「説明可能な情報管理の考え方とその技法について」

yosihiro.com

佐藤　慶浩

twitter.com/4416_310

発表者紹介

yosihiro.com

佐藤　慶浩（さとう　よしひろ）
日本ヒューレット・パッカード　個人情報保護対策室　室長
（併任）内閣官房 情報セキュリティ指導専門官
社外活動
JIPDEC　ﾌﾟﾗｲﾊﾞｼｰﾏｰｸ運営要領改正委員会　委員
(社)ｺﾝﾋﾟｭｰﾀｿﾌﾄｳｪｱ協会　ﾌﾟﾗｲﾊﾞｼｰﾏｰｸ審査判定委員会　委員
JIPDEC　ISMS適合性評価制度技術専門部会　委員
杉並区　住基ネット運用監視委員会　委員

背景
（お話しを聞いて佐藤が仮定している内容）

yosihiro.com

適切な医療行為について、ITシステムにログを残していても、医療結果が期待どおりでないと、ログを改ざんされていると疑われる。
ログに不適切な行為の記録があれば不利な証拠になり、行為が適切なときは、ログの改ざんを疑われてしまうのであれば、ログ記録は百害あって一利なしになると思われ、ログ記録の必要性の理解を妨げている。

改ざんされないログの取り方があるなら、それを知って、ログ記録の必要性を訴求したい。

2010年11月20日 Copyright 1995-2010 佐藤慶浩 スライド 3

本日のご紹介
（前スライドの仮定が正しいとして・・・）

yosihiro.com

・フォレンジック結果への2つの期待
・行為の記録を改変する動機と疑惑
・改変を防ぐ局面
・改変を防ぐ仕組みの例
・技術革新は「わがまま」から生まれる
・人・プロセス・技術で「わがまま」を叶える

2010年11月20日 Copyright 1995-2010 佐藤慶浩 スライド 4

フォレンジック結果への2つの期待

yosihiro.com

●不正行為があったことの確認
と
●不正行為がなかったことの確認

不正だけではなく、不適切な行為も含むが、ここでは便宜上「不正行為」と書くことにする。

一般的に、「ないことの確認」は、「あることの確認」よりも困難なことです。
それについては、デジタルフォレンジックでも同様です。

ただし、どちらの場合でも、「行為の記録を改変できない仕組み」が求められます。

2010年11月20日 Copyright 1995-2010 佐藤慶浩 スライド 5

行為の記録を改変する動機と疑惑

yosihiro.com

●実際に、不正行為があった場合
不正行為の記録を改変する動機は、あり得る。

●実際には、不正行為がなかった場合
不正行為のない記録を改変する動機は、本来ない。
つまり、ないはずの不正行為の記録を作ることはない。
（誰かを、おとしめるという動機ならば、あり得るが）

