



Business content

Training Business

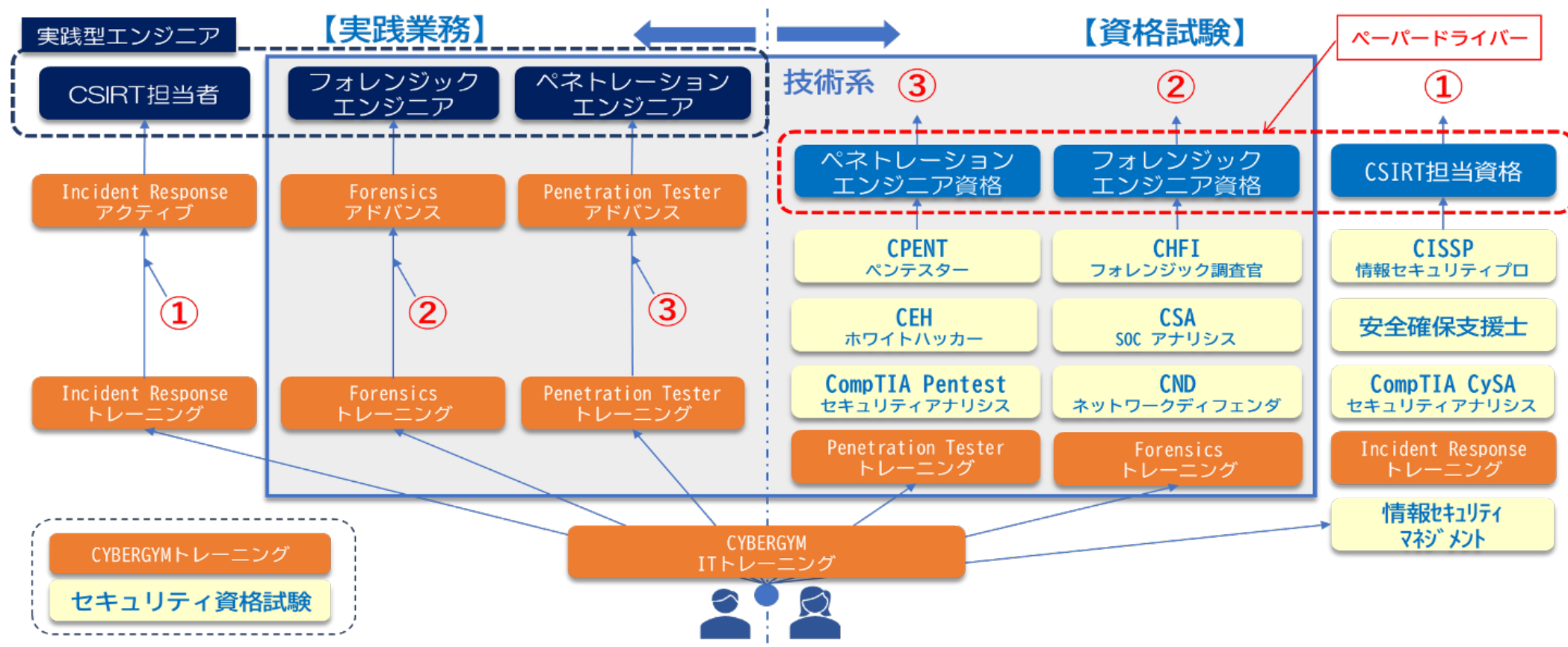
トレーニング事業

サイバーセキュリティ トレーニング ————— P1

DX トレーニング ————— P5



セキュリティ人材は資格取得によってスキルを確保する傾向があるが、
実践で使えるスキルを取得するためには、実践型のトレーニングが必須。
企業や官公庁関係のセキュリティエンジニアの受講者が増加中。



MITRE ATT&CK フレームワークにある、
ハッカーの攻撃を実際に受け、
防御や対策の戦術・テクニックを実体験できる
“日本唯一”のトレーニング。



MITRE | ATT&CK

ATT&CKcon 6.0 is coming October 14-15 in McLean, VA and live online. To potentially join us on stage, submit to our CFP by July 9th.

