection on internal web app	Target organization runs Kansa module and sees your process injection **GO BACK 3 SPACES**	You are able to set up a passive listener on client network	Get additional credentials from configuration files	Look through local system and network shares for interesting files	Outbound firewall configuration limits access **GO BACK 2 SPACES**	That was a honey doc! Busted **SKIP NEXT TURN**	Enumerate users and grab more password hashes

Exploitation

Find GitHub repo with working exploit	Exploit causes app to crash, client mad **SKIP NEXT TURN**	Your custom payload evades AV and IDS	Misconfigured service; no exploit required!	Firewall stops stager from calling home **GO BACK 2 SPACES**

Pivoting

You create your own 0-day	DNS cache shows systems already communicating	Target organization didn't segment networks appropriately; you can pivot with ease	Target organization's SOC detects your lateral movement **SKIP NEXT TURN**	Target organization is not reviewing NetFlow data; you remain undetected

Password Attacks

Cracked service account password	Target organization's admin accounts use multi-factor authentication **GO BACK 2 SPACES**	You use a honey account and get caught **SKIP NEXT TURN**	Crack passwords with Hashcat	Steal hashes with Metasploit hashdump

Scanning

You forget to throttle scan and create disruption **SKIP NEXT TURN**	Discover unpatched remote exploit	Verify findings from search engine recon	Target organization MSSP detects your scans **GO BACK 2 SPACES**	You discover a large number of open TCP and UDP ports

Scoping & Rules of Engagement

Scoping call went great!	Target organization provides lists of systems to attack	Target organization gives your "victory conditions"	Client wants to modify scope **GO BACK TO START**

Reconnaissance

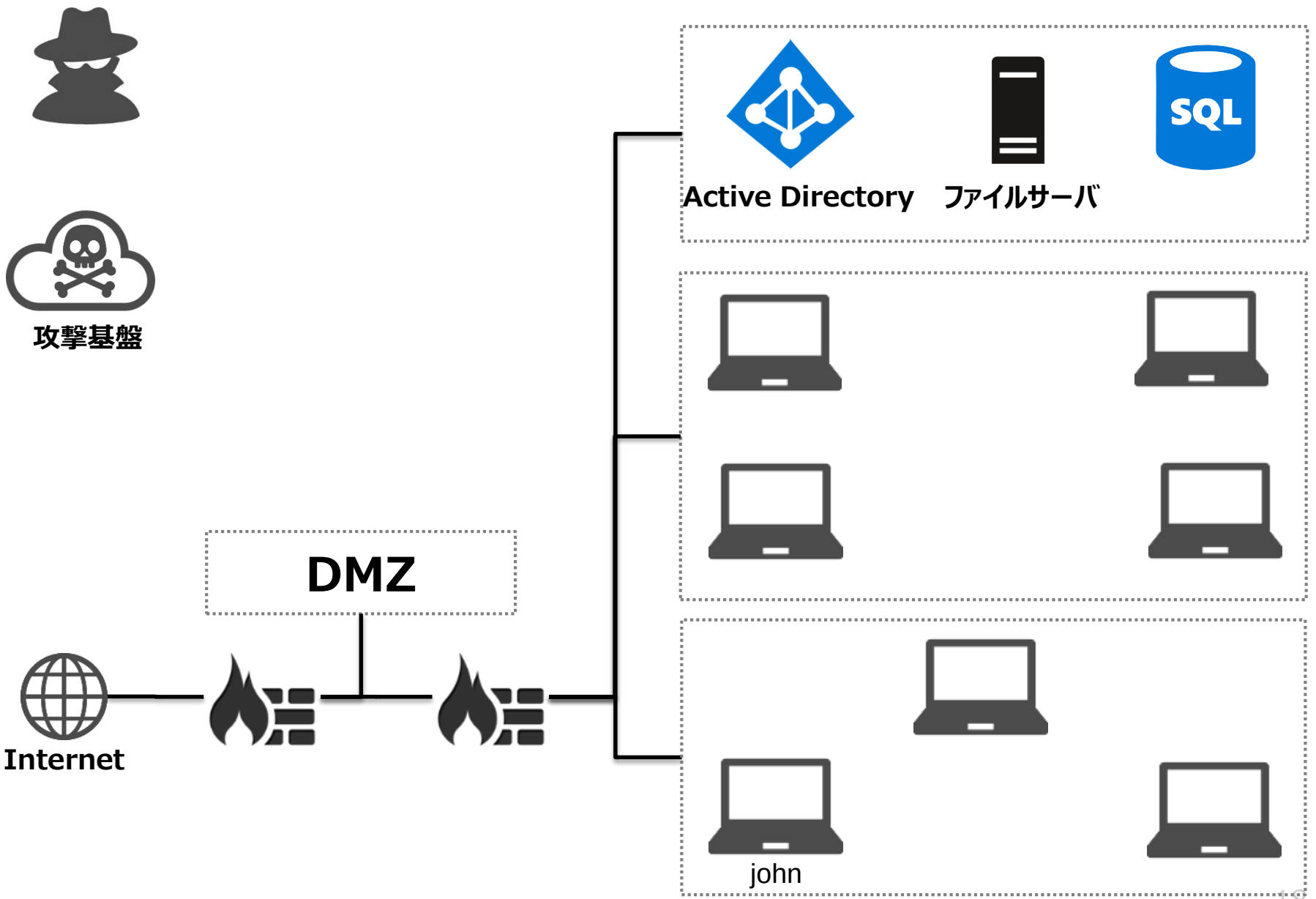
Shodan.io helps you find potential vulnerabilities	You interacted with a honey pot **SKIP NEXT TURN**	Target organization DNS server allows external zone transfers	Search engines reveal data exposure

www.sans.org/boardgame

Source : https://www.sans.org/security-resources/posters

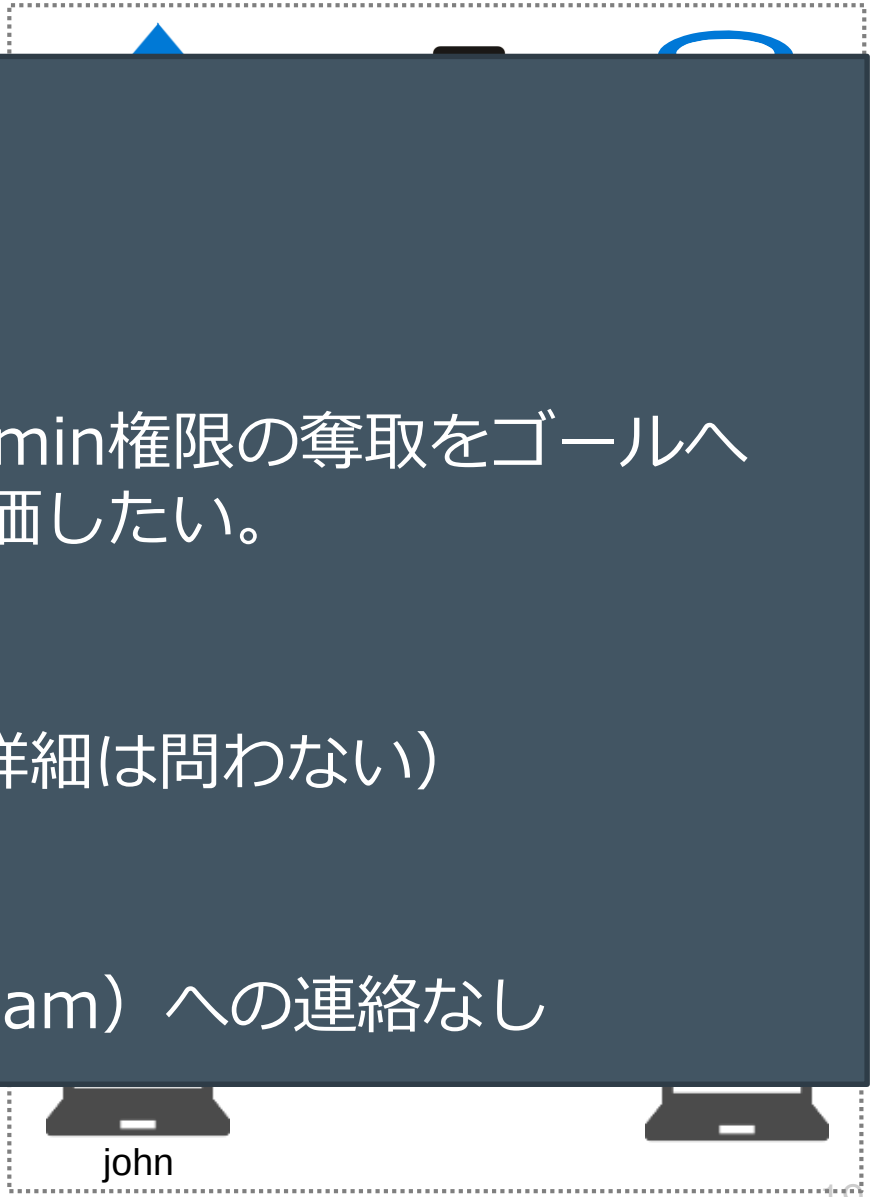
OA環境をターゲットとした標的型攻撃を想定する場合

偵察・武器化
配送
攻撃
インストール
遠隔操作
侵入拡大
目的実行



OA環境をターゲットとした標的型攻撃を想定する場合

偵察・武器化



E-Corp に対するペネトレーションテスト

1）目標

⇒ 機密情報・知的財産の奪取
⇒ 情報が散らばっているため、Domain Admin権限の奪取をゴールへ
⇒ MSSサービス（Blue Team）の実力を評価したい。