行為の記録を改変したという疑惑を受けることはあり得る。しかし、この場合、実際には不正行為はないので、無実の疑惑に過ぎない。

2010年11月20日 Copyright 1995-2010 佐藤慶浩 スライド 6

改変を防ぐ局面

yosihiro.com

行為の記録の改変を、どの場合に防ぐのか？

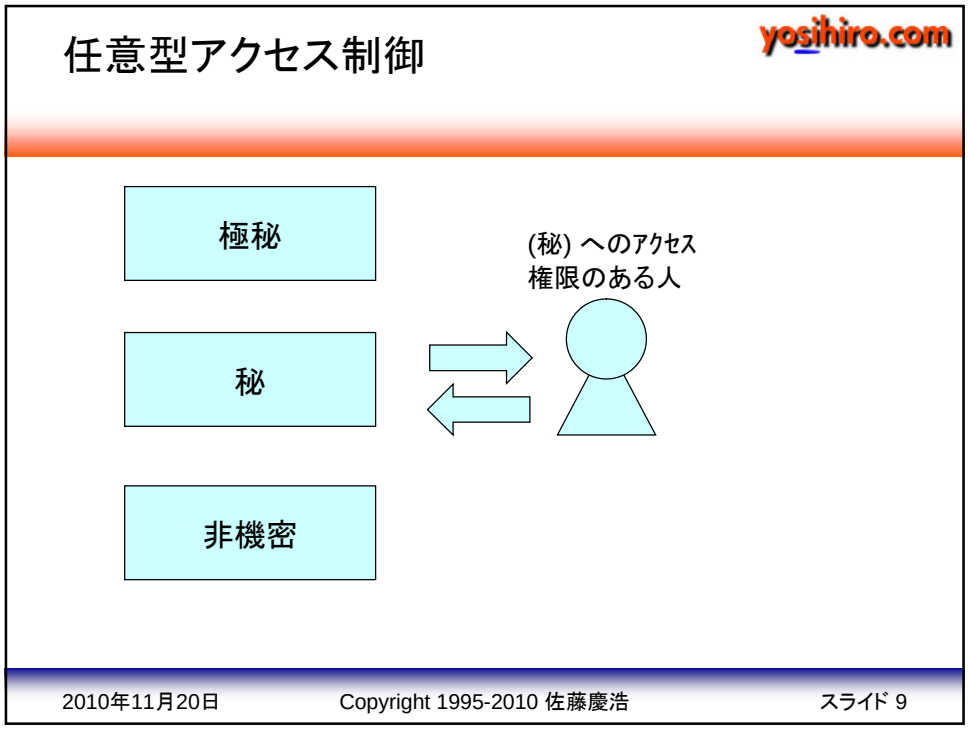
不正行為をしていない場合に備えるには、「不正行為がなかったことの証明」が必要と考えがち。
しかし、「ないことの証明」は困難。
そこで・・・
不正行為をしている場合に、行為の記録を改変できない仕組みを徹底することを考える。
その信頼性が高まれば、
　不正行為の記録がない　→　不正行為がなかった
という図式を組みやすくなる。

