重要な国家インフラにおいて、暗号化された環境が充分に管理されていない場合のリスクについて

Tatu Ylönen（タトゥ・ウロネン）
Founder and CEO
SSH コミュニケーションズ・セキュリティ

www.ssh.com

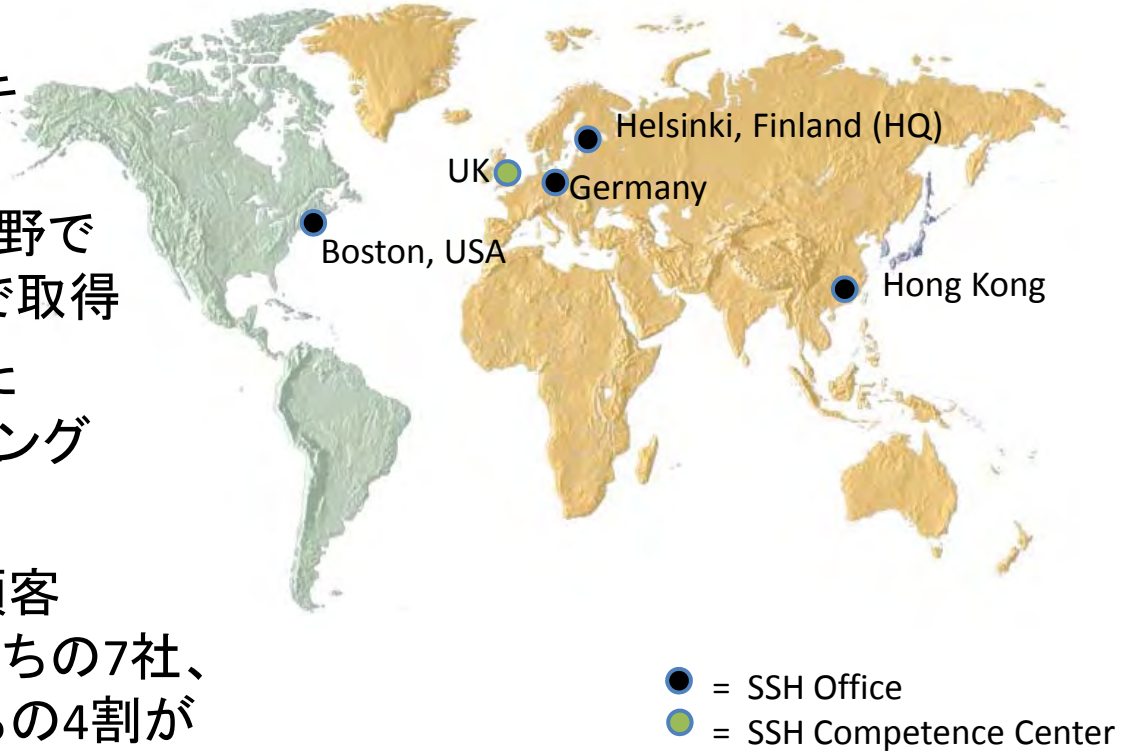
自己紹介

ssh® は、SSH コミュニケーションズ・セキュリティ社の登録消費用です。

- 1995年にオリジナルの SSH を開発、フリーソフトウェアとして公開
- 1995年に SSH コミュニケーションズ・セキュリティ社を創設
- 現在、同社のCEO 及び支配株主
- 他にも様々な会社を起業
- 商用、OpenSSH を含む大規模 SSH 環境のソリューション開発に深く関与

SSH コミュニケーションズ・セキュリティ社

- 1995年設立
- NASDAQ OMXヘルシンキ (SSH1V)上場
- サイバー セキュリティ分野で50を超える特許を各国で取得
- SSH プロトコルを基にしたソリューションのリーディングカンパニー
- 全世界に3,000以上の顧客
  -> フォーチュン10社のうちの7社、フォーチュン500社のうちの4割が同社製品を採用



