Analyzing Investment Incentives under METI's New Rating System via a Stepwise Extension of the Gordon-Loeb Model

RYOMA KANAI[*,†] AND KANTA MATSUURA[*,‡]

[*]*The University of Tokyo*
[†]*rkanai@iis.u-tokyo.ac.jp*, [‡]*kanta@iis.u-tokyo.ac.jp*

Abstract: Against the backdrop of increasingly severe supply chain attacks, Japan's Ministry of Economy, Trade and Industry (METI) is formulating a new institutional system to evaluate and visualize companies' security measures in a stepwise manner, ranging from a three-star rank (★3) to a five-star rank (★5). This system features a discrete rank structure, comprised of basic measures based on self-declaration (for ★3) to advanced measures requiring third-party certification (for ★4 and ★5). However, conventional models premised on the "continuity" of investment effectiveness, such as the Gordon-Loeb model (GL model) and the Matsuura model, fail to sufficiently explain corporate investment decision-making under such a "discrete" scheme or the network externalities associated with its diffusion. In this study, building upon the Matsuura model, we propose a stepwise extension model that incorporates the specific ★ structure of the system and network externalities where transaction opportunities fluctuate. Through analysis using the proposed model, we quantitatively derive the threshold of diffusion (critical mass) required for companies to shift their investment behavior from the status quo (★0) to participation, and further to higher ★s. Our analysis reveals that participation (★0 → 3) is governed by "survival" incentives to avoid market exclusion, whereas transitioning to higher ★s (★3 → 4) is driven by "growth" incentives aimed at capturing further market opportunities, representing decisively different investment incentives. Furthermore, numerical simulation results demonstrate the risk that excessive support measures (such as subsidies) aimed at lowering the entry barrier to ★3 (Basic) may relatively diminish the incentive to transition to ★4 (Standard). This can cause economic stagnation—a phenomenon practically known as the "checkbox compliance trap"—where corporate investment behavior becomes fixed at lower ★s, satisfying minimum requirements without pursuing actual security growth. These findings provide policy implications based on mathematical evidence for designing institutional systems and optimizing subsidy policies to improve the security level of the entire supply chain.

Key words: Economics of Information Security, Gordon-Loeb Model, Matsuura Model, METI's Rating System, Investment Incentive

1. Introduction

1.1. Background

Since its establishment in the early 2000s, the Economics of Information Security has developed as a field analyzing information security issues through economic approaches [1, 2]. A central issue in this field concerns the optimization of information security investment. Specifically, firms must determine how to allocate limited management resources to minimize expected losses from security risks and maximize corporate value. Since perfect security is unrealistic and uneconomical, determining investment levels requires a rational basis, and numerous studies have modeled this decision-making process.

In their pioneering work, Gordon and Loeb [1] mathematically demonstrated that a firm's optimal security investment amount remains below a certain fraction ($1/e$) of the expected loss [3]. Over the subsequent 20 years, the Gordon-Loeb (GL) model has established itself as a standard reference in the field, undergoing validation and various extensions to reflect the complexities of reality [4, 5]. These conventional theoretical models primarily discuss investment optimization assuming market mechanisms and autonomous corporate decision-making, treating investment effectiveness as a continuous variable.

However, recent years have seen progress in implementing "rating systems" with specific and enforceable frameworks at the national level to defend the entire supply chain. In Japan, the Ministry of Economy, Trade and Industry (METI) is constructing a new institutional system that visualizes the status of corporate measures and links them to transaction conditions. It is not self-evident whether conventional investment models assuming continuous variables can directly apply to this new environment characterized by a "discrete rank structure" and "system-driven market access control." We extend existing models to apply insights from the economics of information security to this emerging problem of institutional design.

1.2. METI's New Rating System

1.2.1. Policy Background

In recent years, with the progress of Digital Transformation (DX), dependence on IT systems in corporate activities has increased dramatically. Meanwhile, cyber-attack methods have become more sophisticated. In particular, "supply chain attacks," which target large enterprises and critical infrastructure via small and medium-sized enterprises (SMEs) with weak security measures, have become a serious threat. Under these circumstances, ensuring the security level of the entire supply chain, not just individual companies, is an urgent issue.

Conventionally, ordering companies have confirmed the security of their suppliers using proprietary checklists. However, this imposes a challenge for suppliers, who face the multiple burdens of responding to different formats for each business partner. It also presents a challenge for ordering companies, as verifying the objective validity of the responses proves difficult. To address these issues, METI and the National center of Incident readiness and Strategy for Cybersecurity (NISC) announced a policy to construct the "Security Assessment System for Supply Chain Reinforcement"[1] in December 2025 [6].

1.2.2. Overview of the System

This system aims to strengthen measures across the entire supply chain and facilitate transactions by evaluating corporate security measures based on unified standards and visualizing the results. A primary feature of this system is its evaluation categories, which consist of a stepwise structure according to maturity, rated from a three-star rank (⋆3) to a five-star rank (⋆5).

- **⋆3 (Basic):** A stage where standard measures based on guidelines such as the "Information Security Guidelines for SMEs" are implemented. The evaluation method adopts "Self-Declaration" confirmed by security experts, aiming to raise the baseline of the entire supply chain.
- **⋆4 (Standard):** A stage where more advanced measures, including the construction of management systems and the operation of PDCA cycles, are implemented. To ensure reliability, "Third-party Certification" by an evaluation body is a mandatory requirement.
- **⋆5 (High):** The highest ⋆ corresponding to areas requiring extremely high security levels, such as the defense industry and critical infrastructure. It requires the ability to respond to advanced threats, with a view to consistency with international standards (e.g., NIST SP800-171).

Information on companies that pass the conformity assessment is registered in a public registry and disclosed. This visualization enables ordering companies to refer to ⋆s during procurement, fostering an environment expected to favor firms making appropriate security investments.

1.2.3. Problem Statement

Economically, the decision of whether companies voluntarily invest in these ⋆s—that is, participate in the system ($\star 0 \rightarrow 3$) or transition to higher ⋆s ($\star 3 \rightarrow 4$ or higher)—depends strongly on institutional design parameters. The GLLZ model [7] highlights that information security investment effects are

[1] As of the writing of this paper, an official English name for this system has not been announced by METI. The English name used in this paper is a tentative translation by the authors.

difficult to perceive as direct profit, causing corporate investment to fall below the socially desirable level (under-investment).

Given the discrete structure of stars (⋆) in METI's new system, companies make decisions by comparing costs and benefits not through continuous investment adjustment but from discrete options: "⋆0 (Status Quo)," "⋆3 (Basic)," "⋆4 (Standard)," and "⋆5 (High)." In particular, if the market benefits (increase in transaction opportunities) from acquiring higher ⋆s are insufficient relative to the entry costs for ⋆3 or the transaction costs associated with transitioning to ⋆4 or higher, a risk of falling into the "Checkbox Compliance Trap" arises, where companies stop investing at lower ⋆s that offer better cost-performance.

1.3. Contribution

We propose a stepwise extension of the Gordon-Loeb Model that incorporates the "discrete rank structure" and "special network externalities (fluctuation of transaction opportunities)" characteristic of METI's new system. We build upon the GL model and its extension, the Matsuura model. Using this proposed model, we quantitatively derive the conditions (critical mass) necessary for companies to change their investment behavior step-by-step from status quo (⋆0) to system participation (⋆3), and further to advanced measures (⋆4 and above).

Furthermore, through numerical simulation, we analyze the impact of institutional design parameters (certification costs and market merits) on corporate investment behavior. In particular, we examine the possibility that support measures for lower ⋆s may hinder the transition to higher ⋆s, aiming to provide policy implications for enhancing the effectiveness of the institutional system.

2. Related Work

Scholars have actively discussed the optimization of information security investment for over 20 years since the pioneering GL model [5]. This chapter outlines the history of this research field and clarifies the positioning of our study.

2.1. Verification and Mathematical Refinement of Basic Models

The Gordon-Loeb (GL) model [1] pioneered the field by introducing a vulnerability reduction function based on investment amount and deriving the "$1/e$ rule," stating that the optimal security investment amount does not exceed $1/e$ (approximately 37%) of the expected loss [3]. Subsequent research has verified and generalized the mathematical properties of this model. For example, Willemson [8], Baryshnikov [9], and Lelarge [10] analyzed the mathematical conditions for the $1/e$ rule to hold and exceptions in specific functional forms. Hausken [11] verified the robustness of the model by analyzing investment effects using alternative functional forms other than those adopted in the GL model (Class I/II). These early studies provided the essential theoretical foundation for clarifying the basic structure of investment cost-effectiveness within a static framework.

