情報処理学会論文誌　Vol. 49　No. 9　3199–3208 (Sep. 2008)

構造計算書不正検知システムの提案

植松建至[†1]　芦野佑樹[†1]　藤田圭祐[†1]
多田真崇[†1]　高塚光幸[†1]　佐々木良一[†1]

近年，耐震強度偽装問題に見られる構造計算書の改竄が大きな問題となっている．従来の構造計算書の検査には検証の正確性や検証時間，人員コストなどに問題があった．これらの問題に対して，著者らは電子認証技術の適用が適当であると考えた．しかし，構造計算者自身が不正を行うという特殊なケースであるので，設計者が署名するのではなく，構造計算プログラム自身が署名を行う方式を提案した．また，この方式を採用するにあたり，(a) 署名鍵を不正に使用されない，(b) 正しいプログラムのみが動いていたことを証明できる，といった要件が必要であることを示し，それらの要件を満たすために，耐タンパモジュールとして IC カードを使用し，Windows API を利用したチェックプログラムを用いて解決を図る方式を提案した．最後に，既存方式と比べた場合の特長を述べる．

A Proposal of Detection System against Illegal Structural Design

Kenshi Uematsu,[†1] Yuki Ashino,[†1] Keisuke Fujita,[†1]
Masataka Tada,[†1] Mitsuyuki Takatsuka[†1]
and Ryoichi Sasaki[†1]

In recent years, an interest to illegal structural designs of buildings has been increasing. The conventional method to certificate the structural design has the problems with concerns to the correctness, time for certification and required man powers. To solve these problems, we propose the detection system of illegal structural design based on digital signature. However, in this case, it is impossible to adopt the method that the designer signs the calculated results, because we must consider the illegal behavior of the designers. Therefore, we proposed the method that the computer program for the structural design itself signs the calculated result. In addition, we proposed the techniques to avoid illegal usage of the signing key and the illegal alternation of the program. Finally, we shown the advantages of the proposed methods compared with the conventional methods.

1. はじめに

近年，建築物の安全性に対して関心が高まっている．これは平成 17 年の耐震強度偽装問題の影響が主な原因として考えられる．

耐震強度偽装問題とは平成 17 年 11 月 17 日に国土交通省が建築物の安全性を記した構造計算書が A 元一級建築士によって改竄されていたと発表したことから始まる一連の問題のことである．今年に入っても新たにアパグループの物件に構造計算書の改竄が認められ，大きな問題となっている．これにより，改竄が容易なプログラムが提供されていたこと，構造計算書の偽装が容易であること，そして検査機関による検証システムに不備があることが浮き彫りとなった．

文献 1) によれば，**図 1** で示すように現在，構造計算書は国土交通省の管轄下である性能評価機関の検査を通った大臣認定構造計算プログラムを用いて PC 上で計算し，構造計算に係る書類と電子データを出力し，提出するのが一般的である．

本論文は，事件の再発防止策の一環として構造計算プログラムを用いて作成する電子データに設計者自身が改竄を加えても検知ができるように，既存の電子認証システムを適用し，正確かつ高速な検証を可能とするシステムの提案を行う．

本提案方式は，後で詳しく述べるように以下のような特長を持っている．

(a) 扱う問題の新規性，有用性が高い．

① 現実の問題であり，社会の安全に関わる重要な研究課題である．

② 従来のセキュリティ問題のように第三者からの攻撃ではなくデータ作成者である PC の持ち主の不正を考慮しなければならない解決が困難な問題である．

(b) 扱い方の新規性

① プログラム自体が自らの入出力のペアに対し自動的に署名するという従来にない対策を採用している．

したがって，扱う問題においても，扱い方においても十分に新規性のあるものであると考えている．

本論文では，2 章で既存システムを説明し，3 章で電子認証システムの適用を考察し，4 章で提案システムを説明する．そして 5 章で各システムの評価をし，6 章でまとめを述べる．

†1 東京電機大学
Tokyo Denki University

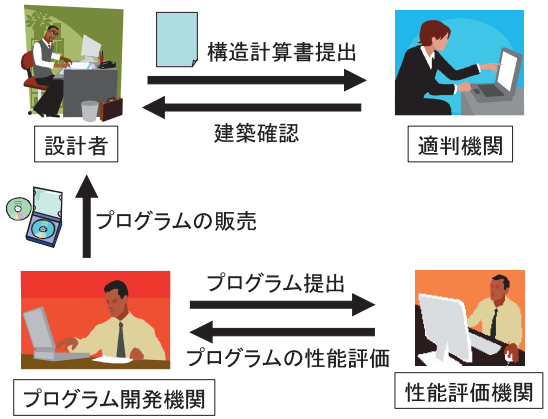

図 1　構造計算書取扱いの全体像
Fig. 1　Overview on treating structural calculation sheets.