Secure Shell (SSH)の誕生

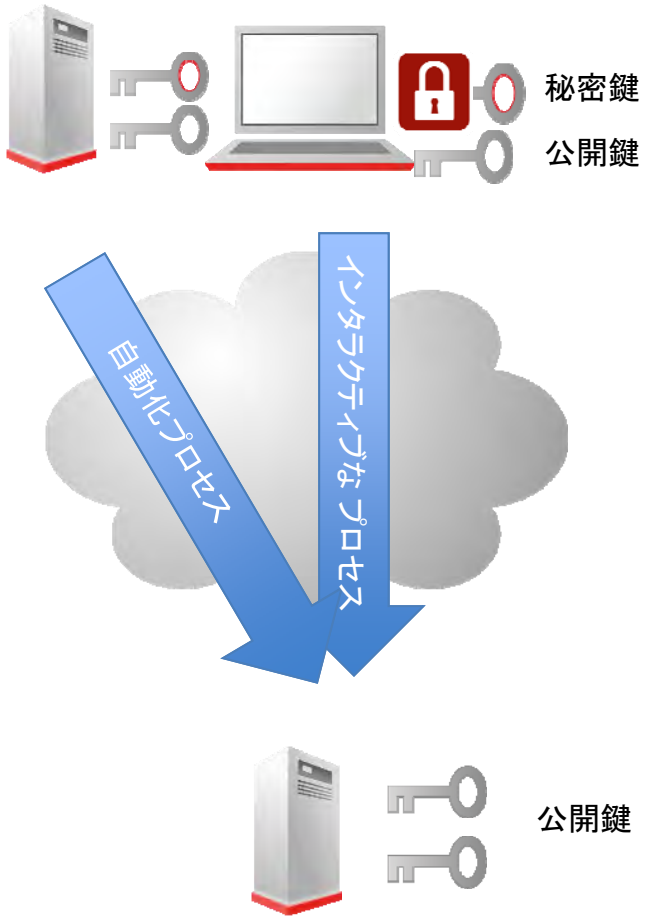
- 1995年ヘルシンキ工科大学の研究員時、パスワード盗聴による攻撃で同学内ネットワークがハッキングされる。
- 同様の攻撃に対抗するために、telnet、ftp、rlogin 及び rcp の置き換えになるツールとして、Secure Shell (SSH) プロトコルを開発 。
- SSH プロトコルの最初のバージョンを、1995年7月にインターネットコミュニティにリリース。
- 1995年末までの半年で、50カ国、2万ユーザーがSSHを使用。
- 2000年までの5年間で、推定200万ユーザーがSSHを使用。
- 今日、世界中の企業、政府機関、調査研究機関、大学等で、ネットワークの内部及び外部において、機密情報の転送をセキュアにするのに広範囲に使用されている。

