IT Risk Management

Protecting policyholders and sustaining insurance services

Yosuke Fujisawa, FIAJ, CERA
Data Science Officer, Sumitomo Life

Agenda

1.	Foundations and ISMS
2.	Cyber threats and IT resilience
3.	Third parties and data protection
	Break
4.	AI risk and use cases
5.	IT governance and management action
6.	Questions and discussion

Introduction

Actuarial and risk management experience across banking, insurance, reinsurance and AI

Yosuke Fujisawa

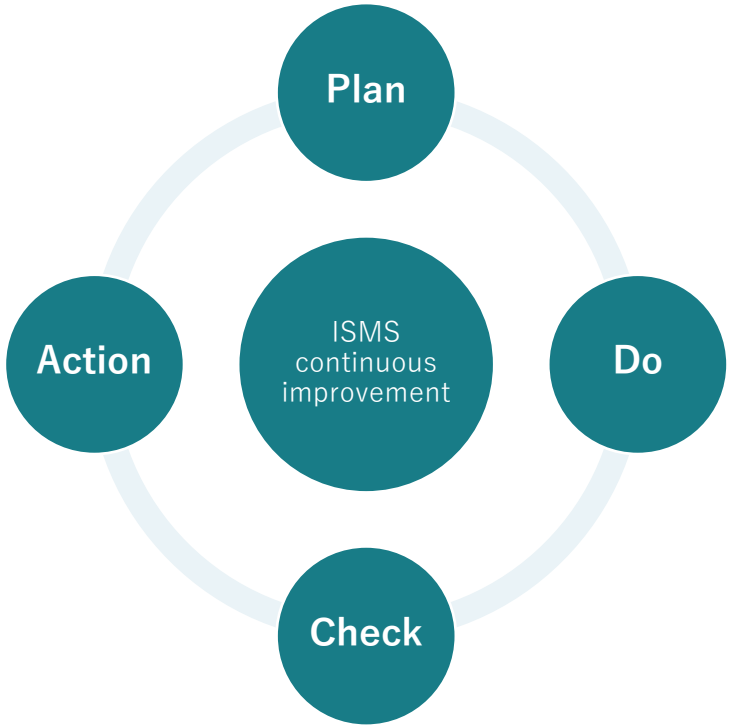
- Information Security Management (SG) – IPA, Japan
- Chair, IAA's Enterprise and Financial Risk Forum
- Chair, IAJ's AI Working Group

2000	Sumitomo Trust & Banking
2008	University of Waterloo
2011	Lifenet Insurance Company
2014	RGA Reinsurance Company
2017	Swiss Reinsurance Company
2020	Sumitomo Life

What Is an ISMS?

Information Security Management System

During my time at Lifenet, we obtained ISMS certification.



Plan — Develop the organization's information security objectives and plans. This includes formulating information security policies and conducting risk assessments.

Do — Implement and operate countermeasures in accordance with the plan. This includes employee training.

Check — Monitor and review implementation status and participate internally

Action — The organization's leadership implements corrective actions and improvements, while maintaining aspects that are already satisfactory.

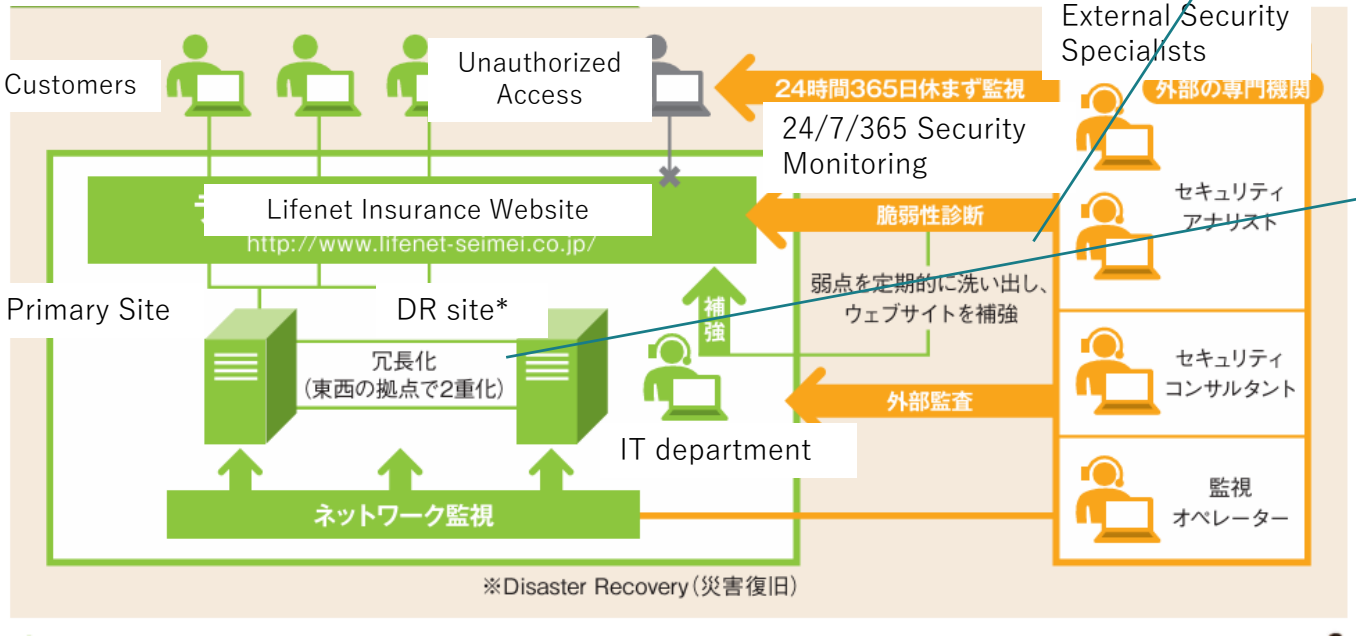
What Is an ISMS?

