～世界最強化セキュリティー提案～

【世界初・業界初】物理学的構造セキュリティ理論の発明

件名

ランサムウェア及び高度化サーバー攻撃に対する
物理学的成立制御セキュリティ基盤の研究・実証提案

提出者：竹内　祐樹/平川　智子/坂上　芳洋
理論名称：無数鍵多重時変成立点理論　関連特許：特許第 7780682 号／特許第 7796450 号

Ⅰ．提案の趣旨

① 何の件で

― 国家及び防衛関連システムのセキュリティ強化 ―

本提案は、防衛関連ネットワーク・クラウド基盤・装備管理系・情報システムに対する

- ランサムウェア攻撃
- 権限昇格型侵害
- 横展開攻撃
- API 悪用
- 内部不正
- AI 高度化攻撃

に対し、「侵入後に対応する構造」から「成立そのものを一瞬に限定する構造」へ転換する

新しいセキュリティ基盤の研究・実証を提案するものです。

最初の説明動画：https://youtu.be/lWAGoHLYWzA?si=y30M_gM2-CaI1QIv

理論の基礎説明動画：https://youtu.be/QduPes0OIT0?si=4OEgN7dKuf6VA9l0

複合特許権の説明動画：https://youtu.be/hxV3rdUfklY?si=UmS8HDkI1nQDP3f9

Ⅱ. 背景（現状課題）

1. 従来型セキュリティの限界

縦資料 p1-2 理論　縦の資料に示される通り、

- 固定 ID
- 固定鍵
- セッション継続
- 再利用可能

という前提構造が存在します。

これにより、

- 一度突破されると横展開可能
- 認証突破後は暗号化実行可能
- AI 自動試行が有効
- 内部者権限濫用が成立

という構造的問題が残ります。

Ⅲ. 提案理論の核心

② どの様な内容で

― 物理学的セキュリティの発明 ―

本理論は

固定の正解を作らず、条件が一瞬一致した時だけ成立空間を生成する

という構造を採用します。

■ 成立空間モデル（防衛向け解釈）

成立空間は

- 平常時：存在しない（無効）
- 条件一致時：瞬間生成（有効）
- 正常終了：即消滅（失効）
- 異常挙動：即遮断（遮断状態）

（5 状態モデル：縦資料 p7 理論　縦の資料）

■ 物理学的転換点

1. 固定秘密を持たない
2. 成立はイベントである
3. 成立後は即無効
4. 再試行は累積しない
5. 実行権は用途別に分離

Ⅳ. ランサムウェア対策としての優位

73 攻撃一覧（ランサムウェア項目）より

③特許＋理論有り-完璧想定-73 攻撃-指標一覧-

■ ランサムウェア（暗号化・二重脅迫）

従来モデル値：

- 防御率：約 10%
- 防衛率：約 55.9%
- 被害確率：約 44.1%

複合成立理論モデル：

- 防御率：約 95%
- 防衛率：**99.74999999525%**
- 被害確率：約 0.25000000475%

■ 防衛率

99.7%以上（設計モデル値）

■ 改善倍率

約 **176 倍**

（暗号化型に対する比較モデル）

■ サーバー侵害・横展開

項目 29〜38 より

③特許＋理論有り−完璧想定−73 攻撃−指標一覧−

- 権限昇格
- 横展開
- VPN 悪用
- クラウド設定ミス
- バックアップ破壊

複合防衛率:
99.7%以上

改善倍率:
約 176 倍（主要項目）

■ 資格情報窃取・API 漏洩

改善倍率:
約 3.6 億倍（モデル値）

■ 物理侵害型（参考）

改善倍率最大:
約 6.7 億倍

