今さら聞けない？
セキュリティ関連用語の解説

yosihiro.com

佐藤　慶浩

twitter.com/4416sato

発表者紹介

yosihiro.com
twitter 4416sato

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

社外の活動
- デジタルフォレンジック研究会　理事
- 情報ネットワーク法学会　副理事長
- (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
- JIPDEC　プライバシーマーク推進センター　客員研究員
- 杉並区　住基ネット運用監視委員会　委員
- など

前回からの つづき

yosihiro.com
twitter 4416sato

前回は、「IT屋に解決して欲しいことがあるのに、『できない』と言われたら・・・」という、お話しをしました。

今回は、原点に戻って、ついつい聞き流してしまう専門用語についての解説です。

なお、前回の発表内容は
http://yosihiro.com/speech/#2010-10-20
からストリーミング視聴できます。

発表内容

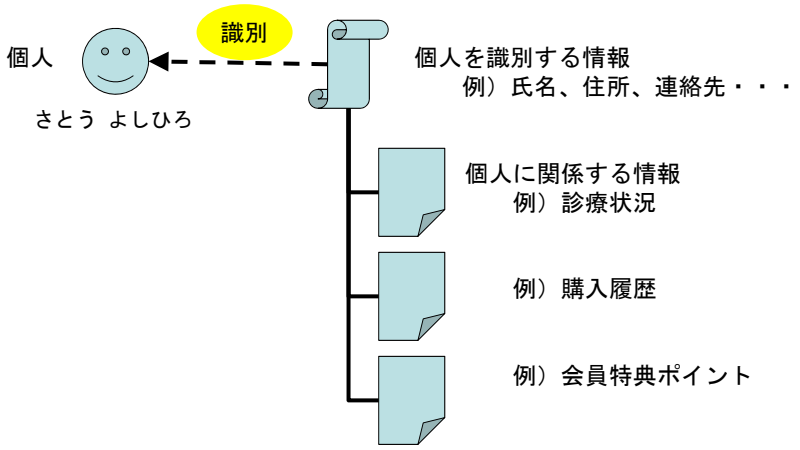
yosihiro.com
twitter 4416sato

- 匿名と仮名、識別(特定)と同定の違い
- 暗号化とパスワード保護の違い
- 秘密分散にすすめ
- 通信路としてのネットワークセキュリティ
- 認証（なりすまし防止）