Secure Shell はどこで使用されているのか

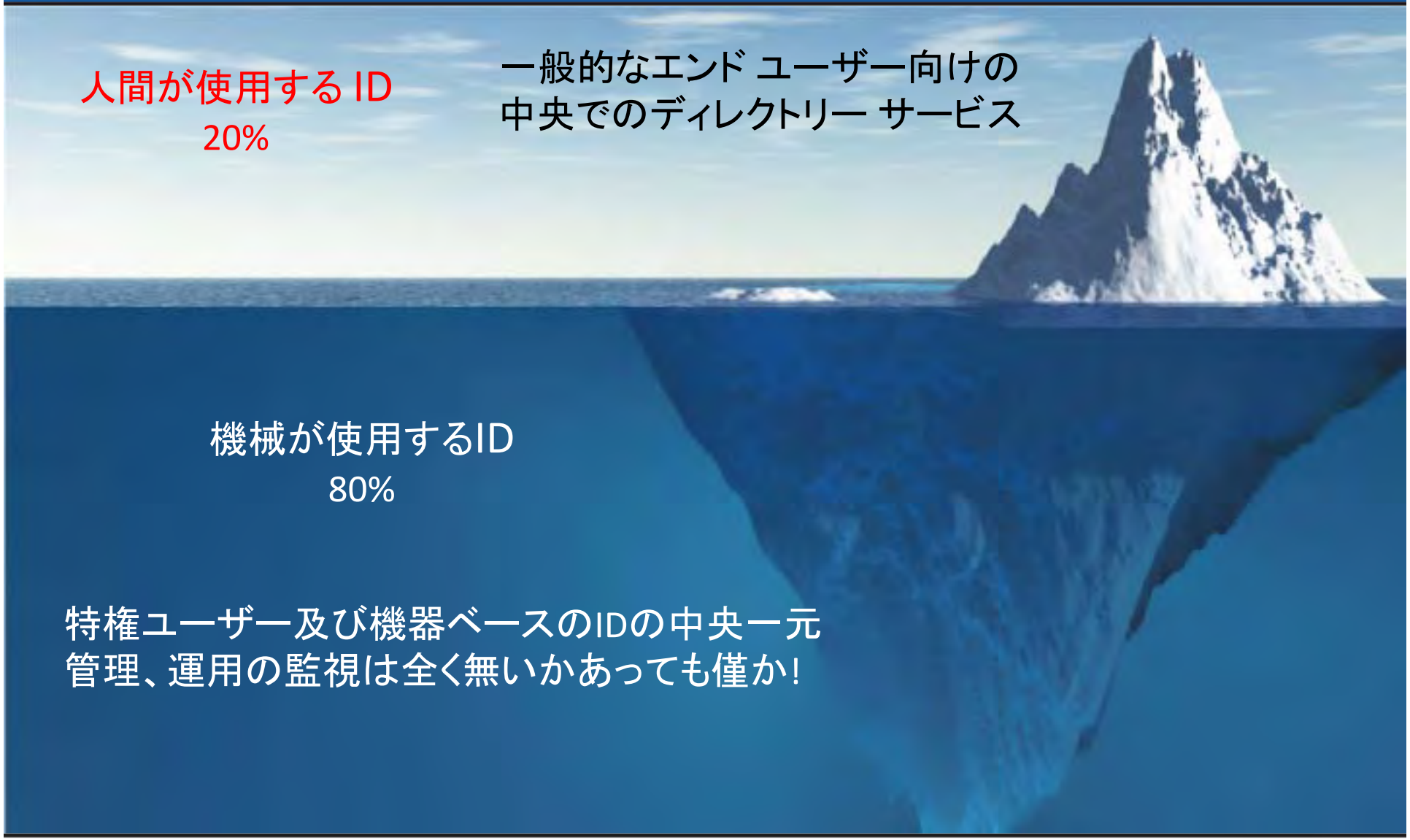
- SSH プロトコルは広範に使用されている:
  - システム管理者による利用
  - システム間の自動化されたプロセスでの利用
- SSH プロトコルの使用される場所:
  - 各種 Unix/Linux コンピュータ
  - クラウド コンピューティング環境
  - 世界半数以上のウェブサイト
  - xDSL モデム、ルーター、テレコミュニケーション システム、その他ネットワーク機器の大半
- SSH プロトコルは1995年以来使用され続け、その使用頻度は拡大していくのみ。
- SSH プロトコルはセキュアなプロトコル。
- しかし、企業・組織でのユーザー認証用の鍵の取り扱いが正しく行われていないのが現状。

Secure Shell 通信で認証に使用する鍵

- 鍵ペアは、公開鍵と秘密鍵からなる
  - 秘密鍵とは「ID鍵」のこと。これは人もしくはプロセスが行うログイン要求に対するIDの確認に使用される。
  - 公開鍵とは「承認済み鍵」のこと。秘密鍵の持ち主にどのレベルのアクセス権を提供するかを決める。
- 自動化プロセス（バッチ処理等）に使用
  - 定期的な自動ファイル転送やその他人手の介在が難しいタスクの認証を実行。
- インタラクティブ な接続に使用
  - 秘密鍵はパスフレーズで保護することも可能。