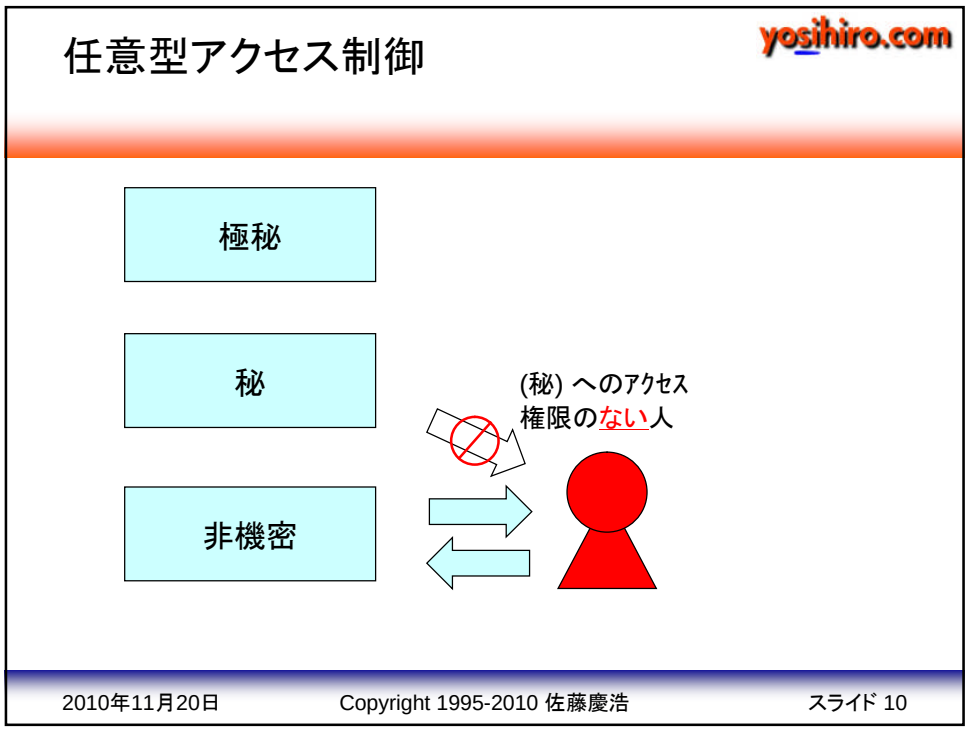
改変を防ぐ仕組みの例

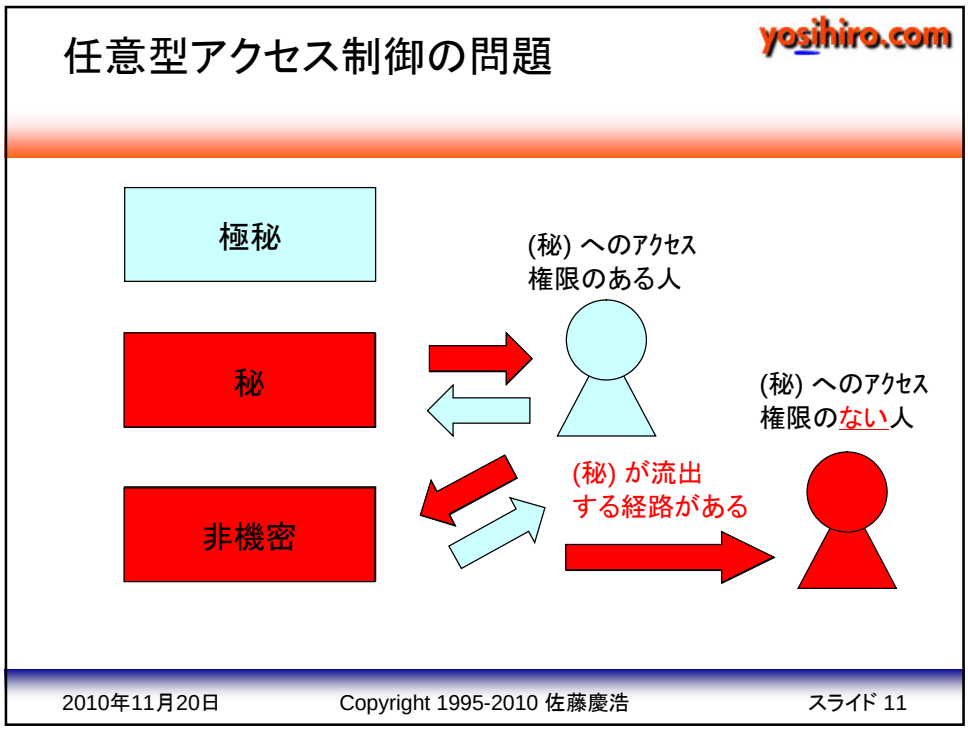
yosihiro.com

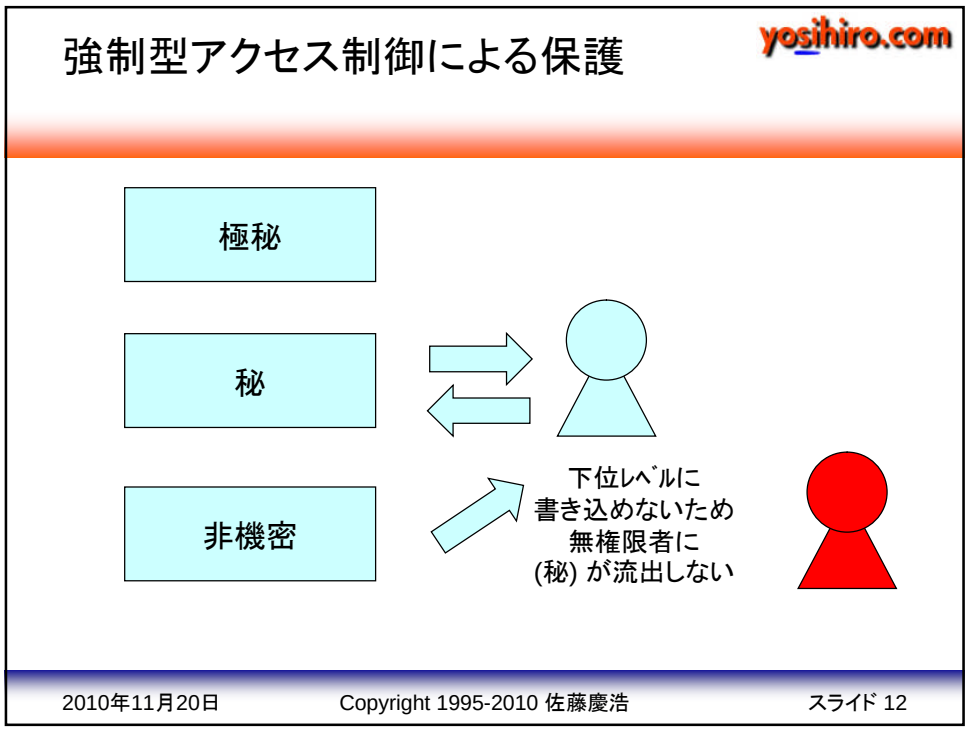
データアクセス制御方式の類型