2.　既存システム

本章では事件前の検証方法を既存システム 1，現在の検証方法を既存システム 2 と表記し，考察していく．

2.1　既存システムの検証方法

文献 3) によると，構造計算書の検査は指定確認検査機関，建築主事，構造適合性判定機関によって行われている．指定確認検査機関は国土交通省，構造適合性判定機関は各都道府県によって認定を受けた機関で，どちらも民間による機関が導入されている．これは年間 100 万件を超える申請数を 1 件ごとに検証する際に発生する膨大な検証時間を短縮しようというものである．

構造計算書の構成は大まかに設計データと安全性評価に分かれる．指定確認検査機関と建築主事は構造計算書に記載されている安全性評価部分の数値が基準に達しているか確認を行う．そこで正当であると認められたものは次の構造適合性判定機関に送られる．この機関では構造計算書に記載されている設計データをプログラムに入力すると本当に記載されている結果部分（安全性評価）が出るのか確認をする．つまり構造計算書の設計データと安全性評価の対が正しいのか確認する機関である．本論文での提案システムの検査はこの構造適合性判定機関での検査を対象としている．過去に印字出力された紙を切り貼りして不正な構造計算書を作成する，という改竄行為も過去に見られた．しかしそれらについては電子透かしの研究などと組み合わせることによって解決できる問題としてここではあくまでも電子データとして提出された構造計算書の検査を対象とする．

これまでの検証方法は，構造計算書に対して大臣認定プログラムの使用証明書が添付されているか確認するものである．添付されている場合は安全性評価のみをチェックして建築確認を行うことになる．証明書がないものについては別途内容確認で検査することになっているが，建築業界では認定プログラムで計算することが一般的でそのようなケースはまれである．この検査方法を既存システム 1 とする．

また平成 19 年 6 月に事件後の対応として検査の厳格化のために建築法の改正が行われた．これは文献 3) にあるように高額な建築物に対し詳細にチェックするというものである．検証方法は申請者側と同一のプログラムを用いて，記載されているデータを入力から再計算を行い，出力された結果が提出された構造計算書と一致していれば正当であると判断する，というものになった．これを既存システム 2 とする．

2.2　既存システムの問題点

既存システムの問題点は以下の 2 点となる．

(A)　正当性検証が不十分
(B)　膨大な検証時間

文献 1) の「建築法改正前の現状報告書」によると，既存システム 1 では認定プログラム使用証明書がついていれば短時間で大量の計算書を処理できるが，逆にいえば証明書さえついていれば構造計算書に不正行為が行われていても見逃してしまう，といった (A) の問題が出てくる．これは設計データと安全性評価の対が正しいか，という検証を行わないためである．

図 2 は姉歯設計事務所やアパグループの物件における構造計算書の偽装事件を示したものである．この際の偽装は既存システム 1 の欠点を利用したもので，構造計算書の結果，つまり安全性評価を都合の良い別の構造計算書の安全性評価と入れ替えるといった偽装が行われていた．しかし認定プログラム使用証明書がついていることによって，適判機関は設計データと安全性評価の組合せに改竄が加えられていることを検知できず，最終的に安全性に問題のある建物が建築されることとなった．

この問題は既存システム 2 のように再計算を行うことによって解決することができるが，これにより 2 つ目の問題である (B) が発生する．これは構造計算プログラムが複数のサブプログラムから構成されていたり，あるいは構造計算者が複数の構造計算プログラムを使用したりすることで，再計算において，プログラム間の入力と出力の関係性を確認するため

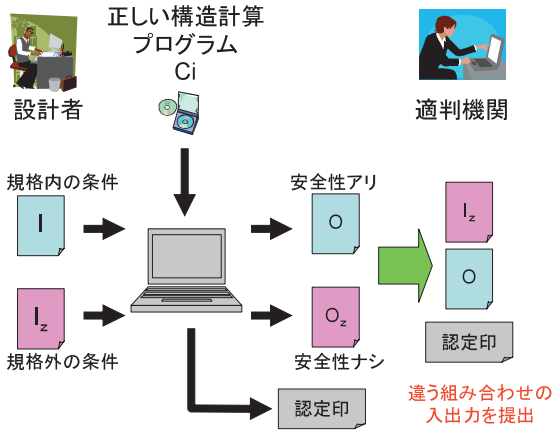

図 2　実際に起こった不正の例
Fig. 2　Case example of fabricating structural calculation sheets.