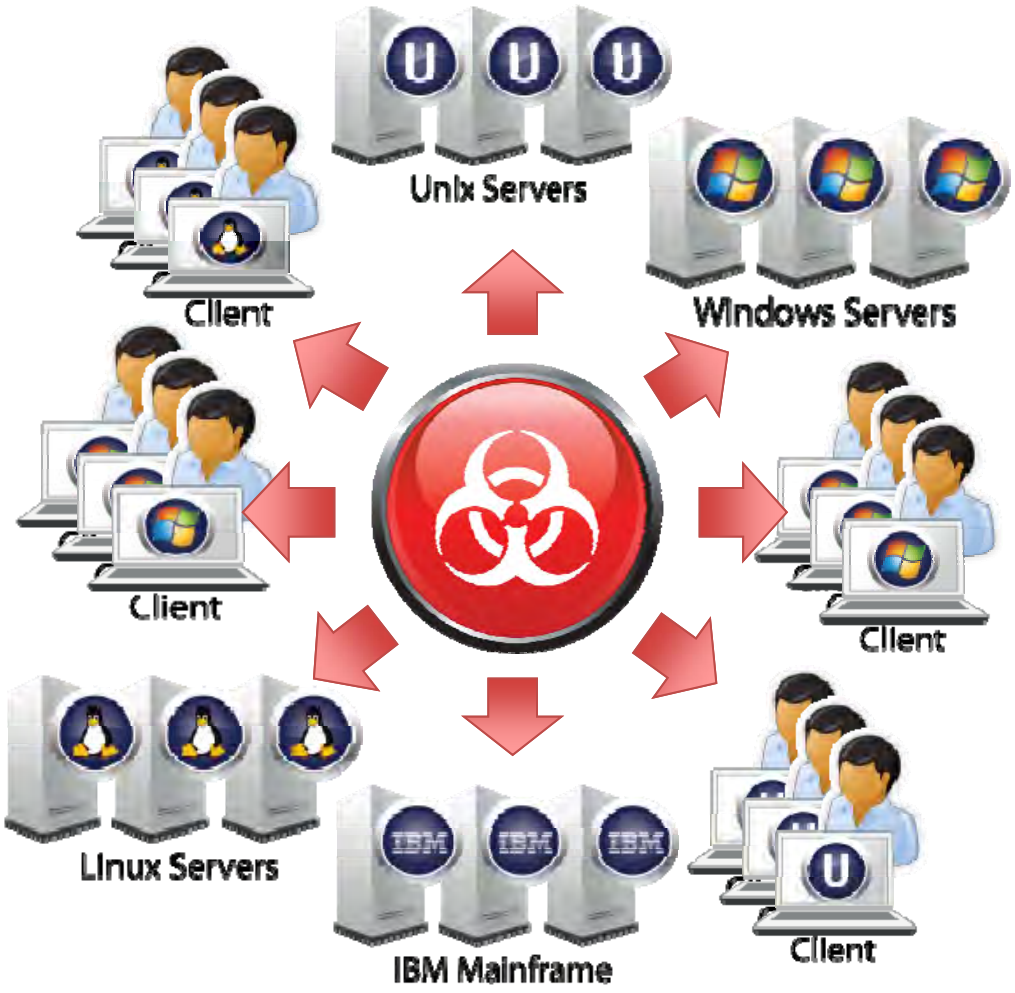
機器が持つIDの激増



承認済み鍵の正しくない管理による脆弱性

- 誰が何にアクセスできるかが不明
- 今、誰が何にアクセスしているかが不明
- 特権アクセス管理システムを迂回
- 承認済み鍵を追加することによるバックドア隠し
- ビジネスパートナーによるファイル転送以外の
  意図しないアクセス (コマンド制限の欠如)
- 文書化されていない環境を跨ぐ接続:
  - 開発/テスト環境 → 本番環境、影響度の低いシステム →影響度の高いシステム、
    PCI 対象外システム → PCI 対象システム
- 従業員又は契約社員が退職する際にアクセスが削除されていない
- 境界を破られた際に拡散が早い (マルウェア、APT) – 重大問題!
- 多くの企業・組織が侵害を受けた後でさえも鍵を実用的に交換する能力がない
- PCI DSS などの政府・業界規制のコンプライアンスが不十分

サイバー兵器及び APT（標的型攻撃）



- ほとんどの企業・組織が、平均 8 ～100+ 個の SSH 鍵を各 Unix/Linux サーバーにアクセスできるよう設定している
- これら鍵はほとんどの場合、高レベルの管理者アクセスを許可
- 鍵ベースアクセスのほとんどが高密度メッシュ構成であるため、攻撃者は組織内のほとんど全てのサーバーにたちまちアクセス可能となる
- 攻撃者がサーバー貫通後、他の攻撃ベクターを使って、「root」（高レベル管理）特権を入手した場合、潜在的なリスクはさらに増大

実例

- 大手金融機関
  - 10,000台以上のサーバーがネットワークに存在
  - 150万個の SSH ユーザー鍵を検出
  - そのうち、10%（150,000個）の鍵がルートアクセスを所有
  - MAS（Monetary Authority of Singapore）及びSOX 監査に失敗
  - 現在、SSH 鍵の運用の適正化のためのプロジェクトを弊社と実行中