（物理侵害モデル）

Ⅴ. 戦略的意義

1. ランサム暗号化実行前遮断

暗号化処理に必要な実行権を成立点制御で遮断可能。

2. 横展開無効化

同一鍵の再利用不可。

3. ログ改ざん困難化

成立後即消滅構造。

4. AI 累積試行無効化

試行回数が優位にならない。

5. 多経路通信耐性

災害・通信断前提設計。

Ⅵ. 既存技術との位置づけ

区分	役割
WAF/EDR	検知
ゼロトラスト	常時検証
本理論	成立そのものの瞬間化

本理論は既存対策を否定せず、
上位構造として統合します。

Ⅶ. どの様にしたいのか

③ 国の部署・研究・協会・企業への紹介先

【優先窓口】

■ 防衛装備庁
・防衛技術研究本部
・サイバー防衛関連研究部門

■ 防衛省 情報本部
・サイバー防衛隊関連部署

■ 内閣官房 NISC
（国家インフラ連携）

■ 経済産業省
・商務情報政策局
・IPA（技術評価）

■ JST
（理論研究指定）

Ⅷ. 提案ステップ

1. 概要ブリーフィング（30 分）
2. 技術評価ワーキング
3. 限定環境 PoC（閉域）
4. 数値実証
5. 指針検討

Ⅸ. 要約

本提案は、固定 ID や固定セッションを前提とする従来型認証構造を転換し、成立を一瞬の例外とする物理学的成立制御理論を用いて、ランサムウェア及び高度化サーバー攻撃を構造的に遮断する次世代セキュリティ基盤の研究・実証を求めるものである。設計モデルにおいて、防衛率 99.7%以上、主要攻撃種別において改善倍率 176 倍以上を確認している。

技術説明書

件名

成立点制御に基づく物理学的サイバー防護基盤の研究提案
― ランサムウェア及び高度化サーバー攻撃に対する実行前遮断モデル ―

提出者：竹内　祐樹／平川　智子／坂上　芳洋
理論名称：無数鍵多重時変成立点理論
関連特許：第 7780682 号／第 7796450 号

1. 提案の目的

本提案は、防衛関連情報システムに対する

- ランサムウェア攻撃
- 権限昇格型侵害
- 横展開攻撃
- API 悪用
- 内部者不正
- AI 自動試行攻撃

に対し、

「侵入後検知型」から
「成立前遮断型」への構造転換

を実現する新しい防護基盤の研究・評価を目的とする。

2. 従来モデルの構造的限界

2.1 固定正解モデル

従来セキュリティは以下を前提とする。

- 固定 ID
- 固定パスワード
- 固定トークン
- 継続セッション

この構造では:

- 一度突破すると横展開可能
- 認証後は実行可能
- 試行回数が攻撃側に有利
- AI 学習が有効

2.2 ランサムウェアにおける弱点

ランサムウェアは

侵入
↓
認証突破
↓
暗号化実行
↓
バックアップ破壊
↓
身代金要求

という実行権依存型構造。従来は「検知・隔離・復旧」に依存。

---

3. 提案理論の核心　3.1 成立空間モデル

成立空間は

- 無効（通常）
- 有効（瞬間）
- 継続（条件維持中のみ）
- 失効（終了）
- 遮断（異常時）

という 5 状態遷移モデル。（縦資料 p7 参照 理論 縦の資料）

3.2 物理学的転換

1. 固定秘密を持たない
2. 成立は時間的イベント
3. 成立後即消滅
4. 再利用不可
5. 試行累積無効

---

4. 数理モデル　4.1 成立犯罪率近似

成立率 ≒ 試行回数 ×（1 − 防御率）　改善倍率=（1−防御率_前）/（1−防御率_後）

4.2 通報到達確率

Pnotify = 1 − (1 − p)^(n(1+r))

