資料1

総務省自治体クラウド研究会　　2010年11月26日（金）

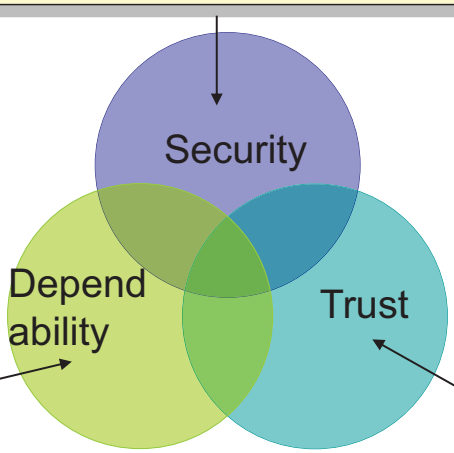
クラウドコンピューティングとセキュリティ

東京電機大学未来科学部教授
情報セキュリティ研究室
佐々木良一
sasaki@im.dendai.ac.jp

クラウドの安全・安心のための課題

①クラウドのセキュリティ対策
（a）クラウドへの攻撃　（b）クラウドを利用した攻撃

今回はここを対象



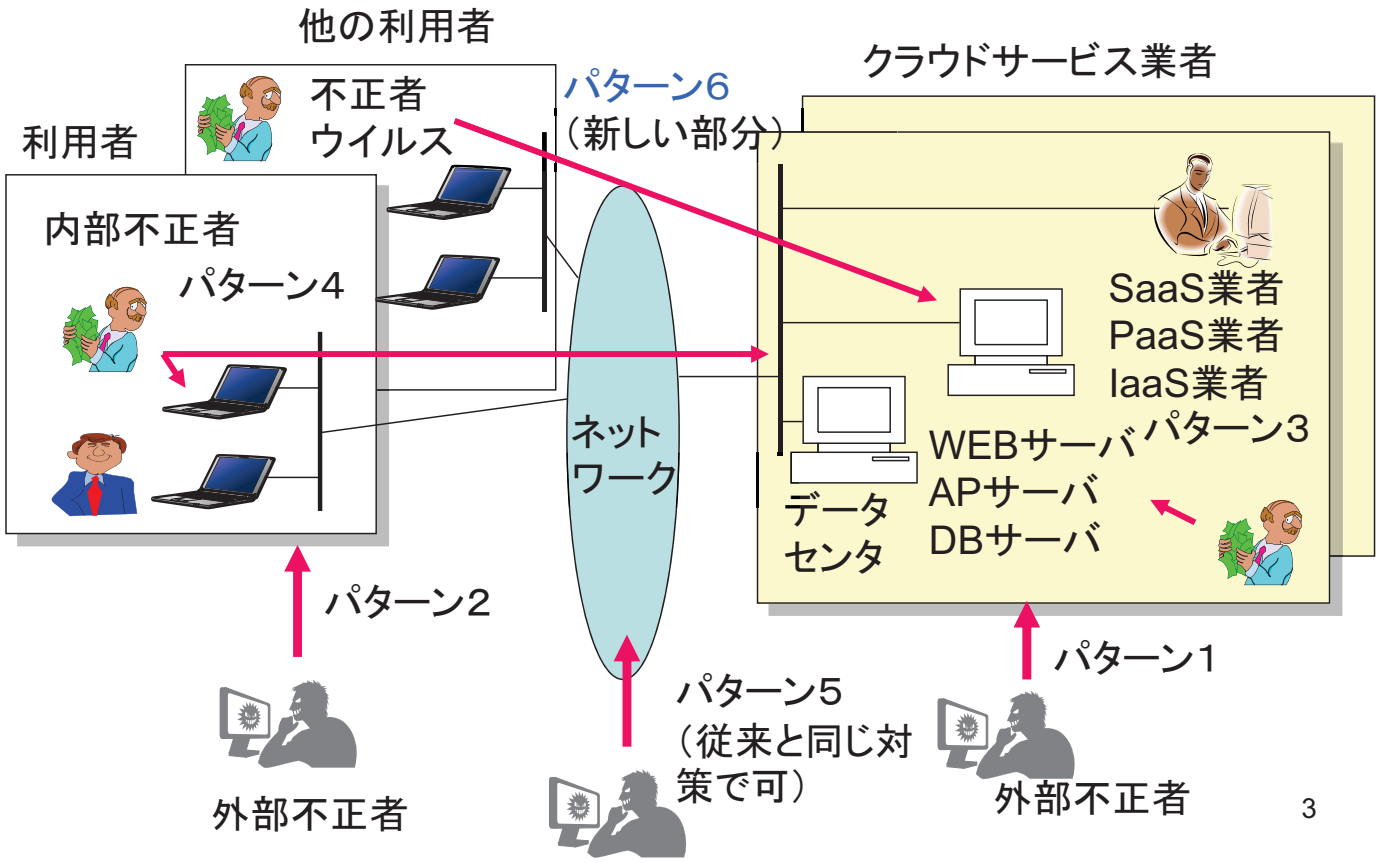
②バグや故障・災害などへの対策
（a）システムの停止
（b）データの喪失
（c）誤処理