Information Security Management System

Information Security

Protecting Our Customers' Personal Information through Robust Security Measures

We recognize that properly handling our customers' valuable personal information is an important corporate social responsibility.
To strengthen our information security, we have invested in robust security systems, including the establishment of geographically separated data centers in eastern and western Japan.



Vulnerability Assessment:
Regularly identify vulnerabilities and strengthen website security

For example, Lifenet implemented a WAF, a type of firewall that inspects attacks on web applications and either blocks or neutralizes the associated traffic.

Redundancy:
Dual-Site Configuration in Eastern and Western Japan

In the wake of the Great East Japan Earthquake in 2011, Lifenet strengthened their disaster recovery site, recognizing that their headquarters was located only in Tokyo.

What Are We Protecting?

Three information security objectives, illustrated for a life insurer

Confidentiality

Only authorized people can access information.

Example: protect medical disclosures and customer records.

Integrity

Information remains accurate and complete.

Example: prevent unauthorized changes to beneficiaries or payment details.

Availability

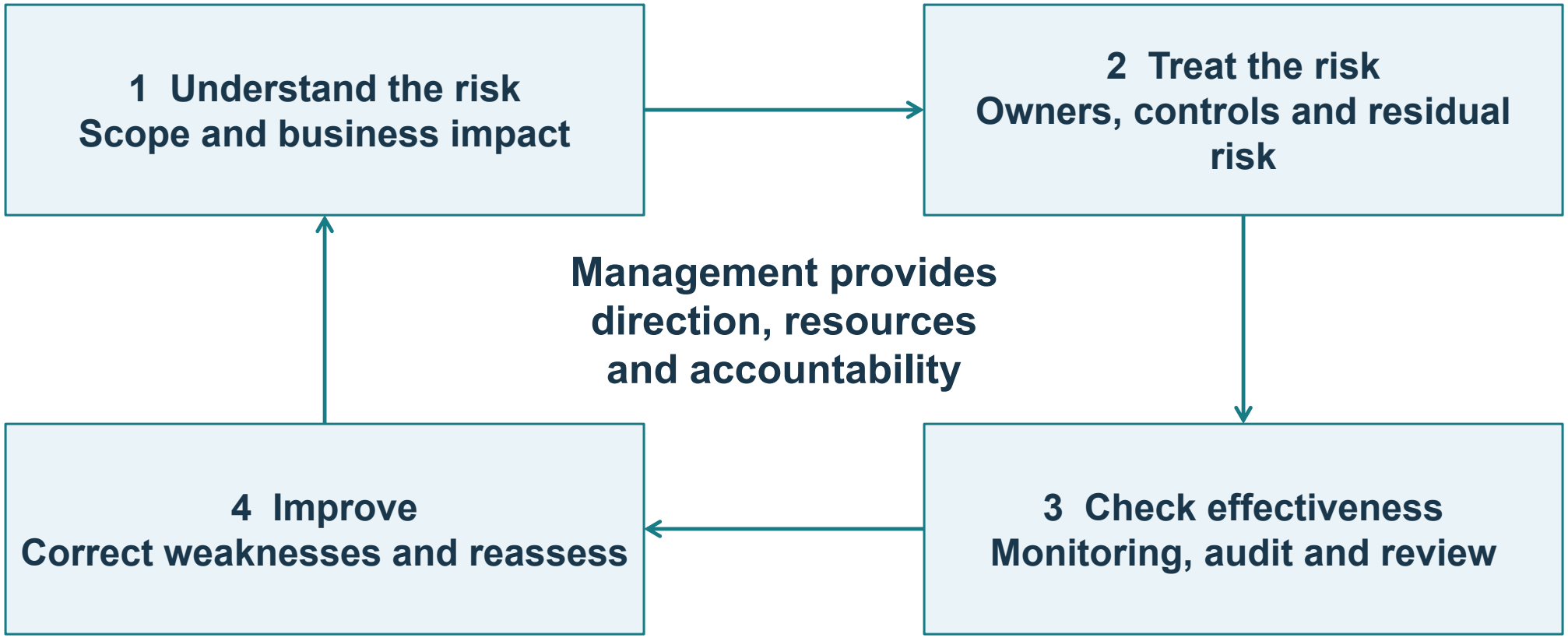
Authorized users can access information when needed.

Example: keep claims information accessible when benefits must be paid.

The business impact determines the level of protection required.

How an ISMS Works in Practice

A recurring management process supported by evidence



What Does ISMS Certification Mean?

Independent assessment of a management system within a defined scope

What is assessed

- A certification body evaluates conformity with ISO/IEC 27001 requirements.
- Certification provides assurance about the management system covered by the certificate.

Questions for management

- Which services, locations and operations are included in the certified scope?
- Are controls working, findings resolved and material changes assessed?

Certification supports assurance; ongoing risk management remains essential.

IT Risk Across the Insurance Business

Technology failures can affect customers even without a cyberattack

Security and privacy	Medical data, identity information and payment instructions require protection.
Service continuity	Claims, premium collection and policy changes depend on working systems.
Change and dependencies	Migrations, software updates and service providers can disrupt operations.
Models and automation	AI errors can affect underwriting, claims decisions and customer treatment.

Business owners remain accountable for the customer outcome.

Japan: IT Failures and Cyberattacks Both Matter

Financial Services Agency (FSA) analysis of reports for April 2025–March 2026

68.5%

Internal causes

39.2% Software failures
29.3% Management or human factors

8.2%

External causes

Unauthorized access and DDoS Attacks

Cyberattacks may account for a smaller share of reported incidents, but their potential impact can be severe.