匿名と仮名、識別(特定)と同定の違い

yosihiro.com
twitter 4416sato

・アイコンの説明

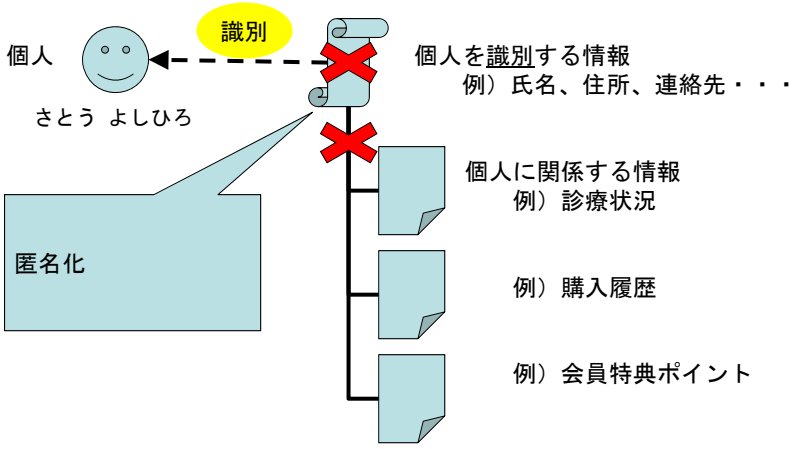


2011年11月22日 Copyright 1995-2011 佐藤慶浩 スライド 5

