



2026 年 10 月 9 日

各 位

会 社 名 abc 株式会社  
代表者名 代表取締役社長 松田 元  
(コード：8783、スタンダード市場)  
問合せ先 経営企画部 部長 谷井 篤史  
<https://abc-chain.com/form/>

**サイバーセキュリティ事業の検討開始および推進組織新設に関するお知らせ**  
～AI で診断・監査し、その履歴をブロックチェーンに記録する「ZEKUU Protect」を  
2026 年 11 月より提供開始予定～

当社は、本日開催の取締役会において、新たな事業としてサイバーセキュリティ事業の検討を開始すること、およびその推進を担う組織として、Web3 事業部内に「サイバーセキュリティ課」を設置することを決議いたしましたので、下記のとおりお知らせいたします。

同課は、2026 年 7 月 22 日付「AI とブロックチェーンを活用した法人向けシステム最適化サービス (ABX) 「ZEKUU (是空)」の提供開始に向けた取り組みに関するお知らせ」にて公表いたしました ABX (AI Blockchain Transformation: AI とブロックチェーンによる企業変革) の取り組みの一環として、AI を活用したサイバーセキュリティ診断・監査サービス「ZEKUU Protect」(以下「本サービス」といいます。)の開発および提供を担います。本サービスは、2026 年 10 月 6 日に開発に着手しており、2026 年 11 月より提供を開始する予定です。

記

**1. サイバーセキュリティ課の設置**

(1) 設置の目的

AI を悪用したサイバー攻撃が広がる中、当社は、AI を活用したサイバーセキュリティの診断および監査と、その記録を第三者が検証できる形で残す仕組みを、新たな事業として推進してまいります。その推進を担う組織として、Web3 事業部内にサイバーセキュリティ課を設置いたしました。

本サービスは、診断および監査の履歴をブロックチェーン上に記録するものであることから、同課を Web3 事業部内に置くことといたしました。

(2) 組織の概要

|     |         |                                                                      |
|-----|---------|----------------------------------------------------------------------|
| (1) | 名 称     | サイバーセキュリティ課                                                          |
| (2) | 所 属     | Web3 事業部                                                             |
| (3) | 設 置 日   | 2026 年 10 月 9 日                                                      |
| (4) | 主 な 業 務 | ・ 本サービスの開発および提供<br>・ 当社グループのサービス基盤を対象とした本サービスの先行適用<br>・ 外部の専門会社等との連携 |
| (5) | 人 員     | 2 名                                                                  |

専門性の高い診断および監査については、外部の専門会社と連携して実施する体制を整えてまいります。

**2. 事業の概要**

(1) 本サービスの内容

本サービスは、AI を活用してサイバーセキュリティの診断および監査を行い、その履歴をブロックチェーン上に記録するサービスです。診断および監査の内容を、第三者が後から検証できる形で残します。ポイントは次の 3 点です。

- 解く課題：サイバーセキュリティの事故が起きた際の説明は当事者の主観に基づくものとなり、第三者がその正しさを確かめることが極めて困難であること
- 仕組み：診断および監査の履歴と、日々のシステムの記録（ログ）のハッシュ値をブロックチェーン上に記録し、実施者にかかわらず第三者が後から検証できる形で残すこと
- 進め方：当社の法人向けシステム最適化サービス「ZEKUU（是空）」の診断と一体で始め、2026 年 11 月より順次提供を開始する予定であること

## （2）解決を目指す課題

サイバーセキュリティの事故が発生した際に、原因究明として表明される内容は、当事者の主観に基づくものであり、その正しさを第三者が評価することは極めて困難です。外部の専門家による調査が行われる場合でも、その元になる記録は当事者の手元にあり、事故の前から変わっていないことを確かめる手段は限られております。当社は、これが最も重要な課題であると考えております。診断や監査についても、システムを構築・運用する事業者自身やその関係者によって行われることが多く、結果の中立性を外部から確かめることは容易ではありません。