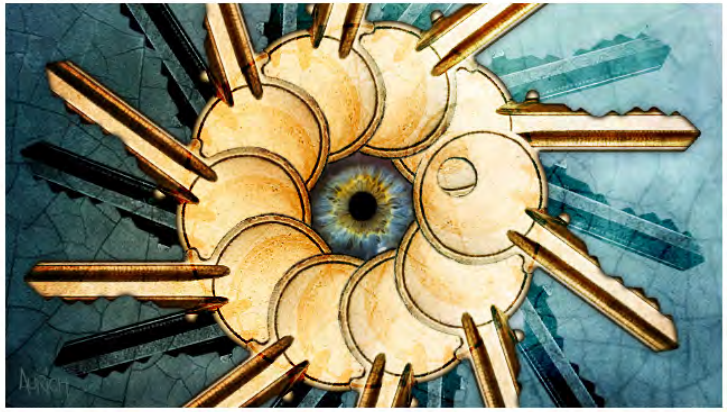
世界での侵害及び漏洩

Former Hostgator employee arrested, charged with rooting 2,700 servers

Prosecutors: Backdoor and digital key gave him near unfettered access.

by Dan Goodin - Apr 19 2013, 7:51pm FLEDT

BLACK HAT INTERNET CRIME 69



COMPUTERWORLD

White Papers Webcasts Newsle

Topics News In Depth Reviews Blogs Opinion

Security Application Security Cybercrime and Hacking Cyberwarfare Malware and Vulnerabilities Mobile Security Privacy

Home > Security

News

Hackers break into two FreeBSD Project servers using stolen SSH keys

Users who installed third-party software packages distributed by FreeBSD.org are advised to reinstall their machines

By Lucian Constantin

November 19, 2012 06:29 AM ET 3 Comments

theguardian

News Sport Comment Culture Business Money Life & style

News Technology Software

GitHub users warned over security risk

Search tool on programming site turns up SSH keys, which could allow attackers to hack sites or alter programs silently

by Michael Mimoso Follow @mike_mimoso July 8, 2013 , 5:18 pm

標準化のイニシアティブ

- PCI DSS 3.0：SSH 鍵ベースのアクセスに関して、様々な要求を規定 (例、カード会員データのセキュリティに影響を与える全てのシステムが規定範囲対象）
  - コンプライアンスに対応するための各種ツールを公開中：http://pages.ssh.com/pci3.html
- シンガポール金融管理局のテクノロジーリスク管理ガイドライン：SSH 鍵ベースのアクセス管理を要求 (例、開発/テスト環境→本番環境の分離)
  - ホワイトペーパーを公開：http://pages.ssh.com/mas.html
- Sarbanes-Oxley (SOX)：誰が財務データにアクセスできるかを管理することを要求
- FISMA及びNIST SP 800-53：様々な方法でのSSH鍵管理を要求
  (NIST Interagency Reportがまもなくリリース!)
- FERC/NERC CIP ルール：誰が重要インフラの設定権限があるかを管理することを要求
- HIPAA：誰が患者データにアクセスできるかを管理することを要求
- IETF draft-ylonen-sshkeybcp-01.txt：ベストプラクティスガイドラインを提供
  (更新待ち!)

殆どの法令規制標準は技術に関する大まかな記述にとどまり、「SSH」と明確に記述はしていないが、SSHの鍵はシステムレベルのアクセスを提供している。

コンプライアンスのためのロードマップ

1. コントロールされた鍵プロビジョニングプロセスを確立する
2. レガシーの鍵の設定を是正
3. 自動化およびインタラクティブなアクセス双方に、鍵の継続的な監視・管理を確立する

1. コントロールされた鍵プロビジョニングプロセスを確立する

- 鍵の新規作成の際には必ず承認手順を踏む
  - アクセス権の付与は必要なものに限り、監査が可能な状態にする
- 承認済みの鍵は、root権限が必要なディレクトリに置く
  - 承認プロセスを簡単にバイパスしてしまう抜け穴や勝手なアクセスの委譲を防ぐ
- 承認された鍵要求に関しては、アクセス権限付与を自動化する
  - セキュリティの強化、エラー・運用コストの削減
- 承認された各鍵の使用目的及びそのオーナーを文書化する
  - 使用目的が不明の場合、アクセス権の削除ができない。また鍵の必要事項について誰に確認すればよいかを明確化。
- 鍵のコマンド制限を強制
  - マルウェアやATPでの攻撃の拡散を限定