ATT&CK®

Get Started Take a Tour
Contribute Blog
FAQ Random Page

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world – by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK Matrix for Enterprise

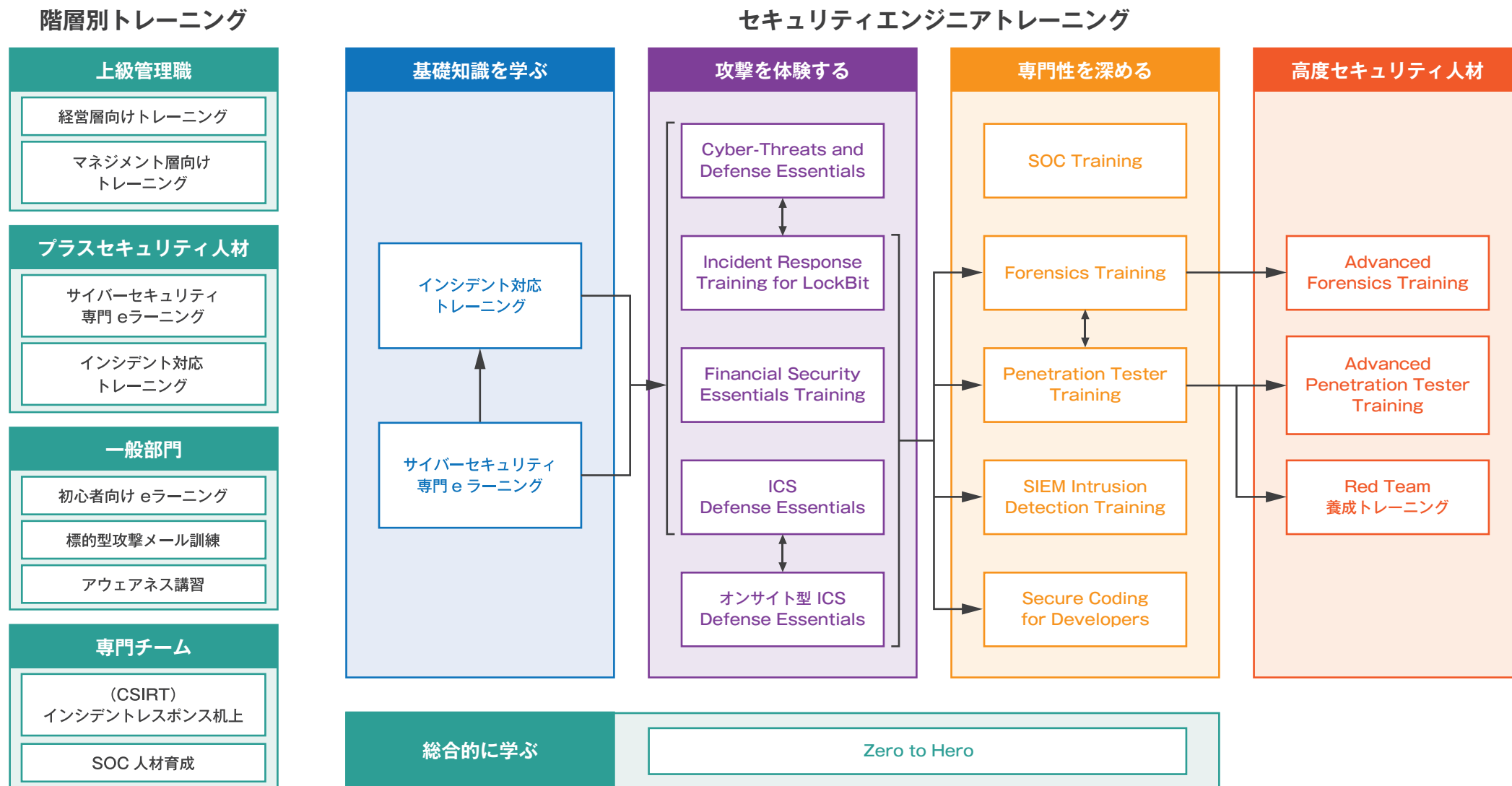
layout: slide show sub-techniques hide sub-techniques

