KITAMURA
ECONOMIC
SECURITY

The Era of “Preemptive Defense” Built by AI

The Asahi GHD Incident as a Turning Point for Japanese Corporations

Shigeru Kitamura

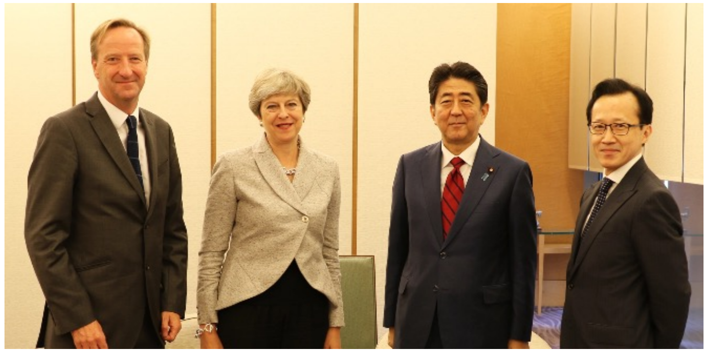
Shigeru Kitamura

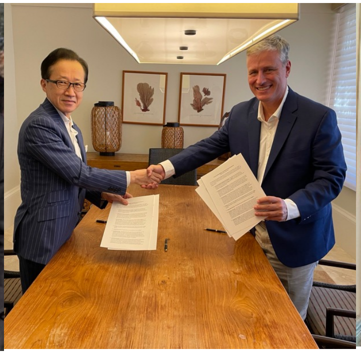
- Long career at the core of Japan’s intelligence and security community.

- Served as Director of Cabinet Intelligence.

- Later became Secretary General of the National Security Secretariat, a role comparable to the U.S. National Security Advisor.

- Worked closely with Shinzo Abe to help establish Japan’s National Security Council and shape key national security legislation.



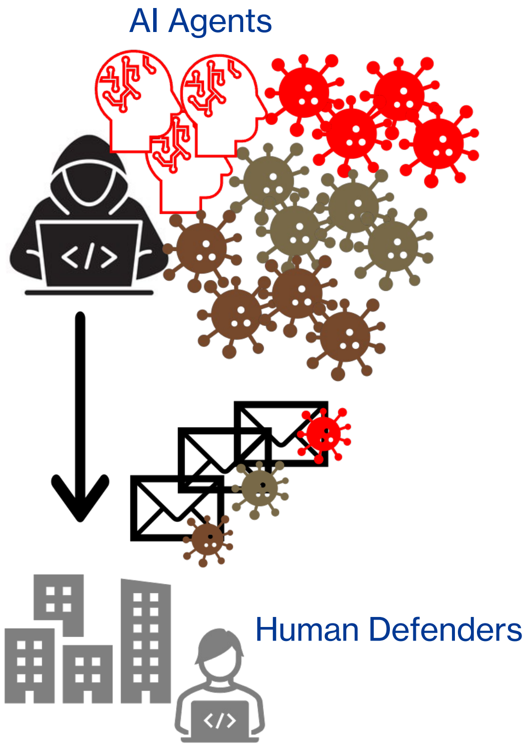


The Asahi GHD Incident: A New Type of Attack

- Late Sep 2025: Asahi Group Holdings operations disrupted by cyberattack
- Core IT systems paralyzed → production and logistics stopped
- Supply chain impact: product shortages across retail and restaurants
- Qilin “double extortion”; possibly state-linked
- Key takeaway: cyberattacks have evolved into weapons of economic coercion

Cyber Defense Is Now Economic Security

- The use of AI by attackers has changed the rules of cyber warfare
- Generative AI enables fast creation of malware and phishing emails that are very precise in context and language
- Core risk: autonomous AI agents coordinating end-to-end attacks
- Relying on human-only analysis and response is too slow
- Operational delays of hours can threaten the entire enterprise (supply chain paralysis)



Active Cyber Defense

- Strengthening information sharing
- Use of communications information for detection
- Empowerment for active prevention and mitigation
- Establishment of a centralized headquarters