2.2. Extensions for Practical and Realistic Requirements

The original GL model was abstract, treating threat occurrence probability and loss magnitude as fixed values and considering only a single investment target. Therefore, researchers have extended the model to apply to more realistic or practical situations. Matsuura [4] extended the GL model by assuming that security investment contributes not only to the reduction of vulnerability but also to the reduction of threat occurrence probability [12]. Farrow and Szanton [13] extended the model using weighted averages to handle optimization problems where multiple investment targets exist or budget constraints apply. They also incorporated the effect whereby security investment reduces not only the breach probability but also the "magnitude of loss" itself upon breach occurrence. Attempts to model investment decisions under complex risk environments include the proposal of multivariate models by Huang and Behara [14]. More recently, Cherubini [15] extended the model to express dependencies between multiple defense targets using copula functions, advancing the refinement of the model. These studies adapt the abstract settings of the GL model to the complex environments faced by real-world companies.

2.3. Consideration of Dynamics, Externalities, and Discrete Structures

Advanced extensions consider time lapse and externalities. Gordon et al. [16] and Tatsumi and Goto [17] analyzed the optimal timing of investment using a real options approach, while Krutilla et al. [18] proposed a dynamic model considering the depreciation of security capital. Recently, Callegaro et al. [19] presented a stochastic differential equation model considering the clustering of attacks. Lelarge [10] extended the GL model to a game of multiple agents in a network environment, analyzing investment incentives where positive network externalities exist—specifically, where one agent's security investment reduces the risk for others. Also, Gordon et al. [7, 20] analyzed the externalities of security investment by extending models to include information sharing effects and social losses, while Skeoch [21] and Mazzoccoli and Naldi [22] discussed risk financing through combinations with cyber insurance. Furthermore, as regulatory frameworks have matured, models have begun to adapt to compliance structures. Notably, Gordon, Loeb, and Zhou [23] pioneered the application of the GL model to the discrete, four-tier compliance structure of the NIST Cybersecurity Framework, elegantly deriving threshold conditions for moving between tiers based on cost-benefit analysis.

2.4. Positioning of This Study

While Gordon, Loeb, and Zhou provided foundational work in applying the GL model to discrete compliance tiers, their model primarily addresses tier transitions based on the firm's internal security cost-benefit analysis. METI's new system possesses an additional, unexplored structural characteristic: a "stepwise change in market access" as a special, market-driven network externality.

In our study, the business benefit of compliance is not a static exogenous constant, but dynamically fluctuates with the system adoption rate. Therefore, we build upon the GL and Matsuura models, integrating the discrete approach of Gordon, Loeb, and Zhou with market-driven network externalities. This combination enables our analysis of macro-level critical mass diffusion and the paradoxical "checkbox compliance trap," representing the primary theoretical novelty of our paper.

3. Base Models

Based on the policy described in the previous chapter, we detail the two single-period models that form the direct basis of this study.

3.1. Gordon-Loeb Model

Gordon and Loeb [1] constructed a mathematical model (GL model) to analyze the cost-effectiveness of information security investment. This model formulates how an investment amount contributes to the reduction of expected losses when a firm makes additional security investments to protect information assets, deriving the optimal investment amount.

3.1.1. Model Definitions and Assumptions

Let L be the potential loss of an information asset held by a firm, and $v \in [0, 1]$ be the probability of a successful security breach (vulnerability) in the initial state. We assume that if the firm invests an amount $z(\geq 0)$ in security measures, the probability of a successful breach reduces to $S(z, v)$. We denote $S(z, v)$ as the Security Breach Probability Function, defined to satisfy the following conditions:

1. $S(0, v) = v$: The probability of a successful breach without investment equals the initial value v.
2. $\frac{\partial S(z,v)}{\partial z} < 0$: As the investment amount increases, the probability of a successful breach decreases.

3. $\frac{\partial^2 S(z,v)}{\partial z^2} > 0$: The reduction effect of investment on the probability of a successful breach exhibits diminishing marginal returns.

Gordon et al. presented the following two classes as specific functional forms for $S(z, v)$:

$$\text{Class I:} \quad S(z, v) = \frac{v}{(\alpha z + 1)^{\beta}} \tag{1}$$

$$\text{Class II:} \quad S(z, v) = v^{\alpha z + 1} \tag{2}$$

Here, $\alpha > 0$ and $\beta \geq 1$ are parameters representing the productivity of security investment.

3.1.2. Optimal Investment Level

The firm's objective is to maximize the "Expected Net Benefit of Information Security (ENBIS)" from security investment. First, the "Expected Benefit of Information Security (EBIS)," which is the amount of reduction in expected loss obtained by an investment amount z, is expressed by Equation (3).

$$EBIS(z) = [v - S(z, v)]L \tag{3}$$

Figure 1 schematically shows the relationship between this $EBIS(z)$ and the investment amount z. As the investment amount increases, EBIS increases, but its rate of increase (marginal benefit) gradually decreases (concave function). Since the ENBIS that the firm should maximize is defined as this expected benefit minus the investment cost z, as in Equation (4), the optimal investment amount z^* corresponds to the point where the marginal benefit equals the marginal cost (= 1).

$$ENBIS(z) = EBIS(z) - z = [vL - S(z, v)L] - z \tag{4}$$

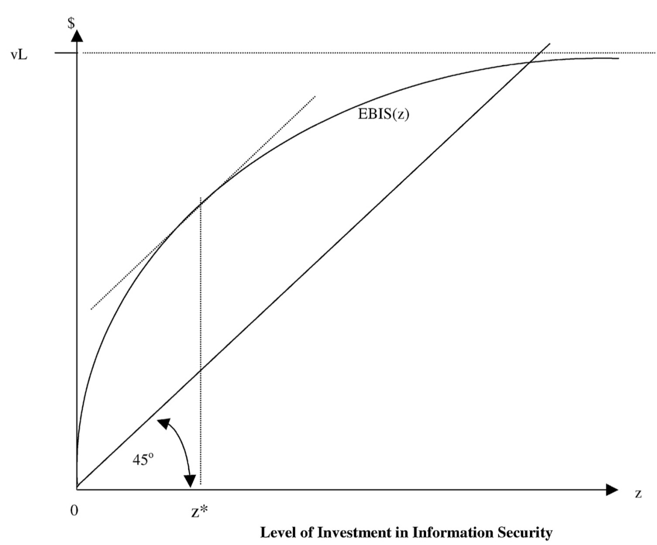


Fig. 1. Conceptual Illustration of EBIS and Investment Level (Based on [3])

Through this analysis, Gordon et al. derived the following important finding (the $1/e$ rule). Equation (5) shows that the optimal security investment amount z^* never exceeds $1/e$ (approximately 37%) of the expected loss vL.

$$z^* < \frac{1}{e} vL \tag{5}$$

3.2. Matsuura Model

Matsuura [4] extended the GL model to capture the effects of security investment in a more multifaceted manner [12]. While the GL model limits the effect of investment to "vulnerability reduction," the Matsuura model introduces a new aspect: "threat reduction."

3.2.1. Extension to Threat Reduction

The Matsuura model perceives the risk of security breach as the product of vulnerability v and threat occurrence probability $t \in [0, 1]$. The model assumes that an investment amount z reduces vulnerability to $S(z, v)$ and simultaneously reduces the threat occurrence probability to $T(z, t)$. In this case, Equations (6) and (7) extend EBIS and ENBIS, respectively. Here, λ represents the conditional loss amount upon breach occurrence, and the potential loss L in the GL model corresponds to $L = \lambda t$ in the initial state.

$$EBIS(z) = [\lambda vt - \lambda S(z, v)T(z, t)] \tag{6}$$

$$ENBIS(z) = EBIS(z) - z \tag{7}$$

The Matsuura model assumes the Class II functional form ($S(z, v) = v^{\alpha z+1}$) of the GL model for the vulnerability reduction function $S(z, v)$. Similarly, it assumes a Class II type functional form for the threat reduction function $T(z, t)$.

$$T(z, t) = t^{\beta z+1} \tag{8}$$

Here, α represents the productivity for vulnerability, and β represents the productivity for threat occurrence probability.

3.2.2. Productivity Space Analysis

Matsuura analyzed optimal investment strategies using a "Productivity Space" defined by the two productivity parameters (α, β). Figure 2 shows the classification of investment strategies by this analysis. As shown in the figure, the optimal investment behavior of firms falls into one of three areas according to the parameter combination.