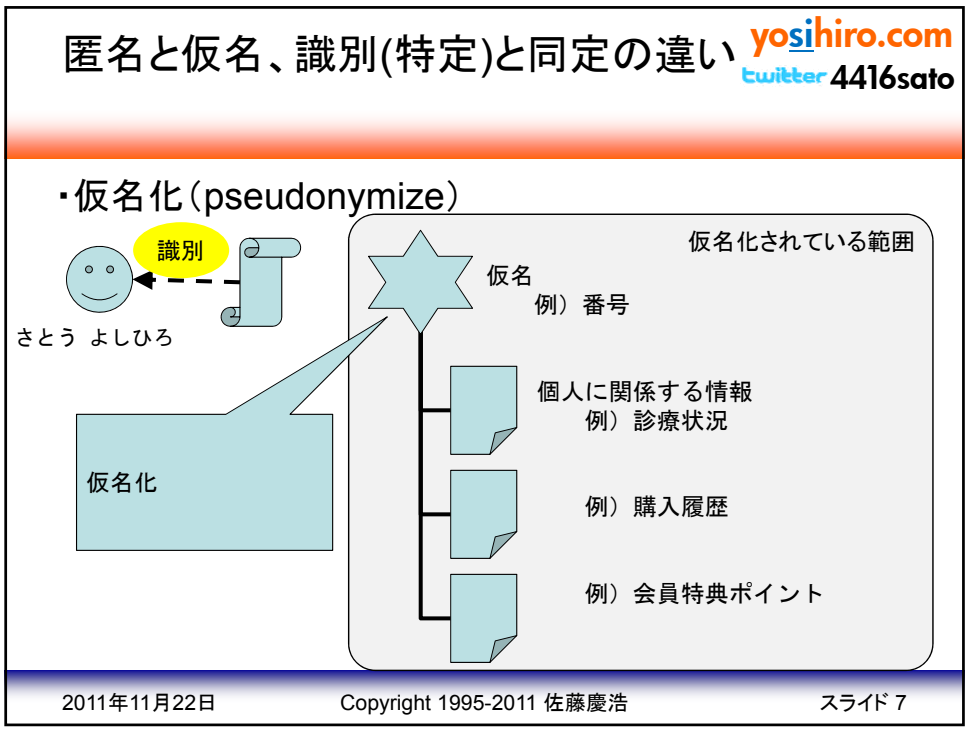
匿名と仮名、識別(特定)と同定の違い

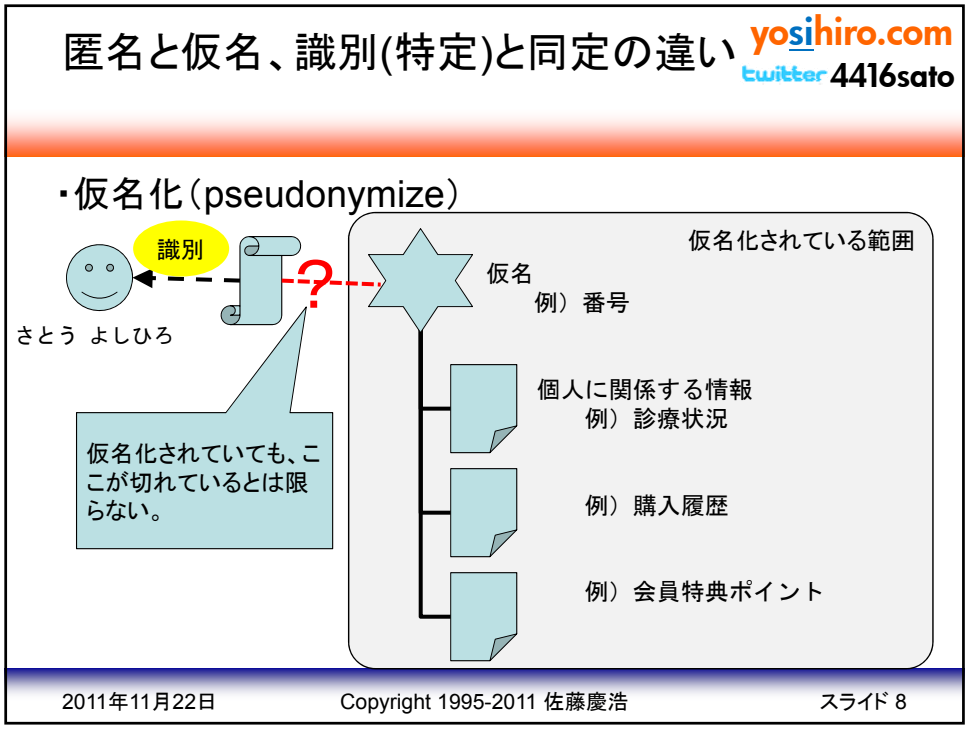
yosihiro.com
twitter 4416sato

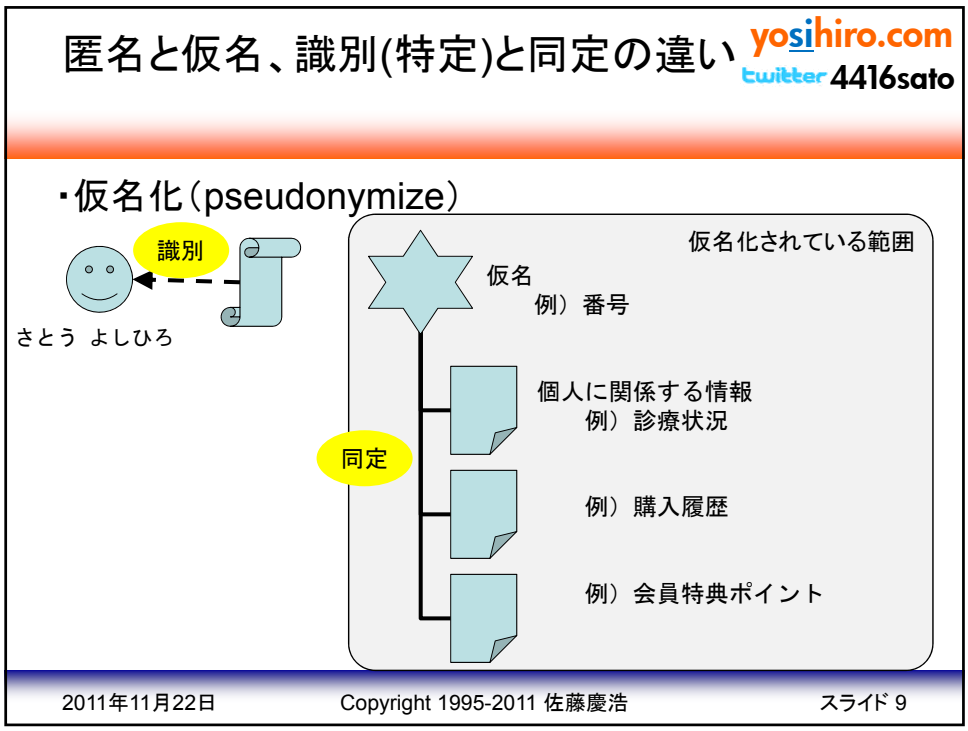