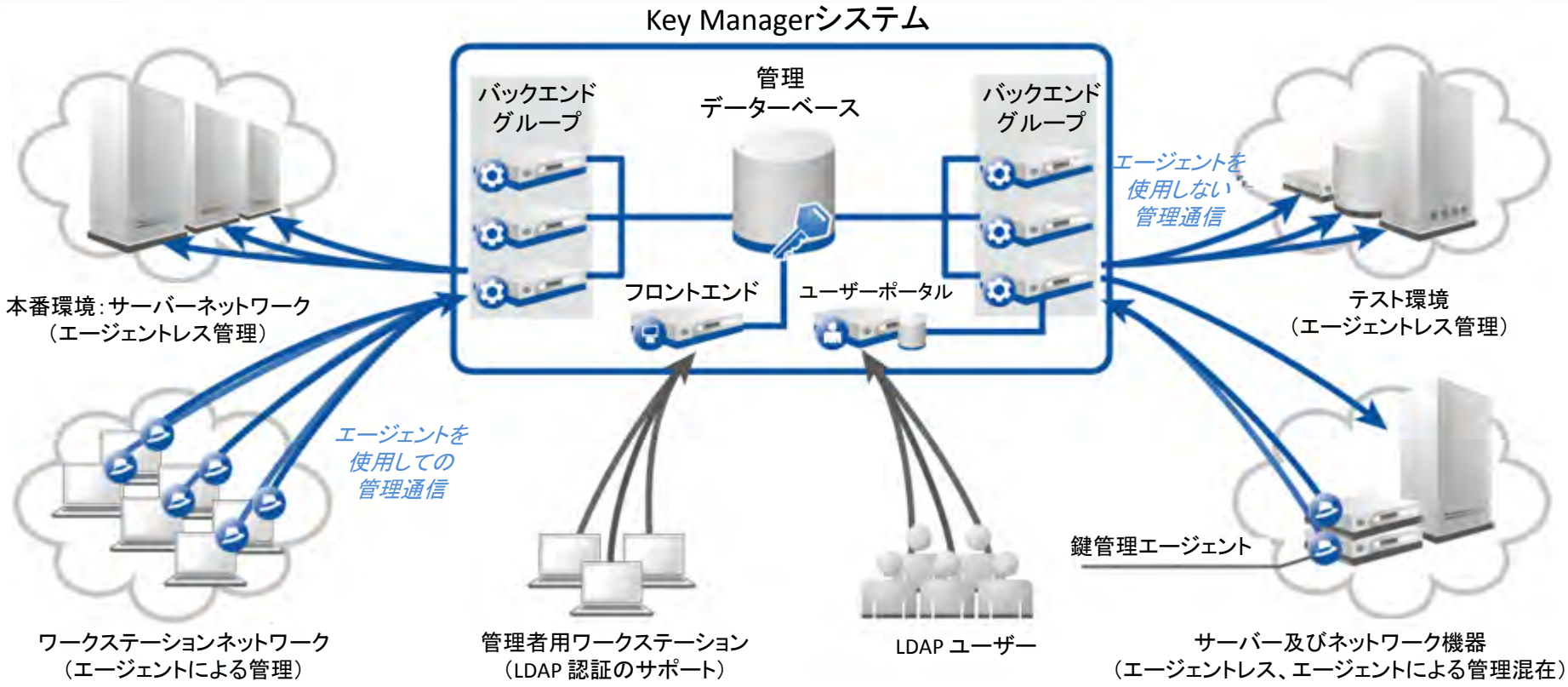
2.レガシーの鍵の設定を是正

- **鍵の検出及び利用の監視**
  - 鍵の使用を監視し、どの鍵がどこから使用されたかを確認する
- **鍵の数を減らす**
  - 使用されていない鍵を削除する
  - ポリシー違反や違反してネットワーク境界を越える鍵を削除する (例、開発環境 → 本番環境)
  - 鍵がビジネスにとって重要な場合バックオフオプションを常に維持することが必要！
- **環境内で使用している鍵のビジネス上の目的とオーナーを明確にする**
  - アプリケーションチームからの承認を得る
  - 目的、オーナー、コンプライアンスやメンテナンスに対する承認を記録する
  - ビジネス上の使用目的が無い鍵が見つかった場合は削除する
- **環境内で使用している鍵にはコマンド制限を行う**
  - マルウェアや ATP での攻撃の拡散を限定