に，途中出力されたパラメータを最低でも 4 回は再入力しながら計算するといった人手のかかる処理を必要とするためである．プログラムを一本化してもこの過程は必要となるため再計算の手間は大きい．検証時間が延びたことで実際に建築法に記載されている検査期間も延長されている．これにより文献 1) の建築着工統計調査報告書にあるように法改正からこれまでの建築物の着工数が減少している．これらの影響はゼネコン・住宅会社だけでなく，建設資材・住宅設備メーカなどにも波及し，さらには日本の GDP にも下押しの影響を与えていることが最近では専門家やメディアなどにも指摘され，大きな問題となっている．

また実際にはこの既存システム 2 における再計算はすべての建築物に適用しているわけではなく，一般の住宅などの比較的安価な建築物に対してはこれまでどおり既存システム 1 で運用していくとし，現状のシステムには多くの問題をかかえていることが分かる．

なお，以降は説明の都合上，構造計算における複数の入出力に関しては，簡略化しワンパスで入出力が取得できるモデルとして説明する．そして，5 章で改めて複数パスのモデルで評価を行う．

3.　電子認証システム

本章では既存システムの問題点を改善するために当然思いつくと考えられる検証者の署名鍵を用いる電子認証システムの適用について説明する．

文献 3) にあるように，電子認証システムとは電子署名技術を用いて完全性と本人性を証明できる認証システムのことである．一般的には本人の秘密鍵で電子署名することによって完全性を確認でき，公開鍵を認証局に登録した際に受け取る電子証明書を用いて本人性を確認できることが知られている．このように電子認証システムは，あるデータが本人によって作成されたか，そして署名後にデータが改竄されていないか，ということを検証できる．またその検証は値を比較するという単純な演算であるので検証時間が既存システム 2 に比べて早いという特徴を持っている．これらの特徴を生かして，電子認証システムを構造計算データの正当性検証に用いることを考える．

3.1　電子認証システムの適用

既存の検証方法に単純に電子認証システムを適用すると，以下の手順を経ることになる．

(1)　設計者が構造計算データに署名を施す．
(2)　電子証明書とともに適判機関に送付する．

検証は現状のシステムのように再計算や認定プログラム使用証明書の有無による判定ではなく，電子署名と電子証明書を用いての正当性検証となる．これにより，構造計算書が設計者によって作成され，署名後に改竄がされていないことを証明できる．もちろん検証時間も電子認証システムの特徴を受け継ぐので高速化される．

3.2　電子認証システムの適用における問題点

通常の電子認証システムの問題点は以下のようになる．

(C)　設計者自身の不正行為を検知できない

本件にそのまま電子認証システムを適用した際に，**図 3** で示すように設計者による署名前の不正行為を検知できないといった，(C) の問題が出てくる．そもそも本件では設計者が不正行為を行う可能性があることも考慮に入れる必要がある．そのため，設計者が署名を施したとしても，その前に設計者本人によってデータの改竄を行ったり，構造設計プログラムを改竄したりすることで，署名検証で不正を検知することができなくなってしまう．なお，ここで，構造設計プログラムの改竄とは，既存のプログラムを直接改竄することだけでなく，別の不正なプログラムで計算したり，レジストリの内容を変更するなどして，別のプログラムに置き換えたり，別のプログラムを追加し出力を変更したりすることなども含むものとする．

図 2 で示したような入力 I と出力 O の組合せの入れ替えについても図 3 の改竄 1 に見られるように防ぐことができないことになる．

この問題点は，従来の情報セキュリティのように外部からの不正行為を考慮するだけで

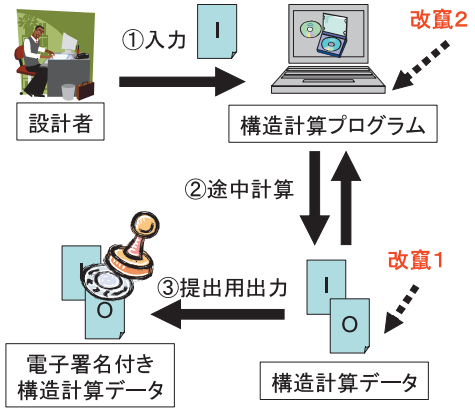

図 3　改竄可能性の概略図
Fig. 3　Possibility of falsification.

なく，PC の所有者からの不正行為に対しても対策をとらなければならないことを示しており，これまでと違った対策が必要とされる．

4. 提案システム

4.1 提案システムにおける要求整理

2.2 節および 3.2 節で示した問題点を考慮して，電子認証システムを適用する際に以下の要求を満たすように拡張する必要があると考えた．

【要求 1】 プログラムが出力したデータの正当性が検証可能であること．具体的には以下の項目が検証できること．

A)　出力後のデータに改竄がされていない．

B)　正しい環境で計算されている．

【要求 2】 検証時間が現実的な時間に短縮されること（内容の確認や再計算による検証はしたくない）．

【要求 3】 新しい機関や特別な装置などを用意しなくても済むこと（PC を用いスタンドアロン環境下で実現，計算センタなどは設けたくない）．

要求 1 の A) は当然の内容であり，B) については 3.2 節で示した問題 (C) のとおり，設計者自身の不正行為がないことを保証するために設けている．要求 2 も 2.2 節で示したとおり，1 件ごとに時間をかけると膨大な時間になるという現状があるため，必然的な要求となる．