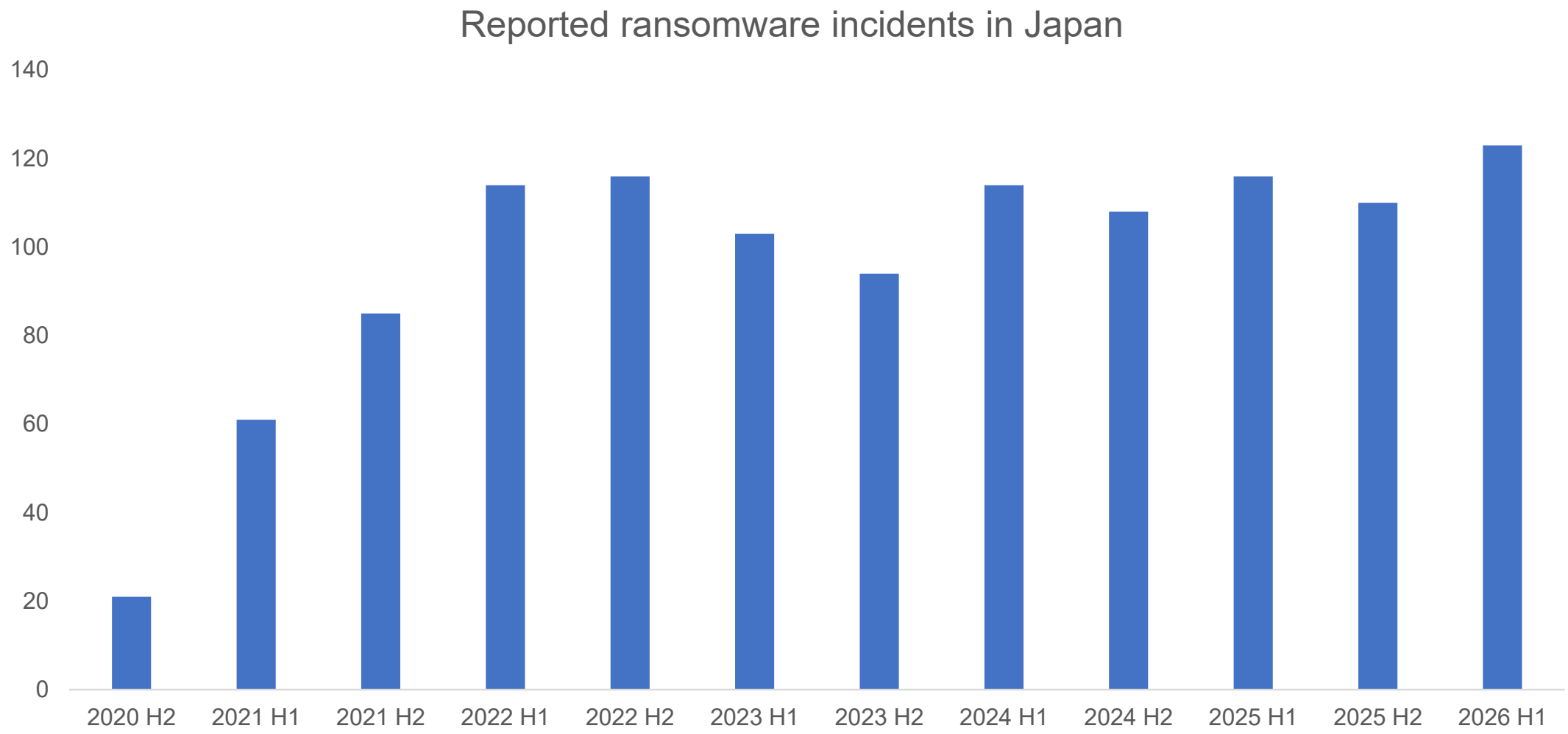
All financial sectors in Japan, not an insurance-only. About 1,600 reports received.

Source: Japan FSA, IT Resilience Analysis Report, July 2026

Agenda: Cyber Threats and IT Resilience

1.	Foundations and ISMS
2.	Cyber threats and IT resilience
3.	Third parties and data protection
	Break
4.	AI risk and use cases
5.	IT governance and management action
6.	Questions and discussion

Japan: Ransomware Reports since 2020



Source: National Police Agency of Japan

Ransomware: The Recovery Burden

Japan, first half of 2026

123

Reported incidents

The highest half-year total since reporting began in H2 2020.

60%

Costs of JPY 10m or more

Investigation and recovery costs can create a substantial financial burden.