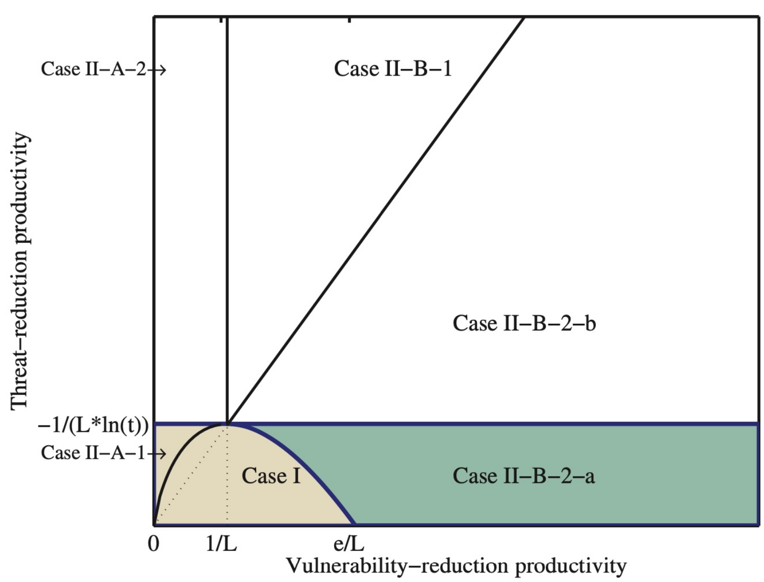


Fig. 2. Productivity Space and Three Optimal Investment Strategies (Based on [12])

1. **No-Investment Area:** When both α and β are low. Since the benefit from investment does not exceed the cost, not investing is optimal.
2. **Mid-Vulnerability Intensive Area:** When α is high and β is low. Similar to the GL model, investing intensively in assets with moderate vulnerability is optimal.
3. **High-Vulnerability Intensive Area:** When β is sufficiently high. Since the effect of deterring the threat itself is high, aggressive investment even in assets with high vulnerability is justified.

Based on the hypothesis that the publication of ⋆s in METI's new system has a deterrence effect (signaling effect) on attackers, we adopt this framework of the Matsuura model (fluctuation of threat occurrence probability due to investment) as a basis.

4. Proposed Model

This section presents the proposed model, which extends the Matsuura model detailed in the previous chapter by incorporating the effects of METI's new system.

4.1. Model Equation

Following the GL and Matsuura models, we formulate corporate security investment behavior as a maximization problem of the Expected Net Benefit of Information Security (ENBIS)[2]. Equation (9) shows the overall model.

$$ENBIS(z) = \underbrace{[\lambda vt - \lambda S(z,v)T(z,t)]}_{\text{Security Benefit}} + \underbrace{[\pi\{n(z,\theta) - n(0,\theta)\}]}_{\text{Business Benefit}} - z \rightarrow \max. \tag{9}$$

The first term on the right-hand side represents the "reduction in expected security losses due to investment (Security Benefit)," the second term represents the "expected operating profit from increased transaction opportunities associated with compliance with the METI's new system (Business Benefit)," and the third term is the investment amount z.

4.1.1. Security Benefit Function

For the security benefit in the first term, the vulnerability reduction function $S(z, v)$ follows Class II of the GL model, defined by Equation (10).

$$S(z,v) = v^{\alpha z+1} \tag{10}$$

In the original Matsuura model, continuous threat reduction ($t^{\beta z+1}$) is primarily driven by technical friction encountered *during* the attack execution phase. For instance, robust firewalls, rate-limiting, or Proof-of-Work (PoW) mechanisms act as physical "watchdogs" that force attackers to abandon their efforts after initial contact. However, this assumes the attacker has already selected the firm as a potential target.

METI's new system introduces a distinct, earlier phase of deterrence operating at the target selection (reconnaissance) phase. By registering and publishing the ⋆ rank in a public ledger, the system resolves information asymmetry before any attack is launched. Attackers conducting Open-Source Intelligence (OSINT) or automated target screening can observe a high-rank label and preemptively exclude the firm from their target list due to anticipated difficulty.

To mathematically distinguish this ex-ante signaling effect from the ex-post technical friction, we introduce the discrete "signaling effect function" $D(z)$. The invisible internal organizational investment

[2]While expressing the objective function as a maximization of differences containing initial expected loss constants (like λvt) might seem unconventional from a strict marginal cost-benefit perspective, we follow the original Gordon-Loeb notation to maintain literature continuity.

z does not deter attackers until it crosses the threshold τ_i and is translated into a public certification. Thus, the extended function $T(z,t)$ elegantly captures a two-stage deterrence mechanism: $D(z)$ filters out attackers at the macroscopic target-screening phase based on public signals, while $t^{\beta z+1}$ reduces the threat from attackers who proceed to the microscopic probing phase and encounter actual technical investments.

$$T(z,t) = D(z)t^{\beta z+1} \tag{11}$$

Let $D(z)$ be the "signaling effect function" according to the ⋆ acquisition status, defined as a step function in Equation (12). Note that τ_i is the minimum investment amount (threshold) required to acquire $\star i$, satisfying the relationship $0 = \tau_0 < \tau_3 < \tau_4 < \tau_5$.

$$D(z) = \begin{cases} 1(= d_0) & (\tau_0 \le z < \tau_3) \\ d_3 & (\tau_3 \le z < \tau_4) \\ d_4 & (\tau_4 \le z < \tau_5) \\ d_5 & (z \ge \tau_5) \end{cases} \qquad (1 > d_3 > d_4 > d_5 > 0) \tag{12}$$

4.1.2. Business Benefit Function

In the second term of Equation (9), π is the expected profit per transaction, and $n(z,\theta)$ is the "transaction opportunity function" dependent on an investment amount z and a system adoption rate θ ($0 \le \theta \le 1$). We model the special network externalities unique to METI's new system—where unprepared companies are excluded from the market as the system spreads, while ⋆-holding companies gain access to new markets—using the weighted average form in Equation (13).

$$n(z,\theta) = \begin{cases} N_{base}(1-\theta) + \theta N_0 & (\tau_0 \le z < \tau_3) \\ N_{base}(1-\theta) + \theta N_3 & (\tau_3 \le z < \tau_4) \\ N_{base}(1-\theta) + \theta N_4 & (\tau_4 \le z < \tau_5) \\ N_{base}(1-\theta) + \theta N_5 & (z \ge \tau_5) \end{cases} \tag{13}$$

Here, N_{base} is the baseline number of transaction opportunities in the pre-system state ($\theta = 0$), and N_i is the maximum number of transaction opportunities a company holding $\star i$ can obtain in a market where the system has fully permeated ($\theta = 1$). We assume $N_0 = 0$ (companies without ⋆ cannot trade in the system-compliant market) and $0 < N_{base} \le N_3 < N_4 < N_5$.

Calculating the "increment of Business Benefit" based on Equation (13) compared to the case of no investment ($z = 0$, ⋆0) leads to Equation (14). Note that $n(0,\theta)$ corresponds to the first row (⋆0) of Equation (13).

$$\begin{aligned} \text{Business Benefit} &= \pi\{n(z,\theta) - n(0,\theta)\} \\ &= \pi[\{N_{base}(1-\theta) + \theta N_i\} - \{N_{base}(1-\theta) + \theta N_0\}] \\ &= \pi\theta(N_i - N_0) \\ &= \pi N_i \theta \quad (\because N_0 = 0) \end{aligned} \tag{14}$$

Equation (14) shows that the business merit of acquiring $\star i$ is proportional to the product of the system adoption rate θ and the market size N_i.

4.2. Derivation of ⋆-Conditional Local Optima

The objective function of the proposed model, Equation (9), is a discontinuous function containing stepwise parameters ($D(z)$ and $n(z,\theta)$) according to the ⋆ level. Therefore, directly deriving the global optimal solution through a uniform differentiation operation is difficult. Thus, we derive the local optimal solution z_i^* within each interval, assuming the company has selected a specific ⋆ ($\star i$).

Within the interval of a specific $\star i$ ($\tau_i \leq z < \tau_{i+1}$), $D(z)$ and $n(z, \theta)$ are constants. Therefore, the Expected Net Benefit $ENBIS_i(z)$ within this interval can be described as a continuous and differentiable function as in Equation (15).

$$\begin{aligned} ENBIS_i(z) &= [\lambda v t - \lambda v^{\alpha z+1} d_i t^{\beta z+1}] + \pi N_i \theta - z \\ &= \lambda v t \{1 - d_i (v^{\alpha} t^{\beta})^z\} + \pi N_i \theta - z \end{aligned} \tag{15}$$

Let $K := v^{\alpha} t^{\beta}$. Since $0 < v < 1$, $0 < t < 1$, $\alpha > 0$, and $\beta > 0$, it holds that $0 < K < 1$. Defining a positive constant $M := -\ln K > 0$ for computational convenience, differentiating Equation (15) with respect to z yields:

$$\frac{dENBIS_i(z)}{dz} = -\lambda v t d_i K^z (\ln K) - 1 = A_i K^z M - 1 \tag{16}$$

where $A_i = \lambda v t d_i$.