3.鍵の継続的な監視・管理

- **ホストをスキャンし鍵を検出し、鍵のアクセスに関する操作を syslog で監視する。**
  - 未承認鍵や未承認鍵を使用したアクセスに関しては直ちに警告
- **定期的な鍵の更新の実施**
  - コピーされた鍵でのアクセスを最終的には確実に中断する
    - 情報漏えいや侵入事件発生後には非常に重要！
- **鍵ベースのアクセスにおいても特権アクセスの監査を実施する**
  - 自動運用（バッチ処理等）に使用する鍵を手動で担当者が使用している場合がある！
  - 特権アクセスの監査を逃れるような利用を防止する
  - 鍵を使った攻撃をできるだけ未然に防止する

ソリューション アプローチ:
中央でのSSHアクセス管理



中央データーベース:
- 全ての設定及び鍵情報を集積

バックエンド:
- ホストとの接続
- ジョブの実行

管理エージェント:
- エージェントベースの展開での接続

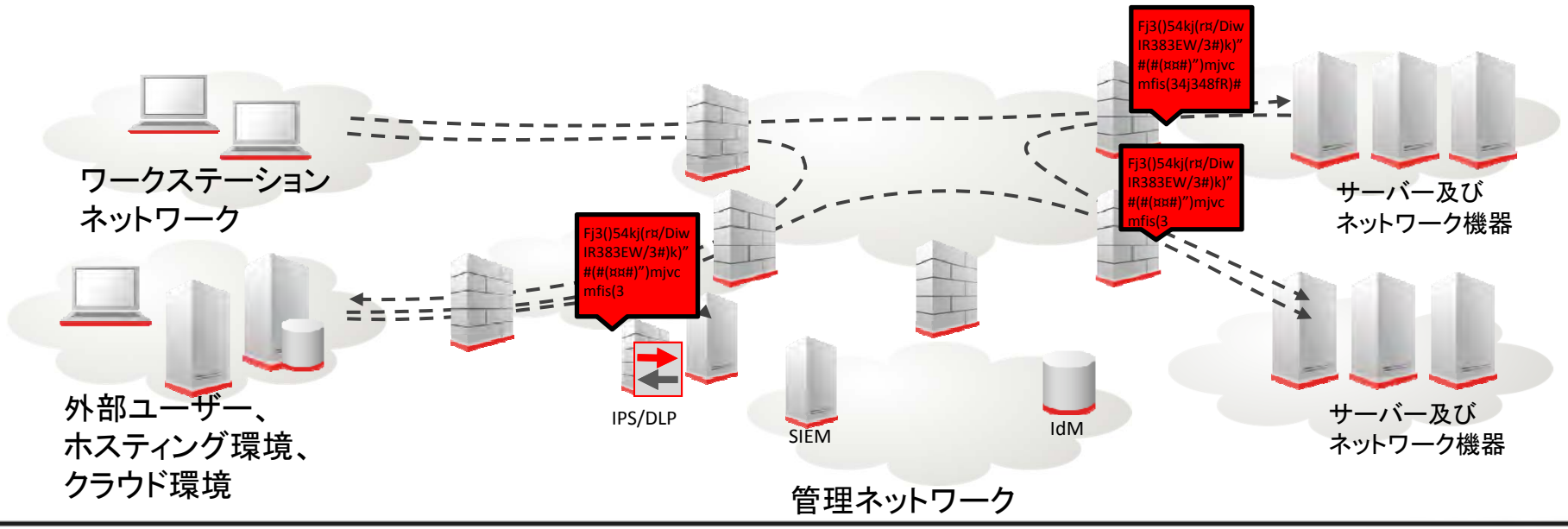
フロントエンド:
- 設定及びレポート用のウェブベースのユーザーインターフェイス
- 設定及びレポート用の API を統合

ユーザーポータル:
- エンドユーザー及びアプリケーションオーナー等向けのウェブベースポータル
- 外部の鍵及びユーザー用の外部の鍵インポート機能
- アクセス要求/削除/制限の実行、サインオフ及び承認プロセス