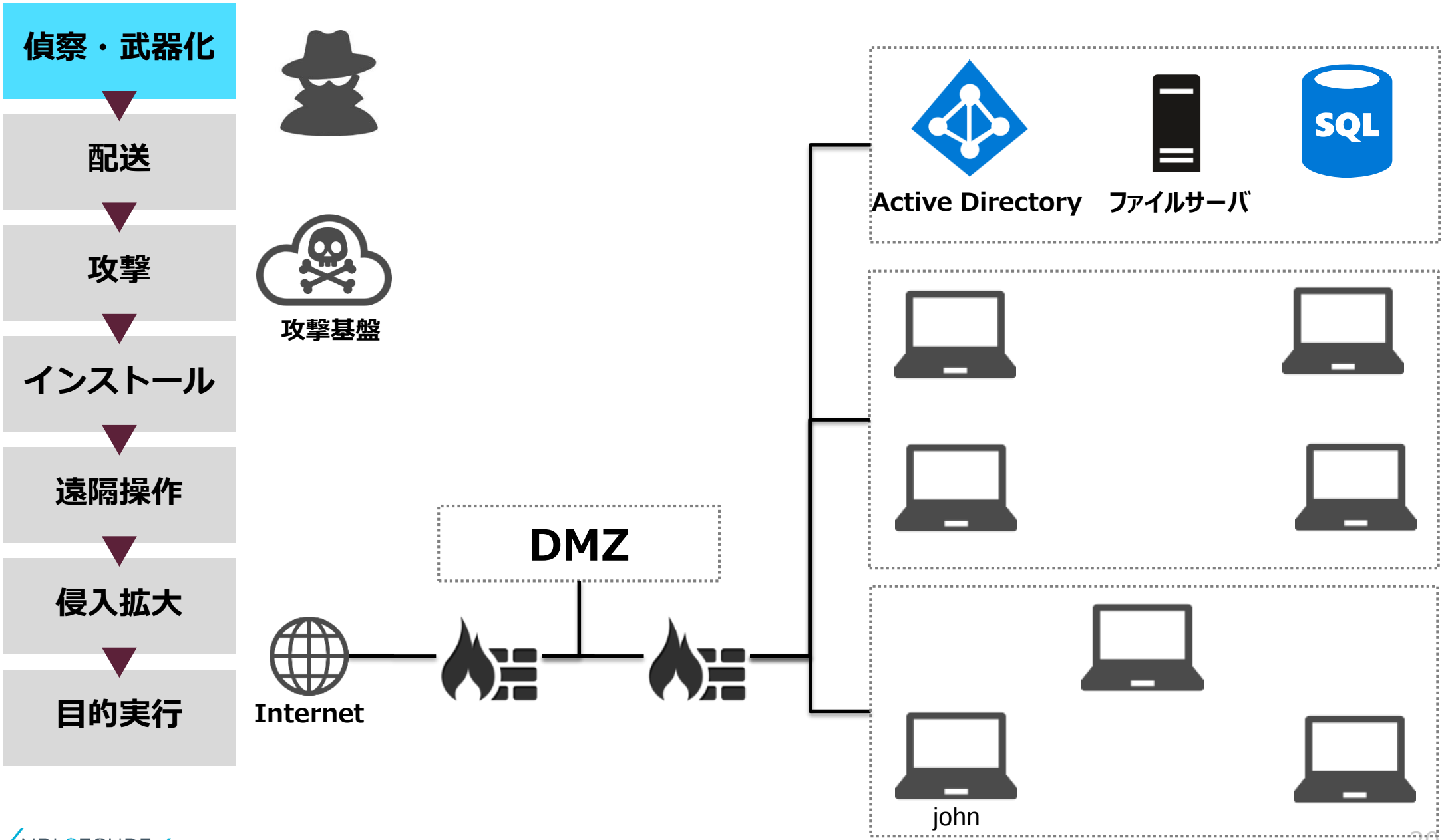
2）スコープ

⇒ 一般的な標的型攻撃を想定（攻撃手法の詳細は問わない）

3）実施条件

⇒ データ破壊の禁止、防御チーム（Blue Team）への連絡なし

OA環境をターゲットとした標的型攻撃を想定する場合



OSINT

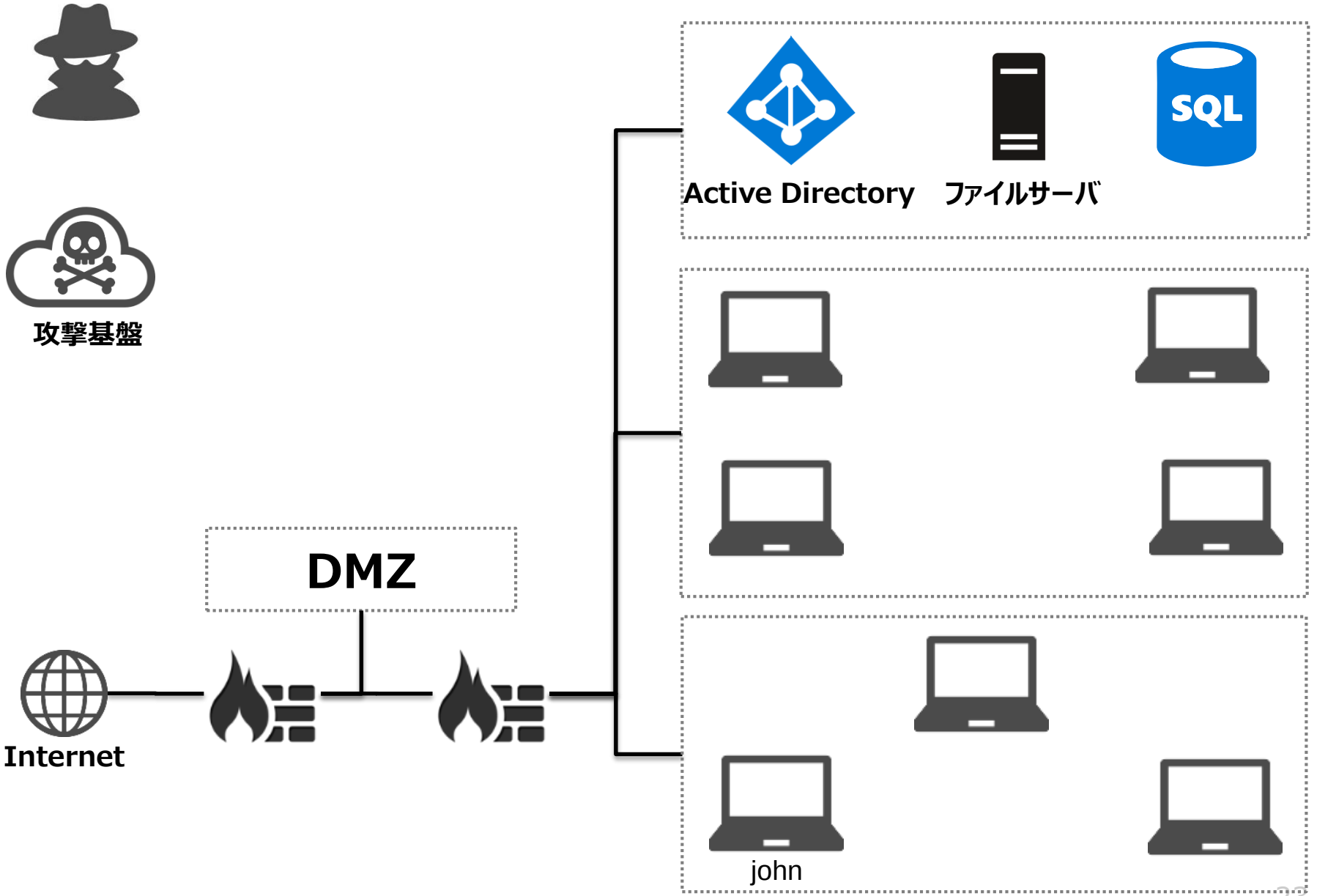
- **OSINT = Open Source INTelligence**
  - 公開情報から攻撃に必要な情報を収集し、攻撃の糸口を探すこと。
  - 最近はビッグデータ分析を利用する手法も利用されている。

  - **主な手法**
    - Host Enumeration
    - Link Analysis
    - Google Hacking
    - Metadata Extraction
    - SOCMINT = **SOC**ial **M**edia **INT**elligence
    - Banner Grabbing / Finger Printing

OSINTの具体事例については、
セミナー当日での閲覧とさせていただきました。

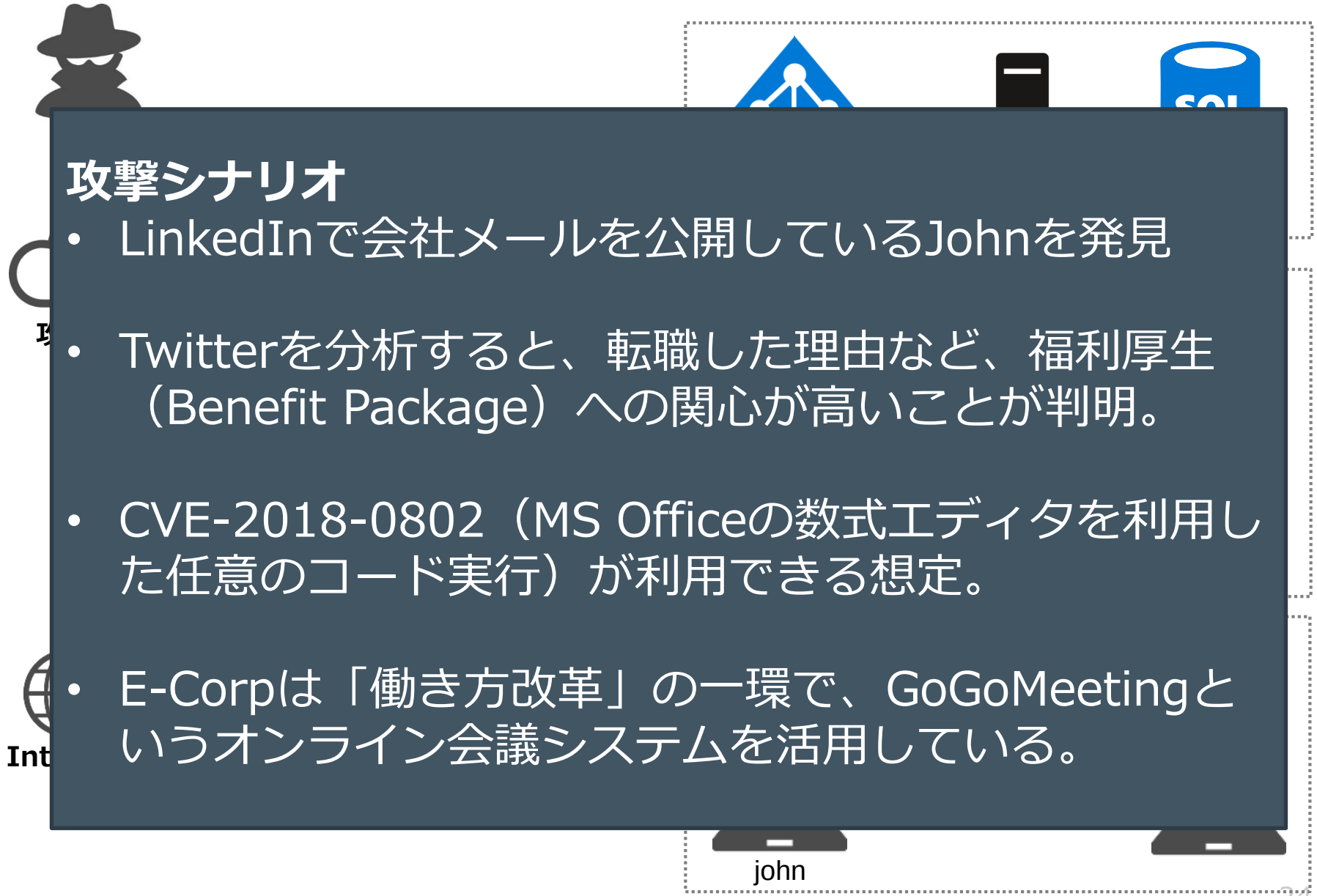
OA環境をターゲットとした標的型攻撃を想定する場合

偵察・武器化
配送
攻撃
インストール
遠隔操作
侵入拡大
目的実行



OA環境をターゲットとした標的型攻撃を想定する場合

偵察・武器化
▼
配送
▼
攻撃
▼
インストール
▼
遠隔操作
▼
侵入拡大
▼
目的実行



攻撃シナリオ

- LinkedInで会社メールを公開しているJohnを発見
- Twitterを分析すると、転職した理由など、福利厚生（Benefit Package）への関心が高いことが判明。
- CVE-2018-0802（MS Officeの数式エディタを利用した任意のコード実行）が利用できる想定。
- E-Corpは「働き方改革」の一環で、GoGoMeetingというオンライン会議システムを活用している。

Phishing Mail Sample

Fri 12/13/2018 10:05 AM

HR (HR@e-corp.com)

Employee Benefit Package Change

To :

Good Morning.

We have recently made several changes to the employee benefits package which effects individuals receiving this message. We have previously recorded a message explaining these changes which can be accessed via the meeting invite below. To access this meeting, please enter your E-Corp credentials and accepts the application prompts. Once authenticated, you will receive personalized documents detailing the specific change of your benefits package which should not be shared with anyone else.