　任意型アクセス制御（DAC：Discretionary Access Control）
　強制型アクセス制御（MAC: Mandatory Access Control）

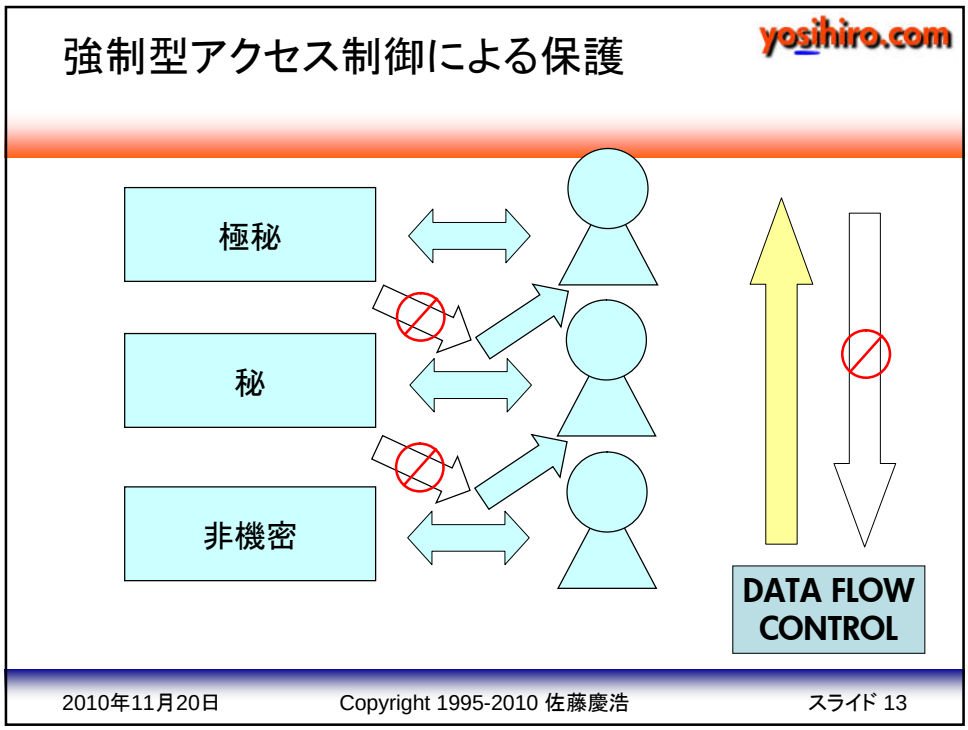
ここから、しばらく技術的な話しをしますが、技術的に深く理解する必要はありません。