Let $\hat{z}_i$ be the theoretical local maximum point (unconstrained optimal solution) without considering interval constraints. Since $\hat{z}_i$ satisfies the first-order condition $\frac{dENBIS_i(\hat{z}_i)}{dz} = 0$, we derive it as follows:

$$\begin{aligned} A_i K^{\hat{z}_i} M = 1 \Leftrightarrow K^{\hat{z}_i} &= \frac{1}{A_i M} \\ \Leftrightarrow \hat{z}_i \ln K &= -\ln(A_i M) \\ \Leftrightarrow \hat{z}_i (-M) &= -\ln(A_i M) \\ \Leftrightarrow \hat{z}_i &= \frac{\ln(\lambda v t \cdot d_i \cdot M)}{M} \end{aligned} \tag{17}$$

In Equation (17), $\hat{z}_i$ is a logarithmically increasing function of d_i. From the model preconditions $d_0 > d_3 > d_4 > d_5$ (as the $\star$ increases, the deterrence effect increases and the coefficient d_i becomes smaller), the following magnitude relationship holds for the theoretical optimal investment amounts at each $\star$:

$$\hat{z}_0 > \hat{z}_3 > \hat{z}_4 > \hat{z}_5 \tag{18}$$

The actual local optimal solution z_i^* is classified into the following three cases, determined by whether the theoretical value $\hat{z}_i$ falls within the definition domain $[\tau_i, \tau_{i+1})$ of the corresponding $\star$.

Case I (Corner Solution): When $\hat{z}_i < \tau_i$

Within the interval, the marginal net benefit is always negative (marginal benefit < marginal cost), making $ENBIS_i(z)$ a monotonically decreasing function. Therefore, the local optimal solution is the lower bound (boundary point) of the interval.

$$z_i^* = \tau_i$$

Case II (Interior Solution): When $\tau_i \leq \hat{z}_i < \tau_{i+1}$

Since the theoretical optimal value exists within the interval, that point directly becomes the local optimal solution.

$$z_i^* = \hat{z}_i$$

Case III (Upper-bound solution): When $\hat{z}_i \geq \tau_{i+1}$

Within the interval, the marginal net benefit is always positive, making $ENBIS_i(z)$ a monotonically increasing function. In this case, since it is rational to acquire a higher $\star$, the solution within this interval becomes the upper bound (effectively implying a transition to the next $\star$).

$$z_i^* \to \tau_{i+1}$$

Here, we introduce an assumption based on the GLLZ model [7]. They pointed out that corporate voluntary investment (private optimum) tends to be less than the socially desirable investment (social optimum). Since METI's new system aims to correct this under-investment, assuming that the minimum investment level required by the system (τ_3) is set higher than the firm's voluntary investment amount in the absence of the system ($\hat{z_0}$) is natural. Thus, we posit the following assumption:

$$\tau_3 > \hat{z_0} \tag{19}$$

Using this assumption and the relationship in Equation (18), we determine the local optimal solutions[3] as follows:

First, for ⋆0, since $\hat{z_0} < \tau_3$, the interior solution is optimal.

$$z_0^* = \hat{z_0} \tag{20}$$

For Ranked cases (⋆3, 4, 5), since $\hat{z_i} < \hat{z_0} < \tau_3 \leq \tau_i$, the theoretical optimum is always below the threshold. This corresponds to the Corner Solution (Case I), so the local optimal solution is the lower limit (threshold) of each ⋆.

$$z_i^* = \tau_i \quad (i = 3, 4, 5) \tag{21}$$

5. Theoretical Analysis

In this section, to answer whether the introduction of the system induces security investment by supply chain companies, we find the system adoption rate θ (jump condition) where acquiring a ⋆ becomes economically rational.

5.1. Jump Condition from No-⋆ to ⋆3

5.1.1. Derivation

The condition for a company to prefer acquiring ⋆3 over maintaining the status quo (No-⋆) is expressed by the following inequality:

$$ENBIS(z_3^*) > ENBIS(z_0^*) \tag{22}$$

Expanding each term based on Equations (15), (20), and (21) yields:

$$\underbrace{\lambda v t\{1 - d_3(v^\alpha t^\beta)^{\tau_3}\}}_{B_3^{\text{sec}}} + \pi N_3 \theta - \tau_3 > \underbrace{\lambda v t\{1 - (v^\alpha t^\beta)^{\hat{z_0}}\}}_{B_0^{\text{sec}}} - \hat{z_0} \tag{23}$$

Here, B_3^{sec} and B_0^{sec} represent the "reduction in expected security losses" upon acquiring ⋆3 and when not acquired, respectively. Rearranging leads to the jump condition (critical mass) $\theta_{0\to3}$:

$$\theta > \frac{(\tau_3 - \hat{z_0}) - (B_3^{\text{sec}} - B_0^{\text{sec}})}{\pi N_3} =: \theta_{0\to3} \tag{24}$$

5.1.2. Discussion

From the structure of Equation (24), we obtain the following insights regarding corporate investment behavior in the initial stage of system diffusion.

First, the numerator represents the "net additional burden" (investment cost increment minus security benefit increment). The smaller this value, the smaller $\theta_{0\to3}$ becomes, promoting early transition.

[3] As long as the vulnerability reduction function $S(z, v)$ satisfies the standard conditions of the Gordon-Loeb model (i.e., monotonically decreasing and strictly convex), the marginal benefit of investment is strictly diminishing. Under the assumption in Equation (19), the theoretical interior optimum inevitably falls below the compliance threshold ($\hat{z_i} < \tau_i$). Consequently, the local optimal strategy within each tier is mathematically forced to the corner solution (τ_i), regardless of the specific functional class of $S(z, v)$.

From a policy perspective, lowering τ_3 through subsidies directly reduces this numerator. Second, the denominator represents the "system-compliant market size (N_3)." The larger this value—that is, the more ⋆3 becomes a mandatory requirement in public procurement and critical infrastructure transactions—the smaller $\theta_{0\to3}$ becomes. This suggests that the transition to ⋆3 is an "investment for survival" to avoid market exclusion, and diffusion will proceed relatively easily if an appropriate market scale is secured.

5.2. Jump Condition from ⋆3 to ⋆4

5.2.1. Derivation

Similarly to Section 5.1.1, we derive the jump condition $\theta_{3\to4}$ for a company to transition from ⋆3 to the higher ⋆4 as follows:

$$\theta > \frac{(\tau_4 - \tau_3) - (B_4^{\text{sec}} - B_3^{\text{sec}})}{\pi(N_4 - N_3)} =: \theta_{3\to4} \tag{25}$$

where

$$B_4^{\text{sec}} = \lambda v t\{1 - d_4(v^{\alpha} t^{\beta})^{\tau_4}\} \tag{26}$$

We derive the jump condition from ⋆4 to ⋆5 similarly.

5.2.2. Discussion considering comparison with $\theta_{0\to3}$

Equation (25) differs decisively from Equation (24) in its economic structure.

First is the "net additional burden" in the numerator. Since ⋆4 assumes third-party certification, τ_4 may increase significantly compared to the self-declaration-based ⋆3 due to transaction costs such as certification fees and audit responses. This causes the numerator to bloat, raising the hurdle for transition.

Second, the more essential difference lies in the "business incentive" of the denominator. While the denominator of Equation (24) was the entire market (N_3), the denominator of Equation (25) is the "market increment ($N_4 - N_3$)." This means that the transition from ⋆3 to ⋆4 is not "survival" but "investment for growth."

This structural difference suggests a significant risk in institutional design. If $N_4 \approx N_3$, that is, if the addressable market does not expand much even if a higher ⋆ is acquired, the denominator approaches zero, and the jump condition $\theta_{3\to4}$ diverges to infinity. This mathematically corroborates the risk that unless a clear market advantage (differential) is secured for higher ⋆s, companies will continue to stay at ⋆3 and stagnation where sophistication does not progress will occur.

6. Numerical Analysis

In this section, based on the theoretical model derived in the previous chapter, we visualize the transformation of corporate investment behavior in response to changes in the system adoption rate θ by performing numerical simulation. We also analyze how the jump conditions for each ⋆ behave in response to parameter fluctuations.

6.1. Simulation Setup

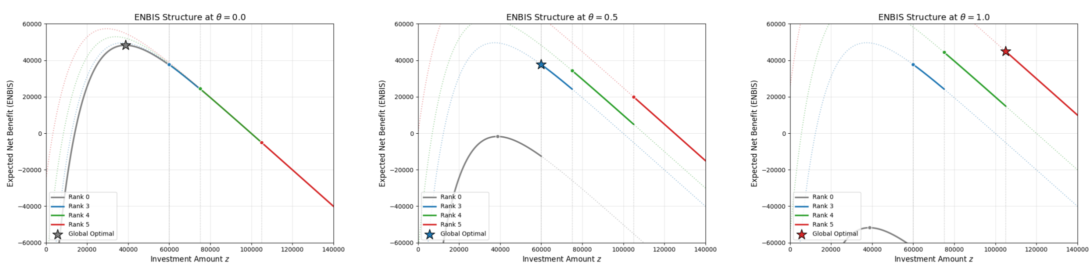
Table 1 shows the parameter settings used for the simulation. For basic parameters $(\lambda, v, t, \alpha, \beta)$, we followed the settings of preceding studies, the Gordon-Loeb model [3] and the Matsuura model [12]. For system-specific parameters (τ_i, d_i, N_i), we used values calibrated so that the economic rationality of each ⋆ competes while satisfying the assumption that companies do not voluntarily invest to meet system standards in the normal state ($\hat{z}_0 < \tau_3$).