Join Our Meeting
Meeting ID : 912-653-1534
GoGoMeeting

Sincerely
HR

Phishing Mail Sample

Fri 12/13/2018 10:05 AM

HR (HR@e-corp.com)

Employee Benefit Package Change

To :

Good Morning.

We have recently made several changes to the employee benefits package which effects individuals receiving this message. We have previously recorded a message explaining these changes which can be accessed via the meeting invite below. To access this meeting, please enter your E-Corp credentials and accepts the application prompts. Once authenticated, you will receive personalized documents detailing the specific change of your benefits package which should not be shared with anyone else.

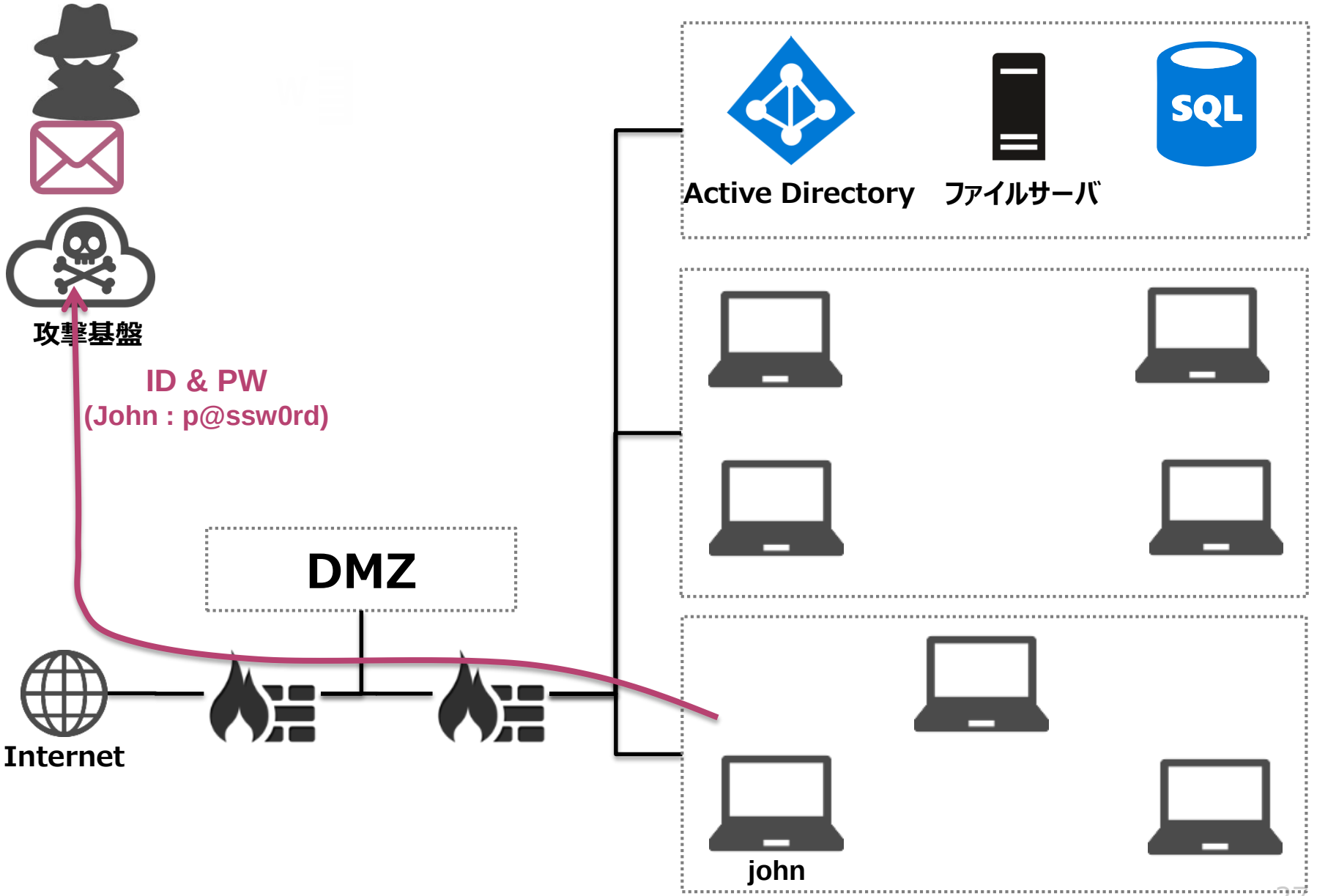
Join Our Meeting

<書いてあること>

- 福利厚生（Benefit Package）が一部変更になる。
- リンクをクリックすると、オンライン会議システム（GoGoMeeting）に繋がるため、E-Corpの認証情報でログインすること。
- ログイン後、説明用動画の閲覧と必要書類がダウンロードされる。