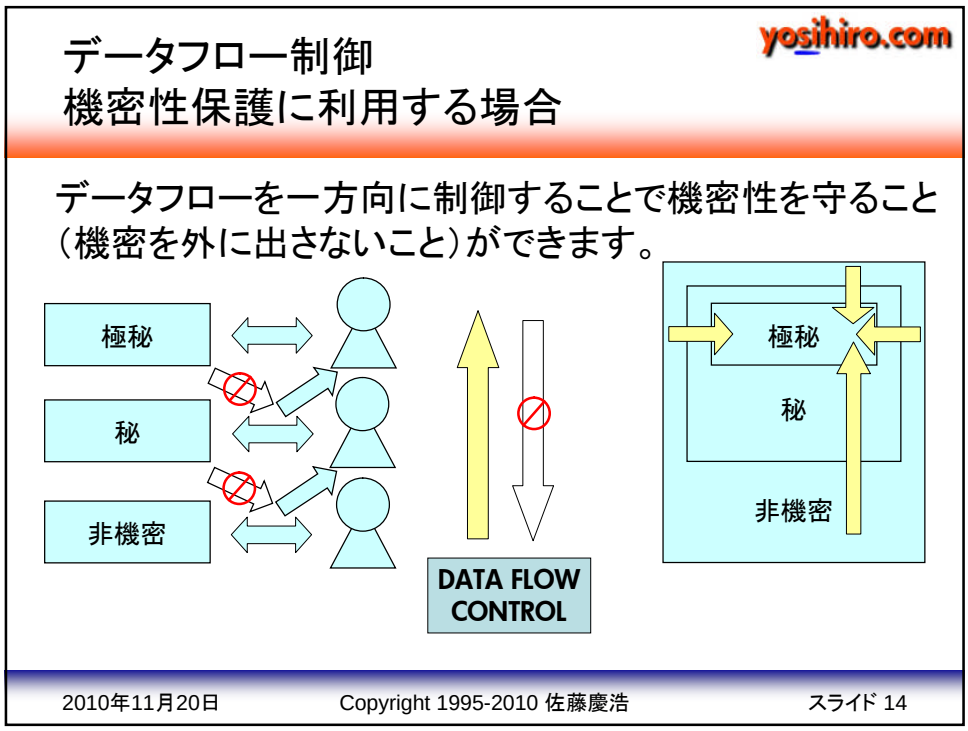

任意型アクセス制御
yosihiro.com
極秘
秘
非機密
(秘) へのアクセス
権限のある人
2010年11月20日
Copyright 1995-2010 佐藤慶浩
スライド 9


任意型アクセス制御
yosihiro.com
極秘
秘
非機密
(秘) へのアクセス
権限のない人
2010年11月20日
Copyright 1995-2010 佐藤慶浩
スライド 10


任意型アクセス制御の問題
yosihiro.com
極秘
秘
非機密
(秘) へのアクセス
権限のある人
(秘) へのアクセス
権限のない人
(秘) が流出
する経路がある
2010年11月20日
Copyright 1995-2010 佐藤慶浩
スライド 11

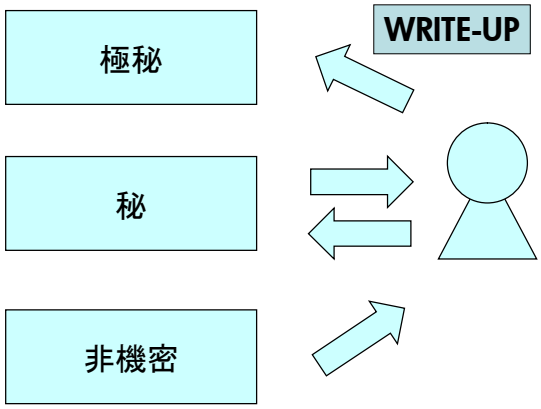

強制型アクセス制御による保護
yosihiro.com
極秘
秘
非機密
下位レベルに
書き込めないため
無権限者に
(秘) が流出しない
2010年11月20日
Copyright 1995-2010 佐藤慶浩
スライド 12