48%

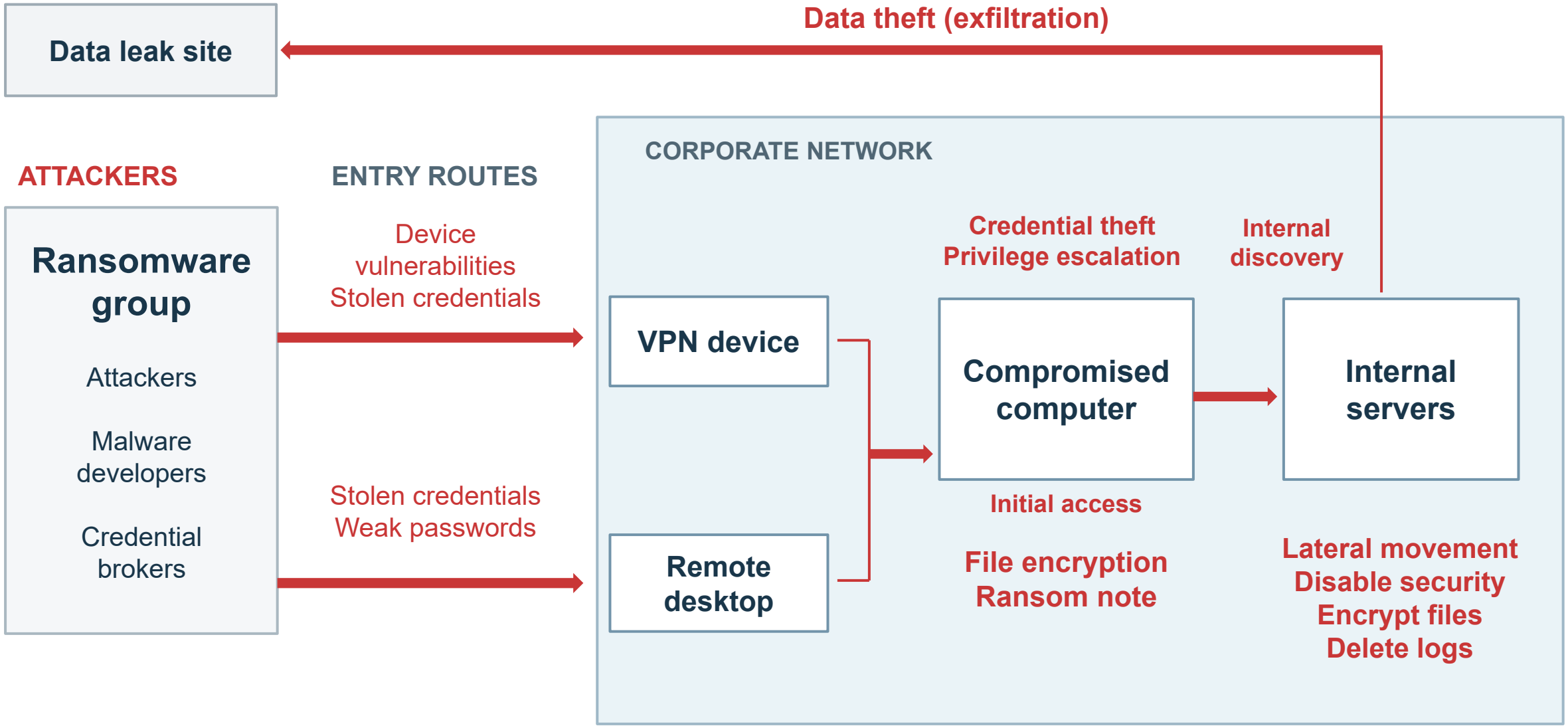
Recovered within one month

Fewer than half of respondents had recovered within one month.

Implication for insurers: test continuity plans for prolonged disruption to claims and outsourced services.

Source: National Police Agency, Japan, Cyber Threat Report, H1 2026

Ransomware attack flow



Risks of Paying a Ransom

01 Repeat attacks

Paying may make the organization a target for further attacks.

02 No guarantee of data recovery

Payment does not guarantee that data will be restored.

03 Legal and regulatory risks

Applicable sanctions and other legal requirements may restrict payment.

04 Reputational damage

Paying may undermine trust among customers and other stakeholders.

05 Funding further cybercrime

Ransom payments fund criminal activity and encourage future attacks.

06 Internal control concerns

Payment decisions may expose weaknesses in governance, approval processes, and oversight.

Case Study: Asahi Group Ransomware Attack (2025)

Asahi, a Japanese beverage group. Ransomware disrupted its Japan operations on September 29, 2025.

IT systems	Multiple servers and PCs were encrypted; affected networks and the data center were isolated.
Business operations	Order and shipment operations and customer call centers were suspended.
Production & distribution	Production and shipments were disrupted; all six domestic Asahi Breweries plants resumed production from October 2, with partial shipments of Asahi Super Dry restarting.
Financial reporting	Access to accounting data was disrupted, forcing the company to postpone its Q3 financial results.
Data risk	The investigation also found indications of unauthorized data transfer.

Ransomware: Prevention and Readiness

Controls need named owners and evidence that they work

Reduce entry routes

Keep an inventory of systems. Patch exposed weaknesses promptly. Use strong authentication and promptly remove unused access.

Limit the damage

Separate critical systems and restrict privileged accounts. Monitor unusual activity and rehearse rapid containment.

Prepare for recovery

Protect backup copies from alteration. Test clean restoration. Agree response roles, external support and the approach to ransom demands.

Source: IPA, Information Security 10 Major Threats 2026; Japan FSA, July 2026

Japan Insurance Case: Payment Delays

An anonymized insurance-sector case in the FSA's July 2026 report

What happened	A security software fault caused repeated computer crashes and restarts. Some surrender-value and other payments were delayed.
Operational gap	The insurer could not promptly identify affected payment processing or route urgent contracts for manual handling.
Response	Improve business-impact reporting and identify payments nearing their due dates for priority handling.

Lesson for insurers: recovery planning needs a payment-priority process.