この課題が残る限り、対策を重ねても、その効果を事後に検証することは困難です。

## （3）記録と検証の仕組み

本サービスでは、診断および監査について、次の3点を、実施の時点でハッシュ値としてブロックチェーン上に記録し、公開する設計としております。

- 計画（どの対象を、どの手順で確かめるか）
- 実行の記録
- 結果

これにより、後日示された記録が当時のものと同一であることを、取引先等の第三者が照合できるようにしてまいります。

診断および監査を誰が実施したかにかかわらず、その過程を、実施者の説明ではなく記録に基づいて検証できる仕組みの構築を目指してまいります。当社が実施する診断および監査も、同じ仕組みの対象といたします。当社は、自らが実施する診断および監査こそ、第三者の照合に耐える形で残すべきものと考えております。

この記録は、利用企業にとっても、診断および監査を実施した側にとっても、実施した内容を示す拠り所になります。

ブロックチェーン上に記録するのは、診断および監査の計画・実行の記録・結果のハッシュ値、診断・監査と是正の件数、日時などです。利用企業を特定できる情報、内容そのものおよび個人情報は記録いたしません。

## （4）事故が起きる前からの記録

利用企業が保全するシステムの記録（ログ）についても、最初の診断の時点から、日ごとなど一定の間隔でハッシュ値をブロックチェーン上に記録してまいります。

事故が起きてからではなく、起きる前から記録がある状態をつくります。事故が生じた際に、いつ何が記録されていたかを、当事者の申告に頼らず、第三者が記録に基づいて検証できるようにすることを目指してまいります。

## （5）診断の始め方

診断は、当社の法人向けシステム最適化サービスにおける現行システムの診断と一体で始めます。

まず、利用企業の支払いの書類（請求書・契約書）から、保守や業務・データを任せている委託先を洗い出します。次に、外部とつながる入口（VPN 機器や、保守業者が遠隔で接続する回線など）を、委託先ごとに確かめます。そのうえで、その範囲を継続的に点検いたします。

診断の結果は、同サービスにおけるシステムの見直しの提案にも生かしてまいります。

## （6）AI と人の役割、情報の取り扱い

- 点検は AI が広く速く行い、対象の範囲に漏れがないかの確認、判断および優先順位付けは人が行います。
- AI が実行した手順とその記録も同じ仕組みで残し、AI が何を確かめたかを後から検証できるようにいたします。
- 外部から見える範囲の点検は、利用企業（必要な場合はその委託先を含みます）の書面による同意に基づき、読み取りのみで行う設計です。
- パスワード等の認証情報はお預かりしない設計といたします。
- AI を用いる範囲は、利用企業の方針（AI の利用に関する社内の定めを含みます）に応じて定めます。
- データの処理の場所は、利用企業の方針に応じた形を検討してまいります。

## 3. 背景および目的

#### (1) AI を悪用したサイバー攻撃への備え

生成 AI の普及に伴い、サイバー攻撃をめぐる状況は変化しており、公的機関の公表資料でも取り上げられております。

- 2025 年 5 月：「重要電子計算機に対する不正な行為による被害の防止に関する法律」が公布されるなど、国によるサイバーセキュリティの強化に向けた施策が進められております。
- 2026 年 1 月：独立行政法人情報処理推進機構（IPA）の「情報セキュリティ 10 大脅威 2026」で、組織向けの脅威の 1 位が「ランサム攻撃による被害」、2 位が「サプライチェーンや委託先を狙った攻撃」となり、3 位には「AI の利用をめぐるサイバーリスク」が初めて選出されました。
- 2026 年 5 月：内閣官房国家サイバー統括室、警察庁、経済産業省など 9 機関が連名で「AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について（重要インフラ事業者等に対する注意喚起）」を公表いたしました（5 月 18 日）。同文書は、AI の悪用により攻撃のスピード・規模が劇的に増加する等の脅威に直面しているとしたうえで、資産管理、脆弱性管理、サプライチェーン・リスクへの対応等の基本的な対策の確実な実施を求めています。