要求 3 は，本研究が現実の問題であるため，現在の政府がとりうる現実的な対策とする必要があるため，追加したものである．具体的には，シンクライアント方式のように計算を特定のセンタに集中させると，(1) システムやセンタを用意するコストがかかる，(2) 設計者がこれまで使用していた環境と入れ替える必要がある，(3) プログラムを提供するメーカに負担がかかる，といった問題が発生する可能性があるとともに，小さな政府を実現するため，政府がセンタを用意しリアルタイムの運用にかかわるというようなことはすべきではないという判断があり，詳細検討から外された．

よって著者らはこれまでの環境を大幅に変えることなく，コストもかからないようにするため，スタンドアロンでこれらの要求を実現するシステムを提案することとした．

4.2 要求へのアプローチ

4.1 節で示した要求の中で重要なのは要求 1 の A)，B) であると考えられる．これは既存の電子認証システムでは自己の操作の正当性を証明できないためである．まず要求 1-A) を満たすために設計者自身が署名を行うのではなく，第三者による署名を行わせることを考える．そこで本論文では構造計算プログラム自体が計算結果に対して署名をして出力させる方法を提案する．このアプローチでは設計者に署名させなくて済むのに加え，出力直後のデータに署名をするため設計者は署名を行うタイミングを選べない．これにより出力後のデータに不正を行うことはできなくなる．これを提案システム 1 とする．このシステムを採用した場合，解決しなければならない問題として以下のものが考えられる．

(a)　署名鍵を不正に使用されてしまう．

これに対しては，耐タンパな領域を持つ IC カードに署名鍵を保持させ，署名を行わせることによって，不正に署名鍵を使用することを防ぐ．この対策をとったシステムを提案システム 2 とする．

次に要求 1-B) を満たすための手法を考える．これは提案システム 2 を採用した場合，構造計算プログラムを改竄したり，IC カードを不正に使用するような不正プログラムが起動したり，といった可能性が残るためである．それらの問題は以下に要約される．

(b)　正しいプログラムで計算された保証がない．

(c)　計算に関係のない不正なプログラムが動いていなかった保証がない．

(b)，(c) に対しては，関連研究である文献 2)，6) にある API フック機能を持つチェックプログラムとホワイトリストを用いる．

API フック機能は Windows が提供する API（Application Program Interface）をフッ

クする．この機能で，OS がプログラムを起動する前に，設計者による構造計算プログラムの起動命令を API の段階でフックするのに使用する．このとき，起動したプログラムが正しいものであるか，プログラムの署名検証をチェックプログラムが行う．ここでの署名は性能評価機関が構造計算プログラムを検査する際に，プログラムに対して署名したものを使用する．同様に，その他のアプリケーションプログラムに対しても起動命令時に API フックを行い，構造計算に関係のないものに関しては起動しないようにチェックプログラムで API の処理内容を変更して停止させる．また，あらかじめ構造計算に必要なアプリケーションのハッシュ値をリストアップし，そのリストに適判機関の署名を付けて構造計算者に提供する．このリストを文献 2) のようにホワイトリストと呼ぶ．このホワイトリストと一致しないプログラムの起動命令が呼び出されたときはチェックプログラムで排除されることになる．

このチェックプログラムはサービスプログラムであり，アプリケーション層に位置している．そのためアプリケーションプログラム同様，不正な変更を加えられる可能性がないとはいえない．しかし，サービスプログラムは，ユーザがログインする前から起動している．また，アプリケーションなどの設定データであるレジストリの内容に対する変更も考えられるが，チェックプログラム導入時にサービスプログラムに対する変更を禁止することが可能である．そのため本論文が扱う構造計算者が不正行為をするというシーンを想定すると，ユーザがログインする前から起動するサービスプログラムに対する不正行為は，通常のアプリケーションプログラムへの不正行為に比べ，技術的に考えて可能性が低く，信頼性を持たせることができると考えた．

ここで上記の (a)，(b)，(c) の対策をすべて適用したシステムを提案システム 3 とする．

4.3　提案システムの詳細

本節では提案システム 3 について説明する．

(1) 登場人物

(a) プログラム開発機関
プログラムを開発し，構造計算者に販売する者．
(b) 構造計算者
プログラムを用いて構造計算を行い，適判機関に対して構造計算書を提出する者．
(c) 適判機関
構造計算データの正当性検証を行う者（数値が基準に達しているかは別の機関が行う）．
(d) 性能評価機関
販売前にプログラムの検査を行う者．