強制型アクセス制御による保護
yosihiro.com
極秘
秘
非機密
DATA FLOW CONTROL
2010年11月20日
Copyright 1995-2010 佐藤慶浩
スライド 13


データフロー制御
機密性保護に利用する場合
yosihiro.com
データフローを一方向に制御することで機密性を守ること
（機密を外に出さないこと）ができます。
極秘
秘
非機密
DATA FLOW CONTROL
極秘
秘
非機密
2010年11月20日
Copyright 1995-2010 佐藤慶浩
スライド 14

強制型アクセス制御による保護

yosihiro.com



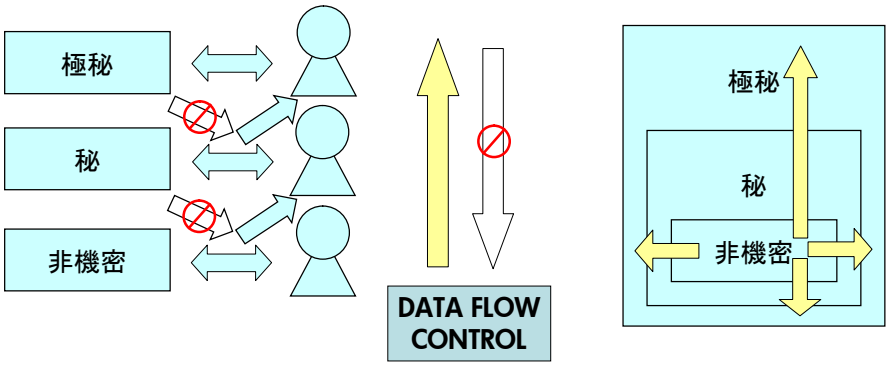
監査証跡は追記専用のため改変が不可能

2010年11月20日 Copyright 1995-2010 佐藤慶浩 スライド 15

データフロー制御 完全性保護に利用する場合

yosihiro.com

データフローを一方向に制御することで完全性を守ること（改変されないようにすること）ができます。



2010年11月20日 Copyright 1995-2010 佐藤慶浩 スライド 16

技術革新は「わがまま」から生まれる
必要な機能を要求することが大切

yosihiro.com

何をお伝えしたかったかというと・・・

ここから、しばらく技術的な話しをしますが、技術的に深く理解する必要はありません。

ここで紹介したIT製品の機能は、利用する側からの要求で用意された機能です。
既製のIT製品の機能の限界で、ITを利用した業務の限界を考えるのではなく、欲している業務を実現するために必要な機能をITに要求してください。
これまでのITの技術革新は、そんな「わがまま」から生まれています。
例）携帯電話機でウェブが見たい。メールがしたい。

2010年11月20日 Copyright 1995-2010 佐藤慶浩 スライド 17

人・プロセス・技術で「わがまま」を叶える
IT製品に使われない気持ちが大切

yosihiro.com

ITを利用した業務を構築するときに、
ITの知識は、IT屋が持っていればよい。

「そんなことは、できない」と言うIT屋は信用しない。
実現するための、条件や制約を教えてくれるIT屋と付き合うことが必要。
条件や制約の対応を、IT屋と一緒に考えればよい。

人の課題、プロセスの課題、技術の課題を、
それぞれ紐解いてゆけば、
できないことは（ほとんど）ない。

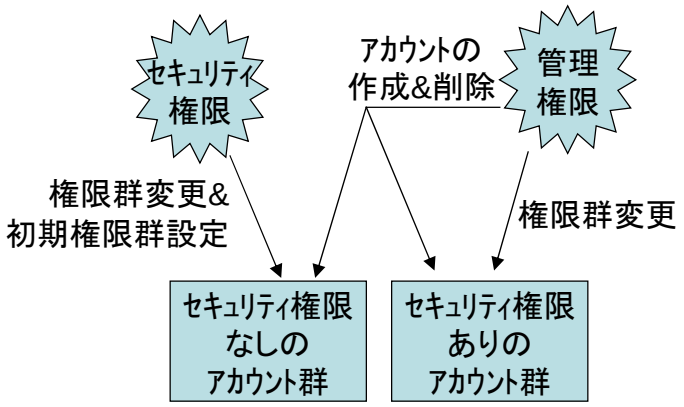
2010年11月20日 Copyright 1995-2010 佐藤慶浩 スライド 18