AI を悪用した攻撃は手口の更新が速く、導入済みの対策が有効であり続けているかを、継続的に確かめることが求められます。

#### (2) 被害の入口

警察庁が 2026 年 3 月に公表した「令和 7 年におけるサイバー空間をめぐる脅威の情勢等について」によれば、次のとおりです。

- 令和 7 年のランサムウェアの被害報告件数は 226 件と、依然として高水準で推移しております。そのうち中小企業が 143 件を占めております。
- 被害を受けた企業・団体等へのアンケートでは、感染経路の有効回答 92 件のうち 61 件が VPN 機器でした。同資料は、主要な侵入経路である VPN 機器等について、速やかな対応が必要であるとしております。

また、漏えいした個人情報、なりすまし等による二次的な被害に用いられるおそれがあり、事故の事実関係を早く正確に確かめられることの重要性は高まっております。

#### (3) 当社が着目した点

機器の保守や業務の委託は、契約と支払いを伴うため、任せている相手は請求書や契約書に現れます。当社の法人向けシステム最適化サービスは、利用企業が現行システムに何をいくら支払っているかを一覧にすることから始めます。同じ書類を起点に委託先を洗い出し、外部とつながる入口を委託先ごとに確かめることができると考えております。

診断や監査の結果は、取引先による確認や、サイバー保険の引受け等の判断の前提にもなります。一方で、診断や監査がどのような手順で行われ、何が確認されたのかを、利用企業の取引先や株主等の第三者が後から確かめる手段は、一般に限られております。

当社は、診断および監査の履歴を改ざんが困難な形で残し、第三者が検証できるようにすることが、事故が生じた際の説明と検証の拠り所になると考えております。

#### (4) 譲渡した事業との違いと、本事業に取り組む経緯

当社は、2026 年 7 月 31 日付「（開示事項の経過）連結子会社の異動（株式譲渡）に関する株式譲渡契約締結のお知らせ」にて公表いたしましたとおり、ネクスト・セキュリティ株式会社について、当社が保有する株式のすべてを譲渡いたしました。同社の事業は、サイバー・セキュリティ・ソリューションの販売、コンサルティングならびに環境の構築・導入・運用支援であり、同社の成長には、同領域に強固な法人顧客基盤を持つ譲渡先のもとで事業を進めることが最善であると判断したものです。

本事業は、製品の販売や導入を行うものではなく、次の点で譲渡した事業とは異なります。

- 提供するもの：AI を活用した診断および監査と、その履歴をブロックチェーン上に記録し、第三者が後から検証できる形で残す仕組みであること
- 用いる経営資源：当社の Web3 事業（ブロックチェーン）と、AI を活用した法人向けシステム最適化サービス「ZEKUU（是空）」の内製による開発体制および顧客との接点であること

本事業は、新たな子会社の設立を伴うものではなく、Web3 事業部内の組織と既存の開発体制により進めるものです。当社は、経営資源の選択と集中の方針のもと、当社の強みを生かせる形でセキュリティ分野に取り組んでまいります。

#### (5) 本サービスの目的

当社は、当社が推進する AI 活用（内製による開発体制）と、当社グループが取り組むブロックチェーン事業の知見を組み合わせ、本サービスの開発に着手いたしました。本サービスを通じて、当社は以下を目指してまいります。

- AI を悪用した攻撃の広がりに対し、AI を活用した診断および監査によって、利用企業が基本的な対策の点検と是正を継続できるよう支援すること

- 診断および監査と是正の履歴を、実施者にかかわらず第三者が検証できる形で残す仕組みを構築すること
- 法人向けシステム最適化サービスをはじめとする当社グループのサービス群との連携により、事業シナジーを創出すること