(2) 前提条件

(a) 性能評価機関は不正をしない．
(b) 適判機関は不正をしない．
(c) 構造計算者は印字出力に対しては改竄を加えられない（印字出力は適判機関で行う）．
(d) OS やサービスは信頼できる．

(3) チェックプログラム

チェックプログラムは OS 起動の直後に起動するサービスプログラムで，適判機関によって導入される．機能は以下のとおりである．
(a) 出力の監視，署名データの取得．
構造計算プログラムから出力を取得し，IC カードに入力して，署名データを取得する．
(b) API フックによるプログラム起動監視．
API 層でプログラムの起動命令を監視する．
(c) API フックによる正当性チェック．
構造計算プログラムを含むアプリケーションプログラムの起動命令を確認したら，ホワイトリスト（下記 (4) を参照）を基に署名検証を行う．ホワイトリストと一致しない，もしくは存在しないプログラムは起動を停止する．

(4) ホワイトリスト

ホワイトリストはチェックプログラムと同様に適判機関から提供される．内容は以下のとおりである．
(a) アプリケーションリスト．
計算に必要な最低限のアプリケーションプログラムのハッシュ値がリストアップされている．
(b) アプリケーションリストの署名データ．
署名は適判機関によるものである．
(c) 適判機関の電子証明書．

(5) IC カード

適判機関によってチェックプログラムとともに配布されるもので，機能は以下のとおりである．
(a) 署名．
チェックプログラムからの入力が来たら，保持している署名鍵で署名をし，出力する．
(b) 電子証明書のコピーを出力する．
署名と同時に出力する．

(c) 耐タンパ領域を持つ．
耐タンパ領域は書き換えや参照のできない安全な領域のことで，ここでは署名に必要な署名鍵や電子証明書を保持しておく．

(6) 処理フロー

処理フローには下記の 3 つのフェーズが存在しており，順を追って説明する．また性能評価機関，プログラム開発機関，構造計算者，適判機関，IC カードを表す引数をそれぞれ pc，pd，d，v，ic とする．またこのフローで出てくる署名鍵はあらかじめ認証局に登録されているものとする．

(a) 開発フェーズ

開発フェーズでは，プログラム開発機関と性能評価機関が下記の項目によりプログラムを提供する．

1. 開発機関はプログラム Ci を作成し，性能評価機関に送る（i はバージョン情報）．
2. 性能評価機関は Ci の動作を検査する．
3. 2. の検査で正当なプログラムであると確認できたら，性能評価機関は署名データ $S_{pc}(h(Ci))$ を作成し，$Cert(P_{pc})$ とともに開発機関に送る．
4. 開発機関は 3. で認定を受けた Ci を構造計算者に販売する（Ci，$S_{pd}(h(Ci))$，$Cert(P_{pd})$ をセットにする）．
5. プログラムが更新，新規作成されるごとに 1. から 4. の項目を行う．

(b) 導入フェーズ

導入フェーズでは，適判機関管轄下の導入者が下記の項目によりシステムの導入を行う．

1. 設計者の PC にチェックプログラムを導入する．
2. 構造計算者に導入したチェックプログラムと対応付けられた IC カードを提供する．

(c) 計算フェーズ

計算フェーズでは，構造計算者が下記の項目により IC カードを用いて構造計算を行う（**図 4**）．

1. 構造計算者は PC の電源を入れる．
2. チェックプログラムが立ち上がる．
3. 構造計算者は IC カードを挿入する．
4. チェックプログラムはアプリケーションプログラムの起動を監視する．
5. プログラムの起動命令を確認したら，ホワイトリストの署名検証を行う．ホワイトリストの正当性が確認できた場合は 6. へ進む．ホワイトリストが不正な場合はプログラムの起動命令を停止してエラーを出してフェーズを終了する．
6. 起動命令が出されているプログラムのハッシュ値がホワイトリストにあるものと一致するか，署名検証で確認する．成功した場合は正しいプログラムであると判断し，起動させ 7. へ進む．不正なプログラムであればプログラムの起動命令を停止してエラーを出してフェーズを終了する．
7. チェックプログラムは常駐プログラムであるため以降の項目でも 4.〜6. の処理は継続して行われている．
8. 構造計算者は入力データ I を正しい構造計算プログラム Ci に入力する（**図 5** ①）．
9. Ci は出力データ $O = Ci(I)$ を計算し，チェックプログラムに (I, O) を出力する（図 5 ②，③）．
10. チェックプログラムは $h(I, O)$ を計算し，IC カードに入力する（図 5 ④）．