「わがまま」の練習
管理者による改変からの保護

yosihiro.com

デュアルロック

※管理権限とｾｷｭﾘﾃｨ権限は排他的にしか獲得できない



「わがまま」の練習
工場～製品納入経路での改変からの保護

yosihiro.com

トラステッド・ディストリビューション

・製品出荷時の管理アカウントのパスワードを固定

・アカウントのパスワード使用有効回数を１回に設定

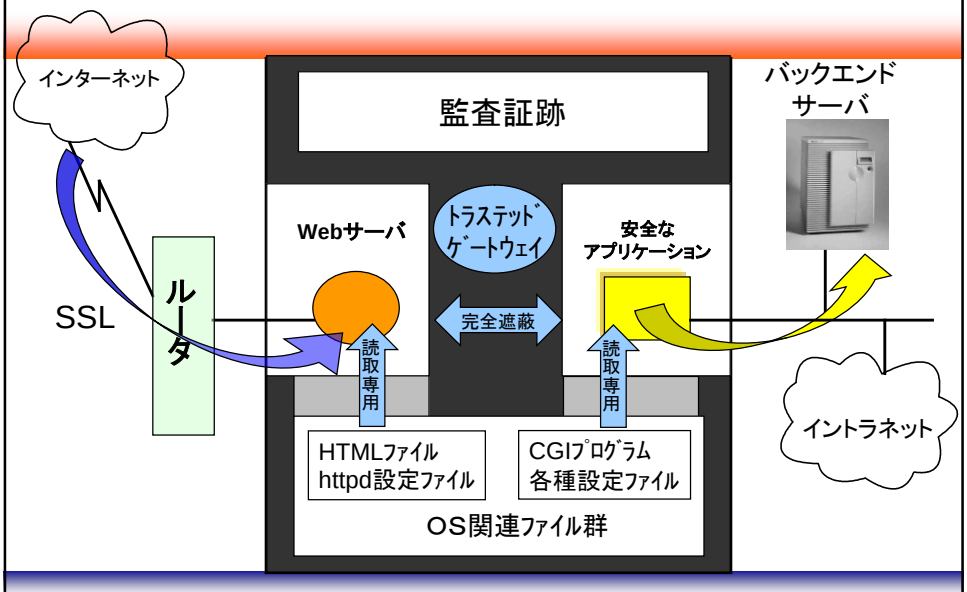
yosihiro.com

参考:
第三者機関によるセキュリティ評価・認証

ISO/IEC 15408

yosihiro.com

金融機関のウェブサーバの例



まとめ

yosihiro.com

・フォレンジック結果への2つの期待
・行為の記録を改変する動機と疑惑
・改変を防ぐ局面
・改変を防ぐ仕組みの例
・技術革新は「わがまま」から生まれる
・人・プロセス・技術で「わがまま」を叶える

紹介内容については、以下のコラムで基本的な考え方を寄稿してあります。
本日は、これの具体的な内容を紹介しました。

IDF研究会　第105号コラム「デジタルデータの改ざん防止とその保証」
http://www.digitalforensic.jp/expanel/diarypro/diary.cgi?no=234&continue=on
又は
http://bit.ly/aVcPIB

2010年11月20日　Copyright 1995-2010 佐藤慶浩　スライド 23

yosihiro.com

本日資料のダウンロード
http://yosihiro.com/speech/#2010-11-20

お問い合わせ
twitter
http://twitter.com/4416_310

2010年11月20日　Copyright 1995-2010 佐藤慶浩　スライド 24