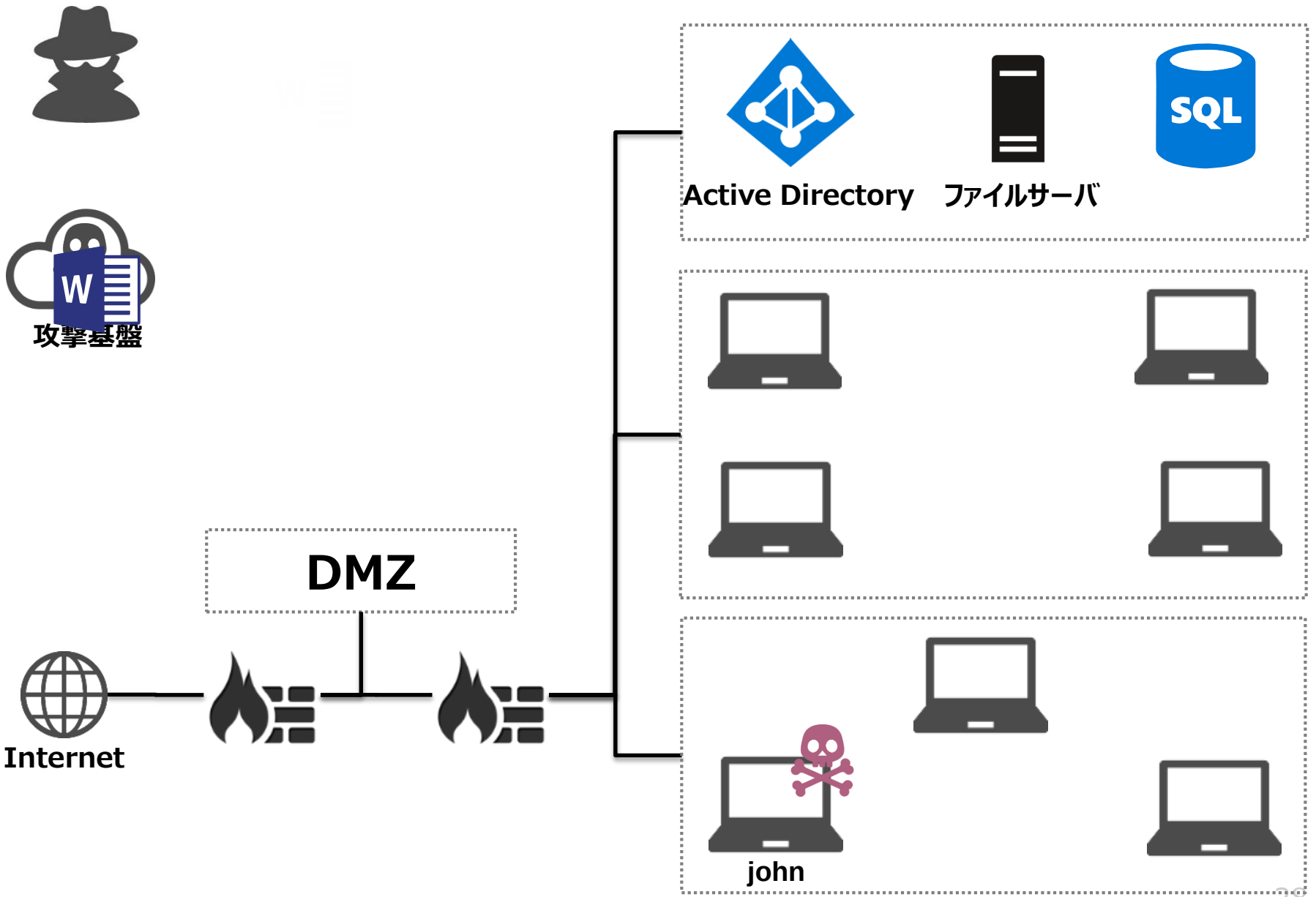
OA環境をターゲットとした標的型攻撃を想定する場合

偵察・武器化
配送
攻撃
インストール
遠隔操作
侵入拡大
目的実行



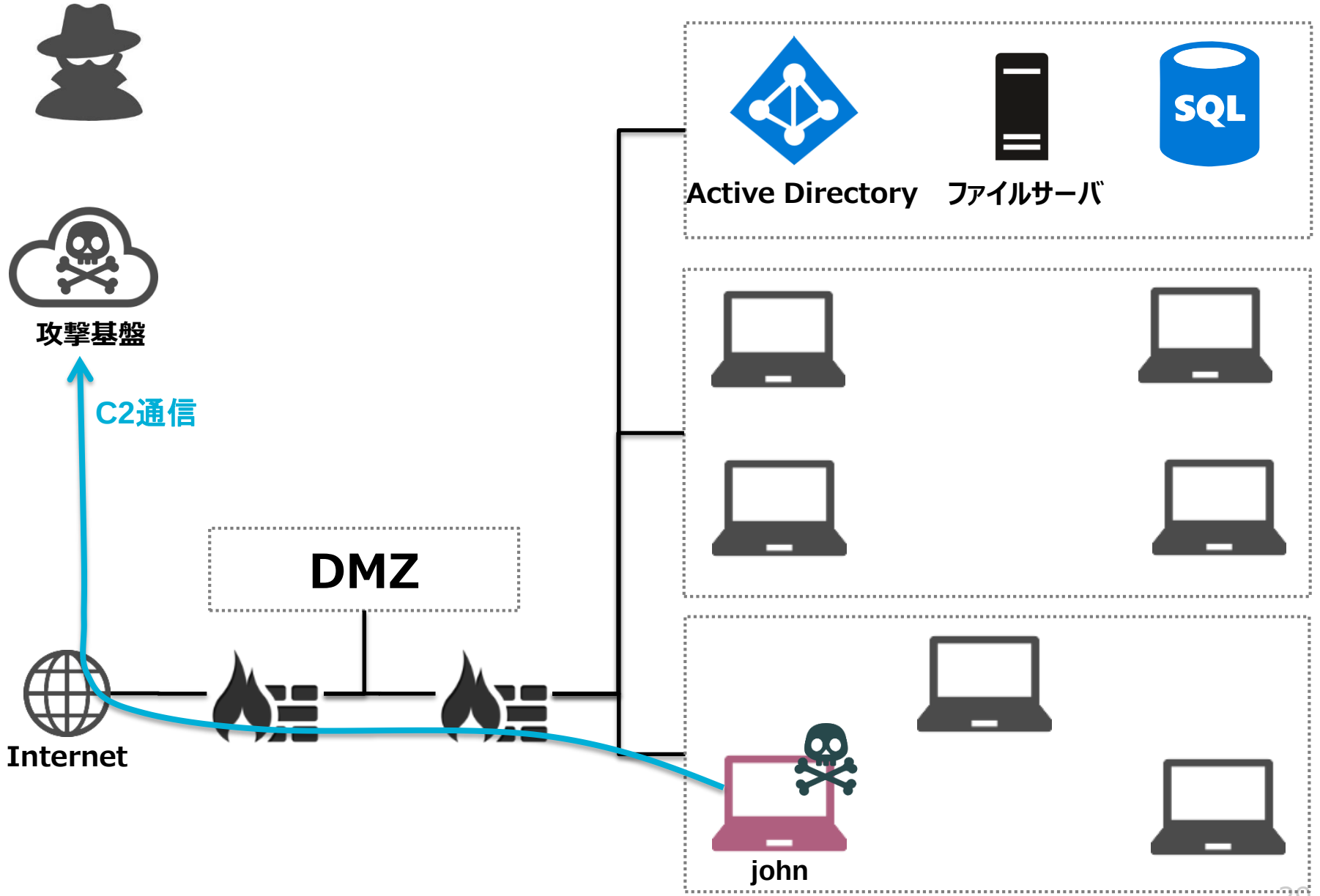
OA環境をターゲットとした標的型攻撃を想定する場合

偵察・武器化
配送
攻撃
インストール
遠隔操作
侵入拡大
目的実行



OA環境をターゲットとした標的型攻撃を想定する場合

偵察・武器化
配送
攻撃
インストール
遠隔操作
侵入拡大
目的実行

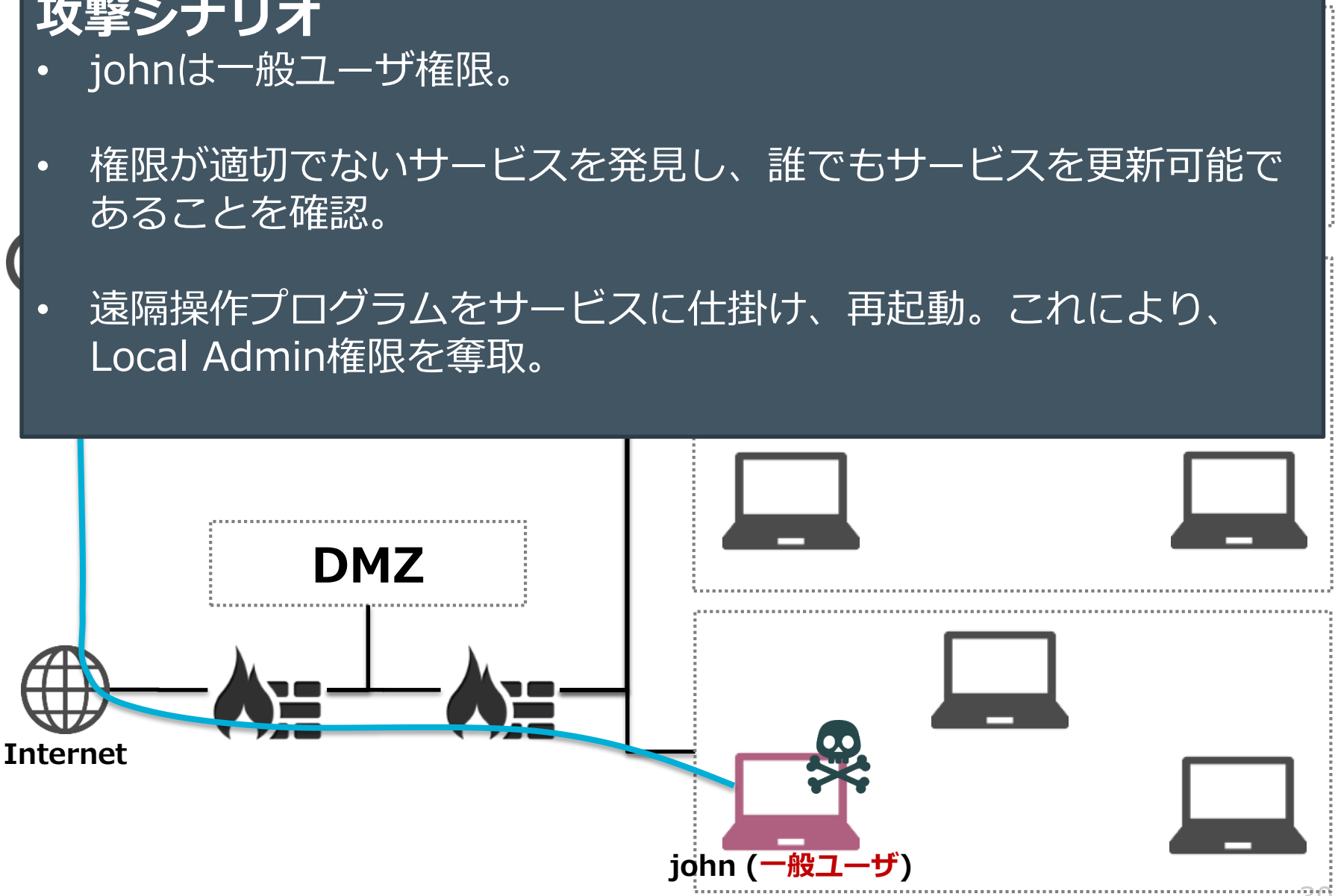


OA環境をターゲットとした標的型攻撃を想定する場合

偵察・武器化
▼
配送
▼
攻撃
▼
インストール
▼
遠隔操作
▼
侵入拡大
▼
目的実行

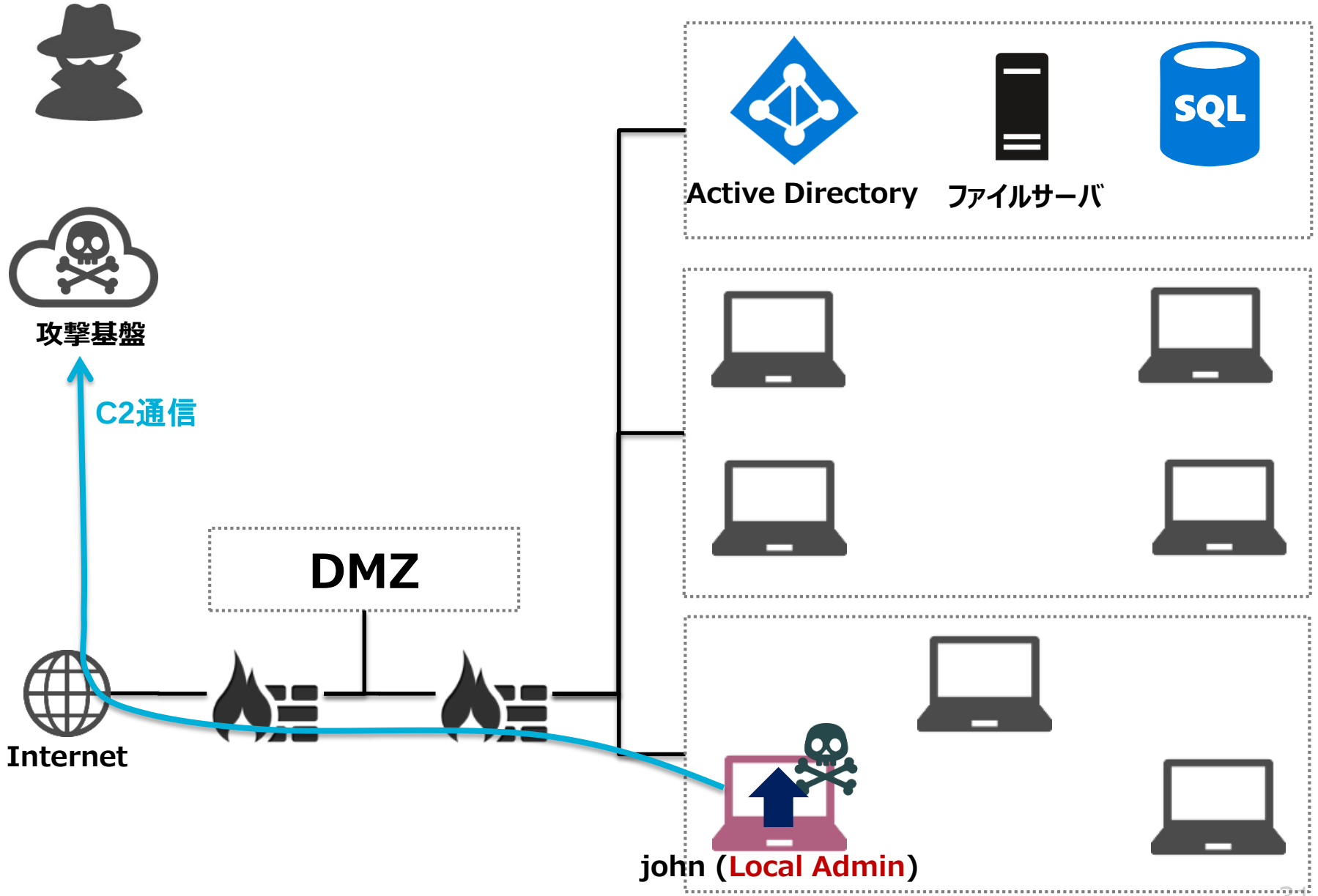
攻撃シナリオ

- johnは一般ユーザ権限。
- 権限が適切でないサービスを発見し、誰でもサービスを更新可能であることを確認。
- 遠隔操作プログラムをサービスに仕掛け、再起動。これにより、Local Admin権限を奪取。