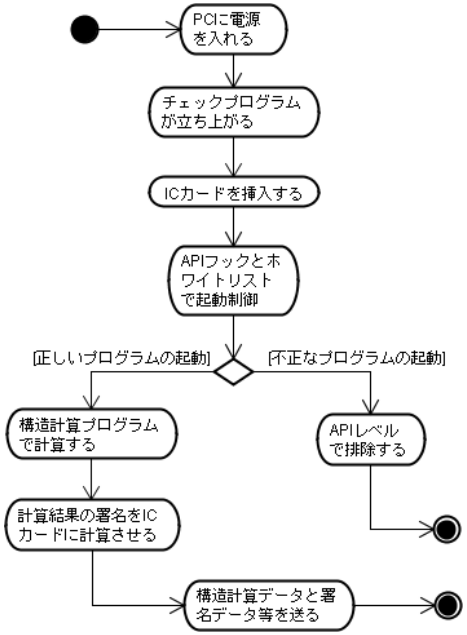

図 4　処理フロー
Fig. 4　Processing flow.

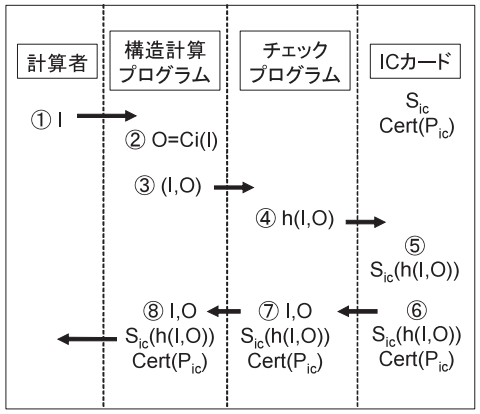

図 5　演算フロー
Fig. 5　Calculation flow.

11.　IC カードは署名鍵 S_{ic} で署名データ $S_{ic}(h(I,O))$ を作成し，チェックプログラムに電子証明書 $Cert(P_{ic})$ とともに出力する（図 5 ⑤，⑥）．
12.　構造計算者は I，O，$S_{ic}(h(I,O))$，$Cert(P_{ic})$ を取得し，適判機関に送信する（図 5 ⑦，⑧）．
13.　構造計算者は構造計算書を作成する際には 1. から 12. の項目を行う．

(d) 検証フェーズ

検証フェーズでは，適判機関が下記の項目により申請された構造計算データを基に正当性検証を行っていく．

1.　電子証明書を認証局に問い合わせて，正当であれば検証に必要な検証鍵 P_{ic} を取得する．
2.　I，O からハッシュ値 h'(I, O) を作成する．
3.　構造計算データの署名 $S_{ic}(h(I,O))$ を検証鍵 P_{ic} で復号し，h(I, O) を取得する．
4.　2. と 3. で取得したデータを比較し，一致した場合は O が正当な Ci に I を入力して出力されたデータであることが証明できたと判断し，フェーズを終了する．不一致の場合は署名検証に失敗したと見なし，エラーを出してフェーズを終了する．

(7) 安全性

以下の不正に対する安全性について考察する．

1.　出力されたデータに対する改竄行為
2.　構造計算プログラムへの改竄行為
3.　構造計算に関係ない不正なプログラムの起動
4.　IC カード内の署名鍵を不正使用

1. は図 3 に示す改竄 1 にあたるものである．これに関してはデータに対して署名が行われているので，検知することができる．

2. は図 3 に示す改竄 2 にあたるもので，これはホワイトリストとの照らし合わせによって改竄が行われた構造計算プログラムはチェックプログラムが起動をさせないので安全であるといえる．

3. に関しても同様にチェックプログラムが不正プログラムの起動を制御できるので安全であるといえる．

4. は IC カードへの不正アクセスを API フックで排除できるが，これはチェックプログラムが事前に導入されていることが重要である．また IC カードは導入されたチェックプログラムと対応するものなので紛失したとしても不正に利用されることはないと考える．

(8) 問題点

この方式では導入フェーズを設ける必要があるが，導入フェーズを用意することで適判機関に若干コストや手間がかかるといえる．

5.　各システムの評価

本章ではこれまでに示した各システムの評価を行う．各システムの特徴は以下のように要約することができる．

既存システム 1 の特徴

- 安全性評価と証明書の確認のみの検証．
- 導入コストや運用コストが少なく検証時間も短い．
- 検証の正確性がない．

既存システム 2 の特徴

- 既存システム 1 に再計算による検証を導入．
- 検証結果が正確で安全である．
- 検証時間や運用コストがかかる．

提案システム 1 の特徴

- プログラムに署名をさせるシステム．
- 署名鍵の更新にコストがかかる．

表 1　不正に対する強度評価
Table 1　Evaluation of safety level.