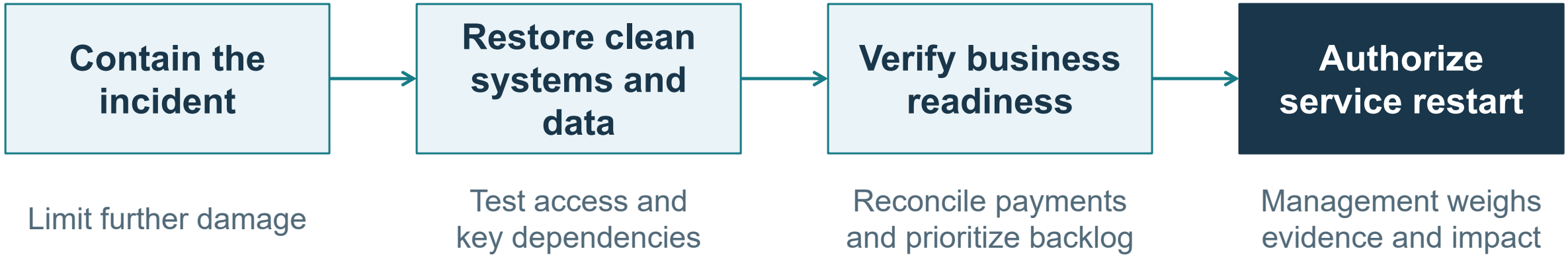
Source: Japan FSA, IT Resilience Analysis Report, July 2026

Recovery Objectives and Business Restart

A restored system still needs a controlled return to insurance operations

Recovery targets

RTO: target time to restore
RPO: acceptable data loss expressed as time



Customer-impact limits guide decisions throughout the response.

Source: Japan FSA, IT Resilience Analysis Report, July 2026

Agenda: Third Parties and Data Protection

1.	Foundations and ISMS
2.	Cyber threats and IT resilience
3.	Third parties and data protection
	Break
4.	AI risk and use cases
5.	IT governance and management action
6.	Questions and discussion

The Life Insurance Supply Chain

Service continuity also depends on partners across the policy lifecycle

LIFE INSURER

Sales & Distribution	Underwriting	Policy Administration	Claims Assessment & Payment
Insurance agencies Banks and brokers Online platforms	Medical examination providers Medical information services Reinsurers	Outsourced processing Call centers Printing and mailing	Claims investigation firms Medical institutions Payment service providers

TECHNOLOGY SUPPORTING ALL FUNCTIONS

Cloud providers, software vendors, IT service providers and telecommunications companies

Further dependencies: subcontractors and their technology providers

A cyber incident at one shared provider can expose customer data or disrupt operations across multiple insurers.

Shinchosha: Risk in Outsourced Investigations

Japan, June 27, 2025. Shinchosha supports application and claims verification.

Incident	A ransomware attack encrypted files on the provider’s computers and servers.
Life insurer example	Insurance companies, including Lifenet, reported customer information leaked or potentially leaked. Some records included disease or hospital names.
Response	Insurance companies announced individual customer contact and stronger oversight of outsourced providers.

Lesson: outsourced claims investigation can expose sensitive medical information.

Dai-ichi Frontier Life: A Subcontractor Breach

Japan life insurer. October 2025 disclosure involving a survey data-entry service.

Service chain

Insurer	Primary contractor	Subcontractor	AI text-reading tool
Dai-ichi Frontier Life	Nomura Research Institute (NRI)	Nippon Aspect Core	Laurel Bank Machines Jijilla service

What happened

Unauthorized access to the input-support service exposed respondent IDs and survey comments.

Six respondents had entered names or other identifying details in their comments.

Implications for insurers

Vendor oversight needs to cover subcontractors and the cloud tools they use.

Minimize data in free-text fields and agree incident reporting duties across the service chain.

Third-Party Oversight Throughout the Contract

An insurer retains responsibility for its services and customer outcomes

Select and contract	Assess criticality, data sensitivity and subcontractors. Agree security duties, notification, evidence access and data return or deletion.
Monitor and challenge	Review independent assurance and unresolved findings. Verify important controls rather than relying only on questionnaires.
Prepare for disruption	Map shared cloud and subcontractor dependencies. Test communications, alternatives and realistic exit arrangements.
Act on deficiencies	Set owners and deadlines. Escalate persistent gaps and reassess continuation of the service.

Different providers may depend on the same underlying service.

Source: Japan FSA, IT Resilience Analysis Report, July 2026

Break

Next: AI risk and use cases

AI-Related Threats and AI Use

The same responsibility for customer protection applies to both

Threats involving AI

How could attackers misuse AI?
Could an AI service expose our data?
Are our existing defenses sufficient?

Risks when insurers use AI

Can we trust the output?
Who owns the decision?
Can customers obtain a human review?

We will examine cyber threats first, then insurance decisions and wider scenarios.

AI-Related Cyber Risk

Ranked third in IPA's 2026 list of threats to organizations; newly selected in 2026

Risk	How it arises	Life insurance example (illustrative)
Data leakage and shadow AI	Employees enter confidential data into unapproved AI tools or personal accounts.	Claims files or medical information leave the approved environment.
Unreliable output and rights risks	AI can invent facts; unreviewed outputs may be inaccurate or infringe others' rights.	An incorrect policy explanation or claims summary reaches a customer.
More capable attackers	AI improves multilingual phishing and makes attack development and automation easier.	Convincing messages target staff, agents or policyholders.
Vulnerabilities in AI services	Malicious prompts can manipulate an AI service and expose data it can access.	An assistant connected to internal documents exposes confidential records.

Source: IPA, Information Security 10 Major Threats 2026

AI Misuse: Cases Reported by Japanese Police

AI can support malware development, service disruption and impersonation

Ransomware creation

Arrest: June 2026

Police allege that a suspect combined AI-generated source code to create ransomware.

Relevance: AI can lower the effort required to build attack tools.

Account disruption

Arrest: July 2026

Police allege that an AI-assisted attack program caused about 46,800 streaming accounts to close in November 2025.

Relevance: vulnerable customer services can face attacks at scale.

AI-generated faces

Arrests: August 2025

Suspects allegedly posed as police officers on video calls and used AI-generated faces to conceal their identities.

Relevance: a convincing video image is insufficient proof of identity.