#### 4. サービスの主な特徴

|     |            |                                                                                                                                                                                    |
|-----|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (1) | サービス名称     | ZEKUU Protect (読み：ゼクウ プロテクト)                                                                                                                                                       |
| (2) | 提供形態       | 次の順で、段階的に伴走して支援<br>①委託先と外部との接続の洗い出し（現行システムの診断と一体で実施）<br>②外部から見える範囲の診断<br>③継続的な点検と記録<br>④是正の支援（必要に応じて、外部の製品・サービスの選定の支援を含む）<br>基本的な診断および監査は当社が実施し、専門性の高い診断および監査は外部の専門会社との連携により実施する予定 |
| (3) | 診断・監査の対象   | ・外部とつながる入口（VPN 機器、保守業者による遠隔接続の回線等）<br>・業務やデータの委託先<br>・外部に公開しているシステムおよびその設定（メールのなりすまし対策の設定を含む）<br>・生成 AI の利用状況                                                                      |
| (4) | 技術的特徴      | ・AI が広く速く点検し、範囲の確認と判断は人が行う体制<br>・診断および監査の計画、実行の記録および結果のハッシュ値をブロックチェーン上に記録・公開し、実施者にかかわらず第三者が照合できる仕組み<br>・AI を用いる範囲は利用企業の方針に応じて定める。データの処理の場所は利用企業の方針に応じた形を検討。AI の学習には用いない            |
| (5) | 収益の形（料金体系） | 次の収益を想定し、段階ごとの料金体系を検討中<br>①診断および監査の料金（都度・定期）<br>②継続的な点検と記録の料金（継続）<br>③是正の支援、および法人向けシステム最適化サービス「ZEKUU（是空）」の提案への接続<br>④損害保険会社との連携（診断および監査の記録の活用と、その対価のあり方を検討）                        |
| (6) | 主な対象       | 中堅・中小企業を中心                                                                                                                                                                         |

（※開発途中のため、内容は今後変更される可能性があります）

（※本サービスにおける「監査」とは、診断の計画・実行・結果が記録のとおりに行われたかを確認、その記録を第三者が照合できる形で残すことをいい、特定の基準への適合を保証するものではありません）

#### 5. 今後の展開

当社は、国策として強化が進むサイバーセキュリティへの対応を見据え、企業の重要な情報について、その記録をブロックチェーン上に残し、第三者が後から検証できるようにする取り組みを推進してまいります。

##### （1）提供開始までの進め方

当社は、2026 年 10 月 6 日より、当社グループのサービス基盤を対象に本サービスの先行適用を開始しており、診断の記録の作成とハッシュ値による照合を、日ごとに行っております。引き続き、診断および監査の品質ならびに提供体制の検証を進めてまいります。

並行して、法人向けシステム最適化サービスの利用企業を中心に、パイロット先の選定および初期提案を進めます。契約条件の策定や法務・商標等の必要な整備を進め、2026 年 11 月より、順次サービスの提供を開始する予定です。

なお、本サービスの名称は、商標等の確認の結果により、提供開始までに変更する場合があります。

（２）損害保険会社との連携

診断および監査の記録を、損害保険会社がサイバー保険の引受けや保険料の算定に活用できる形について、検討してまいります。なお、現時点で、特定の損害保険会社との間で協議または合意している事実はありません。

（３）業績への影響

本件による当期連結業績への影響は現時点では軽微と見込んでおりますが、中長期的には当社グループの収益基盤の拡充および企業価値の向上に寄与するものと考えております。今後、開示すべき事項が生じた場合には、速やかにお知らせいたします。