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 14 techniques	Execution 16 techniques	Persistence 14 techniques	Privilege Escalation 14 techniques	Defense Evasion 41 techniques	Credential Access 17 techniques	Discovery 33 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques
Active Scanning (1)	Acquire Access (1)	Content Injection (1)	Cloud Administration Command (1)	Account Manipulation (1)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Adversary-in-the-Middle (1)	Application Window Discovery (1)	Application Layer Protocol (1)	Adversary-in-the-Middle (1)	Application Layer Protocol (1)	Automated Exfiltration (1)	Account Access Removal (1)
Gather Victim Host Information (1)	Acquire Infrastructure (1)	Drive-by Compromise (1)	Command and Scripting Interface (1)	BITS Jobs (1)	Access Token Manipulation (1)	Access Token Manipulation (1)	Brute Force (1)	Browser Information Discovery (1)	Archive Collected Data (1)	Archive Collected Data (1)	Archive Collected Data (1)	Data Transfer Size Limits (1)	Data Destruction (1)
Gather Victim Identity Information (1)	Compromise Accounts (1)	Exploit Public-Facing Application (1)	Container Administration Command (1)	Boot or Logon Autostart Execution (1)	Account Manipulation (1)	Build Image or Host (1)	Credentials from Password Stores (1)	Cloud Infrastructure Discovery (1)	Automated Spearphishing (1)	Automated Spearphishing (1)	Automated Spearphishing (1)	Data Encrypted for Impact (1)	Data Manipulation (1)
Gather Victim Network Information (1)	Compromise Infrastructure (1)	External Remote Services (1)	Container Deployment Command (1)	Boot or Logon Initialization Script (1)	Boot or Logon Autostart Execution (1)	Debugger Evasion (1)	Exploitation for Credential Access (1)	Cloud Service Dashboard (1)	Remote Service Session Hijacking (1)	Remote Service Session Hijacking (1)	Remote Service Session Hijacking (1)	Exfiltration Over Alternative Protocol (1)	Data Manipulation (1)
Gather Victim Org Information (1)	Develop Capabilities (1)	Hardware Additions (1)	EDK Administration Command (1)	Cloud Application Integration (1)	Boot or Logon Initialization Script (1)	Deobfuscate/Decode Files or Information (1)	Forced Authentication (1)	Cloud Service Discovery (1)	Browser Session Hijacking (1)	Browser Session Hijacking (1)	Browser Session Hijacking (1)	Exfiltration Over C2 Channel (1)	Data Manipulation (1)
Phishing for Information (1)	Establish Accounts (1)	Pushing (1)	Registration for Client Execution (1)	Compromise Host Software Binary (1)	Boot or Logon Initialization Script (1)	Deploy Container (1)	Input Manipulation (1)	Cloud Storage Object Discovery (1)	Clipboard Data (1)	Clipboard Data (1)	Clipboard Data (1)	Exfiltration Over Other Network Medium (1)	Data Manipulation (1)
Search Closed Sources (1)	System Capabilities (1)	Stage Capabilities (1)	Registration for Client Execution (1)	Create or Modify System Process (1)	Create or Modify System Process (1)	Domain or Tenant Policy Modification (1)	Input Manipulation (1)	Cloud Storage Object Discovery (1)	Clipboard Data (1)	Clipboard Data (1)	Clipboard Data (1)	Exfiltration Over Other Network Medium (1)	Data Manipulation (1)
Search Open Technical (1)	Supply Chain Compromise (1)	Supply Chain Compromise (1)	Input Injection (1)	Create or Modify System Process (1)	Create or Modify System Process (1)	Domain or Tenant Policy Modification (1)	Input Manipulation (1)	Cloud Storage Object Discovery (1)	Clipboard Data (1)	Clipboard Data (1)	Clipboard Data (1)	Exfiltration Over Other Network Medium (1)	Data Manipulation (1)
Search Open Websites/Domain (1)	Traffic Relationship (1)	Traffic Relationship (1)	Input Injection (1)	Create or Modify System Process (1)	Create or Modify System Process (1)	Domain or Tenant Policy Modification (1)	Input Manipulation (1)	Cloud Storage Object Discovery (1)	Clipboard Data (1)	Clipboard Data (1)	Clipboard Data (1)	Exfiltration Over Other Network Medium (1)	Data Manipulation (1)
Search Victim-Owned Websites (1)	Valid Accounts (1)	Valid Accounts (1)	Input Injection (1)	Create or Modify System Process (1)	Create or Modify System Process (1)	Domain or Tenant Policy Modification (1)	Input Manipulation (1)	Cloud Storage Object Discovery (1)	Clipboard Data (1)	Clipboard Data (1)	Clipboard Data (1)	Exfiltration Over Other Network Medium (1)	Data Manipulation (1)