Source: National Police Agency, Japan, Cyber Threat Report, H1 2026

Aflac Japan: abuse of normal-looking access

Unauthorised access affected Yorisou Net and the Online Consultation system.

~4.4 million

policyholders with personal data leaked

~220,000

of them had premium bank details exposed

Data included identity and contact details, policy numbers and coverage information.

What failed

Requests resembled normal use, delaying detection. Controls over rapid, high-volume data queries were insufficient. Earlier testing missed this scenario.

Aflac’s response

Stronger authentication and query authorisation, monitoring of bulk access, and stronger security reviews and penetration testing.

Times Car: identity documents exposed

Japan’s car-sharing service reported a data breach in September 2026.

~6.6m

accounts with leaked member data

Includes former members and incomplete applications.

~1.6m

accounts with identity documents leaked

Driving license images and other identity documents.

Potential insurer exposure: reuse of stolen identity evidence in another organisation’s checks.

Potential impact on insurer identity checks

A genuine document image alone cannot establish who is presenting it.

Insurance process	Illustrative misuse scenario	Possible consequence
New policy application	Reuse a stolen ID image and matching personal details	Impersonation at onboarding
Account recovery	Use leaked details to convince a service agent	Unauthorised account access
Payout or bank-detail change	Impersonate a policyholder after bypassing identity checks	Diversion of a legitimate payment

Exposure depends on customer overlap, accepted documents and the strength of each verification process.

FSA response to identity-document leaks

The FSA calls for stronger cyber controls and remote identity verification.

01 **Cybersecurity review**

Review third-party risk and incident response under management leadership. Address gaps promptly, according to risk.

02 **Stronger checks now**

Reinforce scrutiny of ID-document images and customer facial images for signs of manipulation or other irregularities.

03 **Early move to IC-chip reading**

The FSA urges action before 1 April 2027, when the revised rules abolish the ID-image submission method and make IC-chip reading the standard approach in principle.

Source: FSA notice, 9 Oct 2026.

IPA guidance: urgent action after data leaks

Management should lead an urgent review, including overseas operations and suppliers.

01 Public applications and services

Identify exposed systems, review unusual logs and apply missing patches. Expand log reviews from one month to three months.

02 External services and accounts

Inventory cloud and VPN use across the organisation. Check suspicious logins and unexpected or reactivated accounts. Clarify who can access logs.

03 Data minimisation and stronger controls

Keep only necessary data. Review storage, encryption and access logging. Even without detected anomalies, strengthen authentication and permissions, and review API connections, external exposure and log retention.

Abnormal logs or accounts: initiate incident response promptly and seek specialist investigation.

Source: IPA alert, 9 Oct 2026.

Seasar: why continued maintenance matters

Think of a critical component whose original maker no longer provides repairs.

01 What Seasar does

Seasar provides reusable building blocks for Java applications.
Seasar-related code on the Times Car website.

02 Why support status matters

Project maintenance for Seasar2 ended on 26 September 2016.
Continued use needs an alternative plan for security fixes. Without one, newly discovered weaknesses may remain unresolved.

03 The lesson for insurers

Know which older components support customer services. Confirm who will fix security issues, and fund replacement or additional safeguards.

Evidence limit: the cited sources do not establish Seasar as the breach entry point.

The Seasar Project

https://www.seasar.org

Seasar

Site Search

検索

Seasar Banner

Seasar DI Container with AOP

Seasar > ホーム

English | Japanese

利用者向け情報

- ニュース & Wiki
- プロダクト一覧
- メーリングリスト
- Eclipseプラグイン
- Mavenリポジトリ
- ライセンス
- 各種リソース
- イベントサイト
- ファウンデーションサイト

開発者向け情報

- SeasarWiki
- ソースコードリポジトリ
- 課題追跡

EOLについて

Seasarプロジェクトが提供するプロダクトの多くは **2016年9月26日** をもって **EOL (End of Life)** となります。

EOLとなるのは**以下を除いた全プロダクト**です。

- DBFlute
- DBFlute.NET
- Doma
- Emecha
- Mayaa
- S2Container.NET
- S2Dao.NET

上記以外のプロダクトは全て**2016年9月26日**をもってEOLとなり、 **Seasarプロジェクトによるメンテナンスおよびサポートは終了**となります。

EOLとなった後も、以下は引き続き提供されます

Many of the products provided by the Seasar Project will reach EOL (End of Life) on September 26, 2016.

AI Use Cases and Control Priorities

AI introduces risks to decisions as well as dependencies on technology providers

Use pattern	Life insurance example	Suggested control priorities
Staff assistance	Draft meeting notes or internal documents.	Approved tools, permitted inputs and staff review.
Internal knowledge assistant	Retrieve policy wording to support a service representative.	Access controls, current source documents and checks on retrieved evidence.
Customer-facing service	Answer policyholders' questions directly.	Clear service limits, tested responses and escalation to a person.

Retrieval-augmented generation (RAG) supplies documents to an AI model. Source quality and retrieval still need oversight.