以 上

# ZEKUU Protect

ゼクウ プロテクト

AIを活用した  
サイバーセキュリティ診断・監査サービス

診断および監査の履歴を、

第三者が後から検証できる形で残す。

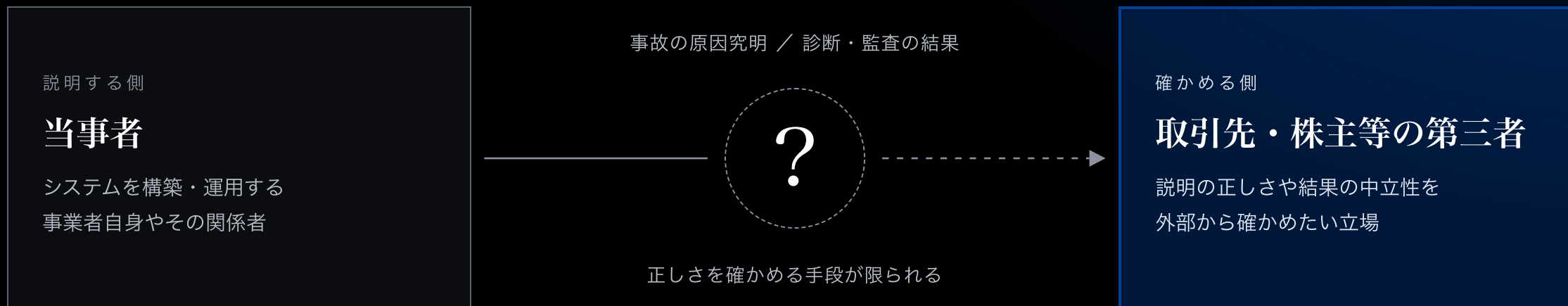
abc株式会社 2026年10月

2026年10月6日 開発着手 / 2026年11月より順次提供開始予定

開発途中のため、内容は今後変更される可能性があります

THE PROBLEM 解決を目指す課題

# 事故の原因究明は、**当事者の主観**に基づいている



## 01 事故のあとの説明

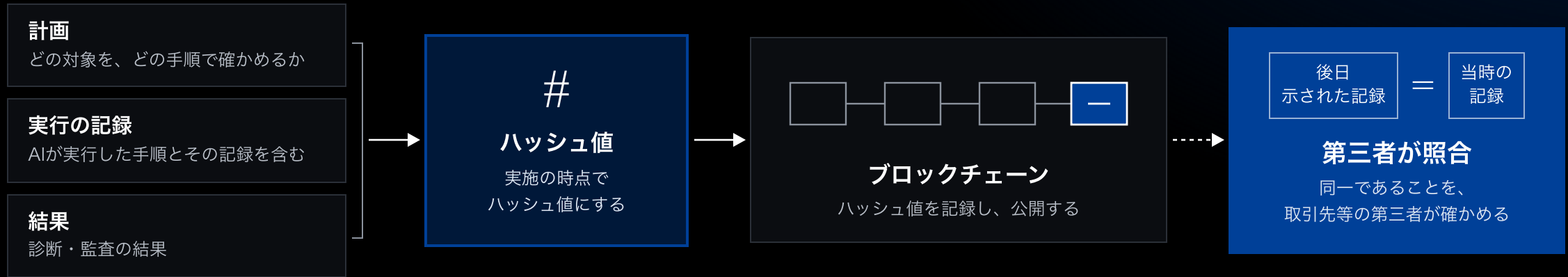
原因究明として表明される内容は当事者の主観に基づき、その正しさを第三者が評価することは極めて困難です。外部の専門家が調査する場合でも、元になる記録は当事者の手元にあり、事故の前から変わっていないことを確かめる手段は限られます。

