

The Fortinet logo, featuring the word "FORTINET" in white capital letters. The "O" is replaced by a red square icon with a white grid pattern.

加速的に進化する脅威に – 脅威インテリジェンスという備え

2026 情報セキュリティワークショップ in 越後湯沢

今野俊一

脅威インテリジェンス研究員 兼

FortiGuard Labs日本向けスポークスパーソン

脅威インテリジェンス

- **従来の脅威インテリジェンス:**

- 侵害の痕跡
- マルウェア
- TTPs
- 守りを固め、脅威を検知して、素早く対応

- **脅威インテリジェンスから行動へ**

- 一歩先の脅威インテリジェンス
 - 演習 (TTX)
 - パートナーシップの重要性

UC Berkeley CTLC Partnership

- 演習 x 脅威インテリジェンス
 - 実際に起きた攻撃を再現することの価値
 - 実践で使える防御へと昇華
- TTXs:
 - AI-Enabled Cybercrime Initiative
 - セキュリティ・学術・政府・法執行機関が一堂に会して机上演習(TTX)を実施

UC Berkeley
CLTC
Partnership



UC Berkeley CTLC Partnership

- 第1回: 演習@ UC Berkeley
 - 参加者
 - サイバーセキュリティの専門化
 - 法執行機関
 - 業界のエキスパート
 - テーマ
 - AIを活用したサイバー攻撃の新たなトレンド
 - 脅威ランandscapeの進化

UC Berkeley
CLTC
Partnership



UC Berkeley CTLC Partnership

- 第2回: シンガポール演習
 - 参加者
 - 重要インフラ
 - 公的機関
 - 民間企業
 - シナリオ
 - AI生成マルウェア/ディープフェイク/電力・水力・交通など、複数の重要インフラへの同時攻撃/海外メディアによる虚偽情報の拡散

UC Berkeley
CLTC
Partnership



UC Berkeley CTLC Partnership

- 第3回: イスラエル演習
 - 参加者
 - 企業の経営幹部
 - 公的機関
 - セキュリティ責任者
 - シナリオ
 - ディープフェイク/取引先の侵害->基幹システムへの侵入/ランサムウェアによる暗号化/データ搾取/業務停止/規制当局への対応

UC Berkeley
CLTC
Partnership



UC Berkeley CTLC Partnership

- 教訓（自助）
 - 事前の備え
 - ガバナンス（組織の意思決定構造）
 - 部門を横断した危機対応チーム
 - 冷静な判断基準の事前設定
 - 本人確認の重要性
 - Secure-by-Design/Secure-by-Default
 - 最終判断は人（AIは仕分けのみ）

UC Berkeley
CLTC
Partnership



UC Berkeley CTLC Partnership

- 教訓（共助）
 - パートナーシップ(官民・産学官・民民)の重要性
 - 攻撃の進化→連携も進化する必要性
 - 業種を超えた、新たな脅威の可視性
 - 規律を持った情報発信
 - 脅威情報の速やかな共有
 - 現実に即したポリシー作り
 - AI時代の根源的なセキュリティ対策

UC Berkeley
CLTC
Partnership



UC Berkeley CTLC Partnership

- 教訓（公助）
 - 大規模なサイバーインシデントは、社会・国家レベルの対応が必要
 - 影響が社会に波及する可能性
 - 地方の法執行機関がインシデントを追跡し、FBI・CISA等の連邦機関に報告できるツール・指針の整備