・匿名化（anonymize）

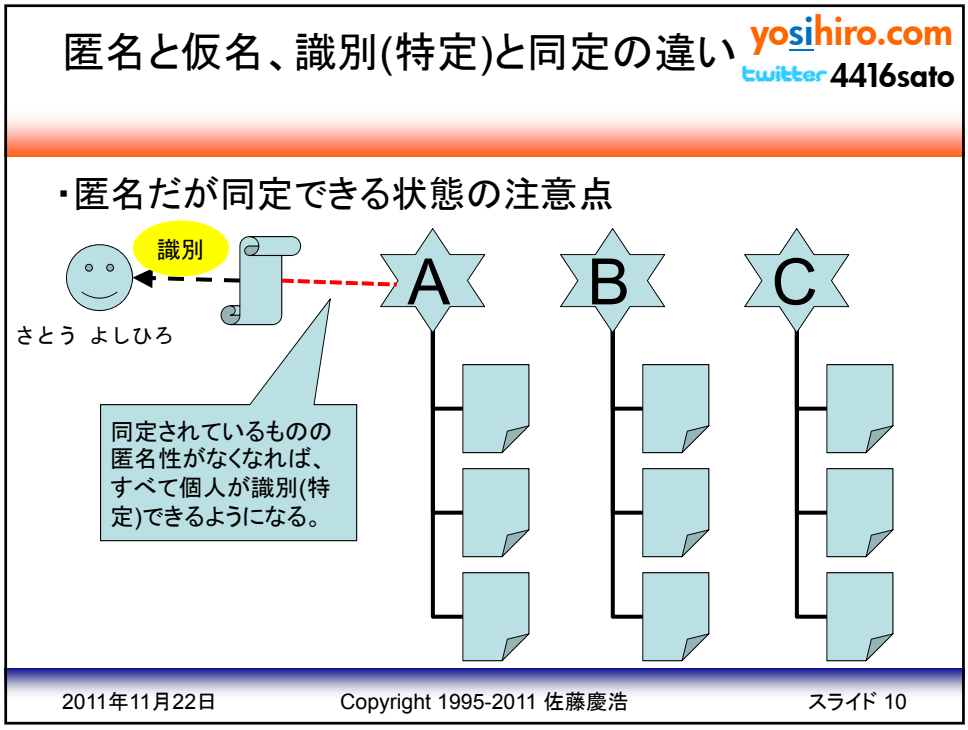


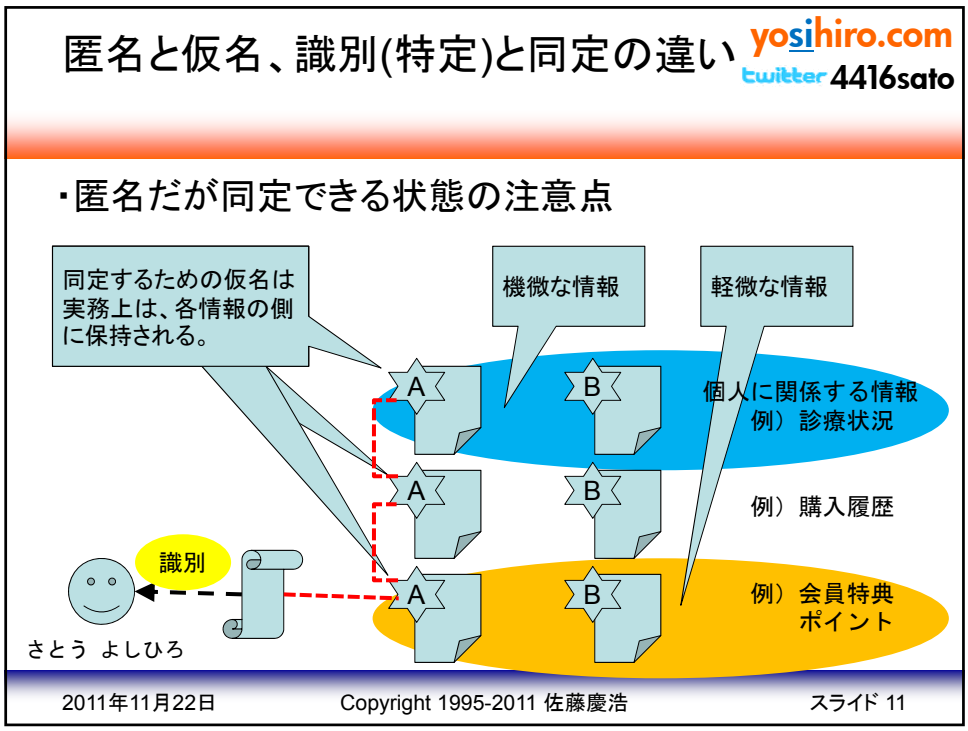
2011年11月22日 Copyright 1995-2011 佐藤慶浩 スライド 6