## 02 診断や監査

構築・運用する事業者自身やその関係者によって行われることが多く、結果の中立性を外部から確かめることは容易ではありません。

この課題が残る限り、対策を重ねても、その効果を事後に検証することは困難です。

# 実施の時点の記録を、後日、第三者が照合できる 設計

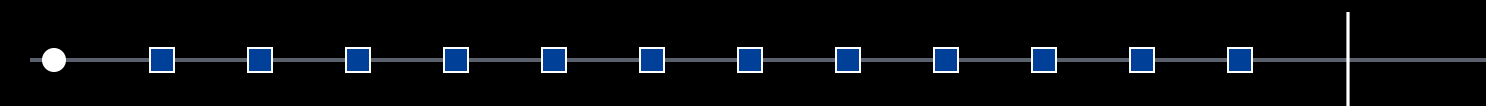


当社が実施する診断および監査も、同じ仕組みの対象といたします。  
自らが実施する診断および監査こそ、第三者の照合に耐える形で残すべきものと考えております。

## BEFORE AN INCIDENT 事故が起きる前から、記録がある状態をつくる

最初の診断

事故が生じた際



最初の診断の時点から、日ごとなど一定の間隔で、  
利用企業が保全するシステムの記録（ログ）のハッシュ値を記録

事故が生じた際に、いつ何が記録されていたかを、  
当事者の申告に頼らず第三者が検証できることを目指す

### 記録する

計画・実行の記録・結果の  
ハッシュ値、診断・監査と是正の  
件数、日時など

### 記録しない

利用企業を特定できる情報、内容  
そのもの、個人情報

# 第三者による照合を、ひと目で確かめられる画面に

abc | ZEKUU Protect

診断・監査の記録

いまの状況

委託先と入口

点検と是正

記録と照合

システムの記録

利用企業 Z社（見本）  
2026.12.04（金）09:30 JST 時点

VERIFICATION 第三者による照合

後日示された記録が、当時の記録と同一かを確かめる

後日示された記録  
11月の定期診断 結果  
ハッシュ値 9f2c...a41e  
照合した日時 2026.12.03 14:20  
照合した人 取引先P社（第三者）

=

ブロックチェーン上の記録（当時）  
11月の定期診断 結果  
ハッシュ値 9f2c...a41e  
記録した日時 2026.11.16 10:42  
取引ID 7ae3...c1f0・公開

照合の結果  
☑ 一致  
当時の記録と同一です  
記録の同一性の照合であり、結果の  
良し悪しを示すものではありません

ハッシュ値はブロックチェーン上に公開され、第三者が自分で照合できます。当社が実施した診断および監査も、同じ仕組みの対象です。

VENDORS 委託先と外部とつながる入口

支払いの書類（請求書・契約書）から洗い出し、委託先ごとに確かめる

| 委託先     | 任せている内容   | 洗い出した書類 | 外部とつながる入口         | 最新の点検       | 状況             |
|---------|-----------|---------|-------------------|-------------|----------------|
| 01 委託先A | 基幹システムの保守 | 契約書・請求書 | VPN機器 1 遠隔接続の回線 1 | 12.04 09:12 | ● 是正を記録（12.02） |
| 02 委託先B | 会計データの処理  | 請求書     | 遠隔接続の回線 1         | 12.04 08:40 | 🕒 人が判断中        |
| 03 委託先C | Webサイトの運用 | 請求書     | 公開しているシステム 2      | 12.04 08:15 | ○ 点検済み         |
| 04 委託先D | 複合機の保守    | 契約書     | 遠隔接続の回線 1         | 12.04 07:58 | ○ 点検済み         |
| 05 委託先E | 給与計算の業務   | 請求書     | 確認中               | —           | 🕒 人が範囲を確認中     |

委託先 5 社 外部とつながる入口 6 か所（1社は確認中） 点検はすべて、書面による同意に基づき読み取りのみで実施

DAILY LOG 事故が起きる前からの記録

日ごとのシステムの記録（ログ）のハッシュ値を、ブロックチェーン上に記録

11.04 最初の診断 30 日分 途切れなく記録 12.04 00:05 今日の記録 b7d0...19fa

AI & PEOPLE AIと人の役割

AI 点検を広く速く行う  
実行した手順とその記録も、同じ仕組みで残す

人 範囲の確認・判断・優先順位付け  
範囲に漏れがないかを確かめ、是正の順を決める

INSPECTION 点検の状況

継続的な点検・直近30日

| 点検               | 是正             | 人が判断中           |
|------------------|----------------|-----------------|
| 1,248 件<br>AIが実施 | 7 件<br>うち今週 2件 | 3 件<br>優先順位を付ける |