Table 1. Parameters for Simulation

Parameter	Symbol	Value
Potential Loss	λ	1,000,000
Initial Vulnerability	v	0.5
Initial Threat	t	0.5
Vuln. Reduction Eff.	α	1.0×10^{-4}
Threat Reduction Eff.	β	1.0×10^{-5}
Profit per Transaction	π	1,000
Base Market Size	N_{base}	100
Threshold Cost (★3)	τ_3	60,000
Threshold Cost (★4)	τ_4	75,000
Threshold Cost (★5)	τ_5	105,000
Deterrence Factor (★3)	d_3	0.9
Deterrence Factor (★4)	d_4	0.7
Deterrence Factor (★5)	d_5	0.5
Market Size (★3)	N_3	100
Market Size (★4)	N_4	120
Market Size (★5)	N_5	150

6.2. Structure of ENBIS Function

Before observing the comparative-static changes in simulation, we confirm the structural characteristics of the Expected Net Benefit $ENBIS(z)$ with respect to investment amount z. Figure 3 shows the shape of $ENBIS(z)$ and the optimal investment amount when the system adoption rate θ is fixed at $0, 0.5$, and 1.0.



(a) $\theta = 0$ (b) $\theta = 0.5$ (c) $\theta = 1.0$

Fig. 3. Structural Transition of ENBIS Function and Global Optimal Investment

In the figures, solid lines represent the effective domain selectable for each ★ ($\tau_i \le z < \tau_{i+1}$), and thin dotted lines represent virtual regions outside of that. From these figures, we confirm the following structural characteristics of this model:

1. **Discontinuous Jump:** At the rank thresholds τ_i, the ENBIS curve shows an upward discontinuous jump due to the improvement of the deterrence effect coefficient $D(z)$ and the expansion of market access.

2. **Nature of Local Optimal Solutions:** For ★0 (gray), a local maximum exists within the interval, which becomes the voluntary optimal investment amount $\hat{z}_0$ (Case II: Interior Solution). On the other hand, for Ranked cases (★3, 4, 5), since the theoretical optimal value is located before the threshold ($\hat{z}_i < \tau_i$), the local optimal solution always sticks to the left edge of the interval (threshold τ_i) (Case I: Corner Solution).

3. **Change in Dominance:** At $\theta = 0$ (Fig. a), $\hat{z}_0$ is at the highest position, but as θ increases, network externalities work to push up the solid line parts of higher $\star$s. At $\theta = 1.0$ (Fig. c), the starting point of the most expensive $\star 5$ changes to the optimal investment amount.

6.3. Optimal Investment Strategy Transition

We continuously track the structural changes confirmed in the previous section with the system adoption rate θ on the horizontal axis. Figure 4 shows the transition of Expected Net Benefit (ENBIS) when selecting each $\star$, and Figure 5 shows the transition of the resulting optimal investment amount z^*.

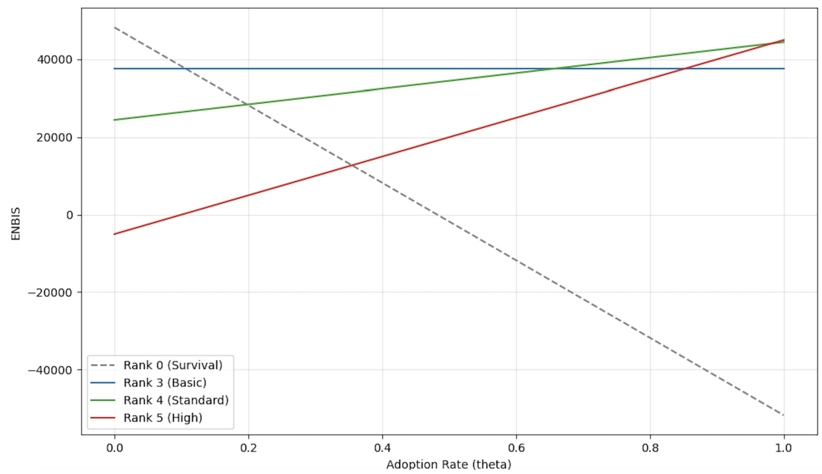


Fig. 4. Competition of Expected Net Benefit (ENBIS) among Ranks

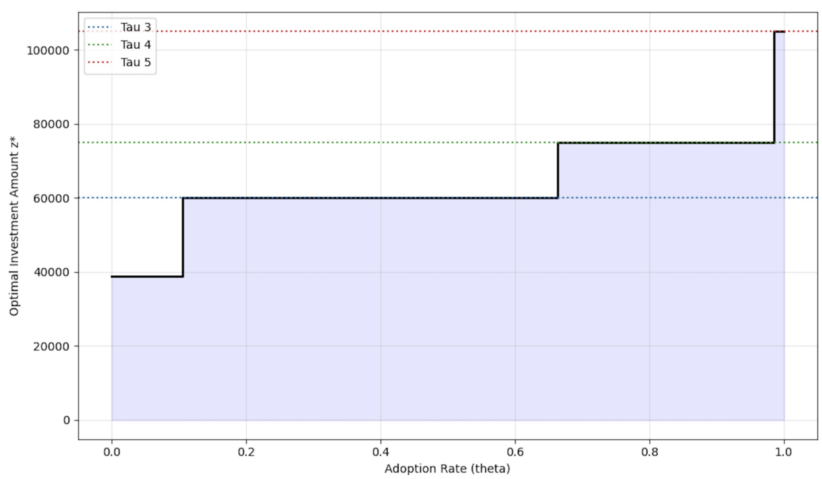


Fig. 5. Transition of Optimal Investment Strategy with respect to Adoption Rate θ

Figure 4 visualizes the competitive relationship of economic advantage among $\star$s accompanying system diffusion. While the benefit of no measures ($\star 0$) decreases due to market exclusion (dashed line), the benefits of Ranked cases (solid lines) increase, and the order reverses at specific intersection points (critical masses).

This reversal phenomenon appears as stepwise investment behavior in Figure 5, and we confirm the following three phase transitions:

1. **Observation Phase ($0 \leq \theta < \theta^*_{0\to3}$):** In the early stage of diffusion, the benefit of ⋆0 is still the largest (corresponding to Fig. 3a), and companies maintain the voluntary optimal investment amount $\hat{z}_0$ that does not meet system standards.

2. **First Jump (Transition to ⋆3):** Around $\theta \approx 0.11$, the benefit curve of ⋆3 exceeds that of ⋆0 (corresponding to Fig. 3b). This is the branching point where the loss due to market exclusion exceeds the system compliance cost, and the company raises its investment amount to τ_3 for the purpose of "survival."

3. **Second & Third Jumps (Transition to ⋆4, 5):** As diffusion progresses further ($\theta \approx 0.66, 0.98$), the benefit curves of ⋆4 and 5, which have higher market access rights, successively take the lead (corresponding to Fig. 3c). This implies a shift to "growth" where companies make additional investments in search of larger market opportunities.

These results suggest that this system induces "stepwise investment behavior" bordered by critical masses rather than continuous investment increases, representing an ideal scenario where the incentive structure of each ⋆ in the institutional design is functioning appropriately.

6.4. Potential Failure Scenarios

The previous section presented a scenario where the system functions ideally. However, if parameter settings are inappropriate, the system may not follow the expected diffusion curve. We show the consequences for ENBIS competition and investment behavior for two representative "failure scenarios" observed in this model.

Case A: Kick-off Failure

Case A is a case where the acquisition cost τ_i for each ⋆ is set excessively high (uniformly $+100,000$ relative to the base values in Table 1).