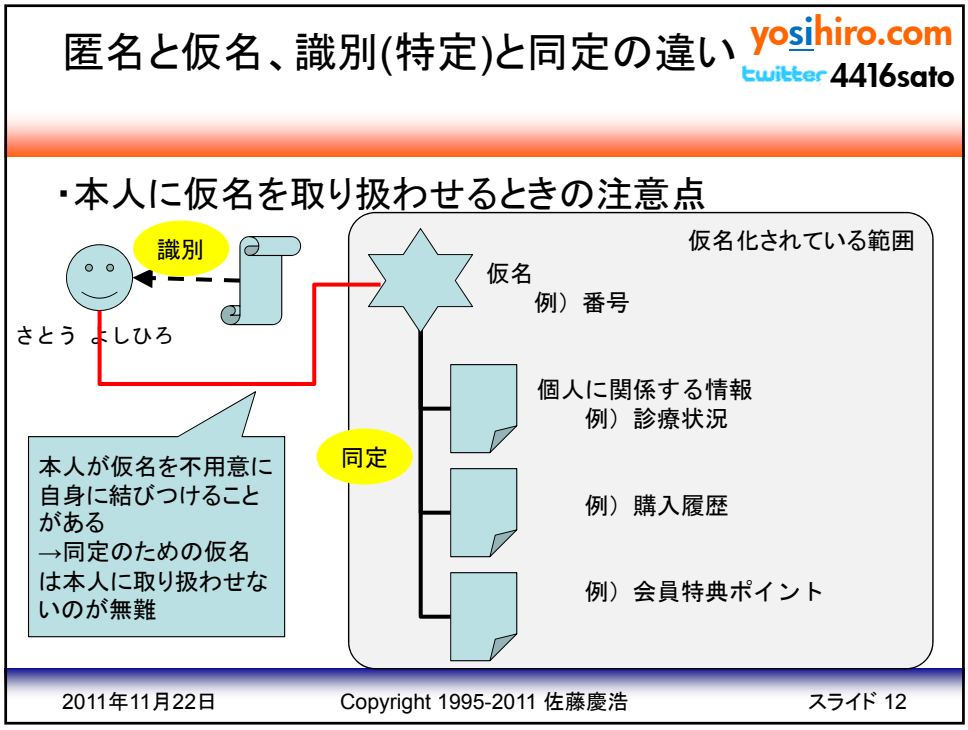

匿名と仮名、識別(特定)と同定の違い
yosihiro.com
twitter 4416sato
・仮名化（pseudonymize）
識別
さとう よしひろ
仮名化
仮名化されている範囲
仮名
例）番号
個人に関係する情報
例）診療状況
例）購入履歴
例）会員特典ポイント
2011年11月22日
Copyright 1995-2011 佐藤慶浩
スライド 7


匿名と仮名、識別(特定)と同定の違い
yosihiro.com
twitter 4416sato
・仮名化（pseudonymize）
識別
?
さとう よしひろ
仮名化されていても、ここが切れているとは限らない。
仮名化されている範囲
仮名
例）番号
個人に関係する情報
例）診療状況
例）購入履歴
例）会員特典ポイント
2011年11月22日
Copyright 1995-2011 佐藤慶浩
スライド 8


匿名と仮名、識別(特定)と同定の違い
yosihiro.com
twitter 4416sato
・仮名化（pseudonymize）
識別
さとう よしひろ
仮名化されている範囲
仮名
例）番号
個人に関係する情報
例）診療状況
同定
例）購入履歴
例）会員特典ポイント
2011年11月22日
Copyright 1995-2011 佐藤慶浩
スライド 9


匿名と仮名、識別(特定)と同定の違い
yosihiro.com
twitter 4416sato
・匿名だが同定できる状態の注意点
識別
さとう よしひろ
A
B
C
同定されているものの
匿名性がなくなれば、
すべて個人が識別(特
定)できるようになる。
2011年11月22日
Copyright 1995-2011 佐藤慶浩
スライド 10


匿名と仮名、識別(特定)と同定の違い
yosihiro.com
twitter 4416sato
・匿名だが同定できる状態の注意点
同定するための仮名は実務上は、各情報の側に保持される。
機微な情報
軽微な情報
A
B
個人に関係する情報
例）診療状況
例）購入履歴
例）会員特典ポイント
識別
さとう よしひろ
2011年11月22日
Copyright 1995-2011 佐藤慶浩
スライド 11


匿名と仮名、識別(特定)と同定の違い
yosihiro.com
twitter 4416sato
・本人に仮名を取り扱わせるときの注意点
識別
さとう よしひろ
本人が仮名を不用意に自身に結びつけることがある
→同定のための仮名は本人に取り扱わせないのが無難
同定
仮名化されている範囲
仮名
例）番号
個人に関係する情報
例）診療状況
例）購入履歴
例）会員特典ポイント
2011年11月22日
Copyright 1995-2011 佐藤慶浩
スライド 12