最新の点検 2026.12.04 09:12 最新の是正 2026.12.02 16:05

ON-CHAIN ブロックチェーン上の記録

11月の定期診断

| 記録したもの             | ハッシュ値            | 実施 当社<br>記録した日時 |
|--------------------|------------------|-----------------|
| 計画<br>対象と手順        | a3e1...07bd      | 11.09 09:00     |
| 実行の記録              | 5c88...e2f0      | 11.12 18:30     |
| AIの手順<br>実行した手順と記録 | 71bd...3c09      | 11.12 18:30     |
| 結果                 | 9f2c...a41e 照合済み | 11.16 10:42     |
| 是正の件数<br>件数と日時     | e04a...5d12      | 12.02 16:05     |

日ごとのシステムの記録（ログ） 11.04 から毎日  
12.03 分 12.04 00:05  
翌日 0時台に記録 b7d0...19fa

記録しない物 利用企業を特定できる情報、内容そのもの、個人情報。  
記録するのはハッシュ値、件数、日時などです。

表示している社名・件数・日時・ハッシュ値はすべて架空の見本です

## 01

## 第三者による照合

後日示された記録と、ブロックチェーン上の当時の記録のハッシュ値を並べ、同一かどうかを示す

## 02

## 委託先と外部とつながる入口

支払いの書類から洗い出した委託先ごとに、入口と点検の状況を一覧にする

## 03

## 事故が起きる前からの記録

日ごとのシステムの記録（ログ）のハッシュ値が、途切れずに並ぶ

WHY NOW 背景

# 導入済みの対策が有効であり続けているかを、 継続的に確かめることが求められている

令和7年のランサムウェアの  
被害報告件数

226 件

そのうち中小企業が143件

出典：警察庁「令和7年におけるサイバー空間をめぐる脅威の  
情勢等について」（2026年3月）

感染経路の有効回答のうち  
VPN機器だったもの

61 / 92 件

被害を受けた企業・団体等へのアンケート。  
主要な侵入経路であるVPN機器等への速やかな  
対応が必要とされている

出典：同上

組織向けの脅威  
（情報セキュリティ10大脅威 2026）

2 位 サプライチェーンや委託先を  
狙った攻撃

3 位 AIの利用をめぐる  
サイバーリスク 初選出

出典：独立行政法人情報処理推進機構（IPA）  
「情報セキュリティ10大脅威 2026」（2026年1月）

2026年5月18日 内閣官房国家サイバー統括室、警察庁、経済産業省など9機関が連名で公表  
「AI性能の高度化を踏まえたサイバーセキュリティ対策の強化について（重要インフラ事業者等に対する注意喚起）」