OA環境をターゲットとした標的型攻撃を想定する場合

偵察・武器化
配送
攻撃
インストール
遠隔操作
侵入拡大
目的実行



Scenario 1

OA環境をターゲットとした標的型攻撃を想定する場合

偵察・武器化

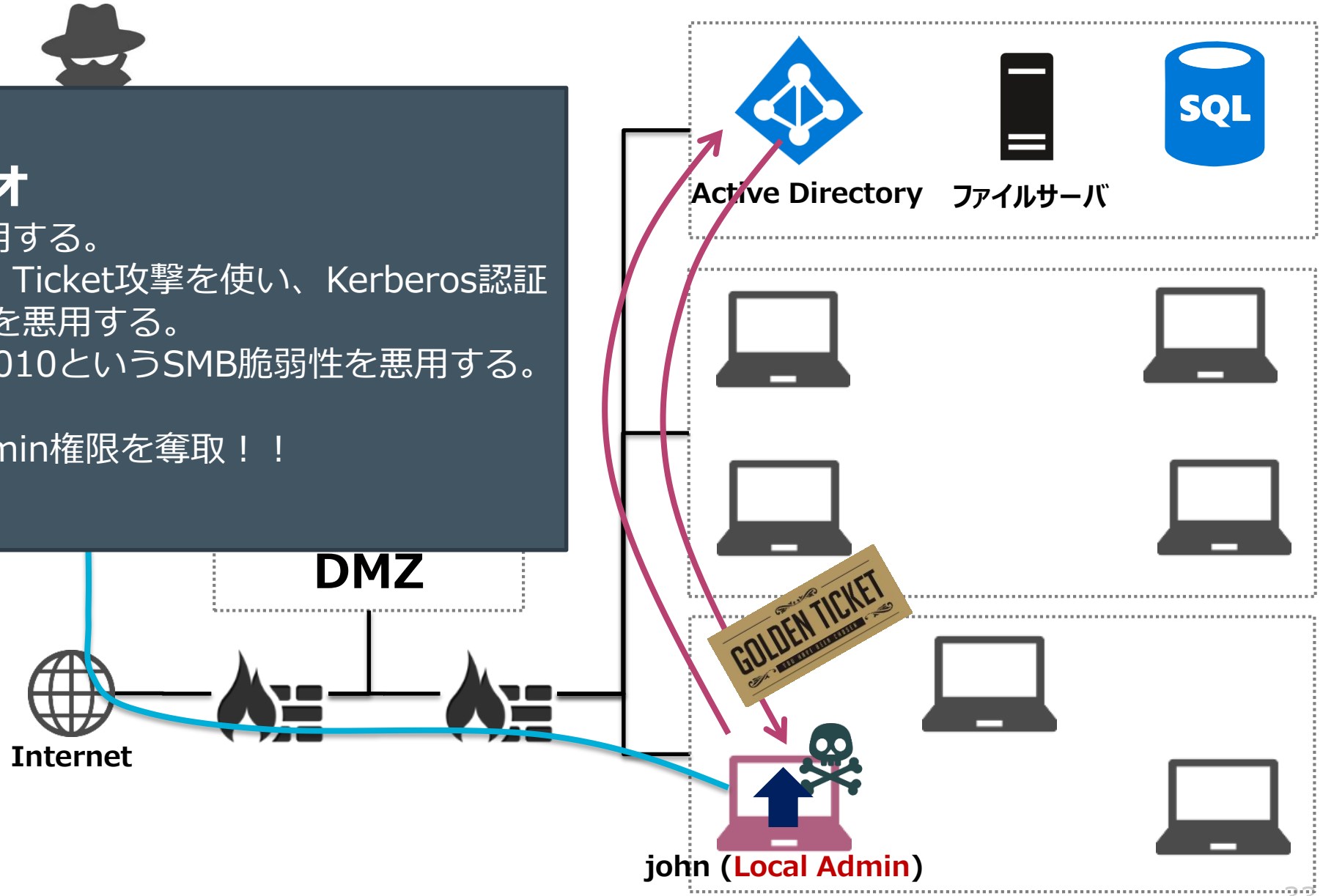
攻撃シナリオ

- 脆弱性を悪用する。
  - Golden Ticket攻撃を使い、Kerberos認証の不備を悪用する。
  - MS17-010というSMB脆弱性を悪用する。