暗号化とパスワード保護の違い

yosihiro.com
twitter 4416sato

・質問：人に見られたくない物をしまうとしたら、どちら？
①ジュラルミンケースに、1桁の番号錠が付いている
②木箱に、5桁の番号錠が付いている

デモ

暗号化とパスワード保護の違い

yosihiro.com
twitter 4416sato

・頑強な箱には、頑強な錠前を付けないと意味がない。

参考：「暗号化」と「暗号で保護する」を使い分ける
http://bit.ly/angou-de-hogo
http://yoshihiro.cocolog-nifty.com/postit/2006/09/post_e9f0.html

秘密分散のすすめ

yosihiro.com
twitter 4416sato

・機密情報の安全な保管・移送に有益な技術

秘密分散
例）1080という数字を分散する

単純：10と80に分割する
　→10か80を知られると半分の情報がわかってしまう
ちょっと複雑：1080を20x54に分割する
　→20か54を知られると、その倍数であることがわかってしまう

2011年11月22日 Copyright 1995-2011 佐藤慶浩 スライド 15

秘密分散のすすめ

yosihiro.com
twitter 4416sato

・機密情報の安全な保管・移送に有益な技術

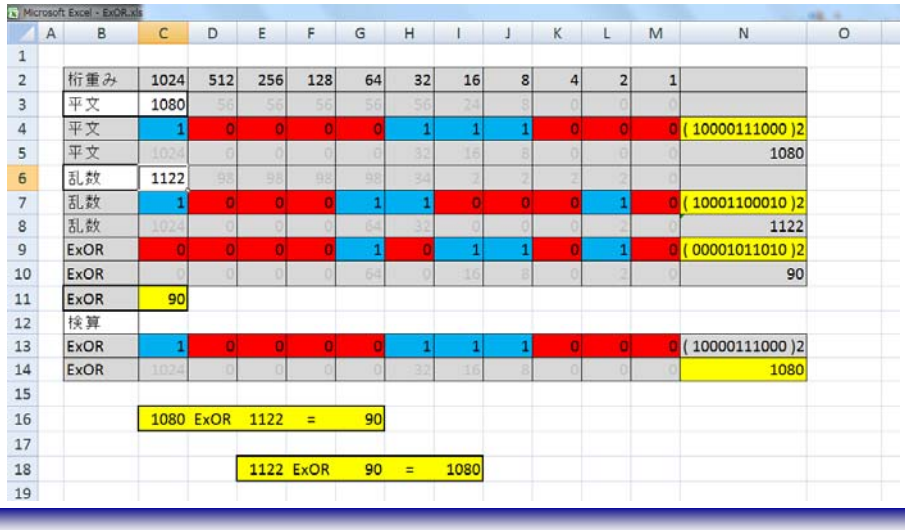
秘密分散
例）1080という数字を分散する

実際には2進数にして排他的論理和という計算をします
排他的論理和(Exclusive OR, ExOR)の特性
　A ExOR B = C ← Bを乱数にするとAがBとCに分散
　B ExOR C = A ← BとCからAを復元できる