p：単発到達率
n：チャネル数
r：再送回数

5. ランサムウェア対策性能（設計モデル）

5.1 ランサムウェア（暗号化型）

従来：

- 防御率 10%
- 防衛率 55.9%
- 被害確率 44.1%

本理論：

- 防御率 95%
- 防衛率 **99.74999999525%**
- 被害確率 約 0.25%

防衛率：99.7%以上（設計モデル値） 改善倍率：約 176 倍

5.2 サーバー侵害（横展開含む）

- 脆弱性悪用
- 権限昇格
- 横展開
- バックアップ破壊

防衛率：**99.7%以上** 改善倍率：約 **176 倍**

5.3 資格情報窃取 改善倍率：約 **3.6 億倍（モデル値）**

6. 防衛用途での応用領域

6.1 情報系ネットワーク

- 管理者権限実行前の成立点判定
- API 実行単位の瞬間化

6.2 装備管理系

- 不正操作の成立前遮断
- 異常時即通報

6.3 クラウド・仮想環境

- コンテナ横展開遮断
- 権限再利用防止

---

7. 既存防御との統合

本理論は

- WAF
- EDR
- SIEM
- ゼロトラスト

を否定しない。

これらの上位で

実行権を物理的に瞬間化

する。

---

8. 実証提案（PoC）

Phase1

閉域環境での成立制御実験

Phase2

ランサム模擬環境での暗号化実行遮断検証

Phase3

横展開抑止評価

評価指標

- 実行成功率
- 遮断率
- 初動時間
- 誤検知率
- 運用負荷

---

9. 研究的意義

本理論は

- ゼロトラスト以降の第 5 段階
- 実行権の時間的瞬間化
- AI 累積攻撃耐性
- 多経路通信耐性

を持つ可能性がある。

---

10. 結論

本提案は、

- ランサムウェア暗号化実行前遮断
- 横展開無効化
- 強要型攻撃抑止
- 多経路通信耐性

を実現する可能性を持つ物理学的成立制御理論であり、それらの本提案する前段階の提案となります。

数理モデル詳細版（式展開・確率論）

0. 目的

本書は、無数鍵多重時変成立点理論＋（関連特許等の統合）を「評価可能な形」に落とすために、

- KPI 定義（防御率・防衛率・被害確率）
- 改善倍率の定義
- 通報到達確率（Pnotify）の式
- 試行回数と時間窓を入れた確率モデル
- 実測データで置換する手順

を明示する。

---

1. 基本定義（KPI の意味を固定する）

1.1 単発イベント（1 回の攻撃試行）に対する確率

攻撃カテゴリ iに対し、次を定義する。

- **防御率** $D_i \in [0,1]$
  「侵入・成立（突破）を防ぐ」確率（Prevent）
- **突破率** B_i

$$B_i = 1 - D_i$$

- **防衛率** $S_i \in [0,1]$
  「突破されても被害化（暗号化・破壊・漏えい・業務停止など）を防ぐ」確率
  （Mitigate/Contain）
- **被害確率** H_i
  73 攻撃一覧の数値体系に合わせるため、まずは

$$H_i = 1 - S_i$$

  として定義する（“防衛できなかった確率”）。
  ※一覧表で「従来_防衛率 55.9% → 従来_被害確率 44.1%」の関係が成立しているため

ここが重要：「被害確率」を厳密に “突破まで含めた全体確率” とするモデルもありますが、
73 攻撃一覧は「被害確率＝(1−防衛率)」の定義で統一されているため、当面この定義で説明します。 実証段階では、後述の総合被害確率モデルへ拡張します。

---

2. 改善倍率（〇〇倍）の定義と式

2.1 改善倍率（被害確率ベース）

攻撃カテゴリ iについて、従来（baseline）と提案（proposed）の被害確率を

- 従来：$H_{i,0}$
- 提案：$H_{i,1}$

とすると、**改善倍率** M_iを

$$M_i = \frac{H_{i,0}}{H_{i,1}}$$

で定義する。

これは、73 攻撃一覧の「改善率（倍率）」の計算と一致する（例：ランサムウェアで約 176 倍）。

2.2 例：ランサムウェア（暗号化・二重脅迫）

73 攻撃一覧のランサム行（C-23）より

③特許＋理論有り-完璧想定-73 攻撃-指標一覧-

- 従来 防衛率：55.9% → 被害確率 $H_0 = 44.1\%$
- 複合 防衛率：99.74999999525% → 被害確率 $H_1 = 0.25000000475\%$

改善倍率は

$$M = \frac{44.1}{0.25000000475} \approx 176.3999966$$

よって **約 176.4 倍**。
（一覧の改善率 176.3999… ）

3.「防衛率 99.7%以上」の扱い（提出用の言い方）

防衛率のモデル値が

$$S_1 = 99.74999999525\%$$

であるため、提出文言は

- **防衛率：99.7%以上（設計モデル値）**
- **被害確率：0.3%以下（設計モデル値）**（0.25000000475%）

のように丸めるのが安全。（丸めても“モデル上の意味”を損ないません）

---

4. 通報到達確率モデル（Pnotify）の式展開

統合提案資料に明示された独立近似モデル に従う。

4.1 定義

- p：単発・単チャネルの到達確率
- n：チャネル数（SMS/Push/音声/メール/衛星/閉域無線等）
- r：再送回数
- **総試行回数**：$m = n(1 + r)$

4.2 到達しない確率

単発で届かない確率は $(1-p)$。独立近似により、m 回すべて届かない確率は

$$(1-p)^m$$

4.3 よって到達確率

$$P_{\text{notify}} = 1 - (1 - p)^{n(1+r)}$$

5.「総合被害確率」への拡張(防衛装備庁向け:評価可能形)

73 攻撃一覧は便宜上 $H = 1 - S$を採用しているが、
実証・評価では「突破から被害まで」を含めた総合モデルが必要になります。

5.1 総合被害確率(単発)