⇒ Domain Admin権限を奪取！！

侵入拡大

目的実行



OA環境をターゲットとした標的型攻撃を想定する場合

偵察・武器化

配送

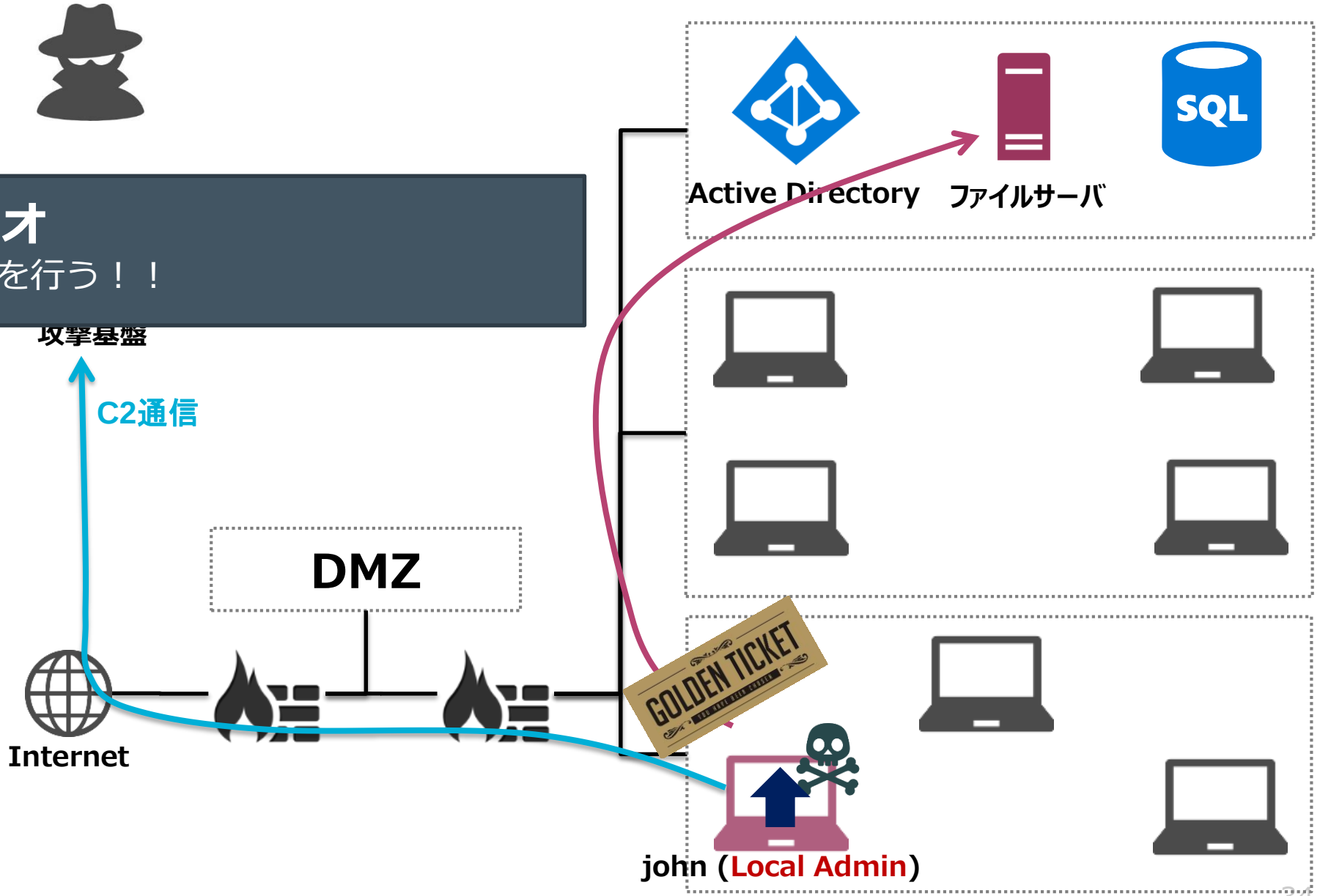
攻撃シナリオ
- 目的の実行を行う！！

インストール

遠隔操作

侵入拡大

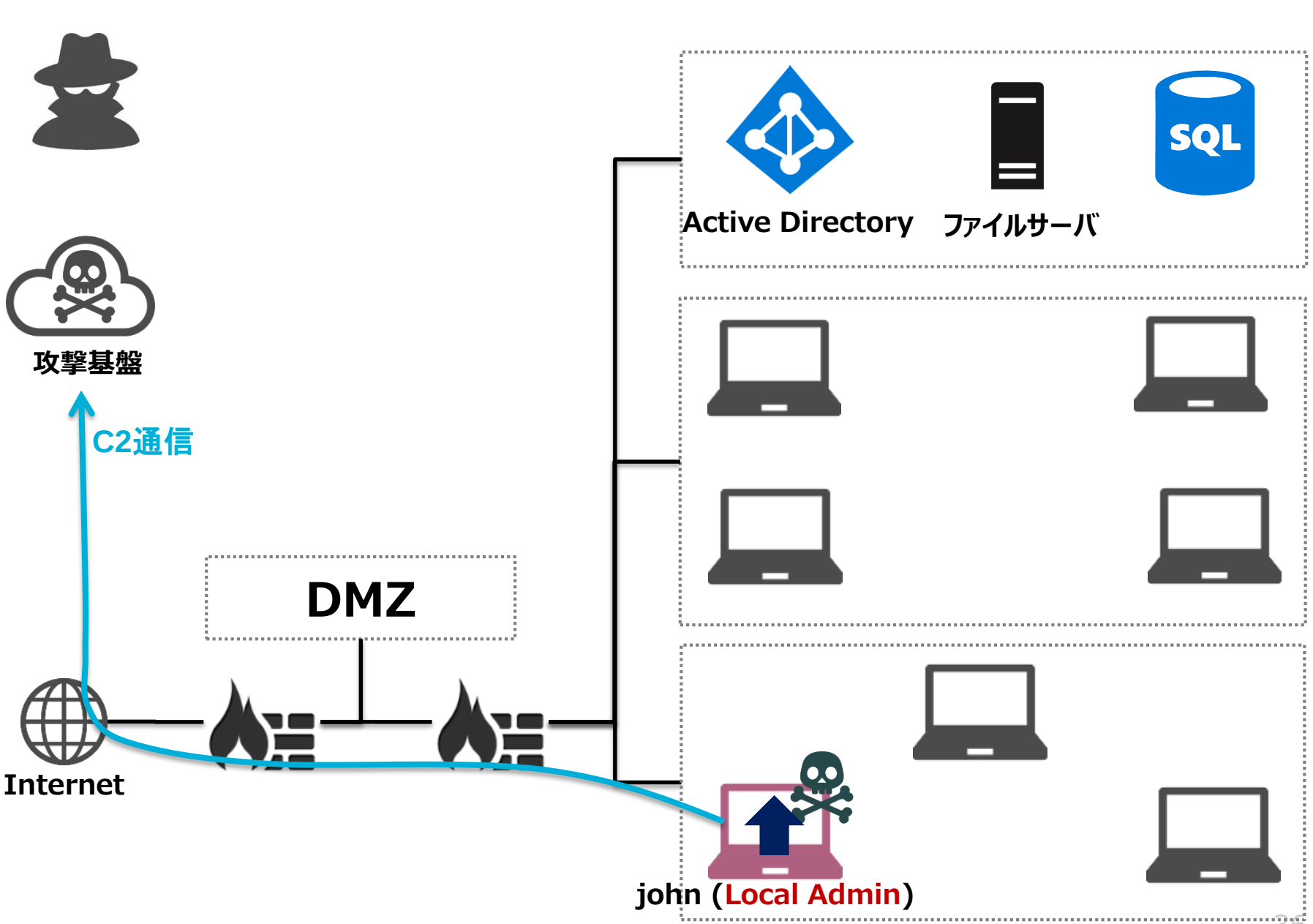
目的実行



Scenario 2

OA環境をターゲットとした標的型攻撃を想定する場合

偵察・武器化
配送
攻撃
インストール
遠隔操作
侵入拡大
目的実行



OA環境をターゲットとした標的型攻撃を想定する場合

偵察・武器化

インストール

遠隔操作

侵入拡大

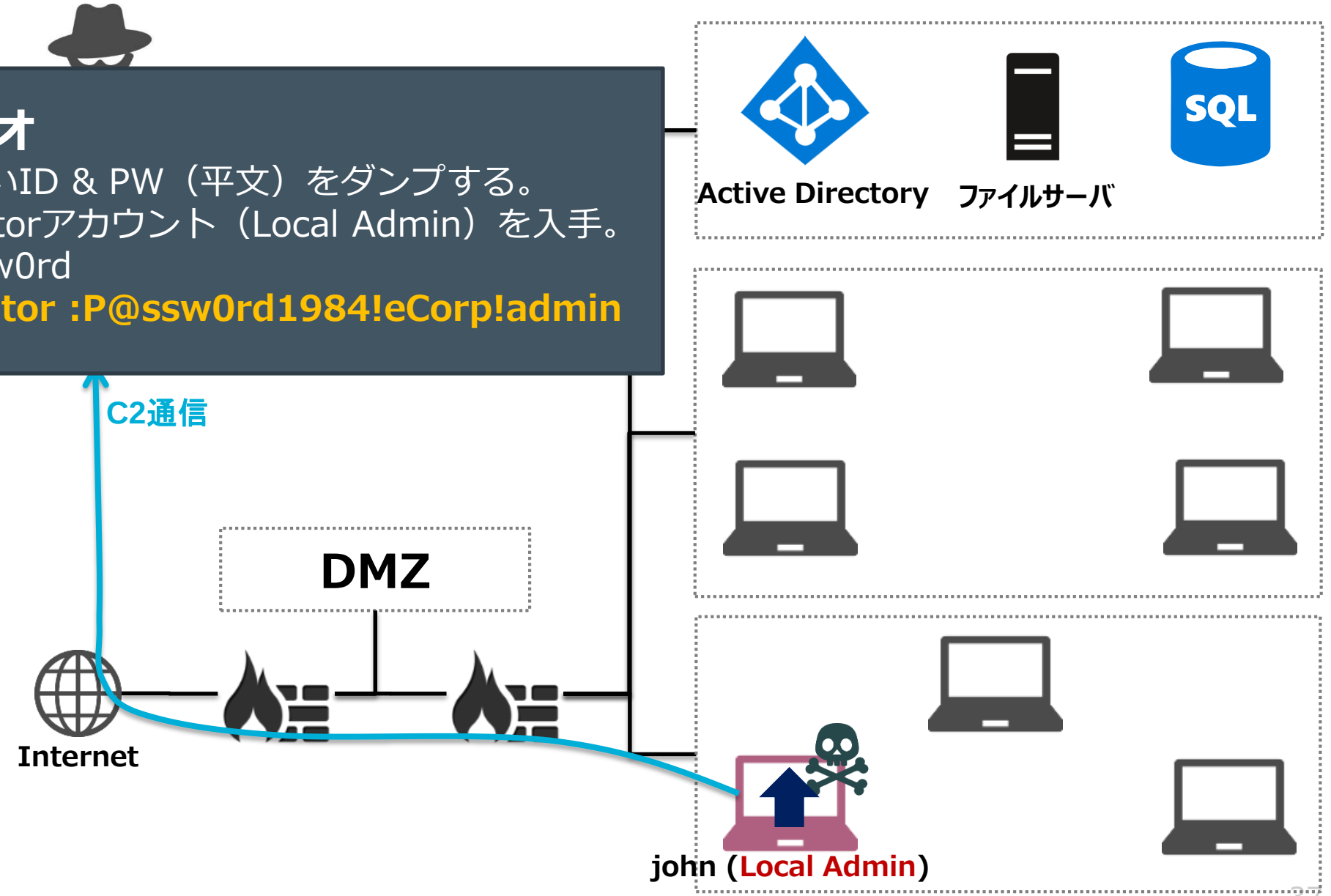
目的実行

攻撃シナリオ

- ツールを使いID & PW（平文）をダンプする。
- Administratorアカウント（Local Admin）を入手。

⇒ john:P@ssw0rd

⇒ **administrator :P@ssw0rd1984!eCorp!admin**



OA環境をターゲットとした標的型攻撃を想定する場合

攻撃シナリオ

⇒ **administrator :P@ssw0rd1984!eCorp!admin**

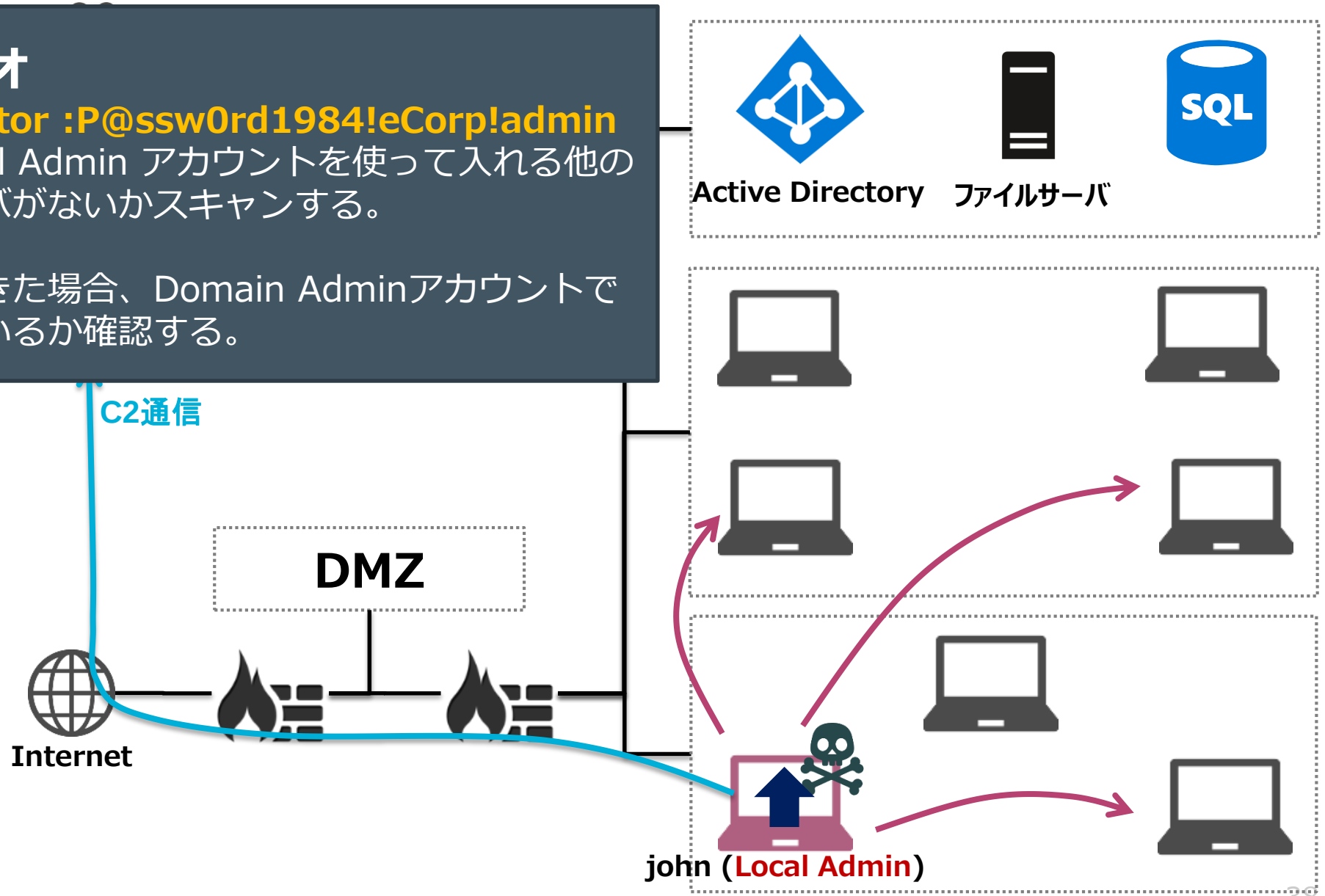
- 上記の Local Admin アカウントを使って入れる他の端末・サーバがないかスキャンする。
- ログインできた場合、Domain Adminアカウントで保存されているか確認する。