	既存1	既存2	提案1	提案2	提案3
難 ↑ OSやサービスプログラムの改竄	×	○	×	×	×
別プログラムを立ち上げて不正をする	×	○	×	×	○
構造計算プログラムを改竄する	×	○	×	×	○
署名鍵を解析する	／	／	×	○	○
↓ 易 出力データをすり替える	×	○	○	○	○

- 署名鍵の運用に関して問題がある．

提案システム 2 の特徴

- 提案システム 1 に耐タンパ性 IC カードを導入．
- プログラムに対して不正の可能性がある．

提案システム 3 の特徴

- 提案システム 2 にチェックプログラムを導入．
- 安全性が高く，検証時間が高速である．
- 導入時に信頼できる第三者が必要である．

表 1 は各システムの不正に対する強度評価をまとめたものである．縦軸は不正行為，横軸は各システムを示している．

当然ながら事件当時に運用されていた既存システム 1 は想定するすべての不正行為を検知できないという評価となる．ここで注目したいのは，強度評価において一番高かったのは既存システム 2 であることである．これは既存システム 2 の検証が，不正者の PC 環境や操作，不正のレベルなどに影響されず，適判機関側で実際に計算を行うからである．著者らが提案するシステムについては対策案を導入するごとに不正の強度評価が上がっていることに注目されたい．このことから各対策案の有効性を確認することができる．また全対策案を導入した提案システム 3 では，前提条件であげた，技術的に困難である OS，サービスプログラムへの不正以外には対応できる，といった評価になった．この評価は 4.2 節で述べたように今回想定する不正者のレベルを考えると，十分な安全性評価が得られたと考える．

表 2　総合評価
Table 2　General evaluation.

	既存1	既存2	提案1	提案2	提案3
不正に対する強度評価	×	◎	×	△	○
検証時間	○	×	○	○	○
開発コスト	○	○	○	△	△
導入コスト	○	△	○	△	△
運用コスト	○	×	○	○	○

次に総合評価を**表 2** に示す．これは表 1 で示した不正に対する強度評価だけでなく，要件にあった検証時間やシステムにかかるコストなどを考慮したものである．

まず既存システム 1 に関しては追加項目において高い評価となったが，一番重要視される不正に対する強度評価が最も低いことから，システムの移行を迫られた背景が分かる．

次に強度評価で一番高い評価であった既存システム 2 であるが，2.2 節で述べたように再計算に要するマンパワーや検証時間が膨大になってしまうといった問題が評価を下げる要因となった．文献 1) の建築着工統計調査報告書によると，既存システム 2 での再計算による検証は一部の高額な建築物のみを対象としているにもかかわらず，全国住宅着工戸数は前年同月比 43%減となっており，検証に要する時間が 1.8 倍近くも増していることが分かる．そのためすべての建築物に対して，この検証方法の適用を継続することに対しては反対意見が非常に強い．

最後に著者らが提案するシステムだが，提案システム 3 では，検証時間が既存システム 2 に比べ大幅に小さいと考えられる．すなわち，既存システム 2 が検証時にも，1 つの入力をプログラムに入れたのち対応した出力を得，その出力値に基づきさらに入力を入れるということを人手で何回もやらなければならないのに対し，提案システム 3 では，計算者によって与えられた複数の入出力の組合せを検証プログラムに最初に 1 度だけ入力すればよいので検証時間とマンパワーを大幅に低減させることができる．

したがって，検証で必要なマンパワーにともなう運用コストは提案方式 3 では十分に小

さく，IC カードやチェックプログラムの開発コスト，導入の際に必要な人員などの導入コストを考慮してもそのコストは十分小さいと考えられる．すなわち，今，提案方式 3 のプログラムの開発コストや導入コストを多めに見積もり，1 億円としても，既存方式 2 に比べ 1 件の検査あたり 1 時間の短縮効果が得られれば最低でも 1,000 円のコスト低減になり，10 万件でコストは同じとなる．現状では年間 100 万件の申請があり，既存方式 2 を使うのが 1 割だとしても 1 年間で提案方式 3 の方が小さなコストとなる．これらの数値は概略値でありさらに詳細な検討が必要であるが，大筋の傾向は間違いないといえるだろう．

このようにコスト面で優位であることは，提案システムが十分実現可能な対策であるともいえる．たとえ印字出力を適判機関で行うとしたとしても，署名検証による検証時間の短縮を考えると，その影響は少ない．

提案システム 3 では，すでに述べたように OS，サービスプログラムへの改竄への対処はできないが，今回想定する不正者のレベルを考えると，十分な安全性を有しているといえよう．したがって，提案システムは，既存のシステムに比べ優位な部分を多く有すると考えられる．