サイバー対処能力強化法※1
及び同整備法※2について

※１　重要電子計算機に対する不正な行為による被害の防止に関する法律
（令和７年法律第42号）

※２　重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（令和７年法律第43号）

令和７年９月
内閣官房国家サイバー統括室

On ACD, from the National Cyber Office

The Limits of Human-Centric Defense

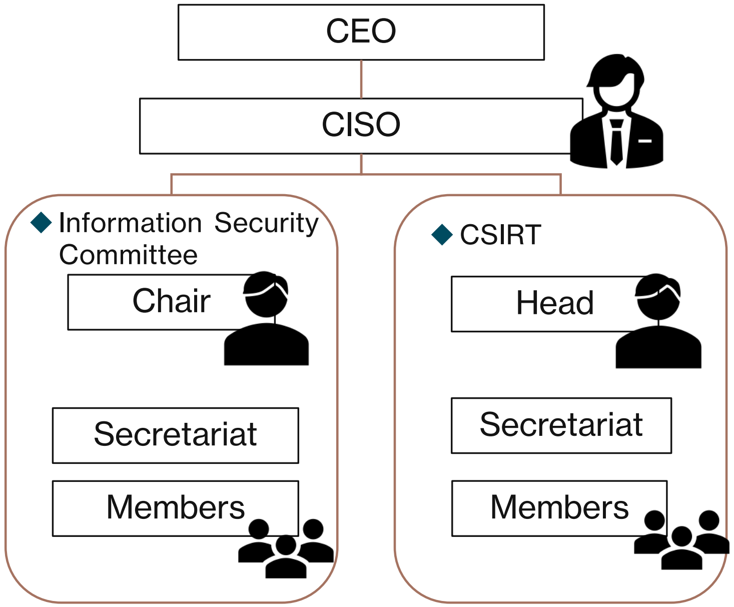
- Traditional hierarchical, human-centric security structures and workflows no longer viable

- Log volume is overwhelming: tens of thousands of alerts per day

- Asymmetry of cybersecurity

- Required shift to Preemptive Defense: autonomous, AI-driven, preemptive judgement and action

Example security management structure



CEO

CISO

◆ Information Security Committee

Chair

Secretariat

Members

◆ CSIRT

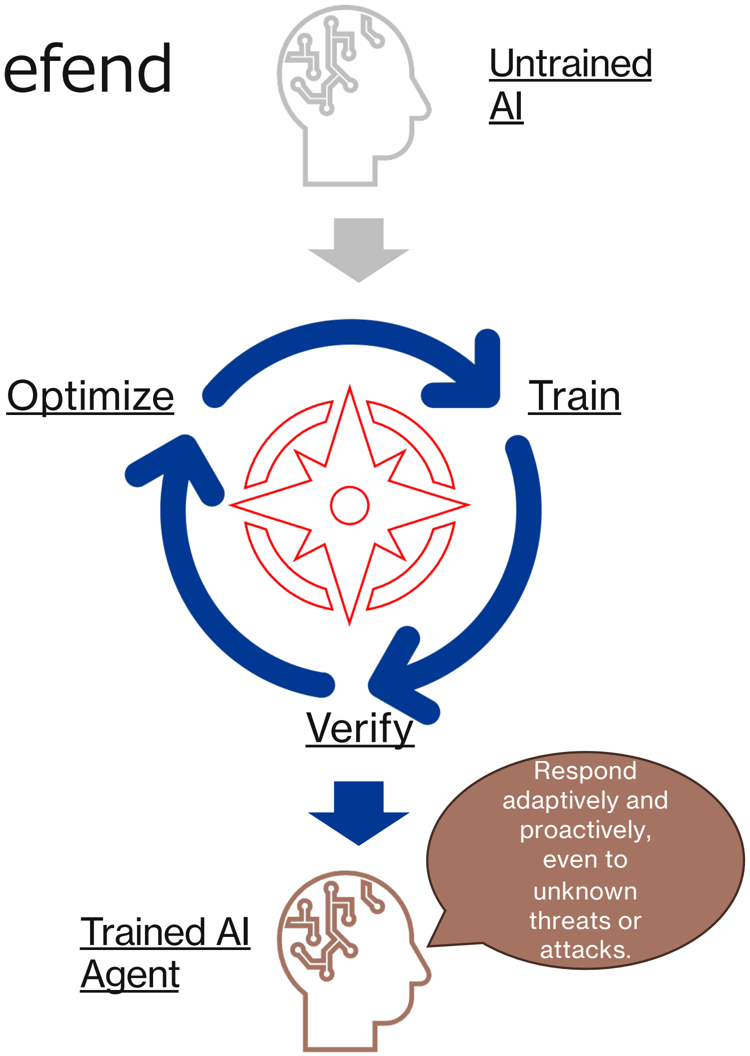
Head

Secretariat

Members

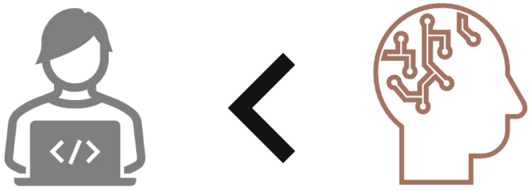
The Cyber Range: Where AI Learns to Defend

- Preemptive Defense requires a dedicated training environment for AI
- A cyber range provides a high-fidelity digital twin of networks, servers, and data flows
- AI agents train against simulated attacks, improving through millions of iterations
- Training must be done carefully (e.g., Proximal Policy Optimization).
- From “thinking after being attacked” to “stopping the attack before it happens”


Untrained AI
Optimize
Train
Verify
Trained AI Agent
Respond adaptively and proactively, even to unknown threats or attacks.