セキュリティの矛盾: セキュリティ対可視化

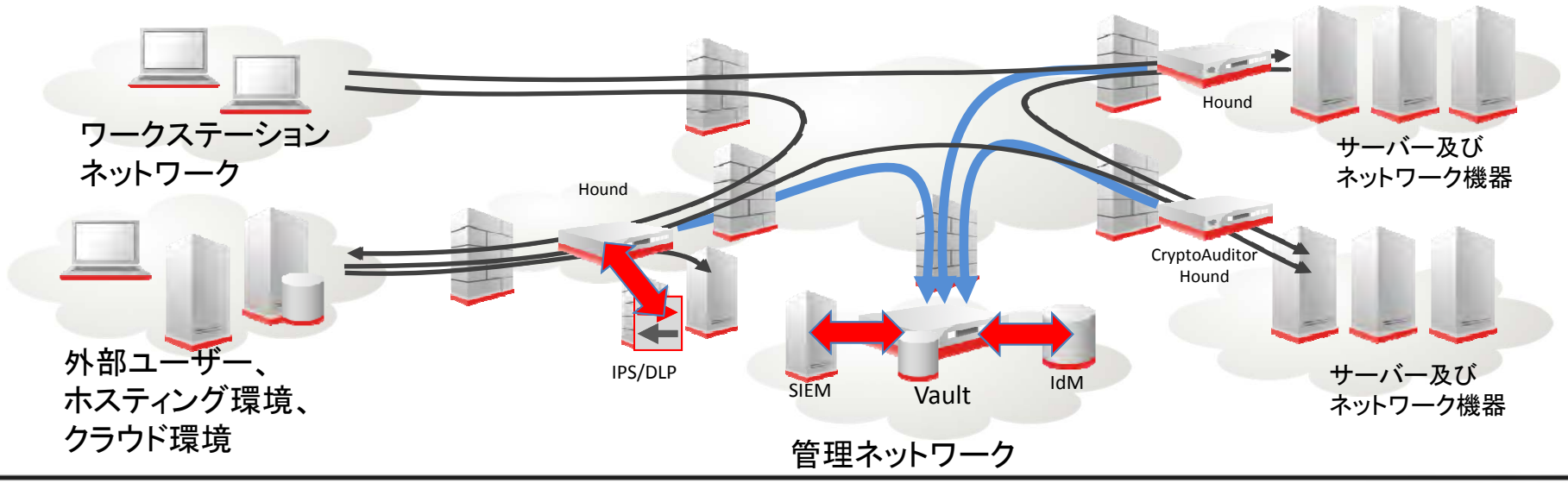
- ビジネス環境における、暗号化されたリモートシステムアクセスとデータ転送:
  - 内部から内部
  - 内部から外部
  - 外部から内部
- 「暗号化」されているということは、実際の通信内容がわからない

- ユーザーのコマンドや操作をどのように追跡、監査するか
- 社内外に流れるデータをどのように検証解析するのか



ソリューション アプローチ:
信頼でき、透過的な監査のポイント

- インライン、エージェント不要、気づかれることなくオンザフライでキャプチャ
- 一元化された管理、レポートおよび暗号化された監査証跡の保管
- 全てのモジュールはバーチャルおよびハードウェア・アプライアンスで提供
- 通信をそのとおりに監査、再生
- リアルタイムのインデックス作成、検索およびレポート
- チャネル及びコンテンツの予防コントロール
- DLP、IPS、SIEMとの統合
- 導入による影響は最小限: ユーザ体験、業務プロセスまたは環境に変更が不要



まとめ

- 大規模な Unix/Linux 環境がある企業・組織は、管理されていない承認済み鍵という重大なセキュリティ及びコンプライアンスの問題を抱えています。
- この問題の範囲及び影響はまだ広く理解されていません。
- 誰がどのシステムや情報にアクセスできるかを知っていることは情報セキュリティにとって重要です。これなしでは機密性、完全性、継続性を維持することはできません。
- これは暗号化アルゴリズムやそのサイズの問題ではなく、アクセスに関する問題です。
- より詳細な情報は、下記URLを参照下さい。
  - http://tools.ietf.org/id/draft-ylonen-sshkeybcp-01.txt

ありがとうございました

www.ssh.com

Tatu Ylönen（タトゥ・ウロネン）
Founder and CEO
SSH コミュニケーションズ・セキュリティ