これらの評価から，あくまでも高い安全性のみを重視する場合には既存システム 2 が最適なシステムである．しかし安全性だけでなく効率面なども重視する場合においては提案システム 3 を採用することは合理的な選択であるといえよう．

また，一部の建築物に対してのみ既存システム 2 の再計算による検証を採用し，それ以外のかなりの部分を提案システム 3 とするなどの対応も考えられる．

6. おわりに

本研究では，スタンドアロン環境下で，構造計算プログラムを用いて作成する電子データに設計者自身が改竄を加えても，正確かつ高速に検証が可能なシステムの提案を行った．

今後は各システムの開発コスト，運用コストなどの定量的なデータを収集し，提案システムの優位性を具体的に示したい．また，提案システム 3 の実装と評価も今後行っていく予定である．

謝辞　研究の初期の段階で貴重なご意見をいただいた北陸先端科学技術大学院大学の宮地充子教授と NTT の金井敦氏，構造計算書の検査方法についてご教授いただいた財団法人建築行政情報センターの清水紀美恵氏にこの場をお借りしてあつく御礼申し上げる．

参 考 文 献

1) 国土交通省 http://www.mlit.go.jp/index.html
2) 藤田圭祐，芦野佑樹，上原哲太郎，佐々木良一：不正プログラムの起動制御機能を持つ DF システムの提案，*CSS2007* (2007).
3) 財団法人日本建築センター：建築基準法等の改正について［建築主/消費者のリーフレット］．http://www.njr.or.jp/m01/07/070622-2/syohisyamukekijyunhoukaisei.pdf
4) 財団法人日本建築センター：改正建築基準法に基づく確認検査の厳格化における措置に対する国交省の対応について．http://www.njr.or.jp/m01/07/070727/index.html
5) 佐々木良一，吉浦　裕，手塚　悟，三島久典：インターネット時代の情報セキュリティ，共立出版株式会社 (2002).
6) 芦野佑樹，佐々木良一：セキュリティデバイスとヒステリシス署名を用いたデジタルフォレンジックシステムの提案と評価，情報処理学会論文誌，Vol.49, No.2, pp.999–1009 (2008).

(平成 19 年 11 月 30 日受付)
(平成 20 年 6 月 3 日採録)

植松　建至（学生会員）

平成 19 年 3 月東京電機大学工学部第一部情報メディア学科卒業．同年 4 月東京電機大学大学院工学研究科情報メディア学専攻修士課程に入学し現在に至る．暗号セキュリティ，デジタルフォレンジックを中心に研究を行っている．

芦野　佑樹（学生会員）

平成 14 年北海道東海大学工学部電子情報工学科卒業．卒業後，会社員としてシステム開発に従事しながら，平成 16 年東京電機大学大学院工学研究科情報メディア学専攻修士課程に入学．平成 18 年 3 月同課程を修了し会社を退職．同年 4 月同大学院先端科学技術研究科情報通信メディア工学専攻博士課程に入学し現在に至る．デジタルフォレンジックシステムを中心に研究を行っている．

藤田　圭祐（学生会員）

平成 19 年 3 月東京電機大学工学部第一部情報メディア学科卒業．同年 4 月東京電機大学大学院工学研究科情報メディア学専攻修士課程に入学し現在に至る．デジタルフォレンジックを中心に研究を行っている．

多田　真崇（学生会員）

平成 18 年 3 月東京電機大学工学部第一部情報メディア学科卒業．同年 4 月東京電機大学大学院工学研究科情報メディア学専攻修士課程に入学．平成 20 年 3 月同課程を修了．同年 4 月に新日鉄ソリューションズに入社し，現在に至る．

高塚　光幸（学生会員）

平成 18 年 3 月東京電機大学工学部第一部情報メディア学科卒業．同年 4 月東京電機大学大学院工学研究科情報メディア学専攻修士課程に入学．平成 20 年 3 月同課程を修了．同年 4 月に NEC ソフトに入社し，現在に至る．

佐々木良一（フェロー）

昭和 46 年 3 月東京大学卒業．同年 4 月日立製作所入所．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．平成 13 年 4 月より東京電機大学工学部教授，平成 19 年 4 月より未来科学部教授．工学博士（東京大学）．平成 10 年電気学会著作賞受賞．平成 14 年情報処理学会論文賞受賞．平成 19 年総務大臣表彰（情報セキュリティ促進部門）．平成 19 年度「情報セキュリティの日」功労者表彰．著書に，『インターネットセキュリティ』（オーム社，1996 年），『インターネットセキュリティ入門』（岩波新書，1999 年），『IT リスクの考え方』（岩波新書，2008 年）等．情報処理学会コンピュータセキュリティ研究会顧問．日本セキュリティ・マネージメント学会会長，情報ネットワーク法学会理事長，日本学術会議連携会員，日本ネットワークセキュリティ協会会長．