Sumitomo Life: GenAI within a company at an individual level

あなたの未来を強くする
住友生命

NEWS RELEASE

2023 年 7 月 13 日
住友生命保険相互会社

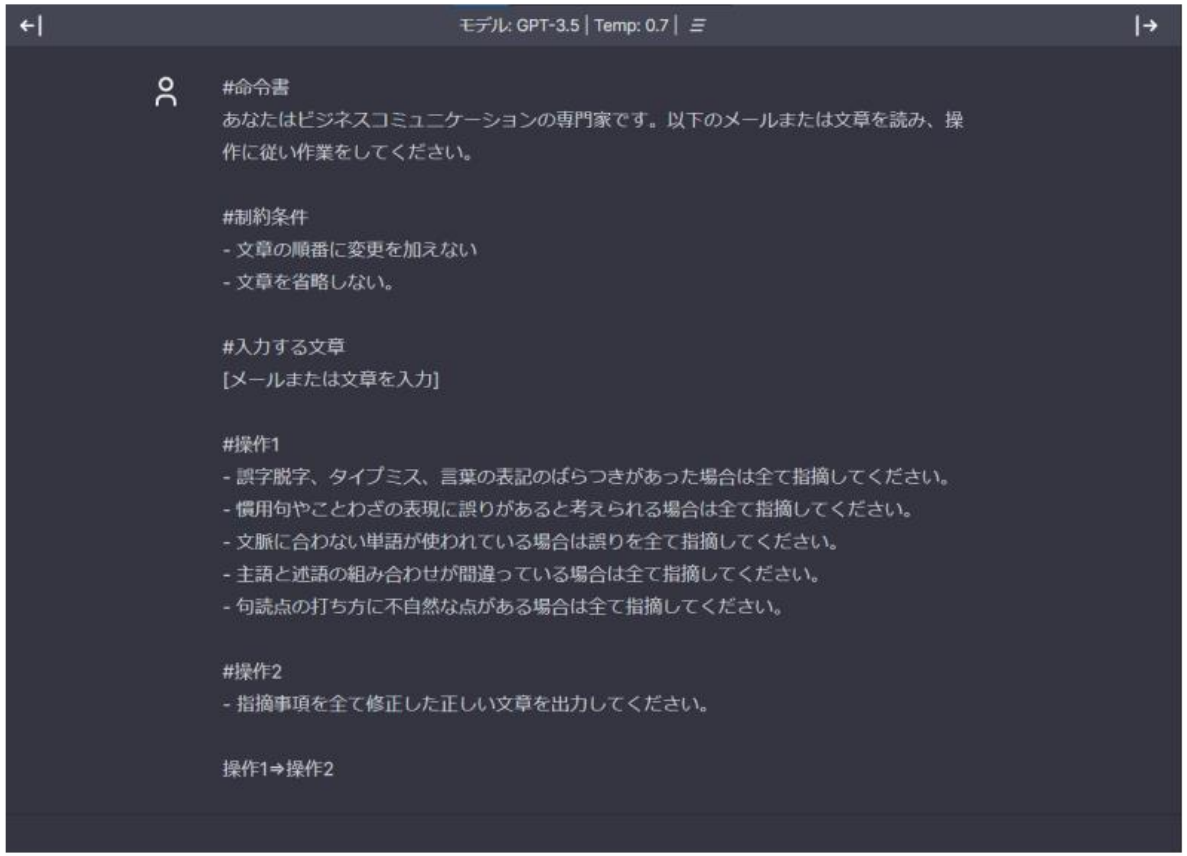
生成系 AI を活用した新たな顧客価値創造や生産性向上の取組み

～１万人の職員に導入 「人」と「デジタル」の融合で ウェルビーイングサービスの創出へ向けて加速～

住友生命保険相互会社（取締役 代表執行役社長 高田 幸徳、以下「住友生命」）は、生成系 AI チャットシステム（Sumisei AI Chat Assistant、以下「本システム」）を、７月 18 日より本社・グループ会社の職員約１万人を対象に運用開始予定です。本システムを通じて日常業務の生産性向上を図るほか、お客さま向けサービスの開発・更なるレベルアップに活用していきます。

住友生命は、「住友生命グループ Vision2030」の中で掲げる全てのステークホルダーの「ウェルビーイング※1」実現に向け、従来の保険会社の姿に留まることなく、“住友生命「Vitality」”をはじめとした、さまざまなよりよく生きるサービス「WaaS（Well-being as a Service）※2」を創出・提供することを目指しています。職員がデジタル・IT に関する知識やスキルを身に付け、さらに生成系 AI システムを活用することで、新たなウェルビーイングサービスの創出に向けた取組みを加速していきます。

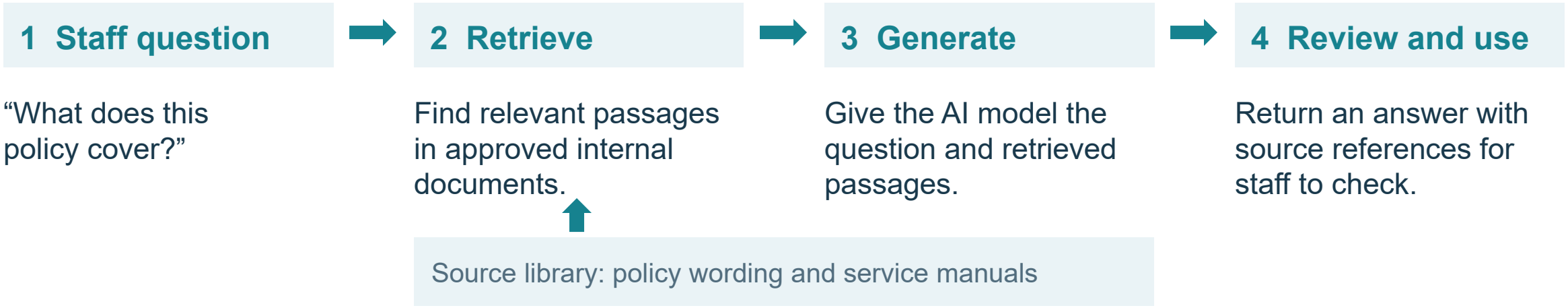
＜本システムのデモ画面：プロンプトの事例＞



Source: Sumitomo Life, 13 July 2023.

How Retrieval-Augmented Generation (RAG) Works

RAG adds relevant source material to a question before an AI model generates an answer.