単発の攻撃試行 1 回に対し、

- 突破する確率:$B = 1 - D$
- 突破後に被害化する確率:$1 - S$

とすると、総合被害確率(単発)は

$$P_{\text{damage,1}} = (1 - D)(1 - S)$$

これにより、**「防御(侵入阻止)」と「防衛(被害抑止)」が分離**され、
防衛装備庁の評価指標(侵入阻止・侵害封じ込め)に合わせやすくなります。

5.2 試行回数がある場合(N 回)

同一カテゴリ攻撃が N回試行され、各試行が独立近似できるなら

$$P_{\text{damage,N}} = 1 - \left(1 - P_{\text{damage,1}}\right)^N$$

すなわち

$$P_{\text{damage,N}} = 1 - (1 - (1 - D)(1 - S))^N$$

5.3 時間窓（成立点の有効時間）を入れる

成立点が有効な時間窓を T秒、攻撃者が 1 秒あたり λ回の有効試行を行えるとすると、時間窓内の試行回数期待値は

$$N = \lambda T$$

これを上式に代入して

$$P_{\text{damage,window}} = 1 - (1 - (1 - D)(1 - S))^{\lambda T}$$

ここが「時変・ワンタイム・成立後即失効」による優位の数理表現になります。
Tを短く、λ を抑える（遮断・条件強化）ほど、被害確率は急減します。
（縦資料の 5 状態モデル「遮断（Blocked）へ遷移しやすい」設計思想とも整合）

---

6. 攻撃が「努力するほど不利」になるモデル（遮断＋条件強化）

縦資料では、失敗が「遮断」と「条件強化」に繋がり、攻撃が累積しない思想が示されている。
これを確率的に表すため、試行 k回目の突破確率を

$$B_k = (1 - D_k)$$

とし、失敗するたびに防御率が上がる（突破確率が下がる）関数を置く。例：

$$D_k = 1 - (1 - D_0)\alpha^k (0 < \alpha < 1)$$

すると突破確率は

$$B_k = (1 - D_0)\alpha^k$$

で指数的に減衰。このとき、N 回までの総合突破確率は

$$P_{\text{breach}} = 1 - \prod_{k=0}^{N-1}(1 - B_k) = 1 - \prod_{k=0}^{N-1}(1 - (1 - D_0)\alpha^k)$$

（独立近似）ここが「攻撃が学習して有利」ではなく「攻撃が試すほど成立しにくい」という数理の形です。

7. 73 攻撃一覧モデルとの整合（提出用の説明テンプレ）

防衛装備庁向けには、次の 3 点セットで説明すると通ります。

1. 73 攻撃一覧の公開値は **設計モデル値**（定義：$H = 1 - S$）
2. 実証段階では **総合被害確率** $(1 - D)(1 - S)$を採用して再評価
3. 通報・証拠化・再送は **Pnotify** で設計し、独立近似の前提を明記

---

8. 実証で収集すべきデータ（式に入れるための最低限）

PoC で置換すべきパラメータはこれだけです。

- D：侵入・実行前遮断の成功率→ 実行 API／KMS アクセス／権限プロキシで計測
- S：突破後の封じ込め成功率→ 暗号化停止、横展開停止、復旧時間短縮など
- p, n, r：通報到達率の設計値（チャネル別到達ログ）
- λ：攻撃試行レート（SIEM/EDR/WAF ログ）
- T：成立点の有効時間（仕様）

---

9. 提出用「数式付き」短文（そのまま貼れる）

本提案では、単発攻撃に対する総合被害確率を
$P_{\mathrm{damage},1} = (1 - D)(1 - S)$と定義し、試行回数 Nに対して
$P_{\mathrm{damage,N}} = 1 - (1 - P_{\mathrm{damage},1})^{N}$を用いて評価する。
また多チャネル通報の到達確率は $P_{\mathrm{notify}} = 1 - (1 - p)^{n(1+r)}$（独立近似）により設計し、実測値で置換する。

---

10. 付録:ランサムウェア数値の「防衛率→被害確率→改善倍率」変換

73 攻撃一覧(ランサム)では

- 被害確率 $H = 1 - S$
- 改善倍率 $M = H_0/H_1$

よって

- $S_1 = 99.74999999525\% \Rightarrow H_1 = 0.25000000475\%$
- $H_0 = 44.1\% \Rightarrow M \approx 176.4$

まとめ

- 公開 KPI(防衛率 99.7%以上、改善倍率 176 倍等)は **設計モデル値**(73 攻撃一覧に準拠)
- 評価・実証段階では、総合被害確率 $(1 - D)(1 - S)$と試行回数モデルで再計算
- 通報・再送・証拠化は Pnotify の式で設計し、到達ログで置換