付録1参照

③サービス提供者へのトラストの確保対策
（a）将来にわたりサービスしてもらえるか
（b）データの目的外使用や不正処理をしていないか
（c）政府などによる検閲のある国で処理してないか
（d）障害や不正があったとき調査などに協力してもらえるか

付録2参照

セキュリティに対する攻撃パターン

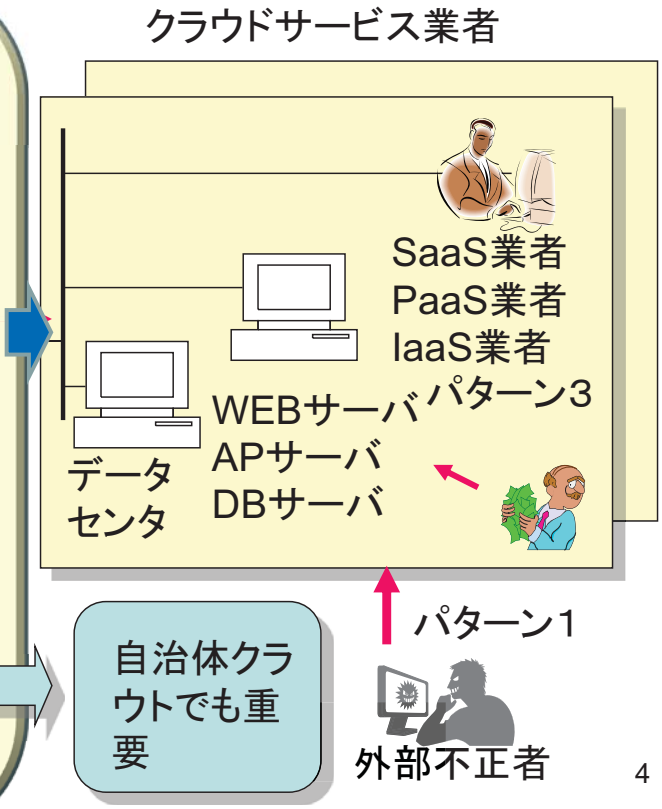


セキュリティ対策の特徴（1）

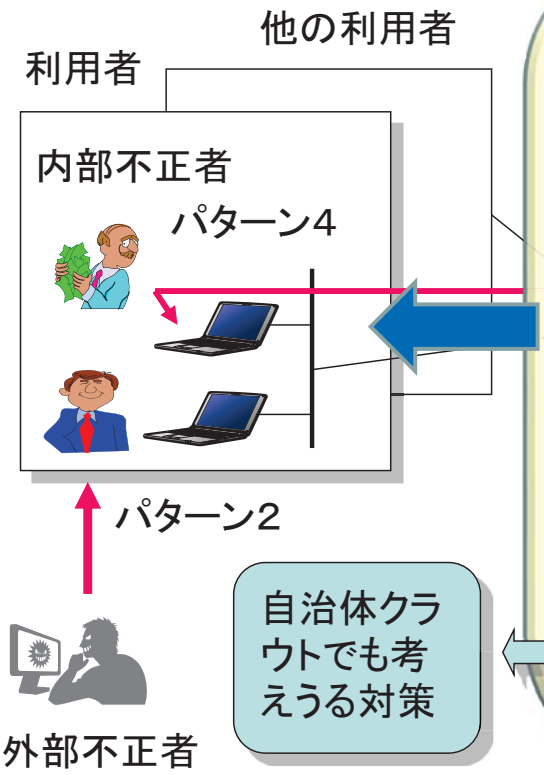
必要な主要対策
（a）入退出管理、監視カメラなどの物理的対策
（b）アクセス制御、暗号化、ウイルス対策、セキュリティ監視などの情報処理的対策
（c）セキュリティ管理、監査などの管理的対策　他