UC Berkeley
CLTC
Partnership

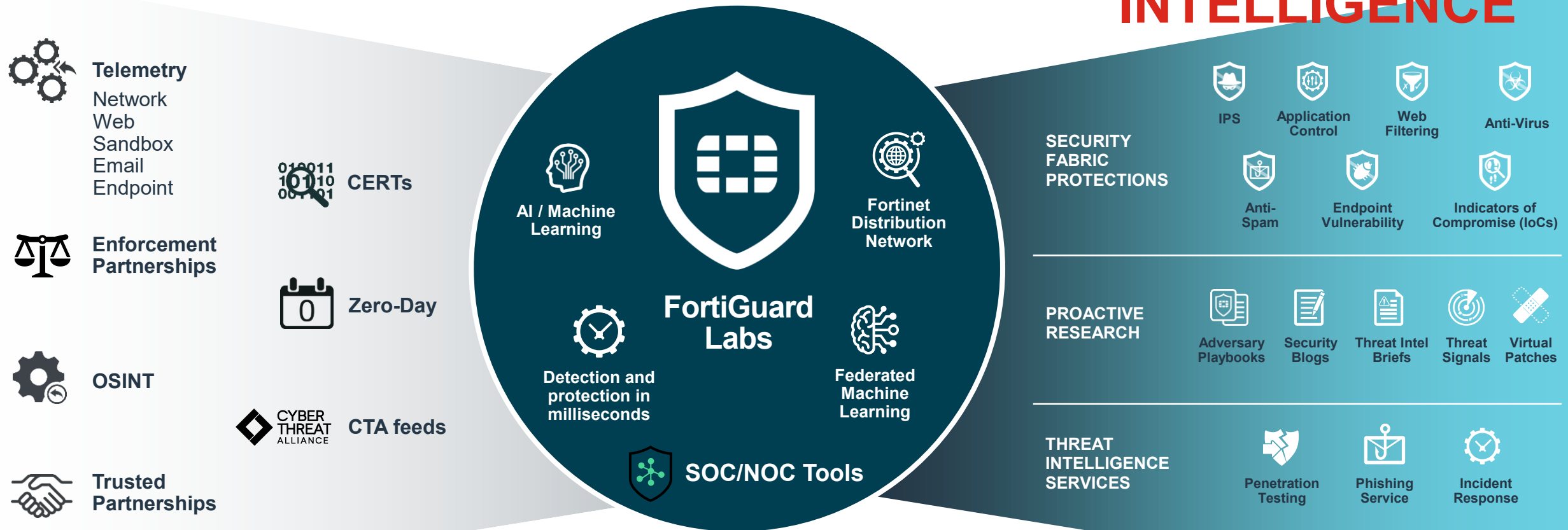


FortiGuard Labs

VISIBILITY

INNOVATION

**ACTIONABLE
THREAT
INTELLIGENCE**



産業化が進むサイバー犯罪

サイバー犯罪は現在、単発的なキャンペーンではなく、マシンスピードで継続的に実行される産業モデルとして運用されています。影響を左右するのは、攻撃の高度化ではなく、規模、自動化、再利用性です。

主な観測結果



グローバルな偵察イベント: **6,400億件**

17億5,000万件 1日あたりのスキャン数
1秒あたり20,000件以上、継続的に更新
前年比で45%減少

産業化が進むサイバー犯罪

主な観測結果



1,219億9,000万件

侵害の試み

前年比で25%の増加



46億2,000万件

ダークネット市場で流通するスティーラーログ

前年比で79%の増加



前年比で48.89%の増加

LOLbinが関係する不審なエンドポイント活動

産業化が進むサイバー犯罪

主な観測結果



635件

実際に悪用された脆弱性



364件

新たに悪用された脆弱性
(57.32%)



TTE (Time-to-Exploit)

0-24-48 Hours

パッチ適用や対応のタイムラインを上回る



Global Cybersecurity Partnerships

Fortinet's historic involvement combatting the **evolving threat landscape**

FIRST.org



Founded CTA



NATO
Cyber Partnership Agreement



WEF C4C
Founding Partner



CISA
JCDC
Partnership



UC
Berkeley
CLTC
Partnership



CRIME STOPPERS
INTERNATIONAL

ITTC INITIATIVE FOR
TRUST & TRANSPARENCY
IN CYBERSECURITY

2012

2013

2014

2015

2016

2018

2019

2021

2023

2024

2025

MITRE | ATT&CK®

MITRE
STIX & TAXII



INTERPOL

Global Cybercrime
Expert Group



INTERPOL

Gateway Partnership

MITRE
GENUITY™

A Foundation for Public Good

Center for Threat Informed
Defense Partner



The Cybercrime
Atlas



まとめ

- 脅威インテリジェンス
 - 脅威は加速的に進化している
 - 知ることから行動へ
 - 自ら備える（自助）
 - 分かち合う（共助）
 - 社会を支える（公助）
- FortiGuard Labsの連携への取り組み

The Fortinet logo, featuring the word "FORTINET" in white capital letters. The letter "O" is replaced by a red square icon with a white grid pattern.

FORTINET

ご清聴ありがとうございました