インストール

遠隔操作

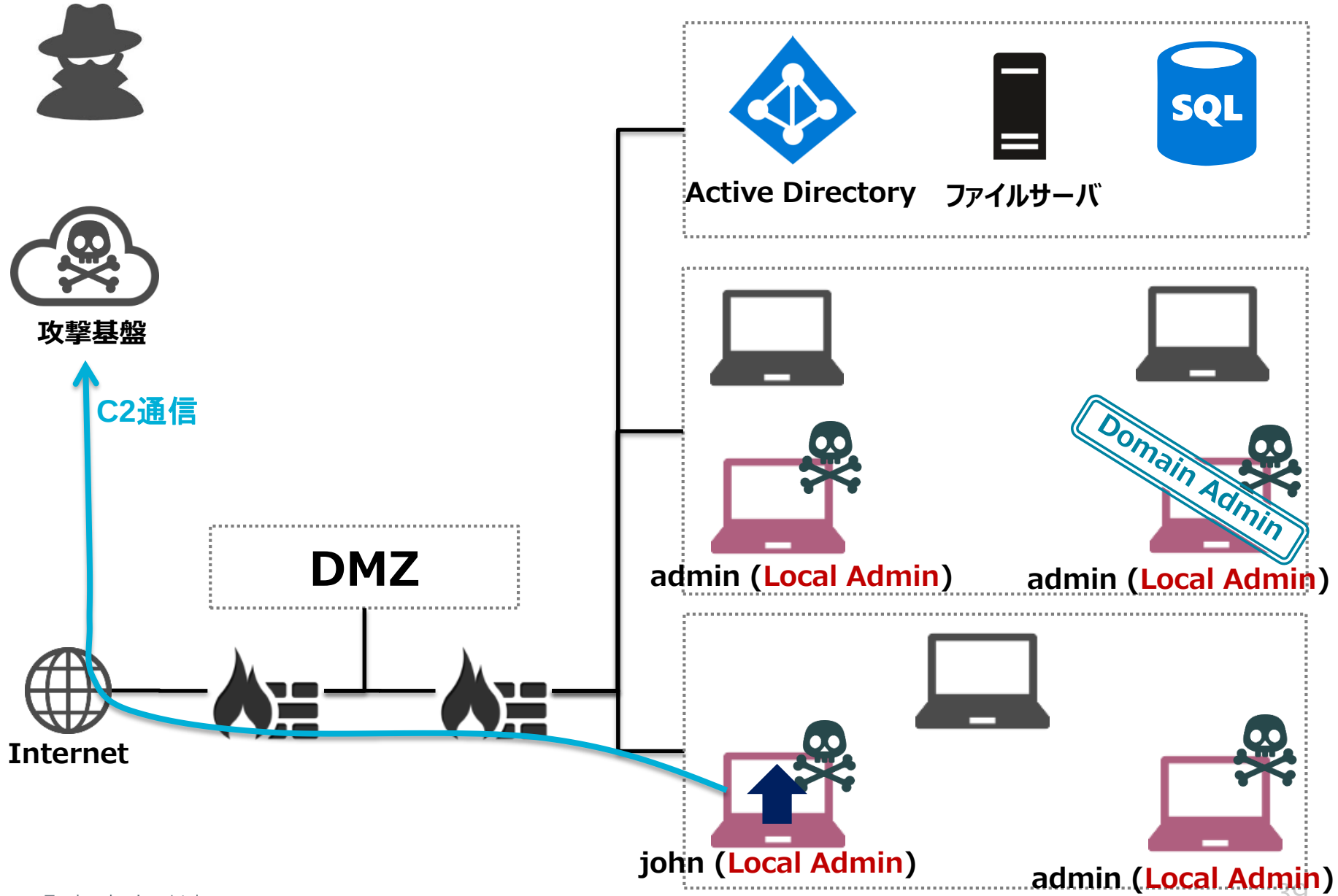
侵入拡大

目的実行



OA環境をターゲットとした標的型攻撃を想定する場合

偵察・武器化
配送
攻撃
インストール
遠隔操作
侵入拡大
目的実行



OA環境をターゲットとした標的型攻撃を想定する場合

偵察・武器化

インストール

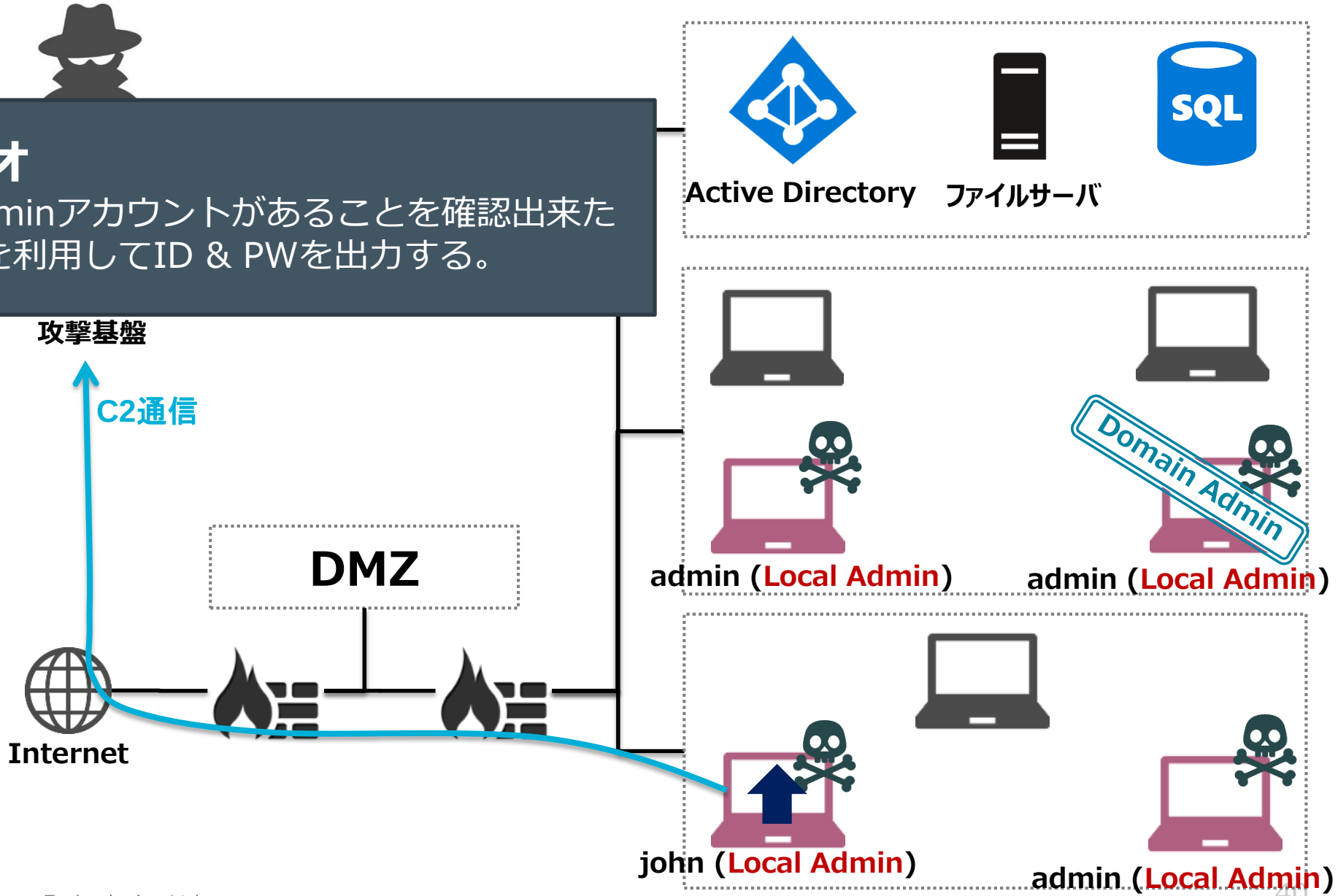
遠隔操作

侵入拡大

目的実行

攻撃シナリオ

- Domain Adminアカウントがあることを確認出来たら、ツールを利用してID & PWを出力する。



OA環境をターゲットとした標的型攻撃を想定する場合

偵察・武器化

攻撃

インストール

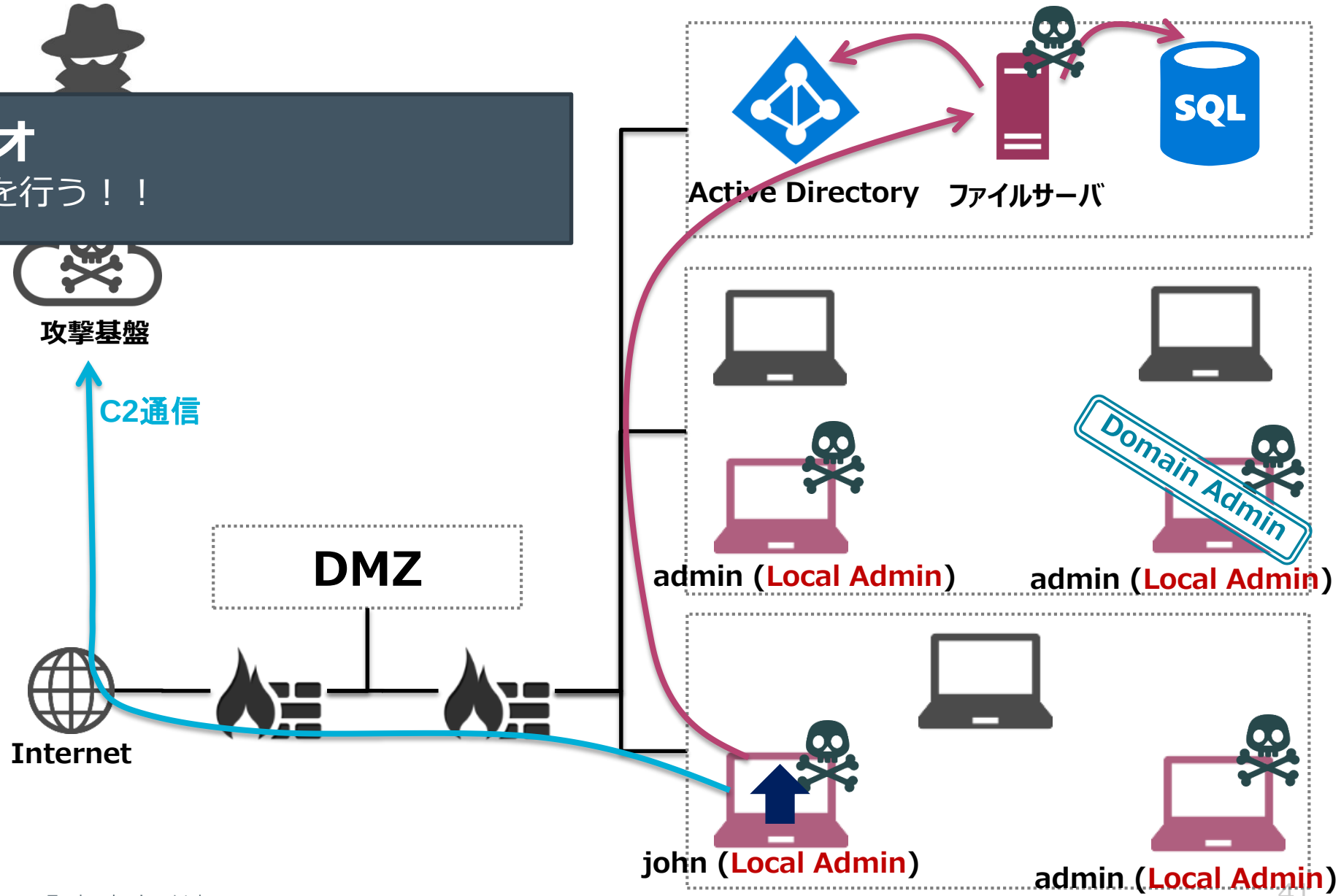
遠隔操作

侵入拡大

目的実行

攻撃シナリオ

- 目的の実行を行う！！



3. 国外の動向

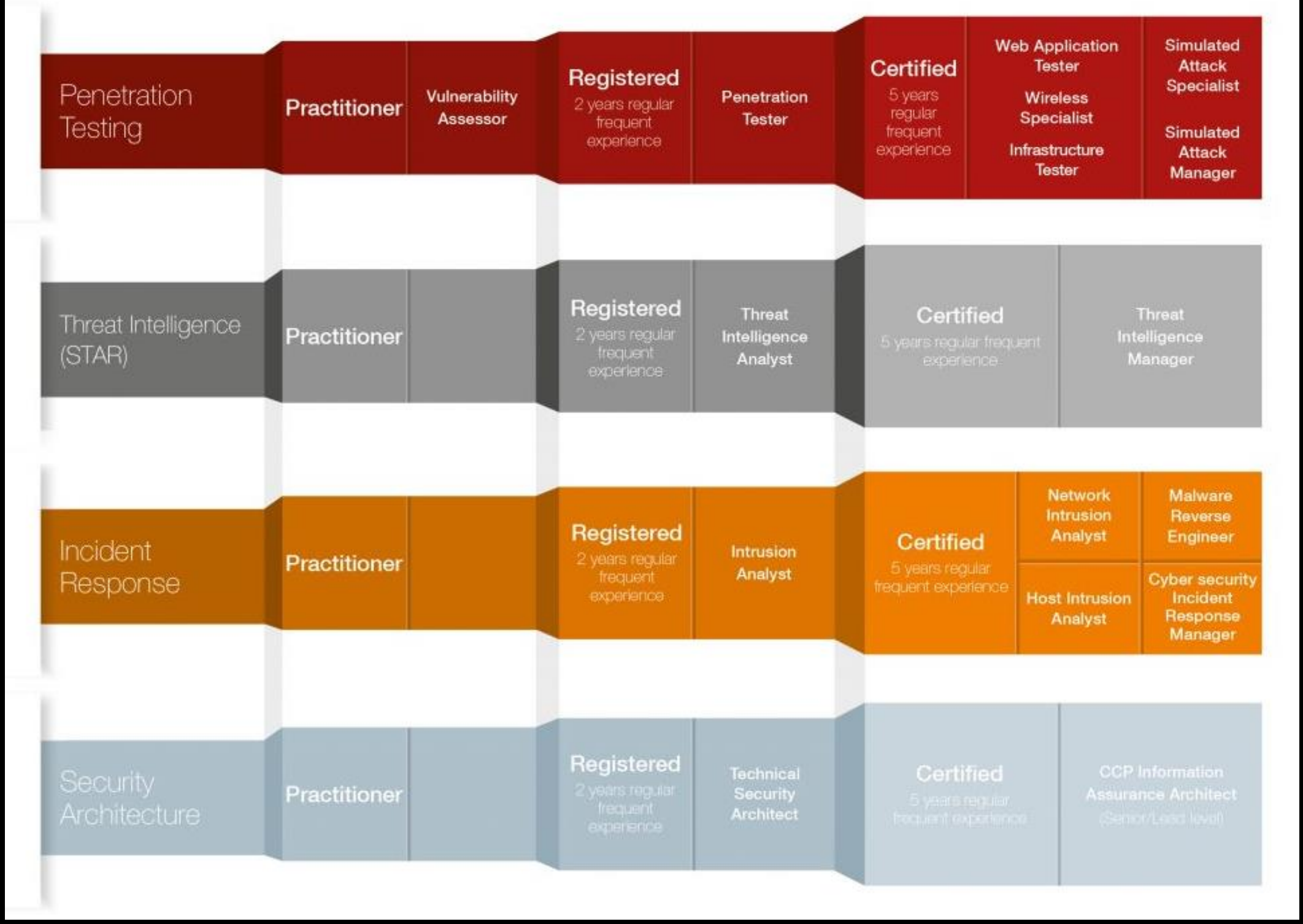
Europe

欧州の動向　～イギリスの場合～

- **CBEST**
  - イングランド銀行（Bank of England）が出したTLPT（Threat Lead Penetration Test）を実現するためのフレームワーク
  - **フレームワークのポイント**
    - Threat Intel Provider + Penetration Testerが協力し、洗練された攻撃者からの現実的な攻撃手法を模倣すること