Control priorities

Source quality and retrieval

Use accurate, current documents and test whether search retrieves the right policy and version.

Access and answer checks

Apply each user’s access rights. Check answers against sources and escalate uncertain cases.

RAG can improve relevance and accuracy, but incorrect answers remain possible.

Sumitomo Life: AI Role-Play for Sales Training

Announced on 24 April 2025, with rollout to new sales staff scheduled for 25 April.

Business need

Limited practice time and available partners, together with uneven coaching, created differences in new staff's skill development.

AI-supported practice

Staff practice with an AI customer avatar. AI evaluates the content and sequence of explanations, including accuracy and prohibited phrases.



Human feedback

Staff review recorded sessions. Managers use the recordings to identify gaps and provide coaching.

FWD Life Japan: AI Support for Underwriters

A Japanese life-insurance use case announced on October 2, 2025

Reported use

The system extracts medical information, summarizes relevant material and recommends underwriting results.

Role of people

The new support feature assists underwriters with cases requiring their judgment.

Questions for risk teams

How are medical facts checked? Who approves decisions? How are model changes and errors monitored?

Underwriting support requires evidence about both efficiency and customer outcomes.

Source: FWD Life Insurance Japan, company announcement, October 2, 2025

AI Risk in Insurance Decisions

Fairness and reliable outputs matter throughout underwriting, claims and customer service

Fairness

Biased data or model behavior may produce unfair outcomes for customer groups.

Illustration: an underwriting model systematically disadvantages a group.

Accuracy

Plausible but incorrect answers can misstate policy terms or distort a claims summary.

Illustration: an assistant describes cover that the policy does not provide.

Performance over time

Changes in customers, products or data can weaken a model's performance after launch.

Illustration: a model validated on past claims performs poorly on a new product.

IAIS: AI Oversight Proportionate to Risk

International Association of Insurance Supervisors. July 2025 guidance on existing principles.

Impact on people and the insurer

- Consider the effect on claims, underwriting and access to insurance.
- Assess customer vulnerability, scale of use and options for redress.
- Consider disruption to critical functions and potential financial impact.

Model and deployment characteristics

- Assess data quality, explainability and the degree of autonomy.
- Review changes to models and dependence on external providers.
- Apply stronger oversight where the assessed risks are higher.

Source: IAIS, Application Paper on the Supervision of Artificial Intelligence, July 2025

IAA: Evidence Throughout the AI Lifecycle

International Actuarial Association. Educational guidance published in November 2025.

Before use	Test unseen data, fairness and robustness; document assumptions and limits.
Independent challenge	Use qualified reviewers separate from development, proportionate to risk.
During operation	Monitor outcomes and changes; reassess whether the system remains fit for purpose.
Vendor models	Obtain documentation, validate outputs and clarify governance in contracts.

Professional judgment remains essential when using external AI.

Source: IAA, Artificial Intelligence Governance Framework (November 2025)

AI Expands the Information Assets We Must Protect

Sensitive information can appear in new forms and pass through more systems and providers.

Asset layer	Insurance examples	What needs protection
Source data and inputs	Claims files, medical records, questions and uploaded files	Confidentiality and permitted use of information sent to AI.
AI knowledge stores	RAG document copies, search indexes and training datasets	Access rights, document accuracy and updates across derived copies.
Models and instructions	Model versions, system prompts and AI configuration	Integrity of the components that shape AI behavior.
Outputs and records	Draft advice, conversation logs and training recordings	Sensitive content, retention and evidence of AI activity.
Connections and access	AI services, connected tools and API credentials	Provider data handling, service availability and access permissions.

Management Decisions Across Risk Horizons

Different risk horizons call for different evidence and actions

Current operations	Protect customer data and maintain essential services. Address known control weaknesses.
AI deployment	Require evidence before launch. Set limits, human review and authority to pause use.
Longer-term scenarios	Monitor emerging capabilities and shared dependencies. Test plausible scenarios and update plans as evidence changes.

Management must set priorities, assign responsibility and fund the response.

Agenda: IT Governance and Management Action

1.	Foundations and ISMS
2.	Cyber threats and IT resilience
3.	Third parties and data protection
	Break
4.	AI risk and use cases
5.	IT governance and management action
6.	Questions and discussion

IT Risk Management as a Management Priority

Cyber, operational and AI risks compete for management attention and resources

Customer protection

Service failures and data breaches can disrupt claims, expose customer information and damage trust.

Sustainable economics

Technology decisions shape operating costs, investment needs and the ability to deliver the business strategy.

Future competitiveness

Delaying change can forfeit better services and cost savings while increasing dependence on aging systems.

Management sets direction and allocates resources. Business and IT leaders share responsibility for delivery.

Source: Japan FSA, IT Governance Discussion Paper, 2nd ed., June 2023

Six Areas of IT Governance

Japan FSA framework, adapted for discussion with insurers in other jurisdictions

Area	Management focus
Leadership	Set the future direction and build digital understanding.
IT and digital transformation strategy	Align architecture and business change with corporate strategy.
Organization and accountability	Define responsibilities across business, IT and transformation teams.
Resources	Develop skills and allocate technology capacity and funding.
Investment management	Assess benefits and adjust funding as evidence develops.
IT risk	Compare adoption risks with the opportunities lost through inaction.

Source: Japan FSA, IT Governance Discussion Paper, 2nd ed., June 2023

Key Takeaways

ISMS, resilience, provider oversight and AI governance protect the insurance promise

Customer protection

Information security and service continuity protect the promise made to policyholders.

Operational evidence

Recovery tests, sound change control and provider oversight show whether plans work.

Management accountability

AI and IT decisions need named owners, independent challenge and action when limits are breached.

Questions and Discussion

Thank you very much for your attention!