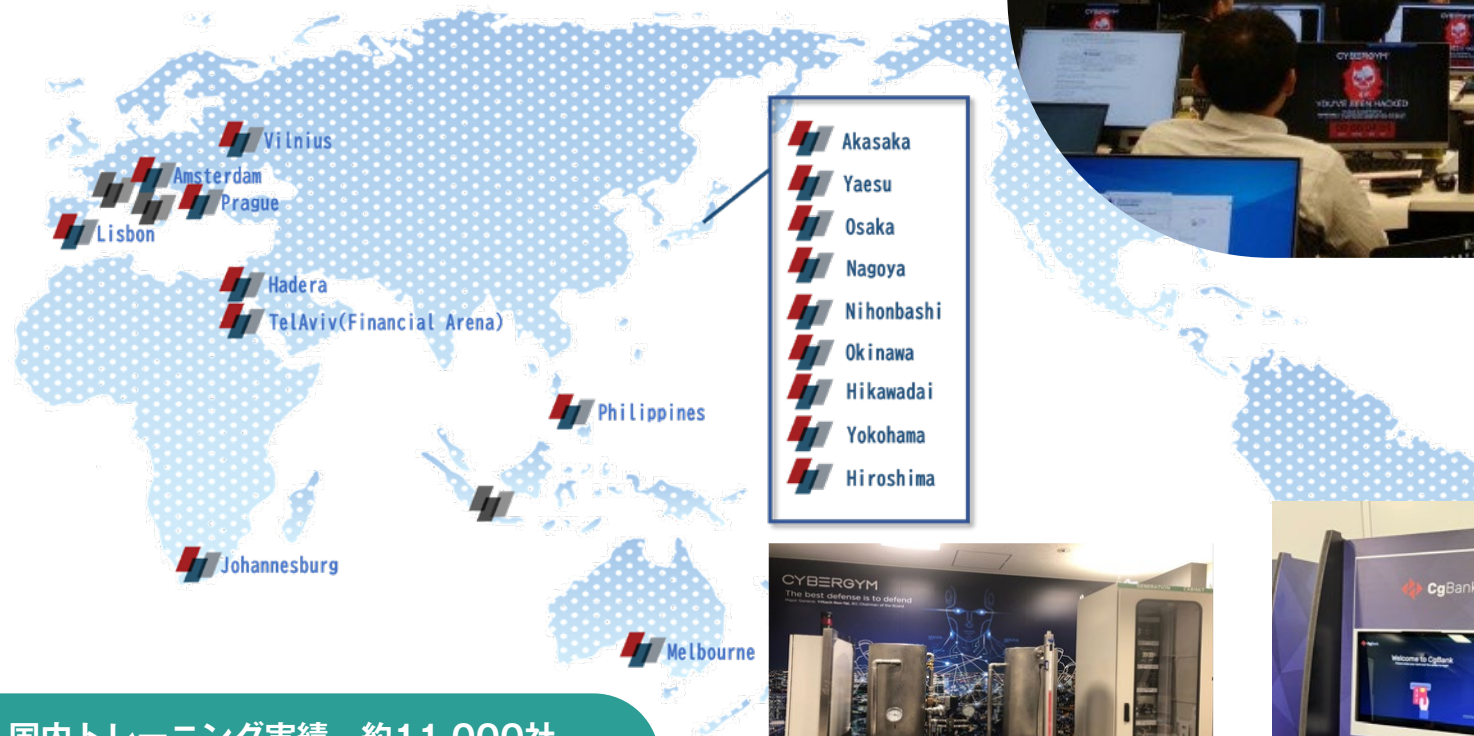
<https://attack.mitre.org/>

- MITRE ATT&CK は、CVE(Common Vulnerabilities and Exposures)をもとに分類された戦術とテクニックを体系化したフレームワーク。
- 攻撃者の手法を理解し、防御策を構築する際に役立つ。
- MITRE は、米国の連邦政府が資金を提供する非営利組織であり、サイバーセキュリティの分野で重要な役割を果たしている。
- このフレームワークは、攻撃者の行動を理解し、対処するための最適な方法を提供。
- 四半期ごとに更新されており、セキュリティアナリストやセキュリティプロフェッショナルにとって貴重なリソースとなっている。

中部地区で“世界クラス”のサイバーセキュリティトレーニングを提供



イスラエルのノウハウを凝縮したサービスを
日本でローカライズ・ブラッシュアップし
アジアへと展開を広げています



国内トレーニング実績 約11,000社
※アリーナで 約2,000社

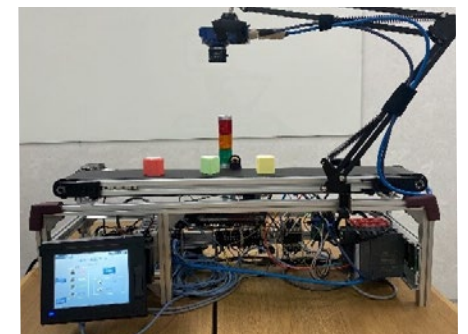
総務省・警察庁主催のトレーニング講師
300ヶ所 × 30社 = 約9,000社



赤坂 OT(制御向け)トレーニング設備



横浜 金融系トレーニング用 ATM



DX リテラシー基礎から専門知識までの教育メニュー