欧州の動向　～イギリスの場合～

- **CREST : The Council of Registered Ethical Security Testers**
  - CBESTを実現するための資格団体・業界団体
  - CRESTは、４種類のドメインを定義
    - **Penetration Testing**
    - **Threat Intelligence**
    - **Incident Response**
    - **Security Architecture**



Source : https://www.crest-approved.org/professional-qualifications/crest-exams/index.html

欧州の動向　～EUの場合～

- **TIBER-EU : Threat Intelligence Based Ethical Red Teaming**
  - ECB（欧州中央銀行）が定義したフレームワーク
  - 基本的な考え方はCBESTと同じ
  - Ex）各国用にカスタマイズ可能
    - TIBER-NL

United States of America

米国の動向

特徴１：各種方面からの実施要請

→ 訴訟リスクや規制的側面から、積極的に実施する傾向がある。

規制（Regulations）：「ペネトレーションテストの実施」

- 例） NYDFS（ニューヨーク州金融サービス局）
- 例）FFIEC IT Examination Handbook
- 例）PCI-DSS（米国内の規制ではないが…）

Form 10-K/20-F（有価証券報告書）における開示要求

- 米国証券取引委員会から「CF Disclosure Guidance: Topic No. 2 Cybersecurity」（2011）が提示される。
- 「サイバーセキュリティリスクやインシデントについて明言されたものはないものの、数多くの開示要件から、上場企業に当該リスク、インシデントの開示を義務付けることができる」と有価証券報告書における実質的な開示要求あり。

米国の動向

特徴１：各種方面からの実施要請

→ 訴訟リスクや規制的側面から、積極的に実施する傾向がある。

情報漏洩時の訴訟制度：Class Action

- 被害者の一部が、（同じ法的利害関係を持つ）の被害者全体（=クラス）に代わって、同意なく訴訟できる制度
- 裁判所は、訴訟前に「クラス」の認定を行う。（連邦地方裁判所規則 23 条）
- 裁判所の決定は、認定されたクラス全体に適用される。

米国の動向

特徴１：各種方面からの実施要請

→ 訴訟リスクや規制的側面から、積極的に実施する傾向がある。

- **情報漏洩時の訴訟制度：Class Action**
- **ターゲット社（2013年・4000万件のカード情報＋7000万件の個人情報漏洩）**
  - 対策費用累計：292 Million USD（＝２９２億円）
  - 100件以上の訴訟 → 多すぎるので、利害関係者ごとにまとめられる
  - 訴訟の原告は、顧客だけでない。支払いは153M USD程度。

	顧客	支払額	支払日
1	顧客	10.0 Million USD	2015.03
2	MasterCard	19.0 Million USD	2015.04
3	Visa	67.0 Million USD	2015.08
4	銀行・クレジットユニオン	39.4 Million USD	2015.12
5	47州政府	18.5 Million USD	2017.04
	合計	153.9 Million USD	

Source : https://corporate.target.com/annual-reports/2016
Source : https://www.thesslstore.com/blog/2013-target-data-breach-settled/

ペネトレーションテストが法的な争点に関連する事例については
セミナー当日での閲覧とさせていただきました。

米国の動向

特徴２：ペネトレーションテスターの品質確保

- Offensive Security社 **OSCP** という資格が着目されている
  - OSCP：Offensive Security Certified Professional

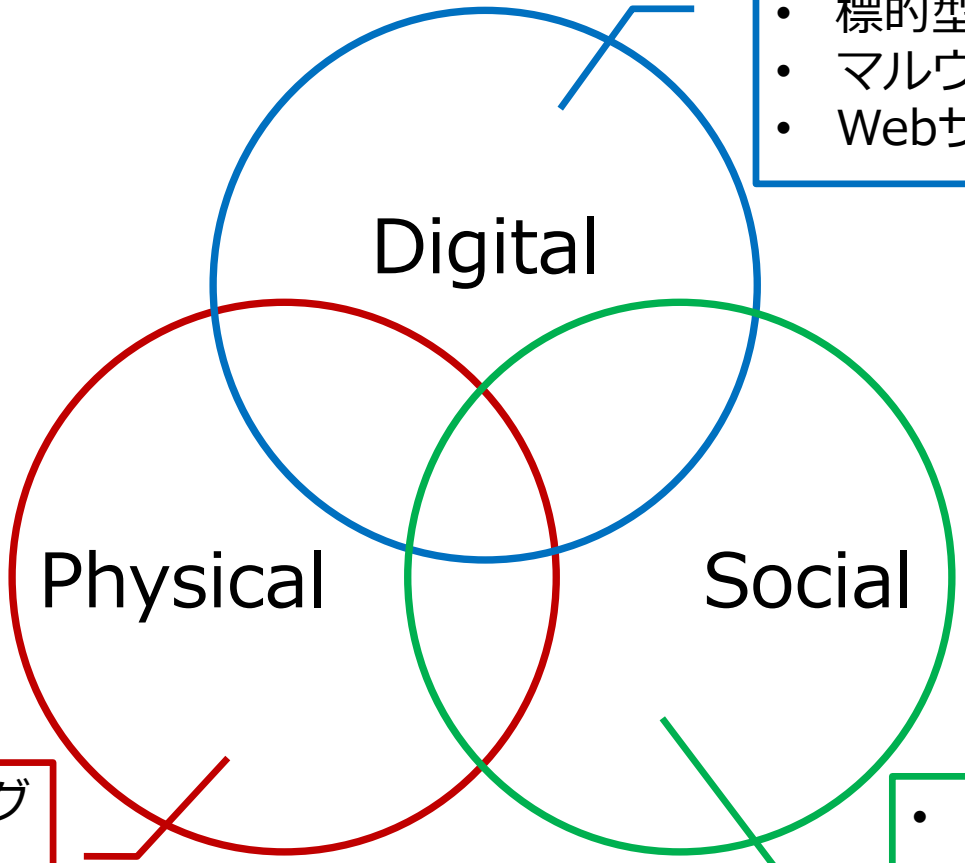
→ 24時間の実践的試験（Lab環境にハッキングを実際に実施）

→ 試験後、24時間以内に英語レポートを書き上げて提出する

米国の動向

特徴３：実際に診断する範囲が広い（＝Red Team Operation）

企業を攻撃するリスクは、サイバーだけではないとして捉えている



- 標的型攻撃
- マルウェア・ランサムウェア
- Webサイトからの情報窃取

- IDカード・クローニング
- ピッキング
- エレベータハッキング

- フィッシング詐欺
- BEC
- なりすましによる物理侵入

当日、Physical Penetration Test / Social Penetration Testのご説明をしましたが、
お見せしたコンテンツはセミナー当日での閲覧とさせていただきました。

4. まとめ


ハードルが高い？
（特に海外レベルだと…）


結局どこまでやればよいか？

- 外部からの脅威を想定
- フェーズ分割して行う

OA環境をターゲットとした標的型攻撃を想定する場合

偵察・武器化
配送
攻撃
インストール
遠隔操作
侵入拡大
目的実行

メール訓練

侵入を前提とした
内部ペネトレーションテスト

Active Directory

ファイルサーバ

john

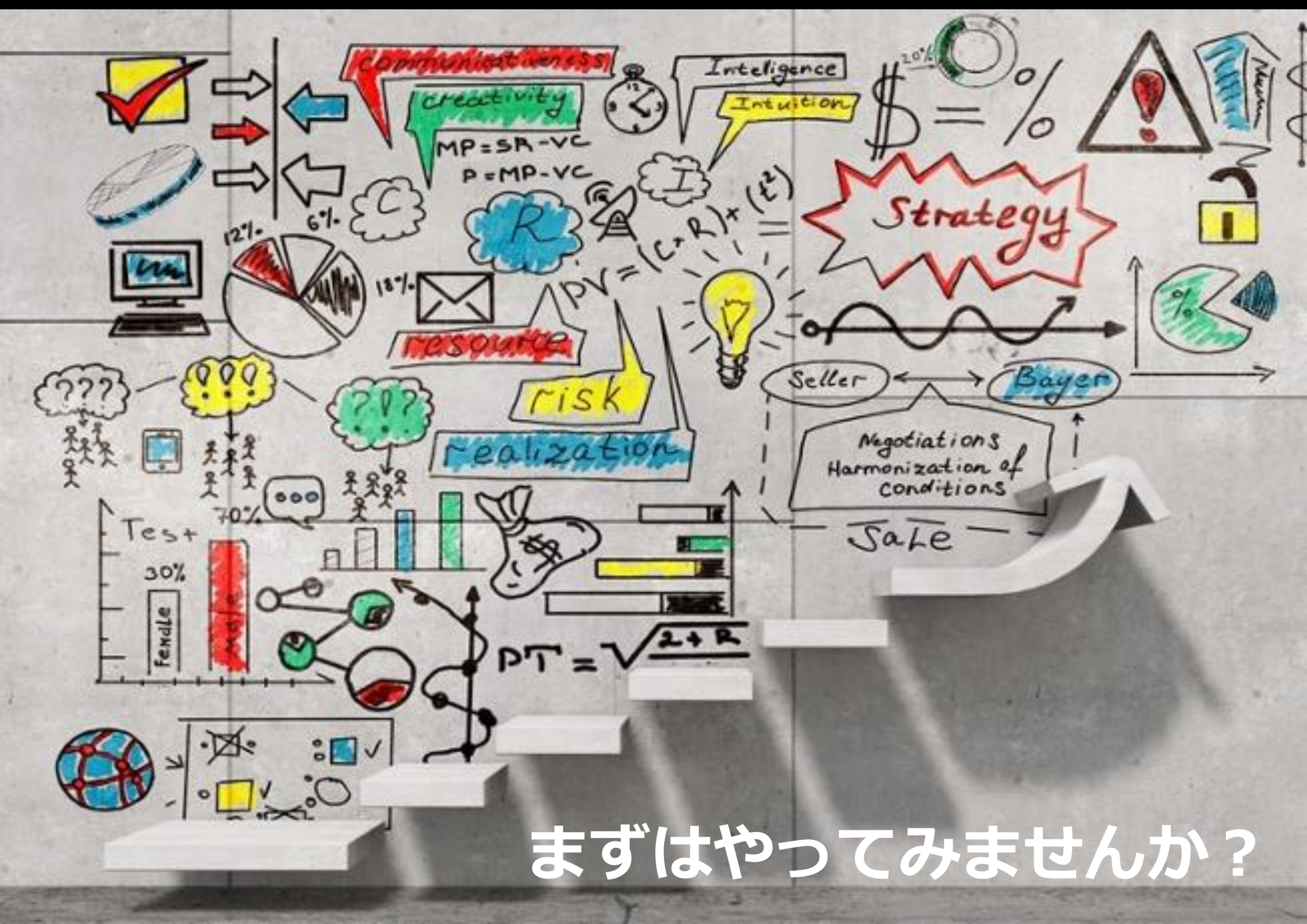
まとめ

ペネトレーションテスト

- **実際の攻撃テクニックで、事前に設定した目標を達成可能か検証し、組織のセキュリティレベルをチェックすること！！**
- 脆弱性診断との性質の違い

トレンド

- 日本：金融庁の指針、TLPT（Threat Lead Penetration Test）
- 欧米：
  - CBEST・CREST・TIBERなどのTLPTと同様の概念が登場している。
  - 資格を使った品質維持
  - Red Team Operationと呼ばれ、サイバー領域以外（Physical・Social）も含めた総合的なリスク分析が行われている。



まずはやってみませんか？

自分達が守るべきもの、自分たちのセキュリティの
健康状態がわかる良いきっかけになります！

ご清聴、ありがとうございました。

NRI SECURE

NRI SecureTechnologies, Ltd.

www.nri-secure.co.jp