①基本的対策は同じだが、仮想環境下での共同利用者による直接的攻撃やウイルスによる攻撃（パターン6）は特殊

② 説明責任を果たすためログの収集などの対策は一般により強く要求される



セキュリティ対策の特徴(2)



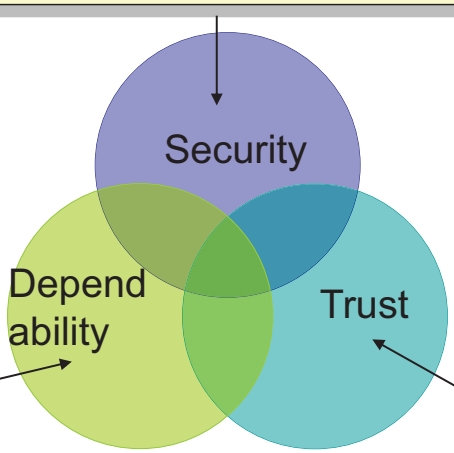
必要な主要対策
(a)セキュリティ監視
(b)セキュリティ教育　他

① これらの企業にもクライアントPCなどは残るが、それに対するセキュリティ対応能力はどんどん落ちる可能性があり、ここへの攻撃が問題になりうる。

② セキュリティトータルサービスのクラウド化:検疫ネットやセキュリティ監視、セキュリティ応急対応と組み合わせたEnd-Endセキュリティサービスのクラウド化も考えられる。

クラウドの安全・安心のための課題

①クラウドのセキュリティ対策
(a)クラウドへの攻撃　(b)クラウドを利用した攻撃



②バグや故障・災害などへの対策
(a)システムの停止
(b)データの喪失
(c)誤処理

③サービス提供者へのトラストの確保対策
(a)将来にわたりサービスしてもらえるか
(b)データの目的外使用や不正処理をしていないか
(c)政府などによる検閲のある国で処理してないか
(d)障害や不正があったとき調査などに協力してもらえるか

クラウドの悪用
（ボットネットの代替として悪用 ）

Amazon EC2を発信元とする攻撃は2008年から2009年にかけて、検知数自体は決して多くないものの、4倍（約70件＝＞約280件）という高い伸びを示している。

このような状況から、クラウドがボットネットの代替として悪用されている状況の一端をうかがい知ることができる。

LAC　新井 悠氏
http://itpro.nikkeibp.co.jp/article/COLUMN/20100412/346910/?ST=cloud

自治体クラウトでも考えておくべき項目　＝＞セキュリティ監視機能は重要

付録1

バグや障害・災害などへの対策

1．通常時対策
（1）機能更新時の変更管理
（2）分散環境におけるデータの同一性保持
（3）負荷変動への対応機能（分散処理技術、サーバ仮想化技術）
2．障害回避対策（フォルトアボイダンス）
（4）バグの少ないソフトの導入など
3．障害時対策（フォルトトレランス）
（6）計算機やネットワーク機能の多重化（フォルトトレランス）
（7）データのバックアップ（消去対応、アーカイビング）
（8）地震などに備えたバックアップセンターの設置（ディザスタリカバリー）
（9）BCP・BCMの推進

付録2

サービス提供者へのトラストの実現

＜信用したい項目＞

（a）将来にわたってサービスをしてもらえるか

（b）データの目的外使用や不正処理をしていないか

（c）希望する安全レベルが確保されているか

（d）政府などによる検閲のある国で処理してないか

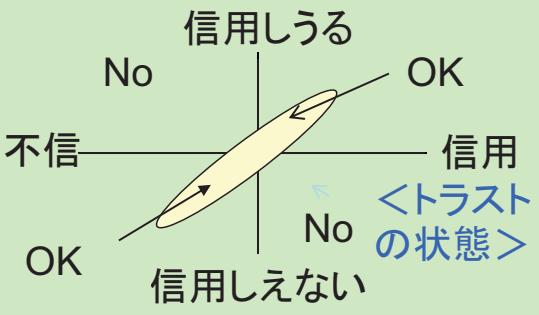
（e）障害や不正があったとき調査などに十分協力してもらえるか

＜トラストの実現のために＞

①利用者は左記の重要性をよく認識する

②トラストの状態と現実が一致

＜現実＞



③より高い信用が必要なら実際に信用できる状態を実現

＜実現手段＞

教育

契約

運用

仕組み

技術