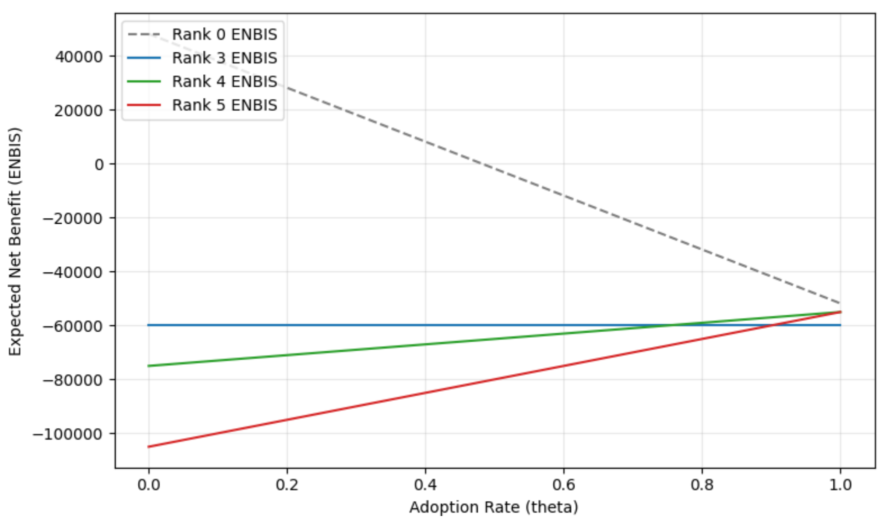


Fig. 6. Case A: ENBIS Competition

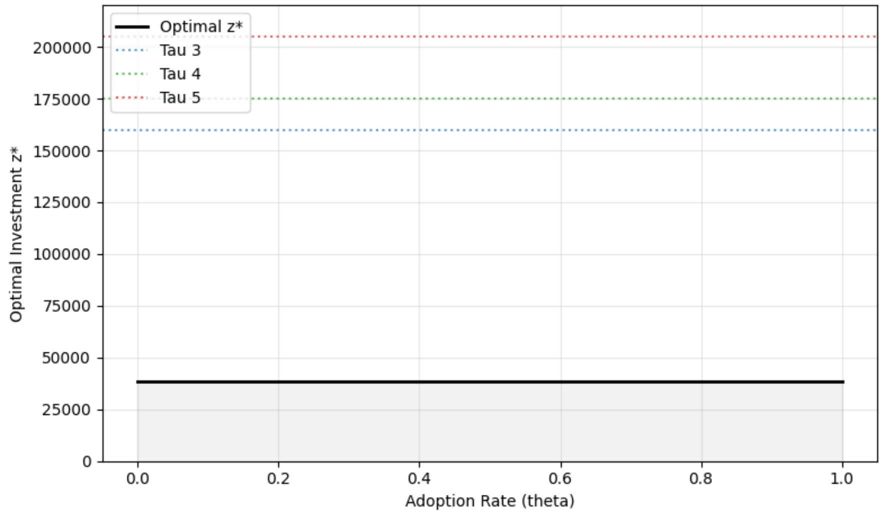


Fig. 7. Case A: Optimal Investment Strategy

Referring to Figure 6, we confirm that the Expected Net Benefit of all Ranked cases (solid lines) is always below that of the status quo ★0 (dashed line). As a result, as shown in Figure 7, even if the system adoption rate θ reaches 1, companies do not enter, and the investment amount remains at the voluntary low level ($\hat{z}_0$).

Case B: Stagnation

Case B is a case where τ_3 was lowered ($\tau_3 = 50,000$) to promote entry into ★3, but the market merits of higher ★s were left unchanged.

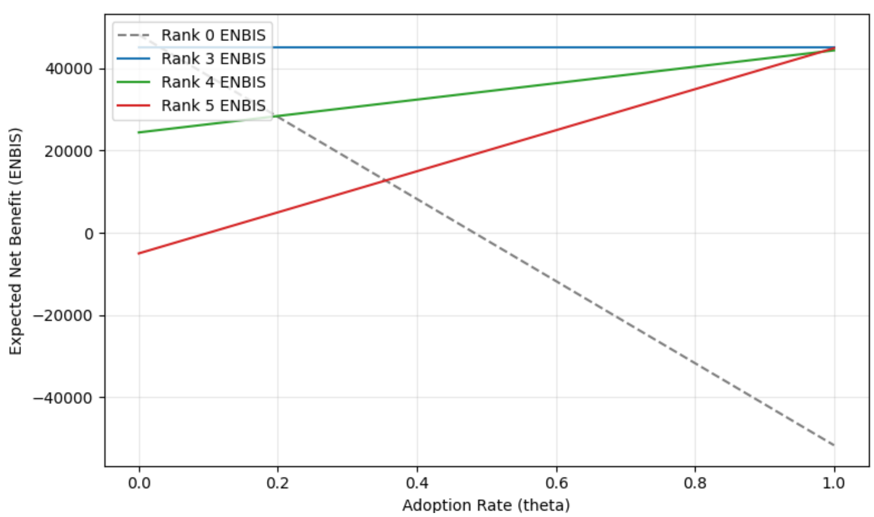


Fig. 8. Case B: ENBIS Competition

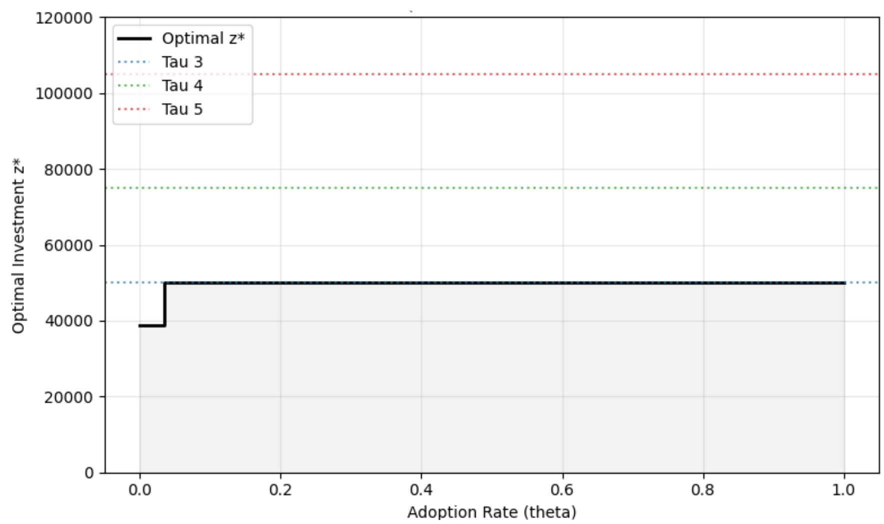


Fig. 9. Case B: Optimal Investment Strategy

Looking at Figure 8, ⋆3 (blue line) exceeds ⋆0 (dotted line) early due to the decrease in τ_3. However, since the transition cost difference to ⋆4 ($\tau_4 - \tau_3$) has relatively expanded, there is no intersection where ⋆4 (green line) overtakes ⋆3. Therefore, as shown in Figure 9, although companies enter ⋆3, they have no incentive to transition higher. Corporate investment behavior completely stagnates at ⋆3, plunging the system into the aforementioned checkbox compliance trap.

In the next chapter, we will discuss generally under what conditions these failures occur through sensitivity analysis.

7. Sensitivity Analysis and Discussion

In this chapter, we generalize and discuss under what mechanisms and conditions the phenomena observed in the previous chapter's simulations (success scenario and failure scenarios Case A, B) occur, through sensitivity analysis.

7.1. Incentives for Market Entry (⋆0 → 3)

First, we examine the conditions for companies to break away from the status quo (⋆0) and enter ⋆3, the gateway to the system. As mentioned earlier, investment in this phase has the nature of "investment for survival" to avoid exclusion from the system-compliant market.

Figure 10 shows the sensitivity analysis results (Map A) of the critical mass $\theta^*_{0\to3}$ when the cost threshold τ_3 required to acquire ⋆3 (Basic) and the size of the system-compliant market N_3 are varied over a wide range.

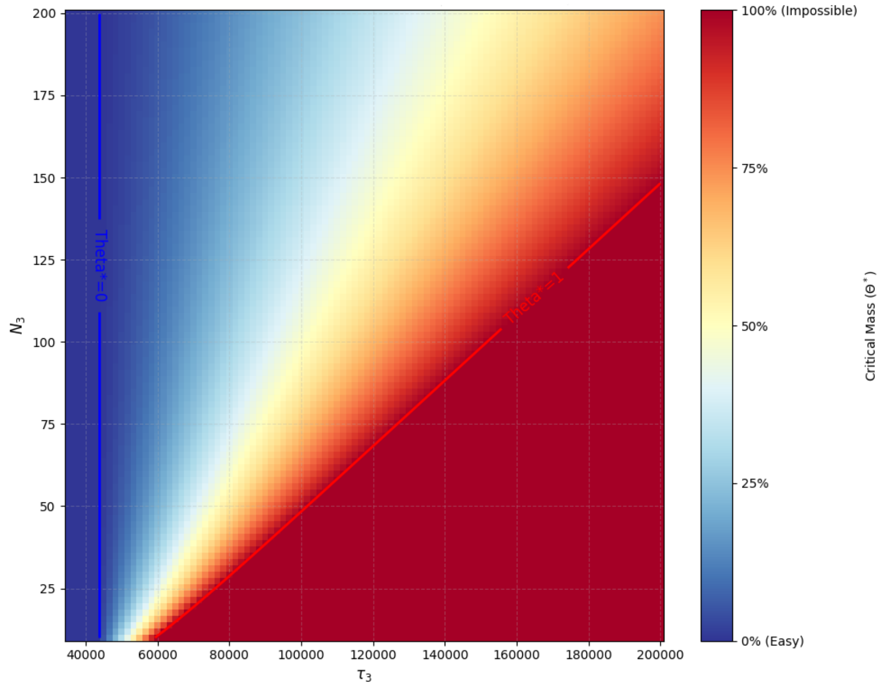


Fig. 10. Map A : Sensitivity Analysis of ⋆0 → 3 Jump

The blue region in the figure indicates $\theta^* \leq 0$ (immediate diffusion), and the red region indicates $\theta^* \geq 1$ (impossible diffusion). From this result, we obtain the following important implications regarding the initial diffusion of the system.