2011年11月22日 Copyright 1995-2011 佐藤慶浩 スライド 16

秘密分散のすすめ

yosihiro.com
twitter 4416sato

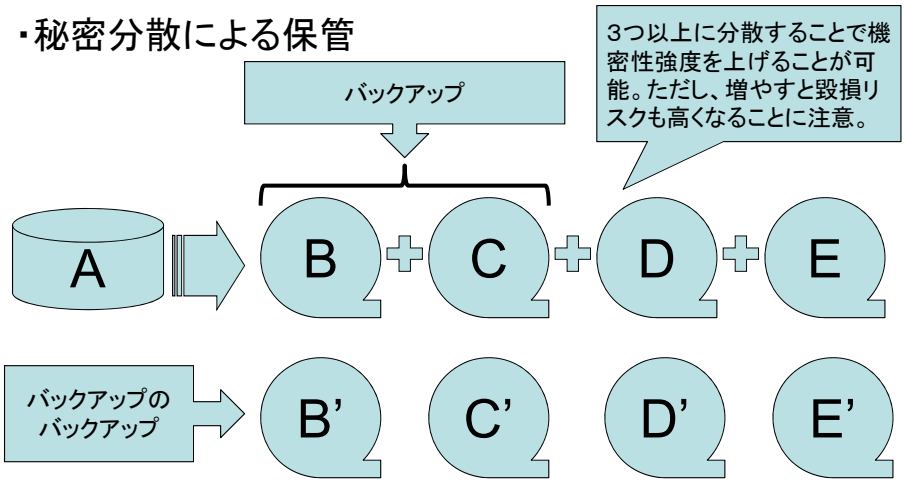


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1															
2		桁重み	1024	512	256	128	64	32	16	8	4	2	1		
3		平文	1080												
4		平文	1	0	0	0	0	1	1	1	0	0	0	(10000111000)2	
5		平文												1080	
6		乱数	1122												
7		乱数	1	0	0	0	1	1	0	0	0	1	0	(10001100010)2	
8		乱数												1122	
9		ExOR	0	0	0	0	1	0	1	1	0	1	0	(00001011010)2	
10		ExOR												90	
11		ExOR	90												
12		検算													
13		ExOR	1	0	0	0	0	1	1	1	0	0	0	(10000111000)2	
14		ExOR												1080	
15															
16			1080 ExOR 1122 = 90												
17															
18					1122 ExOR 90 = 1080										
19															

秘密分散のすすめ

yosihiro.com
twitter 4416sato

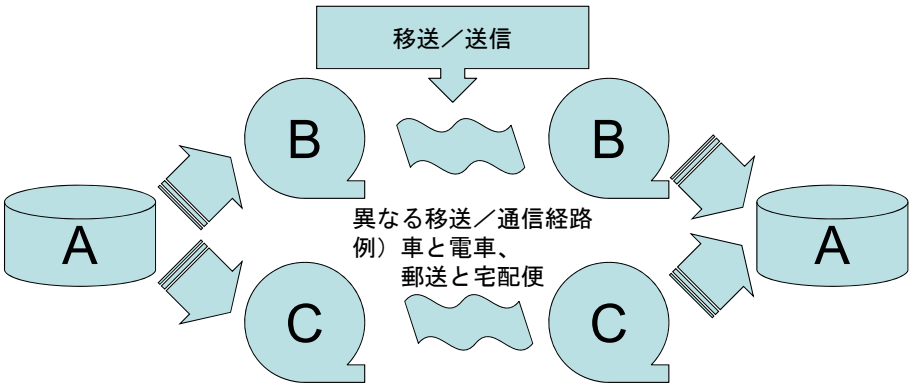
・秘密分散による保管



秘密分散のすすめ

yosihiro.com
twitter 4416sato

・秘密分散による移送／送信



Bの安全な移送／送信完了を待ってから
Cを移送／するのが望ましい→同じ経路も検討可

通信路としてのネットワークセキュリティ

yosihiro.com
twitter 4416sato

・ネットワークセキュリティポリシー
ポリシーの重要性（依存性＝借り物設計の危険性）
トラストとアントラストの区分け
例）境界防御から端末防御へ

・暗号による保護
機密性だけでなく完全性に活用

・秘密分散による保護
単一露呈に対する高い機密性(SPoF対策)

2011年11月22日 Copyright 1995-2011 佐藤慶浩 スライド 20

認証（なりすまし防止）

yosihiro.com
twitter 4416sato

・認証は、本来は第三者による証明のこと
　Aさんが Bさんを信じる為に Cさんによる証明を信じる
　このとき、Cさんが Bさんを認証した。という
・認証は、本来は certification
・authenticationは、本来は真正確認のこと
　AさんとBさんの問題（Cさんは必須ではない）
　AさんがBさんに予め渡したIDとパスワードでBさんの
　真正確認をすることは可能（その場合、Cさんは不要）