A Competition of Intelligence Velocity

- Cyberspace is now a battlefield of intelligence velocity: the time from detection to decision to action.
- AI-driven attacks exploit vulnerabilities faster than human can respond; defenders must operate in milliseconds
- Weaponized AI is no longer hypothetical
- Effective defense needs prediction, not just speed
- Preemptive Defense = anticipate the next move and close the vulnerability before exploitation

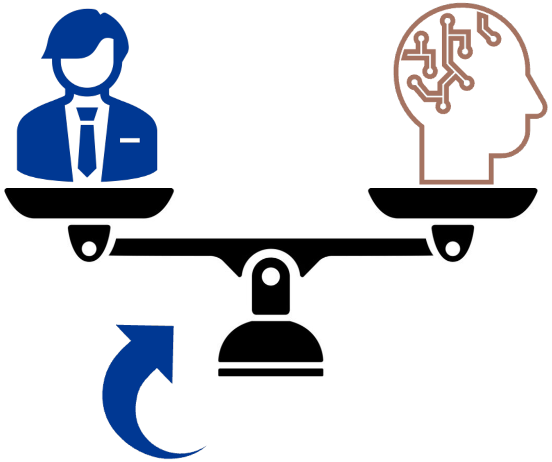


From Cost to Investment

- Security must also be redefined in the boardroom
- Average breach cost ≈ US$4.88m
- Preventing one major incident can justify investment in AI defense
- Real damage goes far beyond money
- Cyber defense is not a cost but an investment that sustains trust
- Investors and credit agencies will evaluate companies based on their security posture

Governance and Accountability

- A CEO cannot say, “The AI made the mistake.”
- Decisions must be explainable: explainability, visualization, and human oversight
- Balancing autonomy and governance



The Key to the Next Generation of Corporate Governance

Avoiding the AI Safety Myth: Three Principles

- Overconfidence is dangerous
- Blind trust in AI is not trust at all – it is abdication of responsibility

Three Principles

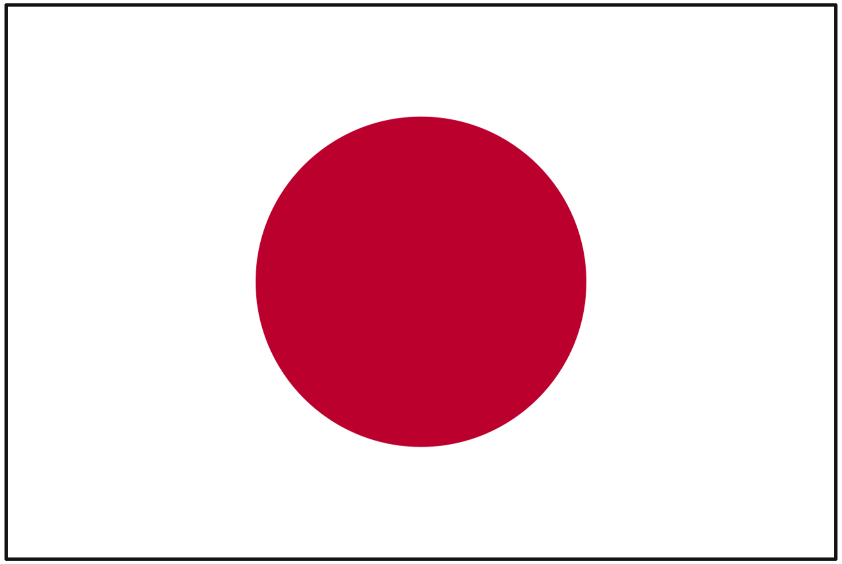
Principle 1: Accurate asset information – no drift between virtual and real systems

Principle 2: Intentional imperfection – training AI for messy reality, not perfect labs

Principle 3: Phased deployment – gradual expansion of trust

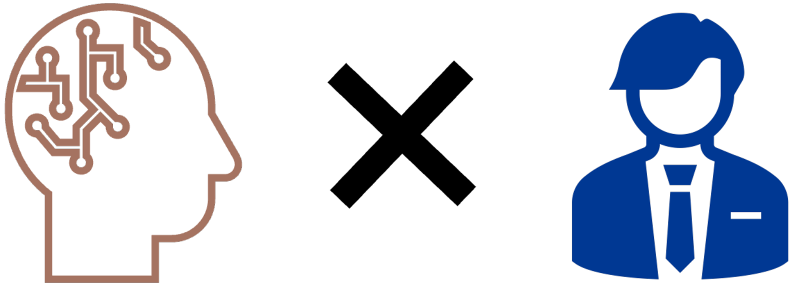
Toward an Ecosystem

- In the U.S., platforms like SimSpace are used jointly by the military, industry, and academia.
- Japan must move beyond isolated efforts. The Asahi incident should be a catalyst for cross-sector cooperation (Active Cyber Defense).



Preemptive Defense as a Management Philosophy

- Cyber defense is no longer a technical issue; it is a philosophy of decision-making
- Looking safe is not the same as *being safe*
- Next-generation defense: AI provides speed, cyber ranges provide verification, humans provide governance.
- Realizing Preemptive Defense: AI shows the signals, humans give them meaning, organizations act.
- Achieving true safety: AI is forged, humans govern, society trusts.



KITAMURA
ECONOMIC
SECURITY

Thank You