First, we observe the existence of the "market failure" region. On the right side of the figure (region where τ_3 is high) and the lower side (region where N_3 is extremely small), there is a wide red area. Case A (Kick-off Failure) shown in the previous chapter can be interpreted as an instance where the coordinates moved to the right due to a uniform increase in costs, entering this "market failure" region. In this region, since the system compliance cost is excessive for SMEs or the referable market is insufficient, maintaining the status quo continues to be selected as a rational judgment of individual companies, and the system never launches.

Second, a trade-off exists between cost and market, highlighting the effectiveness of a policy mix. The boundary line between the blue and red regions describes a curve going from upper left to lower right. This means that to satisfy the conditions necessary for diffusion, either "reduction of cost τ_3 (move left)" or "expansion of market size N_3 (move up)," or both, must function. In particular, to guide the group of companies in a high-cost state like Case A (right side of the figure) to the blue region, merely expanding the market (moving up) may not be sufficient, and intervention to physically lower the cost (moving left) through subsidies or the like becomes essential.

Therefore, to ensure the initial diffusion of the system (0 → 3), we conclude that a policy mix combining the reduction of entry barriers through subsidies and the securing of a minimum market through mandatory requirements in public procurement is effective.

7.2. The Barrier of Marginal Incentive (⋆3 → 4)

Next, we consider the transition conditions from ⋆3 to ⋆4. Unlike ⋆0 → 3, this transition is an **"Investment for Growth"** seeking larger market opportunities. Figure 11 shows the sensitivity analysis results (Map B) with additional cost ($\Delta\tau$) on the horizontal axis and additional market size (ΔN) on the vertical axis.

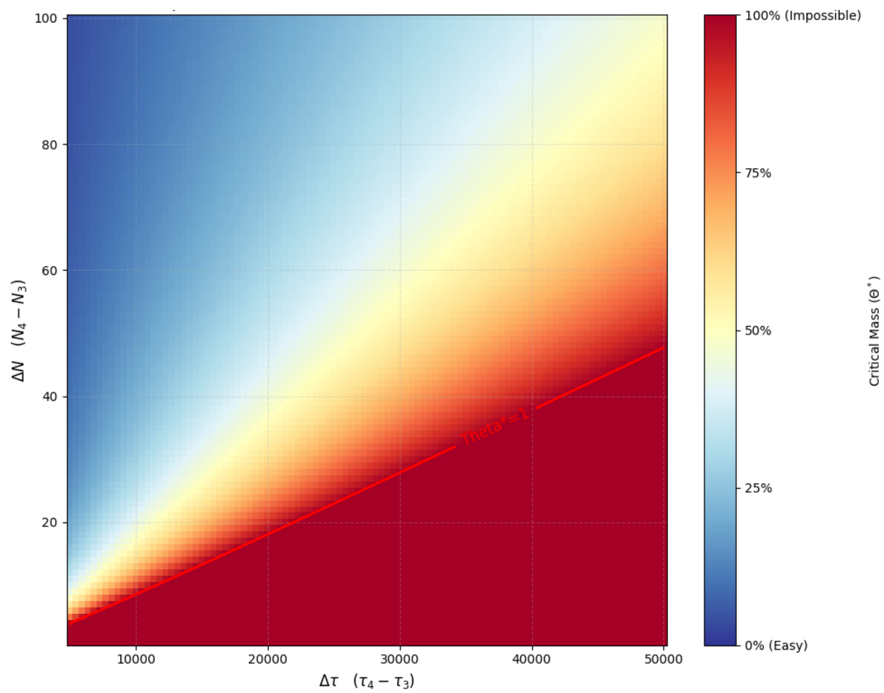


Fig. 11. Map B : Sensitivity Analysis of ⋆3 ⟶ 4 Jump

The shape of the figure is similar to Map A, with an impossible diffusion region (red) spreading in the lower right (high additional cost, low additional market). However, even if the shapes are similar, there is a difference in the difficulty of realization.

While N_3 in the previous section referred to the "entire" system-compliant market, the vertical axis ΔN in this section is strictly the market "increment." Escaping from the lower side (red region) in the figure requires movement in the Y-axis direction (securing ΔN), but adding a "new market where trading is impossible without ⋆4" on top of existing business partners N_3 is structurally not easy.

Notably, in this red region (state where ΔN is small), even if the additional cost $\Delta\tau$ is reduced (moving the X-axis to the left), it is difficult to reach the blue region. This suggests that in guiding to higher ⋆s, mere subsidy policies (cost reduction) have limits, and it is essential to institutionally secure ΔN serving as the denominator by strategically creating markets that require higher ⋆s.

7.3. Policy Interaction and "Checkbox Compliance Trap"

Finally, we analyze the "policy interaction" where support measures for lower ⋆s affect the transition to higher ⋆s. Figure 12 shows the sensitivity analysis results (Map C) with ⋆3 acquisition cost τ_3 on the horizontal axis and ⋆4 market size N_4 on the vertical axis.

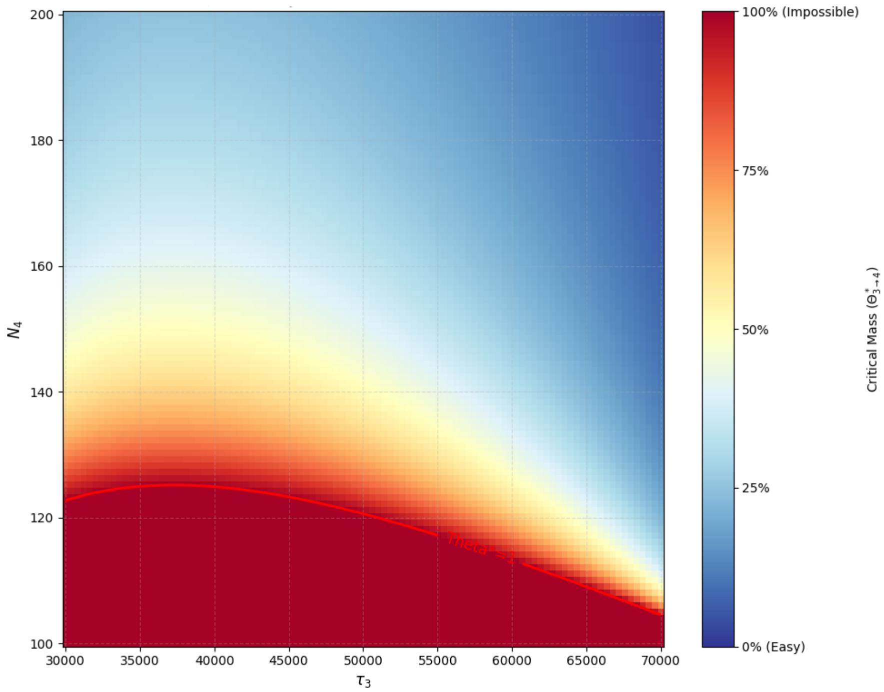


Fig. 12. Policy Interaction and Checkbox Compliance Trap (Map C)

The lower-left region (red) in the figure indicates a phenomenon where, despite the light cost burden for ⋆3 (small τ_3), the transition to ⋆4 does not occur. This result, which seems counterintuitive at first glance, stems from changes in the "relative cost difference" between ⋆s.

Case B (Stagnation) in the previous chapter was caused precisely by this mechanism. In the simulation, the operation of lowering τ_3 to promote entry corresponds to moving the X-axis to the left on Map C. As is clear from the figure, if a movement to the left is made in a situation where the market size N_4 is not sufficiently large (lower side of the figure), one crosses the boundary from the blue region (autonomous diffusion) to the red region (Checkbox Compliance).

This is because the cost-effectiveness of ⋆3 became excessively high due to the decrease in τ_3, and the hurdle of additional cost ($\Delta\tau = \tau_4 - \tau_3$) to transition to ⋆4 relatively rose (assuming τ_4 is constant). As a result, if the additional market merit ($N_4 - N_3$) obtained by ⋆4 cannot justify this expanded cost difference, companies choose to settle for ⋆3, which has extremely good cost-performance.

This result suggests the risk that excessive subsidy policies for ⋆3 intended to expand the base ($0 \longrightarrow 3$) may reinforce companies' status quo bias and cause stagnation that hinders the transition to advanced security measures, which should be the ultimate goal. Therefore, in institutional design, delicate incentive design is required not only to lower entry barriers but also to maintain the "step height (cost difference and merit difference)" between ⋆s in an appropriate balance.

7.4. Applicability and Limitations of the Proposed Model

While this study primarily analyzes incentive-driven diffusion dependent on market adoption (θ), the proposed framework can be broadly applied to other institutional designs. For instance, in mandatory regimes like the EU Cyber Resilience Act (CRA), where certification is legally required, the model can be adapted by simply introducing an expected legal penalty term to the non-compliance state (⋆0). Conceptually, while a massive penalty effectively forces initial entry (overcoming the baseline barrier regardless of θ), it does not inherently provide business incentives for higher-tier growth. Thus, without careful market design, mandatory regimes remain equally vulnerable to the checkbox compliance trap at the minimum mandated tier.