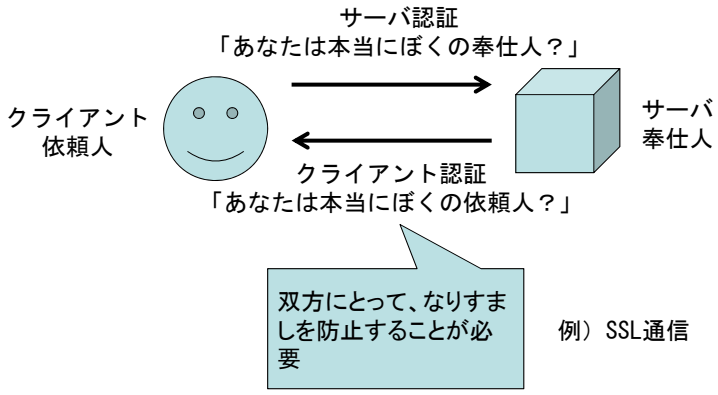
コンピュータ用語に限って
authenticationのことを認証と呼ぶ。（私見：本来、誤訳）

2011年11月22日　Copyright 1995-2011 佐藤慶浩　スライド 21

認証（なりすまし防止）

yosihiro.com
twitter 4416sato

・クライアント認証（client authentication）
・サーバ認証（server certification）

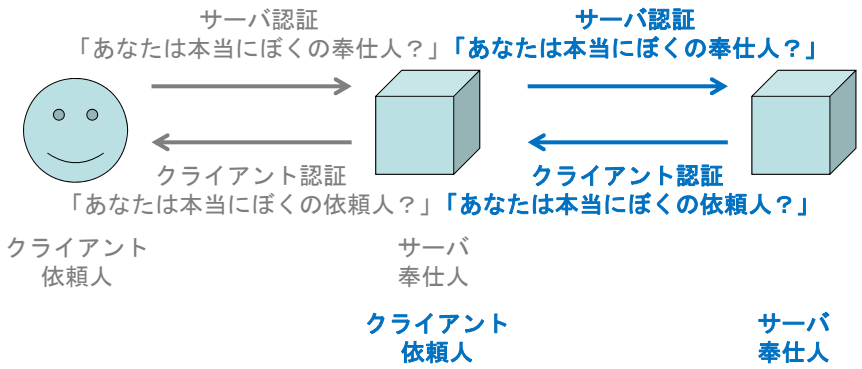


2011年11月22日　Copyright 1995-2011 佐藤慶浩　スライド 22

認証（なりすまし防止）

yosihiro.com
twitter 4416sato

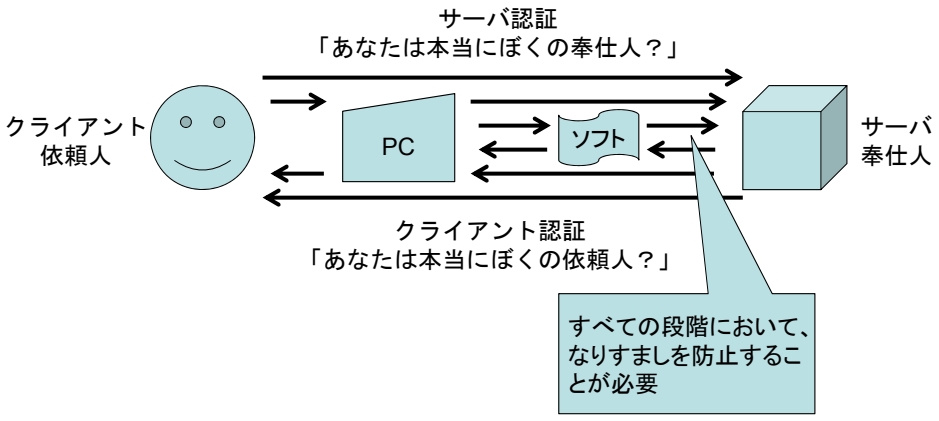
・クライアントとサーバの連鎖



認証（なりすまし防止）

yosihiro.com
twitter 4416sato

・認証の細分化



まとめ

yosihiro.com
twitter 4416sato

・匿名と仮名、識別(特定)と同定の違い
・暗号化とパスワード保護の違い
・秘密分散のすすめ
・通信路としてのネットワークセキュリティ
・認証（なりすまし防止）

異句同義語は、めったにありません。
・用語が異なれば、異なる意味を持っています。
・異なる用語を同義で解釈すると、不正確な理解により、誤った対策になります。

yosihiro.com
twitter 4416sato

本日資料のダウンロード

http://yosihiro.com/speech/#2011-11-22

お問い合わせ

twitter

http://twitter.com/4416_310