WHERE IT STARTS 診断の始め方

# 支払いの書類を起点に、**委託先と外部とつながる入口**を確かめる

法人向けシステム最適化サービス「ZEKUU」の現行システムの診断と一体で始め、診断の結果は、システムの見直しの提案にも生かす。

01

## 支払いの書類

請求書・契約書。保守や業務の委託は、契約と支払いを伴うため書類に現れる

02

## 委託先を洗い出す

保守や業務・データを任せている委託先

03

## 入口を確かめる

外部とつながる入口（VPN機器、保守業者が遠隔で接続する回線など）を、委託先ごとに確かめる

04

## 継続的に点検

その範囲を継続的に点検し、記録する

AI

### 点検を広く速く行う

AIが実行した手順とその記録も同じ仕組みで残し、AIが何を確かめたかを後から検証できるようにする

人

### 範囲の確認・判断・優先順位付け

対象の範囲に漏れがないかの確認、判断および優先順位付けは人が行う

### 情報の取り扱い

主な対象：中堅・中小企業を中心

#### ■ 外部から見える範囲の点検は、読み取りのみ

利用企業（必要な場合はその委託先を含む）の書面による同意に基づいて行う設計

#### ■ パスワード等の認証情報はお預かりしない設計

#### ■ AIを用いる範囲は、利用企業の方針に応じて定める

データの処理の場所は方針に応じた形を検討。AIの学習には用いない

# 診断と監査を入口に、**継続の記録**と**「ZEKUU」の提案**へ

最初の診断は、法人向けシステム最適化サービス「ZEKUU」の現行システムの診断と一体で始める。そこから、次の4つの収益を想定している。

01

都度・定期

## 診断および監査の料金

外部から見える範囲の診断と、診断および監査。専門性の高いものは、外部の専門会社と連携して実施する予定



診断・監査のたびに

02

継続

## 継続的な点検と記録の料金

点検を続け、診断・監査の履歴と、日々のシステムの記録（ログ）のハッシュ値を、ブロックチェーン上に記録し続ける



記録が続く間、継続して

03

提案

## 是正の支援とZEKUUの提案

診断の結果を、システムの見直しの提案に生かす。必要に応じて、外部の製品・サービスの選定を支援



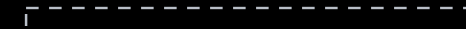
提案が採用されたとき

04

検討中

## 損害保険会社との連携

診断および監査の記録を、サイバー保険の引受けや保険料の算定に活用できる形と、その対価のあり方を検討



形と対価を検討中

### 今後の方向

国策として強化が進むサイバーセキュリティへの対応を見据え、企業の重要な情報について、その記録をブロックチェーン上に残し、第三者が後から検証できるようにする取り組みを推進してまいります。

WHAT'S NEXT 取り組みの転換と今後の展開

# 取り組みの軸を、**診断・監査と検証できる記録**へ

これまで

既存のソリューションの販売を中心とする形



これから

AIを活用した診断および監査と、  
その記録を第三者が検証できる形で残す仕組み

**本サービスは、その第一歩となるものです。**

2026年7月31日付の適時開示にて公表いたしましたとおり、サイバー・セキュリティ・ソリューションの販売等を行う連結子会社であったネクスト・セキュリティ株式会社について、当社が保有する株式のすべてを譲渡いたしました。

ROADMAP 提供開始までの進め方



**2026年10月6日より  
先行適用を開始**

当社グループのサービス基盤を  
対象に、診断の記録の作成と  
ハッシュ値による照合を  
日ごとに実施



**パイロット**

法人向けシステム最適化サービスの  
利用企業を中心に選定・初期提案



**2026年11月より  
順次提供開始予定**

契約条件の策定や法務・  
商標等の必要な整備を進める

**推進体制** 2026年10月、Web3事業部内にサイバーセキュリティ課を設置。同課が  
本サービスの開発および提供を担う

基本的な診断および監査は当社が実施し、専門性の高い診断および監査は外部の専門会社との  
連携により実施する予定

**損害保険会社との連携** 診断および監査の記録を、損害保険会社がサイバー保険の引受けや  
保険料の算定に活用できる形について、検討してまいります

※本サービスにおける「監査」とは、診断の計画・実行・結果が記録のとおりに行われたかを確認、その記録を第三者が照合できる形で残すことをいい、特定の基準への適合を保証するものではありません。

※開発途中のため、内容は今後変更される可能性があります。

※本サービスの名称は、商標等の確認の結果により、提供開始までに変更する場合があります。

※本資料は投資勧誘を目的としたものではありません。投資に関する決定は、ご自身の判断と責任においてお願いいたします。

※本件が当社連結業績に与える影響は軽微です。