However, the proposed model and analysis contain several limitations, which present opportunities for future extensions.

First, regarding the impact of subsidies: the decrease in τ_i in this model implies a "decrease in security defense level accompanying the decrease in investment amount" in the formula. However, "subsidies" as an actual policy reduce only the net burden on companies while maintaining a high defense level. Therefore, the investment inducement effect of actual subsidy policies is considered to be more powerful than the results of this simulation. The results of this study should be interpreted as a baseline that conservatively estimates the effect of subsidies.

Second, regarding the assumption of homogeneous firms: the current model focuses on the micro-level decision-making of a representative firm facing exogenous market adoption rates (θ). In reality, optimal investment levels differ across firms depending on their heterogeneous characteristics, such as potential loss λ and initial vulnerability v. While our framework can individually derive the critical mass for firms with different characteristics, it does not aggregate these diverse decisions into a macro-level general equilibrium. Simulating how heterogeneous firms coexist and endogenously determine θ is a crucial next step.

Finally, regarding the temporal scope: the proposed model is a static, single-period model evaluating decisions from a zero-basis (status quo). While highly effective at analyzing pre-launch critical masses, it fails to fully capture post-launch sequential decision-making. In reality, a company already operating at $\star 3$ must decide whether to upgrade to $\star 4$. This requires introducing an investment reusability parameter ($\rho \in [0, 1]$), denoting how much of the initial τ_3 investment (e.g., audit evidence) can be reused for $\star 4$. Under a low reusability regime, the marginal cost of upgrading becomes $\tau_4 - \rho\tau_3$, creating massive post-launch friction and leading to severe post-launch stagnation.

8. Conclusion and Future Work

8.1. Conclusion

In this study, to analyze the impact of the introduction of the new supply chain security assessment system formulated by the Ministry of Economy, Trade and Industry on corporate investment behavior, we proposed a mathematical model extending the conventional GL model and Matsuura model. The proposed model incorporates the stepwise rank structure unique to the system and network externalities where transaction opportunities fluctuate according to the system adoption rate, quantitatively deriving the jump conditions (critical mass) for companies to change their investment behavior from the status quo to $\star 3$, and further to $\star 4$.

Through analysis via numerical simulation, we obtained the following important findings. First, in the initial stage of system diffusion, autonomous investment behavior cannot be expected, and the creation of initial demand through public procurement is essential. Second, there is a risk that excessive support measures (subsidies, etc.) to lower the barrier to entry for $\star 3$ (Basic) may relatively diminish the incentive to transition to $\star 4$ (Standard). This policy imbalance can cause severe stagnation, trapping corporate investment behavior at lower $\star$s in a state of checkbox compliance. This result suggests that to promote the transition to higher $\star$s, clear differentiation of market merits between $\star$s, such as strategically creating markets accessible only to companies acquiring higher $\star$s, is indispensable, not just cost support.

The scope of application of the "discrete extension model" proposed in this study is not limited to METI's new system in Japan. Attempts to visualize security measure status with stepwise ranks or labels, such as CMMC 2.0 imposed by the US Department of Defense as a procurement requirement and the UK's Cyber Essentials, are becoming a global trend. This model is expected to function as a general-purpose theoretical framework for analyzing the optimal incentive structure in any institutional design that forces these "discontinuous investment decisions."

8.2. Future Work

8.2.1. Endogenization of Attacker Behavior

In this model, the deterrence effect (d_i) was an exogenous constant. However, as the system spreads, attackers may shift targets. Conversely, acquiring the highest rank ($\star 5$) may signal that the firm holds highly valuable assets, paradoxically attracting Advanced Persistent Threats (APTs) and reversing the deterrence effect ($d_5 > d_4$). Future extensions must capture this signaling inversion within a game theory framework.

8.2.2. Complex Supply Chain Topology and Peer Observability

We abstracted the supply chain as a uniform market size N. Actual supply chains possess complex network topologies. Furthermore, the public nature of the registry ensures peer observability, where vendors know their competitors' and suppliers' scores. This enables cascading requirements and signaling competition. Future models will introduce complex network theory to endogenize N and sequential strategic interactions across the supply chain.

8.2.3. Empirical Validation

This system is currently in the introduction phase, and verification using actual data is a future task. After the system operation starts, it is required to collect data such as the actual $\star$ acquisition status of companies and the incident rate by $\star$, calibrate the model parameters (α, β, d_i) and verify the validity of the model.

Acknowledgment

The authors used AI-based tools (Claude and Gemini) for the English translation and editorial refinement of this manuscript. The authors bear full responsibility for all technical content. This work was partially supported by the Designated-Field Research Grant of the SECOM Science and Technology Foundation.

References

1. R. Anderson, "Why information security is hard - an economic perspective," in *Seventeenth Annual Computer Security Applications Conference,* 358–365 (2001).
2. R. Anderson and T. Moore, "The economics of information security," Science **314**, 610–613 (2006).
3. L. A. Gordon and M. P. Loeb, "The economics of information security investment," ACM Trans. Inf. Syst. Secur. **5**, 438–457 (2002).
4. L. Gordon, M. Loeb, and L. Zhou, "Investing in cybersecurity: Insights from the Gordon-Loeb model," J. Inf. Secur. **07**, 49–59 (2016).
5. A. Fedele and C. Roner, "Dangerous games: A literature review on cybersecurity investments," J. Econ. Surv. **36**, 157–187 (2022).
6. Ministry of Economy, Trade and Industry, "Construction policy for the "security assessment system for supply chain reinforcement" (in japanese)," Available at: https://www.meti.go.jp/press/2025/04/20250414002/20250414002-2.pdf (2025). Accessed: 2026-01-25.
7. L. Gordon, M. Loeb, W. Lucyshyn, and L. Zhou, "Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb model," J. Inf. Secur. **06**, 24–30 (2015).
8. J. Willemson, "On the Gordon & Loeb model for information security investment," in *The 5th Workshop on the Economics of Information Security,* (2006).
9. Y. Baryshnikov, "IT security investment and Gordon-Loeb's 1/e rule," in *The 11th Workshop on the Economics of Information Security,* (2012).
10. M. Lelarge, "Coordination in network security games," in *2012 Proceedings IEEE INFOCOM,* 2856–2860 (2012).
11. K. Hausken, "Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability," Inf. Syst. Front. **8**, 338–349 (2006).
12. K. Matsuura, "Productivity space of information security in an extension of the Gordon-Loeb's investment model," in *The 8th Workshop on the Economics of Information Security,* (2009).
13. S. Farrow and J. Szanton, "Cybersecurity investment guidance: Extensions of the Gordon and Loeb model," J. Inf. Secur. **7**, 15–28 (2016).
14. C. D. Huang and R. S. Behara, "Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints," Int. J. Prod. Econ. **141**, 255–268 (2013).

15. U. Cherubini, “Multivariate security breach probability: The Gordon-Loeb model with copulas,” in *Computer Safety, Reliability, and Security. SAFECOMP 2024 Workshops: DECSoS, SASSUR, TOASTS, and WAISE, Florence, Italy, September 17, 2024, Proceedings,* 257–265 (Springer-Verlag, Berlin, Heidelberg, 2024).
16. L. Gordon, M. Loeb, and W. Lucyshyn, “Information security expenditures and real options: A wait-and-see approach,” Comput. Secur. J. **19**, 1–7 (2003).
17. K. Tatsumi and M. Goto, “Optimal timing of information security investment: A real options approach,” in *Economics of Information Security and Privacy,* T. Moore, D. Pym, and C. Ioannidis, eds., 211–228 (Springer US, Boston, MA, 2010).
18. K. Krutilla, A. Alexeev, E. Jardine, and D. Good, “The benefits and costs of cybersecurity risk reduction: A dynamic extension of the Gordon and Loeb model,” Risk Anal. **41**, 1795–1808 (2021).
19. G. Callegaro, C. Hillairet, C. Fontana, and B. Ongarato, “A stochastic Gordon-Loeb model for optimal cybersecurity investment under clustered attacks,” in *arXiv preprint arXiv:2505.01221v1,* (2025).
20. L. A. Gordon, M. P. Loeb, and W. Lucyshyn, “Sharing information on computer systems security: An economic analysis,” J. Account. Public Policy **22**, 461–485 (2003).
21. H. R. Skeoch, “Expanding the Gordon-Loeb model to cyber-insurance,” Comput. Secur. **112**, 102533 (2022).
22. A. Mazzoccoli and M. Naldi, “Robustness of optimal investment decisions in mixed insurance/investment cyber risk management,” Risk Anal. **40**, 550–564 (2020).
23. L. A. Gordon, M. P. Loeb, and L. Zhou, “Integrating cost–benefit analysis into the nist cybersecurity framework via the Gordon–Loeb model,” J. Cybersecur. **6**, tyaa005 (2020).